ivanti

ITSM-On-Premises-2024 (ENU)

ivanti

CONTENTS

1. Overview **4**
2. System Requirements **5**
2.1. Hardware and Software Requirements 6
2.2. About Third-Party Software 14
2.3. Port Requirements 16
2.4. Compatibility Matrix 19
2.5. Troubleshooting - System Requirements 22
3. Installation and Deployment **23**
3.1. Neurons for ITSM Deployment Overview 24
3.1.1. Demonstration or Proof-of-Concept Deployment 25
3.1.2. Minimum Production Deployment 27
3.1.3. Enterprise Production Deployment 29
3.1.4. Security Enterprise Production Deployment 33
3.1.5. Database Deployment Options 35
3.1.6. Operations Console Deployment Options 40
3.1.7. Reporting Services Deployment Options 46
3.1.8. Voice Deployment Options 50
3.2. Neurons for ITSM Installation Prerequisites 52
3.2.1. About Roles 53
3.2.2. About the Different Accounts Used in Neurons for ITSM 55
3.2.3. About Passwords Used in Neurons for ITSM 57
3.2.4. About Using a Virtual Machine with Neurons for ITSM 58
3.2.5. Enabling Attachment File Streaming 59
3.2.6. SSL Configuration 62
3.2.7. Installing Neurons for ITSM Reporting Feature 67
3.2.8. Full Text Search 69
3.2.9. Verifying Server Roles and Features 71
3.3. Installing the Neurons for ITSM System 73
3.3.1. Installing Neurons for ITSM 74
3.3.2. Installing the Reporting Feature 78
3.3.3. Installing Discovery on a Dedicated Server 80
3.3.4. Installing the Knowledge Uploader (Knowledge Import Tool) 81
3.4. Initially Configuring the System 89
3.4.1. Using the System Configuration Wizard 93
3.4.2. Configuring Neurons for ITSM 96
3.4.2.1. Configuring the Configuration Database 97
3.4.2.2. Configuring the Neurons for ITSM Application 103
3.4.2.3. Configuring the Application Server Settings 109
3.4.2.4. Configuring Other Feature Settings 113
3.4.2.5. Configuring the Metrics Server 117
3.4.2.6. Configuring the Discovery Application Server 122
3.4.2.7. Configuring the Discovery Web Server 128
3.4.2.8. Finishing the System Configuration 131
3.4.3. Configuring the Reporting Feature 132
3.4.4. Configuring Discovery 143
3.4.5. Configuring the Deployment on the Neurons for ITSM Operations Console 146
3.4.6. Optional SSL Configuration 151
3.4.7. Optional LDAP Configuration 160
3.4.8. About Configuring with ADFS 161
3.4.9. About Configuring Throttling Settings 162
3.5. Setting up Redis 164
3.6. Logging into Neurons for ITSM 172
3.7. Adding Features and Changing Settings 174
3.8. Upgrading Neurons for ITSM from an Earlier Release 176
3.9. Using the License Manager 184
3.10. Troubleshooting - Installation and Deployment 198
4. Configuration Database **216**
4.1. About Logging into the Configuration Database 217
4.2. Workspaces that Already Exist 218

4.3. Working With Features ... 219
4.4. Internal Use Only Workspaces ... 220
4.5. Workspaces Populated by the System Configuration Wizard ... 221
4.6. Central Config API Authentication ... 222
4.7. Setting up the Teams Bot Integration ... 227
4.8. Enabling the Action Service ... 232
4.9. Workspaces that Can Be Used ... 234
4.9.1. Configuring the Message Queue ... 235
4.9.2. Configuring the Message Queue Handler ... 236
4.9.3. Configuring Email ... 237
4.9.4. Viewing All Logs ... 238
4.9.5. Working With Customer Contacts ... 241
4.9.6. Working With Tenants ... 243
4.9.7. Configuring Manual Load Partitioning ... 246
4.9.8. Firebase Configuration for Mobile Push Notification ... 249
4.9.9. Decommissioning FTP and File on Shared folder Integration ... 264
5. Performance Tuning ... 266
5.1. Server and Connection Tuning ... 267
5.1.1. Working with Log Files and Logging Levels ... 268
5.1.2. Configuring the Application Pool Recycling Schedule ... 269
5.2. Platform and Application Tuning ... 270
5.2.1. Planning and Scheduling Maintenance ... 271
5.2.2. Tuning Business Rules and Workflows ... 274
5.2.3. Best Practices for Dashboards and Layouts ... 275
5.2.4. About Using Combo Boxes Sparingly ... 277
5.2.5. Evaluating Slow Running Queries ... 278
5.3. Database Tuning ... 280
5.3.1. Tuning Indexes ... 288
5.3.2. About Using Full Text Search ... 295
5.4. Performance Monitoring ... 296
5.5. Troubleshooting - Performance Tuning ... 302
5.6. Deleting Inactive Tables and Records ... 303
5.6.1. Best Practices for Deleting Tables and Records ... 304
6. Operations Console ... 306
6.1. Operations Console Overview ... 308
6.1.1. Operations Console Interface ... 309
6.1.2. Terminology ... 311
6.1.3. Installing the Operations Console ... 318
6.2. Before You Begin Migrating Data ... 320
6.2.1. Items Excluded from Migration ... 329
6.3. Starting the Data Migration ... 330
6.4. Migrating Data using Heat Development Project ... 1
6.4.1. Example: Migrating Request Offering Changes By Enabling the Ivanti Service Manager Development Project ... 1
6.5. Troubleshooting and Known Issues ... 1
6.5.1. Configuring Landscapes ... 1
6.5.2. Working with Tenants and Tenant Instances ... 1

1. Overview

Welcome to Neurons for ITSM On-premise online help. If you are an On-premise customers looking for information about installing, configuring, system requirements, ops console, performance tuning, and web services, you are in the right place. Click the tiles below or use the table of content on the left menu to view topics. To search for specific information, use the search bar and search using a relevant keyword.

Installation and Deployment

Configuration Database

System Requirements

Performance Tuning

Ops Console

Web Services

2. System Requirements

The *System Requirements and Compatibility Matrix for* Neurons for ITSM - *Version* 2024.2 is intended for administrators who are going to install Neurons for ITSM on your local computer or virtual machine. This document contains the following sections:

- **Hardware and Software Requirements**. Contains the hardware and software requirements.
- **About Third-Party Software**. Discusses third-party software that is used in Neurons for ITSM.
- **Port Requirements**. Lists the required ports.
- **Compatibility Matrix**. Lists the compatibility of Neurons for ITSM Release 2024.2 with other software.
- **Troubleshooting**. Contains solutions to common problems related to system requirements.

2.1. Hardware and Software Requirements

This section outlines the hardware and software requirements necessary for the installation of Neurons for ITSM.

Application Server Requirements

This section explains the hardware and software specifications needed to properly install, run, and maintain an application server.

Hardware

Component	Recommended
CPU	• 2 core minimum • 4 core recommended for heavy transaction rates and workflow/escalation usage
RAM	• 8 GB minimum, and more depending on transaction rates and workflow/escalation complexity
Hard Disk	• 20 GB minimum free space (approximately 1.1 GB for Neurons for ITSM files and the remaining space for log files). • Best Practice! We recommend that you install Neurons for ITSM in a location other than on the system drive (typically the C drive).

Software

Item	Supported Version
Operating System	• Microsoft Windows Server 2022 recommended (Supported only with ITSM version 2023.4 or later) • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Microsoft .NET Framework	• Microsoft NET. Framework Release 4.6 if FedRAMP feature is not enabled. If FedRAMP feature is enabled, the required Microsoft .NET Framework Release is 4.8. This requires the latest Microsoft Windows update.
Web Server	• Microsoft IIS Release 7.5 • Microsoft IIS Release 8.0 • Microsoft IIS Release 8.5 (recommended) • Microsoft IIS Release 10 (Windows 2016)

Web Server Requirements

This section explains the hardware and software specifications needed to install, configure, and run a web server.

> In multi-server environments, each Neurons for ITSM web server must meet these requirements.

Hardware

Component	Recommended
CPU	• 2 core minimum • 4 core recommended for heavy transaction rates and workflow/escalation usage
RAM	• 8 GB minimum, and more depending on transaction rates and workflow/escalation complexity
Hard Disk	• 20 GB minimum free space (approximately 1.1 GB for Neurons for ITSM files and the remaining space for log files). • Best Practice! We recommend that you install Neurons for ITSM in a location other than on the system drive (typically the C drive).

Software

Item	Supported Version
Operating System	• Microsoft Windows Server 2022 - recommended (Supported only with ITSM version 2023.4 or later) • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Microsoft .NET Framework	• Microsoft .NET Framework Release 4.6 if FedRAMP feature is not enabled. If FedRAMP feature is enabled, the required Microsoft .NET Framework Release is 4.8. This requires the latest Microsoft Windows update or that you download the following security patch: https://www.microsoft.com/en-us/download/details.aspx?id=42327
Web Server	• Microsoft IIS Release 7.5 • Microsoft IIS Release 8.0 • Microsoft IIS Release 8.5 (recommended) • Microsoft IIS Release 10 (Windows 2016)

Database Server Requirements

This section explains the hardware and software specifications needed to install, run, and maintain a database server.

Hardware

Component	Recommended
CPU	• 4 core minimum. Your deployment may require more for heavy transaction rate and workflow or escalation usage
RAM	• 16 GB minimum; however, your deployment may require much more RAM depending on transaction rates and workflow or escalation complexity
Hard Disk	• Best Practice! We recommend that you have separate volumes for the database and the transaction logs. • **Database**: 100 GB minimum free space. For proper disk space sizing, use these guidelines: ◦ Neurons for ITSM application demo database: 500 MB ◦ Average disk space requirement per record (incident, problem, change, configuration): ~200 KB ◦ For storing records more than three years old: more than 60 GB ◦ Average disk space requirement per record (configuration item): ~500 KB. For example, for 20,000 configuration items, we recommend a minimum of 10 GB. ◦ 10 GB minimum free space. This is the minimum. • **Transaction logs**: 60 GB minimum free space.

Software

> If your deployment has the reporting feature installed, you must have Microsoft .NET Framework Release 4.8, which requires the latest Microsoft Windows update or that you download the following security patch: **https://www.microsoft.com/en-us/download/details.aspx?id=42327**.

Item	Supported Version
Operating System	• Microsoft Windows Server 2022 - recommended (Supported only with ITSM version 2023.4 or later) • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Database Management Software	• Microsoft SQL Server 2022 (Supported only with ITSM version 2023.4 or later) • Microsoft SQL Server 2019 • Microsoft SQL Server 2016 • Microsoft SQL Server 2017
Other Software	• iFilters (required for full-text indexing) • An iFilter is a plugin that allows the Microsoft SQL Server to index various file formats so that they become searchable. Download the latest version of the iFilter for the document type (these links are subject to change): ◦ Microsoft Office 2010: **https://www.microsoft.com/en-us/download/details.aspx?id=5829** ◦ Adobe PDF iFilter 64 Release 11.0.01: **http://www.adobe.com/support/downloads/detail.jsp?ftpID=5542**

- Microsoft SQL Server must have full-text search enabled. If it is not enabled, the Neurons for ITSM demo database will not run properly.
- ITSM application does not support case-sensitive SQL Collation.
- ITSM application only supports the SQL Collation of SQL_Latin1_General_CP1_CI_AS.

Reporting Feature Requirements

This section explains the requirements to implement or support a reporting feature in a software system.

Hardware

Component	Recommended
CPU	• 2 core minimum • 4 core recommended for heavy transaction rates and workflow and escalation usage
RAM	• 8 GB minimum, and more depending on transaction rates and workflow and escalation complexity
Hard Disk	• 20 GB minimum free space (approximately 1.1 GB for Neurons for ITSM files and the remaining space for log files). • Best Practice! We recommend that you install Neurons for ITSM in a location other than on the system drive (typically the C drive).

Software

Item	Supported Version
Operating System	• Microsoft Windows Server 2022 - recommended (Supported only with ITSM version 2023.4 or later) • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Microsoft .NET Framework	• Microsoft .NET Framework Release 4.6 if FedRAMP feature is not enabled. If FedRAMP feature is enabled, the required Microsoft .NET Framework Release is 4.8. This requires the latest Microsoft Windows update or that you download the following security patch: https://www.microsoft.com/en- us/download/details.aspx?id=42327
Database Management Software	• Microsoft SQL Server 2022 (Supported only with ITSM version 2023.4 or later) • Microsoft SQL Server 2019 • Microsoft SQL Server 2016 • Microsoft SQL Server 2017
Other Software	• Microsoft SQL Server Reporting Services (SSRS)

Microsoft SSRS Report Designer

Business Intelligence Development Studio (BIDS) is a Microsoft component used in creating reports and report templates for Neurons for ITSM. BIDS comes with Microsoft SQL Express edition. For on-premise users, BIDS comes with Microsft SQL Server

license.

Item	Supported Version
Operating System	• Microsoft Windows Server 2022 recommended (Supported only with ITSM version 2023.4 or later) • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Hard Disk	• 5 GB minimum free space
RAM	• 512 MB minimum, 2GB is recommended
Processors	• **X86**: Pentium III-compatible processor or faster (processor speed of 1.0 GHz or faster) • **X64**: Minimum: AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support (processor speed of 1.0 GHz or faster) • **IA64**: Itanium processor or faster (processor speed of 1.0 GHz or faster)

Discovery Requirements

This section explains the requirements needed to successfully perform automated asset discovery and service mapping across your IT infrastructure.

Hardware

Component	Recommended
CPU	• 2 core minimum • 4 core recommended for heavy transaction rates and workflow and escalation usage
RAM	• 8 GB minimum, and more depending on transaction rates and workflow and escalation complexity
Hard Disk	• 20 GB minimum free space (approximately 1.1 GB for Neurons for ITSM files and the remaining space for log files). • Best Practice! We recommend that you install Neurons for ITSM in a location other than on the system drive (typically the C drive).

Software

Item	Supported Version
Operating System	• Microsoft Windows Server 2022 - recommended (Supported only with ITSM version 2023.4 or later) • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Microsoft .NET Framework	• Microsoft .NET Framework Release 4.6 if FedRAMP feature is not enabled. If FedRAMP feature is enabled, the required Microsoft .NET Framework Release is 4.8. This requires the latest Microsoft Windows update or that you download the following security patch: https://www.microsoft.com/en- us/download/details.aspx?id=42327
Web Server	• Microsoft IIS Release 7.5 • Microsoft IIS Release 8.0 • Microsoft IIS Release 8.5 (recommended) • Microsoft IIS Release 10

Client Computer Requirements

This section explains the requirements that your computer (client) must meet to successfully run a specific application, connect to a server, or access a system.

Hardware

Component	Recommended
CPU	• Single core
RAM	• 4 GB

Mobile

Neurons for ITSM offers native apps for mobile devices for the Android and iOS platforms. The Neurons for ITSM app can be downloaded from their respective platform's app stores.

Software

See the **Browser Compatibility** for browser compatibility information.

There is a Known Issue during installation of the 2017.2 Discovery Client Agent.

Installation pops up Windows Warning for digital signature requirement from Microsoft.

Windows cannot verify the digital signature for this file. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

To correct this, digital signature certificates have been updated. However, Ivanti recommends to apply updates to support Code Signing issues in Windows 7 and Windows Server 2008.

For windows 7, please make sure that System has SP1 installed and install KB from **https://technet.microsoft.com/en-us/library/security/3033929**.

As per MSDN driver signing has changed in Windows 10, version 1607.

Exceptions / Are cross-signed drivers still valid?

- Enforcement only happens on fresh installations, with Secure Boot on, and only applies to new kernel mode drivers:
  - PCs upgrading from a release of Windows prior to Windows 10 Version 1607 will still permit installation of cross-signed drivers.
  - PCs with Secure Boot OFF will still permit installation of cross-signed drivers.
  - Drivers signed with an end-entity certificate issued prior to July 29th, 2015 that chains to a supported cross-signed CA will continue to be allowed.

To prevent systems from failing to boot properly, boot drivers will not be blocked, but they will be removed by the Program Compatibility Assistant. Future versions of Windows will block boot driver.

To summarize, on non-upgraded fresh installations of Windows 10, version 1607 with Secure Boot ON, drivers must be signed by Microsoft or with an end-entity certificate issued prior to July 29th, 2015 that chains to a supported cross-signed CA.

Reference: **https://blogs.msdn.microsoft.com/windows_hardware_certification/2016/07/26/driver-signing-changes-in-windows-10-version-1607/**.

If the certificate uses SHA-2 or has SHA-2 certificates in its chain of trust and it is being used to sign kernel modules, then please be aware of KB3033929, an update for Windows 7 distributed through Windows Update. On versions of Windows 7 without this update, the kernel will reject signatures made with certificates that use SHA-2, so they cannot be used to get a kernel module to load.

Reference: **https://support.comodo.com/index.php?/Knowledgebase/Article/View/1103/0/signing-microsoft-windows-64-bit-kernel-mode-drivers**.

Remote Control Feature

For customers using the legacy Remote Control solution, this feature requires that your browsers enable either TLS 1.0 or TLS 1.1 to support the HTTPS connection between the clients and the remote control server.

Bandwidth and Latency

For optimal application performance, we recommend a latency of 110 ms or below with a minimum of 1.5 MB/sec in bandwidth between the Neurons for ITSM application server and the remote location client machines.

Chat Service Requirements

Software requirements

Component Name	Description
Redis	The Redis server should be running as a Windows service where the Neurons for ITSM installer is being installed.
Microsoft SQL server	The database server should be available to store chat history and other statistics.
Node js	The node software should be installed where Neurons for ITSM installer is being installed. The node software is required to enable the server to run chat as a back-end service.

Points to Note:

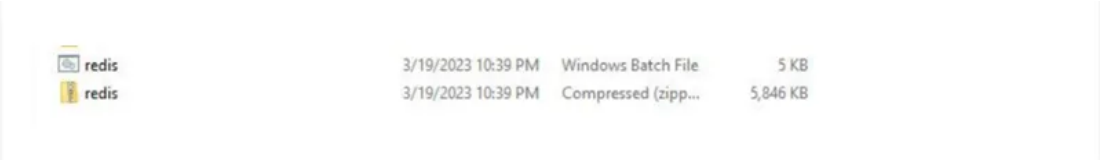
- In the on-premise machine, Chat service is installed as a part of the appserver module installation while Neurons for ITSM installer is installed as software and Chat service runs on IIS.
- Currently installed on-prem node version: 20.5.0.
- Currently installed on-prem Redis server version : 3.0.503.

Redis server installation guide

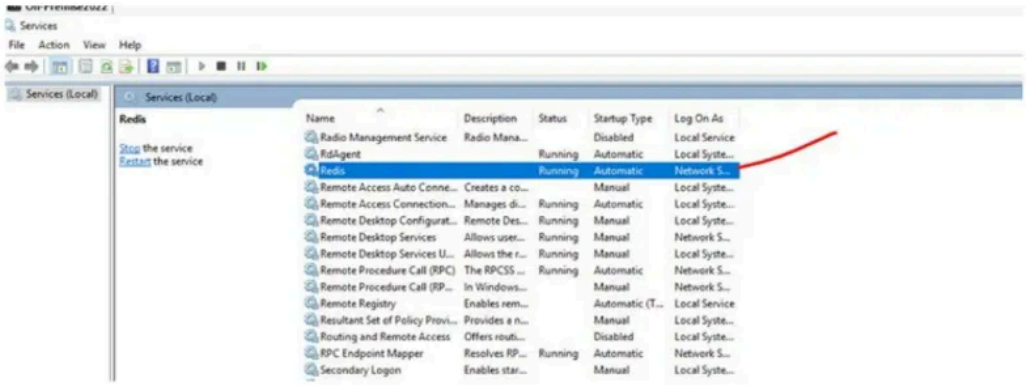
1. Navigate to the following path: C:\Program Files\HEAT Software\HEAT\AppServer\redis.

> The C drive on your machine may differ depending on your system's configuration.

2. Extract the Redis file in the same location.



3. Select the Redis batch file and run it as an administrator.
4. Verify that the Redis server is present in the Windows Services option.



2.2. About Third-Party Software

Neurons for ITSM does not support versions of third-party application that are no longer supported for all customers by the third-party vendor. This policy also applies to any third-party application versions released after the version certified with a specific release of Neurons for ITSM.

Third-Party Software Components

The Neurons for ITSM installation package provides the following required third-party software components:

- Microsoft SQL Server 2014 Shared Management Objects
- Microsoft System CLR Types for Microsoft SQL Server 2014
- Microsoft Exchange Web Services Managed API 2.1
- IISNode
- NodeJs
- Microsoft Access Database Engine 2016 Redistributable
- Microsoft Access Database Engine 2016 Redistributable (x64)
- dotnet core hosting bundle 6.x
- .NET Core Hosting Bundle 6.0.31
- Microsoft .NET Framework 4.8 Full
- URL Rewrite Module 2.1 (English)
- Microsoft SQL Server 2019 Shared Management Objects
- Microsoft System CLR Types for Microsoft SQL Server 2019
- VC++ 2015 Redistributable (x64)
- VC++ 2013 Redistributable (x64)
- VC++ 2012 Redistributable (x64)
- Node.js v20.13
- Microsoft Windows Server Roles and Features
- Redis 6.2
- Microsoft .NET Framework 4.6.1 Full
- Microsoft .NET Framework 4.7.2 Full
- Microsoft .NET Framework 4.8 Full
- Server Roles and Features - Windows Server 2008 R2 (windows feature)
- Server Roles and Features - Windows Server 2008 R2 WCF (windows feature)
- Server Manager - Windows Server 2012 (windows feature)
- Server Manager - Windows Server 2012_WCF (windows feature)
- Server Manager - Windows Server 2012_MSMQ (windows feature)

If the installer does not detect these components on the host system, they are installed automatically.

If you create your own installation packages for remote deployment, include the software components that are listed in the system requirements that follow.

Third-Party Software Support

Ivanti relies on, and integrates with, many different third-party applications.

Ivanti Software regularly performs quality assurance testing in the interactions between Neurons for ITSM and these applications. Our policy is to support any tested version of a third-party application (as certified) and newer versions (as compliant), so long as the third-party vendor claims and maintains backward compatibility.

If Ivanti Software becomes aware that a third-party vendor has not maintained backward compatibility to the most recent certified version, Ivanti Software notes this in the compatibility matrix as an exception.

Neurons for ITSM does not support third-party applications that are older than a certified version. Ivanti Software often certifies more than one version of third-party software when more than one version is in common use; otherwise, the current generally available version is used during each Ivanti Software version quality assurance cycle.

2.3. Port Requirements

Ensure that ports are configured correctly so that all Neurons for ITSM components open correctly.

For All Deployments

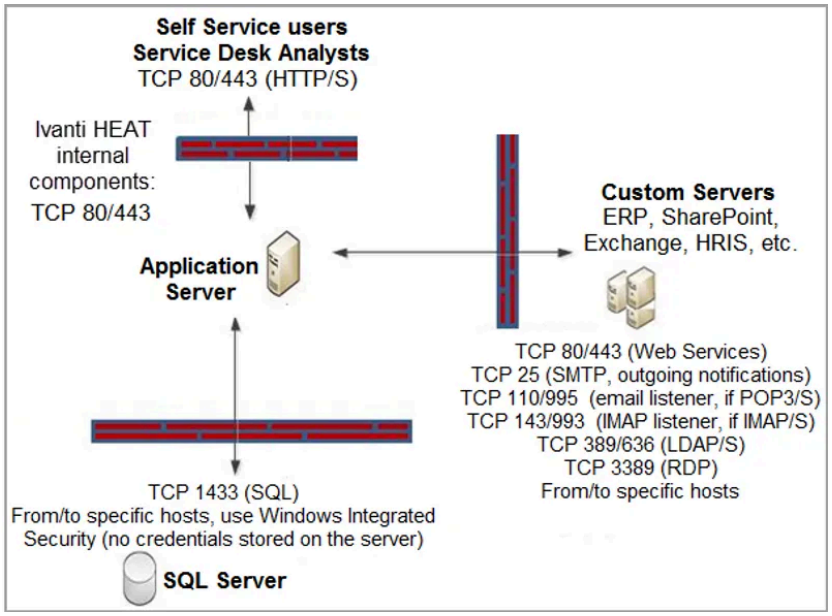
For all deployments, we recommend that you open the following ports:

Port	Service
53	For Active Directory. Select the UDP (for DNS) or TCP protocol.
139 or 445	For deploying agents to other computers. Select the UDP (for DNS) or TCP protocol.
443	For sending surveys. However, port HTTPS 7075 is supported until further notice.
1433	For the SQL server.
2323	Neurons for ITSM Voice web services port: Set to match the web services port set in the Ivanti Service Manager Voice management portal.
5743	For the Neurons for ITSM Voice server.
5986	For WinRM to receive remote commands.
8097	The default proxy port. Used unless defined in the endpoint address. For example, http://company/users:8113.
7200	For the message queue.
61000	The public TCP port of the Neurons for ITSM Voice message server service.
62000	The public TCP port of the Neurons for ITSM Voice reset password service.
6379	For the Redis Enterprise Software.
1213	For Integration Service.

For Deployments With All Components Installed on One Host

Port Configuration shows the port requirements for a deployment where all Neurons for ITSM components are installed on one host.

Fig.1. Port Configuration



The ports to open are as follows:

- Self Service users and Service Desk Analysts:
  - TCP 80/443 (HTTP/HTTPS)
- Neurons for ITSM application server (Neurons for ITSM internal components):
  - TCP 80/443
- Custom servers (ERP, SharePoint, Exchange, HRIS, and so on):
  - TCP 80/443 (web services)
  - TCP 25 (SMTP, outgoing notifications)
  - TCP 110/995 (Email listener if POP3/S is used)
  - TCP 143/993 (IMAP listener, if IMAP/S is used)
  - TCP 389/636 (LDAP/S)
  - TCP 3389 (RDP)
- Microsoft SQL Server:
  - TCP 1433 (SQL)

To and from specific hosts, use Windows Integrated Security. No credentials are stored on the server.

> The outbound port may not be the same as the inbound port. The outbound is determined by your environment.

For Deployments with the Web Server Installed on a Different Host

If your deployment has the Neurons for ITSM web server outside of the firewall, ensure that the following ports are also open:

- TCP 80/443
- TCP 25 (SMTP, outgoing notifications)
- TCP 1433 (SQL)

- TCP 54327 (License)
- TCP 389/636 (LDAP/S)

For Deployments that Include Discovery

> For additional information about the Discovery requirements, see the Neurons for ITSM online help and look for the topic called "Standard Gateway System Prerequisites". See "Related Documentation" for information on accessing the Neurons for ITSM documentation.

- About the Discovery Servers
- Port Information

About the Discovery Servers

The Discovery components reside on two servers: the Discovery web server and the Discovery application server. You can view the components that are deployed to each server from Microsoft IIS.

- The AgentTaskWs and ClientTransportProcessor components reside on the Discovery web server.
- The MessageSender, AssetProcessor, DiscoProcessor, and TaskProcessor components reside on the Discovery application server.

All communication from the gateway or client agent goes to the AgentTaskWs and ClientTransportProcessor components (on the Discovery web server), and those components then relay the messages or requests to the corresponding components on the Discovery application server.

Commands sent to the AgentTaskWs component are relayed to the TaskProcessor component via Net.TCP on port 7100.

Asset and Discovery data sent to the ClientTransportProcessor component is forwarded to the message sender via Net.TCP on port 5000. The message sender component then queues the message on one of the processor queues depending on the message type; you do not need to open a particular port for this.

Port Information

If your deployment includes Discovery, ensure that the following ports are also open for the

Discovery application server:

- TCP 8080
- TCP 5000
- TCP 8382
- TCP 7100

For Deployments with Remote Control

To use the remote control feature without the plugin (using HTML5), port 11438 must be opened. For more information about the remote control feature, see the Neurons for ITSM online help. (See "Related Documentation" for information about accessing the Neurons for ITSM documentation, including the online help.)

2.4. Compatibility Matrix

- Legend
- Server Compatibility
- Microsoft .NET Framework
- Web Servers
- Database Management Software
- Email Servers
- Other Integrations
- Browser Compatibility

See also About Third-Party-Software.

Legend

C	Has been fully tested by Quality Assurance (QA) and indicates compatibility (supported).
W	Has not been fully tested by QA for compatibility and/or integration, but works (supported).
N	Has been tested by QA for compatibility and/or integration but is NOT supported due to test results.
NT	Has not been tested by QA; is currently NOT supported due to lack of testing.
--	Not applicable/not available (not supported).

Server Compatibility

Operating System	Neurons for ITSM Release 2024
Microsoft Windows Server 2016 English - EN-US	C
Microsoft Windows Server 2019 English - EN-US	C
Microsoft Windows Server 2022 English - EN-US	C

Microsoft .NET Framework

Microsoft .NET Framework	Neurons for ITSMRelease 2024
Microsoft .NET Framework Release 1.1 SP1 - 4.0	--
Microsoft .NET Framework Release 4.5	--
Microsoft .NET Framework Release 4.5.2	--
Microsoft .NET Framework Release 4.6	--
Microsoft .NET Framework Release 4.8	C

Web Servers

Web Servers	Neurons for ITSMRelease 2024
Microsoft IIS Release 5.1 - 7.0	--
Microsoft IIS Release 7.5	C
Microsoft IIS Release 8.0	C
Microsoft IIS Release 8.5	C
Microsoft IIS Release 10 (Windows 2016)	W

Database Management Software

Database Management Software	Neurons for ITSMRelease 2024
Microsoft SQL Server 2016*	C
Microsoft SQL Server 2017	C
Microsoft SQL Server 2019	C
Microsoft SQL Server 2022	C
IBM DB2 Version 9.1	--

*Customers using SQL 2022 who are considering migrating to a Cloud deployment of Ivanti Neurons for ITSM, may have to downgrade their SQL 2022 database to SQL 2019 prior to migrating.

- ITSM application does not support case-sensitive SQL Collation.
- ITSM application only supports the SQL Collation of SQL_Latin1_General_CP1_CI_AS.

Email Servers

Email Servers	Neurons for ITSM Release 2024
Lotus Domino	NT
Novell GroupWise	NT
Microsoft Exchange 2010 (supports email server products that support POP3, SMTP, iMAP4)	C
Microsoft Exchange Web Service	C

Other Integrations

Other Integrations	Neurons for ITSM Release 2024
Ivanti Voice	C
Ivanti Service Manager DSM Release 2015.2, Ivanti Service Manager DSM Release 2016.x	W
Citrix	NT
VMWare ESX 4	W
Ivanti Service Manager Mobile	C

Browser Compatibility

> Neurons for ITSM versions 2022.1 and newer do not support Internet Explorer.

Browser	Supported Version
Google Chrome	Ivanti recommends and supports using the latest production version of Google Chrome (not including beta versions) with Neurons for ITSM. If new versions of Google Chrome break compatibility with Neurons for ITSM, we will document those exceptions here and work to support the new browser version with the next release. At time of release, Ivanti has successfully tested Ivanti Neurons for ITSM with Google Chrome version 120.0.6099.224/225. Download and install the **ClickOnce extension** to ensure that the Ivanti Neurons for ITSM reporting feature works correctly.
Mozilla Firefox	Ivanti recommends and supports using the latest production version of Mozilla Firefox (not including beta versions) with Neurons for ITSM. If new versions of Mozilla Firefox break compatibility with Neurons for ITSM, we will document those exceptions here and work to support the new browser version with the next release.
Microsoft Edge	Ivanti recommends and supports using the latest production version of Microsoft Edge (not including beta versions) with Neurons for ITSM. If new versions of Microsoft Edge break compatibility with Neurons for ITSM, we will document those exceptions here and work to support the new browser version with the next release.
Safari	Ivanti recommends and supports using the latest production version of Safari (not including beta versions) with Neurons for ITSM. If new versions of Safari break compatibility with Neurons for ITSM, we will document those exceptions here and work to support the new browser version with the next release.

2.5. Troubleshooting - System Requirements

If you have problems with your installation or deployment, check this section first.

1

Problem: The Neurons for ITSM web servers do not work correctly.

Possible Cause: In multi-server environments, each Neurons for ITSM web server must meet the system requirements.

Solution: See "Web Server Requirements".

2

Problem: I am unable to use integrated components, such as Neurons for ITSM Voice.

Possible Cause: You must use the Microsoft Windows operating system when you use integrated components.

Solution: Change to the Microsoft Windows operating system. See "Client Computer Requirements".

3

Problem: I am using Google Chrome and cannot download or edit reports.

Possible Cause: You have not installed the ClickOnce extension yet.

Solution: Install the ClickOnce extension for Google Chrome. Navigate to **https://chrome.google.com/webstore/detail/meta4-clickonce- launcher/jkncabbipkgbconhaajbapbhokpbgkdc?hl=en** to download the extension. See "Client Computer Requirements".

3. Installation and Deployment

This document is intended for system administrators who are migrating from ITSM Release 6.x, ITSM Release 7.x, ITSM Release 8.x, and Ivanti Classic to Neurons for ITSM - Version 2024.2.

Document Organization

This guide contains the following sections:

- **Neurons for ITSM Deployment Overview**: Describes recommended and optional deployment architectures, including the Neurons for ITSM reporting feature and Ivanti Voice.
- **Neurons for ITSM Installation Prerequisites**: Provides information about confirming your role, the different accounts and passwords used in Neurons for ITSM, using a virtual machine, enabling file streaming and full-text search in Microsoft SQL Server, and verifying server roles and features.
- **Installing the Neurons for ITSM System**: Describes how to install Neurons for ITSM, including the Neurons for ITSM Operations Console, the reporting feature, ISM Discovery, and ISM Knowledge.
- **Initially Configuring the System**: Describes how to use the System Configuration Wizard to configure Neurons for ITSM, including its servers and databases; and how to use the Neurons for ITSM Operations Console to configure the deployment.
- **Upgrading Neurons for ITSM from an Earlier Release**: Contains information and instructions for upgrading Neurons for ITSM from an earlier release to the current release.
- **Using the License Manager**: Explains how to install and use the Neurons for ITSM License Manager.
- **Troubleshooting - Installation and Deployment**: Contains solutions to common problems.

3.1. Neurons for ITSM Deployment Overview

- Hardware Considerations
- Demonstration or Proof-of-Concept Deployment
- Minimum Production Deployment
- Enterprise Production Deployment
- Security Enterprise Production Deployment
- Database Deployment Options
- Operations Console Deployment Options
- Reporting Services Deployment Options
- Voice Deployment Options

Hardware Considerations

The following factors drive the hardware requirements for a new Neurons for ITSM deployment:

Neurons for ITSM supports separate landscapes: development (also called staging), test (also called UAT), and production. You can run these landscapes on the same server or isolate them on separate servers.
If you choose to run them on separate servers, you must provide additional hardware. Except for the demonstration or proof-of-concept deployment, we do not recommend putting all of the landscapes on one server.

- You can adjust the amount of hardware used after you deploy your system, after you have collected usage data. The Neurons for ITSM software is horizontally and vertically scalable, allowing you to add more hardware to increase performance without license changes.

3.1.1. Demonstration or Proof-of-Concept Deployment

- About the Demonstration or Proof-of-Concept Deployment
- Hardware Requirements for the Demonstration or Proof-of-Concept Deployment
- About Installing the Neurons for ITSM Components for the Demonstration or Proof-of-Concept Deployment

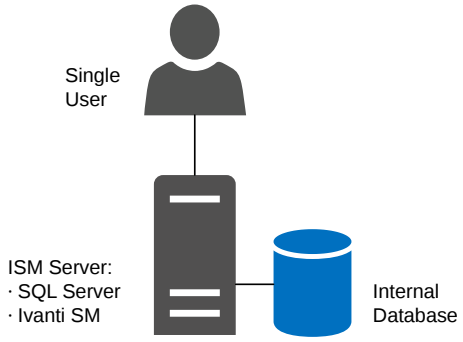
About the Demonstration or Proof-of-Concept Deployment

> This deployment is only recommended for demonstration purposes. Do not use this deployment for any production environment.

You can run the entire Neurons for ITSM system on a single server for the purpose of a demonstration or a proof-of-concept system.

Install Neurons for ITSM, with all options enabled, onto a single server that has Microsoft SQL Server loaded locally. Most users install this deployment in a virtual environment.

Example of Neurons for ITSM *and Databases on a Single Server*



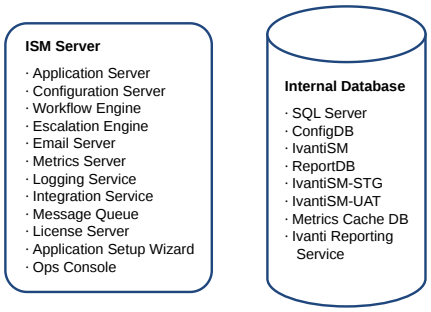
Hardware Requirements for the Demonstration or Proof-of-Concept Deployment

- 1 server, either virtual or physical
- 1 CPU
- 4 GB memory
- 40 GB hard drive

About Installing the Neurons for ITSM Components for the Demonstration or Proof-of-Concept Deployment

The below diagram shows the recommended locations of the various Neurons for ITSM software components in this deployment.

Neurons for ITSM *Components and Databases on a Single Server*



If you plan to include the Neurons for ITSM reporting feature in your deployment, you must install the Microsoft SQL Server Reporting Services (SSRS) component of Microsoft SQL Server. See **Installing Neurons for ITSM Reporting Feature**.

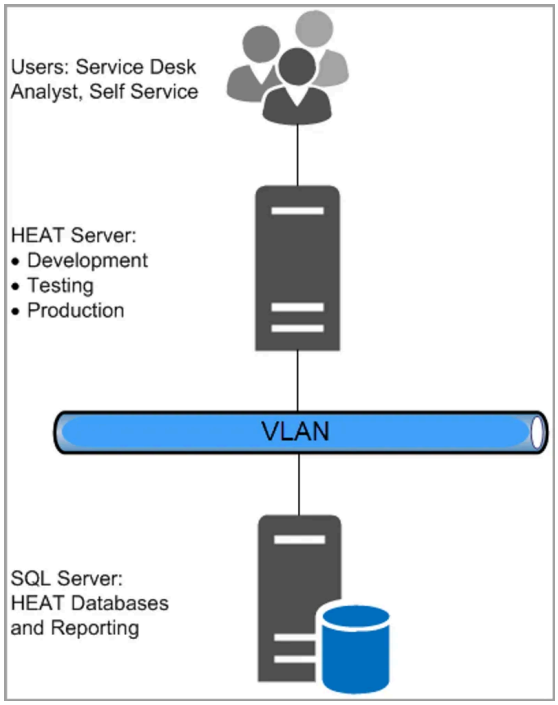
3.1.2. Minimum Production Deployment

- About the Minimum Production Deployment
- Hardware Requirements for the Minimum Production Deployment
- About Installing the Neurons for ITSM Components for the Minimum Production Deployment

About the Minimum Production Deployment

Customers with 10 or fewer users often want to minimize their hardware investment. With the minimum production deployment architecture, you install all Neurons for ITSM components, except for the Neurons for ITSM databases, onto a single server. We recommend that you install the Neurons for ITSM databases onto a separate Microsoft SQL server.

Example of Neurons for ITSM *and Databases on Separate Servers*



In this deployment, all three landscapes (development [staging], testing [UAT], and production) run on the same server. As a result:

- Any issues created during the development cycle might affect production users.
- You cannot perform preupgrade testing.

Hardware Requirements for the Minimum Production Deployment

The following are the hardware requirements for the Neurons for ITSM server:

- One server, either physical or virtual
- 2 CPU
- 4 GB memory
- 200 GB hard drive

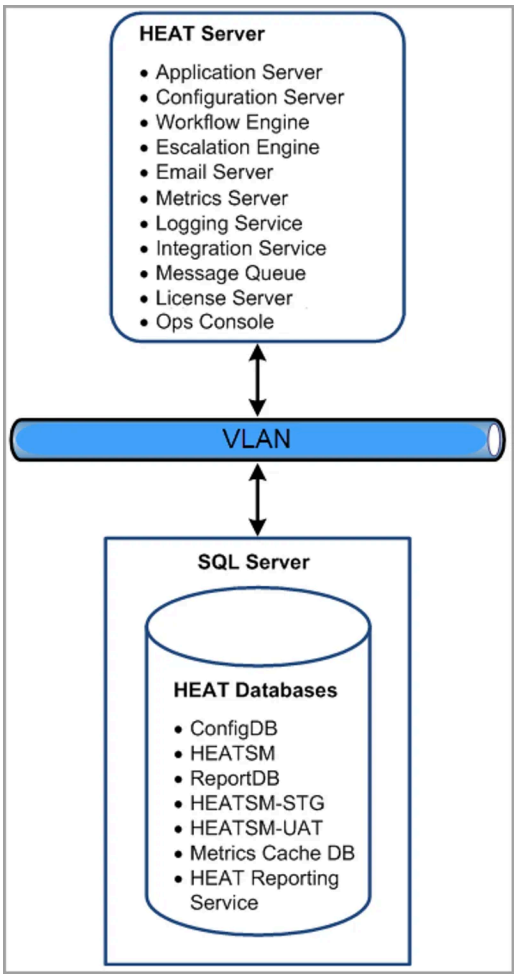
The following are the hardware requirements for the Microsoft SQL server where the databases reside:

- One server (we recommend a physical server)
- 2 CPU
- 8 GB memory
- 1 TB hard drive

About Installing the Neurons for ITSM Components for the Minimum Production Deployment

Neurons for ITSM Components and Databases on Separate Servers shows a diagram of the recommended locations of the various Neurons for ITSM software components in this deployment.

Neurons for ITSM *Components and Databases on Separate Servers*



3.1.3. Enterprise Production Deployment

Customers supporting large user populations of 100 or more are primarily concerned with availability and load management rather than with minimizing hardware expense. Customers with more than 100 users should use this setup as a baseline and then add the equivalent amount of hardware for each additional 100 users. The enterprise production deployment architecture splits Neurons for ITSM into:

- Front-end web servers
- Back-end processing servers

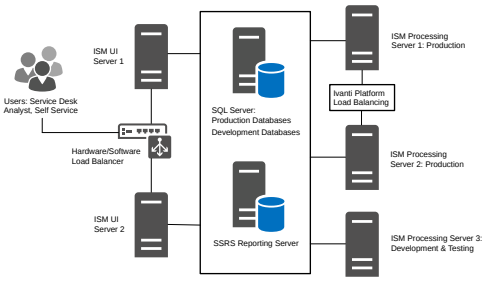
The back-end servers handle workflow, email processing, license allocation, inventory management, and so on. This architecture also separates the production environment from development and testing.

There are two key advantages of separating development and testing from production:

- Any issues created during the development cycle do not affect production users.
- You can perform upgrade testing on the development and testing servers before upgrading the production servers.

Optionally, you can install your development and test landscapes onto separate physical servers.

Example of Neurons for ITSM *in an Enterprise Deployment*



Hardware Requirements for the Enterprise Production Deployment

Web Servers

The following are the hardware requirements for the Neurons for ITSM web servers:

- Two virtual servers
- Outside the firewall
- Load balanced
- 4 CPU
- 16 GB memory
- 200 GB hard drive

Processing Servers (Production)

The following are the hardware requirements for the Neurons for ITSM processing servers used for the production landscape:

- Two virtual servers

- Inside the firewall
- Load balanced
- 4 CPU
- 16 GB memory
- 200 GB hard drive

Processing Servers (Development and Testing)

The following are the hardware requirements for the Neurons for ITSM processing server used for the development (staging) and testing (UAT) landscapes:

- One physical or virtual server
- 2 CPU
- 4 GB memory
- 200 GB hard drive

Microsoft SQL Server Requirements

Microsoft SQL Server is the database server for the deployment. Depending on your needs, you may have multiple database servers. The following are the requirements for the Microsoft SQL server where the databases reside:

- One physical server
- Microsoft SQL Server -
  - Microsoft SQL Server 2012 including Management Studio
  - Microsoft SQL Server 2012 SP2 including Management Studio
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2017
  - Microsoft SQL Server 2019
- Inside the firewall
- 8 CPU
- 24 GB memory
- 1 TB hard drive

> Customers may experience an error when Always On Availability is configured on the database server. Ivanti Service Manager currently does not support Always On Availability. For more details, see **Ivanti Community**.

Microsoft SSRS Reporting Server

The reporting feature requires that Microsoft SQL Server Reporting Services (SSRS) be installed and running on the database server that hosts the Neurons for ITSM reporting feature.

Microsoft SSRS can be installed on the Microsoft SQL server or on a separate Microsoft SSRS server, depending on your preference. We recommend a separate installation in the following situations:

- Multi-tenant environments, including managed service providers and enterprises with multiple Ivanti Service Manager tenants.
- The Microsoft SQL database is used also for applications other than Neurons for ITSM.
- Installations where the database server must remain online, because upgrading Microsoft SSRS often requires a reboot.

The following are the requirements for the Microsoft SQL Server Reporting Services (SSRS) reporting server:

- One physical server
- Microsoft SQL Server Release 2016
- Inside the firewall
- 8 CPU
- 24 GB memory
- 1 TB hard drive

Hardware Requirements when Adding Additional Users

For each additional 100 users, add this to architecture:

- Two additional Neurons for ITSM web servers.
- Two additional Neurons for ITSM processing servers.

System load determines the actual number of servers to add. You can add the web and processing servers on demand.

In most cases, you do not need to add more development (staging) or testing (UAT) servers.

High Availability and Load Balancing

You can achieve high availability through physical load balancing or by load balancing handled within Neurons for ITSM. For example, in the configuration shown in **Example of Neurons for ITSM in an Enterprise Deployment**. The Ivanti Service Manager components are connected to one or more load-balanced servers. In this example:

- The Neurons for ITSM web servers, which contain Neurons for ITSM components that are user-facing, all connect to a physical load-balancing server.
- The Neurons for ITSM process servers, which contain Neurons for ITSM components that are not user-facing, do not connect to a physical load-balancing server, but instead use a built-in load balancer. The escalation engine, workflow engine, and email server have built-in load-balancing mechanisms.
- The Neurons for ITSM web servers and process servers all connect to the same Ivanti Service Manager application database and configuration database. High availability for the Neurons for ITSM databases is achieved through a cluster.

Communication within the system, such as between an Neurons for ITSM process server and an Neurons for ITSM web server, does not require SSL. However, external communication can use SSL.

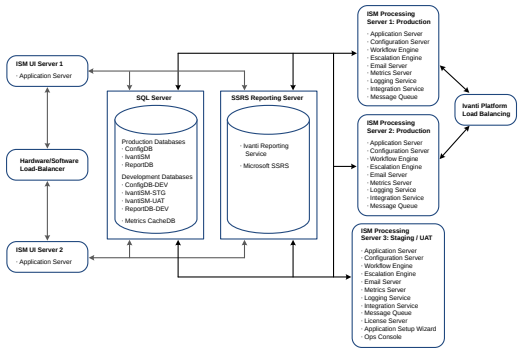
> By default, the **Use SSL** checkbox in all instances will be selected for new customers. New customers must provide the fully qualified domain name for the server location in the **SSL certificate** field. However, the **Use SSL** checkbox is not selected by default for the existing customer, and they have to select **Use SSL** if needed and provide the domain name. For more details on the **SSL Certificate**, see **Optional SSL Configuration**.

When using a hardware load balancer, turn on session persistence so that connections from the web browsers always get directed to the same web server.

About Installing the Neurons for ITSM for the Enterprise Production Deployment

Neurons for ITSM Components and Databases in an Enterprise Deployment shows a diagram of the recommended locations of the various Neurons for ITSM components.

Neurons for ITSM *Components and Databases in an Enterprise Deployment*



3.1.4. Security Enterprise Production Deployment

- About the Security Enterprise Production Deployment
- About Using a DMZ with Web Servers
- About Using a DMZ with Reverse Proxy Servers

About the Security Enterprise Production Deployment

This deployment is based on the Enterprise Production Deployment w ith a DMZ added to provide security where users log in from outside of the company network.

We recommend the following DMZ configurations:

- DMZ with Neurons for ITSM web servers
- DMZ with reverse proxy servers

The DMZ is configured for authenticated access. When web servers are in the DMZ, each user must enter his user name and password to log into Neurons for ITSM. This architecture involves the additional cost of setting up and maintaining two firewalls.

Where you implement reverse proxy servers, you can add another layer of access authentication. This architecture involves the additional cost of setting up and maintaining two reverse proxy servers and a load balancer.

About Using a DMZ with Web Servers

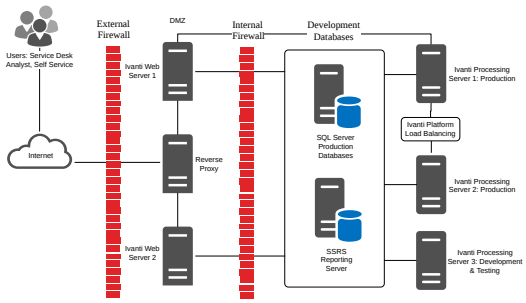
This option offers a greater level of security than placing your Neurons for ITSM web servers outside of a single company firewall. Placing a second firewall between the Internet and the web servers forms a semi-trusted network that prevents external access to your Neurons for ITSM process servers and databases.

We recommend that you harden the Neurons for ITSM web servers by taking the following actions:

- Disabling all unnecessary services
- Running necessary services with the lowest possible privileges
- Requiring strong passwords
- Locking an account after a certain number of login failures
- Deleting or disabling unnecessary user accounts, such as the guest user account
- Renaming or changing the description of the administrator account
- Installing the latest security updates and patches on the server
- Enabling security logging and checking the logs frequently

The same Neurons for ITSM components are installed on the web servers when they are located in the DMZ as when they are located outside of the company firewall. See About Installing the Neurons for ITSM for the Enterprise Production Deployment.

Example of an Enterprise Deployment with Neurons for ITSM *Web Servers in the DMZ*



About Using a DMZ with Reverse Proxy Servers

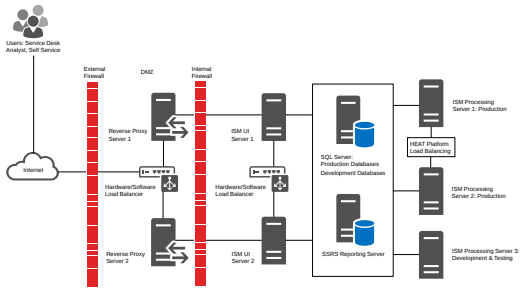
This option offers the greatest level of security by placing your web servers inside the company firewall. By placing reverse proxy servers in the DMZ, you prevent direct user login to the Neurons for ITSM web servers.

In addition, by locating the web servers on the same network as the process servers and databases, you achieve a true three-tier architecture.

The same Neurons for ITSM components are installed on the web servers when they are located inside the firewalls as when the servers are located outside.

This architecture involves the additional costs of servers to host the reverse-proxy service, as well as setting up and maintaining a second firewall. See **About Installing the Neurons for ITSM for the Enterprise Production Deployment**.

Example of an Enterprise Deployment with Neurons for ITSM *Reverse Proxy Servers in the DMZ*



3.1.5. Database Deployment Options

This section describes the different options available for the Neurons for ITSM databases.

- About the Databases Used in Neurons for ITSM
- Diagram Conventions
- Option D1: Separate Database Servers (Recommended and Best Practice)
- Option D2a: Single Database Server (Best Practice)
- Option D2b: Single Database Server
- Option D3: Single Configuration Database on a Single Database Server
- Option D4: Multiple Configuration Databases on a Single Server
- Option D5: Multiple Configuration Databases on Multiple Servers
- Option D6: Single Configuration Database on Separate Database Servers (for MSPs)
- Option D7: Multiple Configuration Databases on Separate Database Servers (for MSPs)

About the Databases Used in Neurons for ITSM

The following are the databases used in Neurons for ITSM:

- configuration database (ConfigDB)
- Neurons for ITSM application database (IvantiSM)
- Neurons for ITSM reporting database (ReportDB). This database is used for the reporting feature. See Reporting Services Deployment Options for more information.
- Metrics cache database (Metrics Cache DB). This database is used to cache the run-time state of the schedule jobs. Only one metrics cache database is needed in each isolated landscape. For example, if the configuration database and the Neurons for ITSM application database are hosted on the same database server, your deployment only needs one metrics cache database.

In addition, there are generally three instances for each tenant:

- Staging
- UAT
- Production

Each tenant instance, Staging (development), UAT (Test) and Production, can have its own database instance or server. These are called:

Database	Description
IvantiSM	Application database for production
IvantiSM-STG	Application database for staging (development)
IvantiSM-UAT	Application database for UAT (testing)
IvantiSM-Dev	Application database for staging (development) and UAT (testing)
ConfigDB	Configuration database for production
ConfigDB-STG	Configuration database for staging (development)
ConfigDB-UAT	Configuration database for UAT (testing)
ConfigDB-Dev	Configuration database for staging (development) and UAT (testing)
ReportServer	Report database for production
ReportServer-STG	Report database for staging (development)
ReportServer-UAT	Report database for UAT (testing)
ReportServer-Dev	Report database for staging (development) and UAT (testing)

The advantage of hosting a database on its own server is that it ensures security by isolating the production landscape. It also enhances performance. When you make multiple changes or upgrades to the staging or UAT landscapes, you do not want that to affect the performance of the production landscape. Separating the different databases makes it easier to upgrade the systems, because when you upgrade the systems you have to shut them down and that affects users in the production landscape.

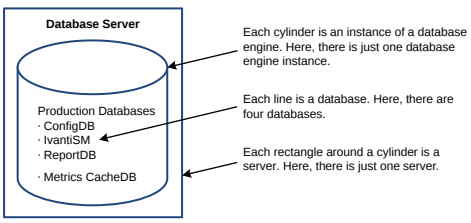
The advantage of hosting everything on one server is that you save money by only having to purchase and administer one server and one Microsoft SQL Server license.

Diagram Conventions

The following conventions are used in the diagrams:

- A line item is considered a database. There can be many databases within one database engine instance.
- A barrel is considered a database engine instance. It can contain multiple database instances.
- A square or rectangle around something means it is on one server (machine). Each server can potentially host multiple database engine instances.

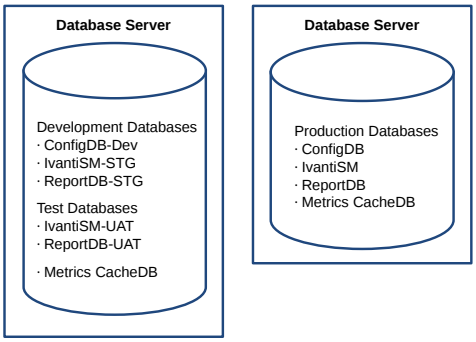
Diagram Conventions



Option D1: Separate Database Servers (Recommended and Best Practice)

In this deployment, there are two separate database servers. One is for the production landscape and the other is for the staging and UAT landscape. The staging and UAT servers share a configuration database.

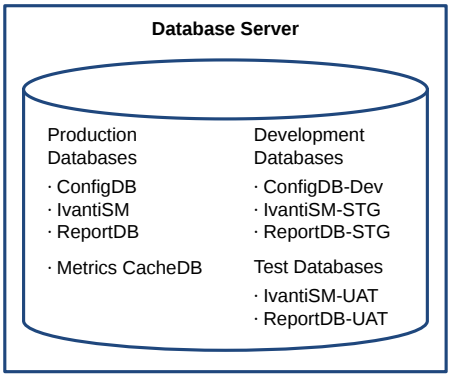
Example of Separate Database Servers



Option D2a: Single Database Server (Best Practice)

In this deployment, there is a single database server and one configuration database (ConfigDB-Dev).

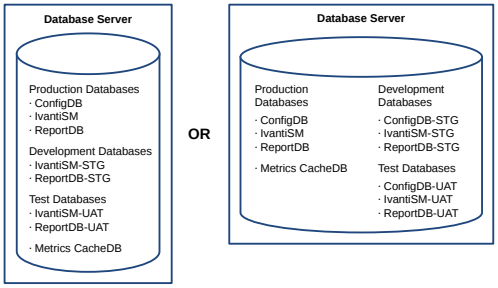
Example of Recommended Single Database Server



Option D2b: Single Database Server

In this deployment, there is a single database server and either no configuration database or two configuration databases (ConfigDB-STG and ConfigDB-UAT).

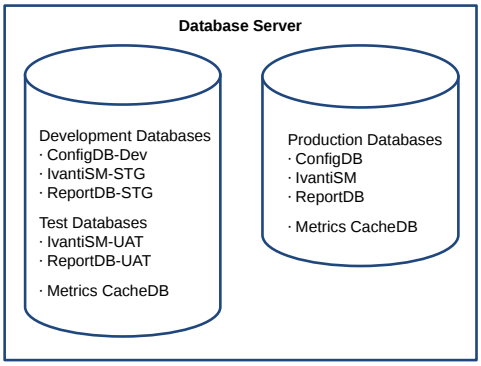
Example of Alternative Single Database Servers



Option D3: Single Configuration Database on a Single Database Server

In this deployment, there is one configuration database for the production landscape and another configuration database shared between the staging and UAT landscapes.

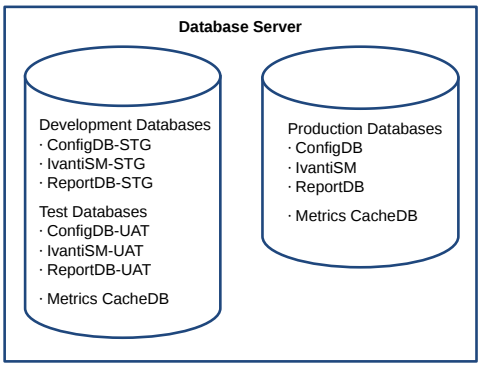
Example of Separate Database Engine Instances on a Single Database Server



Option D4: Multiple Configuration Databases on a Single Server

In this deployment, there are separate configuration databases for the production landscape, the staging landscape, and the UAT landscape.

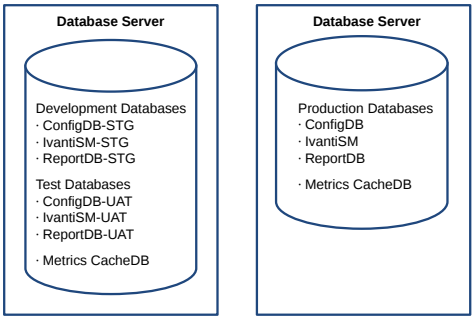
Example of Multiple Configuration Databases on a Single Server



Option D5: Multiple Configuration Databases on Multiple Servers

In this deployment, there are separate configuration databases for the production landscape, the staging landscape, and the UAT landscape and separate instances.

Example of Multiple Configuration Databases on Multiple Servers

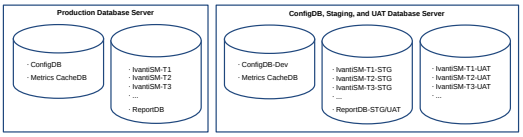


Option D6: Single Configuration Database on Separate Database Servers (for MSPs)

A Managed Service Provider (MSP) is a service partner who provides Neurons for ITSM for multiple tenants or outside customers.

In this deployment, there is a single configuration database shared between landscapes.

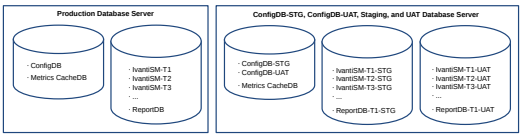
Example of a Single Configuration Database on Separate Database Servers



Option D7: Multiple Configuration Databases on Separate Database Servers (for MSPs)

In this deployment, there are separate configuration databases for the production landscape, the staging landscape, and the UAT landscape and separate instances.

Example of Multiple Configuration Databases on Separate Database Servers



3.1.6. Operations Console Deployment Options

- About the Neurons for ITSM Operations Console Deployment Options
- Option OC1: Separate Configuration Databases and Application Servers for Production and Development (Best Practice)
- Option OC2: Two Configuration Databases and Separate Application Servers for Each Landscape (Best Practice)
- Option OC3: Separate Configuration Databases for Each Landscape (Best Practice)
- Option OC4: One Configuration Database and One Application Server
- Option OC5: One Configuration Database and Separate Application Servers for Each Landscape

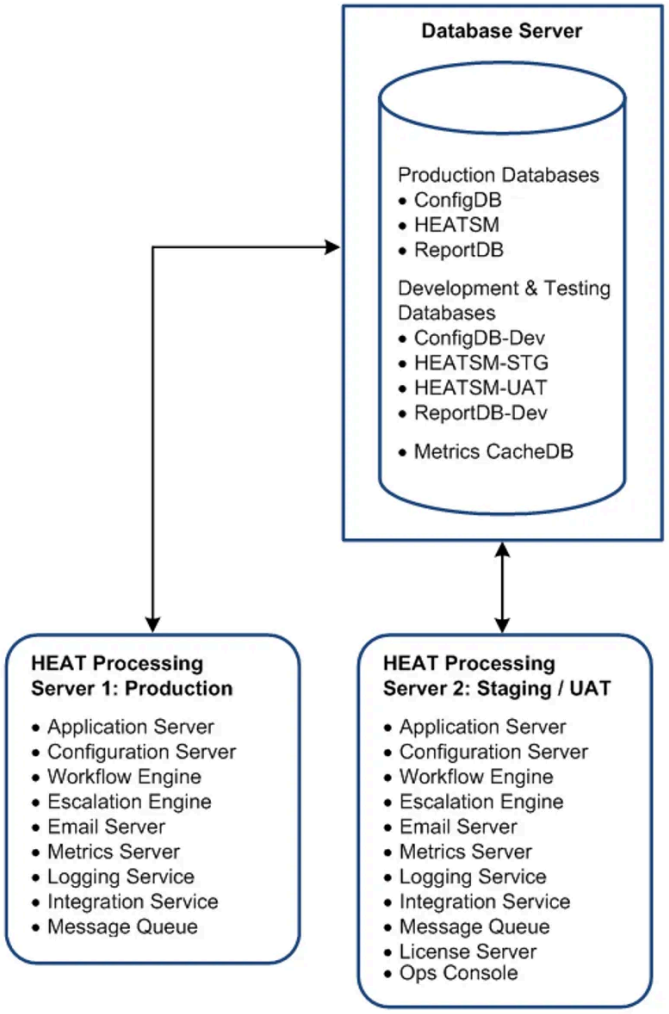
About the Neurons for ITSM Operations Console Deployment Options

- Determine your database deployment options first. In all of the Operations Console deployment options below, you can substitute any of the database deployments described in Database Deployment Options for the database deployments in the figure. So for the database engine instance shown in Option OC1 below, you could substitute Option D1, Option D2a, Option D2b, Option D3, and so on for that database engine instance.
- To use the Operations Console, the production, staging, and UAT application servers must all use the same version of Neurons for ITSM. When you test new versions of Neurons for ITSM, either install the new version in a separate environment or plan the Operations Console pushes before testing the new version.
- We recommend using a deployment that has either two or three configuration databases, such as Option OC1, Option OC2, or Option OC3.

Option OC1: Separate Configuration Databases and Application Servers for Production and Development (Best Practice)

You only install the Operations Console on the staging/UAT server. Do not install it on any other servers.

Example of Separate Configuration Databases and Application Servers for Production and Development



Option OC2: Two Configuration Databases and Separate Application Servers for Each Landscape (Best Practice)

You only install the Operations Console on the staging server. Do not install it on any other servers.

Example of Two Configuration Databases and Separate Application Servers for Each Landscape

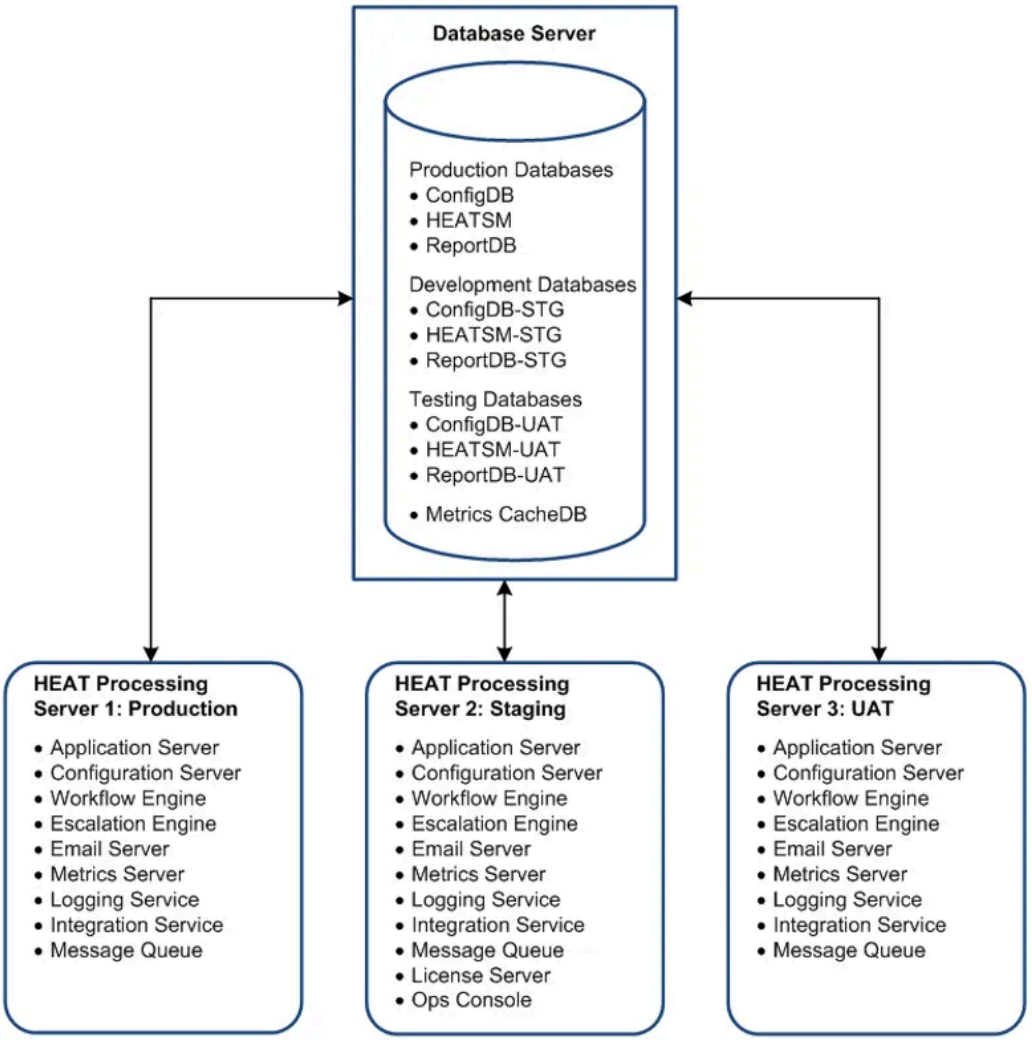


Option OC3: Separate Configuration Databases for Each Landscape (Best Practice)

> The only use case for this option is to upgrade the staging or UAT landscape at different times.

You only install the Operations Console on the staging server. Do not install it on any other servers.

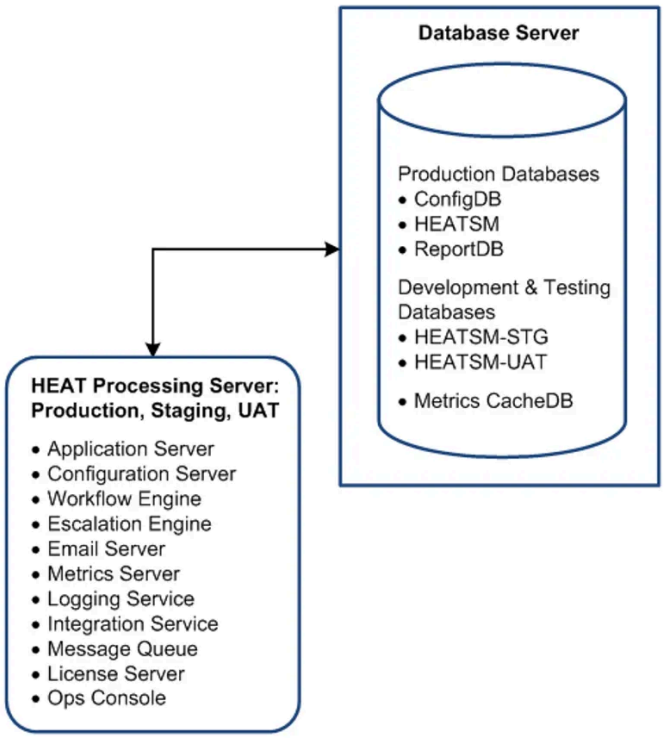
Example of Separate Configuration Databases for Each Landscape



Option OC4: One Configuration Database and One Application Server

We do not recommend using this or any similar deployment that has only one configuration database that is used for IvantiSM, IvantiSM-STG, and IvantiSM-UAT, unless you are setting up a demo environment. The reason for this only being viable for demo environments is that this deployment prevents you from being able to test future upgrades on development tenants without forcing production to upgrade at the same time.

Example of One Configuration Database and One Application Server

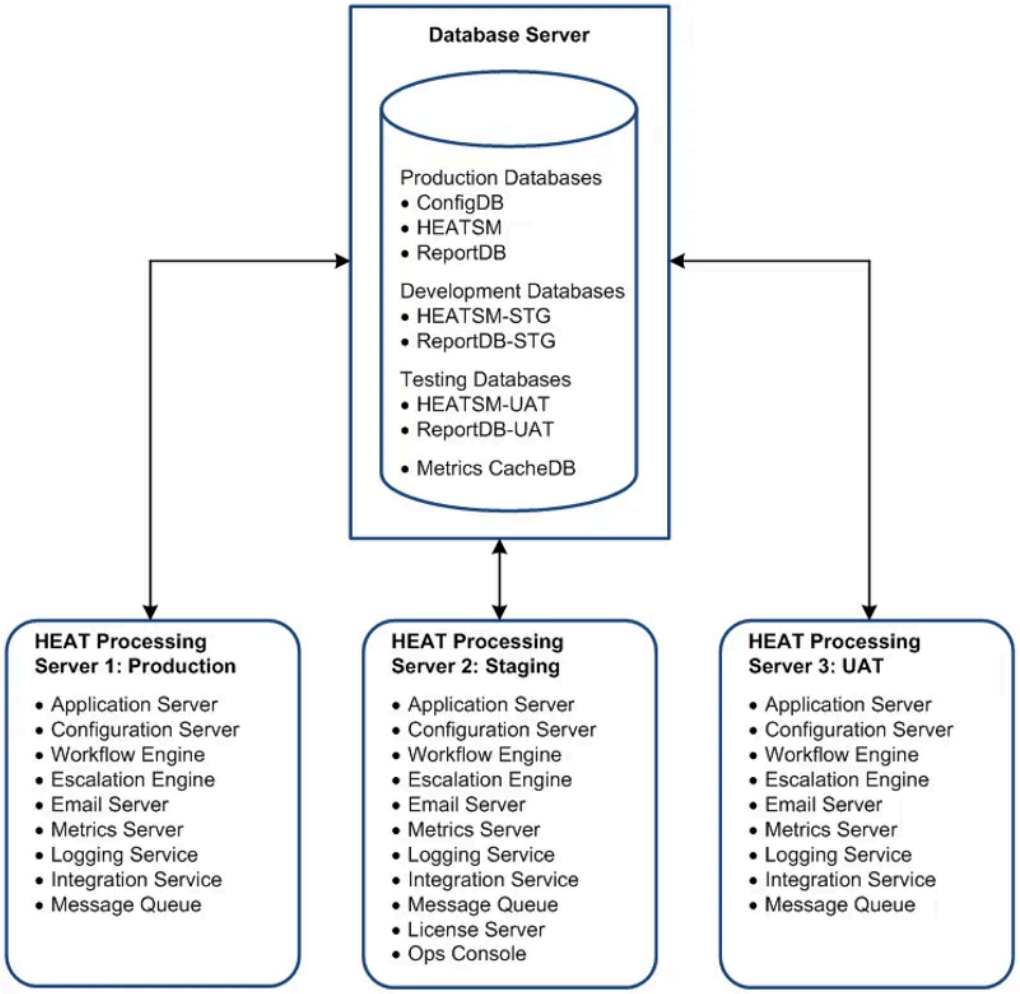


Option OC5: One Configuration Database and Separate Application Servers for Each Landscape

> We do not recommend using this or any similar deployment that has only one configuration database that is used for IvantiSM, IvantiSM-STG, and IvantiSM-UAT, unless you are setting up a demo environment. The reason for this only being viable for demo environments is that this deployment prevents you from being able to test future upgrades on development tenants without forcing production to upgrade at the same time.

You only install the Operations Console on the staging server. Do not install it on any other servers.

Example of One Configuration Database and Separate Application Servers for Each Landscape


Database Server
Production Databases
• ConfigDB
• HEATSM
• ReportDB
Development Databases
• HEATSM-STG
• ReportDB-STG
Testing Databases
• HEATSM-UAT
• ReportDB-UAT
• Metrics CacheDB
HEAT Processing Server 1: Production
• Application Server
• Configuration Server
• Workflow Engine
• Escalation Engine
• Email Server
• Metrics Server
• Logging Service
• Integration Service
• Message Queue
HEAT Processing Server 2: Staging
• Application Server
• Configuration Server
• Workflow Engine
• Escalation Engine
• Email Server
• Metrics Server
• Logging Service
• Integration Service
• Message Queue
• License Server
• Ops Console
HEAT Processing Server 3: UAT
• Application Server
• Configuration Server
• Workflow Engine
• Escalation Engine
• Email Server
• Metrics Server
• Logging Service
• Integration Service
• Message Queue

3.1.7. Reporting Services Deployment Options

- About the Reporting Services Deployment Options
- Option R1: Multiple Microsoft SSRS Instances on the Same Database Server (Best Practice)
- Option R2: Separate Microsoft SSRS Instances and a Separate Database Server (Best Practice)
- Option R3: Separate Microsoft SSRS Instances
- Option R4: Multiple Microsoft SSRS Instances on a Separate Report Server
- Option R5: Single Microsoft SSRS Instance on One Database Server

About the Reporting Services Deployment Options

- Determine your database deployment options first (see **Database Deployment Options**), and then your Operations Console deployment options (see Neurons for ITSM**Operations Console Deployment Options**). Then determine your reporting services deployment options.

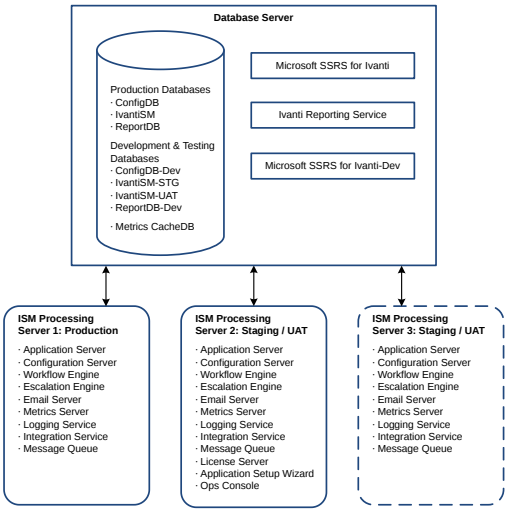
In all of the reporting services deployment options below, note the following:

  - You can substitute any of the database deployments described in **Database Deployment Options** for the database deployments in the figure. For example, for the database engine instance shown in Option R5 below, you could substitute Option D1, Option D2a/b, Option D3, and so on for that database engine instance.
  - You can substitute any of the Operations Console deployments described in Neurons for ITSM**Operations Console Deployment Options** for the Operations Console deployments in the figure. For example, for the single application server shown in Option R5 below, you could substitute Option OC3 for that application server.
- The Neurons for ITSM report database can reside on a separate database instance, or on a database instance on a separate server.
- The Microsoft SSRS instance can run on the Neurons for ITSM database server, application server, or on a separate server.
- The reporting feature should be installed on the Microsoft SSRS Server.
- We recommend using either Option R1 or Option R2.

Option R1: Multiple Microsoft SSRS Instances on the Same Database Server (Best Practice)

This deployment is the most common and recommended for simplicity and security. The advantage of this deployment is that you have a reporting feature for production that is separate from the development environments.

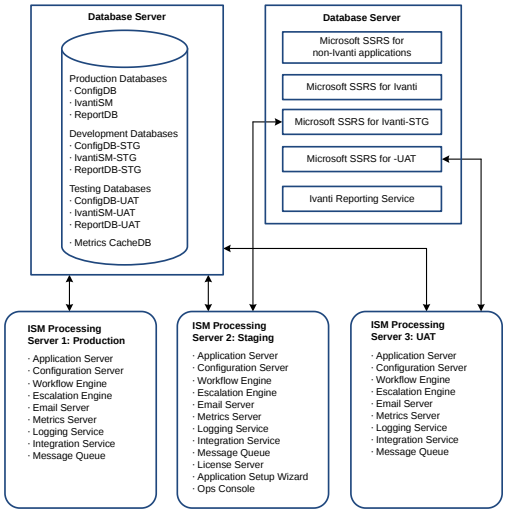
Example of Multiple Microsoft SSRS Instance on One Database Server



Option R2: Separate Microsoft SSRS Instances and a Separate Database Server (Best Practice)

Use this deployment to keep the reporting separate between the production and development environments.

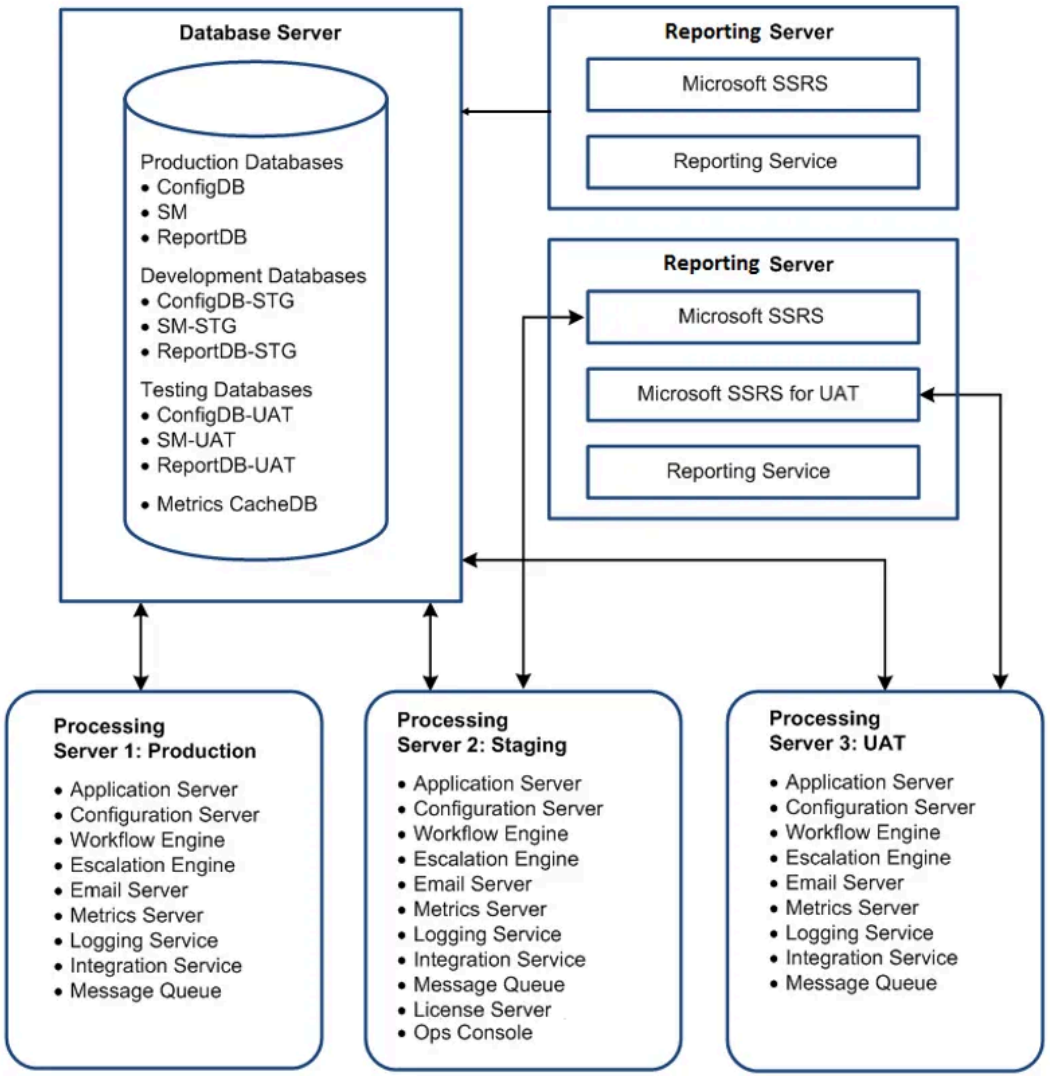
Example of Separate Microsoft SSRS Instances and a Separate Database Server



Option R3: Separate Microsoft SSRS Instances

Use this deployment to keep the reporting separate between the production and staging/UAT environments.

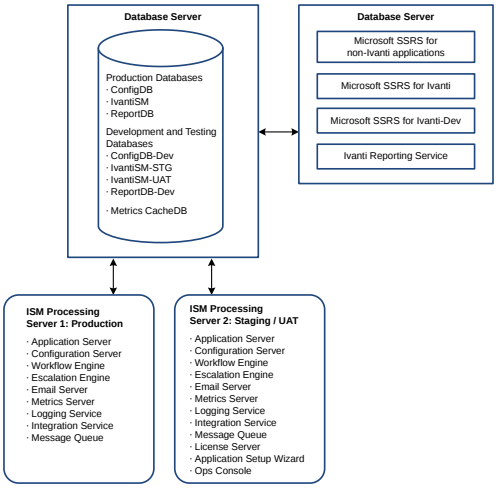
Example of Separate Microsoft SSRS Instances



Option R4: Multiple Microsoft SSRS Instances on a Separate Report Server

This deployment is recommended if you need to maintain your database in a locked down environment and keep it separate from the development environment. We also recommend this deployment if you already have a server with a Microsoft SSRS instance for other applications.

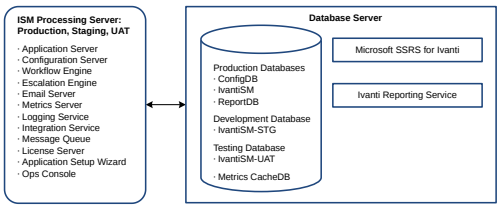
Example of a Multiple Microsoft SSRS Instances on a Separate Report Server



Option R5: Single Microsoft SSRS Instance on One Database Server

> We do not recommend using this deployment unless you are setting up a demo environment.

Example of a Single Microsoft SSRS Instance on One Database Server



3.1.8. Voice Deployment Options

- About Ivanti Voice
- About this Deployment
- Installing and Configuring Ivanti Voice
- Integrating Ivanti Voice with Neurons for ITSM

About Ivanti Voice

Ivanti Voice is the telephony application that integrates automated call routing and management and computer telephone integration to Ivanti Software applications such as Neurons for ITSM. Ivanti Voice uses the next-generation, standards-based IP communication transport, called Session Initiation Protocol (SIP). Neurons for ITSM and Voice are typically installed and maintained on separate servers..

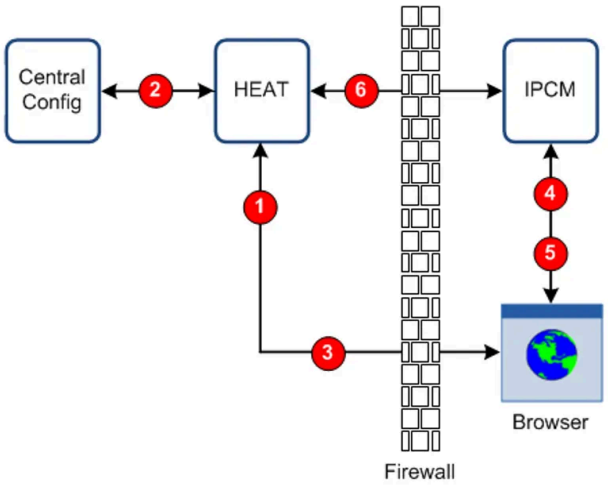
About this Deployment

- Agent Login Sequence
- Incoming Call Sequence

Agent Login Sequence

Agent Login Sequence shows the Voice agent login sequence.

Agent Login Sequence

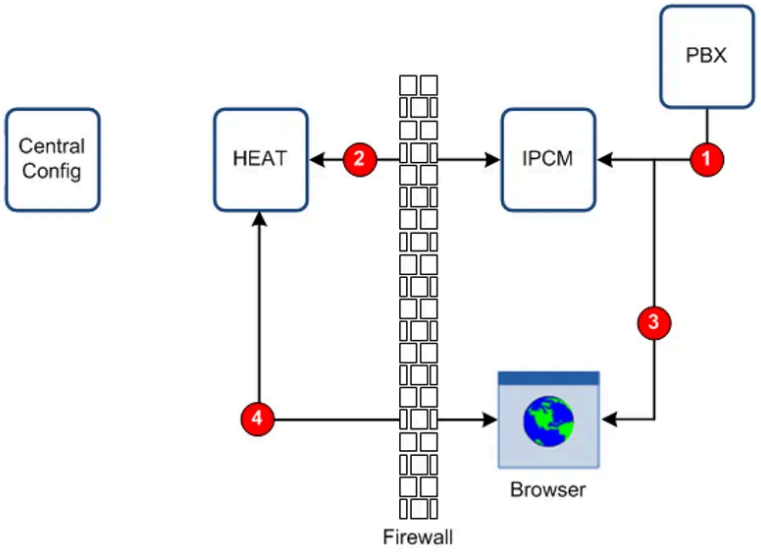


1. The agent logs into a secure (HTTPS) connection.
2. The system verifies the Voice server IP address or domain name.
3. The system obtains the session key from the Ivanti Voice server IP address or domain name.
4. The system verifies the session key (TCP 5743).
5. The system makes the phone connection (SIP UDP 5060).
6. The system validates the session key (HTTPS).

Incoming Call Sequence

Incoming Call Sequence shows the sequence of events for Ivanti Voice incoming calls.

Incoming Call Sequence



1. The system receives a call (SIP UDP 500).
2. The IVR searches and updates the record (HTTPS).
3. The call is forwarded to the agent (SIP UDP 5060, RTP UDP, TCP 5743).
4. The record appears to the agent (HTTPS).

Installing and Configuring Ivanti Voice

For information about installing and configuring Ivanti Voice, see the *IP Communications Management Administrator Guide*.

Integrating Ivanti Voice with Neurons for ITSM

For complete information about integrating Voice with Neurons for ITSM, see *Working with Voice* in the Neurons for ITSM online help.

3.2. Neurons for ITSM Installation Prerequisites

Before you install Neurons for ITSM, do the following:

- Confirm your role. See **About Roles**.
- Create the needed accounts. See **About the Different Accounts Used in Neurons for ITSM**.
- Meet the system, hardware, and software prerequisites. This information is contained in the *System Requirements and Compatibility Matrix for* Neurons for ITSM.
- Configure the ports needed for your deployment. This information is contained in the *System Requirements and Compatibility Matrix for* Neurons for ITSM.
- If you are going to deploy Neurons for ITSM as a virtual image, review the requirements at **About Using a Virtual Machine with Neurons for ITSM**.
- Ensure that the FILESTREAM feature is enabled on the Microsoft SQL Server. See **Enabling Attachment File Streaming**.
- If you are going to deploy the reporting feature, ensure that Microsoft SQL Server Reporting Services (SSRS) is enabled. See **Installing Neurons for ITSM Reporting Feature**.
- Enable full-text search for Microsoft SQL Server. See **Full Text Search** .
- (Optional) Verify the server roles and features described in **Verifying Server Roles and Features**.
- Determine the directories in which to install the Neurons for ITSM components on the host that you are logged into.
- Install the following from the installer package:
  - Prerequisite Installer
  - System Configuration Wizard (SCW)
  - Additional App Domain shared in the package - do this post the SCW installation.

3.2.1. About Roles

- Administrator Account Permissions
- Database Access Rights Needed for Neurons for ITSM
- Database Access Rights Needed for the Reporting Feature

Administrator Account Permissions

Use your account that has local administrator permissions to install Neurons for ITSM, including all optional components. This administrator account must have permission to create and modify folders, files, and registry keys.

Database Access Rights Needed for Neurons for ITSM

The following are the minimum access rights required for the account of the user running the System Configuration Wizard:

Role	Access Right
Server	public
	dbcreator
	securityadmin NOTE: This role is only needed temporarily, to assign the db_owner role to the configuration database and the Neurons for ITSM databases.

If you do not want to give this permission to the user running the System Configuration Wizard, you must go into the Microsoft SQL Server Management Studio and manually assign the service account as the db_owner for the configuration database and the Neurons for ITSM databases.

Database Access Rights Needed for the Reporting Feature

The following are the minimum access rights used in Microsoft SQL Server Management Studio for Neurons for ITSM when also using the reporting feature:

Role	Access Right
Server	public
	dbcreator
	securityadmin *
Database	db_owner of master
	db_owner of msdb
* The securityadmin role, and the db_owner of the master Microsoft database, are only needed if you set up Microsoft SSRS and create a new report server database. If you have already configured Microsoft SSRS and do not make any changes to it, you do not need this role. The securityadmin role creates the following Microsoft SSRS-related roles in the master, msdb, report server, and report server temporary databases: • RSExecRole • SQLAgentOperatorRole • SQLAgentReaderRole • SQLAgentUserRole	

The service account for Microsoft SSRS requires:

Database	Role
MSDB	RSExecRole
	SQLAgentOperatorRole
	SQLAgentReaderRole
	SQLAgentUserRole
Master	RSExecRole
Report server	RSExecRole
	db_owner
Report server temporary	RSExecRole
	db_owner

3.2.2. About the Different Accounts Used in Neurons for ITSM

Before you install and configure Neurons for ITSM, you must create and know the credentials for the following accounts:

- IT Account
- Database Account
- Service Account

During configuration of Neurons for ITSM, you create the following accounts:

- Administrator Account for the Configuration Database
- Administrator Account for Neurons for ITSM
- Administrator Account for the Reporting Service
- Administrator Account for the Operations Console

IT Account

This is the account that you are logged into when installing Neurons for ITSM and running the System Configuration Wizard.

You must create this account before you start the installation. This account must have administrator privileges on the servers on which you install Neurons for ITSM. Your IT department sets up this account for you.

Database Account

You must create this account before you start the installation.

You enter your credentials for the Neurons for ITSM database account on the following System Configuration Wizard pages:

- **Configuration Application**
- **Ivanti Service Manager Application**
- **Metrics Server**
- **Ivanti Discovery Application Server**

If you plan on installing the reporting feature, you also enter your credentials for the Neurons for ITSM database account on the following System Configuration Wizard pages:

- **Microsoft SSRS Configuration**
- **Reporting Service Configuration**

Service Account

You must create this account before you start the installation and configuration and it must have administrator privileges on the Neurons for ITSM application server.

A Neurons for ITSM service account is only required when you:

- Do not use the local system account for the Microsoft IIS application pool identity and Windows service.
- Install the reporting feature.

You enter your credentials for the Neurons for ITSM service account on the following System Configuration Wizard pages:

- **Ivanti Application Server Settings**
- **Microsoft SSRS Configuration**

Administrator Account for the Configuration Database

This account enables you to log into the configuration database.

You create this account during system configuration on the **Configuration Application** page of the System Configuration Wizard.

There will probably be different accounts used for different tenants.

Administrator Account for Neurons for ITSM

This account enables you to log into Neurons for ITSM, with access to the Service Desk Console and Configuration Console.

You create this account during system configuration on the **Ivanti Service Manager Application** page of the System Configuration Wizard.

There will probably be different accounts used for different tenants.

Administrator Account for the Reporting Service

This account enables you to log into the reporting feature.

You create this account during system configuration on the **Reporting Service Configuration** page of the System Configuration Wizard.

Administrator Account for the Operations Console

This account enables you to log into the Operations Console.

You create this account during system configuration when you check Use this host for Operations Console on the **Ivanti Application Server Settings** page of the System Configuration Wizard.

3.2.3. About Passwords Used in Neurons for ITSM

We recommend that you follow industry standards for creating strong passwords.

For more information, refer to **Microsoft - Strong Passwords** and **Microsoft - Password Policy.**

3.2.4. About Using a Virtual Machine with Neurons for ITSM

You can also deploy Neurons for ITSM as a virtual image. If you use a virtual machine, always keep the same universally unique identifier (UUID).

Refer to the documentation specific to the virtual machine you are using for more information.

> Any virtual machine platform that meets the **System Requirements** is compatible with Neurons for ITSM.

3.2.5. Enabling Attachment File Streaming

- About Enabling Attachment File Streaming
- Task 1: Enabling the FILESTREAM Feature
- Task 2: Setting up Neurons for ITSM
- Task 3: Running the File Stream Attachment Script

About Enabling Attachment File Streaming

Microsoft SQL Server 2022 and later versions come with enhanced support for unstructured data in the form of the FILESTREAM data type, which stores unstructured data files in the NTFS file system while storing the metadata about the unstructured data files in the Microsoft SQL Server database. For more information, see https://technet.microsoft.com/en-us/library/bb933993(v=sql.105).aspx.

Beginning with Release 2016.1.1, Neurons for ITSM supports the FILESTREAM attachment type when you perform the tasks below.

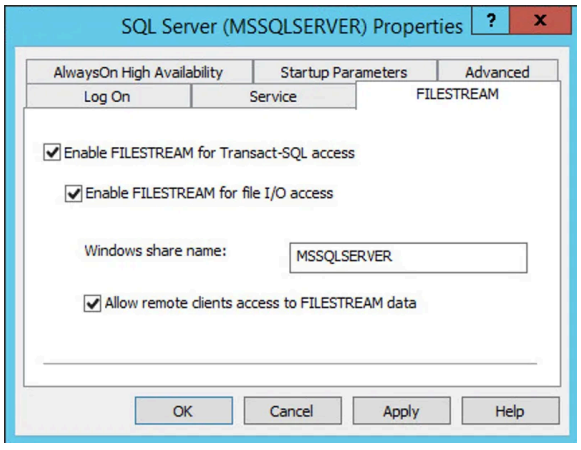
> This procedure is only required for deployments that store FILESTREAM attachments.

Task 1: Enabling the FILESTREAM Feature

You must enable the FILESTREAM feature on the Microsoft SQL Server instances where you plan to install the configuration database and the Neurons for ITSM application database. The database administrator normally performs this task.

1. On the database server, go to the Windows apps menu and click SQL Server Configuration Manager.
2. Navigate to the **SQL Server Services** node and double-click the Microsoft SQL Server instance to modify. For example, select SQL Server (MSSQLSERVER).

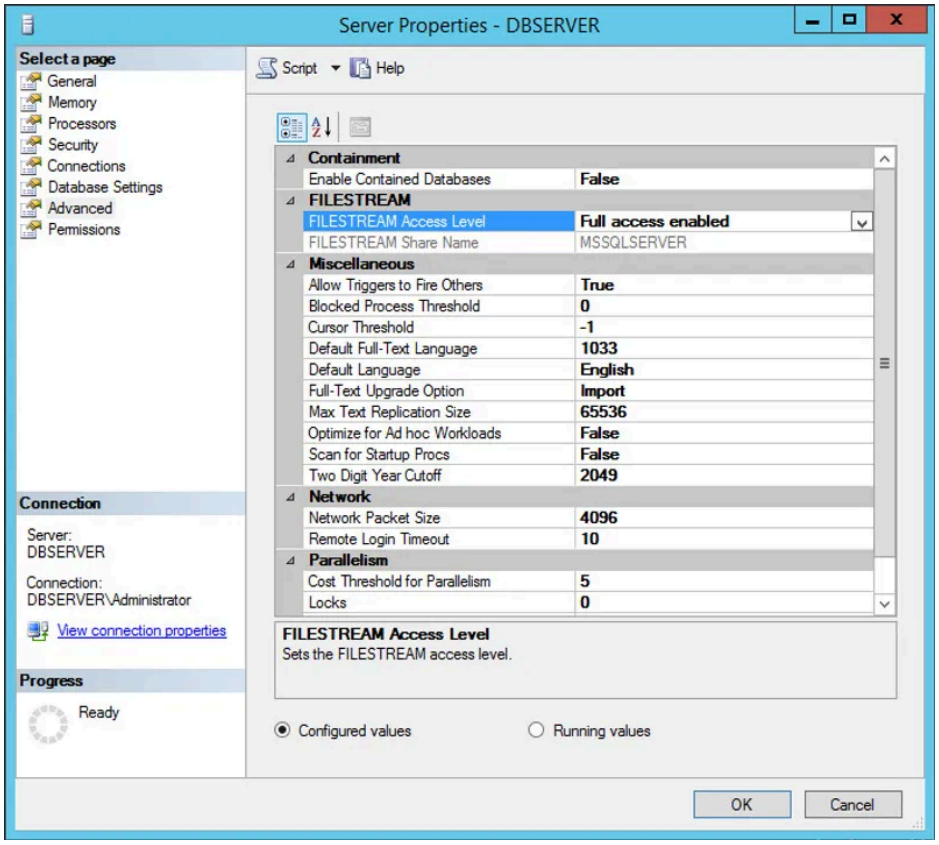
   Microsoft SQL Server Properties Dialog Box

3. Click the **FILESTREAM** tab.
4. Check Enable FILESTREAM for Transact-SQL access and Enable FILESTREAM for file I/O access.
5. Enter a Windows share name for the files.
6. Check Allow remote clients access to FILESTREAM data.
7. Click OK.

8. On the database server, go to the Windows apps menu and click SQL Server Management Studio.
9. In Microsoft SQL Server Management Studio, connect to the database server.
10. Right-click the server and choose Properties from the pop-up menu.
11. Under **Select a page**, click Advanced.
12. Double-click the entry called FILESTREAM Access Level until it displays Full access enabled.
13. Click OK.
14. (Optional) If you see a restart required message, restart the Microsoft SQL Server.

Microsoft SQL Server Properties



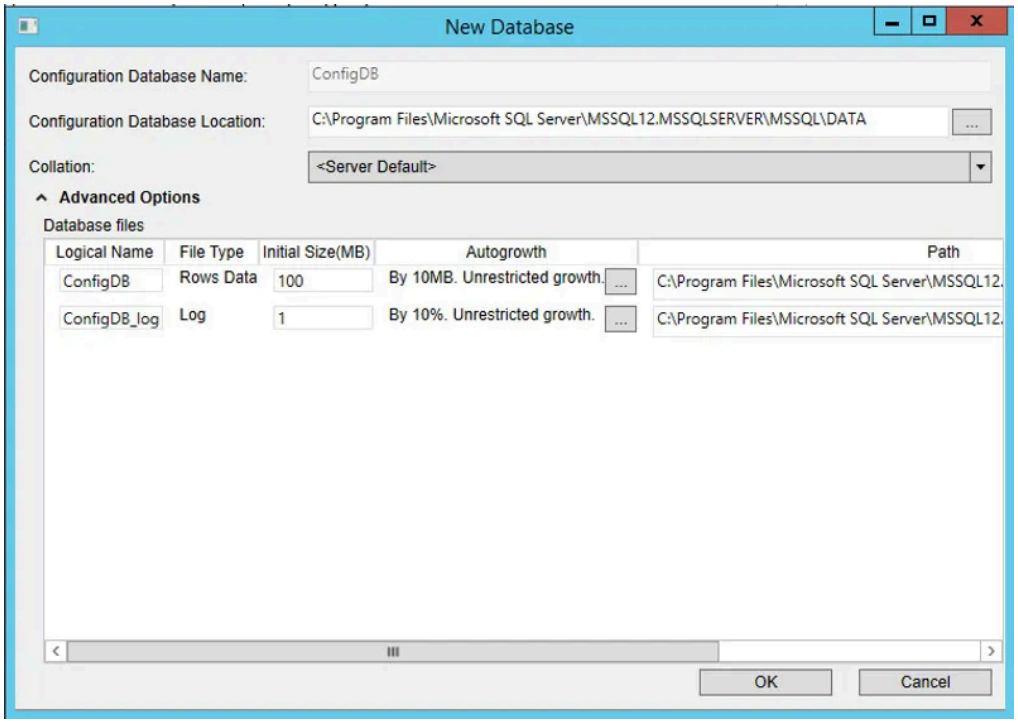
Task 2: Setting up Neurons for ITSM

The Neurons for ITSM application database and the configuration database are Microsoft SQL databases. On Microsoft SQL databases, user accounts with the db_owner fixed database role can perform all configuration and maintenance activities on the database.

These steps are in addition to those described under **Configuring Neurons for ITSM** .

1. On the database server, go to the Windows apps menu and click System Configuration Wizard.
2. On the **Configuration Application** page, specify a configuration database user account that has a db_owner role on Microsoft SQL Server. This is for the **User Name** field. See **Configuring the Configuration Database**.
3. When you create a new configuration database, specify the directory path to the MDF and LDF database files.

Creating a New Configuration Database



4. On the Neurons for ITSM **Application** page, specify a Neurons for ITSM application database user account that has a db_owner role on Microsoft SQL Server. This is for the **User Name** field. See **Configuring the Neurons for ITSM Application**.
5. When you create a new Neurons for ITSM application database, specify an additional path to the server.

Task 3: Running the File Stream Attachment Script

The FileStreamAttachment.sql script is included on the Software product CD. The script creates an attachment filestream database file group and a filestream.

Before you run the script, open it in Microsoft SQL Server Management Studio and read the script notes carefully, so that you understand what the script does.

1. On the Microsoft SQL Server hosting the configuration database, run the FileStreamAttachment.sql script.
2. On the Microsoft SQL Server hosting the Neurons for ITSM application database, run the FileStreamAttachment.sql script.

When you create your Neurons for ITSM application database, you can now specify the FILESTREAM attachment type.

3.2.6. SSL Configuration

This guide explains how to configure Secure Sockets Layer (SSL) on Internet Information Services (IIS) for first-time users.

The configuration of SSL for a site includes the following steps:

- Create an SSL binding on a site.
- Verify the SSL binding by making a request to the site.
- Configure SSL options in IIS by making SSL a requirement for the site.

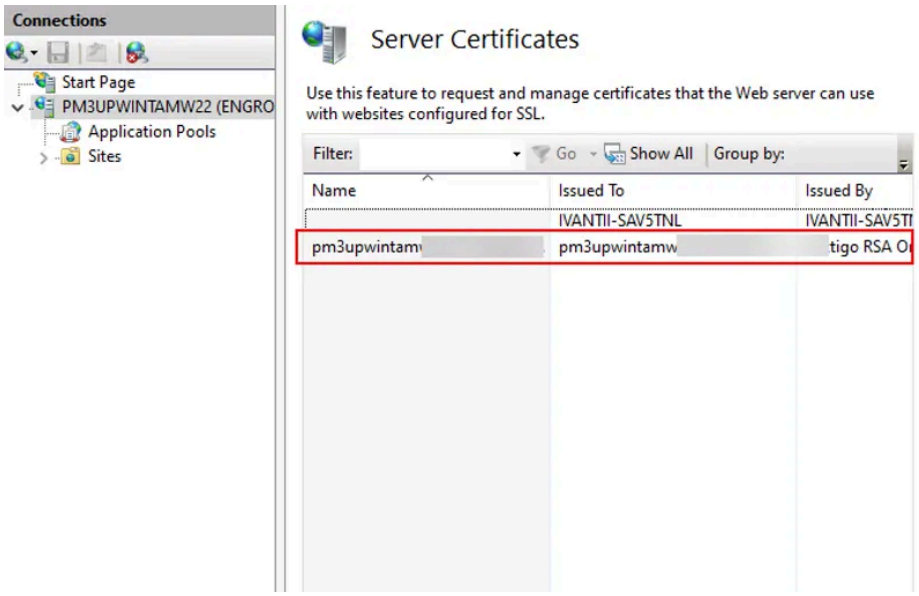
Prerequisites

- Install Microsoft IIS in your virtual machine or computer.
- Obtain appropriate certificate for SSL encryption and for authenticating the identity of the server.

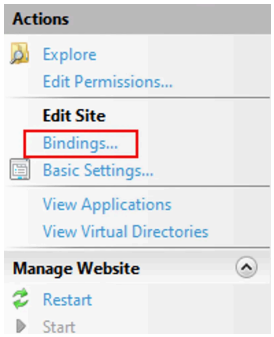
Create an SSL binding

1. Open **Internet Information Services (IIS) Manager**, and open **Server Certificates**.
2. Click **Import**, and upload the certificate.

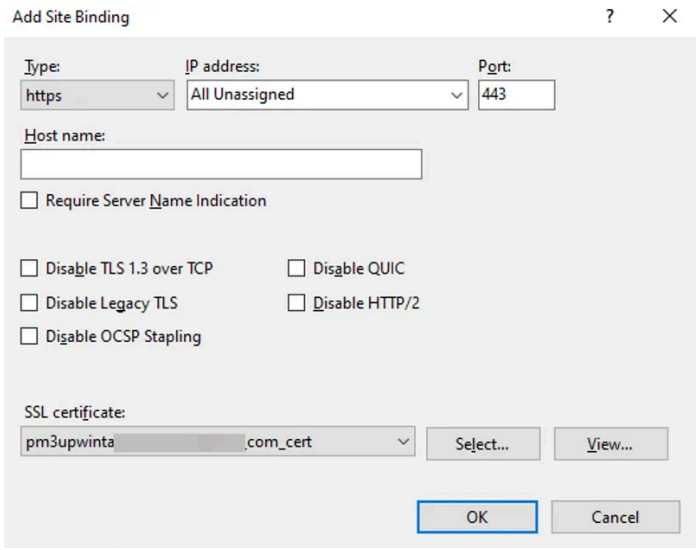
After the certificate is imported, it appears on the **Server Certificates** page.



3. In the **Connections** pane, go to **Sites** > **Default Web Site**.
4. In the **Actions** pane, click **Bindings** to create SSL binding. The Site Bindings window opens.



5. Click **Add**, and enter the required information:



Field	Description
Type	Select **https** from the dropdown menu.
IP address	Select **All Unassigned** from the dropdown menu.
Port	Enter *443*.
Host name	Enter the host name of your virtual machine or computer.
SSL certificate	From the dropdown menu, select the certificate that you uploaded in Server Certificates.

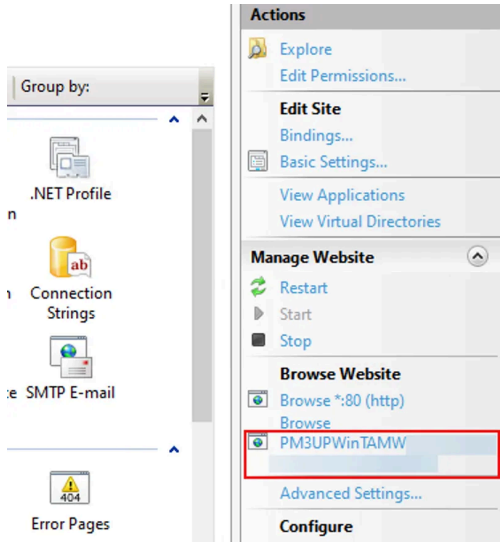
6. Click **OK**.

IIS creates a new SSL binding for your site.

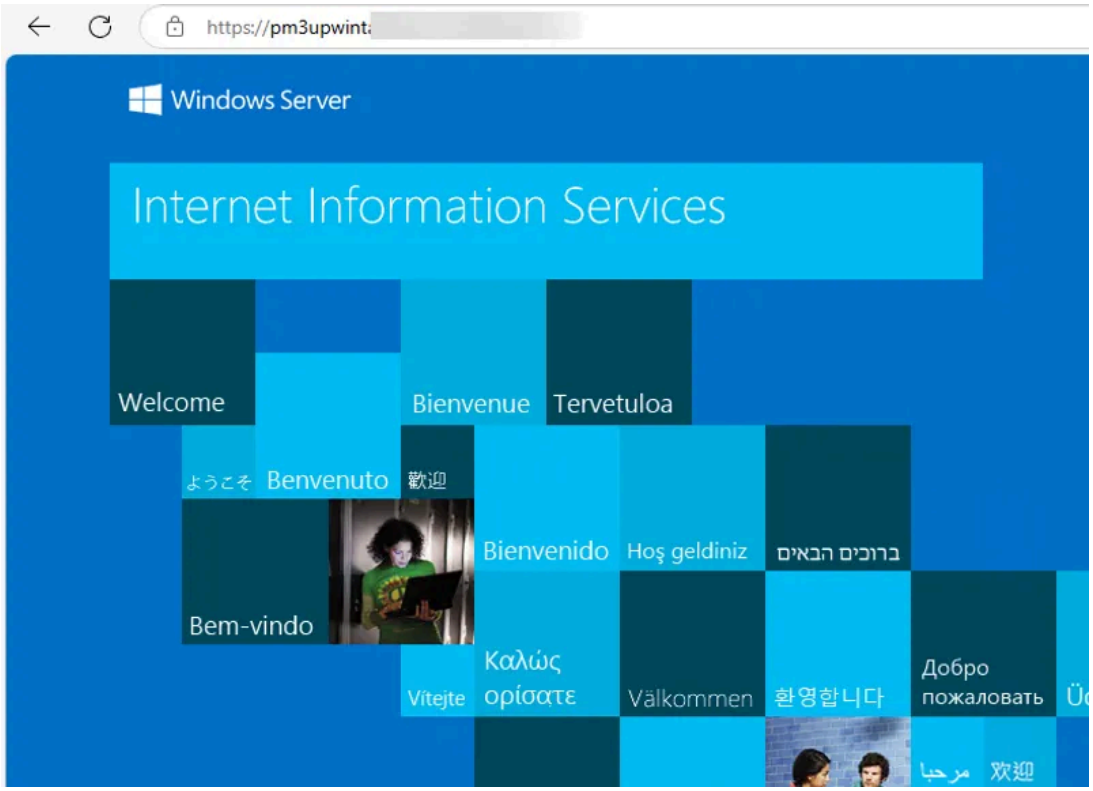
Next, you can verify whether that works.

Verify the SSL binding

1. In the **Connections** pane, go to> **Sites** > **Default Web Site**.
2. In the **Actions** pane, under **Browser Website**, click the site you configured.

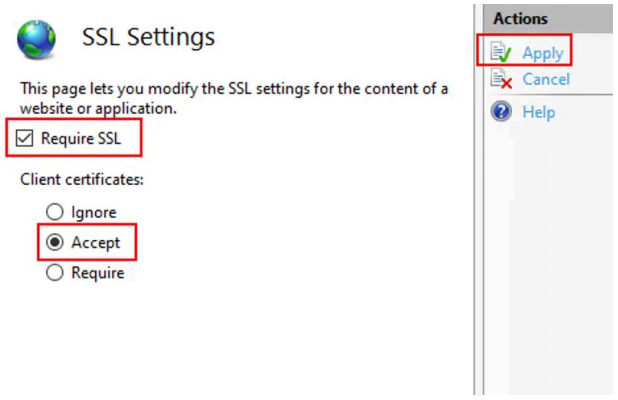


The site opens in your default browser. If SSL is configured correctly, the URL begins with *https*, indicating a secured connection.



Configure SSL options in IIS

1. Go to **Connections** pane > **Sites** > **Default Web Site**.
2. On the **Default Web Site Home** page, open **SSL Settings**.
3. Select the **Require SSL** checkbox.
4. Select the **Accept** button for Client certificates.



5. Click **Apply**.

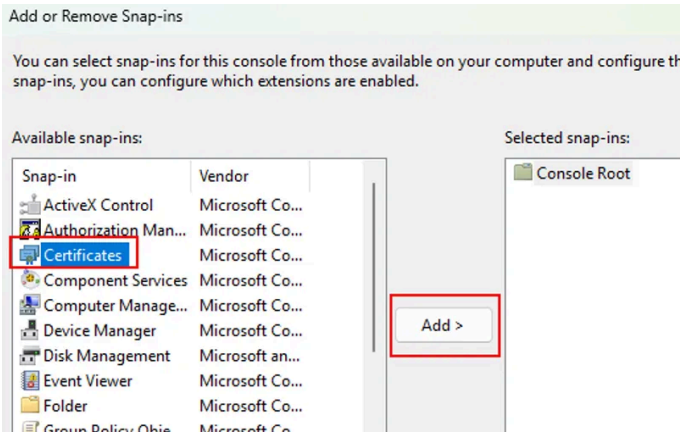
Once you enable this setting, your host device is secured and you can access the application securely with *https*.

Manage trusted root certificates for a local computer

To prevent security warnings in the browser, you need to add the certificate to the **Trusted Root Certification Authorities** store on your local computer so that the browser recognizes it as a trusted source.

To add the certificate to the **Trusted Root Certification Authorities**, follow these steps:

1. Click **Start** and search for **mmc**.
2. On the **File** menu, click **Add/Remove Snap-ins**.
3. Under **Available snap-ins**, select **Certificates** and click **Add**.



4. Select **Computer account**, and click **Next**.
5. Click **Finish**, and then click **OK**.
6. In the console tree, go to **Certificates (Local Computer)** > **Trusted Root Certification Authorities**.
7. Right-click **Certificates**, and go to **All Tasks** > **Import**.
8. Click **Next**, and upload the same certificate you used for SSL binding.

The local computer now trusts your certificate, and any connections or applications that rely on this certificate will recognize it as secure and valid.

If you want to configure both your Neurons for ITSM application database and configuration database to use SSL, refer to **Optional SSL Configuration**.

> SSL offloading is enabled in IIS Reverse Proxy, so we recommend deploying it only inside trusted network zones.

3.2.7. Installing Neurons for ITSM Reporting Feature

- About Microsoft SSRS
- Checking if Microsoft SSRS is Installed
- Installing Microsoft SSRS

About Microsoft SSRS

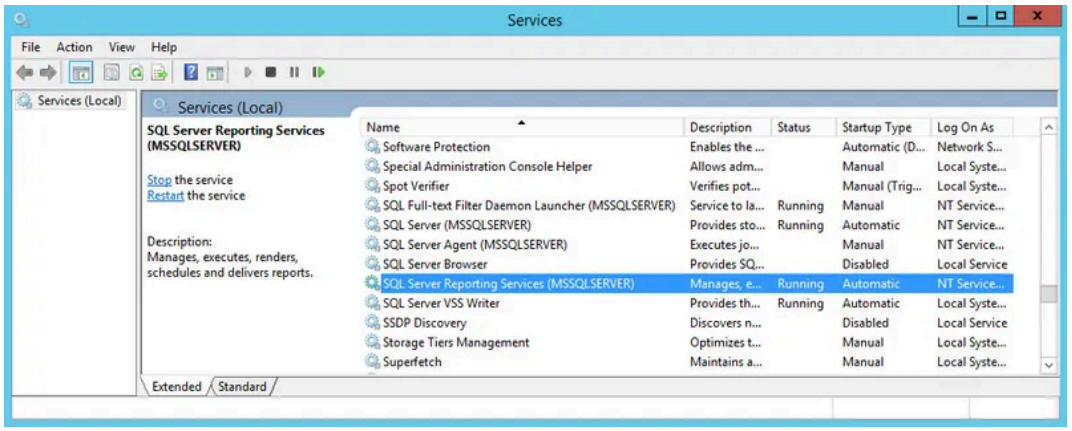
The Neurons for ITSM reporting feature requires that the 64-bit version of Microsoft SQL Server and Microsoft SQL Server Reporting Services (SSRS) are installed and running on the Neurons for ITSM database server. The reporting feature does not support the 32-bit version of Microsoft SQL Server and Microsoft SQL Server Reporting Services (SSRS).

Checking if Microsoft SSRS is Installed

To verify that Microsoft SSRS is installed on your system, do the following:

1. Open the Microsoft Windows **Services** dialog box and look for an entry called SQL Server Reporting Services.

   Windows Services Dialog Box

   The name in parentheses is the Microsoft SSRS instance name. See **Windows Services Dialog Box**. During the reporting feature configuration, you must enter this instance name.

   > The instance name cannot contain any special characters, such as \ , : ; ... and so on. The instance names can contain $ and _. See https://support.microsoft.com/en-us/help/2282743/fix-the-special-characters-are-displayed-incorrectly-in-a-textbox-cont.
   >
   > If the names of the current Microsoft SSRS instances have special characters, you must install an additional Microsoft SSRS instance with an instance name free of special characters.

2. Choose the appropriate action:
   - If Microsoft SSRS is already installed and the instance name (the name in parentheses) has no special characters (-, _, #, and so on), make sure that:
     - The value in the **Status** column is set to Running.
     - The value in the **Startup Type** column is set to either Automatic or Automatic (Delayed Start).

- If Microsoft SSRS is already installed but the instance name has special characters (-, _, #, and so on), use the Microsoft SQL Server Installation Center to add a new Microsoft SSRS instance with an instance name free of special characters.
- If Microsoft SSRS is not installed, use the Microsoft SQL Server Installation Center to add a Microsoft SSRS component to an existing Microsoft SQL installation.

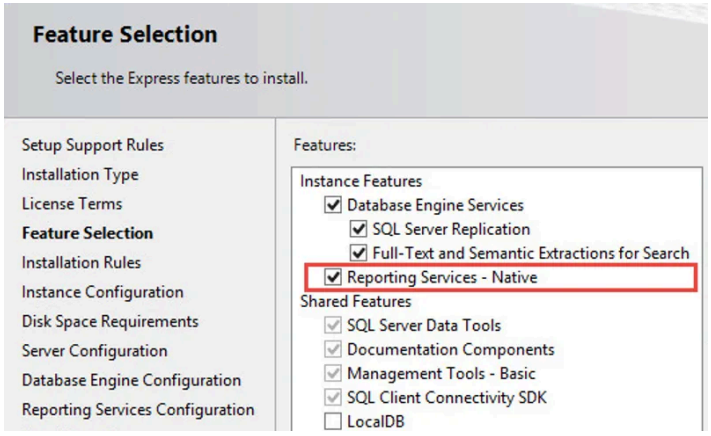
Installing Microsoft SSRS

Microsoft SQL Server Reporting Services (SSRS) is an optional installation feature of Microsoft SQL Server. It is a server-based, report-generating software system.

The Microsoft SSRS feature is disabled by default. This section describes how to enable and configure the Microsoft SSRS feature of Microsoft SQL Server.

1. During Microsoft SQL Server installation, in the **Feature Selection** page of the Microsoft SQL Server setup wizard, check **Reporting Services - Native**.

   Checking Reporting Services - Native

2. As you work your way through the Microsoft SQL Server setup wizard, verify that **Reporting Services - Native** is part of the server configuration.
3. When the installation is complete, go back to Windows Services and verify that Microsoft SQL Server Reporting Services is present. See **Checking Reporting Services - Native**.

With Microsoft SSRS present and running, the database server is ready for you to install and configure Neurons for ITSM.

3.2.8. Full Text Search

The full-text search feature of Microsoft SQL Server is a specialized indexing and querying service for character-based data in Microsoft SQL Server database tables.

By default, the application database is configured to index these incident fields:

- Owner
- ProfileFullName
- Resolution
- Subject
- Symptom

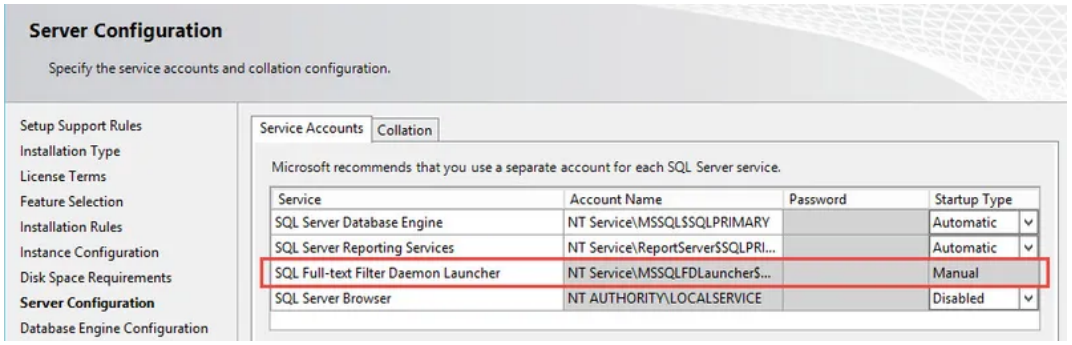
The full-text search feature is disabled by default.

Enabling the Full-Text Search Feature

This section describes how to enable and configure the full-text search feature of Microsoft SQL Server.

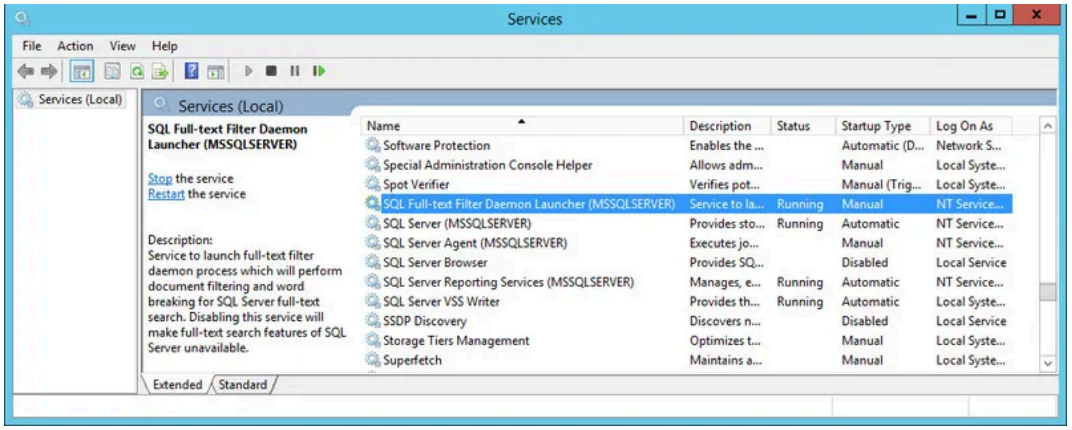
1. During Microsoft SQL Server installation, in the **Feature Selection** page of the Microsoft SQL Server setup wizard, check **Full-Text and Semantic Extractions for Search**.
2. In the **Server Configuration** page of the Microsoft SQL Server setup wizard, ensure that the Microsoft SQL Full-text Filter Daemon Launcher is configured with the local service account.

   Server Configuration



3. In the **Services** panel for the system, ensure that the status for **SQL Full-text Filter Daemon Launcher** says Running.

   Services Dialog Box



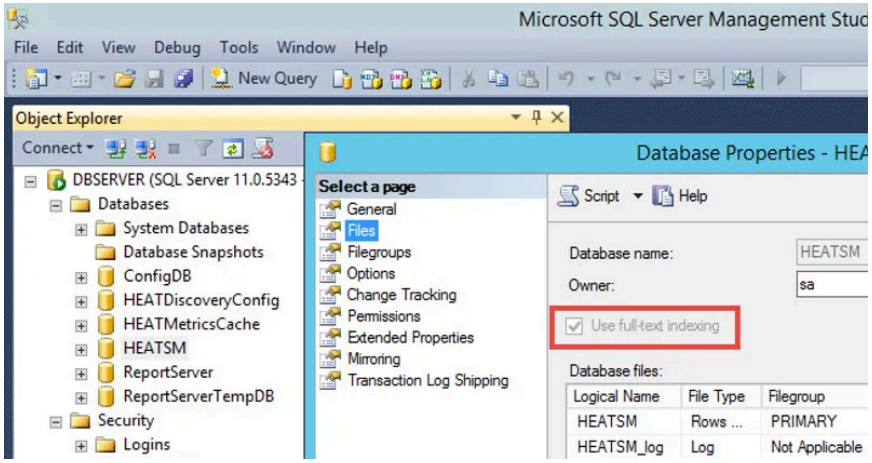
4. Verify that full-text search is configured in Microsoft SQL Server Management Studio by doing the following:

   a. Open the **Files** page from the **Database Properties** dialog box.

   b. Ensure that Use full-text indexing is checked.

   c. If it is not checked, verify that the full-text search services are running as described in **In the Services panel for the system, ensure that the status for SQL Full-text Filter Daemon Launcher says Running.**

   Checking the Use Full-Text Indexing Option



3.2.9. Verifying Server Roles and Features

You can optionally verify which server roles and features are installed by the Neurons for ITSM installer.

If you install Neurons for ITSM on Windows Server 2012 or Windows Server 2016, verify the Microsoft IIS Release 8.0 configuration. See **Verifying Roles and Features for Windows Server 2012 and 2016**.

Verifying Roles and Features for Windows Server 2012 and 2016

1. Go to the Windows apps menu and click Server Manager.
2. Under configure this local server, click Add roles and features.
3. On the **Roles** page, verify that these server roles are installed under Web Server (IIS) > Web Server:
    - Common HTTP features
        - Default Document
        - Directory Browsing
        - HTTP Errors
        - Static Content
    - Health and Diagnostics
        - HTTP Logging
    - Performance
        - Static Content Compression
        - Dynamic Content Compression
    - Security
        - Request Filtering
    - Application Development
        - .NET Extensibility
        - ASP.NET
        - ISAPI Extensions
        - ISAPI Filters
        - Under Web Server (IIS) > Management Tools:
        - IIS Management Console
        - Check the box of any listed server role that is not installed.
4. On the **Features** page, verify that these features are selected:
    - NET Framework 4.5
        - ASP.NET 4.5
        - WCF Services > HTTP Activation
    - Windows Process Activation Service
        - Process Model
        - Configuration APIs

- Check the box of any listed feature that is not installed.

5. Click Next and then click Install.

3.3. Installing the Neurons for ITSM System

This section describes how to install Neurons for ITSM for a new, complete system using the recommended deployment as described in **Neurons for ITSM Deployment Overview**.

- **Installing Neurons for ITSM in the Production Environment**
- **Installing Neurons for ITSM in the Staging and UAT Environments**
- **Installing the Reporting Feature**
- **Installing the Neurons for ITSM Operations Console**

Installing Neurons for ITSM in the Production Environment

To install Neurons for ITSM in the production environment, do the following:

- Install all Neurons for ITSM features except for the Operations Console. See **Installing Neurons for ITSM**.
- Use the System Configuration Wizard to configure your production environment. See **Configuring Neurons for ITSM** .

Installing Neurons for ITSM in the Staging and UAT Environments

- If you are hosting the staging and UAT environments on one server, follow the steps below.
- If you are hosting the staging and UAT environments on separate servers, follow the steps below once for the staging environment and once for the UAT environment.

To install Neurons for ITSM in the staging and UAT environments, do the following:

- Install all Neurons for ITSM features including the Operations Console.

> If you are hosting the staging and UAT environments on separate servers, we recommend only installing the Operations Console on the staging server and not on both.

- Use the System Configuration Wizard to configure your staging and UAT environments. See **Configuring Neurons for ITSM** .

Installing the Reporting Feature

To install the reporting feature, do the following:

- Install the reporting feature on the Neurons for ITSM database server. See **Installing the Reporting Feature**.
- Use the System Configuration Wizard to configure the reporting feature. See **Configuring the Reporting Feature**.

Installing the Neurons for ITSM Operations Console

You use the Neurons for ITSM Operations Console to create the staging and UAT instances of the tenant. (The system automatically created the production instance of the tenant.)

If you have any problems with the installation, you can review the installation log file that resides with the other system temporary files in the system temporary folder at %tmp%.

3.3.1. Installing Neurons for ITSM

This chapter provides an overview of product deployment and associated installation steps.

Where to Install Neurons for ITSM

Before you begin installation, be clear on your deployment plan for Neurons for ITSM. See Neurons for ITSM**Neurons for ITSM Deployment Overview**.

- For the **Demonstration or Proof-of-Concept Deployment**, you install Neurons for ITSM onto the Neurons for ITSM server. With this deployment, you must install Microsoft SQL Server and Microsoft SQL Server Reporting Services (SSRS) on your server before you install Neurons for ITSM.
- For the **Minimum Production Deployment** , you install Neurons for ITSM onto the Neurons for ITSM server.
- For the **Enterprise Production Deployment**, you install Neurons for ITSM onto each of your Neurons for ITSM processing servers and web servers, as described below.

Installing Neurons for ITSM

Prerequisite:

- Without fail take a backup of the entire folder in all the machines where Neurons for ITSM is installed. This step is a mandatory preventive measure, do not miss it.
- Install the prerequisite installer using **Ivanti Service & Asset Manager Prerequisite.exe**.

  The **Ivanti Service & Asset Manager.exe** installs the essential software that is required for running the System Configuration Wizard (SCW) tool.
- Install the **Additional App Domain** provided with the package. Follow instructions given in Additional App Domain Deployment.

> Installing the Additional App Domain is mandatory.

Installation is basically the same for all hosts in your deployment, except for the features to be installed, which happens in **Your selection of features from the Setup Type dialog box depends on the role of the individual host in your deployment plan.**

> After the Additional AppDomain powershell script is successfully run, the cache re-build is automatically executed. If the Additional AppDomains powershell script is not run in same machine, then the Cache Rebuild should be executed manually. For instructions on how to executed Cache Rebuild manually, refer to **Neurons for ITSM Cache Rebuild**.

Do the following on each production server in your deployment:

1. Access the installation folder on the Software product CD or zip file and run **IvantiServiceManager.exe**. Right-click and select Run as Administrator to ensure proper installation.

   The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
2. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.

3. Click **Next**. The system displays the **License Agreement** dialog box.
4. Choose **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
5. Click **Next** to accept the default installation folder, or click **Change** and select a different folder. The system displays the **Setup Type** dialog box.
6. Your selection of features from the **Setup Type** dialog box depends on the role of the individual host in your deployment plan.
    - For the **Demonstration or Proof-of-Concept Deployment**, choose Complete, click Next, and install all components.
    - For the **Minimum Production Deployment** , choose Complete, click Next, and install all components.
    - For the **Enterprise Production Deployment**, your choice depends on the role of the host:
        - Production processing server: Choose Custom, click Next, and install all components except for the Neurons for ITSM Operations Console. You must install this server first before you install the staging, UAT, or web servers.
        - Staging or UAT processing servers: Choose Complete, click Next, and install all components.
        - Web servers: Choose Custom, click Next, and only install the Neurons for ITSM application server.

    For the **Enterprise Production Deployment**, note the following:

        - If your deployment includes different processing servers for production, staging, and UAT, you must install the License Manager in every one of those landscapes.
        - You can choose Complete and install all Neurons for ITSM features on all of your servers, but doing that takes up more disk space than necessary.

    When installing components, note the following:

        - To not install a component, click the down arrow next to the server icon next to the category name, highlight the component, right click, and select This feature will not be available.
        - If your deployment includes DSM, you do not need to install the DSM Integration service because that component has been incorporated into Neurons for ITSM since Release 2015.2.
7. Click Next. The system displays the **Ready to Install the Program** dialog box.
8. Click **Install**. The system begins installing Neurons for ITSM and displays a status dialog box, showing the installation progress of each module over the next few minutes.
9. Click OK if the system displays a dialog box saying that reboot is required after installation.
10. If the system displays a dialog box saying that some of the files that need to be updated are currently in use, choose Automatically close and attempt to restart applications and click OK.

    When the installation is completed, the system displays the System Configuration Wizard.
11. Go to **Configuring Neurons for ITSM** for instructions about using the System Configuration Wizard.

Installing Additional App Domain

You will be prompted to install the App Domain after the SCW installation is complete. Proceed with the installation without skipping.

- Additional components zip file is provided along with the installer.
- All the components in the zip files needs a working setup of Ivanti Service & Asset Manager.
- Powershell script should be run with Administrator privilege.
- Ensure you have atleast 500 MB of free space before running the script.

List of App Domains:

1. Survey
    - SurveyUI
    - SurveyProxy
2. ActionService
3. TeamsBot

Steps to run the script:

1. Extract the zip file provided along with the Installer.

   The setup will have one powershell script named **install.ps1**.

2. Open a powershell window with Administrator privilege.
3. Run the following command from the extracted location:

```Bash
Set-ExecutionPolicy Bypass -Scope Process -Force; .\install.ps1
```

4. Teamsbot is optional component, please type yes to install. If Installing Teamsbot there are two URLs you need to pass where components are installed:
    - AppServer URL
    - CentralConfig URL

   The value can be machine name (if above components are installed on a different server) or localhost (if the components are installed on same server).

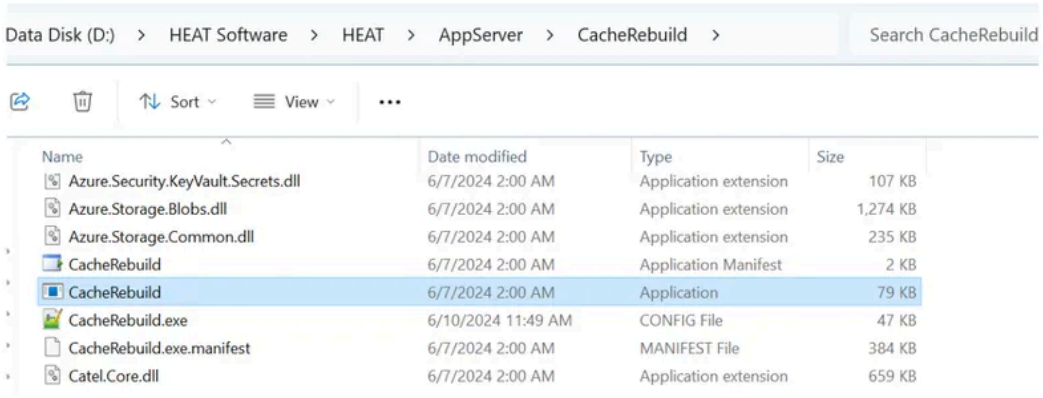
ActionService and Survey will be installed by default with the script as they are necessary components for the application to function properly.

Neurons for ITSM Cache Rebuild

Follow these steps to run the cache rebuild manually:

1. Open the command prompt as an Administrator.
2. Go to "HEAT Software\HEAT" folder on the machine where you have run the installer.

   For example, D:\HEAT Software\HEAT\AppServer\CacheRebuild.

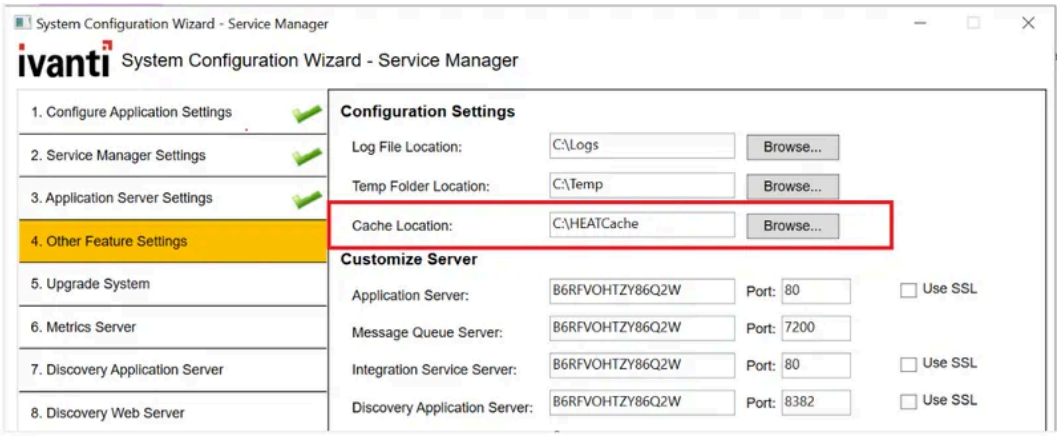


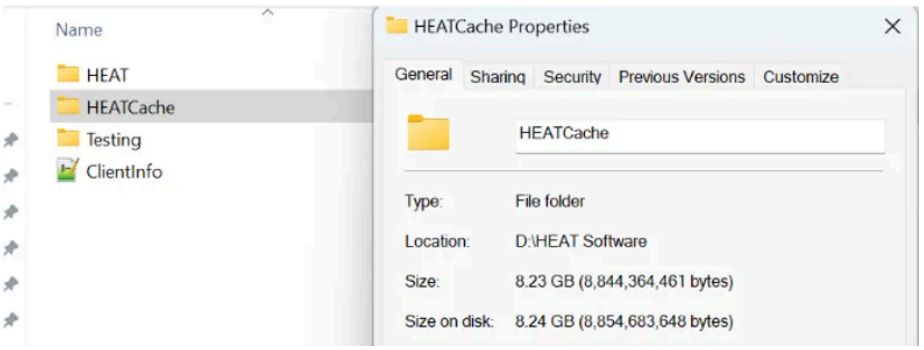
3. In the command prompt once the path is correct, run the **CacheRebuild.exe**.

   For example, D:\HEAT Software\HEAT\AppServer\CacheRebuild>CacheRebuild.exe.

> Do not close the command prompt window while the cache rebuild is running, it will close automatically after it's done.

The CacheRebuild folder will be saved in the path provided in the SCW.





3.3.2. Installing the Reporting Feature

- About Installing the Reporting Feature
- Where to Install the Reporting Feature
- Installing the Reporting Feature

About Installing the Reporting Feature

Neurons for ITSM deployments can have multiple reporting tenant instances. To use the reporting feature in a multi-tenant environment, we highly recommend that you install a separate Microsoft SSRS instance for the reporting feature only. For example, a deployment may have one reporting server for the production instance of the tenant and another reporting server for the staging and UAT instances of the tenant. See Enterprise Production Deployment.

Where to Install the Reporting Feature

Where you install the reporting feature depends on which deployment you have chosen. See Neurons for ITSMNeurons for ITSM Deployment Overview.

- For the Demonstration or Proof-of-Concept Deployment, you install the reporting feature onto the Neurons for ITSM database server, after you have installed Neurons for ITSM.
- For the Minimum Production Deployment , you install the reporting feature on the Neurons for ITSM database server.
- For the Enterprise Production Deployment, you can install the reporting feature on the Neurons for ITSM database servers or on a dedicated reporting server. See Reporting Services Deployment Options.

Installing the Reporting Feature

Before you begin, ensure that you have met all of the prerequisites for installing the Neurons for ITSM reporting feature. See Installing Neurons for ITSM Reporting Feature. In particular, be sure that Microsoft SSRS is installed and running. See Checking if Microsoft SSRS is Installed.

> If you are using SQL 2016 or higher, ensure that you install Microsoft Report Builder manually.

Prerequisite:

- Install the prerequisite installer using **Ivanti Service & Asset Manager Prerequisite.exe**.

  The **Ivanti Service & Asset Manager Prerequisite.exe** installs the essential software that is required for running the system Configuration Wizard tool.

To install the reporting feature, do the following:

1. Access the installation folder on the Software product CD or zip file and run **ReportingServices.exe**. Right-click and select Run as Administrator to ensure proper installation.

   The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.

2. Select **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.

3. Click **Next**. The system displays the **License Agreement** dialog box.
4. Select **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
5. Click **Next** to accept the default installation folder, or click **Change...** and select a different folder.
6. Click Next. The system displays the **Ready to Install the Program** dialog box.
7. Click **Install**. The system begins installing the Neurons for ITSM reporting feature and displays a status dialog box showing the installation progress over the next few minutes.

   When the components are installed, the system automatically launches the System Configuration Wizard.
8. Go to **Configuring the Reporting Feature** for instructions about using the System Configuration Wizard.

3.3.3. Installing Discovery on a Dedicated Server

In small deployments, you install Discovery with the other Neurons for ITSM components on the Neurons for ITSM production servers. For an **Enterprise Production Deployment**, you can either install Discovery on the production servers or, to reduce the load on the production servers, you can configure a dedicated Discovery server. If you install Discovery on your production servers and then experience a significant load increase, we recommend configuring a dedicated Discovery server.

This topic describes how to install Discovery on a dedicated server.

1. Install Neurons for ITSM on your production servers. See **Installing Neurons for ITSM**.
2. On the server dedicated to Discovery, access the installation folder on the Software product CD or zip file and run IvantiServiceManager.exe. Right-click and select Run as Administrator to ensure proper installation.

   The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
3. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
4. Click **Next**. The system displays the **License Agreement** dialog box.
5. Select **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
6. Click **Next** to accept the default installation folder or click **Change...** and select a different folder. The system displays the **Setup Type** dialog box.
7. Select the following components for the **Custom Setup** dialog box. Under Discovery, choose:
   - Web Application Components
   - Discovery Web Server
8. Click Next. The system displays the **Ready to Install the Program** dialog box.
9. Click **Install**. The system begins installing Discovery and displays a status dialog box showing the installation progress of each component over the next few minutes.

   When the components are installed, the system automatically displays the System Configuration Wizard.
10. Go to **Configuring the Discovery Application Server** for instructions about using the System Configuration Wizard.

3.3.4. Installing the Knowledge Uploader (Knowledge Import Tool)

- About the Knowledge Uploader (Knowledge Import Tool)
- Installing the Knowledge Uploader (Knowledge Import Tool)
- Initially Configuring and Logging Into the NXT Knowledge Import Tool
- Using the NXT Knowledge Import Tool
- Initially Configuring and Logging Into the Knowledge Import Tool
- Using the Knowledge Import Tool

About the Knowledge Uploader (Knowledge Import Tool)

You can import knowledge articles from HEAT Classic, ITSM, or a local or networked file system into Neurons for ITSM. Neurons for ITSM currently has two knowledge import tools: the NXT Knowledge Server Tool (for NXT formats such as ITSM or HEAT Classic) and the Knowledge Server Tool (to use with file systems). These tools are collectively called the Knowledge Uploader and are also called the Knowledge Import Tool.

For information about using these tools after you have installed and configured them, see **Using the Knowledge Uploader** in the Neurons for ITSM online help.

Installing the Knowledge Uploader (Knowledge Import Tool)

Most installations of Neurons for ITSM automatically include the Knowledge Uploader (also called the Knowledge Import Tool).

The following procedure is necessary only if you did not install the Knowledge Uploader when you installed Neurons for ITSM.

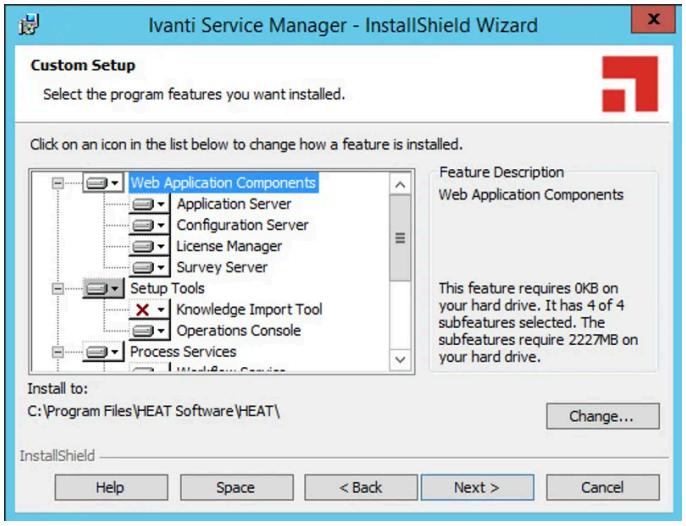
On the server or servers that you are going to use as the production environment, do the following:

1. Access the installation folder on the Software product CD or zip file and run IvantiServiceManager.exe. Right-click and select Run as Administrator to ensure proper installation.

   The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.

2. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
3. Click **Next**. The system displays the **License Agreement** dialog box.
4. Choose **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
5. Click **Next** to accept the default installation folder or click **Change...** and select a different folder. The system displays the **Setup Type** dialog box.
6. Select Custom in the **Setup Type** dialog box and click the Knowledge Import Tool under Setup Tools. See Custom Setup and the Knowledge Import Tool.

   Custom Setup and the Knowledge Import Tool



7. Click Next. The system displays the **Ready to Install the Program** dialog box.
8. Click **Install**. The system begins installing Neurons for ITSM and displays a status dialog box showing the installation progress of each component over the next few minutes.

   When the installation is finished, the system displays the **InstallShield Wizard Completed** dialog box.
9. Click Finish. When the file installation is finished, the system displays the System Configuration Wizard.
10. Close the System Configuration Wizard, as there is no specific configuration for the Knowledge Uploader in the System Configuration Wizard.

The system now has two new applications on it. They are called Knowledge Import Tool and Knowledge Import Tool (NXT).

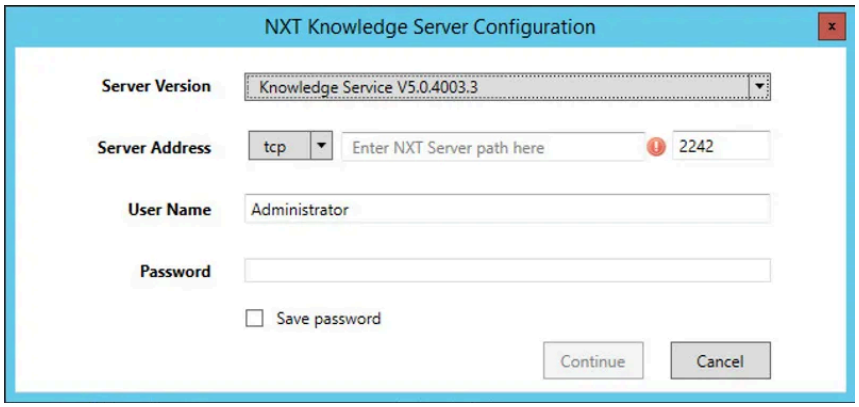
Initially Configuring and Logging Into the NXT Knowledge Import Tool

> There are two knowledge tools. This topic is about the NXT Knowledge Import Tool and NOT the Knowledge Import Tool.

After you have installed Neurons for ITSM, including the Knowledge Uploader (also called the Knowledge Import Tool), do the following to initially configure and log into the NXT Knowledge Import Tool:

1. On the system where you installed Neurons for ITSM, open the application called **Knowledge Import Tool NXT**. The system displays the **NXT Knowledge Server Configuration** dialog box. See NXT Knowledge Server Configuration Dialog Box.

   NXT Knowledge Server Configuration Dialog Box



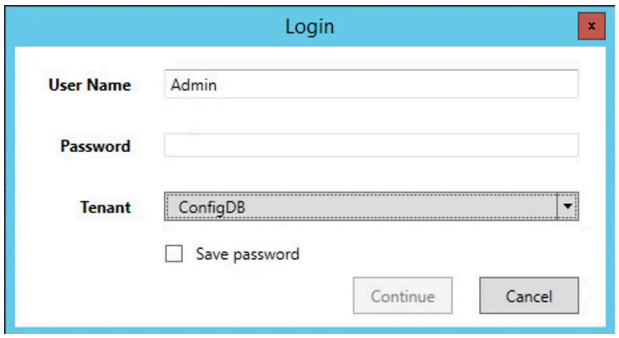
2. Enter information into the fields.

Parameter	Description
Server Version	The version of the NXT server that you are taking the knowledge articles from. To determine the server version, open the program and find the server information. You can choose from any of the following: • Knowledge Service V5.0.4003.3 • Knowledge Service Plus V9.6.1.13 • Knowledge Service Plus V9.6.1.14
Server Address	Enter the following: • The protocol type (uses TCP by default) • The server path of the NXT server that you are taking the knowledge articles from • The port (uses 2242 by default)
User Name	The user name of a person who can access the NXT server that you are taking the knowledge articles from.
Password	The password associated with the user name.
Save password	Saves the password.

> To change these settings after the initial configuration, from the menu bar select Configuration > Configure NXT server.

3. Click Continue.
4. The system displays the **Login** dialog box. See **Knowledge Server Tool Login**.

Knowledge Server Tool Login



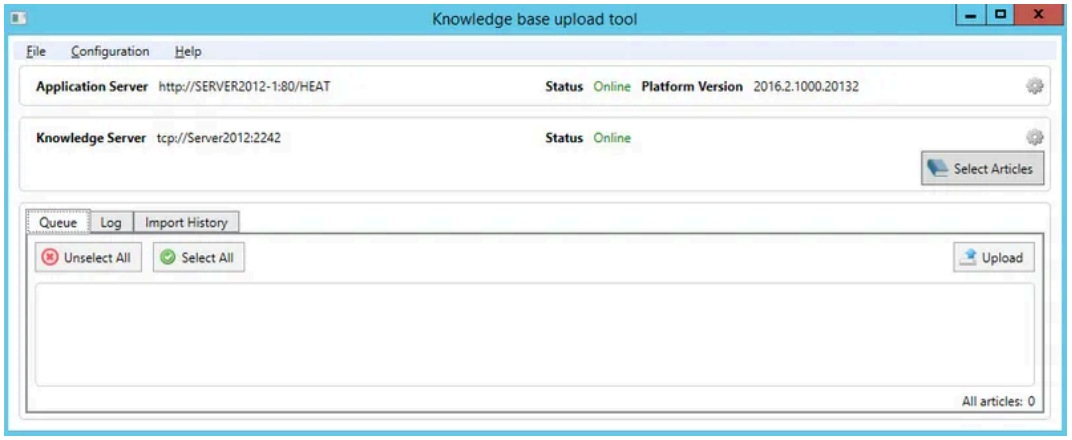
5. Enter information into the fields.

Parameter	Description
User Name	The user name of a person who can access Neurons for ITSM.
Password	The password associated with the user.
Tenant	The tenant to log into. You can select either ConfigDB to log into the configuration database or IvantiSM to log into Neurons for ITSM.
Save password	Saves the password.

> To change these settings after the initial configuration, from the menu bar select Configuration > Configure application server.

6. Click Continue. The system displays the **Select role** dialog box.
7. Select the role to log in as and click Continue. The system displays the **Knowledge base upload tool** page.

Knowledge Base Upload Tool



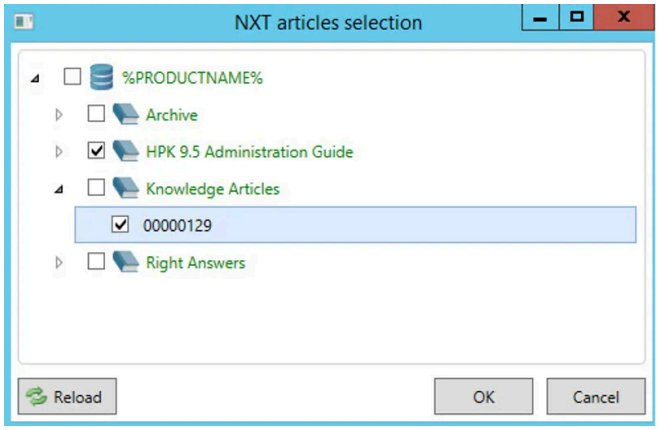
Using the NXT Knowledge Import Tool

> There are two knowledge tools. This topic is about the NXT Knowledge Import Tool and NOT the Knowledge Import Tool.

Follow these steps to import knowledge into Neurons for ITSM.

1. Click Select Articles to select the knowledge articles to import. The system displays the **NXT articles selection** dialog box.
2. Expand the list to see where knowledge articles are located, and then highlight one or more articles.

Select the Knowledge Articles to Import



3. Click OK. The system lists the selected articles on the bottom part of the page.
4. Select the articles to upload and click Upload to launch the **Article Creation** wizard and start the upload process.

   The **Article Creation wizard** page contains two main areas: a **Selected Documents** area on the left containing the list of files to import, and a **Document Properties** area on the right that contains two tabs. One tab is called **Default Values** and the other is called **Selected Documents**.

5. To remove a document from the **Selected Documents** section, check it and click **Remove selected**. By default, the knowledge uploader imports all of the documents in the **Selected Documents**, even if you do not select them.
6. Optionally, use the **Document Properties** section to specify the properties that the knowledge uploader displays together with the files in Neurons for ITSM. You can specify properties for all files (using the **Default values** tab) or for individual files (using the **Selected Document** tab after highlighting the file in the **Selected Documents** section).

   You can specify these properties:

   - **Article Type**: The article type. Select from Document, Error Message, Issue Resolution, Patch, Q&A, or Reference.
   - **Article Status**: The status of the article. Select from Approved, Draft, Expired, Failed Review, Pending Review, Published, or Submitted.
   - **Target collection**: The target. Select from Company Policy & Procedure, Customer Knowledge, Internal Knowledge, IT Knowledge, or Service Desk.
   - **Category**: The category for this knowledge article.
   - **Subject**: The subject of the article.
   - **Resolution**: The resolution details if the knowledge article contains this information.
   - **Description**: A description for the knowledge article.
7. Click **Import**. The system starts importing the selected knowledge articles.

   If you select a file that has already been imported into the knowledge base, the system displays the **Collision warning** dialog box.

8. Depending on what you want to do with the file that has already been imported, click one of the following:
   - **Apply for all**: Applies your choice to all previously imported files that are found during the import process.
   - **Update**: Overwrites the file that already exists in the Knowledge Base with the file that is being imported.
   - **Create New**: Does not overwrite the file being imported with the file that already exists in the Knowledge Base. After importing, there are two knowledge articles with the same name in the Knowledge Base.

- **Cancel**: Cancels the import process.

The system displays a dialog box with the status of the import.

9. Click **OK**.
10. Optionally, do the following:
    - Review the import logs by clicking the **Log** tab. You can clear or save the log.
    - Review the import history by clicking the **Import History** tab. Click a number in the **Imported** column to display more information about an import session.

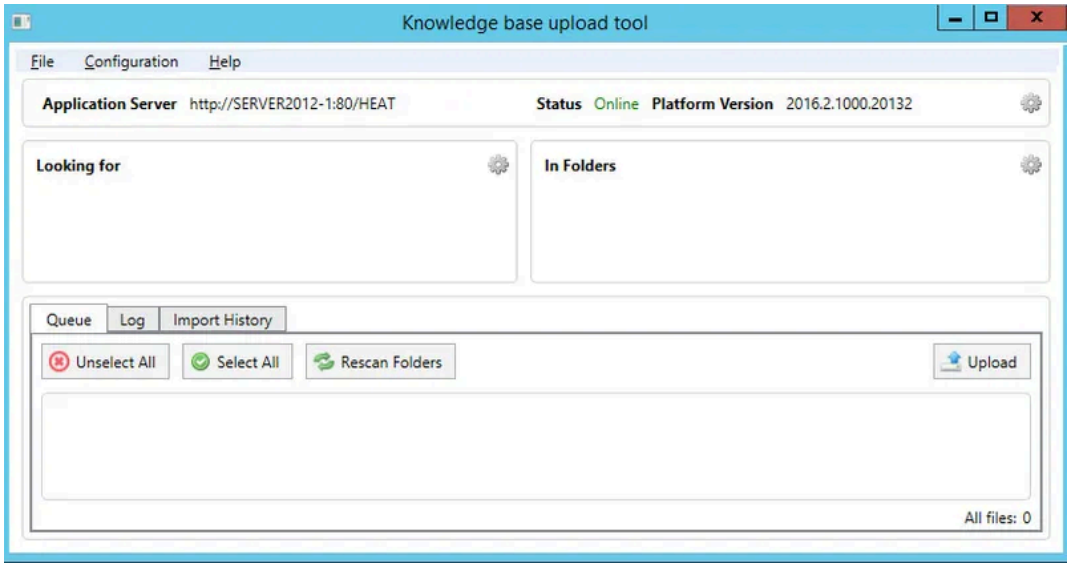
Initially Configuring and Logging Into the Knowledge Import Tool

> There are two knowledge tools. This topic is about the Knowledge Import Tool and NOT the NXT Knowledge Import Tool.

After you have installed Neurons for ITSM, including the Knowledge Uploader, do the following to initially configure and log into the Knowledge Import Tool:

1. On the system where you installed Neurons for ITSM, open the application called **Knowledge Import Tool**. The system displays the **Select role** dialog box.
2. Select the role to log in as and click Continue. The system displays the **Knowledge base upload tool** page.

Knowledge Base Upload Tool



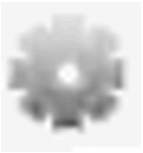
Using the Knowledge Import Tool

> There are two knowledge tools. This topic is about the Knowledge Import Tool and NOT the NXT Knowledge Import Tool.

Follow these steps to import knowledge into Neurons for ITSM.

1. Specify the article file type to search for, by doing the following:

a. Click the **Settings** icon in the **Looking for** section. The system displays the **File search filters** dialog box.



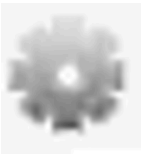
b. In the **Add New** drop-down list, select one or more file types:

- **Microsoft office documents**: Files that have .doc, .docx, .xls, and .xlsx extensions.
- **PDF files**: Files that have a .pdf extension.
- **Images**: Files that have .bmp, .jpg, and .gif extensions.

c. Optionally, you can add more file types by clicking **Custom**. The system adds a line item to the filter list called Custom. Click the line item to open it for editing. You can change the filter name and specify one or more extensions. Click **OK**. The system adds the file types that you specified to the **Looking for** section.

2. Specify which local or network folders to search for knowledge articles and then perform the search:

a. Click the **Settings** icon in the **In Folders** section. The system displays the **Import folders** dialog box.



b. Click **Add New**. The system displays the **Browse For Folder navigation** dialog box.

c. Navigate to a folder and highlight it. (To optionally add a new subfolder to the folder, click **Make New Folder**.)

d. Click **OK**. The system adds the folder to the list of folders to search. If you created a new folder, the system adds it to the file system as an empty folder.

e. Optionally, check **Recursive** for a folder to specify that the system should search the subfolders within the folder.

f. Optionally, check **Monitor for changes** to configure the knowledge uploader to monitor all of the folders on the list for changes to the file types that you specified in step 1b.

g. Repeat steps b-f to continue to add folders to the list as necessary.

h. Click **OK**.

The knowledge uploader performs the search and displays all of the files that meet the search criteria.

3. Select the files to upload:

a. If you think the contents of the scanned folders might have changed, click **Rescan Folders** to regenerate the file list.

b. In the file list, check the files to upload, or click **Select All** to upload all of the files.

c. Click **Upload** to launch the **Article Creation** wizard and start the upload process.

The **Article Creation wizard** page contains two main areas: a **Selected Documents** area on the left containing the list of files to import, and a **Document Properties** area on the right that contains two tabs. One tab is called **Default Values** and the other is called **Selected Documents**.

4. To remove a document from the **Selected Documents** section, check it and click **Remove selected**. By default, the knowledge uploader imports all of the documents in the **Selected Documents**, even if you do not select them.
5. Optionally, use the **Document Properties** section to specify the properties that the knowledge uploader displays together with the files in Neurons for ITSM. You can specify properties for all files (using the **Default values** tab) or for individual files (using the **Selected Document** tab after highlighting the file in the **Selected Documents** section).

   You can specify these properties:

   - **Article Type**: The article type. Select from Document, Error Message, Issue Resolution, Patch, Q&A, or Reference.
   - **Article Status**: The status of the article. Select from Approved, Draft, Expired, Failed Review, Pending Review, Published, or Submitted.
   - **Target collection**: The target. Select from Company Policy & Procedure, Customer Knowledge, Internal Knowledge, IT Knowledge, or Service Desk.
   - **Category**: The category for this knowledge article.
   - **Use file name as Subject**: Check to use the article file name to fill in the **Subject** field.
   - **Subject**: Only use this field if you did not check **Use file name as Subject**. Enter a subject for the article.
   - **Resolution**: Enter the resolution if the knowledge article contains one.
   - **Description**: Enter a description for the knowledge article.
6. Click **Import**. The import process begins.

   If you select a file that has already been imported into the knowledge base, the system displays the **Collision warning** dialog box.
7. Depending on what you want to do with the file that has already been imported, click one of the following:
   - **Apply for all**: Applies your choice to all previously imported files that are found during the import process.
   - **Update**: Overwrites the file that already exists in the knowledge base with the file that is being imported.
   - **Create New**: Does not overwrite the file being imported with the file that already exists in the knowledge base. After importing, there are two knowledge articles with the same name in the knowledge base.
   - **Cancel**: Cancels the import process.

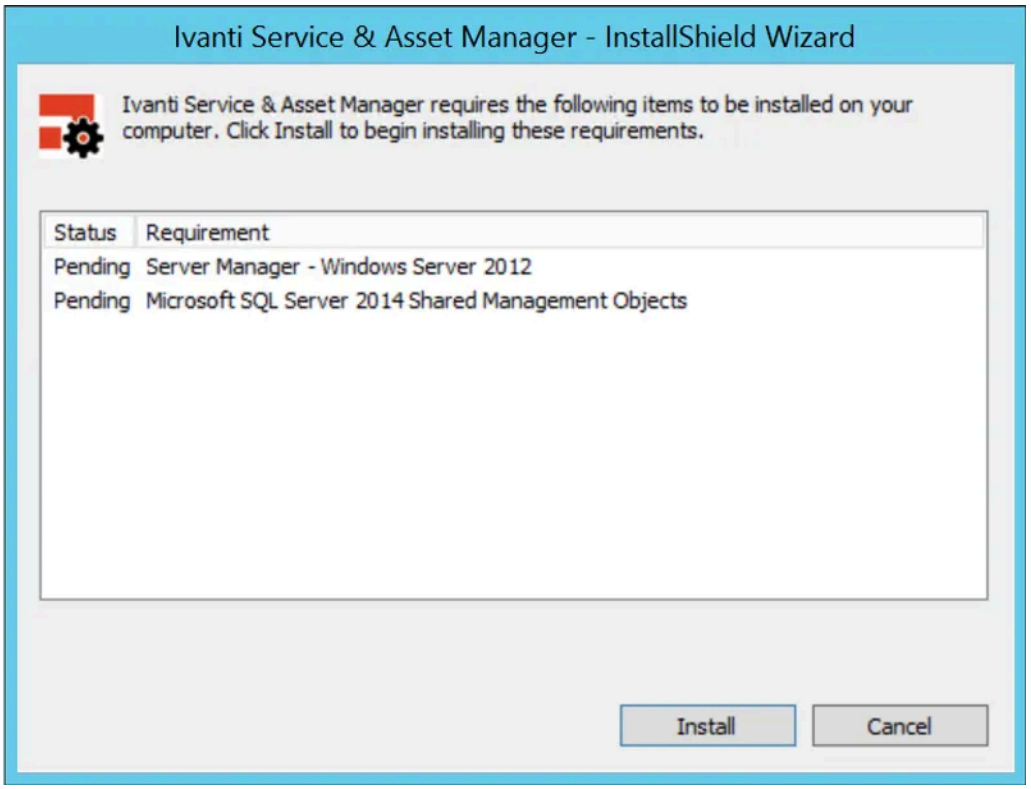
   The system displays an Import dialog box with the status of the import.
8. Click **OK**.
9. Optionally, do the following:
   - Review the import logs by clicking the **Log** tab. You can clear or save the log.
   - Review the import history by clicking the **Import History** tab. Click a number in the **Imported** column to display more information about an import session.

3.4. Initially Configuring the System

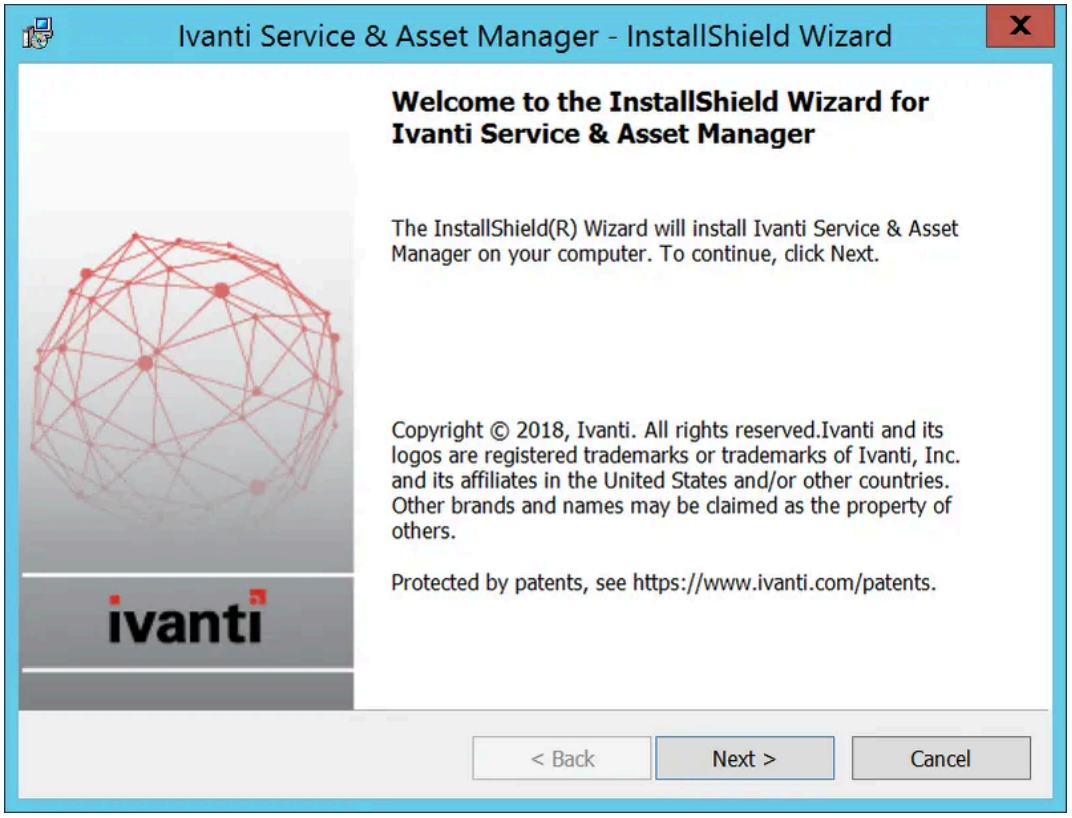
As part of the Neurons for ITSM installation, you must configure the system using the System Configuration Wizard.

The wizard walks you through the first-time set up and configuration as shown in the screen shots below.

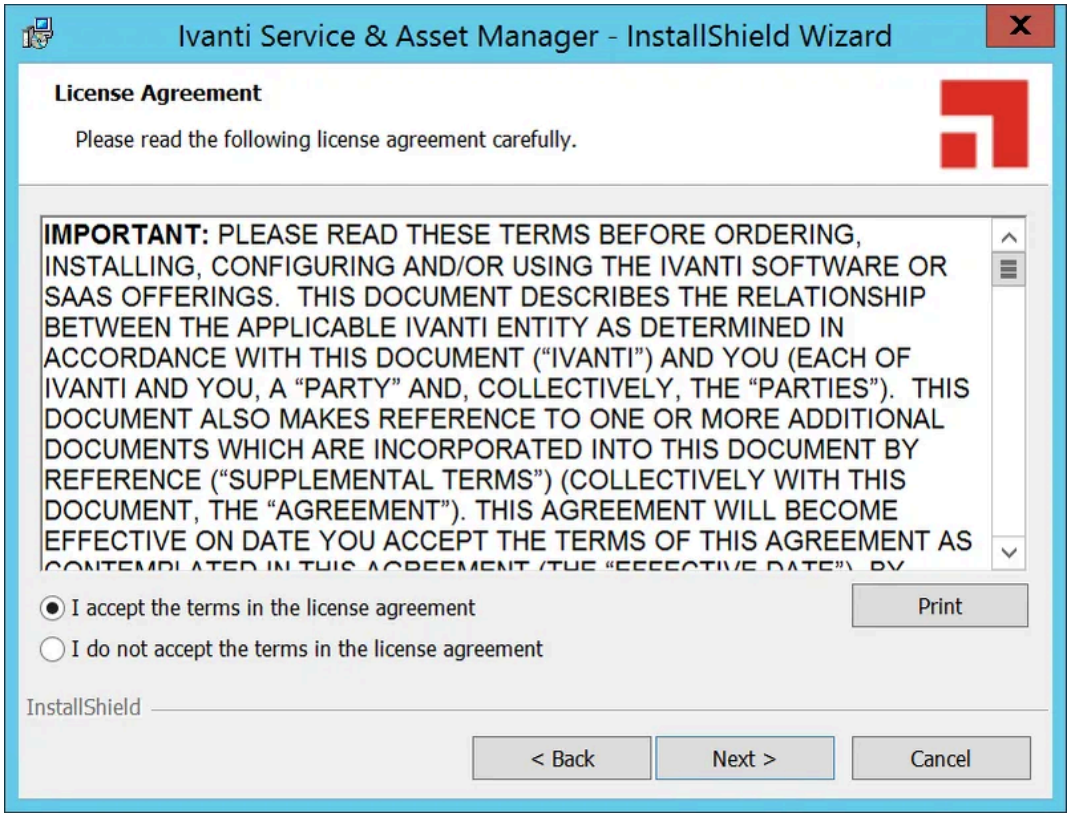
1. Click **Install** to begin the installation.



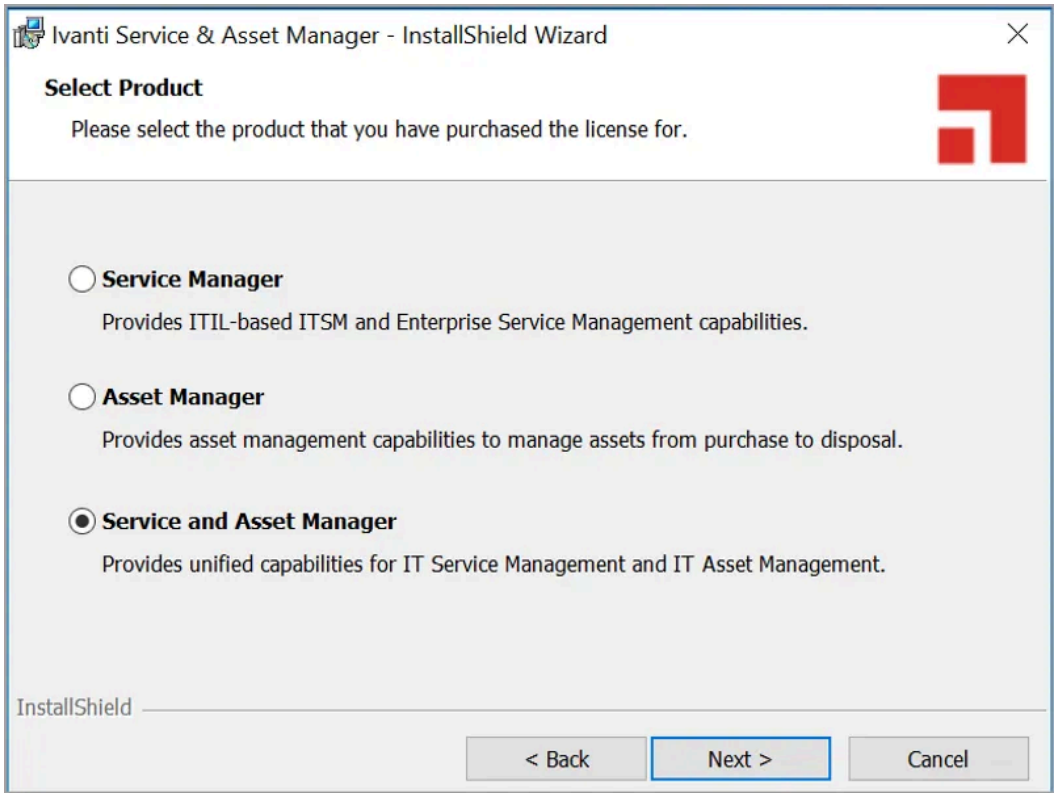
2. Click **Next**.



2. Click **Next** to continue the installation process.

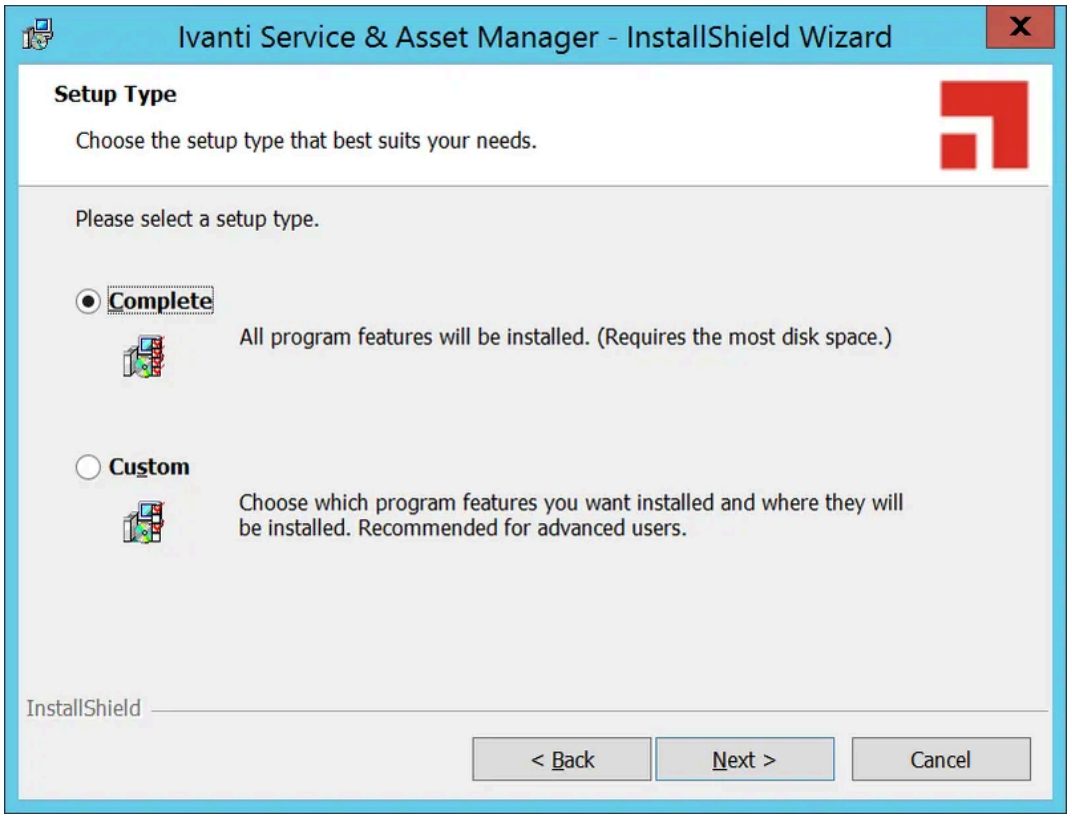


2. Select one of the options, **Service Manager**, **Asset Manager**, or **Service and Asset Manager**.

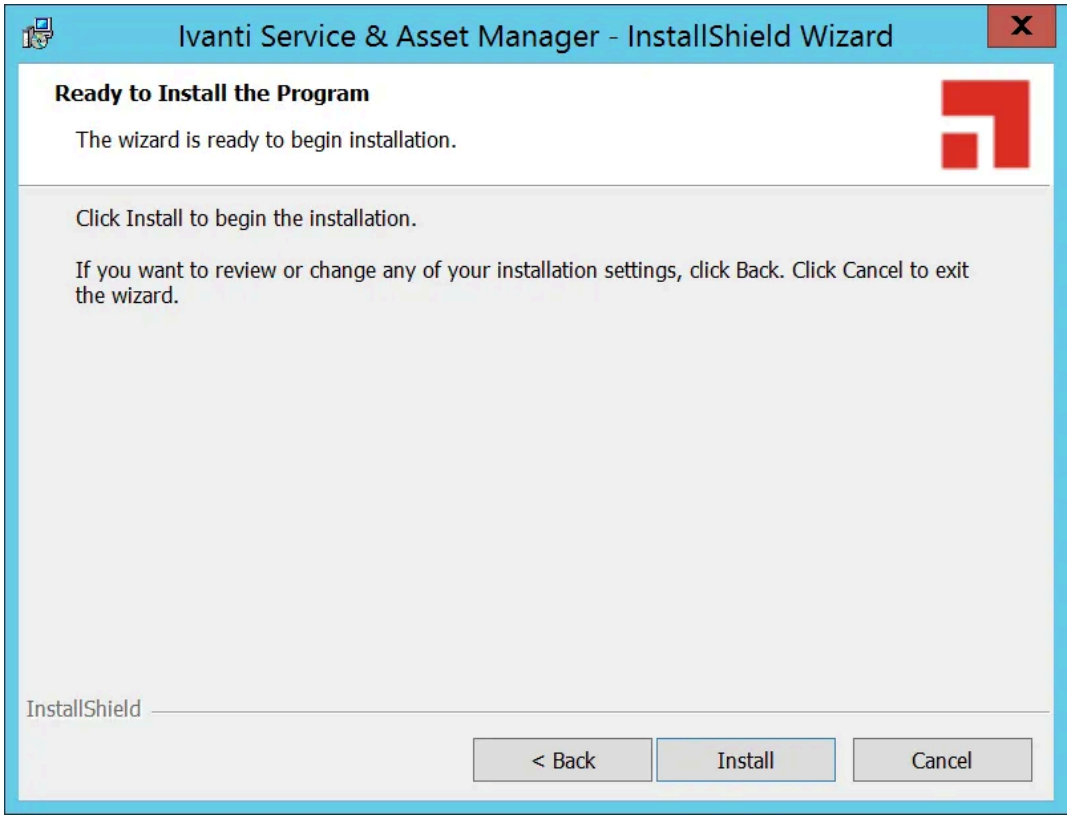


For more information on Asset Manager, access the following URL:
https://help.ivanti.com/docs/help/en_US/IAM/2018/LandingPage.htm

5. Select the **Custom** or **Complete** options.



2. Click **Next**.



The tabs that you see in the wizard depend on which components that you installed. You may see all of the tabs or you may just see a subset of them.

See the following sections:

- Using the System Configuration Wizard
- Configuring Neurons for ITSM
- Configuring the Reporting Feature
- Configuring Discovery
- Configuring the Deployment on the Neurons for ITSM Operations Console
- Optional SSL Configuration
- Optional LDAP Configuration
- About Configuring with ADFS
- About Configuring Throttling Settings

3.4.1. Using the System Configuration Wizard

The System Configuration Wizard provides an interface in which you can perform various configuration tasks for the initial setup of Neurons for ITSM.

- Starting the System Configuration Wizard Manually
- Navigating the System Configuration Wizard
- Actions to Perform in Each Page

Starting the System Configuration Wizard Manually

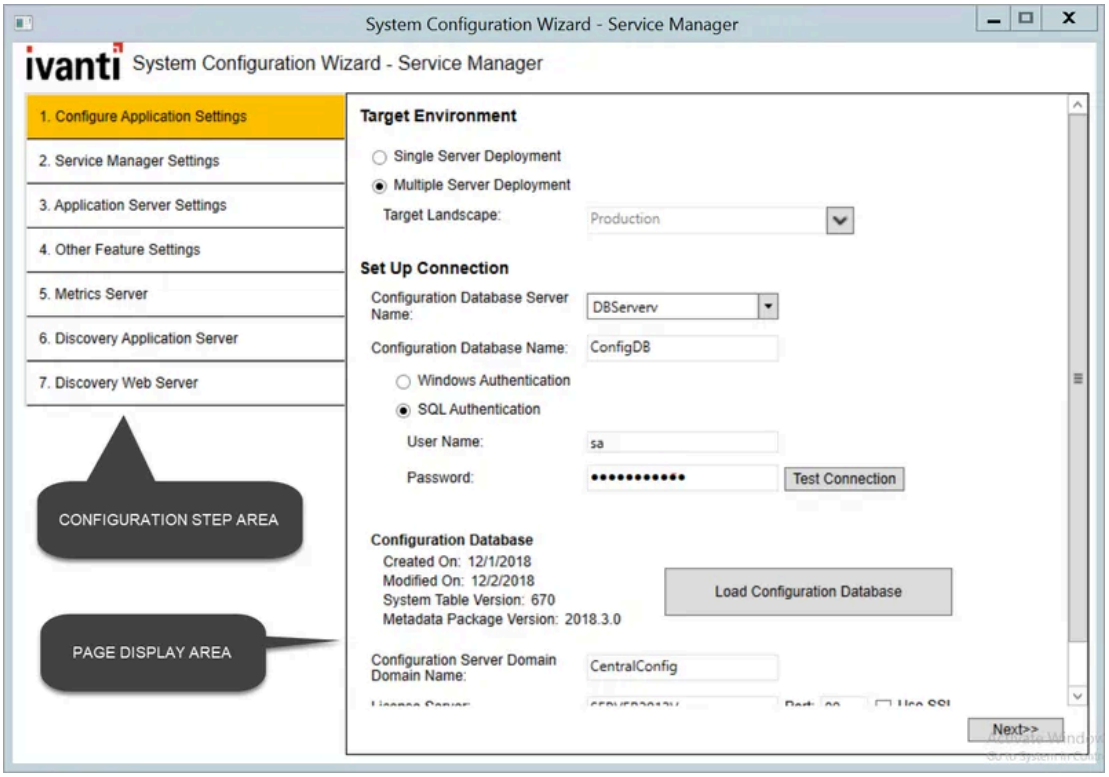
The System Configuration Wizard starts automatically after you finish installing Neurons for ITSM.

You can also start the System Configuration Wizard manually after your system is configured. See Changing Feature Settings by Running the System Configuration Wizard.

Navigating the System Configuration Wizard

The System Configuration Wizard contains the areas shown in System Configuration Wizard Areas.

System Configuration Wizard Areas



- In the configuration step area, the page that you are currently working on is highlighted in yellow.
- After you complete a page and click Next, the system places a green check mark next to the completed page name to show that it has been completed.

> The configuration step area is not a navigation pane. You cannot go to a page by clicking it in the configuration step area. Instead, click the **Next** and **Previous** buttons to move through the pages sequentially.

- The page display area shows the wizard page itself, including the fields and controls that you set the various parameters.

> - Chat Configuration installs Redis version 6.2 re-distributable which requires internet access while configuring the System Configuration Wizard.
> - The default behavior of the System Configuration Wizard with respect to **SSL** check boxes have changed from **non-SSL** to **SSL**. For non-SSL based installation these check boxes need to be cleared.
> - As part of the security fix, the System Configuration Wizard requires host name with domain (Fully Qualified Domain Name). For more information, refer to the **Configuring the Application Server Settings section** in the Installation and Deployment guide.

Actions to Perform in Each Page

The System Configuration Wizard page numbers can change depending on the features you choose to install.

Unless otherwise noted, the settings that you specify in each wizard page are stored in the Configuration Database.

Configuration Application Settings page:

- Specify the name of the configuration database and the authentication method that is used by all supported web applications when connecting to the configuration database.
- Create or recreate the configuration database.
- If you use Windows Integrated Security for the configuration database, specify the Windows domain credentials for the service account.

See **Configuring the Configuration Database**.

Service Manager Settings page:

- Specify the name and authentication method for the server where the Neurons for ITSM application database resides.
- Load the demo database on a server other than the server where the Neurons for ITSM application database resides. This option allows you to review the demo database while the Neurons for ITSM application database continues to run in its current configuration.
- Specify the application name, attachment location, client authorization key, and the type of name to use when accessing the application.

See **Configuring the Neurons for ITSM Application**.

ApplicatioServer Settings page:

- Specify the location of the configuration server and the host name.
- Specify if you will use this server for surveys or the reporting feature.
- If you use Windows Integrated Security for the Neurons for ITSM application server, specify the Windows domain credentials for the service account.

See **Configuring the Application Server Settings**.

Other Feature Settings page:

- Specify the log file and temporary file locations on the configuration server.
- Specify different server hosts and whether to use SSL for the Neurons for ITSM application server.
- Specify the inbound web server information.

See **Configuring Other Feature Settings**.

Metrics Server page:

- Specify the locations for the log file and the Neurons for ITSM configuration server.
- Map applications to the metrics server.

See **Configuring the Metrics Server**.

Microsoft SSRS Configuration page:

- Appears when you install the reporting feature.
- Specify information about the Microsoft SQL Server database for the reporting feature.

See **Configuring the Reporting Feature**.

Reporting Service Configuration page:

- Appears when you install the reporting feature.
- Specify information about the Neurons for ITSM report database for the reporting feature.

See **Configuring the Reporting Feature**.

Discovery Application Server page:

- Specify information about the configuration of the Discovery application server.

See **Configuring the Discovery Application Server**.

Discovery Web Server page:

- Specify information about the configuration of the Discovery web server.
- Upgrade the configuration database and the Neurons for ITSM application database.

See **Configuring the Discovery Web Server**.

Upgrade System page:

- Appears when you upgrade to a newer release of Neurons for ITSM.
- Upgrade the configuration database and the Neurons for ITSM application database.

See **Upgrading Neurons for ITSM from an Earlier Release**.

3.4.2. Configuring Neurons for ITSM

The following sections contain step-by-step instructions for the procedures that you can perform through the System Configuration Wizard.

- About Entering Server Location Names in the System Configuration Wizard
- Configuring the Configuration Database
- Configuring the Neurons for ITSM Application
- Configuring the Application Server Settings
- Configuring Other Feature Settings
- Configuring the Metrics Server
- Configuring the Discovery Application Server
- Configuring the Discovery Web Server
- Finishing the System Configuration

About Entering Server Location Names in the System Configuration Wizard

For all of the fields in the System Configuration Wizard that ask for a server location, unless noted otherwise, you can enter one of three things:

- An IP address
- A machine name
- A fully-qualified domain name

We recommend that you use the same naming format in all server location fields, if possible.

- If you are using SSL, you must enter a fully-qualified domain name.
- If you have a load-balanced system, we recommend using a fully-qualified domain name.

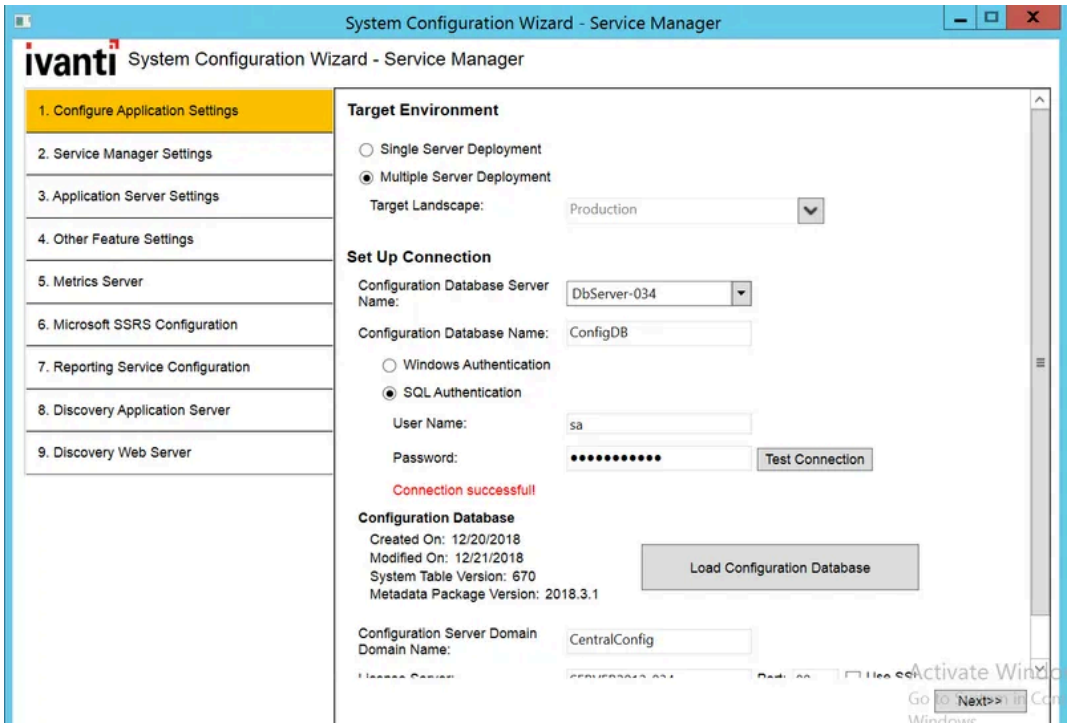
3.4.2.1. Configuring the Configuration Database

After you have installed Neurons for ITSM, the System Configuration Wizard starts automatically and displays the **Configuration Application** page.

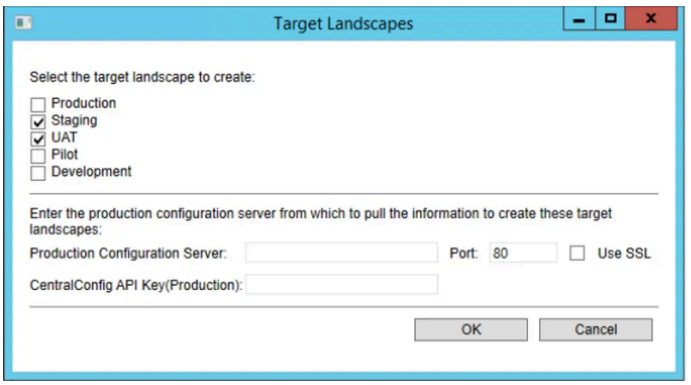
On this page, you will do the following:

- Specify the name of the configuration database and the authentication method that is used by all supported web applications when connecting to the configuration database.
- Create or recreate the configuration database.
- If you use Windows Integrated Security for the configuration database, specify the Windows domain credentials for the service account.

Configuration Application Page



1. Enter values into the fields:

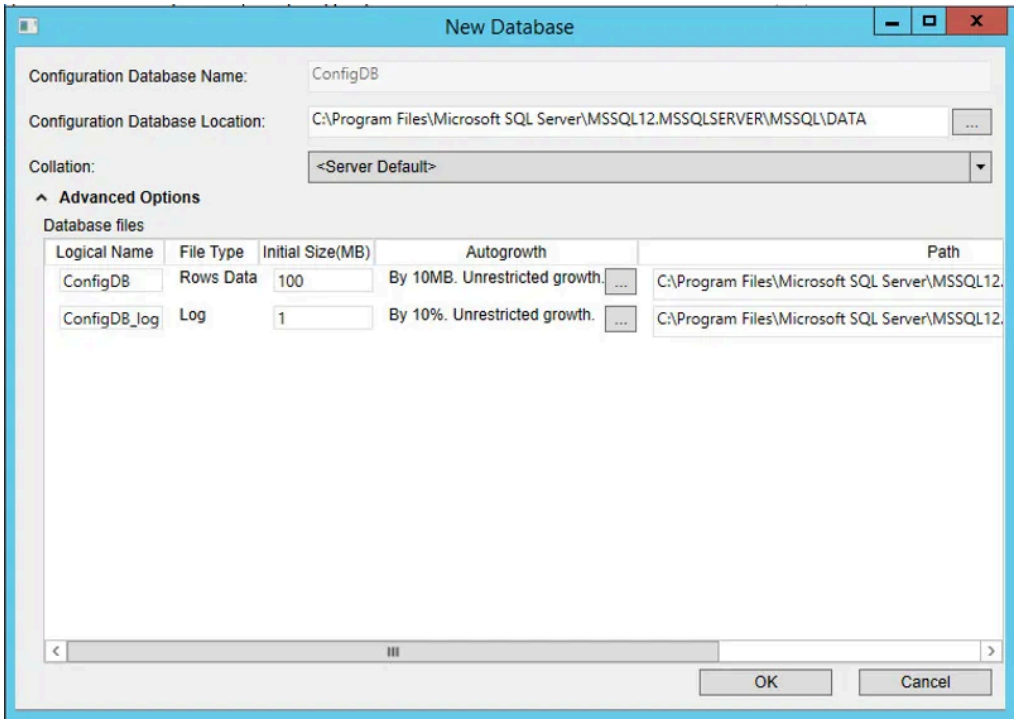
Parameter	Description
Target Environment	
Deployment	Choose one of the following: • Single Server Deployment: If you are setting up the **Minimum Production Deployment** . • Multiple Server Deployment: If you are setting up the **Enterprise Production Deployment**.
Target Landscape	(Only if you selected Multiple Server Deployment) Click the down arrow. The system displays the **Target Landscapes** dialog box. • On the first server that you configure, check Production and click OK. • On subsequent servers, check any combination of landscapes other than production and enter values in the subsequent fields. See below. *Target Landscapes Dialog Box* 
Production Configuration Server	(Only if you selected Multiple Server Deployment and selected anything other than Production in the **Target Landscape** field) The host or domain name of the configuration server for the production instance. Do not enter the information for any other instance; you must enter the information for the production instance.
Port	(Only if you selected Multiple Server Deployment and selected anything other than Production in the **Target Landscape** field) The port number of the production server. The default is 80, or 443 if you check Use SSL.
Use SSL	(Only if you selected Multiple Server Deployment and selected anything other than Production in the **Target Landscape** field) Check to enable SSL encryption to the server.
CentralConfig API Key (Production)	CentralConfig API key of the production environment. To retrieve the CentralConfig API Key,- navigate to the Configuration console > **Configure** > **Security Controls** > **API Keys** > **CentralConfigApiKey (Key groups)** > **CentralConfigApiKey)**.

2. Click OK to close the **Target Landscapes** dialog box.
3. Enter values into the fields:

Parameter	Description
Configuration Database Server Name	The server where the configuration database is located. Do one of the following: • Accept the default value. • Enter the name of the server of the configuration database. • Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click OK. NOTE: Do not choose localhost unless you are setting up a **Demonstration or Proof-of-Concept Deployment**.
Configuration Database Name	The name of the configuration database. The default name is ConfigDB and you cannot change the name.
Authentication Method	Select one of the following: • Windows Authentication: Uses Microsoft Windows authentication. • SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below.
User Name	(Only if you selected SQL Authentication) The user name associated with the Microsoft SQL authentication. NOTE: If your deployment store FILESTREAM attachments, specify a configuration database user account that has a db_owner role on Microsoft SQL Server. See **Task 2: Setting up Neurons for ITSM**.
Password	(Only if you selected SQL Authentication) The password associated with the user name for the Microsoft SQL authentication.

4. Click Test Connection to test the connection to the configuration database server. The system displays *Connection successful!* if the connection is good. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
5. Depending if there is already a configuration database, click Load Configuration Database or Re-Create & Load Configuration DB. If the configuration database already exists, the system asks if you want to recreate the database. Click Yes. The system displays the **New Database** dialog box.

   New Database Dialog Box



6. Enter values into the fields:

Parameter	Description
Configuration Database Name	The name of the configuration database. The default name is ConfigDB and cannot be changed.
Configuration Database Location	The location for the configuration database. NOTE: If you have customized the existing configuration database, specify a different location; otherwise, the system overwrites your customization when you load the recreated database.
Collation	The set of rules that describe how to compare and sort strings, such as the order in which letters are sorted and whether case matters. NOTE: ISM application does not support case sensitive SQL Collation.
Advanced Options	
Logical Name	The logical name of the configuration database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
File Type	The file type, either database records or database logs. These values are read-only.
Initial Size (MB)	The initial file size, in MB, when creating the configuration database.
Autogrowth	Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
Path	The location of the file. Click ... to update the location.
File Name	The name of the file.

7. Click OK. The system creates the configuration database and installs it on the configuration database server that you specified. Several progress dialog boxes appear as various Microsoft SQL scripts execute to create and load the configuration database. After the system loads the configuration database, the **Configuration Application** page displays *Configuration database loaded*.
8. Click Next. The system refreshes the **Configuration Application** page. (If you end up on the next page of the System Configuration Wizard, click Previous to return to the **Configuration Application** page.)
9. Enter values into the fields:

Parameter	Description
Configuration Server Domain Name	The fully-qualified domain name of the configuration server in this format: config.servername.com.
License Server	The name of the license server. We recommend using a fully-qualified domain name.
Port	The port number of the license server. The default is 80, or 443 if you check Use SSL.
Use SSL	Check if the license server uses SSL.
IvantiSM License File-Production	The name of the license file for the Neurons for ITSM production instance. Click Browse..., navigate to the license file, and click Open. License files have a .lic suffix. NOTE: The system displays either one or both of the license fields, depending on your landscape environment. At this point, you only need to enter one license, which allows the License Manager to start and run Neurons for ITSM. You can import additional licenses, if needed, at a later time from within the License Manager. See **Using the License Manager**.
IvantiSM License File-Non-Production	The name of the license file for the Neurons for ITSM non- production instance. Click Browse..., navigate to the license file, and click Open. License files have a .lic suffix. NOTE: The system displays either one or both of the license fields, depending on your landscape environment. At this point, you only need to enter one license, which allows the License Manager to start and run Neurons for ITSM. You can import additional licenses, if needed, at a later time from within the License Manager. See **Using the License Manager**.

10. Create the administrator account for the configuration database. You only need to create this account once. If you return to this page in the System Configuration Wizard later, these fields are not displayed.

    Enter values into the fields:

Parameter	Description
Login ID	The system automatically displays the login ID of HSWAdmin. You cannot change this.
Password	The password associated with the administrator. Record this password for future reference. If you lose the password, you must recreate and load the configuration database.
Confirm Password	Re-enter the password associated with the administrator.
First Name	The first name of the administrator.
Last Name	The last name of the administrator.
Email Address	The email address of the administrator.

11. Do one of the following:
    - If you chose Single Server Deployment, click Next. The system displays the Neurons for ITSM **Application** page.
    - If you chose Multiple Server Deployment, repeat all of the steps in this procedure to create a configuration database for each of your tenants. Then click Next. The system displays the Neurons for ITSM **Application** page.

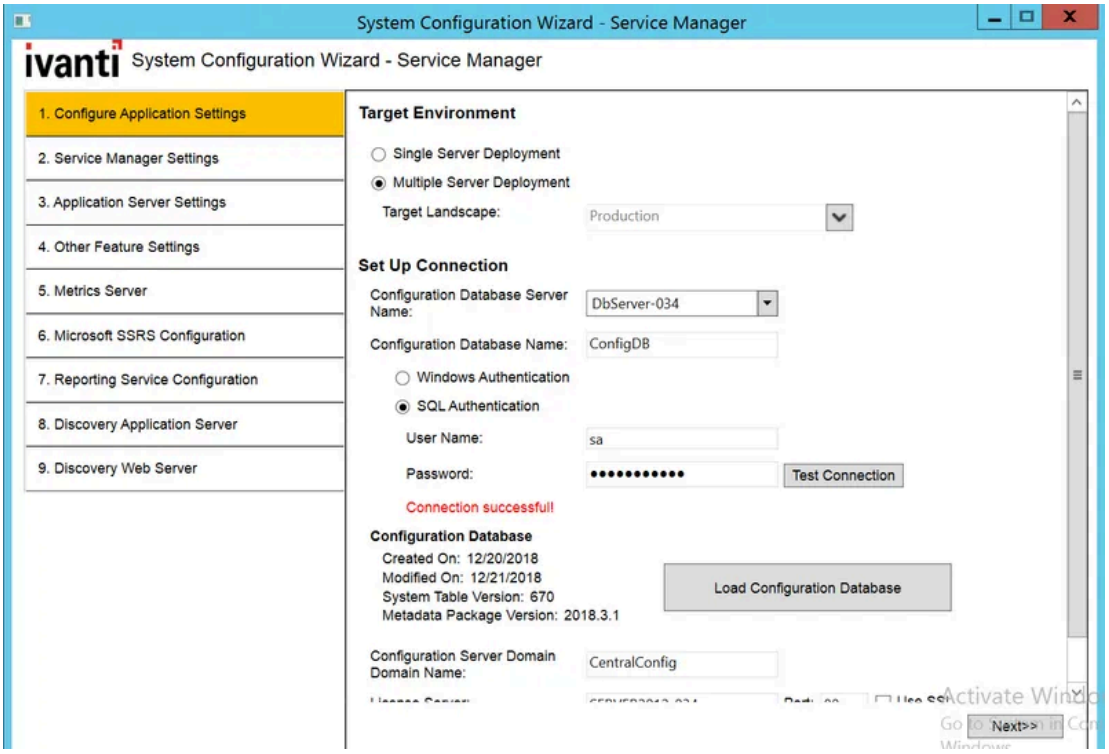
3.4.2.2. Configuring the Neurons for ITSM Application

On this page you will do the following:

- Specify the name and authentication method for the server where the application database resides.
- Load the demo database on a server other than the server where the application database resides. This option allows you to review the demo database while the application database continues to run in its current configuration.
- Specify the application name, attachment location, client authorization key, and the type of name to use when accessing the application.

The first time that you see this page, there is no application database, as shown in **Service Manager Application Page: No Database**.

Service Manager Application Page: No Database

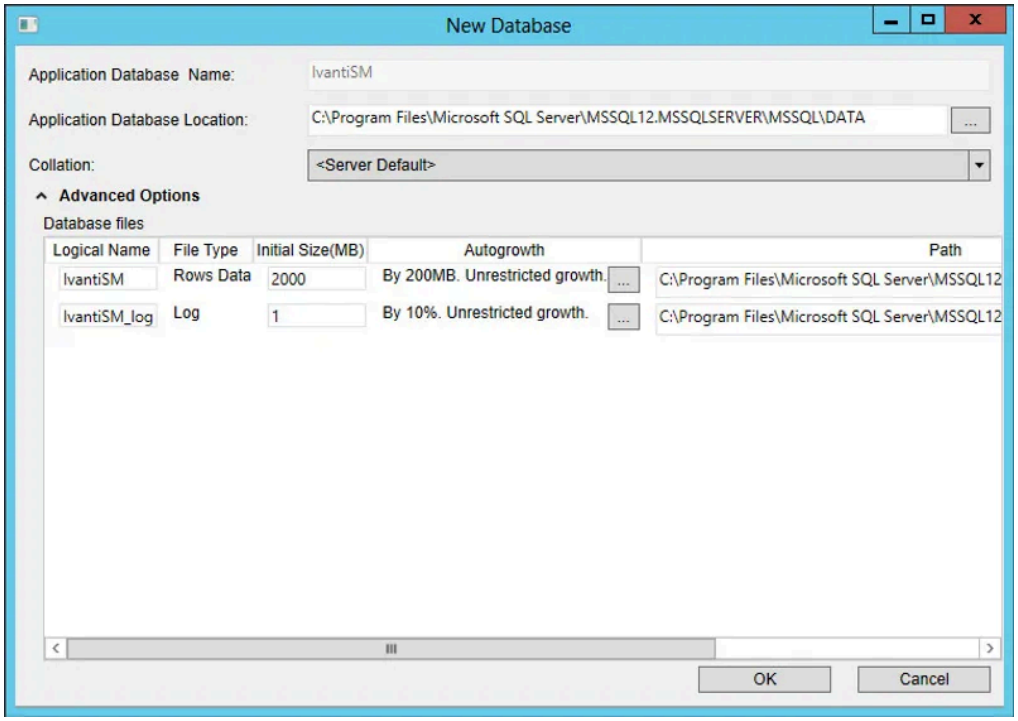


1. Enter values into the fields:

Parameter	Description
Application Database Server	The server where the application database is located. Usually this is the same server where the configuration database is located (specified earlier on the **Configuration Application** page). Do one of the following: 1. Accept the default value. 2. Enter the name of the server of the application database. Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click ODo not choose localhost unless you are setting up a **Demonstration or Proof-of-Concept Deployment**.
Application Database Name	The name of the application database. The default name is IvantiSM. The name that you specify here is used when the application database is created, and later, recreated.
Authentication Method	Select one of the following: • Windows Authentication: Uses Microsoft Windows authentication. • SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below.
User Name	(Only if you selected SQL Authentication) Enter the user name associated with the Microsoft SQL authentication.
Password	(Only if you selected SQL Authentication) Enter the password associated with the user name for the Microsoft SQL authentication.

3. Click Test Connection to test the connection to the application database server. The system displays *Connection successful!* if the connection is good. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
4. Depending if there is already an application database, click Load Application Database or Re-Create & Load Application DB. If the application database already exists, the system asks if you want to recreate the database. Click Yes. The system displays the **New Database** dialog box.

   New Database Dialog Box



5. Enter values into the fields:

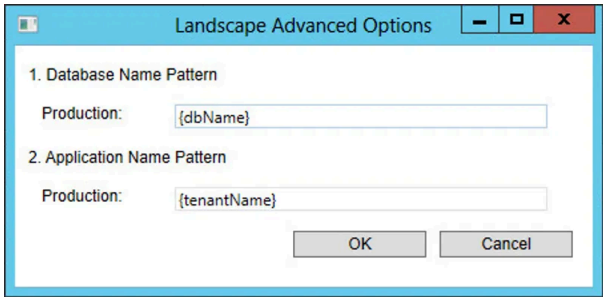
Parameter	Description
Application Database Name	The name of the application database. The default name is IvantiSM and cannot be changed.
Application Database Location	The location for the application database. NOTE: If you have customized the existing application database, specify a different location; otherwise, the system overwrites your customization when you load the recreated database.
Collation	The set of rules that describe how to compare and sort strings, such as the order in which letters are sorted and whether case matters. NOTE: ISM application does not support case sensitive SQL Collation.
Advanced Options	
Logical Name	The logical name of the application database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
File Type	The file type, either database records or database logs. These values are read-only.
Initial Size (MB)	The initial file size, in MB, when creating the application database.
Autogrowth	Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
Path	The location of the file. Click ... to update the location.
File Name	The name of the file.

6. Click OK.

The system creates the application database and installs it on the application database server that you specified. The system displays several progress dialog boxes as the system executes various Microsoft SQL scripts that create and load the application database. After the system loads the application database, the system displays *Application Database loaded*.

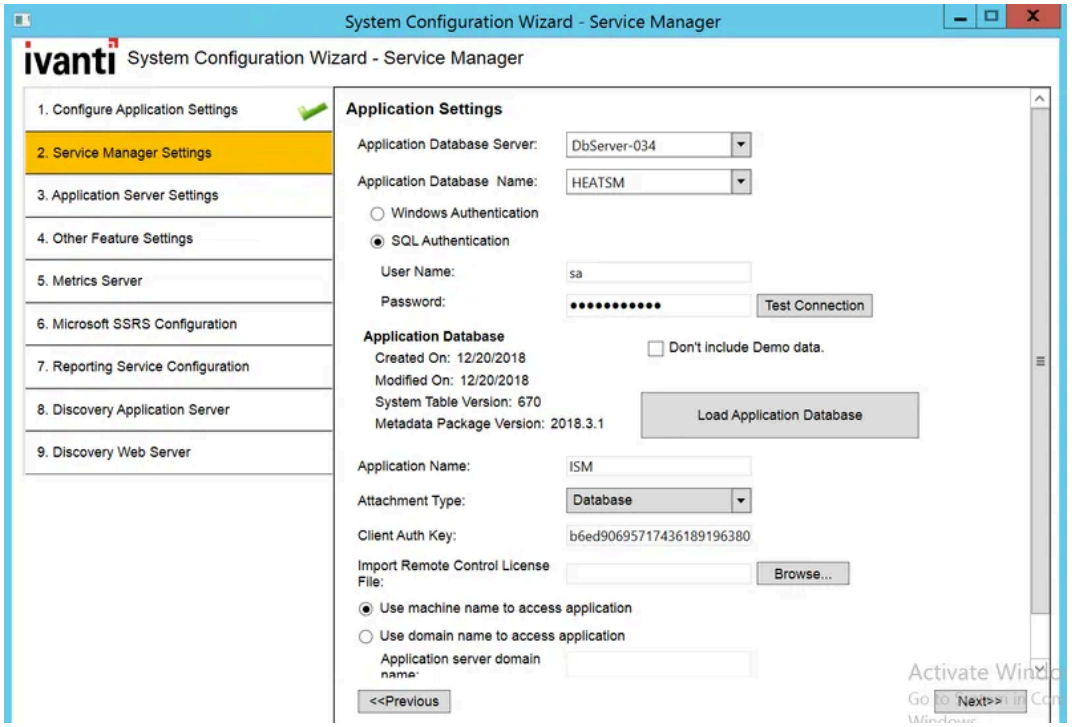
7. (Optional) Click **Advanced Options** to open the **Landscape Advanced Options** dialog box. See the "Adding a Landscape" topic in the *Operations Console User Guide for* Neurons for ITSM for more information about these patterns.

   Landscape Advanced Options Dialog Box



8. Click Next. The system refreshes the **Application** page. See **Application Page: Newly Created Database**. (If you end up on the next page of the System Configuration Wizard, click Previous to return to the **Application** page.)

   Application Page: Newly Created Database



9. Neurons for ITSM comes with optional transaction data that you can use to test and view the analytic metrics, financial, ITFM, and other features.
10. Enter values into the fields:

Parameter	Description
Application Name	The name of the application.
Attachment Type	The location of the folder on the application database server where any Neurons for ITSM attachments reside. Select one of the following: • Database • FILESTREAM • File System
Client Auth Key	The authentication key that is used when the web services API accesses Neurons for ITSM.
Import Remote Control License File	(Optional) If you are going to use the remote control feature, you must have a remote control license. • Contact Ivanti Software to get the license. • To import the remote control license file, click Browse... next to the **Import Remote Control License File** field. • Browse to the location of the license file and click OK to select it.
To access the application	Select whether to use the application database server machine name or the fully-qualified domain name for access to the application database server: • Use machine name to access Ivanti application: When other Neurons for ITSM components log into the application server, they use the machine name of the server. For example, they use **SERVER-01**. If you choose this option, the system detects the current machine name and uses it automatically; you do not need to specify the machine name. • Use domain name to access Ivantiapplication: When other Neurons for ITSM components log into the application server, they use the fully-qualified domain name of the server. For example, they use SERVER-01.company.com. If you plan on using SSL for connecting to the application server (configured later on the **Other Feature Settings** page), you must enter a fully-qualified domain name here, either for an individual machine or for a load-balanced instance.
Application server domain name	(Only if you selected Use domain name to access Ivantiapplication) The domain name of the application server.

11. Click Next to refresh the **Application** page. (If you end up on the next page of the System Configuration Wizard, click Previous to return to the **Application** page.)
12. Create the administrator account for the application database. This login ID and password allows you to access the Neurons for ITSM Service Desk Console and Configuration Console. See Logging into Neurons for ITSM. You only need to create this account once. If you return to this page in the System Configuration Wizard later, these fields are not displayed.

    Enter values into the fields:

Parameter	Description
Login ID	The system automatically displays the login ID of IvantiAdmin. You cannot change this.
Password	The password associated with the administrator. Record this password for future reference. If you lose the password, you must recreate and load the application database.
Confirm Password	Re-enter the password associated with the administrator.
First Name	The first name of the administrator.
Last Name	The last name of the administrator.
Email Address	The email address of the administrator.

13. If you chose Multiple Server Deployment on the **Configuration Application** page, your system has multiple tenants. Each tenant must have an administrator account, so that the administrator can access the Neurons for ITSM Service Desk Console and Configuration Console.

    To create a new administrator account for another tenant instance, do the following:

    a. In the **Application Database Name** field at the top of this page, enter the next tenant to get an account.

        For example, if you named your production tenant IvantiSM, your staging tenant IvantiSM-STG, and your UAT tenant IvantiSM-UAT, then the first time that you are on this page, enter IvantiSM in the **Application Database Name** field. The second time that you are on this page, enter IvantiSM-STG in the **Application Database Name** field. The third time that you are on this page, enter IvantiSM-UAT in the **Application Database Name** field.

    b. Create the administrator account for the application database for the**Configuring Other Feature Settings** tenant. See step 11 above.

    c. Click **Next**. The system displays the **Application Server Settings** page.

    d. Click Previous to return to the Neurons for ITSM **Application** page.

    e. Repeat steps a. through d. for the next tenant.

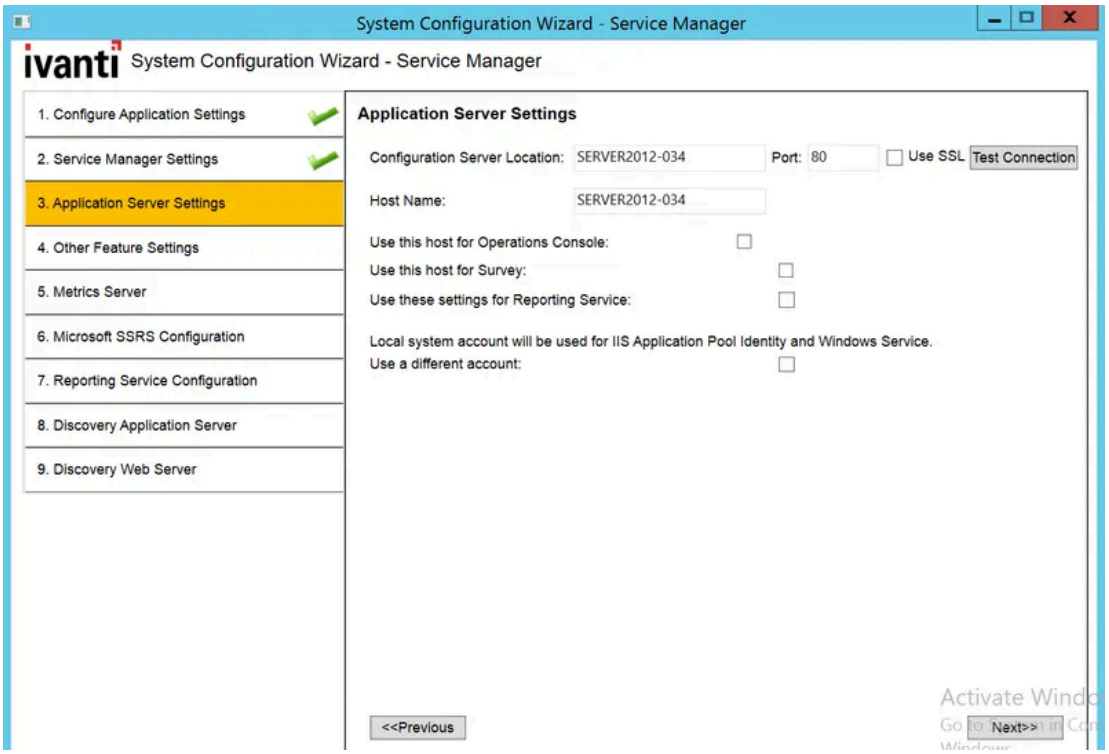
14. After all of your tenants have an administrator account, click Next **Configuring the Reporting Feature**to advance to the **Application Server Settings** page.

3.4.2.3. Configuring the Application Server Settings

You set connections to other databases in Neurons for ITSM on the **Application Server Settings** page. You will do the following:

- Specify the location of the configuration server and the host name.
- Specify if you will use this server for surveys or the reporting feature.
- If you use Windows Integrated Security for the Application Server, specify the Windows domain credentials for the service account.

Application Server Settings Page



1. Enter values into the fields:

Parameter	Description
Configuration Server Location	The host name or domain name of the configuration server. The default value is the name of the server that you are logged into now. If the host that you are logged into now is *not* the configuration server, enter the machine name or fully-qualified domain name of your Configuration Server. If you check Use SSL below, you must enter the host name of the configuration server.
Port	The port number of the configuration server. The default is 80, or 443 if you check Use SSL.
Use SSL	Check to use SSL for connections to the configuration server. NOTE: We do not recommend enabling SSL on the configuration server until you have fully tested Neurons for ITSM to ensure that it works with SSL. For information on configuring Neurons for ITSM with SSL, see **Optional SSL Configuration**.

2. Click Test Connection to test the connection to the configuration server. The system displays a success or failure message. Click OK to close the message.
3. Enter values in the fields:

Parameter	Description
Host Name	The location of the system that hosts the Application Server. The default value is the server that you are logged into now. Do one of the following: • If you are installing all Neurons for ITSM components on the same host, accept the default value. • If you enter a different location, it must be a machine name. Do *not* enter a fully-qualified domain name.
Use this host for Ivanti Operations Console	Uses this server for the Ivanti Service Manager Operations Console. NOTE: If you have an **Enterprise Production Deployment**, we recommend that you only install and use the Neurons for ITSM Operations Console on the staging (STG) instance of the tenant.
Landscape Type	(Only if you checked Use this host for Ivanti Operations Console) Displays the landscape type and cannot be changed.
Database Server	(Only if you checked Use this host for Ivanti Operations Console) Displays the database server and cannot be changed.
Operations Console Backup Location	(Only if you checked Use this host for Ivanti Operations Console) The backup location for the Neurons for ITSM Operations Console. The backup location can either be on a database server or on a network folder. Do one of the following: 1. Accept the default location. 2. Enter a new location. 3. Click Browse... and navigate to a new location.
Test Backup & Restore	(Only if you checked Use this host for Ivanti Operations Console) The database to test to ensure you can back up and restore it. Select one from the drop-down list. We recommend that you select the configuration database since it is small. Click test to test the connection. The system displays a message with the results of the test. Click OK to close the message.
Use this host for Survey	Uses this server for the Neurons for ITSM survey component. If you use Windows Authentication for the configuration server, the system prompts you for the Windows domain account and credentials.
Use these settings for Reporting Service	Uses this server for the Neurons for ITSM reporting feature. Usually, you configure the reporting feature on the **Microsoft SSRS Configuration** and **Ivanti Reporting Service Configuration** pages. However, if you have two different domains and the reporting feature server cannot reach the web server, you can configure these settings to enable the servers to communicate.
Use SSL for Reports	(Only if you checked Use these settings for Reporting Service) Uses SSL for reports.
Use Windows Authentication for SSRS	(Only if you checked Use these settings for Reporting Service) Uses Windows authentication for reports. If you plan on sharing the same Microsoft SSRS instance with other applications besides the reporting feature, you must use Windows authentication.
Web Service Virtual Directory	(Only if you checked Use these settings for Reporting Service) The name of the web service virtual directory.
Ivanti Web Application Pool	(Only if you checked Use these settings for Reporting Service) The application pool identity for the Neurons for ITSM web application pool. Select one of the following:

Parameter	Description
Identity Account	• Keep existing account • Specify new account If you select Specify new account, click Set to enter the credentials.
User Name	(Only if you checked Use these settings for Reporting Service and selected Specify new account for the **Ivanti Web Application Pool Identity Account** field) The user name for the application pool identity for the Neurons for ITSM web application pool.
Password	(Only if you checked Use these settings for Reporting Service and selected Specify new account for the **Ivanti Web Application Pool Identity Account** field) The password associated with the user above. Click OK.

4. If you are using Microsoft SQL authentication for the configuration server, the system displays this message: "Local system account will be used for IIS Application Pool Identity and Windows Service". See **Service Account** for more information about this account.

To use a different account, do the following:

a. Check Use a different account.

b. Click Set.

c. Enter the user name for the service account.

d. Enter the password associated with the service account.

e. Click OK.

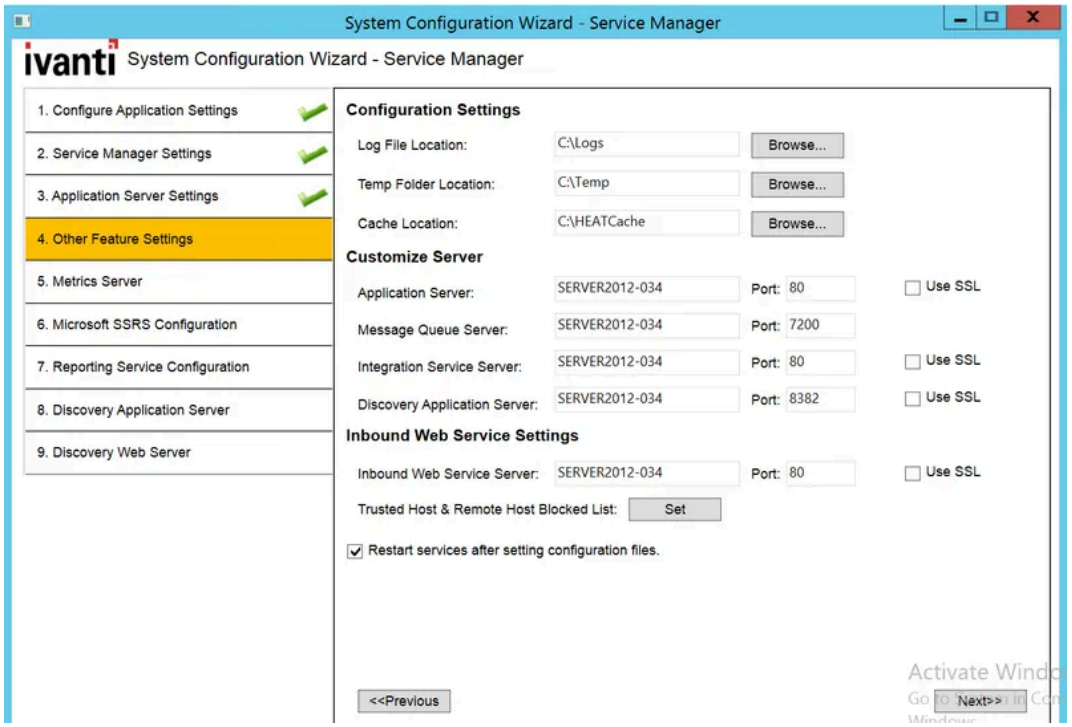
5. Each tenant in a multiple server deployment must have an administrator account. If you selected Multiple Server Deployment on the **Configuration Application** page, click Previous to return to the Neurons for ITSM application page and create additional tenant accounts.

3.4.2.4. Configuring Other Feature Settings

On this page you will do the following:

- Specify the log file and temporary file locations on the configuration server.
- Specify different servers and ports and whether to use SSL for the other Neurons for ITSM servers.
- Specify the inbound web server information.

Other Feature Settings Page



1. Enter values into the fields:

Parameter	Description
Configuration Settings	
Log File Location	The folder on the server that you are logged into now where the log files are located. Do one of the following: 1. Accept the default value. 2. Enter the name of the folder where the log files are located. 3. Browse for a different folder by clicking Browse.... Select a new folder and click OK. You have to provide the path for nlog.config files as well to store the non-configrable files.
Temp Folder Location	The folder on the server that you are logged into now where the temporary files are located. The temporary folder is used to cache JavaScript files and to enable integration server and Neurons for ITSM Operations Console features. Do one of the following: 1. Accept the default value. 2. Enter the name of the folder where the temporary files are located. 3. Browse for a different folder by clicking Browse.... Select a new folder and click OK.
Cache Location	The folder on the server that you are logged into now where the cached files are located. Do one of the following: 1. Accept the default value. 2. Enter the name of the folder where the temporary files are located. 3. Browse for a different folder by clicking Browse.... Select a new folder and click OK.
Customize Server	
Application Server	Where the application server is located. The default value is the server that you are logged into now. Do one of the following: 1. Accept the default value. 2. Enter the name where the application server is located. 3. If you use SSL, you must enter a fully-qualified domain name. NOTE: If you choose a different server for the application server and check Use SSL, SSL is only enabled for the application server. It does not enable SSL for the configuration server.
Port	The port number of the application server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the application server.
Message Queue Server	Where the message queue server is located. The default value is the server that you are logged into now. Do one of the following: 1. Accept the default value. 2. Enter the name where the Neurons for ITSM message queue server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the message queue server. The default is 7200.

Parameter	Description
Use SSL	Enables SSL encryption to the message queue server.
Integration Server	Where the integration server is located. The default value is the server that you are logged into now. Do one of the following: 1. Accept the default value. 2. Enter the server where the Neurons for ITSM integration server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Neurons for ITSM integration server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the Neurons for ITSM integration server.
Discovery Application Server	Where the Discovery application server is located. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the server where the Discovery application server is located. • If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Discovery application server. The default is 8382, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the Discovery application server.
Inbound Web Service Settings	
Inbound Web Server	Where the inbound web server is located. The default value is the server that you are logged into now. Do one of the following: 1. Accept the default value. 2. Enter the server where the Neurons for ITSM inbound web server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Neurons for ITSM inbound web server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the Neurons for ITSM inbound web server.

You can set a list of remote hosts to block and a list of remote hosts to trust. By default, the list is empty.

3. To designate a list of blocked servers, do the following:

   a. Next to the **Trusted Host & Remote Host Blocked List** field, click Set.

   b. In the **Remote Host Blocked List** area, click the plus icon.

   c. Enter the starting IP address and the ending IP address for the blocked servers.

   d. If you are blocking web scripts, check Is Web Script.

   e. Click OK.

4. To designate a list of trusted servers, do the following:

   a. Next to the **Trusted Host & Remote Host Blocked List** field, click Set.

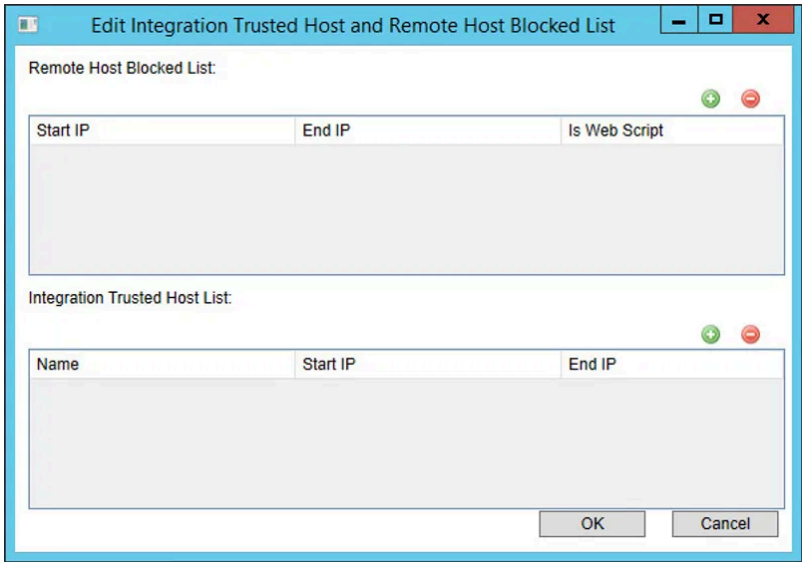
b. In the **Integration Trusted Host List** area, click the plus icon.

c. Enter a name for the trusted host list.

d. Enter the starting IP address and the ending IP address for the trusted servers.

e. Click OK.

Edit Integration Trusted Host and Remote Host Blocked List Dialog Box



To update the list at a later time, run the System Configuration Wizard, advance to the **Other Feature Settings** page, click Set, and make your changes. When you are done, click OK.

5. To restart the Neurons for ITSM services after you exit the System Configuration Wizard, check Restart services after setting configuration files.
6. Verify that the Neurons for ITSM services restart after the wizard closes.
7. If you did not check Restart services after setting configuration files, restart the Neurons for ITSM services manually.
8. Click Next. The system displays the **Metrics Server** page.

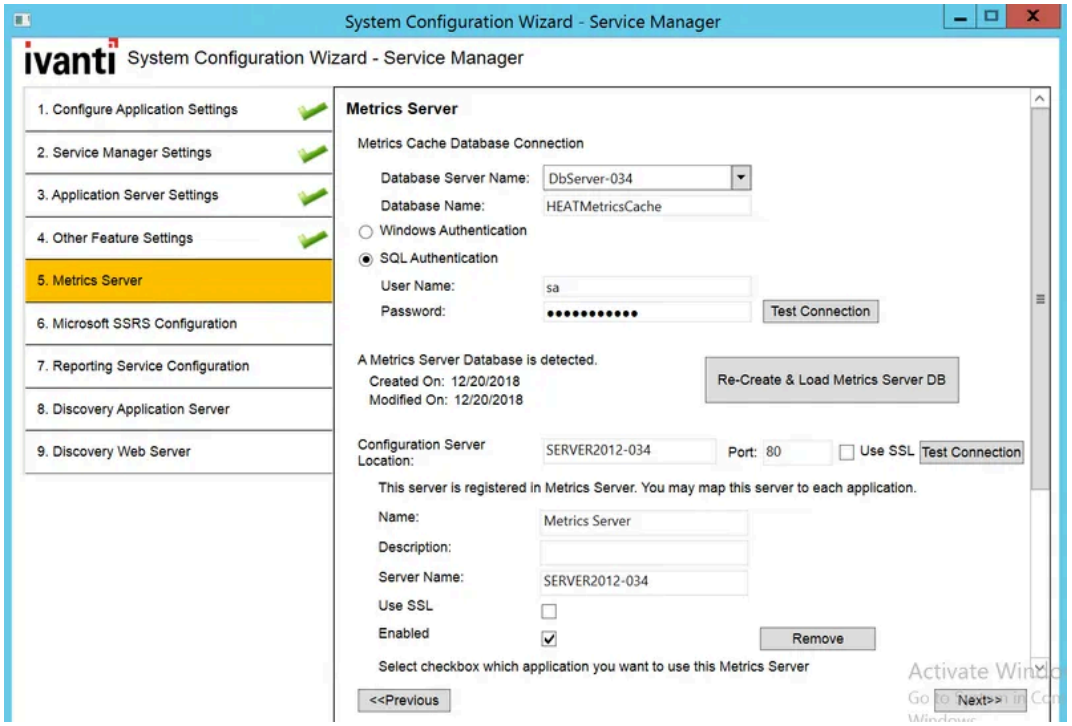
3.4.2.5. Configuring the Metrics Server

Perform these steps to configure one or more Metrics Server databases, which you can use to analyze data. Your deployment can have multiple Metrics Server databases to improve performance.

On this page, you will do the following:

- Specify the locations for the log file and the configuration server.
- Map applications to the Metrics Server.

Metrics Server Page



1. Enter values into the fields:

Parameter	Description
Metrics Cache Database Connection	
Database Server Name	Where the metrics cache database server is located. The default value is the server where the application server is located. Do one of the following: • Accept the default value. • Enter the name of the server of the metrics cache database. • Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays all available database servers in the network for your connection. Choose a server and click OK. NOTE: Do not choose localhost unless you are setting up a **Demonstration or Proof-of-Concept Deployment**.
Database Name	The name of the metrics cache database. Do one of the following: • Accept the default value. • Enter the name of the metrics cache database.
Authentication Method	Select one of the following: • Windows Authentication: Uses Microsoft Windows authentication. • SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below. NOTE: The metrics cache database server is not compatible with SSL if your system has Windows authentication set up.
User Name	(Only if you selected SQL Authentication) The user name associated with the Microsoft SQL authentication.
Password	(Only if you selected SQL Authentication) The password associated with the user name for the Microsoft SQL authentication.

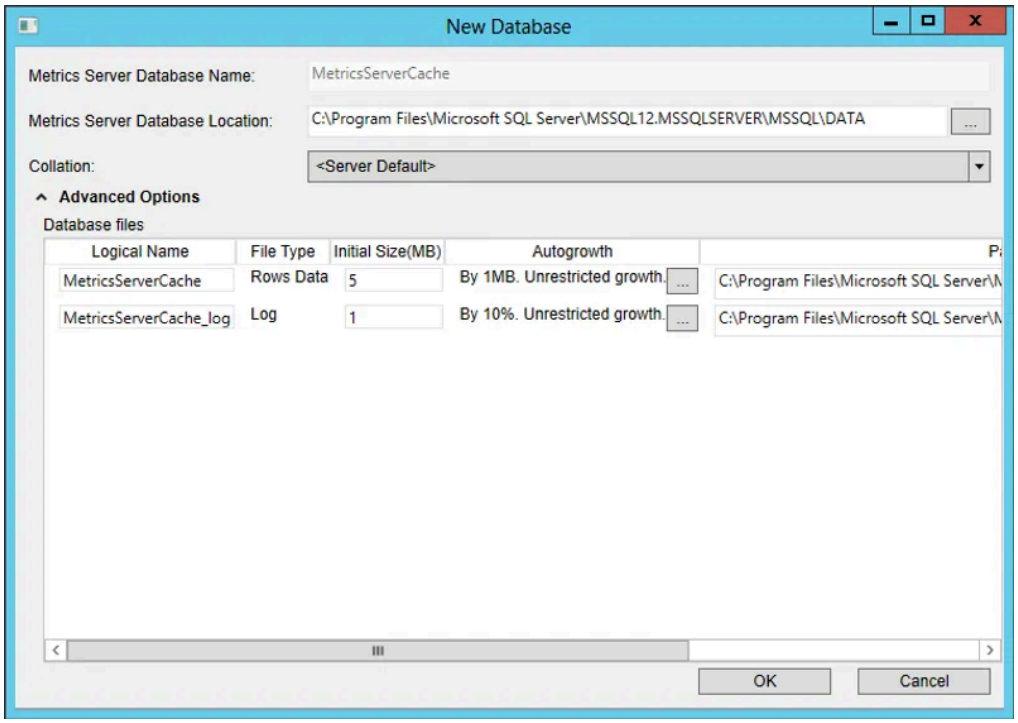
2. Click Test Connection to test the connection to the metrics cache database server. The system displays a success or failure message below the **Test Connection** button. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
3. Do one of the following:
    - If this is the initial setup, go to **Creating a New Metrics Server Database**.
    - If your system already has a metrics server database, go to **Recreating the Metrics Server Database**.

Creating a New Metrics Server Database

An initial installation does not have a metrics server database. Follow these steps to create one.

1. Click Create & Load Metrics Server DB. The system displays the **New Database** dialog box.

   New Database Dialog Box



2. In the **Location** field, select a location for the metrics server database.
3. Click Advanced Options to view and reconfigure these metrics server database settings:
   - Logical name: The logical name of the metrics database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
   - File type: The file type, either database records or database logs. These values are read-only.
   - Initial size in MB: The initial file size, in MB, when creating the metrics database.
   - Autogrowth size: Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
   - The location of the database: The location of the file. Click ... to update the location.
   - File name: The name of the file.
4. Click OK in the **New Database** dialog box.

The **Configuration Server Location** field indicates the location of the system that hosts the configuration server. The default value is the name of the host that you are logged into now.

5. If this is the system that hosts the configuration server, accept the default value.

If the host that you are logged into now is not the configuration server, enter the machine name or fully-qualified domain name of your configuration server.

If you use SSL, you enter the fully-qualified domain name of the configuration server.

6. Enter the port number in the **Port** field. The default value is 80. If you click Use SSL, it changes to 443.
7. Select whether to use SSL for connections to the configuration server.

If you use SSL, you must provide a fully-qualified domain name in the **Configuration Server Location** field.

8. Click Test Connection to test the connection to the configuration server. A pop-up message notifies you of success or failure.

> We do not recommend enabling SSL on the configuration server until you have fully tested Neurons for ITSM to ensure that it works with SSL.
>
> For information on configuring Neurons for ITSM with SSL, see **Optional SSL Configuration**.

9. Enter the following information to register a server in a multi-server deployment to the metrics server database:
    - Accept the default server name or enter a different name.
    - Optional. Enter a description of the server.
    - The default server name value is the name of the host that you are logged into now. You must use this name or localhost.
    - Check the box to use SSL encryption.
    - Check the box to enable this metrics server.
10. Click Save.
11. To map an application to the new metrics server to an application, check Map. You can reference the same metrics server to multiple Neurons for ITSM applications.

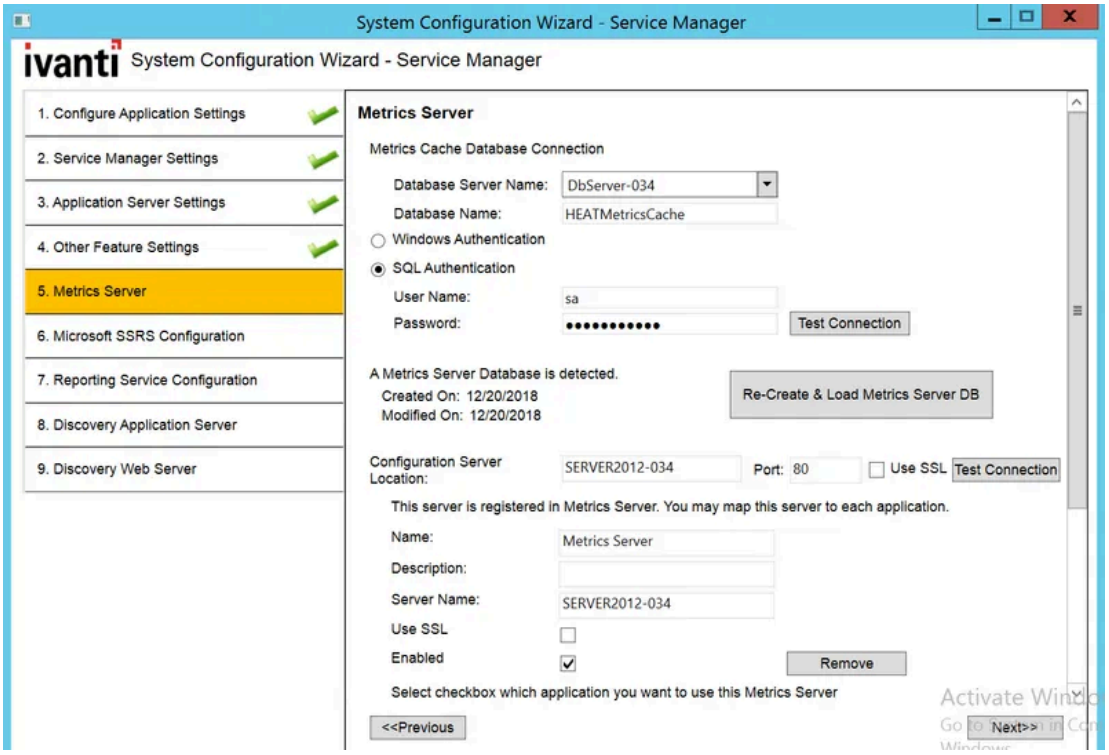
> To change this server at a later time, run the System Configuration Wizard, advance to the **Metrics Server** page, and click Remove.

12. Click Next. The system displays the **Discovery Application Server** page.

Recreating the Metrics Server Database

If you are upgrading or repairing Neurons for ITSM, you already have a metrics server database, and the **Metrics Server** page looks like **Metrics Server Page**.

Metrics Server Page



1. To recreate the metrics server database, click Re-Create & Load Metrics Server DB. The system displays the **New Database** dialog box.
2. Perform steps 2 through 12 in **Creating a New Metrics Server Database**.

If you have customized the existing metrics server database, specify a different location in the **Metrics Server Database Location** field in the **New Database** dialog box. Otherwise, the system overwrites your customization when you load the recreated database.

3.4.2.6. Configuring the Discovery Application Server

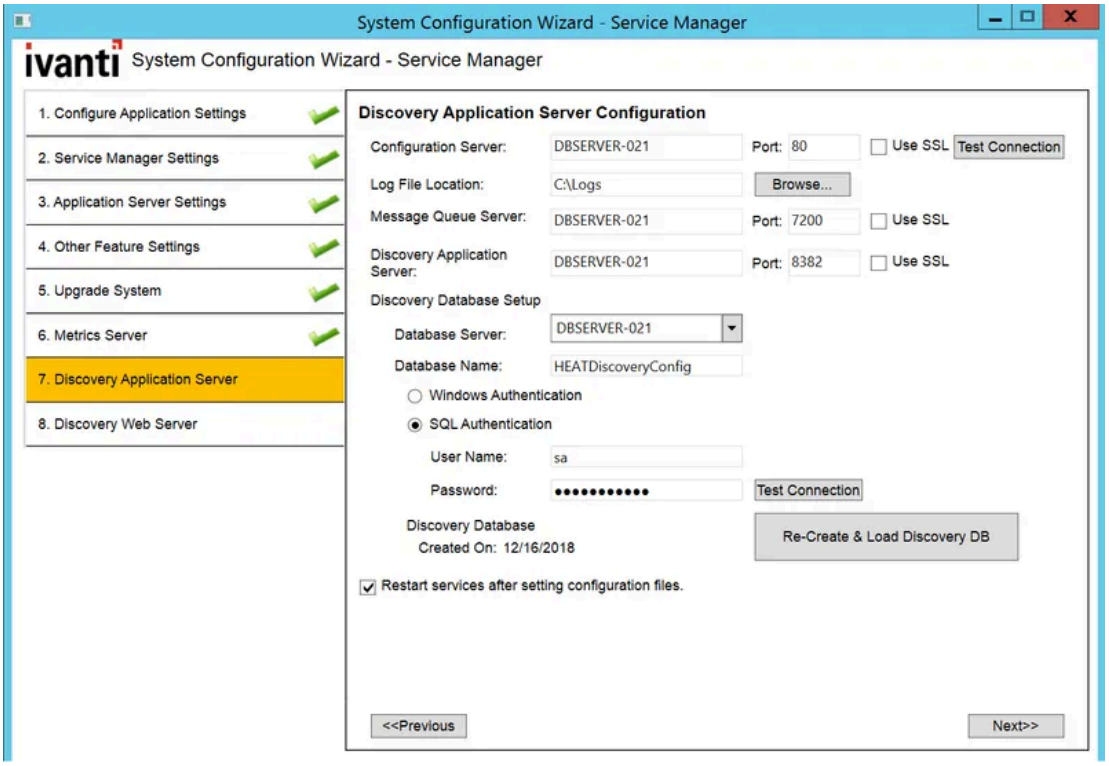
On this page you will specify information about the configuration of the Discovery application server and the Discovery configuration database. Follow these steps:

- Starting the Configuration for the Discovery Application Server
- Configuring a System without a Discovery Configuration Database (Creating a New One)
- Configuring a System with a Discovery Configuration Database (Editing One that Already Exists)

Starting the Configuration for the Discovery Application Server

The first time that you see this page, there is no Discovery configuration database, as shown in Discovery Application Server Page: No Database.

Discovery Application Server Page: No Database



1. Enter values into the fields:

Parameter	Description
Configuration Server	The host name or fully-qualified domain name of the configuration server. The default value is the name of the host that you are logged into now. Do one of the following: • Accept the default value. • Enter the name of the server of the configuration server. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the configuration server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the configuration server.

2. Click Test Connection to test the connection to the configuration server. The system displays a success or failure message. Click OK to close the message. You must have a working connection to the server. You cannot continue with the configuration if this connection does not work.
3. Enter values into the fields:

Parameter	Description
Log File Location	The folder on the server that you are logged into now where the log files are located. The default location for the log files is C:\Logs. Do one of the following: • Accept the default value. • Enter the name of the folder where the log files are located. • Browse for a different folder by clicking Browse.... Select a new folder and click OK.
Message Queue Server	Where the Neurons for ITSM message queue server is located. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name where the Neurons for ITSM message queue server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Neurons for ITSM message queue server. The default is 7200.
Use SSL	Enables SSL encryption to the Neurons for ITSM message queue server.
Discovery Application Server	Where the Discovery application server is located. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name where the Discovery application server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Discovery application server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the Discovery application server.
Discovery Database Setup	
Database Server	The name of the system proposed for the Discovery configuration database. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name of the Discovery configuration database server. • Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click OK.
Database Name	The name of the Discovery configuration database. The default name is HEATDiscoveryConfig and you cannot change the name.

Parameter	Description
Authentication Method	There are two authentication methods for the Discovery configuration database, one for creation and one for access. Select the authentication method for creating the Discovery configuration database: • Windows Authentication: Uses Microsoft Windows authentication. • SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below.
User Name	(Only if you selected SQL Authentication) The user name associated with the Microsoft SQL authentication.
Password	(Only if you selected SQL Authentication) The password associated with the user name for the Microsoft SQL authentication.

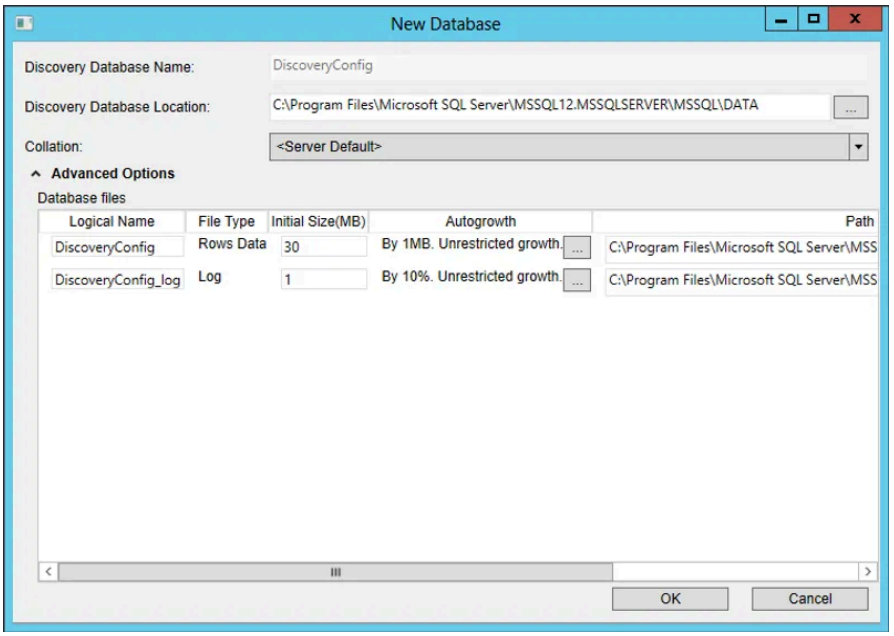
4. Click Test Connection to test the connection to the Discovery configuration database server. The system displays a success or failure message. Click OK to close the message. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
5. Do one of the following:
    - If this is the initial setup, go to **Configuring a System without a Discovery Configuration Database (Creating a New One)**.
    - If your system already has a Discovery configuration database, go to **Configuring a System with a Discovery Configuration Database (Editing One that Already Exists)**.

Configuring a System without a Discovery Configuration Database (Creating a New One)

An initial installation does not have a Discovery configuration database. The system displays this: "No Discovery (HEATDiscoveryConfig) Database is detected."

Follow these steps to create one.

1. Enter values into the fields:

Parameter	Description
Create & Load Discovery DB	Click to create and load a new Discovery configuration database. The system displays the **New Database** dialog box. *New Database Dialog Box* 
Discovery Database Name	The name of the Discovery configuration database. The default name is HEATDiscoveryConfig and you cannot change the name.
Discovery Database Location	The location for the Discovery configuration database.
Collation	The set of rules that describe how to compare and sort strings, such as the order in which letters are sorted and whether case matters. NOTE: ISM application does not support case sensitive SQL Collation.
Advanced Options	
Logical Name	The logical name of the Discovery configuration database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
File Type	The file type, either database records or database logs. These values are read-only.
Initial Size (MB)	The initial file size, in MB, when creating the Discovery configuration database.
Autogrowth	Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
Path	The location of the file. Click ... to update the location.
File Name	The name of the file.

2. Click OK in the **New Database** dialog box. The system creates the Discovery configuration database.

3. To restart the Neurons for ITSM services after you finish the installation, check Restart services after setting configuration files..
4. Click Next. The system displays the **Discovery Web Server** page.

Configuring a System with a Discovery Configuration Database (Editing One that Already Exists)

If you are upgrading or repairing Neurons for ITSM you already have a Discovery configuration database.

1. To recreate the Discovery configuration database, click Re-Create & Load Discovery DB. The system displays a confirmation message.

> If you have customized the existing Discovery configuration database, specify a different location in the **Discovery Database Location** dialog box. Otherwise, the system overwrites your customization when you recreate the database.

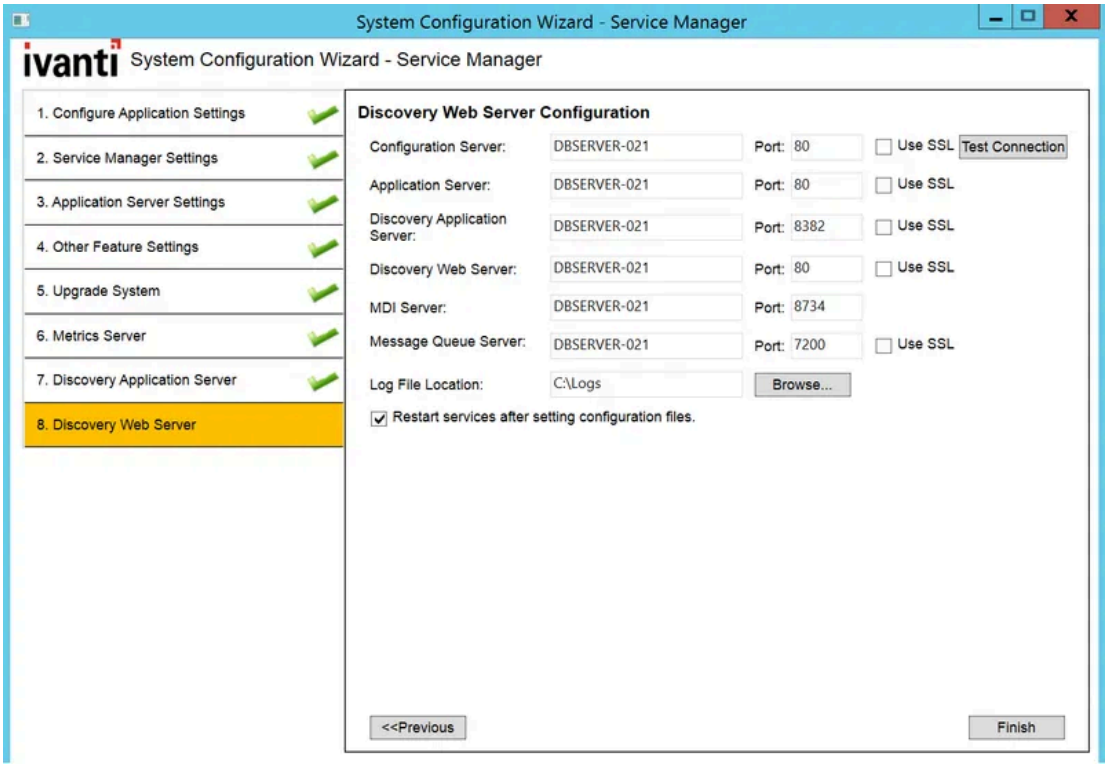
2. Click OK at the confirmation message.
3. To restart the Neurons for ITSM services after you finish the installation, check Restart services after setting configuration files..
4. Click Next. The system displays the **Discovery Web Server** page.

3.4.2.7. Configuring the Discovery Web Server

Configure the relationship between Neurons for ITSM, the Discovery web server, and the Discovery application server from the **Discovery Web Server** page of the System Configuration Wizard.

The system displays the **Discovery Web Server** page. See Discovery Web Server Page.

Discovery Web Server Page



1. Enter values into the fields:

Parameter	Description
Configuration Server	The host name or fully-qualified domain name of the configuration server. The default value is the name of the host that you are logged into now. Do one of the following: • Accept the default value. • Enter the name of the server of the configuration server. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the configuration server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the configuration server.

2. Click Test Connection to verify the connection to the configuration server.
3. Enter values into the fields:

Parameter	Description
Application Server	Where the application server is located. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name where the application server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the application server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the application server.
Discovery Application Server	Where the Discovery application server is located. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name where the Discovery application server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Discovery application server. The default is 8382, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the Discovery application server.
Discovery Web Server	Where the Discovery web server is located. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name where the Discovery web server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Discovery web server. The default is 80, or 443 if you check Use SSL.
Use SSL	Enables SSL encryption to the Discovery web server.
MDI Server	Where the MDI server is located. (The Mobile Device Inventory [MDI] service is bundled with Discovery.) The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name where the MDI server is located.
Port	The port number of the MDI server. The default is 8734.
Message Queue Server	Where the message queue server is located. The default value is the server that you are logged into now. Do one of the following: • Accept the default value. • Enter the name where the Neurons for ITSM message queue server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Neurons for ITSM message queue server. The default is 7200.
Use SSL	Enables SSL encryption to the Neurons for ITSM message queue server.

Parameter	Description
Log File Location	The folder on the server that you are logged into now where the log files are located. The default location for the log files is C:\Logs on the Discovery web server. Do one of the following: • Accept the default value. • Enter the name of the folder where the log files are located. • Browse for a different folder by clicking Browse.... Select a new folder and click OK.

4. To restart the Neurons for ITSM services after you exit the System Configuration Wizard, check Restart services after setting configuration files.
5. Verify that the Neurons for ITSM services restart after the wizard closes.
6. If you did not check Restart services after setting configuration files, restart the Neurons for ITSM services manually.

3.4.2.8. Finishing the System Configuration

When you have finished configuring the ISM Discovery web server, do the following:

1. Click Finish. The System Configuration Wizard closes and the system displays the **Completed** page of the install wizard.
2. Click Finish.
3. Restart the host server that you just configured.
4. Verify that you can access Neurons for ITSM by navigating to http://*server_name*/HEAT.

3.4.3. Configuring the Reporting Feature

If your Neurons for ITSM deployment includes the reporting feature, you need to set up authentication. Authentication is only needed for the reporting feature, and not for deployments that do not use the reporting feature.

- Authenticating the Application Database
- Configuring Microsoft SSRS
- Configuring the Reporting Feature

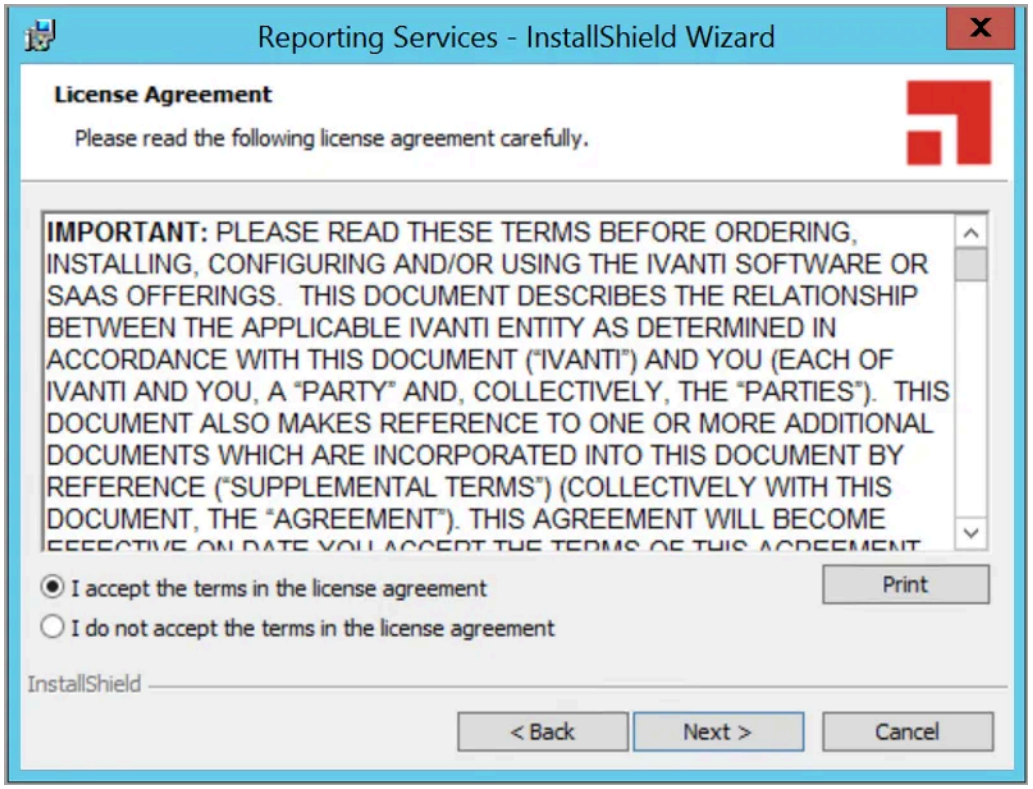
Authenticating the Application Database

The wizard walks you through the first-time set up and configuration as shown in the screenshots below.

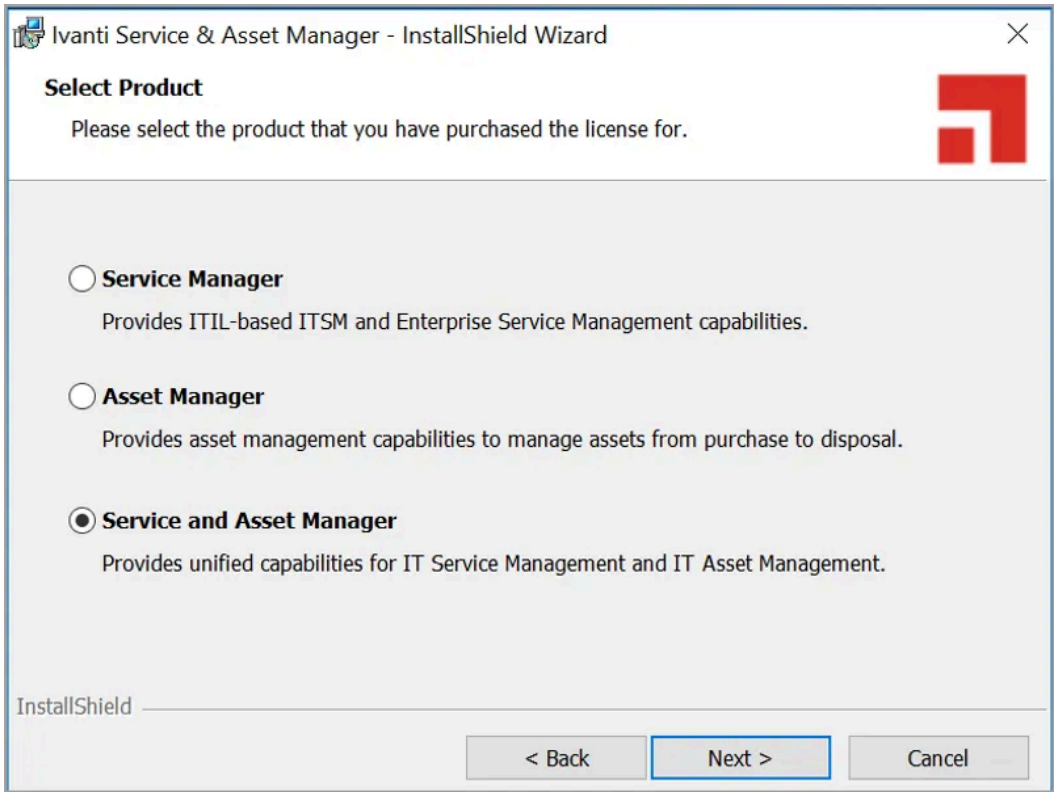
1. Click **Next**.



2. Click **Next** to continue the installation process.

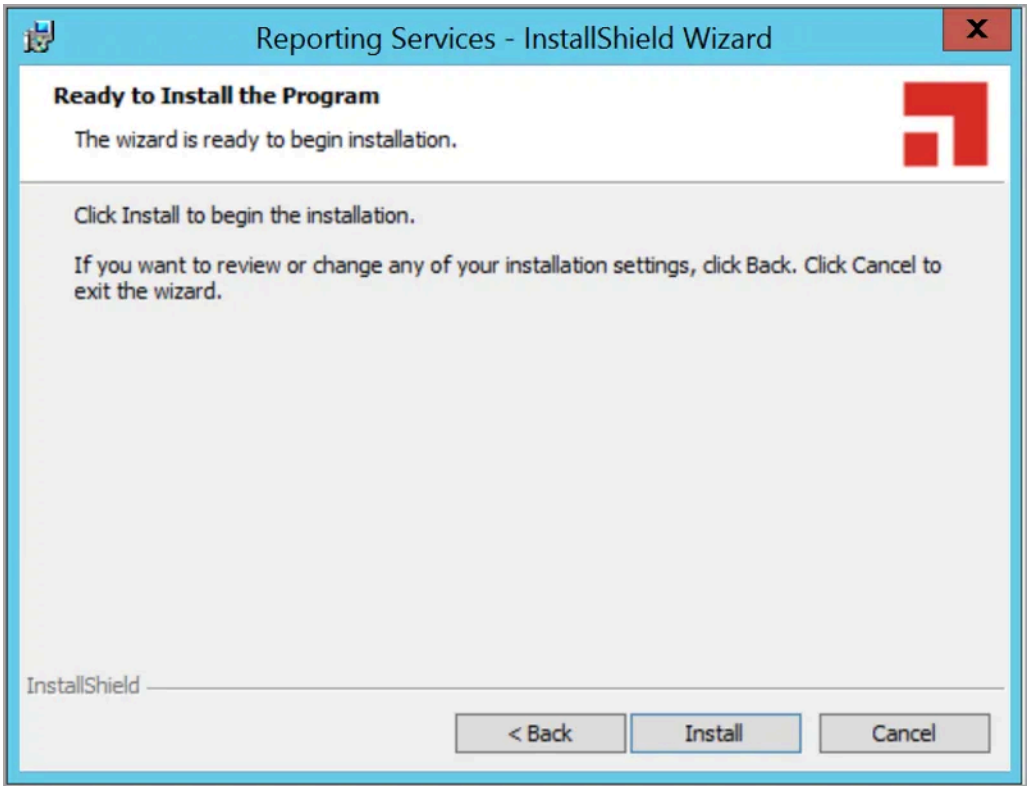


2. Select one of the options, **Service Manager**, **Asset Manager**, or **Service and Asset Manager**.



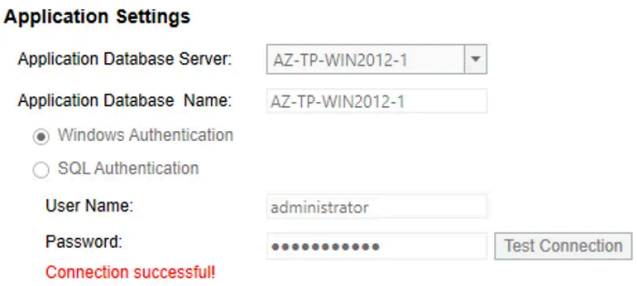
For more information on Asset Manager, access the following URL:
https://help.ivanti.com/docs/help/en_US/IAM/2018/LandingPage.htm

2. Click **Next**.



When you configure Neurons for ITSM, you set the authentication for the application database on the Neurons for ITSM **Application** page of the System Configuration Wizard, as shown in Ivanti Service Manager Application Settings.

Ivanti Service Manager Application Settings



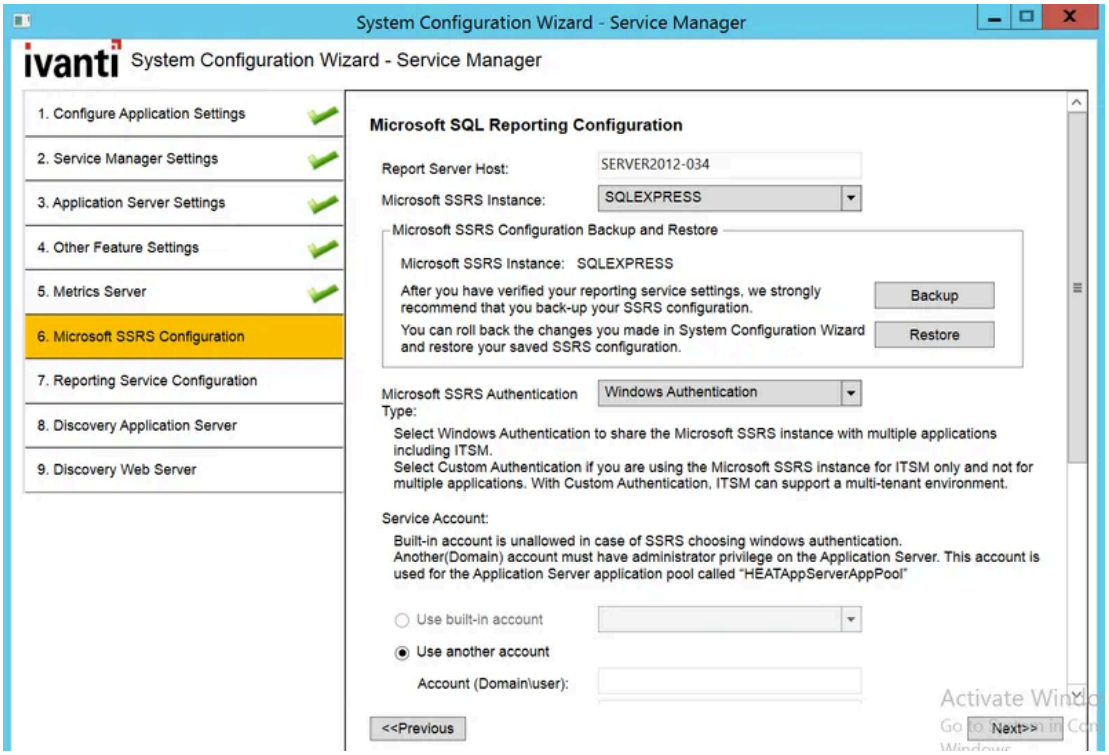
You can select either Windows Authentication or SQL Authentication. (When you configure the reporting feature, you have an opportunity to review and change the authentication method, if necessary, on the **Microsoft SSRS Configuration** page. See Configuring the Reporting Feature.)

- If you select Windows Authentication, you can use the Microsoft SSRS service account, the Microsoft IIS app pool identity account, or any other account, but they must have permission to access the application database and the Microsoft SSRS database.
- If you select SQL Authentication, you can use a different system account.

We recommend having separate authentication for Microsoft SSRS, the application database, and the Microsoft SSRS database.

Configuring Microsoft SSRS

Microsoft SSRS Configuration Page

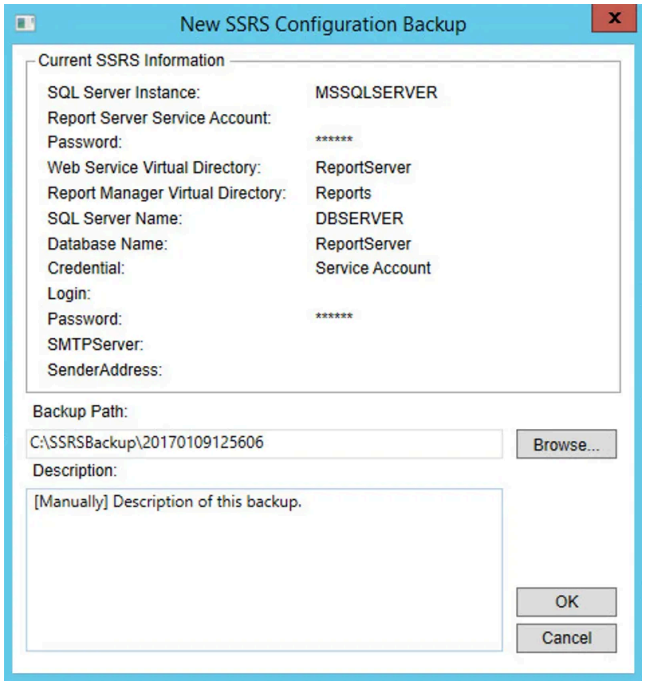


1. Enter values into the fields:

Parameter	Description
Report Server Host	The name of the Neurons for ITSM reporting feature server. The default name is the name of the server that you are currently logged into. You cannot change this value.
Microsoft SSRS Instance	The instance of Microsoft SSRS to use for the Reporting feature. Select a value from the dropdown list.

2. (Recommended) Click Backup to back up your Microsoft SSRS configuration. (If prompted, enter a password to unlock the backup file, and then click OK.) The system displays the **New SSRS Configuration Backup** dialog box with information about the backup.

   New SSRS Configuration Backup Dialog Box



3. To change the location of the backup, click Browse..., select a new location, and click OK.
4. Click OK to close the dialog box. The system displays the **Backup Encryption Key** dialog box. (If you do not see this dialog box immediately, the system displays it after you click Next at the bottom of the page when you are done with the configuration on this page of the System Configuration Wizard.)
5. Do the following:
    - (Optional) Enter a new file location.
    - Enter a password.
    - Confirm the password.
    - Click OK.
6. Select a Microsoft SSRS authentication type:
    - Windows Authentication: Shares the Microsoft SSRS instance with multiple applications, including Neurons for ITSM.
    - Custom Authentication: Does not share the Microsoft SSRS instance with any other applications. The Microsoft SSRS instance is used for Neurons for ITSM only. With custom authentication, you can have a multi-tenant environment.

If you have multiple instances of Microsoft SSRS, choose each instance carefully before choosing the authentication method to use with that instance.

- If you plan to share the same Microsoft SSRS instance with other applications besides the reporting feature, you must use Windows authentication.
- If you plan to create a multiple-tenant environment, you must use custom authentication.
- If you plan to use a dedicated Microsoft SSRS instance only for the reporting feature, you can use either Microsoft SSRS authentication type.

- If you select a Microsoft SSRS instance and select Custom Authentication, the System Configuration Wizard overwrites the existing Microsoft SSRS configuration.
- If the Microsoft SSRS instance that you selected is shared with another application, the Neurons for ITSM installer deletes the configuration for that application. Before proceeding, ensure that the Microsoft SSRS instance is not in use by another application.

7. Enter values into the fields:

Parameter	Description
Service Account	Select the service account to use. This can be the same account that is used for the IIS application pool identity and the Windows service, that you entered on the **Application Server Settings** page. You can select one of the following: • Use built-in account (NOTE: You cannot select this option if you selected Windows Authentication for the Microsoft SSRS authentication type in step 5.) • Use another account
Use built-in account	(Only if you selected Use built-in account) Select the built-in account to use. This can be the same account that is used for the IIS application pool identity and the Windows service, that you entered on the **Application Server Settings** page. You can select one of the following: • Local System: This account has the most permissions. • Network Service: We recommend that you use this account. • Local Service
Account	(Only if you selected Use another account) The name of the service account. Use the format domain/name.
Password	(Only if you selected Use another account) The password associated with the service account.
Web Service Virtual Directory	The name of the web service virtual directory. The system automatically fills in this field with the value that you entered in the **Web Service Virtual Directory** field on the **Application Server Settings** page. See **Configuring the Application Server Settings**. The default value for the web service virtual directory is ReportServer *+ _SSRS_instance_name*. Do one of the following: • Accept the default value. • Enter a new value. Click Advanced... to configure multiple identities for the reporting feature web service.
Report Manager Virtual Directory	The name of the report manager virtual directory. The default value is Reports *+ _SSRS_instance_name*. Do one of the following: • Accept the default value. • Enter a new value. Click Advanced... to configure multiple identities for the report manager.
Database Server	The name of the database server. The system automatically displays the default Microsoft SQL server name. Do one of the following: • Accept the default value. • Enter the name of the server of the configuration database in this format: machinename\instance. • Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click OK.

Parameter	Description
	NOTES: • Do not choose localhost unless you are setting up a **Demonstration or Proof-of-Concept Deployment**. • To restore the Microsoft SQL server name if you changed the name previously, open Microsoft SQL Server Management Studio. The system displays the Microsoft SQL server name in the **Connect to Server** dialog box.
Database Name	The name of the reporting database. The default name is ReportServer + *$SSRS instance name*.
Credentials	The credentials to use with the reporting feature. Select one of the following: • SQL Server Credentials • Windows Credentials • Service Credentials
User Name	The user name for the credential used with the reporting feature.
Password	The password associated with the credential used with the reporting feature.

> We recommend creating passwords using Alphanumeric characters. Special characters are not permitted.

8. Click Test Connection. The system displays *Connection successful!* if the connection is good.
9. Enter values into the fields:

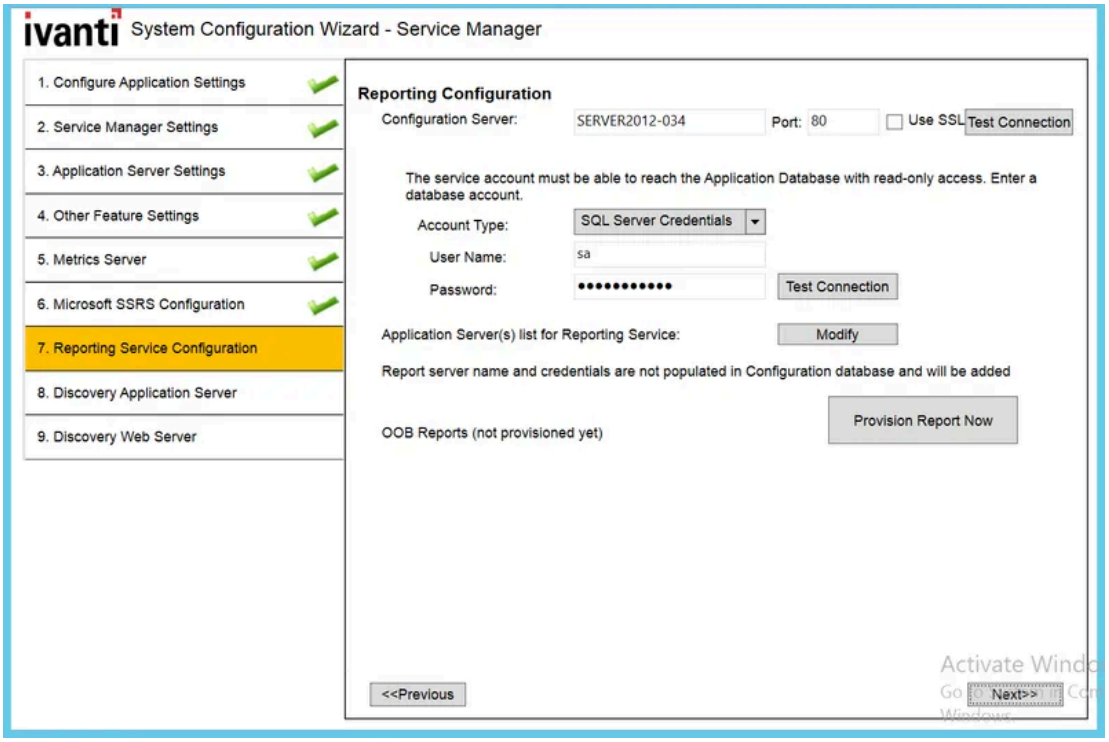
Parameter	Description
SMTP Server	The server that sends out the reports. The system automatically verifies the SMTP server name that you enter. If the name is not valid, the system displays an error message.
Sender Address	The email address for the account that sends out the reports.

10. Click Next. The system displays the **Ivanti Reporting Service Configuration** page. See **Configuring the Reporting Feature**. (If the system displays the Backup Encryption Key dialog box, see step 5.)

Configuring the Reporting Feature

You configure the reporting feature on the**Reporting Service Configuration** page. See **Reporting Service Configuration Page**.

Reporting Service Configuration Page



1. Enter values into the fields:

Parameter	Description
Configuration Server	The host name of the configuration server. The default value is the name of the server that you are logged into now. If the host that you are logged into now is *not* the configuration server, enter the machine name or fully-qualified domain name of your configuration server. If you check Use SSL below, you must enter the fully-qualified domain name of the configuration server.
Port	The port number of the configuration server. The default is 80, or 443 if you check Use SSL.
Use SSL	Check to use SSL for connections to the configuration server. NOTE: We do not recommend enabling SSL on the configuration server until you have fully tested Neurons for ITSM to ensure that it works with SSL. For information on configuring Neurons for ITSM with SSL, see **Optional SSL Configuration**.

2. Click Test Connection to test the connection to the configuration server. The system displays a success or failure message. Click OK to close the message.
3. Enter values into the fields:

Parameter	Description
Account Type	The database account type. Select from one of the following: • SQL Server Credentials • Windows Credentials NOTE: If you selected Custom Authentication in step 6 of **Configuring Microsoft SSRS**, this option automatically displays as SQL Server Credentials and you cannot change it.
User Name	The user name for the Neurons for ITSM database read-only account.
Password	The password associated with the user name.

4. Click Test Connection to test the connection to the configuration server. The system displays *Connection successful!* if the connection is good.
5. Click Modify to add servers to or remove servers from the list of Neurons for ITSM application servers that are used with the reporting feature.

> If you have multiple domains in your deployment, the reporting server may not be able to connect to the web server. In this case, remove the server from the list and configure reporting manually.

6. Enter values into the fields:

Parameter	Description
Report User Name	(Only if you selected Custom Authentication in step 6 of **Configuring Microsoft SSRS**) The user name for the user who configures the reporting feature.
Report User Password	(Only if you selected Custom Authentication in step 6 of **Configuring Microsoft SSRS**) The password associated with the user name.

7. To verify that the configuration settings work, do the following:

   a. Click Reprovision Report Now to update the sample report data to the application. See **Reporting Service Configuration Page**. If the systems returns an exception such as "Cannot Decrypt the Symmetric Key".

   b. Log into Neurons for ITSM as a Report Manager.

   c. Ensure that you can see the sample reports and create one.

8. When you see confirmation that the out-of-the-box reports have been provisioned, that is, the last line of this step changes from *OOB Reports (not provisioned yet)* to *OOB Reports (provisioned on date)*, click Finish to close the System Configuration Wizard.

The system displays the **Completed** page of the System Configuration Wizard.

> If the system displays an error message that the system failed to configure reporting for an Neurons for ITSM application server, ensure that you checked Use these settings for Reporting Service on the **Application Server Settings** page.

9. Restart your system (the host server that you just configured).

10. After the system restarts, ensure that you can access Neurons for ITSM. Go to http://*server_name*/HEAT and ensure that the reporting feature is functional.

3.4.4. Configuring Discovery

This topic describes how to configure Discovery.

- Configuring Discovery on a Dedicated Server
- Configuring Discovery on the Production Servers

Configuring Discovery on a Dedicated Server

After you have installed the Discovery components, the System Configuration Wizard automatically starts and displays the **Configuration Application** page.

1. On the **Configuration Application** page, do the following:

   a. Under **Target Environment**, choose Single Server Deployment.

   b. Under **Setup Connection**, verify that the configuration matches the settings that you configured for the Neurons for ITSM production servers. See Configuring the Configuration Database.

   c. Click Next.

2. On the **Service Manager Application** page, do the following:

   a. Verify that the configuration matches the settings that you configured for the Neurons for ITSM production servers. See Configuring the Neurons for ITSM Application.

   b. Check Discovery Stand alone.

   c. Click Next.

3. On the **Application Server Settings** page, do the following:

   a. Verify that the configuration matches the settings that you configured for the Neurons for ITSM production servers.

   b. Click Next.

4. On the **Other Features Settings** page, do the following:

   a. Under **Customize Server**, in the **Discovery Application Server** field, enter the name of the Discovery dedicated server.

      - If you are not using SSL, enter the host name.
      - If you are using SSL, enter the fully-qualified domain name.

   b. Verify that the rest of the configuration matches the settings that you configured for the Neurons for ITSM production servers. See Configuring Other Feature Settings.

   c. Click Next.

5. On the **Metrics Server** page, do the following:

   a. Verify that the configuration matches the settings that you configured for the Neurons for ITSM production servers. See Configuring the Metrics Server.

   b. Click Next.

6. On the **Discovery Application Server** page, do the following:

a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.

- If you are not using SSL, enter the host name.
- If you are using SSL, enter the fully-qualified domain name.

b. Verify that the rest of the configuration matches the settings that you configured for the Neurons for ITSM production servers. See **Configuring the Discovery Application Server**.

c. Click Next.

7. On the **Discovery Web Server** page, do the following:

a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.

- If you are not using SSL, enter the host name.
- If you are using SSL, enter the fully-qualified domain name.

b. Verify that the rest of the configuration matches the settings that you configured for the Neurons for ITSM production servers. See **Configuring the Discovery Web Server**.

c. Click Finish.

The system displays the **Completed** page of the System Configuration Wizard.

8. Restart your system (the host server you just configured).
9. After the system restarts, ensure that you can access Neurons for ITSM. Go to http://*server_name*/HEAT and ensure that the system is functional.

Configuring Discovery on the Production Servers

Now that there is a dedicated Discovery server in your deployment, you must configure your production servers to recognize it.

On each production server in your deployment, do the following:

1. Go to the Windows apps menu and click System Configuration Wizard. The system opens the System Configuration Wizard and displays the **Configuration Application** page.
2. On the **Configuration Application** page, click Next.
3. On the Neurons for ITSM application page, click Next.
4. On the **Application Server Settings** page, click Next.
5. On the **Other Features Settings** page, do the following:

a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.

- If you are not using SSL, enter the host name.
- If you are using SSL, enter the fully-qualified domain name.

b. Click Next.

6. On the **Metrics Server** page, click Next.
7. On the **Discovery Application Server** page, do the following:

a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.

- If you are not using SSL, enter the host name.

- If you are using SSL, enter the fully-qualified domain name.

b. Click Next.

8. On the the **Discovery Web Server** page:

a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.

- If you are not using SSL, enter the host name.
- If you are using SSL, enter the fully-qualified domain name.

b. Click Finish.

3.4.5. Configuring the Deployment on the Neurons for ITSM Operations Console

- Configuring the Neurons for ITSM Operations Console
- Creating the Staging and UAT Instances of the Tenants
- Making Configuration Changes to Tenants

Perform these steps from the Operations Console, which you installed in the staging/UAT environment.

> This section only contains brief, high-level instructions.
>
> For complete information about using the Operations Console, including how to log in, see the *Operations Console User Guide for* Neurons for ITSM.

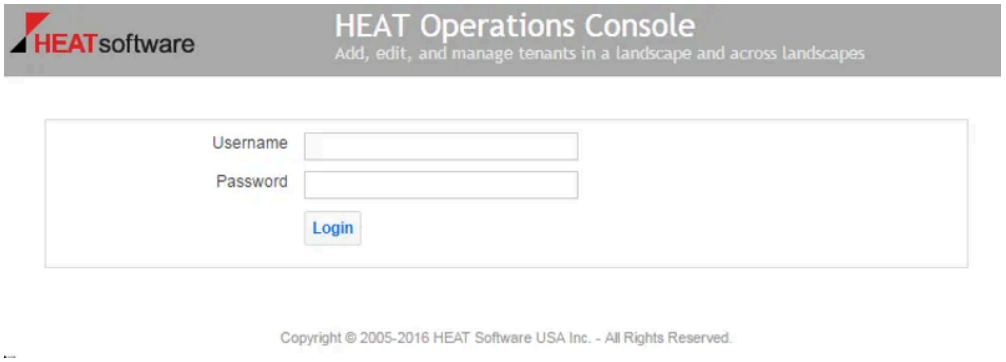
Configuring the Neurons for ITSM Operations Console

To log into the Operations Consoles, do the following:

1. In the **Start** menu, click the down arrow to see the **Apps** menu, and then click HEAT Operations Console.
2. Enter your user name and password and then click Login.

   > The default user name is admin and the default password is manage.

   Operations Console Log In Screen

3. Use the Operations Console to update the values for the Neurons for ITSM application database by doing the following:

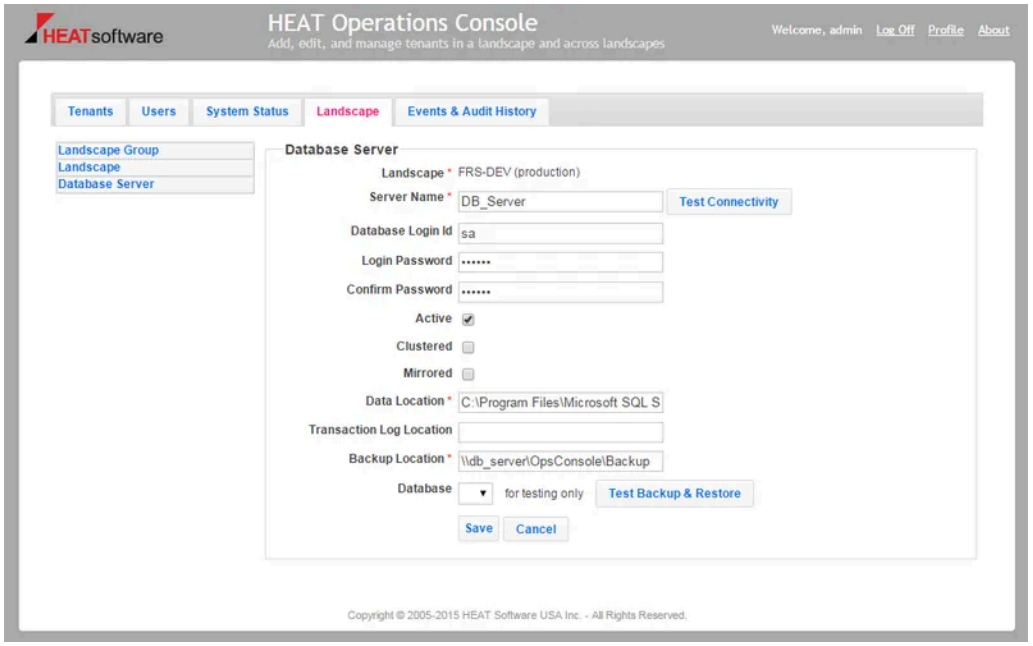
   a. Click the **Landscape** tab.

   b. Click Database Server on the left.

   c. Click Add Database Server.

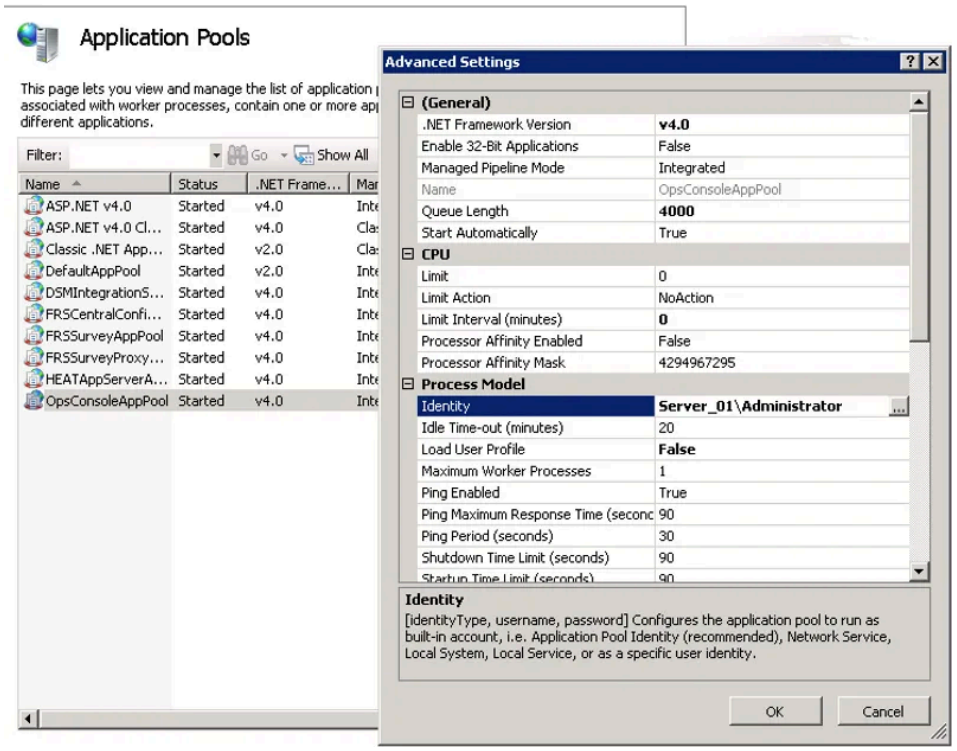
   d. Enter a database login ID and password and set the data and backup locations. See the example values in Adding a Database Server.

   Adding a Database Server



e. For the data and backup locations, change the application pool identity so that it has read access. See **Changing the Application Pool Identity**.

Changing the Application Pool Identity



See the *Working with Database Servers* section of the *Operations Console User Guide for* Neurons for ITSM for complete details about editing a database server.

4. Delete the Neurons for ITSM application databases on the staging and UAT instances of the tenant, by doing the following:

   a. Click the **Tenants** tab.

b. Click Expanded View to view all the details about the tenants.

c. Find the staging instance of the tenant and click Deactivate.

d. Click Deactivate at the confirmation prompt.

e. For the staging instance of the tenant, click Delete.

f. Check Skip Backup and click Delete at the confirmation prompt.

g. Repeat steps c. through f. for the UAT instance of the tenant.

You now have three instances of the configuration database and a production instance of the tenant.

See the *Editing a Tenant* section of the *Operations Console User Guide for* Neurons for ITSM for complete details about deleting tenants and tenant instances.

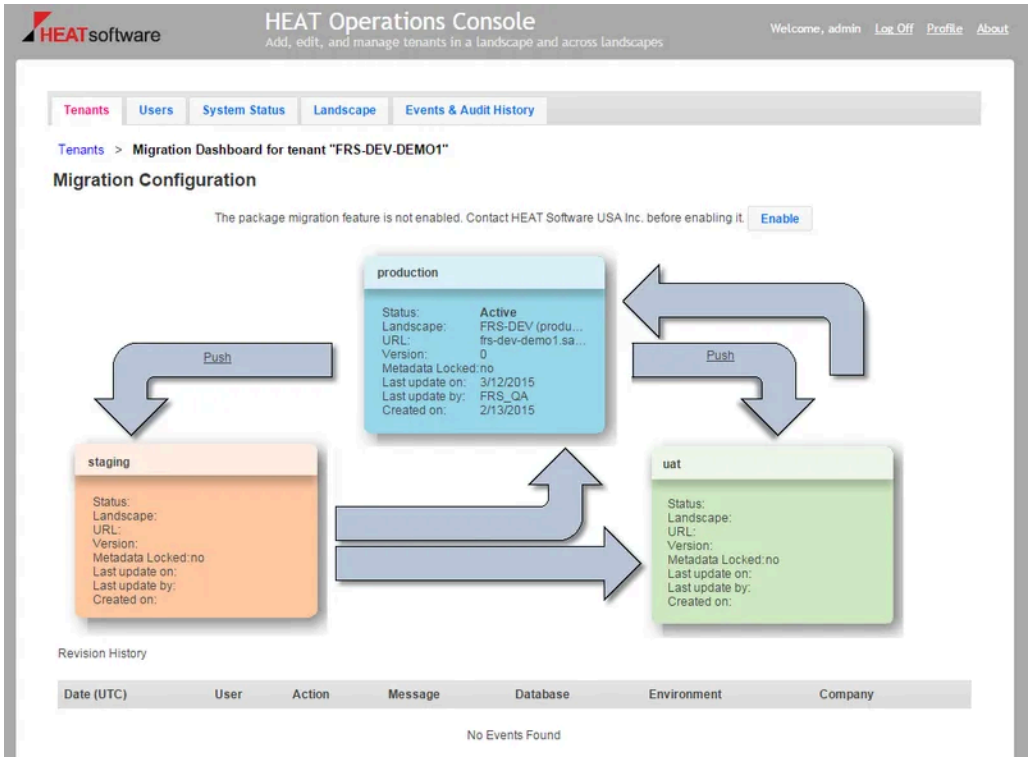
Creating the Staging and UAT Instances of the Tenants

To create the staging and UAT instances of the tenant, based on the production instance, do the following:

1. Log into the Operations Console.
2. Click the **Tenants** tab.
3. Navigate to the production instance of the tenant and click Manage Migration.
4. Create the staging instance of the tenant, by doing the following:

   a. In the migration dashboard, click Push which is located inside the arrow going from the production instance of the tenant to the staging instance of the tenant. See Creating a Staging Instance of the Tenant.

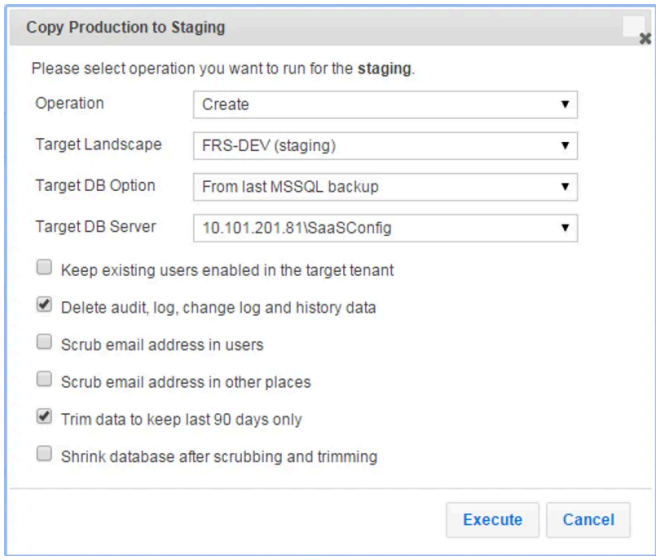
   Creating a Staging Instance of the Tenant



The system displays the **Copy Production to Staging** dialog box.

b. In the **Target DB Option** field, select From live MSSQL backup. See Copy Production Instance of the Tenant to the Staging Instance of the Tenant.

Copy Production Instance of the Tenant to the Staging Instance of the Tenant



c. Click Execute.

5. Create the UAT instance of the tenant:

a. In the migration dashboard, click Push which is located inside the arrow going from the production instance of the tenant to the UAT instance of the tenant. See Creating a Staging Instance of the Tenant. The system displays the **Copy Production to UAT** dialog box.

b. In the **Target DB Option** field, select From live MSSQL backup. See Copy Production Instance of the Tenant to the Staging Instance of the Tenant.

c. Click Execute.

You can now customize Neurons for ITSM and use the Operations Console to push those customizations to the other instances of the tenant.

Making Configuration Changes to Tenants

1. Log into the Operations Console.
2. Click the **Tenants** tab.
3. Make configuration changes in the staging instance of the tenant.
4. Push the configuration changes that you made in the staging instance of the tenant to the UAT instance of the tenant by doing the following:

a. Click Push which is located inside the arrow going from the staging instance of the tenant to the UAT instance of the tenant. See Creating a Staging Instance of the Tenant. The system displays the **Copy Staging to UAT** dialog box.

b. You can use simple mode by leaving Advanced Mode unchecked, or you can use advanced mode by checking Advanced Mode. If you use advanced mode, select Copy Configuration in the **Operation** field and check your options. See Copy

Production Instance of the Tenant to the Staging Instance of the Tenant.

c. Click Execute.

5. Verify that the configuration changes that you made to the staging instance of the tenant (in step 3) were successfully migrated to the UAT instance of the tenant.
6. Make additional configuration changes in the staging instance of the tenant as needed.
7. After you have finished making configuration changes and have verified them, push the configuration changes from the UAT instance of the tenant to the production instance of the tenant.

3.4.6. Optional SSL Configuration

> The Metrics Server is not compatible with SSL if your Neurons for ITSM system has Windows authentication set up.

You can configure Neurons for ITSM for SSL. This configuration is optional. There are three scenarios:

- The Neurons for ITSM application database and the configuration database both use SSL. See **Configuring SSL for the Configuration and Application Databases**.
- The Neurons for ITSM application database uses SSL but the configuration database does not use SSL. See **Configuring SSL for the Application Database Only**.
- Neither the Neurons for ITSM application database nor the configuration database uses SSL. In this scenario, do not check SSL on any of the pages of the System Configuration Wizard.

> For all fields in the System Configuration Wizard that ask for a server location, when using SSL, you must enter a fully-qualified domain name (FQDN). This is because SSL needs a certificate and the certificate authority requires an FQDN.

Configuring SSL for the Configuration and Application Databases

To configure both your Neurons for ITSM application database and the configuration database to use SSL, follow all of the steps in all of these sections:

- **Before You Begin**
- **Configuring SSL in Microsoft IIS Manager**
- **Configuring SSL in the System Configuration Wizard**

Before You Begin

- Ensure that https:\\localhost:443 displays the Microsoft IIS Manager welcome page.
- Ensure that your system has a valid certificate.

Configuring SSL in Microsoft IIS Manager

1. In Microsoft IIS Manager, navigate to Sites > Default Web Site and select SSL Settings.
2. On the **SSL Settings** page, check Require SSL and under client certificates, select Ignore.
3. Navigate to Sites > HEAT and select SSL Settings.
4. On the **SSL Settings** page, check Require SSL and under client certificates, select Ignore.
5. Navigate to Sites > CentralConfig and select SSL Settings.
6. On the **SSL Settings** page, check Require SSL and under client certificates, select Ignore.
7. Navigate to Sites > FRSSurveyProxy and select SSL Settings.
8. On the **SSL Settings** page, check Require SSL and under client certificates, select Ignore.
9. Add an SSL port by doing the following:

   a. Navigate to **Sites > Default Web Site**, right click, and select Edit Bindings....

   b. Click Add....

c. In the **Add Site Binding** dialog box, for the **Type** field, select HTTPS and in the **SSL certificate** field, select the certificate that you received from the certificate authority. The system automatically enters 443 for the port.

d. In the **IP Address** field, enter a fully-qualified domain name.

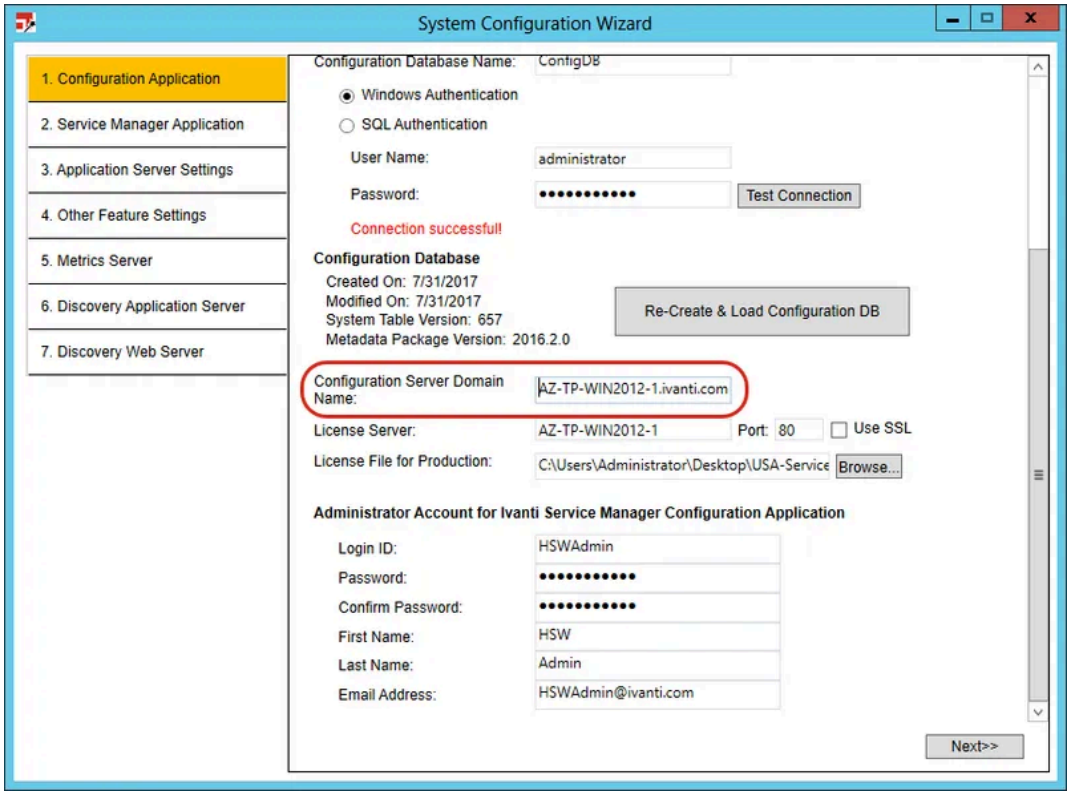
e. Click OK.

10. Verify that you can access https://*fully_qualified_domain_name*.

Configuring SSL in the System Configuration Wizard

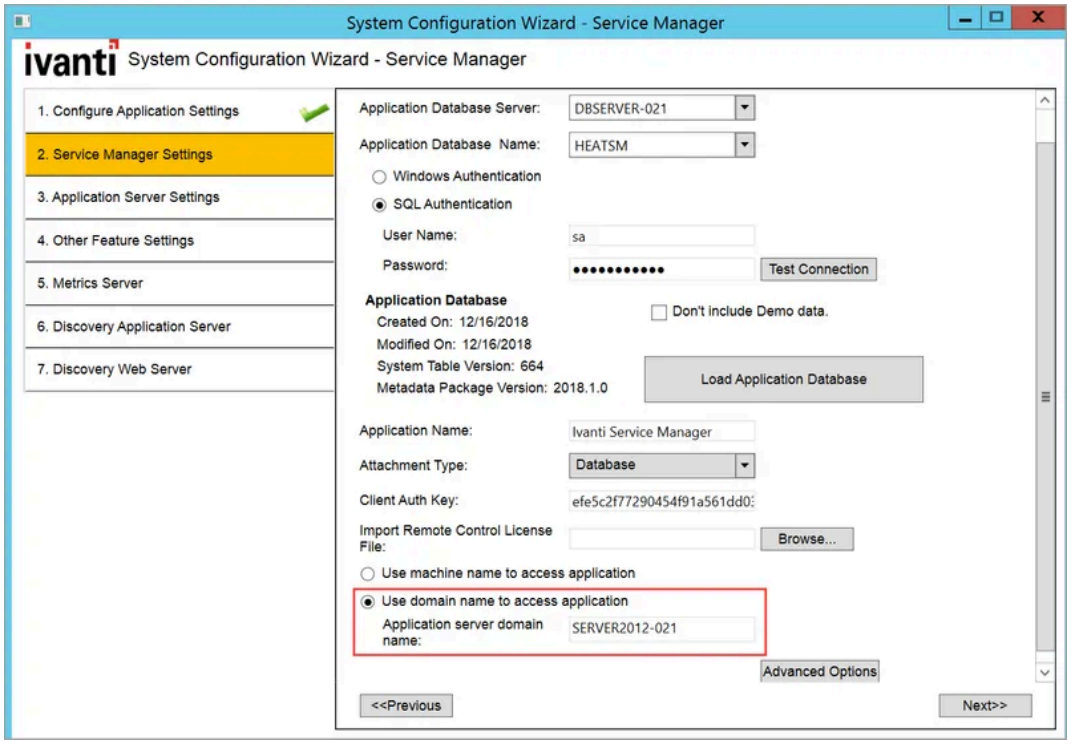
1. In the System Configuration Wizard, on the **Configuration Application** page, ensure that the value in the **Configuration Server Domain Name** field uses a fully-qualified domain name. Do not use a machine name.

   Configuration Application Page



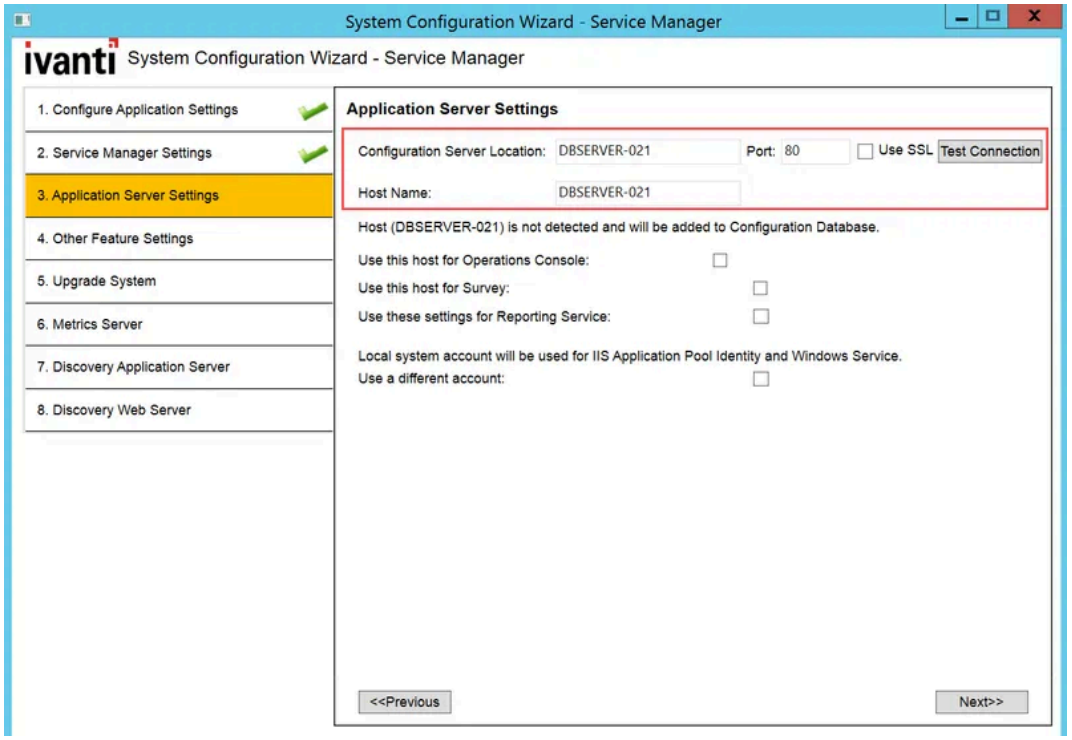
2. On the bottom of the Neurons for ITSM **Application** page, ensure that you check Use domain name to access Application and enter a fully-qualified domain name for the Neurons for ITSM application server. Do not use a machine name.

   Neurons for ITSM *Application Page*



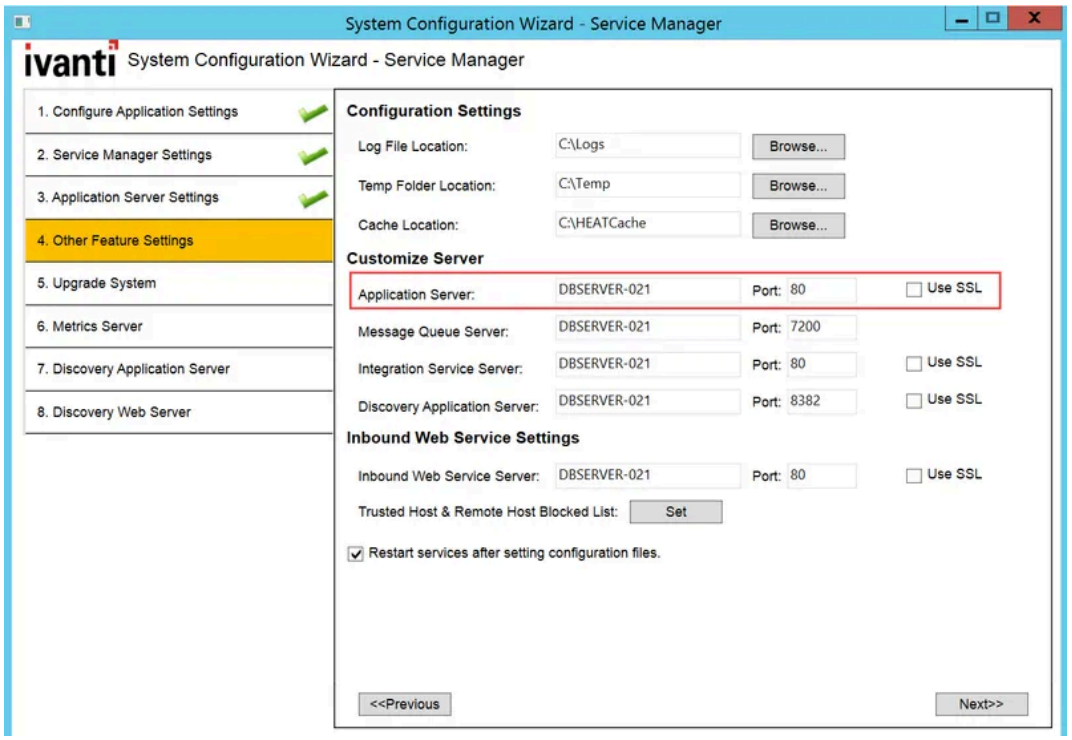
3. On the **Application Server Settings** page, do the following:
   - Ensure that you enter the fully-qualified domain name in the **Configuration Server Location** field.
   - Check Use SSL.
   - Enter the fully-qualified domain name in the **Host Name** field.

Application Server Settings Page.



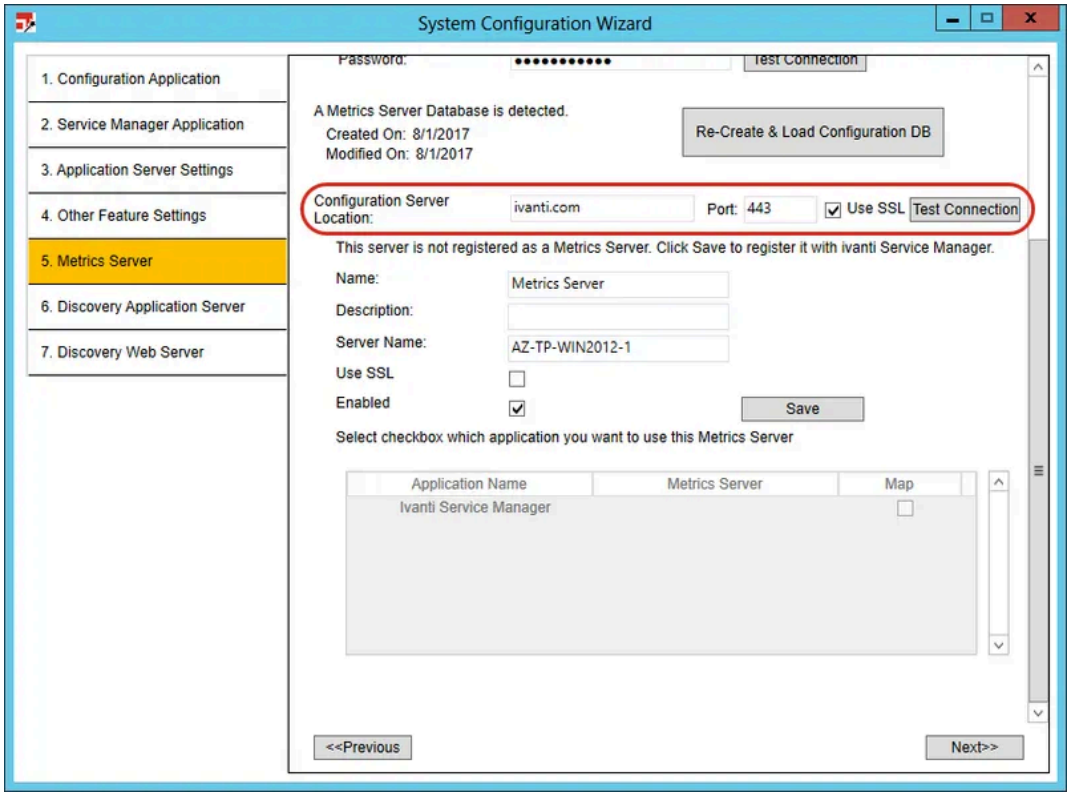
4. On the **Other Feature Settings** page, for the Neurons for ITSM application server, check Use SSL.

Other Feature Settings Page



5. On the **Metrics Server** page, check Use SSL.

Metrics Server Page



Configuring SSL for the Application Database Only

To configure your Neurons for ITSM application database to use SSL but not the configuration database, follow all of the steps in all three sections:

- Before You Begin
- Configuring SSL in Microsoft IIS Manager
- Configuring SSL in the System Configuration Wizard

Before You Begin

- Ensure that https:\\localhost:443 displays the Microsoft IIS Manager welcome page.
- Ensure that your system has a valid certificate.

Configuring SSL in Microsoft IIS Manager

1. In Microsoft IIS Manager, navigate to Sites > Default Web Site and select SSL Settings
2. On the **SSL Settings** page, ensure that Require SSL is not checked. Under client certificates, select Ignore.
3. Navigate to Sites > HEAT and select SSL Settings.
4. On the **SSL Settings** page, check Require SSL and under client certificates, select Ignore.
5. Navigate to Sites > CentralConfig and select SSL Settings.
6. On the **SSL Settings** page, ensure that Require SSL is not checked. Under client certificates, select Ignore.
7. Navigate to Sites > FRSSurveyProxy and select SSL Settings.
8. On the **SSL Settings** page, check Require SSL and under client certificates, select Ignore.
9. Add an **SSL** port by doing the following:

   a. Navigate to **Sites > Default Web Site**, right click, and select Edit Bindings....

   b. Click Add....

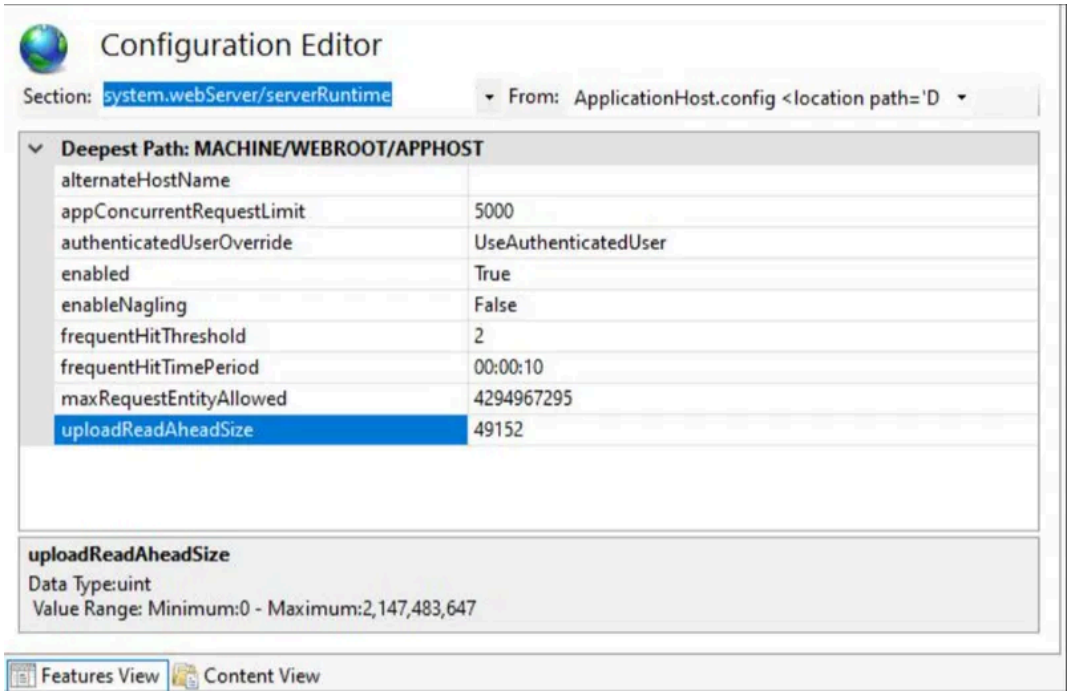
   c. In the **Add Site Binding** dialog box, for the **Type** field, select HTTPS and in the **SSL certificate** field, select the certificate that you received from the certificate authority. The system automatically enters 443 for the port.

   d. In the SSL certificate field, enter a fully-qualified domain name.

   e. Click OK.

10. Double-click **Configuration Editor**.

    The **Configuration Editor** dialog box opens.

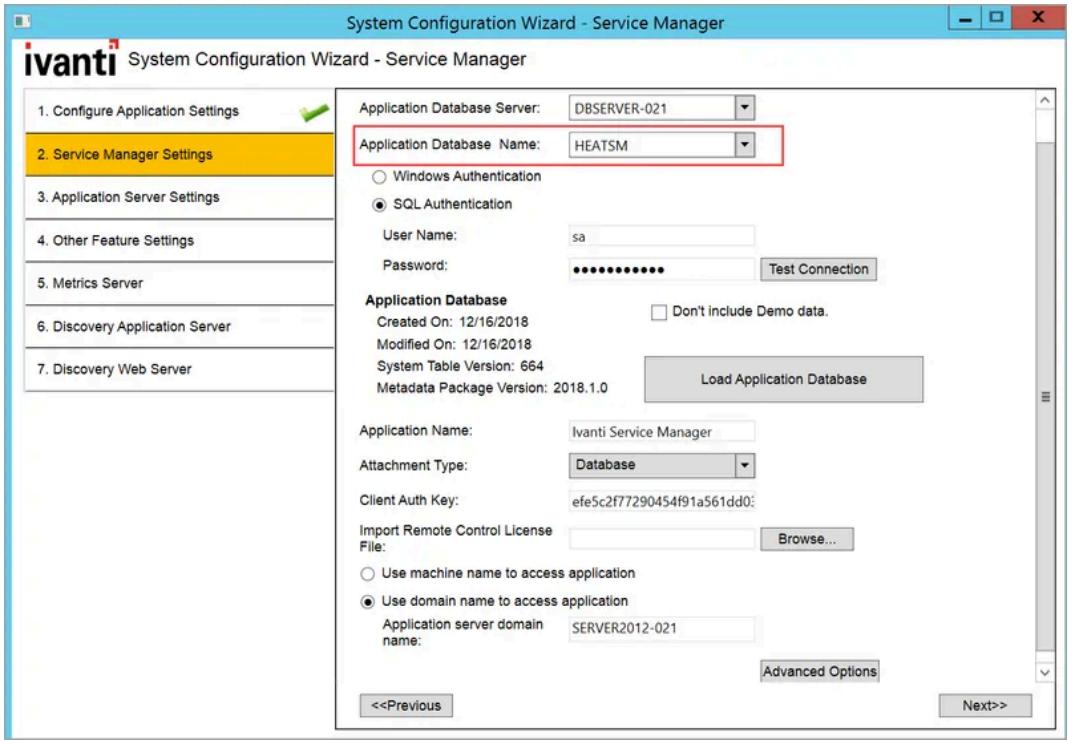


11. Select **System.webServer** and then select **serverRuntime**.
12. Modify the **uploadReadAheadSize** value to `2147483647`.
13. Click **Apply**.
14. Verify if you can access https://*local_host*.

Configuring SSL in the System Configuration Wizard

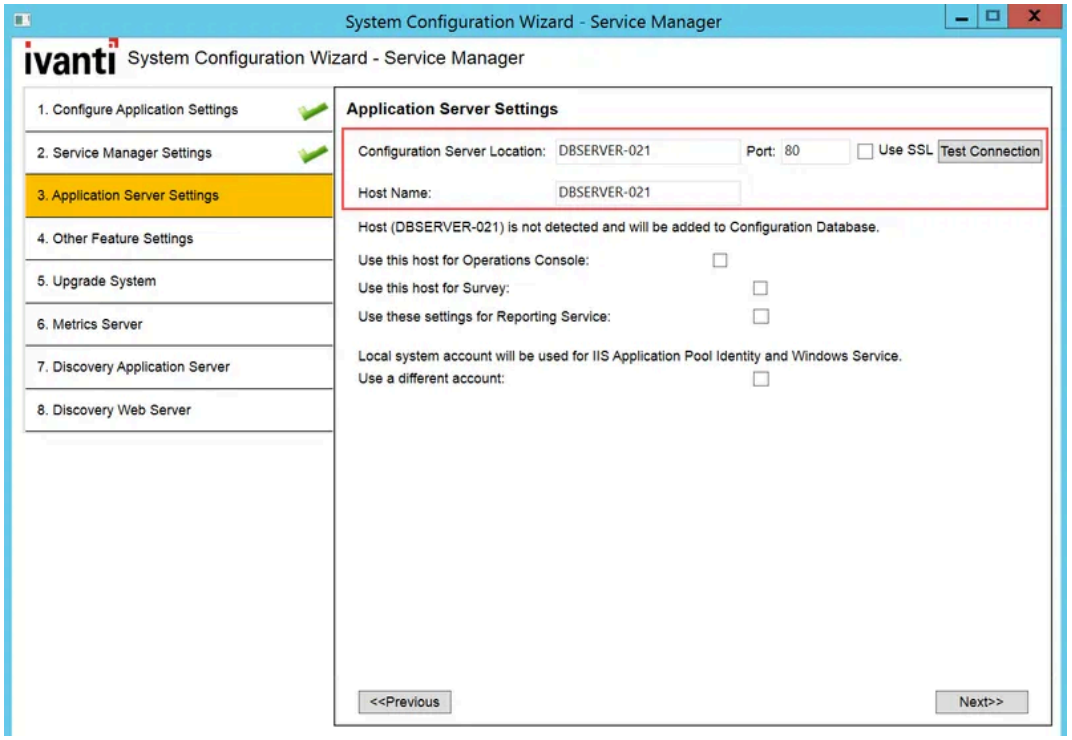
1. In the System Configuration Wizard, on the Neurons for ITSM **Application** page, ensure that the Neurons for ITSM application database uses a fully-qualified domain name and not a machine name.

   Neurons for ITSM *Application Page*



2. On the **Application Server Settings** page, do the following:
   - Ensure that Use SSL is not checked.
   - Ensure that you enter the fully-qualified domain name in the **Configuration Server Location** field.
   - Ensure that you enter the host name, and not the fully-qualified domain name, in the **Host Name** field.

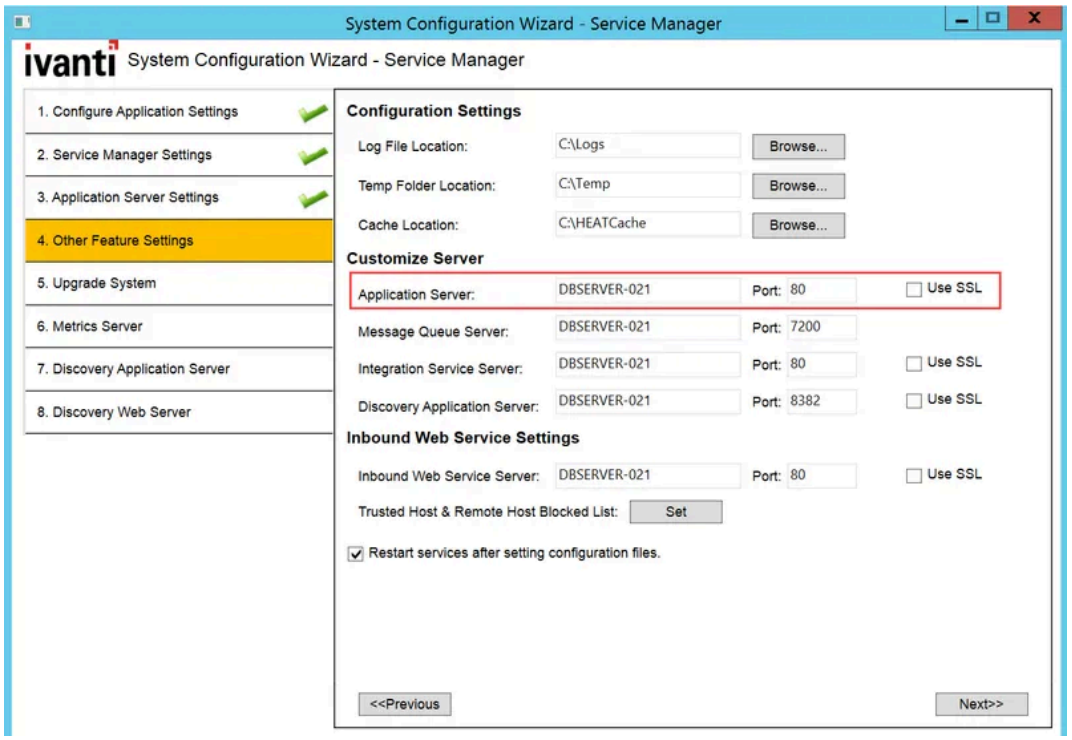
Application Server Settings Page



3. On the **Other Feature Settings** page, check Use SSL.

> This is the *only* place in the System Configuration Wizard where you check Use SSL. Do *not* check Use SSL on any other page.

Other Feature Settings Page



Configuring SSL for Integration Service

Ivanti Integration Service by default configured to work on non-SSL port irrespective of the “SSL” check box is selected in System Config Wizard (SCW).

<That SCW checkbox tells other parts of the product that the integration service is SSL (or not), so it needs to be checked, and the manual edit of the JSON file is also needed.>

1. To make Integration Service work on SSL port, following steps to be performed on each server where Ivanti Integration Service is running.
2. Stop the Ivanti integration service.
3. Add the following entries at the end of appsettings.json of Integration Service.

   The Default Path for Integration Service is “C:\Program Files\HEAT Software\HEAT\IntegrationServer\appsettings.json”

```Bash
,
"Kestrel": {
        "Endpoints": {
            "HttpsInlineCertFile": {
                "Url": "
https://<IntegrationURL>:1213"
,
                "Certificate": {
          "Subject": "<SystemCertificate>",
          "Location": "LocalMachine",
          "AllowInvalid": true
                }
            }
        }
    }
```

The **IntegrationURL** should be replaced with the actual integration URL configured in SCW.
And a trusted certificate is available in your local Computer > Personal certificate store.<Ensure the value in the **appsettingss.json** file is the "Issued To" string.>

Ivanti recommends that there is only one If there is more than one cert here with the same Name, the OS will choose one so it is best practice to ensure only one cert is present with the same name as configured in the json file

SystemCertificate should be replaced with the installed certificate name on server machine where the Integration Service is running.

4. Start the Integration Service.
5. Verify that https://<IntegrationURL>:1213/IntegrationService.svc is the correct URL.

3.4.7. Optional LDAP Configuration

Neurons for ITSM supports LDAP. LDAP is configured from the Configuration Console.

After installation, go to the online help and view the topic called *Configuring LDAP Settings*.

3.4.8. About Configuring with ADFS

Neurons for ITSM supports ADFS. ADFS is configured from the Configuration console.

After installing the system, go to the online help and view the topic called *Working with ADFS/SAML*.

3.4.9. About Configuring Throttling Settings

- About Throttling
- Checking the Throttling Status
- Configuring Outbound Throttling Settings

About Throttling

In Neurons for ITSM, throttling is when the system intentionally slows the speed of web services. We use this process to regulate the network traffic and to minimize bandwidth congestion. When using web services, Neurons for ITSM may limit the message rate, based on overall load. If you exceed the rate of 100,000 API calls per day, you may find your responses slowed to an appropriate rate. This helps ensure that you get a fair share of resources, and Ivanti Software can prevent unintended performance degradation from runaway integrations and denial of service attempts.

For more information about using the Neurons for ITSM integration web services, go to the online help and view the topic called *Working with the Integration Web Service*.

Checking the Throttling Status

Configuring Outbound Throttling Settings

In on-premise implementations, your web service use only affects your environment. If you exceed the recommended rate, you may see performance implications. You can adjust your outbound throttling thresholds to maximize performance. The hardware capacity of your system also affects the values that you set these parameters to.

The following are the outbound throttling parameters:

Parameter	Description
ResetRuntimeCache ExpectedTimeout	The amount of time, in ms, that the system allocates to reset the runtime cache operation. If it takes longer than this, the system moves the operation to the pending actions and marks the server as unhealthy.
ResetRuntimeCache UnhealthyDelayTime	If the server is considered unhealthy, this is the amount of time, in ms, to delay things. After this amount of time has passed, the system executes the action.
PendingActionClean upPeriod	How often, in ms, to clean up the pending actions that are stored in memory.
PendingActionsThres hold	The amount of memory, in bytes, used to store all of the pending actions. Whenever a pending action exceeds the timeout value, the system adds the action to the pending action collection in memory.
ThrottlingEnable	Turns on or off outbound throttling.

Change the throttling parameters as follows:

1. Navigate to the AppServer folder and open the web.config file using a text editor such as Notepad.
2. Search for and find the following strings:

Bash

```
<!--Expected timeout on executing reset runtime cache action
during throttling (value in milliseconds)-->
<add key="ResetRuntimeCacheExpectedTimeout" value="1000" />

<!--Expected delaying on executing reset runtime cache before
executing action in during throttling (value in milliseconds)-->
<add key="ResetRuntimeCacheUnhealthyDelayTime" value="5000" />

<!--Expected period to clean up the pending actions (value
in milliseconds)-->
<add key="PendingActionCleanupPeriod" value="300000" />

<!--Expected size threshold of pending actions collection -->
<add key="PendingActionsThreshold" value="15728640" />

<add key="ThrottlingEnable" value="true" />
```

3. Change the values as needed.
4. Save the file.
5. Perform a Microsoft IIS reset.

3.5. Setting up Redis

You will have to setup Redis if you want to use the Chat service in Neurons for ITSM. All the different setup scenarios are explained below.

> If you have installed Redis but not using the Chat service, you might consider uninstalling it. To uninstall refer to the section **Uninstall Redis**.

Different install and uninstall options and scenarios

Upgrading/Installing Redis for existing/New customer:

- **Installing Redis in Linux Container on Windows**
  - **Installing Linux container on Windows Server with Docker**
  - **Installing Redis 6.2.5 in Docker**
- **Installing Redis on Linux Machine**
  - **Installing Redis on Linux Machine (Ubuntu)**
  - **Establish the remote Redis Connection**
  - **Install Redis on Windows Using WSL2**
- **Uninstalling Redis from Windows Server (existing customer)**
  - **Remote Redis Connection - using redis.bat script**
  - **Remote Redis Connection from Windows UI**
  - **Remote Redis Connection using redis-server.exe**
- **Uninstalling from Linux Container**
- **Uninstall from Linux Machine**

Option 1 – Install Redis in Linux Container on Windows Server

Prerequisite:

- Windows server - version 2019 or above with HyperV enabled.
- For more information on Linux container requirements check out - **Windows container requirements**.
- For upgrading your Windows Servers, check out this **Windows Server Upgrade guide** and look for target version you need to upgrade.

Installation steps:

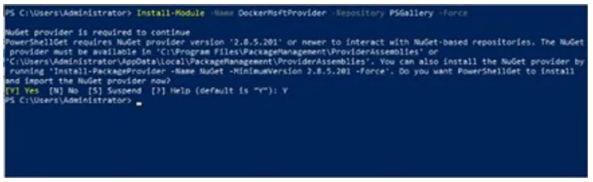
Installing Linux container with docker on Windows Server

1. Open PowerShell as Administrator and run the following command:

```
Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
```

   This installs the Docker-Microsoft PackageManagement provider.

   Sample Output



2. Install the preview build of Docker EE and run the following commands:

Install-Module DockerProvider

Install-Package Docker -ProviderName DockerProvider -RequiredVersion preview

3. Use “Yes” or “Y” to agree to install or use “A” to agree to all.
4. When the installation is complete, reboot the system.
5. To run Linux containers, enable LinuxKit system and use the following command:

[Environment]::SetEnvironmentVariable("LCOW_SUPPORTED", "1", "Machine")

6. Use the following command to restart the system/Docker service after the change:

Restart-Service docker

   The Linux container should now successfully run on your Windows Server.

For more information, refer - **How to run Docker Containers on Windows Server 2019**

Installing Redis 6.2.5 in Docker

1. Open PowerShell as Administrator and run the following command:

docker run -d -p 6379:6379 --name redis-con redis:6.2.5

2. Check if it has successfully installed by executing the command - `docker ps`

Best Practices

- Run the command - `docker update --restart always redis-con` to always restart Redis Container whenever the docker/machine is restarted. If this is not enabled you have to enable Redis container manually everytime the docker/machine is restarted.
- Enable Authentication for Redis. Refer, Add Authentication to Redis.

Setting up Redis Authentication

Add Auth to Redis server

1. Open Powershell and run the command - `docker exec -it redis-con sh`.

   This will give you Redis console.

2. Run **Redis-cli** to set password to Redis server.
3. Run this command to set Redis password - `redis-cli Config Set requirepass <your-password>`.

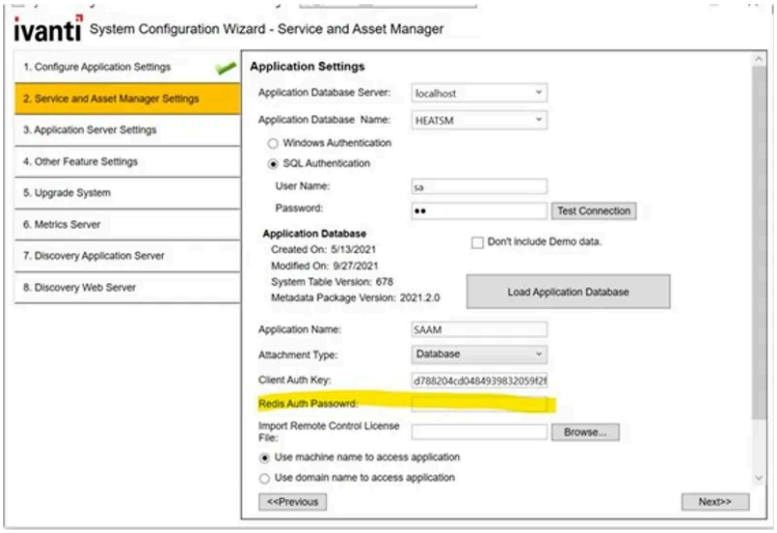
   Your password is successfully set now.

4. To test run the command - `redis-cli Auth <your-password>” it should return “Ok`.

Set the password through SCW for the application to authenticate through Redis password.

In step 2 of SCW configuration (Service and Asset Manager settings) in the field **Redis Auth Password**, enter the same password that is set in the **redis-cli**, and save it.

> Once docker/Redis server/machine is restarted , the auth will be set back to noAuth, sensure to remember and update the password to redis server every time restarted.



Option 2 – Install Redis on Linux Machine

Prerequisite:

- Ubuntu 16.04 or above

Steps to install:

1. Execute the following commands:

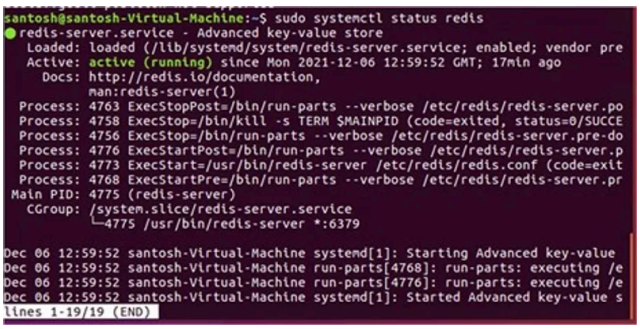
Sudo apt update

Sudo apt install redis-server

2. Check if Redis is set up using the following command:

sudo systemctl status redis

If the result displays as `Active: active (running)` then Redis is successfully setup.



3. Edit the **redis.conf** file to make Redis port available to other servers (by default, the Redis port is on :6379) "*sudo gedit /etc/redis/redis.conf*" or "*sudo nano /etc/redis/redis.conf*"
4. Check for the line "**bind 127.0.0.1**" comment this line by prepending '**#**'

   Since you have removed binding, it is highly recommended to add authentication to Redis Server.
5. Edit **redi.conf "sudo gedit /etc/redis/redis.conf"**
6. Search for requirepass foobared, replace foobared with your_passowrd.
7. Restart the Redis Server to apply changes.

   "sudo systemctl restart redis.service"
8. Then follow "Remote Redis Connection" and "Set password through SCW for the application to authenticate through Redis password."

Option 3 – Install Redis on Windows Using WSL2

This procedure describes how to install Redis on Windows by using Windows Subsystem for Linux (WSL). Redis is installed inside a Linux environment, which runs on Windows through WSL. This method is supported on Windows 10, Windows 11, and Windows Server 2019 or later.

To install Redis on Windows, enable WSL2 (Windows Subsystem for Linux). WSL2 lets you run Linux binaries natively on Windows.

Prerequisites:

- Windows 10, Windows 11, or Windows Server 2019/2022.

Steps to enable WSL:

For Windows 10, Windows 11, or Windows Server 2022.

1. Open **PowerShell** or **Command Prompt** as an administrator.
2. Run the following command:
   wsl --install
3. Restart the system when prompted.

> The **wsl --install** command installs the WSL feature and sets Ubuntu as the default Linux distribution.

For Windows Server 2019 (version 1709 and later)

1. Open **PowerShell** as an administrator.
2. Run the following command:
   Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux
3. Restart your computer when prompted.
4. Download a Linux distribution from the Microsoft WSL Store: *"https://aka.ms/wslstore"*
5. Download the latest **ubuntu** from the following link: *"Manual installation steps for older versions of WSL | Microsoft Learn"*
6. Open PowerShell, Install the downloaded distribution using the following command::
   curl.exe -L -o ubuntu-2004.appx https://aka.ms/wslubuntu2004
7. Replace **app_name.appx** with the actual file name of the downloaded package.

1. Add-AppxPackage .\ ubuntu-2004.appx

8. This installs Linux on your computer.

Steps to Install Redis:

1. Open the installed Linux distribution (for example, Ubuntu) from the Start menu.
2. Update the package list and install Redis:
   curl -fsSL https://packages.redis.io/gpg | sudo gpg --dearmor -o /usr/share/keyrings/redis-archive-keyring.gpg
   echo "deb [signed-by=/usr/share/keyrings/redis-archive-keyring.gpg] https://packages.redis.io/deb $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/redis.list
   sudo apt-get update
   sudo apt-get install redis
3. Start the Redis server:
   sudo service redis-server start
4. Verify that Redis is running:
   redis-cli
   ping
5. If Redis is running correctly, the response will be:
   PONG

Establish the remote Redis Connection

1. Edit the **.env** file in the path "*<install-Path>|Heat|Appserver|chat|.env*"
2. Edit the attribute **REDIS_HOST=localhost to REDIS_HOST=<remote-server-ip>**
3. Save the file.
4. This will install redis successfully.
5. Check if Redis is up by using the command `sudo systemctl status redis" – you should see the active (running status).`

Uninstall Redis for Windows Server (Existing Customer)

This is a mandatory step for existing customers who have already installed Redis and are upgrading to the new version. Uninstall the obsolete Redis version from your machine by following the below server details and uninstall steps.

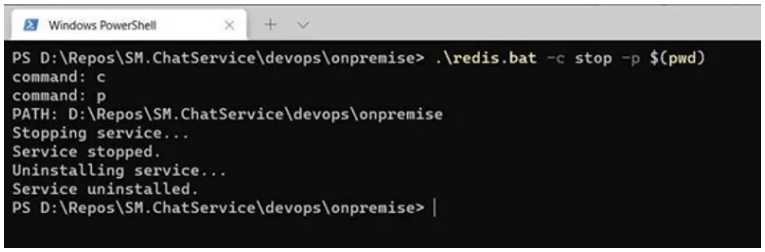
Redis server details:

Version	3.0.503
Path	<install_path>\HEAT\Appserver\AppServer.Main\redis
Project	https://github.com/microsoftarchive/redis
License	https://github.com/microsoftarchive/redis/blob/3.0/license.txt

Option 1 – Uninstall using redis.bat script

1. Run the following in Powershell with administrator privileges.

cd <install_path>\HEAT\Appserver\AppServer.Main\redis; .\redis.bat -p $(pwd) -c stop



2. Optional Step: Cleanup Redis installation files by using the below command:

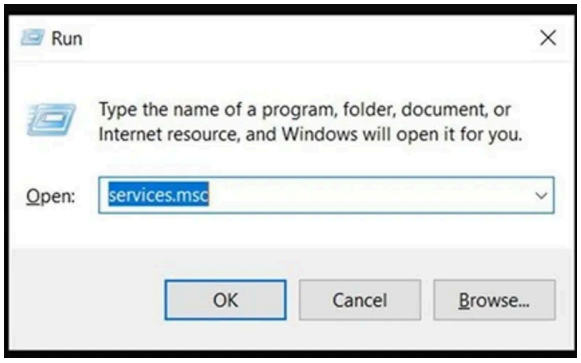
.\redis.bat -p $(pwd) -c cleanup



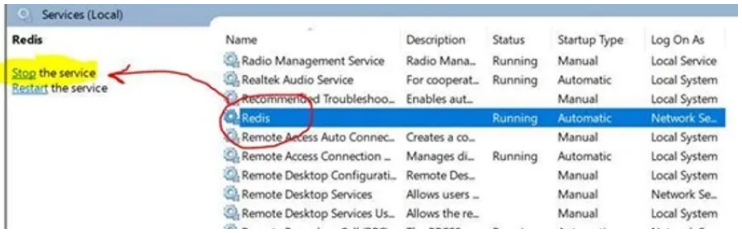
Option 2 – Uninstall from Windows UI

1. Run the following in Powershell with administrator privileges:

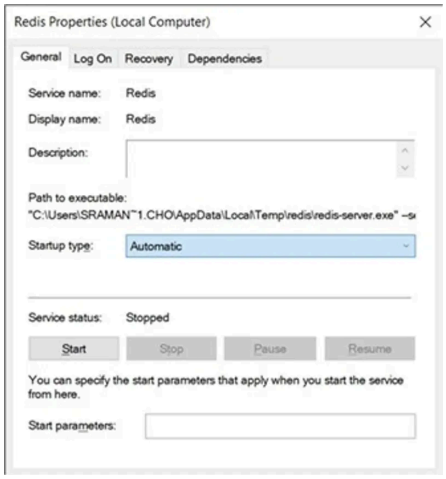
Run services.msc



2. Locate Redis in the list and stop the service.



3. Right click > **Properties**, Change **Startup type** to **Disabled**.



Option 3 – Uninstall using redis-server.exe

Stop the service

Run the following in Powershell with administrator privileges.

.\redis-server.exe --service-stop

```
PS D:\Repos\SM.ChatService\devops\onpremise\redis> .\redis-server.exe --service-stop
[16956] 15 Sep 16:49:03.174 # Redis service successfully stopped.
PS D:\Repos\SM.ChatService\devops\onpremise\redis>
```

Uninstall service

Run the following in Powershell with administrator privileges.

.\redis-server.exe --service-uninstall redis.windows.conf

Uninstall Redis

If you do not want to use the Chat service, you may uninstall Redis by the following the below steps:

Option 1 – Uninstall Redis in container

Execute the following command:

Docker rm /redis-con

Option 2 – Uninstall Redis in Linux Machine

For ubuntu distributions

if you use apt-get to install redis then use

sudo apt-get purge --auto-remove redis-server

if you compiled redis manually then follow the

steps below to remove it completely from linux/ubuntu

sudo service redis_version stop

Now delete everything related to Redis server from /usr/local/bin/

```
sudo rm /usr/local/bin/redis-*

# Now delete Redis Configuration files directory and it's content.

sudo rm -r /etc/redis/

# Delete existing Redis log files.

sudo rm /var/log/redis_*

# Delete existing Redis data directory and it's content.

sudo rm -r /var/lib/redis/

# Delete existing Redis server init scripts

sudo rm /etc/init.d/redis_*

# Remove existing Redis PID files (Only if exists)

sudo rm /var/run/redis_*
```

3.6. Logging into Neurons for ITSM

- Logging In Using the Standard Login Dialog Box
- Logging In Using the Standard Login Dialog Box with an Application Menu
- Adding the Application Menu Option to the Standard Login Dialog Box

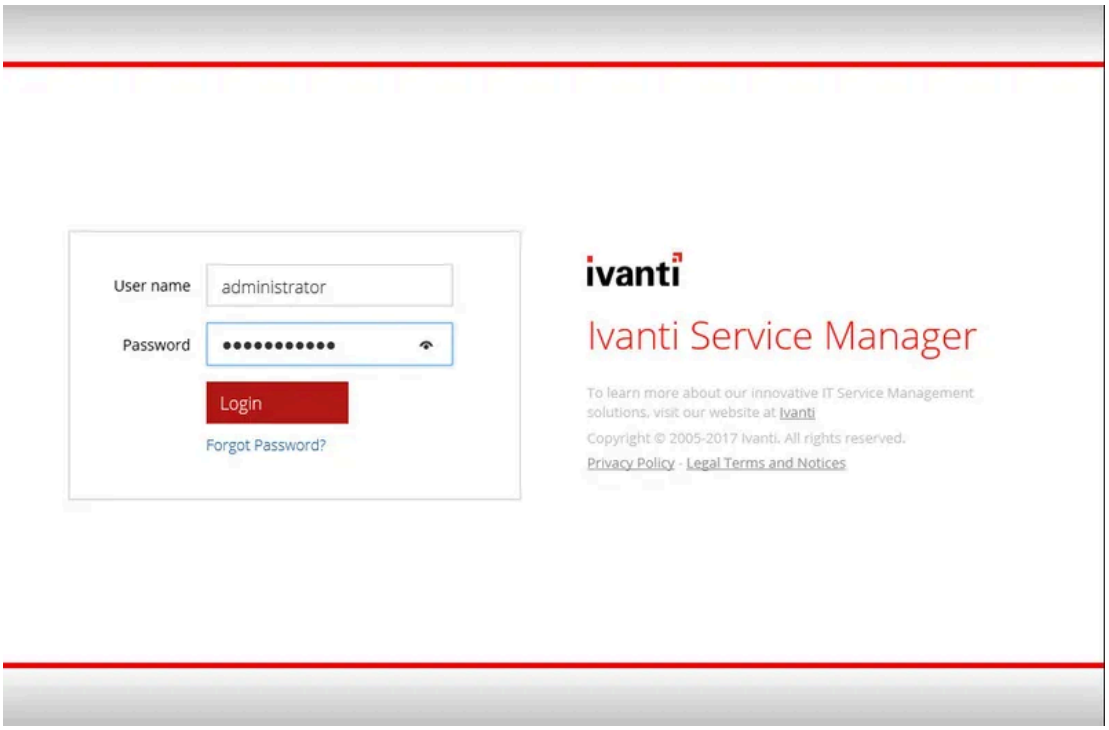
Logging In Using the Standard Login Dialog Box

The standard login dialog box enables you to access Neurons for ITSM on the host that you are logged into now. You see this dialog box when you click the any of the following:

- The Neurons for ITSM desktop shortcut
- The Windows apps menu shortcut

In the dialog box, enter your user name and password, and then click Login.

Standard Login Dialog Box



> The default username for Neurons for ITSM is HEATAdmin. You created the password when you configured the application database.

Logging In Using the Standard Login Dialog Box with an Application Menu

This login dialog box enables you to access the following:

- The Neurons for ITSM system on the host that you are logged into now.
- Individual tenants, such as staging or UAT, if you have more than one.
- The configuration database (ConfigDB).

In the dialog box, enter your user name and password, select an application, and click Login.

- The default username for the configuration database (ConfigDB) is HSWAdmin. You can choose the password when you create the database.
- The default username for Neurons for ITSM is HEATAdmin. You can choose the password when you create the application database.

Adding the Application Menu Option to the Standard Login Dialog Box

To see the login dialog box with the application menu option (only for server-side login), do the following:

1. Go to C:\Program Files\HEAT Software\HEAT\AppServer\.
2. Right-click the HEAT.url file, and choose Properties.
3. Change the host name and port number to localhost. For example, change http://SERVER2012:80/HEAT to http://localhost/HEAT.
4. Click OK.
5. Open a directory window or a browser window and enter either localhost/HEAT or http://localhost/HEAT.

3.7. Adding Features and Changing Settings

- Adding and Deleting Features
- Changing Feature Settings by Running the System Configuration Wizard

Adding and Deleting Features

Adding features to or deleting features from an existing Neurons for ITSM system is much easier than upgrading the system.

If you have an Enterprise Production Deployment, your action might apply to just one, some, or all of the servers, depending on the features that you are adding or deleting.

> To add servers to your deployment, follow the instructions under Installing the Neurons for ITSM System

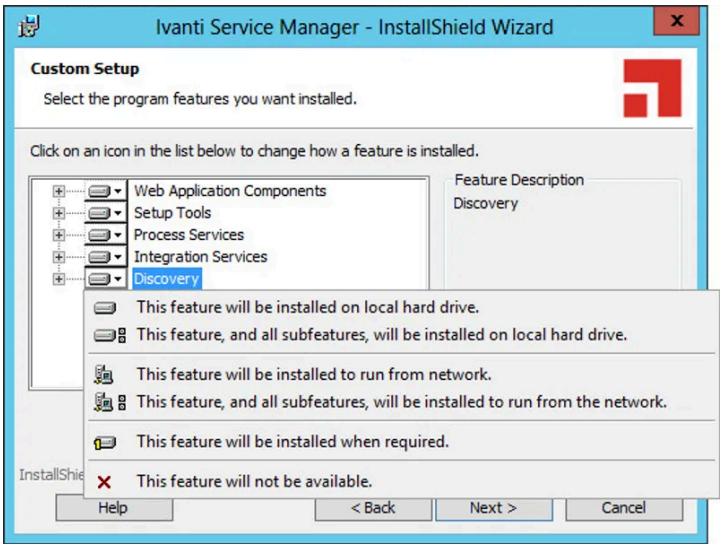
To add features or delete features, do the following:

1. Access the installation folder on the Ivanti Software product CD or zip file and run IvantiServiceManager.exe. Right-click and select Run as Administrator to ensure proper installation.

The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.

2. Select **Install** at prompt. Installation of the prerequisite software can take several minutes.
3. If you are prompted to restart the system, select **Yes**. The system displays the **Welcome** dialog box.
4. Click **Next**. The system displays the **Program Maintenance** dialog box.
5. Choose Modify and click **Next**. The system displays the **Custom Setup** dialog box.

Custom Setup Dialog Box



6. Click the down arrow on each feature and make your selection.

> Adding features requires more hard-drive space. If there is not enough space on your hard drive, the installer displays a message.

7. Click Next and then click Install.

The Neurons for ITSM installation begins. The system displays a status dialog box showing the installation progress of each component over the next few minutes.

8. If you cancel the installation at any time, click Finish to close the installer.

When the components are installed, the system automatically launches the System Configuration Wizard.

9. Go to **Configuring Neurons for ITSM** for instructions about using the System Configuration Wizard.

Changing Feature Settings by Running the System Configuration Wizard

To change settings without adding or deleting features, you do not need the Ivanti Software product CD or zip file.

1. In the **Start** menu, click the down arrow to see the **Apps** menu, and then **About Configuring with ADFS**click System Configuration Wizard.

> You must click Run as administrator when you start the System Configuration Wizard manually.

2. Go to **Configuring Neurons for ITSM** for instructions about using the System Configuration Wizard.

3.8. Upgrading Neurons for ITSM from an Earlier Release

Landscapes

During an Neurons for ITSM upgrade, you can upgrade the development (staging) or testing (UAT) landscapes and test them without affecting the production landscape. After you have verified that the development (staging) or testing (UAT) landscape upgrade was successful, go ahead with production landscape upgrade.

Reporting Feature

You must upgrade both Neurons for ITSM and the reporting feature at the same time. The versions of the software for both Neurons for ITSM and the reporting feature must be the same.

Licenses

Versions of Ivanti Service Management before Release 2015.1 used a different licensing structure. When you upgrade to Neurons for ITSM Release version 2015.1, the system automatically uses the licenses that you used in the previous release.

In the System Configuration Wizard, on the **Configuration Application** page, there are fields to enter the license files. The system populates these fields automatically based on your previous license file. See **Configuring the Configuration Database**.

DSM Integration

If your Neurons for ITSM deployment includes a DSM integration, you must configure and verify your DSM integration for the new release.

- For Ivanti Service Management releases prior to 2015.2, use the DSM Integration service component available in the Neurons for ITSM installer for DSM Integration.
- For Ivanti Service Management releases 2015.2 and later, use the package from the Ivanti App Store for DSM Integration.

After you have upgraded Neurons for ITSM, access the Ivanti Software App Store and the DSM integration by doing the following:

1. Log into **https://support.heatsoftware.com/.**
2. Go to the Ivanti Software App Store by selecting App Store from the top menu.
3. From within the Ivanti Software App Store, open the DSM integration package.
4. Download the DSM integration package for Release 2019.1 and the accompanying instructions.
5. Follow the instructions to configure and verify your DSM integration.

For more information about DSM, see Working with DSM in the online help.

About Upgrading from Earlier Releases

- The upgrade to the N version of Ivanti Service and Asset Manager should always be performed from the N-1 version. For example, upgrading the on-premise version from 2018.1.1 to 2019.1.0 should be done only after the upgrade path of 2018.3.1. Skipping any released version of the application during an upgrade might cause the upgrade to fail or the application to stop working after the upgrade.
- 2019.2 is a cloud-only release and does not include updates for on-premise customers.
- The system upgrade log file under c:\Logs\ReleaseTool will be “ApplyPatchConfigDB2019.3.1.log” for configuration database, which is expected for the 2020.1 release.

To upgrade to Neurons for ITSM Release 2024, you must upgrade your system to every Service Management release between your currently installed release and Neurons for ITSM Release 2020.3 in sequential order. See the table below.

Upgrade From Release	Details	Install Release
2013.1.x	The current Ivanti Service Management version and the Inventory Management component, if present. See **Uninstalling the Inventory Management Component**.	2013.2.2
2013.2.x		2014.1.1
2014.1.x		2014.2.1
2014.2.x		2014.3.1
2014.3.x		2015.1
2015.1.x	Nothing.	2015.2
2015.2.x		2016.1
2016.1.x		2016.2
2016.2.x		2017.2
2017.2.x		2017.3.x
2017.3.x		2018.1.x
2018.1.x		2018.3.x
2018.3.x		2019.1.x
2019.1.x		2019.3.x
2019.3.x		2020.1.x
2020.1.x	Important steps to be performed. **Click here** to view the steps.	2020.2.x
2020.2.x	Nothing	2020.3.x
2020.3.x		2020.4.x
2020.4.x		2021.1.x
2021.1.x		2021.2.x
2021.2.x		2021.3.x
2021.3.x		2021.4.x
2021.4.x		2022.1.x
2022.1.x		2022.2.x
2022.2.x	Install the patch - **HotFix_BUG_997037_994439-OnPrem.zip** (install this patch after upgrading to 2022.3 and on fresh installation).	2022.3.x
2022.3.x		2022.4.x
2022.4.x		2023.1.x
2023.1.x		2023.2.x
2023.2.x		2023.3.x
2023.3.x	Refer to **Installing Neurons for ITSM**	2023.4.x

Upgrade From Release	Details	Install Release
2023.4.x		2024.2.x

For example, if you are currently on Ivanti Service Management Release 2014.1.x and you want to upgrade to Ivanti Service Management Release 2018.3, you must do the following:

1. Uninstall Ivanti Service Management Release 2014.1.x and the Inventory Management component, if present. See **Uninstalling the Inventory Management Component**.
2. Install Ivanti Service Management Release 2014.2.x.
3. Uninstall Ivanti Service Management Release 2014.2.x.
4. Install Ivanti Service Management Release 2014.3.x.
5. Uninstall Ivanti Service Management Release 2014.3.x.
6. Install Ivanti Service Management Release 2015.1.x.
7. Install Ivanti Service Management Release 2015.2.x.
8. Install Ivanti Service Management Release 2016.1.x.
9. Install Ivanti Service Management Release 2016.2.x.
10. Install Ivanti Service Manager Release 2017.3.1
11. Install Ivanti Service Manager Release 2018.1.x
12. Install Ivanti Service Manager Release 2018.3.x
13. Install Ivanti Service Manager Release 2019.1.x
14. Install Ivanti Service Manager Release 2019.3.x
15. Install Ivanti Service Manager Release 2020.1.x
16. Install Ivanti Service Manager Release 2020.2.x - Important steps to be performed. **Click here** to view the steps.
17. Install Ivanti Service Manager Release 2020.3.x
18. Install IvantiNeurons for ITSM 2020.4.x
19. Install IvantiNeurons for ITSM 2021.1.x
20. Install IvantiNeurons for ITSM 2021.2.x
21. Install IvantiNeurons for ITSM 2021.3.x
22. Install IvantiNeurons for ITSM 2021.4.x
23. Install IvantiNeurons for ITSM 2022.1.x
24. Install IvantiNeurons for ITSM 2022.2.x
25. Install IvantiNeurons for ITSM 2022.3.x - **click here for details**
26. Install IvantiNeurons for ITSM 2022.4.x
27. Install IvantiNeurons for ITSM 2023.1.x
28. Install IvantiNeurons for ITSM 2023.2.x
29. Install IvantiNeurons for ITSM 2023.3.x
30. Install IvantiNeurons for ITSM 2023.4.x
31. Install Ivanti Neurons for ITSM 2024.2.x

Upgrading from Ivanti Service Management Release 2017.3.x

If you are upgrading to Neurons for ITSM Version 2018.3, you must first upgrade to Neurons for ITSMVersion 2018.1.1. You do not have to uninstall Ivanti Service Management Release 2017.3.x.

If you have a multiple server environment, you must shut off the notifications to the web servers before you upgrade the system. This is because when you make metadata changes as part of the upgrade, the system tries to synchronize them, but because the versions are different, the system hangs or takes a lot of time. See step 2 below.

Perform these steps on the system that hosts the Neurons for ITSM components:

1. Back up the following items:
    - Neurons for ITSM Configuration Database (ConfigDB)
    - Neurons for ITSM Application Database
    - Attachment folder (if used)
2. (Optional, if your system uses multiple servers) Deactivate the web servers by doing the following:

    a. Log into the Configuration Database. See the *Configuration Database Guide for* Neurons for ITSM for information about using the configuration database.

    b. Open the **Web Servers** workspace. The system displays a list of web servers.

    c. Open a web server record.

    d. Clear the Server is Active check box.

    e. Click Save.

    f. Repeat for all of the web servers.
3. Access the installation folder on the Ivanti product CD or zip file and run IvantiServiceManager.exe. Right-click and select Run as Administrator to ensure proper installation.

    The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
4. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**.
5. In the **Upgrade Confirmation** dialog box, click Yes. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
6. In the **Welcome** dialog box, click **Next**. The system displays the **License Agreement** dialog box.
7. Choose **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
8. Click **Next** to accept the default installation folder, or click **Change** and select a different folder. The system displays the **Setup Type** dialog box.
9. Your selection of features from the **Setup Type** dialog box depends on the role of the individual host in your deployment plan.
    - For the **Demonstration or Proof-of-Concept Deployment**, choose Complete, click Next, and install all components.
    - For the **Minimum Production Deployment** , choose Complete, click Next, and install all components.
    - For the **Enterprise Production Deployment**, your choice depends on the role of the host:
        - Production processing server: Choose Custom, click Next, and install all components except for the Operations Console.

- Staging or UAT processing servers: Choose Complete, click Next, and install all components.
- Web servers: Choose Custom, click Next, and only install the Ivanti Service Manager application server.

For the **Enterprise Production Deployment**, note the following:

- If your deployment includes different processing servers for production, staging, and UAT, you must install the License Manager in every one of those landscapes.
- You can choose Complete and install all Neurons for ITSM features on all of your servers, but doing that takes up more disk space than necessary.

When installing components, note the following:

- To not install a component, click the down arrow next to the server icon next to the category name, highlight the component, right click, and select This feature will not be available.
- If your deployment includes DSM, you do not need to install the DSM integration service because that component has been incorporated into Ivanti Service Management since Release 2015.2.

10. Click Next. The system displays the **Ready to Install the Program** dialog box.
11. Click **Install**. The system begins installing Neurons for ITSM and displays a status dialog box, showing the installation progress of each module over the next few minutes.
12. Click OK if the system displays a dialog box saying that reboot is required after installation.
13. If the system displays a dialog box saying that some of the files that need to be updated are currently in use, choose Automatically close and attempt to restart applications and click OK.

    When the installation is completed, the system displays the System Configuration Wizard.
14. Go through the pages in the wizard making any changes that might be necessary.

> If you already have an existing administrator account, you do not need to create a new account. Just enter the information for your existing administrator account.

15. On the **Upgrade System** page, do not check Do not create backup prior to upgrade unless you already made a backup. Hidden for 2017.1 and 2017.2 Needs to show in 2017.3
16. Notice that the system table version and metadata package version for the configuration database are not the latest versions. See **Upgrade System Page Needs to show in 2017.3**.

Upgrade System Page Needs to show in 2017.3

17. Click the top Upgrade System button.
18. When prompted, enter the administrator role credentials for the configuration database and click OK.
19. If your deployment has additional databases to upgrade, repeat steps 15 and 16 until:

    a. All of your databases have been upgraded:

    - Configuration database
    - Application database (IvantiSM)

    b. All of your environments have been upgraded:

    - Production

- Staging
- UAT
- Development (optional combination of staging and UAT)

20. Click Finish.
21. Restart the host server.
22. (Optional) If you also installed the Neurons for ITSM reporting feature, you must upgrade it to the match the release number of your Neurons for ITSM system. Access the installation folder on the Ivanti Software product CD or download folder and run ReportingService.exe to upgrade Neurons for ITSM reporting feature.
23. Log in to the configuration database and activate the web servers that you deactivated in step 2.

Upgrading from Ivanti Service Management Release 2014.3 or Earlier

- About Upgrading From Ivanti Service Management Release 2014.3 or Earlier
- Uninstalling the Inventory Management Component

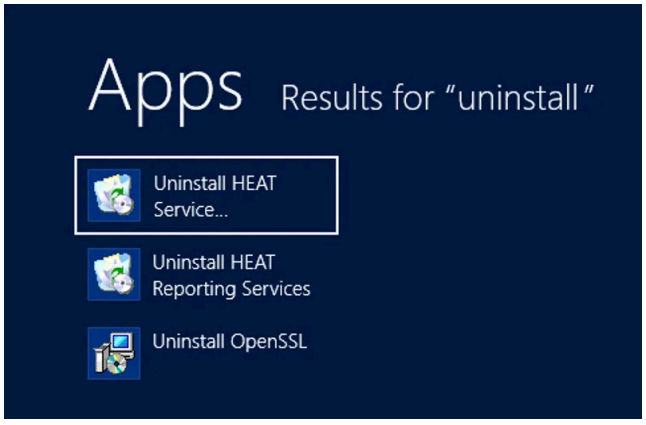
About Upgrading From Ivanti Service Management Release 2014.3 or Earlier

Beginning with Ivanti Service Management Release 2015.1, the Inventory Management component is known as Ivanti HEAT Discovery. As a result, before you can upgrade to the current version of Neurons for ITSM, if you are upgrading from Release 2014.3 or earlier, you must first uninstall the Inventory Management component.

Uninstalling the Inventory Management Component

Perform these steps on the system that hosts Neurons for ITSM:

1. Click the arrow at the bottom of the **Start** menu to view the **Apps** menu.
2. Mouse-over the **Uninstall Ivanti Service Management** icons to find the one for the Inventory Management component.



3. Click Uninstall Ivanti Service Management.
4. In the confirmation dialog box, click Yes.

Upgrading from Ivanti Tryvium 2020.1 Release to 2020.2 Release

The following steps should be performed before installing 2020.2 from 2020.1 release.

1. Log in to Neurons for ITSM with the Administrator role.

2. Open the Configuration console.
3. Under Security Controls, select Security and Sessions.
4. Under Concurrent Session, change the value of Named User, Privileged User, and Non Privileged User to 0.
5. Save the changes and refresh the page and re-validate the values are changed.
6. Now you can install 2020.2 Neurons for ITSM.
7. After installation is complete, you can change the concurrent users values as it was earlier.

3.9. Using the License Manager

- About the License Manager
- Types of Licenses
- About License Bundles
- Using the License Manager

About the License Manager

Use the License Manager to track your license usage.

For the Demonstration or Proof-of-Concept Deployment and Minimum Production Deployment , the License Manager is installed on the Neurons for ITSM server along with the other Neurons for ITSM components.

For the Enterprise Production Deployment, the License Manager is installed on the Neurons for ITSM processing servers along with the other Neurons for ITSM components.

During installation, the System Configuration Wizard enabled you to import one production license, one non-production license, or both, depending on your landscape environment. You can import additional licenses, if needed. See Importing Licenses.

Types of Licenses

Neurons for ITSM mainly uses production and non-production licenses:

License Type	Description	Expiration
Production	Used to access the production landscape of a tenant.	Does not expire unless the MAC address is unspecified. In that instance, the license expires after 30 days. If you move the license to a new server with a different MAC address, then you must acquire a new license tied to the new MAC address.
Development	A non-production license used to access the staging and UAT landscapes.	Expires according to the maintenance agreement between your organization and Neurons for ITSM.
Not For Resale	A non-production license, mainly used by Ivanti Service Manager partners. It can also be used for staging, UAT, or testing if you already have development licenses.	Expires after 30 days if you do not specify the MAC address. After you set the MAC address, it expires according to the maintenance agreement between your organization and Neurons for ITSM.
Evaluation	A non-production license used by potential customers. Has the maximum number of named and concurrent user licenses.	Expires after 30 days. Is not associated with a MAC address.

There are two types of user licenses, for both production and non-production licenses:

- Concurrent licenses: For any user who is currently logged into the system. This is a shared pool of licenses. The concurrent license that is used is specified by the bundle that is specified for each role.

- Named user licenses: Specific to a certain user. The user can log in to the system from many places at one time and it is counted as only one license. You specify which users are named users in the employee record, and you can change which employees get a named user license at any time.

About License Bundles

- List of License Bundles and Components
- Assigning a Bundled License to a Role
- License Tracking in Neurons for ITSM

Neurons for ITSM has defined several license bundles, which are sets of modules, or user interfaces. Each role is associated with a license bundle.

List of License Bundles and Components

License Bundle	Components
Help Desk	• Dashboards and Reporting • Incident Management • Knowledge Management • Mobile • Self Service • Service Catalog • Survey • Voice Automation (optional add-on) • Workflow Automation
Service Desk	• Dashboards and Reporting • Incident Management • Knowledge Management • Mobile • Self Service • Service Catalog • Survey • Voice Automation (optional add-on) • Workflow Automation • Change Management • CMDB • Configuration Management • Problem Management • Service Level Management
Service Management	• Dashboards and Reporting • Incident Management • Knowledge Management • Mobile • Self Service • Service Catalog • Survey • Voice Automation (optional add-on) • Workflow Automation • Change Management • CMDB • Configuration Management • Problem Management

License Bundle	Components
	• Service Level Management • Availability Management • Event Management • Financial Management • Portfolio and Project Management • Release Management

The following are considered license add-on modules:

Add-on Module	Components
Discovery	Discovery
Voice	Voice
Mobile	Mobile

Assigning a Bundled License to a Role

To assign a bundled license to a role, follow the procedure in the "Assigning a Bundled License to a Role" topic in the Neurons for ITSM online help. By default, roles do not have a license bundle associated with them, so you must assign a license bundle to each role manually. If you do not, you may get license violation errors logged in your system even though you have the correct licenses.

> If you have imported licenses but do not see the correct license bundles displayed in the Configuration Console, clear the validation cache.
>
> Go to Configure > Cache Management and then click Reset cached validation lists only.
>
> See the Neurons for ITSM online help for more information.

License Tracking in Neurons for ITSM

You cannot use Neurons for ITSM unless you have a license. When you purchased Neurons for ITSM, you also purchased a set number of licenses. If needed, you can purchase additional licenses.

If you consume more seats than you have licenses for, the system does not log you out. It does, however, log an event into a log file. For example, if you have 10 concurrent licenses and try to log in 11 times, the system allows it.

Due to the way that web browsers work, it is very possible for one user to consume more than one license. For example, if a user logs in to Neurons for ITSM using Microsoft Internet Explorer and then opens Google Chrome and logs in again, another license is consumed. If this happens, the system logs a license violation error that you can view in the License Manager in the **System Audit Information** workspace.

Using the License Manager

- Logging Into the License Manager
- Configuring Landscape Information

- Importing Licenses
- Viewing the Discovery Node Count
- Viewing the Active Licenses
- Configuring the Email Address for Notifications
- Configuring the SMTP Settings
- Working with Scheduled Jobs
- Viewing Reports

Logging Into the License Manager

The License Manager uses the same credentials that are used to access the configuration database.

To log into the License Manager, follow these steps:

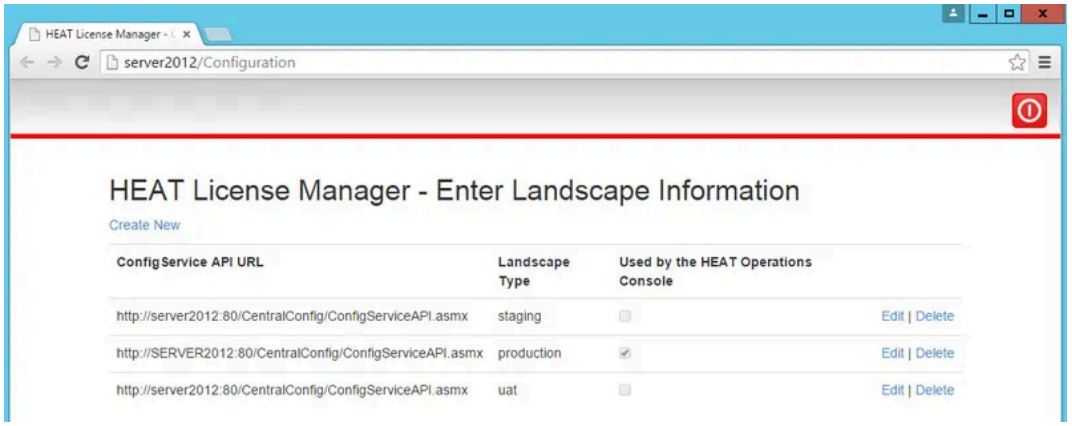
1. In the **Start** menu, click the down arrow to see the **Apps** menu, and then click License Server.
2. Select a landscape.
3. Enter your user ID and password. This is the same user ID and password that you use for the configuration database.
4. Click Continue.

Configuring Landscape Information

You can create, edit, and delete information about the landscapes to which the License Manager is associated.

1. Log into the License Manager.
2. Click either Configure Landscapes in the top right corner of the login page or click Configure Landscape Information from any page in the License Manager. The system opens a new browser window and displays the **Enter Landscape Information** page.

   Enter Landscape Information Page



3. To allow the Operations Console to use this landscape, check Used by the Operations Console on the line associated with the landscape.

   The Operations Console can only use one landscape at a time.

4. To edit the information for an existing landscape, do the following:

   a. Click Edit on the line associated with the landscape. The system displays the **Edit Landscape** page.

b. Make changes as needed.

c. Click Save.

5. To delete the landscape information, do the following:

   a. Click Delete on the line associated with the landscape.

   b. Click Delete at the confirmation message.

6. When you configured Neurons for ITSM using the System Configuration Wizard, the system automatically created a link to the landscape.

Therefore, in general, you do not need to add a link to a landscape. However, if you do need to add a new link to a landscape, follow these steps:

a. Click Create New. The system displays the **Create Landscape** page.

b. In the **ConfigService API URL** field, enter the URL of the configuration server.

c. Check Used by the Operations Console if the system should use this link to connect with the Operations Console. The Operations Console can only connect to one landscape.

d. Click Load Landscape Types and then select a landscape from the drop-down list.

e. Click Create.

Importing Licenses

When you initially configured the License Manager in the System Configuration Wizard, you imported either one production license file, one non-production license file, or both. (See **Configuring Neurons for ITSM** .)

If your deployment has multiple License Managers, when you import a license, ensure that you are importing it on the server that has the same MAC address as the license file.

For example, say you installed License Managers on the following:

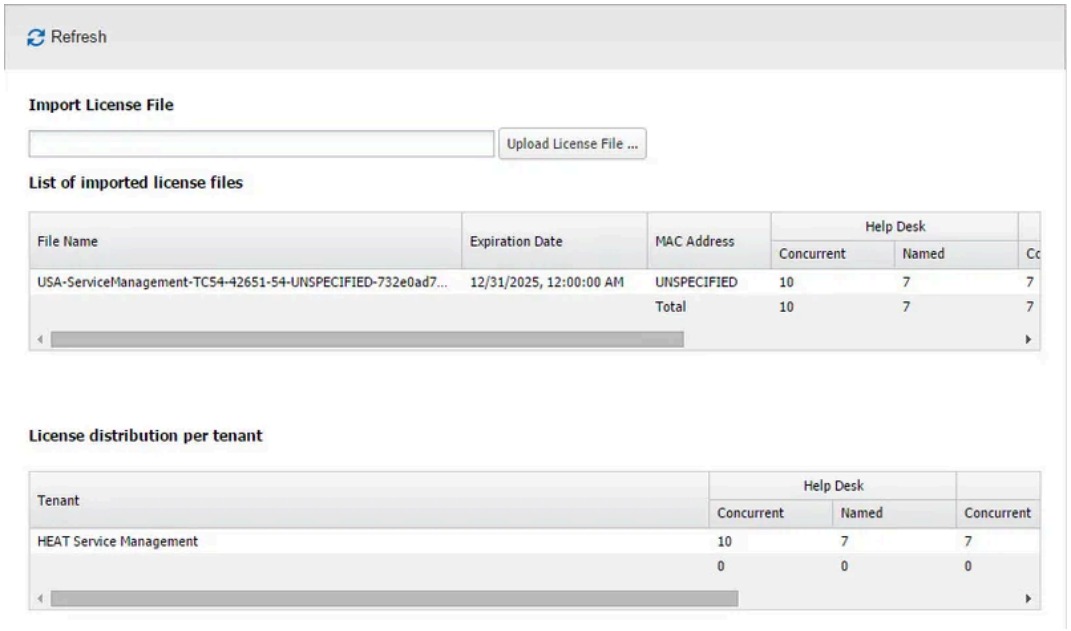
- Application Server 1 with a MAC address of AA🕒23🕒00
- Application Server 2 with a MAC address of BB🕒23🕒00

Then you ask for and receive a production license for MAC address AA🕒23🕒00. You import the license from the License Manager that is installed on Application Server 1. After you have imported the license, the License Managers on both Neurons for ITSM application servers respect the license. You do not need a second license for the second Application Server.

To import additional license files, follow these steps:

1. Log into the License Manager.
2. Click Licensing > Import License Files. The system displays the **Licensing - Import License Files** page.

   Import License Files Page



3. Click Upload License File....
4. Navigate to and select a license file and click Open.

   The system adds the license to the system. This page shows the following information:

Field	Description
File Name	The name of the license file that you uploaded.
Expiration Date	The expiration date of the license file.
MAC Address	The MAC address associated with the license file.
Self Service	Self Service is the bundle name. The number of Self Service licenses contained in the license file. Broken into concurrent and named licenses.
Service Catalog	Service Catalog is the bundle name. The number of Service Catalog licenses contained in the license file. Broken into concurrent and named licenses.
Service Management	Service Management is the bundle name. The number of Service Management licenses contained in the license file. Broken into concurrent and named licenses.

5. Click the **delete** icon to remove the license file and its associated licenses from the License Manager.
6. Click the **show details** icon to display the details. The details contain the following information:

Field	Description
Bundle	The name of the bundle.
Name	The name of the module.
Named Licenses	The number of named licenses contained in the license file.
Concurrent Licenses	The number of concurrent licenses contained in the license file.
Expiration Date	The date when the license expires.

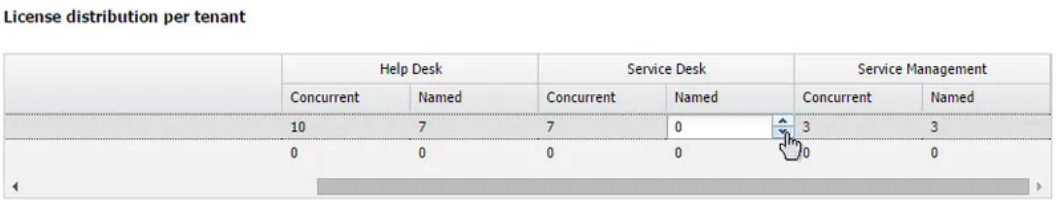
If your deployment only has one tenant, the information displayed here is the same as in the **List of imported license files** section.

If your deployment has more than one tenant, this table displays the license distribution across the tenants.

Field	Description
Tenant	The name of the tenant.
Self Service	The number of Self Service licenses allocated per tenant. Broken into concurrent and named licenses.
Service Catalog	The number of Service Catalog licenses allocated per tenant. Broken into concurrent and named licenses.
Service Management	The number of Service Management licenses allocated per tenant. Broken into concurrent and named licenses.

7. To distribute licenses among multiple tenants, click in a cell and change the number of licenses to allocate to a tenant. The total number of licenses across the tenants cannot exceed the total number of licenses. See **Allocating Licenses Across Tenants**.

   Allocating Licenses Across Tenants



Viewing the Discovery Node Count

This information tracks the trend associated with the Discovery licenses and is based on the Discovery **Count** scheduled job.

1. Log in to the License Manager.
2. Click Licensing > Discovery. The system displays the **Licensing - Discovery** page.

   This page shows the following information:

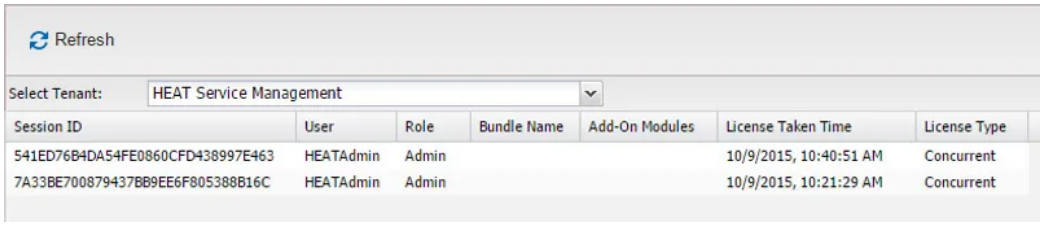
Field	Description
Tenant Name	The name of the tenant.
Last Scan Date	The date and time when the job was run.
Nodes Count	The number of configuration items found during the job.

Viewing the Active Licenses

This page displays the active sessions on Neurons for ITSM. It does not show active sessions on the configuration database.

1. Log in to the License Manager.
2. Click Licensing > Active Licenses. The system displays the **Licensing - Active Licenses** page.

   Active Licenses Page



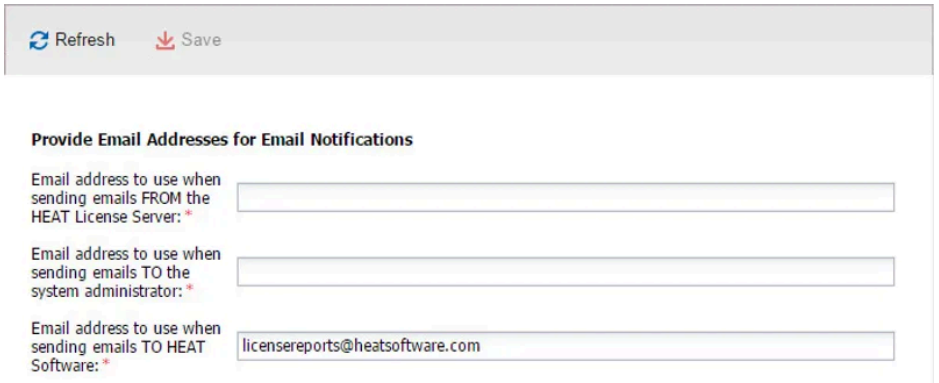
3. Select a tenant from the drop-down list. This page shows the following information:

Field	Description
Session ID	The session ID associated with the logged-in user.
User	The user name of a logged-in user.
Role	The role with which the user is logged in.
Bundle Name	The bundle associated with the license associated with the user. See **About License Bundles**.
Add-On Modules	Any add-on modules associated with the bundle. See **About License Bundles**.
License Taken Time	The time when the system used the license.
License Type	The license type. Can be named or concurrent.

Configuring the Email Address for Notifications

1. Log in to the License Manager.
2. Click Configuration > Email Address. The system displays the **Configuration - Email Address** page.

   Email Address Page



3. Enter the following information:

Field	Description
Email address to use when sending emails from the License Server	The email address to use as the FROM email address for emails sent from the License Manager.
Email address to use when sending emails to Ivanti Software	The email address to use as the TO email address for emails sent from the License Manager to Ivanti Software. The system sends license usage information based on the **License Violation Notification to Frs** scheduled job.
Email address to use when sending emails to the system administrator	The email address to use as the TO email address for emails sent from the License Manager to the system administrator of your organization. The system sends license usage information based on the **License Violation Notification to Admin** scheduled job.

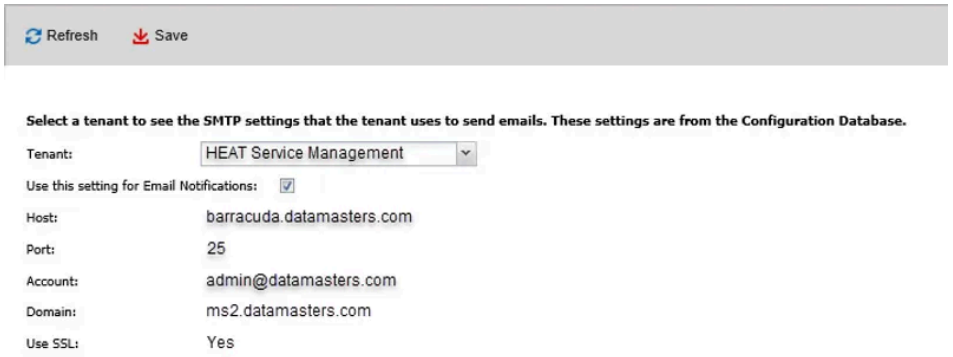
4. Click Save.

Configuring the SMTP Settings

Use this page to view and edit the SMTP settings used to send emails. The information on this page comes from the System Configuration Wizard.

1. Log into the License Manager.
2. Click Configuration > SMTP Setting. The system displays the **Configuration - SMTP Setting** page.

SMTP Setting Page



The system displays the following information:

Field	Description
Host	The email server host.
Port	The port associated with the email server.
Account	The account associated with this tenant. This is the same as the value in the **Username** field on the **Email Configuration** workspace in the Service Desk Console.
Domain	The domain associated with the account.
Use SSL	Specifies if this account should use SSL.

3. Select a tenant from the **Tenant** drop-down list.
4. Check Use this setting for Email Notifications to use these SMTP settings for emails.
5. Click Save.

Working with Scheduled Jobs

The License Manager has several predefined scheduled jobs. These are used to send information to the administrator on a regular basis instead of sending an email every single time there is an event. All violations are listed on the **System Audit Information** page.

The following are the predefined scheduled jobs that cannot be changed:

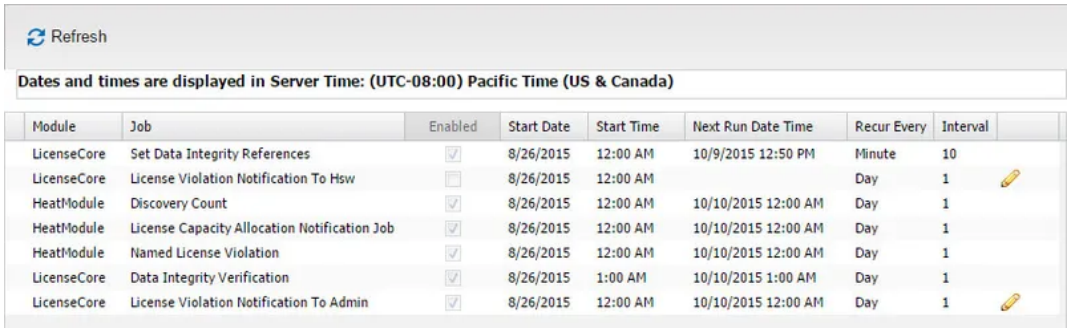
- License Capacity Allocation Notification Job: Determines if your licenses are valid and that you actually have the licenses that you are allocating.
- Named License Violation: Determines if you have more users listed as named users than you have named user licenses.
- Data Integrity Verification: Determines if the licenses have been modified.
- Discovery Count: Determines if the licenses for your configuration items are valid.

The following are the predefined scheduled jobs that you can edit:

- License Violation Notification to FRS: Sends an email to Ivanti Software with information about license violations. By default, this job is disabled.
- License Violation Notification to Admin: Sends an email to your system administrator with information about license violations.

1. Log in to the License Manager.
2. Click **System Jobs**. The system displays the **System Jobs - Scheduled Jobs** page.

   Scheduled Jobs Page



   This page contains the following information:

Field	Description
Module	The name of the module. Can be either LicenseCore or HeatModule.
Job	The name of the job.
Enabled	Specifies if the scheduled job is enabled.
Start Date	The start date of this scheduled job.
Start Time	The start time of this scheduled job.
Next Run Date and Time	The next date and time when the scheduled job runs.
Recur Every	The time period for the recurrence. Can be day, hour, or minute.
Interval	The interval for the recurrence.

For each entry, the system displays additional information at the bottom of the page:

Field	Description
Module	The name of the module. Can be either LicenseCore or HeatModule.
Job	The name of the job.
Run Time	The date and time when the scheduled job was run.
Details	Details of the job. If the job is not successful, contains detailed information.

3. To see the job details in a larger format, click the **show details** icon at the end of the row.
4. You can edit the details associated with the **License Violation Notification To Frs** and the **License Violation Notification to Admin** scheduled jobs.

   To edit a scheduled job, do the following:

   a. Click the **Edit** icon at the end of the row. The system displays a dialog box.

   b. Enter or change any of the following information:

Field	Description
Job	The name of the scheduled job. You cannot change this name.
Description	A description of the scheduled job.
Start Date	The start date and time.
Enabled	Specifies if the scheduled job is enabled.
Next Run Date Time	The next date and time when the scheduled job runs.
Recur Every	Specifies the recurrence for this job.

5. Click Save.

Viewing Reports

You can view two types of reports in the License Manager:

- System audit information

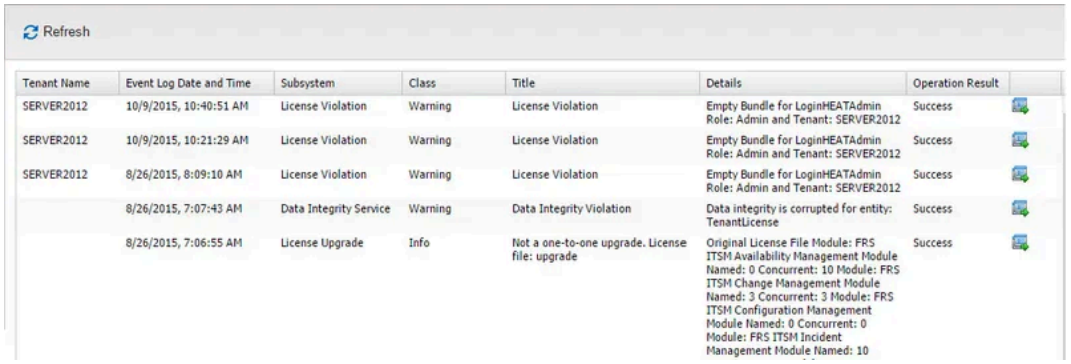
- Logs

Follow these steps to view the reports.

1. Log in to the License Manager.
2. Click Reports.
3. To view the system audit information, click System Audit Information. The system displays the **Reports - System Audit Information** page. See **System Audit Information Page**. Examples of the information on this page include license upgrades and license violations.

   We recommend that you review the information on this page if you have any problems and then review the information on the **Log** page. See **Log Page** .

   System Audit Information Page



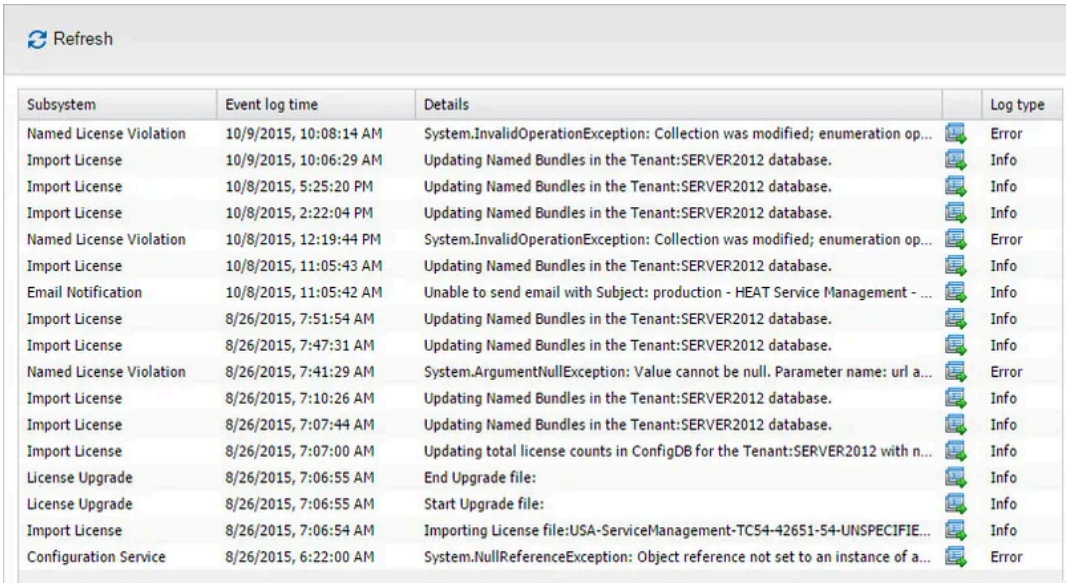
   This page contains the following information:

Field	Description
Tenant Name	The name of the tenant.
Event Log Date and Time	The date and time of the log event.
Subsystem	The specific area. Can be license violation, license upgrade, or data integrity service.
Class	The type of information. Can be warning, info, debug, fatal, or error.
Title	A short description of the event.
Details	A longer description of the event.
Operation Result	The result of the operation. Can be success or failure.

   If you cannot see all of the columns, resize the columns that you can see so that the remaining columns are displayed.

4. Click the **show details** icon at the end of the row to see the details. If you cannot see the **Show Details** icon, resize the columns until it is displayed.
5. To view log information, click Log. The system displays the **Reports - Log** page. Use this information for troubleshooting.

   Log Page



This page contains the following information:

Field	Description
Subsystem	The name of the subsystem. Can be email notification, import license, license upgrade, named license violation, or configuration service.
Event Log Time	The time and date of this log event.
Details	Information about this log event.
Log Type	The type of log. Can be info, error, or warning.

6. To see the log details in a larger format, click the **show details** icon at the end of the row.

3.10. Troubleshooting - Installation and Deployment

If there are problems with your installation or deployment, refer to this topic.

This topic does contain a long list of problems and its solutions which may be difficult to go through, it is recommended you search using relevant keywords to get to the right problem/resolution faster

Problem 1:
Error message "Error upon executing commands: The following error occurred when authenticating with the tenant <tenantUrl>" is displayed.

Status: TenantNotFound

Possible Cause

The tenant specified is invalid.

Solution

Ensure that the tenant URL and tenant ID are valid.

Problem 2:
Error message "Error upon executing commands: The following error occurred when authenticating with the tenant <tenantUrl>" is displayed.
Status: AccessDenied

Possible Cause

Invalid user name or password is provided.

Solution

Ensure that the user name and password are valid.

Problem 3:
Error message "Error upon executing commands: The following error occurred when authenticating with the tenant APPSERVER" is displayed.
Status: InvalidRole

Possible Cause

No administrator rights.

Solution

Ensure administrator credentials exist. See **About Roles**.

Problem: 4
Error message "Error upon executing commands: Could not establish trust relationship for the SSL/TLS secure channel with authority '<IP_address>" is displayed.

Possible Cause

Did not connect to the Neurons for ITSM application server using HTTPS.

Solution

Configure the Neurons for ITSM application server to use SSL. See **Optional SSL Configuration**. Enter the URL for the Neurons for ITSM application server that is configured to use SSL.

Problem 5:
Error message "Failed to execute applyPatch: The remote server returned an unexpected response: (400) Bad ". is displayed.

Possible Cause

The database version is not up to date.

Solution

If the system table upgrade fails, review the log files and fix any metadata issues. Then upgrade the system table.

Problem 6:
Cannot view the login dialog box. This message is displayed - "Please use the subdomain when accessing the application". For example, https://yourname.saas.heatsoftware.com.

Possible Cause

The web.config file parameter "RequireTenantIdInURL" value is set to true.

Solution

1. Go to C:\Program Files\HEAT Software\HEAT\AppServer\ and open the web.config file.
2. Search for the parameter "RequireTenantIdInURL" and change its value to false.
3. Save and close the web.config file.

Problem 7:
After upgrading to the latest version of Neurons for ITSM, the list of tenants in the Operations Console is empty.

Possible Cause

During the upgrade, the system updated the connection strings for the landscape with the incorrect name for the data source.

Solution

In the Operations Console, edit each landscape to update the data source to the correct database server name. See **Upgrading Neurons for ITSM from an Earlier Release** for more information on how to do this.

Problem 8:
Failed to execute applyPatch: The request channel timed out while waiting for a reply after 00:59:59.7741622. Increase the timeout value passed to the call to request or increase the SendTimeout value on the binding. The time allotted to this operation may have been a portion of a longer timeout.

Possible Cause

By default, the upgrade tool is set to wait for one hour for a response from the Neurons for ITSM application server. This message indicates that the Neurons for ITSM application server is still applying the patch or package. The patch can be completed at any time.

Solution

Check the status of the upgrade tool later by looking at the patch log in the Configuration Database.

Problem 9:
Error message "No database backup location specified in configuration database. Please contact support." is displayed.

Possible Cause

- The backup location is not set in the configuration database.
- The backup failed to execute because of permissions issues.

Solution

Ensure the backup location is set the correct permissions are set.

Problem 10:
Error message "Error during metadata commit operation: System.Exception: The following errors were encountered when synchronizing the schema...:" is displayed.

Possible Cause

This indicates a serious problem in business object metadata and is a synchronization schema error. The system cannot synchronize the database schema change with the business object definition. If you get this error, the system usually stops upgrading the metadata.

Solution

If this happens in the production environment, restore the database from a backup that was made before the upgrade. Then contact Ivanti support so that they can look into the error.

Problem 11:
Error message "Error during metadata commit operation: DataLayer.SaaSDbException: Invalid object name 'Frs_ITFM_Account_Status'. ---> System.Data.SqlClient.SqlException: Invalid object name 'Frs_ITFM_Account_Status'" is displayed.

Possible Cause

Part of the database is corrupt.

Solution

Contact Ivanti Software support. They may suggest to restore the database from a backup that was made before the upgrade.

Problem 12:
Error message "Error during metadata commit operation: DataLayer.SaaSDbException: Invalid object name 'Frs_ITFM_Account_Status'. ---> System.Data.SqlClient.SqlException: Invalid object name 'Frs_ITFM_Account_Status'" is displayed.

Possible Cause

Part of the database is corrupt.

Solution

Contact Ivanti Software support. They may suggest that to restore the database from a backup that was made before the upgrade.

Problem 13

**Error message An error occurred when applying patch named <some_filename>.sql in package <some_package>.MetadataPackage to tenant <tenantUrl>.
Unable to execute SQL due to Invalid column name 'IPCMUrlPort'.:
update FRS_IPCM_Integration set IPCMUrlPort = 2323 where IPCMUrlPort is null
Unable to execute SQL due to Invalid column name 'IPCMUrl'.:
update FRS_IPCM_Integration set IPCMUrl = 'http://' + IPCMServerHost + ':' + convert(varchar(6), IPCMUrlPort) where IPCMUrl is null and IPCMServerHost is not null" is displayed.**

Possible Cause

An embedded Microsoft SQL statement is corrupt.

Solution

Review the Microsoft SQL statements.

Problem 14:

**Error message Error during metadata update operation. MetadataType: BusinessObject, ID: Frs_AuthenticationProvider#
SaaS.StandardizedMetadata.UpdateKeyNotFoundException: Update key not found: key = Rel2s
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences)
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider provider, ISessionContext sessionContext, IEnumerable`1 definitionGroup) in c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPatch.cs:line 1034 is displayed.**

Possible Cause

There is a problem updating the metadata and the system did not update the business object.

Solution

Review the business object to make sure it was updated.

Problem: 15

Error Message – Form

Error during metadata update operation. MetadataType: Form, ID: Task.WorkOrder System.Exception: Update key not found: key = Details
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1377
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider provider, ISessionContext sessionContext, IEnumerable`1 definitionGroup) in c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPatch.cs:line 1016.

Error Message – Dashboard

Error during metadata update operation. MetadataType: Dashboard, ID: 8e2cce05-c593-4545-bf4d-5f719a9bd5a5 System.Exception: Update key not found: key = OLA Target Compliance (e94a602f-959e-4cf1-9c07-be4d5eb0da68)
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1377
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider provider, ISessionContext sessionContext, IEnumerable`1 definitionGroup) in c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPatch.cs:line 1016

Error Message – Validation Data

Error during metadata update operation. MetadataType: ValidationData, ID: Justification# System.Exception: Update key not found: key = Justification#_culture#pt-BR
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1377
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1359
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider provider, ISessionContext sessionContext, IEnumerable`1 definitionGroup) in c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPatch.cs:line 1016

Error Message – Rule

Error during metadata update operation. MetadataType: Rule, ID: Incident# System.Collections.Generic.KeyNotFoundException: The given key was not present in the dictionary.
at System.Collections.Generic.Dictionary`2.get_Item(TKey key)
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1386
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement element, XElement differences) in c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensions.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider provider, ISessionContext sessionContext, IEnumerable`1 definitionGroup) in c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPatch.cs:line 1016

Possible Cause

There is a problem updating the metadata.

Solution

No action.

Problem 16:
Error during metadata delete operation. MetadataType: Workflow, ID: 69d31c7248b54f92bc1bff415cd29e0f System.Exception: Could not deactivate workflow definition RecId: 69d31c7248b54f92bc1bff415cd29e0f ---> System.Exception: Error updating existing active workflow definition to inactive, RecId 69d31c7248b54f92bc1bff415cd29e0f at SaaS.WebUI.WorkflowMetadataServices.WorkflowMetadataUpdate.Delete(MetadataType metadataType, String id) in c:\depot\Eng\SaaS\main\Platform\AppServer\BPE\src\WorkflowMetadataServices.cs:line 409 Error during metadata insert operation. MetadataType: Workflow, ID: 871d9466c4754fa19ffb03de179cd057 System.Exception: Inactive definition exists with the same RecId: Name:LDAP Sync_LC_133k134k135k13k14k15k16k17k18k19k, ObjectType:ScheduleEntry, Definition RecId 871d9466c4754fa19ffb03de179cd057 at SaaS.WebUI.WorkflowMetadataServices.WorkflowMetadataUpdate.CreateWorkflowDefinition(String name, String objectType, String defRecId, String typeRecId, XElement workflow) at SaaS.WebUI.WorkflowMetadataServices.WorkflowMetadataUpdate.Insert(MetadataType metadataType, XElement workflow) at SaaS.StandardizedMetadata.MetadataProvidersContainer.Insert(MetadataType metadataType, XElement definition) at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider provider, ISessionContext sessionContext, IEnumerable`1 definitionGroup)

Possible Cause

There is a problem updating the workflows.

Solution

No action.

Problem 17:
Discovery cannot detect assets on the network.

Possible Causes

- Service Center Configuration Manager (SCCM) service is stuck in starting mode.
- Using a domain account for running all Neurons for ITSM services but the domain account has insufficient rights.

Solution

Use the local system account and restart Neurons for ITSM.

Problem 18: System cannot search.Possible Cause Full-text search is disabled. Solution Enable full-text search. See Full Text Search .

Possible Cause

Full-text search is disabled.

Solution

Enable full-text search. See **Full Text Search** .

Problem 19:
The Neurons for ITSM demo database does not load properly.

Possible Cause

Full-text search is disabled.

Solution

Enable full-text search. See **Full Text Search** .

Problem 20:
Web servers do not work correctly.

Possible Cause

In multi-server environments, each Neurons for ITSM web server must meet the system requirements.

Solution

Refer to the *System Requirements and Compatibility Matrix for* Neurons for ITSMfor more information.

Problem 21:
Provision report now returns an exception: Cannot Decrypt the Symmetric Key.

Possible Cause

The Neurons for ITSM reporting server cannot use the symmetric key to access the data from the report server database.

Solution

1. Click **OK**, but do not close the System Configuration Wizard.
2. Start the Reporting Services Configuration Manager and connect to your Microsoft SRSS instance.
3. Select **Encryption Keys** from the list in the left panel.
4. Click **Delete** and then click **Yes** at the confirmation message.
5. Return to the wizard and click **Provision Report Now**.

Problem 22:
Cannot download or edit reports in Chrome.

Possible Cause

The Chrome ClickOnce extension is not installed.

Solution

Install the ClickOnce extension for Chrome. Navigate to https://chrome.google.com/webstore/detail/eeifaoomkminpbeebjdmdojbhmagnncl# and download the extension.

Problem 23:
Cannot download or edit reports in Firefox.

Possible Cause

The Firefox Microsoft .NET framework assistant extension is not installed.

Solution

Install the Microsoft .NET framework assistant extension. Navigate to https://addons.mozilla.org/en-US/firefox/addon/9449 to download the extension.

Problem 24:
Cannot download files or run controls in Internet Explorer.

Possible Cause

Scripting is disabled.

Solution

Set properties in Internet Explorer as follows:

1. Go to the Tools > Internet Options > Security > Custom level page.
2. Set the following options to enable:
3. Run ActiveX controls and plug-ins
4. File download
5. Scripting > Active scripting

Problem 25:
Cannot open websites in Internet Explorer.

Possible Cause

The Neurons for ITSM is not set to be a trusted site.

Solution

Set properties in Internet Explorer as follows:

1. Go to the Tools > Internet Options > Security page.
2. Highlight Trusted sites and click Sites.
3. Click Add.

Problem 26:
Logging into a tenant using Internet Explorer fails.

Internet Explorer displays this message: You cannot login to the system now. Please contact your administrator. Additional information is available in the logs.

Possible Cause

Internet Explorer does not accept cookies if the host name of the DNS server or the server NetBIOS names contain an underscore '_'.

Solution

- Change the host name of the DNS server or its NetBIOS names so they no longer contain an underscore '_'
- Use a Chrome or Firefox browser.

Problem 27:
Unable to use integrated components, such as Voice.

Possible Cause

Using the Microsoft Windows operating system when using integrated components.

Solution

Change to the Microsoft Windows operating system. Refer to the *System Requirements and Compatibility Matrix for* Neurons for ITSMfor more information.

Problem 28:
When trying to access the Configuration Database, the application redirects the user from http://localhost/HEAT to https://localhost on the machine where SSL is not setup.

Possible Cause

There is a known limitation in the 2018.3.1 release with respect to FedRamp requirements related to the URL redirect configuration.

Solution

To resolve this, there is a need to update an entry in the web.config file. Set the parameter highlighted below to ‘false’ and restart IIS. Once the process is completed, try to access **Configuration Database**.

</rule>

<rule name="HTTP to HTTPS redirect" stopProcessing="true">

<match url="(.*)">

</match>

<conditions>

<add input="" pattern="^localhost$" negate="true">

</add>

<add input="" pattern="off" ignoreCase="true">

</add>

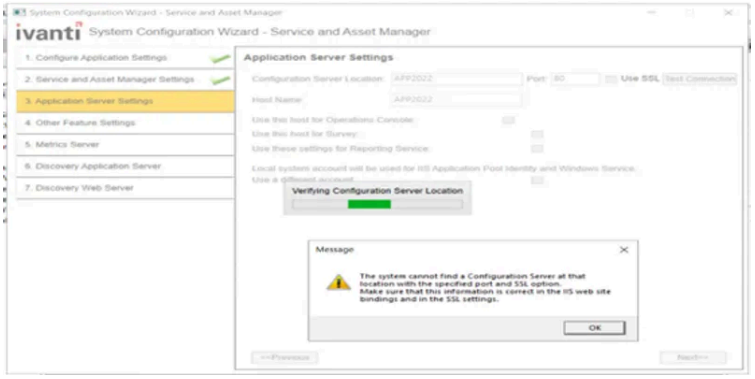
</conditions>

<action type="Redirect" url="https:///{R:1}" redirectType="Permanent">

</action>

</rule>

Problem 29:
From the System Configuration Wizard (SCW) - unable to connect to Central CentralConfig URL configuration.





Possible Cause

ErrorCode - 0x8007000d - URL Rewrite or IIS Hosting Bundle is not installed correctly.

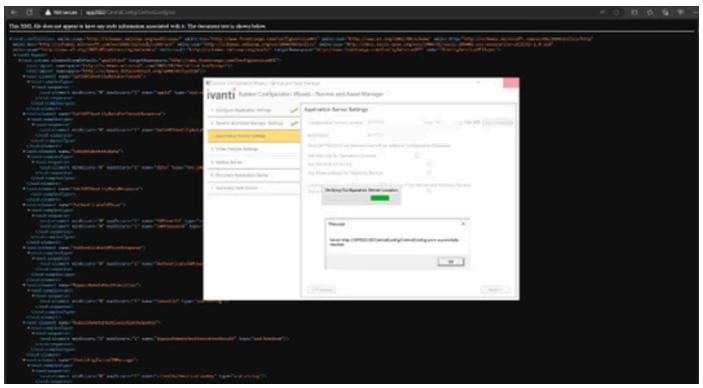
Solution

1. Open IIS.
2. Browse CentralConfig from Default Websites.



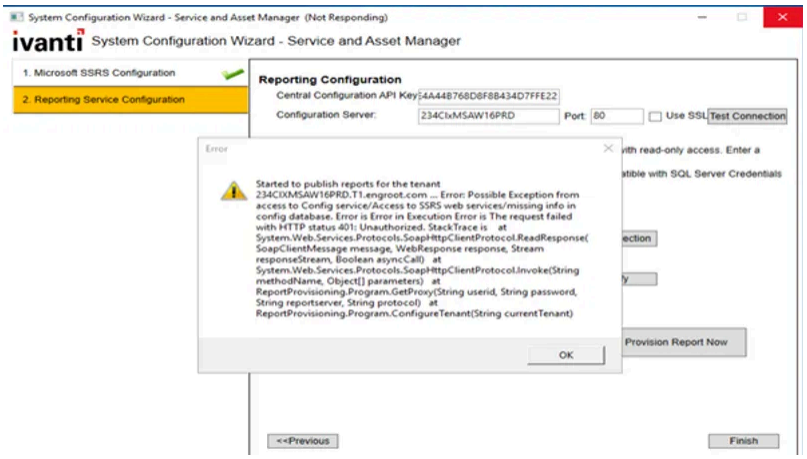
   Check CCF Url - **http(s)://<TenantID>/CentralConfig/CentralConfig.svc**. For example, http://app2022/CentralConfig/CentralConfig.svc.

3. If it is not accessible check error code in the browser - 0x8007000d.
4. Restart IIS and check if the CentralConfig URL is accessible.
5. If the CentralConfig is URL not accessible – install the **IIS Hosting bundle** and the **Restart IIS**.
6. Check the CentralConfig endpoint - http(s)://<TenantID>/CentralConfig/CentralConfig.svc.



7. If the CentralConfig is accessible, continue with the SCW setup.

Problem 30: System Configuration Wizard (SCW) - Report Provisioning fails displaying the following error - "Possible Exception from access to Config service/Access to SSRS web services/missing info in config database. Error is Error in Execution Error is The request failed with HTTP status 401: Unauthorized".



Possible Cause

The SSRS report service is not reachable by SCW.

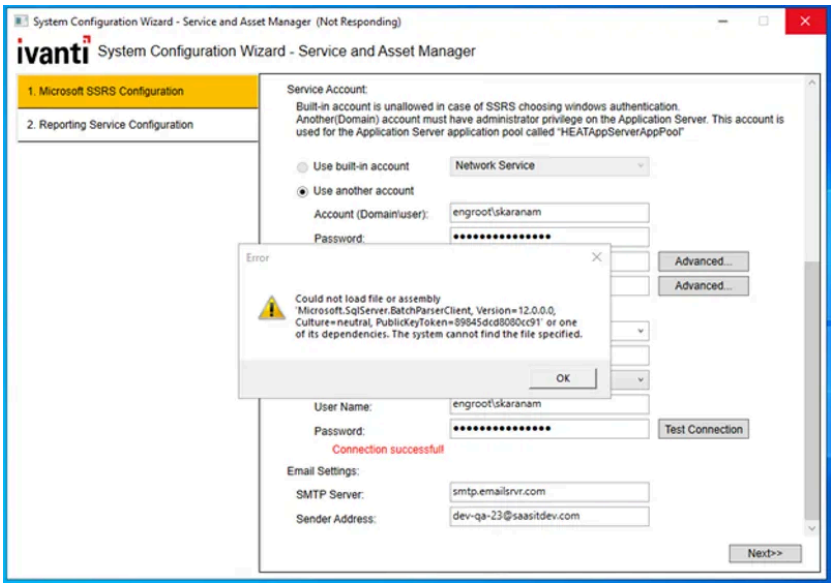
Solution

Check if the SSRS report configuration is reachable. After confirming, restart the SCW configuration.

Steps:

1. Open the Report Server Configuration Manager.
2. Start the SSRS and provide correct configuration details.
3. Recheck the ReportProvisioning.

Problem 31:
While installing System Configuration Wizard (SCW) Report Server in virtual machine, the following error is thrown - "Could not load file or assembly Micrososft.SqlServer.BatchParser,Version=12.0.0.0."



Possible Cause

If the assembly or its dependencies is not present in the VM.

Resolution

1. Install the Pre-Requisite installer given with the installation guide.

   or

2. Download and install the following packages manually:
   - SQLSysClrTypes.msi
   - SharedManagementObjects.msi
3. Install and check Report Server SCW setup.

Problem 32:
Cache rebuild does not run automatically.

Resolution

Run the cache rebuild manually. Refer to Installing Cache Rebuild.

Problem 33:
After updating the application from 2023.3 to 2023.4, if you are using WIS authentication, manually update the web.config file.

Resolution

- Take a backup of the existing file to ensure the configuration is preserved.
- After installation is completed, redo the updates to the **WIS web.config** as per the original configuration document, mainly pointing the **AssertionConsumerHandlerUrls** to the right addresses.

Problem 34:
Integration Service Server issues due to port change.

Resolution

As part of 2023.4 integration service is running as a separate service, hosted on port 1213 by default.

- If value for Integration Service Server is 80, change it to 1213.
- If the value for https port is 443, change it to something else.
- Ensure to have a separate port and not the same as other appdomains.

Problem 35:
License Server Landscape issues such as login issue with error message "Landscape is not defined in License Server" or "Unable to Load License".

Resolution

1. Run the following query:

```
SELECT * FROM .[dbo].[Frs_LS_LicenseServerLandscape]
```

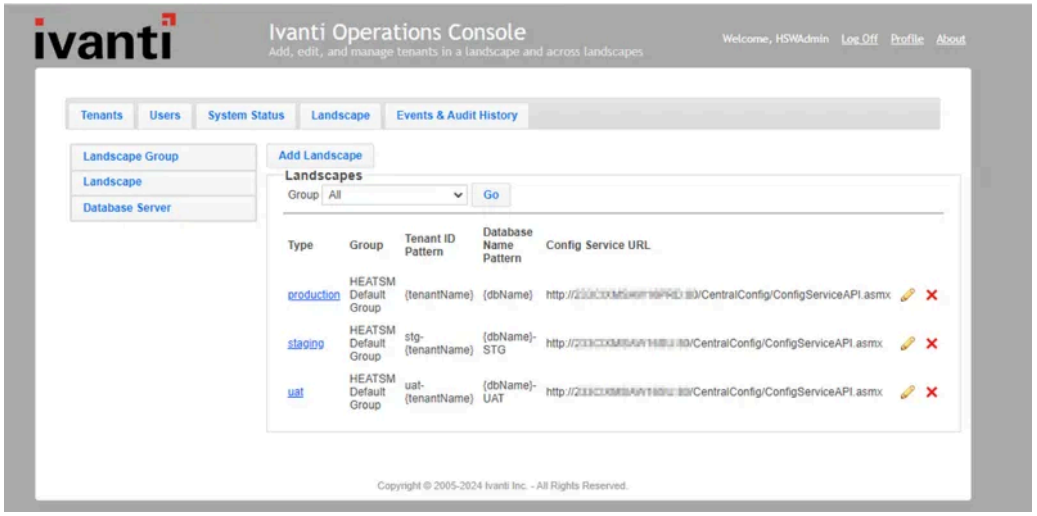
```
"select * from Landscape"
```

> Run both the above queries from the config tenant.

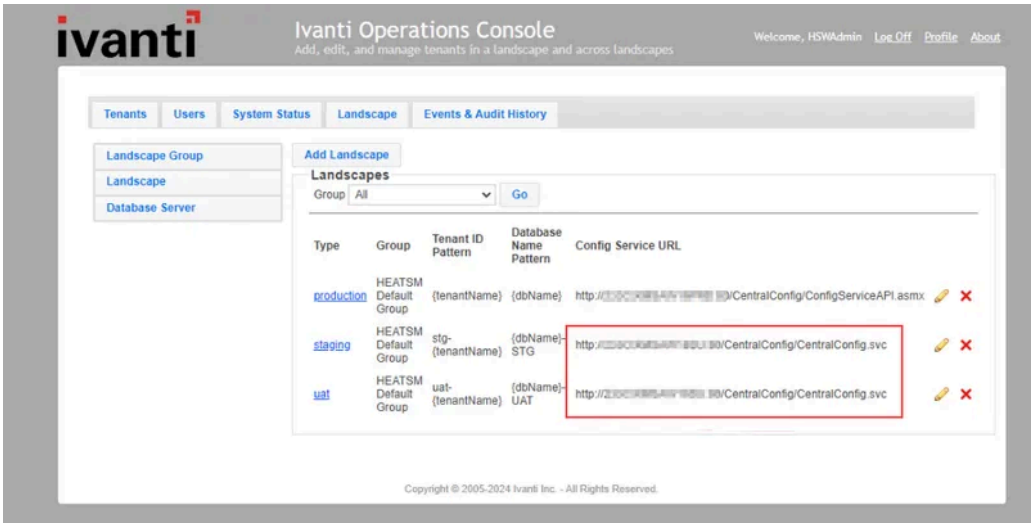
2. Ensure that the value in **ConfigServiceUrl** field is valid (check if the service definition loads when adding it in a browser). If not, update it to a valid central config url, for example, http://domainname/Centralconfig/CentralConfig.svc .

If using OpsConsole, follow the resolution below:

3. Check the landscape configuration from the DB or through ops console. If it is similar as shown the image below, that is if it has - /ConfigServiceAPI.asmx at the end, update those specific landscapes to have /Centralconfig/CentralConfig.svc route instead.



After update, the landscape configuration should be as shown the below image:



4. Restart IIS and login into both AppServer and LicenseManager.

> The **CentralConfig.svc** file should only be present only on the landscapes where the upgrade is executed from.

Problem 36: Cannot find APIKey in Header.

Resolution

The **central-config-api-key** should be the same in all **appdomains appsettings.json** file and in **Frs_data_api_key** table in the ConfigDB.

Update the central-config-api-key in the respective appdomains **appsettings.json** file.

Problem 37:
Issue with ActionServices.

Resolution

Refer to **ActionServices Troubleshooting** topic.

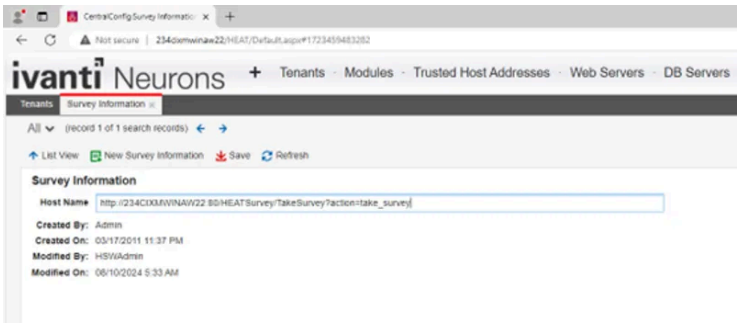
Problem 38:

Survey not opening - getting a 404 error when trying to open survey from incident or email.

Resolution

Open the Survey Information workspace from Config tenant.

Update URL in the Host Name field by removing "/Public" and ".aspx" as shown in the image below:



From {http/https}:///HEATSurvey/Public/TakeSurvey.aspx?action=take_survey to {http/https}:///HEATSurvey/TakeSurvey?action=take_survey

If the survey url opens from the machine where the application is hosted but not from other machines, make sure the {**hostname**} parameter has the fully qualified domain name instead of the machine name.

4. Configuration Database

Use the Neurons for ITSM configuration database (ConfigDB) for the following:

- To manage different instances (such as production, staging, and UAT) of tenants.
- To update your environment. The information in the ConfigDB is originally populated by the System Configuration Wizard, which is used when installing Neurons for ITSM.

> This is the master configuration database for your Neurons for ITSM system. Do not make any changes here, except in the few areas described in the 'Workspaces that Can Be Used' section. Making unauthorized changes to the ConfigDB can lead to disastrous results and may be unrecoverable. Use the ConfigDB with **extreme** caution.

Intended Audience

This guide is intended for advanced on-premise Neurons for ITSM - Version 2024.2 administrators and Ivanti Software personnel.

Document Organization

This help lists the workspaces in the ConfigDB and what, if any, tasks can be performed. This document contains the following sections:

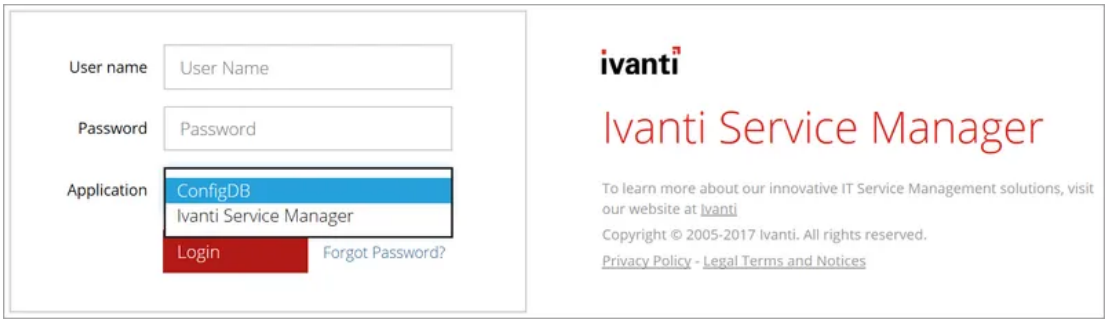
- Information about logging in. See **About Logging into the Configuration Database**.
- Workspaces that are also available in the Neurons for ITSM Service Desk Console or the Neurons for ITSM Configuration Console. See **Workspaces that Already Exist**.
- Workspaces that are for internal use only. See **Internal Use Only Workspaces**.
- Workspaces that are populated by the System Configuration Wizard. Do not make any changes to these workspaces. See **Workspaces Populated by the System Configuration Wizard**.
- Workspaces where you may make changes. See **Workspaces that Can Be Used**.

4.1. About Logging into the Configuration Database

To use the Neurons for ITSM configuration database (called ConfigDB), you must log in first. Only administrators can log into the ConfigDB.

By default, the system displays a drop-down menu allowing you to choose either ConfigDB (the Neurons for ITSM configuration database) or ISM (the Neurons for ITSM application database).

Logging in to the ConfigDB



If you do not see the **Application** drop-down menu, you must configure Neurons for ITSM to show it. For instructions on doing this, see the "Logging into Neurons for ITSM" section of the *Installation and Deployment Guide for* Neurons for ITSM .

4.2. Workspaces that Already Exist

The following workspaces found in the ConfigDB also exist in the Neurons for ITSM Console or the Neurons for ITSM Configuration Console. Therefore, they are not described in this document. For information about these workspaces, see the Neurons for ITSM online help within the application as well as at the Ivanti Product Documentation website. Click the "Service Manager" tile to see a list of the documents available.

- Employee
- All Logs
- Logging Configuration
- Notification
- Patch Log
- Encryption Key
- FRS Application Update Notes
- Ivanti Release Package
- Ivanti Release Project
- Ivanti Transaction Detail
- Ivanti Transaction Set
- Logon History
- Public Key
- Schedule Entry
- WS Mapping
- WS Proxy

4.3. Working With Features

- Adding a New Feature
- Changing the State of a Feature

Adding a New Feature

In Neurons for ITSM, you can add features. An example of a feature is Google Analytics. Follow these steps to add a feature:

1. Log in to the ConfigDB.
2. From the workspace selector bar, click More....
3. Select Feature. The system displays the **Feature** workspace.
4. Click New Feature.
5. In the **Feature Name** field, enter a name for the feature.
6. Click Save.

Changing the State of a Feature

Follow these steps to change the state of an existing feature.

1. Log in to the ConfigDB.
2. From the workspace selector bar, click More....
3. Select Feature Management. The system displays the **Feature Management** workspace.
4. Click New Tenant Feature.
5. Enter information into the fields:
    - In the **Tenant** field, enter or select the tenant that this feature applies to.
    - In the **Feature** field, select the feature.
    - In the **State** field, select a state from the drop-down list. You can choose from the following states: Unconditionally on, Trial period, Trial Completed, Disable.
6. Click Save.

4.4. Internal Use Only Workspaces

The following workspaces in the ConfigDB contain information that you can view, but that you should never change. These workspaces are only used by Ivanti for internal system use.

> Do not change the values in any of these workspaces! Changing any values can lead to system degradation.

- CMDB Import History
- Feature Management
- IM Client Agent Version
- Installer Types
- Logging Server Configuration
- Modules
- Remote Host Blocked List
- Service Names
- User Feature Settings

4.5. Workspaces Populated by the System Configuration Wizard

The following workspaces found in the ConfigDB contain information that was populated based on information entered in the System Configuration Wizard when Neurons for ITSM was installed.

We recommend that you do not change any of the values in these workspaces.

For complete information about the System Configuration Wizard and the Neurons for ITSM installation, see the *Installation and Deployment Guide for* Neurons for ITSM 2024

- Database Servers
- Log Operations Locations
- Integration Services Configuration
- Metrics Server
- Report Server
- Survey Information
- Trusted IP Addresses
- Web Servers

4.6. Central Config API Authentication

APIs in the Central Config can be accessed only by known users by authenticating the API call. The API Header will pass the API Key which will be authenticated and passed by the Central Config server. This prevents un-authorised users from accessing the APIs.

Install/upgrade Ivanti Service Manager System Configuration Wizard

On installing or upgrading the Service Manager System Configuration Wizard, the API Key is auto-generated in the Central Config DB. This key is used to to authenticate the API calls to the Central Config Server. However, the following should be monitored while installing/upgrading.

Verify the webconfig file

Once the installation/upgradation is complete, verify the webconfig file has the following:

- In the config section:

  <section name="CentralConfigApiKey" type="System.Configuration.NameValueSectionHandler" />

- In the new protected section:

  <CentralConfigApiKey> <add key="CentralConfigApiKey" value="" /> </CentralConfigApiKey>

Verify the appsettings.json file

Once the installation/upgradation is complete, verify that the appsettings.json file has the following:

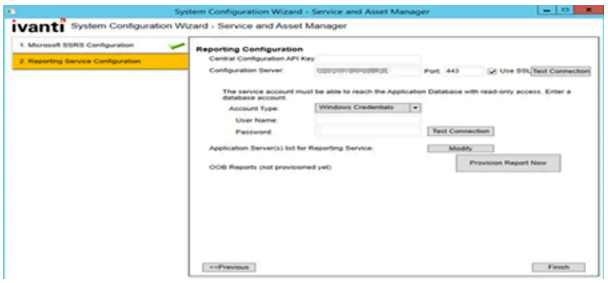
"central-config-api-key": "CAEFXXXX8C847D5XXXX698D8XXXXXX"

Update for Teams Bot Service

If you have installed Teams Bot Service, update the **CentralConfigApiKey** value in appsetting file. from C:\inetpub\TeamBotService/appsettings.json. Get the CentralConfigApiKey from the Central Config DB table (Frs_data_api_key).

Updates if Service Manager System Configuration Wizard and Service Manager Reporting Wizard are installed on different machines

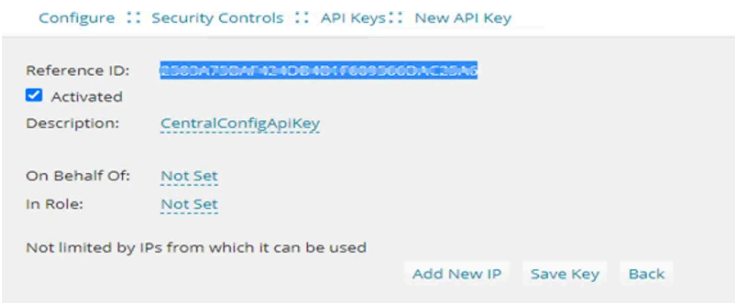
If the Service Manager System Configuration Wizard and Service Manager Reporting Wizard are installed on different machines, update the Centralconfig api key when installing the Reporting Wizard as shown in the below image. Get the CentralConfigApiKey from the Central Config DB table (Frs_data_api_key).



Updating the CentralConfigAPIKey

In case you wish to update/change the CentralConfigAPIKey, do so by following the below steps:

1. Stop all services that are referencing the centralconfig.
2. Log in to Service Manager with Admin credentials and open the Configuration console.
3. Select Security Controls > CentralCofigAPIKeyGroup and note down the description .
4. Delete the existing CentralConfigAPIKey and recreate a new key inside the CentralConfigAPiKeyGroup as shown in the below image.



5. Once the Key is created in the CentralConfig tenants, re-run the System Configuration Wizard to update the webconfig and appconfig files.
6. Restart your machine.

> The CentralConfigAPIKey should be unique, duplicate/multiple keys will break the feature.

Disabling the Centralconfig API Key Feature

Once the installation/upgradation is complete, verify the centralConfig appsettings.json file has: property “DisableApiKeyValidation”:”false” which need to be change to “True” as “DisableApiKeyValidation”:”true”.

1. Log in to the application with Admin credentials and open the Configuration console.
2. Select **Security Controls** > **API Key** and delete the **CentralConfigAPIKey**.

Ensure you **Delete** and not **De-activate** to disable.

Impacted webconfig file list:

AppDomains	Configuration Files
AppServer	Web.config
WorkFlow	WorkflowService.exe.config
Escalation	EscalationService.exe.config
email	EmailWindowsServiceapp.exe.config
bulkupload	KMBulkUploadTool.exe.config
integrationserver	IntegrationServiceHost.exe.config
systemconfigwizard	ServerConfigurationWizard.exe.config
release tool	ReleaseTool.exe.config
Frsloggingservice	FRSLoggingService.exe.config
metric	HEAT.MetricsServer.exe.config
message queue	MessageQueueServiceHost.exe.config
License service	LicenseServerWindowsService.exe.config
report provisioning	reportserver\ReportProvisioning.exe.config
Neurons	appsettings
Teams Bot Service	appsettings
DynamicWebServices	web.config
OpsConsole	web.config
FrsSurvey	web.config
FrsSurveyProxy	web.config
IM	IMServer\IMServices\AssetProcessor\Web.config
IM	IMServer\IMServices\DiscoProcessor\Web.config
IM	IMServer\IMServices\DiscoUtils\Web.config
IM	IMServer\IMServices\IMReadOnlyDataService\Web.config
IM	IMServer\IMServices\TaskProcessor\Web.config
IM	IMServer\WebServices\ClientTransportProcessor\Web.config
reports	C:\Program Files\Microsoft SQL Server\MSRS12.MSSQLSERVER\Reporting Services\ReportServer\Web.config

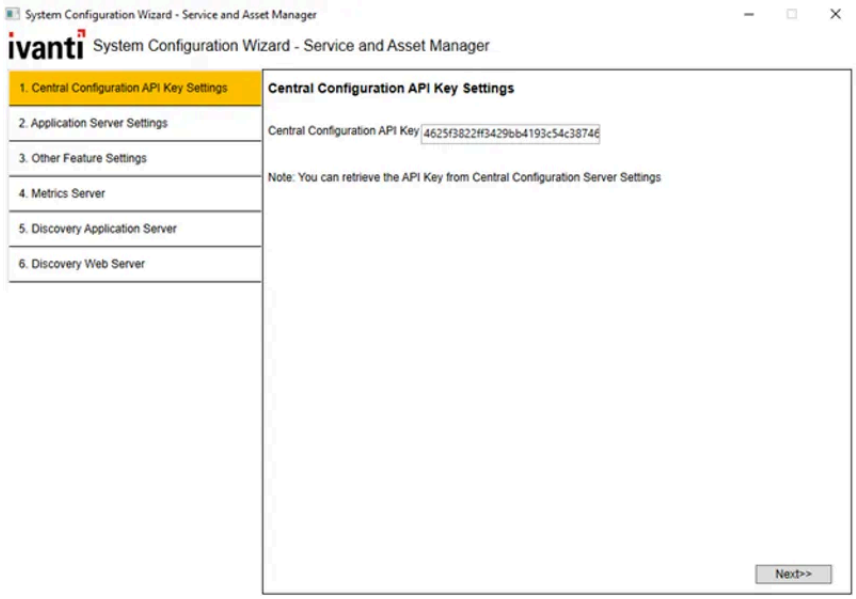
Impacted appsettings.json file of the appdomain

AppDomain
CCF
Appserver
EmailService
EscalationService
FRSSurvey
FRSSurveyProxy
InboundWebService
IntegrationServer
KMImportTool
LicenseManager
LoggingService
MessageQueue
MetricsServer
OpsConsole
ReleaseTool
SystemConfigurationWizard
WorkflowService
Reportserver
IMServer - IMServices
AssetProcessor
DiscoProcessor
DiscoUtils
IMReadOnlyDataService
IvantiCloudDataProcessor
TaskProcessor
WebServices - AgentTaskWs

Custom Installation of SCW

When customers try to install the Configuration Server in one machine and other components in another machine, user has to copy the Central Config API Key from Configuration Server and update the key in the **Central Configuration Settings** page as show in the following image.

Sample image of Custom Installation of SCW


System Configuration Wizard - Service and Asset Manager
ivanti System Configuration Wizard - Service and Asset Manager
1. Central Configuration API Key Settings
2. Application Server Settings
3. Other Feature Settings
4. Metrics Server
5. Discovery Application Server
6. Discovery Web Server
Central Configuration API Key Settings
Central Configuration API Key 4625f3822ff3429bb4193c54c38746
Note: You can retrieve the API Key from Central Configuration Server Settings
Next>>

4.7. Setting up the Teams Bot Integration

Setting up the Central Config API Key

1. Log in to the CentralConfig > **Configure Application** > **Security Controls** > **ApiKeys**.
2. Find the **CentralConfigApiKey** as shown below and copy the value.
3. Paste the copied value in the appsettings.json file for the CentralConfigApiKey. For example, *central-config-api-key"="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"*

Executing the PowerShell Script (from version 2023.4 onwards)

1. Download the zip file to a relevant folder in your machine.
2. Extract the zip file.
3. Open PowerShell as Administrator.
4. Go to the location where the PowerShell script is located, that is, the location where you extracted the zip file.
5. Run the script - `.\install.ps1`.
6. Provide relevant details to the below prompts:
    - Is the Environment SSL Enabled?
    - Please enter the ISM Tenant Id [example: ismtenant.yourdomain.com] only if environment is SSL enabled, otherwise provide app server IP address or host/domain name.
    - Please enter the Central Config Tenant Id [example: configtenant.yourdomain.com] only if environment is SSL enabled, otherwise provide server IP address or host/domain name.

   The configuration is done.

Executing the PowerShell Script (before version 2023.4)

1. Download the zip file to a relevant folder in your machine.
2. Extract the zip file.
3. Open PowerShell as Administrator.
4. Go to the location where the PowerShell script is located, that is, the location where you extracted the zip file.
5. Run the script - `.\TeamsBot.ps1`.
6. You will be prompted for the Appserver as well as the Central Config ipaddress/ Machine name/ localhost name. name/ localhost. Enter the appropriate Address/Machine name/localhost.

   The configuration is done.

Troubleshooting

Incorrect ipaddress/machine name/local host name (version 2023.4 onwards)

If you provide incorrect IP address/machine name/local host name, open the Appsetting.json file from the folder inetpub >Teams Bot Service verify and replace the value for the following:

- AppServerUri
- CentralConfigUri
- ConfigServiceClientUri

Example of the AppSetting.json file:

{ "JsonMaxDepth": 128, "MicrosoftAppId": "", "MicrosoftAppPassword": "",

"IPCMServiceName": "/ServiceAPI/IPCMService.asmx", "LogLevel": "DEBUG", "CacheTimeout": "30",

"isOnPremise": true, "central-config-api-key": "", "AppServerUri": "https://ism-onprem15-

tenant1.ivanticlouddev.com/HEAT", "NoOfFAQ": 2, "NoOfKnowledgeBase": 3, "Soap": {

"OpenTimeout": "2", "CloseTimeout": "2", "SendTimeout": "2",

"ReceiveTimeout": "2" }, "CentralConfigUri": "https://cfg-onprem15-

ism.ivanticlouddev.com/CentralConfig", "BuildVersion": "", "ConfigServiceClientUri": "https://cfgonprem15-
ism.ivanticlouddev.com/CentralConfig", "ISM_ConfigServiceClientName":

"api/centralconfig", "ConfigServiceClientName": "api/centralconfig", "UseInMemoryState": true,

"SecretStorageUri": "", "RedisStorageConfiguration": { "EnableRedisFlag": true,

"RedisConnectionString": "redis.redis.svc.cluster.local",

"sendmessagetochatservice": "reveivemessagefromteams", "closesocketsignal":

"closesocketsignal" }, "IocServices": [{

"LifetimeType": "1", "AssemblyName": "ServiceManager.SimpleStorageStrategy",

"ClassName": "ServiceManager.SimpleStorageStrategy.AzureBlobStorage",

"InterfaceName": "ServiceManager.SimpleStorageStrategy.ISimpleStorageStrategy" },

{ "LifetimeType": "1", "AssemblyName":

"ServiceManager.SimpleStorageStrategy", "ClassName":

"ServiceManager.SimpleStorageStrategy.SecretStorage.AppSettingSecretKey",

"InterfaceName": "ServiceManager.SimpleStorageStrategy.SecretStorage.ISimpleSecretStorageStrategy"

}, { "LifetimeType": "1", "AssemblyName":

"ServiceManager.AppServer.WebReference", "ClassName":

"ServiceManager.AppServer.WebReference.IPCMService", "InterfaceName":

"ServiceManager.AppServer.WebReference.IIPCMService" }, {

"LifetimeType": "1", "AssemblyName": "ServiceManager.CentralConfig.WebReference",

"ClassName": "ServiceManager.CentralConfig.WebReference.Rest.ConfigServiceClientJson",

"InterfaceName": "CentralConfig.Contract.IConfigServiceAPI" }, {

"LifetimeType": "1", "AssemblyName": "ServiceManager.Cache",

"ClassName": "HEAT.Cache.InMemory.InMemoryCache", "InterfaceName":

"HEAT.Cache.Contract.ICache" }] }

Incorrect ipaddress/machine name/local host name (before version 2023.4)

If you provide incorrect IP address/machine name/local host name, open the Appsetting.json file from the folder inetpub >Teams Bot Service and replace the AppserverIPAddress with the correct one.

Example of the AppSetting.json file:

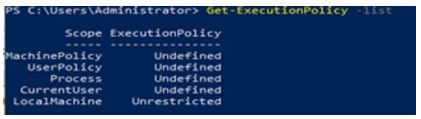
{"MicrosoftAppId"="";"MicrosoftAppPassword"="";"IPCMURL"= "http://$AppserverIPAddress/HEAT/ServiceApi/IPCMService.asmx"; "WorkflowURL"= "http://$AppserverIPAddress/HEAT/ServiceApi/WorkflowService.asmx"; "ConfigURL"= "http://$CentralConfigIPAddress/CentralConfig/ConfigServiceAPI.asmx"; "RetrieveTenantLogLevel_ws_url"= "http=//$CentralConfigIPAddress/CentralConfig/RetrieveTenantLogLevel.ashx"; "EnableCentralLogging"= false; "LoggingService_ws_url"= "http://$AppserverIPAddress/Heat.Logging.Service/api/LoggingService/HeatServiceManagementLogging"; "ElapsedSecondsToFlushLog"= 60; "ItemSizeToFlushLog"= 1000; "LogSettingCacheTimeoutInMinutes"= 5; "SendLogFileLocation"= "C:\logs"; "WriteLogFileLocation"= "C:\logs"; "SendLogWaitInterval"= 300; "WriteLogWaitInterval"= 300; "EnableLogging"= true; "CacheTimeout"= "30"; "isOnPremise": false; ”CentralConfigApiKey”=”” }

Make sure that Boolean values (true/false) don't not have double quotes.

To know the execution policy list

Run the command - `PS C: \Users\Administrator>Get-ExecutionPolicy - List`

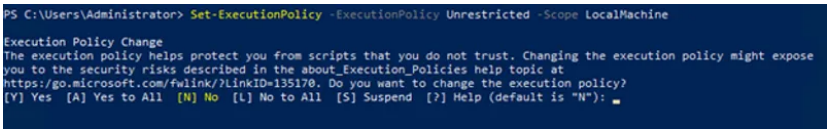
Sample image of the policy list



To set the execution policy

Once the PowerShell script is executed successfully, execute the command - `Set-ExecutionPolicy -ExecutionPolicy “PROVIDE PREVIOUS VALUE” -Scope LocalMachine` to set the execution policy.

Sample image of setting execution policy




```
Bash
```

4.8. Enabling the Action Service

The Action Service can only be enabled per tenant.

Configuring Redis for Action Service

To configure Redis for the Action Service, you have to open **appsettings.json** in the Action Service and enter the following:

```Bash
"RedisConnectionString": "<Redis_Server>:<Port_Number>"

"RedisSettings": {
"ExpirationTimespan": "0.00:15:00",
"ConnectionString": "<Redis_Server>:<Port_Number>,password=<PasswordOfRedisServer>,abortConnect=false"
}
```

For example:

```Bash
"RedisConnectionString": "host.docker.internal:6379"

"RedisSettings": {
"ExpirationTimespan": "0.00:15:00",
"ConnectionString": "host.docker.internal:6379,password=Password@123,abortConnect=false"
}
```

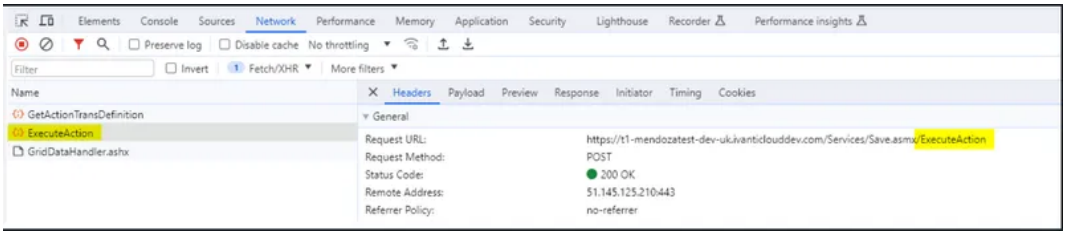
> A Redis server is required for the Action Service. For more details on installing Redis manually, refer **Setting up Redis**.

Enabling Action Service

- Set the **EnableActionService** option in Global Constants as `True`.
- Ensure the **ActionServiceUsage** option is **Disabled** in the Central Config. By default it is **Disabled**.
- Set the **DisableDirectActionServiceUsage** option as **Unconditionally ON** in the Central Config.

Verifying the functioning of Action Service

1. Login to a Neurons for ITSM tenant.
2. Navigate to the **Incident** workspace and open an existing Incident.
3. Open the chrome console > **Network** > **Headers**.
4. Execute a converted quick action. For example, **OOTB** > **More** > **Form Actions** > **Assigned Incident to Me**.
5. Verify if the below endpoint is being called.



Troubleshooting

Problem

After Upgrading, the Action Service is not working when the installation is using Windows Authentication Option.

Resolution

1. Check **IIS settings** > **Application Pool** > **HeatActionServicePool**.
2. Check **Identity Column** to ensure the **Identify Property** has the same value as all other services.

4.9. Workspaces that Can Be Used

There are very few workspaces in the ConfigDB that can be used by administrators. See the following topics for information:

- Configuring the Message Queue
- Configuring the Message Queue Handler
- Configuring Email
- Viewing All Logs
- Working With Customer Contacts
- Working With Tenants
- Configuring Manual Load Partitioning

4.9.1. Configuring the Message Queue

Use the **Message Queue Configuration** workspace to create and configure a message queue.

Follow these steps:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Message Queue Configuration. The system displays the **Message Queue Configuration** workspace.
3. Enter information into the fields.

Parameter	Description
Polling Interval (sec)	Specifies how often to check the message queue. The default value is 120.
Processor Threads	Specifies the number of threads. The value depends on the specifications (such as memory and CPU) of your system. The default value is 250.
Metadata Refresh Interval (min)	Specifies the interval for which to refresh the metadata pertaining to the tenant, which is the amount of time for which to retain the cache. After this amount of time, the system purges the cache and reloads it. The default value is 10.

4. Click Save.

4.9.2. Configuring the Message Queue Handler

Use the **Message Queue Handler** workspace to configure the message queue handler.

Follow these steps:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Message Queue Handler. The system displays the **Message Queue Handler** workspace.
3. Enter information into the fields.

Parameter	Description
Name	Name of the message queue handler web service.
Endpoint	The URL of the message queue handler web service to which queued tasks are dispatched. An example is http://IP_address/IntegrationService.svc.
Dispatch Method	The name of the web method that is implemented as part of the handler web service (which the message queue invokes to dispatch tasks). For example, the Neurons for ITSM XSLT email handler implements a web method called HandleMessage. NOTE: The name of the dispatch web method is case sensitive.
Batch Size	The maximum number of tasks that the message queue can dispatch to a message queue handler.
Active	Specifies if the message queue handler is on or off.
Priority	Specifies the order of this handler, in relation to any other handlers that are defined.
Process Timeout Interval (minutes)	Amount of time to wait for a response from the message queue handler before logging an error or before retrying, if you have not exceeded the number of attempts specified by the **Max number of attempts** parameter.
Include Data with Dispatch	Specifies whether to include the data when this dispatch web method is called. If you do not check this option, the message queue handler must call the dispatch web method to get the data.
Max number of Attempts	The maximum number of times to resend the data before logging an error.
Archive on Completion	Specifies whether to archive the message queue journal, which contains the tasks that the message queue handler has processed. Use this information for troubleshooting purposes. Enabled by default.
Purge Archive after (days)	Set to 30 days by default. The amount of days after which the archive is purged.
Description	A description of the message queue handler.

4. Click Save.

4.9.3. Configuring Email

Use the **Email Configuration** workspace to configure the inboxes for email.

Follow these steps:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Email Configuration. The system displays the **Service Provider Email Configuration** workspace.
3. Enter information into the fields.

Field	Description
Message Queue Handler Name	The name of the message queue handler to use. This must be the same name entered in the **Name** field in the **Message Queue Handler** workspace. See Configuring the Message Queue Handler.
Mailbox Poll Interval	The amount of time, in seconds, after which email configuration changes take affect.

4. Click Save.

4.9.4. Viewing All Logs

If there are any problems with the ConfigDB, such as email issues or workflow errors, they are reported in the logs. Review the logs to determine the underlying issue and to help resolve it.

- Setting the Log Level
- Viewing the Logs

Setting the Log Level

You can set the amount and detail of information in the logs by adjusting the Log Level. You can do this by going to the **Logging Configuration** workspace. See the Neurons for ITSM Online Help.

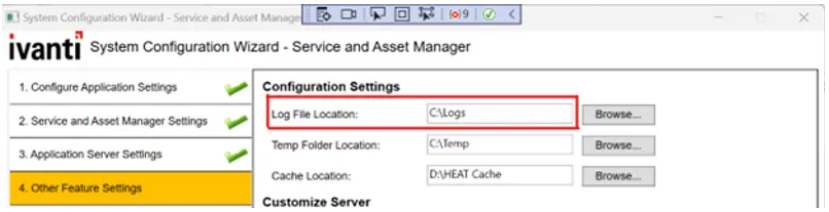
Configuring the Logs

All the logs related to the app domain will be stored in the following locations:

Configurable Logs

- In the step 4 of the System Configuration Wizard, enter the file location in the Log File Location.

  All the configurable logs pertaining to Configuration Wizard and AppServer will be stored in this location.



Non-Configurable Logs

These are logs that depend on the parameters specified in the **nlog.config** file or other AppDomain.

For example, in the **EscalationService appdomain**, go to the path - *HEAT Software|HEAT|EscalationService*, check the **nlog.config** file where the configuration of logs is done in the target node with the name - **logfile** as shown in the image below:

```
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <targets>
    <target name="console" type="Console" layout="${longdate}|${level:uppercase=true}|${logger}|${message}" />
    <target name="debugger" type="Debugger" layout="${longdate}|${level:uppercase=true}|${logger}|${message}" />
    <target name="logfile" type="File" fileName="/ism/logs/escalationsvc/${machinename}.ism.esc.svc.${date:format=MM-dd-yyyy-hh}.log"
  </targets>
  <rules>
    <logger name="*" minlevel="Debug" writeTo="console,debugger,logfile" />
  </rules>
</nlog>
```

For all other AppDomains listed below, the logs will be available in the following format - **C:\ism\logs\esclationssvc**.

- ActionService
- CentralConfiguration
- EmailService
- EscalationService
- FRSSurveyProxy
- FRSSurvey

- OpsConsole
- IntegrationServer
- MessageQueue
- InboundWebService
- LoggingService
- MatricsServer
- WorkFlowService
- AssetProcessor
- DiscoProcessor
- IMReadOnlyDataService
- IvantiCloudDataProcessor
- TaskProcessor
- WebServices - AgentTaskWs

Viewing the Logs

Follow these steps to view all of the logs associated with the ConfigDB:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select **All Logs**. The system displays the **LogsAll** workspace with the following information:

Field	Description
Log Entry Id	A unique ID for this log entry.
Log Time	The time at which the log entry was originally created on the server.
Log DB Time	The time when the log was uploaded into the database.
Client IP Address	The IP address of the service that generated the log, such as the workflow server.
SubSystem Id	The subsystem of the service that generated the log. (Each module has predefined subsystems. For example, for the email server, polling is a subsystem.)
Login Id	The login ID for the user who experienced the log event.
Tenant Id	The tenant instance that is experiencing the log event.
Error Code	The category of the error. An example is "trigger not found".
Current Role	The role assigned to the user if the error is generated by a user. If the error is generated by the system, this field is empty.
Host Name	The machine that is reporting the error.
Thread Name	Internal thread ID. Not applicable.

3. Double-click any log entry to view the log details.
4. To refresh the data, click **Refresh**.

Non-configurable logs that is logs that depend on the parameters specified in the **nlog.config** file are stored in the following path - HEAT Software\HEAT\EscalationService.

4.9.5. Working With Customer Contacts

This section contains the following topics:

- About this Workspace
- Viewing Customer Contacts
- Adding a Customer Contact
- Editing a Customer Contact
- Deleting a Customer Contact

About this Workspace

> This workspace is for deployments with multi-tenant configurations.

You can add, edit, or delete a primary contact for a particular tenant. This is the person you contact for all communications regarding the particular tenant.

This information is also listed in the **Account Information** workspace in the Neurons for ITSM Configuration Console.

Viewing Customer Contacts

Follow these steps to view information associated with customer contacts:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Customer Contacts. The system displays the **Contacts** workspace with the following information:

Field	Description
Login ID	The login ID for the customer contact.
Full Name	The full name of the customer contact.
Primary Email	The primary email address for the customer contact.
Primary Phone	The primary phone number for the customer contact.

3. Double-click any entry to view the details.
4. To refresh the data, click the refresh icon.

Adding a Customer Contact

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Customer Contacts. The system displays the **Contacts** workspace.
3. Click New Contacts. The system displays the **Contacts** page.
4. Enter information into the fields.
5. Click Save.

Editing a Customer Contact

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Customer Contacts. The system displays the **Contacts** workspace.
3. Double-click the entry to edit.
4. Change the entry.
5. Click Save.

Deleting a Customer Contact

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Customer Contacts. The system displays the **Contacts** workspace.
3. Highlight the entry to delete.
4. If there are dependencies on other items, the system display a confirmation message. Click Continue.

4.9.6. Working With Tenants

About the Tenants Workspace

> The information on this page is populated by the System Configuration Wizard.

Although there is a lot of information in this workspace, you should only do the following tasks from within this workspace:

- Reset the cache for a tenant. See **Resetting the Cache for a Tenant**.
- Add a certificate. If you want to use SAML authentication, you must upload a certificate and password so that end users can download it. See **Adding a Certificate to a Tenant**.
- Capture audit files from ISM Discovery, to help with troubleshooting. See **Capturing Discovery Messages for Debugging**.
- Configure how users attach files. See **Configuring Attachment Options**.
- Set metadata to read-only. See **Setting Production Metadata to Read-Only**.
- Set the login URL. See **Setting the Login URL**.

Resetting the Cache for a Tenant

Neurons for ITSM caches information about each tenant in the ConfigDB. Because of this, changes to the tenant, such as updating the status, database information, and so on, are not immediately reflected in the corresponding tenant. This can lead to situations where Neurons for ITSM allows a user to log into a tenant, even though the status of the corresponding tenant in the ConfigDB is set to closed.

To manually reset the cache for a specific tenant, do the following:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Tenants. The system displays the **Tenants** workspace.
3. Highlight the tenant to reset the cache for.
4. Click Reset Tenant Cache.

Adding a Certificate to a Tenant

> If your implementation includes multiple tenants, the certificate should be for the domain and not the specific tenant. For example, the certificate for Cloud tenants is for *.saasit.com, not for a specific tenant such as *mytenant*.saasit.com.

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Tenants. The system displays the **Tenants** workspace.
3. Double-click the tenant for which to add a certificate.
4. Click Add Certificate.
5. Navigate to the certificate location. Highlight it and click Open.
6. Enter the password for the certificate in the **Certificate Password** field.
7. Click Save.

Capturing Discovery Messages for Debugging

Perform the following procedure if you are using Discovery and you need to capture the audit files sent to the server from the Discovery client agents. After you capture the audit files, you can review them in a debug environment to find out more details about the problem. The logging can be very long, so be careful about using this feature. For more information, see the Neurons for ITSM online help.

8. Log in to the ConfigDB.
9. From the workspace selector bar, select Tenants. The system displays the **Tenants** workspace.
10. Double-click the tenant to configure logging for.
11. Check Log Failed IM Message.
12. Click Save.

Configuring Attachment Options

Perform the following procedure to configure how attachments are saved. You may need to change the format for storing files if users regularly store very large files, such as system log files. After you configure this, when a user saves an attachment to a record, the attachment is stored in the location that you specified here. For information about saving attachments as a file stream, see https://msdn.microsoft.com/en-us/library/gg471497.aspx.

We recommend that for system data, such as icons and images, you select Database for the **Attachment Save Type** field.

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Tenants. The system displays the **Tenants** workspace.
3. Double-click the tenant for which to configure attachment options.
4. For the **Attachment Save Type** field, select a type: **Database**, **FILESTREAM**, **File system**, **Amazon S3**, or **Azure Blob**.
5. For the **Attachment Path** field, enter the default path where attachments are saved.
6. Click Save.

Setting Production Metadata to Read-Only

If a user makes a change to the metadata in the production instance of the tenant, such as when configuring a workflow for a request offering, but does not make the same change in the UAT or staging instance of the tenant and then pushes the data from the UAT or Staging instance of the tenant to the production instance of the tenant, the data becomes corrupt and the workflow fails.

To avoid this, set the metadata on the production instance of the tenant to read-only. Follow these steps:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Tenants. The system displays the **Tenants** workspace.
3. Double-click the tenant for which to set the production metadata to read-only.
4. Check **Is Production Metadata Read-only**.
5. Click Save.

If a user tries to edit the workflow for a request offering, the system displays a message stating that the production metadata is read only and cannot be edited. See "Working with Request Offerings" in the Neurons for ITSM online help for more information.

Setting the Login URL

Set the login URL in the following scenarios:

- When configuring Neurons for ITSM Active Directory authentication using Windows Integrated Security (WIS). This feature allows users to access Neurons for ITSM without entering their user name and password. This procedure is only valid for the on-premises version of Neurons for ITSM.
- When configuring the Neurons for ITSM on-premises URL for mobile users.

Follow these steps:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Tenants. The system displays the **Tenants** workspace.
3. Double-click the tenant for which to set the login URL.
4. In the **Login Url** field, enter the URL where users go to log in.
5. Click Save.

Setting the Alternate Login URL (Vanity URL) for an MSP

Besides setting the login URL as described above, you can also specify an alternate login URL, also known as a vanity URL, for a Managed Service Provider (MSP).

Follow these steps:

1. Log in to the ConfigDB.
2. From the workspace selector bar, select Tenants. The system displays the **Tenants** workspace.
3. Double-click the tenant for which to set the alternate login URL (vanity URL).
4. At the bottom, click the **Alternate Login URL** tab.
5. Click New TenantUrlAlias. The system displays the **New TenantUrlAlias** dialog box.
6. In the **Url** field, enter the alternate login URL (vanity URL).
7. Click Save.

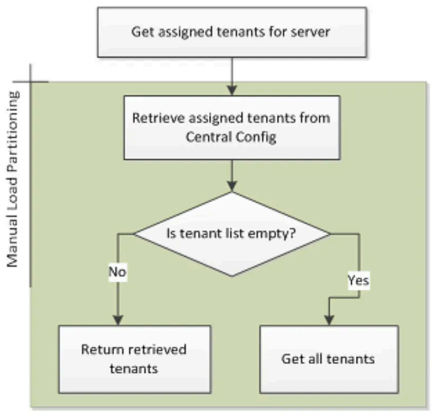
4.9.7. Configuring Manual Load Partitioning

About Manual Load Partitioning

Use the **Service Server** workspace to configure the manual load partitioning feature. The manual load partitioning feature allows you to allocate the load between workflow or email service instances based on your knowledge of the tenant load and server capacity.

When you start up the services, the workflow and email services retrieve the list of assigned tenants. The services only process the tasks for the assigned tenants. The system updates the list of assigned tenants in predefined time intervals. If the list of tenants is empty, the system falls back to the default behavior of processing all of the tenants.

Email Load Balancing Flowchart



> For the email service and workflow service, all load partitioning is done manually. Changes are configured in the **appsettings.json** file at the binary folder. By default **EnableLoadPartitioning** key remains false in the **appsettings.json**, enabling it disrupts the whole Workflow Service.

Assigning Tenants to the Workflow or Email Service

When you configure workflow or email service servers, ensure that at least one server is defined as the "catch all" server. A "catch all" server manages all of the live tenants, even if it does not have any tenants associated with it. Each host should have at least one "catch all" server. This server processes workflow and email events for all tenants.

For each server, you must enable either the email service, the workflow service, or both. If you do not enable a service on the server but the service is running, the service gets an empty tenant list and it runs as a "catch all" server.

If a service instance crashes or stops, the system deletes the partition details from the database and no other instance will pick these tenants except for the "catch all" server.

1. Log in to the ConfigDB.
2. From the workspace selector bar, click More....
3. Select Service Server. The system displays the **Service Server** workspace.
4. Click New Service Server.
5. Enter the host name in the **Host Name** field.
6. If the email service will run on this server, check Is Email Service Enabled.

7. If the workflow service will run on this server, check Is Workflow Service Enabled.
8. If the server is a catch all server, check Is Catch All.
9. If the server is not a catch all server, do the following:

   a. Click the **Tenants** tab.

   b. Click Link.

   c. Highlight a tenant from the list and click Select.
10. Click Save.

Viewing the Results of the Manual Load Partitioning

You can view the results of the manual load partitioning in one of two ways:

- Viewing the INFO log for a service. See **Setting the Log Level for the Workflow or Email Service** and **Viewing the Workflow or Email Manual Load Partitioning**.
- Viewing a report of the load partitioning through Microsoft SQL. See **Viewing a Report of the Manual Load Partitioning**.

Setting the Log Level for the Workflow or Email Service

To configure the logs, do the following:

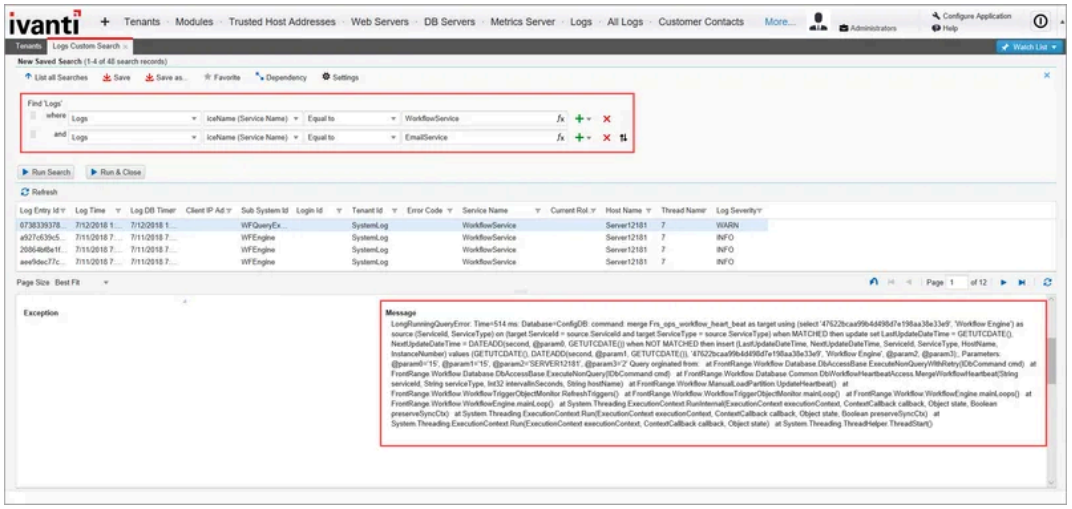
1. Log in to the ConfigDB.
2. Open the **Logging Configuration** workspace.
3. Open the **WorkflowService** service.
4. Change the value of the **Log Level** field to INFO.
5. Open the **EmailService** service.
6. Change the value of the **Log Level** field to INFO.
7. Click Save.

Viewing the Workflow or Email Manual Load Partitioning

After you configure the logs, to view the results, do the following:

1. Log into the ConfigDB.
2. Open the **Logs** workspace.
3. Use a saved search to show all logs with a service name of WorkflowService or a service name of EmailService.

   Logs Saved Search



4. Verify that the tenants listed under the current assigned tenant list match the linked tenants for this server.

Viewing a Report of the Manual Load Partitioning

The workflow or email service retrieves the assigned tenants and updates the **Frs_ops_workflow_heart_beat** and **Frs_ops_workflow_partition** tables in the ConfigDB.

Before you begin, start the workflow or email service. Keep the current session.

Run the following query in Microsoft SQL on the ConfigDB to see the details of the services that are assigned to each tenant:

SELECT ServiceType, HostName, InstanceNumber, TenantId

FROM Frs_ops_workflow_heart_beat heartbeat

JOIN Frs_ops_workflow_partition partition

ON heartbeat.ServiceId = partition.ServiceId

The following is an example of the partitioning details:

Service Type	Host Name	Instance Number	Tenant ID
Workflow Engine	CA-L02552	1	ConfigDB, ITSM_7_Daily_Build
Email Engine	CA-L02552	1	ConfigDB, ITSM_7_Daily_Build

4.9.8. Firebase Configuration for Mobile Push Notification

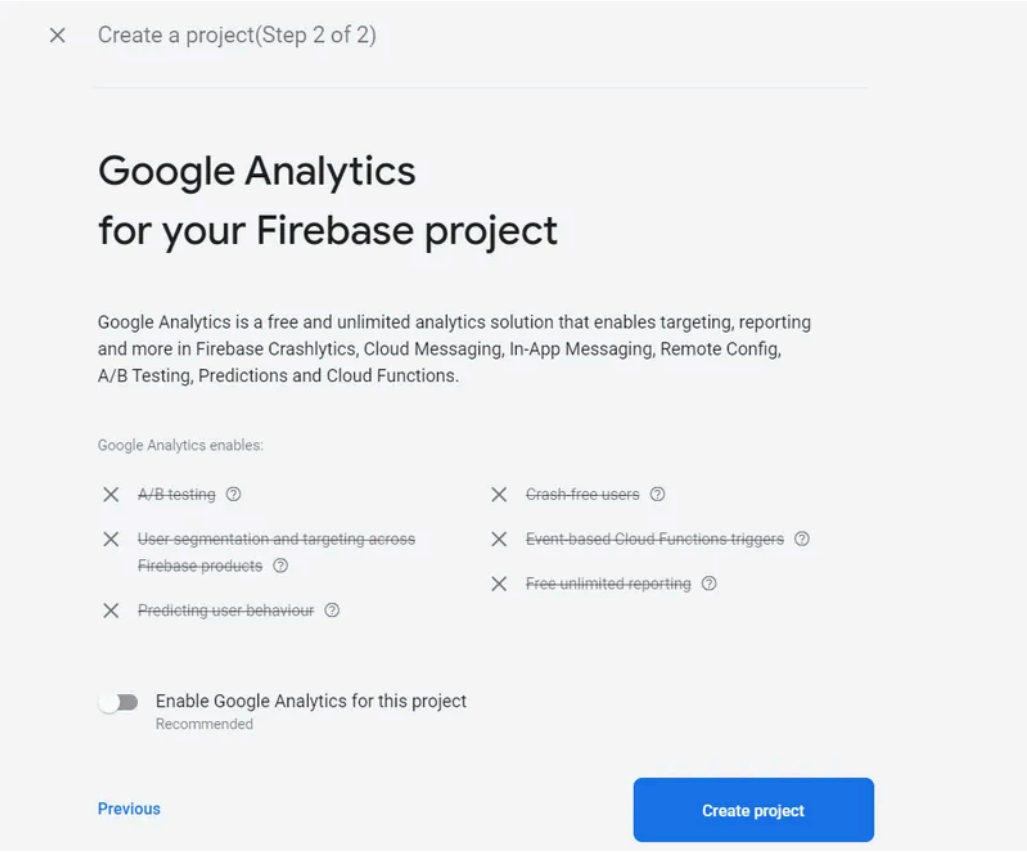
A new workspace - **FCM Configuration** is added to ConfigDB. The following are its sections:

- **Project Id**: Project Id of the firebase which we going to configure in future step. This Id is used by the server to send the push notification.
- **Server Key**: Unique key that is present inside the firebase project. This key is used by the Server to send the push notification.
- **Client configuration for Android**: json configuration which is used by android mobile to generate FCM token. This configuration will be present in Firebase project we need to add in config Database.
- **Client configuration for iOS**: Configuration which used by iOS device to generate FCM token.

The following steps should be performed for Mobile Push Notification to work:

Creating a new Project in Firebase

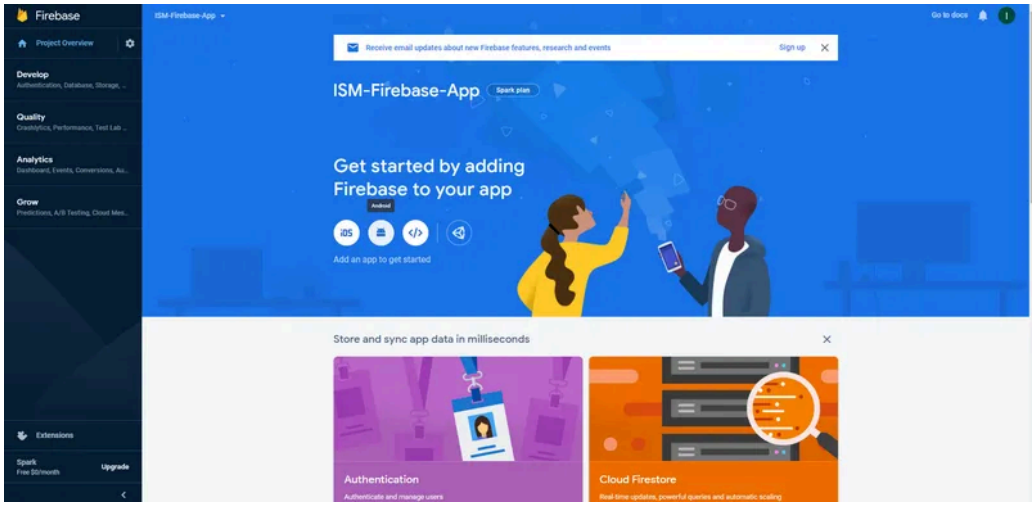
1. Navigate to https://firebase.google.com/ to create a new project. Since Firebase is from Google, you need to sign into your Gmail account so the Firebase project is associated with your Gmail account.
2. Navigate to firebase.com and click **Go to console** on the top right corner of the page.
3. Click the **Create a project** tile (for new Users) or **Add Project** (for existing users) in the Firebase.
4. Type the project name, select the **I accept the firebase terms** check box and click **Continue**.
5. Disable Google Analytics and click **Create Project**.



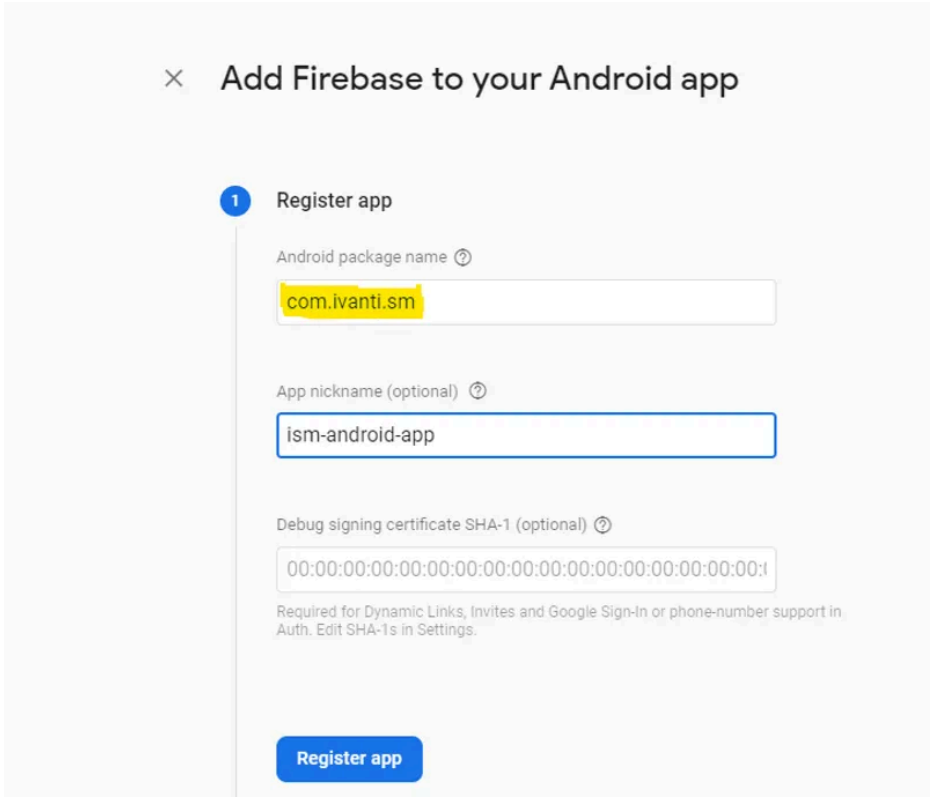
Configure iOS and Android app in Firebase

In this step, you will create iOS and Android app in the firebase project.

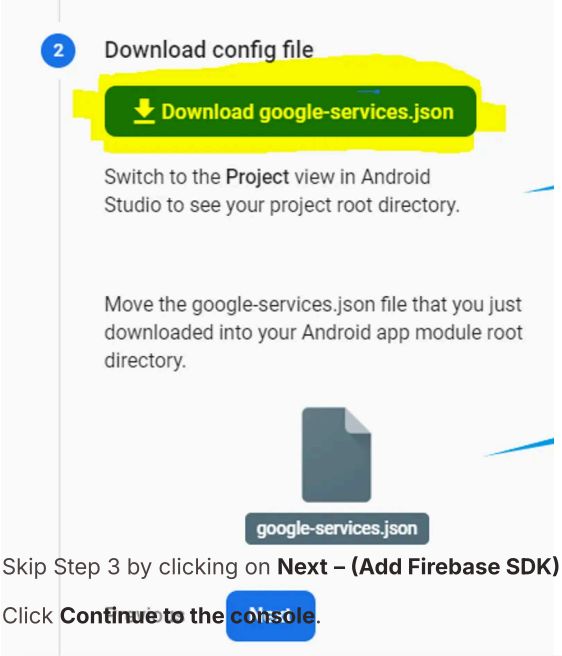
1. Navigate to the newly created project.
2. Click on the **Android** icon to create new Android app.



3. Enter the name of the package - it should always be **com.ivanti.sm**" in the **Android Package name** and enter any name in **App Nickname**. Ensure the package name is right and click on **Register app**.

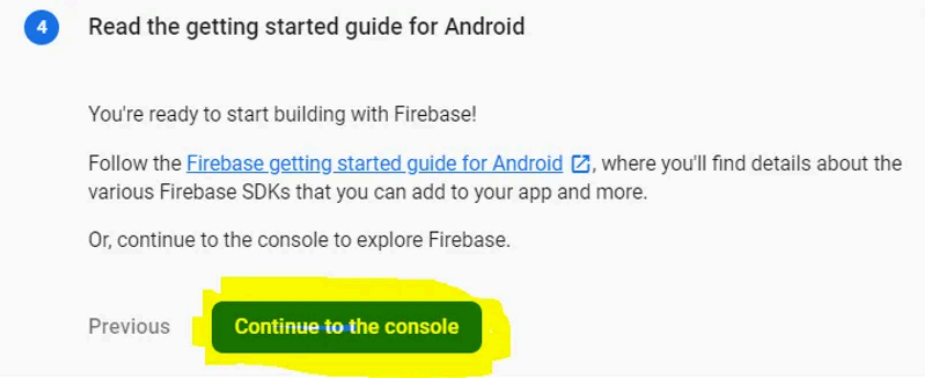


4. Click on **download google.service.json** which is json configuration for Android. Download this file and click **Next**.



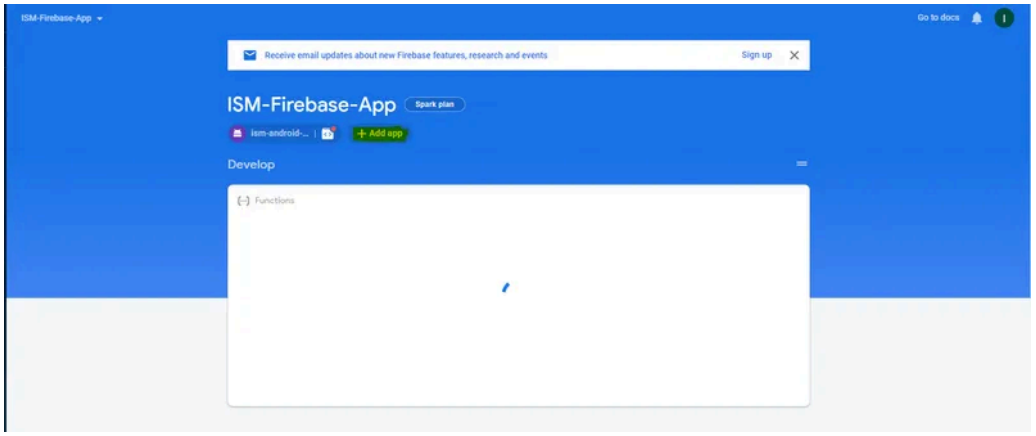
5. Skip Step 3 by clicking on **Next – (Add Firebase SDK)**
6. Click **Continue to the console**.

> If you see "**Run your app to verify installation**" step then you can click on "**Skip this step**" and then click **Continue to console**.

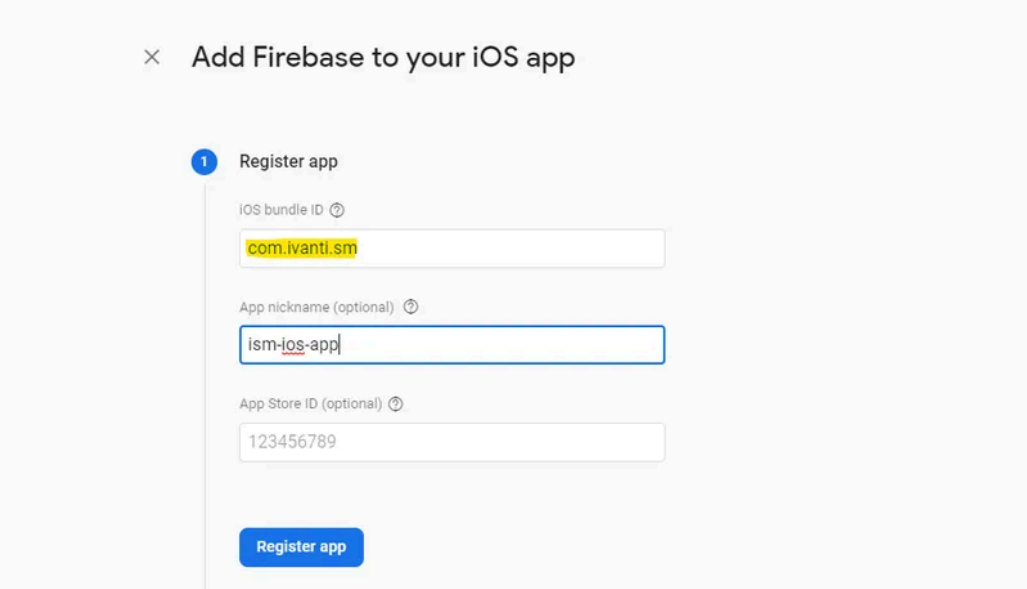


Once all these steps are completed, you have the Android app ready in the Firebase project.

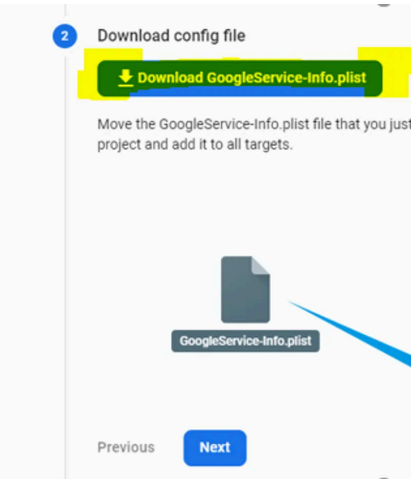
7. Now, do the same for iOS.
8. Click on **Add app** again in the Firebase project and select iOS.



9. Specify the same package name **com.ivanti.sm in** the iOS bundle ID, enter the **App nickname** and click on **Register app**.



10. Click on **Download GoogleServiceInfo.plist** which contains the configuration for iOS device. and click **Next**.



11. Skip Step 3 by clicking on **Next – (Add Firebase SDK)**.
12. Skip Step 4 by clicking on **Next – (Add Initialisation code)**.
13. Click **Continue to Console** in step 5.

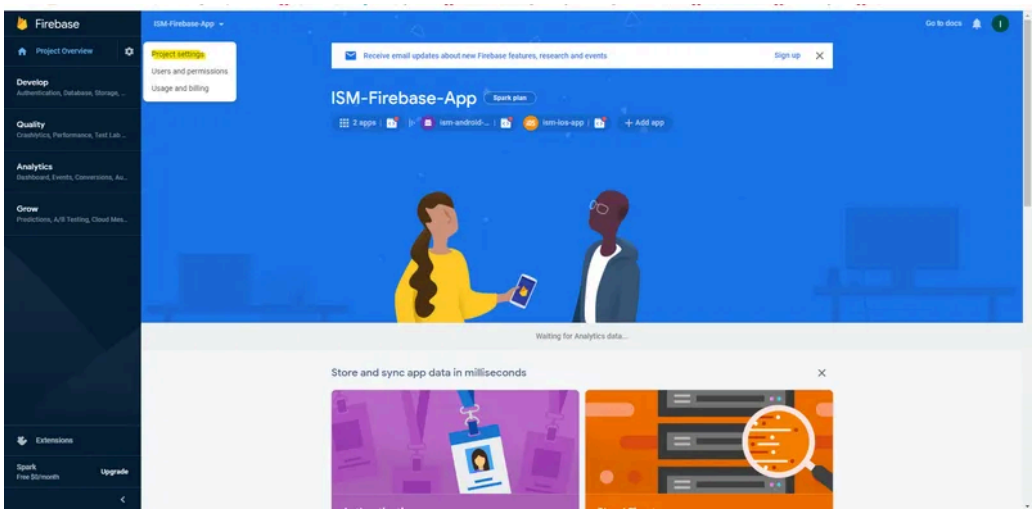
> If you see Run your app to verify installation step, click **Skip this step** and then click **Continue to console**.

Once these steps are completed, you have iOS and Android app configuration is ready in the Firebase.

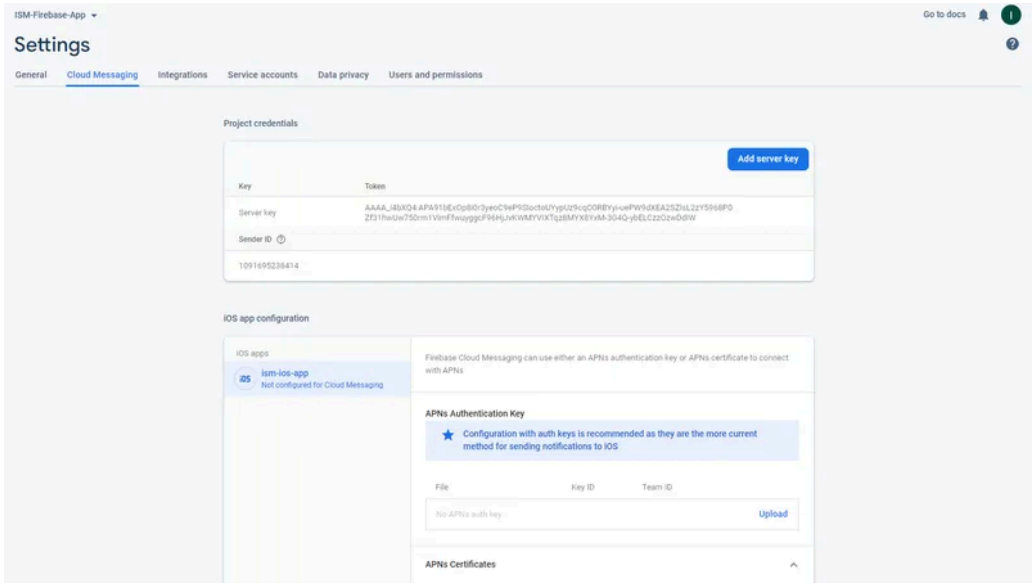
Apply iOS Certificate for iOS app

Ivanti will provide the APNs Certificate for iOS app. You can find the certificate at Ivanti Market Place.

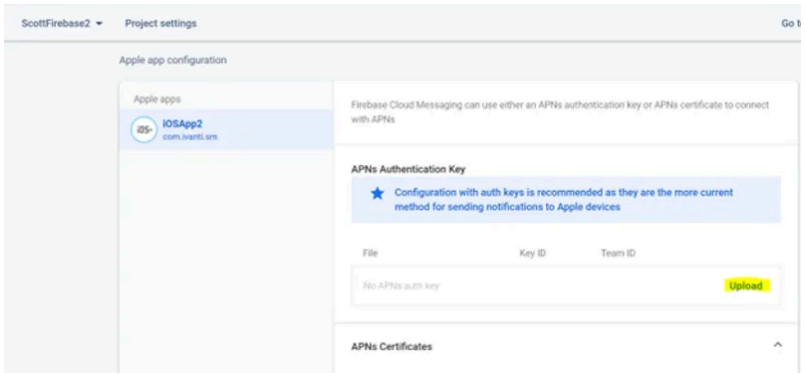
1. Click the **Setting** button from top left and click on **Project settings**.



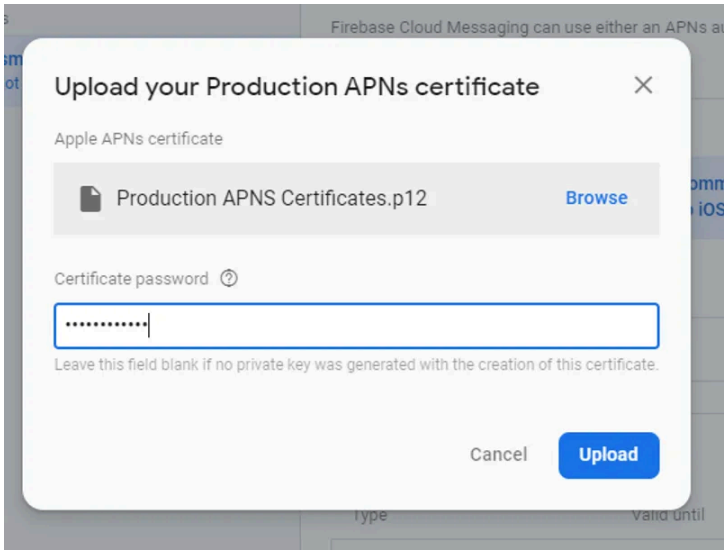
2. Click the **Cloud Messaging** tab.



3. Scroll down to the **APNS Authentication Key** section and click the **Upload** button.



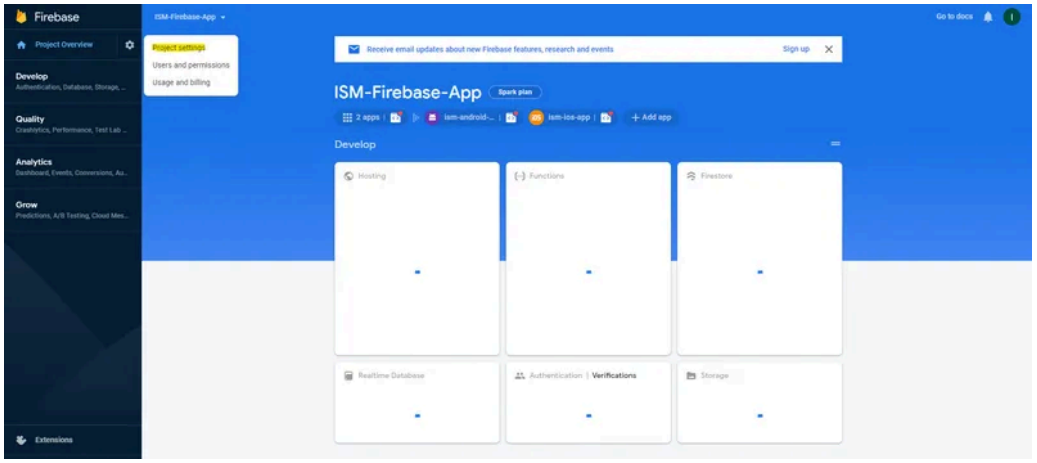
4. Browse to the AuthKey_V65XKX7498.p8 file.



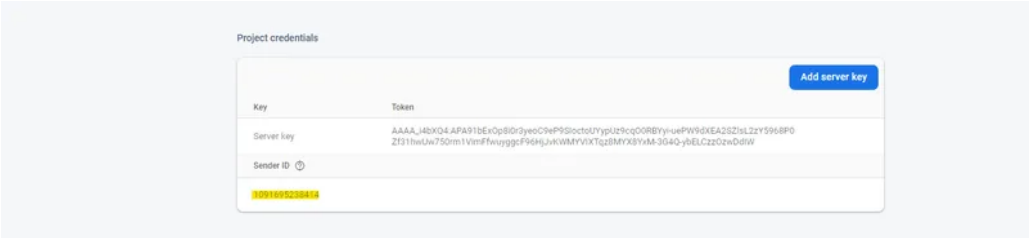
5. Enter the following details:
    - Key ID: V65XKX7498
    - Team ID: B7FW4Y3UP6

Configure Firebase in Config Database of ISM

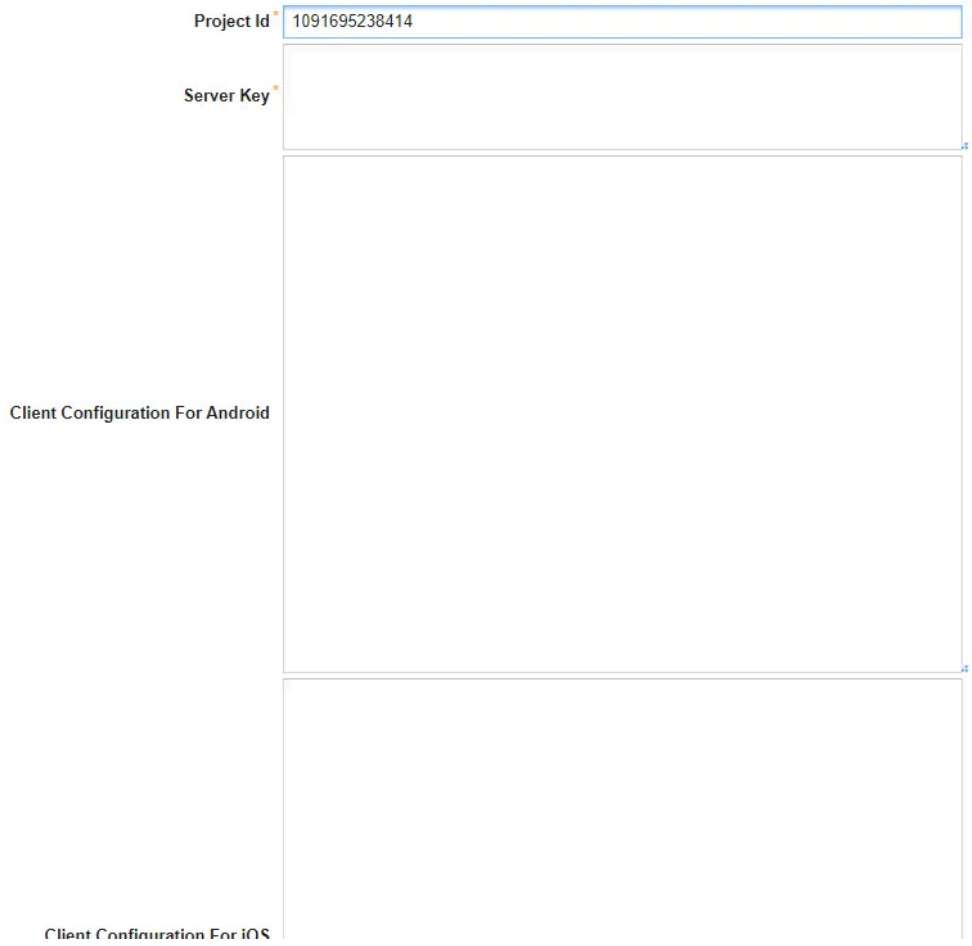
1. Navigate to **Project settings** from the main page of Firebase project.



2. Navigate Cloud Messaging Copy the Sender ID.

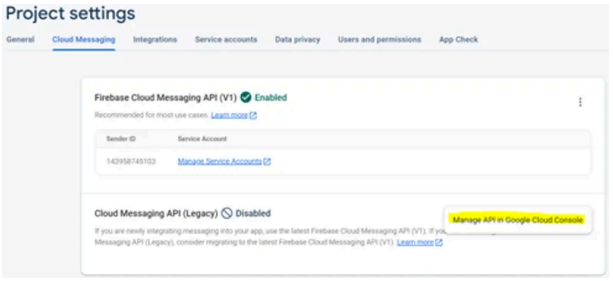


3. Go to **ISM CentralConfig**, open **FCM Configuration** workspace and paste **Sender ID** which is copied to the **Project ID** in workspace.

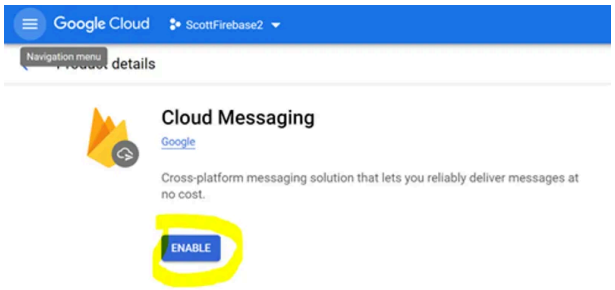


4. Copy the **Server Key** from the **Cloud Messaging** tab.

   a. Under the Cloud Messaging API (Legacy) **Disabled** section, select the ellipses and the option **Manage API** in the Google Cloud console:

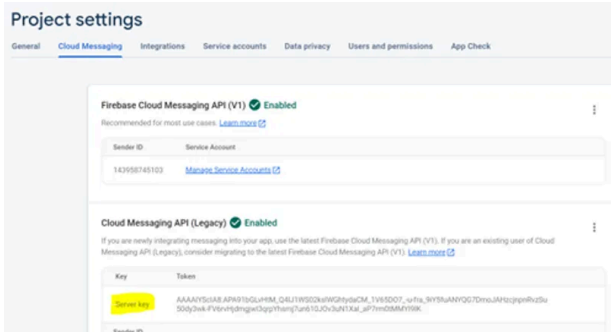


b. Select the **Enable** button for Cloud Messaging.

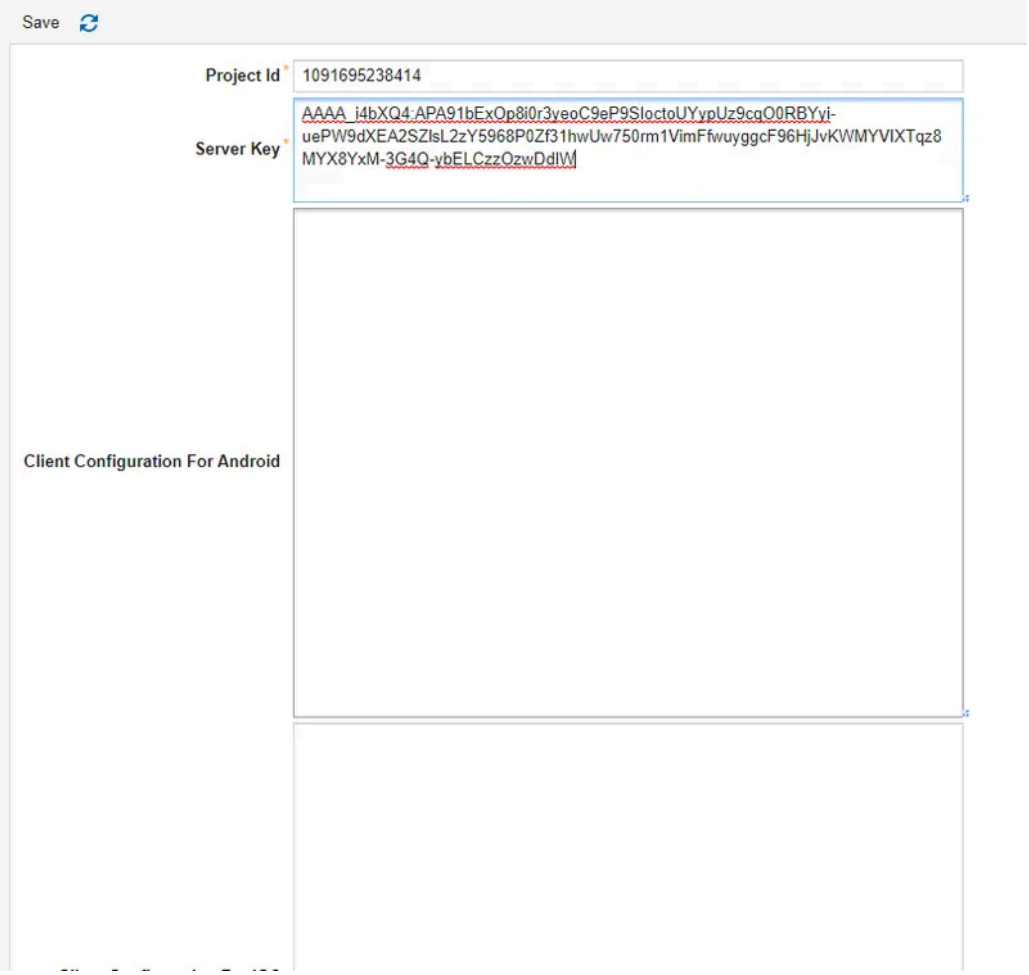


c. Go back to the browser where the console is open and refresh the browser.

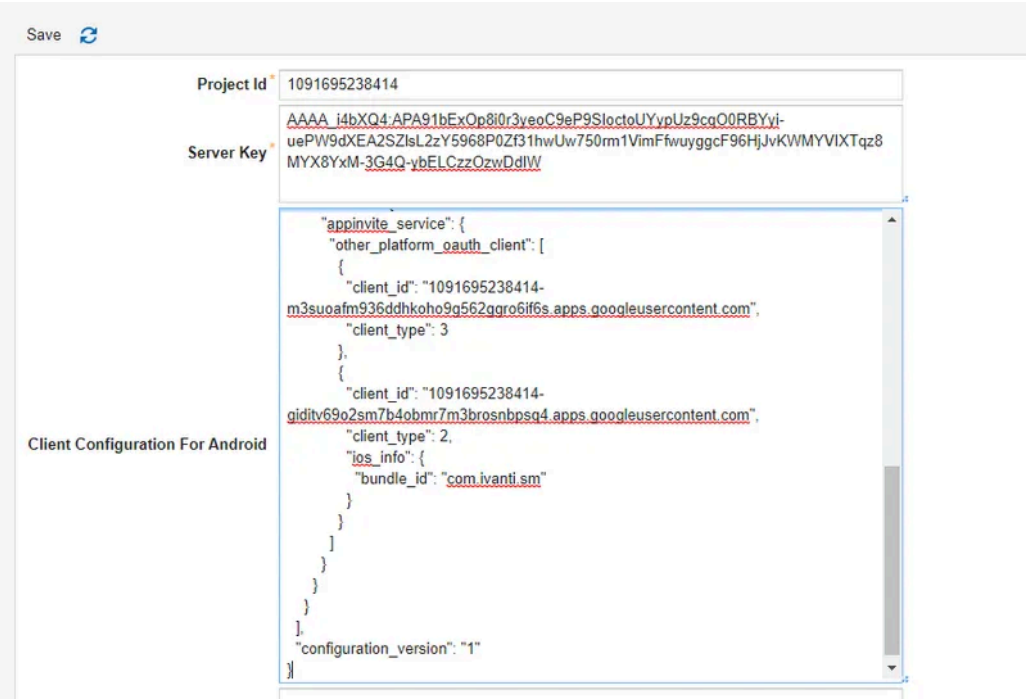
Under Cloud Messaging there should be a Server Key available.



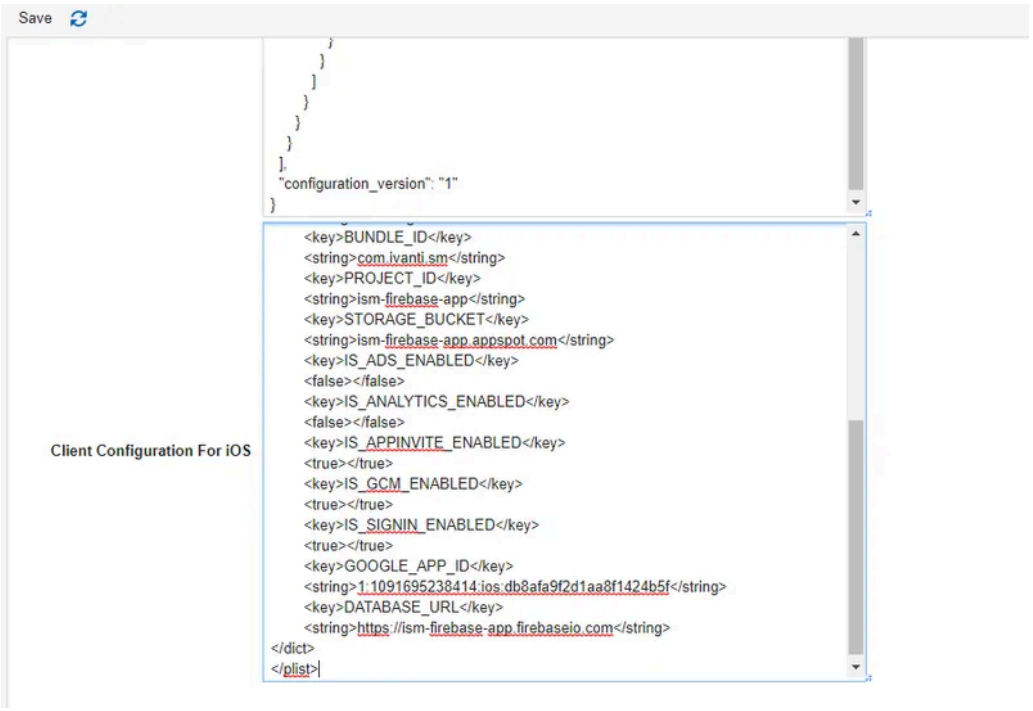
5. Paste the **Server Key** in **FCM Configuration** workspace.



6. Copy the entire content from **google-service.json** which is downloaded from Step – 3 and paste in the **Client Configuration** for Android.



7. Finally, you need to add the **iOS FCM configuration** in **config DB**. Copy the entire content from **GoogleService-Info.plist** which is downloaded in step 3 and paste it in the **Client Configuration for iOS** and **Save**.



4.9.9. Decommissioning FTP and File on Shared folder Integration

Currently, ITSM customers can import data from FTP and Shared Path locations. Since these sources pose a security threat to the cloud environment, restrictions are added to the use of these options. These restrictions are feature flagged which can enable or disable the options available to an end user either while importing or exporting data to ITSM.

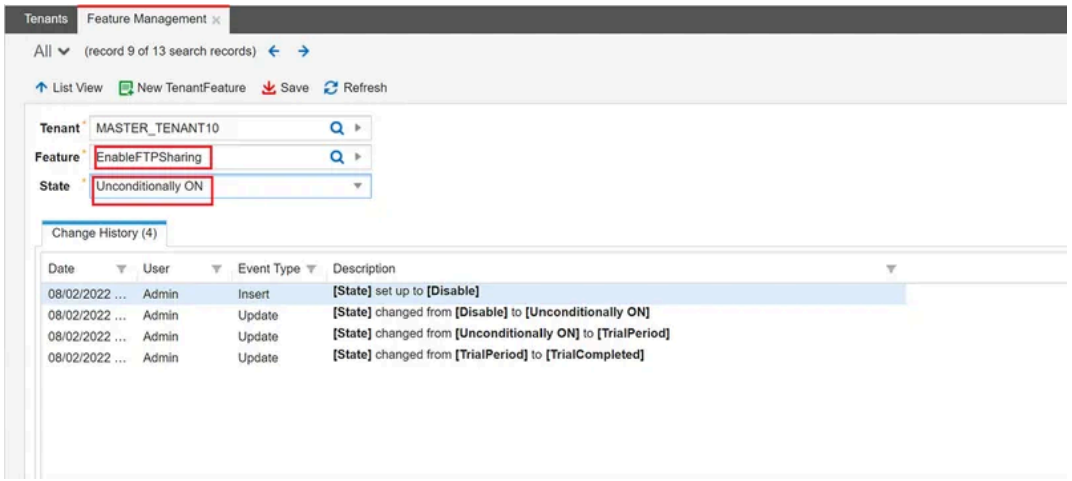
- Both FTP and File on Shared Folder controls are disabled using the feature flag from 2022.3 on wards. These feature flags can be turned off by the Cloud Ops in the Config DB under Feature Management workspace.
- The feature flag is not turned off to make sure both FTP and File on Shared Folder controls are still available and customer can migrate to Secure FTP without impacting their automation. However, it would be temporary.
- It's highly recommended to move your file upload related automation from FTP and File on Shared Folder location to Secure FTP on priority. Refer SecureFTP configuration documentation further.

Steps to enable or disable the feature flag

Navigate to the **Feature Management** Business Object in the Config DB and search for your tenant feature.

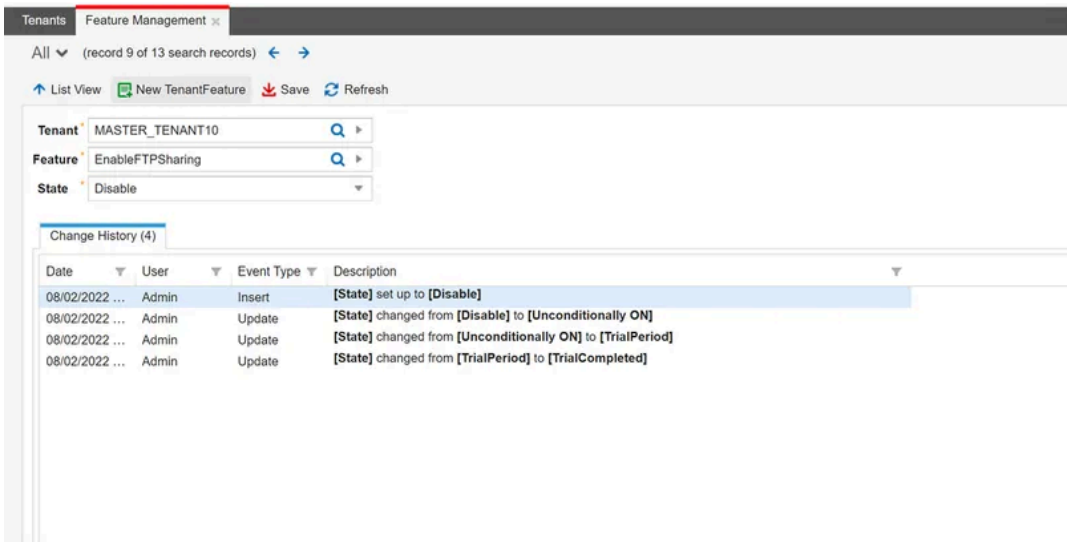
1. Once you open the feature, set the **State** as **Unconditionally ON** to enable the feature.

   Feature flag on



2. Set the **State** as **Disable** or **Trial Completed**, this disables the feature.

   Feature flag off



Post Feature Configuration

1. From the Configuration console navigate to **Data Import Connections** under **Integration tools**.
2. Click **Add new** and select the **Connection Type** field.
    - When the feature is enabled - in the **Connection Type** field drop-down list, **FTP** and **File on Shared Folder** options are available.
    - When the feature is disabled - in the **Connection Type** field drop-down list, **FTP** and **File on Shared Folder** options are not available.
3. Similarly, the **Location** field in the **Data Export Connections**,
    - When the feature is enabled, the **Location** will show **FTP** and **Secure FTP**.
    - When the feature is disabled, the **Location** will show only **Secure FTP**.

5. Performance Tuning

The *Performance Tuning Guide for* Neurons for ITSM describes how to configure Neurons for ITSM including the platform, the Neurons for ITSM application server, and the Neurons for ITSM application database, to optimize performance for Neurons for ITSM .

Intended Audience

This document is intended for system administrators.

To perform the procedures described in this document you should have:

- Expert knowledge of Neurons for ITSM, platform, business objects, definition sets, and the Ivanti Service Manager Configuration Console. The Configuration Console is the interface where you apply changes to the databases to give structure to Ivanti Service Manager.
- Working knowledge of database structure and terminology.
- Working knowledge of the Microsoft Windows operating system.
- Working knowledge of the Microsoft .NET architecture.
- Working knowledge of Microsoft SQL Server Management Studio.

List of Topics

This document contains the following sections:

- **Server and Connection Tuning**: Describes how to configure servers and the connections between them in Ivanti Service Manager to optimize performance.
- **Platform and Application Tuning**: Describes how to configure Ivanti Service Manager and its platform to optimize performance.
- **Database Tuning**: Describes how to tune the Ivanti Service Manager databases for optimal performance.
- **Performance Monitoring**: Lists common performance monitoring parameters.
- **Troubleshooting - Performance Tuning** : Describes how to diagnose and fix common performance issues.
- **Deleting Inactive Tables and Records**: Describes how to delete inactive tables currently residing in the Ivanti Service Manager databases.

5.1. Server and Connection Tuning

This section describes how to configure servers and the connections between them in Ivanti Service Manager to optimize performance.

- Ensuring that Hardware and Software Prerequisites are Met
- Optimizing Network Utilization and Bandwidth
- Deactivating Unused Web Servers in the Ivanti Service Manager Configuration Database
- Working with Log Files and Logging Levels
- Configuring the Application Pool Recycling Schedule

Ensuring that Hardware and Software Prerequisites are Met

Hardware and software requirements for Ivanti Service Manager are listed in the *System Requirements and Compatibility Matrix for Ivanti Service Manager*. Verify that all components in your environment meet those requirements.

Optimizing Network Utilization and Bandwidth

Recommendations for optimal Ivanti Service Manager performance are:

- Latency of 110 ms or less. See Checking Database Latency and Moving Indexes to a Separate Disk for an example Microsoft SQL script that you can execute to check latency.
- A minimum of 1.5m bits/second in bandwidth between the Ivanti Service Manager application server and remotely located client computers.

Deactivating Unused Web Servers in the Ivanti Service Manager Configuration Database

To improve performance, deactivate any unused web servers from the Ivanti Service Manager configuration database. Follow these steps:

1. Log into the Ivanti Service Manager configuration database.
2. Open the **Web Servers** workspace.
3. Click **List View** to see a list of all of the web servers.
4. Open the web server to deactivate.
5. Uncheck Server is Active.
6. Click Save.

5.1.1. Working with Log Files and Logging Levels

Log files for all services, such as workflow and escalation, can provide valuable information for performance tuning.

We recommend that you set the log levels to error. You can set the log level to debug for troubleshooting, but it is very verbose so we do not recommend using that level on a regular basis.

Follow these steps to change the log level for the **WorkflowService** and **EscalationService** logs:

1. Log in to Ivanti Service Manager.
2. Open the **Logging Configuration** workspace.
3. Open an entry.
4. From the **Log Level** field, select a log level.
5. Click Save.

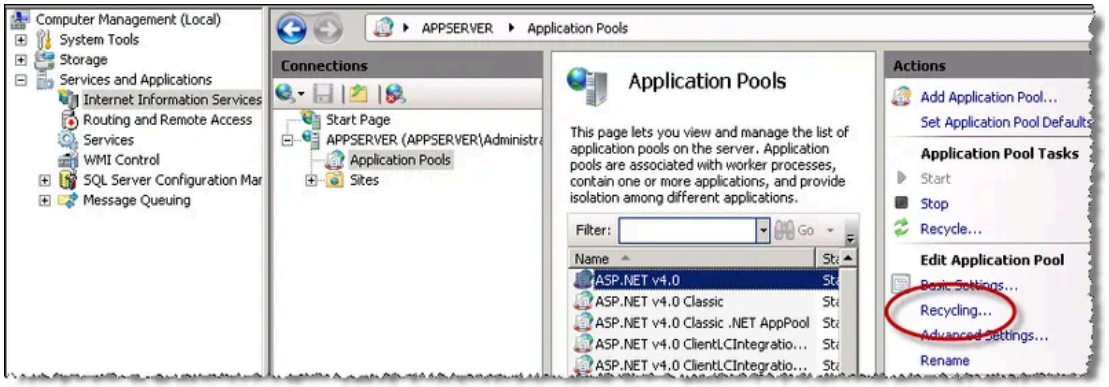
5.1.2. Configuring the Application Pool Recycling Schedule

We recommend that you schedule the application pool recycling to occur at a specific time rather than at an interval. Setting a specific time lets you schedule the recycling for off-peak times when performance is least likely to be impacted.

To configure the application pool recycling schedule, do the following:

1. Open the **Computer Management** panel by going to **Start > Control Panel > Administrative Tools > Computer Management**.
2. In the **Computer Management** panel, double-click **Services and Applications** and double-click **Internet Information Services (IIS)**.
3. In the **Connections** panel, double-click Application Server and double-click **Application Pools**.
4. In the list of application pools, highlight an application pool and click **Recycling...** located in the **Edit Application Pool** area.

Configuring the Application Pool Recycling Schedule



5. In the **Recycling Conditions** dialog box, check **Specific time(s)** and specify an off-hours time for the recycling to occur.
6. Repeat step 4 and step 5 to specify recycling schedules for the other application pools.

5.2. Platform and Application Tuning

This section describes how to configure Ivanti Neurons for ITSM and its platform to optimize performance.

- About the WAN Environment
- Planning and Scheduling Maintenance
- About Reviewing, Closing, and Deleting Records
- Tuning Business Rules and Workflows
- Best Practices for Dashboards and Layouts
- Improving Back-End Processing
- Using Event and Error Log Files for Troubleshooting
- About Using Combo Boxes Sparingly
- Evaluating Slow Running Queries
- About Data and Log Files
- About Snapshot Isolation Levels

About the WAN Environment

Applications built on the Ivanti Neurons for ITSM platform are commonly used over a WAN link. Whether deployed in a remote data center or used from branch offices, users expect performance reasonably similar to that of the LAN environment. Following the practices outlined in this guide result in a well performing application over the WAN that closely resembles performance on the local network.

To address poor performance over a WAN, it is important to clearly understand the problem. Though low bandwidth can have an impact, the foremost issue affecting WAN performance is latency, the time it takes data to travel from one endpoint to another. The higher the latency of the WAN link, the longer it takes data to traverse the link. High latency results in delays that can cause users to wait minutes for simple operations to complete.

To combat the higher latency of a WAN environment, Ivanti Neurons for ITSM was designed to make fewer “chunky” calls, rather than frequent smaller “chatty” calls. In other words, instead of retrieving little bits of data in individual requests, the system retrieves larger data sets in a single request. This well-established design principle reduces the overhead of traversing high-latency links, resulting in much improved application performance.

There are certain configurations and features within Ivanti Neurons for ITSM that can affect the behavior of the application, causing it to be more or less chatty, specifically, caching business objects and definitions and using script expressions. This guide covers these areas in detail and provides guidelines for keeping these areas in check.

This section does not describe how to fix network or WAN problems. Rather, this section focuses on ensuring that Ivanti Neurons for ITSM is configured to behave in a manner that produces acceptable performance on a well performing WAN.

5.2.1. Planning and Scheduling Maintenance

Create and follow a regular maintenance plan. Performing regular, ongoing maintenance is crucial to ensuring optimal system performance. At a minimum, a maintenance plan should include the following:

- A schedule for deleting records and tables. See **Deleting Inactive Tables and Records**.
- Running a tuning advisor tool to determine index tuning actions and then performing those actions. See **Database Tuning**.
- Scanning for duplicate indexes and then removing the duplicates. See **Checking for Duplicate Indexes**.
- Configuring database auto-growth. See **Setting the Value for the Database Auto-Growth Parameter**.

Depending on your system requirements, it is likely that you will perform additional activities as part of a maintenance plan.

The following is an example maintenance plan:

Month	Maintenance Task
January	• Evaluate the current archival plan and modify it as necessary. • Record performance metrics to establish a baseline. • Run the Microsoft SQL tuning advisor to determine recommended index changes. • Apply recommended index changes. • Scan for and delete duplicate indexes. • Check for license renewal requirements.
February	• Evaluate the current archival plan and modify it as necessary. • Troubleshoot errors reported in the event log and message queuing.
March	• Evaluate the current archival plan and modify it as necessary. • Audit log level and location settings. • Review database auto-growth and if necessary reset it to an appropriate static value.
April	• Evaluate the current archival plan and modify it as necessary. • Run the Microsoft SQL tuning advisor to determine recommended index changes. • Apply recommended index changes. • Scan for and delete duplicate indexes.
May	• Evaluate the current archival plan and modify it as necessary. • Troubleshoot errors reported in the event log and message queuing.
June	• Evaluate the current archival plan and modify it as necessary. • Record performance metrics and compare them with the recorded baseline.
July	• Evaluate the current archival plan and modify it as necessary. • Run the Microsoft SQL tuning advisor to determine recommended index changes. • Apply recommended index changes. • Scan for and delete duplicate indexes.
August	• Evaluate the current archival plan and modify it as necessary. • Troubleshoot errors reported in the event log and message queuing.
September	• Evaluate the current archival plan and modify it as necessary. • Review database auto-growth and if necessary reset it to an appropriate static value.
October	• Evaluate the current archival plan and modify it as necessary. • Run the Microsoft SQL tuning advisor to determine recommended index changes. • Apply recommended index changes. • Scan for and delete duplicate indexes.
November	• Evaluate the current archival plan and modify it as necessary. • Troubleshoot errors reported in the event log and message queuing.
December	• Evaluate the current archival plan and modify it as necessary. • Record performance metrics and compare them with the recorded baseline.

Month	Maintenance Task
	• Update infrastructure design plans and other documents. • Update system growth expectations.

About Reviewing, Closing, and Deleting Records

It is not uncommon for systems to have hundreds of thousands of active incident records that no longer need to be open and active. For example, if an incident has not been modified for several months, it can probably be closed.

Dashboard parts and saved searches may query these inactive records daily. Closing records that are older than a specified age (for example, three months) prevents them from being queried by dashboard parts and saved searches, which can significantly improve dashboard and search loading performance. Deleting closed records can also reduce the load on database server infrastructure. Additionally, deleting workflow history and instance tables prevents the workflow engine from having to query them.

We highly recommend that you implement a regularly occurring process to identify records that can be closed and deleted.

You can use service level agreements to automatically trigger a notification when an active record has been open for a specified amount of time. To do this, assign a default service level agreement to all services that do not have an active one. In the service level agreement, set the escalation to notify the owner when an active incident record has been open and active for a certain number of days.

Deleting closed and inactive records can reduce the load on database sever infrastructure. See **Deleting Inactive Tables and Records**.

5.2.2. Tuning Business Rules and Workflows

The following sections describe how to tune business rules and workflows to maximize performance. Implementing these practices can significantly improve overall system performance and reduce deadlocks and timeouts caused by the workflow engine.

- Disabling Inactive Business Rules
- Disabling Inactive Workflows
- Deleting Workflow Tables
- Validating Email Addresses in Notification Workflows

Disabling Inactive Business Rules

Review all active business rules. If a business rule is no longer used, disable it by removing its trigger and updating the rule description to disabled.

Disabling Inactive Workflows

Whenever a workflow is triggered, the system adds it to the event queue where it waits to be processed. Reducing the number of workflows waiting to be processed in the event queue improves performance. Review all active workflows. If a workflow is not used, disable it and update is description to disabled.

Deleting Workflow Tables

It is not uncommon for workflow history tables to contain hundreds of thousands of records. Workflow instance tables can also contain large numbers of records. Deleting workflow history and instance tables prevents the workflow engine from having to query them. Deleting workflow history and instance tables can significantly improve event table performance.

For details about how to deleting tables, see Deleting Inactive Tables and Records.

We recommend that you delete workflow tables on a regular basis (such as one or more times per week, if feasible).

Validating Email Addresses in Notification Workflows

If a notification workflow containing an invalid email address is triggered, event queue resources are wasted while the invalid email address is evaluated and processed. To prevent this situation, add a condition to notification workflows so that email addresses are validated before the workflow is triggered.

5.2.3. Best Practices for Dashboards and Layouts

You can improve Ivanti Service Manager performance by following the dashboard and layout best practices described in these sections:

- Dashboard Best Practices
- Layout Best Practices

Dashboard Best Practices

Because dashboards are created from multiple dashboard parts, they usually execute multiple saved searches when they are opened or updated. You can significantly improve performance by following these best practices:

- Ensure that dashboards display only active records, and that searches configured in dashboard parts do not search for closed or completed records.
- Disable or increase the duration of automatic refresh on all active dashboard parts.
- Use the fewest possible dashboard parts to create a dashboard (no more than four whenever possible).
- Wherever possible, add date filters and remove the all option.
- Wherever possible, remove memo fields from grids.
- Enable auditing only when necessary.

Layout Best Practices

Ensure that tabs in a workspace exist only if they are absolutely necessary. Workspace tabs that contain counters can consume significant resources. If a tab contains a counter, Ivanti Service Manager executes a query to return the number of records available on that tab. Each tab that generates a query adds to the time it takes for the parent workspace to load.

Improving Back-End Processing

This section describes how to tune stored procedures, triggers, and file import processes to improve performance.

- Stored Procedures and Triggers
- File Import Processes

Stored Procedures and Triggers

We recommend that you configure stored procedures and triggers outside of Ivanti Service Manager to avoid any unnecessary problems.

Stored procedures often consist of complex searches that query multiple database tables. A deadlock can result if a stored procedure is scheduled to run too frequently. Wherever possible, minimize the use of frequently scheduled stored procedures and triggers that query primary business objects such as incident, problem, change, journal, task, and other primary business objects. If possible, do not run these procedures at intervals of less than five minutes. If a frequently scheduled stored procedure is necessary, we recommend that you run it outside of normal business hours.

File Import Processes

If there are too many files to process or import in too short of a time (which might occur if the creation of a new record generates multiple queries), system performance can be significantly impacted.

Wherever possible, schedule the file import process to run outside of normal business hours.

Using Event and Error Log Files for Troubleshooting

Microsoft event logs and message queuing error logs are often helpful in determining common configuration errors, especially with regard to the email listener and file import process. We recommend that you review these logs when you troubleshoot performance issues.

5.2.4. About Using Combo Boxes Sparingly

- About Using Combo Boxes
- Creating a Pick List

About Using Combo Boxes

Do not use combo boxes for validating business objects that have a large number of rows. The maximum number of rows a combo box can display is 200. If there are more than 200 rows, the system does not return the excess rows. If a business object has more than 200 rows, we recommend using a text box with a **Search** dialog box.

To effectively validate business objects with more than 200 rows, perform one of the following:

- Change the business object from a combo box to an associated item selector. Access this function from the field control toolbar.
- Constrain the combo box field to validate using another field to reduce the number of rows returned. For example, constrain the **Employee** field to be constrained by the **Department** field, so that when validating the **Department** field, only employees from the department selected are shown.

Creating a Pick List

1. From the Configuration Console, click **Build > Pick Lists** to open the **Pick Lists** workspace. The system displays a list of pick lists.
2. Click **Add New...**. The system displays the **Add New Validation List** page.
3. Enter information into the fields.

Field	Description
List name	The name of the pick list to be stored.
Display name	The name of the pick list to be displayed in Ivanti Service Manager.
Get list data from	Check Business Object and select a business object from the drop-down list.
Display field	The name of the field to display in the pick list.
Value field	A stored field name. Select from the drop-down list.
Sort by field	The field by which to sort. Select a sorting value, either ascending or descending.

4. Add constraints to the pick list to restrict the data presented. Click the **add new** icon to add a constraint formula. This formula is based on the parameter selected in the **Get list data from** field.
5. Click Save.

See the Ivanti Service Manager online help for additional information about creating and modifying a pick list and its values.

5.2.5. Evaluating Slow Running Queries

Queries that take a long time to execute can manifest themselves just about anywhere in Ivanti Service Manager. Dashboards, saved searches, and viewing a business object are all areas impacted by slow running queries. With some familiarity with the tools available, tracking down and fixing these problems is a relatively straight forward task.

- Identifying Problem Queries
- Improving Saved Search Query Performance

Identifying Problem Queries

If queries run slowly, use the Microsoft SQL Server profiling tools to find out which queries are the problem. See Tuning Indexes for more information.

Improving Saved Search Query Performance

Saved searches are used in many places throughout Ivanti Service Manager, especially in dashboards and workspaces. Saved search queries can be complicated because they can involve related data and typically include criteria for more than just a single field. For this reason, dealing with performance problems for a saved search can be a bit more involved. Constructing saved searches in the most efficient way possible can significantly improve performance.

You can create a saved search, modify a saved search, delete a saved search, add a saved search as a favorite, and find saved searches. For more information about using the saved search feature, see the “Using Saved Search” topic in the Ivanti Service Manager online help.

> You can use the CONTAIN operator and LIKE (SQL format) operator in your search query, but this can result in slower query performance. The position of the wild card characters in the query determines the performance and index usage. Hence, your search query should have the wild card characters positioned correctly to improve the query performance.

We recommend the following:

- Using “Begin with”, “Not begin with” and “Not Null” in saved searches by adding Index to fields used in Saved Search. See " About Creating Indexes Using the Configuration Console, Not Third Party Tool " on page 25 for information on how to create indexes using the Ivanti Service Manager database.
- Minimizing sorting and grouping in grids.
- Creating index fields for tables frequently used in saved searches to reduce database access time. Use the Microsoft SQL Server profiling tools to find problem queries and to help identify indexes that can improve performance. See the Ivanti Service Manager online help for information about creating indexes.

About Data and Log Files

Microsoft SQL Server databases generally contain two types of files:

- Data files, which usually use the .mdf extension. These files contain the database data.
- Log files, which usually use the .ldf file extension. These files contain log data which can be verbose.

As a best practice, we recommend that you use house these files on different volumes.

About Snapshot Isolation Levels

- About Snapshot Isolation Levels
- Using Read Committed Snapshot Isolation (RCSI)

About Snapshot Isolation Levels

Isolation levels control how two or more transactions running simultaneously are isolated from each other in terms of locking and blocking resources. The isolation level determines the level of concurrency and data consistency. Ivanti Service Manager uses the following isolation levels:

- Read committed: This is the default transaction isolation level in Microsoft SQL Server. This isolation level prevents "dirty reads" which occur when a transaction is allowed to read data from a row that was modified by another transaction that has not yet been committed. This level acquires shared locks to prevent other transactions from modifying the data during a read operation by that transaction. A shared lock can be acquired only if there is no exclusive lock (required for data modification) by other transactions; this ensures it reads only committed data.
- Read committed snapshot isolation (RCSI): An extension of read committed but with increased concurrency. With this level, the system uses the last committed version before the statement starts, regardless of when the transaction starts.

We recommend that you use RCSI if your system meets any of the following criteria:

- It has a high number of transactions.
- If you encounter a high number of locks in your database.
- Your system has multiple back-end servers, because there could be multiple workflow, escalation, and other tasks that are triggered after the system creates or updates a record.

Note that using RCSI generally increases the CPU utilization due to the additional processing, but lowers the CPU utilization due to a reduction in locks and deadlocks. The net result is lower CPU utilization and therefore, we recommend using RCSI.

Using Read Committed Snapshot Isolation (RCSI)

For the Ivanti Service Manager database, ensure that the following two parameters are set to ON:

- Allow Snapshot Isolation
- Is Read Committed Snapshot On

To set these parameters to on, do the following:

1. Open Microsoft SQL Server Management Studio.
2. Navigate to and highlight the Ivanti Service Manager database to set the properties for.
3. Right-click and select Properties.
4. On the left, select Options.
5. Under **Miscellaneous**, set **Allow Snapshot Isolation** to True and set **Is Read Committed Snapshot On** to True.
6. Click OK.

5.3. Database Tuning

This section describes how to tune the Ivanti Service Manager database for optimal performance. If the system responds slowly while running queries, loading dashboards, or performing other actions, implement the recommendations described here. Information includes:

- Performance Enhancement Recommendations
- Tuning Indexes
- About Using Full Text Search

Performance Enhancement Recommendations

The following sections describe recommendations and caveats to keep in mind when you tune the Ivanti Service Manager database.

- About Tuning the Indexes on a Regular Basis
- Deleting Inactive Tables and Records
- Checking for Under-Utilized Indexes
- Turning on JSON Compression in Microsoft Internet Information Services (IIS)
- Checking Database Latency and Moving Indexes to a Separate Disk
- About Creating Indexes Using the Configuration Console, Not Third-Party Tools
- Checking for Duplicate Indexes
- System Tables to Not Index
- Not Using Include Fields in Indexes
- Ignoring “Create Statistics” Index Results
- Setting the Value for the Database Auto-Growth Parameter
- Monitoring Database Growth and Resetting the Auto-Growth Parameter as Necessary

About Tuning the Indexes on a Regular Basis

Evaluate on an on-going basis the need to perform the re-indexing procedure described in Tuning Indexes. If necessary, you can perform the re-indexing procedure as part of normal maintenance. It does not require hardware or other infrastructure changes.

About Deleting Inactive Tables on a Regular Basis

Whenever possible, delete inactive tables in the Ivanti Service Manager database to keep the database size and complexity to a minimum. See Deleting Inactive Tables and Records for details about deleting.

Checking for Under-Utilized Indexes

Ivanti Service Manager uses indexes to quickly access data. This is defined as reading from the index. Every time that you add a new record, you must also add the new record information to all of the indexes that it applies to. This is defined as writing to an index. While using an index saves time, adding information (writing) to the index takes time.

We recommend that you check your indexes to ensure that they are used frequently. If an index is not used frequently, the performance impact of writing to it initially might not justify the benefits that it provides. One way to check for under-utilization is to

determine the ratio of an index of reads to writes. If you have a table that you are writing records to frequently, but you are not reading using this index very often, it takes more effort to add the new record to the index than it is probably worth.

Calculate the read:write ratio for an index to determine if it is under utilized. If an index has a read:write ratio of 10:1 or less (that is, if total reads to the index does not equal at least 10 times the number of total writes to the index), you should consider deleting the index.

Run the following Microsoft SQL script on the Ivanti Service Manager database to check how often data in an index is read and how often it is written.

Bash

```
-- This script checks for under-utilized indexes.
-- Indexes in which the number of "writes" outnumbers
-- the number of "reads" by far, e.g., 90%, are
-- considered possibly under-utilized indexes.

SELECT OBJECT_NAME(s.object_id)AS 'Table Name',
i.name AS 'Index Name',
i.index_id,
user_updates AS 'Total Writes',
user_seeks + user_scans + user_lookups AS 'Total Reads',
user_updates - (user_seeks + user_scans + user_lookups)
AS 'Difference'

FROM sys.dm_db_index_usage_stats AS s WITH (NOLOCK)
INNER JOIN sys.indexes AS i WITH (NOLOCK)ON s.object_id
= i.object_id
AND i.index_id = s.index_id

WHERE OBJECTPROPERTY(s.object_id,'IsUserTable')= 1
AND s.database_id =DB_ID()
AND user_updates > (user_seeks + user_scans + user_lookups)
AND i.index_id > 1

ORDER BY 'Difference' DESC,
'Total Writes' DESC,
'Total Reads' ASC;
```

Turning on JSON Compression in Microsoft Internet Information Services (IIS)

Follow these steps to improve performance by implementing JSON compression:

1. Open the **Computer Management** panel by going to **Start > Control Panel > Administrative Tools > Computer Management**.
2. In the **Computer Management** panel, double-click **Services and Applications** and double-click **Internet Information Services (IIS)**.
3. On the page for the server (not the site) click Configuration Editor.
4. Expand system.webServer and click httpCompression.
5. Click dynamicTypes to open it.
6. Click mimeType to open the **Properties** dialog box.
7. For the **mimeType** entry, enter application/json, and for the **enabled** entry, enter True.
8. Click Apply.

9. Restart your Microsoft IIS server to load the new module.

Checking Database Latency and Moving Indexes to a Separate Disk

When data and indexes are stored on the same physical disk, resource contention might occur when the system looks up an index and retrieves the corresponding data. Measure the database latency to determine whether resource contention is affecting performance.

Run the following script on the Ivanti Service Manager database to check database latency. If database latency significantly exceeds 110 ms, move indexes to a physical disk that is separate from the disk that stores the Ivanti Service Manager database.

Bash

```
-- Description: This script checks the latency on the
-- different Ivanti databases. Ideally the latency figure
-- should be a single digit value.

SELECT
--virtual file latency
[ReadLatency] =
CASE WHEN [num_of_reads] = 0
THEN 0 ELSE ([io_stall_read_ms] / [num_of_reads]) END,
[WriteLatency] =
CASE WHEN [num_of_writes] = 0
THEN 0 ELSE ([io_stall_write_ms] / [num_of_writes]) END,
[Latency] =
CASE WHEN ([num_of_reads] = 0 AND [num_of_writes] = 0)
THEN 0 ELSE ([io_stall] / ([num_of_reads] + [num_of_writes]))            END,
--avg bytes per IOP
[AvgBPerRead] =
CASE WHEN [num_of_reads] = 0
THEN 0 ELSE ([num_of_bytes_read] / [num_of_reads]) END,
[AvgBPerWrite] =
CASE WHEN [io_stall_write_ms] = 0
THEN 0 ELSE ([num_of_bytes_written] / [num_of_writes]) END,
[AvgBPerTransfer] =
CASE WHEN ([num_of_reads] = 0 AND [num_of_writes] = 0)
THEN 0 ELSE
(([num_of_bytes_read] + [num_of_bytes_written])/
([num_of_reads] + [num_of_writes])) END,
LEFT ([mf].[physical_name], 2) AS [Drive],
DB_NAME ([vfs].[database_id]) AS [DB],
-- [vfs].*,
[mf].[physical_name]
FROM
sys.dm_io_virtual_file_stats (NULL,NULL) AS [vfs]
JOIN sys.master_files AS [mf]
ON [vfs].[database_id] = [mf].[database_id]
AND [vfs].[file_id] = [mf].[file_id]

WHERE DB_NAME ([vfs].[database_id]) like '%HEAT%'

-- and [vfs].[file_id] = 2 -- log files

-- ORDER BY [Latency] DESC
-- ORDER BY [ReadLatency] DESC
ORDER BY [WriteLatency] DESC;

GO
```

About Creating Indexes Using the Configuration Console, Not Third-Party Tools

Do not use third-party tools (such as Microsoft SQL Server Management Studio) to update indexes in the Ivanti Service Manager database. Instead, use the Configuration Console to create new indexes. We recommend this because the Configuration Console creates and maintains index information as Ivanti Service Manager metadata. Ivanti Service Manager uses this metadata whenever tables or indexes in the Ivanti Service Manager database need to be recreated.

Checking for Duplicate Indexes

Check for duplicate indexes in these situations:

- Before creating indexes in the Ivanti Service Manager database, make sure that the table for which you are creating an index does not already have an index containing the same fields.
- If you suspect that duplicate indexes already exist and are impacting performance, find and delete them.

The following sections describe how to check a specific table to determine whether it is indexed, and how to query the Ivanti Service Manager database to identify all duplicate indexes.

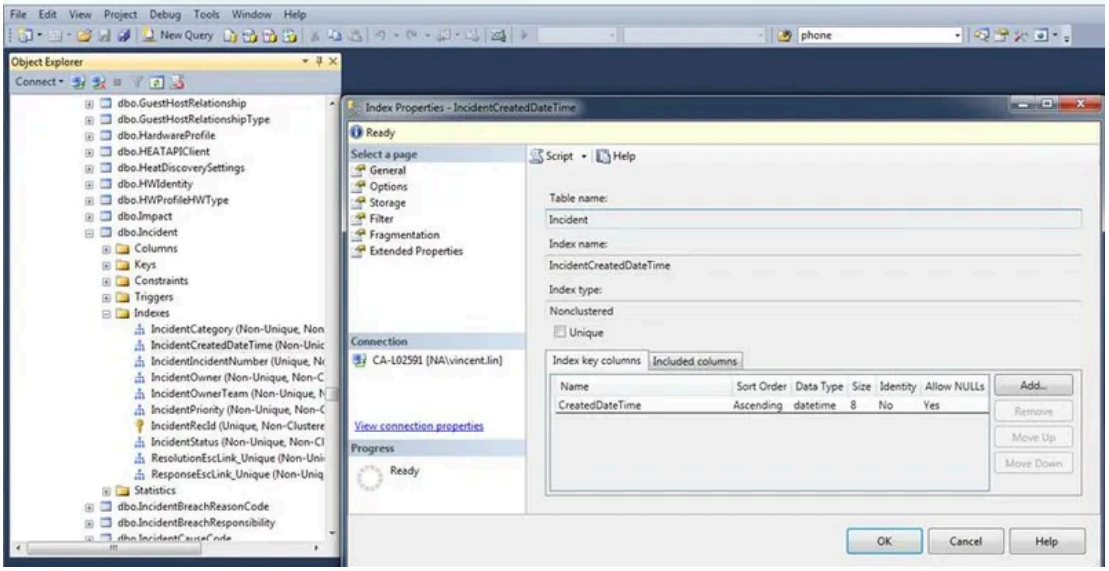
- Checking a Specific Table for Indexes
- Checking for Duplicate Indexes Using a Microsoft SQL Script

Checking a Specific Table for Indexes

Follow these steps:

1. Open Microsoft SQL Server Management Studio.
2. In the **Object Explorer** panel, navigate to the Ivanti Service Manager database.
3. Navigate to **Tables > System Tables > *table_name* > Indexes**.
4. Double-click an index to open it in the **Index Properties** window. Indexed fields are listed in the **Index key columns** area.

Checking for Fields that are Already Indexed



Checking for Duplicate Indexes Using a Microsoft SQL Script

Run the following Microsoft SQL script on the Ivanti Service Manager database to identify duplicate indexes:

Bash

```
-- This script checks for duplicate indexes.

with indexcols AS
(
SELECT object_id AS id,
index_id AS indid, name,
(SELECT case keyno WHEN 0 THEN NULL ELSE colid END AS [data()]

FROM sys.sysindexkeys AS k
where k.id = i.object_id
and k.indid = i.index_id
ORDER BY keyno, colid
for xml path('')) AS cols,

(SELECT case keyno when 0 then colid else NULL end AS [data()]
from sys.sysindexkeys AS k
where k.id = i.object_id
and k.indid = i.index_id

ORDER BY colid
for xml path ('')) AS inc

FROM sys.indexes AS i
)

SELECT object_schema_name(c1.id) + '.' + object_name(c1.id) AS 'table',
c1.name as 'index',
c2.name as 'exactduplicate'

FROM indexcols as c1
JOIN indexcols as c2
ON c1.id = c2.id
AND c1.indid < c2.indid
AND c1.cols = c2.cols
AND c1.inc = c2.inc;
```

System Tables to Not Index

We recommend that you do not index tables that begin with FRS_. These are system tables containing default indexes that are required for Ivanti Service Manager to function properly.

Not Using Include Fields in Indexes

See **Best Practices for Creating New Indexes** for more information.

Ignoring "Create Statistics" Index Results

When creating indexes, ignore the "Create Statistics" results returned by performance tuning tools. See **Best Practices for Creating New Indexes** for more information.

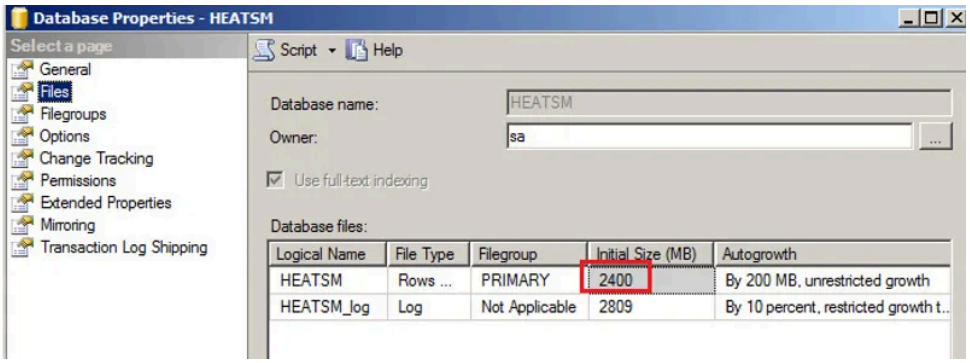
Setting the Value for the Database Auto-Growth Parameter

By default, the auto-growth size of a new database is 1 MB. This is too small for the Ivanti Service Manager database, so you must increase it.

To estimate and configure the appropriate auto-growth size for your Ivanti Service Manager database, do the following:

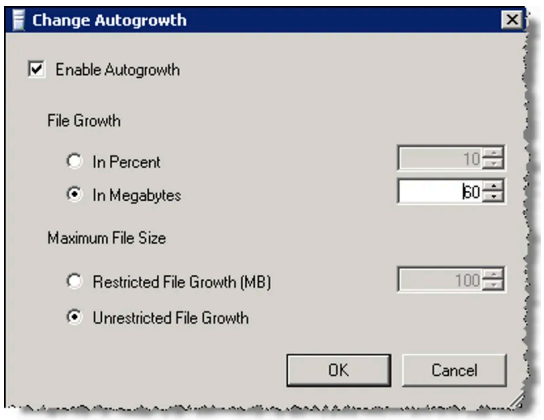
1. Estimate the total size of your initial Ivanti Service Manager database based on expected transactions for incident, service request, and other primary business objects.
2. Open Microsoft SQL Server Management Studio.
3. In the **Object Explorer** panel, navigate to the Ivanti Service Manager database.
4. Right click the Ivanti Service Manager database and select **Properties**.
5. In the **Select a page** panel, click **Files**.
6. In the **Initial Size (MB)** column of the Ivanti Service Manager database line item, set the initial database size based on your estimate from step 1.

Specifying the Initial Size of the Ivanti Service Manager Database



7. Click the **details** icon in the Ivanti Service Manager database line item to open the **Change Autogrowth for Ivanti Service Manager** dialog box.
8. Check Enable Autogrowth, select In Megabytes, and enter a number that is 5 to 10 percent of the initial database size. We recommend that you set the auto-growth parameter using a static value instead of a percentage.

Setting the Auto-Growth Parameter



9. Click **OK**.

Monitoring Database Growth and Resetting the Auto-Growth Parameter as Necessary

We recommend that you periodically evaluate whether the value for the **Enable Autogrowth** parameter is appropriate and reset it as necessary.

After you create the initial Ivanti Service Manager database, monitor its size every month for the first few months to estimate its growth rate. If necessary, reset the value for the **Enable Autogrowth** parameter based on the observed growth rate. After you determine the long-term growth pattern, you can usually wait six months or longer before checking and adjusting the value of the **Enable Autogrowth** parameter.

5.3.1. Tuning Indexes

Perform these steps to re-index the Ivanti Service Manager database:

- Capturing a Database Trace
- Getting Index Tuning Recommendations
- About Creating New Indexes

Capturing a Database Trace

Use the Microsoft SQL Server Profiler in Microsoft SQL Server Management Studio to capture a database trace. You analyze the information from this trace file in Getting Index Tuning Recommendations.

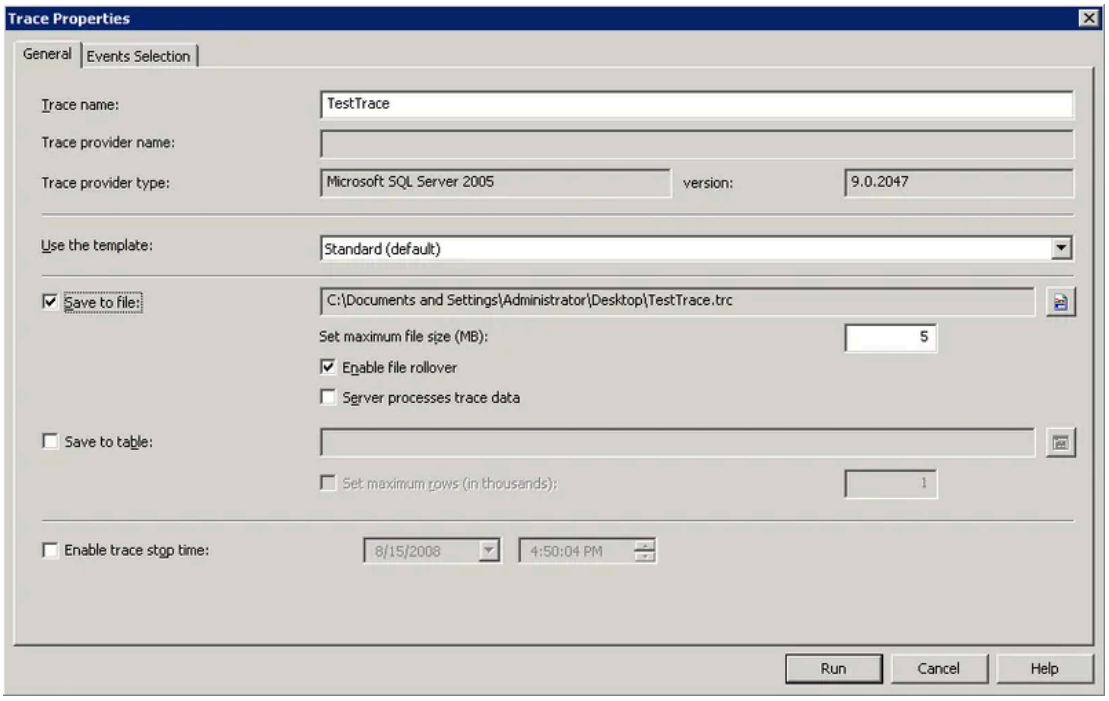
1. Open Microsoft SQL Server Management Studio by selecting **Start > All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio**.
2. Highlight the server that hosts the Ivanti Service Manager database.
3. From the **Tools** menu, select **SQL Server Profiler**.
4. Start a new trace:
    - If you are prompted for login credentials, specify them for Ivanti Service Manager and click **Connect**. The system displays the **Trace Properties** window.
    - If you are not prompted for login credentials, select **File > New Trace** in the **SQL Server Profiler** window. The system prompts you for login credentials. Specify credentials for Ivanti Service Manager and click **Connect**. The system displays the **Trace Properties** window.
5. On the **General** tab, do the following:

    a. In the **Trace name** field, enter a name for the trace.

    b. In the **Use the template** field, select **Standard (default)**.

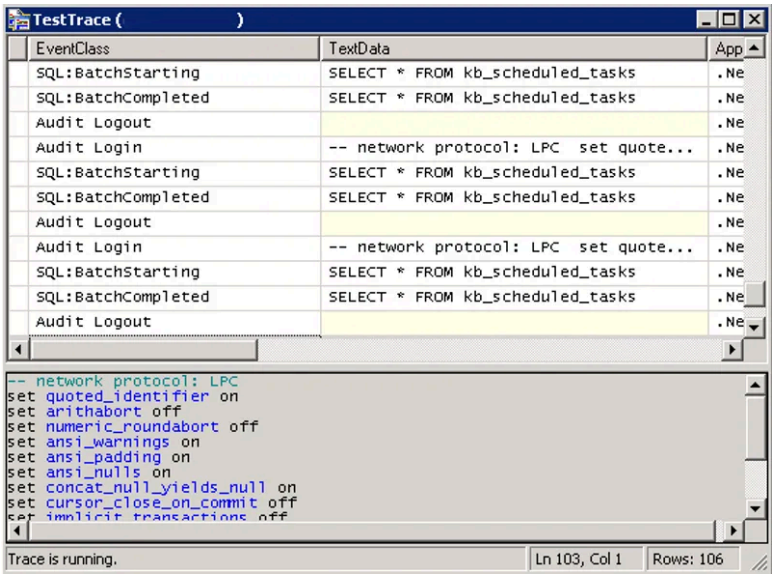
    c. Check **Save to file** and designate a file location for the trace.

Running a Trace From the Trace Properties Window



6. Click **Run** to initiate the trace. The system displays trace information while the trace runs.

A Running Trace



7. When the trace has collected enough information to analyze as described in the next section, select **Pause Trace** or **Stop Trace** from the **File** menu.

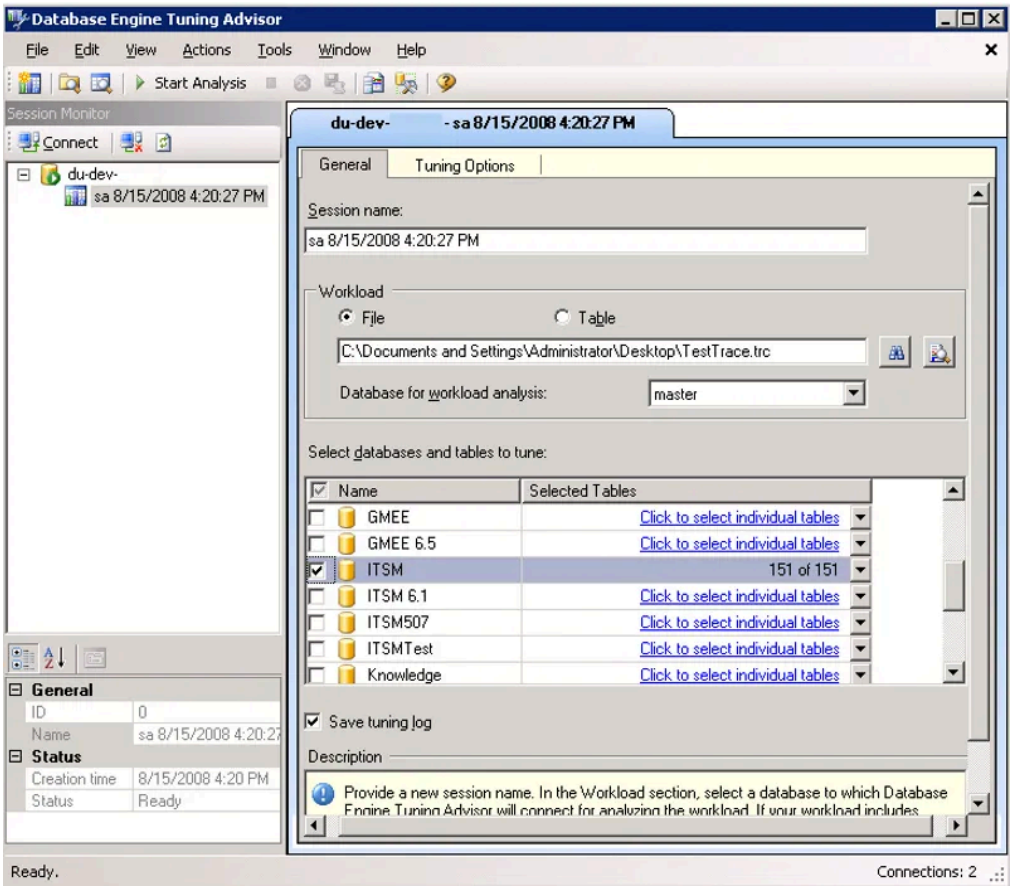
Getting Index Tuning Recommendations

Use the Index Tuning Advisor in Microsoft SQL Server Management Studio to get index tuning recommendations.

1. Open Microsoft SQL Server Management Studio by selecting **Start > All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio**.
2. Highlight the server that hosts the Ivanti Service Manager database.

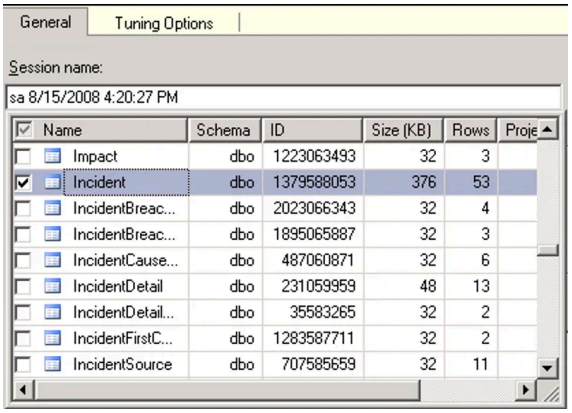
3. From the **Tools** menu, select **Database Engine Tuning Advisor**.
4. Start a new tuning session:
   - If you are prompted for login credentials, specify the credentials for Ivanti Service Manager and click **Connect**. The system displays the **Database Engine Tuning Advisor** window containing a new open session.
   - If you are not prompted for login credentials, select **File > New Session** in the **Database Engine Tuning Advisor** window. The system prompts you for login credentials. Specify credentials for Ivanti Service Manager and click **Connect**. The system opens a new session in the **Database Engine Tuning Advisor** window.
5. On the **General** tab, in the **Workload** area, browse to the trace file that you created in Capturing a Database Trace and click **Open**.
6. In the **Select databases and tables to tune** area, highlight the Ivanti Service Manager database.

Selecting the Ivanti Service Manager Database



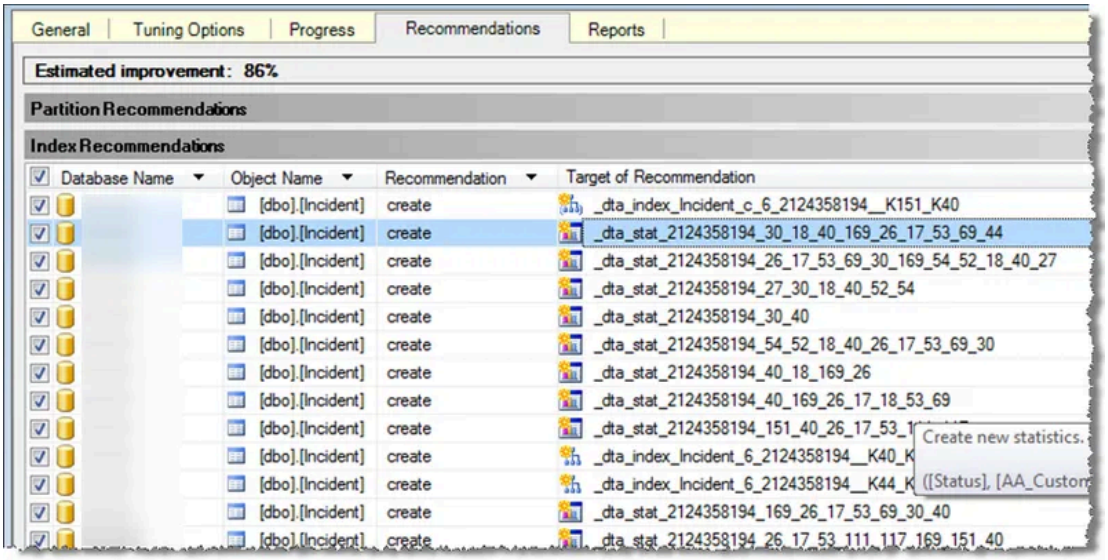
7. From the drop-down menu next to the selected database in the **Selected Tables** column, choose which tables to analyze.

Selecting Tables



8. Click the **Tuning Options** tab.
9. In the **Physical Design Structures (PDS) to use in database** section, select **Indexes**.
10. In the **Partitioning strategy to employ** section, select **No partitioning**.
11. In the **Physical Design Structures (PDS) to keep in database** section, select **Keep all existing PDS**.
12. Click **Start Analysis**.
13. To view progress, select the **Progress** tab.
14. To view recommended indexing actions, click the **Recommendations** tab and go to the **Index Recommendations** section.

Index Recommendations



1. Verify that the indexes recommended for creation do not already exist in the Ivanti Service Manager database as described in Checking for Duplicate Indexes.
2. To view the tuning summary, click the **Reports** tab. You can view reports in the **Tuning Reports** drop-down list beneath the tuning summary.

About Creating New Indexes

After you verify that the indexes recommended for creation do not already exist in the Ivanti Service Manager database, use the Configuration Console to create the indexes.

- Best Practices for Creating New Indexes
- Creating New Indexes

Best Practices for Creating New Indexes

Follow these best practices when you create new indexes:

- Ivanti Service Manager does not create clustered indexes. Disregard any clustered indexes created outside of Ivanti Service Manager.
- Ivanti Service Manager does not create or use include fields or included indexes. You must create and maintain any included indexes that you use outside of the Ivanti Service Manager database. We recommend that you evaluate on a case by case basis the trade off between performance gains and maintenance overhead.
- Ivanti Service Manager maintains statistics only for indexes created in Ivanti Service Manager. Disregard any statistics returned by the create statistics operations in database performance tuning tools.

Creating New Indexes

Perform these steps to create new indexes using the Configuration Console:

1. From the Configuration Console, click **Build > Business Objects**. The system displays the **Business Objects** workspace.
2. Select a business object. The system displays the **Business Object** page.
3. Click the **Indexes** tab. The system displays the **Indexes** workspace with a list of indexes for the business object.
4. To add a new index, click **Add New...**. The system displays index fields associated with this business object.
5. Select the field to index for this business object. You can add more fields later. The system displays the **System Properties** page.
6. Enter information into the fields.

Field	Description
Index Name	A unique name for this index.
Description	A useful description for this index.
Unique	Designates this value as unique, preventing duplicate entries in the index and its backing table. You can create uniqueness by using multiple fields. This option automatically creates an unique index of this field. Unlike the primary key field: • You can have multiple unique fields in the business object. • This field is allowed to contain NULL values (although the NULL values are not indexed).
Clustered	Checks if the business object is part of a clustered index at the database level. Clustered indexes can greatly increase overall speed of retrieval, but usually only where data is accessed sequentially in the same or reverse order of the clustered index, or when a range of items is selected. This is the same as a clustered index function for a Microsoft SQL database. A clustered index cannot contain included fields (it cannot be a cover index). This checkbox is disabled for index fields that have an increasing value, such as GUID.
Key Fields	See **Viewing, Adding, and Deleting Key Fields**
Included Fields	See **Viewing, Adding, and Deleting Included Fields** .
Filter Expression	Optional. You can apply a filter to the index that does not include NULL values. Click the **add new** icon +, then choose a field from the list to create a filter. Repeat as needed. • Operation: Choose an operation from the drop-down list for this filter. • **NotNull**: The filter does not index NULL values. • Value: Enter a string value or expression for this filter.

7. Click Add this Index. The system adds the index to the business object.

Viewing, Adding, and Deleting Key Fields

The system displays the running size, in bytes, of the index for the key fields. The limit is 900 bytes.

1. From the Configuration Console, click **Build > Business Objects**. The system displays the **Business Objects** workspace.
2. Select a business object. The system displays the **Business Object** page.
3. Click the **Indexes** tab. The system displays the **Indexes** workspace with a list of indexes for the business object.
4. Click an index name to open the record.
5. To add a key field, do the following:

   a. Click the **add** icon at the end of the row.



b. Click **not set** to select a field from the drop-down list.

c. Click **Ascending** to change the order. You can select either ascending or descending.

6. To delete a key field, click the **delete** icon ✕ at the end of the row.
7. Click **Save**.

Viewing, Adding, and Deleting Included Fields

1. From the Configuration Console, click **Build > Business Objects**. The system displays the **Business Objects** workspace.
2. Select a business object. The **Business Object** page appears.
3. Click the **Indexes** tab. The system displays the **Indexes** workspace with a list of indexes for the business object.
4. Click an index name to open the record.
5. To add a key field, do the following:

a. Click the **add** icon at the end of the row.



b. Click **not set** to select a field from the drop-down list.

c. Click **Ascending** to change the order. You can select either ascending or descending.

6. To delete a key field, click the **delete** icon ✕ at the end of the row.
7. Click Save.

For additional information about adding indexes, see the Ivanti Service Manager online help. (For information about accessing the Ivanti Service Manager documentation.

5.3.2. About Using Full Text Search

Full text search support was added to enhance the Ivanti Service Manager database performance. This feature is most helpful when you need to perform similar searches against large text fields such as the **Incident.Symptom** field.

5.4. Performance Monitoring

This section describes how to monitor the performance of Ivanti Service Manager.

- Monitoring the Performance of Servers
- Monitoring the Processing Services

Monitoring the Performance of Servers

If you experience performance issues, such as long delays or timeouts, start diagnostics by monitoring the resources used on your system. The following performance monitors provide metrics that you can use to determine if system resources are over utilized.

- On the Ivanti Service Manager application server, monitor the CPU, memory, IO, and network.
- On the Ivanti Service Manager database server, monitor the CPU, memory, IO, and network plus database statistics.
- Also monitor resource utilization. For example, if the average CPU utilization is above 60%, consider adding more CPU on the Ivanti Service Manager application server.

The following are the performance counters on the Ivanti Service Manager application servers. The system samples these counters every five minutes and sends the results:

- Memory:
  - Available MBytes
- Paging file:
  - Percent usage
- Physical disk:
  - Average disk reads per second
  - Average disk writes per second
  - Disk reads per second
  - Disk writes per second
- Processor:
  - Percent processor time (CPU)
- System:
  - Processor queue length
  - Network utilization total, sent, and received per second

The following are the performance counters on the Ivanti Service Manager database server:

- Memory:
  - Available MBytes
- Paging file:
  - Percent usage
- Physical disk:
  - Average disk reads per second
  - Average disk writes per second

    - Disk reads per second
    - Disk writes per second
- Processor:
    - Percent of processor time
- Microsoft SQL Server:
    - Logins per second
    - Logouts per second
    - Lock waits per second
    - Total latch wait time (ms)
    - Total latch waits per second
    - Buffer manager page life expectancy
    - General statistics – user connections
    - Memory manager – memory grants pending
    - Microsoft SQL statistics – batch requests per second
    - Microsoft SQL statistics – compilations per second
    - Microsoft SQL statistics – recompilations per second
- System:
    - Processor queue length
    - Average wait time
    - Number of deadlocks per second
    - Lock timeouts per second

Monitoring the Processing Services

- About Monitoring the Processing Services
- Workflow Service
- Email Service
- Escalation Service
- Message Queue

About Monitoring the Processing Services

You also should monitor the processing services. The Ivanti Service Manager platform includes built-in performance counters for the Ivanti Service Manager message queue, the email service, the escalation service, and the workflow service.

To manage the processing services more effectively, the system implements counters. These counters are implemented per landscape, rather than per service across multiple landscapes. Each of the counters indicates the output across all servers.

For example, the system monitors the counter called “number of tenants” for all servers in the landscape where the service is running. This provides a holistic view of all of the servers and how the service is distributed and consumed. For example, with the workflow service, it shows how the tenants are partitioned versus the non-partitioned servers that act as a catch-all entity.

Workflow Service

The workflow service has these monitors:

Counter	Description
Events handled per poll	Represents the number of events read and handled, per tenant, per poll. If a tenant does not have any events queued, this is zero.
Events handled per second	The number of events read and handled, per tenant, per second.
Events handled versus read per poll percentage	The number of events handled, versus read, per tenant, per poll percentage.
Events read per poll	The number of events read, per tenant, per poll.
Events read per second	The number of events read, per tenant, per second.
Number of busy processor threads	Based on the configured number of processors of the workflow service on a particular server, in the WorkflowService.exe.config file, the counter shows the number of busy processors available per server. The “number of free processor threads” plus the “number of busy processor threads” should equal the total number of processors in the configuration file.
Number of free processor threads	Based on the configured number of processors of the workflow service on a particular server, in the WorkflowService.exe.config file, the counter shows the number of free processors available per server. The “number of free processor threads” plus the “number of busy processor threads” should equal the total number of processors in the configuration file.
Number of outstanding web service calls	The number of outstanding web service calls.
Number of tenants	The number of tenants assigned to the workflow service, per server. Based on partitioning, the number should indicate the total number of active tenants on the landscape.

Email Service

The email service has these monitors:

Counter	Description
Number of busy mailbox poll threads	Number of busy (consumed) mailbox polling threads, per server. The “number of free mailbox poll threads” plus the “number of busy mailbox poll threads” should equal the total number of mailbox poll threads as configured in the configuration file.
Number of busy message processing threads	Number of busy (consumed) message processing threads available, per server. The “number of free message processing threads” plus the “number of busy message processing threads” should equal the total number of message processing threads as configured in the configuration file.
Number of emails read	The number of emails read from customer mailboxes, per tenant.
Number of free mailbox poll threads	Number of free mailbox polling threads available, per server. The “number of free mailbox poll threads” plus the “number of busy mailbox poll threads” should equal the total number of mailbox poll threads as configured in the configuration file.
Number of free message processing threads	Number of free message processing threads available, per server. The “number of free message processing threads” plus the “number of busy message processing threads” should equal the total number of message processing threads as configured in the configuration file.
Number of messages read	The number of email messages read from the database, per tenant.
Number of outstanding web service calls	The number of outstanding web service calls.
Number of polled mailboxes	The number of mailboxes polled.
Number of tenants	The number of tenants assigned to the email service, per server. Based on partitioning, the number should indicate the total number of active tenants on the landscape.

Escalation Service

The escalation service has these monitors:

Counter	Description
Events handled per poll	Represents the number of events read and handled, per tenant, per poll. If a tenant does not have any events queued, this is zero.
Events handled per second	The number of events read and handled, per tenant, per second.
Events handled versus read per poll percentage	The number of events handled, versus read, per tenant, per poll percentage.
Events read per poll	The number of events read, per tenant, per poll.
Events read per second	The number of events read, per tenant, per second.
Number of busy processor threads	Based on the configured number of processors of the escalation service on a particular server, in the EscalationService.exe.config file, the counter shows the number of busy processors available per server. The “number of free processor threads” plus the “number of busy processor threads” should equal the total number of processors in the configuration file.
Number of free processor threads	Based on the configured number of processors of the escalation service on a particular server, in the EscalationService.exe.config file, the counter shows the number of free processors available per server. The “number of free processor threads” plus the “number of busy processor threads” should equal the total number of processors in the configuration file.
Number of outstanding web service calls	The number of outstanding web service calls.
Number of tenants	The number of tenants assigned to the escalation service, per server.

Message Queue

The Ivanti Service Manager message queue has these performance monitors:

Counter	Description
Average message processing time	The average time for a message to be processed by a handler. This does not account for the time that the message spends in the message queue waiting to be dispatched.
Average message size	The average size of the messages received.
Messages created per second	The number of messages received, per second.
Messages processed per second	The number of messages processed, per second by all handlers.
Number of concurrent handlers	The number of handlers that are busy working on items at any given time.
Number of concurrent messages	The number of messages that are being processed (dispatched to its handler) at any given time.
Number of outstanding web service calls	The number of outstanding web service calls.
Number of tenants	The number of tenants assigned to the message queue server.

5.5. Troubleshooting - Performance Tuning

This section describes how to diagnose and fix common performance issues.

Issues occur occasionally in Ivanti Service Manager. This does not necessarily indicate a malfunction. We recommend that you evaluate each issue on a case by case basis.

Symptom	Possible Cause	Action
Dashboards and searches are slow to load.	• Incidents and other records that are no longer active still have open status.	• Close and delete inactive incidents as described in **About Reviewing, Closing, and Deleting Records** and **Deleting Inactive Tables and Records**.
Issues and timeouts that are traceable to the workflow engine occur.	• Workflows that are inactive are still enabled. • Notification workflows do not validate email addresses prior to running.	• Disable inactive workflows as described in **Disabling Inactive Workflows**. • Validate email addresses in workflows as described in **Validating Email Addresses in Notification Workflows**.
Database command timeout errors occur.	• You need to re-index the Ivanti Service Manager database. • In general, when there is a timeout, the environment has insufficient hardware.	• Re-index the Ivanti Service Manager database as described in **Tuning Indexes**. • Verify that your system meets the hardware requirements described in the *System Requirements and Compatibility Matrix for Ivanti Service Manager*.
Workflows take a very long time to execute.		• Delete workflow-related tables as described in **Deleting Inactive Tables and Records** • Increase the processor count in the file called **WorkflowService.exe.config** to 40 as described in **Tuning Business Rules and Workflows**.

5.6. Deleting Inactive Tables and Records

This section describes how to delete inactive tables and records in the Ivanti Service Manager database.

- Best Practices for Deleting Tables and Records
- Deleting Records and Tables from the Ivanti Service Manager Databases

5.6.1. Best Practices for Deleting Tables and Records

These sections describe best practices and general recommendations to consider prior to deleting database tables:

- Identifying the Tables to Delete
- Identifying Criteria for Deleting Tables and Records

After you are familiar with these practices and have followed the described recommendations, see the "About Archiving and Deleting Data from the Ivanti Databases" topic in the in the Ivanti Service Manager online help.

Identifying the Tables to Delete

Identifying which tables to delete depends on customer-specific criteria. In general, deleting primary tables (for example, the **Incident**, **Task**, **Journal**, **Delete**, or other tables) results in the biggest performance improvement. Some tables are candidates for deleting in most situations.

Table Name	Primary Key	Foreign Key	Description
Audit_*Business_object_name*		ParentLink_RecID	Multiple tables that contain audit information generated by Ivanti Service Manager. The information is used by Self Service, the workflow engine, and the escalation engine. An example table name is **Audit_Incident**.
Frs_data_escalation_watch		ParentLink_RecID	Contains escalation tracking information.
Frs_data_workflow_instance	RecID	ParentLink_RecID	Contains workflow execution progress information.
Frs_data_workflow_history		WorkflowInstanceLink_RecID	Contains workflow execution history information.

The most commonly deleted transactional data tables are listed in the following table.

Parent business objects have primary keys. Child business objects have foreign keys. Business objects that can be both parent and child have primary and foreign keys.

Table Name	Primary Key	Foreign Key	Description
Attachment	RecID	ParentLink_RecID	Contains attachments displayed in the **Attachments** tab for major business objects (such as incident). Displays and manages all documents or files that are related to a particular business object. Contains the file name, file path, creator's name, and creation date.
FusionAttachments		RecID	A system business object stored inside an attachment containing the actual attachment block.
FRS_MyItem		SecondParentLink_RecID	Contains **My Item** records. The records contain references to incident, service request, and approval requests displayed in the **My Items** tab in Self Service.
Journal		ParentLink_RecID	Contains notes, email messages, and voice activities displayed in the **Activity History** tab for major business objects (such as incident).
Task	RecID	ParentLink_RecID	Contains task information that is displayed in the **Task** tab for major business objects (such as incident). Information pertains to general, computer provisioning, and software installation tasks.

Identifying Criteria for Deleting Tables and Records

You should only delete inactive records. Do not delete active records that contain data that can be referenced.

There are two ways to determine whether a record is inactive:

- **Based on time only**: Select a cutoff date or time, and if the record was not created or modified after the cutoff date or time, consider it inactive. This method is commonly used for records that do not have a lifecycle or different possible statuses (such as the **Audit History** business object). With this method, you specify a date and time to determine if the record is active.
- **Based on time and status**: Select a cutoff date or time and one or more statuses (or lifecycle stages). If the record was not created or modified after the cutoff date or time, or if the record meets the status criteria that you specify, consider it inactive. This method is commonly used for records that have a lifecycle or different possible statuses (such as the **Task** business object). With this method, you specify both a date and time and a status to determine if the record is active.

Deleting Records and Tables from the Ivanti Service Manager Databases

For information about deleting records and tables from the Ivanti Service Manager database, see the "About Archiving and Deleting Data from the Ivanti Databases" topic in the in the Ivanti Service Manager online help.

6. Operations Console

Use the information in this guide in conjunction with the *Installation and Deployment Guide for* Neurons for ITSM. That guide contains step-by-step instructions for installing and configuring your deployment, while this guide only describes procedures related to using the Operations Console.

> For a complete overview of all types of deployments and step-by-step instructions for installing and configuring each deployment, refer to the *"Installation and Deployment Guide for* Neurons for ITSM - *Version* 2024.2*"*. For information about using Ivanti Neurons for ITSM, including using packages and projects, see the Ivanti Neurons for ITSM online help.

Intended Audience

This document is intended for system administrators, including both Ivanti personnel and members of other organizations, who will be installing and using the Operations Console to manage tenants and tenant instances and to migrate data.

This guide is aimed at the following:

- The system administrator for an on-premise organization that has purchased, installed, and configured Ivanti Service Manager and who needs to migrate data between tenant instances. An on-premise system administrator works only on the Ivanti Service Manager system for his organization.
- The MSP (managed service provider) system administrator for an organization that manages the Ivanti Service Manager systems of several organizations. An MSP system administrator manages the Operations Consoles and migrates data for several organizations. This customer is also called a Software partner.

> This guide uses the term "customer." For MSP system administrators and Ivanti Software employees, the term customer refers to the actual customer (users from a different organization), but for on-premise system administrators, the term customer refers to users within the same organization.

List of Topics

This document contains the following sections:

- **Operations Console Overview**: Describes the Operations Console. Includes a terminology list and instructions for installing and logging in to the Operations Console.
- **Before You Begin Migrating Data**: Lists the four different ways to migrate data and contains conceptual information.
- **Starting the Data Migration**: Contains information such as how to create a tenant and what you must do before you migrate data for every migration method.
- **Migrating Data using Heat Development Project**: Describes how to update an existing tenant instance by migrating data between tenant instances by using the Ivanti Neurons for ITSM development project.
- **Troubleshooting and Known Issues**: Lists troubleshooting tips and known issues with the Operations Console.
- **Appendix A: Using the Operations Console to Perform Administrative Tasks**: Explains how to use the Operations Console to configure landscapes and tenants, as well as how to work with users, system settings, and the audit history.
- **Appendix B: Migrating Data from One Tenant Instance to Another Using Simple Mode or Advanced Mode**: Describes how to update an existing tenant instance by migrating data between tenant instances by using Simple Mode or Advanced Mode.

- **Appendix C: Using the ISM Development Project to Migrate Data**: Contains the information from the Ivanti Service Manager online help that describes how to use the Configuration Console to migrate data using the Ivanti Neurons for ITSM development project.
- **Appendix D: Working with Packages from the App Store**: Describes how to migrate data that came from the App Store.

6.1. Operations Console Overview

This section contains the following:

- A brief description of the Operations Console features. See **About the Operations Console**.
- Instructions for navigating the Operations Console interface. See **Operations Console Interface**.
- A summary of the actions that you can perform from each area of the Operations Console. See **About the Different Workspaces in the Operations Console**.
- Terminology used in this guide, including definitions of data types. See **Terminology**.
- Instructions for installing and logging in to the Operations Console. See **Installing the Operations Console** and **Accessing the Operations Console**.

About the Operations Console

The Operations Console provides an interface in which you can make changes to your Ivanti Service Manager system (usually in the staging instance of the tenant), test the changes (usually in the UAT instance of the tenant), and then deploy them (to the production instance of the tenant). You can manage tenant instances in the production (live system), staging (development system where initial changes are made), UAT (preproduction system where changes are tested), pilot, and other landscapes. For example, in any landscape you can:

- Create tenant instances.
- Edit the properties of tenant instances.
- Lock a tenant instance so that its metadata cannot be modified.
- Deactivate and delete tenant instances.
- Update tenant instances by migrating data from one tenant instance to another.
- Control the timing of tenant development and deployment.

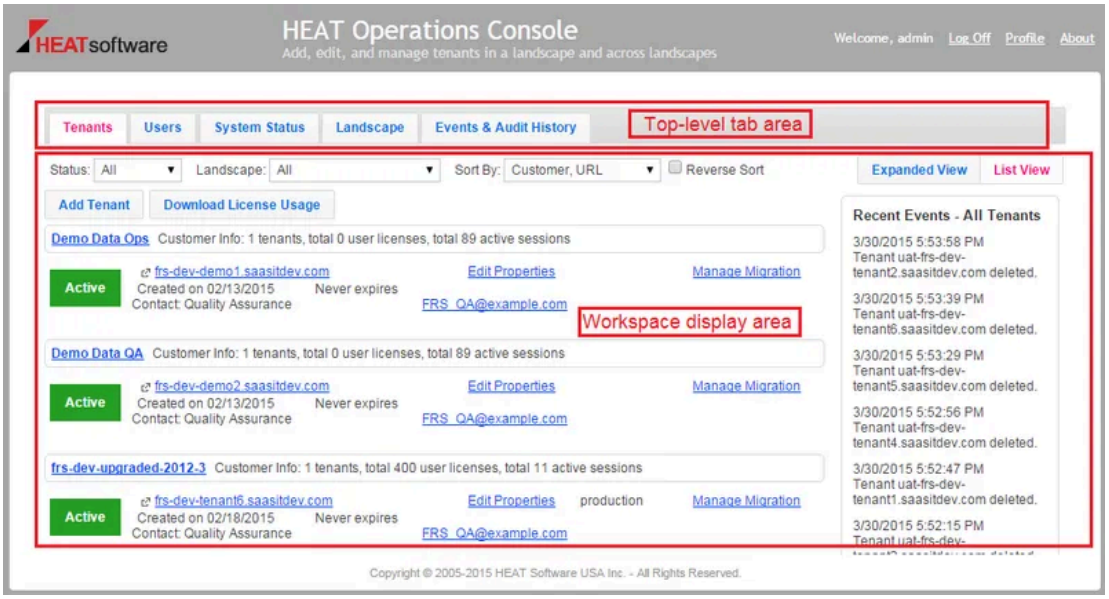
The Operations Console supports these capabilities by connecting to the Ivanti Service Manager configuration server in each landscape. The Operations Console has its own login credentials and database, which provide logging and other tenant management history capabilities.

The Operations Console also provides you with a direct connection to the Ivanti Service Manager configuration database in each landscape, allowing you to manage the Ivanti Service Manager configuration database for that landscape without going through the Ivanti Service Manager configuration server.

The Operations Console requires a database connection to the Ivanti Service Manager configuration database, a database connection to the Ivanti Service Manager application database, and a web services connection to the Ivanti Service Manager application database.

6.1.1. Operations Console Interface

Operations Console Main View (Tenants Workspace Displayed)



The Operations Console, shown in **Operations Console Main View (Tenants Workspace Displayed)**, contains these areas:

- A top-level tab area that you use to select the workspace to display. Click any tab to open it in the workspace display area. When you select a tab, the system displays the tab name in a pink font.
- A workspace display area containing the controls and detailed information for the workspace that opens when you select a top-level tab.

About the Different Workspaces in the Operations Console

Click a top-level tab to open it in the workspace display area. The following sections describe the actions that you can perform in each workspace.

- **About the Tenants Workspace**
- **About the Users Workspace**
- **About the System Status Workspace**
- **About the Landscape Workspace**
- **About the Events & Audit History Workspace**

About the Tenants Workspace

Use the **Tenants** workspace to perform a variety of tenant management activities, including creating, locking, migrating, and deleting tenants and tenant instances. See **Working with Tenants and Tenant Instances**.

About the Users Workspace

Use the **Users** workspace to view and edit information about the users who can access the Operations Console. See **Working With Operations Console Users**.

About the System Status Workspace

Use the **System Status** workspace to view status information about the entire Ivanti Service Manager system. See **Viewing System Information**.

About the Landscape Workspace

Use the **Landscape** workspace to view and edit information about landscapes. See **Configuring Landscapes**.

About the Events & Audit History Workspace

Use the **Events & Audit History** workspace to view information about each action that has occurred on a tenant or tenant instance. See **Viewing Events and Audit History**.

6.1.2. Terminology

This section defines key terms pertaining to the Operations Console and the tenant creation and data migration process.

- General Terms
- Types of Data
- Landscapes
- Tenant and Tenant Instance Types

General Terms

- Operations Console
- Terminology
- Terminology
- Backup Types

Operations Console

The tool used to create tenants and tenant instances, move data from one tenant instance to another (for example, from the staging instance of a tenant to the production instance), and perform various administrative tasks.

Backup Types

There are three steps to the process of backing up a database:

1. Back up the database on the source system.
2. Copy the database from the source system to the target system.
3. Restore the database on the target system.

Use Microsoft SQL to perform the backup. There are several backup types you can choose from when using the Operations Console:

- **From last MSSQL backup**: Copies the source database from the source database backup location to the target database backup location and restores the database from there.
- **From live MSSQL backup**: Performs a live Microsoft SQL backup of the source database and places the backup in the source database backup location. Copies the source database backup to the target database backup location and restores the database from there.
- **From copied MSSQL backup**: The source database has already been manually copied to the target database backup location. If you choose this option, the system adds a field called **Backup Filename** where you enter the name of the Microsoft SQL backup.
- **Database already restored**: The database was already restored manually outside of the Operations Console (for example, through Microsoft SQL Server Management Studio). Choosing this option means the database is not backed up or restored.

Types of Data

- Configuration Data (Settings)
- Master Data

- Metadata
- Transactional Data
- Validation Data

Configuration Data (Settings)

Configuration data, also called settings, is defined as core configuration attributes that define Ivanti Service Manager.

The only configuration data (settings) that the system migrates when you migrate configuration data (settings), as described in Updating Configuration Data (Copy Settings), are the following:

- Allowed attachments
- Authentication providers such as LDAP, SAML, OpenId, and Windows Integrated Security
- Bulk upload profiles
- Dynamic styles
- Global constants
- Integration settings
- LDAP configurations
- Object matching lists
- Password policies
- Voice integrations
- Watch list items
- Email configurations (including approval status keywords, email status update mapping settings, ignore message with subject settings, object mappings for email, task assignment status keywords, truncate body settings, and trusted sender domains)

You cannot migrate other types of configuration data (settings) using the Operations Console. To migrate this data, do so manually outside of the Operations Console by using Microsoft SQL commands.

Master Data

Master data is defined as data sets that are used across an organization and are typically unique to that organization. User and role definitions, role assignments, and categories are examples of master data.

Master data is migrated together with metadata so that it is consistent with the business object definitions. There are four types of master data and you can migrate any or all of them:

- User data, except for user email addresses because they may have been scrubbed.
- User-related data, such as contact group, standard user team, organizational unit, and so on.
- Service request data, such as request offerings, request parameters, and so on.
- Escalation schedule.

You can now track these types of master data:

- Analytic metrics dashboards and configuration
- Schedule entries
- Escalation settings and schedules

- Escalation clock control
- Service level packages
- Service level targets

To see a list of master data for a tenant, if any has been defined, place your mouse over the destination tenant.

The only way to migrate master data is by enabling the Ivanti Service Manager development project and using the push link. See **The Four Ways to Migrate Data** for more information about this method of migrating data and see **Example: Migrating Service Level Data** for an example.

Metadata

Configured business objects, business object attributes, forms, grids, quick actions, searches, and so on. When you reconfigure your Ivanti Service Manager system, most of the changes are implemented by editing metadata.

The types of metadata are as follows:

- Business objects
- Counters
- Forms
- Grids
- Layouts
- Quick actions
- Rules
- Rule overrides
- Branding
- Roles
- Validation (pick list) definitions
- Business rules
- Searches (namely saved searches)
- Dashboards
- Chart-part metadata (one type of dashboard)
- Grid-part metadata (one type of dashboard)
- Special-part metadata (one type of dashboard)
- View-part metadata (one type of dashboard)
- Workflows
- Workflow types
- Reports (subscription, schedule, and distribution are not migrated from source to target)
- Validation data (of pure validation business objects and custom data)
- Images in the frs_def_images table

You can lock all of the metadata, except for quick actions, dashboards, searches, and reports. Those four types of metadata cannot be locked and are always open to be edited in the production instance of the tenant. To lock the other types of metadata, set the

metadata to read-only. Each tenant instance has a **Metadata Locked** field that lets you know if the metadata is locked for an instance of a tenant.

Transactional Data

A customer's data records, including incidents, changes, service requests, and so on.

The only way to migrate transactional data is by enabling the Ivanti Service Manager development project and using the push link. See **The Four Ways to Migrate Data** for more information about this method of migrating data and see **Example: Migrating Service Level Data** for an example.

Validation Data

Validation data objects defined by customers. You must migrate all validation data together at the same time and you must migrate metadata and validation data together in the same migration. This guarantees that when metadata is migrated, it includes all pick list definitions that are associated with validation objects.

Validation data is any data that is configured as part of a *validation* business object. A *validation* business object and its associated data (for example, a pick list and the data in the list) are both considered validation data. But a *standard* business object and its associated data (for example, a pick list and the data in the list) are not both validation data. If the business object is a *standard* business object, then that is validation data, but the associated data is not considered validation data.

Business Object	Is it Validation Data?
Standard business object	Yes
Validation business object	Yes
Data associated with a standard business object	No
Data associated with a validation business object	Yes

Landscapes

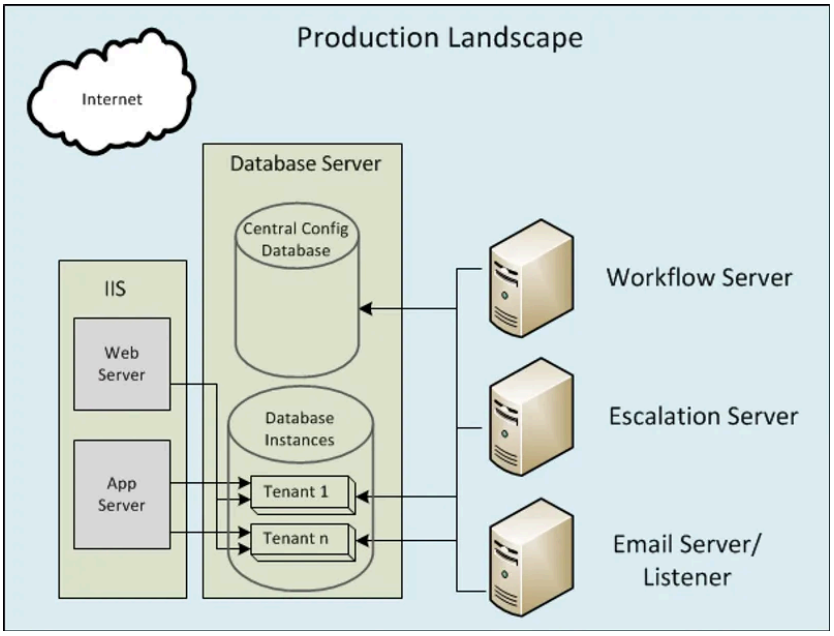
- **Landscape Definition**
- **Landscape Components**
- **Types of Landscapes**
- **Terminology**

Landscape Definition

A landscape is a set of IT infrastructure components that support tenant instances of the same type (where type refers to production, staging, and UAT). The production landscape only contains the production instances of tenants, the staging landscape only contains the staging instances of tenants, and the UAT landscape only contains the UAT instances of tenants.

Typical Production Landscape shows a typical configuration for a production landscape. Components and their locations vary from customer to customer. For example, on-premise customers probably only have one production tenant in their production landscape.

Typical Production Landscape



Landscape Components

At a minimum, a landscape contains these components:

- An individual, isolated Microsoft SQL Ivanti Service Manager application database (called IvantiSM) in each tenant (each tenant instance has its own database, but not its own database instance).
- A central Ivanti Service Manager configuration database (called ConfigDB) containing information about all tenant instances in the landscape.
- A shared pool of Ivanti Service Manager application servers for all Ivanti Service Manager instances in the landscape.
- A shared database cluster for the Ivanti Service Manager configuration and Ivanti Service Manager application databases.
- A shared pool of workflow servers used by all Ivanti Service Manager instances in the landscape.
- A shared pool of escalation engines used by all Ivanti Service Manager instances in the landscape. This is sometimes combined with the workflow server.
- A shared pool of email listeners used by all Ivanti Service Manager instances in the landscape.
- A shared pool of integration servers per function, such as survey, Discovery, Desktop Server and Management (DSM), Report Server, License Server, and so on.

Types of Landscapes

There are six types of landscapes:

- Production landscape: Hosts the production instances of tenants. Used during the data migration lifecycle. This is the environment where the product is deployed.
- Staging landscape: Hosts the staging instances of tenants. Used during the data migration lifecycle. This is the environment where development work is done.
- UAT landscape: Hosts the UAT instances of tenants. Used during the data migration lifecycle. This is the environment where testing is done.
- **Pilot landscape**: Optional. A standalone landscape that hosts the pilot tenant to provide customers with early access to a new Ivanti Service Manager point release.

- Development landscape: Optional. A standalone landscape that hosts tenant templates for demos, test drives, training, and so on.
- Other landscape: Optional. A standalone landscape type that can be used for any purpose.

Tenant and Tenant Instance Types

A tenant is a Ivanti Service Manager system for a particular customer or application.

An instance of the Ivanti Service Manager tenant within a landscape. By default, each customer receives a production instance of the tenant and a staging instance of the tenant. Additional optional tenant instances are also available. The name and URL for each tenant instance must be unique.

> The term "tenant instance" is NOT related to the term "database instance". The use of the word instance, when referring to a tenant, simply means one copy or version of it.

The available tenant instances are:

- **Production instance of a tenant**: A tenant instance containing your production database (including all configuration and transactional data). All customers have a production instance of their tenant. The production instance of the tenant resides in a hardened environment in the production landscape. We do not recommend making metadata or configuration changes directly to the production instance of the tenant during production usage. Instead, make those changes in the staging instance of the tenant, push them to the UAT instance of the tenant for testing, and then push them to the production instance of the tenant.

  You can make some changes to master data (such as adding employees, role assignments, and so on) directly to the production instance of the tenant.
- **Staging instance of a tenant**: A tenant instance for developing and configuring your Ivanti Service Manager system and business processes. This tenant instance is generally used for configuration and metadata changes (but not transactional data changes). It undergoes a baselining process, in which it is updated periodically or by customer request from the production instance of the tenant to ensure that it is in sync with the production instance of the tenant prior to configuration and metadata changes. It can also be used to test new releases, new capabilities, and for training. All customers have a staging instance of their tenant.
- **UAT instance of a tenant**: A temporary tenant instance used for configuration testing and validation before the new configuration is pushed to an existing production tenant instance. The UAT instance of the tenant is required when reconfiguring an existing production instance of the tenant. It is optional when provisioning the production instance of the tenant for the first time or when upgrading to a new Ivanti Service Manager release.

On-premise customers may or may not use a UAT instance of a tenant.

- **Pilot instance of a tenant**: During the upgrade process to a new release, an optional pilot instance of the tenant is made available to customers to allow early access to a new point release. The pilot instance of the tenant resides in the pilot landscape.
- **Development instance of a tenant**: An optional development instance of the tenant for testing or development. The development instance of the tenant resides in the development landscape.
- **Other instance of a tenant**: An optional instance of the tenant for testing or development. The other instance of the tenant resides in the other landscape.
- **Tenant environment**: Infrastructure that ties together the production, staging, and UAT instances of a tenant. This infrastructure allows a complete change management process to manage and control the development and deployment

lifecycles between these instances of the tenant.

- **Tenant template**: A preconfigured ("out-of-the-box") tenant that is typically used to set up a new tenant. A template implements best practices according to ITIL standards, and optimizes processes to allow fast implementation.

6.1.3. Installing the Operations Console

- Installing the Operations Console
- Accessing the Operations Console

Installing the Operations Console

You install the Operations Console when you install Ivanti Service Manager. You can find complete instructions for installing Ivanti Service Manager in the *Installation and Deployment Guide for Ivanti Service Manager*.

We highly recommend that you only install the Operations Console in the staging landscape, and not in any other landscape. For migrating data, you only need to install the Operations Console in one landscape; you should not install it in more than one landscape.

The following is a summary of the installation steps:

1. Access the installation folder on the Ivanti Software product CD or download folder and run IvantiServiceManager.exe. The system displays the **Welcome** dialog box.
2. Click **Next**. The system displays the **License Agreement** dialog box.
3. Select **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
4. Click **Next** to accept the default installation folder. The system displays the **Setup Type** dialog box.
5. Do one of the following:
    - Select **Complete** for the installation type. The installation program installs all of the Ivanti Service Manager components including the Operations Console.
    - Select **Custom** for the installation type. Choose the components to install but ensure that you select Operations Console under Setup/Tools.
6. Click **Install** in the **Ready to Install the Program** dialog box.

The installation begins. The system displays a status dialog box, showing the installation progress of each component over the next few minutes.

7. If prompted, click Run to run the file.

Accessing the Operations Console

The Operations Console has the following default login credentials:

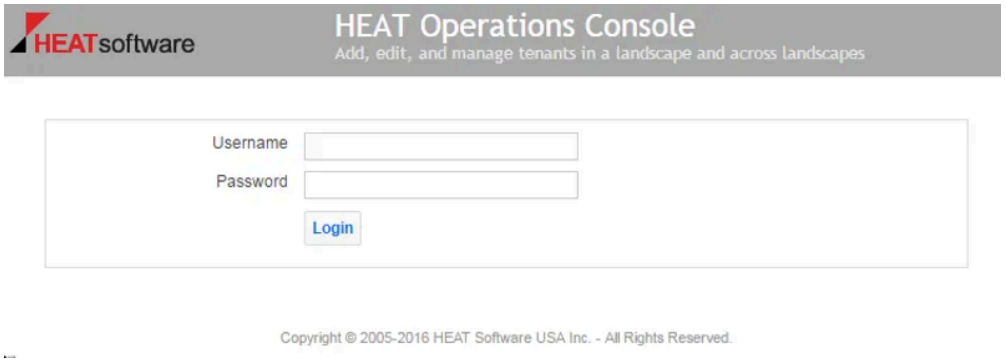
- User name: admin
- Password: manage

We highly recommend that you change the administrator password the first time that you access the system.

After installing Ivanti Service Manager, do the following to access the Operations Console:

1. Either click Start > All Programs > HEAT Software > HEAT > Ops Console or access the Operations Console from a URL in a browser. The system displays the Operations Console login page. See Operations Console Login Page.

    Operations Console Login Page



2. Enter the Operations Console user name and password.
3. Click Login.

6.2. Before You Begin Migrating Data

- The Four Ways to Migrate Data
- About Data Migration
- Conceptual Information: Migration Process Overview
- Items Excluded from Migration

The Four Ways to Migrate Data

Before you begin migrating data, it is very important that you understand the different ways there are to migrate data. There are four ways that you can migrate data:

- Enabling the Ivanti Service Manager development project and applying a package. With a package, you can migrate a very specific set of configuration changes. For example, you can add service request data to a package and migrate it. See Appendix C: Using the ISM Development Project to Migrate Data.
- Enabling the Ivanti Service Manager development project and using the push link. With this method, you can migrate master data, but not configuration data (because that is moved using packages). See Appendix C: Using the ISM Development Project to Migrate Data.
- Disabling the Ivanti Service Manager development project and using Simple Mode. With Simple Mode, you can only copy service request data and escalation schedules. When you use Simple Mode, you copy all of the configuration data from instance of a tenant to another. See How to Use Simple Mode to Migrate Data.
- Disabling the Ivanti Service Manager development project and using Advanced Mode. With Advanced Mode, you can choose which items to copy, such as all business objects but not workflows. However, you cannot specify which business objects (or whichever item you migrate). You can choose the type of items to migrate but not the specific items within that type. With Advanced Mode, you can also specify if you want to migrate master data, which you can use to copy the contents of a business object. See Using Advanced Mode to Migrate Data.

> We plan to remove Simple Mode and Advanced Mode in an upcoming release. The Ivanti Service Manager development project will then be the only data migration method available. This is because Simple Mode and Advanced Mode only migrate the difference in data between the source and the target, and do not take into account the sequence of the data changes between the two systems.

This document includes information about migrating data using all of the methods listed above. However, we highly recommend that you enable and use the Ivanti Service Manager development project, and therefore, this document focuses on those processes.

About Data Migration

The process of migrating data can be defined as moving information from the production instance of the tenant to the staging instance of the tenant, and then optionally moving information from the staging instance of the tenant to the UAT instance of the tenant, and then finally moving information back to the production instance of the tenant (from either the staging or UAT instance of the tenant).

There are two scenarios:

- Production instance → staging instance → UAT instance → production instance.
- Production instance → staging instance → production instance.

The migration process has three parts:

1. Migrating data from the production instance of the tenant to the staging instance of the tenant. This process is described in **Creating the First Staging or UAT Instance of the Tenant from the Production Instance of the Tenant**.
2. Migrating data from the staging instance of the tenant to the UAT instance of the tenant. Although this step is optional, we recommend it. This step is made up of two parts:

   a. Migrating the metadata from the staging instance of the tenant to the UAT instance of the tenant. This process is described in **Appendix B: Migrating Data from One Tenant Instance to Another Using Simple Mode or Advanced Mode**.

   b. Migrating the transactional data from the production instance of the tenant to the UAT instance of the tenant. This is the same process as **Creating the First Staging or UAT Instance of the Tenant from the Production Instance of the Tenant**.
3. Migrating data from the UAT instance of the tenant to the production instance of the tenant (if you migrated from the staging instance to the UAT) or migrating data from the staging tenant to the production tenant (if you did not migrate data to the UAT tenant). This process is described in **Appendix B: Migrating Data from One Tenant Instance to Another Using Simple Mode or Advanced Mode**.

Conceptual Information: Migration Process Overview

There are two scenarios when you perform the migration process:

- When you initially purchase and provision your system. See **About Initially Provisioning the Production Instance of the Tenant**.
- When the database changes. See **About Migrating Data After Creating the Initial Production Instance of the Tenant**.

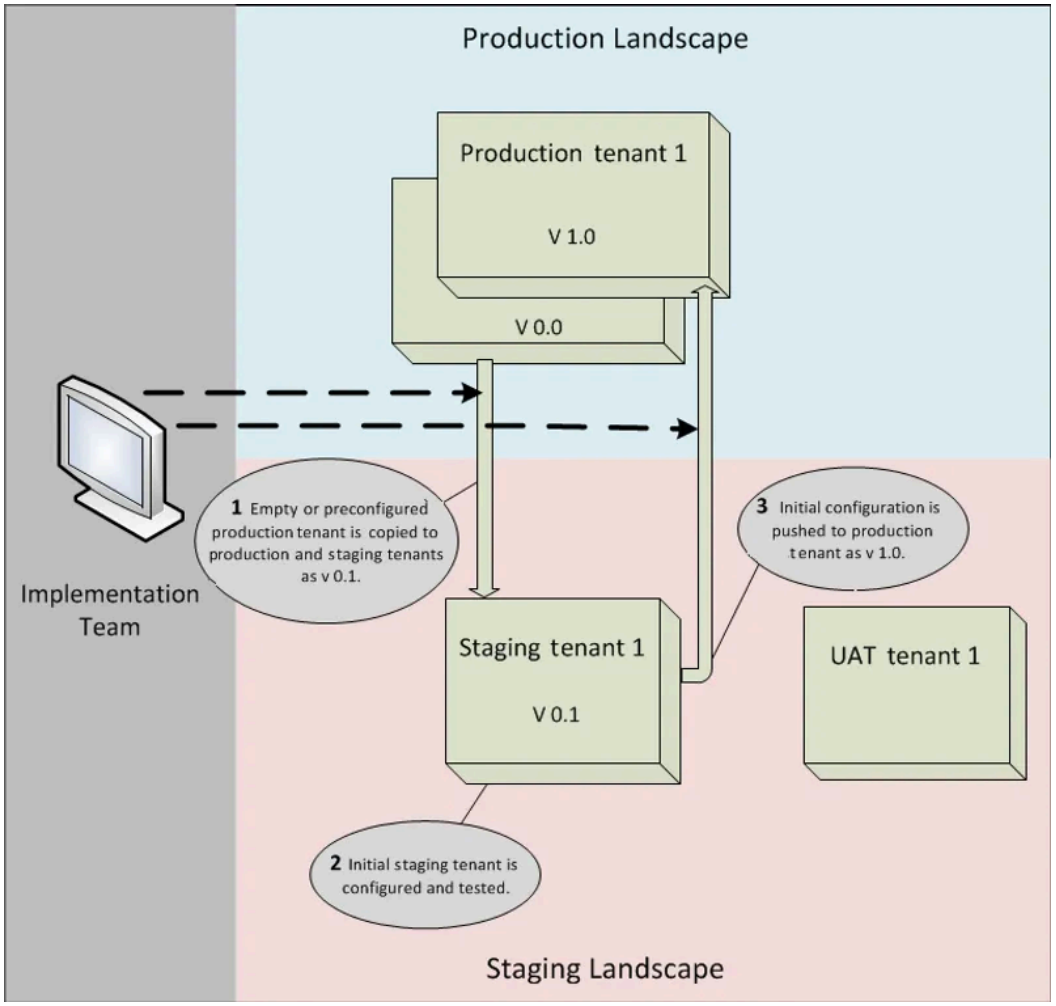
About Initially Provisioning the Production Instance of the Tenant

- **Overview of Initially Provisioning the Production Instance of the Tenant**
- **Overview of the Initial Production Instance of the Tenant Creation Process**

Overview of Initially Provisioning the Production Instance of the Tenant

Adding a Tenant shows the process for migrating data from the initial production instance of the tenant (version 0.0) to the staging instance of the tenant, and then optionally from the staging instance of the tenant to the UAT instance of the tenant, and then from the staging (or UAT) instance of the tenant back to the production instance of the tenant. This process establishes the first production instance of the tenant (version 1.0). See **Overview of the Initial Production Instance of the Tenant Creation Process** for information about the numbered steps shown in **Adding a Tenant**.

Adding a Tenant



Things to note in **Adding a Tenant**:

- The version numbers used in this example are for reference only. The software residing on a tenant does not actually have the version numbers shown here.
- Version 0.0 of the production tenant represents the starting state of the production tenant immediately after it was created. This version (or instance) typically does not contain any transactional (customer) data. You can preconfigure the metadata by either using a customer template, or if no template is available, in a way that provides a default user interface look and feel. Examples of templates are a retail business template and a high tech template.
- When creating the initial version (or instance) of the production tenant (version 1.0), the system usually bypasses the UAT instance of the tenant because there is no baseline configuration to use as a reference for regression testing.

You do not make changes to configuration data and metadata directly in a running database on the production instance of the tenant. Instead, you copy the database to the staging instance of the tenant and makes the changes there. The production instance of the tenant remains unlocked throughout the provisioning and configuration process so that you can update the production instance of the tenant with minimal overhead. The system locks the production instance of the tenant for the first time after you verify the production readiness of the production instance of the tenant.

Overview of the Initial Production Instance of the Tenant Creation Process

The following sections provide a high-level description of the initial production instance of the tenant creation process.

- Before Starting the Migration
- Step 1a: Creating the Initial Production Instance of the Tenant (Version 0.0)
- Step 1b: Creating the Initial Staging Instance of the Tenant (Version 0.1)
- Step 2: Updating the Data on the Staging Instance of the Tenant (Version 0.1)
- Step 3: Pushing the Data from the Staging Instance of the Tenant (Version 0.1) to the Production Instance of the Tenant (Version 1.0)

Before Starting the Migration

- Determine your system requirements to help you design the initial production instance of the tenant (version 0.0).

Step 1a: Creating the Initial Production Instance of the Tenant (Version 0.0)

- Create the initial production instance of the tenant, called version 0.0. This initial production instance of the tenant contains basic help desk and other functionality based on industry standards and preliminary requirements. Version 0.0 is used as a starting point for additional configuration.
- The process for creating the initial production instance of the tenant is described in How to Create a New Tenant.

Step 1b: Creating the Initial Staging Instance of the Tenant (Version 0.1)

- Move the initial production instance of the tenant (version 0.0) to the staging instance of the tenant. The version on the staging instance of the tenant is renamed version 0.1.
- The process for moving the initial production instance of the tenant to the staging instance of the tenant is described in Appendix B: Migrating Data from One Tenant Instance to Another Using Simple Mode or Advanced Mode.
- Timing: This activity typically takes 5 days.

Step 2: Updating the Data on the Staging Instance of the Tenant (Version 0.1)

- Edit the metadata (and optionally configuration data) in version 0.1 on the staging instance of the tenant to meet your requirements.
- Timing: This activity typically takes from two to twelve weeks.

Step 3: Pushing the Data from the Staging Instance of the Tenant (Version 0.1) to the Production Instance of the Tenant (Version 1.0)

- Remove any sample and test data that had been temporarily added to the staging instance of the tenant.
- Push the version 0.1 metadata and configuration data from the staging instance of the tenant to the production instance of the tenant, where it becomes the first fully functional release, called version 1.0.
- The process for moving the staging instance of the tenant to the production instance of the tenant is described in Appendix B: Migrating Data from One Tenant Instance to Another Using Simple Mode or Advanced Mode.
- Verify that the production instance of the tenant configuration (version 1.0) is ready to "go live."
- Lock the production instance of the tenant, either after you receive the "go live" readiness confirmation or 10 days after the "go live" date if you do not receive any confirmation.
- Timing: This activity typically takes from two to eight weeks.

About Migrating Data After Creating the Initial Production Instance of the Tenant

- Requirements Before Migrating Data from the Staging or UAT Instance of the Tenant to the Production Instance of the Tenant
- Overview of the Data Migration Process
- Data Migration Process Overview

Requirements Before Migrating Data from the Staging or UAT Instance of the Tenant to the Production Instance of the Tenant

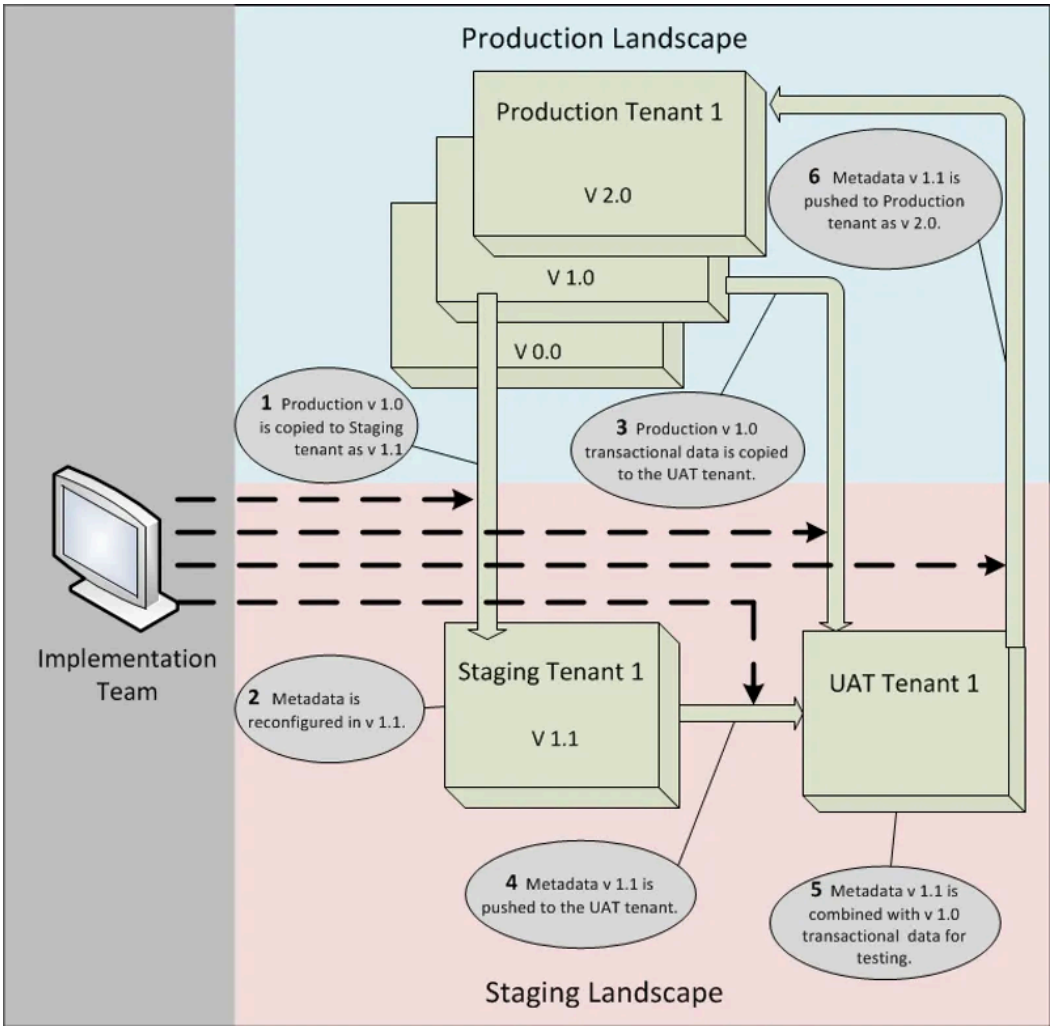
Ensure that you have completed the following requirements before you migrate data from the staging or UAT instance of the tenant to the production instance of the tenant:

- Verify that the logs for the staging or UAT instance of the tenant are free of all configuration-related errors. There cannot be any logs for quick actions, workflow, email, and so on, and there cannot be any “object reference not set to an instance of an object” errors.
- Complete a spreadsheet that lists the data to be cleared from the staging instance of the tenant before migrating the data to the production instance of the tenant. This might include details such as “truncate the following tables", "delete ... when...", and so on. Update the standard objects spreadsheet.

Overview of the Data Migration Process

Data Migration Process shows the steps that occur during a major update to a functioning production tenant instance (in this example, from version 1.0 to version 2.0).

Data Migration Process



Note the following:

- The version numbers used in **Data Migration Process** are for reference only. The software residing on a tenant does not actually have the version numbers shown here.
- Version 1.0 of the production tenant instance represents a functional, running production tenant instance whose configuration remains unchanged until step 6 below.

Data Migration Process Overview

This section describes the actions that occur when data is migrated to the production instance of a tenant.

- **Before Starting the Migration**
- **Step 1**
- **Step 2**
- **Step 3**
- **Step 4**
- **Step 5**
- **Step 6**
- **Afterward**

- If a Step Fails

Before Starting the Migration

- Create a comprehensive project plan describing the requested changes, change verification testing, project team contact information, schedule constraints, and other relevant information.

Step 1

- Copy version 1.0 of the production instance of the tenant in its entirety (that is, master data, metadata, configuration data, and transactional data) to the staging instance of the tenant. The copied version on the staging instance of the tenant is renamed version 1.1.
- Disable all email configurations (@customer.mx.domain) for the production instance of the tenant in the staging instance of the tenant, and enable the staging instance of the tenant email configuration (@tenantname-stg.saasit.com).
- Lock the production instance of the tenant. The production instance of the tenant cannot be reconfigured until approved configuration changes are applied in step 6. While the production instance of the tenant is locked, no one can make changes that will affect the migration process or be overwritten by the new configuration.
- Shrink the data on the production instance of the tenant to 5GB or less.
- The staging instance of the tenant is considered current and active.
- Timing: This step usually takes five days.

Step 2

- Edit the metadata (and optionally the configuration data) in version 1.1 to meet your requirements.
- Record the configuration details in a change register.
- Timing: This step typically takes three weeks. It takes two weeks to prepare and migrate the configuration from the staging instance of the tenant to the UAT instance of the tenant, and one week within the UAT instance of the tenant for final testing.

Step 3

- Copy the transactional data (that is, customer data records) from the version 1.0 production instance of the tenant to the UAT instance of the tenant and if necessary shrink the data to less than 5 GB.
- Use the transactional data to test the metadata and configuration data updates in step 5. Version 1.0 metadata and other configuration data from the production instance of the tenant is not copied to the UAT instance of the tenant.
- Timing: This step typically takes three days.

Step 4

- Review and approve the metadata push from the staging instance of the tenant to the UAT instance of the tenant.
- Complete a tenant instance configuration migration template, which provides details about exactly what data should be migrated.
- Review the migration template.
- Push version 1.1 of the metadata and configuration data to the UAT instance of the tenant. Only migrate the items included in the template. This is a full metadata migration from the source to the target; that is, this is not a delta metadata migration.
- Lock the UAT instance of the tenant, making it read-only and under change control.

- Timing: This step typically takes at least one week.

Step 5

- Perform acceptance testing on the UAT instance of the tenant using version 1.1 metadata and configuration data combined with version 1.0 transactional data. Performs tests based on documented use cases to ensure that the configuration is "go-live" ready.
- Verify that the UAT instance of the tenant configuration and logs are "go-live" ready. Do not update the production instance of the tenant if the UAT instance of the tenant is not "go-live" ready based on predefined requirements.
  - All logs on the UAT instance of the tenant must be clear of any configuration-related failures. For example, there should be no logs reporting failures in workflows, quick actions, email, object references not set to instances of objects, and so on.
  - We recommend that you create documentation such as a completed migration template, updated clean-up scripts (if necessary), descriptions of all configuration changes and additions, and test cases. You can use this information to verify tenant behavior.
- Approve the configuration push from the UAT instance of the tenant to the production instance of the tenant.
- Timing: Testing on the UAT instance of the tenant typically takes two days.

Step 6

- After you have approved the migration and submitted the clean-up scripts, remove any sample and test data that had been temporarily added to the staging instance of the tenant and then migrated to the UAT instance of the tenant.
- Push the UAT instance of the tenant configuration (that is, the version 1.1 metadata and configuration data) to the production instance of the tenant. This is a full metadata migration from the source to the target; that is, it is not a delta metadata migration.
- Timing: Because this step could result in a brief outage of the production instance of the tenant, we recommend that you schedule it to occur during a maintenance window (usually on a Friday or weekend).

Afterward

- Verify that the production instance of the tenant is go-live ready.
- Place the UAT instance of the tenant in maintenance mode. It is no longer available to you.
- Lock the production instance of the tenant.
- Copy the configuration for the new production instance of the tenant to the staging instance of the tenant while the staging instance of the tenant is still locked.
- Unlock the staging instance of the tenant. From now on, you cannot use the staging instance of the tenant for further configuration without refreshing the production instance of the tenant. Refresh the staging instance of the tenant from the production instance of the tenant periodically to ensure that both tenant instances remain synchronized. You can use the staging instance of the tenant for testing and debugging purposes.
- Timing: This activity typically takes three business days.

If a Step Fails

Step 6: If the metadata and configuration data migration from the UAT instance of the tenant to the production instance of the tenant in step 6 fails:

- Roll back the changes (that is, the backup copy is restored).

- Reinitiate the process of migrating the metadata and configuration data from the staging instance of the tenant to the UAT instance of the tenant.

6.2.1. Items Excluded from Migration

- Configuration Data (Settings)
- Master Data

Configuration Data (Settings)

Configuration data, also called settings, is defined as core configuration attributes that define Ivanti Service Manager.

The only configuration data (settings) that the system migrates when you migrate configuration data (settings), as described in **Updating Configuration Data (Copy Settings)**, are the following:

- Allowed attachments
- Authentication providers such as LDAP, SAML, OpenId, and Windows Integrated Security
- Bulk upload profiles
- Dynamic styles
- Global constants
- Integration settings
- LDAP configurations
- Object matching lists
- Password policies
- Voice integrations
- Watch list items
- Email configurations (including approval status keywords, email status update mapping settings, ignore message with subject settings, object mappings for email, task assignment status keywords, truncate body settings, and trusted sender domains)

You cannot migrate other types of configuration data (settings) using the Operations Console. To migrate this data, do so manually outside of the Operations Console by using Microsoft SQL commands.

Master Data

You cannot selectively update master data. If you need to update only certain records of master data (for example, only one record in a table), use Microsoft SQL commands to do so outside of the Operations Console.

6.3. Starting the Data Migration

- Starting the Tenant Instance Migration
- Creating the First Staging or UAT Instance of the Tenant from the Production Instance of the Tenant

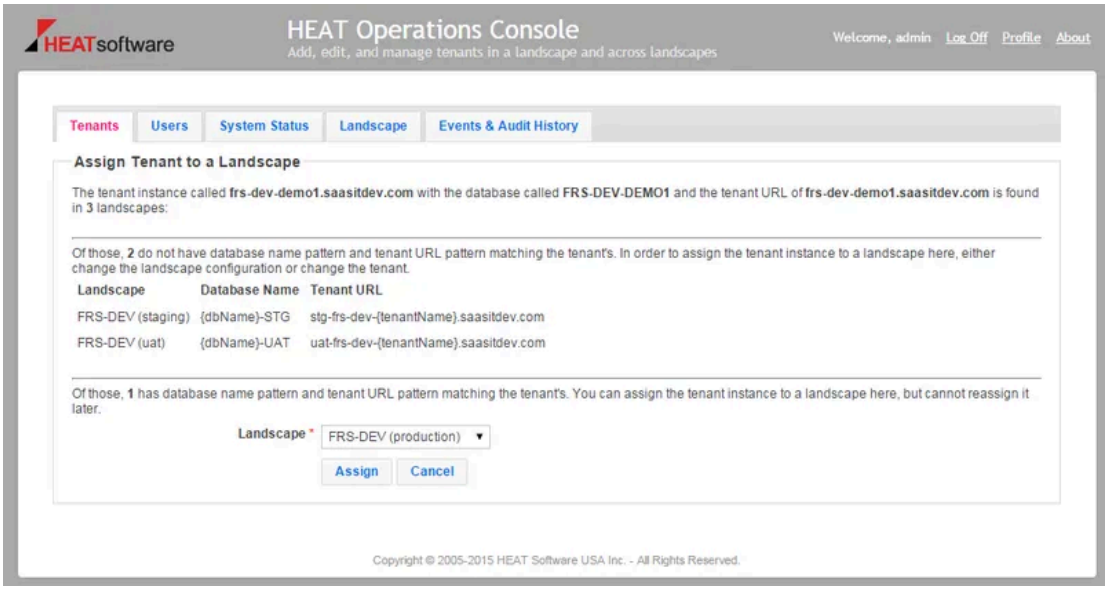
Starting the Tenant Instance Migration

Perform the following steps to start migrating data from the one tenant instance to another. These steps apply for each of the four migration methods. (See The Four Ways to Migrate Data for information about the different migration methods.)

1. Log in to the Operations Console and click the **Tenants** tab.
2. Navigate to the tenant instance to perform the migration for and click **Manage Migration**.

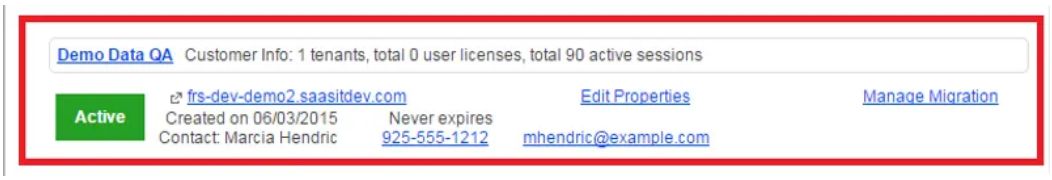
If the tenant instance is not assigned to a landscape, the system prompts you to assign the tenant instance to a landscape to prepare it for migration. See Assigning a Tenant to a Landscape. (If you do not see this screen, your tenant instance is ready for migration. Go to step 5.)

Assigning a Tenant to a Landscape

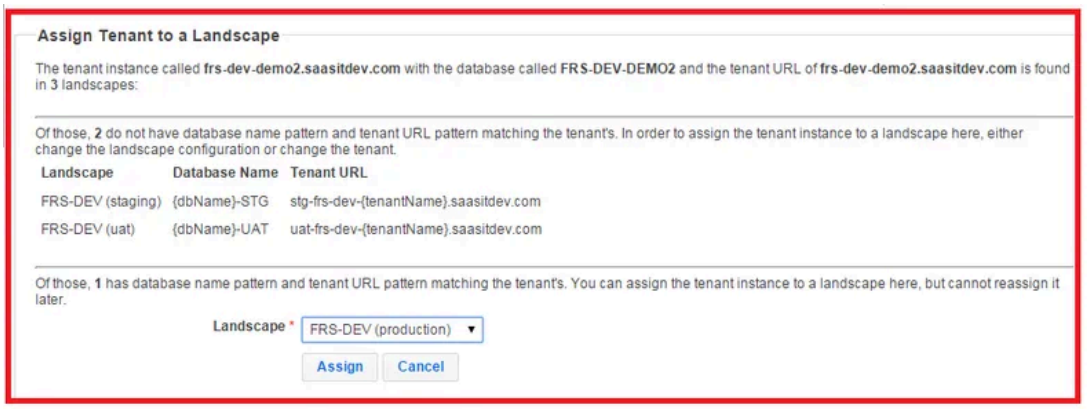


For example, if you click Manage Migration in the screen shown in Database Pattern Screen 1, the system displays the screen in Database Pattern Screen 2.

Database Pattern Screen 1

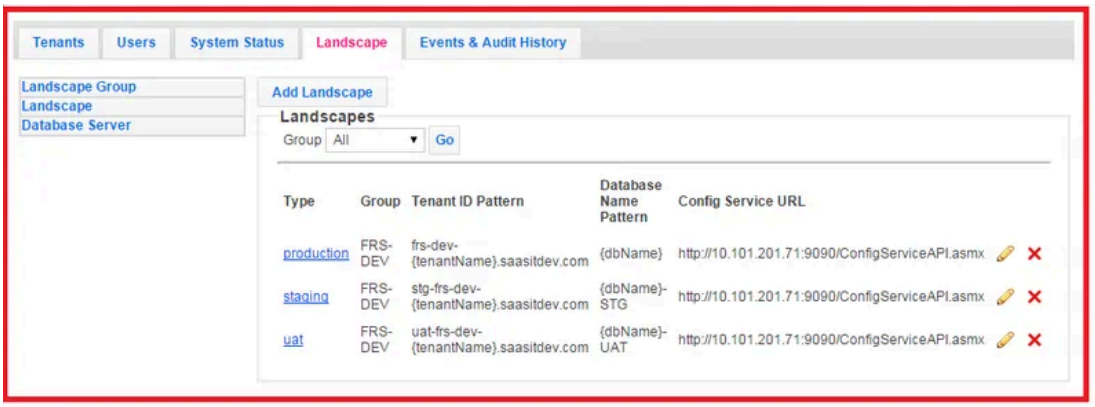


Database Pattern Screen 2



These screens are based on the landscape information, shown in **Database Pattern Screen 3**.

Database Pattern Screen 3



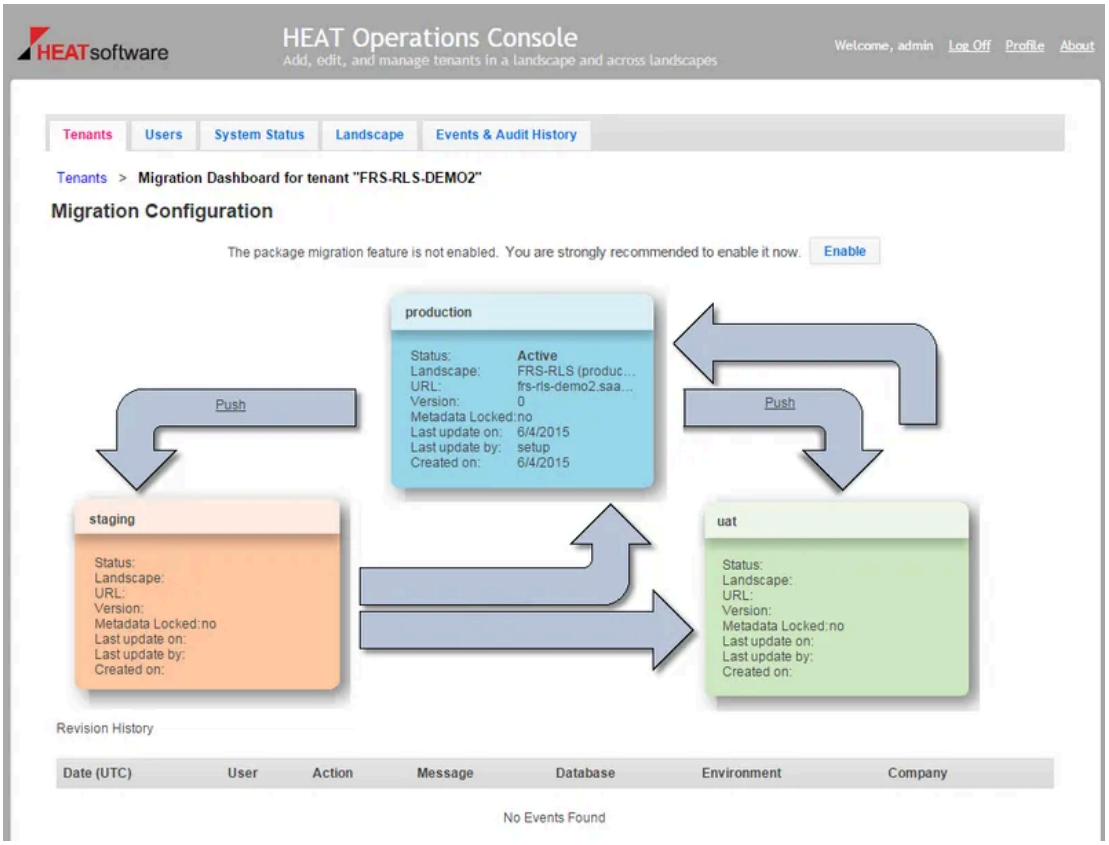
There is only one landscape with the pattern frs-dev-.saasitdev.com and that is the production landscape. Therefore, on the bottom of **Database Pattern Screen 2**, you can assign that tenant instance to that landscape. In the middle part of **Database Pattern Screen 2** are the other available landscapes but these do not have the same pattern.

3. Select a landscape from the **Landscape** drop-down list.

If you do not want to assign it to any of the landscapes in the **Landscape** drop-down list, you can click Cancel and go to the **Edit Landscape** screen to edit the landscape database pattern. See **Editing a Landscape**.

4. Click Assign. The system displays the **Migration Configuration** screen, showing all of the tenants and tenant instances and available migration paths in the landscape. See **Migration Dashboard**.

Migration Dashboard



Things to note in **Migration Dashboard**:

- The display box for each tenant instance (production, staging, and UAT in this example) contains status information that is updated whenever a tenant instance is updated.
- Arrows show all possible migration paths. If an arrow contains a **Push** or **Apply Package** link, the path is available to use based on the current status of all tenant instances in the landscape. Depending on the status of the tenant instance, some migrations paths might not be available.
- A migration history log is displayed at the bottom of the migration dashboard. If no migrations have taken place yet, "No Events Found" displays there as shown in **Migration Dashboard**.
- To enable the Ivanti Service Manager development project to migrate data, click Enable. See **Migrating Data using Heat Development Project**.

5. To start the migration, click either **Push** or Apply Package in the arrow representing the migration path to use. The system displays the **Copy *source_tenant_instance* to *target_tenant_instance*** (for example, **Copy Production to Staging**) dialog box.
6. The remaining steps in the migration procedure differ depending on which migration method you use and whether this is the first migration for this migration path. If this is the first migration, the system *creates* the first configuration on the target tenant instance. If a migration has already been performed and this is a subsequent migration, the result is an *update* of the configuration on the target tenant instance.
   - If this is the first migration, go to **Creating the First Staging or UAT Instance of the Tenant from the Production Instance of the Tenant**. Follow this process for each of the four migration methods. (See **The Four Ways to Migrate Data** for information about the different migration methods.)
   - If this is *not* the first migration and you are enabling the Ivanti Service Manager development project and either using the push link or applying a package, go to **Migrating Data using Heat Development Project**.

- If this is *not* the first migration and you are disabling the Ivanti Service Manager development project and using either Simple Mode or Advanced Mode, go to Starting the Data Migration. *We do not recommend disabling the Ivanti Service Manager development project and using either Simple Mode or Advanced Mode.*

Creating the First Staging or UAT Instance of the Tenant from the Production Instance of the Tenant

This process applies for each of the four migration methods. (See **The Four Ways to Migrate Data** for information about the different migration methods.)

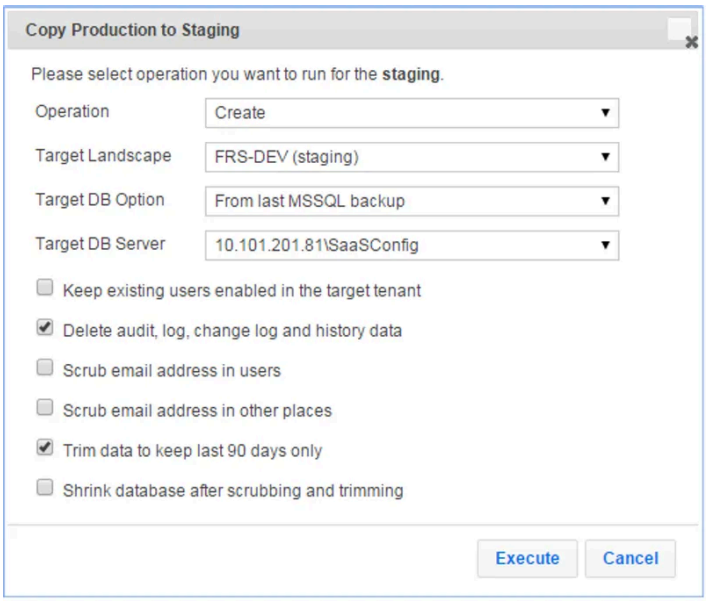
At the beginning of the migration process, you migrate the data from the production instance of the tenant to the staging instance of the tenant. When you migrate the data from the staging instance of the tenant to the UAT instance of the tenant, you must also migrate data from the production instance of the tenant to the UAT instance of the tenant. That way, the UAT instance of the tenant has the latest data from both the staging and production instances of the tenant.

Follow these steps to create the first staging or UAT instance of the tenant from the production instance of the tenant. You also follow these same steps if you want to refresh a staging or UAT instance of the tenant from the production instance of the tenant.

Perform steps 1 to 4 in **Starting the Tenant Instance Migration** before you perform the steps in this section.

When you migrate data from the production instance of the tenant to either the staging or UAT instance of the tenant for the first time, the system creates the first configuration on the staging or UAT instance of the tenant and you see a **Copy Production to Staging** (or **Copy Production to UAT**) dialog box similar to **Copy Dialog Box (Creating a Tenant Instance Configuration from the Production Tenant Instance)**.

Copy Dialog Box (Creating a Tenant Instance Configuration from the Production Tenant Instance)



1. Enter the following information in the **Copy** dialog box:

You cannot enter data for the following:

- In the **Operation** field, **Create** is the only option available. (This is because the system *creates* the first populated iteration of the target tenant instance.)
- For the **Target Landscape**, the system automatically populates this field based on where the **Push** arrow is pointing. For example, in **Migration Dashboard**, if you click Push in the arrow between the production instance of the tenant and the staging instance of the tenant, the system automatically enters the staging tenant instance into this field.

    - Select a backup option in the **Target DB Option** field. Because this is the first time that you are creating the staging or UAT instance of the tenant, there is no backup, so you must select to use a live backup. See **Backup Types** for information about the options.
    - In the **Target DB Server** field, if the target landscape contains more than one database server, select the server that hosts the Configuration Database.
    - Check **Keep existing users enabled in the target tenant** to keep all the users, and not just the administrators, active.
    - Check Delete audit, log, change log and history data to delete the data in these tables:
        - Logs
        - Frs_ops_logon_history
        - Frs_ops_gbu_pipeline_history
        - Frs_ops_metadata_history
        - Frs_ops_upload_cache
        - Journal
        - LDAPImportLog
        - Frs_ops_package_item
        - Frs_ops_package
        - All audit tables, with the name Audit_*table*
    - Check **Scrub email address in users** to ensure that you do not accidentally email users repeatedly during configuration testing on the target tenant instance. If you check this option, the system changes all email fields containing customer email to use the @it.com domain instead of the company domain. This change applies to the user's primary email, contact email, manager email, and team email.
    - Check **Scrub email address in other places** to scrub email accounts saved in transactional data (such as in incidents, service requests, workflow tasks, and so on).
    - Check **Trim data to keep last 90 days only** to only copy transactional data that was created or modified within the last 90 days. If you are updating the database from a copy of your existing customer database, most records are likely to be current within 90 days.

    > Do not check this option if you are creating the database from the sample ("out of the box") database, because the records are likely to be older than 90 days in the sample database.

    - Check **Shrink database after scrubbing and trimming** to truncate unnecessary data when the tenant instance is created from a backup. This is performed as a background task. If the database is very large, this task can take a long time or could abort. The Operations Console does not report any status on this task. If your database is very large, we recommend that you consider shrinking it outside of the Operations Console instead of in this procedure.

2. Click **Execute**. In the confirmation dialog box, click OK.

3. If there are any error or warning messages, the system displays them. Click OK.

The system migrates the data from the production instance of the tenant to the staging or UAT instance of the tenant, and configures the staging or UAT instance of the tenant for the first time.