ivanti

ISEC-Help

ivanti

CONTENTS

1. **Welcome to Ivanti Security Controls** 11
2. **What's New?** 13
   - 2.1. Linux Contentless Patching 28
3. **Evaluation Guide** 30
4. **Installation** 31
   - 4.1. System Requirements 32
   - 4.2. Architecture Considerations 46
   - 4.3. Obtaining the Software 47
   - 4.4. Installing the Prerequisites 48
   - 4.5. SQL Server Pre-Installation Notes 49
   - 4.6. Performing a New Installation 51
   - 4.7. Installing the Console from a Command Line 58
   - 4.8. HTTP Proxy Post-Installation Notes 61
   - 4.9. SQL Server Post-Installation Notes 62
   - 4.10. Your Next Steps 65
   - 4.11. Uninstalling the Product 66
5. **Patch store** 67
6. **About Deployment Templates** 68
7. **About the Deployment Tracker** 69
8. **What is Event History?** 70
9. **About Machine Groups** 72
10. **About Patch Groups** 73
11. **About Patch Scan Templates** 74
12. **About Windows Patch View** 75
13. **About Product Level Groups** 76
14. **About the Deployment Tracker Dialog** 77
15. **About Machine View** 78
16. **About the Operations Monitor** 79
17. **About the Scheduled Console Tasks Manager** 82
18. **About the Scheduled Remote Tasks Manager** 84
19. **About Third-Party Applications** 86
20. **About the My Test Machines Group** 87
21. **Accessing Machine Properties** 88
22. **Accessing Patch Scan Results (Scan View)** 89
23. **Accessing Machine View** 90
24. **Manually Acquiring Patches from the Vendor (Sideloading)** 91
25. **Activating Security Controls** 93
26. **Adding, Editing, or Removing vCenter Servers and ESXi Hypervisors** 111
27. **Adding Organizational Units or Active Directory Security Groups to a Machine Group** 114
28. **Adding Domains to a Machine Group** 117
29. **Adding Virtual Machines Hosted by a Server** 119
30. **Adding Offline Virtual Machines That Reside On Workstations** 122
31. **Adding Machines by IP Address to a Machine Group** 124
32. **Adding Machines by Name to a Machine Group** 127
33. **Advanced Filtering** 130
34. **Agent-Based Patch Management** 131
35. **About the Agent Client Program** 133
36. **Agent Reboot Options** 140
37. **Agent Rollout Options** 143
38. **Performing a New Agentless Operation** 145
39. **Agentless vs. Agent-based Solutions** 147
40. **Agents Options** 149
41. **API Options** 152
42. **Architecture view** 153
43. **Areas That Can be Accessed by the API** 154
44. **Asset Inventory Overview** 155
45. **Asset Scans are Performed as Background Tasks** 157
46. **Asset Management Scan Requirements** 158
47. **Assigning IP Addresses to Distribution Servers** 159

48. Automatically Deploying Patches ... 160
49. Automatically Sending Email Reports and Notifications ... 162
50. Automating Patch Management in an Agentless Environment ... 163
51. How to View Detailed Help Information About the PowerShell Commands ... 170
52. What is a Disconnected Console Configuration? ... 173
53. Before You Begin ... 175
54. Best Approach for Applying Patches in an Agentless Environment ... 177
55. Best Practices When Using Multiple Administrators ... 179
56. Canceling a Task ... 180
57. Canceling a Deployment ... 181
58. Changing a Custom XML File ... 182
59. Viewing Charts ... 183
60. Step 3: Commit the New Sub-Authority Certificate ... 184
61. Commonly Asked Questions ... 186
62. Configuration Options Overview ... 188
63. Configuring Proxy Server Settings for Security Controls Agent ... 189
64. Agentless Patch Management ... 191
65. Configuring a New or Existing Distribution Server ... 192
66. Configuring General Settings for a Security Controls Agent Policy ... 196
67. Configuring System Account Permissions ... 200
68. Configuring the Central Console in a Disconnected Configuration ... 202
69. Configuring the Remote Consoles in a Disconnected Configuration ... 203
70. Console Software and Hardware Recommendations ... 205
71. Assigning Aliases to the Console ... 207
72. Editing the Console Description ... 209
73. Continuous Agentless Scanning ... 211
74. Copy, Delete or Rename a Product Level Group ... 212
75. Creating and Editing a Linux Patch Deployment Configuration ... 213
76. Creating and Editing a Linux Patch Scan Configuration (content-based only) ... 221
77. Creating and Editing a Linux Patch Group ... 224
78. Creating Your Backup Files ... 233
79. Creating a New Asset Task ... 235
80. Creating a New Patch Task ... 238
81. Creating a New Power Task ... 251
82. Creating and Editing a Windows Patch Group ... 254
83. Creating and Editing a Power State Template ... 257
84. Creating and Editing a Product Level Group ... 260
85. Creating and Using a Manual Installation Script ... 262
86. Creating an IAVA Report ... 264
87. Creating an ITScripts Template ... 266
88. Creating a Custom Bulletin ... 268
89. Creating a Custom Patch ... 270
90. Creating a Custom Product ... 271
91. Creating a Custom Script ... 273
92. Creating or Editing a Deployment Template ... 274
93. Creating a New Asset Scan Template ... 275
94. Creating a New Custom XML File ... 277
95. Creating a New Security Controls Agent Policy ... 279
96. Creating Favorites ... 280
97. Creating Machine Groups ... 281
98. Creating or Editing a Patch Scan Template ... 282
99. Credential Handling and Authentication Fallback Behavior ... 286
100. Credential Precedence for Offline Hosted Virtual Machines ... 287
101. Credential Precedence for Physical Machines and Online Virtual Machines ... 288
102. Customizing the Column Headers ... 290
103. Customizing the Column Headers ... 294
104. Customizing the Column Headers ... 298
105. Customizing the Patch View Column Headers ... 301
106. CVE view ... 305
107. Database Maintenance ... 306
108. Data Rollup Options ... 311
109. Managing Data Files and Missing Patches in Disconnected Mode ... 313

110. Defining Credentials 314
111. Defining Nested Groups 316
112. Deleting a User 317
113. Deploying Product Levels 319
114. Deploying All Missing Patches to a Machine 320
115. Deploying Bulletins to Unmanaged Hypervisors 322
116. How to Deploy Bulletins to Your Managed Hypervisors 325
117. Deploying One or More Patches to a Machine 326
118. Deploying Patches to Multiple Machines 327
119. Deploying Patches to Virtual Machines and to Virtual Machine Templates 328
120. Deploying Third-Party Applications 333
121. Scheduling and Configuring a Deployment 334
122. Deployment History 337
123. Deployment Information Tab 338
124. Deployment Template: Maintenance Window Cut-Off Times Tab 340
125. Deployment Template: Custom Actions Tab 341
126. Deployment Template: Distribution Servers Tab 343
127. Deployment Template: Email Tab 346
128. Deployment Template: General Tab 348
129. Deployment Template: Hosted VMs/Templates Tab 350
130. Deployment Template: Post-Deploy Reboot Tab 352
131. Deployment Template: Pre-Deploy Reboot Tab 355
132. Deployment Template: Used By Tab 357
133. DeployState view 358
134. Deploying Patches to All Members of a Domain 359
135. DetectedPatchState view 360
136. Determining How Many Distribution Servers to Use 361
137. Determining Patch Replacements 362
138. Determining Patch Status 363
139. Determining the Currently-Assigned Role 364
140. Determining Which Machines Have Security Controls Agent 365
141. Using Disconnected Mode 366
142. Discovering Machines 367
143. Display Options 368
144. Distributed Environment Management 371
145. How to Download Different Language Versions of a Patch 373
146. Downloading Patches and Product Levels 374
147. Download Options 375
148. Email Options 380
149. Editions of the Program 382
150. Email Overview 383
151. Enabling and Disabling Role-Based Administration 384
152. Entity Relationships 385
153. Entity Relationships 389
154. Configuring an ESXi Bulletin Deployment 392
155. Excluding Certain Machines 395
156. Exporting Reports 396
157. File Version Analysis 398
158. Filtering Windows Patch View by Patch Type 399
159. Filtering Windows Patch View by Product Vendor 400
160. Filtering Patch View 401
161. Obtaining the License 403
162. Guide to Surviving Patch Tuesday 404
163. Help System 406
164. Step 1: How to Issue a New Certificate Using Your Own CA 407
165. How Do I . . .?: Get Started Scanning and Patching Linux Machines 409
166. How to Enable Security Controls Cloud Synchronization 410
167. How to Get Started 411
168. How to Patch Linux Machines That Reside in a Disconnected Environment 413
169. How Do I . . .?: Automate Scheduled Patching 422
170. How Do I . . .?: Collect Data for Technical Support 424
171. How Do I . . .?: Download Approved Patches 425

172. How Do I . . .?: Generate Reports ... 426
173. How Do I . . .?: Get Started Scanning and Patching Windows Machines ... 427
174. How Do I . . .?: Scan and Patch ESXi Hypervisors ... 431
175. How Do I . . .?: Set Up and Monitor Agents ... 432
176. How Do I . . .?: Track Deployment Status ... 433
177. How Do I . . .?: Use A Distribution Server ... 434
178. How Do I . . .?: Use The Asset Inventory Feature ... 436
179. How Do I . . .?: Use The ITScripts Feature ... 437
180. How Do I . . .?: Use The Power Management Feature ... 438
181. How Do I . . .?: View How-to Tutorials ... 440
182. How Licenses are Tracked ... 441
183. How Role-Based Administration Works ... 442
184. How the Agent Process Works ... 443
185. How Security Controls Manages Multiple Administrators ... 445
186. How to Add Virtual Machines to a Machine Group ... 446
187. How to Execute a Script ... 447
188. How to Initiate an Asset Scan ... 452
189. How to Initiate a Remote Desktop Connection ... 457
190. How to Initiate a Patch Scan ... 459
191. How to Initiate a Scan of an ESXi Hypervisor ... 463
192. How to Initiate Power Management Tasks ... 464
193. How to Scan for Third-Party Applications ... 470
194. IAVA Overview ... 472
195. Identifying Effectively Installed Patches ... 473
196. Identifying Explicitly Installed Patches ... 474
197. Implementing an Unattended Console Configuration ... 475
198. Implementing a Data Rollup Configuration ... 477
199. Importing CVEs ... 478
200. Importing User Scripts ... 480
201. Initiating and Monitoring a Power Status Scan ... 481
202. Initiating a Bulletin Deployment to an ESXi Hypervisor ... 482
203. Installing and Supporting Agents on Internet-Based Machines ... 483
204. Installing Agents from the Cloud ... 485
205. How to Install Security Controls Agent from the Console ... 489
206. InstallState view ... 492
207. Introduction to Patch Management Best Practices ... 493
208. Introduction to Database Views ... 494
209. Introducing the Virtual Inventory Feature ... 495
210. Explanation: Connecting to Machines Using IP Address vs Fully Qualified Domain Name (FQDN) ... 497
211. ITScripts Requirements ... 498
212. Step 2: Let the New Certificate Percolate Through Security Controls ... 500
213. Linking Files to a Machine Group ... 501
214. LinuxCompletionCode view ... 504
215. LinuxDetectedPatchState view ... 505
216. LinuxErrorStep view ... 506
217. LinuxInstallState view ... 507
218. LinuxNotification view ... 509
219. LinuxPatch view ... 510
220. LinuxPatchAppliesTo view ... 511
221. LinuxPatchDeployment view ... 512
222. LinuxPatchType view ... 513
223. LinuxPlatform view ... 514
224. Logging on to an ESX or Virtual Infrastructure Server ... 515
225. Logging Options ... 517
226. Machine view ... 519
227. Machine Group Dialog: Bottom Section ... 521
228. Machine Group Dialog: Middle Section ... 526
229. Machine Group Dialog: Top Section ... 527
230. Machine Group Information is Dynamic ... 530
231. Machine Group Information is Dynamic ... 531
232. Machine View Top Pane Summary ... 532
233. Maintenance Window ... 536

234. Using the Navigation Pane 538
235. Managing a Patch Scan Template 543
236. Managing Credentials 544
237. Managing Individual Machine Properties 549
238. Managing Multiple Machine Properties 552
239. Managing Your Agents 556
240. Manually Installing Security Controls Agent 560
241. Manually Sending Email Reports and Notifications 567
242. Menu Commands 568
243. Introduction to the Migration Tool 571
244. Exporting Patches 572
245. Monitoring Agent Actions 573
246. Monitoring an Asset Scan 574
247. Monitoring the Execution of a Script 575
248. Monitoring a Patch Scan 576
249. Monitoring a Power Task 577
250. Monitoring a Scheduled Asset Scan 578
251. Monitoring a Scheduled Patch Scan 579
252. Monitoring a Scheduled Power Task 580
253. Monitoring a Scheduled Script 581
254. Monitoring the Deployment 582
255. Multiple Console Configuration with Agents 584
256. Navigating the Scan View Grid 585
257. Navigating the Interface 586
258. Navigating Machine View 588
259. Navigating Windows Patch View 589
260. Notes About Virtual Machines 590
261. Notes About Virtual Machine Templates 592
262. Notifications and Warnings Options 594
263. Obtaining Support 596
264. Ongoing Maintenance Tasks 597
265. Opening a Windows PowerShell Prompt 598
266. OperatingSystemFamily view 600
267. Organizing Linux Groups and Configurations 601
268. Organizing Machine Groups 603
269. Organizing Patch Deployment Templates 605
270. Organizing Patch Scan Templates 607
271. Output 609
272. Overview of Linux Patch Management 610
273. Overview of the Solution 613
274. Versions of Database Views 616
275. Overview of the PowerShell Command-Line API 617
276. Overview of REST API 619
277. Available Reports 621
278. Overview of the Custom Patch XML Process 626
279. Patch view 628
280. PatchAppliesTo view 629
281. PatchCountsByScanMachine view 630
282. PatchDeployment view 631
283. PatchScan view 632
284. PatchType view 633
285. Patch Deployment Overview 634
286. Patch Deployment Prerequisites 635
287. Patch Deployment Security 636
288. Patch Downloads Are Performed As Background Tasks 637
289. Scan Options 638
290. Patch Scanning Overview 641
291. Performing Patching in a Disconnected Environment 642
292. Performing Actions on a Favorite 644
293. Performing Actions on ESXi Hypervisors 645
294. Performing Actions on a Hypervisor's Virtual Machines 646
295. Performing Actions on Machines 647

296. Performing Actions on Machines 650
297. Performing Actions on Machine Groups 659
298. Performing Actions on Patches 660
299. Performing Actions on Patches 664
300. Performing Actions on Script Results 667
301. Performing Actions on Patches 670
302. Performing Actions on Virtual Machines 672
303. Performing an IAVA Patch Scan 673
304. Populating the Address Book 676
305. Port Requirements and Firewall Configuration 677
306. Post-Migration Tasks 678
307. Potential Issues When Using Multiple Administrators 680
308. ITScripts and Windows PowerShell™ Overview 681
309. Power Management Overview 684
310. Power Management Requirements 686
311. Power State and Credential Requirements for Successful Scans and Deployments to Virtual Machines 688
312. Predefined Patch Scan Templates 690
313. Pre-Execution and Post-Execution Functions 691
314. Preparing to Use Security Controls Agent 692
315. Details on the Product Level and Patch Deployment Process 694
316. Product view 696
317. Proxy Support for Agents 697
318. Internet Proxy Options 706
319. Frequently Asked Questions 708
320. PowerShell API Requirements 710
321. RDP Requirements 711
322. Agent view 712
323. AssessedMachineState view 713
324. Agent view 714
325. Architecture view 715
326. AssessedMachineState view 716
327. CVE view 717
328. LinuxAdvisoryCVE view 718
329. LinuxAdvisoryInstallStatus view 719
330. LinuxAdvisoryPackage view 720
331. LinuxAdvisory view 721
332. LinuxArchitecture view 722
333. LinuxDetectedUpdateAdvisory view 723
334. LinuxDetectedUpdatePackage view 724
335. LinuxDetectedUpdateRepository view 725
336. LinuxDistribution view 726
337. LinuxPackageRemediationDetailedCode view 727
338. LinuxPackageRepository view 728
339. LinuxPackage view 729
340. LinuxRepository view 730
341. LinuxUpdateDeploymentAdvisory view 731
342. LinuxUpdateDeploymentPackage view 732
343. LinuxUpdateDeployment view 733
344. LinuxUpdateSeverity view 734
345. LinuxUpdateType view 735
346. Machine view 736
347. OperatingSystemFamily view 738
348. PatchCountsByScanMachine view 739
349. PatchScan view 740
350. ScanType view 741
351. SourceType view 742
352. WindowsDeployState view 743
353. WindowsDetectedPatchState view 751
354. WindowsInstallState view 752
355. WindowsPatchAppliesTo view 753
356. WindowsPatchDeployment view 754
357. WindowsPatchType view 755

358. WindowsPatch view ... 756
359. WindowsProduct view ... 757
360. WindowsVendorSeverity view ... 758
361. Sample Query: CVE Vulnerability Report ... 759
362. Sample Query: Missing Patches by Agent Policy ... 760
363. Sample Query: Patch Status Detail ... 762
364. Reporting Errors and Checking for Possible Solutions ... 764
365. Reports Dialog ... 765
366. Requirements and Exceptions ... 767
367. Requirements for Using the Migration Tool ... 768
368. Machine Restart Implementation Notes ... 769
369. Restoring Your Console on a New Machine ... 770
370. Roadmap of Tasks for Virtual Machines and Virtual Machine Templates ... 772
371. Using the Run console ITScripts Dialog ... 774
372. Sample Query: CVE Vulnerability Report ... 776
373. Sample Query: Missing Patches by Agent Policy ... 777
374. Sample Query: Patch Status Detail ... 779
375. Saving and Validating Your Changes ... 780
376. Scanning Engine Overview ... 781
377. Patch Scanning Prerequisites ... 782
378. ScanType view ... 784
379. Scan History ... 785
380. Scan Information Tab ... 786
381. Patch Options Menu ... 791
382. Scan View Scan Summary ... 792
383. Scheduled Snapshot Maintenance ... 795
384. How to Schedule a Report ... 798
385. Scheduling Asset Scans ... 801
386. Scheduling Patch Scans ... 803
387. Scheduling Power Tasks ... 806
388. Scheduling a Script ... 808
389. Script Metadata ... 811
390. ITScripts Results View ... 817
391. Managing ITScripts ... 819
392. ITScripts Options ... 822
393. Searching for Event Entries ... 823
394. Searching for Machines in the Top Pane ... 824
395. Searching for Machines in the Top Pane ... 825
396. Searching for Script Results ... 826
397. Searching Machine Groups ... 827
398. Searching for Hypervisors While Viewing a vCenter Server ... 829
399. Searching Patch View ... 830
400. Security Controls Cloud Synchronization Options ... 831
401. Security Controls Cloud Synchronization Overview ... 836
402. Security Controls Cloud Synchronization Requirements and Usage Notes ... 838
403. Potential Security Implications When Sharing Credentials with Background Services ... 840
404. Shared Credentials ... 841
405. Show Me How to Get Started! ... 844
406. Shutdown Implementation Notes ... 846
407. Signing Scripts ... 847
408. Sleep and Hibernation Implementation Notes ... 850
409. SourceType view ... 852
410. Specifying ComputerName and Credential Parameters ... 853
411. Specifying a Default Patch Scan Template ... 855
412. Specifying Which Custom XML Files to Use ... 856
413. Microsoft SQL Server Database Maintenance ... 858
414. Explanation: Deciding Whether to Permit the Use of an SSH Connection ... 860
415. Starting Security Controls ... 862
416. Supplying Scan Credentials for Target Machines ... 863
417. Synchronizing Distribution Servers ... 867
418. Target Type ... 870
419. Testing the Deployment ... 871

420. Tips and Tricks ... 872
421. Troubleshooting Agent Installation Errors ... 874
422. Trusted Domains ... 875
423. Typical Uses of Machine View ... 877
424. What is an Unattended Console Configuration? ... 878
425. Understanding Patch Count Data ... 879
426. Understanding RDP ... 880
427. Understanding the Top Pane ... 881
428. Uninstalling Security Controls Agent ... 882
429. Uninstalling Patches ... 884
430. Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates ... 885
431. Unsupported PowerShell Commands ... 887
432. Upgrade Procedure ... 888
433. Upgrade Requirements ... 892
434. Upgrade Tasks Performed on the Console ... 893
435. Use Examples ... 897
436. User Manager ... 899
437. Using an Agent on a Machine ... 901
438. Using a Patch Group ... 903
439. Using a Product Level Group ... 905
440. Using Patch Deployments to Perform Power Tasks ... 906
441. Using Smart Filter ... 907
442. Using Smart Filter to Filter Information in the Top Pane ... 910
443. Using the ESXi Hypervisors List ... 913
444. Using the Event History Smart Filter ... 914
445. Using the Script Result Smart Filter ... 916
446. Variables and Functions ... 918
447. vCenter Server and ESXi Hypervisor Requirements ... 921
448. vCenter Server Top Pane Summary ... 923
449. Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates ... 924
450. VendorSeverity view ... 926
451. Step 4: Testing for and Verifying the New Certificate ... 927
452. Version and License Information ... 928
453. Viewing Details of Linux Packages ... 929
454. Viewing and Tracking API-Driven Actions ... 930
455. Viewing Patch and Asset Summaries in Machine View ... 931
456. Viewing Asset Scan Results ... 942
457. Viewing Bulletin Status ... 943
458. Viewing Bulletin Status on Unmanaged Hypervisors ... 946
459. Viewing Custom Patches and Products ... 949
460. Viewing Deployment Results ... 950
461. Viewing ESXi Hypervisor Deployment Results ... 951
462. Viewing Information About a vCenter Server ... 953
463. Viewing Machines Affected by a Selected Patch ... 955
464. Viewing Machines Affected by a Selected Patch ... 956
465. Viewing Machines Affected by a Selected Patch ... 957
466. Viewing Patch Information ... 958
467. Viewing Patch Details ... 961
468. Viewing Patch Information ... 964
469. Viewing Patch Summaries in Scan View ... 969
470. Viewing Power Status Scan Results ... 973
471. Viewing Servers and Virtual Machines in a Machine Group ... 976
472. Virtual Machine Overview ... 977
473. Wake-on-LAN Implementation Notes ... 979
474. Watching For Data Rollup Activity ... 981
475. What is the Issue? ... 982
476. What Exactly is Security Controls Agent? ... 983
477. What is a Data Rollup Console Configuration? ... 984
478. What Sets Security Controls Apart from the Others? ... 985
479. When Should I Use Agentless and Agent-based Solutions? ... 987
480. Why Use a Distribution Server? ... 989
481. Why You Might Use Multiple Administrators ... 990

482. Why Use Multiple Consoles? 992
483. Managing a Deployment Template 993
484. Working with a Machine Group 994
485. ISeC 995
486. ISeC CSH 996

1. Welcome to Ivanti Security Controls

Welcome to Ivanti Security Controls, a unified IT management platform used for managing and protecting Windows-based machines, VMware ESXi Hypervisors, and Oracle, Red Hat Enterprise and CentOS Linux machines. Security Controls provides you with one centralized and common interface that you can use to perform the following IT management functions.

> You can also interact with Security Controls using a PowerShell Command-Line API or a REST API. For more information, see **Overview of the PowerShell Command-Line API** and **Overview of REST API**.

How Do I . . .?: Get Started Scanning and Patching Windows Machines

Security Controls' industry-leading patch management function provides the ability to scan all Windows-based machines, **VMware ESXi hypervisors**, and Oracle, RHEL and CentOS Linux-based machines in your network and assess the current patch status of those machines.

Learn more about Patch Management

After a scan is performed you can generate reports that provide additional details about the patch "health" of each machine. Security Controls can then be used to easily and automatically bring each machine up to date. You simply instruct the program to download and deploy the desired patches to the machines of your choosing. You can even dictate when the deployment will occur and if and when each machine should be restarted. In addition, Security Controls can provide email alerts that notify you when patches are available and it can email the results of scans and other information you wish to share with selected users.

The patch management function can be performed with or without agents on Windows-based machines. This unique blending of agentless and agent-based technologies gives you maximum flexibility while minimizing management overhead. Patch management activities on Linux-based machines are always performed using agents.

To get started (Windows): **How Do I Get Started Scanning and Patching?**

To get started (Linux): **Overview of Linux Patch Management**

How Do I . . .?: Use The Asset Inventory Feature

> Asset Inventory is only available on Windows-based machines.

The **asset inventory function** enables you to track your software and hardware assets.

Learn more about Asset Inventory

The function works with both physical and virtual machines. You can perform scans to detect and categorize the software and hardware contained on your physical and online virtual machines. Detailed information about your software and hardware virtual assets is available immediately following a scan. You also have the ability to create reports that can be used to track your asset inventory over time.

Like the patch management function, the asset inventory function can be performed with or without agents.

To get started: **How Do I Use the Asset Inventory Feature?**

How Do I . . .?: Use The Power Management Feature

> Power Management is only available on Windows-based machines when performed from the console.

The **power management function** enables you to control the power state of the machines in your organization.

Learn about Power Management

The primary reasons for using power management are to:

- Prepare your machines for maintenance tasks
- Reduce noise and power consumption
- Reduce operating costs
- Prolong battery life

You can shut down, restart, or awaken machines either immediately or on a scheduled basis. When you perform a scheduled restart you also have the ability to specify what power state to put the machines in: fully powered on, in sleep mode, or in hibernate mode. The power management function can be performed with or without agents.

To get started: **How Do I Use the Power Management Feature?**

How Do I . . .?: Use The ITScripts Feature

> ITScripts is only available on Windows-based machines.

The **ITScripts function** enables you to execute PowerShell scripts against the machines and machine groups you have already defined in Security Controls.

Learn more about ITScripts

With this scripting feature you can:

- Access free scripts and all pre-defined scripts provided by Ivanti
- Execute scripts against target machines
- Execute scripts from the console
- Create PowerShell templates
- Import custom scripts
- Execute scripts immediately
- Schedule script execution to run at some time in the future
- Execute scripts with or without the Windows PowerShell remoting features
- View the results of all scripts that have been initiated from Security Controls

To get started: **How Do I Use the ITScripts Feature?**

> For information about what was included in a release, including lists of issues fixed, see the Security Controls **release notes (opens a new window)**. For links to other sources of information, see **Obtaining Support**.

2. What's New?

This page describes the new features added to the latest releases. For more information about a release, including lists of issues fixed, and for information about earlier releases, see the Security Controls **release notes (opens a new window)**.

Version 2026.3

This release contains the following changes:

- Microsoft introduced checkpoint patches in May 2025 to deliver smaller, incremental updates that include only code changes since the previous deployment. Ivanti Security Controls marks prerequisite patches, not necessarily latest patch, that are part of a checkpoint chain with a flag icon (⚑) in the Windows Patches page for applicable Bulletin Title. This feature is now enhanced to include Agentless Security Controls also. For more information, see **Checkpoint Patch Chains**.
- Security Controls is now available on Oracle Linux 10. For more information, see **System Requirements**.
- The Credentials-based activation method is now deprecated. To obtain your 25 characters license key, retrieve it from the **Ivanti Licensing Portal** under Other License Keys. For more information see, **Obtaining the License**.

Version 2026.2

This release contains the following changes:

- Microsoft introduced checkpoint patches in May 2025 to deliver smaller, incremental updates that include only code changes since the previous deployment. Ivanti Security Controls marks prerequisite patches, not necessarily latest patch, that are part of a checkpoint chain with a flag icon (⚑) in the Windows Patches page for applicable Bulletin Title. This is applicable for Agent based Security Controls only. For more information, see **Checkpoint Patch Chains**.
- Security Controls is now available on Ubuntu 22.04 and Ubuntu 24.04. For more information, see **System Requirements**.

Version 2026.1

This release contains the following changes:

- The Security Controls allows to seamlessly deploy in-house software updates by uploading custom patches with metadata through the new REST APIs. For details, see **API documentation** (opens in a new window).
- Application control is removed and not available on Security Controls.
- The Security Controls allows organizations to define specific time periods for performing planned maintenance activities, such as patching or configuration changes. This feature helps to avoid disruptions during critical times, reducing risk and maintaining stability in production environments. For more information, see **Maintenance Window**.
- Security Controls is now available on Red Hat Linux 10. For more information, see **System Requirements**.
- Agent policy is enhanced to allow administrators to configure LAN and WAN/Internet bandwidth throttling settings. For more information, see **Configuring General Settings for a Security Controls Agent Policy**.

Version 2025.4

This release contains the following changes:

- Strengthen agent registration mechanism to prevent brute-force attacks and ensure adherence to current security compliance standards. For more information, see **Agents Options**.
- The Machine view page is enhanced to display icons to indicate the missing and installed packages for each selected patch.
- Support for Red Hat Enterprise Linux 7 and centOS 7 has ended. However, Ivanti provides extended support on request. Contact **Ivanti support** for more details.
- Windows 11, 25H2 is now supported. For more information, see **System Requirements**.

Version 2025.3

This release contains the following changes:

- The latest Security Controls enables deployment of ARM64-based applications to client devices.
- An option is available for Linux Machines, under **View Machines** page **Patch Information** tab, to right-click the patch tests and assign the patch group or create a new patch group and assign the test.
- An option to drag and drop the updates into the **Included Patches** list in the Linux Patch Group page.
- Trusted Domains supports using wildcard characters like (*) when specifying the domain names.
- Machines REST API is enhanced to include Advisory and Packages metadata. For details, see **Machines** in the separate API documentation (opens in a new window).
- Contentless Linux Patch Groups REST API is enhanced to include CVE import information. For details, see **Contentless Linux Patch Groups** in the separate API documentation (opens in a new window).
- Included REST APIs for Linux Deployments. For details, see **API documentation** (opens in a new window).

Version 2025.2

This release contains the following changes:

- A new column, **DNS Hostname**, is added to the top pane of the Machine View. This feature displays the DNS hostname as applicable to each machine. This column is hidden by default. For more information, see **Machine View Top Pane Summary**.
- An option to choose **Scan for Microsoft Preview patches** is added to the General tab of the New patch Scan template under Windows Patch Scan Templates. Scan for Microsoft Preview patches option allows users the flexibility to include Microsoft preview patches in the system scans. Microsoft preview patches are updates released by Microsoft that allow users to test upcoming features, improvements, or fixes before they are officially rolled out. For more information, see **Creating or Editing a Patch Scan Template**.
- Amazon Linux V2 and Amazon Linux 2023 are now supported. For more information, see **System Requirements**.
- REST API for **Policies** are enhanced to include contentless Linux machines.
- Support for ESXi 8.0.3 is added and support for vCenter 6.5 is removed.
- Included REST APIs for Contentless Linux Patch Deployment Configuration and Contentless Linux Patch groups. For details, see **Contentless Linux Patch Deployment Configuration** and **Contentless Linux Patch Groups** in the separate API documentation (opens in a new window).

Version 2025.1

This release contains the following changes:

- The Machine/OS Listing, Deployment Status by Machine, and Executive Summary reports have been updated to include contentless Linux patching. For more information, see **Available Reports**.
- A new option, **Trusted Domains**, is added under the Tools menu. This feature allows you to add and identify permitted domains by creating a list of trusted domain suffixes. Only the domain suffixes included in this list are allowed to communicate with Security Controls. For more information, see **Trusted Domains**.
- Patch Scans REST API is enhanced to include contentless Linux machines. For details, see **Patch Scans** in the separate API documentation (opens in a new window).
- Included REST APIs for Linux Package Metadata and Linux Advisory Metadata. For details, see **Linux Pacakage Metadata** and **Linux Advisory Metadata** in the separate API documentation (opens in a new window).

Version 2024.4

This release contains the following changes:

- Deploy by Patch severity is now available for the contentless patching for Linux. For more information, see **Creating and Editing a Linux Patch Deployment Configuration**.
- The Power Status and Machine Patch Status reports have been updated to include contentless Linux patching. For more information, see **Available Reports**.
- Windows 11, 24H2 is now supported. For more information, see **System Requirements**.

Version 2024.3

This release contains the following changes:

- Individual packages can now be added to a contentless Linux patch group. For more information, see **Creating and Editing a Linux Patch Group**.
- CVSS scores are now displayed for contentless Linux patches. For more information, see **Viewing Patch and Asset Summaries in Machine View**.
- A new set of database views has been added to the database to enable you to generate custom reports for contentless Linux patching. For more information, see **Versions of Database Views**.
- The POST and DELETE methods **sharewithservice** have been removed from the **Credentials** function of the REST API. For details, see **Credentials** in the separate API documentation (opens in a new window).

Version 2024.2

This release contains the following changes:

- Deploy by Patch Group is now available for the new contentless patching for Linux. You can create patch groups for use with Linux contentless patching from the **New > Linux Patch > Patch Group** menu, from the **Linux Patch Groups** list in the navigation pane, or from the Machine View. There are separate Linux patch groups for contentless patching and content-based patching. Only advisories can currently be added to a Linux contentless patch group. For information about creating patch groups for contentless Linux patching, see **Creating and Editing a Linux Patch Group**.

> If you use distribution servers, you MUST update the Linux engine installer on all distribution servers before creating or updating policies to include Linux patch groups. If this is not done, and a new policy is used with an old engine, scans will not work the old engine will interpret this policy to deploy all patches and not just the patches that were approved in the patch group.

A new option, **Require secure LDAP connections**, has been added to the **Scan Options** dialog to prevent the fallback to using the insecure port 389 when querying for OUs or machines in LDAP both in the machine group editor and during a scan. For more information, see **Scan Options**. By default, this is disabled.

Version 2024.1

This release contains the following changes:

- In 2024, Linux patching in Security Controls is undergoing a major change as it transitions away from the content-based patching of previous versions to contentless patching directly from the distribution's repository. This provides a much more efficient and exhaustive mechanism for patching Linux devices. In this first release, you can scan for all vulnerabilities and then patch all. For more information, see **Linux Contentless Patching**.



- VMware has ended support and technical guidance for versions 6.5, 6.7 and 6.7.1, and security updates are no longer published. Support for these versions will be removed in a future release, leaving the earliest supported version as 7.0. For more information about managing your vCenter servers and ESXi Hypervisors, see **Introducing the Virtual Inventory Feature**.
  With version 2024.1, new options for configuring the encryption of the connection between the console and SQL Server have been added.
  The new options provide more security, but may need further configuration. The upgrade does not change this setting, leaving it at the least secure but most compatible setting. When upgrading, we recommend you review the database connection encryption setting using the Database Setup Tool (see **Set Advanced options - database connection encryption**).
- Windows Server 2008 and Windows Server 2008 R2 endpoints are no longer supported.

Version 2023.4

This release contains the following changes:

- The Security Controls REST API has been updated to provide more control of cultures and to enable specifying an instance name if required when deploying patches. For more information, see **API help** (opens in a new window).
- Windows Server 2012 and Windows Server 2012 R2 clients are supported with **Microsoft Extended Security Updates (ESU)** and an Ivanti ESU – contact your Ivanti supplier.
- Windows Server 2012 and Windows Server 2012 R2 are no longer supported for the console. For a complete list of supported platforms, see **System Requirements**.
- The Ivanti Security Controls Diagnostic Toolkit, which provides utilities to help diagnose your system and provide information to support is now available. For more information, see **Security Controls Diagnostic Toolkit Release Notes** (opens in a new window).

Version 2023.3

This release contains the following changes:

- You can now edit machine details using the REST API. For more information about the REST API, see the separate **help (opens in a new window)**.
- During the automatic cleanup of the download directory, core files are not deleted if the download directory is set to be used as a distribution server. For more information, see **Download Options**.
- Accessibility improvements.

Version 2023.2

This release contains the following changes:

- Use of the Ivanti Scheduler has been discontinued. The Microsoft Scheduler has been improved to the point that the Ivanti Scheduler is no longer needed. The Microsoft Scheduler is now the default scheduler service and is used when performing power state and patch deployment tasks on remote machines. The scheduler is used to initiate the tasks at the specified time, whether immediately or at some specified time.

> With the deprecation of the Ivanti Scheduler, port 5120 is no longer required to be an allowed port in your firewall settings. In addition, when you are certain that all scheduled tasks still using the Ivanti Scheduler have been run, you should **remove the Ivanti Scheduler** from your target machines.

A deployment tool is now being pushed to target machines when a patch deployment is performed from the console. The tool is used to execute a deployment package on the target machine. The capabilities of the deployment tool are not new; they used to be included with the Ivanti Scheduler. With the deprecation of the Ivanti Scheduler, however, the deployment tool is now being delivered as a separate component. It will automatically be pushed to target machines when needed. If needed, you can remove the deployment tool from a target machine by **right-clicking the machine in Machine View** and using the **Uninstall deployment tool** command.

- For offline virtual machines, patching products installed on virtual disks with the disk mode set to either **Independent – Persistent** or **Independent – Nonpersistent** is not supported. If a virtual machine has both dependent and independent disks, you can still install patches for products that are installed on the dependent disks.
- Support for ESXi 6.0 has been dropped and support for ESXi 8.00 and 8.0.1 added. The supported versions of VMware ESXi hypervisors are now ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 8.00, and ESXi 8.0.1.
- Removed Microsoft Visual C++ Redistributable for Visual Studio 2013 as a prerequisite software requirement for the console
- A number of known issues have been resolved. See the **Security Controls 2023.2 Release Notes** for the complete list of resolved issues.

Version 2023.1

This release contains the following changes:

- The **Validate Against Known Hosts File** option is now available when configuring the **SSH server connection** process. You should choose this option if you want to use the **known_hosts** file to validate each target machine before allowing an SSH connection.
- The user interface has been refreshed with new icons and colors, providing a more modern look. A new skin that mimics the look and feel of Windows 11 has also been added. The skin is named **WXI** and can be found on the **Display** tab of the **Options dialog**. WXI is the new default option.
- A number of known issues have been resolved. See the **Security Controls 2023.1 Release Notes** for the complete list of resolved issues.

Version 2022.4

This release contains the following changes:

- A new "Automate to Compliance" **REST API script** is now available. The script automates the steps in the patch process (scan, deploy, reboot), repeating the steps until all patches have been deployed to the designated machines.
- The **Patch Metadata function** in the REST API has been enhanced to provide better sorting and pagination capabilities when viewing the query results.
- The **agent client program** has been updated. Much more information is now provided in the patch task logs about the patch status (downloads, installs, success, failure, error messages).
- A security enhancement has been made to the **SSH server connection** process. You now have the option to specify if an SSH connection can be used when the console communicates with an endpoint that supports SSH and for which SMB fails.
- More information has been added to the error codes that are displayed in the **Windows deployment history tab** in Machine View.
- Deprecation of Windows 8.1: Support for the Security Controls console on the Windows 8.1 operating system is scheduled to end in January 2023.
- A number of known issues have been resolved. See the **Security Controls 2022.4 Release Notes** for the complete list of resolved issues.

Version 2022.3

This release contains the following changes:

- The ability to automatically clean up your patch download directory and your distribution server(s). Any patches that are unlikely to be used in the future will be deleted from these locations, saving disk space. This option is configured on the **Tools > Options > Downloads** tab.
- The number of thread pools used when scanning machine groups that contain machines defined by an IP range, a domain or an organizational unit is now automatically capped. This will improve performance by limiting the number of machine groups that can be scanned at one time, keeping the console machine's processors from becoming overloaded. For more details, see the information on the **Global thread pool** option.
- Localized versions of the **agent user interface** are now available.
- You now have the option to **specify if the agent user interface will be installed**. The agent client currently requires the use of .NET 6, and it will likely continue to be updated in the future to use newer versions of .NET as they become available. One of the reasons you may not want the **agent client** installed is if you have other applications on your machines that also require the use of .NET. If the agent client is not needed, you can shield those machines from the reboots and other effects that occur when an agent is updated to support a new version of .NET.
- Two new Linux patch attributes are now stored in the database and are available for reporting purposes: **InstalledOn date** and **Notification > Title**.
- In addition to checking for application updates and End-of-Life notices on launch, the Security Controls console will now check for updates and notices every 24 hours while the Security Controls console remains open. The administrator can snooze the notifications for up to seven days at a time.
- The **Security Controls Cloud** website has been refreshed. It now has an updated style that is consistent with other Ivanti sites, and modern client libraries are used to help ensure the most secure browsing experience.
- A number of known issues have been resolved. See the **Security Controls 2022.3 Release Notes** for the complete list of resolved issues.

Version 2022.2

This release contains the following changes:

- An example PowerShell script has been added to the Security Controls **REST API Help**. This script shows how to add specific KBs to a new patch group or to existing patch groups. If you need to add an out-of-band security patch to many patch groups at once, this script simplifies the process.
- Additional options allow you to more precisely specify which language should be used within the Security Controls interface. In the **Tools > Options > Display Options dialog**, you can either select a specific language or let the console machine's operating system language setting specify which language should be used. The new language options are applied on a per user basis.
- Support for Red Hat Enterprise Linux 6 has ended. This is because Red Hat has stopped providing maintenance support for Red Hat Enterprise Linux 6.
- Corrected a daylight savings time issue that sometimes caused scheduled scans to run one hour late or become disabled. The fix adds a periodic check that re-enables the scheduled scans.
- A number of known issues have been resolved. See the **Security Controls 2022.2 Release Notes** for the complete list of resolved issues.

Version 2022.1

This maintenance release contains the following changes:

- More complete information is now provided in Machine View and in reports for virtual machines that contain the same name. Previously, only one entry would be created for hosted online virtual machines that had the same name but different vCenter paths. With this release the machines are listed separately, with complete host data path information provided for each machine to show the distinction between the machines.
- Additional context is provided on an error message that precedes the unexpected closing of the Security Controls console. The new text makes it clear that the console is closing because it was unable to download the required content data.
- A number of known issues have been resolved. See the **Security Controls 2022.1 Release Notes** for the complete list of resolved issues.

Version 2021.4

The following features and improvements were introduced in Ivanti Security Controls 2021.4.

Ability to Delete a User Whose Credentials are Shared with Other Users

The **User Role Assignment** dialog has been replaced by the new **User Manager dialog**. In addition to allowing you to assign different roles to different users, the **User Manager** dialog now allows you to **delete any users** who should no longer have access to Security Controls. For example, if one of your administrators has been assigned to a different project or has left your organization, you will want to delete that user. If the user being deleted is currently sharing credentials with one or more users or with background services, you are able to clean up all shared credential associations before you delete the user.

Improved Windows Agent Client Program

The **agent client program** has been totally reworked, providing an updated look and feel. In addition, the program provides more troubleshooting information and does a better job of presenting the information.

Windows 11 and Windows Server 2022 Support

Support has been added for Windows 11 and Windows Server 2022 for use as a console and on target machines that require patching.

Version 2021.2 Update 1

This maintenance release contains the following changes:

- A number of known issues have been resolved. See the **Security Controls 2021.2 Update 1 Release Notes** for the complete list of resolved issues.
- The supported versions of **VMware ESXi hypervisors** are now ESXi 6.0, ESXi 6.5, ESXi 6.7 and ESXi 7.0. Support for ESXi 5.x has been dropped.

> If you are using ESXI 7.0 Update 1 or later, the patch offline bundle must be installed on your hypervisor. For more information, see the **VMware ESXi 7.0 Update 1 Release Notes**.

The following operating systems are no longer **supported**:

- The Security Controls console is no longer supported on Windows Server 2008 R2 and Windows 7 operating systems
- The Security Controls agent is no longer supported on Windows 8 and CentOS 6 operating systems
- Agentless operations are no longer supported on Windows XP, Windows Server 2003, Windows Vista and Windows 8 operating systems

Version 2021.2

Major New Features

Sideload Patches

Sideloading refers to the process of managing patches that cannot be automatically downloaded. The sideload feature greatly simplifies this process. You will need to manually download the patch file, but after that the sideload feature takes over and provides a number of automated services. Specifically, the feature will verify the contents of the manually downloaded patch, rename the file if needed and then automatically save the patch file to the patch download directory. Once there, the patch is ready to be deployed using the normal deployment process.

Automatically Delete Inactive Machines from the Database

The ability to automatically delete inactive machines from the database has been added to the **Database Maintenance tool**. An inactive machine can be a machine that has not had an agent check in with the console, been assessed or been included in a patch deployment for the specified number of days. This is important, because inactive machines do not accurately depict the current state of your organization.

Continuous Agentless Scanning

You now have the option to **configure agentless patch scanning** operations on intervals as short as three minutes. This provides the ability to perform nearly continuous scans of a designated machine group.

Scripted Scans and Deployments Using CVEs

A detailed series of **PowerShell scripts** is provided that show how to scan for and deploy patches using input from a CVE file. The scripts invoke the REST API and perform a number of tasks, including:

- Parsing a CVE file and converting the content to a patch group
- Creating a scan template that scans for the patches contained in the patch group
- Optionally deploying any missing patches

Workstation and Server License Information

Additional details about your current license status are now available in two different locations. You can:

- Select **Help > About Ivanti Security Controls** on the console to view the number of deployment license seats currently used for both your servers and your workstations.
- Generate a **Detailed License Status** report that shows the number of available licensed seats, the number of seats used, how and when the seats were consumed and when they will be available again.

Minor New Features, Enhancements and Changes

- Added a new **Configuration method** in the REST API that enables you to display version information for the Security Controls console.
- In the **Patch Deployments method** in the REST API help, a **DeploymentResult** table has been added containing the codes that identify the various states of a deployment.
- In the **Machines method** in the REST API help:
  - Added the **credentialId** field to the output model
  - Added new PUT operations for assigning and unassigning a credential to a machine

Added Port 902 information to the **Port Requirements** table in the **System Requirements**

- Ended support for CentOS 6 Linux clients. This is because Red Hat has stopped providing maintenance support for CentOS 6.

Version 2021.1

Major New Features

Connect to Machines by Fully Qualified Domain Name (FQDN)

Prior to this release, the Security Controls console made connections with clients using the IP address of the machines. Some networks, however, have begun to operate in stricter environments that employ the use of additional Kerberos security measures. In particular, if the client machines in your environment establish a connection with servers using the Server Message Block (SMB) protocol, a certain level of validation may be required to be performed on the client's Service Principal Name (SPN). For these networks, you now have the option to choose **Fully Qualified Domain Name (FQDN)** as your **connection method**. Doing so will satisfy the additional validation requirements and enable successful connections to your client machines.

Copy Usages Button

For a shared credential, this new button enables you to **add any credential usage** that is not already being used by your user account. You might do this if the credential owner, or another user who is sharing the credential, has added one or more new usages since the credential was initially shared with you and you want to keep in sync with those changes.

REST API Enhancements

Several new capabilities have been added to the following functional areas in the **REST API**:

- **Patch Metadata:** Support has been added for IAVA IDs, and you can now sort and paginate the results of queries. This is implemented with the introduction of three new query URL parameters: **iavaIds**, **orderBy** and **sortOrder**. In addition, nine new output fields are now available: **affectedProducts**, **bulletinTitle**, **familyId**, **familyName**, **fileSize**, **iava**, **summary**, **vendorId** and **vendorName**.
- **Machine Groups:** The **connectionMethod** property has been added to the input and output models. This is being done in conjunction with the *Connect to Machines by Fully Qualified Domain Name (FQDN)* feature (see above).
- **Patch Scans:** You are now able to specify the connection method in conjunction with the endpoint names specified for scanning. This is being done in conjunction with the *Connect to Machines by Fully Qualified Domain Name (FQDN)* feature (see above).
- **Agent Deployments:** The **connectionMethod** property has been added to the input model. This is being done in conjunction with the *Connect to Machines by Fully Qualified Domain Name (FQDN)* feature (see above).
- **Patch Deployments:** You now have the ability to deploy specific patches to specific machines using a designated deployment template. This provides an integrated patching solution for **Ivanti Neurons customers**, and it is useful for existing on-premise customers who wish to tailor their patch deployment. The following input parameters are now available: **deployWhat**, **machines**, and **runAsDefault**.

Support for Red Hat Enterprise Linux 8

All vendor-supported Server, Workstation, Client and Computer Node variants of RHEL 8 (64-bit only) machines are now able to be **scanned and patched using agents**.

> Support for RHEL 8 is made possible through an update to the dynamic data content that is provided by Ivanti. This means that the two previous versions of Security Controls, 2019.3 and 2020.1, are now also able to support RHEL 8.

Version 2020.1

Major New Features

Shared Credentials

You can now **share credentials** with one or more users. This is especially useful in multi-admin environments, as it enables a senior administrator to delegate operations to junior administrators. The junior administrators can interact with endpoints using a secure credential without knowing the password for that credential. In addition, when a password needs updating, it can be updated from a single location.

Grouping of Machines in Machine View and Scan View

The new **Assigned Groups column** in Machine View and Scan View enables you to group related machines, making it easier to perform agentless operations and generate reports on the machines. This column is particularly useful for machines such as **Cloud agents**, as those machines do not belong to a machine group. With the Assigned Group feature, you can now group those machines with other machines that share similar attributes, such as the same physical location or agent policy.

Improved Product Licensing Process

A new **credentials-based activation method** is now available that enables you to specify exactly how many of your available license seats you want to consume on a specific entitlement. This method will be used by new customers who have an internet connection from the console. The legacy key-based activation method is still supported for existing customers who are upgrading and for customers who need to activate from within a disconnected network.

Additional REST API Functionality

The following functional areas are now available through the REST API:

- Cloud Sync
- Machines
- Users

The ability to share credentials and assign a machine to a group has also been added. For complete information, see the **REST API help**.

Minor New Features and Enhancements

Deep Rebrand

References to outdated company and product names have been scrubbed. Directory paths and other items that contain company and/or product names are now current.

Software Distribution Notification

A notification dialog is now provided whenever you **add a software distribution patch to a patch group** or initiate a **scan for third-party applications**. This warning will help prevent the inadvertent installation of third-party applications on your endpoints.

Improved List of Port Requirements

The **Port Requirements** table in the **System Requirements** help topic now contains much greater detail.

Patch Breakdown Column Renamed to Health

Within Machine View and Scan View, the **Patch breakdown** column has been renamed to **Health**. The new name better reflects the purpose of the column, which is to indicate the "health" of a machine by providing a visual representation of the percentage of installed patches vs missing patches.

Carry Original Scan Name into the Associated Deployment Name

When a patch scan is followed by an automatic patch deployment, the scan name is now associated with the corresponding deployment operation.

2.1. Linux Contentless Patching

Before V2024.1, all Linux patching in Security Controls was content-based. Engineers at Ivanti identified and curated the files required to fix a vulnerability, creating a content-based patch that could then be deployed. The main disadvantages of this method are that there is a delay while the content package is being created, and not all vulnerabilities are addressed.

From V2024.1, a new contentless method of Linux patching is being implemented. With this method, the repository for your Linux distribution is the direct source of all patch packages. This means that you have immediate access to all packages, giving you a more efficient and more complete patching mechanism, while maintaining the control and visibility of patching that Security Controls brings.



For a while, both methods will be available through Security Controls, but we recommend you start planning and implementing your migration to contentless patching now, because the old content-based method of patching Linux will be removed in a future release.

What has changed?

The main differences you will notice are:

- The previous Linux patching is available in Security Controls using the name **Linux Patch (Content-Based)** and the icon .
- There is no separate Patch Scan Configuration for the new contentless Linux patching. Whenever a Linux Patch Task runs, it runs a scan for all missing packages and advisories. You can then separately specify **Deploy options** as part of the Linux Patch Task.
- A new column has been added to the grids on the Machine View that, for contentless Linux, shows the source repository of the package.
- For V2024.2, the **Deploy by patch group** option for the new patch configuration supported the patching of packages associated with an advisory only. Adding packages to a patch group was supported in V2024.3, and **Deploy by severity** in V2024.4.

How do I migrate?

We recommend the following strategy to gain confidence in contentless patching and so move away from content-based patching for Linux:

1. Scan your test Linux machines using a **Linux Content-Based Patch Task** configured to scan for **All Patches**, then examine the **Health** column in the Machine View.
2. Deploy patches to your test machines using the existing content-based patch task, then re-examine the **Health** column in the Machine View.
3. Create or update an agent policy that includes a **Linux Patch Task** with the **Deployments** option disabled.
   This creates a scan all task using the new contentless functionality.
4. Install the agent with the new policy on your test Linux machines.
   A scan runs automatically after the engine installation.
5. After the scan has completed, check the **Health** column.
   Notice that new vulnerabilities have been discovered.
6. Enable the **Deployments** option in the new contentless patch task, and re-deploy patches.
7. Check the **Health** column again.
   The vulnerabilities have been remediated.

3. Evaluation Guide

Ivanti Security Controls is a unified IT management platform used for managing and protecting Windows-based machines, Oracle, RHEL and CentOS Linux-based machines and VMware ESXi hypervisors. To help you evaluate Ivanti Security Controls and get you quickly up and running with the program, we have created an Evaluation Guide.

Take me to the Evaluation Guide

4. Installation

File not found!

4.1. System Requirements

You must meet the following requirements when installing the Security Controls console and performing actions on client machines.

CONSOLE

Restrictions

- An NTFS file system is required on the console machine
- If you install the console on a domain controller that uses LDAP certificate authentication, you may need to configure the server to avoid conflict issues between the SSL certificate and the Security Controls program certificate.
- If you install the console on two or more machines that share a database, all of the console machines must have unique security identifiers (SIDs) in order to prevent user credential problems. Machines are likely to have the same SIDs if you make a copy of a virtual machine or if you ghost a machine.
- The console machine should be as fully patched as possible prior to installing Security Controls.

Processor

- Minimum: 2 processor cores 2GHz or faster
- Recommended: 4 processor cores 2GHz or faster (for 500 - 2500 seat license)
- High performance: 8 processor cores 2GHz or faster (for 10000+ seat license)
- Agentless Patch assessment: 8+ processor cores 2GHz or faster

Memory

- Minimum: 2GB of RAM
- Recommended: 4GB of RAM (for 500 - 2500 seat license)
- High performance: 16GB of RAM (for 10000+ seat license)

Video

- Minimum 1024 x 768 screen resolution
- Recommended 1280 x 1024 or higher

Disk Space

- 500 MB for application
- 10GB minimum, 100GB or more recommended for patch repository

Operating System (one of the following)

- Windows Server 2025 family
- Windows Server 2022 family
- Windows Server 2019 family, excluding Server Core and Nano Server (64-bit)
- Windows Server 2016 family, excluding Server Core and Nano Server (64-bit)
- Windows 11 family, including IoT LTSC 2024 24H2 and 25H2
- Windows 10 v1607 Pro, Enterprise or Education Edition (64-bit)

> You can use versions of Windows 10 earlier than v1607 but WMF 5.1 is required, which you may need to install separately. You can download WMF 5.1 from the **Microsoft Download Center**.

> It is recommended to use the latest available version where possible.

Database

- Use of a Microsoft SQL Server database. [Microsoft SQL Server 2012 is supported only for existing installations. For new installations, Microsoft SQL Server 2014 or later is required.]
- If you do not have a SQL Server database, the option to install SQL Server Express Edition will be provided during the prerequisite software installation process.
  Recommended: Microsoft SQL Server 2016 SP1 or higher
- Minimum Size: 30GB
- Medium Size: (500 - 2500 seat license) 30-60GB

- Enterprise Size: (10000+ seat license) 60-100GB

SQL High Availability

If set up in accordance with Microsoft best practices, SQL mirroring is supported by Security Controls.

A witness server is required for automatic failover. Without the witness a manual changeover is required.

SQL mirroring is supported on SQL Server 2014 but not SQL Express edition.

Prerequisite Software

- Use of **Microsoft SQL Server**
- Microsoft .NET Framework 4.8 or later
- Microsoft Visual C++ Redistributable for Visual Studio 2015-2022

Windows Account Requirements

- In order to access the full capabilities of Security Controls, you must run under an account with administrator privileges.

Configuration Requirements

- You must add a number of web URLs to your firewall, proxy and web filter exception lists. The URLs are used by Security Controls to download patch content from third-party vendors.
- For the complete list of URLs that you should add, see the **Ivanti Community (opens in a new window)**.
  When performing an asset scan of the console machine, Windows Management Instrumentation (WMI) service must be enabled and the protocol allowed to the machine. In Windows Firewall, the service is called Windows Management Instrumentation (WMI)/Remote Administration.

Supported Languages

See the **Languages** list on the **Display Options dialog**.

WINDOWS CLIENTS (AGENTLESS)

Operating Systems (32- and 64-bit versions of any of the following)

- Windows 11 family
- Windows 10 family
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016, Essentials Edition
- Windows Server 2016, Standard Edition (excluding Nano Server; Server Core supported with 32-bit subsystem)
- Windows Server 2016, Datacenter Edition (excluding Nano Server; Server Core supported with 32-bit subsystem)
- Windows Server 2019 family (excluding Nano Server; Server Core supported with 32-bit subsystem)
- Windows Server 2022 family
- Windows Server 2025 family

Virtual Machines (offline virtual images created by any of the following)

> Only applicable for Patch Management

- VMware ESXi 7.0.3 or later (VMware Tools is required on the virtual machines)
- VMware vCenter (formally VMware VirtualCenter) 7.0.3 or later (VMware Tools is required on the virtual machines)
- VMware Workstation 9.0 or later

Configuration Requirements

- Remote Registry service must be running
- Server service must be running
- NetBIOS (TCP 139) or Direct Host (TCP 445) ports must be accessible
- Windows Update service must not be disabled; rather, it must be set to either **Manual** or **Automatic** in order to successfully deploy patches. In addition, the Windows Update setting on each target machine (**Control Panel > System and Security > Windows Update > Change settings**) should be set to **Never check for updates**.

> If using Windows 10 or Windows Server 2016, you can disable Automatic Updates by selecting **Disable Configure Automatic Updates** in the **Group Policy Editor**. Please refer to Microsoft Help for guidance on other methods to disable the service.

Remote Desktop connections must be allowed in order for the console to make an RDP connection with the target machine.

- For additional requirements when performing patch scans of remote machines, see Patch Scanning Prerequisites.
- When performing an asset scan, Windows Management Instrumentation (WMI) service must be enabled and the protocol allowed to the machine (TCP port 135). In Windows Firewall, the service is called Windows Management Instrumentation (WMI)/Remote Administration. See Asset Scan Requirements for more details.

Products Supported (for patch program)

- See the Supported Products page on the Ivanti website (opens in a new window) for the current list

Disk Space (for patch program)

- Free space equal to five times the size of the patches being deployed

Supported Languages (for patch program)

See the **Patch View download status indicator language** list on the Display Options dialog.

WINDOWS CLIENTS RUNNING WITH AN AGENT

> An NTFS file system is required on agent machines.

Processor

- 500 MHz or faster CPU

Memory

- Minimum: 256MB RAM
- Recommended: 512MB RAM or higher

Disk Space

- 50 MB for Security Controls Agent client
- Minimum: 2GB or more for patch repository
- Recommended: 10GB

Operating Systems (any of the following except home editions)

- Windows 10 family
- Windows 11 family
- Windows Server 2012 family
- Windows Server 2012 family R2
- Windows Server 2016 family
- Windows Server 2019 family
- Windows Server 2022 family
- Windows Server 2025 family

Configuration Requirements

- Workstation service must be running
- Compatible Tested platforms: Ivanti Community (opens in a new window)
- To run the Ivanti Security Controls Agent UI engine (see Using an Agent on a Machine), the client machine requires .Net v8

LINUX CLIENTS RUNNING WITH AN AGENT

Operating Systems

All vendor-supported Server, Workstation, Client and Computer Node variants of the following systems (64-bit only).

> The libicu package and OpenSSL 1.0.2 or later are required for all distributions and versions.

Contentless

- Amazon Linux V2 and Amazon Linux 2023
- Ubuntu 22.04 and Ubuntu 24.04
- Oracle Linux 8, 9, and 10 (both Red Hat Compatible Kernel and Unbreakable Enterprise Kernel)

> If a machine has both kernels, both kernels are scanned and patched. However, because the non-running kernel is not running and so is not vulnerable, its advisories are always reported as Installed.

Red Hat Enterprise Linux 8, 9, and 10

Content-based

- Red Hat Enterprise Linux 8

Port Requirements

Secure Shell (SSH) and Port 22 are used when push installing an agent to a **Linux machine**.

Authentication Requirements

The SSH authentication type of Password Authentication is required for SSH connections to succeed on push install. On all Linux endpoints, ensure that `PasswordAuthentication` is set to `yes` in `/etc/ssh/sshd_config`.

> After editing this configuration file, restart the sshd service for the change to take effect.

Configuration Requirements

In order to perform a **push install of an agent** from the Security Controls console to a Linux machine, you can connect to the machine using either the root account or passwordless sudo access. For security reasons, using sudo access is the recommended best practice. To implement sudo access, you must manually log on to each Linux machine as root, invoke visudo and then do the following:

- Add the following command to the file.
- `<installUser> ALL=(ALL) NOPASSWD: /bin/sh /tmp/ivanti-[A-Za-z0-9][A-Za-z0-9][A-Za-z0-9][A-Za-z0-9]/install.sh *`
  This command uses sudo (super user do) to grant root privileges to the console so that it can do a push install of an agent to the Linux machine.
  In the file, look for a line that reads `Defaults requiretty` and if it exists, change it to `Defaults !requiretty`.
  This bypasses a known operating system bug by disabling the `requiretty` flag for every user on the machine, enabling sudo to run from means other than just a login session. If you prefer, you can disable the flag for just the install user by changing it to `Defaults:<installuser> !requiretty`.
  This flag is not set in the most current versions of Red Hat and CentOS.

If you choose not to use either root or sudo access from the console to your Linux machines, you can **manually install an agent** on each machine.

> If your Linux machines reside in a disconnected environment, you may want to perform the **disconnected configuration steps** at the same time that you configure each machine for sudo access.

PORT REQUIREMENTS

These are the default port requirements. Several of the port numbers are **configurable**.

> In some locked down environments, you may also need to specifically allow traffic over the default dynamic port range: 49152 - 65535.

Protocol	Port	Source	Destination	Encrypted	Description
UDP	9	Security Controls Console	Agentless System(s)	No	For **Wake-on-LAN** (WoL) and error reporting
TCP	22	Security Controls Console	Linux Agent System(s)	Yes	Allows the console to **push install** an agent to a Linux machine
TCP	80	Security Controls Console	Distribution Server: HTTP	No	Needed for distribution servers to sync patches with console only if using HTTP
		Security Controls Console	Distribution Server: HTTP	No	Needed for distribution servers to sync patches with console only if using HTTP
		Agent System(s)	Distribution Server: HTTP	No	Needed for distribution servers to sync patches with console only if using HTTP
		Security Controls Console	Patch Repositories / Patch Config	No	Patch downloads when HTTPS URLs are not available
TCP	135	Security Controls Console	Agentless System(s)	No	Allows the WMI protocol, which is required for **asset scans**

Protocol	Port	Source	Destination	Encrypted	Description
UDP and TCP (Or substitute TCP 445 for all three ports)	137-138 139	Security Controls Console	Agentless System(s)	No	(Windows file sharing/directory services) required for agentless scan and deployment to work
		Security Controls Console	Distribution Server: UNC	No	(Windows file sharing/directory services) required for agentless scan and deployment to work
		Agent System(s)	Distribution Server: UNC	No	(Windows file sharing/directory services) required for agentless scan and deployment to work
		Agentless System(s)	Distribution Server: UNC	No	(Windows file sharing/directory services) required for agentless scan and deployment to work
TCP	443	Security Controls Console	Distribution Server: HTTPS	Yes	Needed for distribution servers to sync patches with console; only if using HTTPS (Cloud sync)
		Agent System(s)	Distribution Server: HTTPS	Yes	Needed for distribution servers to sync patches with console; only if using HTTPS (Cloud agents)
		Security Controls Console	Patch Repositories / Patch Config	Yes	Patch and content downloads
		Security Controls Console	VMware vCenter	Yes	Used when making a connection to the vCenter Server
		Security Controls Console	VMware ESXi Hypervisor	Yes	Used when making a connection to the ESXi hypervisor
TCP (Or substitute with UDP 137-138 and TCP 139)	445	Security Controls Console	Agentless System(s)	Yes (SMB v3)	(Windows file sharing/directory services) required for agentless scan and deployment to work
		Security Controls Console	Distribution Server: UNC	Yes (SMB v3)	(Windows file sharing/directory services) required for agentless scan and deployment to work

Protocol	Port	Source	Destination	Encrypted	Description
		Agentless System(s)	Distribution Server: UNC	Yes (SMB v3)	(Windows file sharing/directory services) required for agentless scan and deployment to work
TCP	902	Security Controls Console	VMware vCenter / ESXi Hypervisor	Yes (TLS)	Used for disk mounting on offline virtual machines and templates
TCP	3001	Chrome browser	Agent System(s)		Allows the Chrome browser control extension to be installed; configurable via the BrowserAppStorePort setting
TCP	3121	Agent System(s)	Security Controls Console	Yes	Required for Deployment Tracker status updates for patch deployment and agent communication back to console
		Agentless System(s)	Security Controls Console	Yes	Required for Deployment Tracker status updates for patch deployment and agent communication back to console
TCP	4155	Security Controls Console	Agent System(s)	Yes	Allows listening agents to receive commands from console
TCP	5985	Security Controls Console	Agentless System(s)	Yes	Allows you to use the ITScripts feature

Configurable Ports

- **TCP 3000:** Chrome browser extension communication with AC agent
- **TCP 3001:** Chrome browser extension installation
- **TCP 3121:** Data rollup functions
- **TCP 4155:** Listening agents
- **TCP 5985:** ITScripts

URL EXCEPTION LIST

For Security Controls Cloud, add the following URLs to your allowed URL exception list:

- isec.ivanticloud.com
- isecagent.blob.core.windows.net

Depending on your usage, you may also need to include other URLs as listed in URL exception list for Ivanti Security Controls (opens in a new window).

TLS REQUIREMENTS

Different Windows versions support different TLS cipher suites and their priority order. A TLS cipher suite is a collection of cryptographic algorithms that define how encrypted communication is secured. Ivanti recommends using TLS 1.2 or higher along with secure cipher suites to ensure strong protection.

Some legacy systems may still require older TLS versions, but upgrading to TLS 1.2 and above helps to address some known security vulnerabilities.

For more information on TLS, see **Manage Transport Layer Security (TLS) in Windows Server**.

For details on TLS registry configurations, see **Transport Layer Security (TLS) registry settings**.

4.2. Architecture Considerations

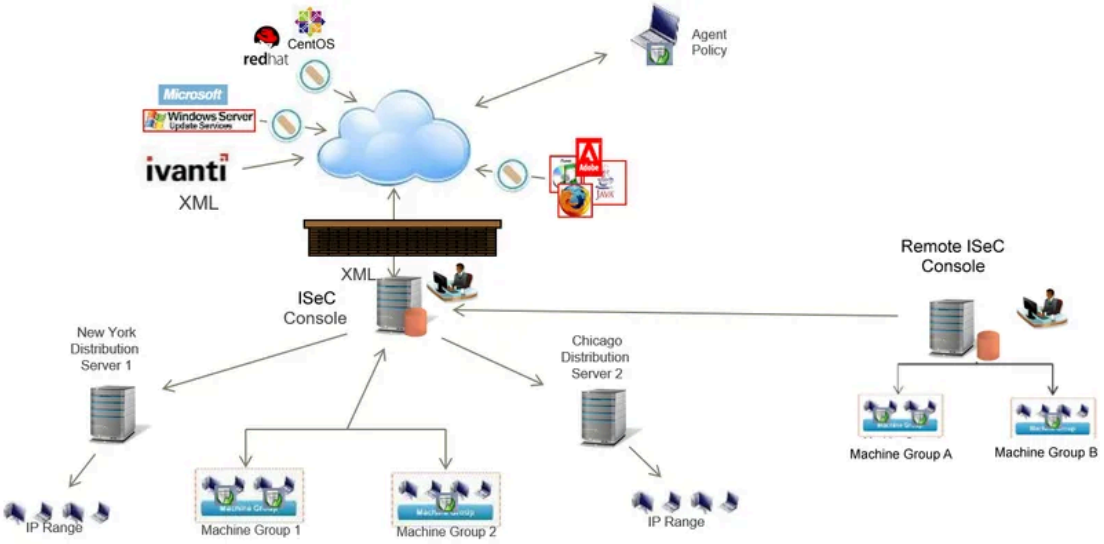
Security Controls is extremely scalable. You can use it in its most basic state immediately after installation to perform a number of agentless operations. If needed, you can choose to implement a number of different architectural features to accommodate large and complex environments. Review the following list and click the provided links to learn more about each feature.

- **Agentless:** Allows you to perform scans and deploy patches immediately after you install the Security Controls console. Used to manage Windows-based networked machines. Can be used to deploy Microsoft and 3rd party vendor patches.
- **Agent-based:** Agents can be installed on both Windows and Linux machines.
  - Windows environment: Agents are frequently used on disconnected machines and machines that reside in a DMZ.
  - Linux environment: Agents are required in order to perform patch management tasks.

Distribution Servers: Used at remote office locations.

- **Remote Security Controls Consoles:** Used within disparate geographic locations and managed regions.
- **Data Rollup:** A central console receives data about machines managed by remote consoles.
- **Security Controls Cloud**: Enables your agents to check in and receive policy updates from the cloud.
- **Disconnected Environments:** A remote console that is located in a network that does not have internet access.

The following diagram illustrates a number of these architectural features.



4.3. Obtaining the Software

Security Controls is available for download from our **Web-based download center** (opens in a new window). The download center always has the most recent version of Security Controls that is available.

Common Criteria Certified version

If you require the Common Criteria Certified version of Security Controls, this is available from the **Ivanti Security Controls Common Criteria Certified Download page** on the Ivanti Community (opens in a new window).

For more information about the Common Criteria Recognition Agreement, see the **Common Criteria web site** (opens in a new window).

- **Certification Report** (opens in a new window)
- **Security Target** (opens in a new window)

Related Topics

- **System Requirements**
- **Installing the Prerequisites**
- **SQL Server Pre-Installation Notes**
- **Performing a New Installation**
- **HTTP Proxy Post-Installation Notes**
- **SQL Server Post-Installation Notes**
- **Your Next Steps**

4.4. Installing the Prerequisites

This topic explains how to obtain and install the prerequisites needed by Security Controls.

Automatic Installation

The prerequisites can be automatically installed during the Security Controls **installation**.

Manual Installation

If you prefer to download and install the prerequisites yourself, you may do so using the following URLs. Your operating system may already contain many of the prerequisites, so only install the prerequisites that you are missing.

SQL Server Express Edition

Required only if you don't already have a full or express edition of SQL Server.

> Microsoft SQL Server downloads page

.NET Framework 4.8

> Microsoft .NET Framework 4.8 offline installer for Windows

Visual C++ 2015-2022 Redistributable (x64)

> Download the Visual C++ redistributable

Windows Management Framework 5.1

> Download WMF 5.1 from Microsoft Download Center

Related Topics

- System Requirements
- Obtaining the Software
- SQL Server Pre-Installation Notes
- Performing a New Installation
- HTTP Proxy Post-Installation Notes
- SQL Server Post-Installation Notes
- Your Next Steps

4.5. SQL Server Pre-Installation Notes

Security Controls will store all scan and patch deployment results in an SQL Server database. The SQL Server backend enables real-time collaboration and knowledge management amongst all individuals responsible for performing patch management tasks. Some of the benefits to using the SQL Server database include:

- High performance when scanning either a handful of machines or many machines
- Storage of data on a remote machine
- Ability for multiple Security Controls consoles to share templates, comments, reports, and scan results

What You Need to Know About SQL Server Before Installing Security Controls

Before installing Security Controls, please review the following SQL Server notes:

- Microsoft SQL Server is required.
  If you do not have SQL Server, the option to install Microsoft SQL Server Express Edition will be provided during the Security Controls installation process.
- The SQL Server Database Engine feature must be installed. No other SQL Server features are required.
- If you will be using an Express Edition of Microsoft SQL Server, you should consider downloading and installing Microsoft SQL Server Management Studio Express. This free software can be used to perform backups and to manage your database.
- Installation of SQL Express may fail if you have a SQL Native Client previously installed. It is strongly recommended you uninstall SQL Native Client using **Add or Remove Programs** before running the installation program.
- You must have access to the specified SQL Server. The program will support either Windows authentication or SQL Server authentication to access the specified SQL server. Although administrative access is not required, this account does need permissions to create and populate the product database on the specified SQL Server. In addition, the Security Controls console machine background services must be able to access the SQL Server. All background services run using the LocalSystem account on the console. If you are using Integrated Windows Authentication on a remote server, be sure to use the machine account when defining the console login account on SQL Server.

> For security purposes, Ivanti recommends using Windows authentication where possible. For information on configuring a remote SQL Server to accept Windows authentication credentials from the Security Controls console, see **SQL Server Post-Installation Notes**.

In order to create the database, the user account you specify during the installation process must be assigned the **dbcreator** role.

- If you are using SQL Server on a remote machine, you must configure the server to allow remote connections. This can be done using SQL Server Configuration Manager.

> For information about configuring the database connection encryption, see **Set Advanced options - database connection encryption**.

If you want to use a clustered configuration for redundancy purposes it must be configured prior to installation. You then reference the virtual clustered instance during the installation process. Clustered configurations are not supported with SQL Server Express Editions.

Related Topics

- **System Requirements**

- Obtaining the Software
- Installing the Prerequisites
- Performing a New Installation
- HTTP Proxy Post-Installation Notes
- SQL Server Post-Installation Notes
- Your Next Steps

4.6. Performing a New Installation

Disconnected Networks

> You can skip this section if you are not installing the console on a disconnected machine.

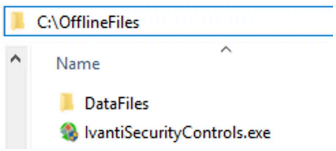
If you are installing the console on a machine that resides in a disconnected network and you are missing any of the **prerequisite software**, you must download the software from a connected machine and then manually install it on the disconnected console before you begin the installation process.

In addition, you must manually download the product core files and move the files to the disconnected machine.

1. **Download the Security Controls executable file** to the root directory on a connected machine.
2. On the connected machine, download the product core files by opening a command prompt and then typing the following command.

```bash
C:\>IvantiSecurityControls.exe /layout:OfflineFiles
```

This will create a `C:\OfflineFiles` folder that contains a copy of the Security Controls executable file plus a `\Datafiles` sub-folder that contains the related product core files.



Copy the entire contents of the `C:\OfflineFiles` folder to a portable device and move the files to the root directory on the disconnected machine.

4. On the disconnected machine, initiate the installation by double-clicking the Security Controls executable file that is located in the `C:\OfflineFiles` folder.
   The installer will check if the `C:\OfflineFiles\DataFiles` sub-directory exists. If it does, it will automatically copy the contents of the `\DataFiles` folder to the proper locations in the `C:\ProgramData` directory.

See the following section for instructions on completing the installation process, beginning with Step 5.

For more disconnected network information, see:

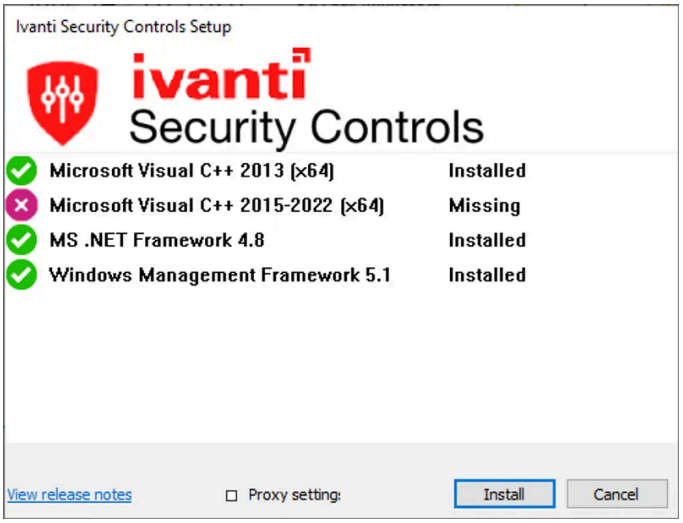
- **Performing Windows Patching in a Disconnected Environment**
- **How to Patch Disconnected Linux Machines**

Installation Process

1. Begin the installation process by double-clicking the Security Controls executable file.

If you receive a prompt indicating that a reboot is required, click **OK** and the installation process will automatically resume after the reboot.

If you are missing any **prerequisites** they are displayed in the **Setup** dialog. If you are not missing any prerequisites you will skip Step 2 - Step 4 and go directly to the **Welcome** dialog described in Step 5.



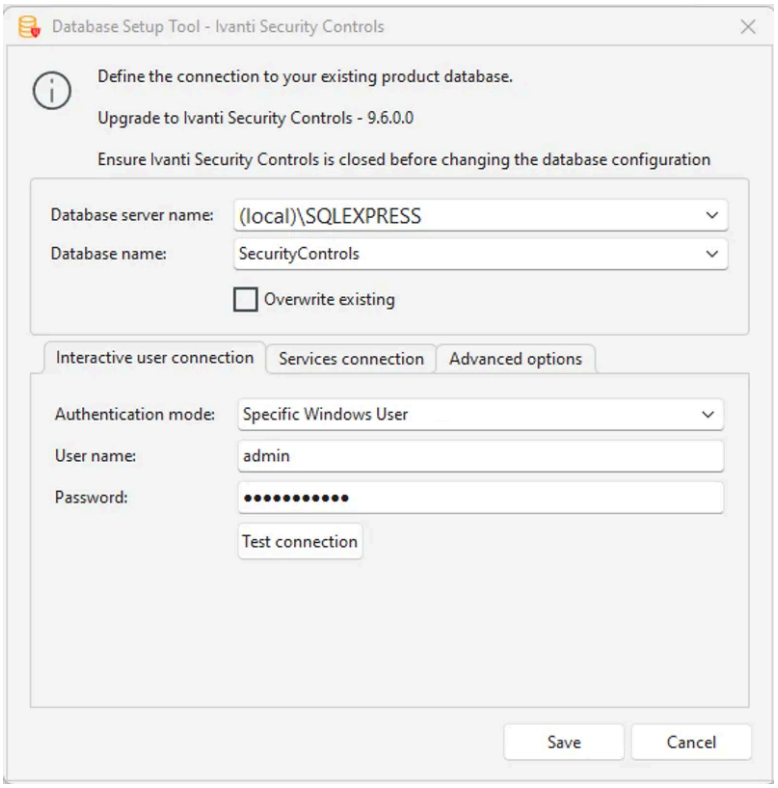
If you are required to enter a user name and password each time you launch your browser and browse the Internet, enable the **Proxy settings** check box, click the link, and type the necessary credentials.
It may be necessary to specify a domain as part of your user name (for example: `mydomain\my.name`). These settings can be modified later by going to **Tools > Options > Proxy**.
It also may be necessary to modify your HTTP proxy information after the installation is complete. See **HTTP Proxy Post Installation Notes** for details.

3. Click the **Install** button to install any missing prerequisites.
   A few of the prerequisites require a reboot after they are installed. In this case the installation program will request a system reboot before continuing. The installation program will restart automatically following the reboot.
4. (Conditional) If you were missing any prerequisites that required a reboot, to continue with the installation after the reboot click **Install**.
5. Read the information on the **Welcome** dialog and then click **Next**.
   The license agreement is displayed. You must agree to the terms of the license agreement in order to install the program.
6. To continue with the installation click **Next**.
   The **Destination Folder** dialog is displayed.
7. If you want to change the default location of the program, click the browse button and choose a new location.

TIP: If you want a shortcut icon to be created and placed on your desktop, enable the **Create a shortcut on the desktop** check box.

When you are done, click **Next**. The **Ready to install** dialog is displayed.
To begin the installation click **Install**.
Near the end of the installation process the **Database Setup Tool** dialog is displayed.

Tip: You can access the Database Setup Tool after the installation is complete by selecting **Start > Ivanti** Security Controls **> Database Setup Tool**.



Use the boxes provided to define how users and services will access the SQL Server database.

10. **Choose a database server and instance**
    - **Database Server name:** You can specify a machine or you can specify a machine and the SQL Server instance running on that machine (for example: *machinename*\SQLExpress). If SQL Server is already installed, this box will be automatically populated with the local SQL Server instance name. You can also click the dropdown arrow and select **Get remote server names** to retrieve a list of available servers.
    - **Database name:** Specify the database name you want to use. The default database name is SecurityControls. You can also click the dropdown arrow and select **Get database names** to retrieve a list of available databases.
    - **Overwrite existing:** If you have a previously installed Security Controls database and you want to preserve your existing data, clear this check box. If you have a previously installed database but you want to overwrite the existing data and start fresh, enable this check box.

Choose how interactive users will connect to the database

On the **Interactive user connection** tab, specify the credentials you want the program to use when a user performs an action that requires access to the database and select the **Authentication mode**:

- **Integrated Windows Authentication:** This is the recommended and default option. Security Controls will use the credentials of the currently logged on user to connect to the SQL Server database. The **User name** and **Password** boxes will be unavailable.
- **Specific Windows User:** Select this option only if the SQL Server database is on a remote machine. This enables you to provide a specific Windows user name and password combination. This option will have no effect if the database is on the local (console) machine (see Supplying Credentials for more information about local machine credentials). All

Security Controls users will use the supplied credentials when performing actions that require interaction with the remote SQL Server database.

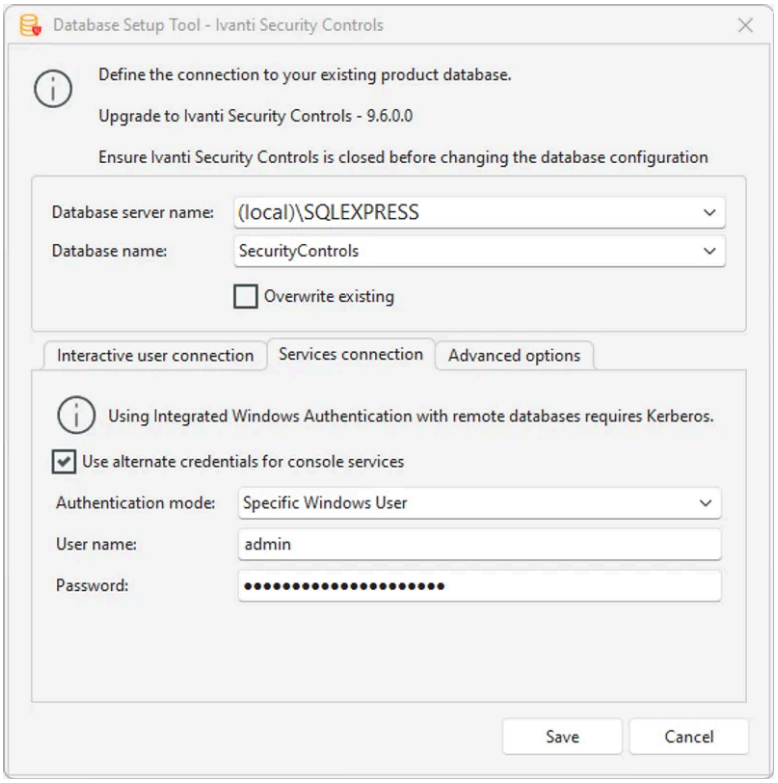
- **SQL Authentication:** Select this option to enter a specific SQL Server user name and password combination that will be used to log on to the specified SQL Server.

> **CAUTION!** If you supply SQL authentication credentials and have not implemented SSL encryption for SQL connections, the credentials will be passed over the network in clear text.

Test server connection: To verify that the program can use the supplied interactive user credentials to connect to the SQL Server database, click this button.

Choose how services will connect to the database

On the **Services connection** tab, specify the credentials you want the background services to use when making the connection to the database. These are the credentials that the results importer, agent operations, and other services will use to log on to SQL Server and provide status information.



- **Use alternate credentials for console services:**
  - If the SQL Server database is installed on the local machine you will typically ignore this option by not enabling this check box. In this case the same credentials and mode of authentication that you specified above for interactive users will be used.
  - You will typically only enable this check box if the SQL Server database is on a remote machine. When the database is on a remote machine you need an account that can authenticate to the database on the remote database server.

Authentication mode: Available only if **Use alternate credentials for console services** is enabled.

- **Integrated Windows Authentication:** Selecting this option means that the machine account will be used to connect to the remote SQL Server. The Kerberos network authentication protocol must be available in order to securely transmit

the credentials. The User name and Password boxes will be unavailable.

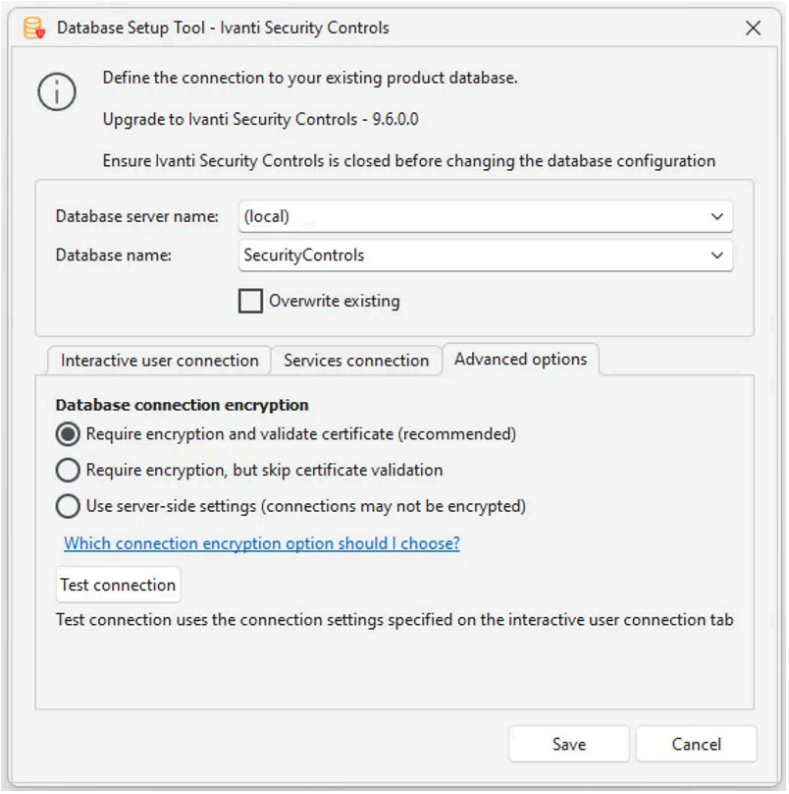
> If you choose Integrated Windows Authentication the installation program will attempt to create a SQL Server login for the machine account. If the account creation process fails, see **SQL Server Post-Installation Notes** for instructions on manually configuring a remote SQL Server to accept machine account credentials. Do this after you complete the Security Controls installation process but before you start the program.

Specific Windows User: Select this option to enter a specific Windows user name and password combination. Security Controls's background services will use these credentials to connect to the SQL Server database. This is a good fallback option if for some reason you have difficulties implementing integrated Windows authentication.

- **SQL Authentication:** Select this option to provide a specific SQL Server user name and password combination for the services to use when logging on to SQL Server.

Set Advanced options - database connection encryption

On the **Advanced options** tab, use the **Database connection encryption** section to set the encryption you want to use between the console and SQL Server. There are three options that provide different levels of security. You can update these settings later if required by running the Database Setup Tool from the Windows **Start** menu.



- **Require encryption and validate certificate (recommended):** This is the most secure but also the most restrictive option. Your server must be configured for TLS encryption, and the server's root certificate must be installed on the machine running the console. If the certificate has expired or is missing from the console machine, you cannot connect.
- **Require encryption, but skip certificate validation:** This will still use encryption, but does not check if the certificates are valid or expired. This option is typically used with a local installation of SQL Server or SQL Express.
- **Use server-side settings (connections may not be encrypted):** This is the least secure but provides the greatest compatibility. This uses whatever you have configured in SQL Server, with no validation.

> For more information, see **Using Encryption Without Validation in SQL Server Native Client** on Microsoft's website (opens in a new window).

Test connection: Tests the connection to the SQL Server database using the supplied database connection encryption settings with the credentials set on the **Interactive user connection** tab.

After providing all the required information, click **Save**.

> If the installation program detects a problem with any of the specified credentials, an error message will be displayed. This typically indicates that a user account you specified does not exist. Make a correction and try again.

The program will create, link to, or upgrade the database. When the database operation is complete the **Database Installation Complete** dialog is displayed.
Click **Next**.
The **Installation Complete** dialog is displayed.

12. Click **Finish**.
    The **Completed** dialog is displayed.



1. If you want to start Security Controls immediately, enable the **Launch** Security Controls check box and then click **Finish**; otherwise, just click **Finish**.

Related Topics

- System Requirements
- Obtaining the Software
- Installing the Prerequisites
- SQL Server Pre-Installation Notes

- HTTP Proxy Post-Installation Notes
- SQL Server Post-Installation Notes
- Your Next Steps

4.7. Installing the Console from a Command Line

This topic explains how to install the Ivanti Security Controls console from a command line, which can then be used to automate the installation.

> The name of the installer executable includes the version number of the release. On this page, the version number is represented by `version`. Remember to replace this with the version you are using.

Silent installation command

Bash

```
IvantiSecurityControls_version.exe /quiet /wi:"parameters"
```

where `parameters` are described below.

Available parameters

Parameter	Allowed values	Notes
CREATEDESKTOPSHORTCUT	#0, #1	`#0` does not create the desktop shortcut `#1` creates a shortcut Default: `#0`
DBCOMMANDTIMEOUT		Command timeout in minutes. Default: `30`
DBCONNECTIONENCRYPTION	RequireEncryptionAndValidateCertificate, RequireEncryptionButSkipCertificateValidation, UseServerSideSettings	Enables you to set the encryption you want to use between the console and SQL Server. For more information, see **Set Advanced options - database connection encryption**. Default: • if the database is local: for new databases or if the database is explicitly specified, `RequireEncryptionButSkipCertificateValidation` • if the database is remote: for new databases or if the database is explicitly specified, `RequireEncryptionAndValidateCertificate` • if the database is NOT explicitly specified and you are upgrading: uses whatever value is in the existing connection properties
DBCREATENEWORUPGRADE	upgrade, createNew	Either upgrades an existing database, or creates a new one. Default: `upgrade`
DBDATABASENAME		Your database name. Default: `SecurityControls`
DBTERMINATECONNECTIONS	true, false	Specifies whether or not to terminate the existing database connection. Default: `false`
DBOVERWRITE	true, false	Specifies whether or not to overwrite the database. Default: `false`
DBSQLSERVER		Your SQL Server instance. Default: `(local)\SQLEXPRESS` If the fallback behavior is not desired, ensure DBSQLSERVER is explicitly set. We recommend ensuring Kerberos authentication is available in the environment when targeting remote SQL Servers for best security and compatibility.
DOWNLOADPATHDIR		Your alternate download path.

Parameter	Allowed values	Notes
		Default: `%ProgramData%\Ivanti\Security Controls\Console\Patches`

Examples

To silently execute a fresh installation using the default local SQL server instance:

```
Bash

IvantiSecurityControls_version.exe /quiet /wi:"CREATEDESKTOPSHORTCUT=#1"
```

To upgrade an existing database:

```
Bash

IvantiSecurityControls_version.exe /quiet /wi:"DBSQLSERVER=(local)\SQLEXPRESS CREATEDESKTOPSHORTCUT=#1 DBCREATENEWORUPGRADE=upgrade"
```

To install-over and overwrite an existing database:

```
Bash

IvantiSecurityControls_version.exe /quiet /wi:"DBSQLSERVER=(local)\SQLEXPRESS CREATEDESKTOPSHORTCUT=#1 DBOVERWRITE=true"
```

To install using remote SQL server instance:

```
Bash

IvantiSecurityControls_version.exe /quiet /wi:"DBSQLSERVER=RemoteSqlBox\Instance CREATEDESKTOPSHORTCUT=#1"
```

To install using local default SQL server instance:

```
Bash

IvantiSecurityControls_version.exe /quiet /wi:"DBSQLSERVER=(local) CREATEDESKTOPSHORTCUT=#1"
```

To set installer fall back to SQL Express:

```
Bash

IvantiSecurityControls_version.exe /quiet /wi:"CREATEDESKTOPSHORTCUT=#1"
```

4.8. HTTP Proxy Post-Installation Notes

If your location uses an HTTP proxy to access the Internet, please note the following requirements:

- You must enable the **Bypass proxy server for local addresses** check box in the browser's proxy server settings. To access these settings, on the **Tools** menu in Internet Explorer, click **Internet Options**, click the **Connections** tab, and then click **LAN Settings**. Enabling the **Bypass proxy server for local addresses** check box specifies that the proxy server should not be used when the Security Controls console connects to a computer on the local network.
- The consoles services will not read or reference any per-user proxy address information. To configure proxy addresses for console services, you must manually modify the `ST.ServiceHost.exe.config` file to include a default proxy XML tag that defines the proxy, bypass local and bypasslist. You do this by adding the following XML beneath the base <configuration> element.

XML

```xml
<system.net>
 <defaultProxy>
  <bypasslist>
   <add address="127.0.0.1" />
   <add address="::1" />
   <add address="RollupConsoleNameOrIPAddress" />
  </bypasslist>
  <proxy bypassonlocal="True" proxyaddress="http://ProxyNameOrIP:Port" />
 </defaultProxy>
</system.net>
```

Related Topics

- System Requirements
- Obtaining the Software
- Installing the Prerequisites
- SQL Server Pre-Installation Notes
- Performing a New Installation
- SQL Server Post-Installation Notes
- Your Next Steps

4.9. SQL Server Post-Installation Notes

Manually Configuring a Remote SQL Server to Accept Machine Account Credentials

> The manual process described here is required only if the automated account creation process failed during product installation.

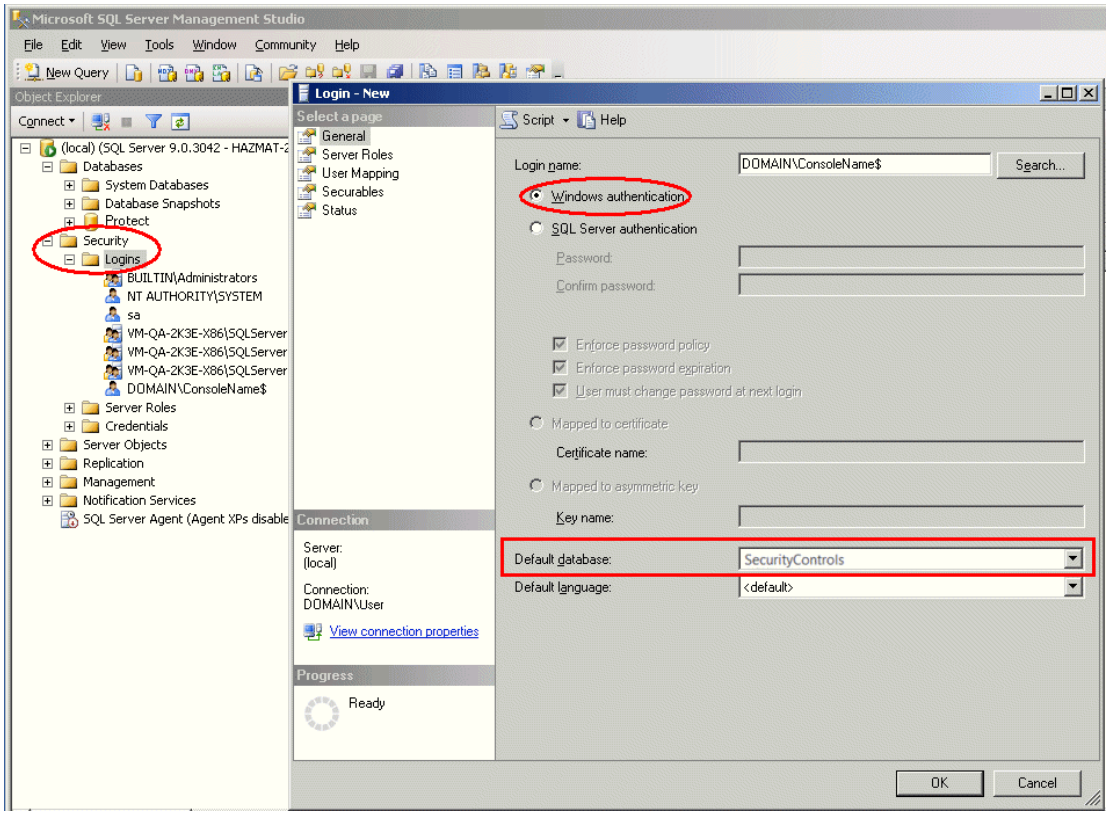
If you are using Integrated Windows Authentication to access a remote SQL Server, in order for Security Controls to interact properly with the server you must configure the server to accept machine account credentials. The best time to do this is immediately after you have installed Security Controls but before you actually start the program. You can, however, perform these steps after starting the program. Any scans you initiate prior to this that require interaction with a remote SQL Server database will probably fail.

This section describes how to configure a remote SQL Server to accept Windows authentication (machine account) credentials from the Security Controls console. For security purposes, Ivanti recommends using Windows authentication where possible. Microsoft SQL Server Management Studio is used as the editor in the following examples but you can use a different tool if you prefer.

1. The Security Controls console and SQL Server must be joined to the same domain or reside in different domains that have a trusted relationship.
   This is so the console and the server can compare credentials and establish a secure connection.
2. On SQL Server, create a new login account for Security Controls to use.
   You must have *securityadmin* privileges in order to create an account.
3. **To do this:** Within the **Security** node, right-click **Logins** and select **New Login**. Type the login name using a SAM-compatible format (domain\machine name). The machine account is your console's machine name and must contain a trailing $.

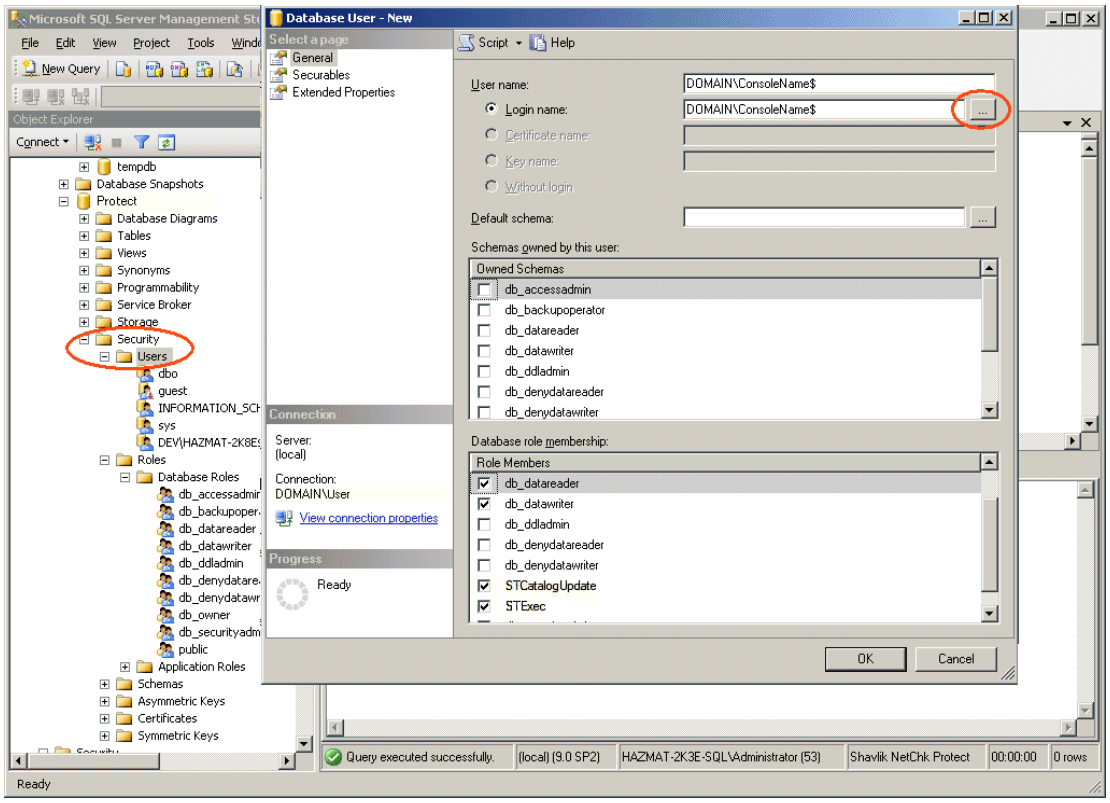
> Do not use the **Search** option. You must manually type the name because it is a special name.

Make sure you choose **Windows Authentication** and that the **Default database** box specifies the Security Controls database.



For your Security Controls database, create a new user login using the console machine account.

4. Right-click the **Users** folder, select **New User**, browse to find the **Login name**, and then paste the name in the **User name** box. Assign the user the **db_datareader**, **db_datawriter**, **STCatalogUpdate**, and **STExec** roles.



Start Security Controls.

5. Perform any troubleshooting as necessary.
    - You can use the SQL Server activity monitor to determine if connection attempts are successful when performing a patch scan.
    - If you ran Security Controls before creating the SQL Server user account, some services may fail to connect to SQL Server. You should select **Control Panel > Administrative Tools > Services** and try restarting the services.
    - If the connection attempts are failing you can view the messages in the SQL Server logs to determine why the failures are occurring.

Allowing Other Users Access to the Program

> This section also applies if you are using the **role-based administration** feature.

If you wish to allow other users access to the program, you may need to configure SQL Server so that those users have the necessary database permissions. Specifically, when using Windows integrated authentication, users without administrative rights on the database machine must be granted read and write permission to all tables and views. They must also be granted execute permission to all stored procedures in the Security Controls application database. They may not otherwise be able to start Security Controls.

One way to grant these permissions is to assign your users the *db_owner* role. For security reasons, however, this may not be the best solution. A safer alternative is to grant execute permission at the database level. You do this by assigning the users in question to the *STExec* role.

Performing Periodic Maintenance on the Database

Security Controls provides the ability to perform periodic maintenance on the database by automatically removing old scans, rebuilding index files, and performing backups. See **Database Maintenance** for details.

Related Topics

- **System Requirements**
- **Obtaining the Software**
- **Installing the Prerequisites**
- **SQL Server Pre-Installation Notes**
- **Performing a New Installation**
- **HTTP Proxy Post-Installation Notes**
- **Your Next Steps**

4.10. Your Next Steps

After you have successfully **installed** and **activated** Ivanti Security Controls you can immediately begin using all areas of the program. For the best experience, however, your suggested next steps are:

- **Create machine groups**: Machine groups are used to logically organize and track the machines in your organization. They are also used by Ivanti Security Controls to perform a number of different actions.
- **Define** and **assign** credentials: A credential consists of a user name and password pair. They are used to access remote machines, perform scans, and push any necessary files.
- (Optional) **Configure your distribution servers**: A distribution server is used to distribute XML data, scan engines, patches, and service packs to agents and to machines on remote sites. **Using one or more distribution server** can help reduce network traffic and speed program operations.
- See the **How to Get Started** section for quick start tips for using the many different features in Security Controls.

Related Topics

- **System Requirements**
- **Obtaining the Software**
- **Installing the Prerequisites**
- **SQL Server Pre-Installation Notes**
- **Performing a New Installation**
- **HTTP Proxy Post-Installation Notes**
- **SQL Server Post-Installation Notes**

4.11. Uninstalling the Product

> It is not necessary to uninstall the product if you are performing an upgrade. See the **Security Controls Upgrade Guide** for complete details.

To manually uninstall Security Controls:

- From the Windows Control Panel dialog, click **Uninstall a Program**, select Ivanti Security Controls and then click **Uninstall**.

If you also want to permanently remove all related artifacts:

> **Important!** Do not delete the following items if you intend to reinstall and use Security Controls at a later date.

- Delete the following items using Registry Editor:
  - HKEY_CURRENT_USER\Software\Ivanti\Security Controls
  - HKEY_CURRENT_USER\Software\LANDESK\Shavlik Protect (if an agent is installed on the console)
  - HKEY_LOCAL_MACHINE\SOFTWARE\Ivanti\Security Controls
  - HKEY_LOCAL_MACHINE\SOFTWARE\LANDESK\Shavlik Protect (if an agent is installed on the console)
  - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\LANDESK\Shavlik Protect

Delete the following directories:

  - %ProgramData%\Ivanti\Security Controls
  - %ProgramData%\LANDESK\Shavlik Protect (if an agent is installed on the console)
  - Users\<name>\AppData\Local\Ivanti_Inc\ST.Protect*

Delete the SQL database

- Delete the root and console certificates
- You can do this using the Certificates snap-in within Microsoft Management Console.
  The root certificate (ST Root Authority) is located in the **Trusted Root Certification Authority > Certificates** folder
- The console certificate, which is issued by ST Root Authority and will have a randomly generated GUID name, is located in the **Personal > Certificates** folder

5. Patch store

Patch store is an informal name for the patch download directory, which is used to store all patches that are downloaded in advance of a patch deployment.

See **Download Options**.

6. About Deployment Templates

When deploying patches to a machine, Security Controls allows you to specify a number of different options such as whether to notify logged on users about a pending deployment, whether the target should be restarted after deployment, whether reports should be sent, and much more.

Security Controls provides four predefined deployment templates:

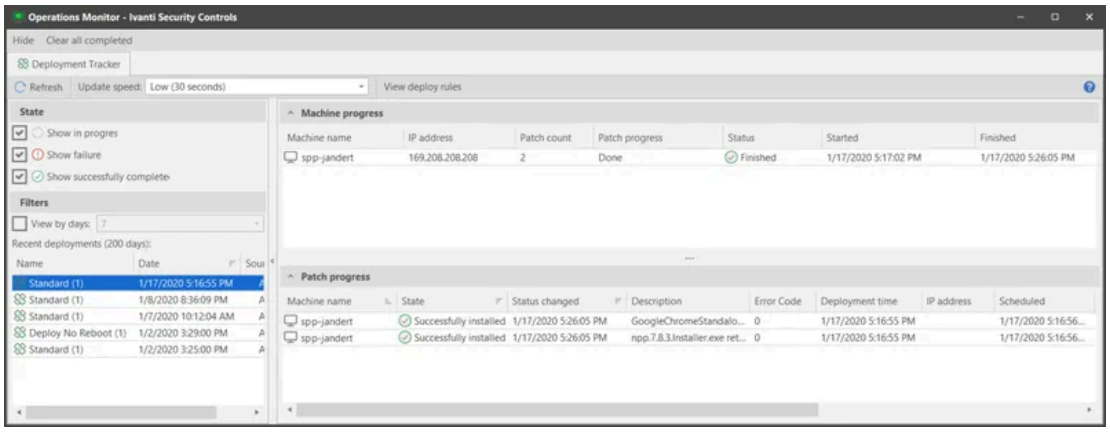
- The **Agent Standard** deployment template is designed to be used with agents. It will perform a post-patch deployment reboot only when needed.
- The **Standard** deployment template is designed to be used with agentless deployments initiated by the console. It will always perform a post-patch deployment reboot. This is the default template.
- The **Standard With Patch Clean-Up** deployment template builds on the **Standard** template by removing temporary patch files that were copied to the target machine during the deployment process.
- The **Virtual Machine Standard** deployment template is designed for use with virtual machines. It will take a **pre-deployment snapshot** of any virtual machine that is hosted on a server, and it will delete old snapshots that are more than four days old.

If you wish to create your own unique deployment template, see **Creating a Deployment Template**.

7. About the Deployment Tracker

Security Controls includes a feature called the Security Controls Deployment Tracker. This feature enables you to monitor the status of patch deployment tasks currently in progress. Deployment Tracker utilizes the Security Controls Patch Service, which is a component of the Security Controls Console Service. This service receives status messages from the target machines that are being patched. The service is installed and started during the Security Controls installation and it listens on the same port as the other console services (TCP port 3121). If this service is stopped, then Deployment Tracker will not be able to provide updated state information.

To start Deployment Tracker, select **View >** Deployment Tracker. For information on how to use the dialog, see **About the Deployment Tracker Dialog**.



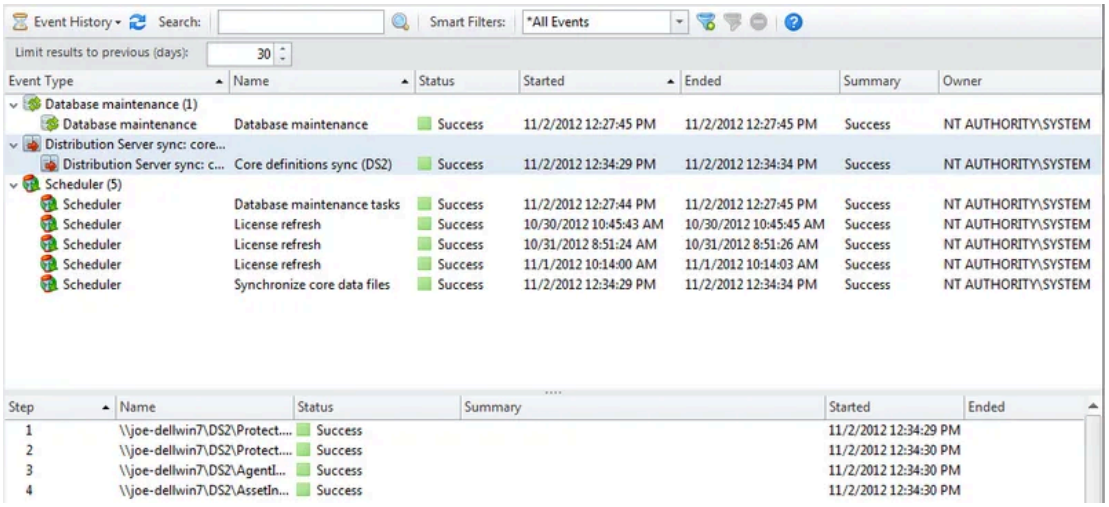
8. What is Event History?

Event History is accessed from the main menu by selecting **View > Event history**. Event History provides a way to view the background operational events that occur within Security Controls. Entries are generated for a large number of events, including:

- Database maintenance
- Distribution server synchronization
- Scheduler events
- Core engines/definitions downloads
- Core engines/definitions synchronization
- Predictive Patch downloads
- Operation result imports (patch scans, etc.)
- ESXi Hypervisor patch deployments
- Agent policy synchronization using Security Controls Cloud
- Console maintenance (a daily background task that checks the status of the certificates used by Security Controls) and determines if they are nearing their expiration date

When a background event occurs, the associated log entries are automatically recorded to Event History. Events that are scheduled will not generate any log entries until after the events have been initiated or finished.

A sample Event History is shown here. You can adjust the amount of information that is displayed by using the **Limit results to previous (days)** option. By default, all background operational events that have been generated within the last 30 days will be displayed. A maximum of 10,000 events can be displayed.



> Event History will be empty if you view it immediately after installing the program; this is because there are no event log entries to display.

Performing Actions

You can right-click on one or more events and perform the following actions:

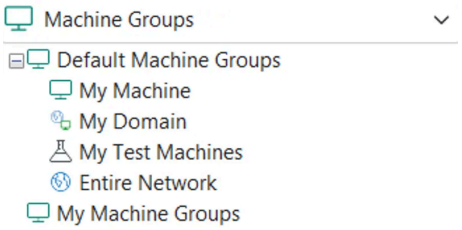
- **Acknowledge:** Changes the status in the **Acknowledge** column from No to Yes so that other administrators know it has been reviewed.
- **Export selected event history to CSV:** Exports information about the selected events to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

Related Topics

- Searching for Event Entries
- Using the Event History Smart Filter

9. About Machine Groups

Security Controls uses machine groups to keep track of the machines that are included in a particular scan. Even the local machine **My Machine** is considered a machine group. Among the predefined machine groups are:



Branch	Description
My Machine	This group includes only the local machine.
My Domain	Includes all of the machines that are a part of the domain to which the scanning computer is joined.
My Test Machines	A group of machines that represent a 'smaller' view of your actual network environment. A machine of each type that is typically scanned should be added to this group and used for testing purposes.
Entire Network	Includes all machines currently viewable in the discoverable network.

You can perform a number of **agentless operation**s on your machine groups. If a machine in a machine group contains an agent, it means the machine can be acted upon by both the console (via an agentless operation) and by the machine's **agent policy**. Agent-based machines that are not part of a machine group can be tracked in Machine View and Scan View using the **Assigned Group** tag.

Related Topics

- **Creating a New Machine Group**
- **Organizing Machine Groups**
- **Performing Actions on Machine Groups**
- **Searching Machine Groups**

10. About Patch Groups

Security Controls provides the ability to **use a patch group** to scan for a particular set of patches.

Example 1: Suppose Company A has a patch approval process under which they've certified four patches as being mandatory for their organization. They want to scan just for those four patches, receive compliance reports, and then be able to patch for those specific items. By creating a patch group, they can then scan for only those selected patches.

Example 2: Suppose you identify a certain patch as being critical for your organization. You can create a patch group with just this patch. When you create the group, you can browse patches from the list and select a product and product level and then a patch. Security Controls will scan for all instances of that QNumber, not just for the product and product level that you select. You can perform a scan using the patch group and a scan will be done just for the selected patch.

When scanning for the specified patches, the program will reference the **Tools > Options > Scan > Use replacement patches setting** to determine if patches that have been replaced should be included in the scan results.

> When Security Controls uses a patch group to scan for selected patches, it always scans for and reports on the status of all product levels.

11. About Patch Scan Templates

Security Controls comes with two predefined patch scan templates: **Security Patch Scan** and **All Patches**. While these templates are good for most scanning activities, some administrators desire a higher level of flexibility when scanning machines. To this end, Security Controls includes the ability to create any number of custom scan templates granting you the means to completely customize the way that machines are scanned.

Patch scan templates enable you to:

- Scan a smaller or larger number of machines simultaneously
- Customize what is actually scanned for or ignored
- Specify which, if any, filters are used (you can filter by product, patch, patch type, or vendor severity level)
- Configure automatic email notifications

12. About Windows Patch View

Windows Patch View is an extremely powerful and flexible tool. It is used to create custom patch groups that enable you to scan for a particular set of patches. Windows Patch View also enables you to display detailed information about every product patch contained in the data definition file. It organizes the information so it is displayed in one comprehensive view, regardless of when the patches were released.

With Windows Patch View you can:

- **Create and maintain patch groups**
- Identify **Checkpoint Patch Chains**
- Quickly and easily display the list of products supported and the associated patches with each product
- Display detailed information about any patch
- Filter the information and drill down into the table for a more detailed analysis
- Search for specific patches or patch components
- Perform actions on each patch
- Quickly determine which machines have a selected patch installed or are missing a selected patch

Windows Patch View is accessed by selecting **View > Windows Patches** or by creating a new patch group (**New > Windows Patch > Patch Group**).

Checkpoint Patch Chains

In May 2025, Microsoft introduced checkpoint patches as a method for delivering smaller and more incremental updates. These updates contain only the code changes that have occurred since the previous deployment, ensuring that each patch is concise and targeted.

Checkpoint patch chains are sequences of updates where each patch depends on the successful installation of its predecessor. By following these chains, systems can be updated incrementally, reducing the risk of errors and ensuring that changes are applied in the correct order.

Within Ivanti Security Controls, certain prerequisite patches that form part of a checkpoint chain are identified with a flag icon (⚑) on the View Machines → Windows Patches tab under the applicable Bulletin Title. It is important to note that the flagged patch is not necessarily the latest patch available, but rather a required prerequisite within the checkpoint chain.

This checkpoint patch identification allows administrators to easily recognise and manage the sequential patches necessary for full compliance and system security.

If you roll back the latest patch in a checkpoint chain, all patches deployed as part of that chain rolls back. This rollback behavior is controlled by Microsoft and applies to all checkpoint-based OS patches.

13. About Product Level Groups

Security Controls provides the ability for agents to use a product level group to deploy a particular set of product levels. A product level might be a particular version of Windows 10 or it might be a service pack for another product or Windows operating system.

Example 1: Suppose Company A has a patch approval process under which they've certified four product levels as being mandatory for their organization. They do not want to deploy any patches, just the four product levels. They also want to be able to receive compliance reports. By creating a product level group they can deploy only the specified product levels and receive a variety of deployment reports.

Example 2: Suppose you identify a certain product level as being critical for your organization. You can create a product level group that contains just this product level. When your agents perform a deployment, the only product level that will be deployed will be the product level defined in the group.

For information on implementing and using product level groups, see **Creating and Editing a Product Level Group** and **Creating and Configuring a Patch Task**.

Notes About Product Level Groups

- Product level groups apply only to agents and not to agentless deployments.
- Product level groups apply only to Windows Patch Tasks and not to Linux Patch Tasks.
- Agent-based product level deployments are tracked the same way as any other agent activity. See **Monitoring Agents** for details.
- If an agent machine is missing multiple product levels, only one product level will be installed at a time. Security Controls Agent will begin by initiating the download of all missing product levels. Operating system product levels are downloaded at a higher priority, but whichever product level is available first is the one that is first installed. After that product level is successfully installed, the machine is restarted, rescanned, and the process is repeated until all product levels are deployed or until the daily limit is reached.
- The downloads occur in the background using idle bandwidth not being used by other applications on the agent machine. Foreground tasks such as Web browsing are not affected by the product level download process.
- The number of product levels that can be deployed in one day is defined by the **Limit deployments (per day)** option on the agent patch task.

14. About the Deployment Tracker Dialog

The Deployment Tracker dialog provides at-a-glance information pertaining to patch deployment status. The information is displayed in two lists in the right pane. The **Machine progress** list shows the status of deployments on a machine basis and the **Patch progress** list shows the status of each individual patch that is scheduled for deployment.

> In order for your agentless machines to send status messages to the console, they need to know the valid name or IP address of the console. The valid names and IP addresses are defined using the **Console Alias Editor** and are passed to the machines when a patch deployment is initiated from the console.

You can view the current state of a deployment in either list. The states of a successful patch deployment are:

- Copied to machine
- Scheduled
- Executing
- Executed (pending reboot)
- Pending rescan
- Successfully installed

You can use the buttons, boxes and check boxes in the dialog to specify what deployment information is displayed in the dialog.

- **Refresh:** Refreshes the content in the dialog.
- **Update speed:** Specifies how often you want the patch deployment information within Deployment Tracker to be updated. Each update request causes the console to access the database and then report the information within Deployment Tracker. You may want to specify a slower update speed if you find that your database is being overtaxed by frequent update requests.
- **View deploy rules:** Shows the patch deployment template rules that were used when scheduling the deployment. This button is not available if the **View by days** check box is enabled.
- **Show in progress:** Shows the patch deployments that have not yet completed installation. If the status remains yellow, it could be an indication that the remote machine cannot communicate back to the Deployment Tracker.
- **Show failures:** Shows patch deployments that didn't fully take and that require more research. The **Operations Monitor** may provide additional information if one of the main steps in the deployment process failed.
- One of the more common reasons for seeing a "Failed" item in Deployment Tracker is because a patch that requires a reboot to complete was deployed but 'Never Reboot' was specified in the deployment template. If you receive a "Failed" status in Deployment Tracker, check the **Patch Details** for the patch in question to see if a reboot is required to complete the installation of this patch.
  Show successfully completed: Shows the deployment tasks that have been successfully implemented.
- **View by days or deployment:** Use this area to specify whether you want to view all of the deployments that have occurred over the last specified number of days or view just a specific deployment.
  - **View by days:** If this check box is enabled, it means that you can specify how many days' worth of deployments to show in the right pane.
  - **Recent deployments:** This area is only available if the **View by days** check box is not enabled. It enables you to select which specific patch deployment you want to see information about in the right pane. When using this area, you can only select one deployment at a time. The patch deployments that are available for selection is defined by the **Tools > Options > Display > Recent items** box.

15. About Machine View

Machine View is an extremely powerful and flexible tool. It enables you to display current information about every machine in your network that has been previously scanned and whose information resides in the database. All of your machine information is available in one location regardless of when the machines were scanned. The information is organized according to the type of action that was performed on each machine (patch scan, asset scan, etc).

Machine View provides an easy method for both viewing and managing the current security state of your machines — across both agent-based and agentless systems. Machine View differs from **Scan View**, which requires you to first locate the scan in which the machine was assessed before drilling down to view the machine's scan summary.

The advantages of Machine View include:

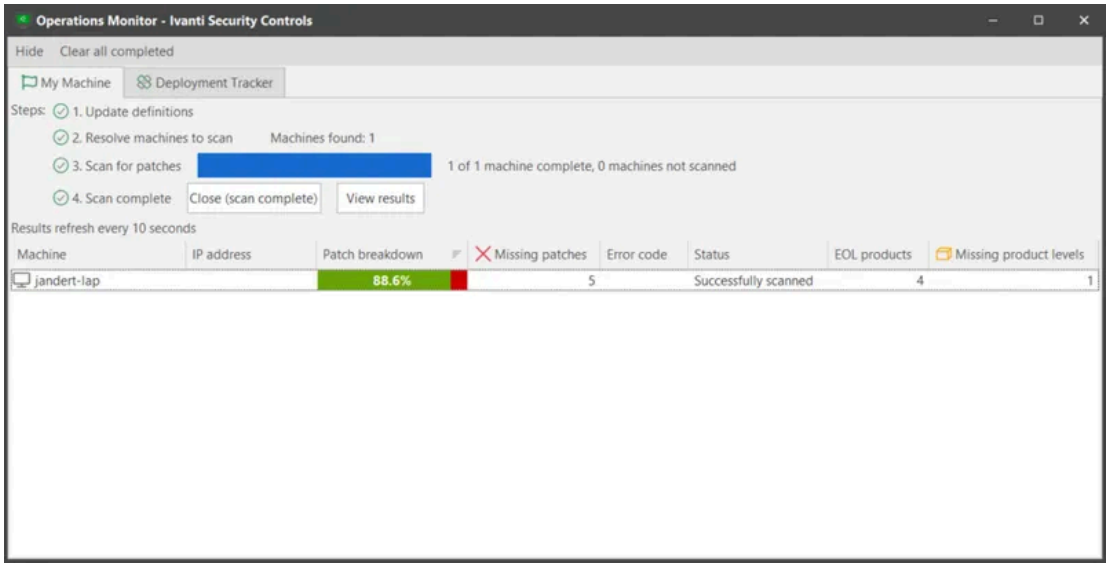
- You are not restricted to viewing just those machines involved in a particular scan. You can view all the machines that have ever been scanned.
- You can quickly assess the status of all machines in your organization.
- You can view patch and asset information from the same location. With Scan View you can only view patch information.

16. About the Operations Monitor

The Operations Monitor is designed to give you a single console from which to monitor background tasks. The background tasks currently monitored include patch scans, patch downloads, patch deployments, ESXi Hypervisor scans and deployments, asset scans, power management tasks, agent installations and results, script executions, and test patch deployments.

The Operations Monitor is displayed automatically whenever one of these background tasks is performed. To manually access the Operations Monitor, select **View > Operations Monitor**.

You can export machine information from any of the Operations Monitor tabs by right-clicking in the machine grid and selecting **Export selected machines to CSV**. To add or remove columns in the bottom pane, right-click on a column heading and select **Column Chooser**.



Field	Description
Hide	Minimizes the Operations Monitor dialog.
Clear All Completed	Removes all completed tasks from all tabs.
Patch scans	Displays a unique tab for each machine group, domain, or favorite that is being scanned. The tab shows the steps involved in the patch scan and the progress of each step. See **Monitoring a Patch Scan** for more information.
Patch downloads tab	Displays status information about patch downloads that have been initiated from the console.
Deployment Tracker tab	Monitors the status of patch deployment tasks. See **About the Deployment Tracker Dialog** for more information.
ESXi Hypervisor scans	Displays a unique tab for each ESXi Hypervisor scan operation. The tab shows the steps involved in the scan and the progress of each step. The results of the scan can be found on the **Bulletins** tab of your **managed** or **unmanaged** hypervisor. Remember to refresh the **Bulletins** tab to view the most current information.
ESXi Hypervisor deployments	Displays a unique tab for each ESXi Hypervisor deployment operation. The tab shows the steps involved in the deployment and the progress of each step. When the operation is complete, a summary of the deployment steps is available within the **Event History** log, which you can get to by clicking the **View deployment details** link.
Asset scans	Displays a unique tab for each machine group, domain, or favorite that is being scanned. The tab shows the steps involved in the asset scan and the progress of each step. See **Monitoring an Asset Scan** for more information.
Power Tasks	Displays status information about power management tasks that run immediately after they are initiated. For more information on power commands initiated using the Power Management function, see **Monitoring a Power Task**. For information about power commands initiated using the Virtual Inventory feature, see **Performing Actions on Virtual Machines**.
Agent Installations tab	Displays status information about agents that have been "push installed" from the console to the machines in your network.
Agent Command Results tab	Displays status information about **commands** that have been issued to your agents.
Script executions	Displays a unique tab for each script that is executed. The tab shows when a script is running, when it is complete, and the status of the script when it is complete (successful, error, etc.).

Field	Description
Test Patch Deployment tab	Security Controls includes the ability to perform a **test deployment** for any patches that are to be deployed. This is especially useful for patch deployment that has been scheduled for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail. The **Test Patch Deployment** tab displays the results of a test deployment. A test deploy returns either a pass or a fail depending on what it finds. For example, if the Workstation or Scheduling services are not started in a particular machine, Security Controls cannot deploy patches to it and a test deploy will return a failing result.

17. About the Scheduled Console Tasks Manager

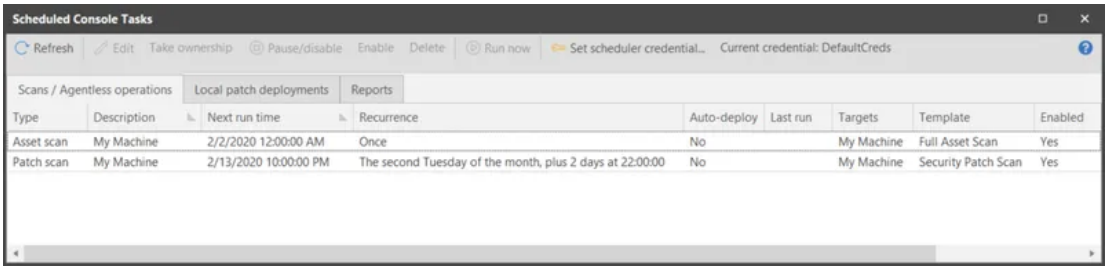
The Scheduled Console Tasks Manager is designed to give you a single location from which to monitor the tasks currently scheduled on the console. These tasks can include patch scans, asset scans, patch deployments to the console machine, patch deployments to hosted virtual machines, power tasks run against the console, script executions, and scheduled reports. The Scheduled Console Tasks Manager uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Scheduler Library > Ivanti > Security Controls** tree.

> To monitor scheduled tasks on your remote machines, use the Scheduled Remote Tasks Manager.

You can use the Scheduled Console Tasks Manager to modify and delete the scheduled tasks. For example, if you know a certain machine will be unavailable on a certain day you can reschedule any scans that are set to be performed on that machine.

How to Access the Scheduled Console Tasks Manager

You access the Scheduled Console Tasks Manager by selecting **Manage > Scheduled Console Tasks**.



The following commands are available using the buttons on the dialog or by right-clicking a task on any of the tabs.

Field	Description
Refresh	Refreshes the content in the dialog.
Edit	Edit the selected task.
Take ownership	Transfers ownership of the selected task(s) to you. For example, you may need to take ownership of one or more tasks that were originally scheduled by someone who is no longer a Security Controls administrator. IMPORTANT! Before taking ownership, make sure you have the credentials needed to access the machines targeted by this scheduled task.
Pause/disable	Pause or temporarily disable the selected task(s). This button is only available if the selected task(s) are currently enabled.
Enable	Enable the selected task(s). This button is only available if the selected task(s) are currently disabled.
Delete	Delete the selected task(s).
Run now	Run the selected task(s) right now. The task(s) will not be deleted and will also be run at their scheduled date and time.
Set scheduler credential	Specify the credential to use for all scheduled tasks. In order to succeed the scheduler credential must match the credential of the person logged on to the console when the schedule process is initiated. If you have **more than one administrator**, each administrator should set their own unique scheduler credential. If you **delete the credential** that is designated as the scheduler credential, the next time you schedule a console task you will be prompted to assign a new scheduler credential.
Current credential	Identifies which credential is currently being used as the scheduler credential.
Scans / Agentless operations tab	Displays tasks that are scheduled on the console and performed on your target machines. This includes all scheduled patch scans, asset scans, script operations runs, Wake-on-LAN requests, patch deployments to offline hosted virtual machines and virtual machine templates, etc.
Local patch deployments tab	Displays all patches that are scheduled to be deployed to the local (console) machine. Power tasks that will run against the console will also be displayed here.
Reports tab	Displays all reports scheduled to be generated.

18. About the Scheduled Remote Tasks Manager

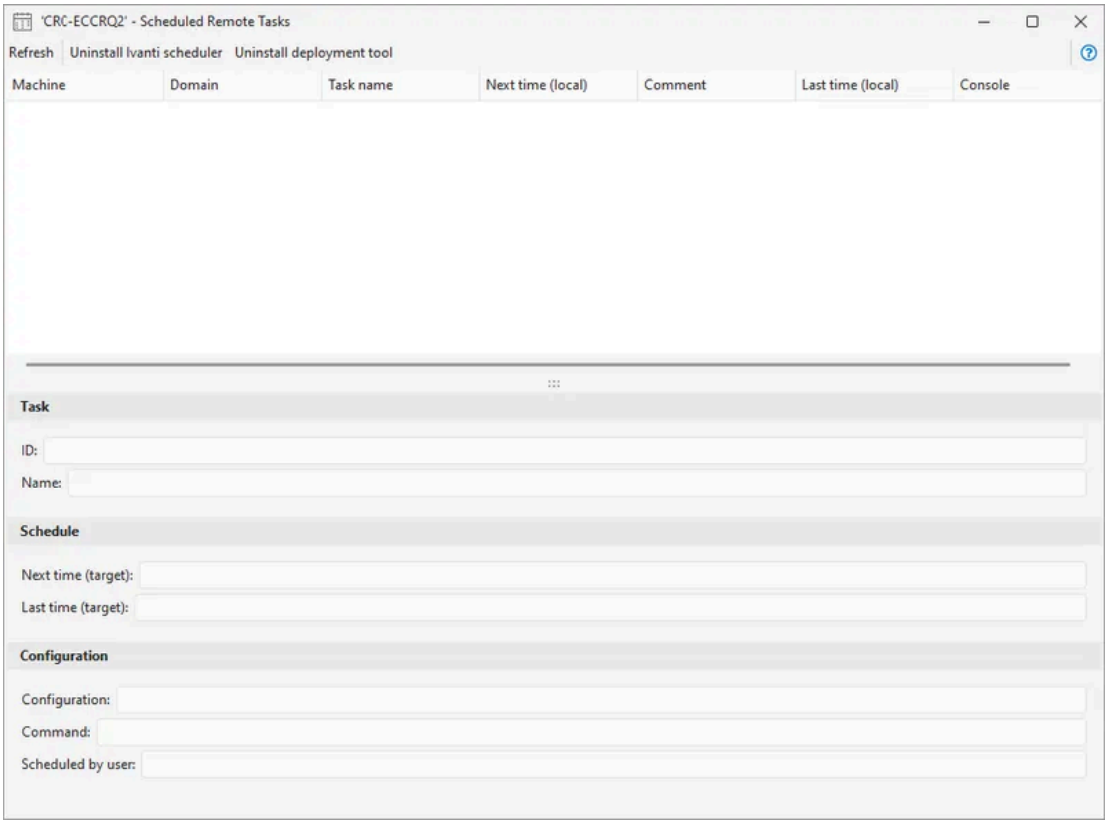
The Scheduled Remote Tasks Manager is designed to monitor the power tasks and patch deployment tasks currently scheduled on a remote target machine. You can use it to modify and delete the scheduled tasks. For example, if you know a certain machine will be unavailable on a certain day you can reschedule any tasks that are set to be performed on that machine.

The Scheduled Remote Tasks Manager uses the services of the Microsoft Task Scheduler 2.0 or later to display and manage the scheduled tasks on a target machine.

> The Scheduled Remote Tasks Manager is different than Deployment Tracker. The Scheduled Remote Tasks Manager enables you to monitor and modify *scheduled* power and patch deployment tasks, while Deployment Tracker only enables you to monitor *active* deployment tasks (and not power tasks).

How to Access the Scheduled Remote Tasks Manager

You access the Scheduled Remote Tasks Manager from Machine View or Scan View by right-clicking on a machine and then selecting **View scheduled tasks**. Multiple instances of the Scheduled Remote Tasks Manager can be active at the same time.



Field	Description
Refresh	Refreshes the information displayed in the dialog.
Uninstall Ivanti Scheduler	Removes the Ivanti Scheduler from the machine. Use of the Ivanti Scheduler was **discontinued in v2023.2** and it should be removed from all target machines. Be careful not to remove the Ivanti Scheduler until you are certain that all scheduled tasks still using this scheduler have been run.
Uninstall deployment tool	Removes the tool used by Security Controls to execute a deployment package on the machine. This tool gets pushed to the target machine when a patch deployment is initiated from the console. You can remove this tool if you want to eliminate any temporary files on the machine.
Top pane	The top pane contains a table that displays the tasks (if any) that are currently scheduled for the selected machine. If you select a task, details about that task are displayed in the bottom pane. You can sort this table a number of different ways simply by clicking the individual column headers. You can also perform a number of actions by right-clicking on a task.
Bottom pane	The bottom pane contains details about the task that is selected in the top pane. You can see the task ID, when it is scheduled and how it is configured.

19. About Third-Party Applications

Security Controls can scan for and deploy a number of free third-party applications, including:

- RealNetworks RealPlayer
- Mozilla Firefox
- Adobe Reader
- Apple QuickTime
- And more ...

To do this you simply scan your machines to identify the machines that are missing the third-party applications and then deploy the desired application(s) to the machines you specify. See **How to Scan for Third-Party Applications** and **Deploying Third-Party Applications** for more details.

20. About the My Test Machines Group

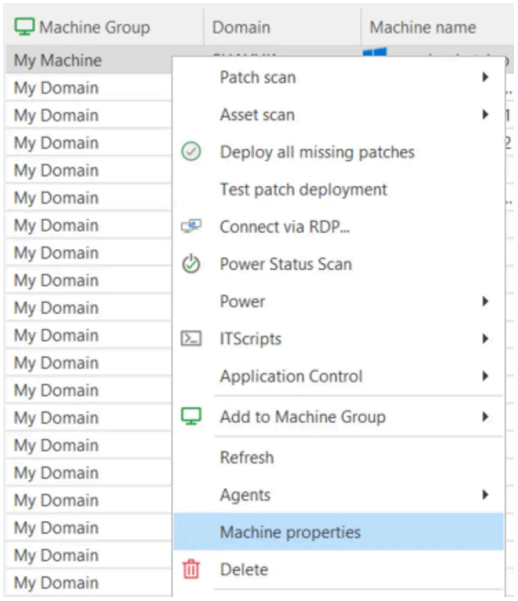
One hard lesson that many administrators have learned is the importance of testing new implementations before rolling them out to critical production systems. In anticipation of this need we have created a default group for you to use for this purpose.

You can use this group just like any other. Simply add either lab machines or low priority production systems to it. You should take care to make sure that you have a representative mix of machines in the group in order to cover the production systems on your network.

For instructions on adding machines to this group, see **Machine Group Pane: Middle Section**.

21. Accessing Machine Properties

You can define several different properties for each machine contained in Security Controls's database of managed machines. You can assign properties to individual machines or to a set of selected machines. You access the **Machine Properties** dialog from within Machine View or Scan View by right-clicking the desired machine(s) and selecting **Machine Properties**.



The **Machine Properties** dialog is displayed. See Managing Individual Machine Properties if you are defining properties for an individual machine or Managing Multiple Machine Properties if you are defining properties for two or more machines.

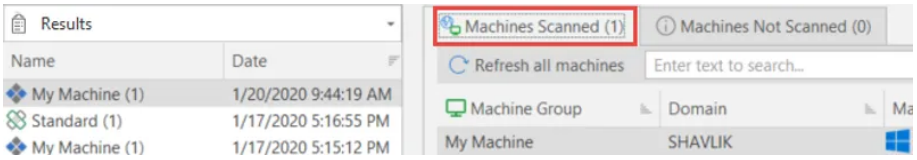
22. Accessing Patch Scan Results (Scan View)

Patch scan results are available immediately following a successful scan by clicking the **View results** link on the **Operations Monitor** dialog (see **Monitoring a Patch Scan**). The scan results are also available when you select a previous scan from the **Results** list in the navigation pane.

> If scan results are not displayed it could be because the program's background services do not have the proper credentials to use when making a connection to the database. For more information see **Performing a New Installation**.

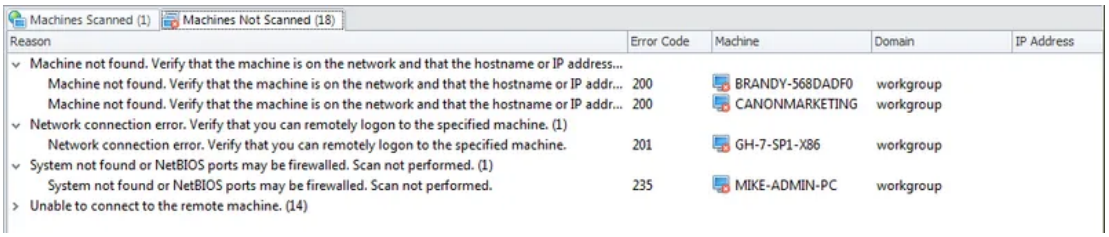
Machines Scanned

Machines that were successfully scanned will be included on the **Machines Scanned** tab. For information on understanding and using your patch scan results, see **Navigating the Scan View Grid**.



Machines Not Scanned

Any machines that the program was unable to scan will be contained on the **Machines Not Scanned** tab. There may be several reasons why a particular machine was not scanned. Error codes are provided that explain the reason for a particular failure. The error codes are described in greater detail in the knowledge base on the **Ivanti Community (opens in a new window)**.

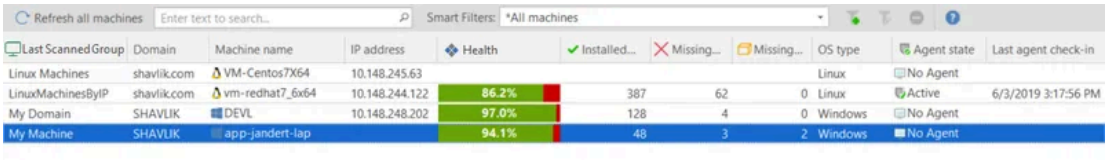


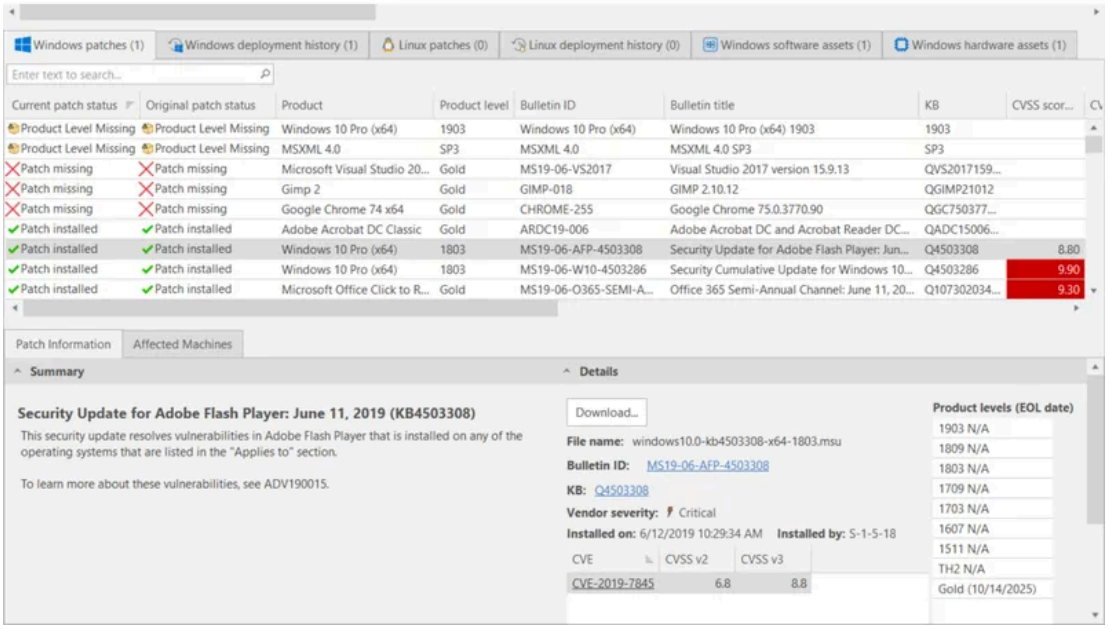
> TIP: You can generate a **Machines Not Scanned report** that will contain additional information.

You can right-click on a machine and perform a number of different actions. See **Performing Actions on Machines** for more details.

23. Accessing Machine View

Machine View is accessed from the main menu by selecting **View > Machines**.





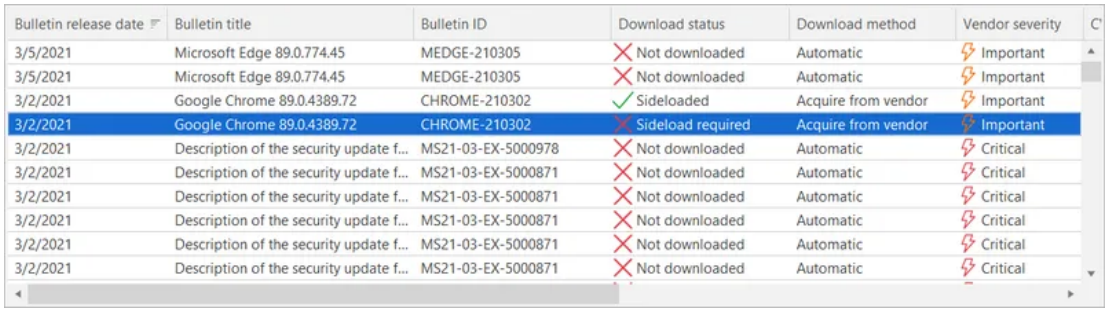
For information on using Machine View, see **Navigating Machine View**.

> Machine View will be empty if you view it immediately after installing the program. This is because there is no machine information in the database to display.

24. Manually Acquiring Patches from the Vendor (Sideloading)

Sometimes a patch cannot be downloaded by Security Controls. This can happen for a number of different reasons. For example, the patch might be an ISO that represents a missing Windows 10 product level, it might be an old patch that has been removed by the vendor, a login to the vendor website might be required to access the patch, the patch might have been only available via a temporary link, etc.

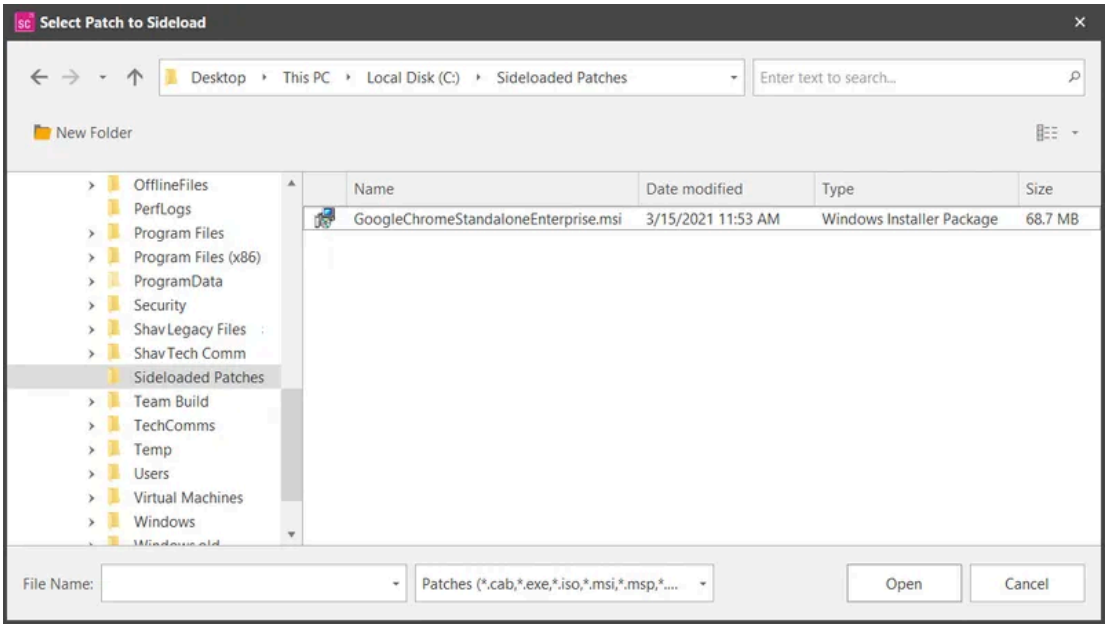
If a patch cannot be automatically downloaded, the phrase **Sideload required** will be displayed in the **Download status** column in Machine View, in Patch View, in Scan View and on the **Deployment Configuration** dialog.



Bulletin release date	Bulletin title	Bulletin ID	Download status	Download method	Vendor severity
3/5/2021	Microsoft Edge 89.0.774.45	MEDGE-210305	Not downloaded	Automatic	Important
3/5/2021	Microsoft Edge 89.0.774.45	MEDGE-210305	Not downloaded	Automatic	Important
3/2/2021	Google Chrome 89.0.4389.72	CHROME-210302	Sideloaded	Acquire from vendor	Important
3/2/2021	Google Chrome 89.0.4389.72	CHROME-210302	Sideload required	Acquire from vendor	Important
3/2/2021	Description of the security update f...	MS21-03-EX-5000978	Not downloaded	Automatic	Critical
3/2/2021	Description of the security update f...	MS21-03-EX-5000871	Not downloaded	Automatic	Critical
3/2/2021	Description of the security update f...	MS21-03-EX-5000871	Not downloaded	Automatic	Critical
3/2/2021	Description of the security update f...	MS21-03-EX-5000871	Not downloaded	Automatic	Critical
3/2/2021	Description of the security update f...	MS21-03-EX-5000871	Not downloaded	Automatic	Critical
3/2/2021	Description of the security update f...	MS21-03-EX-5000871	Not downloaded	Automatic	Critical

In order to deploy a patch that cannot be automatically downloaded, it must first be *sideloaded*. Sideloading means the patch file is downloaded manually, its contents are verified and then the file is saved to the proper directory on the console machine. The exact process is as follows:

1. Select the patch within Machine View, Patch View or Scan View.
2. In the bottom pane, click **Download information**.
   Information on downloading the patch from the vendor's website will be displayed in a browser.
3. Follow the instructions for manually downloading the patch file to the console machine.
   The best approach is to create a new folder that is used exclusively for sideloaded patch files. Be sure to download the correct language version of the patch. The preferred language for your console is specified on the **Patch view download status icon language option**.
4. Select the patch in the grid.
5. Right-click the patch and then select **Sideload patch**.
   The **Select Patch to Sideload** dialog is displayed.



Select the patch file that you previously manually downloaded and then click **Open**.
The file will be processed and readied for deployment. Specifically:

- An attempt is made to verify the digital signature of the patch file.
- If the patch file is not signed, you will be prompted to manually confirm the file details. For your convenience, a SHA-256 file hash of the file will be displayed.
  If needed, the patch file will be renamed to match the naming convention used within Security Controls.
- Oftentimes, the patch name used within Security Controls is different than the name given by the vendor. This is done to avoid duplicate names. One way to see the expected file name is to locate the patch within Machine View or Patch View and view the file name information.
  The patch file is moved to the patch download directory.
  The **default location** is C:\ProgramData\Ivanti\Security Controls\Console\Patches.

When the process is complete, the **Select Patch to Sideload** dialog will close and the patch's download status will change to **Sideloaded**.

At this point, the patch is ready to be deployed using the normal deployment process.

25. Activating Security Controls

Until you activate Security Controls, you are very limited in the actions you are allowed to perform. You can use the following activation methods:

- **License Key Activation Method** This is the primary activation method. It should be used:
  - If you are a new customer and you have an internet connection from the console
  - If you need to refresh your license following an upgrade
  - If you do not have an internet connection from the console

Trial Activation Method This is the activation method that should be used if you are using the program on a trial basis. It enables you to test all the capabilities of Security Controls, but only for 60 days. You are also limited to 50 license seats. When the trial license expires, the program will stop refreshing its data files and many of the program features will no longer be available.

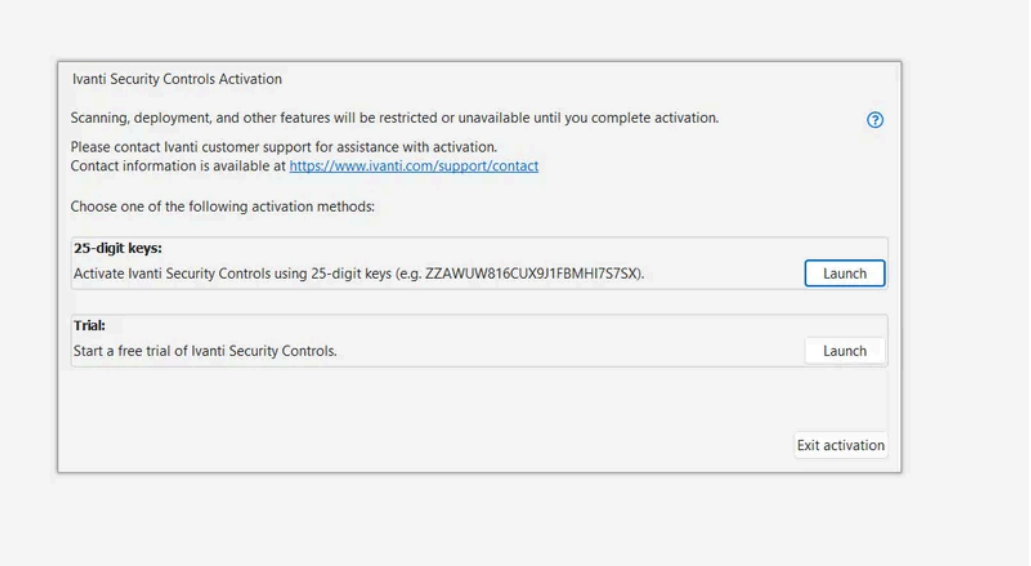
License Key Activation Method

If You Have an Internet Connection

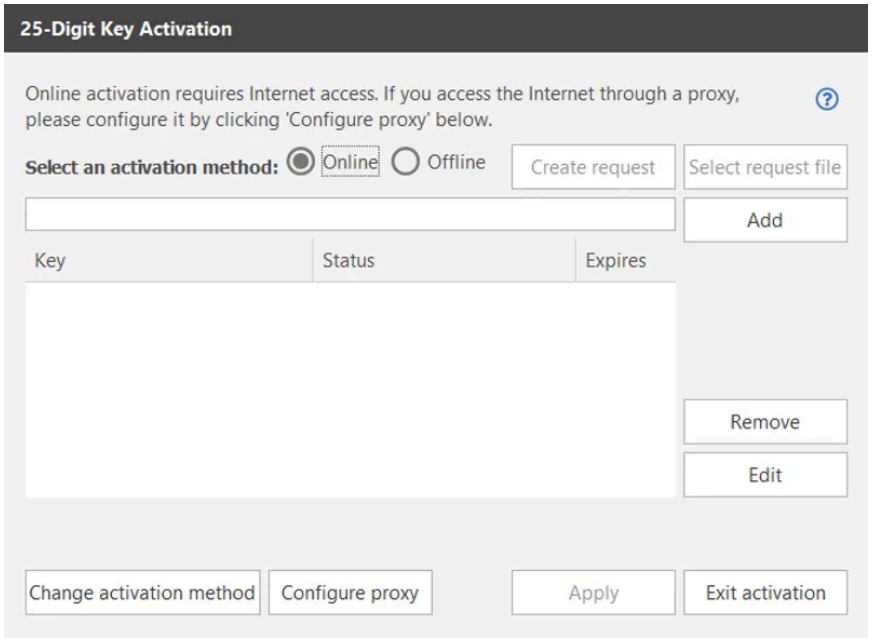
You activate the program by entering one or more activation keys.

1. If you have an electronic copy of your license key(s) copy it to your computer's clipboard.
   Your license key is typically sent to you in an email from Ivanti when you purchase the product.
2. From the Security Controls menu select **Help > Enter/refresh license key**.
   The **Activation** dialog is displayed.

> If you have previously activated Security Controls using a key, the **25-character Key Activation** dialog will instead be displayed.



In the **25-character keys** box, click **Launch**.
The **25-character Key Activation** dialog is displayed.



Choose **Online** activation.

5. Verify that your activation key is specified in table in the center of the dialog.
   The key is automatically pasted here if it is contained on your computer's clipboard when you launch this dialog. If not, copy your key to your computer's clipboard and then paste it in the dialog by pressing Ctrl-v. Or, you can type the 25-character key into the **To manually enter a key, type it here and then click Add** box and then click **Add**.
6. If you have multiple activation keys, repeat this step as needed.
   Click **Apply**.
   If the activation is successful, the message Security Controls **product activation successfully completed** is displayed near the bottom of the dialog.
7. Click **Exit activation**.

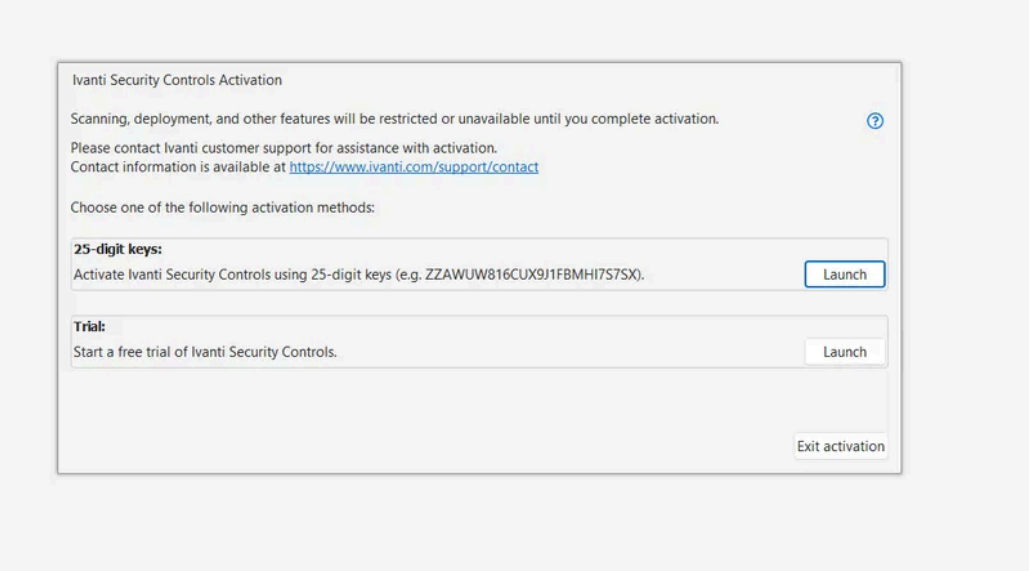
Additional Functionality

- **Remove:** Enables you to remove the selected key.
- **Edit:** Enables you to modify the selected key.
- **Change activation method:** Enables you to change to a different activation method.

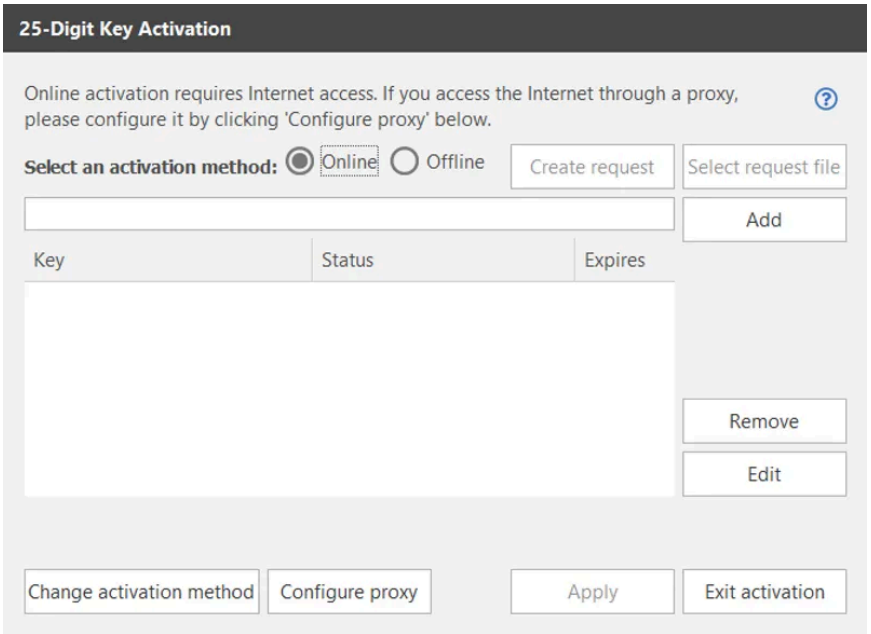
If You Do Not Have an Internet Connection (Disconnected Network Mode)

> This procedure will not work if you are at a secure site that does not allow files to be transferred out of the secure environment. For this case, see the section below titled **If You are Activating From Within a Secure Disconnected Network**.

1. If you have an electronic copy of your license key(s) copy it to your computer's clipboard.
   Your license key is typically sent to you in an email from Ivanti when you purchase the product.
2. From the Security Controls menu select **Help > Enter/refresh license key**.
   The **Activation** dialog is displayed.



In the **25-character keys** box, click **Launch**.
The **25-character Key Activation** dialog is displayed.



Choose **Offline** activation mode.

5. Verify that your activation key is specified in table in the center of the dialog.
   The key is automatically pasted here if it is contained on your computer's clipboard when you launch this dialog. If not, copy your key to your computer's clipboard and then paste it in the dialog by pressing Ctrl-v. Or, you can type the 25-character key into the **To manually enter a key, type it here and then click Add** box and then click **Add**.
6. Click **Create request**.
   Two files are generated and saved to the desktop of your console computer: an XML file named **LicenseInfo.xml** and a text file named **DisconnectedLicenseInfo.txt**. The XML file is used in this procedure; the text file can be ignored.
7. Move the XML activation request file to a computer that has an Internet connection.
8. On the Internet-connected computer, open a browser and go to **https://stlicense.ivanti.com/OfflineActivation**.
9. Upload the **LicenseInfo.xml** activation request file.
   The web portal will process the license information and generate a license file.
10. Download the processed license file and move it to the console computer.
11. Within Security Controls, select **Help > Enter/refresh license key**.
12. In the **25-character keys** box, click **Launch**.
    The **25-character Key Activation** dialog is displayed.
13. Click **Select request file**.

14. Go to the location of the processed license file and then click **Open**.
    Security Controls will process the file and the program will be activated.

Additional Functionality

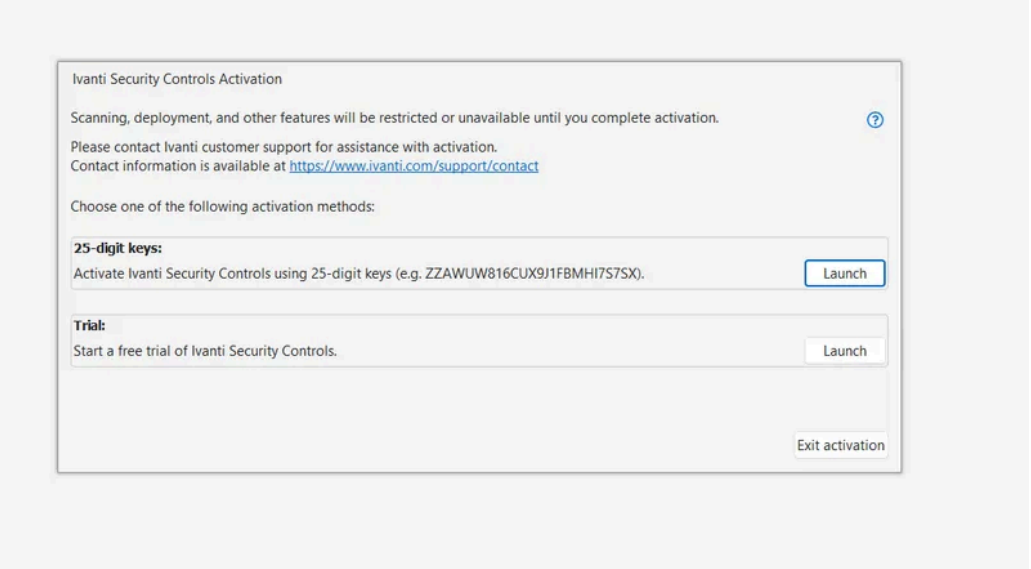
- **Remove:** Enables you to remove the selected key.
- **Edit:** Enables you to modify the selected key.
- **Change activation method:** Enables you to change to a different activation method.

If You are Activating From Within a Secure Disconnected Network

Use this activation procedure if you are at a secure site that does not allow files to be transferred out of the secure environment.

1. If you have an electronic copy of your license key(s) copy it to your computer's clipboard.
   Your license key is typically sent to you in an email from Ivanti when you purchase the product.
2. From the Security Controls menu select **Help > Enter/refresh license key**.
   The **Activation** dialog is displayed.

> If you have previously activated Security Controls using a key, the **25-character Key Activation** dialog will instead be displayed; in this case, skip to Step 4.



In the **25-character keys** box, click **Launch**.
The **25-character Key Activation** dialog is displayed.

4. Choose **Offline** activation mode.
5. Verify that your activation key is specified in table in the center of the dialog.
   The key is automatically pasted here if it is contained on your computer's clipboard when you launch this dialog. If not, copy your key to your computer's clipboard and then paste it in the dialog by pressing Ctrl-v. Or, you can type the 25-character key into the **To manually enter a key, type it here and then click Add** box and then click **Add**.
6. Click **Create request**.
   Two files are generated and saved to the desktop of your console computer: an XML file named **LicenseInfo.xml** and a text file named **DisconnectedLicenseInfo.txt**. The text file is used in this procedure; the XML file can be ignored.
7. Open the **DisconnectedLicenseInfo.txt** file and carefully copy the information contained in it to a piece of paper.
8. On an Internet-connected computer, open a browser and go to **https://stlicense.ivanti.com/OfflineActivation**.
9. Expand the **Manually Enter Activation Request Data** section.
10. Manually enter the **Activation Keys**, **Machine Identity**, **Machine Checksum** from **DisconnectedLicenseInfo.txt**, then click **Submit**.
    The web portal will process the data and generate a license file.

11. Download the processed license file and move it to the console computer.
12. Within Security Controls, select **Help > Enter/refresh license key**.
13. In the **25-character keys** box, click **Launch**.
    The **25-character Key Activation** dialog is displayed.
14. Click **Select request file**.
15. Go to the location of the processed license file and then click **Open**.
    Security Controls will process the file and the program will be activated.

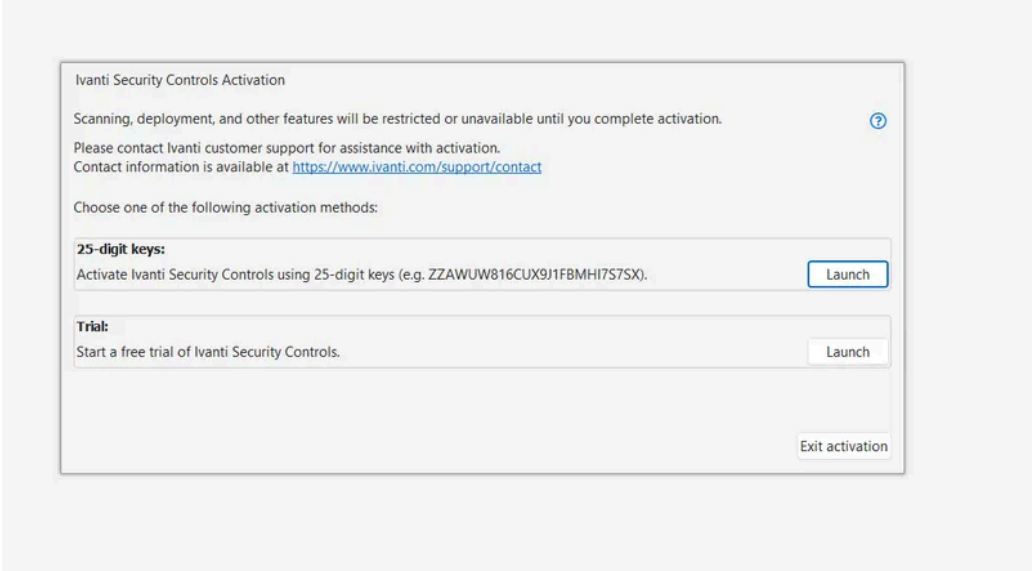
Additional Functionality

- **Remove:** Enables you to remove the selected key.
- **Edit:** Enables you to modify the selected key.
- **Change activation method:** Enables you to change to a different activation method.

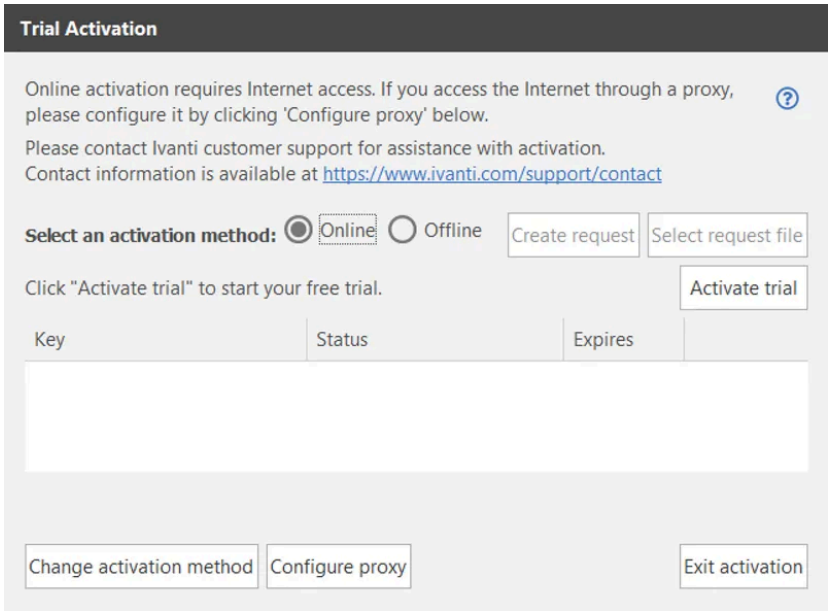
Trial Activation Method

If You Have an Internet Connection

1. From the Security Controls menu select **Help > Enter/refresh license key**.
   The **Activation** dialog is displayed.



In the **Trial** box, click Launch.
The **Trial Activation** dialog is displayed.



Choose **Online** activation mode.

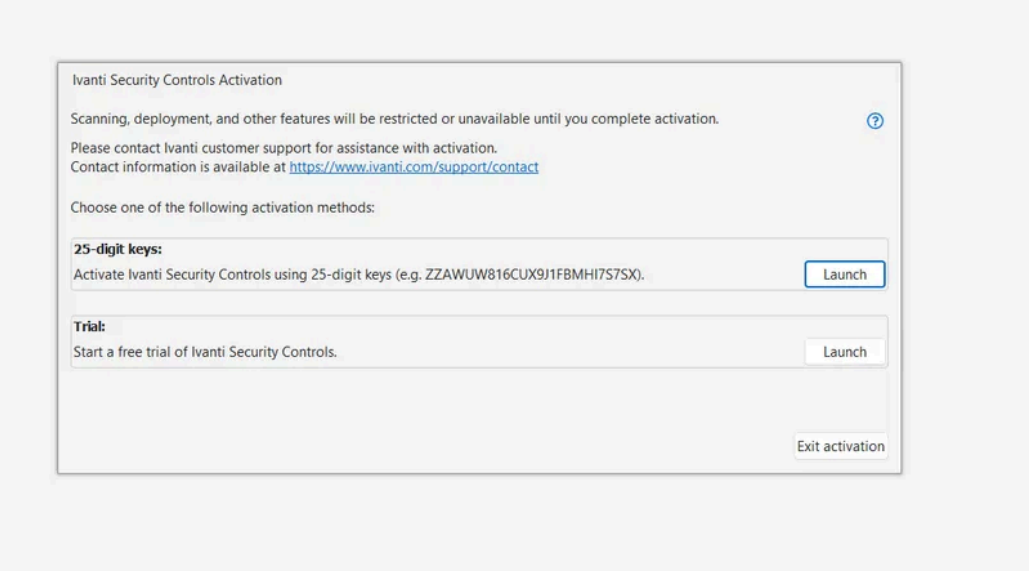
4. Click **Activate trial**.
   The trial key is automatically applied and information about the key is displayed in the dialog. If the activation is successful, the message Security Controls **product activation successfully completed** is displayed near the bottom of the dialog.
5. Click **Exit activation**.

Additional Functionality

If you want to activate the program using a purchased license rather than a trial license, click **Change activation method**.

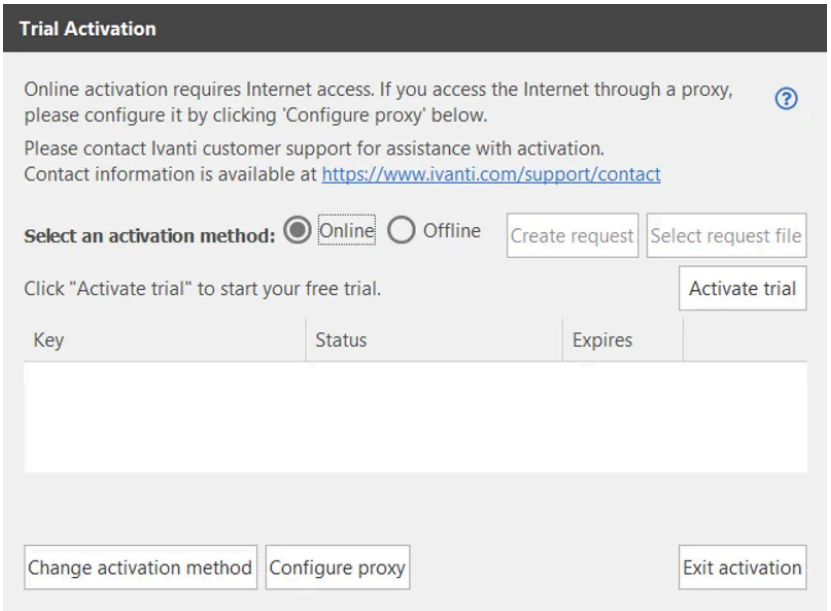
If You Do Not Have an Internet Connection (Disconnected Network Mode)

1. From the Security Controls menu select **Help > Enter/refresh license key**.
   The **Activation** dialog is displayed.



In the **Trial** box, click **Launch**.

The **Trial Activation** dialog is displayed.



Choose **Offline** activation mode.

4. Click **Create request**.
   An XML file named **LicenseInfo.xml** generated and saved to the desktop of your console computer.
5. Move the XML activation request file to a computer that has an Internet connection.
6. On the Internet-connected computer, open a browser and go to **https://stlicense.ivanti.com/OfflineActivation**.

7. Upload the **LicenseInfo.xml** activation request file.
   The web portal will process the license information and generate a license file.
8. Download the processed license file and move it to the console computer.
9. Within Security Controls, select **Help > Enter/refresh license key**.
10. In the **Trial** box, click **Launch**.
    The **Trial Activation** dialog is displayed.
11. Click **Select request file**.
12. Go to the location of the processed license file and then click **Open**.
    Security Controls will process the file and the program will be activated.

Additional Functionality

If you want to activate the program using a purchased license rather than a trial license, click **Change activation method**.

Tracking Your License

You can easily find out information about your license by selecting **Help > About** Security Controls. For more information see **How Licenses are Tracked**.

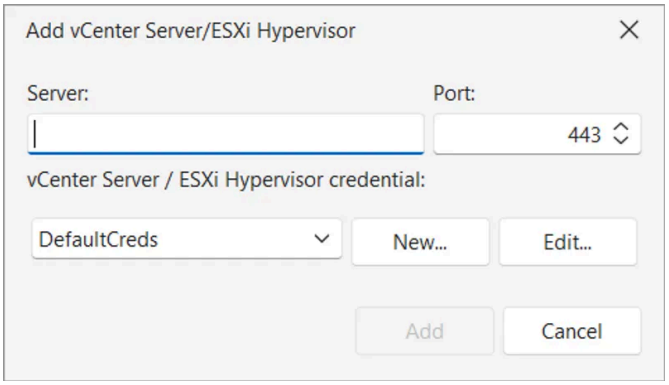
26. Adding, Editing, or Removing vCenter Servers and ESXi Hypervisors

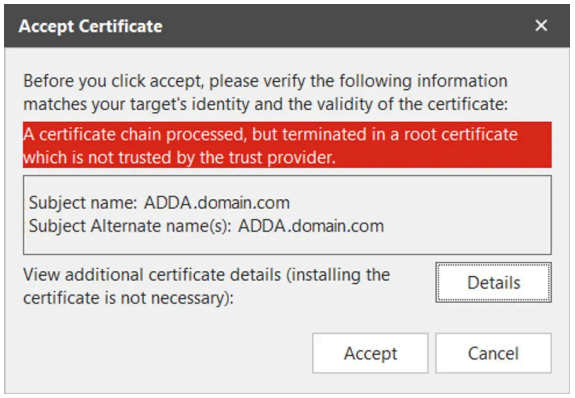
Adding vCenter Servers and ESXi Hypervisors

To add a vCenter Server or an ESXi hypervisor to Security Controls:

1. From the main menu select **Import > Add vCenter Server/ESXi Hypervisor**.
2. Specify the server, port, and credential information.
3. Click **Add**.

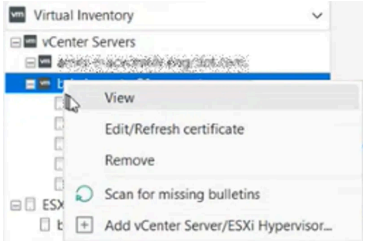
The item is added to the **Virtual Inventory list**. It is also automatically added to the **Hosted Virtual Machines tab** of your existing and future machine groups.



Field	Description
Server	Type the full path name or IP address of the vCenter Server or ESXi hypervisor that you want to add to Security Controls.
Port	The port number used when making a connection to the vCenter Server or ESXi hypervisor. The default value is 443.
vCenter Server / ESXi Hypervisor credential	Select a credential that has access to the vCenter Server or ESXi hypervisor, or click **New** to define a new credential. For more information, see Defining Credentials.
Add	After you have specified all necessary information, click **Add**. If you have not previously connected to this virtual server, a prompt is displayed asking you to verify the server's certificate. If the server's certificate is trusted by the operating system, this prompt will not be displayed.  To review the certificate information, click **Details**. If you are satisfied that you are connecting to the correct virtual server, click **Accept**. The server's certificate thumbprint will be stored and you will not have to repeat this verification process the next time you initiate a connection to this server. After a connection is made, if the item is an unmanaged ESXi hypervisor, the program will add the hypervisor and all virtual machines hosted on the hypervisor to the **Virtual Inventory** list. If the item is a vCenter Server, the program will search for all ESXi hypervisors being managed by the vCenter Server and it will add the vCenter Server, the hypervisors, and the hosted VMs to the **Virtual Inventory** list.

Viewing, Editing, or Removing vCenter Servers and ESXi Hypervisors

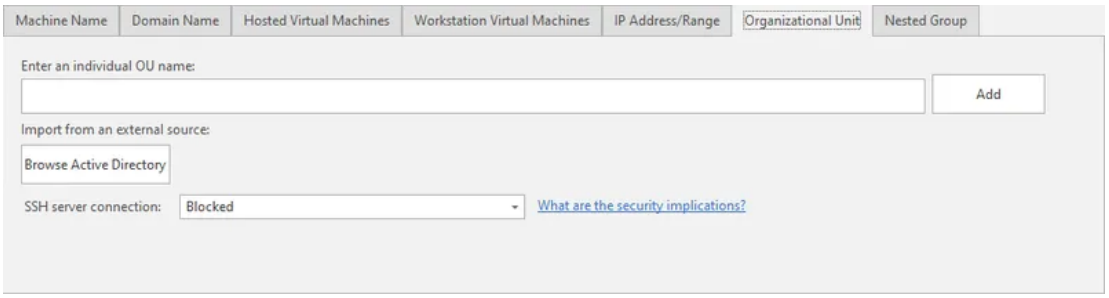
In the Virtual Inventory list, use the right-click menu to view, edit, or remove a vCenter Server or an ESXi hypervisor.



You cannot use the right-click menu to edit or remove individual ESXi hypervisors that are being managed by a vCenter Server. These two right-click menu items apply to vCenter Servers and to hypervisors that are NOT being managed by a vCenter Server (the hypervisors contained in the **ESXi Hypervisors list**).

27. Adding Organizational Units or Active Directory Security Groups to a Machine Group

Companies often split up Active Directory entities by creating multiple Organizational Units (OUs) or Active Directory Security Groups. A machine group in Security Controls can be configured to include specific organization units or Active Directory Security Groups from Active Directory. For example, you might create a machine group that includes all machines from the 'Sales' organizational unit. The machines in the OU will be automatically enumerated when the machine group is scanned.



Adding an Individual Organizational Unit

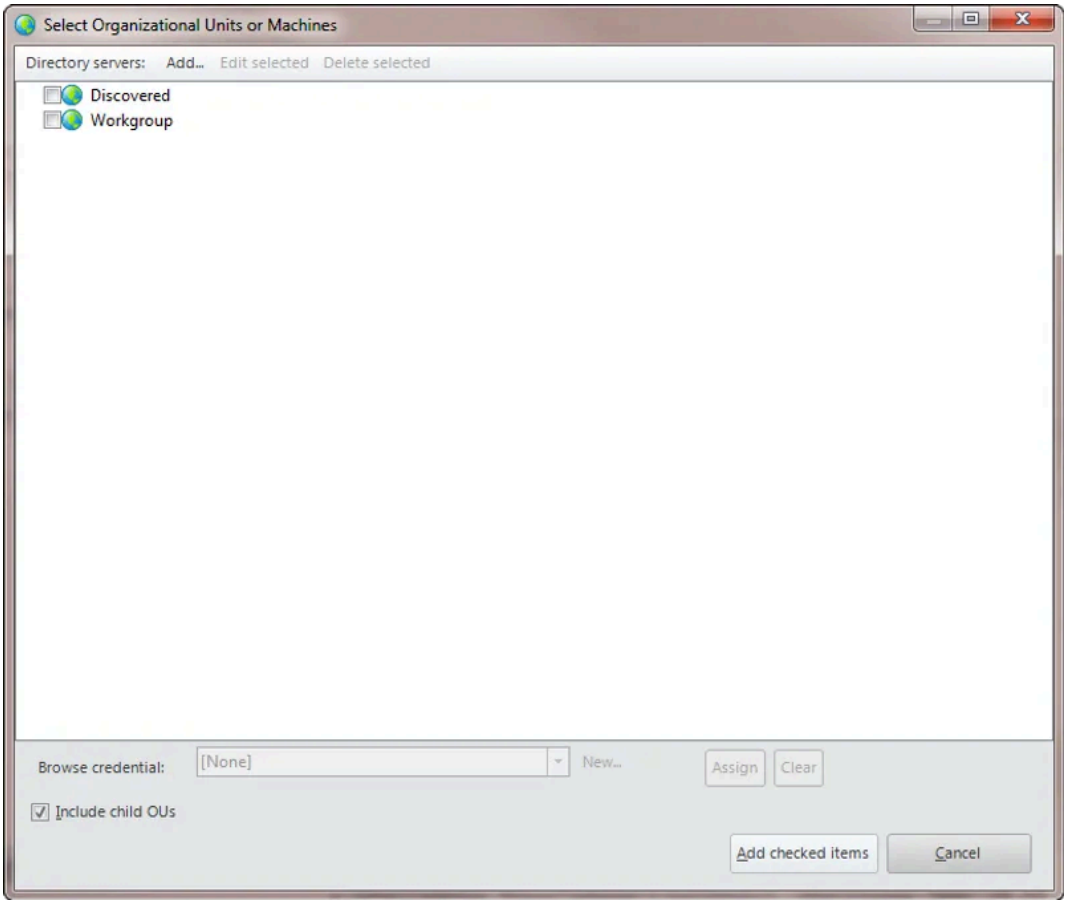
The easiest way to add an organizational unit to a machine group is as follows:

1. Access the machine group.
2. Select the **Organizational Unit** tab.
3. Type the name of the organizational unit in the **Enter an individual OU name** box.
   An OU is added in full LDAP format. For example, to add the Sales OU from the domain example.com, the format is 'ou=sales,dc=example,dc=com'. If you specify a parent OU, all children OUs will be included in the scan.
4. Choose whether you will allow SSH server connections to the machines in this organizational unit.
   The SSH protocol may be used when the console initiates a connection with the specified machines. The primary use cases are when a power status scan or a push installation of an agent are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain that the specified machines are trusted and safe, you should choose to block SSH server connections. For more detailed information, see the SSH Authentication topic.
5. Click **Add**.

Importing OUs from an External Source

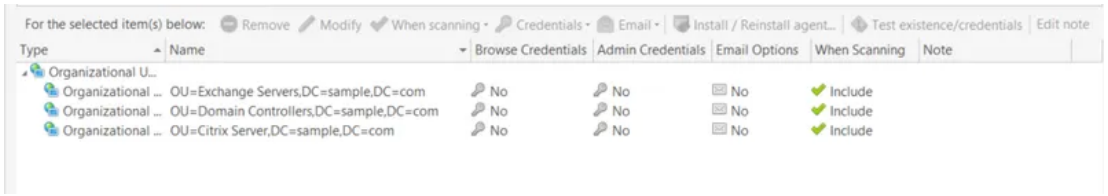
You can also add organizational units by using the **Browse Active Directory** button to import organizational unit names from an external source. This button opens a separate dialog that lists the contents of your Active Directory network. Locate the organizational units and/or machines you would like to add to the custom group, place a check mark in the desired check boxes, and then click **Add checked items**.

- If your Active Directory network is not listed, click **Add**to manually define the network.
- If you need to supply credentials in order to browse the Active Directory OUs on the available domains, in the **Browse credential** box at the bottom of the dialog select the appropriate credential and then click **Assign**.



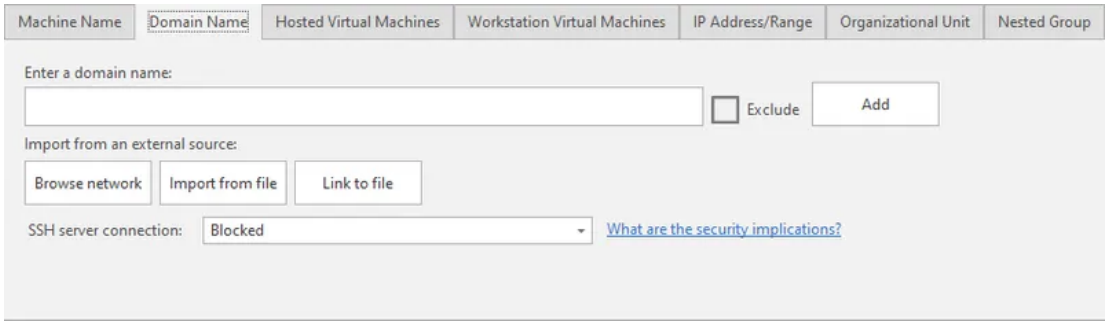
Field	Description
Add	Enables you to add an Active Directory forest that is not broadcasting its availability. You will need to provide credentials that are authorized to enumerate the forest. You can then add any items within that forest.
Edit Selected	Enables you to edit the selected entry.
Delete Selected	Enables you to delete the selected entry.
Browse Credential	To set credentials to use for browsing an Active Directory hierarchy on a remote domain: 1. Select the domain. 2. Select the proper credential. If you need to define a new credential, see **Defining Credentials**. 3. Click **Assign.**
Include Child OUs	If enabled, for every parent OU selected, all children OUs will also be included in the machine group.
Clear	Removes the credentials currently defined for the selected domain.

When organizational units are added, the new entries are displayed within the bottom portion of the machine group pane.


For the selected item(s) below:
Remove
Modify
When scanning
Credentials
Email
Install / Reinstall agent...
Test existence/credentials
Edit note
Type
Name
Browse Credentials
Admin Credentials
Email Options
When Scanning
Note
Organizational U...
Organizational ...
OU=Exchange Servers,DC=sample,DC=com
No
No
No
Include
Organizational ...
OU=Domain Controllers,DC=sample,DC=com
No
No
No
Include
Organizational ...
OU=Citrix Server,DC=sample,DC=com
No
No
No
Include

28. Adding Domains to a Machine Group

Another way that machines can be added to a machine group is by domain. Adding a domain to a machine group will result in all machines that are members of the domain being made a part of the group.



Adding an Individual Domain Name

The easiest way to add a domain to a machine group is as follows:

1. Access the machine group.
2. Select the **Domain Name** tab.
3. Type the name of the domain in the **Enter a domain name** box.
4. Choose whether you will allow SSH server connections to the machines in this domain.
   The SSH protocol may be used when the console initiates a connection with the specified machines. The primary use cases are when a power status scan or a push installation of an agent are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain that the specified machines are trusted and safe, you should choose to block SSH server connections. For more detailed information, see the SSH Authentication topic.
5. Click **Add**.

> If you want to specifically exclude a domain, enable the **Exclude** check box before you click **Add**. The domain will be added to the machine list but will not be included in any scans. See Excluding Certain Machines for more information.

Importing Domain Names From an External Source

You can also add domains by using the following buttons to import domain names from an external source.

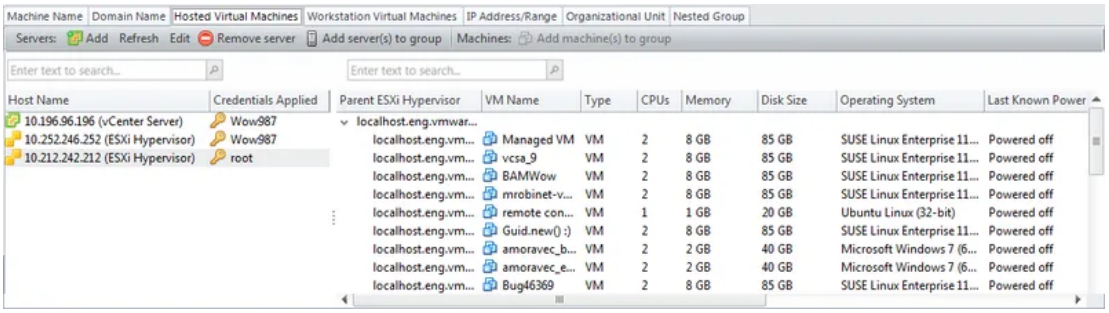
29. Adding Virtual Machines Hosted by a Server

Many organizations will host their virtual machines on one or more VMware servers. Doing so provides the means to manage the virtual machines in an organized fashion. There are two main types of VMware servers:

- **VMware ESX/ESXi Server**: A server dedicated to hosting and managing multiple virtual machines. VMware ESX/ESXi servers (also referred to as ESXi hosts or ESXi Hypervisors) are typically used in small- and medium-sized organizations that want to control multiple virtual machines from one location. The server often runs on a dedicated blade computer that is using a VMware operating system.
- **VMware vCenter Server**: This type of server is typically used by large organizations that need to manage multiple VMware ESX/ESXi servers, each of which may be running multiple VMware images. For example, you can quickly move a highly-utilized virtual machine from a busy ESXi server to another less busy ESXi server.

> TIP: For information on managing your vCenter Servers and ESXi Hypervisors, see **Using the Virtual Inventory Feature**.

You can use the **Hosted Virtual Machines** tab to log on to these servers and select the virtual machines you want to include in your machine group. The virtual machines can be in either offline or online mode. You can also use this tab to add **virtual machine templates** that may be hosted on a server. Finally, you can also add the servers themselves to the group.



1. Log on to the desired server by clicking **Add**.
2. See **Logging on to a Server** for information on logging on to a server. The credentials you use to log on to the server are called *browse credentials*. They will be used to connect to the server and to enumerate the machines hosted by the server.
   After a connection is made the server is displayed in the left-hand pane. The virtual machines hosted by the server are displayed in the right-hand pane. At this point you can either add the server itself to the group or you can add individual virtual machines.

> You must have server permission set on the datacenter, the folder, or the individual virtual machines in order for the machine to be displayed. If you don't have permission for a specific virtual machine it will not be displayed in the right-hand pane.

> TIP: The server will also be displayed in the **Virtual Inventory** list.

Add the server and/or individual hosted machines to the group.

- To add one or more servers to the group, select the server(s) in the left-hand pane and click **Add Server(s) to Group**.
- How a server in a machine group is treated depends on how the group is used. If you perform a **patch scan** on the group, all of the virtual machines hosted by the server will be scanned. If you perform a **bulletin scan** or **run a script against the group**, only the server is affected.
  To add individual hosted machines to the group, in the right-hand pane select the virtual machines you want to add and then click

Add Machine(s) to Group.

The server and/or the virtual machines are added to the bottom pane of the machine group. Be sure to supply any credentials that may be needed for the individual machines.

> You can also add virtual machine templates to the machine group. Templates are identified by a unique icon (). For complete details see Notes About Virtual Machine Templates.

You can log on to multiple servers at the same time. All virtual machines found on the servers are displayed in the right-hand table. The server table identifies the server type (VI = Virtual Infrastructure server, ESX = ESX server) and the server name. The virtual machine table contains a large amount of information about each virtual machine, including:

- **Parent ESX Server**: The name of an ESX server being used to host virtual machines.
- **VM Name**: The name of a virtual machine being managed by a server.
- **CPUs**: The number of Central Processing Units (CPUs) available to the virtual machine.
- **Memory**: The amount of memory (MB) allocated to the virtual machine.
- **Disk Space**: The amount of disk space (GB) allocated to the virtual machine.
- **Operating System**: The operating system being used on the virtual machine.
- **Last Known Power State**: The last known state of the virtual machine (Powered On, Powered Off, or Suspended)
- **IP Address**: The IP address of the virtual machine.
- **Host Name**: The name of the machine on the network that is hosting the virtual machine.

You can reorder the columns in both tables by clicking and dragging the column headers to new locations. You can also click within a column header and sort the column in ascending or descending order.

The **Hosted Virtual Machines** tab contains the following buttons:

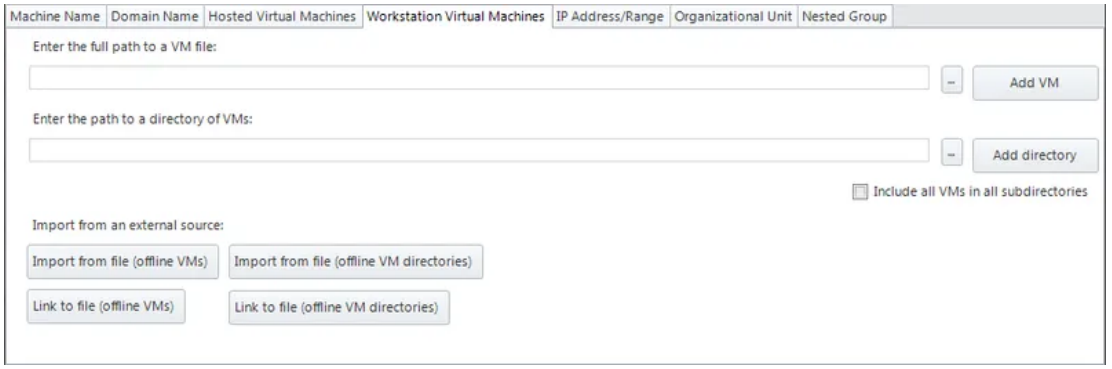
Button	Description
Add Server	Enables you to log on to a VMware ESX server or virtual infrastructure server. After a successful logon the server and its hosted virtual machines are displayed and available for selection.
Refresh Server	Reconnects to the selected server and updates the list of virtual machines hosted by the server.
Edit Server	Allows you to edit the information used to connect to the selected server.
Remove Server	Removes the selected server from the table. All virtual machines hosted by the server will be removed from the right-hand table.
Add Server(s) To Group	In the left-hand pane, select the desired server(s) and then click **Add Server(s) To Group**. The server is added to the bottom pane. When you add a server, it effectively adds all virtual machines hosted by that server to the machine group.
Add Machine(s) To Group	To add individual virtual machines to the machine group, select the desired virtual machines in the right-hand table and then click **Add Machine(s) To Group**. You can add an individual virtual machine even if the server being used to host the virtual machine is already contained in the machine group. Although the virtual machine in this case would technically be listed twice, it will only be scanned once. This applies for all duplicate entries.

30. Adding Offline Virtual Machines That Reside On Workstations

Some virtual machines may reside on individual workstations. Any machine using VMware Workstation software is capable of supporting a virtual machine. The virtual machines may reside almost anywhere, including hard drives, network drives, jump drives, etc. You use the **Workstation Virtual Machines** tab to add these stand-alone offline virtual machines to a machine group.

This tab is used to specify the offline identity of each virtual machine. If a virtual machine added here is online when a scan is performed, a mounting error will occur and the scan of that machine will fail.

TIP: If you want to be absolutely sure that all your virtual machines are successfully scanned, simply add the same machines to the group a second time using one of the other tabs (**Machine Name**, **Domain Name**, or **IP Address/Range**). This duplication assures that each virtual machine will be successfully scanned regardless of its power state (online or offline).



The virtual machines specified here are the actual images and you must therefore specify the full path name. Once the virtual machine is added to a machine group you should also **specify the credentials** used to connect to that virtual machine. This is different from virtual machines hosted by a server. On a server you can simply reference a file that points to the actual virtual machine, letting the server manage the path and credential information.

Adding a virtual machine residing on a workstation

There are two ways to add an offline virtual machine that is hosted on a workstation:

- In the **Enter the full path to a VM file** box, type the full path name of the virtual machine. You must specify the full path name and not just the name of the virtual machine. The name must contain a valid image extension (such as .vmx) and must not contain any illegal characters (such as @, ", etc.). When possible, avoid using network drive letters; the recommended practice is to instead specify the Uniform Naming Convention (UNC) path. For example: ||*machinename*|*sharename*|*directory*|*machine.vmx*.
- **- OR -**
  Click the Browse button (...) and locate the virtual machine by browsing your local machine and your network for the desired file.

Once the virtual machine is defined, click **Add VM** to add it to the machine group list.

Adding a directory of virtual machines

There are two ways to add a directory of offline virtual machines:

- In the **Enter the path to a directory of VMs** box, type the full path name of the directory. When possible, avoid using network drive letters. The recommended practice is to specify the Uniform Naming Convention (UNC) path. For example: *||virtual|directory|*.
- **- OR -**
  Click the Browse button (...) and locate the directory by browsing your local machine and your network for the desired directory.

If you want the program to recursively search all subdirectories for virtual machines when performing a scan, enable the **Include all VMs in all subdirectories** check box.

Once the directory is defined, click **Add directory** to add it to the machine group list.

> Adding a large number of virtual machines that are all hosted on the same workstation could cause a connection limit error to occur when scanning the virtual machines. See **Notes About Virtual Machines** for more information.

Import from file (offline VMs)

You can import a list of offline virtual machines from a previously created text file.

1. Click **Import from file (offline VMs)**.
2. Navigate to the location of the text file and then click **Open**.

The text file can be created manually or it can be created using any network-based tool available to you. When creating the text file, each virtual machine name must be separated by either a carriage return or a comma. For example:

`D:\VMware Images\VM-MAF-FR-XPP\winXPPro.vmx`, `D:\VMware Images\VM-QA-EN-2KS-4\win2000Serv.vmx`, `Z:\VMware Images\WinXP_EN_gold_2\winXPPro.vmx`

Import from file (offline VM directories)

You can import a list of virtual machine directories from a previously created text file.

1. Click **Import from file (offline VM directories)**.
2. Navigate to the location of the text file and then click **Open**.

The text file can be created manually or it can be created using any network-based tool available to you. When creating the text file, each directory name must be separated by either a comma or a carriage return. For example:

`D:\VMware Images\VM-MAF-FR-XPP`, `D:\VMware Images\VM-QA-EN-2KS-4`

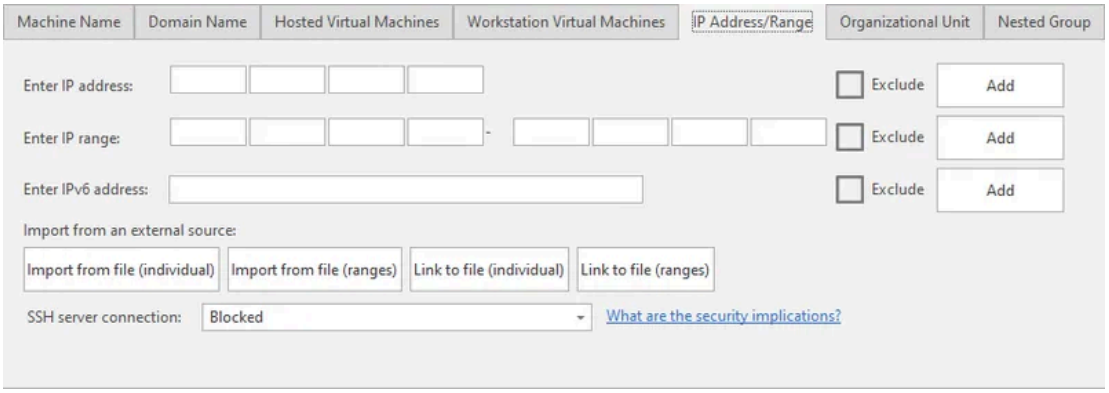
`Z:\VMware Images\WinXP_EN_gold_2`

Link to file (offline VMs) and Link to file (offline VM directories)

Offline virtual machines and virtual machine directories can be dynamically linked to a text file rather than imported. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group. When you link a file to a machine group, any changes that you make to the file are automatically reflected in the next scan. See **Linking Files to Machine Groups** for more information.

31. Adding Machines by IP Address to a Machine Group

Machines can be added to a machine group by entering individual IP addresses or by defining a range of IP addresses.



Adding an Individual IPv4 Address

1. Access the machine group.
2. Select the **IP Address/Range** tab.
3. Type the IP address in the **Enter IP address** box.
4. Choose whether you will allow SSH server connections to this machine.
   The SSH protocol may be used when the console initiates a connection with the specified machine. The primary use cases are when a power status scan or a push installation of an agent are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain that the specified machine is trusted and safe, you should choose to block SSH server connections. For more detailed information, see the SSH Authentication topic.
5. Click **Add**.

> If you want to specifically exclude an IP address, enable the **Exclude** check box before you click **Add individual**. The IP address will be added to the machine list but will not be included in any scans. See Excluding Certain Machines for more information.

Adding a Range of IPv4 Addresses

1. Access the machine group.
2. Select the **IP Address/Range** tab.
3. Type the starting and ending IP addresses in the **Enter IP range** boxes.
4. Choose whether you will allow SSH server connections to the machines in this IP range.
   The SSH protocol may be used when the console initiates a connection with the specified machines. The primary use cases are when a power status scan or a push installation of an agent are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain that the specified machines are trusted and safe, you should choose to block SSH server connections. For more detailed information, see the SSH Authentication topic.
5. Click **Add**.

Adding an IPv6 Address

1. Access the machine group.
2. Select the **IP Address/Range** tab.
3. Type the IPv6 address in the **Enter IPv6 address** box.
4. Choose whether you will allow SSH server connections to this machine.
   The SSH protocol may be used when the console initiates a connection with the specified machine. The primary use cases are when a power status scan or a push installation of an agent are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain that the specified machine is trusted and safe, you should choose to block SSH server connections. For more detailed information, see the SSH Authentication topic.
5. Click **Add**.

Importing IP Addresses from an External Source

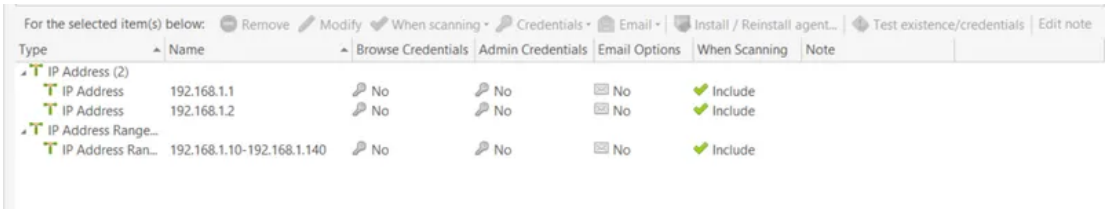
You can also add IP addresses by using the following buttons to import the addresses from an external source.

Button	Description
Import from file (individual) and **Import from file (ranges)**	You can import a list of individual IP addresses or a list of IP address ranges from a previously created text file. The text file can be created manually or it can be created using any network-based tool available to you. Each IP address in the text file must be separated by either a carriage return or a comma. When defining an IP range, include a dash between the beginning and ending IP address:
Link to file (individual) and **Link to file (ranges)**	IP addresses can also be dynamically linked to a text file rather than imported. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group. When you link a file to a machine group, any changes that you make to the file are automatically reflected in the next scan. See Linking Files to Machine Groups for more information.

Bash

```
172.16.1.1-172.16.1.255
```

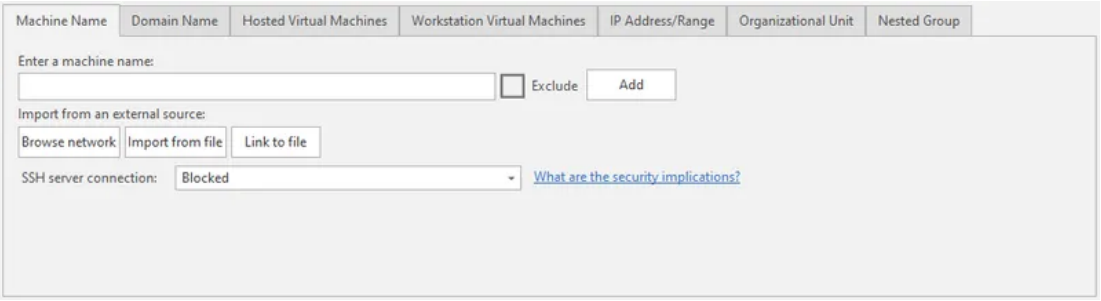
When IP addresses are added, the new entries are displayed within the bottom section of the machine group pane.



The recommended best practice is to always supply credentials for the machines in the machine group. See **Supplying Credentials** for more details.

32. Adding Machines by Name to a Machine Group

One of the ways that a machine can be added to a machine group is by machine name. Like most other tasks in Security Controls, there are many ways that you can add a machine name to a machine group.



Adding an Individual Machine Name

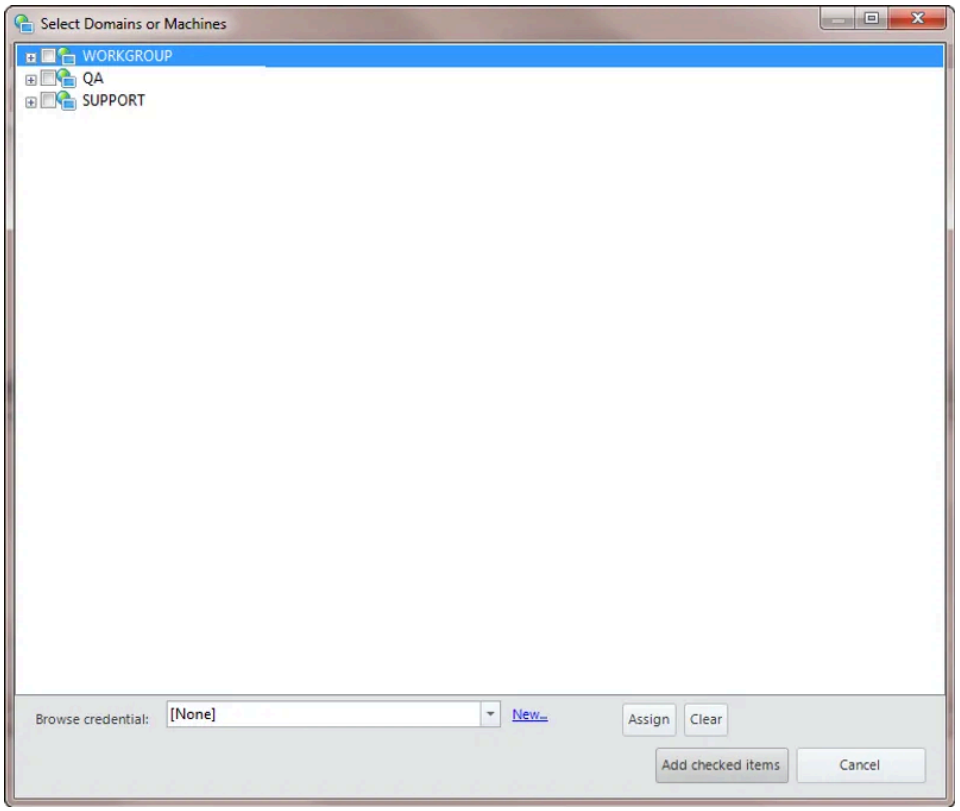
The easiest way to add a machine to a machine group is as follows:

1. Access the machine group.
2. Select the **Machine Name** tab.
3. Type the name of the machine in the **Enter a machine name** box.
   You can specify either the individual machine name or the fully qualified domain name.
4. Choose whether you will allow SSH server connections to this machine.
   The SSH protocol may be used when the console initiates a connection with the specified machine. The primary use cases are when a **power status scan** or a **push installation of an agent** are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain that the specified machine is trusted and safe, you should choose to block SSH server connections. For more detailed information, see the **SSH Authentication** topic.
5. Click **Add**.

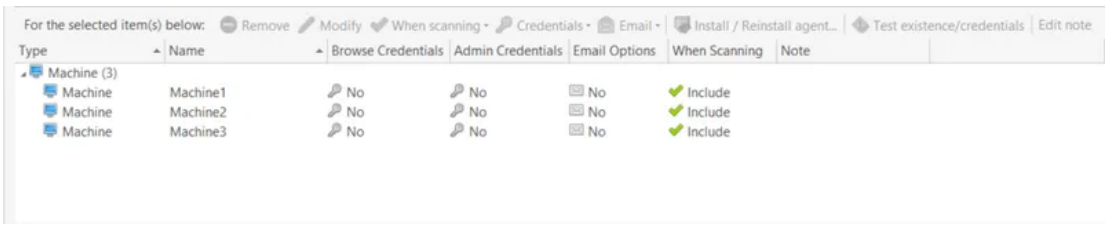
> If you want to specifically exclude a machine, enable the **Exclude** check box before you click **Add**. The machine will be added to the machine list but will not be included in any scans. See **Excluding Certain Machines** for more information.

Importing Machine Names From an External Source

You can also add machines by using the following buttons to import machine names from an external source.

Button	Description
Browse network	This button opens a separate dialog that lists the contents of your Microsoft network. Locate the machines you would like to add to the custom group, place a check mark in the check boxes, and then click **Select**. If you need to supply credentials in order to enumerate one or more nodes, in the **Browse credential** box at the bottom of the dialog select the appropriate credential and then click **Assign**. If you need to define a new credential, see Defining Credentials. 
Import from file	You can import a list of machines from a previously created text file. The text file can be created manually or it can be created using any network-based tool available to you. Each machine name in the text file must be separated by either a carriage return or a comma.
Link to file	Machine names can also be dynamically linked to a text file rather than imported. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group. When you link a file to a machine group, any changes that you make to the file are automatically reflected in the next scan. See Linking Files to Machine Groups for more information.

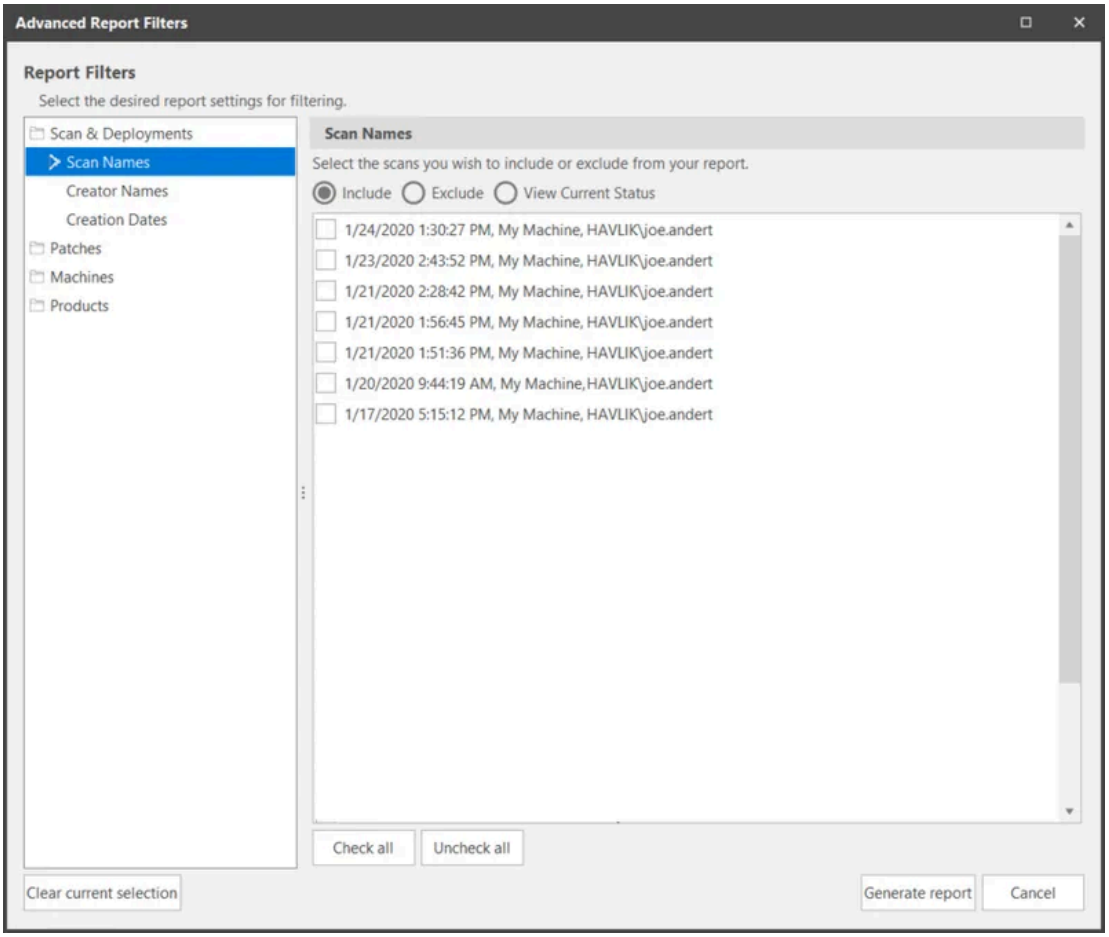
When machines are added or imported by name, the new entries are displayed within the bottom section of the machine group pane.



TIP: The recommended best practice is to always supply credentials for the machines in the machine group. See **Supplying Credentials** for more details.

33. Advanced Filtering

The **Advanced Report Filters** dialog enables you to effectively drill deeper into your scan and deployment results and extract more meaningful information. It does so by enabling you to select exactly which information you want to include in the report.



To use the Advanced Report Filters dialog:

1. Select each of the available options one at a time from the list on the left and on the right-hand side specify the items you want to include or exclude.
2. When you are ready to generate the report, click **Generate report**.

34. Agent-Based Patch Management

Rolling out agents takes a little more preparation work to configure the environment to get the first scans coming in from machines. An agent is a great way to automate the management of some hard to reach machines, so it can be worth the effort to rollout agents to machines.

To configure and install an agent, you must create agent policies to manage different groups of machines. The policies may be based on geographic location, role, or a combination. Each policy can be configured to execute multiple tasks on an hourly, daily, weekly, or monthly basis. Once agent policies are set up the agent can be installed on a machine. Once the agent is installed it will start to manage the machine as it was configured to do.

So, if agents require a longer rollout time, why would they be ideal in some cases? There are three general cases where agents are the preferred solution.

Laptop Users

Laptops come and go in environments today. With the agent loaded on a machine it will not matter if the laptop is not online during a maintenance window. The agent policy can be configured to fill in the gaps and supplement agentless coverage, providing a solid support model for these hard to reach road warriors.

Secure Environments

Demilitarized zones (DMZs) are a good example of an environment that may not allow file and print sharing regardless of the firewall rules and security measures that are in place. With the agent the target can be locked down and only require an outbound port to the console to update its policy. This port is 3121 (inbound port on the console). Internet connectivity may be required if you specify Vender over Internet as a source for data and patches. If internal distribution servers are to be utilized the servers will require ports 137 - 139, 445, or (if using http) whatever port IIS is configured on for the virtual directory.

Be sure to check the **System Requirements** for the latest port information.

Low Bandwidth Connections

The agent offsets the scans to the local machine. One of the advantages of agentless is that the bulk of the processing is done on the console. This involves network traffic and high CPU usage on the console, but the target is virtually unaware of any of this. If the agent runs the scan locally we reduce the WAN traffic from 2 - 4MB on average to 20 - 100KB on average to accurately scan and report the results to the database. An agent that also utilizes distribution servers for deployment purposes would do all of its major traffic on the local LAN and only a fraction of the WAN traffic would be required, reducing the impact on lower bandwidth connections.

Time to Implement

It typically will take 10 – 20 minutes to configure an agent policy. The rollout of the agents to the target machines may take several hours or several days depending on the number of machines and on the rollout option you choose. **Rollout options** are described in the next section.

Related Topics

- **Console Software and Hardware Recommendations**
- **Port Requirements and Firewall Configuration**
- **Distributed Environment Management**

- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

35. About the Agent Client Program

The agent client is a multi-function program that safeguards an end-user's computer. It will track the status of the machine and perform actions that are configured by the program administrator. It can:

- Perform scans to detect all missing patches and product levels
- Deploy any missing patches and product levels in order to close security holes in your software
- Perform scans to detect and categorize the software and hardware assets contained on your machine

As the program administrator, you configure which of these actions the agent program should perform. They will occur automatically, requiring no intervention or assistance.

Accessing the Agent Client Program

You or your end users can access the Security Controls Agent two ways:

- By selecting **Start > Ivanti Security Controls Agent** on the target machine.
- By double-clicking the following executable file:

```bash
C:\Program Files\LANDESK\Shavlik Protect Agent\STUILauncher.exe
```

How to Navigate the Agent Client Program

Navigating the program is easy. You begin on the home page, which is your starting point for all actions. The home page contains a number of different tiles. You can click any of the tiles to view the associated data and perform related tasks.



A limited version of the agent client program is displayed if you happen to launch the program while it is undergoing a software update. If this occurs, simply wait a minute or two and then relaunch the program.

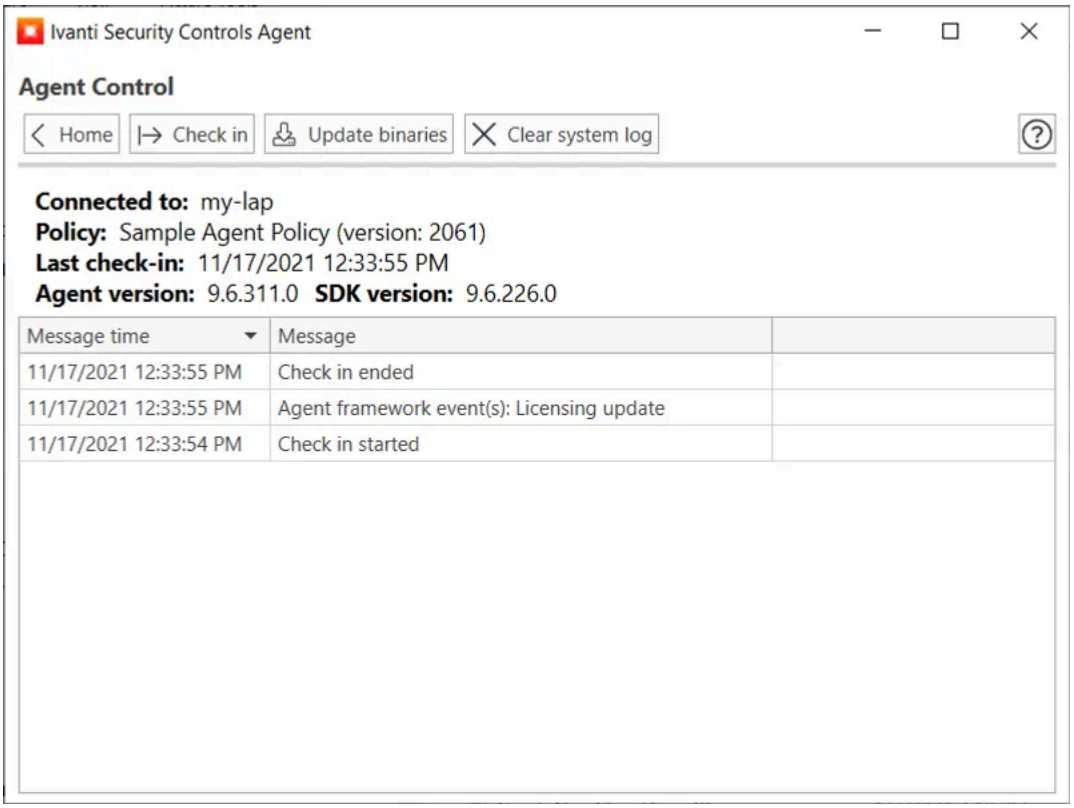
Agent Control Tile

The Agent Control tile is always the first tile contained on the home page. The tile displays general information about the agent, including:

- **Connected to:** The name of the console machine to which the agent is connected.
- **Policy:** The name of the policy that is assigned to this agent.
- **Last check-in:** The date and time that this agent last checked in with the console.
- **Agent version:** The version of the agent software.
- **SDK version**: The version of the agent framework and engine build components.

How to View the Agent Log and Perform Actions

You can click the Agent Control tile to view the agent log and perform a number of actions.



The messages presented in the agent log are system level messages that are provided for informational purposes only. There are no actions you need to take on these messages.

The following buttons are available:

- **Home:** Returns you to the home page.
- **Check in:** Directs the agent to check in with Security Controls and download any policy changes. An end user will typically not need to use this button unless directed by you, the administrator.
- **Update binaries:** Directs the agent to download the latest scan engines and data files. An end user will typically not need to use this button unless directed by you, the administrator.
- **Clear system log:** Clears all information from the log file.

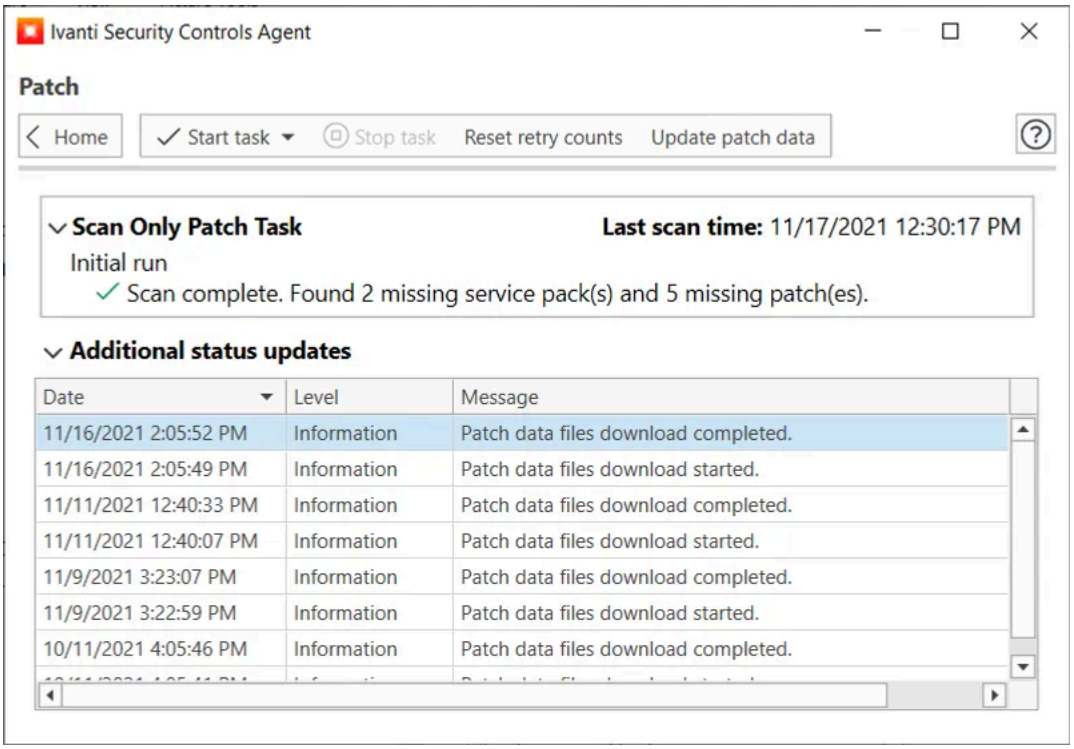
Patch Engine Tile

> The Patch Engine tile will not be displayed if there are no **patch tasks** defined in the agent policy.

The Patch Engine tile displays the number of missing product levels and patches that were detected during the most recent patch scan.

How to View the Available Patch Tasks and Perform Actions

You can click the Patch Engine tile to view the patch tasks that are configured for use.



A log file is provided for each available patch task. Each log contains status messages pertaining to the most recent actions that have been performed by that task. Detailed information is provided about patch downloads, installations, successes and failures. Depending on how you have configured your **agent policy**, there may be several tasks from which to choose.

The following buttons are available:

- **Home:** Returns you to the home page.
- **Start task:** When you click a task name, it starts that task on the computer. The task is performed using the unique options that were configured for the patch task.
- A patch task will scan for software patches and product levels that are missing from the machine. The scan will run in the background, allowing you to continue working while the scan is being performed. Scan results are reported to the Security Controls console. A record of the scan is displayed in the task log.
  Depending on how you configured the patch task, if the scan detects one or more missing patches it may automatically deploy the patches. Patch deployments, if they occur, are reported to the Security Controls console. A record of the deployment is displayed in the task log.
  Refer to your corporate security policy for recommendations on if you or your end users should manually perform a patch task. For example, some organizations may require a patch task every 30 days, or it may be required for machines that have

been powered off or disconnected from the network for an extended time. Other organizations may implement regularly scheduled patch tasks and may not allow manual patch tasks.

Stop task: Stops the patch task currently in progress. A message is recorded in the log whenever you stop a task. If there is no active task, this button will be disabled.

- **Reset retry counts:** Resets all patch counters. A unique patch counter exists for every patch the program tries to download and for every patch the program tries to install. A patch counter will increment whenever a patch download or a patch installation fails. Failed download and installation attempts will be recorded in the patch log. If a patch fails to download after 11 attempts or fails to install after 4 attempts, the client program will stop trying to deploy that particular patch. The only way to resume the deployment of that patch is to click **Reset retry counts**.
- **Update patch data:** Directs the agent to check in with the console and download the latest patch data. An end user will typically not need to use this button unless directed by you, the administrator.

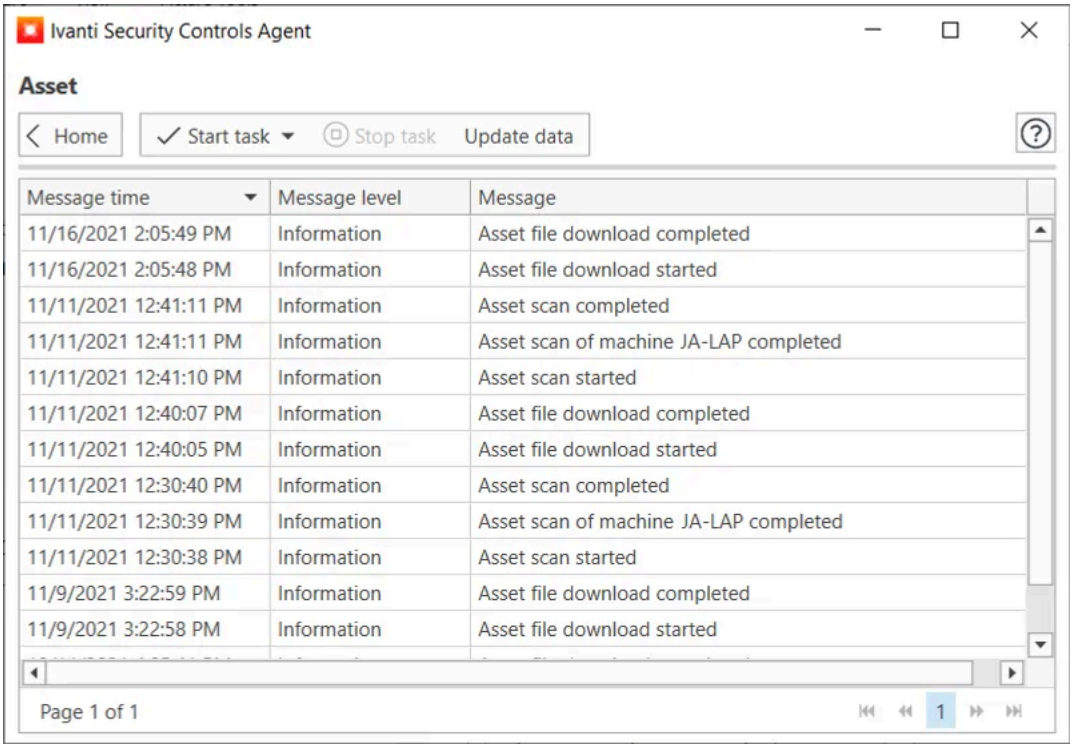
Asset Engine Tile

> The Asset Engine tile will not be displayed if there are no **asset tasks** defined in the agent policy.

The Asset Engine tile enables you to manually start and stop asset tasks. An asset task will identify the software and/or hardware contained on the machine. The task will run in the background, allowing you to continue working while the task is being performed. The task results are reported to the system console. Asset task results are not available within the agent program.

How to View the Asset Log and Perform Actions

You can click the Asset tile to view the asset log and perform actions.



The following buttons are available:

- **Home:** Returns you to the home page.
- **Start task:** When you click a task name, it starts that task on the computer. The task is performed using the unique options that were configured for the asset task. Depending on how you have **configured your agent policy**, there may be several tasks listed here.
- **Stop task:** Stops the asset task currently in progress. A message is recorded in the asset log whenever you stop a task. If there is no active task, this button will be disabled.
- **Update data:** Directs the agent to check in with the system console and download the latest asset data. An end user will typically not need to use this button unless directed by you, the administrator.

Asset Log

The asset log contains status messages pertaining to the actions that have been performed by any of the available asset tasks. For example, the log will record:

- Each time an asset task is manually started or stopped

- Each time a scheduled asset task is automatically started or stopped
- ... and many other asset-related events

There may be a large number of messages displayed in the log. For the most part, the messages are low level messages meant to show that the program is doing its job and working to protect the computer. No actions are typically required on your part.

Agent Commands

You can control an agent using the stagentctl command-line utility. You can learn about the utility by displaying the built-in help information.

1. Open an admin command prompt on the agent machine.
2. Change to the `C:\Program Files\LANDESK\Shavlik Protect Agent` directory.
3. Display help information for the stagentctl utility.

Bash

```
stagentctl
```

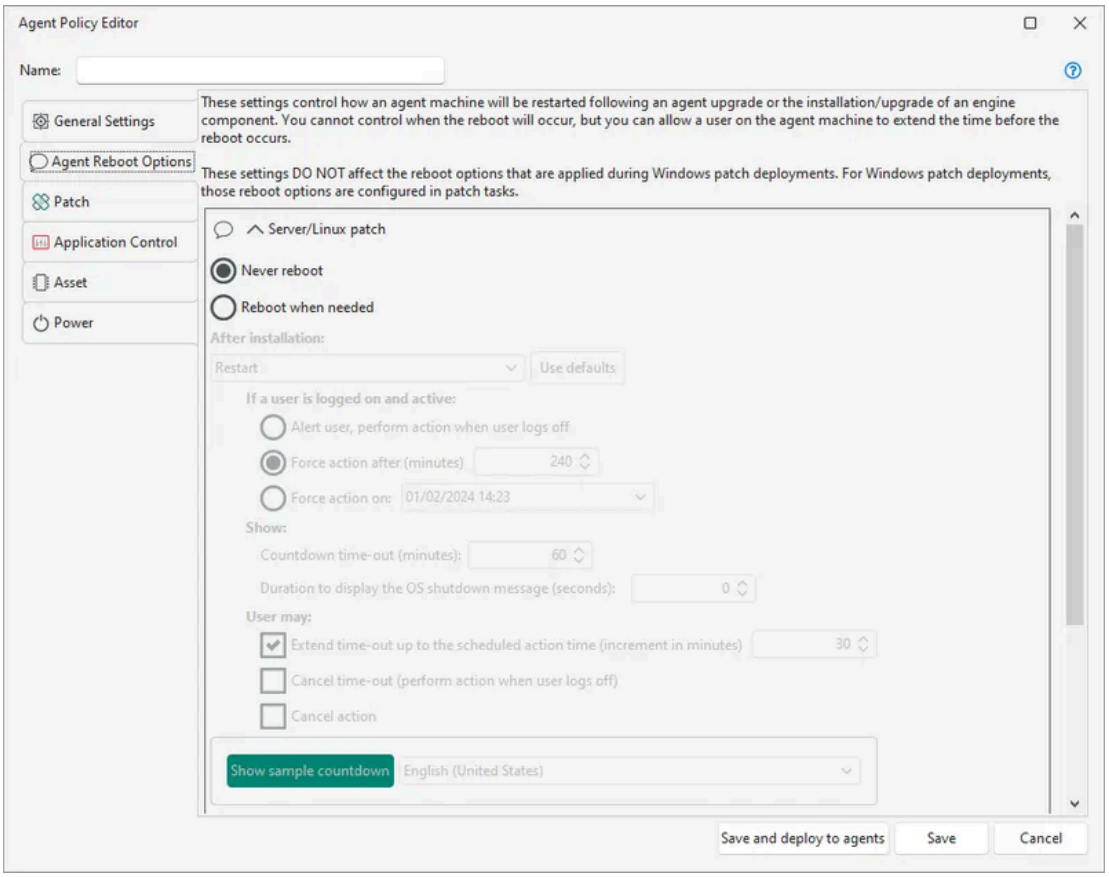
36. Agent Reboot Options

> This tab does not affect the reboot options that are applied during Windows patch deployments. For Windows machines, those reboot options are configured on the patch deployment template that is specified within your **patch task**.
> For Linux machines, you specify if and when you want patch reboots in the patch deployment template (see **Creating and Editing a Linux Patch Deployment Configuration**) that is specified within your **patch task**, but specify countdowns and so on in the **Server/Linux patch** section of this tab.

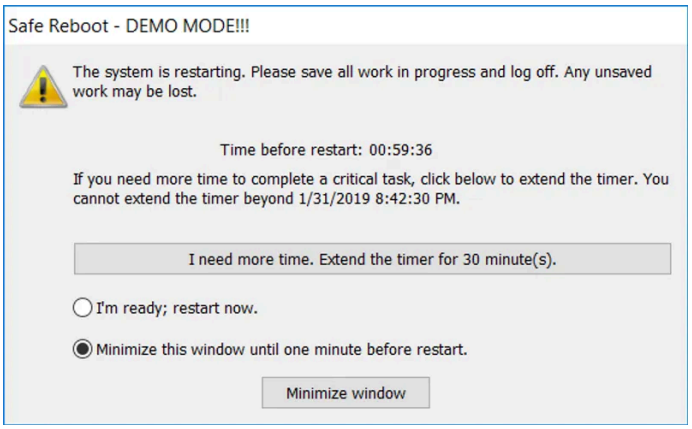
This tab enables you to specify how an agent machine will be restarted after one of the following occurs:

- An agent is upgraded
- An engine component is installed or upgraded

You can specify different reboot options depending on whether the agent is installed on a server or workstation machine.



Field	Description
Never reboot	This SafeReboot capability specifies that it is unnecessary to reboot each machine. The remaining options on this tab will be disabled. As a rule, you should only enable this option if you are concerned about the availability of certain machines, such as servers.
Reboot when needed	This SafeReboot capability specifies that Security Controls will determine whether or not a reboot of each machine is required.
After installation	You can specify what state you want to leave the machines after the reboot. • **Restart:** The machines are restarted and left in a powered on state. • **Restart, then sleep if possible:** The machines are restarted and then put into a sleep state. There is a two minute delay between the completion of the restart and the time the machines are put into the sleep state. The Microsoft Scheduler is used on each target machine to initiate the sleep state following the restart. For more detailed information about sleep state, see **Sleep and Hibernation Notes**. • **Restart, then hibernate if possible:** The machines are restarted and then put into a hibernation state. There is a two minute delay between the completion of the restart and the time the machines are put into the hibernate state. The Microsoft Scheduler is used on each Windows target machine to initiate the hibernation state following the restart. • If a target machine is not **configured to allow hibernation**, the program will instead attempt to put the machine into a sleep state after the restart. If the machine cannot be put into a sleep state no action will occur. For more detailed information about hibernate state, see **Sleep and Hibernation Notes**. • **Restart, then shut down:** The machines are restarted and then powered off. There is a two minute delay between the completion of the restart and the time the machines are shut down. This option is useful if you want to perform a reboot in order to complete a maintenance task but then want the machines to be shut down. The Microsoft Scheduler is used on each Windows target machine to initiate the shutdown following the restart. • **Shut down only, do not restart:** The machines are powered off. This option is also useful if you simply want to make sure non-critical machines are turned off each night or over a weekend, saving energy. For more information about the power management capabilities of Security Controls, see **Power Management Overview**.
Use defaults	This button is tied to the **Restart and power action** box. When you click **Use defaults**, all remaining options on the dialog will be changed to the values recommended for use with the currently selected **Restart and power action**.
If a user is logged on	If you elect to restart the machines, you can specify the amount of warning that a logged-on user with an active session will receive. You can also choose the degree of control the user will have over the restart process. The options do not apply to inactive sessions such as locked machines or disconnected RDP sessions. • Alert the user that a restart will occur when they log off. • Elect to force a restart after a number of minutes have passed. • Elect to force a restart at a specific date and time.

Field	Description
	• Show a countdown dialog on the user's Windows machine in advance of the restart. To preview the dialog box that the user will see, click **Show sample countdown**. The language box to the right can be used to preview this dialog in different languages.  Select the duration to display the standard Windows shutdown message when the shutdown sequence is initiated. • Allow the user to extend the time-out countdown up to a specified maximum. The maximum can be specified as either a duration or as a specific latest time that the restart will occur. • Allow the user to cancel the time-out. If a time-out is cancelled the patches will not be deployed until the user logs off or manually restarts the machine. • Allow the user to cancel the restart. The patches will not be installed until the machine is restarted. User's on Linux machines will not see a countdown dialog as shown above but they will see a notification. They will use the **stagentctl command-line utility** to extend the time-out.

37. Agent Rollout Options

Deploying the agent to an environment is no small task no matter what the product. Installing a piece of software on a machine that has to meet local prerequisites as well as communicate with a remote machine to pull down policy data involves a great many variables that can complicate matters. And then there is the delivery mechanism. Some environments may require multiple ways of installing an agent to do a successful rollout. Ivanti has simplified the agent installation process down to a single universal STPlatformUpdater.exe file. It is the same installer for all Windows customers. This gives you a payload that can be delivered using a number of different methods.

Push Installation from the Console

Using Ivanti's agentless technology, you can push an agent install out by simply selecting a machine from the machine group or from Machine View and installing an agent with the policy desired. This is the quickest and easiest way to rollout the agent, but is bound by the same requirements as agentless scans.

Manual Installation

In cases where there are a small number of machines that are not reachable agentlessly, you can consider performing a manual agent installation. The manual process requires you to enter a few variables (console hostname, port, passphrase or credentials, and policy) during the installation of the agent. This can be done quickly and easily for small numbers of machines, but becomes less viable the larger the target base becomes.

The **STPlatformUpdater.exe** file used for manual installation can be found here:

C:\ProgramData\Ivanti\Security Controls\Console\DataFiles

Installing Agents from the Cloud

If you are using Security Controls Cloud synchronization, you have the ability to install a Security Controls Agent from the cloud. This is particularly helpful if you have target machines that are away from the corporate network and unable to contact the console. For more information, see **Installing and Supporting Agents on Internet-based Machines**.

The requirements for installing an agent with this method are:

- You must have a Security Controls Cloud account
- The target machine must have Internet access
- The Security Controls console must be registered with Security Controls Cloud (**Tools > Options >** Security Controls **Cloud sync**)
- There must be at least one policy that is configured to allow synchronization with Security Controls Cloud (see the **Sync with** Security Controls **Cloud** check box on the **agent policy General Settings tab**)
- You cannot install a cloud-based agent on a Ivanti Security Controls console machine
- Each user that installs an agent must have administrator access on their target machine

Scripted Installation

The **STPlatformUpdater.exe** allows command-line execution so install can be scripted and delivered in a number of different ways. The command-line options are all detailed in the **Creating and Using a Manual Installation Script** topic. Delivery of the **STPlatformUpdater.exe** and execution using a command-line can be performed in a number of different ways quickly and easily. The

problem here typically is how many agent policies need to be rolled out. Each policy means a different script and then sorting out which machines get what can be more difficult.

Custom Patch

The ability to push the agent from the Ivanti Security Controls console is nice to have, but if you are pushing the agent to 1000 machines in a machine group that is setup by an IP range, and if you hit 90% of the targets the first time through, what do you do with the remaining 10%? Using Ivanti Security Controls custom patch feature we can scan the same group and detect if the agent is installed and only install on machines it is not installed on. This can be helpful in many ways. Every few weeks or months an additional scan can be run to pick up machines that may have slipped through the build process and not received an agent.

Other

Using the options above, you can get creative with scripting options and deliver the agent in a number of different ways. The `STPlatformUpdater.exe` file can be wrapped in a self-extracting zip to extract and execute a command-line installation that is delivered via email (the .exe file is roughly 17MB). This can be used to reach some users who are rarely in the office. The same could be delivered through a hosted weblink. The user would simply click on the download and run the file to execute. In this case the user doing the executing would need local administrator rights, but in many cases where the user is at a standalone site or is a heavy remote user this is often the case. For customers who image using ghost or sysprep or some other means, you cannot install the agent and make it part of your image due to the nature of how the agent registers itself with the console for security purposes. You can embed the scripted install into the image so that the first time it reboots it can run the agent installation and be up and running as part of the build process.

Related Topics

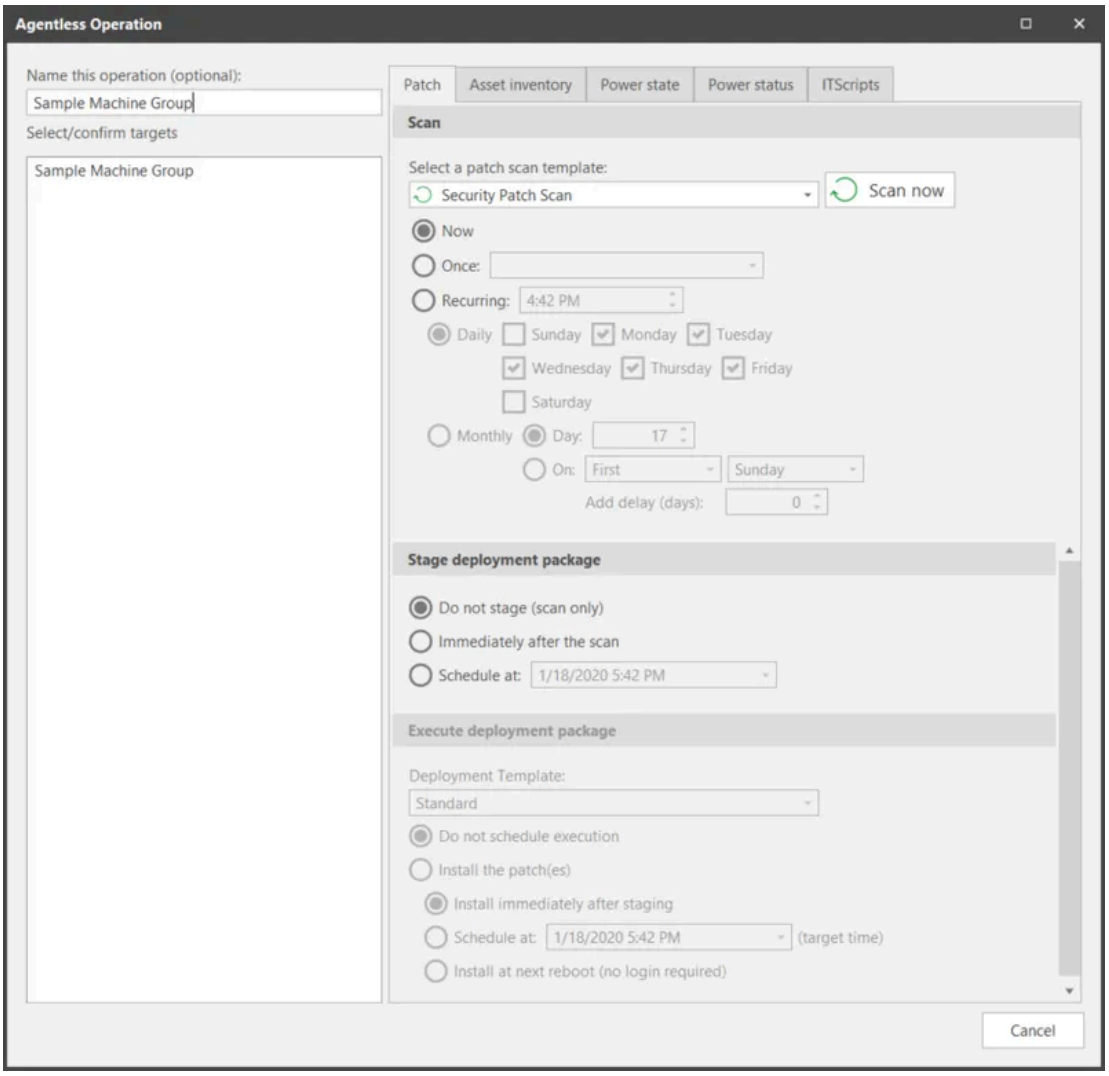
- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

38. Performing a New Agentless Operation

Many of your everyday tasks are performed from the **Agentless Operation** page. This page enables you to quickly configure and initiate patch, asset, power and ITScripts operations.

There are three ways to initiate an agentless operation:

- Select **New > Agentless operation**
- Press Ctrl+N
- Click the **New agentless operation** link on the home page



1 - (Optional) Type a name for the operation you are about to perform. This name will be displayed on a tab within the Operations Monitor to help you track the task as it is being processed. The name is also used in other areas of the program to identify the results of this particular operation. A maximum of 100 characters can be used for the name.

Example: Domain patch scan 01/01/2019

2 - Select the machine group(s) you want to perform the operation on. You must select at least one machine group.

3 - In the right-hand pane, choose the tab that corresponds to the type of agentless operation that you want to perform. Configure the operation on the tab and then initiate the operation.

For more information, see the following:

- **Patch** tab
- **Asset inventory** tab
- **Power state** tab
- **Power status** tab
- **ITScripts** tab

39. Agentless vs. Agent-based Solutions

Security Controls provides both agentless and agent-based solutions. This section describes, in general terms, the benefits of each solution. The sections that follow explain in more detail how to use an agent.

Agentless Solution

> Applies only to Windows-based machines.

Agentless systems are based on push technology and on a centralized design. A central authority is responsible for scanning the machines in the enterprise and for initiating all actions on those machines. Agentless systems have a number of advantages over agent-based systems. Strict agent-based systems can only report on machines that have the agent actively running. If the agent has been disabled the machine will appear to not exist. In addition, new machines can be introduced to a network and these rogue machines will not only be agentless, they may well be invisible. Agentless systems, on the other hand, can scan ranges of IP addresses and report on machines it finds. Even if it cannot access the system, the agentless scanner will at least report that a new IP address is present on the network. In many cases agentless systems lower the cost of ownership, reduce management overhead, and provide for quick and easy deployment. This is especially true in large enterprises managing 10,000 or more machines. An administrator can be scanning and fixing their network within minutes using an agentless system.

In Security Controls, all Windows-based patch, asset, and power management tasks can be performed without agents.

Agent-based Solution

Patch Management and Asset Management

Certain types of users or systems can pose problems for agentless solutions. Machines that must reside in a "de-militarized zone" (DMZ), roaming users, and disconnected or inactive machines can all prove problematic. In these cases an agent-based solution is often the best answer. Agent-based solutions consist of proprietary client-side communications software that resides on a computer and facilitates communications with server-based administrative software. The agent scans the client machine for information and then provides the information directly to the server console.

An agent-based solution is a useful complement to an agentless patch management and/or asset management solution. Outfitting your troublesome systems with agents provides the best of both worlds--agentless solutions to protect machines permanently or newly introduced to the network, and agent-based solutions for the hard-to-reach machines.

Finally, **all Linux-based patch management operations are performed using agents**. This is due to the differing natures between Windows and Linux operating systems. The agent infrastructure lends itself quite well to managing these differences and providing cross platform functionality.

Power Management

An agent-based solution is also well suited for performing power management tasks. For example, if you want to be sure your portable machines are not left powered on late at night or over the weekend, an agent can be used to automatically shut down those machines. In addition to saving power and avoiding unnecessary wear, shutting down your disconnected machines during those times they are likely to be left unattended is also a smart security precaution.

Summary

Agentless

- Designed for centralized, Windows-based environments
- Based on push technology
- Ideal for networks with large amounts of bandwidth
- Dependent on network connectivity
- A central authority does all the scanning and deploying
- Best for performing patch management and asset management tasks on networked machines

Agent-based

- Best for frequently disconnected machines or machines in the DMZ
- Based on pull technology
- Ideal for distributed networks with remote locations that have limited bandwidth
- Less dependent on network connectivity; ideal for mobile computers that are not always connected to the network
- Each agent does its own scanning and deploying based on policies defined on the central console
- Best for performing Windows-based patch management and asset management tasks on disconnected machines
- Used for performing Linux-based patch management tasks

Related Topics

When Should I Use Each Solution?

How the Agent Process Works

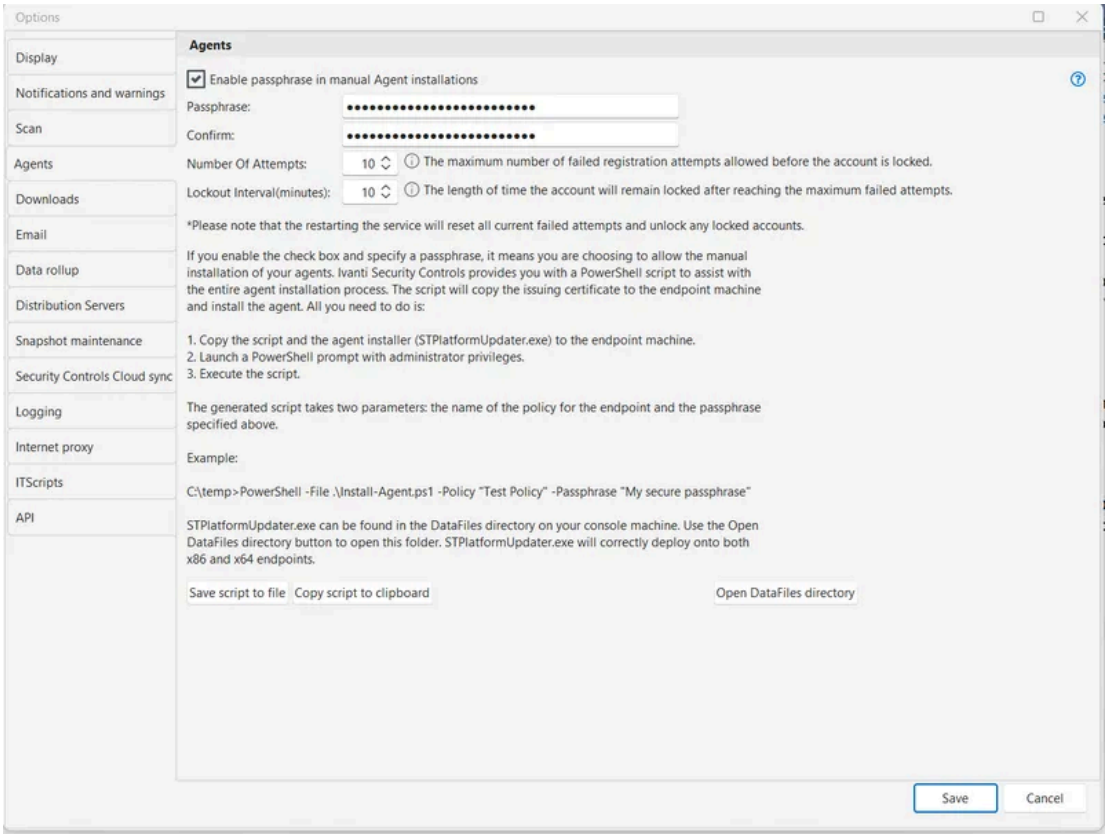
Preparing to Use Agents

Installing Agents from the Console

Manually Installing Agents

40. Agents Options

The **Agents Options** dialog allows you to specify whether manual agent installations will be permitted and the passphrase that must be used during the agent registration process.



Field	Description
Enable passphrase in manual Agent installations	• If enabled, indicates that manual installation of an agent is permitted and that a passphrase will be used to authenticate the agent to the console. Users will be required to specify a matching passphrase during the agent registration process. • If not enabled, indicates that manual installation of an agent is not permitted.
Passphrase	If the **Enable passphrase in manual Agent installations** check box is enabled, type the passphrase you want users to use during the manual agent installation process. The passphrase is case-sensitive.The password must contain at least 12 characters. If you wish, you can change the passphrase periodically for security reasons. Doing so will not affect existing agents that are already installed.
Confirm	Retype the same passphrase in this box to confirm the passphrase.
Number of Attempts	To set the maximum number of failed registration attempts allowed before the account is locked. The default number of wrong password attempts is set to 10.
Lockout Interval(minutes)	To set the time period in minutes the account remains locked after reaching the maximum number of failed attempts.
Save script to file	To copy the custom script to a file, click this button. The file will be saved as a .ps1 file. You can then move the file to the remote machine and run it from within a Windows PowerShell ISE console.
Copy script to clipboard	To copy the custom script to the clipboard on the console machine, click this button. You might choose this option if you want to email the script to one or more users.
Open DataFiles directory	To open the File Explorer folder that contains the STPlatformUpdater.exe file, click this button.

Using the Custom PowerShell Script

If you permit manual installation of your agents, you must provide a secure connection between each remote agent machine and the console by importing the issuing certificate to each remote machine. You can **do this yourself** or you can use the provided PowerShell setup script to automatically perform these steps for you.

The PowerShell script will automatically:

- Copy the ST Root Authority certificate to the current user's Trusted Root Authority certificate store on the remote machine

> The default Security Controls self-signed certificate is contained within the script and that is what gets copied to the remote machine. If you **replace this certificate** you will need to update the script.

Install the agent using the policy and passphrase parameters that you provide

Steps you must perform:

1. Using the **Save script to file** or **Copy script to clipboard** buttons, save the PowerShell script to a local or network folder.
2. Using the **Open DataFiles directory** button, save the agent installer program (**STPlatformUpdater.exe**) to the same local or network folder.

3. Transfer the PowerShell script and the agent installer program to your remote machine.
4. Initiate the PowerShell script on the remote machine using a command similar to the following:

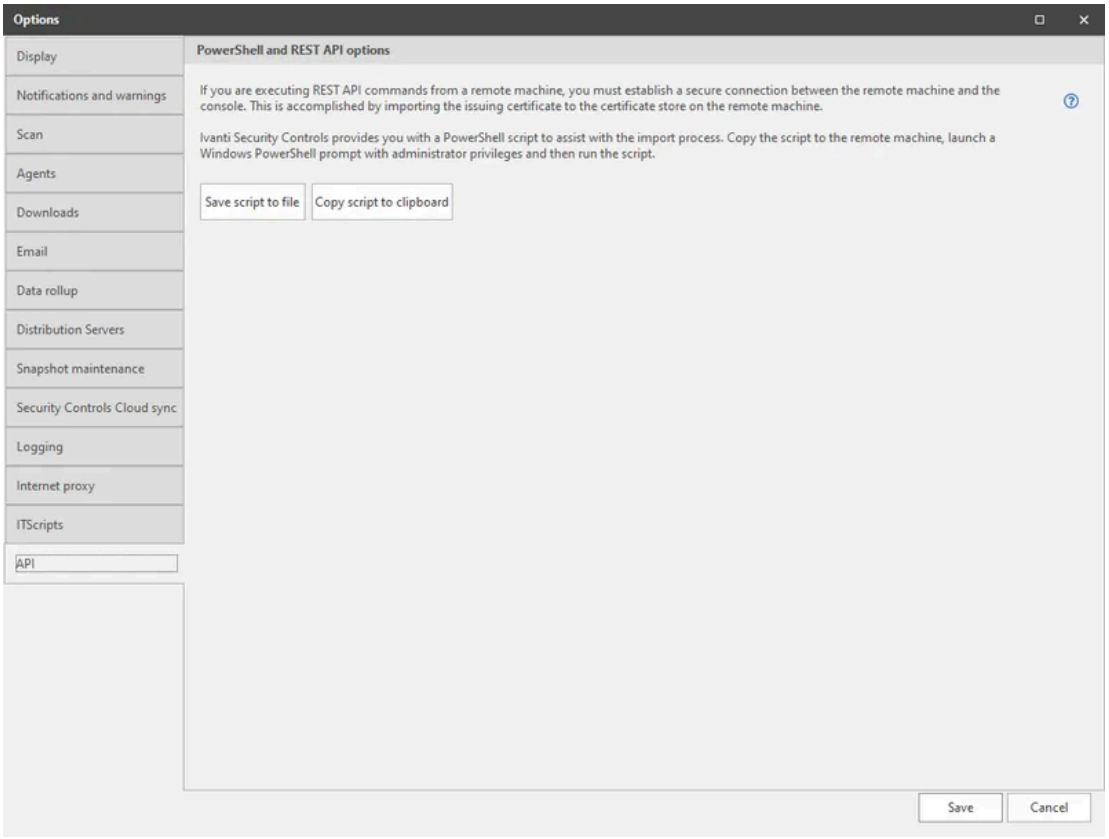
Bash

```
c:\temp>PowerShell -File .\InstallAgent.ps1 -Policy "Test Policy" -Passphrase "My secure passphrase"
```

41. API Options

If you are executing REST API commands from a remote machine, you must properly prepare your environment. You must enable remote system calls using the WinRM service and you must provide a secure connection by importing the issuing certificate to the remote machine.

The **API** tab provides access to a PowerShell script that will automatically export the ST Issuing certificate from the Trusted Root Authority store on the console machine to the current user's Trusted Root Authority certificate store on the remote machine. If there are multiple users on a machine, the script must be run by each user who will execute REST API commands.



Field	Description
Save script to file	To copy the custom script to a file, click this button. The file will be saved as a .ps1 file. You can then move the file to the remote machine and run it from within a Windows PowerShell ISE console.
Copy script to clipboard	To copy the custom script to the clipboard on the console machine, click this button. You might choose this option if you want to email the script to one or more users.

For more information on configuring and using the REST API, see the Security Controls **REST API help system**.

42. Architecture view

The Reporting2.Architecture view describes the architecture types.

Column Name	Data Type	Nullable	Description
Id	smallint		The architecture id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(256)		Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.Architecture view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[Architecture]
```

ID	Value	Description
0	Unknown	Invalid or Unknown type
1	Any	Any architecture.
2	x86	This is an x86 32-bit architecture.
3	x64	This is a 64-bit architecture.
4	PowerPC	This is a PowerPC architecture.
5	Sparc	This is a Sparc architecture.
6	IA64	This is an Intel Itanium architecture.

43. Areas That Can be Accessed by the API

API commandlets are available for use with the following functional areas in Security Controls:

- Patch scanning
- Patch deployment
- Credentials
- Machine groups
- Patch groups
- Power state management

You can leverage existing configuration and workflow concepts in any of these areas within Security Controls. This means you can reference existing credentials, machine groups, templates, logging, etc. within your API commands. You can also use the API to add new credentials, templates and groups.

The commands that you issue from the API will interact the Security Controls user interface. The results of actions that you drive from the API will be visible in Security Controls. For example, if you initiate a patch deployment from the API, the deployment process can be monitored using Deployment Tracker.

44. Asset Inventory Overview

> If you want to perform a virtual asset scan for the properties of your vCenter Servers, ESXi hypervisors and virtual machines, see the **Virtual Inventory feature**.

The asset inventory function enables you to track your software and hardware assets. Performing an asset scan enables you to thoroughly and dynamically discover and catalog your IT assets. You will uncover software applications you didn't know were installed and discover physical machines you didn't even know you had. By eliminating these blind spots, you can quickly close the gaps in your security and policy compliance. By consolidating hardware and software asset information in one location, you have all relevant information about your assets at your fingertips, enabling you to make informed decisions with confidence and accuracy.

The function works by performing scans to detect and categorize the software and hardware contained on your machines. Detailed information about your software and hardware assets is available immediately following a scan.

You also have the ability to create reports that can be used to track your asset inventory over time. For example, you might create a scheduled scan of your domain that automatically generates and sends usage reports to your IT personnel. So in addition to providing you with visibility and understanding of the IT assets in your network, the asset inventory function is also a great record keeping tool for use in audits.

> Asset scans can be performed in either an agentless or an agent-based fashion. This section describes the agentless process. For information on performing agent-based asset scans, see **Creating and Configuring an Asset Task**.

How-To Information

For information on how to perform asset inventory tasks, see:

- **Creating a New Asset Scan Template**
- **How to Initiate an Asset Scan**
- **Monitoring an Asset Scan**
- **Viewing Asset Scan Results**

Software Asset Scan Information

Scans for the software components contained on one or more machines. You can perform this scan on physical machines, online virtual machines, offline virtual machines, and virtual machine templates.

This scan helps you answer the following important questions:

- What software is on the machines in my network?
- Where are the software resources located?
- How many do I own?
- How many different versions of a software program are in use?
- How long ago were the programs installed?
- Are there software programs that shouldn't be on my network? (For example: iTunes, shareware programs, etc.)

Hardware Asset Scan Information

Scans for the hardware components contained on one or more machines. You can perform this scan on physical machines and online virtual machines. Offline virtual machines and virtual machine templates are ignored by this scan.

This scan helps you answer the following important questions:

- What hardware components are on my scanned machines?
- How many do I own?
- How much memory is on each machine?
- What type of processors are on my machines?
- What services are running on my machines?
- What services have failed to start on my machines?

Security Controls's Advantages Over Other Asset Tools

With Security Controls, all the machine information you want is consolidated nicely in one location. With most tools you must spend a lot of time and energy clicking around in different tables to locate the information you want. In order to present it in an organized fashion you need to copy the information from multiple sources and then paste it into a text or spreadsheet program. With Security Controls's asset inventory feature, all the information is readily available in one location and is easily groupable and sortable.

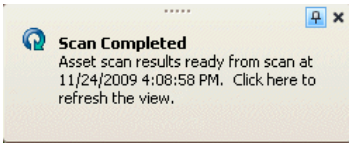
The machine information is also easily distributable. The reporting feature enables you to generate several different reports that contain a considerable amount of information. The reports can be printed or they can be exported to a number of different electronic formats, enabling you save them to disk, view them with the program of your choice, or email them to others.

45. Asset Scans are Performed as Background Tasks

All asset scans are performed as **background tasks** using the services of the **Operations Monitor**. This means you can initiate a scan and then move on to other concurrent work within Security Controls without having to wait for the scan to complete. This also means you can have multiple asset scans active at the same time.

Scanning Considerations

- Is there a practical limit to the number of scans you can have active at the same time?
- Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch downloads, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Security Controls starts responding slowly.
  Is there a problem if the same machine is included in two or more concurrent scans?
- No. Multiple scanning tasks can be performed on a target machine at the same time.
  If I minimize the Operation Monitor window, how will I know when the scan is complete?
- A notification dialog box is displayed in the lower-right corner whenever a scan completes. The dialog box will be displayed for several seconds before slowly fading away. You can pin the dialog box in place by clicking the pin icon.



Will I still be able to immediately view scan results?
Scan results are viewed from within Machine View. See **Viewing Asset Scan Results** for details.

46. Asset Management Scan Requirements

Before attempting an asset scan, please confirm that you meet the following requirements:

- The Windows Management Instrumentation (WMI) service must be enabled and accessible on the target machines.
- TCP port 135 must be configured on your organization's firewall to allow the WMI protocol.
- Credentials must be provided for the target machines. You cannot perform scans using your current logon credentials. See Supplying Credentials for details.
- For target machines using Windows operating systems, which employ the use of User Account Control, you must either:
  - Join the machines to a domain and then perform the scan using domain administrator credentials, or
  - If you are not using the built-in Administrator account on the target machines (and using that account is NOT recommended), you must disable User Account Control (UAC) remote restrictions on the machines. To do this:

1. Click **Start**, click **Run**, type **regedit**, and then press **Enter**.
2. Locate and then click the following registry subkey:
3. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
   If the **LocalAccountTokenFilterPolicy** registry entry does not exist, follow these steps:
   1. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
   2. Type **LocalAccountTokenFilterPolicy** and then press **Enter**.

Right-click **LocalAccountTokenFilterPolicy** and then click **OK**.

5. In the **Value data** box, type **1**, and then click **OK**.
6. Exit Registry Editor.

For more details on disabling UAC remote restrictions, see Microsoft Learn (opens in a new window)

Windows Firewall Requirements for Hardware Asset Scans

Security Controls scans for hardware assets using WMI in semisynchronous mode. This means the firewall policy only requires DCOM connections from the console machine to the target machines. Asynchronous mode, which would require reverse connections back to the console, are not used.

To scan hardware assets of a machine with Windows Firewall running, you must set that machine's firewall to allow remote administration. You can configure the firewall via group policy or local command. The local command is:

Bash

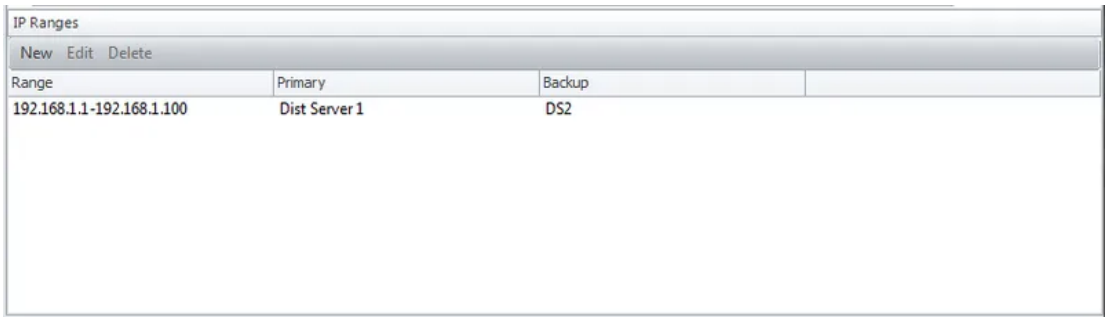
```
netsh firewall set service RemoteAdmin enable
```

If you are unfamiliar with Windows Firewall administration, the following link may help:

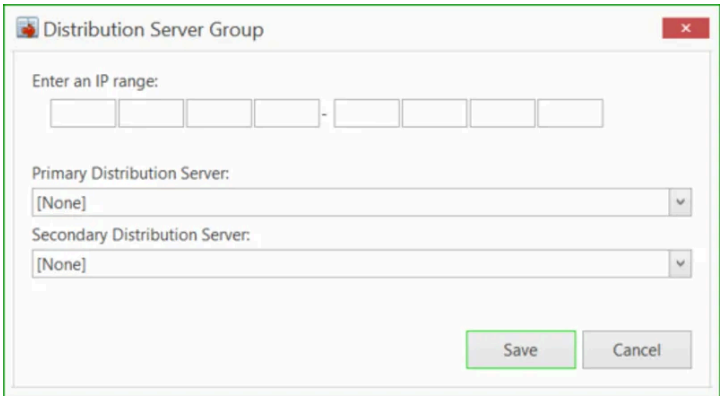
- Microsoft Learn (opens in a new window)

47. Assigning IP Addresses to Distribution Servers

You define which target machines will use a particular distribution server by assigning the IP addresses of the target machines to the distribution server. To assign one or more IP address ranges to a distribution server, select **Tools > Options** and then select the **Distribution Servers** tab. Any currently defined IP address ranges are shown in the **IP Ranges** pane.



To modify an existing entry, select the entry and then click **Edit**. To define a new range of IP addresses, click **New**. The **Distribution Server Group** dialog is displayed.



Field	Description
Enter IP range	Use the available fields to define the new IP address range.
Primary Distribution Server	Select the distribution server you want to use as the primary distribution server for this collection of target machines.
Backup Distribution Server	(Optional) Select the distribution server you want to use as the secondary distribution server for this collection of target machines. The secondary distribution server is only used if the primary distribution server is unavailable.
Save	To accept the current settings, click **Save**.
Cancel	To cancel without saving your changes, click **Cancel**.

48. Automatically Deploying Patches

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

Security Controls can be configured to automatically deploy all missing patches to machines after a scan is performed. When performing domain scans, this can be especially useful as it provides a one-step update. The automatic deployment is performed by enabling the proper deployment package options on the **Agentless Operation page**.

49. Automatically Sending Email Reports and Notifications

> This feature applies only to agentless scans and deployments initiated from the console; it does not apply to agents that may also be using this template.

Messages containing scan reports or deployment reports can be automatically emailed by Security Controls. You simply configure the scan template, the deployment template, the machine group, or the machine of your choosing so that reports are automatically sent each time the template or group is used. You can designate which reports should be sent and to whom the reports should be sent.

In order to use this feature you must enable **email operations**.

Templates

You can configure scan templates to automatically:

- Send PDF versions of reports upon completion of a scan

You can configure deployment templates to automatically:

- Notify users of pending patch deployments
- Send a report upon completion of a deployment

For information on configuring templates to automatically send email reports:

- **Scan templates**: Please see **Creating a New Scan Template** and **Creating a New Asset Scan Template**.
- **Deployment templates**: Please see **Creating a Deployment Template**.

Machines and Machine Groups

For information on configuring the program to automatically send email reports when individual machines are scanned, see **Managing Individual Machine Properties**. For information on configuring a group of machines to automatically send email reports when the machine group is scanned, see **Working With A Machine Group**.

50. Automating Patch Management in an Agentless Environment

The goal of any IT group is to centralize and automate processes to reduce the amount of work needed to maintain your environment. The goal of Ivanti is to provide tools and solutions to help you achieve this level of automation. This section will discuss ways to help automate the patch management process.

Automating Machine Discovery

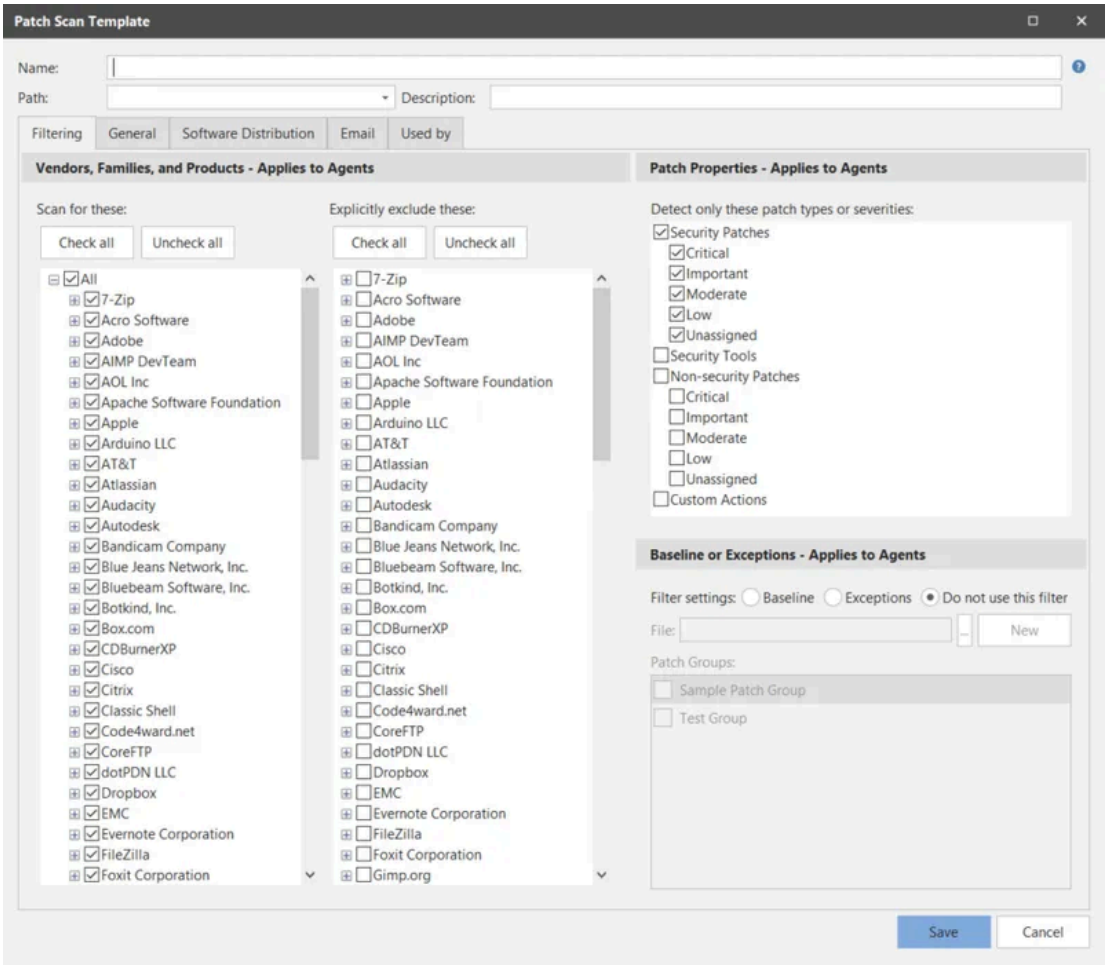
The first goal in automating the patch process is to create your machine groups as dynamically as possible. The easiest way to achieve this is to use Active Directory. If you group the machines in your environment the same way you will be managing the patching of machines, you can use the OU area of the machine group. Each time the machine group is used it will “talk” to Active Directory and pull the current list of machines from the OUs. The same can be said of using the domain area, but that may encompass more than you want in an automated process. Another way to easily create dynamic groups is by IP range. Any new machines in those ranges will be captured whenever you perform a new scan.

Scan Template

When we start talking about automation we need to consider what we will be pushing. Most companies have very loosely defined approval processes for patches. Depending on your needs you will need to decide what works best for your situation. If you are concerned with all security patches, regardless of product, you can use the predefined **Security Patch Scan template** that is built into the product. Any new releases of XML data files will automatically include the security patches in this scan template the next time it is used.

This may be adequate for your end-user environment, but for automating server patching you may want to consider using a patch group. The patch group or approved patch list allows you to define a list of specific patches to scan for. This can be tied to the scan template and then scheduled to scan with automatic deployment to automate the patch process from start to finish. When new patches are released, you can evaluate and determine what patches are approved for deployment in your environment and update your patch group or your approved patch list with the new patches. A scheduled scan will take these changes into account by scanning and deploying the missing patches from the patch list.

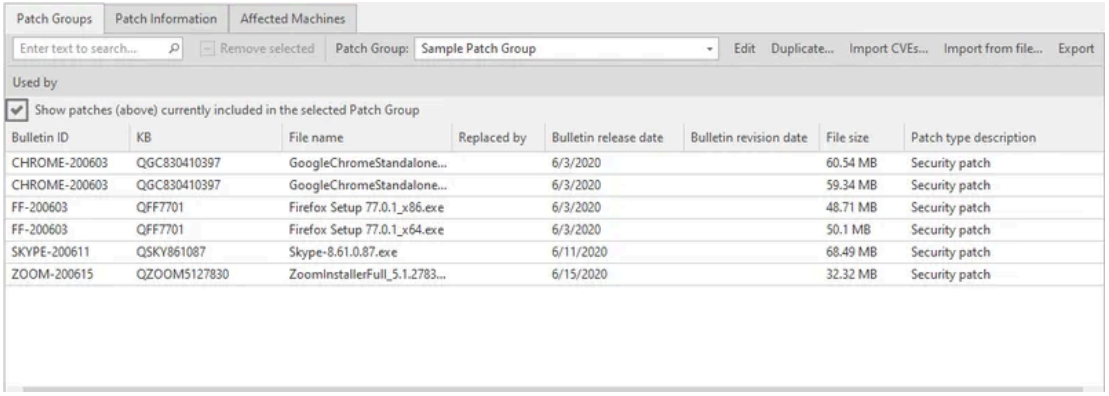
In the following screen shot you can see the scan template **Filtering** tab. You can use the **Baseline** or **Exceptions** filter to specify either an approved patch list or one or more patch groups that collectively represent a baseline set of patches. The section that follows explains how to create a patch group or patch list.



Patch Groups

> When Security Controls uses a patch group to scan for selected patches, it always scans for and reports on the status of all product levels. It will also disable patch replacement, meaning it will show as missing earlier patches that have been replaced by later patches.

To create a new patch group, on the main menu select **New > Windows Patch > Patch Group**. This presents the Patch View dialog. Any existing patch groups are displayed in the bottom pane. Use the Patch View filters to narrow the list of patches displayed in the top pane. You then right-click on the desired patch or patches, select **Add to Patch Group** and choose a patch group name. The patch group is automatically saved.



You might create a Smart Filter that identifies all of the current vendor critical security patches. From this point on, for each patch release you simply use your Smart Filter and from the filtered view select all and add to the existing patch group, creating an easily repeatable process that takes only minutes to maintain.

In your patch scan template, in the **Baseline** or **Exceptions** area, click the browse button and select the patch group(s) you wish to use. Now the scan template is configured to scan for a specific list of patches.

If you choose to use an approved patch list, all you need to do is create a text file and enter patches by KB number, one patch per line. In the **Baseline** or **Exceptions** area of your scan template, click the **File** box's browse button and navigate to your text file. This file is easily distributed to multiple consoles for ease of use and simplification of patch approval across multiple consoles.

Example approved patch list:

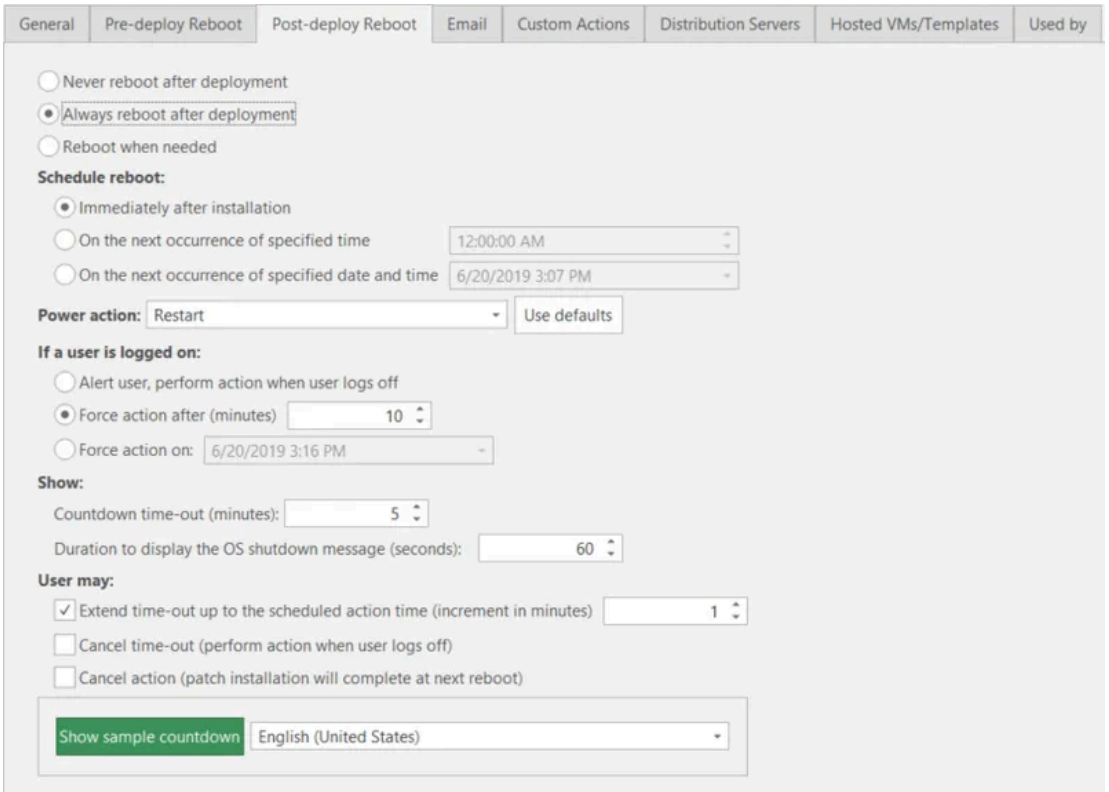
Q123456

Q234567

Q345678

Deployment Template

In your deployment template you will want to configure reboot options to meet the needs of the group you are intending to automate. If you are working with an end-user environment, you may want to set reboot options to be more flexible to work around people potentially working late. For example, on the **Post-deploy Reboot** tab, in the **Schedule reboot** area specify **On the next occurrence of specified time**. You might also enable the **Extend time-out** check box.



For server environments, the recommended reboot option is not as obvious.

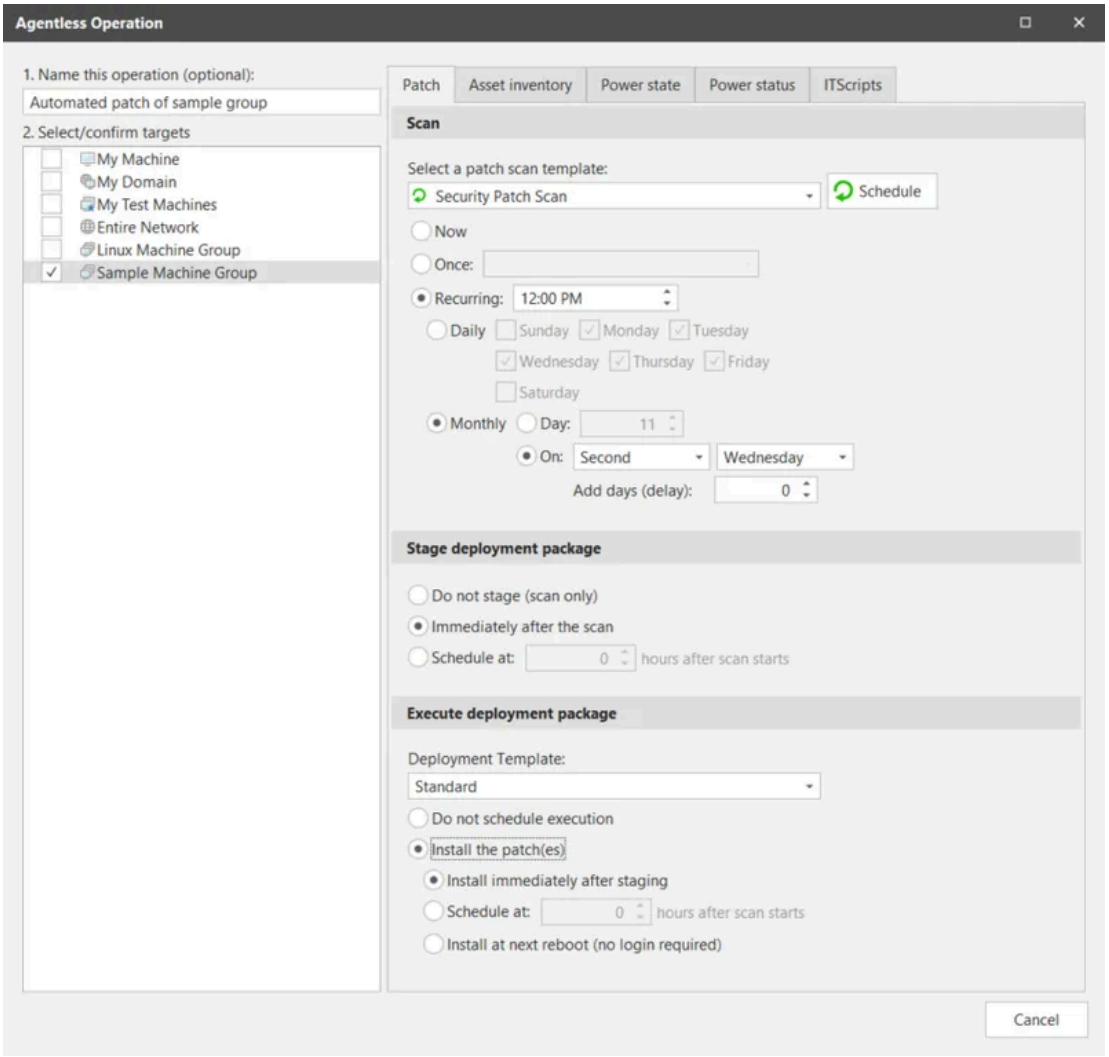
- You may want to configure reboots to be performed immediately after installation. Why? Because you will normally run the scan and deployment in a maintenance window and will want the reboot to follow immediately. You can also shorten the timeouts on

reboot to speed up the process as anyone who would be on these machines should be aware of the maintenance windows in advance.

- On the other hand, you may elect to **Never reboot after deployment** even though a reboot is typically required. This makes sense in situations where server availability is extremely critical to your business. You might want to manually reboot your servers so that you are always onhand in case something should go wrong during the reboot process.

Scheduling Automated Operations

This final step is where it all comes together. Once you have your groups and templates configured you will want to schedule your jobs to execute on a regular basis. To schedule a job to run automatically you start at either the home page or the machine group. When starting from within a machine group, click **Run operation**. You will see a dialog similar to the following:



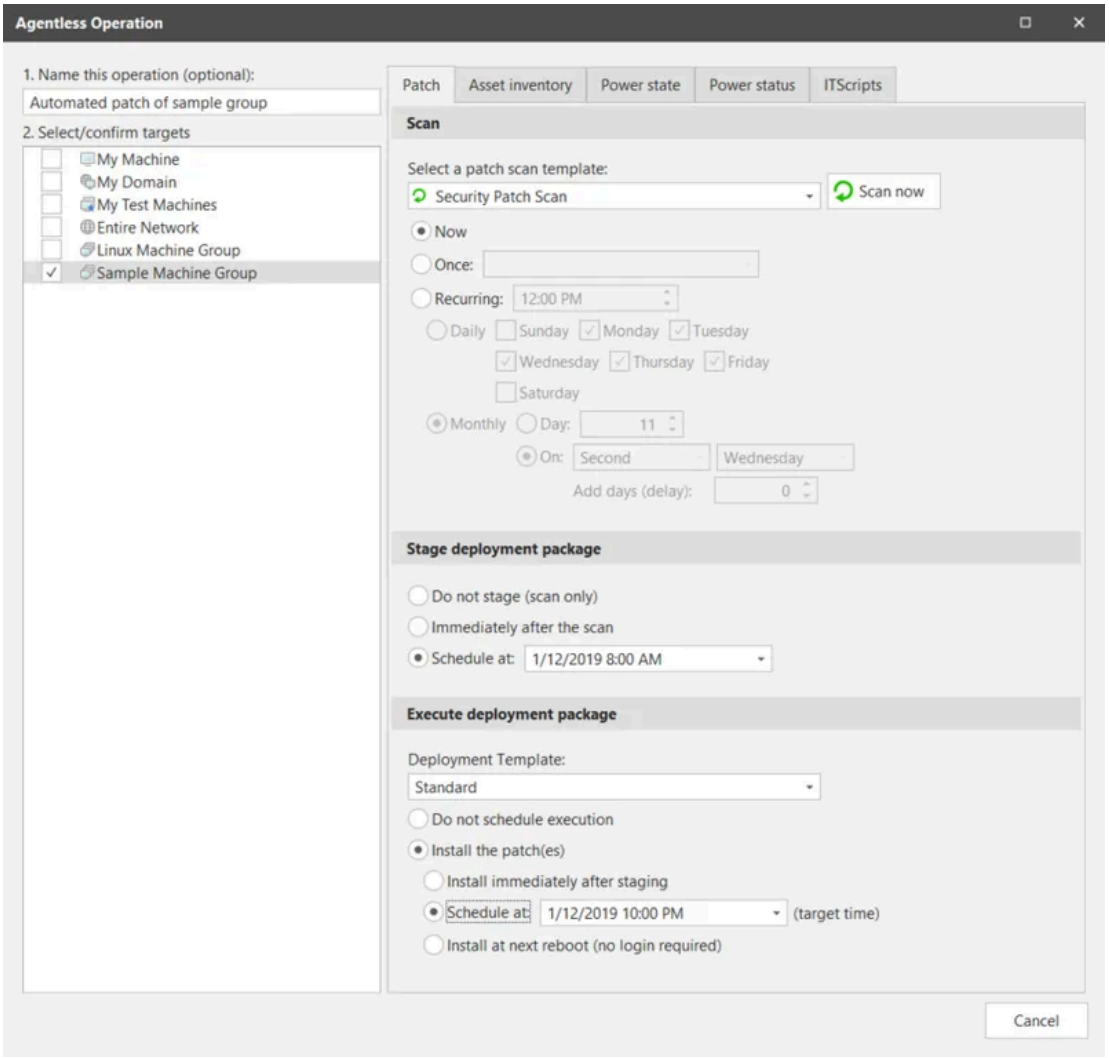
From this dialog you can execute jobs now, schedule to run once at a specific time and date, or schedule recurring jobs to run. You can also elect to immediately deploy patches after the scan. This is the most important option we will discuss in this section. The machine groups and scan and deployment templates we have created previously have fine-tuned what we want to scan and deploy for our environment. With the knowledge of what will be pushed we can now schedule the job to execute from start to finish without the need to handle the job from one stage to the next. In the screen shot above you will see we've defined a recurring scan with immediate deployment that is set to execute on the second Wednesday of every month. This is the day after Patch Tuesday, which will almost always have new patches to push.

When scheduling jobs keep in mind where the scheduled task resides. A scheduled scan with immediate deployment resides on the console until the scan completes. Once the scan completes it will push patches out to machines and execute immediately. The reboot will be scheduled based on the settings in the deployment template and on the target machine's local time.

Staged Deployments

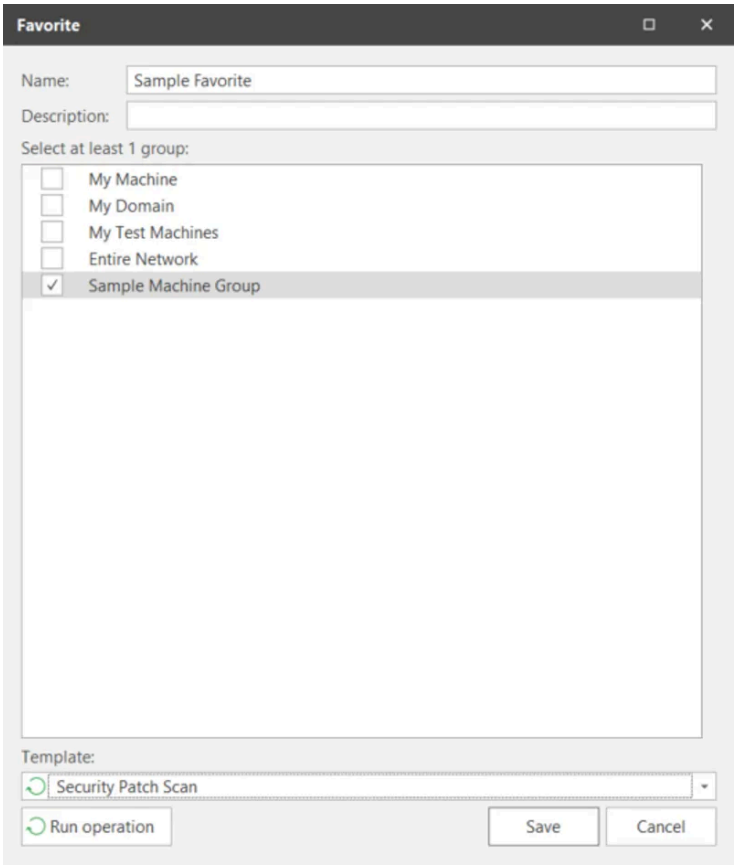
Instead of performing the staging and deployment steps immediately after the scan, you might decide that it makes more sense to schedule the steps at more appropriate times for your organization. For example, your corporate security policy might specify a patch deployment windows that begins at 10:00 p.m. on Saturday. In this case, it might be best to schedule the stage deployment process to begin earlier that day, say at 8:00 a.m. This will give Security Controls all day Saturday to create the deployment packages and copy them to your target machines. You can then schedule the actual execution of the deployment package to occur at the start of your deployment window. When 10:00 p.m. rolls around, everything will be in place and the deployments will occur without delay on your target machines.

You would define your **Agentless Operation** dialog as follows:



Favorites

A favorite is a combination of machine group and scan template for the console to reference when it executes a job. You can reuse favorites to schedule multiple jobs to run at different times. From the favorite you can click **Run Operation** and schedule out additional one time or recurring jobs as needed without having to recreate additional favorites.



Automated Email Reporting

From your machine group, scan template, and deployment template you can configure reports to be automatically generated and emailed to designated recipients. When automating the patching of an environment, this is an easy and efficient tool for keeping all necessary personnel up to date on the state of the environment. There are a variety of different reports to choose from that will present different data for different audiences and needs. You may need to try a few to find the best fit for your reporting needs.

To use the automated email feature you need to setup your email credentials. To do this you select **Tools > Options > Email** and then provide your email server address and authentication information.

Related Topics

- **Console Software and Hardware Recommendations**
- **Port Requirements and Firewall Configuration**
- **Distributed Environment Management**
- **Agentless Patch Management**
- **Best Approach for Applying Patches in an Agentless Environment**
- **Agent-Based Patch Management**
- **Agent Rollout Options**
- **Installing and Supporting Agents on Internet-Based Machines**

- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

51. How to View Detailed Help Information About the PowerShell Commands

There are a number of ways you can find help information for the available PowerShell commands. Simply launch a PowerShell console, import the STProtect module and then type any of the following commands. Full localized help documentation is included as part of the Security Controls installation.

View the complete list of available commands

Bash

```
PS C:\> (Get-Module -Name STProtect).ExportedCommands
```

The available commands are:

- **Add-MachineGroup:** Adds a new machine group with the specified name, description and path.
- **Add-MachineGroupItem:** Adds or updates a set of resolvable machine names to a machine group. The option to specify explicit credentials and set the include/exclude status is supported.
- **Add-PatchGroup:** Adds a new patch group.
- **Add-PatchGroupItem:** Adds patches to an existing patch group.
- **Add-STCredential:** Adds a credential to the current user's credential store for use in patch and deploy operations.
- **Format-PatchDeployTable:** Formats a patch deploy result as a table with top level operation information as well as machine summary statistics.
- **Format-PatchScanTable:** Formats a patch scan result as a table with top level operation information as well as machine summary statistics.
- **Get-MachineGroup:** If a name is provided, a machine group is retrieved by name. Otherwise, all defined machine groups are returned.
- **Get-PatchDeploy:** Interrogates the data store to retrieve recorded patch deploy information, including individual machine deploy states. Partial information is retrieved if the patch deploy is in progress.
- **Get-PatchGroup:** Gets patch group information.
- **Get-PatchScan:** Interrogates the data store to retrieve recorded patch scan information, including individual machine summary statistics. Partial information is retrieved if the patch scan is in progress.
- **Get-PatchScanTemplate:** If a name is provided, a patch scan template is retrieved by name. Otherwise, all defined patch scan templates are returned.
- **Get-STCredential:** Gets one or more credential references from the current user's credential store given the criteria. If no criteria are specified, all credential references are returned.
- **Get-VendorFamilyProductHierarchy:** Retrieves the name id pairs for including/excluding vendors, families and products using New-VendorFamilyProduct.
- **Invoke-DownloadMissingPatches:** Downloads all missing patches detected in a patch scan. If a patch has already been downloaded into the patch store location, no action is taken on that patch.

- **Invoke-PowerStateDeploy:** Executes a power management task against the specified machine targets. A combination of explicitly-defined endpoint names and/or pre-defined machine groups may be used to specify the targets.
- **Invoke-WakeOnLan:** Initiates a new Wake-On-LAN operation against the specified machine targets. The targets specified must have been scanned with a hardware asset scan to identify the MAC address.
- **New-PatchFilter:** Creates a new patch filter. Filters created with this command are used as input to New-PatchScanTemplate or Set-PatchScanTemplate.
- **New-PatchPropertyFilter:** Creates a patch detection filter based on patch properties. Filters created with this command are used as input to New-PatchFilter.
- **New-PatchScanTemplate:** Creates a new patch scan template.
- **New-VendorFamilyProductFilter:** Creates a new Vendor Family Product filter.
- **Remove-MachineGroup:** Removes a machine group and all child items.
- **Remove-MachineGroupItem:** Removes a set of resolvable machine names from a machine group.
- **Remove-PatchGroup:** Delete the patch group information.
- **Remove-PatchGroupItem:** Removes patches from an existing patch group.
- **Remove-PatchScanTemplate:** Removes the patch scan template with the specified name.
- **Remove-STCredential:** Removes a credential from the credential store. Only credentials owned by the current user can be removed.
- **Set-MachineGroupCredential:** Sets or removes a top-level machine group credential to be used as the default credential for all machines defined in a machine group. This credential is used only in cases where no machine or endpoint specific credential has been specified.
- **Set-PatchScanTemplate:** Updates a patch scan template.
- **Start-PatchDeploy:** Queues a new patch operation to deploy all of the patches identified in a patch scan.
- **Start-PatchScan:** Queues a new patch scan operation against the specified machine targets. A combination of explicitly defined endpoint names and/or pre-defined machine groups may be used to specify the targets.
- **Stop-PatchDeploy:** Cancels an active patch deploy operation.
- **Stop-PatchScan:** Cancels an active patch scan operation.
- **Update-STCredential:** Updates a credential in the current user's credential store for use in patch and deployment operations.
- **ValidateElementsNotNullOrWhiteSpace:**
- **ValidateNotNullOrWhiteSpace:**
- **ValidatePSCustomObjectType:**
- **Wait-PatchDeploy:** Waits for an active patch deployment operation to complete.
- **Wait-PatchScan:** Waits for an active patch scan operation to complete.
- **Watch-PatchDeploy:** Monitors an active patch deployment operation, periodically reporting progress and status until it completes. The patch deploy operation, status, percentage complete and elapsed time are all reported as progress.
- **Watch-PatchScan:** Monitors an active patch scan operation, periodically reporting progress and status until it completes. The patch scan operation, status, percentage complete and elapsed time are all reported as progress.

View detailed help for an individual command

```
PS C:\> Get-Help <command> -detailed
```

View complete help for all commands

```
PS C:\> (Get-Module STProtect).ExportedCommands.Values | ForEach-Object { $_ | Get-Help –Full}
```

To pipe the output to a text file:

```
PS C:\> (Get-Module STProtect).ExportedCommands.Values | ForEach-Object { $_ | Get-Help –Full} | Out-File “C:\SampleDirectory\HelpOu
```

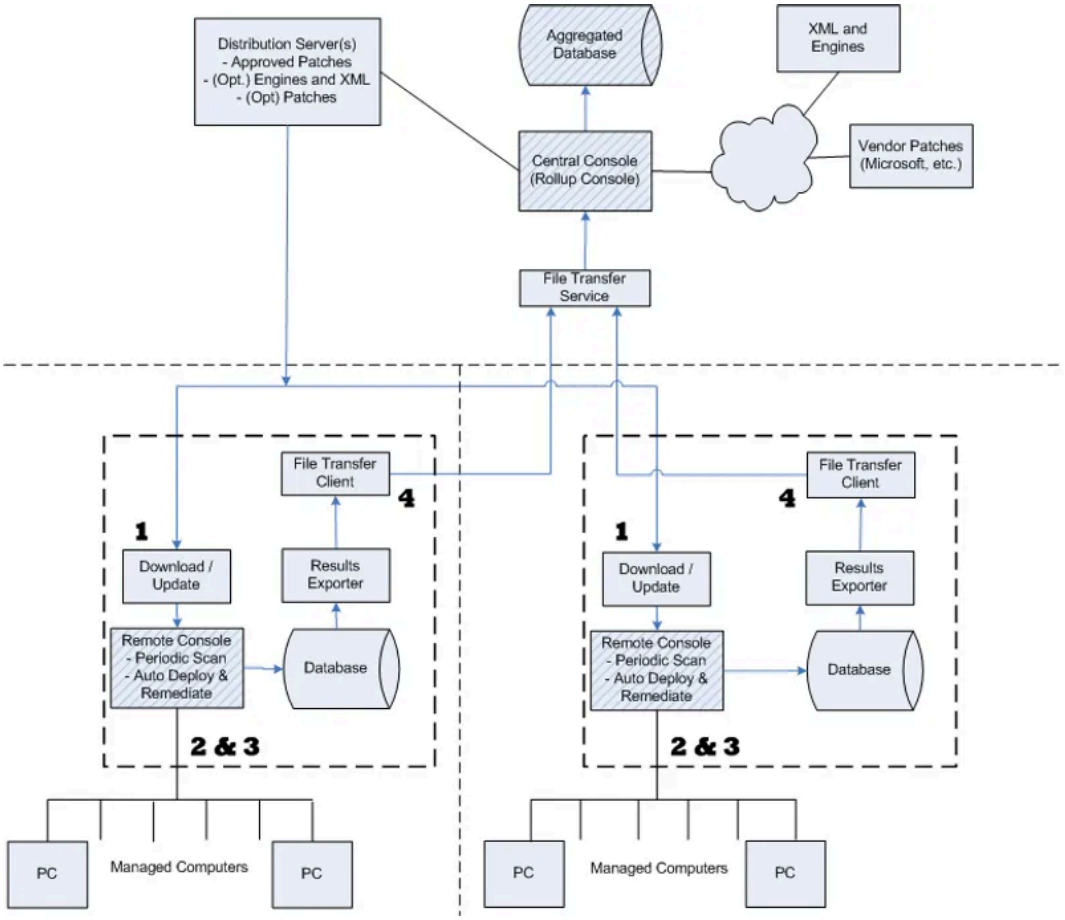
52. What is a Disconnected Console Configuration?

A disconnected console is a remote console that does not have Internet access. The remote console does, however, have access to a local WAN. In this scenario the remote consoles must retrieve the patch files, engine files and data definition files from a networked distribution server rather than from the Web. The central console (which does have Internet access) is responsible for downloading the latest engines, definition files and patches from the Web and for placing these files on one or more distribution servers. The remote consoles can then use the distribution servers to download the required information before performing their scans.

Once the central console has copied the necessary files to the distribution servers, the basic process is as follows:

1. The remote console downloads the latest files from a distribution server.
2. The remote console performs a scan.
3. Based on the scan the remote console performs the necessary patch deployments.
4. The remote console then rolls up the results to the central console, which contains an aggregate database of all scan and patch deployment activity in the network.

The following figure illustrates this process.



Tasks Performed by the Central Console

In this scenario, the main functions of the central console are to:

- Download the latest patches, engines and data definition files from the Web

- Copy the engines, definition files and patches to one or more distribution servers
- Act as the data rollup console by collecting the results of the scans and deployments performed by the remote consoles

For more information, see **Configuring the Central Console in a Disconnected Configuration**.

Tasks Performed by the Remote Consoles

Each remote console is responsible for patching itself and any managed machines that are located at the same site. There may or may not be an administrator at the remote site and the remote sites may or may not have Internet access. The main functions of each remote console in this scenario are to:

- Get the latest engines and data definition files over the WAN from a distribution server
- Scan all the machines at their site
- Download the missing patches from a distribution server
- Deploy all approved patches that are missing
- Roll up the results of the scans and deployments to the central console

For more information, see **Configuring the Remote Consoles in a Disconnected Configuration**.

53. Before You Begin

Read through this entire section before using the Migration Tool.

Target Console Machine Considerations

The machine you are migrating to must:

- Contain one of the approved Windows operating systems
- The version of Security Controls that is on your target console must be equal to the version on your existing console.
- You do not need to activate or configure anything on the newly installed (target) console. The migration tool will provide all of that information during the restore process.
  Not be an active console
  The restore process will overwrite any data that exists on the new Security Controls console machine.

If You are Using Agents

Console Alias List

> **Important!** Perform this step as far in advance of the migration as possible.

The Console Alias list on the existing console must be updated with the host name, IP address, FQDN, etc. of the new target console. This is done so your agents will know to use the new console for their check-ins when the existing console is turned off and becomes unavailable. Use the **Tools > Console alias editor** menu to update the alias list.

You should update the Console Alias list as far in advance of the migration as possible. This is so the agents will have time to check in with the existing console and retrieve the updated Console Alias list. A good rule of thumb is to update the Console Alias list several check-in periods prior to the actual migration.

> **Important!** Any agents that do not check in with the old console and receive an updated alias list will be stranded when the old console is turned off.

> **Tip:** You will avoid stranding any agents if you are using Security Controls Cloud synchronization as a fallback failover destination. If for some reason the agents cannot locate the new console, if you have enabled the use of Security Controls Cloud synchronization in the agent policy, the agents will have the ability to check in with the cloud.

Security Controls Cloud Synchronization

If you are using Security Controls Cloud synchronization, perform a full update by selecting **Tools > Options >** Security Controls **Cloud sync** and then clicking **Force full update now**. This will ensure that the agent policy data contained on the cloud service is up to date.

Upgrading to a More Current Version of SQL Server

If you want to upgrade to a more current version of SQL Server during this migration and you are using:

- **A local SQL Server Express Edition:** No actions are required (do not pre-install any version of SQL Server). The most current supported version of SQL Server Express Edition will be installed automatically when you install Security Controls.

- **A local Full Edition of SQL Server:** Install the desired edition of SQL Server on the new console machine BEFORE you install Security Controls. During the installation of Security Controls you will point to the new local SQL Server instance.
- **SQL Server on a remote server:** To perform the upgrade:
  1. Install the desired edition of SQL Server on the remote server.
  2. Backup your current Security Controls database and restore to the new SQL Server.
  3. Use the Database Setup Tool to point all instances of Security Controls to the new instance.
     To access the Database Setup Tool: **Start > Ivanti** Security Controls **> Database Setup Tool**.
  4. Run the migration.

> You can upgrade your remote SQL Server edition after the migration if you prefer, but the recommendation is to do it before the migration.

Create a Backup of Your Database Before Using the Migration Tool

This is strictly a precaution, but a smart one. If you are using an express edition of SQL Server, you can use the Database Maintenance tool within Security Controls to create the backup. If you are using a full edition of SQL Server, you should use the SQL Server Maintenance Plan Wizard to setup your maintenance plans as this wizard is more robust and provides additional functionality.

Record Your Current License Information

Select **Help > About Ivanti** Security Controls and record your current license key data and product capabilities. You will use this information after the migration is complete to verify that your license information was properly migrated.

If You Have Scheduled Patch Deployments

You should wait for the scheduled patch deployments to complete before you begin the migration. If a scheduled deployment does occur after you begin the migration, the new console will not receive the deployment results.

Related Topics

- Requirements for Using the Migration Tool
- Commonly Asked Questions
- Creating Your Backup Files
- Restoring Your Console on a New Machine
- Post-Migration Tasks

54. Best Approach for Applying Patches in an Agentless Environment

Patch management can be tedious work. This topic is intended to help reduce the amount of deployments to machines to make your work more effective.

The best order of approach to maintaining patch levels on a machine is to start with product levels. Product levels are very involved. Vendors recommend installing product levels one at a time and most should be followed by a reboot before any other patches or product levels are applied. Ivanti enforces this recommendation programmatically in Security Controls by only allowing product levels to be installed one at a time.

Detailed Course of Action

The best course of action is typically as follows:

1. Start with any operating system product levels.
   Be sure to adequately test the product level before deploying it to your entire organization. After **deploying** the product level you should reboot the target machines and then perform a fresh scan. Rescanning will give you the new state of the machine so you can continue applying product levels.

> Note: Operating system product levels change the state of a machine and may inhibit you from rolling back patches that were applied prior to the release of the new product level.

Apply product levels to major products such as Office, Visio, and SQL.
Order does not matter here, but we do recommend rebooting in-between each of these major product levels. Though not as common, these product levels can also change the state of a machine considerably.

3. Deploy any remaining product levels to products such as MSXML, .Net, and MDAC.
   These need to be pushed in separate deployments, but in this case you can do the deployments with no reboot and stagger them apart enough and then reboot after they have all been applied.
4. After all product levels have been deployed and the target machines have been rebooted, deploy any missing Microsoft operating system patches and perform a reboot.
5. Deploy any other missing Microsoft patches such as Office, Internet Explorer, etc. and reboot as needed.
6. Deploy any third party patches and reboot as needed.
7. **Rescan** and **confirm** all has been applied.

> The steps above may span several maintenance windows. In the case that you cannot do all of the above in a single maintenance window, each step should be followed up by a patch deployment to ensure you are not open to security vulnerabilities between maintenance windows.

> **Tip:** The steps above should be built into your machine build policy. This will ensure that machines go into the field as up to date as possible. Maintaining the machines is much easier than catching up on many months' worth of product levels and patches.

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

55. Best Practices When Using Multiple Administrators

Recommendations:

- You should upgrade your hardware platform by increasing the number of processors and the amount of installed memory on the console machine. This will increase performance in those instances when two or more administrators are logged on at the same time and performing tasks.
    - Minimum suggested hardware requirements for two administrators: 2 processor cores and 4 GB RAM
    - For each additional administrator, add 1 processor core and 1 GB RAM
    - For a high performance system, use 16 processor cores and 32 GB RAM

When two administrators log on to the same console they must use different accounts. The same account can be used only when logging on to different consoles.

- If you edit a group that is typically used by another administrator you should notify that person about the change.
- Each administrator should create their own credentials and assign them to machines.
- Each administrator should define default credentials that are the same as their logon credentials. This will eliminate problems that may occur if the administrator forgets to assign machine credentials.

56. Canceling a Task

You can use Deployment Tracker to cancel either an incomplete deployment task or a staged deployment that has been scheduled but not yet performed. To cancel a deployment task, right-click on the scheduled job and then select **Cancel deployment**.

You can also cancel deployments using the **Scheduled Remote Tasks Manager**. See **Canceling a Deployment** for details.

57. Canceling a Deployment

There are several ways to cancel a patch deployment.

- Immediately following the initiation of a patch deployment, the **Operations Monitor** appears and displays the status of the steps in the deployment preparation process. You can use the **Stop deployment** button to cancel any deployment that is still in the preparation stage.
- After the Operations Monitor shows that the deployment preparation process is complete, you can right-click on a scheduled job in either Operations Monitor or Deployment Tracker and select **Cancel deployment**. You can cancel scheduled deployments on multiple machines at one time.
- You can use the **Scheduled Remote Tasks Manager** to delete any patch deployment tasks currently scheduled on any of the machines in your network. Simply right-click the task(s) and select **Delete**.
- You can select a deployment in the **Results list of the navigation pane** and use the right-click menu to cancel the deployment.

58. Changing a Custom XML File

If you make changes to an existing custom XML file, you must use the **Edit Custom Patch Collection dialog** to remove the old version of the custom XML file and then re-import the updated file. If you just save the file without removing and then re-importing it, the program will continue to use the old version of the file.

59. Viewing Charts

You access the charts page by selecting **View > Charts**. The charts page displays a number of charts that show the security status of your network at the time of the most recent machine scans. There are a number of ways to customize this page. You can:

- Click and drag charts to different locations on the page
- Right-click to float or dock an individual chart
- Maximize an individual chart



60. Step 3: Commit the New Sub-Authority Certificate

Automatic commit process

If you have agents and everything has gone according to plan, after 30 days all of your agents should have checked in, received the new certificate and the system will have automatically committed to the new sub-authority certificate. See the section below titled **What happens after the commit is issued?** for more information.

Manual commit process

You may choose to manually issue the commit command for the following reasons:

- If you do not have agents, you can manually force the commit without waiting for 30 days.
- If there are agents and the system has not automatically committed to the new certificate after 30 days (or as defined by Security Controls internal optimization from the maintenance task), evaluate why the commit has not occurred.

> Stmgmt.exe -commit_authority will tell you which machine names it expects to fail when you perform the commit.

There are a number of outstanding issues, errors or warnings that may have occurred that are preventing the commit from happening automatically. The most likely reason is an agent-related problem, such as one or more orphaned agents that have not checked in (and never will). Your options are to (1) figure out a way to get those agents to check in, (2) delete the machines from Machine View, (3) flag the machines to uninstall their agents (even if a machine never checks in to receive the uninstall command, the fact that Security Controls has indicated that the agent should be uninstalled is enough to get past the error/issue with that machine), or (4) you can manually issue the commit and permanently orphan those agent machines.

Test mode

You can use the test mode in the **commit_authority** command to tell you about potential problems with performing the commit. The command is: `stmgmt.exe -commit_authority -test`

By analyzing this information you can make an educated decision on whether to perform the commit. In some circumstances you may choose to force the commit and purposely orphan certain problem machines.

To force the commit

Use the following command: `stmgmt.exe -commit_authority -force`

If you force the commit and you do have agents that haven't checked in that you want to keep, you will need to reinstall the agent on those machines (the agent will be unable to use the configuration information created by the console and will most likely fail to check in).

What happens after the commit is issued?

When the commit command is issued, the system will stop using the original self-signed certificate and will begin using the new sub-authority certificate. In particular, the following actions will occur:

- A new console certificate will be automatically issued from the sub-authority certificate and saved to the computer account's Personal store on the console machine.

- A new agent certificate will be automatically issued whenever a new agent is installed or when an existing agent's certificate needs to be reissued. The process should have very little affect on your network performance.

61. Commonly Asked Questions

What Core Components are Migrated by the Migration Tool?

- Agent policies
- Background tasks
- Certificates
- Credentials
- Custom patch XML files
- Custom PowerShell scripts that have been imported into the database
- Database (local only)
- Distribution servers (remote only)
- Files referenced by the Machine Group **link to** file feature
- Groups (machine, patch, product levels)
- License activation in a non-proxied online environment
- Global and user settings defined on the **Tools > Options** dialog
- Patch store if contained on a local drive (up to 10 GB of data and data that is not more than 90 days old)
- Results (scan results, deployment results, etc.)
- Templates
- Some user-specific options:
  - **Notifications & Warnings:** Display the file size confirmation dialog before downloading
  - **Scans:** Default Patch Scan Template, Use only the browse list, Use replacement patches
  - **Deployment:** Default Deployment Template

What is Not Migrated by the Migration Tool?

See the section titled **Post-Migration Tasks** for a detailed explanation on how to manually manage the items that are not migrated by the tool.

- An agent running on the local console
- Data rollup configuration
- Share information for a distribution server that resides on the local console
- Proxy configurations
- Patch store data beyond the 10 GB limit or older than 90 days
- ITScript run files (the files that contain output information related to the execution of a script)
- Scheduled deployments
- Any user-specific option not identified in the **What Core Components are Migrated** list

When Should You Perform the Migration?

Soon after the completion of your regularly scheduled patch cycle to give yourself time to complete the migration.

How Long Will it Take to Perform the Migration?

- Simple configurations can be migrated in as little as 60 minutes
- Advanced configurations may require a few days of lead time to prepare for the migration and a few hours or days after the migration to perform system verification steps

Who Should Perform the Migration?

- Any administrator with a Security Controls account can perform the core backup and restore. Account data for the administrator currently logged on to the console machine is included in the core backup.
- Each additional administrator with a Security Controls user account must perform a separate User backup and restore.

> You cannot restore multiple users under the same logged in account, and you cannot restore a user using a different account.

I Use a Remote Database, How is That Affected?

The remote database will not be moved but the connections to the remote database will be restored during the core component restoration process. You will restore your user account data using the normal process.

How Long Should I Maintain My Old Console?

- If you are not using agents, you can retire your old console as soon as the migration to the new console is complete.
- If you are using agents, you should continue to run the old console in parallel until all of your agents have checked in with the new console. See the section titled **Before You Begin** for additional information.

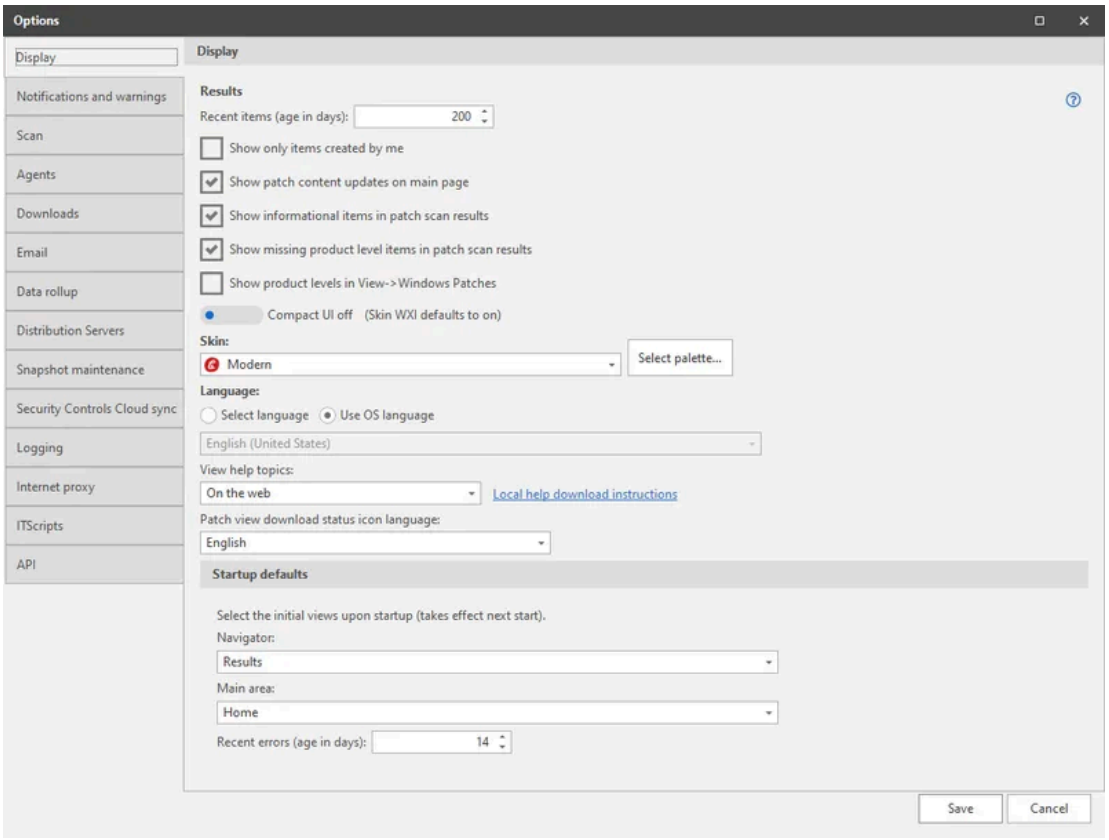
Related Topics

- **Requirements for Using the Migration Tool**
- **Before You Begin**
- **Creating Your Backup Files**
- **Restoring Your Console on a New Machine**
- **Post-Migration Tasks**

62. Configuration Options Overview

You can configure a number of different options within Security Controls. For example, you can define the physical appearance of the program, you can define what notification messages you will see, etc.

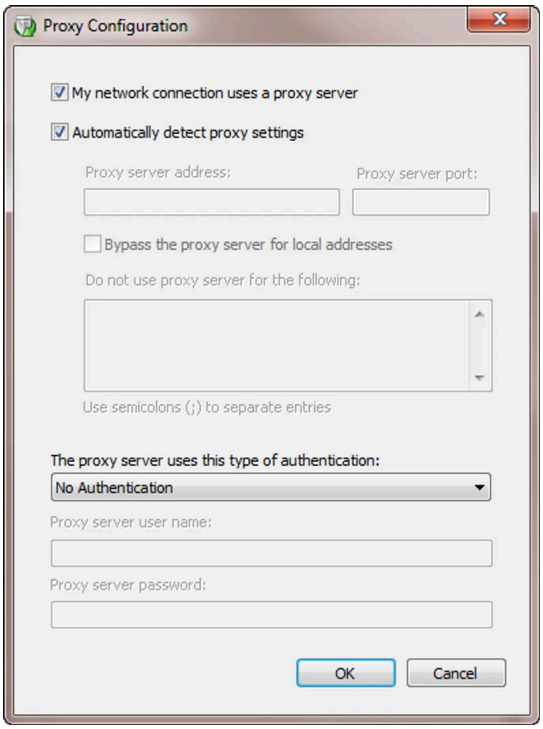
The configuration options are all available from the **Tools > Options** menu, which will cause the **Options** dialog to appear.



To configure an option category, simply select the appropriate tab in the left-hand pane and then configure the related options that appear in the right-hand pane. Each option category is described in detail in the remainder of this section.

63. Configuring Proxy Server Settings for Security Controls Agent

When you click the **Configure Proxy** button on either the **direct connection** or **cloud-based** Security Controls Agent **Registration** dialog, the **Proxy Configuration** dialog is displayed. This dialog enables you to specify the proxy settings the agent will use during the registration process.



Field	Description
My network connection uses a proxy server	If you are required to enter a user name and password each time you launch your browser and access the Internet, it typically means you are using a proxy server and you should enable this check box. If you do not use a proxy server, clear this check box and then click OK (you can ignore the rest of this dialog).
Automatically detect proxy settings	If you want the program to automatically determine the proxy settings by using the Web Proxy Auto Discovery protocol, enable this check box. In this case you can skip the **Proxy server address** and the **Proxy server port** options.
Proxy server address	Type the IP address of your proxy server.
Proxy server port	Type the port number used when accessing your proxy server.
Bypass the proxy server for local addresses	If enabled, this specifies that the proxy server should not be used when the agent connects to a device on the local network.
Do not use proxy server for the following	You can specify one or more IP addresses that do not use the proxy server. If you specify multiple exception entries they must be separated by semicolons.
The proxy server uses this type of authentication	The options are: • **Basic Authentication:** The credentials are sent across the network to the proxy server in plaintext. • **Digest Authentication:** The credentials are encrypted using a hash function before they are sent across the network to the proxy server. • **NTLM Authentication:** Windows NT LAN Manager (NTLM) authentication is used when sending credentials to the proxy server. • **Negotiate Authentication:** The agent and the proxy server will negotiate to determine which authentication method to use.
Proxy server user name	Type the user name to use when authenticating to the proxy server. After the registration process is complete and the agent has a policy, the agent will use the **proxy credentials specified in the agent policy** rather than the user name and password you specify here.
Proxy server password	Type the password to use when authenticating to the proxy server.

64. Agentless Patch Management

The fastest way to get Security Controls configured and patching machines is to do so agentlessly, as described in **Best Approach for Applying Patches in an Agentless Environment**. Once the console is installed it can take as little as a few minutes to setup machine groups to scan an environment. The time to configure will be based on the complexity of the environment and the range of maintenance windows.

Example

An office that contains three floors, with approximately 500 end users per floor as well as a data center with 200 servers, could be broken out many ways. You might create a separate machine group for each floor based on the IP range of the workstations. Servers might be broken down into three more groups: Test, Development, and Production. You might consider breaking the Production department into separate groups such as domain controllers and Exchange / SQL Servers to allow flexibility in scheduling jobs.

Time to Implement

It will take approximately five minutes to create three groups covering the three floors of workstations. Plan on 10-30 minutes to create the server groups; they can be created by OU, by browsing and selecting machines, or by importing identities from a file. Plan on another 15 minutes to schedule the jobs that will scan and optionally auto deploy patches.

The overall time to configure the machine groups and to schedule the scans in this example environment is approximately 45 minutes. Once this is done we are configured and ready to go.

Port Requirements

For agentless scans you will need to be able to resolve the machine by the method you used to create the machine group. You must also be able to access TCP ports 137 - 139 or port 445 on the target machine. File and print sharing and remote registry must be enabled in order to perform the scan. For added security, firewall rules can be applied between vLANs or on the local machine firewall that restrict port access to all but the console's IP. Depending on the environment, complexity, rules, and change control requirements, the amount of time this will add to the initial configuration may vary.

Related Topics

- **Console Software and Hardware Recommendations**
- **Port Requirements and Firewall Configuration**
- **Distributed Environment Management**
- **Best Approach for Applying Patches in an Agentless Environment**
- **Automating Patch Management in an Agentless Environment**
- **Agent-Based Patch Management**
- **Agent Rollout Options**
- **Installing and Supporting Agents on Internet-Based Machines**
- **Agent-Based Product Level and Patch Deployment Process**
- **Guide to Surviving Patch Tuesday**
- **Microsoft SQL Server Database Maintenance**
- **Performing Patching in a Disconnected Environment**

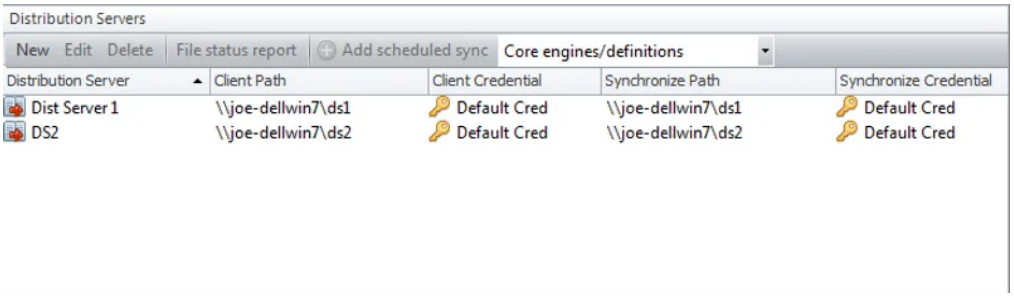
65. Configuring a New or Existing Distribution Server

There are a number of reasons why you may choose to use a distribution server. In Windows environments, a distribution server can be used to store patches as well as the most up-to-date engines and definitions that are available. In Linux agent environments, distribution servers can be used to download core files but not patches. **Linux agents use YUM to download any patches that must be deployed**. For more details on distribution servers, see **Why Use a Distribution Server?**.

IMPORTANT! In addition to using the **Distribution Servers** dialog to configure the distribution server within Security Controls, under certain conditions you will need to provide the LOCAL SYSTEM machine account with the proper sharing and security permissions. See **Configuring System Account Permissions** for details.

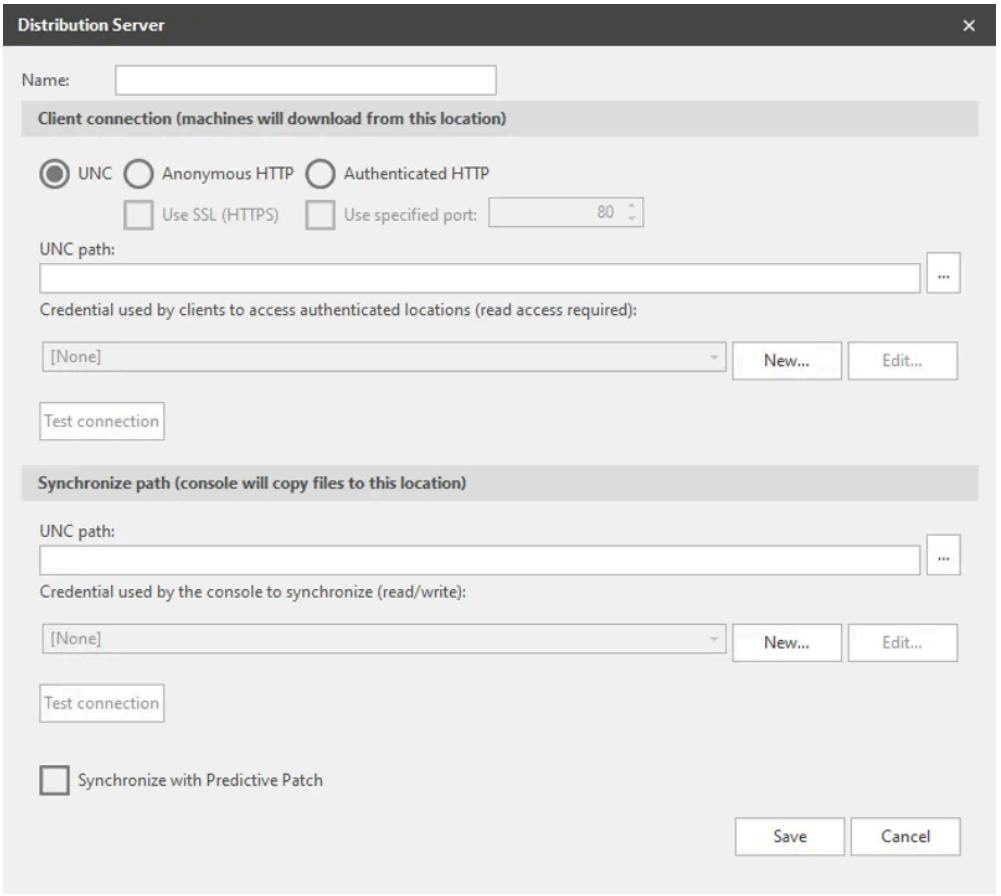
How to Access Your Distribution Servers

To configure a distribution server, select **Tools > Options** and then select the **Distribution Servers** tab. Any currently defined distribution servers are displayed in the top pane.



You cannot delete a distribution server that is currently being used by an **agent policy**. Also, if you edit and save a distribution server that is being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.

To configure an existing distribution server, select the distribution server and then click **Edit**. To configure a new distribution server, click **New**. The **Distribution Server** dialog is displayed.



In the top half of the dialog, be sure to specify a location and authentication method that all the target machines can use when accessing the server. The lower half of the dialog is used to specify how the console will connect to this same location on the distribution server. Although the physical location you specify must be the same in both halves of the dialog, in the top half you can specify the *method* used by the target machines when accessing the data (**UNC** vs. **Anonymous HTTP** vs. **Authenticated HTTP**).

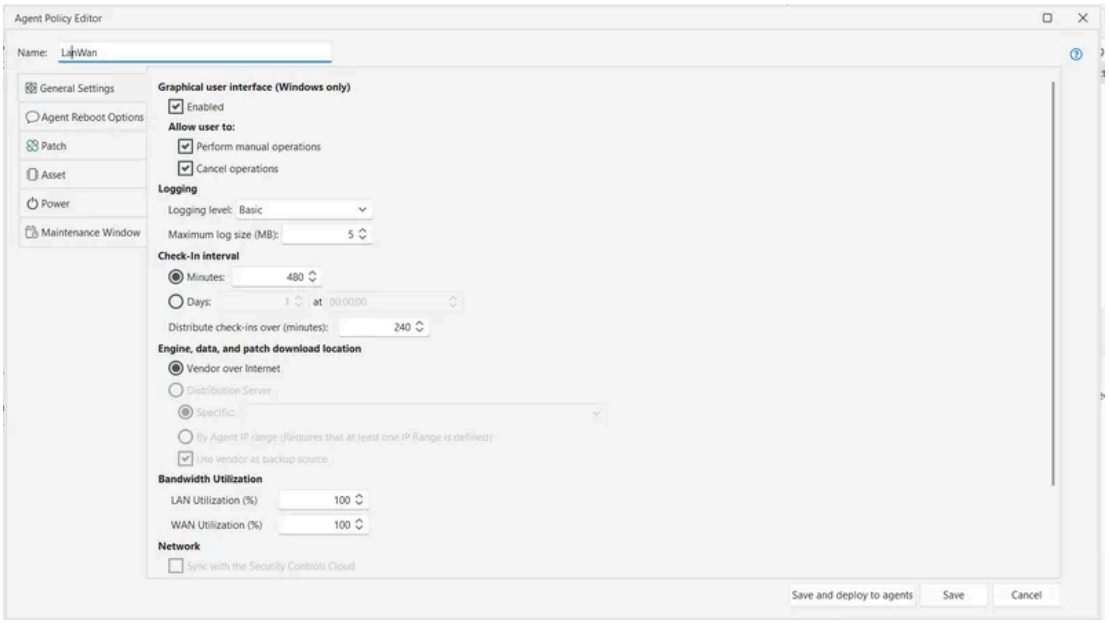
Field	Description
Name	The name you want to give to the distribution server you are configuring. The name can contain letters, numbers, and special characters.
Connection method	Specify how the target machines will access the file repository on the distribution server. • **UNC**: If you want to specify both the path name of the repository on the distribution server and the logon credentials used by the target machines when logging on to the distribution server, enable this option. You must also define the **UNC Path** and the **Assign credentials** options. • **Anonymous HTTP**: If you want the target machines to access the repository via the Internet using an anonymous (unauthenticated) Web connection, enable this option. You must also define the **URL** option. • **Authenticated HTTP**: If you want the target machines to access the repository via a Web browser using a secure Web connection, enable this option. You must also define the **Port**, **URL**, and **Assign credentials** options.
Use SSL (HTTPS)	If you want the target machines to contact the distribution server using an SSL connection, enable this check box. This check box is not available if UNC is selected as a client connection.
Use specified port	Specifies the port used by the target machines when contacting the distribution server via the Web. The default value is 80, or 443 if SSL is selected.
UNC path / URL	The name of this field changes depending on whether UNC or HTTP is selected as the connection method. Specify the UNC path name or the URL path to the repository on this distribution server. The physical location you specify here for the target machines to use should be the same as the location you specify for the console to use (on the **UNC path** option). The *method* (UNC, Anonymous HTTP, Authenticated HTTP) the target machines use when connecting to the distribution server may be different, but the physical location should be the same.
Credential used by clients to access authenticated locations	This box applies only if **UNC** or **Authenticated HTTP** is specified. Select the credential (the user name and password pair) used by the target machines to access the distribution server. To define a new credential click **New**. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See Defining Credentials for information on how to share a credential.
Test Connection	If you want to test the authentication credentials used to access the distribution server, click **Test Connection**. For HTTP[S] distribution servers, a default content page (default.htm) is needed in the distribution server directory in order for the test to work.

The lower half of the dialog is used to specify how the console will connect to and synchronize with the distribution server.

Field	Description
UNC Path	The Universal Naming Convention (UNC) path name of the repository share on the distribution server. This share must be accessible by the console and is used when **synchronizing the contents of the distribution server** with the patches and/or engines and definition files contained on the console. If you don't remember the exact path you want to specify in the **UNC Path** box, or if you need to create a new folder, click `...` to search for or create the path name.
Credential used by the console to synchronize	Access to a distribution server requires authentication. Select the credential (the domain\user name and password pair) used by the console to authenticate to the distribution server. To define a new credential click **New**. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See **Defining Credentials** for information on how to share a credential. Please note the following: • If the distribution server is being used as the **download source for the definition files**, the credentials of the user currently logged on to the console will be used to connect to the server rather than the credentials you supply here. This means the distribution server UNC path must be accessible by all Security Controls administrator accounts. This also means the server must reside in either the same domain as the console or in a trusted domain that will recognize the integrated credentials. • If you do not specify a credential then by default integrated Windows authentication will be used (the authentication credentials of the person currently logged on to the console machine). • If **automatic synchronization** is being used and there are multiple administrators in your organization using Security Controls, at least one of the administrators must specify their credentials here. If you do not specify a credential AND you are using the **automatic synchronization** feature, you must provide the console machine's LOCAL SYSTEM account with read and write access to the distribution server folder. See **Configuring System Account Permissions** for details.
Test Connection	If you want to test the authentication credentials used to access the distribution server, click **Test Connection**. The credentials cannot be verified if the current session is already connected to the share.
Synchronize with Predictive Patch	This is different than the **automatic synchronization** feature, which enables you to synchronize all engines, definitions, and patches contained on the console. If enabled, those patches that have been downloaded to the console by the **Predictive Patch feature** will be synchronized with (copied to) this distribution server. Product levels are not included in this synchronization. The **Patch Sync** column in the top pane of the **Distribution Servers** tab will indicate if Predictive Patch is enabled for a distribution server. A background task will be created when the synchronization is performed. You can track the progress of the synchronization task using **Event History**.

66. Configuring General Settings for a Security Controls Agent Policy

There are a number of general settings to configure for a Security Controls Agent policy. You must configure these settings before installing the agents on the desired target machines.



Field	Description
Enabled	(Windows-based machines only) Specifies if the agent user interface will be installed. One reason you may not want the **agent client program** installed is if you do not allow Microsoft .NET on your agent machines; the agent client requires the use of Microsoft .NET. If the agent client is not installed, you can use the **stagentctl command-line utility** to control the agent on the target machine.
Perform manual operations	(Windows-based machines only) Enables a user on a target machine to manually initiate an operation such as a patch scan.
Cancel operations	(Windows-based machines only) Enables a user on a target machine to stop an operation that is in progress.
Logging level	Specify the amount of logging you want the agent to perform. The options are: • **Basic**: Records *Error*, *Informational*, and *Warning* message types in the log. This is the default value. • **All**: Records *Error*, *Informational*, *Warning*, and *Verbose* message types in the log. Logging all message types is typically only necessary when performing troubleshooting tasks. The log files will reside on each agent machine in the following location: `C:\ProgramData\LANDESK\Shavlik Protect\Logs`
Maximum log size	Specify the maximum log size. Specifying a very large log size will enable you to record a longer log history but it will of course require more system resources. The default value is 5 MB. If the log file becomes full a new log file is opened and logging will continue. If the second log file becomes full, the first log file is deleted and a new log file will be created. This means there will always be a maximum of two log files on the console.

Field	Description
Check-In interval	Specifies how often the agents will check in (synchronize) with the console. At each check-in the agent refreshes its license, it looks for any policy changes and it determines if a newer version of the agent is available. It also checks if it is assigned a distribution server. If it is assigned a distribution server it will use it to download the latest engine components and data definition files. If it is not assigned to a distribution server then the agent downloads the engines and data files from the Web. If an agent machine is offline when the next check-in interval occurs, the agent will immediately check in when network connectivity is restored. Agent licenses must be refreshed at least once every 45 days or they will expire. • **Minutes:** Use this option if you want the agents to check in more than once a day, or if you don't care what time of day the agents will check in with the console and with the distribution server. Valid values are from 10 - 600 minutes. • **Days**: Use this option to specify the number of days between check-ins. You can also use this option to specify a specific time of day for the check-in (for example, late at night when there is more network bandwidth available). • **Distribute check-ins over (minutes)**: Staggers the exact time the agents will check-in so as not to overtax the console (and the default website or the optional distribution server) with simultaneous requests. The valid range is from 1 - 999. As a general rule, the greater the number of agents, the longer the randomized check-in window should be. Values under 30 minutes are not recommended for large environments. The value should, however, be larger than the check-in interval.
Engine, data, and patch download location	Specifies if a distribution server will be used by the agents when downloading the latest engine components, data definition files, and patches. The agents will look for updated files every time they perform a scan. The available options are: In Linux agent environments, distribution servers can be used to download core files but not patches. **Linux agents use YUM to download any patches that must be deployed**. • **Vendor over Internet:** Specifies that the agents will download the files from the default websites. A distribution server will not be used. • **Distribution Server:** Specifies that a distribution server will be used. You must specify which server(s) to use. • If the agents are being used to deploy custom patches then you must specify the use of a distribution server. This is because there is no download URL for custom patches, meaning the agents cannot pull the custom patches from a vendor and must therefore be able to pull them from one or more distribution servers. **Specific**: You can select the name of an existing distribution server. You must have previously configured one or more distribution servers in order for the names to be pre-populated in this box. For more information see **Configuring Distribution Servers**. • **By Agent IP range**: If you have multiple distribution servers defined for your network, each distribution server is typically assigned to service a particular IP address range. The distribution server used when downloading files to a target machine will be determined by the target machine's IP address. See **Assigning IP Addresses to Servers** for more details. • **Use vendor as backup source**: If the designated distribution server is not available, the agent will download the latest engine components and data files from the default websites.
Bandwidth	Specifies the throttle percentage controls of the available network bandwidth the agent is allowed to use during patch downloads. It allows to configure LAN and WAN/Internet bandwidth limits. 100% indicates that the agent can use the full available bandwidth and it is the default value. Minimum throttling limit that can be set is 1%.

Field	Description
Utilization	
Network	• **Sync with the** Security Controls **Cloud:** Specifies that the agent will have the option to use **Security Controls Cloud** to retrieve the latest agent policy information, enabling it to perform synchronization via the cloud. This check box is only available if your console is registered with Security Controls Cloud. When you click **Save and deploy to agents**, a copy of the agent policy and all necessary components will be written to the Security Controls Cloud service. • **Agent listens for updates on port:** Specifies that the agent will listen to the console for **policy updates or commands**. If an agent's policy is updated, or if it is assigned a different policy, the console will issue a "check in now" command to the agent. The agent will immediately download the new or updated policy from the console. Only agent machines that are online and able to communicate with the console will be able to receive the command. • **Port**: Specifies the port used by the agent on the target machine when communicating with the Security Controls console. The default value is 4155. • **Internet proxy credentials**: If the agent machines must authenticate themselves to a proxy server when accessing the Internet, you must provide the proper credentials to the agents. Select the credential (the domain\username and password pair) used to authenticate the agent to the proxy server. To define a new credential click **New**. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See **Defining Credentials** for information on how to share a credential.
Save and deploy to agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for policy updates, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console. The Agent Policy Editor will be closed.
Cancel	Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A *"Do you want to save your changes?"* prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and deploy to agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

67. Configuring System Account Permissions

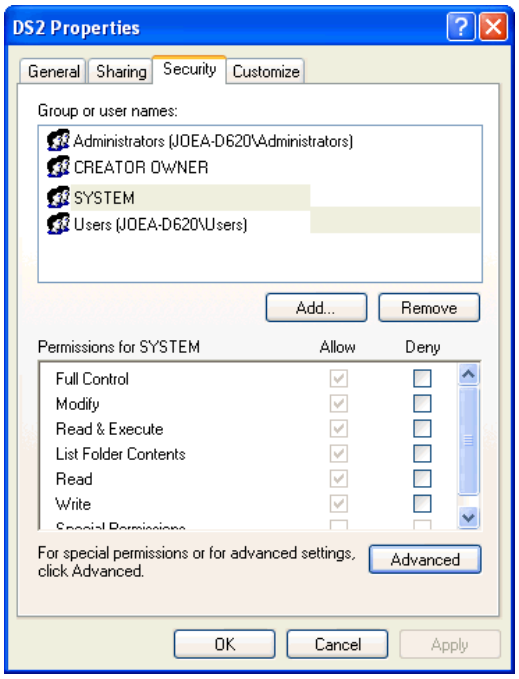
In addition to using the **Distribution Servers dialog** to configure the distribution server within Security Controls, if the following conditions apply you will need to provide the SYSTEM machine account with the proper sharing and security permissions:

- If the distribution server resides on the same machine as the console, the local machine's SYSTEM account must have read and write access to the distribution server folder.
- If an agent will be installed on the distribution server machine, the machine's SYSTEM account must have read access to the distribution server folder.
- If you did not **specify credentials** for the console to use when authenticating to the distribution server AND you are using **automatic synchronization**, the Security Controls console machine's SYSTEM account must have read and write access to the distribution server folder.

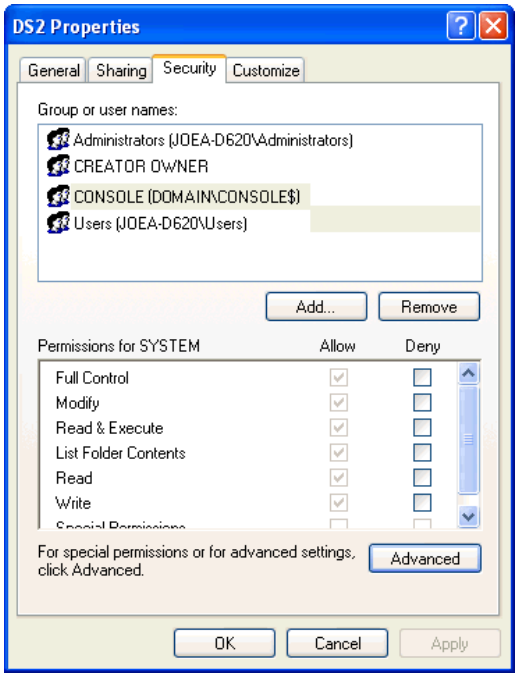
In these three special cases it is the SYSTEM account that is used to access the distribution server and not the credentials supplied on the **Distribution Servers** dialog. If sharing and security permissions are not set, distribution server synchronization errors may occur and/or the local agent may fail to update.

Use Windows Explorer to set the account permissions by right-clicking the distribution server folder, selecting **Properties**, and the clicking the **Sharing** and the **Security** tabs. When setting permissions for the console machine's SYSTEM account (per bullet item #3), you will need to add the console machine's SYSTEM account name to the **Group or user names** list before you can set its permissions. Be sure you specify **Computers** as an object type when adding the name (see Example 2).

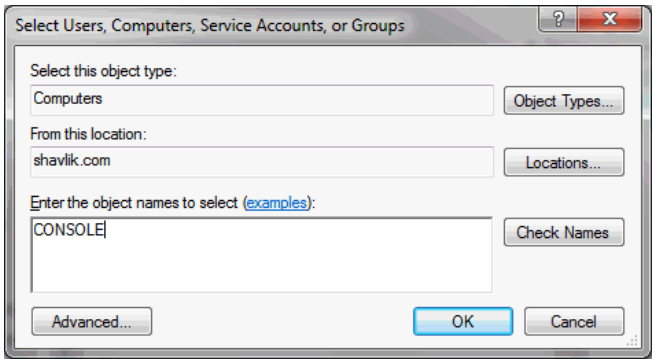
Example 1: Local SYSTEM Account



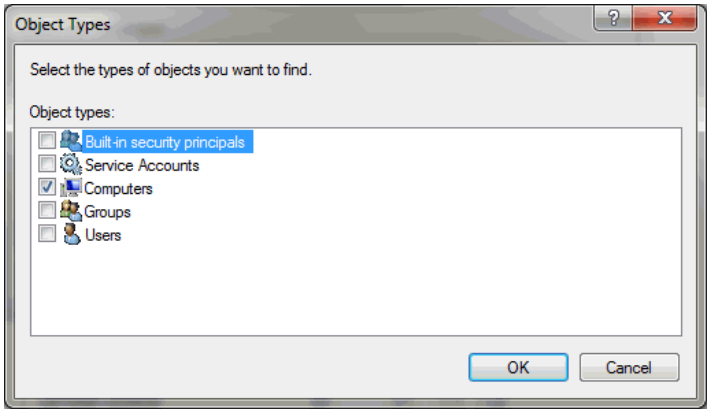
Example 2: Console Machine SYSTEM Account



When adding the console SYSTEM account name...



... verify that **Computers** is enabled on the *Object Types* dialog.



68. Configuring the Central Console in a Disconnected Configuration

I. (Optional) Configure the Data Rollup Service

While this is optional, the recommendation is to use the data rollup feature so that you can track what is happening on each of your remote consoles from one central site.

1. Select **Tools > Options > Data Rollup**.
2. Enable the **Accept and import results from a rollup sender** check box.

II. Set Up a Distribution Server

You must set up a distribution server that the remote consoles can access. The central console will download required files to the distribution server and the remote consoles will download these same files from the distribution server.

See **Configuring Distribution Servers** for detailed information on configuring a distribution server.

III. Update the Distribution Server with the Latest Files

You must first download the latest engine components, data definition files and patches from the Web to the central console's patch download directory.

1. Download the patches that have been approved by your organization.
   See **Downloading Patches** for detailed information on downloading patches.
2. Download the latest engines and data files by selecting **Help > Refresh Files.**

Copy the engines, data files and patches from the central console to the distribution server by synchronizing the central console with the distribution server. For information on this, see **Synchronizing Servers**.

You can also configure Security Controls to automatically download the latest engines and data files and synchronize all your distribution servers. See **Synchronizing Servers** for details.

69. Configuring the Remote Consoles in a Disconnected Configuration

Here are the major steps you must perform when configuring each remote console in a disconnected console configuration.

> For information on how to activate a console in a disconnected environment, see **Activating Security Controls**.

I. (Optional) Configure the Data Rollup Service

While this is optional, the recommendation is to use the data rollup feature so that you can track what is happening on each of your remote consoles from one central site. To implement data rollup, you must configure each remote console so that it rolls up its results to the central console.

1. Select **Tools > Options > Data Rollup**.
2. Enable the **Enable Data Rollup** check box.
3. Specify the IP address/hostname and port number used by the rollup console.
4. In the **Minutes between sending console's results** box, specify how often the data will be rolled up from the remote console to the central console.
   The default value is every 240 minutes (four hours).
5. Click **Register**.

II. Set Up a Distribution Server

You must set up a distribution server that each remote console can access. The remote consoles will download all necessary files (such as patch files, engine components and data definition files) from the distribution server. The distribution server should be the same distribution server you set up on the central console.

See **Configuring Distribution Servers** for detailed information.

III. Create a Machine Group of the Machines at This Site

1. From the main menu select **New > Machine Group** and name the group **All Machines** (or something similar).
2. Add all the machines that are managed by the remote console.

IV. Specify Where to Download Files

Configure the remote console so that prior to a scan it will automatically download the latest files from the distribution server.

1. Select **Tools > Options > Downloads**.
2. In the **Definition download source** area, specify the appropriate distribution server to use when downloading the latest engine components and data files.
3. In the **Patch and product level download source** area, specify the appropriate distribution server to use when downloading the patches and product levels.

V. Create a Patch Scan Template

1. From the main menu select **New > Windows Patch > Patch Scan Template**.
2. Configure the patch scan template as desired.

See Creating a New Patch Scan Template for details.

> If you want to scan for a particular set of patches in an unattended console configuration, see Implementing an Unattended Console Configuration for more information.

VI. Create a New Favorite and Schedule a Periodic Scan

Create a favorite containing the machine group and the scan template you created earlier and then use the favorite to schedule a scan.

1. From the main menu select **New > Favorite**.
2. In the **Select at least 1 group** list, select the new machine group you created earlier.
3. In the **Template** box, select the patch scan template you created earlier.
4. Click **Run operation**.
5. On the **Run Operation** dialog, schedule the recurring patch scan.

When you schedule the patch scan make sure you:

- Select the patch scan template you created in Step V
- Enable the**Auto-deploy patches after scan**check box
- Specify what deployment template to use and when the deployment should occur

70. Console Software and Hardware Recommendations

Recommended Operating Systems

We recommend using one of the more current Windows Server operating systems.

- Windows Server 2019 Family, excluding Server Core and Nano Server
- Windows Server 2016 Family, excluding Server Core and Nano Server

Prerequisites

- Recommend Microsoft SQL Server 2016 SP1 or later
- Microsoft .NET Framework 4.7.2 or later
- Microsoft Visual C++ Redistributable for Visual Studio 2017
- Windows Management Framework 5.1 (contains the Windows PowerShell component, which is required for the ITScripts feature): This prerequisite does not apply to Windows 8.1 or later and Windows Server 2012 R2 or later, as the PowerShell component is already included with these operating systems.

If you are missing any prerequisites, plan on 30 - 60 minutes of installation time depending on the number of missing prerequisites and on your internet speed.

Physical Machine vs. Virtual Machine Considerations

The requirements for installing Security Controls on a virtual machine are the same as for a physical machine. You should have a minimum of 4GB hard disk space for the patch repository and an additional 2GB for each operating system you support. For each additional language you support, add 4GB. If you use the **Predictive Patch feature**, which downloads patches in advance of their anticipated deployment, you should have at least 10GB of available space.

Recommended Console Machine Resources

1 - 250 Seats

- **Processor:** 2 processor cores 2 GHZ or faster
- **Memory:** Minimum 2 GB RAM (recommended 3+ GB RAM if SQL is local)
- **Database:** Microsoft SQL Server 2016 or later

251 - 1000 Seats

- **Processor:** 4 processor cores 2 GHZ or faster
- **Memory:** 4 GB RAM
- **Database:** Microsoft SQL Server 2016 or later

1001+ Seats

- **Processor:** 8 processor cores 2 GHZ or faster
- **Memory:** 8 GB RAM
- **Database:** Microsoft SQL Server 2016 or later

To determine an approximate size for your SQL Server database, use this formula:

> 30KB * machine count * patch operations/month * number of months to retain data * 2 (for index and logging)

Using this formula, if you have 5,000 machines, perform 12 patch operations per month and you retain data for 3 months, your estimated SQL Server database size is:

> 30 * 5000 * 12 * 3 * 2 = 10.8 GB

To increase performance on any of the configurations, increase the number of processors, the amount of installed memory and the database size.

Related Topics

- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

71. Assigning Aliases to the Console

WARNING! Accidentally changing or deleting existing entries on the **Console Alias Editor** dialog may cause problems when your agents attempt to contact the console or when your agentless machines attempt to report deployment status messages. Only qualified system administrators should modify existing names or IP addresses.

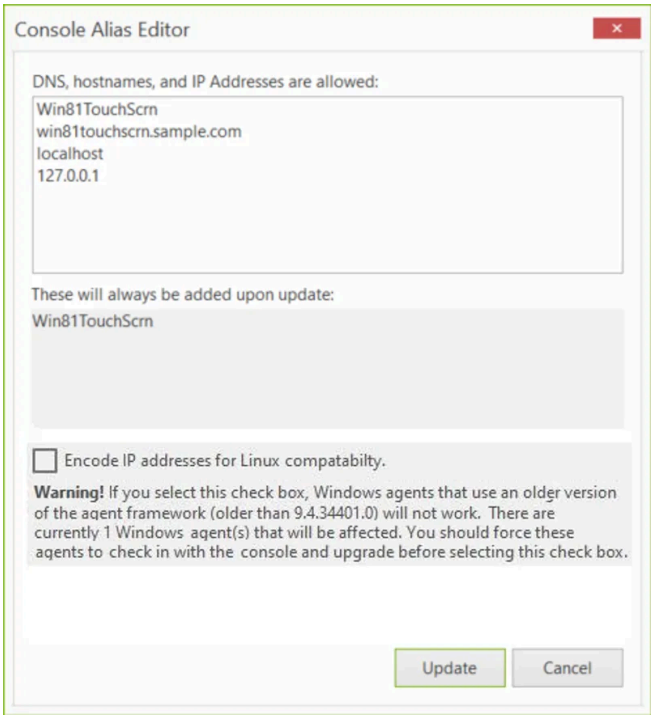
TIP: The most common time to use this tool will be during an upgrade from an earlier version of Security Controls.

There are two primary uses for the **Console Alias Editor** tool.

- **Agent communication:** When an agent communicates with the Security Controls console (for example to check in or as part of its installation) it must verify that the machine it contacted is a trusted machine. It does this using the trusted names and IP addresses contained in the certificate that is exchanged between the agent and the console to establish a secure TLS connection. If you assign the console machine to a new domain or give it a new common name or IP address, any existing agents that recognize the console by its old name or address will no longer trust the console machine. To get around this issue you simply identify the old console names or addresses as trusted aliases. This is done using the **Console Alias Editor** tool.
- **Patch deployment pingback:** Patch deployments to your agentless machines can be monitored using the Security Controls Deployment Tracker. In order for your agentless machines to send status messages to the console they need to know the valid name or IP address of the console. The valid names and IP addresses are defined using the **Console Alias Editor** and are passed to the machines when a patch deployment is initiated from the console.

This menu command is not available to users assigned the Report Only role.

1. Select **Tools > Console alias editor**.
   The **Console Alias Editor** dialog is displayed. It will contain the names and IP addresses currently used to identify the console machine.

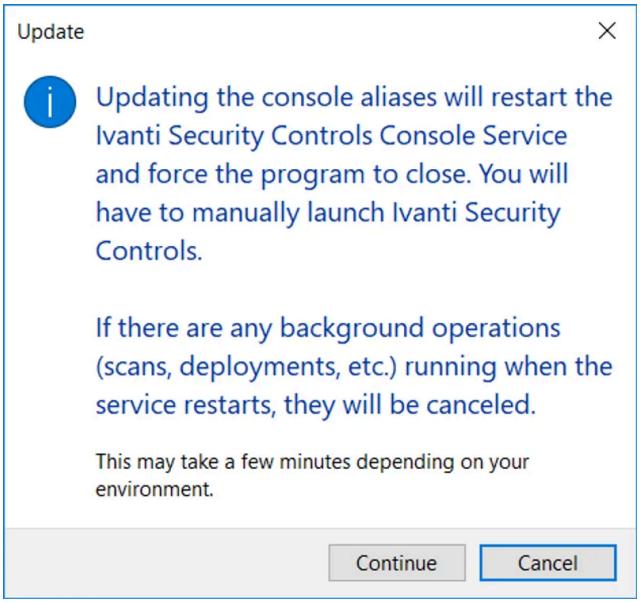


Type the name or IP address that you want to use as an alias for the console machine.
You can specify IP addresses using either an IPv4 or IPv6 format.

3. Determine if you want IP address aliases to function with Linux agents.
   If you enable the check box, any IP address aliases that you specify will be encoded within the console certificate. This is required in order for the IP alias to be honored by Linux agents.

Warning! If you have Windows agents with an older version of the agent framework, they may not work after you enable this check box. You should force those agents to check in with the console and upgrade before enabling the check box. Use the **Agent version** column in **Machine View** to determine which agents are out of date.

Click **Update**.
The **Update** dialog is displayed.



In order to update the console aliases the console service must be restarted and Security Controls must be closed and then manually restarted.

The agents will not recognize a new alias until after they check-in with the restarted console. The check-in must be initiated by an agent either manually using the **agent client program** or **via a scheduled check-in**.

A **check-in command issued from the console** to an agent will not update the console certificate.

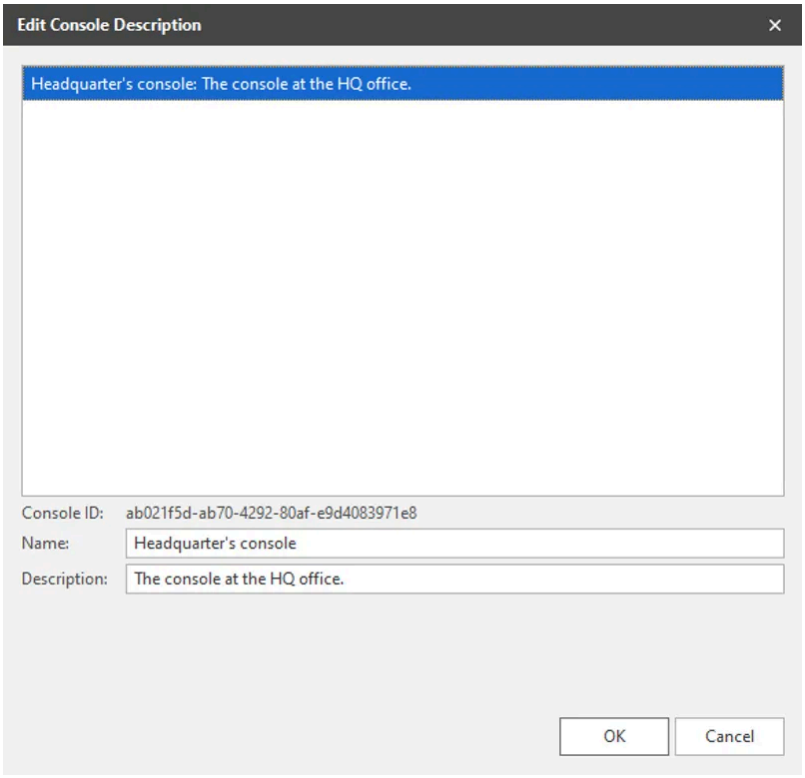
72. Editing the Console Description

You can change the name the program uses when referring to the console. This serves two purposes:

- It enables you to assign a user-friendly name to use for all references to the console. By default the name used is the console's computer name. If there is only one console then the default name may be fine. But in some cases the default name may not have much meaning to you and you'll want to change the name.
- It helps avoid confusion if the console is on a remote server or if two or more consoles are being used.

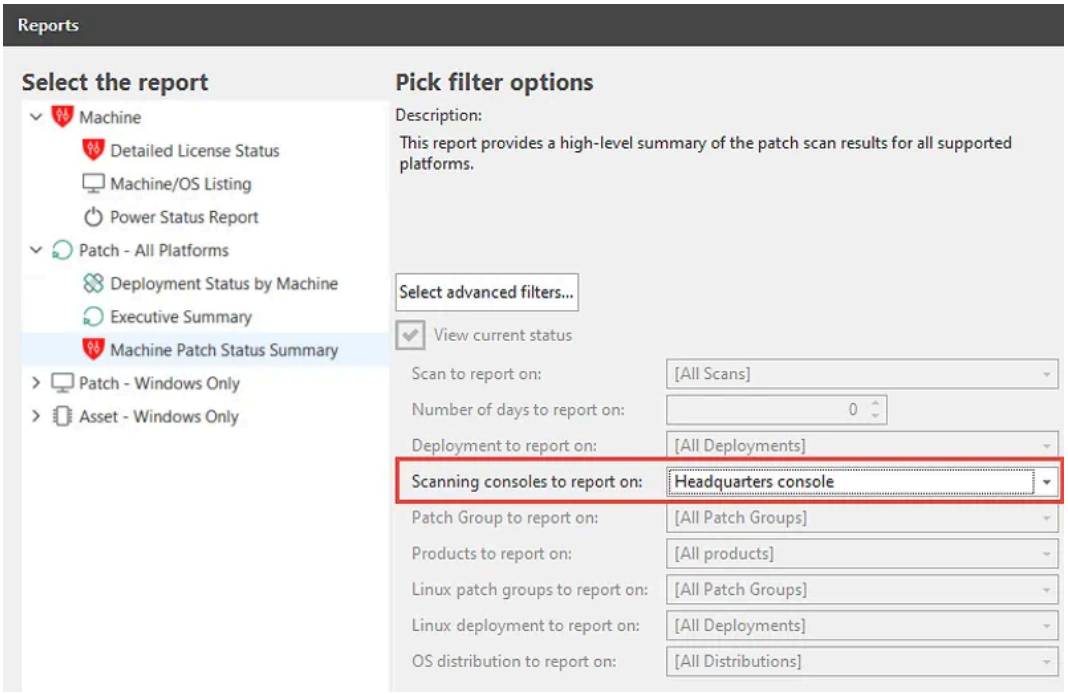
To edit the console name:

1. Select **Tools > Edit console description**.
2. A dialog similar to the following is displayed.



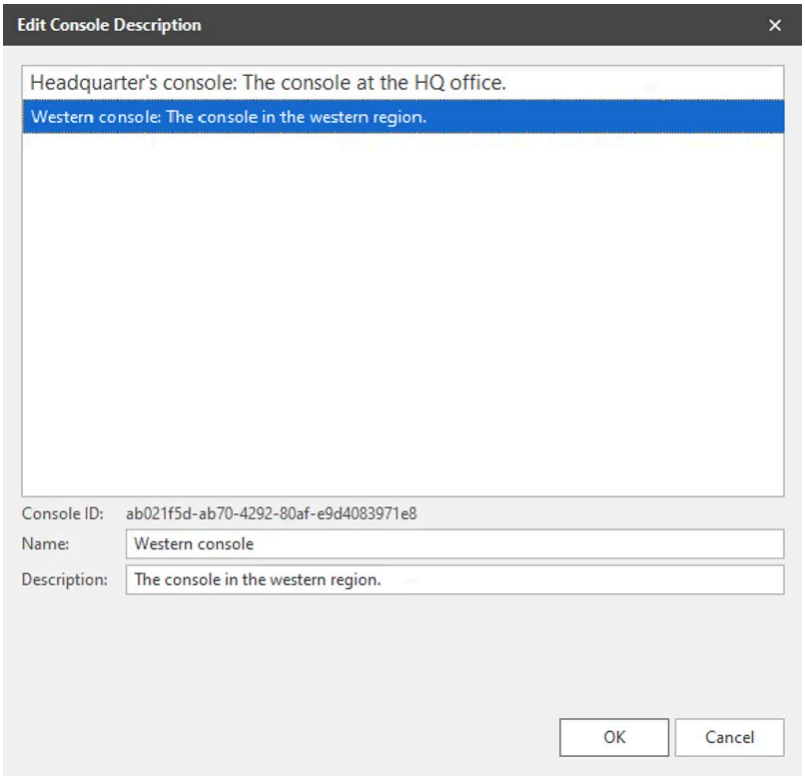
> **Tip:** The **Edit Console Description** dialog displays the console ID, which can be a helpful piece of information if you need to perform some troubleshooting.

Change the name and description as desired.
The program will use the new, friendly name whenever it refers to the console. The new name will be used in any reports you generate for the console. For example, if you changed the name to "Headquarters console" you would see the following:



For Data Rollup Configurations

This feature is particularly useful in data rollup configurations (see **What is a Data Rollup Configuration**), where the central console receives results that are rolled up to it from other remote consoles. An entry is automatically generated in the central console's **Edit Console Description** dialog whenever a remote console imports the central console's data rollup settings. Once an entry is generated, its name and description can be modified, if desired.



73. Continuous Agentless Scanning

On the **Tools > Options > Scan** tab, the **Enable continuous agentless scanning** option should only be used in certain circumstances. Specifically, this option is designed for use in conjunction with Network Access Control (NAC) environments that perform patch security checks on all machines before they are allowed onto the local network. In this scenario, if a machine does not contain all of the required patches, the access control system will place it into a restricted network. The machine remains in this "quarantine" until the necessary security patches are deployed to the machine, at which time it can be reintroduced to the primary network.

If you select **Enable continuous agentless scanning**, a **Minutes scan interval** option becomes available when scheduling recurring patch scans. This enables you to schedule scans on a minute basis, providing nearly continuous patch scans and deployments of the machines that reside within the restricted network. By performing scans at minute-based intervals rather than daily intervals, the amount of time a deficient machine stays in the restricted network is greatly decreased.

The **Enable continuous agentless scanning** option is only recommended for use in this very specific circumstance. The constant scanning is fine for monitoring a small number of devices in an isolated or restricted network, but it is not recommended for general use. The extremely short scan intervals can wreak havoc on your network performance if configured for large networks.

> If you use the **Minutes scan interval** option, the amount of patch scan data that is contained in your database can quickly grow out of hand. Be sure to use the Database Maintenance tool to continually delete old results.

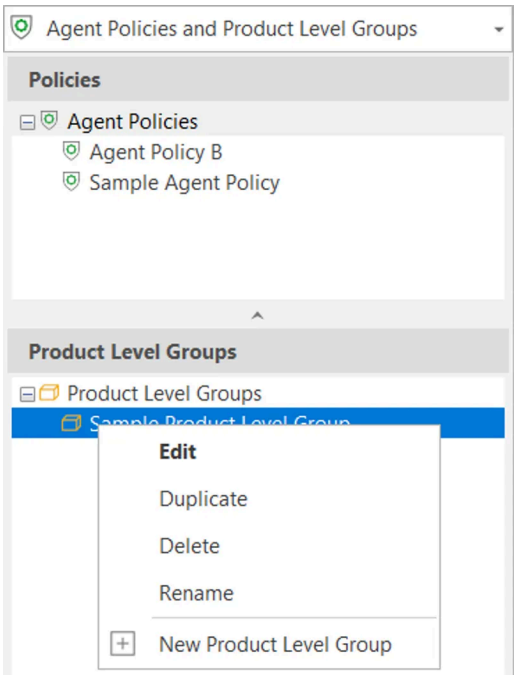
Related Topics

- Scan Options
- Scheduling Patch Scans

74. Copy, Delete or Rename a Product Level Group

To copy, delete, or rename an existing product level group:

1. In the navigation pane select **Agent Policies and Product Level Groups**.
2. Right-click an existing product level group and then select the desired menu item.



75. Creating and Editing a Linux Patch Deployment Configuration

A Linux patch deployment configuration defines how a patch deployment will be performed. There are separate Patch Deployment Configurations for the new contentless Linux patching method and the previous content-based patching method. The new contentless patching method performs a scan for all missing patches as a part of all Patch Deployment Configurations.

Security Controls provides one predefined configuration named **Update All**. This configuration specifies that the agent will deploy all patches that were identified as missing by a **patch scan**. A patch group will not be used and a post-deploy reboot will not be performed.

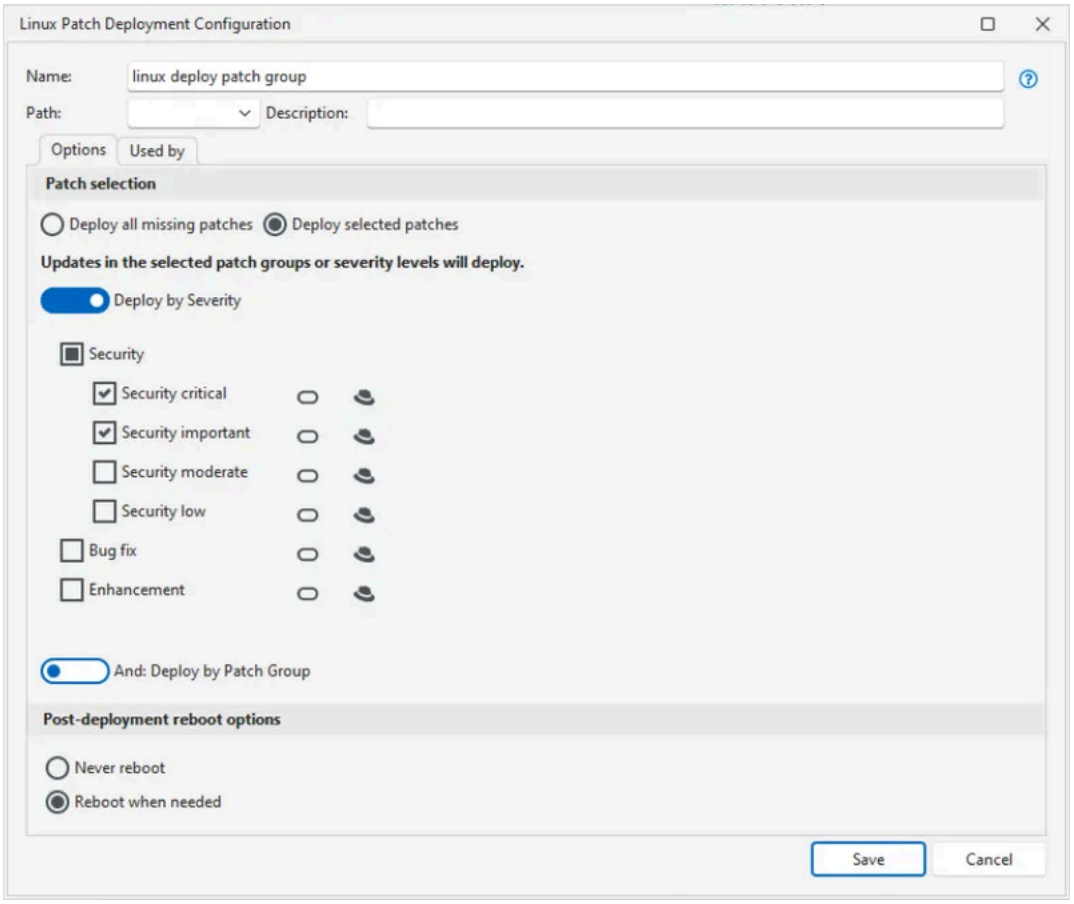
You cannot edit the predefined configuration. If the predefined configuration is not adequate for your needs, you can create a custom configuration, as described separately below for contentless patching and content-based patching.

Contentless patching

To work with a custom contentless Linux patch deployment configuration, do one of the following:

- To create a new deployment configuration:
  - Click **New > Linux Patch > Patch Deployment Configuration**
  - In the **Linux Patch Deployment Configurations** list ( ) in the navigation pane, right-click and select **New Linux Patch Deployment Configuration**

To edit an existing configuration, in the **Linux Patch Deployment Configurations** list, double-click the deployment configuration name



Field	Descriptions
Name	The name that you wish to assign to this configuration.
Path	This box is used to specify the folder path that this configuration will reside in within the **Linux Patch Deployment Configurations** list in navigation pane. If you do not specify a path, the configuration will reside at the root level of the **My Linux Patch Deployment Configurations** list. For more details, see Organizing Linux Patch Groups and Configurations.
Description	A description of the configuration.
Deploy all missing patches	If enabled, all patches that were identified as missing by the scan that is run as part of the deployment will be deployed.
Deploy selected patches	If enabled, only those patches that were identified as missing by the scan that is run as part of the deployment and that match the configured criteria will be deployed. • **Deploy by Severity**: If enabled, allows you to specify the types of patches and the severity levels that you want to include in a deployment. Icons show which Linux distributions support each level. ◦ **Security**: Security bulletin-related patches. You can choose to deploy one or more specific severity levels. ▪ **Security critical**: Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. ▪ **Security important**: Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. ▪ **Security moderate**: Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important

Field	Descriptions
	impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. ▪ **Security low**: All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact. ◦ **Bug fix**: Vendor patches that fix bugs. ◦ **Enhancement**: Vendor patches that provide feature enhancements. • **Deploy by Patch Group**: If enabled, allows you to specify one or more patch groups that contain the patches that you want to include in a deployment. This is a good way to make sure that only approved patches are deployed. Missing patches not contained in selected patch groups will not be deployed unless they meet the requirement specified in the **Deploy by Severity** option. Security Controls follows the convention in patching Linux devices by always updating to the latest package available in the repository, even if an earlier version is selected. Note that for some distributions this is actually the only option available, as earlier versions of a package are not available from the repository.
Post-deployment reboot options	Enables you to specify whether or not to allow post-deployment reboots. You specify settings for reboot countdowns and so on in the **Server/Linux patch** section of the **Agent Reboot Options** tab on the Agent Policy Editor dialog (see Agent Reboot Options). If you select **Deploy selected patches**, packages that are dependencies for the specified advisories are installed in addition to the packages associated with the advisories in the patch groups. If you then set **Post-deployment reboot options** to **Reboot when needed**, these dependencies may additionally cause a reboot. Remember that some updates require a reboot and that in these instances a machine is vulnerable until it reboots, so we recommend **Never reboot** only for servers with scheduled maintenance windows.
Used by tab	This tab shows you the agent policies that are currently using this configuration. This is important to know if you are considering modifying the configuration, as it tells you which agents are affected.

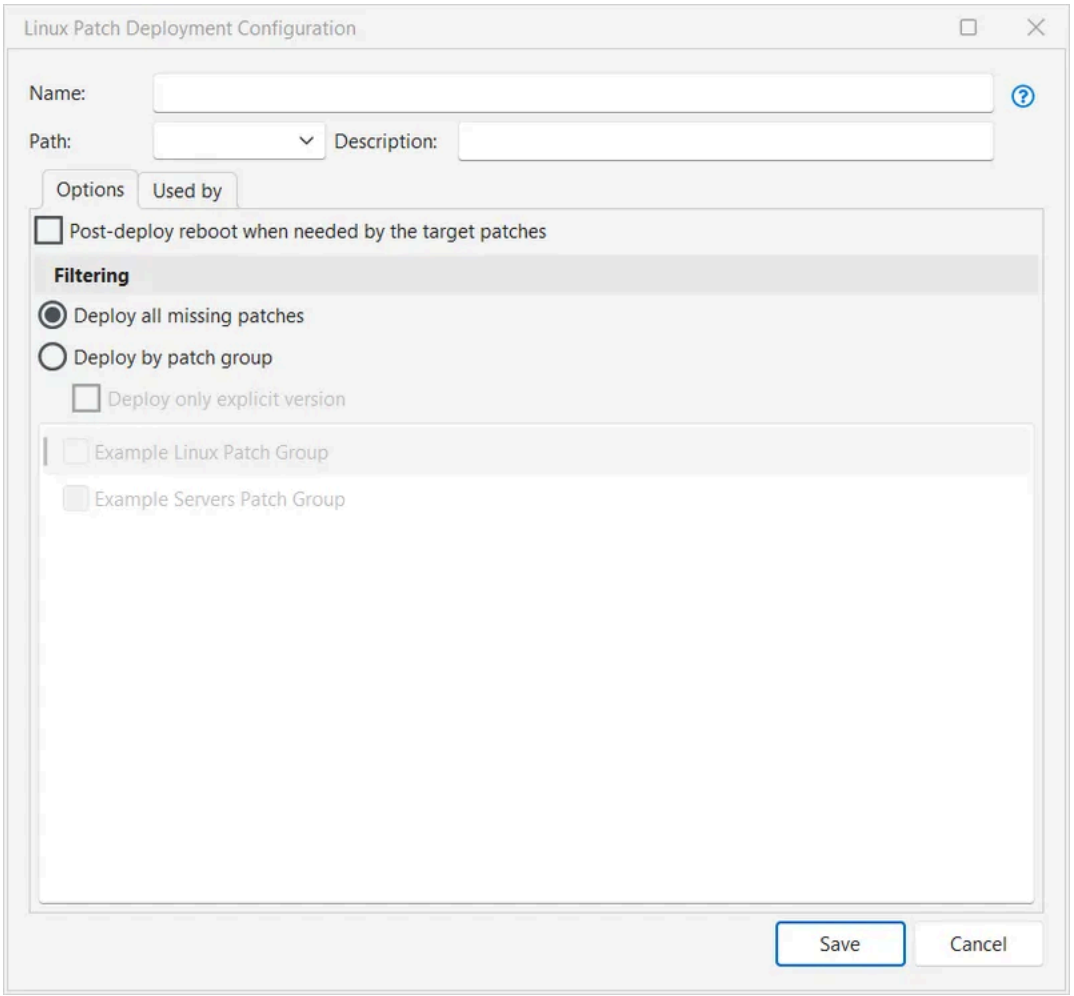
If an Oracle Linux machine has both the Red Hat Compatible Kernel (RHCK) and the Unbreakable Enterprise Kernel (UEK), both kernels are scanned and patched. However, because the non-running kernel is not running and so is not vulnerable, its advisories are always reported as Installed.

Content-based patching

To work with a custom content-based Linux patch deployment configuration, do one of the following:

- To create a new deployment configuration:
  - Click **New > Linux Patch (Content-Based) > Patch Deployment Configuration (Content-Based)**
  - In the **Linux Patch Deployment Configurations (Content-Based)** list ( ) in the navigation pane, right-click and select **New Linux Patch Deployment Configuration**

To edit an existing configuration, in the **Linux Patch Deployment Configurations** list, double-click the deployment configuration name



Field	Descriptions
Name	The name that you wish to assign to this configuration.
Path	This box is used to specify the folder path that this configuration will reside in within the **Linux Patch Deployment Configurations** list in navigation pane. If you do not specify a path, the configuration will reside at the root level of the **My Linux Patch Deployment Configurations** list. For more details, see Organizing Linux Patch Groups and Configurations.
Description	A description of the configuration.
Post-deploy reboot when needed by the target patches	If enabled, specifies that Security Controls will review the patches being deployed and determine whether or not a reboot is required. If you do not enable this option, a reboot will not be performed after deployment. You specify settings for reboot countdowns and so on in the **Server/Linux patch** section of the **Agent Reboot Options** tab on the Agent Policy Editor dialog (see Agent Reboot Options).
Deploy all missing patches	If enabled, all patches that were identified as missing by a patch scan will be deployed.
Deploy by patch group	If enabled, only those patches that were identified as missing by a patch scan and that are contained within the specified Linux patch groups will be deployed.
Deploy only explicit version	If enabled, only the explicit version of the patch that was detected as missing will be deployed. If a newer version of the patch is available it will not be deployed.
Used by tab	This tab shows you the agent policies that are currently using this configuration. This is important to know if you are considering modifying the configuration, as it tells you which agents are affected.

Deployments are Performed Using YUM

Yellowdog Updater, Modified (YUM) is a command-line utility that is used for retrieving, installing and managing RPM packages from official Red Hat and CentOS software repositories. When an agent needs to deploy a patch, it does so by instructing YUM to download and install the patch. If you have Linux client machines that reside in a disconnected network, the agent will not be able to utilize YUM and you must **set up one or more local repositories**.

76. Creating and Editing a Linux Patch Scan Configuration (content-based only)

A Linux patch scan configuration defines how a patch scan will be performed for the content-based method. Security Controls provides two predefined configurations for content-based patch scanning.

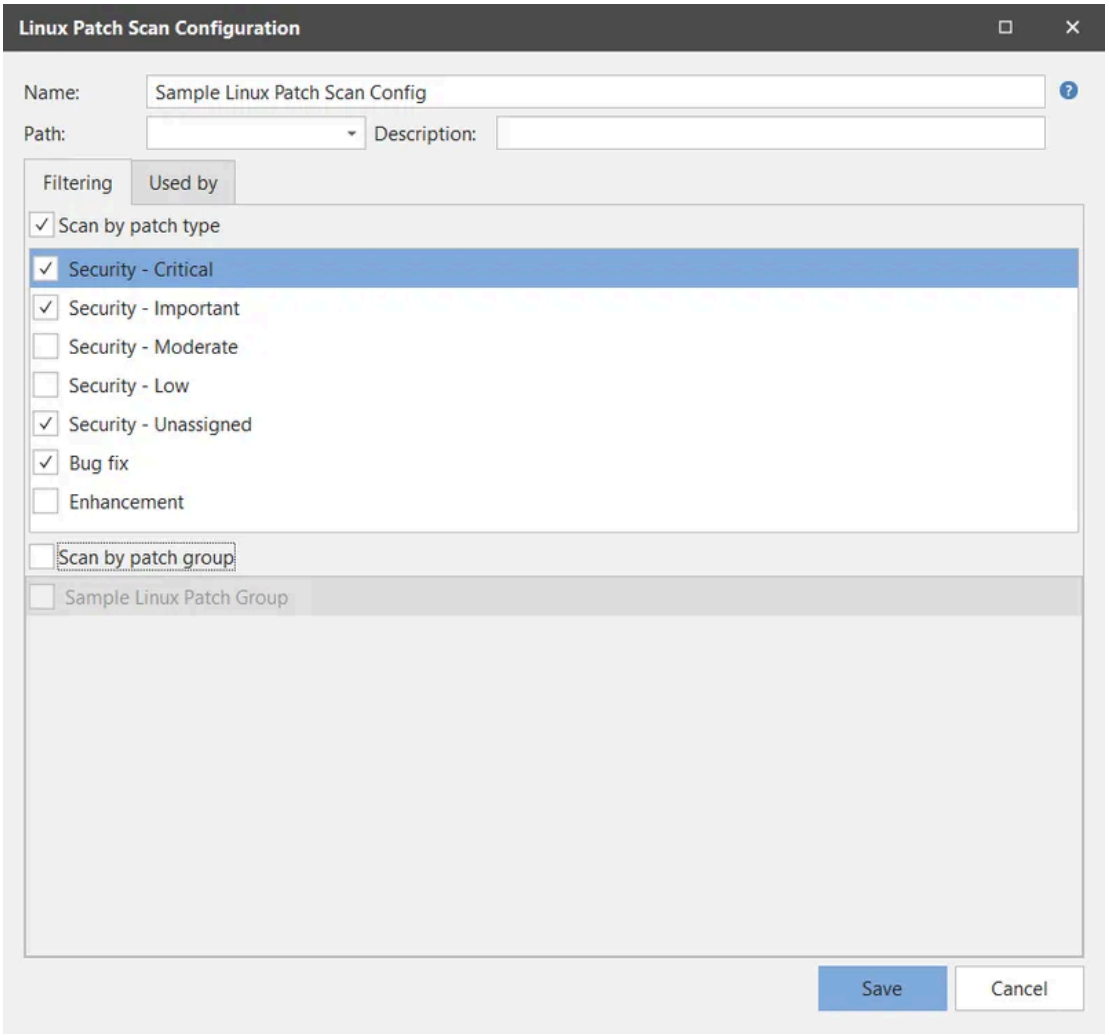
- **All Patches**: Specifies that the agent will scan for all patch types. A patch group will not be used.
- **Security Patches**: Specifies that the agent will scan for only security patches. The agent will not scan for bug fixes or enhancements, and a patch group will not be used.

> For contentless patching Linux machines, a scan for all missing patches is included in all Linux Patch Tasks, so there is no separate patch scan.

You cannot edit the predefined configurations. If the predefined configurations are not adequate for your needs, you can create a custom configuration.

To work with a custom Linux patch scan configuration, do one of the following:

- To create a new patch scan configuration, click **New > Linux Patch (Content-Based) > Patch Scan Configuration**.
- To edit an existing patch scan configuration, in the **Linux Patch Configurations (Content-Based)** list, double-click the configuration name.


Linux Patch Scan Configuration
Name:
Sample Linux Patch Scan Config
Path:
Description:
Filtering
Used by
Scan by patch type
Security - Critical
Security - Important
Security - Moderate
Security - Low
Security - Unassigned
Bug fix
Enhancement
Scan by patch group
Sample Linux Patch Group
Save
Cancel

Field	Descriptions
Name	The name that you wish to assign to this configuration.
Path	This box is used to specify the folder path that this configuration will reside in within the **Linux Patch Scan Configurations** list in navigation pane. If you do not specify a path, the configuration will reside at the root level of the **My Linux Patch Scan Configurations** list. For more details, see Organizing Linux Patch Groups and Configurations.
Description	A description of the configuration.
Filtering tab	There are two different options available on this tab: **Scan by patch type** and **Scan by patch group**. You can select one or both options. • **Scan by patch type:** Specify the types of patches and the vendor severity level of those patches that should be included in the scan. The patch type options are: ◦ **Security**: Security bulletin related patches. You can choose to scan for one or more specific severity levels. ▪ **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. ▪ **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. ▪ **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. ▪ **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact. ▪ **Unassigned:** Security patches that have not been assigned a severity level. **Bug fix:** Patches that fix known bugs. ◦ **Enhancement:** Patches that provide product enhancements. **Scan by patch group:** Specify one or more Linux patch groups that contain the patches you want to use as a baseline.
Used By tab	This tab shows you the agent policies that are currently using this configuration. This is important to know if you are considering modifying the configuration, as it tells you which agents are affected.

77. Creating and Editing a Linux Patch Group

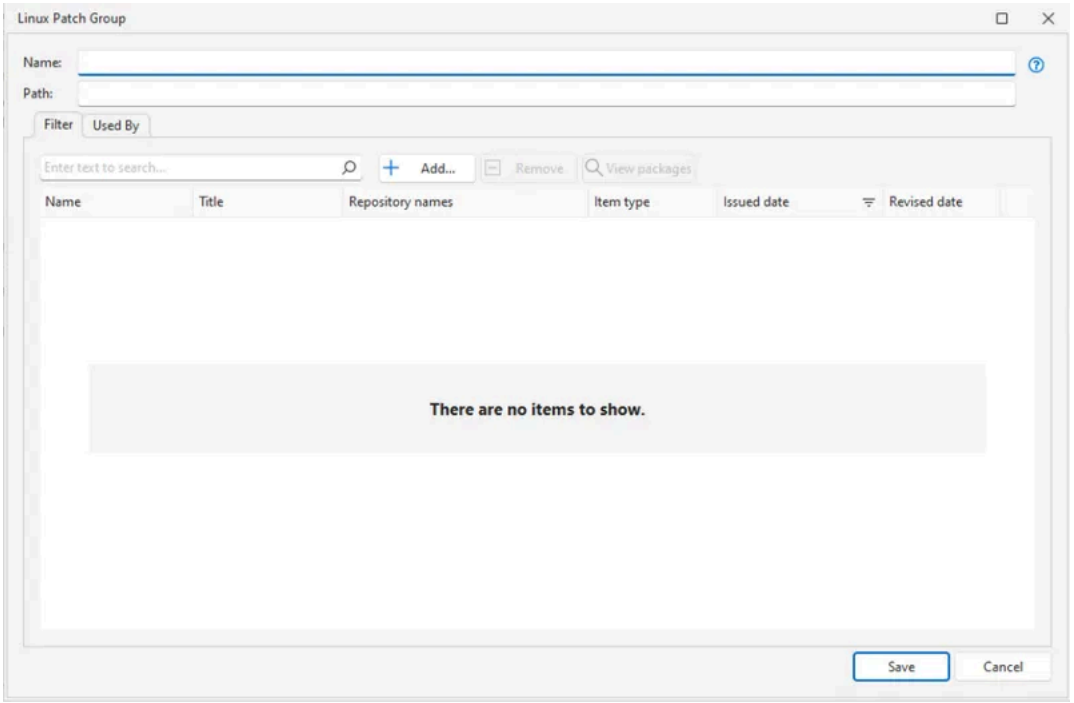
Security Controls provides the ability to use a patch group to scan for (content-based only) or deploy a particular set of updates. There are multiple ways to create or edit Linux patch groups for both contentless patching and content-based patching:

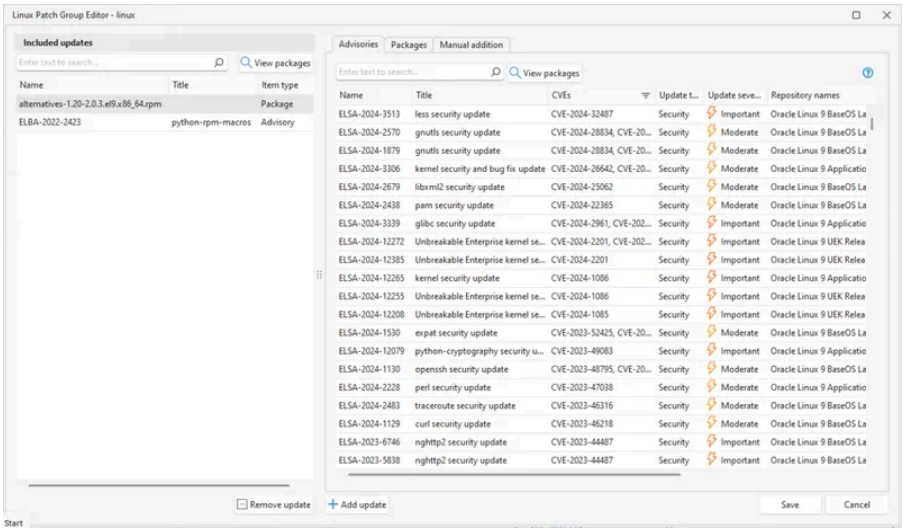
Contentless patching

- To create a new patch group:
  - Click **New > Linux Patch > Patch Group**
  - In the **Linux Patch Groups** list in the navigation pane, right-click and select **New Linux Patch Group**

To edit an existing group, in the **Linux Patch Groups** list under **Linux Patching** in the navigation pane, double-click the patch group name.

> Be careful when editing an existing patch group. Any modifications you make will affect any Linux scan or deployment configuration that references the patch group. Also, if you edit and save a patch group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.



Field	Descriptions
Name	The name that you wish to assign to this patch group.
Path	This box is used to specify the folder path that this patch group will reside in within the **Linux Patch Groups** list in navigation pane. If you do not specify a path, the patch group will reside at the root level of the list. For more details, see Organizing Linux Patch Groups and Configurations.
Filter tab	The **Filter** tab lists the contents of the patch group, providing filters and a search control to help you to find details about specific items in the group. There are three different actions you can perform on this tab: **Add**, **Remove** and **View packages**. • **Add:** Enables you to add one or more updates using the **Linux Patch Group Editor** by selecting the updates and click **Add Update**, or drag and drop the selected updates to the **Included updates** window.  The pane on the left of the dialog shows the updates that have been added to the patch group. The pane on the right enables you to select updates to add to the patch group: ◦ The **Advisories** tab shows advisories that have been discovered on your target machines ◦ The **Packages** tab shows packages that have been discovered on your target machines ◦ The **Manual addition** tab enables you to enter the ID of a specific package or advisory, including those that do not appear in the other tabs **To add advisories from the Advisories tab or packages from the Packages tab:** 1. Use the column headers and filters to group or further refine the information in the grid. 2. Use the search box to locate specific items in the grid. Select one or more items in the grid and then click **Add update**. The updates are added to the **Included updates** list. **To add advisories or packages from the Manual addition tab:** 1. In the **Type** list, select **Advisory** or **Package** as required. 2. In the **Enter identifier** field, type the ID of the advisory or package.

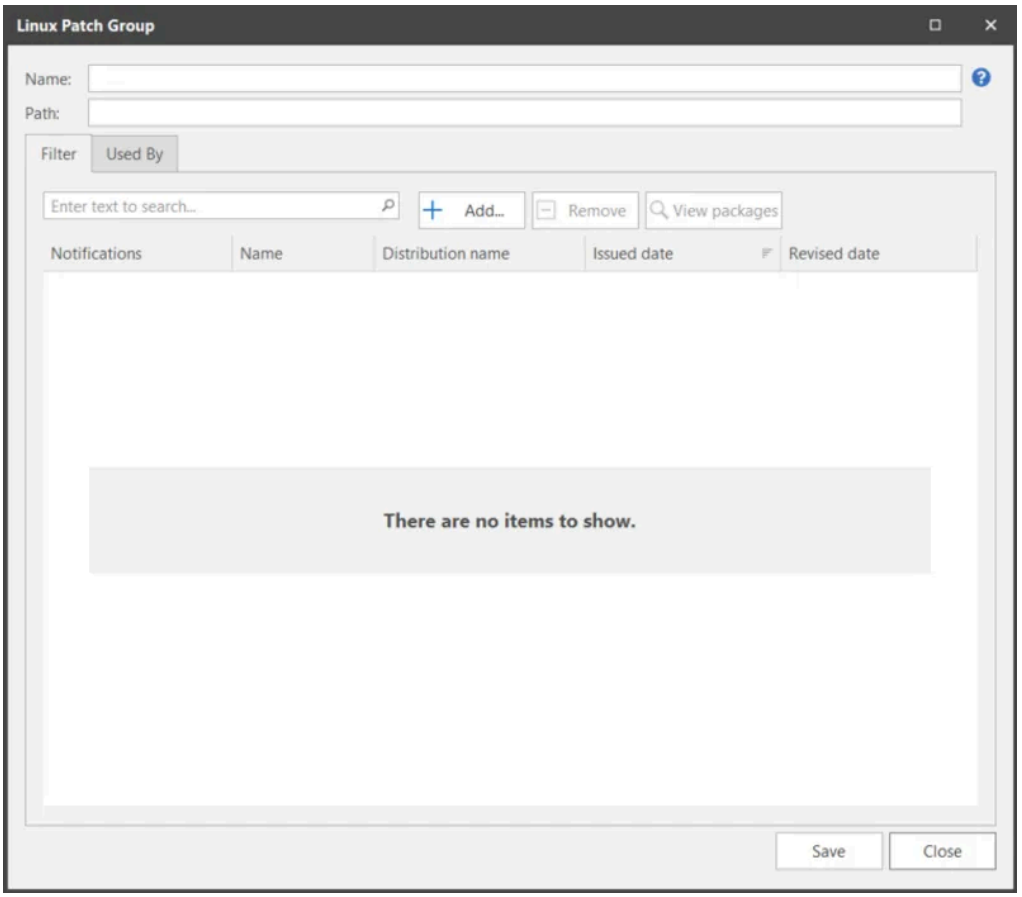
Field	Descriptions
	3. Click **Add update**. The update is added to the **Included updates** list. If the identifier you enter matches a package found in the patch scan metadata, then when you save the changes and close the editor, additional information including the associated repository names appear in the Patch Group dialog. • You can combine updates for different distributions in the same group. You may choose to create separate patch groups for the different distributions, and if you do, you should use the **Path** box to organize the groups. **Remove:** To remove one or more updates from either the **Linux Patch Group** or the **Linux Patch Group Editor** dialog, select the desired updates and then click **Remove update**. • **View packages:** To view the packages that are affected by the updates contained in either the **Linux Patch Group** or the **Linux Patch Group Editor** dialog, select the desired updates and then click **View packages**. A single update may update one or more packages. The packages listed in the **Package view** for a specific advisory may differ depending on the context of which machine you viewed it from. For more information, see Viewing Details of Linux Packages.
Used By tab	This tab shows you the agent policies that are currently using this patch group. This is important to know if you are considering modifying the patch group, as it tells you which agents are affected.
How to delete a patch group	Patch groups can be deleted from the Linux Patch Groups list using the right-click menu.

Content-based patching

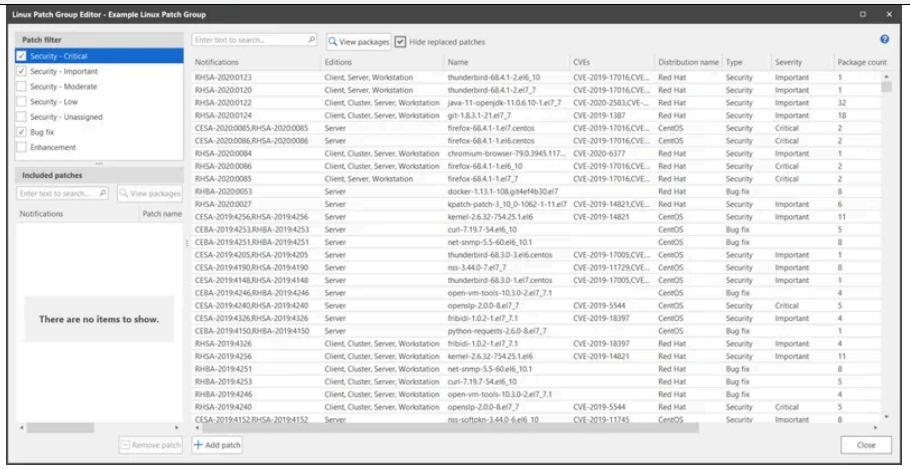
- To create a new patch group:
  - Click **New > Linux Patch (Content-Based) > Patch Group (Content-Based)**
  - In the **Linux Patch Groups (Content-Based)** list in the navigation pane, right-click and select **New Linux Patch Group**

To edit an existing group, in the **Linux Patch Groups** list under **Linux Patching (Content-Based)** in the navigation pane, double-click the patch group name.

> Be careful when editing an existing patch group. Any modifications you make will affect any Linux scan or deployment configuration that references the patch group. Also, if you edit and save a patch group that is currently being used by an **agent policy**, the agents using that policy will be updated the next time they check in with the console.



Field	Descriptions
Name	The name that you wish to assign to this patch group.
Path	This box is used to specify the folder path that this patch group will reside in within the **Linux Patch Groups** list in navigation pane. If you do not specify a path, the patch group will reside at the root level of the list. For more details, see **Organizing Linux Patch Groups and Configurations**.
Filter tab	There are three different actions you can perform on this tab: **Add**, **Remove** and **View packages**. • **Add:** Enables you to add one or more patches using the **Linux Patch Group Editor**.

Field	Descriptions
	 Use the **Patch filter** pane to narrow the list of patches presented in the grid on the right. You can then use the column headers and filters to further refine the information in the grid. Finally, you can use the search box to locate specific items in the grid. To add one or more patches to the group, select them in the grid and then click **Add patch**. The patches will be added to the **Included patches** list. The program will allow you to combine CentOS and Red Hat patches in the same group. You may choose to create separate CentOS and Red Hat patch groups, and if you do, you should use the **Path** box to organize the groups. **Remove:** To remove one or more patches from either the **Linux Patch Group** or the **Linux Patch Group Editor** dialog, select the desired patches and then click **Remove patch**. • **View packages:** To view the packages that are affected by the patches contained in either the **Linux Patch Group** or the **Linux Patch Group Editor** dialog, select the desired patches and then click **View packages**. A single patch may update one or more packages. The packages listed in the **Package view** for a specific advisory may differ depending on the context of which machine you viewed it from. For more information, see Viewing Details of Linux Packages.
Used By tab	This tab shows you the agent policies that are currently using this patch group. This is important to know if you are considering modifying the patch group, as it tells you which agents are affected.
How to delete a patch group	Patch groups can be deleted from the Linux Patch Groups list using the right-click menu.

Tips for Using the Search Tool

You can easily search for patches contained in a Linux patch group. To initiate a search you type the text you want to find and then press Enter. Only those patches matching the search criteria are displayed; all other patches are hidden.

- The Search tool works only on the information currently visible in the grid. You can right-click on the column headers to add or remove columns to be searched.
- If a filter is applied, only patches matching both the search criteria and the filter criteria are displayed.
- All partial matches are displayed.

- The search is not case sensitive.
- The use of wildcards is not allowed.
- To clear the search criteria, click the ⊗ icon located on the right side of the search box.

78. Creating Your Backup Files

You must first create a backup container for your core components. Account data for the user currently logged on is included in the core backup. A backup must also be performed for each additional user account. So, the backup process is:

1. Backup your core components.
2. Backup each additional user account.
   The backups of the additional user accounts can happen after you perform a restore of the core components, but if the other administrators are available, the recommendation is to have them log on and perform their user account backups immediately after the core backup.

Backing Up Your Core Components

This section provides step-by-step instructions for backing up the core components of your current Security Controls console. See the **Commonly Asked Questions** section for the list of core components.

> Make sure that your local or network drive contains enough free space to store the backup archive file. To be safe you should have 20 GB or more free space.

1. Close Ivanti Security Controls.
2. Launch the Migration Tool by selecting **Start > Ivanti** Security Controls **> Migration Tool**.
3. Select **Backup**.
4. Select **Core** mode.
   This specifies that all of Security Controls' core components will be saved to a backup archive file. In addition, the data for the user currently logged on to the console machine will be saved to the archive file.
5. (Optional) If you want to change the default location and name for the **Backup archive file name**, click the browse button and choose a new location.
   You can also type directly in the **Backup archive file name** box to specify a new location and/or name. The file must contain the .bak extension.
6. Secure the backup file by typing and confirming a passphrase.
   The passphrase will be used during the restore process. The data is stored in a secure container and can only be accessed by providing the correct passphrase.
7. Click **Backup core settings**.
   The Migration Tool will show status messages as it backs up the core components.
8. Wait for the confirmation message that indicates the backup was successful and then proceed to the next section for instructions on backing up your user data.

Backing Up Your User Data

The recommendation is to backup all your remaining user accounts immediately following your core backup. If one or more administrators are not available, however, they can backup and restore their user accounts at a later date. Keep in mind, however, that your existing console cannot be turned off until all user accounts are backed up. In addition, if a Security Controls administrator does not backup their account and restore it on the new console before their regularly scheduled tasks are executed, those tasks will be executed on the old console rather than the new console. To avoid these issues, all Security Controls user accounts should be backed up and restored in a timely manner.

1. If needed, launch the Migration Tool by selecting **Start > Ivanti** Security Controls **> Migration Tool**.
2. Select **Backup**.
3. Select **User** mode.
   This will back up all Security Controls data associated with the user currently logged on to the console machine.
4. Type a location and name for the user's backup archive file.
   Make sure to specify a name that uniquely identifies the user. You can also use the browse button to specify the location and file name.
5. Secure the backup file by typing and confirming a passphrase.
   The passphrase will be used during the restore process.
6. Click **Backup user settings**.

The Migration Tool will show status messages as it backs up the user data. A confirmation message will indicate when the user backup is complete.

Repeat this section for each user account. Close the Migration Tool when you are finished.

Related Topics

- Requirements for Using the Migration Tool
- Commonly Asked Questions
- Before You Begin
- Restoring Your Console on a New Machine
- Post-Migration Tasks

79. Creating a New Asset Task

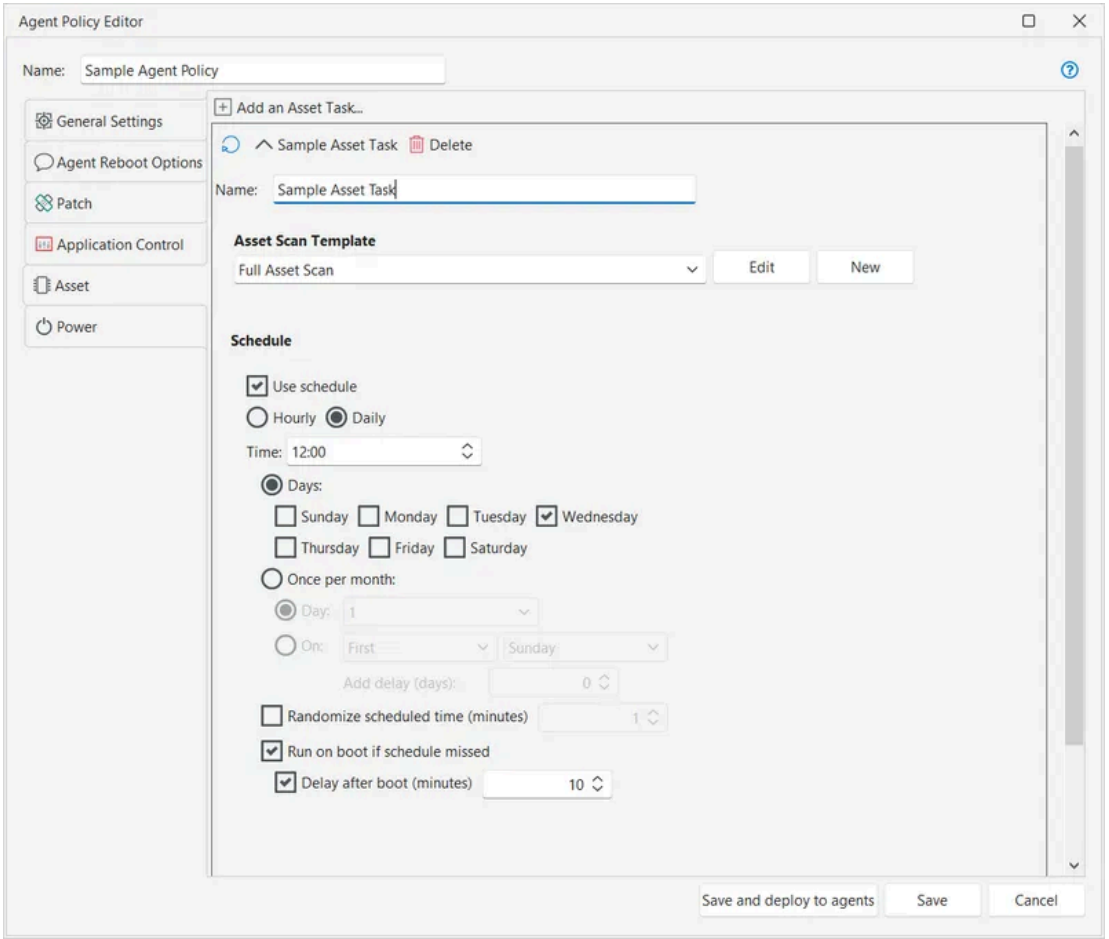
> Applies only to Windows-based machines.

An asset task is used to define how and when the target machines will be scanned to determine their software and hardware assets. If you do not create an asset task, then no asset scanning will be performed by agents that are assigned this policy. For background information about the asset management feature, see **Asset Management Overview**.

You can create multiple asset tasks for one agent policy. Each task can be expanded and collapsed using the Hide/Show triangle that resides on the task title bar. This enables you to view just the task you are working on at any one time.

While there is no theoretical limit to the number of asset tasks you can create for an agent policy, there is a practical limit. For example, it may become difficult to track and manage a policy if it contains too many asset tasks.

You configure agent asset tasks on the **Asset** tab. You can edit an existing asset task, or you can create a new task by clicking **Add an Asset Task**. Be sure to give the task a descriptive name because this is the name the users will see from within the **client program**. The results of an agent-based asset scan are reported to the console and viewable using **Machine View**.



Field	Description
Asset Scan Template	You must specify the template to use when an agent performs an asset scan. The asset scan template dictates exactly what will be scanned for and what will be ignored during a scan. The list of templates available for selection will include the predefined template (**Full Asset Scan**) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new asset scan template from scratch. • **Edit**: Enables you to edit an existing, custom asset scan template. The predefined template cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Asset Scan Template** dialog is displayed. See **Creating a New Asset Scan Template** for details on configuring the template.
Schedule Area	The asset schedule specifies how often the task will run on a target machine. It allows you to regularly run the task at a specific time or using a specified recurrence pattern. A built-in scheduler will be provided for each agent. The scheduler will check for new asset data immediately before starting a scheduled asset task. The agent scheduler will serialize executions of the same agent engine. For example, if you define a policy with two asset tasks that both start at 1:00 AM, they will not both start at 1:00; rather, they will be serialized (run back-to-back). If you have an asset task and a patch task both scheduled for 1:00 AM, however, they will both be started at 1:00 AM as they use different agent engines.
Use schedule	If enabled, the task will run on agent machines on a recurring basis according to the schedule settings. If not enabled, the schedule settings are ignored and the task must be started manually either **from the console** or **on the agent machine**.
Hourly	Allows you to schedule the task to be run on an hourly basis. • **Run every hh hours:** You can specify exactly how many hours there should be between scans. Valid values are from 1 - 100 hours. • **Starting at this time**: The first scan will begin at the specified time. Subsequent scans will be performed at the interval specified on **Run every hh hours.**
Daily	Indicates that the task will be run on the specified days, at the time of your choosing. For example, using this option a scan could be run every night at midnight, or every Saturday at 9:00 pm, or at 1:00 am the first Sunday of every month, etc. You can also use the **Daily** option to schedule a task in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly asset scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the task by one day.
Randomize scheduled time (minutes)	Staggers the exact time the task will be performed so as not to overtax the console or designated distribution server with simultaneous requests to download data files, engine components, etc.
Run on boot if	If a scheduled task is missed while a target machine is powered off, this option enables you to force the task to automatically run whenever the machine is restarted. The task will run immediately unless you enable the **Delay after boot (minutes)** check box, in which case the execution will be delayed by the specified number of minutes.

Field	Description
schedule missed	
Save and update Agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for **policy updates**, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console. The Agent Policy Editor will be closed.
Cancel	Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A *"Do you want to save your changes?"* prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and Update Agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

80. Creating a New Patch Task

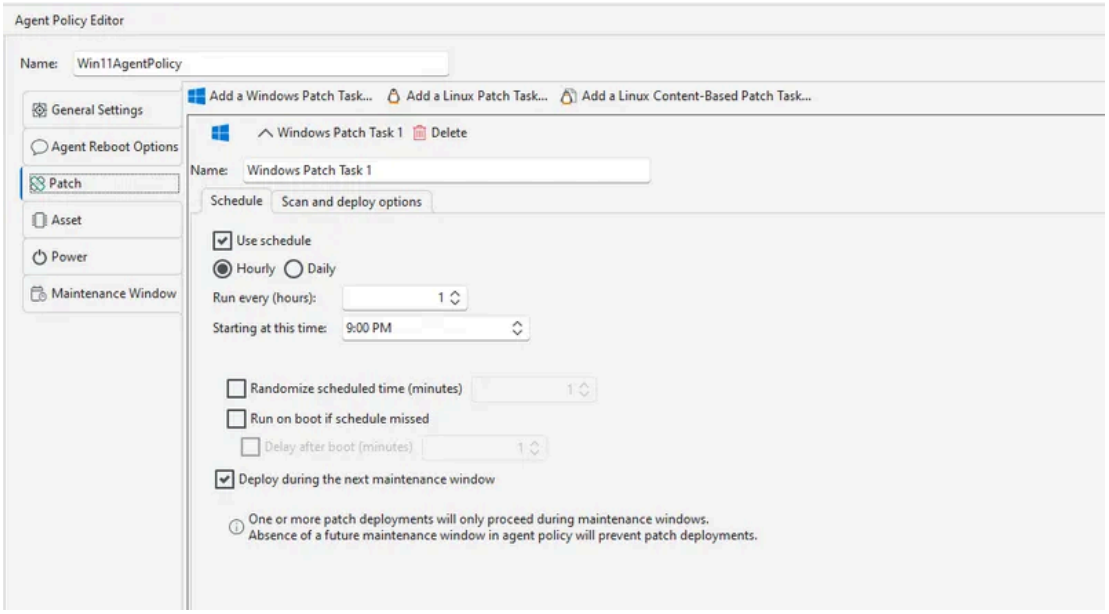
A patch task is used to define how and when the target machines will be scanned for missing patches. It can also be used to optionally deploy any patches identified as missing. If you do not create a patch task, then no patch scanning or patch deployment will be performed by agents that are assigned this policy.

Depending on the operating systems supported in your organization, you may create patch tasks for Windows machines, for Linux machines, or both. There are separate patch tasks for contentless and content-based Linux patching. You can create multiple patch tasks for one agent policy. Each task can be expanded and collapsed using the icon ( ) that resides on the task title bar. This enables you to view just the task you are working on at any one time.

While there is no theoretical limit to the number of patch tasks you can create for an agent policy, there is a practical limit. For example, it may become difficult to track and manage a policy if it contains too many patch tasks. Also, it may be problematic if you enable patch deployment on several different patch tasks. This is because that while scanning is relatively transparent to the user, deploying patches is not, as it often involves a reboot of the user's machine. In addition, you run the risk of multiple deployments occurring on one machine at the same time.

You configure agent patch tasks on the **Patch** tab. You can edit an existing patch task, or you can create a new task by clicking either **Add a Windows Patch Task** or **Add a Linux Patch Task**. Be sure to give the task a descriptive name because this is the name that will appear within the Windows client program.

Configuring a Windows Patch Task



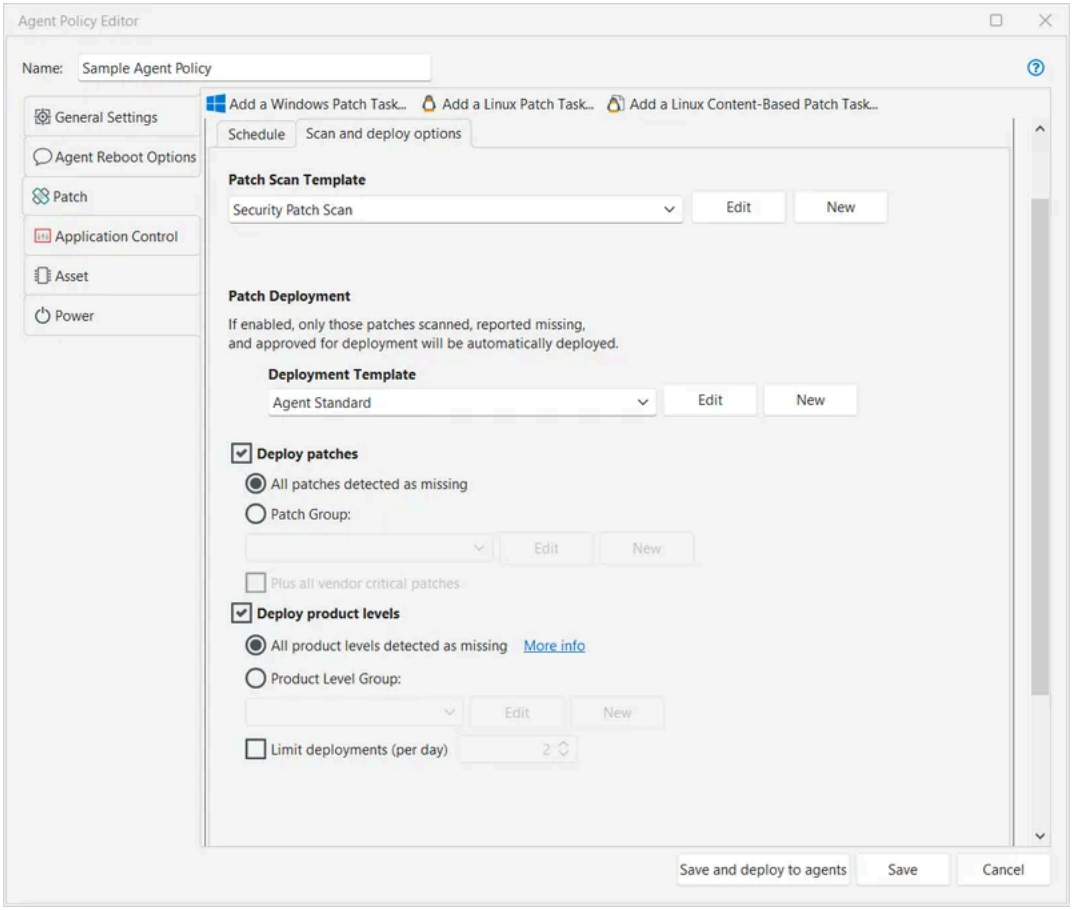
SCHEDULE TAB

The patch schedule specifies how often the task will run on a target machine. It allows you to regularly run the task at a specific time or using a specified recurrence pattern. A built-in scheduler will be provided for each agent. The scheduler will check for new patch data immediately before starting a scheduled patch task.

The agent scheduler will serialize executions of the same agent engine. For example, if you define a policy with two patch tasks that both start at 1:00 AM, they will not both start at 1:00; rather, they will be serialized (run back-to-back).

Field	Description
Use schedule	If enabled, the task will run on agent machines on a recurring basis according to the schedule settings. If not enabled, the schedule settings are ignored and the task must be started manually either **from the console** or **on the agent machine**.
Hourly	Allows you to schedule the task to be run on an hourly basis. • **Run every hh hours:** You can specify exactly how many hours there should be between scans. Valid values are from 1 - 100 hours. • **Starting at this time**: The first scan will begin at the specified time. Subsequent scans will be performed at the interval specified on **Run every hh hours.**
Daily	Indicates that the task will be run on the specified days, at the time of your choosing. For example, using this option a scan could be run every night at midnight, or every Saturday at 9:00 pm, or at 1:00 am the first Sunday of every month, etc. You can also use the **Daily** option to schedule a task in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly patch scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the task by one day.
Randomize scheduled time (minutes) **Run on boot if schedule missed**	Staggers the exact time the task will be performed so as not to overtax the console or designated distribution server with simultaneous requests to download patch files, scan engines, etc. If a scheduled task is missed while a target machine is powered off, this option enables you to force the task to automatically run whenever the machine is restarted. The task will run immediately unless you enable the **Delay after boot (minutes)** check box, in which case the execution will be delayed by the specified number of minutes.
Deploy during the next maintenance window	Uses the next available maintenance window after the deployment schedule for one or more patches.

SCAN AND DEPLOY OPTIONS TAB



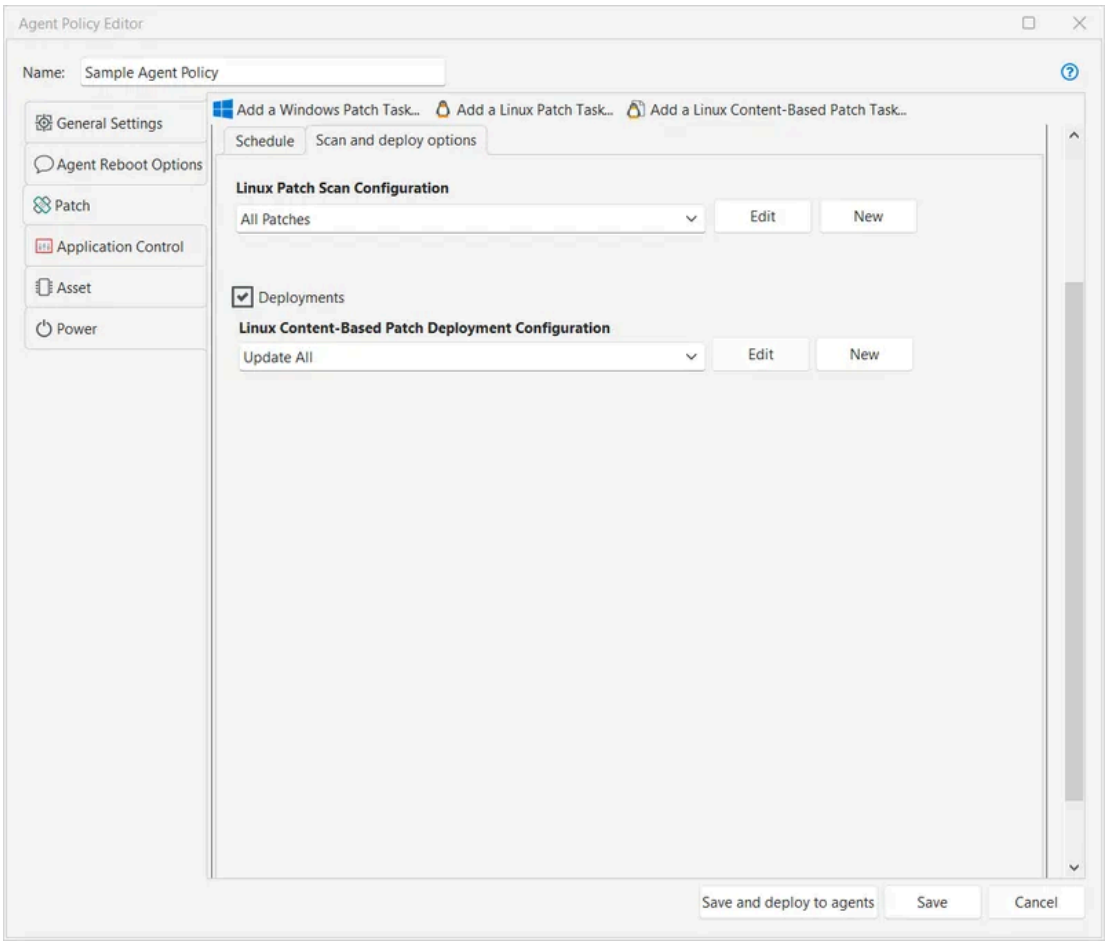
Field	Description
Patch Scan Template	You must specify the template to use when an agent performs a patch scan. The patch scan template dictates exactly what will be scanned for and what will be ignored during a scan. The list of templates available for selection will include the two predefined templates (Security Patch Scan and All Patches) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new patch scan template from scratch. • **Edit**: Enables you to edit an existing, custom patch scan template. The predefined templates cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Patch Scan Template** dialog is displayed. See **Creating a New Patch Scan Template** for details on configuring the template. The automatic deployment function and the automatic email function on the patch scan template is not supported by Security Controls Agent. If these functions are enabled they will be ignored.
Deployment Template	You must specify the template to use when an agent performs a patch deployment. The list of templates available for selection will include the predefined deployment templates (**Agent Standard, Standard, and Virtual Machine Standard**) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new deployment template from scratch. • **Edit**: Enables you to edit an existing, custom deployment template. The predefined deployment template cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Deployment Template** dialog is displayed. See **Creating a Deployment Template** for details on configuring the template. Automatic email notifications, custom actions, and distribution server options that may be specified in the deployment template do not apply to a Security Controls Agent.
Deploy patches	If you want the agent to be able to automatically deploy patches that are identified as missing by the patch scan, enable this check box. When the agents perform a patch deployment they will deploy only those patches that are: • Scanned for by the patch scan template, and • Reported as missing, and • Defined as *approved patches*. The approved patches can be either all patches detected as missing by a scan, or they can be limited to those patches you define in a patch group and/or to those patches deemed critical by the patch vendor. The list of

Field	Description
	approved patches defined here is bound to this particular patch task. The list will not be used by other patch tasks within the agent policy. • **All patches detected as missing:** Specifies that any patch identified as missing will be eligible for deployment. • **Patch Group:** Only those patches contained in the specified patch group will be deployed by the agent. If a scan detects missing patches not included in this group, those patches will not be deployed. • **Plus all vendor critical patches:** Specifies that in addition to the patches defined in the patch group, the list of patches approved for deployment should also include any patches identified as critical by the patch vendor. This gives you the security of knowing that if your patch group is out of date you will still always be able to deploy any new critical patches. To deploy only vendor critical patches, enable this check box and then specify an empty patch group in the **Patch Group** box. **New:** Enables you to make a new patch group. For more information see Creating and Editing a Patch Group. • **Edit:** Enables you to make modifications to the selected patch group. Be careful here, because any modifications you make will affect any other scan templates that are using the patch group. If you edit and save a patch group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you also choose to enable the deployment of product levels (see the **Deploy product levels** option), on an agent machine that is missing both product levels and patches, product levels are deployed first. Once the list of approved patches is determined, the patches are downloaded and installed according to their priority. Security patches are downloaded first, followed by all other patch types. The downloads occur in the background using idle bandwidth not being used by other applications. Foreground tasks such as Web browsing are not affected by the patch download process. Each patch task is allotted a 60 minute window to download the missing patches. (This is part of a two hour total maintenance window that is allocated for downloading missing product levels and patches.) Only those patches that are successfully downloaded during this 60 minute window will be installed by the active patch task. If the patch task cannot finish downloading all missing patches during the 60 minute window, the remaining patches will be identified, downloaded, and installed the next time the patch task is run. If an agent machine becomes disconnected from the network during a file download, the process will be suspended and will automatically resume where it left off when the network is available again. This technique is called checkpoint/restart and is extremely useful for machines that are frequently disconnected.
Deploy product levels	If you want the agent to be able to automatically deploy product levels that are identified as missing by the patch scan, enable this check box. When the agents perform a product level deployment they will deploy only those product levels that are: 1. Scanned for by the patch scan template, and 2. Reported as missing, and 3. Approved for deployment. The approved product levels can be either all product levels detected as missing by a scan, or they can be limited to those product levels you define in a product level group. The list of approved product levels defined here is bound to this particular patch task. The list will not be used by other patch tasks within the agent policy.

Field	Description
	• **More info:** A link to the About Product Level Groups Help topic that explains how product level groups are used by the program. • **All product levels detected as missing:** Specifies that any product level identified as missing will be eligible for deployment. • **Product Level Group:** Only those product levels contained in the specified product level group will be deployed by the agent. If a scan detects missing product levels not included in this group, those product levels will not be deployed. • **Limit deployments (per day):** Specifies the maximum number of product levels that can be deployed to a machine in one day. Product levels can take a long time to deploy and almost always require a reboot of the machine, so you typically want to keep this number rather small. If you do not limit the number of product level deployments in a day you run the risk of overwhelming a machine if it is missing a large number of product levels. If a machine is missing more product levels than the specified limit, the additional product levels will be deployed the next time the patch task is run. • TIP: Note that a "day" in this case is considered to be a calendar date and not a 24 hour period. This means the day is reset at midnight. If you were to schedule the patch task to run on an hourly basis (not recommended), it would allow you to maximize an overnight maintenance window by deploying the maximum number of product levels before midnight and then again immediately after midnight. **New:** Enables you to make a new product level group. For more information see Creating and Editing a Product Level Group. • **Edit:** Enables you to make modifications to the selected product level group. Be careful here, because any modifications you make will affect any patch task that references the product level group. Also, if you edit and save a product level group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If an agent machine is missing multiple product levels, only one product level will be installed at a time. The patch task will begin by initiating the download of all missing product levels. Operating system product levels are downloaded at a higher priority, but whichever product level gets downloaded first is the one that is first installed. After the product level is successfully installed, the machine is restarted, rescanned, and the process is repeated until all product levels are deployed or until the daily limit is reached [see the **Limit deployments (per day)** option]. In addition, each patch task is allotted a 60 minute window to complete the *download > install > restart > rescan* process. (This is part of a two hour total maintenance window that is allocated for downloading missing product levels and patches.) Only those product levels that are successfully downloaded during this 60 minute window will be installed by the active patch task. If the patch task cannot finish downloading all missing product levels during the 60 minute window, the remaining product levels will be identified, downloaded, and installed the next time the patch task is run. The downloads occur in the background using idle bandwidth not being used by other applications. Foreground tasks such as Web browsing are not affected by the product level download process. If an agent machine becomes disconnected from the network during a file download, the process will be suspended and will automatically resume where it left off when the network is available again. This technique is called checkpoint/restart and is extremely useful for machines that are frequently disconnected.

Patch Deployment Process

Configuring a Linux Patch Task



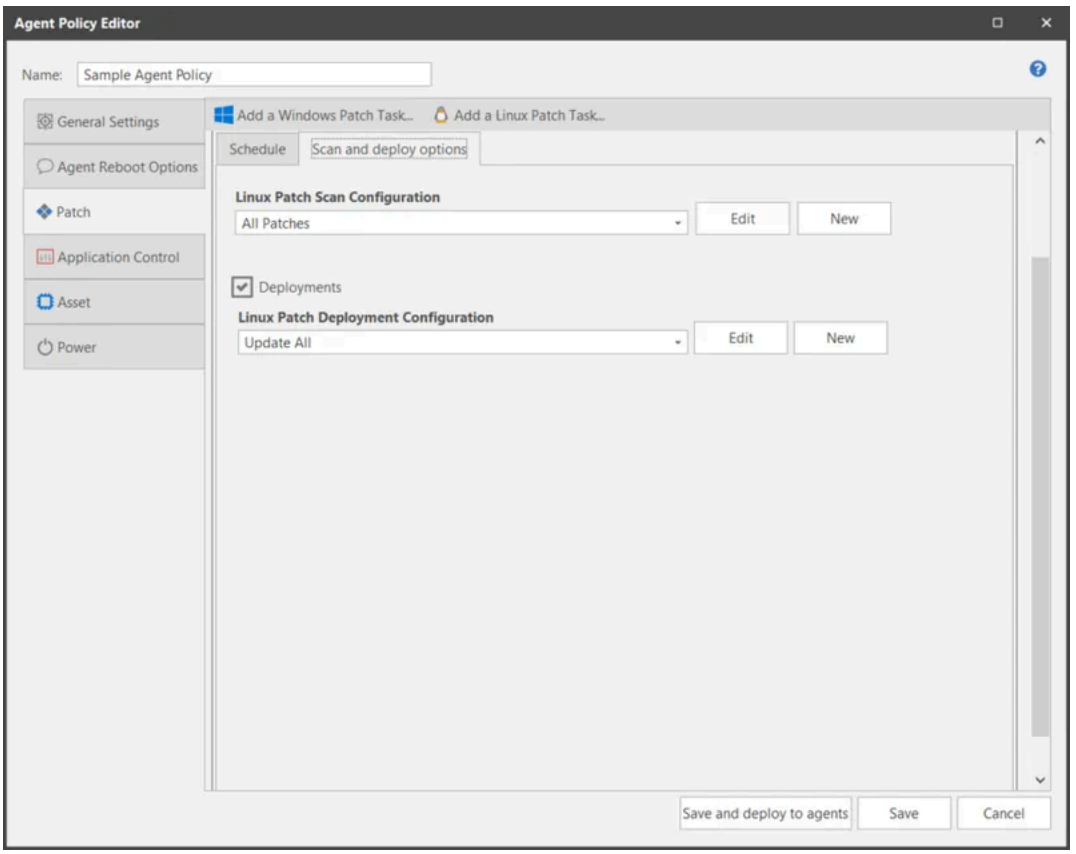
For the contentless Linux patching method, there is no separate Patch Scan Configuration. Whenever a Linux Patch Task runs, it runs a scan for all missing packages and advisories. You can then separately specify **Deploy options** as part of the Linux Patch Task. For the previous content-based Linux patching method, you need to specify **Scan and deploy options**.

SCHEDULE TAB

The patch schedule specifies how often the task will run on a target machine. It allows you to regularly run the task at a specific time or using a specified recurrence pattern.

Field	Description
Use schedule	If enabled, the task will run on agent machines on a recurring basis according to the schedule settings. If not enabled, the schedule settings are ignored and the task must be started manually on the agent machine using a **command-line utility**.
Hourly	Allows you to schedule the task to be run on an hourly basis. • **Run every (hours):** You can specify exactly how many hours there should be between scans. Valid values are from 1 - 100 hours. • **Starting at this time**: The first scan will begin at the specified time. Subsequent scans will be performed at the interval specified on **Run every hh hours.**
Daily	Indicates that the task will be run on the specified days, at the time of your choosing. For example, using this option a scan could be run every night at midnight, or every Saturday at 9:00 pm, or at 1:00 am the first Sunday of every month, etc. You can also use the **Daily** option to schedule a task in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly patch scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the task by one day.
Randomize scheduled time (minutes)	Staggers the exact time the task will be performed so as not to overtax the console or designated distribution server with simultaneous requests to download patch files, scan engines, etc.
Run on boot if schedule missed	If a scheduled task is missed while a target machine is powered off, this option enables you to force the task to automatically run whenever the machine is restarted. The task will run immediately unless you enable the **Delay after boot (minutes)** check box, in which case the execution will be delayed by the specified number of minutes.

DEPLOY OPTIONS or SCAN AND DEPLOY OPTIONS TAB



Field	Description
Linux Patch Scan Configuration (Content-Based only)	For Content-Based Linux patching, you must specify the configuration to use when an agent performs a Linux patch scan. The patch scan configuration dictates exactly what will be scanned for and what will be ignored during a scan. The list of configurations available for selection will include the two predefined configurations (Security Patch Scan and All Patch Scan) plus any custom configurations you've already defined. You can also do the following: • **New**: Enables you to create a new patch scan configuration from scratch. • **Edit**: Enables you to edit an existing, custom patch scan configuration. The predefined configurations cannot be edited. If you edit and save a configuration that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Linux Patch Scan Configuration** dialog is displayed. See Creating and Editing a Linux Patch Scan Configuration for details.
Linux Patch Deployment Configuration	You must specify the configuration to use when an agent performs a patch deployment. The list of configurations available for selection will include the predefined deployment configuration (Linux Patch Deployment) plus any custom configurations you've already defined. You can also do the following: • **New**: Enables you to create a new deployment configuration from scratch. • **Edit**: Enables you to edit an existing, custom deployment configuration. The predefined deployment configuration cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Linux Patch Deployment Configuration** dialog is displayed. See Creating and Editing a Linux Patch Deployment Configuration for details.

Saving an Agent Policy

SAVE OPTIONS

Field	Description
Save and update Agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for **policy updates**, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console. The Agent Policy Editor will be closed.
Save **Cancel**	Saves all changes to the policy file and then closes the Agent Policy Editor. The changes are not pushed out to listening agents. Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A *"Do you want to save your changes?"* prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and Update Agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

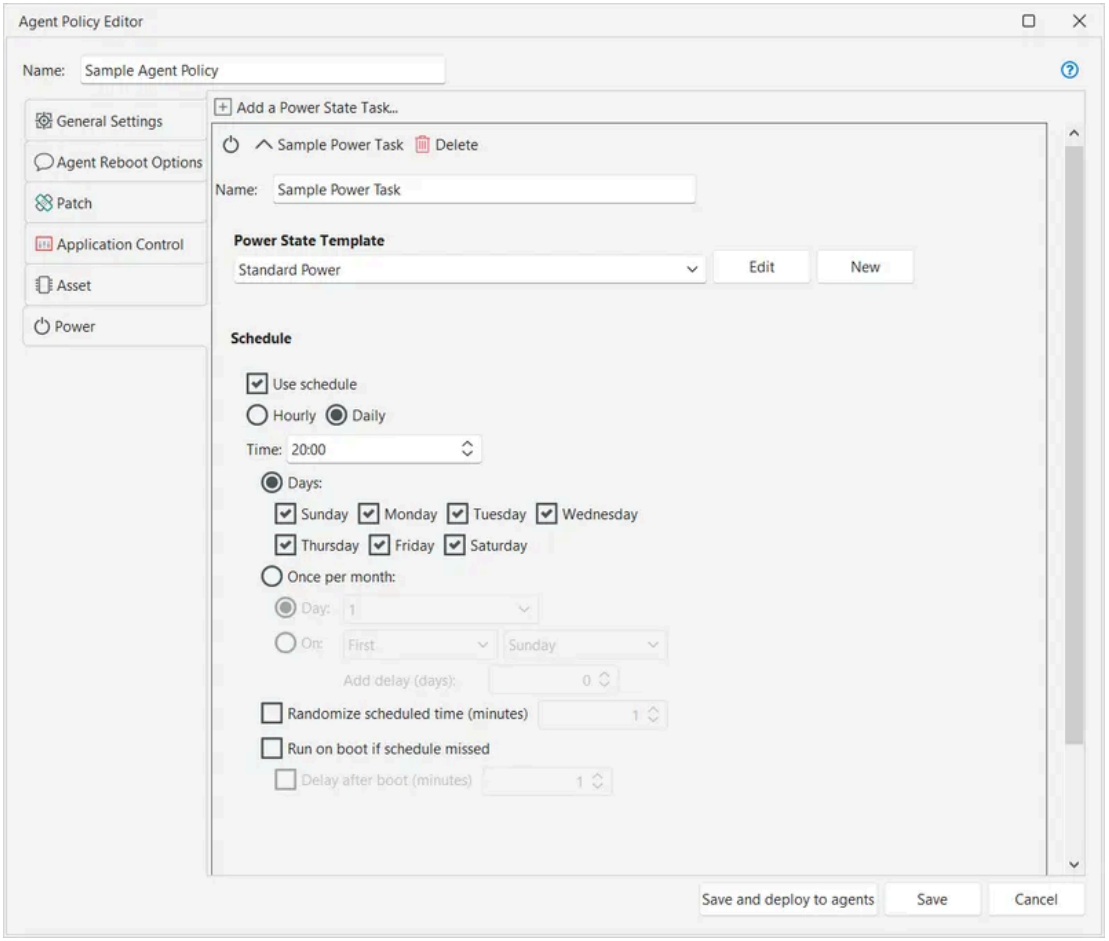
81. Creating a New Power Task

A power state task is used to shut down or restart the target machines and to specify what power state to leave the machines (fully powered on, sleep state, hibernate state, or powered off). If you do not create a power task, then no power state tasks will be performed by agents that are assigned this policy. For information as to why you might want to use an agent-based power state task, see **When should I use each solution?**. For background information about the power management feature, see **Power Management Overview**.

You can create multiple power tasks for one agent policy. Each task can be expanded and collapsed using the triangle that resides on the task title bar. This enables you to view just the task you are working on at any one time.

While there is no theoretical limit to the number of power tasks you can create for an agent policy, there is a practical limit. For example, it may become difficult to track and manage a policy if it contains too many power tasks.

You configure agent asset tasks on the **Power** tab. You can edit an existing power task, or you can create a new task by clicking **Add a Power State Task**.



Field	Description
Power State Template	You must specify the template to use when an agent performs a power task. The **power state template** dictates if and when the agent machines will be shut down or restarted, what control a logged on user will have over the reboot process, and what power state the machine will be left in. The list of templates available for selection will include the predefined template (**Standard Power**) plus any custom templates you've already defined. You can also do the following: • **New**: Enables you to create a new power state template from scratch. • **Edit**: Enables you to edit an existing, custom power state template. The predefined template cannot be edited. If you edit and save a template that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console. If you click **New** or **Edit**, the **Power State Template** dialog is displayed. See **Creating and Editing a Power State Template** for details on configuring the template.
Schedule Area	The power task schedule specifies how often the task will run on a target machine. It allows you to regularly run the task at a specific time or using a specified recurrence pattern. A built-in scheduler will be provided for each agent. The agent scheduler will serialize executions of the same agent engine. For example, if you define a policy with two power state tasks that both start at 1:00 AM, they will not both start at 1:00; rather, they will be serialized (run back-to-back). If you have a power state task and a patch task both scheduled for 1:00 AM, however, they will both be started at 1:00 AM as they use different agent engines.
Use schedule	If enabled, the task will run on agent machines on a recurring basis according to the schedule settings. If not enabled, the schedule settings are ignored and the task must be started manually **from the console**.
Hourly	Allows you to schedule the task to be run on an hourly basis. • **Run every hh hours:** You can specify exactly how many hours there should be between tasks. Valid values are from 1 - 100 hours. • **Starting at this time**: The first task will begin at the specified time. Subsequent tasks will be performed at the interval specified on **Run every hh hours.**
Daily	Indicates that the task will be run on the specified days, at the time of your choosing. For example, using this option a task could be run every night at midnight, or every Saturday at 9:00 pm, or at 1:00 am the first Sunday of every month, etc. You can also use the **Daily** option to schedule a task in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly power task to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the task by one day.
Randomize scheduled time (minutes)	Staggers the exact time the task will be performed. This is probably most useful if a large number of agents will be performing this power task and you don't want all your machines shutting down or restarting simultaneously.
Run on boot if	If a scheduled task is missed while a target machine is powered off, this option enables you to force the task to automatically run whenever the machine is restarted. The task will run immediately unless you enable the **Delay after boot (minutes)** check box, in which case the execution will be delayed by the specified number of minutes.

Field	Description
schedule missed	
Save and update Agents	Saves all changes to the policy file and stores it on the console. Also updates any agent machines that are currently assigned this policy as follows: • If an agent machine is online and configured to listen for **policy updates**, the updated policy will be pushed out to that machine immediately. • If an agent machine is online but is not configured to listen for policy updates, the updated policy will be pushed out the next time the agent checks in with the console. • If an agent machine is not currently online, the updated policy will be pushed out the next time the agent checks in with the console. The Agent Policy Editor will be closed.
Cancel	Indicates you want to exit the Agent Policy Editor without saving your most recent changes. A *"Do you want to save your changes?"* prompt will appear that gives you a second chance to save your changes. If you click **Yes** the policy will be saved and the associated agents updated (the same as **Save and Update Agents**). If you click **No** the Agent Policy Editor will be closed without saving your changes.

82. Creating and Editing a Windows Patch Group

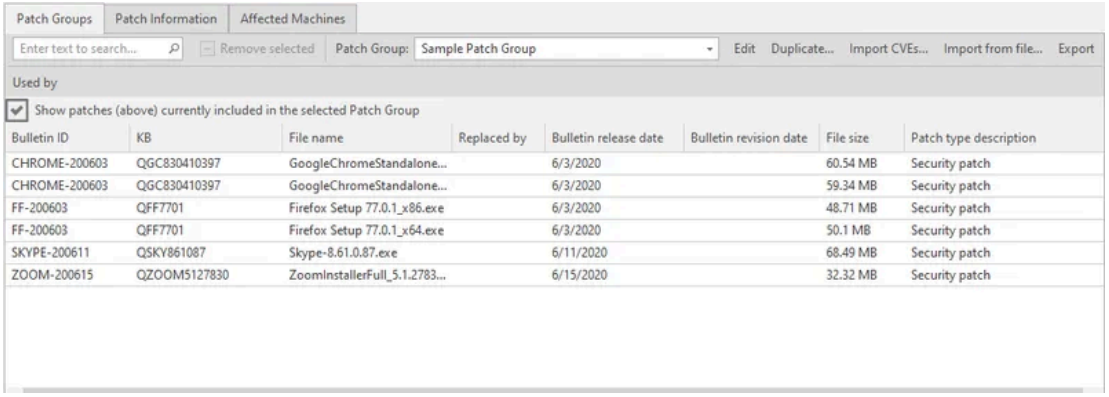
> To import an existing patch group, select **Import > Windows Patch Group**.

You can create a new patch group or modify an existing group.

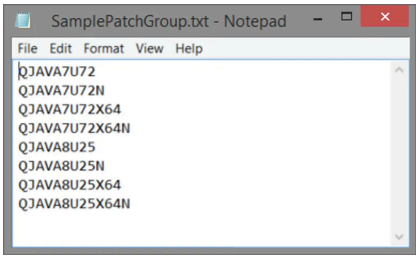
- To create a new patch group, click **New > Windows Patch > Patch Group**.
- In the **New Patch Group** dialog, type a name that you would like to assign to this patch group, add a comment that describes the purpose of the group, and then click **Save**.
  To edit an existing patch group, in the **Patch Groups** list, click the patch group name.

> Be careful when editing an existing patch group. Any modifications you make will affect any scan template that references the patch group. Also, if you edit and save a patch group that is currently being used by an **agent policy**, the agents using that policy will be updated the next time they check in with the console.

The patch group will be displayed on the **Patch Groups** tab in the bottom pane of the **Windows Patches** dialog (also known as **Windows Patch View**). If this is a new patch group, the group will be empty.



Performing Actions on Patch Groups

Action	Description
How to add one or more patches to a patch group	There are several ways to add one or more patches to a patch group. You cannot add product levels to a patch group. You can, however, define separate **product level groups** for use with agents. • In the top pane, right-click on the desired patch or patches, select **Add to Patch Group** and then choose a patch group name. For information on filtering the patches contained in the top pane, see **Filtering Patch View by Patch Type**, **Filtering Patch View by Product Vendor**, and **Filtering Patch View**. • If you attempt to add a software distribution patch, a confirmation dialog will be displayed. This is to ensure that you don't inadvertently scan for and **deploy third-party applications**. You can import a list of patches from a text file. The text file might have been created from another patch group that you have previously exported, or it might be a file that you created manually using a program such as Notepad. The text file must contain just the KB numbers associated with each patch, one entry per line.  You can import a list of CVEs and add the patches that are related to those CVEs. For more information, see the **Import CVEs** button and the **Importing CVEs** help topic. • You can also add to a patch group from **Machine View** or **Scan View**. Select the desired patches and then use the right-click menu to create a new patch group or to add to an existing patch group.
Search	Enables you to search for specific patches contained in a patch group. To initiate a search you simply click in the **Search** box and then type the text you want to find. Only those patches matching the search criteria are displayed; all other patches are hidden. Here are some tips for using the Search tool: • The Search tool works only on the information currently visible in the bottom pane. • All partial matches are displayed. • The use of wildcards in the Search tool is not allowed.
Remove selected	To remove one or more patches from the patch group, select the desired patches and then click **Remove selected**.
Patch Group	Use this box to select the desired patch group.
Edit	Enables you to edit the name and description of the patch group.
Duplicate	Makes a duplicate copy of the patch group. Type a new name for the group and then click **OK**.
Import CVEs	Imports a list of CVEs and adds the patches that are related to those CVEs. For more information, see **Importing CVEs**.

Action	Description
Import from file **Export**	You can import a list of patches from a previously created text file. For more information, see the section above titled **How to add one or more patches to a patch group**. Exports the selected patch group to a text file. This file can be imported into another patch group on the same console or on a different console.
Used By	This button shows you the patch scan templates and agent policies that are currently using this patch group. This is important to know if you are considering modifying the group, as it tells you what other areas of the program are affected.
Show patches (above) currently included in the selected Patch Group	If enabled, patches contained in the selected patch group will also be displayed in the Patch View list in the top pane. If you prefer not to view the same patches in both the Patch View list and the patch group list, then disable this check box.
How to delete a patch group	Patch groups can be deleted from the **Patch Groups list** in the navigation pane using the right-click menu.

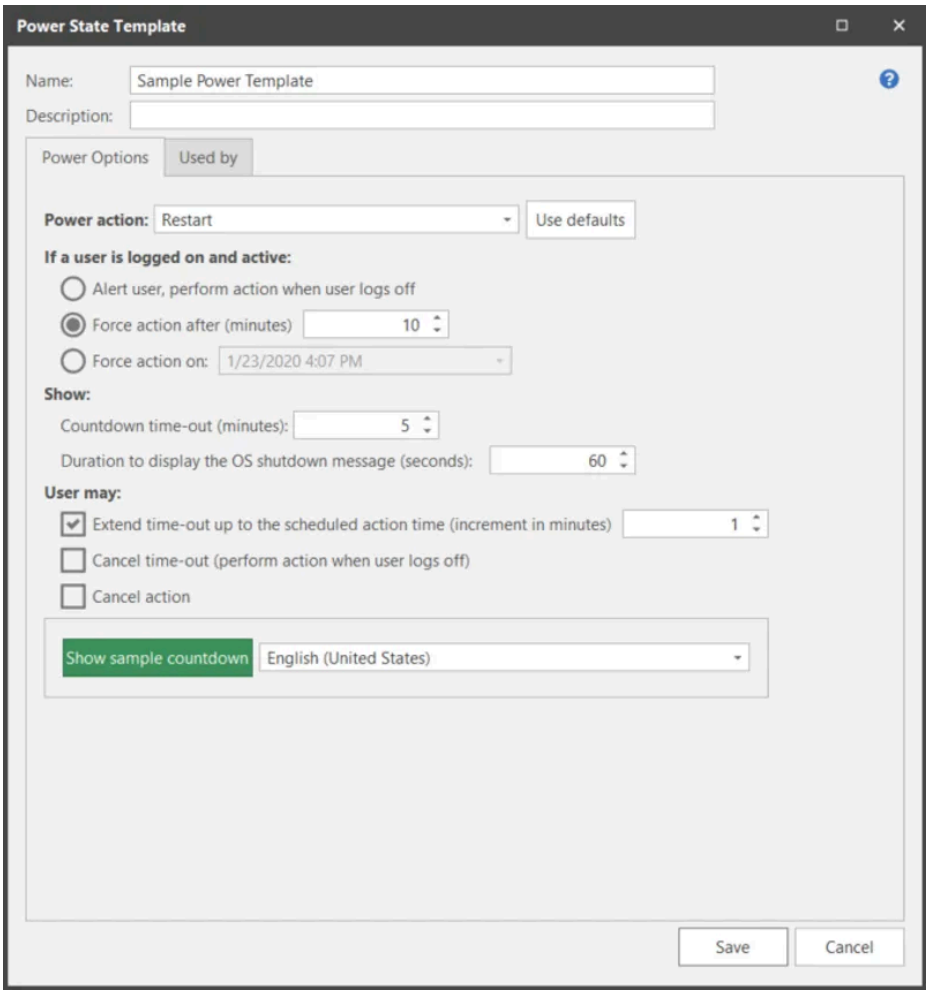
83. Creating and Editing a Power State Template

Security Controls comes with one predefined power state template, named **Standard Power**. This template cannot be modified. It will:

- Initiate an immediate restart of all machines
- Enable a logged on user to extend the reboot in one minute increments up to 10 minutes
- Bring the machines back online after the reboot

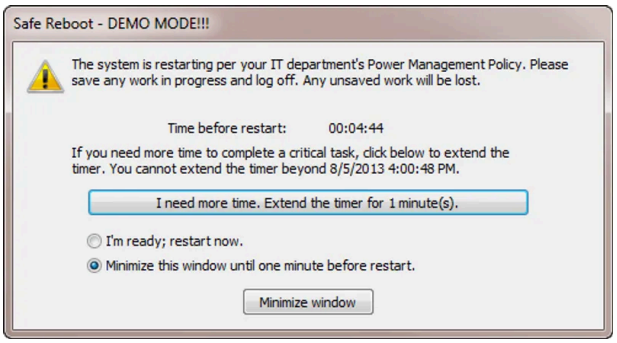
While the Standard template is fine for many instances, you may want to utilize some of the more advanced features, such as the ability to leave the machines in a reduced power or powered off state. To this end, Security Controls enables you to create any number of custom power state templates.

To create a new power state template, from the main menu select **New > Power State Template**. The **Power State Template** dialog will appear.



The **Power State Template** dialog contains two tabs that collectively define the characteristics of the template.

Field	Description
Name	The name that you wish to assign to this power state template.
Description	A description of the template.
Restart and power action	You can specify if a restart should occur and what power state you want to leave the machines. • **Sleep if possible:** The machines are put into a sleep state directly without a restart. This is a low power state that eliminates power to all unneeded areas of a machine. For more detailed information about sleep state, see **Sleep and Hibernation Notes**. • **Hibernate, otherwise try sleep:** The machines are put into a hibernation state without a restart. This is very similar to sleep state, with the difference being that the machine's RAM is copied to a storage areas (such as a hard drive) before hibernation state is initiated. This enables an end user to very quickly restart the machine, restore the previous state, and resume working. • If a target machine is not **configured to allow hibernation**, the program will instead attempt to put the machine into a sleep state. If the machine cannot be put into a sleep state no action will occur. For more detailed information about hibernate state, see **Sleep and Hibernation Notes**. **Shut down:** The machines are powered off. This option is also useful if you simply want to make sure non-critical machines are turned off each night or over a weekend, saving energy. • **Restart:** The machines are restarted and left in a powered on state. • **Restart, then sleep if possible:** The machines are restarted and then put into a sleep state. There is a two minute delay between the completion of the restart and the time the machines are put into the sleep state. The Microsoft Scheduler is used on each target machine to initiate the sleep state following the restart. • **Restart, then hibernate if possible:** The machines are restarted and then put into a hibernation state. There is a two minute delay between the completion of the restart and the time the machines are put into the hibernate state. The Microsoft Scheduler is used on each target machine to initiate the hibernate state following the restart. • If a target machine is not **configured to allow hibernation**, the program will instead attempt to put the machine into a sleep state after the restart. If the machine cannot be put into a sleep state no action will occur. For more detailed information about hibernate state, see **Sleep and Hibernation Notes**. **Restart, then shut down:** The machines are restarted and then powered off. This option enables you to provide a warning to any active users about the pending restart. There is a two minute delay between the completion of the restart and the time the machines are shut down. This option is useful if you want to perform a reboot in order to complete a maintenance task but then want the machines to be shut down. The Microsoft Scheduler is used on each target machine to initiate the shutdown following the restart.
Use defaults	This button is tied to the **Restart and power action** box. When you click **Use defaults**, all remaining options on the dialog will be changed to the values recommended for use with the currently selected **Restart and power action**.
If a user is logged on	If you elect to restart or shut down the machines, you can specify the amount of warning that a logged-on user will receive and you can choose the degree of control the user will have over the process. You can: • Alert the user that a restart (or shutdown) will occur when they log off. • Elect to force a reboot (or shutdown) after a number of minutes have passed. • Elect to force a reboot (or shutdown) at a specific date and time.

Field	Description
	• Show a time-out countdown on the user's machine in advance of the reboot (or shutdown) with a specified initial time-out value. To preview the dialog box that the user will see, click **Show Sample Countdown**. The language box to the right can be used to preview this dialog in different languages.  Select the duration to display the standard Windows shutdown message when the shutdown sequence is initiated. • Allow the user to extend the time-out countdown up to a specified maximum. • Allow the user to cancel the time-out. If a time-out is cancelled the machine will be restarted after the user logs off or manually reboots the machine. • Allow the user to cancel the restart.
Used By tab	This tab shows you the Favorites and the agent policies that are currently using this power state template. This is important to know if you are considering modifying the template, as it tells you what other areas of the program are affected.

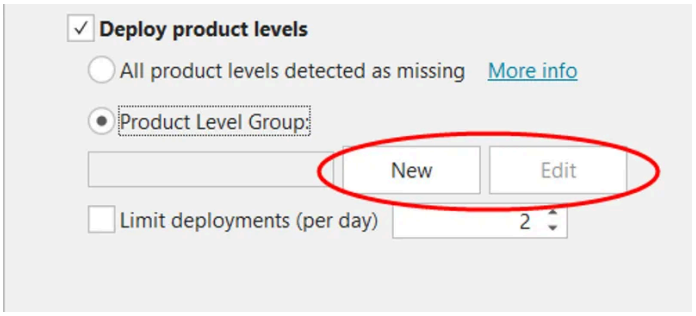
To save the template click **Save**. To close the dialog without saving the changes **Cancel**.

To use a power state template, see **How to Initiate Management Tasks**.

84. Creating and Editing a Product Level Group

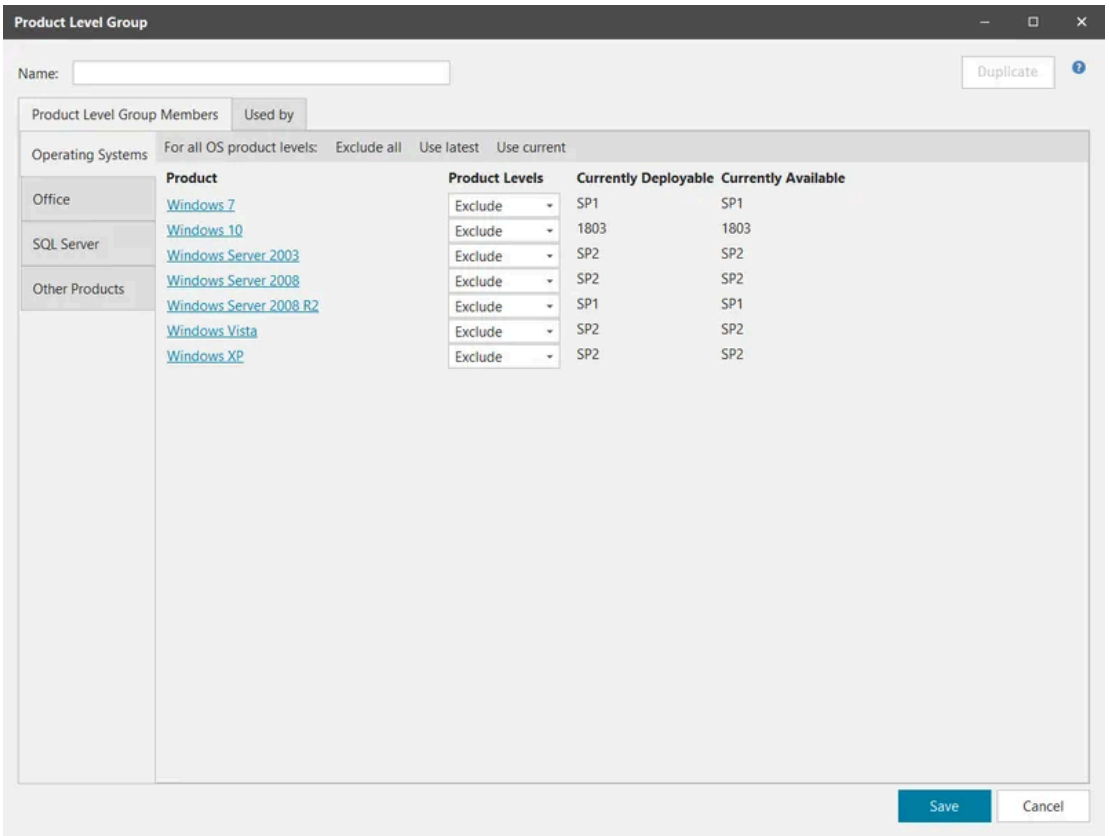
To create a new product level group or edit an existing product level group:

1. From within an agent Windows Patch Task, enable **Deploy product levels**.
2. Enable **Product Level Group** and then click either **New** or **Edit**.



> Another option for creating a new product level group is to select **New > Windows Patch > Product Level Group** from the main menu. Another option for editing an existing product level group is to double-click the group from within the Product Level Groups list. You can also use this list to copy or delete a product level group.

This will display the **Product Level Group** dialog.



Be careful when editing an existing product level group. Any modifications you make will affect any Windows Patch Task that references the product level group. Also, if you edit and save a product level group that is currently being used by an agent policy, the agents using that policy will be updated the next time they check in with the console.

Field	Description
Name	Type a name that you would like to assign to this product level group.
Duplicate	Makes a duplicate copy of the product level group. Type a new name for the group and then click **OK**.
	Displays Help information about this dialog.
Product Level Group Members	This tab enables you to add product levels to this group. The available product levels are separated into four product categories that are represented by the tabs shown along the left side of the dialog. For each product category you can: • **Exclude all**: Excludes every product level in the product category. This is the default value. • **Use latest**: Sets all product levels in the category to **Latest**. This means that the latest product level available for a product always will be deployed. The advantage to this setting is that if a new product level becomes available it will be the one that is automatically deployed. • **Use current**: Sets the value to the product level that is currently available for each product. This value will not change if a new product level becomes available. You can also manually set the product level value for each individual product.
Used By tab	This tab shows you the agent policies that are currently using this product level group. This is important to know if you are considering modifying the group, as it tells you what other areas of the program are affected.

IMPORTANT! If a new product becomes available, the product will be added to the appropriate product category the next time the Security Controls XML files are refreshed. Keep in mind that the default level value for any new product will be **Exclude all**. If you want the new product's level to be included in the group you must revisit the product level group and update the product level setting.

85. Creating and Using a Manual Installation Script

When manually installing Security Controls Agent on machines, one option is to create a script that will automatically pass all necessary agent information to the installation wizard. You can copy the script to a key fob or a USB flash drive and then easily move from machine to machine installing the agent.

> The following scripts are provided only as examples. Do not attempt to use these scripts in your organization without modifying the input values and performing adequate testing.

Example scripts for passphrase authentication

STPlatformUpdater.exe /wi:/qn /wi:"/l*v c:\temp\install.log" /wi:SERVERURI=*https://consolename:3121* /wi:POLICY=*policyname* /wi:AUTHENTICATIONTYPE=PASSPHRASE /wi:PASSPHRASE=*secret*

STPlatformUpdater.exe /wi:/qn /wi:SERVERURI=*https://consolename:3121* /wi:POLICY=*"policy name with spaces"* /wi:AUTHENTICATIONTYPE=PASSPHRASE /wi:PASSPHRASE=*secret*

Example script for Windows authentication

STPlatformUpdater.exe /wi:/qn /wi:"/l*v c:\temp\install.log" /wi:SERVERURI=*https://consolename:3121* /wi:POLICY=*policyname* /wi:AUTHENTICATIONTYPE=WINDOWS /wi:SERVERUSERNAME=*domainname|Your.Name* /wi:PASSWORD=*secret*

Example script for cloud-based agent installation

STPlatformUpdater.exe /wi:"/qn /l*v install.log ACTIVATIONKEY=*12345abc-2abc-3abc-4abc-123456789abc*"

Where:

- **STPlatformUpdater** is a bootstrap installer for the agent platform installation
- **/wi** means pass this to Windows Installer.
- **/qn** means no user interface activity from the installer.
- **/l*v** means write a log for the installation attempt. It has one parameter that specifies the log file name.
- **SERVERURI** is the address, port, and scheme (e.g. https://) used to connect to the console for registration and check-in.
- **POLICY** is the name of the agent policy that will be assigned to the agent.
- **AUTHENTICATIONTYPE** is either PASSPHRASE or WINDOWS (this is dictated by the **Tools > Options >**Agents dialog).
- **PASSPHRASE** is the passphrase used to authenticate the agent to the console (used only if AUTHENTICATIONTYPE=*PASSPHRASE*).
- **SERVERUSERNAME** is the name of a user who has rights to install an agent (used only if AUTHENTICATIONTYPE=*WINDOWS*).
- **PASSWORD** is the password used to authenticate the user to the console (used only if AUTHENTICATIONTYPE=*WINDOWS*).
- **USECURRENTCREDENTIALS=1** can be used in place of SERVERUSERNAME and PASSWORD if you want to authenticate using the credentials of the person who logged on to run the script.
- **ACTIVATIONKEY** is the activation key that was created from one of the following:
  - Security Controls Cloud service
  - Security Controls console
  - Cloudsync function in the REST API

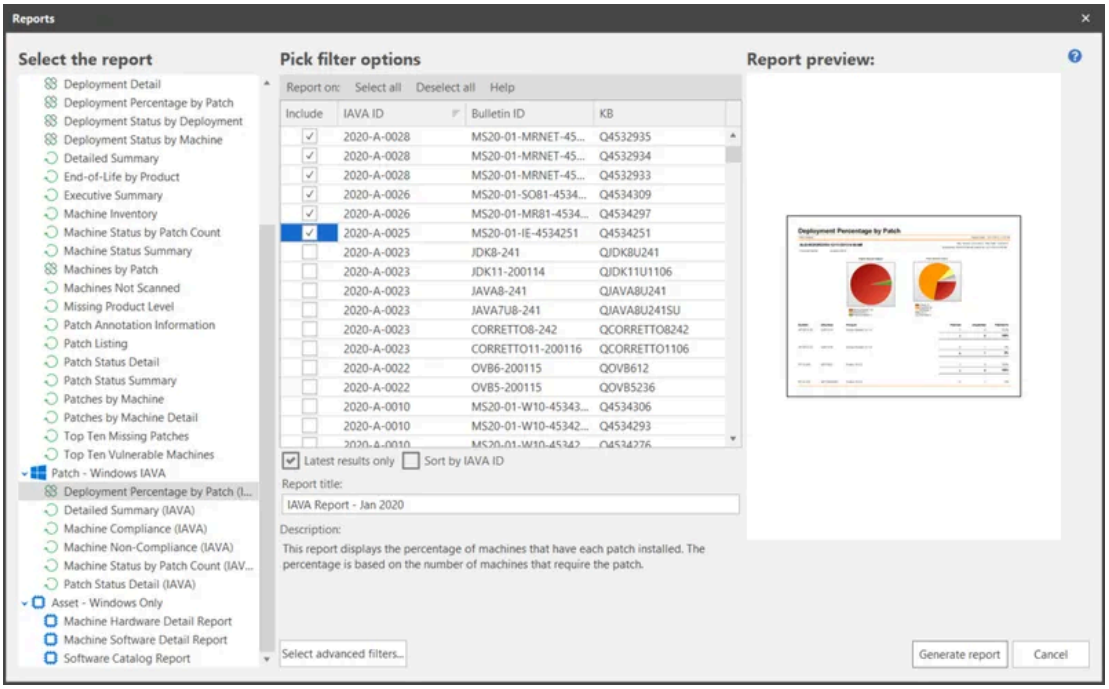
Referencing a key that was created from the console or the REST API enables you to **assign the agent machines to a group** at installation time.

86. Creating an IAVA Report

With the IAVA Reporter you can create a number of different IAVA reports using existing data in the Security Controls database.

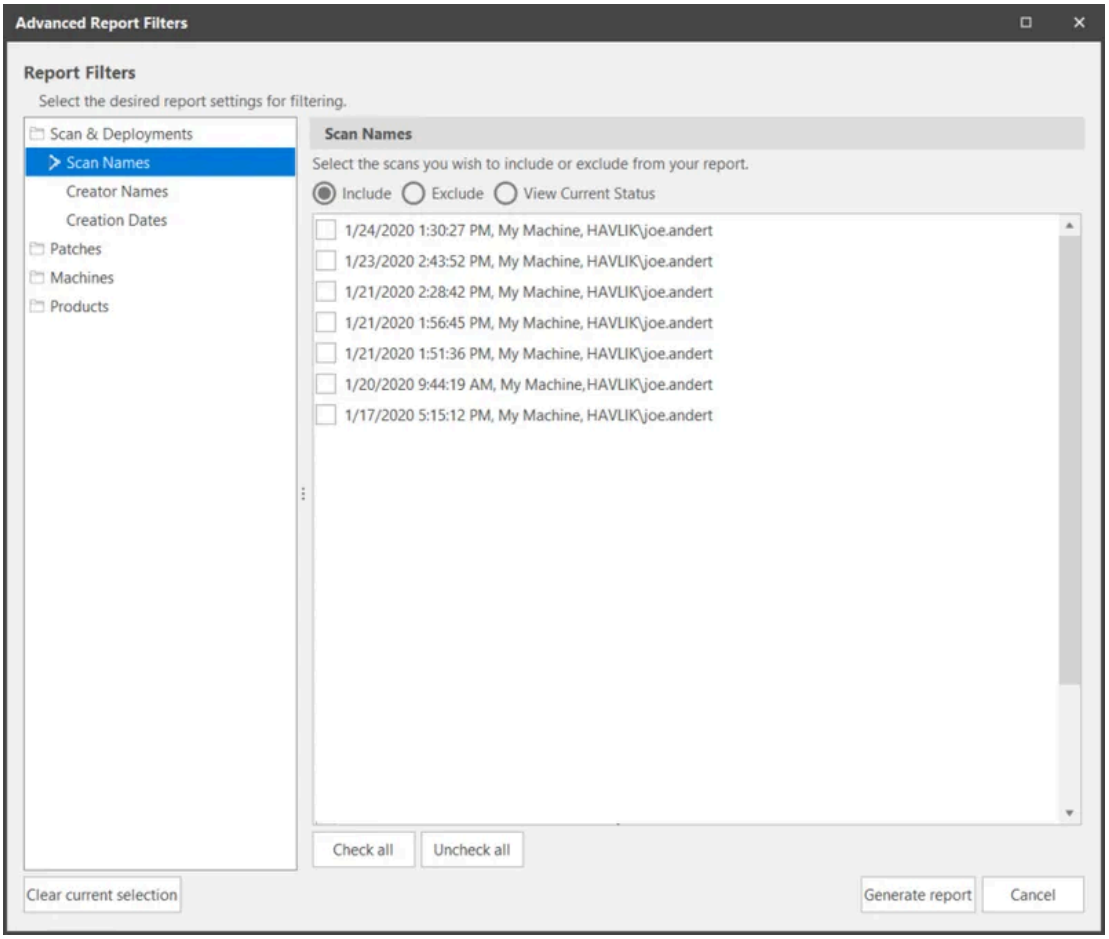
1. Open the **Reports** dialog using the **Tools > Create report** menu.
2. In the **Select the report** list, select the IAVA report you want to generate.
   The IAVA reports are in the **Patch - Windows IAVA** section.
   - **Deployment Percentage by Patch (IAVA):**Displays the percentage of machines that have each patch installed. The percentage is based on the number of machines that require the patch.
   - **Detailed Summary (IAVA):** Shows a summary of the scan, plus it provides a list that shows each machine that was scanned and detailed information about each machine.
   - **Machine Compliance (IAVA):** Provides IAVA machine compliance information.
   - **Machine Non-Compliance (IAVA):** Provides IAVA machine non-compliance information.
   - **Machine Status by Patch Count (IAVA):** Displays the number of machines in groups based on the number of missing patches.
   - **Patch Status Detail (IAVA):** Provides detailed information about each patch discovered by the scan.

Select the specific patches to report on, or select all patches.



Select the desired report customization options:

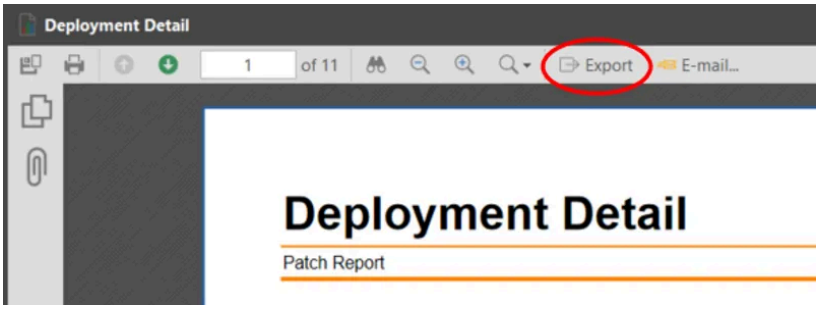
- The **Latest results only** check box enables you to view the current status by limiting the report to the most recent scan results for all machines.
- **Sort by IAVA ID:** Sorts the report results by IAVA number (lowest to highest).
- The **Select advanced filters** button will let you filter the results to specific scans, deployments, consoles, or machines.



In the **Report title** box, type a descriptive title.

6. Click **Generate report**.

The report that is generated can be exported to a variety of different formats by clicking the **Export** button.

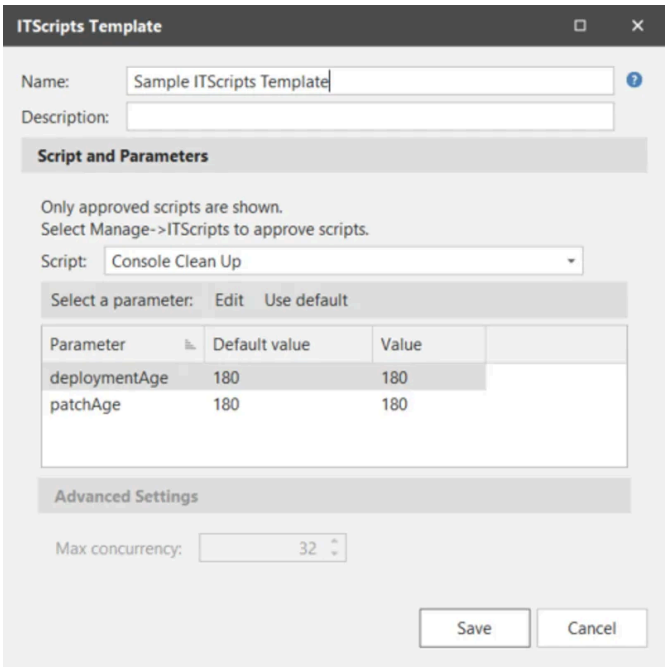


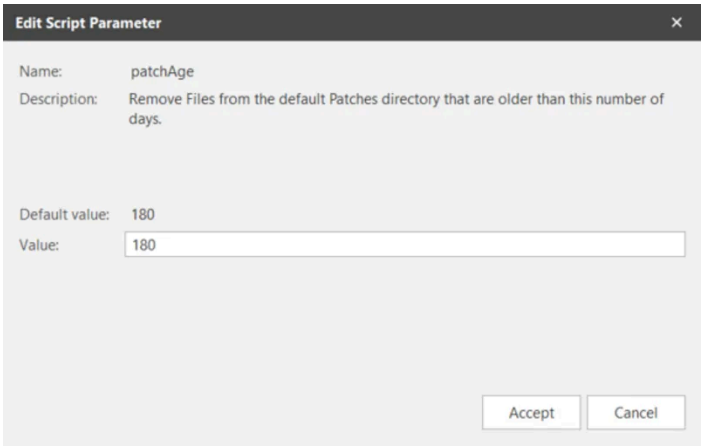
87. Creating an ITScripts Template

An ITScripts template is used to define how a particular script should be executed. The template specifies:

- Which script to execute
- The values of the input parameters used by the script
- The maximum number of machines the script may run on simultaneously (concurrency)

Security Controls allows you to create any number of custom ITScripts templates. To create a new ITScripts template, from the main menu select **New > ITScripts Template**. The **ITScripts Template** dialog will appear.



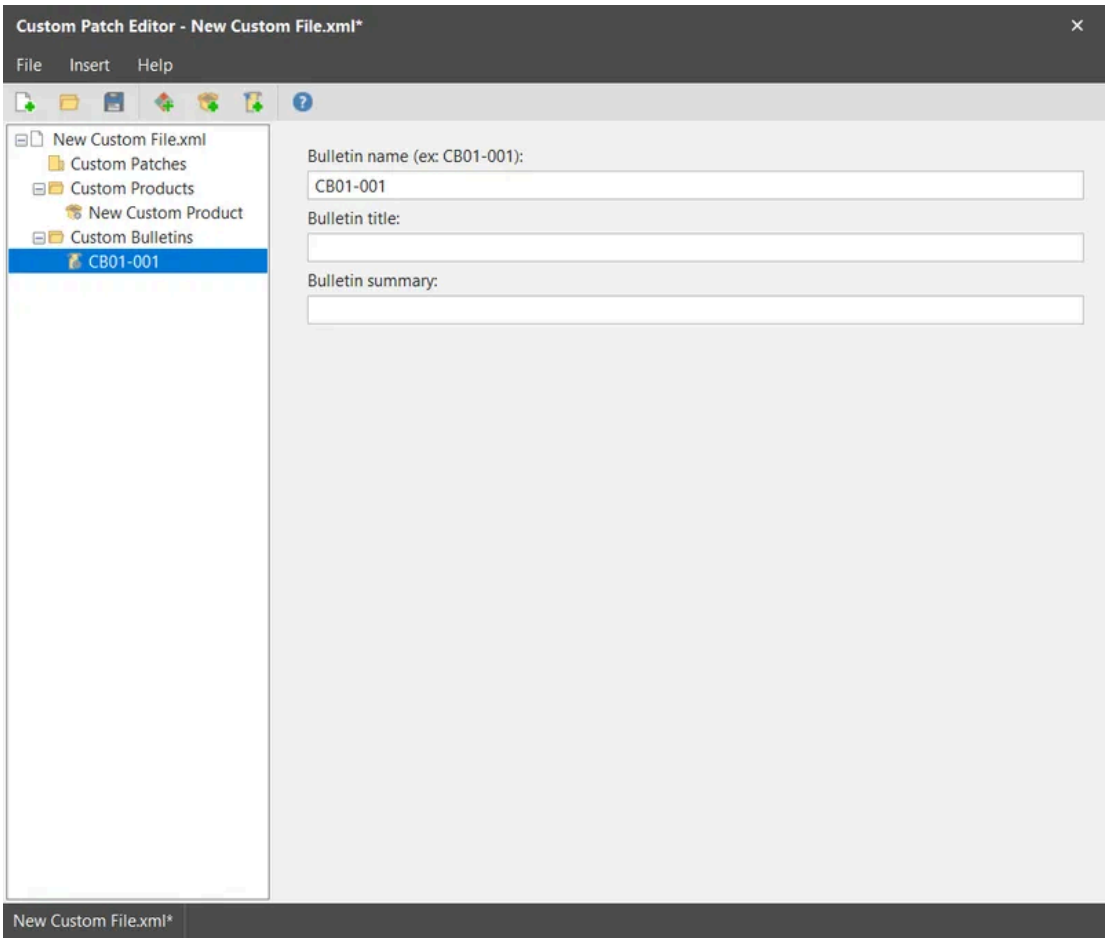
Field	Description
Name	The name that you wish to assign to this template.
Description	A description of the template.
Script	Select the script you want this template to run. Only approved scripts contained in the **Script Catalog Manager** are available for selection. The Script Catalog Manager will also provide detailed information about each script.
Parameters	Displays the input parameters used by the script and the parameter values that will be used by the template. To modify a parameter value, double-click the parameter or select the parameter and click **Edit**. The **Edit Script Parameter** dialog is displayed. The modified parameter value only applies to the template; the value in the original script is unchanged. Also, string values must be contained within quotes (for example, "*"); numeric values do not require quotes. 
Max concurrency	This option does not apply to scripts whose **target type = Console**. Specifies the maximum number of target machines you will allow the script to run on at one time. Valid values are 1 - 256. One suggestion is to set this value to four times the number of CPUs on the console machine. (Example: If you have an eight core machine the **Max concurrency** value should be 32.) Your network speed and bandwidth should also be taken into consideration when setting this value.

To save the template, click **Save**. To close the dialog without saving the changes, click **Cancel**.

88. Creating a Custom Bulletin

A security bulletin provides a summary describing why a custom product or patch is being created. Many times a bulletin will describe a particular software vulnerability that is being addressed by a patch. You must apply a new custom patch to a bulletin, so if you are not tying a patch to an existing bulletin then you must create a new bulletin.

1. To create a custom bulletin, within Custom Patch File Editor select **Insert > Add Bulletin** or click the **Add Bulletin** toolbar icon ( ).
   The new custom bulletin is selected and the bulletin characteristics are displayed in the right pane.
2. Use the options in the right-hand pane to define the new bulletin.



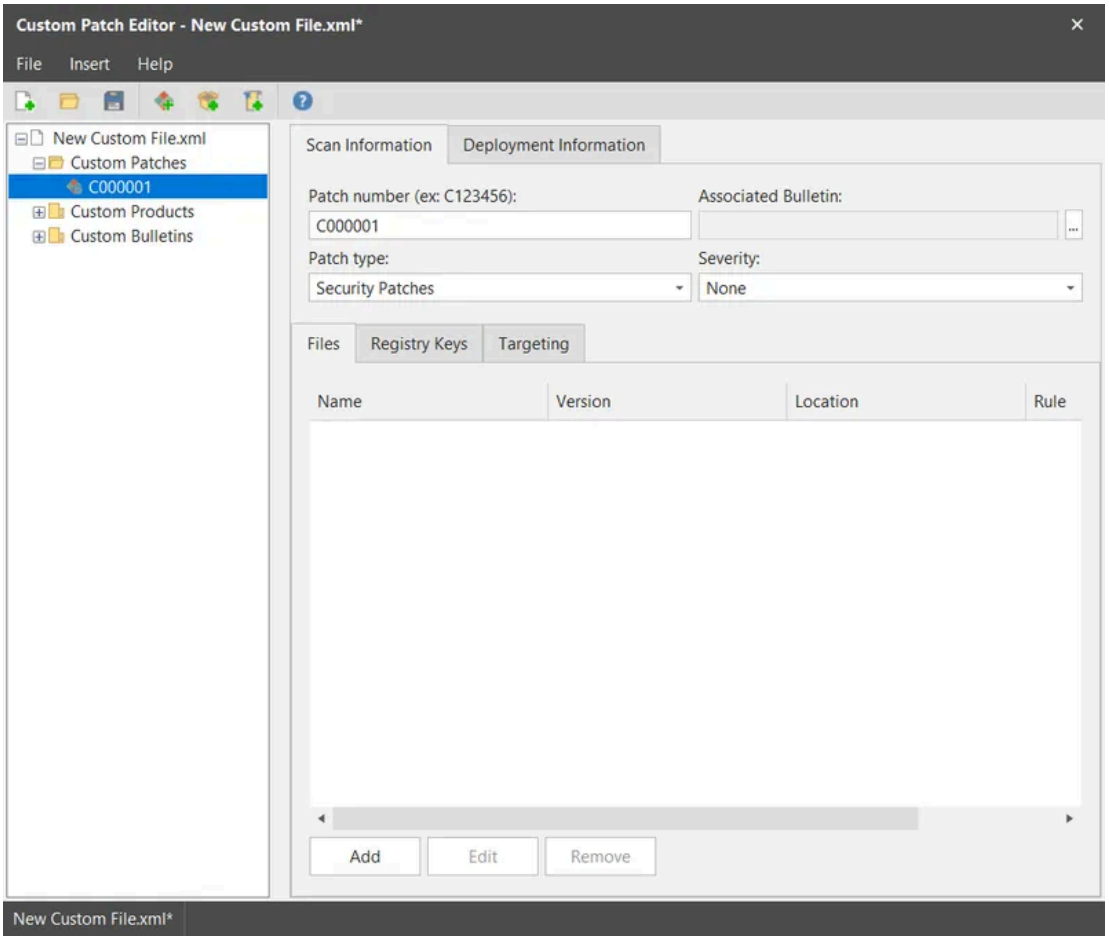
3. When complete, save and then validate the XML file (see Saving and Validating Your Changes).

Field	Description
Bulletin Name	Type a unique name for the bulletin. The name cannot match a bulletin name already defined to the program.
Bulletin Title	Type a short description of the bulletin.
Bulletin Summary	Type a detailed summary that describes the purpose of the bulletin and any related patches and products.

89. Creating a Custom Patch

The Custom Patch File Editor is not used to create the actual patch file. The patch itself is provided by a vendor (e.g. Microsoft) or is created by your organization. When you create a custom patch within the Custom Patch File Editor you are simply defining how to detect if the patch is missing from target machines and how to deploy the patch.

1. To create a custom patch, within Custom Patch File Editor select **Insert > Add Patch** or click the **Add Patch** toolbar icon ( ). The new custom patch is selected and the patch characteristics are displayed in the right pane.



Use the options in the right-hand pane to create the new patch.
Two major tabs are used in the right-hand pane. For detailed information about the options on these two tabs please refer to the following topics:

- **Scan Information Tab**
- **Deployment Information Tab**

IMPORTANT! You should avoid creating a custom patch that requires user interaction. This is because this is no guarantee how the patch installation process will react if there is no response to a user prompt. The most likely scenario is that it will wait a number of hours before eventually timing out. Use **command line switches** if necessary.

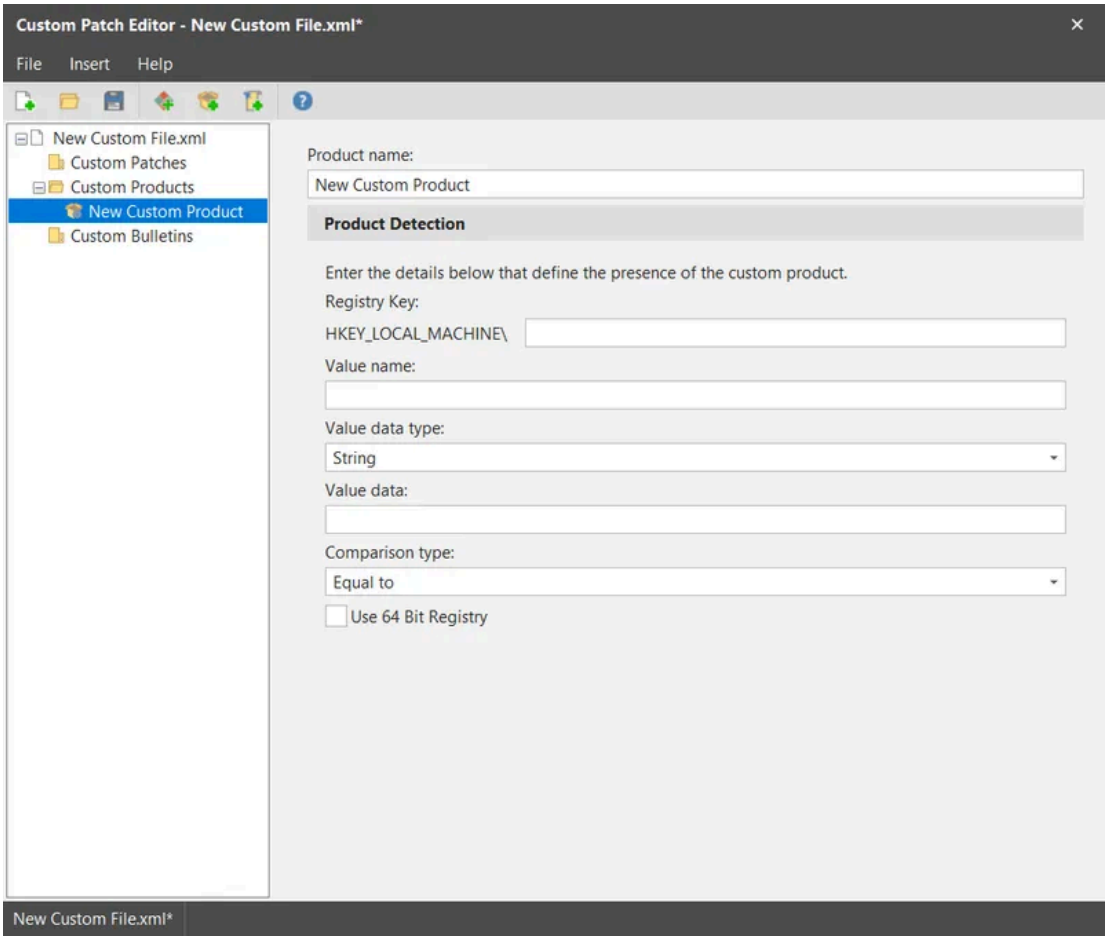
90. Creating a Custom Product

Your organization may use a custom or "home-grown" software product. In order for Security Controls to be able to scan for and patch that product it must be able to detect the product. Creating a custom product provides the registry key information needed for Security Controls to determine whether the custom product exists on the machines it is scanning.

If you have multiple versions of a custom product you must define a unique custom product for each version. For example, assume you currently support both the original version as well as an updated version of a custom CRM product. Within the Custom Patch File Editor you must create a separate custom product for each version.

> TIP: After **importing a new custom XML file**, you can use Patch View to verify the custom product is contained in the updated XML patch data file.

1. To create a custom product, within Custom Patch File Editor select **Insert > Add Product** or click the **Add Product** toolbar icon ( ).
2. Select **New Custom Product** beneath the **Custom Products** folder.
   The new custom product is selected and the product characteristics are displayed in the right pane. For example:
3. Use the options in the right-hand pane to define the new product.



4. When complete, save and then validate the XML file (see **Saving and Validating Your Changes**).

To get the most current registry information we recommend using the Microsoft Registry Editor (regedit), a tool for viewing settings in your system registry. You can copy the required information from this tool to the appropriate fields in this dialog.

Field	Description
Product Name	Provide a unique name for the product. The name cannot match a product name already defined to Security Controls. Once this custom product is defined and saved, the name you provide here will be added to the **Available Products** list that is used during the patch creation process. See the **Targeting** tab section in Patch Scan Information Tab for more information.
Registry Key	You can only specify keys that are relative to the HKEY_LOCAL_MACHINE hive. The easiest and most accurate way to populate this box is to display the desired key from within the Microsoft Registry Editor, copy the key name and then paste the name into this box. The HKEY_LOCAL_MACHINE portion of the name will likely be repeated so you'll need to remove that portion of the name from the box.
Value Name	The name of the specific registry value. You must provide a value and not just a registry key.
Value Data Type	There are two options: • **String:** Specifies that the data must be a string. • **DWORD:** Specifies that the data must be a number.
Value Data	The expected data of the registry value. You can find this value by locating the key within the Microsoft Registry Editor and then looking in the Data column.
Comparison Type	This specifies the test criteria you want to use when determining if a product exists on a scanned machine. While there are many different options here, they can basically be broken down into two categories: Comparisons to value data: The first six options all relate to the value data you specified for the registry key. • **Equal to:** The check passes if the registry value is equal to the reference data • **Not equal:** The check passes if the registry value is not equal to the reference data • **Less than:** The check passes if the registry value is less than the reference data • **Less than or equal:** The check passes if the registry value is less than or equal to the reference data • **Greater than:** The check passes if the registry value is greater than the reference data • **Greater than or equal:** The check passes if the registry value is greater than or equal to the reference data • **Exists, Does not exist:** These two options will simply test whether the registry value itself exists. In either category, if the comparison test passes Security Controls will consider the product installed.
Use 64 Bit Registry	Enable this check box if the registry key is in the 64-bit part of the registry on a 64-bit operating system.

91. Creating a Custom Script

You can create and import your own scripts that will completely integrate into the Security Controls environment. When creating a custom script there are a few basic guidelines you must follow, such as:

- The script must contain metadata that uniquely identifies it and describes its functionality and input parameters
- The script must be signed by an authority that is trusted by the machine that the console is running on
- The script can use any number of variables and functions that are provided by Ivanti and that are designed for use with Security Controls

User scripts can be executed against individual machines and groups of machines in exactly the same manner as executing the scripts provided with Security Controls. Advantages to running scripts in Security Controls include:

- Scripts execute against the machines and machine groups you have already defined in Security Controls
- Use the machine and machine-group credentials you have already entered in Security Controls
- Scripts execute in the background
- Script execution can be run immediately or scheduled to run in the future
- Scripts are executed in parallel against the target machines and usually complete in a fraction of the time that it would take to run them serially and you can control the level of parallelism
- Script output is captured to files that you can review at your convenience
- Status of script execution is displayed within Security Controls
- You can open the result files directly from Security Controls
- Your scripts can be parameterized, and different sets of parameters can be saved in ITScript Templates or provided when you start the script or schedule it for execution
- Scripts can use the PowerShell remoting features, allowing the broadest set of capabilities provided by Windows PowerShell
- Scripts can use PowerShell modules. Different scripts can import different versions of a given module.
- Only scripts signed by authorities that you trust will be allowed to execute
- Security Controls also provides a number of PowerShell variables and functions that help simplify many common operations.

Most PowerShell scripts can be used in Security Controls with only minor modifications. This section describes how to prepare your scripts and import them into Security Controls.

92. Creating or Editing a Deployment Template

To work with a patch deployment template, do one of the following:

- To create a new deployment template, click **New > Windows Patch > Deployment Template**.
- To edit an existing deployment template, in the **My Deployment Templates** list in the navigation pane, click the deployment template name.

> **TIP**: To speed the template creation process, copy an existing template that is similar to the one you want to create. The contents of the copied template will be populated in the new **Deployment Template** dialog and you can simply modify the appropriate items. You copy an existing template by right-clicking it in the **Deployment Templates** pane and then selecting **Copy**.

The **Deployment Template** dialog contains several tabs that collectively define the characteristics of a particular deployment template. The tabs are:

- General tab
- Pre-Deploy Reboot tab
- Post-Deploy Reboot tab
- Email tab
- Custom Actions tab
- Distribution Servers tab
- Hosted VMs/Templates tab
- Used By tab

The dialog also contains **Name**, **Path** and **Description** boxes that apply to the entire template.

Field	Description
Name	The name you wish to assign to this deployment template.
Path	This box is used to specify the folder path that this template will reside in within the **My Deployment Templates** list in navigation pane. If you do not specify a path, the template will at the root level of the **My Deployment Templates** list. For more details, see Organizing Patch Deployment Templates.
Description	A comment that describes the purpose of this deployment template.

Once you have made your selections for this deployment template, click the **Save** button and then the **Close** button to save the template. Click the **Cancel** button and then the **Close** button to close the window without making any changes. Certain types of changes will require you to save the deployment template earlier in the process.

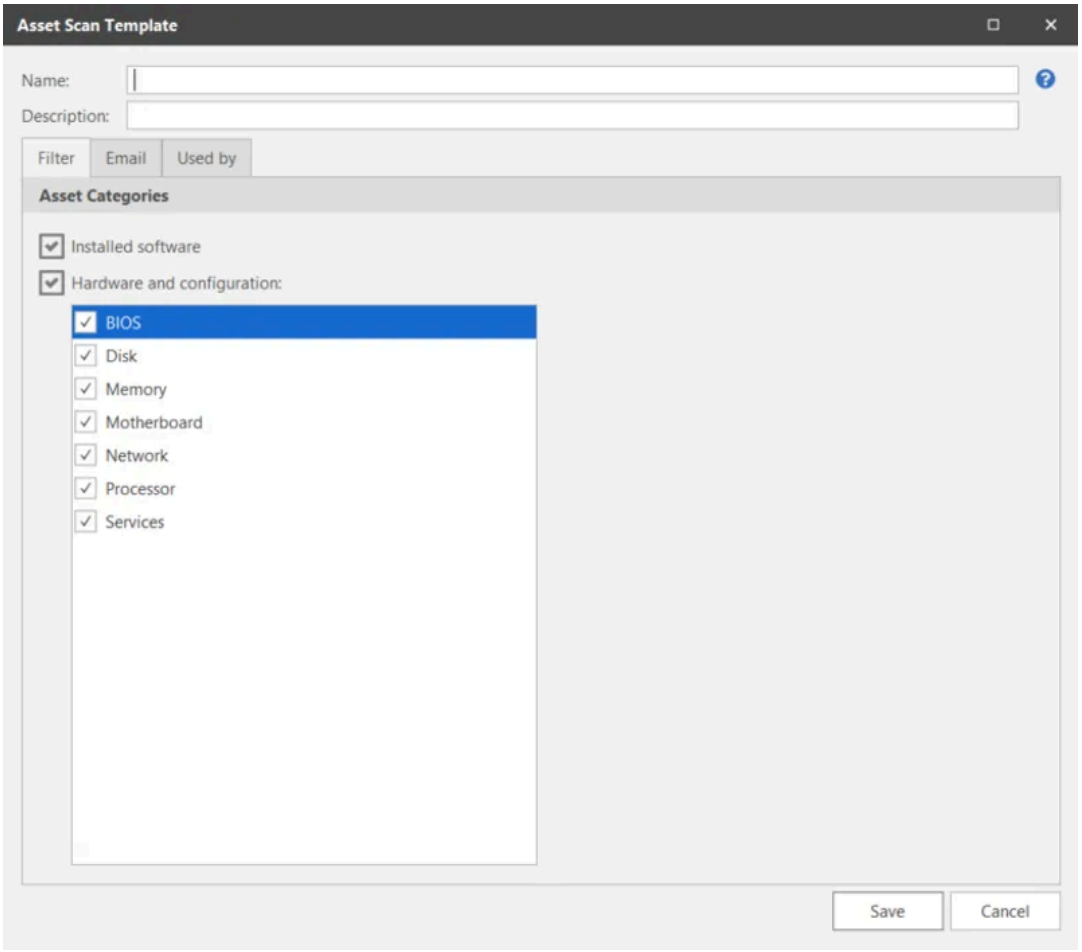
93. Creating a New Asset Scan Template

Security Controls comes with one predefined asset scan template, named **Full Asset Scan**. This template cannot be modified. It will:

- Perform a software asset scan
- Perform a hardware asset scan of all hardware components except services

While this template is fine for most scanning activities, you may desire a higher level of flexibility when scanning machines. To this end, Security Controls includes the ability to create any number of custom asset scan templates.

To create a new asset scan template, from the main menu select **New > Asset Scan Template**. This will display the **Asset Scan Template** dialog.



The **Asset Scan Template** dialog contains three tabs that collectively define the characteristics of the scan template.

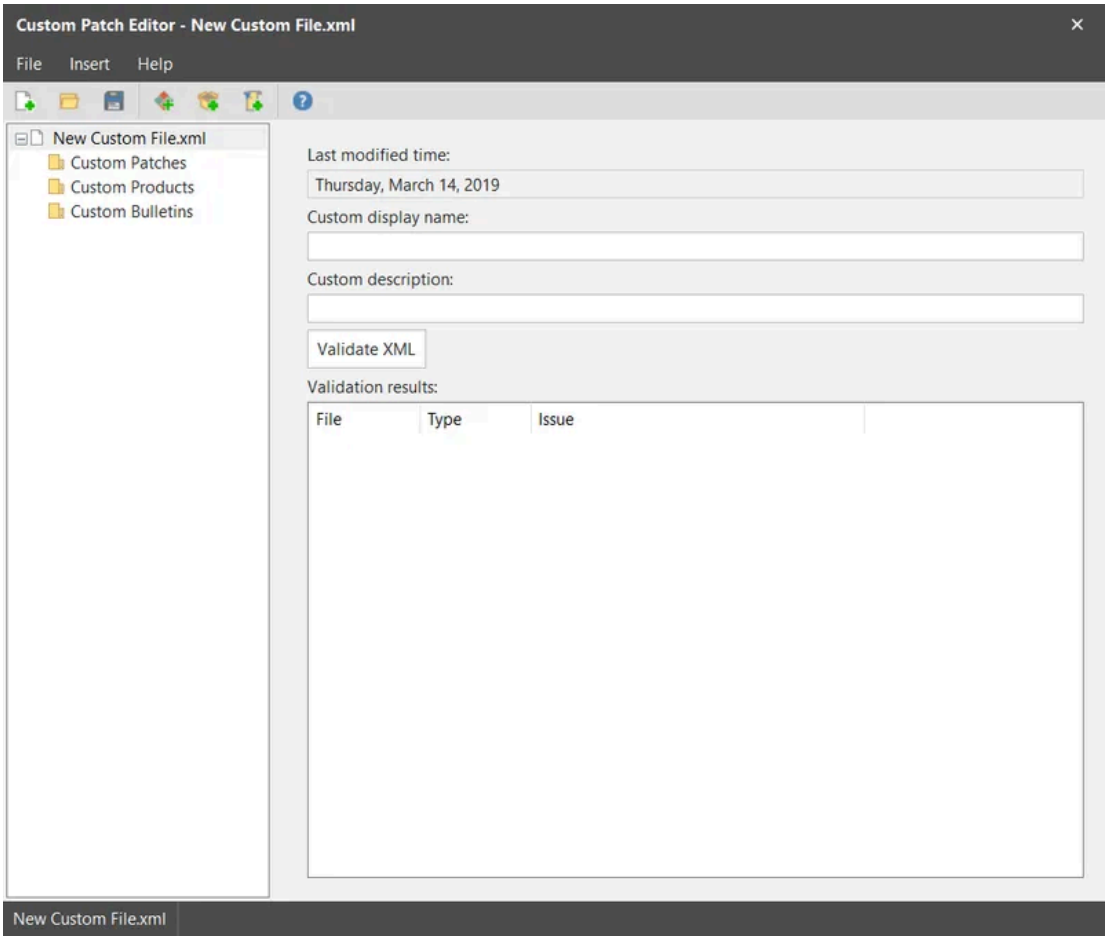
Field	Description
Name	The name that you wish to assign to this scan template.
Description	A description of the template.
Filtering tab	There are three different types of asset scans that can be performed. • **Installed Software:** To scan for the software components contained on a physical machine, an online virtual machine, or an offline virtual machine, enable this check box. • **Hardware and Configuration:** To scan for the hardware components contained on a physical machine or an online virtual machine, enable this check box. Offline virtual machines are ignored by this scan. You can elect to scan for information on a number of different hardware components, including: • BIOS • Disk • Memory • Motherboard • Network • Processor • Services
Email tab	This tab applies only to agentless scans initiated from the console; it does not apply to agents that may also be using this template. This tab enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent when a scan using this template is completed. There are many different reports that can get sent. To understand what a particular report contains, click on the report in the list and view its description immediately above the list. To specify which reports should be automatically sent and to whom they should be sent: New templates must be saved before you can perform these steps. 1. Select a report in the **Reports** list. 2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Save**.
Used By tab	This tab shows you the Favorites and the agent policies that are currently using this asset scan template. This is important to know if you are considering modifying the template, as it tells you what other areas of the program are affected.

To save the template click **Save**. To close the dialog without saving the changes **Cancel**.

94. Creating a New Custom XML File

To create a customized XML file you use the **Custom Patch File Editor**.

1. Access the Custom Patch File Editor by selecting **Tools > Custom Patch Editor**.
   The **Custom Patch File Editor** dialog is displayed.
2. Create a new custom XML file by selecting **File > New** or by clicking the **Create a new custom XML file** link in the right-hand pane.
   The **New Custom File** dialog is displayed.
3. Save the new custom XML file by selecting **File > Save As** and then specifying the name and location of the file.
   You can give the file any unique name you want. The file can be saved anywhere you want, but a logical location is the program's **DataFiles** folder.



4. The **DataFiles** folder is located here: `C:\ProgramData\Ivanti\Security Controls\Console\DataFiles`

This is the directory used to store all the other XML files used by the program.

Use the fields in the right-hand pane to define the file characteristics.

5. Define the bulletins, products, and patches you want included in this custom XML file.

Field	Description
Last Modified Time	This read-only field indicates the last time the custom XML file was changed.
Custom XML Display Name	Type a unique name for the file.
Custom XML Description	Type a description that explains the purpose of the file.
Validate XML	To verify that the XML file is properly formed and valid, click this button. You should validate the XML file anytime you make modifications to the XML file. Be sure to save the file before performing the validation to ensure that you are validating the most current file.
Validation Results	Displays the results of the most recent validation check.

If creating a patch for a new product:	**Then create the items in this order:** 1. **Create the new custom product.** 2. **Create a new bulletin, or tie the patch to an existing bulletin.** 3. **Create the new patch.**
If creating a patch for an existing product:	Then create the items in this order: 1. Create a new bulletin, or tie the patch to an existing bulletin. 2. Create the new patch.

For details, see the following topics:

- Creating a Custom Product
- Creating a Custom Bulletin
- Creating a Custom Patch

95. Creating a New Security Controls Agent Policy

Overview Information

An agent policy defines exactly what an agent can or cannot do. With Security Controls Agent you can create as many different agent policies as is needed. This provides a great deal of flexibility, enabling you to assign different agent policies to different machines in your organization.

All agent policies are configured on the Security Controls console and then either "push installed" to the desired target machines or installed manually. An agent policy can be configured with any combination of patch, asset, and/or power management capabilities.

To create a new Security Controls Agent policy:

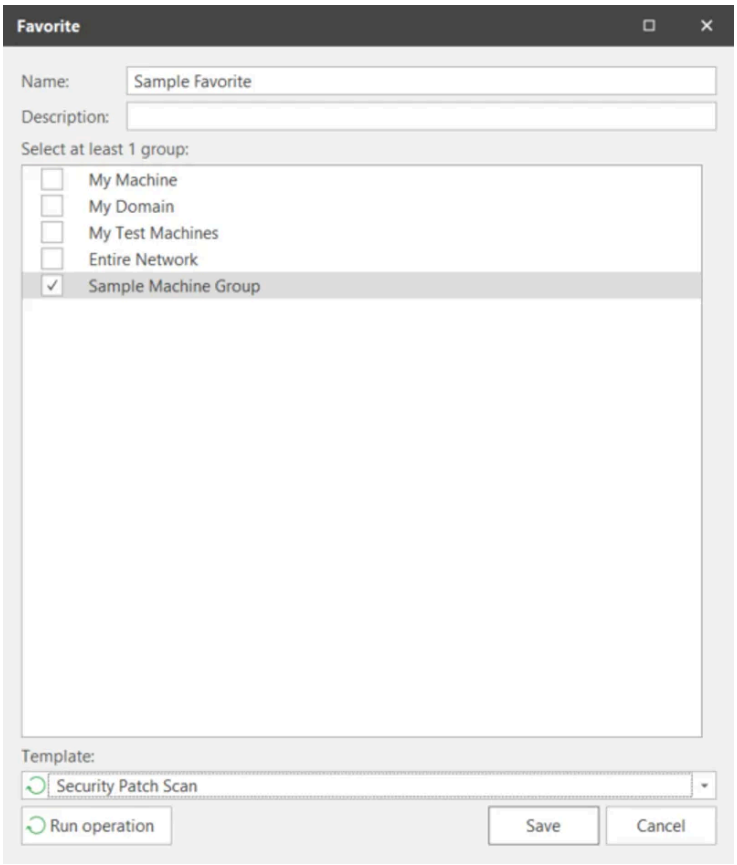
1. From the main menu select **New >Agent Policy**.
2. Type a name for the new agent policy and then click **OK**.
   The **Agent Policy Editor** window is displayed.
3. See the following topics for information on configuring the agent policy:
   - Configuring General Settings
   - Configuring Reboot Options
   - Configuring Patch Tasks
   - Configuring Asset Tasks
   - Configuring Power Tasks
   - Configuring Maintenance Windows

96. Creating Favorites

A favorite is a marriage between machine groups and a template. It consists of one or more machine groups and one template (a patch scan template, an asset scan template, or a power template). You select one or more machine groups and then select a template that specifies what operation to perform on the machines.

To create a new favorite:

1. From the main menu select **New > Favorite**.
   The **Favorite** dialog is displayed.



Give the favorite a unique name (e.g. "Domain Controllers").

3. If desired, provide a description.
   For example "This favorite consists of only domain controllers and will be scanned using the Security Patch Scan template".
4. In the **Select at least 1 group** list, select which machine groups you would like to include in this favorite.

> If you elected to **exclude certain machines** from one or more machine groups, the exclusions will apply to all machine groups you include in this favorite.

Select the template you want to use when performing the desired operation on the machines.

6. Click **Save**.
   A new entry will appear in the **Favorites** pane.

97. Creating Machine Groups

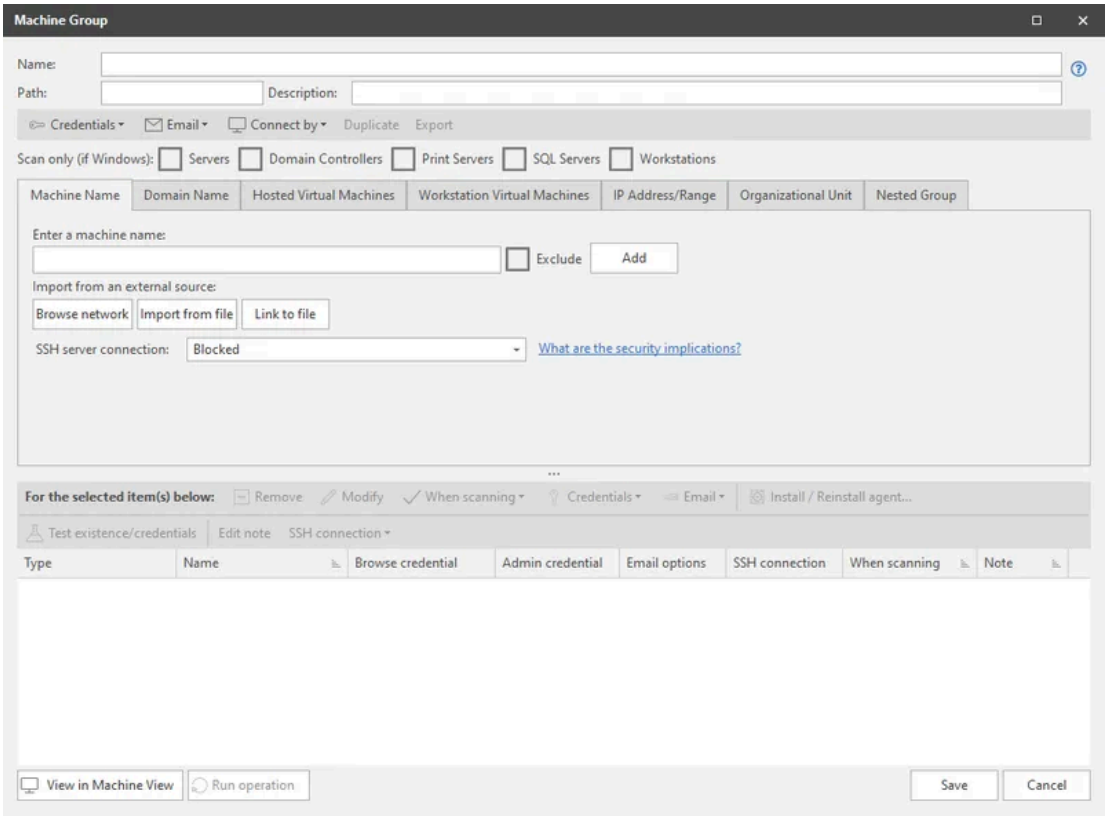
> To import an existing machine group, select **Import > Machine Group**.

There are two ways to create a new machine group:

- From the main menu, select **New > Machine Group**
- In the navigation pane, right-click on either the **Default Machine Groups** list or the **My Machine Groups** list and then select **New Machine Group**

The **Machine Group** dialog is displayed. You must provide a name for the new machine group. If you want to add the group to a new or existing folder in the navigation pane, type a folder path into the **Path** box; see Organizing Machine Groups for more information. You can also provide an optional description that identifies the purpose of the group.

For information on configuring the new machine group, see Machine Group Dialog: Middle Section.



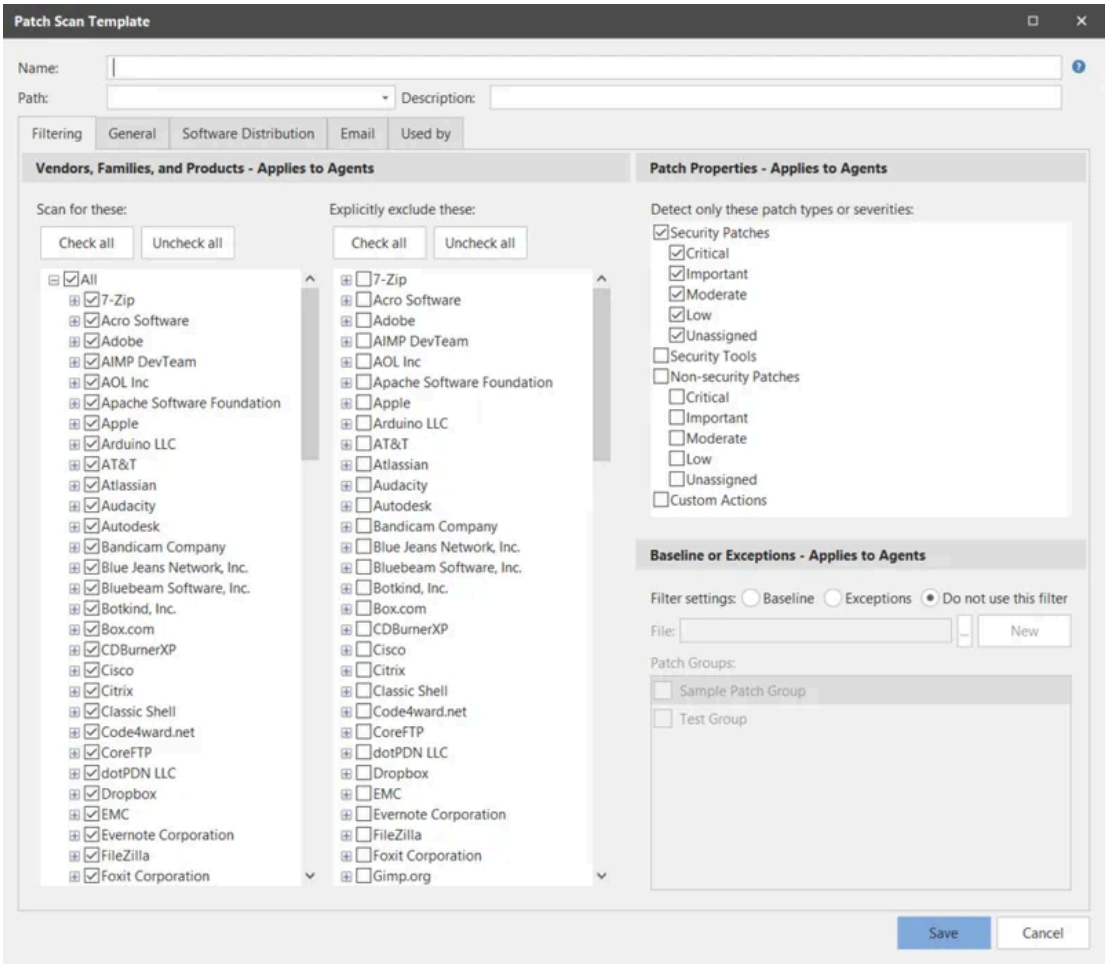
98. Creating or Editing a Patch Scan Template

To work with a patch scan template, do one of the following:

- To create a new scan template, click **New > Windows Patch > Patch Scan Template**.
- To edit an existing scan template, in the **Patch Scan Templates** list in the navigation pane, click the patch scan template name.

This will display the **Patch Scan Template** dialog.

> TIP: To speed the template creation process, copy an existing template that is similar to the one you want to create. The contents of the copied template will be populated in the new **Patch Scan Template** dialog and you can simply modify the appropriate items. You copy an existing template by right-clicking the template name in the **Patch Scan Templates** list and then selecting **Copy**.



The Patch Scan Template dialog contains several tabs that collectively define the characteristics of a particular scan template.

Field	Description
Name	The name that you wish to assign to this scan template.
Path	This box is used to specify the folder path that this template will reside in within the **Patch Scan Templates** list in navigation pane. If you do not specify a path, the template will reside at the root level of the **My Patch Scan Templates** list. For more details, see Organizing Patch Scan Templates.
Description	A description of the template.
Filtering tab	There are three different filters available on this tab. • **Vendors, Families, and Products filter:** Scan for or exclude patches for the specified vendors, product families, and product versions. The items are presented in a hierarchical list. If you enable a check box at one level, all check boxes at lower levels are also enabled. If the same item is checked in both the **Scan for** and **Explicitly exclude** lists, the item will be excluded. • TIP: If you want to exclude a small number of items, the recommendation is to include all items in the **Scan for** list and then use the **Explicitly exclude** list to exclude the desired items. This works because items in the **Explicitly exclude** list override items in the **Scan for** list. Another option is to use just the **Scan for** list and clear the check boxes of the items you want to exclude, but this is often more time consuming and prone to error. **Patch Properties filter:** Specify the types of patches and the vendor severity level of those patches that should be included in the scan. The options are: ◦ **Security Patches**: Security bulletin related patches. You can choose to scan for one or more specific severity levels. ▪ **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. ▪ **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. ▪ **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. ▪ **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact. ▪ **Unassigned:** Security patches that have not been assigned a severity level. **Security Tools**: Updates for security tools such as Windows Defender and Windows Malicious Software Removal Tool. Also includes certificate updates and hotfixes for known security risks that are not yet fully supported by a

Field	Description
	security bulletin. ◦ **Non-security Patches**: Vendor patches that fix known software problems that are not security issues. You can choose to scan for one or more specific vendor severity levels. See **Security Patches** for a description of the available severity levels. ◦ **Custom Actions**: Enables you to perform custom actions even if you are already fully patched. It does this by scanning for a specific QNumber and patch (QSK2745, MSST-001) that will always be found. This null patch can be remediated but no patch will be deployed. The process uses the temporary file *Nullpatch.exe*. **Baseline or Exceptions filter:** Use this filter to define either a baseline set of patches that should be included or a set of patches that should be excluded. ◦ **Baseline:** Specify a patch list and/or one or more patch groups that collectively represent a baseline set of patches. The baseline is often determined by your corporate security policy and is considered the minimum set of patches that should be installed on your machines. The baseline is considered dynamic because, even though you only define it once on the template, you can continually update the patch list as new patches are made available. For an example of how you might use a baseline filter, see Implementing an Unattended Console Configuration. ◦ The **Vendors, Families, and Products** filter and the **Patch Properties** filter are unavailable when **Baseline** is selected. The **Software distribution** check box on the **Software Distribution** tab will also be ignored. **Exceptions:** Specify a patch list and/or one or more patch groups that contain patches that you always want to be excluded. The **Vendors, Families, and Products** filter and the **Patch Properties** filter will be applied first, and then the patches defined here will be excluded. ◦ Be careful when using the **Exceptions** filter. If you exclude a patch that replaces another patch, the program will now scan for the replaced patch. This is done on purpose to avoid any unintentional vulnerabilities. If the intended consequence of excluding a patch is to not automatically deploy it or the related patches, then all the patches in the chain of replaced patches must also be excluded. **Do not use this filter:** Disables this filter. ◦ **File:** Specify a text file that contains the list of patches you want to use as your baseline or that you want to exclude. To create a text file, click New. The text file must contain just the QNumbers associated with each patch, one entry per line. For an example text file, see Implementing an Unattended Console Configuration. ◦ **Patch group(s):** Specify one or more patch groups that contain the patches you want to use as your baseline or that you want to exclude.
General tab	• **Scan For:** During the scanning process, you can choose to scan for just missing patches or for both missing and installed patches. When scanning for both missing and installed patches, ◦ You can include effectively installed patches in the results. These are patches that replace other patches. See Effectively Installed Patches and Determining Patch Replacements for more information. ◦ You can Scan for Microsoft Preview patches. This option allows users the flexibility to include Microsoft preview patches in the system scans. • The following option applies only to the console, not to agents that may also be using this template. **Global Thread Pool Override:** Specify if you want to override the **Global thread pool** setting on the Tools > Options > Scan dialog. You should only do this if you want to temporarily perform some bandwidth testing with your patch scans. The value you specify in the **Restrict scan to maximum number of threads** box defines the maximum

Field	Description
	number of machines that can be simultaneously scanned during one patch scan. The value specified is the actual limit; it is not multiplied by the number of logical CPUs on the console machine as is done on the **Tools > Options > Scan** dialog. You should clear the box when you have finished your testing.
Software Distribution tab	This tab enables you to specify if you want to scan for free third-party products that can be deployed by Security Controls. If you enable the **Software distribution** check box, the available third-party products will be included in the **Patch Missing** list of the scan results. Use the vertical scroll bar to view the complete list of third-party products supported by Security Controls. If you enable the **Software distribution** check box, a confirmation dialog will be displayed. This is to ensure that you are enabling the check box on purpose and not inadvertently scanning for and **deploying third-party applications**. The products that will be displayed are those that are available for the operating system being used on the scanned machine. If you want to include or exclude reporting on a particular product, specify that product in the **Vendors, Families, and Products** filter on the **Filtering** tab.
Email tab	This tab applies only to agentless scans initiated from the console; it does not apply to agents that may also be using this template. This tab enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent when a scan using this template is completed. There are many different reports that can get sent. To understand what a particular report contains, click on the report in the list and view its description immediately below the list. To specify which reports should be automatically sent and to whom they should be sent: New templates must be saved before you can perform these steps. 1. Select a report in the **Reports** list. 2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Save**.
Used by tab	This tab shows you the Favorites and agent policies that are currently using this scan template. This is important to know if you are considering modifying the template, as it tells you what other areas of the program are affected.

99. Credential Handling and Authentication Fallback Behavior

Ivanti Security Controls supports Integrated Authentication to enable modern security features such as MFA, RSA tokens, and CAC/smart cards. When the Console Server connects to managed machines, it follows a defined authentication sequence designed to balance flexibility and security.

When connecting to managed machines, the Console Server uses configured machine credentials and may fall back to the interactive user account under which the Console UI is running. This behavior enables secure, centralized authentication without widespread password distribution.

Ivanti recommends the following best practices to use the features more securely:

- **Use Kerberos**: Wherever possible, use Kerberos and configure your environment to prefer it over legacy protocols like NTLM.
- **Secure SMB communications**: Disable SMBv1, enable SMB signing, and use SMBv2 or SMBv3 only.
- **Run the Console Server under a dedicated, least-privilege service account**: Avoid domain administrator or personal user accounts.
- **Disable insecure name resolution protocols**: Disable protocols such as LLMNR, mDNS, and unnecessary NetBIOS.
- **Monitor and audit authentication activity**: Identify misconfigurations or unexpected behavior.
- **Maintain strong credential hygiene**: Include regular credential rotation, valid certificates, and synchronized system time.

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Performing Patching in a Disconnected Environment

100. Credential Precedence for Offline Hosted Virtual Machines

Initiating actions from the Agentless Operation page, from a machine group, or from a favorite

The **Agentless Operation page**, machine groups and **favorites** can be used to initiate **patch scans**, **asset scans**, **power management** actions, and to **execute scripts**. When performing these actions, Security Controls will attempt to authenticate to each offline hosted virtual machine using the **browse credentials**.

Initiating actions from Machine View or Scan View

When initiating a scan, a **patch deployment** or **a power management action** from Machine View or Scan View, the credentials that will be used to authenticate to an offline virtual machine depends on the power state of the machine when it was initially scanned.

If a machine was originally scanned in offline mode

The program will attempt to authenticate using the **browse credentials**.

If a machine was originally scanned in online mode

The program will attempt to authenticate using a variety of credentials and will do so using the following strategy:

1. Try using any manually or automatically assigned managed machine credentials (see the *Assigning Credentials to Virtual Machines* section in **Supplying Credentials for Machines**.
2. If the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:
    - (a) The administrator credential from the machine group. If the administrator credential exists but fails, the default credentials will not be tried.
    - (b) **Default Credentials** (used if the scan credentials are invalid or missing (for example, if an agent performed the scan rather than the console))

If the credentials used above do not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

> Integrated credentials will not work for **deployments to offline virtual machines** or for **rescans**.

If none of these credentials work then the action will fail.

See also:

Deploying Patches to Virtual Machines

101. Credential Precedence for Physical Machines and Online Virtual Machines

Initiating actions from the Agentless Operation page, from a machine group, or from a favorite

The Agentless Operation page, machine groups and favorites can be used to initiate patch scans, asset scans, power management actions, and to execute scripts. When performing these actions, Security Controls will attempt to authenticate to each machine using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:
    - Machine-level credentials (see the **To Individual Machines in a Machine Group** section in Supplying Credentials for Machines)
    - Group-level credentials (see the **To All Machines in a Machine Group** section in Supplying Credentials for Machines)
    - Default credentials (see Managing Credentials)

Example: If machine-level credentials are not available but group-level and default credentials are available, the program will use the group-level credentials.
If the credential used above does not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

If neither of these credentials work the scans and the power management tasks will fail.

One suggestion is to make your default credentials the same as the account credentials you typically use to log on to the program. This will eliminate problems that may occur if you forget to assign credentials.

Initiating an agent installation from a machine group

When using a machine group to push install the Security Controls Agent service to connected target machines, the credentials used by the program follows the same strategy as above with one major exception -- integrated credentials will not be used. So the agent installation must be successful using machine-level, group-level, default, or explicitly supplied credentials.

Initiating actions from Machine View or Scan View

When initiating a scan, a patch deployment or a power management action from Machine View or Scan View, the program will attempt to authenticate to the target machines using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:
    - Any manually or automatically assigned managed machine credentials (see the **To Individual Machines in a Machine Group** section in Supplying Credentials for Machines and the **Credential** option on the Manage Machine Properties dialog)
    - Default Credentials (used if the machine credentials are missing)

If the credential used above does not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

> Integrated credentials will not work for **deployments to offline virtual machines** or for **rescans**.

If neither of these credentials work then the action will fail.

Initiating an agent installation from Machine View or Scan View

When **using Machine View or Scan View to push install the Security Controls Agent service** to connected target machines, the credentials used by the program follows the same strategy as immediately above with one major exception -- integrated credentials will not be used. So the agent installation must be successful using managed machine credentials, default credentials, or explicitly supplied credentials.

102. Customizing the Column Headers

Show Me!

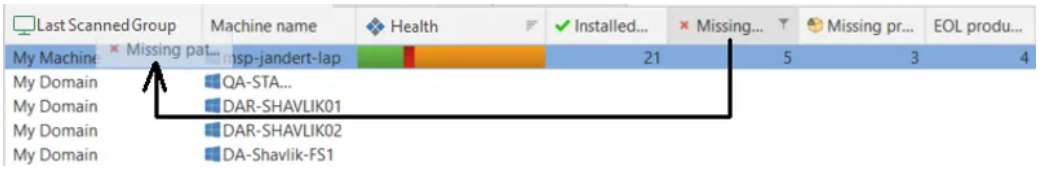
A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

You can easily customize the way information is displayed within any of the panes in Machine View or Scan View.

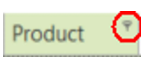
- You can reorder the columns by clicking and dragging the column headers to new locations.
- For example, if you want missing patch information to be displayed in the first column of the top pane, simply click on the **Missing Patch Count** icon and drag it to the first column.



TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

You can apply filters to one or more column headers.

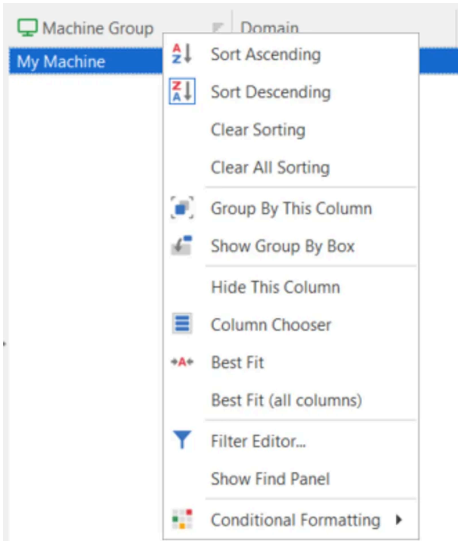
- Hover over a column header and then click the filter icon located in the upper-right corner. For example:

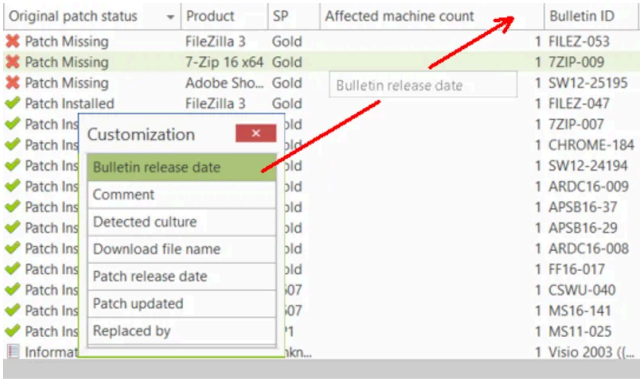


Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied to the current display, and you can edit the filter. For example:



You can right-click within a column header and perform a number of additional actions.



Action	Description
Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One "Group By" box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area. The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and hide information within a pane. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the pane. Simply click and drag the desired column headers from the table to the Customization dialog. For example, if you decide you want to add the Bulletin release date column to the table, simply drag that column header from the Customization dialog to the table.  If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.

Action	Description
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.
Best Fit (all columns)	Resizing the width of all columns in the table so that the header text is displayed in the optimal amount of space.
File Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.
Conditional Formatting	Enables you to highlight information within the table based on criteria that you set.

103. Customizing the Column Headers

Show Me!

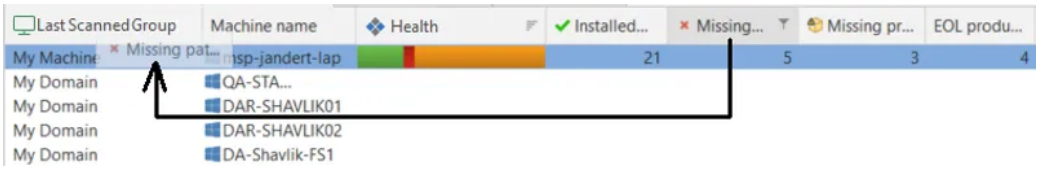
A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

You can easily customize the way information is displayed within any of the panes in Machine View or Scan View.

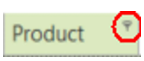
- You can reorder the columns by clicking and dragging the column headers to new locations.
- For example, if you want missing patch information to be displayed in the first column of the top pane, simply click on the **Missing Patches** icon and drag it to the first column.



TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

You can apply filters to one or more column headers.

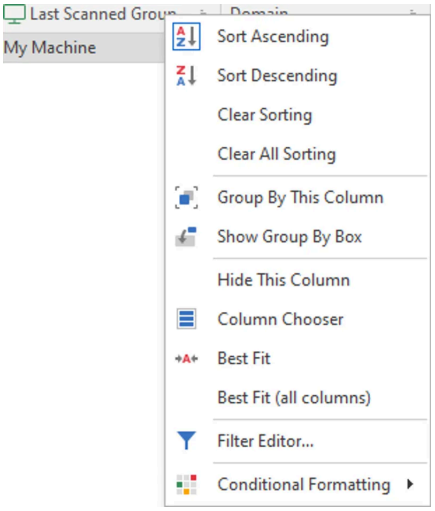
- Hover over a column header and then click the filter icon located in the upper-right corner. For example:

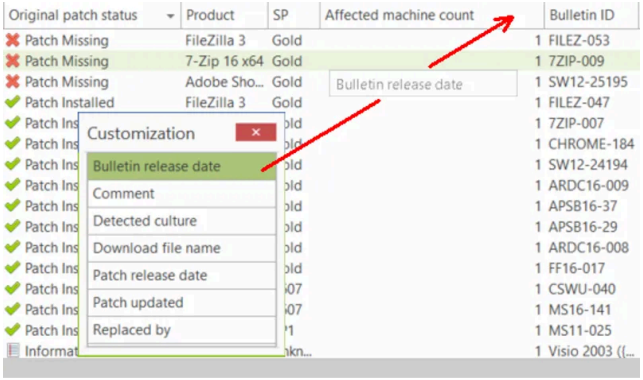


Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied to the current display, and you can edit the filter. For example:



You can right-click within a column header and perform a number of additional actions.



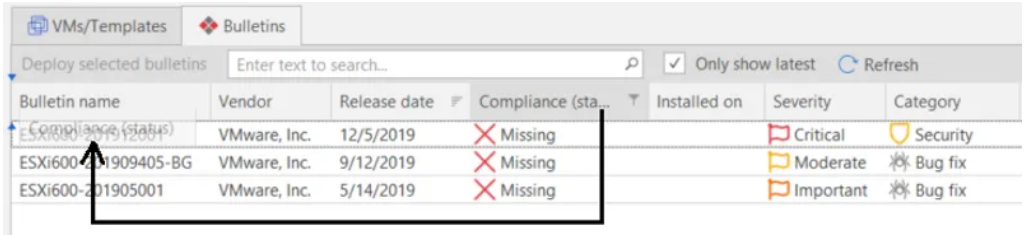
Field	Description
Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Clear All Sorting	Clears the sorting criteria currently set for any column in the table.
Group By This Column	Groups the table by the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One Group By box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area. The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and hide information within a pane. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the pane. Simply click and drag the desired column headers from the table to the Customization dialog. For example, if you decide you want to add the Bulletin release date column to the table, simply drag that column header from the Customization dialog to the table. 

Field	Description
	If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.
Best Fit (all columns)	Resize the width of all columns in the table so that the header text is displayed in the optimal amount of space.
Filter Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.
Conditional Formatting	Enables you to highlight information within the table based on criteria that you set.

104. Customizing the Column Headers

You can easily customize the way information is displayed within any of the Virtual Inventory panes.

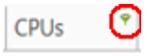
- You can reorder the columns by clicking and dragging the column headers to new locations.
- For example, if you want missing bulletin information to be displayed in the first column, simply click on the **Compliance (Status)** column header and drag it to the first column.



TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

You can apply filters to one or more column headers.

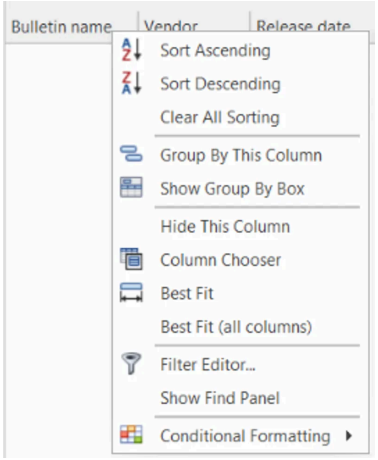
- Hover over a column header and then click the filter icon located in the upper-right corner. For example:



Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied and to edit the filter. For example:



You can right-click within a column header and perform a number of additional actions.



Command	Description
Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / **Hide Group By Box**	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One Group By box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area. The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and hide information within a pane. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the pane. Simply click and drag the desired column headers from the table to the Customization dialog. If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.
Best Fit (all columns)	Resize the width of all columns in the table so that the header text is displayed in the optimal amount of space.
File Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.
Show Find Panel / **Hide Find Panel**	Displays or hides a search box that you can use to find specific patches or text related to any of the patches contained in the patch data file. Here are a few tips for using the search box: • The search works only on the information currently visible in the grid • All partial matches are displayed

Command	Description
	• The use of wildcards is not allowed
Conditional Formatting	Enables you to highlight information within the table based on criteria that you set.

105. Customizing the Patch View Column Headers

Show Me!

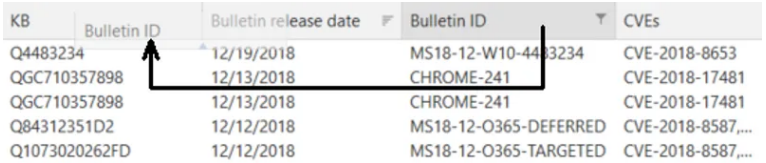
A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

You can easily customize the way information is displayed within Patch View.

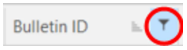
- You can reorder the columns by clicking and dragging the column headers to new locations.
- For example, if you want Bulletin ID information to be displayed in the first column of the top pane, simply click on the Bulletin ID icon and drag it to the first column.



TIP: When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

You can apply filters to one or more column headers.

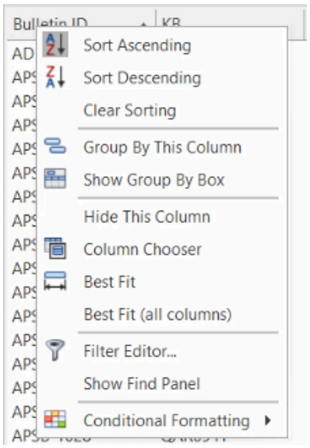
- Hover over a column header and then click the filter icon located in the upper-right corner. For example:

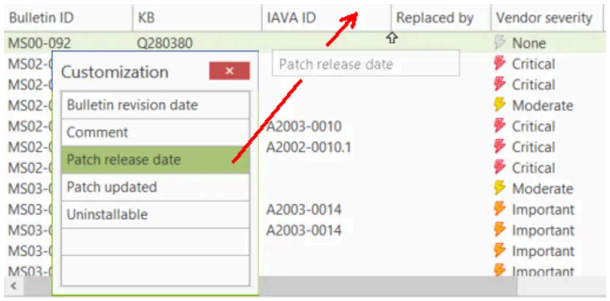


Use the filter menu to select which of the values currently contained in the column should be displayed. When you apply a column filter, the filter definition will be displayed beneath the pane. You can use this to confirm which column filters have been applied to the current display, and you can edit the filter. For example:



You can right-click within a column header and perform a number of additional actions.



Action	Description
Sort Ascending	Sorts the selected column in ascending order. The table will be sorted first using the information in the first column and then by the column you selected.
Sort Descending	Sorts the selected column in descending order. The table will be sorted first using the information in the first column and then by the column you selected.
Clear All Sorting	Clears the ascending or descending sorting criteria currently set for a column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One "Group By" box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area. The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**.
Column Chooser	Enables you to add and remove information from Patch View. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you don't currently want displayed within the table. Simply click and drag the desired column headers from the table to the **Customization** dialog. For example, if you decide you want to add the **Patch release date** column to the table, simply drag that column header from the **Customization** dialog to the table.  If you decide you want an item back in the table, simply click and drag it from the Customization dialog back to the table.
Best Fit	Resize the width of the selected column so that the header text is displayed in the optimal amount of space.

Action	Description
Best Fit (all columns)	Resize the width of all columns in the table so that the header text is displayed in the optimal amount of space.
Filter Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.
Conditional Formatting	Enables you to highlight information within the table based on criteria that you set.

106. CVE view

The Reporting2.CVE view (Common Vulnerabilities and Exposures) displays the common vulnerability and exposure name and the CVSS scores of a patch as it applies to a product.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
Name	nvarchar(20)		The name of the CVE.
CVSSv2	int		The Common Vulnerability Scoring System (CVSS) version 2 score.
CVSSv3	int		The Common Vulnerability Scoring System (CVSS) version 3 score.

107. Database Maintenance

In order to keep Security Controls operating at peak efficiency, it is important to perform periodic maintenance on your database. The database maintenance tool enables you to:

- View and delete old results
- Rebuild your SQL Server indexes
- Create backups of your database

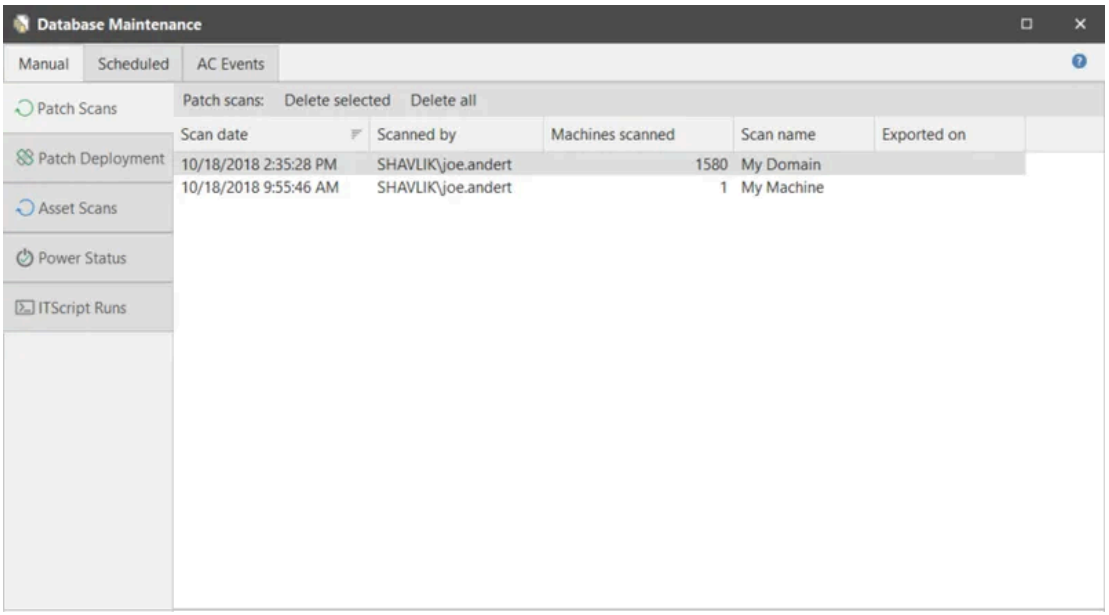
In this section:

- Manual Maintenance
- Scheduled Maintenance

You do this by selecting **Manage > Database Maintenance** and then specifying exactly when and how your database maintenance tasks should be performed.

Manual Maintenance

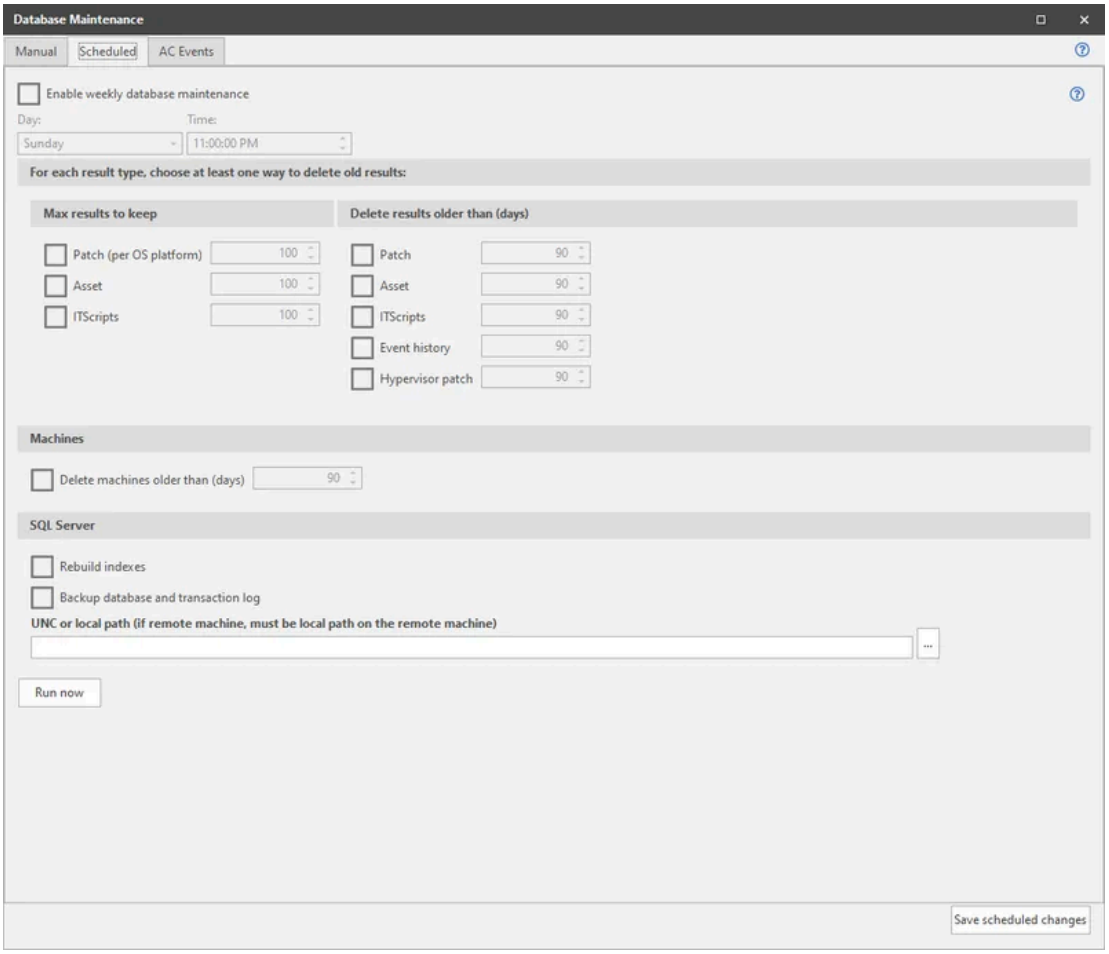
You can get a complete list of available prior scans, script executions, and patch deployments by selecting the **Manual** tab.



If you want to delete certain items in a list, select the desired items in the list and then click **Deleted Selected**. If you would like to remove all items in a list, click **Delete All**. Deleting an item here also deletes it from its associated list (Today's Items, Recent Items, or Archive Items) in the Results pane and permanently removes it from the database.

> TIP: When deleting a large number of items it is smarter to schedule a database maintenance task. The scheduled task will be performed in the background and allow you to perform additional console tasks at the same time. Manual deletions are performed in the foreground and you must wait for the task to complete before performing additional console tasks.

Scheduled Maintenance



If the options on this dialog are unavailable it probably means that another administrator currently has control over the database maintenance operations. See the **Take ownership** option (below) for more details.

Field	Description
Enable weekly database maintenance	If enabled, will perform database maintenance tasks on the specified day and time. The scheduled job is managed by the Security Controls console service; the job cannot be tracked using the Scheduled Task Manager. Maintenance tasks should be performed after hours or on a weekend when database use is at a minimum. If this check box is not enabled you can still configure the remaining database maintenance options on this dialog, but in order to run the maintenance task you must initiate it using the **Run now** button. The database maintenance tasks will not be performed on a regularly scheduled basis.
For each result type, choose at least one way to delete old results	There are two ways to delete old results: • **Max results to keep:** Enables you to specify the maximum number of patch scans, asset scans and script run records you want to store in the database. If the specified number is exceeded, scans will be deleted based on their age (the oldest scans are deleted first). Any patch deployments that are associated with the scans are also deleted. Valid values are 10 - 10,000 for each scan type. • Be careful if you are using Security Controls Agent on your machines. Agents report their results to the console and each result constitutes a scan. If you have many agents there is a chance of exceeding the threshold rather quickly. In this scenario you should consider using the **Delete results older than (days)** option. **Delete results older than (days):** Enables you to specify the maximum number of days that patch results, asset results, event logs, and script run records are allowed to be stored in the database before being deleted. Any patch deployments that are associated with the scans are also deleted. Valid values are 1 - 10,000 days. As a general rule, results that are over 90 days old should be considered too old to accurately depict the current state of your organization. If you choose to implement both methods for a result type, the method that deletes the least number of results is the one that will be used. **Example:** Assume that for patch results you specify **Max results to keep** = 100 and **Delete results older than (days)** = 90. Also assume that there are 150 patch results currently stored in the database but only 10 of them have been there for more than 90 days. When the database maintenance task is run the oldest 10 results will be deleted; the 140 results that are less than 90 days old will be left alone. Each result type consists of the following: • **Patch:** Patch scans and any associated patch deployments • **Asset:** Asset scans • **ITScripts:** Script run records • Event history: Log entries for operational events such as database maintenance and synchronization activities • **Hypervisor patch:** ESXi hypervisor scans and bulletin deployments
Delete machines older than (days)	Enables you to specify the maximum number of days that inactive machines are allowed to be stored in the database before being deleted. An inactive machine can be a machine that has not checked in with the console, been assessed or been included in a patch deployment for the specified number of days. Valid values are 45 - 10,000 inactive days. The default value is 90. As a general rule, machine results that are over 90 days old should be considered too old to accurately depict the current state of your organization.

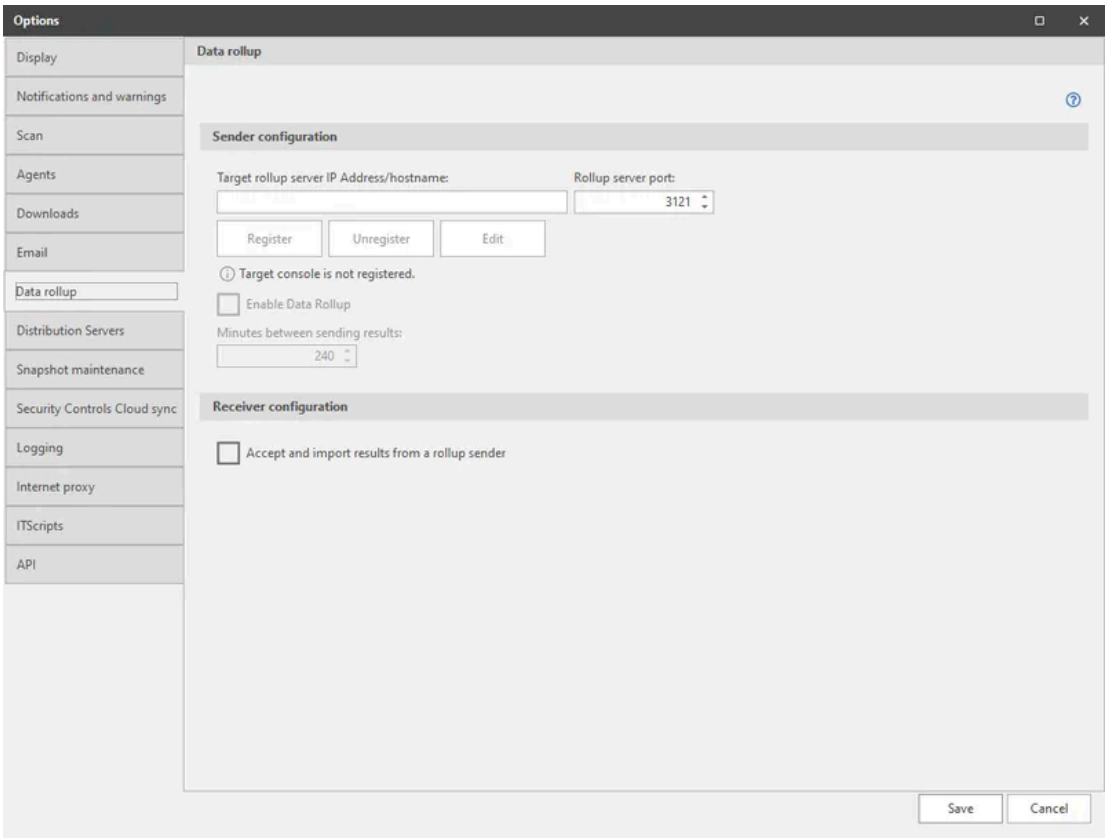
Field	Description
	Another method for deleting inactive machines is to use the REST API. For details, see: **Machines in the API help (opens a new window)**. Security Controls automatically frees up one **license seat** for any machine that has been inactive for more than 45 days, but no machines are automatically deleted from the database unless specified here.
Rebuild indexes	If enabled, each time the database maintenance task is performed it will instruct SQL Server to rebuild the database indexes after the old result data are removed. Doing so will improve the performance of your database. This is particularly valuable when deleting large amounts of data. This option will work on any of the supported editions of SQL Server but it is best suited for use with SQL Server Express editions. If you are using a full edition of SQL Server you might consider using the SQL Server Maintenance Wizard because it provides more control and functionality.
Backup database and transaction log	If enabled, each time the database maintenance task is performed it will instruct SQL Server to create backup copies of the database and the transaction log before removing any data. You must specify where the backup files will be written. You can use either a UNC path (for example: \\server\backup) or a local path (for example: c:\backup) to specify the backup location. The recommendation is to use a UNC path format that specifies a location on a different machine than the one currently running SQL Server. The path name you specify here is simply passed along for use during the backup. No validation is performed on the name. **Notes:** • If you are using a remote SQL Server and you specify a local path, the path you are specifying is located on the remote SQL Server and NOT on the console machine. • If you specify a UNC path to a location on SQL Server, your SQL Server account must have access to the path. If a built-in account is being used (such as Local System or Network Service) then the machine account needs access to the path.
Take ownership	This button is only displayed if you have two or more consoles that share one database. If your organization uses multiple Security Controls consoles that share the same database, only one console will be authorized to use the Database Maintenance tool. If an administrator at another console wants to perform maintenance on the database, that administrator must take ownership of the task before the program will allow the administrator to continue. Any existing maintenance tasks will be allowed to complete before ownership is transferred to another administrator.
Run now	Immediately initiates the database maintenance task. The task is run in the background and requires no user intervention. The task is performed using the current configuration. The current configuration is saved for future use, and if the **Enable weekly database maintenance** check box is enabled this will also schedule the database maintenance task. You can use the **Event History log** to track the progress of the maintenance task. In addition, after the task completes there should be fewer items in the **Results list** and in the **Database Maintenance** list. If you have access to SQL Server Management Studio you can also use its Database Properties feature to track the progress of the task.
Save scheduled changes	Saves the current database maintenance configuration. If the **Enable weekly database maintenance** check box is enabled this will also schedule the database maintenance task.

About the Different Result Types

108. Data Rollup Options

The **Data Rollup** tab enables you to specify how this console will interact with agents and with other consoles.

> Data rollup is for Windows data only.



Field	Description
Enable Data Rollup **Rollup server IP Address/hostname**	If you want this console to roll up and send its scanning and deployment data to a central console, enable this check box. The other options in this area are not available unless this check box is enabled. Specify the IP address or hostname of your Security Controls rollup console. The rollup console will receive scanning and deployment data that is rolled up to it from this console.
Rollup server port	Specify the port used by the rollup console to listen for incoming data from agents and other consoles. The default value is 3121.
Register	To enable this console to send results to the rollup console, click **Register**. This will establish a secure binding between this console and the rollup console. TIP: The registration process will also automatically generate an entry in the **Edit Console Description** dialog on the central console. You can use this dialog to track how many remote consoles are configured to roll up their results to the central console. See Editing the Console Description for more details.
Minutes between sending results	Specify how often you want data from this console to be sent to the rollup console. Valid values are from 10 - 10080 (10 minutes - one week). The default value is every 240 minutes (four hours). Although you can roll up data as often as once every 10 minutes, this is typically impractical. How often you choose to roll up data will depend on a number of things, including how often the console is performing scans and deployments, and how often you want that information reflected in the aggregate database on the rollup console.
Accept and import results from a rollup sender	If enabled, this console will act as a rollup console and will accept scan and deployment data that is sent to it from other consoles. In addition, the sending console(s) must register with this console in order to complete the data rollup configuration. The `C:\ProgramData\Ivanti\Security Controls\Console\Arrivals` directory will be used to store results sent to this console by Security Controls Agent and/or by other consoles.

109. Managing Data Files and Missing Patches in Disconnected Mode

When running in disconnected mode it is necessary to manually manage your data definition files. You can do this two different ways:

- **If your console has an Internet connection:** Select **Help > Refresh files**. This will download the most current versions of the data files and the command files used by the program.
- **If your console does not have an Internet connection:** You must use a machine with Internet access to download the data files and then transfer the files to the Security Controls console. To determine the locations currently being used as the source for the engine components and data definition files, select **Tools > Options > Downloads**.

Data File Locations

The data files need to be located in the following directory on the Security Controls console: `C:\ProgramData\Ivanti\Security Controls\Console\DataFiles`

Downloading Missing Patches

Before you can deploy missing patches you must locate and transfer the missing patches to the disconnected console.

1. Use Machine View to view the list of missing patches.
2. Export the list of missing patches to a .csv file by right-clicking **Patch Missing** and selecting **Export selected patches to CSV**. You can use the .csv file as a reference when downloading the patches from an Internet-facing console. Another option is to generate a report that lists the missing patches.
3. On an Internet-facing console, use the Patch View smart filters to locate the patches that are missing on the disconnected console.
4. Right-click the patches and download them to the Internet-facing console.
   The downloaded patches are stored in the following directory: `C:\ProgramData\Ivanti\Security Controls\Console\Patches`
5. Copy all the files in this folder to a media that can be transported to the disconnected console.
6. Copy all the files to the same folder on the disconnected console.

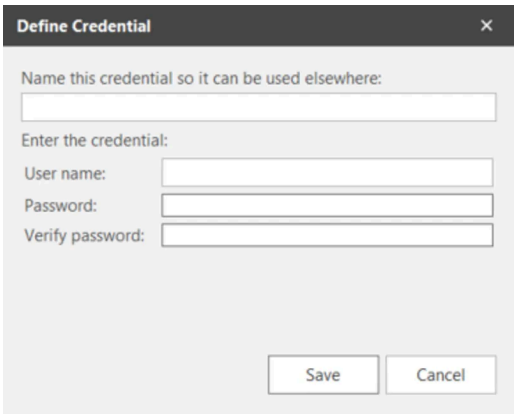
The disconnected console can now deploy patches to the inside machines.

110. Defining Credentials

The **Define Credential** dialog can be accessed anywhere a credential is used within the Security Controls interface (for example, from a **machine group**, from the **Credentials Manager**, etc.). It is used to specify a new user name and password pair that collectively define one credential. The credential is protected with RSA 2048/AES 256 encryption. Security Controls abides by NIST cryptography guidelines and always uses FIPS 140-3 certified cryptographic modules.

Only the administrator that creates the credential will be able to decrypt the credential and access it from within the program. You can, however, elect to **share the credential**, in which case it will be made available to the specified users and/or to Security Controls service components.

> Credentials may be automatically defined for you during a product upgrade or when importing a machine group. Any credentials that are found during these processes are preserved and will be assigned friendly names according to their usage. The term *Discovery filter* is the friendly name assigned by the program to a machine group credential that it identifies during an upgrade or import process. Feel free to change the name to something that more closely reflects the usage of the credential in your organization.

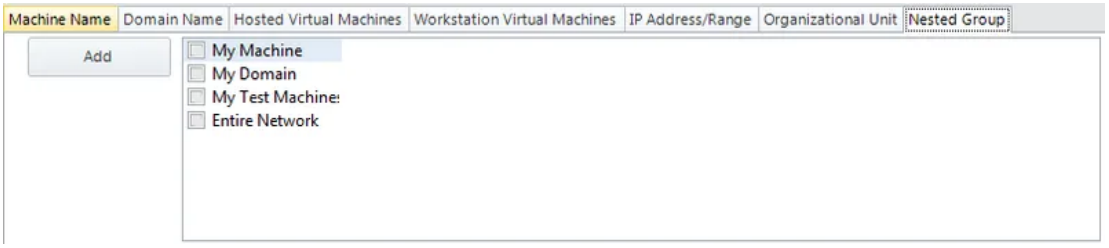


> If you want the credential to be shared with other users and/or with background services, see **Shared Credentials**.

Field	Description
Name this credential so it can be used elsewhere	Provide a friendly name for this credential that describes exactly where it should be used.
User name	Type a user name that has access to the machine(s). When specifying the user name: • If you need to specify a domain as part of the credentials be sure to include the domain name as part of the user name. For example, if you enter User@<Domain>, <Domain>\User, or a fully qualified user name, Security Controls will use the domain account rights. • If you enter <Target Machine>\User, Security Controls will use the target's local account rights. • If you do not include a domain or machine as part of the user name, the name will be qualified to the target machine (<targetmachinename>\User). • Microsoft Windows .alias name formats (for example: '.\username') are supported by Security Controls.
Password	Type the password for the user.
Verify password	Retype the password to verify you specified it correctly.

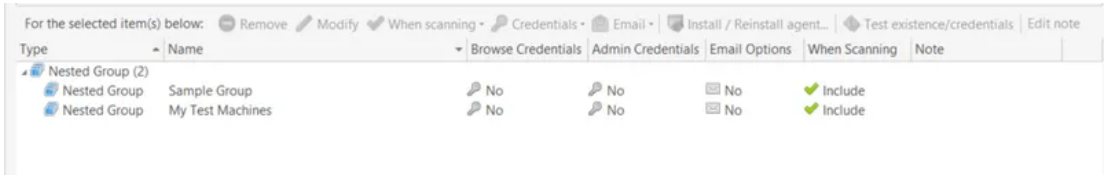
111. Defining Nested Groups

You can use nested groups when configuring a machine group. A nested group is a group that consists of one or more other groups. The primary reason to use a nested group is to easily combine existing groups that have overlapping responsibilities. In general, it is best not to go beyond two levels of nesting.



All currently defined machine groups are listed except the machine group you are currently configuring. To add one or more nested groups, simply enable the check boxes of the desired groups and then click **Add**.

When one or more nested groups are added, the new entries are displayed within the bottom portion of the machine group pane.

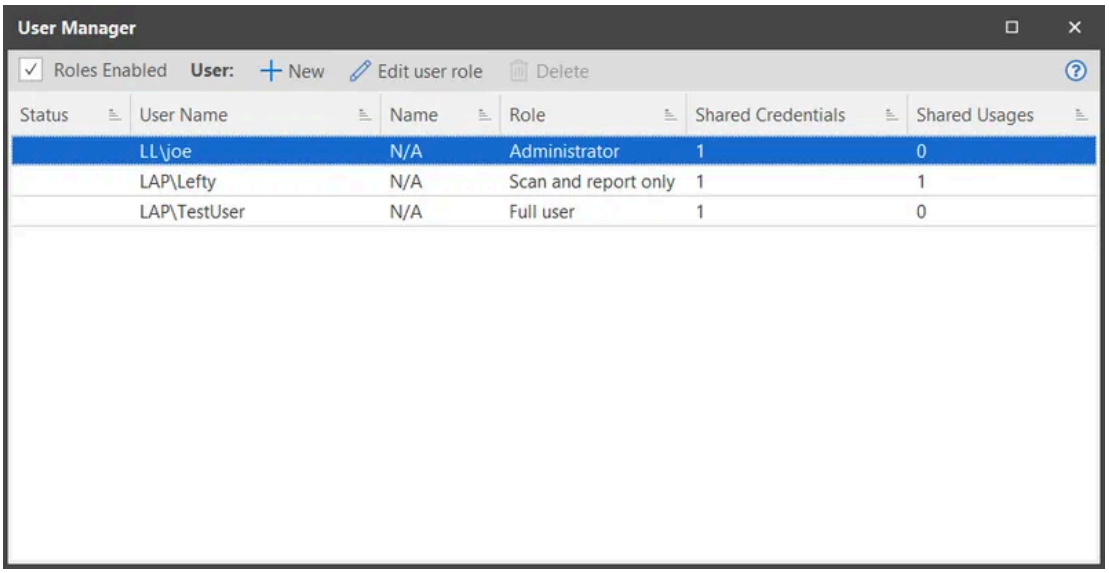


112. Deleting a User

You can delete any user who should no longer have access to Security Controls. For example, you will want to delete an administrator who has been assigned to a different project or who has left your organization.

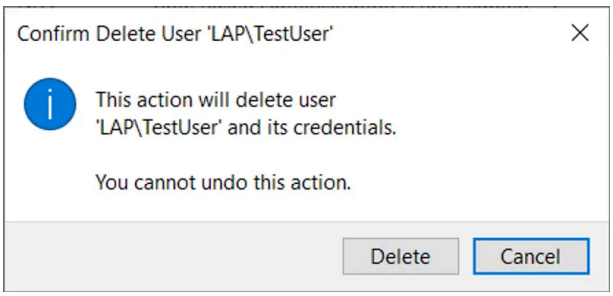
> Deleting a user will also affect your console's **shared credentials** if the user's credentials are being shared with other users.

1. Select **Manage > Users**.
   The **User Manager** dialog is displayed.

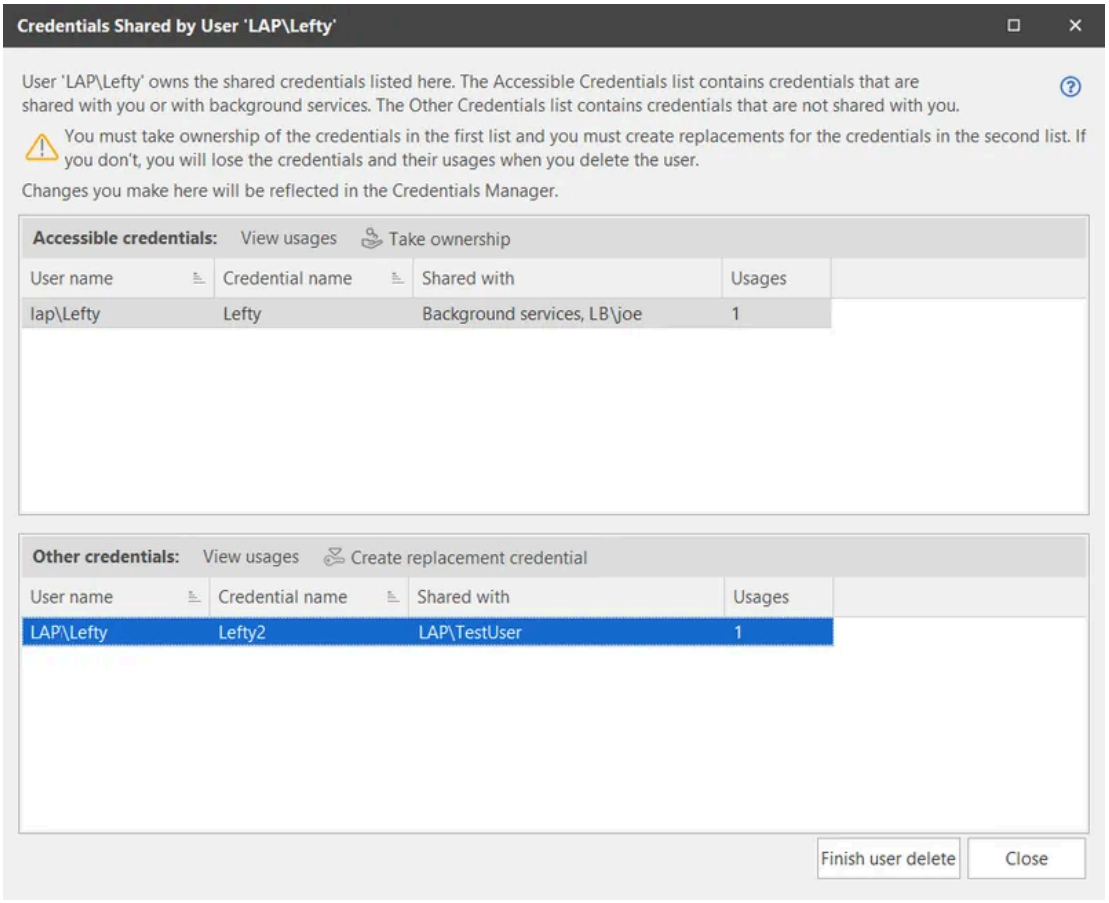


Select the desired user and then click **Delete**.
The confirmation dialog is displayed.

> If the **Credentials Shared by** dialog is displayed rather than the confirmation dialog, see Step 3.



Deleting a user will remove the unique user certificate and associated private key that enabled the user to access Security Controls. (Conditional) If the user who is being deleted is sharing credentials and those credentials are being used by one or more users or by background services, the **Credentials Shared by** dialog is displayed. Use this dialog to clean up all shared credential associations before you delete the user. This process preserves the credential usages for all valid users.



Accessible credentials

If the user who is being deleted is sharing credentials with you or with background services, you must take ownership of those credentials before deleting the user. Do this by selecting the credentials and then clicking **Take ownership**. You can use the Credentials Manager later to view and verify the changes.

Other credentials

If the user who is being deleted is sharing credentials with other users or background services but not with you, you must create a replacement credential before deleting the user. Do this by selecting the credential and then clicking **Create replacement credential**. You can use the Credentials Manager later to view and verify the changes. It will show that you are the owner of the new credentials and that the credentials are shared with the same users and/or services as the original credentials.

After all shared credential issues have been resolved, click **Finish user delete** and confirm the action on the confirmation dialog.

> **Important!** If one or more shared credential issues remain when you click **Finish user delete**, the confirmation dialog will be displayed. Clicking **Delete** to confirm the action will not only delete the user, it will also permanently delete any remaining shared credentials that are owned by the user and those credentials will be lost.

If you want to leave this dialog without deleting the user, click **Close**.

113. Deploying Product Levels

> This describes the process for deploying product levels to agentless machines. For information on deploying product levels to agent-based machines, see **Using a Product Level Group**.

Product level deployments are handled differently than patch deployments. Since Microsoft recommends that a product level be applied before all patches, Security Controls will not allow you to deploy product levels and patches in the same deployment. It is because of this behavior that when you select **Deploy > All Missing Patches**, it literally means to deploy all missing patches; no product levels will be included with this operation.

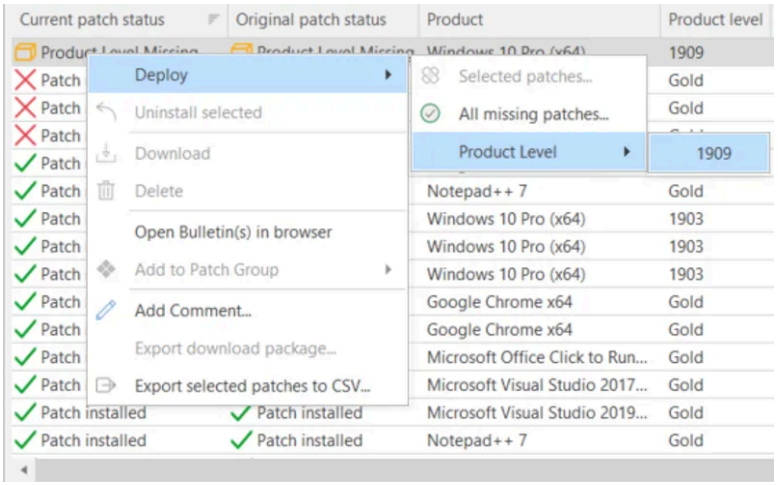
To deploy a product level:

1. In the top pane select a machine.
2. In the middle pane, right-click the desired product level and then select **Deploy > Product Level > specific product level**.

In general, deploying the latest product level will automatically include any previous product levels. Sometimes, however, a previous product level is a prerequisite for a later product level. In this case the program will only let you deploy the prerequisite product level.

In some cases you may want to deploy a product level that is not the latest version. This may be necessary if your organization has not approved the latest product level or if the latest product level is not inclusive (does not include previous product levels).

The following figure illustrates the deployment procedure from within **Scan View**. Product levels can also be deployed in a similar manner from within **Machine View**.

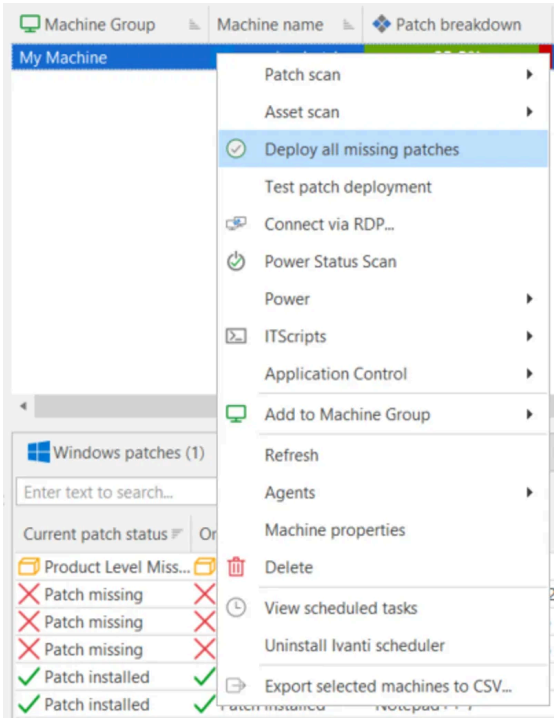


114. Deploying All Missing Patches to a Machine

You can easily deploy all patches that are missing from a machine. There are a couple of ways to do this within Security Controls.

From the Top Pane of Machine View or Scan View

1. In the top pane of **Machine View** or **Scan View**, select the desired machine.
2. Right-click the machine and select **Deploy all missing patches**.

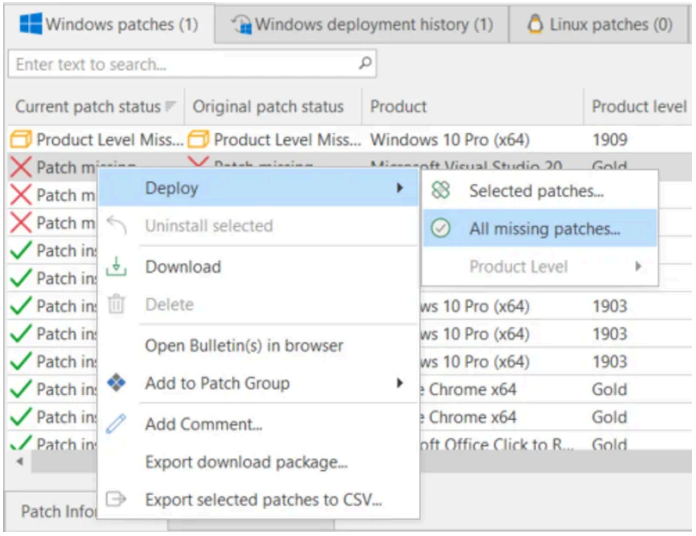


This will launch the **Deployment Configuration** dialog.

> If **default credentials** are not currently assigned the **Assign Credentials** dialog is displayed. If you choose not to assign default credentials by clicking **Cancel**, then the deployment may fail for any machine that does not contain **assigned credentials**.

From the Middle Pane of Machine View or Scan View

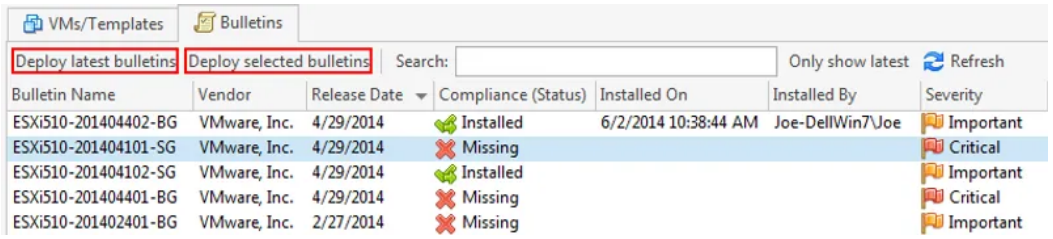
1. In the top pane of **Machine View** or **Scan View**, select the desired machine.
2. In the middle pane, right-click a missing patch and select **Deploy > All missing patches**.


Windows patches (1)
Windows deployment history (1)
Linux patches (0)
Enter text to search...
Current patch status
Original patch status
Product
Product level
Product Level Miss...
Product Level Miss...
Windows 10 Pro (x64)
1909
Deploy
Uninstall selected
Download
Delete
Open Bulletin(s) in browser
Add to Patch Group
Add Comment...
Export download package...
Export selected patches to CSV...
Selected patches...
All missing patches...
Product Level
1903
Chrome x64
Gold
Patch Info

115. Deploying Bulletins to Unmanaged Hypervisors

The **Bulletins** tab can be used to deploy missing bulletins to your ESXi hypervisors and to view information about the bulletins.

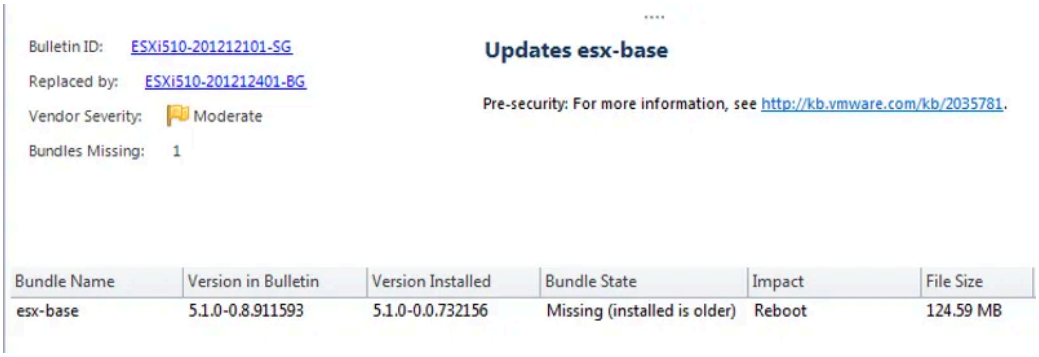
To apply one or more bulletins, select the desired bulletins and then use the buttons along the top of the table.



Field	Description
Deploy latest bulletins	Initiates the deployment of all bulletins that are missing on the ESXi hypervisor. This will include only those bulletins that have not been replaced by newer bulletins. For more information on the bulletin deployment process, see Configuring an ESXi Deployment. TIP: Use the **Only show latest** check box to see which bulletins will be deployed if you click **Deploy latest bulletins**.
Deploy selected bulletins	Initiates the deployment of the selected bulletins. For more information on the bulletin deployment process, see Configuring an ESXi Deployment.

Viewing Bulletin Details

The bottom pane displays detailed information about the bulletin that is selected in the top pane of the **Bulletins** tab. Detailed information will not be displayed if multiple bulletins are selected.



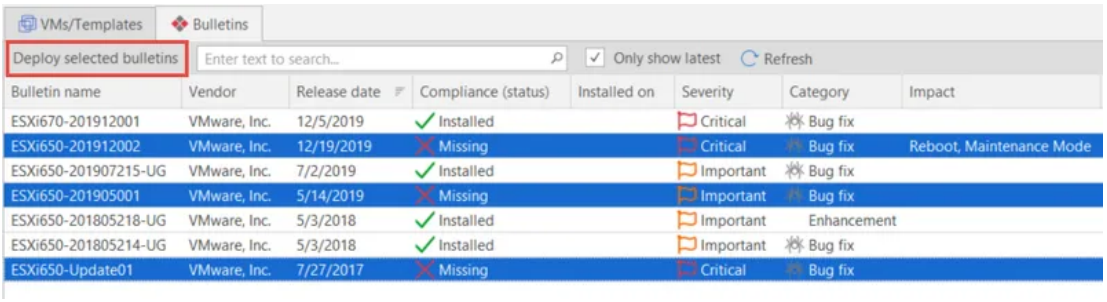
Field	Description
Bulletin ID	Provides a link to the VMware Knowledge Base article that describes the threat addressed by this bulletin.
Replaced by	If shown, indicates that the bulletin has been replaced by a newer bulletin. A link is provided to the VMware Knowledge Base article that describes the newer bulletin.
Vendor Severity	Indicates the severity level of the vulnerability that is corrected by this bulletin. The severity level can be one of the following: • **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. • **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. • **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. • **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
Bundles Missing	The number of bundles that will be installed if the selected bulletin is installed.
Bundle Name	The base name of the bundle within the bulletin. The base name does not include the version information.
Version in Bulletin	The version of the bundle that is specified in the bulletin.
Version Installed	The version of the bundle that is currently installed. The installed version may be older, newer, or the same as the version specified in the bundle. If blank, then no version of this bundle is currently installed.
Bundle	The state indicate how the installed version compares with the required version. The bundle state can be one of the following:

Field	Description
State	• **Installed (exact):** The installed version of the bundle is the same as the version specified in the bulletin. • **Installed (installed is newer):** The installed version of the bundle is newer that the version specified in the bulletin. • **Missing (not installed):** No version of the bundle is currently installed. • **Missing (installed is older):** The installed version of the bundle is older that the version specified in the bulletin.
Impact	Indicates the impact that applying the bulletin will have on the hypervisor.
File Size	The size of the installation bundle file.

116. How to Deploy Bulletins to Your Managed Hypervisors

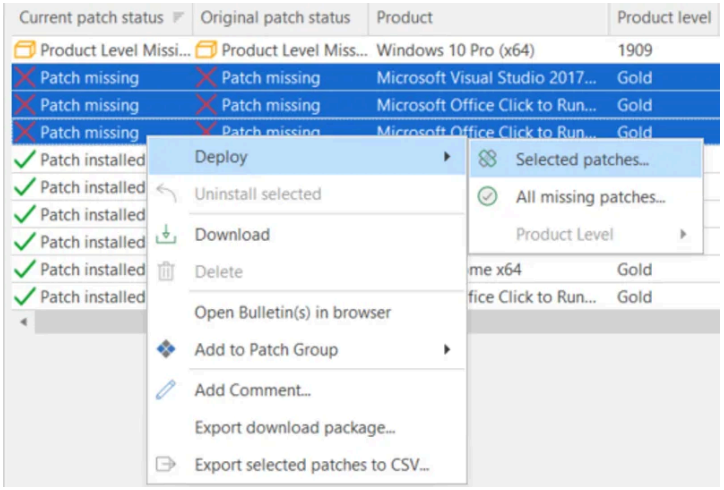
The **Bulletins** tab can be used to deploy missing bulletins to your managed ESXi hypervisors. You simply select the desired bulletin(s) and then click **Deploy selected bulletins**. Note that because you can only deploy bulletins to one hypervisor at a time, if you select bulletins from two or more hypervisors, the **Deploy selected bulletins** button will no longer be available. For more information on the bulletin deployment process, see **Configuring an ESXi Deployment**.

> TIP: Use the **Only show latest check box** to view only those bulletins that are not replaced by newer bulletins.



117. Deploying One or More Patches to a Machine

1. In the middle pane of **Scan View** or **Machine View**, select the patches that you would like to deploy to the selected machine. Multiple patches can be selected by holding down the CTRL key while selecting patches. A contiguous group of patches can be selected by holding down the SHIFT key while selecting the starting and ending patch in the list.
2. Right-click one of the patches that are to be deployed and select **Deploy > Selected Patches** from the shortcut menu.

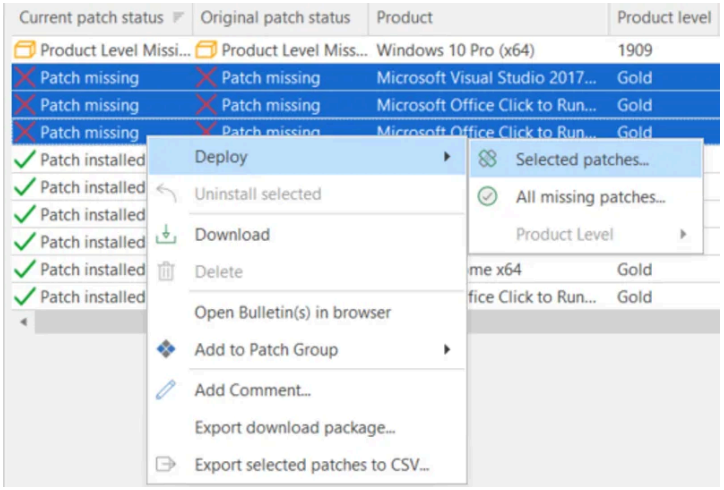


This will launch the **Deployment Configuration** dialog.

> If **default credentials** are not currently assigned the **Default Credentials** dialog is displayed. If you choose not to assign default credentials by clicking **Cancel**, then the deployment may fail for any machine that does not contain **assigned credentials**.

118. Deploying Patches to Multiple Machines

You can deploy patches to multiple machines using **Machine View** or **Scan View**. In the top section select the machines that are missing the patch, and then in the middle section right-click the patch and select **Deploy > Selected Patches**. You can also select multiple patches in the middle section and it will deploy them to all machines selected in the top section that are missing them.



119. Deploying Patches to Virtual Machines and to Virtual Machine Templates

The **method for initiating a patch deployment** is the same regardless of whether you are deploying to a physical machine, an online virtual machine, an offline virtual machine, or a virtual machine template. It's what happens after you initiate the deployment, however, that is slightly different for virtual machines and for virtual machine templates.

> For deployments to virtual machines that are hosted on a server it is recommended you use the **Virtual Machine Standard deployment template**. Also, in all cases, during deployment the virtual network will need to remain connected.

IMMEDIATE PATCH DEPLOYMENTS

> Also applies to **Install at next reboot** patch deployments performed on offline hosted virtual machines.

When you perform an immediate deployment to a physical machine, an online workstation virtual machine, or an offline workstation virtual machine, the files required for the deployment are copied to the target machine immediately and the deployment is scheduled to occur immediately using the scheduler on the target machine. The patch installation is performed on the target machines and the console is not actively involved. If the machine is in a different power state from when it was last scanned, the deployment will fail.

When you perform an immediate deployment to a virtual machine that is hosted on a server, the entire deployment process occurs on the Security Controls console machine. The console determines the online/offline status of the hosted virtual machines and the console service is actively involved during the patch installation. This allows the console service to modify the state of the hosted virtual machines during the deployment.

The following table summarizes what happens at the time you perform an immediate deployment based on where the virtual machines are defined within the machine group.

Machine Group Tab Used to Define the Virtual Machine	Target Machine is Online	Target Machine is Offline
Machine Name, **Domain Name**, **IP Address/Range**, **Organizational Unit**	Push files and initiate deployment immediately.	Fail
Workstation Virtual Machines	Fail	Push files and schedule on target; deployment will occur the next time the virtual machine is brought online.
Hosted Virtual Machines	Push files and initiate deployment immediately. The process is the same as a physical machine except that **snapshots** will be taken and deleted as directed by the deployment template.	*See steps below. VMware tools must be installed on the virtual machine in order for the deployment to be successful.

> If you are operating in an NTLM- or SPN-restricted environment and you specify **FQDN as your connection method**, progress messages will not be displayed when deploying patches to offline hosted virtual machines.

*During deployment to an offline hosted virtual machine or an offline virtual machine template, the following steps occur:

1. **[Conditional: Templates Only]** Convert the virtual machine template to an offline virtual machine.
2. **(Optional)** Take a snapshot if the deployment template is configured to take a **pre-deployment snapshot**.
3. **(Optional)** Delete old snapshots if one of the **snapshot thresholds** defined on the patch deployment template is exceeded.
4. Copy the patches to the offline virtual machine.

5. Reconfigure the following on the offline virtual machine:
    - Disable the network adaptor's **Connect at power on** option. This is done so that the machine is isolated from the network when the patch process is run.
    - Disable Sysprep so it will not automatically configure the machine's operating system when the machine is first powered on.

Power on the virtual machine.

7. Install the patches.
8. Power down the virtual machine.
9. Reset the machine configuration to its original network connection and Sysprep settings.
10. **(Optional)** Take a snapshot if the deployment template is configured to take a **post-deployment snapshot**.
11. **(Optional)** Delete old snapshots if one of the snapshot thresholds defined on the patch deployment template is exceeded.
12. **[Conditional: Template Only]** Convert the offline virtual machine back to a virtual machine template.

SCHEDULED PATCH DEPLOYMENTS

> Also applies to **Install at next reboot** patch deployments performed on online hosted virtual machines and offline workstation virtual machines.

When you schedule a deployment to a physical machine, an online workstation virtual machine, or an offline workstation virtual machine, the files required for the deployment are copied to the target machine immediately and the deployment is scheduled using the scheduler on the target machine. The patch installation is performed on the target machines and the console is not actively involved. At the time of the actual deployment, if the machine is in a different power state from when it was last scanned, the deployment will fail.

When you schedule a deployment to a virtual machine that is hosted on a server, the entire deployment process is scheduled to occur on the Security Controls console machine using the scheduler on the console. The online/offline status of the hosted virtual machines is determined at the scheduled time, and the console is actively involved at the time the patches are installed. This allows the console to modify the state of the hosted virtual machines during the deployment.

The following table summarizes what happens at the time you schedule a deployment based on where the virtual machines are defined within the machine group.

Machine Group Tab Used to Define the Virtual Machine	Target Machine is Online When Scheduled	Target Machine is Offline When Scheduled
Machine Name, **Domain Name**, **IP Address/Range**, **Organizational Unit**	Push files to the target and schedule the deployment on the target. The deployment will occur the next time both of the following are true: • The machine is online • The scheduled time has passed	Fail
Workstation Virtual Machines	Fail	Push files to the target and schedule the deployment on the target. The deployment will occur the next time both these are true: • The machine is online • The scheduled time has passed
Hosted Virtual Machines	Schedule the deployment on the console. At the scheduled time (or, for **Install at next reboot** deployments, when the machine is restarted), treat as an immediate deployment. See **Hosted Virtual Machines** in the previous table.	

If the scheduled deployment contains a mix of hosted virtual machines and other types of machines, the machines are separated into two groups. The deployment of the hosted virtual machines is scheduled to occur on the console at the scheduled time. For

all machines other than hosted virtual machines, the files are copied to the target machines immediately and the deployment is scheduled to occur using the scheduler on the target machine.

CREDENTIAL AND POWER STATE REQUIREMENTS FOR A SUCCESSFUL DEPLOYMENT

> Keep in mind that, from Security Controls's point of view, the definition of a successful deployment depends on where the virtual machine is located. A successful deployment to a hosted virtual machine means the machine is fully patched, while a successful deployment to a workstation-based virtual machine means the patches have been pushed to the offline virtual machine.

When performing the deployment, the program will attempt to authenticate to the target machine using the credentials defined in the **Manage Machine Properties dialog**. If the credential is invalid the deployment will fail. For workstation-based virtual machines, if the power state of the machine has changed since the scan, the deployment will fail.

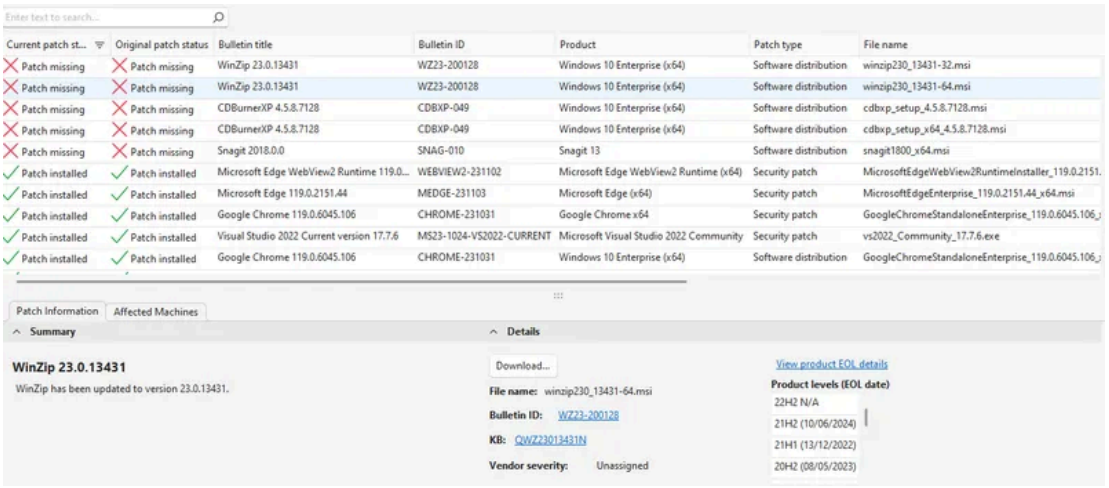
For more information, see **Power State and Credential Requirements for VMs**.

120. Deploying Third-Party Applications

> Click here for information on **how to scan for third-party applications**.

You deploy (install) third-party applications to selected machines in the exact same manner that you deploy missing patches to selected machines. Security Controls will treat the missing application exactly like a missing patch and will simply install the application on the selected machines. Here's an example showing how to deploy a third-party application from Scan View. The procedure is very similar using Machine View.

1. Select the third-party application you want to deploy.

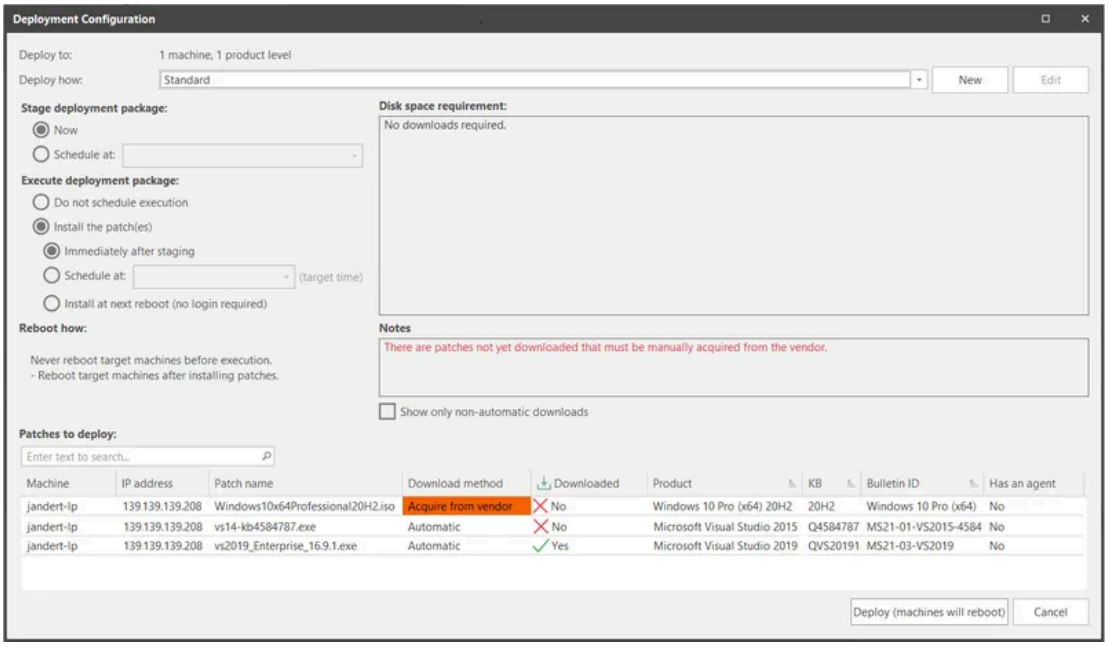


Right-click the selected application and select **Deploy > Selected Patches**.

3. On the confirmation dialog, click **Continue with Software Distribution**.
   The confirmation dialog is presented to ensure that you don't inadvertently install a new application on the selected machines. You continue the deployment as normal using the **Deployment Configuration** dialog.

121. Scheduling and Configuring a Deployment

When a patch deployment is initiated the **Deployment Configuration** dialog is displayed. This dialog enables you to specify exactly when and how the patches will be deployed.

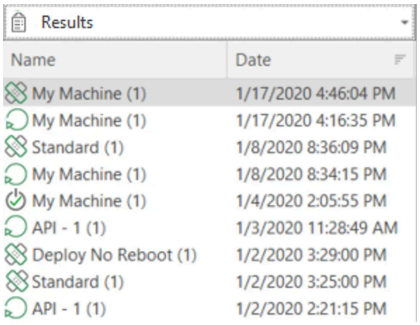


Field	Description
Deploy To	Indicates how many patches are being deployed and to how many machines.
Deploy How	Specify the deployment template you want to use. There are two buttons associated with this field: • **New**: Enables you to create a new deployment template. • **Edit**: Enables you to permanently modify the selected deployment template. The default templates (**Agent Standard , Standard , and Virtual Machine Standard**) cannot be modified. Clicking **Edit** lets you view but not change the default templates.
Disk space requirement	Provides status information about the patches that will be deployed.
Stage deployment package	Specify when you want the patches to be staged. The staging steps include creating the deployment package and copying the package to the target machine. Your options are: • **Now**: The staging process will begin right after you click **Deploy**. • **Schedule at**: Enables you to choose the date and time at which the staging process will occur.
Execute deployment package	Specify when you want to deploy the staged patches. Your options are: • **Do not schedule execution**: Choose this option if you do not want Security Controls to deploy the staged patches. You might choose this option if you want to manually start the patch installation at the remote machines at a later time. • You have two options for deploying the patches after they are copied to the target machines: ◦ Deploy from the console: Initiate the deployment using any of the standard methods. The deployment process will be faster than normal because the patch files have already been downloaded and copied to the target machines. ◦ Deploy from the remote machine: On the remote machine, go to the `C:/Windows/ProPatches/Staged/<timestamp>/` directory and execute the batch file named `InstallPatches-#.bat`. **Install the patch(es):** There are three options for installing patches. ◦ **Immediately after staging:** The staged patches are installed immediately on the target machine. ◦ **Schedule at:** The staged patches are installed on the target machine at the time of your choosing. ◦ **Install at next reboot (no login required)**: The staged patch files will not begin until the next time the target machine is restarted. Offline hosted virtual machines are the exception, for them the deployment process will begin immediately. For more details see **Deploying Patches to Virtual Machines**.
Reboot How	Displays the current reboot instructions defined by the selected template.
Notes	If available, provides additional information about one or more of the patches selected for deployment.
Show only non-automatic downloads	If available, enables you to modify the information in the **Patches to deploy** grid so that the only patches displayed are those that must be manually downloaded.

Field	Description
Patches to deploy	Displays detailed information about the machines and the patches selected for deployment.
Deploy	When you are ready to deploy your patches using the selected deployment options, click this button. If the target machines will reboot as part of the deployment process, the button name will change to **Deploy (machines will reboot)**; this serves as a reminder about the upcoming reboots.

122. Deployment History

Even after a series of deployments, all of the results of prior deployments are just a click away. The deployment results are recorded in the **Results** list in the navigation pane. In addition to deployments, the **Results** list also maintains a list of recent scans. The number of items shown in this list is configurable using **Tools > Options > Display > Recent items**.

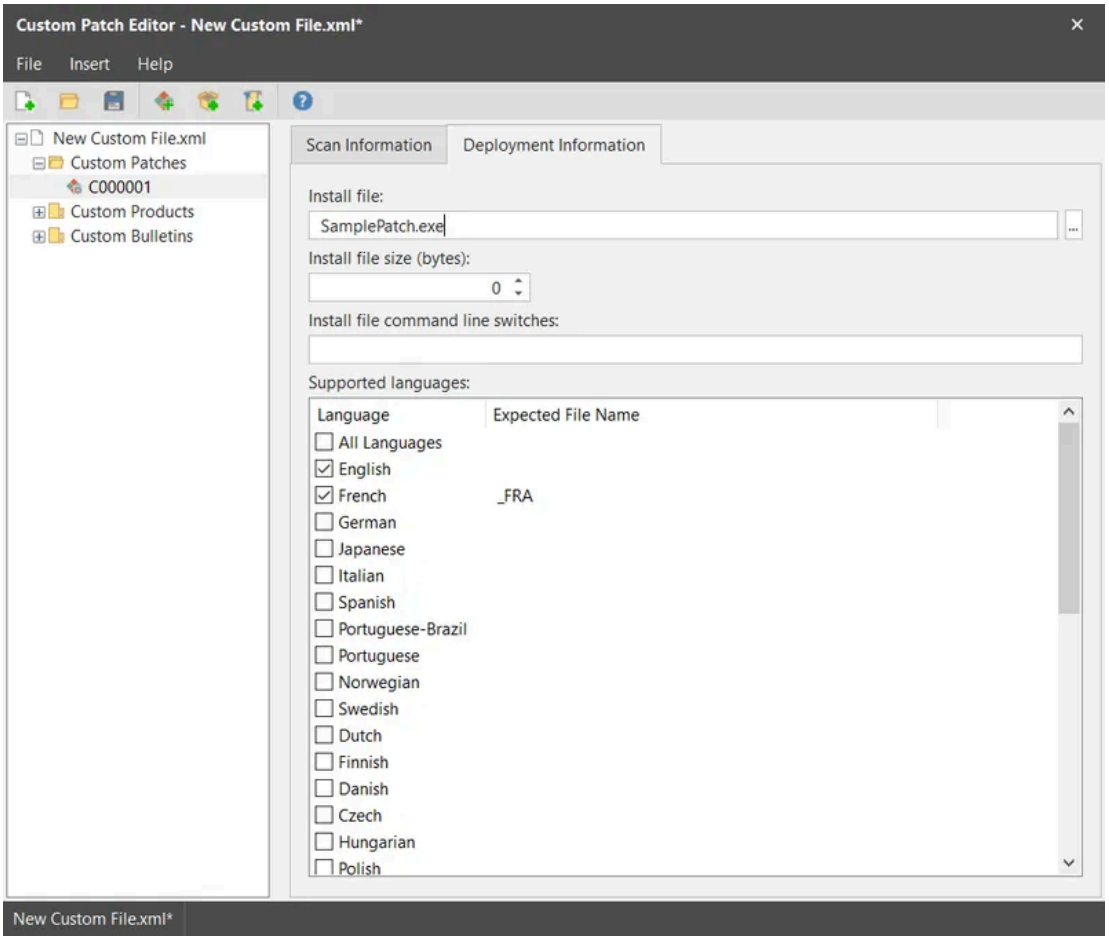


Related Topics

- Viewing Patch and Asset Summaries in Machine View: You can view patch deployment information from selected machines using Machine View.
- Database Maintenance: You can get a complete list of available prior deployments by choosing **Manage > Database Maintenance**.

123. Deployment Information Tab

When creating a custom patch, two major tabs are used in the right-hand pane. This topic describes the options contained on the **Deployment Information** tab.

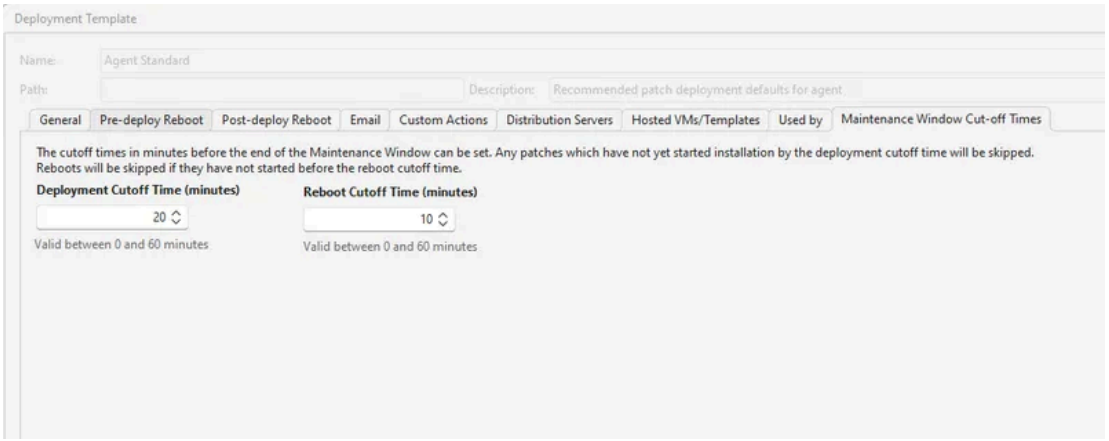


Field	Description
Patch Install File	Batch files (.bat and .cmd file formats) are not supported by the custom patch process and must not be used as a patch install file. This is the patch file that will be used when the conditions specified on the **Scan Information** tab are met. Specify just the file name here and not the full path name to the patch install file. This file is typically supplied by the vendor of the product you are patching. You can use the browse button to locate and select this file. Doing so will automatically populate the **Patch Install File Size** box. IMPORTANT! The actual file used in the patch process may have several different names and you must manually copy the files to every location the patch file is expected to reside, including the console and possibly one or more distribution servers. See the description of the **Patch Supported Languages** option for more information.
Patch Install File Size (bytes)	Specifies the size of the patch install file. This box is automatically filled in when you use the **Browse** button to select the **Patch Install File**. Providing the file size enables the program to accurately determine the progress during the installation process.
Patch Install File Command Line Switches	Specify any command line switches you want to use during the installation of the patch. For example, you might want a silent install (/quiet), you might want to dictate that the target machines are not restarted (/norestart), etc.
Patch Supported Languages	Enable the check boxes for the operating system languages you want to support with this custom patch. There are two reasons for doing this: • It tells the program which languages are supported by the patch. • It tells you what identifying text should be added to the end of the patch file name. IMPORTANT! You must make as many copies of the file as is needed using the appropriate names and then make those files available everywhere the patch file is expected to reside. **Example 1:** Assume your vendor supplied two versions of the same patch, one for English language systems named *SamplePatchENGLISH.exe* and one for French language systems named *SamplePatchFRENCH.exe*. You must add the text shown in the **Expected File Name** column to the end of the associated patch file. In this example the updated file names would be *SamplePatchENGLISH.exe* and *SamplePatchFRENCH_FRA.exe.* (The English language patch does not require the suffix, although *SamplePatchENGLISH_ENU.exe* would also work.) You then place copies of each file in the console's patch download directory and on the appropriate distribution servers. **Example 2:** Assume your vendor supplied a patch file named *SamplePatch.exe* and that file supports English, French, and German language systems. You must make three copies of the file, rename them by adding the text shown in the **Expected File Name** column to the end of each file name, and then place copies of each file on the appropriate distribution servers. In this example the file names would be *SamplePatch.exe*, *SamplePatch_FRA.exe*, and *SamplePatch_GER.exe.*

When complete, save and then validate the XML file (see Saving and Validating Your Changes).

124. Deployment Template: Maintenance Window Cut-Off Times Tab

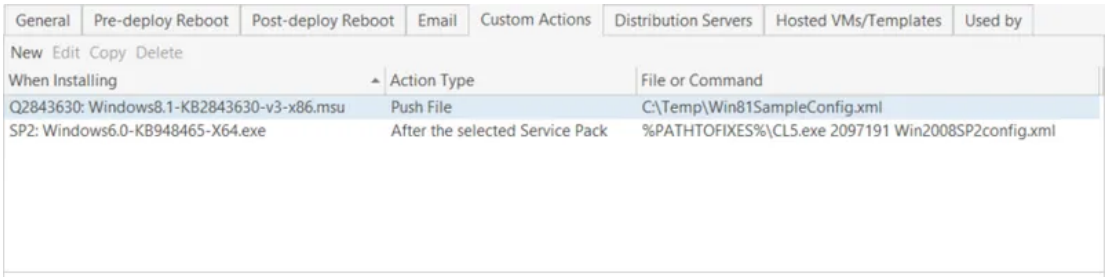
You can configure the cutoff time defined in minutes (0 to 60) relative to the end of the maintenance window.



- **Deployment Cutoff Time**: Time in minutes before window ends to stop launching new deployments. If a patch installation is not started by the specified number of minutes before the maintenance window ends, it is excluded.
- **Reboot Cutoff Time**: Time in minutes before window ends to stop initiating reboots. If a reboot is not initiated by the specified number of minutes before the end of the maintenance window, then reboot is skipped.

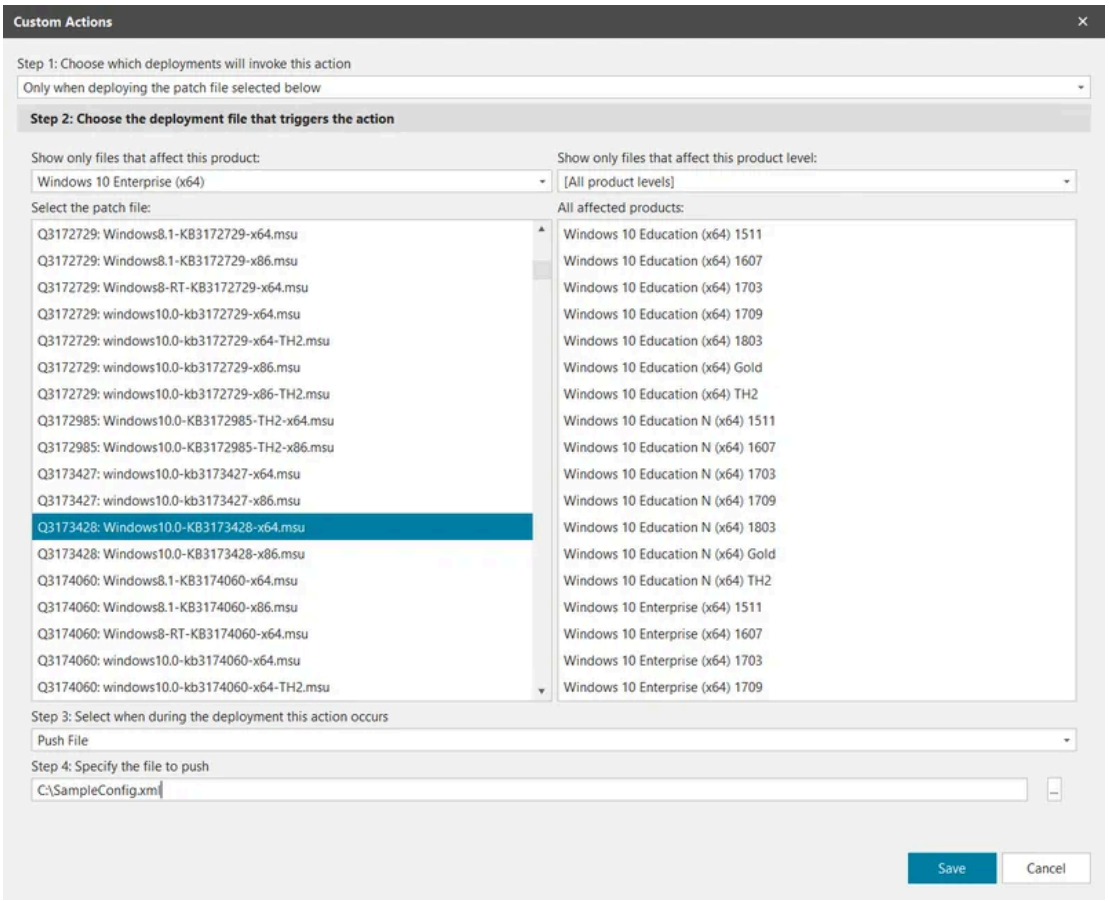
125. Deployment Template: Custom Actions Tab

> The functions on this tab are not supported by Security Controls Agent.



This tab gives you the ability to push custom files to the machines being patched, and to program customized commands that will be executed during patch deployment. A custom action may include executing a specific command or invoking a custom batch file at specified time(s) during the deployment process. You can specify custom files and actions that occur during every deployment that uses the template, or only for those deployments that install a specific patch or product level.

To program a new action, click **New** and the **Custom Action** dialog appears.



Step 1: Specify what patch deployment action will trigger the command.

- **All deployments using this template:** Allows you to perform actions such as custom logging.

- **Only when deploying the patch/product level selected below:** Allows you to perform actions only when pushing a specific patch or product level to a target machine using this deployment template.

Step 2: If in Step 1 you indicate that only the deployment of specific patches or product levels will trigger the command, specify those files here.

Step 3: Specify when during the patch deployment process the command will be triggered. The choices are:

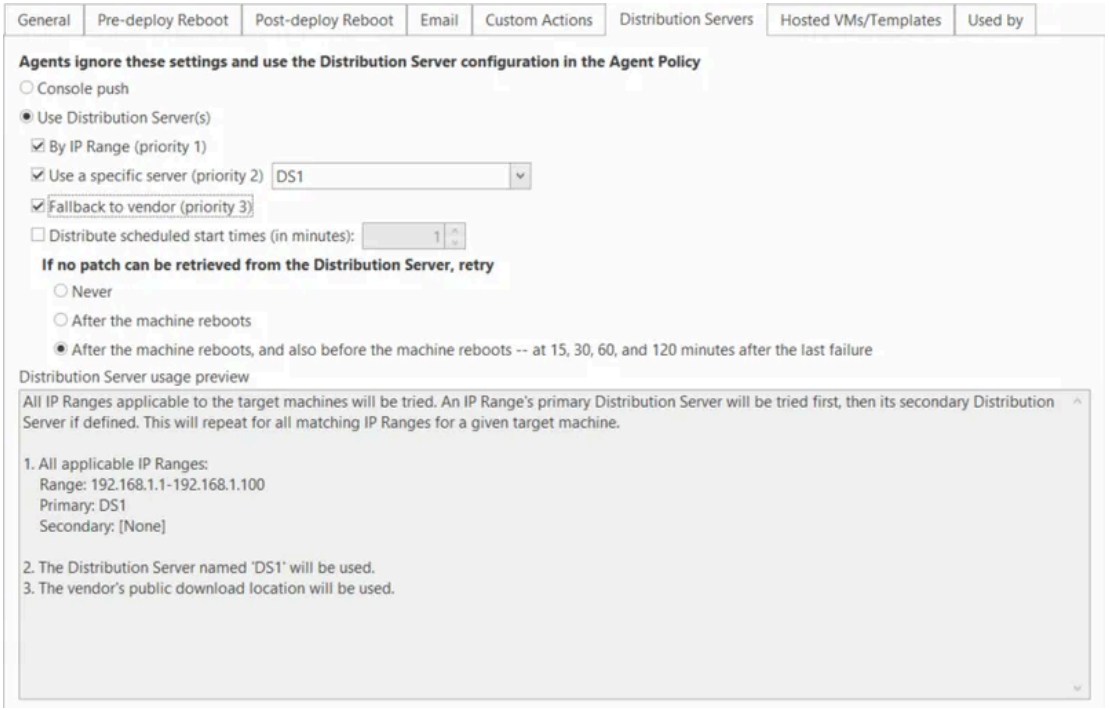
- **Push File** (pushes a custom batch file or custom executable file to the target machines as part of the deployment)
- **Before any patches** are installed
- **Before each patch** or **Before the selected patch/product level** is installed
- **After each patch** or **After the selected patch/product level** is installed
- **After all patches** are installed (but before reboot)
- **After reboot**

Step 4: Specify the file to push or the command to execute. The command will be inserted into the patch installation batch file at the point(s) specified in Step 3. If Step 3 specifies **Push File** then the specified file will be copied to the target machines and put in the `C:\Windows\ProPatches` directory. The base folder location can be changed using the **Patch drive path** option on the **Machine Properties dialog**. You can reference the file in other custom actions by specifying `%PATHTOFIXES%file_name`.

Example 1: If you push the file `myFile.exe`, you can execute that file with the following custom command: `%PATHTOFIXES%myFile.exe`.

Example 2: If you push the batch file `myCommands.bat` to the target machines, you can invoke the batch file at the appropriate point in the deployment with the following custom command: `call %PATHTOFIXES%myCommands.bat`.

126. Deployment Template: Distribution Servers Tab



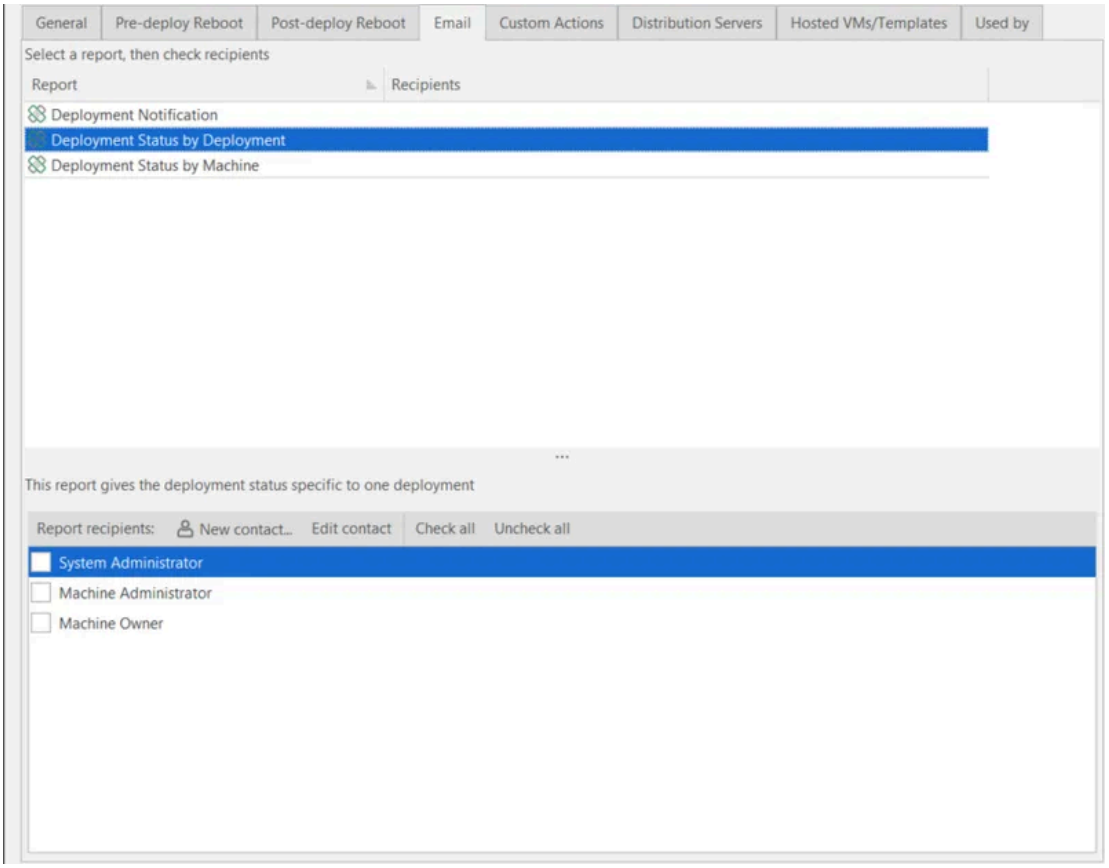
Field	Description
Console push	If enabled, indicates that a distribution server will not be used and the console will serve as the source for all patches.
Use Distribution Server(s)	If enabled, indicates that a distribution server will serve as the source for all patches during deployments that use this template. The three check boxes that immediately follow are used to determine which distribution server to use, if any. The program will search for an available distribution server using only those options that you enable, and the search will be performed in the listed order (priority 1, priority 2 and priority 3). If you enable **Use Distribution Server(s)** but do not specify at least one of the three source options, the deployment will fail. See **Configuring Distribution Servers** and **Assigning IP Addresses to Servers** for information on configuring the distribution servers. When patches are deployed via distribution servers, patches are not pushed to the target machines. Rather, the target machines will download the patches from one or more distribution servers. Patches must be copied from the console's patch download directory to the servers before they will be available for deployment. See **Synchronizing Servers** for information on copying patches to your distribution servers.
By IP Range (priority 1)	If enabled, indicates that the distribution server to use will be determined by the IP address of each target machine. In order for this to work you must have previously **defined one or more IP ranges** and assigned the ranges to a primary distribution server and to a backup server.
Use a specific server (priority 2)	If desired, specify a specific distribution server to use if the primary and backup distribution servers defined by the **By IP Range** option are unavailable. If the **By IP Range** option is not enabled, the server specified here will become the default server.
Fallback to vendor (priority 3)	If the distribution servers identified by the first two options are not available, enabling this check box will allow the machine being patched to try to download the patch from the patch vendor's website. This option does not apply to custom patches because custom patches do not contain download URLs. Custom patches must be either pushed to the target machines from the console's patch download directory or pulled by the target machines from a distribution server.
Distribute scheduled start times (in minutes)	If you are deploying patches to a large number of machines at the same time, all the machines will begin to download the patches from the distribution server at approximately the same time. If you enable this option, the start times for the machines will be randomly distributed over the interval that you specify. This can help to reduce the peak network load.
If no patch can be retrieved from the Distribution Server, retry	If no patches can be obtained from the distribution server at the scheduled deployment time, you can specify how often you want to attempt a retry. If at least one patch is successfully downloaded, the deployment will resume without a retry, even if one or more patches are not successfully downloaded. • **Never:** A retry will not be attempted and the deployment will fail. • **After the machine is rebooted:** A retry will be attempted each time the target machine is rebooted, for up to three reboots. If the download process is still failing after three reboots, the deployment will fail. • **After the machine reboots, and also before the machine reboots -- at 15, 30, 60, and 120 minutes after the last failure:** A retry will be attempted at 15, 30, 60, and 120 minute intervals after the last failure, and also if the target machine is rebooted before all the time interval retries have been attempted. Retries may also

Field	Description
	attempted after subsequent reboots. The deployment will fail after 4 timer attempts or 3 attempts that include a reboot.

127. Deployment Template: Email Tab

> This tab applies only to agentless deployments initiated from the console; it does not apply to agents that may also be using this template.

This tab enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent for each deployment that uses this template.

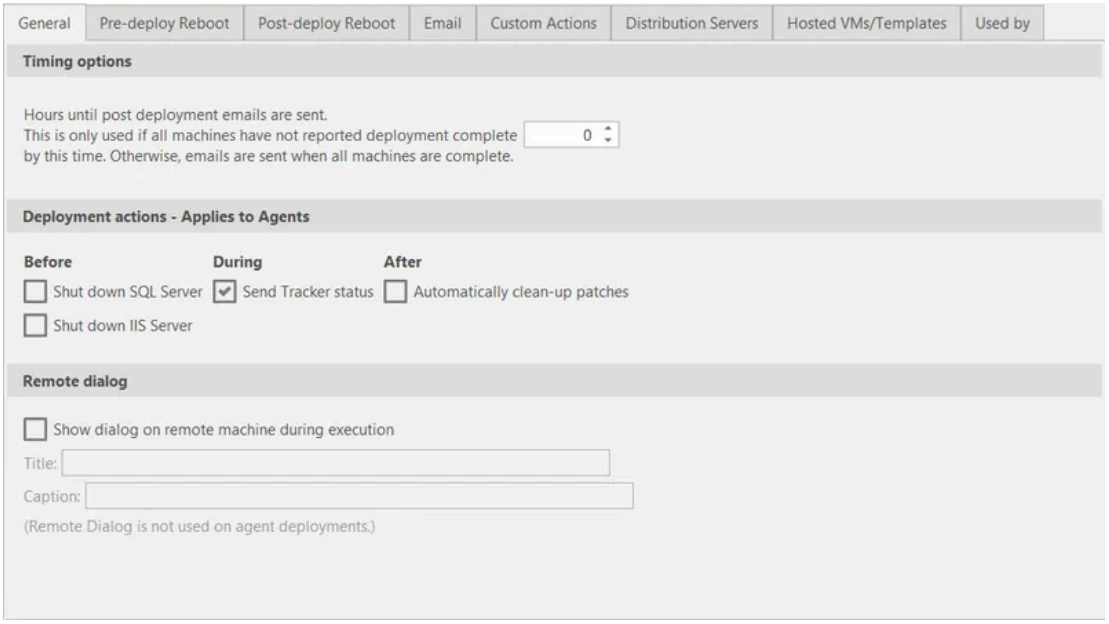


Field	Description
Available Reports	There are three different deployment reports that can get sent: • **Deployment Notification**: This report is sent after the deployment is successfully scheduled. It identifies the patches that will be deployed and the date and time of the pending installation. • **Deployment Status by Deployment**: This report is sent after the deployment is complete and verified or after the maximum time specified on the General tab. The report provides general status information about the deployment. • **Deployment Status by Machine**: This report is sent after the deployment is complete and verified or after the maximum time specified on the General tab. The report identifies each machine included in the deployment and indicates if the patch deployment on each machine was successful or unsuccessful.
Report Recipients	Lists the contacts you want to receive a particular report. The contacts listed are those contained in the address book. You can add new contacts or edit contact information by clicking the **New Contact** and **Edit** buttons, respectively.

To specify which reports should be automatically sent and to whom they should be sent:

1. Select a report in the **Available Reports** list.
2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to.
   You can select all and clear all recipient check boxes using the **Check All** and **Uncheck All** buttons, respectively. The selections you make are added as report recipients in the **Available Reports** list.
3. Repeat Step 1 and Step 2 for each report you want to be automatically sent.
4. When finished, click **Save**.

128. Deployment Template: General Tab



Field	Description
Hours until post deployment emails are sent	Enables you to specify how long to wait for patches to be successfully deployed before sending any automatic email messages. This field forces the email messages to be sent even if the console cannot determine that all the machine deployments completed because Deployment Tracker is not enabled or because a network connection is lost.
Deployment Actions	There are a number of options that can be selected to take place before, during and after patch deployment. **Before** You can choose to shut down the SQL Server and the IIS Server. These services will be automatically shut down when an SQL or IIS patch (respectively) is applied to a remote machine regardless of this setting. Use this setting to shut down these services when installing OS or similar hotfixes, particularly if you are planning to reboot the machine after installation. **During** During the deployment, you can elect not to send Deployment Tracker status messages from the machines being patched. For example, clearing the **Send Tracker status** check box makes sense if the machines will not be attached to the network when the patch installation takes place. **After** After the deployment is complete, you can choose to automatically clean-up patches. This will remove the temporary patch files that were copied during the current deployment process. It will also remove deployment files that are older than 180 days.
Remote Dialog	The Remote Dialog functions are not supported by Security Controls Agent. **Show dialog on remote machine during execution:** If this check box is enabled, then if a user is logged on at the target machine at the scheduled deployment time, a dialog box will be displayed to the user when the deployment begins. **Title:** Type the text you want to appear in the dialog box title. **Caption:** Type the text you want to appear in the dialog box caption.

Handling Sandbox log folders

During patch deployment, the system creates temporary sandbox folders to capture deployment activity for each patch deployment. These folders contain log files and execution artifacts, and the folders are timestamped. By default, the installation media and other temporary files are retained for 7 days, and other log files are retained for 60 days.

To preserve sandbox data for troubleshooting or future analysis, rename and archive the folders to a different location before they are automatically removed.

129. Deployment Template: Hosted VMs/Templates Tab

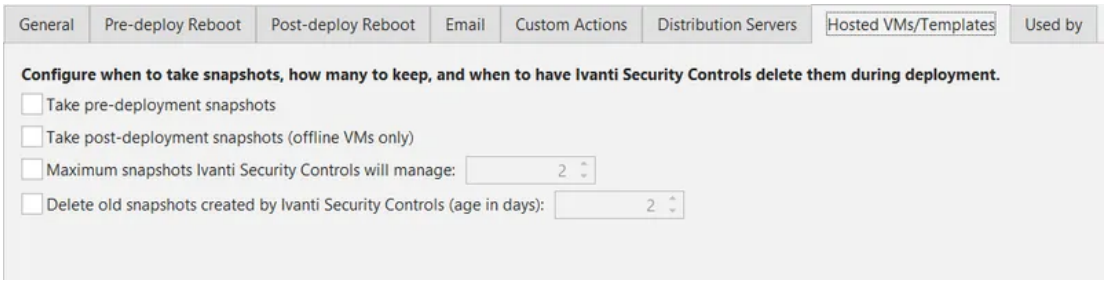
> This tab allows you to remove old snapshots during the patch deployment process. If you want to schedule the removal of old virtual machine snapshots without having to perform a deployment, see **Scheduled Snapshot Maintenance**.

This tab only applies if you have virtual machines in your network that are **hosted on one or more VMware servers**. It enables you to specify if snapshots will be taken of the hosted virtual machines (or of hosted virtual machine templates) immediately before and/or immediately after patches are deployed to the virtual machines. This tab does not apply to virtual machines that **reside on workstations**.

What is a virtual machine snapshot? A snapshot captures the state, configuration, and disk data of a virtual machine at a given time. Snapshots are useful for storing states that an administrator or user might want to return to at some point in the future.

Complete snapshots are taken of offline virtual machines and of **virtual machine templates**. If a virtual machine is online at the time of the patch deployment the memory state will not be included in the snapshot—this will quicken the process and reduce the amount of time that the online virtual machine is affected.

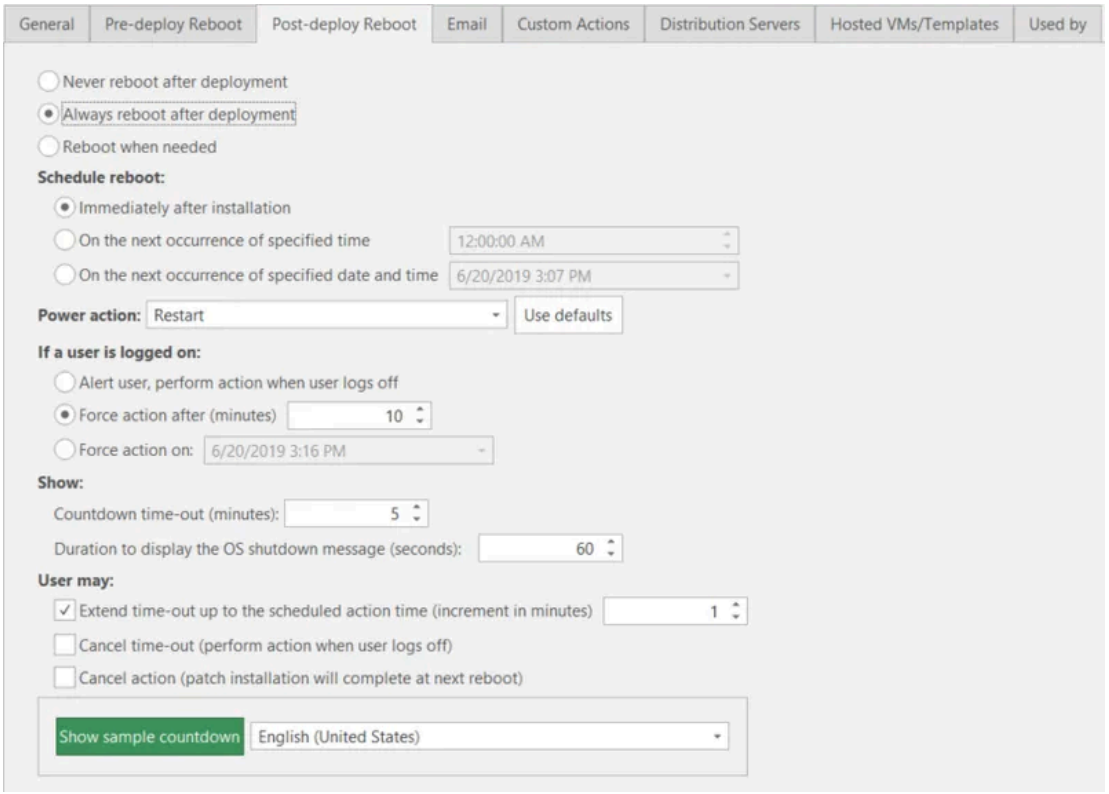
There are reasons why you may choose to NOT take a snapshot. You may have a limited amount of disk space, or you may have performance concerns. Taking a snapshot reduces the performance of the virtual machine while the snapshot is being created.



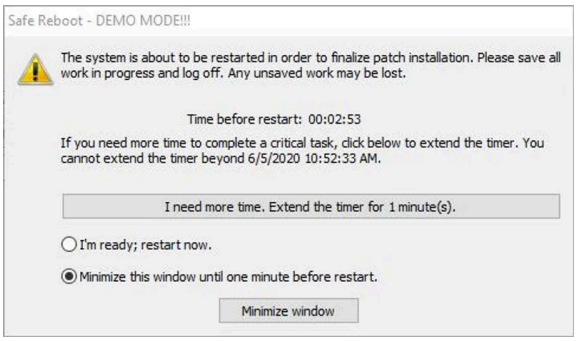
Field	Description
Take pre-deployment snapshots	If enabled, indicates that Security Controls will take a snapshot of the hosted virtual machine or the hosted virtual machine template before deploying missing patches or product levels. Taking a snapshot of the environment is a good precaution to take in the event there is a problem with the deployment or if at some point you simply want to revert to the original environment.
Take post-deployment snapshots	If enabled, indicates that Security Controls will take a snapshot of the offline virtual machine or virtual machine template after deploying missing patches or product levels. Taking a post-deployment snapshot of the environment is a good idea in the event there is a problem down the road and you want to revert to a time immediately following the patch deployment.
Maximum snapshots Security Controls **will manage**	If enabled, indicates the maximum number of snapshots that will be maintained for each offline virtual machine or virtual machine template. Only snapshots created by Security Controls are counted. If the threshold is exceeded the oldest snapshot is deleted. The threshold is checked each time a new pre-deployment or post-deployment snapshot is made. Snapshots are saved to disk and require a certain amount of storage space. It is important to limit the number of snapshots to avoid needless consumption of storage space.
Delete old snapshots created by Security Controls **(age in days)**	If enabled, indicates the number of days a snapshot created by Security Controls will be allowed to exist. Snapshots older than the specified number of days are automatically deleted. The threshold is checked each time a new pre-deployment or post-deployment snapshot is made.

You can choose to manage snapshot retention both by the number of snapshots and by the snapshot age. In this case, when a pre- or post-deployment snapshot is requested, all snapshots created by Security Controls that are older than the specified number of days are deleted. If the number of remaining snapshots still exceeds the maximum number specified, the oldest of those will be deleted until only the maximum number specified remain.

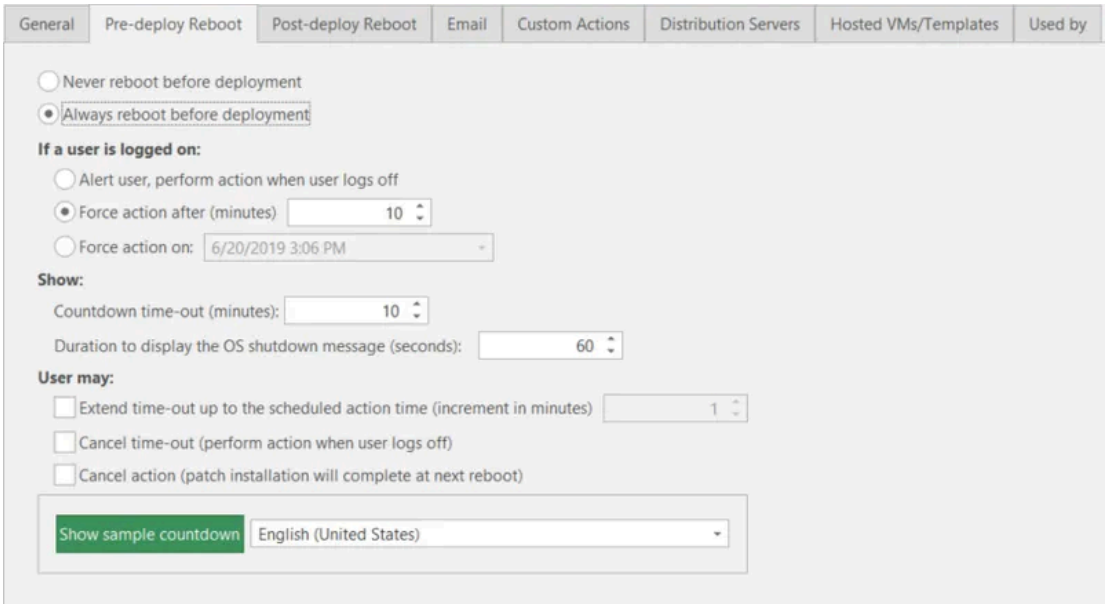
130. Deployment Template: Post-Deploy Reboot Tab

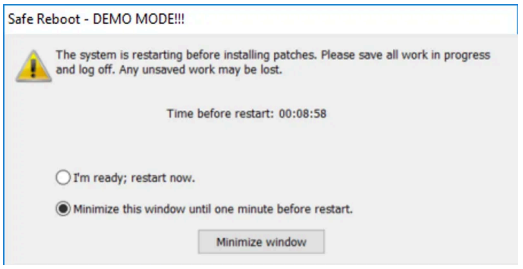


Field	Description
Never reboot after deployment	This SafeReboot capability specifies that it is unnecessary to reboot each machine after the patches are deployed. The remaining options on this tab will be disabled. As a rule, you should only enable this option when you are deploying patches that you know do not require a reboot.
Always reboot after deployment	This SafeReboot capability specifies that each machine should be reboot after the patches are deployed. This is the safest option when deploying patches as most patches require a reboot in order to complete, but there may be times when machines are rebooted unnecessarily.
Reboot when needed	This SafeReboot capability specifies that Security Controls will determine whether or not a reboot of each machine is required.
Schedule reboot	If you elect to reboot the machines, you can specify when the reboot should occur. You can: • Reboot the machines immediately after installation • Reboot at a specific time • Reboot at a specific date and time If a target machine is rebooted before a scheduled reboot occurs, the scheduled reboot is no longer necessary and will be cancelled.
Power action	You can specify what state you want to leave the machines after the reboot. • **Restart:** The machines are restarted and left in a powered on state. • **Restart, then sleep if possible:** The machines are restarted and then put into a sleep state. There is a two minute delay between the completion of the restart and the time the machines are put into the sleep state. The Microsoft Scheduler is used on each target machine to initiate the sleep state following the restart. For more detailed information about sleep state, see **Sleep and Hibernation Notes**. • **Restart, then hibernate if possible:** The machines are restarted and then put into a hibernation state. There is a two minute delay between the completion of the restart and the time the machines are put into the hibernate state. The Microsoft Scheduler is used on each target machine to initiate the hibernation state following the restart. • If a target machine is not **configured to allow hibernation**, the program will instead attempt to put the machine into a sleep state after the restart. If the machine cannot be put into a sleep state no action will occur. For more detailed information about hibernate state, see **Sleep and Hibernation Notes**. **Restart, then shut down:** The machines are restarted and then powered off. There is a two minute delay between the completion of the restart and the time the machines are shut down. This option is useful if you want to perform a reboot in order to complete a maintenance task but then want the machines to be shut down. The Microsoft Scheduler is used on each target machine to initiate the shutdown following the restart. • **Shut down only, do not restart:** The machines are powered off. This option is also useful if you simply want to make sure non-critical machines are turned off each night or over a weekend, saving energy.

Field	Description
	For more information about the power management capabilities of Security Controls, see **Power Management Overview**.
Use defaults **If a user is logged on**	This button is tied to the **Restart and power action** box. When you click **Use defaults**, all remaining options on the dialog will be changed to the values recommended for use with the currently selected **Restart and power action**. If you elect to restart the machines, you can specify the amount of warning that a logged-on user with an active session will receive. You can also choose the degree of control the user will have over the restart process. The options do not apply to inactive sessions such as locked machines or disconnected RDP sessions. You can: • Alert the user that a restart will occur when they log off. • Elect to force a restart after a number of minutes have passed. • Elect to force a restart at a specific date and time. • Show a countdown dialog on the user's machine in advance of the restart. To preview the dialog box that the user will see, click **Show sample countdown**. The language box to the right can be used to preview this dialog in different languages.  Select the duration to display the standard Windows shutdown message when the shutdown sequence is initiated. • Allow the user to extend the time-out countdown up to a specified maximum. The maximum can be specified as either a duration or as a specific latest time that the restart will occur. • Allow the user to cancel the time-out. If a time-out is cancelled the patches will not be deployed until the user logs off or manually restarts the machine. • Allow the user to cancel the restart. The patches will not be installed until the machine is restarted.

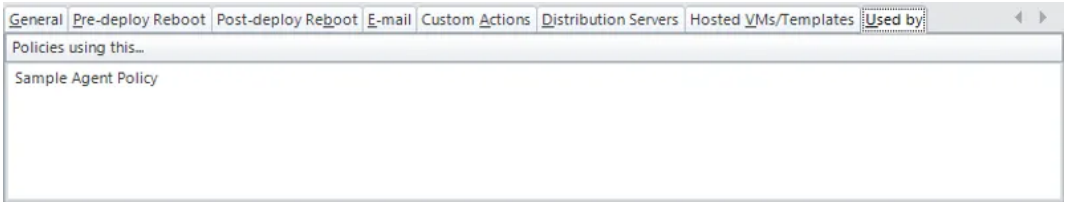
131. Deployment Template: Pre-Deploy Reboot Tab



Field	Description
Never reboot before deployment	This SafeReboot capability specifies that it is unnecessary to reboot each machine before the patches are deployed. The remaining options on this tab will be disabled.
Always reboot before deployment	This SafeReboot capability specifies that each machine should be reboot before the patches are deployed. It is considered a *best practice* to reboot machines before installing significant new software, especially for large software changes such as operating system product levels.
User Interaction	If you elect to reboot the machines, you can then specify the amount of warning that a logged-on user will receive and you can choose the degree of control the user will have over the reboot process. You can: • Alert the user that a restart will occur when they log off. • Elect to force a restart after a number of minutes have passed. • Elect to force a restart at a specific date and time. • Show a countdown dialog on the user's machine in advance of the restart. To preview the dialog box that the user will see, click **Show sample countdown**. The language box to the right can be used to preview this dialog in different languages.  Select the duration to display the standard Windows shutdown message when the shutdown sequence is initiated. • Allow the user to extend the time-out countdown up to a specified maximum. The maximum can be specified as either a duration or as a specific latest time that the restart will occur. • Allow the user to cancel the time-out. If a time-out is cancelled the patches will not be deployed until the user logs off or manually restarts the machine. • Allow the user to cancel the restart. The patches will not be installed until the machine is restarted.

132. Deployment Template: Used By Tab

This tab shows you the agent policies that are currently using this deployment template. This is important to know if you are considering modifying the deployment template, as it tells you what other areas of the program are affected.



133. DeployState view

The Reporting2.DeployState view defines deployment states.

Column Name	Data Type	Nullable	Description
Id	int		The deploy state id.
Value	nvarchar(100)		The value of the deploy state.
Description	nvarchar(512)		A description of the deploy state.

Content

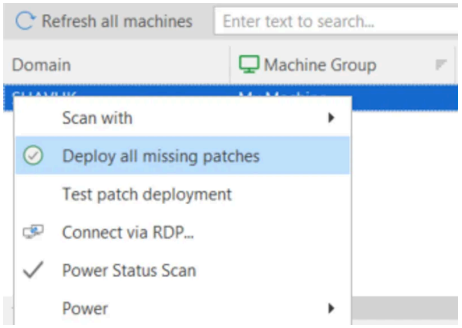
Run the following query to generate the contents for the Reporting2.DeployState view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[DeployState]
```

134. Deploying Patches to All Members of a Domain

Patches can be deployed to all members of a single domain. From within **Scan View** or **Machine View**, group the display by domain by sliding the **Domain** column to the first column. You can then deploy to the machines in the domain using the right-click **Deploy All Missing Patches** menu.



This will launch the **Deployment Configuration** window.

135. DetectedPatchState view

The Reporting2.DetectedPatchState view displays the state of a patch found on a machine.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
AssessedMachineStateId	int		The assessed machine state id. See [Reporting2].[AssessedMachineState].
PatchId	int		The patch id. See [Reporting2].[Patch].
ProductId	int		The product id. See [Reporting2].[Product].
InstalledOn	datetime	X	The date the patch was installed.
InstallStateId	int	X	The install state Id. See [Reporting2].[InstallState]

136. Determining How Many Distribution Servers to Use

Do You Need a Distribution Server?

To determine if you should use one or more distribution servers with Security Controls, apply the following formula:

- If **# of machines * 10Kb > available bandwidth**, then you need at least one distribution server.

Examples

Assume available bandwidth = 500 Kb:

- 100 machines: 100 machines * 10Kb = 1000Kb > 500Kb (need distribution server)
- 20 machines: 20 machines * 10Kb = 200Kb < 500Kb (do not need distribution server)

If You Need Distribution Servers, How Many?

If (using the formula above) you determine you need one or more distribution servers, you still need to determine exactly how many distribution servers are needed. Determining the number of distribution servers that are needed is very simple. The general rule is:

- Use one distribution server for every 2500 machines

For example, if you have 7500 machines you should plan on using three distribution servers.

137. Determining Patch Replacements

One of the benefits of Security Controls is that it only shows you patches that are necessary for your machine to be up to date, and it doesn't show you earlier patches that have been replaced by later patches (although you can **configure the program to do this** if you want).

Many recent Microsoft security patches have been released as 'Cumulative Rollup' patches. Rollup patches include all the previously released security patches for the given product as well as including fixes for the most recently announced issues. A cumulative patch that completely encompasses an earlier patch is said to replace the earlier patch. In order for a patch to be replaced, all the files in the earlier patch must be included in the later patch, all file versions must be revved higher than those in the earlier patch (or the file versions must be the same as the earlier patch), and associated functional registry keys must be included in the replacement patch.

The data definition file contains information on each of the replaced patches. Security Controls evaluates the patch replacement codes to identify patches that are applicable to each system being scanned. Particular attention is paid to replaced patches that span product level applicability. As an example:

- Patch A is applicable to Windows 10 1709
- Patch B replaces Patch A and is applicable to both Windows 10 1709 and 1803
- Patch C replaces Patch B and is applicable to Windows 10 1803

Security Controls correctly scans for the presence of Patch C on Windows 10 1803 machines and for Patch B on Windows 10 1709 machines - even though Patch B is marked in the data file as being replaced by Patch C.

138. Determining Patch Status

Security Controls performs a detailed analysis of each scanned machine to accurately determine its patch status. Unlike other patch management systems, the Security Controls engine goes far beyond the traditional patch detection mechanisms that rely solely on the presence of registry keys.

For Security Controls to determine if a specific patch is or is not installed on a given computer, two items are typically evaluated:

- The registry keys that are installed by the patch
- The file versions for all files installed by the patch

Security Controls compares file versions in the data definition file to the files versions on the computer that is being scanned. If any of the file versions on the scanned computer are less than those stored in the data file, the associated security patch is identified as not installed and the results are displayed on the screen. Specific details about why a patch is considered not installed are also displayed.

139. Determining the Currently-Assigned Role

Information about the currently-assigned role is available in the **About** Security Controls dialog.

1. Select **Help > About** Security Controls.
2. In the upper portion of the dialog you will be able to view the current role assignment.



140. Determining Which Machines Have Security Controls Agent

You can use Machine View to easily determine which machines in your network have Security Controls Agent installed.

1. Select **View > Machines** to view a list of all machines that have been scanned at least once by the program.

> If you want to make sure you get a list of all machines in your network, perform a scan of all machines in your network before going to Machine View.

In the top pane, click the **Agent State** column heading.
This will sort the table, grouping together all machines that have Security Controls Agent installed and placing that group at the top of the table. Click the icon a second time to move to the top of the table the group of machines without Security Controls Agent installed.

3. There are several possible states:
    - Installed (Active)
    - Install Pending
    - Registered Awaiting CheckIn
    - Deployed Awaiting Contact
    - Awaiting Deployment
    - Uninstall Pending
    - Uninstalled
    - None (No Agent)

To sort the list by policy name, click the **Assigned Agent Policy** column heading.

> TIP: Another option in Machine View is to select **Has an Agent Policy** in the **Smart Filters** box. Only machines with Security Controls Agent installed will be displayed.

141. Using Disconnected Mode

If a Security Controls console is in disconnected mode it means it will not attempt to download newer definition files (engine components and data files). Disconnected mode is typically used by sites that require the use of fixed versions of data that have been approved for use. Disconnected mode is also useful if your security policy requires you to perform scans and deployments without downloading data files from the Web.

There are two ways to put the console into disconnected mode:

- Select **Tools > Auto-update definitions** and make sure the command is not enabled
- Select **Tools > Options > Downloads** and then clear the **Auto-update definitions (before scans)** check box

When the console is in disconnected mode the data files already resident on your local machine will be used during all scans and deployments. See **Managing Data Files** for more information.

> Putting a console into disconnected mode does not necessarily mean that the console is disconnected from the Internet. That is a different scenario and is described in **What is a Disconnected Console Configuration?**. Also, disconnected mode has nothing to do with patches. If you are connected to the Internet or a designated distribution server, the console will download required patches even if **Auto-update definitions** is disabled.

Be Careful if Your Site Uses Agents

If you use **agents** you must be careful when putting your console into disconnected mode. If an agent contains newer definition files than the console, and that agent tries to report new results to the console database, the console will reject the updates. If this happens you will need to **manually download new definition files** and copy the files to the console's *|DataFiles* directory. If you are using a distribution server you must then manually **synchronize the console with the distribution server**.

To prevent this issue from happening in the first place, make sure your agents get their definition files from a distribution server and that the files on the distribution server exactly match the files being used by the console.

Possible Issue with .NET Framework Prerequisite

When you run in disconnected mode the console may not detect that the full version of .NET Framework is available. See **Installing the Prerequisites** for a link to use to download the full version of .NET Framework.

142. Discovering Machines

When scanning by domain name, Security Controls does the following to discover the machines in the domain:

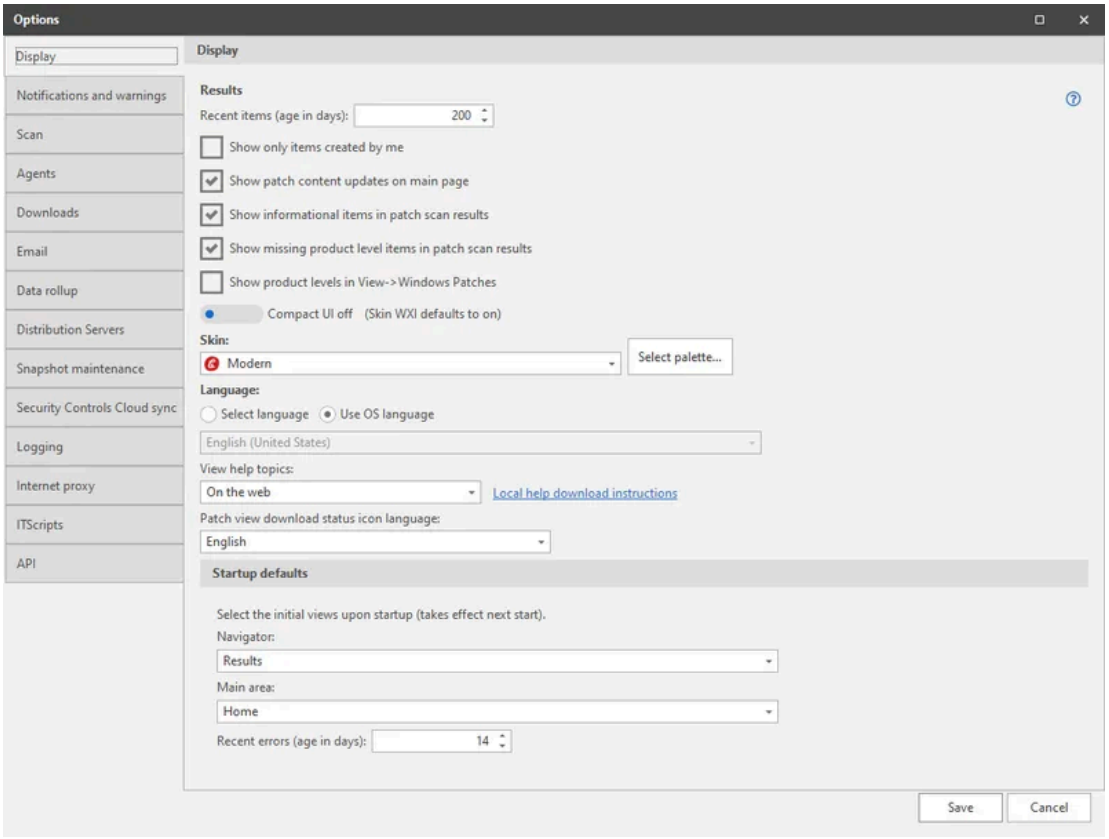
- The domain controller is contacted and its list of machine accounts is enumerated. Browse credentials defined within the machine group are used for this process. If browse credentials are not provided, the credentials of the user running the scan are used.

> You can reduce the number of machines that the program will attempt to connect to by enabling the **Use only the browse list scan option**.

Machines are also enumerated from the network browse list which is the same list of machines seen on a per domain basis when viewing the network, or similar to 'net view /domain:domainname'. No special permissions are required to enumerate machine names this way as Security Controls is using UDP port 137 (NetBIOS name service) to enumerate the browse list. If the scanning machine has just been connected to the network, it may take up to 15 minutes until the machine synchronizes with the browse master and for this list to become available to the scanning machine. The list of machines that are returned represent machines that are currently online or have been within the last 15 minutes. Machines that are 'hidden' via registry modifications won't appear as they don't propagate their machine names to the network browse list. If the scanning machine doesn't have access to the browse list, or the machines are behind filtering devices where the browse list isn't updated, etc. then no machines will appear.

143. Display Options

The **Display Options** dialog allows you to specify the optional items you want displayed in the program.

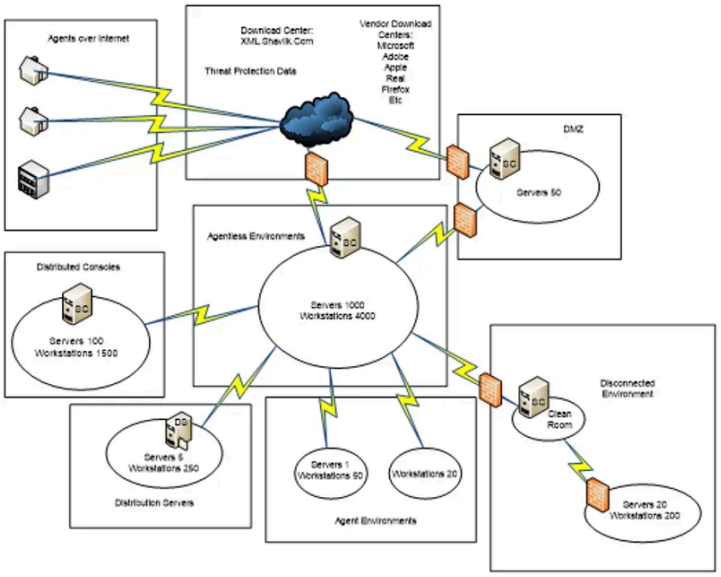


Field	Description
Recent Items	Specifies how many days' worth of scans and deployments to show in the **Results** list in the navigation pane. It also defines how many days' worth of recent patch deployments to show in **Deployment Tracker**. The default value is 200 days.
Show only items created by me	If enabled, shows only those scans and templates that have been created by the current user.
Show patch content updates on main page	If enabled, displays the date that the patch content was last updated. The date is displayed in the upper-right corner of the interface. If you click the date the **Patch Content Update Details** dialog is displayed. Use this dialog to view more detailed information about the current patch data and about previous patch data releases. For more information, see **Navigating the Interface**.
Show informational items in patch scan results	If enabled, displays informational items on the **Patches** tab in **Scan View** and **Machine View**.
Show missing product level items in patch scan results	If enabled, displays missing product level items on the **Patches** tab in **Scan View** and **Machine View**.
Show product levels in View > Windows Patches	If enabled, displays product levels in **Patch View**. Product levels (1803, TH2, SP1, etc.) are by default filtered out from the content displayed in Patch View. This is because product levels are typically not needed in this view; they cannot be added to patch groups and you cannot view detailed information about product levels like you can for patches. The most common reason to display product levels in Patch View is so you can download them in advance of a deployment.
Compact UI on/off	If enabled, reduces the amount of space used to display items in the user interface.
Skin	Specifies the color theme you want to use for the Security Controls interface. If you make a change, the new skin is temporarily applied to the interface so that you can determine if you like it. To make the change permanent, click **Save**; to revert to the original selection, click **Cancel**.
Language	Specifies the language that will be used within the Security Controls interface. You have two options: • **Select language:** If enabled, use the drop-down list to select the desired language. • **Use OS language:** If enabled, the console machine's operating system language setting will determine which language to use within the Security Controls interface. This option will override the language specified by the **Select language** option. This is the default option.

Field	Description
View help topics	Specifies how to view Security Controls help topics. • **On the web:** The help topics will be displayed using a web browser. The help text will be localized according to the language specified in the **Language** box. This option requires an Internet connection to the console. • **Local help viewer:** The help topics will be displayed locally on the console using a .chm file. The help text will be in English. This is the option you should choose if you require an offline version of the help topics. If you choose **Local help viewer**, be sure to click **Local help download instructions** to learn how to manually download and configure the .chm file. The .chm file is not automatically provided with the product. • Local help download instructions: This only applies if you choose **Local help viewer**. It provides instructions for manually downloading and unlocking the .chm help file.
Patch view download status indicator language	Click the drop-down list and select the language that will be represented by the download status indicator located in the top pane of Patch View. If you select the **Universal Installer** option, it represents the universal patch package file that can be used by all languages. For example, assume you select German in this field. If you then go to Patch View and the download status indicator for a particular patch looks like this  (colored) it means the German language version of the patch has been downloaded. If the download status indicator looks like this  (clear), however, it means the German language version of the patch has **not** been downloaded. If the universal installer icon is shown it means that only universal patches are available for the product. For more information, see How to Download Different Language Versions of a Patch.
Navigator	Specifies which program feature to use as the default in the navigation pane when the program is started.
Main area	Specifies what to display in the right pane when the program is started.
Recent errors (age in days)	Specifies how many days' worth of errors to show on the home page.

144. Distributed Environment Management

Security Controls provides a number of features to allow for management of an environment. The following diagram shows a variety of scenarios that will be discussed in this section.



Agentless Environments

Security Controls can be rapidly configured to support large numbers of machines agentlessly. By creating a machine group from hostnames, domains, IP addresses/ranges or OUs, you can identify machines you want to scan and specify administrative credentials for the machines.

Distributed Consoles

Multiple Security Controls consoles can be configured to distribute workload across large numbers of machines and across WANs to distribute management of the enterprise. Data can then be rolled up to a central console for reporting purposes.

Distribution Servers

To reduce WAN traffic a distribution server can be setup at a remote site to distribute data, engines, patches, and service packs to a remote site, reducing data transfer.

Disconnected Environments

Security Controls can be configured to pull data, engines, patches, and service packs from an internal source.

- For partially disconnected environments you can use these features to download from an Internet-connected machine. You then move the files to a clean room and from there into the disconnected environment.
- In a fully disconnected environment the connected console would download everything. You then use a manual or “sneaker net” process to move the files from one console to another.

Agents

Security Controls also includes agents. With the agent, administrators are able to work around many obstacles and reach machines where agentless scans may not gain total coverage. Low bandwidth WAN links, laptops that typically leave the environment, and secure environments such as DMZs are cases where an agent may be ideal.

Demilitarized Zone (DMZ)

Security Controls can be configured in a number of ways to support demilitarized zones (DMZs). The option to use agentless scans by IP address or IP ranges allows administrators to work around name resolution if it is not available in the DMZ. A distributed console can be configured in the DMZ if IP rules on the firewall are not acceptable to support agentless scanning from the network into the DMZ.

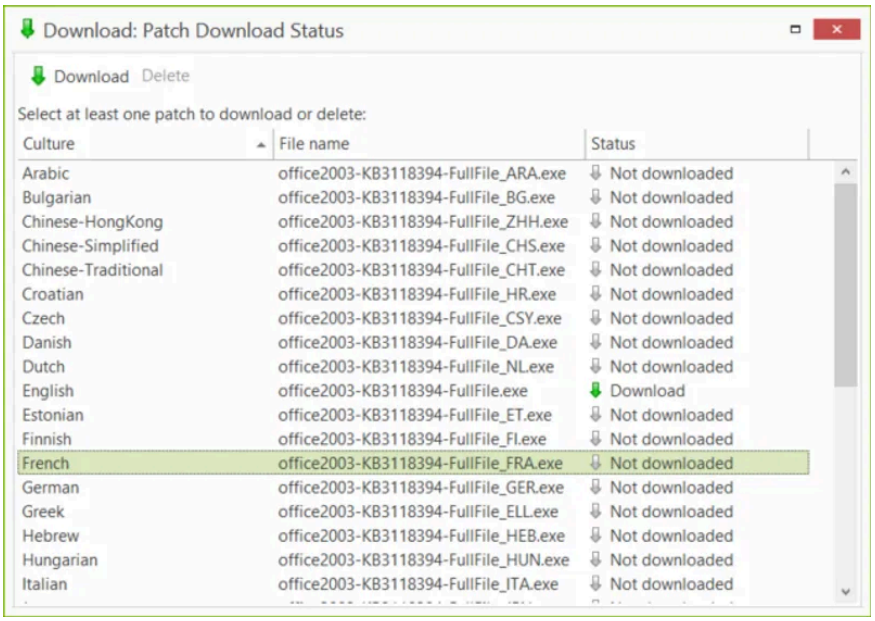
Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

145. How to Download Different Language Versions of a Patch

When you initiate a download by right-clicking one or more patches, Security Controls will immediately begin the download process. The program will automatically detect the operating system languages used on your **managed machines** and then download only those language versions of the patch file that are needed. In many cases, all that is needed is a single universal patch package file that can be used by all languages. If you do not have managed machines that require a particular patch, the program will use the **Patch View download status indicator language option** as the default.

If you initiate the patch download from the **Patch Information** tab in Scan View, Machine View or Patch View, you will have the opportunity to manually select the individual files you want to download. Simply select the desired language versions and then click **Download**.



146. Downloading Patches and Product Levels

Security Controls automatically downloads necessary patches as part of the deployment process, removing the need to manually download them in advance. If needed, however, Security Controls also provides the ability to manually download patches to the **patch download directory** prior to deployment. There are multiple ways to download patch files.

To download a single patch

- From the middle pane of **Scan View**, right-click the patch and choose **Download**.
- From the bottom pane of **Scan View**, on the **Patch Information** tab click **Download**.
- From within the bottom pane of **Machine View**, on the **Patch Information** tab click **Download**.
- From within the bottom pane of **Patch View**, on the **Patch Information** tab click **Download**.

To download multiple patches

- From within the middle pane of **Scan View**, right-click the selected patches and choose **Download**.
- From within the middle pane of **Machine View**, right-click the selected patches and choose **Download**.
- From within the top pane of **Patch View**, right-click the selected patches and choose **Download**.

To download product levels

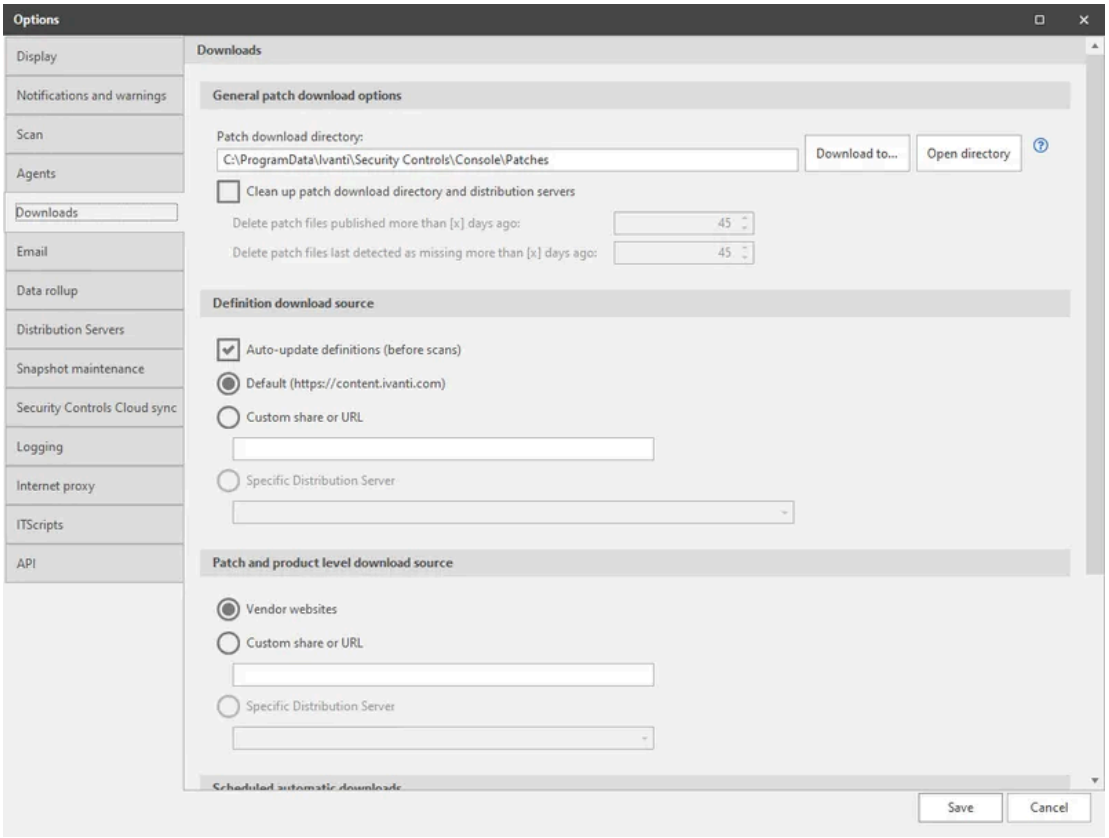
- From within the middle pane of **Scan View**, right-click a product level and choose **Download**.
- From within the middle pane of **Machine View**, right-click a product level and choose **Download**.

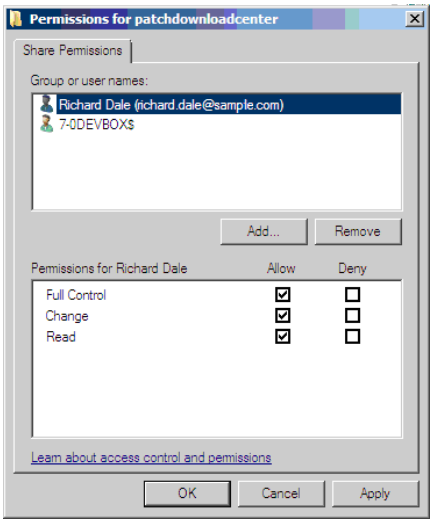
Tips

- If you have trouble downloading a patch, try clearing your browser cache files before attempting another download.
- For information about downloading any custom patches you may have created, please see **Overview of the Custom XML Process**.

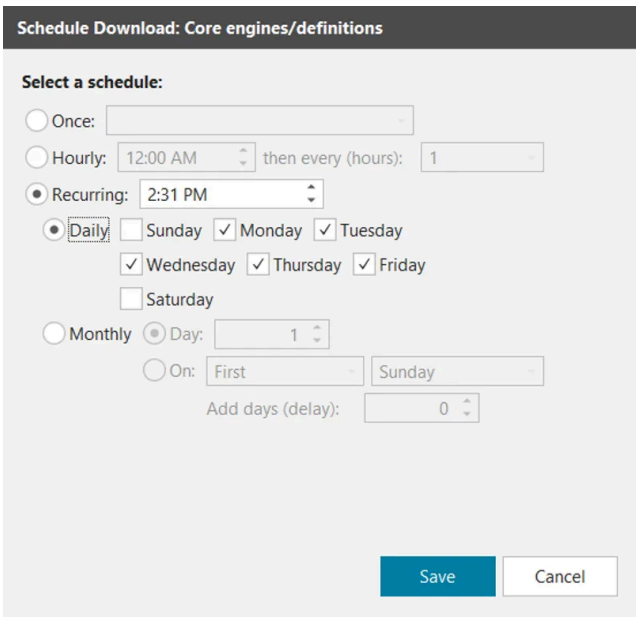
147. Download Options

The **Downloads** tab allows you to specify the location from which the files used by the program will be downloaded and refreshed. The files include the engine components, the news file displayed on the home page, and the deployment information file, as well as download source for the patch and product level files. The program will check an Internet location or the specified distribution server to determine if newer versions of the files are available.



Field	Description
Patch download directory	Displays the location of the patch download directory (also known as the patch store). This directory is used to store all patches that are downloaded in advance of a patch deployment. To change the location, click the browse button. IMPORTANT! If the directory resides on a network drive be sure to use the UNC naming convention; DO NOT SPECIFY A MAPPED DRIVE. If desired, you can specify a remote share directory for the patch download directory. In order for this to work, appropriate permissions need to be set on the remote directory. Both the Security Controls console user and the console machine need to be granted access to the download directory. The console user should have read/write permission to the share and the console machine needs read access. When specifying share permissions for a machine, you must append a "$" to the end of the machine name.  In some configurations additional users may need to be granted access to the download directory. If you specify machine or machine group credentials for machines that download patches from a distribution server, the specified user accounts will require read access to the download directory share. Making the download directory share readable by everyone may or may not be an effective strategy. It depends on: • Whether the credential users and the download directory host belong to the same (or trusted) domain(s) • The specifics of the local security policy
Clean up patch download directory and distribution servers	Allows for the automatic clean up of your patch download directory and your distribution server(s). Any patches that are unlikely to be used in the future will be deleted from these locations. If the download directory is set to be used as a distribution server, core files are not deleted. This option is superior to the **ITScripts Console Clean Up script**, which is not automated nor does it perform clean up of distribution servers. There are two ways to define which patches will be deleted. A patch file must meet both criteria in order to be deleted. • **Delete patch files published more the [x] days ago:** Patches that were published a long time ago are unlikely to be needed and can be safely deleted. The default value is to delete patches that were published more than 45 days ago. • **Delete patch files last detected as missing more than [x] days ago:** Patches detected as missing by scans older than the threshold will be deleted. Patches detected as missing by more recent scans will not be

Field	Description
	deleted. The default value for the threshold is 45 days. Example: Assume you use the default value of 45 days for both options. If a patch file was published 50 days ago, but it was detected as missing in a patch scan that was performed 40 days ago, the patch file will not be deleted. Sideloaded patches are an exception and will not be deleted. Security Controls Agent will not delete any patch files that it has not downloaded. Patches that were previously sideloaded remain intact. However, any patch files that are manually placed in the patch folder are not treated as sideloaded content and will be deleted automatically. The patch download directory clean up task will run automatically once a day. Your distribution servers will be cleaned as they are synchronized with the console.
Definition download source	You can specify where the latest engine components and data files downloaded by this console are located. The available options are: • **Auto-update definitions (before scans)**: If enabled, will cause the program to automatically check for and download updated data definition files whenever a new scan is performed. Enabling this check box will also enable the Tools > Auto-update definitions menu command. • **Default (https://content.ivanti.com)**: Indicates you want to use the default location when downloading the files. The files are located at https://content.ivanti.com. • **Custom share or URL**: You must specify the path name of the share or the URL of the website that will be used when downloading files. It is the administrator's responsibility to make the files available at this location. • **Specific Distribution Server**: You must select the name of the distribution server that will be used when downloading files. You must have previously configured one or more distribution servers in order for the names to be pre-populated in this box. The newest versions of engines and data files can be periodically downloaded and copied to the distribution servers using the server synchronization feature. There are unique credential requirements when using a distribution server as the download source. For more information see Configuring Distribution Servers.
Patch and product level download source	You can specify where the latest patch and product level files downloaded by this console are located. The available options are: • **Vendor websites:** Patches deployed from the console are downloaded directly from the websites of the companies that author the patches. This is the default. The location of the websites are stored in the patch information file. • The other two download options are used if this console does not have an Internet connection or when the patches and product levels are being pre-downloaded to some central location. **Custom share or URL**: If enabled, you must specify the path name of the share or the URL of the website that will be used when downloading files. It is the administrator's responsibility to make the files available at this location. • **Specific Distribution Server**: If enabled, you must select the distribution server that will be used when downloading patch files. You must have previously configured one or more distribution servers in order for the names to be pre-populated in this box. For more information see Configuring Distribution Servers. This option is typically used by unattended console or disconnected console configurations. The patches and product levels are downloaded by a central console, which then pushes the files to the distribution server.

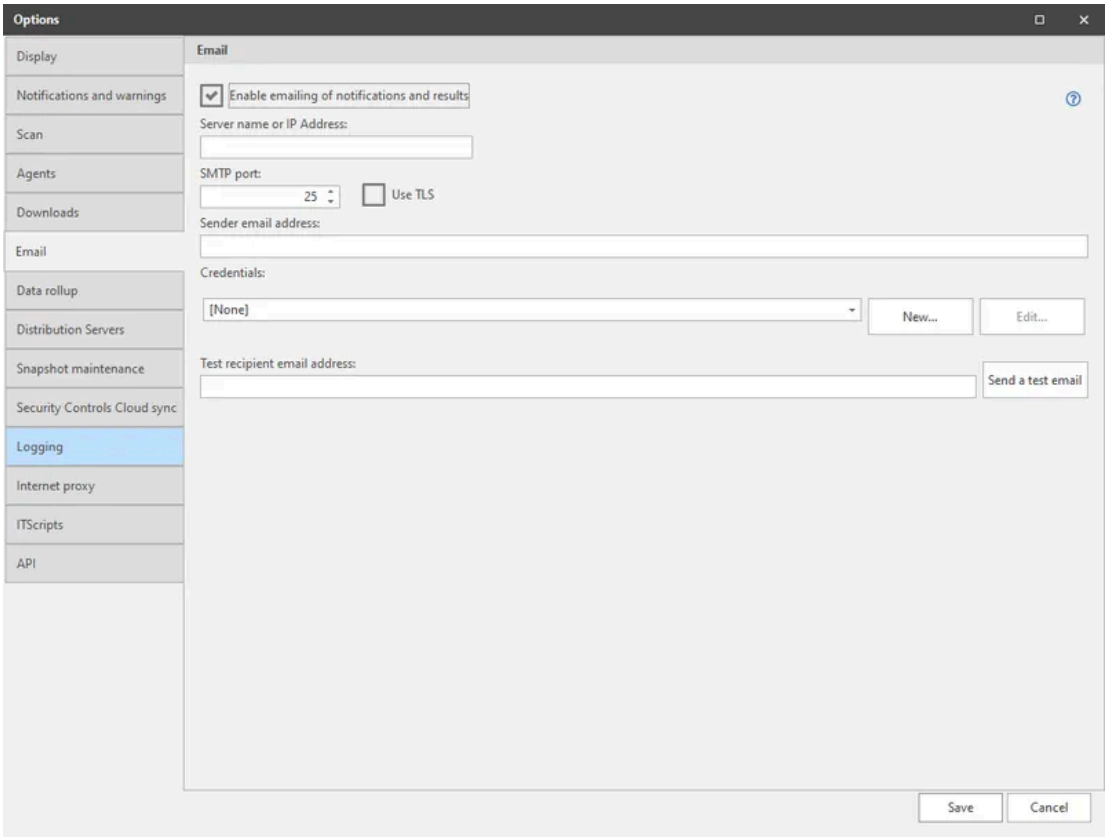
Field	Description
	One interesting but necessary side effect of enabling this option is that you will not be able to schedule an automatic synchronization for the distribution server you specify here. Why? Because in this particular case you do not want the console to synchronize with the distribution server. Doing so would cause the contents of the distribution server (the patches and product levels) to be overwritten by the contents of the console (which may not contain anything at all).
Scheduled automatic downloads	You can configure the program to automatically download the latest versions of the engine components and the data definition files on a regular basis. This can speed your scan processes by making the necessary files available in advance of a scan. You can also choose to automatically download patches and product levels that are likely to be used in future patch deployments. 1. Click **Add**. The **Schedule Download** dialog appears.  Specify when you want the download to occur. The **Add delay (days)** box (available if you download on a monthly basis) allows you to delay the download by up to 31 days. For example, you might use this to schedule a monthly download that is always performed four days after Patch Tuesday. You do this by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by four days. 3. Click **Save**. The new scheduled download entry appears. At the scheduled time, the appropriate engines and definition files will be downloaded to the console. 4. If you want to use the Predictive Patch feature, enable the **Predictive patch downloads** check box. If enabled, patches that are likely to be deployed in the near future are automatically downloaded to the patch download directory. The patches will be downloaded immediately following the scheduled download of the core engines and definitions. Downloading patches in advance of their anticipated deployment will help speed the deployment process. This feature is beneficial for agentless deployments and for agents that deploy patches using the services of a distribution server. Here are some additional details about Predictive Patch: • The following patches will be downloaded to the console's download directory:

Field	Description
	◦ Missing patches that were detected by recent scans but that have not yet been downloaded. A recent scan is defined as a patch scan that was performed within the last 45 days. ◦ Missing patches for products that Security Controls can deduce are on your target machines ◦ Patches that were added to the data definition file within the last 45 days and that apply to products on your target machines. New or missing product levels will be downloaded • The patches and product levels will be downloaded according to age (the most recent will be downloaded first) • The process will download up to 5GB of patches and product levels during a scheduled download session • Patches that already exist in the download directory will not be downloaded. • You can **synchronize Predictive Patch with your distribution servers** so that they receive copies of the downloaded patches • An entry is recorded in **Event History** every time patches are downloaded to the console by Predictive Patch • The patch download is triggered by either a scheduled download of the core engines and definitions or by clicking **Run now** when **Core engines/definitions** is selected • If a patch contains different packages for different languages, only those languages supported by your products are downloaded • Predictive Patch will not download software distribution patches (patches that are actually installation packages for free third-party applications)

Using a Remote UNC Share Directory

148. Email Options

The **Email** tab enables you to specify if you want to use the email feature, and it lets you define the properties of the SMTP server used for sending the email messages and alerts. (See **Email Overview** for more details). To use this feature, enable the **Enable emailing of notifications and results** check box and then specify the name or IP address of the SMTP server you use.



Field	Description
Enable emailing of notifications and results	If you want to use the email feature, enable this check box. Enabling this check box enables the related options on this dialog.
Server name or IP Address	Specify the name or IP address of your local SMTP server. For example: Exchange2.YourCompany.com
SMTP Port	Specify the port used by the SMTP server. The default value is 25.
Use TLS	If you want the target machines to contact the SMTP server using a Transport Layer Security (TLS) connection, enable this check box.
Sender email address	Specify the email address that will be inserted into the **From:** address field of messages that are sent to users. If the default address causes problems for your SMTP server, change the address to an email address accepted by your SMTP server. (Some SMTP servers only accept mail from particular addresses or domains.)
Credentials	Select the credential (the user name and password pair) used to authenticate to the SMTP server. Only shared credentials are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See **Defining Credentials** for information on how to share a credential.
Test recipient email address	Specify a known email address you want to use when testing the email process.
Send a test email	To verify the program can use the specified credentials to contact the SMTP server, click this button.

149. Editions of the Program

There are several different editions of Security Controls. Each edition provides a different level of capabilities. To determine which edition you are running, select **Help > About** to view program details.

This section provides a synopsis of each available edition.

Security Controls, Standard Edition

This is the standard product offering. The Standard Edition includes patch management, asset inventory, power management and ITScript capabilities.

Security Controls, Trial Edition

Security Controls is available on a trial basis. This enables you to test all the capabilities of Security Controls, but only for 60 days. You are also limited to 50 license seats. When the trial license expires the program will stop refreshing its data definition files and many of the program features will no longer be available.

Security Controls, Government Edition

When you purchase the Government Edition of Security Controls you will receive a license key that enables you to use the Information Assurance Vulnerability Alert (IAVA) Reporter. The IAVA-specific files are automatically installed when the Standard Edition of Security Controls is installed. For more information about IAVA, see **IAVA Overview**.

150. Email Overview

The email feature enables you to send email alerts and messages to specified users. This feature has a wide range of applications. You can send scan results and scan reports and you can notify users of pending actions such as patch deployments and reboots.

The email capability is very easy to use. You simply:

- Define your email contacts in the local **Address Book**
- **Define the SMTP server** used for email
- If necessary, **specify the credentials** required to send email messages
- Use the icons in the program interface to **send messages** to specified recipients as needed

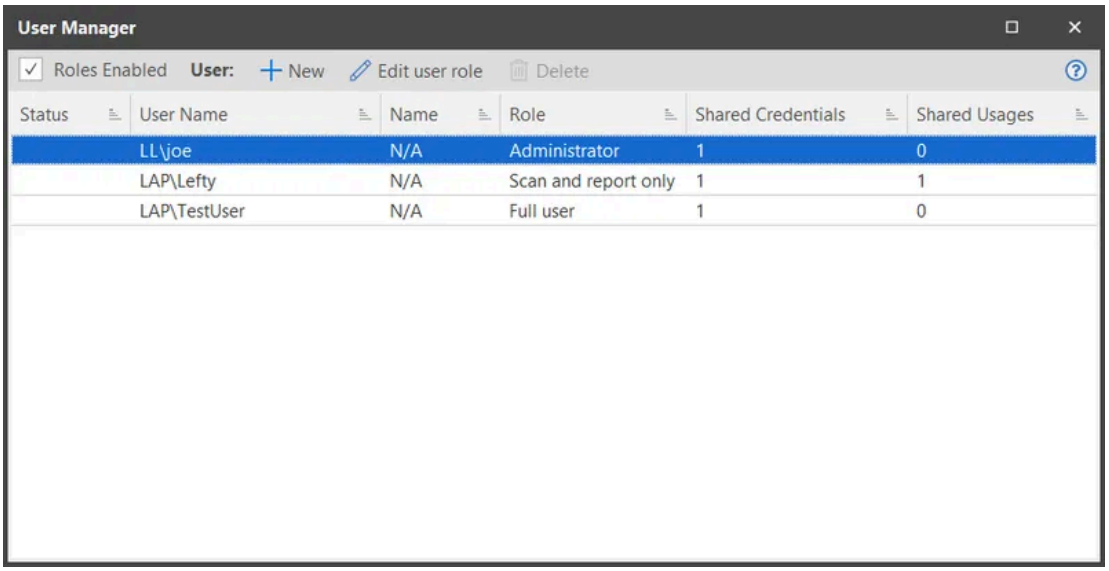
151. Enabling and Disabling Role-Based Administration

Enabling Role-Based Administration

1. Select **Manage > Users**.
   The **Users Manager** dialog is displayed.
2. Enable the **Roles enabled** check box.

> If enabled, this will prohibit other users from accessing this application unless they are explicitly configured and assigned to one of the existing roles.

You must have defined at least one user with the *Administrator* role in order to enable role-based administration. See **User Manager** for detailed information.



Role-based administration takes effect the next time the program is launched.
Add users and assign roles as needed.

Disabling Role-Based Administration

To disable role-based administration, clear the **Roles enabled** check box.

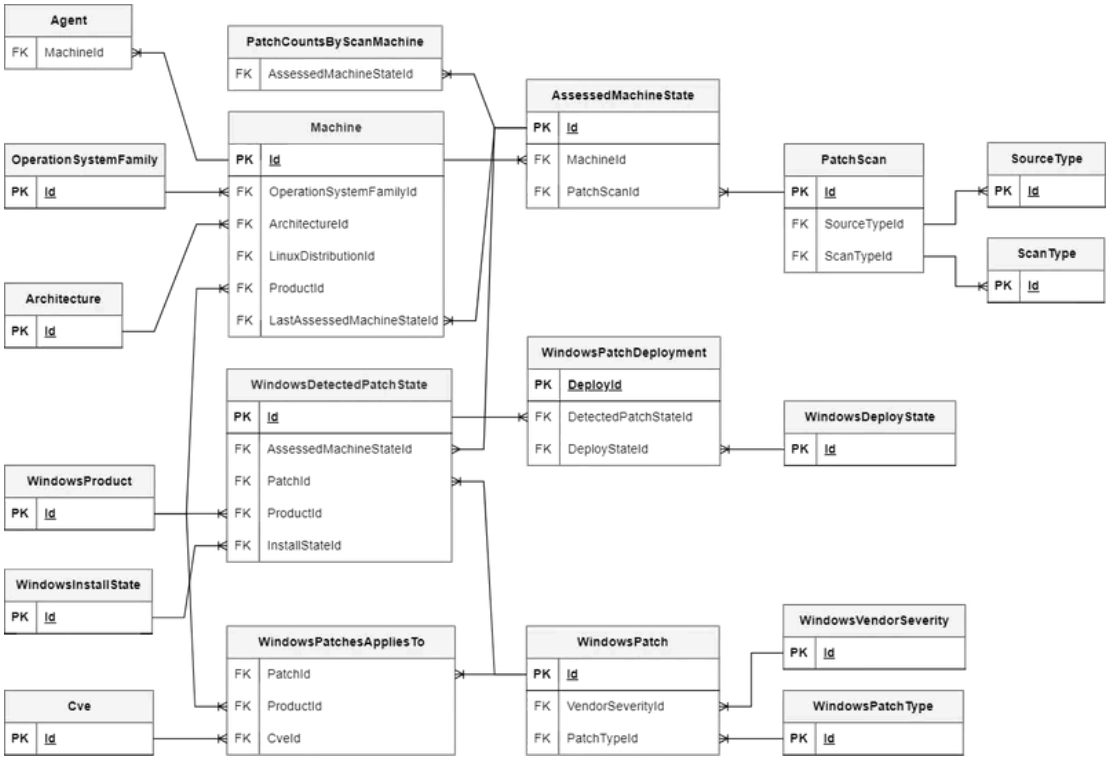
After disabling role-based administration, the next time that Security Controls is launched all users will have full access to the program. Any users that are defined in the **User Manager** dialog will remain but their role assignments will be ignored.

152. Entity Relationships

This page shows the entity relationships in the Reporting3 views, which contain information about Windows and contentless Linux data.

Windows

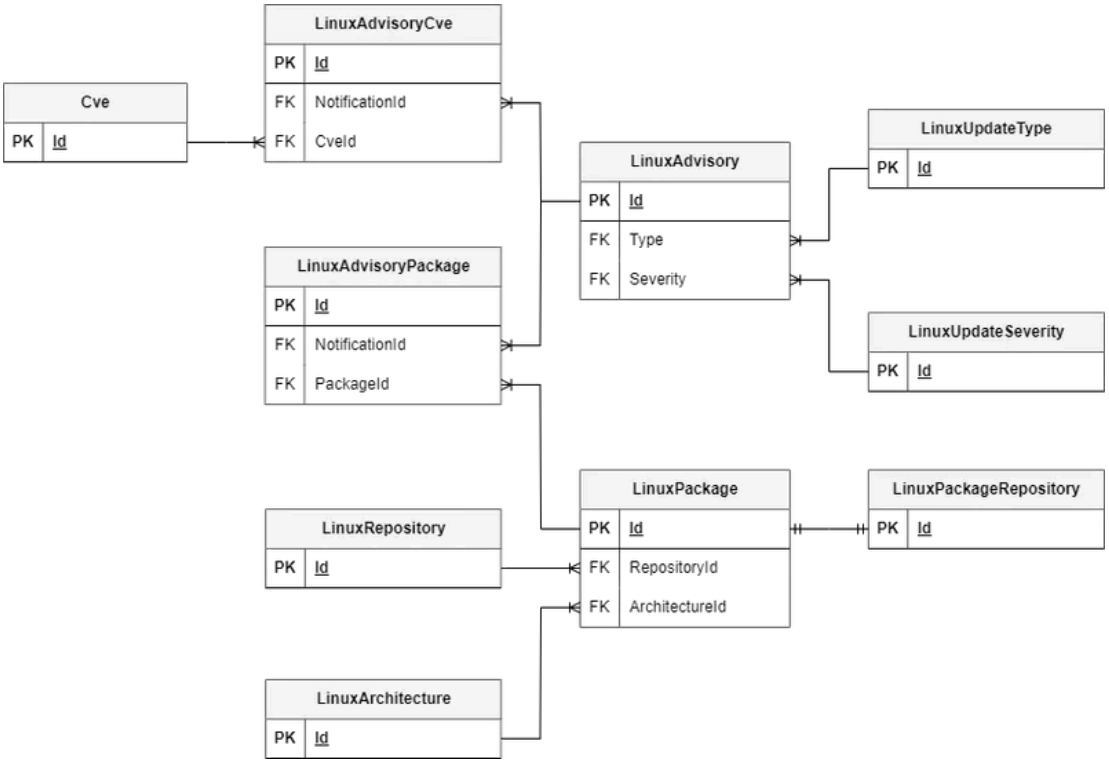
This graphic shows the relationships between the Windows views in the SecurityControls database.



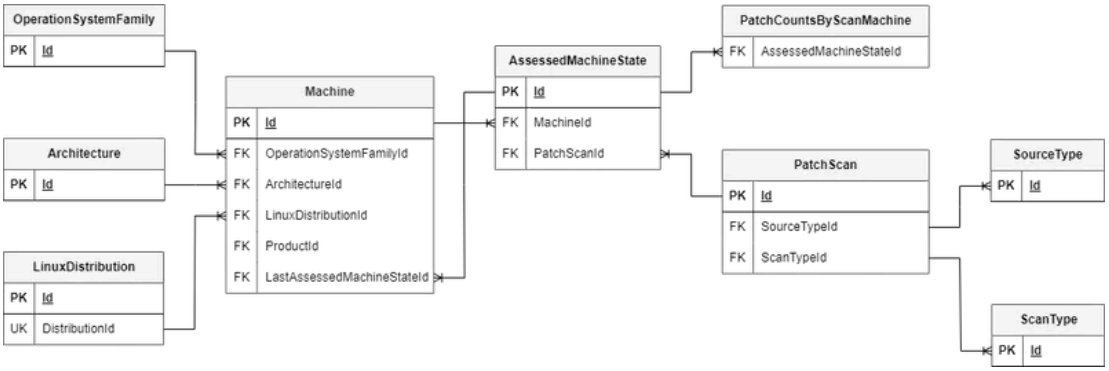
Linux (contentless)

These graphics shows the relationships between the content-based Linux views in the SecurityControls database.

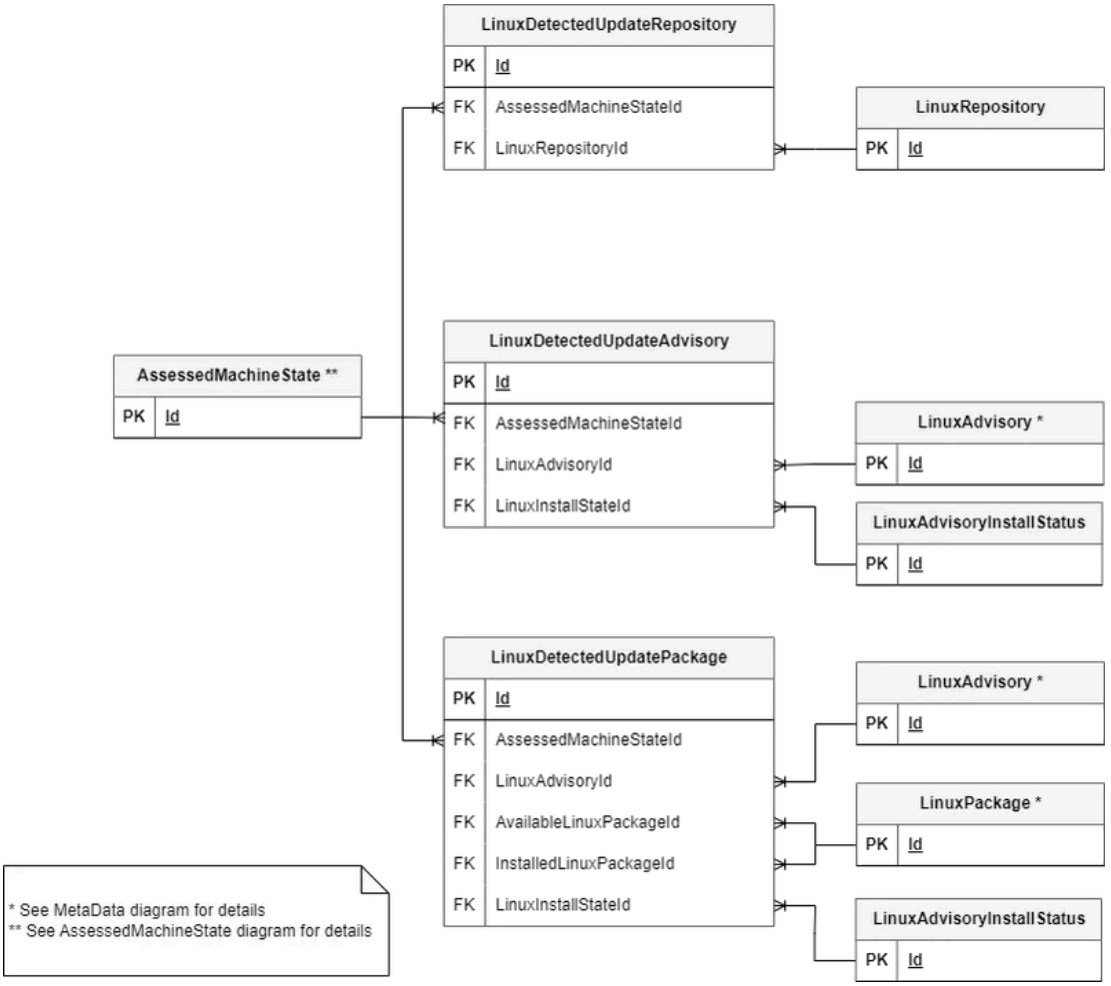
Metadata:



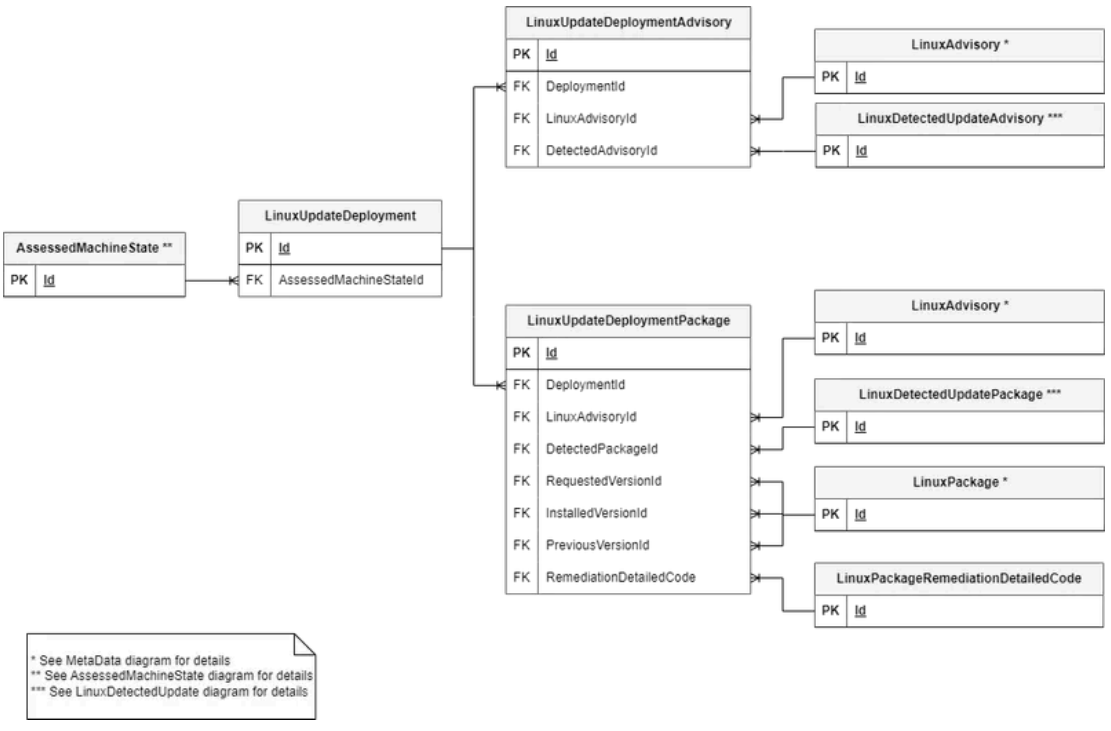
Assessed machine state:



Detected update:

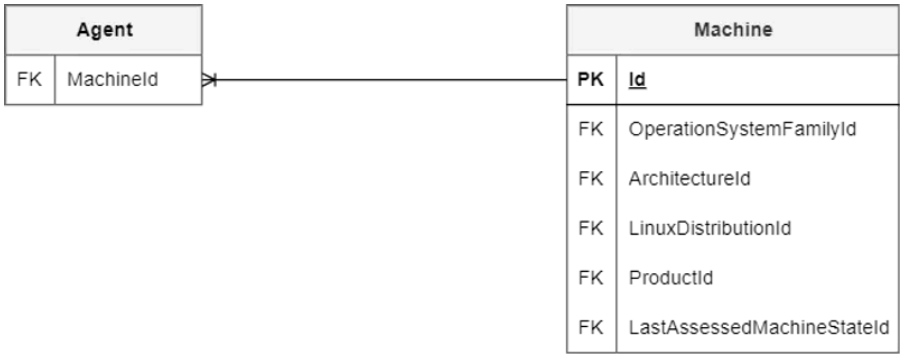


Update deployment:



Agent

This graphic shows the relationships between the agent views in the SecurityControls database.

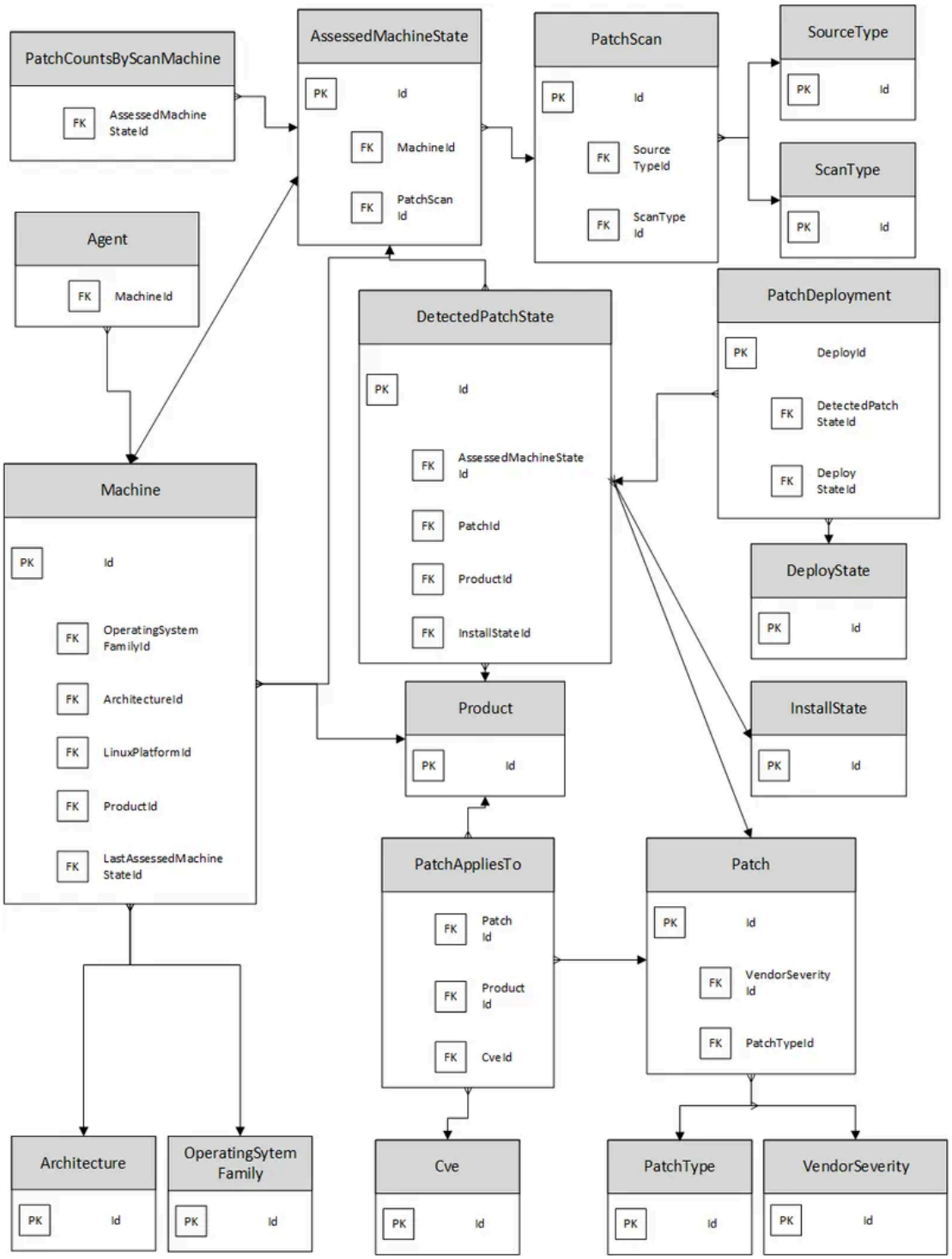


153. Entity Relationships

This page shows the entity relationships in the Reporting2 views, which contain information about Windows and content-based Linux data.

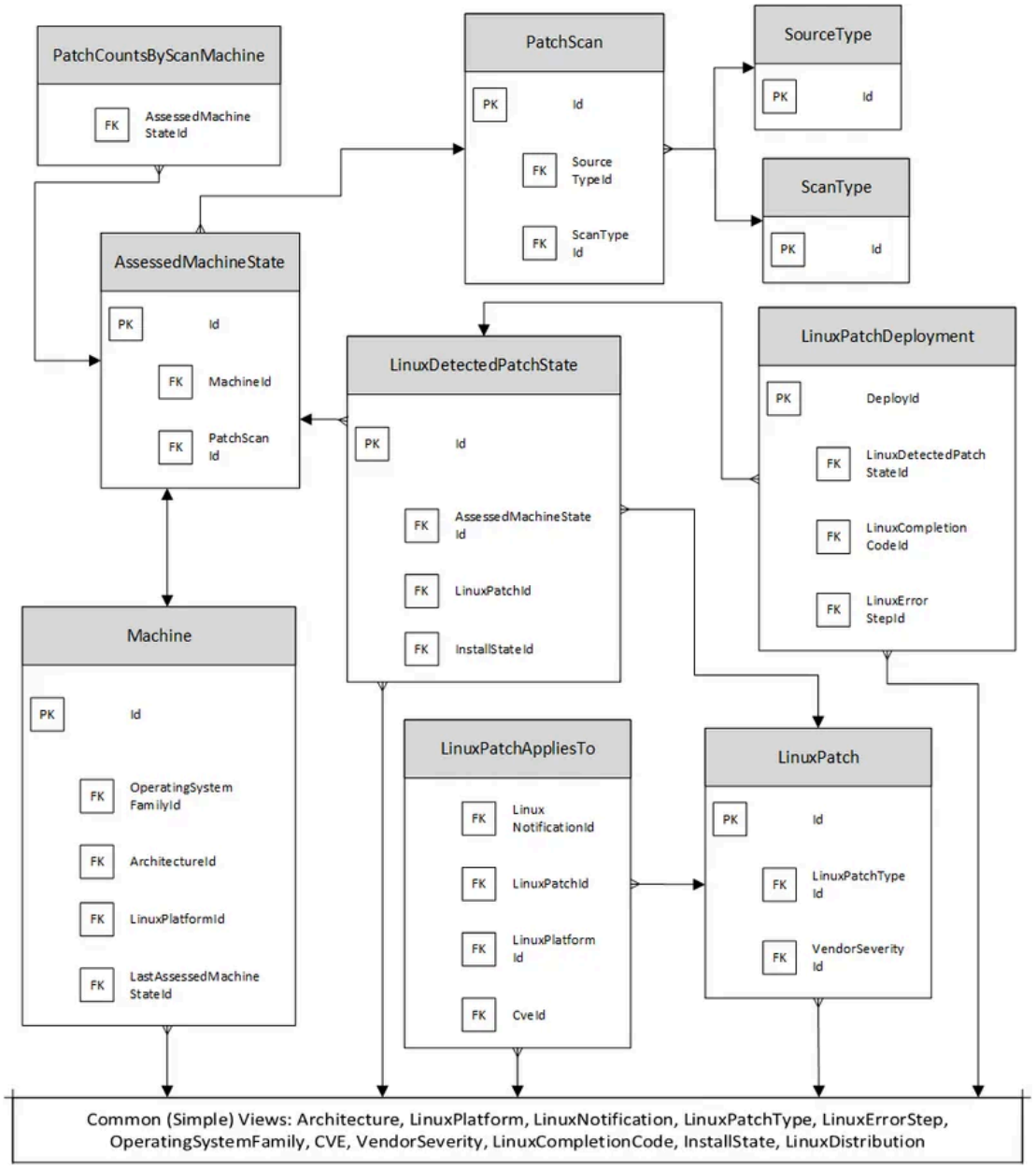
Windows

This graphic shows the relationships between the Windows views in the SecurityControls database.



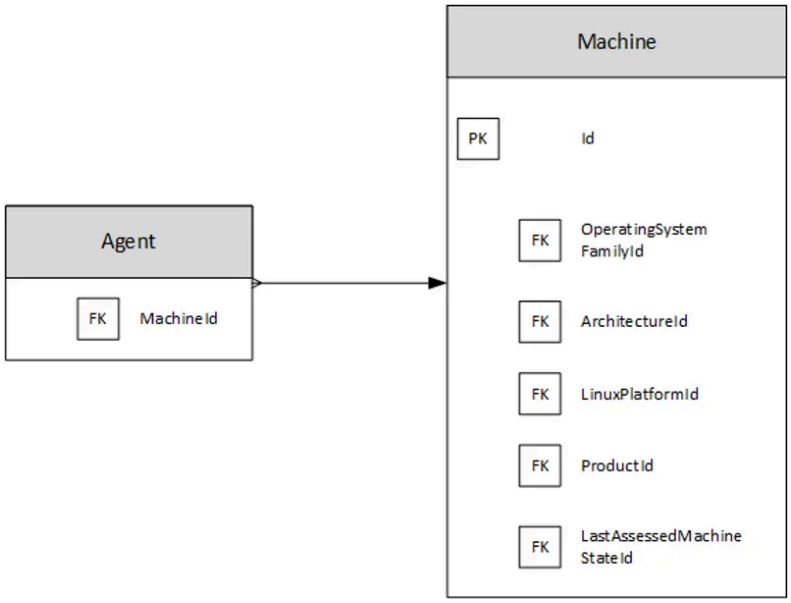
Linux (content-based)

This graphic shows the relationships between the content-based Linux views in the SecurityControls database.



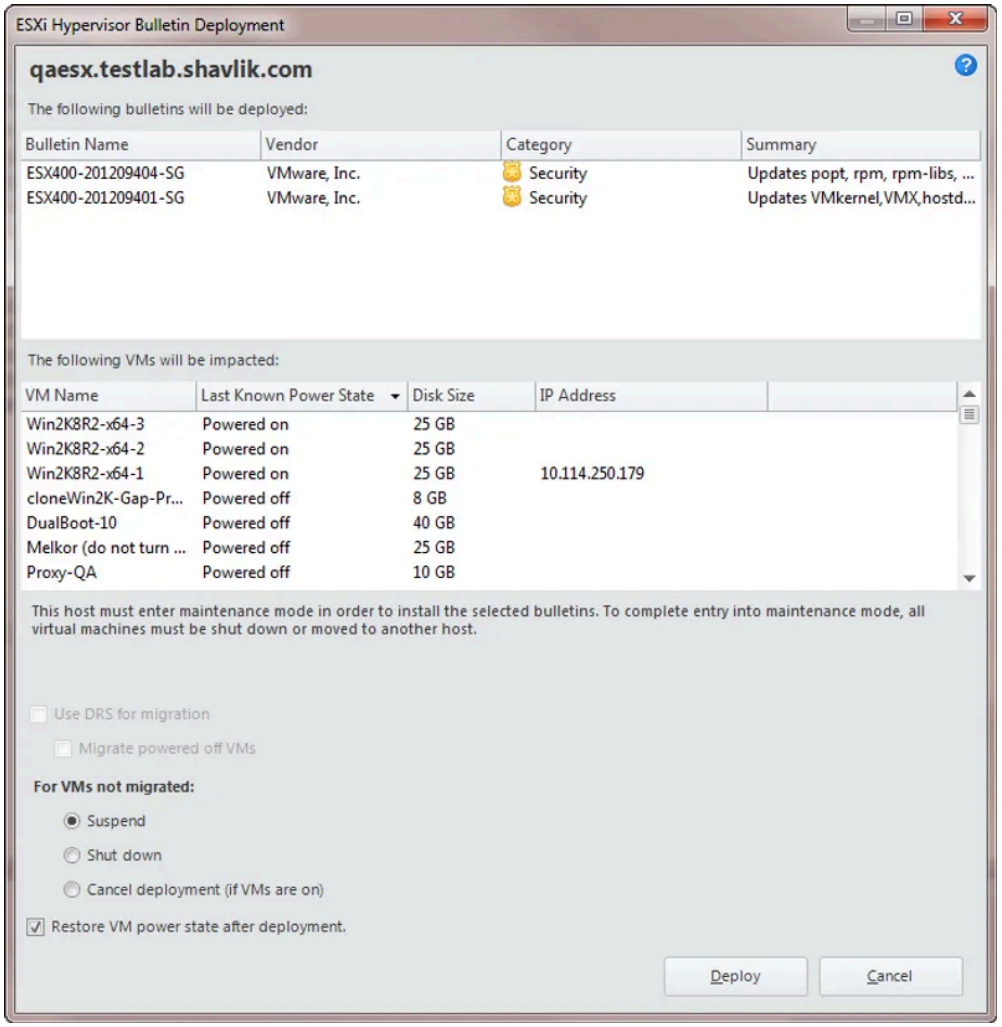
Agent

This graphic shows the relationships between the agent views in the SecurityControls database.


Machine
PK
Id
FK
OperatingSystem FamilyId
FK
ArchitectureId
FK
LinuxPlatformId
FK
ProductId
FK
LastAssessedMachine StateId
Agent
FK
MachineId

154. Configuring an ESXi Bulletin Deployment

When an ESXi hypervisor deployment is initiated the **Bulletin Deployment** dialog is displayed. This dialog enables you to specify how the ESXi hypervisor and the virtual machines contained on the hypervisor will be affected during the bulletin deployment.



Field	Description
The following bulletins will be deployed	Specifies which bulletins are about to be deployed.
The following VMs will be impacted The following options apply only if one or more of the bulletins being deployed will have an **impact on the virtual machines and hypervisor**.	Shows the virtual machines that are hosted by the ESXi hypervisor. Each of the virtual machines may be affected because most deployments require that hosted virtual machines be powered off or moved to another host prior to the bulletin deployment to the hypervisor. The **Last Known Power State** column shows the power state each virtual machine was in at the time of the most recent scan.
Use DRS for migration	If the ESXi hypervisor must enter maintenance mode to deploy the bulletin(s), and if the vCenter Server that is managing this hypervisor is configured to use VMware Distributed Resource Scheduler (DRS), you have the option to allow DRS to migrate the hypervisor's virtual machines to different hypervisors before beginning the deployment process. If you choose not to use DRS, the hypervisor's virtual machines power state will be modified according to the **For VMs not migrated** setting. When the hypervisor update is complete, virtual machines that were migrated to other hosts are not automatically migrated back to this host. If load balancing is enabled, however, DRS will likely migrate some virtual machines back to this host soon after the deployment completes.
Migrate powered off VMs	If enabled, virtual machines that are powered off will be included in a Distributed Resource Scheduler (DRS) migration. If left unchecked, powered off virtual machines will not migrate and cannot be powered on until this hypervisor update is complete.
For VMs not migrated	Indicates what power state to place the hypervisor's virtual machines into if Distributed Resource Scheduler (DRS) is not available or if DRS fails to migrate one or more virtual machines. DRS will be used to migrate a virtual machine only if the following conditions are met: • The hypervisor is managed by a vCenter Server • The hypervisor is in a cluster • DRS is enabled on the cluster • The hypervisor automation level is Fully Automated, or the hypervisor uses the default automation level and the default automation level is Fully Automated. Even if all these conditions are met, migration may fail because other hosts are not available or vSphere HA admission control policies prohibit the migration. The action selected here applies to all powered-on virtual machines that are not configured for migration and virtual machines that fail to migrate for other reasons. • **Suspend**: The hypervisor's virtual machines will be placed into a suspended state before the hypervisor enters maintenance mode.

Field	Description
	• **Shut down**: The hypervisor's virtual machines will be shut down before the hypervisor enters maintenance mode. • **Cancel deployment (if VMs are on)**: The deployment will be canceled if any of the hypervisor's virtual machines are powered on.
Restore VM power state after deployment	If enabled, each virtual machine on the hypervisor that was suspended or shut down during the deployment will be restored to its current power state following the deployment.
Deploy	When you are ready to deploy your bulletins using the selected deployment options, click this button. The Operations Monitor is used to monitor the status of the ESXi Hypervisor bulletin deployment. The following occurs during a bulletin deployment to an ESXi hypervisor: 1. The bulletins are downloaded from the vendor's website and staged to the hypervisor. 2. If any selected bulletin requires that the hypervisor enter maintenance mode or be restarted, the hypervisor's virtual machines that are not configured for DRS migration are suspended or powered off. 3. The hypervisor enters maintenance mode, triggering DRS to begin migrating virtual machines that are properly configured. 4. Virtual machines that fail to migrate are suspended or shut down, or the deployment is canceled, based on the selection made in **For VMs not migrated**. 5. When the migration and/or shut down of virtual machines is complete, the bulletins are installed. 6. The hypervisor is restarted if a reboot is required. 7. The virtual machines that were suspended or powered off during the deployment will be powered on if **Restore VM power after deployment** is enabled. 8. The deployment is recorded in the Event History log. 9. The results are reflected on the **Bulletins** tab after selecting **View > Refresh**.

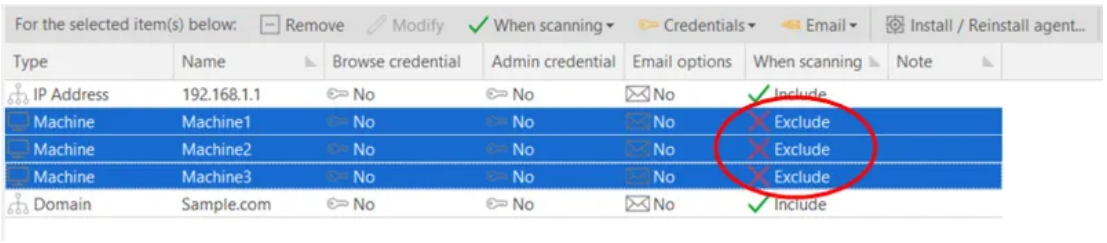
155. Excluding Certain Machines

You can define a number of machines you want to exclude. This is especially useful for defining a machine group that consists of all but a few machines from a large group of machines. For example, if you want to create a machine group that consists of all but two machines in a domain, you simply add the domain and then specify the two machines you want to exclude.

Machines can be added to the "exclude list" by machine name, by domain name, or by IP address. When specifying the name or IP address, simply enable the **Exclude** check box before you click **Add**. Excluded machines are identified in the machine group list by an **Exclude** icon.

If you create a group of excluded machines and then add that group to a nested group, the exclusions will be honored.

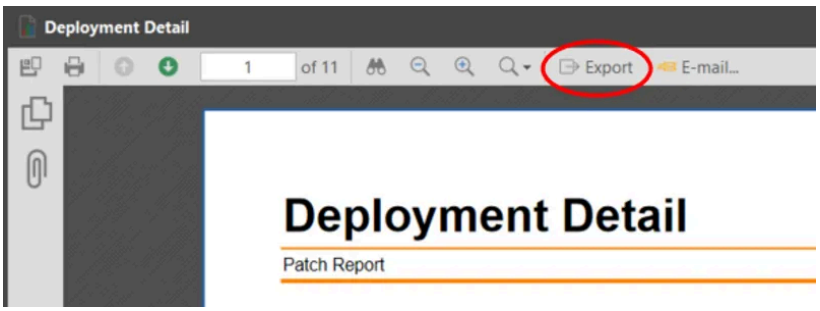
> To specify how Security Controls will react if two machine groups with opposing include/exclude definitions are used in the same scan operation, see the **Always enforce machine group exclusions check box**.



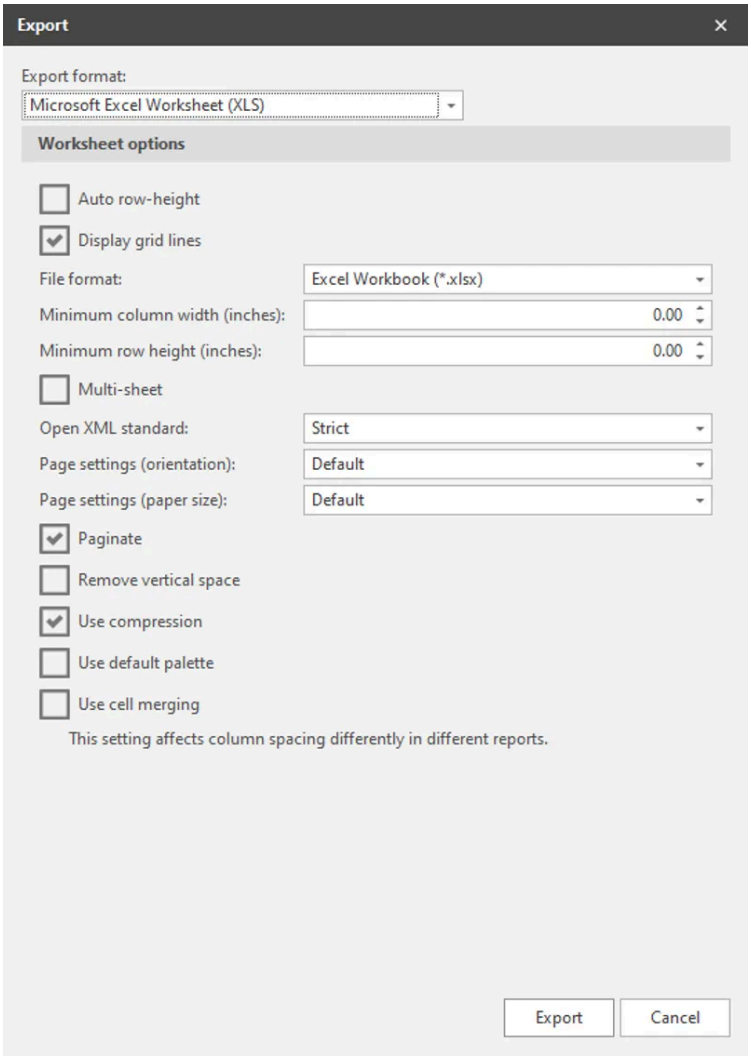
156. Exporting Reports

After a report is generated, it can be exported to a different format from the report viewer.

1. Click **Export** on the toolbar.



The **Export** dialog is displayed.



Select the export format and any available options and then click **Export**.
The **Save As** dialog appears.

3. Specify the name and location of the report file and then click **Save**.

157. File Version Analysis

In order for a system to 'pass' a given patch analysis for a patch that is applicable to the system, the file versions for all patch-related files must match what is stored in the data definition file.

- If the file version for a patch-related file is below what is expected (on the target system), the patch is considered not found, and both the file version found on the system and the file version expected (from the data file) are displayed in the output with a 'Patch Missing' message.
- If the file version of any file on the system is greater than expected, both the existing and the expected file versions are displayed along with a warning message that the file on the system is more recent than expected. This may indicate the presence of a more recent non-security bulletin related hotfix, or the presence of a trojaned file.

158. Filtering Windows Patch View by Patch Type

> If nothing is selected in this filter, then nothing will be filtered out of the patch catalog and all patch types will be included in the top pane.

This filter is used to specify the types of patches, and the vendor severity levels of those patches, that should be displayed in the top pane. The options are:

- **Security Patches**: Security bulletin related patches. You can choose to include one or more specific severity levels. If a bulletin has multiple QNumbers with different severity levels, the most severe level will be shown. The specific states of each QNumber can be viewed by selecting the affected products in the **Patch Information** tab.
  - **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host.
  - **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.
  - **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.
  - **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
  - **Unassigned:** Security patches that have not been assigned a severity level.

Software Distribution: Free third-party products that can be deployed by Security Controls

- **Security Tools**: Updates for security tools such as Windows Defender and Windows Malicious Software Removal Tool. Also includes certificate updates and hotfixes for known security risks that are not yet fully supported by a security bulletin.
- **Non-security Patches**: Vendor patches that fix known software problems that are not security issues. You can choose to include one or more specific vendor severity levels. See **Security Patches** for a description of the available severity levels.
- **Custom Actions**: Displays the null patch (MSST-001) that is used when performing a **custom action**.

159. Filtering Windows Patch View by Product Vendor

> If nothing is selected in this filter, then nothing will be filtered out of the patch catalog and all vendors and products will be included in the top pane.

This filter is used to specify the product vendors that should be displayed in the top pane. You can expand each vendor tree to select individual products from a vendor.

160. Filtering Patch View

Information displayed in the top pane can easily be filtered to narrow the focus to only those patches of interest. One way to do this is by using the Smart Filter.



The Smart Filter initially contains several default filters. Default filters are identified by a leading asterisk. Default filters cannot be modified or deleted.

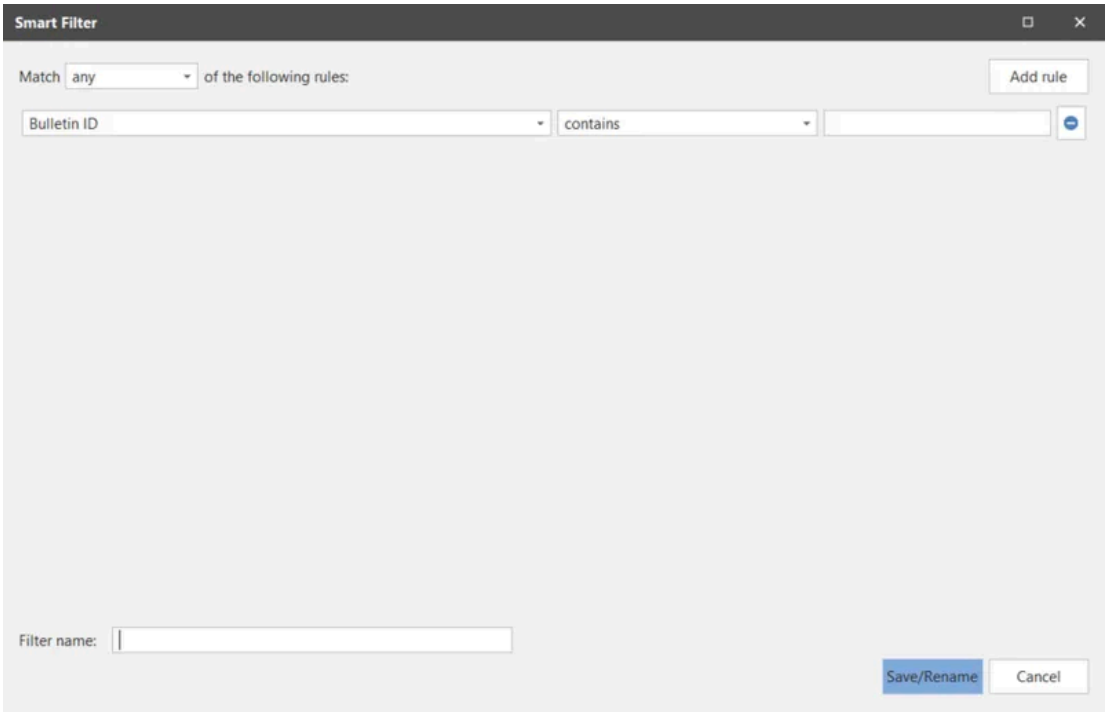
> Another option is to apply filters to individual columns. For more information, see **Customizing the Column Headers**.

Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which patches you want displayed in Patch View. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click **New Smart Filter**.
   The **Smart Filter** dialog is displayed.



Specify which rules in the filter must be matched.

- **All**: Only those patches that match all the rules in the filter will be displayed.
- **Any**: Patches that match at least one rule in the filter will be displayed.

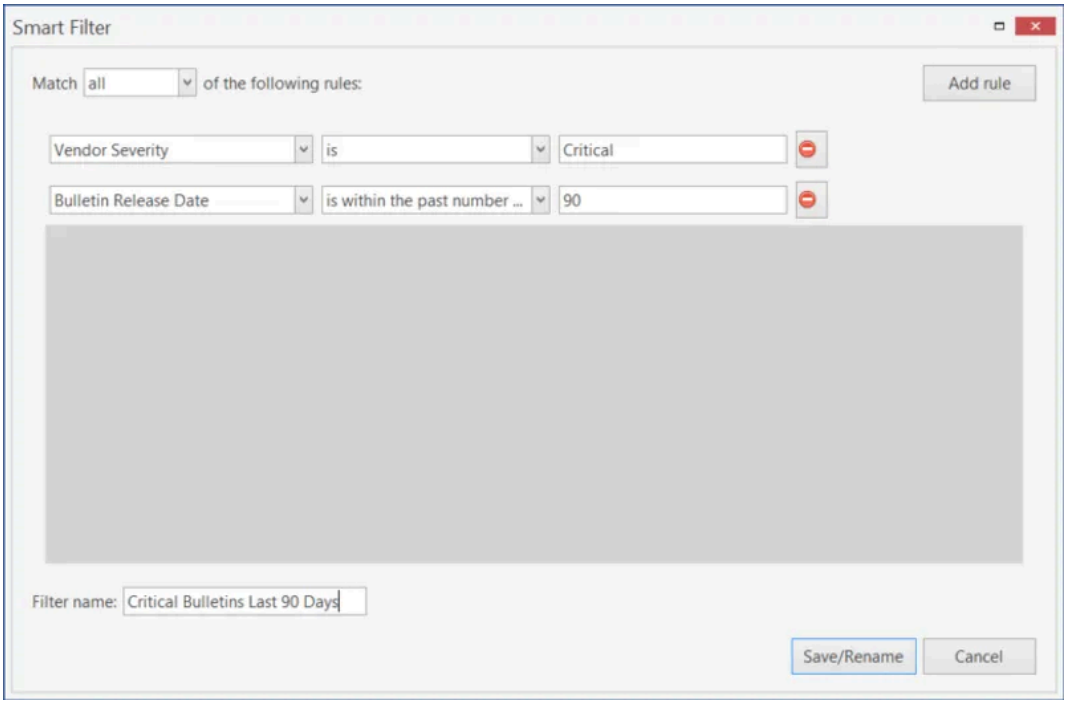
Define one or more rules.
To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule

simply click **Add Rule**.

4. Type a name for the filter.
5. When you are finished defining your custom filter, click **Save/Rename**.

Example

Assume you want to see a list of all critical bulletins that were released within the past 90 days. You simply create a filter similar to the following:

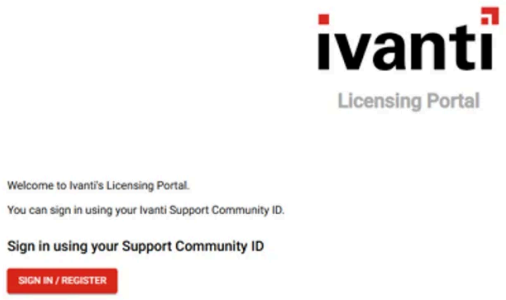


161. Obtaining the License

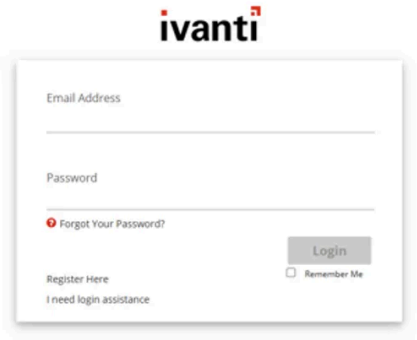
This section describes how to obtain license keys to obtain or update Ivanti Security Controls using a 25 characters license key or trial activation.

The Credentials-based activation method is now deprecated. To obtain your 25 characters license key, retrieve it from the **Ivanti Licensing Portal** under Other License Keys.

1. Open the Ivanti Licensing Portal at **https://portal.ivanti.com/.**



2. Sign in using your Community ID and password.



3. Locate the Other License Keys section to find your Security Controls 25-Characters license keys.

Related Topics

- System Requirements
- Installing the Prerequisites
- SQL Server Pre-Installation Notes
- Performing a New Installation
- HTTP Proxy Post-Installation Notes
- SQL Server Post-Installation Notes
- Activating Security Controls
- Your Next Steps

162. Guide to Surviving Patch Tuesday

Patch Tuesday affects us all. This section is intended to give a work flow for surviving the Patch Day experience.

The first tip to a successful Patch Day is to stay on top of what is being released. Ivanti provides out of the box support for a wide variety of vendors, and keeping up with what each product in your environment is doing can be a daunting task. Below are several sources that can be helpful in keeping up with what patches are being released and what that means for you.

Patch Content Updates / Content Announcements

The single best source for information are the Patch Content Updates / Content Announcements. This mailing list notifies you when new XML is available. This covers all vendors Ivanti supports and is the easiest way to keep up to date on what new patches and products are being supported by Ivanti. You can subscribe to these automatic announcements using any of the following methods:

- **Email:** https://forums.ivanti.com/s/group/0F91B000000PeJxSAK/content-notifications-isec-and-pws
- **RSS:** https://protectessentials.shavlik.com/feed
- **Twitter:** https://twitter.com/ShavlikXML

Previous XML announcements can be viewed by scrolling through the news feed located in the top-right corner of the Ivanti Security Controls home page.

Ivanti Blog

Another excellent source is the Ivanti blog (opens in a new window). We typically provide a preview of new patches that are coming out as well as a round-up discussion of issues uncovered during the implementation of the patches.

Additional Resources

Just knowing what patches are available is great, but where can you go to get more in-depth information on what the real impact of the newly release patches is for your environment? Microsoft provides a free notification service to give you an idea of what is expected to release. They also provide an Exploitability Index that contains additional information about each patch.

- Microsoft Technical Security Notifications (opens in a new window)
- Microsoft Exploitability Index Site (opens in a new window)

Other vendors also realize the importance of a diligent patch management process. For example, Adobe provides a regular release schedule and ongoing security testing for many of its products.

Adobe Acrobat release notes (opens in a new window)

Adobe Connect release notes (opens in a new window)

Ivanti also provides a series of webinars on Minimizing the Impact of Patch Tuesday. This webinar series is typically hosted by a member of the Ivanti Data Team as well as Ivanti engineers who work with the products and customers on a regular basis. The webinars provide insight into each month's patch releases and discusses their real world impact. You can sign up for the next session at the Webinars page (opens in a new window).

Now that you are up to your elbows in what Ivanti, Microsoft and other sources are telling you, let's look to a vendor agnostic source. PatchManagement.org is a website created by security experts to provide a community for discussing all things patch related. This site provides the latest discussions on patches (Windows and Linux\Unix) by a wide variety of security experts. It also has great

information regarding many patch vendors in the market. The goal of this site is patch management awareness and is meant to remain as vendor agnostic as possible.

patchmanagement.org (opens in a new window)

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

163. Help System

A robust Help system is available for the program. To access the Help system, select **Help > View help**.

Context-sensitive help is also available for many of the various program windows and dialogs. Simply click the context-sensitive help icon ( ) or press **F1** to view information specific to the window or dialog currently being displayed.

If you are a non-English user, a localized version of the Help system is available if have an Internet connection and you specify **On the web** for the **View help topics** display option.

If you operate in a disconnected environment, you can view the help system by downloading and using a .chm file. See the **Local help viewer option** for complete information.

164. Step 1: How to Issue a New Certificate Using Your Own CA

The specific actions you take to issue a new sub-authority certificate depends on your environment.

Option A: If your CA is accessible over your network

1. Close Security Controls.
2. Use your local system facilities to issue the new certificate from your CA.
   Make sure the certificate meets all of the **requirements**.
3. Save the new certificate to the console machine's Intermediate Certification Authorities store.
4. On the console, open an administrator command prompt window and change to the Security Controls installation directory.
   The default installation directory is: `C:\Program Files\Ivanti\Security Controls`.
5. Using the STMgmt command-line tool, issue the `select_subauthority -thumbprint <thumbprint>` command to specify that the new certificate should act as the sub-authority certificate.
6. **Example:** `stmgmt.exe -select_subauthority -thumbprint 3e656d7ca744c131c2daba3e4fb4e8731784824e`
   Be sure to include the -thumbprint argument, which indicates to Security Controls that it should use the certificate as the sub-authority certificate. One method for getting the thumbprint is to:
   1. Copy the thumbprint from the new certificate into an application such as Notepad.
   2. Remove any spaces and special characters.
   3. Save the file in an ANSI-encoded format.
   4. Paste the thumbprint character from the Notepad file into the `select_subauthority` command.

For information on using STMgmt, type the following from an administrator command prompt on the console machine:
`C:\Program Files\Ivanti\Security Controls>stmgmt`
See **Let the Certificate Percolate Through the System** for information on whether you need to wait 30 days before committing to the new certificate.

Option B: If your CA is not accessible over your network (the CA is offline or in a disconnected network)

1. On the console, open an administrator command prompt window and go to the Security Controls installation directory.
   The default installation directory is `C:\Program Files\Ivanti\Security Controls`.
2. Using the STMgmt command-line tool, issue a `request_subauthority -of <requestfile>` command to create a sub-authority certificate request.
3. **Example:** `stmgmt.exe -request_subauthority -of samplerequestfilename.req`
   This is the request to issue the new Security Controls sub-authority certificate. It creates all the information necessary for a CA to issue a certificate and save it to a file. This file is a PKCS10 certificate request in binary format and it will be used to generate the certificate on the CA. You may need to convert this file to be Base64-encoded depending on your CA.
   Transport the file to the CA.
4. Have your CA issue the new sub-authority certificate and save it to a file.
   Make sure the certificate meets all of the **requirements**.
5. Transport the file to the console machine and save it to a local directory.
6. Using the STMgmt command-line tool, issue an `accept_subauthority -if <issuedcert>` command.

7. **Example:** `stmgmt.exe -accept_subauthority -if sampleresponsefilename.cer`

   This command does several things. It:

   - Accepts the new certificate that was generated from the trusted CA
   - Binds it back to the private key on the console
   - Specifies that Security Controls should use the certificate as the sub-authority certificate
   - Manages the installation of the new certificate

See **Let the Certificate Percolate Through the System** for information on whether you need to wait 30 days before committing to the new certficate.

165. How Do I . . .?: Get Started Scanning and Patching Linux Machines

All tasks performed on Linux machines are done using agents. For information on how to scan and patch your Linux machines, see **Overview of Linux Patch Management**.

166. How to Enable Security Controls Cloud Synchronization

1. (Recommended) Select **Tools > Edit console description** and make sure that the name the program uses when referring to the console is a friendly name that has some meaning or significance to other users.
2. This is the name that will be displayed within Security Controls Cloud after you register the Security Controls console. For more information on changing the name, see **Editing the Console Description**.
   Select **Tools > Options >** Security Controls **Cloud sync** and register the Security Controls console with the cloud service.
3. The registration process establishes a secure communication channel between the console and the specified Security Controls Cloud account. For details on the console registration process, see **Security Controls Cloud Sync Options**.
   In a new or existing agent policy, enable the **Sync with the Security Controls Cloud check box**.
4. In the agent policy click **Save and update Agents**.
5. A copy of the agent policy and all necessary components is written to the associated Security Controls Cloud account. You can view the steps in the policy synchronization process by viewing the **Event History log**.
   The next time your agents check in with the console they will receive an updated policy that allows them to use the cloud as a backup source for reporting information and receiving policy updates. This provides a layer of redundancy and is the primary benefit of using Security Controls Cloud synchronization.
   (Optional) If you are using multiple Security Controls consoles, and if one of your consoles is using Security Controls Cloud synchronization and another is not, you can be notified of this situation by selecting **Tools > Options > Notifications & Warnings** and enabling the **Warn if** Security Controls **Cloud sync is not enabled on this console** check box.
   This is especially important if two or more consoles are sharing the same database. Each console that uses a Security Controls Cloud sync-enabled policy must be registered with Security Controls Cloud.

167. How to Get Started

Here are the basic steps for getting started with API calls that are executed from a PowerShell console.

1. From the Security Controls console, launch a Windows PowerShell console.
   Be sure to specify *Run as Administrator* when launching the PowerShell console.
2. Load the STProtect API module by executing the following PowerShell command:

```Bash
PS C:\Import-Module STProtect –PassThru
```

The STProtect API module contains API calls that allow you to interact with many of the functional areas within Security Controls. The optional `–PassThru` option provides diagnostic feedback about how the module is loaded.
You should always load the module first whenever you write a script. One way to ensure that the module is always loaded is to add the module import command to your PowerShell user profile.
Load any other required Windows or third-party modules.
You may need commandlets from other modules in order to interact with other devices in your environment. For example:

- Servermanager: Required in order to interact with the SQL cluster.
- Failoverclusters: Loads Windows feature RSAT-Clustering.

Execute individual commands or scripted commands.

> For the complete list of available commands, see **How to View Detailed Help Information About the PowerShell Commands**.

Here are a few popular examples:

Perform a patch scan

```Bash
Start-PatchScan –MachineGroups “My Machine”
```

Start and view results of a patch scan

```Bash
Start-PatchScan –MachineGroups “My Machine” | Watch-PatchScan
```

Deploy missing patches

```Bash
Start-PatchDeploy –Uid 12345678-3BD2-A0ED-FFCC-9876DE8EBBAA
```

When finished, close the Windows PowerShell console.

All modules that you imported or items that you stored in memory will be erased when the PowerShell console is closed. Scan or deployment operations that you initiated will not stop when PowerShell closes.

168. How to Patch Linux Machines That Reside in a Disconnected Environment

If you have Linux client machines that reside in a disconnected environment, the agent will not be able to utilize YUM to download RPM packages from the internet. You will instead need to do the following:

- Set up and populate one or more local "on-premise" repositories that contains the entire library of available RPMs
- Configure your client machines to look to the correct local repository for the missing RPMs rather than to the internet

> The following information is meant as a general guideline for setting up and using a local repository. If you have specific questions or issues, please contact your Linux operating system vendor.

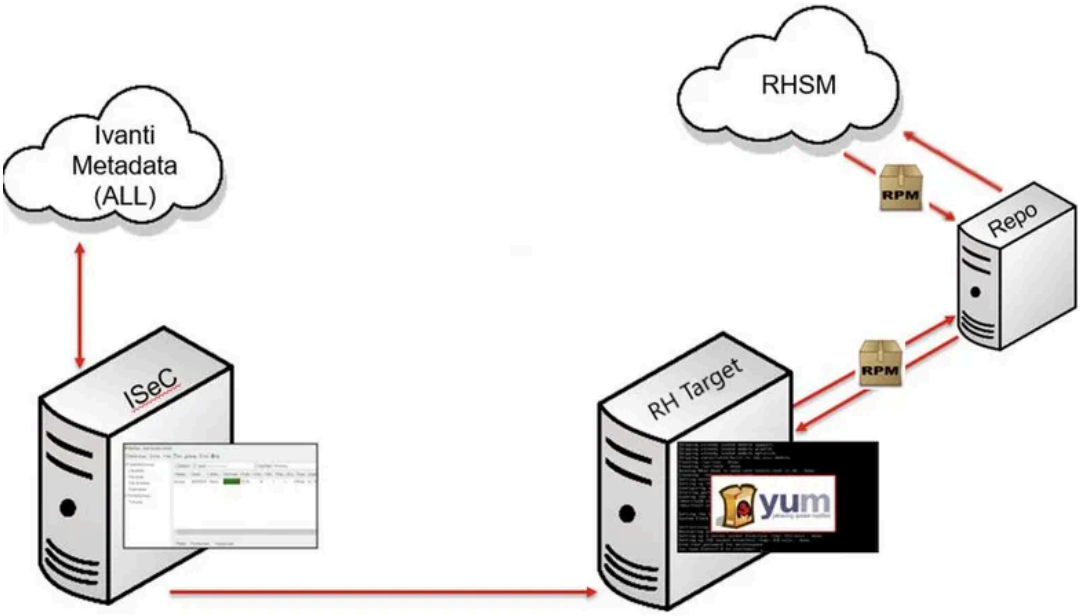
How to Set Up a Local Repository

Requirements

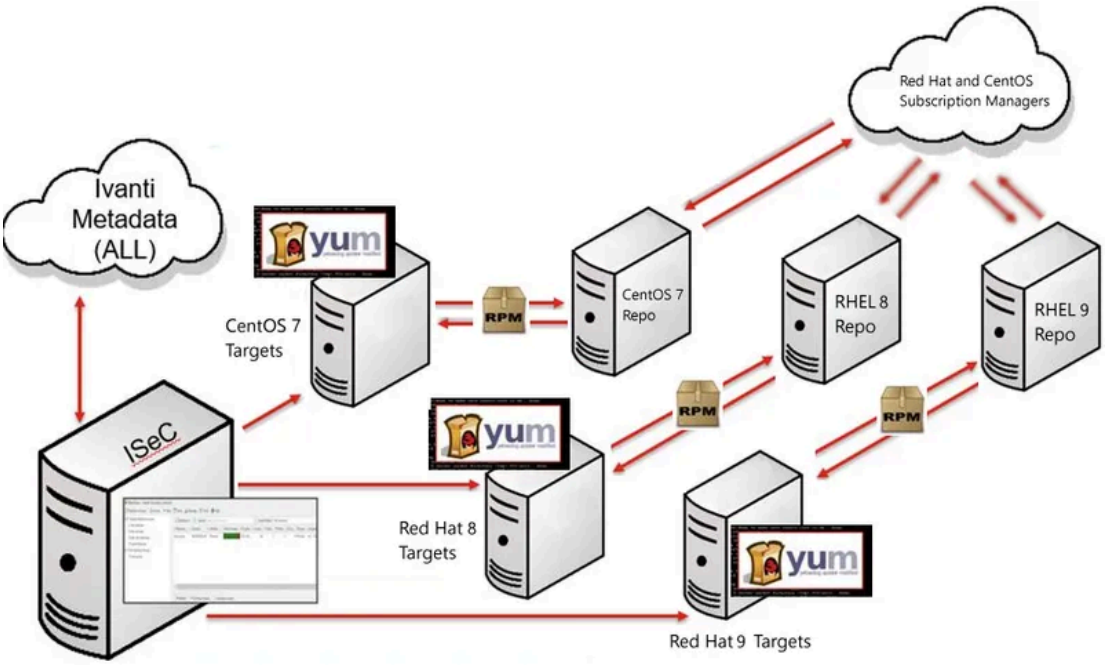
You can use any supported Linux server machine as your local repository. The only requirement is that it contain enough available disk space to contain the entire inventory of available RPM packages. There are many different public repositories that contain RPM packages. For example, there is a public repository for RHEL 9 RPMs, another public repository for RHEL 8 RPMs, etc. As a general rule, your local repository machine should contain at least 100GB of disk space for each public repository that you will download.

You will likely need two or more Linux server machines for this process.

- **Scenario 1:** You might choose to use one machine that will be used as the local repository for all of the different versions of RPMs. In this scenario, the machine you use as the repository can download RPMs of the same version of the distribution that is used on the repository machine. You will, however, need a separate machine to download the RPMs for each different version of each distribution that is used within your organization.
- For example, if your organization contains RHEL 9 x64, RHEL 8 x64 and CentOS 7 x64 client machines, you might use a RHEL 9 x64 server machine as the local repository and use it to download all RPMs for your RHEL 9 servers, workstations, desktops, etc. You would use separate RHEL 8 x64 and CentOS 7 x64 machines to download all the RPMs for your RHEL 8 and CentOS servers, workstation, desktops, etc. and then transfer those RPMs to the local repository machine.



Scenario 2: You might choose to maintain three different local repositories: one for all RHEL 9 RPMs, another for all RHEL 8 RPMs and a third for all CentOS 7 RPMs. This scenario requires three dedicated machines to act as your repositories but it eliminates the additional transfer step and the hassle of maintaining the joint repository.



Configuration Process

Because it is likely to take several hours to download the entire library of available RPM packages to your local repository, the recommendation is to perform the configuration process in two different phases. Phase 1, in which you will download all available RPMs, should be performed at the end of the work day so that the download process can run overnight. Phase 2 can then be performed the following day.

> You must have root privilege to execute the following commands.

Phase 1

1. Make the directory you want to use as the repository.
   For example, the following command creates a directory that will be used to contain Red Hat 9 RPMs.

```bash
mkdir -p /repos/redhat/9
```

Display the list of public repositories that are available for you to use to populate your local repository.
The public repositories that are available to you is based upon your RHEL subscription.

```bash
yum repolist
```

Using YUM, install the package that includes reposync.

```bash
yum install yum-utils
```

Download all available packages from the public repository of your choosing.
For example, the following command downloads RPMs from the rhel-9-for-x86_64-baseos-rpms public repository.

```bash
reposync --gpgcheck -l --repoid=rhel-9-for-x86_64-baseos-rpms --download_path=/repos/redhat/9
```

The download process will take a long time, so plan accordingly. The -gpgcheck option removes packages that fail the signature check during the download process.
Repeat Step 3 for each required public repository variant.
For example, if your organization contains RHEL 9 on both Intel and ARM, you will need to download the RPMs from both of the associated public repositories. You may need several days to the perform all of the necessary downloads.

> Do not attempt to download RPMs for a different version of Red Hat or CentOS. For example, a RHEL 9 machine cannot be used to download RPMs for RHEL 8 x64 machines.

Phase 2

The process described here creates a repository that is accessible via HTTP. There are other methods that can be used to create a repository. Feel free to use whatever method with which you are most familiar.

1. Using YUM, install the program that provides the ability to create a repository.

```bash
yum install createrepo
```

Create the repository.

```bash
createrepo /repos/redhat/9
```

If you receive an error stating it cannot open a *.rpm file, verify that you have not run out of disk space. If space is not an issue, repeat the download step (Step 3 in Phase 1). It is possible that some files were missed the first time the download was performed.
Install the Apache web service.
This will provide the ability to access your local repository using the HTTP protocol.

```bash
yum install httpd
```

Open Port 80 in your local firewall.
This is because we are setting up the repository to use HTTP. HTTPS is also an option but HTTP is used here to simplify the example.

5. Edit the httpd.conf file and add any of the following entries that are missing.

```bash
vi /etc/httpd/conf/httpd.conf
```

```bash
```

```bash
ServerAdmin root@localhost
```

```bash
DocumentRoot /var/www/html
```

Bash

```
ServerName <machinename>
```

Link your new repository to the default website location.

Bash

```
ln -s /repos/redhat /var/www/html/redhat
```

Verify the syntax of the Apache web service.

Bash

```
httpd -t
```

Start the Apache web service.

Bash

```
systemctl start httpd
```

> You may need to repeat this command each time the server is restarted. You can use the following commands to automatically start the service whenever the server is restarted: `systemctl enable httpd`.

Get the updateinfo.xml.gz zip file.

> Steps 9 - 13 apply only to Red Hat machines.

Bash

```
yum list-sec
```

Copy the *updateinfo.xml.gz files from the default location to the /repodata folder.

Bash

```
cp /var/cache/yum/x86_64/9rhServer/rhel-9-for-x86_64-baseos-rpms/*updateinfo.xml.gz /repos/redhat/9/repodata/
```

Uncompress the *updateinfo.xml.gz file.

```bash
gzip -d /repos/redhat/9/repodata/*updateinfo.xml.gz
```

Rename the *updateinfo.xml file to eliminate unnecessary leading characters.

```bash
mv /repos/redhat/9/repodata/*updateinfo.xml /repos/redhat/9/repodata/updateinfo.xml
```

Modify the repository to acknowledge that it contains the updateinfo.xml file.

```bash
modifyrepo /repos/redhat/9/repodata/updateinfo.xml /repos/redhat/9/repodata/
```

(Applies only to machines that have SELinux enabled) Provide permission for www/html/redhat to access /repos/redhat.

```bash
cd /var/www/html
```

```bash
chcon -R -t httpd_sys_content_t redhat/
```

Repeat the Configuration Process for Other Linux Versions and Distributions

You will need to repeat some or all of the configuration process for each different version of each distribution of Linux that is supported in your organization. For example, you must use a RHEL 9 machine to download RHEL 9 RPMs, a CentOS 7 x64 machine to download CentOS 7 x64 RPMs, a RHEL 8 x64 machine to download RHEL 8 x64 RPMs, etc. Alter the commands as needed for each unique version of Linux.

Scenario 1: If you are using one repository for all of the different Linux versions

Assuming you are using a Red Hat 9 machine as your repository, here is what you would need to repeat in order to retrieve Red Hat 8 RPMs:

1. On the Red Hat 9 repository machine, repeat Phase 1, Step 1 except specify /repos/redhat/8.
2. On a Red Hat 8 machine, perform Phase 1, Steps 3 & 4.
   In Step 3, the repos/redhat/9 directory will not exist on the Red Hat 8 machine, so either remove the -download_path option and let it go to the default location or specify a different location.
3. When you have finished downloading the RPMs, transfer them to the repos/redhat/8 directory on your local repository.
   When you are done you will have one repository on one machine that contains RPM packages for all supported versions of Red Hat.

Scenario 2: If you are maintaining separate repositories for each different Linux version

Repeat the entire configuration process for each different version of Linux that is supported by your organization.

Point Your Linux Client Machines to the Local Repository

You must modify YUM on each Linux client so that it searches the local repository for RPMs rather than on the internet.

> If you chose to maintain a different local repository for each version of Linux, make sure you point each client to the correct local repository.

1. Log on to the client machine.
2. Change to the directory that lists where the repositories are located.

Bash

```
cd /etc/yum.repos.d
```

Create a file named local.repo and then configure it to point to your new local repository.

Bash

```
nano local.repo
```

Bash

```
[mylocalrepo]
```

Bash

```
name=Local Rhel9 Server Repo
```

Bash

```
baseurl=http://es-nxt-rhel9-repo.example.com/redhat/9
```

Bash

```
gpgcheck=0
```

Specify that if an RPM is missing from the local repository, the client should not try to find it on the internet (disconnects the client machine).

Bash

```
ls
```

Bash

```
vi any file other than local.repo (example redhat.repo)
```

Bash

```
Look for your repoid (example rhel-9-for-x86_64-baseos-rpms)
```

Bash

```
Set enabled = 0
```

Periodic Maintenance of Your Repository

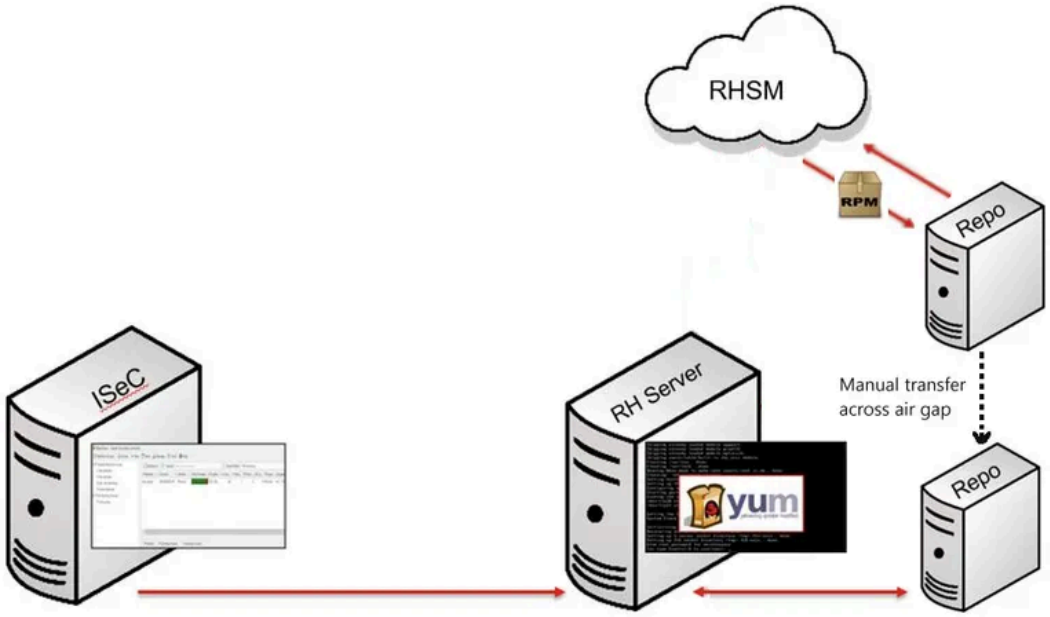
You will need to keep your local repository current by periodically resyncing it with the public repository. When you perform the following command, only new RPM packages will be downloaded to your local repository.

Bash

```
reposync –gpgcheck –l –repoid=rhel-9-for-x86_64-baseos-rpms –download_path=/repos/redhat/9
createrepo --update /repos/redhat/9
```

Air Gap Networks

If your organization maintains an "air gap" network, meaning no client machine is allowed to connect to any machine that has internet access, you must configure and maintain a second repository. This is illustrated in the following diagram.



In this case, after setting up and configuring your connected repository as described above, you will set up a second repository on a disconnected machine and then use a removable media to manually transfer the files from the connected repository to the disconnected repository. Your Linux client machines should then be configured to point to the disconnected repository rather than to the connected repository.

Related Information

https://access.redhat.com/solutions/23016

169. How Do I . . .?: Automate Scheduled Patching

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

A scheduled scan enables you to specify exactly when a scan should be performed. You can configure Security Controls to automatically perform recurring scheduled scans and to automatically deploy any missing patches it detects during a scan.

1. (Optional) **Create a custom patch group** and a **custom patch scan template**.
   This step is necessary if you want to control exactly which patches you scan for and deploy. You do this by first creating a patch group that contains just your approved patches, and then using it as a patch filter in a custom patch scan template.

> If the scheduled scan is something you intend to perform regularly (for example, to coincide with Microsoft's monthly patch release), you will also have to update the patch group on a regular basis.

(Optional) Create a custom **machine group** or a **favorite**.
Using one of the default machine groups will work, too.

3. (Optional) Create a **deployment template**.
   Using one of the default templates will work, too.
4. **Initiate a scan** from the **Agentless Operation page**, from a machine group, or from a favorite.
5. On the **Agentless Operation** page, choose the **Recurring** option and specify when you want the scheduled scans to be performed.

You can schedule a scan to run once at a specific time, or you can schedule a recurring scan. See **Scheduling Patch Scans** for complete details.

6. Enable the **Auto-deploy patches after scan** check box.
7. Select the desired deployment template and specify when the deployment should occur.
8. Click **Schedule**.
9. If prompted, select credentials that can be used to schedule the job on the console machine.
10. Use the **Scheduled Console Tasks Manager** to review scheduled scans.

170. How Do I . . .?: Collect Data for Technical Support

If you ever have a question or issue with Security Controls that requires help from the Ivanti **Technical Support** staff, please have the following information available when opening a support request or calling:

- What version of Security Controls are you using? Please include the build number (available via **Help > About** Security Controls).
- What operating system is the console installed on? Please include the product level.
- What operating system(s) are the target machines running? Please include the product level and architecture version (32-bit or 64-bit).
- What exactly were you doing when the issue occurred, or what exactly do you want to do? Please be as descriptive as possible.
- Provide your Security Controls license key.
- Provide screen shots or text of any on-screen errors.

Ivanti Security Controls Diagnostic Toolkit

The Ivanti Security Controls Diagnostic Toolkit provides utilities to help diagnose your system and provide information to support. See the **Security Controls Diagnostic Toolkit Release Notes (opens in a new window)** for more information.

Installation Log Files

The installation logs are located in the following directory: `C:\Users\<username>\AppData\Local\Temp`

There are two installation log files within the directory:

- Main installation log file: ProtectSetup_<date_time>.log
- Windows Installer log file: ProtectInstall_<date_time>.log

Program Log Files

If necessary, you may be asked to capture program log files.

1. Select **Tools > Options > Logging** and in the **User Interface** and **Services** boxes specify **All**.
2. Restart the program.
3. Recreate the issue.
   Please note the steps you took to recreate the issue. Also note the date and time of day so our analysts know where to look in the log files.
4. Once the issue is recreated, and before you close or restart the program, make a copy of all the logs and include them in your email correspondence.
   The logs are located in the following directory: `C:\ProgramData\Ivanti\Security Controls\Logs`

171. How Do I . . .?: Download Approved Patches

There are a couple of reasons for downloading patches in advance of a patch deployment:

- If you are using one or more distribution servers to store patches you wish to deploy, you must download the patches to the console's patch download directory before you can copy them to the desired distribution servers. See **Synchronizing Servers** for more details.
- It will speed the deployment process. The act of deploying one or more patches will automatically download those patches not already resident in the patch download directory, but downloading them in advance will make the deployment process much faster.

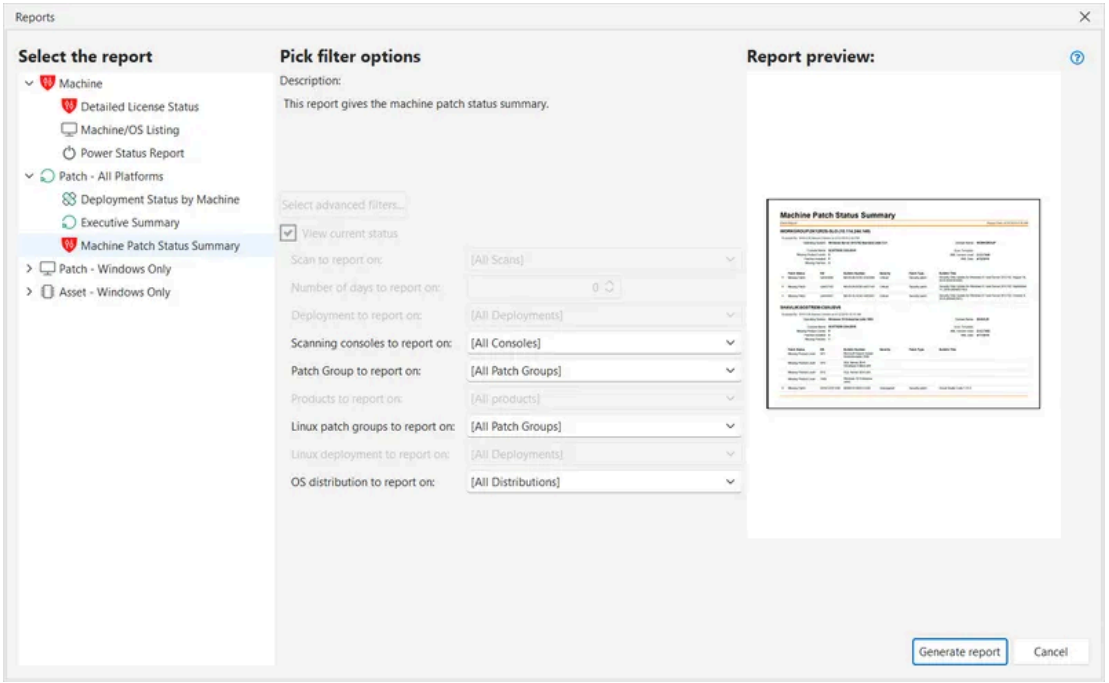
Security Controls provides a number of different ways to download patches.

- From within the top pane of **Patch View**, select the desired patches, right-click the patches, and then select **Download > Patches**.
- From within the middle pane of **Scan View**, right-click the selected patches and select **Download Selected**.
- From within the middle pane of **Machine View**, right-click the selected patches and select **Download Selected**.

172. How Do I . . .?: Generate Reports

There are a number of different reports you can generate to view the state of the machines in your network.

1. Select **Tools > Create report** from the main menu.
2. Select a report from the drop-down list at the top of the **Reports** dialog.



For a list of all available reports, see **Overview of Reports**.

Select your filtering options.

For details, see **Report Gallery**.

4. Click **Generate report**.

   The report is generated and displayed within the report viewer.
5. (Optional) If you elected to use advanced filtering, specify the advanced filtering options.

   For details, see **Advanced Filtering**.
6. If desired, export the report to a number of different formats.

   For details, see **Exporting Reports**.

173. How Do I . . .?: Get Started Scanning and Patching Windows Machines

Show Me!

How to Scan for and Deploy Patches

A video tutorial is available on this topic. To access the video, click the following link:



How to Stage Patch Deployments

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

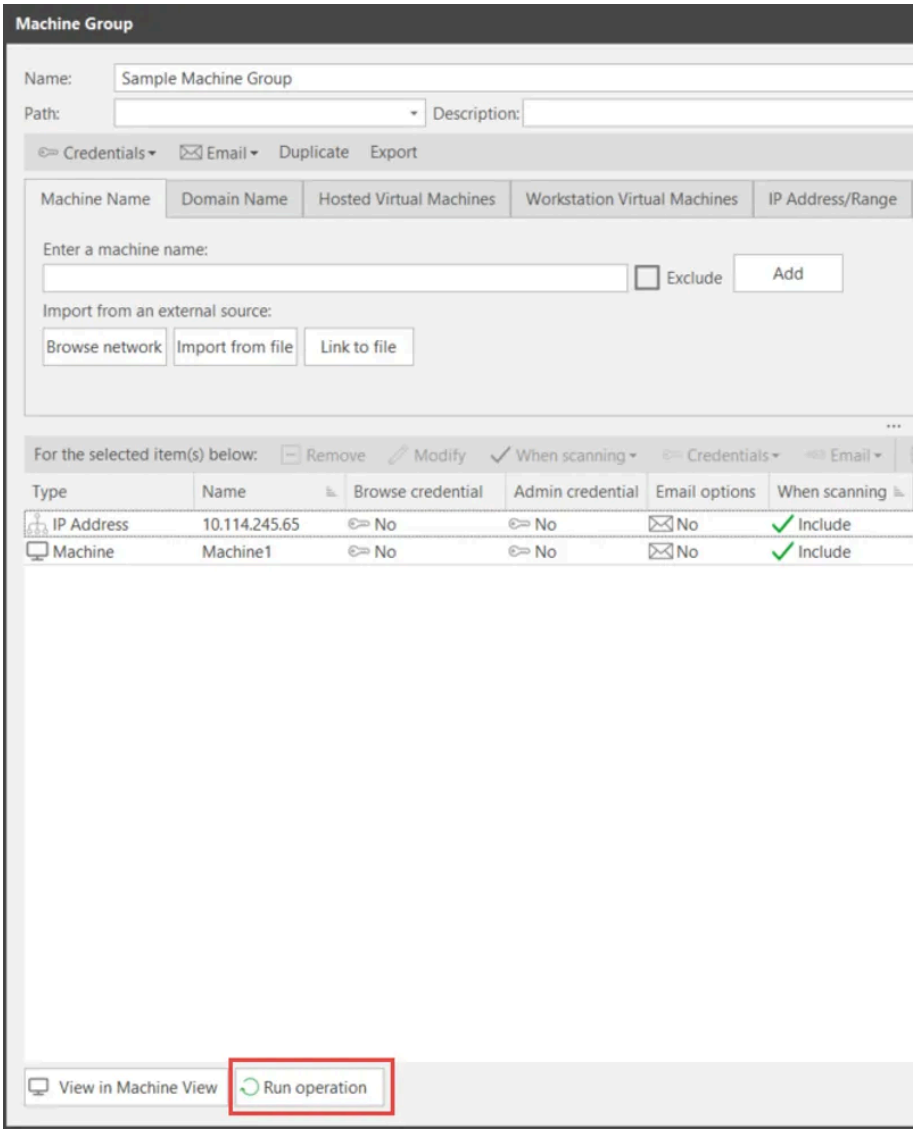
Scanning for and deploying missing patches is easy! You simply do the following:

1 A) Create and Configure a Machine Group

The quickest way to evaluate many machines at once is to create and configure a machine group. For details, see **Creating a New Machine Group**, **Configuring a Machine Group**, and **Supplying Credentials for Target Machines**.

1 B) Perform a Scan of the Machine Group

After creating and configuring the machine group, to initiate a patch scan you simply click **Run Operation**. On the **Agentless Operation page**, verify the default options and then click **Scan Now**. This will immediately begin a scan of all machines in the machine group. (For other options see **How to Initiate a Patch Scan**.)

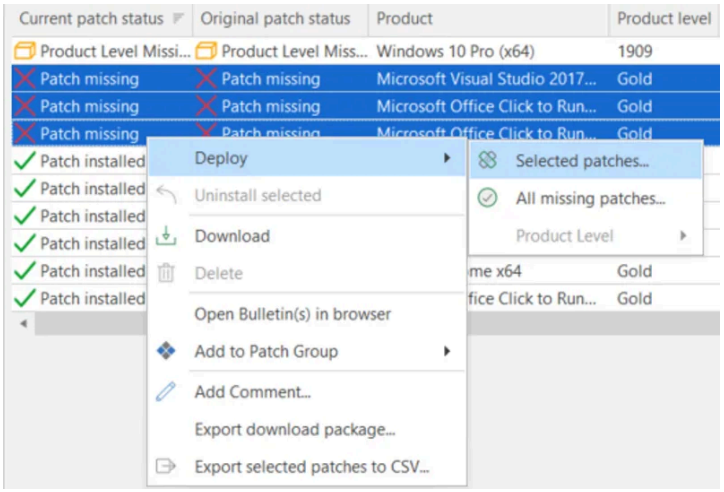


2 Review the Scan Results

Scan results are available immediately following a successful scan. For details, see **Accessing Patch Scan Results**.

3 Deploy Any Missing Patches

You can immediately deploy any patches that are missing on your machines. For details, see **Deploying One or More Patches**.


Current patch status
Original patch status
Product
Product level
Product Level Missi...
Product Level Miss...
Windows 10 Pro (x64)
1909
Patch missing
Patch missing
Microsoft Visual Studio 2017...
Gold
Patch missing
Patch missing
Microsoft Office Click to Run...
Gold
Patch missing
Patch missing
Microsoft Office Click to Run...
Gold
Patch installed
Patch installed
Patch installed
Patch installed
Patch installed
Patch installed
Deploy
Uninstall selected
Download
Delete
Open Bulletin(s) in browser
Add to Patch Group
Add Comment...
Export download package...
Export selected patches to CSV...
Selected patches...
All missing patches...
Product Level
me x64
Gold
fice Click to Run...
Gold

174. How Do I . . .?: Scan and Patch ESXi Hypervisors

The Virtual Inventory feature is used to scan and patch the ESXi hypervisors (ESXi hosts) that are used in your organization. The process is simple:

1. **Add your managed and unmanaged ESXi hypervisors** to Security Controls.
2. **Perform a scan** of the managed and unmanaged ESXi hypervisors.
3. View the security bulletins that are missing on the **managed** and **unmanaged** ESXi hypervisors.
4. **Initiate a deployment** of any missing security bulletins.
5. Specify how the ESXi hypervisor and the virtual machines contained on the hypervisor will be **affected during the bulletin deployment**.
6. **View the deployment results**.

175. How Do I . . .?: Set Up and Monitor Agents

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

Setting up and using agents consists of the following general steps:

Create and Configure an Agent Policy

An agent policy defines exactly what an agent can or cannot do. With Security Controls Agent you can create as many different agent policies as is needed. This provides a great deal of flexibility, enabling you to assign different agent policies to different machines in your organization. A policy can be used to scan for missing patches, to determine software and hardware assets, and to perform power state tasks.

See **Creating a New Agent Policy** for complete information.

Install the Agent Policy On the Desired Machines

Agents can be **push-installed from the console** to the desired target machines, or they can be **installed manually**.

Monitor the Agents as They Protect Your Machines

You can **monitor the agents from the console** or you can use the **Security Controls Agent client program** to perform additional actions directly on the agent machine.

176. How Do I . . .?: Track Deployment Status

Overview Information

It is very simple to track the status of patch deployment tasks.

- Scheduled patch deployments can be managed using the **Scheduled Task Manager**.
- Active patch deployments can be monitored using the **Security Controls Deployment Tracker**.
- When a deployment is finished, you can review the status of the deployment by selecting the deployment in the **Patch Results** pane in the navigation bar.

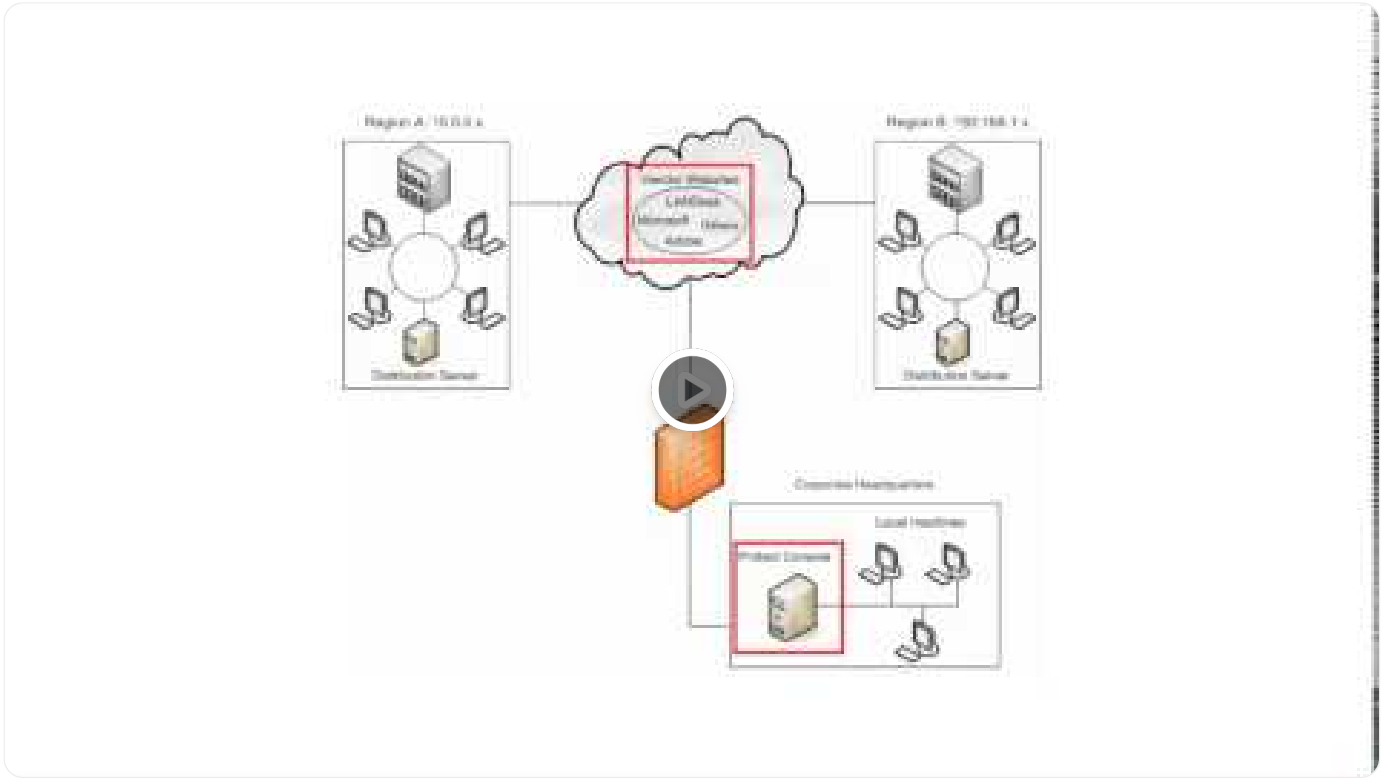
Monitoring Post-patch Machine Status

To verify the status of the updated machine(s), simply perform a new scan and review the updated results using **Machine View**.

177. How Do I . . .?: Use A Distribution Server

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:

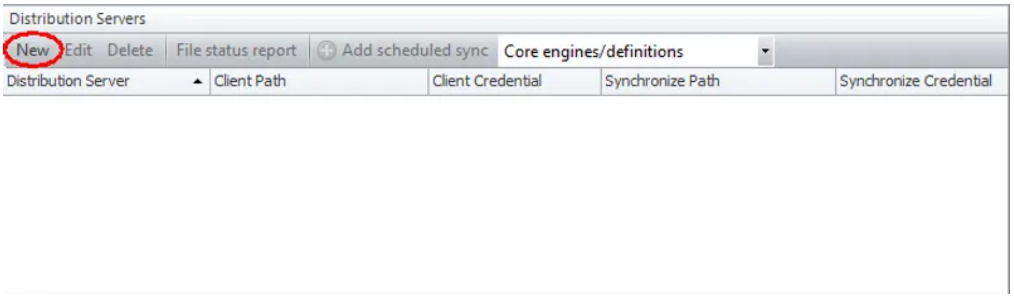


Overview Information

Distribution servers can be used as an alternate location for storing the engine components, the data definition file and the patches used by Security Controls. There are a number of reasons you may want to use a distribution server. For details, see **Why Use a Distribution Server?**

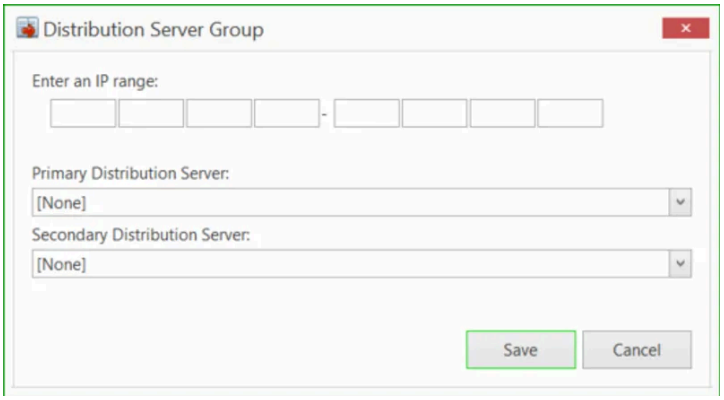
To use a distribution server you do the following:

1. Create and configure a new distribution server.
   Select **Tools > Options > Distribution Servers** and then click **New**. For details, see **Configuring Distribution Servers**.



Define which target machines will use the distribution server.
In the **IP Ranges** pane, click **New** and then specify the IP ranges you want to associate with the server. For details, see **Assigning IP**

Addresses to Servers.



Update the distribution server with the latest files.

You do this by synchronizing the distribution server with the console. For details, see Synchronizing Servers.

178. How Do I . . .?: Use The Asset Inventory Feature

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

The asset inventory feature enables you to track your software, hardware, and virtual assets. You can perform scans to detect and categorize the software and hardware contained on your physical and online virtual machines. You can also scan for the properties of your online and offline virtual machines.

To use the asset inventory feature you do the following:

1. Determine if you want to use the default asset scan template or a custom asset scan template.
   See **Creating a New Asset Scan Template** for information on creating your own unique asset scan templates.
2. Initiate an asset scan of the desired machines.
   Asset scans can be initiated from the **Agentless Operation page**, from a machine group, from a favorite, or from Machine View.
   See **How to Perform Asset Scans** for details.
3. View the asset scan results.
   Asset scan results are available within **Machine View**.

179. How Do I . . .?: Use The ITScripts Feature

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

The ITScripts feature enables you to execute PowerShell scripts against the machines and machine groups you have already defined in Security Controls.

To use the ITScripts feature you do the following:

1. Review the **ITScripts Overview topic** to familiarize yourself with the capabilities of this feature.
2. Use the **Script Catalog Manager** to specify which scripts are approved for use within your organization.
3. **Execute the desired script** from within the Security Controls interface.
4. Review the results using **ITScript Results View**.

180. How Do I . . .?: Use The Power Management Feature

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



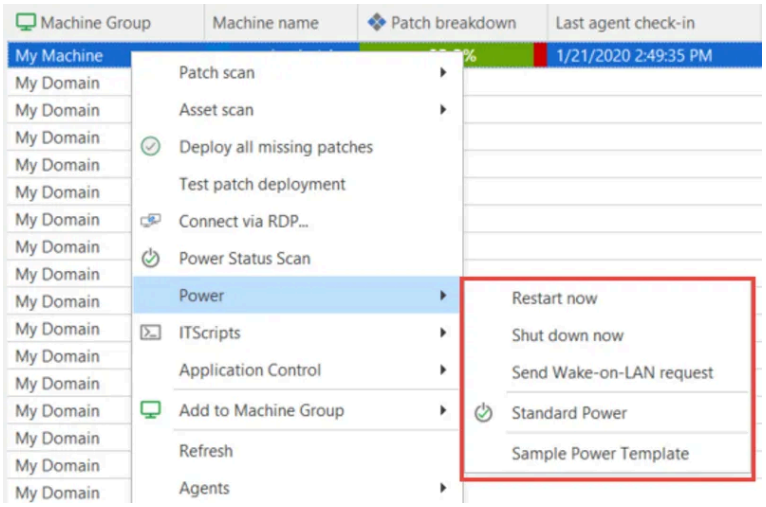
Overview Information

The power management feature enables you to control the power state of the machines in your organization. The primary reasons for using power management are to:

- Prepare your machines for maintenance tasks
- Reduce power and noise consumption
- Reduce operating costs
- Prolong battery life

To use the power management feature you do the following:

1. Initiate power management commands from either Machine View or Scan View.
   Use the right-click menu to immediately restart, shut down, or wake up machines. See **How to Initiate Power Management Tasks** for details.



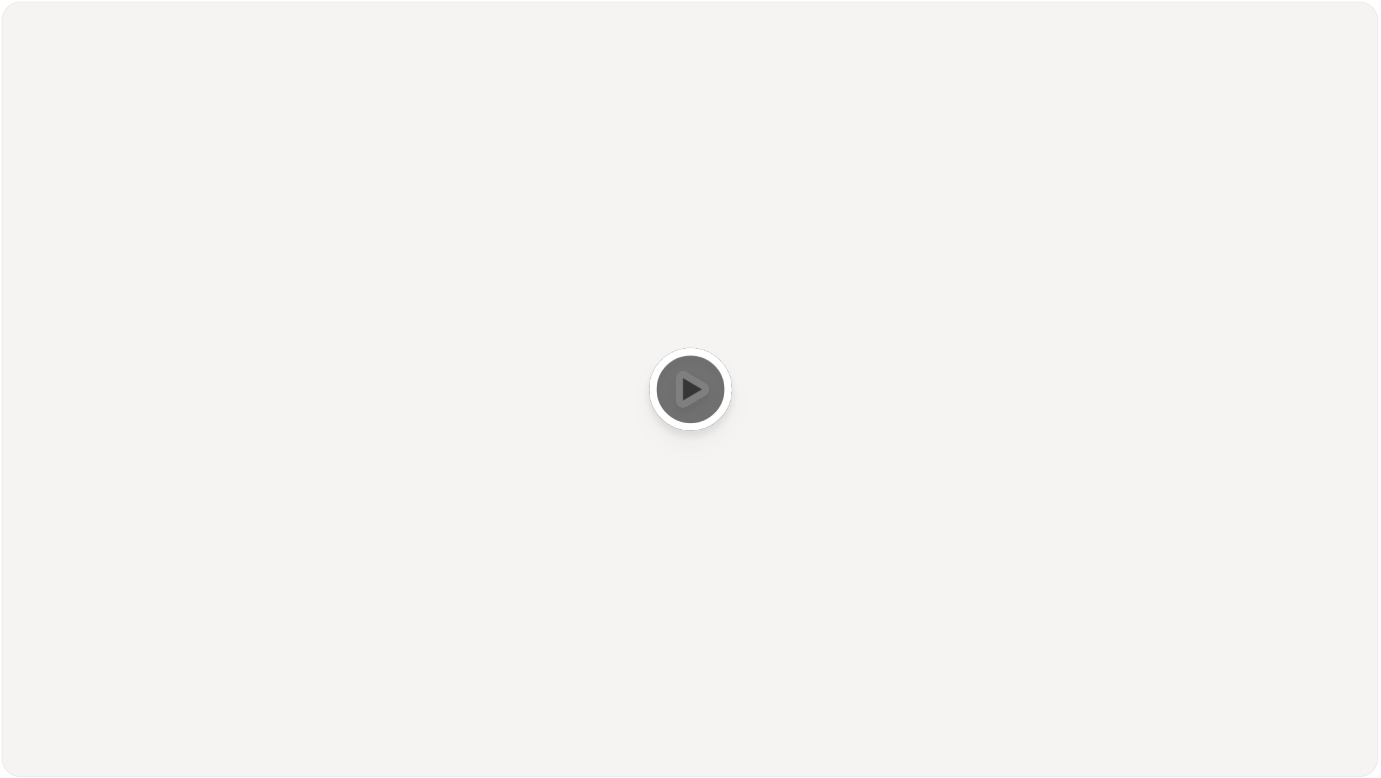
Track the status of power commands using the Operations Monitor.
See **Monitoring a Power Task** for details.

3. To schedule a restart or a shutdown you use a power management template.
   See:
   - **Creating and Editing a Power State Template**
   - **How to Initiate Power Management Tasks**
   - **Scheduling Power Management Tasks**

Before using the Wake-on-LAN feature be sure to read **Wake-on-LAN Implementation Notes**.
You can use the Wake-on-LAN feature to wake up machines that are sleeping, hibernating, or powered off. For example, you might want to wake up your machines during a maintenance window so they can receive critical security updates. Or you might schedule a wake-up call for a group of machines that you put to sleep the night before so they are ready for the work day.

5. Power management tasks can also be performed by agents.
   See **Creating and Configuring a Power Task** for details.
6. Perform a power status scan to verify the updated power status of your machines.
   See **Performing a Power Status Scan** and **Viewing Power Status Scan Results**.

181. How Do I . . .?: View How-to Tutorials

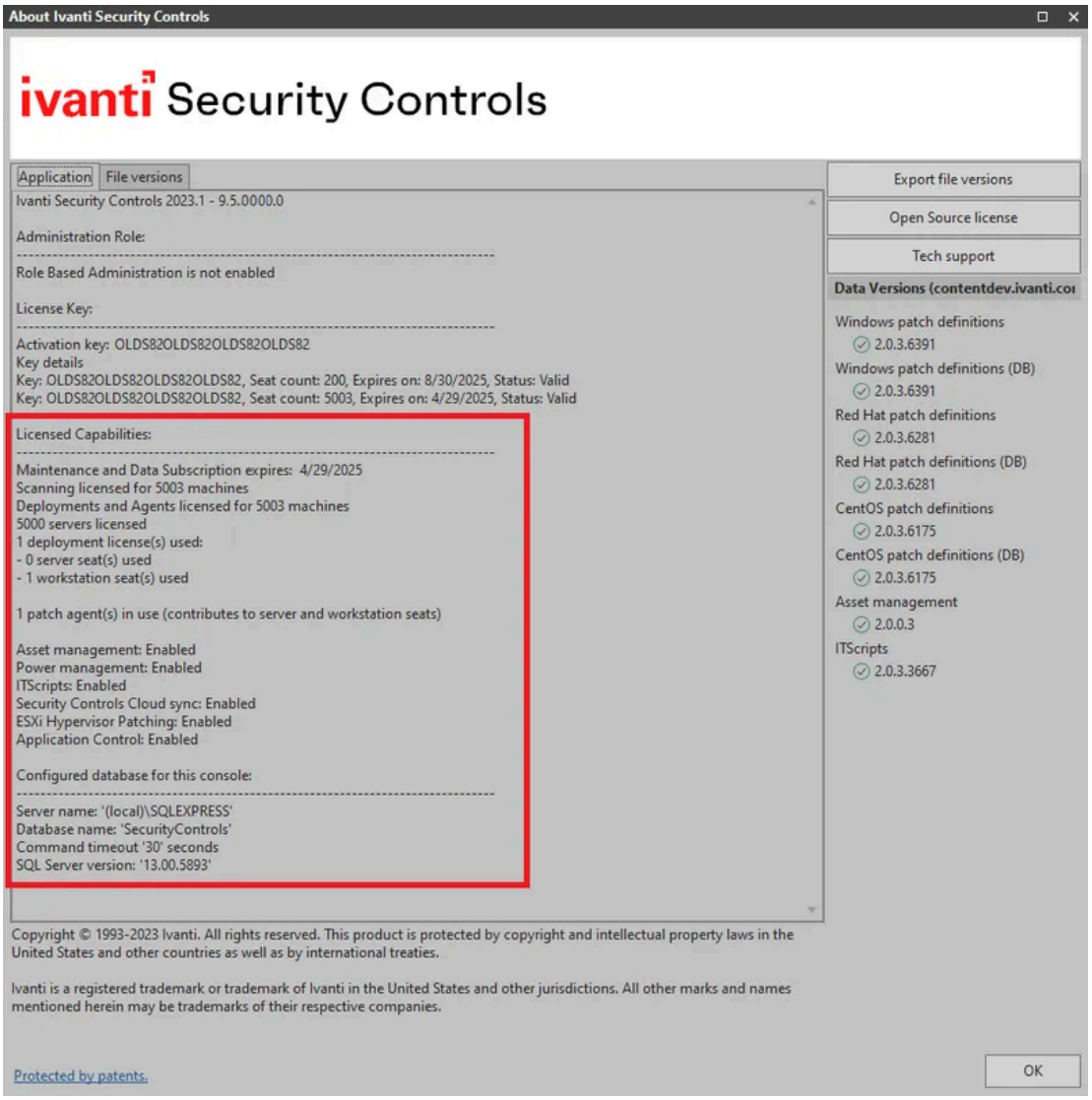


This channel contains a number of video tutorials. The tutorials walk you through the product interface, showing you exactly how easy it is to use Security Controls and how to get the maximum benefit from the product.

182. How Licenses are Tracked

When a patch deployment is performed, Security Controls records the machine name in the database if it does not already exist. From there, the number of remaining seats available for deployment is reduced by one for each target. If you elect to use Security Controls Agent, each agent machine is allocated a license and also counts against the total number of license seats available. If the same machine is managed in both an agentless and agent-based manner, that machine is counted only once. Similarly, when scanning virtual machines, a machine is counted only once even if it is scanned both in online (powered on) mode and offline (powered off) mode.

You can easily find out how many license seats have been used by choosing **Help > About** Security Controls.



183. How Role-Based Administration Works

This feature is not available to unlicensed users.

You can **assign different roles** to different users of Security Controls. This enables you to make the program available to a wide variety of people within your organization while maintaining control over its use. The role assigned to a user determines what that particular user can do.

Here's how it works. When Security Controls is launched it checks if role-based administration is enabled. If so, the program then looks to see if the current user has been assigned a role. If the user has been assigned a role, the program grants that user access to only those features allowed by their role. For example, you may have a number of users who are allowed to create reports, but only one or two users who have permission to deploy patches.

Features that are not available due to role limitations will be either grayed out or removed from the interface. If a user has not been assigned a role they will not be able to start the program. It is not possible for a user to switch roles while within the program.

Role-based administration is initially disabled. Until you enable this feature, all users will have full access to the program. You enable and configure role-based administration via the **Manage > Users** menu. See **Enabling and Disabling Role-based Administration** and **User Manager** for detailed information.

184. How the Agent Process Works

Agents are configured via the Security Controls interface and then installed on the desired machines. Once installed, each agent will periodically check in with the console, or if it is a disconnected agent it may check in with the **Security Controls Cloud service**. How often an agent checks in is a **configurable item**, but the check-ins typically occur at least once a day. An agent can also be configured to listen to the console for policy updates and download the new policy immediately.

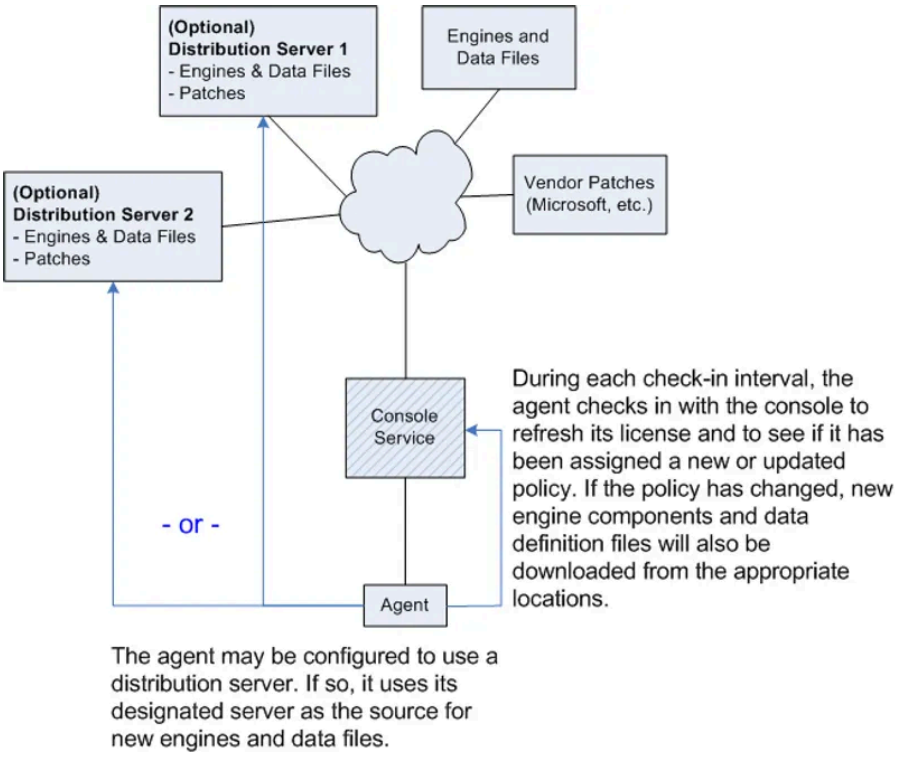
During each check-in the agent checks with the console and does the following:

> The process is a bit different if you are using Security Controls Cloud synchronization; see **Security Controls Cloud Synchronization Overview** for details.

- It refreshes its license. An agent license is valid for 45 days from the most recent check-in.
- It checks if it is assigned a distribution server, and if so, which one.
- It checks for any policy configuration changes. If the policy has been changed, the new policy will be pushed from the console to the agent.
- It automatically receives any new engine and data files that have become available. The agent will receive these files from either the default websites or from its assigned distribution server.
- It automatically receives a new version of the agent if it has become available.
- It receives any credential information it needs in order to authenticate itself to any distribution servers or proxy servers.

An agent will also download new engine and data files from the default website or from its assigned distribution server whenever a scheduled scan is performed.

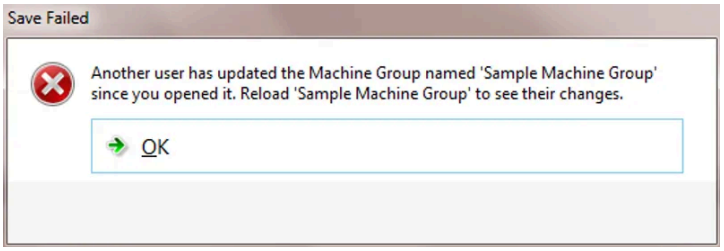
The following figure illustrates the agent process.



185. How Security Controls Manages Multiple Administrators

Security Controls contains a number of built-in checks to guard against simultaneous and conflicting commands from different administrators. For example:

- The program will not allow duplicate group names or template names.
- The program will not allow simultaneous updates to any groups, templates, distribution servers, or agent policies by different administrators. If this situation should occur the second administrator will receive a warning message.



Only one console will be authorized to use the **Database Maintenance tool**. If an administrator at another console wants to perform maintenance on the database, that administrator must **take ownership** of that task before the program will allow the administrator to continue.

186. How to Add Virtual Machines to a Machine Group

Virtual machines can be added to a machine group. The recommended best practice is to create a machine group consisting of nothing but virtual machines. You can, however, add both physical machines and virtual machines to the same machine group if you wish.

There are four different ways to add virtual machines to a machine group:

- If **virtual machines are hosted by a server** you can add the server to the machine group. This effectively adds all virtual machines hosted by the server to the machine group. The virtual machines can be in either online or offline mode.

> The server will also be added to the **Virtual Inventory list**, which is used to manage your ESXi Hypervisors.

If **virtual machines are hosted by a server** you can add individual virtual machines to the machine group. The virtual machines can be in either online or offline mode.

- You can also add **virtual machine templates** that may be hosted on a server.
  If virtual machines reside on individual workstations, you may consider adding the machines to the group twice to ensure that each virtual machine is successfully scanned regardless of its current power state (online or offline).
  - You can add the full path names or directory names of the offline virtual machines to the machine group using the **Workstation Virtual Machines** tab. The virtual machines defined using this tab are scanned only if they are in offline mode.
  - You can add the virtual machines to the machine group using the **Machine Name** tab, the **Domain Name** tab, or the **IP Address/Range** tab. Virtual machines defined using these tabs are scanned only if they are in online mode.

> For overview information about scanning for and deploying patches to virtual machines, see **Virtual Machine Overview**.

187. How to Execute a Script

> When executing a script, a **default credential** must be specified or a credential must be assigned to the target machine or machine group.

All scripts can be executed using an **ITScripts template**. You can also execute a script directly without a template if the script does not require input parameters or if you want to use the default parameter values.

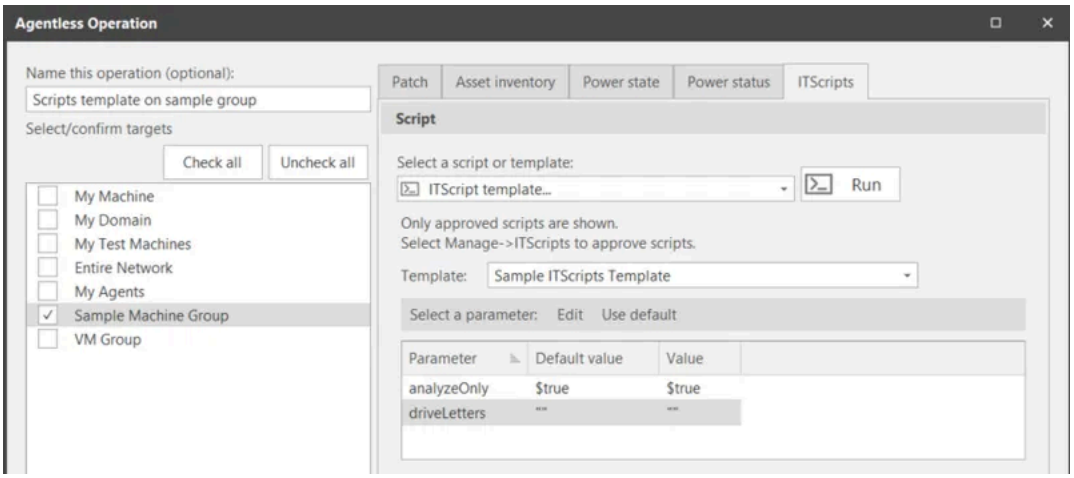
You can initiate the execution of a script from several different areas of the interface.

> A console must trust the authority that issued the certificate in order to import or execute the script on that console. If you **import user scripts** on one console, they will appear on other consoles that are using the same database. If the other consoles don't trust the signer, however, they will not be able to execute the scripts.

FROM THE AGENTLESS OPERATION PAGE

You can use the Agentless Operation page to execute a script on any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or on a custom machine group.

1. Type a name for the operation you are about to perform.
2. One suggestion is to specify which machines are affected and the purpose of the operation (for example, *Sample Group GetRebootTime*). You may wish to include other identifiers such as the template being used, if it is a regularly scheduled operation or an out of band task, etc. A maximum of 80 characters can be used for the name.
   A date and time stamp will be automatically appended to the name. If you do not specify an operation name, the date and time stamp will be used as the name.
   Select the desired machine group(s).



On the ITScripts tab, select how you want to execute the script.

- **ITScript:** When this option is selected, additional fields are displayed that let you:
  - Choose the script you want to execute (scripts defined as target type = Console are not available here)
  - Edit any parameters associated with the script

  ITScript template: When this option is selected, this area lets you choose the template you want to use when executing the script.

Select when you want to execute the script (**Now**, **Once**, or **Recurring**).

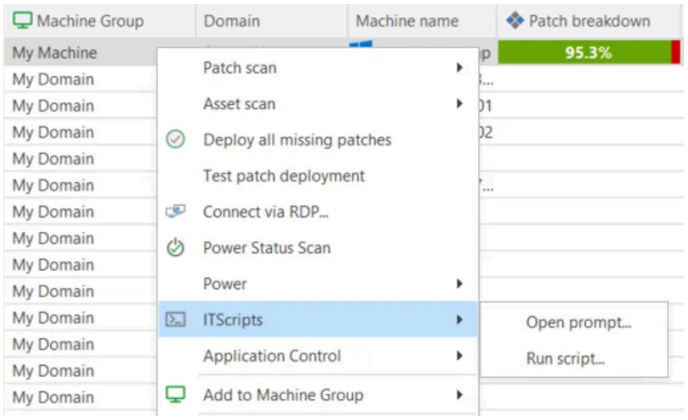
5. Click either **Run** or **Schedule**.
   - **Run:** This is the button name if **Now** is your selected scheduling option. This will immediately begin executing the script on the machines in the machine group(s). The Operations Monitor is used to track the progress of the script.
   - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Scripts and Monitoring a Scheduled Script for more details.

You can review the results of the script using ITScripts Results View.

FROM MACHINE VIEW OR SCAN VIEW

You can execute a script from within Machine View or Scan View by using right-click commands.

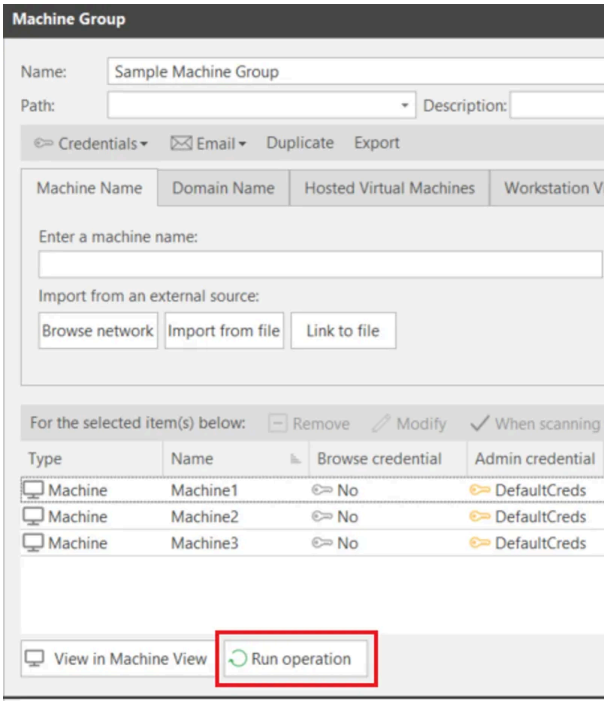
1. Select one or more machines.
2. Right-click the machine(s), select **ITScripts**, and then specify how you want to execute the script.



- **Open prompt:** Enables you to start a Windows PowerShell session with the selected machine. For details see **Opening a PowerShell Prompt**.
- **Run script:** Opens the **Agentless Operation dialog**, which enables you to run a script with or without a template.

FROM A MACHINE GROUP

1. In the **Machine Groups** pane select the desired machine group.
2. Within the machine group dialog click **Run Operation**.



On the Agentless Operation dialog, select when and how you want to execute the script.

- **ITScript:** When this option is selected, additional fields are displayed that let you:
  - Choose the script you want to execute (scripts defined as target type = Console are not available here)
  - Edit any parameters associated with the script

  ITScript template: When this option is selected, this area lets you choose the template you want to use when executing the script.

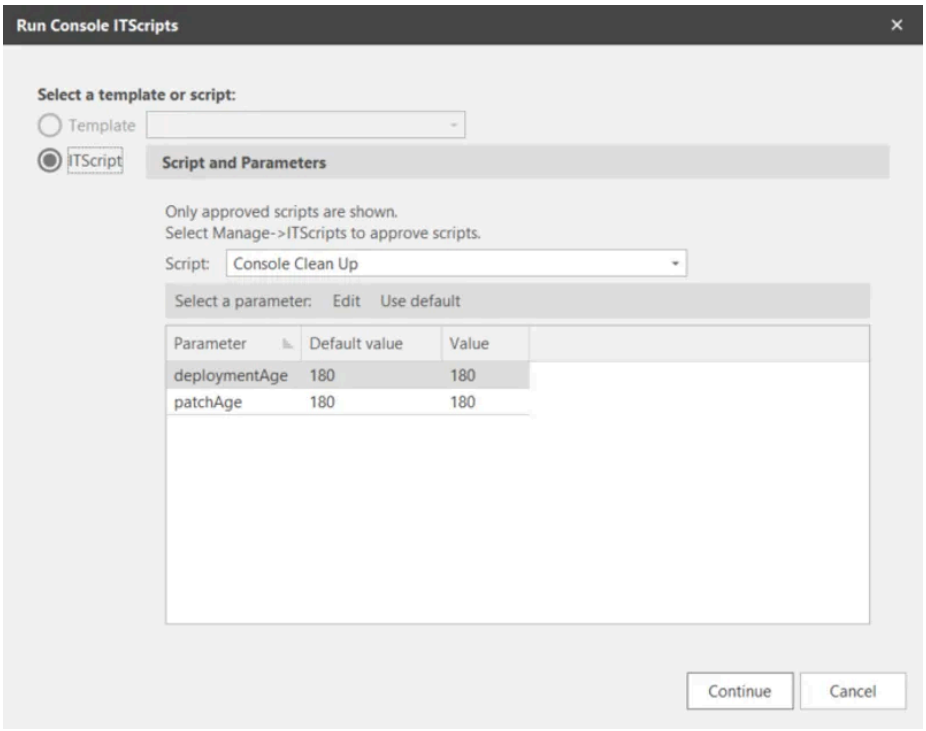
Click either **Run** or **Schedule**.

- **Run:** This is the button name if **Now** is your selected scheduling option. This will immediately begin executing the script on the machines in the machine group. The Operations Monitor is used to track the progress of the script.
- **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Scripts and Monitoring a Scheduled Script for more details.

You can review the results of the script using ITScripts Results View.

FROM THE TOOLS > RUN CONSOLE ITSCRIPTS MENU

The **Tools > Run console ITScripts** command enables you to select and run Console mode scripts. These are scripts that are designed to run only on the console machine and not against target machines. The **Run console ITScripts** dialog is displayed.



This dialog enables you to run a console-only script with or without a template.

- If you choose a template you will execute the associated script using predefined parameter values.
- If you choose to run the script directly without a template you have the ability to modify the values of any input parameters associated with the script.

After making your selections, click **Continue** and use the **Agentless Operation dialog** to specify when the Console mode script should be run.

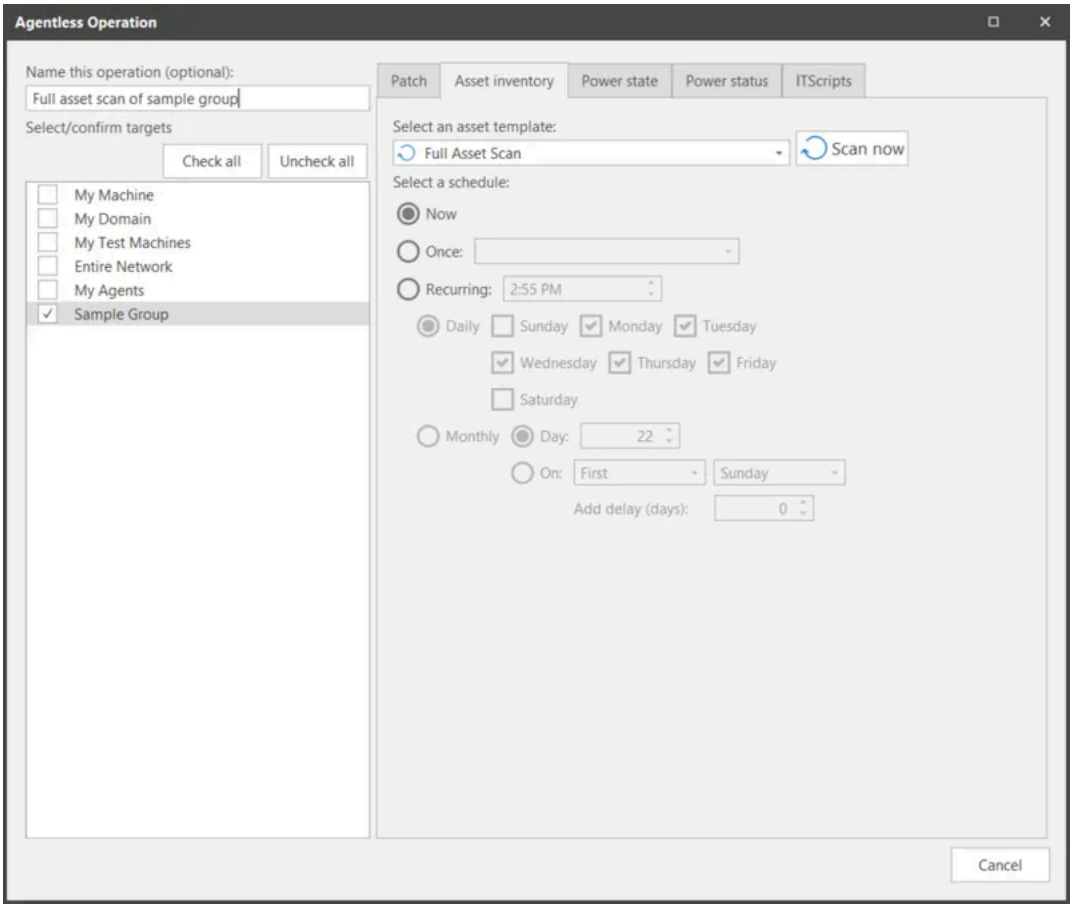
188. How to Initiate an Asset Scan

An asset scan can be initiated from the **Agentless Operation** page, from a machine group, from a favorite, or from Machine View.

FROM THE AGENTLESS OPERATION PAGE

You can use the Agentless Operation page to initiate a scan of any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or of a custom machine group.

1. Type a name for the operation you are about to perform.
   At a minimum the name should indicate what you are scanning and when it is being scanned (for example, *Machine group name mm/dd/yy*). You may wish to include other identifiers such as the scan template being used, if it is a regularly scheduled scan or an out of band task, etc. A maximum of 100 characters can be used for the name.
2. Select the machine group you want to scan.



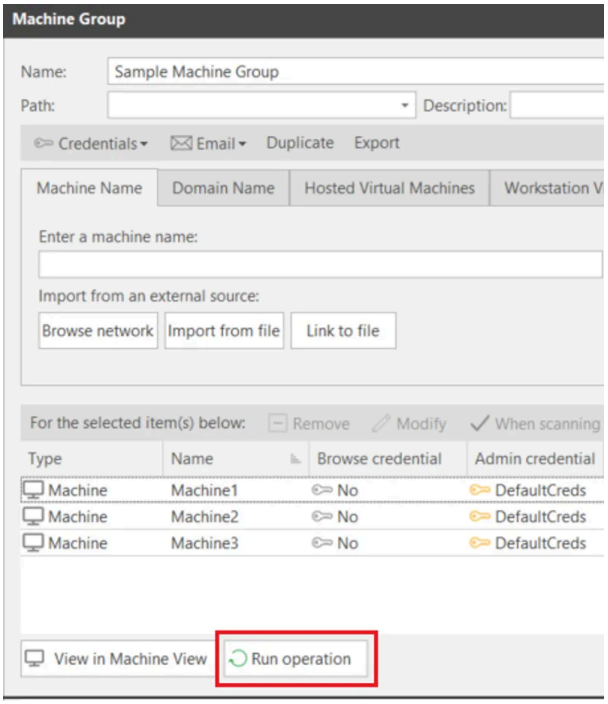
On the **Asset inventory** tab, select the template you want to use when performing the asset scan (Full Asset Scan or a custom asset scan template).

4. Choose when you want to perform the scan (**Now**, **Once**, or **Recurring**).
5. Click either **Scan now** or **Schedule**.
   - **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to track the progress of the asset scan.
   - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Asset Scans and Monitoring a Scheduled Asset Scan for more details.

You can review the results of the asset scan using Machine View.

FROM A MACHINE GROUP

1. In the **Machine Groups** pane select the desired machine group.
2. Within the machine group dialog click **Run Operation**.



On the **Run Operation** dialog select when you want the asset inventory scan to run and which asset scan template you want to use.

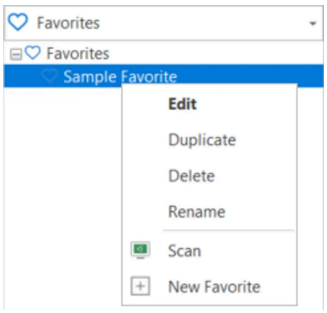
4. On the **Run Operation** dialog click either **Scan now** or **Schedule**.
    - **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to **track the progress of the asset scan**.
    - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See **Scheduling Asset Scans** and **Monitoring a Scheduled Asset Scan** for more details.

You can review the results of the asset scan using **Machine View**.

FROM A FAVORITE

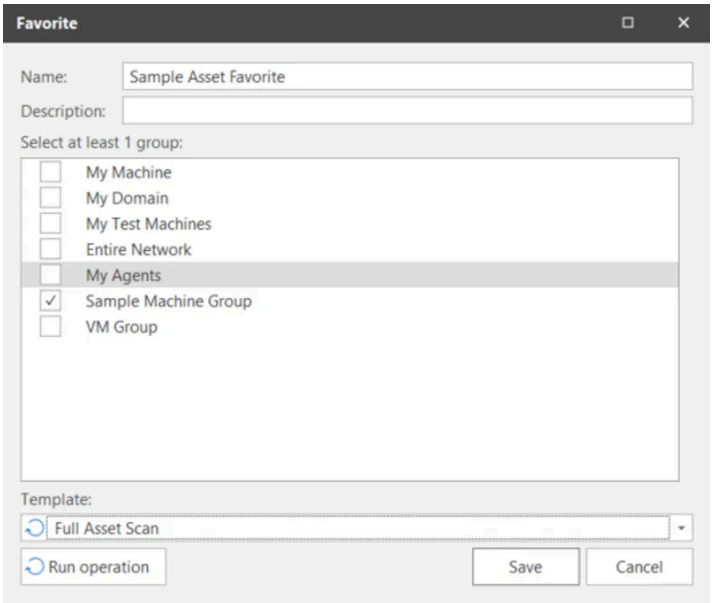
A favorite consists of one or more machine groups and one template. You select the machine groups you want to scan and then specify how the machines should be scanned. A favorite is typically used to initiate a **scheduled scan**.

One way to initiate an asset scan of a favorite is to right-click the favorite in the **Favorites** list and then select **Scan**. This will enable you to specify when to perform the scan but not how (the asset scan template previously configured for use with this favorite will always be used).



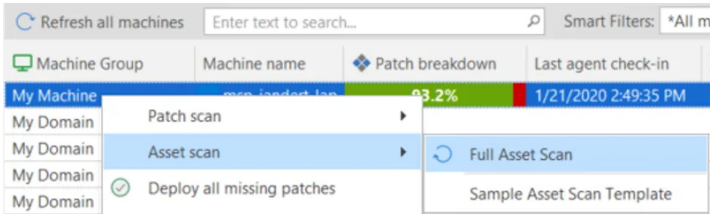
If you want to verify and/or change the configuration of the favorite before you initiate the scan you simply:

1. Select the desired favorite in the **Favorites** list.
   The **Favorite dialog** is displayed. It shows the current configuration of the favorite.
2. Review the configuration, make any desired changes, and then click **Run Operation**.



FROM MACHINE VIEW

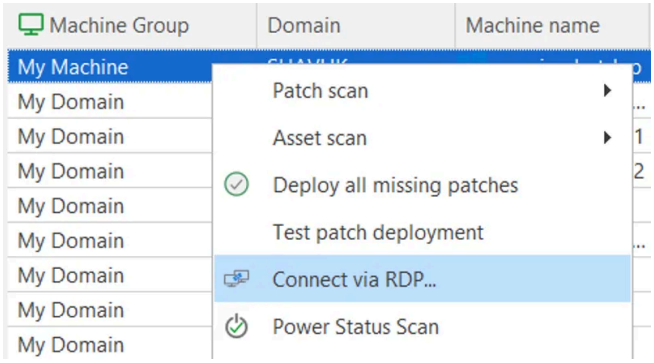
1. Select one or more machines.
2. Right-click the machine(s) and then select the desired asset scan template.



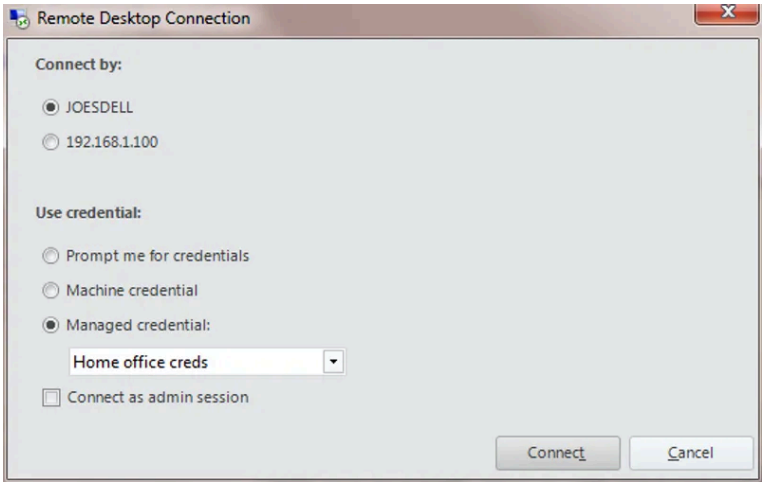
189. How to Initiate a Remote Desktop Connection

A Remote Desktop connection can be initiated from either Machine View or Scan View by using the right-click menu.

1. Select the desired target machine.
2. Right-click the machine and then select **Connect via RDP**.



Use the **Remote Desktop Connection** dialog to specify how you will make the connection.



Field	Description
Connect by	You can make the connection using either the machine name or the IP address. Both options should work equally well. If your scan information is old and you cannot depend on the IP address you may want to use the host name. If your organization is experiencing DNS issues and cannot properly resolve the host name you should use the IP address.
Use credential	You must specify which credential to use when making the RDP connection. • **Prompt me for credentials:** Will display a separate dialog that you can use to provide the user name and password credentials. This is a good option to use for rogue machines for which you do not have predefined credentials.  **Machine credential:** Will use the credential assigned on the **Machine Properties** dialog. This is a convenient option for machines you have previously assigned credentials. • **Managed credential:** Enables you to choose which credential to use when making the connection. This is the preferred option for those machines that use your managed credentials. See **Managing Credentials** for more information. If the credential you choose does not work and you are unexpectedly prompted for credentials, check to see if the user name contains *.|Administrator*. Some newer operating systems translate this term to *consolemachinename|Administrator*and the credentials will be rejected. The solution is to use *Administrator* rather than *.|Administrator*.
Connect as admin session	If enabled, specifies that the remote connection will be made to the "session 0" session of the server (the target machine). Session 0 is required to perform certain administrative tasks on some Windows operating systems.
Connect **Cancel**	To initiate the RDP connection, click **Connect**. To cancel without making the connection, click **Cancel**.

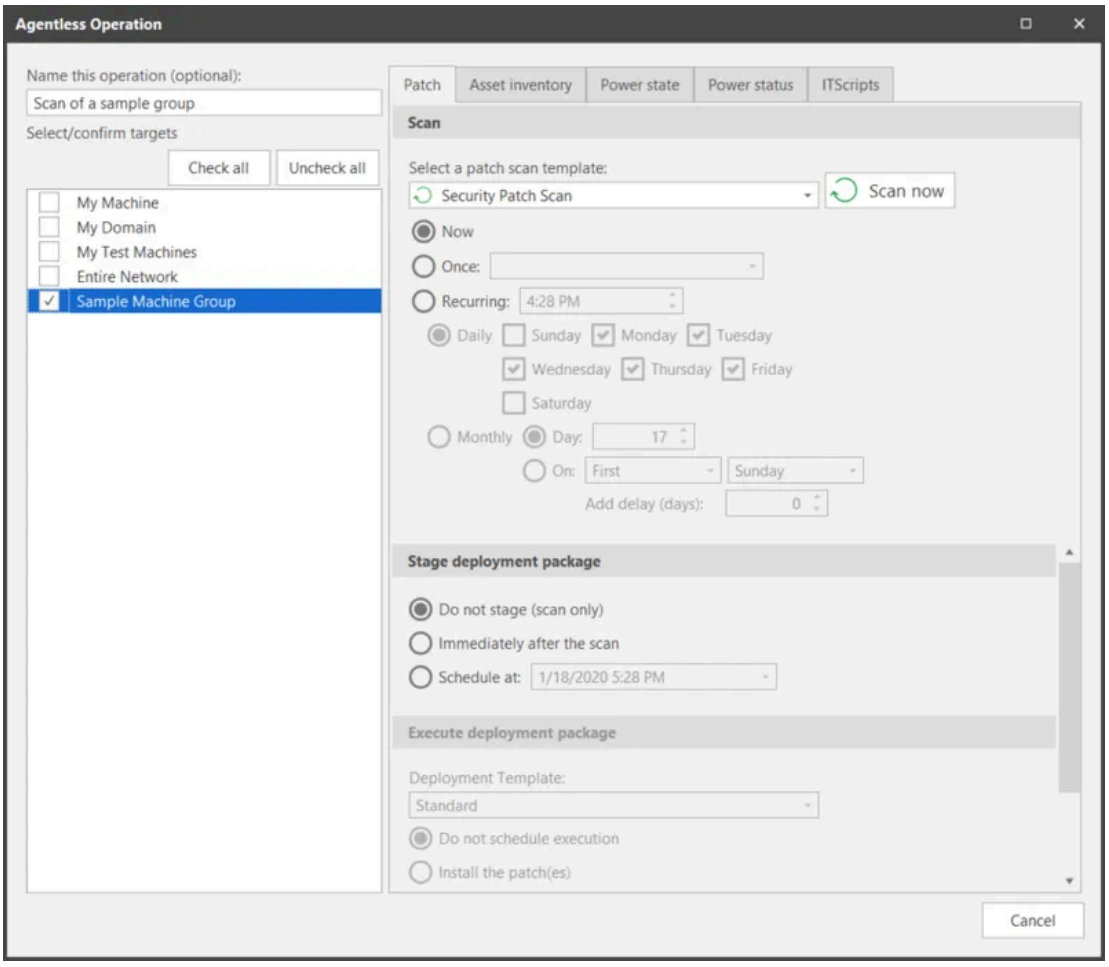
190. How to Initiate a Patch Scan

A patch scan can be initiated from the **Agentless Operation** page, from a machine group, from a favorite, or from Machine View or Scan View.

From the Agentless Operation Page

You can use the Agentless Operation page to initiate a scan of any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or of a custom machine group.

1. (Optional) Type a name for the operation you are about to perform (for example, My machine scan mm/dd/yy).
   A maximum of 100 characters can be used for the name.
2. Select the machine group you want to scan.

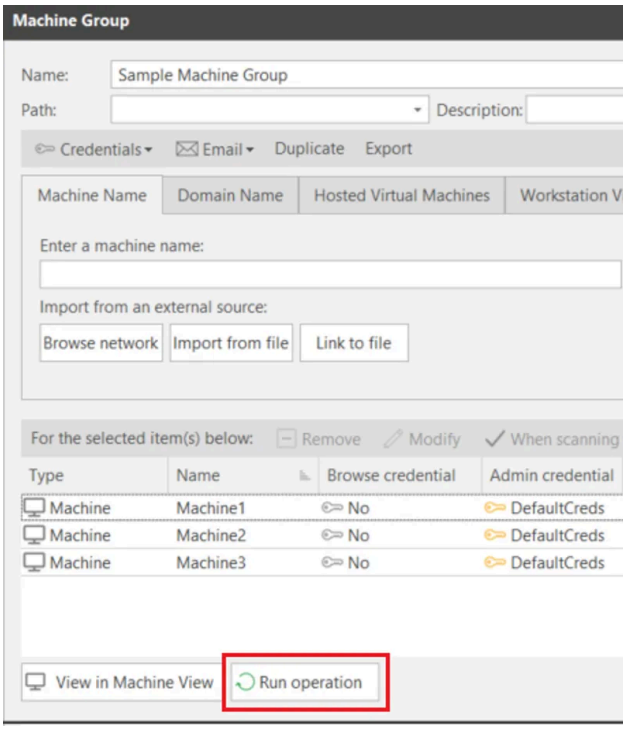


1. Select the template you want to use when performing the patch scan (Security Patch Scan, All Patches or a custom patch scan template).
2. Choose when you want to perform the scan (**Now**, **Once**, or **Recurring**).
3. If you want to perform just a scan without automatically deploying any missing patches, choose **Do not stage (scan only)**.
   For information on automatically staging and executing patch deployments, see Automatically Deploying Patches.
4. Click either **Scan Now** or **Schedule**.

- **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to track the progress of the patch scan.
- **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Patch Scans and Monitoring a Scheduled Patch Scan for more details.

From a Machine Group

1. In the **Machine Groups** list select the desired machine group.
2. Within the machine group dialog click **Run Operation**.

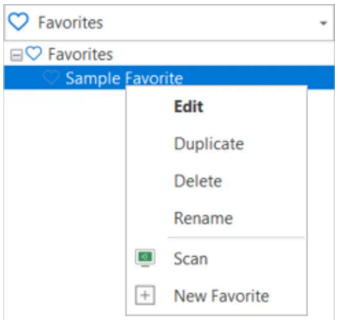


1. On the **Run Operation** dialog select when you want the scan to run and which patch scan template you want to use.
2. If you want to perform just a scan without automatically deploying any missing patches, choose **Do not stage (scan only)**. For information on automatically staging and executing patch deployments, see Automatically Deploying Patches.
3. On the **Run Operation** dialog click either **Scan now** or **Schedule**.
   - **Scan now:** This is the button name if **Now** is your selected scheduling option. A scan of all machines in the machine group will begin immediately. The Operations Monitor is used to track the progress of the patch scan.
   - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Patch Scans and Monitoring a Scheduled Patch Scan for more details.

From a Favorite

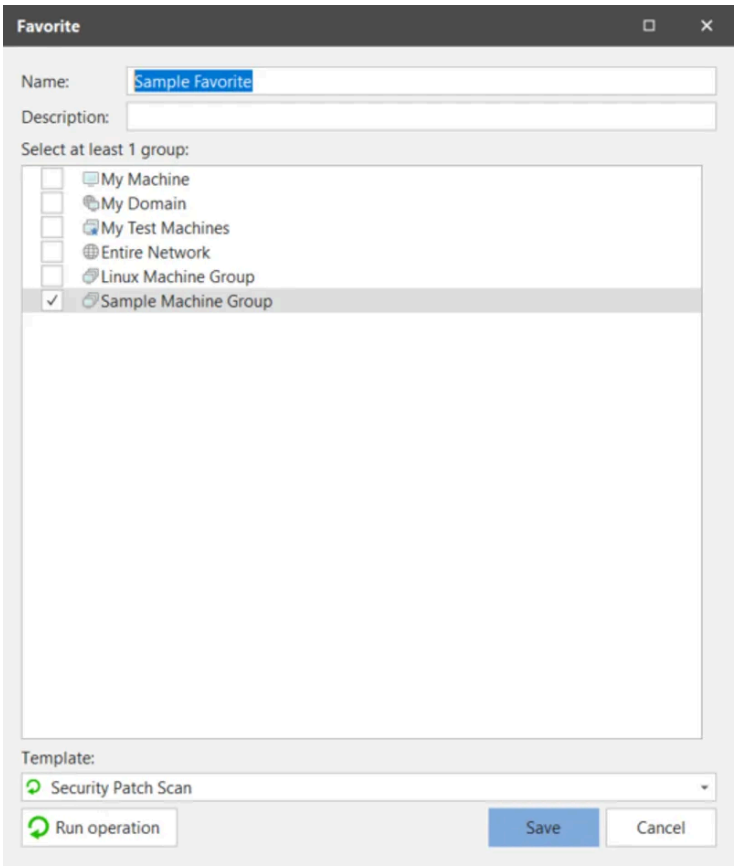
A favorite consists of one or more machine groups and one template. You select the machine groups you want to scan and then specify the template to use when performing the scan.

The quickest way to initiate a patch scan of a favorite is to right-click the favorite in the **Favorites** list and then select **Scan**. This will enable you to specify when to perform the scan but not how (the patch scan template specified in the favorite will always be used).



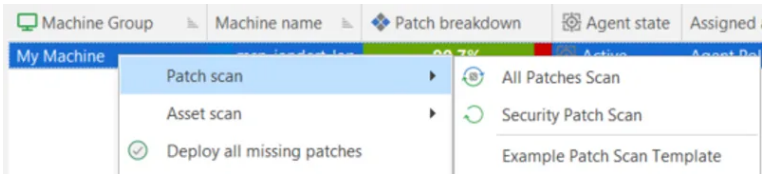
If you want to verify the configuration of the favorite before you initiate the scan you simply:

1. Select the desired favorite in the **Favorites** list.
   The Favorite dialog is displayed. It shows the current configuration of the favorite.
2. Verify the configuration and then click **Run Operation**.



From Machine View or Scan View

1. Select one or more machines.
2. Right-click the machine(s) and then select the desired patch scan template.



From the API

For information, see:

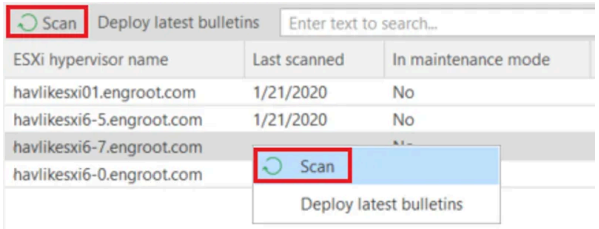
- Overview of the REST API
- Overview of the PowerShell Command-Line API

191. How to Initiate a Scan of an ESXi Hypervisor

There are multiple ways to initiate a scan of your ESXi hypervisors.

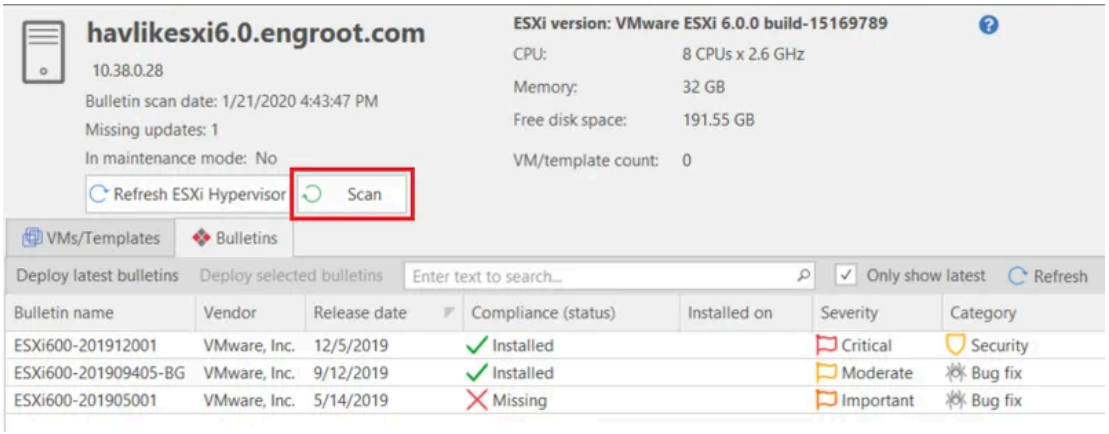
Scanning One or More Managed ESXi Hypervisors

1. In the **vCenter Servers list**, select the desired vCenter Server.
2. In the top pane, select the desired ESXi hypervisor(s).
3. Initiate the scan using either the **Scan** button along the top of the table or the right-click menu.



Scanning a Managed or Unmanaged ESXi Hypervisor

1. In the **vCenter Servers list** or the **ESXi Hypervisors list**, select the desired ESXi hypervisor.
2. In the header area, click **Scan**.



Viewing Scan Results

The **Operations Monitor** is used to monitor the status of the hypervisor scan. The bulletins discovered during the scan can be found on the **Bulletins** tab of your **managed** or **unmanaged** hypervisor. Remember to select **View > Refresh** to view the most current information.

192. How to Initiate Power Management Tasks

There are a number of power management tasks that you can perform on the machines in your organization, including:

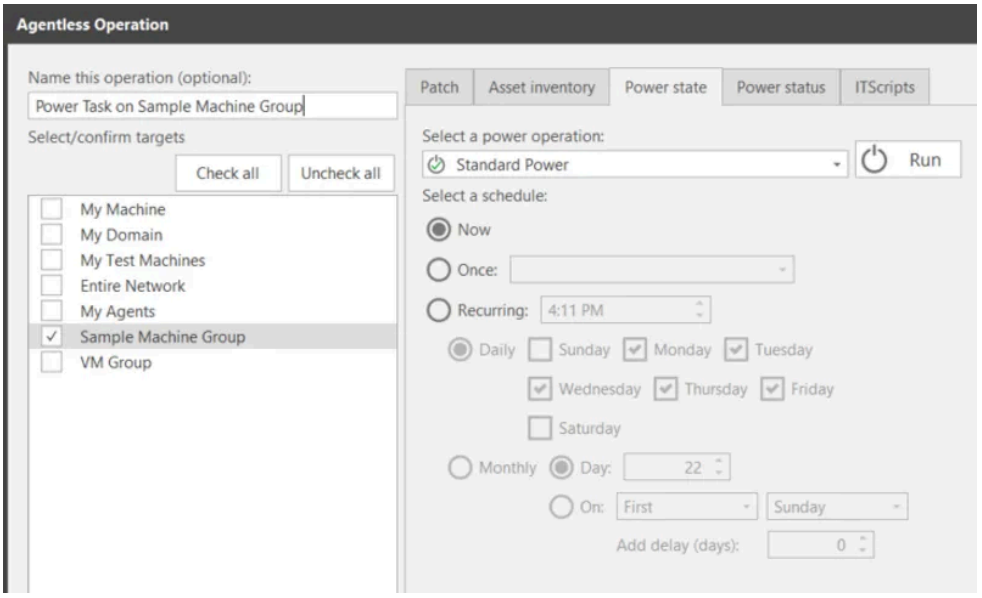
- Restart now
- Shut down now
- Send a Wake-on-LAN request (immediate or scheduled)
- Determine the current power state by performing a **power status scan**
- Modify the power state using a **power state template** (immediate or scheduled)

Power management tasks can be initiated from several different areas of the interface.

FROM THE AGENTLESS OPERATION PAGE

You can use the Agentless Operation page to initiate a power task on any of the four pre-defined groups (**My Machine**, **My Domain**, **My Test Machines**, **Entire Network**) or of a custom machine group.

1. Type a name for the operation you are about to perform.
   At a minimum the name should indicate which machines will be affected and when the power task will be run (for example, *Machine group name mm/dd/yy*). You may wish to include other identifiers such as the power state template being used, if it is a regularly scheduled task or an out of band task, etc. A maximum of 100 characters can be used for the name.
2. Select the desired machine group.

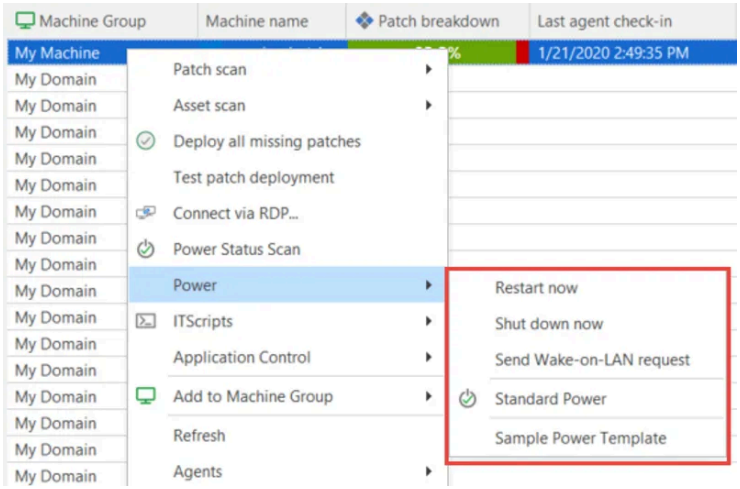


1. Choose either the **Power state** tab or the **Power status** tab.
   The **Power state** tab is used if you want to modify the power state of your machines and the **Power status** tab is used if you want to determine the current power state of your machines.
2. (Conditional) If you choose the Power state tab, select the power task you want to perform (either the **Standard Power** template or a custom power state template).
3. Choose when you want to perform the power task (**Now**, **Once**, or **Recurring**).
4. Click either **Run/Scan now** or **Schedule**.
   - **Run/Scan now:** When **Now** is the scheduling option, the button name will be either **Run** (if a power template is selected) or **Scan now** (if **Power Status Scan** is selected). The power task will begin immediately on all machines in the machine group. The Operations Monitor is used to track the progress of the power task.
   - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See Scheduling Power Tasks and Monitoring a Scheduled Power Task for more details.

FROM MACHINE VIEW OR SCAN VIEW

You can initiate a number of different power management tasks from within Machine View or Scan View by using right-click commands.

1. Select one or more machines.
2. Right-click the machine(s) and then select either a power management command or the desired power state template.

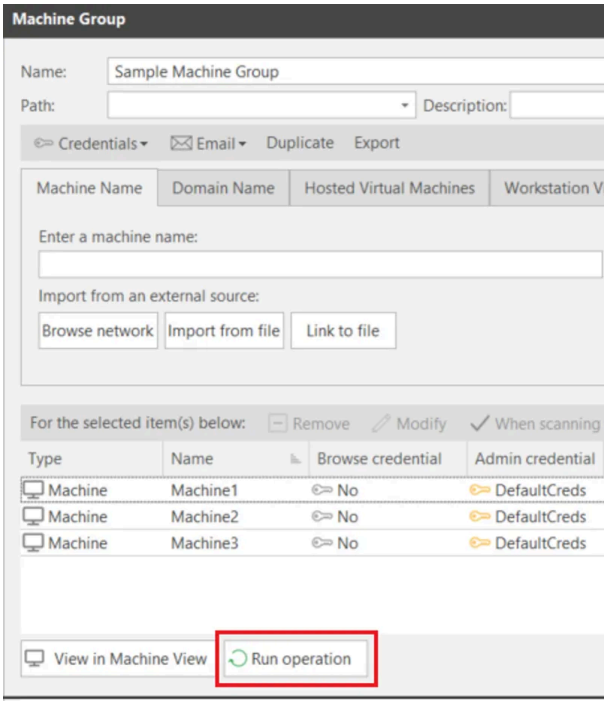


The first two power management commands enable you to immediately restart or shut down the selected machines. The **Send Wake-on-LAN request** can be sent to the selected machines immediately or it can be scheduled for a later date and time. The **Status Scan** command initiates a power status scan of the selected machines. Finally, a power state template can be used to put the selected machines into a particular state (powered on, in sleep mode, in hibernate mode, or powered off).
For more specifics please see the following:

- Scheduling Power Management Tasks
- Restart Implementation Notes
- Shutdown Implementation Notes
- Wake-on-LAN Implementation Notes
- Sleep and Hibernation Implementation Notes
- Monitoring a Power Status Scan

FROM A MACHINE GROUP

1. In the **Machine Groups** pane select the desired machine group.
2. Within the machine group dialog click **Run Operation**.



On the **Run Operation** dialog select when you want the power state or power status task to run.

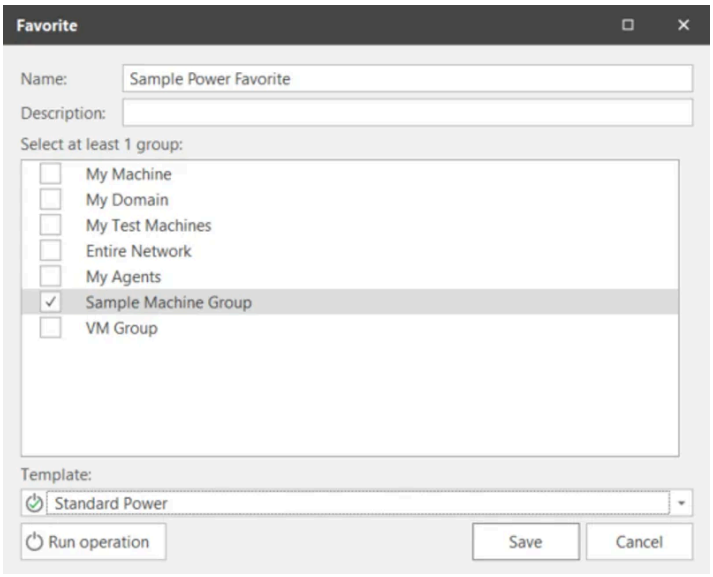
4. On the **Run Operation** dialog click either **Run/Scan now** or **Schedule**.
    - **Run/Scan now:** When **Now** is the scheduling option, the button name will be either **Run** (if a power template is selected) or **Scan now** (if **Power Status Scan** is selected). The power task will begin immediately on all machines in the machine group. The Operations Monitor is used to **track the progress of the power task**.
    - **Schedule**: This is the button name if **Once** or **Recurring** is your scheduling option. See **Scheduling Power Tasks** and **Monitoring a Scheduled Power Task** for more details.

What state the machines are left in following a restart is dependent on how the power template is configured.

FROM WITHIN A FAVORITE

You can schedule one or more machine groups for a shutdown or a restart by using a power state template.

1. In the **Favorites** pane select the desired favorite.
2. In the **Favorite** dialog select the desired machine group(s).
3. In the **Template** box select the desired power state template.
4. See **Creating and Editing a Power State Template** for information on creating your own unique power state templates.



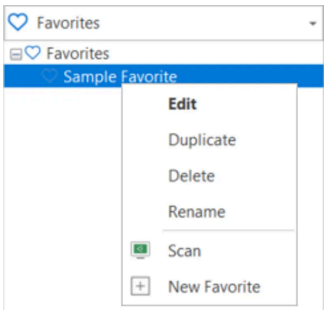
Click **Run operation**.

The **Run Operation** dialog is displayed, enabling you to schedule the power state job to run now or at some time in the future. What state the machines are left in following a restart is dependent on how the power template is configured.

BY RIGHT-CLICKING A FAVORITE

> With this method the favorite must already specify the power state template to use.

1. In the **Favorites** pane, right-click the desired favorite.



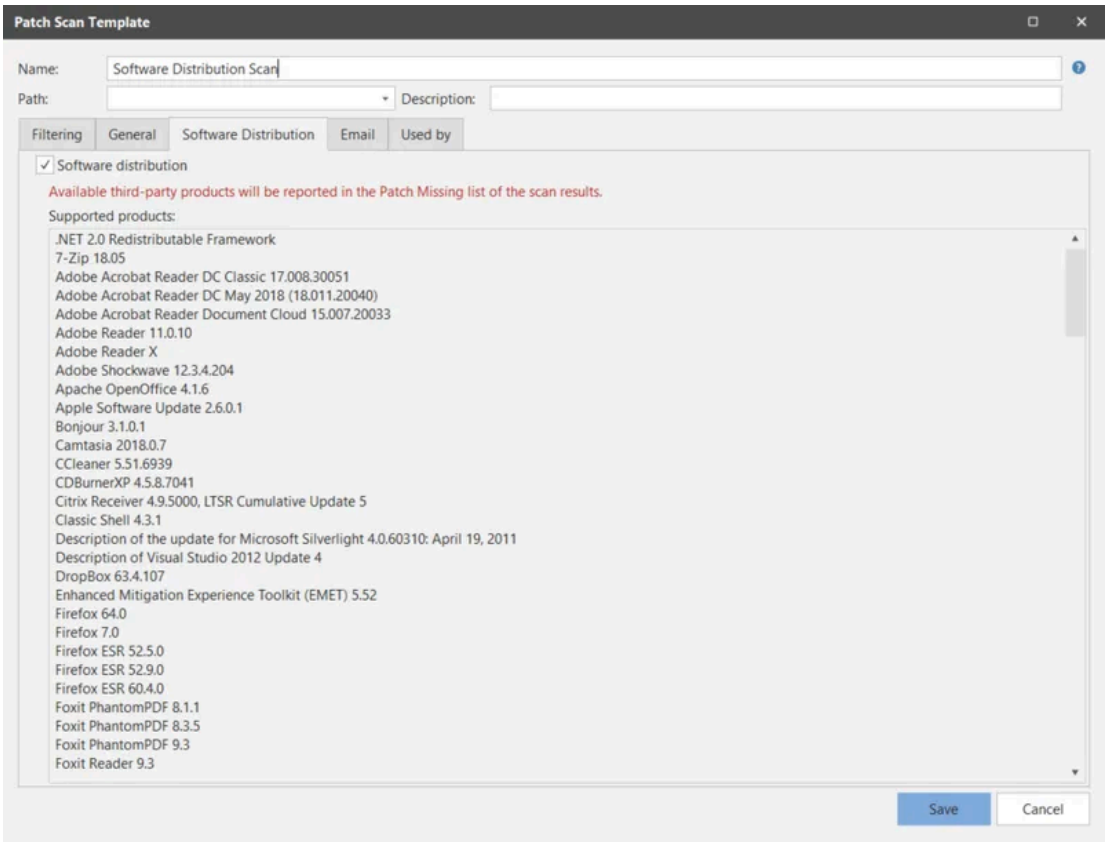
Select **Scan**.

Security Controls will not actually scan the machines; rather, it will launch a **Run Operation** dialog that enables you to schedule the power state job to run now or at some time in the future. What state the machines are left in following a restart is dependent on how the power template used by this favorite is configured.

193. How to Scan for Third-Party Applications

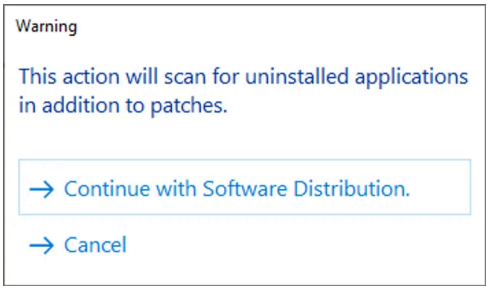
This topic describes how to scan for third-party applications that you want to install on your target machines.

1. From the main menu click **New > Windows Patch > Patch Scan Template**.
   The **Patch Scan Template** dialog appears.
2. In the **Name** box, type a name for this custom scan (for example, Software Distribution Scan).



On the **Software Distribution tab**, enable the **Software distribution** check box.

4. A confirmation dialog will be displayed. This is to ensure that you are enabling the check box on purpose and not inadvertently scanning for and **deploying third-party applications**.



Click **Continue with Software Distribution**.

5. On the **Filtering tab**, specify the operating systems that should be included in the scan.
   The software distribution patches (applications) that will be displayed in the scan results are those that are available for the operating system being used on the scanned machine. For example, if you are scanning Windows 10 and Windows Server 2019

machines, make sure those are enabled within the Microsoft family of products in the **Vendors, Families, and Products** filter on the **Filtering** tab.

6. Click **Save**.
7. Initiate a scan using this new scan template.
8. When the scan is complete, see Deploying Third-Party Applications for information on installing the applications.

194. IAVA Overview

When you purchase the Government Edition of Security Controls you will receive a license key that enables you to use the Information Assurance Vulnerability Alert (IAVA) Reporter. The IAVA-specific files are automatically installed when Security Controls is installed.

The IAVA Reporter provides a cross reference of the existing patch definition file supplied by Ivanti and the IAVA IDs compiled by the U.S. Government. To get the latest version of the patch definition file, select **Help > Refresh files** on the Security Controls console.

See also:

- Creating an IAVA Report
- Performing an IAVA Patch Scan

195. Identifying Effectively Installed Patches

Security Controls can also scan for 'effectively installed patches.' A common case is when you install a single patch that **replaces** other patches. In this circumstance, the patches that were not installed but that have been replaced by the newer patch are considered effectively installed since you have at least the expected file version or greater for each of the files. For example, suppose you install a new Windows machine and then install a patch that replaces 20 earlier patches. While you've only 'installed' one patch, you've effectively installed 20 other patches.

196. Identifying Explicitly Installed Patches

In order to identify that a patch has been explicitly installed, several criteria must be met.

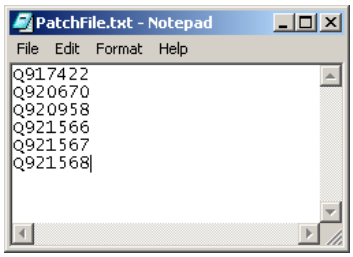
- The patch must include a registry key that gets written to the machine on which it will be installed.
- Some types of patches do not write registry keys to the system on which they're being installed. Since there is no explicit indication that the patch has been applied, it cannot be determined that the patch was specifically installed at any point in time. To ensure that these systems are up to date, run a scan against the system and ensure that there are no patches that appear as 'Patch Missing.'
  If Security Controls deploys the patch, however, it will write its own registry key to the remote system. This data is encrypted to prevent tampering. So, even if the patch doesn't normally write a registry key during deployment (SQL Patches, Office patches, etc), Security Controls will write a registry key that is then read by the scanner during the assessment phase. The application can read that all these patches are installed, what account was used to install the application, and when the patch was installed. This information is displayed on the patch details panel as well as a mouse over on 'Patch Found' text in the patch summary pane. The registry key must exist on the system being scanned.
- All the files in the patch (as defined by the data definition file) that were written to the remote system must be equal to or greater than the file versions recorded in the data file. If any of the file versions on the remote system are below what is expected, the patch is considered not installed even if the registry key is present.

197. Implementing an Unattended Console Configuration

> This scenario assumes all the consoles have Internet access.

On the Distribution Server

Create a text file that contains the list of patches you want each unattended console to scan for and deploy. You manually create the text file and save it on the distribution server. The text file must contain just the QNumbers associated with each patch, one entry per line.

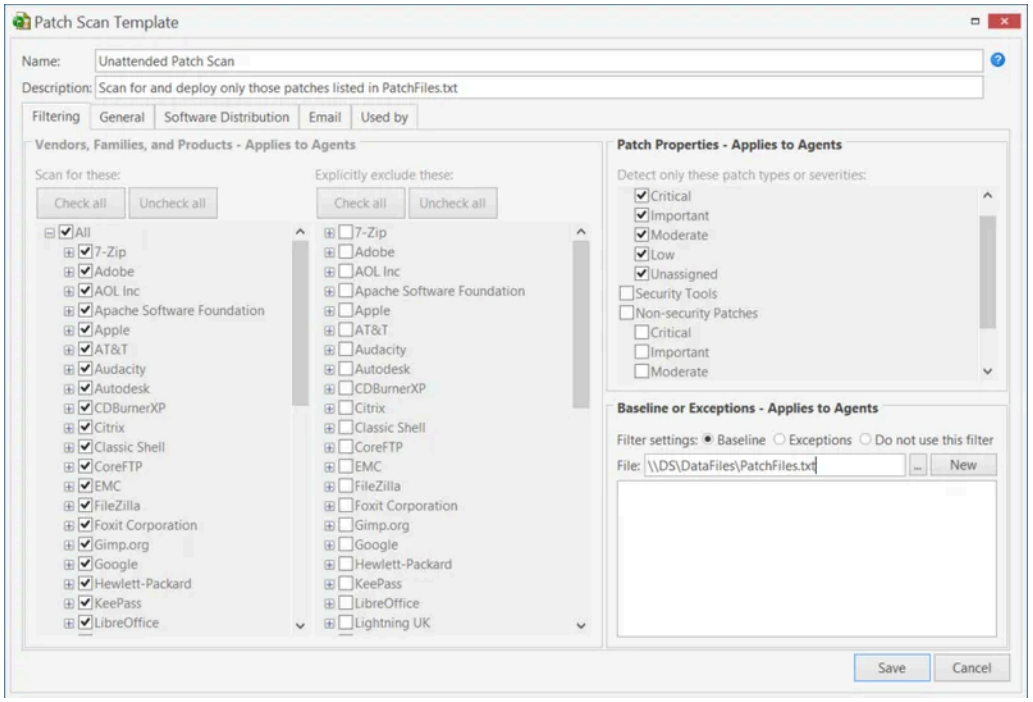


The QNumber is the unique identifier for the patch.

> TIP: You can use **Patch View** to determine the QNumber associated with each patch.

On Each Unattended Console

1. Create a patch scan template that scans for just the patches specified in the custom patch file.
    1. From the main menu select **New > Patch Scan Template**.
    2. Type a name and a description.
    3. On the **Filtering** tab, enable the **Baseline** filter.
    4. In the **File** box, specify the UNC path to the patch text file that is located on your distribution server.



For more detailed information about creating patch scan templates, see **Creating a New Patch Scan Template**.

When you **schedule the periodic patch scans**, make sure you:

- Select the patch scan template you created in Step 1
- Choose to stage the deployment package immediately or at a scheduled time
- Specify what deployment template to use and when the deployment should occur

Ongoing Maintenance

You simply update the patch list on the distribution server as needed. The unattended console will automatically reference the updated list the next time it performs a scan and will deploy the missing patches to each of its managed machines.

198. Implementing a Data Rollup Configuration

Implementing a data rollup console configuration is very easy. You simply perform a few configuration steps on the central console and on each remote console. Implement data rollup only if your remote consoles are each using their own separate database that is also distinct from the one used by your central console.

> If your SQL Server does not run on the same machine as the Security Controls console, you will need to run Security Controls with user credentials that have access to SQL Server. For more detailed information see **SQL Server Notes**.

On the Central Console

1. Select **Tools > Options > Data Rollup**.
2. In the **Data Rollup Receiver Configuration** area, enable the **Accept and import results from a rollup sender** check box.

On Each Remote Console

You must configure each remote console to roll up its results to the central console.

1. Select **Tools > Options > Data Rollup**.
2. In the **Data Rollup Sender Configuration** area, enable the **Enable Data Rollup** check box.
3. Specify the IP address/hostname of the central (rollup) console and the port used by the rollup console to listen for incoming data.
4. In the **Minutes between sending results** box specify how often the data will be rolled up from the remote console to the central console.
5. Click **Register**.

> TIP: The registration process will also automatically generate an entry in the **Edit Console Description** dialog on the central console. You can use this dialog to track how many remote consoles are configured to roll up their results to the central console. See **Editing the Console Description** for more details.

See **Data Rollup Operations** for more detailed configuration information.

199. Importing CVEs

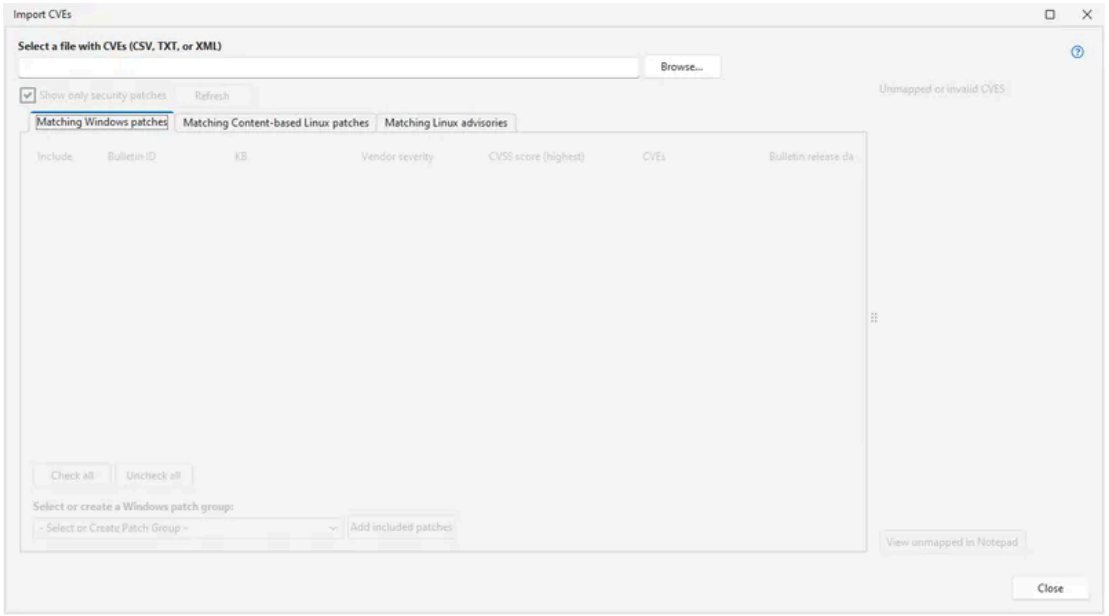
The Common Vulnerabilities and Exposures (CVE) List is a public reference of known cybersecurity vulnerabilities. This list, available from cve.org, continually changes as new vulnerabilities are detected. If your organization uses the CVE list, it can be difficult to determine exactly which patches you need to deploy to protect your machines from the threats identified in the list.

Fortunately, Security Controls simplifies this process. You simply import a list of CVEs from a text file that has typically been produced by your vulnerability scanner. Security Controls will automatically extract the CVEs, determine which patches are related to each CVE and then display those patches for your review. You select which patches to add to a patch group and then use that patch group in your scans and deployments.

You can initiate the import process three different ways:

- Select **Import > CVEs**
- On the home page, click the **Import CVEs into a patch group** link
- While creating or editing a **Windows patch group**

You use the **Import CVEs** dialog to complete the process.



Field	Description
Select a file with CVEs	Use the **Browse** button to locate the file that contains the list of CVEs. The file can be in any valid text file format such as .csv, .txt, .xml, etc. The CVEs will be automatically extracted and the related patches populated in the **Matching Windows patches**, **Matching content-based Linux patches, Matching Linux Advisories** tabs.
Show only security patches	If enabled, shows only security bulletin-related patches. All other patch types are ignored.
Refresh	If you modify the CVE file after it has been initially processed, you can force a refresh by clicking this button. If the file is large, the refresh process (which consists of extracting the CVEs and determining the related patches) may take a few minutes to complete.
Matching Windows patches / Matching content-based Linux patches/ Matching Linux Advisories **Invalid or unmapped CVEs**	These tabs contain all valid CVEs that were detected during the extraction process and that are mapped to at least one patch set. By default, all of the patches populated in these panes will be marked as **Include**. If you want to exclude one or more patches prior to adding them to a patch group, clear their respective check boxes. This pane contains all invalid or unmapped CVEs that were detected during the extraction process. A CVE may be invalid due to an incorrect name. A CVE is considered unmapped if there are no known patches related to the CVE. If you want to export this list to a text file to use as a reference for further investigation, click **View unmapped in Notepad**.
Check all / Uncheck all	Use these two buttons to enable and clear all the check boxes on the selected tab.
Select or create a patch group **Add included patches**	Use this box to specify a patch group that will be used to contain the selected Windows or Linux patches. You can choose an existing patch group or type the name of a new patch group. When you click this button, all patches marked as **Include** in the selected Windows or Linux tab will be added to the specified patch group. **To view the new or updated patch group:** • Windows: In the navigation pane, select **Windows Patch Templates and Groups** and then double-click the group in the **Windows Patch Groups** list. • Content-based Linux: In the navigation pane, select **Linux (Content-Based) Patch Configurations and Groups** and then double-click the group in the **Linux Patch Groups** list. • Contentless Linux: In the navigation pane, select **Linux Patch Configurations and Groups** and then double-click the group in the **Linux Patch Groups** list.

Related Topics

Creating and Editing a Windows Patch Group

Viewing Patch and Asset Summaries

200. Importing User Scripts

Tip: Don't forget to configure the console for use with ITScripts. For information, see ITScripts Options.

Once you've created a script with the required metadata and digital signature, you can import it into Security Controls.

1. Select **Manage > ITScripts**.
   The **Manage IT Scripts** dialog will appear.
2. Click **Import scripts**.
3. Navigate to the signed script file and click **Open**.
   The script will be imported into Security Controls.
4. Select the script in the list and click **Approve**.

This script will now appear along with the approved Ivanti-provided scripts throughout the application.

A console must trust the authority that issued the certificate in order to import or execute the script on that console. If you import user scripts on one console, they will appear on other consoles that are using the same database. However, if the other consoles don't trust the signer, they will not be able to execute the scripts.

201. Initiating and Monitoring a Power Status Scan

You can easily determine the current power state of one or more machines in your organization by performing a power status scan.

Initiating a Power Status Scan

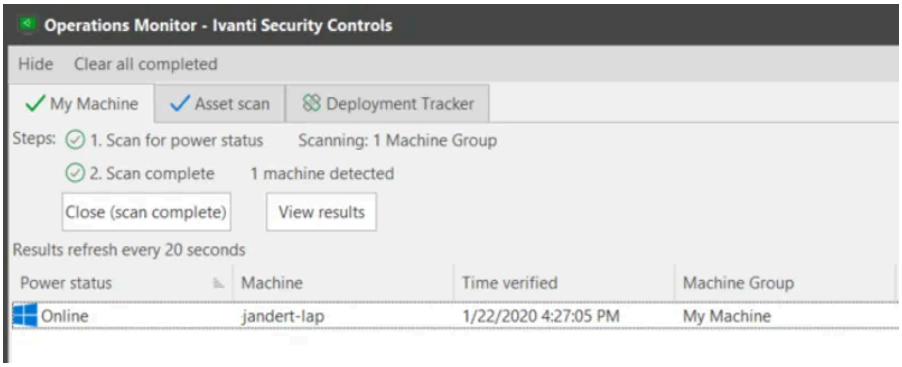
You can initiate a power status scan a number of different ways:

- From the Agentless Operation page by selecting the desired machines, selecting the **Power status** tab and then clicking **Scan now**.
- From Machine View or Scan View by right-clicking the desired machines and then selecting **Power Status scan**.
- From a machine group by clicking **Run Operation**, selecting the **Power status** tab and then clicking **Scan now**.

For more details see How to Initiate Power Management Tasks.

Monitoring a Power Status Scan

In all cases the Operations Monitor will be used to display the status of the power status scan.



When the power status scan is complete you can:

- View the results by clicking **View results**. The Operations Monitor will be closed and the scan results will be displayed. See Viewing Power Status Scan Results for details.
- Remove the current tab by clicking **Close (scan complete)**. Any other tabs on the Operations Monitor will remain open.
- Minimize the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor.
- Remove the current tab and all other tabs by clicking **Clear All Completed**.
- Generate a Power Status report.
- View summary information about each machine that was scanned. Right-click on a column heading and select Column Chooser to add or remove columns from the display.

202. Initiating a Bulletin Deployment to an ESXi Hypervisor

1. In the vCenter Servers list or the ESXi Hypervisors list, select the desired ESXi hypervisor.
2. On the **Bulletins** tab, select the desired bulletin(s).
   You can deploy an individual bulletin, multiple bulletins, or all missing bulletins to a single ESXi hypervisor.
3. Click either **Deploy latest security bulletins** or **Deploy selected bulletins**.
   - **Deploy latest security bulletins:** Initiates the deployment of the latest security patches approved by VMware that are missing on the ESXi hypervisor. This will include only those security bulletins that have not been replaced by newer bulletins.

     > Select Only show latest to see which bulletins will be deployed if you click **Deploy latest security bulletins**.

   Deploy selected bulletins: Initiates the deployment of the selected bulletins.

This will launch the ESXi Hypervisor Deployment dialog, which you will use to configure the deployment.

203. Installing and Supporting Agents on Internet-Based Machines

This section provides a base recommendation for configuring an agent policy that supports machines outside the network environment. This configuration is ideal for laptop users who are frequently disconnected from the network but who are regularly connected to the internet. It is also useful for standalone sites that do not have direct network connectivity but that do have internet access.

In this solution your agents check in and receive policy updates from the cloud. This is accomplished using an Ivanti Security Controls feature called Security Controls Cloud synchronization. It allows you to manage agents on machines that are not able to communicate directly with the console.

See the following topics for background information on Security Controls Cloud Synchronization:

- **Security Controls Cloud Synchronization Overview**
- **Security Controls Cloud Synchronization Requirements and Usage Notes**
- **How to Enable Security Controls Cloud Synchronization**

Agent Installation

There are two primary options for installing agents on machines that are located outside the network environment.

- You can perform a **manual installation** of the agent on each target machine
- You can **install agents via the cloud** using Security Controls Cloud

A manual installation is fine if you only have a small number of machines. If you have a large target base, however, the recommendation is to perform the agent installations via the cloud.

When the process is complete, all of your agents should be able to pull policy updates and roll up results both internally and externally. You can test this by connecting a machine to the internet outside your network, kicking off a scan manually and then watching for the results; repeat this from within your network.

Configuration of the Agent Policy

1. On the main menu select **New > Agent Policy**.
2. Name the policy.
3. Configure options on the **General Settings** tab.
4. You can configure the **Allow the user to** settings as you see fit. The recommendation is to disable **Cancel operations** as most users (if they are aware) will stop a scan whenever they know it is running, preventing the agent from performing its task.
   In the **Check-In interval** area the recommendation is to configure frequent check-ins. This will keep the agent responsive to policy changes in your environment.
   In the **Engine, data, and patch download location** area, **Vendor over Internet** is recommended in this case as the agents are expected to be primarily outside the network. If you are configuring a significant number of agents you may choose to enable **Distribution Server** and **Use vendor as backup source**. Agents will check for the latest engines and XML data file on the distribution server first, and they will use the vendor Web sites if the distribution server is not available.
   In the **Network** area, enable the **Sync with the** Security Controls **Cloud** check box. This specifies that the agent will have the option to use Security Controls Cloud to retrieve the latest agent policy information, enabling it to perform synchronization via the

cloud. This check box is only available if your console is registered with Security Controls Cloud. When you click **Save and deploy to agents**, a copy of the agent policy and all necessary components will be written to the Security Controls Cloud service. **Agent listens for updates on port** can be enabled. If you do, the recommended best security practice is to modify the firewall rules to block the port when outside the network and open the port while inside the network.

On the **Patch** tab, click **Add a Windows Patch Task**, name the task, and configure the task.

5. This policy is intended to focus on securing the target machine, so on the **Scan and deploy options** tab we recommend using **Security Patch Scan** as the patch scan template. You can choose to use a custom template if you wish, but we will stick to the basic security best practice for this example.

   Verify that the **Deploy patches** check box is enabled.

> Choose a deployment template that specifies the following on the Post-deploy Reboot tab:
> - Reboot when needed
> - Scheduled reboot on the next occurrence of specified time
> - Specify a time that is after hours so as not to interrupt the end users work day

You can specify **All patches detected as missing**, which would be the most secure, or you can deploy based on a Patch Group and enable the **Plus all vendor critical patches** check box. This option ensures that even if you have not applied the latest security patches to the patch group, or the agent has not pulled down an updated list, it will still deploy critical security patches released in the latest XML data files.

Enable the **Deploy product levels** check box. You can choose to deploy all product levels that are identified as missing by a scan, or you can limit the deployment to only those product levels you define in a product level group. See Product Level and Patch Deployment Process for more information.

On the **Schedule** tab, choose **Daily** and specify a time that the machine will commonly be on but when network traffic might be lower (like the lunch hour). You can typically specify one day during the work week. If you choose to do a time of day that is outside normal business hours, it is recommended that you enable the **Run on boot if schedule missed** check box to ensure that the assessment occurs even if the last scheduled task was missed.

Click **Save and update Agents**.

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

204. Installing Agents from the Cloud

If you are using **Security Controls Cloud synchronization**, you have the ability to install a Security Controls Agent from the cloud. This is particularly helpful if you have target machines that are away from the corporate network and unable to contact the console.

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Requirements

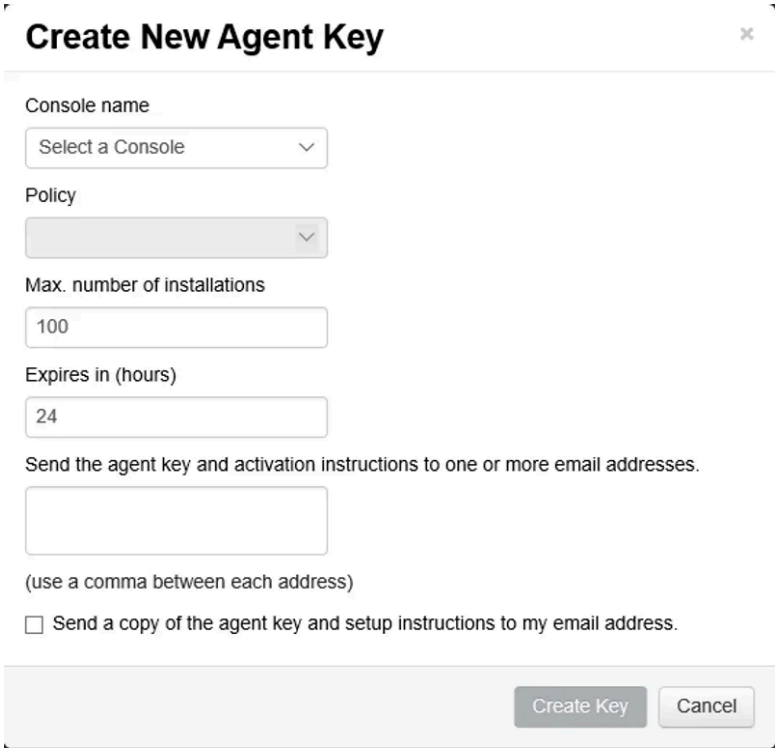
- The target machine must have Internet access
- The Security Controls console must be registered with **Security Controls Cloud**
- Outgoing TCP ports 80 (http) and 443 (https) must be available when communicating with Security Controls Cloud
- The URL *isec.ivanticloud.com* must be accessible when communicating with Security Controls Cloud
- There must be at least one agent policy that is configured to allow **synchronization with Security Controls Cloud**
- You cannot install a cloud-based agent on a Security Controls console machine
- Each user that installs an agent must have administrator access on their target machine

Installation Instructions

> This section describes the web-based method for creating and distributing an agent key. Another option is to **create the key from the Security Controls console**.

From Your Web Browser

1. Go to https://isec.ivanticloud.com and log on to your account.
   If you don't already have an account, click **Register** to quickly setup an account.
2. On the **Registered Consoles** tab, verify that your Security Controls console is registered with Security Controls Cloud.
3. Select the **Agent Keys** tab.
4. Click **New**.
   The **Create New Agent Key** dialog is displayed. Use this dialog to create an activation key that can be used to install one or more agents. You also use this dialog to specify the email addresses of the users you want to receive this key.
5. Provide all necessary information and then click **Create Key**.
   The agent key is created and then emailed to the specified recipients. The email message also contains a web link for downloading the agent installation program and detailed instructions on how to install the agent.



Field	Description
Console Name	Select the Security Controls console that will be used to manage the agent. TIP: If the console does not contain a user-friendly name that has some significance to other users, before proceeding you might consider **changing the name** within Security Controls and then **re-registering the console** with Security Controls Cloud.
Policy	Select the agent policy that you want to assign to the agent. Only those policies that are configured for **synchronization with Security Controls Cloud** will be available for selection.
Max. Number of installations	Specify the maximum number of agent installations you will allow to be performed using this agent key. **Example:** Assume you want to install agents on all of the machines at a remote site. You are not certain how many machines are at the site but you are confident that there are fewer than 10 machines. By specifying a maximum of 10 installations for this key, you are enabling all the machines at the remote site to install agents and yet limiting the number of license seats that can be consumed using this key. You cannot install an unlimited number of agents because the Security Controls console will not allow you to exceed your license count.
Expires in (hours)	Specify how long the key can be used to install new agents. For example, if you know that an administrator will be at a remote site for two days to help with the agent installations, you can specify that the key is only valid for 48 hours. This allows you to control your exposure to other people consuming license seats from the console.
Send the agent key and activation instructions to one or more email addresses	An email message containing the agent key will be sent to each address. Use a comma to separate each address.
Send a copy of the agent key and setup instructions to my email address	If you want to receive a copy of the email message that will be sent to the specified recipients, enable this check box.

On the Target Machine

1. Log on to the target machine using an administrator account.
2. Open the Security Controls Cloud Sync email message that contains the agent key and the installation instructions.

> If you do not have access to the Security Controls Cloud Sync email message but you have a Security Controls Cloud account, you can create your own agent key by opening a web browser on the target machine and then following the instructions shown above in the **From your web browser** section. After the key is created and while you are still logged in to Security Controls Cloud, click the **Download Agent** link that is located to the right of the new key; this enables you to download the agent installation program to the target machine.

Use the instructions to install and register the agent.
You will install the agent, specify that you are connecting to the console through the cloud, paste the activation key, and then click **Register**.

4. Wait for the agent registration process to complete; this may take up to 20 minutes or more to complete.
   The agent will be initially placed into a temporary provisional state while the registration is processed. During this time the Security Controls console will learn about the registration request, verify that enough license seats are available, and provide the Security Controls Cloud service with the necessary files. After the registration process is complete, at the next check-in time the agent will retrieve its assigned agent policy from the cloud and will become a fully-functional agent.

> **Tip:** After the agent checks in with the console, you might consider using the **Assigned Group column in Machine View** to group the agent machine with other machines that share similar attributes, such as physical location or the same agent policy

205. How to Install Security Controls Agent from the Console

> Your Linux target machines must be properly configured before you can perform a push install of an agent. See **System Requirements** for more details.

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

You can use the console to "push install" the Security Controls Agent to connected target machines. In order to perform the push install, each target machine must be online and have an active network connection to the console during the Security Controls Agent installation. This connection is required in order to exchange security information that will be used to establish an encrypted link for all future communication between the console and its agents. The agent machines must also be able to perform name resolution in order to locate the console machine. See **Assigning Aliases to the Console** to see how to add trusted names and IP addresses contained in the certificate that is exchanged between the agent and the console to establish a secure TLS connection.

You must have the proper credentials in order to authenticate to each of the target machines. See **Credential Precedence** for details.

Some target machines may have a firewall enabled that blocks the incoming **ports required** to install Security Controls Agent. On these machines you must manually install Security Controls Agent. See **Manually Installing Agents** for details.

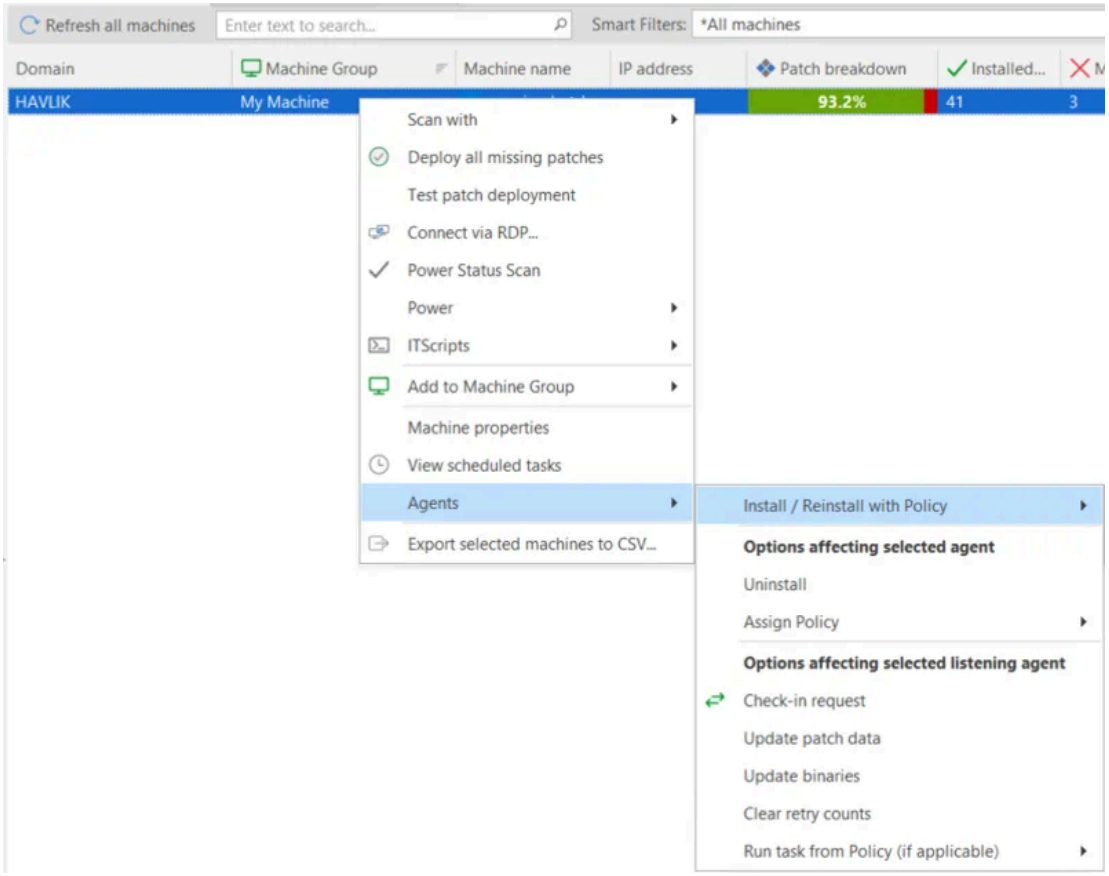
> Installing an agent on a distribution server is a special case that requires the server machine's SYSTEM account to have read access to the distribution server folder. See **Configuring System Account Permissions** for details.

You can perform a push install of the Security Controls Agent service two different ways from the console.

For Machines That Have Been Previously Scanned

You can install agents onto machines that have been previously scanned and that are contained in the program database.

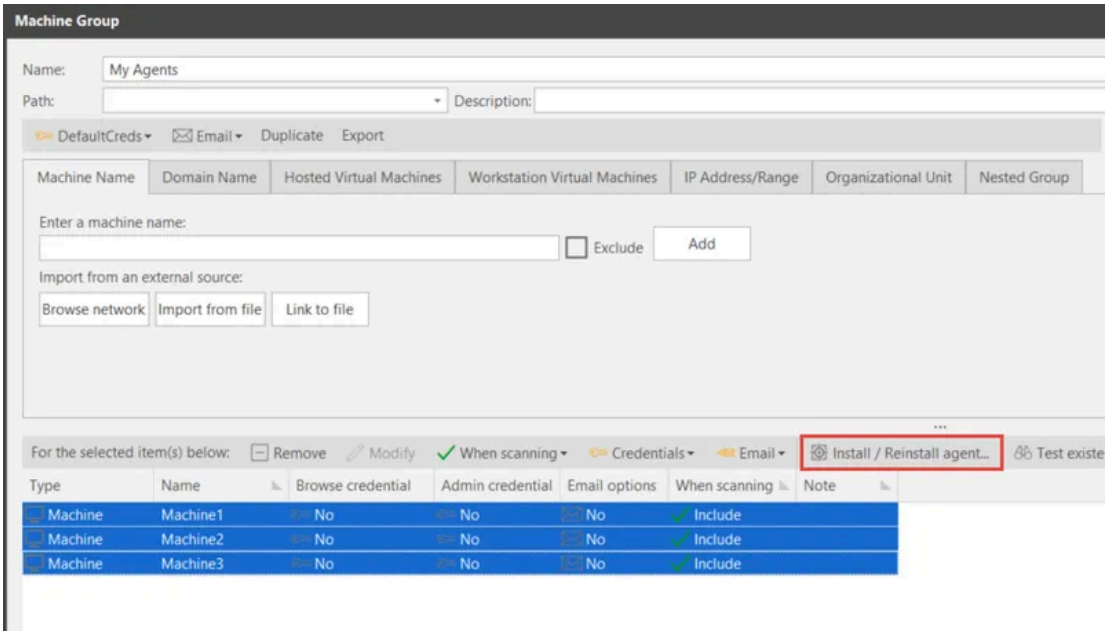
1. Go to either Machine View or Scan View.
2. Right-click the desired machines, select **Agents > Install/Reinstall with Policy** and then select the desired agent policy.



For Machines That Have Not Been Previously Scanned

You can install agents on machines that have not been previously scanned and are therefore not contained in the machine database. You simply create a machine group that contains all the machines that will run a particular agent policy and then use the **Install / Reinstall Agent** button to install an agent policy on those machines.

> There are a couple of caveats:
> - The machines must be added to the machine group using a machine name, domain name, or IP address. You cannot use the **Install / Reinstall Agent** button to install agents on machines that were added as organizational units, nested groups, or IP address ranges.
> - The machines must be online and connected to the network. If the console cannot make a connection to a machine the install will fail for that machine.



> You will be prompted to select the policy you want installed. See **Creating A New Agent Policy** for information on configuring policies.

The following occurs when you push install the Security Controls Agent service to a machine:

- The **Operations Monitor** is displayed and shows the status of the installation request.
- You can verify the installation was successful by doing the following:
  - By using **Machine View** to check the status of the machine. You'll have to wait until the next time the agent machine **checks in** with the console, but once that occurs, the Agent State column should indicate that the machine contains an agent.
  - By using the Service Control Manager on the agent machine to verify that the agent services are running (stDispatch, stAgent).

Once the Security Controls Agent configuration is successfully installed on a target machine, the agent is automatically started on the machine. See **Using Agents on a Target Machine** for information on using the agent.

- After an agent is installed on a machine, that machine becomes a managed machine and can be viewed using **Machine View**.

Related Topics

Preparing to Use Agents

Manually Installing Agents

Installing Agents from the Cloud

206. InstallState view

The Reporting2.InstallState view defines installation states.

Column Name	Data Type	Nullable	Description
Id	int		The install state id.
Value	nvarchar(100)		The string value of the Id
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.InstallState view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[InstallState]
```

ID	Value	Description
-1	Not Recorded	A service pack level detection error has occurred or the product level is an unsupported version.
0	Warning	Indicates a problem with the patch and rarely, if ever, occurs. This value can, however, occur in old patch data.
1	Note	A note exists for this patch. Please reference the QNumber on vendor web sites for more information.
2	Informational	No patches were detected for this product. Either all patches were applied or no patches exist.
3	Installed	A patch is installed.
4	Missing Patch	A missing patch was detected.
5	Missing Product Level	A missing product level was detected.

207. Introduction to Patch Management Best Practices

This section provides recommendations on configuring Security Controls for optimum performance. It also describes the best approach to use for a number of common patch management situations. Many of the following best practices are based on actual customer examples. This information has been compiled by Support and Sales Engineering personnel at Ivanti.

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

208. Introduction to Database Views

This section describes how to use database views within SQL Server database queries to generate custom reports for Ivanti Security Controls.

When you install Ivanti Security Controls it creates a number of defined views in the SecurityControls SQL Server database. You can reference these views within custom queries that you write to extract exactly the information you want. By executing the custom queries and exporting the results to the format of your choice you effectively create your own customized reports for Ivanti Security Controls.

The benefits of writing your own database queries are:

- You can mine the SecurityControls database for the exact information you want.
- You can go beyond the predefined reports provided within Ivanti Security Controls. While the predefined reports are sufficient for many organizations, you may have the need to produce one or more custom reports that provide more specific information about the status of your machines.
  You can export the query results and present the information in the format of your choosing.

You can, of course, opt to write custom queries without using the SecurityControls views. When you add the use of SecurityControls views to your custom queries, however, you gain a number of other benefits:

- Nothing will be removed from view schemas in future versions of Ivanti Security Controls; only additive changes will be made.
- Future versions of Ivanti Security Controls may modify the tables in the database. By referencing SecurityControls views in your queries rather than the tables, you will be guaranteed that your custom queries will not break when upgrading to future versions. The queries are not as complex and are easier to write.
- The views do some of the work for you. Your custom queries will not need to reference as many SecurityControls database tables. The views join multiple tables to gather relevant information and they pull different columns from multiple tables.
  Ivanti will continue to build out the SecurityControls views in future versions, providing greater capabilities.
- Custom queries can be shared by trusted members of the Ivanti community.

The process for creating a custom report is as follows:

1. Familiarize yourself with the SQL Server database views that are provided with Ivanti Security Controls.
2. Write a database query that references the Ivanti Security Controls views and that generates the information you want.
3. Export the query results into the user-friendly format of your choosing.

Related Topics

- Overview of Database Views
- Sample Queries

209. Introducing the Virtual Inventory Feature

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



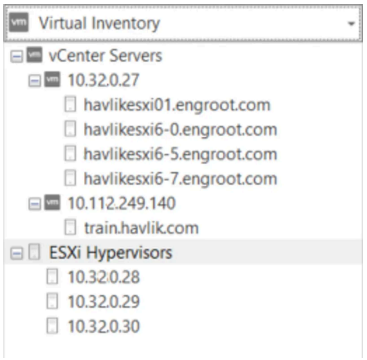
Overview Information

> For information on managing your online and offline virtual machines, see **Roadmap of Tasks for Virtual Machines**.

The Virtual Inventory feature is used to manage and track the vCenter Servers and the ESXi hypervisors (ESXi hosts) that are used in your organization. It may also help you discover virtual machines you didn't even know you had. You can use the Virtual Inventory feature to:

- **Add vCenter Servers and ESXi hypervisors** to Security Controls
- View basic configuration information about the **vCenter Servers** and the **ESXi hypervisors**
- **Perform a scan** of the managed and unmanaged ESXi hypervisors, honoring all of the configured download sources in your vSphere Lifecycle Manager
- View the security bulletins that have already been installed on the **managed** and **unmanaged** ESXi hypervisors
- View the security bulletins that are missing on the **managed** and **unmanaged** ESXi hypervisors
- **Deploy any missing security bulletins** to the ESXi hypervisors
- Upgrade minor versions, such as from 7.0.1 to 7.0.2
- Power on and off the virtual machines that reside on your **managed** and **unmanaged** ESXi hypervisors
- Add the virtual machines and virtual machine templates to a **new or existing machine group**

The vCenter Servers and the ESXi hypervisors that are currently defined to Security Controls can be viewed by selecting **Virtual Inventory** at the top of the navigation pane. The **vCenter Servers** list shows the vCenter Servers you are using and the ESXi hypervisors they are managing. The **ESXi Hypervisors** list shows the hypervisors that are not being managed by a vCenter Server. It is possible for a managed hypervisor to appear in both lists if you import the hypervisor as a standalone device and you also import the vCenter Server that is managing the hypervisor.



210. Explanation: Connecting to Machines Using IP Address vs Fully Qualified Domain Name (FQDN)

For networks that use either NTLM or a basic Kerberos configuration as the authentication protocol, specifying **IP address** as the connection method will typically work just fine. This means that the Security Controls console will connect to clients using the IP address of the machines. This is the default setting.

Some networks, however, operate in stricter environments. They may restrict NTLM, or they may employ the use of additional Kerberos security measures that are implemented using Group Policy. In particular, if the client machines in your environment establish a connection with servers using the Server Message Block (SMB) protocol, a certain level of validation may be required to be performed on the client's Service Principal Name (SPN). If this is the case, you must choose **Fully Qualified Domain Name (FQDN)** as your **connection method**. Doing so will satisfy the additional validation requirements. Connecting using the IP address will not satisfy the SPN validation requirements, and the console will not be able make a connection with your client machines.

> There is one caveat. If you are operating in an NTLM- or SPN-restricted environment and you specify FQDN as your connection method, progress messages will not be displayed when **deploying patches to offline hosted virtual machines**.

Newer versions of Windows are the most likely to employ the stricter security measures. Older versions of Windows machines that do not use the restrictions will be able to operate using the FQDN connection method. So if you have a mix of machines, choose **Fully Qualified Domain Name (FQDN)**.

For more details, see **this article from Microsoft**.

> When in doubt, choose **IP address** and then perform some test scans on your client machines to verify that connections are being made. If the scans fail due to connection errors, choose **Fully Qualified Domain Name (FQDN)** and see if that resolves the problem.

Related Topics

- **Scan Options**
- **Machine Group Dialog: Top Section**
- **Managing Individual Machine Properties**
- **Managing Multiple Machine Properties**

211. ITScripts Requirements

Setup Requirements

For information on configuring the console for use with ITScripts, see **ITScripts Options**.

License Requirements

The following ITScripts features are available to you with a standard license key.

- Access to free scripts created by Ivanti
- Execute scripts against target machines
- Execute scripts from the console
- Create PowerShell Templates
- Access all predefined scripts provided by Ivanti
- Import your own custom scripts
- Import scripts that use custom PowerShell modules
- Execute custom scripts on the console (target type = Console)
- Execute custom scripts on the console against target machines (target type = Any)
- Execute predefined and custom scripts against ESXi Servers and vCenter Servers (target type = ESXi Hypervisor)
- Schedule scripts

Script Requirements

There are two basic requirements for using a script within Security Controls:

- The script must contain metadata that uniquely identifies it and describes its functionality and input parameters
- The script must be signed by an authority that is trusted by the machine that the console is running on

See **Creating a Custom Script** for more information on these and other script requirements.

Console Requirements

- Microsoft .NET Framework 4.6.1 or later
- Windows PowerShell 4.0 or later: Windows PowerShell is a command-line shell and scripting language that is designed for system administration and automation
- Operating System: All operating systems that **support the Security Controls console** will also support PowerShell 4.0

Target Machine Requirements

You do not need to install any additional software on the target machines. Scripts of type **Any** or **Console** are run against the selected target machines or machine groups **without** the services of WinRM (PowerShell remoting). The PowerShell client on the console will communicate with the target machines by using other Windows remoting services such as remote registry service, remote Windows file sharing, WMI services, etc. The actual service used will depend on the script. The only ports required are the ports required by the Windows services being used.

Scripts with a target type of **WinRM Remoting** are slightly different. They are implemented by **creating a custom ITScript** and specifying **remote** as the **metadata type**.

212. Step 2: Let the New Certificate Percolate Through Security Controls

After the new certificate has been issued by your CA and specified as the sub-authority certificate, the certificate is said to be in a pending state. The next step is to let the pending certificate work its way through Security Controls.

30 day waiting period

There is a 30 day period during which the pending certificate will be distributed to your agent machines. Here's how it works:

1. Your agents will check in during this 30 day period.
2. The agents will receive a copy of the new certificate.
3. The certificate will be stored in the Intermediate store on the agent machine.

The agents will not use the pending certificate just yet, but they will have it in their possession for when the transition to the sub-authority certificate is made permanent. The pending certificate is made permanent when the system automatically issues a commit command after 30 days. If problems occur during the 30 day period, you may need to manually perform the commit.

For information about the commit process, see **Commit to the New Sub-Authority Certificate**.

Bypassing the 30 day waiting period

The system will wait for 30 days before it automatically commits to the new sub-authority certificate, and it does this regardless of whether you have any agents. If you do not have agents and you want to commit to the new certificate without waiting the 30 days, you can do so by manually issuing the commit command. For information about the commit process, see **Commit to the New Sub-Authority Certificate**.

There are other reasons you may choose to manually issue the commit command. If you have **forced your agents to check in** and you are certain they have all received the new certificate, you can manually issue the commit command and move forward without waiting for the 30 day waiting period to expire. Or, problems may occur that prevent the commit command from being issued automatically. For more information, see **Commit to the New Sub-Authority Certificate**.

> Be careful when forcing agents to check in. Some agents may not receive the check-in request if they are not listening, are offline or are **cloud agents**.

213. Linking Files to a Machine Group

Security Controls provides a dynamic mechanism for keeping a machine group current. This is especially useful if your machine list changes from time to time and you want an easy way to update it. Linking a file to a machine group is different than importing its contents. Importing contents is a one-time operation after which the information from the file becomes a part of the machine group.

When you link files to a machine group, any changes that you make to the files are reflected upon the next scan. In other words, if you add machines to and delete machines from a linked file between scans, any new machines added to the file will be scanned while any machines removed will not.

When defining a machine group you can link to files containing **machine names**, **domains**, **IP addresses**, and **virtual machines**. The following table describes how to create each particular link file, which you can then use by clicking **Link to file** on the appropriate tab on the Machine Group dialog.

Action	Description
Link Machine File	Provide the name of a file containing machine names. One machine name per line with a carriage return at the end. **Sample:**
Link Domain File	Provide the name of a file containing domain names. One domain name per line with a carriage return at the end. **Sample:**
Link Virtual Machine File	Provide the name of a file containing virtual machines. One virtual machine name per line with a carriage return at the end, or separate each name by a comma. **Sample:**
Link IP Address File	Provide the name of a file containing IP addresses. One IP address per line with a carriage return at the end. You cannot combine individual IP addresses and IP ranges in the same file. **Sample:**
Link IP Range File	Provide the name of a file containing IP ranges. IP ranges in the format of x.x.x.x-y.y.y.y are acceptable. One per line with a carriage return at the end. **Sample:**

Bash

```
dbserver
```

Bash

```
mail
```

Bash

```
dc
```

Bash

```
machine2
```

Bash

```
machine1
```

Bash

```
dmz
```

Bash

```
redmond
```

Bash

```
corp
```

Bash

```
yourcompany
```

Bash

```
example
```

Bash

Bash

```
Z:\VMware Images\WinXP_EN_gold_2\winXPPro.vmx
```

Bash

```
D:\VMware Images\VM-MAF-FR-XPP\winXPPro.vmx, D:\VMware Images\VM-QA-EN-2KS-4\win2000Serv.vmx
```

Bash

```
172.16.1.5
```

Bash

```
10.1.1.10
```

Bash

```
192.168.29.132
```

Bash

```
172.16.2.20-172.16.2.99
```

Bash

```
192.168.29.1-192.168.29.5
```

214. LinuxCompletionCode view

The Reporting2.LinuxCompletionCode view describes the completion codes.

Column Name	Data Type	Nullable	Description
Id	smallint		The completion code id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(256)		Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.LinuxCompletionCode view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[LinuxCompletionCode]
```

215. LinuxDetectedPatchState view

The Reporting2.LinuxDetectedPatchState view defines source types.

Column Name	Data Type	Nullable	Description
Id	int64		The unique identifier.
AssessedMachineStateId	Int		The assessed machine state ID. See [Reporting2].[AssessedMachineState].
LinuxPatchId	int		The Linux patch ID. See [Reporting2].[LinuxPatch].
LinuxInstallStateId	tinyint		The Linux install state ID. See [Reporting2].[LinuxInstallState].
InstalledOn	DateType2	X	The date the patch was installed.

216. LinuxErrorStep view

The Reporting2.LinuxErrorStep view defines source types.

Column Name	Data Type	Nullable	Description
Id	smallint		The error step id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(512)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.SourceType view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[LinuxErrorStep]
```

ID	Value	Description
0	PreInstall	The error occurred prior to installation.
1	PostInstall	The error occurred after the installation.
2	Install	The error occurred during installation.

217. LinuxInstallState view

The Reporting2.LinuxInstallState view describes install state codes.

Column Name	Data Type	Nullable	Description
Id	smallint		The install state id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(256)		Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.SourceType view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[LinuxInstallState]
```

ID	Value	Description
0	Undetermined	Calculation has not been made. Expect to overwrite with one of the values below.
1	Does not apply	Patch does not apply to the product being scanned.
2	Missing	Product was scanned and found to be in need of this patch or one that replaces it.
3	Not missing	Either the file tests of this patch were satisfied, or those of an applicable replacing patch were satisfied. Direct installation evidence was either not found or not evaluated. Legacy "effectively installed".
4	Installed	Either the file tests of this patch were satisfied, or those of an applicable replacing patch were satisfied. Legacy refinement of Not Missing, where direct installation evidence of this patch was found. A.k.a. "explicitly installed".
5	No advisories or packages for product	Result placeholder when there are no applicable patches at all for a product.
6	Note	Detection of this patch was not defined in content. It is merely applicable, not detectable.
7	Error	Scanning conclusion not reachable. Replacement-wise, a patch in this state is calculated as not applicable, although it is reportable.

218. LinuxNotification view

The Reporting2.LinuxNotification view displays information about Linux advisories.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Name	nvarchar(255)		The advisory name.
Posted	Datetime2		The date the advisory was posted.
Revised	Datetime2	X	The date the advisory was revised.
Title	nvarchar(255)	X	The title of the advisory.

219. LinuxPatch view

The Reporting2.LinuxPatch view displays patch information.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Name	nvarchar(255)		The patch name.
LinuxPatchTypeId	tinyint		The Linux patch type ID. See [Reporting2].[LinuxPatchType].
VendorSeverityId	tinyint	X	The vendor severity ID. See {Reporting2].[VendorSeverity].

220. LinuxPatchAppliesTo view

The Reporting2.LinuxPatchAppliesTo view identifies the products and CVEs that a patch applies to.

Column Name	Data Type	Nullable	Description
LinuxPatchId	int		The ID of the Linux patch. See [Reporting2].[LinuxPatch].
LinuxNotificationId	int		The ID of the Linux advisory. See [Reporting2].[LinuxNotfication].
CveId	int	X	The CVE ID. See [Reporting2].[Cve].
LinuxPlatformId	int		The ID of the Linux platform. See [Reporting2].[LinuxPlatform].

221. LinuxPatchDeployment view

The Reporting2.LinuxPatchDeployment view displays patch deployment information.

Column Name	Data Type	Nullable	Description
DeployId	Int		The deployment ID.
LinuxDetectedPatchStateId	Int64		The Linux detected patch state ID. See [Reporting2].[LinuxDetectedPatchState].
InstallEndedOn	Datetime2		The date the install ended.
InstallStartedOn	Datetime2		The date the installation started.
LinuxCompletionCodeId	Int		The completion code. See [Reporting2].[LinuxCompletionCode].
ErrorCode	int	X	The error code for failed instructions.
LinuxErrorStepId	tinyInt	X	The ID of the Linux error step. See [Reporting2].[LinuxErrorStep].

222. LinuxPatchType view

The Reporting2.LinuxPatchType view describes patch type codes.

Column Name	Data Type	Nullable	Description
Id	smallint		The Linux patch type id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(512)		Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.SourceType view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[LinuxPatchType]
```

ID	Value	Description
0	None	None
1	Security	Security patch
2	Bug	Bug patch
3	Enhancement	Enhancement patch

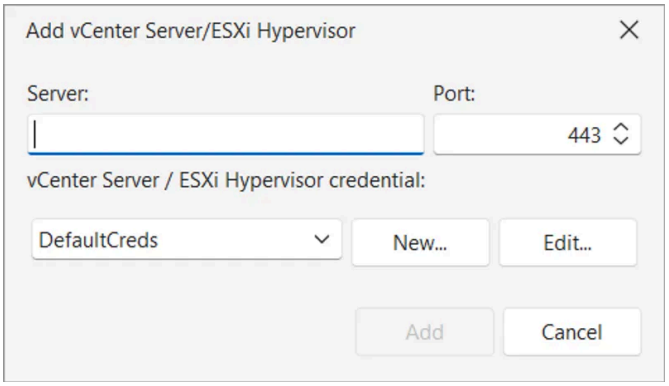
223. LinuxPlatform view

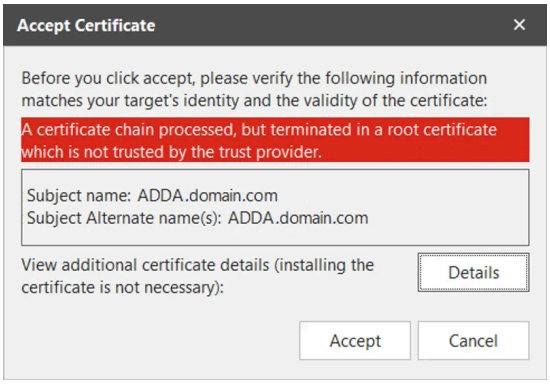
The Reporting2.LinuxPlatform view identifies the Linux platform.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Name	nvarchar(255)		The platform name.
LinuxDistributionId	int		The Linux distribution ID.
ArchitectureId	tinyint		The architecture ID. See [Reporting2].[Architecture].
Edition	nvarchar(100)		The edition.

224. Logging on to an ESX or Virtual Infrastructure Server

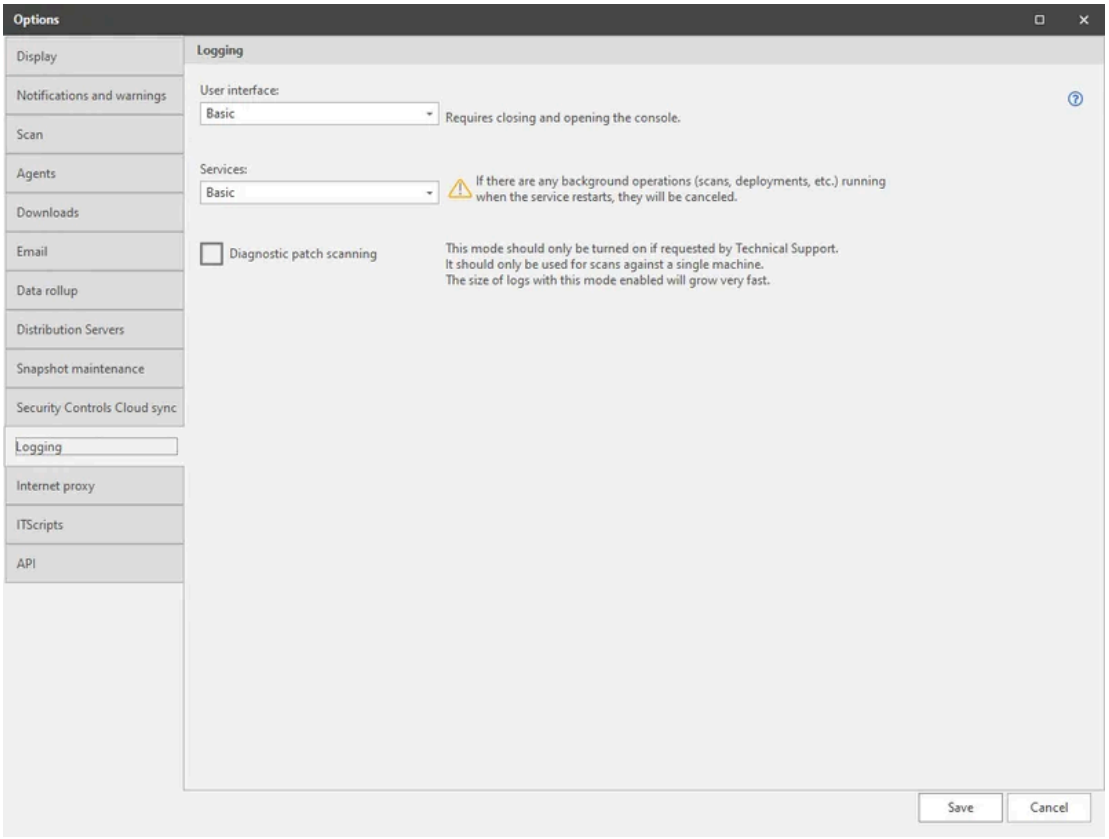
When you click **Add** or **Edit** on the **Hosted Virtual Machines** tab the **Add vCenter Server/ESXi Hypervisor** dialog is displayed.



Field	Description
Server **Port**	Type the full path name or IP address of the vCenter Server or ESXi Hypervisor that you want to add to Security Controls. The port number used when making a connection to the vCenter Server or ESXi Hypervisor. The default value is 443.
vCenter Server / ESXi Hypervisor credential	Select a credential that has access to the vCenter Server or ESXi Hypervisor, or click **New** to define a new credential. For more information, see Defining Credentials.
Add	After you have specified all necessary information, click **Add**. If you have not previously connected to this virtual server, a prompt is displayed asking you to verify the server's certificate.  To review the certificate information, click **Details**. If you are satisfied that you are connecting to the correct virtual server, click **Accept**. The server's certificate thumbprint will be stored and you will not have to repeat this verification process the next time you initiate a connection to this server. After a connection is made, the program will search for all ESXi Hypervisors being managed by the vCenter Server and for all virtual machines hosted on the ESXi Hypervisor(s) and use that information to populate the table.

225. Logging Options

The **Logging Options** dialog allows you to specify how much data you want the program to record in the program logs.



Field	Description
Logging levels	Specify how much data you want the program to record in the program logs. You can specify different recording levels for user interface activity and for background services activity. For each category the options are: • **All:** Records all events in the log, including *Start*, *Stop*, *Suspend*, *Transfer*, and *Resume* events. • **Basic:** Records *Critical*, *Error*, *Warning*, and *Information* events in the log. This is the default value.
Diagnostic patch scanning **Log file locations**	If enabled, captures a large amount of diagnostic data in order to troubleshoot patch scanning issues. IMPORTANT! Do not enable this check box unless directed by Technical Support. The logs are located in the following directory on the console: `C:\ProgramData\Ivanti\Security Controls\Logs` Several of the log files will include the administrator's name as part of the file name. This is especially useful when two or more administrators have access to the program.

Debug Logging

Super admins have the option to enable or disable the P2Z engine debug logs using command line. The super admin must establish an SSH connection to the agent machine and execute the following commands with super user privileges.

- To enable the debug logs use command on the terminal: `touch /opt/ivanti/isec/data/agentPatchP2Z_EnableDebugLog`
- To disable the debug logs use command on the terminal: `rm -f /opt/ivanti/isec/data/agentPatchP2Z_EnableDebugLog`

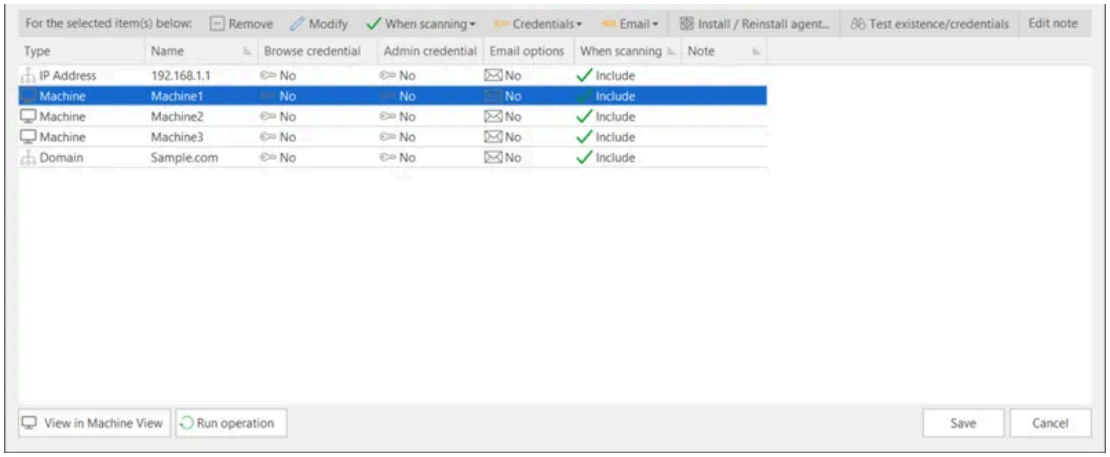
226. Machine view

The Reporting2.Machine view displays currently known information about a machine that has been assessed.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
DnsName	nvarchar(255)	X	The DNS name of this machine.
Domain	nvarchar(255)	X	The domain name of this machine.
Language	int	X	The language used on this machine.
Name	nvarchar(255)	X	The netbios name of this machine.
OperatingSystemFamilyId	int		The ID of the operating system family. See [Reporting2].[OperatingSystemFamily].
ArchitectureId	int		The ID of the architecture. See [Reporting2].[Architecture].
Distribution	nvarchar(100)	X	The distribution.
LinuxPlatformId	int	X	The Linux platform ID. See [Reporting2].[Product].
ProductId	int	X	The product id. See **[Reporting2].[Product]**.
LastKnownIP	nvarchar(45)	X	The IP address of this machine. This will be displayed in IPV4 or IPV6 format.
LastPatchAssessedOn	datetime	X	The time this machine was last assessed upon. (This is the date the machine was scanned, not the date of the patch scan scheduled).
LastAssessedMachineStateId	int	X	The id of the last assessed machine state. See [Reporting2].[AssessedMachineState].
LastPatchMachineGroupName	Nvarchar(255)	X	The name of the machine group where this machine was defined.
AssignedGroup	nvarchar(255)		The name of the group the machine is assigned to within Machine View and Scan View.
VirtualInventoryPath	nvarchar(260)	X	The virtual inventory path.
VirtualServerName	nvarchar(256)	X	The virtual server name.

227. Machine Group Dialog: Bottom Section

When **viewing a machine group**, the bottom section of the machine group dialog displays the machines that are currently members of the group. The bottom section also enables you to perform actions on individual machines within the group.



The bottom section contains the following items and capabilities:

- Machine-level buttons: Buttons that perform actions on individual machines within the group.

> These actions can also be performed by right-clicking on one or more machines.

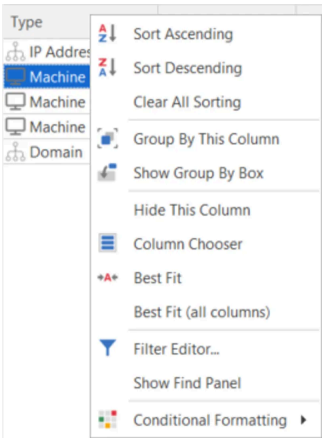
Action	Description
Remove	Removes the selected machines from the current machine group.
Modify	Enables you to modify the name or IP address of an existing group item. The item is displayed in the middle pane, allowing you to modify the name and then add the item back to the group using the new name.
When Scanning	**Include:** The selected machines will be included when scans are performed on this machine group. **Exclude:** The selected machines will be excluded when scans are performed on this machine group.
Credentials	- **Set Admin Credentials:** The ability to provide administrative credentials for the selected machines in the group. Credentials assigned to individual machines will take precedence over credentials assigned to the group. When credentials are applied to the selected machines, the name of the assigned credential is displayed next to the icon. - **Set Browse Credentials:** Applies only to domains and organizational units. Enables you to provide browse credentials that are used to locate all machines in a specific domain or OU. These credentials may be different than the administrator credentials used to connect to the machines in the domain or OU. When credentials are applied, the name of the assigned credential is displayed next to the icon. - **Remove:** Removes specified credentials from the selected machines. The credentials icon will become dimmed ( ). Any group-specific credentials will still be applied to the machines. For more information on setting credentials see **Defining Credentials**.
Email	**Set email:** Defines email options for the selected machines. Defining email options for individual machines overrides any email options defined for the group. The email options enable you to define which reports (if any) will be automatically sent— and to whom they will be sent— whenever the machines are used in a scan. To specify which reports should be automatically sent and to whom they should be sent: 1. In the **Automated Email Settings** dialog, select a report in the **Reports** list. 2. In the **Report Recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Close**. **Remove email:** Removes all email settings currently applied to the selected machines.
Install/Reinstall Agent	Installs Security Controls Agent on the selected machines. • The machines must be added to the machine group using a machine name, domain name, or IP address. You cannot use the **Install / Reinstall Agent** button to install agents on machines that were added as organizational units, nested groups, or IP address ranges. • The machines must be online and connected to the network. If the console cannot make a connection to a machine the install will fail for that machine. See **Installing Agents from the Console** for more details.
Test existence/ credentials	Performs a **power status scan** to verify the existence of the selected machines and to verify that the credentials defined for the selected machines can be used to access the machines.
Edit note	Enables you to add a note to one or more machines in the group. For example, you might use a note to indicate why a certain machine is being excluded from scans that are performed on the group.

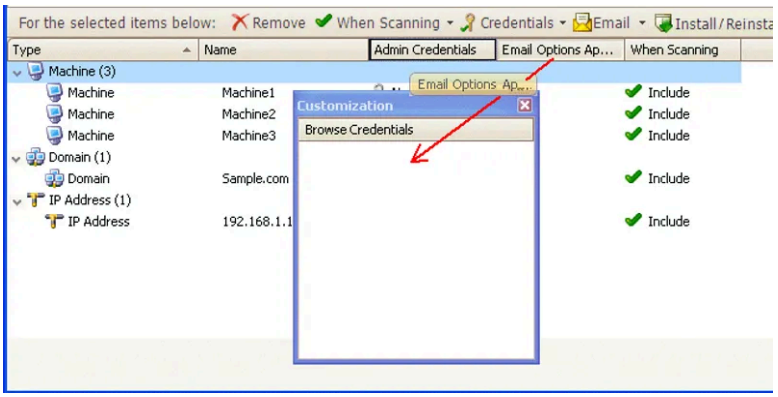
Action	Description
	• To edit an existing note: Select the note, click **Edit note**, and modify the text. • To remove an existing note: Select the note, click **Edit note**, and replace the text with a space.
SSH connection	Enables you to change the SSH connection setting. For more information, see the **SSH Authentication** topic.

- The ability to display the machines in the group a number of different ways.
  - You can click on a column heading to sort the table by that information.
  - You can reorder the columns by clicking and dragging the column headers to new locations. For example, if you want administrator credential information to be displayed in the first column, simply click on the **Admin Credentials** column header and drag it to the first column.

    > When reordering columns, the column header you are moving will always be placed in front of the column you drag it to.

You can right-click within a column header and perform a number of additional actions.



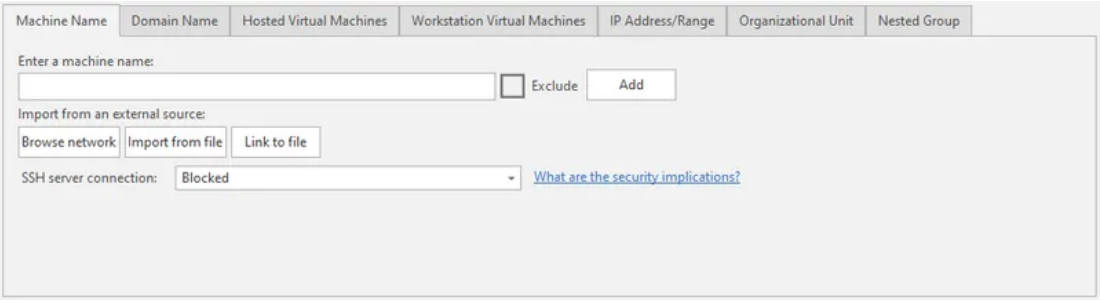
Action	Description
Sort Ascending	Sorts the selected column in ascending order.
Sort Descending	Sorts the selected column in descending order.
Clear All Sorting	Clears the sorting criteria currently set for this column.
Group By This Column	Groups the table using the data in the selected column. It does this by moving the data into expandable lists that are located in the body of the grid. One expandable list will be created for each possible column value. If you perform this action on any subsequent columns, that data will be presented as nested groups at increasingly lower levels within the expandable lists. If **Show Group By Box** is enabled, this will also create a "Group By" box in the area immediately above the column headers. TIP: To turn off the **Group By This Column** feature and revert to the original view: Enable **Show Group By Box**, drag the Group By boxes back to the column header and then right-click in the column header and select **Hide Group By Box**.
Show Group By Box / Hide Group By Box	Displays or hides an area immediately above the column headers that contains "Group By" boxes. One Group By box will be displayed for each column header for which **Group By This Column** is currently enabled. You can also drag column headers to and from this area. The table will be grouped according to the data in the box. If there are two or more boxes then the grouping will be nested, with the left-most box presented at the highest level, the second box presented at the second level, etc.
Hide This Column	Removes the column from the table. You can add the column back to the table using the **Column Chooser**
Column Chooser	Enables you to add and remove information from the table. When you select **Column Chooser** the **Customization** dialog is displayed. This dialog is used to store the columns you currently don't want displayed within the table. Simply click and drag the desired column headers from the table to the **Customization** dialog. For example, if you decide you don't want **Browse Credentials Applied** and **Email Options Applied** information displayed in the table, simply drag those column headers into the **Customization** dialog. 

Action	Description
	If you decide you want an item back in the table, simply click and drag it from the **Customization** dialog back to the table.
Best Fit	Resize the width of the selected column so that all information in the column is displayed in the optimal amount of space.
Best Fit (all columns)	Resize the width of all columns in the table so that information in the columns is displayed in the optimal amount of space.
File Editor	The **Filter Editor** dialog will show any filters that are currently active in the column headers. You can use the editor to modify the existing filter criteria and to build new criteria using the available filter conditions and logical operators.
Show Find Panel / Hide Find Panel	Displays or hides a search box that you can use to find specific patches or text related to any of the patches contained in the patch data file. Here are a few tips for using the search box: • The search works only on the information currently visible in the grid • All partial matches are displayed • The use of wildcards is not allowed
Conditional Formatting	Enables you to apply additional formatting to the table.

- **View in Machine View:** Displays this group in Machine View, which shows the most recent scan information for every machine in the group.
- **Run operation** button: Enables you to initiate an operation (a patch scan, a power management task, etc.) on all machines in the machine group.

228. Machine Group Dialog: Middle Section

When viewing a machine group, the middle section of the machine group dialog enables you to add machines to the group.

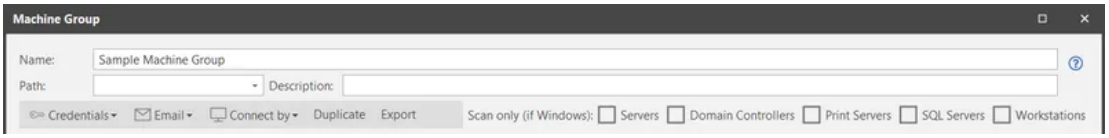


You can add machines a number of different ways. See the following topics for details:

- Adding Machines by Name
- Adding Domains
- Adding Virtual Machines
- Adding Machines by IP Address
- Adding Organizational Units or Active Directory Security Groups
- Defining Nested Groups

229. Machine Group Dialog: Top Section

When viewing a machine group, the top section of the machine group dialog contains buttons, links, and filters that apply to the entire group.



This section contains the following items:

- **Name:** Provide a descriptive name for the new machine group.
- **Path:** If you want to add the group to a new or existing folder in the navigation pane, type a folder path into the **Path** box; see Organizing Machine Groups for more information.
- **Description:** Provide a description that identifies the purpose of the group.
- There are several buttons that apply to the group as a whole.

Action	Description
Credentials	Enables you to select one of the following options: • **Set credentials:** Enables you to assign common credentials to every machine in the group. Be sure the credential you select includes the domain name when defining the user name (for example: SampleDomain\Sample.Name). • When credentials are assigned, the button name will change to the name of the assigned credential. For more information see **Defining Credentials**. **Remove credentials:** Enables you to remove any credentials defined for the group. When credentials are not defined the icon will be dimmed ( ).
Email	Defines email options for the entire group. The email options enable you to define which reports (if any) will be automatically sent— and to whom they will be sent— whenever this group is used in a scan. To specify which reports should be automatically sent and to whom they should be sent: 1. Click **Email > Set email**. 2. In the **Automated Email Settings** dialog, select a report in the **Reports** list. 3. In the **Report recipients** list, select the groups and/or individuals you want to email the report to. 4. Repeat Step 2 and Step 3 for each report you want to be automatically sent. 5. When finished, click **Close**.
Connect by	Specifies the method to use when connecting to your client machines. There are three options: • **IP address:** The console will connect to clients using the IP address of the machines. This is the default setting. • **Fully qualified domain name (FQDN):** You may need this method if Kerberos authentication is used in your environment, and if Service Principal Name (SPN) validation is required for Server Message Block (SMB) endpoint connections. • **Use console-wide setting:** The option specified on the **Tools > Options > Scan dialog** will be used. This is the default setting. For more detailed information, see **IP Address vs FQDN**. This setting can be overridden at the **machine level** for scans that are initiated from Machine View or Scan View.
Duplicate	Copies the current machine group to a new group. Type a name for the new group and then click **OK**.
Export	TIP: To import an existing machine group, select **New > Import Machine Group**. Enables you to export the group definition to an encrypted XML file. This file can be imported into another machine group on the same console or on a different console. You will be asked to supply a passphrase when exporting a group file. This is done to secure the contents of the file and prevent an unauthorized person from learning about

Action	Description
	your network topology, from discovering your machine credentials, etc.
	Displays online Help information about machine groups.

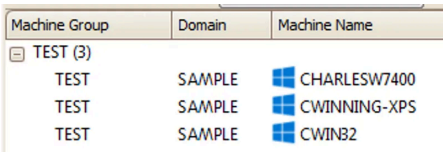
- **Scan only**: There are a variety of filters that can be applied to the machines in this group.

  Filters enable you to specify the types of machines you want included in a scan. For example, if you want to scan all the print servers within a domain, you would specify the desired domain on the **Domain Name** tab and then in the **Scan only** area you would select **Print Servers**. All other machine types are ignored.

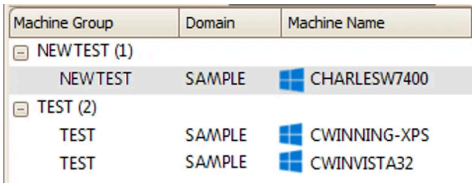
  To specify one or more machine types, simply enable the check box in front of the machine type(s) you want included in the scan. If no check boxes are enabled then no filters are applied.

230. Machine Group Information is Dynamic

The machine group information that is displayed is based on the machine group used to perform the most recent action on each machine. So it is possible for the machine group information to change. For example, if you perform a scan of a group containing three machines, the information displayed will be similar to the following:



If you then re-scan the first machine from a different machine group, the refreshed display will reflect this change:

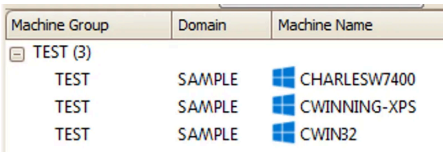


The first machine is no longer listed with its original group because the most recent scan of the machine was initiated from a different machine group.

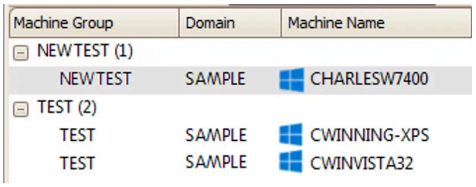
When agents check in with the console they will be listed with the machine group from which they were last scanned from the console.

231. Machine Group Information is Dynamic

The machine group information that is displayed is based on the machine group used to perform the most recent action on each machine. So it is possible for the machine group information to change. For example, if you perform a scan of a group containing three machines, the information displayed will be similar to the following:



If you then re-scan the first machine from a different machine group, the refreshed display will reflect this change:



The first machine is no longer listed with its original group because the most recent scan of the machine was initiated from a different machine group.

When agents check in with the console they will be listed with the machine group from which they were last scanned from the console.

232. Machine View Top Pane Summary

The grid in the top pane contains detailed information about every machine in your network that has been scanned and whose information resides in the database. Click on a column heading to sort the grid by that information. Right-click on a column heading and select **Column Chooser** to add or remove columns from the display.

The refresh icon () refreshes all machine information in the top pane. The latest information for all machines is retrieved and newly scanned machines may appear.

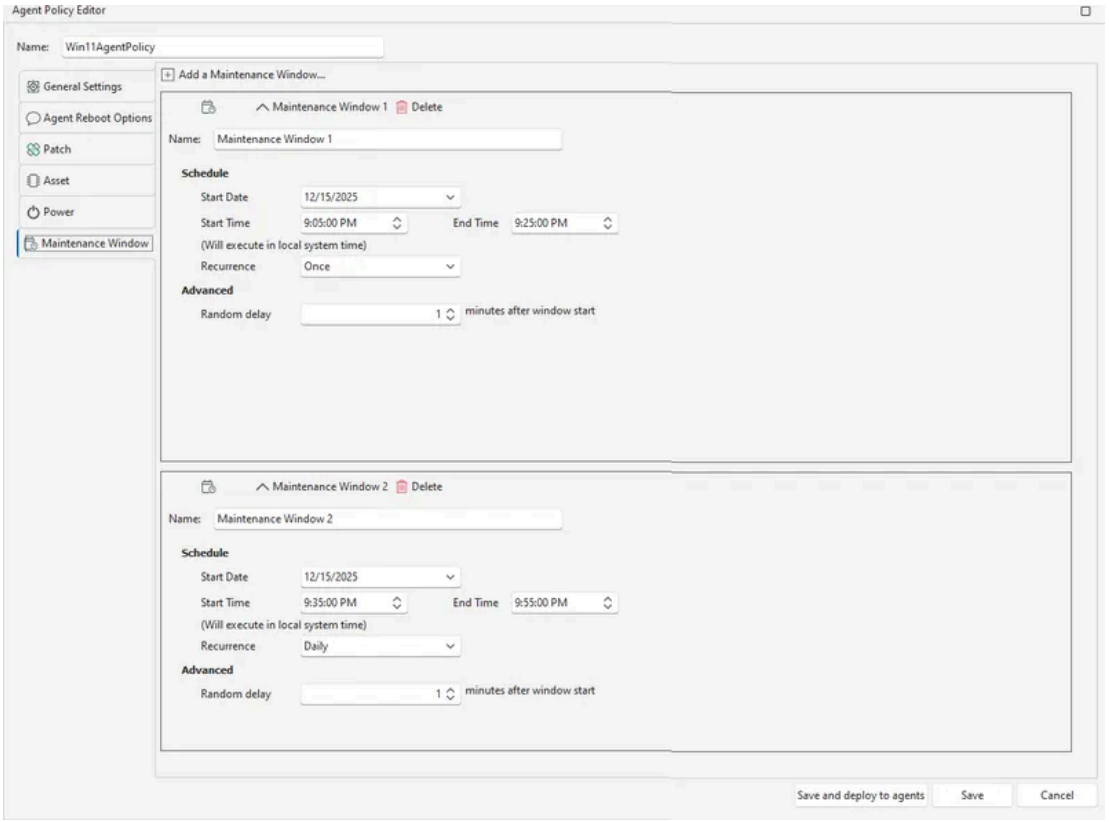
Field	Description
Last scanned group	The machine group the machine belonged to at the time of the most recent scan. Because a machine can change machine groups or be in multiple machine groups, the name is dynamic.
Assigned group	The group to which this machine is assigned within Machine View and Scan View. An assigned group is not the same as a machine group. An assigned group is only used within Machine View and Scan View. This column is used for organizational purposes within Machine View and Scan View. For example, machines that share similar attributes such as physical location or the same agent policy might be assigned to the same group. The group assignment is preserved regardless of whether the **Last Scanned Group** value changes. For this reason, the **Assigned Group** column is often used within Machine View to sort, filter and search for specific assigned groups and then perform actions on the machines in those groups. This column is particularly useful with machines such as Cloud agents, as they do not belong to a machine group and will not be automatically assigned to a group. Machines can be assigned to a group a number of different ways. • The default group is the machine group name and it will be applied during agentless operations such as patch scans, asset scans and power status scans, or a push installation of an agent from a machine group. • You can manually assign machines to a group using the **Machine Properties** dialogs. For information on how to manually assign machines to a group, see Managing Individual Machine Properties and Managing Multiple Machine Properties. • Agent machines can be assigned to a group during deployments initiated from the REST API. • Agent machines can be assigned to a group if the agent activation key is created from the console machine or from the cloudsync function in the REST API. The assigned group information becomes a part of the agent key and is automatically included when you specify the ACTIVATIONKEY in an agent manual installation script or some other deployment tool.
Domain	The domain of the scanned machine.
DNS Hostname	The DNS host name of the machine in the network. This column is hidden by default.
Machine name	The name of the machine. The associated icon indicates whether the computer is a physical or online virtual Windows machine (), a Linux machine (), an offline virtual machine (), or a virtual machine template ().
IP address	The IP address of the scanned machine.
Health	A visual representation of the percentage of installed patches (green) vs. missing patches (red).
Installed patches	The total number of patches found on the scanned machine.
Missing patches	The total number of patches missing on the scanned machine.

Field	Description
Missing product levels	(Windows only) The total number of product levels missing on the scanned machine.
EOL products	The number of software products on the machine that have been designated as at End-of-Life by their vendor.
OS type	The type of operating system used on this machine.
OS language	The locale of the machine operating system (e.g., en-US).
OS	The operating system being used on the scanned machine. If the operating system is shown in red it indicates that it has reached its end-of-life (EOL) phase and the vendor will limit support for the product.
Agent state	The current state of the agent installed on the machine. If an agent is not installed the **No Agent** icon is displayed.
Assigned agent policy	The name of the agent policy currently assigned to the scanned machine.
Last agent check In	Shows the last time the agent checked in with the console.
Agent version	The version number of the agent currently installed on this machine.
Virtual server	(Windows only) The name of the server that is hosting the virtual machine. This column does not apply to physical machines.
VM name	(Windows only) The name of the virtual machine. This column does not apply to physical machines.
VM inventory path	The full path name of the hosted virtual machine. This column does not apply to physical machines.
Latest patch scan date	Shows the last time a patch scan was performed on the scanned machine.
Assigned credential name	The credentials currently assigned to this machine.

Field	Description
Console	The console that most recently managed this machine.
Asset definition	The version of the Asset Definition data used in the last asset scan of this machine.
Last asset scan template	The Asset Scan Template used in the latest asset scan of this machine.
Last patch scan template	The Patch Scan Template used in the latest patch scan of this machine.
Latest asset scan date	The date of the most recent asset scan of this machine.
Patch definition	The version of the Patch Definition data used in the last patch scan of this machine.
Reported agent policy	This applies only to agent machines. This is the agent policy last reported by the agent. It may differ from the Assigned Agent Policy if a new policy has been assigned but the agent has not checked in since the assignment was made.
Using latest policy	Specifies if the machine is using the latest agent policy. If it is not, it may because a new policy has been assigned but the agent has not checked in to receive the latest policy.
RDP port	The port on this machine that is used to make a Remote Desktop connection.
Machine criticality	The criticality assigned to this machine in the Manage Machine Properties dialog. Right-click one or more machines and select **Machine Properties** to edit this value.
Custom 1 **Custom 3**	These columns display text entered in the **Custom** tab of the Manage Machine Properties dialog. Right-click one or more machines and select **Machine Properties** to edit these values.

233. Maintenance Window

The Maintenance Windows feature allows organizations to define specific time periods for performing planned maintenance activities, such as patching or configuration changes. The feature helps to avoid disruptions during critical times, reducing risk and maintaining stability in production environments.



You can define one or more Maintenance Windows (MWs) to control timing of the rolled out updates. When an update is available, the Agent checks if it is within the timespan of MW and updates it. If the updates do not fall within the time span of MW, it waits until the next MW.

You configure maintenance windows tasks on the **Maintenance Window** tab. You can edit an existing maintenance window, or you can create a new task by clicking **Add a Maintenance Window**.

To create a Maintenance window:

1. On the Agent policy Editor, click **Maintenance Window** tab and **Add a Maintenance Window**.
   The **Maintenance Window** screen appears.
2. Enter a name for the maintenance window in the **Name** field.
3. Perform the following to set the schedule:
   - **Start Date**: The system selects the current date by default. To change it, type a new date or click the date list to pick one from the calendar.
   - **Start Time**: Select the time to begin the maintenance window.
   - **End Time**: Select the time to end the maintenance window.
   - Choose how often you want the maintenance task to run. By default, it is set to **Once**, meaning the task runs only once at the scheduled date and time. If you select **Recurrence**, the system runs the maintenance window on a repeating schedule for up

to five years from the chosen **Start Date**.

- **Daily** - The task runs on the **Start date**, then the next task runs everyday at the time you set in the MW.
- **Weekly** - Select the day(s) of the week on which you want to run the maintenance window at the scheduled time.
- **Monthly** -
  - **On day** – Choose the exact day of the month for the maintenance window. For example: If you select Day 10 the maintenance runs on 10th of every month.
  - **On the** – Choose a specific week and weekday, plus an optional offset in days. For example: If you select On the 2nd Tuesday, and set an offset of 1 day, the maintenance runs on the Wednesday following the 2nd Tuesday of each selected month.

- **Advanced**: You can set the **Random delay** of number of minutes. This adds a specified minutes of delay after the scheduled maintenance window starts. This may be useful in distributing the tasks or events to avoid simultaneous start.

4. Click **Save** or **Save and deploy to Agents**.

After you add the maintenance window, you can edit or delete it. The maintenance window is saved only when you save the **Policy**.

The agent follows these rules when installing updates:

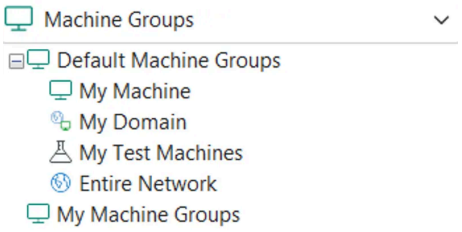
- If a maintenance window is not defined in the policy, updates and installations run immediately.
- If updates have been deferred for more than 72 hours, the agent overrides the maintenance window and starts the update process. This action may prompt users to restart their devices outside the scheduled window.
- If the device is within the defined maintenance window, updates and installations run as scheduled.
- If the policy is changed, the agent installs new engines immediately, regardless of any maintenance window.
- If an update is triggered by a reboot task, new engines are installed whether or not a maintenance window is set.

This behavior helps to ensure devices are updated in a timely manner. Users might receive prompts to restart during daytime hours if updates have been previously deferred for three or more days, or if there has been a policy change.

234. Using the Navigation Pane

The following program features are available using either the selection box located at the top of the navigation pane or the shortcut buttons located along the side.

Machine Groups



Machine groups are used to define the machines you want included in a particular scan. Many actions within the program are performed using machine groups. The Machine Groups list contains the following:

- **My Machine:** A default group consisting of only the console machine.
- **My Domain:** A default group consisting of the machines in the local domain.
- My Test Machines: A default group that is initially empty. You should add machines to this group that represent a 'smaller' view of your actual network environment and use the group to perform tests.
- **Entire Network:** A default group consisting of all machines visible on the network.
- **My Machine Groups:** Contains a list of your custom machine groups. To create a custom machine group, select **New > Machine Group**.

Agent Policies and Product Level Groups



The **Agent Policies and Product Level Groups** list contains two types of items.

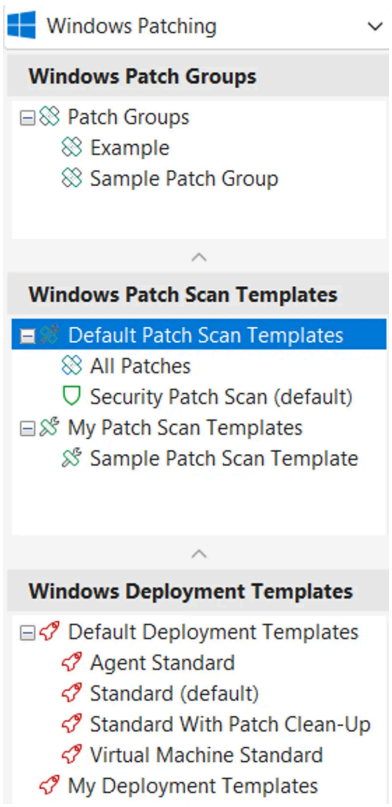
- An agent policy defines exactly what an agent can and cannot do. With Security Controls Agent you can create as many different agent policies as is needed. A policy can be used to scan for missing patches, to determine software and hardware assets, and to perform power state tasks. To create a new agent policy, select **New > Agent Policy**.
- A product level group is a collection of product levels that you wish to deploy using agents. Product level groups can represent required or mandatory product levels that have been approved for your organization. To create a new group, select **New > Product Level Group**.

Favorites



A favorite is a collection of machines to scan and a choice of how to scan them. To create a new favorite, select **New > Favorite**. Select the machine groups you want to scan and then select the desired scan template.

Windows Patching

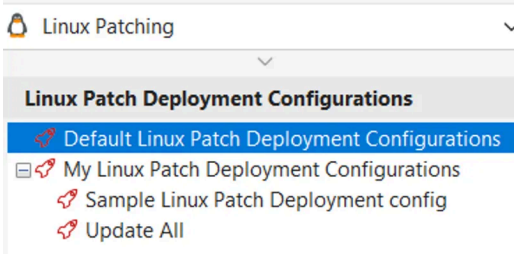


The **Windows Patching** list contains three types of items.

- A patch group is a collection of patches that you wish to scan for and/or deploy. Patch groups can represent required or mandatory patches that have been approved for your organization. To create a new group, select **New > Windows Patch > Patch Group**.
- A patch scan template defines exactly how a patch scan will be performed. The available patch scan templates are:
  - **Security Patch Scan:** Scans for missing and installed security patches.
  - **All Patches:** Scans for both security patches and non-security patches.
    To create your own custom patch scan template, select **New > Windows Patch > Patch Scan Template**.

A deployment template provides a way to save desired settings for patch deployment and have them quickly available for future deployments. To view the settings for the three default templates, click **Agent Standard**, **Standard**, or **Virtual Machine Standard**. To create a new template, select **New > Windows Patch > Deployment Template**.

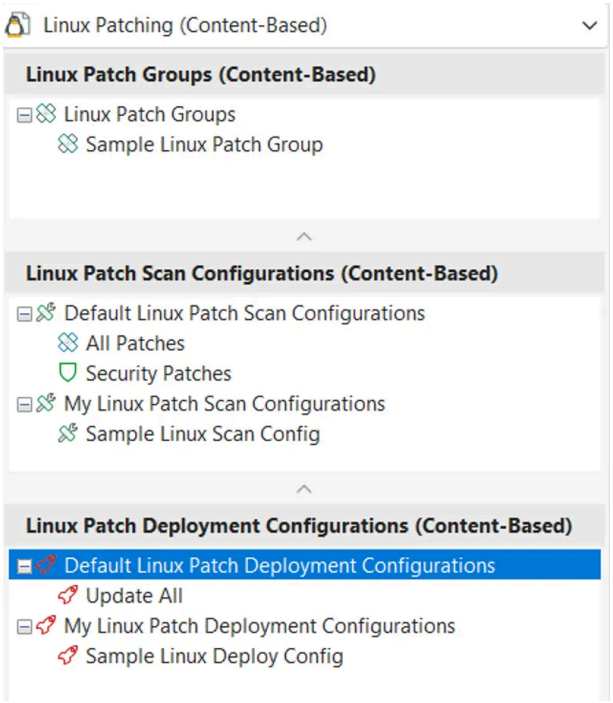
Linux Patching



The **Linux Patching** list relates to the contentless Linux patching method.

- A Linux patch deployment configuration defines how an agent will perform a patch deployment. Whenever a Linux Patch Task runs, it runs a scan for all missing packages and advisories. The predefined configuration, named **Update All**, specifies that an agent will deploy all missing patches. To create your own custom deployment configuration, select **New > Linux Patch > Patch Deployment Configuration**.

Linux Patching (Content-Based)

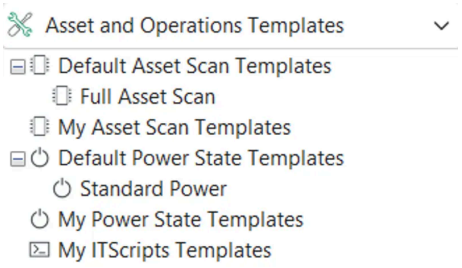


The **Linux Patching (Content-Based)** list contains three types of items, relating to the content-based Linux patching of earlier releases.

- A patch group is a collection of patches that you wish to scan for and/or deploy. To create a new group, select **New > Linux Patch (Content-Based) > Patch Group (Content-Based)**.
- A Linux patch scan configuration defines how an agent will perform a patch scan. The predefined configurations are:
  - **All Patches:** Specifies that the agent will scan for all patch types. A patch group will not be used.
  - **Security Patches:** Specifies that the agent will scan only for security patches. A patch group will not be used.
    To create your own custom patch scan configuration, select **New > Linux Patch (Content-Based) > Patch Scan Configuration (Content-Based)**.

A Linux patch deployment configuration defines how an agent will perform a patch deployment. The predefined configuration, named **Update All**, specifies that an agent will deploy all missing patches. To create your own **custom deployment configuration**, select **New > Linux Patch (Content-Based) > Patch Deployment Configuration (Content-Based)**.

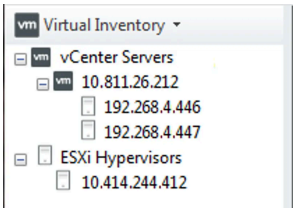
Asset and Operations Templates



The **Asset and Operations Templates** list supports the use of a number of different types of templates.

- An asset scan template defines exactly how an **asset scan** will be performed. The default asset scan template is configured to perform a software and hardware scan.
  You can also create your own unique asset scan template by selecting **New > Asset Scan Template**.
- A power state template defines what **power management** tasks should be performed. The default power state template is named **Standard Power** and is configured to initiate a restart of the selected machines. It enables a logged on user to extend the reboot in one minute increments up to 10 minutes.
  You can also create your own unique power state template by clicking **New > Power State Template**.
- An ITScripts template specifies which script to execute and what parameter values and mode to use when executing the script.
  You can create an ITScripts template by clicking **New > ITScripts Template**.

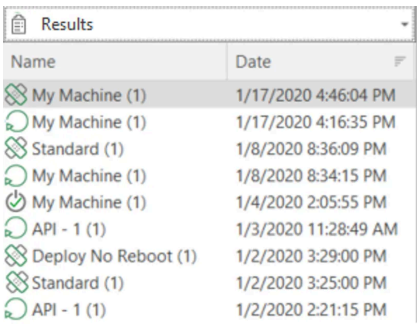
Virtual Inventory



The Virtual Inventory list is used to manage and track the vCenter Servers and the ESXi hosts that are used in your organization. You can use the Virtual Inventory feature to:

- **Add vCenter Servers and ESXi hosts** to Security Controls
- View basic configuration information about the **vCenter Servers** and the **ESXi hosts**
- **Perform a patch scan** of the managed and unmanaged ESXi hosts
- View the security bulletins that have already been installed on the **managed** and **unmanaged** ESXi hosts
- View the security bulletins that are missing on the **managed** and **unmanaged** ESXi hosts
- **Deploy the patches** associated with each missing security bulletin
- Power on and off the virtual machines that reside on your **managed** and **unmanaged** ESXi hosts
- Add the virtual machines and virtual machine templates to a **new or existing machine group**

Results



A history of the **patch scans**, **patch deployments**, and **power status scans** that you have performed is available in the **Results** list. The number of days' worth of items displayed in the **Results** list is configured using **Tools > Options > Display**.

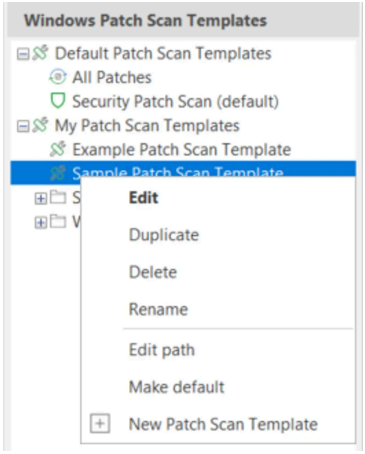
To view the results of a scan or deployment, select the desired item. Detailed information about scans will be presented in **Scan View** and detailed information about deployments will be presented in **Deployment Tracker**.

You can right-click on an item to either delete it from the list or to rename it. Here's a quicker method for deleting many items at once from any of these lists:

1. Select **Manage > Database maintenance**.
2. On the summary screen that appears select the items you want to delete.
3. Click **Delete Selected**.

235. Managing a Patch Scan Template

Custom patch scan templates are contained in the **Windows Patch Scan Templates** list in the navigation pane. You can edit an existing template by clicking the template name. You can also right-click a template and perform a number of different actions.



Action	Description
Edit	Enables you to edit the selected template.
Duplicate	Enables you to create a new template by using the existing template as a base. The name of the new template will be 'Duplicate of { selected template name }'. Change the name and the other template characteristics as desired.
Delete	Deletes the current template. You cannot delete a template that is currently being used by an **agent policy**.
Rename	Enables you to change the name of the patch scan template. Be careful if you rename a template that is currently being used by an agent policy.
Edit path	Enables you to change which **folder** the template resides in within the navigation pane.
Make default	Sets the selected patch template as the default template.
New Patch Scan Template	Enables you to create a new custom **patch scan template**.

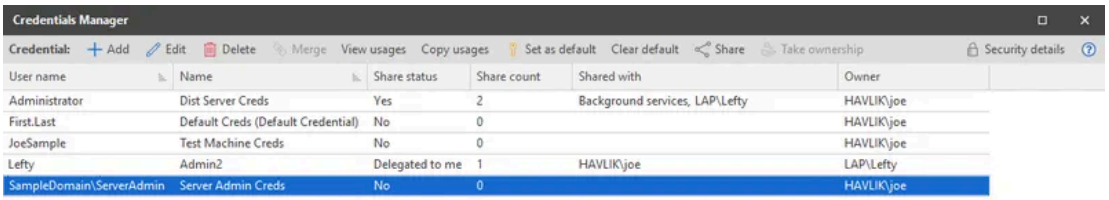
236. Managing Credentials

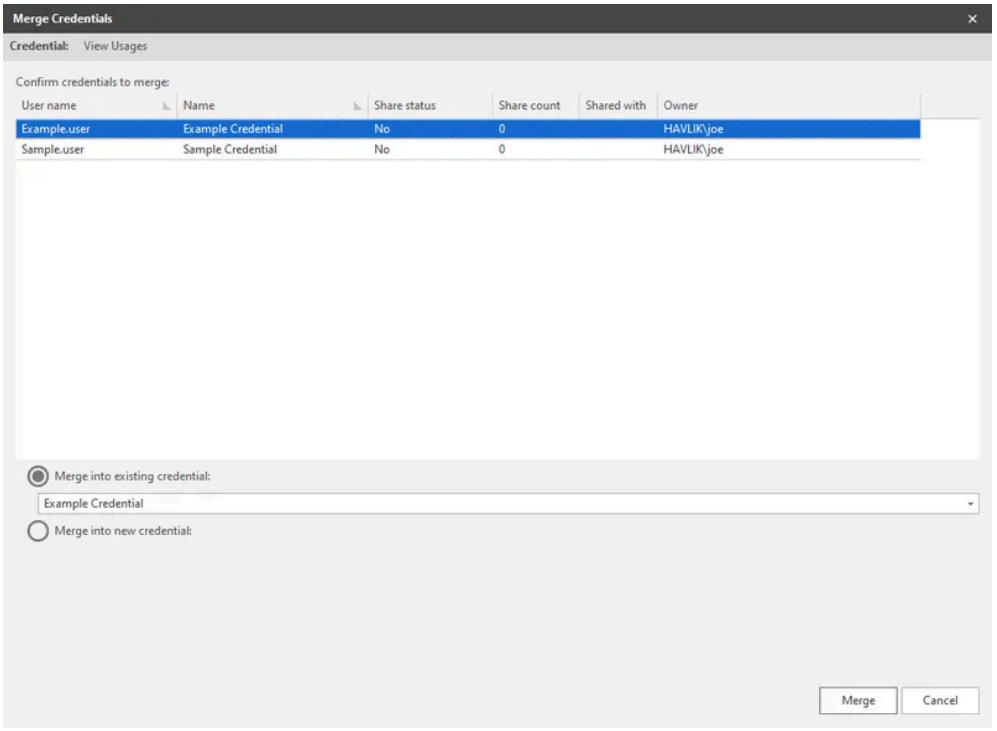
IMPORTANT! If there are two or more administrators using Security Controls, you will likely want to use **shared credentials**. If you choose not to use shared credentials, each administrator will need to provide their own machine credentials. For details, see **Potential Issues When Using Multiple Admins**.

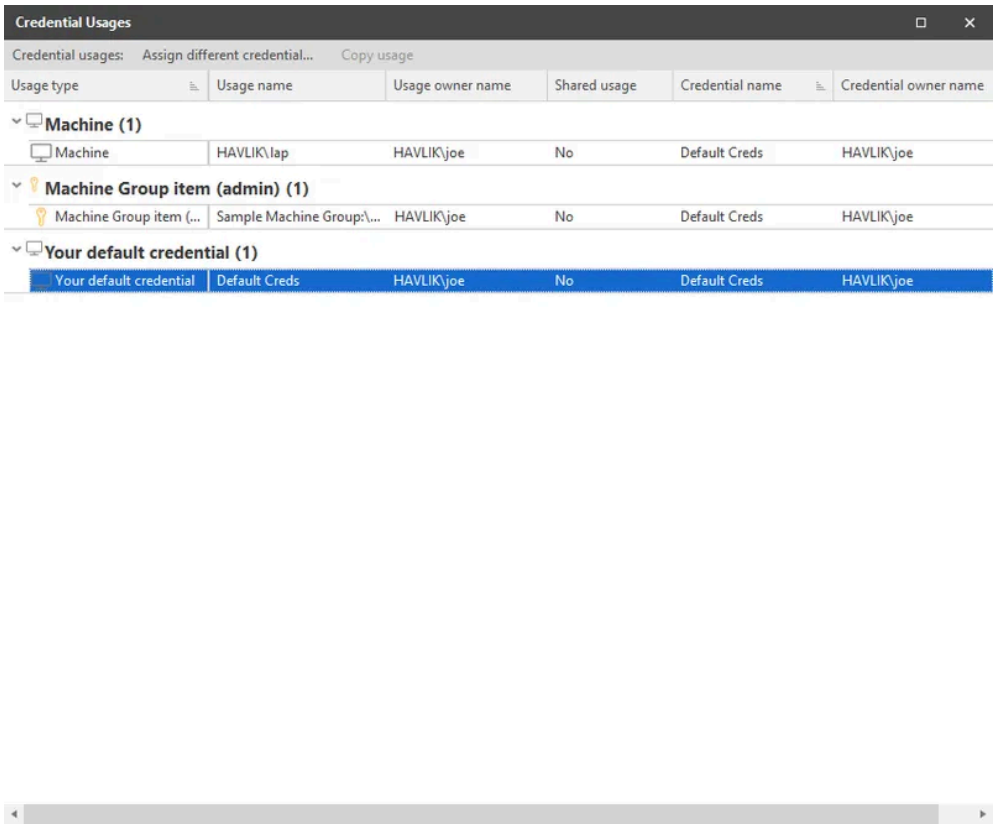
The Credentials Manager is used to manage all credentials used within the program. It is also used to set the default credential for the program.

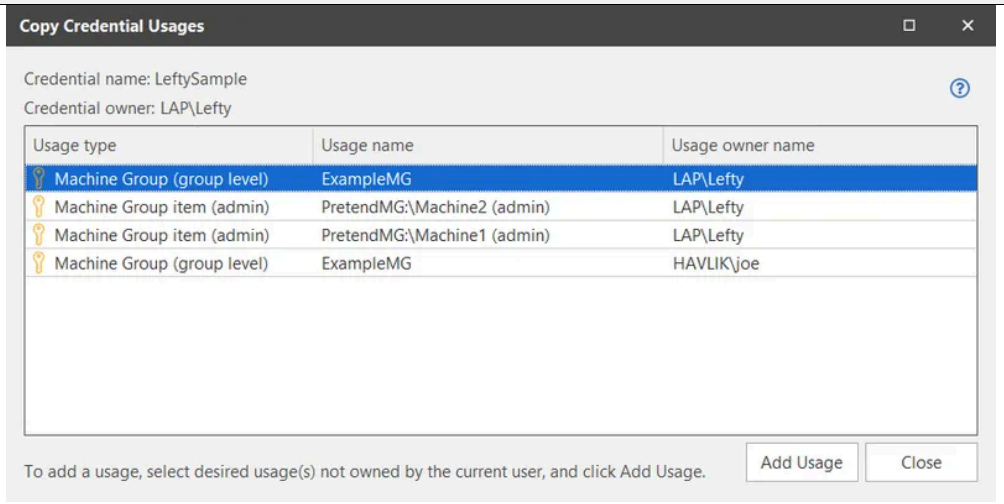
Although you can **supply new credentials** from several different areas of the program, all of the credentials can be edited and deleted from this single location. This greatly simplifies the credentials management process. For example, if a password that is used to authenticate a specific group of machines changes, you simply use the Credentials Manager to update the associated credential. All items assigned to that credential are automatically updated with the new password.

To manage the credentials used by the program, select **Manage > Credentials**.



Field	Description
Add	Enables you to add a new credential. See **Defining Credentials** for details.
Edit	Enables you to modify the selected credential. See **Defining Credentials** for details.
Delete	Deletes the selected credential. You can delete multiple credentials at the same time. When you delete a credential the following occurs: • The credential itself is deleted • All usages of the credential throughout the program are deleted • If it is a shared credential, the shared credential and all its usages are deleted CAUTION! Any items using the deleted credential will no longer be assigned a credential. Before you delete a credential, you should use the **View usages** button to verify the credential is not being used.
Merge	Enables you to merge two or more credentials that contain the same user name and password. Or, you can merge several different credentials into one new credential that is effective in all situations. By eliminating duplicate and unneeded credentials, you reduce confusion and lessen the chance for human error. The resulting credential will automatically be applied to every area of the program that currently uses any of the credentials that are being merged (see **View usages**). 1. On the **Credentials Manager** dialog, select the credentials you want to merge together. Credentials that are **shared with you** cannot be merged. 2. Click **Merge**. The **Merge Credentials** dialog is displayed.  At the bottom of the dialog, select one of the following: ◦ **Merge into existing credential:** The credentials specified in the **Confirm credentials to merge** list will be merged with the credential that you choose here.

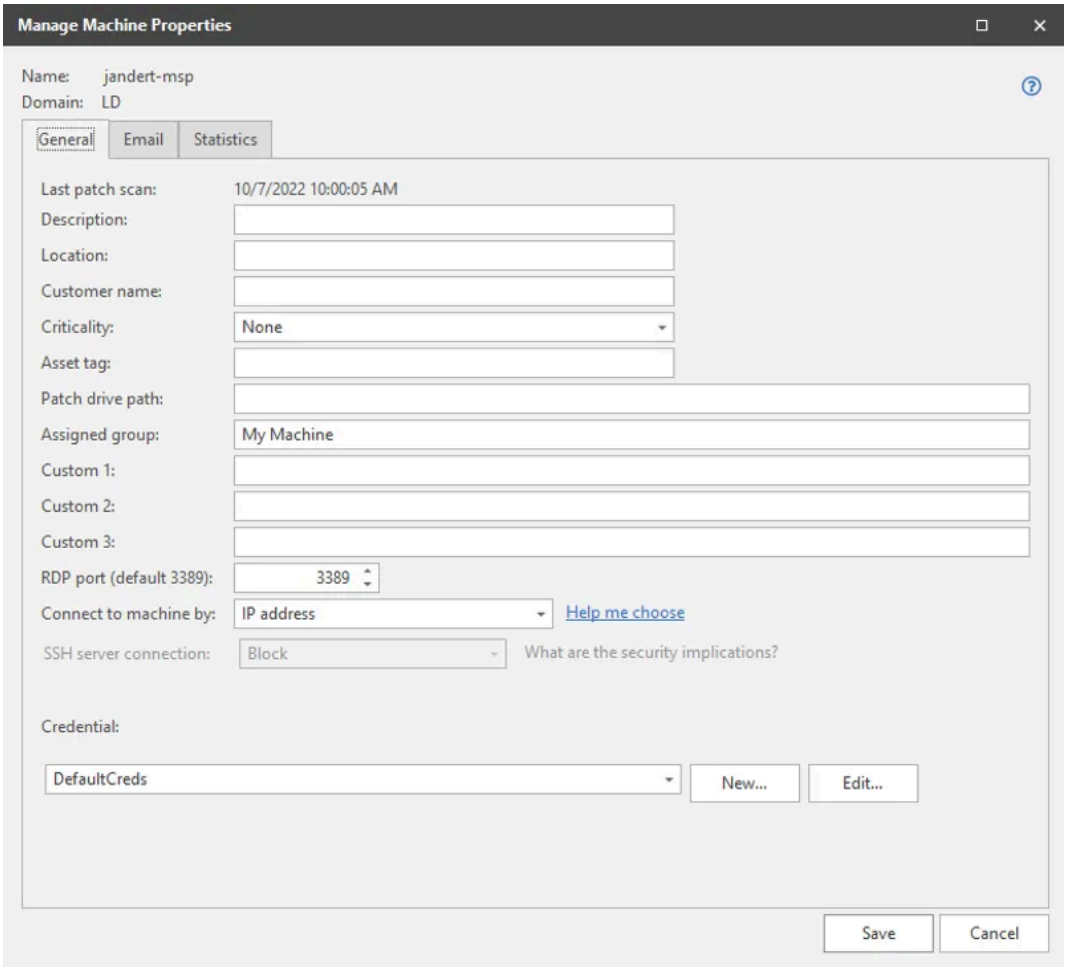
Field	Description
	◦ **Merge into new credential:** The credentials specified in the **Confirm credentials to merge** list will be merged into a new credential that you create here. For security purposes, the resulting credential will not be shared with other users even if the merged credentials were being shared. If you want to share the new credential, see Shared Credentials. Click **Merge**. 5. Read the message on the confirmation dialog and if you agree with the merger, click **Merge**.
View usages	Enables you to see how and where the selected credentials are being used in the program. Only those credentials that are currently being used in the program will be displayed in the **Credential Usages** dialog. A credential may be listed multiple times if it is used in different areas of the program.  **Assign different credential:** Enables you to assign a different credential to the selected item(s). You can assign a different credential to multiple items at once but only if they all have the same **Shared Usage** value (Yes or No). **Copy usage:** Enables you to propagate to your user account any usage that is owned by another user. You can also right-click on any list item and perform a number of additional actions. • **Expand all:** Expands all lists. • **Collapse all:** Collapses all lists. • **Export selected credential usages to CSV:** Export information about the selected items to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.
Copy usages	Enables you to see where a shared credential is being used within the program, and by whom. You can then add any usage that is not already being used by your user account. You might do this if the credential owner, or another user who is sharing this credential, has added one or more new usages and you want to keep in sync with those users. You might also do this if usages were never copied to you when the credential owner initially shared the credentials with you.

Field	Description
	 Select the usages that you want and then click **Add Usage**. When you are finished, click **Close**. You can verify the usage assignments using the **View usages** button.
Set as default	Assigns the selected credential as the default credential. The program will use the default credential if other credentials are missing or invalid. See **Credential Precedence** for information on when the default credential is used.
Clear default	Removes the default credential assignment.
Share	Enables you to **share the selected credential** with other users and with background services. It also enables you to modify existing shared settings. This button is only available if you are the owner of the credential.
Take ownership	Allows you to assume control of a credential that is being **shared with you and/or background services**. You might do this if you need to make changes to the credential and the original owner is not available to make the changes.
Security details	See **Potential Security Implications When Sharing Credentials**.
User name	Displays the user name portion of each credential.
Name	Displays the unique name assigned to each credential.
Share	Displays whether the credentials are **shared credentials**. Possible values are: • **Yes:** Indicates that the credential is being shared with other users and/or with **background services**.

Field	Description
status	• **No:** Indicates that the credential is not being shared. Only the owner may use this credential. • **Delegated to me:** Indicates that the owner of the credential has shared the credential with you. • **Background services only:** Indicates that the credential is being shared with **background services** and possibly with other users, but not with you.
Share count	Displays the number of users with whom the credential is shared. If the credential is **shared with background services**, that counts as one user.
Shared with	Displays the names of the users who have the ability to use this credential. If this credential is also **shared with background tasks**, the term **Background services** will be displayed.
Owner	Displays the name of the user who owns the credential. Only an owner can modify or share a specific credential.

237. Managing Individual Machine Properties

The **Manage Machine Properties** dialog is accessed from within Machine View or Scan View by double-clicking a machine or by right-clicking the desired machine and then selecting **Machine properties**. The dialog contains several tabs that enable you to define many different properties for an individual machine.

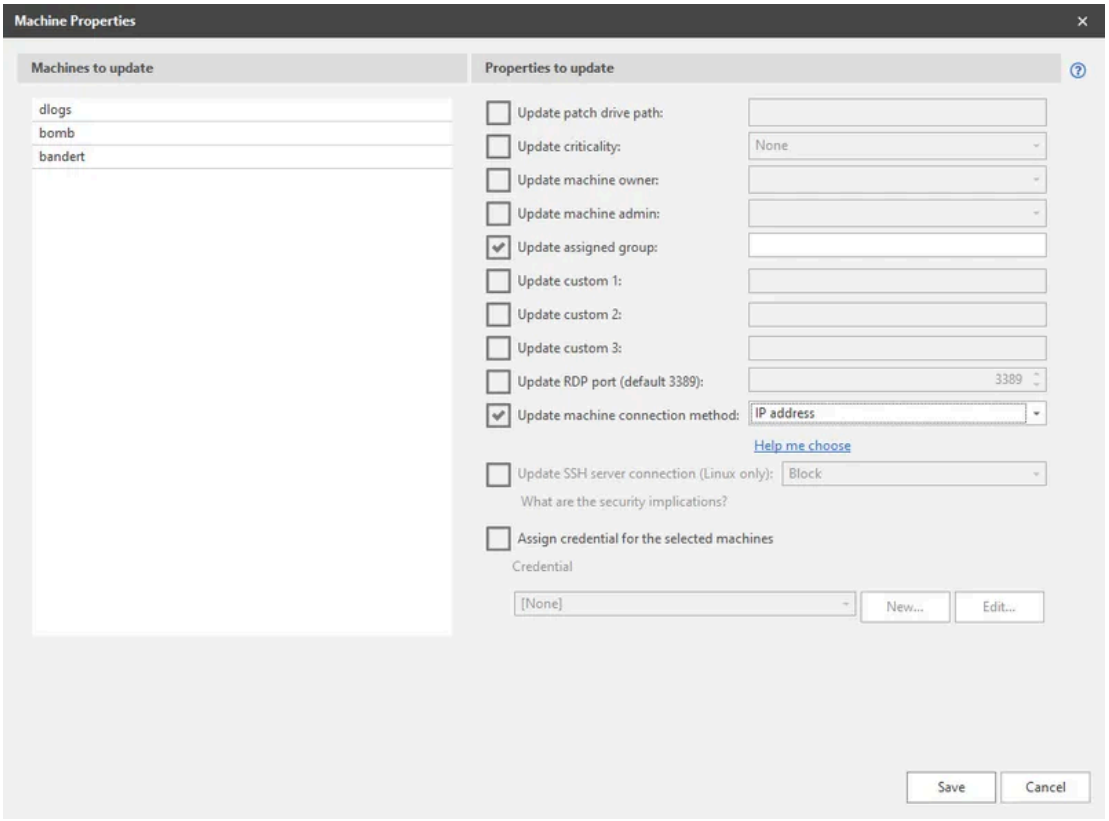


Tab	Description
General	Enables you to define a variety of general information about the machine, including: • **Description**, **Location**, **Customer Name**, **Criticality**, **Asset tag**: Site-specific information you want to provide for the machine. The **Criticality** level can be used to **sort the grid within Machine View**. • **Patch drive path:** Enables you to specify the drive and the path to use on the target machine when patch deployment packages and tools are downloaded during a patch deployment. Do this only if you do not want to use the default location (`C:\Windows\ProPatches`). For example, if the C: drive on your target machines is low on space, you might specify that the patch deployment packages and tools are instead written to the D: drive. The "ProPatches" name is automatically appended to whatever path you specify. For example, if you specify " `D:\ABC` ," the final destination for the patch deployment packages and tools will be " `D:\ABC\ProPatches` ." Separate subfolders will be created for the patches, the logs, etc. • The use of environment variables (such as `%windir%`) is not supported. **Assigned group:** The static group that this machine is assigned to within **Machine View** and **Scan View**. The group is used for organizational purposes. For example, you might sort, filter and search for a specific assigned group and then perform actions on the machines in that group. • **Custom 1 - 3:** These three fields enable you to write custom notes about properties that are unique to this machine. For example, you might use Custom 1 to specify the machine type (laptop, desktop, server, etc.), Custom 2 to specify the machine location (St. Paul, Dallas, Seattle, etc.), and Custom 3 to specify the department that owns the machine (HR, Accounting, IT, etc.). You can use the fields to filter or sort machines within **Machine View** and **Scan View** and when **scheduling reports**. • **RDP port:** Defines the **Remote Desktop Protocol (RDP) port** to use when making a remote desktop connection with this machine. • **Connect to machine by:** Specifies the method to use when connecting to your client machine. There are two options: ◦ **IP address:** The console will connect to clients using the IP address of the machines. This is the default setting. ◦ **Fully qualified domain name (FQDN):** You may need this method if Kerberos authentication is used in your environment, and if Service Principal Name (SPN) validation is required for Server Message Block (SMB) endpoint connections. For more detailed information, see **IP Address vs FQDN**. The setting specified here will be used for scans or agent installations that are initiated from Machine View or Scan View. **SSH server connection:** Choose whether you will allow SSH server connections to this Linux machine. • This option is only configurable on Linux machines. If this is a Windows machine, the ability to modify this option is disabled. The SSH protocol is used when the console initiates a connection with the specified Linux machine. The primary use cases are when a **power status scan** or a **push installation of an agent** are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain that the specified Linux machine is trusted and safe, you should choose to block SSH server connections. For more detailed information, see the **SSH Authentication** topic. **Credential:** Specifies the credential used when authenticating Security Controls to the machine. The credential you supply here will override credentials **specified in other areas of the program**. If you select **None** you effectively remove the credential currently assigned to the machine. There may be several reasons for providing different credentials to a machine after a scan has been performed. If you have multiple administrators in your organization and each is responsible for a different domain, they will need to set

Tab	Description
	their own credentials before performing an action. Or, your organization's policy may be to separate scan (assessment) duties from deployment duties, in which case different credentials are probably required.
Email	Enables you to specify which reports should be automatically sent and to whom the reports should get sent. The specified reports will be sent whenever the machine is involved in a scan or a deployment. To configure reports: 1. Select a report in the **Report** list. 2. In the **Report recipients** list, select the groups and/or individuals you want to email the report to. 3. Repeat Step 1 and Step 2 for each report you want to be automatically sent. 4. When finished, click **Save**. You can use the **Machine owner** and **Machine admin** boxes to define the owner and administrator of this machine. If you need to define a new contact or change the email address for a contact, select **Manage > Address Book**.
Statistics	Displays a trend chart showing the number of found and missing patches detected in the last several scans. This enables you to quickly determine if the patch security state of a machine is trending up or down.

238. Managing Multiple Machine Properties

The **Machine Properties** dialog is accessed from within Machine View or Scan View by right-clicking the desired machines and then selecting **Machine properties**. The dialog enables you to define several common properties for two or more machines. Values that you change here will overwrite corresponding values on the individual machines.



Field	Description
Machines to update	Contains a list of the machines that will be affected by the properties you define.
Patch drive path	Enables you to specify the drive and the path to use on the target machines when patch deployment packages and tools are downloaded during a patch deployment. Do this only if you **do not** want to use the default location (`C:\Windows\ProPatches`). For example, if the C: drive on your target machines is low on space, you might specify that the patch deployment packages and tools are instead written to the D: drive. The "ProPatches" name is automatically appended to whatever path you specify. For example, if you specify "`D:\ABC`," the final destination for the patch deployment packages will be "`D:\ABC\ProPatches`." Separate subfolders will be created for the patches, the logs, etc. The use of environment variables (such as `%windir%`) is not supported.
Criticality	(Red) Critical (Orange) High (Yellow) Medium (Gray) Low (White) Ignore

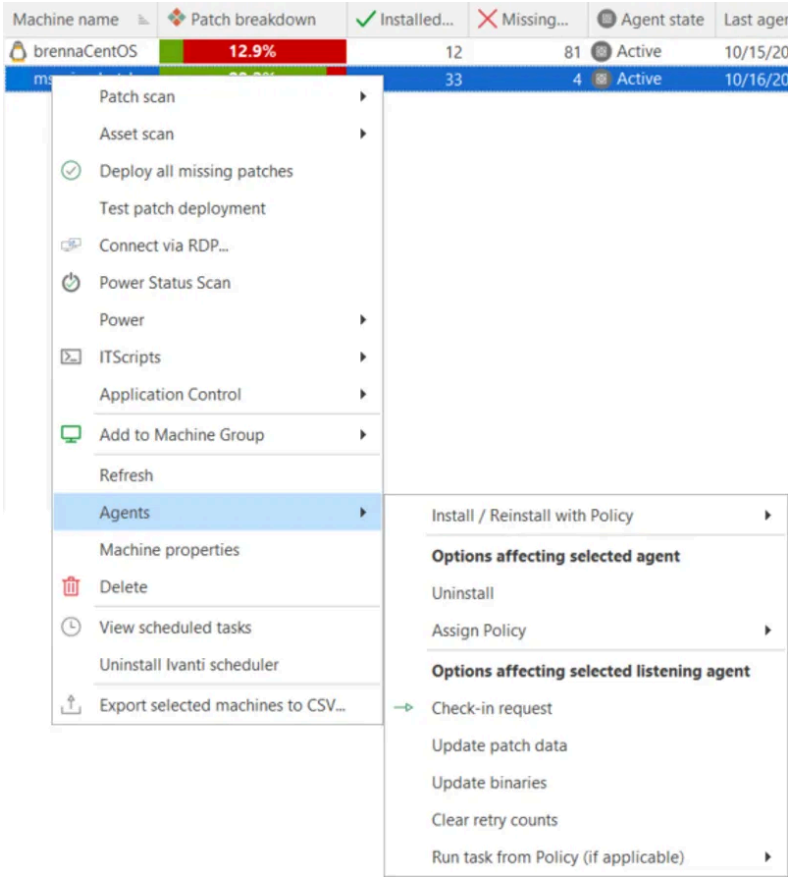
Field	Description
	Enables you to specify a custom criticality level for the listed machines. This value is something you assign and use for your own purposes. For example, if you have a set of machines that are of particular importance to your company, you can assign a criticality level to the machines and then use the filtering and sorting capabilities in **Machine View** to quickly locate the machines and determine their status. If you assign a custom criticality level, the flag displayed in the **Machine Criticality** column of Machine View will change to the appropriate color.
Machine owner	Defines the owner of the selected machines. If you need to define a new contact or change the email address for a contact, select **Manage > Address Book**. Use the **Update** check box to specify if you want this field to be updated when you click **Save**.
Machine admin	Defines the administrator of the selected machines. If you need to define a new contact or change the email address for a contact, select **Manage > Address Book**. Use the **Update** check box to specify if you want this field to be updated when you click **Save**.
Assigned group	The static group that the machines are assigned to within **Machine View** and **Scan View**. The group is used for organizational purposes. For example, you might sort, filter and search for a specific assigned group and then perform actions on the machines in that group.
Custom 1, **Custom 2** and **Custom 3**	**Custom 1 - 3:** These three fields enable you to write custom notes about properties that are unique to the listed machines. For example, you might use Custom 1 to specify the machine type (laptop, desktop, server, etc.), Custom 2 to specify the machine location (St. Paul, Dallas, Seattle, etc.), and Custom 3 to specify the department that owns the machine (HR, Accounting, IT, etc.). You can use the fields to filter or sort machines within **Machine View** and **Scan View** and when **scheduling reports**. Use the **Update** check box to specify if you want these fields to be updated when you click **Save**.
RDP Port	Defines the **Remote Desktop Protocol (RDP) port** to use when making a remote desktop connection with the machines.
Machine connection method	Specifies the method to use when connecting to your client machines. There are two options: • **IP address:** The console will connect to clients using the IP address of the machines. This is the default setting. • **Fully qualified domain name (FQDN):** You may need this method if Kerberos authentication is used in your environment, and if Service Principal Name (SPN) validation is required for Server Message Block (SMB) endpoint connections. For more detailed information, see **IP Address vs FQDN**. The setting specified here will be used for scans or agent installations that are initiated from Machine View or Scan View.
SSH server connection	Choose whether you will allow SSH server connections to the machines. The selected machines may contain a mix of both Windows and Linux machines. Only Linux machines are affected by changes made at this level. For Windows machines, this value will always be **Block**. The SSH protocol may be used when the console initiates a connection with the specified machines. The primary use cases are when a **power status scan** or a **push installation of an agent** are initiated from the console to a Linux machine. Security Controls does not currently support the use of SSH server authentication, so unless you are certain

Field	Description
	that the specified machines are trusted and safe, you should choose to block SSH server connections. For more detailed information, see the **SSH Authentication** topic.
Credential	Specifies the credential used when authenticating Security Controls to the machines. The credential you supply here will override credentials **specified in other areas of the program**. If you select **None** you effectively remove the credential currently assigned to the machines. There may be several reasons for providing different credentials to machines after a scan has been performed. If you have multiple administrators in your organization and each is responsible for a different domain, they will need to set their own credentials before performing an action. Or, your organization's policy may be to separate scan (assessment) duties from deployment duties, in which case different credentials are probably required.

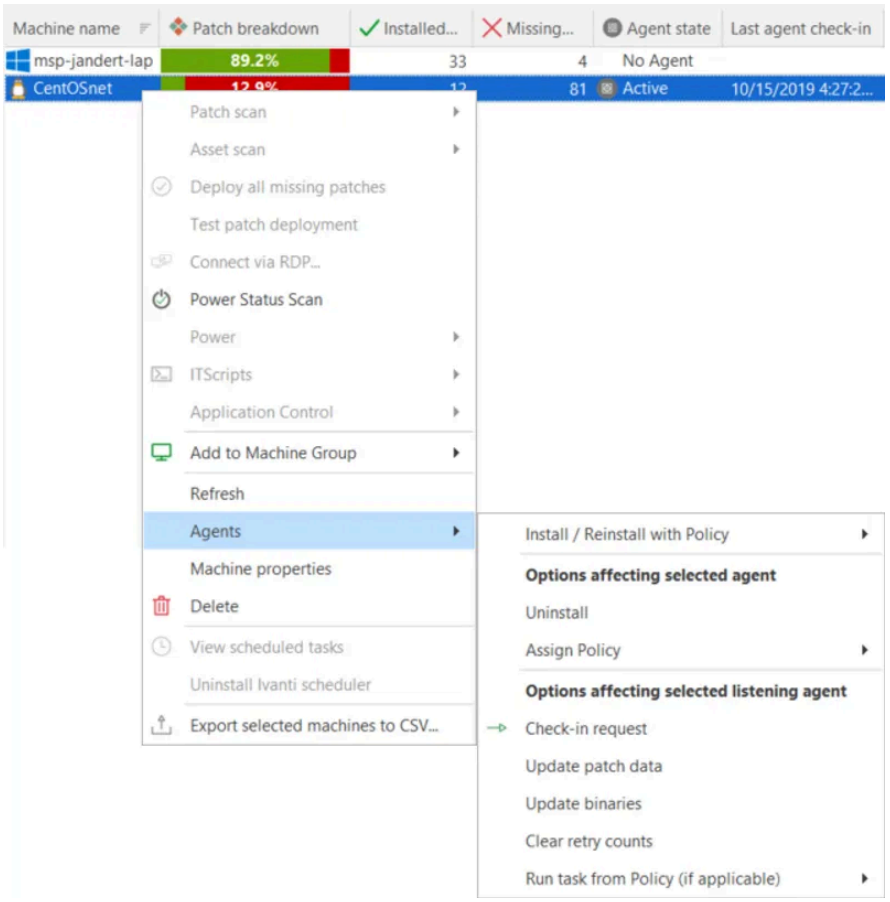
239. Managing Your Agents

You can use Machine View or Scan View to manage the machines that are running an agent policy. You can install an agent onto machines, you can assign a different policy to machines that already contain an agent, you can uninstall agents from machines, and you can issue a number of commands. You can also use the **Agent State** column in Machine View to determine which machines have Security Controls Agent installed.

All actions are performed by right-clicking the desired machines and then selecting the **Agents** menu.



Windows Machines



Linux Machines

Field	Description
Install / Reinstall with Policy	Installs an agent on the selected machine(s). If an agent already exists on a machine, it will reinstall the agent with the selected policy. The installation process will begin immediately. The target machine(s) must be online and able to communicate with the console. If a machine is not online the installation will fail. TIP: If you have target machines that are away from the corporate network and unable to contact the console, consider **installing agents from the cloud**.
Uninstall	Will remove the agent from the selected machine(s). • If an agent machine is online and configured to listen for **policy updates**, the agent will be uninstalled immediately. • If an agent machine is online but is not configured to listen for policy updates, the agent will be uninstalled the next time the agent checks in with the console. • If an agent machine is not currently online, the uninstall will be performed the next time the agent is online and checks in with the console or **the cloud**.
Assign Policy	Applies only to machines that already have agents installed. It will assign a different policy to the selected agent machines. • If an agent machine is online and configured to listen for **policy updates**, the new policy will be assigned immediately. • If an agent machine is online but is not configured to listen for policy updates, the new policy will be assigned the next time the agent checks in with the console. • If an agent machine is not currently online, the new policy will be assigned the next time the agent is online and checks in with the console or **the cloud**. The advantage of **Assign Policy** over **Install / Reinstall with Policy** is that it is quicker. This is because it is only updating policy files and not installing an entire agent.
The following commands apply only to machines that already have agents installed, that are online and that are configured to be **listening agents.**	
Check-in request	Forces the selected agent machines to immediately check-in with the console and download the latest policy.
Update patch data	Directs the agents to download the latest patch data.
Update binaries	Directs the agents to download the latest scan engines and data files.
Clear retry counts	Clears all patch counters on the agents. A unique patch counter exists for every patch an agent tries to download and for every patch an agent tries to install. A patch counter will increment whenever a patch download or a patch installation fails. Failed download and installation attempts will be recorded in the patch log. If a patch fails to download after 11 attempts or fails to install after

Field	Description
	3 attempts the agent will stop trying to deploy that particular patch. The only way to resume the deployment of that patch is to clear the counter.
Run task from policy	Enables you to initiate any of the tasks currently defined within the selected agents. When you select a task name a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See **Creating a New Agent Policy** for information on the types of tasks that may be available.

240. Manually Installing Security Controls Agent

You must manually install Security Controls Agent on machines that are guarded by a firewall. You do this by copying the agent installation files to the desired target machines and then running the Security Controls Agent installation wizard on each machine.

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Requirements

- The target machines must be able to communicate with the console.
- You must configure at least one Security Controls Agent policy before manually installing an agent. See **Preparing to Use Agents** for details.
- You must specify how the agent will authenticate itself to the console during the registration process. See **Agent Options** for details.
- The Security Controls issuing certificate must be in each target machine's certificate store to ensure a secure connection to the console.
- Installing an agent on a distribution server is a special case that requires the server machine's SYSTEM account to have read access to the distribution server folder. See **Configuring System Account Permissions** for details.

Windows Installation Procedure

There are two different methods you can use for manually installing agents.

Option 1: PowerShell Script Installation Method

Go to the **Agents Options** tab to learn how to use a PowerShell script that will copy the issuing certificate to the target machine's certificate store and install the agent on the target machine.

Option 2: Manual Installation Method

If you prefer not to use the provided PowerShell script, you must manually copy the issuing certificate to the target machine's certificate store and then run the agent installation wizard.

Copy the Console Certificate to the Target Machine

1. Export the ST Root Authority certificate from the Trusted Root Authority store on the console machine.
2. Import the certificate to the Trusted Root Authority on the remote machine.

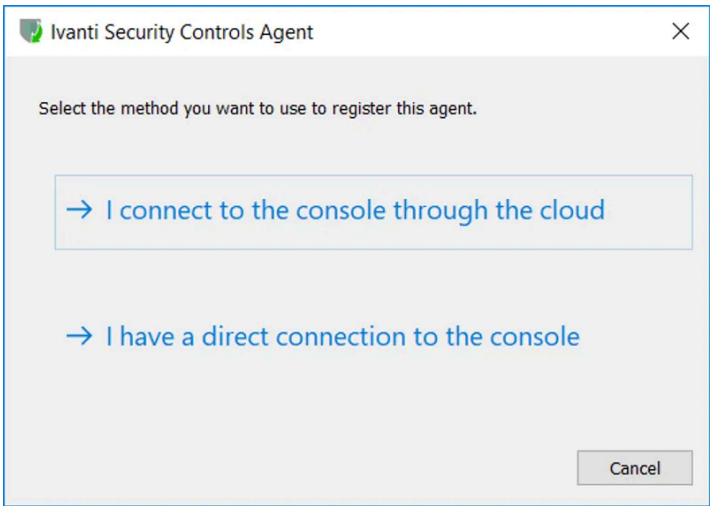
Install the Agent Using the Installation Wizard

1. On the Security Controls console, locate the **STPlatformUpdater.exe** file.
   The file is located in the `C:\ProgramData\Ivanti\Security Controls\Console\DataFiles` directory.
2. Copy the .exe file to the desired target machines.
   You can distribute this file using Active Directory, or you can simply copy it to a physical media such as a CD or flash drive and manually distribute it to the desired machines.

> When distributing this file you may choose to create an **installation script** that automatically passes all necessary information to the installation wizard.

Log on to the target machine using an administrator account.

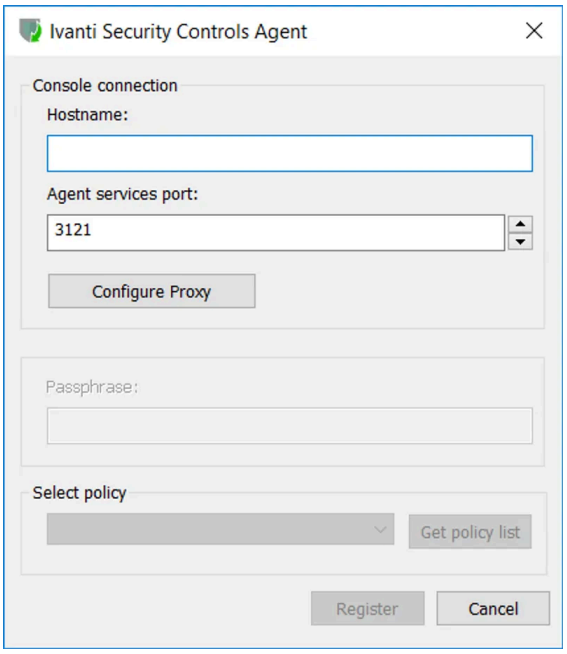
4. Double-click the file named **STPlatformUpdater.exe**.
   The agent is installed. When the installation is complete the **Agent Registration** dialog is displayed.



Click **I have a direct connection to the console**.

> The **I connect to the console through the cloud** button is used if you are installing the agent via the cloud.

The following dialog is displayed.



Provide the required information.

- **Hostname**: Type either the hostname or the IP address of the Security Controls console. Examples: Myconsole or 192.168.1.100.

  > If an IP address is used, the IP address must be added to the Console Alias list.

  Agent services port: Specify the port number used for forwarding information to the console. 3121 is the default port number.

- **Configure Proxy**: Click this button to specify the proxy settings the agent will use during the registration process. See Configuring Proxy Server Settings for details.
- **Passphrase**: Type the passphrase that is specified on the **Tools > Options >** Agents dialog.
- **Select policy**: Click **Get policy list** to connect to the console and populate the **Select policy** box with the list of all available agent policies. Select the policy you want assigned to this agent.

On the **Agent Registration** dialog click **Register**.

8. On the **Agent Setup Wizard** dialog, click **Finish**.

The agent installation routine will:

- Install the necessary .exe and other supporting files in the `C:\Program Files\LANDESK\Shavlik Protect Agent` directory
- Install the certificates needed to communicate securely with the console

- Acquire an agent license
- Retrieve the assigned policy, the engine components and the data files and store them.
  The files are stored in the `C:\ProgramData\LANDESK\Shavlik Protect\Agent` directory.

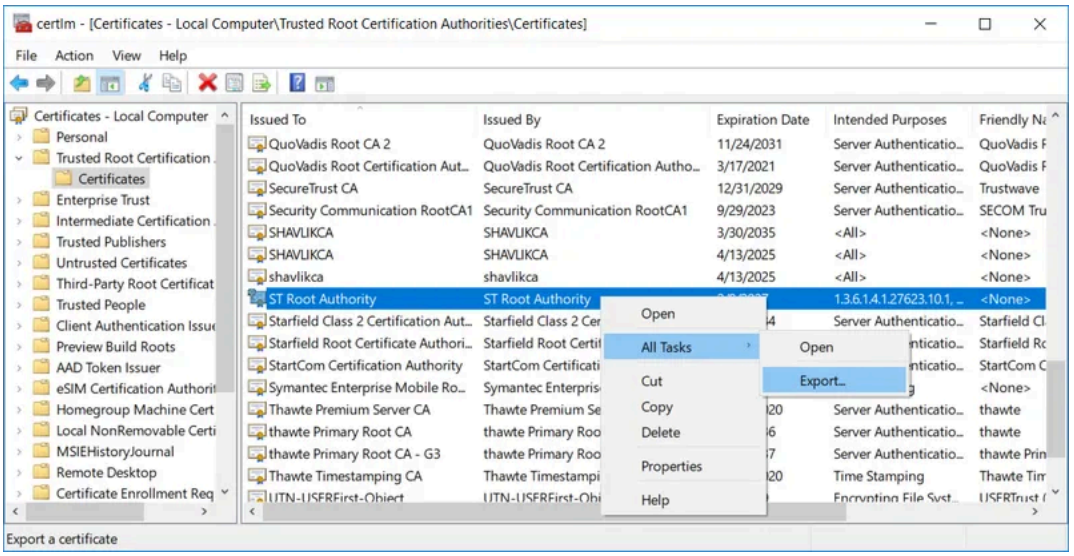
When the download is complete the agent will be started automatically. You can check the status of the agent using the Security Controls Agent client program, available by selecting **Start > All Programs >** Security Controls **>** Security Controls Agent. You can use this program to configure any settings that were marked as user-configurable.

Linux Installation Procedure

1. Using the Security Controls console, select **Tools > Options > Agents** and verify that you have enabled the passphrase option and specified a passphrase.
2. On the console machine, export the Security Controls issuing certificate to a DER file.

> If you have replaced the default Security Controls certificate with your own authority certificate, export that certificate rather than the Security Controls issuing certificate. The authority certificate that you generated will likely be contained in the Intermediate Certification store.

Using Microsoft Management Console (MMC), go to the **Certificates - Local Computer > Trusted Root Certification Authorities > Certificates** folder. Right-click the certificate named **ST Root Authority** and then select **All Tasks > Export**.



Follow the steps in the Certificate Export Wizard. When prompted, specify that you do not want to export the private key. Save the file to your console machine in DER Encoded Binary X.509 format using an easy-to-remember file name (e.g. ISECCert.cer).
On the console machine, locate the appropriate **ISecAgent** TAR file.
The TAR files are located in the `C:\ProgramData\Ivanti\Security Controls\Console\DataFiles` directory. Be sure to locate the file that is associated with the operating system used on your Linux machines. For example, if you have RedHat 7.x machines you will want the file named ISecAgent-Rhel7.tar.

4. Copy the TAR file to the same folder as the exported certificate file from Step 2.
5. Distribute the certificate file and the TAR file to the desired target machines.
   You can do this using whatever mechanism works best for your organization. You might use a secure file transfer tool such as WinSCP, or you can simply copy the files to a physical media such as a flash drive and manually distribute them to the desired machines.
6. On a Linux machine, launch a terminal and change to the path that contains the certificate file and the TAR file.
7. Extract the contents of the TAR file.
8. For example:
   ```
   # tar -xf ISecAgent-Rhel7.tar
   ```
   Display the list of extracted files.

9. `# ls`

   The **install.sh** file should be listed.

   Use the **install.sh** file to install the agent and register it with the console.

   `# ./install.sh --host <consolename> --port 3121 --passphrase <passphrase> --issuer-certificate <exported_root_cert.cer> --selected-policy <agent_policy_name>`

   where:

   - `<consolename>` is the name of your console machine. The name you specify must match an entry in the **console alias list**.
   - 3121 is the default port number but it can be configured by editing the C:\Program Files\Ivanti\Security Controls\STEnvironment.config file.
   - `<passphrase>` is the passphrase you specified on the **Tools > Options > Agents tab.**
   - `<exported_root_cert.cer>` is the name of the exported root certificate file.
   - `<agent_policy_name>` is the name of the agent policy you want to assign to the agent.

If the process is successful you will see the message `Agent is fully registered`. Repeat Steps 6 - 9 for each Linux machine.

You can use the stagentctl command-line utility to manage an agent. For details, see **Using an Agent on a Target Machine**.

Related Topics

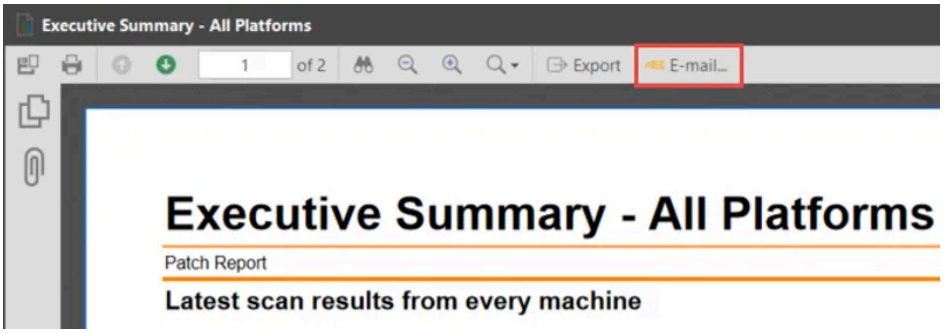
Preparing to Use Agents

Installing Agents from the Console

Installing Agents from the Cloud

241. Manually Sending Email Reports and Notifications

While viewing a report you generated, you can email the report by clicking the **E-mail** button. This button is only available if you have enabled email operations.



242. Menu Commands

> The menu commands that are available are dependent upon your particular product license.

The Security Controls menus enable you to do the following:

Home:

Takes you to the **home page**.

New:

- **Agentless operation**: Perform a new **agentless operation**
- **Machine Group:** Create a new machine group
- **Agent Policy**: Create a new agent policy
- **Favorite:** Create a new favorite
- **Windows Patch:**
  - **Patch Group:** Create a new Windows patch group
  - **Patch Scan Template:** Create a new Windows patch scan template
  - **Deployment Template:** Create a new Windows deployment template
  - **Product Level Group**: Create a new Windows product level group

Linux Patch:

- **Patch Deployment Configuration**: Create a new Linux patch deployment configuration for use within an agent policy

Linux Patch (Content-Based):

- **Patch Group (Content-Based)**: Create a new Linux patch group
- **Patch Scan Configuration (Content-Based)**: Create a new Linux patch scan configuration for use within an agent policy
- **Patch Deployment Configuration (Content-Based)**: Create a new content-based Linux patch deployment configuration for use within an agent policy

Power State Template: Create a new power state template

- **Asset Scan Template**: Create a new asset scan template
- **ITScripts Template**: Create a new ITScripts template

Import:

- **Machine Group**: Imports an existing group definition from an encrypted XML file
- **Windows Patch Group**: Imports an existing patch group definition from a text file
- **CVEs**: Import a list of CVEs
- **Add vCenter Server/ESXi Hypervisor**: Add a vCenter Server or an ESXi Hypervisor to your virtual inventory

View:

- **Charts:** Displays a number of charts that show the security status of your network at the time of the most recent machine scans
- **Machines:** Displays current information about every machine in your network that has been previously scanned
- **Windows Patches:** Provides detailed information about patches for the various operating systems and applications scanned for by Security Controls
- **ITScript results:** Displays information about the scripts that have been executed on your target machines
- **Event History:** Displays log entries that are generated by background operational events
- **Operations Monitor:** Launches the Security Controls Operations Monitor, which tracks a number of different background tasks
- Deployment Tracker: Launches Security Controls Deployment Tracker, which tracks deployment tasks that are currently in progress
- **Refresh:** Refresh the information displayed in the right-hand pane

Manage:

- **Address Book**: Displays the address book used to store the names and email addresses of contacts you wish to send reports
- **Credentials**: Launches the Credential Manager, which manages all credentials used within the program
- **Database Maintenance**: Displays a list of all prior scans and patch deployments and enables you to perform maintenance tasks on the database
- **ITScripts**: Launches the Script Catalog Manager, which enables you to specify which scripts are approved for use within your organization
- **Users**: Used to assign specific roles to specific administrators
- **Custom Patches**: Used to create and manage custom patches, products, and bulletins
- **Scheduled Console Tasks:** Launches the Scheduled Console Tasks Manager, which is used to monitor the status of tasks that have been scheduled to run on the console

Tools:

- **Search Machine Groups**: Launches the Search Machine Groups dialog, which enables you to search for names in any of your existing machine groups.
- **Edit console description**: Launches the Edit Console Description dialog, which is used to change the name the program uses when referring to the console
- **Console alias editor**: Launches the Console Alias Editor dialog, which is used to assign trusted names and IP addresses to the console certificate
- **Create report**: Launches the Report Gallery, which is used to generate a variety of reports on any of the scans and patch deployments that have been performed
- **Schedule report:** Launches the Schedule Report dialog
- **Custom Patch Editor**: Used to create and manage custom patches, products, and bulletins
- **Run console ITScripts**: Enables you to select and run those scripts that run on the console machine but not against target machines
- **AC Configuration comparison**: Launches the , which enables you to view the differences between two configuration versions.
- **Auto-update definitions**: Automatically downloads new data definition files immediately before performing a new scan. Enabling this check box will also enable the **Auto-update definitions (before scans)** check box on the Tools > Options > Downloads dialog.
- **Options**: Launches the Options dialog, which enables you to configure a number of different program options

Help:

- **Enter/refresh license Key**: Enables you to activate the program or to upgrade your program license
- **Check for program updates**: Checks if a new version of the program is available
- **Refresh files**: Downloads new versions of the data definition files and the command files used by the program
- **View how-to tutorials**: Provides links to a website that contains tutorials that show you how to perform certain tasks
- **View help**: Display the Help system
- **Submit a feature request**: Links to a webpage that enables you to provide feedback on Ivanti products
- **Contact Technical Support**: Opens the Security Controls Community page within your default web browser
- **About** Security Controls: Displays program version information as well as information about your licensed capabilities

243. Introduction to the Migration Tool

Ivanti provides a Migration Tool that is used to migrate your existing Security Controls console to a new machine. The Migration Tool simplifies the migration process. The tool captures core and user data from your existing console and rewrites it into a new Security Controls installation.

The most common reasons for migrating a Security Controls console to a new machine are:

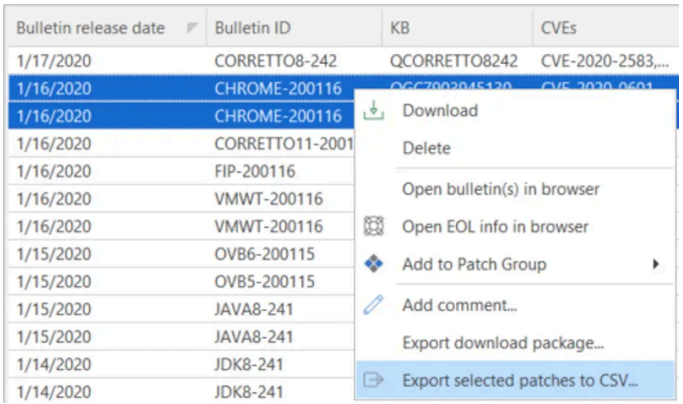
- Migrate off an operating system that is no longer supported by the latest version of Security Controls
- Migrate off an operating system that has been marked for end-of-life
- Migrate to better, faster hardware

Related Topics

- Requirements for Using the Migration Tool
- Commonly Asked Questions
- Before You Begin
- Creating Your Backup Files
- Restoring Your Console on a New Machine
- Post-Migration Tasks

244. Exporting Patches

Use the right-click menu to export information about selected patches to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.



245. Monitoring Agent Actions

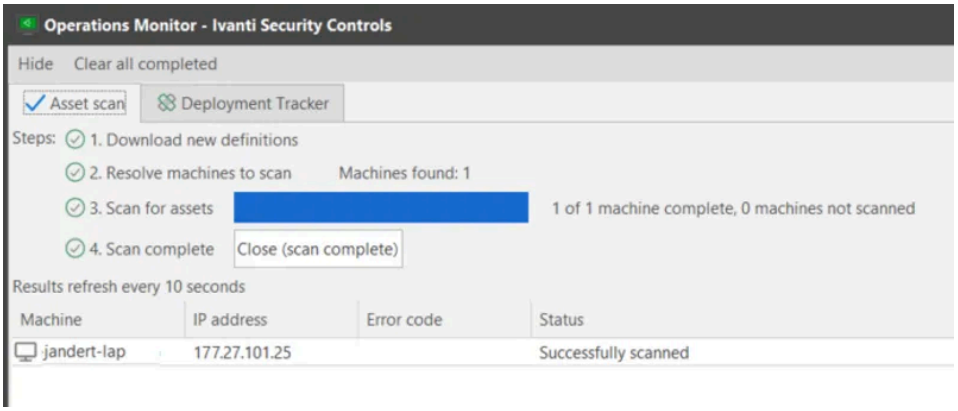
You cannot use the console to watch the actual scans, patch deployments, etc. as they are performed by agents on each target machine. For that you must use the **Windows agent client program**. You can, however, view the most recent results of agent scans and deployments using **Machine View**. The results are reported to the console and displayed on the appropriate tabs in the middle pane. The top pane can be used to determine which machines have successfully installed Security Controls Agent; it does this by displaying **Active** in the **Agent State** column. The top pane of Machine View will also display the **Assigned Agent Policy**, the **Reported Agent Policy**, the **Last Agent Check-In**, and the time of the last scans. See **Determining Which Machines Have Agents** for more information.

When agents check in with the console they will be listed in the machine group from which they were last scanned from the console. See **Machine Group Information is Dynamic** for more information.

If you wish to produce one or more reports that show the agent activity that has been reported to the console you can do so using the **Report Gallery** (Windows agents only).

246. Monitoring an Asset Scan

The Operations Monitor is automatically displayed whenever an agentless asset scan is initiated. It shows the steps involved in the asset scanning process and the progress of each step.



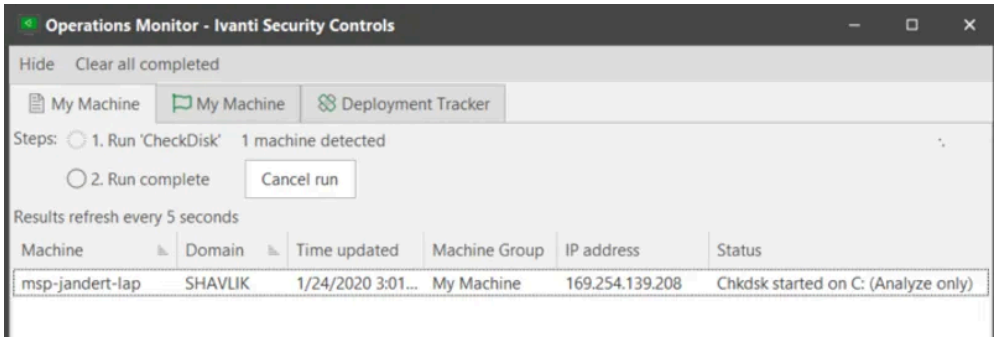
Using the Operations Monitor you can:

- Cancel the asset scan by clicking **Cancel scan**.
- Remove the current asset scan tab by clicking **Close (scan complete)**. Any other tabs on the Operations Monitor will remain open.
- Close the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor. Select **View > Operations Monitor** to reopen the window.
- Remove the current tab and all other tabs with completed tasks by clicking **Clear All Completed**.
- View summary information about each machine that was scanned. Right-click on a column heading and select **Column Chooser** to add or remove columns from the display.

To view the results of the scan, see **Viewing Asset Scan Results**.

247. Monitoring the Execution of a Script

The Operations Monitor is automatically displayed whenever a script is executed. It shows the steps involved in the process and the progress of each step.



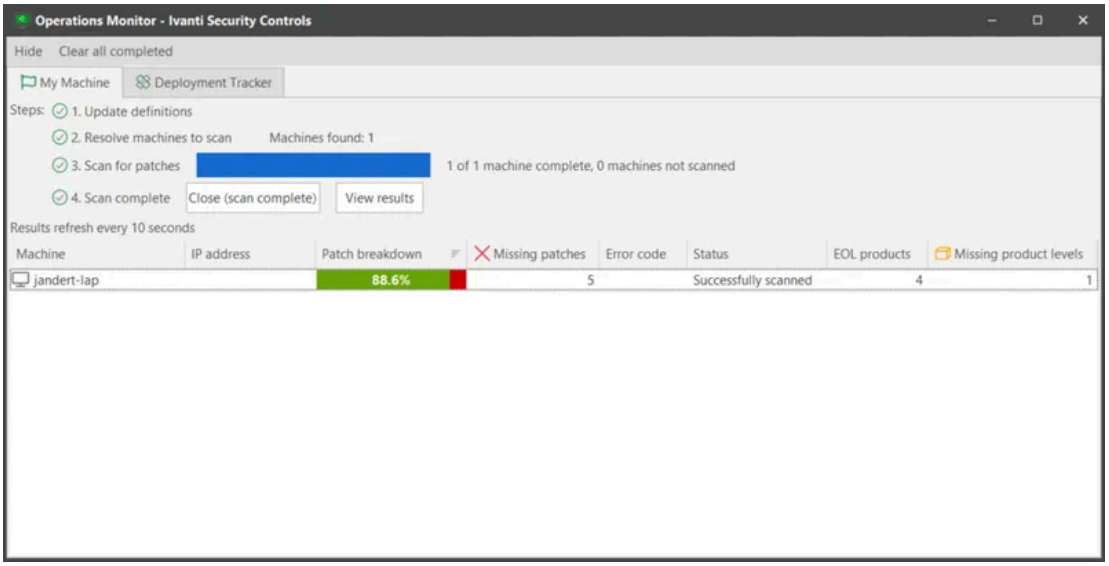
Using the Operations Monitor you can:

- Remove the active tab by clicking **Close**. Any other tabs on the Operations Monitor will remain open.
- Close the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor. Select **View > Operations Monitor** to reopen the window.
- Remove the active tab and all other tabs with completed tasks by clicking **Clear All Completed**.

To view the results of the script, see **ITScripts Results View**.

248. Monitoring a Patch Scan

The **Operations Monitor** is automatically displayed whenever a patch scan is initiated. It shows the steps involved in the patch scanning process and the progress of each step.



When the patch scan process is complete you can:

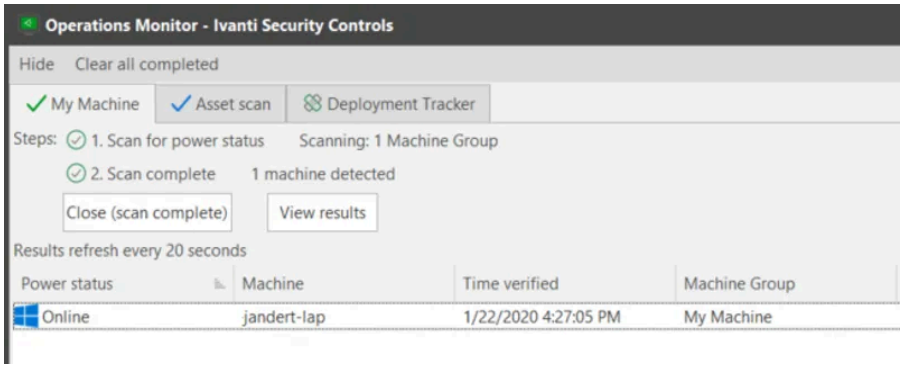
- View the patch scan results by clicking **View results**. The current patch scan tab will be removed from the Operations Monitor, the Operations Monitor will be closed, and the scan results will be displayed. See **Accessing Patch Scan Results** for details.
- Remove the current patch scan tab by clicking **Close (scan is complete)**. Any other tabs on the Operations Monitor will remain open.
- Minimize the Operations Monitor by clicking **Hide**. No tabs are removed from the Operations Monitor.
- Remove the current tab and all other tabs by clicking **Clear All Completed**.
- View summary information about each machine that was scanned. Right-click on a column heading and select **Column Chooser** to add or remove columns from the display.

249. Monitoring a Power Task

The Operations Monitor is automatically displayed whenever an agentless power management task is initiated. This includes:

- Restart now
- Shut down now
- Send Wake-on-LAN request (Run now)
- Power state template (Run now)
- Power Status scan (this is a special case, see **Monitoring a Power Status Scan**)

The Operations Monitor will show the requested action, the status, and any errors that occur.



The Operations Monitor will display the status of power tasks that are performed immediately. It will also show whether scheduled tasks are successfully scheduled on the target machines. See **Monitoring a Scheduled Power Task** for more details.

250. Monitoring a Scheduled Asset Scan

When you click **Schedule** on the **Asset inventory** tab of the Agentless Operation page, a scheduled task is created on the console that will launch the scan at the appointed day and time. To view the scheduled task, select **Manage > Scheduled Console Tasks**.

The Scheduled Console Tasks Manager uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Schedule Library > Ivanti > Security Controls** tree.

251. Monitoring a Scheduled Patch Scan

When you click **Schedule** on the Agentless Operation page, a scheduled task is created on the console that will launch the scan at the appointed day and time. To view the scheduled task, select **Manage > Scheduled Console Tasks**.

The Scheduled Console Tasks Manager uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Schedule Library > Ivanti > Security Controls** tree.

252. Monitoring a Scheduled Power Task

When you click **Schedule** on the **Power state** tab of the **Agentless Operation page**, a scheduled task is created on the console that will launch the scan at the appointed day and time. To view the scheduled task, right-click the desired machine **View scheduled tasks**. If the power task is scheduled to run against the console, you can view that by selecting **Manage > Scheduled Console Tasks** and then selecting the **Local Patch Deployments** tab.

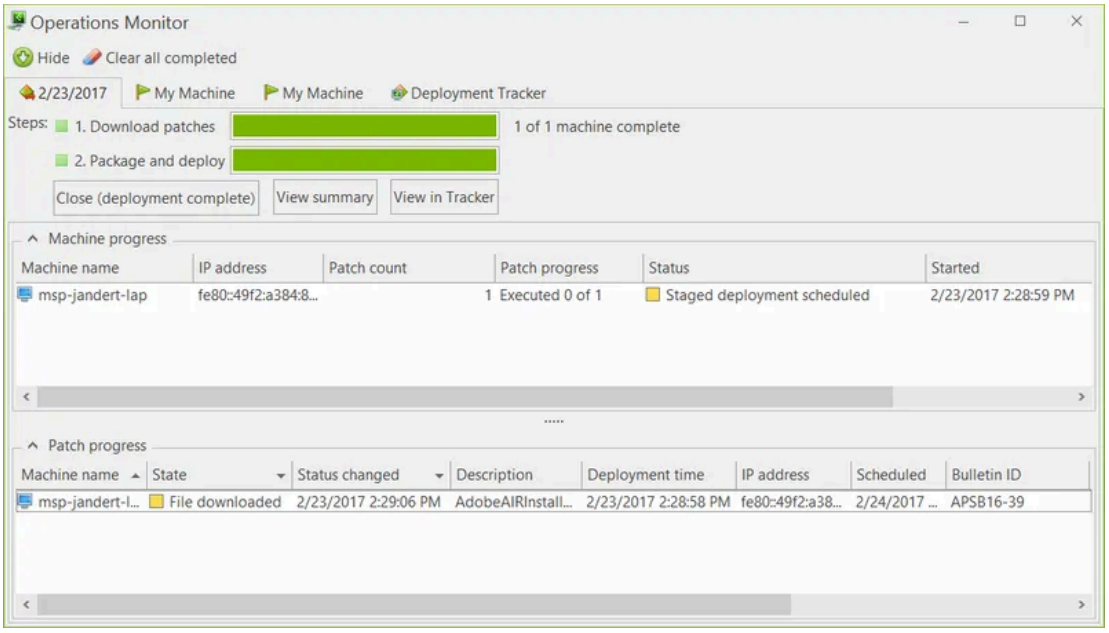
253. Monitoring a Scheduled Script

When you click **Schedule** on the **ITScripts** tab of the **Agentless Operation page**, a scheduled task is created on the console that will launch the script at the appointed day and time. To view the scheduled task, select **Manage > Scheduled Console Tasks**.

The **Scheduled Console Tasks Manager** uses the services of the Microsoft Task Scheduler to schedule and initiate each task. If you prefer, you can view the tasks within the Microsoft Scheduler by accessing the **Task Scheduler** dialog on your Windows console machine and then expanding the **Task Schedule Library > Ivanti > Security Controls** tree.

254. Monitoring the Deployment

The Operations Monitor is used to track the status of each patch deployment. It is displayed automatically and it provides progress information about each step in the deployment process. You can expand the list in the **Patch progress** table to view deployment information on individual patches. You can also sort the tables by dragging a column to the first position.



Scheduled patch deployments can be managed using the Scheduled Remote Tasks Manager.

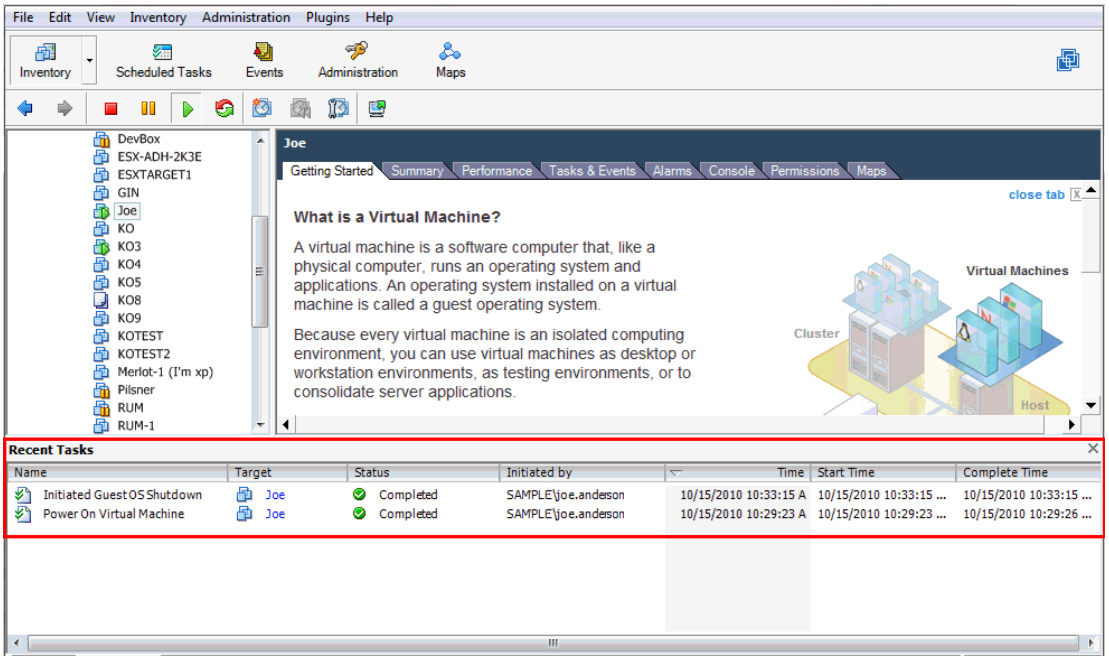
Active patch deployments can be monitored using the Deployment Tracker.

Completed patch deployments can be reviewed by selecting the deployment in the **Results** list. See Viewing Deployment Results for details.

Patch deployment information can be reviewed on a machine basis using Machine View.

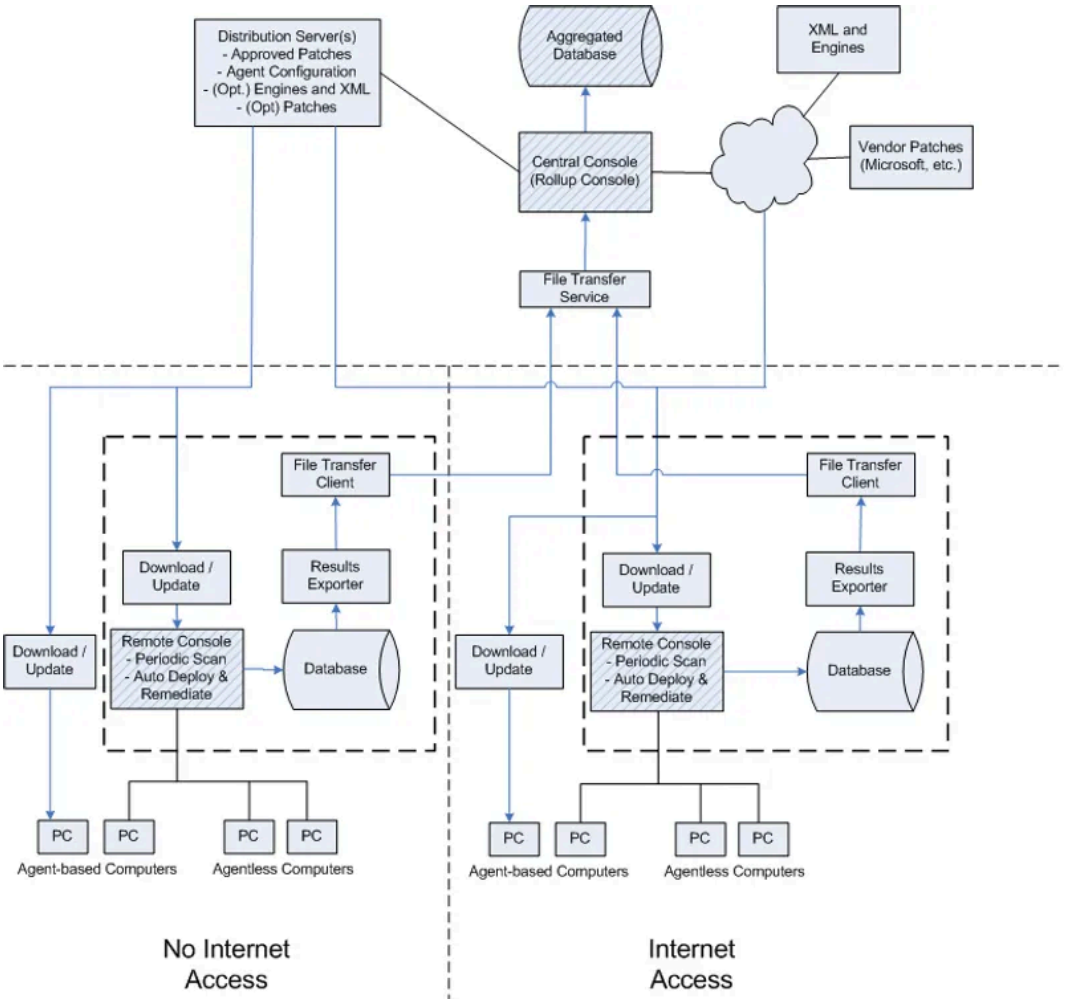
Tips for Monitoring Patch Deployments to Virtual Machines

- When using Deployment Tracker, if you notice that a server task has failed for a virtual machine (for example, taking a snapshot or re-enabling the network), you can complete the task using your client software.
- In addition to using the tracking tools provided by Security Controls, for virtual machines that are hosted on a server you can also use your client software to monitor the patch deployment progress. For example:


File Edit View Inventory Administration Plugins Help
Inventory
Scheduled Tasks
Events
Administration
Maps
DevBox
ESX-ADH-2K3E
ESXTARGET1
GIN
Joe
KO
KO3
KO4
KO5
KO8
KO9
KOTEST
KOTEST2
Merlot-1 (I'm xp)
Pilsner
RUM
RUM-1
Joe
Getting Started
Summary
Performance
Tasks & Events
Alarms
Console
Permissions
Maps
close tab
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.
Virtual Machines
Cluster
Host
Recent Tasks
Name
Target
Status
Initiated by
Time
Start Time
Complete Time
Initiated Guest OS Shutdown
Joe
Completed
SAMPLE\joe.anderson
10/15/2010 10:33:15 A
10/15/2010 10:33:15 ...
10/15/2010 10:33:15 ...
Power On Virtual Machine
Joe
Completed
SAMPLE\joe.anderson
10/15/2010 10:29:23 A
10/15/2010 10:29:23 ...
10/15/2010 10:29:26 ...

255. Multiple Console Configuration with Agents

It is possible to combine the use of agentless and agent-based machines with multiple consoles. Agent-based machines are implemented using Security Controls Agent. Detailed information about using Security Controls Agent is provided in the following section.



256. Navigating the Scan View Grid

Patch scan results are presented in a Scan View grid that contains three separate panes. Each pane displays unique information and provides unique functionality. The panes are interrelated in that the information presented in a lower pane is dependent on what is selected in the pane directly above it. This "top down" approach means you use the top pane to view high-level information and the two lower panes to drill down to more detailed information.

> While the two are extremely similar in look and feel, Scan View is different than **Machine View**. Scan View represents a point in time (the date and time the scan was performed) for the machines specified in the scan. Machine View, however, displays the most current information for all machines that have ever been scanned.

- The top pane displays all machines that were either successfully or unsuccessfully scanned. See the following topics for information on using the top pane:
  - **Searching for Machines**
  - **Filtering Info in the Top Pane**
  - **Performing Actions on Machines**

The middle pane displays patch information about the machine(s) selected in the top pane. See the following topics for information on using the middle pane:

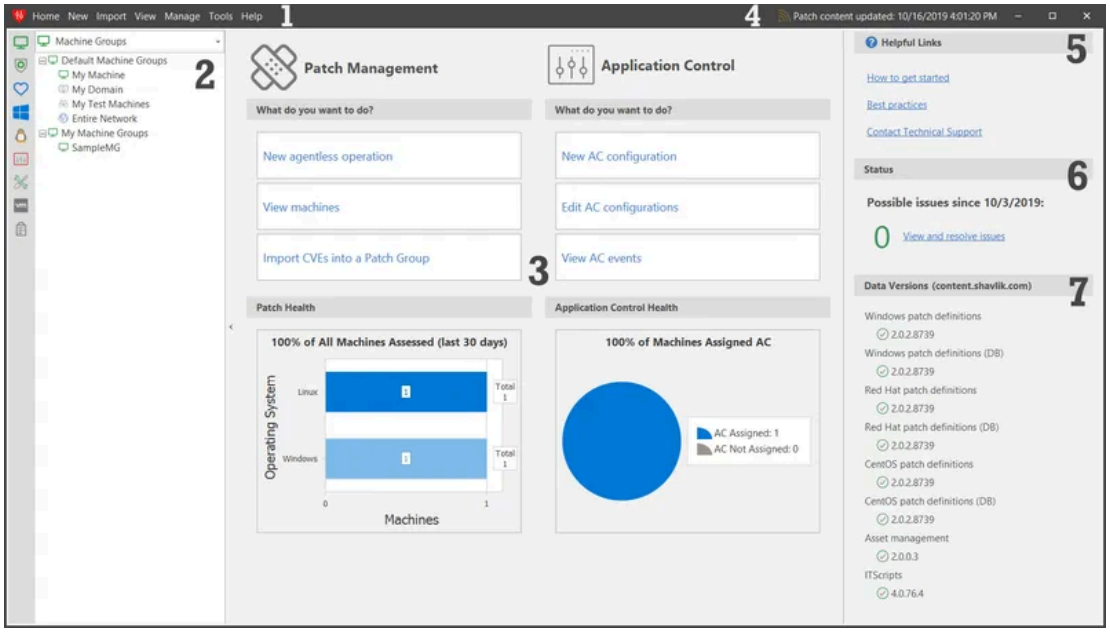
  - **Viewing Scan Result Patch Summaries**
  - **Performing Actions on Patches**

The bottom pane displays detailed information about the patch selected in the middle pane. See the following topics for information on using the bottom pane:

  - **Viewing Patch Details**
  - **Viewing Machines Affected by a Selected Patch**

257. Navigating the Interface

The Security Controls interface is designed to be simple yet powerful, enabling you to perform any number of activities quickly and easily. An annotated home page is shown here. For information about each area of the interface, see below.



1 - The **menu bar** provides quick access to many of the functions of the program.

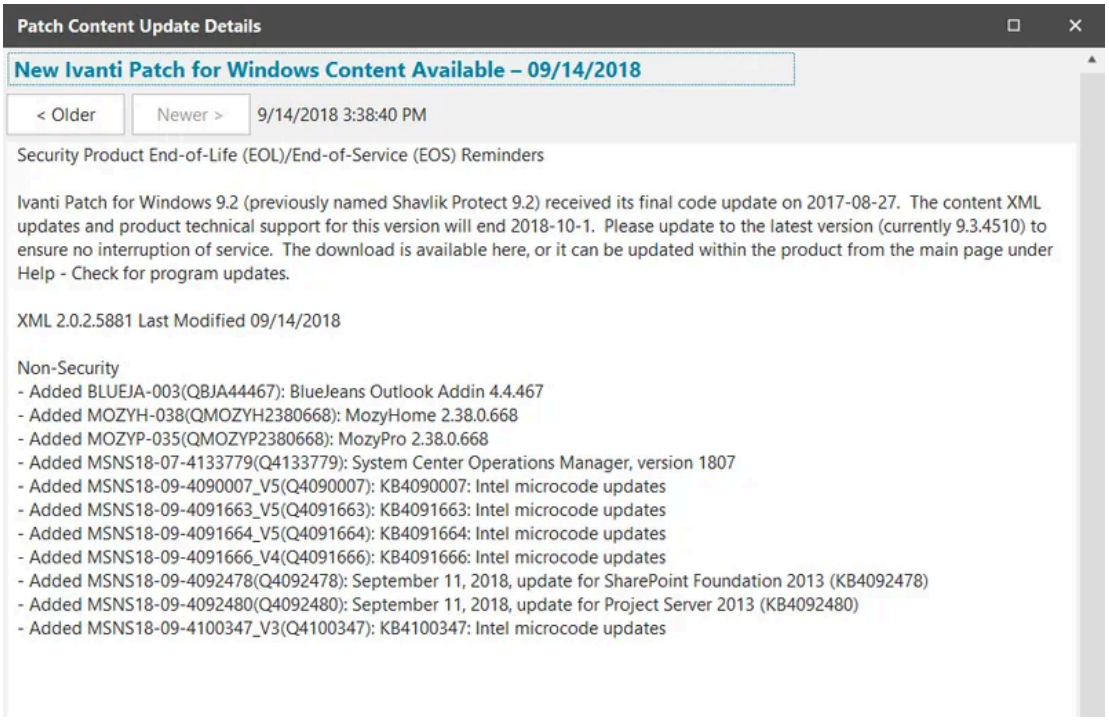
2 - The navigation pane displays whatever **primary feature** is currently selected. You can choose a different feature using either the selection box located at the top of the pane or the shortcut buttons located along the side. There can be only one feature active at a time. In this example the Machine Groups feature is the active feature.
You can collapse the navigation pane by clicking the icon. This maximizes the size of the right-hand pane.

3 - This area of the home page provides at-a-glance statistics and links to some of the most commonly performed tasks.

> **TIP:** Many of your everyday tasks are performed from the **Agentless Operation page**. You can access this page three different ways: (1) Press Ctrl+N, (2) Select **New > Agentless operation**, or (3) Click the **New agentless operation** link on the home page.

4 - This shows the date that the patch content was last updated. This is a configurable item and can be disabled using the **Tools > Options > Display > Show patch content updates on main page check box**.

If you click the date, the **Patch Content Update Details** dialog is displayed. Use this dialog to view more detailed information about the current patch data and about previous patch data releases. This newsfeed will also be used to display important security-related news and messages from Ivanti.



5 - This area provides you with some links that will help you quickly get started with the program.

6- This area displays the number of possible issues that have occurred within the program since the specified date. The issues may or may not require administrative action. The number of days' worth of issues to show is a configurable item; see the **Recent errors option**. If you click **View and resolve issues**, you can review the list of issues within **Event History**.

7 - This areas shows the versions of the data files currently being used within the program.

258. Navigating Machine View

Machine View consists of three panes. Each pane displays unique information and provides unique functionality. The panes are interrelated - the information presented in a lower pane depends on what is selected in the pane directly above it. This "top down" approach means you use the top pane to view high-level information and the two lower panes to drill down to more detailed information.

- The top pane displays all machines that have been scanned at some point and that are "known" by the program. See the following topics for information on using the top pane:
  - **Searching Machine View**
  - **Filtering Machine View**
  - **Performing Actions on Machines**
  - **Customizing the Column Headers**

The middle pane displays patch and asset information about the machine selected in the top pane. See the following topics for information on using the middle pane:

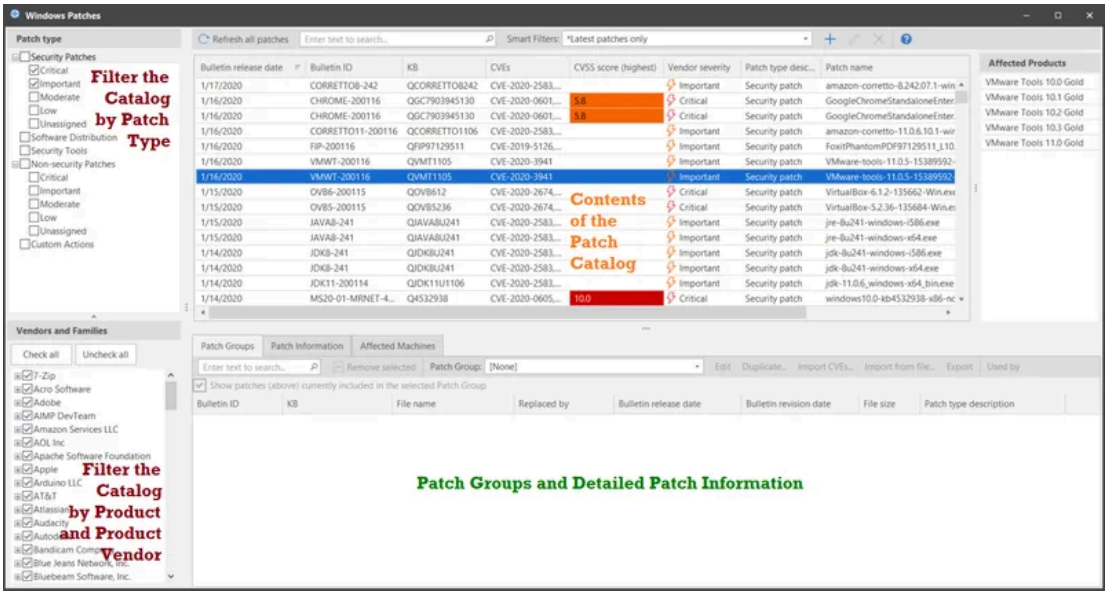
  - **Viewing Patch and Asset Summaries**
  - **Performing Actions on Patches**
  - **Customizing the Column Headers**

The bottom pane displays detailed information about the patch selected in the middle pane. See the following topics for information on using the bottom pane:

  - **Viewing Patch Information**
  - **Viewing Machines Affected by a Selected Patch**
  - **Customizing the Column Headers**

259. Navigating Windows Patch View

Windows Patch View consists of several different panes. Each pane displays unique information and provides unique functionality.



- The two left-hand panes are used to filter the content in the patch catalog. They dictate what patch content is displayed in the top pane.
    - Filtering by Patch Type
    - Filtering by Product Vendor

The top pane displays all patches in the patch catalog that are not filtered out by the two left-hand panes. You can apply additional filters, you can view information about individual patches and you can add patches to new or existing patch groups.

- Searching Patch View
- Filtering the Top Pane
- Performing Actions on Patches
- Customizing the Column Headers

The bottom pane displays the contents of any patch groups that you have defined. It also displays detailed information about the patch selected in the top pane. The patch status for missing and installed patches are clearly indicated.

- Creating and Editing Patch Groups
- Viewing Patch Details
- Viewing Machines Affected by a Selected Patch
- Customizing the Column Headers

The top and bottom panes are interrelated in that the information presented in the bottom pane is dependent on what is selected in the top panes. This "top down" approach means you use the top pane to view high-level information and the bottom pane to drill down to more detailed information.

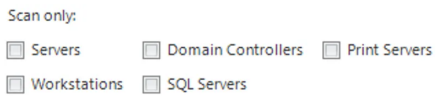
260. Notes About Virtual Machines

Requirements

- Dual boot systems (for example, a virtual machine with two partitions, each containing a different operating system) are not supported.
- When scanning offline virtual machines that are supported by VMware, please keep in mind the following:
  - You cannot mount encrypted virtual disks.
  - You cannot mount a virtual disk if any of its .vmdk files are compressed or have read-only permissions.
  - You cannot mount a virtual disk that is currently being used by a running or suspended virtual machine.
  - Linked clones and compressed images are not supported.

General Notes

- Only the current state of the virtual machine will be scanned and patched. Snapshots of virtual machines are not scanned or patched.
- A virtual machine is counted only once against the total number of license seats available, even if it is scanned both in online (powered on) mode and offline (powered off) mode.
- In machine groups and in scan results, special icons will distinguish an offline virtual machine ( ) from a physical machine or an online virtual machine ( ) and from a **virtual machine template** ( ).
- Avoid using network drive letters when defining offline virtual machines in a machine group. The recommended practice is to instead specify the Uniform Naming Convention (UNC) path. This comes into play when performing a scheduled scan on an offline virtual machine. Network drive mappings are session-specific, so it is very possible that a specified mapping will no longer exist when the scheduled scan process is run.
- Within a machine group, the **Scan only filters** do not apply to offline virtual machines or to virtual machine templates.



It is possible for two offline virtual machines to have the same domain and computer name. This will be the case if you clone a virtual machine and do not change either the computer name or domain on one or both machines. In this situation, of the two duplicate virtual machines, only the last one scanned will be visible in Machine View. The machines displayed in Machine View are keyed on domain and computer name and duplicates are not allowed.

- Virtual machines that are offline (powered off) will be mounted before they are scanned. Virtual machines that are online (powered on) do not need to be mounted as they are treated no differently than a physical machine.
- When performing a patch scan or an asset scan, a virtual machine that was added to a machine group as an offline virtual machine but that is online at the time of a scan will be scanned if it is hosted on an ESX server and if the **proper credentials** are available in order to access that machine. Online virtual machines that are hosted on workstations will fail to mount and will not be scanned.
- When performing a patch scan, all of the configured download sources in your vSphere Lifecycle Manager are honored.
- Upgrades of minor versions, such as from 7.0.1 to 7.0.2 are supported.
- When scanning or deploying to an offline virtual machine, **TCP Port 902** must be available in order for the virtual disk to be mounted.

- When scanning multiple offline virtual machines that are hosted on one workstation, it is possible to reach the connection limit for that workstation. If the connection limit is reached an error will occur and the scans will fail. The maximum number of simultaneous connections supported varies for each Windows OS.

Patch Deployments

- When deploying patches to an offline virtual machine that is hosted on a server, the virtual machine will be powered on, the patches installed, and the virtual machine powered down. See **Deploying Patches to Virtual Machines** for more details.
- When deploying patches to an offline virtual machine that is hosted on a server, VMware tools must be installed on the virtual machine.
- When deploying patches to an offline virtual machine that is hosted on a server, the following VMware server permissions are required in order to manage snapshots and to change the power state of the machine during the deployment process:
  - VirtualMachine.State.CreateSnapshot
  - VirtualMachine.State.RemoveSnapshot
  - VirtualMachine.Interact.PowerOn
  - VirtualMachine.Interact.PowerOff
  - VirtualMachine.Interact.DeviceConnection (to disable/enable the network card)

For offline virtual machines, patching products installed on virtual disks with the disk mode set to either **Independent – Persistent** or **Independent – Nonpersistent** is not supported. If a virtual machine has both dependent and independent disks, you can still install patches for products that are installed on the dependent disks.

- When deploying patches to an offline virtual machine that resides on a workstation, the new deployment job will overwrite any older deployment jobs that have not yet been performed. For this reason you should deploy all desired patches in a single deployment.
  Example: You deploy Patch A to a workstation-based offline virtual machine. The virtual machine is still offline a month later when you deploy Patches B and C. Because the first deployment job was never executed it gets overwritten and only Patches B and C are now scheduled for deployment. To avoid this you simply include Patch A along with Patches B and C in the second deployment job.
  One way to manage this is to use a patch group to define the patches you want deployed to your workstation-based offline virtual machines. When new patches are identified you simply add them to the list of patches in the patch group. This is particularly useful when specifying a patch group within a patch scan template and then choosing to automatically deploy missing patches on the **Run Operation** dialog. See **Creating a New Patch Scan Template** and **Automatically Deploying Patches** for more details about these options.

Agents

- Security Controls Agent operations are not supported on offline virtual machines.
- If you install Security Controls Agent on an online virtual machine and then later scan the virtual machine while it is in an offline state, Security Controls may report the wrong agent status for that image. For example, it may show that the agent is not installed, or it may let you attempt to uninstall the agent. This occurs because Security Controls Agent operations are not supported on offline virtual machines. The correct status will be reported once the virtual machine is brought back online and rescanned by Security Controls.

261. Notes About Virtual Machine Templates

General Notes

- For information on using virtual machine templates in patch scans, asset scans, and patch deployments, see **Roadmap of Tasks**.
- The type of virtual machine template (server template, workstation template, etc.) does not matter, they are all supported by Security Controls.
- Only virtual machine templates that are hosted on a VMware server are supported by Security Controls. The templates are added to a machine group using the **Hosted Virtual Machines tab**. Virtual machine templates that reside on **individual workstations** are not supported.
- A unique icon () is used to identify virtual machine templates. You will see this icon when adding a template to a machine group and when viewing scan results in **Scan View** and in **Machine View**.
- As with anything that involves components on a network, errors can occur if connections go bad, if servers are shut down, if a template is modified while being accessed by Security Controls, etc. In general, the templates should not be touched at any time during the scanning or patch deployment process.
- When you initiate a patch or an asset scan of a virtual machine template, Security Controls will scan the template in its current state and will report the results the same way it does for virtual machines and physical machines.
- During a scan, a template will be accessed using the **VMware server credentials**. Any individual credentials supplied for the template are ignored.
- You should supply online credentials for any virtual machine template that will be included in a patch deployment process. During the patch deployment process the template is converted to a virtual machine and powered on -- Security Controls will need the supplied credentials in order to access the online virtual machine.
- When scanning or deploying to an offline virtual machine template, **TCP Port 902** must be available in order for the virtual disk to be mounted.

Patch Deployments

- When deploying patches to a virtual machine template, the following VMware server permissions are required in order to manage snapshots and to perform the deployment:
  - VirtualMachine.State.CreateSnapshot
  - VirtualMachine.State.RemoveSnapshot
  - VirtualMachine.Provisioning.MarkAsTemplate
  - VirtualMachine.Provisioning.MarkAsVM

When you initiate a patch deployment to a virtual machine template, Security Controls will do the following:

1. Convert the virtual machine template to an offline virtual machine.
2. **(Optional)** Take a snapshot if the patch deployment template is configured to take a **pre-deployment snapshot**.
3. **(Optional)** Delete old snapshots if one of the **snapshot thresholds** defined on the patch deployment template is exceeded.
4. Push the patches to the offline virtual machine.
5. Reconfigure the following on the offline virtual machine:
   - Disable the network adaptor's **Connect at power on** option. This is done so that the machine is isolated from the network when the patch process is run.

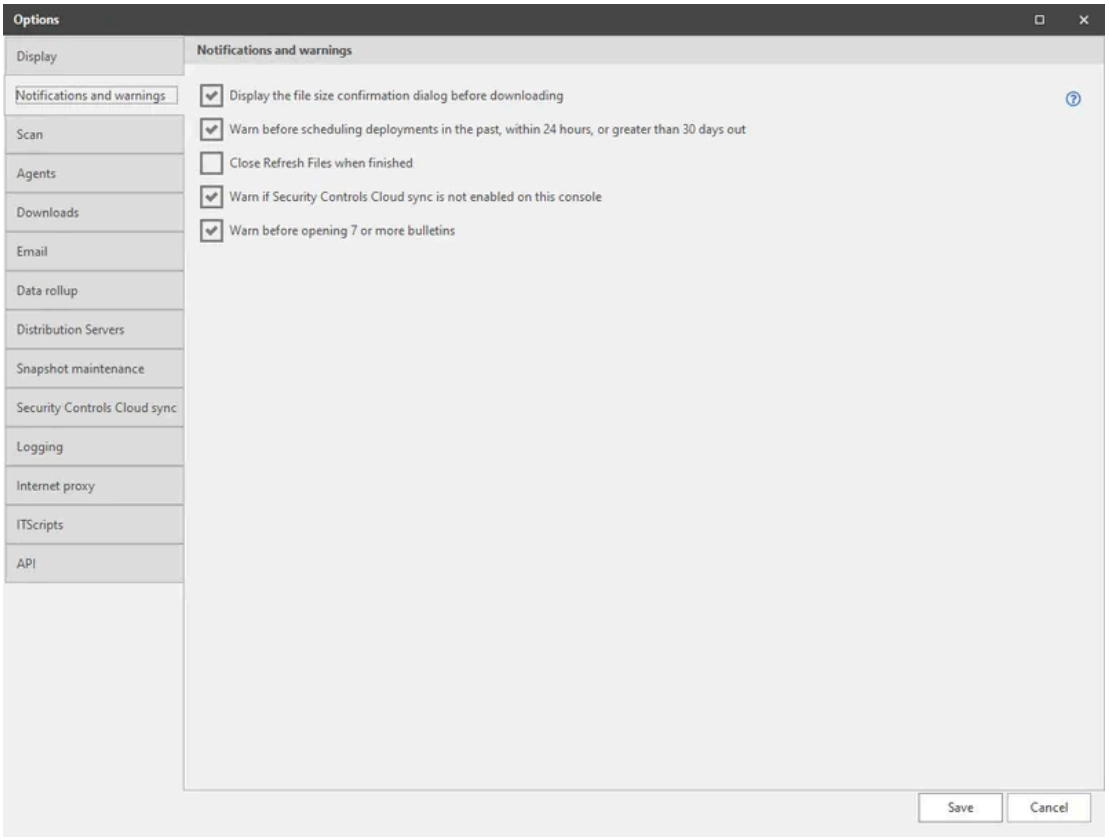
- If Sysprep is scheduled to run, disable it so it will not automatically configure the machine's operating system when the machine is first powered on.

Power on the virtual machine.

7. Install the patches.
8. Power down the virtual machine.
9. Reset the machine configuration to its original network connection and Sysprep settings.
10. **(Optional)** Take a snapshot if the patch deployment template is configured to take a **post-deployment snapshot**.
11. **(Optional)** Delete old snapshots if one of the **snapshot thresholds** defined on the patch deployment template is exceeded.
12. Convert the offline virtual machine back to a virtual machine template.
    - The patch deployment template you use must not specify the use of a distribution server. The offline virtual machine will be disconnected from the network and unable to download the patches from the distribution server.
    - The patch deployment template you use should not specify a pre-deploy reboot (the program will be unable to initiate the reboot because the machine will be offline) and it should always perform a post-deploy reboot (this is a "best practice" when deploying patches). For deployments to virtual machine templates it is recommended you use the **Virtual Machine Standard deployment template**.
    - During a patch deployment, a virtual machine template that may normally be available only to an administrator will become visible to other users. This is because during the patch deployment process the template is temporarily converted to a virtual machine and powered on.

262. Notifications and Warnings Options

The **Notifications and Warnings** dialog allows you to specify when you want Security Controls to inform you about potential operational issues.

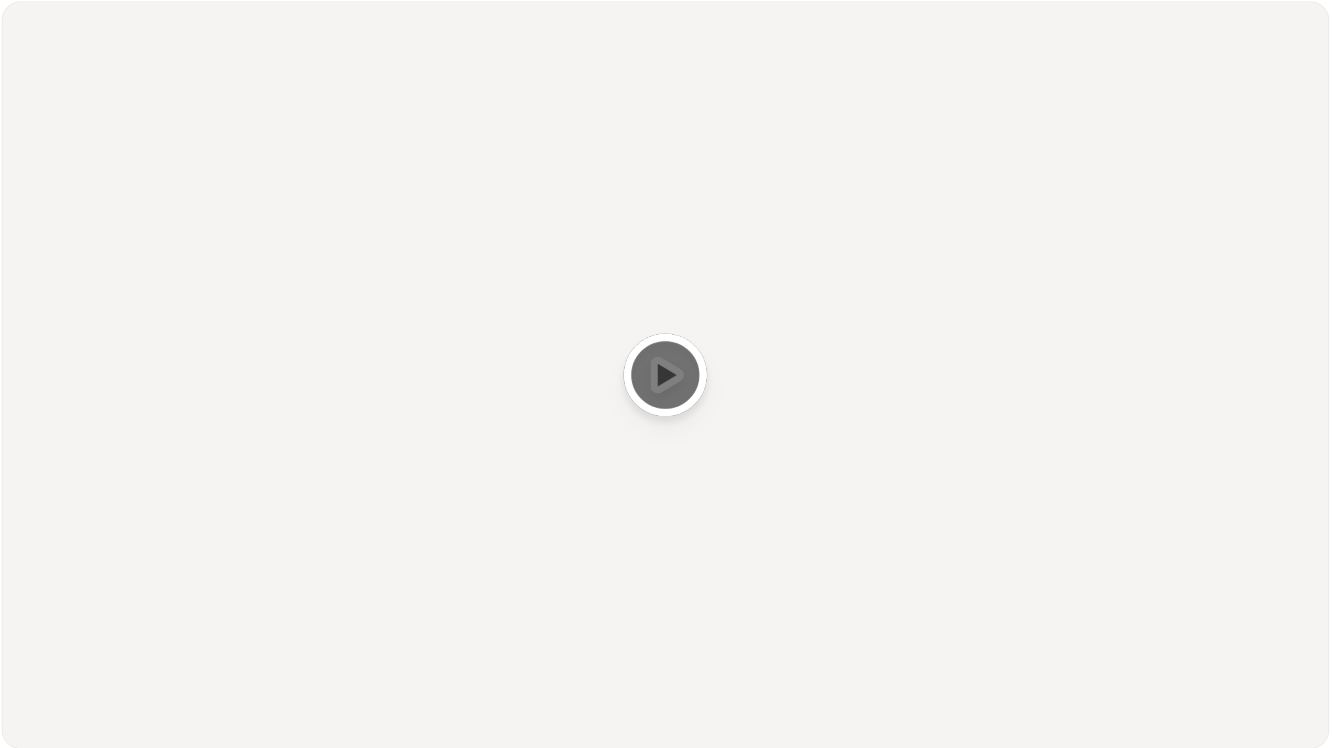


Field	Description
Display the file size confirmation dialog before downloading	Specify if you want the program to inform you of the file size of the patch before it is downloaded. You may want to enable this option if you have a low-speed Internet connection and you want the ability to cancel the download of particularly large files.
Warn before scheduling deployments in the past, within 24 hours, or greater than 30 days out	If enabled, will cause a warning dialog to be displayed anytime you attempt to schedule a patch deployment to run within in the past, within the next 24 hours, or more than 30 days out. The dialog is a reminder that the deployment may run immediately depending on the time zone of the target machine(s).
Close Refresh Files when finished	If enabled, whenever files are automatically refreshed within the program, the refresh dialog will close automatically. This affects the **Help > Refresh files** command and the **Import ITScripts** dialog that is displayed whenever you select **Manage > ITScripts**.
Warn if Security Controls **Cloud sync is not enabled on this console**	If you are using multiple Security Controls consoles, and if one of your consoles is using Security Controls Cloud sync and another is not, enabling this check box will notify you of this situation. This is especially important if two or more consoles are sharing the same database. Each console that uses a Security Controls Cloud sync-enabled policy must be **registered with Security Controls Cloud**.
Warn before opening 7 or more bulletins	If enabled, will cause a warning dialog to be displayed anytime you select seven or more patches and then use the right-click menu to **Open Bulletin(s) in Browser**. Opening many vendor bulletins at once may be a slow process and can degrade the performance of your machine.

263. Obtaining Support

For technical assistance with Security Controls, please refer to one of the following support options:

- View product documentation at **help.ivanti.com**



- Browse the **Ivanti Community Site (opens a new window)**
- Contact our Technical Support Team at **https://www.ivanti.com/support/contact**
- The Ivanti Security Controls Diagnostic Toolkit, which provides utilities to help diagnose your system and provide information to support, is available. See the **Security Controls Diagnostic Toolkit Release Notes (opens in a new window)** for more information.
- View the Security Controls **release notes (opens a new window)**

If you have a question or issue with Security Controls that requires help from our Technical Support staff, please see **How Do I Collect Data for Tech Support** before opening a support request or calling.

264. Ongoing Maintenance Tasks

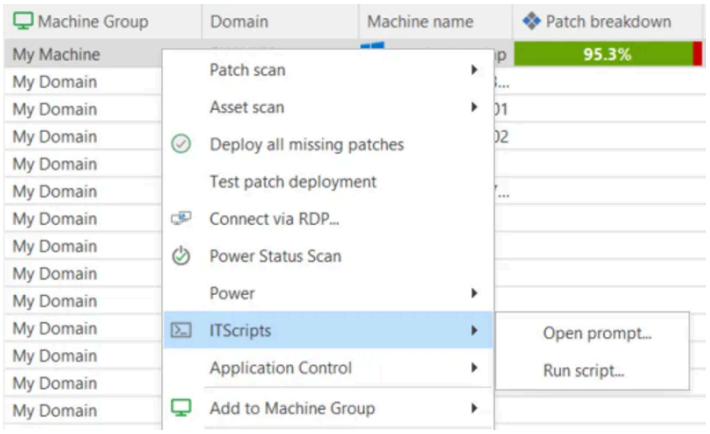
If the agents do not have Internet access, in most cases this means they will be downloading the latest engine components, data files and patch files from one or more distribution servers rather than from the default websites. In this case you will need to make sure the files on the distribution server(s) are updated on a regular basis. This can be done either automatically or manually. See **Synchronizing Servers** for complete details.

265. Opening a Windows PowerShell Prompt

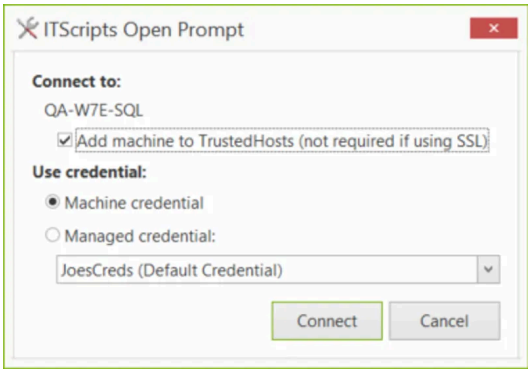
> The target machine must meet all PowerShell Remoting requirements; for details see **ITScripts Requirements**.

You can start a Windows PowerShell session with any single target machine. Doing so will enable you to execute PowerShell commands as an administrator on the target machine.

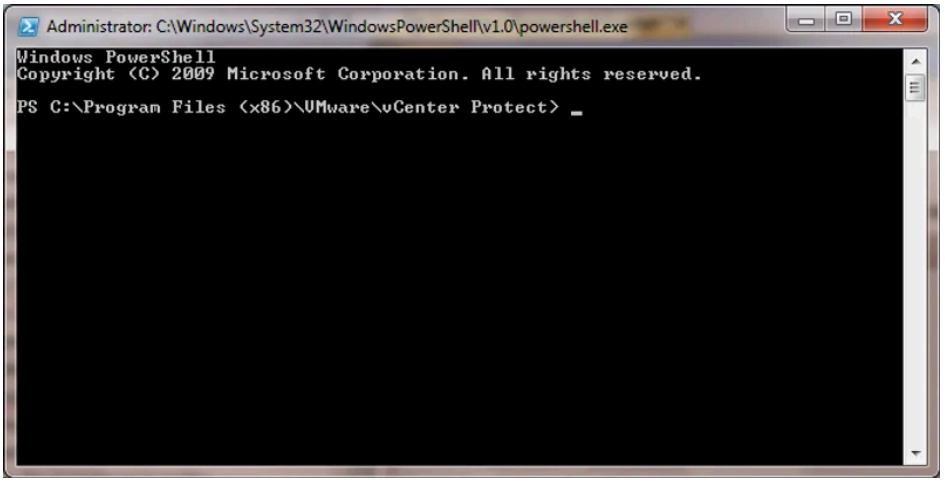
From either Machine View or Scan View, simply right-click the desired machine and select **ITScripts > Open prompt**.



You will need to provide the necessary credentials on the **ITScripts Open Prompt** dialog in order to make the connection. For credential information see **Defining Credentials**.



After making the connection the Windows PowerShell prompt is displayed.


Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
PS C:\Program Files (x86)\VMware\vCenter Protect> _

266. OperatingSystemFamily view

The Reporting2.OperatingSystemFamily view defines the operating system family.

Column Name	Data Type	Nullable	Description
Id	smallint		The operating system family id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(256)		Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.OperatingSystemFamily view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[OperatingSystemFamily]
```

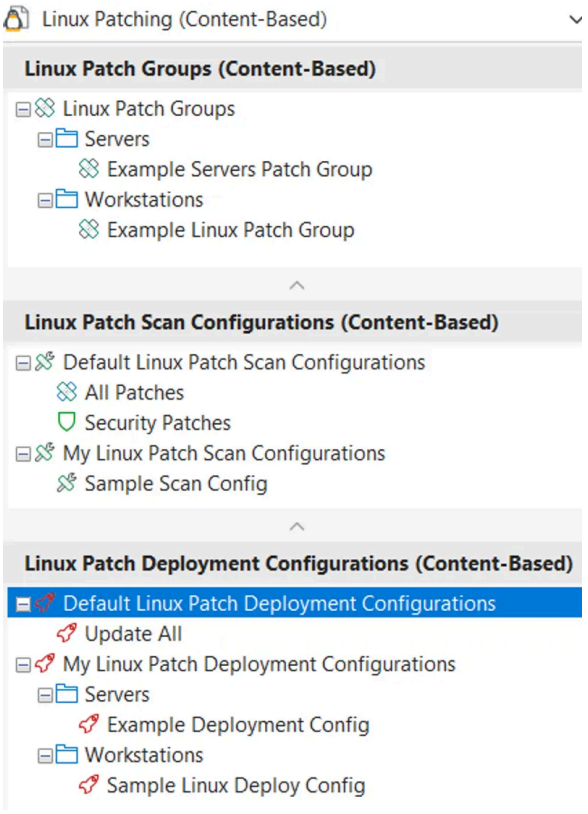
ID	Value	Description
0	Unknown	Invalid or Unknown type.
1	AIX	This is an AIX operating system.
2	Hpux	This is an HP-UX operating system.
3	Linux	This is a Linux operating system.
4	Mac	This is a MAC operating system.
5	Solaris	This is a Solaris operating system.
6	Windows	This is a Windows operating system.

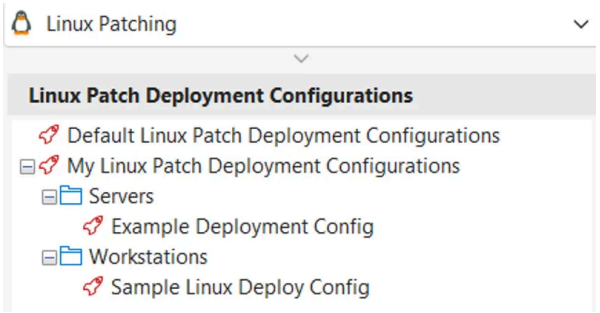
267. Organizing Linux Groups and Configurations

If you create many Linux patch groups, patch scan configurations and patch deployment configurations, you should consider organizing them into logical folders. Doing so will enable you to quickly locate and manage these items. You can create as many folders and sub-folders as needed within each list in the navigation pane.

> The lists available depend on if you are using **Linux Patching** ( ) or **Linux Patching (Content-Based)** ( ).

Sample Organizational Scheme





Content-Based - Contentless

To create a new folder:

In the **group**, **scan** or **deployment** configuration dialog, type a folder path into the **Path** box. You can specify as many folder levels as needed by using a backslash (\) to separate the levels in the name. The folder will be created when you save the group or configuration. If you do not specify a path, the item will be contained at the root level of the group or configuration list.

Folder path examples:

- \Servers
- \Workstations
- \Workstations\Location A
- \Workstations\Location B

To assign an item to a different folder, do one of the following:

> An item can belong to only one folder.

- In the **group**, **scan** or **deployment** configuration dialog, type a new folder path into the **Path** box.
- In the navigation pane, click and drag the item to a different folder.
- **Right-click the item** and select **Edit path**.

To assign a folder and its contents to a different folder:

- Click and drag the folder to another existing folder.
  The folder you move becomes a sub-folder.

To delete a folder, do one of the following:

- Change or remove the folder name in the **Path** box of all groups or configurations contained in that folder
- Click and drag the items to a different folder
- Delete all items contained in the folder path

The folder will be automatically deleted when the last item is removed from the folder.

268. Organizing Machine Groups

Show Me!

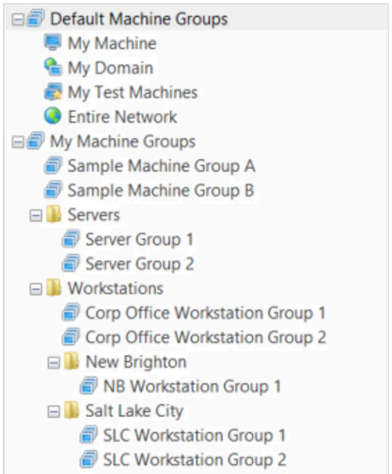
A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

If you create many machine groups, you should consider organizing the groups into logical folders. Doing so will enable you to quickly locate and manage your groups. You can create as many folders and sub-folders as needed within the **My Machine Groups** list in the navigation pane. For example, you might choose to organize your groups based on the types of machines they contain, by location, etc.

Sample Organizational Scheme



To create a new folder:

In the Machine Group dialog, type a folder path into the **Path** box. You can specify as many folder levels as needed by using a backslash (\) to separate the levels in the name. The folder will be created when you save the machine group. If you do not specify a path, the machine group will be contained at the root level of the **My Machine Groups** list.

Folder path examples:

- \Servers
- \Workstations
- \Workstations\Location A
- \Workstations\Location B

To assign a machine group to a different folder, do one of the following:

> A machine group can only belong to one folder.

- In the Machine Group dialog, type a new folder path into the **Path** box
- In the navigation pane, click and drag the machine group to a different folder
- Right-click the machine group and select **Edit path**

To assign a folder and its contents to a different folder:

- Click and drag the folder to another existing folder.
  The folder you move becomes a sub-folder.

To delete a folder, do one of the following:

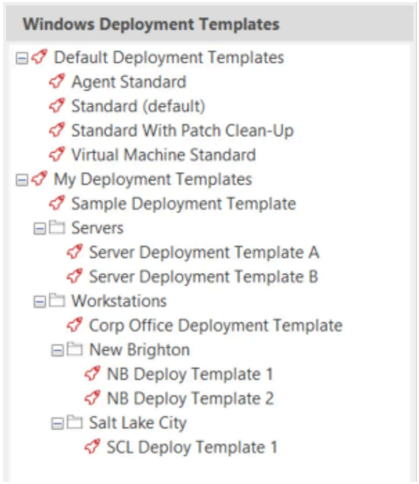
- Change or remove the folder name in the **Path** box of all machine groups contained in that folder
- Click and drag the machine groups to a different folder
- Delete all machine groups contained in the folder path

The folder will be automatically deleted when the last machine group is removed from the folder.

269. Organizing Patch Deployment Templates

If you create many patch deployment templates, you should consider organizing the templates into logical folders. Doing so will enable you to quickly locate and manage your templates. You can create as many folders and sub-folders as needed within the **My Deployment Templates** list in the navigation pane. For example, you might choose to organize your deployment templates based on the reboot requirements, by location, etc.

Sample Organizational Scheme



To create a new folder:

In the Deployment Template dialog, type a folder path into the **Path** box. You can specify as many folder levels as needed by using a backslash (\) to separate the levels in the name. The folder will be created when you save the template. If you do not specify a path, the template will be contained at the root level of the **My Deployment Templates** list.

Folder path examples:

- \Servers
- \Workstations
- \Workstations\Location A
- \Workstations\Location B

To assign a template to a different folder, do one of the following:

> A deployment template can only belong to one folder.

- In the Deployment Template dialog, type a new folder path into the **Path** box
- In the navigation pane, click and drag the template to a different folder
- Right-click the template and select **Edit path**.

To assign a folder and its contents to a different folder:

- Click and drag the folder to another existing folder.
  The folder you move becomes a sub-folder.

To delete a folder, do one of the following:

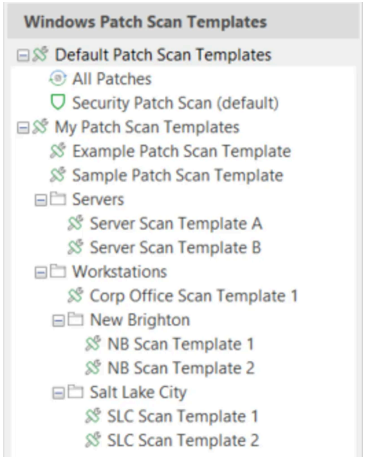
- Change or remove the folder name in the **Path** box of all patch scan templates contained in that folder
- Click and drag the templates to a different folder
- Delete all templates contained in the folder path

The folder will be automatically deleted when the last template is removed from the folder.

270. Organizing Patch Scan Templates

If you create many patch scan templates, you should consider organizing the templates into logical folders. Doing so will enable you to quickly locate and manage your templates. You can create as many folders and sub-folders as needed within the **My Patch Scan Templates** list in the navigation pane. For example, you might choose to organize your patch scan templates based on the type of machines that will be scanned, by location, by the vendors and products that will be scanned, etc.

Sample Organizational Scheme



To create a new folder:

In the Patch Scan Template dialog, type a folder path into the **Path** box. You can specify as many folder levels as needed by using a backslash (\) to separate the levels in the name. The folder will be created when you save the template. If you do not specify a path, the template will be contained at the root level of the **My Patch Scan Templates** list.

Folder path examples:

- \Servers
- \Workstations
- \Workstations\Location A
- \Workstations\Location B

To assign a template to a different folder, do one of the following:

> A patch scan template can only belong to one folder.

- In the Patch Scan Template dialog, type a new folder path into the **Path** box
- In the navigation pane, click and drag the template to a different folder
- Right-click the template and select **Edit path**.

To assign a folder and its contents to a different folder:

- Click and drag the folder to another existing folder.
  The folder you move becomes a sub-folder.

To delete a folder, do one of the following:

- Change or remove the folder name in the **Path** box of all patch scan templates contained in that folder
- Click and drag the templates to a different folder
- Delete all templates contained in the folder path

The folder will be automatically deleted when the last template is removed from the folder.

271. Output

Output that is written to the standard output stream will be written to the machine output file. If errors are detected by the Security Controls script engine, detailed error messages will be written to the machine error file.

We recommend that you explicitly format the output as you would like it to appear in the output file. If you do not explicitly format the output, the default formatter will be used. This will limit the fields that are output and the way in which they are presented.

It is particularly important to format output for scripts that are using PowerShell remoting. The default behavior for remote scripts is to serialize the script output objects on the target machine and deserialize then on the console. The deserialized objects are snapshots that have properties but no methods. You may get errors or unexpected results unless you explicitly format the output as strings.

There are several ways to format your output. Here are some of them.

- **Out-String:** Outputs a series of strings
- **Format-List:** Formats the output as a list of properties with each property on a new line
- **Format-Table:** Formats the object as a table
- **Format-Wide:** Formats objects as a wide table that displays only one property of each object
- **Select-Object:** Select the properties you want to output and optionally change the property names. This allows you fine control over what is output.
- **Export-CSV:** Save the output as a CSV file. You can output to a temporary file, then use Get Content to write it to the standard output.

The following example retrieves a list of services, and then creates CSV output of the computer name, status, service name, and display name.

Bash

```
$fn = [io.path]::GetTempFileName()
Get-Service -ComputerName "$ST_ComputerName" | select-object
@{Name="ComputerName"; Expression={$ST_ComputerName}}, Status, Name,
DisplayName | export-csv "$fn" -notype
get-content $fn
remove-item $fn
```

272. Overview of Linux Patch Management

> Only those Linux machines that meet the minimum requirements are eligible to be scanned and patched by an agent. See the **System Requirements** for complete information.

Linux machines are scanned and patched using agents. The process depends on whether you are using the new contentless Linux patching method or the old content-based method. See **Linux Contentless Patching** for information about this change.



1. Identify your Linux machines.
    - If you know the identities or whereabouts of all your Linux machines, you can **create a Linux machine group**.
    - If you are unsure about the identities and locations of all your Linux machines, perform a **power status scan** on the **My Domain** or **Entire Network** group. The scan will identify the OS type of each machine in the group and your Linux machines will be displayed on the **Linux patch** tab in **Machine View**.

Create one or more Linux patch groups and configurations.

- Create a **Linux patch group**: This is optional but can give you greater control over your scans and deployments, enabling you to scan for (content-based only) or deploy a particular set of patches. You create separate patch groups for contentless Linux patching and for content-based Linux patching.
- Create a **Linux patch scan configuration** (content-based only): You use this configuration to specify exactly how your Linux machines will be scanned. Contentless patching always performs a patch scan for all missing patches before any deployment method so does not require a patch scan configuration.
- Create a **Linux patch deployment configuration**: You use this configuration to specify exactly how patches will be deployed to your Linux machines. You create separate patch deployment configurations for contentless Linux patching and for content-based Linux patching.

Create one or more **agent policies**.

4. An agent policy defines exactly what an agent can or cannot do. You will create one or more Linux patch tasks in the agent policy. In each task, you specify when the task will run on an agent machine and which configurations should be used during the scan and deployment processes.

> It is perfectly fine to mix Windows tasks and Linux tasks in the same agent policy. Windows tasks will be ignored by your Linux machines, and vice versa.

Install the **agent policy**.

> Each Linux target machine must be properly configured before you can perform a push install of an agent. See **System Requirements** for more details.

One option is to perform a "push install" of the agent from the Security Controls console. You can do this a couple of different ways:

- Within your Linux **machine group**, select the machines in the bottom pane and then click **Install / Reinstall agent**.
- In **Machine View**, right-click the Linux machines and install the desired agent policy.
  If you performed a power status scan on your Linux machines, you can also perform this step from the **Results list** in the navigation pane.

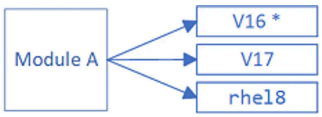
Another option is to manually install an agent on each of your Linux machines. For details, see **Manually Installing Agents**.
Use the agent.
The agent will automatically perform its tasks and **report the results to the console**. You can use Machine View or Scan View to **manage the machines that are running an agent policy**. If you want to manually control the agent, you do so using a command line utility. For details, see **Using an Agent on a Target Machine**.

> When a Linux agent needs to deploy a patch, it does so using Yellowdog Updater, Modified (YUM). YUM is a command-line utility that is used for retrieving, installing and managing RPM packages. If you have Linux client machines that reside in a disconnected network, the agent will not be able to utilize YUM and you must **set up one or more local repositories**.

Modules and versions

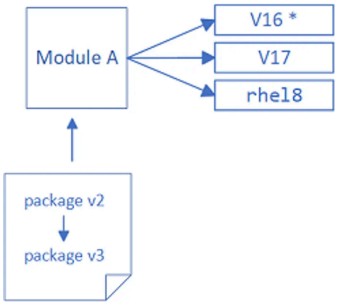
You can't always install the latest version of a package on a Linux machine.

For Red Hat Linux and distributions derived from Red Hat, a machine may have modules installed that have several streams, only one of which can be enabled on a machine.



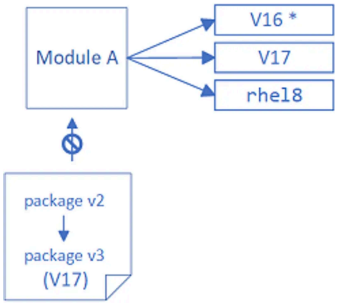
module A has three streams, only one of which is enabled on the machine

Consider the case where an advisory wants to update a package in one of these types of module.



Update a package within a module that has several streams

If the new version of the package is for a specific stream that differs from the enabled stream on a machine, then the updated package is incompatible and cannot be installed. As a result, a later version of a package for a module will be available than the version that can be installed on a machine.



The new package depends is for a different stream of the module than the enabled stream on the machine, so the new package cannot be installed

Similarly, it may appear that the latest package hasn't been installed because of module dependencies. For example, the module `perl-DBD-SQLite` appears to have several module updates for the `perl-DBD-SQLite` package:

- `perl-DBD-SQLite-0:1.58-2.module+el8.1.0+2940+55ca6856.x86_64`
- `perl-DBD-SQLite-0:1.58-2.module+el8.1.0+2940+f62455ee.x86_64`
- `perl-DBD-SQLite-0:1.58-2.module+el8.2.0+4265+ff794501.x86_64`
- `perl-DBD-SQLite-0:1.58-2.module+el8.6.0+13408+461b4ab5.x86_64`

However, each of these packages has a dependency on a specific perl stream. The first can be installed only when perl:5.24 is enabled, and the last only when perl:5.32 is enabled, so it may be that what appears to be the latest version of a package cannot be installed on a specific machine.

273. Overview of the Solution

A process is available for you to use your own CA to generate a new authority certificate and replace the default self-signed root certificate created by Security Controls. The authority certificate that you generate will in turn be used to issue console, agent and scheduler certificates for Security Controls.

Major steps in the process

Here are the major steps for using your own CA to issue a new certificate:

1. Issue a new sub-authority certificate from your CA.
   For details on performing this step, see **How to Issue a New Certificate**.
   - If your CA is accessible over the network, you can use your local system facilities to create the new certificate. If you are using a Microsoft CA infrastructure, use the Subordinate Certificate Authority certificate template when creating the certificate.
   - If your CA is on a disconnected network, you will use the STMgmt command-line tool to request and then accept the new sub-authority certificate.

Let the new certificate work its way through Security Controls.
For details on this step, see **Let the New Certificate Percolate Through the System**.

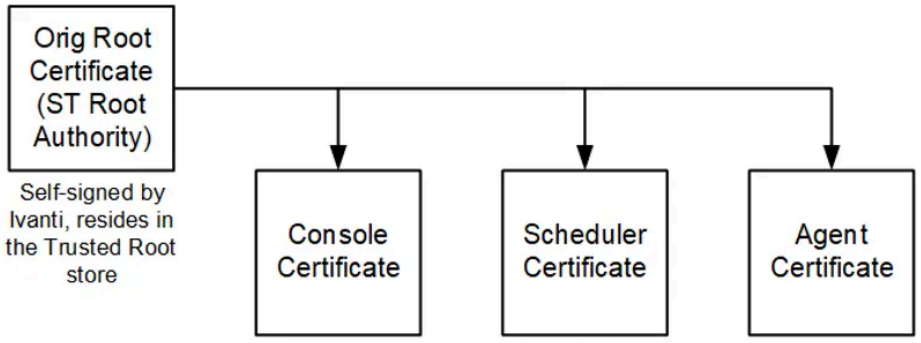
3. Commit the new sub-authority certificate.
   For details on performing this step, see **Commit the New Sub-Authority Certificate**.
4. Test and verify that new console, scheduler and agent certificates are in place.
   For details on performing this step, see **Testing for and Verifying the New Certificate**.

Before and after views of your certificate environment

The following diagrams illustrate the state of the Security Controls certificates as originally installed and after using your own CA to issue new certificates.

As originally installed with Security Controls

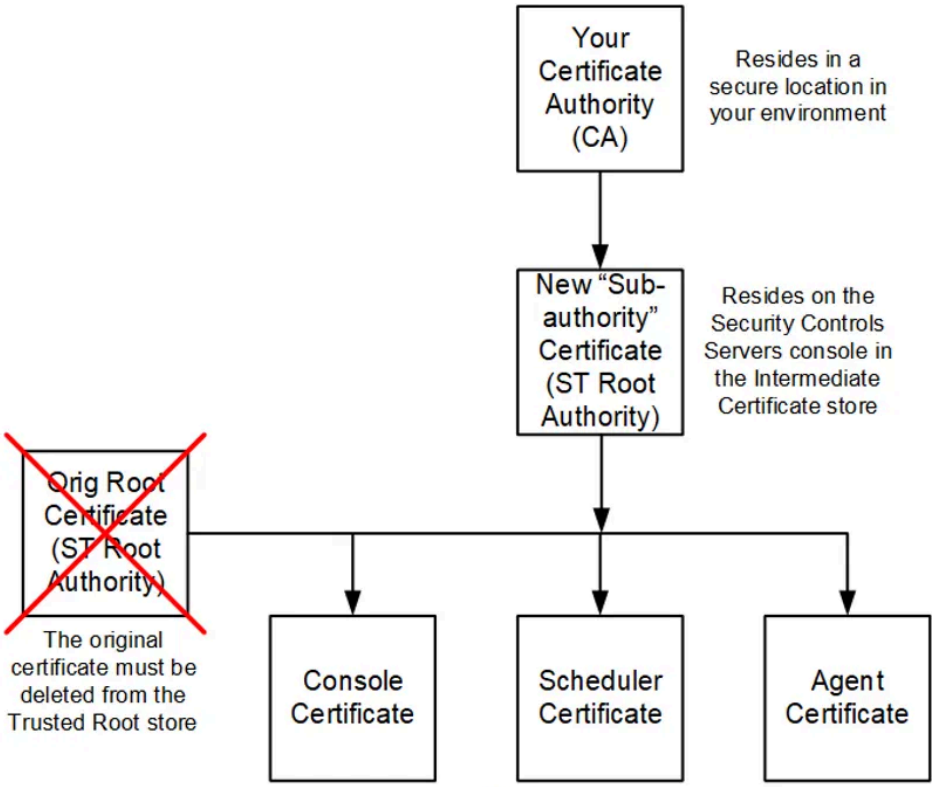
Here is the relationship of the certificates after initially installing Security Controls. The console, scheduler and agent certificates are all issued by the self-signed root certificate.



- The console certificate resides on the Security Controls Servers console in the computer account's Personal store.
- The deployment tool certificates reside in the /ProPatches/Scheduler directory.
- On agent machines, the console certificate and the agent certificate reside in the Ivanti Security Controls Agent store.

After using a trusted CA to issue a new authority certificate

Here is the relationship of the certificates if you choose to issue a replacement certificate using your own CA. In Ivanti parlance, the new certificate that is issued by your CA is known as a *sub-authority*. A total of four unique certificates will be issued during the entire process. Your CA will issue a sub-authority certificate, and the sub-authority certificate will in turn issue a console certificate, a scheduler certificate and (if you use agents) an agent certificate. Multiple scheduler and agent certificates may exist, one for each scheduler and one for each agent you install.



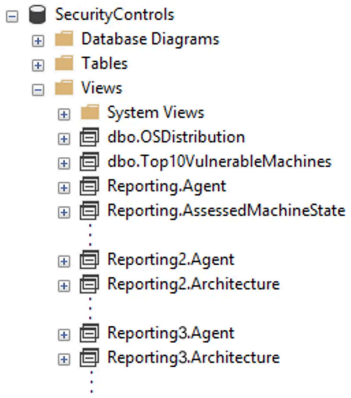
- The console certificate resides on the Security Controls Servers console in the computer account's Personal store.
- The deployment tool certificates reside in the /ProPatches/Scheduler directory.
- On agent machines, the console certificate and the agent certificate reside in the Ivanti Security Controls Agent store.

274. Versions of Database Views

The following sections describe the database views that can be used within a custom query. Each view provides information about the current known state of machines, focusing on patch assessments. The name of each SecurityControls view begins with Reporting.

There are different versions of the database views available, some of which are intended only for legacy queries:

- `Reporting.*` views contain information about Windows data only and are for legacy queries only
- `Reporting2.*` views contain information about Windows and content-based Linux data
- `Reporting3.*` views contain information about Windows and contentless Linux data



275. Overview of the PowerShell Command-Line API

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

The API feature is meant for advanced users who have a working knowledge of PowerShell and who want to perform tasks beyond those available through the Security Controls user interface. The feature exposes the Security Controls API stack, enabling you to execute API-level calls from the command-line or from a PowerShell console. You can use the API feature to:

- Interact with different systems in your environment.
- You are now able to integrate your patching and power state processes with items such as vulnerability scanners, password management tools, SQL Server clusters and orchestrators such as Chef or Puppet.
  Script a sequence of complex events that contain dependencies.
- Using PowerShell, you can script out interesting and complicated workflows. You can include checks within the script to make sure that everything goes according to plan. For example, you might patch one machine in a cluster and make sure that everything goes according to plan before proceeding with the other machines in the cluster.
  You might also script out actions such as suspending nodes, starting and stopping services at certain points, restarting machines in a specific order, etc.
  Perform bulk operations or process list inputs from other systems.
- For example, you might dynamically perform a scan operation by targeting systems listed in a file.
  Programmatically stage patch deployments or initiate patch downloads.

Related Topics

PowerShell API Requirements

How to Get Started

How to View Detailed Help Information About the PowerShell Commands

Tips and Tricks

Use Examples

Frequently Asked Questions

276. Overview of REST API

The REST API allows for remote access and control of the Security Controls console. The feature provides a simple RESTful interface with lightweight JSON-formatted responses that enables you to read and write data to/from the program. It allows you to automate many of your day-to-day operations, saving you considerable time and effort. The REST API allows you to fully integrate Ivanti Security Controls into your orchestration and automation systems.

For complete information, see **https://help.ivanti.com/iv/help/en_US/isec/API/Topics/Welcome.htm**.

Show Me!

Two video tutorials are available on this topic. To access the videos, click the following links:




ivanti

277. Available Reports

The following reports are available in Security Controls. The reports you have access to is dependent upon your current license level. The reports in the **Machine** and **Patch - All Platforms** categories apply to all platforms, providing access to both Windows reports and Linux reports. The reports in the other categories apply only to Windows machines.

> For information on using Security Controls database views to generate your own custom reports, please see **Introduction to Database Views**.

To choose a report, select **Tools > Create report** from the main menu and then select a report from the list in the left pane of the **Reports dialog**.

Category	Report	Description
Machine		
	Detailed License Status	This report lists license seat information, including the number of licensed seats, the number of seats used, how and when the seats were consumed and when they will be available again.
	Machine/OS Listing	This report lists the operating systems for each machine scanned.
	Seat License Status	This report provides information about the number of license seats available and the number of seats used. There is no filtering capability for this option.
	Power Status Report	This report provides a list of machines and their power state at a specific time. The report is organized by machine group.
Patch - All Platforms		
	Deployment Status by Machine	This report provides information about patch deployments made to one or more specified machines.
	Executive Summary	This report provides a high-level summary about the patches and the machines discovered by the scan.
	Machine Patch Status Summary	This report provides the patch status of each machine discovered by the scan.
Patch - Windows Only		
	Condensed Patch Listing	A concise, six-column report displaying the machine name and patch status for each scanned host. Patch items are displayed as bulletin numbers (MS00-000).
	Deployment Detail	This report provides detailed information about a particular patch deployment.
	Deployment Percentage by Patch	This report displays the percentage of machines that have each patch installed. The percentage is based on the number of machines that require the patch.
	Deployment Status by	This report provides information about the success or failure of one or more specified patch deployments.

Category	Report	Description
	Deployment	
	Deployment Status by Machine	This report provides deployment information specific to one or more machines.
	Detailed Summary	This report shows a summary of the scan, plus it provides a list that shows each machine that was scanned and detailed information about each machine.
	End-of-Life by Product	This report shows all detected end-of-life products and the machines that have them installed.
	Executive Summary	This report provides a high-level summary about the patches and the Windows machines discovered by the scan.
	Machine Inventory	This report provides a complete list of all software products installed on each machine discovered by the scan.
	Machine Status by Patch Count	This report displays the number of machines in groups based on the number of missing patches.
	Machine Status Summary	This report displays the status of machines in the selected database.
	Machines by Patch	Displays patch status for each machine sorted by Bulletin ID and QNumber.
	Machines Not Scanned	This report lists all machines not scanned and the reason they were not scanned.
	Missing Product Level	This report is a quick overview of all machines that are missing product levels for supported products. This report skips the simple criteria filter and displays the advanced criteria filter immediately.
	Patch Annotation Information	This report lists all patch annotations.
	Patch Listing	A concise listing (one line per patch processed) of all patches for all scanned machines sorted by 'Missing', 'Found', 'Informational' and 'Warning', then sorted by user preference.
	Patch Status Detail	This report provides detailed information about each patch discovered by the scan.
	Patch Status Summary	This report provides a descriptive summary about each patch discovered by the selected scan(s). The report includes both found and missing patches. Use the Next Page and Previous Page icons to navigate through the report.

Category	Report	Description
	Patches by Machine	Displays patch status for each machine sorted by machine name.
	Patches by Machine Detail	A detailed listing of every patch found sorted by machine name. For each patch, the entire summary and reason is listed in the report. Note that this report can take very long if executed against thousands of computers.
	Top Ten Missing Patches	This report lists the ten patches that are missing the most often.
	Top Ten Vulnerable Machines	This report lists the ten most vulnerable machines discovered by the program during the selected scan(s). The machines with the most missing patches and product levels are judged to be the most vulnerable.
Patch - Windows IAVA		
	Deployment Percentage by Patch (IAVA)	(Available only if you have a Government Edition of Security Controls.) This report displays the percentage of machines that have each patch installed. The percentage is based on the number of machines that require the patch.
	Detailed Summary (IAVA)	(Available only if you have a Government Edition of Security Controls.) This report gives a detailed scan summary.
	Machine Compliance (IAVA)	(Available only if you have a Government Edition of Security Controls.) This report gives IAVA machine compliance information.
	Machine Non-Compliance (IAVA)	(Available only if you have a Government Edition of Security Controls.) This report gives IAVA machine non-compliance information.
	Machine Status by Patch Count (IAVA)	(Available only if you have a Government Edition of Security Controls.) This report displays the number of machines in groups based on the number of missing patches.
Asset - Windows Only	**Patch Status Detail (IAVA)**	(Available only if you have a Government Edition of Security Controls.) This report gives detailed patch status information.

Category	Report	Description
	Machine Hardware Detail Report	This report provides a detailed list of hardware assets on each machine.
	Machine Software Detail Report	This report provides a detailed listing of software installed on each machine.
	Software Catalog Report	This report provides a list of all software installed on the scanned machines. The version number and install count information is displayed for each software product that is detected. If multiple versions of a product are detected, the machines using a particular version are listed in multiple columns.

278. Overview of the Custom Patch XML Process

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

> CAUTION! Creating and using custom patch XML files should only be attempted by experienced administrators. Creating and deploying inaccurate custom patches may have seriously adverse effects on the performance of the programs in use at your organization.

Security Controls provides the ability to scan for and deploy patches not supported in the primary data definition file. It does this by allowing you to create your own custom patch XML files that contain the information about the additional patches and products you want to support. Security Controls will then combine your custom XML files with the primary data file and use that modified file when performing scans and deployments.

Within each **custom XML file** you can define multiple custom products, bulletins, and patches.

- **Custom product**: A product not currently supported by the primary XML patch data file. For example, you might have a product that was developed strictly for use within your organization.
- **Custom bulletin**: Used to announce and describe a security update. A custom XML file can contain multiple bulletins, and each bulletin can contain multiple patches. Some of the information typically included in a bulletin includes a summary, known issues, a list of all affected software, and a link to the security update (patch) file. Of course, in this case the patch is contained in the same XML file as the bulletin.

- **Custom patch**: A software update that is not currently supported by the primary data definition file. A custom patch can be applied to either an existing product or to a custom product. For example, you might receive a special private patch from a vendor, you might create your own patch to a vendor's product, or you might create a patch for your own custom product.

One major difference between a regular patch and a custom patch is that you cannot download a custom patch to the patch download directory in advance of a deployment. Rather, you must make the patch available by manually copying the patch to all expected locations (typically to the console as well as any distribution servers).

If you are using agents to deploy custom patches, be certain you enable the **Use Server by IP Range** check box on the deployment template used by the agents. Custom patches cannot be downloaded from a vendor and the agents must therefore be able to download the custom patches from one or more distribution servers. See **Deployment Template: Distribution Servers Tab** for more information.

279. Patch view

The Reporting2.Patch view displays patch information.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Bulletin	nvarchar(255)		The patch bulletin.
ONumber	nvarchar(255)		The ONumber.
BulletinTitle	nvarchar(255)	X	The patch bulletin title.
VendorSeverityId	int	X	The minimum vendor severity of the patch. See [Reporting2].[VendorSeverity].
IsCustomPatch	bit		Indicates if this is a custom patch.
PatchTypeId	int	X	The patch type id. See [Reporting2].[PatchType].
ReleaseOn	datetime	X	The date this patch was released.
lavaID	nvarchar(50)	X	The unique lava identifier.

280. PatchAppliesTo view

The Reporting2.PatchAppliesTo view identifies the products and CVEs that a patch applies to.

Column Name	Data Type	Nullable	Description
PatchId	int		The patch id.
ProductId	int		The product id. See [Reporting2].[Product].
CveId	int	X	The cve id. See [Reporting2].[Cve].

281. PatchCountsByScanMachine view

The Reporting2.PatchCountsByScanMachine view displays patch scan information.

Column Name	Data Type	Nullable	Description
PatchFoundOrInstalled	int	X	Indicates if the patch was found or installed on the machine.
PatchMissing	int	X	Indicates if the machine was missing the patch.
ProductLevelMissing	int	X	Indicates if the machine was missing the product level.
AssessedMachineStateId	int		The state of the machine being assessed. See [Reporting2].[AssessedMachineState].

282. PatchDeployment view

The Reporting2.PatchDeployment view displays Windows patch deployment information.

Column Name	Data Type	Nullable	Description
DeployId	int		Identifies the deployment associated with this patch.
DetectedPatchStateId	int		The detected patch state id. See {Reporting2].[DetectedPatchState].
DeployScheduledOn	datetime	X	The date the patch was scheduled for deployment (local time).
DeployStartedOn	datetime	X	The date the patch installation started (GMT).
DeployEndOn	datetime	X	The date the patch installation ended (GMT).
DeployStateId	int		The deployment status Id. See [Reporting2].[DeployState].
ResultCode	int	X	The result code from a patch deployment. Common result codes are: • 0: Installed, no reboot required • 3010: Installed, reboot required Other error codes are patch specific.

Content

You can run the following query to display DisplayStateID values and descriptions.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[DeployState]
```

283. PatchScan view

The Reporting2.PatchScan view displays assessment information.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
ConsoleName	nvarchar(100)		The console name where this patch was performed.
DefinitionDate	datetime	X	The assessment data definition.
DefinitionVersion	nvarchar(23)	X	The assessment data definition version.
EndedOn	datetime		The date the assessment ended.
IsScanComlete	int		Determines if the scan is complete. • Value = 0 indicates the scan is not complete • Value = 1 indicates the scan is complete
Name	nvarchar(255)	X	The scan name.
StartedOn	datetime	X	The date the scan started.
ScanTemplateName	nvarchar(255)	X	The scan template name.
User	nvarchar(256)	X	The name of the user that performed the scan.
SourceTypeId	Tinyint		The source type ID. See **[Reporting].[SourceType]**.
ScanTypeId	Tinyint		The scan type ID.

284. PatchType view

The Reporting2.PatchType view defines Windows patch types.

Column Name	Data Type	Nullable	Description
Id	int		The patch type id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.PatchType view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[PatchType]
```

ID	Value	Description
0	Security Patches	Microsoft Security Patches
1	Security Patches	
2	Software Distribution	
3	Security Tools	
4	Non-Security Patches	
6	Custom Actions	

285. Patch Deployment Overview

Security Controls allows local and remote patch deployment via a few simple mouse clicks. From one management console you can deploy missing patches and product levels to a single machine or to many machines.

> Product levels should be applied before all patches. For this reason Security Controls will not allow you to deploy product levels and patches in the same deployment.

> If you deploy a patch to a specific SQL Server instance, the patch is applied to all instances on that machine.

Patch Deployments Are Performed As Background Tasks

All patch deployments are performed as background tasks, regardless of how they are initiated. In other words, the deployment is launched as its own separate Windows task. This means you can initiate a patch deployment and then move on to other concurrent work within Security Controls without having to wait for the deployment to complete. This also means you can have multiple patch deployments active at the same time.

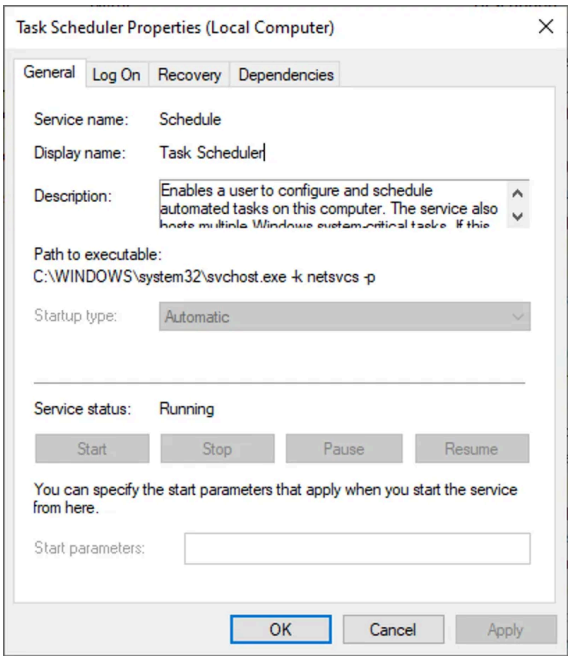
Deployment Considerations

- Is there a practical limit to the number of deployments you can have active at the same time?
- Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch downloads, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Security Controls starts responding slowly.
  Is there a problem if the same machine is included in two or more concurrent deployments?
- You should avoid concurrent deployments to the same machine. Exactly what will happen is dependent on a number of issues. The second deployment may overwrite the patch files already deployed, it may fail if the files are currently in use by the first deployment, or it may fail if the first deployment reboots the machine while the second deployment is still in progress.
  How will I know when a deployment is complete?
  The **Operations Monitor** will display the status of the patch deployment. From the Security Controls console's perspective, the deployment is complete when all necessary files have been copied to the target machine and the deployment is scheduled.

286. Patch Deployment Prerequisites

In addition to the scanning prerequisites, the following are required in order to successfully deploy patches to target machines:

- The Windows Update service must not be disabled; rather, it must be set to either **Manual** or **Automatic** in order to successfully deploy patches. In addition, the Windows Update setting on each target machine (**Control Panel > System and Security > Windows Update > Change settings**) should be set to **Never check for updates**.
- The machine credentials that you supply are used to provide access to the remote machine and to push the necessary patch deployment files. See Credential Precedence for information on what occurs if machine credentials are not supplied. The actual deployment, however, will be run under the remote machine's Local System account.
- A scheduler is required on the machines being patched to ensure a successful deployment. You may need to enable the Windows Task Scheduler on the machines being patched. On most Windows machines you can access the Task Scheduler by selecting **Start > Administrative Tools > Services** and then right-clicking **Task Scheduler**.



287. Patch Deployment Security

Security Controls takes the security of patch deployment very seriously. To that end, each patch undergoes up to three signature validation checks and is stored in a location on the remote machine with tight security permissions. If any of the signature checks fail, the patch will not be deployed.

During deployment, when a patch is copied to a remote system, the copy is not initiated unless the patch is signed. This is to prevent someone from tampering with the copy of the patch stored in the patch download directory. Before a patch is pushed out, it is always checked for a valid signature to ensure you are getting a legitimate patch.

Once the patch is copied to the deployment target it might sit for a period of time for a scheduled deployment. To prevent someone from tampering with the patch, the signature is checked again before deploying on that machine. Additionally, the patch directory that Security Controls creates on the remote machine has permissions set to LOCALSYSTEM and Local Administrators only so other users will not be able to modify, add or remove files from the deployment directory.

288. Patch Downloads Are Performed As Background Tasks

All patch downloads are performed as **background tasks**, regardless of how they are initiated. In other words, the download is launched as its own separate Windows task. This means you can initiate a patch download and then move on to other work within Security Controls without having to wait for the download to complete. This also means you can have multiple patch downloads active at the same time.

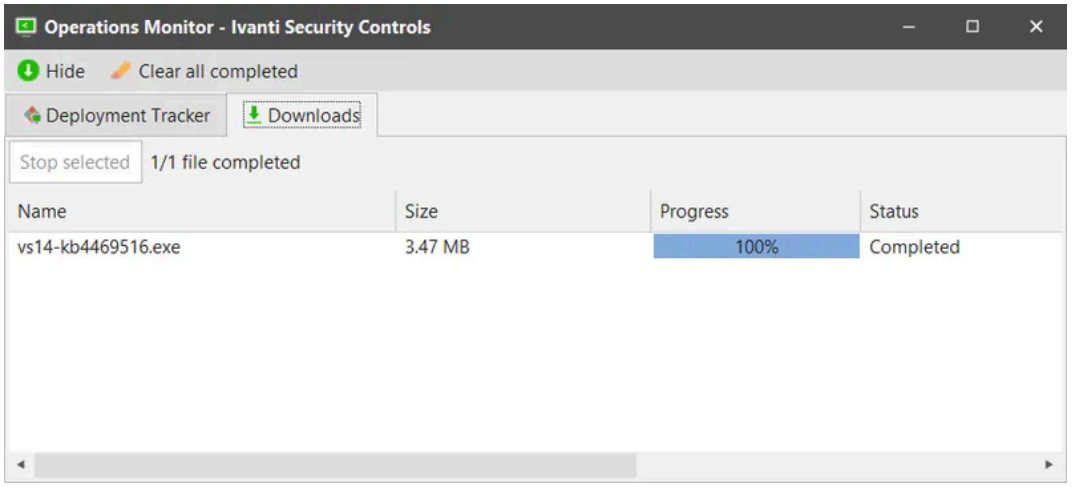
Download Considerations

- Is there a practical limit to the number of patch downloads you can have active at the same time?

  Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch scans, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Security Controls starts responding slowly.

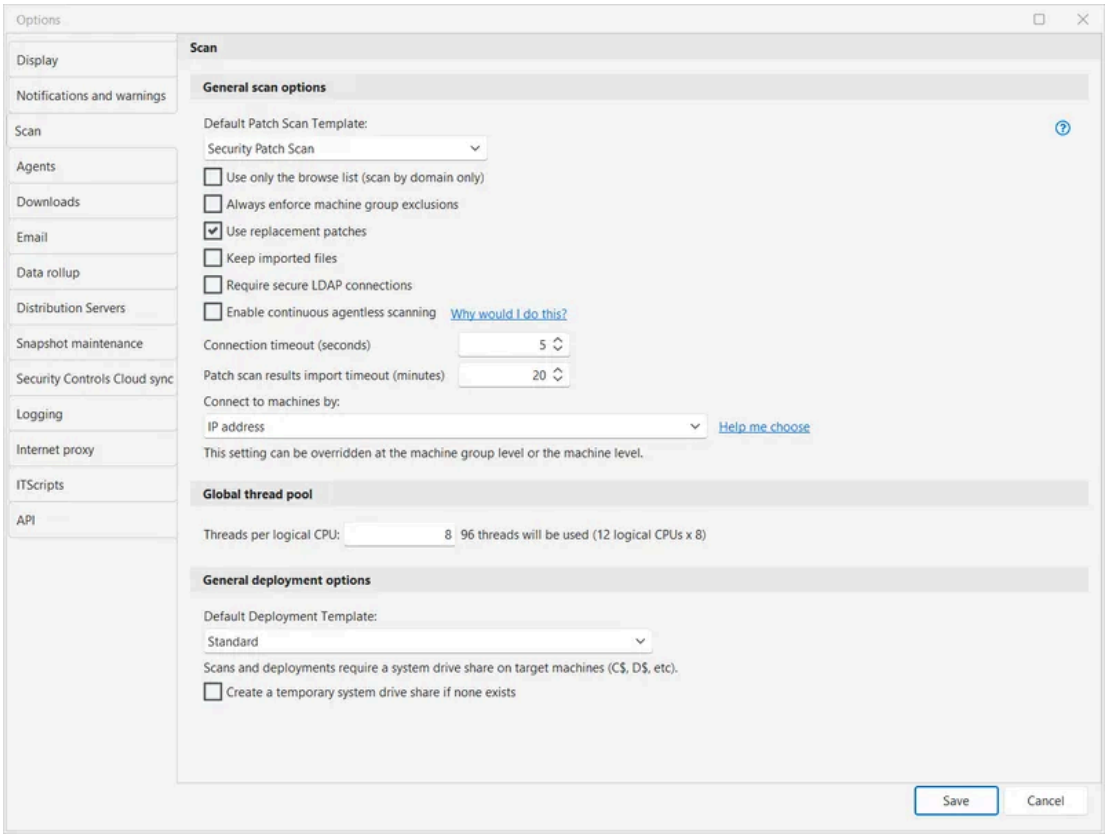
- How will I know when a download completes?

  The **Operations Monitor** will display the status of the patch download.



289. Scan Options

The **Scan Options** dialog allows you to specify patch scanning and deployment options.



Field	Description
Default Patch Scan Template	The **scan template** you wish to set as the default when performing patch scans.
Use only the browse list (scan by domain only)	When scanning domains, the machines scanned are those contained in the "browse list" of machines in your Microsoft network rather than all the machines in the domain as specified by the domain controller. Using this option will typically reduce the number of machines that the program will attempt to connect to when performing the scan. For more information, see **Discovering Machines**.
Always enforce machine group exclusions	When using multiple machine groups in a scan operation, if a machine is **excluded** from one machine group but is included in another, the machine will be excluded from the operation. If the **Always enforce machine group exclusions** check box is not enabled, for this same situation the machine will be included in the operation. **Examples:** • On the **Agentless Operation page** you select two machine groups that you want to scan. MachineA is excluded from one group but is included in the other group. If the **Always enforce machine group exclusions** check box is enabled, MachineA will not be included in the scan. If the **Always enforce machine group exclusions** check box is not enabled, MachineA will be included in the scan. • You scan a **nested group** that consists of two groups. In one of the groups the domain ABC.com is excluded, while the other group contains three machines from the ABC.com domain. If the **Always enforce machine group exclusions** check box is enabled, the three machines will not be included in the scan. If the **Always enforce machine group exclusions** check box is not enabled, the three machines will be included in the scan.
Use replacement patches **Keep imported files**	Instructs Security Controls to only scan for patches that are not replaced, ignoring patches that have been replaced by other patches. For example, instead of reporting on all missing Internet Explorer patches, only the latest and most current IE patches will be reported. The results files used by a scan operation are stored on disk indefinitely rather than being deleted after the results are imported into the program.
Require secure LDAP connections	Prevents the insecure port 389 from being used if the secure port 636 fails when querying for OUs or machines in LDAP both in the machine group editor and during a scan. By default, this is disabled. Port 389 is always used when browsing domains after clicking **Browse Active Directory** on the Machine Group editor. However, the data sent to it is encrypted using Kerberos, so there is no security risk.
Enable continuous agentless scanning **Connection timeout**	Adds an option to **schedule recurring agentless patch scans** at minute-based intervals. This is only recommended for use under certain circumstances within Network Access Control (NAC) environments. For more detailed information, see **Continuous Agentless Scanning**. If this option is enabled and there are scheduled scans that are using minute-based intervals, you will not be able to disable this option until you delete those scheduled scans using the **Scheduled Console Tasks Manager**. The maximum amount of time to wait for a target machine to respond to the console during a scan. If the console cannot make a connection to the target machine in the specified number of seconds the machine is skipped. A

Field	Description
(seconds)	connection attempt may timeout earlier than the specified value, this simply puts a maximum value on the wait time.
Patch scan results import timeout (minutes)	The maximum amount of time to wait for the console to import scan results from all target machines. If all machines have not reported results within the specified number of minutes, the console will stop waiting and will proceed with any post-scan activities such as generating reports and sending email.
Connect to machines by	Specifies the method to use when connecting to your client machines. There are two options: • **IP address:** The console will connect to clients using the IP address of the machines. This is the default setting. • **Fully qualified domain name (FQDN):** You may need this method if Kerberos authentication is used in your environment, and if Service Principal Name (SPN) validation is required for Server Message Block (SMB) endpoint connections. For more detailed information, see **IP Address vs FQDN**. This setting can be overridden at the **machine group level**. It can also be overridden at the **machine level** for scans that are initiated from Machine View or Scan View.
Global thread pool	Specifies the total number of threads that can be used during a patch scan or deployment, an asset scan, or a power status scan. The value you specify will be multiplied by the number of logical CPUs on the console machine to determine the maximum number of threads that may be used during a scan instance. One thread will be used to scan one machine, so if you specify a maximum of 64 threads it means that 64 machines can be simultaneously scanned during one scan. Allowing many machines to be scanned at the same time requires more network resources. Reduce this number if you are scanning over a slow link. If you are scanning machine groups that contain machines defined by an IP range, a domain or an organizational unit, this option will also be used prior to the scan. It will limit the number of threads that are used to determine which machines should be scanned.
Default Deployment Template	Specifies the deployment template to use as the default. Any new deployment templates you previously defined will be included in the drop-down list. For more information see **About Deployment Templates**.
Create a temporary system drive share if none exists	Enables Security Controls to create and use a temporary administrator share name on a target machine during the authentication process. The share name will be removed from the target machine when the scan or deployment is complete. While this option does not apply to most organizations, if you are an organization that for whatever reason has disabled or renamed the administrator share names (C$, D$, etc.) on your target machines, then you must enable this check box in order for Security Controls to access those machines.

290. Patch Scanning Overview

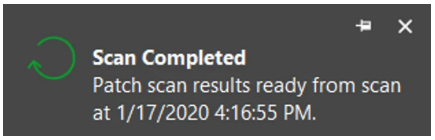
Security Controls allows you to perform a patch scan via a few simple mouse clicks. From one management console you can initiate a patch scan of a single machine or of many machines.

Scans Are Performed As Background Tasks

All patch scans are performed as background tasks using the services of the **Operations Monitor**. This means you can initiate a scan and then move on to other concurrent work within Security Controls without having to wait for the scan to complete. This also means you can have multiple patch scans active at the same time.

Scanning Considerations

- Is there a practical limit to the number of scans you can have active at the same time?
- Yes. It is dependent on the CPU and memory size of the console machine. It is also dependent on the number of other tasks currently active (for example, other patch downloads, patch deployments, etc.). While there is no exact answer, you'll know you've reached a practical limit if Security Controls starts responding slowly.
  Is there a problem if the same machine is included in two or more concurrent scans?
- No. Multiple scanning tasks can be performed on a target machine at the same time.
  If I minimize the Operation Monitor window, how will I know when the scan is complete?
- A notification dialog box is displayed in the lower-right corner whenever a scan completes. The dialog box will be displayed for several seconds before slowly fading away. You can pin the dialog box in place by clicking the pin icon.



Will I still be able to immediately view scan results?
Yes. You can either click the **View results link** within the Operations Monitor or you can select the scan from within the **Today's Items list** of the **Patch Results** pane.

291. Performing Patching in a Disconnected Environment

If you have a console that is operating in a disconnected environment, you must perform a few extra steps before the console is ready to be use for patch management tasks.

1. Install and activate the console.
2. See:
   - **Performing a New Installation**
   - **Activating the Program**

Update the program files.

> Another option is to **use a distribution server**.

1. On a Ivanti Security Controls console that is connected to the internet, update the current data files on it by selecting **Help > Refresh files**.
   This will download the latest scan engines and XML data files to `C:\ProgramData\Ivanti\Security Controls\Console\DataFiles`.
2. Copy all the files in this folder to a media that can be transported to the disconnected console.
3. Copy all the files to the same folder on the disconnected console.

Download missing patches.
Once the data files are updated on the disconnected console you can begin performing patch scans of your inside (non-networked) machines. Before you can deploy missing patches you must locate and transfer the missing patches to the disconnected console.

1. Use **Machine View** to view the list of missing patches.
2. Export the list of missing patches to a .csv file by selecting all missing patches and then using the **Export selected patches to CSV** right-click menu.
   You can use the .csv file as a reference when downloading the patches from the Internet-facing console. Another option is to generate a report that lists the missing patches.
3. On the Internet-facing console, use the **Patch View** smart filters to locate the patches that are missing on the disconnected console.
4. Right-click the patches and download them to the Internet-facing console.
   The downloaded patches are stored in the following directory:
5. `C:\ProgramData\Ivanti\Security Controls\Console\Patches`
   Copy all the files in this folder to a media that can be transported to the disconnected console.
6. Copy all the files to the same folder on the disconnected console.

The disconnected console can now deploy patches to the inside machines.

> **Tip:** Using the **sideload process** is another option for copying the files to the disconnected console.

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance

292. Performing Actions on a Favorite

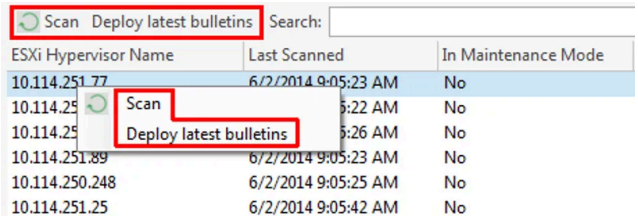
When you select a favorite from the **Favorites** list the Favorite dialog is displayed. It shows the current configuration of the favorite. If you want to immediately perform an operation using this favorite, click **Run operation**. To edit the configuration, simply make the desired changes and then click **Save**.

You can also right-click a favorite and perform the following actions:

Field	Description
Edit	Enables you to edit the selected favorite.
Duplicate	Makes a copy of the selected favorite. The new favorite will contain the same settings as the selected favorite.
Delete	Deletes the selected favorite.
Rename	Enable you to rename the favorite.
Scan	Initiates a scan of the machines specified within the favorite. Initiating a scan from a favorite is an easy way to schedule a scan for a later time or date.

293. Performing Actions on ESXi Hypervisors

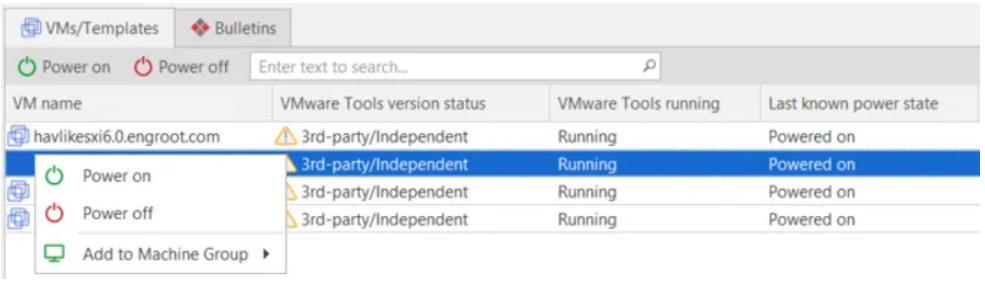
You can perform a number of different actions on the ESXi hypervisors that are being managed by a vCenter Server. You simply select the desired ESXi hypervisors and then either use the buttons along the top of the table or use the right-click menu.



Action	Description
Scan	Enables you to initiate a scan of the selected ESXi hypervisors. The **Operations Monitor** is used to monitor the status of the hypervisor scan. The results of the scan can be found on the **Bulletins tab**. Remember to refresh the **Bulletins** tab to view the most current information.
Deploy latest bulletins	Enables you to deploy bulletins currently missing on the selected ESXi hypervisor. If this option is not available it means one of the following: the ESXi hypervisor has not been previously scanned, there are multiple ESXi hypervisors selected (you can only deploy bulletins to one hypervisor at a time), or all bulletins have been applied. For more information on deploying bulletins to an ESXi hypervisor, see **Configuring an ESXi Deployment**.

294. Performing Actions on a Hypervisor's Virtual Machines

The **VMs/Templates** tab can be used to power on and off the virtual machines that are contained on the selected hypervisor. You can also add the virtual machines and templates to a new or existing machine group. To perform these actions you simply select the desired virtual machines and/or templates and then either use the buttons along the top of the tab or use the right-click menu.

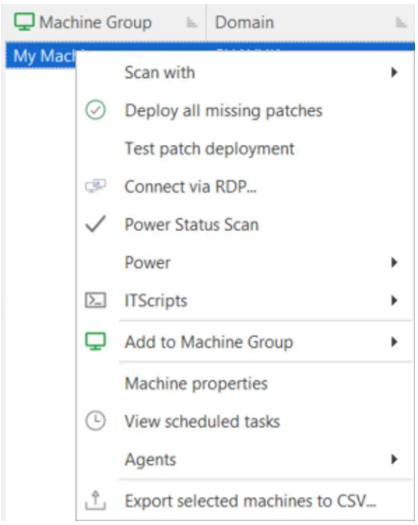


Field	Description
Power on	Enables you to immediately power on the selected virtual machine(s). The **Operations Monitor** is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Power off	Enables you to immediately power off the selected virtual machine(s). The **Operations Monitor** is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See **Creating A New Machine Group** for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (**Hosted virtual machines** are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the **default credentials** will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See **Supplying Credentials** for more information.

295. Performing Actions on Machines

Right-Click Menu

You can right-click on any machine in the top pane and perform a number of different actions.



Action	Description
Scan With	Enables you to initiate a patch scan of the selected machines using any of the available patch scan templates.
Deploy All Missing Patches	Enables you to deploy (install) all patches currently missing on the selected machine. See **Deploying All Missing Patches to a Machine** for more information. If you deploy a patch to a specific SQL Server instance, the patch is applied to all instances on that machine.
Test Patch Deployment	Enables you to perform a test deployment to the selected machines. This is especially useful for patch deployments you want to schedule for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail. See the **Operations Monitor** for more information.
Connect via RDP	Enables you to make a Remote Desktop connection to the selected machine. See **How to Initiate a Remote Desktop Connection** for more details.
Power Status Scan	Enables you to perform a **power status scan** on the selected machines.
Power	Enables you to modify the power state of the selected machines. You can immediately restart, shut down, or awaken the machines, or you can use a power state template to schedule a reboot of the machines and leave them in a particular state (fully powered on, in sleep mode, in hibernate mode, or powered off). See **How to Initiate Power Management Tasks** for more information.
ITScripts	Enables you to either open a Windows PowerShell™ prompt or select and execute an approved script. See **How to Execute a Script** for details.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See **Creating A New Machine Group** for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. If no machine credentials are available, no credentials will be assigned and the **default credentials** will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See **Supplying Credentials** for more information.
Machine Properties	Enables you to view and edit machine properties. See **Managing Individual Machine Properties** for more information.
View schedu	Enables you to view the **Scheduled Remote Tasks Manager**, which gives you a single location from which to monitor the power tasks and patch deployment tasks currently scheduled on this machine.

Action	Description
led tasks	
Agents	Enables you to: • **Install** an agent, assign a different policy to the agent, or **uninstall** an agent. • Send a number of different commands to the selected agents. The commands apply only to machines that already have agents installed, that are online, and that are configured to be **listening agents**. See the **Send command** description for detailed information about the available commands. • **(Machine View only)** Initiate any of the tasks currently defined within the selected agents. When you select a task a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See **Creating a New Agent Policy** for information on the types of tasks that may be available.
Export selected machines to CSV	Export information about the selected machines to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.
Set/Change automated email	This option is only available if you have enabled the **email feature and defined an SMTP server**. It enables you to set or change the automated report settings for this machine. Changes you make here will override email settings you specified on the **Manage Machine Properties dialog**.
Email Machine Status Summary	This option is only available if you have enabled the **email feature and defined an SMTP server**. It enables you to send a **Machine Status Summary** report to one or more recipients.

Keyboard Shortcuts

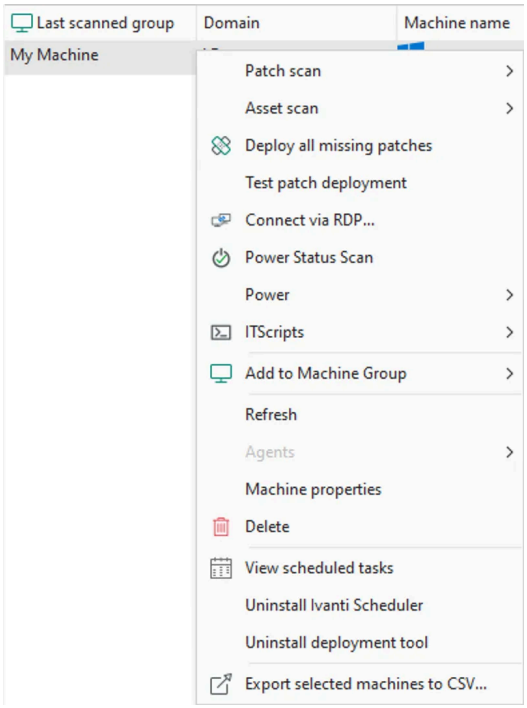
The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all machines.
- **CTRL+click**: Multiple machines can be selected by holding down the CTRL key while selecting machines.
- **SHIFT+click**: A contiguous group of machines can be selected by holding down the SHIFT key while selecting the starting and ending machines in the list.
- **SHIFT+PAGE UP**: Selects a range of machines from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of machines from the one currently selected to the bottom of the table.

296. Performing Actions on Machines

Windows Machines

You can right-click on any Windows machine in the top pane and perform a number of different actions.



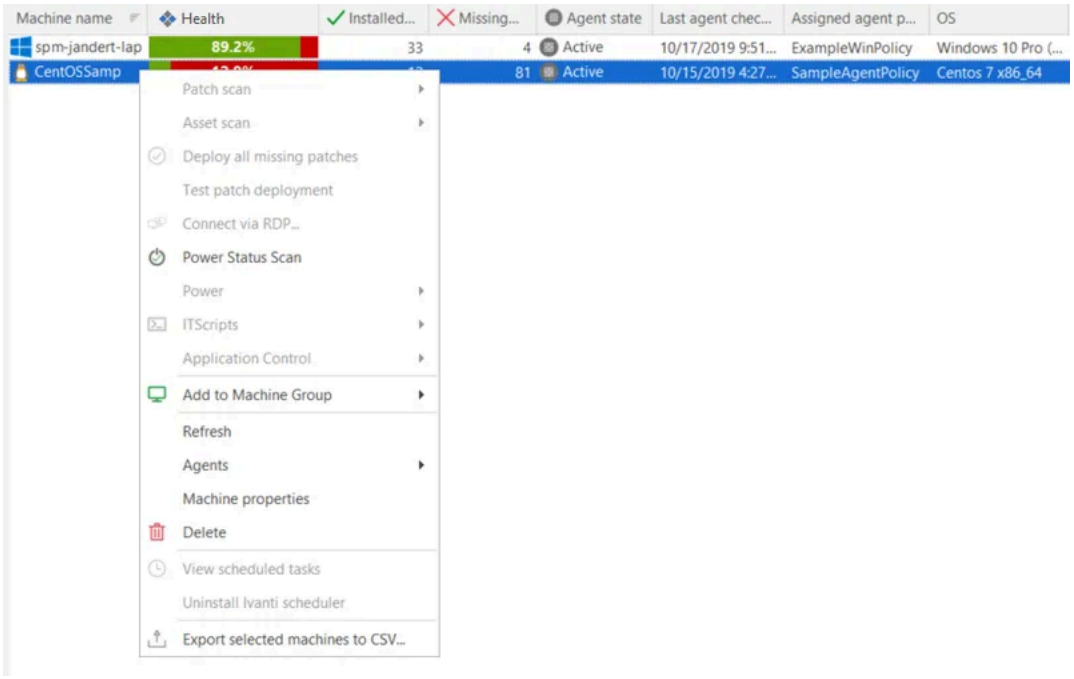
Field	Description
Patch Scan	Enables you to initiate a patch scan of the selected machines using any of the available patch scan templates.
Asset Scan	Enables you to initiate an asset scan of the selected machines using any of the available asset scan templates.
Deploy all missing patches	Enables you to deploy (install) all patches currently missing on the selected machine. See **Deploy to All Scanned Machines** for more information. If you deploy a patch to a specific SQL Server instance, the patch is applied to all instances on that machine.
Test patch deployment	Enables you to perform a test deployment to the selected machines. This is especially useful for patch deployments you want to schedule for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail. See the **Operations Monitor** for more information. Test deployments will not work on **offline virtual machines**.
Connect via RDP	Enables you to make a Remote Desktop connection to the selected machine. See **How to Initiate a Remote Desktop Connection** for more details.
Power Status Scan	Enables you to perform a **power status scan** on the selected machines.

Field	Description
Power	Enables you to modify the power state of the selected machines. You can immediately restart, shut down, or awaken the machines, or you can use a power state template to schedule a reboot of the machines and leave them in a particular state (fully powered on, in sleep mode, in hibernate mode, or powered off). See **How to Initiate Power Management Tasks** for more information.
ITScripts	Enables you to either open a Windows PowerShell™ prompt or select and execute an approved script. See **How to Execute a Script** for details.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See **Creating A New Machine Group** for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (**Hosted virtual machines** are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the **default credentials** will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See **Supplying Credentials** for more information.
Refresh	Refreshes the information displayed in the top pane.
Agents	Enables you to: • **Install** an agent, assign a different policy to the agent, or **uninstall** an agent. • Send a number of different commands to the selected agents. The commands apply only to machines that already have agents installed, that are online, and that are configured to be **listening agents**. See **Managing Your Agents** for detailed information about the available commands. • **(Machine View only)** Initiate any of the tasks currently defined within the selected agents. When you select a task a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See **Creating a New Agent Policy** for information on the types of tasks that may be available.
Machine Properties	Enables you to view and edit machine properties. See **Managing Individual Machine Properties** for more information.
Delete	Deletes the selected machine from Machine View. If the machine is rescanned it will be re-added to Machine View. Deleting a machine from Machine View also affects the information displayed for that machine within Scan View (see **Accessing Patch Scan Results**). The machine will be moved to the **Machines Not Scanned** tab and all previous scan information for that machine will be lost.
View scheduled tasks	Enables you to view the **Scheduled Remote Tasks Manager**, which gives you a single location from which to monitor the power tasks and patch deployment tasks currently scheduled on this machine.
Uninstall	Removes the Ivanti Scheduler from the machine. Use of the Ivanti Scheduler was **discontinued in v2023.2** and it should be removed from all target machines.

Field	Description
Ivanti Scheduler	Be careful not to remove the Ivanti Scheduler until you are certain that all scheduled tasks still using this scheduler have been run.
Uninstall deployment tool	Removes the tool used by Security Controls to execute a deployment package on the machine. This tool gets pushed to the target machine when a patch deployment is initiated from the console. You can remove this tool if you want to eliminate any temporary files on the machine.
Export selected machines to CSV	Export information about the selected machines to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

Linux Machines

You can right-click on any Linux machine in the top pane and perform a number of different actions.



Field	Description
Power Status Scan	Enables you to **initiate a power status scan** of the selected machines.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See **Creating A New Machine Group** for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. If no machine credentials are available, no credentials will be assigned and the **default credentials** will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See **Supplying Credentials** for more information.
Refresh	Refreshes the information displayed in the top pane.
Agents	Enables you to **install** an agent, assign a different policy to the agent or **uninstall** an agent. Enables you to: • **Install** an agent, assign a different policy to the agent, or **uninstall** an agent. • Send a number of different commands to the selected agents. The commands apply only to machines that already have agents installed, that are online, and that are configured to be **listening agents**. See **Managing Your Agents** for detailed information about the available commands. • **(Machine View only)** Initiate any of the tasks currently defined within the selected agents. When you select a task a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See **Creating a New Agent Policy** for information on the types of tasks that may be available.

Field	Description
Machine Properties	Enables you to view and edit machine properties. See **Managing Individual Machine Properties** for more information.
Delete	Deletes the selected machine from Machine View. If the machine is rescanned it will be re-added to Machine View.
Export selected machines to CSV	Export information about the selected machines to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

Keyboard Shortcuts

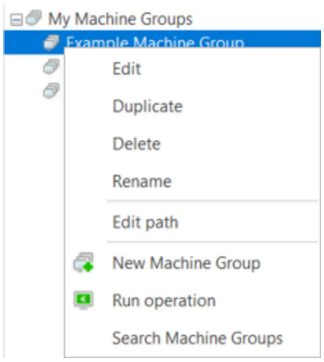
The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all machines.
- **CTRL+click**: Multiple machines can be selected by holding down the CTRL key while selecting machines.
- **SHIFT+click**: A contiguous group of machines can be selected by holding down the SHIFT key while selecting the starting and ending machines in the list.
- **SHIFT+PAGE UP**: Selects a range of machines from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of machines from the one currently selected to the bottom of the table.
- **HOME:** Moves the focus to the first cell in the table.
- **END**: Moves the focus to the last cell in the table.

297. Performing Actions on Machine Groups

Right-Click Menu

You can right-click on any machine group in the navigation pane and perform a number of different actions.



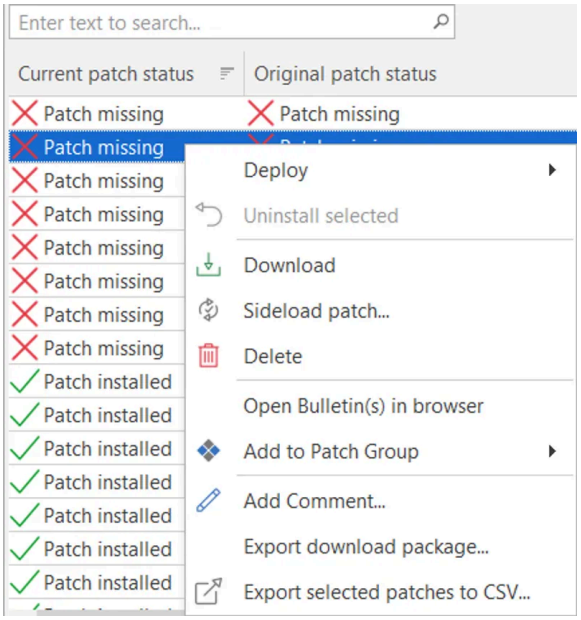
Action	Description
Edit	Enables you to edit the selected machine group.
Duplicate	Makes a copy of the selected machine group. Type a name for the new group and then click **Save**.
Delete	Deletes the selected machine group.
Rename	Enables you to rename the selected machine group.
Edit path	Enables you to change the folder path of the selected group. Doing so will relocate the machine group to a different folder in the **My Machine Groups** list in the navigation pane. For more details, see Organizing Machine Groups.
New Machine Group	Enables you to create a new machine group. See Creating a New Machine Group for more details.
Run operation	Enables you to initiate a patch, asset, power or ITScripts operation on the machine group.
Search Machine Groups	Enables you to search for alphanumeric characters in any of your existing machine groups. See Searching Machine Groups for details.

298. Performing Actions on Patches

You can easily search for patches contained in the middle pane. All searches are performed using the Search tool. To initiate a search you type into the box the alphanumeric characters that you want to find. Only those patches matching the search criteria are displayed; all other patches are hidden. For tips on using the Search tool, see **Searching for Machines**.

In addition, you can right-click on any patch on the **Windows patches** or **Linux patches** tabs and perform a number of different actions.

Windows Machines

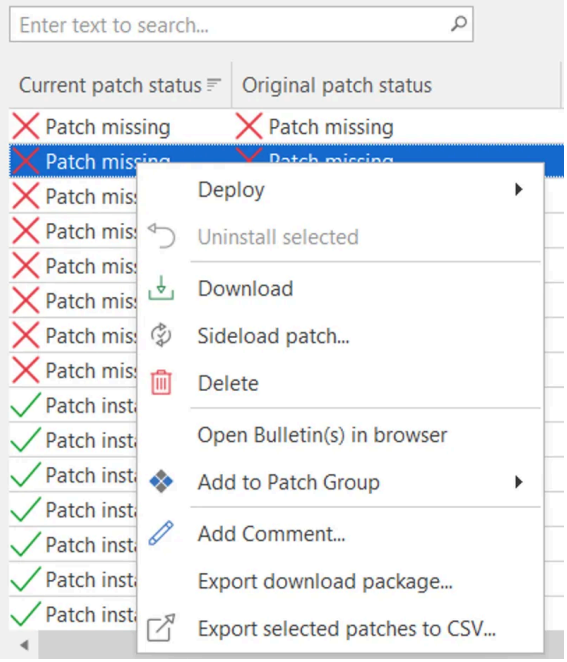


Action	Description
Deploy **Uninstall Selected**	Enables you to deploy (install) patches or product levels currently missing on the machine(s) selected in the top pane. See **Deploying One or More Patches to a Machine** for more information. Enables you to uninstall (rollback) the selected patch. See **How to Uninstall Patches** for more information.
Download **Sideload patch**	Enables you to download to the patch download directory the selected patches or product levels. See **Downloading Patches** for more information. The **Download** command is only available if the patch can be downloaded automatically. For more information see the description of the **Download method column**. Enables you to manage patches that cannot be automatically downloaded by Security Controls. See **Manually Acquiring Patches from the Vendor (Sideloading)** for more information. **Tip:** In some cases, you may choose to use the sideload process on patches that can be automatically downloaded (for example, when downloading patches for use in a **disconnected network**).
Delete	Enables you to delete selected patches from the patch download directory.
Open Bulletin(s) in Browser **Add to Patch Group**	Displays the related Microsoft security bulletin within a Web browser. Enables you to add the selected patch(es) to an existing patch group or to a new patch group. See **Creating and Editing a Patch Group** for more information.
Add Comment	Enables you to add your own specific comment about the patch.
Export download package	Export the download links for the selected patches to a Comma Separated Values (CSV) file. This is especially useful for a console that is in a **disconnected environment**. The CSV file can be used by a connected machine to download the patches and the patches can then be copied into the disconnected console's patch directory. A File Downloader PowerShell script is available to assist with the file download process; contact the **Support group** for more details.

299. Performing Actions on Patches

You can easily search for patches contained in the middle pane. All searches are performed using the Search tool. To initiate a search you type the alphanumeric characters that you want to find and then press **Enter** or click the search icon (). Only those patches matching the search criteria are displayed; all other patches are hidden. For tips on using the Search tool, see **Searching for Machines**.

In addition, you can right-click on any patch in the middle pane and perform a number of different actions.



Action	Description
Deploy	Enables you to deploy (install) patches or product levels currently missing on the machine(s) selected in the top pane. See **Deploying One or More Patches to a Machine** for more information.
Uninstall Selected	Enables you to uninstall (rollback) the selected patch. See **How to Uninstall Patches** for more information.
Download	Enables you to download to the patch download directory the selected patches or product levels. See **Downloading Patches** for more information. The **Download** command is only available if the patch can be downloaded automatically. For more information see the description of the **Download method column**.
Sideload patch	Enables you to manage patches that cannot be automatically downloaded by Security Controls. See **Manually Acquiring Patches from the Vendor (Sideloading)** for more information. **Tip:** In some cases, you may choose to use the sideload process on patches that can be automatically downloaded (for example, when downloading patches for use in a **disconnected network**).
Delete	Enables you to delete selected patches from the patch download directory.
Open Bulletin(s) in Browser	Displays the related Microsoft security bulletin within a Web browser.
Add to Patch Group	Enables you to add the selected patch(es) to an existing patch group or to a new patch group. See **Creating and Editing a Patch Group** for more information.
Add Comment	Enables you to add your own specific comment about the patch.
Export download package	Export the download links for the selected patches to a Comma Separated Values (CSV) file. This is especially useful for a console that is in a **disconnected environment**. The CSV file can be used by a connected machine to download the patches and the patches can then be copied into the disconnected console's patch directory. A File Downloader PowerShell script is available to assist with the file download process; contact the **Support group** for more details.
Export selected patches to CSV	Export information about the selected patches to a CSV file. The CSV file can then be used by a spreadsheet program.

Keyboard Shortcuts

The following keyboard shortcuts are available:

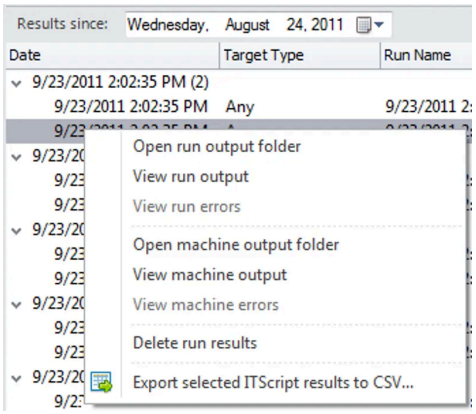
- **Ctrl+A**: Selects all patches.
- **CTRL+click**: Multiple patches can be selected by holding down the CTRL key while selecting patches.
- **SHIFT+click**: A contiguous group of patches can be selected by holding down the SHIFT key while selecting the starting and ending patches in the list.

- **SHIFT+PAGE UP**: Selects a range of patches from the one currently selected to the top of the table.
- **SHIFT+PAGE DOWN**: Selects a range of patches from the one currently selected to the bottom of the table.

300. Performing Actions on Script Results

Right-Click Menu

You can right-click on any result entry within **ITScripts Results View** and perform a number of different actions.



Run Results vs Machine Results

- **Run** results contain execution information about the script (when the script was run, whether the script was successful, etc.). It also contains output for each of the machines scanned by the script.
- **Machine** results contain the output that was created when the script was run on a particular machine.

All results are located in the following directory: `C:\ProgramData\Ivanti\Security Controls\Console\ITScriptsOutput`

Command Descriptions

Field	Description
Open run output folder	This command is available only if **Result Type = Run** and if the run generated an output file. The command uses Windows Explorer to open the output folder associated with this run. The output folder contains a sub-folder for each machine that was in the run. Within each machine sub-folder is a text file that contains the machine output.
View run output	This command is available only if **Result Type = Run**and if the run generated an output file. It displays a text file containing output information related to the execution of the script.
View run errors	This command is available only if **Result Type = Run**and if the run generated an error file. It displays a text file containing the errors that occurred when the script was executed. For example, if a machine could not be resolved and a connection error occurred, that error would be displayed here.
Open machine output folder	This command is available only if **Result Type = Machine** and if an output file or an error file was generated. The command uses Windows Explorer to open the output folder associated with this machine. The output folder contains the machine output text file and/or the machine error text file.
View machine output	This command is available only if **Result Type = Machine**and if an output file was generated. It displays the output that was created when the script was run on the selected machine.
View machine errors	This command is available only if **Result Type = Machine** and if an error file was generated. It displays a text file containing the errors that occurred when the script was executed on the selected machine.
Delete run results	Deletes all output for the selected run (both the run output files and the machine output files).
Export selected ITScript results to CSV	Export information about the selected script results to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program. The **ITScript Results > Export visible ITScript results to CSV** menu command is similar except that it exports all results in the right pane rather than just selected results.

Double-Click Shortcut

You can double-click any result entry to immediately view its results. If there are multiple result types available for an entry the program will choose either the output file or the error file first, and if neither of these are available it will display the output folder.

Keyboard Shortcuts

The following keyboard shortcuts are available:

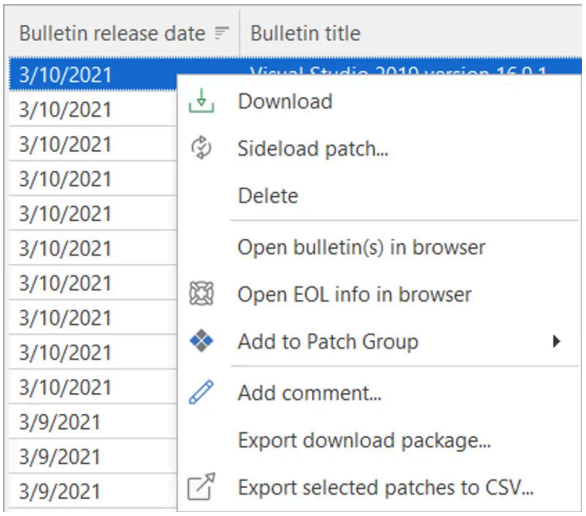
- **Ctrl+A**: Selects all script results.
- **CTRL+click**: Multiple script results can be selected by holding down the CTRL key while selecting script results.
- **SHIFT+click**: A contiguous group of script results can be selected by holding down the SHIFT key while selecting the starting and ending script results in the list.
- **SHIFT+PAGE UP**: Selects a range of script results from the one currently selected to the top of the table.

- **SHIFT+PAGE DOWN**: Selects a range of script results from the one currently selected to the bottom of the table.
- **CTRL+HOME:** Moves the focus to the first cell in the table.
- **CTRL+END**: Moves the focus to the last cell in the table.

301. Performing Actions on Patches

Right-Click Menu

You can right-click on any patch or product level in the top pane of Patch View and perform a number of different actions.



Action	Description
Download	Enables you to download the selected patches or product levels to the **patch download directory**. For more information on the download process, see **Downloading Patches and Product Levels**. The **Download** command is only available if the patch can be downloaded automatically. For more information see the description of the **Download method column**.
Sideload patch	Enables you to manage patches that cannot be automatically downloaded by Security Controls. See **Manually Acquiring Patches from the Vendor (Sideloading)** for more information. **Tip:** In some cases, you may choose to use the sideload process on patches that can be automatically downloaded (for example, when downloading patches for use in a **disconnected network**).
Delete	Enables you to delete the selected patches from the patch download directory. If the selected patches have never been downloaded, this command will be unavailable.
Open bulletin(s) in browser	Enables you to display, within your default Web browser, vendor information about the selected patch bulletin.
Open EOL info in browser	Enables you to display, within your default Web browser, End of Life information for the product affected by the selected bulletin.
Add to Patch Group	Enables you to add the selected patches to a new or existing patch group. See **Creating and Editing a Patch Group** for more information.
Add comment	Enables you to provide a comment about the patch.
Export download package	Export the location of the download packages for the selected patches to a Comma Separated Values (CSV) file.
Export selected patches to CSV	Export information about the selected patches to a CSV file. The CSV file can then be used within a spreadsheet program.

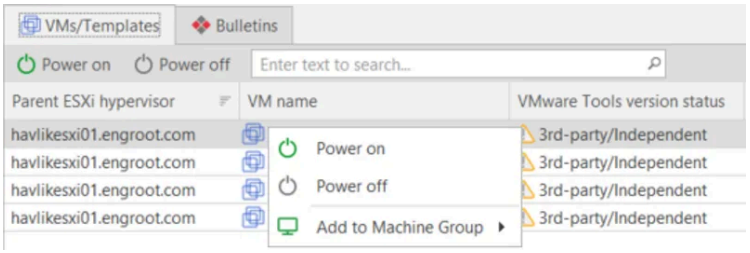
Keyboard Shortcuts

The following keyboard shortcuts are available:

- **Ctrl+A**: Selects all patches.
- **CTRL+click**: Multiple patches can be selected by holding down the CTRL key while selecting patches.
- **SHIFT+click**: A contiguous group of patches can be selected by holding down the SHIFT key while selecting the starting and ending patches in the list.
- **SHIFT+PAGE UP**: Selects a range of patches from the one currently selected to the top of the display. Each time you press **Page Up** an additional range of patches is added to the selection.
- **SHIFT+PAGE DOWN**: Selects a range of patches from the one currently selected to the bottom of the display. Each time you press **Page Dn** an additional range of patches is added to the selection.

302. Performing Actions on Virtual Machines

The **VMs/Templates** tab can be used to power on and off your virtual machines. You can also add the virtual machines to a new or existing machine group. To do this you simply select the desired virtual machines and then either use the buttons along the top of the tab or use the right-click menu.

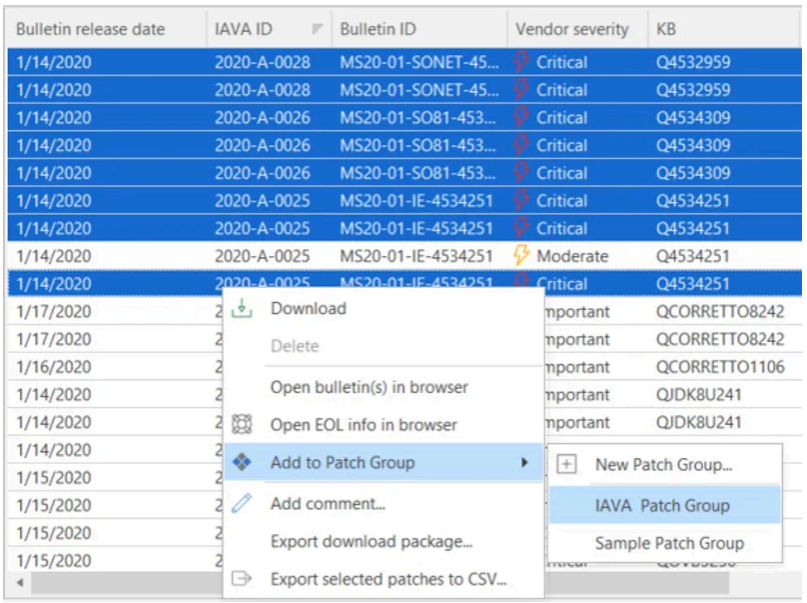


Field	Description
Power on	Enables you to immediately power on the selected virtual machine(s). The **Operations Monitor** is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Power off	Enables you to immediately power off the selected virtual machine(s). The **Operations Monitor** is used to monitor the status of the power operation. To view the updated power state, refresh the information displayed on the tab by selecting **View > Refresh**.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See **Creating A New Machine Group** for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (**Hosted virtual machines** are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the **default credentials** will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See **Supplying Credentials** for more information.

303. Performing an IAVA Patch Scan

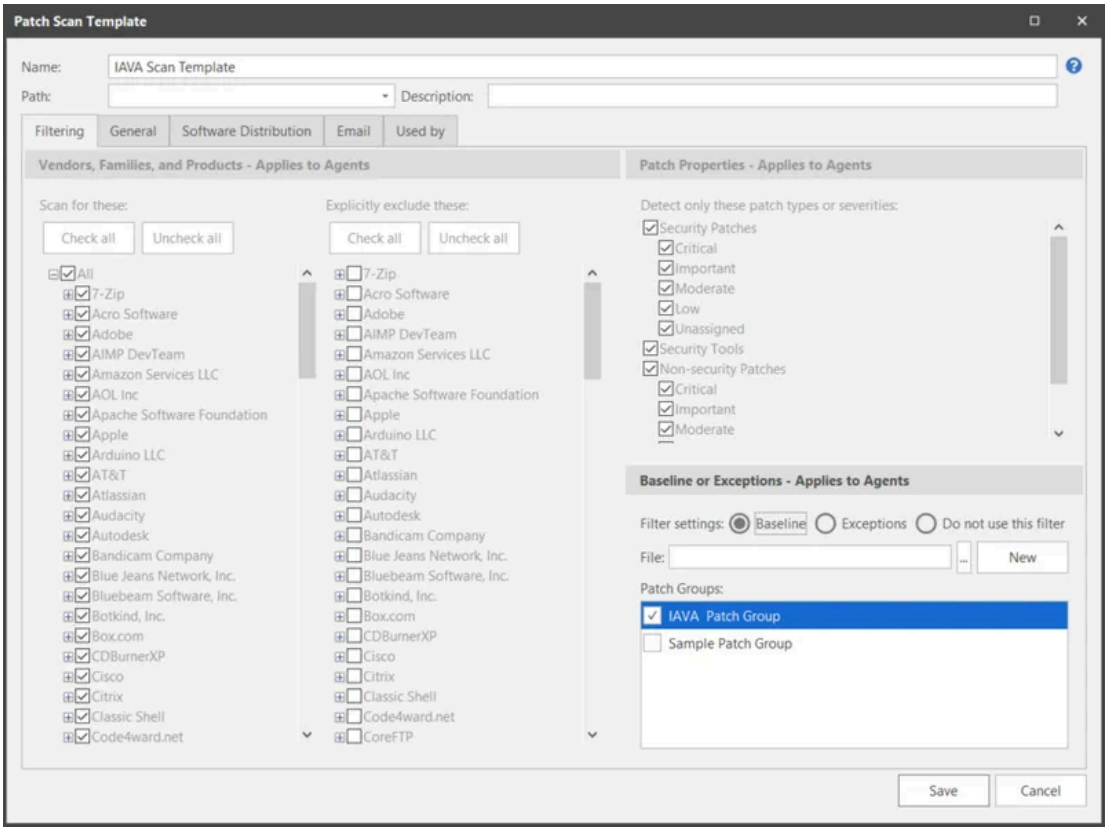
Another common use of the reporting tool is to create a patch group that contains one or more patches that are of particular interest. You then specify the patch group within a Security Controls patch scan template and use the template to scan your machines on a regular basis.

1. Create a patch group that contains the patch or patches you would like to scan for (or deploy).
2. To do this, select either **View > Windows Patches** or **New > Windows Patch > Patch Group** and then use a Smart Filter to narrow the focus to only those patches of interest. You can then click the **IAVA ID** column header to sort the remaining patches by their IAVA ID. After selecting the desired patches, use the right-click menu to add the patches to a new or existing patch group.



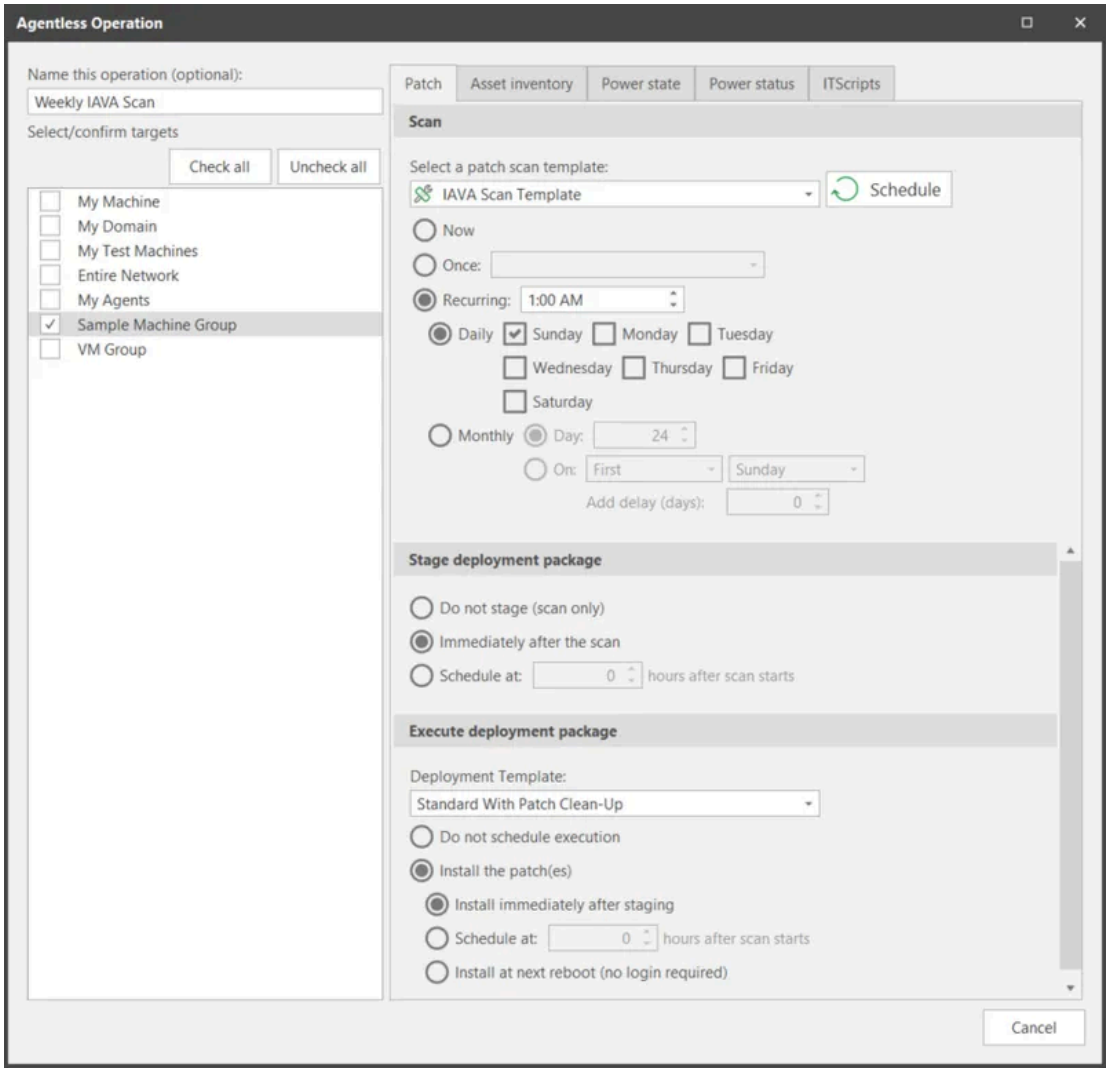
From the main menu select **New > Windows Patch > Patch Scan Template**.

3. On the **Patch Scan Template** dialog, type a name for the new template.
4. On the **Filtering** tab, in the **Baseline or Exceptions** area, choose **Baseline**.
5. Select the patch group you created earlier.



Save the scan template.

7. On the Agentless Operation page, in the **Select/confirm targets** area, select the machine group you want to scan.
8. On the **Patch** tab, select the patch scan template you just created.

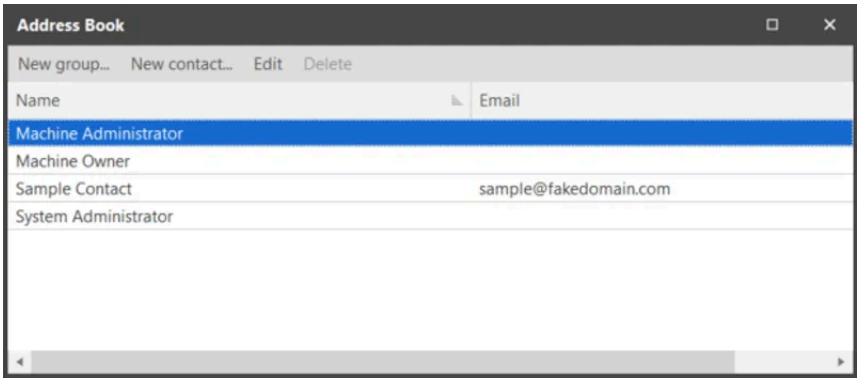


Schedule the scan to occur at the desired date and time.

10. (Optional) If you want to automatically deploy the patches in the patch group, select the desired deployment options in the **Stage deployment package** and **Execute deployment package** areas.
11. Click **Schedule**.

304. Populating the Address Book

The address book is used to store the email addresses of those users you want to send messages or alerts. You can also define one or more email groups. To add, delete, or modify the contents of the address book, select **Manage > Address Book**. The **Address Book** dialog is displayed.



The address book initially contains default entries for the machine administrator, the machine owner, and the system administrator. More than one contact can be defined as a system administrator.

Defining a New Contact

1. Click **New Contact**.
2. Type the name of the contact as you want it to appear in the address book.
3. Type the email address of the contact.
4. If you want the contact to receive messages that are automatically sent to all system administrators, enable the **System Administrator** check box.

Defining a New Email Group

1. Click **New Group**.
2. Type the name of the group you want to create.
3. To populate the group, enable the desired check boxes in the list of available contacts and then click **Save**.
    - If you want to add every contact in the list to the group, click **Check All**.
    - If you want to define a new contact, click **New Contact**.

Deleting an Existing Contact or Group

1. Select the contact or group you want to delete.
   You can select multiple entries at one time by pressing and holding the **Ctrl** key while you select each entry.
2. Click **Delete**.

305. Port Requirements and Firewall Configuration

Port Requirements

See the **System Requirements** for the complete list of port requirements. Using that list, an administrator can configure firewalls in the environment and on the local machines to allow proper traffic in and out of machines for Security Controls to manage the environment.

Firewall Configuration

A number of different Web addresses must be accessible in order for Security Controls to download the necessary patches, service packs, engines and XML files. This means you may need to add the Web addresses to your firewall rules and proxy exceptions list. For the complete list of Web addresses that must be accessible, go to the community page at: **https://forums.ivanti.com/s/article/URL-exception-list-for-Ivanti-Security-Controls**.

Related Topics

- **Console Software and Hardware Recommendations**
- **Distributed Environment Management**
- **Agentless Patch Management**
- **Best Approach for Applying Patches in an Agentless Environment**
- **Automating Patch Management in an Agentless Environment**
- **Agent-Based Patch Management**
- **Agent Rollout Options**
- **Installing and Supporting Agents on Internet-Based Machines**
- **Agent-Based Product Level and Patch Deployment Process**
- **Guide to Surviving Patch Tuesday**
- **Microsoft SQL Server Database Maintenance**
- **Performing Patching in a Disconnected Environment**

306. Post-Migration Tasks

In order to complete the migration, you must perform the following tasks on the new Security Controls console. The sooner you perform these tasks the sooner you can permanently retire your old console. You want to retire your old console as soon as possible to eliminate duplicate and time-consuming tasks from being performed by both consoles.

Manually Migrating Items Not Moved by the Tool

- If you are in a proxy environment or a disconnected environment:
- The Security Controls license is not automatically activated in these environments. To activate your license, from the Security Controls menu select **Help > Enter/refresh license key**.
  If you had an agent running on the local console:
- This agent will not be migrated and must be reinstalled after the migration.
  If you are using custom patch XML files:
- Custom patch XML files must be moved manually because they are saved to a location that cannot be referenced by the Migration Tool.
  If you are using a data rollup configuration:
  - **Rollup (central) console:** After the migration, go to **Tools > Options > Data Rollup** and confirm that **Accept and import results from a rollup sender** is enabled.
  - **Remote console:** After the migration, go to **Tools > Options > Data Rollup**, confirm the rollup server information and then click **Register**.

If you are using a distribution server that resides on the local console:

- The distribution server configuration and the files contained on the distribution server will be moved. The folder representing the distribution server, however, must still be defined as a shared folder, the Windows permissions to access the shared folder must be updated, and the path to the folder must be updated in the distribution server configuration on the new console.
  If you were using customized user-specific options:
  Go to **Tools > Options** and reset any custom setting that was not migrated.

Verification Checklist

Perform the tasks in this checklist to verify that your new Security Controls console is operating properly.

- Select **Help > Refresh files** and make sure no errors occur.
- Select **Help > About Ivanti** Security Controls and verify that your license key data is valid and that the correct product capabilities are enabled.
- Run a scan and a patch deployment to verify that your credentials can access the machines in your machine groups.
- Download a patch and verify that the download is successful.
- If you are configured to use the Database Maintenance feature, select **Manage > Database Maintenance** and on the **Scheduled** tab or the **AC Events** tab, click **Run now** to verify that the feature is working properly.
- If you are using agents, check that they have all checked in with the new console. You can do this from Machine View by using the **Has an Agent Policy** filter and then sorting by the **Last Agent Check In** column. All check-in dates should be after the date you modified the Console Alias list on the old console.

- If you have enabled the use of Security Controls Cloud synchronization in an agent policy, you must register the new console and force a full update. To do this, select **Tools > Options >** Security Controls **Cloud sync** and click **This console is registered** (the text on the button in this case is misleading because it is referring to the old console). When the registration is complete, click **Force full update now**.
- If you are using the distribution server synchronization feature, verify that it succeeds the first time it is scheduled to execute.
- If you have multiple consoles and are using data rollup, check that the rollup succeeds on the proper schedule.
- If you have scheduled tasks such as patch scans or patch deployments, watch closely the first time through to make sure the tasks are successfully completed.
- Use the **Tools > Console alias editor** menu to remove the old console's information from the Console Alias list. Also, if the new console is on a domain-joined machine, you will need to add the fully qualified name of the new machine to the alias list.

When and How to Retire Your Old Console

You can retire your old console when the migration is complete and all of your agents are successfully checking in with the new console. The recommended steps are:

1. Verify that the Security Controls Console Service is stopped on the old console.
   This will effectively disable the old console and route all traffic to the new console.
2. Go through one or more maintenance cycles.
   Do this to verify that everything is working properly on the new console.
3. Retire the old console.
   How exactly you retire the console is up to you and your organization's policies. You might simply power off the machine, or you might perform a backup and then uninstall Security Controls.

Related Topics

- Requirements for Using the Migration Tool
- Commonly Asked Questions
- Before You Begin
- Creating Your Backup Files
- Restoring Your Console on a New Machine

307. Potential Issues When Using Multiple Administrators

Usage Issues

You must take a few common sense precautions when using multiple administrators. Even though Security Controls contains a number of built-in safety checks, it cannot guard against all possibilities. The program may act in unpredictable ways if the following occur:

- If two administrators try to scan the same machine group or ESXi Hypervisor at the same time.
- The machines will be scanned twice, causing potential performance issues. In addition, there may be administrative rights errors due to the multiple connections.
  If two or more administrators try to deploy patches or bulletins to the same machine at the same time.

The most likely result is that one deployment task will succeed and the other will fail. But because the deployment that succeeds will likely perform a restart of the target machines, the machines may be in an unknown state when the other deployment fails.

Credential Issue

If You Choose Not to Use Shared Credentials

When you create credentials and assign them to machines, those credentials belong to your administrator account. If a different administrator (Administrator B) logs on and uses Security Controls, they will not have access to the machine credentials you provided. The second administrator must provide their own machine credentials.

One of the ways this can be confusing is if Administrator B fails to provide their own machine credentials and tries to schedule a patch deployment from a scan that was performed by Administrator A. The deployment can be successfully scheduled if **default credentials** are available, but the actual patch deployment will likely fail because the patch deployment requires machine credentials -- credentials that were provided by Administrator A but that are not available to Administrator B.

Recommendations:

- Each administrator should create their own credentials and assign them to machines
- Each administrator should define default credentials that are the same as their logon credentials. This will eliminate some of the problems that may occur if the administrator forgets to assign machine credentials.

If You Choose to Use Shared Credentials

Much of the pain described above can be eliminated by using shared credentials. Sharing a credential enables other users to use the credential without knowing the secure details about the credential. For complete details, see **Shared Credentials**.

Virtual Inventory Consideration

Unlike machine groups (which can be viewed by all administrators), vCenter Servers and ESXi Hypervisors can only be viewed by the administrator that added them to Security Controls. If two different administrators want to manage the same vCenter Server or ESXi Hypervisors, both administrators must add the item to the **Virtual Inventory list**.

308. ITScripts and Windows PowerShell™ Overview

Windows PowerShell™ is a task automation framework. It is built on Microsoft .NET Framework and provides administrators the ability to quickly and easily perform management tasks on Windows machines and applications. The ITScripts function of Security Controls supports the use of PowerShell 4.0, enabling you to execute a variety of scripts on the console and on remote target machines. It also enables you to start a **Windows PowerShell session** between the console and a selected machine.

> You may also be interested in learning about the **PowerShell API** and **REST API** functionality available in Security Controls.

HOW-TO INFORMATION

For setup and system requirements information, see:

- **ITScripts Options**
- **ITScripts Requirements**

For information on how to perform ITScripts tasks, see:

- **Creating an ITScripts template**
- **How to Execute a Script**
- **Monitoring an ITScript**
- **ITScripts Results View**

WHY USE WINDOWS POWERSHELL SCRIPTS?

PowerShell scripts enable you to perform a wide variety of administrative tasks on the machines in your organization -- from the most rudimentary task to highly advanced and complex operations. You might want to search your target machines for a particular type of data, gather and read log files, install software, create a report, determine the status of a service, read the registry, etc. PowerShell scripts are a great way to automate repetitive tasks across a large number of machines.

WHY USE Security Controls TO RUN SCRIPTS?

The advantages to running scripts in Security Controls include:

- Scripts execute against the machines and machine groups you have already defined in Security Controls
- Use the machine and machine group credentials you have already entered in Security Controls
- Scripts execute in the background
- Script execution can be run immediately or scheduled to run in the future
- Scripts are executed in parallel against the target machines and usually complete in a fraction of the time that it would take to run them serially (and you can control the level of parallelism)
- Script output is captured to files that you can review at your convenience
- Status of script execution is displayed within Security Controls
- You can open the result files directly from Security Controls
- Your scripts can be parameterized, and different sets of parameters can be saved in a template or provided when you start the script or schedule it for execution
- Scripts can use the PowerShell remoting features, allowing the broadest set of capabilities provided by Windows PowerShell

MANY PREDEFINED SCRIPTS ARE AVAILABLE

The ITScripts function comes with a number of predefined scripts. This includes basic scripts that are used to perform various utility tasks and advanced scripts that are used to perform more complicated tasks.

You can use the **Script Catalog Manager** to view the predefined scripts that are available to you.

CREATE AND IMPORT CUSTOM SCRIPTS

You can import custom scripts that you created or that were created by someone you trust. Any custom scripts you import will appear in the Script Catalog Manager along with the predefined scripts. Custom PowerShell modules are also supported. You can create and import modules containing cmdlets, providers, functions, variables, and aliases that you can use in your other custom scripts. For more information, see **Creating a Custom Script**.

TARGET TYPES

Security Controls provides several target types for executing scripts. The target type indicates what the target machine requires when executing a script. The target type is set by the script author using the scriptType element and cannot be altered by Security Controls. A script can only be run in one mode. In all cases the script engine runs on the Security Controls console.

- **Console:** The script runs only against the console and not against a set of target machines. For example, you might use a Console script to query or modify Active Directory.
- **Any:** The script is run against selected target machines or machine groups **without** the services of WinRM (PowerShell remoting). The PowerShell client on the console will communicate with the target machines by using other Windows remoting services such as remote registry service, remote Windows file sharing, WMI services, etc. The actual service used will depend on the script. The scripts will be run in parallel, not one machine at a time.
- You do not need to install any additional software on the target machines when executing scripts of this type. The only ports required are the ports required by the Windows services being used.
- **ESXi Hypervisor:** The script runs against an ESXi Server or a vCenter Server. This type of script may use VMware vSphere PowerCLI. VMware vSphere PowerCLI lets you automate all aspects of vSphere management, including network, storage, VM, guest OS and more. Scripts of this type only run against machine groups that contain ESXi servers. If the machine group contains any other machines, they will be ignored when this script executes. For information on creating a machine group that contains ESXi servers, see **Adding Virtual Machines Hosted by a Server**.

You can use the **Script Catalog Manager** to identify the target type that will be used by a script.

SECURITY CONSIDERATIONS

Security Controls provides a number of security features when using the ITScripts function.

- Only scripts that are signed by authorities that you trust can be imported to the Script Catalog Manager and made available for use.
- Scripts created by Ivanti will be signed by Ivanti. If you create a custom script you must sign it using your own certificate and you will accept all liability for use of that script.
  Security Controls will use the credentials that are already associated with your machine groups to run the scripts.
- Only those scripts that you approve will be available within the Security Controls interface.
- Scripts are not encrypted. This enables you to inspect and review the scripts before they are run.

VIRTUAL MACHINE CONSIDERATIONS

Scripts can be executed on online virtual machines but not on offline virtual machines.

309. Power Management Overview

The power management function enables you to control the power state of the physical machines and the online virtual machines in your organization. The primary reasons for using power management are to:

- Prepare your machines for maintenance tasks
- Reduce power consumption and noise
- Reduce operating costs
- Prolong battery life

You can shut down, restart, or wake up machines either immediately or on a scheduled basis. You also have the ability to put machines into a sleep or hibernate state.

> TIP: If you want to perform power tasks on offline virtual machines that reside on an ESXi Hypervisor, you can do so using the **Virtual Inventory feature**.

How-To Information

For information on how to perform power management tasks, see:

- **Creating and Editing a Power State Template**
- **How to Initiate Power Management Tasks**
- **Monitoring a Power Task**
- **Initiating and Monitoring a Power Status Scan**
- **Viewing Power Status Scan Results**

Extremely Flexible Implementation Options

Security Controls provides a number of ways for you to implement the power management options.

- **Immediate Shutdowns or Restarts With No User Warning:**You can immediately shut down or restart one or more connected machines from Machine View or Scan View by using a **right-click command**. The machines must be in a fully powered on state in order to accept the shutdown or restart command. These immediate actions will typically be used for maintenance purposes when you cannot wait for machines to be shut down or restarted. When performing an immediate restart of a machine it will always be returned to a fully powered on state. For more information, see **Shutdown Implementation Notes** and **Restart Implementation Notes**.
- **Scheduled Shutdowns or Restarts With A User Warning:** You can shut down or restart one or more connected machines by using a **power state template**. The advantage of using a power state template is that it gives you the option to provide a warning to any active users of the machines. It also enables you to schedule the action to happen immediately or at some time in the future.
- Scheduled shutdowns and restarts are typically used for reducing power or turning off machines at night, over weekends, or on holidays. This can be used to fulfill a corporate "green" initiative by saving power when machines are not being used. The machines must initially be in a fully powered on state in order for the scheduled job to be performed.
  Initiate sleep or hibernate state with or without a prior restart: A power state template can be used to put machines into a sleep state or a hibernate state. You can choose to perform the action with or without a prior restart of the target machines. As with all

jobs initiated using a power state template, you can schedule the job to run now or at some time in the future. For more information, see **Sleep and Hibernation Implementation Notes**.

- **Immediate or scheduled Wake-on-LAN:** The Wake-on-LAN (WoL) feature is used to return machines to a fully powered on state. This is performed from Machine View or Scan View by using a **right-click command**. Any connected machine that is sleeping, hibernating, or powered off (but with power available to the network card) can be awakened by a WoL request. One typical reason for using WoL is to turn on machines that have been powered off overnight or over a long holiday weekend, making the machines ready for use for the coming work day. Another reason may be to power on machines prior to performing maintenance tasks such as console-based patch or asset scans. Machines that are sleeping, hibernating, or powered off cannot be scanned, so using the WoL feature ensures that your maintenance tasks will be performed on schedule.
  The Wake-on-LAN request can be issued immediately, or it can be scheduled to occur at a specific time. It's like scheduling a wakeup call for each machine. For more information on WoL, see **Wake-on-LAN Implementation Notes**.
  Machines that are sleeping, hibernating, or powered off cannot be restarted or awakened using a power state template, they must be awakened using the WoL feature.

Agentless vs. Agent-based

Power management tasks can be performed using either an agentless or an agent-based method. This section describes the agentless method. For information on performing agent-based power tasks, see **Creating and Configuring a Power Task**.

> An agentless power state task will push a small number of files from the console to each target machine. If a large number of machines are involved it may affect the performance of your network.

310. Power Management Requirements

Before performing a power management task, please confirm that you meet the following requirements.

General Requirements

- Power management tasks performed from machine groups will be successful on physical machines and online virtual machines, but not on offline virtual machines
- In order for power state changes to be made to a target machine, a user must be logged on to the machine or the local security policy **Interactive logon: Do not require CTRL+ALT+DEL** must be disabled.
- When initiating a power management action, the program will attempt to authenticate to the target machines using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:
    1. Any **managed machine credentials** (if initiating the action from Machine View or Scan View) or **machine group credentials** (if initiating the action from a machine group or favorite)
    2. **Default credentials** (used if the machine credentials are missing)

If the credential used above does not work, the Integrated Windows Authentication credentials (the credentials of the person currently logged on to the program) will be used.
If neither of these credentials work then the action will fail.

Sleep and Hibernate Requirements

In order to put a machine in or take a machine out of a sleep or hibernate state, its operating system must be configured to allow the operation.

Wake-on-LAN (WoL) Requirements

Hardware Requirements

- WoL tasks must be performed on physical machines, not on virtual machines
- WoL must be enabled in the BIOS of the target machines. See your hardware vendor's product documentation for details.
- Target machines must have either a wired or a wireless Network Interface Card (NIC) that supports WoL. See your hardware vendor's product documentation for details.
- The target machines can be in sleep, hibernate, or powered off states.
- The network cards on the target machines must have power available (either electric or battery).
- Any intervening routers may need to be configured to forward subnet-directed broadcasts. See your hardware vendor's product documentation for details on configuring your routers.
  Whether you need to configure your routers depends on where your target machines are located. If all the target machines are located on the same subnet as the console then your routers do not need to be reconfigured. If some of your target machines are behind one or more routers and thus on different subnets, then the intervening routers must be configured to forward subnet-directed broadcasts on UDP port 9.

Software Requirements

- A hardware asset scan of each target machine must be performed prior to initiating a WoL request. The scan is needed in order to obtain the MAC address of each target machine. When configuring the hardware asset scan make sure the **Network** option is selected.
- Each target machine's operating system must be configured to allow WoL.
- Outbound UDP port 9 must be open on the console machine.

Power Status Scan Requirements

A **power status scan** can be performed on physical machines, online virtual machines, and offline virtual machines.

311. Power State and Credential Requirements for Successful Scans and Deployments to Virtual Machines

An offline virtual machine (workstation-based or hosted on a server) is a file or set of files. To scan or deploy to an offline virtual machine requires permissions to the file system where the files reside. An online virtual machine is almost indistinguishable from a physical machine. To scan or deploy patches to an online virtual machine requires credentials for an administrator account on the virtual machine operating system.

Because of these differences between online and offline virtual machines, you may need to provide two sets of credentials – one for when the virtual machine is in the online state and one for when it is in the offline state.

For workstation virtual machines, if you wish to scan and/or deploy to the virtual machine in either its online or offline state, you should add the virtual machine to the machine group twice:

- For its online state, enter the machine identifier and online credentials in the machine group as you would any physical machine – on the **Machine Name**, **Domain Name**, **IP Address/Range**, or **Organizational Unit** tab.
- For its offline state, enter the information and credentials for the virtual machine file locations on the **Workstation Virtual Machines** tab.

For hosted virtual machines, you only need to specify the machine once, on the **Hosted Virtual Machines** tab. Separate credentials, however, are still required to access the machine in either the online or offline state. The **browse credentials** you enter when **connecting to the VMware server** are used when the machine is in the offline state. You should enter online credentials for each hosted virtual machine using the **Set Admin Credentials** option in the **bottom pane of the machine group editor**.

The following table summarizes the credentials used for various machine types.

Machine Type	Machine State	Machine Group Tab Used to Define the Virtual Machine	Credentials Required
Physical Machine	Online	**Machine Name**, **Domain Name**, **IP Address/Range**, **Org Unit**	Machine or machine group **credentials**
Workstation VM	Online	**Machine Name**, **Domain Name**, **IP Address/Range**, **Org Unit**	Machine or machine group **credentials**
Workstation VM	Offline	**Workstation Virtual Machines**	Machine or machine group **credentials**
Hosted VM	Online	**Hosted Virtual Machines**	Machine or machine group **credentials**
Hosted VM	Offline	**Hosted Virtual Machines**	**Browse credentials** (the creds used to log on to the VM server)

> Integrated credentials will not work for deployments to offline virtual machines.

If you specify both online and offline credentials for virtual machines, you will be able to scan and deploy to those virtual machines whether they are online or offline.

For more information, see **Deploying Patches to Virtual Machines**.

312. Predefined Patch Scan Templates

Security Patch Scan and **All Patches** are the predefined patch scanning templates provided with Security Controls. The predefined templates cannot be modified. Both predefined templates do the following:

- Perform patch scans
- Use data from the data definition file
- Report on all installed and missing patches

The primary differences between the templates are:

- **Security Patch Scan:** Scans for missing and installed security patches. This is the default scan template.
- **All Patches:** Scans for missing and installed security patches and non-security patches.

If the predefined templates are not adequate for your needs, you can create a **new scan template**.

313. Pre-Execution and Post-Execution Functions

The Security Controls script engine executes the script in parallel against multiple target machines. Sometimes you may want to do some setup operations on the console computer prior to executing the script and/or some finalization operations after all machines are complete. To specify the setup operations, include a function named “ST ConsoleBegin” within your script. This function will be called before the script is executed against any target machines. To specify finalization operations, include a function named “ST ConsoleEnd” within your script. This function will be called after the main script is executed against all target machines.

These functions must take zero parameters and be formatted as follows:

Bash

```
function ST-ConsoleBegin
{
#body of function indented from left margin
}
function ST-ConsoleEnd
{
#body of function indented from left margin
}
```

The function declarations and the opening and closing braces must begin in column 1. All other lines of the functions should not begin in column 1.

These functions are executed on the console only. Therefore, it is generally not necessary to use the **ComputerName** or **Credential** parameters on any of the cmdlets invoked in these functions.

314. Preparing to Use Security Controls Agent

All agents are configured on the Security Controls console and then either push installed from the console to the desired target machines or manually installed by an administrator. The agents can be configured with any combination of patch management capabilities, asset management capabilities, and/or power management capabilities. This section provides a roadmap of tasks you must perform when preparing to use Security Controls Agent.

> The agent machine hardware and software requirements are found in the **System Requirements** topic.

I. (Optional) Set Up and Synchronize a Distribution Server

Setting Up a Distribution Server

You have the option of setting up a distribution server that the agents can periodically access to download various files. There are a couple of reasons for using a distribution server, including:

- If some of your agents do not have Internet access and therefore won't be able to download the latest engine components, data files and patch files from the default websites. In this case you will need to store these files on a distribution server that the agents can access.
- If you have defined **custom patches** that are not available from the default websites. You must make the custom patches available by manually copying the patches to one or more distribution servers.

See **Configuring Distribution Servers** for detailed information on configuring a distribution server. In addition, when you configure your agent policy you should specify which distribution server your agents should use; see **Configuring General Settings** for details.

Synchronizing the Distribution Server

To update a distribution server with the latest patches, engine components and data files, you *synchronize* the server with the files contained on the console. See **Synchronizing Servers** for detailed information. Custom patches must be manually copied to the distribution server.

II. Create and Configure a Security Controls Agent Policy

1. From the main menu select **New >Agent Policy**.
2. Type a unique name for the policy.

There are many features you can configure within an agent policy. See **Creating A New Agent Policy** for complete details.

III. Install the Agent on the Desired Machines

There are a couple of ways you can push install an agent on one or more machines.

- For machines that have been scanned at least once and are contained in the program database, you can use the **Machine View** right-click menu (**Agents > Install/Reinstall with Policy**).
- For machines that have not been scanned and are not contained in the database, you can create a machine group containing all the machines that will run a particular agent policy and then use the **Install Agent** button to install an agent on those machines that are online.

See **Installing Agents from the Console** for detailed information on installing agents on target machines.

When performing a push install of an agent, each target machine must have a network connection to the console during the installation. This connection is required in order to exchange security information that will be used to establish an encrypted link for all future communication between the console and its agents. The agent machines must also be able to perform name resolution in order to locate the console machine.

315. Details on the Product Level and Patch Deployment Process

You have the ability to use agents to deploy both product levels and patches. On an agent machine that is missing both product levels and patches, product levels are deployed first.

Product Level Deployment Process

If an agent machine is missing multiple product levels, only one product level will be installed at a time. The agent patch task will begin by initiating the download of the first product level. Operating system product levels are downloaded at a higher priority than product levels for products. After the product level is successfully installed, the machine is restarted, rescanned, and the process is repeated until all product levels are deployed or until the daily limit is reached [see the **Limit deployments (per day)** option].

Limiting the Number of Product Levels That Can be Deployed in One Day

You can use the **Limit deployments (per day) option** to specify the maximum number of product levels that can be deployed to a machine in one day. Product levels can take a long time to deploy and almost always require a reboot of the machine, so you typically want to keep this number rather small. If you do not limit the number of product level deployments in a day you run the risk of overwhelming a machine if it is missing a large number of product levels. If a machine is missing more product levels than the specified limit, the additional product levels will be deployed the next time the patch task is run.

Note that a "day" in this case is considered to be a calendar date and not a 24 hour period. This means the day is reset at midnight. If you were to schedule the patch task to run on an hourly basis (not recommended), it would allow you to maximize an overnight maintenance window by deploying the maximum number of product levels before midnight and then again immediately after midnight.

Patch Deployment Process

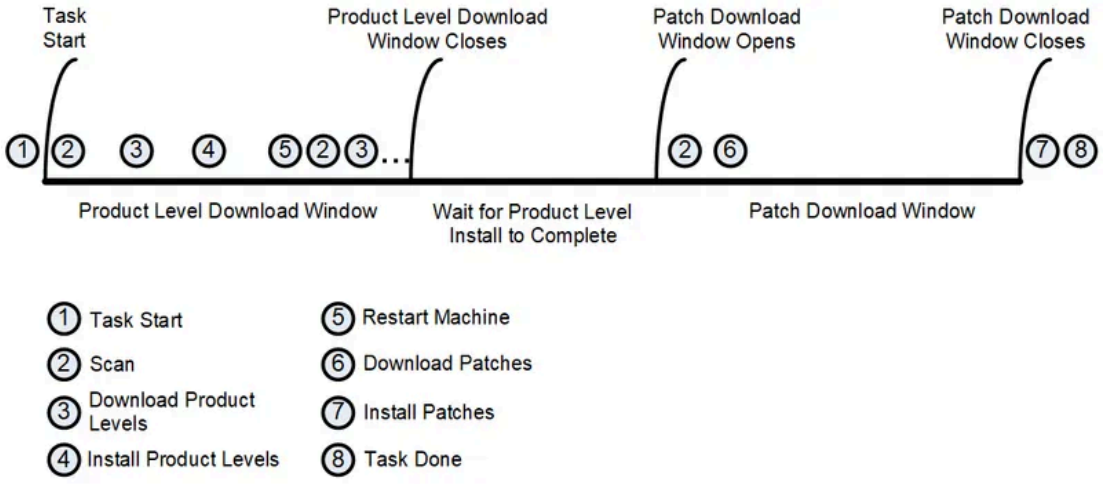
Once the list of approved patches is determined, the patches are downloaded and installed according to their priority. Security patches are downloaded first, followed by all other patch types.

Product Level and Patch Download Process

Each agent patch task is allocated a two hour total maintenance window that is allocated for downloading missing product levels and patches.

- Product levels are allotted a 60 minute window to complete the download > install > restart > rescan process.
- Patches are allotted a separate 60 minute window to download the missing patches.

Only those product levels and patches that are successfully downloaded during their respective 60 minute window will be installed by the active patch task. If the patch task cannot finish downloading all missing product levels during the first 60 minute window, the remaining product levels will be identified, downloaded, and installed the next time the patch task is run. Likewise, if the patch task cannot finish downloading all missing patches during its 60 minute window, the remaining patches will be identified, downloaded, and installed the next time the patch task is run.



Background Downloads and Checkpoint/Restart

The downloads occur in the background using idle bandwidth not being used by other applications. Foreground tasks such as Web browsing are not affected by the product level and patch download process.

If an agent machine becomes disconnected from the network during a file download, the process will be suspended and will automatically resume where it left off when the network is available again. This technique is called checkpoint/restart and is extremely useful for machines that are frequently disconnected.

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Guide to Surviving Patch Tuesday
- Microsoft SQL Server Database Maintenance
- Performing Patching in a Disconnected Environment

316. Product view

The Reporting2.Product view identifies unique Windows product and product level combinations.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Name	nvarchar(255)		The product name.
ProductLevelName	nvarchar(50)		The product level name.
ProductLevelOrder	int	X	The product level order.
EndOfLifeOn	datetime	X	The end of life date of this product.

317. Proxy Support for Agents

Proxy support for Linux and Windows Agents are now available with Security Controls.

Proxy for Linux Agents

Linux Agents

Adding a Proxy

To add a new proxy server, enter
`stagentctl proxy --add https://{isec.sever.dnsname}:3121`

> Only HTTP proxies without credentials are supported.

Listing Configured Proxies

To display all configured proxies and exclusions, enter
`stagentctl proxy --list`

Removing a Proxy

- **To remove a specific proxy from the configuration**, enter
  `stagentctl proxy --remove https://{isec.sever.dnsname}:3121`
- **To remove all configured proxies**, enter
  `stagentctl proxy --remove all`
- Command returns a configuration state after execution
  If the result is 'No proxy configured' it means that after command execution there are no proxies left.

Managing Proxy Exclusion

- **To manage hosts that should be accessed directly use the following command to exclude a specific hostname, such as "host.com'**,
  `stagentctl proxy --addexclusion host.com`
- **For suffix match exclusions, use the following command to exclude all hosts that end with '.org'.**
  For example, adding '.com' excludes all hosts ending with '.com'.
  `stagentctl proxy --addexclusion .org`
- The leading dot in the exclusion command, for example '.org' serves as a wildcard, indicating that any host ending with the specified suffix should be excluded.
- **To completely disable the proxy for all hosts use the following command**:
  `stagentctl proxy --addexclusion "*"`
- **To remove a specific host exclusion use the following command**:
  `stagentctl proxy --removeexclusion host.com`
- **To clear all exclusions use the following command**:
  `stagentctl proxy --removeexclusion all`

Registering with Proxy Configuration

- When registering the agent, add `--addproxy` parameter such as
  `stagentctl register --addproxy https://{isec.sever.dnsname}:3121`.
  This proxy is used for the registration and saved for use in future communications.
- Additionally, at the moment of registration, configuration is gathered from `http_proxy` or `HTTP_PROXY` environment variables and saved.

- It is also possible to add proxies and exclusions with `proxy --add` and `proxy --addexclusion` commands before registration attempt.

Proxy Servers with Authorization

- You can authorize proxy servers with credentials using the `--proxyauth` option when you add or perform agent registration with the `--addproxy`.
- Supports Digest, Negotiate, and NTLM methods for authorization.
- For example, use the following command when you use a proxy with authorization:
  `stagentctl proxy --add http://user:pass@host:port --proxyauth ntlm`
  `stagentctl register --addproxy http://user:pass@host:port --proxyauth ntlm`

> Ensure the `--authtype` parameter is provided if you have credentials to authenticate the proxy server. Adding a proxy with a host name that already exists overwrites the existing one with the provided parameters (authentication type, port, or credentials). `http_proxy` and `HTTP_PROXY` environment variables are ignored along with all proxy-related environment variables.

Important Notes

- A list of proxies is supported. In case of connection failure, the next proxy in the list is tried, eventually attempting a connection without a proxy. The application cycles back to the first proxy after exhausting all options or when a timeout

occurs, prioritizing the initial entries.

- The `register --addproxy` command adds a proxy to the top of the list, giving priority to the provided proxy.

Security and Communication

The application ensures that all communication via proxies is securely tunneled using the CONNECT method, suitable for encrypted communications where the proxy only acts as a tunnel provider. All proxy configurations are validated to ensure the use of the HTTP scheme without credentials and may include a port number.

Proxy for Windows Agents

Windows Agents

The web proxy for Windows Agents can be set in several ways. All methods have the same available proxy properties and differ by point of entry. Select the method appropriately.

- **Method 1**: Set proxy settings as part of an agent installation.
- **Method 2**: Set proxy settings for an installed agent that is registering, or reregistering.
- **Method 3**: Set proxy settings for an agent that is already installed and registered.

> An Agent's existing proxy config is overwritten when any of these methods are used.
> For example, an Agent that has explicit proxy settings set using proxyConfig, have those proxy settings overwritten by subsequent registration.

Method 1: During initial installation and registration

Use this method when the proxy configuration is well known at the time of agent setup, such as mass deployment of new agents. The proxy properties may be set in the silent command in the case of mass deployment, or in the registration GUI or accompanying options file that for one-off installations.

- A silent (unattended) installation initiated in Security Controls requires proxy properties to be added to the command.

For example: `IvantiSecurityControls.exe --tenantid 11111… --activationkey BLtwU… --cloudhost isec.ivanticloud.com --mode unattended --proxyMode Custom --proxyServerList ProxyServer.localdomain.com:8080 --proxyBypassList contoso.org;acme.com --proxyAuthType Basic --proxyUsername admin1 --proxyPassword password1`

- An interactive installation initiated in Security Controls requires proxy properties to be added in the accompanying options file.

For example :

```Bash
tenantid=1111….
```

```Bash
activationkey=BLtwU….
```

```Bash
cloudhost=https://isec.ivanticloud.com
```

```Bash
proxyMode=Custom
```

Bash

```
proxyServerList=ProxyServer.localdomain.com:8080
```

```
Bash

proxyBypassList=contoso.org;acme.com
```

```
Bash

proxyAuthType=Basic
```

```
Bash

proxyUsername=admin1
```

```
Bash

proxyPassword=password1
```

- Alternative to an interactive installation, specify the settings in the registration GUI under **Configure proxy**.

Method 2: Explicit registration configuration

Use this method when (re)registration is required, and reinstallation is not required. That is, the agent is already installed but registration requires changes. This approach requires also having registration information in addition to the proxy information.

The STAgentManagement tool is available with installed agents in C:\Program Files\Ivanti\Ivanti Cloud Agent.

Run `./STAgentManagement.exe` directly for help documentation.

- Use the silent flag to use the command line only

```
Bash

STAgentManagement.exe -register -p silent=true -p proxyMode=Custom -p proxyServerList=ProxyServer.localdomain.com:8080 -p proxyA
```

```
Bash

proxyPassword=password1 <and additional arguments for registration>
```

- Run the register command to bring up the registration and Proxy Configuration GUIs.

```
Bash

STAgentManagement.exe -register
```

Method 3: Explicit proxy configuration

Use this method when web proxy updates are required without changes to registration or installation.
For example, the proxy credentials or proxy server changed.

The STAgentManagement tool is found for installed agents in C:\Program Files\Ivanti\ISEC.

Run `./STAgentManagement.exe` directly for help documentation.

- Use the silent flag to use only the command line.

```
STAgentManagement.exe -proxyConfig -p silent=true -p proxyMode=Custom -p proxyServerList=ProxyServer.localdomain.com:8080 -p proxyAuthType=Basic proxyUsername=admin1 proxyPassword=password1
```

- Run the proxyConfig command to bring up 'Proxy Configuration' GUI.

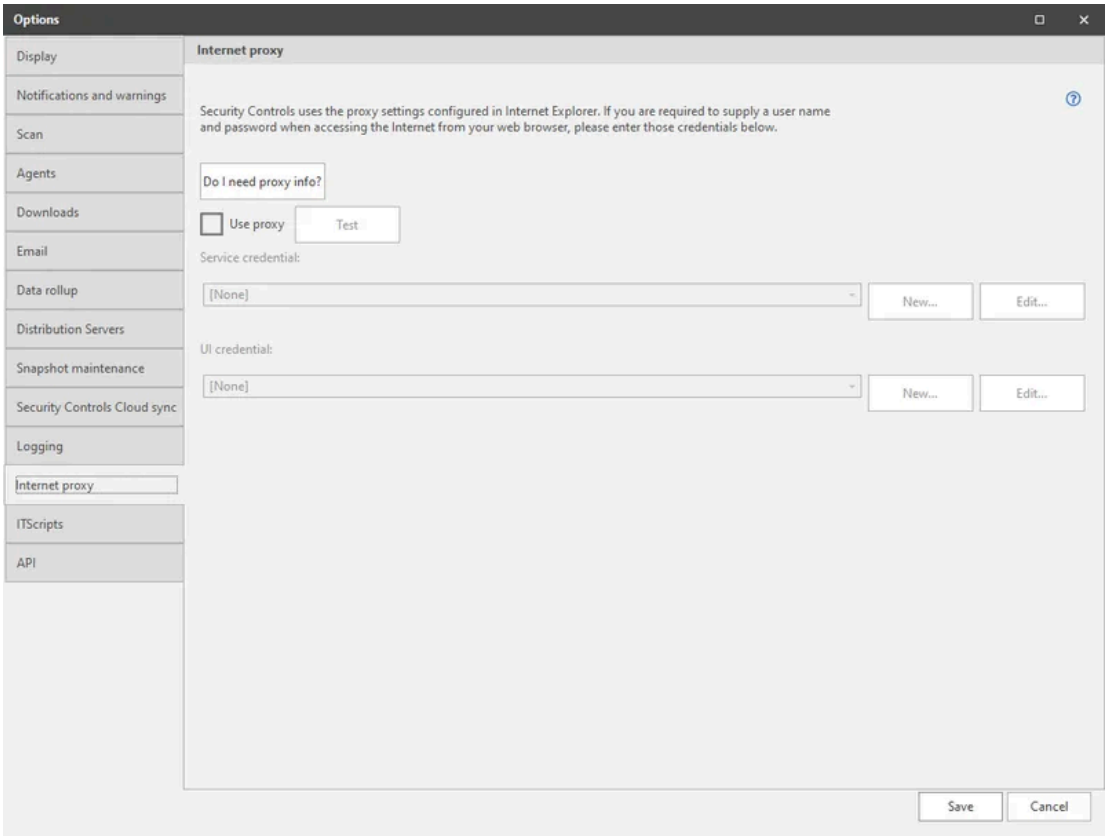
```
STAgentManagement.exe -proxyConfig
```

Properties for Proxy on Windows Clients:

1. **Proxy Mode**
   Description: Sets the proxy mode.
   - 'None' refers that no proxy is used.
   - 'Auto' refers to the proxy mode that is detected from current OS settings. It is the Default mode.
   - 'Custom' refers to other proxy properties are used.
2. **Server List**
   Description: The proxy server name and corresponding port; multiple servers may be specified.
3. **Bypass List**
   Description: The addresses that are allowed to be bypassed by the proxy.
4. **Auth Type**
   Description: Sets the authentication type for the proxy.
   - 'Basic' requires a username and password to be defined which are used.
   - Other options are 'Digest', 'NTLM', 'Negotiate', and 'None' which means no credentials are used.
   - 'None' is the default value.
5. **Username and password**
   Description: Credentials are securely stored to be used with auth types of 'Basic'.
6. **Update WinHttp Proxy**
   Description: This is only available via the command line and not in any GUI. Only customers that require the agent to not interfere with the WinHTTP proxy settings should set this.

318. Internet Proxy Options

The **Internet Proxy Options** dialog allows you to modify the proxy settings used by Security Controls when accessing the Internet using your Web browser. In general, Security Controls checks the proxy settings in Internet Explorer and conducts an Internet connectivity test to determine whether or not proxy server settings are necessary. If Security Controls is unable to access the Internet using these settings, or if you are required to enter a user name and password each time you launch your browser and browse the Internet, you will need to configure the proxy options.



Field	Description
Do I need Proxy Info?	To see if Security Controls can use your current Internet Explorer proxy settings to access the Internet and perform other operations, click this button. If the test is successful then nothing further is required. If the test fails it typically means you utilize authorization and you need to modify your proxy settings by specifying console and service credentials.
Use proxy	If enabled, indicates that you will supply proxy credentials and allows you to specify user name and password information. If you clear the check box after specifying credentials, the credentials will be saved but not used. Proxy Auto-Configuration (PAC) files are not supported for proxy configuration.
Service credential	Select the credential (the user name and password pair) used by the program service when accessing the Internet. The same service credential can be used by different administrators. Only credentials that are shared with background services are contained in this list. If the credential you are looking for is not listed it probably means it is not defined as a shared credential. See **Shared Credentials** for information on how to share a credential with background services.
UI credential	Select the credential (the user name and password pair) you use when accessing the Internet with your Web browser. It may be necessary to specify a domain as part of your user name (for example: mydomain\my.name). There may be multiple credentials available here for selection, one for each of your Security Controls administrators.
Test	To test the credentials, click this button.

IMPORTANT! See **HTTP Proxy Post Installation Notes** for additional details about using an HTTP proxy.

319. Frequently Asked Questions

Here are some questions that are frequently asked by new Security Controls API users.

- Can I use the API to schedule scans and deploys?
- Yes, you can schedule a script to run at a specific time. You can utilize the existing scheduling capabilities of an orchestrator or of Windows Task Scheduler, or you can do a scheduled scan in Security Controls.
  Can I use the API to create, configure and delete credential, templates and groups?
- Yes. You can reference existing credentials, machine groups, templates, etc. within your API commands. You can also use the API to add new credentials, templates, machine groups and patch groups.
  Can I still get reports?
- Yes, all manually created Security Controls reports will continue to work and will include operations initiated by the API. Scheduled reports that are based on date ranges will also be automatically generated, but reports will not be automatically generated for patch scans initiated from the API.
  What about logging?
- The same logging levels are available at both the user interface level and the API level.
  Can we show members of an object coming out of a scan commandlet?
- Yes. Here's an example of how to show the 10 most recent scans:

Bash

```
> $scans = Get-PatchScan –count 10
```

Bash

```
> $mostRecentScan = $scans[0]
```

Bash

```
> $mostRecentScan | Get-Member
```

Bash

```
> $mostRecentScan | Format-PatchScanTable
```

Bash

```
> $mostRecentScan.MachineStates[0] | Get-Member
```

```
Bash

>
```

Can I exclude certain machines before performing a deployment?

- Yes, you will do this by controlling the scan input. You will specify which machines should be scanned, pare that down using attributes and then feed the pared down scan into the deployment process.
  Can I check to see if a patch install fails (post-deploy)?
- Yes. See the error code. You can view this information using Deployment Tracker or by using the Get-PatchDeploy command.
  Can I retrieve patch scan deployment results (even UI-initiated scans) for reporting purposes?
  Yes.

320. PowerShell API Requirements

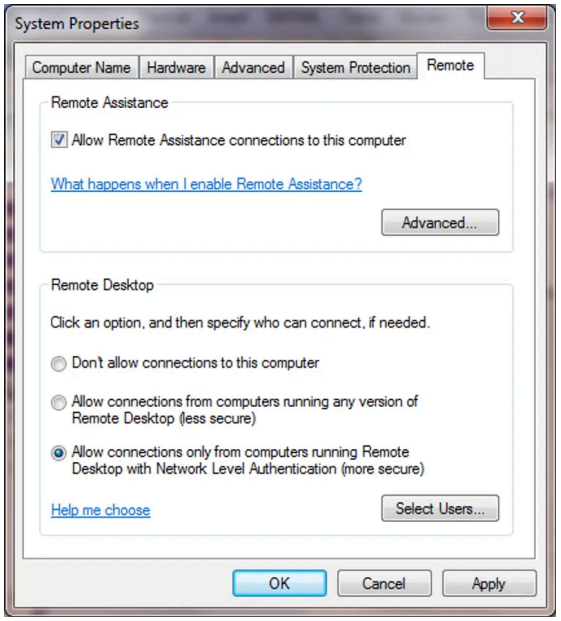
The following are required in order to use the API feature:

- Ivanti Security Controls 2018.3 or later
- The API and Windows PowerShell components and modules are automatically installed with Ivanti Security Controls 2018.3 or later. No configuration is required.
  Must be run from the Ivanti Security Controls console.
- The API commands will run in a user session on the console. The user's context is handed off to the Protect service so that the lifetime is decoupled from the interactive session.
  Windows PowerShell v4.0 or later must be installed on the console.
- The Windows PowerShell console must be run with administrator rights.
- The STProtect API module must be imported before executing any PowerShell commands.

321. RDP Requirements

Before attempting a Remote Desktop connection, please confirm that you meet the following requirements.

- The Security Controls console must have network access to the target machine.
- The RDP port specified by Security Controls must be the same as the RDP port specified by the target machine.
- If the target machine is not using the default RDP port (3389), use the **Machine Properties** dialog to match the port value specified on the target machine.
  The target machine must be powered on; it cannot be in sleep or hibernation mode.
- You must have access to a user account on the target machine.
- The target machine must be configured to allow Remote Desktop Connection.
  1. On the target machine, right-click the **Computer** icon and choose **Properties**.
  2. Select the more secure connection option when possible.



You must have permission to connect to the target machine.
For permission to connect, you must be on the list of users. On the **System Properties** dialog (shown above), click **Select Users** and add the name of the user.

322. Agent view

The Reporting2.Agent view displays currently known information about an installed agent.

Column Name	Data Type	Nullable	Description
MachineId	int		The machine id where the agent is installed. See [Reporting2].[Machine].
AssignedPolicyName	nvarchar(256)	X	The assigned policy name.
LastCheckIn	datetime	X	The time the agent last checked in.
PatchDataVersion	nvarchar(23)	X	The patch data version used for agent assessments.

323. AssessedMachineState view

The Reporting2.AssessedMachineState view displays all assessments performed on a machine.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
MachineId	int	X	The machine id of this assessment. See **[Reporting2].[Machine]**.
PatchScanId	int	X	The patch scan id of this assessment. See **[Reporting2].[PatchScan]**.
IPAddress	nvarchar(45)	X	The IP address of this machine. This will be displayed in IPV4 or IPV6 format.
AssessedOn	datetime	X	The assessment date.

324. Agent view

The Reporting3.Agent view displays currently known information about an installed agent.

Column Name	Data Type	Nullable	Description
MachineId	int		The machine id where the agent is installed. See **Machine view**.
AssignedPolicyName	nvarchar(256)	X	The assigned policy name.
LastCheckIn	datetime	X	The time the agent last checked in.
PatchDataVersion	nvarchar(23)	X	The patch data version used for agent assessments.

325. Architecture view

The Reporting3.Architecture view describes the architecture types.

Column Name	Data Type	Nullable	Description
Id	smallint		The architecture id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(256)		Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.Architecture view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[Architecture]
```

Id	Value	Description
0	Unknown	The type is unknown.
1	Any	Any architecture.
2	X86	This is an X86 - 32 bit architecture.
3	X64	This is an X86 - 64 bit architecture.
4	PowerPC	This is a PowerPC architecture.
5	Sparc	This is a Sparc architecture.
6	IA64	This is an Intel Itanium architecture.

326. AssessedMachineState view

The Reporting3.AssessedMachineState view displays all assessments performed on a machine.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
MachineId	int	X	The machine id of this assessment. See **Machine view**.
PatchScanId	int	X	The patch scan id of this assessment. See **PatchScan view**.
IPAddress	nvarchar(45)	X	The IP address of this machine. This is displayed in IPV4 or IPV6 format.
AssessedOn	datetime	X	The assessment date.

327. CVE view

The Reporting3.Cve view (Common Vulnerabilities and Exposures) displays the common vulnerability and exposure name and the exploitability index of a patch as it applies to a product.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
Name	nvarchar(20)		The name of the CVE.
CVSSv2	decimal		The Common Vulnerability Scoring System (CVSS) version 2 score.
CVSSv3	decimal		The Common Vulnerability Scoring System (CVSS) version 3 score.

328. LinuxAdvisoryCVE view

The Reporting3.LinuxAdvisoryCve view displays information about Linux notifications.

Column Name	Data Type	Nullable	Description
Id	bigint		This is the unique identifier.
NotificationId	int	X	The advisory ID. See **LinuxAdvisory view**.
CveId	int	X	The CVE ID. See **CVE view**.

329. LinuxAdvisoryInstallStatus view

The Reporting3.LinuxAdvisoryInstallStatus view describes Linux advisory install status codes.

Column Name	Data Type	Nullable	Description
Id	smallint		The id of install status.
Value	nvarchar(100)		The value of install status.
Description	nvarchar(256)		The description of install status.

Content

You can run the following query to verify the contents of the Reporting3.LinuxAdvisoryInstallStatus view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[LinuxAdvisoryInstallStatus]
```

Id	Value	Description
0	Unspecified	Unspecified.
1	Not applicable	Not applicable.
2	Missing	Missing.
4	Currently Installed	Currently Installed.
8	Older than current	Older than current.

330. LinuxAdvisoryPackage view

The Reporting3.LinuxAdvisoryPackage view displays package information included in an advisory.

Column Name	Data Type	Nullable	Description
Id	bigint		This is the unique identifier.
NotificationId	int	X	The advisory ID. See **LinuxAdvisory view**.
PackageId	int	X	The Linux package ID. See **LinuxPackage view**.
ManagedMachineId	int	X	Managed machine ID.
StaticInfo	bit	X	If this is a static info.

331. LinuxAdvisory view

The Reporting3.LinuxAdvisory view displays information about Linux advisories.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Name	nvarchar(255)		The advisory name.
Title	nvarchar(1024)	X	The advisory title.
Description	nvarchar(4000)	X	Description of the advisory.
IssuedOn	Datetime2	X	The date the advisory was issued.
UpdatedOn	Datetime2	X	The date the advisory was revised.

332. LinuxArchitecture view

The Reporting3.LinuxArchitecture view describes Linux machine architectures.

Content

You can run the following query to verify the contents of the Reporting3.LinuxArchitecture view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[LinuxArchitecture]
```

Id	Value	Description
0	unspecified	unspecified
1	x86_64	x86_64
2	i386	i386
3	i586	i586
4	i686	i686
5	noarch	noarch

333. LinuxDetectedUpdateAdvisory view

The Reporting3.LinuxDetectedUpdateAdvisory view identifies the advisories detected in an assessment.

Column Name	Data Type Nullable	Description
Id	bigint	This is the unique identifier.
AssessedMachineStateId	Int	The id of the assessed machine state. See **AssessedMachineState view**.
LinuxAdvisoryId	Int	The advisory ID. See **LinuxAdvisory view**.
LinuxInstallStateId	tinyint	The install state of the advisory. See **LinuxAdvisoryInstallStatus view**.

334. LinuxDetectedUpdatePackage view

The Reporting3.LinuxDetectedUpdatePackage view identifies the packages detected in an assessment.

Column Name	Data Type	Nullable	Description
Id	bigint		This is the unique identifier.
AssessedMachineStateId	int		The ID of the assessed machine state. See **AssessedMachineState view**.
LinuxAdvisoryId	int	X	The advisory ID. See **LinuxAdvisory view**.
AvailableLinuxPackageId	int	X	The available Linux package ID. See **LinuxPackage view**.
InstalledLinuxPackageId	int	X	The installed Linux package ID. See **LinuxPackage view**.
LinuxInstallStateId	tinyint	X	The install state of the package. See **LinuxAdvisoryInstallStatus view**.

335. LinuxDetectedUpdateRepository view

The Reporting3.LinuxDetectedUpdateRepository view identifies the repositories reported in an assessment.

Column Name	Data Type	Nullable	Description
Id	bigint		This is the unique identifier.
AssessedMachineStateId	int		The ID of the assessed machine state. See **AssessedMachineState view**.
LinuxRepositoryId	int		The repository ID. See **LinuxRepository view**.
MetaDataExpiringOn	datetime2	X	The date meta data expires on.
RepositoryUpdatedOn	datetime2	X	The date the repository was updated on.

336. LinuxDistribution view

The Reporting3.LinuxDistribution view displays Linux distributions that have been reported from current machines.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Uid	uniqueidentifier		GUID.
DistributionId	nvarchar(255)		The distribution ID.
Name	nvarchar(255)		The distribution name.

337. LinuxPackageRemediationDetailedCode view

> This view has been deprecated.

The Reporting3.LinuxPackageRemediationDetailedCode view describes package remediation detailed codes.

Content

You can run the following query to verify the contents of the Reporting3.LinuxPackageRemediationDetailedCode view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[LinuxPackageRemediationDetailedCode]
```

Column Name	Data Type	Nullable	Description
Id	smallint		The id of Linux package remediation detailed code.
Value	nvarchar(100)		The value of Linux package remediation detailed code.
Description	nvarchar(256)		The description of Linux package remediation detailed code.

Id	Value	Description
0	Unspecified	Unspecified
1	Installed	Installed
2	Failed	Failed
3	Removed	Removed
4	Updated	Updated
5	Pending Reboot	Pending Reboot

338. LinuxPackageRepository view

The Reporting3. LinuxPackageRepository view joins package view and repository view.

Column Name	Data Type	Nullable	Description
PackageId	int		This is the unique identifier.
FullName	nvarchar(255)		The package full name.
ShortName	nvarchar(255)		The package short name.
RepositoryId	int		The repository ID. See **LinuxRepository view**.
PackageVersion	nvarchar(255)	X	The package version.
ArchitectureId	tinyint	X	The architecture ID. See **LinuxArchitecture view**.
VendorRepositoryId	nvarchar(255)		Repository ID string set by vendor.
RepositoryName	nvarchar(255)		Name of the repository.
LastMetaDataExpiringOn	datetime2	X	The latest date meta data expires on.
RepositoryUrl	nvarchar(255)		URL of the repository.

339. LinuxPackage view

The Reporting3.LinuxPackage view identifies the Linux packages.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
FullName	nvarchar(255)		The package full name.
ShortName	nvarchar(255)		The package short name.
RepositoryId	int		The repository ID. See **LinuxRepository view**.
Version	nvarchar(255)		The package version.
ArchitectureId	tinyint		The architecture ID. See **LinuxArchitecture view**.

340. LinuxRepository view

The Reporting3.LinuxRepository view describes Linux package repositories.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
VendorRepositoryId	nvarchar(255)		Repository Id string set by vendor.
Name	nvarchar(255)		Name of the repository.
LastMetaDataExpiringOn	datetime2	X	The latest date meta data expires on.
LastRepoUpdatedOn	datetime2	X	The latest date the repository was updated on.
Url	nvarchar(255)		URL of the repository.

341. LinuxUpdateDeploymentAdvisory view

The Reporting3.LinuxUpdateDeploymentAdvisory view describes the deployments of advisories.

Column Name	Data Type	Nullable	Description
Id	bigint		This is the unique identifier.
DeploymentId	int		Deployment ID. See **LinuxUpdateDeployment view**.
LinuxAdvisoryId	int		The advisory ID. See **LinuxAdvisory view**.
DetectedAdvisoryId	bigint	X	The id of the detected update advisory ID. See **LinuxDetectedUpdateAdvisory view**.
RemediationState	tinyint		The remediation state of the advisory: `0` – Success `1` – Failed `2` – Pending Reboot
ExitCode	int	X	Exit code. Success is null or `0`.
ErrorNote	nvarchar(max)	X	Detailed error message.
PolicyRequested	bit	X	If this advisory was specified in the patch group.

342. LinuxUpdateDeploymentPackage view

The Reporting3.LinuxUpdateDeploymentPackage view describes deployments of packages.

Column Name	Data Type	Nullable	Description
Id	bigint		This is the unique identifier.
DeploymentId	int		Deployment ID. See **LinuxUpdateDeployment view**.
LinuxAdvisoryId	int	X	The advisory ID. See **LinuxAdvisory view**.
DetectedPackageId	bigint	X	The id of the detected update package ID. See **LinuxDetectedUpdatePackage view**.
RequestedVersionId	int	X	The requested Linux package ID. See **LinuxPackage view**.
InstalledVersionId	int	X	The installed Linux package ID. See **LinuxPackage view**.
PreviousVersionId	int	X	The previous Linux package ID. See **LinuxPackage view**.
RemediationDetailedCode	tinyint		Remediation detailed code. See **LinuxPackageRemediationDetailedCode view**. This view has been deprecated.
RemediationState	tinyint		Remediation state of the package. `0` – Success `1` – Failed `2` – Pending Reboot
ExitCode	int	X	Exit code. Success is null or `0`.
ErrorNote	nvarchar(max)	X	Detailed error message.
PolicyRequested	bit	X	If this package was specified in the patch group.

343. LinuxUpdateDeployment view

The Reporting3.LinuxUpdateDeployment view describes deployments of advisories and packages.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Uid	uniqueidentifier		Deployment GUID.
ConsoleId	int		Console ID.
AssessedMachineStateId	int		The id of the assessed machine state. See **AssessedMachineState view**.
StartedOn	datetime2		The date the deployment started on.
EndedOn	datetime2		The date the deployment ended on.
RebootRequested	bit	X	If a reboot is requested.
RebootScheduled	bit	X	If a reboot is scheduled.
ExitCode	int	X	Exit code. Success is null or `0`.
ErrorNote	nvarchar(max)	X	Detailed error message.

344. LinuxUpdateSeverity view

The Reporting3.LinuxUpdateSeverity view describes advisory severity levels.

Column Name	Data Type	Nullable	Description
Id	smallint		The id of advisory severity level.
Value	nvarchar(100)		The value of advisory severity level.
Description	nvarchar(256)		The description of advisory severity level.

Content

You can run the following query to verify the contents of the Reporting3.LinuxUpdateSeverity view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[LinuxUpdateSeverity]
```

Id	Value	Description
0	Unspecified	Unspecified
1	Critical	Critical
2	Important	Important
3	Moderate	Moderate
4	Low	Low

345. LinuxUpdateType view

The Reporting3.LinuxUpdateType view describes the Linux advisory types.

Column Name	Data Type	Nullable	Description
Id	smallint		The ID.
Value	nvarchar(100)		The value.
Description	nvarchar(256)		The description.

Content

You can run the following query to verify the contents of the Reporting3.LinuxUpdateType view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[LinuxUpdateType]
```

Id	Value	Description
0	Unknown	Unknown
1	Security	Security
2	Bugfix	Bugfix
3	Enhancement	Enhancement

346. Machine view

The Reporting3.Machine view displays currently known information about a machine that has been assessed.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
DnsName	nvarchar (255)	X	The dns name of this machine.
Domain	nvarchar (255)	X	The domain name of this machine.
Language	Int	X	The detected language of this machine.
Name	nvarchar (255)	X	The netbios name of this machine.
OperatingSystemFamilyId	Int		The id of the operating system family. See **OperatingSystemFamily view**.
ArchitectureId	Int		The id of the architecture. See **Architecture view**.
Distribution	nvarchar (100)	X	The distribution.
LinuxDistributionId	Int	X	The Linux platform ID. See **LinuxDistribution view**.
ProductId	int	X	The product ID. See **WindowsProduct view**.
LastKnownIP	nvarchar (45)	X	The IP address of this machine. This is displayed in IPV4 or IPV6 format.
LastPatchAssessedOn	datetime	X	The time this machine was last assessed upon. (This is the date the machine was scanned, not the date of the patch scan scheduled).
LastAssessedMachineStateId	Int	X	The id of the last assessed machine state. See **AssessedMachineState view**.
LastPatchMachineGroupName	nvarchar (255)	X	The name of the machine group where this machine was defined.
AssignedGroup	nvarchar (255)		The name of the machine group for grouping agents in Machine view.
VirtualInventoryPath	nvarchar (260)	X	The virtual inventory path.
VirtualServerName	nvarchar (256)	X	The virtual server name.

347. OperatingSystemFamily view

The Reporting3.OperatingSystemFamily view describes the operating system family.

Column Name	Data Type	Nullable	Description
Id	smallint		The operating system family ID.
Value	nvarchar(100)		The string value of the ID.
Description	nvarchar(256)		Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.OperatingSystemFamily view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[OperatingSystemFamily]
```

Id	Value	Description
0	Unknown	The type is unknown.
1	Aix	This is an AIX operating system.
2	Hpux	This is an HP-UX operating system.
3	Linux	This is a Linux system.
4	Mac	This is a Mac system.
5	Solaris	This is a Solaris operating system.
6	Windows	This is a Windows system.

348. PatchCountsByScanMachine view

The Reporting3.PatchCountsByScanMachine view displays patch scan information.

Column Name	Data Type	Nullable	Description
PatchFoundOrInstalled	Int	X	The number of patches installed.
PatchMissing	Int	X	The number of patches missing.
ProductLevelMissing	Int	X	The number of product levels missing.
AssessedMachineStateId	Int		The assessed machine state ID. See **AssessedMachineState view**.

349. PatchScan view

The Reporting2.PatchScan view displays assessment information.

Column Name	Data Type	Nullable	Description	
Id	int		The unique identifier.	
ConsoleName	nvarchar(100)		The console name where this patch was performed.	
DefinitionDate	datetime	X	The assessment data definition date.	
DefinitionVersion	nvarchar(23)	X	The assessment data definition version.	
EndedOn	datetime		The date the assessment ended.	
IsScanComlete	int		Determines if the scan is complete: `0` : The scan is not complete. `1` : The scan is complete.	
Name	nvarchar(255)	X	The scan name.	
StartedOn	datetime	X	The date the scan started.	
ScanTemplateName	nvarchar(255)	X	The scan template name.	
User	nvarchar(256)	X	The name of the user that performed the scan.	
SourceTypeId	tinyint		The source type id. See Reporting3.SourceType.	
ScanTypeId	tinyint		The scan type id. See Reporting3.ScanType.	

350. ScanType view

The Reporting2.ScanType view describes the scan type.

Column Name	Data Type	Nullable	Description
Id	smallint		The scan type ID.
Value	nvarchar(100)		The string value of the ID.
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting3.ScanType view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[ScanType]
```

351. SourceType view

The Reporting3.SourceType view defines source types.

Column Name	Data Type	Nullable	Description
Id	smallint		The source type ID.
Value	nvarchar(100)		The string value of the ID.
Description	nvarchar(512)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting3.SourceType view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[SourceType]
```

Id	Value	Description
0	Unknown	Invalid or unknown source.
1	Interactive User	
2	Agent	
3	API	

352. WindowsDeployState view

The Reporting3.DeployState view defines deployment states.

Column Name	Data Type	Nullable	Description
Id	int		The deploy state ID.
Value	nvarchar(100)		The value of the deploy state.
Description	nvarchar(512)		A description of the deploy state.

Content

Run the following query to generate the contents for the Reporting3.WindowsDeployState view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[WindowsDeployState]
```

Id	Value	Description
0	None	Initial value when record is created.
1	Failed	Deployment failed.
2	Copied	Files/data were copied.
3	Scheduled	Deployment was scheduled.
4	Executing	Before executing the patch file.
5	Executed	After executing the patch file if deployment template specified no reboot.
6	Pending Reboot	Deployment is pending reboot. • After executing patch file if the deployment template specifies reboot always • After running a patch uninstall
7	Verified Missing	Rescan completed and found the patch is missing.
8	Verified Fixed	Rescan completed and found the patch is not missing.
9	Unable To Verify	Could not perform the rescan (for example, failed to connect to the target machine).
10	Canceled	Deployment was canceled.
11	Complete Not Verified	Deployment is complete but could not be verified.
12	Pending Rescan	Deployment is pending rescan.
13	Install success inferred	Install success inferred.
20	Waiting for virtual server	Waiting for virtual server.
21	Initializing virtual deployment	Initializing virtual deployment.
22	Disabling network	Disabling network.
23	Powered on	Powered on.
24	Monitoring install status	Monitoring install status.
25	Powering off	Powering off.

Id	Value	Description
26	Enabling network	Enabling network.
27	Enabling sysprep	Enabling sysprep.
28	Taking snapshot	Taking snapshot.
29	Removing snapshots	Removing snapshots.
30	Converting to template	Converting to template.
31	Patch download failed - retry scheduled	Patch download failed - retry scheduled.
32	Building the deployment package	Building the deployment package.
33	Deploying packages	Copying files and scheduling the installation.
34	Finished pending reboot	Installation complete and reboot is scheduled.
35	Downloaded	Downloaded.
36	Rescan In progress	Rescan In progress.
37	Files necessary to the deployment are being downloaded	Files necessary to the deployment are being downloaded.
38	File download starting	File download starting.
39	File download failed	File download failed.
40	File download succeeded	File download succeeded.
41	File downloads complete	File downloads complete.

Id	Value	Description
42	File downloads failed	File downloads failed.
43	Deployment operation executing	Deployment operation executing.
44	Waiting for the machine to reboot	Waiting for the machine to reboot.
45	The machine has rebooted	The machine has rebooted.
80	Unable to connect	Error: 452 - Unable to connect to the remote machine.
81	Unable to connect	Error: 453 - Unable to connect to the remote machine.
82	General network error	Error: 230 - A general network error has occurred. Please refer to the system documentation for more information.
83	No registry access	No registry access.
84	Platform is not NT	Platform is not NT.
85	Unsupported operating system service pack	Unsupported operating system service pack.
86	No Administrator share access	No Administrator share access.
87	Machine not found	Machine not found.
88	Credentials invalid	Credentials invalid.
89	Machine not found	Machine found, but not listening on port 139 or 445.
90	Not administrator	User does not have Administrator permissions.
91	Network problem	Error: 201 - A network problem is preventing the specified machine from being scanned. Check to see that your computer (the scanning machine) is properly connected to the network and that you can remotely log on to the specified machine.

Id	Value	Description
92	Machine not found on ports	Machine not found on port 139 or 445 (firewalled?)
93	Network or system error	Error: 202 - A network or system error occurred while the scan was in process. Check to see that your scanning machine is properly connected to the network and the machine being scanned is still connected to the network. Also ensure that the remote machine is running the Server service.
94	Unknown exception	An unknown exception occurred.
95	Virtual deployment failed	Virtual deployment failed.
96	Virtual deployment already in progress	Virtual deployment already in progress.
97	Pre-deploy snapshot failed	Pre-deploy snapshot failed.
98	Convert to virtual machine failed	Convert to virtual machine failed.
99	Deployment complete	Entire deployment/installation is complete including reboot if required.
100	Uninstall succeeded	Uninstallation is complete, not waiting (or no longer waiting) for reboot.
101	Staged deployment scheduled	Staged deployment scheduled.
102	Failed to schedule staged deployment	Failed to schedule staged deployment.
103	User canceled	The scheduled deployment task was deleted.
150	Virtual deployment failed	Error.
151	Disabling network failed	Disabling network failed.
152	Powering on failed	Powering on failed.

Id	Value	Description
153	Invalid host credentials	Invalid host credentials.
154	Invalid guest credentials	Invalid guest credentials.
155	Powering off failed	Powering off failed.
156	Enabling network failed	Enabling network failed.
157	Enabling sysprep failed	Enabling sysprep failed.
158	Taking snapshot failed	Taking snapshot failed.
159	Removal of snapshot failed	Removal of snapshot failed.
160	Converting to template failed	Converting to template failed.
161	Invalid state	Invalid state.
162	Virtual deployment time expired	Virtual deployment failed due to deployment expiration.
163	Virtual deployment time exceeded	Virtual deployment failed. Time exceeded.
164	VMware Tools must be running	VMware Tools must be running.
165	Virtual machine locked	Unable to open virtual disk because it is locked. It may be running or suspended.
166	Offline operations not supported	Offline operations not supported on this virtual server version.

Id	Value	Description
180	Error	An error occurred.
181	Unable to connect to virtual server	Unable to connect to virtual server.
182	Unable to find virtual machine	Unable to find virtual machine.
183	Error creating deployment package	Error creating the deployment package. See log for details.
184	Unable to deploy to suspended virtual machine	Unable to deploy to suspended virtual machine.
185	Unable to deploy using a distribution server	Unable to deploy to an offline virtual machine using a distribution server due to network isolation.
186	Online credentials are not available	Online credentials are not available for the virtual machine.
187	Failed to schedule patch deployment	Failed to schedule patch deployment.
188	Patch copy failed	Unable to copy the file to target machine.
189	Patch removed due to missing file	Patch was removed because the uninstall file does not exist on target machine.
190	Not licensed to deploy patch	Your license does not support deployment of this patch.
191	Language download not available	Patch is not available for the language selected.
192	File validation failed	File validation failed.
193	File missing	File missing.

Id	Value	Description
194	Deployment licenses exceeded	Deployment licenses exceeded.
195	Target machine out of disk space	Target machine out of disk space.
270	Machine name mismatch	The current machine name does not match the expected machine name.
817	Unable to read VMX file	The VMX file for the specified VMware Workstation image was not found or was not accessible.

353. WindowsDetectedPatchState view

The Reporting3.DetectedPatchState view displays the state of a patch found on a machine.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
AssessedMachineStateId	int		The assessed machine state ID. See **AssessedMachineState view**.
PatchId	int		The patch ID. See **WindowsPatch view**.
ProductId	int		The product ID. See **WindowsProduct view**.
InstalledOn	datetime	X	The date the patch was installed.
InstallStateId	int	X	The install state ID. See **WindowsInstallState view**.

354. WindowsInstallState view

The Reporting3.WindowsInstallState view defines installation states.

Column Name	Data Type	Nullable	Description
Id	int		The install state ID.
Value	nvarchar(100)		The string value of the ID.
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting3.WindowsInstallState view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[WindowsInstallState]
```

Id	Value	Description
-1	Not Recorded	A service pack level detection error has occurred or the product level is an unsupported version.
0	Warning	Indicates a problem with the patch and rarely, if ever, occurs. This value can, however, occur in old patch data.
1	Note	A note exists for this patch. Please reference the QNumber on vendor websites for more information.
2	Informational	No patches were detected for this product. Either all patches were applied or no patches exist.
3	Installed	A patch is installed.
4	Missing Patch	A missing patch was detected.
6	Missing Service Pack	A missing service pack was detected.

355. WindowsPatchAppliesTo view

The Reporting3.WindowsPatchAppliesTo view identifies the products and CVEs that a patch applies to.

Column Name	Data Type	Nullable	Description
PatchId	int		The patch ID.
ProductId	int		The product ID. See **WindowsProduct view**.
CveId	int	X	The cve ID. See **CVE view**.

356. WindowsPatchDeployment view

The Reporting3.WindowsPatchDeployment view displays windows patch deployment information.

Column Name	Data Type	Nullable	Description
DeployId	Int		The unique identifier of the deployment.
DetectedPatchStateId	Int		The detected patch state id. See **WindowsDetectedPatchState view**.
DeployScheduledOn	datetime	X	The date the patch was scheduled for deployment (local time).
DeployStartedOn	Datetime	X	The date the patch installation started (GMT).
DeployEndOn	Datetime	X	The date the patch installation ended (GMT).
DeployStateId	Int	X	The deployment status Id. See **WindowsDeployState view**.
ResultCode	Int	X	The result code from a patch deployment. Common results codes are: `0` : Installed, no reboot required `3010` : Installed, reboot required Other error codes are patch specific.

357. WindowsPatchType view

The Reporting3.WindowsPatchType view defines windows patch types.

Column Name	Data Type	Nullable	Description
Id	int		The patch type ID.
Value	nvarchar(100)		The string value of the ID.
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting3.WindowsPatchType view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[WindowsPatchType]
```

Id	Value	Description
0	Security Patches	Microsoft Security Patches.
1	Security Patches	
2	Software Distribution	
3	Security Tools	
4	Non-security Patches	
6	Custom Actions	

358. WindowsPatch view

The Reporting3.Patch view displays windows patch information.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Bulletin	nvarchar(255)		The patch bulletin.
QNumber	nvarchar(255)		The QNumber.
BulletinTitle	nvarchar(255)	X	The patch bulletin title.
VendorSeverityId	Int	X	The minimum vendor severity of this patch. See **WindowsVendorSeverity view**.
IsCustomPatch	bit		Indicates if this is a custom patch.
PatchTypeId	Int	X	The patch type ID. See **WindowsPatchType view**.
ReleaseOn	datetime	X	The date this patch was released.
IavaId	Nvarchar(50)	x	The iava id.

359. WindowsProduct view

The Reporting2.Product view identifies unique windows product and service pack combination.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Name	nvarchar(255)		The product name.
ProductLevelName	nvarchar(50)		The product level name.
ProductLevelOrder	int	X	The product level order.
EndOfLifeOn	datetime	X	The end of life date of this product.

360. WindowsVendorSeverity view

The Reporting2.WindowsVendorSeverity view defines vendor severity states.

Column Name	Data Type	Nullable	Description
Id	smallint		The vendor severity ID.
Value	nvarchar(100)		The value of the vendor severity.
Description	nvarchar(256)		The vendor severity description.

Content

You can run the following query to verify the contents of the Reporting3.WindowsVendorSeverity view.

SQL

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting3].[WindowsVendorSeverity]
```

Id	Value	Description
0	None	None.
1	Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
2	Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.
3	Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
4	Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

361. Sample Query: CVE Vulnerability Report

The Security Controls views provide access to data that is in the Ivanti Security Controls database but that is not available in the **predefined reports**. This section provides sample queries that illustrate how to reference a Security Controls view.

This is a CVE vulnerability report that displays the CVE name and how many machines are affected because of a missing patch on the latest patch scan.

Query

SQL

```sql
SELECT
    cve.[Name] AS [CVE Name],
    cve.[Id] AS [CVE ID],
    patch.[Bulletin] AS [Bulletin Id],
    patch.[QNumber] AS QNumber,
COUNT( DISTINCT machine.[Id]) AS [Machines Missing Count]
FROM
    [Reporting3].[Machine] AS machine
INNER JOIN
    [Reporting3].[AssessedMachineState] AS latestAssessedMachineState ON
    latestAssessedMachineState.[machineId] = machine.[Id] AND
    latestAssessedMachineState.[Id] = machine.[LastAssessedMachineStateId]
INNER JOIN
    [Reporting3].[WindowsDetectedPatchState] AS detectedPatchState ON
    detectedPatchState.[AssessedMachineStateId] = latestAssessedMachineState.[Id]
INNER JOIN
    [Reporting3].[WindowsInstallState] AS installState ON
    installState.[Id] = detectedPatchState.[InstallStateId]
INNER JOIN
    [Reporting3].[WindowsPatch] AS patch ON
    patch.[Id] = detectedPatchState.[PatchId]
INNER JOIN
    [Reporting3].[WindowsPatchAppliesTo] AS patchAppliesTo ON
    patchAppliesTo.[PatchId] = patch.[Id]
INNER JOIN
    [Reporting3].[Cve] AS cve ON
    cve.[Id] = patchAppliesTo.[CveId]
WHERE
    /* Id 4 indicates a missing patch */
    installState.[Id] = 4
GROUP BY
    cve.[Name],
    cve.[Id],
    patch.[Bulletin],
    patch.[QNumber];
```

362. Sample Query: Missing Patches by Agent Policy

Select all missing patches for the last scan of machines associated to an agent policy. The following data is displayed:

- Assigned Policy Name
- Machine Name
- Bulletin Id
- QNumber
- Product Name
- Service Pack
- Patch Install State

Query

SQL

```sql
SELECT
    agent.[AssignedPolicyName] AS [Assigned Policy Name],
    machine.[Name] AS [Machine Name],
    machine.[Domain] AS Domain,
    patch.[Bulletin] AS [Bulletin Id],
    patch.[QNumber] AS QNumber,
    product.[Name] AS [Product Name],
    product.[ProductLevelName] AS [Product Level],
    installState.[Value] AS [Patch Install State],
    product.[id] AS ProductId,
    detectedPatchState.[ProductId] AS [detectedPatchState ProductID]
FROM
    [Reporting3].[Agent] AS agent
INNER JOIN
    [Reporting3].[Machine] AS machine ON
    machine.[Id] = agent.[MachineId]
INNER JOIN
    [Reporting3].[AssessedMachineState] AS assessedMachineState ON
    assessedMachineState.[Id] = machine.[LastAssessedMachineStateId]
INNER JOIN
    [Reporting3].[WindowsDetectedPatchState] AS detectedPatchState ON
    detectedPatchState.[AssessedMachineStateId] = assessedMachineState.[Id]
INNER JOIN
    [Reporting3].[WindowsPatch] AS patch ON
    patch.[Id] = detectedPatchState.[PatchId]
INNER JOIN
    [Reporting3].[WindowsProduct] AS product ON
    product.[Id] = detectedPatchState.[ProductId]
INNER JOIN
    [Reporting3].[WindowsInstallState] AS installState ON
    installState.[Id] = detectedPatchState.[InstallStateId]
WHERE
    /* Id 4 indicates a missing patch */
    installState.[Id] = 4
ORDER BY
    agent.[AssignedPolicyName],
    machine.[Name],
    machine.[Domain],
    patch.[Bulletin]
```

363. Sample Query: Patch Status Detail

This sample query gets a list of installed and missing patches from the latest scan for each machine.

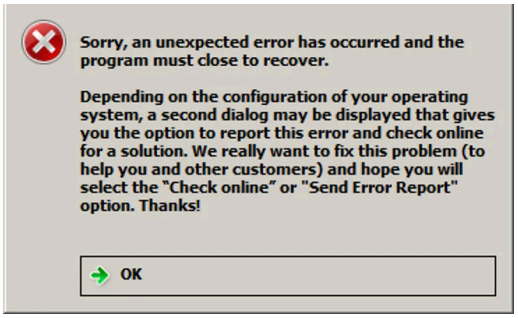
Query

SQL

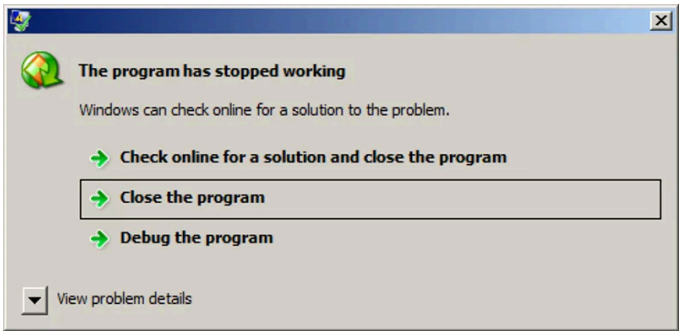
```
SELECT DISTINCT
    patch.[QNumber] AS [QNumber],
    patch.[Bulletin] AS [Bulletin Id],
    patch.[ReleasedOn] AS [Released On],
    product.[Name] AS [Product Name],
    product.[ProductLevelName] AS [Product Level Name],
    installState.[Value] AS [Install state],
    patchScan.[StartedOn] AS [ScanDate],
    machine.[Name] AS [Machine Name],
    machine.[Domain] AS Domain,
    locale.[name] AS [Language Name],
    machine.[LastKnownIP] AS [IP Address],
    machine.[LastPatchAssessedOn] AS [Scan Date],
    detectedPatchState.[InstalledOn] AS [Installed On]
FROM
    [Reporting3].[PatchScan] AS patchScan
INNER JOIN
    [Reporting3].[AssessedMachineState] AS assessedMachineState ON
    assessedMachineState.[PatchScanId] = patchScan.[Id]
INNER JOIN
    [Reporting3].[Machine] AS machine ON
    machine.[LastAssessedMachineStateId] = assessedMachineState.[id]
INNER JOIN
    [Reporting3].[WindowsDetectedPatchState] AS detectedPatchState ON
    detectedPatchState.[AssessedMachineStateId] =  assessedMachineState.[Id]
INNER JOIN
    [Reporting3].[WindowsPatch] AS patch ON
    detectedPatchState.[PatchId] = patch.[Id]
INNER JOIN
    [Reporting3].[WindowsInstallState] AS installState ON
    installState.[Id] = detectedPatchState.[InstallStateId]
INNER JOIN
    [Reporting3].[WindowsProduct] AS product ON
    product.[Id] = detectedPatchState.[ProductId]
LEFT OUTER JOIN
    [sys].[syslanguages] AS locale ON
    machine.[Language] = locale.[lcid] /* machine.[Language] is used to index into [sys].[syslanguages] */
WHERE
    (
    detectedPatchState.[InstallStateId] = 3 OR  /* Installed Patch */
    detectedPatchState.[InstallStateId] = 4     /* Missing Patch */
    )
ORDER BY
    patch.[Bulletin],
    patch.[QNumber],
machine.[Name]
```

364. Reporting Errors and Checking for Possible Solutions

If an error occurs that requires the program to close in order to recover, an error dialog will be displayed.



If your operating system is configured to allow the capture and reporting of errors, after you click **OK** a second dialog will be displayed. This dialog gives you a couple of error reporting options.



Check Online for a Solution

This dialog gives you the option to send information about the error to Ivanti and to receive a possible solution to the problem. Ivanti recommends selecting the **Check online for a solution and close the program** option. This option will:

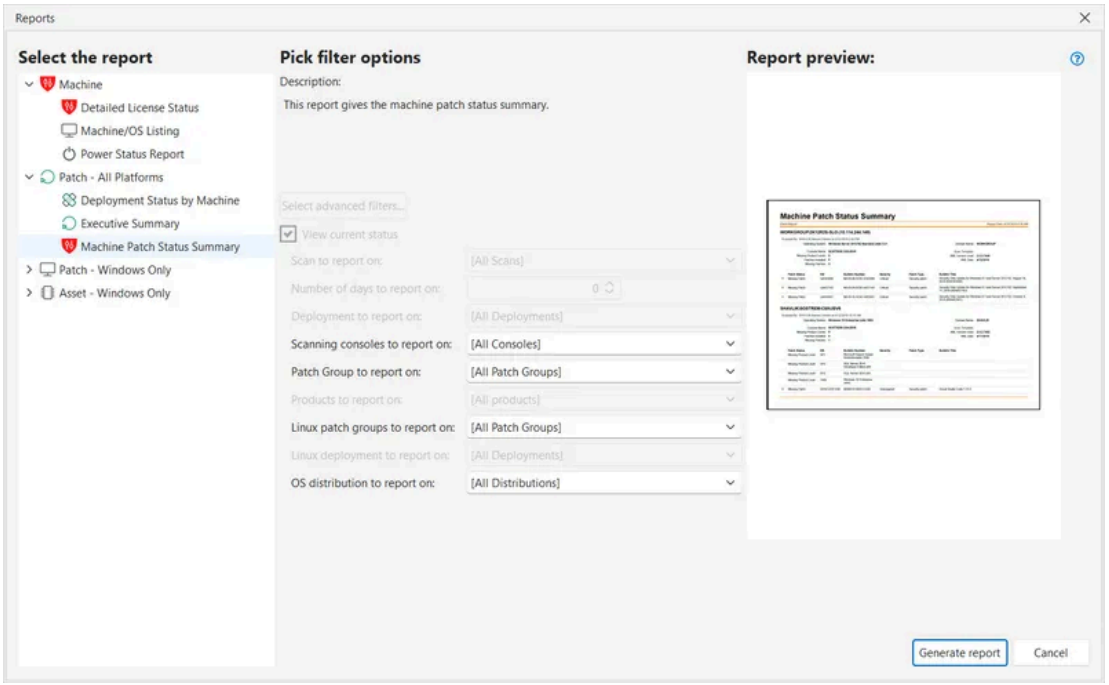
- Send information about the problem to Ivanti so the problem can be researched and fixed.
- Query an online database for a possible solution to the problem. If a solution exists it will be displayed on the console machine in a separate dialog.

Privacy and Security Concerns

Only information pertaining to the specific problem will be sent to Ivanti; no personal, machine, or network information is collected or sent. The information is sent anonymously and the process will not impact your network.

365. Reports Dialog

The **Reports** dialog is designed to provide you with an assortment of different report filtering options. You can open the **Reports** dialog using the **Tools > Create report** menu. The **Reports** dialog consists of a single dialog in which you make all of your selections.



Select a Report

Use the **Select the report** list to select which report you want to generate. When you select a report, the description of that report is displayed and a sample of the report is shown on the right side of the dialog.

Pick Filtering Options

Security Controls's reporting utility includes powerful filtering options. Depending on the report you choose, you have choices between basic and/or **advanced** filtering options.

Basic Filtering Options

- If you want the report to contain information from the most recent scan of each machine managed by the console (and of each machine managed by the associated remote consoles, if this is a **data rollup** console), enable the **View current status** check box. Not all reports allow the use of this check box. Enabling this check box will make the **Scan to report on** option unavailable.
- The basic filtering options allow you to choose which deployments, which scanning databases, which patch groups, and what products would you like to report on.
- Once you have made your selections, click **Generate report** to see the results.

Advanced Filtering Options

If you need even more granularity or different sorting options, click the **Select advanced filters** button. The advanced filter options are presented in the **Advanced Report Filters** dialog. The report will be generated after you specify your advanced filtering options.

Scheduling a Report

If you want to schedule a report to run at some time in the future, select **Tools > Schedule report**. A scheduled report can be generated once or on a recurring basis. See **How to Schedule a Report** for more information.

Generating a Report from a Data Rollup Console

If a console is a data rollup console, in addition to containing information about each machine it manages, it will also contain information about all the machines managed by the associated remote consoles. The information sent by the remote consoles and collected by the data rollup console is stored in an *aggregate database*. When you generate reports from the rollup console you automatically have access to all the information contained in the aggregate database.

366. Requirements and Exceptions

This section identifies the requirements you must meet if you choose to use your own CA to generate a new authority certificate.

> You cannot use a server SSL certificate (such as a wild card certificate) as your sub-authority certificate.

Requirements of the New Sub-Authority Certificate

When issuing the certificate

- Must have a basic constraints extension
- The extension indicates that the certificate is able to issue other certificates. You may choose to specify that the path length is 0 (meaning that certificate cannot be used to create an issuing certificate). For more information, see **RFC 5280**.
  Must have KeyCertSign and CrlSign key usage extensions
- Must use DER ASN.1
- A separate certificate must be issued for each console server - you cannot issue a single certificate for multiple console servers

When installing the certificate on the console machine

- Must have an associated private key
- Must be located in the computer account's Intermediate Certification Authorities certificate store

Exceptions

When you configure your environment to work with a third-party CA, the console will no longer automatically update an **expiring root certificate**. Security Controls will provide a warning when the certificate is nearing its expiration date, but it will be up to the local administrator to manually create the new certificate using their own CA.

367. Requirements for Using the Migration Tool

In order to use the Migration Tool you must meet the following requirements:

- During the migration, the version and build number of Security Controls that is on your target console must be the same as the version and build number that is on your existing console.
- For example, you can migrate from version 9.4.34268 to 9.4.34268 but not from 9.4.34105 to 9.4.34268. You can upgrade to a newer version after you migrate to a new machine.
  The Microsoft SQL Server version used by the new console must be equal to or later than the current version.
- For example, you can move from SQL Server 2014 to SQL Server 2016 but you cannot move from SQL Server 2016 to SQL Server 2014.
  The target machine must be using a **supported operating system**.
- You must have 20 GB or more free disk space to hold the backup archive files.
- The backup archive file can be written to either the local hard drive or to a network drive.
  The Migration Tool requires a certain amount of temporary disk space during the backup process. If the hard drive on your existing console is nearly full, you may need to change the location of your System Temp folder. For information on how to do this, see the **community site**.

Related Topics

- **Commonly Asked Questions**
- **Before You Begin**
- **Creating Your Backup Files**
- **Restoring Your Console on a New Machine**
- **Post-Migration Tasks**

368. Machine Restart Implementation Notes

There are two methods you can use to restart the connected machines in your organization and leave them in a fully powered on state.

- You can use the right-click **Power > Restart now shortcut command** from within Machine View or Scan View. With this method:
  - The console machine is not affected
  - The selected machines will be restarted immediately
  - No warning will be issued to active users of those machines

You can use a **power state template** to schedule a reboot. With this method:

  - The console machine is eligible for a restart
  - You can schedule the reboot to happen immediately or at some point in the future
  - A warning will issued to all active users of those machines

The Restart command works with the following target machine states:

Initial Power State of Target Machine	Target Machine Left in Fully Powered On State?
Fully powered on	Yes
Sleep state	No action
Hibernate state	No action
Powered off	No action

369. Restoring Your Console on a New Machine

The restore process is as follows:

1. Restore your core components on the new console and begin running verification tests.
2. Restore all remaining user accounts on the new console.

Restoring Core Components

Important! The restore process will overwrite any data that exists on the new Security Controls console machine.

1. Log on to the new console machine using the same user account that was used to create the core backup file.
2. Install Security Controls on your new machine.
   The version of Security Controls that you install must be equal to the version on your old console machine. You do not need to activate your license on the new console or perform any configuration steps; this will be done when you perform the restore.
3. Close Security Controls.
4. (Conditional) If your organization uses a proxy server, make sure the proxy configuration is correct on the new console machine before you restore the core components.
5. (Optional) Move the core backup file from your old console machine to your new console machine.
   This is done to improve speed, performance and stability during the restoration process. The backup file can, however, reside on an accessible location on your network.
6. Start the Migration Tool on the new console machine by selecting **Start > Ivanti** Security Controls **> Migration Tool**.
7. Restore the core components.
   1. Select **Restore**.
   2. Select **Core**.
   3. Specify the core backup file.
   4. Click **Restore core settings**.
   5. Watch the progress messages and wait for the completion message to appear.
   6. Check the **Restore Results** file for any error messages.

Start Security Controls.
An informational dialog may appear that reminds you to add the fully qualified name of the new machine to the console alias list. See the Verification Checklist section for more details.

9. On the old console, stop the Security Controls Console Service.

Restoring User Account Data

You cannot restore user data until after you have completed the core migration.

1. Log on to the new console machine using the same user account that was used to create the user backup file.
2. (Optional) Move the user backup file from your old console machine to your new console machine.
   This is done to improve speed, performance and stability during the restoration process. The backup file can, however, reside on an accessible location on your network.

3. Start the Migration Tool on the new console machine.
4. Select **Restore**.
5. Select **User**.
6. Specify a user backup file.
7. Click **Restore user settings**.
8. Watch the progress messages and wait for the completion message to appear.
9. Repeat this process for all Security Controls administrator accounts.

Related Topics

- Requirements for Using the Migration Tool
- Commonly Asked Questions
- Before You Begin
- Creating Your Backup Files
- Post-Migration Tasks

370. Roadmap of Tasks for Virtual Machines and Virtual Machine Templates

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Patch Tasks

Security Controls can scan and deploy patches to online virtual machines, to offline virtual machines, and to virtual machine templates. You do this by performing the following tasks:

1. Create one or more machine groups that contain the virtual machines and virtual machine templates you want to scan and patch. See **How to Add Virtual Machines**.
2. Supply credentials for the virtual machines.
   When performing scans, the recommended best practice is to always supply credentials for the virtual machines and virtual machine templates. When performing patch deployments, credentials must be set at the machine, group, or default level. See **Supplying Credentials** for more details.
3. Use the machine group in a scan. See **How to Initiate a Patch Scan** for details.
4. Review the scan results. See **Accessing Patch Scan Results** for details.
   In the scan results, unique icons will distinguish an offline virtual machine ( ) from a physical machine or an online virtual machine ( ) and from a **virtual machine template** ( ). When viewing machines in **Machine View** the **Offline Scan** column in the top pane will indicate if a virtual machine was online or offline at the time of the scan.
5. (Optional) If you want to take snapshots of your hosted virtual machines and templates immediately before and/or immediately after the deployment process, make sure you specify this on the **Hosted VMs/Templates tab** of the deployment template you

plan to use.

6. **Deploy the desired patches** to the desired virtual machines and virtual machine templates. See **Deploying Patches to Virtual Machines** for details.
   You may not know if a particular virtual machine is online or offline at the time you perform a deployment, and it typically doesn't matter. The following guidelines apply for patch deployments to virtual machines:
   - If a virtual machine is **hosted on a server**, the deployment can be successful regardless of whether the virtual machine is online or offline at the time of the deployment.
   - If a virtual machine is defined in a machine group using the **Workstation Virtual Machines tab**, the deployment can be successful as long as the virtual machine is offline.
   - If a virtual machine is defined in a machine group using the **Machine Name**, **Domain Name**, or **IP Address/Range** tab, the deployment can be successful as long as the virtual machine is online.

If a virtual machine is online the patch deployment is performed in the same manner as for a physical machine. Patch deployments to offline virtual machines and to virtual machine templates are performed by Security Controls in a slightly different manner. See **Deploying Patches to Virtual Machines** for details.
Monitor the deployment activities. See **Monitoring the Deployment** for details.

Asset Management Tasks

Security Controls can perform asset management scans of online virtual machines, of offline virtual machines, and of virtual machine templates. You do this by performing the following tasks:

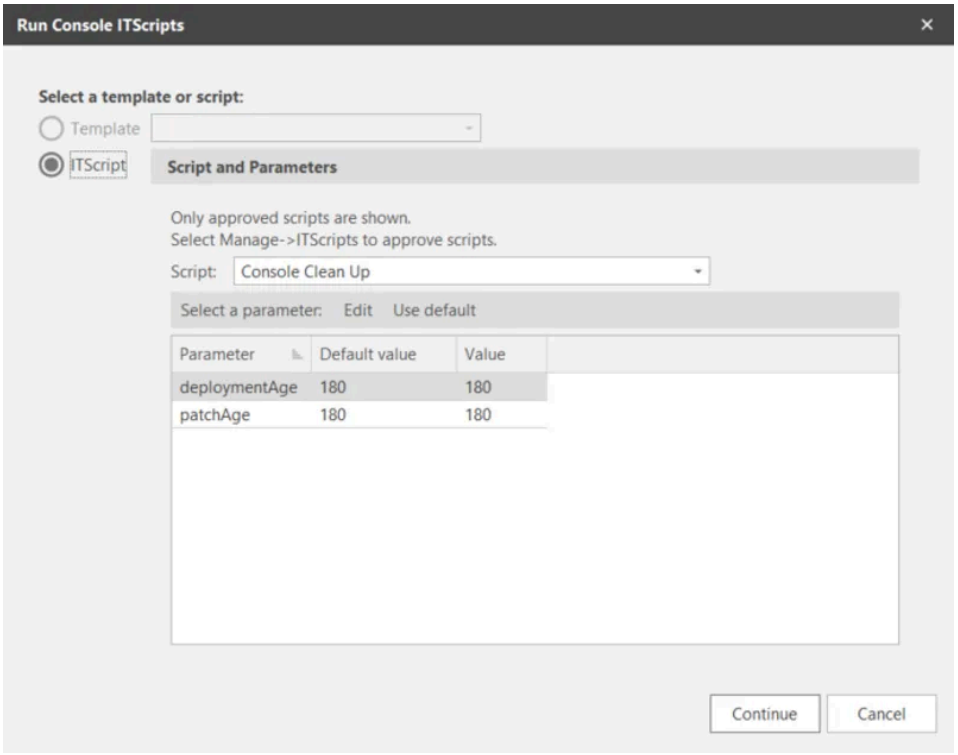
1. Create one or more machine groups that contain the virtual machines and templates you want to scan.
   See **How to Add Virtual Machines**.
2. Supply credentials for the virtual machines and virtual machine templates.
   See **Supplying Credentials** for details.
3. Use the machine group in an asset scan. See **How to Perform Asset Scans** for details.
4. Review the asset scan results. See **Viewing Asset Scan Results** for details.
   When viewing machines in **Machine View** the Offline Scan column in the top pane will indicate if a virtual machine was online or offline at the time of the scan.

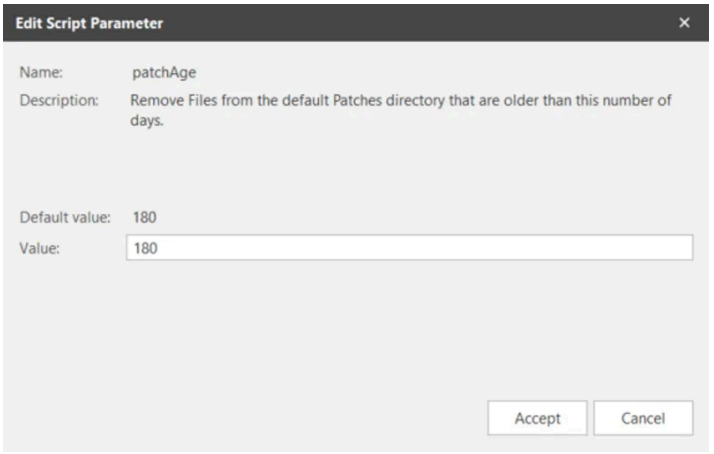
Power Management Tasks

You can use Security Controls to power on and off the virtual machines that reside on your **ESXi hosts**. For more information, see **Performing Actions on Virtual Machines**.

371. Using the Run console ITScripts Dialog

The **Run console ITScripts** dialog enables you to select and run those scripts that are designed to run only on the console machine (and not against target machines). You access this dialog by selecting **Tools > Run console ITScripts**.



Field	Description
Template	If you choose to run a console-only script using a template you will execute the script using predefined parameter values.
Script	If you choose to run a script directly without a template you have the ability to modify the values of the input parameters associated with the script. All approved console-only scripts contained in the **Script Catalog Manager** are available for selection. The Script Catalog Manager will also provide detailed information about each script.
Parameters	Displays the input parameters used by the script and the parameter values that will be used by the template. To modify a parameter value, double-click the parameter or select the parameter and click **Edit**. The **Edit Script Parameter** dialog is displayed. 

To execute the selected script, click **Continue**. To close the dialog without initiating a script, click **Cancel**.

372. Sample Query: CVE Vulnerability Report

The SecurityControls views provide access to data that is in the Ivanti Security Controls database but that is not available in the predefined reports. This section provides sample queries that illustrate how to reference a SecurityControls view.

Query

This is a CVE vulnerability report that will display the CVE name and how many machines are affected due to a missing patch on the latest patch scan.

SQL

```sql
SELECT
    cve.[Name] AS [CVE Name],
    cve.[Id] AS [CVE ID],
    patch.[Bulletin] AS [Bulletin Id],
    patch.[QNumber] AS QNumber,
COUNT( DISTINCT machine.[Id]) AS [Machines Missing Count]
FROM
    [Reporting2].[Machine] AS machine
INNER JOIN
    [Reporting2].[AssessedMachineState] AS latestAssessedMachineState ON
    latestAssessedMachineState.[machineId] = machine.[Id] AND
    latestAssessedMachineState.[Id] = machine.[LastAssessedMachineStateId]
INNER JOIN
    [Reporting2].[DetectedPatchState] AS detectedPatchState ON
    detectedPatchState.[AssessedMachineStateId] = latestAssessedMachineState.[Id]
INNER JOIN
    [Reporting2].[InstallState] AS installState ON
    installState.[Id] = detectedPatchState.[InstallStateId]
INNER JOIN
    [Reporting2].[Patch] AS patch ON
    patch.[Id] = detectedPatchState.[PatchId]
INNER JOIN
    [Reporting2].[PatchAppliesTo] AS patchAppliesTo ON
    patchAppliesTo.[PatchId] = patch.[Id]
INNER JOIN
    [Reporting2].[Cve] AS cve ON
    cve.[Id] = patchAppliesTo.[CveId]
WHERE
    /* Id 4 indicates a missing patch */
    installState.[Id] = 4
GROUP BY
    cve.[Name],
    cve.[Id],
    patch.[Bulletin],
    patch.[QNumber];
```

373. Sample Query: Missing Patches by Agent Policy

Select all missing patches for the last scan of machines associated to an agent policy. The following data is displayed:

- Assigned Policy Name
- Machine Name
- Bulletin Id
- QNumber
- Product Name
- Service Pack
- Patch Install State

SQL

```
SELECT
    agent.[AssignedPolicyName] AS [Assigned Policy Name],
    machine.[Name] AS [Machine Name],
    machine.[Domain] AS Domain,
    patch.[Bulletin] AS [Bulletin Id],
    patch.[QNumber] AS QNumber,
    product.[Name] AS [Product Name],
    product.[ProductLevelName] AS [Product Level],
    installState.[Value] AS [Patch Install State],
    product.[id] AS ProductId,
    detectedPatchState.[ProductId] AS [detectedPatchState ProductID]
FROM
    [Reporting2].[Agent] AS agent
INNER JOIN
    [Reporting2].[Machine] AS machine ON
    machine.[Id] = agent.[MachineId]
INNER JOIN
    [Reporting2].[AssessedMachineState] AS assessedMachineState ON
    assessedMachineState.[Id] = machine.[LastAssessedMachineStateId]
INNER JOIN
    [Reporting2].[DetectedPatchState] AS detectedPatchState ON
    detectedPatchState.[AssessedMachineStateId] = assessedMachineState.[Id]
INNER JOIN
    [Reporting2].[Patch] AS patch ON
    patch.[Id] = detectedPatchState.[PatchId]
INNER JOIN
    [Reporting2].[Product] AS product ON
    product.[Id] = detectedPatchState.[ProductId]
INNER JOIN
    [Reporting2].[InstallState] AS installState ON
    installState.[Id] = detectedPatchState.[InstallStateId]
WHERE
    /* Id 4 indicates a missing patch */
    installState.[Id] = 4
ORDER BY
    agent.[AssignedPolicyName],
    machine.[Name],
    machine.[Domain],
    patch.[Bulletin]
```

374. Sample Query: Patch Status Detail

This sample query gets a list of installed and missing patches from the latest scan for each machine.

SQL

```
SELECT DISTINCT
    patch.[QNumber] AS [QNumber],
    patch.[Bulletin] AS [Bulletin Id],
    patch.[ReleasedOn] AS [Released On],
    product.[Name] AS [Product Name],
    product.[ProductLevelName] AS [Product Level Name],
    installState.[Value] AS [Install state],
    patchScan.[StartedOn] AS [ScanDate],
    machine.[Name] AS [Machine Name],
    machine.[Domain] AS Domain,
    locale.[name] AS [Language Name],
    machine.[LastKnownIP] AS [IP Address],
    machine.[LastPatchAssessedOn] AS [Scan Date],
    detectedPatchState.[InstalledOn] AS [Installed On]
FROM
    [Reporting2].[PatchScan] AS patchScan
INNER JOIN
    [Reporting2].[AssessedMachineState] AS assessedMachineState ON
    assessedMachineState.[PatchScanId] = patchScan.[Id]
INNER JOIN
    [Reporting2].[Machine] AS machine ON
    machine.[LastAssessedMachineStateId] = assessedMachineState.[id]
INNER JOIN
    [Reporting2].[DetectedPatchState] AS detectedPatchState ON
    detectedPatchState.[AssessedMachineStateId] =  assessedMachineState.[Id]
INNER JOIN
    [Reporting2].[Patch] AS patch ON
    detectedPatchState.[PatchId] = patch.[Id]
INNER JOIN
    [Reporting2].[InstallState] AS installState ON
    installState.[Id] = detectedPatchState.[InstallStateId]
INNER JOIN
    [Reporting2].[Product] AS product ON
    product.[Id] = detectedPatchState.[ProductId]
LEFT OUTER JOIN
    [sys].[syslanguages] AS locale ON
    machine.[Language] = locale.[lcid] /* machine.[Language] is used to index into [sys].[syslanguages] */
WHERE
    (
    detectedPatchState.[InstallStateId] = 3 OR  /* Installed Patch */
    detectedPatchState.[InstallStateId] = 4     /* Missing Patch */
    )
ORDER BY
    patch.[Bulletin],
    patch.[QNumber],
    machine.[Name]
```

375. Saving and Validating Your Changes

Anytime you create a new custom XML file or make changes to an existing custom XML file, you should save your changes and then perform a validation. The validation ensures that the custom XML is properly formed and will interact correctly with Security Controls's primary patch XML file.

You should always save the custom XML file before performing the validation. If you don't save the file the validation will be performed on the previously saved version of the file.

To validate a custom XML file:

1. Save the file by selecting **File > Save**.
2. In the left-hand pane select the topmost folder.
   This folder specifies the location of the custom XML file.
3. In the right-hand pane click **Validate XML**.
   The results are displayed in the **Validation Results** section at the bottom of the right-hand pane. If an error is detected you must correct that error before attempting to use the custom XML file.

376. Scanning Engine Overview

The Security Controls scan engine performs security patch assessment against a variety of Windows-based operating systems and products from Microsoft and other product vendors.

The Security Controls engine uses a data definition file that contains information about which security hotfixes are available for each product. The data file contains security bulletin name and title, and detailed data about product-specific security hotfixes, including:

- Files in each hotfix package and their file versions
- Registry changes that were applied by the hotfix installation package
- Information about which patches replace which other patches
- Related Microsoft Knowledge Base article numbers
- Cross references to the Common Vulnerabilities and Exposures (CVE) database hosted by **cve.org** (formerly cve.mitre.org) (CVEID)

The data definition file, which is contained **on the console** in a secured file named `WindowsPatchData.zip`, is created and hosted by Ivanti.

When you run Security Controls (without specifying advanced file input options), the program must download a copy of this XML file so that it can identify the hotfixes that are available for each product. The XML file is a digitally signed CAB file and is available on the Ivanti website. Security Controls downloads the CAB file, verifies its digital signature, and then extracts the XML file to your local computer. Note that a CAB file is a compressed archive that is similar to a ZIP file.

After the data file is extracted, Security Controls scans your machine (or the selected machines) to determine the operating system, product levels, and programs that you are running. Security Controls then identifies security patches that are available for your combination of installed software. Patches that are applicable to your machine but are not currently installed are displayed as **Missing Patch** in the resulting output. In the default configuration, Security Controls output displays only those patches that are necessary to bring your machine up to date. Security Controls recognizes roll-up packages and does not display those patches that are **replaced by later patches**.

377. Patch Scanning Prerequisites

The following criteria must be met to ensure a successful **patch scan**:

When scanning your local (console) machine

- You must be an administrator on your local machine.
- Credentials must be provided for the local machine. See **Supplying Credentials** for details.
- The machine must be capable of obtaining the data definition file, either from a location on the Internet (via http or https) or from another specified location (either on the local machine or from a specified network location).
- The local machine's Workstation service must be started.

> The Server service is not required to be started on the local machine.

When scanning a remote machine, you must meet all the requirements for the local scan above, plus the following:

- You must have local administrative rights on the remote machine and be able to logon to this machine from the workstation performing the scan.
- Credentials must be provided for the target machines. See **Supplying Credentials** for details.
- The credentials you supply must have access to the control panel on the target machine. If control panel access is disabled through group policy, Security Controls will be unable to connect to the target machine.
- File and Print Sharing must be enabled.
- The NetBIOS (tcp139) or Direct Host (tcp445) ports must be accessible on the remote machine.
- The remote machine must be running the Server service.

> The Workstation service is not required to be started on the remote machine.

The remote machine must be running the Remote Registry service.

> The remote registry service is disabled by default on Windows machines. You must enable the remote registry service (either manually or via group policy) before performing remote scans of Windows machines.

The %systemroot% share (usually C$ or similar) must be accessible on the remote machine. For information about how to create a temporary system drive share if none exists, see **Scan Options**.

- All drives where applications are installed must be accessible on the remote machine.
- For machines using Windows operating systems that use User Account Control, you must either:
  - Join the machines to a domain and then perform the scan using domain administrator credentials, or
  - If you are not using the built-in Administrator account on the remote machines (and using that account is NOT recommended), you must disable User Account Control (UAC) remote restrictions on the machines. To do this:

1. Click **Start**, click **Run**, type **regedit**, and then press **Enter**.

2. Locate and then click the following registry subkey:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. If the **LocalAccountTokenFilterPolicy** registry entry does not exist, follow these steps:
   1. a. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
   2. b. Type **LocalAccountTokenFilterPolicy** and then press **Enter**.

Right-click **LocalAccountTokenFilterPolicy** and then click **OK**.

5. In the **Value data** box, type **1**, and then click **OK**.
6. Exit Registry Editor.
   For more details on disabling UAC remote restrictions, see **Microsoft Learn (opens in a new window)**.

378. ScanType view

The Reporting2.ScanType view defines source types.

Column Name	Data Type	Nullable	Description
Id	smallint		The scan type id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.ScanType view.

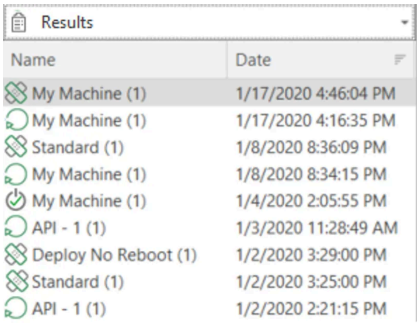
Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[ScanType]
```

ID	Value	Description
0	Unknown	Invalid or Unknown type.
1	Patch	The scan was a Windows patch scan.
2	Deprecated	Deprecated value.
3	Asset	The scan was an asset scan.
4	PowerStatus	The scan was a power status scan.
5	Deprecated	Deprecated value.
6	WakeOnLan	Not a scan; reserved value.
7	PowerOptions	Power State Template or ad hoc power action.
8	PowerShell	The scan was a PowerShell scan.
9	Nix	The scan was a Linux scan.

379. Scan History

Even after a series of scans, all of the results of prior scans are just a click away. The scans are recorded in the **Results** list in the navigation bar.



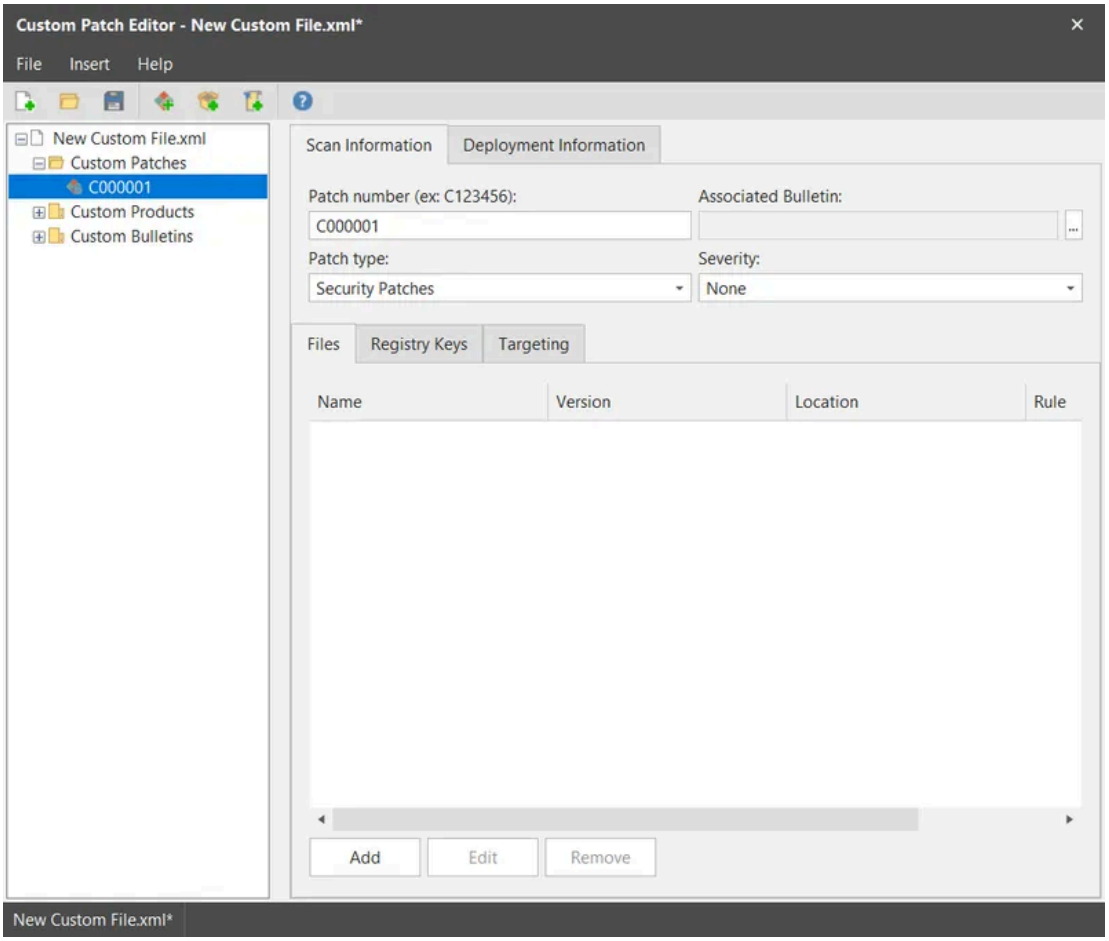
Additionally, you can get a complete list of available prior scans by selecting **Manage > Database** from the main menu.

380. Scan Information Tab

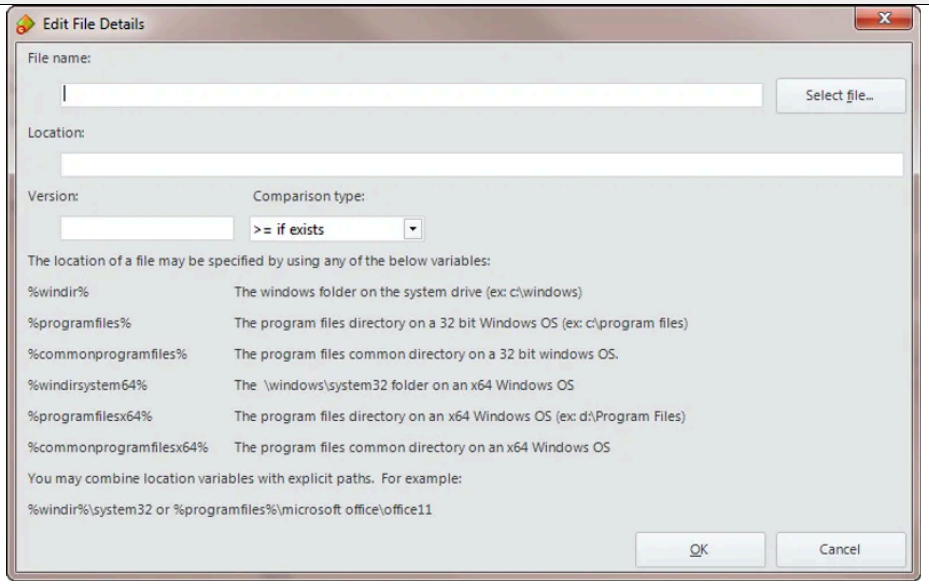
When creating a custom patch, two major tabs are used in the right-hand pane. This topic describes the options and sub-tabs contained on the **Scan Information** tab.

This tab contains two sub-tabs that enable you to specify criteria for determining whether or not a patch is installed. You must use your own discretion in determining whether to specify detection criteria on the **Files** tab, the **Registry Keys** tab, or both. If your requirements are that a specific file version and a specific registry key value must both be detected in order to declare that the patch is installed, then by all means do it. The recommendation, however, is to keep things as simple as possible. If detecting an old file version is criteria enough to determine that a patch is required, you probably don't need to also specify registry key information (and vice versa).

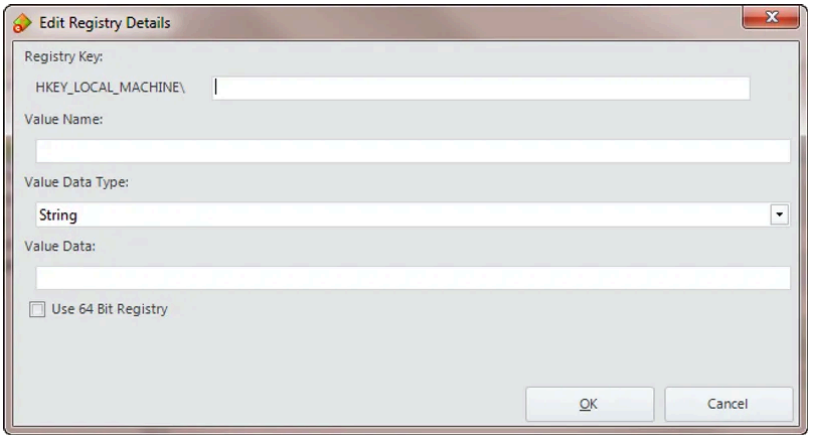
> If you do not specify registry key information, patches that were not installed by Security Controls will be reported as *Effectively Installed*. In order for Security Controls to display a patch as Effectively Installed you must use a scan template that scans for both missing and installed patches. See **Creating a New Patch Scan Template** for more information.



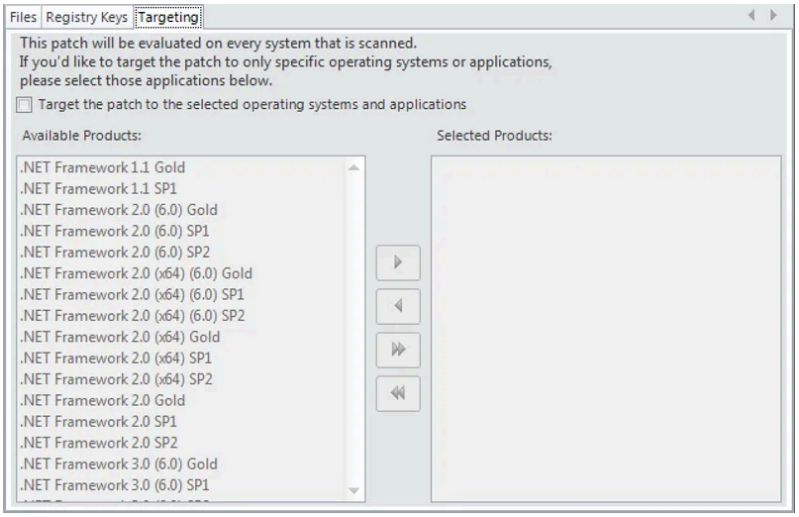
Field	Description
Patch Number	An identifying number for this patch. You can follow whatever numbering convention you want when defining the patch number. The only rule is that the number must be no more than 10 alphanumeric characters. Although it is not mandatory for the number to be unique, in almost all cases it makes sense to make it unique. Only in extremely rare cases is it advisable to assign the same patch number to two or more patches. The patch number specified here will be the number shown within the Security Controls interface when referring to the patch. It is also the identifier used by such things as patch groups when specifying which patches belong to a certain group. As a point of reference, the patch number is akin to the knowledge base number (or QNumber) used to identify patches in the Microsoft world. By default the first patch in the custom XML file is C000001. This number is automatically incremented for each new patch.
Associated Bulletin	You must associate each patch with an existing bulletin. The bulletin can be one that you created or one that was issued by another vendor. To see the list of all available bulletins, click the **Browse** button (...). In the dialog that appears, select the desired bulletin and then click **OK**.
Patch Type	Specify the types of patch you are creating. • **Security Patches:** Security bulletin related patches. This is the default setting. • **Non-security Patches:** The set of patches supported by Microsoft Software Update Services (driver updates not supported). • **Security Tools:** Patches for the malware tool provided by Microsoft. • **Software Distribution:** Free third-party applications that can be deployed by Security Controls. • **Custom Actions:** Enables you to perform custom actions even if you are already fully patched. It does this by scanning for a specific QNumber and patch (QSK2745, MSST-001) that will always be found. This null patch can be remediated but no patch will be deployed. The process uses the temporary file Nullpatch.exe.
Severity	Assign one of the following four severity levels based on the perceived threat of the vulnerability related to the patch. • **Critical:** The problem or issue associated with the patch is deemed critical in nature. • **Important:** The problem or issue associated with the patch is deemed important to fix. • **Moderate:** The problem or issue associated with the patch is of moderate severity. • **Low:** While the problem or issue is real, the security risk or capability is deemed to be low.
Files tab	One of the ways to determine if a patch should be installed is to check the version number of the affected file on the machines being scanned. The **Files** tab is used to specify the file version information. If you also specify criteria on the **Registry Keys** tab, the tests on that tab must also be satisfied in order for the patch to be installed. • **Add:** To add a new file definition, click this button. • **Remove:** To remove an existing file definition, click this button. • **Edit:** To edit an existing file definition, click this button. After clicking **Add** or **Edit**, the **Edit File Details** dialog is displayed.

Field	Description
	 • **Filename:** The name of the portable executable format file affected by the patch. For most instances the file will therefore be either an .exe or a .dll file. The file must contain version information for this check to be correct. • **Select File:** Use this button to browse the local computer or network for the file affected by the patch. When you use this button to find the file, the program will use information about the file you select to also populate the Location and Version boxes. For this reason you will typically use this button when defining the Filename box. • **Location:** Specify the location of the affected .exe or .dll file. You must provide the full directory path when specifying the location. If this box was automatically populated by the Select File button, you may need to edit the path if the location represents the position of the file on the local machine and is not representative of where it will be located on all other machines. • **Version:** Specify the version number of the affected .exe or .dll file. • **Comparison Type:** This specifies the test criteria you want to use when determining if a scanned machine needs this patch. The two available options have very similar names so be careful when making your selection. ◦ **If the file exists, its file version must be equal to or greater than the specified version:** The only way to fail this test is if the file exists on the scanned machined but its version number is less than the number specified in the Version box. If the file does not exist on the scanned machine then the patch does not apply. ◦ **The file must exist and its file version must be equal to or greater than the specified version:** There are two ways to fail this test. (1) If the file does not exist on the scanned machine then the test fails and the patch is required. (2) If the file does exist but its version number is less than the number specified in the Version box then the test fails and the patch is required. **File Location Parameters:** Shows the parameters that can be used when specifying a file location. Rather than specifying one hard coded location that may not apply to every machine in your organization, you can use parameters to specify variable locations. For example, if you want to specify the Windows folder but the folder may be located at C:\Windows, D:\Windows, or C:\WinNT on the different machines in your organization, you can accommodate all options by using the %windir% parameter. You can use a parameter within a location path and you can use multiple parameters within a path.
Registry	Another way to determine if a patch should be installed is to check for the data defined on certain registry keys on the machines being scanned. The **Registry Keys** tab is used to specify the registry information. If the scanned machine

Field	Description

Keys tab	satisfies the criteria specified here then the patch will be applied.
	If you also specify criteria on the **Files** tab, the tests on that tab must also be satisfied in order for the patch to be installed.
	• **Add:** To add new registry key information, click this button.
	• **Remove:** To remove existing registry key information, click this button.
	• **Edit:** To edit existing registry key information, click this button.
	
	After clicking **Add** or **Edit**, the **Edit Registry Details** dialog is displayed.
	
	To get the most current registry information we recommend using the Microsoft Registry Editor (regedit), a tool for viewing settings in your system registry. You can copy the required information from this tool to the appropriate fields in the **Edit Registry Details** dialog.
	• **Registry Key:** You can only specify keys that are relative to the HKEY_LOCAL_MACHINE hive. The easiest and most accurate way to populate this box is to display the desired key from within the Microsoft Registry Editor, copy the key name and then paste the name into this box. The HKEY_LOCAL_MACHINE portion of the name will likely be repeated so you'll need to remove that portion of the name from the box.
	• **Value Name:** The name of the specific registry key.
	• **Value Data Type:**
	  ◦ **String:** Specifies that the data must be a string.
	  ◦ **DWord:** Specifies that the data must be a number.
	
	Value Data: The expected value of the registry key. You can find this value by locating the key within the Microsoft Registry Editor and then looking in the Data column.
	• **Use 64 Bit Registry:** Enable this check box if the registry key is in the 64-bit part of the registry of a 64-bit architecture.

Targeting tab	This tab enables you to specify which products apply to this patch. By default all available operating systems will be evaluated. You can greatly speed the evaluation process if you can narrow the list of products. Targeting the patch to a limited number of products can be a real time saver during the scan process as it eliminates the scanning of unnecessary products. **Said Another Way:** If you do not specify any products in the **Selected Products** list, the patch will be associated with all available operating systems. The program will scan for the patch regardless of what is installed on the target machines. This can be useful if you want to perform a mass distribution of the patch, but it can also be quite time consuming. If you

Field	Description
	specify one or more products in the **Selected Products** list, the patch will be associated with only those products and not with any unspecified operating systems. TIP: After **importing a new custom XML file**, you can use Patch View to verify the custom patch is associated with the correct product(s).  To narrow the list of products: 1. Enable the **Target the patch to the selected operating systems and applications** check box. 2. In the **Available Products** list, select the desired product and move it to the **Selected Products** list. The **Available Products** list contains all products currently defined in the XML patch data file plus any new custom products you may have defined using the **Custom Patch File Editor**. 3. Repeat Step 2 for each product that applies to this patch.

When complete, save and then validate the XML file (see **Saving and Validating Your Changes**).

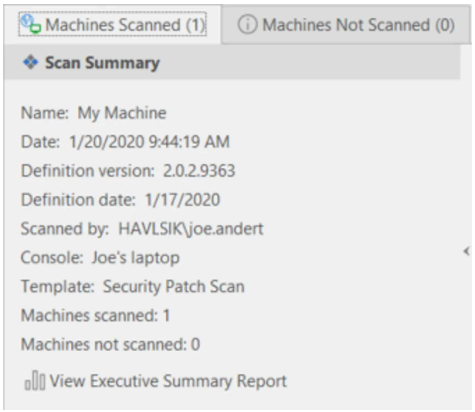
381. Patch Options Menu

Additional scanning options can be set using the **Tools > Options** menu. See **Patch Options** for details.

382. Scan View Scan Summary

Scan View is accessible immediately following a successful scan or by selecting a previous scan from the **Results** list in the navigation pane.

The left side of the top pane contains a Scan Summary sub-pane. This pane provides summary information about the scan. The pane can be collapsed to provide more room in the top pane.



The top pane in the scan summary also displays a table containing detailed information about each machine that was scanned. Click on a column heading to sort the table by that information. You can also specify what information is presented by right-clicking the table heading and selecting or clearing the available items.



Field	Description
, , , or	Indicates whether the computer is a physical or online virtual Windows machine ( ), a Linux machine ( ), an offline virtual machine ( ), or a virtual machine template ( ).
Last Scanned Group	The **machine group** the machine belonged to **at the time of the most recent scan**. Because a machine can change machine groups or be in multiple machine groups, the name is dynamic.
Assigned Group	The group to which this machine is assigned within Scan View and Machine View. An assigned group is not the same as a machine group. An assigned group is only used within Scan View and **Machine View**. This column is used for organizational purposes within Scan View and Machine View. For example, machines that share similar attributes such as physical location or the same agent policy might be assigned to the same group. The group assignment is preserved regardless of whether the **Last Scanned Group** value changes. For this reason, the **Assigned Group** column is often used within Scan View to sort, filter and search for specific assigned groups and then **perform actions** on the machines in those groups. This column is particularly useful with machines such as **Cloud agents**, as they do not belong to a machine group and will not be automatically assigned to a group. Machines can be assigned to a group a number of different ways. • The default group is the machine group name and it will be applied during agentless operations such as patch scans, asset scans and power status scans, or a push installation of an agent from a machine group. • You can manually assign machines to a group using the **Machine Properties** dialogs. For information on how to manually assign machines to a group, see **Managing Individual Machine Properties** and **Managing Multiple Machine Properties**. • Agent machines can be assigned to a group during deployments initiated from the **REST API**. • Agent machines can be assigned to a group if the agent activation key is **created from the console machine** or from the **cloudsync function in the REST API**. The assigned group information becomes a part of the agent key and is automatically included when you specify the ACTIVATIONKEY in an agent **manual installation script** or some other deployment tool.
Domain	The domain of the scanned machine.
Machine Name	The machine name.
IP Address	The IP address of the scanned machine.
Virtual Server	The name of the server that is hosting the virtual machine. This column does not apply to physical machines.
VM Name	The name of the virtual machine. This column does not apply to physical machines.
VM Inventory Path	The full path name of the hosted virtual machine. This column does not apply to physical machines.
Health	A visual representation of the percentage of installed patches (**green**) vs. missing patches (**red**).

Field	Description
Installed Patch Count	The total number of patches installed on the scanned machine.
Missing Patch Count	The total number of patches missing on the scanned machine.
Missing Product Level Count	The total number of product levels missing on the scanned machine.
EOL Products	The number of software products on the machine that have been designated as at End-of-Life by their vendor.
Operating System With Product Level	The operating system and product level level being used on the scanned machine. If the operating system is shown in **red** it indicates that it has reached its end-of-life (EOL) phase and the vendor will limit support for the product.
Operating System Language	The operating system language being used on the scanned machine.
Assigned credential name	The **credentials** used when authenticating Security Controls to the machine.
Last Scan Template	The template that was most recently used to scan the machine.
Machine Criticality	The **criticality level** assigned to this machine.
Custom	Any **custom notes** that describe unique properties about the machine.

383. Scheduled Snapshot Maintenance

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



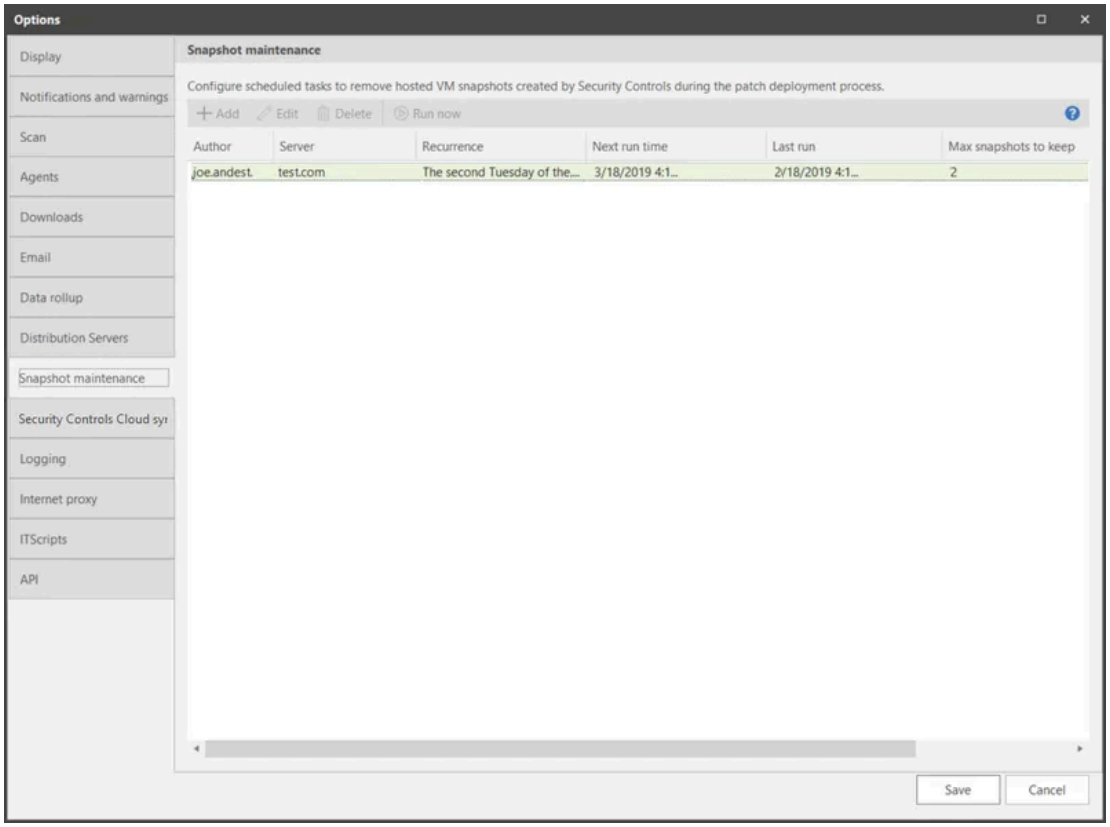
Overview Information

> This option allows you to schedule the removal of old virtual machine snapshots. If you want to remove old snapshots in real-time (as new snapshots are created during the patch deployment process), see **Deployment Template: Hosted VMs/Templates Tab**.

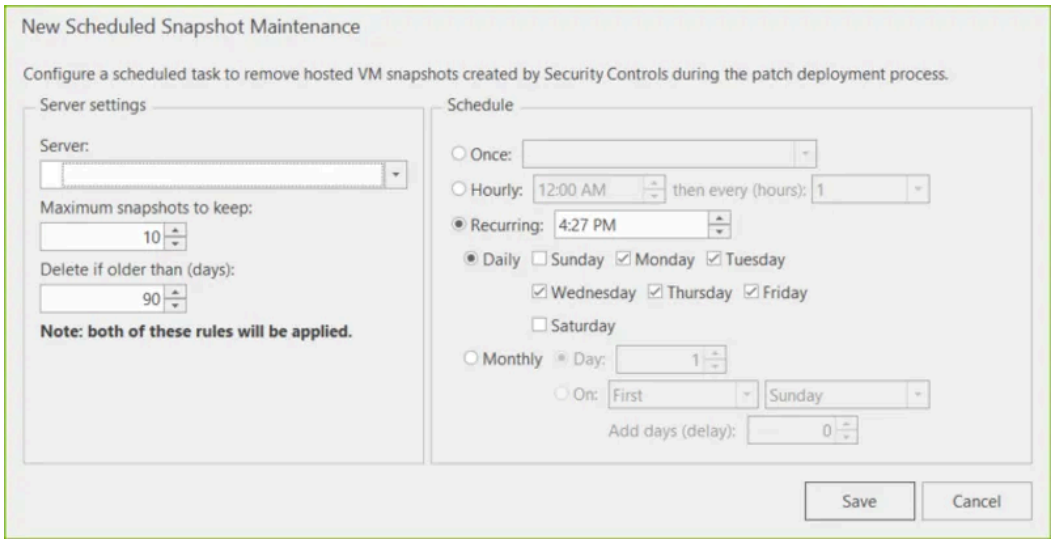
The **Snapshot Maintenance** dialog applies only if you have virtual machines in your network that are **hosted on one or more VMware servers**. It allows you to configure a one-time or recurring task that will remove old virtual machine snapshots from the server. The snapshots that exist were created on the server during patch deployments to the server's hosted virtual machines.

Any currently defined snapshot maintenance tasks are displayed in a list on the dialog. You can perform the following actions:

- **Add:** Adds a new snapshot maintenance task
- **Edit:** Edits the selected snapshot maintenance task
- **Delete:** Deletes the selected maintenance task
- **Run now:** Causes the selected maintenance task to be run right now



When you click **Add** or **Edit**, the **Scheduled Snapshot Maintenance** dialog is displayed. This dialog is used to configure the snapshot maintenance task.



Field	Description
Server	Choose the **VMware server** from which you want to remove virtual machine snapshots.
Maximum snapshots to keep	Indicates the maximum number of snapshots created by Security Controls that will be allowed to remain on the server. If the threshold is exceeded, the oldest snapshots are deleted until the number of snapshots no longer exceeds the limit.
Delete if older than (days)	Indicates the number of days a snapshot created by Security Controls will be allowed to exist. Snapshots older than the specified number of days are automatically deleted. The threshold is checked each time this maintenance task is run.
Schedule	There are three scheduling options: • **Once** indicates that the operation will be run once at the specified day and time. • **Hourly** indicates that the operation will be run multiple times a day. The operation will be run at the start time and then again every X hours. • **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly snapshot maintenance task to occur four days after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by four days.

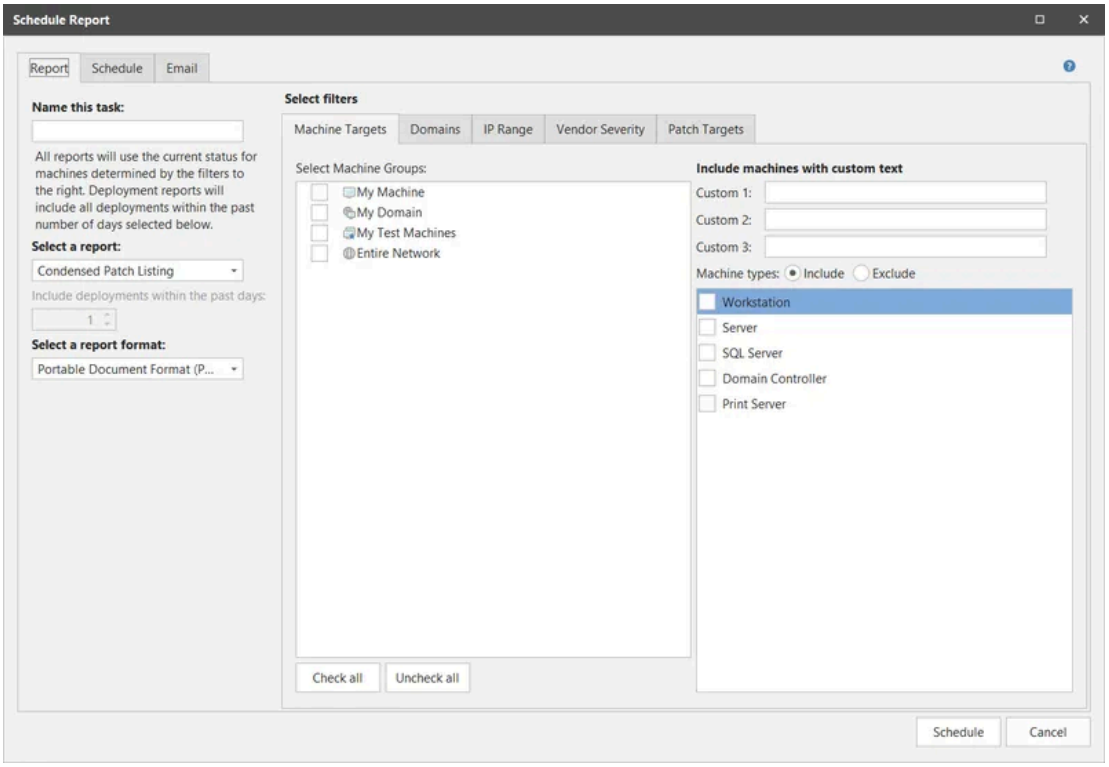
384. How to Schedule a Report

The **Schedule Report** dialog enables you to automatically generate a report at some time in the future. The report can be automatically generated once or on a recurring basis. The report content will be based on the last known status of the machines (as determined by the latest scan).

The generated reports can be found here: `C:\ProgramData\Ivanti\Security Controls\Console\TempReports`. In addition, the reports can also be sent as an email attachment to one or more recipients.

How to Access the Scheduling Dialog

To schedule a report select **Tools > Schedule report**. The **Schedule Report** dialog is displayed.



Report Tab

This tab enables you to specify which report you want to generate and what file format to use when saving the report. This tab also provides several powerful filtering options that enable you to specify the exact information you want to include in the report. The filtering options that are available will vary depending on the report you choose. If you do not specify any filtering options, the report will contain information on all of the machines detected in the latest scan.

Field	Description
Name this task	The name that you wish to assign to the task that will generate the scheduled report.
Select a report	Select the report that you want to generate. The filters that are available in the right pane will change depending on which report you select.
Select a report format	The report will be generated in the format you choose.
Machine Targets tab	Use this tab to specify which machines you want to include in the report. You can specify filtering criteria in any or all of the available areas. • **Select Machine Groups:** You can select one or more existing machine groups. • **Include machines with custom text:** If you have provided **custom notes** about the properties of your machines, use this filter to specify which of those machines are included in the report. All machines not containing the specified custom text will be excluded from the report. • **Machine types:** You can include or exclude specific machine types. **Example:** If you select **Entire Network** in the **Select Machine Groups** area and **Server** in the **Machine types area**, only the server machines in your network will be included in the report. **Example:** If you select **Entire Network**, specify **St. Paul** in the **Custom 2** box, and **Server** in the **Machine types** area, only the server machines located in the city of St. Paul will be included in the report.
Domains tab	Select the domains that you want to include or exclude from the report. Only those domains that have been detected by previous scans are available for selection.
IP Range tab	Specify the starting and ending IP addresses of the target machines you want to include or exclude from the report.
Vendor Severity tab	Specify the vendor severity level(s) of the patches that you want to include or exclude from the report. The **vendor severity** is assigned to each patch by Ivanti based on the perceived threat of the vulnerability related to the patch.
Patch Targets tab	Select the patch groups that you want to include or exclude. Only those **patch groups** that you have previously defined are available for selection. In addition, you can specify the patch status(es) that you want to include or exclude. The patch status is the current status of a patch on a target machine. You can specify a patch status without specifying a patch group (and vice versa).

Schedule Tab

Use this tab to specify when you want the report to be generated. The report must be scheduled at least five minutes in the future.

Field	Description
Once	If you only want to generate the report once at some date and time in the future, choose this option. Click in the box to select the date that you want to generate the report. The time will automatically default to the current time. Click in the box to manually change the time to the desired value.
Recurring	If you want to generate the report on a recurring basis, choose this option. Use the day and time boxes to specify when the report should be generated. The **Add delay (days)** box (available if you generate a report on a monthly basis) allows you to delay the generation of the report by up to 31 days. For example, you might use this to schedule a monthly report that is always generated four days after Patch Tuesday. You do this by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by four days.

Email Tab

Use this tab to specify who will receive the report as an attachment in an email message.

> You must configure the SMTP server in order to send an email message. See **Email Operations** for details on configuring the server.

Field	Description
Email subject	Specify what should appear in the subject line of the email message.
Select recipients	Select the groups and/or individuals you want to receive the report. You can define new groups or contacts if needed.

Scheduling the Report

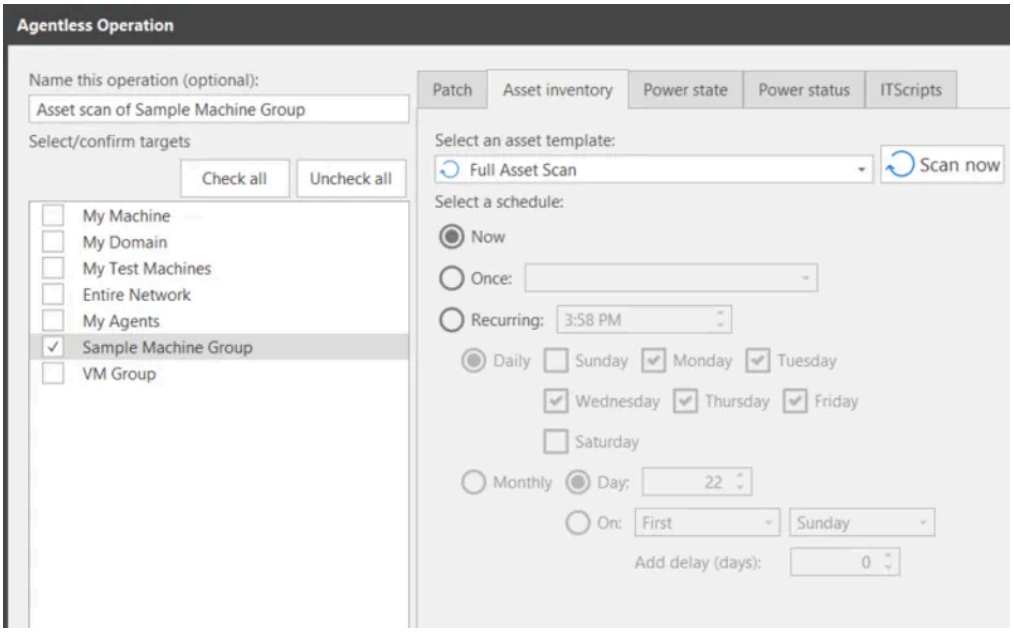
Once you have made your selections, click **Schedule** to schedule the report. You can view the scheduled report task by selecting **Manage > Scheduled Console Tasks** and then selecting the **Reports** tab.

If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks dialog** to view and modify which credential is being used as the scheduler credential.

385. Scheduling Asset Scans

When you initiate an asset operation from a machine group or from a Favorite the **Agentless Operation** dialog is displayed. This dialog enables you to specify if the operation should run now or be scheduled for a future time or date.

> Make sure you assign credentials for all machines involved in the scheduled scan.



Field	Description
Name this operation (optional)	Enables you to provide a unique name for the operation. By default the name of the machine group or favorite used to initiate the operation will be used. The name is displayed in the **Results pane**.
Select/confirm targets	This list is a reminder of the machine group(s) that will be affected by the operation. If the wrong group is listed, click**Cancel**and re-initiate the operation using the correct group.
Select an asset template	Enables you to select the asset scan template you want to use when performing the operation.
Select schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Scan now** or **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected. • **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly asset scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day.

When the desired options are selected, click **Scan now** or **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

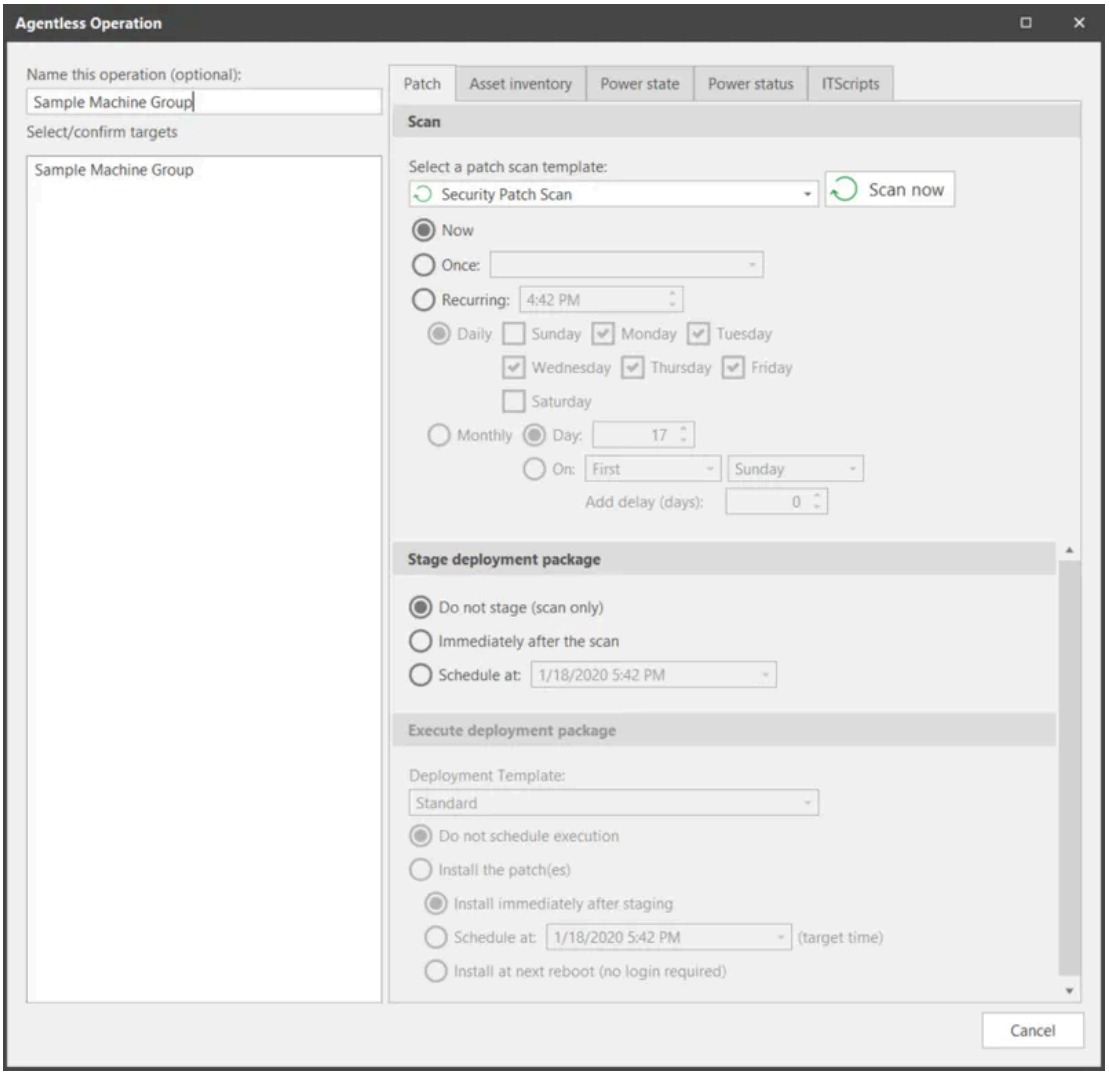
- **Scan now/Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The scan operation is **scheduled on the console machine**. See **Monitoring an Asset Scan** for details.
  If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks dialog** to view and modify which credential is being used as the scheduler credential.

> The scheduled credentials are only used to schedule the operation on the console machine. The scheduled credentials are (typically) different from the **machine-level credentials** that are used to perform the actual operations on the target machines.

386. Scheduling Patch Scans

When you initiate a patch operation from a machine group, from a favorite, or from Machine View, the **Agentless Operation** dialog is displayed. This dialog enables you to specify if the operation should run now or be scheduled for a future time or date. You can also specify if you want to automatically stage and deploy any missing patches detected by the scan.

> Make sure you assign credentials for all machines involved in the scheduled scan.



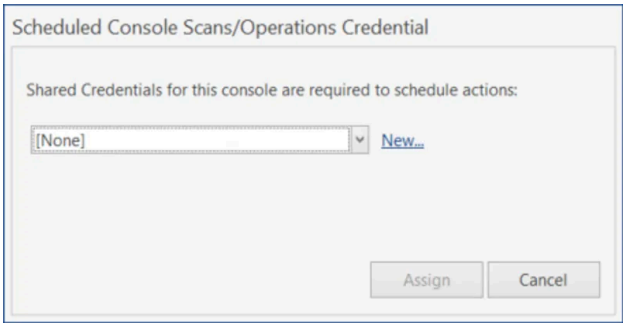
Action	Description
1. Name this operation	Enables you to provide a unique name for the operation. By default the name of the machine group or favorite used to initiate the operation will be used. The name is displayed in several locations: **Scheduled Task Manager**, **Operations Monitor**, the **Results pane** and the Scan View **scan summary.**
2. Select/confirm targets	This list is a reminder of the machine group(s) that will be affected by the operation. If the wrong group is listed, click **Cancel** and re-initiate the operation using the correct group.
Select a patch scan template	Select the template you want to use when performing the patch scan (Security Patch Scan, All Patches, or a custom patch scan template).
Select schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Scan now** or **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected. • **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, every Saturday at 9 PM, every weekday at 11 PM, or at any other user-selected time and interval. In addition to monthly and daily intervals, a **minute-based interval** may also be available. You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly patch scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day.
Stage deployment package	This area enables you to choose if you want to automatically stage a deployment package following the scan. • If you only want to perform a scan, choose **Do not stage (scan only)**. • If you want to automatically stage a deployment package for any patches that are detected as missing by the scan, choose either **Immediately after the scan** or **Schedule at**. The staging process includes creating the deployment package and copying the package to the target machine. For information on automatically staging and executing patch deployments, see **Automatically Deploying Patches**.
Execute deployment package	This area enables you to specify if and when a deployment package should be executed on a target machine. This area is not available if **Do not stage (scan only)** is selected. For more information, see **Automatically Deploying Patches**.

When the desired options are selected, click **Scan now** or **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

- **Scan now/Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The scan operation is **scheduled on the console machine**. See **Monitoring a Scheduled Patch Scan** for details.
  If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You

must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks dialog** to view and modify which credential is being used as the scheduler credential.

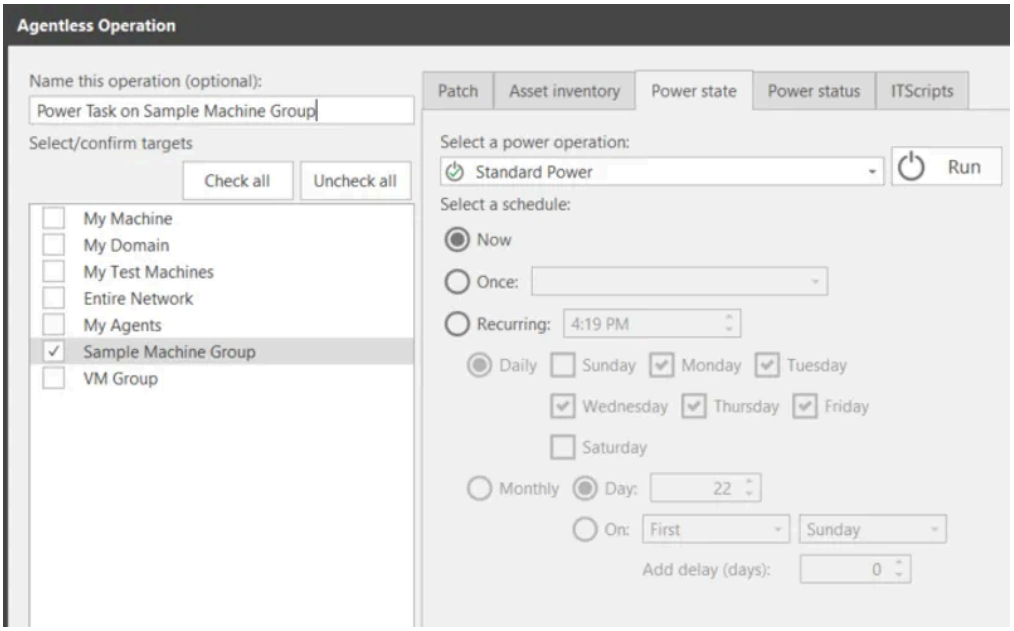
> The scheduled credentials are only used to schedule the operation on the console machine. The scheduled credentials are (typically) different from the **machine-level credentials** that are used to perform the actual operations on the target machines.



387. Scheduling Power Tasks

When you initiate a task from a machine group or from a Favorite, or when you initiate a Wake-on-LAN request, the **Agentless Operation** dialog is displayed. You can use the dialog to schedule the power task immediately or at some point in the future.

> Make sure the proper credentials are available for all machines involved in the scheduled task.



Field	Description
Name this operation (optional)	Enables you to provide a unique name for the operation. By default the name of the machine group or favorite used to initiate the operation will be used. The name is displayed in the **Results pane**.
Select/confirm targets	This list is a reminder of the machine group(s) that will be affected by the operation. If the wrong group is listed, click **Cancel** and re-initiate the operation using the correct group.
Select a power operation	Enables you to select the power state template you want to use when performing the operation.
Select a schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Scan now** or **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected. • **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule a power status scan in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a monthly power status scan to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day. The **Add delay (days)** option is not available for other power state operations.

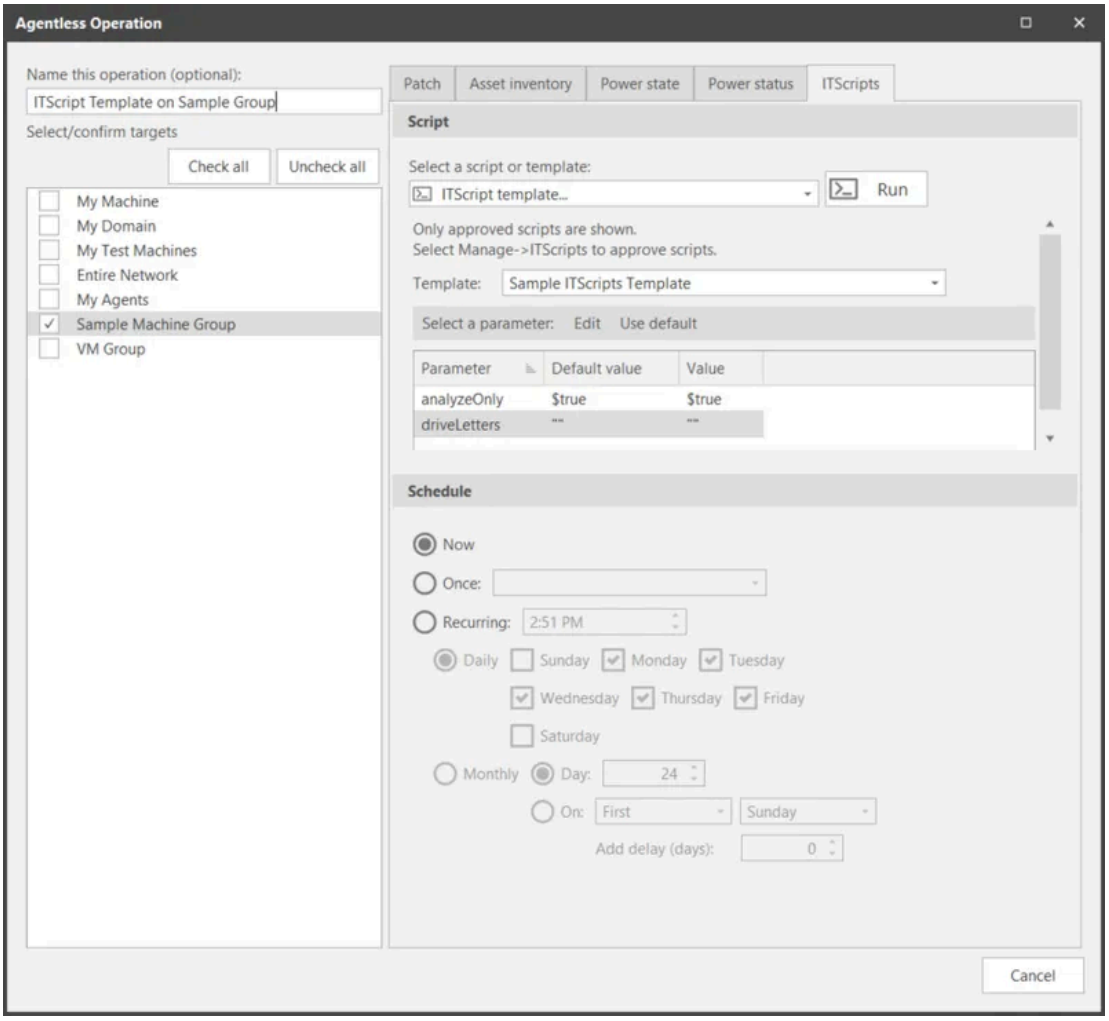
When the desired options are selected, click **Scan now** or **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

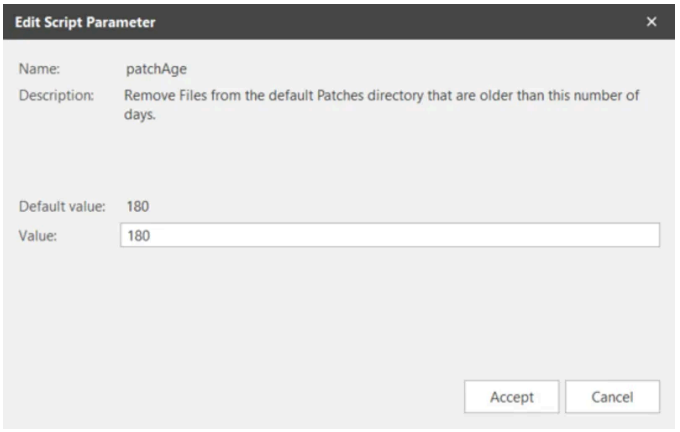
- **Scan now/Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The operation is **scheduled on the target machine**.

388. Scheduling a Script

When you initiate a script operation the **Agentless Operation** dialog is displayed. This dialog enables you to specify if the operation should run now or be scheduled for a future time or date.

> Make sure you assign credentials for all machines involved in the operation.



Field	Description
Name this operation (optional)	Enables you to provide a unique name for the operation. By default, the name of the machine group used to initiate the operation and the current date/time will be used. The name is displayed in the **Results pane**.
Select/confirm targets	This list is a reminder of the machines and machine groups that will be affected by the operation. If the wrong machines or groups are listed, click**Cancel**and re-initiate the operation using the correct targets.
Select a script or template	Enables you to select the ITScript or ITScript template you want to use when performing the operation. • If you choose to run a script using a template you will execute the script using predefined parameter values. The template also defines the maximum number of machines the script may run on simultaneously (concurrency). • If you choose to run the script directly without a template you have the ability to modify the values of any input parameters associated with the script. All **approved scripts** of type **Any or ESXi Hypervisor** are available for selection. The Script Catalog Manager will also provide detailed information about each script. • To run a script of type **Console** see **Using the Run console ITScripts dialog**. Any input parameters used by the script will be displayed. To modify a parameter value, double-click the parameter or select the parameter and click **Edit**. The **Edit Script Parameter** dialog is displayed. String values must be contained within quotes (for example, "*"); numeric values do not require quotes. 
Schedule	There are three scheduling options: • **Now** runs the operation as soon as the **Run** button is clicked. • **Once** indicates that the operation will be run once at the day and time selected. • **Recurring** allows an administrator to regularly schedule operations at a specific time and using a specified recurrence pattern. For example, using this option, an operation could be run every night at midnight, or every Saturday at 9 PM, every weekday at 11 PM, or at any other user selected time and interval. You can also use the **Recurring** option to schedule an operation in conjunction with a regular monthly event such as Microsoft's Patch Tuesday. For example, you might schedule a script operation to occur the day after Patch Tuesday by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by one day.

When the desired options are selected, click **Run** (if **Now** is selected) or **Schedule** (if **Once** or **Recurring** is selected).

- **Run:** The operation is initiated immediately and the **Operations Monitor** is displayed.
- **Schedule:** The operation is **scheduled on the console machine**. See **Monitoring a Scheduled Script** for details.
  If scheduled credentials are not currently assigned the **Scheduled Console Scans/Operations Credential** dialog is displayed. You must assign a shared credential to perform a schedule action. You can use the **Set scheduler credential** button on the **Scheduled Console Tasks dialog** to view and modify which credential is being used as the scheduler credential.

> The scheduled credentials are only used to schedule the operation on the console machine. The scheduled credentials are (typically) different from the **machine-level credentials** that are used to perform the actual operations on the target machines.

389. Script Metadata

In order for a script to be used in Security Controls, it must contain metadata that uniquely identifies the script and describes its functionality and input parameters. This section will describe how to create that metadata.

Let's start with a simple one-line script that has one input parameter:

Bash

```
Get-Service $serviceName -ComputerName "$ST_ComputerName"
```

The complete script with the metadata that is required by Security Controls is shown below. Some of the information is optional, and each element will be described in detail later.

Bash

```
<#
<stScript uid="d0d3c64c-19a3-4879-9396-ac8769d60c9c">
<name>GetServices</name>
<version>1.0.0.0</version>
<author>My Company</author>
<scriptType type="any" />
<minEngineVersion>8.0.0.0</minEngineVersion>
<modifiesTarget>false</modifiesTarget>
<options>
<option name="OutputMachineResults" value="true" />
<option name="OutputRunResults" value="true" />
<option name="CombineOutputFiles" value="false" />
<option name="DeleteMachineFiles" value="false" />
</options>
<concurrency default="16" />
<description>
<category>Information</category>
<purpose>Get the services on the target machine</purpose>
<inputs>Wildcard of service name</inputs>
<outputs>List of installed services</outputs>
</description>
<parameters>
<parameter>
<name>serviceName</name>
<description> Wildcard service(s) to query </description>
<default>”*”</default>
</parameter>
</parameters>
</stScript>
#>
Get-Service $serviceName -ComputerName "$ST_ComputerName"
```

Metadata Block

The metadata is an XML fragment inside a script comment.

The script comment delimiters are “<#” and “#>. For our purposes, these delimiters must be on lines by themselves and begin in column 1.

The root element of the XML document is “stScript”. It has one attribute, the unique identifier of the script. This is a globally unique identifier (GUID). A GUID is specified by 32 hex characters in the format “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. There are many standard tools for generating GUIDs.

The beginning and ending elements must be on lines by themselves, beginning in column 1. Therefore, all script used in Security Controls should begin with these two lines (substituting a different GUID for each script):

```Bash
<#
<stScript uid="d0d3c64c-19a3-4879-9396-ac8769d60c9c">
```

and end with these two lines:

```Bash
</stScript>
#>
```

The other elements should appear in the order described below.

name

This required element provides the name of the script as it will appear within Security Controls. The name must be between 1 and 100 characters. The name may contain spaces and special characters.

Example:

```Bash
<name>GetServices</name>
```

version

This required element specifies the version of the script. The version is specified as four integer numbers separated by periods. When you modify a script, the newer version must have a version which is greater than any previous versions you have used.

Example:

```Bash
<version>1.0.0.0</version>
```

author

This required element identifies the author of the script. It is customary to use either the author's name or the name of the company. This field must be between 1 and 256 characters and must not be blank.

Example:

```Bash
<author>My Company</author>
```

scriptType

This optional element specifies the type of script execution. It has a required attribute, "type", which must contain one of the following:

- **type="any"** indicates that the script runs against one or more target machines, but does not require PowerShell remoting. This is the most common script type and is the default if the scriptType element is not specified.
- **type="consoleOnly"** indicates that the script does not run against a set of target machines. This type of script cannot be run against machine groups or selected machines. Such a script will appear in the available scripts only when your select Tools > Run console ITScripts from the Security Controls menu.
- **type="remote"** indicates that the script runs against one or more target machines and requires PowerShell remoting to be available and configured on the target machines.
- **type="esxServer"** indicates that the script runs against an ESXi Server or a vCenter Server. Scripts of this type run only against machine groups that contain ESXi Servers. If the machine group contains any other machines, they will be ignored when this script executes.

Example:

```Bash
<scriptType type="any" />
```

minEngineVersion

This optional element specifies the minimum ITScripts engine version required to execute this script. If not specified, the script should be written to run with any version of the ITScripts engine.

Example:

```Bash
<minEngineVersion>8.0.0.0</minEngineVersion>
```

modifiedTarget

This optional element indicates whether the script makes any modifications to the target machines. If not specified, it defaults to "false", suggesting that the script only gathers information but does not modify the target machines. This is for documentation only. Its value does not guarantee that the script does not modify the target machines.

Example:

```Bash
<modifiesTarget>false</modifiesTarget>
```

options

This optional element and its four sub-elements tell the ITScripts engine which standard output files should be generated. By default, the engine will generate these standard output files:

- **runoutput.txt:** One file for the entire run if any run output is generated
- **runerror.txt:** One file for the entire run if errors were detected
- **machineoutput.txt:** One file for each target machine if any machine output is generated
- **machineerror.txt:** One file for each target machine if errors were detected

If you specify the following in the metadata, the runoutput.txt and runerror.txt files will not be generated:

```Bash
<option name="OutputRunResults" value="false" />
```

If you specify the following in the metadata, the machineoutput.txt and machineerror.txt files will not be generated:

```Bash
<option name="OutputMachineResults" value="true" />
```

If you'd like all the machineoutput.txt files for all machines to be concatenated into the runoutput.txt file, and all the machineerror.txt files concatenated into runerror.txt, then specify this option:

```Bash
<option name="CombineOutputFiles" value="true" />
```

If you choose to combine the individual machine output and error files, then you can choose to delete the individual files by specifying the following:

```Bash
<option name="DeleteMachineFiles" value="true" />
```

Example:

Bash

```
<options>
<option name="OutputMachineResults" value="true" />
<option name="OutputRunResults" value="true" />
<option name="CombineOutputFiles" value="false" />
<option name="DeleteMachineFiles" value="false" />
</options>
```

concurrency

This optional element specifies the default maximum concurrency level to use when a script is executed against a set of target machines. You can override this in Security Controls by creating an ITScripts template and specifying a different concurrency value. If not specified, the default maximum concurrency is set to 32.

Example:

Bash

```
<concurrency default="16" />
```

description

The “description” element and its four sub-elements are all required. The information entered here will be displayed within Security Controls.

category

The required “category” element is a child of the description element. The category helps in organizing your scripts. The category must be between 1 and 50 characters. Standard categories might include: “Configuration”, “Group Policy”, “Information”, “Maintenance”, “Monitoring”, and “Support”.

purpose

The required “purpose” element is a child of the description element. It must contain between 1 and 1024 characters. It should contain a concise and accurate description of what the script is used for.

inputs

The required “inputs” element is a child of the description element. It must contain between 1 and 1024 characters. This should accurately describe the input parameters required by the script. If there are no input parameters, simply specify “None”.

outputs

The required “outputs” element is a child of the description element. It must contain between 1 and 1024 characters. This should accurately describe the output generated by the script.

Example:

```
Bash
```

```
<description>
<category>Information</category>
<purpose>Get the services on the target machine</purpose>
<inputs>Wildcard of service name</inputs>
<outputs>List of installed services</outputs>
</description>
```

parameters

The “parameters” element must be specified if the script requires any input parameters. There must be one “parameter” child element for each input parameter. Each “parameter” element must have three child elements:

- **name:** The input parameter name with no leading ‘$’. The name must be the valid PowerShell variable name used in the script.
- **description:** This description will appear in Security Controls.
- **default:** This element specifies the default parameter value that will be used for the parameter unless the user specifies an alternate value in a template or when starting or scheduling the script execution. If the default is a string, enclose it in apostrophes or quotes. Apostrophes allow the string to contain characters that have special meaning in PowerShell, such as the $ and quote. To embed such characters within quotes, precede them with the tic character (`).

Example:

```
Bash
```

```
<parameters>
<parameter>
<name>serviceName</name>
<description>Wildcard service(s)to find</description>
<default>”*”</default>
</parameter>
</parameters>
```

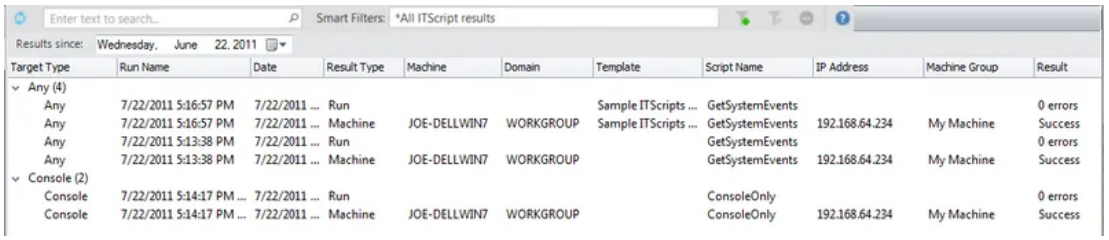
390. ITScripts Results View

ITScript Results View provides a way to view the results of all scripts that have been run from Security Controls. It displays all results that have ever been reported to the console, providing a complete historical record for your organization.

When a script is executed on one or more target machines the results are automatically reported to the console. ITScript Results View is accessed from the main menu by selecting **View > ITScript results**.

You can adjust the amount of information that is displayed by using the **Results since** option, the **Smart Filter**, or the **Search** option. By default, all script results that have been reported to the console within the last 30 days will be displayed.

> ITScript Results View will be empty if you view it immediately after installing the program or if no script results have been reported to the console. This is because there is no script information in the database to display.



Field	Description
Target Type	Identifies the mode that was used when the script was run. • **Console:** The script was run on the Security Controls console only and not against a set of target machines. • **Any:** The script was run on the console against selected target machines or machine groups without the services of WinRM (PowerShell remoting). • **ESXi Hypervisor:** The script was run against ESXi Servers and/or vCenter Servers.
Run Name	Identifies the name specified in the **Name this operation** box when the script was run. (See **How to Execute a Script** and **Scheduling Scripts**.)
Date	Identifies the date and time that the script was run.
Result Type	Identifies whether the line of output shows run results or machine results. • Run results contain output information related to the execution of the script. • Machine results contain the output that was created when the script was run against the selected machine.
Machine	Identifies the machine that the script was run against.
Domain	Identifies the domain to which the machine is assigned.
Template	Identifies the **ITScripts template** that was used to **initiate the script**.
Script Name	Identifies the name of the script that was run.
IP Address	Identifies the IP address of the machine.
Machine Group	Identifies the machine group that the machine was selected from (machines can belong to more than one group).
Result	Provides a short summary or status. For detailed result information you must **view the result output file**.

For additional information, see:

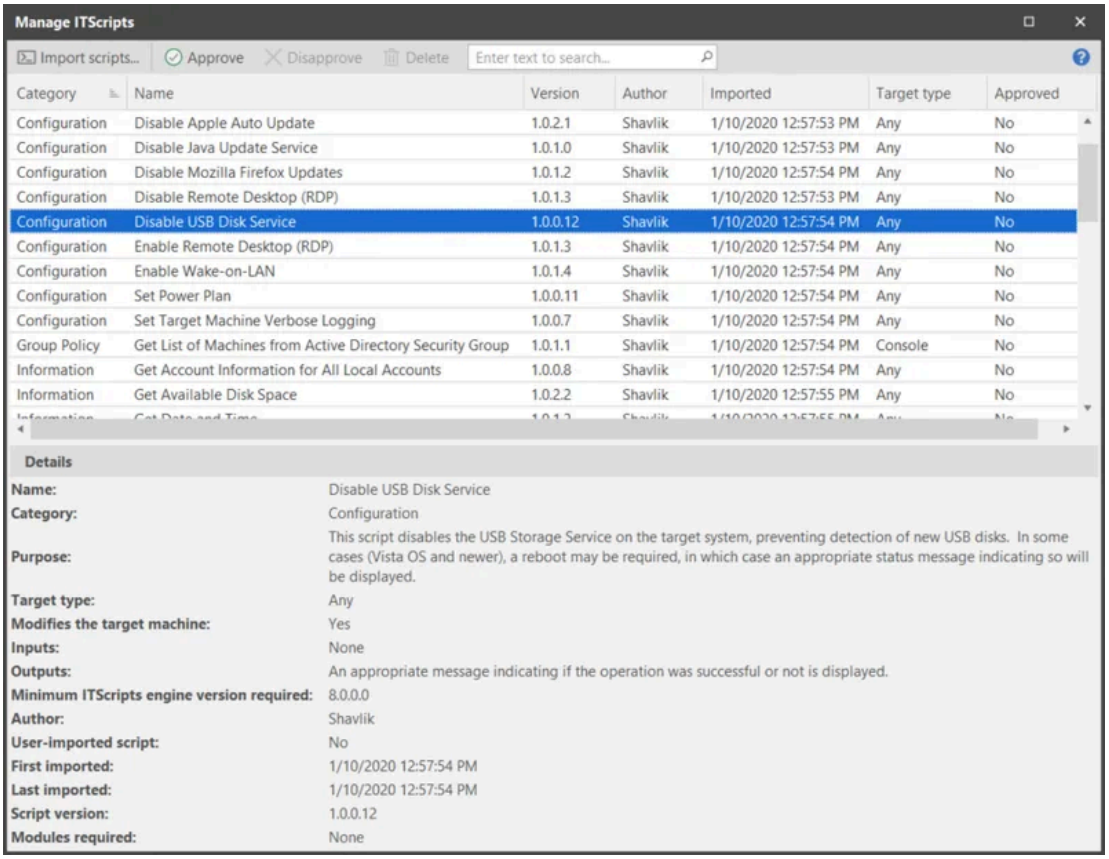
- **Performing Actions on Script Results**
- **Searching for Script Results**
- **Using the Script Result Smart Filter**

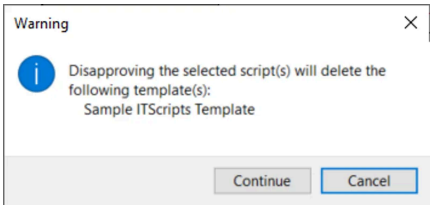
391. Managing ITScripts

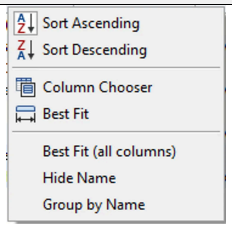
The Script Catalog Manager displays the scripts that are available and specifies which scripts are approved for use within your organization. Only those scripts that you approve will be available in other areas of the Security Controls interface. You can use the Script Catalog Manager to:

- View the list of all currently available scripts (predefined scripts and custom scripts)
- Import new custom scripts that you have created or that were created by someone you trust
- Approve, disapprove, and delete scripts
- Display details about an individual script

To access the Script Catalog Manager, select **Manage > ITScripts**. The program will automatically download and import the latest scripts available from Ivanti. When the process is complete the available scripts are displayed in the **Manage ITScripts** dialog.



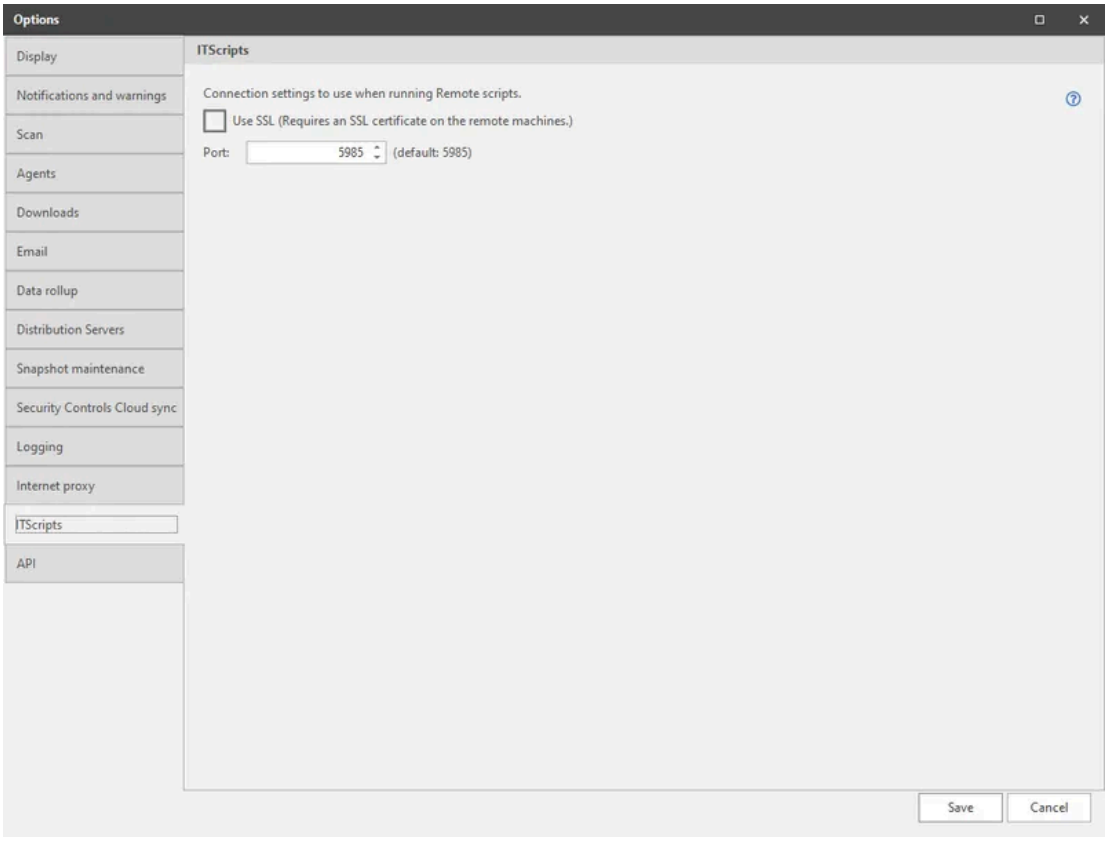
Field	Description
Import scripts	Import custom scripts that you created or that were created by someone you trust. In order to import a script the script must: • Be digitally signed by an authority that you trust • Contain metadata that uniquely identifies it and describes its functionality and input parameters If you are importing a script that was created by a third party your process should be as follows: • Download the script to an accessible location • Review the script for accuracy and for security issues • Re-sign the script with your own certificate or by someone you trust • Import the script into the Script Catalog Manager A console must trust the authority that issued the certificate in order to import or execute the script on that console. If you import user scripts on one console, they will also appear on other consoles that are using the same database. If the other consoles don't trust the signer, however, they will not be able to execute the scripts.
Approve	Approves the selected script(s) for use within the program.
Disapprove	Disapproves the selected script(s). The scripts will still be displayed in the dialog but they will not be available for selection elsewhere in the program. If you attempt to disapprove a script that is currently being used by an ITScripts template, a warning dialog is displayed. Verify that the script and the template are not needed before continuing. 
Delete	Deletes the selected script(s) from the Script Catalog Manager. Only custom scripts can be deleted.
Search	You can easily search for scripts contained in the top pane. All searches are performed using the Search tool.  To initiate a search you type the item you want to find and then press **Enter**. Only those scripts matching the search criteria are displayed; all other scripts are hidden. • The Search tool works only on the information currently visible in the pane. • All partial matches are displayed. For example, if you search for scripts named *Test*, any script with "test" in its name will be considered a match (e.g. TestScript1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
Column headers	• You can reorder the columns by clicking and dragging the column headers to new locations. • For example, if you want category information to be displayed in the first column, simply click on the **Category** column header and drag it to the first column. You can right-click within a column header and perform a number of additional actions.

Field	Description
	
Details	Displays the metadata that describes the selected script.

Tips for Using the Search Tool

392. ITScripts Options

The **ITScripts Options** dialog enables you to specify how the console will connect with remote target machines.



Field	Description
Use SSL	If you want the console to contact the target machines using an SSL connection, enable this check box. In addition, each target machine must contain a signed certificate and a WinRM HTTPS Listener.
Port	Specifies the port used by the console when contacting the target machines. The default value is as follows: • If you are NOT using SSL the default value is 5985 • If you ARE using SSL the default value is 5986

393. Searching for Event Entries

You can easily search for log entries contained in Event History. All searches are performed using the Search tool.



To initiate a search you type the term you want to find and then press **Enter** or click the search icon ( ). Only those event entries matching the search criteria are displayed; all other event entries are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the pane. The **Limit results to previous (days) option** can be used to adjust the amount of information that is displayed.
- If a **Smart Filter** is applied, only event entries matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for entries named *data*, any entry with "data" in its name will be considered a match (e.g. Synchronize core data files, database, etc.).
- The use of wildcards in the Search tool is not allowed.

394. Searching for Machines in the Top Pane

You can easily search for machines contained in the top pane. All searches are performed using the Search tool.



To initiate a search you type the machine name you want to find and then press **Enter** or click the search icon (🔍). Only those machines matching the search criteria are displayed; all other machines are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- If a **Smart Filter** is applied, only items matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for items named *Test*, any item with "test" in its name will be considered a match (e.g. TestMachine1, Contest, etc.).
- The use of wildcards in the Search tool is not allowed.

395. Searching for Machines in the Top Pane

You can easily search for machines contained in the top pane. All searches are performed using the Search tool.



To initiate a search you type the machine name you want to find into the Search box. Only those machines matching the search criteria are displayed; all other machines are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- If a **Smart Filter** is applied, only machines matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for machines named *Test*, any machine with "test" in its name will be considered a match (e.g. TestMachine1, Contest, etc.).
- The use of wildcards in the Search tool is not allowed.

396. Searching for Script Results

You can easily search for specific results contained in the Script Results View. All searches are performed using the Search tool.



To initiate a search you type the item you want to find and then press **Enter**. Only those scripts matching the search criteria are displayed; all other scripts are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the pane. The **Results since option** can be used to adjust the amount of information displayed within the pane.
- If a **Smart Filter** is applied, only script results matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for scripts named *Get*, any result with "get" in its name will be considered a match (e.g. GetServicesAsCSV, GadgetScript, etc.).
- The use of wildcards in the Search tool is not allowed.

397. Searching Machine Groups

Show Me!

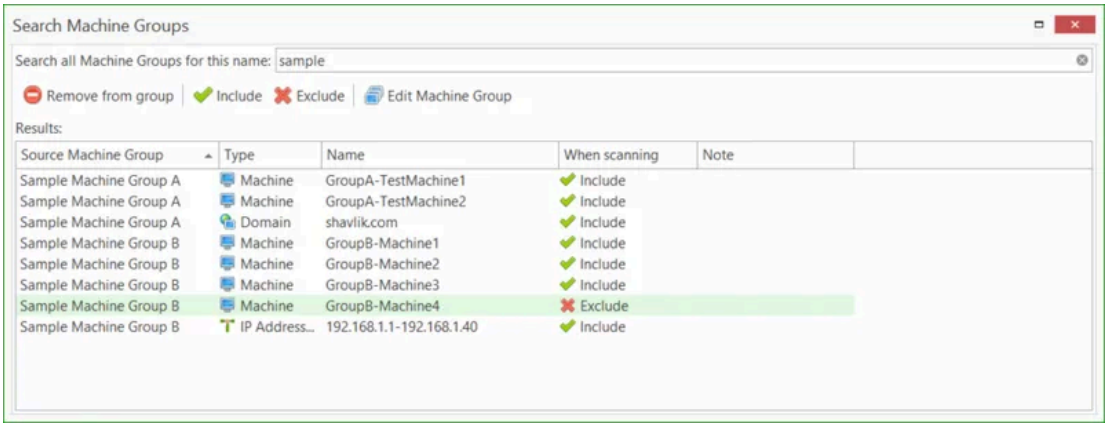
A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

You can search for names in any of your existing machine groups. This enables you to quickly locate specific machines and machine groups. This is especially useful for determining if a machine belongs to more than one machine group.

To initiate a search, right-click on any machine group in the navigation pane and select **Search Machine Groups**. The **Search Machine Groups** dialog is displayed. For example:



In the **Search all Machine Groups for this name** box, type the alphanumeric characters you want to find. Any machines or machine groups matching the search criteria will be displayed. Here are some tips for using the search tool:

- The search will look for matching characters in all columns except the **Type** column.
- All partial matches are displayed. For example, if you type *Test* as your search criteria, any machine with "test" in its name will be considered a match (e.g. TestMachine1, ContestantMachine, etc.).
- The use of wildcards is not allowed.

In addition, you can use the following buttons or right-click menu options to perform the following actions.

Action	Description
Remove from group	Deletes the selected machine from its machine group. You can use the Crtl or Shift keys to select multiple machines and delete all of the machines from the selected groups at once. If you want to delete a specific machine from all its groups: 1. Hover over the **Name** column header and in the upper-right corner click the column filter icon (). 2. In the column filter menu, select the desired machine name. 3. Multi-select all occurrences of the machine. 4. Click **Remove from group**.
Include	Includes the machine in any scans performed on the machine group. See the **When scanning** column for the current status.
Exclude	Excludes the machine from any scans performed on the machine group. For more information, see **Excluding Certain Machines**.
Edit Machine Group	Enables you to edit the selected machine group.

398. Searching for Hypervisors While Viewing a vCenter Server

You can easily search for hypervisors contained in the top pane. All searches are performed using the Search tool.



To initiate a search you simply type the search criteria in the **Search** box. Only those hypervisors that match the search criteria are displayed; all other hypervisors are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- The search will be performed on all information in the pane, not just the **ESXi Hypervisor Name** column.
- All partial matches are displayed. For example, if you search for hypervisors named *Test*, any hypervisor with "test" in its name will be considered a match (e.g. TestHypervisor1, Contest, etc.).
- The use of wildcards in the Search tool is not allowed.

399. Searching Patch View

You can easily search for specific patches contained in the top pane. All searches are performed using the Search tool.



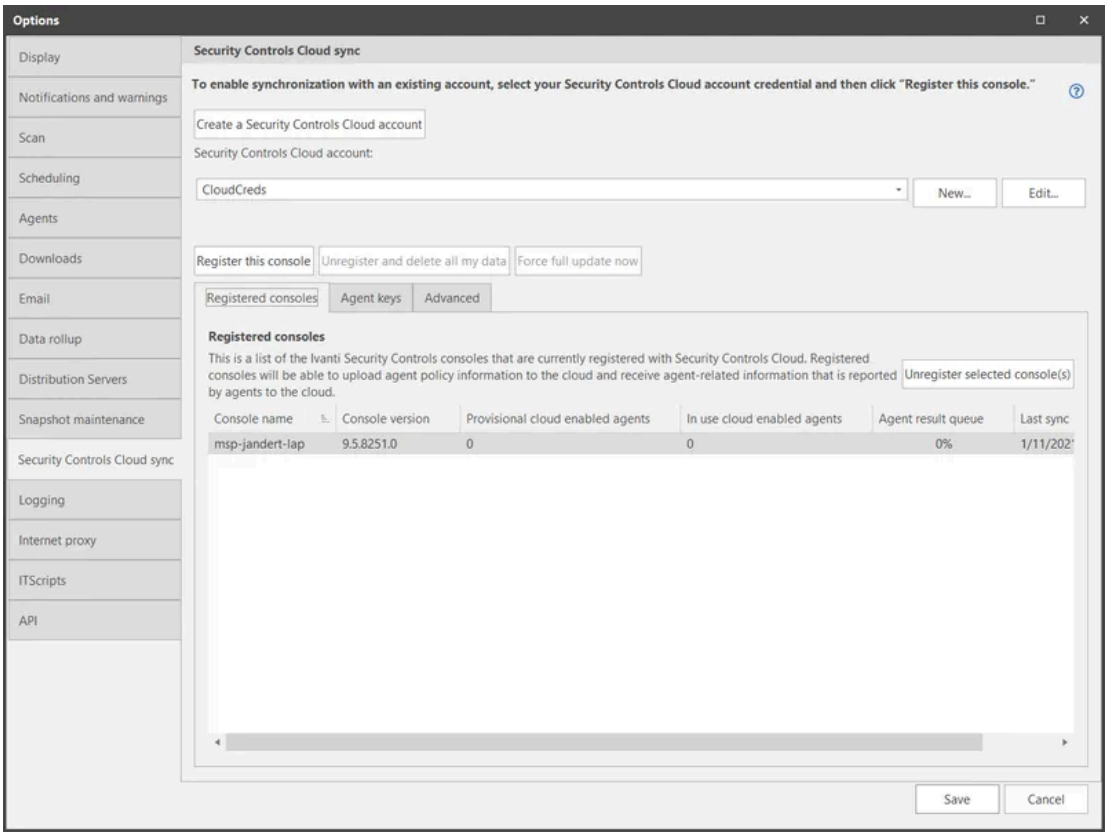
To initiate a search you simply click in the Search box and then type the text you want to find. Only those patches matching the search criteria are displayed; all other patches are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane.
- If a **Smart Filter** is applied, only patches matching BOTH the search criteria and the smart filter criteria are displayed.
- All partial matches are displayed. For example, if you search for patches that contain the text *acrobat*, any patch with "acrobat" in its name will be considered a match (e.g. Acrobat Distiller, Acrobat Reader, etc.).
- The use of wildcards in the Search tool is not allowed.

400. Security Controls Cloud Synchronization Options

The **Tools > Options >**Security Controls **Cloud Sync** tab is used to register your Security Controls console with the Security Controls Cloud service. Registering the console is the first step you must perform when configuring and using the **Security Controls Cloud synchronization feature**. After the registration process is complete, the console will be able to upload agent policy information to the cloud service and it will be able to receive agent-related information that is reported to the cloud service by agents.



Field	Description
Create a Security Controls **Cloud account**	If you do not have a Security Controls Cloud account, you can create an account by clicking this link or by going to **https://isec.ivanticloud.com/web/**. You can configure your Security Controls agents to use Security Controls Cloud as a cloud-based source for checking in and receiving policy updates.
Security Controls **Cloud account**	Select the credential (the user name and password pair) that you use to authenticate to your Security Controls Cloud account. If you have not defined your Security Controls Cloud credentials within Security Controls, you can do so by clicking **New**. For more information, see **Defining Credentials**.
Register this console	Uses the specified credentials to contact your Security Controls Cloud account and register the Security Controls console. When the process is complete the message **This console is registered** is displayed. You can also find a record of the registration within **Event History**.
Unregister and delete all my data	Unregisters the console and deletes all policy and agent data that resides on Security Controls Cloud. IMPORTANT! Any agent that communicates with the console solely via Security Controls Cloud will be effectively orphaned and will eventually uninstall itself.
Force full update now	Initiates an immediate update of your Security Controls Cloud account. Current copies of all agent policies that are configured to use Security Controls Cloud are synchronized with Security Controls Cloud. You should perform this action only if you have a concern that the agent policy data contained on the cloud service is not up to date. **Outbound port 443** must be available to complete this action.
Registered consoles / Agent keys	These two tabs show the console machines and agent keys that are being managed by Security Controls Cloud. For more information, see the next section, *How to Install Cloud Agents*.
Advanced	This tab is used to control the rate at which data is uploaded from the console to the cloud. Do not change the default settings unless you are experiencing synchronization issues or you are directed to by Ivanti Support. You can configure the following: • **Policies:** Specifies the number of policies to include in a single synchronization POST command. • **Agent configurations:** Specifies the number of agent configurations to include in a single synchronization POST command.

How to Install Cloud Agents

> Tip: You can perform these same steps from the Cloud. For more information, see **Installing Agents from the Cloud**.

If you are using **Security Controls Cloud synchronization**, you have the ability to install a Security Controls Agent from the cloud. This is particularly helpful if you have target machines that are away from the corporate network and unable to contact the console.

Requirements

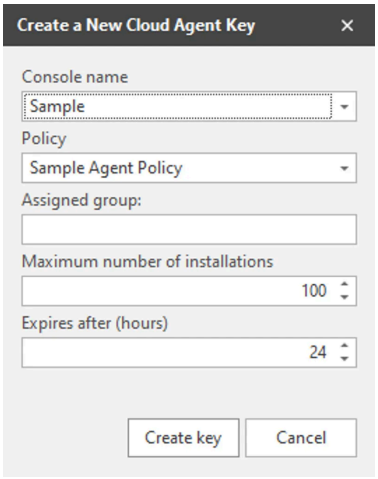
- The target machine must have Internet access

- The Security Controls console must be registered with Security Controls Cloud
- Outgoing TCP ports 80 (http) and 443 (https) must be available when communicating with Security Controls Cloud
- The URL *isec.ivanticloud.com* must be accessible when communicating with Security Controls Cloud
- There must be at least one agent policy that is configured to allow **synchronization with Security Controls Cloud**
- You cannot install a cloud-based agent on a Security Controls console machine
- Each user that installs an agent must have administrator access on their target machine

Installation Instructions

On the Security Controls **Console**

1. Select **Tools > Options >**Security Controls **Cloud Sync**.
2. On the **Registered consoles** tab, verify that your Security Controls console is registered with Security Controls Cloud.
3. Select the **Agent keys** tab.
4. Click **New key**.
   The **Create a New Cloud Agent Key** dialog is displayed. Use this dialog to create an activation key that can be used to install one or more agents.
5. Provide all necessary information and then click **Create key**.
   The agent key is created.



Field	Description
Console name	Select the Security Controls console that will be used to manage the agent. TIP: If the console does not contain a user-friendly name that has some significance to other users, before proceeding you might consider **Console_Alias_Editor.htmchanging the name** within Security Controls and then re-registering the console with Security Controls Cloud.
Policy	Select the agent policy that you want to assign to the agent. Only those policies that are configured for **synchronization with Security Controls Cloud** will be available for selection.
Assigned group	Type the name of the group to which the agent machine will be assigned within Machine View and Scan View. You might assign all Cloud agents to the same group, or you might choose to group the agents with other machines that share similar attributes such as physical location or the same agent policy. After the agent checks in with the console, you will be able to use the **Assigned Group column in Machine View** to sort the grid and easily locate the Cloud agents.
Max. number of installations	Specify the maximum number of agent installations you will allow to be performed using this agent key. **Example:** Assume you want to install agents on all of the machines at a remote site. You are not certain how many machines are at the site but you are confident that there are fewer than 10 machines. By specifying a maximum of 10 installations for this key, you are enabling all the machines at the remote site to install agents and yet limiting the number of license seats that can be consumed using this key. You cannot install an unlimited number of agents because the Security Controls console will not allow you to exceed your license count.
Expires after (hours)	Specify how long the key can be used to install new agents. For example, if you know that an administrator will be at a remote site for two days to help with the agent installations, you can specify that the key is only valid for 48 hours. This allows you to control your exposure to other people consuming license seats from the console.

6. Email the agent key to the desired users.

Use the **Copy key to clipboard** button to copy the key and then paste it into your email message. You message should also include a web link for downloading the agent installation program and detailed instructions on how to install the agent. Here's a sample message:

Hello:

This message contains the information you need to install Security Controls Agent onto your computer using the Security Controls Cloud synchronization process.

Agent Download: https://content.ivanti.com/data/isec/v9.5/binaries/5973/STPlatformUpdater.exe

Agent Activation Key: b468b9aab468b9aab468b9aa468b9aa

Expiration Date: 1/9/2021 2:26:10 PM (Central Standard Time)

1. Click the **Agent Download** link and save the file named **STPlatformUpdater.exe** to your local hard drive.
2. Double-click the file named **STPlatformUpdater.exe.**
3. On the **Agent Registration** dialog, click **I connect to the console through the cloud**.
4. Paste or type the agent activation key.
5. (Optional) If you use a proxy server to access the Internet, click **Configure proxy** and provide your proxy information.
6. Click **Register**.

The agent will be placed into a temporary provisional state until the registration request is processed. The registration process may take several minutes to complete. After the registration is approved, the next time the agent checks in it will receive its agent policy and it will become a fully-functional agent.

On the Target Machine

1. Log on to the target machine using an administrator account.
2. Open the Security Controls Cloud Sync email message that contains the agent key and the installation instructions.

> If you do not have access to the Security Controls Cloud Sync email message but you have a Security Controls Cloud account, you can create your own agent key by opening a web browser on the target machine and then following the instructions in the **From your web browser** section in the **Installing Agents from the Cloud** help topic. After the key is created and while you are still logged in to Security Controls Cloud, click the **Download Agent** link that is located to the right of the new key; this enables you to download the agent installation program to the target machine.

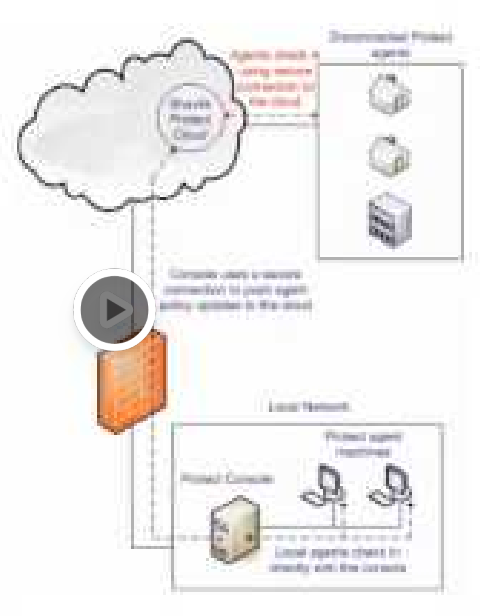
Use the instructions to install and register the agent.
You will install the agent, specify that you are connecting to the console through the cloud, paste the activation key, and then click **Register**.

4. Wait for the agent registration process to complete; this may take up to 20 minutes or more to complete.
   The agent will be initially placed into a temporary provisional state while the registration is processed. During this time the Security Controls console will learn about the registration request, verify that enough license seats are available, and provide the Security Controls Cloud service with the necessary files. After the registration process is complete, at the next check-in time the agent will retrieve its assigned agent policy from the cloud and will become a fully-functional agent.

401. Security Controls Cloud Synchronization Overview

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:

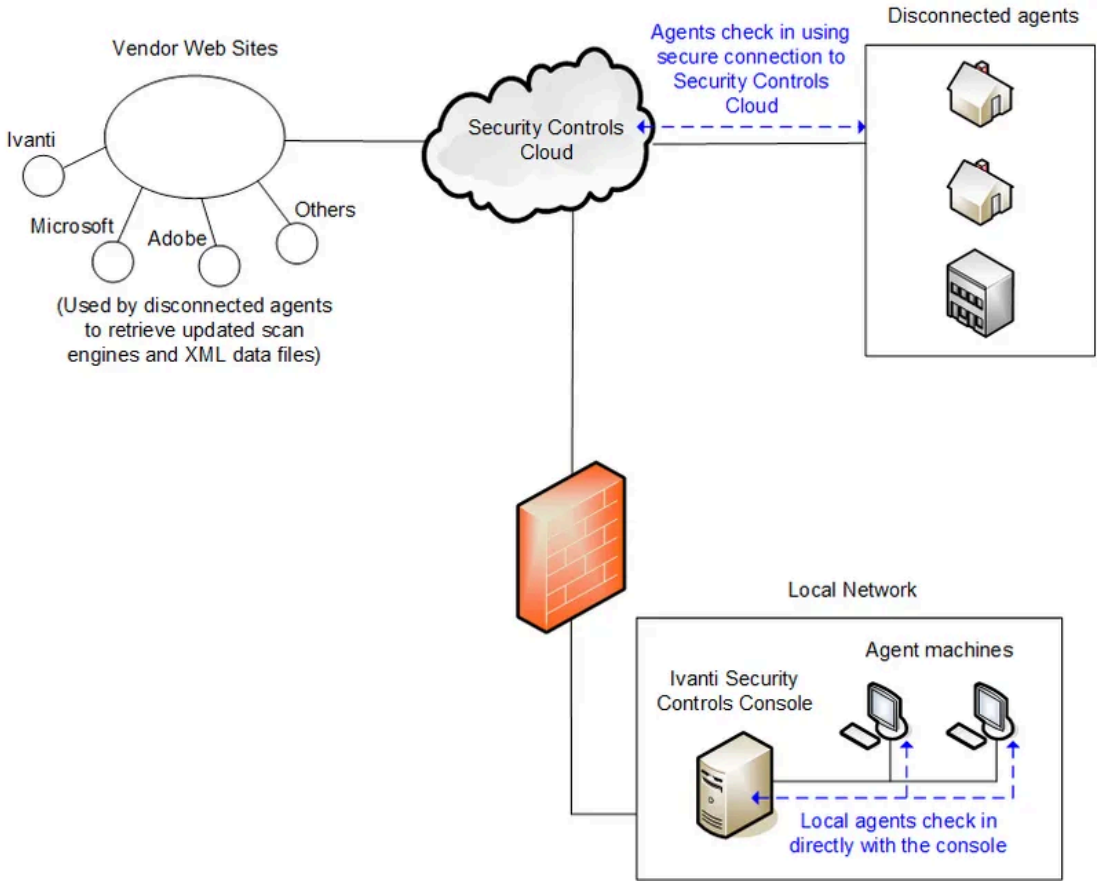


Overview Information

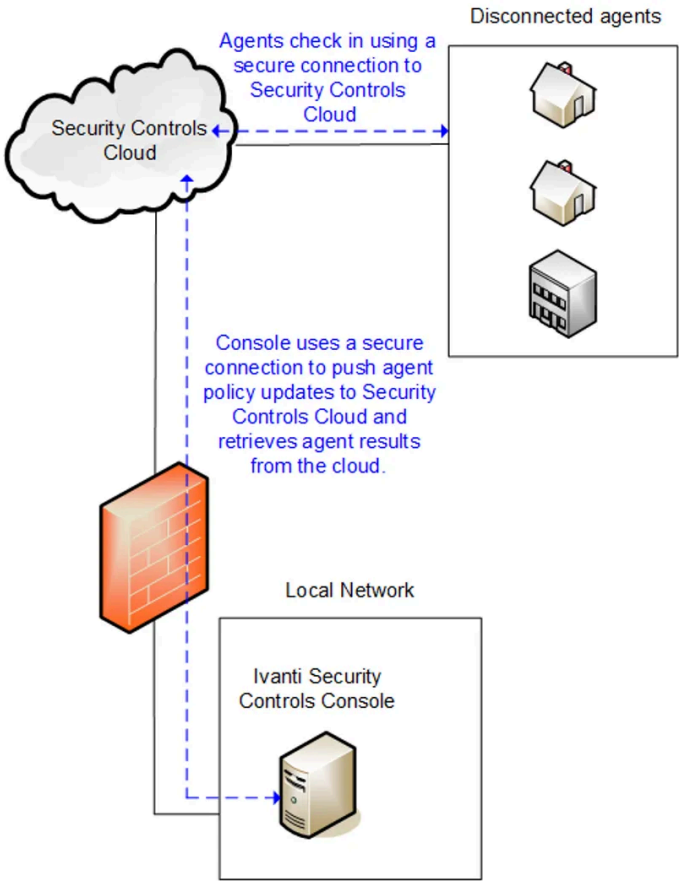
The Security Controls Cloud synchronization feature enables your agents to check in and receive policy updates from the cloud. This allows you to manage agents on machines that are not able to communicate directly with the console. This feature also provides you with the ability to **install a Security Controls Agent using the cloud**.

Agents that are configured to use Security Controls Cloud will have two check-in options: they can continue to check in with the Security Controls console, but they will also be capable of checking in and receiving policy updates via the cloud. This is particularly useful for disconnected agent machines that are away from the corporate network and unable to contact the console for updates. As long as an agent machine has Internet access, it will be able to send results and get updates using the cloud.

The following diagram illustrates the two agent check-in options:


Vendor Web Sites
Ivanti
Microsoft
Adobe
Others
(Used by disconnected agents to retrieve updated scan engines and XML data files)
Security Controls Cloud
Agents check in using secure connection to Security Controls Cloud
Disconnected agents
Local Network
Agent machines
Ivanti Security Controls Console
Local agents check in directly with the console

402. Security Controls Cloud Synchronization Requirements and Usage Notes



Requirements

- Must be running Security Controls Standard or Security Controls Advanced
- Must have a Security Controls Cloud account
- Applies only to agents that are **configured to use Security Controls Cloud synchronization**
- The console must have a reliable Internet connection
- Outgoing TCP ports 80 (http) and 443 (https) must be available when communicating with Security Controls Cloud
- The URL *isec.ivanticloud.com* must be accessible when communicating with Security Controls Cloud

Usage Notes

- When using Security Controls Cloud synchronization, the agent check-in process is as follows: At the scheduled check-in time, the agent will attempt to check in with the console. If the agent can access the console it will check in directly with the console. If the agent does not have access to the console but it does have Internet access, it will perform the check-in using the cloud.
- When a disconnected agent checks in with the cloud it reports the same information (scan results, etc.) that it would to the Security Controls console. Security Controls Cloud provides a generous amount of storage to cache results until the consoles retrieves the data. The console will automatically retrieve data from the cloud several times every hour.

- Engine components and data files are not a part of the Security Controls Cloud synchronization process. Agents will continue to receive updated engines and data files from either the console or the vendor websites. If an agent is using a policy that specifies the use of a distribution server, it is strongly recommended that you enable the **Use vendor as backup source** check box.
- A listening agent is treated no differently than any other agent. If a listening agent is on the local network and receives notice from the console that there is a policy change, it will receive the updated policy from the console. If a listening agent is away from the local network and unable to communicate with the console, it will perform its check-in using the cloud.

403. Potential Security Implications When Sharing Credentials with Background Services

When you **share a credential with background services**, that credential becomes available to all other administrators for use with Security Controls service components. For example, say Administrator A creates a credential, enables it for sharing with background services and then assigns it to the proxy service. Administrator B is now free to assign that same credential to other service areas of the program.

Therefore:

- Only enable sharing with background services on those credentials that are needed by Security Controls service components.
- **DO NOT** enable sharing with background services on credentials that allow access to secure areas of your organization.

It is recommended that you create a service account to perform background service functions rather than using a domain administrator account.

Security Controls supports Kerberos authentication for background service interaction with various resources in addition to explicitly specified credentials. Granting permissions to the `Domain\Machine$` account can be used to provide access to network shares and distribution servers in scenarios where it is not desirable or possible to create a service account.

Further, shared service credentials can be updated at any time. This makes password update maintenance easy.

404. Shared Credentials

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:

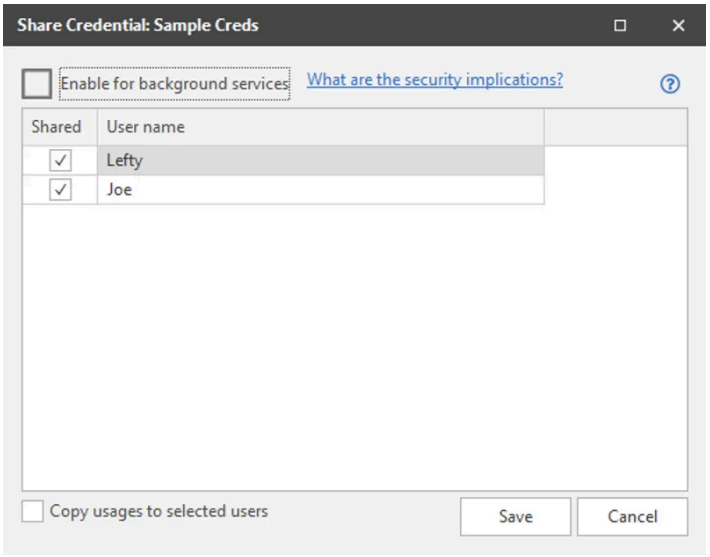


Any credential that you own can be shared with other users of the program. In this case, a "user" can be another person who has logged on to the console machine and launched Security Controls, or it can be a user you have created using a **REST API request**. Sharing a credential enables other users to use the credential without knowing the secure details about the credential. For example, a senior administrator may possess credentials that provide access to a secure area of your organization. The senior administrator can share the credential with one or more junior administrators. This enables the junior administrators to access the required areas and perform their jobs without revealing the password.

All credentials are stored with strong encryption techniques. Only the credential owner and those users the owner has elected to share the credential with are able to decrypt and use the credential.

> The credentials are encrypted using NIST recommendations and FIPS 140-3 certified algorithms.

To share a credential, on the **Manage Credentials** dialog, select the desired credential and then click **Share**. The **Share Credential** dialog is displayed.



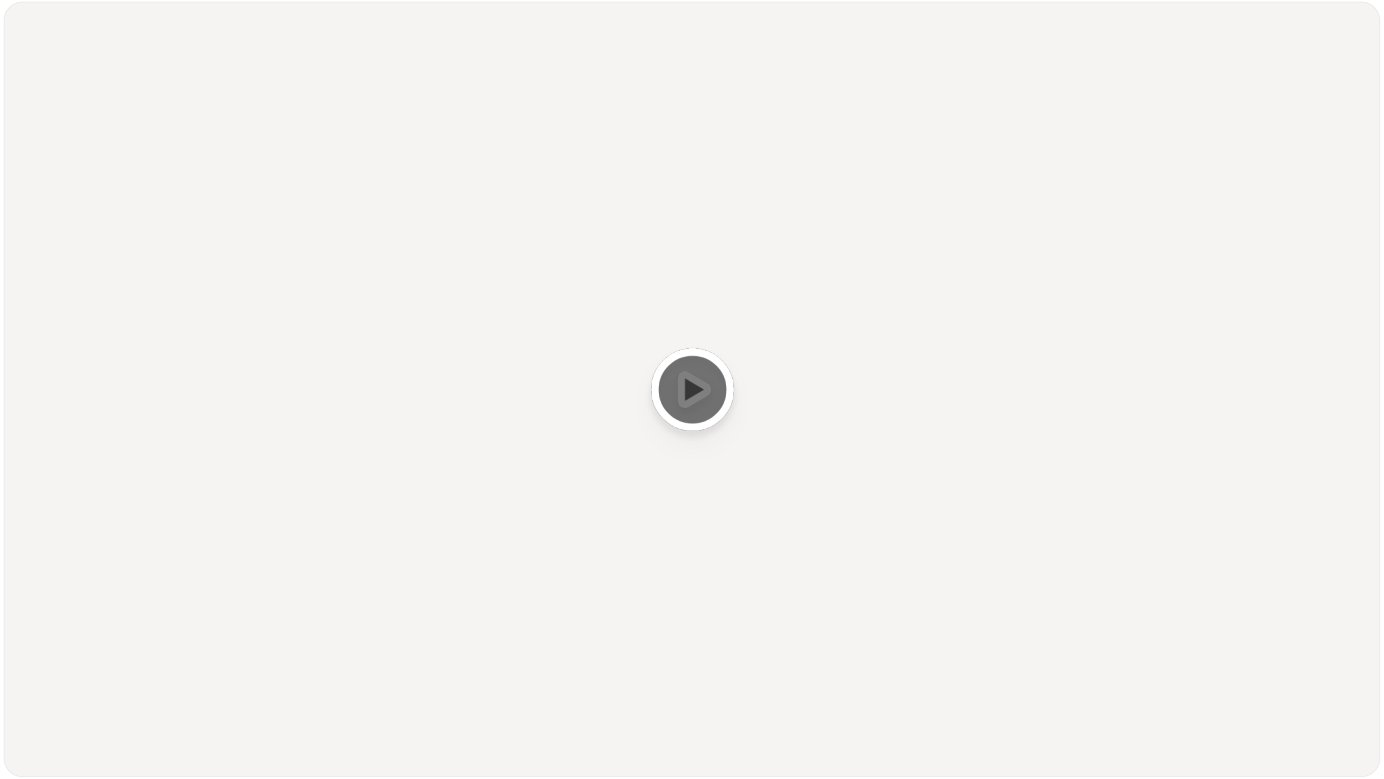
The credential whose shared settings are being edited is shown in the title of the dialog.

Field	Description
Enable for background services	If enabled, the credential shown in the dialog title can be used to specify credentials for service components within the program. The credential account must have administrator rights on the console server. The service components within Security Controls that require a shared credential include the following: • Agent Internet proxy • Console scheduler • Distribution servers • Email service • License server when using the Credentials Activation Method • Proxy service Why is it necessary to share a credential with background services? Credentials are encrypted, so you must share a credential so that the service components can access and decrypt it when needed. **Example:** If you select **Tools > Options > Internet proxy** and attempt to assign **Service credentials**, only credentials that are shared with background services are available for selection. The service must have access to the credential in order to decrypt it.
What are the security implications?	It is recommended that you create a service account to perform background service functions rather than using a domain administrator account. For more information, see Potential Security Implications When Sharing Credentials.
Shared	Indicates if the credential will be shared with the associated user name.
User name	Any user who has previously logged on to the Security Controls console machine will be displayed in this list. Each user is assigned a unique user certificate and an associated private key that enable the user to encrypt and decrypt shared credentials. Any user without a user certificate is not eligible to be assigned a shared credential and will not be displayed in the list. If the list contains users who are no longer affiliated with this project, you can delete them using the User Manager dialog.
Copy usages to selected users	If enabled, all usages of the credential by the credential owner will be propagated to the selected users. For example, if you share a credential that is being used to schedule console tasks, enabling this check box will automatically update the console scheduler credential assignment for the shared users. You can verify the usage assignments using the View usages button on the **Credentials Manager** dialog.

405. Show Me How to Get Started!

Most tasks in Security Controls are simple to perform, you just need to know how to get started!

The following table lists a number of the most commonly performed tasks in Security Controls. For each task you can click the **Read a Help Topic** link to view the associated Help topics, or you can click the **View a Video Tutorial** link to view the associated "How-to" video.



Task Category	Read a Help Topic	Inline image View a Video Tutorial
Patch Management (Windows)	Scan for and Deploy Patches	
	Track Deployment Status	
	Automate Scheduled Patching	
Patch Management (Linux)	Create a Custom Patch XML File Overview of Linux Patch Management	
Asset Inventory	Use the Asset Inventory Feature	
Power Management	Use the Power Management Feature	
Agents	Create an Agent Policy Install an Agent Policy Implementing Cloud-based Synchronization	
Virtual Machines	Deploying ESXi Hypervisor Bulletins Manage Your Virtual Machines	
ITScripts	Use the ITScripts Feature	
Distribution Servers	Use a Distribution Server	
General Operation	Generate Reports Manage Credentials Shared Credentials Initiate a Remote Desktop Connection	

406. Shutdown Implementation Notes

There are two methods you can use to shut down the connected machines in your organization.

- You can use the right-click **Power > Shut down now shortcut command** from within Machine View or Scan View. With this method:
    - The console machine is not affected
    - The selected machines will be shut down immediately
    - No warning will be issued to active users of those machines

You can use a **power state template** to schedule a shutdown. With this method:

- The console machine is eligible to be shut down
- You can schedule the shutdown to happen immediately or at some point in the future
- A warning will issued to all active users of those machines

The Shutdown command works with the following target machine states:

Initial Power State of Target Machine	Target Machine Shut Down?
Fully powered on	Yes
Sleep state	No action
Hibernate state	No action
Powered off	No action

407. Signing Scripts

A script must be signed by an authority trusted by the console in order to be imported or executed by Security Controls. All scripts provided with Security Controls are signed by Ivanti. During the installation of Security Controls, the Ivanti certificate is added to the trusted certificate store on the console machine.

You must sign scripts that you create before importing them into Security Controls. To do this, you need a signing certificate. That certificate must be issued by an authority that is in the trust list for the console(s) that are going to execute the scripts you create.

This section will describe one way to create a signing certificate and add it to the trusted certificates on the console.

Creating a Root Certificate Capable of Issuing a Code Signing Certificate

> This step requires the use of Windows 10 or Windows Server 2016 or later.

To create a new root certificate capable of issuing a code signing certificate, use the following command.

Bash

```
PS C:\> $signerRoot = New-SelfSignedCertificate -Subject "CN=PowerShell Local Certificate Root2" -HashAlgorithm Sha256 -CertStoreLoc
```

Creating a Signing Certificate

> This step requires the use of Windows 10 or Windows Server 2016 or later.

The next step is to create a signing certificate that is issued by the root certificate. To do so, enter the following at the command prompt:

Bash

```
PS C:\> $powershellSignerSigner = New-SelfSignedCertificate -Subject "CN=PowerShell User" -HashAlgorithm Sha256 -CertStoreLocation C
```

Verifying the Signing Certificate

You can verify the certificate from within PowerShell by entering the following command:

Bash

```
Get-ChildItem cert:\LocalMachine\My -codesigning | Where-Object {$_.Subject -match "CN=PowerShell User"}
```

If the certificate is found, it will display the thumbprint and subject of the certificate, similar to this:

```
Thumbprint                                Subject
----------                                -------
8249ABF7E1CE182DBE43D4FB522CC08C07907299  CN=PowerShell User
```

Move the Signing Certificate to the Trusted Root Certificate Store

You must move the signing certificate from the "My" certificate store into the trusted "Root" certificate store. This builds up the chain of trust to the root store.

Bash

```
PS C:\> Move-Item -Path "Cert:\LocalMachine\My\$($signerRoot.Thumbprint)" -Destination Cert:\LocalMachine\Root
```

Signing a Script

This section will describe how to sign a script file from a PowerShell prompt or within the PowerShell ISE.

From the PowerShell command prompt, change to the directory containing your script file. In this example, it is named test-script.ps1. Then enter the following two commands:

> The first command should be entered on a single line. The CN=PowerShell User should match the name you specified when creating the signing certificate.

Bash

```
$cert = @(Get-ChildItem cert:\LocalMachine\My -codesigning | Where-Object {$_.Subject -match "CN=PowerShell User"})[0]
Set-AuthenticodeSignature .\test-script.ps1 $cert
```

The first command will locate the certificate in the certificate store. The second command signs the script using that certificate.

Signing the script will add a block at the end of the script that looks similar to this:

Bash

```
# SIG # Begin signature block
# MIIEMwYJKoZIhvcNAQcCoIIEJDCCBCACAQExCzAJBgUrDgMCGgUAMGkGCisGAQQB
# gjcCAQSgWzBZMDQGCisGAQQBgjcCAR4wJgIDAQAABBAfzDtgWUsITrck0sYpfvNR
# AgEAAgEAAgEAAgEAAgEAMCEwCQYFKw4DAhoFAAQU4QyppfQY+5HviH7wuIBvvmRf
……
# SIG # End signature block
```

If you make any changes to the script, you will need to re-sign it.

Signing a Script Using a PFX File

If you'd like to sign scripts using the same signing certificate on multiple machines without installing the signing certificate on each machine, you can use a PFX (Personal Information Exchange) file.

To create a PFX file:

1. Run `CertMgr.exe`.
2. On the **Personal** tab, select the signing certificate.
3. Click **Export**.
4. On the first export wizard screen, click **Next**.

5. Select the **Personal Information Exchange** option.
   If there is an **Enable strong protection** option, choose it.
6. Enter a password when prompted.
   This will be required when using this pfx file to sign scripts.
7. When prompted, type a name for the pfx file.

To sign a script using the PFX file, enter the following commands in PowerShell:

Bash

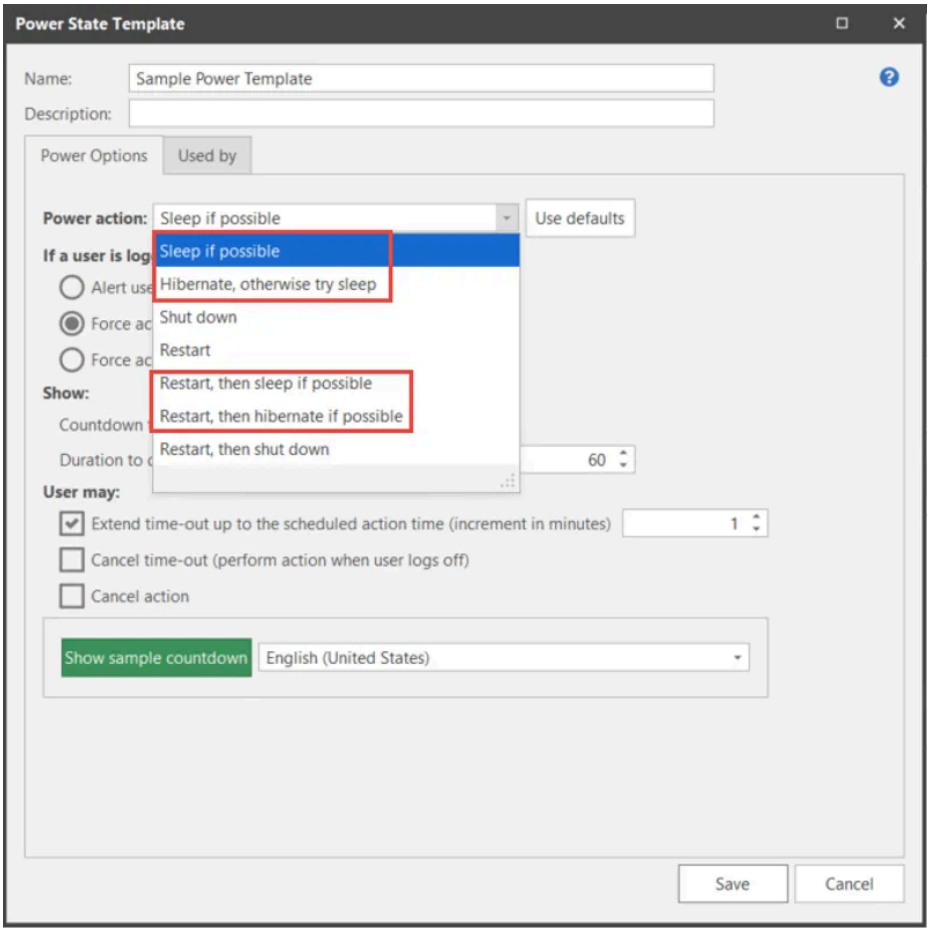
```
$cert = Get-PfxCertificate mycert.pfx
Set-AuthenticodeSignature .\test-script.ps1 $cert
```

When prompted, supply the password you created in Step 6.

408. Sleep and Hibernation Implementation Notes

You can use a **power state template** to put your machines into a sleep state or a hibernate state.

- **Sleep state:** This is a low power state that eliminates power to all unneeded areas of the machine.
- **Hibernate state:** This is very similar to sleep state, with the difference being that the machine's RAM is copied to a storage area (such as a hard drive) before hibernate state is initiated. This enables a user to very quickly restart the machine, restore the previous state, and resume working. If a target machine is not **configured to allow hibernation**, the program will instead attempt to put the machine into a sleep state. If the machine cannot be put into a sleep state no action will occur.



The machines can be put into sleep or hibernate state immediately, or they can be restarted before being left in the desired power state.

Like any other job that is scheduled from the console, the power state job will only work on those target machines that are in a fully powered on state when the job is initiated. Machines that are in a reduced power or powered off state are not affected.

The following table indicates when a sleep or hibernate command will work on a target machine:

Initial Power State of Target Machine	Logged On Users?	Action Taken?
Fully powered on	Yes	Yes, unless the user cancels the action
	No	Yes
Sleep state	N/A	No action
Hibernate state	N/A	No action
Powered off	N/A	No action

409. SourceType view

The Reporting2.SourceType view defines source types.

Column Name	Data Type	Nullable	Description
Id	tinyint		The source type id.
Value	nvarchar(100)		The string value of the id.
Description	nvarchar(512)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the Reporting.SourceType view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[SourceType]
```

ID	Value	Description
0	Unknown	Invalid or Unknown source
1	Interactive User	
2	Agent	
3	API	

410. Specifying ComputerName and Credential Parameters

When creating custom scripts, you specify the target type in the script metadata. Keep the target type in mind when writing the script. The primary thing to consider when writing the script will be whether you should include the ComputerName and Credential parameters on the commands. The ITScripts environment provides the computer name in the ST_ComputerName variable and the credential for that computer in the ST_Credential variable. For example, when writing a script with target type of “Any” you might specify this command:

```Bash
Get-WmiObject win32_Share -ComputerName $ST_ComputerName -Credential $ST_Credential
```

However, this command will fail if run against the local machine with the following error:

```Bash
Get-WmiObject : User credentials cannot be used for local connections
```

In other words, this command will work if the target type is “Any” and the target machine is not the console, but it will fail in the following cases:

- Target type is ‘Console’
- Target type is ‘WinRM Remoting’
- Target type is ‘Any’ and the target is the console computer

To take these cases into account, your script may need to test whether it is using remoting, or if the target is the console machine. To simplify script creation, ITScripts provides two functions: **ST-ComputerAndCredential** and **ST-SubCC**.

ST-ComputerAndCredential

This function returns a string containing the appropriate string to use for the

-ComputerName and -Credential parameters based on the type of script, whether it is executing on the console, and whether credentials were provided for the machine. It will return one of these strings:

```Bash
“-ComputerName $ST_ComputerName –Credential $ST_Credential”
“-ComputerName $ST_ComputerName”
“”
```

You can use this in your script command without concern for the environment you are executing in. For example:

```Bash
$cc = ST-ComputerAndCredential
$shares = Invoke-Expression "Get-WmiObject win32_Share $cc"
```

Invoke-Expression is used in order to substitute the value of $cc before executing the command. The issue with this construct is that you must remember to escape special characters in your command. For example, the "$" and quote characters need to be escaped in the following command:

```Bash
$ST_CC = ST-ComputerAndCredential
$registryObject = Invoke-Expression "Get-WmiObject -list
-namespace root\default $ST_CC |
where-object { `$_.name -eq `"StdRegProv`" }"
```

The following function makes this even simpler.

ST-SubCC

This function combines the two commands shown in the previous example. The first time it is invoked, it puts the result of ST-ComputerAndCredential into a PowerShell variable named ST_CC. It then passes the resulting command to Invoke-Expression. The thing to remember when using ST_SubCC is to place the command inside single quotes, not double quotes. The previous examples would be:

```Bash
$shares = ST-SubCC 'Get-WmiObject win32_Share $ST_CC'
```

```Bash
$registryObject = ST-SubCC 'Get-WmiObject -list
-namespace root\default $ST_CC |
where-object { $_.name -eq "StdRegProv" }'
```

411. Specifying a Default Patch Scan Template

To specify which patch scan template Security Controls should use as the default, you can do one of the following:

- In the **Patch Scan Templates** list, right-click the template name and select **Make default**.
- Select **Tools > Options > Scan** and specify the default scan template in the **Default Patch Scan Template** box.

When you have identified a default template, the word **(default)** will be appended to the template name. The default template will be used for all one-click scanning operations on the **Agentless Operation page**.

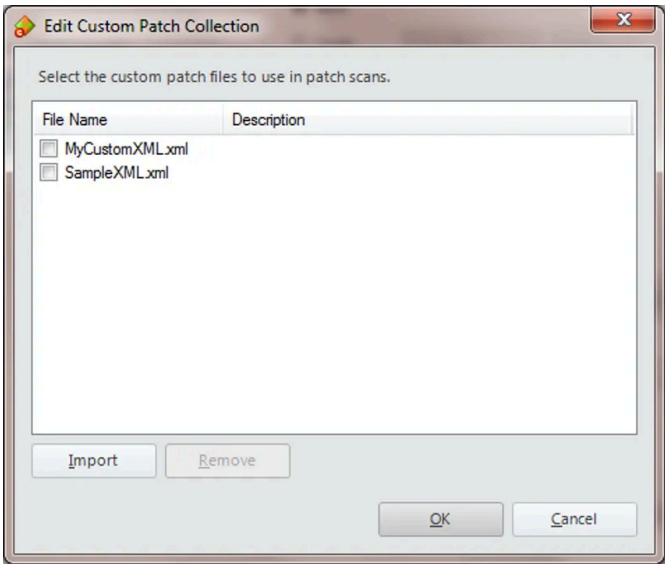
412. Specifying Which Custom XML Files to Use

Security Controls enables you to create many different custom XML files. However, you may not want to use all your custom XML files all the time. For this reason Security Controls also enables you to specify which of your custom XML files (if any) that you want to use in your scans and deployments.

> For information on creating custom XML files, see **Creating A New Custom XML File**.

To specify the custom XML files that will be used in your scans and deployments:

1. From the Security Controls menu select **Manage > Custom Patches**.
   The **Edit Custom Patch Collection** dialog is displayed. It contains a list of custom XML files you have previously imported into the dialog.



(Optional) If you have created additional custom XML files that are not currently in the list, you can add them to the list by clicking **Import**.
Navigate to the custom XML file you want to add and then click **Open**. The new XML file is added to the list. Repeat this step for each new custom XML file you want to add to the list.

> IMPORTANT! Any custom XML file that has been changed since it was initially imported must be removed and then re-imported. If you just re-import a changed file without first removing it, the program will continue to use the old version of the file.

Enable the check boxes for the custom XML files you wish to include in your patch scans and deployments.
The XML files included in all future scans and deployments will be the standard XML patch file plus any of the custom XML files enabled here. The available XML files are called your *collection*; the custom XML files currently enabled for use is called your *active collection*.

4. Click **OK**.
   Security Controls will perform a validation process to ensure that all the selected custom XML files and the primary XML patch file can be successfully combined. Although you should have already validated each individual custom XML file, Security Controls must make sure that the files collectively are okay. For example, if you inadvertently used the same name for two different custom products in two different custom XML files, the validation process will catch this.

If an error occurs during the validation process the custom XML files will not be used. You must correct the problem and try again.

Removing a Custom XML File

To remove a custom XML file that has been previously combined with the primary XML file:

1. On the **Edit Custom Patch Collection** dialog, clear the check box of the custom XML file you no longer want to use.
2. Click **OK**.

Only those custom XML files still enabled will be included in the validation process and used with the primary XML file.

413. Microsoft SQL Server Database Maintenance

If you are at a company that is running Ivanti products in a full SQL Server environment and have a database administrator on staff with SQL Server maintenance and backup policies already running against our databases, great! If you are running SQL Server Express or a full edition of SQL Server but don't have a maintenance and backup plan in place, please keep reading.

Database instability and corruption is the single biggest cause of an upgrade issue that is encountered and the root cause of many GUI performance issues that can be mitigated and, in many cases, resolved by proactive maintenance on the database. Below are our recommendations for good regular maintenance on your database so you keep it running slim and clean for good performance and to reduce issues.

Keep in mind this is a starting point. If you have regulatory needs that require more data kept live you should adjust to keep more data live. If that is the case you may want to analyze how frequently you are scanning. 1000 agents scanning eight times a day will grow your database at a much more rapid rate than once per day or once per week. And in most cases, you don't really need all of that data.

The following are our recommendations for regular database maintenance.

Data Retention

Determine the amount of data that needs be kept on hand for operational purposes. Typically 60-90 days is acceptable for operational purposes. Use the Ivanti Security Controls Database Maintenance tool to cleanup anything older than that number of days and schedule the task to run on a regular basis.

Reporting

Determine what report data is required for audit\regulatory requirements. Run monthly reports to fulfill these needs and keep the reports on file as far back as your policy requires. Typically, 13 months is an acceptable amount of time to save report data.

Database Backups

Ivanti recommends running weekly incremental and monthly full backups. The backup should be run just before your scheduled purge. Keep backups as far back as the reporting data.

Database Maintenance Schedule

- **Backups:** Full monthly, just after patch maintenance for that month. Incremental weekly, end of each week (after weekend patch windows preferably).
- **Purge Data:** After the full monthly backup is run
- **Reindex:** After purge data is run
- **Integrity:** After reindex is run

Database Maintenance Tool

SQL Server Express users who do not have access to the SQL Server Maintenance Plan Wizard can use the Ivanti Security Controls Database Maintenance tool. The Database Maintenance tool enables you to:

- Delete old results
- Rebuild your SQL Server indexes

- Create backup copies of your database and your transaction log

You do this by selecting **Manage > Database maintenance** and then specifying exactly when and how your database maintenance tasks should be performed. For more information, see the Database Maintenance help topic.

SQL Server Maintenance Plan Wizard

If you are using a full edition of SQL Server, you should use the SQL Server Maintenance Plan Wizard to setup your maintenance plans. You could use the Ivanti Security Controls Database Maintenance tool, but the SQL Server Maintenance Plan Wizard is more robust and provides additional functionality.

Related Topics

- Console Software and Hardware Recommendations
- Port Requirements and Firewall Configuration
- Distributed Environment Management
- Agentless Patch Management
- Best Approach for Applying Patches in an Agentless Environment
- Automating Patch Management in an Agentless Environment
- Agent-Based Patch Management
- Agent Rollout Options
- Installing and Supporting Agents on Internet-Based Machines
- Agent-Based Product Level and Patch Deployment Process
- Guide to Surviving Patch Tuesday
- Performing Patching in a Disconnected Environment

414. Explanation: Deciding Whether to Permit the Use of an SSH Connection

The **SSH server connection** setting specifies if an SSH connection can be used when the console communicates with an endpoint. There are potential security risks when using an SSH connection, so before making a decision, it is important to understand how and when SSH is used within Security Controls.

Background Information

The first thing to know is that Security Controls uses the SMB protocol to communicate with Windows machines and the SSH protocol to communicate with Linux machines. When attempting to discover and communicate with unknown machines, the console will first try SMB; if that fails, SSH is used. SSH provides secure communication between two endpoints. If an endpoint responds to the SSH request, an attempt is made to authenticate to the endpoint using credentials that are provided by the console.

Although SSH provides encrypted transport, any data sent using SSH, including user names and passwords, are visible and available to the SSH server. To ensure the security of data that is sent using an SSH connection, many organizations require that the client validate the authenticity of the remote system it is connecting to before sending any data. Security Controls does not currently support the use of SSH server authentication. This means you must decide whether to block the SSH connections from happening or allow the console to skip the SSH server authentication process.

How to Decide

Your decision on how to configure the **SSH server connection** setting boils down to whether the machines you are configuring are trusted machines in your network. The setting appears in two places within the Security Controls user interface, and the scope and impact of the setting is different for each area.

- In a machine group on the **Machine Name**, **Domain Name**, **IP Address/Range** and **Organizational Unit** tabs
- When performing discovery operations on machines defined in a machine group, you often have no idea what type of machine might be listening on the other end. It is possible that you might know that the machines defined by a certain IP range in your network are trusted Linux machines. For those machines, you might choose to allow the SSH connection by either skipping the authentication process or requiring each machine to undergo a validation step. When adding domains or organizational units to a machine group, however, it is very likely that you are not as certain about the operating system type of the machines or about their trustworthiness. In this case, you should choose to block the SSH connections, The downside, of course, is that you won't be able to manage your Linux machines in the normal manner, but **there are workarounds available**.
  On the **Machine Properties** dialog
  Unlike machines in a machine group that have yet to be discovered, machines in **Machine View** or Scan View are known to the console. The amount of information about a machine, however, may be limited if the discovery operation was performed while SSH connections were blocked. There may be clues about a machine, such as an address that you recognize as a static IP, that enable you to determine if a machine is a trusted machine. In this situation, you might use the **Machine Properties** dialog to change the **SSH server connection** setting from **Block** to either **Validate Against Known Hosts File** or **Skip Server Authentication**. This will enable you to perform a complete **power status scan** and then a **push installation of an agent** to the Linux machine.

Summary of Your SSH Server Connection Options

- **Block:** Choose this if:
  - You don't have any Linux machines in your environment

- You have Linux machines, but you are not certain that all SSH servers in your network are trusted and safe
- You are uncertain about the OS type of machines that will be discovered

You will not be able to perform a power status scan of the machines or perform a push installation of an agent to the machines. Choosing **Block** has no effect on listening agent commands or on results being returned to the console.
Validate Against Known Hosts File: Choose this if you want to use the `known_hosts` file to validate each target machine before allowing an SSH connection. The `known_hosts` file resides on the console machine and is unique to the user who is currently logged on to the console. The validation process performed by Security Controls is as follows:

> An SSH client must be installed on the Security Controls console in order to use this process. You may need to manually download and install an SSH client if your console is on an older version of Windows or Windows Server.

- Look for the `known_hosts` file on the console machine.
- The file will be located in the `C:\Users\<username>\.ssh` path. If the file does not exist, the SSH connection will be blocked.

  > You can create the `known_hosts` file by opening a PowerShell prompt on the Security Controls console and manually initiating an SSH connection to the target machine. During the process, the target machine's host key is acknowledged and then added to a newly created `known_hosts` file.

  If the `known_hosts` file exists and an entry for the target machine is contained in the file, then query the target machine for its SSH key. Security Controls will compare that key with the one in the `known_hosts` file. If the two keys match, then allow the connection.
  The key known by Security Controls is originally created using the user name and password credential that is specified for the machine.

Skip Server Authentication: Choose this only if you are certain that the machines are trusted and safe Linux machines.

Work-Around Solutions if You Choose Blocked

Power status scans

If a Linux machine is in a machine group, the machine will be discovered, but no operating system information will be detected by the scan. If you determine that the machine is a known device in your network and is known to be safe, you can go to the machine Properties dialog to change the **SSH server connection** setting to either **Validate Against Known Hosts File** or **Skip Server Authentication**. Future scans of the machine will complete as expected and will provide full details about the machine.

Installing a Linux Agent

You will not be able to perform a push installation of an agent to a Linux machine if the SSH connection to that machine is blocked. You can, however, manually install an agent on the machine. After that, the agent will function normally, as regular communication with the console does not use an SSH connection.

Related Topics

- Managing Individual Machine Properties
- Managing Multiple Machine Properties

415. Starting Security Controls

> In order to access the full capabilities of Security Controls, you must run under a Windows account with administrator privileges.

You can start Security Controls two ways:

- Tap or double-click the Security Controls icon on your desktop
- Select **Start >** Ivanti Security Controls **>** Ivanti Security Controls

After starting the program the home page is displayed. See **Navigating the Interface** for detailed information.

416. Supplying Scan Credentials for Target Machines

> Browse credentials are slightly different from the scan credentials described in this section. Browse credentials are used by servers, domains, and organizational units to enumerate machines but do not actually authenticate to the individual machines. See **Adding Virtual Machines Hosted by a Server** and **Machine Group Dialog: Bottom Section** for information on specifying browse credentials.
>
> In addition, Security Controls also uses a **scheduler credential** for all tasks scheduled to be run on the console. You set this credential from the **Scheduled Console Tasks** dialog.

This section provides information on how to define new scan credentials and how to assign the credentials to target machines. Credentials consist of a user name and password pair used to authenticate the program to specified target machines. One credential can be associated with any number of operations or entities. The credentials are stored with strong encryption techniques and are not available to anyone except the user who provided them.

The scan credentials you supply will be used to access remote machines, perform any scans, and push any necessary files. The supplied credentials will NOT be used to:

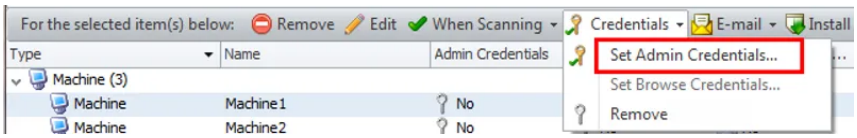
- Authenticate to the local (console) machine
- Rather, the program uses the credentials of the currently logged on user to authenticate to resources on the local machine. Therefore, in order to perform tasks on the local machine, make sure you log on using an account that has administrator and local machine access rights.
  Perform a patch deployment
  The machine credentials that you supply are used to provide access to the remote machine and to push the necessary patch deployment files. The actual deployment, however, will be run under the remote machine's Local System account.

You use a machine group to initially assign scan credentials to target machines. You can assign credentials to individual machines, to all machines in a machine group, or both. After a machine has been scanned and is contained in Security Controls's database of managed machines, you can use the **Machine Properties dialog** to assign different credentials if desired.

> IMPORTANT! If there are two or more administrators using Security Controls, each administrator should provide their own machine credentials. For details see **Potential Issues When Using Multiple Admins**.

ASSIGNING CREDENTIALS TO INDIVIDUAL MACHINES IN A MACHINE GROUP

To assign credentials to one or more machines in a machine group, in the bottom pane select the machines and then select **Credentials > Set Admin Credentials**.



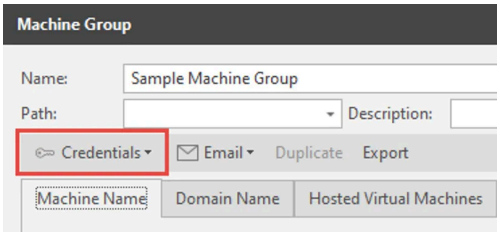
On the **Assign Credentials** dialog, select from the list of available credentials or click **New** to define new credentials.



When credentials are applied to the selected machines, the name of the assigned credential is displayed next to the icon.

ASSIGNING CREDENTIALS TO ALL MACHINES IN A GROUP

To assign credentials to all machines in a machine group, in the top pane select **Credentials > Set Credentials**.



On the **Assign Credentials** dialog, select from the list of available credentials or click **New** to define new credentials.

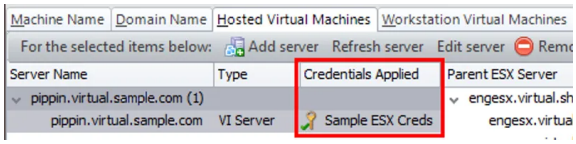


When credentials are assigned, the button name will change to the name of the assigned credential.

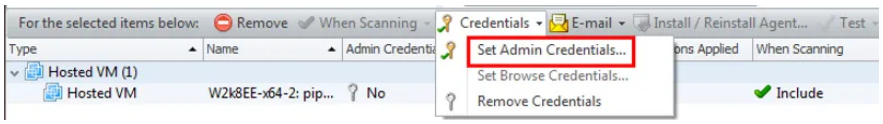
ASSIGNING CREDENTIALS TO VIRTUAL MACHINES

There are several different tabs that can be used to add virtual machines to a machine group. The credentials that will be used to scan and/or deploy patches to these machines depends on how the machines are defined to the group and on the current power state of each machine.

- **Hosted Virtual Machines tab**: Used to add virtual machines that are hosted by a server. The credentials used to scan each machine depends on the current power state of the machine.
  - A hosted virtual machine that is *offline* at the time of a scan will be accessed using the **server's browse credentials**. Any individual credentials supplied for the machine are ignored.



A hosted virtual machine that is *online* at the time of a scan will be accessed using scan credentials for that machine. See *Assigning Credentials to Individual Machines in a Machine Group*, above.



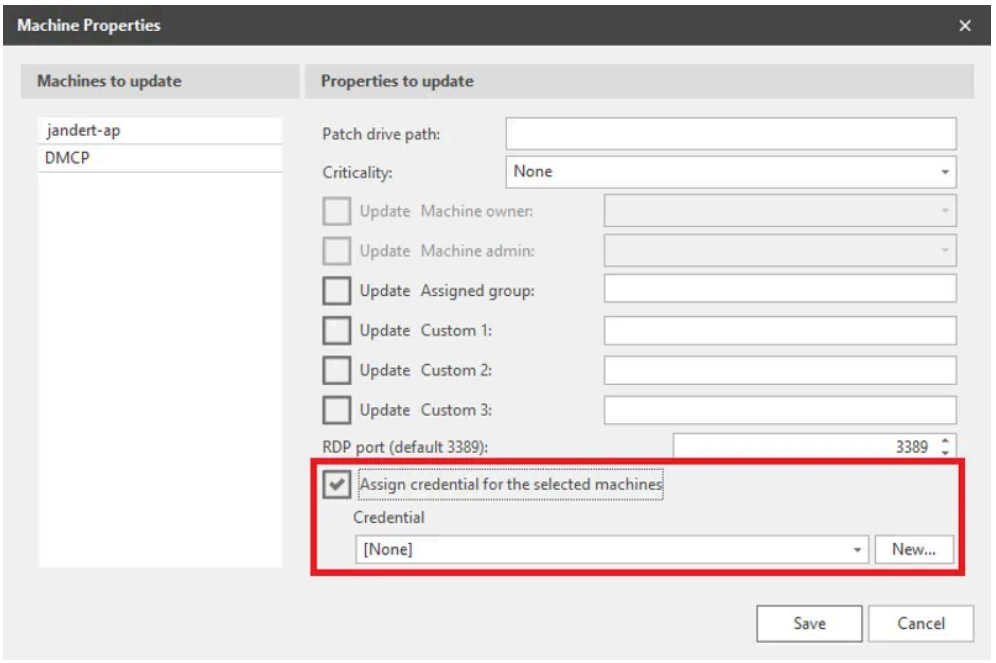
Workstation Virtual Machines tab: Used to add *offline* virtual machines that reside on individual workstations. You should assign individual machine credentials for each virtual machine defined using this tab. If appropriate, credentials can also be assigned at the machine group level. The credentials are used during the mounting process and provide permission for Security Controls to access the virtual machine files on the workstation. See *Assigning Credentials to Individual Machines in a Machine Group*, above.

- **Machine Name** tab, **Domain Name** tab, or **IP Address/Range** tab: Used to add virtual machines that reside on individual workstations and that are *online* at the time of a scan. See *Assigning Credentials to Individual Machines in a Machine Group*, above.

ASSIGNING NEW CREDENTIALS TO MACHINES AFTER THEY HAVE BEEN SCANNED

After one or more machines have been scanned and are contained in Security Controls's database of managed machines, you can use the **Machine Properties dialog** to assign different credentials or to remove credentials.

There may be several reasons for providing different credentials to machines after a scan has been performed. If you have multiple administrators in your organization and each is responsible for a different domain, they will need to set their own credentials before performing an action. Or, your organization's policy may be to separate scan (assessment) duties from deployment duties, in which case different credentials are probably required.



See also:

Credential Precedence for Physical Machines and Online VMs

Credential Precedence for Offline Hosted VMs

Deploying Patches to Virtual Machines

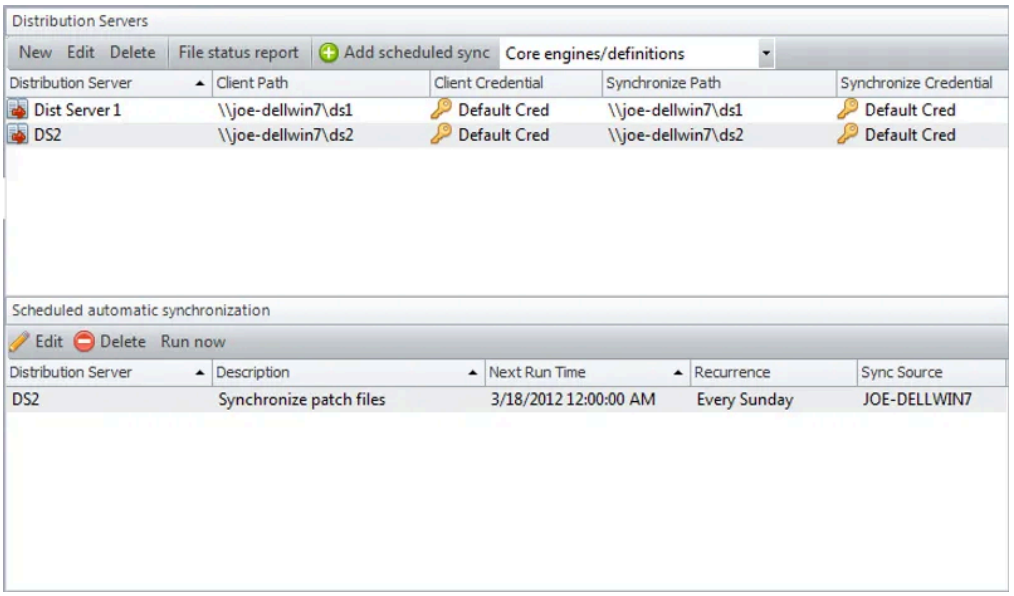
417. Synchronizing Distribution Servers

When you synchronize a distribution server it means you are updating the server with the latest patches and/or engines and data definition files contained on the console. To synchronize your distribution servers, select **Tools > Options** and then click the **Distribution Servers** tab.

You can automatically synchronize distribution servers on a periodic basis. You can also manually synchronize the distribution servers directly. This section will cover both options.

Make sure the console contains the necessary files before attempting to synchronize all your distribution servers. For information on downloading patches to the patch download directory, see **Downloading Patches**. To download the latest engines to the console, select **Help > Refresh files**.

> Another option for automatically synchronizing your distribution servers is to use Distributed File System (DFS) Replication. DFS Replication is available beginning with Windows Server 2003 R2 and requires the use of Active Directory.



Creating a Status Report

If you want to create a report that shows which of the patches contained in the **download directory** are missing or are out-of-date on the distribution servers, select the desired distribution server(s) and then click **File Status Report**. The report will list which downloaded patches are not contained on the selected distribution servers or are out of date. The report does not report if engines and data files are missing or out of date.

Automatically Synchronizing Distribution Servers

To configure the program to automatically synchronize engines, definitions, and/or patches with a distribution server:

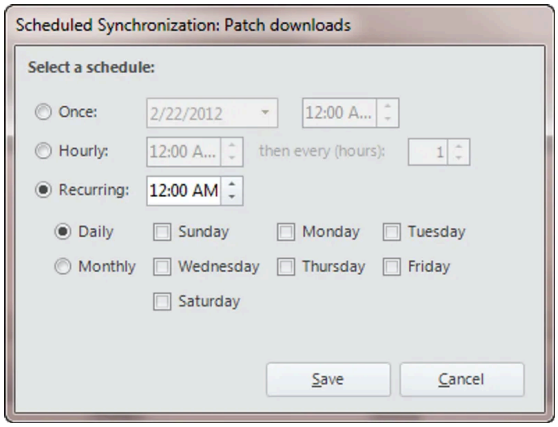
1. In the **Add scheduled sync** box in the top pane, select the component you want to synchronize.
   The components that you can choose to synchronize are:
   - **Core engines/definitions:** The latest versions of the engine components and all data definition files will be copied to the distribution server. If you have more than one console sharing a database, only one console can synchronize core engines/definitions to a given distribution server.

- **Patch downloads:** All patches contained in the console's patch download directory will be copied to the distribution server.
- **All engines, definitions, and patch downloads**: All relevant components are synchronized.

In the top pane, select which distribution server you want to synchronize with the console.

> If the **Add scheduled sync** button becomes unavailable after you select a specific distribution server, it probably means the server is being used as the **download source for patches and product levels**.

Click **Add scheduled sync**.
The **Scheduled Synchronization** dialog appears.



Specify when you want the synchronization to occur.
The **Add delay (days)** box (available if you synchronize on a monthly basis) allows you to delay the synchronization by up to 31 days. For example, you might use this to schedule a monthly synchronization that is always performed four days after Patch Tuesday. You do this by specifying **The Second Tuesday** and then using the **Add delay (days)** option to delay the operation by four days.

5. Click **Save**.

The new scheduled synchronization entry appears in the **Scheduled automatic synchronization** pane. At the scheduled time, the appropriate files will be copied to your distribution server. If the synchronization time happens to coincide with a download of new files to the console, the synchronization process is queued and is performed when the download is complete.

The **Scheduled automatic synchronization** pane will show scheduled synchronizations for all consoles that share the database. If you select a schedule created by a different console, you can delete the schedule but you cannot edit it or run it immediately. This allows you to move the synchronization process to the current console by deleting the remote schedule and then creating a new local schedule. It also allows you to delete schedules for consoles that no longer exist.

> If you did not specify **credentials for the console to use** when authenticating to the distribution server, in order for automatic synchronization to work the console machine's SYSTEM account must have read and write access to the distribution server folder. See **Configuring System Account Permissions** for details.

Manually Synchronizing Selected Distribution Servers

You have the option to manually synchronize a distribution server with the console. This initiates a synchronization right now so you don't have to wait for the next scheduled interval. A background task will be created to perform the synchronization. You can continue using the rest of the program while the synchronization process is performed.

To perform a manual synchronization:

1. If you are manually synchronizing the engine components and data files, make sure you have the latest files on the console by selecting **Help > Refresh files**.
   This will download the latest files from the location specified on the **Tools > Options > Downloads** page and store them in the console's default data directory:
2. `C:\ProgramData\Ivanti\Security Controls\Console\DataFiles`
   If you are manually synchronizing patches, make sure the console's patch download directory contains all the patches you want on your distribution server(s). See **Downloading Patches** for details.
   The patches are contained in the default patches directory:
3. `C:\ProgramData` `\Ivanti\Security Controls\Console\Patches`
   In the **Schedule automatic synchronization** pane, select one or more scheduled synchronization entries.
4. Click **Run now**.

This will immediately copy all appropriate files from the console to the specified distribution server(s). You can use **Event History** to track the progress of the synchronization task.

418. Target Type

Security Controls simplifies many IT functions, including patch management, asset management and script execution. The machines that are being managed are referred to as the “target machines,” or “managed machines.”

The ITScripts feature supports four different script execution environments. In the Script Catalog Manager, these are distinguished by their target type.

Console

Console scripts run on the console and do not target a group of managed machines. In the Script Catalog Manager, these have a target type of “Console” since the default target of script commands is the console (the local machine). These scripts are executed by selecting **Tools > Run console ITScripts**.

Any

These scripts target a group of managed machines without using PowerShell remoting. In the Script Catalog Manager, these have a target type of “Any” since the target machines generally do not require any special configuration. These scripts are executed from the home screen, Machine View, or Scan View. The commands in this type of script typically specify the target computer and credentials by using the **ComputerName** and **Credential** parameters on the command.

WinRM Remoting

These scripts target a group of managed machines using PowerShell remoting. In the Script Catalog Manager, these have a target type of “WinRM Remoting” and require that PowerShell remoting is configured on target machines. These scripts are executed from the home screen, Machine View, or Scan View. Because these scripts are executed on the target machine, the target of commands is typically the local machine, and therefore the **ComputerName** and **Credential** arguments do not need to be specified on the command.

ESXi Hypervisor

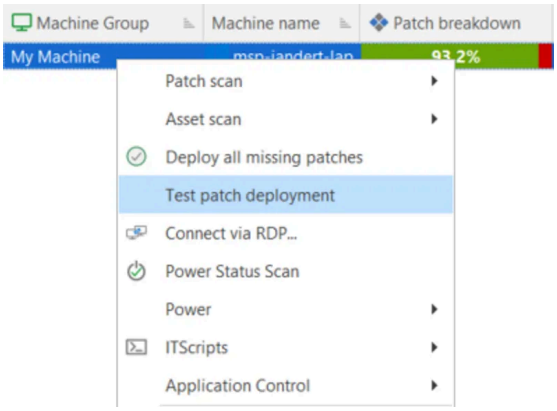
The script runs against an ESXi Server or a vCenter Server. This type of script may use VMware vSphere PowerCLI. VMware vSphere PowerCLI lets you automate all aspects of vSphere management, including network, storage, VM, guest OS and more. Scripts of this type only run against machine groups that contain ESXi servers. If the machine group contains any other machines, they will be ignored when this script executes.

419. Testing the Deployment

Security Controls includes the ability to perform a test deployment to one or more machines. This is especially useful if you intend to schedule a patch deployment for a later time. Testing the deployment allows you to correct any potential problems in a deployment and make it less likely that a deployment will fail.

How to Perform a Test Deployment

You perform a test deployment from **Machine View** or **Scan View**. Simply right-click the machine, machine group, or domain you want to test and then select **Test patch deployment**.



The test is conducted using a non-security patch named TEST-PATCH. The patch does not modify the state of the target machine. The test will exercise all of the actions in the deployment process, including:

- Testing for available deployment seats
- Verifying port requirements and the availability of a secure connection
- Downloading and copying files to the target machine
- Verifying patch signatures
- Scheduling the patch task
- Executing the deployment package
- Delivering status messages

Test deployment results are reported in the **Operations Monitor**. Status messages are provided for each major step in the process.

A test deploy may fail for a number of different reasons. For example, if the workstation or scheduling services are not started in a particular machine, Security Controls cannot deploy patches to it and a test deploy will return a failing result. If a test does fail you can click the available link for information on why the test failed.

420. Tips and Tricks

Here are a few tips and tricks that will improve your experience with the API.

- When typing PowerShell commands, use the Tab button to auto-complete the command.
- Use pipelining within your commands to string together a series of actions.
- If you want to view the output when performing a patch scan, be sure to use the **Watch-PatchScan** parameter.
- Example:

```Bash
Start-PatchScan –MachineGroups “Sample Group” | Watch-PatchScan
```

You can assign the result of any command to a variable and interact with that variable later in the same PowerShell session.

- Examples:

```Bash
$credReference = Get-STCredential
```

```Bash
$credReference | Where-Object
```

```Bash
{ $_.UserName.Contains(“foo”) }
```

```Bash
$myScan = Start-PatchScan –MachineGroups “My Machine”
```

```Bash
Wait-PatchScan –Uid ($myScan.Uid)
```

If you want to perform a patch deployment against the results of a particular patch scan, store the patch scan in a variable and pipe it to the deployment operation.

- Example:

```bash
$myScan = Start-PatchScan –MachineGroups “Sample Group”;
```

```bash
$myScan | Watch-PatchScan
```

```bash
Start-PatchDeploy –ScanUid ($MyScan.Uid) –TemplateName “Sample Deploy Template”
```

If you are scripting a patch scan followed by a patch deployment, be sure to use the **Wait-PatchScan** parameter to allow time for the scan to complete before the deployment is initiated.

- Example:

```bash
$MyScan = Start-PatchScan –MachineGroups “Sample Group” | Wait-PatchScan
```

```bash
Start-PatchDeploy –ScanUid ($MyScan.Uid) –TemplateName “Sample Deploy Template”
```

Be sure to load any additional modules that might be needed.

- Example: When interacting with a SQL cluster you might load the following modules:
  - Import-Module ServerManager
  - Add-WindowsFeature RSAT-Clustering
  - Import-Module FailoverClusters

To minimize downtime, you can use the `Invoke-DownloadMissingPatches` command before deploying.
This would enable you to perform a scan one day and then use the `Get-PatchScan` command to deploy from that scan on a different day.

421. Troubleshooting Agent Installation Errors

If an error occurs during an agent installation, the error messages displayed in the **Operations Monitor** are the best place to begin the troubleshooting process.

- **Failure copying files:** This normally indicates a problem with the credentials being used to connect to the agent machine. The default credentials or "last used" credentials may not be the correct credentials to use for a particular machine.
- **Registration failure:** This normally indicates that the agent cannot establish a connection with the console. There may be a firewall issue, there may be **ports** that are unopened, there may be a DNS issue, or the agent service may not be active on the agent machine.
- **Check-in failure:** This normally indicates a timeout or network issue, and the agent will fail to download all necessary files.

You can also view the Security Controls Agent installation log on the agent machine. The log file is located in the `C:\WINDOWS\Temp\<GUID>` directory. The installation log will show any error messages that were generated during the agent installation process.

Troubleshooting Linux Agent Installation Issues

Here's a quick checklist of things to try when troubleshooting agent installation issues on a Linux machine.

- Are you able to test existence or perform a power status scan from the machine group?
- Try installing the agent from a machine group using specific credentials for the client.
- Set the **logging level** to **All**, reproduce the issue and look in the logs for an error.
- The logs are located here: `C:\ProgramData\LANDESK\Shavlik Protect\Logs\`. Do a search for the letter e with a space on each side (e).
  Use NotePad++ when reviewing the logs.
- This allows you to open all logs and search them at the same time.
  Verify DNS from and to Red Hat Enterprise Linux.
  In the logs, determine if machine name or FQDN is being used and then make sure that ping and nslookup are working.

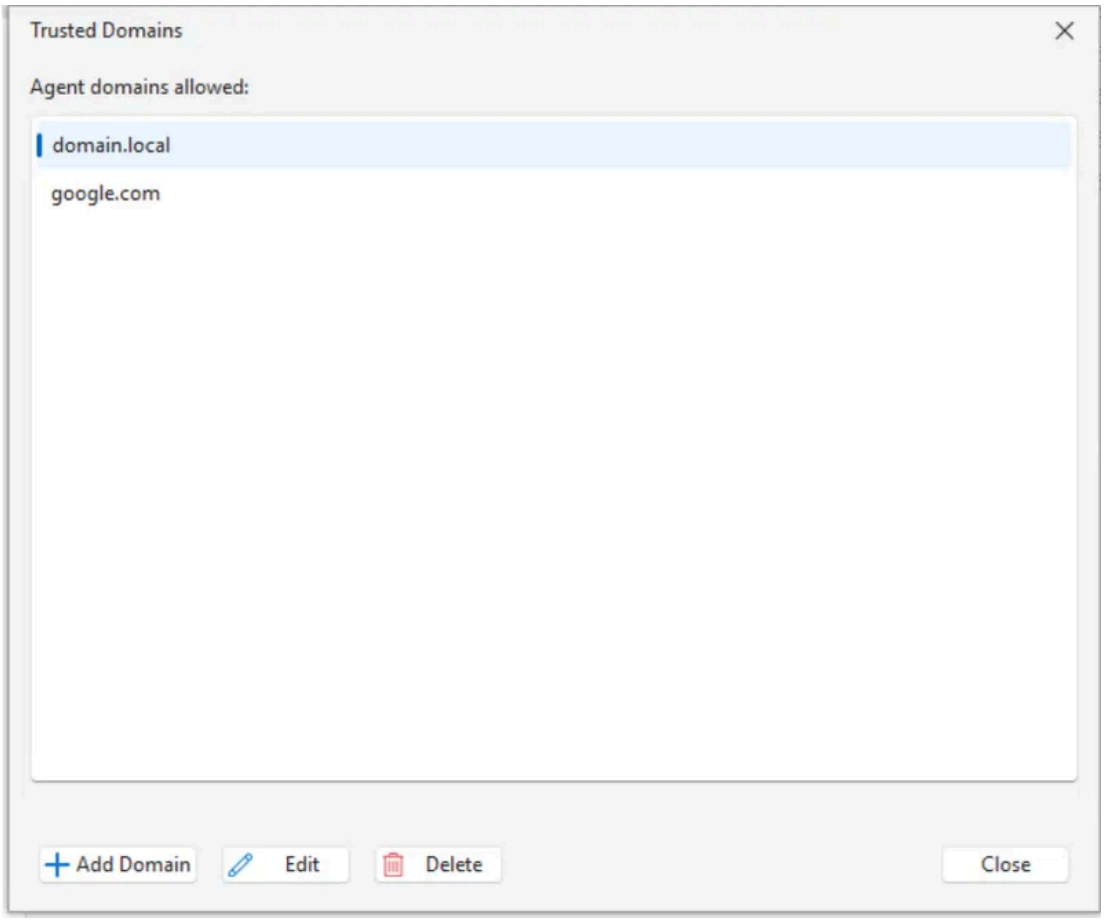
422. Trusted Domains

You can add, edit, or delete domain suffixes used by Security Controls to validate an agent's domain suffix. This feature ensures that only agents from the specified domains are permitted to communicate with the Security Controls Console.

This feature helps to identify and block the access to domains that are not permitted.

To add or modify Trusted Domains:

1. Select **Tools > Trusted Domain**.
2. A dialog displays that allows to add the list of domains. Domains must be added as separate lines.



Add a list of allowed domains, edit a domain from the list, or delete any domains that are not allowed or trusted anymore from the list. You can use wildcard characters (*) to specify multiple domain levels. Each (*) represent a sub domain level. For example, *.example.com allows one subdomain level or *.*.example.net allows two subdomain levels.

> Domains do not match if they contain more subdomain levels than the number of wildcards specified. Domain values do not have the character limit.

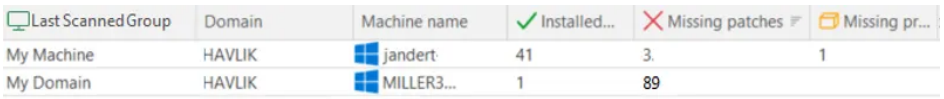
Only domain suffixes listed in the Trusted Domains dialog are considered trusted. Agent registration and certificate requests from devices with untrusted domains will be rejected. These rejected registrations are logged in the Event History view under **Agent Registration** with a **Failure** status.

If a domain suffix is deleted, existing agents associated with that domain suffix continues to function. Those agents continue to function and renew their certificates even after expiration. If an agent is using a domain suffix at the time of deletion, a confirmation prompt appears.

423. Typical Uses of Machine View

Machine View is extremely powerful and flexible, and there are many, many uses for it. Here are just a few examples.

- "Do I have any machines that are missing a large number of patches?"
- To see if your network contains one or more machines that are "bad eggs," click the **Missing Patches** column header and sort the table in descending order. The machines that are missing the most patches are shown at the top of the table. The following figure shows a very simple example containing two scanned machines. One of the machines needs a little work (it is missing 3 patches), but the other machine needs immediate attention as it is missing 89 patches. You can immediately rectify the situation by simply right-clicking the machine and selecting **Deploy all missing patches**.



Last Scanned Group	Domain	Machine name	Installed...	Missing patches	Missing pr...
My Machine	HAVLIK	jandert	41	3	1
My Domain	HAVLIK	MILLER3...	1	89	

"Can I compare all the machines within a machine group?"

- Yes. Simply click and drag the **Last Scanned Group** column header to the first column. This will order the machines by the name of the machine group that was used during the most recent scan.
  "A recently released Windows patch has been deemed mandatory by my organization. How do I see which machines have the patch installed and which machines are missing the patch?"
- You can do this very easily. In the top pane select the desired domain or machine group, in the middle pane select the patch, and then in the bottom pane use the **Affected Machines** tab.
  "How do I know which machines have Security Controls Agent installed?"
  In the top pane, click the **Agent State** column heading. This will sort the table, grouping together all machines that have Security Controls Agent installed and placing that group at the top of the table. Click the icon a second time to move to the top of the table the group of machines without Security Controls Agent installed. For more information, see **Determining Which Machines Have Agents**.

424. What is an Unattended Console Configuration?

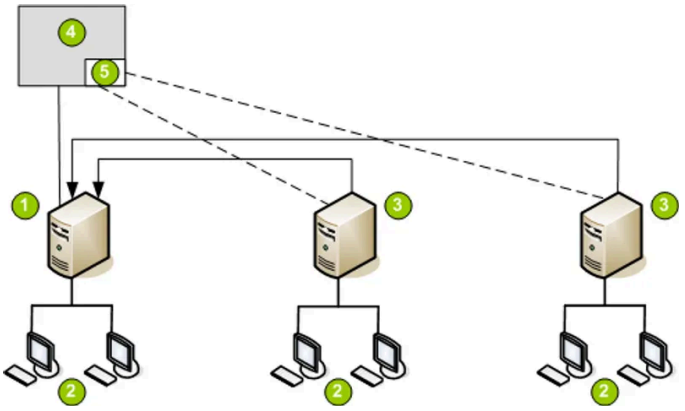
An unattended console is a console you set up once. After that the console automatically updates its own files and manages its machines without human assistance.

Here's how it works: The unattended console is configured to automatically perform periodic scans and to automatically deploy any patches it detects as missing on its target machines. The console will contain a patch scan template that is defined to look for a particular set of patches. The set of patches is contained in a patch list that resides on a distribution server.

Now, when new patches are released by a vendor (for example, the monthly patches released by Microsoft Corporation), an administrator simply updates the patch list on the distribution server. When the unattended console performs its next scheduled scan it will automatically reference the updated list and will patch its target machines, all without human intervention.

Of course, the unattended consoles can also be configured to use the data rollup feature so that you can track what is happening on each of your unattended consoles from one central site.

The following figure illustrates an unattended console configuration.



1 - Rollup console

2 - Managed machines

3 - Unattended console

4 - Distribution server

5 - Patch list

For more information, see **Implementing an Unattended Console Configuration**.

425. Understanding Patch Count Data

The values for the **Installed Patches** and **Missing Patches** columns in the top pane may not always match the values shown in the middle pane. This is because the top pane counts every patch on every machine, while the middle pane counts only unique patches and ignores duplicates. You can use the **Affected Machines tab** in the bottom pane to determine if a particular patch is missing on multiple machines.

426. Understanding RDP

The Microsoft Remote Desktop Protocol (RDP) provides the ability to remotely manage Windows-based machines over a network connection. RDP capabilities are supported in Security Controls, enabling you to use stored machine credentials to quickly connect the Security Controls console to a target machine. With Remote Desktop you can access the target machine's programs, files, and resources as if you were physically sitting in front of the machine. For a complete list of the features of Remote Desktop, please visit any number of sites on the Web.

For information on using the Remote Desktop feature, see the following topics:

- **RDP Requirements**
- **How to Initiate a Remote Desktop Connection**

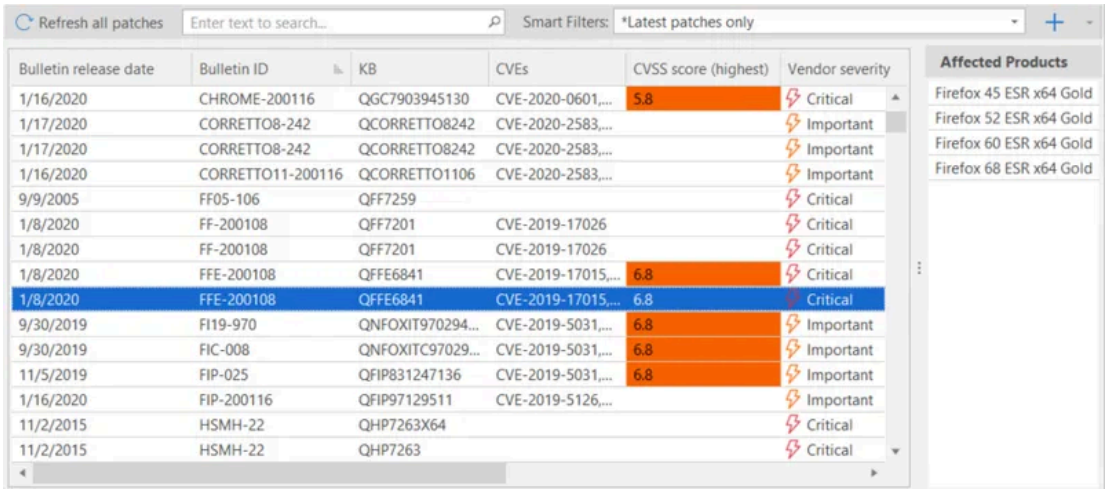
427. Understanding the Top Pane

The top pane in Patch View displays a table containing detailed information about each patch in the XML patch catalog. Click on a column heading to sort the table by that information. You can also specify what information is presented by right-clicking the table heading and selecting or clearing the available items.

If you select a patch, information about that patch is displayed on the **Patch Information** tab of the bottom pane. Products affected by the selected patch are displayed in the **Affected Products** table that is located on the right side of the top pane.

No information is displayed on the **Patch Information** tab if you select a product level (represented by SP1, SP2, etc. in the **KB** column). In addition, most products contain a unique entry whose **Product Level Name** and **KB** are both **Gold**. These entries represent the "out of the box" base installation of a product, they contain no downloaded files, and are therefore neither a patch nor a product level.

> By default, product levels are not displayed in Patch View. To view product levels, select **Tools > Options** and on the Display tab enable the **Show product levels in View > Patches** check box.



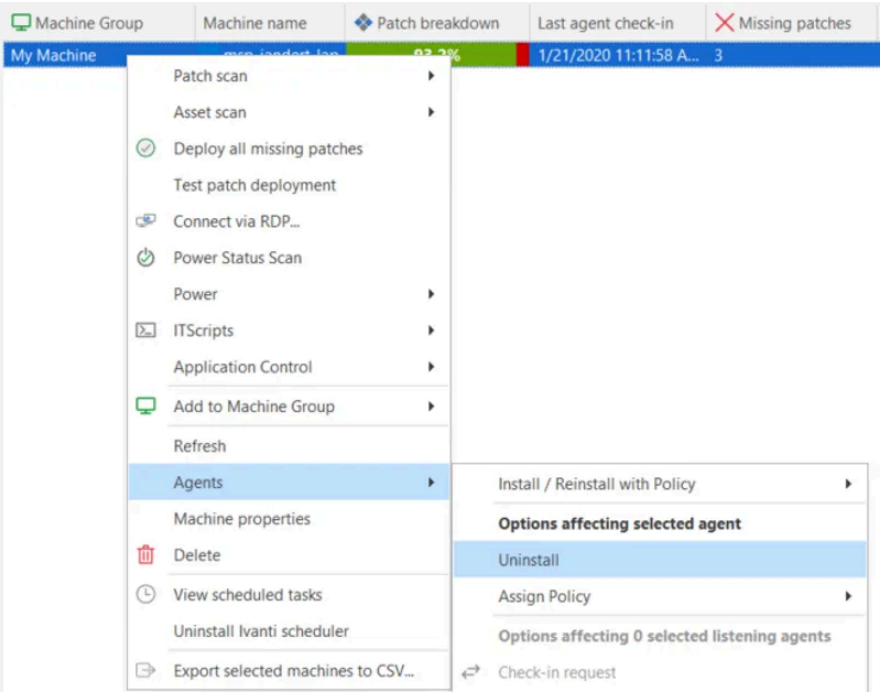
428. Uninstalling Security Controls Agent

Windows Agents

Using Machine View to Uninstall Agents

You can use the console to uninstall agents from both connected and disconnected machines. The uninstall will occur immediately for agent machines that are online and able to communicate with the console. For disconnected machines, the uninstall will occur the next time the agent checks in with the console or the cloud and sees it is no longer assigned to a policy.

To initiate the uninstall, from within Machine View, right-click the selected machines and select **Agents > Uninstall**.



Manually Uninstalling Security Controls Agent

To manually uninstall Security Controls Agent from a target machine:

1. Select **Start > Control Panel > Programs and Features**.
2. If the agent policy contains a patch task, locate the program named Security Controls **Patch Engine**, select it, and then click **Remove**.
3. If the agent policy contains an asset task, locate the program named Security Controls **Asset Engine**, select it, and then click **Remove**.
4. Locate the program named Security Controls Agent, select it, and then click **Remove**.

The disadvantage of using this method is that the uninstall will not be reported back to the console.

Linux Agents

1. Log on as root.
2. Open a terminal.
3. Type the remove command.
4. `# yum remove ISecAgent`

   At the **Is this ok [y/N]** prompt, type **y**.

429. Uninstalling Patches

Security Controls provides the ability to uninstall selected patches. Not all patches can be uninstalled; only patches identified by the rollback icon can be uninstalled. Uninstalling or "rolling back" patches restores a machine to its original state before the patch was deployed. Patches must be rolled back in the reverse order in which they were installed.

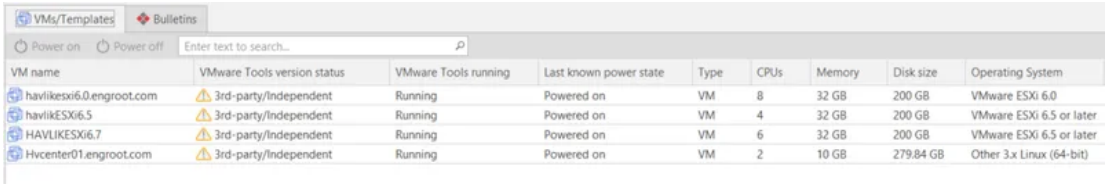
You can uninstall one or more patches from **Scan View**, **Machine View**, or Patch View.

1. In the top pane, select the desired machine(s).
2. In the middle pane, select the desired patch(es).
3. Right-click the patch(es) and then select **Uninstall Selected**.

430. Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates

The **VMs/Templates** tab displays summary information about the virtual machines and virtual machine templates that are contained on the selected ESXi hypervisor.

You can customize the way information is displayed within this pane. See **Customizing the Column Headers** for information.



Field	Description
Power on	See **Performing Actions on Virtual Machines**.
Power off	See **Performing Actions on Virtual Machines**.
Search	Enables you to search for virtual machines contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those virtual machines that match the search criteria are displayed; all other virtual machines are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the **VM Name** column. • All partial matches are displayed. For example, if you search for virtual machines named *Test*, any virtual machine with "test" in its name will be considered a match (e.g. TestVM1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
VM Name	The virtual machine name.
VMware Tools Version Status	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. This column identifies the version of VMware Tools currently in use on the virtual machine.
VMware Tools Running Status	Indicates if VMware Tools is running on the virtual machine.
Last Known Power State	The last known state of the virtual machine (Powered on, Powered off, or Suspended).
Type	Indicates if the device is a virtual machine (VM) or a virtual machine template.
CPUs	The number of Central Processing Unit (CPUs) available to the virtual machine.
Memory	The amount of memory (MB) allocated to the virtual machine.
Disk Size	The amount of disk space (GB) allocated to the virtual machine.
Operating System	The operating system being used on the virtual machine.
IP Address	The IP address of the virtual machine.
Hostname	The name of the machine on the network that is hosting the virtual machine.

431. Unsupported PowerShell Commands

The Security Controls scripting engine differs somewhat from running scripts in a PowerShell command window or in the PowerShell_ISE application. Each PowerShell application is a different “host” environment and supports different host options. The Security Controls script engine does not currently implement the following host commands. Attempting to use these commands in your scripts will result in an error.

- Out-Host
- Read-Host
- Write-Host
- Out-GridView

Use Out-Default, Out-String, or Write-Output in place of Out-Host and Write-Host. Since Security Controls scripts run in a background service, interactive scripts are not supported. Therefore, there is no substitute for Read-Host or Out-GridView.

432. Upgrade Procedure

Overview

This section describes how to upgrade to Security Controls 2026.1 from Security Controls 2022.2 or later.

- If you are taking this opportunity to move the console to a new machine and you want to perform the migration using the Migration Tool, see the **Migration Tool User's Guide** before performing the upgrade.
- If you are taking this opportunity to also upgrade your operating system, you should do so on a new server rather than attempt an in-place upgrade of the operating system.

Before upgrading, read the appropriate sections of **What's New?** so you are aware of how the upgrade will affect your system. You also may want to make a note of all your current custom user settings as some are not preserved during the upgrade.

> Be aware that after the upgrade of the console is complete, any agents that are installed on your target machines will be automatically upgraded the next time they check in with the console.

Before You Upgrade

1. Free up unused space in the database that is used to store scan results and patch deployment results.
   You can do this in SQL Server Management Studio by right-clicking the Protect database and selecting **Tasks > Shrink > Database**.
2. Create a backup of your current database using SQL Server Management Studio.
   The database contains results from program operations and it also contains configuration information. Backing up your database is an important step.
3. If your database is in a SQL Server high availability group, it must be removed prior to upgrading.
   The upgrade process will fail if the database is in a high availability group.
4. If your current console resides on a virtual machine, you should take a snapshot prior to the upgrade.
   This is simply a precaution in the event there is a problem during the upgrade and you want to revert to your original environment.

Performing the Upgrade

> If your console machine resides in a disconnected network, there are a few extra steps you must take in order to (a) download and install any missing prerequisite software and (b) download the product core files. For complete instructions, see a **Performing a New Installation**.

1. Close all programs running on the console machine, including Security Controls.
2. Download the Ivanti Security Controls 2026.3 executable file to your console machine using the following link:
3. **https://forums.ivanti.com/s/article/Ivanti-Security-Controls-Download**
   Begin the installation process using one of the following methods:
   - Double-click the file named `IvantiSecurityControls.exe`

-OR-

   - Type the file name at a command prompt. Doing so enables you to use one or more command-line options. You should consider this method if you are upgrading a very large database. The DBCOMMANDTIMEOUT option is used to specify the

SQL command timeout value during installation. The default value is 15 minutes per GB. The minimum timeout value is the greater of 15 minutes per GB or 1800 seconds (30 minutes). You should override the default value only if you expect the upgrade to take an exceptionally long time due to constrained resources.

For example, if you have a 4 GB database, to double the default timeout value from 3600 seconds (60 minutes) to 7200 seconds (120 minutes) you would type the following command:

```bash
IvantiSecurityControls /wi:"DBCOMMANDTIMEOUT=7200"
```

> If you receive a prompt indicating that a restart is required, click **OK** and the installation process will automatically resume after the restart.

Respond to the dialog that asks if you want to continue with the upgrade.

If you click **Yes** and your console machine is missing one or more prerequisites, a dialog appears listing the prerequisites. If you are not missing any prerequisites, skip the following step and proceed with the **Welcome** dialog.



Click Install to install any missing prerequisites.

The Setup Wizard may need to perform a reboot during this portion of the installation process. If a reboot is required, when the machine is restarted the Setup dialog will reappear. Simply click **Install** again to proceed with the upgrade.

The **Welcome** dialog is displayed.

6. Read the information on the **Welcome** dialog and then click **Next**.
   The license agreement is displayed. You must accept the terms of the license agreement in order to install the program.
7. Enable the **I accept the terms in the License Agreement** check box and then click **Next**.
   The **Destination Folder** dialog is displayed.
8. If you want to change the default location, click the browse button and choose a new location.
9. Click **Next**.
   The **Ready to Install** dialog is displayed.
10. To begin the installation, click **Install**.
    Your existing database is automatically upgraded.

11. On the **Completed the Ivanti Security Controls Setup Wizard** dialog, enable the **Launch Ivanti Security Controls** 2026.3 check box and then click **Finish**.



The core engines and definition files are updated and Security Controls is started.

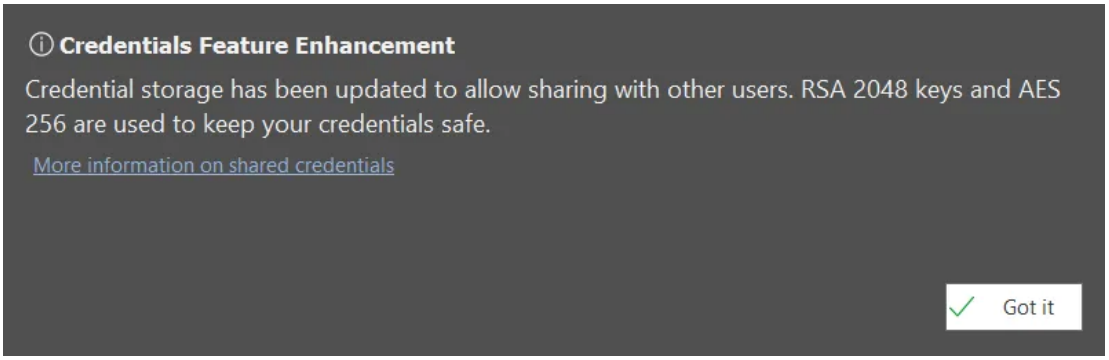
After Upgrading

If you are upgrading from Security Controls 2024.1 or earlier and you use distribution servers, you MUST update the Linux engine installer on all distribution servers before creating or updating policies to include Linux patch groups. If this is not done, and a new policy is used with an old engine, scans will not work the old engine will interpret this policy to deploy all patches and not just the patches that were approved in the patch group.

If you are upgrading from Security Controls 2023.4.1 or earlier, we recommend you review the database connection encryption setting using the Database Setup Tool (see **Set Advanced options - database connection encryption**). With version 2024.1, new options for configuring the encryption of the connection between the console and SQL Server were added. The new options provide more security, but may need further configuration. The upgrade does not change this setting, leaving it at the least secure but most compatible setting.

What You May See the First Time Security Controls is Started

If you are upgrading from Security Controls 2019.3, the first time you launch a later version, a one-time notification is displayed that informs you about the **Shared Credentials** feature. This feature enables you to share credentials with one or more users. The notification also briefly describes the security precautions that are in place to keep all credentials safe. You can click the embedded help link for more information.



Related Topics

- Upgrade Requirements
- Upgrade Tasks Performed on the Console

433. Upgrade Requirements

New System Requirements

The following operating systems are no longer supported for use by the Security Controls console:

- Windows Server 2012 family
- Windows Server 2012 R2 family

A new version of the Microsoft Visual C++ Redistributable for Visual Studio 2015 – 2022 is available, so this will likely be identified as missing during the prerequisite check of the upgrade process.

For a complete list of requirements for the console, your agentless clients and your agent-based clients, see **System Requirements**.

User Account Requirements for Performing an Upgrade

In order to perform an upgrade, your user account must meet the following requirements:

- The user performing the database upgrade must be a member of the db_owner role.
- If you have multiple consoles that share a database and are linking an additional console to a database that is already upgraded, the user account you use must be a member of the following database roles:
  - db_datareader
  - db_datawriter
  - STExec
  - STCatalogupdate

  In addition, the service account used for background operations must be a member the db_owner role. If your account is a member of the db_securityadmin and db_accessAdmin roles, the database upgrade tool will automatically attempt to map and configure the required roles for you.

Related Topics

- **Upgrade Procedure**
- **Upgrade Tasks Performed on the Console**

434. Upgrade Tasks Performed on the Console

In order to complete the upgrade, the following tasks must be performed on the Ivanti Security Controls console.

IMPORTANT! If you need to refresh your license or enter a new add-on license key, the **License Key Activation Method** should be used. If for some reason you are using the legacy **Credential Activation Method** and you have agents deployed to your endpoints, you must wait for the agents to check in with the console and be upgraded to v2026.3 before you change licensing methods. All Linux agents and few Windows agents will fail if you change licensing methods before the agents are upgraded.

Refresh Your License (Offline Consoles Only)

If your console is offline (it does not have an internet connection), in order to view and use the new features in Security Controls 2026.3, you must manually refresh your license. For information on activating a disconnected console, see **Activating the Program**.

If the console is online the license will be automatically refreshed during the upgrade process.

Initialize Users for Credential Sharing

Each user in your organization will be assigned a user certificate and a public/private key pair the first time they launch Security Controls after the upgrade. The certificate and keys are required in order for the users to participate in the **Shared Credentials**. Encourage each Security Controls user to launch the program as soon as reasonably possible.

The other option for getting users to be recognized by Security Controls is to issue a **REST API request**.

Review Credentials That are Shared with Background Services

Enabling a credential for use with background services is now performed on the new **Share Credential** dialog, rather than the **Define Credential** dialog. Any credential that was being shared with background tasks, agents and other features will be automatically converted to the new convention during the upgrade. You can access the **Share Credential** dialog by selecting **Manage > Credentials** and then clicking the **Share** button.

You should experience no interruption in service or scheduled background operations. If a background service is using credentials that for some reason cannot be decrypted, then the **Credential Reset** dialog will be displayed and that dialog can be used to recover from the situation.

For more information, see **Shared Credentials**.

Uninstall the Ivanti Scheduler from Your Target Machines

Use of the Ivanti Scheduler was discontinued in v2023.2. All scheduling on target machines is now performed using the Microsoft Scheduler. Once you are certain that all scheduled tasks using this scheduler have been run, it is recommended that you **uninstall the Ivanti Scheduler** from your target machines at your earliest convenience. This is strictly a house cleaning procedure and no harm will be done if the Ivanti Scheduler is not immediately removed following the upgrade.

With the deprecation of the Ivanti Scheduler, port 5120 is no longer required to be an allowed port in your firewall settings.

Confirm Your SSH Server Connection Setting

The **SSH server connection** option, which was introduced in v2022.4, specifies if SSH connections can be used when the console communicates with an endpoint. For security reasons, the default setting for this option is **Block**. For more detailed information, see the SSH Authentication topic.

Assign Groups in Machine View and Scan View

The **Assigned Group** column in Machine View and Scan View, which was introduced in v2020.1, enables you to group related machines, making it easier to perform agentless operations and generate reports on the machines. If you are upgrading from v2019.3, the values in this column will be empty immediately following the upgrade. Values will be automatically assigned during future scan operations that involve machine groups, or you can manually assign values using the **Machine Properties** dialog. For more information, see the Assigned Group column description.

Review Your Scheduled Tasks

Scheduled tasks are monitored and managed from two separate areas. You should review both scheduled tasks managers to verify that your existing tasks were properly ported.

- The **Scheduled Console Tasks Manager** provides one location to view tasks currently scheduled on the console such as patch scans, asset scans, patch deployments to the console machine, script execution and scheduled reports. To access this dialog, select **Manage > Scheduled Console Tasks**.
- The **Scheduled Remote Tasks Manager** provides one location from which to view power tasks and patch deployments tasks currently scheduled on your remote target machines. You access the Scheduled Remote Tasks Manager from Machine View by right-clicking on a machine and then selecting **View scheduled tasks**.

Synchronize Your Distribution Servers

You must update your distribution servers with the latest patches and/or scan engines and XML definition files contained on the console. This is particularly important if your agents use distribution servers to download these files. The distribution servers must be synchronized with the updated console files prior to the agents performing their check-in.

To synchronize your distribution servers:

1. Select **Help > Refresh files** to make sure the console contains all the latest files.
2. Select **Tools > Options > Distribution Servers**.
3. In the top pane, select which distribution server you want to synchronize with the console.
4. In the **Add scheduled sync** box in the top pane, select the component you want to synchronize.
5. Click **Add scheduled sync**.
6. Specify when you want the synchronization to occur and then click **Save**.
7. In the **Schedule automatic synchronization** pane, select the scheduled synchronization entry.
8. Click **Run now**.

Don't worry if the agents happen to check in before you have finished synchronizing the distribution servers. The agents will be updated the next time a scheduled task is run or the agent updates its binaries.

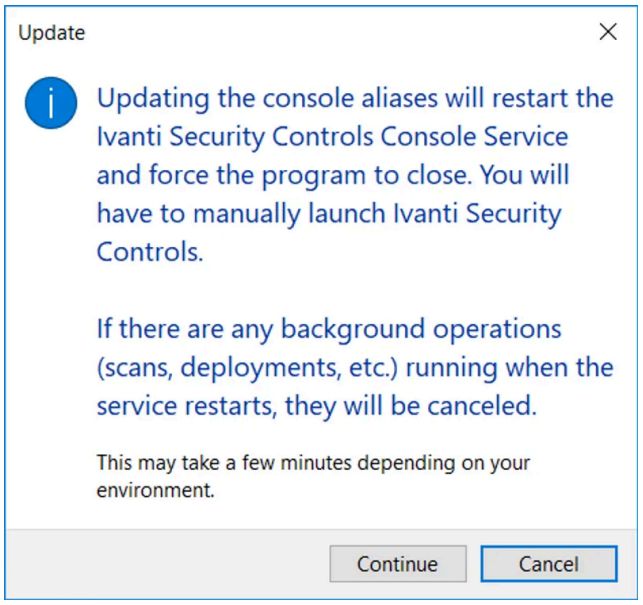
Assign Aliases to the Console

This task is necessary if one or more of the following conditions apply:

- You have assigned the console machine to a new domain
- You have given the console a new common name or IP address
- You manually installed agents and they use an IP address to communicate with the console

Under these conditions, you must use the **Console Alias Editor** tool to identify the old console names or addresses as trusted aliases. If you don't, when an agent checks in with the Security Controls console or when an agentless machine attempts to send patch deployment status messages to the console, they will not be able to verify that the machine they contacted is a trusted machine.

1. Select **Tools > Console alias editor**.
   The **Console Alias Editor** dialog is displayed. It will contain the names and IP addresses currently used to identify the console machine.
2. Type the names and/or IP addresses that you want to use as an alias for the console machine.
   You can specify IP addresses using either an IPv4 or IPv6 format.
3. Click **Update**.
   The following dialog is displayed:



1. Click either **Continue** or **Cancel**.
   If you click **Continue**, both the console service and the Security Controls program will be automatically restarted; this is necessary in order to update the console aliases list. If you click **Cancel**, the console aliases list will not be updated.

IMPORTANT! The agents will not recognize a new alias until after they check in with the restarted console. The check-in must be initiated by an agent either manually using the agent client program or via a scheduled check in; a check-in command issued from the console to an agent will not update the console certificate on the agent machine.

Check Your Custom User Settings

The following custom user settings are not preserved during the upgrade.

- Tools > Options > Display tab:
  - Recent item (days)
  - Show only items created by me

- Show patch content updates on main page
- Show informational items in patch scan results
- Show product levels in View → Windows Patches

Tools > Options > Notifications and Warnings tab:

- Warn before scheduling deployments
- Close Refresh Files when finished
- Warn if Protect Cloud sync is not enabled on this console
- Warn before opening 7 or more bulletins

Tools > Options > Logging tab:

- Diagnostic patch scanning

Deployment Tracker:

- Update speed
- Days to show
- Show failures
- Show in progress
- Show successfully completed

ESXi Hypervisor Bulletins tab:

- Only show latest

Event History

- Limit results to previous (days)

ITScripts Results View

- Results since

If You Use the CHM Version of the Help

The CHM version of the Security Controls help is no longer included with the installation package. If you use the CHM file, you will need to **follow the instructions** for downloading and configuring the 2026.3 version of the file.

If You Use an Agent on the Console

If you have an agent installed on the Security Controls console, you should manually reinstall that agent. This should be done in order to ensure that the console agent is properly upgraded with the new agent certificate. No actions are required for agents that are installed on target machines.

Related Topics

- **Upgrade Requirements**
- **Upgrade Procedure**

435. Use Examples

There are many possible uses of the API feature. Here are two examples that many Security Controls customers are likely to find useful.

Integrate Security Controls with a Vulnerability Scanner

If you use a vulnerability scanner to identify weaknesses in your network, the scanner may detect hundreds or even thousands of issues on your machines. At first this might seem a bit overwhelming, but what's likely happening is that the vulnerability scanner is simply producing a lot of noise. The scanner will often report every single missing patch as a vulnerability, when in reality the machines are probably only missing a few key patches that supersede a large number of older patches. It often takes very few patches to resolve many so-called vulnerabilities.

To address this, you can use the API to:

- Make calls to the vulnerability scanner
- Extract the vulnerability list (consisting of CVEs)
- Import those CVEs into a Security Controls patch group
- Perform patch scans and deployments using that patch group

The patch engine will eliminate all of the superseded patches and will identify the handful of patches that are actually missing. If you rerun the vulnerability scanner after deploying the patches, most of the vulnerabilities will likely go away.

Use a PowerShell Script to Patch a Clustered SQL Server

This example shows how to use a PowerShell script to control the patch scanning and patch deployment processes on machines in an SQL cluster. The goal in this example is to coordinate events and provide zero downtime while patching.

Bash

```
Import-Module STProtect –PassThru
Import-Module ServerManager
Add-WindowsFeature RSAT-Clustering
Import-Module FailoverClusters

Write-Host “Scanning SampleSQL1”
$scan = Start-PatchScan –EndpointName “SampleSQL1”
–CredentialFriendlyName “Sample Domain Cred” –TemplateName “Security Patch Scan”

$scan | Watch-PatchScan
Write-Host “Scanning SampleSQL1 Complete”

$scanDetail = $scan | Get-PatchScan
Write-Host “SampleSQL1 Final Details”
$scanDetail | Format-PatchScanTable

#Identify if there are missing patches on the target node. If yes, stop the node in the cluster and patch the system.
If ($scanDetail.MachineStates[0].MissingPatches –ne 0)
{
$totalMissingPatches = scanDetail.MachineStates[0].MissingPatches

Write-Host “$totalMissingPatches total missing patches will be deployed. Starting deploy . . .”
Write-Host “Stopping cluster node on SampleSQL1”
Suspend-ClusterNode –Name SampleSQL1 –Cluster SampleSQLCluster –Drain

$deploy = $scan | Start-PatchDeploy –TemplateName “Standard”
$deploy | Watch-PatchDeploy | Format-Table

Write-Host “Starting cluster node on SampleSQL1”
Resume-ClusterNode –Name SampleSQL1 –Cluster SampleSQLCluster –Failback NoFailback
}
```

In particular, this example script will:

1. Import the required modules.
2. Scan a single node in a SQL cluster.
3. Watch the patch scan, blocking further action until it completes.
4. Get the results of the scan.
   The output will include details such as information about the targeted machine, the number of missing and installed patches, a message indicating that the scanning process is complete, etc.
5. If there are missing patches, suspend the node in the SQL cluster and prepare to patch the system.
   Do this by suspending the node in the cluster and draining all current sessions from this node to another node.
6. Start the patch deployment using the Standard template.
7. Watch the progress of the patch deployment, blocking other actions until it completes.
   This will display the current status of the deployment including scheduled, complete and reboot, pending rescan, and finished.
8. Add the node back to the SQL cluster and resume operation.

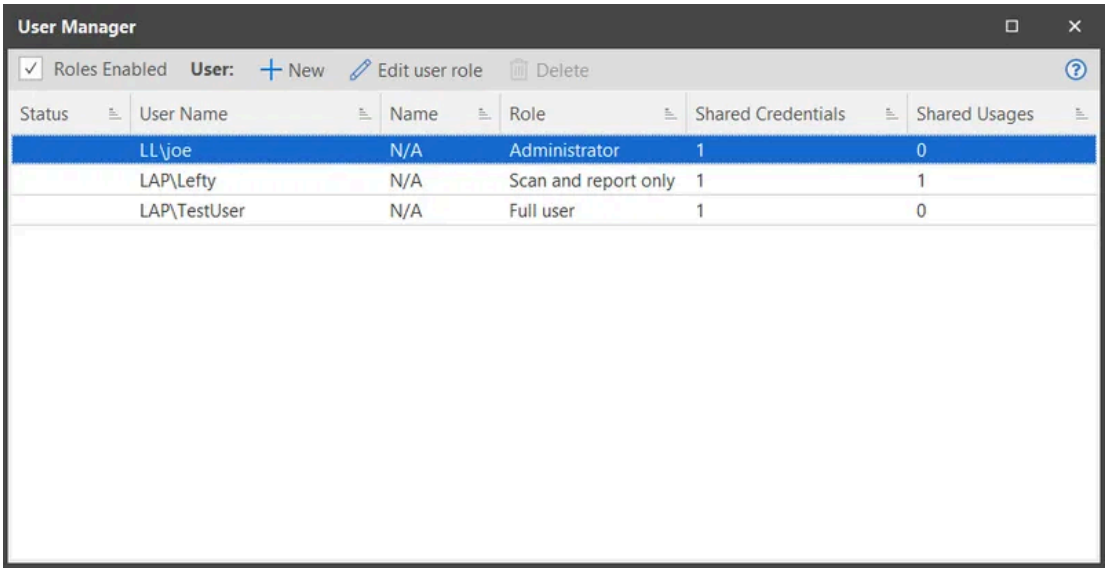
Repeat the process as needed for additional SQL Server instances or nodes in the cluster.

436. User Manager

You can assign roles to as many users as needed. At least one user must be assigned the administrator role.

> If you want to delete a user who should no longer have access to Security Controls, see **Deleting a User**.

1. Select **Manage > Users**.
   The **User Manager** dialog is displayed.



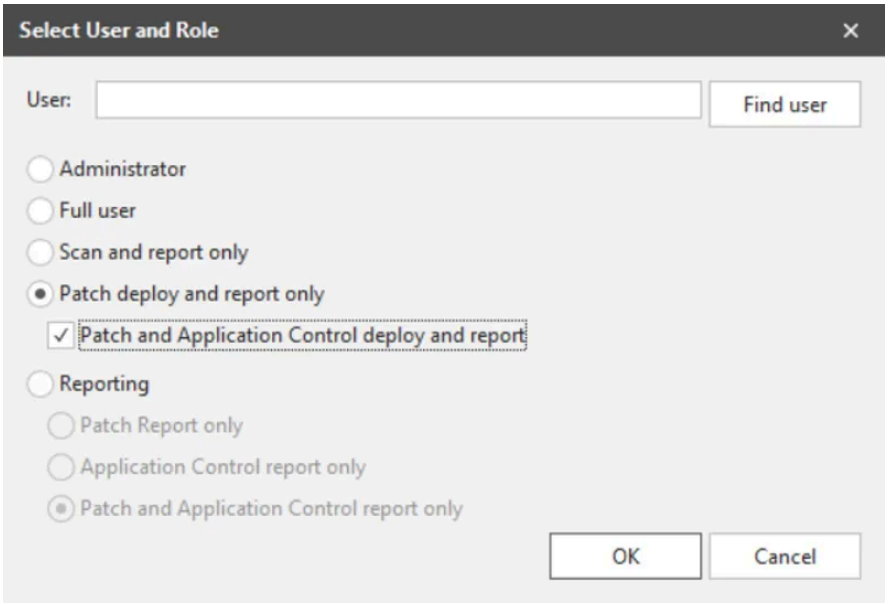
> For information on what it means for a user to be sharing credentials or sharing credential usages, see **Shared Credentials**.

Make sure the **Roles Enabled** check box is enabled.
You cannot add or edit a user unless **role-based administration** is enabled.

3. Click **New** or select an existing user and then click **Edit user role**.

> You cannot edit your own role.

The **Select User and Role** dialog is displayed.



Type a user name and then select the role you want to assign to that user.

- When specifying the user name you must use the following format: *domain|user*.
- If you are unsure of the correct domain and user name, you can view a list of all available domains and users by clicking **Find User**. The resulting dialog enables you to conduct either a quick search of just the *Users* organizational unit or a more comprehensive search of the entire active directory.
- Role definitions:
  - **Administrator:** Full access to all features of the program. Only an administrator user can modify the roles assigned to other users.
  - **Full user:** Access to all features except for the ability to administer roles.
  - **Scan and report only:** Can only perform patch scans and generate reports.
  - **Patch deploy and report only:** Can only perform patch deployments and generate reports.
  - **Reporting:** Can only generate reports for:
  - **Patch Report only**

Click **OK**.

All configured users must have access to the database. If users without administrative rights on the console machine receive an error when starting Security Controls, it probably means they don't have the necessary SQL Server permissions. See **SQL Server Preinstallation Notes** for more information.

437. Using an Agent on a Machine

The users of each agent machine can, if you permit, control many of the Security Controls Agent features on their machine.

Windows Agent Machines

Your Windows users can control the agent using the Security Controls Agent client program. They can access this program in two ways:

- By selecting **Start >** Ivanti Security Controls **Agent** on the target machine.
- By double-clicking the following executable file:

```bash
C:\Program Files\LANDESK\Shavlik Protect Agent\STUILauncher.exe
```

For information on how to use the client program, see **About the Agent Client Program**. This topic also provides information on how to control an agent using the stagentctl command-line utility.

Resetting Retry Counts within the Client Program

The Patch Engine tile includes a **Reset retry counts** button that resets all patch counters. A unique patch counter exists for every patch the program tries to download and for every patch the program tries to install. A patch counter will increment whenever a patch download or a patch installation fails. Failed download and installation attempts will be recorded in the patch log. If a Windows patch fails to download after 10 attempts or fails to install after three times in an individual patch cycle and five times in total for the endpoint, the client program will stop trying to deploy that particular patch. The only way to resume the deployment of that patch is to click **Reset retry counts**.

Linux Agent Machines

Your Linux users can control the agent on their machines using the stagentctl command-line utility. They can learn about the utility by displaying the built-in help information.

1. Launch a Terminal.
2. Change to the /opt/ivanti/isec/bin directory.
3. `cd /opt/ivanti/isec/bin`
   Display help information for the stagentctl utility.
   `./stagentctl`

Examples

View available tasks in the agent policy

Command

```
# ./stagentctl available-tasks
```

Sample Output

```
1. SampleLinuxPatchTask
```

```
2. Update asset data
```

```
3. Update agent binaries
```

```
4. Update patch data
```

```
5. Perform Agent check-in
```

> For a description of the available tasks, see **Managing Your Agents**.

Start a check-in job

Command

```
# ./stagentctl dispatch --index 5
```

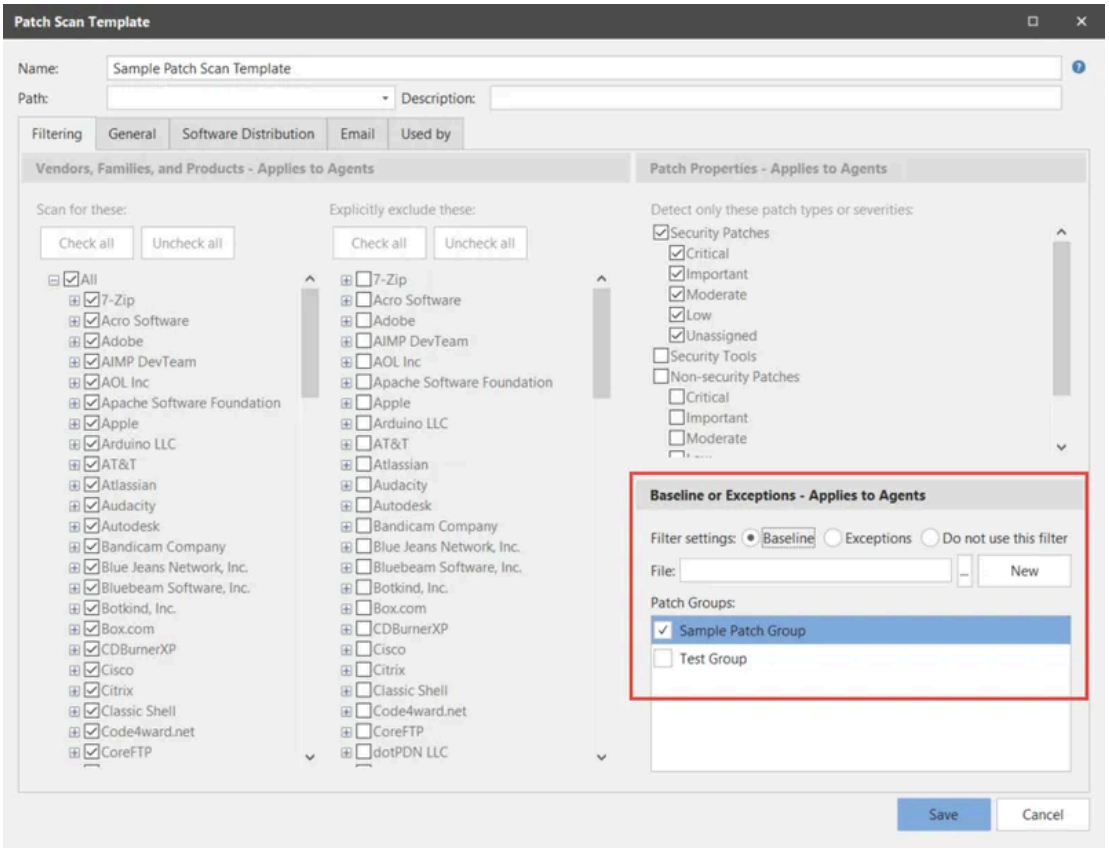
Sample Output

```
Task id: 96E17378-4833-BF52-4358-FC5CC14DF963
```

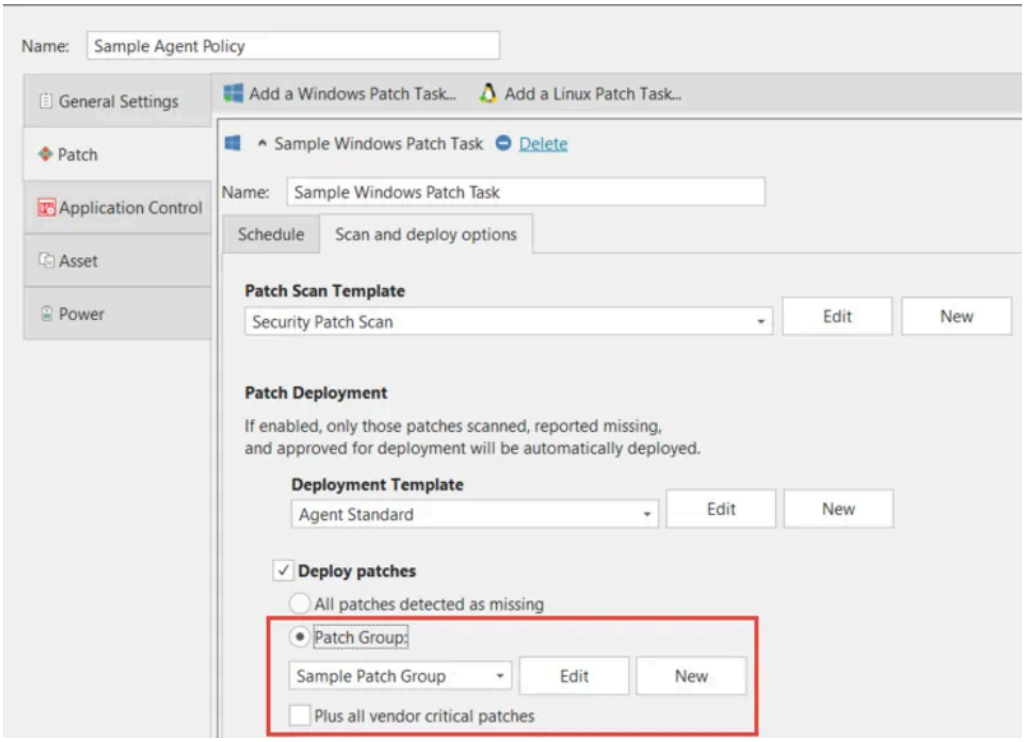
438. Using a Patch Group

To use a patch group in a custom scan template:

1. In the **My Patch Scan Templates** list, click the desired custom patch scan template.
2. In the scan template, on the **Filtering** tab, select either **Baseline** or **Exceptions**.
3. In the **Patch Groups** box, select the patch group(s) that contain the patches you want to use as your baseline or that you want to exclude.

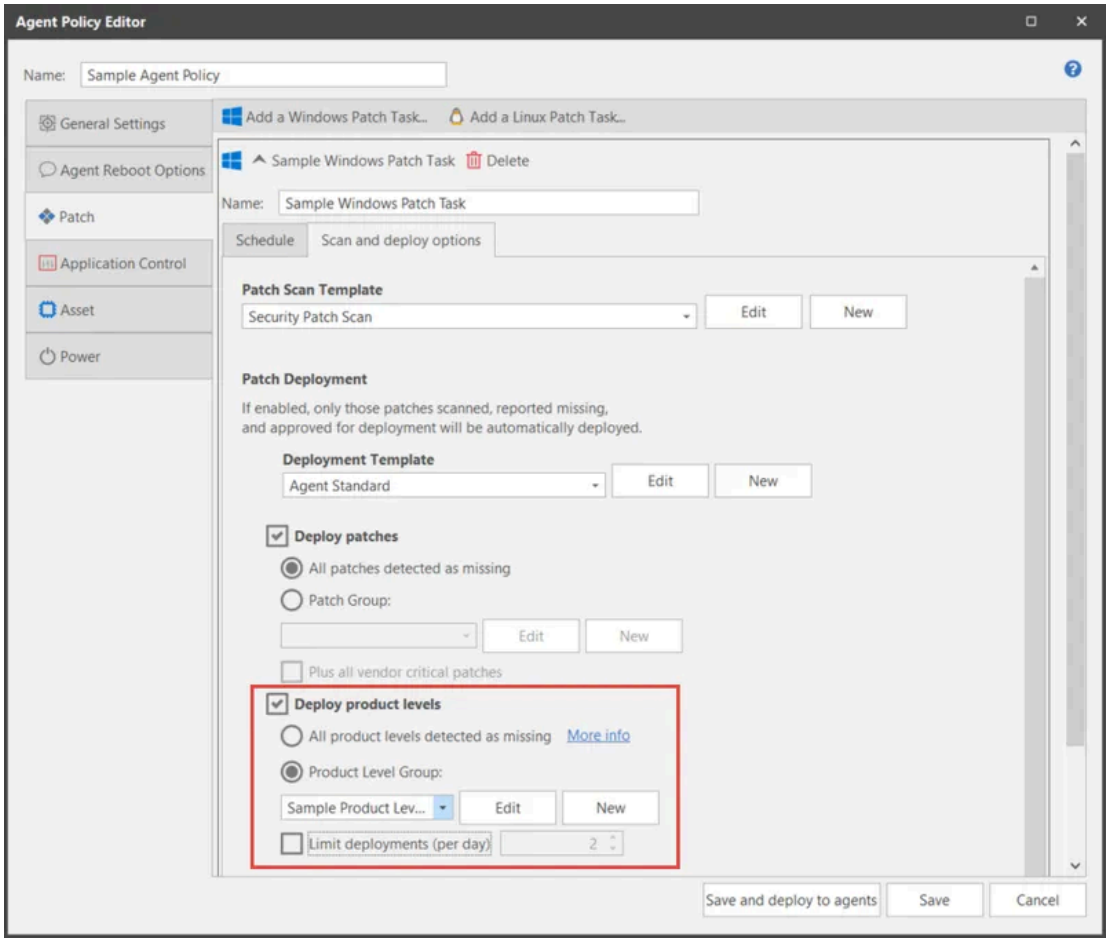


A patch group can also be used in an **agent policy**.


Name: Sample Agent Policy
General Settings
Patch
Application Control
Asset
Power
Add a Windows Patch Task...
Add a Linux Patch Task...
Sample Windows Patch Task
Delete
Name: Sample Windows Patch Task
Schedule
Scan and deploy options
Patch Scan Template
Security Patch Scan
Edit
New
Patch Deployment
If enabled, only those patches scanned, reported missing,
and approved for deployment will be automatically deployed.
Deployment Template
Agent Standard
Edit
New
Deploy patches
All patches detected as missing
Patch Group:
Sample Patch Group
Edit
New
Plus all vendor critical patches

439. Using a Product Level Group

A product level group is used within a Windows Patch Task in an agent to specify exactly which product levels should be deployed. For more information, see **Creating and Configuring a Patch Task**.



440. Using Patch Deployments to Perform Power Tasks

A power state template is not the only means for putting your machines into a sleep or hibernation state, you can also use a patch deployment template to perform these tasks. The **Post-deploy Reboot** tab can be used to configure the program to place your machines into the desired state following a patch deployment. For more details see **Deployment Template: Post-deploy Reboot Tab**.

441. Using Smart Filter

Information displayed in the list can be easily filtered to narrow the focus to only those machines of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

> Another option is to apply filters to individual columns. For more information, see **Customizing the Column Headers**.

Default Filters

The default filters are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

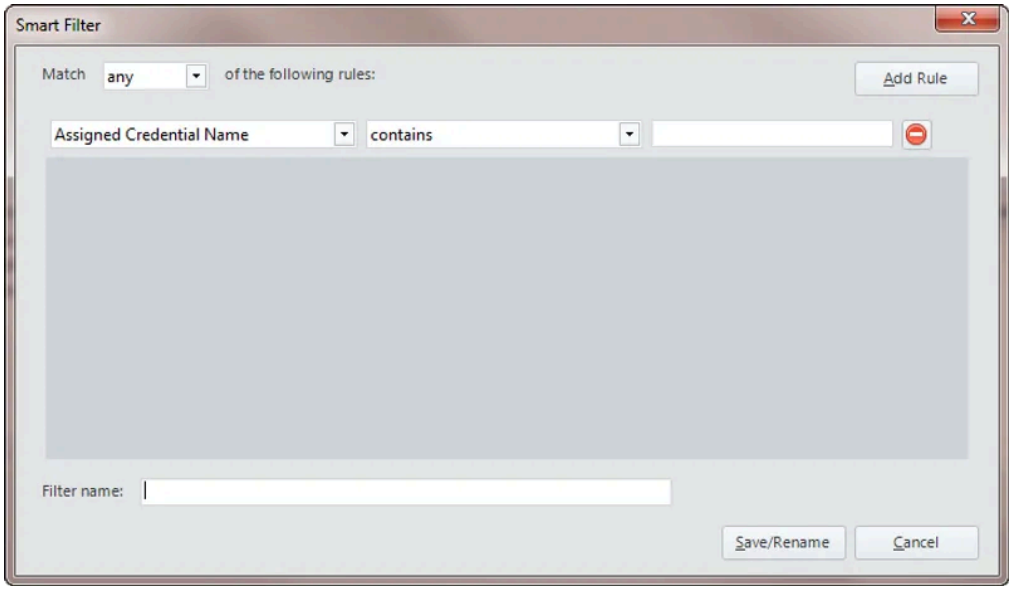
- ***All Machines**: All machines are displayed, including servers and workstations.
- ***Servers**: Only servers are displayed.
- ***Workstations**: Only workstations are displayed.
- ***Today**: Only those machines that have been scanned within the last 24 hours are displayed.
- ***Last 7 Days**: Only those machines that have been scanned within the last seven days are displayed.
- ***Last 14 Days**: Only those machines that have been scanned within the last 14 days are displayed.
- ***Last 30 Days**: Only those machines that have been scanned within the last 30 days are displayed.
- ***Last 60 Days**: Only those machines that have been scanned within the last 60 days are displayed.
- ***Last 90 Days**: Only those machines that have been scanned within the last 90 days are displayed.
- ***Missing at least 1 patch**: Only those machines that are missing at least one patch are displayed.
- ***Has an Agent Policy**: Only those machines that have Security Controls Agent installed are displayed.
- ***Does not have an Agent Policy**: Only those machines that do not have Security Controls Agent installed are displayed.

Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which machines you want displayed in the top pane. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the Create a New Smart Filter icon (+).
   The **Smart Filter** dialog is displayed.



Specify which rules in the filter must be matched.

- **All**: Only those machines that match all the rules in the filter will be displayed.
- **Any**: Machines that match at least one rule in the filter will be displayed.

Define one or more rules.
To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

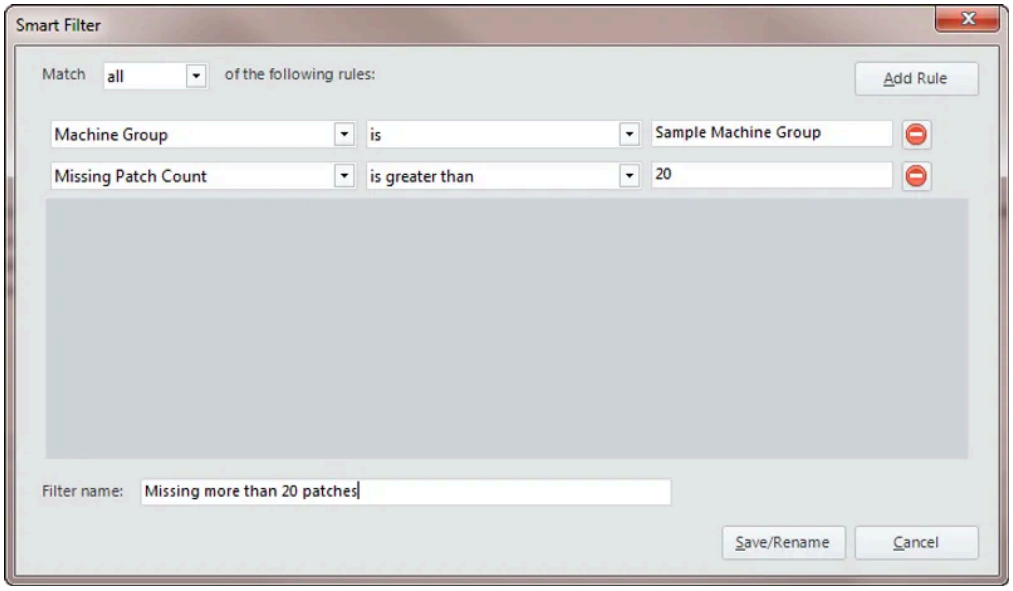
> If you define a rule that does not make sense (for example, "Machine Name is greater than 3") the rule will simply be ignored.

Type a name for the filter.

5. When you are finished defining your custom filter, click **Save/Rename**.

Example

Assume you want to see which machines in a particular machine group are missing more than 20 patches. You simply create a filter similar to the following:


Smart Filter
Match
all
of the following rules:
Add Rule
Machine Group
is
Sample Machine Group
Missing Patch Count
is greater than
20
Filter name:
Missing more than 20 patches
Save/Rename
Cancel

442. Using Smart Filter to Filter Information in the Top Pane

Information displayed in the list can be easily filtered to narrow the focus to only those machines of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

> Another option is to apply filters to individual columns. For more information, see **Customizing the Column Headers**.

Default Filters

The default filters are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

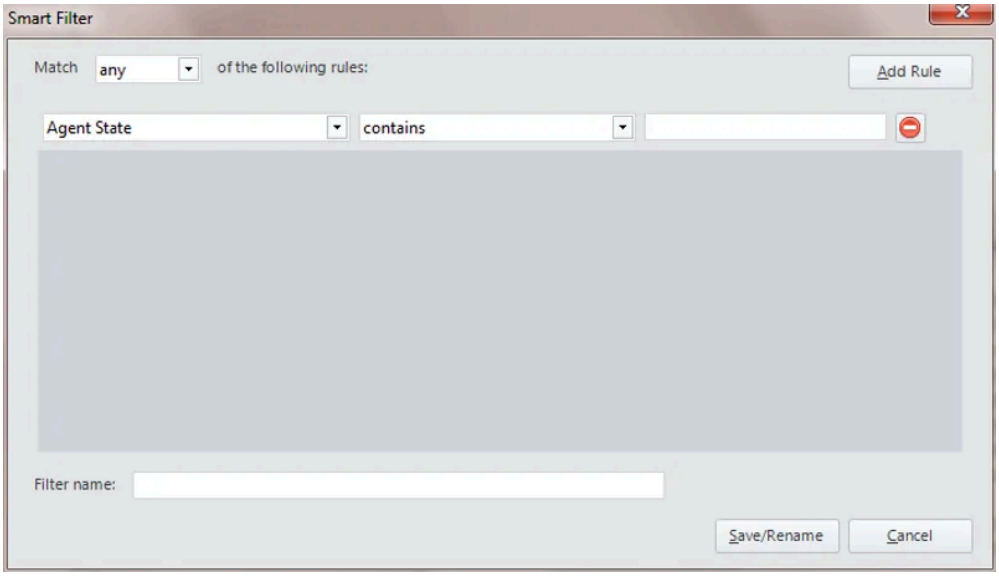
- ***All Machines**: All machines are displayed, including servers and workstations.
- ***Does not have an Agent Policy**: Only those machines that do not have Security Controls Agent installed are displayed.
- ***Has an Agent Policy**: Only those machines that have Security Controls Agent installed are displayed.
- ***Last 7 Days**: Only those machines that have been scanned within the last seven days are displayed.
- ***Last 14 Days**: Only those machines that have been scanned within the last 14 days are displayed.
- ***Last 30 Days**: Only those machines that have been scanned within the last 30 days are displayed.
- ***Last 60 Days**: Only those machines that have been scanned within the last 60 days are displayed.
- ***Last 90 Days**: Only those machines that have been scanned within the last 90 days are displayed.
- ***Linux machines**: Only Linux machines are displayed.
- ***Missing at least 1 patch**: Only those machines that are missing at least one patch are displayed.
- ***Never patch scanned**: Only those machines that have not been scanned for missing patches are displayed.
- ***Out of date agents**: Only those machines with out-of-date agents are displayed.
- ***Out of date patch scans**: Only those machines with out-of-date patch scans are displayed.
- ***Servers**: Only servers are displayed.
- ***Today**: Only those machines that have been scanned within the last 24 hours are displayed.
- ***Windows machines**: Only Windows machines are displayed.
- ***Workstations**: Only workstations are displayed.

Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which machines you want displayed in the top pane. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the Create a New Smart Filter icon ( ).
   The **Smart Filter** dialog is displayed.



Specify which rules in the filter must be matched.

- **All**: Only those machines that match all the rules in the filter will be displayed.
- **Any**: Machines that match at least one rule in the filter will be displayed.

Define one or more rules.
To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

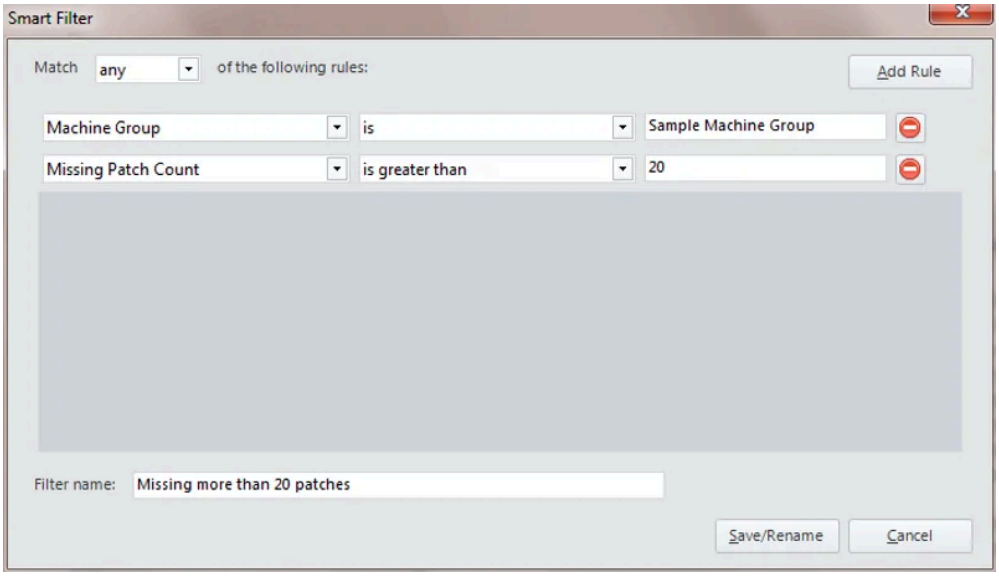
> If you define a rule that does not make sense (for example, "Machine Name is greater than 3") the rule will simply be ignored.

Type a name for the filter.

5. When you are finished defining your custom filter, click **Save/Rename**.

Example

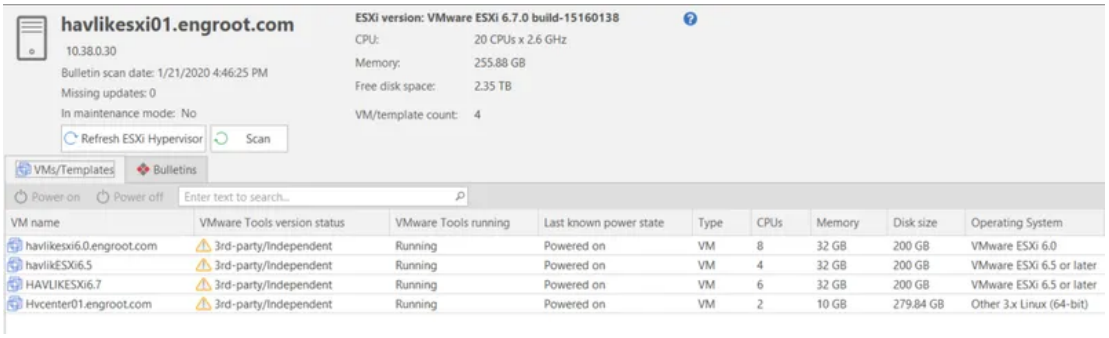
Assume you want to see which machines in a particular machine group are missing more than 20 patches. You simply create a filter similar to the following:


Smart Filter
Match
any
of the following rules:
Add Rule
Machine Group
is
Sample Machine Group
Missing Patch Count
is greater than
20
Filter name:
Missing more than 20 patches
Save/Rename
Cancel

443. Using the ESXi Hypervisors List

The **ESXi Hypervisors** list contains those hypervisors that are not being managed by a vCenter Server. When you right-click an individual hypervisor in this list or in the **vCenter Servers list** and then click **View**, information about that ESXi hypervisor is displayed in a header area and on two tabs in the lower pane.

- The header area provides basic configuration information about the selected ESXi hypervisor. It also contains a **Scan** button that enables you to initiate a bulletin scan of the ESXi hypervisor. For more information, see **How to Initiate a Scan of an ESXi Hypervisor**.
- The **VMs/Templates** tab **displays information** about the virtual machines and virtual machine templates that are contained on the selected ESXi hypervisor. You can use this tab to **power the virtual machines on and off**, and you can add the virtual machines to a machine group.
- The **Bulletins** tab shows the **status of the security bulletins** that have been issued for the ESXi hypervisor(s). You can also use this tab to **deploy missing bulletins** to your ESXi hypervisors.



444. Using the Event History Smart Filter

Information displayed within Event History can be easily filtered to narrow the focus to only those event entries of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

> The **Limit results to previous (days) option** can be used to adjust the amount of information displayed within Event History prior to using the Smart Filter.

Default Filters

The Smart Filter contains several default filters that are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

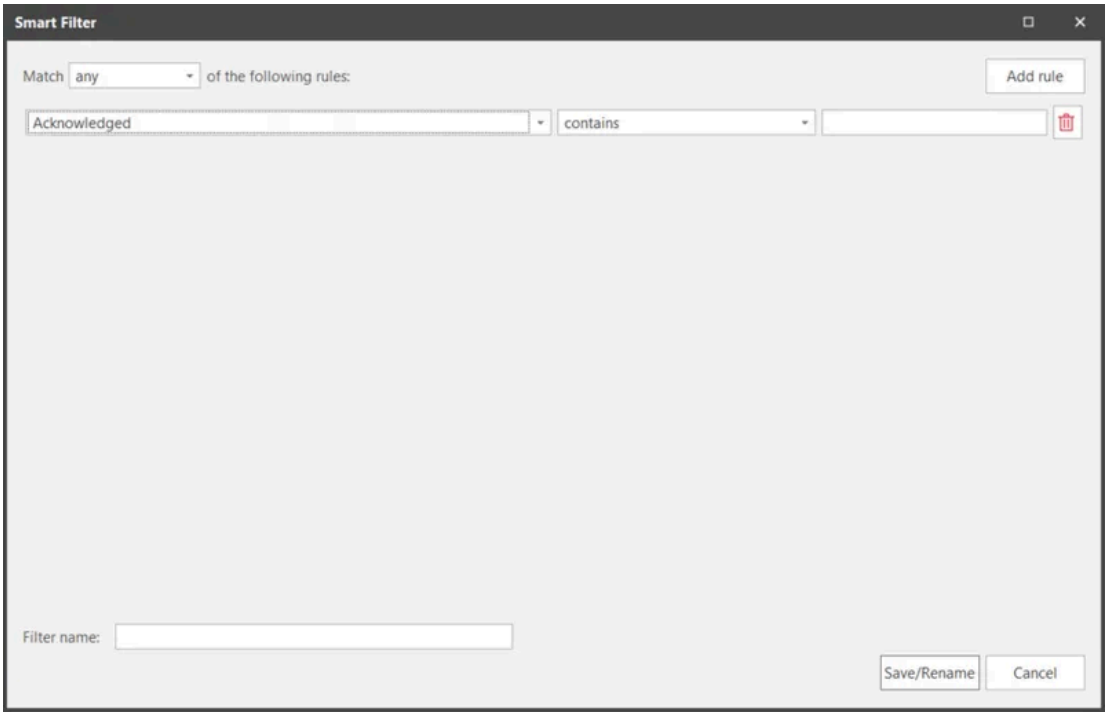
- ***All Operations**: All event entries are displayed.
- ***Failures:** Only those entries whose status is **Failure** are displayed.
- ***In Progress:** Only those entries whose status is **In progress** are displayed.
- ***Last 7 Days:** Only those entries that have been generated within the last 7 days are displayed.
- ***Today**: Only those entries that have been generated within the last 24 hours are displayed.

Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which entries you want displayed. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the New Smart Filter icon ( ).
   The **Smart Filter** dialog is displayed.



Specify which rules in the filter must be matched.

- **All**: Only those entries that match all the rules in the filter will be displayed.
- **Any**: Entries that match at least one rule in the filter will be displayed.

Define one or more rules.
To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

> If you define a rule that does not make sense (for example, "Name is greater than 3") the rule will simply be ignored.

Type a name for the filter.

5. When you are finished defining your custom filter, click **Save/Rename**.

445. Using the Script Result Smart Filter

Information displayed in the list can be easily filtered to narrow the focus to only those script results of interest. One way to do this is by using the Smart Filter.



The Smart Filter contains several default filters. You can also define your own custom filters.

> The **Results since** option can be used to adjust the amount of information displayed within the pane prior to using the Smart Filter.

Default Filters

The Smart Filter contains several default filters that are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

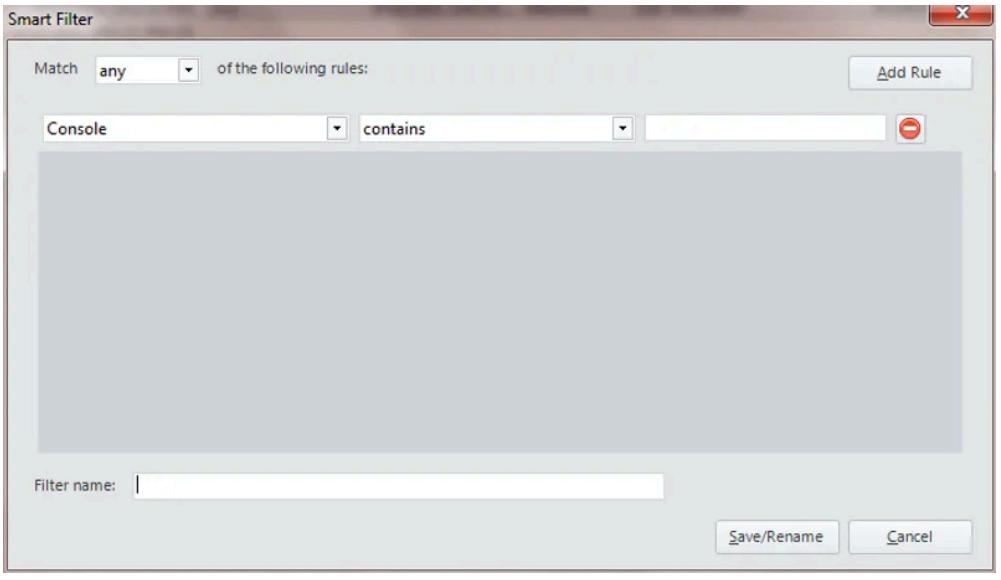
- ***All ITScript Results**: All script results are displayed.
- ***Today:** Only those script results that were generated today are displayed.
- ***Last 30 Days:** Only those script results that were generated within the last 30 days are displayed.
- ***Last 60 Days:** Only those script results that were generated within the last 60 days are displayed.
- ***Last 90 Days:** Only those script results that were generated within the last 90 days are displayed.

Custom Filters

You can create your own custom filters. This is a powerful tool that enables you to specify exactly which results you want displayed. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the Create a New Smart Filter icon ( ).
   The **Smart Filter** dialog is displayed.



Specify which rules in the filter must be matched.

- **All**: Only those events that match all the rules in the filter will be displayed.
- **Any**: Events that match at least one rule in the filter will be displayed.

Define one or more rules.
To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add Rule**.

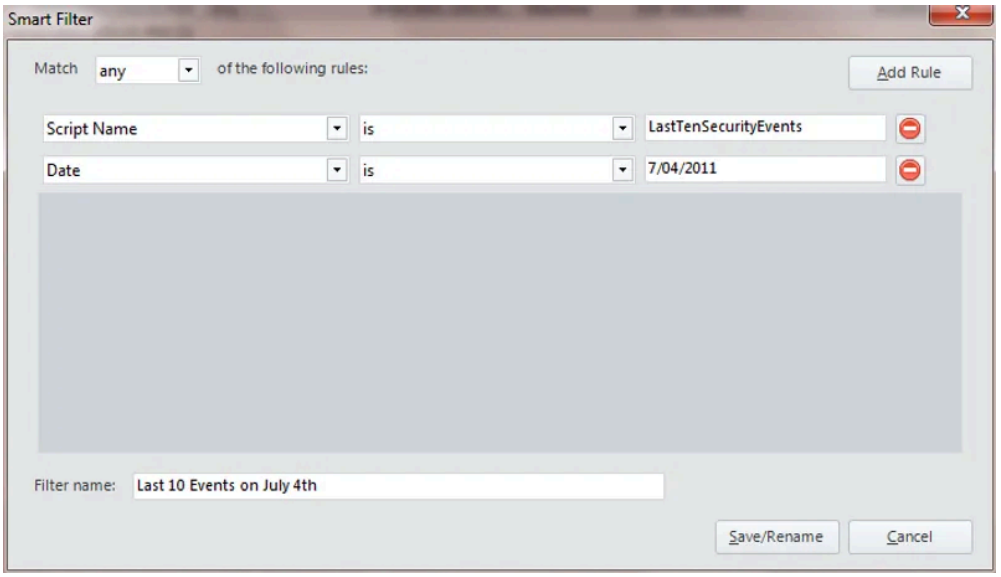
> If you define a rule that does not make sense (for example, "Script Name is greater than 3") the rule will simply be ignored.

Type a name for the filter.

5. When you are finished defining your custom filter, click **Save/Rename**.

Example

Assume you want to see the security events that occurred on your target machines on a specific date. You simply create a filter similar to the following:



446. Variables and Functions

Security Controls provides a set of PowerShell variables and functions to every script. The variable names all begin with “ST_”. The function names all begin with “ST-“. You can use these variables and functions in your scripts.

PowerShell variables can have different scopes:

- Global: Available to the current PowerShell session
- Script: Declared in the script (outside of functions) and local to that script
- Private: Declared in a function and local to that function
- Local: The current scope, which can be global, script, or private

The variables supplied with Security Controls are declared at the global scope. Since each target machine is running in its own PowerShell session, this is equivalent to being declared in the scope of the script.

Run Variables

The following table lists the per-run variables. All machines will see the same value for these variables. Do not modify the values of variables marked as [Read-only].

Variable Name	Description
ST_OutputDirectory	The full path to the base output directory. A subdirectory will be created for the run. [Read-only]
ST_RunDirectory	The full path to the run output directory. [Read-only]
ST_RunErrorFile	The full path to the run error file. Errors that are not specific to a particular machine should be written to this file. This file will also contain messages about machines that could not be resolved to an IP address, and no machine-specific subfolder will be created for machines that could not be resolved. [Read-only]
ST_RunName	The name of the run specified in the user-interface when the run was initiated or scheduled, with the run time appended. The default is the name of the script or template. [Read-only]
ST_RunOnConsole	Set to $false if the script is using PowerShell remoting; otherwise $true. [Read-only]
ST_RunOutputFile	The full path to the standard run output file. All output that would appear on the console if run at a command prompt will be placed in this file. [Read-only]
ST_RunResult	This is a short run result that will appear in the Operations Monitor. It is limited to 100 characters in length. If you do not explicitly set this variable in your script, it will be set to indicate the number of machines that had errors and the number of machine resolution errors.

Machine Variables

The following table lists the per-machine variables. The value of these variables may be different for each target machine. You should not modify the values of variables marked as [Read-only].

Variable Name	Description
ST_ComputerName	The name of the target computer. [Read-only]
ST_Credential	A PSCredential object that contains the user name and SecureString password used to connect to the target machine. This variable can be passed to any command that supports the the Credential parameter. [Read-only]
ST_DomainName	The name of the target computer domain or workgroup. [Read-only]
ST_MachineDirectory	The full path to the machine directory. This will typically be the machine name, but if the machine name contains characters that are not allowed in folder names, then those characters will be replaced with underscore characters. [Read-only]
ST_MachineError	A Boolean value indicating that one or more errors were detected during the execution of this script targeting this specific machine.
ST_MachineErrorFile	The full path to the machine error file. If errors are detected during execution of the script, they will appear in this file. [Read-only]
ST_MachineOutputFile	The full path to the machine output file. Output generated by the script to the standard output will be captured in this file.
ST_MachineResult	This is a short machine result that will appear in the Operations Monitor. It is limited to 100 characters in length. If you do not explicitly set this variable in your script, it will be set to “Success” if no machine errors were detected, or to the error message of the first error encountered for that machine. Use the ST-SetMachineResult function to explicitly set the value of this variable.
ST_MachineResultSet	A Boolean value indicating that the script set the ST_MachineResult variable. Use the ST-SetMachineResult function to set both the ST_MachineResult variable and this variable.

Functions

Security Controls provides a set of functions that are available to every script you create. They are listed in the following table.

Variable Name	Description
ST-GetTargetOS	This function attempts to connect to the target system, query WMI and retrieve the Win32_OperatingSystem object.
ST-SetMachineResult	This function takes a string parameter. It sets the ST_MachineResult variable to the string passed in and set ST_MachineResultSet to $true.
ST-SetMachineError	This function takes a string argument. It sets the ST_MachineResult variable to the string passed in. It also sets the ST_MachineResultSet and ST_MachineError variables to $true.
ST-SendMessage	This function takes a string parameter. The string will be displayed in the Operations Monitor. Use this function to monitor the progress of long-running scripts. When the script is complete the string in ST_MachineResult will be displayed in the operations monitor. Except during debug, you should avoid calling this method in scripts that execute quickly. The string will be truncated to 100 characters if a longer string is passed in.
ST-CreateMachineDirectory	Normally, the machine directory is not created until output is written. If your script is creating files in the machine directory, you should invoke this function to create the directory before writing anything to the directory. Calling this function more than once will have no negative effect.
ST-CreateRunDirectory	Normally, the run directory is not created until the run writes some output. If your script is creating files in the run directory, you should invoke this function to create the directory before writing anything to the directory. Calling this function more than once will have no negative effect.
ST-ComputerAndCredential	This function returns appropriate values to use for the ComputerName and Credential parameters for the target machine. See **Specifying ComputerName and Credential Parameters** for details.
ST-SubCC	This function takes a string parameter, which is a valid PowerShell command. This function substitutes “$ST_CC” in that command string with appropriate values to use for the ComputerName and Credential parameters for the command. It then executes the resulting command and returns the results of the execution. See **Specifying ComputerName and Credential Parameters** for details.

447. vCenter Server and ESXi Hypervisor Requirements

The **functions provided by the Virtual Inventory feature** are designed for use with the following VMware vSphere licensed environments: VMware vSphere Essentials, Essentials Plus, Standard, and Standard with Operations Management. While the functions can be used in enterprise-level environments, the user experience and performance has been optimized for use in small and medium-sized business environments.

vCenter Server Requirements and Recommendations

- The vCenter Servers that are **added to the Virtual Inventory list** must be at VMware vCenter Server 7.0 or later
- You must have valid credentials for the vCenter Server
- You must be able to connect to the vCenter Server
- If the hypervisors in your organization are managed by a vCenter Server, you should add those hypervisors to Security Controls by adding the managing vCenter Server. The scanning and deployment actions you take on the hypervisors are more complete when performed through a vCenter Server.

ESXi Hypervisor Scanning Requirements

You must meet the following requirements in order to successfully scan an ESXi hypervisor:

- You must have valid credentials for the ESXi hypervisor
- You must be able to connect to the ESXi hypervisor
- The hypervisor must be using ESXi version 7.0 or later

> If you are using ESXI 7.0 Update 1 or later, the patch offline bundle must be installed on your hypervisor. For more information, see the **VMware ESXi 7.0 Update 1 Release Notes**.

Your firewall must be configured to allow an HTTP Client connection

ESXi Hypervisor Deployment Requirements and Recommendations

You must meet the following requirements in order to successfully deploy bulletins to ESXi hypervisors:

- The Security Controls console must be online
- The ESXi hypervisor must be online in order to access assessment data and download updates
- The hypervisor must be using ESXi version 7.0 or later
- Port 443 must be open on the hypervisor
- The latest version of VMware Tools is required on all virtual machines running on the hypervisor
- You must have previously **scanned the ESXi hypervisor** to identify the missing bulletins
- You can only deploy bulletins to one ESXi hypervisor at a time in a single deployment. You can, however, start multiple deployments to different hypervisors and have them run concurrently (do not do this if the hypervisors are being managed by the same vCenter Server).
- You cannot schedule deployments

- For vCenter Servers using fully automated Distributed Resources Scheduler (DRS), during a deployment Security Controls will attempt to put the ESXi hypervisor into maintenance mode and allow DRS to manage the virtual machines. Security Controls will not support DRS for vCenter Servers that have their DRS automation level set to **Manual** or **Partially Automated** because these DRS settings require user intervention at the vSphere client level. In this case Security Controls may suspend or shut down the virtual machines, or it may cancel the deployment.
- You should not attempt to patch a hypervisor that contains a vCenter Server or vCenter Server Appliance without first moving the vCenter Server to another hypervisor. Consider **using DRS** to move the vCenter Server.
- You should not attempt to patch a hypervisor that contains the Security Controls console without first moving the console to another hypervisor. Consider **using DRS** to move the console.
- You must use a role that contains the following permissions on the ESXi hypervisor:
    - Global
        - Act as vCenter Server
        - Cancel task
        - Diagnostics
        - Licenses
        - Log event
        - Proxy

    Host: Configuration

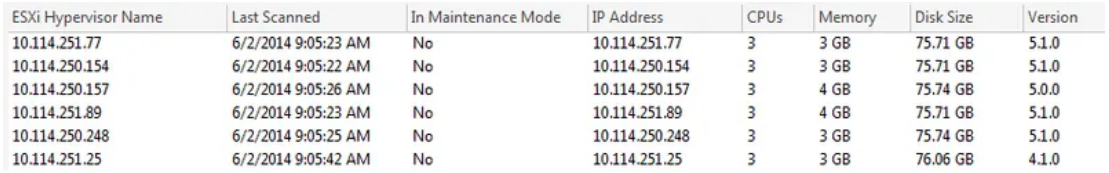
        - Connection
        - Maintenance
        - Power
        - Query patch
        - System Management
        - System resources

    Host: Replication

    - Resource
    - Scheduled task
    - Sessions
    - Tasks
    - vApp
    - vCenter Inventory Services (v7.0 or later)
    - vService (v7.0 or later)
    - Virtual machine

448. vCenter Server Top Pane Summary

The top pane contains basic information about each ESXi hypervisor that is being managed by the vCenter Server. Click on a column heading to sort the table by that information.



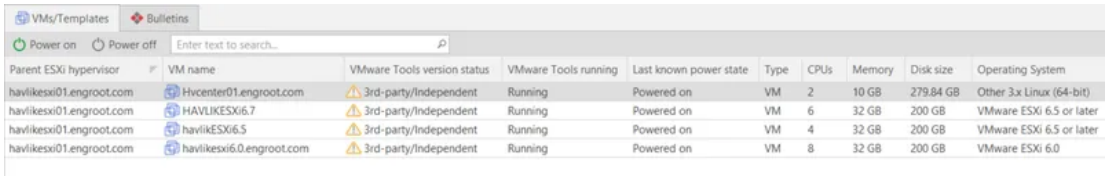
ESXi Hypervisor Name	Last Scanned	In Maintenance Mode	IP Address	CPUs	Memory	Disk Size	Version
10.114.251.77	6/2/2014 9:05:23 AM	No	10.114.251.77	3	3 GB	75.71 GB	5.1.0
10.114.250.154	6/2/2014 9:05:22 AM	No	10.114.250.154	3	3 GB	75.71 GB	5.1.0
10.114.250.157	6/2/2014 9:05:26 AM	No	10.114.250.157	3	4 GB	75.74 GB	5.0.0
10.114.251.89	6/2/2014 9:05:23 AM	No	10.114.251.89	3	4 GB	75.71 GB	5.1.0
10.114.250.248	6/2/2014 9:05:25 AM	No	10.114.250.248	3	3 GB	75.74 GB	5.1.0
10.114.251.25	6/2/2014 9:05:42 AM	No	10.114.251.25	3	3 GB	76.06 GB	4.1.0

Column	Description
ESXi Hypervisor Name	The name or IP address of the ESXi hypervisor.
Last Scanned	Shows the date and time that the ESXi hypervisor was last scanned.
In Maintenance Mode	Indicates if the ESXi hypervisor was in maintenance mode at the time of the last scan.
IP Address	The IP address of the ESXi hypervisor.
CPUs	The number of CPUs contained on the ESXi hypervisor.
Memory	The amount of memory contained on the ESXi hypervisor.
Disk Size	The amount of total disk space contained on the ESXi hypervisor.
Version	The software version of the ESXi hypervisor.

449. Viewing a Summary of the ESXi Hypervisor's Virtual Machines and Virtual Machine Templates

The **VMs/Templates** tab displays summary information about the virtual machines and virtual machine templates that are contained on the ESXi hypervisor(s) selected in the top pane. If multiple hypervisors are selected in the top pane, this tab will display virtual machine information for all the selected hypervisors.

You can customize the way information is displayed within this pane. See **Customizing the Column Headers** for information.



Field	Description
Power on	See **Performing Actions on Virtual Machines**.
Power off	See **Performing Actions on Virtual Machines**.
Search	Enables you to search for virtual machines contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those virtual machines that match the search criteria are displayed; all other virtual machines are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the VM Name column. • All partial matches are displayed. For example, if you search for virtual machines named Test, any virtual machine with "test" in its name will be considered a match (e.g. TestVM1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
Parent ESXi Hypervisor	The name or IP address of the ESXi hypervisor that is hosting the virtual machine or virtual machine template.
VM Name	The virtual machine name.
VMware Tools Version Status	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. This column identifies the version of VMware Tools currently in use on the virtual machine.
VMware Tools Running Status	Indicates if VMware Tools is running on the virtual machine.
Last Known Power State	The last known state of the virtual machine (Powered on, Powered off, or Suspended).
Type	Indicates if the device is a virtual machine (VM) or a VM template.
CPUs	The number of Central Processing Unit (CPUs) available to the virtual machine.
Memory	The amount of memory (MB) allocated to the virtual machine.
Disk Size	The amount of disk space (GB) allocated to the virtual machine.
Operating System	The operating system being used on the virtual machine.
IP Address	The IP address of the virtual machine.
Hostname	The name of the machine on the network that is hosting the virtual machine.

450. VendorSeverity view

The Reporting2.VendorSeverity view defines vendor severity states.

Column Name	Data Type	Nullable	Description
Id	int		The vendor severity id.
Value	nvarchar(100)		The value of the vendor severity.
Description	nvarchar(256)		The vendor severity description.

Content

You can run the following query to verify the contents of the Reporting.VendorSeverity view.

Bash

```
SELECT [Id]
,[Value]
,[Description]
FROM [SecurityControls].[Reporting2].[VendorSeverity]
```

ID	Value	Description
0	None	None
1	Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
2	Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users'' data, or of the integrity or availability of processing resources.
3	Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
4	Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

451. Step 4: Testing for and Verifying the New Certificate

You can use the Test Console Configuration command to verify your new certificate environment.

```
C:\Program Files\Ivanti\Security Controls>stmgmt.exe -test_console
```

The section titled `Testing for console issuing certificate configuration` of the command output will show that your sub-authority certificate was found and that it was issued by your root authority.

Another way to verify your new environment is to check that the new console and agent certificates have been issued and distributed to the correct certificate stores.

- The new console certificate will be issued and distributed automatically and in very short order as part of using Security Controls.
- A new agent certificate will be automatically issued whenever a new agent is installed or when an existing agent's certificate needs to be reissued.

452. Version and License Information

Selecting **Help > About** Security Controls will provide a variety of information about Security Controls.

Application and Version Information

The center portion of the **Help > About** dialog is used to view both application and version information.

- **Application tab**: Displays application information for Security Controls and information about the database being used by the program, including:
  - **Program Version**: Displays both the version and the edition of the program being used.
  - **Administration Role**: If role-based administration is enabled, displays the current role assignment.
  - **License Key and Licensed Capabilities**: Displays license key information and identifies which features are enabled.
  - **Configured Database**: Displays the current database being used.

File versions tab: Displays version information about each of the program components being used by the program. This can be helpful if you ever need to perform any troubleshooting of the program as you can quickly determine if you are using the most current data.

Export Information

To save the version information to a Notepad file, click **Export file versions**.

Open Source License

To view license information for the open source packages distributed with Security Controls, click **Open Source license**.

Technical Support

To learn about technical support options, click **Tech support**.

Data Versions and Product End of Life Notification

The **Data versions** area on the right shows the current versions of the definition files being used by the program.

In addition, if the version of Security Controls that you are using is nearing its end of life (EOL) date, the EOL date will be displayed. No new updates to the data files will be provided after the EOL date, rendering the program ineffective. You should upgrade to the latest version of the program well in advance of the EOL date. As an aid, if an EOL date has been announced for your version of the program, a notification will be displayed when you start Security Controls. The notification will indicate when the version will expire and it will provide a link to get the latest version.

453. Viewing Details of Linux Packages

From the **Linux patches** tab on the middle pane of the Machine View or from either the **Linux Patch Group** or the **Linux Patch Group Editor** dialog, you can click **View packages** to display more information about the packages associated with an advisory. The indicators display the status of each package.

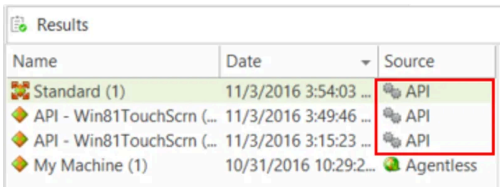
> For a specific advisory applying to a specific machine, the metadata from the contentless Linux engine reports all the packages already installed on the machine that are related to that advisory. All required packages will be listed. However, there could be other optional packages (for example, debug versions, symbols, localizations, etc) that could also apply to this advisory that are not installed on that machine and so are not reported.
>
> This means that if another machine that already has any of these optional packages installed on it is scanned by the contentless agent, these packages will be included in the results. This will make it look like the same advisory requires different packages depending on which machine you viewed it from.

454. Viewing and Tracking API-Driven Actions

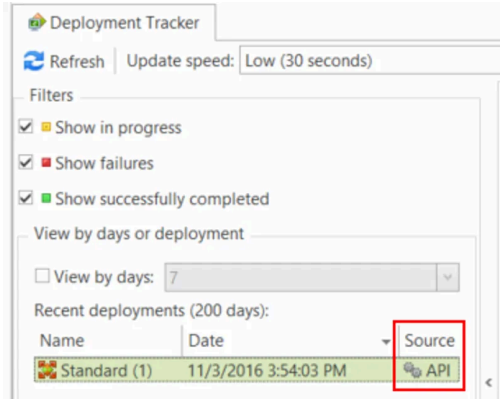
Actions that you drive from the API will be reflected in the Security Controls user interface. They are labeled to distinguish between API-initiated runs and console-initiated runs. Actions receive the same level of tracking regardless of whether they are initiated from the user interface or at the API level.

Examples

- The results of patch scans and deployments performed from the API are identified within the Results pane in the **Source** column.



Patch deployments performed from the API can be tracked using the **Operations Monitor** and **Deployment Tracker**.



455. Viewing Patch and Asset Summaries in Machine View

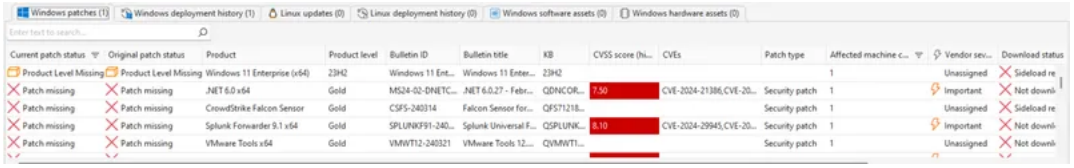
The middle pane displays general patch and asset information about the machine(s) selected in the top pane. If multiple machines are selected in the top pane, the middle pane will display information for all selected machines. For example, if you select multiple domains in the top pane, summary information about all the machines in all domains will be displayed.

You can customize the way information is displayed within this pane. See **Customizing the Column Headers** for information.

Tabs are used to divide the information into several distinct categories.

Windows patches

Displays patch status information for the Windows machines selected in the **top pane**. If you select an individual patch, detailed information about it is displayed in the **bottom pane**.



The **Affected machine count** column indicates how many of the selected machines are affected by a specific patch or product level.

A patch that is scheduled for deployment is considered to be still missing. This status will change after the patch is successfully installed.

The values for the **Installed patches** and **Missing patches** columns in the top pane may not always match the values shown in the middle pane. This is because the top pane counts every patch on every machine, while the middle pane counts only unique patches and ignores duplicates. You can use the **Affected Machines tab** in the bottom pane to determine if a particular patch is missing on multiple machines. Also, the middle pane breaks the patches into different categories and does not consider patches that are scheduled for installation or that are pending a reboot to be installed.

> You can right-click on any patch and perform a number of different actions. For more information, see **Performing Actions on Patches**.

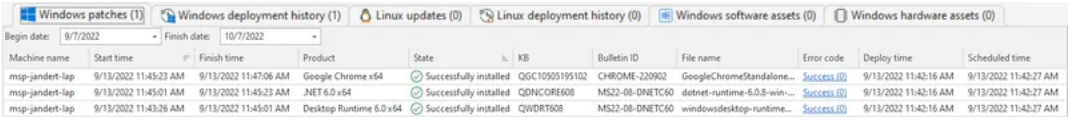
Column	Description
Current patch status	The current status of the patch. This may be different from the status of the patch when the scan was originally performed. (For example, the patch may have been deployed since the scan was originally performed.). The indicators display the status.
Original patch status	Indicates the patch status at the time the patch scan was performed. The indicators display the status.
Product	The software product affected by this patch.
Product level	The product level of the patch. For original patches the level will be Gold.
Bulletin ID	Identifies the Microsoft Security Bulletin article that describes the threat addressed by the patch.
Bulletin title	The descriptive title of the Microsoft Security Bulletin article that describes the threat addressed by the patch.
KB	The knowledge base number used to identify the Microsoft-based patch.
CVSS score (highest)	The highest Common Vulnerability Scoring System (CVSS) score of all CVEs associated with this patch. The more a vulnerability is validated by the vendor or other reputable sources, the higher the score.
CVEs	The **Common Vulnerabilities and Exposures (CVEs)** that are associated with the patch.

Column	Description
Patch type	Indicates the patch type. The possible types are: • **Non-security Patches:** The set of patches supported by Microsoft Software Update Services • **Security Patches:** Security bulletin-related patches • **Security Tools:** Patches for the malware tool provided by Microsoft Corporation • **Software Distribution:** Free third-party products that can be deployed by Security Controls
Affected machine count	Indicates the number of machines that are missing the patch. This number only applies to those machines that are selected in the top pane.
Vendor severity	One of four severity levels assigned by Ivanti based on the perceived threat of the vulnerability related to the patch. • (Red): Ivanti has deemed the problem associated with this patch to be **Critical** in nature. • (Orange): Ivanti considers the problem related to this patch **Important** to correct. • (Yellow): The related vulnerability is of **Moderate** severity. • (Gray): Ivanti has not assigned a severity level to this problem.
Download status	Indicates if the patch has been downloaded to the patch download directory. Some patches may require sideloading.
File name	The name of the patch file.
EOL	The date that the software product affected by the patch will be designated as at End-of-Life by the vendor.
Uninstallable	Indicates if the patch can be uninstalled. Uninstalling a patch restores a machine to its original state before the patch was deployed. Patches must be uninstalled in the reverse order in which they were installed.
Bulletin release date	The original publication date of the security bulletin that identifies the vulnerability.
Comment	A user-supplied comment about the patch.
Detected culture	The local form of the operating system language detected on the target machine.
Download method	Indicates if the patch can be downloaded automatically by the program or if it must be downloaded manually. There may be a number of different reasons why a patch cannot be automatically downloadable. For example, you may have a patch that was created for a proprietary software program, or you may receive patches for a program that is no longer officially supported by the vendor.

Column	Description
	If the value in this column is **Automatic**, it means that Security Controls can download the patch automatically. If the value is **Acquire from vendor** or some other value, it means that you must manually download the patch on your own and then move it into the **patch download directory** using the **sideload process**. Once the patch is there it can be deployed using the normal deployment process.
File size	The patch file size.
IAVA ID	This column is available only if you have a **Government Edition of Security Controls**. The number used to identify patches in the Information Assurance Vulnerability Alert **(IAVA) XML file** compiled by the U.S. Government.
Patch release date	The date the patch was originally published.
Patch updated	The date an updated version of the patch was published.
Replaced by	The bulletin ID that identifies a more recent update for the vulnerability.

Windows deployment history

Displays patch deployment information for the Windows machines selected in the top pane.

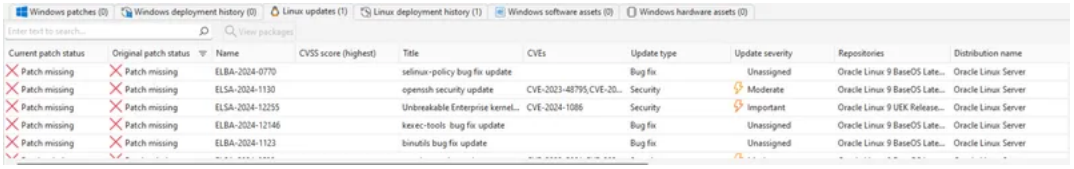


Use the **Begin date** and **Finish date** boxes to specify the range of dates that will be displayed. By default the range will be 30 days and will begin on the date you first accessed Machine View. Be sure to update the date range as needed to view the latest deployments.

You can right-click on one or more patches and export the deployment information to a CSV file.

Linux updates

Displays update status information for the Linux machines selected in the **top pane**. If you select an individual update, detailed information about it is displayed in the **bottom pane**. Some columns are specific to contentless or content-based patching, so not all fields will contain values.



For more details about the packages associated with an advisory, select it in the list, then click **View packages**. For more information, see **Viewing Details of Linux Packages**.

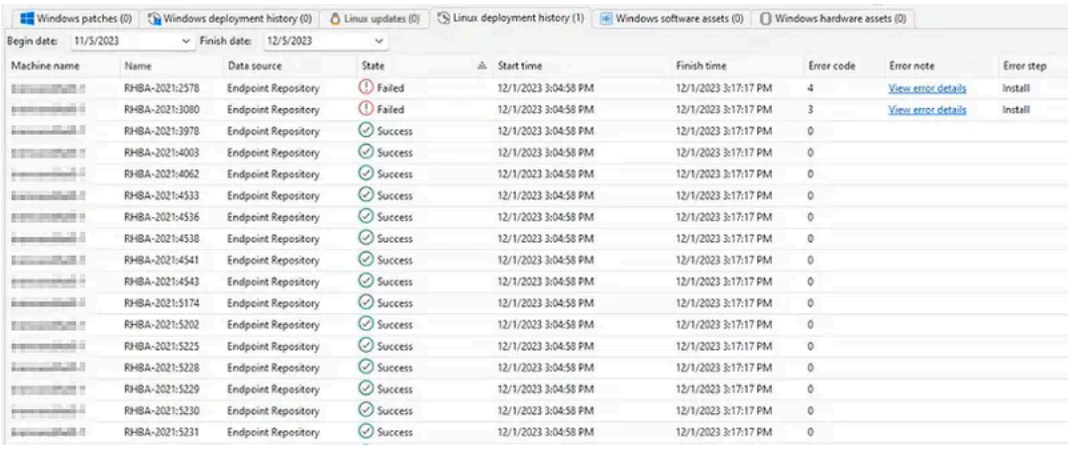
> You can right-click on any update and perform a number of different actions. For more information, see **Performing Actions on Patches**.

Column	Description
Current patch status	The current status of the patch. This may be different from the status of the patch when the scan was originally performed. (For example, the patch may have been deployed since the scan was originally performed.) The indicators display the status.
Original patch status	Indicates the patch status at the time the patch scan was performed. The indicators display the status.
Advisory name	Identifies the package name or the security advisory or bug advisory that describes the threat addressed by the patch.
CVSS score (highest)	The highest Common Vulnerability Scoring System (CVSS) score of all CVEs associated with this patch. The more a vulnerability is validated by the vendor or other reputable sources, the higher the score.
CVEs	The **Common Vulnerabilities and Exposures (CVEs)** that are associated with the patch.
Patch type	Indicates the patch type. The possible types are: • **Security :** Security advisory-related patches • **Enhancement:** Patches that provide product enhancements • **Bug:** Patches that fix known bugs

Column	Description
Patch severity	One of four severity levels assigned to the update based on the perceived threat of the vulnerability related to it. For contentless patching, these are defined in the distribution's repository and for content-based patching they are defined by Ivanti. • (red): **Critical** • (orange): **Important** • (yellow): **Moderate** • (gray): no severity assigned
Repositories (Contentless only)	The repository associated with the package.
Distribution name	Identifies the version of Linux that is affected by the patch.
Data source	Identifies the source of the data: • **Endpoint Repository:** uses the new patching method • **Ivanti Content:** uses the Content-Based Linux patching method
Affected machine count	Indicates the number of machines that are missing the patch. This number only applies to those machines that are selected in the top pane.
Patch name (Content-Based only)	The name of the RPM file.
Package count	Indicates the number of packages that are affected by a specific patch or advisory.
Issued date	The original publication date of the advisory that identifies the vulnerability.
Revised date	The latest publication date of the advisory that identifies the vulnerability.
Replaced by (Content-Based only)	The advisory ID that identifies a more recent update for the vulnerability.
Requires reboot	Specifies whether a reboot is required after the patch is deployed.

Linux deployment history

Displays patch deployment information for the Linux machines selected in the top pane.



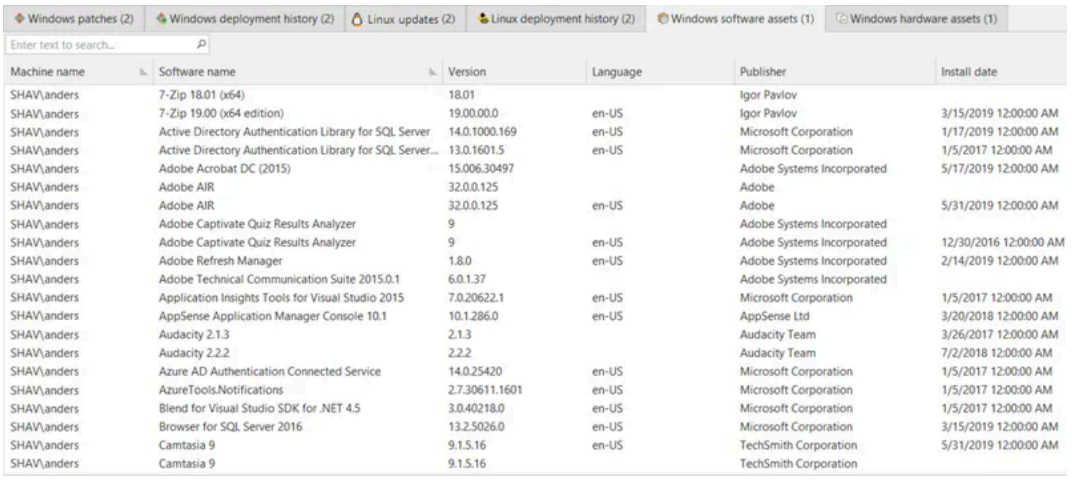
Use the **Begin date** and **Finish date** boxes to specify the range of dates that will be displayed. By default the range will be 30 days and will begin on the date you first accessed Machine View. Be sure to update the date range as needed to view the latest deployments.

You can right-click on one or more patches and export the deployment information to a CSV file.

If a deployment fails and additional error information is available, a **View error details** link is provided in the **Error note** column.

Windows software assets

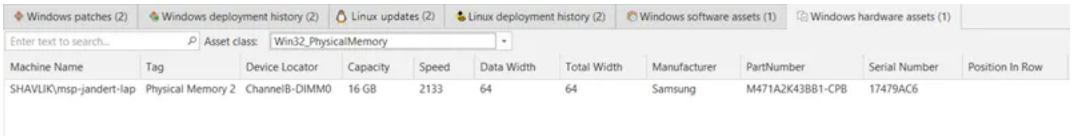
Displays software asset scan information for the Windows machines selected in the top pane. You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.



Windows hardware assets

Displays **hardware asset scan** information for the Windows machines selected in the top pane. The information that is displayed is dependent on the platform and on the product vendor. Not all vendors make every piece of information available so some columns may be blank. You can customize the way information is displayed within this pane. See **Customizing the Column Headers** for information.

> Results are not available for virtual machines that were offline at the time of a scan.



Filtering the Contents

You can use a filter to specify the type of hardware information that is displayed. The number of filters available within the **Filter by** box is dependent on the hardware components that were enabled on the **asset scan template** used to perform the scan.

456. Viewing Asset Scan Results

Asset scan results are available within **Machine View**.

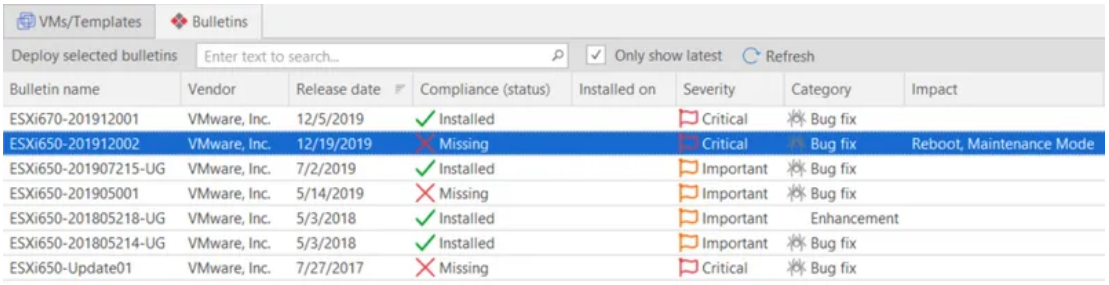
457. Viewing Bulletin Status

The **Bulletins** tab displays the status of the security bulletins that have been issued for the ESXi hypervisor(s) selected in the top pane. If multiple hypervisors are selected in the top pane, this tab will display bulletin information for all selected hypervisors.

A bulletin that is scheduled for deployment is considered to be still missing. This status will change after the bulletin is successfully installed and the screen is refreshed.

You can export the bulletins by right-clicking the list, then clicking **Export bulletins to CSV**.

You can customize the way information is displayed within this tab. See **Customizing the Column Headers** for information.



Field	Description
Deploy selected bulletins	See **How to Deploy Bulletins to Your Managed Hypervisor**.
Search	Enables you to search for bulletins contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those bulletins that match the search criteria are displayed; all other bulletins are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the **Bulletin Name** column. • All partial matches are displayed. For example, if you search for bulletins named *Test*, any bulletin with "test" in its name will be considered a match (e.g. Testbulletin1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
Only show latest	If enabled, filters the contents of the tab so that the only bulletins displayed are those that are not replaced by newer bulletins. Use this check box to identify the vulnerabilities that have not yet been addressed.
Refresh	Updates the bulletin information that is displayed on the tab.
ESXi Hypervisor	The name or IP address of the ESXi hypervisor.
Bulletin Name	The bulletin name.
Vendor	Identifies the name of the vendor that released the bulletin.
Release Date	The original publication date of the bulletin that corrects this vulnerability.
Compliance (Status)	Indicates the bulletin status at the time the scan was performed.
Installed On	Shows the date and time that the bulletin was installed. This information will not be available if the bulletin was installed using a different Security Controls database or if the bulletin was not installed by Security Controls.
Installed By	Shows the name of the user who installed the bulletin. This information will not be available if the bulletin was installed using a different Security Controls database or if the bulletin was not installed by Security Controls.
Severity	Indicates the severity level of the vulnerability that is corrected by this bulletin. The severity level can be one of the following:

Field	Description
	• **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. • **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. • **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. • **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
Category	The bulletin category can be one of the following: • **Security:** The bulletins that belong to this category fix one or more potential security vulnerabilities. The bulletin may also contain bug fixes. • **Bug fix:** The bulletins that belong to this category contain one or more bug fixes. • **Other:** For backward compatibility. For example, for updates without a category specified or for obsolete categories.
Impact	Indicates the impact that applying the bulletin will have on the virtual machine and hypervisor.
Replaced By	The bulletin that contains a more recent update for the vulnerability.
Summary	Provides a short description of the bulletin.

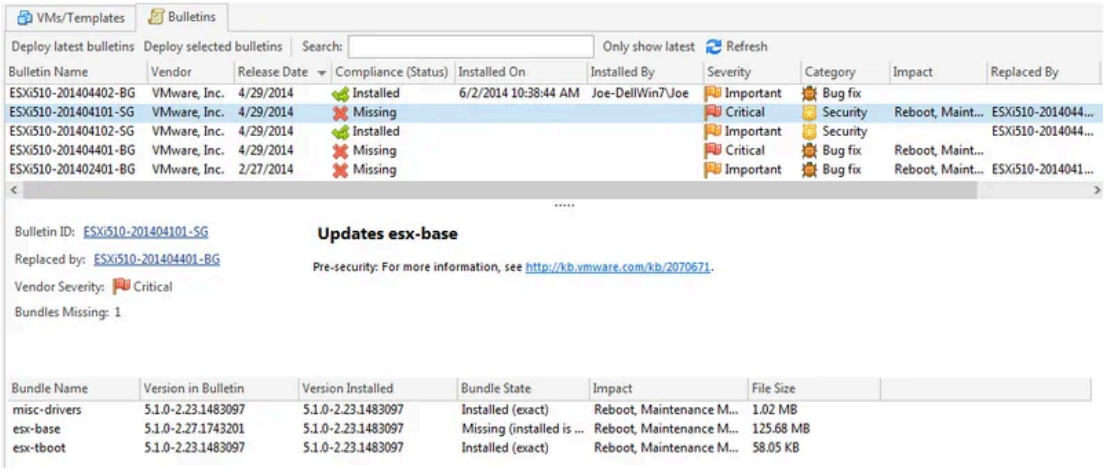
458. Viewing Bulletin Status on Unmanaged Hypervisors

The **Bulletins** tab displays the status of the security bulletins that have been issued for the selected ESXi hypervisor. If you select a bulletin, information about it is displayed in the bottom pane.

A bulletin that is scheduled for deployment is considered to be still missing. This status will change after the bulletin is successfully installed and the screen is refreshed.

You can export the bulletins by right-clicking the list, then clicking **Export bulletins to CSV**.

You can customize the way information is displayed within this tab. See **Customizing the Column Headers** for information.

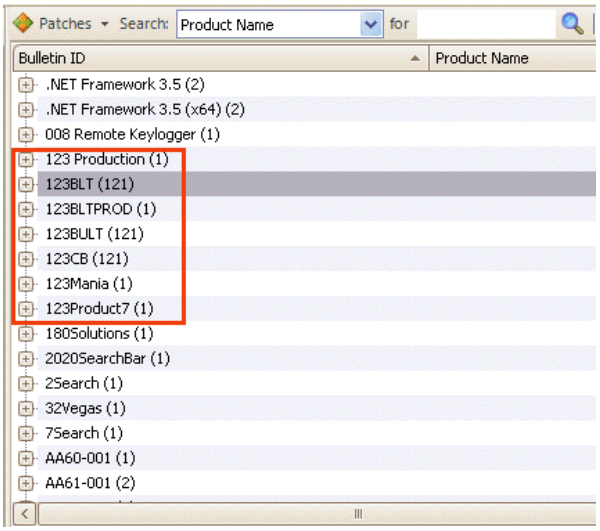


Field	Description
Deploy latest bulletins **Deploy selected bulletins**	See Deploying Bulletins to Unmanaged ESXi Hypervisors.
Search	Enables you to search for bulletins contained on the tab. To initiate a search you simply type the search criteria in the **Search** box. Only those bulletins that match the search criteria are displayed; all other bulletins are hidden. • The Search tool works only on the information currently visible on the tab. • The search will be performed on all information on the tab, not just the **Bulletin Name** column. • All partial matches are displayed. For example, if you search for bulletins named *Test*, any bulletin with "test" in its name will be considered a match (e.g. TestBulletin1, Contest, etc.). • The use of wildcards in the Search tool is not allowed.
Only show latest	If enabled, filters the contents of the tab so that the only bulletins displayed are those that are not replaced by newer bulletins. Use this check box to identify the vulnerabilities that have not yet been addressed.
Refresh	Updates the information that is displayed on the tab.
Bulletin Name	The bulletin name.
Vendor	Identifies the name of the vendor that released the bulletin.
Release Date	The original publication date of the bulletin that corrects this vulnerability.
Compliance (Status)	Indicates the bulletin status at the time the bulletin scan was performed.
Installed On	Shows the date and time that the bulletin was installed. This information will not be available if the bulletin was installed using a different Security Controls database or if the bulletin was not installed by Security Controls.
Installed By	Shows the name of the user who installed the bulletin. This information will not be available if the bulletin was installed using a different Security Controls database or if the bulletin was not installed by Security Controls.
Severity	Indicates the severity level of the vulnerability that is corrected by this bulletin. The severity level can be one of the following:

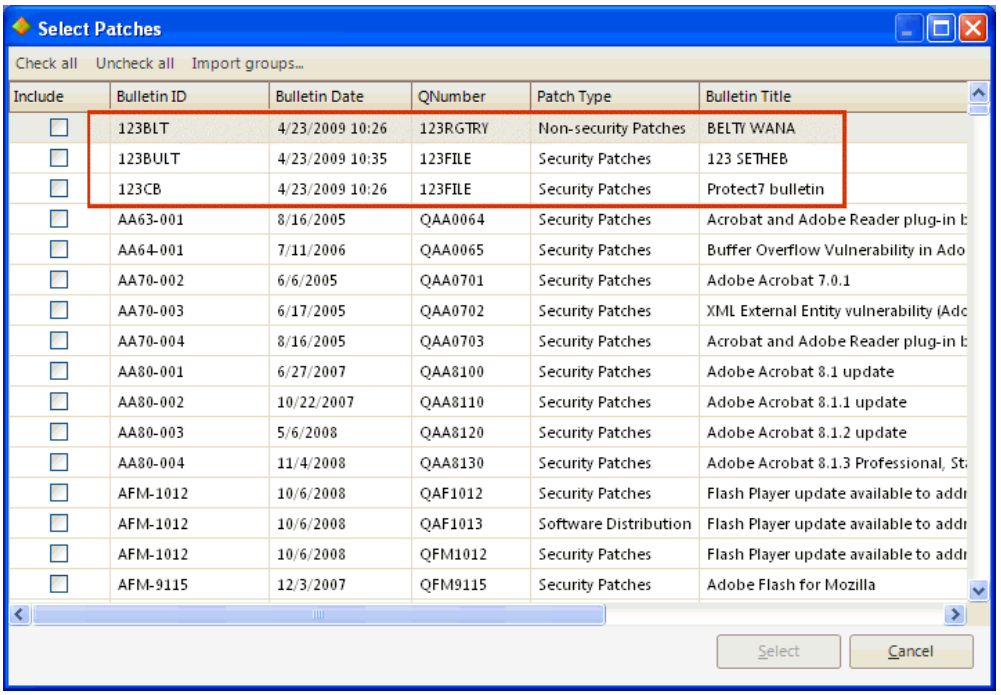
Field	Description
	• **Critical:** Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest/host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, availability user data, or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host. • **Important:** Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws could allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service. • **Moderate:** Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations. • **Low:** All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
Category	The bulletin category can be one of the following: • **Security:** The bulletins that belong to this category fix one or more potential security vulnerabilities. The bulletin may also contain bug fixes. • **Bug fix:** The bulletins that belong to this category contain one or more bug fixes. • **Other:** For backward compatibility. For example, for updates without a category specified or for obsolete categories.
Impact	Indicates the impact that applying the bulletin will have on the virtual machine and hypervisor.
Replaced By	The bulletin that contains a more recent update for the vulnerability.
Summary	Provides a short description of the bulletin.

459. Viewing Custom Patches and Products

Once a custom XML file is used within a scan, the custom products and patches defined within the custom XML file will be displayed in Patch View.



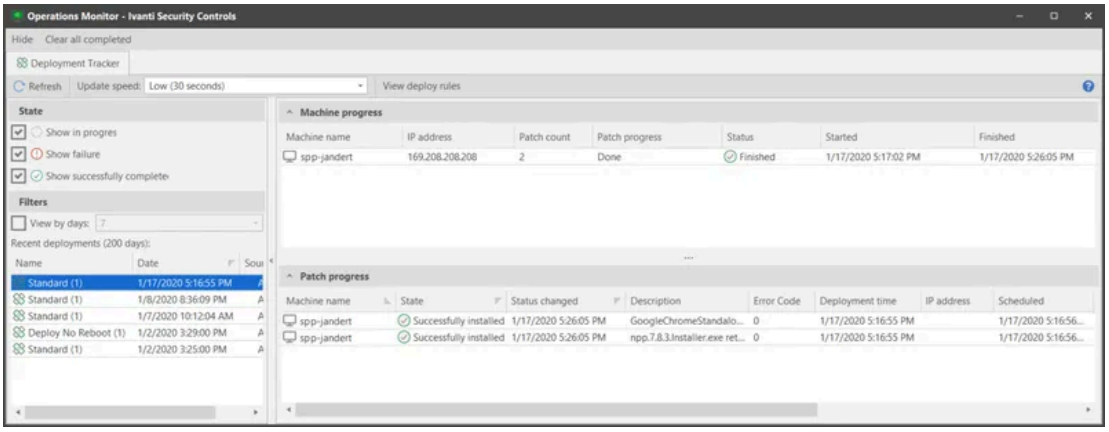
They will also be displayed when adding patches to a patch group.



Be careful though. Just because a custom product or patch is displayed in Patch View or in a patch group doesn't guarantee it is still being used in scans and deployments. It only indicates that the custom product or patch was at some point included in a scan or deployment. If you remove a custom XML file from the list of active custom XML files (see **Specifying Which Custom XML Files to Use**), the products and patches within that custom XML file will not be used in subsequent scans and deployments. A custom XML file must be active in order to be used.

460. Viewing Deployment Results

If you select a deployment from the **Results** list in the navigation pane, details about the deployment are displayed on the Deployment Tracker tab within the Operations Monitor. The top pane displays a list of the machines involved in the deployment and shows how many patches each machine received. The lower pane provides information about how the patches were deployed. For more information, see **About the Deployment Tracker Dialog**.



Deployment results are also reflected on a machine basis within Machine View. For more information, see **Viewing Patch and Asset Summaries**.

461. Viewing ESXi Hypervisor Deployment Results

There are three places to view the results of a bulletin deployment to an ESXi hypervisor.

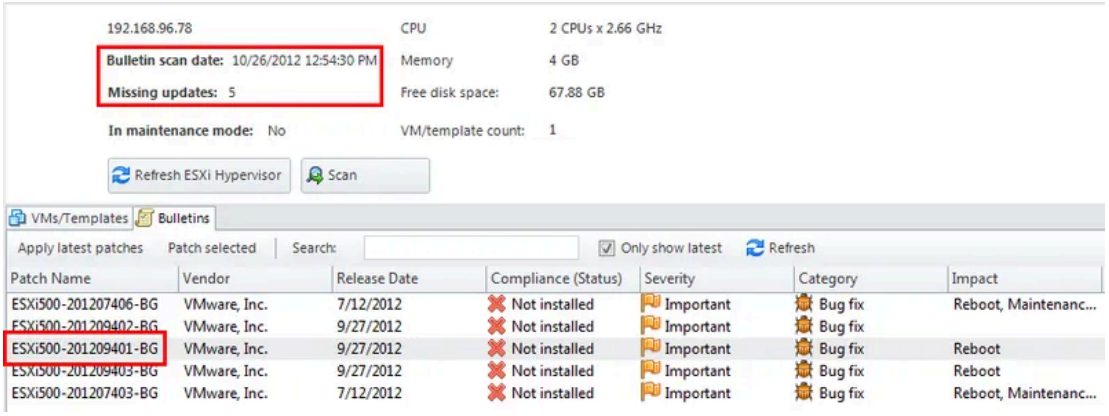
- From the Operations Monitor
- From the Event History log
- From the ESXi hypervisor **Bulletins** tab

Using the Bulletins Tab to View Bulletin Deployment Results

While viewing a vCenter Server or an ESXi hypervisor, select **View > Refresh** to see the most current information. The information in the header area and on the **Bulletins** tab will be updated to reflect the successful bulletin deployment.

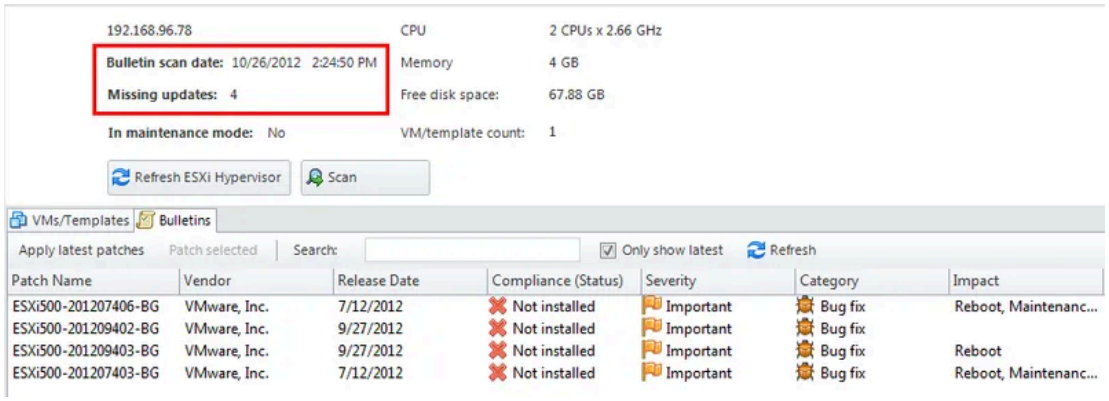
Example: Before deployment

The ESXi hypervisor shown here is missing five bulletins, including bulletin **ESXi500-201209401-BG**. To simplify things the **Only show latest** check box is enabled, which means that the only bulletins being displayed are those that have not been replaced by newer bulletins and whose vulnerabilities have not been addressed.



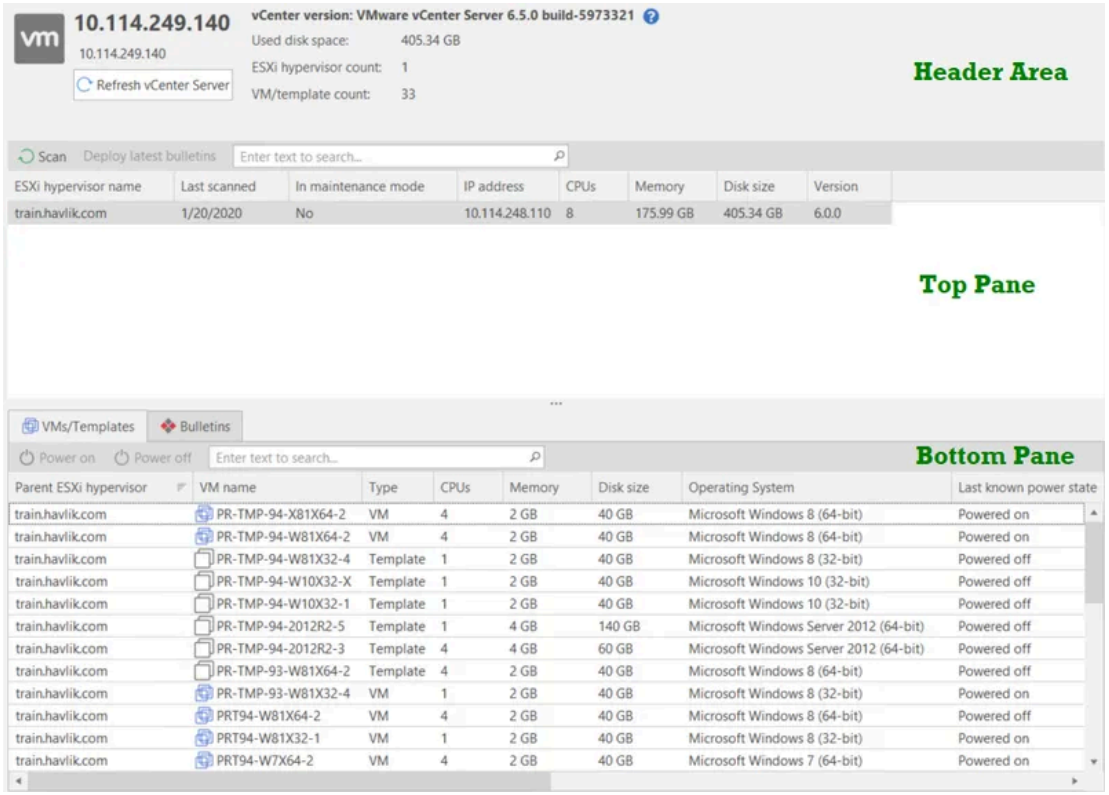
Example: After deployment

The ESXi hypervisor is now missing only four bulletins, and bulletin **ESXi500-201209401-BG** is no longer included in the list. Note that the **Bulletin scan date** information has also changed; this is because a new bulletin scan is one of the last steps that are performed during the bulletin deployment process.



462. Viewing Information About a vCenter Server

When you right-click a vCenter Server then click **View** in the Virtual Inventory list, information about that vCenter Server is displayed in a header area and in two panes. Both panes display unique information and provide unique functionality. The two panes are interrelated—the information presented in the bottom pane is dependent on what is selected in the top pane. This "top down" approach means you use the top pane to view overview information about the hypervisors being managed by the vCenter server, and you use the bottom pane to drill down to more detailed information about specific hypervisors.



- The header area provides basic configuration information about the selected vCenter server.
- The top pane displays the ESXi hypervisors that are being managed by the selected vCenter Server. See the following topics for information on using the top pane:
  - Searching the List of Hypervisors
  - Scanning One or More Hypervisors
  - Deploying Bulletins to a Hypervisor
  - Customizing the Column Headers

The bottom pane contains two tabs: The **VMs/Templates** tab displays information about the virtual machines and virtual machine templates that are contained on the selected ESXi hypervisor(s). The **Bulletins** tab shows the status of the security bulletins that have been issued for the selected hypervisor(s). See the following topics for information on using the bottom pane:

  - Powering On and Off the Virtual Machines and Virtual Machine Templates
  - Adding the Virtual Machines to a Machine Group
  - Searching the List of Virtual Machines
  - Applying Missing Bulletins to an ESXi Hypervisor

- Customizing the Column Headers

463. Viewing Machines Affected by a Selected Patch

The **Affected Machines** tab in the bottom pane displays which of your **managed machines** are affected by the patch that is selected in the top pane. The listed machines will be in one of two lists:

- **Missing:** These machines are vulnerable to the threat corrected by the patch.
- **Installed:** These machines already contain the selected patch.

Managed machines that are not listed are not affected by the selected patch.



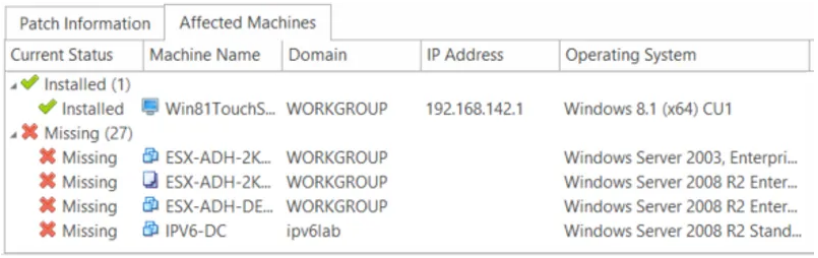
The **Affected Machines** table can be sorted and customized. See **Customizing The Patch View Column Headers** for more information.

464. Viewing Machines Affected by a Selected Patch

The **Affected Machines** tab in the bottom pane displays which of your selected **managed machines** are affected by the patch that is selected in the middle pane. The listed machines will be in one of two lists:

- **Missing:** These machines are vulnerable to the threat corrected by the patch.
- **Installed:** These machines already contain the selected patch.

Managed machines that are not listed are not affected by the selected patch.



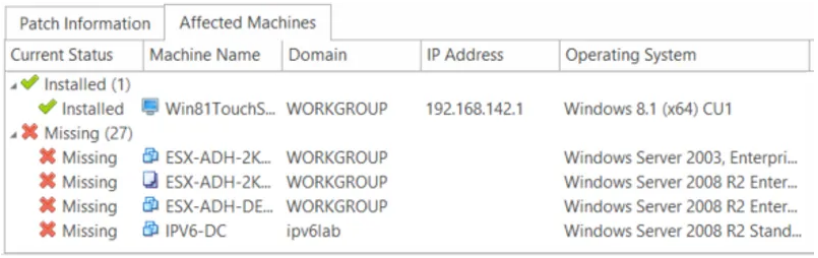
The **Affected Machines** table can be sorted and customized. See **Customizing The Patch View Column Headers** for more information.

465. Viewing Machines Affected by a Selected Patch

The **Affected Machines** tab in the bottom pane displays which of your selected **scanned machines** are affected by the patch that is selected in the middle pane. The listed machines will be in one of two lists:

- **Missing:** These machines are vulnerable to the threat corrected by the patch.
- **Installed:** These machines already contain the selected patch.

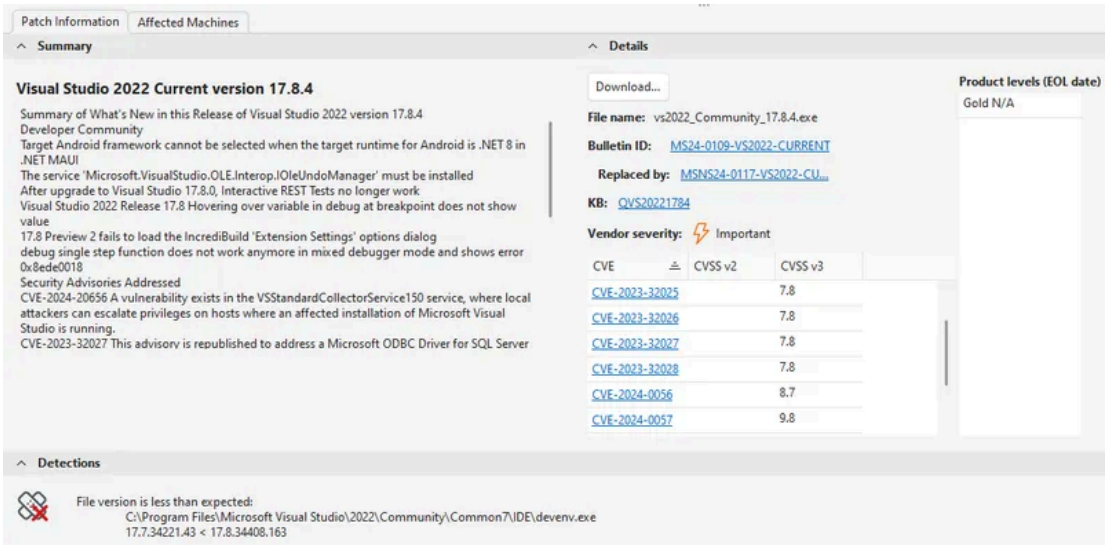
Managed machines that are not listed are not affected by the selected patch.



The **Affected Machines** table can be sorted and customized. See **Customizing the Patch View Column Headers** for more information.

466. Viewing Patch Information

The **Patch Information** tab in the bottom pane displays detailed information about the patch, product level, or informational item selected in the middle pane. Detailed information will not be displayed if multiple patch items are selected in the middle pane.

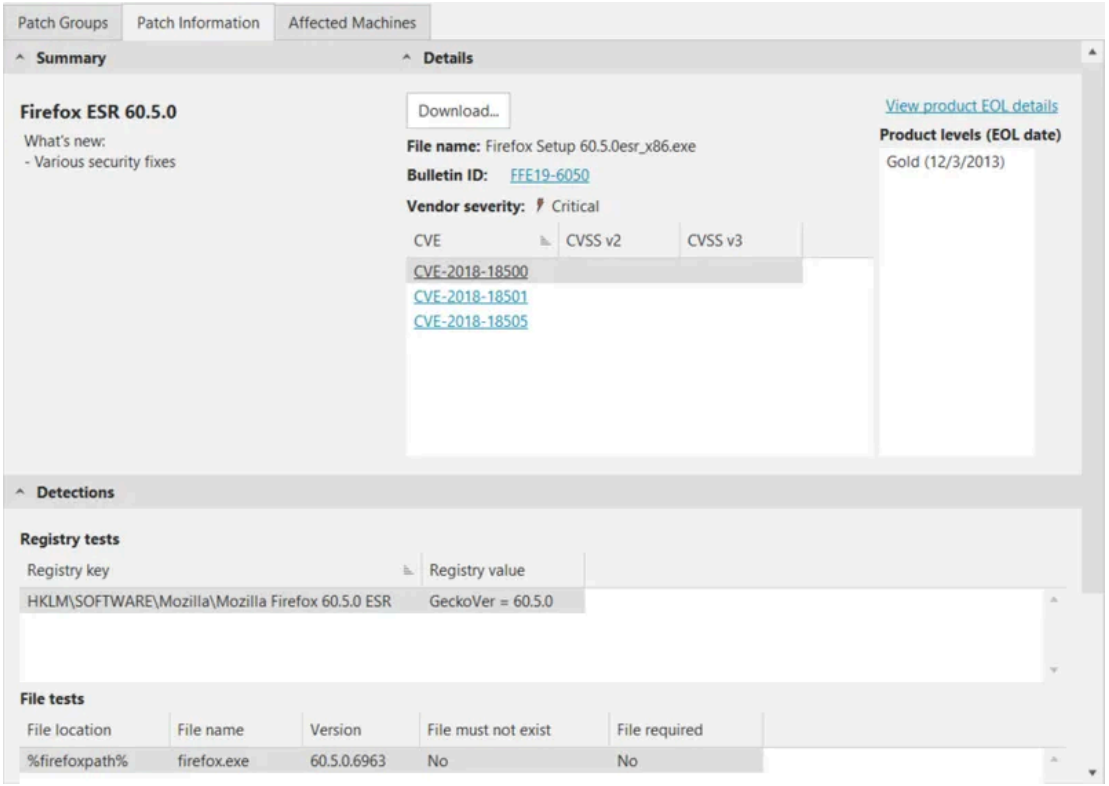


Field	Description
Summary	Provides a concise description of the threat addressed by this patch.
Comments	If shown, provides comments from Ivanti about this patch.
Download	Enables you to download the patch to the patch download directory. When you click this button the **Patch Download Status** dialog is displayed. Use this dialog to select which language version of the patch you want to download. On the dialog, if the download icon is grayed out () it indicates the patch has not yet been downloaded. If the icon is green () it indicates the patch has already been downloaded and verified.
Bulletin ID	Provides a link to the Microsoft Security Bulletin article that describes the threat addressed by this patch.
Replaced by	If shown, indicates that the patch is replaced by another more recent patch.
KB	Provides a link to the associated Knowledge Base article that provide more information about the flaw.
Vendor Severity	(Red) Ivanti has deemed the problem associated with this patch to be Critical in nature. (Orange) Ivanti considers the problem related to this patch Important to correct. (Yellow) The related vulnerability is of Moderate severity. (Gray) While it poses a security risk, Ivanti deems that risk to be Low. Ivanti assigns one of four severity levels based on its perceived threat of the vulnerability related to the patch.

Field	Description
Product Levels (EOL date)	If shown, indicates that the patch is contained in one or more product levels. Also indicates the End Of Life (EOL) date for the product level.
Description	Identifies the product that is affected by this patch, and describes how the product is vulnerable.
Registry Key table	Identifies the registry key information used to determine whether the product in question exists on the target machines. This table can be sorted by clicking within a column header.
File Location table	Shows the file criteria used for determining whether or not a patch is installed. This table can be sorted by clicking within a column header.

467. Viewing Patch Details

The **Patch Information** tab in the bottom pane displays detailed information about the patch, product level, or informational item selected in the top pane. Detailed information will not be displayed if multiple patch items are selected in the top pane.



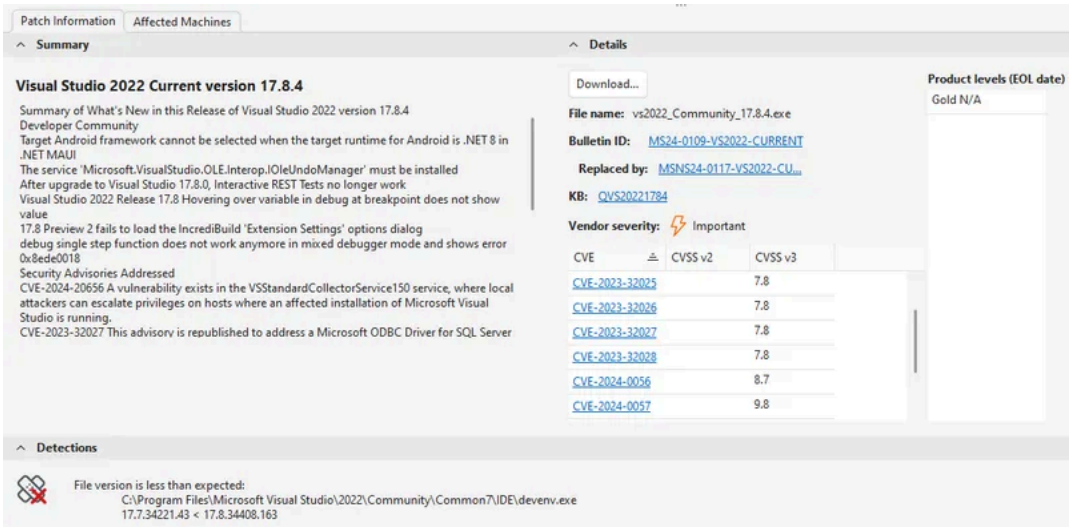
Field	Description
Replaced by	If shown, indicates that the patch is replaced by another more recent patch.
Summary	Provides a concise description of the threat addressed by this patch. It identifies the product that is affected by this patch and describes how the product is vulnerable.
Download	Enables you to download the patch to the patch download directory. When you click this button the **Patch Download Status** dialog is displayed. Use this dialog to select which language version of the patch you want to download. On the dialog, if the download icon is grayed out () it indicates the patch has not yet been downloaded. If the icon is green () it indicates the patch has already been downloaded and verified.
Bulletin ID	Provides a link to the Microsoft Security Bulletin article that describes the threat addressed by this patch.
KB	Provides a link to the associated Knowledge Base article that provide more information about the flaw.
Vendor Severity	(Red) Ivanti has deemed the problem associated with this patch to be Critical in nature. (Orange) Ivanti considers the problem related to this patch Important to correct. (Yellow) The related vulnerability is of Moderate severity. (Brown) While it poses a security risk, Ivanti deems that risk to be Low. Ivanti assigns one of four severity levels based on its perceived threat of the vulnerability related to the patch.
CVE number	Provides a cross reference to the Common Vulnerabilities and Exposures (CVE) database hosted by cve.org (CVEID).

Field	Description
Comments	If shown, provides comments from Ivanti about this patch.
View product EOL details	If shown, provides a link to a webpage that may supply additional End of Life information about the product.
Product levels (EOL date)	If shown, indicates that the patch is contained in one or more product levels. Also indicates the End Of Life (EOL) date for the product level.
Registry Key table	Identifies the registry key information used to determine whether the product in question exists on the target machines. This table can be sorted by clicking within a column header.
File Location table	Shows the file criteria used for determining whether or not a patch is installed. This table can be sorted by clicking within a column header.

468. Viewing Patch Information

The **Patch Information** tab in the bottom pane displays detailed information about the patch, product level, or informational item selected in the middle pane. Detailed information will not be displayed if multiple patch items are selected in the middle pane.

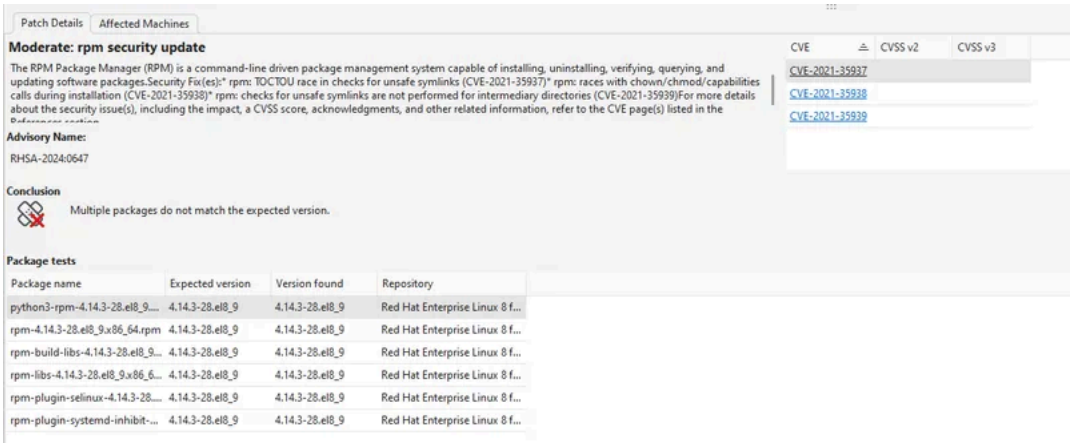
Windows Machines



Field	Description
Summary	Provides a concise description of the threat addressed by this patch.
Comments	If shown, provides comments from Ivanti about this patch.
Download	Enables you to download the patch to the patch download directory. When you click this button the **Patch Download Status** dialog is displayed. Use this dialog to select which language version of the patch you want to download. On the dialog, if the download icon is grayed out () it indicates the patch has not yet been downloaded. If the icon is green () it indicates the patch has already been downloaded and verified.
Bulletin ID	Provides a link to the Microsoft Security Bulletin article that describes the threat addressed by this patch.
Replaced by	If shown, indicates that the patch is replaced by another more recent patch.

Field	Description
KB	Provides a link to the associated Knowledge Base article that provide more information about the flaw.
Vendor Severity	(Red) Ivanti has deemed the problem associated with this patch to be Critical in nature. (Orange) Ivanti considers the problem related to this patch Important to correct. (Yellow) The related vulnerability is of Moderate severity. (Gray) While it poses a security risk, Ivanti deems that risk to be Low. Ivanti assigns one of four severity levels based on its perceived threat of the vulnerability related to the patch.
Product Levels (EOL date)	If shown, indicates that the patch is contained in one or more product levels. Also indicates the End Of Life (EOL) date for the product level.
Description	Identifies the product that is affected by this patch, and describes how the product is vulnerable.
Registry Key table	Identifies the registry key information used to determine whether the product in question exists on the target machines. This table can be sorted by clicking within a column header.
File Location table	Shows the file criteria used for determining whether or not a patch is installed. This table can be sorted by clicking within a column header.

Linux Machines



Field	Description
Summary **Advisory Name**	Provides a concise description of the threat addressed by this patch. The advisory name associated with this patch.
CVE	Shows the CVE IDs that are associated with this patch.
CVSS	Shows the Common Vulnerability Scoring System (CVSS) score for each CVE associated with this patch or package.
Package tests	Shows the file criteria used for determining whether or not a patch is installed. This table can be sorted by clicking within a column header. An option is available to right-click the patch test and assign the patch group or create a new patch group and assign the test.

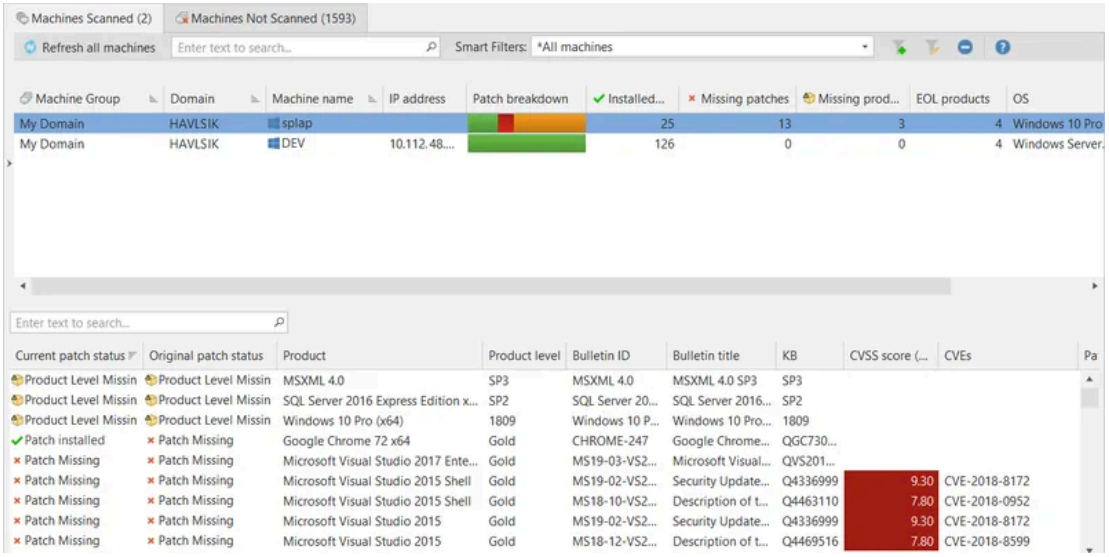
469. Viewing Patch Summaries in Scan View

The middle pane displays general patch information about the machine(s) selected in the top pane. If multiple machines are selected in the top pane, this pane will display patch information for all selected machines. For example, if you select two domains in the top pane, summary information about all the machines in both domains will be displayed. The **Affected Machine Count** column indicates how many of the selected machines are affected by a specific patch or product level.

The values for the **Installed Patch Count** and **Missing Patch Count** columns in the top pane may not always match the values shown in the middle pane. This is because the top pane counts every patch on every machine, while the middle pane counts only unique patches and ignores duplicates.

If you refresh Scan View during or after a patch deployment, the **Current Patch Status** column will reflect the new patch status. For example, in the following figure, the Google Chrome 72 patch that was originally detected as missing is now being reported as installed.

You can customize the way information is displayed within this pane. See Customizing the Column Headers for information.



Field	Description
Current patch status	The current status of the patch. This may be different from the status of the patch when the scan was originally performed. (For example, the patch may have been deployed since the scan was originally performed.)
Original patch status	Indicates the patch status at the time the patch scan was performed.
Product	The software product affected by this patch.
Product level	The product level of the patch. For original patches the level will be Gold.
Affected machine count	Indicates the number of machines that are missing the patch. This number only applies to those machines that are selected in the top pane.
Patch type	Indicates the patch type. The possible types are: • **Non-security Patches:** The set of patches supported by Microsoft Software Update Services • **Security Patches:** Security bulletin-related patches • **Security Tools:** Patches for the malware tool provided by Microsoft • **Software Distribution:** Free third-party products that can be deployed by Security Controls
Bulletin ID	Identifies the Microsoft Security Bulletin article that describes the threat addressed by the patch.
Bulletin title	The descriptive title of the Microsoft Security Bulletin article that describes the threat addressed by the patch.
Download method	Indicates if the patch can be downloaded automatically by the program or if it must be downloaded manually. There may be a number of different reasons why a patch cannot be automatically downloadable. For example, you may have a patch that was created for a proprietary software program, or you may receive patches for a program that is no longer officially supported by the vendor. If the value in this column is **Automatic**, it means that Security Controls can download the patch automatically. If the value is **Acquire from vendor** or some other value, it means that you must manually download the patch on your own and then move it into the patch download directory using the sideload process. Once the patch is there it can be deployed using the normal deployment process.
Download status	Indicates if the patch has been downloaded to the patch download directory. Some patches may require sideloading.
KB	The knowledge base number used to identify the Microsoft-based patch.
CVSS score	The highest Common Vulnerability Scoring System (CVSS) score of all CVEs associated with this patch. The more a vulnerability is validated by the vendor or other reputable sources, the higher the score.

Field	Description
(highest)	
CVEs	The **Common Vulnerabilities and Exposures (CVEs)** that are associated with the patch.
IAVA ID	This column is available only if you have a **Government Edition of Security Controls**. The number used to identify patches in the Information Assurance Vulnerability Alert **(IAVA) XML file** compiled by the U.S. Government.
Vendor severity	(Red) Ivanti has deemed the problem associated with this patch to be Critical in nature. (Orange) Ivanti considers the problem related to this patch Important to correct. (Yellow) The related vulnerability is of Moderate severity. (Gray) Ivanti has not assigned a severity level to this problem. One of four severity levels assigned by Ivanti based on the perceived threat of the vulnerability related to the patch.
Uninstallable	Indicates if the patch can be uninstalled. Uninstalling a patch restores a machine to its original state before the patch was deployed. Patches must be uninstalled in the reverse order in which they were installed.
File name	The name of the patch file.
File size	The patch file size.
EOL	The number of software products on the machine that have been designated as at End-of-Life by their vendor.
Bulletin release	The original publication date of the security bulletin that identifies the vulnerability.

Field	Description
date	
Comment	A **user-supplied** comment about the patch.
Detected culture	The local form of the operating system language detected on the target machine.
Download file name	The file name used by Security Controls when downloading and deploying the patch. The name may include a three letter identifier that specifies the operating system language supported by the patch.
Patch release date	The date the patch was originally published.
Patch updated	The date an updated version of the patch was published.
Replaced by	The bulletin ID that identifies a more recent update for the vulnerability.

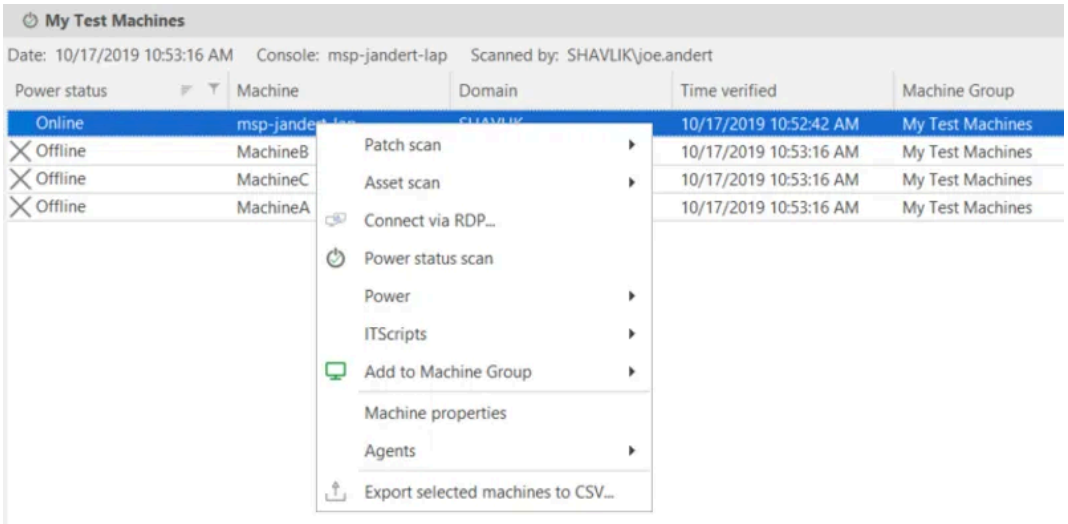
470. Viewing Power Status Scan Results

Power status scan results are available immediately following a successful scan by clicking the **View results** link on the **Operations Monitor** dialog (see Performing a Power Status Scan). The scan results are also available when you select a scan from the Results pane.

> TIP: Another option for viewing results is to generate a Power Status report.

You use the **Power Status** column to determine the current power state of the scanned machines. Machines will be categorized as either offline or online. The summary table contains a number of other columns that uniquely identify each machine. You can click on a column heading to sort the table by that information. You can also specify what information is presented by right-clicking the table heading and using **Column Chooser** to add or clear items.

Finally, you can right-click one or more machines and perform the following actions:

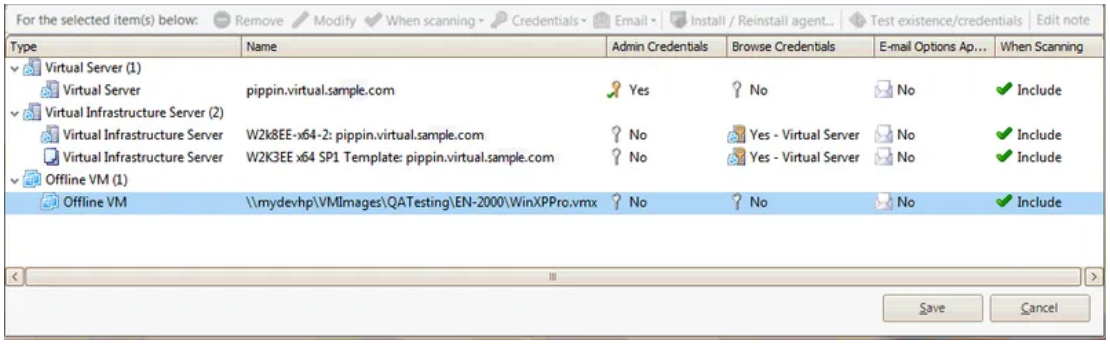


Field	Description
Patch Scan	Enables you to initiate a patch scan of the selected machines using any of the available patch scan templates.
Asset Scan	Enables you to initiate an asset scan of the selected machines using any of the available asset scan templates.
Connect via RDP	Enables you to make a Remote Desktop connection to the selected machine. See **How to Initiate a Remote Desktop Connection** for more details.
Power status scan	Enables you to perform a **power status scan** on the selected machines.
Power	Enables you to modify the power state of the selected machines. You can immediately restart, shut down, or awaken the machines, or you can use a power state template to schedule a reboot of the machines and leave them in a particular state (fully powered on, in sleep mode, in hibernate mode, or powered off). See **How to Initiate Power Management Tasks** for more information.
ITScripts	Enables you to either open a Windows PowerShell™ prompt or select and execute an approved script. See **How to Execute a Script** for details.
Add to Machine Group	Enables you to add the selected machines to a new machine group or to an existing machine group. See **Creating A New Machine Group** for more information. IMPORTANT! Machines you add to the machine group are automatically assigned the associated machine credentials. (**Hosted virtual machines** are the exception, they are assigned the last known machine group credentials.) If no machine credentials are available, no credentials will be assigned and the **default credentials** will be used in any subsequent scans. If the default credentials are not valid for the machines, and if the account credentials of the person currently logged on to the program are also not valid for the machines, scans of the machines you just added to the group will fail. To prevent scanning errors, always supply credentials for machines you add to a machine group. See **Supplying Credentials** for more information.
Machine Properties	Enables you to view and edit machine properties. See **Managing Individual Machine Properties** for more information.
Agents	Enables you to: • **Install** an agent, assign a different policy to the agent, or **uninstall** an agent. • Send a number of different commands to the selected agents. The commands apply only to machines that already have agents installed, that are online, and that are configured to be **listening agents**. See the **Send command** description for detailed information about the available commands. • **(Machine View only)** Initiate any of the tasks currently defined within the selected agents. When you select a task a confirmation dialog is displayed. If you choose to continue, the task is immediately started on the agent machines. See **Creating a New Agent Policy** for information on the types of tasks that may be available.

Field	Description
Export selected machines to CSV	Export information about the selected machines to a Comma Separated Values (CSV) file. The CSV file can then be used within a spreadsheet program.

471. Viewing Servers and Virtual Machines in a Machine Group

When servers, virtual machines, and virtual machine templates are added to a machine group, the new entries are displayed within the bottom section of the machine group dialog.



The recommended best practice is to always supply credentials for the VMware servers, the **virtual machine templates**, and the workstation virtual machines. See **Supplying Credentials** for details. Be careful if you have multiple console administrators, as different administrators are likely to provide different server credentials.

472. Virtual Machine Overview

Show Me!

A video tutorial is available on this topic. To access the video, click the following link:



Overview Information

> TIP: For information on managing and tracking the vCenter Servers and the ESXi hosts that are used in your organization, see **Introducing the Virtual Inventory Feature**.

A virtual machine is not actually a physical machine but rather a software environment (usually an operating system) designed to emulate a physical machine. A virtual machine can run programs just like a physical machine. The physical machine used to host the virtual machine can often support multiple virtual machines.

Security Controls can scan for and deploy patches to the virtual machines on your network regardless of whether they are online or offline. It can also perform a software asset scan of your online and offline virtual machines.

Online Virtual Machines

A virtual machine that is online and running is treated by Security Controls the same as a physical machine. Patch scans and asset scans will be performed in the same manner as on a physical machine. Any patches that may be missing can also be deployed in the same manner to both your physical machines and your online virtual machines. This means that your online virtual machines are protected by the latest software patches just like your physical machines.

Offline Virtual Machines

Security Controls also enables you to scan and patch offline virtual machines. Offline virtual machines are those that aren't powered on when a patch scan or an asset management scan is performed. These virtual machines may be powered on for only a few hours or days a month and then powered off until they are needed again the next month. It's important to ensure that these systems are patched so that when they are brought online they don't place your network at risk.

Security Controls makes it easy to scan these offline virtual machines. When you initiate a scan of a machine group that contains offline virtual machines, Security Controls will perform a full assessment of the offline virtual machines and display the scan results alongside the results for running systems. Offline virtual machines will be differentiated in the scan results by a unique icon (). The scan results may even identify offline virtual machines that you don't know about. When viewing machines in **Machine View** the **Offline Scan** column in the top pane will indicate if a virtual machine was offline at the time of the scan.

Patching offline virtual machines is similarly simple. You simply highlight the machines and patches you'd like to install and then select **Deploy** from the Security Controls menu. For offline virtual machines that are **hosted on a server**, the machines will be powered on, the patches installed, and the machines powered back down. For virtual machines that **reside on workstations**, the patches will be copied to the offline virtual machines and will be installed the moment that the virtual machine is started (or according to the scheduled patch deployment time).

Virtual Machine Templates

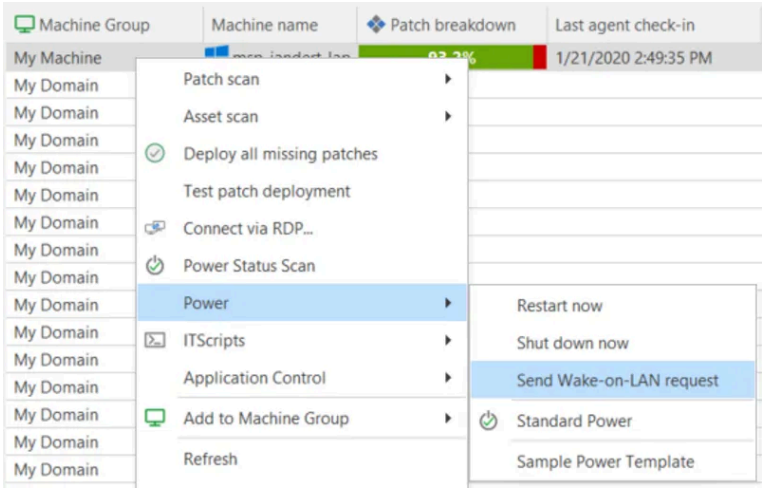
Virtual servers and virtual workstations are often created using a template. Templates enable you to quickly create new virtual machines that conform to your particular configuration requirements. A template that is offline poses no danger to your organization. A template that is brought online, however, is no different than an online virtual machine. It can perform tasks just like any other virtual machine, and it can also contain the same viruses, spyware, and other types of malware that target improperly patched machines. For this reason it is critical that your virtual machine templates receive the same patch management care as your physical and virtual machines.

Security Controls enables you to patch your virtual machine templates. You simply add your templates to a machine group and Security Controls will take care of the rest. For complete details on the virtual machine template scan and deployment process, see **Notes About Virtual Machine Templates**.

473. Wake-on-LAN Implementation Notes

IMPORTANT! You must perform a **hardware asset scan** on your target machines prior to initiating a WoL request. The scan is required in order to obtain the MAC address of each machine.

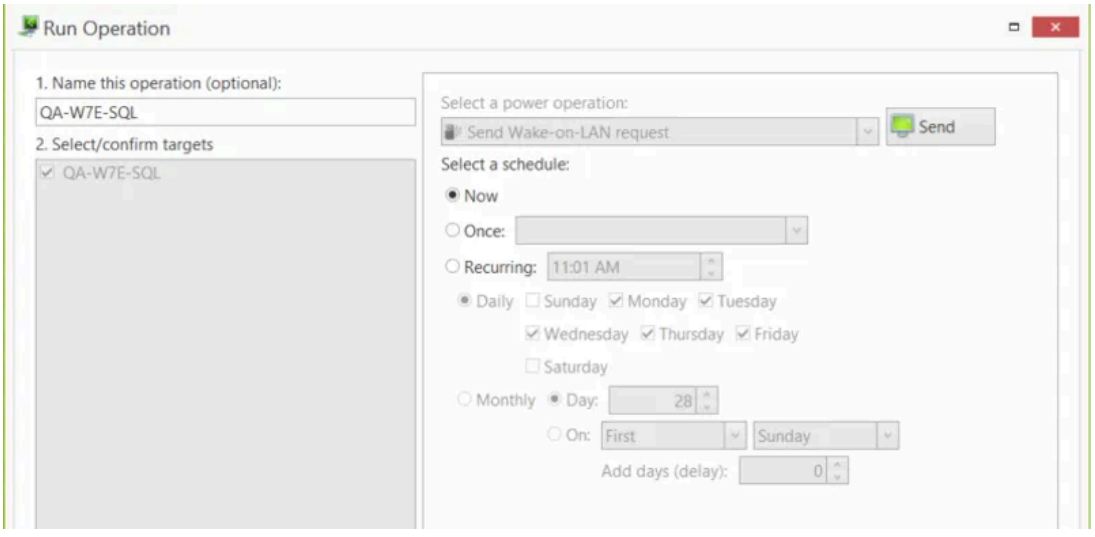
The Wake-on-LAN (WoL) feature is used to wake up machines that are powered off or in reduced power states. This is performed from Machine View or Scan View by using a **right-click command**.



Machines that are sleeping, hibernating, or powered off cannot be restarted or awakened using a power state template, they must be awakened using the Wake-on-LAN feature.

Any connected machine that is sleeping, hibernating, or powered off (but with power available to the network card) can be awakened by a WoL request. One typical reason for using WoL is to turn on machines that have been powered off overnight or over a long holiday weekend, making the machines ready for use for the coming work day. Another reason may be to power on machines prior to performing maintenance tasks such as console-based patch or asset scans. Machines that are sleeping, hibernating, or powered off cannot be scanned, so using the WoL feature ensures that your maintenance tasks will be performed on schedule.

The Wake-on-LAN request can be issued immediately, or it can be scheduled to awaken machines at a certain time. It's like scheduling a wakeup call for each machine.



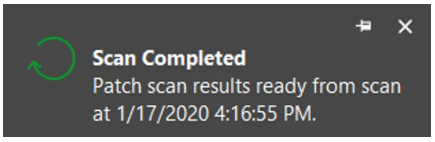
The **Power > Send Wake-on-LAN request** command works with the following target machine states:

Initial Target Machine Power State	Target Machine Awakened?
Fully powered on	No action
Sleep state	Yes
Hibernate state	Yes
Powered off	Yes

474. Watching For Data Rollup Activity

A notification dialog box is displayed in the lower-right corner whenever a remote console rolls data up to the central console. The dialog box will be displayed for several seconds before slowly fading away. You can pin the dialog box in place by clicking the pin icon. If you are viewing results, the display will not be automatically updated when new results arrive. In order to see the new information related to the data rollup, you can click the notification dialog box or you can select **View > Refresh** from the main menu.

Notification dialogs are not displayed if Security Controls is not running on the console machine.



475. What is the Issue?

Security Controls uses a self-signed SHA-2 root certificate to issue the console, agent and scheduler certificates used within the product. Some security tools, however, may see the self-signed certificate as a medium level security risk. To be clear, Security Controls does **not** have a certificate security issue, but these tools have no way of determining that information. If you want to stop the Security Controls certificate from being flagged as a warning, you have the option to use a trusted certificate authority (CA) from your own PKI infrastructure to issue a replacement root certificate for Security Controls.

This section describes the tasks you must perform if you wish to replace the default Security Controls root certificate with a certificate that is issued by your own CA.

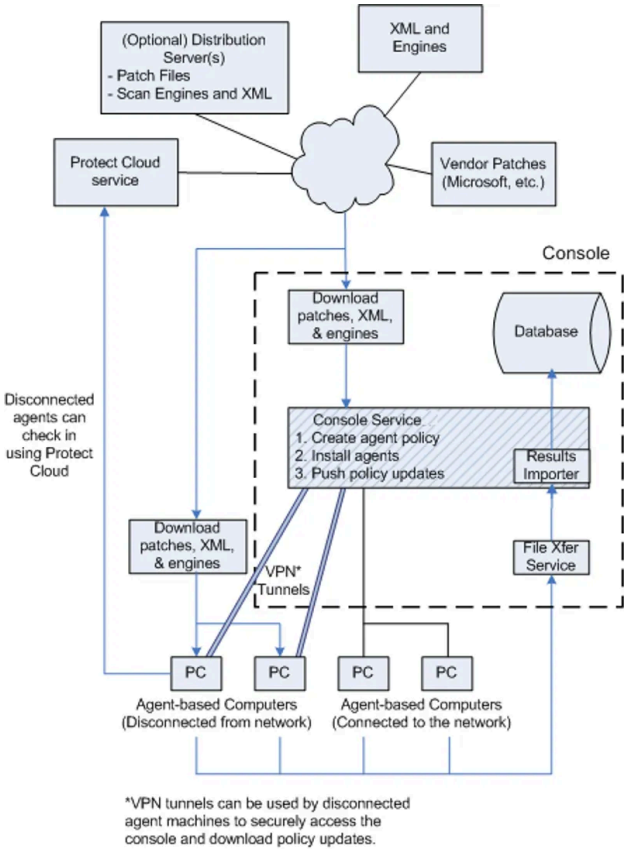
476. What Exactly is Security Controls Agent?

Security Controls Agent is an agent service. The agents configured by Security Controls Agent are distributed agents, meaning they are installed on distinct physical and online virtual machines and have the ability to independently initiate specific actions. They are configured via the Security Controls interface and then installed on the desired machines either by pushing them from the Security Controls console or by manually installing them on individual machines.

Depending on how they are configured, when installed on a machine a Security Controls Agent can:

- Scan for and deploy missing patches
- Scan for asset information (Windows-based machines only)
- Shut down or restart the agent machine on specific days and times (Windows-based machines only)
- Listen to the console or **the cloud** for policy updates and download the new policy immediately
- Report the results to the local console

The following figure illustrates how Security Controls Agent works in your environment.

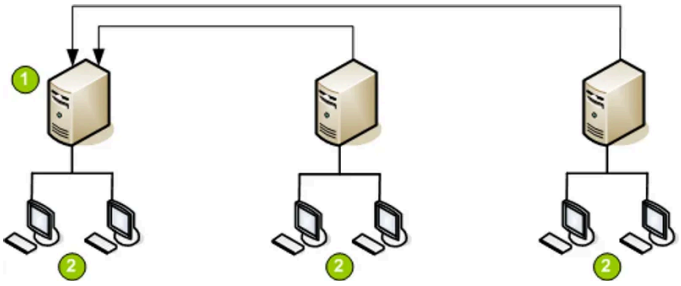


477. What is a Data Rollup Console Configuration?

> Data rollup is for Windows data only and each connected console must use its own separate database.

In a data rollup console configuration, one console acts as the central console. In addition to receiving scan and deployment data from the machines it manages, the central console also receives data about machines managed by other consoles. The central console is therefore also known as the rollup console because the data from all the other consoles is rolled up to it. This enables you to track what is happening throughout your organization from one central site.

The following figure illustrates a data rollup console configuration.



1 - Rollup console

2 - Managed machines

For more information, see **Implementing a Data Rollup Configuration**.

478. What Sets Security Controls Apart from the Others?

Features

Item	Description
Ease of use	Security Controls can be installed and used to deploy missing patches within minutes; not days, weeks, or months.
Real-time patch validation	Security Controls utilizes data files that are updated the moment a security patch is released.
Agentless and agent-based operation	Provides the ability to manage network machines directly from a console and to manage hard-to-reach and cloud-connected machines (such as roaming laptops) using agents.
Background (non-modal) tasking	Enables multiple tasks to run at the same time. Simultaneously perform patch and asset scans, download files, deploy patches, perform power management tasks, install agents, and keep on working.
Patch replacement	Only those patches that are necessary and applicable to the scanned platform are evaluated during the scan process. Unnecessary and replaced patches are not presented (although you can **configure the program to do this** if you want).
Dynamic product detection (DPD)	Provides the ability to support additional non-Microsoft products simply by updating the necessary data files.
Virtual machine support	Operates exactly the same on both physical machines and on virtual machines that are online. Can perform patch assessment of offline virtual machines without powering them on. Missing patches are copied into the virtual image so when the offline image is powered on it immediately patches itself.

Security and Integrity

Item	Description
Detailed Patch Analysis and Validation	File versions and registry keys are evaluated to aid in determining patch status. Solutions that rely solely on registry keys and/or minimum file versions are unable to differentiate between legitimate files and trojaned files, including patches that have been re-released by Microsoft.
External validation data	File data used to perform patch validation tests are obtained from a signed source independent of the machine being scanned.
Data file anti-spoofing protection	The data definition file is parsed only if obtained from a valid, specifically signed CAB file or SSL location.
Trojan protection	All digitally-signed vendor files are validated prior to patch deployment.

479. When Should I Use Agentless and Agent-based Solutions?

Security Controls is, at its roots, an agentless solution. With a few simple configuration steps, however, Security Controls can also provide agent-based services. This section explains when to implement each solution.

WINDOWS ENVIRONMENTS

For Patch Management and Asset Management Tasks

Start with the Agentless Features of Security Controls

For large enterprises containing thousands of machines, the ease of use provided by the agentless technology of Security Controls can be used to address the patch management and asset management needs of the vast majority of the machines in your enterprise. Security Controls can be used to discover which target machines are missing patches and automatically deploy the missing patches. It can also scan your target machines and report on the software, hardware, and virtual assets contained on the machines. Using Security Controls you can scan and fix, from one central location, the vast majority of the machines in your network within minutes.

Polish Things Off with the Agent-based Features of Security Controls

Most large enterprises have machines in hard-to-reach places: machines in remote locations, laptops that roam to different locations or that park and dock outside the office, machines in protected zones (DMZs), etc. For these devices you can use the agent-based features provided by Security Controls, which are implemented using Security Controls Agent. With Security Controls Agent you can be sure that these machines are scanned regularly, even if they are disconnected from your enterprise network.

> There is one exception; agents can be used to perform software asset scans and hardware asset scans, but they cannot perform virtual asset scans.

For Power Management Tasks

A number of the power management tasks apply only to agentless situations. This includes the Shutdown now, Restart now, and Wake-On-LAN tasks that are initiated from Machne View or Scan View. These tasks require the target machines to be accessible from the console and are therefore not implemented within an agent policy.

Power management tasks that use a **power state template**, however, can be implemented in either an agentless or agent-based manner. You may consider using an agent-based power state task under the following conditions:

- If you want to apply your power management policy consistently across all machines within your organization (connected and disconnected).
- If you have machines that may not always be reachable from the console (for example, machines in a DMZ).
- If you are concerned with network bandwidth issues.
  An agentless power state task will push a small number of files from the console to each target machine -- if a large number of machines are involved it may affect the performance of your network.

LINUX ENVIRONMENTS

Patch Management Tasks

All patch management tasks on Linux-based machines are performed using agents. For more information, see **Overview of Linux Patch Management**.

Power Management Tasks

Only a **power status scan** can be performed on Linux machines from the console . All other **power management tasks** on Linux-based machine are performed using agents.

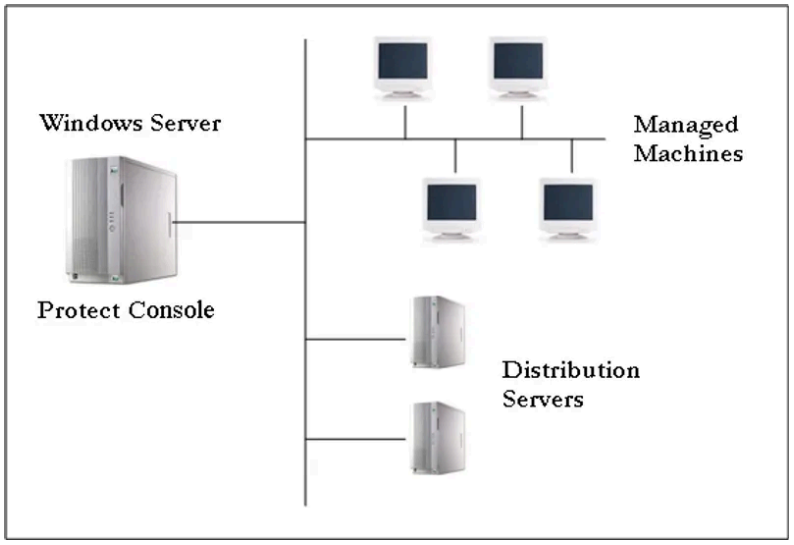
480. Why Use a Distribution Server?

> All of the following features apply to Windows agentless and agent-based environments. For Linux agent environments, distribution servers can be used to download core files but not patches. **Linux agents use YUM to download any patches that must be deployed**.

Distribution servers can be used in a number of different scenarios:

- Distribution servers can be used to store patches that you wish to deploy. Distribution servers can be physically located near each group of machines you are managing. The console can copy patches to the distribution servers only, rather than to each individual machine. Each machine can then download the patches it needs from the nearest distribution server. This can greatly reduce network traffic in a distributed environment and be of huge benefit in wide-area networks. This is true in both agentless environments and agent-based environments. In agentless environments, using distribution servers means the console does not need to push patches to individual machines and individual machines do not need to download patches from patch vendor. In an agent-based environment, it can keep each machine from downloading the patches it needs from the patch vendor over the Internet.
- Distribution servers can be used to store the most up-to-date engines and XML files that are available. In a multi-console or agent-based environment, this can reduce the number of machines that need to download updated files over the Internet.
- Distribution servers allow consoles and agents to operate in environments where they do not have Internet access but still need access to the most up-to-date engines and XML files. See **What is a Disconnected Console Configuration** for more information.
- Distribution Servers can be used to store any custom patches you may have defined. This is particularly important for agent-based environments. See **Preparing to Use Agents** for more information.

The following figure illustrates the use of distribution servers in a network.



481. Why You Might Use Multiple Administrators

Security Controls will allow two or more administrators to access the program at the same time. There are two basic scenarios in which multiple administrators might be used.

For more information see:

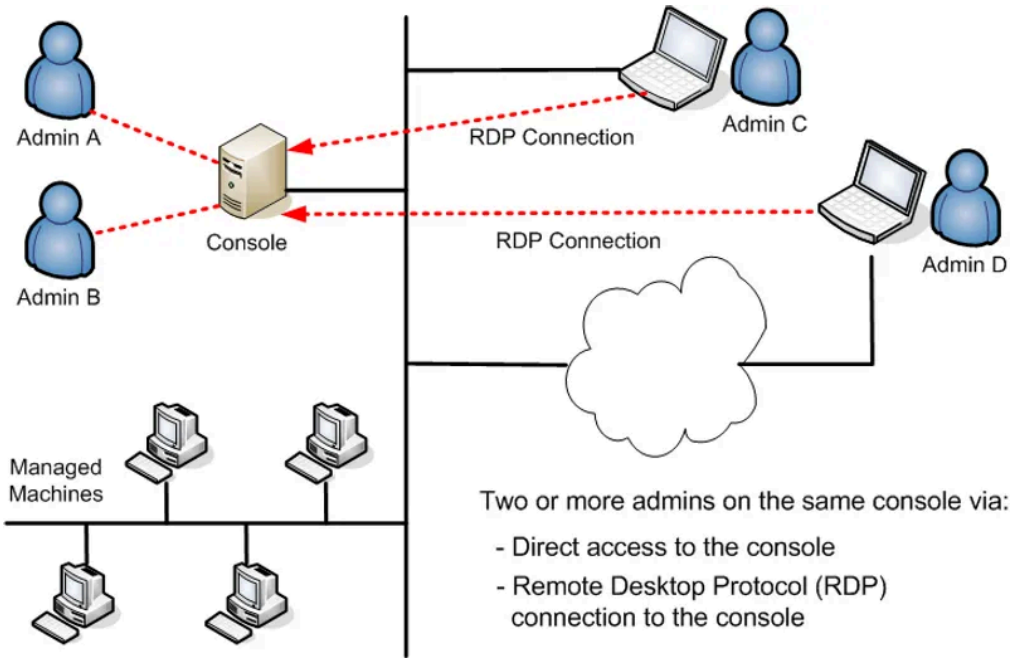
- How Security Controls Manages Multiple Administrators
- Potential Issues When Using Multiple Administrators
- Best Practices When Using Multiple Administrators

Scenario 1: Two or More Administrators on the Same Console Machine

It is very common for two or more administrators to use a single Security Controls console. For example:

- Your company might assign a primary and a backup Security Controls administrator
- Your company might assign a different administrator to manage each unique domain within the organization
- Your company might assign a different administrator to manage each physically distinct office location

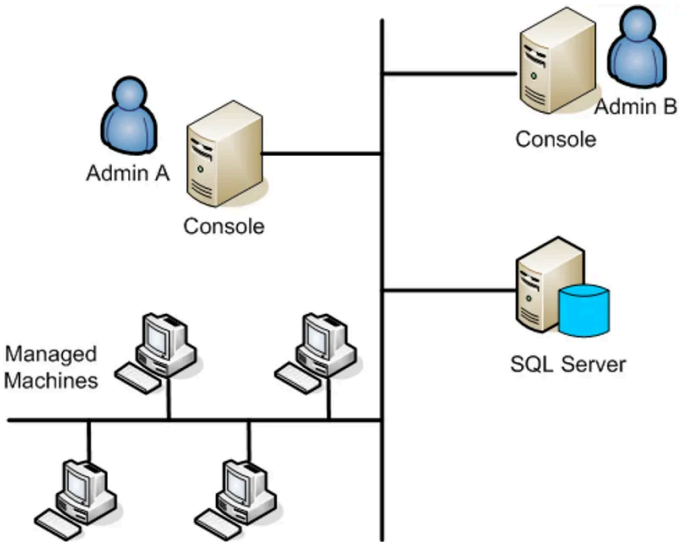
The following figure illustrates how multiple administrators might access a Security Controls console.



Scenario 2: Two or More Consoles Sharing One Database

To understand why you might choose to use more than one console, see Why Use Multiple Consoles?

The following figure illustrates a typical two console scenario with a different administrator assigned to each console.


Admin A
Console
Console
Admin B
SQL Server
Managed
Machines

482. Why Use Multiple Consoles?

Organizations with many office sites located across the country may choose to maintain multiple Security Controls consoles. One console is typically deemed the *central* console. The central console will typically reside at a central site, such as your company headquarters. Each remote office site will contain a *remote* console. Each remote console is responsible for performing scans and patch deployments on the machines in their local network and for rolling up the results of these actions to the central console.

The central console can be thought of as a *Central Policy Manager*. It is the console capable of tracking the results of actions performed on all the other consoles. Likewise, a remote console can be thought of as a *Distributed Policy Manager*. It is responsible for enforcing your organization's patch policies at remote locations. By adding a distribution server into the mix you can implement a *Distributed Policy Service*. The distribution server can be used to store the data files that effectively represent your organization's policy. The files are downloaded and used by the remote consoles, thus implementing your policy.

There are several additional advantages to maintaining multiple consoles:

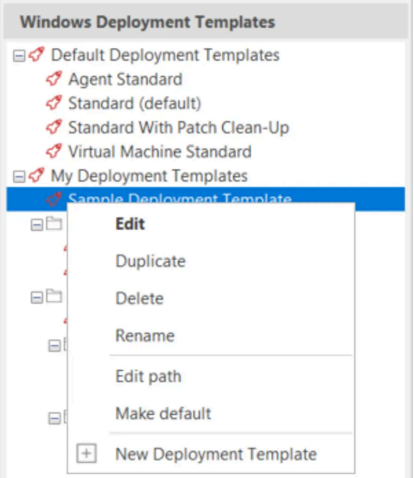
- The consoles can reside at physically distinct locations and be close to the machines they are managing
- You can distribute the workload across multiple consoles
- The scans and deployments are performed much quicker
- You won't tie up your network trying to scan hundreds of geographically distinct machines from one location
- It cuts down on a lot of network traffic, especially over WANs (which can be expensive)
- The results from each console that uses a different database can be rolled up to and viewed from one central location
- If you maintain **multiple consoles within the same network** the consoles can all use one shared database, making it possible to share templates, comments, reports and scan results

There are many possible multiple console configurations, from a basic data rollup configuration to an advanced configuration that combines multiple consoles with Security Controls Agent. Each of these multiple console configurations is described in detail in the following sections:

- **What is a Data Rollup Configuration?**
- **What is an Unattended Console Configuration?**
- **What is a Disconnected Console Configuration?**

483. Managing a Deployment Template

Custom deployment templates are contained within the **My Deployment Templates** list in the navigation pane. You can edit an existing deployment template by clicking the template name. You can also right-click a template and perform a number of different actions.



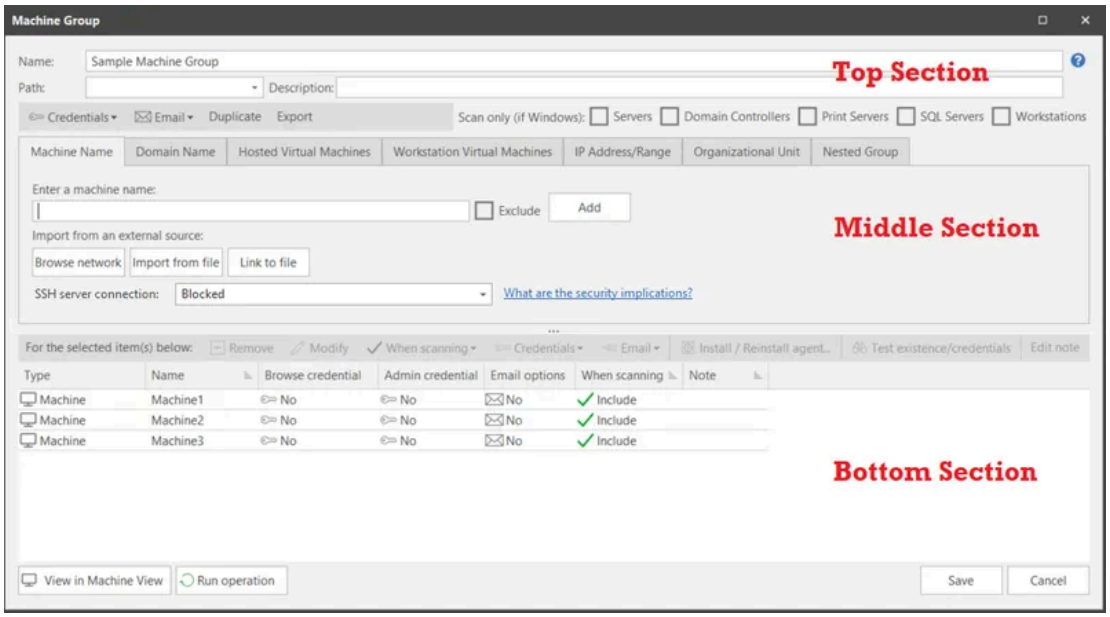
Action	Description
Edit	Enables you to edit the selected template.
Duplicate	Duplicates the selected template. The name of the new template will be 'Duplicate of { selected template name }'. Change the name and the other template characteristics as desired.
Delete	Deletes the current template. You cannot delete a template that is currently being used by an **agent policy**.
Rename	Enables you to change the name of the deployment template. Be careful if you rename a template that is currently being used by an **agent policy**.
Edit path	Enables you to change which **folder** the template resides in within the navigation pane.
Make Default	Selecting this option will use the currently selected template as the default.
New Deployment Template	Enables you to create a new custom **patch deployment template**.

484. Working with a Machine Group

When a machine group is selected in the navigation bar, the details for it are shown in a separate dialog. The dialog is logically separated into three functional sections:

- **Top section**: Contains buttons, links, and filters that apply to the entire machine group.
- **Middle section**: Enables you to add machines to the group.
- **Bottom section**: Enables you to perform actions on individual machines within the group.

For example, here are the details for a group named *Sample Machine Group*.



485. ISeC

486. ISeC CSH