ivanti

# NMDM Admin Guide KO

ivanti

# CONTENTS


1. **MDM용 Ivanti Neurons 소개** ..... **9**
2. **새 기능 요약** ..... **10**
3. **비디오** ..... **13**
4. **시작하기** ..... **16**
   - 4.1. macOS 기기 구성하기 ..... 23
   - 4.2. 등록 확인 이메일 구성 및 사용 ..... 26
   - 4.3. 정책 규정 준수 알림 이메일 구성 및 사용 ..... 27
   - 4.4. 주문형 기능 ..... 28
   - 4.5. Android Enterprise 기기 지원 준비 ..... 30
5. **대시보드** ..... **31**
   - 5.1. 위젯 작업 ..... 32
   - 5.2. 앱 인사이트 ..... 38
   - 5.3. 정기 보고서 사용 ..... 42
   - 5.4. 사용자 지정 보고서 사용 ..... 49
6. **사용자** ..... **56**
   - 6.1. 사용자 추가 ..... 57
   - 6.2. 사용자 그룹 ..... 61
   - 6.3. 사용자 설정 ..... 65
   - 6.4. 사용자 브랜딩 ..... 75
   - 6.5. Apple Business Manager로 사용자 등록 ..... 76
   - 6.6. 사용자 라이센스 ..... 84
   - 6.7. 사용자 관리 ..... 85
     - 6.7.1. Cisco ISE 작업에 API 사용자 추가 ..... 86
     - 6.7.2. 사용자에게 역할 할당하기 ..... 87
     - 6.7.3. 사용자 역할 ..... 89
     - 6.7.4. 사용자 찾기 및 필터링 ..... 92
     - 6.7.5. 사용자 그룹에 사용자 할당하기 ..... 95
     - 6.7.6. 사용자 초대하기 ..... 96
     - 6.7.7. 사용자 활성화 및 비활성화 ..... 97
     - 6.7.8. 다중 관리자 로그인 관리 ..... 99
     - 6.7.9. 비밀번호 변경하기 ..... 100
     - 6.7.10. 메시지 보내기 ..... 102
     - 6.7.11. 사용자 그룹에서 사용자 삭제하기 ..... 104
     - 6.7.12. 사용자 삭제하기 ..... 105
     - 6.7.13. 사용자 내보내기 ..... 106
     - 6.7.14. 사용자에게 사용자 지정 속성 할당 ..... 107
     - 6.7.15. 사용자에게서 사용자 지정 속성 제거 ..... 108
     - 6.7.16. 사용자 로캘 변경 ..... 109
     - 6.7.17. 사용자 이름 편집 ..... 110
     - 6.7.18. 위치 데이터 수집 기능 해제하기 ..... 111
     - 6.7.19. 시간제한 정보 ..... 112
     - 6.7.20. 시스템 사용량 분석 기능 해제 ..... 113
     - 6.7.21. PIN 생성을 통한 기기 등록 ..... 114
7. **기기** ..... **115**
   - 7.1. 기기 시작하기 ..... 116
   - 7.2. 기기 그룹 ..... 129
   - 7.3. 비관리 기기 ..... 135
   - 7.4. 앱 인벤토리 ..... 136
   - 7.5. 기기 관리하기 ..... 139
     - 7.5.1. Apple 장치 배포 ..... 141
     - 7.5.2. Windows 기기 배포 ..... 149
     - 7.5.3. macOS 기기에서 Apple 원격 데스크톱 설정 ..... 152
     - 7.5.4. 기기 등록(iOS, macOS, Android) ..... 153
     - 7.5.5. 기기 등록(Windows 10+ PC 및 Microsoft Hololens 2) ..... 156
     - 7.5.6. LAPS(로컬 관리 비밀번호 솔루션) ..... 159
     - 7.5.7. PIN으로 패키지 등록 프로비저닝 ..... 161
     - 7.5.8. Windows 기기의 대량 등록 사용 ..... 164
       - 7.5.8.1. Ivanti 대량 등록 ..... 165
     - 7.5.9. 암호 설정 변경하기 ..... 167

7.5.10. 기기 이름 변경 168
7.5.11. 기기 찾기 및 필터링 169
7.5.12. 기기 소유자 이용하기 171
7.5.13. 작업 프로필이 있는 관리되는 기기 178
7.5.14. Android의 대량 등록 사용 179
7.5.15. CSV 파일 업로드를 사용한 대량 등록 181
7.5.16. Device_to_User_BulkEnrollment 184
7.5.17. Samsung Knox 모바일 등록 사용 185
7.5.18. Oculus 기기 등록 186
7.5.19. 기기에 Bluetooth 활성화 188
7.5.20. iOS 업데이트 일정 설정 189
7.5.21. iOS 시스템 앱 재설치 190
7.5.22. 새로운 사용자에게 기기 할당하기 191
7.5.23. Android 기기 재할당 192
7.5.24. 기기의 강제 체크인 193
7.5.25. 장치 위치 확인하기 194
7.5.26. 장치 잠금 설정하기 195
7.5.27. Apple 분실 모드에서 기기 관리하기 196
7.5.28. 분실 모드에서 Android 기기 관리하기 198
7.5.29. 디버그 로그 요청 200
7.5.30. Apple_Enhanced_Logging 201
7.5.31. 장치 폐기하기 202
7.5.32. 장치 소유권 포기 203
7.5.33. 장치 지우기 204
7.5.34. 기기 삭제 205
7.5.35. 장치 잠금 해제하기 206
7.5.36. 기기 재시작/종료 208
7.5.37. 제한 비밀번호 삭제(iOS만 해당) 210
7.5.38. 기기에 대한 Sentry 연결 삭제 211
7.5.39. 장치에 사용자 지정 속성 할당 212
7.5.40. 장치에서 사용자 지정 속성 제거 213
7.5.41. 앱 피드백 동기화 및 가져오기 214
7.5.42. 펌웨어 비밀번호 설정 215
7.5.43. 새 개인 복구 키 재발급하기 216
7.5.44. 복구 잠금 설정 또는 변경 217
7.5.45. Apple 액세스 관리 218
7.5.46. 그룹 정책 등록 219
**8. 앱 220**
8.1. 앱 카탈로그 221
8.2. 선언적 기기 관리(DDM) 앱 관리 238
8.2.1. DDM 앱 관리 설정 240
8.3. Apps@Work(iOS, Android, Windows, macOS) 243
8.4. iOS Apps@Work AppStore 기능 246
8.5. iOS Go 고급 기능 249
8.6. 앱 상세 정보 보기 254
8.7. 앱 구성 257
8.8. 앱에 사용자 지정 속성 할당 272
8.9. 관리되는 Android 구성 273
8.10. Google Play 앱 관리 278
8.11. App Catalog에서 앱 삭제 279
8.12. 인하우스 앱 업그레이드 280
8.13. Android 앱의 패키지 이름 찾기 281
8.14. 범주 282
8.15. 배포 필터 283
8.16. 앱 제외 또는 배포 286
8.17. 검토 287
8.18. Apple Apps 및 Books 289
8.19. 카탈로그 설정 298
8.20. 앱 종속성 배포하기 301
8.21. Android Enterprise로 Divide Productivity 배포 304
8.22. Provisioner 앱 설정 306
8.23. Windows 애플리케이션 관리 308

8.24. Ivanti Bridge ... 311
**9. 컨텐츠 ... 316**
9.1. 콘텐츠 관리 ... 317
9.2. 범주 ... 319
**10. 구성 ... 320**
10.1. 구성 작업 ... 321
10.2. 사용자 셀프 서비스 포털 구성 만들기 ... 333
10.3. 사용자 지정 구성 ... 335
10.4. 사용자 지정 구성을 사용하여 장치에 SyncML 푸시 ... 337
10.5. 홈 화면 레이아웃 구성 ... 338
10.6. 앱 컨트롤 구성: 기기당 설치된 앱 컨트롤 ... 340
10.7. 앱 알림 구성 ... 342
10.8. 구성 내보내기 ... 344
10.9. 구성 우선순위 지정 ... 345
10.10. 구성 관리하기 ... 346
10.10.1. 구성 유형 ... 347
10.10.2. 변수 ... 359
10.10.3. AppConnect 구성 ... 364
10.10.3.1. AppConnect 개요 ... 365
10.10.3.2. AppConnect 암호 ... 366
10.10.4. 보안 구성 ... 367
10.10.4.1. Android Enterprise ... 369
10.10.4.2. Apple 암호 키 증명 ... 370
10.10.4.3. 앱 개인정보 보호 기본값 ... 371
10.10.4.4. Android Enterprise 기본 구성 편집 ... 373
10.10.4.5. Android Enterprise 설정 ... 374
10.10.4.6. Android Enterprise: 업무 관리형 기기 비 GMS (AOSP) 모드 ... 380
10.10.4.7. Android 작업 챌린지 ... 381
10.10.4.8. 인증서 구성 ... 386
10.10.4.9. 인증서 투명성 ... 388
10.10.4.10. 인증서 해지 확인 구성 ... 389
10.10.4.11. 자치 단일 앱 모드 구성 만들기 ... 390
10.10.4.12. DNS 프록시 구성 생성 ... 391
10.10.4.13. 장치 로깅 구성 ... 392
10.10.4.14. 디스크 관리 구성 ... 394
10.10.4.15. Android 암호화 ... 395
10.10.4.16. 암호화된 DNS ... 396
10.10.4.17. 외부 인텔리전스 설정 ... 399
10.10.4.18. 위협 방어 ... 400
10.10.4.19. FileVault 2 ... 401
10.10.4.20. FileVault 복구 키 ... 402
10.10.4.21. FileVault 옵션 구성 ... 403
10.10.4.22. ID 인증서 ... 404
10.10.4.23. Apple 활성화 잠금 구성 ... 410
10.10.4.24. iOS 사용자 지정 구성 ... 413
10.10.4.25. 인텔리전스 설정 ... 414
10.10.4.26. iOS 제한 ... 417
10.10.4.27. 회의실 디스플레이 ... 432
10.10.4.28. 키보드 설정 ... 433
10.10.4.29. 잠금 및 키오스크: Android 기기 관리 모드 ... 435
10.10.4.30. Android용 키오스크 모드 설정 ... 438
10.10.4.31. Android 공유 기기 키오스크 설정 ... 440
10.10.4.32. 잠금 및 키오스크: Android Enterprise ... 441
10.10.4.33. 잠금 및 키오스크: Samsung Knox 표준 ... 464
10.10.4.34. 로컬 관리자 암호 솔루션 구성 ... 468
10.10.4.35. macOS 방화벽 ... 469
10.10.4.36. macOS 제한 ... 470
10.10.4.37. macOS 앱스토어 제한 사항 ... 477
10.10.4.38. macOS 디스크 굽기 제한 사항 ... 478
10.10.4.39. 허용된 미디어 제어(더 이상 사용되지 않음) ... 479
10.10.4.40. macOS 파인더 설정 ... 482
10.10.4.41. macOS 커널 확장 정책 ... 483

10.10.4.42. macOS용 Mobile@Work 484
10.10.4.43. macOS 소프트웨어 업데이트 규칙 구성 489
10.10.4.44. 인증서 환경설정 490
10.10.4.45. 활성 디렉토리(macOS) 491
10.10.4.46. ID 환경설정 494
10.10.4.47. Office 365 자동 계정 생성(macOS) 495
10.10.4.48. 인증 497
10.10.4.49. Apple 앱 카탈로그 498
10.10.4.50. 관리되는 도메인 499
10.10.4.51. 암호 구성 500
10.10.4.52. 개인정보 보호 환경 설정(macOS) 503
10.10.4.53. 개인정보 보호 설정 505
10.10.4.54. 클라이언트 개인정보 보호방침 정보 508
10.10.4.55. Ivanti Go Client 설정 509
10.10.4.56. Siri 설정 511
10.10.4.57. 서비스 구성 파일 설정 513
10.10.4.58. 소프트웨어 업데이트 514
10.10.4.59. 소프트웨어 업데이트 설정 구성 521
10.10.4.60. 보안 기본 설정 구성 524
10.10.4.61. 시간 서버 525
10.10.4.62. 웹 컨텐츠 필터 526
10.10.4.63. Windows 방화벽 529
10.10.4.64. Windows 정보 보호 532
10.10.4.65. Windows 제한 536
10.10.4.66. Windows 데스크톱 제한 541
10.10.4.67. Windows 10 데스크톱 설정 543
10.10.4.68. Windows Hello for Business 구성 545
10.10.4.69. Windows AI Management 구성 546
10.10.4.70. Play Integrity(구 SafetyNet Attestation) 548
10.10.4.71. 고급 Android 암호 및 잠금 화면 549
10.10.4.72. 엔드포인트용 Microsoft Defender 550
10.10.4.73. 인증서 기반 인증 551
10.10.5. 사용자 리소스 구성 552
10.10.5.1. CalDAV 설정 553
10.10.5.2. CardDAV 설정 554
10.10.5.3. Google 구성 555
10.10.5.4. 이메일 설정 557
10.10.5.5. Exchange 구성 560
10.10.5.6. 폰트 설정 564
10.10.5.7. 구독한 달력 설정 565
10.10.5.8. 웹 클립 구성 만들기 566
10.10.5.9. Office 365 설치 568
10.10.5.10. Windows GPO 설정 570
10.10.5.11. BitLocker 암호화 구성 572
10.10.6. 엔터프라이즈 네트워크 액세스 구성 576
10.10.6.1. AirPlay 설정 577
10.10.6.2. AirPrint 설정 578
10.10.6.3. Always On VPN 구성 579
10.10.6.4. 기본 앱 런타임 권한 583
10.10.6.5. 교육 585
10.10.6.6. 글로벌 프록시 설정 586
10.10.6.7. 전역 프록시 구성(Android) 587
10.10.6.8. LDAP 설정 588
10.10.6.9. macOS 서버 구성 589
10.10.6.10. Tunnel 590
10.10.6.11. AppTunnel 설정 591
10.10.6.12. 퍼앱 VPN 구성 596
10.10.6.13. Single Sign-On 설정 604
10.10.6.14. 네트워크 릴레이 구성 612
10.10.6.15. iOS용 다중 사용자 보안 로그인 614
10.10.6.16. Android APN 설정 구성 616
10.10.6.17. VPN 구성 620

10.10.6.18. VPN(요청 시) 632
10.10.6.19. Wi-Fi 구성 639
10.10.7. 셀룰러 네트워크 구성 648
10.10.7.1. APN 설정 649
10.10.7.2. 휴대폰 650
10.10.7.3. 셀룰러 사설 네트워크 구성 653
10.10.7.4. iOS 텔레콤 사전 설정 구성 654
10.10.7.5. 향상된 5G 네트워크 슬라이싱 구성 655
10.10.7.6. eSIM 구성 657
10.10.8. 기타 구성 660
10.10.8.1. 관련 도메인 구성 662
10.10.8.2. Android 파일 전송 구성 663
10.10.8.3. Apple TV 설정 666
10.10.8.4. AirPlay 미러링 667
10.10.8.5. 브라우저 설정 669
10.10.8.6. iOS에서 단일 앱 모드 구성 672
10.10.8.7. iOS MDM 프로필 구성 674
10.10.8.8. macOS MDM 프로필 구성 675
10.10.8.9. 콘텐츠 캐싱 676
10.10.8.10. Android 바로가기 생성 680
10.10.8.11. 접근성 설정 구성 생성 681
10.10.8.12. 화면 보호기 구성 생성 684
10.10.8.13. 사용자 화면 보호기 구성 685
10.10.8.14. 기기 이름 설정 686
10.10.8.15. 기기 배경화면 설정 687
10.10.8.16. EMA 서버 통합 구성 690
10.10.8.17. 절전 구성 691
10.10.8.18. 이더넷 구성(macOS) 697
10.10.8.19. Google BeyondCorp 구성 701
10.10.8.20. 잠금 화면 메시지 구성 705
10.10.8.21. 로그인 창 구성 - macOS 707
10.10.8.22. macOS 시스템 확장 구성 708
10.10.8.23. MAM 전용 709
10.10.8.24. 관리되는 Google Play 구성 711
10.10.8.25. 마이그레이션 지원 설정 712
10.10.8.26. 알림 구성 713
10.10.8.27. 프린터 설정 714
10.10.8.28. 블로트웨어 제거 구성 716
10.10.8.29. Safari 확장 및 설정 구성 717
10.10.8.30. Samsung Phone 제한 구성 720
10.10.8.31. 기본 브라우저 구성 - iOS 및 visionOS 721
10.10.8.32. 화면 공유 호스트 설정 구성 722
10.10.8.33. Single App 모드 설정 723
10.10.8.34. 소프트웨어 업데이트 권장 케이던스 구성 725
10.10.8.35. 시작 메뉴 및 작업 표시줄 726
10.10.8.36. 시스템 업데이트 구성 728
10.10.8.37. Windows 10 업데이트 관리 733
10.10.8.38. Windows 앱 일정 설정 735
10.10.8.39. Windows BIOS 구성 736
10.10.8.40. Windows BitLocker 744
10.10.8.41. Windows 키오스크 구성 745
10.10.8.42. Windows 라이선스 구성 749
**11. 정책 750**
11.1. 정책 작업 751
11.2. 사용자 지정 정책 757
11.3. 허용 앱 모니터링 및 제어 778
11.4. 정책 우선순위 지정 785
11.5. Windows 하드웨어 정책 786
**12. 관리 787**
12.1. 시스템 788
12.1.1. 속성 789
12.1.2. 장치 정리 설정 795

12.1.3. GDPR 프로필 800
12.1.4. 알림 이메일 802
12.1.5. 역할 관리 803
12.1.6. 공간 809
12.1.6.1. 공간 810
12.1.6.2. 공간 관리 812
12.1.6.3. 공간 예 817
12.1.6.4. 기기 위임 819
12.1.6.5. 앱 위임 820
12.1.7. 지원 관리자 821
12.1.8. 관리 > 시스템 사용 알림 822
12.2. 인프라 824
12.2.1. 액세스 825
12.2.2. 앱 목록 826
12.2.3. 감사 내역 내보내기 827
12.2.4. 인증서 관리 830
12.2.5. 외부 인증기관용 SCEP 구성 837
12.2.6. 파생된 자격 증명 제공자 838
12.2.7. Connector 839
12.2.8. Connector용 httpproxy 명령 사용 841
12.2.9. Help@Work 842
12.2.10. 인프라 ID 845
12.2.10.1. ID 제공자 구성 846
12.2.10.2. SCIM을 사용한 사용자 프로비저닝 850
12.2.10.2.1. Entra ID IDP의 사용자 프로비저닝 853
12.2.10.2.2. Okta IDP의 사용자 프로비저닝 858
12.2.11. LDAP 서버 구성 861
12.2.12. Sentry 870
12.3. Apple 설정 871
12.3.1. Apple Configurator 872
12.3.2. 계정 기반 등록 874
12.3.3. 기기 등록 876
12.3.4. 베타 등록 890
12.3.5. 설정 도우미 구성 891
12.3.6. MDM 인증서 설치 892
12.3.7. 기업용 공유 iPad 기기 893
12.3.8. School Manager 897
12.3.9. 설정(Apple) 900
12.4. Windows 기기 사용 작업 902
12.4.1. Windows Autopilot 프로필 구성 903
12.4.2. Windows Autopilot 프로필의 감사 추적 909
12.4.3. TenantLockdown CSP 910
12.4.4. ADMX(GPO) 브라우저 911
12.4.5. 앱 인벤토리 간격 설정 912
12.4.6. 하드웨어 인벤토리 913
12.5. Microsoft Azure 설정 914
12.5.1. Microsoft Azure 사용하기 915
12.5.2. Entra ID Windows 10 통합 엔드포인트 관리 설정 918
12.5.3. Entra ID UEM 앱 할당 919
12.5.4. Entra ID 사용자 소스로 MDM용 Ivanti Neurons 연결 920
12.5.5. Azure 테넌트 922
12.5.5.1. Azure Tenant Requirements 923
12.5.5.2. 기기 사용자에 Intune 라이센스 적용 924
12.5.5.3. 규정 준수 파트너로 MobileIron 추가하기 925
12.5.5.4. Microsoft Endpoint Manager에서 조건부 액세스 정책 만들기 926
12.5.5.5. Microsoft Azure와 MDM용 Ivanti Neurons 연결 중 927
12.5.5.6. 파트너 기기 컴플라이언스 정책 만들기 928
12.5.5.7. MDM용 Ivanti Neurons에서 Azure로 기기 상태 보고 930
12.5.5.8. Azure 테넌트의 프로비저닝 해제 932
12.5.6. 관리 > Microsoft Azure > Office 365 앱 보호 933
12.6. Google Apps와 연결 941
12.6.1. 관리되는 Google Play 계정(Android Enterprise 계정) 942

12.6.2. Android 기기 등록 945
12.6.3. Android 관리 API 946
12.6.4. Google Apps API 952
12.6.5. 관리 - Android Enterprise 953
12.7. ChromeOS 장치 작업 955
12.7.1. ChromeOS 및 MDM용 Ivanti Neurons 956
12.7.2. ChromeOS 장치에 Android 앱 배포 958
12.7.3. ChromeOS 확장 앱 추가 및 배포 959
12.7.4. ChromeOS Blueprint 구성 960
12.7.5. 기기 작업 961
12.7.6. FAQ 962
12.7.7. 평가를 위한 권장 단계 964
12.8. 펌웨어 관리 965
12.8.1. Zebra OTA 서비스에 등록 966
12.8.2. 삼성 E-FOTA 라이선스 관리(지원 중단) 967
12.9. 스크립트 및 파일 관리 968
12.9.1. 모든 스크립트 969
12.9.2. 파일 973
12.10. 브랜딩 974
12.10.1. 관리 > Apple 앱 카탈로그(브랜딩) 975
12.10.2. Android App Catalog 브랜딩 976
12.10.3. 관리 > Android 키오스크 브랜딩 977
12.10.4. 이메일 템플릿 브랜딩 978
12.10.5. 셀프 서비스 포털 986
12.10.6. 셀프 서비스 포털(브랜딩) 988
12.10.7. 다중 사용자 로그인(웹 클립) 브랜딩 989
12.10.8. 조직 990
12.11. 비 iOS 기기 관리 추가 991
**13. 패키지 992**
13.1. 업그레이드하기 996
**14. 장치 라이센스 998**
14.1. 테넌트 정지 999
**15. 지원 티켓 열기 1000**
**16. 타사 속성 1001**
**17. Apps@Work 1002**
**18. MDM용 Ivanti Neurons 및 SCEP 서버 사이에 Kerberos 인증 활성화 1004**
**19. MDM용 Ivanti Neurons 127 관리자 가이드 1006**
**20. Welcome 1007**
**21. Welcome CSH 1008**
**22. Windows 업데이트 관리 1009**

# 1. MDM용 Ivanti Neurons 소개

최신 모바일 보안 접근 방법인 MDM용 Ivanti Neurons는 고도로 확장 가능하고 안전하며 쉽게 업데이트할 수 있는 인프라를 통해 UEM(통합 엔드포인트 관리) 솔루션을 제공하며 전 세계의 수백만 기기를 지원합니다.

- 즉각적인 업데이트: 자동 소프트웨어 및 보안 업데이트를 사용 가능해진 순간 곧바로 다운로드하여 새 기능에 액세스할 수 있습니다.
- 주문형 확장성: 비즈니스에 변화가 필요해지면 용량 계획에 대한 우려 없이 배포를 확장할 수 있습니다.
- 하드웨어 비용 최소화: 온프레미스 하드웨어를 유지 관리할 필요가 없으므로 Cloud 기반 서비스를 관리하기 위한 풋프린트가 필요하지 않습니다.
- 높은 가동 시간 및 가용성.
- 기존 투자의 효율 극대화: IT 리소스를 하드웨어 유지 관리에서 보다 전략적인 작업으로 재할당하여 비즈니스 가치를 추가할 수 있습니다.

이번 릴리스에서 사용할 수 있는 새 기능 요약 요약이 보입니다.

# 2. 새 기능 요약

이 섹션에서는 이 릴리스에서 이용 가능한 새 기능과 성능 향상에 대한 요약을 제공합니다. 이러한 기능 및 성능 향상에 대해 설명하는 문서 참조 또한 이용 가능 시 제공됩니다.


일반 기능 및 성능 향상

Android 기능

iOS, macOS, watchOS, visionOS, tvOS 기능

Windows 기능


## 일반 기능 및 성능 향상

- **향상된 macOS 패키지 ID 처리**: 앱 업로드 중 올바른 패키지 ID를 자동으로 감지하여 입력하고 동일한 패키지 ID가 기기로 전송되도록 하여 macOS 사내 PKG 앱 배포가 개선되었습니다 이를 통해 앱 식별 정확도가 향상되고 서버와 기기 간 설치 상태 불일치가 해결되며 설치 상태 보고가 개선됩니다. 번들 ID는 업로드 중에 검토하고 편집할 수 있으며 배포 후에는 잠깁니다.
- **설치된 앱의 번들 ID 표시**: 이제 기기 상세 정보 페이지의 설치된 앱 섹션에 번들 ID 열이 포함되며, 페이지 설정에서 이 열을 표시하거나 숨길 수 있습니다.
- **실패한 Android 앱 설치 자동 재시도**: 이제 설치 오류 상태가 된 Android 앱 설치는 기기 등록 1시간 후부터 자동으로 재시도됩니다. 앱 배포 성공률을 높이기 위해 설치 명령이 30분마다 최대 5회까지 다시 전송됩니다.
- **공간의 기기 이동 감사 내역**: 공간 간 기기 이동을 추적할 수 있도록 공간에서 기기 등록 및 등록 해제에 대한 감사 내역 활성화 설정이 추가되었습니다. 자세한 정보는 감사 내역 내보내기를 참조하십시오.
- **기기 정리 설정의 OS 플랫폼 필터**: 이제 관리자는 폐기된 기기 및 폐기 보류 중인 기기를 제거할 때 OS 플랫폼별로 기기 정리 작업을 필터링할 수 있습니다. 기본적으로 지원되는 모든 플랫폼이 선택된 상태로 유지되어 기존 동작이 그대로 유지됩니다. 관리자는 필요에 따라 선택 항목을 수정하고 정리 작업을 특정 플랫폼으로 제한할 수 있습니다. 자세한 내용은 장치 정리 설정을 참조하십시오.
- **Office 365 앱 보호 정책 동기화**: 이전에는 관리자가 앱 보호 정책을 생성하거나 수정할 때 MDM용 Ivanti Neurons 내에서 직접 앱을 선택할 수 있었습니다. Microsoft는 사용 가능한 앱 목록을 검색하는 데 사용되던 API를 더 이상 지원하지 않아 보호된 앱 목록이 MDM용 Ivanti Neurons에서 비어 있는 것으로 표시됩니다. Microsoft Office 365 앱 보호 정책 관리가 Microsoft Intune의 변경 사항에 맞게 업데이트되었습니다. 이제 Intune에서 구성된 애플리케이션이 MDM용 Ivanti Neurons에 자동으로 동기화되어 보호된 앱을 계속 확인할 수 있습니다. MDM용 Ivanti Neurons에서는 앱 제거가 계속 지원되지만 새 앱 할당은 Microsoft Intune에서 구성해야 하며 자동으로 반영됩니다.
- **공간의 기기 이동 감사 로깅**: 이제 관리자는 감사 로그를 통해 공간 간 기기 이동을 추적할 수 있습니다. 활성화하면 새로운 감사 설정에서 기기가 한 공간에서 제거되어 다른 공간에 추가될 때마다 이벤트를 기록하여 자동 및 규칙 기반 공간 할당에 대한 가시성을 높입니다. 자세한 내용은 감사 내역 내보내기을 참조하십시오.
- **기기 그룹을 사용한 사용자 정의 속성 자동 할당**: 이제 관리자는 기기 그룹 수준에서 사용자 정의 속성을 할당할 수 있습니다. 기기 그룹의 구성원인 기기는 구성된 속성 값을 자동으로 상속하므로 수동 구성이 줄어들고 일관된 기기 분류를 유지하는 데 도움이 됩니다. 자세한 내용은 기기 그룹을 참조하십시오.
- **OS 수준 기기 등록 제한**: 플랫폼별로 기기 등록을 제한하여 승인된 **Apple**, **Android**, **Windows** 기기만 등록할 수 있도록 합니다. 자세한 내용은 사용자 설정을 참조하십시오.

## Android 기능

- **앱 사용 중 앱 업데이트 방지**: 이제 관리자는 관리되는 Android 앱이 사용 중일 때 업데이트되지 않도록 할 수 있습니다. **앱 사용 중 업데이트 안 함**을 활성화하면 사용자가 앱을 닫거나 백그라운드로 이동할 때까지 앱 업데이트가 연기되어 활성 세션 중 중단을 최소화하는 데 도움이 됩니다. 자세한 내용은 앱 구성을 참조하십시오.

- **잠금 정책 변경 시 키오스크 모드 유지**: 잠금 정책 변경 시 키오스크 모드를 유지할 수 있도록 지원이 추가되었습니다. 잠금 정책이 업데이트된 후 기기가 자동으로 키오스크 모드로 돌아가므로 수동 개입이 줄어들고 전용 기기의 중단이 최소화됩니다. 자세한 내용은 **잠금 및 키오스크: Android Enterprise**를 참조하십시오.
- **가려지지 않은 알림 활성화**: 기기 소유자 기기에서 잠금 화면 알림의 표시 여부를 구성할 수 있도록 지원이 추가되었습니다. 관리자는 잠금 화면에서 알림 콘텐츠를 표시하거나 숨기거나 가려서 알림 기능을 유지하면서 민감한 정보를 보호할 수 있습니다. 자세한 내용은 **고급 Android 암호 및 잠금 화면**을 참조하십시오.
- **프로필 대량 등록 중 기기-사용자 매핑 지원**: 대량 등록 프로필의 기기-사용자 매핑에 대한 지원이 추가되었습니다. 관리자는 대량 등록 CSV 파일을 통해 또는 기기를 수동으로 추가할 때 각 기기에 특정 사용자를 할당하여 등록 중 사용자를 자동으로 할당하고 등록 후 관리 작업을 줄일 수 있습니다. 관리자는 기기를 등록하기 전에 사용자 할당을 업데이트할 수도 있습니다. 자세한 내용은 **대량 등록 프로필의 기기-사용자 매핑**을 참조하십시오.

## iOS, macOS, watchOS, visionOS, tvOS 기능

- **기기 등록 프로필을 위한 새로운 건너뛰기 키**: 이제 관리자는 기기 등록 프로필을 생성할 때 다음 건너뛰기 키를 사용할 수 있습니다.
  - **Liquid Glass 창 건너뛰기**(iOS 27.0+ 및 macOS 27.0+)
  - **접근성 모양 창 건너뛰기**(iOS 27.0+)
    이러한 건너뛰기 키를 사용하면 관리자가 기기 등록 중 특정 설정 창을 숨길 수 있어 등록 환경을 간소화할 수 있습니다. 자세한 내용은 **기기 등록**을 참조하십시오.
- **DDM 기기 시스템 상태 지원**: 이제 MDM용 Ivanti Neurons에서 **기기 상세 정보** 페이지에 DDM 기기 시스템 상태를 지원합니다. 관리자는 **기기 구성요소 상태** 섹션에서 이 상태를 확인하여 감독 모드 기기에서 보고한 시스템 상태를 모니터링할 수 있습니다. 자세한 내용은 **기기 시작하기**를 참조하십시오.
- **Apple 기기에 대한 새로운 기기 상세 정보 필드 추가됨**: Apple 기기 관리 상태를 보다 명확하게 파악할 수 있도록 **기기 상세 정보** 필드가 새로 추가되었습니다. 이제 관리자는 다음 상세 정보를 볼 수 있습니다.
  - iOS 27.0+에서 작동하는 기기의 **다중 사용자 모드**. 이 필드는 iPad가 공유 기기로 구성되어 있는지 여부를 나타냅니다.
  - iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+ 및 watchOS 27.0+에서 작동하는 기기의 **MDM 등록 유형**.
  - iOS 27.0+ 및 visionOS 27.0+에서 작동하는 기기의 앱 보존을 통한 **MDM 서비스 복귀**.
    이러한 필드를 통해 관리자는 기기 상세 정보 페이지에서 기기 구성 및 등록 정보를 직접 검토할 수 있습니다. 자세한 내용은 **기기 시작하기**를 참조하십시오.
- **앱 개인정보 보호 기본값 구성 지원**: 이제 관리자는 Apple 기기 선언적 관리(DDM)를 사용하여 하나 이상의 앱에 **앱 개인정보 보호 기본값**을 구성할 수 있습니다. 앱을 처음 실행하면 카메라, 마이크, 위치, Bluetooth 및 로컬 네트워크 액세스와 같이 지원되는 개인정보 보호 구성요소에 대한 권장 권한을 허용하거나 나중으로 미룰 수 있는 동의 메시지가 한 번 표시됩니다. 자세한 내용은 **앱 개인정보 보호 기본값**을 참조하십시오.

> 이제 macOS 27.0+ 감독 모드 기기에서 앱 개인정보 보호 기본값 구성이 지원됩니다.

- **새로운 DDM 앱 관리 속성 추가됨**: '고급 검색' 및 기기 목록 페이지에 DDM 앱 관리 속성인 **Apple DDM 앱 활성화됨** 필드가 추가되었습니다. DDM을 통해 앱이 배포된 기기를 보여 줍니다. 관리자는 사용자 설정에서 이 기능을 활성화할 수 있습니다. 자세한 내용은 **기기 시작하기**를 참조하십시오.
- **향상된 macOS 확장 가능 SSO 구성**: **preferred_username** 및 **name**과 같은 토큰 속성을 올바르게 매핑하도록 macOS 확장 가능 SSO 구성이 업데이트되었습니다. 이를 통해 유효하지 않은 토큰-사용자 매핑으로 인해 발생하는 구성 오류가 해결되고 SSO 프로필을 기기에 성공적으로 배포할 수 있습니다.
- **Apple 강화된 로깅**: 관리자는 AppleCare에서 제공한 토큰을 사용하여 지원되는 Apple 기기에서 Apple 강화된 로그 수집을 시작할 수 있습니다. 기기 상세 정보에는 세션 상태, 토큰 및 타임스탬프 정보가 표시되며, 필요한 경우 활성 세션을 취소할 수 있습니다. 자세한 내용은 **Apple 강화된 로깅**을 참조하십시오.

- **잠금 모드 상태**(iOS 27+, macOS 27+): **기기 상세 정보** 페이지, **고급 검색** 및 기기 그룹 규칙의 새로운 **보안 잠금 모드** 필드를 사용하여 잠금 모드 상태별로 기기를 확인하고 필터링할 수 있도록 지원이 추가되었습니다. 이 필드는 기기에서 잠금 모드가 활성화됨(**true**) 또는 비활성화됨(**false**)으로 되어 있는지를 나타냅니다. 자세한 내용은 기기 시작하기, 기기 그룹 및 사용자 지정 정책을 참조하십시오.
- **macOS 소프트웨어 업데이트 설정 지원 업데이트**: **macOS 소프트웨어 업데이트 설정** 구성은 macOS 27 이상 기기에서 더 이상 지원되지 않습니다. 이제 이 구성은 macOS 26.x까지의 지원되는 버전에만 적용됩니다. 자세한 내용은 **macOS 소프트웨어 업데이트 규칙 구성**을 참조하십시오.
- **제한 지원 업데이트**(iOS 27+, macOS 27+): **백그라운드 보안 개선 사항 설치 허용** 및 **백그라운드 보안 개선 제거 허용** 제한이 iOS 27 이상 및 macOS 27 이상 기기에서 더 이상 지원되지 않음을 나타내도록 업데이트되었습니다. 자세한 내용은 **iOS 제한** 및 **macOS 제한**을 참조하십시오.
- **Siri 설정 구성 업데이트**(iOS 27.0+, macOS 27.0+, tvOS 27.0+ 및 visionOS 27.0+): Siri 설정 구성에 새로운 제한 설정에 대한 지원이 추가되었습니다. 자세한 내용은 **Siri 설정**을 참조하십시오.
- **인텔리전스 설정 구성 업데이트**(iOS 27.0+, macOS 27.0+ 및 visionOS 27.0+): 인텔리전스 설정 구성에 새로운 제한 설정에 대한 지원이 추가되었습니다. 자세한 내용은 **인텔리전스 설정**을 참조하십시오.
- **Safari 개인정보 보호 설정**(iOS 27.0+, macOS 27.0+): Safari 확장 프로그램 및 설정 구성에서 Safari 개인정보 보호 설정에 대한 지원이 추가되어 관리자가 Apple 선언적 기기 관리(DDM)를 사용하여 특정 웹 사이트에 대한 기본 카메라 및 마이크 권한을 구성할 수 있습니다. 자세한 내용은 **Safari 확장 및 설정 구성**을 참조하십시오.

## Windows 기능

- **Windows AI 관리 구성**: 이제 Windows AI 관리에서 Microsoft Copilot, Windows Recall 및 Microsoft Paint AI 기능을 관리하기 위한 추가 Windows AI CSP 정책을 지원합니다. 관리자는 Copilot 하드웨어 키 비활성화, Microsoft Copilot 앱 제거, Recall의 AI 데이터 분석 비활성화, Recall 스냅샷 저장소 제한 구성, Paint의 Image Creator, Cocreator 및 Generative Fill 비활성화를 수행할 수 있습니다. 사용자 범위 및 기기 범위 정책에 대한 지원도 추가되어 Windows 기기의 AI 기능을 보다 세부적으로 제어할 수 있습니다. 추가 정보는 **Windows AI Management 구성**을 참조하십시오.

## 모바일 위협 방어 기능

모바일 위협 방어(MTD)는 기기, 네트워크, 애플리케이션에 영향을 미치는 모바일 위협 및 취약성으로부터 관리 기기를 보호합니다. 최신 릴리스에 적용할 수 있는 MTD 관련 기능에 대한 자세한 내용은 Ivanti 제품 문서 페이지의 모바일 위협 방어 섹션에서 사용하는 플랫폼에 맞는 모바일 위협 방어 솔루션 가이드를 참조하십시오.

> 각 버전의 MTD 가이드에는 현재 완전한 테스트를 거쳐 서버 환경과 클라이언트 환경에 사용할 수 있는 모바일 위협 방어 전체 기능이 나와 있습니다. 서버 릴리스와 클라이언트 릴리스 간의 차이로 인해 MTD 가이드의 신규 버전은 기능이 완전히 이용 가능할 경우에 최종 릴리스에서 시리즈로 사용할 수 있게 됩니다.

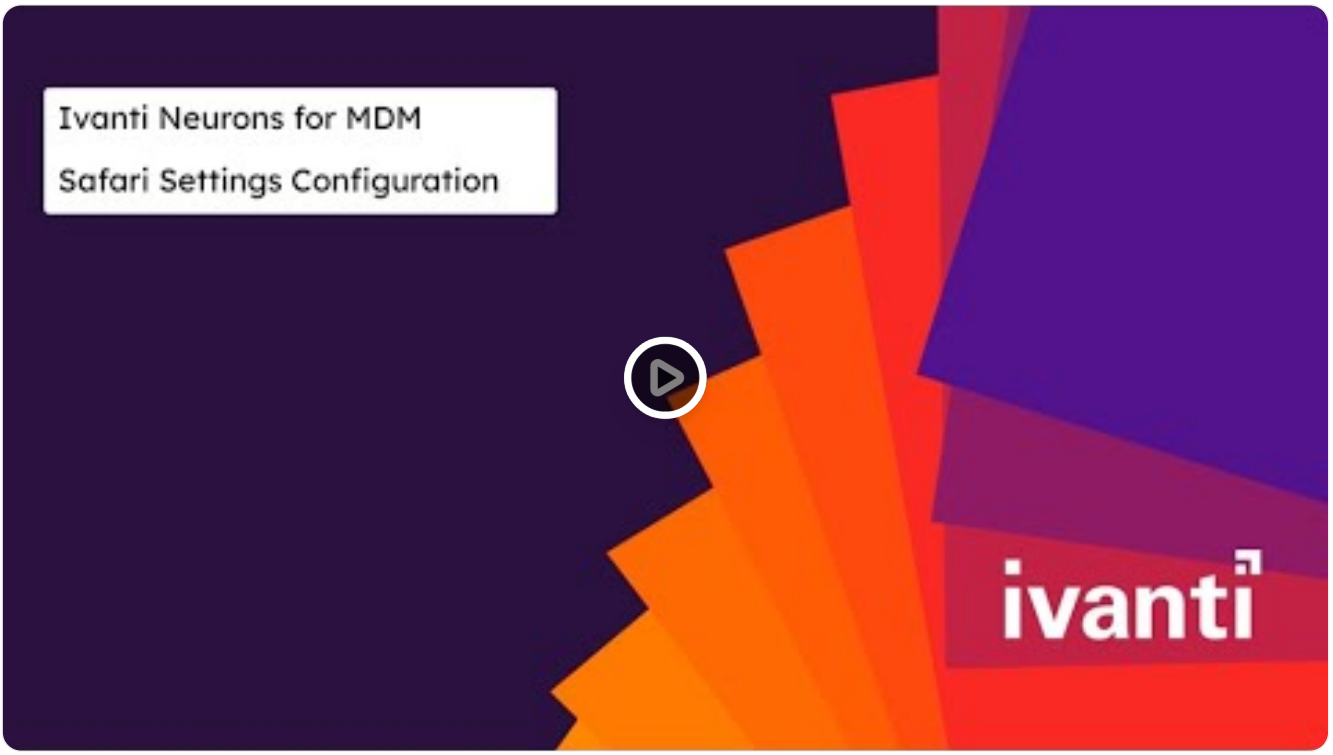
# 3. 비디오

추천 동영상


Ivanti N-MDM
Privacy Configuration
ivanti
Copyright © 2025 Ivanti. All rights reserved.


Neurons for MDM R120
Appending the
Organization Name to the
Subject of System-
generated Emails
ivanti
Copyright © 2025 Ivanti. All rights reserved.


Neurons for MDM R119
Block App Uninstall for In
House Apps
ivanti
Copyright © 2025 Ivanti. All rights reserved.




MDM용 Ivanti Neurons에서 특정 기능이나 특징에 대한 동영상을 찾고 계신가요? 문서 내 각 페이지의 "**이 글이 도움이 되었나요?**" 섹션을 통해 피드백을 공유해 주시기 바랍니다.

# 4. 시작하기

이 섹션에서는 MDM용 Ivanti Neurons 포털에서 상호 작용이 필요한 기능의 설정 및 사용 개요를 제공합니다. 이 섹션에는 다음 주제가 포함됩니다.


- 솔루션 개요
  - 핵심 기능
  - 아키텍처 다이어그램
  - MDM용 Ivanti Neurons 애플리케이션
  - 역할
  - 시작하기
- 브라우저에서 선호하는 언어 설정
- MDM용 Ivanti Neurons 및 Access의 통합 탐색 인터페이스
- Android 기기를 관리하는 기기 관리자(DA) 모드 - 지원 종료됨


## 솔루션 개요

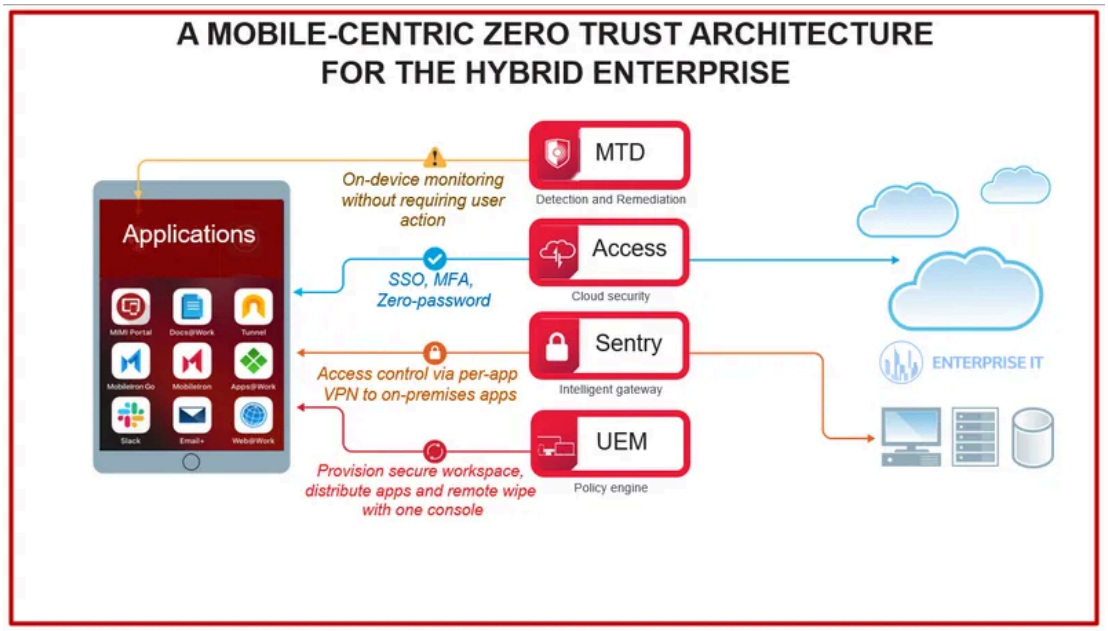
모바일 기기를 비롯하여 기업 네트워크 밖에 있는 기타 엔드포인트에서 비즈니스 데이터에 지속적으로 액세스하려면 보안에 특히 집중할 필요가 있습니다. 현재의 보안 요구를 충족하기 위해 기업은 어떻게 해야 다음이 가능할지 고려해야 합니다.

- 휴대폰 및 노트북과 같은 엔드포인트 공급
- 필수 데이터 집합 기준으로 액세스 허가
- 비사용 시 및 이동 중의 데이터 보호
- 필요에 따른 조치 시행

이러한 최신 문제에 대한 Ivanti 솔루션은 모든 챌린지를 해결합니다. 엔드포인트를 감시하고 적응형 정책을 시행하여 위협을 해소하고 기기를 격리하고 규정을 준수할 수 있습니다. 또한 다음 요소들로 기업이 모바일 중심의 제로 트러스트 프레임워크를 실현할 수 있습니다.

- MDM용 Ivanti Neurons - 역할 기반의 사용자를 위한 앱, 구성 및 정책으로 어떤 기기에서든 안전한 작업 영역을 생성할 수 있습니다. 사용자는 생산성을 위해 필요한 리소스에 쉽고 안전하게 액세스할 수 있습니다.
- **Sentry** - 온프레미스 리소스에 안전하게 액세스할 수 있도록 하는 인라인 인텔리전트 게이트웨이입니다.
- **Access** – 사용자, 기기, 앱, 네트워크 유형 및 위협의 존재를 검증할 수 있습니다. 적응형 액세스 제어 검사는 제로 트러스트 모델의 기초입니다. 액세스는 클라우드에 SSO(싱글 사인 온) 및 보안 기능을 제공합니다.
- **모바일 위협 방어** - MDM용 Ivanti Neurons 및 모바일 위협 방어(MTD)의 조합은 첨단 암호화 및 위협 모니터링을 통해 기기, 네트워크 및 앱 수준 공격을 감지하여 기기 및 네트워크 상의 데이터를 보호합니다.

다음 그림은 솔루션의 개요를 보여줍니다.



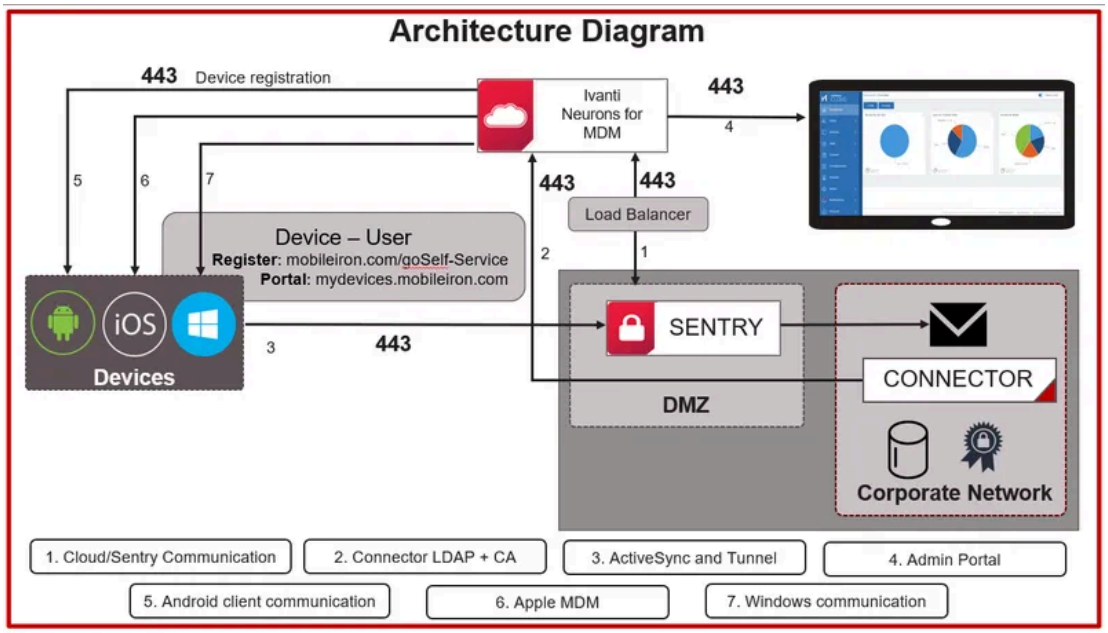

## 핵심 기능

MDM용 Ivanti Neurons 플랫폼은 비즈니스에 중요한 데이터에 액세스하는 회사 또는 직원 소유의 모바일 기기, 데스크톱을 보호, 관리 및 모니터링하는 데 필요한 기본적인 표시 유형 및 IT 제어 기능을 제공합니다. MDM용 Ivanti Neurons 플랫폼을 통해 조직은 조직 내에서 사용되는 방대한 양의 직원 기기를 보호하는 한편, 다음을 비롯하여 기기의 전체 수명 주기를 관리할 수 있습니다.

- 정책 구성 관리 및 시행
- 애플리케이션 배포 및 관리
- 데스크톱 기기용 스크립트 관리 및 배포
- 기기 작업
- 액세스 제어 및 다단계 인증
- 위협 감지 및 해결

## 아키텍처 다이어그램

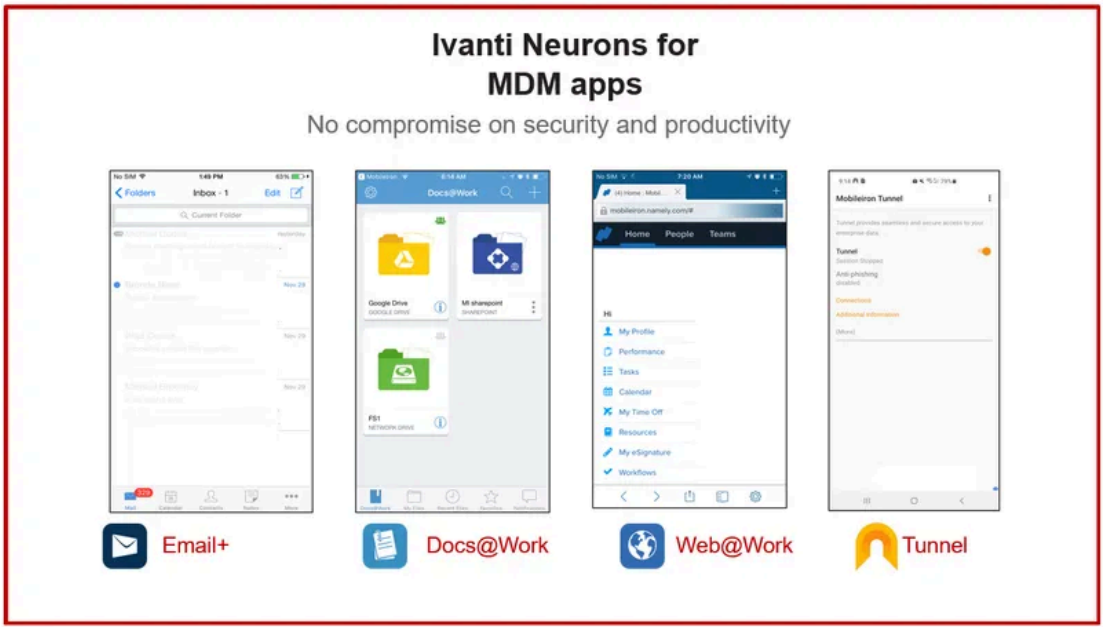
다음 다이어그램은 MDM용 Ivanti Neurons UEM 플랫폼의 구조적 개요를 보여줍니다.




## MDM용 Ivanti Neurons 애플리케이션

- **App Catalog** – App Catalog는 사용자 정의 가능한 엔터프라이즈 앱 스토어입니다. IT 관리자는 최종 사용자 기기에 비공개 또는 인하우스 앱을 직접 게시할 수 있습니다. 또한 App Catalog를 Apple 볼륨 구매 프로그램과 조합하여 iOS 기기에서 모바일 앱을 안전하게 배포하도록 할 수 있습니다. 향후에 Ivanti는 iOS 관리 앱과 Android Enterprise에서 볼 수 있는 기능을 제공할 수 있습니다. 이로써 MDM용 Ivanti Neurons UEM 플랫폼 내에서 쉽게 구성할 수 있도록 고급 앱 보안 기능을 위한 앱 수준 설정 및 보안 정책을 제공할 수 있습니다.
- **Email+** - iOS 및 Android용 PIM 애플리케이션을 보호하기 위한 교차 플랫폼입니다. Email+는 사용자 기업의 ActiveSync 서버와 통신하면서 기업 소유 기기 및 개인용 기기의 이메일, 일정, 연락처 및 작업을 안전하게 보호합니다.
- **Docs@Work** - 사용자가 Microsoft Share Point와 같은 리포지토리와 Box 및 Dropbox와 같은 클라우드 서비스에서 콘텐츠를 안전하게 액세스, 생성, 편집, 마크업, 공유할 수 있습니다. 이것은 사용자가 지속적으로 생산성을 극대화할 수 있다는 점에서 중요합니다.
- **Web@Work** - 엔터프라이즈 사용자가 기업 인트라넷에서 웹 콘텐츠에 안전하게 액세스할 수 있도록 하는 보안 브라우저입니다. Web@Work를 사용하면 권한 있는 사용자만 엔터프라이즈 데이터에 액세스하도록 제한할 수 있습니다. Web@Work를 App Tunnel과 함께 전개하면 이동 중에도 엔터프라이즈 데이터를 보호할 수 있습니다. Web@Work를 통해 사용자는 내부 웹 리소스에 빠르고 쉽게 액세스할 수 있습니다.

다음 이미지는 MDM용 Ivanti Neurons 애플리케이션을 보여줍니다.




## 역할

**관리자** - 엔터프라이즈 관리자는 다음 작업을 책임집니다.

- 엔터프라이즈 사용자가 회사 이메일, 애플리케이션, 설정, Wi-Fi 및 VPN과 같은 연결 등에 원활하고 안전하게 액세스할 수 있도록 합니다.
- 직원 기기에서 개인 데이터를 비즈니스 데이터와 분리하여 비즈니스 데이터가 개인 앱으로 유출되거나 IT 팀에서 본의 아니게 개인 데이터에 액세스하는 일이 없도록 합니다.

**사용자** - 엔터프라이즈 사용자는 안전한 최신 모바일 기기, 데스크톱 및 클라우드 서비스에서 비즈니스 애플리케이션 및 개인 데이터에 원활하게 액세스할 수 있습니다. 사용자로서 수행할 수 있는 다양한 작업에 대한 자세한 내용은 사용자 및 역할 관리를 참조하십시오.

## 시작하기

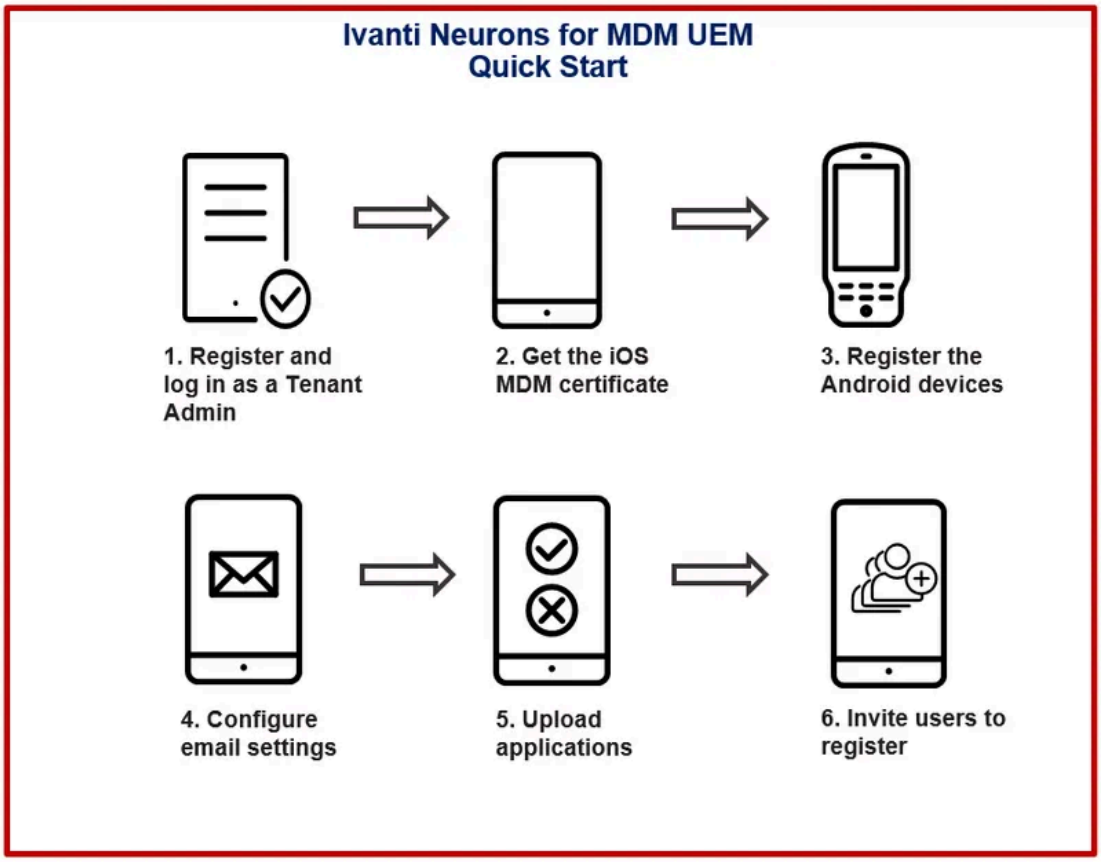
신규 등록 사용자라면 이 섹션에 나오는 단계를 수행하여 신속하게 MDM용 Ivanti Neurons 서비스에 온보딩할 수 있습니다.

MDM용 Ivanti Neurons 플랫폼을 구독하고 나면 Ivanti는 구독자를 위한 MDM용 Ivanti Neurons 테넌트를 생성합니다. 사용자는 등록한 이메일 주소로 이메일을 수신하며, 이메일에는 엔터프라이즈를 위해 생성된 테넌트에 관한 다음과 같은 정보가 담긴 PDF가 포함되어 있습니다.

- 구매한 소프트웨어 번들에 대한 정보
- 테넌트의 URL 및 슈퍼 관리자 로그인 자격 증명
- MDM용 Ivanti Neurons의 지원 커뮤니티 및 FAQ에 액세스하는 방법
- 기술 문서에 액세스하고 소프트웨어를 다운로드할 위치

> Ivanti, Inc 에서는 소프트웨어 키를 제공하지 않습니다. 슈퍼 관리자 자격 증명으로 MDM용 Ivanti Neurons 테넌트에 로그인하고 서비스 이용약관에 동의하면 MDM용 Ivanti Neurons 제품을 활성화하게 됩니다.

다음 다이어그램은 MDM용 Ivanti Neurons 시작하기 단계를 나타냅니다.




**절차**

1. 테넌트 등록 이메일에 제공된 URL을 클릭합니다. 비밀번호 재설정 프롬프트가 나타납니다.
2. 비밀번호를 변경합니다.
3. ID와 비밀번호를 사용하여 테넌트 계정에 로그인합니다. 시작 마법사가 나타납니다.
4. **시작** 양식에 세부 사항을 작성하고, 이용 약관을 수락한 후 **계속**을 클릭합니다.
5. iOS MDM 인증서를 설치하려면 **MDM 인증서 설치**를 참조하십시오.

> iOS 기기를 나중에 관리하려는 경우에는 iOS MDM 인증서 설치 단계를 건너뛸 수 있습니다. 그러면 엔터프라이즈의 Android 기기를 등록하기 위한 마법사가 나타납니다. iOS MDM 인증서 설치를 건너뛰면 iOS 기기를 등록할 수 없습니다. 사용자에게 iOS 기기 등록이 활성화되지 않았다는 메시지가 표시됩니다.

6. Android Enterprise(AE) 모드에서 Android 기기를 등록하려면 **관리되는 Google Play 계정(Android Enterprise 계정)**을 참조하십시오. 그러면 이메일 계정을 설정하라는 프롬프트가 나타납니다.

> Android 기기를 나중에 관리하는 경우에는 Android 관리 Google Play 계정 등록을 건너뛸 수 있습니다. 관리되는 Google Play 계정 등록을 건너뛰면 Android Enterprise 기기를 등록할 수 없습니다. Android 기기는 여전히 장치 관리자로 등록할 수 있지만 관리되는 Google Play 및 앱 구성과 같은 주요 기능을 사용할 수 없습니다.

7. 이메일 설정 및 ActiveSync를 구성하려면 **Exchange 구성** 및 **이메일 설정**을 참조하십시오.
8. **계속**을 클릭합니다. 암호 생성 프롬프트가 나타납니다.
9. 암호 유형을 선택한 후 **계속**을 클릭합니다.

10. 업로드하려는 애플리케이션을 선택한 후 **계속**을 클릭합니다.
11. 사용자의 이메일 주소를 지정하고 **계속**을 클릭합니다. 사용자는 모바일 기기를 등록하기 위한 이메일을 수신하게 됩니다. 구성의 요약이 표시됩니다.
12. **완료됨**을 클릭합니다. 대시보드 페이지가 표시됩니다.
13. 더 자세히 알아보려면 다음을 수행합니다.
    - **사용자**로 이동합니다. 초대된 사용자가 모두 열거됩니다.
    - **앱**으로 이동합니다. 업로드한 애플리케이션이 모두 열거됩니다.
    - **구성**으로 이동합니다. 등록 중에 푸시한 구성이 모두 열거됩니다.

관리자로서 수행할 수 있는 다양한 작업에 대한 추가 정보는 관리 섹션을 참조하십시오.

## 브라우저에서 선호하는 언어 설정

사용자가 브라우저 언어를 지원되지 않는 언어로 설정한 경우에는 en_US(영어, 미국)를 포털의 기본 언어로 설정할 수 있습니다.

macOS 10.15+ 기기에서 실행되는 Safari 브라우저에 대한 언어를 설정하려면 다음과 같이 선호하는 언어를 설정하면 됩니다.

1. macOS 기기에서 **시스템 환경설정**으로 이동합니다.
2. **언어 및 지역 > 일반**으로 이동합니다.
3. **en_US**(또는 기타 언어 옵션)를 **기본 설정 언어**로 설정합니다.

## MDM용 Ivanti Neurons 및 Access의 통합 탐색 인터페이스

일부 클러스터의 신규 고객의 경우, Access를 MDM용 Ivanti Neurons(이)가 있는 통합 탐색 인터페이스로 사용할 수 있습니다.
MDM용 Ivanti Neurons 관리자 자격 증명으로 로그인. Access 옵션은 좌측 탐색 창에서 별도의 탭으로 사용할 수 있습니다. Access에 대한 자세한 정보와 Access 설정 방법은 제품 문서 페이지로 이동하여 Access를 클릭하여 참조하십시오.

통합 탐색 인터페이스에는 다음 기능이 포함됩니다.

- MDM용 Ivanti Neurons 및 Access 모두에 통합 로그인.
- MDM용 Ivanti Neurons 및 Access 제품 간을 전환하는 좌측 탐색 창의 제품 피커.
- 제품 선택 메모리: 처음 로그인하면 MDM용 Ivanti Neurons 관리자 포털이 나타납니다. 그 이후에 로그인하거나MDM용 Ivanti Neurons Access가 나타나면 처음 로그인 시 선택한 제품을 미러링합니다.
- MDM용 Ivanti Neurons 및 Access 모두에 대한 좌측 탐색 창.
- 업그레이드 옵션, 문서, 지원 포털, 비밀번호 변경 및 로그아웃과 같은 옵션에 대한 링크가 포함된 통합 계정 설정 창

## Android 기기를 관리하는 기기 관리자(DA) 모드 - 지원 종료됨

Android 기기를 관리하는 기기 관리자(DA) 모드가 MDM용 Ivanti Neurons 78부터 단계적으로 지원 종료되고 있습니다.

MDM용 Ivanti Neurons 78에서 새로운 테넌트를 생성한 모든 신규 사용자는 DA 모드로 기기(Android 6 이상 버전)를 등록할 수 없습니다. Android 6~Android 9의 DA 등록 활성화를 원하는 새로운 테넌트는 Ivanti 지원팀에 문의하십시오.

- Android 10 이상 기기는 계속 DA 모드로 등록할 수 없습니다.
- 기존 사용자(기존 DA 배포 여부 무관)의 경우 기존 DA 기기(Android 6~Android 11) 관리와 관련된 변경 사항이 없습니다. 그러나 MDM용 Ivanti Neurons 78로 업그레이드할 경우, 기존 테넌트에서 Android 10+을 실행 중인 신규 등록된 장치도 DA 모드에서 실행할 수 없게 됩니다. 이러한 기존 테넌트는 Android 6~Android 9 버전의 기기만 DA 모드로 등록할 수 있습니다.

- 사용자가 DA 장치를 핵심 인스턴스에서 MDM용 Ivanti Neurons R78로 마이그레이션할 경우, 마이그레이션을 트리거하기 전에 Android Enterprise가 활성화되어 있고 적어도 하나의 시스템 구성이 대상 세트인 PO, DO 또는 COPE에 배포되었는지 확인해야 합니다. 이 단계는 마이그레이션 후 장치 사용 중지를 방지하는 데 필수적입니다.

| DA 등록 유형 | 기존 테넌트(78로 업그레이드) | 새 테넌트 |
|---|---|---|
| OS 10 이상 기기에서의 새로운 DA 등록 | 허용되지 않음 | 허용되지 않음 |
| OS 10 미만 기기에서의 새로운 DA 등록 | 허용됨 | 허용되지 않음 |
| OS 10 이상의 기존 DA 기기 | 활성 유지 예정 | NA |
| OS 10 미만의 기존 DA 기기 | 활성 유지 예정 | NA |
| OS 10 이상의 마이그레이션 DA 기기 | 폐기 예정 | 폐기 예정 |
| OS 10 미만의 마이그레이션 DA 기기 | 활성 유지 예정 | 폐기 예정 |

# 4.1. macOS 기기 구성하기

공통 절차와 MDM용 Ivanti Neurons에서 macOS 기기를 구성하는 것과 관련된 기타 내용을 제공하는 개요 주제입니다.
MDM용 Ivanti Neurons*관리자 가이드*에서는 모든 macOS 주제에 액세스할 수 있습니다.

**컨텐츠**


- 기기 등록하기
- 사용자 초대 템플릿 구성하기
- Zero Sign-on 기능 설정하기
- macOS 클라이언트용 Mobile@Work 설정하기
- macOS 쉘 스크립트 설정하기
- macOS 구성 설정하기
- macOS 정책 설정하기


## 기기 등록하기

대부분의 사용자들은 장치 등록부터 시작합니다. 다음 중 원하는 방법을 이용해 등록 절차를 실행할 수 있습니다.

- 한 명 이상의 최종 사용자(iReg 등록)에게 초대장을 보냅니다. 자세한 내용은 기기 등록 섹션의 *macOS 기기 등록* 항목을 확인하십시오.
- 기기 등록 및 Apple Business Manager를 통한 사용자 등록

**자세한 내용은 기기 등록을 참조하십시오.**

## 사용자 초대 템플릿 구성하기

최종 사용자 이메일 초대 브랜딩을 통해 최종 사용자에게 더 친근한 카탈로그를 제공할 수 있습니다. 자세한 내용은 **이메일 템플릿 브랜딩**을 참조하십시오.

사용자가 사용자가 인식할 이름과 로고로 기기 등록 절차를 사용자 지정할 수 있습니다. 자세한 내용은 **사용자 브랜딩**을 참조하십시오.

자세한 내용은 **등록 확인 이메일 구성 및 사용**을 참조하십시오.

## Zero Sign-on 기능 설정하기

Zero Sign-on 관련 문서는 *Access 가이드*의 Access가 있는 Zero Sign-on을 참조하십시오.

**제로터치 자동화 등록에 대해서는 사용자 설정 주제의 새 기기 등록 설정 구성하기 섹션 13단계를 참조하십시오.**

## macOS 클라이언트용 Mobile@Work 설정하기

macOS용 Mobile@Work 앱 제공 사항:

- macOS 기기의 스크립팅 기능
- 최종 사용자용 App Catalog
- 푸시 알림
- 자동화 기기 등록을 위한 사용자 온보딩(환영/상태) 화면

최종 사용자에게 Mobile@Work를 푸시하기 전에 **Mobile@Work for macOS Configuration.htmmacOS용 Mobile@Work**을 만들어 대상 macOS 기기에 배포 설정이 되었는지 확인하십시오.

자동화 **기기 등록** 프로세스 중에 macOS 기기에 대한 사용자 온보딩을 활성화할 수 있습니다. 기기 등록이 완료되자마자 macOS용 Mobile@Work가 프로필, 구성 및 앱과 함께 기기로 푸시됩니다.

## macOS 쉘 스크립트 설정하기

MDM용 Ivanti Neurons을(를) 통해 자신만의 macOS 쉘 스크립트를 생성할 수 있으며 그런 다음, 이를 MDM용 Ivanti Neurons에 업로드하여 관리되는 macOS 기기에서 실행할 수 있습니다. macOS 스크립트용 Mobile@Work 구성을 사용하여 스크립트를 구성할 수 있습니다. macOS용 Mobile@Work는 스크립트 실행 결과를 MDM용 Ivanti Neurons(으)로 반환하며, 이는 기기 로그에 나타납니다. **로그** 탭의 macOS 기기 상세 정보 페이지에서 기기 로그를 확인할 수 있습니다. 스크립트 리포지토리 생성, 업로드 및 관리에 대한 자세한 내용은 **모든 스크립트**를 참조하십시오.

macOS 기기에서 쉘 스크립트를 실행하기 전 사용자는 기기에서 macOS용 Mobile@Work 앱이 실행되고 있는지, 그리고 macOS용 Mobile@Work 구성이 기기로 푸시되었는지 확인하십시오. 스크립트는 한 번 또는 반복적으로 실행할 수 있습니다. MDM용 Ivanti Neurons에서의 스크립팅으로 관리자가 기기에서 정보를 수집하고 MDM용 Ivanti Neurons에 사용자 지정 속성으로 이를 저장할 수도 있습니다. 예를 들어 macOS 기기에서 Java 버전에 대해 알아야 할 경우 이 정보를 수집하여 사용자 지정 기기 속성에 기기별로 저장할 수 있습니다. 자세한 내용은 **macOS용 Mobile@Work**에서 *macOS용 Mobile@Work 스크립트 구성 생성*을 참조하십시오.

## macOS 구성 설정하기

**구성**은 기기에 보내는 여러 설정 값의 모음입니다. 예를 들어, 구성을 이용해 자동으로 VPN 및 장치 암호 규격 관련 설정을 할 수 있습니다. **구성** 페이지를 이용해 구성을 선택, 설정, 배포할 수 있습니다. 다양한 **구성 유형**을 활용할 수 있습니다. **페이지**에서는 다음 구성을 비롯하여 사용 가능한 macOS 구성 목록을 볼 수 있습니다.

- **Wi-Fi**
- **암호**
- **VPN**
- **암호화된 DNS**
- **FileVault 2**
- **FileVault 복구 키**
- **macOS 방화벽**
- **macOS 제한**
- **macOS 앱스토어 제한 사항**
- **macOS 파인더 설정**
- **macOS 커널 확장 정책**
- **활성 디렉토리(macOS)**
- **Office 365 자동 계정 생성(macOS)**

**사용자 지정 구성**을 사용하여 사전 정의된 구성 파일을 가져오고 배포할 수 있습니다.

## macOS 정책 설정하기

**정책** 메뉴에서는 기기 요건을 비롯해 기기가 요건을 충족하지 않을 경우 발생하는 결과값을 설정할 수 있습니다. 각 정책은 하나의 규칙과 컴플라이언스 조치(규칙을 위반한 경우 결과)로 구성됩니다. **정책** 페이지에서 정책을 선택하고 설정, 배포할 수 있습니다. 데이터 보호/암호화 비활

성화됨 및 **허용된 앱**은 macOS 관련 정책입니다. **사용자 지정 정책**을 사용하여 지정하는 기기 및 사용자 속성, 섹션 기준, 값 및 컴플라이언스 조치를 바탕으로 사용자 지정 정책을 생성할 수 있습니다.

## macOS 앱 배포하기

MDM용 Ivanti Neurons 에서는 Apple의 MDM 프로토콜 및 Mobile@Work 앱을 통해 macOS **앱** 배포를 지원합니다. 관리자는 다음 접근법 중 하나 또는 둘 모두를 선택할 수 있습니다.

- Apple의 MDM 프로토콜 - 관리자는 인하우스 앱으로 특정 PKG 형식(배포 형식)만을 업로드할 수 있으며 Mac App Store에서 앱을 배포할 수도 있습니다(Apple의 Apps 및 Books 라이센스 지원 포함). 그러나 이러한 접근을 통해 관리자가 DMG 및 기타 PKG를 배포할 수 있는 것은 아닙니다.
- macOS용 Mobile@Work 앱 - 앱을 사용자에게 배포할 수 있는 방법으로, 관리자는 MobileIron Packager(MIP) 앱을 사용하여 PKG, DMG 또는 .app 파일을 MIP 파일로 변환할 수 있습니다. MIP 파일을 인하우스 앱으로 MDM용 Ivanti Neurons에 업로드합니다.

> MobileIron 소프트웨어 다운로드에서 MDM용 Ivanti Neurons Mac Packager 유틸리티를 다운로드할 수 있습니다.

관리자는 Mobile@Work를 사용하여 DMG, PKG 또는 .app 형식에 있는 인하우스 앱을 배포할 수 있습니다. Mac App Store에서만 사용할 수 있는 앱의 경우 관리자는 계속해서 Apple의 기본 MDM 기능을 사용할 수 있으며, 여기에는 Apple Apps 및 Book 라이센스 기능이 포함됩니다.

# 4.2. 등록 확인 이메일 구성 및 사용

관리자는 등록을 완료한 후 이메일을 구성하고 사용자에게 트리거할 수 있습니다. 등록에 성공한 후 이 이메일에는 예를 들어 사용자에 대한 추가 지침이 포함될 수 있습니다. 관리자는 사용자 초대 중 이 이메일의 전송을 활성화할 수 있습니다.

프로세스:

- **기능 구성하기:**
  - 이메일 템플릿 구성: 영문 이메일 템플릿의 기본값은 이와 같지만, **이메일 템플릿 브랜딩**의 **이메일 템플릿 사용자 정의하기**에 제시된 지침에 따라 수정하면 목적에 더욱 부합하도록 조정할 수 있습니다.



  - 등록 확인 이메일을 켭니다. **사용자 설정**에서 **사용자 등록 확인 이메일 구성하기**를 확인하십시오.
- **기능 사용하기:**
  - **사용자 초대하기**에 제시된 설명에 따라 사용자에게 등록 초대를 전송합니다. 사용자가 등록에 성공하면 MDM용 Ivanti Neurons에서 해당 사용자에게 등록 확인 이메일을 전송합니다.

# 4.3. 정책 규정 준수 알림 이메일 구성 및 사용

관리자는 사용자 지정 정책 및 허용된 앱 정책의 이메일 전송 조치에 따라 보유 기기가 규정 준수 범위를 벗어난 사용자에게 보내는 이메일을 정책 규정 준수 알림 이메일 템플릿에 래핑할 수 있습니다. 다음 프로세스는 구성에 대해 설명합니다.

- **기능 구성하기:**
  - **이메일 템플릿을 구성합니다.**
    영문 이메일 템플릿의 기본값은 이와 같지만, 이메일 템플릿 브랜딩의 이메일 템플릿 사용자 정의하기에 제시된 지침에 따라 수정하면 목적에 더욱 부합하도록 조정할 수 있습니다.
    
  - **정책 규정 준수 알림 템플릿을 켭니다.** 이 템플릿은 사용자 지정 정책 및 허용된 앱 정책의 이메일 전송 조치를 사용하여 작성한 메시지와 함께 동작합니다. MDM용 Ivanti Neurons는 그러한 이메일 조치에서 지정한 정보를 정책 규정 준수 알림 템플릿에 삽입합니다. 사용자 지정 앱 또는 허용된 앱 정책을 만들거나 수정할 때 정책 규정 준수 이메일 템플릿을 켤 수 있습니다. 사용자 지정 정책 또는 허용된 앱 정책 각각에 대한 정책 규정 준수 알림 템플릿을 활성화하는 방법에 대한 자세한 지침은 사용자 지정 정책 추가 및 허용된 앱 정책 생성을 각각 참조하십시오.
- **기능 사용하기:**
  - 기기가 정책 알림 템플릿이 활성화된 사용자 지정 앱 또는 허용된 앱 정책을 준수하지 않는 경우, MDM용 Ivanti Neurons에서 기기 소유자에게 이메일을 전송하고 정책 알림 템플릿에 해당 이메일을 먼저 배치합니다. 사용자와 이 기능의 상호 작용은 위에서 요약한 대로 기능을 구성하는 것이지만, MDM용 Ivanti Neurons는 이 기능을 그대로 사용합니다.

# 4.4. 주문형 기능

MDM용 Ivanti Neurons 에는 기본적으로 비활성화되어 있는 특정 주문형 기능이 포함되어 있습니다. 해당 기능은 성능에 약간의 영향을 미칠 수 있으며 실운영에 배포될 준비가 완료되지 않은 상태일 수 있습니다.

기본적으로 비활성화된 테넌트 기기에서 온디맨드 기능을 하나 이상 활성화하는 데 관심이 있는 관리자는 **지원** 부서에 문의하면 됩니다.

다음 표에는 문서로 작성된 주문형 기능의 목록이 포함되어 있습니다.

| 기능 | 설명 | 플랫폼 | 라이센스 |
| --- | --- | --- | --- |
| Windows 10 기능 | Windows 10 기기에 적용 가능한 기능. | Windows 10 | • 레거시: Gold<br>• 현재: 보안 EUM 레거시 및 현재 제품에 관한 자세한 내용은 **패키지**를 참조하십시오. |
| 앱 카탈로그 URL 클립보드에 복사 | 관리자가 앱에서 앱 카탈로그 URL을 클립보드에 복사할 수 있는 권한을 제공합니다. 해당 URL은 이메일을 통해 사용자에게 배포될 수 있습니다. 사용자가 등록된 기기에서 링크를 클릭할 경우, 앱이 포함된 앱 카탈로그가 브라우저에 실행되며, 사용자는 앱 설치 여부를 선택할 수 있습니다.<br>관리자는 대상이 되는 사용자에 대한 URL 배포를 제한할 책임이 있습니다. | • iOS<br>• macOS | NA(테넌트 특정) |
| 웹 클립을 앱으로 설정 | App Catalog에 **웹 클립**을 앱으로 설정하면 사용자가 App Catalog에서 웹 애플리케이션을 사용할 수 있습니다. 웹 클립은 구성으로 정의될 수 있지만 구성은 관리자만이 푸시할 수 있습니다. 사용자는 기기에서 웹 애플리케이션 설치 또는 해제를 선택할 수 있습니다. 하지만 사용자에게는 웹 클립 구성을 해제할 옵션이 없습니다. | iOS | NA(테넌트 특정) |
| 허용 목록에 있는 기기의 등록 켜기 | 사용자 > **사용자 설정** > 기본값 기기 등록 설정에서 허용 목록에 있는 일련 번호를 기반으로 기기 등록을 허용합니다. | • iOS<br>• macOS | NA(테넌트 특정) |
| 인증서 기반 인증 | **인증서 기반 인증** 기능을 활용하면 관리자는 디지털 인증서와 테넌트 지정 호스트 이름 또는 베니티 호스트 이름을 사용하여 로그인할 수 있습니다. 이러한 인증 설정은 **관리** 탭의 아래 베니티 호스트 구성을 사용하여 구성할 수 있습니다. | 이 기능은 플랫폼에 고유한 것이 아닙니다. | NA(테넌트 특정)<br>이 기능은 지원팀이 활성화하는 경우 NA3 클러스터 환경에서만 이용할 수 있습니다. |
| 전용 기기 구성 생성(기업 소유의 일회용 기기 또는 COSU 기기) | 관리자는 전용 기기(기업 소유의 일회용 기기 또는 COSU 기기)를 사용하여 Android Enterprise를 사용하는 고유의 목적에 사용할 수 있는 전용 기기를 구성할 수 있습니다. **COSU 구성**은 사용자가 키오스크 모드에서 사용할 수 있는 유일한 앱을 제공하기 위해 업무 관리 기기(기기 소유자 모드)에 배포됩니다. | Android Enterprise | 라이센스 |
| 대시보드 비활성 기간 | 기본적으로 대시보드 비활성 기간은 15일로 설정됩니다. 이는 테넌트의 니즈에 따라 업데이트할 수 있으며 설정 가능한 최장 기간은 30일입니다. 비활성 기간을 더 길게 설정해야 할 경우 **지원** 팀에 문의하십시오. | 이 기능은 플랫폼에 고유한 것이 아닙니다. | |

# 4.5. Android Enterprise 기기 지원 준비

이 섹션에서는 Android Enterprise 기기의 최소 네트워크 요구 사항에 대해 설명합니다. 일반적으로, Android 기기에서는 올바로 기능하기 위해 방화벽에서 인바운드 포트를 열지 않아도 됩니다. 그러나 관리자가 Android 엔터프라이즈 기기용 네트워크 환경을 설정할 경우 알아둬야 할 아웃바운드 연결이 다수 존재합니다.

다음 표에 제시되는 네트워크 변경 사항 목록은 완전한 것이 아니라 바뀔 수 있으며 엔터프라이즈 관리 API 및 GMS 앱의 현재 및 과거 버전에 대한 알려진 엔드포인트를 다룹니다.

> 다음 표에 나열된 포트 외에도 Android Enterprise 기기는 MDM용 Ivanti Neurons에 액세스해야 합니다.

Android Enterprise 기기 요구 사항에 대한 정보는 Android Enterprise 도움말의 **Android Enterprise 네트워크 요구 사항**을 참조하십시오.

Google은 특정 IP를 제공하지 않으므로 방화벽이 여기(**http://bgp.he.net/AS15169#_prefixes**)에 나열된 15169의 Google ASN에 열거된 IP 차단에 포함된 모든 IP 주소로 나가는 연결을 수용하도록 허용해야 합니다.

> Google 피어 및 에지 노드의 IP는 AS15169 차단에 나열되어 있지 않습니다. Google의 에지 네트워크에 관한 자세한 내용은 **https://peering.google.com/**을 참조하십시오.

# 5. 대시보드

대시보드에서는 등록된 기기 및 사용자에 관한 중요 통계 정보를 확인할 수 있습니다. 대시보드의 각 섹션을 위젯이라고 합니다. 각 위젯의 설정 항목:

- 화면에 표시된 데이터의 범주(기기나 사용자 등)
- 데이터 그룹화 방법(OS 버전 또는 모델별 등)
- 데이터 필터링 방법(iOS 기기만 표시 또는 OS 빌드 버전별 표시 등)
- 데이터 표시 방법(원 그래프, 막대 그래프 등)

## 보고서 및 기타 정보 확인하기

**대시보드**에서는 등록된 기기와 사용자에 관한 중요 통계 정보를 확인할 수 있습니다. 대시보드의 각 섹션을 위젯이라고 합니다.

다음과 같이 추가 정보를 확인할 수 있습니다.

- **알림 검토**: **대시보드 > 알림** 페이지로 이동하거나 오른쪽 상단의 벨 아이콘을 클릭하여 알림을 검토하고 필요한 경우 조치를 취합니다.
- **보고서**: **대시보드 > 보고서** 페이지로 이동하여 통합 엔드포인트 관리(UEM) 시스템의 데이터에 액세스합니다.
- **감사 내역**: **대시보드 > 감사 내역** 페이지로 이동하여 MDM용 Ivanti Neurons 내 모든 엔터티에서 수행된 활동을 수집하여 시간 순서대로 작성한 기록 세트에 액세스합니다. 이 기능을 활성화하려면 **관리자 > 인프라 > 감사 내역** 페이지로 이동하여 **감사 내역 활성화**를 클릭합니다.
- 앱 인사이트 - **대시보드 > 앱 인사이트** 페이지로 이동하여 앱 배포 및 기타 앱 상세 정보를 보고 분석합니다.

이 섹션에는 다음 항목도 포함됩니다.

- 위젯 작업
- 앱 인사이트
- 정기 보고서 사용
- 사용자 지정 보고서 사용

# 5.1. 위젯 작업

이 섹션에는 다음 주제가 포함됩니다.

- 위젯 추가
- 위젯 배치
- 위젯 수정
- 알림 검토
- 보고서
- 감사 내역

대시보드에서는 등록된 기기 및 사용자에 관한 중요 통계 정보를 확인할 수 있습니다. 대시보드의 각 섹션을 위젯이라고 합니다. 각 위젯의 설정 항목:

- 화면에 표시된 데이터의 범주(기기나 사용자 등)
- 데이터 그룹 설정 기준(OS 버전이나 모델별 등)
- 데이터 필터링 방법(예: iOS 기기만 표시하기 등)
- 데이터 표시 방법(원 그래프, 막대 그래프 등)

## 위젯 추가

1. **추가**(우측 상단)를 클릭합니다.
2. 추가할 위젯 이름을 설정하세요.
3. 데이터 범주를 선택하세요.
4. 화면에 표시되는 필터링 옵션을 설정하세요.
5. 기본 표시 유형(원그래프, 막대그래프, 선그래프)을 선택하세요.
6. **완료**를 클릭합니다.

## 위젯 배치

위젯은 항상 한 줄에 3개씩 표시됩니다. 단, 위젯이 표시되는 순서는 변경할 수 있습니다.

1. **배치**(우측 상단)를 클릭합니다.
2. 위젯을 표시하고 싶은 순서대로 박스를 드래그하세요.
3. **확인**을 클릭합니다.

## 위젯 수정

1. 원하는 위젯의 설정 아이콘(우측 상단)을 클릭하세요.
2. **편집**을 선택합니다.
3. 원하는 속성을 수정하세요.
4. **완료**를 클릭합니다.

## 알림 검토

벨 아이콘(우측 상단)을 클릭하거나 **대시보드 > 알림** 페이지로 이동하여 알림을 검토한 후 다음 기준에 따라 필요한 경우 조치를 취합니다.

- 구성요소 유형
  - 앱
  - LDAP
  - Entra ID
  - 기기 허용 목록
  - Apps 및 Books
  - iOS
  - 안드로이드
  - macOS
  - visionOS
  - watchOS
  - tvOS
  - 테넌트
  - CA
  - Connector
  - Sentry
  - 기기 등록 서버 토큰

알림 유형

  - 만료
  - 데이터 동기화
  - 사용 제한
  - 관리 작업
  - 서버 인증 오류
  - 검증 오류
  - 상태 변경

심각도

  - 지워짐
  - 정보
  - 위험
  - 경고

관리자는 알림 페이지와 벨 알림 섹션에서 앱 구성 요소를 선택하여 모든 앱별 알림을 신속하게 검토할 수 있습니다. Google Play 앱에 대해 허용할 새 권한이 있는 경우 관리자는 각 앱 페이지를 방문하여 해당 권한을 검토하고 허용하는 대신 해당 알림을 클릭하면 권한을 허용할 수 있습니다.

> MDM용 Ivanti Neurons 고객/테넌트는 Android Go 앱을 앱 카탈로그로 가져오지 않은 경우에도 Android Go 앱 승인 알림을 받게 됩니다.

### 사용자 비밀번호 만료와 ID 변경 알림 검토

관리자는 **알림** 페이지에서 예정된 비밀번호 만료 기간을 확인할 수 있습니다. 관리자는 2주에서 하루 전까지 사전에 비밀번호 만료 알림을 받을 수 있습니다. 이 알림에는 해당 사용자 명단을 포함한 CSV 보고서 파일 링크도 있습니다. 비밀번호가 만료되고 나면 알림이 더 이상 생성되지 않습니다.

또한, 관리자는 지난 LDAP 동기화에서 ID(UID)가 변경된 것으로 탐지된 사용자 명단 알림도 확인할 수 있습니다.

**알림 지우기**

필요할 때면 언제든 **알림** 페이지에서 심각도에 대한 이러한 알림을 수동으로 지울 수 있습니다.

1. **알림** 페이지에서 지우려는 알림에 대한 **작업** 열의 아이콘을 클릭하십시오. **알림 지우기 확인** 창이 표시됩니다.
2. **알림 지우기**를 클릭합니다. 지울 때 알림 상태가 **상태** 열에서 **지워짐**으로 변경됩니다.

> **알림** 페이지에 지워진 알림의 총 개수가 표시됩니다.

## 보고서

**대시보드 > 보고서** 페이지에서 Unified Endpoint Management(UEM) 시스템 데이터에 액세스할 수 있습니다. 예를 들어 관리자는 기기 및 차단된 기기 보고서를 작성하면서 해당 필터 옵션을 사용하여 기기 공간 이름 및 기기 사용자 지정 속성과 같은 정보를 보고서에 추가할 수 있습니다. 따라서 이러한 보고서에는 기기 공간 이름 및 기기 사용자 지정 속성에 해당하는 열이 각각 생기게 됩니다. 사용자 지정 기기 속성은 보고서를 작성하는 동안 필터링 옵션 아래에서 사용할 수 있습니다. 관리자는 기기에 사용된 사용자 지정 기기 속성 키 목록에서 선택하고 사용 가능한 운영자를 선택할 수 있습니다.

76부터MDM용 Ivanti Neurons모든 보고서 템플릿에 대한 연산자는 표준 연산자를 갖습니다. 다음 템플릿의 운영자는 이 릴리스에서 표준화됩니다.

- 대시보드 > 보고서 > 보고서 생성

보고서 워크플로:

1. 선택 - 사전 정의된 보고서 템플릿을 선택합니다.
2. 범위 정의 - 보고서 데이터 기간을 설정합니다.
3. 세부 정보 설정 - 보고서 이름을 입력하고 맞춤 설정합니다.
4. 실행/예약 - 보고서를 즉시 실행하거나 예약을 생성합니다.
5. 공유 - 보고서 수신 대상을 지정합니다.

**관련 항목**:

- 대시보드 > 보고서(예약됨)
- 대시보드 > 보고서(사용자 지정)

**빠른 검색:** 보고서 탭으로 이동합니다. 빠른 검색 필드를 통해 다음과 같은 열에서 검색할 수 있습니다. 띄어쓰기 또는 특수문자를 포함하여서도 검색할 수 있습니다.

- 이름
- 설명
- 템플릿 이름

## 감사 내역

**감사 내역**은 MDM용 Ivanti Neurons에서 수행된 활동을 시간순으로 기록합니다. 이러한 기록에는 관리자, 최종 사용자 및 시스템 구성요소가 수행한 작업이 포함됩니다.

관리자는 **감사 내역**을 사용하여 변경 사항을 검토하고, 작업을 확인하고, 문제를 해결하고, 규정 준수 검사를 지원합니다. **감사 내역**은 기기를 포함한 관리형 엔터티의 추가, 업데이트 및 삭제 등의 작업을 추적합니다. 자세한 내용은 기기 등록(iOS, macOS, Android)을 참조하십시오.

## 감사 내역 활성화

MDM용 Ivanti Neurons 내에서 수행된 활동을 캡처하려면 **감사 내역** 옵션을 활성화해야 합니다.

**절차**

1. **관리** > **인프라** > **감사 내역**으로 이동합니다.
   **감사 내역** 창이 나타납니다.
2. **감사 내역 내보내기** 토글 버튼을 선택하여 ON으로 설정합니다.

> 감사 내역 옵션을 활성화한 후에는 비활성화할 수 없습니다. 비활성화하려면 Ivanti 지원에 문의하십시오.

## 감사 내역 보기

**감사 내역**에 대한 자세한 내용을 보려면 다음 단계를 따르십시오.

**절차**

1. **대시보드** > **감사 내역**으로 이동합니다.

**감사 내역** 창이 나타납니다.

2. 다음 표에는 **감사 내역** 창에 표시되는 상세 정보가 나열되어 있습니다.

| 설정 | 설명 |
| --- | --- |
| 아이콘 | 감사 이벤트의 활동 아이콘을 표시합니다. |
| 활동 | 기기 체크인 또는 관리자 로그인 등 발생한 작업을 표시합니다. |
| 상태 | 활동의 성공 또는 실패 여부를 표시합니다.<br>보고서가 실패하면 **보고서 기록**에서 보고서 작업을 다시 시도할 수 있습니다. 새 보고서 일정을 생성하지 않고 실패한 작업을 다시 실행하려면 이 옵션을 사용합니다. |
| 수행자 | 활동을 수행한 관리자 또는 사용자를 표시합니다. |
| 수행 위치 | 활동이 발생한 날짜 및 시간을 표시합니다. |
| 수행된 날짜 | 활동의 영향을 받는 기기, 계정 또는 개체를 표시합니다. |
| 상세 정보 | 활동에 대한 추가 정보를 표시합니다. |
| 유형 | 기기 작업 또는 계정 등의 활동 유형을 표시합니다. |
| 범주 | 기기 관리 또는 관리자 포털 액세스 등의 활동과 관련된 기능 영역을 표시합니다. |

3. **작업** 버튼을 클릭하여 다음 옵션을 수행합니다.
- **감사 내역 설정 구성**: 이 옵션을 선택하면 **관리** > **인프라** > **감사 내역**에 **감사 내역** 구성이 표시됩니다.
- **CSV로 내보내기**: **감사 내역**을 내보내고 다운로드하려면 이 옵션을 선택합니다.
4. (선택 사항) **필터**를 사용하여 특정 **감사 내역**을 볼 수 있습니다.

## 활동 상세 정보 보기

**변경 - 이전 & 이후** 아이콘이 **대시보드** > **감사 내역** > **상세 정보** 열에 표시됩니다. 관리자가 감사된 작업 전후의 특성 값을 비교하는 데 도움이 됩니다. 이 비교를 통해 변경된 내용을 더 쉽게 식별하고, 사용자 또는 시스템 활동을 확인하며, 구성 업데이트 문제를 해결할 수 있습니다.

아이콘을 클릭하여 **감사 내역 변경 - 이전 & 이후** 창에서 감사 내역 비교 상세 정보를 확인하면 다음의 상세 정보가 표시됩니다.

| 설정 | 설명 |
| --- | --- |
| 속성 | 수정된 속성의 이름을 표시합니다.<br>예를 들어, `createdAt` 입니다. |
| 이전 | 작업이 수행되기 전의 속성 값을 표시합니다.<br>빨간색으로 강조 표시됩니다. |
| 이후 | 작업이 수행된 후의 속성 값을 표시합니다.<br>녹색으로 강조 표시됩니다. |

## 감사 내역의 고급 검색

고급 검색 옵션을 사용하여 규칙을 기준으로 감사 내역을 검색합니다. 활동을 식별하고 확인하기 위한 특정 기준을 정의합니다. 다음 속성을 사용하여 고급 검색을 수행할 수 있습니다.

- **활동**
- **범주**
- **만든 시간**
- **수행자**
- **수행된 날짜**
- **공간 이름**
- **상태**
- **유형**

## 감사 내역 보고서 생성

**감사 내역** 보고서를 12시간 또는 24시간마다 실행하도록 예약하거나 사용자 지정 보고서를 생성할 수 있습니다. 또한 필요에 따라 **감사 내역** 보고서를 실행할 수 있습니다. 온디맨드 보고서는 예약되지 않으며 지난 24시간의 **감사 내역** 데이터를 포함합니다.

다음 형식 중 하나로 감사 내역 보고서를 생성할 수 있습니다.

- CSV
- JSON
- CEF

또한 **감사 내역** > **보고서 배포**에 대한 보고서를 생성할 때 **SFTP 내보내기** 옵션을 선택하여 모든 감사 내역 정보를 특정 서버 위치로 내보내고 업로드할 수 있습니다. 감사 내역 내보내기에는 SFTP(Secure Shell File Transfer Protocol)가 사용됩니다. 기본 포트를 통해 서버에 액세스할 수 있어야 합니다. **감사 내역 내보내기** 설정을 구성하여 감사 내역 아카이브를 특정 위치에 매일 자동으로 업로드할 수 있습니다. 자세한 정보는 감사 내역 내보내기를 참조하십시오.

보고서 생성에 대한 자세한 내용은 정기 보고서 사용 및 사용자 지정 보고서 사용을 참조하십시오.

# 5.2. 앱 인사이트

이 섹션에는 다음 주제가 포함됩니다.

- 앱 배포 보기
- 앱 상세 정보 보기
- 단일 앱 배포 차트 추가
- 비관리 iOS 앱 파트 추가
- 설치된 관리 앱 상위 10개 추가
- 상위 5개 등급 인하우스 앱 추가

앱 인사이트는 다음 앱 배포를 확인 및 분석하는 데 도움이 되는 대시보드 내의 기능입니다.

- 설치가 필요한 인하우스 앱 배포
- 설치가 필요한 퍼블릭 앱 배포
- 비관리 iOS 앱
- 설치된 관리 앱 상위 10개
- 상위 5개 등급 인하우스 앱

설치가 필요한 상위 5개 앱 분석: 이 앱들은 다수의 사용자에게 배포되었지만 그에 비해 설치율이 낮은 인하우스 또는 퍼블릭 앱입니다. 비관리 iOS 앱 차트는 기기의 비관리 앱에 대한 정보를 제공합니다. 비관리 앱 목록, 설치되어 있는 기기 목록을 확인하고, 앱을 관리 앱으로 변환하기 위한 조치를 취할 수 있게 됩니다. 이는 배포를 개선하기 위한 관리자의 주의 또는 조치가 필요한 앱 배포입니다. 이 차트는 이미 앱이 설치된 기기를 나타냅니다. 도넛 차트는 퍼블릭 및 인하우스 앱 배포에 대한 높은 수준의 개요를 제공합니다. 이는 앱 설치가 필요한 기기의 수를 분석하는 데 도움이 될 뿐만 아니라 차트의 특정 부분을 클릭하여 앱별 정보를 얻을 수 있습니다. 또한, 단일 앱의 버전별 배포를 나타내는 단일 배포 차트를 추가할 수도 있습니다.

> 대시보드에는 지난 15일 동안 확인된 기기에 대한 정보만 표시됩니다.

## 앱 배포 보기

**대시보드**의 **앱** 페이지에서 다음 차트를 볼 수 있습니다.

- 설치가 필요한 인하우스 앱 배포
- 설치가 필요한 퍼블릭 앱 배포
- 비관리 iOS 앱

기본적으로 인하우스 앱 5개, 퍼블릭 및 비관리 iOS 앱 5개에 대한 차트가 표시됩니다. 그래프는 미설치율이 높은 앱 순서대로 왼쪽에서 오른쪽으로 나열되어 있습니다.

도넛 차트는 2개의 색상을 표시하여 설치 상태를 나타냅니다. 파란색은 앱이 설치된 기기의 수를 나타냅니다. 빨간색은 설치가 필요한 기기의 수를 나타냅니다. 각 색상을 마우스로 가리키면 기기의 수가 표시됩니다.

상단 우측의 삭제 옵션을 클릭하여 차트를 삭제할 수 있습니다.

## 앱 상세 정보 보기

도넛 차트의 중앙에도 설치가 필요한 기기의 수가 표시됩니다. 예: 750/1000은 기기 1000개 중 750개에서 설치가 필요하다는 것을 의미합니다.

도넛 차트는 3개의 색상을 표시하여 앱 배포 상태를 나타냅니다.

- 파란색은 앱이 설치된 기기의 수를 나타냅니다. 차트의 파란색 부분을 클릭하면 **기기** 페이지로 이동합니다. **기기** 페이지의 **앱 버전** 열은 설치된 앱 버전과 앱이 설치된 날짜를 표시합니다.

> 좌측 패널의 **버전** 섹션에서 옵션을 선택하여 설치된 앱 버전을 기준으로 기기를 확인할 수 있습니다.

- 빨간색은 앱 설치가 필요한 기기의 수를 나타냅니다. 차트의 빨간색 부분을 클릭하면 **기기** 페이지로 이동합니다. **기기** 페이지에서 앱 설치가 필요한 기기를 볼 수 있습니다.

차트 중앙에 앱 아이콘이 표시됩니다. 아이콘을 클릭하면 **앱 > App Catalog**의 앱 상세 정보 페이지로 이동합니다.

이 페이지에서 **앱이 설치된 기기** 탭을 클릭하여 선택한 앱의 기기 목록을 확인합니다.

**앱이 설치되지 않은 기기** 탭을 클릭하여 선택한 앱이 설치되지 않은 기기 목록을 확인합니다.

## 단일 앱 배포 차트 추가

앱 페이지에서 특정 버전 앱의 단일 배포 도넛 차트를 추가할 수 있습니다. 빨간색은 앱이 설치되어 있어야 하는 기기의 목록을 의미합니다. 이 차트는 앱 배포에 대한 다음 세부 정보를 도표로 나타냅니다.

- 특정 버전의 앱이 설치된 기기
- 다른 버전의 앱이 설치된 기기
- 앱이 설치되지 않은 기기

**절차**

1. **앱** 페이지에서 **+추가**를 클릭합니다. **앱 차트 추가** 창이 표시됩니다.
2. **차트 유형** 드롭다운 목록에서 **단일 앱 배포**를 선택합니다.
3. 단일 앱 배포 차트를 보고자 하는 앱 목록의 체크박스를 선택합니다.

> 앱 검색 필드에서 앱 이름을 입력하여 특정 앱을 검색할 수 있습니다.

4. **차트 추가**를 클릭합니다. 앱 페이지에 단일 앱 배포 차트가 표시됩니다.

> 목록에서 최대 9개 앱을 선택할 수 있습니다.

차트 중앙에 특정 앱 버전이 설치된 기기 수가 표시됩니다.

예: 5/10는 기기 10개 중 5개에 특정 앱 버전이 설치되었다는 것을 의미합니다.

도넛 차트는 3개의 색상을 표시하여 앱 배포 상태를 나타냅니다.

- 녹색은 특정 버전의 앱이 설치된 기기의 수를 나타냅니다. 차트의 녹색 부분을 클릭하면 **기기** 페이지로 이동합니다. 기기 페이지에는 특정 버전의 앱이 설치된 기기 목록이 표시됩니다. 좌측 패널의 **AppVersion** 섹션에서 옵션을 선택하여 다른 설치된 앱 버전을 기준으로 기기를 볼 수 있습니다.
- 밝은 녹색은 다른 버전의 앱이 설치된 기기의 수를 나타냅니다. 차트의 밝은 녹색 부분을 클릭하면 **기기** 페이지로 이동합니다. 기기 페이지에는 다른 버전의 앱이 설치된 기기 목록이 표시됩니다. 좌측 패널의 **AppVersion** 섹션에서 버전 옵션을 선택하여 다른 설치된 앱 버전을

기준으로 기기를 볼 수 있습니다.
- 빨간색은 앱이 설치되지 않은 기기의 수를 나타냅니다. 각 색상을 마우스로 가리키면 기기의 수가 표시됩니다. 차트의 빨간색 부분을 클릭하면 **기기** 페이지로 이동합니다. 기기 페이지에는 앱이 설치되지 않은 기기 목록이 표시됩니다. 좌측 패널에는 App catalog에서 앱을 사용할 수 있게 되는 날짜가 표시됩니다.

차트 중앙에 앱 아이콘이 표시됩니다. 아이콘을 클릭하면 **앱 > App Catalog**의 앱 상세 정보 페이지로 이동합니다. 이 페이지에서 **앱이 설치된 기기** 탭을 클릭하여 선택한 앱의 기기 목록을 확인합니다. **앱이 설치되지 않은 기기** 탭을 클릭하여 선택한 앱이 설치되지 않은 기기 목록을 확인합니다.

상단 우측의 삭제 옵션을 클릭하여 차트를 삭제할 수 있습니다.

## 비관리 iOS 앱 파트 추가

앱 페이지에서 비관리 iOS 앱 차트를 추가하여 비관리 앱 목록을 파악하고 볼 수 있습니다. 이 차트는 관리자가 비관리 iOS 앱을 카탈로그에 추가할 때 자동으로 나타납니다. 관리자는 필요에 따라 이 차트를 삭제 또는 추가할 수 있습니다.

**절차**

1. **앱** 페이지에서 **+추가**를 클릭합니다. **앱 차트 추가** 창이 표시됩니다.
2. **차트 유형** 드롭다운 목록에서 **비관리 iOS 앱**을 선택합니다.
3. **차트 추가**를 클릭합니다. 비관리 iOS 앱 차트가 **앱** 페이지에 표시됩니다.

차트가 앱 카탈로그 내 비관리 앱 개수를 표시합니다. 차트 하단에 다음과 같은 상세 정보가 담긴 3개의 열이 표시됩니다.

- **비관리 iOS 앱이 있는 기기** - 비관리 iOS 앱의 개수를 표시합니다. 링크를 클릭하여 비관리 iOS 앱이 있는 기기 창에서 비관리 앱이 있는 기기 목록을 보십시오.
- **앱 카탈로그 내 총 앱 개수** - 앱 카탈로그에서 사용 가능한 앱의 총 수를 표시합니다.
- **비관리 iOS 앱(%)** - 비관리 iOS 앱을 퍼센트로 표시합니다.

iTune App Store에서 앱이 이미 설치되어 있는 경우, 앱과 그 데이터를 관리 앱으로 변환할 수 있습니다. 앱을 관리 앱으로 변환하는 방법:

1. **비관리 iOS 앱이 있는 기기 열**에서 숫자 링크를 클릭합니다. **비관리 iOS 앱** 창이 표시됩니다.
2. 목록에서 1개 이상의 비관리 앱을 선택하고 비관리 iOS 앱 아래의 숫자 링크를 클릭합니다. 선택된 앱이 관리 앱으로 변환되고 다음 기기 체크인 시 상태가 업데이트됩니다.

> **CSV로 내보내기** 링크를 클릭하여 관리되지 않는 앱의 데이터를 CSV 형식으로 내보낼 수 있습니다.

## 설치된 관리 앱 상위 10개 추가

앱 페이지에서 설치된 관리 앱 상위 10개를 사용하여 설치된 관리 앱 상위 10개 목록을 파악하고 볼 수 있습니다. 관리자는 필요에 따라 이 차트를 삭제 또는 추가할 수 있습니다.

기본적으로 설치된 관리 앱 상위 10개 차트는 **앱** 페이지에서 사용할 수 있습니다. 차트가 삭제된 경우, 관리자가 **앱** 페이지에서 추가할 수 있습니다.

**절차**

1. **앱** 페이지에서 **+추가**를 클릭합니다. **앱 차트 추가** 창이 표시됩니다.
2. **차트 유형** 드롭다운 목록에서 **설치된 관리 앱 상위 10개**를 선택합니다.
3. **차트 추가**를 클릭합니다. 설치된 관리 앱 상위 10개 차트가 **앱** 페이지에 표시됩니다.

**보기** 드롭다운 목록에서 선택한 범주에 따라 설치된 관리 앱 상위 10개를 볼 수 있습니다. 이용 가능한 범주는 다음과 같습니다.

- **모든 앱**(기본으로 선택됨)
- **인하우스 앱**
- **퍼블릭 앱**

차트의 각 막대가 각각의 특정 앱에 표시되며 앱 이름 또한 표시됩니다. 각 바를 마우스로 가리켜서 플랫폼(Android, iOS 또는 Windows) 및 앱으로 설치된 기기 수를 보십시오.

특정 앱의 바를 클릭하면 앱으로 설치된 기기 세부 사항을 표시하는 **기기** 페이지로 이동합니다. 기기 페이지의 좌측 패널은 앱으로 설치된 기기 수를 나타냅니다. 좌측 패널의 X 버튼을 클릭하면 다시 대시보드의 **앱** 페이지로 이동합니다.

상단 우측의 삭제 옵션을 클릭하여 차트를 삭제할 수 있습니다.

## 상위 5개 등급 인하우스 앱 추가

앱 페이지에서 상위 5개 등급 인하우스 앱 차트를 사용하여 상위 5개 등급 인하우스 앱 목록을 파악하고 볼 수 있습니다. 관리자는 필요에 따라 이 차트를 삭제 또는 추가할 수 있습니다.

기본적으로 상위 5개 등급 인하우스 앱 차트는 **앱** 페이지에서 사용할 수 있습니다. 차트가 삭제된 경우, 관리자가 **앱** 페이지에서 추가할 수 있습니다.

**절차**

1. **앱** 페이지에서 **+추가**를 클릭합니다. **앱 차트 추가** 창이 표시됩니다.
2. **차트 유형** 드롭다운 목록에서 **상위 5개 등급 인하우스 앱**을 선택합니다.
3. **차트 추가**를 클릭합니다. 상위 5개 등급 인하우스 앱 차트가 **앱** 페이지에 표시됩니다.

이 차트는 앱에 대한 별표 등급과 함께 해당 앱에 대한 로고를 통해 데이터를 나타냅니다. 별표 등급은 정수 표시(최대 5 등급)와 함께 별표 이미지로 나타납니다. 앱의 등급을 매긴 사용자 수도 표시됩니다.

> 앱에 대한 등급 수는 해당 관리자와 공간에 국한된 기기만이 아니라 모든 앱 사용자의 등급을 기반으로 합니다. 등급은 등록된 기기의 Apps@Work에서 해당 앱을 본 다양한 사용자가 해당 앱에 대해 제시한 모든 등급의 평균입니다.

특정 앱을 클릭하면 앱의 특정 상세 정보가 표시된 **앱 상세 정보** 페이지를 탐색합니다.

상단 우측의 삭제 옵션을 클릭하여 차트를 삭제할 수 있습니다.

# 5.3. 정기 보고서 사용

**라이센스**: Silver

정기 보고서 기능을 사용하면 바로 사용할 수 있는 사전 패키지 템플릿으로 다양한 지표에 관한 보고서를 예약하고 생성할 수 있습니다. 이 기능에 접근하려면 시스템 관리자 또는 시스템 읽기 전용 권한이 있어야 합니다. 보고서는 현재 최대 40개까지 생성할 수 있습니다.

> 기기에 다수의 Tunnel 인스턴스가 생성된 경우 동일 기기에 대한 정책 위반 보고서에 여러 개의 레코드가 있을 수 있습니다. 이것은 표준 보고서뿐 아니라 사용자 지정 보고서에도 해당됩니다.

## 보고서 생성

보고서를 예약하고 생성할 수 있습니다.

**절차**

1. **대시보드** > **보고서**로 이동합니다.
2. **보고서 생성**을 클릭해 보고서 템플릿 선택 페이지를 표시합니다.
3. 구성한 옵션에서 보고서의 템플릿을 선택합니다.
   - **차단된 기기**: Sentry가 현재 액세스가 차단된 기기에 대해 보고합니다.
   - **기기:**: 시스템의 모든 파티션에 있는 기기에 대해 보고합니다.
   - **정책 위반**: 시스템에서 정책 위반에 대해 보고합니다.
   - **사용자**: 시스템에서 사용자에 대해 보고합니다.
   - **사용자 비밀번호 만료 상태**: 시스템에서 사용자의 비밀번호 만료 상태를 보고합니다.
   - **가장 많이 설치된 앱**: 시스템의 모든 애플리케이션에 대해 보고하며, 각 애플리케이션이 설치된 횟수로 정렬합니다.
   - **비관리형 앱**: 시스템에서 비관리형 애플리케이션에 대해 보고합니다.
   - **모든 애플리케이션**: 사용자가 관리하는 기기의 모든 애플리케이션에 대해 보고합니다.
   - **감사 내역**: MDM용 Ivanti Neurons 내의 모든 엔터티에서 수행된 모든 활동에 대해 보고합니다.
4. **다음**을 클릭합니다.
   **보고서 세부 정보** 페이지가 표시됩니다.
   - **보고서 이름**을 입력하십시오.
   - (선택사항) 보고서에 대한 **설명**을 입력하십시오.

다음 옵션에서 **이벤트 범위**를 선택합니다.
기존 보고서의 경우:

- **모든 이벤트**
- **전날**
- **지난주**
- **지난달**
- **이전 범위** - MDM용 Ivanti Neurons 관리 포털의 이전 릴리스에서 범위 슬라이더를 사용하여 만든 보고서를 표시합니다. 관리자가 보고서에 대해 위의 옵션 중 하나를 선택하여 저장하면 이전 범위 옵션이 표시되지 않습니다. 범위 값은 보고서 요약 페이지에 표시됩니다.

새 보고서의 경우:

- **모든 이벤트**
- **전날**
- **지난주**
- **지난달**

**다음**을 클릭합니다. 보고서 데이터 페이지가 표시됩니다.

6. **보고서 열** 섹션에서 열을 추가, 제거 또는 재정렬하려면 **열 사용자 지정**을 클릭합니다. 또는 열 이름을 클릭하여 추가된 열을 제거합니다.
7. (선택 사항) **모든 열 선택** 확인란을 사용하여 목록에 표시된 모든 열을 선택합니다.
8. **기본값 복원**을 클릭하여 앞서 생성된 열로 되돌립니다. 사용자 지정 항목이 없는 열로 되돌리려면 **보고서 템플릿 선택** 페이지에 있는 템플릿 중 하나를 선택하면 됩니다.
9. **고급 필터** 섹션의 특정 규칙을 기반으로 필터를 생성합니다.

> 일부 보고서에는 모든 필터 옵션을 사용할 수 없습니다. 사용 가능한 필터 목록에 대한 자세한 내용은 이 절차 아래의 필터 항목을 참조하십시오.

> 보고서 생성 시 Windows 장치에서 BitLocker 암호화, OS 버전, 시스템 버전, 마더보드 제조업체, 마더보드 제품, 마더보드 상태, BIOS 제조업체, BIOS 버전, 하드 드라이브 파티션, 광학 드라이브 유형, CPU 이름, CPU 상태와 같은 신규 하드웨어 특성을 사용할 수 있습니다.

10. (선택 사항) **+** 아이콘을 클릭하면 다른 규칙을 추가할 수 있으며, **그룹 추가** 아이콘을 클릭하여 규칙 그룹을 추가할 수도 있습니다.
11. **다음**을 클릭합니다. 보고서 일정 페이지가 표시됩니다.
12. 보고서를 다운로드하려면 다음 형식 중 *하나*를 선택합니다.
    - CSV
    - PDF
    - **CSV 및 PDF**
      PDF 보고서 파일의 경우, 최대 10개의 열이 허용됩니다. 보고서 차트 섹션에는 PDF 보고서에 포함될 두 가지 유형의 차트가 표시됩니다.
      **모든 애플리케이션** 보고서는 CSV 형식만 지원합니다.

반복을 설정하여 보고서가 자동으로 실행되도록 설정하려면 **자동 예약**을 클릭합니다. 또는 **수동**을 클릭하여 보고서를 한 번 실행하면 이메일로 전송됩니다.

- **반복 보고서** 옵션 중 *하나*를 선택합니다.
  - **일일**
  - **주간**
  - **월간**
  - **이전 일정** - 기존 보고서의 경우
- **시작 날짜**와 **종료 날짜**를 선택합니다(선택 사항).

14. **다음**을 클릭합니다. 보고서 배포 페이지가 표시됩니다. 보고서 수신자를 선택합니다.
15. (선택 사항) **외부 이메일 추가** 링크를 클릭하여 외부 이메일 ID를 추가합니다.
16. **완료**를 클릭합니다. **보고서 배포 요약이** 나타납니다.

17. (선택 사항) **편집**을 클릭하여 보고서를 수정합니다.
18. **저장**을 클릭하세요.
19. 다운로드 아이콘을 클릭하고 보고서 형식을 선택합니다. 보고서를 다운로드할 수 있는 **보고서 다운로드** 버튼이 포함된 이메일을 보고서의 수신자에게 전송합니다.

## 필터

| 규칙 옵션 | 설명 |
| --- | --- |
| **활성화 잠금 활성화됨** | **예** 또는 **아니요**로 활성화되는 활성화 잠금 기반 규칙.<br>규칙 예: '활성화 잠금 활성화는 예와 같음'. |
| **앱 터널 상태** | **차단** 또는 **허용**으로 지정되는 앱 터널 상태 규칙.<br>규칙 예: '앱 터널 상태가 차단과 같음'. |
| **배터리 수준** | 기기의 배터리 수준 값.<br>규칙 예: "배터리 수준이 1,080임"<br>배터리 수준에 입력한 값은 초 단위여야 합니다. |
| **클라이언트 마지막 체크인** | 날짜 범위 내 클라이언트 마지막 체크인을 기반으로 하는 규칙.<br>규칙 예: '클라이언트 마지막 체크인이 범위 04/02/2019 06:00:00,04/05/2019 17:00:00 내에 있음'. |
| **준수 상태** | 컴플라이언스 상태 **예** 또는 **아니요**를 기반으로 하는 규칙.<br>규칙 예: '컴플라이언스 상태는 예입니다'. |
| **현재 국가 이름** | 현재 국가 이름을 입력합니다.<br>규칙 예: '컴플라이언스 상태는 프랑스와 같음'. |
| **현재 MCC** | 현재 모바일 국가 코드를 기반으로 한 규칙.<br>규칙 예: '현재 MCC는 410임'. |
| **현재 MNC** | 현재 모바일 네트워크 코드를 기반으로 한 규칙.<br>규칙 예: '현재 MNC는 06임'. |
| **기기 등록 활성화됨** | **예** 또는 **아니요**로 활성화되는 기기 등록 기반 규칙<br>규칙 예: '기기 등록 활성화됨은 예와 같음' |
| **피싱 방지 기본 상태** | 다음 피싱 방지 기본 상태 옵션 중 하나를 선택하십시오.<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 활성화 안 됨<br>• 해당 없음<br>• 활성화됨<br>• 알 수 없음 |
| **피싱 방지 VPN 상태** | 다음 피싱 방지 VPN 상태 옵션 중 하나를 선택하십시오.<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 활성화 안 됨<br>• 해당 없음<br>• 활성화됨<br>• 알 수 없음 |

| 규칙 옵션 | 설명 |
| --- | --- |
| **기기 등록에 등록됨** | **예** 또는 **아니요**로 기기 등록에 등록된 기반 규칙<br>규칙 예: '기기 등록에 등록됨은 예와 같음' |
| **데이터 보호** | 기기에서 데이터 보호가 활성 상태인지 나타냅니다. 가능한 값은 **예** 또는 **아니요**입니다.<br>규칙 예: '데이터 보호는 예와 같음'. |
| **데이터 로밍 활성화됨** | **예** 또는 **아니요**로 활성화되는 데이터 로밍 기반 규칙.<br>규칙 예: '데이터 로밍 활성화는 예와 같음'. |
| **기기 차단 상태** | 기기 차단 상태를 기반으로 한 규칙.<br>규칙 예: '기기 차단 상태가 차단과 같음'. |
| **기기 ID** | 특정 기기 ID 또는 기기 ID 범위 내에 있는 규칙입니다.<br>규칙 예: '기기 ID는 45보다 큽니다'. x |
| **자국 MCC** | 자국 모바일 국가 코드를 기반으로 한 규칙.<br>규칙 예: '홈 MCC는 310임'. |
| **자국 MNC** | 자국 모바일 네트워크 코드를 기반으로 한 규칙.<br>규칙 예: '홈 MNC는 510임'. |
| **IMEI** | 특정 IMEI 값에 대한 규칙입니다.<br>규칙 예: 'IMEI가 9900으로 시작' |
| **초대 상태** | 다음 초대 상태 옵션 중 하나를 선택합니다.<br>• 없음<br>• 보류 중<br>• 만료됨<br>• **완료됨**<br>규칙 예: '초대 상태가 보류 중입니다'. |
| **로케이터 서비스 활성화됨** | **예** 또는 **아니요**로 활성화되는 로케이터 서비스 기반 규칙.<br>규칙 예: '로케이터 서비스 활성화는 예와 같음'. |
| **MTD 활성 상태** | 다음 MTD 활성화 상태 옵션 중 하나를 선택하십시오.<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 해당 없음<br>• 오류<br>• 보류 중<br>• 보호됨 |
| **격리 상태** | **예** 또는 **아니요**로 활성화되는 로케이터 서비스 기반 규칙.<br>규칙 예: '격리 상태는 예와 같음'. |

| 규칙 옵션 | 설명 |
| --- | --- |
| **등록된 시간** | 기기가 등록된 시간의 날짜 및 시간 범위를 선택하기 위한 규칙입니다.<br>규칙 예: '등록된 시간 범위: 10/03/2017 09:00:00,10/20/2017 17:00:00'. |
| **로밍** | 로밍을 기반으로 하는 규칙입니다(**예** 또는 **아니요**).<br>규칙 예 '로밍은 예입니다' |
| **상태** | 다음 초대 상태 옵션 중 하나를 선택합니다.<br>• 활성화<br>• 폐기 보류 중<br>• 폐기 전송<br>• 폐기됨<br>• 폐기 취소됨<br>• 지우기 보류 중<br>• 지우기 전송됨<br>• 지워짐<br>• 지우기 취소됨<br>규칙 예: '상태는 폐기 보류 중과 같음'. |
| **음성 로밍 활성화됨** | **예** 또는 **아니오**로 활성화되는 음성 로밍 기반 규칙<br>규칙 예 '음성로밍 활성화는 예입니다' |
| **Wi-Fi MAC 주소** | 특정 Mac 주소 값을 입력합니다.<br>규칙 예: 'Wifi Mac 주소는 00-14-22-01-23-45입니다'. |
| **iCloud 백업 기능 활성화됨** | **예** 또는 **아니요**로 활성화되는 iCloud 백업 기능 기반 규칙.<br>규칙 예: 'iCloud 백업 기능 활성화는 예와 같음' |
| **iTunes Store 계정 활성화 상태** | **예** 또는 **아니요**로 지정되는 iTunes Store 계정 활성화 상태 기반 규칙.<br>규칙 예: 'iTunes Store 계정 활성화 상태는 아니요와 같지 않음.' |
| **플랫폼 유형** | 모든 애플리케이션 보고서에 적용 가능합니다. |
| **소스** | 모든 애플리케이션 보고서에 적용 가능합니다. |
| **사용자 지정 속성** | 모든 애플리케이션 보고서에 적용 가능합니다. |
| **관리형** | 모든 애플리케이션 및 가장 많이 사용된 애플리케이션 보고서에 적용 가능합니다. |
| **앱 식별자** | 모든 애플리케이션 보고서의 기본값입니다. |
| **MEID** | 비관리형 앱 보고서에 적용됩니다. |

## 예약된 보고서 페이지에서 보고서 작업 수행

예약된 보고서 페이지에서 다양한 작업을 수행할 수 있습니다.

**절차**

1. **대시보드** > **보고서**로 이동합니다.
2. **내 예약된 보고서** 페이지에서 **작업** 드롭다운 메뉴를 클릭한 후 다음 옵션 중 하나를 선택합니다.

| 작업 옵션 | 수행된 작업 |
| --- | --- |
| **보기** | 보고서를 확인할 수 있습니다. |
| **편집** | 보고서를 편집할 수 있습니다. 이 보고서를 사용하면 마지막 릴리스에서 이전 범위로 선택한 범위도 볼 수 있습니다. |
| **지금 실행** | 보고서를 실행합니다. |
| **CSV 다운로드** | CSV 포맷의 보고서를 다운로드합니다. |
| **PDF 다운로드** | PDF 형식으로 보고서를 다운로드합니다. |
| **삭제** | 보고서를 삭제합니다. |

## 보고서 세부 정보 보기

보고서 세부 정보를 확인하고 생성된 보고서에 대해 일부 작업을 수행할 수 있습니다.

**절차**

1. **대시보드** > **보고서**로 이동합니다.
2. **내 예약된 보고서** 페이지에서 보고서 이름을 클릭하여 보고서 세부 정보를 확인합니다. 보고서 페이지가 열립니다.
3. 이 페이지에서 보고서 요약 및 보고서 기록을 볼 수 있습니다.

관련 주제:

- 사용자에게 사용자 지정 역할을 할당하려면 **역할 할당**을 참조하십시오.
- 기본 역할 목록은 **사용자 역할**을 참조하십시오.
- **역할 관리**
- **사용자 지정 보고서 사용**

# 5.4. 사용자 지정 보고서 사용

**라이센스**: Gold

사용자 지정 보고서 기능을 통해 사용 준비가 된 템플릿으로 다양한 메트릭에서 보고서를 사용자 지정하고 생성할 수 있습니다. 이 기능에 접근하려면 시스템 관리자 또는 시스템 읽기 전용 권한이 있어야 합니다. 보고서는 현재 최대 40개까지 생성할 수 있습니다.

이 섹션에는 다음 주제가 포함됩니다.

보고서 생성

보고서 작업 수행

보고서 세부 정보 보기

## 보고서 생성

MDM용 Ivanti Neurons 관리 포털에서 보고서를 예약 및 생성할 수 있습니다.

**절차**

1. **대시보드** > **보고서**로 이동합니다.
2. **보고서 생성**을 클릭해 보고서 템플릿 선택 페이지를 표시합니다.
3. 구성한 옵션에서 보고서 템플릿을 선택합니다.
   - **차단된 기기**: Sentry가 현재 액세스가 차단된 기기에 대해 보고합니다.
   - **기기:**: 시스템의 모든 파티션에 있는 기기에 대해 보고합니다.
   - **정책 위반**: 시스템에서 정책 위반에 대해 보고합니다.
   - **사용자**: 시스템에서 사용자에 대해 보고합니다.
   - **사용자 비밀번호 만료 상태**: 시스템에서 사용자의 비밀번호 만료 상태를 보고합니다.
   - **가장 많이 설치된 앱**: 시스템의 모든 애플리케이션에 대해 보고하며, 각 애플리케이션이 설치된 횟수로 정렬합니다.
   - **비관리형 앱**: 시스템에서 비관리형 애플리케이션에 대해 보고합니다.
   - **모든 애플리케이션**: 사용자가 관리하는 기기의 모든 애플리케이션에 대해 보고합니다.
   - **감사 내역**: MDM용 Ivanti Neurons 내의 모든 엔터티에서 수행된 모든 활동에 대해 보고합니다.
4. **다음**을 클릭합니다. 보고서 세부 정보 페이지가 표시됩니다.
5. **보고서 이름**을 입력하십시오.
6. (선택사항) 보고서에 대한 **설명**을 입력하십시오.
7. 다음 옵션에서 **이벤트 범위**를 선택합니다.
   기존 보고서의 경우:
   - **모든 이벤트**
   - **전날**
   - **지난주**
   - **지난달**
   - **이전 범위** - MDM용 Ivanti Neurons 관리 포털의 이전 릴리스에서 범위 슬라이더를 사용하여 만든 보고서를 표시합니다. 관리자가 보고서에 대해 위의 옵션 중 하나를 선택하여 저장하면 이전 범위 옵션이 표시되지 않습니다. 범위 값은 보고서 요약 페이지에 표시됩니다.

새 보고서의 경우:

- **모든 이벤트**
- **전날**
- **지난주**
- **지난달**

**다음**을 클릭합니다. 보고서 데이터 페이지가 표시됩니다.

9. **사용자 지정**을 클릭해 사용자 지정 보고서를 생성합니다.

> **대시보드 > 보고서** 페이지에서 템플릿 이름 열에 괄호 안에 "사용자 지정"이 표시되어 보고서가 사용자 지정되었음을 나타냅니다.

10. **보고서 열** 섹션에서 열을 추가, 제거 또는 재정렬하려면 **열 사용자 지정**을 클릭합니다. 또는 열 이름을 클릭하여 추가된 열을 제거합니다.
11. (선택 사항) **모든 열 선택** 확인란을 사용하여 목록에 표시된 모든 열을 선택합니다.
12. **기본값 복원**을 클릭하여 앞서 생성된 열로 되돌립니다. 사용자 지정 없이 열로 되돌리려면 **보고서 템플릿 선택** 페이지에서 템플릿 중 하나를 선택할 수 있습니다. 기본 열은 자물쇠 아이콘으로 표시됩니다.
13. **고급 필터** 섹션의 특정 규칙을 기반으로 필터를 생성합니다.

> 일부 보고서에는 모든 필터 옵션을 사용할 수 없습니다. 사용 가능한 필터 목록에 대한 자세한 내용은 이 절차 아래의 필터 항목을 참조하십시오.

> 보고서 생성 시 Windows 장치에서 BitLocker 암호화, OS 버전, 시스템 버전, 마더보드 제조업체, 마더보드 제품, 마더보드 상태, BIOS 제조업체, BIOS 버전, 하드 드라이브 파티션, 광학 드라이브 유형, CPU 이름, CPU 상태와 같은 신규 하드웨어 특성을 사용할 수 있습니다.

14. (선택 사항) **+** 아이콘을 클릭하면 다른 규칙을 추가할 수 있으며, **그룹 추가** 아이콘을 클릭하여 규칙 그룹을 추가할 수도 있습니다.
15. **다음**을 클릭합니다. 보고서 일정 페이지가 표시됩니다.
16. 보고서를 다운로드하려면 다음 형식 중 *하나*를 선택합니다.
    - **CSV**
    - **PDF**
    - **CSV 및 PDF**
      PDF 보고서 파일의 경우, 최대 10개의 열이 허용됩니다. 보고서 차트 섹션에 PDF 보고서에 포함될 2가지 유형의 차트가 표시됩니다. **모든 애플리케이션** 보고서는 CSV 형식만 지원합니다.

반복을 설정하여 보고서가 자동으로 실행되도록 설정하려면 **자동 예약**을 클릭합니다. 또는 **수동**을 클릭하여 보고서를 한 번 실행하면 이메일로 전송됩니다.

- **반복 보고서** 옵션 중 *하나*를 선택합니다.
  - **일일**
  - **주간**
  - **월간**
  - **이전 일정** - 기존 보고서의 경우
- **시작 날짜**와 **종료 날짜**를 선택합니다(선택 사항).

지금 실행 옵션은 일회성 보고서를 생성합니다. 동일한 템플릿을 사용하여 예약된 보고서를 생성할 수 있습니다. **대시보드 > 보고서** 페이지의 빈도 및 다음 예약 열에 이러한 보고서의 예약되지 않은 상태가 표시됩니다.

18. **다음**을 클릭합니다. 보고서 배포 페이지가 표시됩니다. 보고서 수신자를 선택합니다.
19. (선택 사항) **외부 이메일 추가** 링크를 클릭하여 외부 이메일 ID를 추가합니다.
20. **완료**를 클릭합니다. **보고서 배포 요약이** 나타납니다.
21. (선택 사항) **편집**을 클릭하여 보고서를 수정합니다.
22. **저장**을 클릭하세요.
23. 다운로드 아이콘을 클릭하고 보고서 형식을 선택합니다. 보고서를 다운로드할 수 있는 **보고서 다운로드** 버튼이 포함된 이메일을 보고서의 수신자에게 전송합니다.

## 필터

| 규칙 옵션 | 설명 |
| --- | --- |
| **활성화 잠금 활성화됨** | **예** 또는 **아니요**로 활성화되는 활성화 잠금 기반 규칙.<br>규칙 예: '활성화 잠금 활성화는 예와 같음'. |
| **앱 터널 상태** | **차단** 또는 **허용**으로 지정되는 앱 터널 상태 규칙.<br>규칙 예: '앱 터널 상태가 차단과 같음'. |
| **배터리 수준** | 기기의 배터리 수준 값.<br>규칙 예: "배터리 수준이 1,080임"<br>배터리 수준에 입력한 값은 초 단위여야 합니다. |
| **클라이언트 마지막 체크인** | 날짜 범위 내 클라이언트 마지막 체크인을 기반으로 하는 규칙.<br>규칙 예: '클라이언트 마지막 체크인이 범위 04/02/2019 06:00:00,04/05/2019 17:00:00 내에 있음'. |
| **준수 상태** | 컴플라이언스 상태 **예** 또는 **아니요**를 기반으로 하는 규칙.<br>규칙 예: '컴플라이언스 상태는 예입니다'. |
| **현재 국가 이름** | 현재 국가 이름을 입력합니다.<br>규칙 예: '컴플라이언스 상태는 프랑스와 같음'. |
| **현재 MCC** | 현재 모바일 국가 코드를 기반으로 한 규칙.<br>규칙 예: '현재 MCC는 410임'. |
| **현재 MNC** | 현재 모바일 네트워크 코드를 기반으로 한 규칙.<br>규칙 예: '현재 MNC는 06임'. |
| **기기 등록 활성화됨** | **예** 또는 **아니요**로 활성화되는 기기 등록 기반 규칙<br>규칙 예: '기기 등록 활성화됨은 예와 같음' |
| **피싱 방지 기본 상태** | 다음 피싱 방지 기본 상태 옵션 중 하나를 선택하십시오.<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 활성화 안 됨<br>• 해당 없음<br>• 활성화됨<br>• 알 수 없음 |
| **피싱 방지 VPN 상태** | 다음 피싱 방지 VPN 상태 옵션 중 하나를 선택하십시오.<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 활성화 안 됨<br>• 해당 없음<br>• 활성화됨<br>• 알 수 없음 |

| 규칙 옵션 | 설명 |
| --- | --- |
| **기기 등록에 등록됨** | **예** 또는 **아니요**로 기기 등록에 등록된 기반 규칙<br>규칙 예: '기기 등록에 등록됨은 예와 같음' |
| **데이터 보호** | 기기에서 데이터 보호가 활성 상태인지 나타냅니다. 가능한 값은 **예** 또는 **아니요**입니다.<br>규칙 예: '데이터 보호는 예와 같음'. |
| **데이터 로밍 활성화됨** | **예** 또는 **아니요**로 활성화되는 데이터 로밍 기반 규칙.<br>규칙 예: '데이터 로밍 활성화는 예와 같음'. |
| **기기 차단 상태** | 기기 차단 상태를 기반으로 한 규칙.<br>규칙 예: '기기 차단 상태가 차단과 같음'. |
| **기기 ID** | 특정 기기 ID 또는 기기 ID 범위 내에 있는 규칙입니다.<br>규칙 예: '기기 ID는 45보다 큽니다'. x |
| **자국 MCC** | 자국 모바일 국가 코드를 기반으로 한 규칙.<br>규칙 예: '홈 MCC는 310입니다'. |
| **자국 MNC** | 자국 모바일 네트워크 코드를 기반으로 한 규칙.<br>규칙 예: '홈 MNC는 510임'. |
| **IMEI** | 특정 IMEI 값에 대한 규칙입니다.<br>규칙 예: 'IMEI가 9900으로 시작' |
| **초대 상태** | 다음 초대 상태 옵션 중 하나를 선택합니다.<br>• 없음<br>• 보류 중<br>• 만료됨<br>• **완료됨**<br>규칙 예: '초대 상태가 보류 중입니다'. |
| **로케이터 서비스 활성화됨** | **예** 또는 **아니요**로 활성화되는 로케이터 서비스 기반 규칙.<br>규칙 예: '로케이터 서비스 활성화는 예와 같음'. |
| **MTD 활성 상태** | 다음 MTD 활성화 상태 옵션 중 하나를 선택하십시오.<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 해당 없음<br>• 오류<br>• 보류 중<br>• 보호됨 |
| **격리 상태** | **예** 또는 **아니요**로 활성화되는 로케이터 서비스 기반 규칙.<br>규칙 예: '격리 상태는 예와 같음'. |

| 규칙 옵션 | 설명 |
| --- | --- |
| **등록된 시간** | 기기가 등록된 시간의 날짜 및 시간 범위를 선택하기 위한 규칙입니다.<br>규칙 예: '등록된 시간 범위: 10/03/2017 09:00:00,10/20/2017 17:00:00'. |
| **로밍** | 로밍을 기반으로 하는 규칙입니다(**예** 또는 **아니요**).<br>규칙 예 '로밍은 예입니다' |
| **상태** | 다음 초대 상태 옵션 중 하나를 선택합니다.<br>• 활성화<br>• 폐기 보류 중<br>• 폐기 전송<br>• 폐기됨<br>• 폐기 취소됨<br>• 지우기 보류 중<br>• 지우기 전송됨<br>• 지워짐<br>• 지우기 취소됨<br>규칙 예: '상태는 폐기 보류 중과 같음'. |
| **음성 로밍 활성화됨** | **예** 또는 **아니오**로 활성화되는 음성 로밍 기반 규칙<br>규칙 예 '음성로밍 활성화는 예입니다' |
| **Wi-Fi MAC 주소** | 특정 Mac 주소 값을 입력합니다.<br>규칙 예: 'Wifi Mac 주소는 00-14-22-01-23-45입니다'. |
| **iCloud 백업 기능 활성화됨** | **예** 또는 **아니요**로 활성화되는 iCloud 백업 기능 기반 규칙.<br>규칙 예: 'iCloud 백업 기능 활성화는 예와 같음' |
| **iTunes Store 계정 활성화 상태** | **예** 또는 **아니요**로 지정되는 iTunes Store 계정 활성화 상태 기반 규칙.<br>규칙 예: 'iTunes Store 계정 활성화 상태는 아니요와 같지 않음.' |
| **플랫폼 유형** | 모든 애플리케이션 보고서에 적용 가능합니다. |
| **소스** | 모든 애플리케이션 보고서에 적용 가능합니다. |
| **사용자 지정 속성** | 모든 애플리케이션 보고서에 적용 가능합니다. |
| **관리형** | 모든 애플리케이션 및 가장 많이 사용된 애플리케이션 보고서에 적용 가능합니다. |
| **앱 식별자** | 모든 애플리케이션 보고서의 기본값입니다. |
| **MEID** | 비관리형 앱 보고서에 적용됩니다. |

## 보고서 작업 수행

예약된 보고서 페이지에서 다양한 작업을 수행할 수 있습니다.

**절차**

1. **대시보드** > **보고서**로 이동합니다.
2. **내 예약된 보고서** 페이지에서 **작업** 드롭다운 메뉴를 클릭한 후 다음 옵션 중 하나를 선택합니다.

| 작업 옵션 | 수행된 작업 |
|---|---|
| **보기** | 보고서를 확인할 수 있습니다. |
| **편집** | 보고서를 편집할 수 있습니다. |
| **지금 실행** | 보고서를 실행합니다. |
| **CSV 다운로드** | CSV 포맷의 보고서를 다운로드합니다. |
| **PDF 다운로드** | PDF 형식으로 보고서를 다운로드합니다. |
| **삭제** | 보고서를 삭제합니다. |

## 보고서 세부 정보 보기

보고서 세부 정보를 확인하고 생성된 보고서에 대해 일부 작업을 수행할 수 있습니다.

**절차**

1. **대시보드** > **보고서**로 이동합니다.
2. **내 예약된 보고서** 페이지에서 보고서 이름을 클릭하여 보고서 세부 정보를 확인합니다. 보고서 페이지가 열립니다.
3. 다음 옵션 중 하나를 선택합니다.

| 작업 옵션 | 수행된 작업 |
|---|---|
| **토글** | 보고서를 활성화/비활성화할 수 있습니다. |
| **지금 실행** | 보고서를 실행합니다. |
| **보기** | 보고서 상세 정보를 확인할 수 있습니다. 작업 드롭다운 메뉴를 사용하면 다음 작업을 모두 수행할 수 있습니다.<br>• **비활성화**<br>• **최신 CSV/PDF 다운로드**(CSV, PDF, CSV & PDF 등 선택한 보고서 형식에 따라 다운로드 옵션 표시)<br>• **이력**<br>• **삭제** |
| **삭제** | 보고서를 삭제합니다. |

**관련 항목**:

- 사용자에게 사용자 지정 역할을 할당하려면 **역할 할당**을 참조하십시오.
- 기본 역할 목록은 **사용자 역할**을 참조하십시오.
- 역할 관리
- 정기 보고서 사용

# 6. 사용자

사용자를 초대해 모바일 기기를 등록하려면 먼저 해당 사용자 항목을 생성해야 합니다. 또한, MDM용 Ivanti Neurons를 사용하여 기기 관리 또는 콘텐츠 발행을 지원할 담당자(관리자)들의 사용자 계정도 생성해야 합니다.

이 섹션에는 다음 주제가 포함됩니다.


- 사용자 그룹
- 사용자 설정
- 사용자 브랜딩
- Apple Business Manager로 사용자 등록
- 계정 기반 사용자 등록
- 사용자 라이센스
- 사용자 관리

# 6.1. 사용자 추가

이 섹션에는 다음 주제가 포함됩니다.

- 사용자 추가
- 여러 사용자 추가
- 파일을 업로드하여 여러 사용자 추가
- 관리자 추가
- Nobody 사용자
- 기기 등록 PIN 정보 보기

사용자는 한 명씩 등록할 수도 있고 한꺼번에 여러 명을 등록할 수도 있습니다. 여러 명의 사용자를 추가한 경우에는 화면을 필터링하여 원하는 부분만 표시할 수 있습니다.

현재 페이지에 제공되는 기타 사용자 관련 기능:

- 사용자 그룹에 할당/사용자 그룹에서 삭제
- 메시지 보내기
- 등록 초대
- 역할 할당
- 비밀번호 변경
- 삭제
- PIN 생성

모든 기기 소유자 프로필에는 기기 계정이 할당됩니다. 기기 계정이 할당되는 기기 수 제한이 없습니다. 작업 프로필(직원 소유)에는 사용자 계정이 할당됩니다.

## 사용자 추가

**절차**

1. **사용자**를 선택하세요.
2. **+ 추가**(우측 상단)를 클릭합니다.
3. **단일 사용자**를 선택합니다.
4. 사용자 정보를 입력하십시오.
    - 이메일 주소(필수)
    - 이름
    - 성

> 사용자 이름 칸에는 입력한 이메일 주소가 표시됩니다. 해당 값은 기본값으로, 수정하지 않는 것이 좋습니다. 자세한 내용은 사용자 이름 수정이 필요한 경우를 참조하십시오.

    - 표시 이름

> 현재 사용자의 화면 표시 이름을 변경하려면 **표시 이름** 칸의 기본값을 수정하시기 바랍니다.

5. 비밀번호를 설정하려면 **비밀번호** 및 **비밀번호 확인** 필드에 비밀번호를 입력해 주십시오.
    - 설정한 비밀번호는 기기를 등록할해당 사용자에게 알려야 합니다.
    - 비밀번호를 설정하지 않을 경우, 사용자가 기기 등록 중 직접 비밀번호를 생성해야 합니다.
6. 드롭다운 목록에서 **로캘**을 선택합니다.
7. **관리되는 Apple ID**를 입력합니다. 관리되는 Apple ID에 대해 서브도메인으로 "appleid"를 포함하여 기존 Apple ID와의 충돌을 방지할 수 있습니다. 예를 들어 user@appleid.yourdomain.com 등을 사용할 수 있습니다. 서브도메인은 Apple Business Manager에서 유효한 확인된 서브도메인이어야 합니다.

> 현재 계정의 관리되는 Apple ID에 활성 사용자 등록 기기가 있으면 다른 관리되는 Apple ID로 계정을 업데이트할 수 없습니다.

(선택 사항) 하나 이상의 사용자 그룹을 할당합니다. 관리되는 Apple ID는 "활성" 및 "폐기 보류 중" 상태인 기기가 있으면 업데이트할 수 없습니다.

10. 사용자를 초대하기에 앞서 우선 다른 기능을 설정하려면 **지금 초대 보내기** 옵션의 선택을 해제하세요. 이 옵션의 선택을 해제하지 않을 경우 **완료**를 클릭하면 바로 초대 이메일이 전송됩니다.
11. **완료**를 클릭하면 해당 사용자가 등록됩니다.

Android 기기의 경우 기기 계정은 기기를 등록하는 데 단일 로컬 서비스 계정을 사용할 수 있는 일회용 관리 기기를 위해 설계되었습니다. 새 사용자를 생성하는 동안 **관리자 > Google > Android Enterprise**에서 사용할 수 있는 Android 엔터프라이즈 장치 계정을 활성화해야 합니다. 장치 소유자 관리형 Google Play 계정 등록에 대해 장치 계정이 기본적으로 (사용자 계정 대신) 활성화됩니다.

이 계정에 연결된 Android Enterprise 작업 관리형 장치 등록이 Google 장치 계정에 자동으로 할당되도록 하려면 **Android Enterprise 장치 계정** 확인란을 선택합니다.

Android 장치에 대한 로컬 또는 LDAP 사용자를 편집하는 동안 다음 조건이 충족되는 경우 사용자와 연결된 Android Enterprise 장치 소유자 관리형 Google Play 계정 장치에 장치 계정이 할당됩니다.

- **Android 엔터프라이즈 기기 계정** 체크박스를 선택하면 해당 기능이 활성화됩니다.
- Android 기기의 Go 앱 버전은 47 이상입니다.

## 여러 사용자 추가

**절차** :

1. **사용자**로 이동합니다.
2. **+ 추가**(우측 상단)를 클릭합니다.
3. **여러 사용자**를 선택합니다.
4. 기본적으로 이메일 주소를 **수동으로** 입력할 수 있습니다. 원하는 사용자들의 이메일 주소를 각각 쉼표로 구분해 입력하거나 붙여넣으세요.
5. 예: jdoe@mycompany.com, jsmith@mycompany.com, tjones@mycompany.com
   사용자를 초대하기에 앞서 우선 다른 기능을 설정하려면 **지금 초대 보내기** 옵션의 선택을 해제하세요.
6. 이 옵션의 선택을 해제하지 않을 경우 **완료**를 클릭하면 바로 초대 이메일이 전송됩니다.
   **완료**를 클릭하면 사용자가 등록됩니다.

## 파일을 업로드하여 여러 사용자 추가

**절차**:

1. **사용자**를 선택하세요.
2. **+ 추가**(우측 상단)를 클릭합니다.
3. **여러 사용자**를 선택합니다.
4. **CSV 업로드**를 선택합니다.
5. **CSV 템플릿 다운로드**를 클릭합니다.
6. 각 사용자에 대한 다음 정보로 템플릿을 편집하세요.
    - 사용자 ID(필수)
    - 이메일 주소(필수)
    - 비밀번호
    - 이 름
    - 가족 성
    - 표시 이름
    - 사용자 그룹
    - 커스텀 속성
7. 이것은 단일 사용자 추가하기 시에 입력한 정보와 동일합니다. 파일 안의 항목이 10,000개를 넘어서는 안 됩니다.
   파일을 저장합니다.
8. 업로드 영역으로 드래그하거나 **CSV 업로드**를 선택하여 파일을 선택하세요.
9. 업로드한 사용자 정보가 표시되면 필요한 대로 편집하세요.
10. **다음**(우측 하단)을 클릭합니다.
11. 지금 바로 초대를 보내고 싶지 않다면 **초대장 발송 안 함**을 선택합니다.
12. **완료**를 클릭하세요.

## 관리자 추가

**절차** :

1. **추가**(우측 상단)를 클릭하세요.
2. **단일 사용자**를 선택합니다.
3. 사용자 정보를 입력하십시오.
    - 이메일 주소
    - 이름
    - 성
4. **사용자 이름** 필드에는 입력한 이메일 주소가 표시됩니다.
   현재 사용자의 화면 표시 이름을 변경하려면 **표시 이름** 칸의 기본값을 수정하시기 바랍니다.
5. **비밀번호** 필드에 비밀번호를 할당합니다.
6. **비밀번호 확인** 필드에 비밀번호를 다시 입력합니다.
7. **완료**를 클릭하면 해당 사용자가 등록됩니다.
8. 설정한 비밀번호를 해당 기기 관리자에게 전달하시기 바랍니다.

## Nobody 사용자

Nobody 사용자는 기본 사용자로 삭제가 불가능합니다. 이 사용자에게는 폐기된 기기처럼 연동 사용자가 없는 기기가 자동 할당됩니다.

## 기기 등록 PIN 정보 보기

새 사용자를 추가하는 동안 생성된 등록 PIN 정보가 관리자에게 표시됩니다(기기 등록 인증 유형이 PIN만으로 설정된 경우). 이 정보는 사용자의 장치 등록을 지원할 때 유용할 수 있습니다.

- 단일 사용자의 경우 **사용자 > 등록을 위해 사용자 초대** 작업이나 사용자 상세 정보 페이지의 PIN 정보 섹션에서 PIN을 확인할 수 있습니다.
- 여러 사용자의 경우 PIN은 사용자 목록 페이지의 열로 표시되며 PIN 상태(유효함 또는 만료됨), PIN 발급됨, 및 PIN 만료 열에도 표시됩니다.

**사용자** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 사용자 관리

# 6.2. 사용자 그룹

이 섹션에는 다음 주제가 포함됩니다.

- 동적으로 관리되는 사용자 그룹 생성
- 수동으로 관리되는 사용자 그룹 생성
- 중복 사용자 그룹 중 하나에서 사용자 그룹 생성하기
- CSV 파일 업로드로 사용자 그룹 생성

사용자 그룹을 생성하면 다수의 사용자에게 앱과 역할을 할당할 수 있습니다. 예를 들어 모든 부서 관리자를 앱과 콘텐츠의 관리자로 지정하고자 하는 경우 관리자 그룹을 생성할 수 있습니다.

다음 방법 중 하나로 관리할 사용자 그룹을 생성할 수 있습니다.

- **동적으로 관리됨(가장 일반적):** 특정 규칙 및/또는 속성에 기반하여 동적으로 로컬 및 LDAP 사용자를 그룹에 추가/제거합니다.
- **수동으로 관리됨(제한된 목적):** 그룹에/에서 사용자를 수동으로 추가/제거합니다. 수동으로 관리되는 그룹은 권한이 덜 필요한 테스트 목적으로만 권장합니다.

**검색** 필드에 텍스트를 입력하여 이름이 입력된 텍스트로 시작하는 모든 사용자 그룹의 목록을 표시할 수 있습니다.

- 텍스트를 입력함과 동시에 검색 결과가 일치 가능한 항목 목록으로 표시됩니다.
- 다음 작업을 위해 일치 가능한 항목 목록에서 원하는 사용자 그룹 이름을 선택합니다.
- 검색 일치 항목은 대/소문자를 구분하지 않습니다.

## 동적으로 관리되는 사용자 그룹 생성

> 다음 절차는 동적 사용자 그룹에는 적용되지 않습니다.

**절차**

1. **+추가**를 클릭합니다.
2. **이름** 필드에 사용자 그룹 이름을 입력합니다.
3. (선택 사항) **설명 추가**를 클릭하여 사용자 그룹에 대한 설명을 추가합니다.
4. **동적으로 관리됨(가장 일반적)** 옵션을 클릭합니다.
5. 요구 사항에 따라 규칙 및/또는 속성을 설정합니다. 사용 가능한 규칙 옵션은 다음과 같습니다.
    - 사용자 지정 LDAP 속성
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname

    기본 LDAP 속성

        - samAccountName
        - userPrincipalName

    기본 사용자 속성

        - email_address
        - distinguished_name
        - last_name
        - display_name
        - first_name
        - 사용자 그룹
        - 사용자 지정 사용자 속성

    사용자 그룹 DN

        - 사용자 그룹 GUID
        - 사용자 그룹 이름

6. 각 규칙에 대해 로컬 및 LDAP 사용자를 선택합니다. 사용자는 **사용자 그룹** 필터 기준을 사용하여 하위 그룹을 포함하거나 제외할 수 있습니다.
7. + 아이콘을 클릭하여 더 많은 규칙을 추가합니다.
   추가된 규칙에 **일부** 또는 **모두** 조건부 필터를 설정할 수 있습니다.
8. + 아이콘 옆에 있는 계층 아이콘을 클릭하여 규칙 그룹을 생성합니다.
9. 규칙 선택 옵션 아래에 표시된 텍스트 쿼리에서 사용자 그룹의 규칙 및 속성을 검토합니다.
10. **결과** 섹션에서 구성된 기준과 일치하는 사용자 상세 정보를 검토합니다. 규칙 또는 속성을 추가하거나 수정하면 일치하는 사용자가 표시되는 것을 확인할 수 있습니다(존재하는 경우).
11. **저장**을 클릭하여 구성된 사용자 그룹을 저장합니다.

## 수동으로 관리되는 사용자 그룹 생성

1. **+추가**를 클릭합니다.
2. 그룹 이름을 입력합니다.
3. (선택 사항) **설명 추가**를 클릭하여 설명을 추가합니다.
4. **수동으로 관리됨(제한된 목적)** 옵션을 선택합니다.
5. **사용자 검색** 필드에 그룹에 포함할 각 사용자의 이메일 주소를 입력합니다.
   입력하면 일치하는 사용자를 찾아 표시합니다(존재하는 경우).
6. 그룹에 추가하고자 하는 사용자를 선택합니다. 필요한 경우 더 많은 사용자를 검색 및 추가할 수 있습니다.
7. **저장**을 클릭하세요.

> 수동으로 관리되는 사용자 그룹을 생성한 후 해당 그룹을 동적으로 관리되는 사용자 그룹에 추가할 수 있습니다. 이러한 시나리오에서는 수동으로 관리되는 사용자 그룹을 편집해도 동적으로 관리되는 사용자 그룹 규칙은 위반되지 않습니다. 수동으로 관리되는 사용자 그룹이 동적으로 관리되는 사용자 그룹에 추가된 경우 해당 그룹을 삭제할 수 없습니다.

## 중복 사용자 그룹 중 하나에서 사용자 그룹 생성하기

MDM용 Neurons 127부터 관리자 포털은 규칙 작성기에서 사용자 그룹 이름 속성을 선택할 때 중복 그룹을 식별할 수 있도록 중복 사용자 그룹 수 및 해당 GUID 수를 표시합니다.또한 이 규칙 아래에 있는 표에는 중복 사용자 그룹 목록과 사용자 그룹 이름, GUID, 소스, 배포된 이름(DN)과 같은 세부 정보가 표시됩니다.

**절차**

1. MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **사용자**, **사용자 그룹**으로 이동합니다.
3. **+추가**를 클릭합니다. 사용자 그룹 만들기 마법사가 열립니다.
    1. **이름** 필드에서 이름을 지정합니다.
    2. 규칙 작성기에서 **사용자 그룹 이름**을 선택하고 **같음**을 선택한 다음, 중복 그룹 이름 중 *하나*를 선택합니다.
    3. 규칙을 더 추가하려면 **+**(플러스) 아이콘을 클릭합니다.
    4. **사용자 그룹 GUID**, **같음**을 선택합니다.
    5. 중복 사용자 이름 및 GUID 목록이 표시된 표에서 GUID를 복사하여 붙여 넣습니다. 새 그룹에 추가될 연결된 사용자가 결과에 표시됩니다.
    6. **저장**을 클릭합니다. 열거된 사용자가 이제 새로 생성한 사용자 그룹에 추가됩니다.

**사용자 그룹** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 사용자 관리

## CSV 파일 업로드로 사용자 그룹 생성

새로 추가된 기능을 통해 관리자는 사용자 그룹을 생성하고, 생성된 그룹에 CSV 파일을 이용하여 사용자를 추가할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **사용자**, **사용자 그룹**으로 이동합니다.
3. **+추가**를 클릭합니다.
4. **CSV에서 사용자 그룹 가져오기**를 선택합니다. 사용자 그룹 가져오기 마법사가 열립니다.
    1. CSV 다운로드 섹션에서 **CSV 템플릿 다운로드**를 클릭하여 CSV 템플릿을 다운로드합니다. 템플릿을 사용하면 파일을 편집하여 사용자 그룹을 생성하고 사용자를 신규/기존 사용자 그룹에 추가할 수 있습니다.
    2. CSV 파일을 편집하고 저장한 후 **파일 선택**을 클릭하여 CSV 파일을 업로드합니다.
    3. **업로드**를 클릭합니다. 업로드가 성공적이라는 확인 메시지가 표시됩니다.

| 속성 | 설명 |
| --- | --- |
| **CSV 파일 크기 제한** | 가져올 수 있는 CSV 파일의 최대 크기는 2MB로 제한됩니다. |
| **CSV 파일 형식 요구 사항** | CSV 파일에는 accountUid 및 groupName이라는 정확히 2개의 열이 포함되어야 합니다.<br>• accountUid 및 groupName 값은 모두 필수입니다.<br>• 이러한 기준을 충족하지 못하는 기록은 가져오는 동안 폐기됩니다.<br>관리자는 참조용으로 가져오기 섹션에서 샘플 CSV 파일을 다운로드할 수 있습니다. |
| **가져오기 중 오류 처리** | CSV 가져오기 중에 오류가 발생하거나 실패하면 오류 파일이 생성됩니다.<br>• 관리자는 이 오류 파일을 다운로드하여 실패한 CSV 행을 검토하고 실패 원인을 파악할 수 있습니다.<br>• 오류 파일에는 실패한 특정 CSV 행이 포함되어 있으며 실패에 대한 설명이 제공됩니다. |
| **가져오기 성공 조건** | 사용자 그룹이 로컬이고 수동으로 관리되는 경우에만 사용자를 사용자 그룹으로 가져오는 데 성공합니다.<br>• 가져오기가 성공하려면 시스템에 사용자가 있어야 합니다. |

## 샘플 CSV 파일을 사용하여 사용자 그룹 생성 및 사용자 추가 조건

샘플 CSV 파일 세부 정보 -

**accountUid**: test_user_1@org.com

**groupName**: test_group_1

| 조건 | 설명 |
| --- | --- |
| **존재 그룹** | test_group_1 그룹이 이미 존재하는 경우 test_user_1@org.com 사용자가 그룹에 연결됩니다. |
| **존재하지 않는 그룹** | test_group_1 그룹이 없으면 test_group_1이라는 이름의 새 그룹이 생성되고 test_user_1@org.com 사용자가 이 그룹에 연결됩니다. |
| **비로컬 그룹** | test_group_1 그룹이 존재하지만 로컬 그룹이 아닌 경우 이 레코드는 '로컬 그룹이 아님'이라는 이유와 함께 오류 CSV 파일에 포함됩니다. |
| **수동으로 관리되지 않는 그룹** | test_group_1 그룹이 존재하지만 수동으로 관리되는 그룹이 아닌 경우 '그룹이 수동으로 관리되지 않음'이라는 이유와 함께 이 레코드가 오류 CSV 파일에 포함됩니다. |
| **존재하지 않는 사용자** | test_user_1@org.com 사용자가 존재하지 않는 경우 이 레코드는 '사용자를 찾을 수 없음'이라는 이유와 함께 오류 CSV 파일에 포함됩니다. |
| **존재하지 않는 사용자 및 그룹** | test_user_1@org.com 사용자와 test_group_1 그룹이 모두 존재하지 않는 경우 test_group_1이라는 이름의 새 그룹이 생성되고 이 레코드는 '사용자를 찾을 수 없음'이라는 이유와 함께 오류 CSV 파일에 포함됩니다. |

# 6.3. 사용자 설정

이 섹션에는 다음 주제가 포함됩니다.


- 기본 설정 수정
- 사용자 지정 설정 추가
- 사용자 지정 설정 삭제
- 새 기기 등록 설정 구성하기
- 사용자당 기기 제한 구성
- 기기 지우기 제한 구성
- 사용자 설정
- 셀프 서비스 포털 인증 구성
- 비밀번호 복잡도 설정
- 서비스 약관 정의
- 사용자 초대 알림 이메일 구성
- 사용자 등록 확인 이메일 구성하기
- 사용자 작업 일정 설정 구성
- 관리 포털 인증 설정 구성


사용자 설정을 통해 장치 등록 옵션을 설정할 수 있습니다. 다음 몇 가지 유형이 제공됩니다.

- **기기 등록 설정**: 비밀번호, PIN 또는 둘 다로 인증을 설정합니다. Apple 등록 유형 및 기기 소유권.
    - 이전에는 SAML 인증/IdP를 설정할 경우 기기 등록 및 포털 인증에 모두 SAML 인증이 사용되었습니다.
    - **플랫폼 기기 등록 설정** - 이제 관리자는 특정 Apple, Android 및 Windows 플랫폼이 시스템에 등록되지 않도록 제한하여 운영 체제 수준에서 기기 등록을 제어할 수 있습니다. 이 새로운 OS 수준 제한 설정은 상위 등록 제어 기능으로 적용되며, 특정 플랫폼에 대해 활성화하면 해당 플랫폼과 관련된 등록 제한이 자동으로 비활성화됩니다. 이를 통해 조직은 등록 정책을 적용하고 지원되지 않는 기기 플랫폼이 등록되는 것을 방지할 수 있습니다.

기기 제한 설정: 사용자가 등록할 수 있는 기기의 수를 설정할 수 있습니다.

- **지우기 제한 설정**: 한 번에 지울 수 있는 최대 기기 수에 대한 제한을 설정합니다.
- **셀프 서비스 포털 인증 설정:** 셀프 서비스 포털에 대한 비밀번호 인증 유형을 설정합니다.
- **비밀번호 복잡도 설정**: 기기 등록에 사용된 로컬 계정에 대해 비밀번호 복잡도 및 정책 매개 변수를 설정한 후 관리 포털 및 자체 서비스 포털에 액세스하십시오.
- **서비스 이용약관 설정**: 기기를 등록할 때 사용자에게 표시되는 서비스 이용약관을 설정할 수 있습니다.
- **사용자 초대 알림 설정**: 사용자 초대 이메일을 보낼 날짜와 빈도를 설정합니다.
- **사용자 등록 확인 설정:** 사용자 등록 확인 이메일을 전송할 수 있는 기능을 제어합니다. 솔루션 개요는 등록 확인 이메일 구성 및 사용을, 특정 사용자 설정 지침은 아래의 사용자 등록 확인 이메일 구성하기을 참조하십시오.
- **사용자 작업 일정 설정:** 정해진 근무 시간 외에 Sentry에서 관리되는 기기로의 모든 통신을 차단하는 사용자 작업 일정을 구성할 수 있는 기능을 제어합니다. 연결을 해제할 권리 법률이 있는 로캘에 유용합니다.
- **관리 포털 인증 설정:** MDM용 Ivanti Neurons가 관리자에게 비밀번호만 요구하도록 할 것인지, 비밀번호와 PIN을 요구하도록 할 것인지를 제어합니다.

**전체 사용자** 그룹의 기본 설정을 편집할 수 있으며, 사용자 지정 설정을 추가한 후 해당 설정을 다른 사용자 그룹에 할당할 수도 있습니다.

## 기본 설정 수정

잠금 아이콘이 있는 설정의 **편집** 링크를 클릭합니다. 기본 설정은 삭제할 수 없습니다.

## 사용자 지정 설정 추가

**특정 사용자 그룹의 설정 추가** 링크를 클릭합니다.

## 사용자 지정 설정 삭제

X 아이콘을 클릭합니다.

## 새 기기 등록 설정 구성하기

새 장치 등록 시 최소 OS 버전, 인증 유형 및 장치 소유권을 구성할 수 있습니다. MDM용 Ivanti Neurons 이전 버전에서 생성된 기기 등록 URL은 현재 버전과의 작동을 중단합니다. 관리자는 기기 등록을 위해 기기 등록 URL을 다시 생성해야 합니다.

#### 기기 허용 목록 등록

기기 등록 허용 목록 옵션은 기본 사용자 설정에서만 이용 가능하며, 사용자 지정 사용자 설정에서는 이용할 수 없습니다. 몇몇 기기를 허용 목록으로 지정하는 데 사용되는 일련 번호 및 사용자 지정 기기 속성이 포함된 템플릿을 사용하여 CSV 파일을 업로드할 수 있습니다. 하나 이상의 기존 사용자 지정 기기 속성을 포함하여 허용 목록을 생성할 수 있습니다. 이를 통해 등록 후 속성을 기기 그룹 또는 공간에 할당할 수 있게 됩니다.

사용자 지정 속성을 생성하려면 **관리 > 속성**으로 이동합니다. 허용 목록 기능이 활성화되어 있고 CSV 파일에 기기 일련 번호가 언급되어 있지 않을 경우 iOS 및 macOS 기기는 iReg를 통해 등록할 수 없습니다. CSV 파일에 중복 일련 번호가 포함되어 있을 경우, CSV 파일의 마지막 항목이 고려되며 등록 중 기기 할당에 대해 해당 항목과 연관된 사용자 지정 기기 속성이 고려됩니다.

**기기 허용 목록** 옵션을 활성화하면 허용 목록에서 지정된 기기만 MDM용 Ivanti Neurons에 등록할 수 있습니다. 이 기능은 웹 기반 등록 프로세스를 통해 등록하는 기기에만 적용됩니다. MDM용 Ivanti Neurons에 이미 등록된 기기에는 영향을 미치지 않습니다. 등록 후, 기기 일련 번호가 CSV 파일에서 제거된 경우 기기가 폐기되지 않습니다. CSV 파일에서 언급된 사용자는 선택 사항이며 사용자가 CSV 파일에 언급되어 있고 유효한 사용자일 경우에만 할당됩니다.

새 CSV 파일을 업로드하고자 할 경우 기존 CSV 파일을 삭제하고 새 파일을 업로드할 수 있습니다. 허용 목록 지정은 iReg에서만 지원되며, Go 클라이언트가 필요할 경우 제로 터치 등록을 선택하십시오. AppConnect 및 Threat Defense와 같은 기능이 작동하려면 Go 클라이언트가 시스템에 설치되어 있어야 합니다. 인앱 등록을 지원하지 않기 때문에 사용자는 먼저 iReg를 통해 기기를 등록할 수 있으며 그 후 Go 앱이 App Catalog에서 기기로 푸시될 수 있습니다. 사용자가 앱 설치를 수락하면 기기는 관리형 기기가 되며 모든 기능은 등록 후에 계속 작동합니다. AppConnect 상태가 활성 또는 비활성인 기기에서는 제로 터치(Zero-touch) 구성을 사용할 수 없습니다. 제로 터치 구성은 AppConnect 상태가 없음일 때만 사용할 수 있습니다. iReg를 통해 등록한 후 기기에서 Go 클라이언트가 실행될 때까지 AppConnect 상태는 없음으로 유지됩니다.

#### 절차

1. MDM용 Ivanti Neurons에 로그인합니다.
2. **사용자** > **사용자 설정**으로 이동합니다.
3. **기기 등록 설정**에서 **+특정 사용자 그룹에 대한 설정 추가**를 클릭합니다.
4. 기본값 **기기 등록 인증 유형** 설정을 편집하거나 새 설정을 추가합니다.
5. **이름** 필드에 이름을 입력합니다.

6. (선택 사항) 설정에 대한 설명을 입력합니다.
7. **OS 설정** 섹션에서 iOS, macOS 또는 Windows의 최소 OS 버전을 정의합니다.
8. **최소 버전 활성화** 토글 버튼을 선택하고 드롭다운 목록에서 OS 버전을 선택합니다.

> 최소 버전 활성화 설정은 DEP 기기 등록에 적용할 수 없습니다.

**Android**의 경우:

- **최소 보안 패치** 옵션(Android 전용)을 활성화하고 다음 드롭다운 목록 옵션에서 기간 유형을 선택하여 기간을 지정합니다.
  - **일**
  - **월**
  - **년**

  **제조업체 허용 목록/차단 목록**을 활성화하고 다음 옵션 중에서 선택합니다.
  - **허용 목록 생성** - 이 제조업체의 기기만 등록할 수 있습니다.
  - **차단 목록 생성** - 이 제조업체의 기기가 등록되지 않도록 합니다.
    제조업체 추가 방법:
    1. **제조업체 추가**를 클릭합니다.
    2. **제조업체 이름** 필드에 제조업체 이름을 입력합니다.
    3. **저장**을 클릭합니다. 추가된 제조업체 이름이 표에 표시됩니다.

    > 제조업체 이름은 대소문자를 구분합니다. 추가된 제조업체 이름을 편집하거나 삭제하려면 제조업체의 **편집** 또는 **삭제** 옵션을 클릭합니다.

Apple 등록 섹션에서 Apple 등록 유형을 선택합니다.

- **기기 등록**
- **사용자 등록** - 기본적으로 사용자 등록은 iOS 및 iPadOS 기기에 적용됩니다.
- (선택 사항) **macOS 기기 포함(macOS 10.15+)** - macOS 기기에도 사용자 등록이 적용되도록 하려면 이 옵션을 선택합니다.

**등록 초대 방법(iOS 및 Android만 해당)** 섹션에서 **MAM만 등록**을 활성화합니다.

> 이 옵션은 MAM-Only 기기 등록에 대해 활성화되어야 하며 활성화되면 AppStation 클라이언트 앱을 다운로드하기 위해 사용자가 공개 App Store로 리디렉션됩니다.

11. **기기 등록 인증 유형** 섹션의 **등록 유형 선택** 드롭다운에서 다음 등록 유형 옵션 중 하나를 선택합니다. 기기 등록을 사용하는 경우 기기 등록 구성이 선택과 일치하는지 확인합니다.
    - **비밀번호만**
    - **PIN 전용** 이 옵션을 선택하면 IdP 기기 등록 인증 우회 토글 버튼이 잠깁니다.
    - **비밀번호 및 PIN**

      > 사용자는 계정 활성화를 완료하기 위해 여전히 PIN 입력을 요청받을 수도 있습니다.

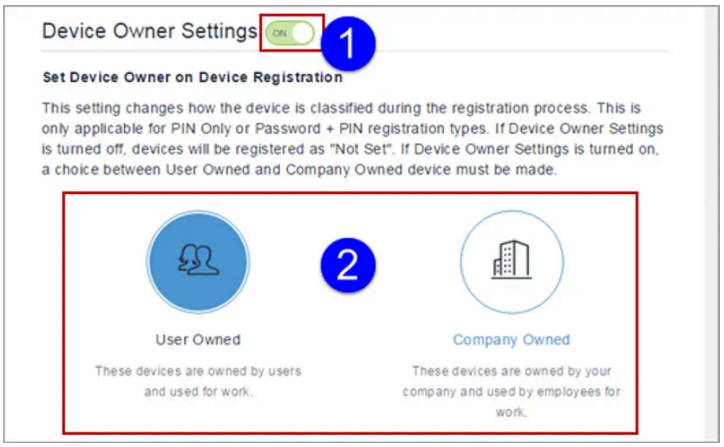
> 이 설정은 일반 등록 및 기기 등록 등록에 모두 영향을 미칩니다.

PIN의 경우 다음을 지정합니다. 기기 등록 중 필요한 경우 사용자가 **PIN 재전송**을 클릭할 수 있습니다.

- **PIN 수명:** PIN 유효 기간(1~30일).
- **PIN 길이:** 문자 수(4~12).
- **사용자가 새로운 PIN을 생성하도록 허용**: (잊어버렸거나 만료된 경우)

아니면, **기기 소유자 설정**을 켠 다음 **사용자 소유** 또는 **회사 소유**를 클릭해도 됩니다. 이 설정은 등록 과정 중 기기의 분류 방식을 변경합니다.

- **기기 소유자 설정**이 켜져 있는 상태에서 관리자가 기기를 사용자 소유로 표시한 경우에는 사용자에게 기기 등록 과정과 셀프 서비스 포털에서도 기기를 사용자 소유 또는 회사 소유로 표시하는 옵션이 나타납니다. 사용자 등록 등록된 기기의 경우 관리자의 선택과 관계 없이 기본 기기 소유자 설정은 "사용자 소유"가 됩니다.
- 감독 기기는 기기 소유자 설정이 "회사 소유"가 됩니다.




설정을 배포할 하나 이상의 사용자 그룹에 대해 **+추가**를 클릭합니다.

15. 필요 시 **기기 허용 목록** 옵션을 켜고 허용 목록의 일련 번호를 기반으로 기기 등록을 허용합니다(iOS 및 macOS 기기만 해당하는 주문형 기능).
16. **다음**을 클릭합니다. 사용자 설정 배포 페이지가 열립니다.
17. 사용자 그룹 배포를 선택합니다.
18. **완료**를 클릭하세요.
19. 사용자에게 초대장을 발송합니다. 자세한 내용은 사용자 초대하기를 참조하십시오.

참고:

> 사용자 기기가 PIN 전용 옵션을 사용하여 등록된 경우 사용자는 인증을 위한 PIN이 포함된 등록 확인 이메일을 받게 됩니다.

- 사용자 이메일 ID로 PIN이 전송됩니다.
- 사용자가 PIN을 기기 등록 페이지에 입력합니다.
- PIN이 정확하면 사용자는 등록 프로세스를 완료하도록 안내됩니다.

SAML-기반 ID 제공자(IdP)를 사용하여 구성한 사용자의 경우 MDM용 Ivanti Neurons은(는) 기기 등록 시 PIN 기반 인증을 지원합니다. 기기 등록 인증 유형은 PIN 또는 PIN 및 비밀번호여야 합니다. PIN 및 비밀번호 기능은 추가 보안을 위해 이중 인증 역할을 합니다. 이 경우 해당하는 사용자가 기기를 등록하려고 하면:

- 사용자 이메일 ID로 PIN이 전송됩니다.
- 사용자가 PIN을 기기 등록 페이지에 입력합니다.
- PIN이 올바를 경우 사용자가 IdP 사용자 이름 및 비밀번호를 입력하는 IdP 로그인 페이지로 리디렉션됩니다.
- IdP 자격 증명이 올바를 경우 등록 프로세스를 완료할 수 있도록 사용자가 기기로 리디렉션됩니다.

## 사용자당 기기 제한 구성

**절차**

1. 기본값 **기기 제한** 설정을 편집하거나 새로 추가하십시오.
2. (선택 사항) **+ 특정 사용자 그룹에 대한 설정 추가**를 클릭하여 특정 사용자 그룹에 대한 장치 제한을 설정합니다.
3. 해당 설정의 이름을 수정 또는 설정하세요.
4. 해당 설정에 대한 간략한 설명(선택사항)을 입력하세요.
5. **활성 장치의 최대 수**의 드롭다운 메뉴에서 활성 Apple 장치 제한을 선택합니다.
6. **iPhone과 페어링할 수 있는 Apple watchOS 장치의 최대 수**의 드롭다운 메뉴에서 iPhone과 페어링할 수 있는 활성 Apple watchOS 장치 제한을 선택합니다.
7. (선택 사항) **+ 특정 사용자 그룹에 대한 설정 추가**를 선택한 경우 **다음**을 클릭하고 이 설정을 배포할 사용자 그룹을 최소한 하나 이상 선택합니다.
8. **완료**를 클릭하세요.

## 기기 지우기 제한 구성

**절차**

1. 기본 **기기 지우기 제한** 설정을 편집합니다.
2. **모든 사용자에게 지우기 제한 활성화(기본 역할 포함)** 옵션을 켭니다.
3. **사용자가 한 번에 삭제할 수 있는 최대 기기 수** 필드에서 한 번에 삭제할 수 있는 최대 기기 수를 입력합니다. 기본 값은 1입니다. 기기 지우기 제한 값은 최대 200까지 설정할 수 있습니다.
4. **완료**를 클릭하세요.

## 셀프 서비스 포털 인증 구성

**절차**

1. 기본 **셀프 서비스 포털 인증** 설정을 편집하거나 **+ 특정 사용자 그룹을 위한 설정 추가**를 클릭하여 새 설정을 추가합니다.
2. 해당 설정의 이름을 수정 또는 설정하세요.
3. 해당 설정에 대한 간략한 설명(선택사항)을 입력하세요.
4. 드롭다운에서 **셀프 서비스 포털 인증 유형**을 선택합니다. 유형은 다음 옵션 중 하나가 될 수 있습니다.
    - 비밀번호
    - 인증서
5. **다음**을 클릭하세요.
6. 해당 구성을 배포할 하나 이상의 사용자 가룹을 선택합니다.
7. **완료**를 클릭하세요.

# 비밀번호 복잡도 설정

기기 등록에 사용된 로컬 계정에 대해 비밀번호 복잡도 및 정책 매개 변수를 설정한 후 관리 포털 및 자체 서비스 포털에 액세스할 수 있습니다.

> 아래의 비밀번호 길이, 특징 및 정책은 비밀번호 보안 수준을 결정합니다.

또한 유효한 비밀번호를 선택하는 사용자와 관련된 난이도를 정의합니다. 최종 사용자에 대해 로컬 계정을 사용하고 보안 비밀번호로 관리 포털에 액세스하도록 하려면 기기 등록 시 PIN을 사용하여 비밀번호 복잡도가 기기 등록을 방해하지 않도록 하는 것이 좋습니다. **사용자 설정 > 기기 등록 설정**에서 "기기 등록 인증" 유형 설정을 사용하여 기기 등록을 위한 인증 모드를 선택합니다.

**절차**

1. 기본 **비밀번호 복잡도** 설정을 편집합니다.
2. 다음 비밀번호 복잡도 설정을 정의합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| 최소 비밀번호 길이 | 슬라이더를 움직여 비밀번호의 최소 길이를 지정하여 사용자가 짧고 안전하지 않은 비밀번호를 생성하지 못하도록 설정합니다.<br>숫자의 범위는 8부터 32입니다. |
| 필수 특징 | 사용자가 비밀번호를 선택할 때 충족해야 하는 비밀번호 문자 수를 지정합니다. 충족해야 하는 최소 문자 수는 3입니다(정부 고객의 경우 4). |
| 필수 특수 문자(기호) | 비밀번호가 포함해야 하는 영숫자가 아닌 문자 수를 지정합니다. |
| 필수 대문자 수 | 비밀번호가 포함해야 하는 알파벳 대문자 수를 지정합니다. |
| 필수 소문자 문자 수 | 비밀번호가 포함해야 하는 알파벳 소문자 수를 지정합니다. |
| 필수 숫자 수 | 비밀번호가 포함해야 하는 숫자 수를 지정합니다. |
| **비밀번호 검사** | |
| 허용되는 숫자 시퀀스 | 시퀀스로 반복되는 숫자 수를 선택합니다.<br>예: 123 |
| 허용되는 반복 문자 | 시퀀스로 반복되는 알파벳 문자 수를 선택합니다.<br>예: bbc |

3. 다음 비밀번호 정책 설정을 설정하여 행동을 사용자 지정합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| 유지된 비밀번호 기록 | 슬라이더를 움직여 이전 비밀번호를 사용하기 전 사용자 계정과 관련이 있어야 하는 새 비밀번호 수를 선택합니다.<br>숫자의 범위는 3부터 36입니다. |
| 비밀번호 만료 기간 | 슬라이더를 움직여 비밀번호 만료 기간을 일 단위로 선택합니다.<br>숫자의 범위는 30부터 365일입니다. |
| 비활성 시간제한 | 슬라이더를 움직여 관리자 포털 또는 셀프 서비스 포털 세션 시간 전에 사용자가 비활성 상태를 유지할 수 있는 시간을 지정합니다.<br>숫자 범위는 5~60(분)입니다. |
| 로그인 실패 임계값 | 슬라이더를 움직여 5분간 계정이 잠기는 것이 시행되기 전 로그인 실패 시도 횟수를 선택합니다.<br>숫자의 범위는 2부터 5입니다.<br>실패 시도 횟수가 임계값 제한 내에 있으면 잠금 화면에서 나중에 로그인을 시도하라는 메시지가 사용자에게 표시됩니다.<br>실패 시도 횟수가 임계값 제한을 초과하면 잠금 화면에서 지정된 시간(분) 이후 로그인을 시도하라는 메시지가 사용자에게 표시됩니다. |

4. **완료**를 클릭합니다. 비밀번호 복잡도 기본 설정을 변경했을 경우 기존 로컬 계정의 예전 비밀번호는 변경되지 않습니다. 만료 시 비밀번호를 재설정하라는 메시지가 사용자에게 표시됩니다. 관리자 포털에 로그인하려는 관리자의 경우 헬프 데스크에 문의하여 비밀번호 재설정 안내를 받을 수 있습니다.

> 기기 등록 시에는 PIN만 등록 모드를 사용하는 것이 좋습니다.

## 서비스 약관 정의

**절차**

1. 새 **서비스 이용약관** 설정을 생성합니다.
2. 설정을 식별할 수 있는 이름을 설정하세요.
3. 해당 설정에 대한 간략한 설명(선택사항)을 입력하세요.
4. **사용자에게 확인**을 선택합니다. 옵션을 클릭합니다.
5. 화면에 표시할 소유자과 내용을 입력하세요.
6. 설정을 배포할 하나 이상의 사용자 그룹에 대해 **+추가**를 클릭합니다.
7. **저장**을 클릭하세요.

> 확정된 서비스 이용약관은 삭제할 수 없습니다. 그러나 **사용자에게 확인**을 삭제하면 새 등록의 메시지를 끌 수 있습니다. 옵션을 클릭합니다.

## 사용자 초대 알림 이메일 구성

관리자는 이 설정을 사용하여 사용자 초대 알림 이메일을 보냄으로써 기기 등록을 독려할 수 있습니다.

**절차**

1. 기존 **사용자 초대 알림 설정**을 편집하거나 새로 추가하십시오.

2. 해당 설정의 이름을 수정 또는 설정하세요.
3. 해당 설정에 대한 간략한 설명(선택사항)을 입력하세요.
4. **사용자 초대 알림** 옵션이 켜져 있는지 확인하십시오.
5. 시작 및 종료 날짜 정의 영역에서 이메일 알림 보내기를 시작하고 중지할 시기를 선택하십시오.

> 보낼 수 있는 최대 이메일 수는 30개입니다. 이 제한을 초기화하려면 관리자가 초대를 다시 보내야 합니다.

6. 빈도 정의 영역에서 이메일 알림을 얼마나 자주 보낼 것인지를 선택하십시오.
7. **다음**을 클릭하세요.
8. 이 구성에 대한 배포를 선택합니다.
9. **완료**를 클릭하세요.

## 사용자 등록 확인 이메일 구성하기

관리자는 등록을 완료한 새 사용자에게 이메일을 발송할 수 있습니다.

**절차**

1. 기존 **사용자 등록 확인 설정**을 편집하거나 새로 추가합니다.
2. 해당 설정의 이름을 수정 또는 설정하세요.
3. 해당 설정에 대한 간략한 설명(선택사항)을 입력하세요.
4. **사용자 등록 성공 후 확인 이메일 발송** 옵션이 켜져 있는지 확인하십시오.
5. **다음**을 클릭하세요.
6. 이 구성에 대한 배포를 선택합니다.
7. **완료**를 클릭하세요.

## 사용자 작업 일정 설정 구성

관리자는 정해진 근무 시간 외에 Sentry에서 관리되는 기기로의 모든 통신을 차단하는 사용자에 대한 사용자 작업 일정을 구성할 수 있습니다. 이는 연결을 해제할 권리 법률이 있는 로캘의 사용자에게 유용합니다.

**절차**

1. **사용자**를 선택합니다.
2. **사용자 설정**을 선택합니다.
3. **사용자 작업 일정 설정** 섹션에서, **+특정 사용자 그룹에 대한 설정 추가**를 선택합니다.
4. 설정에 대한 이름을 제공합니다.
5. 설정을 켭니다.
6. 시간대를 선택합니다.
7. MDM용 Ivanti Neurons가 Exchange ActiveSync 프로토콜, AppConnect 지원 앱 및 관리형 앱을 차단하는 시간을 구성합니다.
8. **다음**을 클릭하세요.
9. 배포를 구성한 다음, **완료**를 클릭합니다.

> 변경 사항이 기기에 적용되려면 최대 1시간 15분 정도 걸릴 수 있습니다.

# 관리 포털 인증 설정 구성

관리자는 사용자 로그인 인증을 위한 인증 유형을 설정할 수 있습니다. 이 설정을 통해 사용자가 비밀번호만 입력하도록 할지 비밀번호와 PIN 모두 입력하도록 할지 표시됩니다.

**절차**

1. 기존 **관리자 포털 인증 설정**을 편집하거나 새로 추가합니다.
2. 해당 설정의 이름을 수정 또는 설정하세요.
3. 해당 설정에 대한 간략한 설명(선택사항)을 입력하세요.
4. **관리자 포털 인증 유형**에서 다음 옵션 중 하나를 선택하십시오.

| 옵션 | 설명 |
| --- | --- |
| **비밀번호** | 비밀번호만 사용하여 로그인을 인증하려면 이 옵션을 선택합니다.<br>사용자는 계정 활성화를 완료하기 위해 여전히 PIN 입력을 요청받을 수도 있습니다. |
| **비밀번호 및 PIN** | 비밀번호와 PIN을 사용하여 로그인을 인증하려면 이 옵션을 선택합니다.<br>이 옵션을 선택하면 다음과 같은 항목이 추가로 표시됩니다.<br>• **PIN 수명:** 드롭다운 항목에서 PIN 수명의 분 단위를 선택합니다. 1분에서 15분 사이의 범위내에 있어야 합니다.<br>• **PIN 길이:** 드롭다운 항목에서 PIN 문자 길이를 선택합니다. PIN 길이는 4자에서 12자 사이의 범위내에 있어야 합니다.<br>이 옵션은 LDAP 관리자 계정이 아닌 로컬 계정에만 해당됩니다. |
| **사용자가 새로운 PIN을 생성하도록 허용** | 사용자가 새로운 PIN을 생성하도록 허용하려면 이 옵션을 선택합니다. |

5. **다음**을 클릭하세요.
6. 이 구성에 대한 배포를 선택합니다.
7. **완료**를 클릭하세요.

SAML-기반 ID 제공자(IdP)를 사용하여 구성한 사용자의 경우 MDM용 Ivanti Neurons는 관리자 포털에 대한 PIN 기반 인증을 지원합니다. 관리자 포털 인증 유형은 PIN 및 비밀번호이어야 합니다. 이 기능은 추가 보안을 위한 2단계 인증 역할을 합니다. 이 경우 해당하는 사용자가 포털에 로그인려고 하면:

- 사용자 이메일 ID로 PIN이 전송됩니다.
- 사용자가 관리자 포털 로그인 페이지에 PIN을 입력합니다.
- PIN이 올바를 경우 사용자가 IdP 사용자 이름 및 비밀번호를 입력하는 IdP 로그인 페이지로 리디렉션됩니다.
- IdP 자격 증명이 올바를 경우 사용자가 관리자 포털로 리디렉션됩니다.

관리자 포털에 로그인할 경우 **비밀번호 찾기**를 클릭하여 비밀번호를 재설정할 수 있습니다. 다음 화면에서 사용자의 이메일 주소로 전송된 새 비밀번호 및 PIN을 입력할 수 있습니다(이전 사용자의 인증 모드 설정에 따라 표시됨). 필요한 경우 **PIN 재전송**을 클릭합니다. 비밀번호 찾기 요청을 한 후에 다시 동일한 요청을 하려면 15분간 기다려야 합니다.

> 이 구성이 기기에 배포된 후 사용자가 비밀번호 또는 PIN을 사용한 로그인 시도에 연속적으로 실패하면(기본값: 5회) 계정이 잠기고 사용자에게 계정 잠김 메시지가 표시됩니다.

# 6.4. 사용자 브랜딩

사용자 브랜딩을 통해 사용자가 인식할 이름과 로고로 기기 등록 절차를 사용자 지정할 수 있습니다. 다음 방법으로 사용자 측 브랜딩을 설정할 수 있습니다.

- 등록 URL에 사용자 지정 호스트 이름 설정
- 등록 이메일과 등록 화면에 로고를 표시합니다.
- 등록 작업을 하는 동안 사용자 지정 favicon을 표시합니다.

> 위 설정을 업데이트하면 **$**에서 참조하는 값이 변경됩니다.

**라이센스**: Gold

**필수 조건**:

- 사용자 지정 URL에서 사용하고 싶은 호스트 이름을 결정합니다. 다음 요건을 충족해야 합니다.
  - 공백 포함하지 않음
  - 특수 문자 포함하지 않음

다음 요건을 충족시키는 로고 파일 확보:

  - PNG 형식
  - 580 x 80픽셀

다음 요건을 충족시키는 favicon 파일 확보:

  - PNG 형식
  - 64 x 64픽셀

**절차**:

1. **사용자 > 사용자 브랜딩**을 선택하세요.
2. **사용자 지정**(우측 상단)을 클릭하세요.
3. **호스트 이름** 필드에 URL에서 호스트 이름으로 사용할 약식 이름을 입력합니다.
4. **사용 가능성 확인**을 클릭하여 입력한 호스트 이름을 다른 사람이 사용하고 있는지 확인합니다.
5. 호스트 이름을 사용할 수 없다면 다른 이름을 입력합니다.
6. **URL 미리보기**에서 최종적인 등록 URL을 확인할 수 있습니다.
7. **다음**을 클릭하세요.
8. **로고**에서 **파일 선택**을 클릭하여 등록 이메일과 등록 화면에서 사용할 로고를 업로드합니다.
9. **다음**을 클릭하세요.
10. **Favicon**에서 **파일 선택**을 클릭하여 등록 활동을 하는 동안 MDM용 Ivanti Neurons favicon 대신에 표시할 favicon을 업로드합니다.
11. **완료**를 클릭하세요.

# 6.5. Apple Business Manager로 사용자 등록

이 섹션에는 다음 주제가 포함됩니다.

**적용 대상**:

- MDM용 Ivanti Neurons가 지원하는 최신 버전을 통해 iOS 13.0이 설치된 비감독 기기
- macOS 10.15 또는 지원되는 최신 버전이 있는 기기MDM용 Ivanti Neurons.

Apple Business Manager는 IT 팀이 기기 배치를 자동화하고 콘텐츠를 구매, 배포하고 조직 내 역할을 관리할 수 있는 장소입니다. Apple Business Manager 구현 사용자 등록 - BYOD(Bring Your Own Device)를 구현하는 회사를 위해 설계된 등록 옵션입니다. 사용자 등록은 사용자 개인정보에 초점을 맞춰 기업에서 필요로 하는 보안 수준을 구현한 수정된 버전의 MDM 프로토콜입니다.

사용자 등록을 통해 관리자는 다음을 수행할 수 있습니다.

- 관리되는 애플리케이션의 설치 및 제거
- 네트워크 구성의 설치 및 제거
- 앱 및 계정을 관리하기 위해 범위가 지정된 부분 VPN 설치
- 비밀번호 사용 요구

## 사용자 등록 활성화 요구

아래는 사용자 등록을 활성화하는 데 필요한 요구 사항입니다. 다음 중 하나라도 충족되지 않는 경우 등록 유형은 등록된 기기가 됩니다.

- MDM용 Ivanti Neurons에서 지원하는 iOS 13.0 이상 최신 버전이 설치된 비감독 기기 또는 macOS 10.15 또는 지원되는 최신 버전 MDM용 Ivanti Neurons가 설치된 기기
- Apple 등록 유형 필드에 대한 사용자 설정은 "사용자 등록"이어야 합니다.
- Apple Business Manager 계정.
    - Apple 앱 라이센스 계정은 동일한 Apple Business Manager 계정의 일부여야 합니다.
    - Apple Business Manager 내에서 위치에 열거된 계정이 있는 경우 같은 위치에 일치하는 Apps 및 Books가 있어야 합니다. 새로운 위치를 추가해야 할 수도 있습니다(예: West Coast).

관리되는 Apple ID - 등록된 각 기기와 연결된 관리되는 Apple ID입니다.

- 관리되는 Apple ID는 MDM 관리 및 앱 라이센스에 대한 인증을 제공합니다.
- MDM이 앱 및 미디어를 푸시다운하면 필요한 Apple 라이센스는 기기와 연결된 관리되는 Apple ID에 할당됩니다.
- GDPR 규정 준수의 일환으로, 관리되는 Apple ID는 Apple ID가 사용자 데이터가 될 것이라 간주하여 사용자 목록 및 사용자 상세 정보에 가려진 상태로 표시됩니다.
- 관리되는 Apple ID는 처음에 Apple School Manager를 이용했으나 이제는 사용자 등록을 위해 Apple Business Manager를 이용합니다.

> 기기의 관리되는 Apple ID와 Apps 및 Books 위치 토큰은 동일한 Apple Business Manager 계정의 조직에서 가져온 것이어야 합니다.

이 둘이 달라 앱에서 라이센스 할당이 실패하는 경우 MDM용 Ivanti Neurons 관리자 포털에 알림이 표시됩니다.

페더레이션 인증용으로 구성된 Microsoft Entra ID 또는 검증된 도메인으로 Apple Business Manager에서 수동으로 생성된 Apple ID입니다.

- Federated Authentication에 대한 지침은 Apple 웹 사이트의 **Apple Business Manager 사용자 가이드**를 참조하십시오. 로그인이 필요합니다.

LDAP에 동기화된 기기 사용자는 관리되는 Apple ID로 기기 관리에 할당됩니다.

사용자 목록 페이지와 기기 목록 페이지에서 관리되는 Apple ID 열을 추가하여 모든 사용자에게 표시할 수 있습니다. 기기 목록 페이지에서 사용자 등록 등록됨 열을 추가하여 사용자 등록 기기의 상태를 표시할 수 있습니다. 또한, 사용자 및 기기 내보내기의 CSV 파일에 이 열이 포함되어 있습니다.

## 등록 우선순위

- 사용자 등록은 iOS 클라이언트 및 iReg를 통해 지원됩니다. Apple은 더 이상 iOS 및 iReg용 Ivanti Go를 통한 사용자 등록을 지원하지 않습니다. **계정 기반 사용자 등록**은 해당 기기의 직장 또는 학교 계정에서만 사용할 수 있습니다.
- 자동화 기기 등록 및 Apple Configurator 등록은 항상 기기 등록입니다.
- MAM 구성이 기기에 적용되면 MAM 등록이 사용자 등록보다 우선합니다.
- 인증 전용 및 사용자 등록이 충돌하면 사용자 등록이 우선합니다.
- iOS용 Go 클라이언트에서 기기를 재등록하면 등록 유형은 MDM용 Ivanti Neurons에서의 등록 유형 변경에 상관없이 기기 등록 시의 유형과 같아집니다. 예를 들어 기기가 사용자 등록되고 MDM용 Ivanti Neurons에서 기기 등록 유형이 바뀌었으며 Go 클라이언트의 기기를 다시 등록했다면 기기는 여전히 사용자 등록 상태이며 기기 등록 상태가 아닙니다.

## 표준 MDM 등록과 사용자 등록의 차이점

이 섹션에서는 Apple Business Manager를 통한 표준 MDM 등록과 사용자 등록의 차이점에 대해 안내합니다.

### 표준 MDM 등록

다음 목록은 사용자 등록 모드에서는 불가능하지만 표준 MDM 등록에서는 MDM용 Ivanti Neurons 서버로 할 수 있는 것을 나타냅니다.

MDM 서버:

- 기기를 삭제할 수 없습니다.
- 기기 사용자가 기기에 설치한 개인 앱을 볼 수 없습니다.
- 사용자가 설치한 앱을 MDM으로 관리되는 앱으로 변환할 수 없습니다.
- 기기 암호를 삭제할 수 없습니다(예: 기기 잠금 해제).
- 길고 복잡한 기기 암호 요건을 설정할 수 없습니다.
- 기기 전체 VPN 또는 Wi-Fi 프록시를 구성할 수 없으며 휴대폰 기능을 관리할 수 없습니다.
- UDID, 일련 번호, IMEI 등의 기기 식별자를 볼 수 없습니다.
- 많은 기기 전체 제한(앱 콘텐츠 평가 제한 등), iCloud 차단, 감독되는 제한을 적용할 수 없습니다.

### Apple Business Manager로 사용자 등록

사용자 등록에서 MDM 서버로 엔터프라이즈 앱, 계정, 데이터를 관리하기 위한 모든 것을 할 수 있습니다.

사용자 등록으로 가능한 사항:

- 사용자 기반 (Apple) Apps 및 Books 라이센스를 통해 인하우스 앱 또는 앱을 설치합니다.
  - 선착순으로 라이센스가 적용되며 이는 관리되는 Apple ID로 사용됩니다.
  - 사용자 등록 기기에 설치된 앱에서 사용되는 라이센스는 기기 등록된 기기에 설치된 동일한 앱에서 사용되는 라이센스와 다릅니다.

- 라이센스 사용 탭을 통해 사용자 상세 정보 페이지에서 Apple Apps 및 Books 애플리케이션에 대한 라이센스 유형을 확인합니다. 등록 유형이 사용자 등록 또는 기기 등록으로 표시됩니다.

암호 페이로드 설정을 실행합니다. 예:

- allowSimple = false
- forcePIN = true
- minLength = 6

엔터프라이즈 관리 앱, 인증서, 프로필에 관련된 데이터를 쿼리합니다.

- MDM이 설치한 앱, 메일, 연락처, 캘린더에 대한 퍼앱 VPN을 구성합니다.
- 관리되는 오픈인, 관리되는 연락처, 잠금 화면에서 관리되는 데이터 및 여러 제한을 실행합니다.

엔터프라이즈 데이터는 등록에 생성되어 기기 사용자 데이터에 별도로 암호화된 개별 Apple File System(APFS) 볼륨에 저장됩니다. 이 볼륨에는 관리되는 앱, 엔터프라이즈 노트, 엔터프라이즈 iCloud 드라이브 문서, 엔터프라이즈 키체인 입력, 관리되는 메일 첨부파일 및 본문, 캘린더 첨부파일이 저장됩니다. MDM에서 등록 취소되면 볼륨 및 키를 제거합니다.

모든 타사 앱은 개인 앱이거나 MDM용 Ivanti Neurons를 통한 관리형 앱입니다. MDM 서비스는 기기 사용자가 이미 설치한 관리 앱을 시작할 수 없습니다. 이 경우 관리자는 기기 사용자가 MDM을 통해 앱을 설치하기 전 개인 앱을 삭제하도록 요구할 수 있습니다. MDM 서비스는 사용자가 이미 설치한 관리 앱을 시작할 수 없습니다. 그러나 노트 및 파일 등 일부 시스템 앱은 작업 및 개인 계정을 모두 지원합니다.

## macOS 기기용 사용자 등록

사용자 등록은 macOS 10.15 또는 지원되는 최신 MDM용 Ivanti Neurons 버전이 있는 기기에 지원됩니다.

- macOS용 Mobile@Work는 macOS 사용자 등록 등록된 기기에 대해서는 지원되지 않습니다.
  - macOS 사용자 등록 등록된 기기에 앱이 배포된 경우에도 앱은 MDM에서 기기로 푸시되지 않습니다.
  - 따라서 Packager(MIP) 앱에 대한 스크립트 관리 및 앱 관리와 같은 Mobile@Work 기능은 macOS 사용자 등록 등록된 기기에 대해 지원되지 않습니다.

macOS 사용자 등록 등록된 기기의 앱 종속성 및 동작 변경 사항.

- macOS 사용자 등록 등록된 기기에서는 MDM이 메인 앱을 배포하기 전 필수 조건 앱의 설치 상태에 대해 인지하지 못하므로(확인할 수 없으므로) 앱 종속성이 최선을 다해 작동합니다.
- 앱 및 구성은 macOS 사용자 등록 등록된 기기에 속하는 사용자 및 사용자 그룹에 배포될 수 있습니다. 그러나 MDM이 macOS 사용자 등록 등록된 기기에 앱의 설치 상태를 표시할 수 없기 때문에 앱은 "설치됨" 대신 항상 **설치** 버튼을 표시합니다.
- macOS 사용자 등록 등록된 기기가 앱이 인벤토리 보고서에 설치되었는지 설치되지 않았는지 MDM용 Ivanti Neurons 서버에 알리지 않으므로 설치된 앱은 **기기 > 앱 인벤토리** 페이지에 요청된 앱으로 표시됩니다.

앱용 배포 필터에서 사용자 등록 등록됨 및 자동화 기기 등록 등록됨 속성을 필요한 만큼 사용자 지정 배포에 사용할 수 있습니다.

- 사용자 기반 라이센스가 지원되어 Apple ID를 사용하여 Apple Apps 및 Books 애플리케이션을 설치합니다. 기기 기반 라이센스는 허용되지 않습니다. App Catalog에는 Apple Apps 및 Books 애플리케이션만 표시됩니다.
- 모든 구성, 정책, 작업이 허용되는 것은 아닙니다. 이 절차 후 열거되는 구성 및 정책 전체 목록을 확인하십시오.
  - 지원되지 않는 구성이 macOS 사용자 등록 등록된 기기로 배포될 경우 기기에 배포되거나 적용되지 않으며, "제한 - 이는 유효한 요청 유형이 아닙니다"와 같은 메시지가 표시될 수 있습니다.
  - 이와 유사하게 지원되지 않는 관리자 기기 작업이 MDM용 Ivanti Neurons UI에 설명됩니다.
  - 지원되지 않는 보고서는 MDM용 Ivanti Neurons에서 전송하지 않습니다.

다음은 macOS 사용자 등록 등록된 기기에 배포될 지원되지 않는 구성 및 정책입니다.

- 암호
- Tunnel
- Tunnel(주문형)
- VPN 구성
- Office 365 자동 계정 생성
- macOS 커널 확장 정책
- 개인정보 보호 환경설정
- macOS 제한
- 소프트웨어 업데이트
- AirPrint
- MI 클라이언트 개인정보 보호
- FileVault 2
- FileVault 복구 키
- 방화벽
- 시스템 정책 규칙
- 인증서 환경설정
- 시스템 정책 제어
- 관리되는 시스템 정책
- macOS 앱스토어 제한 사항
- macOS 디스크 굽기 제한 사항
- macOS 파인더 설정
- macOS용 Mobile@Work
- macOS 스크립트용 Mobile@Work
- 허용된 미디어 컨트롤
- 시간 서버
- 허용된 앱 정책

## 사용자 등록과 기기 등록의 차이점

이 섹션에서는 사용자 등록과 기기 등록의 차이점을 설명합니다.

사용자 등록은 iOS 13.0 및 macOS 10.15 이상 최신 버전이 설치된 기기에 적용됩니다. iOS 13.0 및 macOS 10.15 이하 기기는 기기 사용자가 사용자 등록을 위해 활성화했는지 여부에 관계 없이 "기기 등록"으로 간주합니다.

> Apple Business Manager를 위한 사용자 등록은 지우기 또는 잠금 해제를 허용하지 않습니다. 그러나 작동하지 않더라도 사용자 포털에 해당 옵션이 여전히 있습니다.

| 사용자 등록 vs 기기 등록 | | |
|---|---|---|
| 기능 | 사용자 등록 | MAM 기기 등록 |
| 기기 삭제 및 사용자의 개인 앱 보기 | ✗ | ✗ ✓ |
| 관리에서 비관리로, 또는 그 반대로 변환 | ✗ | ✗ ✓ |
| 기기 암호 지우기, 기기 전체 VPN 또는 Wi-Fi 프록시 구성 또는 휴대폰 기능 관리 | ✗ | ✗ ✓ |
| 일련 번호, IMEI 등 기기 식별자 보기 | ✗ | ✗ ✓ |
| 감독되는 제한 적용 | ✗ | ✗ ✓ (감독되는 기기 전용) |
| 앱 및 계정 설치 및 구성 가능 | ✓ | ✓ ✓ |
| MDM으로 설치된 앱, 메일, 연락처, 캘린더에 대한 퍼앱 VPN 구성 가능 | ✓ | ✗ ✓ |
| 관리되는 오픈인, 관리되는 연락처, 잠금 화면에서 관리되는 데이터 및 여러 제한 실행 가능 | ✓ | ✗ ✓ |
| 엔터프라이즈 관리 앱, 인증서, 프로필에 관련된 데이터 쿼리 가능 | ✓ | ✗ ✓ |

# MDM용 Ivanti Neurons와 Apple Business Manager 연결

이 섹션에서는 Apple Business Manager를 위한 사용자 등록 활성화에 대해 설명합니다.

**필수 조건**

- Apple Business Manager 계정이 있어야 합니다. **https://business.apple.com/**을 참조하십시오.
- iOS 기기를 관리하려면 Apple **MDM 인증서**를 요청해 설치해야 합니다.

## 사용자 등록을 활성화하기 위한 로컬 사용자 생성

이 섹션에서는 로컬 및 LDAP 사용자 생성 및 비감독 Apple 기기에 대한 사용자 등록에 대해 설명합니다. 사용자 등록은 감독되는 기기 또는 Apple 기기 등록에 등록된 기기에서 실행되지 않습니다.

## 수동으로 관리되는 (정적) 사용자 그룹 생성

이는 일회용 절차입니다. 이미 이 그룹을 생성했다면 "사용자 등록을 위한 사용자 생성" 섹션은 건너뜁니다.

**절차**

1. **사용자 >** 사용자 그룹으로 이동합니다.
2. 사용자 등록 그룹 등의 수동으로 관리되는 (정적) 사용자 그룹을 생성하여 장치 등록 유형을 가진 사용자를 사용자 등록 유형으로 추가합니다.
3. **저장**을 클릭하세요.

## 기기 등록 유형 설정을 생성합니다.

이는 일회용 절차입니다. 이미 이 그룹을 생성했다면 "사용자 등록을 위한 사용자 생성" 섹션은 건너뜁니다. 사용자 등록 등록된 기기의 경우 기기 소유자 설정은 "사용자 소유"입니다.

**절차**

1. **사용자 > 사용자 설정**으로 이동합니다.
2. 기기 등록 설정 섹션에서 **+ 특정 사용자 그룹 설정 추가**를 클릭합니다.
3. 사용자 등록으로 기기 등록 유형이 있는 사용자들을 위해 UE 등록 등의 새로운 설정을 생성합니다.
4. Apple 등록 섹션에서 Apple 등록 유형으로 **사용자 등록**을 선택합니다.
5. **다음**을 클릭하세요.
6. 사용자 설정 배포 페이지에서 사용자 등록 그룹 등의 새로 생성된 사용자 그룹을 선택합니다.
7. **완료**를 클릭하세요.

## 사용자 등록을 위한 로컬 사용자 생성

필수 조건으로 수동으로 관리되는 사용자 그룹 및 사용자 등록을 위한 기기 등록 설정을 생성합니다.

**절차**

1. 사용자로 이동합니다.
2. **+추가** > **단일 사용자**를 클릭합니다.
   새 사용자 정보를 입력하고 이를 사용자 등록 그룹 등의 새로 생성된 사용자 그룹에 추가합니다. 자세한 내용은 사용자 항목에서 *사용자 추가*를 참조하십시오.

## 사용자 등록을 활성화하기 위한 LDAP 사용자 불러오기

**필수 조건**

- 필수 조건으로 **LDAP** 리소스에 액세스하는 MDM용 Ivanti Neurons 커넥터를 설정합니다.
- **관리형 Apple ID** 설정이 **패턴**(사용자 이메일 주소)으로 설정되어 있어야 합니다. 관리되는 Apple ID의 패턴이 고유한지 확인합니다. 그렇지 않은 경우 다른 계정에 관리되는 Apple ID가 있으면 계정이 관리되는 Apple ID로 업데이트되지 않을 수 있습니다.
- (선택 사항) 기존 Apple ID와의 충돌을 방지하기 위해 “appleid” 하위 도메인을 포함합니다.
- LDAP에서 사용자를 불러와 사용자 등록으로 초대할 수 있습니다. 불러온 LDAP 사용자는 사용자 등록에 필요한 MDM용 Ivanti Neurons와 동기화된 관리되는 Apple ID를 가질 수 있습니다.

**절차**

1. **사용자**를 선택하세요.
2. **+추가 > LDAP에서 사용자 초대**를 클릭합니다.
3. LDAP 서버 항목에서 **사용자 선택**을 클릭합니다.
4. LDAP 사용자 추가 페이지에서 사용자, 그룹 또는 OU를 검색 필드에 입력합니다.
5. 새 사용자 또는 그룹을 추가하려면 추가하려는 항목 옆의 **+추가**를 클릭합니다.
6. **완료**를 클릭하세요.

## 사용자 등록을 활성화하기 위한 Entra ID 사용자 불러오기

필수 조건으로 Microsoft Entra ID(Entra ID)를 사용하여 MDM용 Ivanti Neurons에 연결합니다.

사용자 등록을 위해 Entra ID 사용자를 초대할 수 있습니다. 불러온 Entra ID 사용자는 MDM용 Ivanti Neurons와(과) 동기화된 관리형 Apple ID를 가지게 되며 이는 사용자 등록에 필요합니다.

**절차**

1. **관리자 > Entra ID 사용자 소스**로 이동합니다.
2. 설정을 편집합니다.
3. **이 Entra ID 활성화**를 선택합니다.
4. 관리형 Apple ID 설정에서 다음 옵션 중 하나를 선택합니다.
   - **패턴**
     - **사용자 이메일 주소** - 관리형 Apple ID의 패턴이 고유해야 합니다. 그렇지 않은 경우 다른 계정에 관리되는 Apple ID가 있으면 계정이 관리되는 Apple ID로 업데이트되지 않을 수 있습니다.
     - 또는 **userUPN**을 선택합니다.
5. (선택 사항) 기존 Apple ID와의 충돌을 방지하기 위해 “appleid” 하위 도메인을 포함합니다.
6. **Entra ID에서 불러온 사용자를 자동으로 초대**를 선택합니다. Entra ID에서 MDM용 Ivanti Neurons(으)로 불러온 사용자에게 자동으로 등록 초대 이메일을 보냅니다.
7. **저장**을 클릭하세요.

## 사용자 등록을 이용해 등록하기 위한 기기 사용자 지침

이 섹션에서는 Apple 사용자 등록을 등록하기 위해 필요한 기기 사용자 작업에 대해 안내합니다.

**절차**

1. 등록하려는 iOS 기기에서 최종 사용자를 mobileiron.com/go 등의 등록 링크로 안내하는 링크 및 텍스트를 포함한 이메일 초대를 엽니다.
2. Safari에서 등록 링크를 엽니다.
3. 로그인 페이지가 표시됩니다. 기기 사용자는 로컬 사용자 또는 LDAP 자격 증명을 사용하여 로그인합니다.
   프로필을 다운로드했다는 메시지와 함께 등록 페이지가 표시됩니다.
   설정을 누릅니다. 설정 페이지가 표시됩니다.
4. [Your Company Name]에 등록을 누릅니다.
5. 사용자 등록 페이지가 나타납니다.
6. 내 [Your Device] 등록을 누릅니다. 을 누릅니다. 예: 나의 iPhone 등록을 누릅니다.
   취소 및 프로필 삭제를 누르면 등록 절차를 모두 다시 시작해야 합니다.
   Apple 또는 Federated 계정에 대한 로그인이 나타납니다. 관리되는 Apple ID의 비밀번호를 입력합니다. (관리되는 Apple ID가 로그인 페이지 상단에 열거됩니다.)
   로그인 상태를 유지할 것인지 선택하는 옵션이 나타납니다.
   페이지에 "등록 성공"이 표시됩니다.

## 문제 해결을 위한 기기 로그 사용

사용자 등록 기기의 오류 또는 문제를 해결하려면 기기 로그부터 검토합니다.

**절차**

1. 기기로 이동합니다.

2. 기기를 클릭해 기기 상세 정보 페이지를 표시합니다. 사용자 등록 등록됨 및 등록된 관리되는 Apple ID 필드를 검증할 수 있습니다.
3. 로그 탭을 선택합니다.
4. 필터 영역에서 작업 이름(예: 체크아웃, 기기 이름, 부트스트랩 토큰 설정, 부트스트랩 토큰 받기 등), 상태, 시작 날짜, 종료 날짜 등을 기반으로 필터를 사용하여 기기 로그를 구체화합니다.
5. 작업 열에서 눈 모양 아이콘을 클릭해 등록 ID 등의 기기 로그 상세 정보를 표시합니다.
6. **확인**을 클릭하세요.

# 6.6. 사용자 라이센스

MDM용 Ivanti Neurons 사용자 기반 라이선스는 등록 가능한 사용자 수, 사용자 라이선스당 허용되는 기기 수, 기기 배포용으로 구성 가능한 콘텐츠 양, 사용 가능한 기능을 정의합니다. 사용자 한도에 도달할 경우 관리 페이지에 빨간 삼각형이 표시됩니다. 컨텐츠 양이 지정된 최대 한계에 도달하면 컨텐츠 추가가 차단되면서 지정된 최대 한계에 도달했다는 메시지가 표시됩니다.

사용자 라이센스 수를 정할 때에는 다음 사항을 참고하시기 바랍니다.

- Secure UEM 또는 Secure UEM Premium 패키지에서 구매한 각 사용자 라이센스로 기기를 최대 5개까지 등록할 수 있습니다.
- 사용자가 기기를 5대 이상 등록하면 추가 사용자 라이센스가 필요합니다.
- 사용자가 요청할 수 있는 사용자 라이센스 수에는 강제적 제한은 없다.
- 장치가 폐기되거나 지워지면 라이센스가 취소된다.

예를 들어, 어떤 사용자가 업무 첫날 업무용 전화를 등록하면 해당 사용자에게는 사용자 라이센스 하나가 필요합니다. 다음 주, 해당 사용자가 같은 라이센스로 2개의 개인전화와 태블릿을 등록합니다. 그런 다음, 태블릿을 하나 더 등록하게 되면 기기 5대를 등록한 것이므로 사용자 라이센스 하나가 추가적으로 필요합니다. 해당 사용자가 개인전화를 분실해 삭제하면 추가 사용자 라이센스가 취소됩니다.

## 사용자 기기/라이선스 수 보기

**절차**:

1. **사용자**를 선택하세요.
2. 원하는 사용자의 링크를 클릭하세요.

왼쪽 창에 사용 중인 라이센스 수를 포함한 사용자 정보가 목록으로 표시됩니다.

# 6.7. 사용자 관리

이 섹션에는 다음 주제가 포함됩니다.


- Cisco ISE 작업에 API 사용자 추가
- 사용자에게 역할 할당하기
- 사용자 역할
- 사용자 찾기 및 필터링
- 사용자 그룹에 사용자 할당하기
- 사용자 초대하기
- 사용자 활성화 및 비활성화
- 다중 관리자 로그인 관리
- 비밀번호 변경하기
- 메시지 보내기
- 사용자 그룹에서 사용자 삭제하기
- 사용자 삭제하기
- 사용자 내보내기
- 사용자에게 사용자 지정 속성 할당
- 사용자에게서 사용자 지정 속성 제거
- 사용자 로캘 변경
- 사용자 이름 편집
- 위치 데이터 수집 기능 해제하기
- 시간제한 정보
- 시스템 사용량 분석 기능 해제
- PIN 생성을 통한 기기 등록

# 6.7.1. Cisco ISE 작업에 API 사용자 추가

Cisco ISE가 MDM용 Ivanti Neurons에서 Cisco ISE API와 상호작용하도록 하는 'Cisco ISE 작업' 역할이 부여된 API 사용자를 추가할 수 있습니다. 이 사용자를 생성한 뒤에는 Cisco ISE로부터 이 사용자 자격 증명을 사용하여 MDM용 Ivanti Neurons에 API 호출을 인증합니다. 이 API를 사용하면 Cisco ISE가 장치 정보를 가져와서 작업을 수행할 수 있습니다. 예를 들어, 전체 지우기, 기업 지우기, 핀 잠금, 장치로 메시지 전송 등이 가능합니다.

> API 사용자는 관리자 포털에 로그인할 수 없게 됩니다. 이 사용자는 API 사용 활성화 전용입니다.

> 테넌트의 슈퍼 관리자에게만 기본적으로 Cisco ISE 작업 역할이 부여됩니다. 슈퍼 관리자는 시스템에서 이 역할을 맡을 다른 사용자를 명시적으로 선택하고 역할을 할당해야 합니다. Cisco ISE 작업 역할을 할당받은 사용자는 시스템의 다른 적절한 사용자에게 역할을 할당할 수 있습니다.

**절차**

1. **사용자** > **사용자**로 이동합니다.
2. **추가**를 클릭합니다.
3. **API 사용자**를 선택합니다.
4. 그 결과로 표시되는 양식에 사용자 정보를 입력합니다:
    - 이메일 주소
    - 이름
    - 성

> 사용자 이름 칸에는 입력한 이메일 주소가 표시됩니다. 해당 값은 기본값으로, 수정하지 않는 것이 좋습니다. 사용자 이름 수정이 필요한 경우를 참고하세요.

현재 사용자의 화면 표시 이름을 변경하려면 **표시 이름** 칸의 기본값을 수정하시기 바랍니다.

6. **비밀번호**와 **비밀번호 확인** 필드에 이를 입력하여 비밀번호를 할당합니다.
7. **API Management Cisco ISE 작업** 역할이 **역할 할당** 섹션에 선택된 채로 남겨둡니다.
8. **완료**를 클릭하면 해당 사용자가 등록됩니다.

**사용자** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 사용자 관리

# 6.7.2. 사용자에게 역할 할당하기

역할을 할당하여 사용자에게 (Undefined variable: 사용자 그룹) 데이터 및 기능에 대한 액세스 권한을 부여할 수 있습니다.사용자나 사용자 그룹에 직접 역할을 할당할 수 있습니다. {{사용자 그룹}}에 역할을 할당하면 해당 역할이 그룹 내 모든 사용자에게 할당됩니다.

> 사용자 읽기 전용 역할은 기본적으로 사용자에게 할당되지 않습니다.
> 역할 페이지 및 관련 옵션은 Ivanti Neurons for UEM 및 MDM용 Ivanti Neurons에 모두 액세스할 수 있는 테넌트에 대해 숨겨집니다.

사용자는 이미 가지고 있지 않은 권한을 할당할 수 없습니다. 사용자에게 할당되지 않는 권한과 역할은 선택에 표시되지 않습니다. 이러한 경우 오류 메시지가 표시됩니다. MDM용 Ivanti Neurons 관리자 또는 파트너 관리자가 파트너 관리자에게 역할 할당을 시도하면 MDM용 Ivanti Neurons은(는) 파트너 관리자가 서비스 공급자 포털에서 이 작업을 수행해야 함을 알리는 메시지를 표시합니다.

역할 관련 자세한 내용은 **Roles_Management.htm**을 참조하십시오.

**절차:**

1. 다음으로 이동합니다.
   - **사용자 > 사용자** *또는*
   - 사용자 > 사용자 그룹

하나 이상의 사용자나 사용자 그룹을 선택합니다.

3. **작업**을 선택하세요.
4. 사용자 상세 정보 페이지 또는 사용자 그룹 상세 정보 페이지에서 **역할 할당**을 클릭하거나 *또는* 사용자 목록 또는 사용자 그룹 목록 페이지에서 **역할 추가**를 선택합니다.
5. 다음 중에서 할당하려는 하나 이상의 역할을 선택합니다.
   - 시스템 관리 | 공간 교차
   - 시스템 읽기 전용 | 공간 교차
   - 사용자 관리 | 공간 교차
   - 사용자 읽기 전용 | 공간 교차
   - LDAP 사용자 가져오기 및 초대 | 공간 교차
   - 기기 관리 | 공간별
   - 기기 읽기 전용 | 공간별
   - 앱 및 콘텐츠 관리 | 공간별
   - 앱 및 콘텐츠 읽기 전용 | 공간별
   - 기기 작업 | 공간별
   - Cisco ISE 작업 | 공간 교차
   - 예약된 작업 관리 | 공간 교차
   - 공통 플랫폼 서비스(CPS) | 공간 교차
   - 낮은 사용자 영향 마이그레이션 관리 | 공간 교차
   - 사용자 지정 기기 등록 | 공간 교차
   - Microsoft Graph 편집 | 공간 교차
   - 지우기 보내기/취소 | 공간 교차

- Microsoft Graph 보기 | 공간 교차
- Access 통합 관리 | 공간 교차

**다음**을 클릭하세요.

7. 선택한 역할이 공간에 제한된 경우 모든 공간 제한 역할에 대한 공간을 선택합니다.

> 한 공간(기본 공간)만 있는 경우 공간 연결 역할을 할당할 때 공간 지정 단계를 건너뜁니다.

요약 페이지가 공간 연결 라운드의 공간 이름을 기본 공간으로 표시합니다.
할당할 역할의 요약을 검토하고 **완료**를 클릭합니다.

## 헬프데스크 직원에게 기본 기기 작업 사용 권한 부여

일반적으로 헬프데스크 역할을 이용하면 직원이 데이터를 볼 수 있습니다. 그러나 일부 조직은 다음과 같은 기본 기기 작업을 포함시키는 것을 선호합니다.

- 강제 체크인
- 잠금
- 잠금 해제
- 메시지 보내기
- 폐기
- 지우기

**절차**

작업에 대한 권한을 제공할 수 있습니다.

1. **사용자 > 사용자*** 또는 ***사용자 > 사용자 그룹**으로 이동합니다.
2. 하나 이상의 사용자나 사용자 그룹을 선택합니다.
3. **작업**을 선택하세요.
4. 사용자 상세 정보 페이지 또는 사용자 그룹 상세 정보 페이지에서 **역할 할당***을 선택하거나*
   사용자 목록 또는 사용자 그룹 목록 페이지에서 **역할 추가**를 선택합니다.
5. **기기 읽기 전용**을 선택합니다.
6. 기기 작업**을 선택하십시오**.
7. **완료**를 클릭하세요.

> 기기 작업을 선택하여 사용자에게 예상한 권한을 제공하기 전에 반드시 기기 읽기 전용을 선택합니다.

# 6.7.3. 사용자 역할

사용자 역할은 사용자가 MDM용 Ivanti Neurons에서 볼 수 있는 페이지와 사용자가 수행할 수 있는 작업을 결정합니다. 할당할 수 있는 역할 종류와 관련 내용을 아래 표에서 확인하실 수 있습니다.

| 역할 | 설명 | 공간별 |
| --- | --- | --- |
| 시스템 관리 | 관리자가 테넌트 수준 설정(예: MDM 인증서, App Catalog 설정 등)을 관리할 수 있습니다. | 아니요 |
| 시스템 읽기 전용 | 관리자가 테넌트 수준 설정(예: MDM 인증서, App Catalog 설정 등)을 확인할 수 있습니다. | 아니요 |
| 사용자 관리 | 관리자가 사용자를 추가 및 제거하거나 역할을 할당하거나 사용자를 사용자 그룹에 추가할 수 있습니다. | 아니요 |
| 사용자 읽기 전용 | 관리자가 사용자 및 사용자 그룹뿐만 아니라 앱과 콘텐츠 카탈로그를 확인할 수 있습니다. | 아니요 |
| 기기 관리 | 관리자가 기기 그룹, 구성 및 정책을 관리할 뿐만 아니라 모든 기기 작업을 수행할 수 있습니다. | 예를 눌러 |
| 장치 읽기 전용 | 관리자가 기기 그룹, 구성, 정책을 확인할 수 있습니다. | 예를 눌러 |
| 앱 및 컨텐츠 관리 | 관리자가 앱과 콘텐츠를 추가 및 배포하고 삭제할 수 있습니다. | 예를 눌러 |
| 앱 및 컨텐츠 읽기 전용 | AppConnect 작업을 포함하여 사용자, 앱, 콘텐츠의 데이터 보기 | 예를 눌러 |
| 기기 작업 | 관리자가 다음과 같은 기기 작업을 시작할 수 있습니다.<br>• 강제 체크인<br>• 잠금<br>• 잠금 해제<br>• 메시지 보내기<br>• 폐기<br>• 지우기<br>기기 작업을 선택하기 전에 장치 읽기 전용을 선택해야 합니다. 그렇지 않을 경우 사용자가 원하는 권한을 받을 수 없습니다. | 예를 눌러 |
| LDAP 사용자 가져오기 및 초대 | 관리자가 LDAP 사용자를 등록하고 초대를 보내 기기를 등록할 수 있습니다. | 아니요 |
| Cisco ISE 작업 | 관리자가 Cisco ISE 통합에 필요한 API를 불러올 수 있습니다. | 아니요 |
| 예약된 작업 관리 | 관리자가 다양한 관리 작업을 위해 예약된 작업을 생성하고 관리할 수 있습니다. | 아니요 |
| 공통 플랫폼 서비스(CPS) | 관리자가 공통 플랫폼 서비스를 사용할 수 있습니다. | 아니요 |
| 낮은 사용자 영향 마이그레이션 관리 | 관리자가 사용자 영향 마이그레이션 설정을 관리할 수 있습니다. | 아니요 |
| 사용자 지정 기기 등록 | 관리자가 사용자 지정 기기 등록으로 기기를 등록할 수 있습니다. | 아니요 |
| Microsoft Graph 편집 | 관리자가 Office 365 앱 보호에 사용되는 Microsoft Graph API 설정을 편집할 수 있습니다. | 아니요 |
| Microsoft Graph 보기 | 관리자가 Office 365 앱 보호에 사용되는 Microsoft Graph API 설정을 확인할 수 있습니다. | 아니요 |

| 역할 | 설명 | 공간별 |
| --- | --- | --- |
| 지우기 전송/취소 | 관리자가 기기로 지우기 명령을 전송하거나 실행되기 전에 발행된 지우기 명령을 취소할 수 있습니다. | 아니요 |
| Access 통합 관리 | 관리자가 Access 통합을 관리할 수 있습니다. | 아니요 |

자세한 내용은 **역할 할당하기**를 참조하십시오

# 6.7.4. 사용자 찾기 및 필터링

이 섹션에는 다음 주제가 포함됩니다.

## 사용자 검색

여러 사용자를 등록한 경우, 필터나 검색 기능을 이용하면 특정 사용자 위치를 빠르게 파악할 수 있습니다.

**절차**

1. **사용자**를 선택하세요.
2. 검색 상자에 검색어를 입력합니다.

## 사용자 고급 검색 사용

특정 기준에 따라 사용자를 식별하고 보려면 고급 검색 옵션을 사용하여 규칙에 기반한 사용자를 검색할 수 있습니다. 규칙 옵션은 임의(OR) 또는 모두(AND) 옵션을 사용하여 중첩될 수 있습니다. 섹션 하단에 규칙과 일치하는 사용자가 표시됩니다. 규칙은 다음 연산자를 이용해 구성할 수 있습니다.

- 다음으로 시작
- 끝
- 포함
- 포함되지 않음
- 다음으로 시작하지 않음
- 다음으로 끝나지 않음
- 보다 작음
- 보다 큼
- 범위에 있음
- 같음
- 다음과 같지 않음

MDM용 Neurons 127부터 MDM용 Ivanti Neurons 관리자는 규칙 작성기에서 사용자 그룹 이름 속성을 선택할 때 중복 그룹을 식별할 수 있도록 중복 사용자 그룹 수 및 해당 GUID 수를 표시합니다. 또한 이 규칙 아래에 있는 표에는 중복 사용자 그룹 목록과 사용자 그룹 이름, GUID, 소스, 배포된 이름(DN)과 같은 세부 정보가 표시됩니다.

**절차**

1. 사용자 페이지에서 **고급 검색** 링크를 클릭합니다.
2. 사용자가 규칙 중 하나 이상을 충족해야 할 경우에는 **일부**를 선택하고 사용자가 모든 규칙을 충족해야 할 경우에는 **모두**를 클릭합니다.
3. 사용자 그룹, 사용자 지정 사용자 속성 및 사용자 지정 LDAP 속성 등, 검색 기준을 정의하는 규칙을 생성합니다.
4. (선택 사항) 필요할 경우 +를 클릭하여 추가 규칙을 생성할 수 있습니다.
5. (선택 사항) 쿼리를 저장하려면 **저장**을 클릭합니다.
6. **검색**을 클릭합니다. 검색 기준에 부합하는 사용자 목록이 페이지에 표시됩니다.

## 사용자 검색 쿼리 로드

**절차**

1. 사용자 페이지에서 **고급 검색** 링크를 클릭합니다.
2. '폴더' 아이콘을 클릭합니다. **고급 검색** 창이 표시됩니다. 생성된 검색 쿼리 목록이 **쿼리 로드** 섹션에 표시됩니다. 이 섹션에 다음 상세 정보가 표시됩니다.
   - **쿼리 이름** - 로드된 쿼리 이름.
   - **쿼리 콘텐츠** - 검색 쿼리를 정의하는 규칙에 콘텐츠를 표시합니다.
   - **작업** - 쿼리에서 수행할 작업을 선택합니다.
3. 로드된 쿼리에 정의된 기준에 부합하는 사용자 목록을 보려면 **작업** 열에서 **쿼리 로드**를 클릭합니다.
   로드된 쿼리를 삭제하려면 삭제 아이콘을 클릭합니다.

## 사용자 필터링

필터 측면 탐색 모음에는 전체 사용자 목록에서 특정 사용자를 검색할 수 있는 다양한 섹션이 나열되어 있습니다. 필터 관리 마법사에는 필터 탐색 모음에 표시할 수 있는 모든 섹션의 목록이 포함되어 있습니다.

**절차**

1. **사용자**를 선택하세요.
2. 필터 관리 마법사에 나열된 섹션에서 관련 체크박스를 클릭합니다. 다음 섹션에서 검색할 수 있습니다.
   - 관리자
   - Google 상태
   - 초대 상태
     - 완료(사용자가 초대를 받고 답변한 상태)
     - 만료(사용자가 시간 안에 답변을 안 한 상태)
     - 초대 안 됨(해당 사용자를 초대하지 않은 상태)
     - 보류 중(사용자 응답 보류)

   비밀번호 만료
     - 만료(비밀번호 만료 옵션을 특정 날짜로 설정하는 사용자)
     - 만료 안 됨(비밀번호 만료 옵션을 만료 안 됨으로 설정하는 사용자)
   - 사용자 그룹(원하는 {{사용자 그룹}} 선택)
   - 사용자 소스
     - LDAP
     - Entra ID
     - 명단
     - Salesforce
     - 로컬
   - 동기화
     - 직접 동기화 - LDAP 서버에서 직접 동기화된 사용자 목록 나열
     - 동기화 없음 - LDAP 서버에서 제거된 사용자 목록 나열
     - 간접 동기화 - LDAP 서버에서 간접 동기화된 사용자 목록 나열

- 해당 없음

3. (선택 사항) **기본값 복원**을 클릭하면 선택 사항을 기본값 필터로 복원할 수 있습니다. 필터 탐색 모음에 선택한 섹션이 표시됩니다. 필터 관리 마법사에서 모든 체크박스의 선택을 해제하면 필터 측면 탐색 모음에 모든 섹션이 표시됩니다.
4. 마법사를 종료하려면 필터 관리 마법사 바깥 영역을 아무 곳이나 클릭합니다.
5. 필터 측면 탐색 모음을 닫으려면 x 아이콘을 클릭하고 측면 탐색 모음을 다시 열려면 **필터**를 클릭합니다.

# 6.7.5. 사용자 그룹에 사용자 할당하기

이 섹션에는 다음 주제가 포함됩니다.

- 사용자 페이지에서 사용자 할당하기
- 사용자 그룹 페이지에서 사용자 할당하기

사용자 그룹에 사용자를 할당하면 다음과 같은 작업의 반복횟수를 최소화할 수 있습니다.

- 앱 배포
- 역할 할당

## 사용자 페이지에서 사용자 할당하기

1. **사용자**를 선택하세요.
2. 원하는 사용자를 선택하세요.
3. **작업**을 선택하세요.
4. **그룹으로 할당**을 선택하십시오.
5. 그룹을 선택하거나 **새로 생성**을 클릭해 새로운 그룹을 만듭니다.
6. **저장**을 클릭하세요.

## 사용자 그룹 페이지에서 사용자 할당하기

1. **사용자 > 사용자 그룹**을 선택하세요.
2. 원하는 사용자 그룹을 선택하세요.
3. **작업**(우측 상단)을 클릭하세요.
4. **사용자 할당**을 선택합니다.
5. 각 사용자의 이메일 주소를 입력하세요.
6. **사용자 할당**을 클릭하세요.

# 6.7.6. 사용자 초대하기

사용자를 등록할 경우 해당 사용자를 초대해 기기를 등록할 수 있습니다. 이 항목은 기본값으로 선택됩니다. 초대를 받은 사용자에게는 등록에 필요한 정보가 담긴 이메일 메시지가 발송됩니다. **사용자 > 사용자** 페이지에서 사용자를 초대(또는 다시 초대)할 수도 있습니다.

**절차**

1. **사용자**를 선택하세요.
2. 초대할 사용자를 선택하세요.
3. **작업 > 초대 보내기**를 선택합니다. 기기 소유권을 **사용자소유** 또는 **회사 소유** 로 설정하는 옵션과 함께 초대 미리보기가 나타납니다.

4. 필요에 따라 **기기 소유자 설정**을 켭니다.
5. **사용자 소유** 또는 **회사 소유**를 클릭합니다. 이 설정은 등록 과정 중 기기의 분류 방식을 변경합니다. PIN만 또는 비밀번호 + PIN 등록 유형에만 해당됩니다. **기기 소유자 설정**이 꺼져 있으면 기기가 "설정되지 않음"으로 등록됩니다. 감독 대상 기기의 경우 기기 소유자 설정은 "회사 소유"입니다.
6. **보내기**를 클릭하세요. PIN 기반 기기 등록이 수행된 경우 사용자는 등록된 이메일 주소로 PIN을 받게 됩니다. QR 코드 기반 등록이 설정되면 사용자는 QR 코드를 받게 됩니다.
7. **확인**을 클릭합니다.

> 등록 확인 이메일 구성 및 사용에 제시된 설명대로 등록 확인 이메일 기능이 활성화되어 있을 경우, 등록이 완료되면 사용자가 등록 확인 이메일을 수신하게 된다는 알림도 표시됩니다. 사용자가 이메일을 수신하려면 사용자 등록 확인 이메일 구성하기의 사용자 설정에서 지정한 배포 목록에 포함되어야 합니다.

자세한 내용은 **LDAP 사용자 불러오기**를 참조하십시오.

# 6.7.7. 사용자 활성화 및 비활성화

이 섹션에는 다음 주제가 포함됩니다.

- 로컬 사용자 활성화 및 비활성화
- LDAP 사용자 활성화 및 비활성화

로컬 및 LDAP 사용자는 활성화 또는 비활성화 상태가 될 수 있습니다. 사용자 상태를 기반으로 사용자 활성화 조건을 사용하고 규칙 작성기에서 조건에 대한 작업을 설정함으로써 사용자 지정 정책을 생성할 수 있습니다. 예를 들어 비활성화된 로컬/LDAP 사용자에게 속하는 기기를 폐기하는 사용자 지정 정책이 있을 수 있습니다.

## 로컬 사용자 활성화 및 비활성화

기본적으로 로컬 사용자가 생성되면 활성화 상태가 됩니다.

**절차**

1. **사용자**를 선택하세요.
2. 원하는 사용자의 표시 이름을 클릭합니다.
3. **편집**을 클릭합니다. **인증 필요** 창이 표시됩니다.
4. 관리자 비밀번호를 입력하고 **인증**을 클릭합니다.

> 여러 번 잘못된 비밀번호를 입력하고 '비밀번호 복잡도 설정'에 설정된 '로그인 실패 임계값 제한'을 넘어갈 경우 계정이 잠기며 현재 세션에서 로그아웃됩니다.

5. **활성화** 옵션을 선택 또는 선택 해제하여 개별적으로 로컬 사용자를 활성화 또는 비활성화합니다.
6. **저장**을 클릭하세요.

## LDAP 사용자 활성화 및 비활성화

Microsoft Active Directory에 대한 LDAP 사용자만 활성화 또는 비활성화할 수 있습니다. Microsoft Active Directory에서 사용자 계정 속성을 열 때 **계정** 탭을 클릭한 다음, **계정** 옵션 대화 상자의 체크박스를 선택 또는 선택 해제하면 **UserAccountControl** 속성에 숫자로 된 값이 할당됩니다. Windows는 속성에 할당된 값을 통해 어떤 옵션이 활성화되었는지 구분합니다. UserAccountControl 속성에 값을 할당하고 나면 LDAP와 MDM용 Ivanti Neurons를 동기화한 후 사용자 상태가 반영됩니다.

다음 값을 할당할 수 있습니다.

- 512 - 활성화.
- 514 - 비활성화.
- 66048 - 활성화. 비밀번호가 만료되지 않음.
- 66050 - 비활성화. 비밀번호가 만료되지 않음.

### 사용자 계정 보기

**절차**

| | | |
|---|---|---|
| | 1. | **시작**을 클릭합니다. |

| | | |
|---|---|---|
| | 2. | 프로그램으로 이동합니다. |
| | 3. | 관리 도구로 이동합니다. |
| 4. | Active Directory 사용자 및 컴퓨터를 클릭합니다. | |

자세한 내용은 https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro를 참조하십시오.

Ldp.exe 도구 또는 Adsiedit.msc 스냅인을 이용해 속성을 보고 편집할 수 있습니다. 경험이 많은 관리자만이 이 도구를 사용하여 액티브 디렉토리를 편집해야 합니다. 두 도구 모두 기존 Windows 설치 미디어에서 지원 도구를 설치한 이후 이용할 수 있습니다.

# 6.7.8. 다중 관리자 로그인 관리

MDM용 Ivanti Neurons개의 여러 관리 포털 세션이 지원되므로 관리자는 포털의 서로 다른 페이지를 동시에 볼 수 있습니다. 관리자는 마지막 로그인 날짜를 확인해 다중 로그인을 기록을 살펴볼 수 있습니다.

## 마지막 관리자 로그인 보기

**절차**

1. **계정**을 클릭합니다.
2. **마지막 로그인:** 항목을 확인합니다.

# 6.7.9. 비밀번호 변경하기

이 섹션에는 다음 주제가 포함됩니다.


- 사용자 탭에서 비밀번호 변경
- 비밀번호가 만료되지 않도록 적용
- 비밀번호가 만료되지 않도록 하는 설정 제거


> 사용자에게 시스템 관리 역할이 있을 경우 슈퍼유저 또는 현재 로그인한 사용자에게만 **암호 변경** 옵션이 표시됩니다.

MDM용 Ivanti Neurons 비밀번호를 변경할 수 있습니다. 해당 권한이 있으면 다른 사용자의 비밀번호 변경도 가능합니다.

**절차**

1. 계정 아이콘(우측 상단)을 클릭하세요.
2. 
   풀다운 메뉴에서 **비밀번호 변경**을 선택합니다.
3. 현재 비밀번호를 입력하세요.
4. 변경할 비밀번호를 입력하세요.
5. 변경할 비밀번호를 다시 입력하세요.
6. 비밀번호가 만료되지 않도록 설정하려면 **비밀번호가 만료되지 않도록 설정**을 선택합니다.

> 비밀번호가 만료되지 않도록 설정하면 사용자 > 사용자 설정 > 비밀번호 복잡도 설정에서 정의된 **비밀번호 만료 기간**보다 우선적으로 적용됩니다.

7. **완료**를 클릭하세요.

> 로컬 계정 비밀번호가 만료되도록 재설정하려면 **비밀번호가 만료되지 않도록 설정**을 선택 해제합니다. 이 옵션을 선택 해제하고 나면 사용자에게 적용되었던 이전 비밀번호 만료 날짜가 팝업 창에 나타납니다.

## 사용자 탭에서 비밀번호 변경

**절차**

1. **사용자**를 선택하세요.
2. 원하는 사용자의 화면 표시 이름을 클릭하세요.
3. **편집**을 클릭합니다(좌측 상단). **인증 필요** 창이 열립니다. 관리자(로컬 사용자 또는 LDAP 사용자)는 사용자를 편집하기 전에 관리자 비밀번호를 입력하여 인증해야 합니다.
4. 관리자 비밀번호를 입력하고 **인증**을 클릭합니다.

> 여러 번 잘못된 비밀번호를 입력하고 '비밀번호 복잡도 설정'에 설정된 '로그인 실패 임계값 제한'을 넘어갈 경우 계정이 잠기며 현재 세션에서 로그아웃됩니다.

5. **현재 비밀번호** 필드에 현재 비밀번호를 입력하십시오.

> 이 필드는 다른 사용자에 대해 비밀번호를 변경하는 경우에는 표시되지 않습니다.

6. **비밀번호 변경** 필드에 새 비밀번호를 입력합니다.
7. 변경할 비밀번호를 확인하세요.
8. **저장**을 클릭합니다(좌측 상단).

## 비밀번호가 만료되지 않도록 적용

1. **사용자**를 선택하세요.
2. 한 명 이상의 사용자를 선택합니다.
3. **작업**을 선택하세요.
4. **만료되지 않는 비밀번호 할당**을 선택합니다. **로컬 계정 비밀번호가 만료되지 않도록 설정** 창이 표시됩니다.
5. **제출**을 클릭합니다.

## 비밀번호가 만료되지 않도록 하는 설정 제거

1. **사용자**를 선택하세요.
2. 한 명 이상의 사용자를 선택합니다.
3. **작업**을 선택하세요.
4. **만료되지 않는 비밀번호 삭제**를 선택합니다. **로컬 계정 비밀번호가 만료되지 않도록 하는 설정 제거** 창이 표시됩니다.
5. **제출**을 클릭합니다. 이 설정을 제거하고 나면 이전 비밀번호 만료 날짜가 사용자에게 적용됩니다.

# 6.7.10. 메시지 보내기

이 섹션에는 다음 주제가 포함됩니다.

- 사용자에게 메시지 전송
- 기기로 메시지 전송

알려진 사용자에게 메시지를 보낼 수 있습니다. 메시지에는 이메일 또는 {{푸시 알림}}이 있습니다. 푸시 알림은 등록된 장치 사용자만 수신할 수 있습니다.

**필수 조건**

- iOS 장치의 경우 Go 클라이언트가 설치되어 있는지 확인합니다.
- macOS 장치의 경우 Mobile@Work 클라이언트가 설치되어 있는지 확인합니다.

## 사용자에게 메시지 전송

1. **사용자 > 사용자**를 선택하세요
2. 메시지를 보낼 대상을 선택하세요.
3. **작업**(우측 상단)을 클릭하세요.
4. **메시지 보내기**를 클릭합니다.
5. 이메일을 보내고 싶지 않다면 **이메일 보내기** 체크박스의 선택을 해제합니다.
6. 이메일을 보내려면, 소유자과 내용을 입력하세요.
7. 푸시 알림을 보내려면 **푸시 알림 보내기**를 체크한 후 메시지 내용을 입력합니다.
8. **보내기**를 클릭하세요.

## 기기로 메시지 전송

1. **장치 > 장치**를 선택하세요.
2. 메시지를 보낼 장치를 선택하세요.
3. **작업**(우측 상단)을 클릭하세요.
4. **메시지 보내기**를 클릭합니다.
5. 필요에 따라 기기 이름 링크를 클릭해 기기 상세 정보 페이지로 이동하고 **메시지 전송**  아이콘을 클릭합니다.
6. 이메일을 보내고 싶지 않다면 **이메일 보내기** 체크박스의 선택을 해제합니다.
7. 이메일을 보내려면, 소유자과 내용을 입력하세요.
8. 푸시 알림을 보내려면 **푸시 알림 보내기**를 체크한 후 메시지 내용을 입력합니다.

> 푸시 알림 메시지에는 사용자가 액세스할 수 있는 URL이 포함될 수도 있습니다.

9. **보내기**를 클릭하세요.
   푸시 알림이 사용자에게 전송된 경우 사용자는 기기 화면 도구 모음에서 벨 아이콘을 볼 수 있습니다. 벨 아이콘을 누르면 사용자는 받은 알림 기록을 볼 수 있으며 작업을 수행하거나 알림을 삭제할 수 있습니다.

**기기** 및 **사용자** 페이지에서 관리자는 특정 기기 또는 사용자 속성을 메시지에 삽입할 수 있으며, 해당 메시지는 최종 사용자에게 전달되도록 대기열에 등록됩니다.

# 6.7.11. 사용자 그룹에서 사용자 삭제하기

이 섹션에는 다음 주제가 포함됩니다.

- 사용자 페이지에서 사용자 제거
- 사용자 그룹 페이지에서 사용자 제거

사용자 그룹에서 사용자 삭제 시

- 소속 그룹 일원으로서 해당 사용자에게 할당되었던 모든 역할이 삭제됨
- 해당 그룹에 할당된 앱은 더 이상 사용자의 {{App Catalog에서 이용할 수 없습니다.}}
- 제거 가능하도록 설정되었던 앱이 해당 사용자의 장치에서 제거됨

## 사용자 페이지에서 사용자 제거

1. 원하는 사용자를 선택하세요.
2. **작업**(우측 상단)을 클릭하세요.
3. **그룹에서 삭제**를 선택하십시오.
4. 해당 그룹을 선택하세요.
5. **삭제**를 클릭하세요.

## 사용자 그룹 페이지에서 사용자 제거

1. 원하는 사용자 그룹을 선택하면 해당 세부정보가 표시됩니다.
2. **수정**(우측 상단)을 클릭하세요.
3. 삭제할 사용자 옆의 **삭제** 링크를 클릭하세요.
4. **저장**(우측 상단)을 클릭하세요.

# 6.7.12. 사용자 삭제하기

이 섹션에는 다음 주제가 포함됩니다.

- 로컬 사용자 삭제 시
- LDAP 사용자의 경우

**절차**

1. **사용자 > 사용자**로 이동합니다.
2. 삭제할 사용자 항목을 선택하세요.
3. **작업**(우측 상단)을 클릭하세요.
4. **삭제**를 선택합니다.

MDM용 Ivanti Neurons 관리자 또는 파트너 관리자가 파트너 관리자 삭제를 시도하면 MDM용 Ivanti Neurons은(는) 파트너 관리자가 서비스 공급자 포털에서 이 작업을 수행해야 함을 알리는 메시지를 표시합니다.

> 사용자의 계정과 연결된 장치가 있는 경우 먼저 장치 사용을 중지하고 삭제한 다음 사용자를 삭제해야 합니다. 사용자에게 장치가 없는 경우, 사용자 삭제 시 사용자 정보도 삭제될 수 있습니다.

## 로컬 사용자 삭제 시

- 삭제된 사용자 관련 정보가 모두 시스템에서 삭제됩니다.
- 해당 사용자와 연동된 장치가 폐기됩니다.
- 해당 사용자가 업로드한 컨텐츠는 유지됩니다.
- 해당 사용자 계정으로 더 이상 장치 등록을 할 수 없습니다.

## LDAP 사용자의 경우

- LDAP 서버가 비활성 상태인 경우, LDAP 사용자의 영구 삭제가 불가능합니다. 삭제된 LDAP 사용자는 다음 LDAP 데이터 동기화 때 복구됩니다.
- LDAP 서버 또는 그룹이 삭제되면, 해당 LDAP 사용자는 로컬 사용자로 전환되며 삭제가 가능해집니다.
- 사용자는 LDAP에서 삭제되어도 클라우드에서 삭제되지 않습니다. 동기화 상태는 "NO_SYNC"로 전환되지만, 사용자는 제거되지 않습니다.

# 6.7.13. 사용자 내보내기

관리자는 MDM용 Ivanti Neurons에서 사용자 목록을 내보낼 수 있습니다.

> 사용자 기기 등록 PIN을 CSV 파일로 내보내면 보안을 위해 실제 PIN 대신 ''와 같이 마스킹 처리됩니다.

**절차**

1. **사용자 > 사용자**를 선택하세요
2. 목록에서 하나 이상의 사용자를 선택하십시오
3. **CSV로 내보내기**를 클릭합니다.

보고서 내보내기를 처리하는 데 다소 시간이 소요된다는 내용의 팝업이 표시됩니다. 요청을 제출한 이후 관리자는 요청이 완료될 때까지 기다린 후 다른 요청을 제출해야 합니다. 보고서가 준비되면 생성된 보고서를 다운로드하거나 삭제하라는 메시지가 표시됩니다. 또한 관리자는 보고서 다운로드 링크가 포함된 이메일을 수신하게 됩니다.

> 다른 세부 정보와 함께 **사용자 지정 사용자** 및 **LDAP** 속성 세부 정보도 CSV 파일로 내보낼 수 있습니다.

> 사용자가 필드 값에 +,-,=, @ 문자를 추가하면 내보낸 CSV 파일의 사용자 데이터 필드 앞에 자동으로 작은따옴표(')가 붙고 수직선(|) 기호가 백슬래시(\)와 함께 추가됩니다. 이것은 Excel 삽입 취약성을 예방하기 위함입니다.

# 6.7.14. 사용자에게 사용자 지정 속성 할당

부서와 같은 사용자 지정 속성을 한 명 이상의 사용자에게 할당할 수 있습니다. 각 속성에는 구성 및 사용자 그룹 생성과 같이 작업에 사용할 수 있는 값이 있습니다. 사용자 지정 속성을 한 명 이상의 사용자에게 할당할 수 있습니다.

**절차**

1. **관리자 > 시스템 > 속성**으로 이동하여 새 사용자 지정 속성을 생성합니다(필요한 경우).
2. **사용자**를 선택하세요.
3. 한 명 이상의 사용자를 선택합니다.
4. **작업**을 선택하세요.
5. **사용자 지정 속성 할당**을 선택합니다.
6. 다음 옵션 중 하나를 선택합니다.
    - 기존 값을 발견한 경우에도 모든 속성을 강제 할당(덮어쓰기)합니다.
    - 값이 비어 있는 경우에만 덮어쓰기를 진행하며 기존 값이 있는 속성은 건너뜁니다.

할당하려는 속성을 선택하고 값을 입력합니다(빈 값은 허용되지 않음).

8. **할당**을 클릭합니다.

**관련 주제:**

- 속성
- 변수

# 6.7.15. 사용자에게서 사용자 지정 속성 제거

한 명 이상의 사용자에게서 사용자 지정 속성을 제거할 수 있습니다.

> 이 작업은 되돌릴 수 없으니 주의해서 진행하십시오.

**절차**

1. **사용자**를 선택하세요.
2. 한 명 이상의 사용자를 선택합니다.
3. **작업**을 선택하세요.
4. **사용자 지정 속성 제거**를 선택합니다.
5. 제거할 속성을 선택합니다.
6. **삭제**를 클릭하세요.

**관련 주제:**

- 속성
- 변수

# 6.7.16. 사용자 로캘 변경

기본적으로 사용자 로캘은 테넌트 로캘로 설정됩니다. 필요한 경우 한 사용자의 로캘을 변경할 수 있습니다.

**절차**

1. **사용자**를 선택하세요.
2. 원하는 사용자의 화면 표시 이름을 클릭하세요.
3. **편집**을 클릭합니다. **인증 필요** 창이 표시됩니다.
4. 관리자 비밀번호를 입력하고 **인증**을 클릭합니다.

> 여러 번 잘못된 비밀번호를 입력하고 '비밀번호 복잡도 설정'에 설정된 '로그인 실패 임계값 제한'을 넘어갈 경우 계정이 잠기며 현재 세션에서 로그아웃됩니다.

5. 로캘 필드 아래에서 **변경**을 클릭합니다.
6. **사용자 로캘 변경** 창에서 **사용자 로캘을 다음으로 변경:** 드롭다운 목록에서 필요한 로캘을 선택합니다.
7. **완료**를 클릭하세요.
8. **저장**을 클릭하세요.

# 6.7.17. 사용자 이름 편집

사용자를 등록할 때, 이메일 주소를 입력하면 해당 주소가 자동으로 사용자 이름에도 표시됩니다. 자동으로 입력된 사용자 이름 값은 다음 이유로 수정하지 않는 것이 좋습니다.

- 이메일 주소 형식의 사용자 이름을 사용해야 합니다.
- {{구성}}의 사용자 변수를 사용하는 것이 편리하지만 이메일 주소를 사용해도 됩니다.

사용자 이름 수정이 필요할 때는 동일한 사용자 이름이 이미 사용되고 있는 경우뿐입니다. 전체 기기 관리 시스템 내에서 중복되는 사용자 이름은 사용할 수 없습니다. 예를 들어, 한 조직 내 두 부서에서 동시에 장치 관리 시스템에 등록할 경우 충돌이 발생할 수 있기 때문입니다.

## 중복 사용자 이름으로 충돌 발생 시

사용자 이름 중복으로 인해 사용자를 등록할 수 없는 경우에는 이메일 주소 형식의 사용자 이름을 입력하시기 바랍니다. 실제 사용하는 이메일 계정이 아닌 이메일 주소를 입력해도 됩니다. 예를 들어 다음 이메일 주소를 변경할 수 있습니다.

ksmith@mycompany.com을

-

이메일 주소를 변경해 입력할 수 있습니다.

사용자 이름을 변경하면 해당 사용자 이름이 변수로 사용된 설정은 모두 해당 사용자에게 적용되지 않게 됩니다. 이럴 경우에는 이메일 주소 변수를 사용해 대체 설정값을 생성하시기 바랍니다.

# 6.7.18. 위치 데이터 수집 기능 해제하기

이 섹션에는 다음 주제가 포함됩니다.


- iOS 기기의 경우
- Android 기기의 경우


개인 정보 구성에서 위치 데이터 수집 활성화가 적용된 경우 기기 사용자가 구성을 재정의할 수 있습니다.

## iOS 기기의 경우

iOS 기기 사용자가 장치 관리 시스템으로의 위치 데이터 전송을 막으려면 다음 설정에서 위치 서비스를 끄면 됩니다.

**설정 > 개인정보 설정 > 위치 서비스**

## Android 기기의 경우

Android 기기 사용자가 위치 데이터 수집을 막으려면 위치 설정을 끄면 됩니다. 이 설정 위치는 제조사별로 다릅니다. Android 기기 사용자에게도 위치 데이터 수집에 대한 동의 요청 메지시가 표시됩니다.

# 6.7.19. 시간제한 정보

관리 포털의 비활동 시간제한은 5~60분이며 제한 시간은 24시간입니다.

**절차**

1. **사용자 > 사용자 설정**으로 이동합니다.
2. 기본 **비밀번호 복잡도** 설정을 편집합니다.
3. 비밀번호 정책 섹션에서 **비활성 시간 제한** 슬라이더를 움직여 관리자 포털 또는 셀프 서비스 포털 세션 시간 전에 사용자가 비활성 상태를 유지할 수 있는 시간을 지정합니다. 숫자 범위는 5~60(분)입니다.
4. **완료**를 클릭하세요.

# 6.7.20. 시스템 사용량 분석 기능 해제

제품 개선에 도움이 되도록 익명 제품 진단 및 사용 데이터가 수집됩니다.

사용 현황 데이터를 회사 소유로 계속 유지하고 싶은 경우 시스템 사용 현황 분석 전송 선택을 취소하면 됩니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털에서 페이지 하단에 있는 **사용 현황 데이터** 링크를 클릭합니다.**사용량 데이터** 창이 표시됩니다.
2. **진단 및 사용 현황 데이터 전송** 확인란을 지웁니다.
3. **저장**을 클릭하세요.

# 6.7.21. PIN 생성을 통한 기기 등록

이 섹션에는 다음 주제가 포함됩니다.


- 사용자 랜딩 페이지의 단일 또는 여러 사용자인 경우
- 사용자 세부 정보의 단일 사용자인 경우


초대 이메일을 보내지 않고도 사용자를 위한 기기 등록 PIN을 생성하여 기기 등록 프로세스를 간소화할 수 있습니다.

## 사용자 랜딩 페이지의 단일 또는 여러 사용자인 경우

1. **사용자** > **사용자**로 이동합니다.
2. 등록 PIN을 생성하려는 사용자를 선택합니다. 한 명 또는 여러 명의 사용자를 선택할 수 있습니다.
3. **작업** 버튼을 클릭합니다.
4. 드롭다운 메뉴에서 **PIN 생성**을 선택합니다.
5. 생성된 PIN은 **등록 핀** 열에 표시됩니다.
6. PIN을 보려면 **PIN 보기**를 클릭합니다.

## 사용자 세부 정보의 단일 사용자인 경우

1. **사용자** > **사용자**로 이동합니다.
2. 등록 PIN을 생성하려는 사용자 이름을 클릭하여 사용자 세부 정보를 엽니다.
3. 사용자 정보 섹션에서 **PIN 생성**을 클릭합니다.
4. **PIN 보기**를 클릭하여 생성된 PIN을 확인합니다.

> 사용자를 위한 등록 PIN을 생성할 수 있는 적절한 권한이 있는지 확인합니다. PIN 생성 옵션은 기기 등록 상태가 '비밀번호 및 PIN'인 사용자에 대해서만 활성화됩니다.

# 7. 기기

이 섹션에는 다음 주제가 포함됩니다.

- 기기 시작하기
- 기기 그룹
- 앱 인벤토리
- 기기 관리하기

# 7.1. 기기 시작하기

이 섹션에는 다음 주제가 포함됩니다.

- 기기 관리하기
- 기기에서 작업 수행
- 기기 표준 시간대 설정
- 기준별로 기기 나열
- 기기 세부 정보 표시
- 기기에 사용자 및 사용자 지정 속성 대량 할당/변경기기에 사용자 및 사용자 지정 속성 대량 할당/변경
- CSV 파일로 기기 내보내기
- 기기 로그 검색

**기기** 페이지의 각 항목은 MDM용 Ivanti Neurons에 등록된 모바일 기기를 나타내며 해당 기기에 대한 중요 정보를 나열합니다. 기기 목록 페이지에는 다음과 같은 정보가 있는 기기가 표시됩니다.

- 이름
- 이메일 주소
- 전화 번호
- OS
- 기기 유형
- 상태
- 마지막 체크인
- 위반 개수
- 공간
- 법적 소유자(공유 iPad)

Wi-Fi IP 주소가 MDM용 Ivanti Neurons 서버에 보고됩니다. IP 주소 변경 사항은 체크인할 때마다 보고됩니다. 기기 목록 페이지 및 기기 상세 정보 페이지에서 GDPR을 준수하는 IP 주소를 옵션으로 사용할 수 있습니다. 이 기능을 사용하려면 MDM용 Ivanti Neurons에서 지원하는 iOS용 Go 5.5 이상 버전 및 Android용 Go 72 이상 버전을 통해 기기를 등록해야 합니다.

> 새 GDPR 필드(예: IP 주소 및 eSIM ID)가 MDM용 Ivanti Neurons 릴리스에서 추가되면 GDPR을 이미 구성한 관리자는 새 필드를 숨기려는 경우 GDPR 프로필을 편집해야 합니다.

장비 식별자(EID)는 기기 목록을 스프레드시트(CSV) 형식으로 내보낼 때 iOS 속성으로 나타납니다. EID 및 모바일 EID(MEID)(있는 경우)는 각각 EID 스트링 또는 MEID 스트링이 앞에 붙습니다.

> MDM용 Ivanti Neurons 서버는 클라이언트 식별자가 다르고 여러 테넌트에 등록된 기기를 처리할 수 없습니다. 다른 클라이언트 식별자를 가지며 한 테넌트에 등록된 같은 기기의 인스턴스만 처리할 수 있습니다.

## 기기 관리하기

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **기기**로 이동합니다.
3. 원하는 장치를 1개 이상 선택하세요.
4. **작업** 드롭다운 목록에서 작업을 선택합니다.

다음 표에는 기기 페이지에서 사용 가능한 작업이 나열됩니다.

| 범주 | 작업 |
| --- | --- |
| 공통 | • 그룹에 추가<br>• AppConnect 잠금 해제 ><br>• 사용자 지정 속성 할당<br>• 사용자에게 할당<br>• 기기 규정 준수 상태 동기화<br>• 원격 데스크톱 비활성화<br>• 원격 데스크톱 활성화<br>• Bluetooth 활성화/비활성화<br>• 강제 체크인<br>• 잠금<br>• 사용자 지정 속성 제거<br>• 다시 시작/종료<br>• 기기 규정 준수 상태 동기화<br>• 기기 폐기<br>• 메시지 보내기<br>• 소유권 설정<br>• 잠금 해제<br>• 지우기 |
| iOS<br><br><br><br>macOS<br><br><br><br>안드로이드<br><br><br>Windows | • 법적 소유자에게 할당(공유 iPad만)<br>• iOS 시스템 앱 재설치<br>• 표준 시간대 설정<br><br>• macOS 자동 관리자 비밀번호 설정<br>• 펌웨어 비밀번호 설정/변경<br>• 복구 잠금 설정/변경<br><br>• 키오스크 모드 입력<br>• Kiosk 모드 나가기<br><br>Ivanti Bridge를 통한 스크립트 및 작업 |

## 기기에서 작업 수행

작업 메뉴(생략 부호 버튼)을 사용하면 선택한 기기에서 다양한 작업을 수행할 수 있습니다.

**절차**

1. 기기 이름을 클릭합니다. 기기 세부 정보 페이지가 열립니다.
2. 작업(생략 부호) 메뉴를 클릭하여 다음 기기 작업 중 하나를 수행합니다.
    - 기기 이름 변경
    - 기기 삭제
    - 그룹 구성원 편집
    - Bluetooth 활성화/비활성화
    - Ivanti Bridge를 통한 스크립트 및 작업
    - Ivanti Bridge 로그 끌기
    - 소유권 넘기기
    - 디버그 로그 요청
    - 기기 다시 시작/종료
    - 폐기
    - 소유권 설정
    - 복구 잠금 설정/변경
    - 지우기
    - 기기 규정 준수 상태 동기화

## 기기 표준 시간대 설정

**적용 대상:** iOS 14.0+ 및 tvOS 14.0+ 기기

이 작업에는 위치 서비스가 필요하지 않습니다. 표준 시간대 기기 작업은 기기 상세 정보 페이지에도 표시됩니다. 기기에서 이루어진 표준 시간대 변경 사항은 MDM용 Ivanti Neurons 서버에도 적용됩니다.

> iOS 제한 구성에서 **자동 날짜 및 시간 강제** 제한이 활성화되면 이 기기 작업은 오류를 트리거합니다.

**절차**

1. 원하는 장치를 1개 이상 선택하세요.
2. 선택한 기기에 대해 **작업** > **표준 시간대 설정**을 클릭합니다.
3. 표준 시간대 문자열을 Olson 표준 시간대 ID 형식으로 입력합니다. Pacific/ Midway를 예로 들 수 있습니다.
4. **표준 시간대 설정**을 클릭합니다.

## 기준별로 기기 나열

필터 측면 탐색 모음을 사용하여 전체 기기 목록에서 특정 기기를 검색하고 확인할 수 있습니다. 공간 드롭다운 목록을 사용하여 공간 전체 또는 일부를 선택하여 기기와 관련된 정보를 확인합니다. 디스플레이 버전 또는 번들 버전을 사용하여 기기를 검색할 수도 있습니다. 기기 페이지에 기기의 번들 버전과 디스플레이 버전이 모두 표시됩니다.

기기 그룹 페이지에서 이동하여 **앱 인벤토리** 페이지의 **기기 수** 열 또는 **#설치됨** 열 아래에 나열된 수를 클릭하면 기기가 나열된 공간의 이름을 나타내는 메시지가 해당 페이지에 표시됩니다.

## 기기 세부 정보 표시

각 항목의 이름 열에 위치한 링크를 클릭하면 기기 상세 정보 페이지가 표시됩니다. 기기 상세 정보 페이지에는 다음 정보를 구성하는 여러 탭이 포함되어 있습니다.

- **개요** - 다음 표에는 개요 탭에 표시되는 모든 세부정보가 나열되어 있습니다.
- **구성** - 적용되는 {{구성}}의 세부 정보를 표시합니다. 자세한 내용은 구성 작업을 참조하십시오.

| 섹션 이름 | 설명 |
| --- | --- |
| 일반 | • 기기 위치<br>• 제조업체<br>• Wi-Fi MAC 주소<br>• Wi-Fi IP 주소(Android 기기)<br>• 네트워크 테더링 - (iOS 기기)<br>• 배터리 있음 - (macOS 13.3 이상에만 해당)<br>• IP 주소<br>• 공용 IP 주소 - Android 또는 ChromeOS에 대한 장치의 IP 주소를 표시합니다. 장치가 VPN 또는 프록시 서버에 연결되면 프록시 WAN IP 주소가 표시됩니다.<br>• 모델 번호 - (macOS 13.3+, iOS 16.4+)<br>• 일련 번호<br>• 대체 일련 번호(Android 기기) - 기기 관리자 또는 기기 소유자 모드에서 Samsung 기기에 해당되는 제조업체의 특정 일련 번호<br>• PIN 잠금 - 관리자는 관리되는 기기를 원격으로 잠그고 수동 잠금 해제를 위해 고유 PIN을 생성할 수 있습니다. 관리자 권한이 있는 사용자의 경우 **기기 상세 정보** 페이지에 PIN을 표시하려면 **보기**를 선택합니다. macOS 기기에만 적용 가능합니다.<br>• 스토리지 사용 - 기기의 내부 스토리지에서 사용됨(Windows 제외) 및 사용 가능<br>• 사용 가능한 배터리(Android)<br>• 배터리 상태(Android) - 충전, 방전, 완전 충전, 충전 안 됨<br>• 남은 예상 배터리 충전량(Windows)<br>• 예상 배터리 런타임(Windows)<br>• 업데이트 이용 가능(macOS)<br>• 이용 가능한 업데이트 이름(macOS)<br>• OS 버전<br>• OS 빌드 버전<br>• 추가 빌드 버전<br>• 추가 OS/버전 기타<br>• Apple 실리콘 기기<br>• 펌웨어 버전<br>• 기기 소스<br>• 법적 소유자<br>• 다중 사용자 모드<br>• 표준 시간대<br>• 마지막으로 알려진 기기 잠금 해제 비밀번호<br>• 보안 잠금 모드<br>• 시스템 업데이트(Android 기기) |

| 섹션 이름 | 설명 |
| --- | --- |
| | • Zebra 패치 버전(Android 기기)<br>• 마지막 핫픽스 ID - (Windows 기기)<br>• 설치된 마지막 핫픽스 ID - (Windows 기기)<br>• MDM 등록 유형<br>• MDM 서비스 복귀(iOS 27.0+ 및 visionOS 27.0+) |
| **판독값 사이의 설정** | • 기기 이름<br>• 기기 식별자<br>• 기기 GUID<br>• 기기 등록 기기(Apple 기기)<br>• 기기 등록 등록됨(Apple 기기)<br>• 자동화된 기기 등록 활성화됨<br>• 자동화된 기기 등록 등록됨<br>• 사용자 등록 등록됨(Apple 기기)<br>• 관리되는 Apple ID 등록됨(Apple 기기)<br>• 기기 그룹<br>• 언어<br>• MDM 기기 식별자<br>• 기기 클라이언트 ID<br>• 클라이언트 앱 버전<br>• 클라이언트 앱 번들 ID<br>• 클라이언트 등록됨<br>• EAS 기기 식별자<br>• 활성화 잠금 활성화됨<br>• Apple 선언적 관리 활성화됨<br>• Apple DDM 앱 활성화됨<br>• 활성화 잠금 우회 코드<br>• 서비스 조건<br>• 소유권<br>• iTunes 계정 활성화<br>• 기기 로케이션 서비스 활성화됨<br>• 격리됨<br>• Sentry 차단됨<br>• 액세스 차단됨<br>• 정책 준수 활동 차단됨<br>• APNS 가능 |

| 섹션 이름 | 설명 |
| --- | --- |
| | • 감독 모드(iOS 및 macOS 기기) - 감독되는 기기를 식별합니다. 기기는 계속해서 IT 팀에 의해 직접 제어됩니다. 감독 모드는 추가 기기 성능(예: 현장 서비스 배포, 소매 POS(Point Of Sale) 기기), 숙박 및 서비스에 사용되는 "대체품" 기기, 교실 실험실에서 학생들 간에 공유되는 기기를 사용 설정합니다.<br>• 지우기 PIN - PIN을 표시하려면 **보기**를 클릭합니다.<br>• 관리되는 macOS 관리 사용자(macOS 기기)<br>• 로컬 macOS 관리자 비밀번호(macOS 기기) - **보기**를 선택하고 자동화된 기기 등록을 통해 등록된 기기 및 관리형 기기에 대해 **관리 비밀번호**, **마지막 비밀번호 회전 시점**, **다음 회전**, **이유** 정보를 확인할 수 있습니다.<br>관리자가 비밀번호를 확인한 후, 표시된 **다음 회전** 시간에 따라 비밀번호가 회전하기까지 최대 1시간(다음 체크인 시점)이 추가로 소요될 수 있습니다.<br>• 기기 암호화 상태(macOS 기기)<br>  ◦ FileVault 암호화 활성화됨<br>  ◦ 개인 복구 키가 사용됨<br>  ◦ 기관 복구 키가 사용됨<br>• 부트스트랩 토큰 사용 가능<br>• 시스템 무결성 보호 활성화됨<br>• 펌웨어 비밀번호<br>  ◦ 비밀번호<br>  ◦ 변경 보류 중<br>  ◦ 명령 상태<br>  ◦ 옵션 ROM 허용<br>• 복구 잠금<br>  ◦ 비밀번호<br>  ◦ 복구 잠금 활성화됨<br>• macOS용 Mobile@Work를 통해 스크립트 적용<br>• 방화벽 설정(macOS 기기)<br>  ◦ 방화벽 활성화됨<br>  ◦ 모든 수신 차단<br>  ◦ 은폐 모드<br>• 애플리케이션 방화벽 상태(macOS 기기)<br>• 방화벽 상태(Windows 장치)<br>• iCloud 마지막 백업(iOS 기기)<br>• 암호 잠금 유예 기간(iOS 기기)<br>• Android ID<br>• Android 보안 패치 수준(Android 기기)<br>• 키오스크 모드(Android 기기)<br>• Android SafetyNet 인증 유형(Android 기기) |

| 섹션 이름 | 설명 |
| --- | --- |
| | • Android 엔터프라이즈 실행 가능(Android 기기)<br>• Android 작업 지원(Android 기기)<br>• Samsung SAFE 실행 가능(Android 기기)<br>• Android 업무 관리 기기(기기 소유자)가 활성화됨<br>• 회사 소유 기기의 Android 작업 프로필이 활성화됨<br>• 피싱 방지 기본 상태<br>• 피싱 방지 상태<br>• 피싱 방지 VPN 상태<br>• 작업 프로필이 있는 Android 관리 기기<br>• 회사 소유 기기의 Android 작업 프로필이 잠금 활성화됨<br>• Help@Work 사용 가능<br>• Zebra 지원<br>• Secure Apps 상태<br>• Secure Apps 암호화 상태<br>• 보안 앱 암호화 모드<br>• FCM 활성화됨<br>• MTD 활성화 상태 |
| **Windows 정보 보호 (Windows 기기)** | • WIP<br>• 앱 락커 구성됨<br>• EDP 필수 설정 |
| **전화 통신** | **장치 서비스 구독**<br>• 전화 번호<br>• 휴대폰 기술<br>• IMSI<br>• ICCID<br>• IMEI<br>• IMEI 2(듀얼 SIM 포트가 있는 Android 기기에만 해당. Android 8.0 이상에 적용)<br>• MEID<br>• 기기 위치<br>• 통신사<br>• 홈 MCC<br>• 홈 MNC<br>• 현재 국가 이름<br>• 주요 국가 이름<br>• 휴대폰 기술 |

| 섹션 이름 | 설명 |
| --- | --- |
| | • 로밍<br>• 현재 연산자<br>• 현재 MCC<br>• 현재 MNC<br>• 데이터 로밍<br>• 음성 로밍<br>• EID - (지원되는 Android 기기에 적용 가능)<br>**SIM 서비스 구독** - (지원되는 iOS 기기에 적용 가능)<br>지원되는 iOS 기기의 경우 여러 eSIM 활성 서비스 구독에 대해 이 속성이 표시됩니다.<br>• 통신사 설정 버전<br>• 통신사 설정 네트워크<br>• 현재 MCC<br>• 현재 MNC<br>• EID<br>• ICCID<br>• IMEI<br>• 데이터 우선<br>• 음성 우선<br>• 레이블<br>• 라벨 ID<br>• 전화번호<br>• SIM 슬롯<br>• 로밍 중<br>• 가입자 통신사 네트워크<br>**SIM 서비스 구독** - (지원되는 Android 기기에 적용 가능)<br>지원되는 Android 기기의 경우 여러 활성 서비스 구독에 대해 이러한 속성이 표시됩니다.<br>• 통신사 설정 버전<br>• 현재 MCC<br>• 현재 MNC<br>• ICCID<br>• 데이터 우선<br>• 음성 우선<br>• 구독 ID<br>• 전화번호<br>• SIM 슬롯<br>• 임베디드됨 |

| 섹션 이름 | 설명 |
| --- | --- |
| | • 관리됨 |
| **Azure 기기 컴플라이언스** | • Azure 기기 식별자<br>• Azure 기기 컴플라이언스 상태<br>• Azure 클라이언트 상태 코드<br>• Azure 기기 컴플라이언스 보고서 시간<br>• Azure Intune 기기 사용자 UPN |
| **Google BeyondCorp 장치 규정 준수** | • 기기 식별자<br>• 규정 준수 상태<br>• 규정 준수 보고 시간<br>• 사용자 |
| **배터리 정보** | • 배터리 수준 - Android OS에서 보고하는 현재 배터리 충전 수준을 표시합니다<br>• 배터리 상태 - Android, Mac, iOS, iPad 기기에서 보고하는 상태를 표시합니다.<br>• 배터리 충전 상태 - Android OS에서 보고하는 상태를 표시합니다<br>• 배터리 성능 백분율(OEM별) - Zebra 기기와 같이 지원되는 기기 제조업체의 배터리 성능을 백분율로 표시합니다<br>• 배터리 제조일자(OEM) - Zebra 기기와 같이 지원되는 기기 제조업체의 배터리 제조일자를 표시합니다<br>• 배터리 충전 주기(OEM) - Zebra 기기와 같이 지원되는 기기 제조업체의 완료된 총 주기 수를 표시합니다 |
| **기기 구성요소 상태**(iOS 27.0+ 및 macOS 27.0+ 감독 모드 기기에 적용) | • **베이스밴드**: 기기의 베이스밴드 상태를 나타냅니다.<br>• **카메라**: 기기의 카메라 상태를 나타냅니다.<br>• **디스플레이**: 기기의 디스플레이 상태를 나타냅니다.<br>• **Face ID**: 기기의 Face ID 상태를 나타냅니다.<br>• **근거리**: 기기의 근거리 무선 통신(NFC) 상태를 나타냅니다.<br>• **Touch ID**: 기기의 Touch ID 상태를 나타냅니다.<br>• **초광대역**: 기기의 초광대역 상태를 나타냅니다. |

- **설치된 앱** - 기기에 설치된 애플리케이션의 세부정보를 표시합니다. 설치된 앱의 현재 버전 설치 날짜는 **앱 보고 날짜** 열 아래에 표시됩니다. 다음과 같이 기기에 설치된 앱을 검색합니다.
- 앱 이름
- 번들/패키지 ID

> 격리가 해제된 기기의 앱 설치 날짜는 기기가 격리에서 제거된 날짜입니다.

> Android 엔터프라이즈 기기의 경우 일, 주, 월 또는 연도별로 정렬된 설치된 앱 사용 세부정보를 볼 수도 있습니다. 이 세부정보를 보려면 **구성 설정** 섹션에서 사용 가능한 **앱 사용 데이터 수집 활성화** 옵션을 선택한 후 **앱 사용 - 일**, **앱 사용 - 주**, **앱 사용 - 월**, **앱 사용 - 년** 옵션을 선택하여 앱 사용 세부정보를 볼 수 있습니다.

- **사용 가능한 앱** - 장치에 사용 가능한 애플리케이션의 세부 정보를 표시합니다. 다음과 같이 장치에서 사용 가능한 앱을 검색합니다.
- 앱 이름
- 번들/패키지 ID

**앱 구성** 열에서 **구성 이름**을 선택하면 앱 카탈로그의 **앱 구성** 탭으로 이동하여 앱 구성 옵션을 검토할 수 있습니다.필요한 경우 **앱 구성 요약** 페이지에서 장치의 앱 구성을 수정할 수 있습니다. 앱 구성에 대한 자세한 내용은 앱 구성을 참조하세요.

**앱 구성** 열에서 **구성 이름**을 선택하면 앱 카탈로그의 **앱 구성** 탭으로 이동하여 앱 구성 옵션을 검토할 수 있습니다. 필요한 경우 **앱 구성 요약** 페이지에서 장치의 앱 구성을 수정할 수 있습니다. 앱 구성에 대한 자세한 내용은 앱 구성을 참조하세요.

> **앱 구성** 페이지에서 할당된 장치에 대한 특정 앱 구성의 이름과 유형을 기억하세요.

> **상태** 열은 장치의 애플리케이션 설치 상태를 나타냅니다. 앱 설치 상태는 관리되는 애플리케이션에 대해서만 캡처됩니다. 관리되지 않는 앱의 애플리케이션 설치 상태는 설치되지 않음으로 표시됩니다. 올바른 설치 상태를 보려면 애플리케이션을 관리형으로 변환해야 합니다.

- **AppConnect 앱** - 설치된 AppConnect 앱의 세부정보입니다.
- **정책** - 적용된 {{정책}}의 세부정보입니다. 손상된 기기의 경우 위반 열에서 위반 이유를 점검합니다. 기기가 루팅된 경우 시스템은 **위반** 열에 제시된 이유를 표시합니다.

| 우선순위(1 = 가장 높음) | 위반 |
|---|---|
| 1 | 플러그인 손상됨 |
| 2 | 클라이언트 변경됨 |
| 3 | 알 수 없는 기기 제조업체: 알 수 없음 |
| 4 | 의심되는 폴더 감지됨: [경로] |
| 5 | 의심되는 바이너리가 다음에서 발견됨: [경로] |
| 6 | /data 폴더를 검색할 수 있거나 /data/data 폴더 검색 가능 |
| 7 | /system/app/Superuser.apk 발견됨 |
| 8 | 패키지 관리자 손상됨 |
| 9 | 의심되는 앱 발견됨: [패키지] |

- **인증서** - 설치된 인증서 상세 정보.
  인증서를 사용하려면 사용 유형 열을 확인합니다. 기기 인증서인 경우 사용 유형이 '기기'로 표시됩니다. 사용자 인증서인 경우 사용 유형이 '사용자'로 표시됩니다.
- **Sentry** - Sentry 정보(ActiveSync 연결)
- **속성** - 사용자 지정 속성 및 기기 속성
- **사용자** – 관리 상태의 macOS 기기에 대해 활성 사용자 목록을 표시합니다.

**사용자** 탭이 개선되고 관리형 Apple ID를 하이퍼링크로 표시합니다. 이 링크를 클릭하면 공유 iPad 기기의 사용자 계정 세부 정보 페이지로 리디렉션됩니다.

- **로그** - 장치 필터를 보고 사용자 지정합니다. 필터에서 다음을 수행할 수 있습니다.
  - 애플리케이션 작업을 기반으로 장치를 필터링하려면 작업 이름을 선택합니다.
  - 상태를 선택합니다.
  - 시작 날짜와 종료 날짜를 지정합니다,
- **하드웨어** – 하드웨어 인벤토리 상세 정보(시스템, 마더보드, BIOS, 하드 드라이브, CD ROM, 프로세서 및 실제 메모리)

## 기기에 사용자 및 사용자 지정 속성 대량 할당/변경

업로드를 통한 대량 할당 아이콘을 사용하여 CSV 파일을 업로드한 다음, 기기에 사용자 및/또는 사용자 지정 속성을 대량으로 할당하거나 변경할 수 있습니다.

**절차**

1. 기기 페이지에서 **업로드를 통한 대량 할당** 아이콘(작업 버튼 옆)을 클릭합니다.
2. **다운로드 템플릿**을 클릭하여 편집과 업로드가 가능한 CSV 템플릿 파일을 저장합니다(선택 사항).
3. CSV 파일이 준비되면 **파일 선택**을 클릭하여 CSV 파일 위치를 찾거나 CSV 파일을 파일 데이터 섹션에 끌어다 놓습니다.
4. 다음 옵션 중 하나를 선택합니다.
   - **기존 값을 발견한 경우에도 모든 속성 강제 할당(덮어쓰기)**
   - **값이 비어 있는 경우에만 덮어쓰기를 진행하며 기존 값이 있는 속성은 건너뛰기**

**업로드**를 클릭하세요.

## CSV 파일로 기기 내보내기

**기기** 페이지의 **CSV로 내보내기** 옵션을 사용하여 특정 기기의 기기 세부 정보를 내보낼 수 있습니다.

**절차**

1. **기기**로 이동합니다.
2. 특정 공간과 관련된 정보를 확인하려면 모든 공간을 선택하거나 다수의 공간을 선택합니다.
3. 기기 수 링크를 클릭합니다. 선택한 공간과 관련된 기기 목록 페이지가 표시됩니다.
4. **CSV로 내보내기** 옵션을 클릭하여 기기 목록과 관련 세부 정보를 CSV 파일로 내보냅니다. 보고서 내보내기에 일정 시간이 소요된다는 팝업 메시지가 표시됩니다. 요청이 완료되기를 기다린 후 다른 요청을 제출합니다. 보고서가 준비되면 보고서를 다운로드하거나 삭제하라는 메시지가 표시됩니다.
5. **다운로드**를 클릭합니다. 또한 관리자는 보고서 다운로드 링크가 포함된 이메일을 수신하게 됩니다.
6. (선택 사항) 보고서를 삭제하려면 **삭제**를 클릭합니다.

## 기기 로그 검색

**절차**

1. **기기** > **기기**로 이동하여 항목의 **이름** 열 링크를 클릭합니다.
2. **로그** 탭을 클릭합니다.

3. 작업, 상태, 시작 날짜, 종료 날짜 필터를 사용하여 표시되는 장치의 범위를 좁힙니다. 필터에서 다음을 수행할 수 있습니다.
    1. 애플리케이션 작업을 기반으로 장치를 필터링하려면 작업 이름을 선택합니다.
    2. 상태를 선택합니다.
    3. 시작 날짜와 종료 날짜를 지정합니다,
4. 기기 세부 정보 열에는 다음과 같이 애플리케이션의 상태가 표시됩니다.
   모든 기기에 대해 상태는 다음 세부 정보를 표시합니다.
    - 앱 이름, 앱 버전, 번들 또는 패키지 ID
    - 설치 상태
    - 오류 및 오류 이유
      예 - appOrConfigName=Name:<app name>;Identifier=<bundleid>;iTunesStoreId:<itunesid>;Status:<status or error reason from Apple>version: <app version>

Windows 기기의 경우 상태에 다음 세부 정보가 표시됩니다.

- 번들 ID 또는 패키지 ID, 상태 및 오류 포함
  예 -
- 유형의 경우 - 애플리케이션 인벤토리 및 상태 - 승인 - 표시 - appType
- 유형의 경우 - 애플리케이션 인벤토리 및 상태 - 전송 중 - 아무것도 표시하지 않음
- 유형의 경우 - 설치/제거 및 상태 - 성공/실패/전송 - 번들 ID 또는 패키지 ID, 상태, 이름, 버전 및 오류 포함 표시

**기기** 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 기기 관리
- 장치 읽기 전용

# 7.2. 기기 그룹

이 섹션에는 다음 주제가 포함됩니다.

- 기기 그룹 추가
- 기기 그룹 제거
- CSV 파일로 기기 내보내기
- 기기 그룹에 사용자 정의 속성 할당

**기기 그룹** 페이지에서 동일한 방식으로 처리하려는 기기 목록을 만들 수 있습니다. 정책과 구성을 정의하여 기기 그룹에 할당할 수 있습니다. 다음은 MDM용 Ivanti Neurons에서 생성된 기본 기기 그룹입니다.

- 모든 기기
- Android 기기
- Android Enterprise 기기
- iOS 기기
- 디바이스 유형(Apple)
- tvOS 기기
- macOS 기기
- visionOS 기기
- watchOS 장치
- Windows 기기

특정 기기 그룹에 할당된 앱의 상세 정보는 특정 기기 그룹의 **앱** 탭 아래에 표시됩니다.

## 기기 그룹 추가

> 기기 그룹 추가는 동적 사용자 그룹에는 적용되지 않습니다.

보유한 라이선스 유형에 따라 규칙 기반의 새 기기 그룹을 추가하여 특정 기준으로 기기를 식별할 수 있습니다. 규칙 작성기 섹션 밑에 규칙과 일치하는 기기가 표시됩니다. 규칙은 ANY(OR) 또는 ALL(AND) 옵션을 사용하여 중첩될 수 있습니다. 규칙은 다음 연산자를 이용해 구성할 수 있습니다.

- 다음으로 시작
- 끝
- 포함
- 포함되지 않음
- 다음으로 시작하지 않음
- 다음으로 끝나지 않음
- 보다 작음
- 보다 큼
- 범위에 있음
- 같음

- 같지 않음
- 공백이 아님
- 공백임

MDM용 Ivanti Neurons 관리자는 규칙 작성기에서 사용자 그룹 이름 속성을 선택할 때 중복 그룹을 식별할 수 있도록 중복 사용자 그룹 수 및 해당 GUID 수를 표시합니다. 또한 이 규칙 아래에 있는 표에는 중복 사용자 그룹 목록과 사용자 그룹 이름, GUID, 소스, 배포된 이름(DN)과 같은 세부 정보가 표시됩니다.

**Bronze 라이센스:**

다음과 같은 기준으로 규칙을 통해 기기를 확인합니다.

- 기기 유형
- OS - 운영 체제(자동 입력)
- OS 버전
- 버전이 있는 OS
- 사용자 그룹

**Silver 라이센스:**

다음과 같은 기준으로 규칙을 통해 기기를 확인합니다.

- Entra ID 등록됨
- 대체 일련 번호(Android 전용 - 기기 관리자 또는 기기 소유자 모드에서 Samsung 기기에 해당됨)
- Android 전용 기기
- Android 엔터프라이즈 지원
- 작업 프로필이 있는 Android 관리 기기
- Android SafetyNet 인증 유형
- Android Work 활성화됨
- Android 보안 패치 수준(Android 기기)
- Android 업무 관리 기기(기기 소유자)가 활성화됨
- Android 작업 프로필 활성화됨
- 회사 소유 기기의 Android 작업 프로필이 활성화됨
- 피싱 방지 기본 상태
- 피싱 방지 상태
- 피싱 방지 VPN 상태
- APNS 가능
- Apple 실리콘 기기
- 자동화된 기기 등록 활성화됨
- 자동화된 기기 등록 등록됨
- Azure 기기 식별자
- Azure 기기 컴플라이언스 상태
- Azure 클라이언트 상태 코드

- Azure 기기 컴플라이언스 보고서 시간
- 베이스밴드 상태
- BitLocker 암호화
- Sentry 차단됨
- 액세스 차단됨
- 부트스트랩 토큰 사용 가능
- 대량 제공 유형(Apple Configurator 또는 없음)
- 통신사
- 카메라 상태
- 클라이언트 마지막 체크인
- 등록된 클라이언트
- 컴플라이언스
- 정책 준수 활동 차단됨
- 현재 국가 이름(드롭다운 목록에서 현재 국가 이름 선택)
- 현재 MCC
- 현재 MNC
- 사용자 지정 기기 속성
- 사용자 지정 LDAP 속성
- 사용자 지정 사용자 속성
- 데이터 로밍
- 기기 이름
- 기기 등록됨
- 기기 소스
- 기기 유형
- 표시 이름
- 디스플레이 상태
- 암호화 활성화됨
- Face ID 상태
- 하드 드라이브 파티션
- 홈 국가 이름(드롭다운 목록에서 홈 국가 이름 선택)
- 홈 MCC
- 홈 MNC
- IMEI
- IMEI2(듀얼 SIM 포트가 있는 Android 장치에만 해당되고 Android 8.0 이상 장치에 적용 가능)
- 기관 복구 키 활성화됨
- IP 주소
- Kiosk 모드

- 마지막 체크인
- MAM 전용
- 제조업체
- MDM 등록 유형
- MDM 서비스 복귀(iOS 27.0+ 및 visionOS 27.0+)
- 다중 사용자 모드(iOS 27.0+)
- MTD 활성화 상태
- NFC 상태
- OS
- OS 빌드 버전
- OS 버전
- OS 버전
- 버전이 있는 OS
- 소유권
- 전화 번호
- 공개 IP 주소(Android 또는 ChromeOS 장치)
- 개인 복구 키 활성화됨
- 격리됨
- 복구 잠금 활성화됨
- 로밍
- Secure Apps 상태
- 보안 잠금 모드
- 일련 번호
- 상태
- 감독됨
- 시스템 버전
- 총 기기 용량
- 총 메모리(MB)
- TPM 버전
- Touch ID 상태
- 토큰 잠금 해제 사용 가능(iOS)
- 사용자 등록 활성화됨
- 사용자 그룹`
- 초광대역 무선 상태
- 음성 로밍
- macOS 개인 복구 키 에스크로됨
- macOS 복구 키 유형

**절차**

1. **추가**를 클릭합니다.
2. 그룹 이름을 입력합니다.
3. 그룹에 대한 설명을 입력합니다(선택 사항).
4. 생성할 기기 그룹의 유형을 선택합니다.
   - **동적으로 관리됨**: 규칙을 이용하여 해당 그룹에 어떤 기기를 넣을지 지정하십시오.
     - **고급 검색에서 불러오기**: 저장된 검색 라이브러리를 열려면 이 옵션을 선택합니다. 쿼리를 선택하면 선택한 검색을 기반으로 기기 그룹 이름과 규칙 기준이 자동으로 입력됩니다.

     > **기기** > **기기** > **고급 검색**으로 이동하여 이러한 쿼리를 작성하고 저장할 수 있습니다. 해당 위치에 저장된 모든 쿼리는 여기에서 자동으로 불러올 수 있습니다.

   **수동으로 관리됨**: 해당 그룹에 포함시킬 기기의 각 사용자를 입력하십시오.
5. 동적으로 관리되는 그룹:
   1. 해당 그룹을 정의할 규칙을 생성하세요.
   2. **예**: OS는 iOS
      필요할 경우 **+**를 클릭하여 추가 규칙을 생성할 수 있습니다.
   3. **예**: 기기는 iPhone 5S
      기기가 하나 이상의 규칙을 충족해야 할 경우에는 **일부**를 클릭합니다.
   4. 기기가 모든 규칙을 충족해야 할 경우에는 **모두**를 클릭합니다.
6. 수동으로 관리되는 그룹:
   1. 추가할 기기의 사용자 이름을 입력하세요.
   2. 표시된 목록에서 기기를 선택합니다.
   3. 모든 기기가 목록에 표시될 때까지 a와 b 단계를 반복합니다.

**저장**을 클릭하세요.

## 기기 그룹 제거

**절차**

1. **기기** > **기기 그룹**으로 이동합니다.
2. 제거할 기기 그룹의 체크박스를 클릭합니다.
3. **기기 그룹 삭제**를 클릭합니다.

## CSV 파일로 기기 내보내기

**기기 그룹** 페이지의 **CSV로 내보내기** 옵션을 사용하여 특정 기기 그룹의 기기 세부 정보를 내보낼 수 있습니다.

**절차**

1. **기기** > **기기 그룹**으로 이동합니다.
2. 특정 공간과 관련된 정보를 확인하려면 모든 공간을 선택하거나 다수의 공간을 선택합니다.
3. 기기 그룹 수 링크를 클릭합니다. 선택한 공간과 관련된 기기 목록 페이지가 표시됩니다.

4. **CSV로 내보내기** 옵션을 클릭하여 기기 목록과 관련 세부 정보를 CSV 파일로 내보냅니다. 보고서 내보내기에 일정 시간이 소요된다는 팝업 메시지가 표시됩니다. 요청이 완료되기를 기다린 후 다른 요청을 제출합니다.
5. **다운로드**를 클릭합니다. 그러면 보고서 다운로드 링크가 포함된 이메일을 수신하게 됩니다.
6. (선택 사항) 보고서를 삭제하려면 **삭제**를 클릭합니다.

**기기 그룹** 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.

- 기기 관리
- 장치 읽기 전용

## 기기 그룹에 사용자 정의 속성 할당

이제 관리자는 기기 그룹에 사용자 정의 속성을 직접 할당할 수 있습니다. 기기 그룹의 구성원이 되는 모든 기기는 구성된 사용자 정의 속성 값을 자동으로 상속하므로 등록 후 개별 기기에 속성을 수동으로 할당할 필요가 없습니다. 기기 그룹을 사용하여 그룹의 구성원이 되는 기기에 사용자 정의 속성 값을 자동으로 할당합니다.

**절차**

1. **기기** > **기기 그룹**으로 이동합니다.
2. 기존 그룹을 선택하거나 새 그룹을 생성합니다.
3. 기기 그룹 상세 정보 페이지에서 **속성**을 클릭합니다.
4. **새로 추가**를 클릭합니다.
5. 사용자 정의 속성을 선택하고 필요한 값을 지정합니다.

# 7.3. 비관리 기기

이 섹션에는 다음 주제가 포함됩니다.

- 기기 차단
- 기기 차단 해제
- 기기 목록에서 기기 삭제

**라이센스**: Silver

Sentry 이메일 접근 관리 설정이 된 후 해당 이메일 시스템에 접속하는 모든 미등록 기기를 비관리 기기라고 합니다. **Sentry 설정**시 비관리 기기의 이메일 접속을 기본으로 허용할지 여부를 설정합니다. 그런 다음 해당 기기의 이메일 접속을 수동으로 허용 또는 차단할 수 있습니다.

> 비관리 기기 페이지는 5분마다 업데이트됩니다. 따라서 관리 설정을 변경해도 바로 반영되지 않습니다.

## 기기 차단

**절차**

1. 원하는 장치를 선택하세요.
2. **작업 > 차단**을 선택하세요.

해당 기기는 **작업 > 허용** 또는 **작업 > 삭제**가 선택되기 전까지 차단 상태가 유지됩니다.

## 기기 차단 해제

**절차**

1. 원하는 장치를 선택하세요.
2. **작업 > 허용**을 선택하세요.

해당 기기는 **작업 > 차단** 또는 **작업 > 삭제**가 선택되기 전까지 이메일 접속이 가능합니다.

## 기기 목록에서 기기 삭제

**절차**

1. 원하는 장치를 선택하세요.
2. **작업 > 삭제**를 선택합니다.

해당 기기는 다음 번 이메일 시스템 접속 시도 시 이 목록에 다시 나타납니다. 따라서 목록에 나타날 때마다 해당 기기에 기존 적용되었던 차단 또는 허용 동작을 반복해서 수행해야 합니다.

# 7.4. 앱 인벤토리

이 섹션에는 다음 주제가 포함됩니다.


- 앱 디스플레이 필터링
- 특정 앱용으로 설치된 기기 표시
- 앱 목록 표시
- 장치에 설치된 Win32 또는 Win32 스토어 앱 표시
- 사용자 지정 보기 권한 생성
- 앱 인벤토리 내보내기


앱 인벤토리는 등록 기기에서 검색되는 앱의 목록입니다. 관리자는 이 페이지를 이용해 등록된 기기에서 사용 중인 앱의 정보를 가져올 수 있습니다. 다음과 같은 질문에 답변할 수 있습니다.

- 가장 인기 있는 앱은 무엇인가요?
- iOS 기기의 앱은 App Store에서 직접 제공되나요?
- {{인하우스 앱}}(선택 사항)을 다운로드한 Android 사용자가 몇 명입니까?
- 이전 버전 앱이 사용되고 있는 장치는 몇 대인가요?

## 앱 디스플레이 필터링

**기기 > 앱 인벤토리** 페이지에서 전체 앱 목록을 확인할 수 있습니다. 필터 기능 (좌측 작업창)을 이용해 특정 앱만 화면에 표시할 수 있습니다. 예를 들어 Google Play에서 비공개 앱만 표시하도록 목록 범위를 좁히려면 **소스** 섹션에서 **비공개**를 선택합니다.

드롭다운 목록에서 여러 공간을 선택하여 모든 또는 여러 공간 기기 전반의 앱 인벤토리를 볼 수 있습니다. 표시되는 앱 위에 마우스를 놓으면 기기 개수가 나타납니다. 앱에 대한 개수를 클릭하면 앱이 들어 있는 모든 기기가 나타납니다. 각 앱 인벤토리 기록은 공간별로 묶입니다.

앱 이름이나 번들/패키지 ID로 검색할 수 있습니다.

여러 공간을 선택한 경우 **설치된 개수** 열의 **총계** 값 위에 마우스를 놓으면 장치 공간당 설치 수가 표시됩니다.

## 특정 앱용으로 설치된 기기 표시

**관리**, **비관리**, 또는 **총** 숫자를 **설치된 수** 열 목록에서 클릭하세요.

## 앱 목록 표시

앱을 요청한 기기를 보려면 앱 인벤토리에서 앱에 대해 **# 요청됨**을 클릭합니다. 이는 MAM 전용 기기에만 적용됩니다.

## 장치에 설치된 Win32 또는 Win32 스토어 앱 표시

장치의 개인정보보호 구성에서 해당 장치의 모든 앱 정보를 수집할 수 있는 경우 앱 인벤토리에 Win32 또는 Win32 스토어 앱이 표시됩니다. 귀하는 기기의 개인 정보 정책을 구성할 수 있습니다.

**절차**

1. 원하는 기기에 적용할 개인정보 보호 설정을 기기의 지침에 따라 결정합니다.
2. **구성**으로 이동합니다.
3. 개인정보 보호 설정의 경우 1단계 참고:

1. 원하는 구성을 선택하세요.
2. 편집을 클릭하세요.
3. **앱 인벤토리 수집**에서 **기기의 모든 앱**을 선택합니다.
4. **완료**를 클릭하세요.

> Win32AppInventory CSP는 장치에서 인벤토리 검색이 실행된 후 24시간마다 장치에 설치된 모든 Win32 및 Win32 스토어 앱 목록을 반환합니다.

## 사용자 지정 보기 권한 생성

귀하는 사용자의 사용자 지정 보기 권한을 지정할 수 있습니다.

**절차**

1. **관리**로 이동합니다.
2. **역할 관리**로 이동합니다.
3. **사용자 지정 역할 추가**를 클릭합니다.
4. **공간별 역할** 옵션을 선택합니다.
5. **이름** 필드에 사용자 이름을 입력합니다.
6. **기기** 메뉴에서 **앱 인벤토리**를 클릭합니다.
7. **보기** 체크박스를 선택합니다.
8. **기기** 메뉴에서 **기기 작업**을 클릭합니다.
9. **저장**을 클릭하세요.
10. 메인 메뉴에서 **사용자**로 이동합니다.
11. 생성한 새 사용자를 클릭합니다.
12. **역할 할당**을 클릭합니다.
13. **앱 | 공간별** 체크박스를 선택하고 **다음**을 클릭합니다.
14. **요약** 페이지에는 생성한 역할에 할당되는 권한이 표시됩니다.
15. **완료**를 클릭하세요.
16. 새 사용자로 로그인합니다.
17. 메인 메뉴에서 **기기**를 클릭합니다.
18. **앱 인벤토리**를 클릭합니다.
19. **앱 인벤토리** 페이지에는 이제 사용자에 대해 허용된 애플리케이션만 표시됩니다.

## 앱 인벤토리 내보내기

관리자는 **CSV로 내보내기** 옵션을 사용하여 앱 인벤토리 보고서를 요청할 수 있습니다.

**절차**

1. **장치 > 앱 인벤토리**로 이동합니다.
2. 목록에서 인벤토리를 선택합니다.
3. **CSV로 내보내기**를 클릭합니다.

4. 다음 옵션 중 하나를 선택합니다.

- **앱을 CSV로 내보내기**는 앱 인벤토리의 모든 애플리케이션을 내보냅니다.
- **장치를 CSV로 내보내기**는 다음 표에 따라 특정 애플리케이션을 내보냅니다.

| 옵션 | 설명 |
| --- | --- |
| 번들 ID | 애플리케이션의 번들/패키지 ID를 입력하세요. |
| 내보내시겠습니까? | 다음 옵션 중 하나를 선택합니다.<br>• 총 설치 수<br>• 관리형<br>• 비관리<br>• 요청됨(MAM 전용 장치) |

5. **내보내기**를 클릭하세요.

관리자에게 보고서 내보내기를 처리하는 데 다소 시간이 소요된다는 내용의 팝업이 표시됩니다. 요청을 제출한 이후 관리자는 요청이 완료될 때까지 기다린 후 다른 요청을 제출해야 합니다. 보고서가 준비되면 관리자에게 생성된 보고서를 다운로드하거나 삭제하라는 메시지가 표시됩니다. 또한 관리자는 보고서 다운로드 링크가 포함된 이메일을 받게 됩니다.

**앱 인벤토리** 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 기기 관리
- 장치 읽기 전용

# 7.5. 기기 관리하기

이 섹션에는 다음 주제가 포함됩니다.


- Windows 기기 배포
- macOS 기기에서 Apple 원격 데스크톱 설정
- 기기 등록(iOS, macOS, Android)
- 기기 등록(Windows 10+ PC 및 Microsoft Hololens 2)
- PIN으로 패키지 등록 프로비저닝
- Windows 기기의 대량 등록 사용
- 암호 설정 변경하기
- 기기 이름 변경
- 기기 찾기 및 필터링
- 기기 소유자 이용하기
- 작업 프로필이 있는 관리되는 기기
- Android의 대량 등록 사용
- CSV 파일 업로드를 사용한 대량 등록
- Samsung Knox 모바일 등록 사용
- Oculus 기기 등록
- 기기에 Bluetooth 활성화
- iOS 업데이트 일정 설정
- iOS 시스템 앱 재설치
- 새로운 사용자에게 기기 할당하기
- Android 기기 재할당
- 기기의 강제 체크인
- 장치 위치 확인하기
- 장치 잠금 설정하기
- Apple 분실 모드에서 기기 관리하기
- 디버그 로그 요청
- 장치 폐기하기
- 장치 소유권 포기
- 장치 지우기
- 기기 삭제
- 장치 잠금 해제하기
- 기기 재시작/종료
- 제한 비밀번호 삭제(iOS만 해당)
- 기기에 대한 Sentry 연결 삭제
- 장치에 사용자 지정 속성 할당

- 장치에서 사용자 지정 속성 제거
- 앱 피드백 동기화 및 가져오기
- 펌웨어 비밀번호 설정
- 새 개인 복구 키 재발급하기
- 복구 잠금 설정 또는 변경
- Apple 액세스 관리
- 그룹 정책 등록

# 7.5.1. Apple 장치 배포

MDM용 Ivanti Neurons는 모든 Apple 장치의 관리를 지원합니다. 보유 중인 모든 장치를 프로비저닝, 관리, 업데이트 및 보호하는 포괄적인 솔루션으로 최종 사용자에게 최고의 사용 경험을 제공합니다.

이 섹션에는 다음 주제가 포함됩니다.

- Apple MDM 인증서 설치
- Apple 장치 등록
- iOS 클라이언트용 Ivanti Go
- Apple 장치용 애플리케이션 관리
- 구성 관리하기
- 소프트웨어 업데이트 관리
- iOS/iPadOS 장치 설정
- watchOS 장치 설정
- watchOS 장치에 지원되는 장치 작업
- visionOS 기기 설정
- visionOS 기기에 지원되는 기기 작업
- macOS 장치 설정
- TvOS 장치 설정
- 선언적 기기 관리(DDM) 지원

## Apple MDM 인증서 설치

Apple 장치를 관리하려면 먼저 iOS 장치 관리를 위한 Apple MDM 인증서를 요청하고 설치해야 합니다. Apple MDM 인증서를 1년에 한 번씩 갱신하세요. (인증서 생성에 사용된 Apple 계정은 만료 날짜가 가까워지면 Apple 사이트에서 알림을 받습니다.) MDM 인증서 페이지를 사용하여 이 인증서를 추가하거나 갱신합니다.

MDM 인증서 설치에서 설명하는 단계를 따르세요.

## Apple 장치 등록

다음 방법 중 하나를 선택하여 장치를 등록할 수 있습니다.

- 자동 장치 등록
- Apple School Manager
- Apple Configurator

## iOS 클라이언트용 Ivanti Go

다음 단계로 회사에서 장치에 허용하는 등록 유형을 선택합니다. MDM용 Ivanti Neuros는 현재 다음을 지원합니다.

- 기기 등록(iOS, macOS, Android)
- Apple Business Manager로 사용자 등록
- 계정 기반 사용자 등록

- 설정(Apple)

## Apple 장치용 애플리케이션 관리

MDM용 Ivanti Neurons의 앱 카탈로그 페이지는 관리자가 앱 카탈로그를 효율적으로 관리하는 인터페이스 역할을 합니다. 이 기능은 공용 앱 스토어와 MDM용 Ivanti Neurons를 통해 배포하도록 지정된 앱 스토어 모두에서 최종 사용자가 사용할 수 있는 모바일 앱의 조정을 포함합니다.

지원되는 앱:

앱 카탈로그 페이지에 공용 AppStore 앱, 맞춤형 앱, 자체 개발 앱, AppConnect 지원 앱, iOS용 GoClient, macOS용 M@W 등 다양한 유형의 앱이 모여 있어 후속 구성 및 배포를 위한 가져오기 프로세스가 간소화됩니다.

MAM(모바일 앱 관리) 전용 구성으로 작동하는 장치에서 iOS 사용자는 앱 카탈로그에 액세스할 때 인증서를 선택하라는 메시지가 표시됩니다. 이 인증 단계는 앱 목록에 대한 액세스를 보호하고 강력한 보안 기준을 준수하는 데 중요합니다.

> Apple의 M1 칩셋 MacBook은 [귀하의 소프트웨어 제품] 내에서 iPhone 및 iPad VPP 앱에 전문적인 지원을 제공합니다. 특히 지원되는 iPhone 및 iPad VPP 앱을 푸시할 수 있는 권한은 관리자만이 갖고 있어 사용자가 앱에서 직접 설치하지 못하게 제한합니다.

자세한 구현 지침 및 구성 옵션은 아래 관리 가이드 및 리소스에서 제공되는 종합 문서를 참조하십시오.

- 앱 관리
- 앱 카탈로그 설정
- Apple Apps 및 Books 설정
- Apps@Work 기업 앱 스토어
- macOS AppStore 제한 사항

## 구성 관리하기

구성은 관리자가 장치에 보내는 여러 설정 값의 모음입니다. 예를 들어, 구성을 이용해 자동으로 VPN 및 기기 암호 규격 관련 설정을 할 수 있습니다. 구성 페이지에 시스템의 기존 구성이 나열됩니다. 구성 페이지에서 구성을 여러 개 선택하고 한 번에 다수의 장치로 푸시할 수 있습니다. 공간별 장치로 이러한 구성을 푸시할 수 있으며, 대상 공간이 아닌 다른 공간에는 영향을 미치지 않습니다. 한 번에 하나의 공간이나 여러 공간, 모든 공간에 구성을 푸시할 수 있습니다.

MDM용 Ivanti Neurons의 대부분 구성은 모든 플랫폼에 공통됩니다. 구성 작업 방법에 대한 자세한 내용은 구성 작업을 참조하십시오.

일부 구성은 특정 플랫폼에서만 지원됩니다. 구성 유형에서 지원되는 플랫폼별 목록을 검토할 수 있음

## 소프트웨어 업데이트 관리

iOS 및 macOS 장치의 소프트웨어 업데이트 구성을 설정하여 시작할 수 있습니다.

> 소프트웨어 업데이트 예약 창을 설정할 때 업데이트가 해당 창을 놓치지 않도록 매시간 OS 업데이트 명령이 장치에 푸시됩니다. Apple 동작에 따라 장치에서 OS 업데이트 명령을 받을 때마다 팝업이 나타나 사용자에게 업그레이드를 알립니다. 최대 3번까지 연기할 수 있습니다. Apple 동작에 따라 세 번째에는 장치가 강제 업그레이드됩니다.

MacOS 장치에는 적용할 수 있는 몇 가지 특정 규칙이 있습니다. macOS 소프트웨어 업데이트 규칙 구성 보기

### iOS용 OS 업데이트 명령

장치 목록이나 장치 페이지에서 하나 이상의 장치를 업데이트하도록 일회성 명령을 보낼 수도 있습니다. OS 업데이트 명령 예약을 참조하십시오.

## iOS/iPadOS 장치 설정

iOS/iPadOS에 지원되는 구성:

- iOS/iPadOS 제한 사항
- eSIM 구성
  - 데이터 보존 계획
- 모바일 네트워크 구성
- 분실 모드 사용
- iOS MDM 프로필 구성
- 단일 앱 모드
  - 자치 단일 앱 모드
- 기업용 공유 iPad
- 교육 설정
- iOS 커스텀 구성
- 잠금 화면 메시지

## watchOS 장치 설정

이제 iOS 기기와 페어링하는 동안 Apple watchOS 기기를 Ivanti N-MDM에 등록할 수 있습니다.

이 기능은 현재 watchOS 10 이상을 지원합니다.

**Procedure절차**

1. iOS 17+ 관리 대상 장치를 등록해야 합니다.
2. Apple Watch 등록 구성을 iOS 장치에 할당합니다.
3. 이제 Apple Watch를 iPhone에 페어링할 수 있습니다.

> Watch 구성을 iPhone에 푸시한 후 Apple Watch를 페어링할 수 있습니다. 페어링 후 Watch 구성이 iPhone에 푸시되면 Apple Watch 원격 관리를 활성화할 수 없습니다.

watchOS 장치에 지원되는 구성:

- Cellular_Configuration
- 인증서 구성
- 인증서 투명성
- Identity_Certificate_Configuration
- iOS 제한
- Passcode_Settings
- Per-App_VPN_Configuration
- Wi-Fi_Configuration

## watchOS 장치에 지원되는 장치 작업

watchOS 장치에 지원되는 장치 작업:

- 비밀번호 지우기
- Apple Watch 잠금
- Apple Watch 초기화
- MDM용 Ivanti Neurons에서 Apple Watch 등록 취소

> 페어링된 iOS 기기 등록을 취소하면 Watch가 재설정되고 iOS 기기와의 페어링이 해제됩니다.

## macOS 장치 설정

macOS에 지원되는 구성:

- **macOS 제한**
- **macOS 장치 구성**
- **스크립트 및 Mobile@Work 클라이언트 작업**
- **macOS MDM 프로필 구성**
- **펌웨어 비밀번호 설정**
- **FileVault 활성화**
  - **FileVault 복구 키**
  - **FileVault 옵션 구성**
- **플랫폼 및 확장형 SSO**
- **활성 디렉토리 macOS**
- **방화벽**
- **이더넷**
- **Office 365 계정 생성**
- **macOS 시스템 확장**
- **미디어 디스크 굽기 제한 사항**
- **개인정보 보호 설정**

## TvOS 장치 설정

tvOS에 지원되는 구성:

- **Apple TV 설정**
- **Apple TV 제한 사항**
- **회의실 디스플레이**
- **AirPlay 미러링**

## visionOS 기기 설정

이제 Apple visionOS 기기를 MDM용 Ivanti Neurons에 등록할 수 있습니다.

이 기능은 현재 visionOS 1.1 이상을 지원합니다

다음 방법 중 하나를 사용하여 visionOS 장치를 등록할 수 있습니다.

- 계정 기반 장치 등록
- 계정 기반 사용자 등록
- 기기 등록

visionOS 기기에 지원되는 구성:

- CalDAV 설정
- CardDAV 설정
- 인증서 구성
- 인증서 해지 확인 구성
- 인증서 투명성
- DNS 프록시 구성 생성
- 암호화된 DNS
- 이메일 설정
- Exchange 구성
- Google 구성
- ID 인증서
- iOS 제한
- LDAP 설정
- 관리되는 도메인
- 네트워크 릴레이 구성
- 퍼앱 VPN 구성
- Single Sign-On 설정
- 구독한 달력 설정
- VPN 구성
- 웹 컨텐츠 필터
- Wi-Fi 구성

## visionOS 기기에 지원되는 기기 작업

visionOS 기기에 지원되는 기기 작업:

- Apple Vision Pro 지우기
- Apple Vision Pro 폐기
- Apple Vision Pro 잠금 해제

## 선언적 기기 관리(DDM) 지원

Apple의 선언적 기기 관리는 관리형 기기가 더 적은 통신으로 자체 관리 설정을 능동적이고 자율적으로 적용할 수 있도록 하는 최신 관리 프로토콜입니다. 선언적 기기 관리는 등록 중 새로 등록된 기기에, 또는 이미 등록된 기기의 체크인 중에 활성화됩니다.

선언적 기기 관리는 다음 적격 기기에서 자동으로 활성화됩니다.

- macOS 13 이상이 설치된 컴퓨터
- iOS 16 또는 iPadOS 16 이상이 설치된 기기
- 사용자 등록을 통해 등록된 기기는 iOS 또는 iPadOS 15 이상에서 선언적 기기 관리를 지원합니다.
- tvOS 16 이상이 설치된 Apple TV 기기
- watchOS 10 이상이 설치된 Apple Watch 기기
- visionOS 1.1 이상이 설치된 Apple Vision Pro 기기

현재 지원되는 선언적 관리 기능:

- **상태 채널**:
  - OS 버전 변경
  - 암호 규정 준수
  - 암호 유무
- **구성**:
  - 선언적 관리 구성

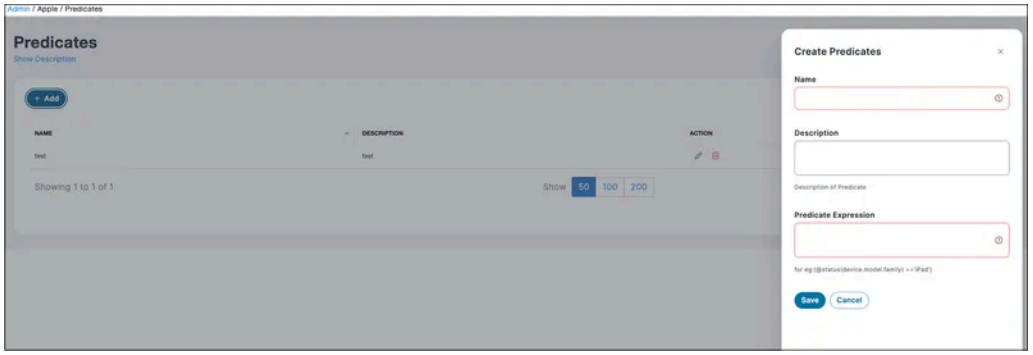
## DDM 구성의 조건자

조건자는 장치 구성 활성화에 유연성과 세분성을 제공할 수 있는 Cocoa 언어의 표현식입니다. 표현식은 장치에 상주하며 이 조건자의 조건이 충족될 때 적용됩니다. DDM 구성에 조건자를 생성, 저장, 적용할 수 있는 새로운 기능이 추가되었습니다.

DDM 구성에는 분포 페이지에 조건자를 적용하는 새 옵션이 표시됩니다. 이미 생성된 조건자는 이 섹션의 드롭다운 목록에서 찾을 수 있습니다.

조건자 생성

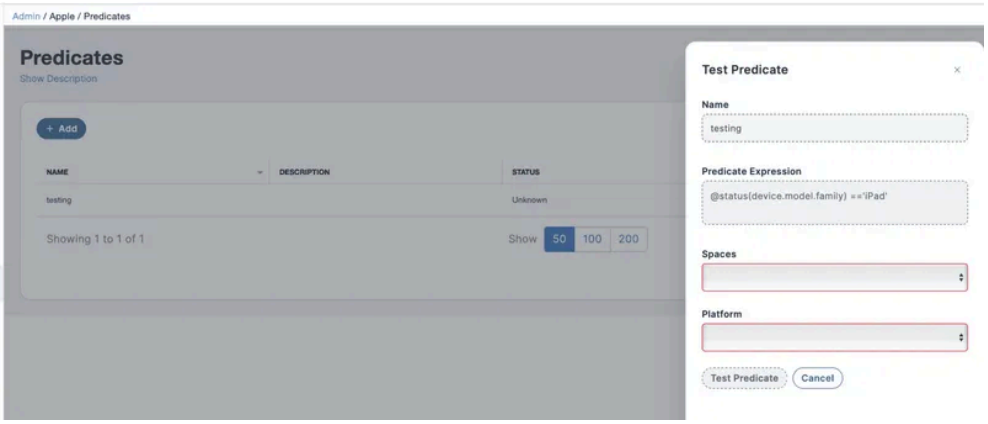
1. **관리자** > **Apple** > **조건자**로 이동합니다.
2. **추가**를 클릭합니다. 화면에 **조건자 생성** 창이 표시됩니다.
3. 다음 정보를 입력합니다.
   - **이름** – 조건자의 이름
   - **설명** – 관련 설명을 추가합니다.
   - **조건자 표현식** - 조건자 표현식입니다. 예: @status(device.model.family) =='iPad'




4. **저장**을 클릭합니다. 화면에 조건자 생성을 확인하는 대화 창이 나타납니다.
5. 페이지를 새로 고친 후 STATUS 필드에 표시되는 값(값: **알 수 없음**, **진행 중**, **유효함**, **유효하지 않음**)을 확인하여 조건자 구문이 올바른지 확인합니다.

1. **테스트**를 클릭합니다. 그러면 화면에 **테스트 조건자** 창이 표시됩니다.
2. 다음 정보를 입력합니다.
   - **이름** - 기본
   - **조건자 식** - 기본
   - **공간** - 기본 공간
   - **플랫폼** - iOS/macOS
   - **기기 이름** - 조건자 식과 관련된 기기 이름입니다.

     > 드롭다운 메뉴에서 **공간**과 **플랫폼** 필드 세부 정보를 선택한 이후에만 **플랫폼** 필드 아래에 **기기 이름** 필드가 표시됩니다.




3. **테스트 조건자**를 클릭합니다.
4. 화면에 테스트 조건자 시작을 확인하는 대화 창이 나타납니다.
5. 조건자 구문 상태를 찾으려면 페이지를 새로 고칩니다.
   - 조건자 식이 올바르면 상태가 **알 수 없음** > **진행 중** > **유효함**으로 변경됩니다.
   - 조건자 식이 올바르지 않으면 상태가 **알 수 없음** > **진행 중** > **유효하지 않음**으로 변경됩니다.
6. 다른 조건자 표현식을 사용하여 여러 개의 조건자를 생성하려면 이 절차를 반복합니다.

## DDM 구성을 위한 조건자 배포

1. DDM 지원 구성을 만듭니다.
2. 토글 스위치 "조건자를 사용한 활성화"를 ON으로 설정하고 + 버튼을 눌러 (필요에 따라) 조건자를 포함합니다.




조건자를 편집하거나 삭제하려면 **관리자** > **Apple** > **조건자**로 이동합니다. 이 페이지에서 사용 가능한 조건자 목록을 확인할 수 있습니다. **편집**을 클릭하여 기존 조건자를 변경하고 저장할 수 있습니다. 마찬가지로, 기존 조건자를 삭제하려면 조건자를 선택하고 **삭제**를 클릭합니다.

구성과 연관된 조건자는 삭제할 수 없습니다.

## DDM 구성에 대한 관리 속성

관리자는 다음을 사용하여 조건자를 만들 수 있습니다:

- 사용자 및 기기 변수
- 사용자 속성
- 기기 속성

조건자에서 관리 속성을 사용하는 예(사용자 정의 속성):

사용자의 이름이 'test'인지 확인하는 조건자 @property(userFirstName)=='test'

## 더 많은 예

- 기기의 하드웨어 제품군: (Mac, iPhone, iPad 등)
  @status(device.model.family) =='iPad'
  참인 경우, 기기에 암호가 있습니다. 거짓인 경우, 기기에 암호가 없습니다.
  @status(passcode.is-present)==true
- 기기에서 사용 중인 운영 체제 제품군(예: macOS 또는 iOS)
  @status(device.operating-system.family)=='iPadOS'
- 기기에서 사용 중인 운영 체제 버전(예: 15.0)
  @status(device.operating-system.version)=='18.2'
  @status(device.operating-system.version)<'18.3'
  @status(device.operating-system.version)>='18.2'
- 기기에서 File Vault 활성화 상태를 지정하는 부울 값
  @status(diskmanagement.filevault.enabled)==true
- 관리 속성(사용자 정의 속성)의 예:
  사용자의 이름이 'test'인지 확인하는 조건자
  @property(userFirstName)=='test'

# 7.5.2. Windows 기기 배포

이 섹션에는 다음 주제가 포함됩니다.


- 개요
- 기기 관리
- Windows 장치 등록
- Windows 업데이트 관리
- 앱 관리 및 배포
- 앱 컨트롤
- Windows 장치 관리 구성
- Windows 장치 규정 준수
- Windows 앱 및 하드웨어 인벤토리


## 개요

MDM용 Ivanti Neurons를 사용하면 구성, 등록, 프로비저닝, 보안, 애플리케이션, 관리, 모니터링, 소프트웨어, OS 업데이트, 폐기 등 HoloLens 2 엔드 투 엔드 기기 수명 주기 관리를 비롯하여 모든 Windows 노트북과 데스크톱을 관리할 수 있습니다.

## 기기 관리

지원되는 Windows 장치:

- Windows PC 10+
- Microsoft HoleLens 2

장치 관리 및 보고 기능에 대한 자세한 내용은 기기를 참조하십시오.

## Windows 장치 등록

MDM용 Ivanti Neurons 은(는) Windows 기기에 대해 모든 표준 기기 등록 방법을 지원합니다.

- 수동 등록
- 대량 등록
- SCCM 및 Ivanti EPM
- Windows Autopilot
- Entra ID 등록

등록 방법에 대한 자세한 내용은 **Microsoft Azure 사용하기**을 참조하십시오.

다중 사용자 지원에 대한 내용은 **Using_Microsoft_Azure.htm#Multi**을(를) 확인하십시오.

## Windows 업데이트 관리

- Windows 업데이트 구성 및 예약 - Windows 업데이트를 구성하고 예약하려면 구성 - **소프트웨어 업데이트**를 사용하여 구성을 만듭니다.
- Windows 업데이트 관리 - Windows 업데이트 관리를 사용하여 업데이트할 Windows 장치에서 보고된 업데이트를 확인하고 승인할 수 있습니다. 이 기능을 사용하면 필요하지 않거나 장치에서 설치 테스트가 완료되지 않은 업데이트를 방지할 수 있습니다. 자세한 내용은

Windows 업데이트 관리를 참조하십시오.

## 앱 관리 및 배포

사용자는 Windows 애플리케이션의 전체 앱 수명 주기(가져오기, 구성, 예약, 배포, 업데이트, 제거)를 관리할 수 있습니다.

지원되는 앱 유형:

- 인하우스
- MSB
- 공용 스토어

지원되는 앱 확장:

- MSI
- MSIX
- APPX
- APPX 번들
- EXE(Bridge)

Windows 앱 관리에 대한 자세한 내용은 앱 구성을 참조하십시오. 앱 업데이트를 자동화하려면 Windows 앱 일정 설정 및 구성 작업을 참조하십시오.

## 앱 컨트롤

앱 컨트롤 구성을 통해 앱을 기기 수준에서 허용 목록 또는 차단 목록으로 분류할 수 있습니다. 이미 설치된 앱은 표시되지 않으며 시작할 수 없습니다. 앱은 App Store에 계속 표시되지만 다운로드하거나 시작할 수 없습니다. 앱 컨트롤 구성이 배포된 모든 장치는 이 구성을 사용하며, 모든 허용된 앱 정책 설정을 무시합니다. 앱 컨트롤 구성은 대상 장치의 동일한 앱에 적용되는 모든 앱 관련 정책에 우선합니다.

자세한 내용은 앱 컨트롤 구성: 기기당 설치된 앱 컨트롤을 참조하십시오.

## Windows 장치 관리 구성

Windows 10+ PC 및 Microsoft HoloLens 2에 대한 지원에는 다음 기능이 포함됩니다.

- 기기 등록(Windows 10+ PC 및 Microsoft Hololens 2)
- 암호 구성
- Exchange 구성
- 구성
- 기기
- 앱
- Windows 앱 일정 설정
- 앱 컨트롤 구성: 기기당 설치된 앱 컨트롤
- Windows 업데이트 관리
- MDM용 Ivanti Neurons에서 Azure로 기기 상태 보고
- Windows Autopilot 프로필 구성
- 사용자 지정 구성을 사용하여 장치에 SyncML 푸시

- 정책
- Windows 제한
- ID 인증서
- Windows Hello For Business
- Wi-Fi 및 VPN 프로필

> 이 장치 유형에서 지원하지 않는 HoloLens 장치에 배포된 구성은 장치 세부 정보의 구성 탭에 배포된 구성으로 보고되지 않습니다.

Windows 기능(Windows PC에서만 지원):

- **Ivanti Bridge**
- **Windows BIOS 구성**
- **Windows BitLocker**
- **Windows 키오스크 구성**
- **Windows 라이선스 구성**
- **EMA 서버 통합 구성**
- 프린터 설정
- 블로트웨어 제거 구성
- **ADMX(GPO) 브라우저**

## Windows 장치 규정 준수

MDM용 Ivanti Neurons는 Windows 데스크톱 및 Windows 10+에서 실행되는 태블릿 기기 사용자가 원활하게 등록할 수 있도록 Microsoft Azure로 설정할 수 있습니다. Azure 테넌트 통합을 구성하여 Windows 장치 규정 준수를 활성화하려면 **Microsoft Azure 사용하기**을 참조하십시오.

## Windows 앱 및 하드웨어 인벤토리

### Windows 앱 인벤토리

앱 인벤토리는 등록 장치에서 검색되는 앱의 목록입니다. 이 페이지에서는 등록된 장치에서 사용 중인 앱 관련 정보를 확인할 수 있습니다. 자세한 내용은 앱 인벤토리를 참조하십시오.

> 장치의 개인정보보호 구성에서 해당 장치의 모든 앱 정보를 수집할 수 있는 경우 앱 인벤토리에 Win32 또는 Win32 스토어 앱이 표시됩니다.

### 앱 인벤토리 간격 구성

여러 앱 소스 유형 인벤토리의 Windows 10 앱 인벤토리 수집 간격을 설정할 수 있습니다. 개인 정보 보호 구성이 장치의 모든 앱을 수집하도록 설정된 경우 간격이 사용됩니다.

자세한 내용은 앱 인벤토리 간격 설정을 참조하십시오.

### Windows 하드웨어 인벤토리

Windows 10+ 장치에서 하드웨어 정보 수집을 활성화할 수 있습니다. 이러한 세부 정보는 Bridge를 사용하여 검색합니다. 자세한 내용은 하드웨어 인벤토리를 참조하십시오.

# 7.5.3. macOS 기기에서 Apple 원격 데스크톱 설정

이 섹션에는 다음 주제가 포함됩니다.


- macOS 기기에서 Apple 원격 데스크톱 활성화
- macOS 기기에서 Apple 원격 데스크톱 비활성화


## macOS 기기에서 Apple 원격 데스크톱 활성화

Apple 원격 데스크톱 기능을 통해 화면 공유 기능을 활성화하면 기기를 원격으로 관리할 수 있습니다. Apple 원격 데스크톱 기능은 감독 대상인 macOS 10.14.4+ 기기에서 사용할 수 있습니다.

**절차**

1. **기기**로 이동하여 감독 대상인 macOS 기기를 하나 이상 선택합니다.
2. 기기에 대한 **작업** > **원격 데스크톱 활성화** 작업을 클릭합니다.
3. **원격 데스크톱 활성화**를 클릭하여 확인합니다.

## macOS 기기에서 Apple 원격 데스크톱 비활성화

**절차**

1. **기기**로 이동하여 감독 대상인 macOS 기기를 하나 이상 선택합니다.
2. 기기에 대한 **작업** > **원격 데스크톱 비활성화** 작업을 클릭합니다. 화면 공유 기능을 비활성화하면 기기를 원격으로 관리할 수 없습니다.

# 7.5.4. 기기 등록(iOS, macOS, Android)

이 섹션에는 다음 주제가 포함됩니다.

- 관리 프로필의 수동 설치
- 초대장 전송(iOS, macOS, Android)
- 최종 사용자에게 앱 다운로드 안내(iOS 및 Android)

대부분의 사용자들은 장치 등록부터 시작합니다. 다음 중 원하는 방법을 이용해 등록 절차를 실행할 수 있습니다.

- 최종 사용자 1명 이상에게 초대장 발송(iReg 등록)
- 최종 사용자에게 Go을 다운로드하도록 안내(인앱 등록)

> iOS 및 macOS 기기 MDM 등록이 *프로필 설치 실패. SCEP 서버가 잘못된 응답을 반환했습니다* 오류와 함께 실패하는 경우, 기기 사용자는 기기 등록 프로세스를 처음부터 다시 시작해야 합니다. 이는 프로필이 기기에 다운로드된 후 기기 사용자가 iOS 및 macOS 기기 MDM 등록 프로세스를 완료하는 데 예상보다 시간이 오래 걸리는 경우 주로 발생합니다. 자세한 내용은 Ivanti 지원 팀에 문의하십시오.

MDM용 Ivanti Neurons 는 macOS 기기에서 단일 사용자(로컬 사용자 또는 등록된 Active Directory(AD) 사용자)의 사용자 수준 관리를 지원합니다. 관리자는 사용자를 위해 기기를 관리하고 기기 프로필 및 사용자 프로필을 적용할 수 있으므로, 결과적으로 App Store, 앱 배포, 구성 및 정책(Apps@Work, 제한, 보안 포함)을 사용할 수 있습니다.

AD 사용자가 포함된 macOS 기기를 관리하려면 AD 사용자가 등록 시 로그인한 사용자여야 합니다. 등록되지 않은 기타 사용자는 등록된 사용자의 프로필(예: ID 인증, VPN)을 볼 수 없습니다. 그러나 로그인한 사용자는 기기 수준 구성을 보고 사용할 수 있습니다.

> 기기 등록 프로세스를 시작하기 전에 최종 MDM용 Ivanti Neurons사용자에게 계정이 있어야 합니다. LDAP 사용자의 경우, Connector와 LDAP 서버 설정이 필요하며, 해당 사용자를 LDAP 서버에서 불러와야 합니다. 로컬 사용자의 경우, 사용자 추가가 필요합니다.

> MDM용 Ivanti Neurons 이전 버전에서 생성된 기기 등록 URL은 현재 버전과의 작동을 중단합니다. 관리자는 기기 등록을 위해 기기 등록 URL을 다시 생성해야 합니다.

## 관리 프로필의 수동 설치

**적용 가능 운영 체제:**

- iOS 12.2부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- macOS 11.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

### iOS 기기 등록

iOS 기기에 인앱 등록 시:

- Go app을(를) 사용하여 기기를 등록하는 동안 프로필 설치 지침이 있는 페이지가 나타납니다.
- **다운로드한 프로필 설치** 옵션을 클릭하고 **이해함** 클릭합니다.
- 다운로드된 프로필은 몇 분 동안 유효하며 그 후에는 다시 등록해야 합니다.

### macOS 기기 등록

셀프 서비스 포털에 macOS 기기를 등록하려면 사용자는 다음 절차를 수행해야 합니다.

**절차**

1. 해당하는 자격 증명으로 로그인합니다.
2. 관리 프로필 설치 페이지에서 프로필을 사용자의 로컬 시스템에 다운로드합니다.
3. 다운로드한 프로필을 두 번 클릭하여 사용자의 시스템 기본 설정에서 보이도록 설정합니다.

> 사용자가 무효가 되기 전에 프로필을 설치할 수 있는 시간 제한이 있습니다.

4. 시스템 기본 설정에서 **프로필**을 엽니다. 프로필이 기기에 다운로드되면 사용자는 프로필 링크가 있는 웹 페이지를 볼 수 있습니다. 설정 앱을 열려면 **프로필**을 클릭합니다.
5. **설치**를 클릭하여 관리 프로필을 설치합니다.
6. 설치 절차를 계속하여 마칩니다. 프롬프트가 나타나면 시스템 비밀번호를 입력합니다.

## 초대장 전송(iOS, macOS, Android)

초대장을 보내 등록 프로세스를 시작합니다. MDM용 Ivanti Neurons 에서 다음 방법으로 최종 사용자에게 기기 등록 초대장을 보낼 수 있습니다.

- 시작 마법사에서
- 1명 이상 사용자를 추가할 경우
- 사용자 페이지(작업 > 초대장 보내기)에서

> 최종 사용자가 초대장을 분실한 경우 초대장에 나열된 URL을 공유할 수 있습니다. URL 끝에 **/go**를 추가해야 합니다.

비밀번호가 설정된 MDM용 Ivanti Neurons 계정이 있는 최종 사용자는 등록 프로세스를 시작하는 데 초대장이 필요하지 않습니다. 해당 사용자들에게는 초대장에 제공되는 URL만 발송하면 됩니다.

## 최종 사용자에게 앱 다운로드 안내(iOS 및 Android)

Go 애플리케이션은 Android 및 iOS 기기에서 사용할 수 있습니다. 공개 앱 스토어에서 애플리케이션을 다운로드하고 앱에서 등록 프로세스를 시작하는 방법에 대한 지침을 최종 사용자에게 제공할 수 있습니다. 이메일 초대장에는 다음 정보가 포함되어 있습니다.

- 등록 페이지의 링크
- 1회용 PIN(관리자가 설정한 경우)
- 다음 단계에 대한 기본 지침

계정 비밀번호를 이미 설정했다면 최종 사용자의 기업 이메일 주소로 암호를 전송할 수 있습니다. 인증에 LDAP를 사용하는 경우에는 최종 사용자에게 네트워크 자격 증명이 필요하다는 점을 안내해야 합니다.

사용자가 등록 중 MDM 프로필 설치를 완료하지 않을 경우 MDM용 Ivanti Neurons에서 주기적으로 기기에 푸시 알림을 보내 등록 절차를 완료하라는 메시지를 표시합니다.

사용자는 사용자 이름과 비밀번호를 사용하거나 QR 코드를 스캔하여 Go app에서 기기 등록을 시작할 수 있습니다. 세부 정보는 다음과 같습니다.

- **사용자 이름**: 이메일 주소
- **비밀번호**: 사용자 설정에서 지정하고 관리자가 임시 비밀번호를 정의한 경우

- **QR 코드**: MDM용 Ivanti Neurons 셀프 서비스 포털에서 QR 코드를 생성합니다. **QR 코드 스캔** 옵션을 사용하여 QR 코드를 스캔할 경우에는 기기의 카메라 액세스 권한을 요청하는 메시지가 화면에 표시됩니다. 권한을 부여하고 나면 카메라가 QR 코드를 스캔하고 기기가 등록됩니다. 이 옵션은 Android 9 이상, iOS 14 이상 버전에서 지원됩니다.

최종 사용자의 경우, 모바일 기기에서 등록 이메일을 수신하면 링크를 탭하여 등록 프로세스를 시작합니다. 노트북이나 데스크톱에서 이메일을 수신하면 모바일 기기로 브라우저에 URL을 입력하여 등록 프로세스를 시작합니다.

MDM용 Ivanti Neurons 사용자 계정의 비밀번호가 정의되어 있지 않거나 사용자 설정에 등록 PIN이 필요한 경우 1회용 PIN이 포함됩니다. 이 PIN을 입력하고 나면 계정의 비밀번호가 없는 경우 사용자에게 비밀번호를 설정하라는 메시지가 표시됩니다.

> Android Enterprise 기기의 경우, 등록이 완료되면 회사 소유 기기나 업무 관리 기기의 작업 프로필에 수동으로 설치된 모든 CA 인증서가 삭제됩니다.

## iOS 기기 재등록

기기를 재등록하려면 다음과 같이 할 수 있습니다.

1. 기기에서 Go 클라이언트를 시작합니다.
2. **설정** > **문제 해결** > **기기 재등록**으로 이동합니다. 재등록 프로세스가 시작되고 확인을 위한 몇 가지 메시지가 표시됩니다.
3. 메시지에 **예**를 누릅니다.

> 프로필 설치 중 **취소**를 누르면 등록 과정이 중단되고 MDM용 Ivanti Neurons 서버가 기기 MDM을 비활성화합니다.

재등록 프로세스를 다시 시작하려면 이미 다운로드한 프로필을 다시 설치해야 합니다. 다운로드한 프로필은 Go 클라이언트에서 재등록을 수행해야 하는 몇 분 동안만 유효합니다.

**Android 기기 재등록**

관리자는 기존의 활성 항목을 수동으로 지우지 않고도 폐기, 지우기 또는 삭제 작업을 사용하여 기기를 다시 등록할 수 있습니다. 이 방법은 신규 항목과 기존 항목이 동일한 테넌트에 속한 경우에 재등록할 때 특히 유용합니다. 기기 페이지에는 다음과 같이 MDM용 Ivanti Neurons 관리 포털의 기기 상태가 표시됩니다.

- **활성** - 기기 등록이 완료됨
- **폐기** - 기기가 재설정되고 폐기 상태로 표시됨
- **지우기** - 기기가 재설정되고 지우기 상태로 표시됨
- **재설정** - 기기가 재설정되고 다음 등록 전까지 서버에 활성 상태로 표시됨

감사 내역 페이지에는 Android 기기의 기기 등록, 재등록, 폐기 상태가 나열됩니다. 자세한 내용은 위젯 작업을 참조하십시오.

> Android 9.x 및 이전 버전의 경우 재등록 후 단일 항목이 표시됩니다. Android 10.x 및 이후 버전의 경우 여러 항목이 표시됩니다. 그러나 마지막 항목만 활성화되며 이전 항목은 폐기 상태가 됩니다.

# 7.5.5. 기기 등록(Windows 10+ PC 및 Microsoft Hololens 2)

이 섹션에는 다음 주제가 포함됩니다.

기기 등록 프로세스에는 다음의 두 가지 유형이 있습니다.

- 수동 등록
  - 초대
  - 최종 사용자 등록
- Windows Autopilot
- PIN으로 패키지 등록 프로비저닝을 통한 SCCM 및 Ivanti EPM. **PIN으로 패키지 등록 프로비저닝**을 참조하십시오.
- **대량 등록**

## 수동 등록

대부분의 사용자들은 장치 등록부터 시작합니다. 다음 중 원하는 방법을 이용해 등록 절차를 실행할 수 있습니다.

- 이메일 초대
- 사용자 실행을 위한 URL로 안내
- 기기 등록 절차를 시작하기 전에 최종 **사용자에게 MDM용 Ivanti Neurons 계정**이 있어야 합니다. LDAP 사용자의 경우, **Connector**와 **LDAP 서버** 설정이 필요하며, 해당 사용자를 LDAP 서버에서 불러와야 합니다. 로컬 사용자의 경우, **사용자 추가**가 필요합니다.
- MDM용 Ivanti Neurons 이전 버전에서 생성된 기기 등록 URL은 현재 버전과의 작동을 중단합니다. 관리자는 기기 등록을 위해 기기 등록 URL을 다시 생성해야 합니다.

## 초대장 보내기

대부분의 경우 초대장을 발송해 등록 절차를 실행하게 됩니다. MDM용 Ivanti Neurons에서 다음 방법으로 최종 사용자에게 기기 등록 초대장을 전송할 수 있습니다.

- **시작 마법사**에서 발송
- **1명 이상 사용자를 추가**할 때 발송
- 사용자 페이지(**작업 > 초대장 보내기**)에서

초대장을 분실한 사용자, 데스크톱이나 노트북 컴퓨터로 수신한 사용자, 또는 특정한 이유로 수신하지 못한 사용자에게는 초대장에 제공되어 있는 URL을 보내면 됩니다. 서비스 URL 마지막에 **\go**를 추가하기만 하면 됩니다.

비밀번호가 설정된 MDM용 Ivanti Neurons 계정이 있는 최종 사용자는 등록 프로세스를 실행하는 데 초대장이 필요하지 않습니다. 해당 사용자들에게는 초대장에 제공되는 URL만 발송하면 됩니다.

## 최종 사용자 등록 절차 완료

기기 사용자에게 등록 절차를 완료하는 방법을 안내합니다. 다음 지침을 템플릿으로 사용하여 필요한 사항을 변경할 수 있습니다.

**절차**

1. Windows 10+ PC에서 브라우저를 엽니다.

2. mobileiron.com/go로 이동합니다.
   등록 URL이 포함된 새 페이지로 이동합니다.
3. 등록 URL을 클립보드에 복사합니다.
4. **설정** 페이지 하단의 **계정 추가**를 누릅니다.
5. 수령한 초대장과 관련된이메일 주소를 입력합니다.

> 사용자의 MDM용 Ivanti Neurons 사용자 이름이 MDM용 Ivanti Neurons에 입력한 사용자의 이메일 주소와 일치하지 않는 경우, 이메일 주소를 입력하라는 메시지가 표시될 때 사용자 이름을 입력하라는 안내가 나타납니다.

복사한 작업 공간 서버 URL을 다음 텍스트 필드에 붙여넣습니다.

7. **로그인**을 누릅니다.
8. 다음 필드에 비밀번호를 입력합니다.
9. 다른 필드는 빈 상태로 둡니다.
10. **로그인**을 누릅니다.
11. **추가된 계정** 화면에서 **완료**를 클릭합니다.
    작업 공간 시작 화면에 계정이 추가되었다고 표시됩니다.

## Windows Autopilot

Windows Autopilot은 관리자가 새로운 기기로 언제든 비즈니스를 수행할 수 있도록 설정하고 사전 구성하는 데 도움을 주는 Microsoft 기능입니다. Autopilot 기능은 Windows Desktop 또는 HoloLens2 기기를 빠르고 안정적이며 원활하게 프로비저닝하는 데 유용합니다. 뿐만 아니라 Autopilot 기능은 다음 작업을 수행하는 데 도움을 줍니다.

- Entra ID(Entra ID)에 기기 자동 연결
- MDM 서비스에 장치 자동 등록
- 기기 프로필을 기반으로 기기를 생성하여 구성 그룹에 자동 할당합니다.
- 등록 환경을 사용자 정의합니다.
- 구성 및 정책을 적용합니다.
- 필수 애플리케이션을 설치합니다.

Ivanti는 Autopilot 프로필의 모든 모드를 지원합니다.

- 사용자 주도
- 사용자 주도의 사전 프로비저닝(구 White Glove)
- 자체 배포 모드

자세한 내용은 **Windows Autopilot 프로필 구성**을 참조하십시오.

> 기기의 보안 및 무단 사용 방지를 위해 TenantLockdown CSP 기능을 사용하여 모든 Autopilot Windows 기기를 테넌트에 잠글 수 있습니다. 이 기능을 사용하려면 Autopilot 옵션을 사용하여 기기를 등록해야 합니다. 이 구성은 기기 수준에서 적용됩니다.
> **TenantLockdown CSP**를 참조하십시오.

## Entra ID 표준 등록

Entra ID 테넌트에 사용자가 추가될 경우 회사 계정을 통해 기기를 직접 등록할 수 있습니다.

**절차**

1. Windows 장치의 경우 **설정 > 계정 > 직장 또는 학교 액세스**로 이동합니다.
2. 직장 또는 학교 계정을 선택하고 **연결**을 클릭합니다.
3. 회사 계정의 이메일 주소를 입력합니다.

기기가 MDM용 Ivanti Neurons에 자동으로 등록됩니다.

# 7.5.6. LAPS(로컬 관리 비밀번호 솔루션)

**LAPS(로컬 관리자 비밀번호 솔루션)**은 Windows 기기 비밀번호의 안전한 관리를 자동화합니다. LAPS는 무작위이고 정기적인 비밀번호 변경을 강제로 시행하며, 이 비밀번호를 디렉터리에 안전하게 저장하여 침해 발생 시 수평 이동 위험을 줄입니다.

최신 LAPS는 Azure 및 최신 Windows 기기 관리 플랫폼과 통합되어 Ivanti Neurons for MDM 및 Azure 포털을 통해 안전한 비밀번호 저장, 검색 및 정책 구성을 지원합니다. 이를 통해 관리자 자격 증명이 보호되고, 레거시 및 클라우드 관리형 Windows 엔드포인트 모두에서 감사 추적이 가능합니다.

> LAPS를 MDM용 Ivanti Neurons과(와) 함께 사용하려면, Azure 관리자는 N-MDM 앱이 필수 LAPS 권한(**DeviceLocalCredential.Read.All**)으로 Azure 테넌트에 추가되어 있는지 확인해야 합니다.

> **관리자 계정 이름** 정책 설정을 사용해 LAPS가 적용되는 로컬 관리자 계정을 지정할 수 있습니다.구성에서 지정된 계정 이름이 기기에 존재하지 않으면, 해당 계정 이름은 관리될 수 없습니다. 단, **관리자 계정 이름**을 비워두면, 정책은 기기의 기본 내장 로컬 관리자 계정으로 기본 설정됩니다. 이 계정은 잘 알려진 RID(상대 식별자)로 식별됩니다.

> LAPS 구성이 적용되면, 기기의 로컬 관리자 계정 비밀번호는 관리자가 관리하며, 비밀번호는 Azure Active Directory에서 생성됩니다.

## LAPS의 추가 기능

- Azure에 비밀번호 저장 – 로컬 관리자 비밀번호는 이제 Azure 기기 개체에 안전하게 저장될 수 있습니다.
- 비밀번호 검색 – 관리자가 Azure 포털을 통해 기기 비밀번호를 직접 검색할 수 있습니다.
- 구성 가능한 설정 – LAPS 구성 가능한 설정은 MDM용 Ivanti Neurons 포털에서 관리할 수 있습니다.
- 요구 시 비밀번호 주기적 변경 – 관리자가 MDM용 Ivanti Neurons 포털에서 수동으로 기기 비밀번호를 주기적 변경할 수 있습니다.
- 사용 시 자동 비밀번호 재설정 – 비밀번호가 사용되면 자동으로 재설정될 수 있습니다.

## LAPS 구성 생성

필수 조건

- 기기에 대해 LAPS 솔루션이 활성화되어야 합니다 이 솔루션은 기본적으로 모든 사용자에게 제공되지는 않습니다. 도움이 필요하면 기술 지원팀에 문의하십시오.
- 기기는 ADO(Azure Device Operations)에 등록되어 있어야 합니다.

**절차**

1. 구성 관리 플랫폼에서 LAPS 구성을 생성하기 시작합니다.
2. **필수 매개변수 설정**:
    - **백업 디렉터리** - 비밀번호를 Microsoft Entra ID에만 백업하도록 선택합니다.
    - **로컬 관리자 이름** - 시스템의 관리자 계정 이름을 지정합니다(예: Admin).
3. **추가 설정 구성** - 조직의 보안 정책에 따라 추가 설정을 구성합니다. 지정하지 않은 경우 기본값이 사용됩니다.
    - **PasswordAgeDays** - 로컬 관리자 비밀번호가 자동으로 회전되기 전의 일 수를 지정합니다.
    - **PasswordComplexity** - 비밀번호 복잡성 요구 사항을 지정합니다(예: 영숫자, 특수문자).
    - **PasswordLength** - 로컬 관리자 비밀번호의 원하는 길이를 설정합니다.

- **PostAuthenticationActions** - 인증 후 수행되어야 할 작업을 정의합니다.
- **PostAuthenticationResetDelay** - 인증 후 비밀번호를 재설정하기까지의 지연 시간(시간/분 단위)을 설정합니다.

4. **LAPS 구성 배포**
   - ADO에 등록된 사용자/기기에 LAPS 구성 프로필을 할당합니다.
   - 구성을 적용하면 무작위 로컬 관리자 비밀번호가 생성되어 다음의 Microsoft Entra ID에 안전하게 저장됩니다: **기기 → 기기 관리 → 로컬 관리자 비밀번호 복구**.
5. **비밀번호 주기적 변경**
   - 비밀번호는 **PasswordAgeDays**에 설정된 값에 따라 자동으로 주기적 변경됩니다.
   - 기기 로그에서 비밀번호 주기적 변경 상태를 확인할 수 있습니다.

## 비밀번호 주기적 변경

로컬 관리자 비밀번호를 즉시 주기적으로 변경하려면 다음 단계를 따르십시오:

1. **기기 세부 정보 페이지로 이동** - 관리 콘솔에서 기기 세부 정보 페이지로 이동합니다.
2. **비밀번호 주기적 변경 시작**
   - 점 세 개 메뉴(...)를 클릭합니다.
   - **로컬 관리자 비밀번호 주기적 변경**을 선택합니다.
   - 메시지가 표시되면 작업을 확인합니다. 비밀번호 주기적 변경 요청이 제출됩니다.
3. **체크인 및 확인**
   - 기기는 다음번 강제 체크인 중에 비밀번호 변경을 처리합니다.
   - Microsoft Entra ID에서 페이지를 새로 고침하여 비밀번호 복구 섹션에서 업데이트된 비밀번호를 확인합니다.

# 7.5.7. PIN으로 패키지 등록 프로비저닝

관리자는 SCCM 또는 Ivanti Endpoint Manager에서 관리하는 기기를 MDM용 Ivanti Neurons에 등록할 수 있습니다. 배포 패키지 도구를 사용하면 다운타임이나 최종 사용자 중단 없이 Windows 기기를 MDM용 Ivanti Neurons Modern Management로 간편하게 전환할 수 있습니다. MDM용 Ivanti Neurons 콘솔에서 고유한 배포 패키지를 다운로드한 다음 기존 관리 도구 또는 도메인을 통해 이를 배포하여 원활하게 전환할 수 있습니다. 패키지가 실행되면 지속적인 관리를 위해 엔드포인트를 MDM용 Ivanti Neurons에 자동으로 등록합니다. 관리자는 이 접근 방법을 통해 먼저 기기를 쉽게 마이그레이션한 다음, 나중에 무선으로 기기를 유연하게 구성할 수 있습니다. 기기가 자동으로 MDM용 Ivanti Neurons에 등록되면 MDM과 결합하며 두 가지 관리 권한에 의해 공동 관리됩니다. 관리자가 MDM용 Ivanti Neurons에서 바람직한 Windows 환경을 설정했다면 레거시 관리 플랫폼을 해체하여 MDM용 Ivanti Neurons(을)를 기기의 단일 관리 권한으로 남겨둘 수 있습니다.

> 기기가 MEM(Microsoft Endpoint Manager) 또는 이전 SCCM에서 전환되는 경우 이 규칙에 대한 예외가 있습니다. 기존 MEM 클라이언트는 MEM 플랫폼이 해체될 때까지 공존 모드(공동 관리 모드의 반대)로 계속 작동합니다. 공존 모드가 활성화되면 MEM 클라이언트는 이러한 워크로드를 제공하는 MDM용 Ivanti Neurons(을)를 위해 특정 기능을 자동으로 비활성화합니다. 자세한 내용은 **Microsoft의 공존 문서**를 참조하십시오.

MEM 및 타사 관리 플랫폼을 사용할 때 보다 정확한 동작을 수행할 수 있도록 하기 위해 Ivanti는 사용자 환경에서 MDM용 Ivanti Neurons 배포 패키지 도구를 먼저 테스트할 것을 제안합니다.

**필수 조건**

- 사용자 계정은 LDAP, Entra ID(Entra ID), 로컬 사용자 업로드 또는 기타 ID 통합을 사용하여 MDM용 Ivanti Neurons에서 가져와야 합니다.
- 모든 기기에는 **Windows 구성 디자이너**가 설치되어 있어야 합니다.
- MDM용 Ivanti Neurons에서 PIN 기반 등록 활성화
- 사용자 이름에 공백이 있으면 안 되며, 이로 인해 사용자 기기 전환이 실패할 수 있습니다.
- 이 도구는 Entra ID를 활용하지 않는 환경에 배포할 수 있습니다.
- MDM용 Ivanti Neurons Modern Windows Management Suite의 기본 요소에는 Entra ID가 필요하지 않습니다. 공동 관리 또는 공존을 위해서는 전환 중 영향을 피하기 위해 자동 등록 시 특정 워크로드/구성을 배포해야 할 수 있습니다.
- 배포 패키지는 현재 SCCM 및 Ivanti Endpoint Manager에 대해서만 지원됩니다.

**절차**

1. **관리자 > Windows > 배포 패키지**로 이동합니다.
2. **사용자** 또는 **사용자 그룹**을 선택하여 PIN을 생성한 후 **배포 패키지 다운로드**(.zip 파일)를 클릭합니다.
3. 배포 패키지는 SCCM/Ivanti Endpoint Manager 관리자에게 제공되어 이러한 관리자가 관리하는 각 기기에 파일의 압축을 풀고 전송할 수 있습니다. 이 단계를 수행하는 방법에 대한 자세한 내용은 **Configuration Manager의 패키지 및 프로그램**을 참조하십시오.
4. 전송 후 관리자는 기기에서 setup.ps1 스크립트를 원격으로 트리거합니다. 스크립트 트리거에 대한 자세한 내용은 **구성 관리자에서 스크립트 생성 및 배포**를 참조하십시오.
5. 기기는 MDM용 Ivanti Neurons에서 등록됩니다.

> 

사용자용으로 생성된 PIN은 24시간 동안만 유효합니다. PIN이 만료되면 새 PIN을 생성해야 합니다.

PIN을 포함하는 파일은 등록 시도가 완료된 후 기기에서 삭제됩니다.

## MDM용 Ivanti Neurons에 SCCM 기기 등록

**절차**

1. 선택한 사용자에 대해 MDM용 Ivanti Neurons에서 모든 배포 관련 파일을 다운로드합니다.
2. 등록해야 하는 계정 또는 그룹을 선택합니다.
3. SCCM을 사용하여 패키지 파일을 클라이언트 기기에 배포합니다.
    1. 필요한 클라이언트가 SCCM에 있는지 확인합니다. Windows-configuration-designer가 클라이언트에 없으면 관리자는 디자이너를 푸시하고 클라이언트에 배포해야 합니다.
    2. SCCM 서버에서 폴더를 만들고 배포 zip 파일을 복사하고 파일 내용을 추출합니다.
    3. 파일이 추출된 폴더의 콘텐츠를 클라이언트 기기에 복사할 .bat 파일을 만듭니다.
    4. SCCM에서 **소프트웨어 라이브러리 > 애플리케이션 관리 > 패키지**로 이동하고 폴더의 콘텐츠를 클라이언트에 복사할 패키지를 만듭니다. 콘텐츠를 복사할 대상 폴더를 입력합니다.
    5. 기기 또는 기기 위치에 패키지를 배포합니다.
    6. 모니터링 섹션에서 배포 상태를 모니터링하고 파일이 클라이언트 대상 폴더에 복사되었는지 확인할 수 있습니다.
4. 스크립트를 실행하여 기기 등록:
    1. **소프트웨어 라이브러리 > 스크립트**로 이동하여 스크립트를 생성합니다.
    2. 스크립트 이름을 입력하고 압축을 푼 폴더에서 PowerShell 스크립트 **setup.ps1**을 가져옵니다.
    3. 스크립트를 승인하고 대상 기기에서 해당 스크립트를 실행합니다.
    4. **지금 시작**을 선택하고 **저장**을 클릭합니다. 예약된 작업이 스크립트 실행을 시작합니다. 성공적으로 실행되면 상태가 녹색으로 됩니다.
5. 기기 등록을 확인하려면 **설정** > **프로비저닝 패키지 추가 또는 제거** > **세부 정보**로 이동합니다.

## MDM용 Ivanti Neurons에 Ivanti Endpoint Manager 기기 등록

**절차**

1. 선택한 사용자에 대해 MDM용 Ivanti Neurons에서 모든 배포 관련 파일을 다운로드합니다.
2. 등록해야 하는 계정 또는 그룹을 선택합니다.
3. **사례 1**: 동일한 사용자 이름으로 기기를 등록할 때 기기 이름 고려 - 이 경우 이메일 주소는 유효한 사용자 이메일 주소가 아닙니다. 기기 이름이 AD 도메인과 연결된 이메일은 등록 이메일 주소로 간주됩니다. 관리자는 계정을 LocalSystemAccount로 설정하고 setup.ps1을 기본 파일로 사용하여 PowerShell 실행을 시작해야 합니다.
   **사례 2**: 유효한 사용자 이메일 주소가 기기 등록에 고려되고 기기 위치에서 파일 수정에 대한 제한 없음 - 등록을 위해 로그인한 사용자의 이메일 주소를 사용합니다. 이 등록을 활성화하려면 관리자가 계정을 현재 사용자 계정으로 설정하고 setup.ps1을 기본 파일로 사용하여 PowerShell 실행을 시작해야 합니다.
   **사례 3**: 기기 위치에서 파일 수정에 대한 제한이 있는 기기 등록을 위해 유효한 이메일 주소 고려 - 등록을 위해 로그인한 사용자의 이메일 주소를 사용합니다. 이 경우 다음 두 가지 하위 사례가 있습니다.
    - 등록에 두 개의 스크립트 사용 - **setupEPMCopyContentsToTempFolderStep1.ps1**을 사용하여 배포 패키지를 만들고 현재 사용자 계정으로 실행합니다. 파일이 임시 위치에 복사됩니다. **setupEPMCopyContentsToTempFolderStep2.ps1**을 사용하여 또 다른 배포 패키지를 만들고 로컬 시스템 계정으로 실행합니다.

      > 기기 사용자에 패키지 파일이 포함된 폴더 수정에 제한이 있을 경우 - 파일을 임시 폴더에 복사하고 사용자 ID를 확인한 후 PowerShell 패키지를 생성합니다. PowerShell 패키지는 **setupEPMCopyContentsToTempFolderStep2.ps1** 스크립트로 실행합니다. 설치 후 임시 폴더는 삭제됩니다.

UAC 활성화/비활성화

1. 레지스트리 항목을 업데이트하여 UAC 제어를 비활성화하고 컴퓨터 재부팅
2. setup.ps1을 사용하여 현재 사용자 계정으로 PowerShell 패키지 실행
3. UAC 제어를 활성화하고 시스템을 재부팅하도록 레지스트리 항목 업데이트

PowerShell 패키지 생성:

1. Endpoint Manager에 필수 클라이언트가 있는지 확인합니다.
2. 파일을 C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\에 복사합니다. 이 폴더 내에 하위 폴더를 만들고 파일을 추출합니다.
3. 패키지 생성: **배포 > 배포 패키지 > 새로 만들기 > Windows > PowerShell**.

   > 관리자는 기기에 설정된 제한 수준에 따라 패키지를 다른 기기에 배포할 수 있습니다.

4. 기본 파일 섹션에서 패키지 이름을 입력하고 복사된 파일이 있는 폴더에서 setup.ps1을 업로드합니다.
5. 추가 파일 섹션에서 **추가**를 사용하여 나머지 파일(setup.ps1 스크립트 제외)을 복사합니다.
6. 계정 섹션에서 현재 사용자 계정을 선택합니다.
7. **저장**을 클릭하세요.

4. 예약된 작업 생성:
   1. 생성된 패키지를 선택하고 마우스 오른쪽 버튼을 클릭하여 **예약된 작업 생성**을 선택합니다. 예약된 작업이 생성됩니다.
   2. 기기를 끌어 예약된 패키지 섹션에 추가합니다.
   3. 예약된 패키지에서 마우스 오른쪽 버튼을 클릭하여 **속성**을 선택합니다.
   4. 패키지를 확인합니다.
   5. 작업 유형에서 **푸시**를 선택합니다.
   6. **지금 시작**을 선택하고 **저장**을 클릭합니다. 예약된 작업이 스크립트 실행을 시작합니다. 성공적으로 실행되면 상태가 녹색으로 됩니다.
5. 기기 등록을 확인하려면 **설정** > **프로비저닝 패키지 추가 또는 제거** > **세부 정보**로 이동합니다. 또는 관리자가 기기의 진단 로그에서 기기 등록을 확인할 수 있습니다.

# 7.5.8. Windows 기기의 대량 등록 사용

대량 등록 기능을 통해 여러 Windows 기기를 MDM용 Ivanti Neurons에 신속하게 등록할 수 있습니다.

**필수 조건:**

- Entra ID(Entra ID) 프리미엄 계정을 사용하여 MDM용 Ivanti Neurons에 사용자 계정을 가져와야 합니다.
- 모든 기기에는 **Windows 구성 디자이너**가 설치되어 있어야 합니다.

**절차:**

1. MDM용 Ivanti Neurons와(과) Entra ID 테넌트를 연결합니다. **Windows 10 기기용 UEM에 Entra ID 연결**을 참조하십시오.
2. **Windows 구성 디자이너** 앱을 열고 **데스크톱 기기 프로비전**을 선택합니다. 화면에 새 프로젝트 창이 표시됩니다.
3. 다음 세부 정보를 입력합니다.
    - 이름 - 프로젝트의 고유한 이름
    - 프로젝트 폴더 - 기기에서 프로젝트를 저장할 위치
    - 설명 - 프로젝트 설명(선택 사항)

**완료**를 클릭하여 새 프로젝트 창을 닫고 순서대로 단계를 수행합니다.

5. **기기 설정**
   기기의 고유한 이름을 입력합니다. 이름에는 일련 번호(%SERIAL%) 또는 무작위의 문자가 포함될 수 있습니다.
6. 필요에 따라 Windows 업데이트를 진행하는 경우, 기기를 공유용으로 구성하는 경우, 사전 설치된 소프트웨어를 제거하는 경우에 제품 키를 입력할 수 있습니다.
7. **네트워크 설정**
   필요에 따라 처음 시작 시 연결할 Wi-Fi 네트워크 장치를 구성할 수 있습니다. 네트워크 장치가 구성되지 않은 경우, 기기를 처음 시작할 때 유선 네트워크 연결이 필요합니다.
8. **계정 관리**
   **Entra ID에서 등록**을 선택하고 **대량 토큰 만료** 날짜를 입력한 후 **대량 토큰 가져오기**를 클릭합니다.
9. Entra ID 자격 증명을 입력하여 대량 토큰을 가져옵니다.
10. **모든 앱에서 로그인 상태 유지** 페이지에서 **아니요, 이 앱에만 로그인합니다**를 클릭합니다.
    - 대량 토큰을 가져왔다면 다음을 클릭하고 패키지를 생성합니다.
    - Azure 포털 - 사용자 기본 이름에 프로비저닝 패키지가 있는 사용자가 생성됩니다(예: package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com). 스토리지 기기에 파일(런타임 패키지 도구)을 복사합니다.

> 대량 토큰 생성용 Entra ID 사용자와 패키지 사용자는 MFA를 활성화해서는 안 됩니다. 확인하려면 해당 사용자에 대해 OOBE + Entra ID 조인을 수행해야 합니다.

패키지 사용자(Azure에서 생성됨)를 다시 생성하거나 MDM용 Ivanti Neurons에 동기화합니다.

프로비저닝 패키지에 포함된 플래시 드라이브로 기기를 대량 등록합니다. 기존 기기를 두 번 클릭하여 포스트 OOBE 환경을 수행할 수도 있습니다. 첫 시도에서 패키지를 설치하지 못한 경우에는 두 번째 시도에서도 실패합니다. 새 기기가 MDM용 Ivanti Neurons에 생성되었으며 Entra ID가 패키지 사용자에게 연결되어 있는지 확인하십시오.

# 7.5.8.1. Ivanti 대량 등록

관리자는 (ppkg를 통해) 접두사 **windows-bulkenroll**로 시작하는 일반 사용자로 여러 Windows 기기를 등록한 후 나중에 사용자를 할당할 수 있습니다.

**필수 조건:**

- MDM용 Ivanti Neurons에서 접두사가 **windows-bulkenroll**인 사용자 계정을 만듭니다. 예를 들어, **windows-bulkenroll**-user1@abc.com, **windows-bulkenroll**-user2@abc.com과 같은 형식입니다.

**Windows Configuration Designer를 사용하여 PPKG 패키지 만들기**

1. **Windows 구성 디자이너**를 다운로드하여 설치합니다.
2. 새 프로젝트를 만듭니다.
3. **데스크톱 프로비저닝**을 클릭합니다.
4. 프로젝트 이름을 입력하고 경로를 선택합니다.
5. **기기 설정** 섹션에 기기 이름을 입력합니다.
6. **네트워크 설정** 섹션에 네트워크 이름을 입력합니다(필요한 경우 네트워크를 설정하거나 비활성화할 수 있음).
7. **계정 관리** 섹션에서 **로컬 관리자에 등록**을 선택합니다. **사용자 이름**과 **비밀번호**를 입력하고 **다음**을 클릭합니다.
8. **애플리케이션 추가** 섹션에서 **다음**을 클릭합니다.
9. **인증서 추가** 섹션에서 **고급 편집기로 전환**을 선택하고 **진행** > **예**를 클릭합니다.
10. **RuntimeSettings** > **Workplace 등록**으로 이동합니다. **UPN**(전제 조건 섹션의 MDM용 Ivanti Neurons에서 생성한 동일한 사용자)을 입력합니다. 다음 옵션을 선택합니다:
    - AuthPolicy: OnPremise
    - DiscoveryServiceFullUrl: https://login.mobileiron.com
    - Secret: 비밀번호 입력

**파일** > **저장**을 클릭합니다.

12. **내보내기** > **패키지 프로비저닝**을 클릭합니다.
13. 이후 화면에서 **다음**을 클릭하고 **빌드**를 클릭합니다.
    ppkg 파일이 지정된 위치에 저장됩니다.

**ppkg를 사용하여 OOBE 모드에서 기기 프로비저닝**

위 섹션에서 새로 만든 ppkg 패키지 파일로 기기를 프로비저닝합니다. 기기가 등록되고 체크인이 성공적으로 완료되면, MDM 서버에서 접두사가 **windows-bulkenroll**인 사용자가 있는 기기 항목을 확인할 수 있습니다.

**사용자에게 기기 할당**

1. 기기 페이지에서 접두사가 **windows-bulkenroll**인 사용자를 클릭합니다.
2. **사용자에게 할당**을 클릭합니다. '사용자에게 할당' 창이 열립니다.
3. 목록에서 기기를 선택하거나 검색합니다.
4. 필요한 기기를 선택합니다.
5. **사용자에게 할당**을 클릭합니다. 선택한 기기가 사용자에게 할당됩니다.

사용자가 처음으로 기기에 로그인하는 경우, 비밀번호를 변경해야 합니다.

'사용자에게 할당' 옵션은 Ivanti 대량 등록 기기에서만 사용할 수 있습니다.

이 카테고리에 등록된 기기에는 기기 범위 구성 및 애플리케이션만 작동합니다. 사용자 범위 구성 및 애플리케이션은 지원되지 않습니다.

# 7.5.9. 암호 설정 변경하기

이 섹션에는 다음 주제가 포함됩니다.


- 할당된 암호 구성 변경
- 다른 암호 설정 할당


기기에 할당된 **암호 구성**을 사용하여 암호 설정을 변경합니다. 다음 중 원하는 방법으로 암호 설정을 변경할 수 있습니다.

- 기존 암호 설정을 변경

또는

- 다른 암호 설정 할당

**암호 설정을 변경하면 해당 설정이 적용되어 있는 모든 기기의 설정도 함께 변경됩니다.**

## 할당된 암호 구성 변경

**절차**

1. **기기**로 이동합니다.
2. 목록에서 원하는 장치 항목을 확인하세요.
3. **이름** 열의 링크를 클릭합니다.

> 이미 암호 설정이 할당되어 있는 경우, 해당 설정이 설정 탭에 표시됩니다.

구성 탭에서 **암호 구성** 링크를 클릭합니다.

5. **수정**(우측 상단)을 클릭하세요.
6. 필요한 설정을 변경하세요.

## 다른 암호 설정 할당

**절차**

1. 이미 생성되어 있는 설정만 할당이 가능합니다.
2. **기기**로 이동합니다.
3. 목록에서 원하는 장치 항목을 확인하세요.
4. **이름** 열의 링크를 클릭합니다.

# 7.5.10. 기기 이름 변경

관리자는 수동으로 기기의 이름을 변경할 수 있습니다(기기 이름 구성 편집을 사용하지 않음).

**적용 가능 운영 체제:**

- iOS 감독 기기
- tvOS 감독 모드 기기
- macOS 10.10+ 기기

**절차**

1. **기기**로 이동합니다.
2. 목록에서 원하는 장치 항목을 확인하세요.
3. 다음 작업 중 하나를 수행합니다.
    - 아직 추가하지 않았다면 오른쪽에 있는 설정 기어 아이콘을 클릭하고 **기기 이름**을 선택하여 **기기 이름** 열을 추가합니다.
    - **이름** 열에 위치한 링크를 클릭하면 기기 상세 정보 페이지로 이동합니다.
4. 기기 이름 옆의 **편집** 연필 아이콘을 클릭합니다.
5. 새 기기 이름을 입력한 후 체크 표시 아이콘을 클릭합니다.
6. 기기 이름 덮어쓰기 표시 상자에서 메모를 검토한 후 **확인**을 클릭합니다.

변경된 이름은 다음에 체크인할 때 기기에 푸시됩니다. 이 작업은 실행 취소할 수 없습니다.

> 기본 기기 이름 구성이 이미 설정된 경우 이 작업은 구성에 설정된 이름을 덮어씁니다.

# 7.5.11. 기기 찾기 및 필터링

이 섹션에는 다음 주제가 포함됩니다.


- 기기 검색
- 기기 필터링
- 고급 검색 사용
- 검색 쿼리 로드


## 기기 검색

MDM용 Ivanti Neurons 관리 포털은 규칙 작성기에서 사용자 그룹 이름 속성을 선택할 때 중복 그룹을 식별할 수 있도록 중복 사용자 그룹 수 및 해당 GUID 수를 표시합니다.또한 이 규칙 아래에 있는 표에는 중복 사용자 그룹 목록과 사용자 그룹 이름, GUID, 소스, 배포된 이름(DN)과 같은 세부 정보가 표시됩니다.

**절차**

1. **기기**로 이동합니다.
2. **검색** 필드에 기기 이름을 입력합니다. 문자가 포함된 모든 기기가 나열됩니다.

## 기기 필터링

필터 측면 탐색 모음에는 전체 기기 목록에서 특정 기기를 검색할 수 있는 다양한 섹션이 나열되어 있습니다. 필터 관리 마법사에는 필터 탐색 모음에 표시할 수 있는 모든 섹션의 목록이 포함되어 있습니다.

**절차**

1. **기기**로 이동합니다.
2. 필터 측면 탐색 모음에 나열된 섹션에서 관련 체크박스를 클릭합니다.
   **예**:
   - **사용자 활성화됨** 섹션에서 **예**를 선택하면 사용자가 활성화 상태인 기기만 표시됩니다.
   - 기기에 사용자 지정 속성을 할당했다면 설정(cog) 아이콘을 클릭하여 속성에 따라 기기를 필터링할 수 있습니다.
   - **상태** 섹션에서 **폐기됨**과 **iOS**를 선택하면 폐기된 iOS 기기만 표시됩니다.

(선택 사항) **기본값 복원**을 클릭하면 선택 사항을 기본값 필터로 복원할 수 있습니다. 필터 탐색 모음에 선택한 섹션이 표시됩니다. 필터 관리 마법사에서 모든 체크박스의 선택을 해제하면 필터 측면 탐색 모음에 모든 섹션이 표시됩니다.

4. 마법사를 종료하려면 필터 관리 마법사 바깥 영역을 아무 곳이나 클릭합니다.
5. (선택 사항) 필터 측면 탐색 모음을 닫으려면 x 아이콘을 클릭하고 측면 탐색 모음을 다시 열려면 **필터**를 클릭합니다.
   - Apache SOLR 서버 구성의 일부인 stopwords.txt 파일에 나열된 중지 단어를 사용할 경우 해당 단어는 색인 처리되지 않습니다. 따라서 중지 단어가 포함된 모든 엔터티는 검색 결과에 표시되지 않습니다.
   - 엔터티 예 - 기기, 사용자, 그룹, 속성, 애플리케이션, 인증서, 감사 내역, 콘텐츠, 알림 모듈
   - 중지 단어 예 - a, an, if, be, into 등

## 고급 검색 사용

특정 기준이 있는 기기를 식별하고 보려면 고급 검색 옵션을 사용하여 규칙에 기반한 기기를 검색할 수 있습니다. 이 규칙은 "다음으로 시작", "다음으로 끝", "포함", "미포함", "다음으로 시작하지 않음", "다음으로 끝나지 않음", "보다 작음", "보다 큼", "범위에 있음", "다음과 같음", "다음과 같지 않음" 연산자를 사용하여 구성할 수 있습니다. 규칙 옵션은 임의(OR) 또는 모두(AND) 옵션을 사용하여 중첩될 수 있습니다. 규칙을 충족하는 기기가 섹션 아래에 표시됩니다.

MDM용 Ivanti Neurons 관리 포털은 규칙 작성기에서 사용자 그룹 이름 속성을 선택할 때 중복 그룹을 식별할 수 있도록 중복 사용자 그룹 수 및 해당 GUID 수를 표시합니다. 또한 이 규칙 아래에 있는 표에는 중복 사용자 그룹 목록과 사용자 그룹 이름, GUID, 소스, 배포된 이름(DN)과 같은 세부 정보가 표시됩니다.

**절차**

1. 기기 페이지에서 **고급 검색** 링크를 클릭합니다. 고급 검색 마법사가 열립니다.
2. 다음 옵션 중 하나를 클릭합니다.
   - **일부** - 기기가 하나 이상의 규칙을 충족해야 할 경우 클릭
   - **모두** - 기기가 모든 규칙을 충족해야 할 경우

검색 기준을 정의하는 규칙을 생성합니다. **예**: APNS 가능은 예와 같습니다.

4. (선택 사항) **+**를 클릭하여 추가 규칙을 생성할 수 있습니다.
5. **검색**을 클릭합니다. 검색 기준에 부합하는 기기 목록이 표시됩니다.
   - iOS 14.0+ 기기의 경우, 기기의 eSIM ID(EID)를 기기 상세 정보 페이지에서 사용할 수 있습니다. 통신사는 eSIM ID(EID)를 통해 특정 기기에 SIM을 할당할 수 있습니다. eSIM ID(EID) 필드는 GDPR을 준수합니다.
   - 새 GDPR 필드(예: IP 주소 및 eSIM ID)가 MDM용 Ivanti Neurons 릴리스에서 추가되면 GDPR을 이미 구성한 관리자는 새 필드를 숨기려면 GDPR 프로필을 편집해야 합니다.
   - 고급 검색은 기기의 복구 잠금 상태를 보여줍니다.

## 검색 쿼리 로드

저장된 검색 쿼리 목록을 볼 수 있습니다.

**절차**

1. 고급 검색을 클릭하고 폴더 아이콘을 클릭합니다. 생성된 검색 쿼리 목록이 **쿼리 로드** 섹션에 표시되고 다음과 같은 세부 정보가 표시됩니다.
   - **쿼리 이름** - 로드된 쿼리 이름.
   - **쿼리 콘텐츠** - 검색 쿼리를 정의하는 규칙에 콘텐츠를 표시합니다.
   - **작업** - 쿼리에서 수행할 작업을 선택합니다.
2. 로드된 쿼리에 정의된 기준에 부합하는 기기 목록을 보려면 **작업** 열에서 **쿼리 로드**를 클릭합니다.
3. **삭제**를 클릭하여 로드한 쿼리를 삭제합니다.

# 7.5.12. 기기 소유자 이용하기

이 섹션에는 다음 주제가 포함됩니다.

- QR 코드 또는 NFC 범프를 사용하여 Android Enterprise 기기 프로비저닝
- 클라이언트 토큰을 사용하여 Android Enterprise 기기 프로비저닝

**라이센스**: Gold

기기를 등록한 후에는 기기를 기업 소유 또는 직원 소유로 지정할 수 있습니다. 이러한 지정은 사용자가 개인용 기기 또는 기업 소유 기기를 갖고 있는지 여부를 기준으로 하는 정책을 관리하는 데 도움이 됩니다. 적절한 라이센스가 있으면 규칙에 소유권을 이용하여 기기 그룹을 생성할 수 있습니다.

새로운 기기 또는 공장 초기화된 기기에서 **Provisioner** 앱을 사용하여 다음 중 한 가지 옵션으로 기기 소유자를 프로비저닝합니다.

- NFC(근거리 무선통신) bump
- QR 코드 스캔

NFC bump는 새로운 기기 또는 공장 초기화된 기기에 대하여 마스터 또는 템플릿 기기를 눌러 프로비저닝하는 작업을 포함합니다.

QR 코드 스캔은 새로운 기기 또는 공장 초기화된 기기의 화면을 누르고, Wi-Fi 네트워크를 구성하고, 기기를 프로비저닝할 준비가 되었을 때 코드를 스캔하는 작업을 포함합니다.

NFC 또는 QR 코드를 사용하여 기기 소유자 모드를 프로비저닝하는 동안 Provisioner 앱이 등록 토큰을 수락합니다. 등록 시, 등록 토큰이 서버로 전송됩니다. 서버에 존재하고 기기가 사용자에게 할당될 경우, 기기가 성공적으로 등록됩니다.

기기 소유자 모드일 경우 Go 클라이언트가 기기를 제어하며 사용자가 프로비저닝 프로세스를 중단하는 것을 방지하기 위해 기기를 MDM용 Ivanti Neurons에 등록할 때까지 화면을 잠급니다. 기기 소유자 모드는 키오스크 모드도 지원합니다. 구성 정보는 다음으로 이동하십시오.잠금 및 키오스크 구성.

**중요**

- 기기 소유자 모드에서 기기를 폐기하면 이 기기는 설정 초기화됩니다.
- 필요에 따라 기기 소유자 모드에서 모든 기기에 모든 시스템 앱이 활성화될 수 있습니다.
- 기기는 한번에 하나의 활성 기기 소유자만 가질 수 있습니다.
- Android Enterprise 지원 기기만 기기 소유자 모드로 프로비저닝할 수 있습니다.
- 기기 소유자 모드 상태인 Samsung KNOX Standard 기기의 경우 사용자에게 Samsung ELM 라이센스를 활성화하라는 메시지가 표시됩니다. Go 클라이언트 앱이 이전 버전에서 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전으로 업그레이드된 경우, 기기 소유자 모드 상태인 Samsung 기기에도 이 메시지가 표시됩니다. 활성화하면 기기 상세 정보 페이지에 일련 번호(기기 > 설정 > 일련 번호 필드에 있는 번호와 일치)가 표시됩니다.

## QR 코드 또는 NFC 범프를 사용하여 Android Enterprise 기기 프로비저닝

QR 코드 또는 NFC 범프를 사용하여 Android Enterprise 기기를 프로비저닝하려면 마스터 기기의 Google Play에서 Provisioner 앱을 다운로드하고 설치해야 합니다.

**호환되는 구성 요소**

Provisioner 버전: 1.3.0.

Provisioner는 다음과 호환되거나 연동됩니다.

| 항목 | 버전 |
| --- | --- |
| Android OS<br>(프로비저닝 대상 기기) | • 5.0 - 또는 NFC를 사용하는 경우 지원되는 최신 버전 필요.<br>• 7.0 - 또는 QR 코드를 사용하는 경우 지원되는 최신 버전 필요.<br>기기는 Android Enterprise를 지원해야 합니다. |
| Android OS(마스터 기기) | 5.1 - 가장 최신 릴리스 버전까지.<br>NFC bump를 사용하려면 기기에 NFC가 있어야 합니다. QR 코드에는 필요하지 않습니다. |
| Android Enterprise용 UEM 서버 제품 | 다음 중 하나:<br>MDM용 Ivanti Neurons 또는 허용 레이블 지정 MDM용 Ivanti Neurons |
| Android 클라이언트 앱 | Provisioner에 의해 프로비저닝된 기기에최신 클라이언트 앱 버전이 설치됩니다. |

**필수 조건**

Android Enterprise 기기를 작업 관리형 장치로 프로비저닝하려면 다음을 수행해야 합니다.

- 필요한 Android Enterprise 관련 구성이 정의되어 있고 등록된 기기에 적용되어야 합니다.

> 기본 Android Enterprise: 작업 관리형 기기 구성이 기기에 대해 활성화되어야 합니다.

서버에서 Android Enterprise를 활성화합니다.

- NFC 가능 Android 기기(NFC를 사용하는 경우만)가 Provisioner 앱이 설치된 상태에서 마스터 역할을 하도록 해야 합니다.
- 프로비저닝할 Android Enterprise 지원 기기가 있습니다.

NFC bump를 사용하도록 Android 빔을 활성화하는 방법:

**절차**

1. 기기에서 **설정**으로 이동합니다.
2. **네트워크 > 무선 네트워크**로 이동합니다.
3. **연결 섹션**에서 **공유 및 연결**을 선택합니다.
4. **NFC** 스위치를 **켜기** 쪽으로 밉니다.
5. **Android 빔** 스위치를 **켜기** 쪽으로 밉니다.

> Android 빔과 NFC를 활성화하기 위한 단계는 기기마다 다를 수 있습니다.

## 작업 관리형 기기가 되도록 Android Enterprise 기기 프로비저닝

**절차**

1. Android 마스터 기기를 사용하여 Google Play에서 Provisioner 앱을 다운로드하고 앱을 설치합니다.
2. 마스터 기기에서 Provisioner를 시작합니다.
3. 프로비저닝 방법으로 NFC 또는 QR 코드를 선택합니다.
4. **프로비저닝을 위한 앱**을 누르고 프로비저닝된 기기에 설치할 클라이언트 앱을 선택합니다.

| 이 클라이언트 앱을 선택합니다. | 이 UEM 서버에 등록하려면: |
| --- | --- |
| 이동 | MDM용 Ivanti Neurons |
| 작업 UEM | (허용 레이블 지정) MDM용 Ivanti Neurons |

5. Provisioner 앱에서 나머지 필드를 채웁니다. 지원되는 Wi-Fi 유형이 존재하는 경우 일부 필드는 자동으로 채워질 수 있습니다. QR 코드를 선택한 경우에는 Wi-Fi 필드가 표시되지 않습니다. 다음의 지침을 사용합니다.

| 필드 | 값 |
| --- | --- |
| 프로비저닝을 위한 앱 선택 | Go 또는 At Work |
| 표준 시간대 | 기기에 구성할 표준 시간대를 입력합니다. |
| 로캘 | 기기에 구성할 로캘을 입력합니다. |
| 모든 시스템 앱 활성화 | 모든 시스템 앱을 활성화하려면 체크박스를 클릭합니다. |
| Wi-Fi 네트워크 SSID | 대상 기기가 사용할 Wi-Fi SSID를 입력합니다. |
| Wi-Fi 보안 유형 | Wi-Fi 보안 유형을 입력합니다. |
| Wi-Fi 비밀번호 | Wi-Fi 비밀번호를 입력합니다. |
| 대량 등록 | 대량 등록 기능은 선택 사항입니다. 대량 등록 기능을 사용하려면 호스트 이름이 필요합니다. 필요에 따라 사용자 이름을 입력하고 빠른 시작 옵션을 선택할 수도 있습니다. 대량 등록 기능을 건너뛰려면 이 필드를 공백으로 남겨 놓아야 합니다. |

6. **계속**을 누릅니다.
7. **NFC**를 선택했으면 **계속**을 누릅니다. 마스터 기기에 **기기를 맞부딪히세요!** 화면이 표시됩니다. 아래의 **NFC Bump** 섹션을 따라 작업을 계속합니다.
8. **QR 코드**를 선택했다면 마스터 기기에 **이 QR 코드를 스캔하세요!** 화면이 나타납니다. 아래의 **QR 코드** 섹션을 따라 작업을 계속합니다.

**NFC Bump의 경우 아래 단계 사용**

대상 기기에 Android 시작 화면이 표시되는지 확인합니다.

9. 대상 기기와 뒷면을 마주한 마스터 기기를 눌러 NFC 전송을 시작합니다. NFC 전송이 성공하면 대상 기기에 소리가 울릴 수 있으며 이후에 클라이언트 앱의 다운로드를 진행합니다. Wi-Fi에 연결할 수 없거나 기기가 클라이언트 앱을 다운로드할 수 없는 경우에는 기기가 공장 초기화를 자동으로 수행합니다.
10. 소리가 들리거나 시작 화면이 아닌 화면이 보이면 기기를 디커플링할 수 있습니다. 보통 몇 초 정도 걸립니다. 기기가 암호화되지 않은 경우 계속 진행하기 전에 암호화 과정이 시작됩니다.
11. 기기를 마스터 기기에 "맞부딪"혀 추가 기기를 계속 프로비저닝할 수 있습니다. 대상 기기에 시작 화면이 표시되어야 하고, 마스터 기기에는 “기기를 맞부딪히세요!” 화면이 표시되어야 합니다.

**QR 코드 프로비저닝의 경우 아래 단계 사용**

대상 기기에 Android 시작 화면이 표시되는지 확인합니다.

12. 대상 기기의 Android 시작 화면에서 화면의 같은 자리를 여섯 번 누릅니다.
13. 설정 마법사가 QR 코드 판독기를 대상 기기에 다운로드할 수 있도록 Wi-Fi 네트워크를 구성하라는 메시지가 표시됩니다.
14. QR 코드 판독기가 다운로드되면 카메라가 시작됩니다.
15. QR 코드가 성공적으로 스캔될 때까지 대상 기기를 마스터 기기 위에 약간의 거리를 유지한 채 둡니다. 그러면 설정 마법사가 클라이언트 앱 다운로드를 진행합니다. 클라이언트 앱을 다운로드할 수 없는 경우에는 공장 초기화를 자동으로 수행합니다.
16. 마스터 기기에서 QR 코드를 스캔하여 추가 기기를 계속 프로비저닝할 수 있습니다. 대상 기기에서는 카메라가 스캔할 준비가 되어 있어야 하고, 마스터 기기에는 "이 QR 코드를 스캔하세요" 화면이 표시되어야 합니다.
17. 공유 아이콘을 눌러 QR 코드를 내보낼 수도 있습니다. 내보내기 옵션은 기기마다 다릅니다.

## 클라이언트 토큰을 사용하여 Android Enterprise 기기 프로비저닝

NFC 범프 또는 QR 코드 방법을 사용하는 대신 브랜딩 클라이언트 토큰을 사용하여 기기 소유자 모드에서 Android Enterprise 기기를 프로비저닝할 수 있습니다. 이 방법을 사용하면 Go 또는 At Work 클라이언트의 자동 설치와 기기 소유자 모드에서의 프로비저닝을 수월하게 하는 토큰을 사용하여 기기에 로그온할 수 있습니다.

> 브랜드 클라이언트 토큰은 Android 6 또는 지원되는 최신 버전을 사용하여 관리되는 Google Play 계정이 프로비저닝된 기기에서 지원됩니다. 자세한 내용은 Android UEM 개발자 가이드를 참조하십시오. **https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.**

**이 방식을 사용하기 위한 요건:**

- Android Enterprise 계정으로 등록해야 합니다.
- 기기는 Android Enterprise를 지원해야 합니다.
- 기기가 Android 6 이상 최신 릴리스 버전을 사용해야 합니다.
- 새로운 기기 또는 공장 초기화된 기기가 있어야 합니다.

## 구성(Android 5.0+ 실행 기기)

**절차**

1. MDM용 Ivanti Neurons 포털에서 **구성**으로 이동합니다.
2. **+추가**를 클릭합니다.
3. **잠금 및 키오스크: Android Enterprise**를 선택합니다.
4. **잠금 및 키오스크 생성: Android Enterprise 구성** 페이지가 표시됩니다.

구성 이름 및 설명을 입력합니다.

5. 잠금 유형을 선택합니다.

**업무 관리 기기(기기 소유자)**를 클릭합니다.

6. Android 기기 소유자 잠금 설정 옵션이 표시됩니다.

필요에 따라 다음을 선택합니다.

- Wi-Fi 또는 Wi-Fi 설정 비활성화
- 카메라 비활성화
- Bluetooth 비활성화
- Bluetooth 설정 허용 불가
- 화면 캡처 비활성화
- 마스터 볼륨 음소거
- 앱 제어 금지
- 자격 증명 허용 불가
- 긴급 방송 허용 불가
- 모바일 네트워크 허용 불가
- 테더링 허용 불가
- VPN 허용 불가
- 공장 초기화 허용 불가
- 공장 초기화 보호 활성화.

> 필요에 따라 공장 초기화 후 기기를 프로비저닝할 수 있는 공인 Google 계정 ID(정수 값) 목록을 지정하거나 도움말 아이콘을 마우스로 가리켜서 공인 계정 ID 검색을 위한 도움말을 볼 수 있습니다.

계정 수정 금지

- NFC(플래시 불빛) 비활성화
- 발신 전화 허용 불가
- 안전 모드 허용 불가
- 위치 공유 금지
- 디버깅 기능 금지
- 앱 확인
- SMS 허용 불가
- 마이크 음소거 해제 허용 불가
- 자동 시간 비활성화
- 자동 표준 시간대 비활성화
- 데이터 로밍 비활성화
- Wi-Fi 절전 모드 비활성화
- 입력 방법 제한
- 접근성 서비스 제한
- USB 파일 전송 비활성화
- 외부 미디어 비활성화
- Keyguard 비활성화(PIN/비밀번호가 설정되어 있는 경우 효과 없음)
- 전원에 연결되어 있는 동안 화면 켜기 유지
- 창 생성을 허용하지 않음

- 최초 사용 힌트 건너뛰기

**시스템 앱 활성화/비활성화** 섹션에서, 필요에 따라 다음 시스템 앱을 활성화/비활성화하도록 선택할 수 있습니다.

7. 필요에 따라 **키오스크 모드** 활성화를 선택합니다.

| 항목 | 버전 |
| --- | --- |
| **시스템 앱 사전 설정** | |
| **내장 카메라** | 토글 버튼을 클릭하여 내장 카메라 앱을 **켜기** 또는 **끄기**로 설정합니다. |
| **내장 전화** | 토글 버튼을 클릭하여 내장 전화 앱을 **켜기** 또는 **끄기**로 설정합니다. |
| **시스템 앱 패키지 이름** | 사전 설정된 시스템 앱이 아닌 다른 시스템 앱을 활성화하거나 비활성화하려면 +(더하기) 아이콘을 클릭하고 시스템 앱 패키지 이름을 추가합니다. 시스템 앱을 제거하려면 -(빼기) 아이콘을 클릭합니다. |

다음과 같은 설정이 표시됩니다:

- 작업 잠금 모드 활성화
- 자동으로 키오스크 입력(최초 설정 시에만)
- 빠른 설정 비활성화
- Wi-Fi 설정에 대한 사용자 액세스 허용
- Bluetooth 설정에 대한 사용자 액세스 허용
- 위치 설정에 대한 사용자 액세스 허용
- 사용자의 애플리케이션 업데이트 지연 허용
- 날짜 및 시간 설정에 대한 사용자 액세스 허용
- 모바일 네트워크 설정에 대한 사용자 액세스 허용
- 사용자가 언어를 선택할 수 있음
- 공유 기기 활성화(다음 옵션 중 무엇이든 선택)
  - 로그인 활성화
  - 로그아웃 활성화(시간 제한을 시간 단위로 제시)

필요에 따라 드롭다운 목록에서 기본 또는 사용자 지정 브랜딩 옵션을 선택합니다.

8. 필요에 따라 키오스크 모드를 종료하기 위해 키오스크 종료 핀을 생성하여 사용합니다.
9. 필요에 따라 키오스크 모드에서 사용자가 사용할 수 있는 앱의 허용 목록을 생성합니다.

## 기기 프로비저닝

**절차**

1. 기기 전원을 켜고 Wi-Fi 비밀번호를 입력합니다. 기기에서 다른 비밀번호를 요구할 수도 있습니다.
2. **계정 확인** 화면에서 Android Enterprise 토큰을 입력합니다. **다음**을 클릭하세요.
3. **Google Services** 화면에서 **설치**를 클릭합니다.
4. 이용약관에 동의합니다.

5. 업무 기기 설정 화면에서 **다음**을 클릭합니다. Go 또는 At Work 클라이언트가 기기에 다운로드되고 설치됩니다. 기기가 이제 기기 소유자 모드로 전환됩니다.

**관련 주제**

- Android의 대량 등록 사용
- 기기 그룹

# 7.5.13. 작업 프로필이 있는 관리되는 기기

회사 소유 기기의 작업 프로필이 있는 관리되는 기기는 Android Enterprise 기기가 나머지와 구분되는 개인 데이터가 있는 기업 소유 기기인 모드입니다. 이 모드는 관리되는 프로필 내부에 작업 앱을 배포하고 개인적인 공간이 있는 사용자를 가질 수 있는 두 가지 프로필을 지원합니다. 회사 소유 기기의 작업 프로필이 있는 관리되는 기기 모드는 작업 프로필이 있는 관리되는 기기 구성을 기기 소유자 모드에서 프로비저닝되는 기기로 배포하여 생성됩니다.

작업 프로필 잠금 설정이 있는 관리되는 기기에 관한 자세한 정보는 **잠금 및 키오스크: Android Enterprise**를 참조하십시오.

> 이 모드에는 Android 8.0 이상 최신 릴리스 버전이 필요합니다.

앱 구성, 프로필에서 위젯을 공유하는 앱, 클라이언트 인증서 별명 및 ID 인증서는 작업 프로필이 있는 관리되는 기기에 적용될 수 있습니다.

다음 구성은 작업 프로필이 있는 관리되는 기기에 해당됩니다.

- 고급 암호
- Always On VPN
- 인증서
- ID 인증서
- Google 계정
- 암호
- Samsung 휴대폰 제한 사항
- 위협 방어
- Wi-Fi
- 기본 앱 런타임 권한
- SafetyNet 인증
- 암호
- Threat Defense 로컬 작업

# 7.5.14. Android의 대량 등록 사용

대량 등록 기능을 통해 여러 Android 기기를 MDM용 Ivanti Neurons로 신속하게 등록할 수 있습니다.

라이센스: Silver

대량 등록을 사용하기 전에 다음 작업을 수행하십시오.

1. Android 디버그 브릿지(adb)를 포함하는 Android SDK를 기기 등록에 사용되는 컴퓨터에 설치합니다.
   Android 디버그 브릿지에 대한 자세한 내용은 이 페이지(http://developer.android.com/tools/help/adb.html)를 참조하십시오.
2. USB 디버깅을 활성화합니다.
   Android 기기에서 USB 디버깅을 활성화하는 절차는 Android 릴리스에 따라 달라집니다. USB 디버깅 활성화에 대한 내용은 http://developer.android.com/tools/device.html을 참조하십시오.
3. 각 기기에 Go 클라이언트를 설치합니다.
4. USB 케이블을 통해 기기를 등록에 사용될 프로비저닝 컴퓨터로 연결합니다.

Go은(는) Android 디버그 브릿지(adb) 쉘을 이용하여 시작하고 서버에 등록할 수 있습니다. Android 디버그 브릿지는 Windows의 명령 줄에서, 또는 iOS의 Terminal 유틸리티에서 사용할 수 있는 툴입니다. 이를 통해 연결된 Android 기기와 통신할 수 있습니다. adb 쉘에서 명령 형식은:

> adb shell

$ am start -a android.intent.action.MAIN -d "mirp://na1.mobileiron.com?key=value&key=value" -n com.mobileiron.anyware.android/com.mobileiron.polaris.manager.ui.StartActivity

> 등록 프로토콜(**mirp**)은 등록을 위한 관련 데이터의 암호화에 사용됩니다.

유효한 키와 값:

| 키 | 값 |
|---|---|
| 사용자<br><br>비밀번호 | 사용자 이름 필드에 입력되었을 사용자의 이메일 주소(iReg를 사용하는 경우).<br>필요합니다.<br><br>사용자 비밀번호 |
| pin | 사용자 |
| quick Start | **TRUE로 설정된 경우:** 시작 화면이 나타나지만 잠시 후 사라집니다. 시작 화면에서 스피너가 계속 버튼으로 바뀌면 계속을 누를 필요 없이 화면이 자동으로 진행됩니다. 또한 다음과 같은 능률적 인 프로비저닝 흐름이 모든 장치에서 발생합니다.<br>• 사용자의 개인정보 보호 및 바로가기 프롬프트는 건너뜁니다.<br>• 제브라 기기에서 클라이언트는 사용자 프롬프트 없이 관리자 권한을 부여해야 합니다. Zebra MX 4.3의 최소 버전이 필요합니다.<br>**FALSE로 설정된 경우:** 평소와 같이 시작 화면이 나타나며 사용자는 시작 화면에서 계속을 눌러야 합니다. 필요에 따라 기본값은 FALSE가 됩니다. |

> 대량 등록을 사용하려면 비밀번호, PIN 또는 토큰을 사용해야 합니다.

이 명령 예는 서버, 사용자, 비밀번호, PIN 및 빠른 시작을 지정합니다.

am start -a android.intent.action.MAIN -d "mirp://ppp183.auto.mobileiron.com?user=miadmin@auto0001.mobileiron.com&password=P@$$W0R3&pin=12345&quickStart=true" -n com.mobileiron.anyware.android.qa/com.mobileiron.polaris.manager.ui.StartActivity

**샘플 대량 등록 스크립트**

자신의 대량 등록 스크립트를 설계할 때 사용할 예로 이 스크립트를 사용할 수 있습니다. 이 샘플 스크립트는 같은 사용자와 비밀번호로 프로비저닝 머신에 연결되는 모든 기기를 등록합니다.

```
for i in `adb devices | grep -v devices |
do
    echo "Registering $i"
    adb -s $i shell "am start -a android.intent.action.MAIN -d \"mirp://<servername?user=user email addresspassword=password
done
```

**잠재적 오류 메시지**

대량 등록을 사용할 경우 발생할 수 있는 오류는 다음과 같습니다.

| 오류 | 해결 |
|---|---|
| mirp 체계를 찾을 수 없음 | mirp 체계를 사용하는 명령의 예: am start -a Android.intent.action.MAIN -d "xxxmirp://? |
| 잘못된 URL | 데이터 문자열을 전혀 보내지 않은 경우에 발생합니다. URL이 올바른지 검증합니다. |
| 서버 정보를 찾을 수 없음 | 서버 정보가 누락되거나 잘못 입력되었습니다. |
| 사용자 정보를 찾을 수 없음 | 사용자 키가 입력되었는지 검증합니다. |
| 비밀번호/핀 정보를 찾을 수 없습니다. | 핀 또는 비밀번호 키가 입력되었는지 검증합니다. |

대량 등록을 위해 생성된 프로필이 여러 개인 경우:

- 기본적으로 등록된 완전 관리형 Android Enterprise 장치는 첫 번째 프로필로 생성된 사용자 지정 속성을 받습니다.
- 장치를 마이그레이션할 때 장치가 대량 등록 프로필에 있는 경우 대량 등록 프로필에서 마이그레이션하는 장치에 대해 정의된 사용자 지정 특성이 마이그레이션 시 장치에 적용됩니다. 이 동작은 첫 번째 프로필의 사용자 지정 특성을 받기 때문에 마이그레이션된 완전 관리형 Android Enterprise 장치에서도 동일합니다.

또한 해당 장치에 대해 생성된 모든 프로필은 활성 상태로 표시됩니다.

# 7.5.15. CSV 파일 업로드를 사용한 대량 등록

대량 등록을 통해 기기 식별자를 사용하여 여러 Android 기기를 등록할 수 있습니다. CSV 파일을 업로드하여 기기를 대량으로 추가하면 됩니다.

**절차**

1. **기기** 페이지에서 **대량 등록** 탭을 클릭합니다. **대량 등록** 페이지가 나타납니다.
2. **추가**를 클릭합니다.
3. **프로필 이름** 텍스트 필드에 프로필의 이름을 입력합니다. 필요에 따라 **+설명 추가**를 클릭하여 CSV 파일에 대한 설명을 입력합니다.
4. **CSV 업로드** 섹션에서 **CSV 템플릿 다운로드**를 클릭하여 CSV 템플릿을 다운로드합니다. 기존 형식을 이용하여 파일을 편집하여 기기를 추가할 수 있습니다.

> 대량 등록 CSV에서는 한 번에 최대 200,000개의 행이 허용됩니다.

5. CSV 파일을 편집하고 저장한 후 **CSV 업로드**를 클릭하여 CSV 파일을 업로드합니다. 업로드가 성공적이라는 확인 메시지가 표시됩니다.

> 행에 정보가 충분하지 않은 경우 CSV 업로드가 실패할 수 있습니다. 각 레코드에 일련 번호와 제조업체 정보(IMEI 값)이 있어야 하며, 그 외 기타 정보도 포함할 수 있습니다.

> 추가된 CSV 파일을 제거하려면 '빼기' 아이콘을 클릭합니다. 업로드할 다른 CSV 파일을 선택하려면 **다른 파일 선택** 링크를 클릭합니다.

6. 선택 사항: 토큰을 생성하지 않고 모든 유형의 기기를 대량 등록하려면 **토큰 없이 사용자 지정 속성 할당**을 선택하십시오. 이 옵션은 기본으로 선택 해제되어 있습니다.

업로드한 CSV 파일에 IMEI 또는 일련 번호 및 제조업체의 조합(사용자 지정 속성 포함 또는 비포함)이 제공되어 있으면 토큰 없이 대량 등록도 적용될 수 있습니다. 그러나 장치 등록은 CSV 파일에 업로드된 속성 값의 정확도에 따라 다릅니다. 다음 표는 대량 등록을 위해 입력한 속성 값 조합에 따른 결과에 대한 시나리오를 설명합니다.

| 시나리오 | 입력한 속성 값 | | | 기기 등록 상태 |
|---|---|---|---|---|
| | **IMEI** | **일련 번호** | **제조업체** | |
| 1 | 정확 | 부정확 | 부정확 | 기기가 등록됨 |
| 2 | 부정확 | 정확 | 정확 | 기기가 등록됨 |
| 3 | 부정확 | 부정확 | 정확 | 기기가 등록되지 않았습니다 |
| 4 | 부정확 | 정확 | 부정확 | 기기가 등록되지 않았습니다 |

> 제조업체 이름은 대소문자를 구분하지 않습니다.

7. **사용자 선택** 필드에서는 사용자를 반드시 선택해야 합니다.
   등록 토큰이 등록 토큰 열에 표시됩니다. 등록 토큰을 새로 고치려면 **새로 고침**을 클릭합니다.

토근의 만료 날짜가 **토큰 만료** 섹션에 표시됩니다. 토큰 만료 기간을 연장하려면 **연장**을 클릭합니다. **연장 일수** 필드에 토큰을 연장할 일수를 입력합니다.

> 지정 일수는 7~999 사이여야 합니다. 기본적으로 토큰은 7일 후 만료됩니다.
> **토큰 없이 사용자 지정 속성 할당** 옵션을 선택한 경우에는 이 페이지가 표시되지 않습니다.

8. **완료**를 클릭하세요.

업로드 후, 업로드된 CSV 파일의 다음 세부 정보가 **대량 등록 프로필** 페이지의 표에 표시됩니다.

| 설정 | 설명 |
|---|---|
| **프로필 이름** | 프로필의 이름 |
| **설명** | 간단한 프로필 설명 |
| **최종 수정** | CSV 파일의 최종 수정 날짜 |
| **유형** | 자체 관리 프로필 -> 자체 관리의 경우 |
| **기기 수** | 대량으로 등록하는 기기의 수 |
| **관련 사용자** | 관련 사용자의 이름 |
| **사용자 이름** | 기기와 연결된 사용자를 지정합니다. 기기-사용자 매핑이 활성화된 경우 필수입니다. 사용자는 MDM용 Ivanti Neurons 내에 있어야 합니다. |
| **작업** | 다음 작업을 수행할 수 있습니다.<br>**기존 인벤토리 다운로드** - 이 버튼을 클릭하면 프로필에서 사용 가능한 모든 기기의 세부 정보를 다운로드할 수 있습니다.<br>**보기** - 이 링크를 클릭하여 등록을 위해 대량으로 업로드한 프로필의 세부 정보를 봅니다.<br>**편집** - 이 버튼을 클릭하면 프로필 세부 정보를 편집할 수 있습니다. 이 옵션은 하나의 기기 옵션이 선택되어 있을 때만 사용 가능합니다.<br>**삭제** - 이 링크를 클릭하여 프로필을 삭제합니다. 확인 창에서 **예**를 클릭하여 업로드한 프로필이 삭제된 것을 확인합니다. |

> CSV 업로드 시 생성되는 토큰을 등록에 사용해야 합니다. 다른 토큰을 입력하면 ID/비밀번호를 입력해야 하는 일반 IReg 플로로 리디렉션됩니다.

## 작업

프로필 보기 세부 정보 섹션에서 대량 등록 프로필을 확인할 경우 프로필 보기 세부 정보 페이지의 작업 탭에서 다른 작업을 수행할 수 있습니다.

- **더 많은 장치 추가** - 이 옵션을 사용하면 프로필에 더 많은 장치를 추가할 수 있습니다. **IMEI 번호**나 **일련번호** 또는 둘 다, **제조업체**, 그리고 선택적으로 **사용자 정의 속성** 정보를 입력한 다음 **저장**을 클릭해야 합니다.
- **구성 수정** - 이 옵션을 사용하면 기존 구성을 수정할 수 있습니다. **Ivanti 전용 키**를 추가할 수 있습니다. **사전 정의된 Android System Extras** 또는 **사용자 지정 Android System Keys**를 변경한 후 **업데이트**를 클릭합니다.
- **QR 코드 생성** - 이 옵션을 사용하여 프로필 일괄 등록을 위한 QR 코드를 만들 수 있습니다.

- **토큰 새로 고침** - 이 옵션을 사용하면 토큰을 새로 고침하거나 토큰의 유효 기간을 연장할 수 있습니다. 유효기간은 7~999일 범위에서 설정하거나 **만료되지 않음**으로 설정할 수 있습니다.
- **연결된 사용자 변경** - 이 옵션을 사용하여 연결된 사용자를 변경합니다. **연결된 사용자 변경** 팝업 창에서 사용자를 검색한 후 선택하고 **적용**을 클릭합니다.
- **편집** - 이 옵션을 사용하면 선택한 프로필에서 기기를 편집할 수 있습니다. 기기를 선택하고 **편집** 버튼을 클릭해야 합니다.
- **삭제** - 이 옵션을 사용하면 선택한 프로필에서 기기를 삭제할 수 있습니다. 기기를 선택하고 삭제 버튼을 누르면 화면에 확인 팝업 상자가 표시됩니다. **삭제**를 클릭합니다.

> 자체 관리 기기는 서로 다른 기기 상태를 가집니다. **Samsung Knox 모바일 등록 사용**에서 더 자세한 내용을 확인할 수 있습니다.

# 7.5.16. Device_to_User_BulkEnrollment

File not found!

# 7.5.17. Samsung Knox 모바일 등록 사용

Samsung Knox 모바일 등록을 사용하면 관리자가 정규화된 Samsung 기기를 MDM용 Ivanti Neurons에 등록할 수 있습니다. Knox 모바일 등록을 사용하면 기기를 공인 리셀러에게서 최종 사용자에게로 곧바로 배송할 수 있으며 Go Android 클라이언트가 등록 데이터가 미리 채워진 상태로 다운로드됩니다. 자세한 내용은 **Android Enterprise용 Samsung Knox 모바일 등록**을 참조하세요.

## 요건

- IMEI별 기기 목록
- IMEI 또는 일련번호, 선택적으로 사용자 이름과 등록 비밀번호와 함께 기기 목록이 포함된 CSV 파일.
- MDM용 Ivanti Neurons(현재 릴리스).
- 모바일 등록을 위해 승인된 Samsung Knox 계정
- Samsung 지원 기기. Samsung 지원 기기 목록은 여기에서 확인할 수 있습니다.

# 7.5.18. Oculus 기기 등록

MDM용 Ivanti Neurons 은(는) 이제 Quest for Business 기기(Oculus 기기)를 관리할 수 있습니다. 현재 Meta는 MDM에 대해 OFB(Oculus for Business) 및 QFB(Quest for Business) 기기를 지원합니다. MDM에 대해 기기를 준비하고 MDM용 Ivanti Neurons에 등록하려면 Meta 콘솔에서 몇 가지 기본적인 작업을 수행해야 합니다.

Meta Workplace 콘솔의 기기 관리자에서 Oculus 기기 플릿을 등록할 수 있습니다. 등록된 이메일로 공유된 자격 증명을 사용하여 Oculus Business Workplace에 로그인해야 합니다. 홈 페이지의 기기 플릿 섹션에 모든 기기 정보가 표시됩니다. 기기 플릿 섹션에는 기기 관리에서 사용 가능한 모든 기기의 개요가 표시됩니다. 이러한 세부 정보에는 기기 이름, 기기 상태, OS(운영 체제), 모델 등이 포함됩니다.

이 섹션에는 다음 주제가 포함됩니다.

- Oculus 기기 등록의 전제 조건
  - 기기 관리자에서 MDM 앱 설정
  - Oculus 기기 설정

MobileIron Go로 OFB 기기 등록

  - MDM용 Ivanti Neurons 콘솔
  - Go 클라이언트

## Oculus 기기 등록의 전제 조건

### 기기 관리자에서 MDM 앱 설정

기기/헤드셋은 **Oculus for Business v28** 이상으로 프로비저닝 및 업데이트됩니다. Meta 콘솔의 기기 관리자에서 관리자는 MDM을 설정하고 특정 MDM 서비스에 Oculus 기기를 매핑해야 합니다.

**절차**

1. **Oculus Business Workplace**의 홈 페이지에서 **앱**을 선택합니다.
2. **앱 라이브러리**에서 설치할 제3자 MDM 앱을 클릭하고 **업데이트**를 클릭합니다.
3. **모바일 기기 관리** 아래의 목록에서 앱에 적절한 MDM을 선택하고 **앱 업데이트**를 클릭합니다.
4. MDM을 설치할 Oculus 기기 헤드셋을 클릭합니다. 화면에 기기 정보가 표시됩니다.
5. **정보** 탭에서 **모바일 기기 관리자**로 스크롤을 내립니다.
6. **MDM 권한** 옵션 옆의 **편집** 버튼을 클릭합니다.

> 기본값으로 Oculus 기기 관리자 옵션이 선택됩니다. MDM 권한 앱 목록에서 MDM 권한 앱을 선택하고 **MobileIron Go**를 선택해야 합니다.

**저장**을 클릭합니다. 기기가 자동으로 재설정되며, 설정 앱을 통해 Oculus 기기를 설정해야 합니다.

### Oculus 기기 설정

기기 설정 앱을 사용하여 Oculus Quest 2 헤드셋 기기를 추가할 수 있습니다. 필요한 사용자에게 이 앱을 공유해야 사용자가 각자의 Android 기기에서 앱을 다운로드하고 설치할 수 있습니다.

**절차**

1. **기기 플릿** 섹션에서 **구성되지 않은 기기**를 클릭합니다.
2. **설정 앱 가져오기**를 클릭합니다. 화면에 **다운로드 링크 보내기** 페이지가 표시됩니다.
3. 목록에서 하나 이상의 팀 구성원을 선택하거나 목록에서 **수신자 추가**를 클릭합니다.
4. **링크 보내기**를 클릭합니다. 선택한 사용자에게 **기기 설정** 앱 설치 링크가 포함된 이메일이 전송됩니다.
5. 이메일의 **기기 설정 앱 다운로드** 링크를 클릭하고 Android 기기에서 **기기 설정 앱**을 설치합니다.

> 다운로드가 완료되면 앱이 기기의 앱 스토어에 표시되지 않습니다. 기기의 다운로드 섹션에서 가져와 설치해야 합니다.

Android 기기에서 **Oculus for Business** 앱을 엽니다.

7. 전원 버튼을 2초간 눌러 Oculus 기기의 전원을 켭니다.
8. 블루투스를 켜고 설정이 완료될 때까지 Android 기기를 Oculus 기기 가까이에 둡니다.
9. Android 기기의 블루투스 기능을 사용하여 Oculus 기기를 검색합니다.
10. 필요한 Oculus 기기를 찾았다면 Wi-Fi 네트워크에 연결해야 설정을 완료할 수 있습니다.
11. **Wi-Fi 정보 입력**을 클릭하고 네트워크 이름과 암호를 입력한 다음 **저장**을 클릭합니다. 이제 Oculus 기기가 Wi-Fi 네트워크에 연결됩니다.
12. **설정 시작**을 클릭합니다. 화면에 설정이 진행 중이라는 알림이 표시됩니다. 설정 중에는 앱을 닫거나 헤드셋을 사용해서는 안 됩니다. 화면에 확인 메시지가 표시됩니다. **더 많은 기기 찾기** 버튼을 사용하여 더 많은 기기를 검색할 수 있습니다.

# MobileIron Go로 OFB 기기 등록

## MDM용 Ivanti Neurons 콘솔

MDM용 Ivanti Neurons 콘솔에서 MobileIron Go로 OFB 기기를 등록할 수 있습니다. 단, **구성** 아래의 업무 관리형 기기 및 업무 관리형 기기 - 비 GMS 모드(AOSP) 구성을 OFB 기기 그룹에 배포해야 합니다.

## Go 클라이언트

MobileIron Go 클라이언트에서 OFB 기기를 등록할 수 있습니다. OFB 기기를 등록하려면 다음 작업을 수행해야 합니다.

- OFB 설정 앱을 사용하여 설정을 완료한 후 화면에 표시되는 OFB 헤드셋 지침을 따라 기기 설정을 완료합니다.
- 자동으로 MobileIron Go 앱이 시작되며 로그인 자격 증명을 입력하고 MDM 지침을 따라 등록을 완료해야 합니다.

이제 기기가 DO 모드에서 프로비저닝되며 MDM에서 관리할 수 있도록 설정되었습니다.

# 7.5.19. 기기에 Bluetooth 활성화

**적용 가능 운영 체제:**

- iOS 11.3+
- macOS 10.13 4+

기기에 Bluetooth를 활성화하거나 비활성화할 수 있습니다.

**절차**

1. 기기 페이지에서 원하는 기기로 이동합니다.
2. 다음 작업 중 하나를 수행합니다.
    - 목록에서 해당 기기를 선택합니다.
    - 기기 이름을 클릭해 기기 상세 정보 페이지를 표시합니다.
3. **작업** 메뉴에서 **Bluetooth 활성화/비활성화**를 클릭합니다.
4. **확인**을 클릭하세요.

변경된 이름은 다음번에 기기가 체크인 시 기기에서 푸시됩니다.

# 7.5.20. iOS 업데이트 일정 설정

**적용 가능 운영 체제:**

- iOS 9.0+ 감독 기기 등록 기기
- iOS 10.3+ 감독 기기

최신 iOS 버전을 사용 가능할 때 iOS 기기 업데이트 일정을 설정합니다. **기기** > **작업** 메뉴 옵션인 현재 감독 대상인 iOS 기기의 **OS 버전 업데이트**는 기기에 적용 가능한 iOS 버전의 목록만을 표시합니다.

**절차**

1. 기기 페이지에서 원하는 기기로 이동합니다.
2. 기기 이름을 클릭해 기기 상세 정보 페이지를 표시합니다.
3. **작업** 메뉴에서 **OS 버전 업데이트**를 클릭합니다.
4. **OS 버전 업데이트** 마법사의 **버전으로 업데이트** 드롭다운 목록에서 iOS 버전을 검토하고 OS 버전을 선택합니다.

> 동일한 버전 또는 이전 버전을 입력할 경우, 대상 iOS 버전은 현재 버전보다 최신 버전이어야 함을 나타내는 오류 메시지가 표시됩니다.

5. **업데이트**를 클릭합니다.

장치를 체크인할 때 사용 가능한 최신 iOS 버전을 업데이트하도록 예약합니다. 장치에 암호가 있을 경우, MDM이 장치에 업데이트를 전송한 후 장치가 업데이트 대기열을 조정하며 사용자에게는 설치를 시작하려면 암호를 입력하라는 메시지가 표시됩니다. 자세한 내용은 **Software_Updates**를 참조하십시오.

# 7.5.21. iOS 시스템 앱 재설치

**적용 가능 운영 체제:**

- iOS 11.3+ 기기

iOS 기기에 삭제된 iOS 시스템 앱을 재설치합니다.

**절차**

1. 기기 페이지로 이동합니다. 아니면, 기기 이름을 클릭하여 기기 상세 정보 페이지에서 이 작업을 수행할 수 있습니다.
2. iOS 기기를 1개 이상 선택합니다.
3. **작업** 메뉴에서 **iOS 시스템 앱 재설치**를 클릭합니다.
4. iOS 시스템 앱 재설치 디스플레이 상자에서 기기에 설치될 사용 가능한 시스템 앱을 1개 이상 선택합니다.
5. **앱 재설치**를 클릭합니다.

기기가 체크인할 때 앱이 선택되고 호환되는 iOS 기기에 설치됩니다. 이러한 방식으로 설치된 시스템 앱은 관리 앱으로 간주되지 않습니다. 선택된 호환 가능 기기가 없을 경우, 시스템 앱이 해당 기기에 설치되지 않는다는 메시지를 받게 됩니다.

자세한 내용은 **Software_Updates**를 참조하십시오.

# 7.5.22. 새로운 사용자에게 기기 할당하기

사용자의 역할이 변경되거나 이전 사용자와 회사의 관계가 변경된 경우, 기존에 등록된 기기를 새로운 사용자용으로 다시 프로비전해야 할 수 있습니다. 이 단계는 기기를 폐기하고 다시 등록하는 번거로움을 없애줍니다.

**절차**:

1. 기기 페이지에서 원하는 기기로 이동합니다.
2. 기기 이름을 클릭해 기기 상세 정보 페이지를 표시합니다.
3. **사용자에게 할당**  아이콘을 클릭합니다.

> 또는 **기기** 페이지에서 기기를 선택하고 **작업** 메뉴에서 **사용자에게 할당** 옵션을 클릭할 수 있습니다.

**사용자 검색**에 사용자 이름 입력을 시작합니다. 제한합니다.

5. 원하는 사용자를 선택합니다.
6. **사용자에게 할당**을 클릭하세요.
   기기가 해당 사용자에게 프로비전됩니다.

> 사용자 기반 시나리오와 라이센스 기반 시나리오에서는 할당된 기기 제한을 초과하는 사용자에게 기기를 할당할 수 있습니다. 기기 제한 기능의 목적은 BYOD(Bring Your Own Device) 시나리오 지원에서 기기 등록을 제한하는 것이기 때문입니다.

기기 기반 및 사용자 기반 라이센스에서 기기 제한은 중요하지 않습니다. 기기 기반 라이센스의 경우, 시스템의 기기 합계가 변경되지 않으므로 최종 사용자의 비용이 변경되지 않습니다. 사용자 기반 라이센스는 이런 검사가 없기 때문에 오히려 고객에게는 이익입니다. 예를 들어, U1~U5까지 5명의 사용자가 있고 각각 기기가 5개라고 가정해 봅시다. 사용자 기반 라이센스에서는 5개의 라이센스가 사용됩니다. 대신 U4와 U5의 기기 2개를 U1과 U2로 이동하면 라이센스 사용량은 5개에서 3개로 줄어듭니다.

# 7.5.23. Android 기기 재할당

관리자는 Android 기기의 소유권을 한 사용자에서 다른 사용자에게 이전할 수 있습니다. 재할당 프로세스 중에 기기의 관리 프로필이 재구성되거나 현재 사용자에서 Android Enterprise 모드의 새 사용자로 다시 매핑됩니다. 재할당은 AMAPI(Android Management API) 기기를 제외한 모든 Android Enterprise 기기에서 수행할 수 있으며 Google Domain Android Enterprise 기기에서는 수행할 수 없습니다.

> 기기 재할당은 동일한 모드의 기기에서만 수행할 수 있습니다. 예를 들어 작업 관리형 기기 모드의 기기는 같은 모드의 다른 사용자에게 재할당할 수 있습니다.

기기 재할당 프로세스에는 다음과 같은 상태가 있습니다.

- 시작됨
- 성공
- 실패함
- 보류 중

**기기 세부 정보** 페이지 -> **개요** 탭 -> **마지막 재할당 상태**에서 기기의 마지막 재할당 상태를 볼 수 있습니다.

**절차**

1. **기기**로 이동합니다.
2. 목록에서 하나 이상의 기기를 선택합니다.
3. **작업** 목록에서 **사용자에게 할당**을 클릭합니다.
4. 또는 기기 이름을 클릭할 수 있습니다. **기기 세부 정보** 페이지가 열립니다. **사용자에게 할당** 아이콘을 클릭하여 사용자에게 할당 화면을 표시하고 필요한 사용자를 선택합니다.
5. **사용자에게 할당**을 클릭합니다. 선택한 기기를 선택한 사용자에게 재할당할 수 있는지 여부를 확인하기 위해 선택한 옵션의 유효성이 검사됩니다.
   유효성 확인 및 재할당에 성공하면 화면에 확인 메시지가 나타납니다.

> 최대 10개의 기기를 선택한 경우, 화면에 “할당 시작됨” 메시지가 나타납니다. 11개 이상의 기기를 선택한 경우, 화면에 “유효성 검사 진행 중” 팝업이 나타납니다.

> Android 기기 재할당은 이전에 등록한 사용자가 남긴 데이터를 제거하는 데 중점을 두고 고유하게 설계된 혁신적인 솔루션이며 SUEM-Premium SKU에서만 사용할 수 있습니다.

# 7.5.24. 기기의 강제 체크인

정보를 제공하고 수신하려면 기기를 MDM용 Ivanti Neurons에 연결(체크인)해야 합니다. 체크인 스케줄은 주기적으로 설정됩니다. 장치가 요청 시에만 체크인되도록 설정할 수도 있습니다. 장치가 강제로 체크인되도록 하면 {{설정}} 적용, {{정책}} 업데이트 등의 과정이 빨라집니다.

**절차**

1. **장치 > 장치**를 선택하세요.
2. 원하는 장치를 선택하세요.
3. **작업**을 선택하세요.
4. **강제 체크인**을 선택하십시오.
5. 선택적으로 장치 이름 링크를 클릭하여 장치 상세 정보 페이지로 이동하고 **강제 체크인**  **아이콘을** 클릭한 다음, **확인**을 클릭합니다.

> 기기에 결함이 있는 상태에서 체크인 중에 구성 설치 명령을 처리하면 MDM용 Ivanti Neurons는 나중에 체크인할 때 기기에 자동으로 구성 설치를 재시도하지 않습니다. 관리자는 기기의 기기 상세 페이지에서 수동으로 구성 설치를 다시 시도해야 합니다. 그렇게 하려면 구성 탭으로 이동하여 오류 구성을 선택한 다음, **설치 다시 시도**를 클릭하십시오.

# 7.5.25. 장치 위치 확인하기

장치 위치 확인 기능을 설정하면 해당 장치의 최근 위치가 표시됩니다. 위치 데이터 수집을 활성화하고 해당 구성을 기기에 적용하여 이 기능을 활성화하려면 **개인정보 보호 설정**을 편집해야 합니다. 해당 기기에서도 이 기능이 지원되어야 하며, 사용자는 위치 데이터 공유에 동의해야 합니다.

**절차**

1. **장치** 페이지에서 위치를 확인할 장치로 이동하세요.
2. **이름** 열의 링크를 클릭합니다.
3. **개요** 탭에서 **기기 위치** 아래의 링크를 클릭합니다.

페이지에 다음 상세 정보가 표시됩니다.

| 필드 이름 | 설명 |
| --- | --- |
| **마지막으로 위치를 찾은 시기** | 마지막으로 기기의 위치를 찾은 날짜 및 시간을 표시합니다. |
| **좌표** | 기기의 위도(북-남 위치) 및 경도(동-서 위치)를 표시합니다. |

페이지에도 기기 위치 지도가 표시됩니다.

# 7.5.26. 장치 잠금 설정하기

장치에 화면 잠금을 실행할 수 있습니다. 잠금 기능 지원 범위는 기기별로 다릅니다.

**절차**

1. **장치 > 장치**를 선택하세요.
2. 원하는 장치를 선택하세요.
3. **작업**을 선택하세요.
4. **잠금 설정**을 선택하세요.
5. 또는, 장치 이름 링크를 클릭하여 장치 세부 정보 페이지로 이동하고 **잠금**  아이콘을 클릭하고 **확인**을 클릭합니다.
6. AppConnect Android 앱의 경우, 잠금 명령을 사용하여 컨테이너에 들어오지 못하게 사용자를 잠그고 기기도 잠급니다. 사용자는 기기 암호와 AppConnect 암호를 사용하여 각각 기기와 AppConnect 앱에 다시 로그인할 수 있습니다.
7. iOS 7 기기의 경우, 화면에 표시할 메시지와 전화번호(선택사항)를 입력할 수 있습니다.
   해당 항목을 입력해 기기 사용자들에게 기기 잠금이 설정된 이유와 잠금 해제를 원할 경우 문의할 연락처를 제공할 수 있습니다.
8. macOS 기기의 경우, 기기에 액세스하려면 6자리 PIN 암호를 입력하라는 메시지가 표시됩니다. 화면 잠금을 진행하려면 기기 사용자가 다음을 수행해야 합니다.
   1. PIN을 입력합니다.
   2. 체크 박스를 선택해 기기 잠금을 확인합니다.
   3. **예, 잠금 설정 명령을 전송해주세요**를 클릭합니다.

> macOS에서 사용자는 기기 잠금 암호 설정 중 선택 사항인 잠금 화면 메시지와 전화 번호를 추가할 수 있습니다.

9. ChromeOS 장치의 경우 잠금 작업을 수행하면 "장치를 잠그면 사용자가 장치에 액세스하기 위해 암호를 입력해야 할 수 있습니다"라는 팝업 창이 화면에 나타납니다. **잠금**을 클릭하면 장치 상태가 **보내기 사용 안 함**으로 업데이트되고 정기 장치 동기화 완료 후 업데이트된 장치 상태가 표시됩니다.

기기 잠금 대체 방법

- 기기 사용자는 자체 서비스 포털을 통해 잠금 작업을 수행할 수 있습니다.
- 관리자는 관리자 포털에서 잠금 작업을 수행할 수 있습니다.

# 7.5.27. Apple 분실 모드에서 기기 관리하기

이 섹션에는 다음 주제가 포함됩니다.

- 분실 모드 활성화
- 분실 모드 작업 수행
- 분실 모드 비활성화

**적용 대상:** iOS 10.3+ 관리 상태인 기기.

MDM용 Ivanti Neurons을 통해 감독 대상 기기를 분실 모드로 설정할 수 있습니다. Apple 서버에 기기가 분실되었다고 보고하고 마지막으로 기록된 기기 위치를 조회할 수 있습니다. 기기를 발견하면 분실 모드를 비활성화할 수 있습니다.

## 분실 모드 활성화

기기를 분실 모드로 설정하면 Apple 서버에 분실 기기를 보고할 수 있습니다. 기기를 분실 모드로 설정한 이후:

- 기기가 폐기되었다면 분실 모드를 비활성화할 수 없습니다.
- 기기가 삭제되었다면 기기 위치를 확인하거나 추적할 수 없습니다.

**절차**

1. **기기**로 이동합니다.
2. 기기의 체크박스를 선택합니다.
3. **작업** > **공통** > **분실 모드 활성화**를 선택합니다.
4. 또는 기기 이름 링크를 선택하여 **기기 세부 정보** 페이지로 이동합니다. 기기의 작업 아이콘을 클릭하고 **분실 모드 사용**을 선택합니다.

## 분실 모드 작업 수행

분실 모드가 활성화되면 분실 기기 모드 섹션에서 다음과 같은 작업을 수행할 수 있습니다.

- 메시지/전화번호를 iPhone에 푸시
  - 분실 기기의 잠금 화면에 표시할 메시지를 입력합니다.
  - 분실 기기의 잠금 화면에 표시할 연락처를 입력합니다. 다른 사람이 기기를 발견하면 이 번호로 전화하여 보고할 수 있습니다.

장치 잠금 설정

- **기기 위치 새로 고침**

> 기기가 지워지면 기기 위치를 지정할 수 없게 됩니다.

- **분실 모드 사운드 재생**

> 사운드는 기기에서 분실 모드를 해제하거나 사용자가 기기에서 사운드를 비활성화할 때까지 재생됩니다.

- **위치 새로 고침**
  **위치 새로 고침** 옵션이 **분실 모드**에 추가되어 장치 위치를 볼 수 있습니다. 다음 세부 사항이 나타납니다.
  - **위도**: 장치 위치의 위도입니다.
  - **타임스탬프**: 페이로드의 시간 및 날짜 타임스탬프가 표시됩니다.

- **경도**: 장치 위치의 경도입니다.

## 분실 모드 비활성화

분실 모드로 설정한 기기를 찾거나 분실 모드를 잘못 활성화했을 때 분실 모드를 비활성화할 수 있습니다.

> 분실된 기기가 MDM용 Ivanti Neurons에서 사용 중지되면 분실 모드 비활성화가 작동하지 않습니다.

**절차**

1. **기기**로 이동합니다.
2. 기기의 체크박스를 선택합니다.
3. **작업** > **공통** > **분실 모드 비활성화**를 선택합니다.
4. 또는 기기 이름 링크를 클릭하여 **기기 세부정보** 페이지로 이동하고 **분실 기기 모드: 활성화됨** > **분실 모드 비활성화**를 선택합니다.

# 7.5.28. 분실 모드에서 Android 기기 관리하기

이 섹션에는 다음 주제가 포함됩니다.


- 분실 모드 활성화
- 분실 모드 비활성화


## 분실 모드 활성화

**적용 대상:** Android 8+ 기기

MDM용 Ivanti Neurons를 통해 여러 Android 기기를 분실 모드로 동시에 설정할 수 있습니다. 즉, 기기를 분실 모드로 설정하면 화면에 사용자 지정 메시지, 전화번호, 각주를 표시하고 사운드 재생 옵션을 표시함으로써 분실 기기를 MDM용 Ivanti Neurons에 신고할 수 있습니다.

> 이 기능은 GMS가 아닌 기기를 포함한 완전 관리형 기기만 지원합니다.

**절차**

1. **기기**로 이동합니다.
2. 기기의 확인란을 선택합니다.
3. **작업 > 분실 모드 활성화**를 선택합니다.
4. 또는, 기기 이름 링크를 클릭하여 기기 세부 정보 페이지로 이동하고 ⋮ 아이콘을 클릭합니다. **분실 모드 사용**을 선택합니다.
5. 분실 기기의 잠금 화면에 표시될 잠금 화면 메시지나 전화번호 또는 둘 다를 입력합니다. 관리자는 각주와 **분실 모드 사운드 재생** 옵션을 선택할 수도 있습니다. 누군가 기기를 발견하면 해당 번호로 전화해 신고할 수 있습니다.

> **분실 모드 활성화** 옵션을 활성화하려면 각 필드에 메시지 또는 전화번호를 입력해야 합니다.

> 분실 모드 사운드는 휴대폰이 잠금 해제되거나 통화 버튼이 눌리거나 관리자가 사운드가 재생되는 시간 내에 분실 모드를 비활성화하지 않으면 5분 동안 재생됩니다. 소리를 재생하려면 기기에서 분실 모드를 다시 활성화합니다.

6. Android 기기를 분실 모드로 설정하려면 **분실 모드 활성화**를 선택합니다.

분실 모드를 활성화하면 다음 작업이 비활성화됩니다:

- 잠금 해제
- 키오스크 입력/존재
- 공유 키오스크에 대한 강제 로그아웃
- 사용자에게 할당
- 메시지 보내기
- 소유권 설정

> 장치에서 분실 모드가 활성화되면 서버의 분실 모드 옵션이 비활성화됩니다.

## 분실 모드 비활성화

분실 모드에 있는 기기가 검색되거나 분실 모드가 실수로 활성화된 경우, 분실 모드를 비활성화할 수 있습니다.

분실 기기가 MDM용 Ivanti Neurons에서 지워지면 분실 모드 비활성화가 작동하지 않습니다.

**절차**

1. **기기**로 이동합니다.
2. 기기의 확인란을 선택합니다.
3. **작업 > 분실 모드 비활성화**를 선택합니다.
4. 또는, 기기 이름 링크를 클릭하여 기기 세부 정보 페이지로 이동하고 **분실 기기 모드: 활성화됨 > 분실 모드 비활성화**를 선택합니다.

**세부 정보** 섹션에서 **분실 모드 비활성화**는 **분실 모드 활성화**가 활성화된 후에만 표시됩니다. **분실 모드 비활성화**가 활성화되면 **분실 모드 비활성화** 옵션이 포함된 **분실 기기 모드: 활성화됨** 옵션이 사라집니다.

이전에 키오스크 모드에 있었던 기기는 분실 모드가 비활성화된 후 키오스크로 다시 진입해야 합니다.

# 7.5.29. 디버그 로그 요청

기기 문제 해결을 위한 디버그 로그를 검색하기 위해 iOS, macOS 및 Android 작업 관리 기기에 요청을 보낼 수 있습니다. 기기 페이지의 "디버그 로그 요청" 명령을 사용하면 이벤트의 작업 및 성공 또는 실패가 디버그 로그에 캡처됩니다.

이 기능을 사용하려면 다음 클라이언트가 필요합니다.

- iOS 기기에는 iOS용 Go 5.3.0 또는 지원되는 최신 버전이 필요합니다. Ivanti EPMM에서 MDM용 Ivanti Neurons(으)로 마이그레이션된 기기의 경우, 이 기능을 사용하기 위해 iOS용 Mobile@Work 12.2.0 또는 지원되는 최신 버전이 필요합니다.
- macOS 기기에는 macOS용 Mobile@Work 1.5 또는 지원되는 최신 버전이 필요합니다.
- Android 작업 관리형 기기에는 Android용 Go 65 또는 지원되는 최신 버전이 필요합니다.

**절차**

1. **장치 > 장치**를 선택하세요.
2. 기기를 선택하고 기기 이름 링크를 클릭하여 기기 상세 정보 페이지로 이동합니다.
3. ⋮ 아이콘을 클릭합니다.
4. **디버그 로그 요청**을 선택하고 **확인**을 클릭합니다.

요청이 전송되고 기기에 로그가 준비되면 알림이 관리자에게 전송되고 기기 로그에 표시됩니다. 기기 로그는 링크를 클릭하여 다운로드할 수도 있습니다.

# 7.5.30. Apple_Enhanced_Logging

File not found!

# 7.5.31. 장치 폐기하기

기기를 사용 중지하면 MDM용 Ivanti Neurons와의 관계가 종료됩니다. 다음과 같은 경우 장치 폐기가 필요할 수 있습니다.

- 사용자가 퇴사를 한 경우
- 사용자가 장치를 교체한 경우
- 완료된 관리 업무를 취소해야 하는 경우(처음부터 다시 시작)

**절차**

1. **장치 > 장치**를 선택하세요.
2. 원하는 장치를 선택하세요.
3. **작업**(우측 상단)을 클릭하세요.
4. **폐기**를 선택하세요.
5. 필요에 따라 기기 이름 링크를 클릭해 기기 상세 정보 페이지로 이동하고 ⋮ 아이콘을 클릭합니다.
6. **폐기**를 선택하고 **확인**을 클릭합니다.

> 활성 상태인 장치에서 사용 중지 작업을 수행하면 해당 장치의 사용이 즉시 중지됩니다.

# 7.5.32. 장치 소유권 포기

회사 소유 기기의 작업 프로필 모드에 있는 Android 기기에 해당됩니다.

회사 소유 기기의 작업 프로필 모드에 있는 기기의 소유권을 넘기면 개인 앱 및 데이터에 영향을 주지 않고 작업 프로필이 제거되며 MDM용 Ivanti Neurons에서 기기를 폐기합니다. 그러면 최종 사용자는 모든 기기 제어장치와 설정에 완전한 액세스 권한을 통해 개인 기기로 기기를 사용할 수 있습니다.

> Google Zero Touch 또는 Knox 모바일 등록 포털에서 장치를 제거해야 합니다.

다음과 같은 경우 기기 소유권 포기를 할 수 있습니다.

- 사용자가 퇴사를 한 경우
- 사용자가 장치를 교체한 경우

**절차**

1. **장치 > 장치**를 선택하세요.
2. 원하는 장치를 선택하세요.
3. **기기 상세 정보 페이지**를 클릭하고 ⋮ 아이콘을 클릭합니다.
4. **소유권 포기** 을 선택합니다.

# 7.5.33. 장치 지우기

기기를 지우면 모든 데이터가 삭제되고 기기는 초기화 설정으로 돌아갑니다.

**절차**

1. **장치 > 장치**를 선택하세요.
2. 원하는 장치를 선택하세요.
3. **작업**(우측 상단)을 클릭하세요.
4. **지우기**를 선택합니다.
5. 또는 기기 이름 링크를 클릭해 기기 상세 정보 페이지로 이동하고 ⋮ 아이콘을 클릭합니다. **지우기**를 선택하고 **확인**을 클릭합니다.
6. 기본적으로, **데이터 플랜 유지** 옵션이 선택되어 있습니다.
   (선택 사항, iOS 11.3+ 기기에 해당) **근접 설정 건너뛰기** 옵션을 선택합니다.
7. **서비스** 복귀 옵션을 선택하면 데이터가 삭제된 후 자동으로 다시 등록되기 때문에, 초기화 후 기기를 수동으로 다시 등록할 필요가 없습니다. DEP 모드로 등록된 iOS 17+ 기기에만 적용됩니다.
   1. 드롭다운 메뉴에서 **Wi-Fi 구성**을 선택합니다. 사용자는 모든 활성화 잠금을 비활성화해야 합니다. DEP 모드로 등록된 iOS 17+ 기기에만 적용됩니다.
   2. (선택 사항) 기존 앱을 유지한 상태로 기기를 서비스로 복귀시키려면 **앱 보존** 옵션을 선택합니다. Ivanti N-MDM을 통해 높은 우선순위로 설치된 앱만 유지됩니다. iOS 26+ 기기에만 적용됩니다.
8. macOS 기기의 경우 암호로 6자리 PIN을 기기에 전송할 수 있습니다. 기기에 액세스하려면 PIN를 입력하라는 메시지가 사용자에게 표시됩니다. 지우기 작업을 계속하려면 기기 사용자는:
   1. PIN을 입력합니다.
   2. 체크 박스를 선택해 기기 지우기 작업을 확인합니다.
   3. **예. 완전히 지워주세요**를 클릭합니다.
9. ChromeOS 장치의 경우 **장치 세부 정보** 또는 **장치 목록** 페이지에서 지우기 작업을 수행하면 "장치를 지우면 공장 설정으로 돌아가므로 장치의 데이터가 손실될 수 있습니다. 지우기 작업은 플랫폼마다 다릅니다."라는 메시지가 화면에 나타납니다.
   1. 장치 지우기 작업을 확인하려면 "지우기를 되돌릴 수 없다는 것을 이해하였습니다" 확인란을 선택합니다.
   2. **지우기**를 클릭하여 장치를 지웁니다.

> 장치 상태가 "**지우기 전송됨**"으로 변경됩니다. 업데이트된 장치 상태는 정기 장치 동기화 완료 후에 표시됩니다.

> Android Enterprise 기기에서는 기기 재부팅 후 여전히 잠긴 상태에서도 기기 **지우기** 작업을 수행할 수 있습니다.

> **지우기 보류 중** 상태인 Android 기기는 **기기 세부 정보** 페이지에 있는 **기기 삭제** 옵션으로 삭제할 수 있습니다. 일단 기기를 삭제하면 서버 연결이 끊기고 호환되지 않습니다. 따라서 공장 재설정 후 사용자가 기기를 재등록해야 합니다.

# 7.5.34. 기기 삭제

폐기한 장치는 삭제가 가능합니다. 장치를 삭제하면 해당 장치가 모든 페이지에서 제거됩니다. 상태가 폐기됨, 폐기 보류, 지워짐 또는 지우기 보류인 경우에만 기기를 삭제할 수 있습니다.

**절차**

1. **기기 > 기기**로 이동합니다. 화면에 기기 목록이 나타납니다.
2. 삭제하려는 기기를 선택합니다.
3. **작업**을 클릭합니다.
4. **공통** 섹션 아래에서 **기기 삭제** 옵션을 선택합니다. 화면에 팝업이 표시됩니다.
5. "삭제는 되돌릴 수 없다는 것을 이해합니다" 옵션을 선택한 다음 **기기 삭제**를 클릭합니다.
6. 또는 아래 단계에 따라 기기를 삭제할 수 있습니다.
    - **기기** > **기기**로 이동합니다.
    - **사용자 표시 이름** 열 아래에 있는 아무 링크를 클릭합니다. 화면에 **기기 세부 정보** 페이지가 나타납니다. **기기 세부 정보**를 클릭합니다. 화면에 팝업이 나타납니다. 경고를 확인하고 **확인**을 클릭하면 구체적인 기기가 삭제됩니다.

## 여러 기기 삭제

삭제하려는 기기를 모두 선택하면 여러 기기를 삭제할 수 있습니다.

**절차**

1. **장치 > 장치**를 선택하세요.
2. 사용 가능한 기기 목록에서 기기를 선택합니다.
3. **작업** 탭을 클릭하고 **공통** 제목 아래에서 **기기 삭제** 옵션을 선택합니다.
4. **기기 삭제** 창에서:
    1. **삭제는 되돌릴 수 없다는 것을 이해합니다** 확인란을 선택합니다.
    2. **유효한 기기 삭제**를 클릭하여 선택한 기기를 삭제합니다.

# 7.5.35. 장치 잠금 해제하기

이 섹션에는 다음 주제가 포함됩니다.

- Android 기기 잠금 해제
- Android 앱용 AppConnect 잠금 해제
- iOS 기기 잠금 해제
- ChromeOS 장치 잠금 해제

기기 잠금 해제 방법:

장치의 화면 잠금을 해제할 수 있습니다. 잠금 기능 지원 범위는 기기별로 다릅니다.

**절차**

1. **장치 > 장치**를 선택하세요.
2. 원하는 장치를 선택하세요.
3. **작업**을 선택하세요.
4. **잠금 해제**를 선택하세요.
5. 또는, 장치 이름 링크를 클릭하여 장치 세부 정보 페이지로 이동하고 **잠금 해제** 아이콘을 클릭하고 **확인**을 클릭합니다.

## Android 기기 잠금 해제

Unlock(잠금 해제) 명령이 수신되면 Android 앱은 암호 재설정을 시도합니다. 장치 관리자 및 장치 소유자 모드에서는 잠금 해제 코드가 재설정되는 반면, 프로필 소유자 및 회사 소유 개인 활성화 모드에서는 작업 프로필 잠금 해제 코드가 재설정됩니다.

Unlock(잠금 해제) 명령은 관리자가 영숫자의 조합으로 잠금 해제 코드를 설정할 수 있는 옵션을 제공합니다. 잠금 해제 코드를 '0000'으로 설정하는 기본 옵션은 여러 장치에서 수행할 수 있습니다. 그러나 새로운 옵션인 Android용 사용자 지정 잠금 해제 코드는 한 번에 하나의 장치에서 수행할 수 있습니다. 최소 문자 수는 6자, 최대 문자 수는 8자여야 합니다. 이 옵션은 **작업** 탭과 **장치 세부 정보** 페이지에서 사용할 수 있습니다. **작업** 탭 또는 **기기 세부 정보** 페이지에서 잠금 해제 옵션을 선택하면 다음 두 가지 옵션이 표시됩니다.

- 기본
- (Android만 해당) 잠금 해제 코드 제공 - 이 섹션에서 잠금 해제 코드를 제공하고 **잠금 해제**를 클릭할 수 있습니다.
    - 기기의 암호 재설정 프롬프트 건너뛰기 - 암호 구성이 기기에 푸시되는 경우 암호 재설정을 건너뛰도록 선택합니다.

잠금 해제 코드를 설정한 후 관리자는 **감사 시도** 페이지 및 **장치 로그** 페이지에서 잠금 해제 코드를 찾을 수 있습니다.

> Directboot 잠금 해제는 기본 잠금 해제 옵션인 '0000' 잠금 해제 코드에서만 작동합니다. 직접 부팅을 위한 사용자 지정 잠금 해제 코드는 지원되지 않습니다.

## Android 앱용 AppConnect 잠금 해제

AppConnect 앱의 경우 **AppConnect 잠금 해제** 명령은 사용자가 올바르지 못한 암호로 여러 번 로그인하려고 시도함으로 인해 잠긴 컨테이너를 잠금 해제하는 데 도움이 됩니다. 이 잠금 해제는 장치를 잠금 해제하지는 않습니다.

## iOS 기기 잠금 해제

iOS 앱은 잠금 해제 명령이 수신되면 해당 기기에서 암호를 제거합니다. **암호 설정**에 새로운 암호가 필요하다고 지정된 경우 암호 구성에 정의된 규칙을 준수하는 새 암호를 설정하라는 메시지가 표시됩니다. 사용자가 60분 안에 이 설정을 변경하지 않을 경우, 앱이 사용자에게 암호 재설정이 필요함을 알립니다.

## ChromeOS 장치 잠금 해제

ChromeOS 장치를 선택하고 **잠금 해제** 옵션을 클릭하면 화면에 팝업 창이 나타납니다. "잠금 해제 시 사용자가 장치에 액세스할 수 있도록 기존 암호가 지워질 수 있습니다. 잠금 해제는 플랫폼마다 다릅니다." **잠금 해제**를 클릭하면 장치 상태가 "보내기 잠금 해제"로 업데이트되고 해당 상태는 정기 장치 동기화 후 표시됩니다.

# 7.5.36. 기기 재시작/종료

이 섹션에는 다음 주제가 포함됩니다.

- 기기 재시작
- 기기 종료

**적용 대상:** Android 7.0+(관리형 기기), iOS 10.3+ 감독 모드, tvOS 10.3+ 감독 모드, macOS 10.13+, Windows 10+ 기기.

관리자는 기기 상세 정보 페이지에서 iOS 감독 모드 기기를 개별적으로 다시 시작하거나 종료하거나 기기 목록 페이지에서 대량 처리할 수 있습니다.

## 기기 재시작

**절차**

1. **기기**로 이동합니다.
2. 삭제할 장치로 이동하세요.
3. **이름** 열의 링크를 클릭합니다.
4. **작업** 버튼을 클릭합니다.
5. **기기 재시작/종료**를 클릭합니다.

> 지원되지 않는 기기는 다시 시작할 수 없습니다.

6. 화면에 표시된 경고 안내를 확인하세요.
7. (선택 사항) 재시작 시 기기 암호를 삭제하는 옵션을 선택합니다. 암호를 삭제하지 않으면 기기에 암호를 입력해야 합니다. 재시작 후, Wi-Fi에 연결할 수 없습니다.
8. 아직 **기기 재시작**을 선택하지 않았다면 선택합니다.
9. 그래도 기기 재시작을 원할 경우 **기기로 보내기**를 클릭합니다. 을 클릭합니다. 그렇지 않으면 **취소**를 클릭합니다.

> Android 기기의 경우 관리자는 기기 상세 정보 페이지의 **작동 시간**에서 기기의 재시작 시점에 대한 정보를 확인할 수 있습니다.

여러 대의 지원되는 기기를 **기기** 목록 페이지에서 다시 시작할 수 있습니다. 이렇게 하려면 기기를 선택하고 **작업 > 기기 재시작/종료**를 클릭한 다음, 화면의 지시를 따릅니다.

## 기기 종료

**절차**

1. **기기**로 이동합니다.
2. 삭제할 장치로 이동하세요.
3. **이름** 열의 링크를 클릭합니다.
4. **작업** 버튼을 클릭합니다.
5. **기기 재시작/종료**를 클릭합니다.

> 지원되지 않는 기기는 다시 시작할 수 없습니다.

6. 화면에 표시된 경고 안내를 확인하세요.
7. **기기 종료**를 선택합니다.
8. 그래도 기기 종료를 원할 경우 **기기로 보내기**를 클릭합니다. 을 클릭합니다. 그렇지 않으면 **취소**를 클릭합니다.

여러 대의 지원되는 기기를 **기기** 목록 페이지에서 종료할 수 있습니다. 이렇게 하려면 기기를 선택하고 **작업 > 기기 재시작/종료**를 클릭한 다음, 화면의 지시를 따릅니다.

# 7.5.37. 제한 비밀번호 삭제(iOS만 해당)

관리 상태인 iOS 8 기기에서 사용자가 설정한 제한 비밀번호를 삭제할 수 있습니다. 이 작업은 활성 장치에서만 사용할 수 있습니다.

**절차**

1. 장치 > 장치를 선택하세요.
2. 장치 항목을 선택합니다.
3. 작업 > 제한 비밀번호 삭제를 선택합니다.
4. 메시지가 표시되면 작업을 확인합니다.

# 7.5.38. 기기에 대한 Sentry 연결 삭제

기기에 대한 이메일 액세스를 제어하는 앱 터널링 또는 ActiveSync 활성화 이메일 시스템용 기기에 Sentry가 연결됩니다. 필요한 경우 다음과 같이 Sentry와 연결된 모든 기기의 연결을 끊을 수 있습니다.

**절차**

1. **기기**로 이동합니다.
2. **이름** 열에서 Sentry 연결을 삭제할 기기의 기기 링크를 클릭합니다.
3. **Sentry** 탭을 클릭합니다.
4. **작업** 열에서 **삭제**를 클릭합니다.

# 7.5.39. 장치에 사용자 지정 속성 할당

내부 ID와 같은 사용자 지정 기기 속성을 하나 이상의 기기에 할당할 수 있습니다. 각 속성에는 구성 및 기기 그룹 생성과 같이 작업에 사용할 수 있는 값이 있습니다. 생성된 사용자 지정 속성을 여러 장치에 할당할 수 있습니다. 속성 관리에 대해 자세히 알아보려면 속성을 참조하십시오.

**절차**

1. 관리 포털에 로그인합니다.
2. **기기**로 이동합니다.
3. 원하는 장치를 1개 이상 선택하세요.
4. **작업**을 선택하세요.
5. **사용자 지정 속성 할당**을 선택합니다.
6. 다음 옵션 중 *하나*를 선택합니다.
    - 기존 값을 발견한 경우에도 모든 속성을 강제 할당(덮어쓰기)합니다.
    - 값이 비어 있는 경우에만 덮어쓰기를 진행하며 기존 값이 있는 속성은 건너뜁니다.

할당하려는 속성을 선택하고 값을 입력합니다(빈 값은 허용되지 않음).

8. **할당**을 클릭합니다.

> **장치 세부 정보** 페이지에서 **사용자 지정 장치 속성**과 그 값을 CSV 형식으로 내보낼 수 있습니다.

# 7.5.40. 장치에서 사용자 지정 속성 제거

이 작업은 되돌릴 수 없으므로 신중하게 진행하십시오. 하나 이상의 장치에서 사용자 지정 속성을 제거하려면 다음을 수행합니다.

**절차**

1. **기기**로 이동합니다.
2. 원하는 장치를 1개 이상 선택하세요.
3. **작업**을 선택하세요.
4. **사용자 지정 속성 제거**를 선택합니다.
5. 제거할 속성을 선택합니다.
6. **삭제**를 클릭하세요.

# 7.5.41. 앱 피드백 동기화 및 가져오기

Android 기기에 설치된 앱에 요청을 보내 앱에 대한 현재 앱 구성 상태의 세부 정보를 받아볼 수 있습니다. 요청이 전송되면 기기에 대한 앱 구성 피드백 보고서가 수신됩니다.

**절차**

1. **기기**로 이동합니다.
2. 요청을 보내려는 기기를 클릭합니다.
3. **작업**을 선택하세요.
4. **앱 피드백 동기화 및 가져오기**를 선택합니다. 앱 구성 피드백을 동기화하고 가져오기 위한 요청이 전송됩니다. 클라이언트 마지막 체크인 옆에 있는 앱 피드백 마지막 동기화 필드가 업데이트됩니다.
5. **설치된 앱** 탭의 **앱 피드백** 열에서 앱의 **상세 정보 보기** 링크를 클릭합니다.**앱 피드백** 창이 표시됩니다.
   **키** - 상세한 정보를 제공하며, 앱으로부터 받은 피드백에 기반하여 앱의 관리형 앱 구성에서 보고된 설정의 배치를 제공합니다.
   **타임스탬프** - 키의 시간 및 날짜입니다.
   **심각도** - 키의 중요성을 지정합니다. 예: '정보', 오류'.
   **메시지** - 앱 구성 피드백으로부터 수신되는 메시지 유형입니다. 예: '실패'.
   **데이터** - 앱 구성 피드백으로부터 수신되는 데이터의 상세 정보입니다.

## App Catalog에서 앱 구성 피드백 보기

App Catalog에서 특정 앱에 대한 앱 구성 피드백 보고서를 볼 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 상세 정보를 보려는 앱을 선택합니다.
3. **앱 구성 피드백** 탭을 클릭합니다. **기기 수** 열에 앱 구성 피드백 보고서의 각 키에 대한 기기 수(하이퍼링크)가 표시됩니다.
4. 기기 하이퍼링크 수를 클릭하여 기기에 대한 상세 정보를 봅니다. 예를 들어, 하이퍼링크 5를 클릭하면 기기 5개에 대한 상세 정보가 표시됩니다. 다음 표 위에 표시되는 '키' 및 '심각도' 두 항목에 대해 다음 상세 정보가 표시됩니다.
   **이메일 주소** - 사용자 이름을 지정합니다. 사용자 이름 링크를 클릭하면 **기기 > 기기 상세 정보** 아래의 **설치된 앱** 탭으로 이동합니다.
   **기기 유형** - 기기 모델을 지정합니다.
   **OS** - Android OS 버전 번호입니다.
   **일련 번호** - 기기의 일련 번호입니다.
   **타임스탬프** - 마지막으로 업데이트된 시간 및 날짜입니다.
   **메시지** - 앱 구성 피드백으로부터 수신되는 메시지 유형입니다. 예: '실패'.
   **데이터** - 앱 구성 피드백으로부터 수신되는 데이터의 상세 정보입니다.

벨 아이콘(상단 우측)을 클릭하거나 **대시보드 > 알림** 페이지에서 Android 기기에 대한 앱 구성 피드백 오류 알림을 볼 수 있습니다. 알림 링크를 클릭해 **앱 구성 피드백** 탭을 탐색하여 앱 피드백 보고서를 볼 수 있습니다.

> 기기가 지워지거나 폐기되면 앱 구성 피드백 보고서가 제거되어 표시되지 않게 됩니다. 24시간마다 한 번 실행되는 배경 작업은 7일이 지난 데이터를 제거합니다.

# 7.5.42. 펌웨어 비밀번호 설정

**적용 대상:** macOS 10.13 또는 지원되는 최신 버전.

관리자는 macOS 기기에 대한 펌웨어(EFI) 비밀번호를 설정 또는 업데이트할 수 있습니다. 펌웨어 비밀번호를 통해 기기 사용자가 선택한 시작 디스크가 아닌 다른 내부 또는 외부 저장 기기로부터 macOS 기기 시작을 차단합니다. 결과적으로 대부분 시작 키 조합을 사용하는 기능도 차단하게 됩니다.

**절차**:

1. **기기**로 이동합니다.
2. 단일 기기의 펌웨어 비밀번호 설정 또는 변경:
    1. 기기 상세 정보 페이지를 보려면 기기와 연결된 사용자 이름을 클릭합니다.
    2. 일반 섹션에서 **펌웨어 비밀번호**를 확장하고 **비밀번호 설정**을 클릭하거나 기기 작업 메뉴에서 **펌웨어 비밀번호 설정/변경**을 클릭합니다.
    3. 이 섹션에서 다음 정보가 표시됩니다.
        1. **비밀번호:** 비밀번호 또는 가능한 비밀번호 목록.

            > 관리자가 펌웨어 비밀번호를 설정하면 명령이 기기로 전송됩니다. 기기가 시간 내에 응답하지 않는 경우 비밀번호가 일시적으로 저장되어 이 필드에 표시됩니다. 새 비밀번호는 기기가 이를 승인하고 기기가 재시작될 때까지 어떠한 영향을 미치지 않습니다. 그때까지는 모든 가능한 비밀번호가 표시됩니다. 기기가 재시작되고 비밀번호 변경이 승인된 이후에는 모든 원치 않는 비밀번호가 삭제됩니다.

        2. **변경 보류 중 -** 암호 변경이 보류 중인지 여부를 나타냅니다.
        3. **명령 상태 -** 암호 변경이 성공했는지 실패했는지 나타냅니다.
        4. **OptionROM 허용 -** 옵션 ROM을 활성화할지 여부가 나타납니다. 기본적으로 아니오로 설정됩니다.

하나 이상의 기기에서 펌웨어 비밀번호 설정 또는 변경:

1. 원하는 장치를 선택하세요.
2. 작업 메뉴에서 **펌웨어 비밀번호 설정/변경**을 클릭합니다.

현재 비밀번호와 새 비밀번호를 입력합니다.

처음인 경우 현재 비밀번호는 빈칸일 수 있습니다.

비밀번호를 재설정하려면 새 비밀번호를 빈칸으로 둡니다.

5. **저장**을 클릭하세요.

> 지원되는 macOS 버전의 기기만 새 비밀번호로 업데이트됩니다. 지원되지 않는 기기는 건너뜁니다.

# 7.5.43. 새 개인 복구 키 재발급하기

**적용 대상:** macOS용 Mobile@Work 1.66 이상 또는 지원되는 최신 버전이 있는 macOS 기기.

다른 MDM 솔루션에서 MDM용 Ivanti Neurons로 이동할 때, 관리자는 등록 전 개인 복구 키(PRK)가 이전에 발급된 경우 등록하자마자 새 PRK를 재발급해달라고 OS에 요청할 수 있습니다. 이는 키가 MDM용 Ivanti Neurons에 저장되도록 합니다.

PRK 작업에 대한 감사 내역 로그 항목을 다음과 같이 볼 수 있습니다.

1. **대시보드 > 감사 추적**으로 이동합니다.
2. 유형 필터에서 **개인 복구 키**를 선택합니다. PRK 항목은 “개인 복구 키 확인됨”과 같은 기기 관리 카테고리 및 활동에 표시됩니다.

**필수 조건**

이 절차를 수행하기 전에 기기에 다음 구성을 배포하십시오.

- macOS용 Mobile@Work 구성
- FileVault 복구 키 구성

**절차**

1. 지원팀에 문의하여 기기에서 새 PRK를 생성할 스크립트를 요청하십시오.
2. 스크립트에서 사용되는 이름 "deviceprk"가 포함된 기기 사용자 지정 속성을 만듭니다.
3. **관리 > 스크립트 및 파일 > 모든 스크립트**의 저장소에 스크립트를 업로드합니다.이 때 "deviceprk" 사용자 지정 속성을 선택하십시오.
4. 기존 MDM 솔루션에서 PRK가 회수되지 않은 기기에 대해 동적 기기 그룹을 만듭니다. 다음과 같이 기기 그룹 규칙을 선택합니다. "**Platform=macOS**, **암호화 기능 활성화는 예와 같음**, **macOS 개인 복구 키 에스크로됨은 아니요와 같음** 및 **macOS 복구 키 유형은 개인과 같음**."
5. 리포지토리에서 PRK 스크립트를 선택할 수 있는 macOS 스크립트용 Mobile@Work 구성을 만듭니다. 구성을 새 기기 그룹으로 배포하십시오.
6. 스크립트를 예약하여 하루 한 번 또는 원하는 대로 실행합니다. 이 스크립트는 매 실행 시 사용자 비밀번호를 요청합니다. 기본적으로, 스크립트 실행에 대한 시간 제한은 60초입니다. **최대 실행 시간** 필드를 300초로 설정하여 해당 macOS용 Mobile@Work 구성에서 제한 시간을 연장하는 것이 좋습니다.

- 암호화 해제된 키는 기기 암호화 상태 섹션에서 기기의 기기 상세 정보 페이지에서 사용 가능합니다. FileVault 암호화 활성화 필드 옆의 **보기**를 클릭하십시오.
- PRK를 획득할 때는 기기가 기기 그룹 밖으로 나옵니다. 따라서 스크립트 구성은 더 이상 적용되지 않으며 기기에서 삭제됩니다.
- MDM이 스크립트를 사용하여 기기의 복구 키를 회수한 후, 스크립트는 기기에서 설치 해제됩니다.

관련 주제:

- 속성
- 모든 스크립트
- 기기 그룹
- macOS용 Mobile@Work
- FileVault 복구 키

# 7.5.44. 복구 잠금 설정 또는 변경

**적용 대상:** macOS 11.5+

관리자가 Apple 실리콘에서 실행되는 macOS 기기에 대해 기기 재부팅 복구 잠금을 설정하거나 변경할 수 있습니다. 복구 잠금을 통해 암호를 입력하지 않으면 복구 모드에서 macOS 기기를 시작할 수 없습니다.

**절차**:

1. **기기**로 이동합니다.
2. 재부팅을 위한 복구 잠금 설정 또는 변경 방법:
    1. 기기 상세 정보 페이지를 보려면 기기와 연결된 사용자 표시 이름을 클릭합니다. 다음 작업 중 하나를 수행합니다.
    2. **개요** 섹션에서 **복구 잠금**을 확장하고 **비밀번호 설정** 또는 **비밀번호 변경**을 클릭합니다. 또는 **작업** 생략 부호를 클릭하고 **복구 잠금 설정/변경**을 클릭합니다.
    3. **복구 잠금 설정/변경** 대화 상자에서 다음을 수행합니다.
        1. **현재 비밀번호**: 여기에 현재 비밀번호를 입력합니다. 처음으로 설정하는 경우에는 공백을 유지하십시오.
        2. **비밀번호**: 설정하고자 하는 비밀번호를 입력합니다.
        3. **비밀번호 확인**: 설정하고자 하는 비밀번호를 다시 입력합니다.

**복구 잠금 설정/변경**을 클릭합니다.

> 개요에서 **복구 잠금 활성화됨**은 복구 잠금 암호의 상태를 나타냅니다.

> 관리자는 기존 암호를 제거하여 암호를 지우고 **복구 잠금 설정/변경**을 클릭할 수도 있습니다.

# 7.5.45. Apple 액세스 관리

**전제 조건**:

- Apple Business Manager 또는 Apple School Manager에서 도메인을 확인하고 잠금 설정합니다.
- MDM용 Ivanti Neurons에 관리형 Apple ID가 있는 Apple Business Manager 또는 Apple School Manager 조직에서 하나 이상의 MDM 서버를 구성합니다.

관리형 Apple ID에 로그인을 통해 조직에서 사용자가 액세스할 수 있는 Apple 서비스와 기능을 제어할 수 있습니다.

Apple Business Manager 또는 Apple School Manager에서는 설정에서 **관리형 Apple 계정 허용**은 사용자가 관리형 Apple ID로 로그인할 수 있는 위치를 제어합니다. 관리자는 이 설정을 관리형 기기 또는 감독 대상 기기에 로그인하도록 제한하거나 모든 기기에서 허용하도록 구성할 수 있습니다.

- **모든 기기**(기본): 사용자는 MDM 솔루션의 관리 여부에 관계없이 모든 기기에서 관리형 Apple ID로 로그인할 수 있습니다.
- **관리형 기기만 해당**: 사용자는 토큰 받기 엔드포인트를 지원하는 MDM 솔루션에서 관리하는 기기에서만 로그인할 수 있습니다.
- **감독 대상 기기만 해당**: 사용자는 토큰 받기 엔드포인트를 지원하는 MDM 솔루션에서 감독(및 관리)하는 기기에서만 로그인할 수 있습니다.

이 설정은 Apple Business Manager 및 Apple School Manager 내의 더 광범위한 Apple 서비스용 "액세스 관리"의 일부입니다.

> 보안 기능이 향상되어 관리형 또는 감독 대상 기기에 대한 로그인 제한은 제어형 기기에서만 업무 관련 데이터에 액세스할 수 있도록 하여 데이터 보안을 강화할 수 있습니다.

**기기 등록** 탭에 기기 등록 MDM 서버 조직이 없거나 여러 개이고, Apple Business Manager 또는 Apple School Manager에서 **액세스 관리** > **Apple 서비스** 아래 설정의 **관리형 Apple 계정 허용**이 "감독 대상 기기 전용" 또는 "관리형 기기 전용"으로 설정되어 있으면 관리형 Apple 계정 로그인에 실패합니다.

> MDM용 Ivanti Neurons 기기 등록 MDM 서버에 **관리형 Apple** 계정이 없으면 기기 로그인에 실패합니다.

# 7.5.46. 그룹 정책 등록

Windows 10/11 기기는 그룹 정책을 사용하여 MDM용 Ivanti Neurons에 등록할 수 있습니다. 그룹 정책을 생성하면 Azure AD에 하이브리드 방식으로 조인된 모든 기기가 자동으로 등록됩니다.

**Procedure그룹 정책으로 기기 등록하기**

| | |
|---|---|
| 1. | 기기가 **Azure AD에 하이브리드 방식으로 조인되어 있는지 확인합니다. 자세한 내용은 Microsoft 문서: Hybrid Azure AD 조인된 기기를 참조하십시오.** |
| 2. | **그룹 정책 개체를 생성합니다. 자세한 내용은 Microsoft 문서: 기기 그룹에 대한 자동 등록 구성을 참조하십시오.** |
| 3. | **등록할 기기를 포함하는 보안 그룹을 생성합니다. 자세한 내용은 Microsoft 문서: Active Directory 보안 그룹을 참조하십시오.** |
| 4. | **그룹 정책 개체를 보안 그룹에 연결합니다. 자세한 내용은 Microsoft 문서: 도메인에 GPO 연결을 참조하십시오.** |

## 사용자 경험

사용자가 Azure AD 자격 증명으로 기기에 로그인하면 Microsoft는 해당 조직에 속한 Azure AD 기반 MDM 구성을 찾습니다. 기기는 MDM용 Ivanti Neurons에 등록되어 있으며 정책과 명령을 받을 수 있습니다.

# 8. 앱

이 섹션에는 다음 주제가 포함됩니다.


- 앱 카탈로그
- Apps@Work
- iOS Apps@Work AppStore 기능
- 앱 상세 정보 보기
- 앱 구성
- 앱에 사용자 지정 속성 할당
- 관리되는 Android 구성
- Google Play 앱 관리
- App Catalog에서 앱 삭제
- 인하우스 앱 업그레이드
- Android 앱의 패키지 이름 찾기
- 범주
- 배포 필터
- 앱 제외 또는 배포
- 검토
- Apple Apps 및 Books
- 카탈로그 설정
- 앱 종속성 배포하기
- Android Enterprise로 Divide Productivity 배포
- Provisioner 앱 설정
- Windows 애플리케이션 관리
- Ivanti Bridge

# 8.1. 앱 카탈로그

이 섹션에는 다음 주제가 포함됩니다.


- 앱 기능 라이센스 관련
- 목록 및 그리드 보기 전환
- Android Enterprise에 대해 Google Play Store 앱 추가
- 공개 스토어에서 앱 추가 방법
- 인하우스 앱 추가
- Android Enterprise 인하우스 앱용 기기 권한 위임
- iOS용 인하우스 앱에서 프로비저닝 프로필 상태 표시하기
- iOS용 인하우스 앱에서 프로비저닝 프로필 업데이트
- 인하우스 앱을 Google Play에서 배포하기
- Android Enterprise 기기용 웹 앱 추가
- iOS 기기 웹 앱 추가
- 고급 검색 사용
- CSV 파일로 앱 내보내기


앱 카탈로그 페이지에서 앱 카탈로그를 관리할 수 있습니다. 앱 카탈로그에는 사용자들이 사용할 수 있도록 설정된 모바일 앱 목록이 제공됩니다. 여기에는 사용자가 공개 앱 스토어에서 다운로드할 수 있는 앱과 MDM용 Ivanti Neurons를 사용하여 배포하려는 앱(인하우스 앱)이 포함됩니다. 앱 카탈로그 페이지에서 AppConnect 지원 앱, iOS용 GoClient, macOS용 M@W 또한 비즈니스 앱으로 이용 가능하므로 구성 및 배포를 위해 가져오는 절차를 단순화합니다. MAM-Only 기기에서 App Catalog를 열 때 이 앱에 대한 액세스를 인증하기 위해 인증서를 선택하라는 메시지가 iOS 사용자에게 표시됩니다.

Apple의 M1 칩셋 MacBook은 iPhone 및 iPad VPP 앱을 지원합니다. 지원되는 iPhone 및 iPad VPP 앱을 푸시할 수 있는 사람은 관리자뿐입니다. 사용자는 App Catalog에서 설치하는 데 이 옵션을 사용할 수 없습니다.

Android 기기가 있는 MDM용 Ivanti Neurons 테넌트에 대해서는 Android Enterprise가 2021년 3월 말까지 활성화되지 않을 경우 관리자가 이름으로 앱을 검색할 수 없게 됩니다. 이 변경에 대한 전달은 App Catalog 페이지에 액세스할 때 배너 메시지로 표시됩니다. 이 배너 메시지는 이러한 테넌트에서 Android Enterprise가 활성화되고 '다시 표시하지 않음' 확인란 옵션이 선택되지 않을 때까지 계속 표시됩니다.

- 자동 앱 설치 방법은 공개 macOS 앱에서 사용할 수 없습니다. macOS 앱은 기기 기반 라이센스를 통한 Apple Apps 및 Books와 등록 시 자동 앱 설치를 통해 배포될 수도 있습니다.
- Ivanti Go 앱을 MDM용 Ivanti Neurons 서버에 업로드하는 동안 **관리형 앱으로 전환** 옵션을 선택해야 하는 경우, **기기에 설치** 옵션도 활성화해야 합니다.
- App Catalog 및 앱 설치는 Sonim XP5s 기기에서 지원되지 않습니다.
- Android에서는 활성 관리자 권한이 포함된 앱을 제거할 수 없습니다. 이 앱을 제거하려면 **기기 설정 > 보안 > 기기 관리자**로 이동해서 기기 관리자 권한을 비활성화합니다. 그 다음, 앱을 제거합니다.
- Android Enterprise Play Store를 통해 Android Enterprise 앱을 기기에 수동으로 설치한 경우, 관리자가 이후 앱의 배포를 중단하면 해당 앱도 수동으로 제거해야 합니다.
- 앱이 압축 또는 난독 처리되어 있는 경우에는 인하우스 Android 앱을 업로드할 수 없습니다.
- 공용 앱은 공유 iPad에서 지원되지 않습니다.
- Apple의 제한에 따라 앱 카탈로그에서 사용할 수 있는 B2B iOS 앱의 경우 **세부 정보** 탭에 앱의 설명과 스크린샷이 표시되지 않습니다.

- 앱 카탈로그는 관리 포털에서 앱을 검색할 경우 검색 결과는 **앱 이름**, **코멘트**, **설명**, **표시 버전**, **신규 사항**에 기반합니다. 검색한 앱 데이터가 이러한 필드와 일치할 경우 검색 결과로 표시됩니다.

## 앱 기능 라이센스 관련

다음 앱 카탈로그 기능을 이용하려면 별도의 라이센스가 필요합니다.

- 자동 앱 설치/제거: Silver 라이센스
- 퍼앱 구성: Gold 라이센스
- AppConnect 사용자 정의 구성: Gold 라이센스
- **Android Enterprise** 사용자 지정 구성: 실버 라이선스

Android 기기가 키오스크 모드인 경우:

기기가 키오스크 모드일 때는 인하우스 앱만 설치 가능합니다. 공개 앱을 설치할 수 있지만, 기기에서 키오스크 모드를 종료해야 이러한 앱을 설치할 수 있습니다. 또한 키오스크 모드의 기기에서 사용할 수 있는 앱을 제한하여 회사에서 승인하거나 허용 목록에 등록된 앱만 사용하도록 할 수 있습니다. Android 4.1을 사용하는 기기에서 승인된 앱이 허용 목록에 포함되지 않은 앱을 시작하는 경우 이 앱은 시작된 후에 즉시 최소화됩니다. Android 5.0을 사용하는 기기에서는 허용 목록에 포함된 앱에서 시작된 미승인 앱을 계속 사용할 수 있습니다.

## 목록 및 그리드 보기 전환

앱 카탈로그 화면 오른쪽에 있는 목록 또는 그리드 아이콘을 클릭합니다.

## Android Enterprise에 대해 Google Play Store 앱 추가

- Google Play 스토어의 앱을 앱 카탈로그에 추가하고 사용자가 사용할 수 있도록 할 수 있습니다. Android Enterprise에서 Google Play Store의 앱을 추가하려면, 앱이 App Catalog에 포함되도록 승인해야 합니다.
- Android Enterprise 기기용 Google Play 스토어 레이아웃에는 Core에서 관리되는 마이그레이션 기기에 대한 홈페이지와 MDM용 Ivanti Neurons에서 관리되는 모든 애플리케이션을 표시하는 MDM용 Ivanti Neurons로 연결되는 빠른 링크가 있습니다. Core에서 MDM용 Ivanti Neurons로 Android Enterprise 기기를 마이그레이션하면 Core와 MDM용 Ivanti Neurons 앱 카탈로그 간에 공통적인 애플리케이션만 기기의 작업 프로필 Google Play 스토어에 나열됩니다. MDM용 Ivanti Neurons 버튼을 클릭하면 MDM용 Ivanti Neurons 앱 카탈로그에서 사용 가능한 모든 애플리케이션 목록을 볼 수 있습니다.

Android Enterprise 기기용 Google Play 스토어 레이아웃에는 Core에서 관리되는 마이그레이션 기기에 대한 홈페이지와 MDM용 Ivanti Neurons에서 관리되는 모든 애플리케이션을 표시하는 MDM용 Ivanti Neurons로 연결되는 빠른 링크가 있습니다. Core에서 MDM용 Ivanti Neurons로 Android Enterprise 기기를 마이그레이션하면 Core와 MDM용 Ivanti Neurons 앱 카탈로그 간에 공통적인 애플리케이션만 기기의 작업 프로필 Google Play 스토어에 나열됩니다. MDM용 Ivanti Neurons 버튼을 클릭하면 MDM용 Ivanti Neurons 앱 카탈로그에서 사용 가능한 모든 애플리케이션을 볼 수 있습니다.

**필수 조건**

- Google Play Store 애플리케이션에 액세스하여 이를 App Catalog에 추가하려면 Android Enterprise를 활성화해야 합니다.

**Procedure절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **추가**를 클릭합니다(좌측 상단).

> 드롭다운 목록에서 Google Play를 선택하여 Google Play Store에서 앱을 검색합니다. Android Enterprise가 등록되면 Google Play iFrame이 표시됩니다.

3. 검색 필드에서 앱을 검색하고 앱을 클릭합니다.
4. **완료**를 클릭하세요.

승인된 앱은 추후 **승인되지 않음**을 클릭하여 승인을 취소할 수 있습니다.

| 옵션 | 설명 |
| --- | --- |
| **승인 설정** | |
| 앱에서 새로운 권한 요청 시 승인 상태 유지 | 사용자가 업데이트된 앱을 설치하도록 허용 |
| 이 앱에서 새로운 권한 요청 시 앱 승인 철회 | **다시 승인될 때까지 스토어에서 앱을 제거합니다.** |
| **승인 설정** | |
| 구독자 추가 | 승인한 앱에 새로운 권한이 필요할 때 이메일 주소를 입력하여 이메일로 알림을 보낼 구독자를 추가합니다. |

## 공개 스토어에서 앱 추가 방법

공공 스토어에서 App Catalog로 앱을 추가하고 사용자가 이용할 수 있도록 할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **추가**를 클릭합니다.
3. 원하는 앱을 선택하세요.
4. 해당 앱스토어를 선택합니다.
5. 앱 이름을 입력합니다.
6. 목록에서 해당 앱을 선택합니다.
7. **다음**을 클릭하세요.
8. 앱 정보를 입력하세요.
9. 범주를 추가 또는 삭제합니다.
10. 필요한 경우 간략한 설명을 입력합니다(선택사항).
11. **다음**을 클릭하세요.
12. 앱 배포 관련 설정을 하세요.
13. 배포 방법을 선택하세요.
14. **고급 옵션 및 앱 구성** 섹션을 확장합니다.
15. 다음 지침을 사용하여 옵션을 완료합니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 기기에 설치 | 이 옵션을 선택하면 등록 후에 바로 설치를 시작합니다. 다음 상황을 제외하고 사용자에게 앱 설치를 확인하라는 메시지가 표시됩니다.<br>• 이 기기는 새로운 앱 설치와 앱 업데이트를 위한 관리 상태인 iOS 기기입니다.<br>• 이 기기는 앱 업데이트를 위한 iOS 비감독 기기입니다.<br>• Apps 및 Books 프로그램에 등록된 사용자입니다.<br>• 이 기기는 Samsung Knox 기기이며 아래의 자동 설치 옵션이 선택되었습니다.<br>iOS 공개 앱의 경우 기기에 처음 설치되면 App Catalog에 사용자가 앱을 다시 설치할 수 있는 "재설치"버튼이 표시됩니다.<br>기기에 설치된 앱 버전이 iOS App Store에 있는 버전과 다르면 재설치를 수행합니다. |
| 최종 사용자 App Catalog에서 앱 표시 안 함 | 사용자가 기기에 있는 앱 카탈로그에서 앱을 보기를 원하지 않는 경우 이 옵션을 선택합니다. |
| 앱 설치 우선 순위 설정 | 사용자 온보딩 중에 앱 설치 우선순위를 설정하기 위해 높음, 중간, 낮음 중에서 선택합니다. 사용자 온보딩 중에 높은 우선순위 앱만 설치됩니다. |
| 실패 시도 횟수를 초과한 후 앱 다시 푸시 일시 중단(iOS만 해당) | 다시 푸시 시도가 설정된 횟수만큼 실패한 후에는 다음 설정을 사용하여 토글 스위치를 ON으로 전환하여 앱 다시 푸시를 일시 중단합니다.<br>**다음 횟수 이후 다시 푸시 중지** - 다시 푸시가 중단될 다시 푸시 시도 실패 횟수를 입력합니다. 입력한 값은 **1**~**999**여야 합니다.<br>**시도 실패 및 다음 시간 이후 다시 시도** - 다시 푸시가 실패한 후 다시 푸시를 다시 시도할 수 있는 시간 간격을 입력합니다. 입력한 값은 **3**~**48**시간이어야 합니다. |
| (Android만 해당) Samsung Knox 기기에 자동 설치 | 이 옵션은 공개 앱에 적용되지 않습니다. |
| (iOS 및 macOS만 해당) 이 앱에 대한 퍼앱 VPN 활성화 | 이 옵션을 선택하면 이 앱에서 **퍼앱 VPN 구성**을 사용합니다.<br>드롭다운 목록에서 사용할 퍼앱 VPN 구성을 선택합니다.<br>macOS의 경우 Tunnel 퍼앱 VPN 구성만 선택하십시오. |
| (iOS만 해당) iCloud와 iTunes 백업 차단 | 이 옵션을 선택하면 이 앱과 관련된 데이터가 iCloud와 iTunes에 백업되지 못하게 합니다. |
| (iOS만 해당) 미등록 앱 제거 | MDM용 Ivanti Neurons에서 더 이상 기기를 관리하지 않으면 이 옵션을 선택하여 이 앱을 삭제합니다. |
| (iOS만 해당) AppConnect 사용자 지정 구성 | AppConnect 지원 앱의 경우, 사용자 지정 구성 기본 설정을 지정하는 키와 값을 입력합니다. 사용 가능한 키에 관한 정보는 해당 앱 관련 문서를 참조하십시오. |
| iOS 7+ 관리되는 앱 설정 | iOS 7+ 관리 앱으로서 이 앱에 지정된 키와 값을 입력합니다. 지원되는 키에 관한 정보는 해당 앱 관련 문서를 참조하십시오. |

> **Android Enterprise** 앱에는 다른 옵션이 있습니다.

**다음**을 클릭합니다.

4. 프로모션 방법을 선택합니다.

5. **+설명 추가**를 클릭하여 구성에 대한 간단한 설명을 입력합니다.

- 추천 안 함
- 추천 리스트
- 추천 배너
- 추천 배너를 선택한 경우 다음 세부 정보를 지정합니다.
    1. **제목** - 애플리케이션 제목을 지정합니다.
    2. **설명** - 애플리케이션 세부 정보를 지정합니다.
    3. **배너 스타일** - 배너 색상을 선택합니다.

6. 필요에 따라 구성 배포를 변경합니다.
7. **완료**를 클릭하여 앱 구성을 저장합니다.
8. **완료**를 클릭하세요.

> 앱 카탈로그에서 Windows 앱을 검색할 때 **앱 이름**을 이용하거나 드롭다운 목록에서 **AppStore ID** 옵션을 이용하면 일치하는 앱을 검색할 수 있습니다.

- **앱 이름** - 이 옵션을 선택하고 앱 이름 입력
- **AppStore ID** - 이 옵션을 선택하고 AppStore ID 입력

Windows 스토어 앱 검색은 Win32 스토어 앱을 지원합니다.

Win32 스토어 앱을 관리하기 위해 장치에서 Winget 도구를 사용할 수 있는지 확인하십시오.

## 인하우스 앱 추가

다음 파일 형식으로 인하우스 앱을 앱 카탈로그에 업로드할 수 있습니다. 대용량 파일은 업로드하는 데 몇 분 정도 걸릴 수 있습니다. 인하우스 애플리케이션 버전의 수는 100개로 제한됩니다. 해당 수가 초과되면, MDM용 Ivanti Neurons 시스템이 가장 오래된 버전의 애플리케이션을 제거합니다. 애플리케이션 업로드 및 제거 상태가 표시되며 감사 내역 페이지에서 볼 수 있습니다.

Mobile@Work에서 반환한 MIP 앱 인벤토리는 몇몇 앱에서 정확하지 않을 수 있습니다. Mobile@Work은 기본 위치에 설치되지 않은 앱의 설치 상태를 감지하지 못할 수도 있습니다. 그런 앱의 경우 감지 스크립트를 추가하면 기기에 설치된 앱의 올바른 상태를 식별하는 데 도움이 됩니다. Mobile@Work는 감지 스크립트의 종료 코드가 0인 경우 앱의 존재 여부를 결정합니다. 다른 종료 코드의 경우에는 앱이 설치되지 않은 것으로 결정됩니다. 감지된 앱을 토대로 Mobile@Work는 기기에 대한 인벤토리 보고서를 준비합니다.

- IPA (iOS)
- MIP(Packager macOS 앱)
- PKG (macOS)
- APK (Android)
- APPX, APPXBUNDLE, EXE 및 MSI(Windows)

> 스크립트를 사용하는 PKG나 스크립트를 사용하는 PKG가 있는 DMG 같은 애플리케이션의 경우 macOS용 Mobile@Work는 성공적인 설치 요청만 감지합니다. 앱이 삭제되었거나 설치된 스크립트가 제거되었을 경우 보고되지 않습니다. 따라서 MDM용 Ivanti Neurons 서버로부터 설치 명령이 다시 전송되지 않습니다. 앱 다운로드 도중 연결이 끊어질 경우 체크인을 실행하여 앱을 다시 설치하십시오. MIP 앱의 경우 PKG나 스크립트를 사용하는 PKG가 있는 DMG를 통해 설치된 기기에서 앱이 제거되더라도 클라이언트 기기의 수신 폴더에 PKG 항목이 있으면 Mobile@Work는 MIP 앱을 설치하지 않습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **추가**를 클릭합니다(좌측 상단).
3. **파일을 업로드할 플랫폼을 선택합니다**에서 플랫폼 카테고리(예: **Apple 앱**)를 선택하고, 특정 OS(예: Apple 앱의 드롭다운에서 iOS 또는 macOS)를 선택합니다.

> 사용자가 플랫폼을 선택한 후 충돌하는 파일 유형을 업로드하려고 하면(예: Apple 선택 후 .apk 업로드), 시스템은 "Not a valid file format" 오류를 트리거합니다.

4. 앱 파일을 점선 박스로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다. 그리고 **확인**을 클릭합니다.
5. **다음**(우측 하단)을 클릭합니다.
6. 사용자용 앱 정보를 입력하고 필수 설치 앱을 구성합니다.
7. 범주를 추가합니다.
8. macOS 패키지를 추가할 때 해당 패키지 파일이 한 개 이상의 앱을 포함하는 경우(예를 들면, Microsoft Office와 Cisco AnyConnect 패키지) 선택한 기본 앱은 패키지가 설치되었는지를 식별하는 데 사용됩니다. 구성되어 있는 경우 퍼앱 VPN이 이러한 앱에 적용됩니다.
9. 필요한 경우 간략한 설명을 입력합니다(선택사항).
10. **MSI 제품 코드**: MSI 앱을 업로드할 때 MSI 앱의 제품 코드가 이 필드에 자동으로 채워집니다.

> 올바른 GUID가 입력되었는지 확인하려면 "MSI 제품 코드를 확인했습니다"라는 옵션을 선택해야 합니다.

**오버라이드 URL:** 선택 사항인 앱 소스 URL 오버라이드를 입력하여 다른 소스에서 앱을 다운로드하거나 로컬 네트워크(HTTP 및 HTTPS)에서 Microsoft Office 설치 매체와 같은 큰 파일을 받는 것을 허용할 수 있습니다. 이 옵션을 사용하려면 보안 내부 네트워크에 액세스하고 앱이 저장된 대체 서버에서 수동으로 동기화해야 합니다. 필요한 인프라를 설정하기 전에는 값을 입력하지 마십시오. 특정 앱에 대한 앱 설정을 편집하면서 이 값을 편집할 수 있습니다.

- iOS 앱의 경우 앱 우선 적용 URL은 HTTP 또는 HTTPS 형식이어야 합니다.
- Android 및 macOS 앱의 경우 앱 우선 적용 URL은 HTTPS 형식이어야 합니다.
- macOS 앱의 경우, URL은 .pkg 확장자로 끝나야 합니다.

6. **명령 줄**(Windows 32비트 MSI 앱 전용): 명령 줄 스위치를 입력하여(선택 사항) MSI 파일을 배포하는 동안 패키지에 포함되지 않는 추가 정보를 지정할 수 있습니다. 예를 들어 출력 파일에 설치 로그를 작성하려면 이 필드에 "/log output.txt"를 입력할 수 있습니다. C:\Windows\System32 폴더에 output.txt 파일이 생성됩니다. 기본적으로 자동 설치를 위한 명령 줄 옵션 /qn은 MSI 앱 업로드 중에 자동으로 채워집니다.

> 업로드될 MSI 앱의 패키지 이름은 명령 줄 인수의 일부로 추가될 수 없습니다. 추가된 경우에는 앱의 패키지 이름이 명령 줄 인수에서 제거될 때까지 업로드가 제한됩니다. 지원되는 명령 줄 옵션의 전체 목록은 추가 링크에 제공됩니다. 이 링크는 앱의 보기 및 편집 모드에서 볼 수 있습니다.

Win32용 .EXE: 관리자 PowerShell 모드를 사용하여 Bridge를 통해 설치됩니다. 사용 가능한 경우 Bridge 기능이 자동 사용됩니다.

- **디스플레이 버전**과 **번들 버전** 간 일관성을 유지하는 업데이트 버전
- 설치 프로그램(.EXE) 위치
- 설치 프로그램 명령줄 매개변수: 파일을 자동으로 실행하는 인수(예: /SILENT 또는 /VERY SILENT)는 필수입니다.
- 설치 프로그램은 사용자로 실행: 사용자의 자격 증명을 사용하여 설치하려면 '사용자 권한으로 실행' 옵션을 선택합니다.

Win32 스토어 앱용: 관리자 PowerShell 모드를 사용하여 Bridge를 통해 설치됩니다.

9. Packager macOS 앱의 경우 필수 설치 앱(선택 사항)을 구성합니다. 필수 설치 앱 기능에 대한 개요는 Packager 인하우스 macOS 앱 이해를 참조하십시오.
10. **URL 실행**: AppStation에서 앱을 실행하기 위한 사용자 지정 URL을 입력합니다. AppStation을 사용해 MAM-only 배포 시 AppConnect가 지원되지 않는 앱을 추가하는 경우에만 필요하며 iOS 앱에만 적용됩니다.
11. 앱 위임을 구성합니다.

> 필수 설치 앱을 위임하고 나면 기본 공간이 아닌 공간의 앱에 대한 필수 설치 앱이 되며 필수 설치 관계부터 제거해야만 해당 앱의 위임을 해제할 수 있습니다.

**다음**을 클릭하세요.

13. **다음**을 클릭하세요.
14. (선택사항) 해당 앱의 화면 캡처를 추가합니다.
15. (선택 사항) 앱(iOS, MacOS 및 Windows 앱)의 아이콘을 추가 또는 교체합니다.
16. **다음**을 클릭하세요.
17. Packager macOS의 경우 앱 설치 전 및/또는 후에 실행할 설치 스크립트를 정의하거나 선택합니다. 검색 상자에 입력하거나 링크를 클릭하여 스크립트 목록을 확인하여 다음 스크립트 중 하나 또는 둘 모두를 선택합니다 **다음**을 클릭합니다.
18. 스크립트는 **관리 > 스크립트 및 파일 > 모든 스크립트** 페이지에서 생성할 수 있습니다. 앱을 업그레이드하는 경우 이전 앱에서 스크립트를 복사하여 스크립트를 실행함으로써 앱을 업그레이드할 수 있습니다. 이 섹션을 건너뛰면 앱을 나중에 편집하여 스크립트를 구성할 수 있습니다.

- **스크립트 사전 설치** - 앱 설치 전에 스크립트 이름을 입력하여 실행할 스크립트를 선택합니다. 스크립트 사전 설치는 클라이언트로부터 스크립트 실행 성공 상태가 수신될 때까지 실행되거나 재시도됩니다. 그 이후에만 앱 설치 명령이 발송됩니다. **로그** 탭의 기기 상세 정보 페이지에서 스크립트 실행 현황을 볼 수 있습니다.
- **스크립트 사후 설치** - 앱 설치 후에 스크립트 이름을 입력하여 실행할 스크립트를 선택합니다.
- **스크립트 설치 해제**: 서버에서 앱이 더 이상 장치에 배포되지 않음을 감지할 때 서버가 장치로 보내는 스크립트 이름을 입력합니다.
- **감지 스크립트**: 앱 감지를 위해 서버가 기기로 보내는 스크립트 이름을 입력합니다. 앱의 감지 스크립트 결과는 기기에 있는 앱의 기본 인벤토리 결과를 덮어씁니다. 앱이 기기에 배포되었는지 여부와 관계없이, 기기에 앱이 있는지 여부를 평가하기 위해 모든 앱의 감지 스크립트가 기기로 전송됩니다.
  감지 스크립트 샘플은 아래와 같습니다.

```
#!/bin/bash
app_name="Name of the App"
count="$(system_profiler SPApplicationsDataType | grep "$app_name" -c)"
echo "$app_name count $count"
if [ $count -ge 1 ]
then
echo "$app_name is installed"
else
echo "$app_name is not installed"
exit 1
fi
exit 0
```

앱 배포 관련 설정을 하세요.

12. 프로모션 방법을 선택합니다.
13. 배포 방법을 선택하세요.
14. **고급 옵션 및 앱 구성** 섹션을 확장합니다.
15. 다음 지침을 사용하여 옵션을 완료합니다.
16. **다음**을 클릭하세요.

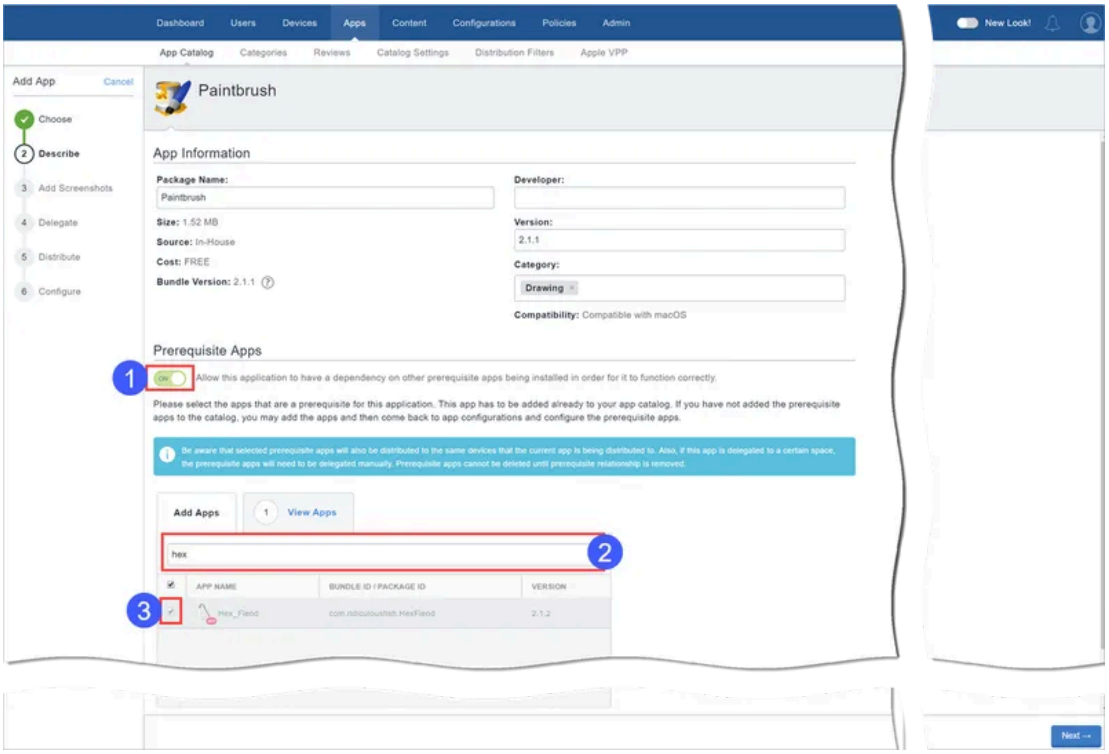
| 설정 항목 | 설정하기 |
| --- | --- |
| 기기에 설치 | 이 옵션을 선택하면 등록 후에 바로 설치를 시작합니다. 다음 상황을 제외하고 사용자에게 앱 설치를 확인하라는 메시지가 표시됩니다.<br>• 이 기기는 관리 상태인 iOS 기기입니다.<br>• 이 기기는 Samsung Knox 기기이며 아래의 자동 설치 옵션이 선택되었습니다. |
| 최종 사용자 App Catalog에서 앱 표시 안 함 | 사용자가 기기에 있는 앱 카탈로그에서 앱을 보기를 원하지 않는 경우 이 옵션을 선택합니다. |
| 앱 설치 우선 순위 설정 | 사용자 온보딩 중에 앱 설치 우선순위를 설정하기 위해 높음, 중간, 낮음 중에서 선택합니다. 사용자 온보딩 중에는 우선순위가 높은 앱만 설치됩니다. |
| 실패 시도 횟수를 초과한 후 앱 다시 푸시 일시 중단(iOS만 해당) | 다시 푸시 시도가 설정된 횟수만큼 실패한 후에는 다음 설정을 사용하여 토글 스위치를 ON으로 전환하여 앱 다시 푸시를 일시 중단합니다.<br>**다음 횟수 이후 다시 푸시 중지** - 다시 푸시가 중단될 다시 푸시 시도 실패 횟수를 입력합니다. 입력한 값은 **1~999**여야 합니다.<br>**시도 실패 및 다음 시간 이후 다시 시도** - 다시 푸시가 실패한 후 다시 푸시를 다시 시도할 수 있는 시간 간격을 입력합니다. 입력한 값은 **3~48**시간이어야 합니다. |
| (Android만 해당) Samsung Knox 기기에 자동 설치 | 사용자에게 Samsung Knox 기기 설치를 확인하라는 메시지를 표시하지 않으려면 이 옵션을 선택합니다. |
| (iOS 및 macOS만 해당) 이 앱에 대한 퍼앱 VPN 활성화 | 이 옵션을 선택하면 이 앱에서 **퍼앱 VPN 구성**을 사용합니다.<br>드롭다운 목록에서 사용할 퍼앱 VPN 구성을 선택합니다.<br>macOS의 경우 Tunnel 퍼앱 VPN 구성만 선택하십시오. |
| (iOS만 해당) iCloud와 iTunes 백업 차단 | 이 옵션을 선택하면 이 앱과 관련된 데이터가 iCloud와 iTunes에 백업되지 못하게 합니다. |
| (iOS만 해당) 미등록 앱 제거 | MDM용 Ivanti Neurons에서 더 이상 기기를 관리하지 않으면 이 옵션을 선택하여 이 앱을 삭제합니다. |
| (iOS만 해당) AppConnect 사용자 지정 구성 | AppConnect 지원 앱의 경우, 사용자 지정 구성 기본 설정을 지정하는 키와 값을 입력합니다. 사용 가능한 키에 관한 정보는 해당 앱 관련 문서를 참조하십시오. |
| iOS 7+ 관리되는 앱 설정 | iOS 7+ 관리 앱으로서 이 앱에 지정된 키와 값을 입력합니다. 지원되는 키에 관한 정보는 해당 앱 관련 문서를 참조하십시오. |

17. **완료**를 클릭하세요.
    - 추천 안 함
    - 추천 리스트

- 배너

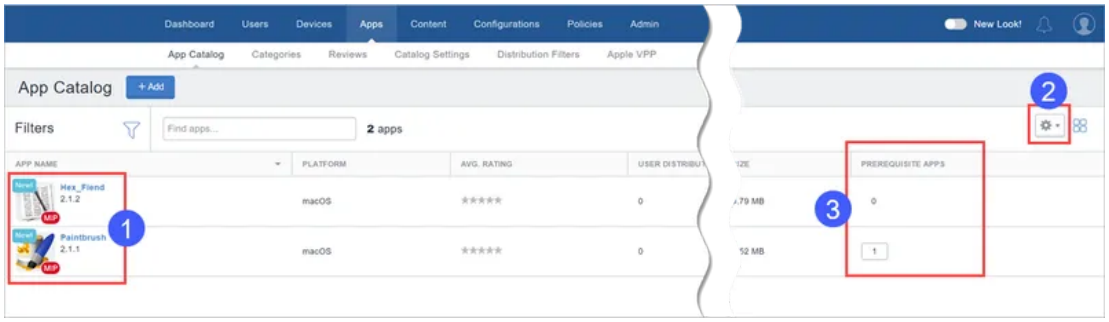
## Packager 인하우스 macOS 앱 이해

Packager 인하우스 macOS 앱을 가져올 경우 관리자는 필수 설치 앱 기능을 활성화하고 1 검색해 2 관리자가 가져오는 앱을 설치하기 전에 클라이언트에 설치해야 할 필수 앱을 선택 3 할 수 있습니다.




가져오고 나면, Packager macOS 인하우스 앱이 App Catalog에 MIP 배지와 함께 아래 1 와 같이 표시됩니다. 그러면 열 설정( 2 )을 사용하여 필수 설치 앱 열( 3 )을 추가하고 종속성이 있는 앱, 즉 필수 설치 앱이 있는 앱을 한 눈에 볼 수 있습니다.

- MIP, 비 MIP 및 공개 앱(Apps 및 Books와 macOS App Store 공개 앱)을 검색하고 필수 설치 앱으로 선택할 수 있습니다.
- Apps 및 Books 필수 설치 앱이 자동으로 설치되도록 하려면 Apps 및 Books 라이센스를 수락해야 합니다.
- 비 Apps 및 Books 공개 필수 설치 앱의 경우 관리자는 공개 앱을 명시적으로 배포해야 하고 사용자는 공개 앱을 설치해야 합니다. 공개 앱(Apps 및 Books와 비 Apps 및 Books 앱)이 필수 설치 앱 목록에 나타나도록 하려면 App Catalog로 가져와야 합니다. 소스 열은 필수 설치 앱의 유형을 나타냅니다.
- 비 MIP 필수 설치 앱이 포함된 비 MIP 인하우스 앱을 설치하려면 MDM 체크인이 필요합니다.
- 사용자는 공개 비 Apps 및 Books 필수 설치 앱을 수동으로 설치해야 합니다.
- Apps 및 Books 토큰이 제거되거나 라이센스가 모두 사용된 경우 필수 설치 앱으로 선택되어 메인 앱이 된 Apps 및 Books 앱은 설치되지 않습니다. 관리자는 Apps 및 Books 앱에 이런 상황이 발생하는 경우 최선의 방법에 따라 사용자에게 미리 알려야 합니다.

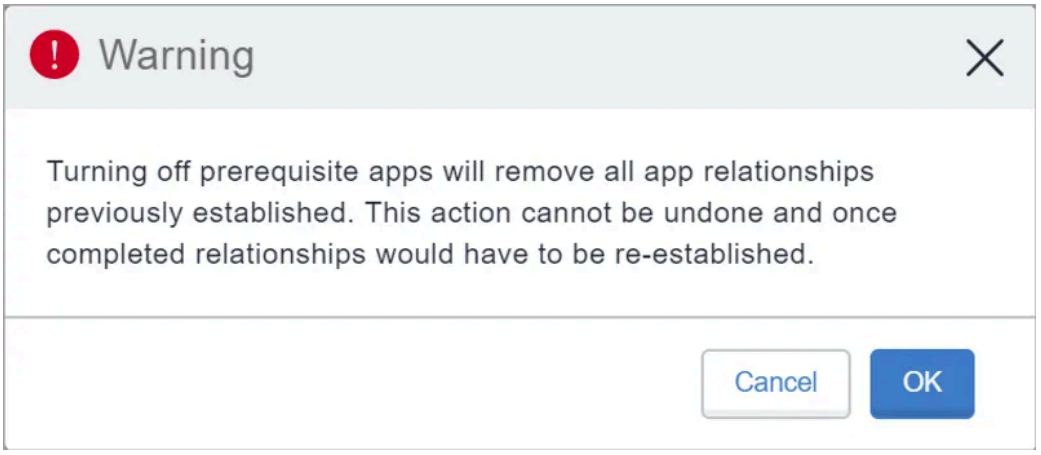



필수 설치 앱은 명시적으로 배포된 경우 사용자가 다운로드할 수 있는 독립 앱으로 사용될 수도 있습니다. 사용자가 필수 설치 앱을 제거하려 하는 경우:

- 다음 장치 체크인 시 필수 앱이 다시 설치되는지 확인하십시오.
- 동일한 기기에 종속 메인 앱이 설치되지 않은 경우에는 필수 설치 앱이 제거됩니다.
- 필수 설치 앱이 명시적으로 배포되지 않은 경우에는 필수 설치 앱이 메인 앱과 함께 제거됩니다.
- 필수 설치 앱이 명시적으로 배포된 경우 필수 설치 앱은 기기에 남아 있습니다.
- 필수 설치 앱에 종속 앱이 있는 경우 필수 설치 앱은 기기에 남아 있습니다.

**필수 설치 앱 기능 끄기**

종속성과 필수 설치 앱이 있는 앱에 대해 해당 앱을 업데이트하거나 삭제 또는 위임하는 등의 작업을 하는 경우 앱의 종속성 또는 필수 설치 상태가 수행하려는 작업에 미치는 영향을 알려주는 시스템 메시지가 표시됩니다. 예를 들어 앱에 대한 필수 설치 앱 기능을 해제하고자 하면 아래와 같은 메시지가 나타납니다.




- 앱의 필수 설치 앱 기능을 끄면 필수 설치 앱에 대한 상세 정보가 삭제됩니다. 여기에는 하위 공간에서 필수 설치 앱의 자동 위임 및 위임 해제가 포함됩니다.
- Apps@Work에서는 저장 클라이언트에 설치되어 있지 않은 필수 설치 앱의 종속 앱에 대한 설치 버튼이 표시되지 않습니다.
- 사용자 기기의 경우, 사용자가 종속성이 있는 인하우스 앱을 설치하려고 하면 필수 설치 앱이 먼저 설치되고(아직 설치되지 않은 경우) 그 다음으로 메인 앱이 설치됩니다. 설치에 몇 분쯤 소요될 수 있습니다. 종속 앱 목록은 설치 상태와 함께 사용자에게 표시됩니다.

**공간에서 필수 설치 앱 위임 및 위임 해제**

- 메인 앱이 하위 공간에 위임되면 앱(메인 앱)에 종속된 필수 설치 앱이 자동으로 위임됩니다.
- 메인 앱이 하위 공간에서 위임 해제되면 필수 설치 앱이 명시적으로 배포되지 않은 곳에서도 필수 설치 앱이 위임 해제됩니다. 그러나 한 개 이상의 메인 앱에 종속된 필수 설치 앱은 위임 해제되지 않습니다.

- 필수 설치 앱이 명시적으로 위임된 경우에는 자동으로 위임 해제되지 않습니다.

## Android Enterprise 인하우스 앱용 기기 권한 위임

Android Enterprise 관리형 기기 및 AMA 기기에 적용할 수 있는 인하우스 앱에 위임된 권한을 할당할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **App Catalog**에서 기기 권한을 위임하고자 하는 앱을 선택합니다.
3. **앱 구성** 탭을 클릭합니다.
4. 위임된 권한(인하우스 Android Enterprise 앱)에서 앱에 필요한 권한을 선택합니다.

> COSU 배포만 AMAPI를 사용합니다. 자세한 내용은 AMAPI 섹션을 참조하십시오.

   - **타사 앱 런타임 사용 권한 구성**
   - **타사 앱 숨기기 및 중단**
   - **인증서 관리**
   - **앱 구성 관리**
   - **앱 제거 차단 관리**
   - **시스템 앱 활성화 관리**
   - **인증서 선택 관리**(AMAPI 모드에서는 지원되지 않음)
   - **설치되지 않은 앱 유지 관리**(AMAPI 모드에서는 지원되지 않음)
   - **네트워크 로그 수집 관리**(한 번에 하나의 앱에서만 지원됨)
   - **보안 로그 수집 관리**(한 번에 하나의 앱에서만 지원)
   - **기존 앱의 설치 관리**(AMAPI 모드에서는 지원되지 않음)
   - **패키지 설치 및 제거**(AMAPI 모드에서는 지원되지 않음)

패키지 설치 및 제거 옵션은 지원되는 모든 Android 기기 소유자 모드 기기(7.0 이상)에서 사용할 수 있습니다. 기타 위임된 권한은 Android 8.0 이상에만 해당됩니다.
**앱을 소유한 모든 사람**, **없음**, **사용자 지정** 중 하나를 선택하여 배포 옵션을 구성합니다.

6. **저장**을 클릭하세요.

## iOS용 인하우스 앱에서 프로비저닝 프로필 상태 표시하기

iOS용 인하우스 앱의 App Catalog 페이지에 프로비저닝 프로필 상태를 표시합니다. 프로필 이름 옆의 툴팁은 프로필의 만료 날짜까지 남은 일수를 표시합니다. 이 상태는 인하우스 앱의 프로비저닝 프로필이 만료되는 날짜를 확인할 때 유용하게 쓰일 수 있습니다.

이 상태는 인하우스 앱의 프로비저닝 프로필이 만료되는 날짜를 확인할 때 유용합니다. 적절한 프로비저닝 프로필이 없을 경우 앱은 설치되지만 열리거나 시작되지 않습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 우측 상단의 기어 아이콘을 클릭하여 열을 표시합니다.
3. **프로비저닝 프로필**을 선택하여 App Catalog 페이지에 앱 목록 열을 표시합니다.

프로비저닝 프로필 설정 섹션의 앱 상세 정보 페이지에서도 프로비저닝 프로필 정보를 볼 수 있습니다.

## iOS용 인하우스 앱에서 프로비저닝 프로필 업데이트

프로비저닝 프로필은 특정 iOS 인하우스 앱에 적용됩니다. 앱의 프로비저닝 프로필 상세 정보는 앱 상세 정보 페이지에서 확인할 수 있습니다. 기기에서 실행하려면 iOS 인하우스 앱에 만료되지 않은 프로비저닝 프로필이 필요합니다. 만료되었을 경우, 앱 상세 정보 페이지에 프로비저닝 프로필을 업로드하여 프로필을 업데이트할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 프로비저닝 프로필 업데이트가 필요한 앱을 클릭합니다. 앱 상세 정보 페이지가 표시됩니다.
3. **편집**을 클릭합니다.
4. **프로비저닝 프로필** 섹션에서 **파일 선택**을 클릭합니다.
5. 업로드할 프로비저닝 프로필 파일(파일 확장자 .mobileprovision)을 선택하여 **저장**을 클릭합니다.

## 인하우스 앱을 Google Play에서 배포하기

인하우스 앱을 Google Play 비공개 채널에 업로드하고 MDM용 Ivanti Neurons에 가져와서 Android Enterprise 지원 기기에 배포합니다.

**절차**

1. Google 비공개 앱 콘솔 로그인: https://play.google.com/apps/publish.
2. 왼쪽 메뉴에서 **모든 애플리케이션**을 클릭합니다.
3. **새 애플리케이션 만들기**를 클릭하고 애플리케이션 이름을 입력합니다.
4. **APK 업로드**를 클릭하고 생성한 .apk 파일을 업로드합니다.
5. **스토어 리스팅**을 클릭합니다.
   - 간단한 설명과 전체적 설명을 입력합니다.
   - 모든 탭의 스크릿샷을 업로드합니다.
   - 고해상도 아이콘을 업로드합니다.
   - 기능 그래픽 아이콘(graphic.png)을 업로드합니다.
   - 범주화, 연락처 세부 정보, 개인정보 보호 정책에 필수 정보를 입력합니다.
   - 앱 평가의 설문조사를 작성합니다.
6. **가격 및 배포**를 클릭합니다.
   모든 필수 정보가 입력되었다면 페이지 상단에 발행 준비 완료가 표시됩니다.
7. MDM용 Ivanti Neurons의 앱 탭으로 이동합니다.
8. **이용 가능한 카탈로그 새로고침**을 클릭하여 개인 앱을 동기화합니다.

> 앱을 게시하는 데 수 시간이 걸릴 수 있습니다.

## Android Enterprise 기기용 웹 앱 추가

웹 앱은 웹 사이트 링크로, 기기에 바로가기로 설치됩니다. 웹 앱은 다른 앱과 유사한 방식으로 작동합니다. 따라서 앱과 동일한 기준으로 배포될 수 있습니다. App Catalog에 표시되며 다른 앱과 마찬가지로 사용자가 설치할 수 있습니다. 하지만 웹 앱은 단일 버전만을 보유할 수 있고 자동 설치가 지원되지 않습니다. 웹 앱은 웹 클립을 사용하고 기기에는 구성으로서 설치되지만 앱처럼 작동합니다.

App Catalog에 웹 클립을 앱으로서 설정하면 사용자가 App Catalog에서 웹 앱을 사용할 수 있습니다. 웹 클립은 구성으로 정의될 수 있지만 구성은 관리자만이 푸시할 수 있습니다. 사용자는 기기에서 웹 앱 설치 또는 해제를 선택할 수 있습니다. 하지만 사용자에게는 웹 클립 구성을 해제할 옵션이 없습니다.

Android Enterprise에서 웹 앱은 작업 프로필 내에서 Google Chrome을 통해 실행되는 내장형 웹 앱입니다. Android Enterprise의 VPN 또는 SSO 솔루션과 결합할 수 있습니다. 웹 앱이 만들어진 후, 앱은 다른 Android 앱과 같이 작동하며, 필요한 만큼 배포할 수 있습니다. 웹 앱을 실행하려면 회사 소유 기기의 작업 프로필에 Chrome이 설치되어 있어야 합니다.

> 이 기능 사용과 관련한 문제가 있을 경우 관리자는 지원팀에 문의할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **+ 추가**를 클릭합니다.
3. 드롭다운 목록에서 **Google Play**를 선택하여 Google Play Store에서 앱을 검색합니다. Android Enterprise가 등록된 경우 Google Play iFrame이 표시됩니다.
4. **웹 애플리케이션**을 클릭합니다.
5. 앱 정보를 입력하세요.
    1. 앱 제목 또는 이름
    2. 앱 URL.
    3. 웹 앱에 대한 유형 표시
    4. 512px 단위 정방형 PNG 또는 JPEG 이미지일 수 있는 아이콘을 업로드합니다.

**생성**을 클릭합니다. 앱이 iFrame에 게시되도록 기다립니다. 몇 분이 소요될 수 있습니다. 닫았다가 나중에 돌아갈 수 있습니다.

7. 웹 앱이 게시된 후, 배포를 위해 앱을 App Catalog로 가져옵니다. 웹 앱 아이콘을 클릭합니다.
8. 스크롤을 내려 **선택**을 클릭합니다.
9. 범주 및 선택 사항 설명을 추가합니다.
10. **다음**을 클릭하세요.
11. 다음 앱 위임 옵션 중 하나를 선택합니다.
    - 이 앱을 모든 공간에 위임합니다.
    - 이 앱을 모든 공간에 위임하지 않습니다.

**다음**을 클릭하세요.

13. 애플리케이션 배포 옵션을 선택합니다.
14. **완료**를 클릭합니다.

웹 앱을 추가한 후 필요할 때면 언제든지 웹 앱을 편집할 수 있습니다. 불러오는 방법은 다음과 같습니다.

1. **App Catalog** 페이지에서 기존 웹 앱 이름을 클릭합니다.
2. **편집**을 클릭하여 웹 앱 필드를 편집합니다.

## iOS 기기 웹 앱 추가

웹 앱은 웹 사이트 링크로, 기기에 바로가기로 설치됩니다. 웹 앱은 다른 앱과 유사한 방식으로 작동합니다. 따라서 앱과 동일한 기준으로 배포될 수 있습니다. App Catalog에 표시되며 다른 앱과 마찬가지로 사용자가 설치할 수 있습니다. 하지만 웹 앱은 단일 버전만을 보유할 수 있고 자

동 설치가 지원되지 않습니다. 웹 앱은 웹 클립을 사용하고 기기에는 구성으로서 설치되지만 앱처럼 작동합니다.

앱 카탈로그에서 웹 클립을 앱으로 설정하여 사용자가 앱 카탈로그에서 웹 앱을 사용할 수 있도록 합니다. 웹 클립은 구성으로 정의될 수 있지만 구성은 관리자만이 푸시할 수 있습니다. 사용자는 기기에서 웹 앱 설치 또는 해제를 선택할 수 있습니다. 하지만 사용자에게는 웹 클립 구성을 해제할 옵션이 없습니다.

> 이 기능 사용과 관련한 문제가 있을 경우 관리자는 지원팀에 문의할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **+ 추가**를 클릭합니다(좌측 상단).
3. **웹 앱**을 클릭합니다.
4. 앱 정보를 입력하세요.
    1. 앱 이름.
    2. 앱 URL.
    3. 플랫폼 유형.
    4. 앱 아이콘.
    5. 범주를 추가 또는 삭제합니다.
    6. 전체 화면 - 선택하면 웹 앱이 전체 화면 애플리케이션으로 표시됩니다.
    7. 제거 가능 - 선택하면 웹 앱이 제거 가능해집니다.
    8. **다음**을 클릭하세요.

다음 앱 위임 옵션 중 하나를 선택합니다.

- 이 앱을 모든 공간에 위임합니다.
- 이 앱을 모든 공간에 위임하지 않습니다.

**다음**을 클릭하세요.

7. 애플리케이션 배포 옵션을 선택합니다.
8. **완료**를 클릭합니다.

### 웹 앱 편집

웹 앱을 추가한 후 필요할 때면 언제든지 웹 앱을 편집할 수 있습니다.

**절차**

1. **App Catalog** 페이지에서 기존 웹 앱 이름을 클릭합니다.
2. **편집**을 클릭하여 웹 앱 필드를 편집합니다.

## 점진적 롤아웃 배포

**점진적 롤아웃 배포** 설정을 사용하면 관리자가 새 버전의 애플리케이션을 기기에 점진적으로 자동 배포할 수 있습니다. 느린 롤아웃 배포 방법 사용 옵션은 애플리케이션의 후속 릴리스를 롤아웃할 때 사용할 수 있습니다. MDM용 Ivanti Neurons 관리 포털을 사용하면 느린 롤아웃이 일시 중지된 경우에도 애플리케이션을 편집할 수 있습니다.

한 릴리스에 느린 롤아웃을 설정하면 후속 릴리스에 마지막 설정과 동일한 백분율을 적용할 수 있습니다. 배포를 100%로 설정할 경우 애플리케이션 배포를 일시 중지할 수 있습니다. 그러나 배포 목표를 100%로 설정할 경우 UI가 0%로 재설정하므로 다음 버전의 배포 목표 백분율을 수동으로 설정해야 합니다.

**절차**

| | | |
|---|---|---|
| | 1. | **앱의 App Catalog로 이동하여 배포 모드 옵션 중 하나를 선택합니다.** |
| | 2. | **선택 요약의 사용자 지정 기기 %(느린 롤아웃) 옵션을 선택합니다.** |
| | 3. | **느린 롤아웃 설정에서 배포 목표 % 지정의 슬라이더를 드래그합니다.** |
| | 4. | **확인을 클릭하고 완료를 클릭합니다. 최신 앱 버전의 상태가 표시됩니다. 앱 카탈로그 페이지에 테이블의 느린 롤아웃 상태가 표시됩니다.** |

**App Catalog** 페이지에서 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 앱 및 콘텐츠 관리 역할이 필요합니다.

## 고급 검색 사용

고급 검색 옵션으로 규칙 기반 앱을 검색하여 특정 기준에 해당하는 앱을 식별하고 조회할 수 있습니다. 규칙은 '같음', '보다 작음', '보다 큼', '다음과 같음', '다음과 같지 않음' 연산자를 사용하여 구성할 수 있습니다. 규칙 옵션은 임의(OR) 또는 모두(AND) 옵션을 사용하여 중첩될 수 있습니다. 규칙과 일치하는 앱이 섹션 하단에 표시됩니다.

> 검색에 사용되는 사용자 지정 속성 값은 대소문자를 구분합니다.

**절차**

1. 앱 카탈로그 페이지에서 **고급 검색** 링크를 클릭합니다. 고급 검색 마법사가 열립니다.
2. 다음 옵션 중 하나를 클릭합니다.
   - **임의** - 앱이 하나 이상의 규칙을 충족하는 경우
   - **모두** - 앱이 모든 규칙을 충족하는 경우

검색 기준을 정의하는 규칙을 생성하려면 다음 옵션 중 하나를 선택하고 적절한 관련 작업을 선택하십시오.

- AppConnect 활성화됨
- 평균 등급
- 번들 ID
- 범주
- 비용
- 사용자 지정 속성
- AppCatalog에 날짜가 추가되었습니다
- 수정된 날짜
- 장치 배포
- 장치 그룹 배포

- 장치 유형
- 그룹 배포
- 최소 OS 버전
- 이름
- OS 플랫폼
- 프로비저닝 프로필
- 크기
- 소스
- 사용자 분포
- 사용자 그룹 이름
- 버전

4. (선택 사항) **+**를 클릭하여 추가 규칙을 생성할 수 있습니다.
5. **검색**을 클릭합니다. 검색 기준에 부합하는 앱 목록이 표시됩니다.

### 검색 쿼리 로드

저장된 검색 쿼리 목록을 볼 수 있습니다.

**절차**

1. 고급 검색을 클릭하고 폴더 아이콘을 클릭합니다. 생성된 검색 쿼리 목록이 **쿼리 로드** 섹션에 표시되고 다음과 같은 세부 정보가 표시됩니다.
   - **쿼리 이름** - 로드된 쿼리 이름.
   - **쿼리 콘텐츠** - 검색 쿼리를 정의하는 규칙에 콘텐츠를 표시합니다.
   - **작업** - 쿼리에서 수행할 작업을 선택합니다.
2. **작업** 열에서 **쿼리 로드**를 클릭하면 로드된 쿼리에서 정의된 기준에 부합하는 앱 목록이 보입니다.
3. **삭제**를 클릭하여 로드한 쿼리를 삭제합니다.

## CSV 파일로 앱 내보내기

앱 카탈로그 페이지에서 CSV로 내보내기 옵션을 사용하여 앱을 내보낼 수 있습니다.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. **CSV로 내보내기**를 클릭하여 앱 목록과 관련 세부 정보를 CSV 파일로 내보냅니다.

> 선택한 공간에 나열된 앱만 포함되며 페이지가 매겨진 모든 결과는 단일 파일에 컴파일됩니다.

> 필터나 검색 결과를 사용하면 관련 앱만 내보냅니다.

3. **계속** 및 **취소** 버튼이 포함된 팝업 메시지가 나타나 내보내기 프로세스가 시작되었음을 알리고, 곧 보고서를 사용할 수 있습니다.
4. **계속**을 클릭하고 요청이 완료되기를 기다린 후 다른 요청을 제출합니다.
5. **앱 카탈로그 - CSV 보고서 완료** 상태임을 알리는 메시지가 나타나며 여기에는 **다운로드** 및 **삭제** 버튼이 있습니다.

6. 보고서를 다운로드하려면 **다운로드**를 클릭하세요.
7. (선택 사항) 보고서를 삭제하려면 **삭제**를 클릭합니다.

> **CSV로 내보내기** 옵션은 **다운로드** 또는 **삭제** 옵션을 선택한 후에만 다시 활성화됩니다.

> 앱 버전이 여러 개인 경우 앱 버전당 하나의 항목이 표시됩니다.

**관련 주제**

- 사용자 역할
- App Catalog에서 앱 삭제
- 앱 종속성 배포하기

# 8.2. 선언적 기기 관리(DDM) 앱 관리

## 개요

**선언적 기기 관리(DDM) 앱 관리**에 iOS 및 iPadOS 기기에서 애플리케이션을 배포하고 수명 주기를 관리하기 위한 Apple의 선언적 관리 프레임워크 지원이 새롭게 도입되었습니다. 지속적인 명령 전달 및 주기적인 폴링에 의존하는 대신, DDM을 사용하면 기기가 선언을 로컬에서 적용하고 상태 변경 사항을 사전에 보고할 수 있습니다.

DDM을 사용하면 서버가 선언을 기기에 한 번만 전송합니다. 그런 다음 기기는 구성을 적용하고 상태를 모니터링하며 상태 변경 사항을 서버에 다시 보고합니다. 이러한 기기 중심 접근 방식은 서버 통신을 줄이고 확장성을 향상하며 애플리케이션 배포에 대한 상태 업데이트를 보다 적시에 제공합니다.

현재, DDM 앱 관리는 지원되는 Apple 기기의 핵심 애플리케이션 관리 기능에 중점을 둡니다.

## DDM 앱 관리 워크플로

DDM 워크플로에서 서버는 원하는 상태를 기기에 전달하고, 기기는 해당 상태를 유지하고 보고하는 역할을 담당합니다.

애플리케이션이 DDM이 활성화된 기기에 할당되는 경우:

1. 서버는 애플리케이션 선언을 기기로 전송합니다.
2. 기기는 선언을 로컬에서 처리합니다.
3. 기기는 할당된 구성에 따라 애플리케이션을 설치, 업데이트 또는 유지 관리합니다.
4. 기기는 애플리케이션 상태를 지속적으로 모니터링합니다.
5. 설치 상태 또는 상태 변경 사항이 즉시 서버에 다시 보고됩니다.

이 선언적 모델을 사용하면 주기적인 상태 폴링 없이도 애플리케이션 배포 진행 상황을 거의 실시간으로 확인할 수 있습니다.

## DDM 앱 관리 활성화

DDM 앱 관리는 사용자 설정을 통해 활성화되며 특정 사용자 그룹에 할당됩니다.

DDM 앱 관리를 활성화하려면:

1. **사용자** > **사용자 설정**으로 이동합니다.
2. **Apple DDM 설정**에서 **+ 특정 사용자 그룹에 대한 설정 추가**를 클릭합니다. **Apple DDM 설정** 페이지가 열립니다.
3. 이름을 입력하고 **DDM 앱 관리 활성화** 슬라이더를 전환합니다.
4. **다음**을 클릭합니다. **사용자 설정 배포** 배포 페이지가 열립니다.
5. DDM 앱 관리를 사용할 사용자 그룹을 선택합니다.
6. **완료**를 클릭하세요.

사용자 그룹에 DDM이 활성화되면 해당 그룹의 사용자에게 할당된 모든 지원되는 애플리케이션이 DDM 앱 관리를 통해 처리됩니다. DDM 구성은 테넌트 전체에 적용되지만 사용자 그룹 할당을 통해 적용되므로 조직은 선택한 사용자 또는 그룹에 DDM을 점진적으로 배포할 수 있습니다.

### 지원되는 등록 방법

DDM 앱 관리는 다음을 사용하여 등록된 iOS/iPadOS 기기를 지원합니다:

- iReg/관리형 Ivanti Go Client

- 기기 등록 프로필(DEP)
- 계정 기반 기기 등록

### 지원되는 애플리케이션 유형

DDM 앱 관리는 다음 애플리케이션 유형을 지원합니다.

- 공개 애플리케이션
- VPP 애플리케이션(기기 등록에만 해당)
- 내부 애플리케이션

애플리케이션 할당 및 배포 워크플로는 기존 N-MDM 배포와 거의 동일하게 유지됩니다. 기존 애플리케이션 배포 프로세스는 계속 작동하면서 DDM의 향상된 상태 보고 기능을 활용합니다.

# 8.2.1. DDM 앱 관리 설정

일반적으로 앱 관리에는 다음 설정이 포함됩니다.

- iCloud에 백업 방지
- 새로 등록된 기기에 앱을 설치하지 않음
- 셀룰러 5G
- DNS 프록시
- 관리형 앱 구성
- 비즈니스 앱 – Apps@Work, Email+ 등
- 앱별 VPN
- 네트워크 릴레이
- 웹 콘텐츠 필터
- App Store 업데이트 허용

위에 나열된 설정 외에도 DDM 앱 관리에는 DDM 관리 기기에서만 사용할 수 있는 여러 기능이 도입되었습니다.

## 앱 버전 고정

앱 버전 고정을 사용하면 관리자가 DDM 관리 기기 전반에 특정 애플리케이션 버전을 배포하고 유지 관리할 수 있습니다.

버전 고정이 활성화된 경우:

- 기기는 지정된 애플리케이션 버전을 설치합니다.
- 새 버전으로의 자동 업그레이드가 방지됩니다.
- 관리자가 새 버전을 명시적으로 선택할 때까지 애플리케이션은 할당된 버전으로 유지됩니다.

이 기능을 통해 애플리케이션 버전 일관성과 단계적 업그레이드 배포를 더욱 세밀하게 제어할 수 있습니다.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. 표시된 목록에서 앱을 클릭합니다. **앱 상세 정보** 페이지가 열립니다.
3. **앱 구성** 탭에서 **Apple 앱 설정**을 클릭합니다.
4. 나열된 기존 설정 중 하나를 클릭합니다.
5. **편집**을 클릭합니다.
6. **기기에 앱 버전 고정** 섹션에서 **앱 버전 고정** 옵션을 선택합니다.
7. **앱 버전 선택** 목록에서 필요한 앱 버전을 선택합니다.

> 기기에 기존 버전의 앱이 있는 경우 이전 버전으로 교체할 수 없습니다.

8. **업데이트**를 클릭합니다.

## 자동화된 App Store 업데이트 제어(자동 앱 업데이트)

관리자는 관리형 애플리케이션에 대한 App Store 업데이트 처리 방식을 구성할 수 있습니다 이 기능을 통해 애플리케이션 업데이트 동작을 더욱 세밀하게 제어할 수 있으며 조직에서 내부 유효성 확인 및 롤아웃 프로세스에 맞게 업데이트를 조정할 수 있습니다.

## 셀룰러를 통한 다운로드 허용

DDM에는 셀룰러 네트워크를 통한 애플리케이션 다운로드 및 업데이트를 제어하는 전용 설정이 도입되었습니다.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. 표시된 목록에서 앱을 클릭합니다. **앱 상세 정보** 페이지가 열립니다.
3. **앱 구성** 탭에서 **기기에 설치**를 클릭합니다.
4. 나열된 기존 설정 중 하나를 클릭합니다.
5. **편집**을 클릭합니다.
6. **셀룰러 네트워크를 통한 다운로드 허용** 섹션에서 다음 옵션 중 하나를 선택합니다.
    - **스토어 설정** – 기본 옵션입니다. 기기는 앱을 다운로드할 때 해당 스토어의 설정을 사용합니다.
    - **항상 켜짐** – 기기에 Wi-Fi 연결이 없는 경우에도 앱 다운로드가 허용됩니다.
    - **항상 꺼짐** – 기기에 Wi-Fi 연결이 없는 경우 앱 다운로드가 허용되지 않습니다.
7. **업데이트**를 클릭합니다.

### 애플리케이션 설치 워크플로

애플리케이션 배포 프로세스는 기존 N-MDM 앱 관리와 유사하게 유지됩니다.

관리자는 다음을 수행할 수 있습니다:

- 앱 할당
- 앱 배포
- 앱 설치

그러나 DDM에서는 배포 상태가 전달되는 방식이 변경됩니다. 서버 폴링에 의존하는 대신 기기는 작업이 완료되는 즉시 애플리케이션 상태 변경 사항을 보고합니다. 이를 통해 설치 진행 상황 및 배포 결과에 대한 정보를 더욱 정확하고 시기적절하게 제공합니다.

### 상태 보고 및 모니터링

DDM 앱 관리의 주요 이점 중 하나는 사전 예방적 상태 보고입니다.

**DDM 사용 시**:

- 기기는 애플리케이션 상태를 로컬에서 모니터링합니다.
- 설치 및 업데이트 이벤트가 즉시 감지됩니다.
- 상태 변경 사항은 서버에 자동으로 보고됩니다.
- 배포 정보는 예약된 폴링 간격을 기다리지 않고 제공됩니다.

이를 통해 관리자는 다음 항목을 더 빠르게 파악할 수 있습니다.

- 애플리케이션 설치 진행 상황
- 설치 완료 항목

- 애플리케이션 업데이트 완료
- 애플리케이션 상태 변경 사항
- 배포 실패 항목

실시간 보고를 통해 문제 해결이 개선되고 더욱 신속한 애플리케이션 관리 환경이 제공됩니다.

## 요건

DDM 앱 관리는 다음에서만 지원됩니다.

- iOS 26 이상
- iPadOS 26 이상
- 관리형 Ivanti Go Client 126 이상

이러한 요구 사항을 충족하지 않는 기기는 기존 N-MDM 앱 관리를 계속 사용합니다.

> 기기가 DDM 앱 관리를 통해 처리된 후에는 이 정책 배포를 비활성화하거나 업데이트해도 기기가 MDM 앱 관리로 되돌아가지 않습니다. 기기를 MDM 앱 관리로 되돌리려면 정책 할당을 제거하고 기기를 다시 등록합니다.

# 8.3. Apps@Work(iOS, Android, Windows, macOS)

Apps@Work는 소프트웨어 및 앱의 안전한 배포를 용이하게 하는 엔터프라이즈 앱스토어입니다. Apps@Work는 iOS, Android, macOS, Windows 기기에서 사용할 수 있습니다. Apps@Work 기업 앱스토어는 iOS, Android 및 macOS용 Ivanti Go app 및 Mobile@Work 클라이언트에 통합되었습니다. Windows 기기의 경우 기본 독립 실행형 애플리케이션입니다. 이 섹션에는 다음 주제가 포함됩니다.

- **iOS Apps@Work**
- **Android Apps@Work**
- **macOS Apps@Work**
- **Windows Apps@Work**

## iOS Apps@Work

Apps@Work 기본 앱스토어는 Go 클라이언트와 함께 자동으로 배포됩니다. 관리자의 조치가 필요하지 않습니다. Apps@Work 탭은 Go 클라이언트 작업 표시줄에 표시됩니다. 최종 사용자는 이 탭으로 이동하여 회사에서 승인한 앱을 보고 설치할 수 있습니다. 자세한 내용은 **iOS Apps@Work AppStore 기능**을 참조하십시오.

앱 업데이트에 대한 iOS Apps@Work 최종 사용자 알림은 기본적으로 활성화되어 있습니다. 설정을 변경하려면 **카탈로그 설정**의 **알림** 토픽을 확인하십시오.

## iOS Apps@Work Webclip을 사용하는 기존 고객

기존 iOS Apps@Work Webclip이 배포된 고객은 기본적으로 Native Integrated AppCatalog를 받지 못합니다. iOS Apps@Work Native 카탈로그로 전환하고 기기에서 Apps@Work 웹 클립을 제거하려면 다음 단계를 수행하십시오.

### 구성 푸시

Go 클라이언트 애플리케이션의 기본 앱스토어 환경에서 Apps@Work를 사용할 수 있도록 하려면 관리자가 네이티브 클라이언트용 앱 카탈로그 구성을 기기에 푸시해야 합니다. 자세한 내용은 **구성 작업**을 참조하십시오.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성** > 필터로 이동하여 **클라이언트 서비스**를 선택합니다. 클라이언트 구성이 모두 열거됩니다.
3. **네이티브 클라이언트용 앱 카탈로그**를 선택합니다. 네이티브 클라이언트용 앱 카탈로그 구성 페이지가 열립니다.
4. **배포 편집** 아이콘을 클릭합니다. 배포 편집 페이지가 열립니다.
5. 다음 옵션 중 하나를 선택합니다.
   - **모든 기기**
   - **기기 없음** - 기기에 배포하지 않으려는 경우
   - **사용자 지정** - 기기, 기기 그룹, 사용자, 사용자 그룹을 선택할 수 있습니다.
6. 구성이 배포된 후 사용자는 Go 클라이언트 버전을 83 이상으로 업그레이드해야 합니다. 이제 Apps@Work 탭이 Go app 클라이언트에 표시됩니다.

> 기기에서 Go 클라이언트를 사용할 수 없기 때문에 iReg를 사용하여 등록된 기기에 대한 구성을 푸시할 수 없습니다. 기본 앱 카탈로그를 가져오려면 Go app 클라이언트를 설치해야 합니다. 자세한 내용은 **기기 등록(iOS, macOS, Android)**을 참조하십시오.

## iOS Apps@Work Webclip 제거

기기에 Apps@Work Webclip이 배포되어 있고 이미 Apps@Work Native 환경으로 마이그레이션한 고객의 경우 iOS Apps@Work Webclip을 제거할 수 있습니다.

**절차**

1. **구성**으로 이동합니다.
2. 구성 필터링 – **Apple App Catalog**.
3. **편집**을 클릭합니다.
4. **배포**에서 **기기 없음으로 배포**를 선택합니다.
5. **저장**을 클릭합니다.

## Android Apps@Work

Apps@Work 기본 앱스토어는 MI Go 클라이언트와 함께 자동으로 배포됩니다. 관리자의 조치가 필요하지 않습니다. Apps@Work 탭은 Mi Go 클라이언트 작업 표시줄에 표시됩니다. 최종 사용자는 이 탭으로 이동하여 회사에서 승인한 앱을 보고 설치할 수 있습니다. 자세한 내용은 관리 - Android Enterprise를 참조하십시오.

## macOS Apps@Work

macOs Apps@work가 macOS Mobile@Work 클라이언트에 통합되었습니다. 기기가 MDM용 Ivanti Neurons에 등록되면 클라이언트가 전환되어 Apps@Work로 표시됩니다. 새로 생성된 테넌트의 경우 Apple App Catalog Webclip 구성이 macOS 기기로 푸시되지 않습니다. 필요한 경우 관리자는 Apps@Work Webclip 구성을 macOS 기기에 배포할 수 있습니다. 자세한 내용은 **macOS 기기 구성하기**을 참조하십시오.

### macOS 앱 배포하기

- Ivanti는 Apple MDM 프로토콜과 Mobile@Work 앱을 사용하여 macOS 앱 배포를 지원합니다. 관리자는 다음 접근법 중 하나 또는 둘 모두를 선택할 수 있습니다.
    - Apple의 MDM 프로토콜 - 관리자는 인하우스 앱으로 특정 PKG 형식(배포 형식)만을 업로드할 수 있으며 Mac App Store에서 앱을 배포할 수도 있습니다(Apple의 Apps 및 Books 라이센스 지원 포함). 그러나 이러한 접근을 통해 관리자가 DMG 및 기타 PKG를 배포할 수 있는 것은 아닙니다.
    - macOS용 Mobile@Work 앱 - 앱을 사용자에게 배포할 수 있는 방법으로, 관리자는 MobileIron Packager(MIP) 앱을 사용하여 PKG, DMG 또는 .app 파일을 MIP 파일로 변환할 수 있습니다. MIP 파일을 인하우스 앱으로 MDM용 Ivanti Neurons에 업로드하십시오.

소프트웨어 다운로드 사이트에서 유틸리티를 다운로드할 수 있습니다.

- 관리자는 Mobile@Work를 사용하여 DMG, PKG 또는 .app 형식에 있는 인하우스 앱을 배포할 수 있습니다. Mac App Store에서만 사용할 수 있는 앱의 경우 관리자는 계속해서 Apple의 기본 MDM 기능을 사용할 수 있으며, 여기에는 Apple Apps 및 Book 라이센스 기능이 포함됩니다. 자세한 내용은 **macOS 기기 구성하기**을 참조하십시오.

## Windows Apps@Work

Apps@Work는 Microsoft Store에서 다운로드하거나 MDM용 Ivanti Neurons에서 직접 푸시할 수 있는 독립 실행형 기본 앱입니다. MDM용 Ivanti Neurons의 Windows 10+ 기기에서 Windows 공용 및 인하우스 앱을 사용할 수 있습니다. Apps@Work는 지원되는 Windows 10+ 기기에 자동으로 설치됩니다.

자세한 내용은 앱 구성을 참조하십시오.

## Windows Apps@Work 사용

Apps@Work를 사용하면 MDM용 Ivanti Neurons의 Windows 10 기기에서 Windows 공용 및 인하우스 앱을 사용할 수 있습니다. Apps@Work는 지원되는 Windows 10 기기에 자동으로 설치됩니다.

### Apps@Work 인증서 인증

Windows Apps@Work의 인증서 인증 사용 방법:

1. **관리자 > Windows > Apps@Work 인증서 인증**으로 이동합니다.
2. 설정을 **켜기**로 전환합니다.

> 설정을 **끄기**로 전환하면 사용자 이름과 비밀번호를 사용하도록 적용됩니다.

> SAML에서는 Windows용 Apps@Work가 지원되지 않습니다.

Apps@Work용 앱을 구성하려면:

1. Windows 앱을 선택합니다.
2. **앱 구성** 탭을 클릭합니다.
3. **기기에 설치**를 클릭합니다.
   Windows 인하우스 앱 구성을 자동 설치 플래그로 설정하거나 Apps@Work를 사용해 설치할 수 있습니다. 퍼블릭 앱은 자동 설치로 설정할 수 없습니다.
4. 필요에 따라 Apps@Work 카탈로그에 앱을 표시하거나 숨기도록 선택합니다.
   이 옵션은 인하우스 앱에만 적용됩니다.
5. **프로모션** 탭을 클릭합니다.

> Apps@Work는 현재 배너 프로모션을 지원하지 않으므로 사용 가능한 옵션은 **추천** 및 **추천하지 않음**입니다.
>
> **프로모션** 옵션만이 공개 앱에 표시됩니다.

# 8.4. iOS Apps@Work AppStore 기능

Apps@Work 탭에는 다음과 같은 기능이 있습니다.

- Go 애플리케이션에서 Go 애플리케이션에서 Apps@Work 탭에 액세스
- 검색
- 앱 설치 - 버튼 상태
- 추천 애플리케이션 및 배너
- 애플리케이션 업데이트 알림
- 설정-내 기기

## Go 애플리케이션에서 Apps@Work 탭에 액세스

**절차**

1. iOS 기기에서 Go app에 로그인합니다.
2. **Apps@Work** 아이콘을 누릅니다.모든 앱과 범주라는 두 개의 기본 탭을 사용할 수 있습니다.

3. **모든 앱** 탭을 누릅니다. 모든 앱 탭에는 모든 앱이 알파벳 순서로 나열됩니다.
4. **범주** 탭을 누릅니다. 범주 탭에는 다음과 같이 애플리케이션이 포함된 범주만 표시됩니다.
    - 각 범주는 해당 범주에 있는 애플리케이션의 수를 표시합니다.
    - 범주 탭 아래의 MyApps 행은 설치된 모든 애플리케이션이 포함된 목록 항목입니다. MyApps 행은 항상 첫 번째 범주가 되고 나머지 범주는 알파벳순으로 나열됩니다.
    - 설치된 애플리케이션이 없으면 MyApps 목록에 없음이 표시됩니다.
    - 범주를 클릭하면 해당 범주와 관련된 모든 애플리케이션이 설치 옵션과 함께 나열됩니다. **설치**를 클릭하여 각 애플리케이션을 개별적으로 설치하거나 **모두 설치**를 클릭하여 범주의 모든 애플리케이션을 설치할 수 있습니다. 각 애플리케이션에 대한 설치를 허용할지 묻는 메시지가 표시됩니다.

## 검색

**절차**

1. iOS 기기에서 Go app에 로그인합니다.
2. **Apps@Work** 아이콘을 누릅니다.
3. 검색(렌즈) 아이콘을 눌러 다음을 검색합니다.
    - **새 릴리스**-검색창에 텍스트를 입력하지 않으면 새로 출시된 앱 목록 표시

    - 텍스트를 입력하면 일치하는 해당 애플리케이션을 검색 필드에서 동적으로 예측하고 표시합니다.
    - 검색 결과 개수가 부제목으로 표시
    - 세부 정보 페이지로 이동하지 않고 **설치** 버튼을 눌러 애플리케이션을 설치할 수도 있습니다.


## 앱 설치 - 버튼 상태

앱 설치는 서버에서 요청을 처리하고 애플리케이션을 기기에 푸시해야 하기 때문에 설치 버튼이 실시간으로 진행 상황을 표시하지 않습니다. 설치 버튼은 설치 > 요청됨 > 설치됨에서 상태를 변경합니다.

**절차**

1. iOS 기기에서 Go app에 로그인합니다.
2. **Apps@Work** 아이콘을 누릅니다.
3. **설치**를 누르면 상태 알림이 다음과 같이 나타납니다.
    - 처음에는 설치가 요청되었음을 나타내는 경고 메시지가 나타납니다.
    - 요청됨 버튼을 누릅니다. 경고 메시지가 나타납니다.

    > 설치됨 상태는 버튼이 아닙니다.



## 추천 애플리케이션 및 배너

추천 탭은 관리자가 푸시한 구성을 기반으로 표시됩니다. 추천 탭은 사용 가능한 업데이트가 없을 때 표시되는 기본 랜딩 페이지입니다.



**절차**

1. iOS 기기에서 Go app에 로그인합니다.
2. **Apps@Work** 아이콘을 누릅니다.
3. **추천** 탭을 누릅니다.
    - 추천 앱 배너는 배너에 하나의 애플리케이션을 표시합니다.
    - 추천 앱에는 모든 추천 애플리케이션 목록이 포함되어 있습니다.



## 애플리케이션 업데이트 알림

최종 사용자는 사용 가능한 애플리케이션 업데이트가 있을 때 기기에서 알림을 받습니다. 알림에는 업데이트에 사용할 수 있는 애플리케이션 수가 포함됩니다. 사용자가 알림을 클릭하면 Apps@Work가 열립니다.

**절차**

1. iOS 기기에서 Go app에 로그인합니다. Apps@Work 아이콘은 보류 중인 업데이트가 있는 애플리케이션 수를 표시합니다.
2. 애플리케이션 업데이트 알림을 누르면 Apps@Work의 모든 앱 탭으로 리디렉션됩니다. 다음의 표시가 나타납니다.
    - 모든 앱 탭 아래의 사용 가능한 업데이트 하위 섹션에는 업데이트에 사용할 수 있는 애플리케이션 수가 표시됩니다.
    - 업데이트가 필요한 모든 애플리케이션에 대해 빨간색 점 아이콘이 표시됩니다.



## 설정-내 기기

**절차**

1. iOS 기기에서 Go app에 로그인합니다.
2. **설정** 아이콘을 누르세요.

- 내 기기 탭을 설정에서 사용할 수 있습니다.
- 이제 내 기기가 인증 아래의 개별 항목으로 나열됩니다.

# 8.5. iOS Go 고급 기능

키-값 쌍은 키(설정의 이름)와 값(적용하려는 구성)으로 이루어진 간단한 애플리케이션 설정입니다. Ivanti Go for iOS에서는 조직이 KVP를 사용하여 앱 업데이트 없이 기능을 활성화 또는 비활성화하거나 앱 동작을 조정할 수 있습니다.

Ivanti Go가 조직에서 관리되는 iPhone 또는 iPad에서 실행될 때, 시작 시 또는 체크인 과정에서 이러한 KVP 설정을 읽습니다. 앱은 업데이트를 즉시 적용하여 구성 변경 사항이 빠르고 일관되게, 그리고 올바른 사용자에게 전달되도록 합니다.

## Ivanti Go 앱 구성에서 KVP 사용

위반 메시지 사용자 정의용 KVP는 Ivanti Go 앱에서 지원됩니다. Ivanti Go 앱 설정 내에서 KVP를 구성하여 애플리케이션을 사용자 정의할 수 있습니다.

### 절차

1. AppCatalog에서 **Ivanti Go 앱**을 엽니다.
2. **구성**을 선택합니다.
3. **추가**를 클릭하여 새로운 **Apple 앱 구성**을 생성합니다.
4. KVP를 수동으로 추가합니다:
    - **키** 열에 사용자 정의하려는 구성 키를 입력합니다.
    - **값** 열에 기기에 적용하려는 값을 입력합니다.
5. (선택 사항) 적용하려는 사전 정의된 KVP가 포함된 *.plist* 파일을 업로드합니다.
6. 구성을 **저장**합니다.
7. 업데이트된 KVP는 다음 체크인 시 기기에 적용됩니다.

### 특정 iOS 앱에 plist 추가(여러 KVP용)

관리자는 앱 일련번호, 번들 식별자, 버전 정보 또는 기타 메타데이터를 사용하여 iOS 앱에 여러 키-값 쌍(KVP)을 구성할 수 있습니다. 이는 MDM용 Ivanti Neurons 콘솔에서 .plist 파일 업로드를 통해 효율적으로 수행할 수 있습니다.

### 절차

1. **앱**으로 이동합니다.
2. **앱 카탈로그**를 엽니다.
3. 구성하려는 **특정 iOS 앱**을 선택하여 엽니다.
4. 앱 구성 탭으로 이동합니다.
5. **Apple 관리형 앱 구성**을 선택합니다.
6. **추가 버튼**을 클릭합니다.
7. 구성의 **이름**을 입력합니다.
8. **.plist 사용**을 클릭합니다.
9. **해당 옵션 중 하나 선택**을 선택합니다.
10. plist 파일을 찾아 선택한 후 **열기**를 클릭합니다. 시스템이 plist의 키-값 쌍을 자동으로 구성 테이블에 채웁니다.
11. 구성을 적용할 사용자 그룹 또는 기기 그룹을 선택합니다.

12. **이 앱 구성 배포**를 클릭합니다.
13. **저장**을 클릭하여 과정을 완료합니다.

> 업로드한 파일은 반드시 .plist 확장자여야 합니다. 텍스트 편집기 등에서 파일을 수동으로 생성한 경우, 업로드하기 전에 확장자를 *.txt*에서 *.plist*로 변경해야 합니다.

# 등록 중 Ivanti Go를 단일 앱 모드로 실행

이 기능을 통해 관리자는 기기 등록 중 키-값 쌍을 사용하여 iOS용 Ivanti Go를 자동으로 단일 앱 모드(SAM)로 실행할 수 있습니다. 기기 등록이 시작되면, 구성된 키-값 쌍에 의해 Ivanti Go가 즉시 열립니다. 이 과정에서 사용자에게 다음 메시지가 표시됩니다:

기기가 구성되는 동안 기다려 주십시오.

이 동작을 활성화하려면, 등록 워크플로 이전 또는 도중에 단일 앱 모드 구성이 설치되어야 하며, 해당 구성은 iOS용 Ivanti Go를 대상으로 명시적으로 지정되어야 합니다. 등록이 성공적으로 완료되면, 단일 앱 모드가 자동으로 종료됩니다. 이후 해당 기기는 최종 사용자에게 정상적인 사용을 위해 전달되며, 등록 이후 사용을 제한하지 않으면서도 안전한 설정이 보장됩니다.

이 기능은 Ivanti Mobile@Work 환경을 지원하며, 감독된 iOS 기기를 위한 안전한 등록 흐름을 제공합니다.

## Zero Touch 활성화 설정

Ivanti Go의 Zero Touch 활성화를 실행하려면 다음 단계를 완료하십시오:

1. *Client Registered = No*인 기기만 포함하는 그룹을 설정합니다.
2. Ivanti Go 애플리케이션에 대한 단일 앱 모드(SAM) 구성을 생성합니다. 이 구성을 *1단계*에서 생성한 기기 그룹에만 할당합니다.
3. Ivanti Go 앱 구성에 zero_touch_activation 키-값 쌍(KVP)을 추가합니다. 이전 단계에서 사용한 동일한 기기 그룹을 대상으로 지정합니다.

## KVP 구성

| 키 | 값 | 유형 | 설명 |
|---|---|---|---|
| zero_touch_activation | True | Boolean | 값이 true로 설정되면, Ivanti Go 앱은 SAM 구성 설정을 통해 현재 단일 앱 모드(SAM)에서 실행 중임을 인식합니다. SAM 구성은 Ivanti Go 앱을 실행하며, 이 값은 앱이 SAM 모드에서 올바르게 작동할 수 있도록 하는 추가 설정으로 기능합니다. 등록이 완료되면 기기는 단일 앱 모드를 종료하고 최종 사용자가 정상적으로 사용할 수 있게 됩니다. |

# Ivanti Go에서 서비스로 복귀 버튼 활성화(iOS 18 이상)

**서비스로 복귀** 기능을 사용하면 데이터가 삭제된 후 기기가 자동으로 재등록되어, 삭제 이후 수동으로 기기를 다시 등록할 필요가 줄어듭니다.

관리자는 구성 가능한 키-값 쌍(KVP)을 사용하여 서비스로 복귀 버튼을 활성화하거나 비활성화할 수 있습니다. KVP가 앱 구성의 일부로 Ivanti Go에 배포되는 경우:

- 서비스로 복귀 옵션이 최종 사용자에게 표시됩니다.
- 사용자는 Ivanti Go에서 직접 재설정 과정을 시작할 수 있습니다.
- 기기는 Apple에서 관리되는 '서비스로 복귀' 재설정을 수행합니다.

- 관리 프로필과 필수 앱은 그대로 유지됩니다.
- 기기는 재프로비저닝 흐름을 완료하고 재사용할 준비가 됩니다.

이 기능은 iOS용 Ivanti Go에서 지원되며, DEP 모드로 등록된 iOS 18 이상 기기에서 사용할 수 있습니다.

### KVP 구성

MDM용 Ivanti Neurons의 Ivanti Go 관리형 앱 구성에 다음 KVP를 추가합니다:

| 키 | 값 | 설명 |
|---|---|---|
| ReturnToServiceEnabled | true | Ivanti Go에서 **서비스로 복귀** 버튼을 활성화합니다. false로 설정하거나 생략하면, 이 기능은 숨겨진 상태로 유지됩니다. |

## SAML 인증 화면에서 스크린샷 보호 비활성화

iOS용 Ivanti Go는 기기 등록 중 보안을 강화하기 위해 스크린샷 보호 기능이 내장되어 있습니다. 기본적으로 SAML 인증 화면을 통한 등록 시 다음이 차단됩니다:

- 스크린샷
- 화면 녹화
- 화면 공유

이 보호 기능은 사용자 이름, 암호 및 SAML 기반 로그인 콘텐츠와 같은 민감한 인증 데이터가 승인 없이 캡처되거나 공유되지 않도록 보장합니다.

관리자는 KVP 구성을 사용하여 관리형 기기에서 스크린샷 보호를 비활성화할 수 있습니다. 이 구성이 적용되면 Ivanti Go 앱은 SAML 인증 화면에서만 스크린샷 및 녹화를 허용하며, 앱 전체에서는 다른 모든 보안 메커니즘이 유지됩니다.

### KVP 구성

SAML 인증 화면에서 스크린샷 보호를 비활성화하려면 MDM의 Ivanti Go 앱 구성에 다음 KVP를 적용합니다:

| 키 | 값 | 설명 |
|---|---|---|
| SCREENSHOT_PROTECTION_DISABLED | True | SAML 인증 화면에서 스크린샷, 화면 녹화 및 화면 공유 보호를 비활성화합니다. 생략하거나 False로 설정하면 보호 기능은 기본적으로 활성화된 상태로 유지됩니다. |

## 정책 위반 메시지 사용자 정의용 KVP

이러한 KVP를 사용하면 관리자는 정책 위반이 감지될 때 최종 사용자에게 전송되는 메시지를 사용자 정의할 수 있습니다.

이 사용자 정의용 KVP는 관리자가 iOS용 Ivanti Go 앱 동작을 사용자 정의할 수 있도록 KVP 및 위반 유형을 설명합니다. 해당 KVP는 기기 사용자에게 상세 알림을 제공하거나 iOS용 Ivanti Go에서 연락처를 내보내는 등의 앱 동작을 정의합니다.

위반 유형은 서로 배타적이지 않습니다. 여러 위반이 있는 경우, iOS용 Ivanti Go에 메시지 목록이 표시됩니다.

| 키-값 쌍(KVP) | 기본 메시지 |
| --- | --- |
| compliance.message.COMPROMISED | • 탈옥으로 인해 기기가 손상되었습니다. 기기를 탈옥되지 않은 상태로 복원하거나 관리자에게 문의하여 이 문제 해결을 요청하십시오. |
| compliance.message.DATA_PROTECTION_DISABLED | • 데이터 보호를 위해 기업 액세스가 비활성화되었습니다. 관리자에게 문의하여 이 문제 해결을 요청하십시오. |
| compliance.message.OUT_OF_CONTACT | • iOS 기기가 연결되지 않았습니다. 관리자에게 문의하여 이 문제 해결을 요청하십시오. |
| compliance.message.APPS | • 기기에 필수 앱이 없거나 허용되지 않은 앱이 있습니다. 필수 앱을 추가/제거하거나 관리자에게 문의하여 이 문제 해결을 요청하십시오. |
| compliance.message.MDM_DISABLED<br><br>compliance.message.ROAMING | • MDM 기능이 비활성화되어 기기가 규정을 준수하지 않습니다. 기기를 다시 등록하거나 관리자에게 문의하여 이 문제 해결을 요청하십시오. |
| compliance.message.generic | • 알 수 없는 사유로 기업 액세스가 비활성화되었습니다. 관리자에게 문의하여 이 문제 해결을 요청하십시오. |
| compliance.message.header | 다음 사유로 인해 기기가 규정을 준수하지 않습니다:<br>위반 유형이 CUSTOM 또는 CUSTOM_NOTIFY_ONLY인 경우, 시스템은 헤더 없이 독립적인 메시지를 표시합니다. |
| compliance.message.CUSTOM | 기기에서 조치가 필요할 수 있습니다. 필요 시 관리자에게 문의하십시오. |
| compliance.message.CUSTOM_NOTIFY_ONLY | 기기가 규정을 준수하지 않으며 알림이 전송되었습니다. 자세한 내용은 알림 탭 또는 이메일을 확인하시기 바랍니다. |

위반 유형 목록에는 매핑된 메시지가 있는 위반이 포함되어 있지 않지만, 매핑된 메시지가 없는 위반이 하나 이상 포함되어 있는 경우 다음과 같은 기본 메시지를 표시합니다:

- 알 수 없는 사유로 기업 액세스가 비활성화되었습니다. 관리자에게 문의하여 이 문제 해결을 요청하십시오.

메시지 목록에 하나 이상의 위반 메시지가 포함된 경우, 목록 위에 다음 헤더를 표시합니다:
다음 사유로 인해 기기가 규정을 준수하지 않습니다:

기본 메시지를 변경하지 않으려면, 해당 메시지에 대한 키-값 쌍(KVP)을 포함하지 마십시오. 수정하려는 메시지에 대해서만 KVP를 정의하십시오.

## 관리형 앱 구성을 사용하여 기본 브라우저 및 이메일 클라이언트 구성

키 값 쌍(KVP)을 사용하면 관리자는 관리형 앱 구성을 통해 웹 링크를 열고 이메일을 작성할 때 **Ivanti Go**가 사용할 브라우저와 이메일 클라이언트를 구성할 수 있습니다.

관리자는 관리형 앱 구성 KVP를 사용하여 **지원** 탭 내에서 링크가 처리되는 방식을 다음과 같이 제어할 수 있습니다.

| 키 | 값 | 유형 | 설명 |
| --- | --- | --- | --- |
| default_browser | safari, edge, chrome, firefox, brave, opera, webatwork, duckduckgo | 문자열 | Ivanti Go가 지원 탭에서 웹 링크를 여는 데 사용하는 브라우저입니다. http/https 링크는 구성된 브라우저의 체계로 리디렉션됩니다. **구성되지 않은 경우 기본값**: 시스템 기본 브라우저. |
| Allow_browser_fallback | true, false | Boolean | **기본 브라우저가 설치되어 있지 않은 경우의 동작**:<br>**True**: 기본 시스템 브라우저로 폴백합니다.<br>**False**: 링크가 열리지 않고 사용자에게 "<Browser> 설치되지 않음" 경고가 표시됩니다.<br>**구성되지 않은 경우 기본값**: True |
| restrict_log_sharing_to_email | true, false | Boolean | 로그/지원 공유를 이메일로만 제한할지 여부를 나타냅니다(default_email 사용).<br>로그 자동 첨부는 Email+ 및 Native mail에서 작동합니다.<br>**allow_email_fallback**과 함께 작동합니다.<br>**True**: 이메일로만 공유합니다.<br>**False**: 표준 공유 옵션을 사용할 수 있습니다.<br>**구성되지 않은 경우 기본값**: false. |
| default_email | nativemail, outlook, gmail, yahoo, citrixmail.emailplus, spark, protonmail | 문자열 | Ivanti Go가 지원 탭의 mailto 링크에서 이메일을 작성하는 데 사용하는 이메일 클라이언트입니다. mailto는 클라이언트의 작성 URL로 변환됩니다 **구성되지 않은 경우 기본값**: 기본 메일 애플리케이션. default_email 클라이언트가 설치되어 있지 않은 경우 링크 확인 및 로그 공유에서 이중 역할을 합니다. |
| Allow_email_fallback | True, False | Boolean | **기본 이메일이 설치되어 있지 않은 경우의 동작입니다**.<br>**True**: 구성된 이메일 클라이언트가 설치되어 있지 않은 경우 이메일 작성에 기본 메일 애플리케이션이 사용되며, 로그 공유에는 대체 전달 방법을 사용할 수 있습니다.<br>**False**: 이메일 작성이 차단되며, 구성된 이메일 클라이언트를 사용할 수 없는 경우 사용자에게 "**설치되지 않음**" 경고가 표시됩니다. 로그 공유 제한은 폴백 옵션 없이 적용됩니다.<br>**구성되지 않은 경우 기본값**: true. (폴백 동작이 활성화됨) |

# 8.6. 앱 상세 정보 보기

앱 카탈로그에서 카탈로그 내 모든 앱에 관한 앱 상세 정보까지 드릴 다운할 수 있습니다. 표시 버전(예: 1.5.0), 번들 버전(예: 1.5.0.42), 최소 OS 버전 필수(예: Android의 경우 5.0) 등 앱의 상세 정보가 앱 상세 정보 페이지에 표시됩니다.

최소 OS 버전 필수 필드에 지정된 버전에 부합하지 않는 앱은 Apps@Work 카탈로그에 표시되지 않습니다. 따라서 해당 앱은 기기에 배포되도록 사용할 수 없습니다. 최소 OS 버전 필수 필드는 앱에 대한 감사 내역의 일환으로 표시되기도 합니다.

**절차**

1. **앱**을 클릭합니다.
2. **앱 카탈로그**를 클릭합니다.
3. 앱을 선택합니다.

앱 세부 정보 창이 표시됩니다.

> iOS 인하우스 앱의 경우 앱 세부 정보 페이지에서 **프로비저닝 프로필 만료 날짜**를 확인할 수 있습니다.

> 이제 앱 정보에 모든 iOS 및 iPadOS VPP 앱에 대한 옵션으로 **배포 시 M1 기기에 앱 설치 허용**이 표시됩니다. 관리자는 M1 macOS 기기에 설치할 수 있는 iOS 또는 iPad VPP 애플리케이션에 대해서만 **배포 시 M1 기기에 앱 설치 허용** 옵션을 활성화해야 합니다. 관리자는 이 옵션을 활성화해야만 애플리케이션 설치 중에 M1 macOS 기기를 볼 수 있습니다. 관리형 앱 구성은 M1 Mac 기기의 iOS VPP 애플리케이션에서 지원됩니다.

> iOS 및 macOS App Store 앱(B2B 포함)의 경우, **새 버전 동기화**는 App Store에서 앱 업데이트를 확인하고 동기화합니다. 업데이트된 앱 버전은 앱 동기화 일정에 따라 12~24시간 이내에 표시됩니다.

> **필수 앱**용 토글 버튼이 기기 상세 정보에 추가되었습니다. 관리자는 이 옵션을 선택하여 메인 앱의 필수 조건으로 앱을 추가할 수 있습니다.

앱이 여러 장치에 배포되면 **장치 요약** 탭에서 앱 배포 상태를 볼 수 있습니다. 장치 요약 탭에는 적격 장치 수, 앱이 설치된 장치 수, 앱 설치가 보류 중인 장치 수, 앱 설치에 실패한 장치 수에 대한 정보도 있습니다. 이 상자의 장치 수는 필수 앱 설치가 있는 장치를 기반으로 하므로 관리자는 필수 앱의 초기 배포를 추적할 수 있습니다.

일반 애플리케이션 수(사용자가 설치한 애플리케이션 포함)를 보려면 앱 인벤토리 검색을 이용하세요.

> 기기에서 제외된 앱은 배포 보류 중 상태입니다.

다음 표에는 iOS/OSX 앱에서 앱 설치가 실패하는 이유가 나열되어 있습니다.

| 이유 | 설명 |
| --- | --- |
| AppAlreadyInstalled | '앱이 이미 설치되었습니다.' |
| AppStoreDisabled | '앱 스토어가 비활성화되었습니다.' |
| CouldNotVerifyAppID | '앱 ID를 확인할 수 없습니다.' |
| 실패함 | '알 수 없는 오류로 인해 앱 설치에 실패했습니다.' |
| ManagedButUninstalled | '앱이 관리되지만 사용자가 삭제했습니다. 앱이 다시 설치되면(사용자가 하더라도) 다시 한번 관리됩니다.' |
| ManagementRejected | '사용자가 관리되지 않는 앱을 관리되는 앱으로 전환하는 것을 거부했습니다.' |
| NotAnApp | '앱이 아닌 자산으로 확인되는 잘못된 애플리케이션 식별자로 인해 InstallApplication 명령이 거부되었습니다.' |
| NotSupported | '지원되지 않는 앱입니다.' |
| 기타 | '새로 추가된 오류의 이유입니다.' |
| PurchaseMethodNotSupported | 'iOS 7 이상에서는 구매 방법이 잘못되면 앱을 설치할 수 없습니다(VPP 앱만 해당).' |
| UserInstalledApp | '관리 앱 설치가 이루어지기 전에 사용자가 앱을 설치했습니다.' |
| UserRejected | '사용자가 앱 설치 제안을 거부했습니다.' |
| UpdateRejected | '사용자가 앱 업데이트 제안을 거부했습니다.' |

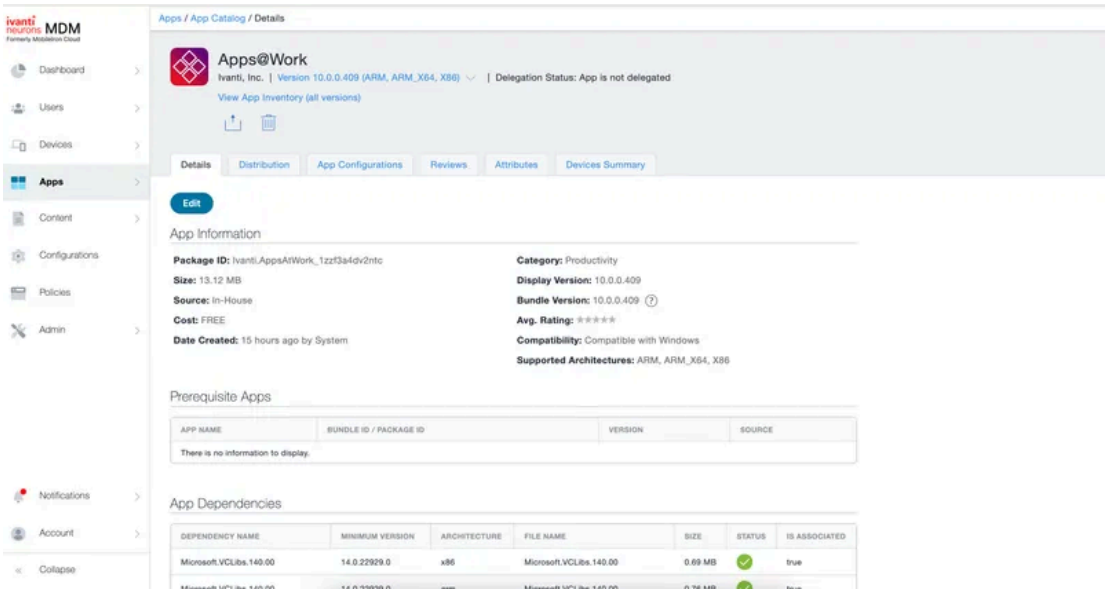
다음 표에는 Android 앱의 앱 설치 실패 이유가 나열되어 있습니다.

| 이유 | 설명 |
| --- | --- |
| USER_INSTALLED | '이미 장치에 설치되었습니다(MDM 외부).' |
| UNSUPPORTED | '지원되지 않습니다.' |
| USER_REJECTED_INSTALL | '사용자가 애플리케이션 설치를 거부했습니다.' |
| ERROR_INSTALL | '설치하는 동안 오류가 감지되어 설치하지 못했습니다.' |
| UNRECOGNIZED | '항목을 찾을 수 없거나 더 이상 추적되지 않습니다(예: 오류/장치에서 제거되고 추적에서 제거됨).' |
| UNSUPPORTED_INSTALL | '3.0 Android 클라이언트/22.0.0 서버용으로 업데이트됨: 설치 및 제거를 추적하는 특정 상태가 필요합니다.' |
| HIDDEN | '격리 중에는 숨김/제거됨 상태가 전송됩니다. 격리 해제는 다시 설치된 상태로 되돌립니다.' |
| 기타 | '새로 추가된 오류의 이유입니다.' |

Windows 장치의 경우 앱 구성에서 앱이 자동으로 설치되도록 설정된 경우 장치 요약에는 앱에 대하여 적격, 설치, 보류 또는 실패한 장치 수가 표시됩니다.

## 앱 세부 정보 페이지에서 앱 인벤토리 정보 보기

앱 인벤토리 정보를 보려면 **앱 인벤토리 보기(모든 버전)**를 클릭하여 **장치 > 앱 인벤토리**에서 해당 앱의 번들 ID별로 필터링된 목록을 확인합니다.



# 8.7. 앱 구성

이 섹션에는 다음 주제가 포함됩니다.

- 앱 기능 라이센스 관련
- 여러 앱에 공통되는 구성 단계
- 앱 숨기기 및 일시 중단(Android만 해당)
- 네트워크 릴레이 구성
- 셀룰러 5G 슬라이싱 구성
- 웹 콘텐츠 필터 구성을 사용하여 애플리케이션 배포
- DNS 프록시를 사용하여 애플리케이션 배포
- Android Enterprise 기기의 앱 캐시 지우기

앱 구성을 통해 사용자 기기에 배치하는 각 앱의 설치, 프로모션 및 배포를 사용자 지정할 수 있습니다. 앱은 자체 인하우스 앱, 공개 스토어의 앱 또는 MDM용 Ivanti Neurons 앱이 될 수 있습니다. 사용자는 각 수신자를 위해 특별히 맞추어진 고유 이름 및 구성으로 다른 여러 사용자와 그룹에 자유롭게 앱을 배치할 수 있습니다. 인하우스 애플리케이션 버전의 수는 100개로 제한됩니다. 해당 수가 초과되면, MDM용 Ivanti Neurons 시스템이 가장 오래된 버전의 애플리케이션을 제거합니다. 애플리케이션 업로드 및 제거 상태가 표시되며 감사 내역 페이지에서 볼 수 있습니다.

> App Catalog 또는 관리 앱 구성 프로필 내 앱의 앱 구성 값을 변경하는 경우 1 ~ 2번의 기기 체크인을 해야 기기에 새 구성 값을 받을 수 있습니다.

## 앱 기능 라이센스 관련

> 다음 기능을 이용하려면 별도의 라이센스가 필요합니다.

- 자동 앱 설치/제거: Silver 라이센스
- 퍼앱 구성: Gold 라이센스
- AppConnect 사용자 정의 구성: Gold 라이센스

향후 기기 유형이 Windows OS로 지정될 수 없으므로 여러 애플리케이션 패키지에는 훌륭한 그룹 관리가 필요합니다. 그러한 경우 적절한 앱 버전을 설치하는 유일한 방법은 관리자가 올바른 애플리케이션에 대해 올바른 그룹을 사용하는 것입니다.

## 여러 앱에 공통되는 구성 단계

이 단계를 먼저 실행한 다음 배치하고자 하는 각 앱의 구성 단계를 진행하십시오. 동일한 앱에 여러 구성을 설계할 수 있으며 각 구성에 고유 이름을 부여할 수 있습니다. 각 구성의 배포 및 프로모션 수준을 사용자의 배포 전략에 맞추어 설정할 수 있습니다. 인하우스 애플리케이션 버전의 수는 100개로 제한됩니다. 해당 수가 초과되면, MDM용 Ivanti Neurons 시스템이 가장 오래된 버전의 애플리케이션을 제거합니다. 애플리케이션 업로드 및 제거 상태가 표시되며 감사 내역 페이지에서 볼 수 있습니다. 한 번에 최대 100명의 사용자나 사용자 그룹, 기기, 기기 그룹에 애플리케이션을 배포할 수 있습니다. 앱 카탈로그에 추가할 앱을 선택할 수 있습니다. MDM용 Ivanti Neurons 에는 iOS 앱의 설치/업데이트 요청 전송 명령에 대한 비동기 프로세스가 있습니다. 설치/업데이트 요청 전송 명령을 사용하면 MDM용 Ivanti Neurons 관리 포털에 다음과 같은 메시지가 표시됩니다.

- 프로세스가 백그라운드에서 계속 실행됨
- 프로세스 완료됨

- 프로세스의 성공 여부 또는 오류 발생 여부 상태

**절차**

1. **앱 > App Catalog**로 이동하여 **+추가**를 클릭합니다.
2. 풀다운 메뉴를 사용하여 App Store, Google Play 또는 인하우스 앱 스토어를 선택하고 카탈로그에 추가할 앱을 선택합니다.
   라이센스 계약에 따라 사용자의 카탈로그에 앱을 추가하여 사용할 수 있습니다.
3. 필요에 따라 앱 범주를 편집합니다.
4. 필요에 따라 **설명** 필드에 앱에 대한 간단한 설명을 추가합니다.
5. **다음**을 클릭하세요.
6. 이 앱 구성의 배포 수준을 선택합니다.
   - **전체 사용자 대상** - 모든 사용자의 호환 기기에 앱이 추가됩니다.
   - **배포하지 않음** - 앱을 추후에 배포하도록 준비합니다.
   - **사용자 지정 배포** - 다음 옵션 중에서 선택합니다.
     - **사용자/사용자 그룹** - 선택한 사용자 또는 사용자 그룹에게만 앱이 배포됩니다.
       사용자를 선택하려면 **사용자** 탭을 클릭합니다.
       사용자 그룹을 선택하려면 **사용자 그룹** 탭을 클릭합니다.
     - **기기/기기 그룹** - 선택한 기기 또는 기기 그룹에게만 앱이 배포됩니다.
       기기를 선택하려면 **기기** 탭을 클릭합니다.
       기기 그룹을 선택하려면 **기기 그룹** 탭을 클릭합니다.
7. **다음**을 클릭하세요.

## 설치 옵션 구성하기

설치 구성 옵션을 선택할 수 있습니다.

**절차**

1. **애플리케이션 구성 설정 설치**를 클릭하거나 **+** 아이콘을 클릭하여 **구성 설정** 페이지에서 확인할 다른 구성을 추가합니다.
2. 구성 이름을 **이름** 필드에 입력합니다.
3. 필요에 따라 설치 구성에 대한 간단한 설명을 **설명** 필드에 입력합니다.
4. **기기 설치 구성** 옵션을 선택합니다.
5. 다음 옵션 중 하나를 선택합니다.
   - **기기에 설치 필요**
   - **기기 등록 시 한 번만 설치**
6. 이미 설치된 앱을 더 낮은 버전으로 다운그레이드하지 않으려면 **특정 앱 버전이 필요하지 않음** 옵션을 선택하십시오. 이 옵션은 최신 앱에 한하여 사용할 수 있었습니다.
7. 다음 옵션을 선택합니다.
   - **Samsung Knox 워크스페이스 및 Zebra 기기에 자동 설치**(Android만 해당)
   - **최종 사용자 앱 카탈로그에서 앱 표시 안 함**.
   - **새로 등록된 기기에 앱 설치 안 함**: 기존 기기는 영향을 받지 않으며 기기 앱 카탈로그에 앱이 계속 표시됩니다.
     - 이 배포에 새로 등록된 기기의 경우 앱이 나열되거나 푸시되지 않습니다.
     - 관리자가 설치/업데이트 명령을 보내면 해당 명령이 기기로 전송됩니다.

- **앱 업데이트 지연**: 이 옵션을 사용하여 새 앱 버전의 설치를 지연할 수 있습니다. 이 설정은 구성된 기간에 따라 새 앱 버전의 자동 설치를 지연합니다.
- **앱 업데이트 모드**(AMAPI 기기에도 지원됨). (Android만 해당)
  이 옵션에서 다음 세 가지 모드 중 하나를 사용하여 앱을 최신 버전으로 업데이트합니다.
  - **기본**: 앱 업데이트 모드 옵션을 선택하면 이 모드가 선택됩니다. 이 모드에서는 앱 사용이 가능한 때로부터 24시간 이내에 업데이트가 실행됩니다.
  - **90일 동안 연기**: 이 업데이트 모드를 선택하면 90일 동안 앱 업데이트를 연기할 수 있습니다. 90일 후 관리 Google Play 구성의 기타 설정에 따라 앱이 자동으로 업데이트됩니다.
  - **높은 우선순위**: 이 업데이트 모드를 선택하고 사용자 기기가 온라인 상태이면 Google Play 스토어에서 앱을 사용할 수 있게 된 직후에 앱이 업데이트됩니다.
- **앱 설치 우선 순위 설정** - 자세한 내용은 앱 우선순위 구성 항목을 참조하십시오.

> Android 장치에서는 자동 설치 옵션을 선택하지 않아도 자동 업데이트 옵션을 사용하여 앱 업데이트가 허용됩니다. 관리자는 필수가 아닌 앱이나 사용자가 직접 설치한 앱에 대한 앱 업데이트를 제어할 수 있습니다.

- **앱 사용 중 업데이트 안 함**: 사용자가 애플리케이션을 사용 중일 때 애플리케이션이 업데이트되지 않도록 하려면 이 옵션을 선택합니다. 이 옵션을 활성화하면 다음과 같이 작동합니다.
  - 애플리케이션이 포그라운드에서 실행되는 동안 애플리케이션 업데이트가 지연됩니다.
  - 사용자는 중단 없이 애플리케이션을 계속 사용할 수 있습니다.
  - 보류 중인 업데이트는 애플리케이션이 종료되거나 백그라운드로 이동하면 자동으로 설치됩니다.

**배포가 제거될 때 애플리케이션 제거됨(Android)**
관리되는 Google Play 애플리케이션의 경우 애플리케이션이 더 이상 기기에 할당되지 않으면 MDM용 Ivanti Neurons가 Android 기기에서 애플리케이션을 자동으로 제거합니다.
애플리케이션은 다음의 시나리오에서 제거됩니다.

- 애플리케이션 배포가 '아무에게도 배포 안 함'으로 변경됩니다.
- 애플리케이션이 App Catalog에서 삭제됩니다.
- 기기가 애플리케이션 배포에서 제외됩니다.

선택한 앱에 따라서 추가 구성 선택 항목이 있을 수도 있습니다. 이러한 선택 항목에는 여러 가지 키와 값 쌍을 추가하는 기능이 포함될 수 있습니다. 이런 경우에는 **+ 추가**를 클릭하여 키와 값 쌍을 입력합니다. 자세한 내용은 앱 카탈로그의 **공개 스토어에서 앱 추가 방법**을 참조합니다.

9. (macOS 11+) 앱을 관리되는 앱으로 설치 및 구성하려면 옵션을 선택합니다.
   - **관리되는 앱으로 설치**
   - **관리되는 앱으로 변환**

   > macOS 12.0+에서는 사용자 등록 기기에서 관리되는 앱 지원을 이용할 수 있습니다.

## 앱 숨기기 및 일시 중단(Android만 해당)

이제 Android 기기에서 **작업 프로필**, **완전 관리형 기기**, **작업 프로필이 있는 완전 관리형 기기**, **회사 소유 기기의 작업 프로필** 모드에서는 앱을 설치한 후 숨기거나 일시 중단할 수 있습니다.

**절차**

| | | |
|---|---|---|
| | 1. | 기기에 숨기기 또는 일시 중단 작업을 적용할 앱을 하나 이상 설치합니다. |
| | 2. | 앱 제어 구성을 만들고 숨기기 목록 또는 일시 중단 목록에 관리형 앱을 추가합니다. |
| 3. | | 기기에 변경 사항을 적용합니다. |

앱이 숨기기 목록과 일시 중단 목록에 모두 있다면, 숨기기 목록이 우선시되므로 앱은 숨겨집니다.

## 앱 우선순위 구성하기

처음으로 등록될 때(구체적으로 등록 날짜 및 시간 후 최초 20분 이내) 기기에서 앱이 수신되고 필수 앱이 설치를 위해 푸시되는 순서를 정의할 수 있습니다. 다른 앱 전에 특정 앱의 다운로드 우선순위를 지정할 수 있습니다. 예를 들어 중요하지 않은 다른 앱 전에 Tunnel 및 이메일 앱의 다운로드 우선순위를 지정하는 것입니다. 이 기능은 공개 및 비공개 앱에 적용됩니다. 필수 앱은 종속 앱 전에 푸시됩니다.

이 기능은 iOS(iOS용 AppStation 제외), Android(Enterprise용 Android 제외), macOS(인하우스 PKG 앱 및 Apple 앱 및 Books 앱) 및 Windows 기기에서 지원됩니다.

이 기능은 새로운 등록 기기에 대해 사용 가능합니다. 기본적으로 모든 앱은 보통 우선순위로 설정됩니다. 이 프로세스 중에 사용자는 설치할 리소스를 놓고 앱이 경쟁하고 우선순위가 높은 앱보다 먼저 대기할 수 있지만 카탈로그에 있는 앱을 수동으로 설치하도록 선택할 수 있습니다.

Windows 앱의 경우 Bridge 앱이 다른 앱보다 우선순위가 가장 높습니다.

**앱 설치 우선순위 설정** 옵션을 사용하여 앱 우선순위를 설정하는 절차는 이전 섹션인 "설치 옵션 구성하기"를 참조하십시오. 앱의 우선순위는 높음, 중간 또는 낮음으로 설정할 수 있습니다. 동일한 우선순위를 가진 앱은 특별한 순서 없이 설치됩니다. 사용자가 이미 앱을 설치했을 때는 앱 업데이트 중 앱 우선순위가 사용되지 않습니다.

## Apple 애플리케이션 관리 구성 설정 선택

이 설정은 이 앱에만 적용되고 **앱 > 카탈로그 설정**에서 선택한 모든 글로벌 설정을 재정의합니다. **Apple 앱 관리** 설정 선택 섹션을 참조하십시오.

**절차**

1. **Apple 앱 설정**을 클릭하거나 **+** 아이콘을 클릭하여 **구성 설정** 페이지에서 확인할 다른 구성을 추가합니다.
2. 구성 이름을 **이름** 필드에 입력합니다.
3. 구성에 대한 간단한 설명을 **설명** 필드에 입력합니다.
4. **Apple 관리 설정**에서 다음 옵션 중 하나 이상을 선택하거나 선택 해제합니다.
   - **iCloud 및 iTunes에 대한 백업 방지**
   - **미등록 앱 제거**
   - (iOS 14.0+) **이 앱의 제거 및 오프로딩 허용** - 이 옵션을 선택 해제하여 사용자가 관리형 앱을 제거 및 오프로딩하지 못하도록 할 수 있습니다.
   - (선택 사항) **Apple 관리형 앱 구성** 추가
5. **업데이트**를 클릭합니다.

## 앱 프로모션 수준 선택

앱의 프로모션 수준을 설정할 수 있습니다.

**절차**

1. **프로모션 배포 구성 설정**을 클릭하거나 **+** 아이콘을 클릭하여 **프로모션 구성** 페이지에서 확인할 다른 구성을 추가합니다.
2. **편집**을 클릭합니다.
3. 프로모션 배포 구성 설정 이름을 **이름** 필드에 입력합니다.
4. 필요에 따라 설치 구성에 대한 간단한 설명을 **설명** 필드에 입력합니다.
5. 앱이 수신하고자 하는 프로모션 수준, 즉 **추천 안 함**, **추천 리스트** 또는 **추천 배너** 사용을 선택합니다. **추천 안 함**을 선택하면 해당 앱이 열거되지 않습니다.
6. 추천 배너를 선택한 경우 다음 세부 정보를 지정합니다.
    1. **제목** - 애플리케이션 제목을 지정합니다.
    2. **설명** - 애플리케이션 세부 정보를 지정합니다.
    3. **배너 스타일** - 배너 색상을 선택합니다.
7. **+설명 추가**를 클릭하여 구성에 대한 간단한 설명을 입력합니다.
8. 필요에 따라 구성 배포를 변경합니다.
9. **완료**를 클릭하여 앱 구성을 저장합니다.

## AppTunnel 트래픽 규칙 구성

AppTunnel 구성을 이용해 Sentry를 통해 특정 서비스에 대한 액세스를 허용하는 트래픽 규칙을 다음과 같이 정의합니다.

AppTunnel 구성 추가에 대한 내용은 *MDM용 Ivanti Neurons에 관한 AppConnect 가이드*의 "AppTunnel 구성 추가"를 참조하십시오.

## 관리 앱 구성

**절차**

1. **+** 아이콘을 클릭하여 구성 페이지를 엽니다.
2. **+설명 추가**를 클릭하여 구성에 대한 간단한 설명을 입력합니다.
3. **+ 추가**를 클릭하여 키와 값을 입력합니다.
4. 배포 수준을 선택합니다.
5. **다음**을 클릭하세요.

## 퍼앱 VPN을 사용하여 각 앱의 VPN 구성하기

**절차**

1. **+** 아이콘을 클릭하여 구성 페이지를 엽니다.
2. 이 앱의 VPN 이름을 **이름** 필드에 입력합니다.
3. **+설명 추가**를 클릭하여 구성에 대한 간단한 설명을 입력합니다.
4. **이 앱의 퍼앱 VPN 활성화** 옵션을 클릭하고 이용 가능한 퍼앱 VPN 구성을 선택합니다.
5. (선택 사항) macOS 앱의 경우 식별자 "\%s\" 형식으로 **지정된 요구 사항** 문자열을 입력합니다. 예: 식별자 "com.google.Chrome". 이 필드로 여러 패키지 macOS 앱을 활성화하여 Tunnel 같은 퍼앱 VPN을 사용합니다.

6. **이 앱 구성 배포**의 방법을 선택합니다.
7. **다음**을 클릭하세요.

## Apple 관리 앱 구성 사용하기

Apple 관리 앱 구성을 사용하면 설치된 관리 앱에 특정한 설정을 구성할 수 있습니다. 애플리케이션에는 개발자가 실행하거나 제한하는 구성 매개 변수가 있을 수 있습니다. 이러한 제한이 있는 애플리케이션의 경우 구성 옵션이 제한적으로 표시될 수 있습니다. Apple에서 관리되는 앱을 구성할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 앱을 선택합니다.
3. **앱 구성** 탭을 클릭합니다.
4. **Apple 관리 앱 구성** 또는 **+** 버튼을 클릭합니다.
   Apple 관리 앱 구성에 몇 가지 기본 구성 설정이 있습니다.
5. 필요한 경우 **추가**를 클릭하여 다른 구성을 추가합니다. 필요에 따라 구성의 이름을 클릭하여 구성을 편집합니다.
6. **구성 소스**에서 다음 **소스 유형** 옵션 중 선택합니다.

- **AppConfig 커뮤니티** - 이 옵션은 커뮤니티 리포지토리에서 사용할 수 있는 앱 구성 사양이 있는 앱에만 사용 가능합니다. 이 옵션을 사용할 수 있는 경우 기본적으로 선택되어 있습니다.
- **.xml 사양 사용** - 이 옵션을 선택하여 앱이 특정 앱 구성 버전을 푸시할 수 있는 스키마를 업로드합니다. **파일 선택**을 클릭하여 .xml 파일을 업로드합니다. .xml 파일에 번들 ID와 버전이 포함되어 있는지 확인하십시오. 파일의 번들 ID가 앱의 번들 ID와 일치하지 않을 경우에는 오류 메시지가 표시됩니다.
- **없음** - 앱에 대해 어떠한 스키마도 적용하고 싶지 않을 경우에는 이 옵션을 선택합니다. 이 옵션은 **AppConfig 커뮤니티** 옵션을 사용할 수 없는 경우 기본적으로 선택되어 있습니다.
  업로드한 .xml 파일이 **구성 소스** 섹션에 표시됩니다. 삭제 아이콘을 클릭하여 업로드한 .xml 파일을 삭제합니다.

7. **Apple 관리 앱 설정**에서는 구성 옵션을 설정하여 키 값 쌍을 입력할 수 있습니다.

- **추가**를 클릭하여 키 값 쌍을 관리형 앱 구성에 추가하면 iReg 또는 Apple 기기 등록 중에 Go 클라이언트에서 등록 이름 ID를 검색할 수 있습니다.
  키 값 쌍에 대한 데이터 형식(String, Integer, Boolean, Long Float, Double, Date, String Array, Integer Array, Double Array, Float Array, Long Array)을 선택할 수 있습니다.

> iReg 또는 Apple 기기 등록 도중 Go 클라이언트별 등록 이름 정보를 검색하려면 관리 앱 구성에 다음과 같은 키 값 쌍을 추가하십시오.

| 키 | 값 | 유형 |
|---|---|---|
| registration.username | $ | 문자열 |
| registration.token | $ | STRING |
| registration.token.expirationSeconds | $ | 문자열 |
| registration.url | $ | 문자열 |

iReg 또는 Apple 장치 등록 중에 mac 에이전트(Mobile@Work)에서 등록 이름 ID를 검색하려면 관리형 앱 구성에 다음의 키 값 쌍을 추가합니다:

| 키 | 값 | 유형 |
|---|---|---|
| 클라이언트 등록 URL | $ | 문자열 |
| 토큰 | $ | 문자열 |
| TokenExpiresAt | $ | 문자열 |

최종 사용자가 Ivanti Go 애플리케이션을 종료하는 경우 **편집**을 클릭하여 다음 중 하나를 수행하도록 애플리케이션을 설정합니다.

| 키 | 값 | 유형 |
|---|---|---|
| 기본 알림을 표시하려면 다음 값을 사용합니다. | | |
| enableAppTerminationNotification | 참/거짓 또는 1/0 | 부울 OR 문자열 |
| 사용자 지정 알림을 표시하려면 다음 값을 사용합니다. | | |
| appTerminationNotificationMessage | 사용자 지정 알림 | 문자열 |
| enableAppTerminationNotification | 참/거짓 또는 1/0 | 부울 OR 문자열 |

- **.plist 사용** - .plist 파일에는 대량으로 업로드할 여러 개의 키 값 쌍이 포함되어 있습니다. **파일 선택**을 클릭하여 .plist 파일을 업로드합니다. 검증된 plist 데이터가 **Apple 관리 앱 설정** 표에 표시됩니다.

중첩된 사전이 있는 plist는 유효하지 않습니다.

8. **업데이트**를 클릭하여 항목을 저장합니다.

## 네트워크 릴레이 구성

VPN에 연결하지 않아도 앱의 네트워크 트래픽을 더 사적이고 안전하게 만들기 위함입니다. 자세한 내용은 네트워크 릴레이 구성을 참조하십시오.

1. **네트워크 릴레이 + 아이콘**을 클릭하여 구성 페이지를 엽니다.
2. 이름 필드에 이 앱의 **네트워크 릴레이** 이름을 입력합니다.
3. + **설명 추가**를 클릭하여 구성에 대한 간략한 설명을 입력합니다.
4. 이 앱에 대해 **네트워크 릴레이 활성화** 옵션을 클릭하고 사용 가능한 **네트워크 릴레이 구성**을 선택합니다.
5. 이 앱 구성의 **배포** 방법을 선택합니다.
6. **다음**을 클릭하세요.

## 셀룰러 5G 슬라이싱 구성

셀룰러 5G 네트워크 슬라이싱 지원을 사용하면 (모든 iOS 앱에서) 개별 관리형 앱을 특정 네트워크 기능과 특성을 제공하는 네트워크 슬라이스에 할당할 수 있어 앱 경험을 최적화할 수 있습니다. 할당은 MDM 앱 설치 명령 또는 선언적 앱 구성에서 새로운 **CellularSliceUUID** 앱 속성을 사용하여 수행됩니다. 키에 넣을 네트워크 슬라이스의 문자열 값은 지원 통신사에서 제공해야 합니다.

> 특정 앱이나 전체 장치가 VPN을 사용하도록 구성된 경우 5G 네트워크 슬라이싱은 사용되지 않습니다.

**Procedure절차**

1. **앱 > 앱 카탈로그 > 앱 구성 > 셀룰러 5G 슬라이싱**으로 이동하고 **추가**를 클릭합니다.
2. **구성 설정** 섹션에서 다음 필드를 업데이트합니다.
   - 이름
   - **5G 네트워크 슬라이싱 활성화** 옵션을 선택하십시오.
   - **DNN** 또는 **앱 카테고리**(네트워크 제공업체에 따라 다름)를 선택하십시오.
3. 이 앱 구성의 배포 수준을 선택합니다.
4. **저장**을 클릭하세요.

## 웹 콘텐츠 필터 구성을 사용하여 애플리케이션 배포

웹 콘텐츠 필터 구성을 사용하여 DNS 프록시 서버 대신 애플리케이션을 배포할 수 있습니다. 웹 콘텐츠 필터 구성을 생성한 후 배포용 애플리케이션에 구성을 추가할 수 있습니다. 웹 콘텐츠 필터 구성에 대한 자세한 내용은 **웹 컨텐츠 필터**를 참조하십시오.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. 앱을 선택합니다.
3. **다음**을 클릭하세요.
4. 위임 옵션을 선택하고 **다음**을 클릭합니다.
5. 배포 옵션을 선택하고 **다음**을 클릭합니다.
6. **웹 콘텐츠 필터 구성**을 선택하고 **+** 아이콘을 클릭합니다.
7. **이름**을 지정합니다.
8. **이 앱에 대해 웹 콘텐츠 필터 사용** 확인란을 선택합니다.
9. 드롭다운 메뉴에서 **웹 콘텐츠 필터**를 선택합니다.
10. 이 앱 구성의 배포 수준을 선택합니다.
    1. **전체 사용자 대상** - 모든 사용자의 호환 기기에 앱이 추가됩니다.
    2. **배포하지 않음** - 앱을 추후에 배포하도록 준비합니다.
    3. **사용자 지정 배포** - 다음 옵션 중에서 선택합니다.
       - **사용자/사용자 그룹** - 선택한 사용자 또는 사용자 그룹에게만 앱이 배포됩니다.
         사용자를 선택하려면 **사용자** 탭을 클릭합니다.
         사용자 그룹을 선택하려면 **사용자 그룹** 탭을 클릭합니다.
       - **장치/장치 그룹** - 선택한 장치 또는 장치 그룹에만 앱이 배포됩니다.
         기기를 선택하려면 **기기** 탭을 클릭합니다.
         기기 그룹을 선택하려면 **기기 그룹** 탭을 클릭합니다.
11. **다음**을 클릭하세요.

12. **완료**를 클릭합니다. 선택한 앱은 웹 콘텐츠 필터 구성을 통해 특정 사용자에게 배포됩니다.

## DNS 프록시를 사용하여 애플리케이션 배포

DNS 프록시 구성을 사용하여 애플리케이션을 배포할 수 있습니다. DNS 프록시 구성을 생성한 후 배포용 애플리케이션에 구성을 추가할 수 있습니다. DNS 프록시 구성에 대한 자세한 내용은 **DNS 프록시 구성 생성**을 참조하십시오.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. 앱을 선택합니다.
3. **다음**을 클릭하세요.
4. 위임 옵션을 선택하고 **다음**을 클릭합니다.
5. 배포 옵션을 선택하고 **다음**을 클릭합니다.
6. **DNS 프록시 구성**을 선택하고 **+** 아이콘을 클릭합니다.
7. **이름**을 지정합니다.
8. **이 앱에 대해 DNS 프록시 사용** 확인란을 선택합니다.
9. 드롭다운 메뉴에서 DNS 프록시를 선택합니다.
10. 이 앱 구성의 배포 수준을 선택합니다.
    1. **전체 사용자 대상** - 모든 사용자의 호환 기기에 앱이 추가됩니다.
    2. **배포하지 않음** - 앱을 추후에 배포하도록 준비합니다.
    3. **사용자 지정 배포** - 다음 옵션 중에서 선택합니다.
        - **사용자/사용자 그룹** - 선택한 사용자 또는 사용자 그룹에게만 앱이 배포됩니다.
          사용자를 선택하려면 **사용자** 탭을 클릭합니다.
          사용자 그룹을 선택하려면 **사용자 그룹** 탭을 클릭합니다.
        - **장치/장치 그룹** - 선택한 장치 또는 장치 그룹에만 앱이 배포됩니다.
          기기를 선택하려면 **기기** 탭을 클릭합니다.
          기기 그룹을 선택하려면 **기기 그룹** 탭을 클릭합니다.
11. **다음**을 클릭하세요.
12. **완료**를 클릭합니다. 선택한 앱은 DNS 프록시 구성을 통해 특정 사용자에게 배포됩니다.

## 앱 구성 설정 복제

동일한 설정을 다른 기기에 적용할 수 있도록 관리되는 앱의 구성 설정을 복제할 수 있습니다. 복제된 설정을 변경하고 이름을 변경할 수도 있습니다.

**안드로이드**

Android 기기에서 구성 설정을 복제할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 구성 설정을 복제할 앱을 선택합니다.
3. **앱 구성**을 클릭합니다.

4. **앱 구성 요약** 섹션에는 Android 기기에서 사용할 수 있는 구성 목록(**Android용 관리되는 구성**, **기기에 설치**, **프로모션**, **위임된 기기 권한**, **Google Play 릴리스**)이 있습니다.
5. 사용 가능한 구성을 클릭합니다.
6. **작업**에서 **복제**를 클릭하여 복제 프로세스를 시작합니다.
7. 기본적으로, 복제된 구성 이름은 <Copy of the Cloned Configuration name>이 됩니다. 그러나 **이름** 상자에 원하는 이름을 입력하여 이름을 수정할 수 있습니다.
8. (선택 사항) **설명** 상자에 복제된 설정에 대한 텍스트를 입력합니다.
9. **계속**을 클릭하세요.

앱 구성 설정 복제가 완료되었음을 나타내는 확인 창이 나타납니다. 앱 구성 요약 및 복제된 앱 내에서 복제된 버전을 볼 수 있습니다.

**iOS**

iOS 기기에서 관리되는 앱 구성 설정을 복제할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 구성 설정을 복제할 앱을 선택합니다.
3. **앱 구성**을 클릭합니다.
4. **앱 구성 요약** 섹션에는 iOS 기기에서 사용할 수 있는 구성 목록(**기기에 설치**, **Apple 앱 설정**, **프로모션**, **AppConnect 사용자 지정 구성**, **앱 터널**, **Apple에서 관리되는 앱 구성**, **앱 VPN당**)이 있습니다.
5. 복제하고자 하는 필수 구성을 클릭합니다.
6. **작업**에서 **복제**를 클릭하여 복제 프로세스를 시작합니다.
7. 기본적으로, 복제된 구성 이름은 <Copy of the Cloned Configuration name>이 됩니다. 그러나 **이름** 상자에 원하는 이름을 입력하여 이름을 수정할 수 있습니다.
8. (선택 사항) **설명** 상자에 복제된 설정에 대한 텍스트를 입력합니다.
9. **소스 유형** 목록에서 구성 소스를 선택합니다.
10. **Apple에서 관리되는 앱 설정** 섹션에 **키**, **값**을 입력하고 목록에서 **유형**을 선택합니다.
    **키**, **값**, **유형**에 대한 자세한 내용은 **Apple에서 관리되는 앱 구성 사용**을 참조하십시오.
11. **계속**을 클릭하세요.
    앱 구성 설정 복제가 완료되었음을 나타내는 확인 창이 나타납니다. **Apple에서 관리되는 앱 구성 사용** 섹션에서 복제된 버전을 볼 수 있습니다.

**Windows**

Windows 기기에서 앱 구성 설정을 복제할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 구성 설정을 복제할 앱을 선택합니다.
3. **앱 구성**을 클릭합니다.
4. **앱 구성 요약** 섹션에는 **기기에 설치** 및 **프로모션** 구성이 있습니다.
5. 복제하고자 하는 필수 구성을 클릭합니다.
6. **작업**에서 **복제**를 클릭하여 복제 프로세스를 시작합니다.

7. 기본적으로, 복제된 구성 이름은 <Copy of the Cloned Configuration name>이 됩니다. 그러나 **이름** 상자에 원하는 이름을 입력하여 이름을 수정할 수 있습니다.
8. (선택 사항) **설명** 상자에 복제된 설정에 대한 텍스트를 입력합니다.
9. **계속**을 클릭하세요.

앱 구성 설정 복제가 완료되었음을 나타내는 확인 창이 나타납니다. 앱 구성 요약 및 복제된 앱 내에서 복제된 버전을 볼 수 있습니다.

## 인하우스 카탈로그용 Windows 10 앱 선택하기

인하우스 앱 카탈로그에 추가할 앱을 선택합니다. 인하우스, Microsoft Store, 비즈니스용 Microsoft 앱은 Windows 10에서 지원됩니다. Windows 10은 사용자가 허용하거나 허용하지 않는 앱을 기반으로 기기에 직접 컴플라이언스를 적용합니다.

> Windows 10 체크인 주기는 기본적으로 60분에 1회입니다. 기기 및 앱 상태를 업데이트하기 위해 강제로 기기 체크인을 시행할 수 있습니다.

지원되는 조치는 다음과 같습니다.

- 새로운 앱 업로드
- 자동 설치
- Apps@Work에서 수동으로 설치
- 새 버전의 앱 추가
- 앱 삭제

지원되는 형식은 다음과 같습니다.

- APPX
- APPXBUNDLE
- MSI 래핑된 Win32 - 사전 포함된 Win32 앱
- MSIX(RS5 및 Windows 10 이상 기기에서 지원됨)
- .EXE(Bridge 사용)

> **Ivanti Neurons 에이전트** 앱은 **Windows** 장치용 **앱 카탈로그**에서 사용 가능합니다. 관리자는 **Ivanti Neurons 에이전트** 앱을 사내 앱으로 배포할 수 있으며, 따라서 Windows 장치에 이 앱을 배포할 수 있습니다.

## Windows 10 앱 구성

**절차**

1. 주 탐색 표시줄에서 **기기**를 클릭합니다.
2. MDM용 Ivanti Neurons에 등록한 Windows 10 기기를 선택합니다.
3. **앱 > 앱 카탈로그**를 클릭합니다.
4. 앱을 선택합니다.
5. **작업** 풀다운 메뉴를 사용하여 카탈로그에서 앱을 추가하거나 삭제합니다.
   필요에 따라 새 버전의 앱을 추가합니다.
   - **작업** 풀다운 메뉴를 클릭합니다.

- **새 버전 추가**를 선택합니다.
- 카탈로그에서 새 버전의 앱을 선택합니다.
- **업데이트 및 저장**을 클릭하면 앱 정보 화면이 표시됩니다.

6. **버전** 풀다운 메뉴를 이용해 사용할 버전을 선택합니다.
7. **편집**을 클릭하여 상세 정보를 변경합니다.
   - 필요 시 **범주**를 편집합니다.
   - 필요 시 **설명**을 입력합니다.
   - 필요한 경우 스크린샷을 추가합니다.
8. **저장**을 클릭합니다.
9. **배포** 탭을 클릭하고 **편집**을 클릭하여 배포 수준을 변경합니다.
10. **저장**을 클릭합니다.
11. **앱 구성** 탭을 클릭하여 현재 구성의 요약을 확인합니다.
12. 필요한 경우 앱 설명을 입력합니다.
13. 앱 구성 요약 페이지에서 **기기에 설치**를 클릭합니다.
    자동 설치가 기본 설정이며 변경할 수 없습니다.
14. 좌측 탐색 창에서 **프로모션**을 클릭하고 **프로모션 배포 구성 설정**을 클릭하여 프로모션 수준을 변경합니다.
    - **편집**을 클릭하여 프로모션 수준 설정을 변경합니다.
    - 구성 이름을 입력합니다.
    - 구성 설명을 입력합니다.
    - 프로모션 수준을 선택합니다.
    - **업데이트**를 클릭하여 변경 사항을 저장합니다.
15. **검토** 탭을 클릭하여 검토 정보를 확인합니다.
    필요한 경우 스프레드시트에 평가 데이터를 내보내기합니다.

## Windows 10 앱 구성 설정 편집하기

**절차**

1. **정책 > 구성**을 클릭합니다.
2. **+추가**를 클릭합니다.
3. **Windows 앱 제어**를 선택하여 **Windows 앱 제어 구성** 화면을 확인합니다.
4. 구성의 **이름**과 **설명**을 입력합니다.
5. 앱 유형의 정의는 다음과 같습니다.
   - 허용됨(허용 목록으로 설정됨) - 해당 앱만 허용됩니다. 기기에 이미 설치되지 않은 경우 해당 앱이 자동으로 설치됩니다.
   - 허용되지 않음(차단 목록으로 설정됨) - 기기에 설치되어 있는 경우, 시작 시 해당 앱이 차단됩니다.
6. 앱 유형 및 앱 식별자에 대한 규칙 정의를 명시합니다.
7. **앱 조회**를 클릭하여 **Windows 10 앱 검색** 화면을 확인합니다.
8. 앱 이름을 입력하여 Windows 스토어를 검색합니다.
9. 표시된 선택에서 앱을 선택하여 앱 식별자에 추가합니다.

10. 필요에 따라 앱 유형 풀다운 메뉴를 이용해 앱 식별자에 경로 정의를 설정하여 특정 경로를 이용한 앱을 허용 또는 허용하지 않거나 해당 경로에 설치된 모든 앱을 차단합니다.
    앱 유형 **게시자/PFN 같음**은 PFN을 지원하는 Windows 10 이상의 장치에 적용됩니다. **EXE/Win32 같음**.
11. **다음**을 클릭하세요.
12. 배포 수준을 선택합니다.
    - **모든 기기**.
    - **기기 없음**.
    - **사용자 지정** - 앱을 수신할 사용자나 그룹을 입력합니다.
13. **완료**를 클릭합니다.
14. 앱 유형을 선택하고 앱 식별자를 명시할 규칙 정의를 편집할 수 있습니다.
    - **작업** 풀다운 메뉴를 클릭합니다.
    - **새 버전 추가**를 선택합니다.
    - 새 버전의 앱을 선택합니다.
    - **업데이트 및 저장**을 클릭하면 **앱 정보** 화면이 표시됩니다.

## Windows의 설치 후 기기 재부팅 옵션 구성

**설치 후 기기 재부팅** 옵션을 사용하면 앱 설치 후 기기를 재부팅하도록 구성할 수 있습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 목록에서 Windows 앱을 선택합니다.
3. **앱 구성 > 기기에 설치 > 애플리케이션 설치 구성 설정**으로 이동합니다.
4. **편집**을 클릭하고 **설치 후 기기 재부팅** 옵션을 ON으로 설정합니다.
5. 장치를 재부팅할 일정 옵션 중 하나를 선택합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| **설치 직후** | 애플리케이션을 설치한 직후 장치를 재부팅하려면 이 옵션을 선택합니다. |
| **하루 중 특정 시간에** | 애플리케이션을 설치한 후 하루 중 특정 시간에 장치를 재부팅하려면 이 옵션을 선택합니다. |
| **몇 분 후** | 애플리케이션을 설치한 후 **15**분, **30**분, **60**분 또는 **120**분 후에 장치를 재부팅하려면 이 옵션을 선택합니다. |

6. **업데이트**를 클릭합니다.

예정된 시간에 기기가 재부팅됩니다.

> 공개 앱이나 MSB(Microsoft Store for Business) 앱의 경우 **앱 구성** 섹션에서 **Windows 기기에서 자동으로 설치** 설정을 ON으로 지정해야 합니다.

## Apps@Work를 사용해 앱을 설치

Apps@Work를 사용해 앱을 설치하려면:

1. **Apps@Work** 앱을 클릭합니다.
   관리자 이메일 주소 및 서버 URL이 Apps@Work 로그인 대화 상자에 이미 입력되어 있습니다.
2. 비밀번호를 입력하고 로그인을 클릭하여 앱 페이지를 표시합니다.
3. 설치할 앱을 선택합니다. 필수 설치 앱이 클라이언트에 설치되어 있지 않을 경우 필수 설치 앱에 대한 종속성이 있는 앱을 설치할 수 없습니다.
   iOS 기기용 Apps@Work의 경우 필요에 따라 **모두 설치** 버튼을 클릭하여 모든 앱을 설치할 수 있습니다. 이 옵션은 **새 릴리스**, **추천 앱** 및 **범주** 화면에서 사용할 수 있습니다.

> Apps 및 Books 앱 라이센스를 앞서 수락하지 않은 경우에는 Apps 및 Books 앱이 설치되지 않습니다.

4. **업데이트 및 저장**을 클릭하면 **앱 정보** 화면이 표시됩니다.

### Android Enterprise 기기용 앱 설치 및 업데이트

관리자는 일반 사용자가 액세스할 수 있도록 앱을 카탈로그에 게시하는 동시에, 즉시 사용할 수 있도록 특정 기기에 배포할 수도 있습니다. 이렇게 하면 사용자는 앱을 직접 받을 수 있고, 앱은 카탈로그에서도 사용 가능하므로 다른 사용자들도 필요에 따라 설치할 수 있습니다.

앱 및 업데이트 설치 방법

1. **앱 > 앱 카탈로그**로 이동합니다.
2. 원하는 앱을 선택합니다.
3. **세부 정보** 화면에서 **작업**을 클릭합니다. **설치/업데이트 요청 전송**이 표시됩니다.
4. 설치/업데이트 요청 전송을 클릭합니다. **설치/업데이트 요청 전송** 대화 상자가 표시됩니다.
5. **기기에 이 애플리케이션의 설치 및 업데이트 알림 전송**에서 다음을 수행합니다.
   - 새 애플리케이션을 설치하려면 **새 애플리케이션 요청 전송(아직 앱이 설치되지 않은 기기에 적용)** 확인란을 선택합니다.
   - 설치된 애플리케이션을 업데이트하려면 **업데이트 요청 전송(앱이 설치되어 있지만 업데이트가 있는 기기에 적용)** 확인란을 선택합니다.
6. **요청을 전송할 사용자 선택** 아래에서 다음을 수행합니다.
   - 호환되는 모든 사용자에게 구성을 배포하려면 **모든 사용자**를 클릭합니다. 그러면 사용자의 앱 카탈로그에 앱이 나타납니다.
   - 앱 카탈로그에서 애플리케이션을 보는 사용자 그룹 또는 사용자를 정의하려면 **사용자 정의**를 클릭합니다.

     > **설치/업데이트 요청 전송** 배포는 앱 배포 프로세스의 일부입니다. **배포** 화면에서 선택하는 설정에 따라 앱을 받을 기기가 정해집니다.

앱 설치가 완료되었음을 나타내는 확인 창이 표시됩니다.

새 설치 또는 업데이트에 따른 변경 사항은 **대시보드** > **감사 내역**에 표시됩니다.

> 공개 앱 및 비공개 앱의 경우, **업데이트 요청 전송(앱이 설치되어 있지만 업데이트가 있는 기기에 적용)**이 비활성화됩니다. **새 애플리케이션 전송 요청**만 허용됩니다.

**관련 주제:**

- 앱 카탈로그

## Android Enterprise 기기의 앱 캐시 지우기

**앱 캐시 지우기 요청**을 이용하여 관리자는 MDM용 Ivanti Neurons 사용을 통해 Android Enterprise 기기에 설치된 선택한 애플리케이션의 캐시 데이터를 원격으로 지울 수 있습니다. 이 작업은 앱을 제거하거나 다시 설치하지 않고도 느린 성능, 예기치 않은 오류 또는 구버전 임시 데이터와 같은 공통 앱 문제를 해결하는 데 도움이 됩니다. 이 요청은 앱의 캐시만 지우며 사용자 데이터, 앱 설정 및 구성은 유지합니다. 관리자는 이 기능을 사용하여 최종 사용자에게 미치는 영향을 최소화하면서 앱의 정상 동작을 신속하게 복구합니다.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. 앱을 선택하여 엽니다.
   앱 **상세 정보** 페이지가 나타납니다.
3. 앱 **상세 정보** 페이지에서 작업 메뉴(⋮)를 클릭합니다.
4. **앱 캐시 지우기 요청** 옵션을 선택합니다.
   **앱 캐시 지우기 요청** 창이 나타납니다.
5. 앱 캐시 지우기 요청을 배포하려면 **요청 보낼 사용자 선택** 섹션에서 다음 작업 중 하나를 수행합니다:
   - 앱이 설치된 모든 호환 기기에 요청을 보내려면 **모든 사용자**를 선택합니다.
   - 특정 사용자, 사용자 그룹, 기기 또는 기기 그룹에 요청을 보내려면 **사용자 정의**를 선택합니다.
6. (선택 사항) **다른 배포 필터 옵션** 아래에서 기존 배포 목록을 검색합니다.
7. (선택 사항) **+ 배포 필터 추가**를 선택하여 **배포 필터 만들기** 창에서 배포 필터를 만듭니다.

> 이 옵션을 사용하여 DO 또는 EPO 모드 기기와 같은 특정 기기 집합에 **앱 캐시 지우기 요청**을 보냅니다.

8. **보내기**를 클릭하세요.
9. **앱 캐시 지우기** 확인 대화 상자에서 **확인**을 클릭합니다.
   MDM용 Ivanti Neurons 에 **앱 캐시 지우기 요청**을 받은 기기 수를 나열하는 알림이 표시됩니다.

> **앱 캐시 지우기** 요청을 완료하면 모든 앱 상세 정보(버전, 이름, platformAppId, displayVersion 및 bundleVersion)가 **감사 내역** 페이지에 기록됩니다.

# 8.8. 앱에 사용자 지정 속성 할당

생성된 사용자 지정 속성을 하나 이상의 애플리케이션에 할당할 수 있습니다. 각 속성에는 애플리케이션 그룹 생성과 같이 작업에 사용할 수 있는 값이 있습니다. 속성 관리에 대해 자세히 알아보려면 속성을 참조하십시오.

## 개별 애플리케이션의 사용자 지정 속성 만들기 및 할당

단일 애플리케이션에 사용자 지정 속성을 할당할 수 있습니다.

**절차**

1. 관리 포털에 로그인합니다.
2. **앱** > **앱 카탈로그**로 이동합니다.
3. 애플리케이션을 선택하고 **속성**을 클릭합니다.
4. **+새로 추가**를 클릭하고 **속성 이름** 드롭다운 메뉴에서 값을 선택합니다.
5. **값** 필드에 속성 값을 지정합니다.
6. **저장**을 클릭합니다. 애플리케이션에 사용자 지정 속성이 추가됩니다.

## 여러 애플리케이션에 사용자 지정 속성 할당

사용자 지정 속성을 한 명 이상의 애플리케이션에 할당할 수 있습니다. 여러 애플리케이션을 선택할 경우 애플리케이션의 모든 버전에 사용자 지정 속성이 적용됩니다. 특정 애플리케이션을 선택하고 속성 탭으로 이동하면 특정 애플리케이션 버전의 사용자 지정 속성 세부 정보를 변경할 수 있습니다.

**절차**

1. 관리 포털에 로그인합니다.
2. **앱** > **앱 카탈로그**로 이동합니다.
3. 하나 또는 여러 애플리케이션의 체크박스를 선택합니다.
4. **작업**을 클릭합니다.
5. **사용자 지정 속성 할당**을 선택합니다. 앱에 사용자 지정 속성 할당 마법사가 표시됩니다.
6. 다음 옵션 중 *하나*를 선택합니다.
    - 기존 값을 발견한 경우에도 모든 속성을 강제 할당(덮어쓰기)합니다.
    - 값이 비어 있는 경우에만 덮어쓰기를 진행하며 기존 값이 있는 속성은 건너뜁니다.
7. 하나 또는 여러 속성의 체크박스를 선택합니다.
8. 값 필드에 값을 지정합니다(값은 비워둘 수 없음).
9. **할당**을 클릭합니다. 선택된 애플리케이션의 모든 버전에 사용자 지정 속성이 할당됩니다.
10. (선택 사항) 단일 애플리케이션 버전의 사용자 지정 속성을 변경하고자 할 경우, 버전 드롭다운에서 애플리케이션 버전을 선택하고 편집을 클릭합니다.

> **장치 세부 정보** 페이지에서 **사용자 지정 앱 속성**과 그 값을 사용하여 보고서를 작성하고 CSV 형식으로 내보낼 수 있습니다.

# 8.9. 관리되는 Android 구성

이 섹션에는 다음 주제가 포함됩니다.

- Android Enterprise 관리 구성 사용
- 인하우스 앱의 앱 제한 및 권한
- Android Enterprise로 Gmail 설정

MDM용 Ivanti Neurons(이)가 Android Enterprise를 지원하는 경우 Android Enterprise 구성은 앱별로 사용할 수 있습니다.

## Android Enterprise 관리 구성 사용

1. **앱**을 클릭합니다.
2. **앱 카탈로그**를 클릭합니다.
3. Android Enterprise 구성을 설정할 앱을 선택합니다.
4. **앱 구성**을 클릭합니다.
5. **관리되는 Android 구성**을 클릭합니다.
6. 구성 이름을 입력합니다.
7. 필요에 따라 설명을 입력합니다.
8. 관리 구성 필드를 이용해 관리되는 구성 동작을 설정합니다.
9. **Tunnel 구성 설정**을 사용하여 Android 기기에서 Tunnel 앱을 Ivanti Go 앱과 직접 통합합니다. 이 설정을 적용하려면 **Tunnel 구성 활성화** 옵션을 선택합니다. 이 개선으로 관리자는 Ivanti Go를 통해 Tunnel 기능을 활성화하고 기존 Tunnel 구성을 사용하여 보안 연결을 구성할 수 있습니다. 이 기능은 새로 등록된 Android 기기에서 사용할 수 있습니다. 원활한 전환을 위해 독립 실행형 Tunnel 앱은 계속 지원됩니다. 그러나 독립 실행형 Tunnel 앱이 설치된 기기에는 Ivanti Go의 통합 Tunnel 환경이 표시되지 않습니다. 독립 실행형 Tunnel 앱이 제거되면 Go 앱 내에서 통합 Tunnel 기능을 사용할 수 있습니다. 한 번에 하나의 Tunnel 구성만 기기에 적용할 수 있습니다.

| 설정 항목 | 설명 |
| --- | --- |
| 앱이 프로필에서 위젯을 공유하지 못하게 차단 | 앱이 자동으로 설치되지 않은 경우에만 앱이 프로필에서 위젯을 공유하지 못하도록 차단합니다. 사용자가 로그인할 필요 없이 정보에 액세스할 수 있도록 홈 화면에서 위젯을 표시하기 위해 Android Enterprise 프로필에 신뢰할 수 있는 앱을 배포하도록 비활성화 상태를 유지합니다. |
| 사용자가 앱을 제거하지 않도록 차단 | MDM용 Ivanti Neurons가 앱을 자동 설치한 후 사용자가 앱(공개, 개인용 또는 내부 앱)을 제거하지 못하도록 차단을 활성화합니다. |
| 최소 버전 코드 | 앱이 기본 업데이트 작업을 재정의하는 데 필요한 최소 버전 코드를 설정합니다. 현재 기기에 설치된 앱의 버전 코드가 지정된 최소 버전 코드보다 작은 경우 앱은 즉시 최신 버전으로 업데이트됩니다. |
| 설치 시 자동 시작 | 설치 후 자동으로 앱을 시작하려면 이 옵션을 선택합니다. 이 기능은 버전 업데이트용이 아니라 기기에 앱이 새로 설치되었을 경우에만 사용 가능합니다. 작업 프로필 및 회사 소유 기기의 작업 프로필의 경우 Go 앱이 활성 상태이며 포그라운드에 있어야 합니다.<br>Android 10+에 대한 제한으로 인해, 작업 프로필 및 회사 소유 기기의 작업 프로필의 경우 사용자가 여러 앱을 푸시할 경우에 하나의 앱만 자동 시작됩니다. |

10. 관리자는 기기에 전송해도 되거나 전송해서는 안 되는 앱 구성 필드를 제어할 수 있습니다. 일반적으로 구성을 다른 기기로 푸시할 때는 기본값이 설정됩니다. 관리형 구성 섹션의 **기기로 푸시** 설정에서 **모든 설정 푸시** 또는 **값이 정의된 설정만 푸시**를 선택합니다.

## 관리형 구성

각 Android Enterprise 앱 구성은 각 텍스트 필드에 대한 인증서 활성화 버튼을 표시하며 이를 클릭하면 텍스트 필드가 인증서 드롭다운 목록으로 교체됩니다. 인증서는 구성되면 사용자 인증 없이도 자동으로 적용됩니다.

기존 인증서 활성화 필드는 필드 옆의 동일한 버튼을 클릭하면 텍스트 활성화 필드로 변경할 수 있습니다. 인증서 활성화 필드로 변경된 텍스트 활성화 필드는 동일한 버튼을 클릭하면 다시 텍스트 활성화 필드로 변경할 수 있습니다. (기본 드롭다운 필드는 다시 텍스트 활성화 필드로 변경할 수 없음).

> 구성된 ID 인증서가 없는 경우 인증서 활성화 버튼을 사용하여 텍스트에서 드롭다운으로 전환하면 드롭다운 목록에 '없음' 옵션만 표시됩니다.

**권한 관리**를 클릭하여 API 23 이상과 Android 6.0 이상을 대상으로 하는 애플리케이션의 런타임 권한을 선택하고 구성합니다.

특정 애플리케이션에 적용 가능한 위험한 권한만 선택을 위해 나열됩니다. 위험한 권한(예: 연락처 읽기, 기기에서 계정 찾기, 호출 로그 쓰기 등)의 전체 목록은 **https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups**에서 확인할 수 있습니다.

11. 각 권한에 할당할 수 있는 권리:
    - 권한은 애플리케이션이 권한을 요청하는 경우에만 적용됩니다.
    - 사용자가 이전에 권한을 수락했거나 거부한 경우에는 권한이 적용되지 않습니다.
    - 자동 부여
    - 자동 거절 이 설정은 주의해서 사용해야 합니다.
    - 기본/글로벌

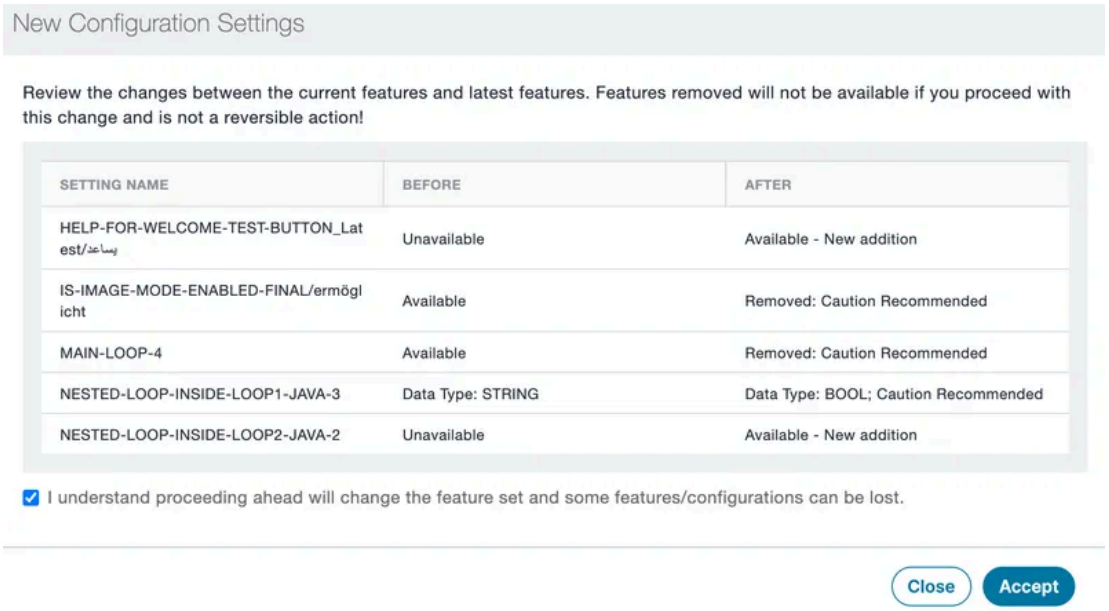
**앱을 소유한 모든 사람**, **없음**, **사용자 지정** 중 하나를 선택하여 배포 옵션을 구성합니다.

12. **저장**을 클릭합니다.

## 새로운 구성 설정

앱 버전이 업데이트되고 기존 구성에 변경 사항이 있는 경우 구성 세부 정보 페이지를 편집하게 되면 **최신 기능으로 업데이트** 버튼이 나타납니다.

1. **최신 기능으로 업데이트**를 클릭합니다.
   최신 기능으로 이동하면 사용자가 이전 버전의 애플리케이션에 액세스할 수 없다는 경고 메시지가 화면에 나타납니다. 경고 메시지는 최신 버전의 애플리케이션을 원활하게 통합하기 위한 단계를 권장합니다.
2. **다음**을 클릭하세요.
3. 화면에 **새로운 앱 구성** 페이지가 표시됩니다.




**새로운 구성 설정** 창에는 구성에 존재했던 다양한 설정과 업데이트 후 각 설정의 상태가 나열됩니다. 새 구성 설정 창에는 데이터베이스의 모든 제한 사항이 나열되며 Google 스키마에는 다음 상태가 나열됩니다.

- 추가됨
- 제거됨
- 수정됨

확인란을 선택하고 **수락**을 클릭하여 업데이트를 진행합니다.
최신 기능으로 구성이 성공적으로 업데이트되었다는 확인 메시지가 화면에 나타납니다. 이제 변경 사항을 적용하기 위해 구성을 배포하고 저장할 수 있습니다.

## 인하우스 앱의 앱 제한 및 권한

관리자는 인하우스 앱에 대해 일부 앱 제한을 설정하고 권한을 제한하거나 승인할 수 있습니다. 이 기능은 공개 앱에 한하여 사용할 수 있었습니다. 하지만 이제 인하우스 앱에서도 이 기능을 사용할 수 있습니다.

> 앱에서 **앱 제한** 및 **권한** 기능을 사용하려면 관리자가 인하우스 앱을 다시 업로드해야 합니다. 새 버전을 업로드하기 전에 기존 앱을 삭제하는 것이 권장됩니다.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. 목록에서 **인하우스** 앱을 선택합니다.
3. **앱 구성**을 클릭합니다.
4. **관리형 Android 구성**을 클릭합니다.
5. **추가**를 클릭합니다.
6. 화면에 **앱 제한** 섹션이 표시됩니다.
   사용 가능한 제한에 대해 필요한 값을 입력합니다.
7. **권한 관리**를 선택합니다.

8. 화면에 **권한 선택** 창이 표시됩니다.
   목록에서 필요한 권한을 선택하고 **선택**을 클릭합니다.
9. **런타임 권한** 섹션에서 선택한 권한의 값을 입력합니다.
10. **이 앱 구성 배포** 섹션에서 다음 **앱 배포** 옵션 중 하나를 선택합니다.
    - **앱을 소유한 모든 사람**
    - **없음**
    - **사용자 지정**
11. **저장**을 클릭하세요.
    인하우스 앱에 선택한 제한과 권한이 적용됩니다.

## Android Enterprise로 Gmail 설정

Android Enterprise에 MDM용 Ivanti Neurons을 설정했다면 Android Enterprise 기기에 Gmail을 배포할 수 있습니다. Android Enterprise로 Gmail을 설정하려면

1. **앱 > 앱 카탈로그**를 선택하세요.
2. Android Enterprise 구성을 설정할 Gmail 앱을 선택합니다. 구성 설정 섹션이 표시됩니다.
3. 구성 이름을 입력합니다.
4. 필요에 따라 설명을 입력합니다.
5. **관리 구성** 필드를 이용해 관리되는 구성 동작을 설정합니다.

> **모두 확장** 및 **모두 축소** 옵션은 중첩 또는 계층 구조 제한에만 사용할 수 있습니다.

| 설정 | 설명 |
| --- | --- |
| **기기로 푸시** | 모든 설정 푸시 - 이 옵션을 선택하면 값이 없는 설정을 포함하여 모든 토글을 활성화합니다.<br>값이 정의된 설정만 푸시 - 이 옵션을 선택하면 정의된 값이 있는 모든 토글을 활성화하고 값이 없는 설정의 토글은 비활성화합니다.<br>많은 경우, 기본값 설정은 이미 사용 가능한 상태입니다. 하지만 관리자는 필수 앱 구성 설정을 선택하거나 기기에 반드시 전송해야 하는 변수를 편집할 수 있습니다. |
| **이메일 주소** | 대체 변수를 입력하여 이메일 주소를 정의합니다. 일반적으로 $emailaddress$을(를) 입력합니다. UEM은 이 필드를 사용하여 Active Directory에서 사용자 자격 증명을 끌어올 수 있습니다. |
| **호스트 이름 또는 호스트** | hostname.company.com:443/path 등의 Active Sync 서버의 호스트 이름을 입력합니다. |
| **사용자 이름** | 사용자의 Active Directory를 위해 정확한 사용자 이름(예: 홍길동) 또는 템플릿으로 만든 값($username$)을 사용합니다. |
| **인증 유형** | 허가된 인증 유형을 포함하는 문자열 목록을 선택합니다. |
| **SSL 필요** | 이 옵션을 선택하면 활성화되고 호스트 이름과 함께 사용되는 포트 번호의 SSL이 필요합니다. |
| **모든 인증서 신뢰** | 앱이 신뢰하지 않는 인증서를 자동으로 수락하도록 할 경우에만 이 옵션을 선택합니다. 이 옵션은 테스트 환경에서의 디버깅 또는 개발용으로만 사용합니다. |
| **로그인 인증서 별명** | ActiveSync 서버를 인증하는 로그인 인증서의 별명을 입력합니다. |
| **관리되는 계정 허용** | 사용자가 이 관리형 구성에 지정된 계정 외의 Exchange 계정을 추가하거나 제거하는 것을 허용하려면 이 옵션을 선택합니다. |
| **기본 이메일 서명** | 모든 아웃바운드 이메일 메시지 텍스트 하단에 추가하기 위해 기본 이메일 서명을 구성하는 문자열을 입력합니다. |
| **기본 동기화 창** | EAS(Exchange Active Sync)와 동기화하기 위한 시간 창을 나타내는 값을 0에서 5까지 입력합니다. |

**다음**을 클릭하세요.

7. **앱을 소유한 모든 사람**, **없음**, **사용자 지정** 중 하나를 선택하여 배포 옵션을 구성합니다.
8. **저장**을 클릭하세요.

# 8.10. Google Play 앱 관리

Google Play 앱에서 어떤 바이너리가 특정 그룹 또는 개인으로 배포되어야 하는지 정의할 수 있습니다.이 배포는 Android 엔터프라이즈 배포에 적용할 수 있습니다. 또한 앱 개발자는 알파 또는 베타 채널 앱을 배포할 수 있도록 조직을 허용 목록에 등록해야 합니다.

1. **앱**을 클릭합니다.
2. **App Catalog**에서 Google Play 릴리스 구성을 구성할 앱을 선택합니다.
3. **앱 구성** 탭을 클릭합니다.
4. **Google Play 릴리스**를 클릭합니다.

> Google 릴리스 구성은 Android Enterprise 앱에만 적용됩니다. 기본적으로 새로 추가된 앱에 대해 Google 릴리스 구성이 선택되지 않은 경우 생산 옵션이 적용되지 않습니다.

**추가**를 클릭합니다.

6. 구성 이름을 입력합니다.
7. 필요에 따라 설명을 입력합니다.
8. 드롭다운 목록에서 옵션을 선택하여 이 앱을 받는 사용자와 기기에서 이용 가능한 바이너리를 선택합니다. 옵션은 다음과 같습니다.
    - 프로덕션
    - 알파
    - 베타

    > 프로덕션 옵션은 기기에 이미 푸시된 앱에만 기본적으로 적용됩니다.

9. **앱을 소유한 모든 사람**, **없음**, **사용자 지정** 중 하나를 선택하여 배포 옵션을 구성합니다.
10. **사용자 지정**은 사용자 그룹 내의 앱을 기기 필터와 함께 배포합니다.
    **저장**을 클릭하세요.

## 다중 릴리스 구성 우선순위 지정

여러 개의 Google 릴리스 구성이 추가되었을 때 어떤 Google 릴리스 구성이 적용될지에 관한 우선순위를 지정할 수 있습니다.

1. **앱 구성**에서 **우선순위 지정 구성**을 클릭합니다.

> 이 버튼은 목록에 여러 구성이 있는 경우에만 표시됩니다.

나열된 구성에서 우선순위로 적용될 구성을 목록 상단으로 끌어다 놓습니다.

3. **업데이트**를 클릭합니다.

> 최우선순위의 구성이 삭제되면 이전에 열거된 아래 구성이 최우선순위가 됩니다.

# 8.11. App Catalog에서 앱 삭제

앱 카탈로그에서 공공 앱이나 인하우스 앱을 삭제할 수 있습니다. 필수 설치 앱은 삭제할 수 없습니다. 해당 앱을 삭제하기 전에 필수 조건 관계를 제거해야 앱을 편집할 수 있습니다. 장치에 설치되어 있는 앱을 삭제할 경우, 해당 앱은 장치가 다음 번 체크인할 때 삭제됩니다. 자동 앱 설치/제거는 기기 관리자 모드의 Samsung 및 Zebra 기기 또는 기기 소유자 모드의 모든 기기에서 지원됩니다.

인하우스 앱의 경우 화면에 구성 창이 표시됩니다. 삭제 작업을 계속하려면 승인을 선택하고 **앱 삭제**를 클릭합니다. 여러 앱을 삭제하려 하는데 일부 앱을 삭제할 수 없을 경우, 화면에 표시된 창에 삭제할 수 없는 앱의 정보와 그 이유가 제시됩니다.

앱 카탈로그에서 하나 이상의 앱을 삭제하려 할 경우 다음과 같은 조건이 적용됩니다.

- 인하우스 앱의 한 버전을 삭제할 수 없을 경우 모든 버전을 삭제할 수 없습니다.
- 인하우스 앱의 한 버전이 필수 앱일 경우 해당 앱은 삭제할 수 없으며, 어떤 버전도 삭제할 수 없습니다.
- 인하우스 앱의 전체 또는 일부를 선택하여 앱 카탈로그에서 삭제할 경우 선택된 인하우스 앱의 모든 버전이 삭제됩니다.
- Space에서 위임된 인하우스 앱은 삭제할 수 없습니다.

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 원하는 앱의 링크를 클릭하세요.
3. **작업 > 카탈로그에서 삭제**를 선택하세요.
4. 앱을 삭제할 경우 어떤 결과가 발생하는지 알리는 경고 메시지가 표시됩니다.
5. 앱 삭제 Apps 및 Books 라이센스(iOS)와 앱 평가(모든 OS)까지 삭제된다고 알리는 메시지입니다.
   삭제 작업을 계속하려면 "본인은 앱 삭제의 결과를 이해합니다" 체크박스를 선택합니다.
6. **앱 삭제**를 클릭하세요.

# 8.12. 인하우스 앱 업그레이드

인하우스 앱을 업데이트하려면 다음 절차를 사용합니다.

1. **앱 > 앱 카탈로그**를 선택하세요.
2. 업그레이드할 앱을 선택하세요.
3. **동작 > 새 버전 추가**를 선택하세요.
4. 원하는 앱을 **앱 업로드** 영역으로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택하세요.
5. 기존 앱 버전을 어떻게 처리할지에 따라 다음 옵션 중 하나를 선택하세요:
   - **설명, 화면 캡처, 배포, 앱 필수 조건, 앱 구성을 동일하게 유지:** App Catalog 내의 기존 버전이 새 버전으로 교체됩니다.
   - **설명, 화면 캡처, 배포, 앱 필수 조건 또는 앱 구성 변경**: App Catalog 내의 두 버전이 모두 포함됩니다.
6. **새로운 기능**에 새 버전이 어떻게 다른지 사용자에게 알려줄 설명을 입력하세요.
7. 입력한 설명은 사용자가 설치할 앱을 선택하면 기기에 표시됩니다.
   설명이나 화면 캡처, 배포 설정을 변경하기로 선택한 경우, 해당 내용을 수정하세요.
8. **완료**를 클릭하세요.

카탈로그에 기존 앱 버전을 유지하기로 선택할 경우, **앱 > 앱 카탈로그**에 한 항목만 표시됩니다. 왼쪽 끝 창에 해당 항목에 대해 확인된 앱 수가 표시됩니다. 차후 최신 버전을 삭제하게 되면 설치된 기기의 기존 버전으로 자동 교체됩니다.

## 앱 버전 목록 표시

관리자는 버전은 같으면서 아키텍처는 다른 앱을 업로드할 수 있습니다.

**Procedure절차**

1. **앱 > App Catalog**에서 원하는 앱 링크를 클릭하십시오.
2. **버전** 탭을 클릭합니다.
   카탈로그 내에 여러 앱 버전이 있을 경우 드롭다운 메뉴에 해당 버전이 모두 표시됩니다. 버전은 같지만 아키텍처는 다른 여러 앱을 업로드하는 경우 드롭다운에 지원되는 아키텍처 세부 사항이 표시됩니다. 또한, 앱에 지원되는 아키텍처는 **앱 정보** 아래에 표시됩니다.

# 8.13. Android 앱의 패키지 이름 찾기

Google Play Store에서 이용할 수 있는 **공개 앱**:

1. 웹 브라우저를 사용하여 Google Play Store에서 앱을 찾습니다.
2. 앱을 선택합니다.
3. 브라우저에 표시된 URL을 검사합니다.

패키지 이름은 아래와 같이 URL에서 id= 다음에 있습니다.

https://play.google.com/store/apps/details?id=<package name>

**Play Store에서 이용할 수 없는 인하우스 앱 및 기타 앱의 경우** 패키지 이름 뷰어 또는 Google Play Store에서 유사한 앱을 다운로드하십시오.

# 8.14. 범주

이 섹션에는 다음 주제가 포함됩니다.

- 범주 추가
- 범주 삭제

범주는 앱의 유형을 설명하며, 사용자가 앱 카탈로그를 탐색할 때 앱을 구성하는 데 도움이 됩니다. 모든 앱에는 1개 이상의 범주가 할당되어야 합니다. MDM용 Ivanti Neurons 사용을 시작하면 공통 앱 카테고리 목록을 사용할 수 있습니다. 해당 페이지에서 앱 범주를 관리할 수 있습니다.

## 범주 추가

여기에서 새로운 범주를 추가할 수도 있고, **앱 카탈로그**에 앱을 추가할 때 범주를 추가할 수도 있습니다.

1. **추가**를 클릭합니다(좌측 하단).
2. 해당 범주 이름을 입력하세요.
3. 범주 이름은 대소문자를 구분하지 않습니다(예: MINE과 Mine은 동일).
   **저장**을 클릭하세요.

## 범주 삭제

- 삭제할 범주 옆의 X를 클릭하세요.

**앱 범주** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 앱 및 컨텐츠 관리

# 8.15. 배포 필터

이 섹션에는 다음 주제가 포함됩니다.

- 배포 필터 구성
- 위임 관리자에 대한 배포 필터 구성

배포 필터를 사용해 설치할 수 있는 앱을 제한합니다. 배포 필터를 통해 기기에 적용할 수 있는 앱만을 앱 카탈로그에 표시할 수 있습니다.

**라이센스**: Silver

이 필터는 기본적으로 다음과 같이 이용할 수 있습니다.

- **Android 엔터프라이즈 지원 앱** - Android 엔터프라이즈 지원 기기에 한해서만 앱 배포를 제한합니다.
- **iPad 전용 앱** - iPad 기기로 앱 배포를 제한합니다.
- **iPhone 전용 앱** - iPhone 기기로 앱 배포를 제한합니다.

## 배포 필터 구성

1. **앱 > 배포 필터**로 이동합니다.
   기본 앱 필터 및 생성된 앱 필터가 여기에 나열됩니다.
2. **+추가**를 클릭하여 **배포 필터 생성** 대화 상자에 액세스합니다.
3. 해당 필드에 이름과 설명을 입력합니다.
4. 규칙 정의를 선택합니다. 이러한 규칙은 "포함", "보다 작음", "보다 큼", "범위에 있음", "다음과 같음", "다음과 같지 않음" 등의 해당 연산자를 사용하여 구성할 수 있습니다. 규칙은 ANY(OR) 또는 ALL(AND) 옵션을 사용하여 중첩될 수 있습니다. 앱 배포 필터는 다음과 같습니다.
   - 액세스 차단됨
   - APNS 가능
   - 작업 프로필이 있는 Android 관리 기기
   - Android Work 활성화됨
   - Android 보안 패치 수준(Android 기기)
   - Android Work 관리 기기(기기 소유자) 활성화
   - 회사 소유 기기의 Android 작업 프로필이 활성화됨
   - 클라이언트 마지막 체크인
   - 등록된 클라이언트
   - 컴플라이언스
   - 정책 준수 활동 차단됨
   - 현재 국가 이름
   - 현재 MCC
   - 현재 MNC
   - 사용자 지정 기기 속성
   - 사용자 지정 LDAP 속성
   - 사용자 지정 사용자 속성

- 사용자 지정 IDP 속성
- 기기 유형
- 주요 국가 이름
- 홈 MCC
- 홈 MNC
- IMEI
- IMEI2(듀얼 SIM 포트가 있는 Android 장치에만 해당되고 Android 8.0 이상 장치에 적용 가능)
- Kiosk 모드
- 제조업체
- OS 버전
- 소유권
- 전화 번호
- 로밍
- Secure Apps 상태
- 감독됨
- Sentry 차단됨
- 사용자 등록 등록됨
- 자동화된 기기 등록 등록됨
- 자동화된 기기 등록 활성화됨

5. **배포 필터 생성**을 클릭합니다.
6. 필요한 경우, 업데이트할 사용자 지정 필터를 선택합니다.
    1. **편집**을 클릭하여 **배포 필터 업데이트** 페이지를 표시합니다.
    2. 해당 필드에 이름과 설명을 입력합니다.
    3. 풀다운 메뉴를 사용하여 필터 규칙을 정의합니다.
    4. **배포 필터 업데이트**를 클릭합니다.
7. 앱을 선택합니다.
8. 앱 상세 정보 페이지에서 **배포** 탭을 선택합니다.
9. **편집**을 클릭합니다.
10. 앱 배포 옵션을 선택합니다.
    - **모두**
    - **아무에게도 배포 안 함**
    - **사용자 지정**

    > 배포 필터 섹션은 **모두** 또는 **사용자 지정** 배포 옵션을 선택한 경우에만 표시됩니다.

11. 배포 필터 옵션을 선택합니다.
    1. **기존 배포 필터 검색**에서 필터 이름을 입력합니다. 이미 생성된 필터를 찾습니다.
    2. **+배포 필터 추가**를 클릭하여 새 필터를 추가합니다.

카탈로그에 배포 필터를 추가하기 전에 이를 생성 또는 앱에 할당할 수 있습니다. 배포 필터의 변경 사항은 해당 필터를 사용 중인 앱의 배포에 영향을 미칩니다(모든 공간).

필터가 설정되었고 **배포 시 M1 기기에 앱 설치 허용**이 활성화된 경우, 결과는 macOS M1 기기를 채웁니다. iOS VPP 앱은 **배포 시 M1 기기에 앱 설치 허용**이 활성화되고 배포 필터가 **모두** 또는 **사용자 정의**인 경우 모든 Mac 기기에서 사용할 수 있습니다. iOS 앱에는 macOS 관련 속성의 배포 필터가 지원되지 않습니다.

## 위임 관리자에 대한 배포 필터 구성

위임 관리자는 위임된 공간에서 배포 프로세스 중에 개별 앱에 추가된 생성된 필터를 관리하고 편집할 수 있습니다. 하지만 위임 관리자는 다른 공간의 기본 공간에서 생성된 배포 필터를 사용할 수 없고 위임된 앱에만 사용할 수 있습니다.

위임 관리자는 자신이 액세스할 수 있는 특정 공간에서 배포 필터를 생성, 관리 및 편집할 수 있습니다. 배포 필터는 해당 필터가 생성된 공간에서만 사용할 수 있습니다. 앱 배포 필터는 위임할 수 없습니다.

앱 및 시스템 관리 역할의 위임 관리자가 위임된 공간에서 배포 필터를 사용하여 앱을 추가한 경우에는 자신의 공간에 있는 기기 그리고 다른 공간에 있는 기기의 기기 상세 정보를 볼 수 있습니다.

시스템 관리 또는 시스템 읽기 전용 역할을 가진 사용자는 다른 공간에 있는 배포 필터를 생성, 업데이트 또는 삭제할 수 없게 됩니다.

앱 및 컨텐츠 관리자 역할의 위임 관리자는 배포 필터에 액세스하지 못할 수도 있습니다. 이로 인해

- 배포 필터를 사용하여 앱을 생성할 수 없습니다. 이러한 상황은 위임 관리자로 로그인한 상태에서 앱을 추가할 때 발생합니다.
- 시스템 읽기 전용 역할 이상의 위임 관리자만 앱을 배포 필터와 함께 추가할 수 있습니다. 시스템 관리자 역할이 없는 위임 관리자는 배포 필터 없이 앱을 추가할 수 있습니다.

위임 관리자는 다음 옵션을 선택하여 앱 카탈로그의 위임 상태를 필터링할 수 있습니다.

- 위임됨
- 위임되지 않음

# 8.16. 앱 제외 또는 배포

iOS, macOS, Windows 장치의 사내 및 공용 앱에 대한 앱 배포 구성을 변경하지 않고 장치에서 관리되는 앱을 제외하거나 배포합니다. 모든 관리형 앱의 경우 이러한 옵션은 모든 장치에 대해 **사용 가능한 앱** 섹션의 **작업** 열에 있습니다.

### 권한

장치에서 애플리케이션을 제외하거나 장치에서 배포하려면 다음 권한이 있어야 합니다.

- 공간(파티션)에서 장치 액세스
- 장치에서 사용 가능한 앱에 액세스합니다.

## 제외

선택한 앱의 제외 옵션은 장치에서 관련 데이터를 설치 제거하고 삭제합니다. 필수 앱을 제외하려면 워크플로를 따르십시오. 팝업 확인은 필수 앱을 제외하고 있음을 나타내므로 장치에서 기본 앱이 제외됩니다.

여러 버전의 사내 앱을 제외하면 장치에서 배포되지 않은 모든 앱 버전이 제외됩니다. 장치에서 앱을 제외하면 Apps@Work 및 Ivanti Go에서 삭제됩니다. 앱 카탈로그에서 앱을 제외 및 삭제한 후 다시 추가하면 해당 앱은 더 이상 해당 장치에서 제외된 상태로 유지되지 않습니다. 장치에서 관리형 앱을 제외하면 관리자가 앱을 제외한 후 배포할 수 있도록 **장치** > **장치** > **사용 가능한 앱** 목록에 해당 앱이 표시되어야 합니다.

## 배포

관리자가 앱에서 **Send install(설치 보내기)** 명령을 실행하면 관리자가 장치의 **사용 가능한 앱**에서 앱을 배포하기로 결정할 때까지 앱이 설치되지 않습니다. 앱을 다운로드하지 않는 장치에 대해 새 제외 메시지가 나타납니다. 관리자가 사용 가능한 애플리케이션을 배포하면 다음 동기화에서 배포된 애플리케이션을 장치에 설치합니다.

# 8.17. 검토

이 섹션에는 다음 주제가 포함됩니다.

- 등급 및 평가 보기
- 등급 및 평가 비활성화
- 평가 삭제
- CSV 파일로 리뷰 내보내기

리뷰는 사용자가 앱과 앱 카탈로그에 대해 제공하는 코멘트와 평점(별)입니다. 관리자와 앱을 설치하려는 사용자 모두에게 중요한 정보를 제공하는 페이지입니다. **평가** 페이지에 게시된 등급 및 평가를 확인하거나 삭제할 수 있습니다. 시일이 지났거나 적절하지 않은 평가 및 등급은 삭제가 필요할 수 있습니다.

- 장치 사용자에 한해 앱 등급 및 평가 의견을 생성할 수 있습니다.
- 장치 사용자는 직접 작성한 등급이나 평가 의견을 수정은 할 수 있지만 삭제는 할 수 없습니다.
- 관리자만 앱 평가 내용을 삭제할 수 있습니다.
- 앱 등급은 삭제가 불가능합니다. 등급 및 평가 기능을 해제해도 앱에 매겨진 등급(별 개수)은 **앱 > 앱 카탈로그** 페이지에 계속 남습니다.

## 등급 및 평가 보기

- **앱 > 평가** 페이지를 실행하면 배포했던 앱에 대해 사용자가 남긴 전체 평가 의견 및 등급(별 개수)을 확인할 수 있습니다.
- **앱 > 앱 카탈로그**로 이동하여 총 리뷰 수와 평균 평점에 대한 **평균 평점** 열을 확인합니다.
- **앱 > 앱 카탈로그**에서 **앱 이름**을 클릭하면 **평가** 탭에서 원하는 앱에 대한 등급 및 평가를 확인할 수 있습니다.

## 등급 및 평가 비활성화

1. **앱 > 카탈로그 설정**을 선택하세요.
2. **최종 사용자 앱 카탈로그의 등급 및 평가 활성화**를 선택 해제하세요.
3. **저장**을 클릭하세요.

## 평가 삭제

1. **앱 > 평가**를 선택하세요.
2. 삭제할 평가 항목을 선택하세요.
3. 페이지 우측 상단의 **작업** 버튼을 클릭하세요.
4. **삭제**를 선택하세요.
5. **평가 삭제** 확인 창이 뜨면 **예**를 클릭하세요.

**검토** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.

- 앱 및 컨텐츠 관리

## CSV 파일로 리뷰 내보내기

**리뷰** 페이지의 **CSV로 내보내기** 옵션을 사용하여 앱 리뷰를 내보낼 수 있습니다.

**절차**

1. **앱 > 평가**를 선택하세요.
2. **CSV로 내보내기** 옵션을 클릭하여 리뷰 목록과 관련 세부 정보를 CSV 파일로 내보냅니다.
3. **계속** 및 **취소** 버튼이 포함된 팝업 메시지가 나타나 내보내기 프로세스가 시작되었음을 알리고, 곧 보고서를 사용할 수 있습니다.
4. **계속**을 클릭하고 요청이 완료되기를 기다린 후 다른 요청을 제출합니다.
5. **앱 리뷰 - CSV 보고서 완료** 상태임을 알리는 메시지가 나타나며 여기에는 **다운로드** 및 **삭제** 버튼이 있습니다.
6. 보고서를 다운로드하려면 **다운로드**를 클릭하세요.
7. (선택 사항) 보고서를 삭제하려면 **삭제**를 클릭합니다.

# 8.18. Apple Apps 및 Books

이 섹션에는 다음 주제가 포함됩니다.


- 한 공간에서 여러 Apple Apps 및 Books 계정에 걸친 앱 라이센스 배포
- 기기 기반 및 사용자 기반 라이센스 배포
- 기기 기반 라이센스 옵션 사용
- 사용자 기반 라이센스 옵션 사용
- Apps 및 Books 앱을 카탈로그에 추가
- Apps 및 Books 계정 추가
- Apps 및 Books 보안 토큰 업데이트
- Apps 및 Books 계정의 우선순위 업데이트
- Apps 및 Books 보안 토큰 삭제
- 카탈로그의 Apps 및 Books 앱 라이센스 배포
- 사용자별 앱 라이센스 보기
- Apps 및 Books 라이센스 사용 알림
- Apps 및 Books 라이센스 사용 보기
- 앱에 대한 Apps 및 Books 라이센스 철회
- macOS 및 iOS 기기의 Apps 및 Books 동작
- 기기가 공간을 이동할 때의 Apps 및 Books 라이센스 권한


**라이센스:** Silver

**Apple Apps 및 Books** 화면은 **앱 카탈로그 설정**에서 Apple Apps 및 Books가 설정된 경우에만 사용 가능합니다. 이 화면에서는 Apple Apps 및 Books를 통해 Apple 기기용으로 구매한 앱 라이센스 및 사용된 라이센스 개수를 확인할 수 있습니다. 다음과 같은 기능이 제공됩니다.

- 카탈로그에 포함될 Apple Apps 및 Books 앱 선택
- Apps 및 Books 앱에 대한 라이센스 배포

앱 및 책으로 앱을 배포하는 방법에 대한 자세한 내용은 Ivanti 커뮤니티 문서인 **MDM용 Ivanti Neurons: VPP를 사용하여 앱을 배포하는 방법**을 참조하십시오.

> 일부 국가 또는 지역에서는 Apple Books가 제공되지 않을 수도 있습니다. Apple의 Apps 및 Books를 통해 앱용 라이센스를 배포하려면 Apple에서 제공하는 sToken을 입력해야 합니다.

## 한 공간에서 여러 Apple Apps 및 Books 계정에 걸친 앱 라이센스 배포

- 동일한 앱이 여러 Apps 및 Books 계정에 존재하는 경우 라이센스는 계정의 우선순위 순으로 계정에서 배포됩니다.
- 동일한 앱이 여러 Apps 및 Books 계정에 존재하고 우선순위가 더 높은 Apps 및 Books 계정의 앱 라이센스가 모두 사용된 경우, 사용자 또는 기기가 다음 우선순위 계정의 라이센스 배포 목록에 있는 경우에만 앱에 다음 우선순위 계정의 라이센스가 배포됩니다.
- 라이센스는 Apps 및 Books 계정의 우선순위 변경 시 철회 및 재할당되지 않습니다. 앱에 첫 번째 계정의 라이센스가 배포됩니다. 첫 번째 계정에서 라이센스가 모두 사용된 경우 앱에 다음 우선순위 계정 등의 라이센스가 배포됩니다.

- 사용자는 App Catalog 페이지에서 앱의 모든 라이센스를 철회할 수 있는 옵션이 있습니다. 이 작업은 사용 가능한 모든 Apps 및 Books 계정에서 해당 앱의 라이센스를 철회합니다.
- 예약된 라이센스는 Apps 및 Books 계정의 우선순위보다 우선합니다.

## 기기 기반 및 사용자 기반 라이센스 배포

앱의 라이센스가 기기 기반 또는 사용자 기반인지 여부는 할당하는 방식에 따라 다릅니다. 앱 라이센스를 기기로 할당하는 경우 기기 기반 라이센스가 됩니다. 앱 라이센스를 사용자로 할당하는 경우 사용자 기반 라이센스가 됩니다.

라이선스는 Apps and Books 앱을 기기에 설치할 때 또는 해당 앱에 대한 토큰이 발급될 때 배포됩니다. 해당 앱에 라이센스를 사용할 수 없는 경우 사용자가 앱 자체를 설치하여 지불할 수 있는 옵션이 있습니다. 사용자가 필수 Apps 및 Books 앱에 대한 사용자 기반 라이센스를 이미 할당받은 경우, Apps 및 Books 라이센스가 아닌 기존 사용자 기반 라이센스를 이용해 앱을 설치합니다.

> 공유 iPad의 경우 Apps 및 Books는 기기 기반 라이센스가 선택되었는지 여부와 관계없이 기기 기반 라이센스를 기준으로 설치됩니다.

## 기기 기반 라이센스 옵션 사용

기기 기반 라이센스가 있으면 사용자는 Apps 및 Books에 등록할 필요가 없습니다. 필수 앱이 자동적으로 설치됩니다. 회사 감독 기기는 IT 소유 Apple ID를 다룰 필요가 없습니다.

기기 체크인 중에 기기는 일련 번호로 식별되며 사용 가능한 라이센스가 있는 경우 필요한 앱을 설치합니다. 라이센스를 사용할 수 없는 경우 앱이 설치되지 않습니다. 앱에 대한 라이센스를 보유한 경우 앱 설치 시에는 기기 기반 라이센스가 할당되지 않습니다.

> 기기 기반 Apps 및 Books 라이센스로 배포된 앱의 애플리케이션 업데이트는 관리자가 제어합니다.

앱 업데이트 방식을 제어하려면 **앱 > App Catalog**에서 **기기에서 앱 구성/설치** 탭으로 이동합니다. 다음 기기 체크인 시 즉시 업데이트를 선택하거나 새 버전이 나왔을 때 자동으로 앱을 업데이트하도록 선택할 수 있습니다.

**중요:** 기기 기반 라이센스를 B2B(기업간) 앱 또는 생산성 앱에 할당하기 전에 해당 앱이 앱 개발자와의 기기 기반 라이센스에 적합한지 확인하십시오.

## 사용자 기반 라이센스 옵션 사용

기기가 손실 또는 도난당하거나 사용자가 새로운 기기로 업그레이드하여 한 기기에서 다른 기기로 이동해야 하는 경우 사용자 기반 라이센스는 이 사용자에 대하여 여전히 유효합니다. 사용자는 먼저 사용자 기반 라이센스로 Apple Apps 및 Books에 등록해야 합니다. 등록은 최종 사용자가 App Catalog에서 완료해야 하는 수동 작업입니다. 사용자가 Apps 및 Books에 등록할 때까지 필수 Apps 및 Books 앱을 기기에 설치할 수 없습니다.

앱이 필수 Apps 및 Books 앱이며 라이센스 배포가 사용자 기반인 경우:

- 사용자가 Apps 및 Books 프로그램에 등록하지 않으면 필수 앱 설치가 이루어지지 않습니다.
- 사용자가 Apps 및 Books 프로그램에 등록되고 라이센스를 사용할 수 있는 경우 필수 앱이 설치될 수 있습니다.
- 사용자가 Apps 및 Books에 등록되었으나 사용 가능한 라이센스가 없는 경우 앱은 설치되지 않습니다.

## Apps 및 Books 앱을 카탈로그에 추가

**절차**

1. **앱 > 앱 카탈로그**를 선택하세요.

2. 앱을 선택하고 **카탈로그에 추가**를 클릭합니다. **다음**을 클릭하세요.
3. 선택 사항. 앱의 설명을 추가합니다. **다음**을 클릭하세요.
4. 배포 방법을 선택합니다. **다음**을 클릭하세요.
5. **앱 구성** 탭을 클릭합니다.
6. 필요에 따라 **기기에 설치**를 선택합니다. 이 구성 옵션으로 감독한 iOS 기기에서 사용자에게 메시지를 표시하지 않고 앱을 설치합니다.
7. 필요한 경우 다른 구성 옵션을 선택합니다.

Apps 및 Books 토큰 정보 페이지에 다음과 같은 토큰 상세 정보가 표시됩니다.

- 생성 날짜
- 위치(토큰에 이 정보가 포함되어 있을 경우)
- 만료 날짜

## Apps 및 Books 계정 추가

MDM용 Ivanti Neurons 는 단일 공간에 여러 Apps 및 Books 보안 토큰을 추가하여 여러 Apps 및 Books 계정을 추가할 수 있습니다.

한 공간에 Apps 및 Books 보안 토큰을 추가하려면 다음 단계를 수행합니다.

1. **앱 > Apple Apps 및 Books**로 이동합니다.
2. **+Apps 및 Books sToken 추가**를 클릭합니다.
3. 이름을 입력하고 토큰 파일을 선택합니다.
4. (선택 사항) **모든 사용자에게 자동으로 Apps 및 Books 앱 배포** 옵션을 선택 취소합니다. 이 옵션은 기본 선택되며 이 경우 전체 사용자 그룹이 FCFS 라이센스를 배포하는 데 사용됩니다.
5. (선택 사항) 이 토큰과 연결된 모든 앱 라이센스를 제거하려면 **이전 Apps 및 Books 라이센스에서 모든 데이터 지우기** 옵션을 선택합니다.
6. **저장**을 클릭하세요.

계정이 추가된 후 추가된 모든 Apps 및 Books 계정 목록이 표에 표시됩니다.

## Apps 및 Books 보안 토큰 업데이트

**절차**

1. **앱 > Apple Apps 및 Books**로 이동합니다.
2. Apps 및 Books 계정 이름을 클릭합니다.
3. 토큰 탭에서 **sToken 업데이트**(.stoken file)를 클릭합니다.
4. 토큰 이름을 입력하고 토큰 파일을 선택합니다.
5. (선택 사항) **모든 사용자에게 자동으로 Apps 및 Books 앱 배포** 옵션을 선택 취소합니다. 이 옵션은 기본 선택되며 이 경우 전체 사용자 그룹이 FCFS 라이센스를 배포하는 데 사용됩니다.
6. (선택 사항) 이 토큰과 연결된 모든 앱 라이센스를 제거하려면 **이전 Apps 및 Books 라이센스에서 모든 데이터 지우기** 옵션을 선택합니다.
7. **업데이트**를 클릭합니다.

Apple의 Apps 및 Books 서비스에서 모든 앱과 라이센스 정보의 전체 동기화를 수행하려면 토큰 탭에서 **Apps 및 Books 라이센스 이용 정보 재동기화**를 클릭합니다. 이 작업은 MDM용 Ivanti Neurons의 라이센스 할당 정보가 정확하지 않은 경우에만 필요합니다. 이러한 부정확성은 Apple Apps 및 Books API의 불일치로 인해 발생할 수 있습니다.

## Apps 및 Books 계정의 우선순위 업데이트

관리자는 사용될 라이센스에 따라 한 Apps 및 Books 계정에 우선순위를 할당할 수 있습니다. Apps 및 Books 계정의 우선순위는 예측 가능한 라이센스 배포 시스템을 보유하고 사용자 또는 기기가 동일한 앱에 대해 Apps 및 Books 계정의 라이센스를 받을 자격이 있을 때 충돌을 해결하는 데 사용됩니다.

**절차**

1. **앱 > Apple Apps 및 Books**로 이동합니다.
2. 필수 Apps 및 Books 계정 이름에 대해 **우선순위 편집**을 클릭합니다.
3. 우선순위 편집 창에서 새로운 우선순위를 선택합니다.
4. **저장**을 클릭하세요.

## Apps 및 Books 보안 토큰 삭제

Apps 및 Books 보안 토큰을 제거하면 복구할 수 없으며 소멸적입니다. 토큰이 제거되는 경우:

- 토큰을 예약한 앱의 토큰이 제거됩니다.
- 결제가 완료된 앱이 카탈로그에 남아 있어 사용자가 직접 금액을 지불할 수 있습니다.
- 최종 사용자가 회사 Apps 및 Books 계정을 통해 설치한 앱을 사용하고자 하는 경우 개인 계정으로 전환해야 할 수 있습니다. 사용자에게는 전환하기 위한 30일의 유예 기간이 있습니다.

**절차**

1. **앱 > Apple Apps 및 Books**로 이동합니다.
2. Apps 및 Books 계정 이름을 클릭합니다.
3. 토큰 탭에서 **삭제**를 클릭합니다.
4. Apps 및 Books 보안 토큰 삭제 창에서 **예. Apps 및 Books 보안 토큰 삭제** 옵션을 선택하여 확인합니다.
5. **삭제**를 클릭하세요.

## 카탈로그의 Apps 및 Books 앱 라이센스 배포

1. 메인 메뉴에서 **앱 > Apple Apps 및 Books**를 선택합니다.
2. Apps 및 Books 계정 목록이 표시됩니다. 각 계정에 Apps 및 Books 프로그램을 통해 구입한 앱의 목록이 표시됩니다.
   앱을 선택하고 **라이센스 배포**를 클릭합니다.
3. Apps 및 Books 라이센스 섹션에서 배포 옵션인 **선착순**, **예약**, 또는 **허용 불가**를 선택합니다.

## 사용자별 앱 라이센스 보기

라이센스 사용 탭을 이용하여 사용자에 대한 라이센스 환경설정을 볼 수 있습니다.

1. **사용자** 탭을 클릭합니다.
2. 사용자를 선택합니다.
3. **라이센스 사용** 탭을 클릭하세요.
   앱 목록이 Apps 및 Books 라이센스 유형 및 라이센스 할당 상세 정보와 함께 표시됩니다.

사용자별 각 앱에 대한 라이센스 사용을 보려면:

1. MDM용 Ivanti Neurons 메인 메뉴에서 **사용자**로 이동합니다.

2. 사용자를 선택합니다.
3. 기본값으로 **기기** 탭이 표시됩니다.
   **라이센스 사용** 탭을 클릭합니다.
   라이센스 상태를 포함하여 사용자 기기에 설치된 모든 앱의 목록이 표시됩니다. 기기의 일련 번호는 기기 기반 라이센스에 대한 Apps 및 Books 라이센스 유형 열에 기재되어 있습니다.
   - 앱 이름
   - 앱 버전
   - 앱 비용
   - 앱이 할당된 날짜
   - Apps 및 Books 라이센스 유형
   - 작업(라이센스 상태.)
   - 라이선스 플랫폼 정보 세부 사항입니다.

각 앱에 대한 Apps 및 Books 라이센스 사용도 볼 수 있습니다.

1. MDM용 Ivanti Neurons 메인 메뉴에서 **앱 > 앱 카탈로그**로 이동합니다.
2. 앱을 선택합니다.
3. **Apps 및 Books 라이센스** 탭이 있는 경우 클릭합니다.
4. 계정 이름을 클릭합니다. Apps 및 Books 프로그램을 통해 구입한 앱만 이 탭에 표시됩니다.

각 Apps 및 Books 라이센스 유형에 대한 별도의 탭이 표시됩니다.

| 라이센스 유형 및 로그 | 설명 |
|---|---|
| 선착순(FCFS) - 어떤 사용자 그룹이 이러한 라이센스 유형을 수신할지 선택할 수 있는 옵션이 있습니다. | • 사용자 요청 앱 - 사용자가 설치하기로 선택한 앱. 사용자 기반 라이센스는 기본임<br>• 필수 앱 – 이 앱은 필수적이며 **기기에 설치** 설정을 사용하는 관리자 구성에 의해 설치됩니다. 이 앱은 기본적으로 기기 기반 라이센스를 사용합니다. |
| 예약 | 예약된 라이센스는 FCFS 라이센스보다 우선순위가 높습니다. 여기에서 앱에 대한 예약 라이센스를 확보할 사용자 또는 기기를 선택할 수 있습니다. |
| 허용 불가 | 이 앱에 대한 라이센스를 가질 수 없는 사용자를 입력합니다. 이 사용자는 계속해서 앱을 설치할 수 있지만 구입해야 합니다. |
| 작업 로그 | 사용자, 이들에게 할당된 Apps 및 Books 라이센스의 유형, 할당된 날짜, 및 라이센스에서 한 최종 작업을 표시합니다. |

기기별 각 앱에 대한 자세한 라이센스 사용을 보려면:

1. MDM용 Ivanti Neurons 메인 메뉴에서 **기기**로 이동합니다.
2. 기기를 선택합니다.
3. **설치된 앱** 탭을 클릭합니다.
4. 라이센스 상태를 포함하여 선택한 기기에 설치되어 있는 관리되는 앱 전체의 목록이 표시됩니다.
   - 앱 이름
   - 앱 버전

- 지원 플랫폼
- 앱 소스
- 앱 크기
- Apps 및 Books 라이센스 유형
- iOS 앱에 대한 앱 보고(설치) 날짜

다음과 같이 기기에 설치된 앱을 검색합니다.

- 앱 이름
- 번들/패키지 ID

## Apps 및 Books 라이센스 사용 알림

Apps 및 Books 알림을 통해 Apps 및 Books 라이센스 사용을 추적할 수 있습니다. 알림 임계의 정의는 다음과 같습니다.

- 정보 알림은 라이센스의 50% 이상을 사용했을 때 실행됩니다.
- 경고 알림은 라이센스의 70~80%를 사용했을 때 실행됩니다.
- 위험 알림은 라이센스의 90~100%를 사용했을 때 실행됩니다.
- 사용 현황이 50% 이하로 떨어지면 알림이 사라집니다.

각 앱에 대한 라이센스 정보를 보려면:

1. **앱 > Apple Apps 및 Books**를 클릭합니다.
2. 라이센스 정보에 표시되는 내용은 다음과 같습니다.
   - 앱 이름.
   - 라이센스 비용.
   - 이용 가능한 라이센스 수.
   - 교환된 라이센스 수.

**대시보드 > 알림**으로 이동하여 라이센스 알림의 상세 정보를 확인합니다.

3. 알림 페이지가 표시됩니다.
   알림 제목을 클릭하여 상세 정보를 확인합니다. 사용 가능한 알림은 대시보드를 확인합니다.

### Apps 및 Books 라이센스 사용 알림

| 트리거 | 심각도 | 알림 유형 | 구성요소 유형 |
|---|---|---|---|
| 50% 교환됨 | 정보 | 라이센스 사용 | Apps 및 Books |
| 70% 교환됨 | 경고 | 라이센스 사용 | Apps 및 Books |
| 80% 교환됨 | 경고 | 라이센스 사용 | Apps 및 Books |
| 90% 교환됨 | 경고 | 라이센스 사용 | Apps 및 Books |
| 100% 교환됨 | 경고 | 라이센스 사용 | Apps 및 Books |

## Apps 및 Books 라이센스 사용 보기

사용자별 라이센스 사용 정보가 라이센스 열의 라이센스 사용 표에 표시됩니다.

1. 원하는 앱을 클릭하세요.
2. **라이센스 사용** 탭을 클릭하세요.
3. 검색 필드에 사용자 이름을 입력하세요.

## 앱에 대한 Apps 및 Books 라이센스 철회

Apps 및 Books 라이센스는 다음과 같은 경우 철회됩니다.

- (폐기 또는 지워짐) VPP 라이센스가 철회됩니다.
- Apps 및 Books 앱이 삭제됨
- 기기가 폐기되면 기기 기반 라이센스가 철회됩니다.
- Apps 및 Books 토큰이 삭제됨

앱에 대한 Apps 및 Books 라이센스 철회 방법:

1. **앱 > 앱 카탈로그**에서 원하는 앱을 선택합니다
2. **Apple Apps 및 Books 라이센스** 탭이 있는 경우 클릭합니다.
3. 다음 작업 중 하나를 수행합니다.
    1. 모든 사용자 또는 기기에서 모든 라이센스를 철회하려면 **모든 라이센스 철회**를 클릭합니다.
    2. **작업 로그** 탭을 클릭합니다. **작업** 열을 사용하여 사용자별 또는 기기별로 개별 라이센스를 철회합니다.
- iOS 기기에서 Apple은 Apps 및 Books 라이센스가 철회된 이후 Apps 및 Books 앱에 30일의 유예 기간을 제공합니다. 따라서 해당 기간 동안에는 Apps 및 Books 앱 설치가 가능합니다.
- macOS 기기는 Apps 및 Books 라이센스가 철회된 이후에도 앱이 기기에 남아 있습니다.

사용자에 대한 Apps 및 Books 라이센스 철회 방법:

1. 원하는 앱을 클릭하세요.
2. **라이센스 사용** 탭을 클릭하세요.
3. 라이센스 사용 권한을 삭제해야 할 사용자의 **라이센스 철회** 링크를 클릭하세요.

> Apps 및 Books 라이센스는 해당 사용자가 삭제되거나 사용자가 기기에서 MDM 프로필을 삭제할 경우 자동으로 철회됩니다.

### Apps 및 Books 인증 오류 알림

Apple Apps 및 Books 서비스를 사용할 때 인증 오류가 발생할 수 있습니다. 이러한 Apps 및 Books 인증 오류 알림은 다음과 같습니다.

| 오류 알림 | 작업 |
| --- | --- |
| 유효하지 않은 인증 토큰 | 유효한 Apps 및 Books sToken 업로드 |
| 만료된 토큰 | 회사 계정을 사용해 온라인으로 새 토큰 생성 |
| sToken을 성공적으로 해지했습니다. | 유효한 Apps 및 Books 업로드 |
| 로그인 필요 | Apps 및 Books 서비스에 로그인 |

## macOS 및 iOS 기기의 Apps 및 Books 동작

### iOS의 Apps 및 Books

| 작업 | 기기 기반 라이센스 | 사용자 기반 라이센스 |
| --- | --- | --- |
| 사용자에 대한 배포에서 Apps 및 Books 앱 제거 | 앱이 사용자의 기기에서 제거됨 | 앱이 사용자의 기기에서 제거됨 |
| Apps 및 Books 앱 위임 해제 | 앱이 기본 공간이 아닌 공간에 있는 모든 기기에서 제거됨 | 앱이 기본 공간이 아닌 공간에 있는 모든 기기에서 제거됨 |
| 기본 또는 사용자 지정 공간에서 Apps 및 Books 앱 삭제하기 | 앱이 모든 기기에서 제거됨 | 앱이 모든 기기에서 제거됨 |

### macOS의 Apps 및 Books

| 작업 | 기기 기반 라이센스 | 사용자 기반 라이센스 |
| --- | --- | --- |
| 사용자에 대한 배포에서 Apps 및 Books 앱 제거 | 앱이 사용자의 기기에서 제거되지 않음 | NA |
| Apps 및 Books 앱 위임 해제 | 앱이 기본 공간이 아닌 공간에 있는 모든 기기에서 제거되지 않음 | NA |
| 기본 또는 사용자 지정 공간에서 Apps 및 Books 앱 삭제하기 | 앱이 모든 기기에서 제거되지 않음 | NA |

## 기기가 공간을 이동할 때의 Apps 및 Books 라이센스 권한

기기가 새 공간으로 이동할 때 기기 또는 기기 소유자에게 할당된 Apps 및 Books 라이센스는 철회됩니다. 새 공간의 가용성에 따라 새 Apps 및 Books 라이센스가 할당됩니다.

다음은 Apps 및 Books 라이센스 권한 시나리오입니다.

| 시나리오 | 권한 |
| --- | --- |
| Apps 및 Books 라이센스가 소스 공간의 기기 또는 기기 소유자에게 할당되고 동일한 앱에 대한 Apps 및 Books 라이센스가 대상 공간에서 이용 가능합니다. | 대상 공간의 Apps 및 Books 토큰으로부터 라이센스를 할당합니다. |
| Apps 및 Books 라이센스가 소스 공간의 기기 또는 기기 소유자에게 할당되고 동일한 앱에 대한 Apps 및 Books 라이센스가 대상 공간에서 이용 불가합니다. | 소스 공간의 Apps 및 Books 토큰으로부터 라이센스를 철회합니다. |
| Apps 및 Books 라이센스가 소스 공간의 기기 또는 기기 소유자에게 할당되지 않고 모든 설치된 Apps 및 Books 앱에 대한 Apps 및 Books 라이센스가 대상 공간에서 이용 가능합니다. | 대상 공간의 Apps 및 Books 토큰으로부터 라이센스를 할당합니다. |

**앱 범주** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 앱 및 컨텐츠 관리

# 8.19. 카탈로그 설정

이 섹션에는 다음 주제가 포함됩니다.

- Apple 앱 관리 설정 변경
- 기본 App Store 지역 설정
- iOS 앱 업데이트 활성화/비활성화
- 애플리케이션 등급 및 평가 기능 설정/해제 방법
- iOS/macOS Apps 및 Books sToken 업로드 또는 업데이트 방법(라이센스: Gold)
- MDM용 Ivanti Neurons 서비스에서 iOS/macOS 앱 및 Books sToken 제거

**앱** > **카탈로그 설정** 페이지에서 앱 카탈로그의 모든 앱에 적용할 기본 설정을 구성합니다. 다음을 수행할 수 있습니다.

- 기기 체크인 중에 앱 업데이트 포함
- iCloud 및 iTunes의 백업 차단(iOS만 해당)
- 기본 App Store 영역 설정(Apple 및 Microsoft)
- 장치가 미등록 상태일 경우 iOS 앱 제거
- MDM용 Ivanti Neurons "등급 및 평가" 활성화
- iOS 및 macOS Apps and Books 토큰 업로드(Gold 라이선스 필요)

## Apple 앱 관리 설정 변경

개별 앱에 대해 앱 관리 구성이 생성되지 않은 한 이 설정은 모든 앱에 적용됩니다.

1. 다음 체크박스 중 하나 이상을 선택하거나 삭제합니다.
    - **기기 체크인 중 앱 업데이트**(기본 선택됨)
    - **iCloud 및 iTunes에 대한 백업 방지**
    - **미등록 앱 제거**

**저장**을 클릭하세요.

## 알림

1. **Apple 앱 스토어 및 Google Play 스토어에서 새로운 앱 버전이 사용 가능해질 때 시스템 알림 생성** 아래의 드롭다운 목록을 클릭하고 다음 옵션 중 하나를 선택합니다.
    - **1주일에 한 번**
    - **하루 한 번**

**AppCatalog에서 사용할 수 있는 새로운 앱 업데이트에 대한 최종 사용자 알림 생성** 아래의 드롭다운 목록을 클릭하고 다음 옵션 중 하나를 선택합니다.

- **1주일에 한 번**
- **하루 한 번**

## 기본 App Store 지역 설정

App Catalog 설정에서 Apple 및 Microsoft App Store에 대한 기본 지역을 설정합니다.

1. 기본 App Store 지역 섹션에서:
    - **Apple App Store 지역**을 선택합니다.
    - **Microsoft App Store 지역**을 선택합니다.
2. 마지막으로 선택한 App Store 지역을 각 관리자에 대한 기본 지역으로 사용하는 옵션을 선택하거나 삭제합니다. 이 옵션을 선택할 경우 App Store 지역이 각 관리자가 마지막으로 선택한 지역으로 설정되며 이전 설정을 재정의하게 됩니다. 이번이 관리자가 처음으로 이 기능을 사용하는 것일 경우 기본 App Store 지역이 이 절차의 이전 설정으로 설정됩니다.
3. **저장**을 클릭하세요.

## iOS 앱 업데이트 활성화/비활성화

1. **기기 체크인 중 앱 업데이트**를 선택하거나 삭제합니다.
    - 이 옵션은 기본적으로 선택됩니다.
    - 선택을 해제할 경우 기기 체크인 중 앱 업데이트가 되지 않습니다(관리자의 강제 체크인 포함).
    - 그러나 사용자는 기기 앱 카탈로그에서 강제 체크인을 클릭하여 수동으로 앱을 업데이트할 수 있습니다.
    - 새로운 앱 설치와 기타 모든 구성 및 설정은 기기 체크인 중에 업데이트됩니다.

**저장**을 클릭합니다.

관리되는 앱의 경우 관리자는 앱 상세 정보 페이지의 **업데이트** 버튼을 클릭하여 App Store의 최신 버전으로 앱을 수동 업데이트할 수 있습니다.

사용자 기기에서 앱 카탈로그 메뉴의 **강제 체크인** 버튼을 클릭하여 기기 체크인을 허용하고 다른 구성 및 설정과 함께 앱 업데이트가 이루어지도록 허용할 수 있습니다.

이러한 설정을 이용하여 최종 사용자가 앱 업데이트 시점을 선택할 수 있도록 허용합니다.

- 데이터 요금을 부담하지 않으려면 Wi-Fi에 연결한 후에 사용하십시오.
- 앱 업데이트 중에 불편한 잠금 상황을 막을 수 있습니다.

## 애플리케이션 등급 및 평가 기능 설정/해제 방법

이를 통해 사용자가 애플리케이션의 등급을 지정 및 검토하고 다른 사용자가 해당 검토를 읽을 수 있습니다.

1. **최종 사용자 App Catalog 등급 및 평가 기능 설정**을 선택 또는 해제합니다.
2. **저장**을 클릭하세요.

> Apps 및 Books sToken 형식이 변경되었습니다. 이전 버전의 문자열 대신 이제 문자열이 vpptoken 파일 형식의 텍스트 파일로 저장됩니다. 처리를 위해 이 파일을 관리자 콘솔에 직접 업로드하세요. Apps 및 Books 계정 페이지가 업데이트되어 Apps 및 Books 조직 이름과 만료일을 보여줍니다.

## iOS/macOS Apps 및 Books sToken 업로드 또는 업데이트 방법(라이센스: Gold)

1. **Apps 및 Books sToken 추가**를 선택합니다.
2. **별칭 이름** 필드에 sToken 파일의 이름을 입력합니다.
3. sToken 파일을 지정된 영역에 드래그하거나 **파일 선택**을 클릭해 sToken 파일로 이동합니다.
4. **저장**을 클릭하거나, sToken 파일을 업데이트하는 경우 **업데이트**를 클릭합니다.

5. **Apple Apps 및 Books** 페이지를 실행해 현재 토큰과 연동된 앱을 확인합니다.

> MDM용 Ivanti Neurons의 이전 릴리스에서 Apps 및 Books 토큰이 개별 사용자에게 예약된 경우, 해당 토큰이 아직 사용자에게 예약된 상태인지 확인하고 필요한 경우 다시 예약해야 합니다.

## MDM용 Ivanti Neurons 서비스에서 iOS/macOS 앱 및 Books sToken 제거

더 이상 사용자에게 필요하지 않은 앱을 철회하고 필요한 경우 재할당할 수 있습니다. 앱이 iOS/macOS용 MDM와 함께 관리되는 앱으로 배포되었다면 앱과 모든 데이터를 즉시 제거할 수 있습니다.

1. 제거할 앱을 선택합니다.
2. **삭제**를 클릭하세요.
   경고 대화상자가 나타납니다.
3. 필요에 따라 사용자에게 30일간의 유예 기간을 제공하여 사용자로 하여금 다음과 같은 조치를 취하도록 할 수 있습니다.
   - 데이터를 저장합니다.
   - 개인적으로 앱 복사본을 구매합니다.
   - 이 Apps 및 Books 계정으로 설치한 앱을 개인 계정으로 전송하여 계속 사용합니다.

**카탈로그 설정** 창의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할이** 필요합니다.

- 앱 및 컨텐츠 관리

# 8.20. 앱 종속성 배포하기

인하우스 애플리케이션 번들을 업로드하면 MDM용 Ivanti Neurons가 애플리케이션을 스캔하여 종속성을 식별합니다. 종속성을 발견했을 경우 MobileIron Cloud는 앱 추가 마법사의 세 번째 단계에서 종속성을 나열합니다. 애플리케이션 종속성을 위해 관리자는 종속성 파일 업로드를 선택할 수 있습니다. 단, 일부 애플리케이션은 종속성 파일을 업로드하지 않으면 설치되지 않을 수 있습니다.

관리자는 특정 앱을 설치할 때 앱 종속성을 설정할 수 있는 옵션이 있습니다. 이러한 경우 기본 앱으로 태그가 지정된 하나 이상의 앱이 있을 수 있습니다. 사용자가 기본 앱을 설치하려고 하면 기본 앱과 함께 설치될 종속 앱에 대한 알림이 표시됩니다.

> 이 기능은 iOS, Android, Windows 및 macOS 기기에서 지원됩니다.

애플리케이션 종속성 및 필수 조건에 대한 다음 사항에 유의하십시오.

- 관리자는 애플리케이션을 기기에 설치하기 전에 필수 조건인 종속 애플리케이션을 설정할 수 있습니다. 필수 조건 애플리케이션은 인하우스, 공개, 비공개(Android) 또는 VPP 애플리케이션일 수 있습니다.
- 이제 필수 애플리케이션의 수가 App Catalog 페이지의 필수 앱 열에 표시됩니다. 숫자 위에 마우스 커서를 놓으면 필수 애플리케이션 목록이 표시됩니다.
- 메인 애플리케이션 설치가 시작되면 필수 애플리케이션이 직접 다운로드됩니다.
- 메인 애플리케이션이 위임되면 연관된 필수 애플리케이션이 자동으로 위임됩니다.
- 필수 관계가 제거될 때까지는 App Catalog에서 필수 애플리케이션을 삭제할 수 없습니다.
- 한 애플리케이션의 버전마다 서로 다른 필수 애플리케이션을 가질 수 있습니다.
- 감사 추적 페이지는 iOS, Android, macOS용 필수 애플리케이션의 추가, 제거, 자동 위임을 기록합니다.
- 관리자 또는 최종 사용자가 필수 애플리케이션인 애플리케이션을 설치하면 메인 애플리케이션이 설치되기 전에 필수 애플리케이션이 설치됩니다. 모든 필수 애플리케이션이 설치되기 전에 기기 체크인이 발생하면 모든 필수 애플리케이션이 설치 제거됩니다.

> 애플리케이션에 종속성 파일이 필요하더라도 MDM용 Ivanti Neurons에서는 앱을 배포하기 위해 파일을 업로드할 필요가 없습니다.

> Samsung 기기의 경우 관리자는 키오스크 모드 허용 앱 목록에 필수 앱을 추가해야 합니다. 허용된 앱 목록에 추가된 필수 앱은 블랙리스트에 있는 앱 목록에 추가되지 않습니다.

> Samsung이 아닌 기기의 경우 기본 앱이 키오스크 모드 허용 앱 목록에 추가되면 필수 앱이 백그라운드에서 자동으로 실행되어야 합니다. 관리자가 이 앱을 키오스크 모드로 설정한 경우에만 키오스크 모드에서 필수 앱을 볼 수 있습니다.

> **Windows 기기** - Bridge 앱이 배포되지 않은 필수 앱이며 메인 앱이 자동으로 배포되는 .exe일 경우 종속성이 제거되면 Bridge 앱은 삭제되지만 이 단계 이후 .exe에 오류가 발생합니다. 관리자는 Bridge 앱이 기본값으로 배포되었는지 확인해야 합니다.

> **Windows 기기** - 메인 앱이 자동으로 배포되지 않고 메인 앱에 배포되지 않은 필수 앱이 있을 경우, 필수 앱이 우선 설치되며 성공적으로 완료됩니다. 그러나 메인 앱을 설치하지 못한 경우 필수 앱은 즉시 삭제됩니다. 사용자가 설치 요청을 트리거한 경우에만 오류가 발생한 메인 앱 설치를 다시 시도합니다.

## 인하우스 애플리케이션 추가

1. **앱 > 앱 카탈로그**를 선택하세요.

2. **추가**를 클릭합니다.
3. 앱 파일을 점선 박스로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다. 그리고 **확인**을 클릭합니다.
4. **다음**(우측 하단)을 클릭합니다. MDM용 Ivanti Neurons가 앱을 스캔하여 종속성 파일을 찾고 이를 **앱 종속성** 표에 나열합니다.
5. 앱 정보를 검토하고 올바른 앱을 선택했는지 확인합니다.
6. **작업** 열에서 업로드 아이콘을 클릭합니다. **종속성 업로드** 창이 표시됩니다.
7. **파일 선택**을 클릭하여 파일의 로컬 복사본을 탐색하고 위치를 확인한 다음, **업로드**를 클릭합니다.
8. MDM용 Ivanti Neurons는 선택 사항인 앱용 패키지(있는 경우)를 스캔하여 이를 선택 사항 패키지 표에 나열합니다. 열거된 경우에는 작업 열에서 업로드 아이콘을 클릭합니다. 선택 사항 패키지 업로드 창이 표시됩니다.
9. 앱 정보를 검토하고 올바른 앱을 선택했는지 확인합니다.
10. **파일 선택**을 클릭하여 파일의 로컬 복사본을 탐색하고 위치를 확인한 다음, 업로드를 클릭합니다.
11. **다음**을 클릭하세요.
12. (선택 사항) 앱의 화면 캡처를 추가하고 **다음**을 클릭합니다.
13. 애플리케이션에 다른 필수 애플리케이션이 필요한 경우.
    1. **필수 앱** 섹션에서 **켜기** 옵션을 선택합니다.
    2. **앱 추가** 탭에서 필수 애플리케이션을 검색합니다.
    3. 애플리케이션을 선택합니다.
    4. **저장**을 클릭하세요.
14. 앱 배포를 정의하고 **다음**을 클릭합니다.
15. 앱 구성 섹션을 정의하고 **완료**를 클릭합니다. 이후에 기기가 MDM용 Ivanti Neurons와 동기화할 경우 기기에 앱과 종속성 파일이 함께 배포됩니다.

> 종속성 추가 단추를 클릭하여 종속성을 추가할 수 있습니다. 업로드한 추가 종속성은 앱 종속성 표에 나열됩니다. 관리자는 콘텐츠 전용 유형의 선택 사항 패키지를 수동으로 추가할 수도 있습니다. 이 패키지 유형은 버전에 따라 달라지지 않습니다.

## 필수 앱 추가

필수 애플리케이션을 메인 애플리케이션에 추가할 수 있습니다. 메인 애플리케이션의 버전마다 서로 다른 필수 애플리케이션을 추가할 수 있습니다. App Catalog 페이지에서 설명, 스크립트, 스크린샷, 배포, 앱 필수 구성 요소, 앱 구성 등을 기존 애플리케이션 버전의 그것과 동일하게 유지하거나 연결된 필수 애플리케이션을 변경할 수 있는 옵션을 제공합니다. 메인 애플리케이션과의 연관성을 제거하지 않으면 필수 애플리케이션을 삭제할 수 없습니다.

이제 감사 내역 페이지의 특정 필드에는 다음과 같이 지원되는 필수 애플리케이션이 표시됩니다.

감사 추적 페이지의 지원되는 iOS, Android, macOS 애플리케이션에 대한 필수 애플리케이션 섹션에는 다음 필드가 표시됩니다.

appVersionId

이름

platformAppId

다음 필드를 포함하여 자동 위임 또는 위임 취소되는 필수 애플리케이션이 표시됩니다.

dmPartitionDistributionType

dmPartitionDistributionReason

**절차**

1. **App Catalog**에서 애플리케이션을 선택합니다.
2. **편집**을 클릭합니다.
3. **앱 위임**으로 스크롤하여 **이 앱을 모든 공간에 위임** 옵션을 선택합니다.
4. **저장**을 클릭하세요.

> 여러 애플리케이션을 위임한 후에 메인 애플리케이션에서 위임을 제거하려고 하면 필수 애플리케이션은 위임에서 자동으로 제거되지 않습니다.

# 8.21. Android Enterprise로 Divide Productivity 배포

Divide Productivity는 Android Enterprise 장치에 배포할 수 있는 PIM 앱입니다.

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **비즈니스 앱**에서 **Divide Productivity**를 클릭합니다.
3. 추가 카테고리나 설명을 입력합니다.
4. **다음**을 클릭하세요.
5. 표시된 권한을 수락합니다.
6. **다음**을 클릭하세요.
7. 배포 방법을 선택하세요.
8. **고급 옵션 및 앱 구성**을 확장합니다.
9. 다음 지침을 사용하여 옵션을 활성화합니다.
10. 프로모션 방법을 선택하세요.

| 설정 | 설정하기 |
| --- | --- |
| 앱을 제거하지 않도록 차단 | 앱이 자동으로 설치되었을 때 최종 사용자가 앱을 삭제하지 못하게 할 경우 이 옵션을 선택합니다. |
| 메일 주소 | 변수를 사용하여 앱과 연동할 이메일 주소를 정의합니다. |
| 비밀번호 | 변수를 사용하여 이메일 계정의 비밀번호를 정의합니다. 이 필드를 비워두면 사용자에게 비밀번호를 묻는 메시지가 표시됩니다. |
| 호스트 | 사용할 메일 서버의 호스트 이름을 입력합니다. ActiveSync 서버의 전체 도메인 이름을 입력합니다. 독립 실행형 Sentry를 사용 중인 경우, 전체 도메인 이름(FQDN)을 입력합니다.<br>예:<br>mySentry.mycompany.com |
| 서버 유형 | 메일 서버 유형을 선택합니다. |
| 사용자 이름 | 변수를 사용하여 이메일 계정의 사용자 이름을 정의합니다. |
| SSL 필요 | 호스트 필드에서 지정한 서버에 https를 사용하는 보안 통신을 원할 경우 이 옵션을 선택합니다. |
| 모든 인증서 신뢰 | 앱이 신뢰하지 않는 인증서를 자동으로 수락하도록 할 경우에만 이 옵션을 선택합니다.<br>일반적으로 시험 환경에서 작업할 경우에만 이 옵션을 선택합니다. |
| 기본 이메일 서명 | 모든 이메일에 대한 기본 이메일 서명을 입력합니다.<br>최종 사용자는 이때 이 옵션을 변경할 수 있습니다. 기기 사용자가 이 옵션을 변경하면 이 필드를 나중에 변경해도 효과가 없습니다. |
| 이메일 최대 첨부 크기 | 첨부 파일에 허용되는 최대 크기를 입력합니다. |
| 작업 활성화 | 작업을 동기화할 때 선택합니다. |
| 로그인 인증서 별명 | 로그인 증서의 별칭을 입력합니다. |
| Smime 서명 인증서 별명 | 현재 지원되지 않습니다. |
| Smime 암호화 인증서 별명 | 현재 지원되지 않습니다. |
| **고급 옵션** | |
| 기기에 설치 | 사용자에게 앱 설치 메시지를 표시할 경우 이 옵션을 선택합니다. |
| Samsung Knox 기기에 자동 설치 | Samsung Knox 기기에 앱을 자동으로 설치하려는 경우 이 옵션을 선택합니다. |
| 최종 사용자 App Catalog에서 앱 표시 안 함 | 기기에 있는 앱 카탈로그에서 앱을 보지 않을 경우 이 옵션을 선택합니다. |

11. **완료**를 클릭합니다.

# 8.22. Provisioner 앱 설정

이 섹션에는 다음 주제가 포함됩니다.


- 프로비저닝 요건
- NFC bump를 사용하도록 Android 빔을 활성화
- 기업 소유 기기의 프로비저닝
- 기기 등록
- 기기 등록 상태 검증


Provisioner는 회사 소유 장치를 프로비저닝하여 업무 관리형 장치로 등록하고 장치 소유자 모드로 배치될 수 있도록 하는 데 사용되는 MDM용 Ivanti Neurons 앱입니다.

기업 관리 기기는 기업 프로필만 있으며 개인 프로필은 없습니다. 관리자는 카메라, 전화, SMS, 네트워킹 등 기기 기능을 제한할 수 있는 20가지 이상의 잠금을 기기에서 설정할 수 있습니다.

Provisioner 앱은 NFC 범프로 Android Enterprise 대상 장치의 구성을 시작하는 장치에 필요합니다. 기업 소유 기기를 제공하려면 Provisioner 앱을 마스터 기기에 설치하고 NFC(근거리 무선통신) bump를 사용하여 새로운 기기를 제공합니다. Bump는 두 기기를 함께 누릅니다. 기기는 다음 클라이언트 앱 중 하나를 이용하여 프로비저닝될 수 있습니다.

- MDM용 Ivanti Neurons와 Go 사용
- 브랜드 없는 클라이언트 앱인 At Work UEM은 MDM용 Ivanti Neurons와 함께 사용합니다.

## 프로비저닝 요건

기업 소유의 Android Enterprise 장치를 업무 관리형 장치로 프로비저닝하려면 다음 단계를 진행합니다.

- 기업 소유의 기본 Android Enterprise 지원 장치는 프로비저닝 이전에 공장 재설정해야 합니다.
- Android 장치 그룹에 Android Enterprise 구성을 정의하고 적용해야 합니다.
- NFC 가능 Android 기기는 Provisioner 앱이 설치된 상태에서 마스터 또는 템플릿 역할을 하도록 지정해야 합니다.
- Android Enterprise 지원 장치를 프로비저닝합니다.
- Provisioner 앱
  Android용 Provisioner 앱을 Google Play에서 다운로드합니다.

## NFC bump를 사용하도록 Android 빔을 활성화

**절차**

1. 기기에서 **설정**으로 이동합니다.
2. **무선 & 네트워크**로 이동하여 **더 보기**를 클릭합니다.
3. **NFC** 체크박스를 선택합니다.
4. **Android 빔**을 클릭하고 **켜기** 쪽으로 밀어 전환합니다.

> 정확한 단계는 기기마다 약간 다를 수 있습니다.

## 기업 소유 기기의 프로비저닝

**절차**

1. Provisioner 앱을 Android 마스터 기기로 사용할 기기에 설치합니다.
2. 마스터 기기에서 Provisioner를 시작합니다.
3. 드롭다운 메뉴에서 앱을 선택합니다.
4. Provisioner 앱에서 요청한 정보를 입력합니다. 지원되는 Wi-Fi 유형이 존재하는 경우 일부 필드는 자동으로 채워질 수 있습니다. 다음의 지침을 사용합니다.

| 필드 | 값 |
|---|---|
| 프로비저닝을 위한 앱 선택 | Go(MDM용 Ivanti Neurons와 사용하려면 선택)<br>At Work UEM(브랜드 없는 클라이언트 앱, 브랜드 있는 MDM용 Ivanti Neurons와 함께 사용하기 위해 선택). |
| Wi-Fi 네트워크 SSID | 마스터 기기를 사용할 Wi-Fi SSID를 입력합니다. |
| Wi-Fi 보안 유형 | Wi-Fi 보안 유형을 입력합니다. |
| Wi-Fi 비밀번호 | Wi-Fi 비밀번호를 입력합니다. |
| 표준 시간대 | 지역의 현재 표준 시간대를 입력합니다. |
| 로캘 | 로캘을 입력합니다. |

5. **계속**을 클릭하세요.
   마스터 기기에 **기기를 맞부딪히세요** 화면이 표시됩니다.
6. 대상 기기를 켜고 Android 시작 화면을 표시하면서 대상 기기와 마주한 마스터 기기를 눌러 NFC 전송을 시작합니다.
   NFC 전송이 성공하면 대상 기기에 소리가 울릴 수 있으며 이후에 선택한 클라이언트 앱의 다운로드를 진행합니다. 기기가 암호화되지 않은 경우 계속 진행하기 전에 암호화 과정이 시작됩니다.
7. 기기를 두드려 별도의 기기를 계속 프로비저닝합니다. 대상 기기에는 시작 화면이 표시되어야 하고, 마스터 기기에는 **기기를 맞부딪히세요** 화면이 표시되어야 합니다.

## 기기 등록

기업 소유 기기를 NFC bump로 프로비저닝한 경우 선택한 클라이언트 앱이 설치됩니다. 클라이언트 앱을 시작하고 기기를 등록합니다.

## 기기 등록 상태 검증

**절차**

1. **장치 > 장치**를 선택하세요.
2. 세부 정보를 표시할 기기 링크를 클릭합니다.
3. 기기 상태가 좌측 작업창에 표시됩니다.

# 8.23. Windows 애플리케이션 관리

사용자는 Windows 애플리케이션의 전체 앱 수명 주기를 관리(가져오기, 구성, 예약, 배포, 업데이트, 삭제)할 수 있습니다. MDM 콘솔을 통해 앱 배포 및 앱 업데이트 프로세스가 지원됩니다. Windows 앱 및 기타 애플리케이션의 세부 정보를 확인하려면 앱 구성, 앱 인사이트, 앱 카탈로그를 참조하십시오.

## 지원되는 앱 유형

- 인하우스(앱 카탈로그 섹션에서 **인하우스 앱 추가** 옵션 확인)
- MSB(Microsoft Store for Business integration)
- 공용 스토어(기본 Microsoft Store 통합 경유) Microsoft Store 지역은 앱 > 카탈로그 설정에서 설정할 수 있습니다. 자세한 내용은 앱 카탈로그 섹션의 **공용 스토어에서 앱 추가**를 참조하십시오.

## 지원되는 앱 확장

- MSI
- MSIX
- APPX
- APPX 번들
- EXE(**Ivanti Bridge**를 통해)

## 앱 컨트롤

앱 컨트롤 구성은 장치별 앱 설치를 제어합니다. 자세한 내용은 앱 컨트롤 구성: 기기당 설치된 앱 컨트롤을 참조하십시오.

## 패키지 및 종속성

다음과 같은 다양한 기능을 사용할 수 있습니다.

1. Windows 앱은 모든 애플리케이션 유형의 필수 구성 요소로 설정할 수 있습니다. 앱 필수 구성 요소를 설정하는 방법에 대한 자세한 내용은 앱 종속성 배포하기를 참조하십시오.
2. APPX 및 APPX 번들 앱 종속성과 기타 패키지 종속성. 앱 상세 정보 보기 페이지에서 **앱 종속성과 기타 패키지** 섹션을 살펴보십시오.
3. Win32 앱은 올바른 제품 코드(MSI)와 명령줄, 변수의 선택을 지원합니다. 일반 명령줄 옵션의 목록은 여기에서 확인하실 수 있습니다.

## 스크립트

스크립트는 Ivanti Bridge Client를 통해 지원됩니다. 스크립트 지원에 대한 자세한 내용은 **Ivanti Bridge**를 참조하십시오.

장치에 Ivanti Bridge가 설치되면 스크립트가 다음과 같이 배포됩니다.

- Ivanti Bridge를 통해 스크립트 및 작업의 장치 수준에서
- Ivanti Bridge 구성을 통해(**구성** > **브리지**로 이동)

**기기의 기존 버전 확인** 확인란은 내부 MSI 및 EXE 애플리케이션의 **스크립트 및 파일** 탭에서 사용할 수 있으며, Windows 기기에서 앱이 설치되는 방식을 제어합니다. 이 옵션을 활성화하면 기기는 체크인을 실행하여 앱이 이미 설치되어 있는지 확인하고 해당 버전을 식별합니다. MDM용 Ivanti Neurons 에서는 앱이 설치되어 있지 않거나 설치된 앱 버전이 필수 버전보다 이전 버전인 경우에만 앱을 설치하거나 업그레이드합니다. 동일하거나 더 최신 버전이 있으면 설치를 건너뜁니다. 이 옵션을 활성화하려면 먼저 하나 이상의 기기에 앱이 설치되어 있어야 합니다.

## 설치 전, 설치 후 스크립트 및 파일

**.exe 파일 및 .MSI 파일**

PowerShell 설치 전, 설치 후 스크립트, 레지스트리 스크립트, Windows 실행(.exe) 파일을 구성하고 앱 세부 정보 수준에서 Windows 앱의 다른 파일 유형을 다운로드할 수 있습니다.

설치 전, 설치 후 스크립트 또는 파일을 새로 추가할 때 Ivanti Bridge 화면이 나타납니다. 스크립트 또는 파일을 첨부하고, 스크립트 인수를 추가하고, 파일의 대상 위치를 제공할 수 있습니다. 앱 설치 명령을 기기로 보내기 전에 기기에서 설치 전 스크립트를 성공적으로 실행해야 합니다. 설치 전, 설치 후 스크립트와 파일은 콘솔 업로드와 동일한 순서대로 실행/설치됩니다. 설치 전 스크립트 다운로드 또는 설치에 실패한 경우 앱 설치를 진행할 수 없습니다.

설치 후 스크립트가 실패한 경우 기기 로그 섹션 밑에 있는 기기 세부 정보 페이지에서 오류를 확인할 수 있습니다. 또한 설치 후 작업에 실패하더라도 설치 전 스크립트/다운로드한 파일과 설치한 .exe 파일은 되돌릴 수 없습니다.

스크립트 및 파일 우선순위 지정 옵션을 사용하여 설치 전 또는 설치 후 스크립트 및 파일을 재정렬할 수 있습니다. 이 옵션은 사용 가능한 스크립트나 파일이 둘 이상인 경우에만 사용할 수 있습니다. 이 옵션을 사용하면 한 섹션에서 다른 섹션으로가 아니라 각각의 사전 또는 사후 섹션 내에서 파일이나 스크립트를 끌어다 놓을 수 있습니다.

## 설치 동작 및 구성

Windows 애플리케이션은 다음 기능을 지원합니다.

- 자동 설치
- **Windows 앱 일정 설정**
- 다시 부팅 옵션

설치 동작 옵션에 대한 자세한 내용은 **앱 구성**을 참조하십시오.

> MSI 앱 및 EXE 앱(Bridge를 사용하여 설치됨)은 사용자 없는 MDM 세션에 대한 설치를 지원합니다.

다음과 같은 시나리오를 예로 들 수 있습니다.

- 장치가 다시 시작되었으며 아직 로그인한 사용자가 없습니다
- 사용자가 Windows 세션에서 로그아웃했습니다
- 장치가 Autopilot 사용자 없음(셀프 배포 또는 사전 프로비저닝) 모드에 등록되었습니다
- 장치 수준에서 애플리케이션이 설치됩니다

> 보다 효율적인 방식의 MSI 앱 설치를 허용합니다. 예를 들어, Autopilot 등록 중이나 Windows 장치로 작업하는 사람이 없는 야간에 앱을 설치합니다. MSI에서 EXE에 단순한 리패킹을 사용할 경우 설치는 가능하지만 업그레이드하거나 삭제할 수는 없습니다. 실제 MSI 패키지는 CSP와 연결되어 있습니다. 다른 애플리케이션 유형은 사용자 로그인 이후에 설치됩니다.

## Windows용 터널(앱별 VPN)

터널은 독립 실행형 기본 Windows 애플리케이션입니다. 현재 Microsoft Store에서 장치 배포용으로 사용할 수 있습니다. 앱별 VPN 구성을 만듭니다. Sentry 배포가 필요합니다. 터널 앱을 구성하려면 **구성** > **+추가** > 터널 검색(Windows 장치를 지원하는 구성 선택)으로 이동합니다. Sentry 프로필을 선택하고 설정을 구성하여 Sentry를 통한 앱 데이터 터널링을 시작합니다. Sentry 서버를 설정하려면 **관리자** > **인프라** > **Sentry**로 이동합니다.

## 앱 인벤토리

Windows 장치에 설치된 애플리케이션 및 소프트웨어 인벤토리는 두 가지 단계로 추적할 수 있습니다.

- 여러 장치에 설치된 애플리케이션을 확인하려면 **장치** > **앱 인벤토리**로 이동합니다
- 장치 수준에서 인벤토리를 확인하려면 장치로 이동하여 장치를 선택하고 설치된 앱을 클릭합니다.

관리자는 Windows 애플리케이션 인벤토리 수집 간격을 설정할 수 있습니다. 관리 > Windows > 앱 인벤토리 간격으로 이동합니다 개인 정보 보호 구성이 장치의 모든 앱을 수집하도록 설정된 경우 간격이 사용됩니다. 개인 정보 보호 구성을 구성하려면 구성 > +추가로 이동하여 개인 정보 보호를 검색하고 장치의 모든 앱에 대해 앱 인벤토리 수집을 선택합니다. 수집할 앱 유형을 선택합니다.

## 기업 앱 카탈로그(Apps@Work)

고객은 Windows 장치에서 Apps@Work를 사용하여 기업 카탈로그를 활성화할 수 있습니다. Apps@Work는 UEM용 Neurons의 앱 카탈로그를 통해 사용하고 배포할 수 있습니다. 자세한 내용은 **Apps@Work(iOS, Android, Windows, macOS)**를 참조하십시오.

# 8.24. Ivanti Bridge

이 섹션에는 다음 주제가 포함됩니다.


- Bridge 지원 파일 유형
- Bridge 설정
- Bridge 로그
- Bridge Last Check-in
- Bridge 서비스 장애 복구


Ivanti Bridge는 단일 콘솔과 커뮤니케이션 채널을 사용하여 Windows 10의 모바일 및 데스크톱 작업을 통합합니다. 또한 UEM 기능을 관리 중인 PC로 확장하고 조직에서는 크게 줄어든 비용과 향상된 효율성을 활용하면서 모든 PC와 모바일에서 일관된 보안을 유지할 수 있습니다. Ivanti Bridge를 사용하면 기업은 지원되는 Windows 모바일 장치와 같이 Windows 10 Desktop 장치에 대해 단일 프로토콜을 사용하여 OS의 레거시 애플리케이션에 정보를 전송할 수 있습니다.

Ivanti Bridge를 사용하면 IT 부서가 중요한 기능을 포기하지 않고도 UEM에서 Windows 작업을 현대화할 수 있습니다. IT 부서는 시스템 이미징, 도메인 가입 또는 기기에 대한 다중 통신 채널을 요구하지 않고도 이미 활용되고 있는 정책과 스크립트를 적용할 수 있습니다.

조직은 이제 Ivanti Bridge를 통해 다음과 같은 작업을 진행할 수 있습니다.

- UEM으로 PC를 완벽하게 제어
- 무선으로 원격 PC 관리
- 데스크톱 영상화 필요성 감소
- UEM에서 배포한 PowerShell 스크립트로 GPO 기반 명령 활용
- 레지스트리를 쉽게 편집 및 관리
- 비 MSI 래핑된 Win32 앱 및 Win32 스토어 앱을 손쉽게 배포
- 파일 시스템 확인 가능

> Ivanti Bridge는 Windows 11 이상의 기기 및 ARM 프로세서에서 지원됩니다. Ivanti Bridge는 Windows 10 홈 데스크톱 장치를 지원하지 않습니다.

## Bridge 지원 파일 유형

Ivanti Bridge는 다음 유형의 지원을 포함합니다.

- PowerShell
  Bridge 지원팀에서 명명한 인수를 사용하여 기기에 푸시된 PowerShell 스크립트입니다.
  64비트 PowerShell 스크립트가 64비트 Windows 10 데스크톱 기기에 지원됩니다.

> PowerShell 스크립트 전송 후 결과를 기다리는 서버 측의 Bridge 시간 제한은 약 20분입니다. 제한 시간을 초과할 경우 실패로 로그됩니다. 하지만 장치의 스크립트는 계속해서 작동합니다.

> PowerShell 스크립트 실행 프로세스를 기다리는 장치 측의 Bridge 시간 제한은 약 60분입니다. 60분 후 프로세스가 종료되며 스크립트의 출력이 저장되지 않습니다. 그리고 서버로 새로운 실패가 전송됩니다.

> 서버 측, 장치 측 제한 시간을 초과할 경우 실패로 로그됩니다. 두 번째 시간 제한을 패스하고 스크립트가 일부 출력을 생성할 경우 서버 측에 출력이 로그되지 않습니다.

레지스트리

- VB 스크립트
- Win32 애플리케이션 배포용 .EXE
- Win32 스토어 앱은 WinGet 도구를 사용하여 앱을 설치 및 제거합니다.

> 관리자가 Win32(.EXE) 파일을 기기(예: Windows 인하우스 앱)로 푸시해야 하는 경우 Bridge 기능이 자동으로 사용됩니다(해당되는 경우). 파일을 자동으로 실행하려면 인수를 입력해야 합니다(예: /SILENT 또는 /VERYSILENT).
> .EXE 앱은 PowerShell 관리 모드를 사용하여 Bridge를 통해 설치됩니다. Windows 기기의 경우, 사용자 자격 증명을 사용하여 설치하려면 "사용자로 실행" 옵션을 선택하십시오.

> 관리자는 사용자를 위해 앱을 설치하려면 **앱 설치 프로그램 - 설정**에서 **설치 프로그램을 사용자로 실행** 확인란을 선택해야 합니다. 시스템 수준에서 앱을 설치하려면 확인란을 선택하지 마십시오.

Ivanti Bridge를 사용하여 다음과 같은 핵심 영역에서 장치를 확대할 수 있습니다.

- **레지스트리**: 레지스트리 값을 읽고, 쓰고, 업데이트합니다.
- **파일**: 파일 내용을 확인하고, 읽고, 업데이트합니다.
- **애플리케이션 배포:** 데스크톱 기기에 .EXE 기반 애플리케이션을 설치할 수 있는 기능을 추가합니다. 이러한 애플리케이션은 MDM용 Ivanti Neurons 서버 또는 클라우드의 CDN(콘텐츠 전송 네트워크)에 있을 수 있습니다.

# Bridge 설정

Ivanti Bridge를 설정하려면 관리자가 다음과 같은 순서로 단계를 완료해야 합니다.

1. Bridge 라이선스 활성화
2. Bridge 앱 설치
3. 기기에 영구 또는 1회용 장치에 스크립트 업로드

## Bridge 라이선스 활성화

Ivanti Bridge는 레거시 골드 패키지의 일부이자 현재 보안 UEM의 일부입니다.

## Bridge 앱 설치

Ivanti Bridge 라이선스를 활성화한 후 Bridge 모바일 애플리케이션을 다음과 같이 설치할 수 있습니다.

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **+추가**를 클릭합니다.
3. 비즈니스 앱 섹션에서 **Ivanti Bridge**를 클릭합니다.
4. 확보한 라이센스에 따라 세부 정보를 추가하고 사용자 지정한 다음, 필요한 Bridge 모바일 애플리케이션을 필요한 장치에 배포합니다. **Windows 기기에 자동 설치** 옵션을 활성화했다면 브리지 모바일 애플리케이션이 자동 설치되고 기기에서 Bridge 서비스가 실행됩니다.

> Bridge 앱은 기본적으로 App Catalog에 추가될 뿐 아니라 기본적으로 모든 기기에 배포됩니다.

> 관리자는 최신 버전의 Ivanti Bridge를 테넌트의 카탈로그로 가져온 후 새로 정렬된 앱 버전을 볼 수 있습니다.

## 장치에 스크립트 업로드

관리자는 새로운 Bridge 구성을 생성하여 영구적인 사용을 위해 기기에 스크립트를 업로드할 수 있습니다.

1. **구성 > +추가**로 이동합니다.
2. **Windows용 Ivanti Bridge 스크립트 및 작업 구성**을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. Ivanti Bridge 구성 섹션에서 다음 두 가지 옵션 중 하나를 사용하여 스크립트를 업로드합니다.
   - 스크립트 라이브러리에서 스크립트 선택 - 목록에서 사용 가능한 스크립트 중 하나를 선택합니다.
   - 또는
     스크립트 업로드 - 7단계의 표에 설명된 대로 설정을 지정합니다.
     - **스크립트 파일** 스크립트 파일 카테고리 설정을 입력하여 기기에 푸시하거나 실행할 설치 스크립트를 지정합니다.
     - (선택 사항) **실행 취소스크립트 파일** 카테고리 설정을 입력하여 기기에 푸시되거나 실행될 제거 스크립트를 지정합니다. 이는 장치 폐기 또는 구성 삭제와 같은 작업에 유용합니다.
     - (선택 사항) Bridge를 사용하여 Microsoft Outlook을 기기에 구성하려면 **Outlook 구성** 옵션을 선택합니다.

       > Outlook 2010 및 2013에서만 지원됩니다.

**다음**을 클릭하세요.

7. 이 구성에 대한 배포를 선택합니다.
   이러한 기기 작업에는 강제 체크인이 자동으로 수행됩니다.

| 범주 | 설정 | 설정하기 |
| --- | --- | --- |
| | 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| | 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 스크립트 파일 | **모든 버전(Windows 10+ 데스크톱)**<br>스크립트 파일 | 유효한 스크립트 또는 실행 파일(.ps1, .reg, .exe)을 선택하십시오.<br>• 지정된 스크립트 파일 또는 실행 파일(.ps1, .reg, .exe)이 자동으로 실행됩니다.<br>• 다른 파일 유형은 대상 폴더로만 복사됩니다. |
| | 스크립트 인수 | 스크립트 파일의 인수 목록을 지정합니다.<br>• Win32(.exe) 파일의 경우 파일을 자동으로 실행하려면 인수를 입력해야 합니다(예: /SILENT 또는 /VERYSILENT). 이는 필수입니다. |
| 스크립트 파일 실행 취소 | 대상 폴더<br>**모든 버전(Windows 10+ 데스크톱)** | 스크립트 파일의 대상 폴더를 지정합니다.<br>• 대상 폴더를 지정하지 않을 경우 %TEMP% 시스템 환경 변수 값이 대상 폴더로 사용됩니다. |
| | 스크립트 파일 | 유효한 스크립트 또는 실행 파일(.ps1, .reg, .exe)을 선택하십시오.<br>• 지정된 스크립트 파일 또는 실행 파일(.ps1, .reg, .exe)이 자동으로 실행됩니다.<br>• 다른 파일 유형은 대상 폴더로만 복사됩니다. |
| | 스크립트 인수<br>대상 폴더 | 스크립트 파일의 인수 목록을 지정합니다.<br>• Win32(.exe) 파일의 경우 파일을 자동으로 실행하려면 인수를 입력해야 합니다(예: /SILENT 또는 /VERYSILENT). 이는 필수입니다.<br>스크립트 파일의 대상 폴더를 지정합니다.<br>• 대상 폴더를 지정하지 않을 경우 기본적으로 %TEMP% 시스템 환경 변수 값이 사용됩니다. |

## 장치에 1회용 스크립트 업로드

관리자는 기기에 1회용(ad hoc) 스크립트를 업로드할 수 있습니다.

1. **장치 > 장치**를 선택하세요.
2. 기기 이름 링크를 클릭하여 기기 상세 정보 페이지로 이동합니다. 1회용 스크립트는 Windows 10 데스크톱 장치에서만 푸시/실행됩니다.
3. ⋮ 아이콘을 클릭하고 **Ivanti Bridge를 통한 스크립트 및 작업**을 클릭합니다.
4. 이름을 입력합니다.
5. 스크립트 파일 섹션에서 이전 표에서 설명한 대로 장치에서 푸시/실행될 스크립트를 지정합니다.
6. **적용**을 클릭합니다.
   스크립트 실행은 대기 상태가 되고 완료하는 데 다소 시간이 걸릴 수 있습니다. 로그 탭으로 이동하여 상태를 확인합니다 (출력 또는 오류 메시지). 이러한 기기 작업에는 강제 체크인이 자동으로 수행됩니다.

## Bridge 로그

이 기능을 사용하면 개별 장치의 Ivanti Bridge 로그를 끌어와 문제 해결 및 애플리케이션 진단에 사용할 수 있습니다. 로그는 다음 기기 체크인 시 전송됩니다. 다음 예약된 동기화 일정을 기다리거나 강제 장치 체크인을 수행하여 로그를 빠르게 얻을 수 있습니다.

기기에서 로그를 끌어오는 방법:

1. **장치 > 장치**를 선택하세요.
2. 기기 이름 링크를 클릭하여 기기 상세 정보 페이지로 이동합니다. 1회용 스크립트는 Windows 10 데스크톱 장치에서만 푸시/실행됩니다.
3. ⋮ 아이콘을 클릭하고 **Ivanti Bridge 로그 끌어오기**를 클릭합니다. **Ivanti Bridge 로그 끌어오기** 창이 표시됩니다.
4. 다음 옵션 중 하나를 선택합니다.
   **단일 로그** – 기기에 최신 Bridge 로그를 끌어오도록 MDM용 Ivanti Neurons에 요청합니다.
   **모든 로그** – 기기에 모든 로그(최장 30일)를 끌어오도록 MDM용 Ivanti Neurons에 요청합니다.
5. **로그 끌어오기**를 클릭합니다. 기기가 이를 MDM용 Ivanti Neurons로 전송한 후에는 기기 세부 정보 페이지의 로그 탭에서 Bridge 로그를 볼 수 있습니다.

> **모든 로그** 옵션을 사용하여 전송된 로그만 zip 파일로 다운로드할 수 있습니다.

## Bridge Last Check-in

Bridge Last Check-in 열에는 장치 페이지상 Bridge 서비스의 마지막 체크인 날짜와 시간이 나열됩니다. 열 사용자 지정 옵션을 사용하여 장치 페이지에 열을 추가할 수 있으며, 표시되지 않는 것이 기본값입니다.

이 열을 표시하려면 **장치** > **열 사용자 지정** > **Bridge Check-in**을 선택합니다.

> 해당하는 경우 내보낸 데이터에도 Bridge Last Check-in 세부 정보가 포함됩니다.

## Bridge 서비스 장애 복구

Bridge 서비스 장애 복구는 Bridge 2.1.14 버전에 도입되었습니다. 기본적으로 이 버전은 모든 사용자의 앱 카탈로그로 도입됩니다. 드문 경우지만 알려진 이유 없이 브리지 서비스에 장애가 발생할 수 있습니다. 이러한 경우 Bridge 2.1.14 이상 버전에서 지원이 가능합니다.

# 9. 컨텐츠

콘텐츠 페이지를 사용하여 외부 소스에 의해 호스트되는 콘텐츠를 배포합니다. 콘텐츠에는 영업용 안내자료, 이미지, 가격표, 문서와 같이 사용자가 다운로드할 수 있는 파일이 포함될 수 있습니다.

이 섹션에는 다음 주제가 포함됩니다.

- 콘텐츠 관리
- 범주

# 9.1. 콘텐츠 관리

이 섹션에는 다음 주제가 포함됩니다.

- 호스트된 콘텐츠 배포
- 콘텐츠 삭제

호스트된 콘텐츠는 다운로드 가능한 콘텐츠를 외부 URL을 사용하여 배포할 수 있도록 지원합니다. 외부 URL은 다운로드 가능한 PDF 또는 EPUB 또는 IBOOK 파일에만 연결되어야 하며, 외부 URL에 이러한 확장자가 붙어야 합니다.

VPP Book 라이선스 배포는 지원되지 않으므로 iTunes Store ID 기반의 Apple Books 배포는 지원되지 않습니다.

기기에서 Books 또는 Pages 앱을 사용하여 MDM용 Ivanti Neurons에서 푸시된 콘텐츠에 액세스합니다. 라이브러리 섹션에서 액세스할 수 있습니다.

**iBook 및 EPUB** 컨텐츠가 iOS 8+ iPad 기기(Gold 라이센스)로 배포될 수 있습니다. 이 형식은 iPad로 제한되는데, 이는 Apple이 이러한 형식의 사내 배포를 iPad로만 지원하기 때문입니다. 이러한 제한은 iOS 9 기기에는 적용되지 않습니다.

> 이러한 형식에는 콘텐츠 미리 보기가 제공되지 않습니다.

**PDF** 콘텐츠의 경우 iOS 8+ 기기의 iBook 앱으로 문서를 푸시할 수도 있습니다.

## 호스트된 콘텐츠 배포

새 문서를 MDM용 Ivanti Neurons에 업로드할 수 없더라도 콘텐츠가 호스트된 경로(URL)를 제공하고 기기 그룹에 배포할 수 있습니다.

**절차**

1. **콘텐츠 > 호스트된 콘텐츠**로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. 다음 정보를 입력합니다.
    - 소유자
    - 작성자
    - 범주
    - (선택 사항) 설명
4. **호스트된 콘텐츠 경로** 필드에서 업로드하려는 파일의 URL을 입력합니다.
5. **다음**을 클릭하세요.
6. 필요한 경우 배포 설정을 수정하세요.
7. **완료**를 클릭하세요.

호스트된 콘텐츠를 수정하는 경우 이전의 콘텐츠는 삭제하고 새로 호스트된 콘텐츠를 추가하여 배포해야 합니다.

URL이 아닌 설정을 수정하는 경우

1. **콘텐츠 > 호스트된 콘텐츠**로 이동합니다.
2. **이름** 열에서 문서로 연결되는 링크를 클릭합니다.
3. 편집 아이콘을 클릭합니다.
4. 원하는 설정으로 변경합니다.

5. **다음**을 클릭하세요.
6. 필요한 경우 배포 설정을 수정하세요.
7. **완료**를 클릭합니다.

## 콘텐츠 삭제

1. **이름** 열에서 문서로 연결되는 링크를 클릭합니다.
2. **작업 > 현재 문서 삭제**를 선택합니다.
3. 삭제를 원하면 체크박스를 클릭하세요.
4. **문서 삭제**를 클릭합니다.

삭제한 문서는

- 시스템에서 제거됩니다.
- 더 이상 컨텐츠 카탈로그에서 사용할 수 없습니다.
- 해당 문서를 다운로드했던 장치에서 삭제됩니다.

**콘텐츠** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할이 필요합니다.

- 앱 및 컨텐츠 관리

# 9.2. 범주

이 섹션에는 다음 주제가 포함됩니다.

- 범주 추가
- 범주 삭제

> 2017년 4월 15일에 발표된 컨텐츠 지원 종료의 일환으로, 새 컨텐츠를 추가하는 기능이 비활성화됩니다. 현재 업로드된 컨텐츠는 계속해서 Apple iBooks 앱에 배포하고 사용할 수 있습니다.

범주에서는 {{콘텐츠 카탈로그}} 내의 {{콘텐츠}} 유형을 설명합니다. 범주는 컨텐츠를 구성해 사용자가 원하는 항목을 간편하게 찾을 수 있도록 도와줍니다. 컨텐츠 카탈로그에 등록된 각 항목에는 반드시 1개 이상의 범주를 할당해야 합니다.

## 범주 추가

**절차**

1. **추가**를 클릭합니다(좌측 하단).
2. 범주 이름을 입력합니다. 범주는 대소문자를 구분하지 않습니다.
3. **저장**을 클릭하세요.

## 범주 삭제

범주 옆에 있는 X를 클릭하여 범주를 제거할 수 있습니다.

**콘텐츠(콘텐츠)** 페이지의 작업을 수행할 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할이 필요합니다.

- 앱 및 컨텐츠 관리

# 10. 구성

구성은 장치에 보낸 여러 설정 값의 모음입니다. 예를 들어, 구성을 이용해 자동으로 VPN 및 기기 암호 규격 관련 설정을 할 수 있습니다. 시스템의 기존 구성이 구성 페이지에 나열됩니다.

이 섹션에는 다음 주제가 포함됩니다.


- 구성 작업
- 사용자 셀프 서비스 포털 구성 만들기
- 사용자 지정 구성
- 사용자 지정 구성을 사용하여 장치에 SyncML 푸시
- 홈 화면 레이아웃 구성
- 앱 컨트롤 구성: 기기당 설치된 앱 컨트롤
- 앱 알림 구성
- 구성 내보내기
- 구성 우선순위 지정
- 구성 관리하기

# 10.1. 구성 작업

이 섹션에는 다음 주제가 포함됩니다.

- 구성 디스플레이 필터링
- 구성 추가
- 구성 배포
- 구성의 점진적 롤아웃 배포
- 여러 기기로 구성 푸시
- 구성 제외
- 제외된 구성 푸시
- 구성 내보내기
- 구성 가져오기
- 구성 편집
- 구성 삭제
- 인하우스 애플리케이션 업데이트 예약
- 활성 사용자 세션이 필요한 Windows 구성

구성은 관리자로서 장치에 보낸 여러 설정 값의 모음입니다. 예를 들어, 구성을 이용해 자동으로 VPN 및 기기 암호 규격 관련 설정을 할 수 있습니다. 구성 페이지에 시스템의 기존 구성이 나열됩니다. 구성 페이지에서 구성을 여러 개 선택하고 한 번에 다수의 장치로 푸시할 수 있습니다. 공간별 장치로 이러한 구성을 푸시할 수 있으며, 대상 공간이 아닌 다른 공간에는 영향을 미치지 않습니다. 한 번에 하나의 공간이나 여러 공간, 모든 공간에 구성을 푸시할 수 있습니다.

다양한 구성 유형을 활용할 수 있습니다. 구성은 기본적으로 다음 범주로 분류됩니다.

- 보안
- 사용자 리소스
- 엔터프라이즈 네트워크 액세스
- 휴대폰 네트워크
- 기타(추가 설정)

대부분의 구성에 대해 다음 작업을 수행할 수 있습니다.

- 추가
- 수정
- 복제
- 삭제
- 특정 기기에서 한 개 이상의 구성 제외
- 한 개 이상의 제외된 구성을 특성 기기에 푸시

일부 구성은 작업이 제한됩니다.

- 일부 구성을 추가 또는 복제할 수 없습니다. iOS 활성화 잠금은 이러한 구성 유형의 예입니다. 그러므로, 이러한 구성은 구성을 추가할 때 나열되는 타일에 나타나지 않습니다. 이러한 구성은 구성 페이지에만 나열됩니다.

- 시스템 자체에서 정의된 구성은 수정이나 삭제가 불가능합니다. iOS 등록을 위한 SCEP가 이러한 구성 유형의 예입니다.
- 일부 구성은 기기에서 삭제 또는 재설치할 수 없는 것으로 표시될 수 있습니다. 이러한 구성은 기기에 제외 또는 푸시할 수 없습니다.

## 구성 디스플레이 필터링

**구성** 페이지에서 전체 구성 목록을 확인할 수 있습니다. 이 목록을 특정 구성으로 좁히려면 OS 및 구성 유형에서 필터(왼쪽 창)를 사용하십시오. 예를 들어 macOS 구성만 표시하도록 목록 범위를 좁히려면 **OS** 섹션에서 **macOS**를 선택합니다.

드롭다운 목록에서 여러 공간을 선택하여 모든 또는 여러 공간 기기 전반의 구성을 볼 수 있습니다. 표시된 구성 위에 마우스를 놓으면 공간 목록이 있는 팝업 창이 표시됩니다. 공간을 클릭하여 구성 상세 정보 페이지를 표시할 수 있습니다.

DDM 관련 구성을 쉽게 파악하고 구성 유형을 더 명확하게 구분할 수 있도록 **Apple DDM** 아래의 **지원됨** 필터를 적용합니다.

기존 구성을 이름에 따라 검색하려면 **검색** 필드에 구성 이름을 입력합니다.

MDM용 Ivanti Neurons 릴리스 81부터 전역 관리자는 모든 기기 및 사용자 지정 배포 옵션에서 동적으로 생성된 ID 인증서를 편집할 권한을 공간 관리자에게 위임할 수 있습니다.

## 구성 추가

이 옵션은 드롭다운 목록에서 하나의 공간이 선택된 경우에만 활성화됩니다.

> 한 번에 최대 100개의 구성 파일을 배포할 수 있습니다.

**절차**

1. **추가**를 클릭합니다.
2. 생성할 구성 유형을 선택하세요.
3. **다음**을 클릭하세요.
4. 이 구성을 즉시 활성화하지 않으려면 **이 구성 활성화** 옵션을 지웁니다.
5. 구성의 배포 수준을 선택합니다.
    - **모든 기기** - 사용 가능한 모든 기기에 구성을 배포합니다. 공간 전체에 구성을 위임하려면 다음 옵션 중 하나를 선택합니다.
        - **다른 공간에 적용하지 마십시오**.
        - 모든 공간에 구성을 위임하려면 **배포 요약** > **다른 공간에 있는 기기에 적용**을 선택합니다.
            - 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.
    - **배포 안 함** - 나중에 배포하려면 이 구성을 선택합니다.
    - **사용자 지정** - 이 구성을 전송할 특정 기기 그룹을 정의합니다. 공간 전체에 구성을 위임하려면 다음 옵션 중 하나를 선택합니다.
        - **다른 공간에 적용하지 마십시오**.
        - **배포 요약** > **다른 공간에 있는 기기에 적용**.
            - 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.

    > 관리자는 사용자 지정 배포 옵션을 사용하여 기기, 기기 그룹, 사용자, 사용자 그룹으로 구성을 사용자 지정을 배포할 수 있습니다. 다음 구성에 대해 사용자 또는 사용자 그룹으로 구성 할당 또는 배포를 사용할 수 없습니다.

- Android Enterprise: 직장 프로필(Android for Work)
- Android Enterprise: 회사 관리형 장치(Android for Work)
- Android Enterprise: 직장 프로필/회사 소유 기기에 직장 프로필이 있는 관리형 기기
- 업무 관리형 기기 비 GMS 모드(AOSP) 기기용 Android 업무 관리형 기기(기기 소유자)

6. 서비스에 공간이 정의된 경우 이 구성을 다른 공간에 적용할지 여부와 우선순위를 명시해야 합니다.
7. **완료**를 클릭하세요.

> 기기에 프로필을 설치하는 대신 기기에 명령을 내리는 구성의 경우, 구성 상세 정보에는 다른 기기에 적용된 것과 같은 구성이 나열되지 않습니다.

## 구성 배포

전역 관리자는 공간 관리자에게 모든 장치 및 사용자 지정 배포 옵션에 대해 동적으로 생성된 ID 인증서를 편집하도록 위임할 수 있습니다. 동적으로 생성된 인증서의 경우 **이 구성을 모든 공간에서 사용할 수 있도록 허용합니다** 옵션을 필요에 따라 선택할 수 있습니다. 이 옵션을 선택하면 동적으로 생성된 ID 인증서를 모든 공간에서 사용할 수 있게 되며, Exchange, Wi-Fi, VPN, 기타 관리되는 앱 구성을 포함한 해당 구성 모두에서 사용할 수 있습니다. 이 옵션은 동적 생성 ID 인증서가 연결된 구성의 일부로 기기(기본 공간이 아닌 공간에 있음)에만 배포되고 개별 구성으로 배포되지 않아야 하는 시나리오에 사용될 수 있습니다.

**절차**

1. 해당하는 경우 개별 구성에 대해 표에 지정된 정보를 사용하여 설정 필드를 지정합니다.
2. **다음**을 클릭하세요.
3. **이 구성 활성화** 옵션을 선택합니다.
4. (선택 사항) **이 구성을 모든 공간에서 사용할 수 있도록 허용합니다**를 선택합니다.
5. 다음 배포 옵션 중 하나를 선택합니다.
   - **모든 기기**. 다음 옵션 중 하나를 선택합니다.
     - **다른 공간에 적용하지 마십시오**.
     - **다른 공간에 있는 기기에 적용하십시오**.
     - **다른 장치 공간의 모든 장치에 최우선 순위로 적용**. (Wi-Fi 구성에만 적용)
     - **다른 장치 공간의 모든 장치에 가장 낮은 우선순위로 적용**. (Wi-Fi 구성에만 적용)
       - 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.
   - **배포 안 함**(기본값)
   - **사용자 지정**다음 옵션 중 하나를 선택합니다.
     - **다른 공간에 적용하지 마십시오**.
     - **다른 공간에 있는 기기에 적용하십시오**.
     - **다른 장치 공간의 모든 장치에 최우선 순위로 적용**. (Wi-Fi 구성에만 적용)
     - **다른 장치 공간의 모든 장치에 가장 낮은 우선순위로 적용**. (Wi-Fi 구성에만 적용)
       - 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.

> 공간에 관계없이 동적으로 생성된 ID 인증서는 모든 공간에 구성되고 모든 기기에 배포되며 기타 기기 공간에 있는 모든 기기에 적용될 수 있습니다.

6. **완료**를 클릭합니다.

## 구성의 점진적 롤아웃 배포

**사용자 정의** 옵션을 사용하여 구성을 배포하는 경우 점진적 롤아웃 프로세스로 일정에 따라 구성을 단계적으로 배포할 수 있습니다. 점진적 롤아웃 배포는 수동 또는 예약 방식으로 예약할 수 있습니다.

> 점진적 롤아웃 배포는 VPN 및 Wi-Fi 구성에서만 지원됩니다.

**절차**

1. **구성** > **추가**로 이동합니다.
2. 필수 구성을 검색합니다.
3. **이름**, **설명** 등의 상세 정보를 입력합니다. 구성에 따라, **다음**을 클릭합니다.
4. 배포 옵션으로 **사용자 정의**를 선택합니다. 화면에 **점진적 롤아웃 배포** 섹션이 표시됩니다.
5. **점진적 롤아웃 배포 방법 사용**을 선택합니다. **수동 롤아웃** 및 **예약된 롤아웃** 옵션이 화면에 표시됩니다.
   - **수동 롤아웃** - 이 옵션을 사용하여 배포 대상의 백분율을 수동으로 설정할 수 있습니다. 지정한 백분율에 해당하는 기기에만 배포됩니다 또는 **선택 요약에 포함된 모든 기기**를 선택하여 모든 기기에 구성을 배포할 수 있습니다.
   - **예약된 롤아웃** - 이 옵션을 사용하여 배포를 4단계로 롤아웃합니다. 각 단계에서 롤아웃 백분율을 지정할 수 있으며, 각 후속 단계의 백분율은 이전 단계보다 높아야 합니다. 단계 간 기간은 최소 1일 이상이어야 하며, 30일을 초과할 수 없습니다. 가장 최근에 저장된 구성은 이후 구성에서 편집 가능한 템플릿으로 자동으로 사전 로드됩니다.
6. 구성을 배포할 대상 그룹을 선택합니다.
7. **완료**를 클릭하세요.

상세 정보는 **구성** > 새로 만든 구성 > **상세 정보**에서 확인할 수 있습니다. 상세 정보 페이지에서 롤아웃을 일시 중지하거나 재개할 수 있습니다.

> 예약된 롤아웃으로 새 구성을 만들면 기존 구성을 만들 때 지정한 백분율이 새 구성에도 그대로 적용됩니다. 상세 정보를 편집하거나 기존 백분율을 그대로 사용할 수 있습니다.

## 기기로 구성 푸시

제외된 구성을 기기에 다시 설치하고자 하는 경우 구성을 푸시할 수 있습니다.

**절차**

1. **기기** > **기기**로 이동합니다.
2. 세부 정보 페이지를 표시할 기기 이름을 클릭합니다.
3. **구성**으로 이동합니다.
4. 확인란을 선택하여 기기로 푸시할 특정 구성을 선택합니다.
5. **프로필 푸시**를 클릭합니다.
6. 1개의 구성을 푸시하려면 **작업** 열 아래의 **푸시**를 클릭합니다.

## 여러 기기로 구성 푸시

구성 페이지에서 여러 구성을 선택하여 이를 한 번에 여러 기기로 푸시할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**으로 이동합니다.
3. 확인란을 선택하여 특정 구성을 선택합니다.
4. **작업**을 클릭하고 기기로 **선택한 구성 푸시**를 선택합니다. 푸시 구성 마법사가 열리며 모든 구성과 그 푸시 상태가 표시됩니다.
5. **유효한 구성 푸시**를 클릭합니다. 구성이 모든 기기로 대량 푸시됩니다. **기기** > **구성** 탭에서 특정 기기에 대해 제외된 구성은 푸시되지 않습니다.

## 구성 제외

이전에 배포된 일부 구성을 제외하여 이를 기기에서 수동으로 제거할 수 있습니다.

**절차**

1. **기기** > **기기**로 이동합니다.
2. 세부 정보 페이지를 표시할 기기 이름을 클릭합니다.
3. **구성**으로 이동합니다.
4. 확인란을 선택하여 특정 구성을 선택합니다.
5. **프로필 제외**를 클릭합니다.

> 1개의 구성을 제외하려면 **작업** 열 아래의 **제외**를 클릭하십시오. 선택한 구성이 이제 제외된 구성 탭에 열거됩니다.

## 제외된 구성 푸시

**절차**

1. **기기** > **기기**로 이동합니다.
2. 세부 정보 페이지를 표시할 기기 이름을 클릭합니다.
3. **구성** > **제외된 구성**으로 이동합니다.
4. 기기에 푸시할 1개 이상의 구성을 선택합니다.
5. **프로필 푸시**를 클릭합니다.
6. 1개의 구성을 푸시하려면 **작업** 열 아래의 **푸시**를 클릭합니다.

## 구성 내보내기

선택한 구성의 상세 정보 또는 선택한 공간의 모든 구성을 개별 파일로 내보낼 수 있습니다.

**절차**

1. **구성**으로 이동합니다.
2. 확인란을 선택하여 특정 구성을 선택합니다.

3. **작업** > **선택한 구성 및 상세 정보 내보내기**를 클릭합니다. 모든 구성을 내보내려면 **상세 정보가 있는 모든 구성 내보내기**를 선택합니다.
   YAML 파일 집합은 .ZIP 파일에 포함되어 있습니다. 보고서에는 선택한 공간의 모든 기존 구성 상세 정보가 포함됩니다.

### 모든 구성 내보내기

구성 파일을 내보내어 지원 팀에 전송하면 진단 보조 자료로 사용할 수 있습니다. 단일 구성 파일을 YAML 형식의 파일로 내보내거나 모든 구성을 .zip 파일로 내보낼 수 있습니다. 내보낼 구성에 따라 구성 페이지의 다른 영역에서 파일을 내보낼 수 있습니다.

**절차**

1. **구성**으로 이동합니다.
2. 확인란을 선택하여 특정 구성을 선택합니다.
3. **작업** > **선택한 구성 및 상세 정보 내보내기**를 클릭합니다. 모든 구성을 내보내려면 **상세 정보가 있는 모든 구성 내보내기**를 선택합니다.
   YAML 파일 집합은 .ZIP 파일에 포함되어 있습니다. 보고서에는 선택한 공간의 모든 기존 구성 상세 정보가 포함됩니다.

### 사용자 지정 구성 내보내기

**절차**

1. **구성**으로 이동합니다.
2. **+추가**를 클릭하여 구성을 선택합니다.
3. 단계에 따라 구성을 사용자 지정합니다.
4. **다음**을 클릭하세요.
5. 배포 수준을 선택합니다.
6. **완료**를 클릭하세요.
7. **구성** 페이지의 목록에서 방금 만든 구성을 선택합니다.
8. **작업** 풀다운 메뉴와 **내보내기를 차례로 클릭합니다.**

---

를 클릭합니다. 해당 구성의 이름을 가진 파일과 timestamp_yyyymmdd.yaml 파일이 기기에 다운로드됩니다.

### 기존 구성 내보내기

**절차**

1. **구성**으로 이동합니다.
2. 기존 구성을 선택합니다.
3. **작업** 풀다운 메뉴를 클릭하고 **내보내기**를 클릭합니다.
   해당 구성의 이름을 가진 파일과 timestamp _yyyymmdd.yaml 파일이 다운로드됩니다.

## 구성 가져오기

구성 세부 정보가 포함된 YAML 파일을 가져올 수 있습니다. YAML 파일의 세부 정보를 편집하여 구성을 편집할 수 있습니다. 구성을 선택하고 파일을 불러오면 구성에 업데이트된 값이 표시됩니다. 하나 이상의 구성이나 공간을 선택한 경우 가져오기 버튼이 비활성화됩니다. 잘못된 파일 유형을 선택한 경우 오류 메시지가 표시됩니다. 구성에 필요한 세부 정보와 다른 세부 정보가 포함된 YAML 파일을 선택할 경우 오류 메시지가 표시됩니다.

**절차**

1. **구성**으로 이동합니다.
2. 구성을 선택하고, **가져오기**와 **파일 선택**을 차례로 클릭하고, YAML 파일을 선택하고, **가져오기**를 클릭합니다. 구성 세부 정보가 포함된 YAML 파일을 가져옵니다.

### 지원되는 화이트리스트로 지정된 구성

- CERTIFICATE
- VPN
- WEBCLIP
- IDENTITY_CERTIFICATE_DG
- RESTRICTIONS
- ANDROID_WORK_DEVICE_OWNER_LOCKDOWN
- PASSCODE
- HOME_SCREEN_LAYOUT
- ANDROID_ADVANCED_PASSCODE_AND_LOCK_SCREEN
- IOS_APP_CONTROL
- SCEP
- ANDROID_SAMSUNG_SAFE_LOCKDOWN
- ANDROID_WORK_DEVICE_OWNER_WITH_WORK_PROFILE_LOCKDOWN
- ANDROID_WORK_LOCKDOWN
- DEVICE_NAME
- MOBILE_THREAT_DEFENSE
- PRIVACY
- APP_LOCK
- GOOGLE_ACCOUNT
- ANDROID_WORK_APP_RUNTIME_PERMISSION
- IDENTITY_PREFERENCE
- MAC_OS_AGENT
- MANAGED_GOOGLE_PLAY
- ANDROID_MI_TUNNEL
- ANDROID_ENCRYPTION
- ANDROID_APP_CONNECT
- APPCONNECT_DEVICE_SETTINGS
- ANDROID_WORK_DEVICE_OWNER_SYSTEM_UPDATE
- DOMAINS
- END_USER_PRIVACY
- EXCHANGE
- MI_CLIENT_PRIVACY
- APP_UPDATE_SCHEDULE

- ZERO_PASSWORD
- WINDOWS_PRINTER
- PRINTING
- AUTH_ONLY
- SAFETYNET
- OSX_RESTRICTIONS
- WATCH_OS_RESTRICTIONS
- VISION_OS_RESTRICTIONS
- ANDROID_APP_CONTROL
- WINDOWS_APP_CONTROL
- ANDROID_SAMSUNG_PHONE_RESTRICTIONS
- MAM
- ANTI_PHISHING
- SETUP_ASSISTANT
- DNS_SETTINGS
- WINDOWS_KIOSK
- FIDO_AGENT
- WINDOWS_BITLOCKER
- WINDOWS_DEVICE_ADMIN_RESTRICTIONS
- TELECOM_SETTINGS
- IDENTITY_CERTIFICATE_UP
- IDENTITY_CERTIFICATE_DC
- WIFI
- NOTIFICATIONS
- WEB_CONTENT_FILTER
- WINDOWS_AI_MANAGEMENT
- WINDOWS_ENERGY_SAVER
- WINDOWS_BROWSER
- WINDOWS_DESKTOP
- WINDOWS_PHONE_RESTRICTIONS
- WINDOWS_UPDATE
- WINDOWS_GPO_ADMX
- WINDOWS_LICENSE
- WINDOWS_ATP
- WINDOWS_LAPS
- WINDOWS_EDP
- WINDOWS_BIOS

- WINDOWS_BLOATWARE_REMOVER
- WINDOWS_HELLO
- WINDOWS_START_MENU

## YAML 파일을 사용하여 구성 만들기

YAML 파일로 구성을 만들 수 있습니다. 배포 관련 사양은 YAML 파일의 일부가 아닙니다. 배포의 기본 설정은 장치 없음입니다.

**절차**

1. **구성**으로 이동합니다.
2. **가져오기**와 **파일 선택**을 차례로 클릭하고 YAML 파일을 선택한 후 **가져오기**를 클릭합니다. 구성 세부 정보가 포함된 YAML 파일을 가져옵니다. 만들기 구성 페이지가 열리고 YAML 파일에 추가된 모든 세부 정보가 표시됩니다.
3. 배포 유형 중 *하나*를 선택합니다.
    - **모든 기기**
    - **기기 없음**
    - **사용자 지정**
4. 구성의 세부 정보를 확인하고 다음 배포 요약 옵션 중 *하나*를 선택합니다.

> 일부 구성에서는 배포 요약을 사용할 수 없습니다.

    - **다른 공간에 적용하지 않음**
    - **다른 공간의 장치에 적용**
5. 구성의 새 이름이 기존 구성 이름과 일치할 경우 오류 메시지가 표시됩니다. **확인**과 **뒤로**를 차례로 클릭한 후 구성 이름을 편집합니다.
6. **다음**을 클릭하고 **완료**를 클릭합니다.

## 구성 편집

구성을 열고 구성의 세부 정보를 직접 편집할 수도 있고, 모든 필요한 세부 정보가 포함된 YAML 파일을 가져올 수도 있습니다. 하나 이상의 구성이나 공간을 선택한 경우 가져오기 버튼이 비활성화됩니다.

**절차**

1. **구성**으로 이동합니다.
2. 구성을 선택하여 열고 편집(연필) 아이콘을 클릭하여 구성을 편집합니다.
3. 또는 구성 편집 페이지에서 **가져오기** 아이콘을 클릭하고 YAML 파일을 선택한 후 **가져오기**를 클릭합니다. 구성 편집 페이지가 열리고 YAML 파일에 추가된 모든 세부 정보가 표시됩니다.
4. 구성의 세부 정보를 확인하고 다음 배포 요약 옵션 중 하나를 선택합니다.

> 일부 구성에서는 배포 요약을 사용할 수 없습니다.

    - **다른 공간에 적용하지 마십시오**.
    - **다른 공간의 장치에 적용**

        > 배포의 기본 설정은 장치 없음입니다.

5. **완료**를 클릭합니다.

## 구성 삭제

선택한 구성을 삭제할 수 있습니다.

**절차**

1. 확인란을 선택하여 특정 구성을 선택합니다.
2. **작업** > **삭제**를 클릭합니다.

## 인하우스 애플리케이션 업데이트 예약

MDM용 Ivanti Neurons 는 기기가 체크인할 때 사내 애플리케이션을 자동으로 업데이트합니다. 이제 관리자는 서버 시간대를 기준으로 인하우스 애플리케이션 업데이트를 예약할 수 있습니다. 애플리케이션은 기기가 예약된 시간 내에 체크인하는 경우에만 업데이트됩니다. 기본적으로 애플리케이션 업데이트 예약 기능은 비활성화되어 있습니다.

> 이 구성은 업데이트에만 적용되며 새 설치에는 적용되지 않습니다. 설치/업데이트 요청 보내기 명령을 사용하여 iOS 애플리케이션의 자동 업데이트 일정을 재정의할 수 있습니다. 앱 수준 또는 카탈로그 수준에서 자동 업데이트가 활성화된 경우 예약된 앱 구성보다 우선하고 앱은 체크인 즉시 업데이트됩니다.

구성은 다음 애플리케이션 유형에만 적용할 수 있습니다.

- iOS 인하우스 애플리케이션
- Android 인하우스 애플리케이션(DO 모드에서만)
- .pkg 및 .MIP 형식의 macOS 애플리케이션
- Windows 애플리케이션

**필수 조건**

구성이 원하는 대로 기능하려면 다음 필수 조건이 충족되어야 합니다.

- iOS 및 Android의 경우 애플리케이션이 관리 상태여야 합니다. macOS의 경우 애플리케이션이 관리 상태일 수도 있고 관리되지 않는 상태일 수도 있습니다.
- 애플리케이션 구성의 기기에 설치 옵션이 활성화된 상태여야 합니다.
- 예약된 시간 동안 기기가 체크인되어야 합니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**으로 이동합니다.
3. **추가**를 클릭합니다. 추성 추가 페이지가 열립니다.
4. **앱 자동 업데이트**를 검색합니다. 앱 자동 업데이트 구성 생성 페이지가 열립니다.
5. **이름** 필드에서 이름을 지정합니다.
6. **구성 설정** 섹션의 드롭다운 목록에서 **시간대**를 선택합니다.
7. 드롭다운 목록에서 **시작 시간**을 선택한 다음, 드롭다운 목록에서 **기간**을 선택합니다.
8. **다음**을 클릭하세요.
9. 필수 사용자 및 기기 그룹을 선택한 다음, **이 구성 활성화** 체크박스를 클릭합니다.

10. **완료**를 클릭합니다. 구성이 적용되어 앞으로 애플리케이션은 지정된 일정에만 업데이트됩니다.

구성 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 기기 관리
- 장치 읽기 전용

**관련 주제:**

- 공간
- 구성 우선 순위 지정

## 활성 사용자 세션이 필요한 Windows 구성

일부 Windows 구성은 프로비저닝하기 전에 활성 사용자 세션(기기에 로그인한 사용자)이 필요합니다. 로그인한 사용자가 없는 경우 MDM 사용자가 기기에 로그인한 후 이러한 구성이 적용됩니다.

다음 구성에는 활성 사용자 세션이 필요합니다.

- 암호
- 사용자 인증서(사용자 범위 ID 인증서)
- Windows 방화벽
- 구성을
- VPN
- Windows 라이선스
- 엔드포인트용 Microsoft Defender
- Windows 설정(사용자 범위)
- Bridge 서비스 종속 구성
- Modern/UWP 애플리케이션

### Bridge 서비스 종속 구성

Ivanti Bridge 서비스가 필요한 구성은 활성 사용자 세션을 사용할 수 있는 경우에만 프로비저닝됩니다. 예를 들면 Windows 데스크톱 제한, 브라우저 설정, 시작 메뉴, 키오스크, BIOS, Windows 스크립트, GPO 및 기타 Bridge 서비스 종속 구성이 있습니다.

**예외**: 다음 기본 Bridge 스크립트에는 활성 사용자 세션이 필요하지 않으며 MDM 사용자의 로그인 여부와 관계없이 기기로 전송됩니다.

- get-device-data.ps1
- get-bitlocker-status.ps1
- device-hardware.ps1

### Modern/UWP 애플리케이션

Modern/UWP 애플리케이션은 활성 사용자 세션을 사용할 수 있는 경우에만 프로비저닝됩니다. 여기에는 다음이 포함됩니다.

- .appx 또는 .appxbundle로 패키징된 내부 애플리케이션
- Microsoft Store/UWP 애플리케이션

기존 MSI 및 EXE 애플리케이션에는 이 요구 사항이 적용되지 않습니다.

구성 배포가 예약된 시점에 필요한 사용자 세션을 사용할 수 없는 경우 MDM 사용자가 기기에 로그인하면 구성이 자동으로 프로비저닝됩니다.

# 10.2. 사용자 셀프 서비스 포털 구성 만들기

엔터프라이즈 사용자는 셀프 서비스 포털을 사용하여 기기와 인증서를 관리할 수 있습니다. 내 기기 탭에는 사용자가 등록한 기기가 표시됩니다.

내 기기 탭에서는 다음 작업을 수행할 수 있습니다.

- 잠금
- 잠금 해제
- 폐기
- 보안 앱 암호 재설정

내 인증서 탭에서는 다음 작업을 수행할 수 있습니다.

- 인증서 업로드

> 한 번에 최대 100개의 구성 파일을 배포할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **추가**를 클릭합니다.
3. **사용자 셀프 서비스 포털 구성 만들기**를 검색합니다.
4. **다음**을 클릭하세요.
5. 이 구성을 즉시 활성화하지 않으려면 **이 구성 활성화** 옵션을 지웁니다.
6. 구성의 배포 수준을 선택합니다.
    - **모든 기기** - 사용 가능한 모든 기기에 구성을 배포합니다. 공간 전체에 구성을 위임하려면 다음 옵션 중 하나를 선택합니다.
        - **다른 공간에 적용하지 마십시오**.
        - 모든 공간에 구성을 위임하려면 **배포 요약** > **다른 공간에 있는 기기에 적용**을 선택합니다.
            - 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.
    - **배포 안 함** - 나중에 배포하려면 이 구성을 선택합니다.
    - **사용자 지정** - 이 구성을 전송할 특정 기기 그룹을 정의합니다. 공간 전체에 구성을 위임하려면 다음 옵션 중 하나를 선택합니다.
        - **다른 공간에 적용하지 마십시오**.
        - **배포 요약** > **다른 공간에 있는 기기에 적용**.
            - 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.
7. 서비스에 공간이 정의된 경우 이 구성을 다른 공간에 적용할지 여부와 우선순위를 명시해야 합니다.
8. **완료**를 클릭하세요.

> 기기에 프로필을 설치하는 대신 기기에 명령을 내리는 구성의 경우, 구성 상세 정보에는 다른 기기에 적용된 것과 같은 구성이 나열되지 않습니다.

# 10.3. 사용자 지정 구성

이 섹션에는 다음 주제가 포함됩니다.

- 사용자 지정 구성 정의
- 사용자 지정 구성 설정

**라이센스: Silver**

**적용 대상:** iOS, macOS, tvOS, Android, Windows

**설명**

사전 정의된 구성 파일을 가져오고 배포합니다.

유효한 구성 파일 형식은 다음과 같습니다.

| OS | 유효한 구성 파일 형식 |
|---|---|
| iOS 및 tvOS | • .plist<br>• .mobileconfig<br>• .xml |
| macOS | • .plist<br>• .mobileconfig |
| 안드로이드 | .xml. 지금은 Zebra 기기에 .xml 구성 파일만 지원됩니다. |
| Windows | SyncML |

## 사용자 지정 구성 정의

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 "사용자 지정"을 입력하고 **사용자 지정** 구성을 클릭합니다.
   사용자 지정 구성 상세 페이지가 나타납니다.
4. 이 페이지에서 설정을 구성합니다. 값에 대한 안내는 사용자 지정 구성 설정 섹션의 표를 참조하십시오.
5. **다음**을 클릭해 배포 설정을 구성합니다.
6. (macOS 기기) 이 구성에서 원하는 동작에 따라 **구성 적용 대상** 설정의 추가 옵션을 선택합니다.
   - 기기 전체(일반적으로 사용).
   - 사용자별(현재 등록 사용자).

**완료**를 클릭하세요.

## 사용자 지정 구성 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| OS 선택 | OS 아이콘을 클릭하여 선택한 아이콘에 해당하는 구성 파일을 업로드합니다. |
| 파일 선택 | 이 옵션은 OS를 선택한 이후에 나타납니다. 구성 파일을 드래그 앤 드롭 박스로 끌어 놓거나 **파일 선택** 버튼을 클릭해 구성 파일을 선택합니다. |

## 사용자 지정 CSP 구성(Windows만 해당)

Windows 기기에서만 맞춤 CSP 구성을 만들 수 있습니다. OS 선택 섹션에서 Windows OS를 선택하면 다음 두 가지 옵션이 표시됩니다.

**옵션 1 - CSP XML 파일** - 이 옵션을 선택하고 **파일 선택** 설정에 대해 언급된 동일한 프로세스를 따릅니다.

**옵션 2 - 사용자 지정 CSP OMA-URI 스키마 노드**

**절차**

1. 목록에서 사용자 지정 CSP OMA-URI 스키마 노드 옵션을 선택합니다. 화면에 사용자 지정 CSP 구성 섹션이 표시됩니다.
2. **작업**에서 + 버튼을 클릭하여 다른 OMA-URI 필드로 구성 만들기를 시작합니다.
3. 다음 필드가 있는 화면에 **행 추가** 팝업 창이 나타납니다.
    - 설명 - 설정에 대한 일반 정보를 입력합니다.
    - OMA-URI - 설정으로 사용하려는 OMA-URI를 입력합니다.
    - 데이터 유형 - 이 설정에 사용할 데이터 유형 선택 - DATE, FLOAT, BASE64, NODE, XML, BINARY, CHARACTER, TIME, BOOLEAN, INTEGER
    - 값 - 선택한 데이터 유형과 연관된 값을 입력합니다.
    - 액세스 유형 - 추가, 삭제, 실행, 교체, 가져오기

**저장 후 닫기**를 클릭하여 세부정보가 제공된 창을 닫습니다. **저장 및 추가**를 눌러 다른 항목에 대한 행을 새로 만듭니다.

5. **다음**을 클릭하세요.
6. 배포 모드를 선택하고 **완료**를 클릭합니다.

**관련 주제**

- 사용자 지정 구성을 사용하여 기기에 SyncML 푸시
- 구성을 생성하는 방법

# 10.4. 사용자 지정 구성을 사용하여 장치에 SyncML 푸시

자신만의 SyncML(Synchronization Markup Language) 구성 파일을 생성하거나 제3의 소스를 통해 파일을 확보하고 이를 사용자 지정 구성에 추가하여 사용자 지정 기능을 실행할 수 있습니다.

**지원되는 플랫폼:**

- Windows

**지원되는 기기:**

- Windows 10+
- Microsoft HoloLens 2

**절차**

1. **구성**으로 이동합니다.
2. **+추가**를 클릭합니다.
3. **사용자 지정 구성**를 클릭하여 **사용자 지정 구성 생성** 페이지를 표시합니다.
4. 구성 이름을 입력합니다.
5. Windows OS 아이콘을 클릭합니다.
6. SyncML 파일을 인터페이스에 드래그하거나 **파일 선택**을 클릭하여 기기에 업로드할 파일을 검색합니다.

> MDM용 Ivanti Neurons는 파일의 코드에 대한 유효성 검사를 수행하지 않습니다.

7. **다음**을 클릭하세요.

**사용자 지정 SyncML 로그**

Windows 장치로 전송된 SyncML 명령과 장치에서 이 명령에 대한 SyncML 응답은 장치 로그 탭에서 볼 수 있습니다. 이 로그 정보는 **Windows Custom SyncML** 구성을 보낸 후에 사용할 수 있습니다. 시스템에서 사용자 지정 SyncML 구성을 보내면 SyncML 응답과 관계없이 구성에 대한 장치 "구성" 탭에 항상 "설치됨" 상태가 표시됩니다.

# 10.5. 홈 화면 레이아웃 구성

홈 화면 레이아웃 구성은 홈 화면에 대한 앱, 폴더 및 웹 클립의 레이아웃을 정의합니다.

이 섹션에는 다음 주제가 포함됩니다.

- 홈 화면 레이아웃 구성 정의
- 홈 화면 레이아웃 구성 설정

**라이센스**: Silver

**해당하는 기기**:

- iOS 9.3+ 감독 모드 전용
- tvOS 감독 모드 전용

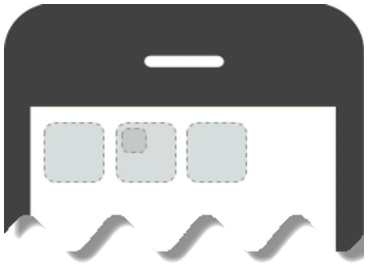
## 홈 화면 레이아웃 구성 정의

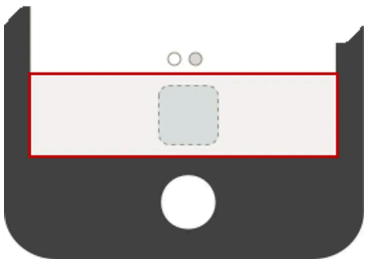
**절차**

1. **구성**으로 이동하여 **+추가**를 클릭합니다.
2. 검색 필드에 "홈"을 입력하고 **홈 화면 레이아웃** 구성을 클릭합니다. 홈 화면 레이아웃 구성 세부 정보 페이지가 열립니다.
3. 이 페이지에서 설정을 구성합니다. 값에 대한 안내는 Home_Screen_Layout_Configuration_Settings 섹션의 표를 참조하십시오.
4. **다음**을 클릭해 배포 설정을 구성합니다. 공유 iPad 기기의 경우 **기기** 채널 또는 **사용자** 채널을 선택합니다. 자세한 내용은 구성 작업을 참조하십시오.
5. **완료**를 클릭하세요.

### 홈 화면 레이아웃 구성 설정

| 설정 항목 | 수행 작업 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 도크 | + 아이콘을 클릭하여 여기에 강조 표시된 홈 화면의 도크에 앱 또는 웹 클립을 추가한 다음, 후속 화면의 지시를 따릅니다.<br><br>'com.apple'으로 시작하는 Apple 번들 ID를 입력하여 수동으로 시스템 앱을 추가할 수도 있습니다. 예를 들어, 'Files' 앱을 추가하려면 'com.apple.DocumentsApp'을 입력합니다. |
| 페이지 1 | ⊕ 아이콘을 클릭하여 앱이나 웹클립을 홈 화면의 페이지 영역에 추가합니다(강조된 부분). 그 이후에 나오는 화면의 지시를 따릅니다.<br><br>페이지 추가를 클릭하여 전화기 디스플레이에 다른 페이지를 추가할 수 있습니다. |







# 10.6. 앱 컨트롤 구성: 기기당 설치된 앱 컨트롤

앱 컨트롤 구성을 통해 앱을 기기 수준에서 허용 목록 또는 차단 목록으로 분류할 수 있습니다. 이미 설치된 앱은 표시되지 않으며 시작할 수 없습니다. 앱은 App Store에 계속 표시되지만 다운로드하거나 시작할 수 없습니다. 이 구성이 배포되는 기기는 모두 이 구성을 사용하고 모든 허용된 앱 정책 설정을 무시합니다. 이 구성은 대상 장치에서 동일한 애플리케이션을 참조하는 모든 앱 관련 정책을 대체합니다.

이 구성은 대상 장치에서 동일한 애플리케이션을 참조하는 모든 앱 관련 정책을 대체합니다. Windows 10 장치의 경우 장치 수준에서 제한이 발생하므로 구성은 앱 규칙을 적용하는 유일한 방법입니다.

앱 컨트롤 구성을 통해 다음을 만들 수 있습니다.

- **허용 목록:** 이 목록에 명시적으로 추가된 앱만 허용합니다. 기기에 다른 앱을 설치할 수 없게 됩니다.
- **차단 목록:** 특정 앱이 기기에 설치되지 않도록 합니다.

**지원되는 기기**

앱 컨트롤 구성을 사용하여 다음 기기에서 앱을 차단 목록 또는 허용 목록으로 등록할 수 있습니다.

- 회사 소유 기기의 Android 작업 프로필
- iOS 9.3+ 감독 전용
- tvOS 11+
- Windows

## 앱 컨트롤 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+추가**를 클릭하고
3. 결과로 표시되는 **구성 선택** 필드에 **앱 컨트롤**을 입력한 다음, **앱 컨트롤** 구성을 선택합니다.
4. 구성 이름 및 설명을 입력합니다.
5. OS를 선택한 다음 OS에 적용하는 섹션 아래의 '계속'을 선택합니다.

### 회사 소유 기기의 Android 작업 프로필

사용자는 허용 목록 또는 차단 목록 그룹에 최대 50개의 애플리케이션 ID를 추가할 수 있습니다.

**절차**

1. **개인 앱용 허용 목록 생성** 또는 **개인 앱용 차단 목록 생성**을 선택하여 적절한 애플리케이션 목록을 허용 목록 또는 차단 목록에 추가합니다.
2. 애플리케이션 ID(com.example.com)를 입력하고 추가를 클릭합니다.
3. **다음**을 클릭한 후 배포 옵션을 선택합니다.
4. **완료**를 클릭하세요.

### iOS 9.3 감독 기기

**절차**

1. 만들고자 하는 허용 목록 또는 차단 목록을 선택합니다.

2. **앱 추가**를 클릭합니다.
3. 다음 탭 중 하나 또는 두 개 모두를 클릭하여 허용 목록 또는 차단 목록에 등록할 앱을 선택합니다.
    - **조회로 추가**를 클릭하여 App Store 또는 App Catalog에서 앱을 검색하고 선택합니다.
    - **수동 추가**를 클릭하여 Apple System 앱에 대해서만 Apple 번들 ID("com.apple"로 시작)를 입력하여 앱을 선택합니다.

**허용 목록** 또는 **차단 목록** 탭을 클릭하여 허용 목록 또는 차단 목록에 등록할 앱 목록을 검토합니다.

5. (선택 사항) **모든 웹클립 포함** 옵션을 선택합니다.
6. **다음**을 클릭한 다음 배포 방법을 선택합니다.
7. **완료**를 클릭하세요.

## Windows 기기

**절차**

1. **허용됨** 또는 **허용되지 않음**을 선택하여 허용 목록 또는 차단 목록에 등록할 해당 애플리케이션 목록을 추가합니다.
2. **규칙 정의** 섹션에서, 목록에서 **앱 유형**을 선택합니다.
3. **앱 식별자** 상자에 식별자 이름을 입력하여 앱을 검색합니다. **앱 조회** 링크를 사용하여 새 대화상자를 열어 Windows 전용 앱 식별자를 검색할 수도 있습니다.
4. (선택 사항) **앱 설명** 상자에 앱에 관한 몇 가지 설명을 입력합니다.
5. **+추가** 링크를 사용하여 규칙 정의를 추가하고 허용 목록이나 차단 목록에 앱을 등록합니다.
6. **다음**을 클릭한 후 배포 옵션을 선택합니다.
7. **완료**를 클릭하세요.

# 10.7. 앱 알림 구성

사용자가 선택한 앱에서 알림을 수신할 방법을 선택합니다.

**적용 대상:** iOS 9.3+ 감독 기기.

## 앱 알림 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 알림을 입력한 다음, **앱 알림** 구성을 클릭합니다. 앱 알림 구성 설정 페이지가 나타납니다.
4. 구성의 이름 및 설명을 입력합니다.
5. AppStore에서 조회하거나 번들 ID를 입력하여 수동으로 앱을 추가합니다.
6. 앱 알림 설정을 적용할 앱을 선택합니다.
7. 알림 설정을 구성합니다. 다음은 선택할 수 있는 알림입니다.
    - 알림 허용
        - 알림 센터에 표시
        - 소리
        - 배지 앱 아이콘
        - 잠금 화면에 표시
        - (iOS 12.0+ 감독) CarPlay를 사용할 때 중요 경고 표시
        - (iOS 12.0+ 감독) 중요 경고 활성화 허용("해 금지"무시)
    - 경고 스타일 잠금 해제
        - 배너
        - 모달 경고
        - 없음
    - (iOS 12.0+ 감독) 그룹화 유형
        - 자동
        - 앱별로
        - 끄기
    - (iOS 14.0+) 알림 미리 보기 유형 - 기기 알림 메시지 미리 보기에 표시할 미리 보기 유형을 선택합니다.
        - 사용자 제어 - 기기에서 앱의 사용자 설정에 따라 메시지 미리 보기를 표시합니다.
        - 항상 - 메시지 미리 보기를 표시합니다.
        - 잠금 해제 시 - 기기가 잠금 해제된 경우에만 메시지 미리 보기를 표시합니다.
        - 안 함 - 앱이 알림에 메시지 미리 보기를 표시하지 않도록 합니다.
8. **다음**을 클릭해 배포 설정을 구성합니다.
9. **완료**를 클릭합니다.

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.8. 구성 내보내기

구성 파일을 내보내어 지원 팀에 전송하면 진단 보조 자료로 사용할 수 있습니다. 한 개의 구성 파일을Yaml 형식 파일로 보낼 수도 있고, 모든 구성을 .zip 파일로 내보낼 수 있습니다.

**절차**

## 구성 내보내기

내보낼 구성에 따라 구성 페이지의 다른 영역에서 파일을 내보낼 수 있습니다.

### 모든 구성 내보내기:

1. **구성**으로 이동합니다.
2. 확인란을 선택하여 특정 구성을 선택합니다.
3. **작업** > **선택한 구성 및 상세 정보 내보내기**를 클릭합니다. 모든 구성을 내보내려면 **상세 정보가 있는 모든 구성 내보내기**를 선택합니다.
   YAML 파일 집합은 .ZIP 파일에 포함되어 있습니다. 보고서에는 선택한 공간의 모든 기존 구성 상세 정보가 포함됩니다.

### 사용자 지정 구성 내보내기:

1. **구성**으로 이동합니다.
2. **+추가**를 클릭하여 구성을 선택합니다.
3. 단계에 따라 구성을 사용자 지정합니다.
4. **다음**을 클릭하세요.
5. 배포 수준을 선택합니다.
6. **완료**를 클릭하세요.
7. **구성** 페이지의 목록에서 방금 만든 구성을 선택합니다.
8. **작업** 풀다운 메뉴와 **내보내기를 차례로 클릭합니다.**

---

를 클릭합니다. 해당 구성의 이름을 가진 파일과 timestamp_yyyymmdd.yaml 파일이 기기에 다운로드됩니다.

### 기존 구성 내보내기:

1. **구성**으로 이동합니다.
2. 기존 구성을 선택합니다.
3. **작업** 풀다운 메뉴를 클릭하고 **내보내기**를 클릭합니다.
   해당 구성의 이름을 가진 파일과 timestamp _yyyymmdd.yaml 파일이 다운로드됩니다.

# 10.9. 구성 우선순위 지정

구성을 위해 여러 기기 그룹을 선택하면 특정 기기에 같은 유형의 여러 구성이 할당될 수도 있습니다. 같은 유형의 구성들이 동일한 기기에 적용되면, 정해진 우선순위에 따라 어떤 구성을 적용할지 결정합니다. 우선순위가 높을수록 번호가 낮아집니다. 예를 들어, 우선순위 번호가 1001인 구성은 1002인 구성보다 우선순위가 높습니다. 우선순위 번호는 시스템에서 자동으로 할당됩니다.

> Wi-Fi 우선순위는 기기에 적용될 수 없으며, 우선순위에서 예외가 됩니다.

이 옵션은 해당 페이지에 2개 이상의 동일한 유형 구성이 들어있는 경우에 한해, 그리고 드롭다운 목록에서 하나의 공간이 선택된 경우에 지원됩니다. 구성 우선순위를 변경할 수 있습니다.

**절차**

1. **구성**으로 이동합니다.
2. 아무 구성도 선택하지 않은 상태에서 **작업 > 우선순위 지정 구성**을 선택하십시오.
   **작업**이 표시되지 않으면, 우선 순위 지정이 필요한 여러 구성 유형이 존재하지 않는 것입니다.
3. 화살표로 구성 항목을 이동해 우선순위를 변경하되, 최우선순위 구성이 최상위에 위치하도록 합니다.

> 잠금 아이콘은 구성 내의 모든 기기 배포 설정을 편집해야 구성의 우선순위를 변경할 수 있음을 의미합니다.

**저장**을 클릭합니다.

> 최대 400개 구성까지 우선순위를 지정할 수 있습니다.

구성 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.

- DeviceManagement
- DeviceReadOnly

# 10.10. 구성 관리하기

이 섹션에는 다음 주제가 포함됩니다.

- AppConnect 구성
- 보안 구성
- 사용자 리소스 구성
- 엔터프라이즈 네트워크 액세스 구성
- 휴대폰
- 기타 구성

# 10.10.1. 구성 유형

이 섹션에는 다음 주제가 포함됩니다.

- 구성 검색
- 보안
- 사용자 리소스
- 엔터프라이즈 네트워크 액세스
- 휴대폰 네트워크
- 추가 구성
- 기기 동기화 구성

## 구성 검색

**구성 선택** 페이지에서 검색 및 필터 기능을 사용하여 적용할 구성을 찾습니다.

**절차**

1. **구성** 선택.
2. 나열된 구성 중 하나를 선택하거나 **+추가** 버튼을 클릭합니다.
3. **구성 선택** 페이지가 표시됩니다.
   나열된 구성 중 하나를 선택하거나
   - 검색 상자에서 구성 이름을 입력합니다.
   - 검색 상자의 오른쪽에 있는 필터 아이콘을 클릭하면 플랫폼과 호환되는 구성 유형이 표시됩니다.

구성 버튼을 클릭하여 구성 설정 옵션에 액세스합니다.

자세한 내용은 구성 작업을 참조하십시오.

## 보안

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| Android Enterprise | Android Enterprise 옵션을 지정합니다. | Android Enterprise | 라이센스 |
| AppConnect 장치 | 장치에서 보안 설정 AppConnect가 활성화된 앱을 지정합니다. | • 안드로이드<br>• iOS | 업그레이드 |
| Apple 암호 키 증명 | Apple 기기에서 특정 패스키에 대해 WebAuthn 엔터프라이즈 인증을 활성화합니다. | • macOS | |
| Entra ID(Azure 테넌트) | MDM용 Ivanti Neurons와 Entra ID를 연결하면 관리형 기기의 기기 규정 준수 상태를 사용하여 조건부로 Microsoft 365 앱에 액세스할 수 있습니다. | • iOS<br>• Android | • 새 고객: Secure UEM Premium<br>• 기존 고객: Platinum |
| 인증서 | 서버와의 신뢰 구축 | • Android<br>• iOS<br>• macOS<br>• watchOS<br>• visionOS<br>• tvOS | |
| 인증서 투명성 | 장치 프로필에만 표시할 수 있는 인증서 투명도 적용을 컨트롤합니다. | • iOS<br>• macOS<br>• tvOS<br>• watchOS<br>• visionOS | |
| 장치 로깅 | 장치에서 네트워크 및 보안 로그와 같은 추가 로그를 검색합니다. | • Android Enterprise | |
| 디스크 관리 구성 | 외부 및 네트워크 저장소의 관리 정책을 정의합니다. | • 감독 대상인 macOS 15.0+ | |
| Android 암호화 | 사용자에게 암호화를 시작하라는 메시지가 표시됩니다. | 안드로이드 | |
| 암호화된 DNS | VPN을 구성할 필요 없이 보안을 강화할 수 있습니다. | • iOS<br>• macOS<br>• visionOS | 업그레이드 |

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| 외부 인텔리전스 설정 | 외부 인텔리전스 통합을 허용합니다. | • iOS 26.4+<br>• macOS 26.4+<br>• visionOS 26.4+ | |
| 모바일 위협 방어 | 기기, 네트워크, 애플리케이션에 영향을 미치는 모바일 위협 및 취약성으로부터 관리 기기를 보호합니다. | • Android<br>• iOS | |
| 위협 방어 로컬 작업 | 위협 방어가 활성화된 클라이언트에서 위협을 감지하면 지원되는 Android 기기에서 수행할 로컬 작업을 정의하는 기기 구성을 만들어 배포합니다. | 안드로이드 | |
| FileVault 2 | 볼륨 컨텐츠에서 전체 XTS-AES 128 디스크 암호화를 수행할 수 있는 기능을 제공합니다. | macOS | 업그레이드 |
| FileVault 복구 키 | FileVault 복구 키를 회사 서버로 리디렉션하기 위한 설정을 확인합니다. | macOS | 업그레이드 |
| ID 인증서 | • 서버에 기기 인증<br>• 네트워크 리소스에 기기 인증 | • 안드로이드<br>• iOS<br>• macOS<br>• watchOS<br>• visionOS | |
| iOS 활성화 잠금 | 감독 기기에서 Apple 활성화 잠금 기능을 활성화합니다. | iOS | 라이센스 |
| iOS 커스텀 구성 | 다른 앱에서 생성된 iOS 구성 프로필을 배포합니다. | iOS | |
| iOS 제한 | • 기기 기능 잠금을 설정합니다.<br>• 기기 기능을 활성화합니다. | • iOS<br>• watchOS<br>• visionOS | |
| 인텔리전스 설정 | Apple Intelligence 통합을 허용합니다. | • iOS 26.4+<br>• macOS 26.4+<br>• visionOS 26.4+ | |
| 회의실 디스플레이 | Apple TV에서 회의실 디스플레이 모드를 켭니다. | tvOS 10.2+ | |
| 키보드 설정 | 기기에서 키보드 동작, 입력 옵션 및 관련 사용자 경험 설정을 관리하는 방식 | • iOS 26.4+ | |

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
|---|---|---|---|
| | 을 제어할 수 있습니다. | • macOS 26.4+ | |
| 잠금 및 키오스크: Android | • 기기 기능 잠금을 설정합니다.<br>• 기기 기능을 재활성화합니다.<br>• 키오스크 기능을 적용합니다. | 안드로이드 | |
| 잠금 및 키오스크: Android Enterprise | • Android 엔터프라이즈 기기에서 제한되는 기능 및 앱을 정의합니다.<br>• 키오스크 기능을 적용합니다. | Android 5.0 + | |
| 잠금 및 키오스크: Samsung Knox 표준 | • Samsung KNOX Standard 기기에서 제한되는 기능 및 앱을 정의합니다.<br>• 키오스크 기능을 적용합니다. | Samsung Knox | |
| 로컬 관리자 암호 솔루션 구성 | 관리자가 관리형 macOS 기기에서 일정한 간격으로 로컬 관리자 비밀번호를 자동으로 재생성할 수 있도록 합니다 | macOS | |
| macOS 방화벽 | macOS 기기에서 보안 기본 설정 작업창에서 액세스할 수 있는 애플리케이션 방화벽 설정을 관리합니다.<br>관리자는 Ping 명령으로 발견할 수 없는 기기를 지정하여 은폐 모드를 활성화할 수 있습니다. | macOS 10.12+ | 업그레이드 |
| macOS 제한 | macOS 장치에서 활성화할 제한을 확인합니다. | macOS | 업그레이드 |
| macOS 앱스토어 제한 사항 | macOS AppStore에서 어떤 제한을 활성화할지 정의합니다. | macOS | 업그레이드 |
| macOS 디스크 굽기 제한 사항 | macOS의 디스크 굽기 제한을 관리합니다. | macOS | 업그레이드 |
| macOS용 Mobile@Work | macOS용 Mobile@Work에 대한 실행 규칙을 생성 및 배포합니다. | macOS | 업그레이드 |
| macOS 스크립트용 Mobile@Work | macOS용 Mobile@Work에 배포할 스크립트를 만듭니다. | macOS | 업그레이드 |
| ID 환경설정 | 동일 프로필에 포함된 ID 페이로드를 참조하는 사용자의 키체인에서 ID 환경설정 항목을 확인합니다. | macOS | 업그레이드 |
| 인증서 환경설정 | 동일 프로필에 포함된 인증서 페이로드를 참조하는 사용자의 키체인에서 인증서 환경설정 항목을 확인합니다. | • macOS | 업그레이드 |
| 허용된 미디어 컨트롤 | 실제 미디어 마운팅, 마운팅 해제 및 추출 옵션을 구성합니다. | macOS | 업그레이드 |
| macOS 파인더 설정 | macOS의 Finder 앱 설정을 관리합니다. | macOS | 업그레이드 |

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
|---|---|---|---|
| macOS 커널 확장 정책 | 사용자 승인 커널 확장 로드를 위한 제한 및 설정 제어 | macOS | 업그레이드 |
| 활성 디렉토리(macOS) | 인증 및 보안을 위해 활성 디렉토리(AD)를 사용하는 소프트웨어 서비스에 액세스하려면 macOS 기기를 AD 도메인에 바인딩하도록 고급 옵션을 구성합니다. | macOS | 업그레이드 |
| Office 365 자동 계정 생성(macOS) | 사용자 정보 및 옵션을 구성하여 모든 Microsoft Office 365 애플리케이션에 대한 최초 구성을 설정합니다. | macOS | 업그레이드 |
| Apple 앱 카탈로그 | 웹 클립을 통한 Apple 앱 카탈로그의 액세스를 관리합니다. | • iOS<br>• macOS | |
| 관리되는 도메인 | 신뢰할 수 있는 이메일과 웹 도메인을 지정합니다. | • iOS 8+<br>• visionOS 1.1+ | 라이센스 |
| 암호 | • 암호를 필수 항목으로 설정합니다.<br>• 암호 길이 및 내용을 지정합니다.<br>• 암호 요건을 변경합니다. | • 안드로이드<br>• iOS<br>• macOS<br>• watchOS | |
| 개인정보 보호 환경 설정(macOS) | 시스템 서비스, 시스템 파일, 시스템 리소스에 대한 액세스를 허용할 애플리케이션을 구성합니다. | macOS | 업그레이드 |
| 인증 | 클라우드 서비스 및/또는 데스크톱 로그인에 대해 암호 없는 인증을 제공합니다. | • macOS<br>• Windows | |
| 개인정보 보호 설정 | 위치 데이터의 수집 여부를 지정합니다. | • iOS<br>• 안드로이드<br>• Windows | |
| 클라이언트 개인정보 보호방침 정보 | Go 클라이언트의 사용자에게 개인 정보 정책을 표시합니다. | • 안드로이드<br>• 안드로이드 엔터프라이즈<br>• iOS | |
| Ivanti Go Client 설정 | 문제를 해결하고 최고 품질의 서비스를 유지하기 위한 기기 및 이용 정보를 포함한 데이터를 MixPanel을 통해 수집하도록 구성합니다. | • iOS<br>• macOS | |

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| Safari 확장 설정 구성 | 다양한 도메인의 Safari 브라우저 확장 프로그램을 관리합니다. | • 감독 대상 iOS 18.0+<br>• 감독 대상인 macOS 15.0+ | |
| Siri 설정 | 기기가 Siri 설정에 액세스하고 이를 사용하는 방식을 관리할 수 있습니다. | • iOS 26.4+<br>• macOS 26.4+<br>• watchOS 26.4+<br>• visionOS 26.4+ | |
| 서비스 구성 파일 설정 | 관리자는 다양한 시스템 서비스용 구성 파일을 중앙에서 관리하고 배포할 수 있습니다. | macOS | |
| 소프트웨어 업데이트 | OS 업데이트 규칙을 만들고 배포합니다. | • iOS<br>• macOS<br>• Windows | |
| 소프트웨어 업데이트 설정 구성 | 소프트웨어 업데이트 적용 설정을 만들고 업데이트합니다. | • 감독 대상 iOS 18.0+<br>• 감독 대상인 macOS 15.0+ | |
| 시간 서버 | 기기가 사용자 지정 시간 서버에 연결되도록 허용합니다. | macOS | 업그레이드 |
| 웹 컨텐츠 필터 | Safari 컨텐츠를 제어합니다. | • 감독 중인 iOS 7<br>• visionOS 1.1+ | Silver |
| Windows_Firewall | Windows 방화벽 구성에는 다양한 방화벽 제한 사항이 있습니다. 관리자가 적용한 방화벽 제한 사항에 따라 방화벽 상태는 Windows 장치의 보안 기본 설정 창에서 다음 방화벽 상태 중 하나가 됩니다.<br>• 방화벽이 켜져 있고 모니터링 중입니다.<br>• 방화벽이 비활성화되었습니다.<br>• 방화벽이 일부 네트워크를 모니터링하지 않거나 일부 규칙이 해제되었습니다.<br>• 방화벽이 일시적으로 모든 네트워크를 모니터링하지 않습니다.<br>• 해당 없음 | Windows 10+ | |

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| Windows 정보 보호 | 기업 데이터를 보호하기 위한 WIP(Windows 정보 보호) 설정을 정의합니다. | Windows 10+ | 업그레이드 |
| Windows 제한 | Windows 10 이상 장치에서 사용할 수 있는 기능을 결정합니다. | Windows 10+ | |
| Windows AI Management 구성 | Windows AI 설정 및 구성을 관리할 수 있습니다. | Windows 10+ | |

## 사용자 리소스

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| CalDAV | • CalDAV 서버(Google Calendar 등) 접속 설정 | • iOS<br>• visionOS | |
| CardDAV | • CardDAV 서버(Google Contacts 등) 접속 설정 | • iOS<br>• visionOS | |
| 이메일 | • POP/IMAP 이메일(Gmail 등) 접속 설정 | • iOS<br>• visionOS | |
| 구성을 | • Android 및 iOS 모바일 기기용 ActiveSync 기반 이메일 (Outlook 등) 접속 설정<br>• macOS 기기용 EWS(Exchange Web Services) 기반 이메일 설정<br>• 장치에 동기화할 범위 지정<br>• 이메일 보안 설정 | • 안드로이드<br>• iOS<br>• macOS<br>• visionOS | • Sentry를 통한 Exchange는 macOS에서 지원되지 않습니다.<br>• 동기화 이전 일 수 이메일 플래그는 macOS에 적용할 수 없습니다. |
| Google | • iOS 9.3.2+ 기기를 Google 계정에 연결하는 Google 계정 구성 생성<br>• Google 시스템에서 연락처에 전화를 거는 데 사용하는 앱 지정 | • iOS<br>• visionOS | |
| 글꼴 | • 정상적인 문서 실행에 필요한 규격 외 폰트 설치 | • iOS | |
| 구독한 달력 | • 인터넷 달력 구독 설정 | • iOS<br>• visionOS | |
| 웹 클립 | • 웹 페이지에 단축키(아이콘) 표시 | • iOS<br>• macOS | |
| 콘텐츠 캐싱 | • App Store 소프트웨어의 로컬 사본을 활성화하기 위해 콘텐츠 캐싱 서비스를 제공하며,<br>• 더 빠른 소프트웨어와 앱 다운로드를 위해 연결된 클라이언트를 활성화합니다. | • macOS | |

## 엔터프라이즈 네트워크 액세스

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| AirPlay | • 미디어 디스플레이 대체 기기 접속 설정 | • iOS<br>• macOS | Silver |
| AirPrint | • 무선 프린팅 설정 | • iOS<br>• macOS | Silver |
| Always On VPN | • 사용자 인증 없이 VPN 서버로 접속 설정 | • Android 7.0+<br>• iOS 8+ | • Android 엔터프라이즈 Gold<br>• iOS: Silver |
| 기본 앱 런타임 권한은 | • Android 엔터프라이즈 기기에 배포된 앱의 런타임 권한 구성을 설정합니다. | • Android API 23 이상을 대상으로 개발되었고 Android 엔터프라이즈 기기에서 Android 6.0 이상을 실행하는 앱. | |
| 교육 | • Apple Education 페이로드 및 리더 및 구성원용 Classroom 앱을 구성할 수 있습니다. | • supervised iOS 9.3+ | 업그레이드 |
| 전역 프록시 | • 장치에서 프록시 서버로 HTTP 트래픽이 전달되도록 설정 | • 관리 상태인 iOS 7<br>• 감독 모드 tvOS | Silver |
| LDAP | • 회사 디렉토리 접속 설정 | • iOS<br>• visionOS | |
| 터널 | • Tunnel을 사용하여 클라이언트와 Sentry 간의 앱별 VPN 연결 정의 | • iOS 7+<br>• macOS 10.13+<br>• Windows 10+<br>• 안드로이드 | |
| Bridge | • IT 부서에서 MobileIron Bridge를 활용하여 중요한 기능을 포기하지 않고도 UEM에서 Windows 작업을 현대화할 수 있음 | • Windows 10+ 데스크톱 | Bridge 라이선스 |
| macOS 서버 | • 구성된 계정 유형과 관련 설정으로 macOS Server 계정 정의. 사용자가 서버에서 파일 공유를 활성화하도록 허용합니다. | • iOS 10+ | |
| 퍼앱 VPN | • 특정 앱과 VPN 서버 간 연결 설정 | • iOS<br>• watchOS<br>• visionOS<br>• tvOS | Silver |
| 네트워크 릴레이 구 | • 네트워크 릴레이 설정을 정의하는 구성 추가 | • iOS<br>• macOS | |

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| 성 | | • visionOS | |
| Single Sign-On | • 관리 상태인 특정 앱의 Single Sign-On 설정 | • iOS<br>• macOS<br>• visionOS | |
| 다중 사용자 보안 로그인 | • 웹 클립으로 다중 사용자 보안 로그인을 설정합니다. | • iOS | |
| VPN | • VPN 서버 접속 설정 | • 안드로이드<br>• Windows<br>• iOS<br>• macOS<br>• visionOS<br>• tvOS | |
| 요청 시 VPN | • 도메인, 호스트 이름 등 기반 VPN 서버 접속 설정 | • iOS | |
| Wi-Fi | • 무선 네트워크 접속 설정 | • 안드로이드<br>• Windows<br>• iOS<br>• macOS<br>• watchOS<br>• visionOS<br>• tvOS | |

## 휴대폰 네트워크

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| APN | • 장치의 휴대폰 엑세스 지점 이름 설정 | • iOS | |
| 휴대폰 | • 휴대폰 네트워크 접속 설정 | • iOS<br>• watchOS | |
| 셀룰러 사설 네트워크 구성 | • 사설 네트워크 배포에 대한 장치 정보를 제공하는 페이로드 설정 | • iOS | |
| iOS 텔레콤 사전 설정 구성 | • 로밍 제한 기본값 설정<br>• 개인 핫스팟 제한 기본값 설정 | • iOS | |

## 추가 구성

| 유형 | 상세 기능 | 적용 기기 | 이 라이센스 필요 |
| --- | --- | --- | --- |
| Apple TV | • Apple TV 언어 및 로캘 설정 | • 관리 상태인 iOS 7 | Silver |
| 기본 장치 이름 | • 변수를 사용하여 기본 장치 이름을 지정합니다. | • 관리 상태인 iOS 8 | Silver |
| iOS 배경화면 | • 홈 화면 및 잠금 화면 배경화면 설치 | • 관리 상태인 iOS 7 | Silver |
| macOS 배경 화면 | • 기기에 홈 화면 및 잠금 화면의 배경화면을 설치합니다. 배경화면은 사용자가 변경할 수 있지만 배포 후에는 기기에서 삭제할 수 없습니다. | | 필요하지 않음 |
| 마이그레이션 지원 설정 | 기기 설정 또는 마이그레이션 중에 관리자와 사용자가 데이터, 앱 및 설정을 전송할 수 있도록 지원합니다. | • macOS 26.4+ | |
| 단일 앱 모드 | • 장치에서의 특정 앱 사용 제한 설정 | • 관리 상태인 iOS 7<br>• 감독 모드 tvOS | Silver |
| 관련 도메인 구성 | • 관련 도메인 구성은 연결된 도메인에 앱을 매핑하는 사전입니다.<br>• 관련 도메인은 Extensible AppSSO, 유니버설 링크, 암호 자동 완성과 같은 기능과 함께 사용할 수 있습니다. | • macOS 10.15+ | Gold |
| 화면 공유 호스트 설정 구성 | • 관리형 기기 전반에서 관리자가 macOS 화면 공유 기능을 안전하게 제어할 수 있도록 합니다. | • macOS 14+ | |

## 기기 동기화 구성

기기 동기화 설정은 기기에서 모니터할 수 있는 리스트 데이터 지점을 제공합니다. 기기 동기화 구성을 편집할 수 없습니다. 선택된 설정 목록을 볼 수 있습니다.

**절차**

1. **구성**으로 이동합니다.
2. **장치 동기화 구성**을 클릭합니다. **장치 동기화 구성** 페이지의 세부 정보 탭과 확인한 항목의 목록이 표시됩니다.

| 판독값 사이의 설정 | 시간(단위: 분) |
|---|---|
| 인증서 목록 | |
| 장치 정보 | 60 |
| 설치된 앱 리스트 | 60 |
| 관리되는 앱 리스트 | 60 |
| 프로필 리스트 | 60 |
| 프로비저닝 프로필 리스트 | 60 |
| 제한 | 60 |
| 보안 정보 | 60 |
| **iOS 9+** | |
| 업데이트 확인 | 1440 |

## 관련 주제

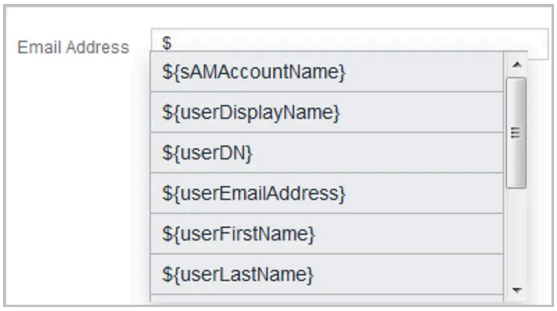
- 변수
- 구성 작업

# 10.10.2. 변수

특정 설정 필드의 변수를 현재 사용자의 전용 값으로 설정할 수 있습니다. 변수를 지원하는 모든 필드에 $를 입력하면 지원되는 변수 목록이 표시됩니다. 이 섹션에는 다음 주제가 포함됩니다.

## 지원되는 사용자 계정 변수

### 사용자 변수

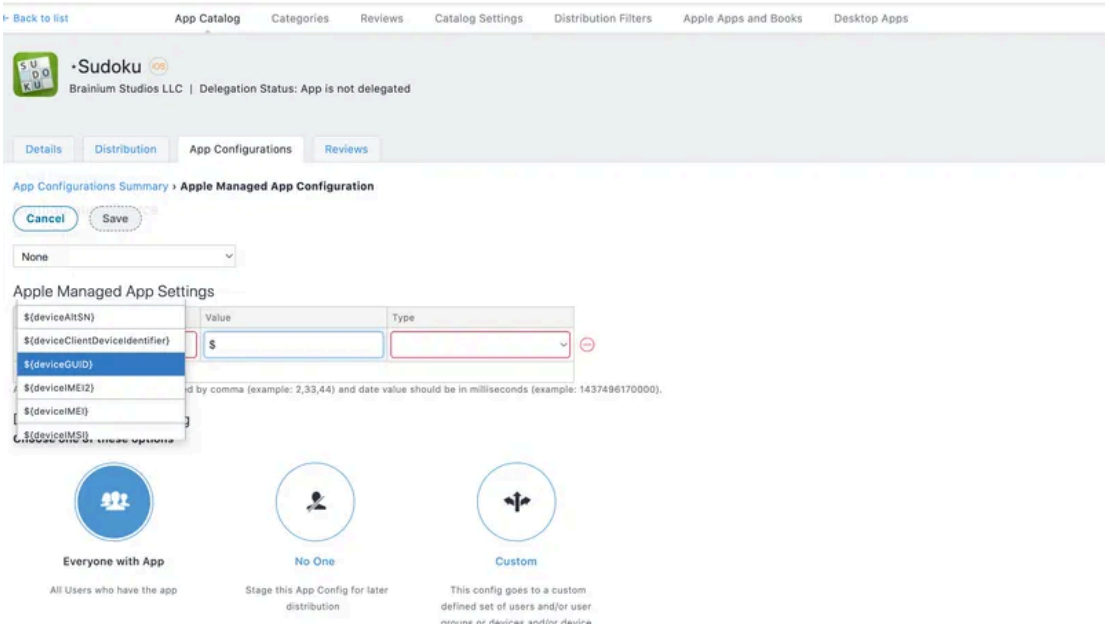


| 변수 키 | 값 설명 |
| --- | --- |
| $ | 부서 속성(Entra ID 필요) |
| $ | 전자 데이터 교환-개인 식별자 |
| $ | 사용자의 관리되는 Apple ID |
| $ | sAMAccountName 속성(Active Directory 필요) |
| $ | 고유 이름에서 추출된 공통 이름(CN) 속성(LDAP 필요) |
| $ | 표시 이름 |
| $ | 고유 이름(LDAP 필요) |
| $ | 이메일 주소의 도메인 부분('@' 이후 부분) |
| $> | 이메일 주소의 로컬 부분('@' 이전 부분) |
| $ | 이메일 주소 |
| $ | 이름 |
| $ | 성 |
| $ | 로캘 |
| $ | 고유 이름에서 추출된 조직 단위(OU) 속성(LDAP 필요) |
| $ | Kerberos 영역 정보(Active Directory 필요) |
| $ | 로그인 ID의 도메인 부분('@' 이후 부분) |
| $ | 로그인 ID의 로컬 부분('@' 이전 부분) |
| $ | 로그인 ID(이메일 주소 형식) |
| $ | userPrincipalName 속성(Active Directory 필요) |

## 지원되는 기기 변수

기기 변수를 사용하여 모바일 기기에 대한 정보를 지정합니다.

### 기기 변수


Back to list
App Catalog
Categories
Reviews
Catalog Settings
Distribution Filters
Apple Apps and Books
Desktop Apps
·Sudoku
Brainium Studios LLC | Delegation Status: App is not delegated
Details
Distribution
App Configurations
Reviews
App Configurations Summary › Apple Managed App Configuration
Cancel
Save
None
Apple Managed App Settings
${deviceAltSN}
${deviceClientDeviceIdentifier}
${deviceGUID}
${deviceIMEI2}
${deviceIMEI}
${deviceMSI}
Value
Type
$
d by comma (example: 2,33,44) and date value should be in milliseconds (example: 1437496170000).
Everyone with App
All Users who have the app
No One
Stage this App Config for later distribution
Custom
This config goes to a custom defined set of users and/or user

| 변수 키 | 값 설명 |
| --- | --- |
| $ | 클라이언트가 마지막으로 체크인된 날짜(가장 최근 체크인 - MDM 또는 클라이언트) |
| $ | 대체 일련 번호 |
| $ | 클라이언트 애플리케이션에 사용하는 식별자 |
| $ | 전역 고유 기기 식별자 |
| $ | ICCID |
| $ | IMEI2 |
| $ | IMEI |
| $ | IMSI |
| $ | 기기가 마지막으로 체크인된 날짜(가장 최근 체크인 - MDM 또는 클라이언트) |
| $ | 내부 기기 식별자 |
| $ | MDM에 사용되는 식별자 |
| $ | MEID |
| $ | 모델 |
| $ | 기기 이름 |
| $ | 기기 전화 번호 |
| $ | 클러스터 고유 기기 식별자 |
| $ | 일련 번호 |
| $ | iOS UDID |
| $ | Wi-Fi MAC 주소 |

## 이메일 템플릿 변수

| 변수 키 | 값 설명 |
| --- | --- |
| $ | 이메일 본문 |
| $ | 이메일 제목 |

## 타임스탬프 변수

| 변수 키 | 값 설명 |
| --- | --- |
| $ | 현재 타임스탬프(Epoch 이후의 밀리초) |

## 정책 템플릿 변수

| 변수 키 | 값 설명 |
| --- | --- |
| $ | 정책 이름 위반 |
| $ | 메시지를 보낸 후 수행할 다음 계층화된 규정 준수 작업(대기 및 사용 중지와 다름) |
| $ | 기기가 비준수 상태였던 기간(일) |
| $ | 정책 위반이 처음 트리거된 타임스탬프(UTC DD-MM-YYYY 형식) |
| $ | 규칙 정의(지금 표시되는 쿼리 문자열) |

**관련 주제:**

- 속성

# 10.10.3. AppConnect 구성

이 섹션에는 다음 주제가 포함됩니다.

- AppConnect 개요
- AppConnect 암호

# 10.10.3.1. AppConnect 개요

AppConnect는 iOS 및 Android 기기의 데이터를 보호하기 위해 앱을 컨테이너에 담는 기능입니다. 각 AppConnect 지원 앱은 데이터가 암호화된 보안 컨테이너가 되고 무단 액세스 및 제거로부터 보호됩니다. 각 사용자에게는 여러 개의 비즈니스 앱이 있기 때문에 각 앱 컨테이너도 다른 보안 앱 컨테이너와 연결됩니다. 이 연결을 통해 AppConnect 지원 앱은 데이터를 문서처럼 공유할 수 있습니다. MDM용 Ivanti Neurons는 정책을 사용하여 AppConnect 지원 앱을 관리합니다.

AppConnect 및 AppConnect 앱을 구성하고 배포하는 방법에 대한 자세한 내용은 *MDM용 Ivanti Neurons에 관한 AppConnect 가이드*를 참조하십시오.

## 보안 앱 상태

**기기 > 기기** 페이지에서 기기를 클릭하여 **개요** 페이지로 이동합니다. 사용자는 이 페이지에서 다음 정보와 함께 보안 앱의 상태를 확인할 수 있습니다.

- **보안 앱 상태** - AppConnect의 활성화 여부를 나타냅니다.
- **보안 앱 암호화 상태** - AppConnect 암호의 활성화 여부를 나타냅니다.
- **보안 앱 암호화 모드** - 암호화 모드(예: AES 256)를 나타냅니다.

다음과 같은 필드도 사용할 수 있습니다.

- 사용자가 기기를 검색/필터링하려고 할 때 표시되는 기기 항목 범위를 좁히는 필터로 사용할 수 있습니다.
- 동적으로 관리되는 기기 그룹을 생성하는 동안 규칙으로 사용할 수 있습니다.
- 정의된 규칙에 따라 배포될 기기 앱을 구체화하는 배포 필터로 사용할 수 있습니다.

관리자는 기기 상세 정보 페이지의 **구성** 탭에서 각 보안 앱의 컨테이너 정책과 구성 상태(설치됨, 적용됨, 전송됨, 설치 보류 중)를 검토할 수 있습니다.

# 10.10.3.2. AppConnect 암호

이 섹션에는 다음 주제가 포함됩니다.

- 암호 변경/재설정
- iOS 기기용 보안 앱 암호 재설정을 위한 일회용 PIN 생성

AppConnect 암호(보안 앱 암호)를 요구할 수 있습니다. AppConnect 암호로 한 번 로그인하면 기기 사용자는 모든 보안 앱에 액세스할 수 있습니다. 관리자 포털에서 AppConnect 암호 규칙을 구성합니다. AppConnect 암호는 기기의 잠금을 해제하는 암호와는 다릅니다.

## 암호 변경/재설정

사용자는 Android 기기의 경우 Secure Apps Manager 앱에서, iOS 앱의 경우 Go에서(AppConnect 구성에서 허용된 경우) 보안 앱 암호를 변경 또는 재설정할 수 있습니다. iOS 기기:

**절차**

1. iOS용 Go 앱을 엽니다.
2. **보안 앱**을 클릭합니다.
3. **인증**을 클릭합니다.
4. **보안 앱 암호 변경**을 클릭하고 지침에 따라 암호를 변경/재설정합니다.

Android 기기:

1. Secure Apps Manager 앱을 엽니다.
2. 옵션 메뉴에서 **암호 변경**을 클릭합니다.
3. **비밀번호 분실**을 클릭하여 암호를 재설정합니다.

## iOS 기기용 보안 앱 암호 재설정을 위한 일회용 PIN 생성

관리자는 iOS 기기 사용자가 보안 앱(AppConnect) 암호를 잊어버렸을 경우 재설정을 허용하도록 MDM용 Ivanti Neurons를 구성할 수 있습니다. 이 옵션을 구성하면 사용자 이름 및 비밀번호를 사용하여 MDM용 Ivanti Neurons에 등록한 기기 사용자는 iOS용 Go 3.1.0 또는 지원되는 최신 버전에서 자격 증명을 입력하고 인증을 받은 다음, 보안 앱 암호를 재설정할 수 있습니다. 하지만 비밀번호와 PIN을 잊어버린 기기 사용자의 경우 인증을 받으려면 다른 방법이 필요합니다.

**절차**

1. MDM용 Ivanti Neurons에서 관리자는 기본 iOS AppConnect 구성(또는 다른 iOS AppConnect 구성)에 있는 **보안 앱 암호** 옵션을 켭니다.
2. 사용자는 자체 서비스 사용자 포털에서 **보안 앱 암호 재설정**을 클릭하고 지침을 따름으로써 특정 iOS 기기에 대한 일회용 PIN을 생성합니다. 1회용 PIN은 30분 동안 유효합니다.
3. 기기에 있는 iOS용 Go에서 사용자는 잊어버린 보안 앱 암호 재설정 지침을 따릅니다.
4. 사용자 자격 증명 메시지가 표시될 때 사용자는 사용자 이름과 정규 암호 대신 1회용 PIN을 입력합니다.
5. 사용자가 보안 앱 암호를 재설정합니다.

# 10.10.4. 보안 구성

이 섹션에는 다음 주제가 포함됩니다.

- Android Enterprise
- Android Enterprise 기본 구성 편집
- Android Enterprise 설정
- Android 작업 챌린지
- 인증서 구성
- 인증서 투명성
- 인증서 해지 확인 구성
- 자치 단일 앱 모드 구성 만들기
- DNS 프록시 구성 생성
- 장치 로깅 구성
- 디스크 관리 구성
- Android 암호화
- 암호화된 DNS
- 외부 인텔리전스 설정
- 위협 방어
- FileVault 2
- FileVault 복구 키
- FileVault 옵션 구성
- ID 인증서
- Apple 활성화 잠금 구성
- iOS 사용자 지정 구성
- 인텔리전스 설정
- 키보드 설정
- iOS 제한
- 회의실 디스플레이
- 잠금 및 키오스크: Android 기기 관리 모드
- Android용 키오스크 모드 설정
- Android 공유 기기 키오스크 설정
- 잠금 및 키오스크: Android Enterprise
- 잠금 및 키오스크: Samsung Knox 표준
- macOS 방화벽
- macOS 제한
- macOS 앱스토어 제한 사항
- macOS 디스크 굽기 제한 사항

- 허용된 미디어 제어(더 이상 사용되지 않음)
- macOS 파인더 설정
- macOS 커널 확장 정책
- macOS용 Mobile@Work
- macOS 소프트웨어 업데이트 규칙 구성
- 인증서 환경설정
- 활성 디렉토리(macOS)
- ID 환경설정
- Office 365 자동 계정 생성(macOS)
- 인증
- Apple 앱 카탈로그
- 관리되는 도메인
- 암호 구성
- 개인정보 보호 환경 설정(macOS)
- Ivanti Go Client 설정
- 개인정보 보호 설정
- 클라이언트 개인정보 보호방침 정보
- Safari 확장 설정 구성
- 소프트웨어 업데이트
- 소프트웨어 업데이트 설정 구성
- 보안 기본 설정 구성
- Siri 설정
- 시간 서버
- 웹 컨텐츠 필터
- Windows 방화벽
- Windows 정보 보호
- Windows 제한
- Windows 데스크톱 제한
- Windows 10 데스크톱 설정
- Windows Hello for Business 구성
- Windows AI Management 구성
- Play Integrity(구 SafetyNet Attestation)
- 고급 Android 암호 및 잠금 화면
- 엔드포인트용 Microsoft Defender
- 인증서 기반 인증

# 10.10.4.1. Android Enterprise

**라이센스**: Silver

Android Enterprise 구성은 지원 장치에서 활성화한 **Android Enterprise** 옵션을 정의합니다. 다양한 기기 그룹에 대체 구성을 생성하거나 기본 구성을 편집할 수 있습니다. Android Enterprise를 지원하는 기기 목록은 **Android** 공식 페이지를 참조하십시오.

## Android Enterprise 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 화면 캡처 비활성화 (Android 5.0 +) | 기기에서 기본 화면 캡처 기능을 사용하지 못하도록 하려면 선택합니다. |
| 앱 제어 비활성화(Android 5.0 이상) | 사용자가 설정 또는 시작 관리자에서 앱을 수정하지 못하도록 하려면 선택합니다. |
| 구성 자격 증명 허용 안 함 (Android 5.0 이상) | 사용자가 사용자 자격 증명을 설정할 수 없도록 하려면 이 옵션을 선택합니다. |
| 프로필 간 복사/붙여넣기 허용 안 함(Android 5.0 이상) | 기기가 다른 Android Enterprise 작업 프로필에 복사 및 붙여넣지 못하게 하려면 선택합니다. |
| 계정 수정 허용 안 함 (Android 5.0 이상) | 사용자가 계정을 추가 및 제거하지 못하도록 하려면 선택합니다. |
| 플래시 불빛 금지 (Android 5.0 +) | 사용자가 NFC를 사용하여 앱 데이터를 전송하지 못하도록 하려면 선택합니다. |
| 위치 공유 허용 안 함 (Android 5.0 이상) | 웹사이트 및 앱에서 기기 사용자가 기기 위치를 공유하지 못하도록 하려면 이 옵션을 선택합니다. |
| 입력 방법 제한(Android 5.0 이상) | 허용된 패키지 이름 목록을 지정하여 입력 방법을 제한하려면 선택합니다. 허용된 패키지가 없으면 시스템 입력 방법만 허용됩니다. 입력 방법은 작업 앱에만 국한되지 않고 전체 기기에 적용됩니다. |
| 접근성 서비스 제한 (Android 5.0 +) | 허용된 패키지 이름 목록을 지정하여 입력 방법을 제한하려면 선택합니다. 허용된 패키지가 없으면 시스템 접근성 서비스만 허용됩니다. 입력 방법은 작업 앱에만 국한되지 않고 전체 기기에 적용됩니다. |
| 발신자 ID 비활성화(Android 6.0 +) | 전화 수신 시 직장 프로필의 발신자 ID 정보를 기기에 표시할지 여부를 설정합니다. |

**관련 주제**

- **Android Enterprise 설정**

# 10.10.4.2. Apple 암호 키 증명

Passkey Attestation 구성을 사용하여 특정 암호 키에 대해 WebAuthn 엔터프라이즈 증명을 허용하도록 기기를 구성합니다.

사용자가 Passkey를 이용해 인증하고 기기를 등록하면, Apple Passkey Attestation 구성은 엔터프라이즈 관리 자격 증명(Enterprise Managed Credential)을 사용하여 회사 인증서로 Passkey를 검증합니다. 지원되는 자격 증명에는 SCEP, ACME, ID 자격 증명이 포함됩니다.

암호 키 증명은 다음을 지원합니다.

- 지원되는 최소 운영 체제 버전: macOS 14
- 지원되는 등록 방법: 기기 등록
- 관리형 Apple 계정은 암호 키 동기화를 제어해야 합니다.
- ABM의 액세스 관리와 함께 사용할 수 있습니다.

> Mac에서 Passkey 페이로드 오류.

암호 키 구성을 생성할 때, 먼저 ID 인증서 구성을 생성하고 암호 키 구성에 이를 연결해야 합니다. 또한, 보안 암호 키 증명 구성 섹션에 다음 세부 정보를 입력합니다.

| 필드 | 설명 |
| --- | --- |
| 이름 | 암호 키 이름 |
| 설명 | 구성에 대한 모든 정보 |
| 증명 ID 자산 참조<br>• 증명 ID 키는 추출 가능 | 암호 키 구성에 연결하기 위해 생성한 자산 참조 ID를 입력합니다.<br>ID 키의 추출 가능 여부를 확인하려면 이 옵션을 선택합니다. |
| 신뢰 당사자 | 인증된 도메인의 세부 정보를 입력합니다. |

# 10.10.4.3. 앱 개인정보 보호 기본값

**앱 개인정보 보호 기본값**을 사용하여 감독 모드 기기의 앱에 대한 기본 개인정보 보호 권한을 정의합니다. 관리자는 앱에서 사용하는 개인정보 보호 구성요소를 식별하고, 구성에 앱과 해당 구성요소를 나열하며, 개인정보 보호 기본값을 설정할 수 있습니다. 사용자가 앱을 실행하면 앱은 구성된 개인정보 보호 기본값을 확인하고 사용자에게 권한 부여를 요청하는 메시지를 표시하는 한편, 사용자가 권한 부여를 나중으로 미루거나 기기 설정에서 권한을 관리할 수 있도록 합니다.

**적용 대상**:

- iOS 27.0+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- iPad 27.0+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- macOS 27.0+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **앱 개인정보 보호 기본값** 구성을 검색하여 선택합니다.
3. **이름** 필드에 이 구성을 식별하는 이름을 입력합니다.
4. **설명** 필드에 이 구성의 목적을 명확히 설명하는 내용을 입력합니다.
5. **구성 설정** 창에서 **조회하여 추가**를 선택합니다.
6. 다음 옵션 중 하나를 선택하여 **앱 개인정보 보호 기본값**을 구성할 앱 이름을 입력합니다.

- iOS Store
- 앱 카탈로그
- visionOS Store
- OS X Store(macOS)

> 여러 앱을 선택할 수 있습니다.

7. (선택 사항) 앱을 선택하려면 **수동으로 추가**를 선택합니다.
8. (선택 사항) 앱의 **패키지 이름**을 입력합니다.
9. (선택 사항) **앱 추가**를 클릭합니다.
10. **앱 보기**를 선택합니다.

**앱 보기** 창에 선택한 모든 애플리케이션이 나열됩니다.

11. 각 애플리케이션에서 **기본값 추가**를 클릭하여 앱 개인정보 보호 기본값을 개별적으로 구성합니다.

**기본값 추가** 창이 나타납니다.

12. **기본값** 및 **제한**을 선택합니다.

| 기본값 | 제한 설정 |
| --- | --- |
| Camera | 다음 옵션 중 하나를 선택합니다.<br>• 허용<br>• 없음 |
| Bluetooth | 다음 옵션 중 하나를 선택합니다.<br>• 허용<br>• 없음 |
| 접근성 | 다음 옵션 중 하나를 선택합니다.<br>• 허용<br>• 없음 |
| 받아쓰기 | 다음 옵션 중 하나를 선택합니다.<br>• 허용<br>• 없음 |
| 마이크 | 다음 옵션 중 하나를 선택합니다.<br>• 허용<br>• 없음 |
| 위치 | 다음 옵션 중 하나를 선택합니다.<br>• 사용하는 동안<br>• 없음<br>• 항상 |
| 위치 정확도 | 다음 옵션 중 하나를 선택합니다.<br>• 대략적<br>• 정확한<br>• 없음 |
| 로컬 네트워크 | 다음 옵션 중 하나를 선택합니다.<br>• 허용<br>• 없음 |
| 조직 정당성 | **조직 정당성** 메시지에는 조직 이름, 앱 이름, 관리자가 제공한 정당성 및 권장 개인정보 보호 기본값이 있는 각 구성요소의 상세 정보가 표시될 수 있습니다.<br>사용자가 **허용**을 선택하면 시스템에서 권장 개인정보 보호 기본값을 적용합니다. 사용자가 **나중에**를 선택하면 앱이 사용자 기기의 지정된 구성요소에 액세스할 때 동의 메시지가 표시됩니다. |

13. **저장**을 클릭하세요.
14. **다음**을 클릭해 배포 설정을 구성합니다.
15. **앱 개인정보 보호 기본값** 구성을 설정하려면 배포 옵션 중 하나를 선택합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
16. **완료**를 클릭하세요.

# 10.10.4.4. Android Enterprise 기본 구성 편집

전역 관리자는 사용자 지정 공간에서 공간 관리자가 아래 Android Enterprise 기본 구성의 배포를 편집하도록 허용할 수 있습니다.

- Android Enterprise: 회사 소유 장치의 작업 프로필(Android for Work)
- Android Enterprise: 회사 관리형 장치(Android for Work)
- Android Enterprise: 작업 프로필이 있는 관리형 장치
- Android enterprise: AOSP

## 위 구성에 대한 배포 편집

**절차**

1. 구성 탭에서 편집할 구성을 선택합니다.
2. 편집 아이콘을 클릭합니다.
3. **다음**을 클릭합니다.
4. 다음 배포 수준 중에서 선택하여 배포 페이지에서 편집하고 구성합니다.
    - **모든 장치**: 다음 옵션 중 하나를 선택하여 호환되는 모든 장치에 구성을 배포합니다.
        1. 다른 공간에 적용하지 않음
        2. 다른 공간의 장치에 적용합니다.
    - **장치 없음**(기본값)
    - **사용자 정의**: 다음 옵션 중 하나를 선택하여 모든 호환 장치 또는 사용자에게 구성을 배포합니다.
        1. **사용자/사용자 그룹**: 사용자 또는 사용자 그룹 옆의 확인란을 선택합니다. 또는 사용자 또는 사용자 그룹을 입력하고 검색해도 됩니다.
        2. **장치/장치 그룹**: 장치 또는 장치 그룹 옆의 확인란을 선택합니다. 또는 장치 또는 장치 그룹을 입력하고 검색해도 됩니다.
        **배포 요약**에서 다음 옵션 중 하나를 선택하여 공간 전체에 구성을 활성화 또는 비활성화합니다.
            - 다른 공간에 적용하지 마십시오.
            - 다른 공간의 장치에 적용합니다.

            > **다른 공간의 장치에 적용**을 선택하면 **공간 관리자가 배포를 편집하도록 허용** 확인란이 표시되고, 위임된 공간 관리자가 특정 공간을 위한 배포를 편집할 수 있습니다.

> 배포 옵션을 편집하는 경우 "**Android Enterprise 장치 모드 구성 배포를 변경하면 기존 장치에서 해당 구성이 제거될 경우 장치를 사용할 수 없게 되거나 지워질 수 있음을 이해합니다.**" 확인란을 선택해야 합니다.

5. **완료**를 클릭하세요.

이 구성이 공간에 적용되면 공간 관리자는 사용자 지정 공간에서 배포 아이콘을 클릭하여 배포를 편집할 수 있습니다.

# 10.10.4.5. Android Enterprise 설정

이 섹션에는 다음 주제가 포함됩니다.


- 지원되는 기기
- Android Enterprise와 MDM용 Ivanti Neurons 연결
- Android 엔터프라이즈 자격 증명 가져오기
- Android 엔터프라이즈 MDM 토큰을 MDM용 Ivanti Neurons에 추가
- MDM용 Ivanti Neurons 및 Google 간 사용자 동기화
- Active Directory/LDAP 사용자
- 로컬 사용자
- 지원되는 기기에 Android Enterprise 배포
- 등록 기기 폐기
- 기기 배포
- 배포 확인
- Android Enterprise 앱 배포
- 비즈니스 앱 구성


**라이센스: Silver**

Android Enterprise는 모바일 관리자가 다음을 수행할 수 있도록 Google에서 제공하는 프로그램입니다.

- 업무와 개인 데이터 분리
- 엔터프라이즈 앱 보안 및 관리
- 시스템 앱 제어(카메라와 갤러리 등)
- Android Enterprise 컨테이너에서 중앙 집중식으로 앱 프로비저닝 및 구성
- 데이터 손실 방지(화면 캡처)

MDM용 Ivanti Neurons을(를) Android Enterprise를 관리하는 UEM 서버로 구성할 수 있습니다. Android Enterprise에는 Android 3.0 이상이 필요합니다. Android Enterprise에는 기기 소유자 및 관리 프로필(직원 소유)의 두 가지 지원 구성이 있습니다.

## 지원되는 기기

MDM용 Ivanti Neurons 은(는) 현재 Android 5.0을 실행하고 제조업체에서 Android Enterprise를 활성화한 기기에서만 Android Enterprise를 지원합니다. Android 5.0을 실행하는 기기의 키오스크 모드에는 Android Enterprise가 필요합니다.

**필수 조건**

아직 Google에 도메인을 등록하지 않은 경우 먼저 Google 웹 사이트에서 해당 프로그램에 등록해야 합니다.

https://admin.google.com.

이 과정은 다음 단계를 거칩니다.

- 도메인 요청(사용자 이메일 주소의 도메인과 일치해야 함)
- 토큰 받기
- JSON 클라이언트 ID 다운로드

MDM용 Ivanti Neurons에서 Android Enterprise를 설정하는 경우는 두 항목이 모두 필요합니다.

이 과정을 거치면 요청한 도메인 소유를 확인하기 위한 안내 사항이 담긴 이메일이 전송됩니다.

**회사에서 회사용 Google Apps에 가입하기 위한 도메인 이름을 사용하고 있는 경우** Android 엔터프라이즈 활성화에 대한 정보는 https://support.google.com/work/android/answer/6174062를 참조하십시오.

## Android Enterprise와 MDM용 Ivanti Neurons 연결

Android Enterprise에 가입했으면 MDM용 Ivanti Neurons을(를) UEM 서버로 설정합니다.

## Android 엔터프라이즈 자격 증명 가져오기

**절차**

1. **관리자 > Android Enterprise**로 이동합니다.
2. **Google 개발자 콘솔**을 클릭합니다.
3. 처음 표시된 링크를 클릭하여 Google 개발자 콘솔로 이동합니다.
4. 드롭다운 메뉴에서**프로젝트 생성**을 선택합니다.
5. 프로젝트 이름을 입력합니다.
6. 서비스 이용약관에 동의합니다.
7. **생성**을 클릭합니다.
8. **API**를 클릭합니다.
9. **API**를 선택합니다.
10. 검색 필드에서 **emm**을 입력하여 Google Play EMM을 찾습니다.
11. **Google Play EMM API** 링크를 클릭합니다.
12. **API 활성화**를 클릭합니다.
13. **자격 증명**을 클릭합니다.
14. **서비스 계정**을 선택합니다.
15. **생성**을 클릭하여 JSON 파일을 저장합니다.

## Android 엔터프라이즈 MDM 토큰을 MDM용 Ivanti Neurons에 추가

**절차**

1. https://admin.google.com에 로그인합니다.
2. **보안**을 클릭합니다.
3. Android Enterprise 설정이 표시되지 않으면 **더 보기**를 클릭합니다.
4. **Android Enterprise 설정**을 선택합니다.
5. **엔터프라이즈 이동성 관리 공급자 관리**에서 MDM 토큰을 복사합니다.
6. MDM용 Ivanti Neurons 포털로 돌아갑니다.
7. **완료**를 클릭합니다.
8. 박스 2에서 방금 복사한 MDM 토큰을 붙여넣습니다.
9. **도메인** 필드에 Google로 요청한 도메인을 입력합니다.

10. **파일 선택**을 클릭하고 다운로드한 JSON 파일을 업로드합니다.
11. **연결**을 클릭합니다.
    연결에 성공하면 **Google에 연결됨** 메시지가 표시됩니다.
12. 박스 3에서 **승인**을 클릭하여 Google 사용자 데이터에 대한 MDM용 Ivanti Neurons 액세스 권한을 제공하고자 한다는 것을 표시합니다.
13. **수락**을 클릭합니다.
    MDM용 Ivanti Neurons 포털에 **사용자에 연결됨** 메시지가 표시됩니다.

## MDM용 Ivanti Neurons 및 Google 간 사용자 동기화

MDM용 Ivanti NeuronsMDM용 Ivanti Neurons에서 관리하는 Android 사용자에게 Android Enterprise를 배포하기 전에 각 사용자는 Google 관리 포털에 해당 레코드가 있어야 합니다. MDM용 Ivanti Neurons 및 Google 관리 포털 간 사용자 정보를 동기화하는 데 필요한 단계는 조직의 디렉토리 서비스(AD/LDAP)와의 통합을 설정했는지 여부에 따라 달라집니다.

## Active Directory/LDAP 사용자

MDM용 Ivanti Neurons와(과)의 AD/LDAP 통합을 설정한 경우, Google 앱 디렉토리 동기화를 사용하여 Google 관리 포털과 AD/LDAP 통합을 설정해야 합니다. 자세한 내용은 https://support.google.com/a/answer/106368?hl=en을 참조하십시오.

## 로컬 사용자

MDM용 Ivanti Neurons에서 로컬 사용자만 생성하고 디렉토리 서비스와 통합하지 않으려는 경우, 다음 단계를 완료하여 해당 사용자를 Google 관리 포털과 동기화합니다.

**절차**

1. Google 관리 포털(https://admin.google.com)에 로그인합니다.
2. **사용자**를 클릭합니다.
3. 오른쪽 하단 모서리에 있는 **사용자 추가** 또는 **여러 사용자 추가** 아이콘을 클릭합니다.
4. Android Enterprise를 사용할 각 MDM용 Ivanti Neurons 사용자에 대해 MDM용 Ivanti Neurons 사용자와 동일한 사용자 이름 및 이메일 주소를 가진 Google 사용자를 추가합니다.
5. Google 관리 포털에 방금 추가한 각 MDM용 Ivanti Neurons 사용자의 MDM용 Ivanti Neurons 포털에서:
   a. 사용자 탭에서 사용자 이름 링크를 클릭하여 사용자의 세부 정보를 표시합니다.
   b. **Google 사용자 디렉토리와 사용자 동기화**를 선택합니다.
   c. **Google 사용자 디렉토리와 동기화**를 클릭합니다.
   d. Google 상태가 활성화됨으로 표시되는지 확인합니다.

## 지원되는 기기에 Android Enterprise 배포

Android Enterprise를 배포하려면 다음 두 가지 구성이 필요합니다.

- Android Enterprise: 회사 소유 기기의 작업 프로필 구성은 Android Enterprise를 활성화합니다.
- 잠금 및 키오스크 구성은 적용할 Android Enterprise 제한 사항을 정의합니다.

## 등록 기기 폐기

BYOD 시나리오에서 회사 소유 기기의 작업 관리자에서 Android Enterprise 작업 프로필로 이동할 때 기기를 사용 중지하고 재등록할 필요가 없습니다. 기기 지우기 또는 폐기는 기기 관리자에서 기기 소유자 모드로 이동하는 데에만 필요합니다.

사용 중지 작업에 장치 소유자/향상된 프로필 소유자/회사 소유의 개인 사용 모드로 등록된 장치를 선택하면 "조직 소유의 장치에는 사용 중지 명령이 지원되지 않습니다"라는 팝업이 화면에 표시됩니다.

## 기기 배포

**절차**

1. MDM용 Ivanti Neurons 포털에서 **구성**으로 이동합니다.
2. **Android Enterprise: 작업 프로필**을 클릭합니다.
3. **편집**을 클릭합니다.
4. **다음**을 클릭하세요.
5. **모든 기기** 또는 **사용자 지정**을 선택합니다.
6. **사용자 지정**을 선택한 경우 회사용 Android 설정을 수신해야 하는 기기 그룹을 검색하여 선택합니다.
7. **완료**를 클릭합니다.
8. **목록으로 돌아가기**(좌측 상단 모서리)를 클릭합니다.
9. **+추가**를 클릭합니다.
10. **잠금 및 키오스크: Android Enterprise**를 클릭합니다.
11. **이름** 필드에 구성을 식별할 수 있는 텍스트를 입력합니다.
12. **잠금 유형 선택**에서 **작업 프로필**을 선택합니다.
13. 대상 기기에 적용할 잠금 설정을 선택합니다.
14. **다음**을 클릭하세요.
15. **모든 기기** 또는 **사용자 지정**을 선택합니다.
16. 사용자 지정을 선택한 경우 Android Enterprise 설정을 수신해야 하는 기기 그룹을 검색하여 선택합니다.
17. **완료**를 클릭합니다.

> 배포된 이후에는 생성된 프로필을 변경할 수 없습니다. 대신 새 Android Enterprise 구성을 만들고 배포해야 합니다.

## 배포 확인

다음과 같은 방법으로 Android Enterprise의 배포를 확인할 수 있습니다.

- **사용자 > 사용자**에서 사용자 항목을 찾은 다음 **Google 상태**가 **활성화됨**인지 확인합니다.
- **기기 > 기기**에서 기기에 대한 링크를 클릭한 다음 **Android Enterprise**의 상태가 **활성화됨**으로 설정되어 있는지 확인합니다.

사용자에 대한 **Google 상태**가 **활성화됨**으로 표시되어야 합니다. 활성화되어 있지 않으면 사용자가 기기를 등록할 수 없습니다.

> GSuite를 구독하지 않은 기업의 경우 관리형 Google Play 계정 메서드를 사용하면 사용자의 Android Enterprise 등록을 허용할 수 있습니다. Android Enterprise가 관리형 Google Play 계정으로 등록된 경우, Android Enterprise 기기가 등록될 때까지 사용자가 **Google 상태: 활성화됨**으로 표시되지 않습니다. 관리되는 Google Play 계정에 대한 자세한 내용은 관리되는 Google Play 계정을 참조하십시오.

## Android Enterprise 앱 배포

Android Enterprise용으로 개발된 모든 앱에는 MDM용 Ivanti Neurons을(를) 통해 구성할 수 있는 옵션이 포함될 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 포털에서 **앱 > 앱 카탈로그**로 이동합니다.
2. Google Play Store에서 앱을 찾습니다.
3. 앱 입력을 클릭합니다.
4. Android Enterprise 사용자를 대신하여 권한을 수락합니다.
5. **다음**을 클릭하세요.
6. 배포 방법을 선택하세요.
7. **고급 옵션 및 앱 구성**을 확장합니다.
8. 다음 지침을 사용하여 옵션을 완료합니다.
9. **다음**을 클릭하세요.

| 설정 | 설명 |
| --- | --- |
| **기기에 설치** | 이 옵션을 선택하면 등록 후에 바로 설치를 시작합니다. 기기가 Samsung Knox 기기이며 아래의 자동 설치 옵션이 선택된 경우를 제외하고 사용자에게 앱 설치를 확인하라는 메시지가 표시됩니다. |
| **최종 사용자 앱 카탈로그에서 앱 표시 안 함** | 사용자가 기기에 있는 앱 카탈로그에서 앱을 보기를 원하지 않는 경우 이 옵션을 선택합니다. |
| **Samsung Knox 기기에 자동 설치** | 사용자에게 Samsung Knox 기기 설치를 확인하라는 메시지를 표시하지 않으려면 이 옵션을 선택합니다. |
| **앱 설치 우선순위 설정** | Android Enterprise 앱의 경우 다른 앱보다 특정 앱의 다운로드를 우선할 수 있습니다. 예를 들어 중요하지 않은 다른 앱 전에 Tunnel 및 이메일 앱의 다운로드 우선순위를 지정할 수 있습니다. 사용 가능한 우선순위 레벨 옵션은 다음과 같습니다.<br>• **높음**<br>• 중간(기본적으로 선택됨)<br>• **낮음**<br>이 설정은 인하우스, 공개, 비공개, 웹 앱에 적용할 수 있습니다. 인하우스 앱은 클라이언트를 통해 설치되며 공개 및 비공개 앱은 Google을 통해 설치됩니다. 앱 우선순위는 동일한 채널을 통해 설치된 앱에만 적용됩니다. |
| **Wi-Fi에 연결된 경우에만 설치** | 이 옵션을 선택하면 기기가 Wi-Fi에 연결된 경우에만 앱을 설치합니다. |
| **충전 중에만 설치** | 이 옵션을 선택하면 기기 충전이 진행 중인 경우에만 앱을 설치합니다. |
| **유휴 상태일 경우에만 설치** | 이 옵션을 선택하면 기기가 유휴 상태(사용자가 적극적으로 사용하지 않음)일 경우에만 앱을 설치합니다. |
| **설치 시 자동 시작** | 이 옵션을 선택하면 설치 후 앱을 자동으로 시작합니다. 이 기능은 버전 업데이트용이 아니라 기기에 앱이 새로 설치되었을 경우에만 사용 가능합니다. |

10. 프로모션 방법을 선택하세요.
11. **완료**를 클릭하세요.

## 비즈니스 앱 구성

Android Enterprise 앱은 다음 앱을 비롯한 앱 카탈로그의 비즈니스 앱에서 사용할 수 있습니다.

- **Divide Productivity**
- 이메일+
- Tunnel
- Gmail

# 10.10.4.6. Android Enterprise: 업무 관리형 기기 비 GMS (AOSP) 모드

MDM용 Ivanti Neurons는 업무 관리형 기기 비 GMS 모드(AOSP) 기기 소유자 등록을 지원하며 Google Mobile Services(GMS)는 필요하지 않습니다. 이것은 시스템 구성이며 관리자는 구성을 추가할 수 없습니다. 관리자는 이것을 배포 또는 배포 취소할 수 있습니다.

**절차**

1. 사용자 자격 증명으로 MDM용 Ivanti Neurons에 로그인합니다.
2. Android Enterprise용 검색 구성: 업무 관리형 기기 비 GMS 모드(AOSP).
3. 구성을 편집하여 적절한 기기 그룹에 배포합니다. 예: Android 기기.
4. **완료**를 클릭하세요.

# 10.10.4.7. Android 작업 챌린지

이 섹션에는 다음 주제가 포함됩니다.

- Android Work Challenge 구성 생성:
- 구성 설정

**라이센스**: Silver

Android 워크 챌린지 구성은 사용자가 Work Profile 데이터 및 앱에 액세스할 때 사용하는 안전한 비밀번호를 정의합니다. Android Enterprise 작업 프로필이 필요합니다.

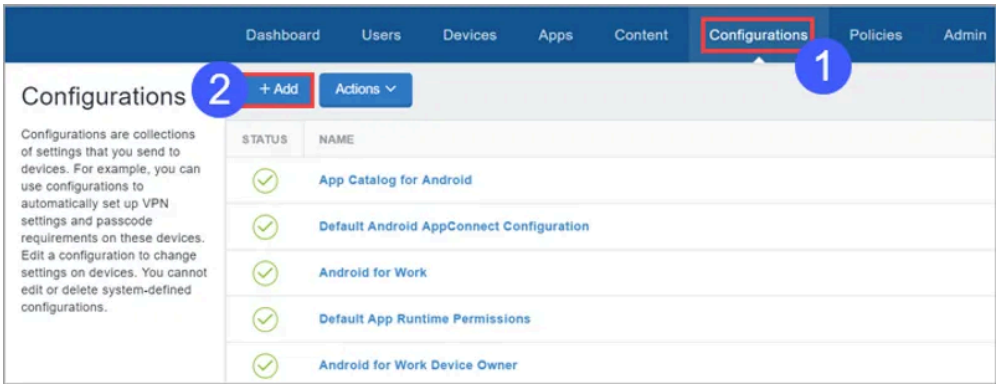
구현 노트:

- 관리자는 기기 비밀번호 정책과 업무 프로필 비밀번호 정책을 독립적으로 적용할 수 있습니다.
- Android 7.0 이전 버전의 기기는 해당 기능을 지원하지 않으므로 MDM용 Ivanti Neurons는 이러한 버전을 사용하는 클라이언트에게는 이 구성을 전송하지 않습니다.
  MDM용 Ivanti Neurons는 Android Enterprise 작업 프로필이 있는 기기에만 이 구성을 전송합니다.

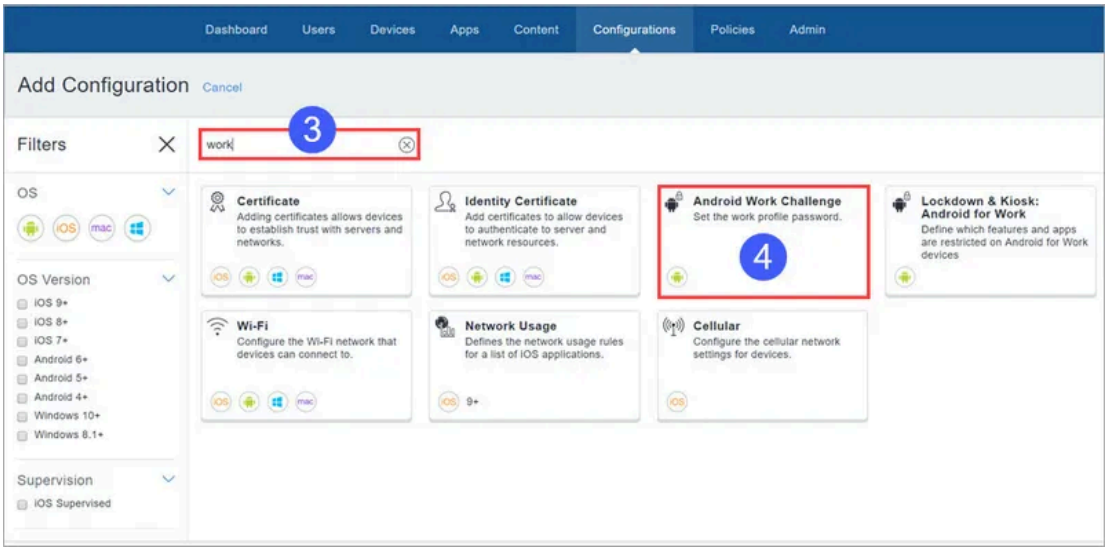
## Android Work Challenge 구성 생성:

**절차**

1. **구성**을 클릭합니다.

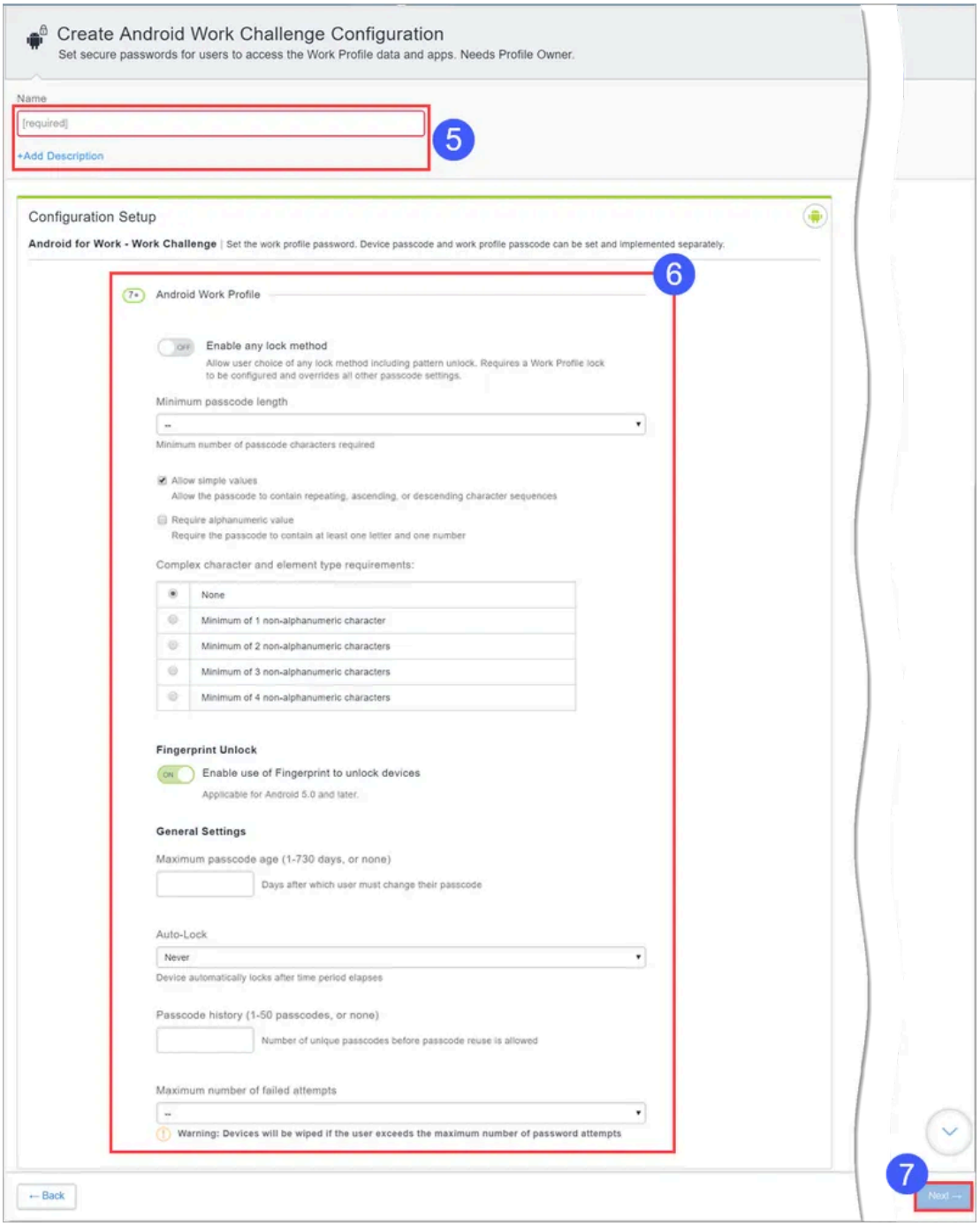



**+추가**를 클릭합니다.



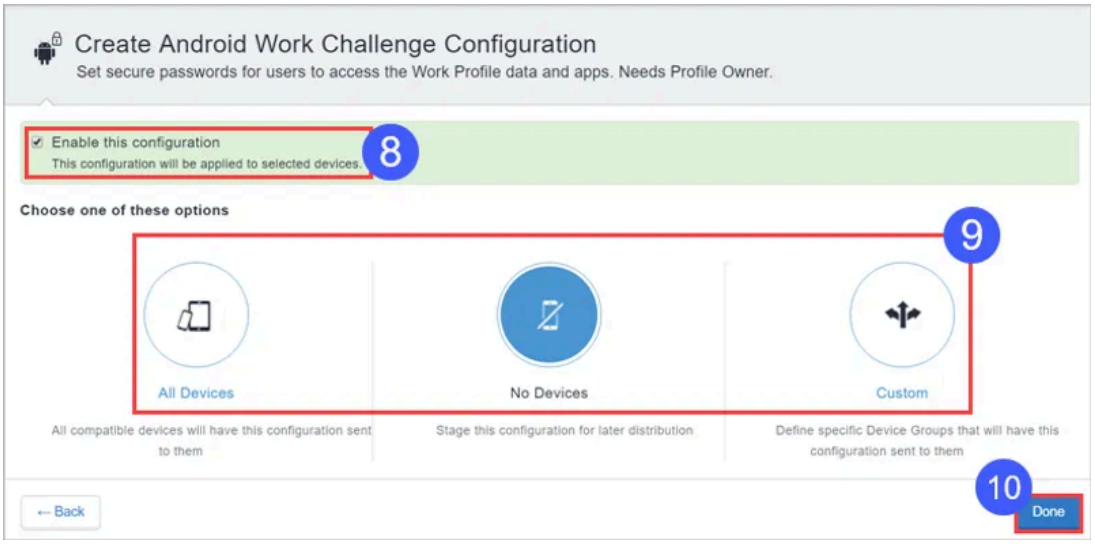

검색 필드에 “워크(work)”를 입력합니다.

4. **Android 작업 챌린지** 구성을 선택합니다.




구성 이름을 입력하고 필요한 경우 설명도 입력합니다.

6. 구성 설정 필드를 사용하여 구성을 생성합니다. 구성 설정을 참조하여 설정의 상세 정보를 지정합니다.
7. **다음 ->**을 클릭합니다.




원한다면 구성을 활성화합니다.

9. 모든 기기나 사용자 지정 기기에 배포 설정을 구성하거나 아무 기기에도 배포 설정을 구성하지 않을 수 있습니다.
10. **완료**를 클릭하세요.

## 구성 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 모든 잠금 방법 활성화 | 사용자가 패턴 잠금 해제 등의 모든 잠금 방식을 선택할 수 있습니다. 기타 모든 암호 설정을 재정의합니다. |
| 최소 암호 길이 | 최소 암호 길이를 4~16자까지 선택합니다. |
| 단일 값 허용 | 비밀번호에 반복, 내림차순, 오름차순 문자를 포함하려면 활성화합니다. |
| 영숫자 값 필요 | 비밀번호에 문자 1개와 숫자 1개 이상 포함되도록 하려면 활성화합니다. |
| 복잡한 문자 및 요소 유형 특징 | 복잡한 문자 및 요소 유형 요구 사항 구성 범위<br>• 없음<br>• 최소 1개의 영숫자 이외 문자<br>• 최소 2개의 영숫자 이외 문자<br>• 최소 3개의 영숫자 이외 문자<br>• 최소 4개의 영숫자 이외 문자 |
| 지문 잠금 해제 | 사용자가 지문으로 기기 잠금을 해제하게 하려면 활성화합니다. |
| 최대 암호 사용기간 | 최대 비밀번호 사용 기간을 0~730일까지 설정합니다. |
| 자동 잠금 | 기기가 자동으로 잠기는 시간을 선택합니다. 시간 범위는 0~15분입니다. |
| 암호 이력 | 비밀번호 재사용을 허용하기 전에 필요한 고유 비밀번호 개수를 지정합니다. 비밀번호 개수 범위는 0~50개입니다. |
| 최대 실패 시도 횟수 | 최대 실패 시도 횟수를 선택합니다. **경고: MDM용 Ivanti Neurons는 사용자가 비밀번호 입력 최대 횟수를 초과하면 기기를 삭제합니다!** |

# 10.10.4.8. 인증서 구성

인증서 구성으로 기기에 배포할 인증서를 확인할 수 있습니다. 인증서를 통해 장치는 서버 및 네트워크 리소스와의 신뢰를 구축합니다. 릴리스 76부터 v3 인증서만 지원됩니다.

관리자는 이제 스마트 카드 로그온과 사용자 지정 개체 ID(OID)에 대해 MDM용 Ivanti Neurons 인증서를 생성할 수 있습니다. 다음 인증 옵션에 대해 인증서를 생성할 수 있습니다.

- 클라이언트 인증 - 기본적으로 활성화됨
- IPSEC – 선택 사항, 관리자가 활성화할 수 있음
- 스마트 카드 로그온 - 선택 사항, 관리자가 활성화할 수 있음
- 사용자 지정 OID - 선택 사항, 관리자가 활성화할 수 있음

> 이 기능은 다음 인증 기관(CA)에 대해서만 해당됩니다.

- 로컬 인증 기관
- 중간 인증 기관
- 외부 인증 기관 - IPSEC, 스마트 카드 로그온 및 사용자 지정 OID를 지원하도록 NDES 서버에서 CA 템플릿의 애플리케이션 정책 구성
- 온프레미스 SCEP 인증 기관

## 구성 배포 중

MDM용 Ivanti Neurons 릴리스 91부터 전역 관리자는 모든 기기 및 사용자 지정 배포 옵션에서 인증서 구성을 편집할 권한을 공간 관리자에게 위임할 수 있습니다. 인증서 구성의 경우 '이 구성을 모든 공간에서 사용할 수 있도록 허용' 옵션을 선택적으로 선택할 수 있습니다. 이 옵션을 사용하면 인증서 구성을 모든 공간에서 사용할 수 있고 Exchange, Wifi, VPN, 앱별 VPN 및 기타 적용 가능한 구성에서 사용할 수 있습니다. 이 옵션은 연결된 구성의 일부로 인증서 구성이 기기(기본 공간이 아닌 공간)에 배포되고 개별 구성으로 배포되지 않는 데만 필요한 시나리오에서 사용할 수 있습니다.

**절차**

1. 이름 필드에 이름을 입력합니다.
2. 인증서 파일을 업로드합니다.
3. **다음**을 클릭하세요.
4. **이 구성 활성화** 옵션을 선택합니다.
5. 다음 배포 옵션 중 하나를 선택합니다.
    - **모든 기기**. 다음 옵션 중 하나를 선택합니다.
        - **다른 공간에 적용하지 마십시오**.
        - **다른 공간에 있는 기기에 적용하십시오**.
            - 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.
    - **배포 안 함**(기본값)
    - **사용자 지정**다음 옵션 중 하나를 선택합니다.
        - **다른 공간에 적용하지 마십시오**.
        - **다른 공간에 있는 기기에 적용하십시오**.

- 위임된 공간 관리자에게 특정 공간을 위한 배포를 편집할 수 있도록 허용하려면 **공간 관리자가 배포를 편집하도록 허용** 확인란을 선택합니다.

> 공간에 관계없이 모든 공간에 인증서 구성을 구성하고 모든 기기에 배포하고 다른 기기 공간의 모든 기기에 적용할 수 있습니다.

6. **완료**를 클릭합니다.

## 인증서 설정

관리자는 온프레미스 비 SCEP 인증 기관을 구성할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **관리자** > **인프라** > **인증서 관리** > **인증 기관**으로 이동합니다.
3. **+추가**를 클릭합니다. 다음 옵션이 열거됩니다.

- **MDM용 Ivanti Neurons에서 제공하는 로컬 인증 기관 생성**
- **자체 기존 CA로 MDM용 Ivanti Neurons의 로컬 CA에 로그인합니다**.
- **공개적으로 신뢰할 수 있는 Cloud 인증 기관에 연결**
- **온프레미스 SCEP 인증 기관 연결**
- **온프레미스 비 SCEP 인증 기관에 연결합니다**.

4. 다음 해당 필드를 완료합니다.
5. **완료**를 클릭하세요.

| 설정 항목 | 설정하기 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| URL | 관리자가 OpenTrust에서 확보해야 할 OpenTrust CA URL. |
| 비밀번호 | 인증서 인증을 위한 비밀번호를 입력합니다. |
| 인증서 인증 | OpenTrust/IDnomic이 제공하는 .p12 파일 형식을 수락합니다. |
| TLS CA 인증서 체인 | OpenTrust/IDnomic이 제공하는 PEM 파일 형식을 수락합니다. |

온프레미스 비 SCEP 인증 기관을 구성한 후 ID 인증서를 생성해야 합니다. 프로필 ID를 기반으로 모든 필수 필드를 작성하여 설정을 완료합니다.

> 다음 두 가지 이유로 SCEP CA 인증서 생성이 실패하고 2단계 시간 초과에 도달하면 알림이 생성됩니다.

1. 커넥터에 연결할 수 없습니다
2. CA 서버에 연결할 수 없습니다

# 10.10.4.9. 인증서 투명성

**적용 대상:** iOS 12.1.1, macOS 10.14.2, tvOS 12.1.1, watchOS 10.0 이상, visionOS 1.1 이상 및 지원되는 최신 버전.

장치 프로필에만 나타날 수 있도록 인증서 투명성 적용을 제어합니다. 여러 인증서를 포함하고 필요에 따라 도메인을 비활성화할 수 있습니다.

## 인증서 투명성 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **인증서**를 입력한 다음, **인증서 투명성** 구성을 클릭합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. **비활성화할 도메인**을 지정합니다. **+도메인 추가**를 클릭하여 하나 이상의 도메인을 추가합니다. 하위 도메인과 일치하도록 앞에 마침표를 사용할 수 있지만, 도메인 일치 규칙이 최상위 도메인 내의 모든 도메인과 일치해서는 안 됩니다. 예를 들어 ".example.com" 및 ".example.co.uk"는 허용되지만 ".com" 및 ".co.uk"는 허용되지 않습니다. 와일드카드 도메인은 지원되지 않습니다.
6. 알고리즘(SHA 256)을 선택하고 **인증서 해시**를 지정합니다. **+추가**를 클릭하여 한 개 이상의 인증서 해시를 추가합니다.
7. **다음**을 클릭해 배포 설정을 구성합니다.
8. **완료**를 클릭하세요.

subjectPublicKeyInfo 사전에서 해시 키로 지정한 데이터를 생성하려면 PEM 인코딩 인증서에 대해 다음 명령을 사용하십시오.

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

인증서가 DER로 인코딩된 경우에는 다음 명령을 사용하십시오.

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.4.10. 인증서 해지 확인 구성

이 구성을 통해 관리자가 기기에서 해지된 인증서 배열을 확인할 수 있습니다. 관리자는 구성을 통해 인증 기관(CA)에 연결된 모든 인증서에 대해 해지 확인을 활성화할 수 있는 해당 CA를 지정할 수 있습니다.

적용 대상: iOS 14.2 이상, visionOS 1.1 이상

**절차**

1. 구성 > +추가로 이동합니다.
2. 검색 필드에 인증서를 입력한 다음, 인증서 해지 확인 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. 알고리즘을 SHA 256으로 선택하고 루트 인증서의 해시를 입력합니다.

> 해시에서는 인증서 공개 키의 Base64 부호화(바이너리) SHA-256 해시를 입력해야 합니다. Apple 운영 체제에 대해 사용 가능하고 신뢰할 수 있는 루트 인증서는 **Apple 문서**를 참조하십시오. 이 구성에서 여러 개의 루트 인증서를 추가할 수 있습니다.

5. 다음을 클릭하세요.
6. 이 구성 활성화 옵션을 선택합니다.
7. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
8. 완료를 클릭하세요.

# 10.10.4.11. 자치 단일 앱 모드 구성 만들기

자치 단일 앱 모드 구성을 통해 장치에서 특정 애플리케이션만 실행하도록 할 수 있습니다. 사용자가 다른 애플리케이션을 시작하려 시도하더라도 구성은 특정 애플리케이션만 실행합니다.

**절차**

1. **구성** > **추가** > **자치 단일 앱 모드**로 이동합니다.
2. 다음 지침을 사용하여 앱과 관련 설정을 정의하세요.
3. **다음**을 클릭하세요.

| 설정 항목 | 설정하기 |
| --- | --- |
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **구성 설정** | **번들 식별자** - (필수) 고유한 번들 식별자입니다. 두 개의 사전에 동일한 BundleIdentifier 값이 있지만 TeamIdentifier 값이 다를 경우, 이는 오류로 간주되며 프로필이 설치되지 않습니다. |
| | **팀 식별자** - (필수) 개발자의 팀 식별자로서 앱 서명에 사용됩니다. |

4. **배포** 화면에서 이 구성을 수신할 그룹을 선택합니다.
5. **완료**를 클릭하세요.

# 10.10.4.12. DNS 프록시 구성 생성

MDM용 Ivanti Neurons 관리자는 iPhone 및 iPad 장치 사용자를 위해 DNS 프록시 구성을 사용하여 DNS 프록시 설정을 구성할 수 있습니다. DNS 프록시 페이로드를 사용하여 DNS 프록시 네트워크 확장 및 기타 공급업체별 값을 제공하는 애플리케이션을 지정할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**으로 이동합니다.
3. 검색 필드에 **DNS**를 입력하고 **DNS프록시 구성**을 클릭합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. 다음 DNS 프록시 구성 설정을 입력합니다.
    - 앱 번들 식별자(필수)
    - 공급자 번들 식별자.
    - 공급자 구성(키-값).
6. **다음**을 클릭합니다.
7. **이 구성 활성화** 옵션을 선택합니다.
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정

**완료**를 클릭하세요.

# 10.10.4.13. 장치 로깅 구성

장치 로깅 구성을 통해 Android 장치의 네트워크와 보안 로그를 활성화할 수 있습니다.

## 장치 로깅 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에서 **장치 로깅**을 입력하고 구성을 선택합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. **구성 설정** 섹션에서 하나의 옵션을 선택하거나 두 옵션을 모두 선택합니다.
    - 네트워크 로깅 활성화
    - 보안 로깅 활성화

> 보안 및 네트워킹 로깅이 지원되는 Android 버전에 대한 정보는 **보안 로깅 매트릭스**의 표를 참조해 주십시오.

**다음**을 클릭해 배포 설정을 구성합니다.

7. **완료**를 클릭하세요.

**보안 로깅 매트릭스**

| 장치 유형 | 지원되는 Android 버전 |
|---|---|
| 업무 관리형 기기 및 업무 관리형 기기 - 비 GMS 모드(AOSP) | 7, 8, 9, 10, 11, 12, 13 |
| 작업 프로필이 있는 관리 장치 | 8, 9, 10 |
| 작업 프로필 | NA |
| 회사 소유 장치의 작업 프로필 | 11, 12, 13 |

**네트워크 로깅 매트릭스**

| 장치 유형 | 지원되는 Android 버전 |
|---|---|
| 업무 관리형 기기 및 업무 관리형 기기 - 비 GMS 모드(AOSP) | 8, 9, 10, 11, 12, 13 |
| 작업 프로필이 있는 관리 장치 | 8, 9, 10 |
| 작업 프로필 | 12, 13 |
| 회사 소유 장치의 작업 프로필 | 12, 13 |

장치에 장치 로깅 구성을 설치한 후 사용자는 장치 관리 및 네트워크 로깅에 대한 정보가 포함된 알림을 받습니다. **확인**을 클릭하여 알림을 승인합니다.

## 디버그 로그 요청

**절차**

1. MDM용 Ivanti Neurons에 로그인합니다.
2. **장치** > **장치 세부 정보**로 이동합니다.
3. **개요** 섹션에서 **강제 체크인** 버튼 옆의 세로 점 3개 버튼을 클릭합니다.
4. **디버그 로그 요청**을 선택합니다.
5. 다음 2가지 옵션 중 하나를 선택합니다.
    - 버그 보고서 제외 - 이 옵션을 선택하고 다음을 클릭하면 화면에 확인 창이 표시됩니다. **디버그 로그 요청**을 클릭합니다. 사용자는 이 옵션에 대한 동의를 제공할 필요가 없으며, 이러한 로그에서 선택한 Android 장치에 대한 버그 보고서가 제외됩니다.
    - 버그 보고서 포함 - 이 옵션을 선택하고 다음을 클릭하면 화면에 확인 창이 표시됩니다. **디버그 로그 요청**을 클릭합니다. 사용자는 반드시 버그 보고서 공유에 동의해야 합니다. Android 장치의 경우 버그 보고서를 포함하기 위해 장치 로그를 제출하라는 메시지가 표시됩니다.

# 10.10.4.14. 디스크 관리 구성

MDM용 Ivanti Neurons 디스크 관리 구성 설정은 외부 및 네트워크 저장소의 데이터를 효과적으로 관리하기 위한 정책을 정의합니다.

**적용 대상**: 감독 대상인 macOS 15.0부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **디스크 관리** 구성을 검색하고 선택합니다.
3. 다음 표에 따라 **디스크 관리** 설정을 구성합니다.

| 설정 항목 | 설명 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **디스크 관리** | |
| 외부 저장소 | 드롭다운 목록에서 다음 값 중 하나를 선택합니다.<br>• **허용**: 저장소의 읽기와 쓰기를 허용합니다.<br>• **읽기 전용**: 저장소를 읽을 수 있습니다.<br>• **허용 안 함**: 저장소 액세스를 허용하지 않습니다. |
| 네트워크 저장소 | 드롭다운 목록에서 다음 값 중 하나를 선택합니다.<br>• **허용**: 저장소의 읽기와 쓰기를 허용합니다.<br>• **읽기 전용**: 저장소를 읽을 수 있습니다.<br>• **허용 안 함**: 저장소 액세스를 허용하지 않습니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **디스크 관리** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.15. Android 암호화

암호화 구성은 기기 관리자 모드에서 Android 기기에 대한 기기 암호화 요구 사항을 정의합니다. 기기 암호화는 알려진 탈옥 또는 루트 공격을 통해 중요한 회사 데이터에 액세스할 수 없도록 보장합니다. 암호화를 하면 해당 기기의 데이터가 판독이 불가능한 형태로 저장되어 기기 도난 시 타인의 데이터 접속을 차단할 수 있습니다.

암호화 기능이 설정되면 해당 기기 사용자는 기기를 암호화하고 기기 암호를 설정해야 합니다. 암호는 데이터를 읽을 수 있도록 해독하는 데 필요합니다. 암호가 설정되면 Android 엔터프라이즈(작업 프로필 또는 관리되는 기기) 또는 iOS 기기에서 기기 암호화가 자동으로 활성화됩니다. 암호화하는 중에는 기기를 사용할 수 없습니다. 암호화가 설정되면 해제할 때 기기의 공장 초기화가 필요합니다.

## 암호화 설정

| 설정 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 기기 암호화 활성화 | 이 항목을 선택하면 해당 설정값을 수신하는 암호화 가능 Android 기기에 모두 암호화 기능이 설정됩니다. |

> Android 암호화 구성은 Android 11의 장치 관리 모드에서 Samsung 장치에 대해 더 이상 사용되지 않습니다. 이 암호화는 장치 암호가 설정된 경우 Android Enterprise 장치에서 기본으로 지원됩니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.16. 암호화된 DNS

**라이센스:** Gold

**적용 가능 운영 체제:**

- iOS 14.0 또는 지원되는 최신 버전.
- macOS 11.0 또는 지원되는 최신 버전.
- visionOS 1.1 또는 지원되는 최신 버전.

VPN을 구성할 필요 없이 보안을 강화할 수 있게 해줄 암호화된 DNS를 구성하십시오.

이 섹션에는 다음 주제가 포함됩니다.


- 암호화된 DNS 구성
- 암호화된 DNS 구성 설정


## 암호화된 DNS 구성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **DNS**를 입력한 다음, **암호화된 DNS** 구성을 클릭합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. 암호화된 DNS 구성 설정을 입력합니다.
6. **다음**을 클릭하세요.
7. **이 구성 활성화** 옵션을 선택합니다.
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
9. **완료**를 클릭합니다.

## 암호화된 DNS 구성 설정

다음 표의 설정을 사용하여 암호화된 DNS를 구성합니다. 이 설정에 대한 자세한 내용은 **Apple 문서**를 참조하십시오.

| 설정 항목 | 설명 |
| --- | --- |
| **DNS 설정** | 암호화된 DNS 서버에 대한 구성을 정의하는 사전입니다. |
| DNS 프로토콜 | DNS 서버와 통신하는 데 사용되는 암호화된 수송 프로토콜을 지정합니다. 다음 프로토콜 중 하나를 선택하십시오.<br>• HTTPS<br>• TLS |
| 서버 URL | RFC 8484에 정의된 대로 DNS-over-HTTPS 서버의 URI 템플릿입니다. 이 URL은 https:// 체계를 사용해야 하며 URL의 호스트 이름이나 주소는 서버 인증서를 검증하는 데 사용됩니다. 서버 주소가 제공되지 않을 경우 URL의 호스트 이름이나 주소는 서버 주소를 결정하는 데 사용됩니다. 이 키는 DNS 프로토콜이 HTTPS일 경우에만 존재해야 합니다. |
| 서버 주소 | DNS 서버 IP 주소 문자열의 순서 없는 목록입니다. 이들 IP 주소는 IPv4 및 IPv6 주소의 혼합이 될 수 있습니다.<br>하나 이상의 서버 주소를 추가하려면 **추가**를 클릭하십시오. |
| 보완 일치 도메인 | 어떤 DNS 쿼리가 DNS 서버를 사용할 지 결정하는 데 사용되는 도메인 문자열의 목록입니다. 이 배열이 제공되지 않을 경우 모든 도메인이 DNS 서버를 사용하게 됩니다.<br>하나 이상의 도메인을 추가하려면 **추가**를 클릭하십시오. |
| 사용자가 DNS 설정을 비활성화하지 못하도록 금지 | 사용자가 DNS 설정을 비활성화하지 못하도록 금지합니다. 이 키는 감독 기기에서만 사용할 수 있습니다. |
| **요청 규칙** | DNS 설정을 정의하는 규칙의 배열입니다. 규칙이 존재하지 않을 경우 시스템은 언제나 DNS 설정을 적용합니다.<br>하나 이상의 요청 규칙 세트를 추가하려면 **+ 요청 규칙 추가**를 클릭하십시오. |
| 네트워크 | 이 사전이 현재 네트워크에 일치할 경우 취해야 할 조치입니다. 다음 작업 중 하나를 선택하십시오.<br>• **연결:** 사전이 일치할 때 DNS 설정을 적용합니다.<br>• **연결 해제:** 사전이 일치할 때 DNS 설정을 적용하지 않습니다.<br>• **연결 평가:** 사전이 일치할 때 도메인당 예외가 있는 DNS 설정을 적용합니다. |
| 연결 평가 | 이 네트워크 옵션에는 다음과 같은 설정이 있습니다.<br>• **도메인 작업** - 지정된 도메인에 대한 DNS 설정 행동입니다. 다음 작업 중 하나를 선택하십시오.<br>◦ **연결하지 않음** - 지정된 도메인에 대해 DNS 설정을 사용하지 않습니다.<br>◦ **필요 시 연결** - 지정된 도메인에 대한 DNS 설정 사용을 허용합니다.<br>• **도메인** - 이 평가가 적용되는 도메인입니다. 하나 이상의 도메인을 추가하려면 **+추가**를 클릭하십시오. |
| **규칙** | 하나 이상의 규칙을 추가하여 다음 매개변수를 해당 지정 값과 일치시키려면 **+추가**를 클릭하십시오. |
| DNS 도메인 일치 | 도메인 이름의 배열입니다. 이 규칙은 지정된 목록의 도메인 이름이 기기의 검색 도메인 목록의 도메인과 일치할 경우에 일치합니다. |
| DNS 서버 주소 일치 | IP 주소의 배열입니다. 이 규칙은 네트워크의 지정된 DNS 서버가 배열의 항목과 일치할 경우에 일치합니다. |
| SSID 일치 | 현재 네트워크에 대해 일치하는 SSID 배열입니다. 네트워크가 Wi-Fi 네트워크가 아니거나 SSID가 이 배열에 나타나지 않을 경우 일치에 실패합니다. |

| 설정 항목 | 설명 |
| --- | --- |
| | 이 키, 그리고 SSID와 일치할 해당 배열을 생략하십시오. |
| 인터페이스 유형 일치 | 인터페이스 유형입니다. 지정된 경우 이 규칙은 기본 네트워크 인터페이스 하드웨어가 지정된 유형과 일치할 경우에만 일치합니다. 다음 중 하나를 선택합니다.<br>• 이더넷<br>• Wi-Fi<br>• 휴대폰 |
| URL 문자열 검색 | 조사할 URL입니다. 이 URL을 리디렉션 없이 성공적으로 가져올 경우(200 HTTP 상태 코드로 복귀), 이 규칙이 일치합니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.17. 외부 인텔리전스 설정

**외부 인텔리전스 설정**을 사용하여 감독 모드 기기에서 외부 인텔리전스 통합을 구성합니다. 이 구성은 관리자가 기기에서 지원되는 외부 인텔리전스 서비스에 연결하고 이를 사용하는 방식을 제어하는 일관된 정책 기반 설정을 적용하는 데 도움이 됩니다.

**적용 대상**:

- iOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- macOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- visionOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **외부 인텔리전스 설정** 구성을 검색하여 선택합니다.
3. 다음 표에 따라 **외부 인텔리전스 설정** 구성을 구성합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 외부 인텔리전스 통합 허용 | 확인란을 선택하여 외부 인텔리전스 통합을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 외부 인텔리전스를 활성화합니다. |
| 외부 인텔리전스 통합 로그인 허용 | 확인란을 선택하여 외부 인텔리전스 통합 로그인을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 외부 인텔리전스 통합 로그인을 활성화합니다. |
| 허용된 외부 인텔리전스 작업 공간 ID | 외부 인텔리전스를 활성화할 Workspace ID를 입력합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 입력한 작업 공간 ID에 대해 외부 인텔리전스를 활성화합니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **외부 인텔리전스 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.18. 위협 방어

**적용 가능 운영 체제:**

- iOS용 Go 클라이언트 버전 3.2.0 또는 지원되는 최신 버전.
- Android용 Go 버전 52 또는 지원되는 최신 버전.

MDM용 Ivanti Neurons에는 Android 및 iOS 클라이언트용 Go로 통합된 위협 방어 기술을 사용하기 위한 활성화 토큰 배포 기능이 포함되어 있습니다. Threat Defense는 기기, 네트워크, 애플리케이션에 영향을 미치는 모바일 위협 및 취약성으로부터 관리 기기를 보호합니다.

이 구성이 MDM용 Ivanti Neurons에서 활성화되어 기기에 적용되면 Go 클라이언트에서 위협 방어 라이브러리가 활성화됩니다. Threat Defense 서비스는 라이센스 토큰을 제거하고 라이센스 구성을 클라이언트로 다시 보내 비활성화할 수 있습니다.

Threat Defense는 다음을 모니터링합니다.

- 기기 수준: 의심되거나 악의적인 활동을 식별하기 위해 시스템 매개 변수, 구성, 펌웨어 및 라이브러리를 모니터링합니다.
- 네트워크 수준: 네트워크 트래픽과 모바일 기기에 대한 의심스러운 연결을 모니터링합니다.
- 앱 수준: 위험 평가 및 코드 분석을 통해 유출 앱(엔터프라이즈 데이터를 위험에 빠뜨릴 가능성이 있음)과 악성 앱을 모니터링합니다.

## 최신 문서

최신 Threat Defense 지침은 제품 설명서 사이트의 **MDM용 Ivanti Neurons 제품 설명서**에서 *MDM용 Ivanti Neurons Threat Defense 솔루션 가이드*를 참조하십시오.

# 10.10.4.19. FileVault 2

**라이센스:** Gold

FileVault 2는 볼륨 컨텐츠에서 전체 XTS-AES 128 디스크 암호화를 수행할 수 있는 기능을 제공합니다.

FileVault 2를 활성화하면 다음 설정을 구성에 사용할 수 있습니다.

| 범주 | 설정 |
| --- | --- |
| FileVault 사용자 설정 | • SetupAssist에서 FileVault 활성화<br>**기본값** : 거짓<br>• 참이고 설정 도우미에서 MDM용 Ivanti Neurons에 등록한 후 페이로드가 설치된 경우, 설정 시 FileVault를 활성화하도록 설정 도우미에게 요청합니다. 또한 이 페이로드에서 ShowRecoveryKey를 제외한 다른 모든 키는 시스템이 무시합니다.<br>**전제 조건** : - 설정 도우미에서 파일 보관소를 활성화하기 전에 장치 등록 프로필에서 **장치 등록 설정 중 장치 구성 대기**가 활성화되어 있는지 확인하십시오.<br>• 지정된 사용자가 로그아웃할 때까지 FileVault 활성화 연기<br>◦ FileVault를 활성화할 때는 항상 사용자에게 확인<br>◦ 사용자가 FileVault 활성화를 우회할 수 있는 최대 횟수<br>사용자 로그아웃 시 FileVault 활성화를 요청하지 않음 |
| 출력 경로<br><br>개인 복구 키 | 복구 키와 컴퓨터 정보 plist가 저장될 위치에 경로를 입력합니다.<br>• 개인 복구 키 생성<br>• FileVault를 활성화한 후 사용자에게 개인 복구 키 표시<br>이 옵션은 **개인 복구 키 생성**이 활성화되어 있을 때만 보입니다. 기본적으로 옵션이 비활성화되어 있습니다.<br>• 기관 복구 키 활성화: 키체인 사용 - 이 페이로드에 인증서 정보가 제공되지 않은 경우, /Library/Keychains/FileVaultMaster.keychain에 이미 생성된 키체인을 사용합니다.<br>다음 옵션 중 하나를 선택합니다.<br>◦ 인증서 업로드<br>◦ 인증서<br>◦ 사용자 시스템에서 키체인 사용 |
| __일 후 FileVault 키 순환 | 관리자는 배포된 장치의 보안 위험을 완화하기 위해 macOS 장치에 대한 FileVault 키의 주기적인 순환을 구성할 수 있습니다. 관리자는 일 단위로 순환 간격을 설정할 수 있습니다.<br>개인 복구 키만 순환됩니다. |

# 10.10.4.20. FileVault 복구 키

**라이센스:** Gold

FileVault 복구 키 구성은 FileVault 복구 키를 회사 서버로 리디렉션 및 에스크로 하는지 여부를 결정합니다.

> macOS 기기가 구성을 다시 푸시할 때 복구 키 보내기를 중지하므로, FileVault 복구 키 제외 및 다시 푸시 구성이 비활성화됩니다.

다음과 같은 옵션을 설정할 수 있습니다.

| 설정 항목 | 설명 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | (선택 사항) 이 구성의 목적에 대한 간략한 설명을 입력합니다. |
| **macOS 10.13 미만 버전 구성 설정** | |
| MDM용 Ivanti Neurons 테넌트에 대한 저장소 복구 키 | MDM용 Ivanti Neurons 활성화를 선택하여 테넌트에 키를 저장합니다. 필요한 경우 기기 상세 정보 페이지에서 키의 암호화를 해제할 수 있습니다. |
| URL을 서버로 리디렉션 | 다음 설정을 입력합니다.<br>• Apple 대신 FDE 복구 키를 전송해야 하는 곳으로 **리디렉트 URL**을 입력합니다. URL은 반드시 https://로 시작되어야 합니다.<br>• 드롭 다운 목록에서 인증서를 선택합니다. PKCS1 형식 인증서만이 지원됩니다. |
| **macOS 10.13 이상 버전 구성 설정** | |
| 위치 | (필수) 복구 키가 보관될 위치에 대한 간단한 설명을 입력합니다. 해당 텍스트는 FileVault가 활성화될 때 사용자가 보는 메시지에 삽입됩니다. |
| 기기 키 | (선택 사항) 사용자가 비밀번호를 잊어버린 것으로 보일 경우에 도움말 텍스트에 넣을 문자열을 입력합니다. |

# 10.10.4.21. FileVault 옵션 구성

이 구성을 통해 관리자는 시스템이 대기 모드일 때 FileVault를 활성화 또는 비활성화하고 FileVault 키를 제거할 수 있습니다.

적용 대상: macOS 10.7+

**절차**

1. **구성** > **추가**로 이동합니다.
2. 검색 필드에 FileVault를 입력한 다음, FileVault 옵션 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. 구성 설정에서 필수 옵션을 선택합니다.
    - 시스템이 대기 모드가 되면 FileVault 키 제거
    - 전체 디스크 암호화의 비활성화를 허용하지 않음
    - 전체 디스크 암호화의 활성화를 허용하지 않음
5. 다음을 클릭하세요.
6. 이 구성 활성화 옵션을 선택합니다.
7. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
8. 완료를 클릭하세요.

# 10.10.4.22. ID 인증서

이 섹션에는 다음 주제가 포함됩니다.

- ID 인증서 설정
- 구성 배포

ID 인증서 구성을 통해 모바일 기기 인증서의 인증 방법을 설정할 수 있습니다. ID 인증서는 X.509 인증서(.p12 또는 .pfx)입니다. ID 인증서는 인증 기관을 소스로 사용하여 동적으로 생성할 수도 있습니다. 먼저 모바일 기기에 인증서를 어떻게 배포할지를 정해야 합니다. 필요한 인증 기관을 구성할 수 있습니다.

> 릴리스 91부터 Apple 기기의 기기 ID 인증서는 만료 30일 이내에 자동으로 갱신됩니다. iOS 기기는 일반 기기 체크인 흐름의 일부로 MDM용 Ivanti Neurons로부터 갱신된 MDM 인증서를 받습니다. 그러나 iOS 기기는 만료되기 전에 체크인하여 MDM 인증서를 갱신시키지 않고 오래 오프라인 상태로 두어 인증서를 만료시키는 경우 MDM용 Ivanti Neurons에 다시 등록해야 합니다.

- SHA-1 인증서는 ID 인증서를 생성하는 동안 사용되지 않습니다. 다른 알고리즘을 선택할 수 있습니다. 인증서를 업데이트하는 동안 이전 인증서에서 SHA-1을 사용하는 경우 동일한 SHA-1 알고리즘을 사용할 수 있습니다. 이전 인증서에서 SHA-1 위의 알고리즘을 사용하는 경우 SHA-1으로의 전환이 허용되지 않습니다.
- ID 인증서를 구성하고 나면 **테스트 구성 및 계속하기**를 클릭하여 테스트 인증서를 발급하고 유효성을 검증합니다. 소유자 이름이 로컬 인증 기관과 동일한 경우 새로 생성되거나 기존의 동적으로 생성된 ID 인증서 구성에 대해 이 테스트를 수행하면 오류가 표시될 수 있습니다. 이 오류 메시지가 표시되면 ID 인증서 소유자 이름을 로컬 인증 기관 소유자 이름과 다르게 수정해야 합니다. 소유자 이름으로 수정한 기존 ID 인증서 구성인 경우 인증서가 재발급되고 구성이 다시 푸시됩니다.
  **동적으로 생성된** 인증서 배포에 대하여 테스트 인증서를 발급하지 않고 구성을 생성하는 옵션을 설정하는 경우 **계속**을 클릭하십시오.
- 인증서는 자동으로 재발급됩니다.
- ID 인증서가 Android 앱에 할당되면, 사용자의 앱은 사용자에게(앱 대신에) 인증서 사용 허용 알림 없이 ID 인증서를 얻습니다. 이것은 Email+, Gmail 등의 앱을 포함합니다.
- Email+는 사용자가 제공하는 ID 인증서를 통해 구성된 후 Android Enterprise 기기에 앱 구성으로 적용되고 할당될 수 있습니다. 이는 회사 소유 기기의 작업 프로필과 기기 소유자 모드에서만 적용됩니다.

## ID 인증서 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 인증서 배포 | 설정할 인증서 배포 유형을 선택할 수 있습니다.<br>• **단일 파일**: 기기 배포용으로 기존 인증서를 업로드할 수 있습니다.<br>• **동적으로 생성됨**: 로컬 또는 외부 인증서 권한을 사용하여 요청 시 인증서를 생성합니다.<br>• **사용자 제공**: 사용자가 업로드할 인증서 유형에 대한 레이블을 생성할 수 있습니다. 레이블이 생성되면 사용자가 자체 서비스 포털에서 생성된 레이블(옵션)을 볼 수 있고 해당 레이블에 맞는 인증서를 업로드할 수 있습니다.<br>• **파생된 자격 증명:** 파생된 자격 증명에 대해 다음 사용 중 하나를 지정할 수 있습니다.<br>◦ 인증<br>◦ 암호화<br>◦ 서명<br>◦ 암호 해독<br>• **SCEP 구성**: SCEP 서버에서 인증서를 요청하는 방법을 지정합니다. 다음 구성 중 하나를 선택합니다.<br>◦ Apple 구성<br>◦ Windows 구성<br>선택 항목에 따라 나머지 설정 항목이 달라집니다. |
| 모든 앱이 개인 키에 액세스할 수 있도록 허용(macOS 10.10+)<br><br>단일 파일<br><br>ID 인증서 데이터<br><br>비밀번호<br><br>**동적으로 생성됨**<br><br>소스 | **적용 대상:** 단일 파일, 동적으로 생성됨, 사용자 제공, SCEP Apple 구성 ID 인증서.<br>PKCS#12 인증서의 경우 **모든 앱의 개인 키 액세스 허용** 옵션을 활성화하여 모든 앱이 개인 키에 액세스할 수 있도록 합니다(선택 사항).<br>예를 들어 사용자가 VPN에 사용된 인증서에 액세스할 수 있도록 비밀번호를 요청하는 경우 이 키를 사용할 수 있습니다.<br><br><br>인증서 파일을 점선 박스로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다.<br><br>PKCS#12 인증서 파일을 보호하는 비밀번호를 입력합니다. 이 비밀번호는 메시지를 표시하지 않는 설치에 사용됩니다.<br><br><br>드롭다운 목록에서 원하는 로컬 인증 기관을 선택할 수 있습니다. 이 인증 기관은 **관리 > 인증 관리**에서 이미 생성되어 있어야 합니다. |
| 테스트 인증서를 발급하지 않고 구성 만들기 | 테스트 인증서를 발급하지 않고 구성을 생성할 확인란을 선택하십시오. |
| Windows 전용 - 대상 인증서 스토어<br><br>**사용자 제공** | 관리자는 이제 Windows 기기에서 대상 인증서 스토어를 선택할 수 있습니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| 인증서 표시 이름 | 인증서 이름을 입력합니다. 이 인증서는 테넌트에 대해 고유하며 사용자는 인증서를 업로드하는 동안 자체 서비스 포털에서 이름을 볼 수 있습니다. |
| 개인 키 삭제 | 이 옵션을 선택하여 *n*(1~30)일 후 인증서의 개인 키를 삭제할 수 있습니다.<br>이 작업에 대해 MDM용 Ivanti Neurons에서 제공하는 API를 사용할 수도 있습니다. API에 대한 자세한 정보는 MDM용 Ivanti Neurons*API 가이드*를 참조하십시오.<br>개인 키가 삭제된 후 어떠한 구성에서든 이 인증서를 사용하려 할 경우(예를 들어 애플리케이션을 인증하거나 Wi-Fi 또는 VPN 구성을 푸시하는 경우) 작업이 실패하게 됩니다. 개인 키가 삭제되기 전에 작업이 수행되도록 하십시오. |
| 다음 일 후에 개인 키 삭제 | 인증서의 개인 키가 추후 삭제될 일 수(1~30)를 선택할 수 있습니다. 기본값은 2일입니다. |
| **파생된 자격 증명** | |
| 파생된 자격 증명 사용 | 다음 옵션 중 하나를 선택합니다.<br>• **인증** - 파생된 자격 증명이 인증에 사용되도록 지정합니다.<br>• **암호화** - 파생된 자격 증명이 암호화에 사용되도록 지정합니다.<br>• **서명** - 파생된 자격 증명이 서명에 사용되도록 지정합니다.<br>• **암호 해독** - 파생된 자격 증명이 암호 해독에 사용되도록 지정합니다. |
| 브랜드<br><br>**ACME 구성 - iOS/iPadOS16+ /macOS14+에만 적용 가능** | 다음 옵션 중에서 사용할 파생된 자격 증명 제공자를 선택합니다.<br>• **Entrust**<br>• **Intercede**<br>• **Purebred**<br>사용 중인 사용자 지정 파생된 자격 증명 제공자를 추가하려면 파생된 자격 증명 제공자를 참조하십시오. |
| 클라이언트 식별자 | 특정 장치를 식별하는 고유 문자열 |
| 디렉토리 URL | (필수) ACME 서버의 디렉토리 URL입니다. URL은 반드시 https 체계를 사용해야 합니다. |
| 확장 키 사용 | 이 값은 문자열의 배열입니다. 각 문자열은 점 표기법으로 지정된 OID입니다. 예를 들어 ["1.3.6.1.5.5.7.3.2", "1.3.6.1.5.5.7.3.4"]는 클라이언트 인증 및 이메일 보호를 나타냅니다.<br>장치는 ACME 서버가 발급하는 인증서에 대해 이 필드를 요청합니다. ACME 서버는 발급한 인증서에서 이 필드를 우선 적용하거나 무시할 수 있습니다. |
| 키 크기 | (필수) KeySize의 유효 값은 KeyType 및 HardwareBound의 값에 따라 다릅니다. 특정 요구 사항은 해당 키를 참조하십시오. |
| 키 유형 | (필수) 생성할 키 쌍의 유형입니다. |
| 주제 | (필수) 쉼표로 구분된 OID 및 값 배열로 표시되는 X.500 이름을 입력합니다. 통상적으로, 소유자는 사용자의 전체 도메인 이름으로 설정됩니다. 예: C=US,DC=com,DC=MobileIron,OU=InfoTech 또는 CN=www.mobileiron.com. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| 주제 대체 이름 | OID에 변수를 붙여 원하는 소유자로 설정할 수도 있습니다. 예: CN=www.mobileiron.com-${{deviceGUID}}.<br>간편한 구성을 위해 $ 변수를 사용하여 제목을 사용자의 FQDN으로 채울 수도 있습니다.<br>제목 이름에 백슬래시 문자()를 사용하지 마십시오.<br><br>ACME 서버가 발급하는 인증서에 대해 장치가 요청하는 주체 대체 이름입니다. ACME 서버는 발급한 인증서에서 이 필드를 우선 적용하거나 무시할 수 있습니다. |
| 키 사용<br><br>하드웨어 바인딩 | 이 값은 비트 필드입니다.<br>비트 0x01은 디지털 서명을 나타냅니다.<br>비트 0x10은 키 동의를 나타냅니다.<br>장치는 ACME 서버가 발급하는 인증서에 대해 이 키를 요청합니다. ACME 서버는 발급한 인증서에서 이 필드를 우선 적용하거나 무시할 수 있습니다.<br><br>하드웨어 바인딩이 true로 설정된 경우 개인 키는 장치에 바인딩되고 키 유형은 ECSECPrimeRandom이어야 하고 키 크기는 256 또는 384여야 합니다. |
| 보증 | true인 경우 장치는 ACME 서버에 대한 장치 및 생성된 키를 설명하는 증명을 제공합니다. 보증이 true일 경우 하드웨어 바인딩도 true여야 합니다. |
| SCEP 구성 - Apple 구성<br><br>ID 인증서(SCEP)<br><br>로컬 인증 기관<br><br>URL<br><br>CA 식별자<br><br>주제 | <br><br>SCEP 서버를 지정하도록 선택합니다.<br><br>**관리 >** 인증 관리에서 이미 생성된 로컬 인증 기관을 지정하려면 선택하십시오. 해당 항목을 선택하면 나타나는 드롭다운 목록에서 사용할 로컬 인증기관을 선택할 수 있습니다.<br><br>SCEP 서버의 URL을 입력합니다.<br><br>인증 기관이 제공하는 식별자를 입력합니다.<br><br>콤마로 구분되는 OID 및 값의 배열로 표기하는 X.500 이름을 입력합니다. 통상적으로, 소유자는 사용자의 전체 도메인 이름으로 설정됩니다. 예: C=US,DC=com,DC=MobileIron,OU=InfoTech 또는 CN=www.mobileiron.com.<br>OID에 변수를 붙여 원하는 소유자로 설정할 수도 있습니다. 예: CN=www.mobileiron.com-$DEVICE_CLIENT_ID$.<br>또한 $USER_DN$ 변수를 사용해 사용자의 FQDN이 포함된 소유자로 채우면 더 편리하게 설정을 할 수 있습니다.<br>소유자 이름에는 역슬래시(\) 문자를 사용하지 마십시오. |
| 소유자 대체 명칭 유형 | 인증서 템플릿의 속성을 바탕으로 RFC 822 이름, DNS 이름, 균일 리소스 식별자 또는 없음을 선택할 수 있습니다. |
| 소유자 대체 명칭 값<br><br>NT 사용자 이름 | 해당 유형의 값을 입력할 수 있습니다. 첫 문자로 '$'를 입력할 경우, 가능한 사용자 지정 LDAP 및 Entra ID 속성과 함께 드롭다운 목록이 표시됩니다. 목록에서 적절한 사용자 지정 속성을 선택하십시오.<br>Entra ID 값이 사용될 경우 'onPremisesImmutableId'만 지원됩니다. fn:base64tohex($) 입력<br><br>Microsoft 환경의 소유자 대체 명칭을 입력할 수 있습니다. 일반적으로 사용자의 UPN(사용자 원이름)이 포함되도록 구성됩니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| 챌린지 | (선택 사항) 자동 등록을 위해 사전 공유된 비밀로 사용됩니다. |
| 재시도 | 첫 번째 '지연 중' 상태가 표시된 후 인증이 시도될 횟수를 목록에서 선택해 설정할 수 있습니다. |
| 재시도 연기 | 재시도 전에 대기할 시간을 초 단위로 설정할 수 있습니다. |
| 키 크기 | 1024, 2048 또는 4096비트 중에서 선택할 수 있습니다. |
| 디지털 서명으로 사용 | 인증서가 서명에 사용될 수 있는 경우 선택합니다. |
| 키 암호화로 사용 | 인증서가 암호화에 사용될 수 있는 경우 선택합니다. |
| CA 지문 | 사용 중인 인증 기관의 HTTP를 이용하는 경우, 해당 인증 기관의 인증서 지문처럼 사용될 16진수 문자열을 입력할 수 있습니다. MD5 지문을 지원합니다.<br>인증서에서 직접 지문을 생성할 수도 있습니다. 인증서를 지정된 영역으로 드래그하거나 **인증서에서 생성**을 클릭해 파일 시스템의 인증서를 선택하기만 하면 됩니다. |
| SCEP 구성 - Windows 구성 | |
| CA(인증 기관) | **관리 >** 인증 관리에서 이미 생성한 인증 기관을 지정하려면 선택합니다. 이 옵션을 선택하면 나타나는 드롭다운 목록에서 원하는 인증 기관을 선택합니다. |
| 주제 | 콤마로 구분되는 OID 및 값의 배열로 표기하는 X.500 이름을 입력합니다. 통상적으로, 소유자는 사용자의 전체 도메인 이름으로 설정됩니다. 예: C=US,DC=com,DC=MobileIron,OU=InfoTech 또는 CN=www.mobileiron.com.<br>OID에 변수를 붙여 원하는 소유자로 설정할 수도 있습니다. 예: CN=www.mobileiron.com-$DEVICE_CLIENT_ID$.<br>또한 $USER_DN$ 변수를 사용해 사용자의 FQDN이 포함된 소유자로 채우면 더 편리하게 설정을 할 수 있습니다.<br>소유자 이름에는 역슬래시(\) 문자를 사용하지 마십시오. |
| 소유자 대체 명칭 유형 | **+ 추가**를 클릭합니다. 인증서 템플릿의 속성을 바탕으로 RFC 822 이름, DNS 이름, 균일 리소스 식별자 또는 없음을 선택할 수 있습니다. |
| 재시도 | 첫 번째 '지연 중' 상태가 표시된 후 인증이 시도될 횟수를 목록에서 선택해 설정할 수 있습니다. |
| 재시도 연기 | 재시도 전에 대기할 시간을 초 단위로 설정할 수 있습니다. |
| 키 길이 | 키 크기를 1024, 2048 또는 4096비트 중에서 선택할 수 있습니다. |
| 사용 선택 | 한 가지 이상의 옵션 선택:<br>• 디지털 서명으로 사용 - 인증서가 서명에 사용될 수 있는 경우 선택합니다.<br>• 키 암호화로 사용 - 인증서가 암호화에 사용될 수 있는 경우 선택합니다. |
| 유효성 | 유효성을 일, 월 또는 연 단위로 선택합니다. |
| CA 지문 | 사용 중인 인증 기관의 HTTP를 이용하는 경우, 해당 인증 기관의 인증서 지문처럼 사용될 16진수 문자열을 입력할 수 있습니다. MD5 지문을 지원합니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| | 인증서에서 직접 지문을 생성할 수도 있습니다. 인증서를 지정된 영역으로 드래그하거나 **인증서에서 생성**을 클릭해 파일 시스템의 인증서를 선택하기만 하면 됩니다. |
| 해시 알고리즘군 | SHA-2 또는 SHA-3 알고리즘을 선택합니다. |

> 챌린지 암호 설정 없이 ID 인증서를 기기의 작업 프로필에 적용하는 경우, 기기는 워크 챌린지 암호 대신 기기 암호를 요청합니다.

자세한 내용은 구성 작업을 참조하십시오.

# 10.10.4.23. Apple 활성화 잠금 구성

**라이센스:** Silver

이 섹션에는 다음 주제가 포함됩니다.


- iOS 활성화 잠금 활성화
- 감독 기기에서 iOS 활성화 잠금 기능 활성화
- macOS 활성화 잠금 활성화
- 감독 기기에서 macOS 활성화 잠금 기능 활성화
- iOS 활성화 잠금 우회 코드 사용
- iOS 활성화 잠금 우회 코드 삭제


활성화 잠금은 다른 사람이 분실 또는 도난당한 기기를 이용하지 못하도록 설계된 Apple 기능입니다. 내 찾기를 활성화하면 iCloud 계정과 해당 기기의 하드웨어 식별자 간의 매핑이 Apple 활성화 서버에 저장됩니다. 이 순간부터 누구도 기존 Apple ID와 비밀번호를 입력하지 않고 내 찾기를 비활성화하거나 기기를 삭제하거나 다시 활성화할 수 없습니다. 사용자 이외의 누군가가 기기를 삭제하고 이것을 다시 활성화하여 사용하려고 하는 경우, 설정 길잡이에 Apple ID와 비밀번호를 입력해야 합니다.

최종 사용자가 내 기기 찾기를 활성화한 경우, 활성화 잠금을 비활성화하더라도 감독 기기에서 이 기능을 비활성화할 수 없습니다. 설정 길잡이에서 기기가 재설정되거나 원격으로 삭제되었을 때 사용자에게 조치를 취하라는 메시지가 표시됩니다.

활성화 잠금은 감독 기기의 도난을 방지할 수 있는 더 많은 옵션을 관리자에게 제공합니다. 그러나 활성화 잠금은 주로 소비자 기능이기 때문에 대부분의 기업 관리자가 이 기능을 비활성화하는 경향이 있습니다. 다음 표는 기업 책임 배포용 옵션을 요약한 것입니다.

| 기기 유형 | 결과 |
| --- | --- |
| 기업 책임 및 감독 | • 활성화 잠금은 기본적으로 감독 기기에 대해 비활성화됩니다.<br>• 기기 사용자는 활성화 잠금을 켤 수 없습니다. |
| 기업 책임 및 비감독 | • 활성화 잠금은 최종 사용자가 Apple ID로 iCloud에 로그인하여 내 기기 찾기를 켜자마자 활성화됩니다.<br>• MDM용 Ivanti Neurons을 포함한 MDM 서버는 비감독 대상 기기에서 활성화 잠금을 제어할 수 없습니다. 기기 사용자는 자신의 사용자 정보로 활성화를 잠금으로써, 회사에 의지하지 않아도 됩니다. |

## iOS 활성화 잠금 활성화

**적용 대상:** iOS 7+ 감독 기기

이 구성은 내 찾기 기능이 활성화된 감독 기기(iOS 7 이상)에 적용됩니다. 관리자나 다른 사용자가 기기를 삭제하거나 활성화하거나, 내 기기 찾기 기능을 비활성화하려고 시도할 경우 Apple 활성화 잠금 화면이 표시됩니다. 진행하려면 iTunes 자격 증명이나 우회 코드를 입력해야 합니다.

감독 기기의 우회 코드는 활성화와 함께 저장되며 기기 세부 정보에서 확인할 수 있습니다. 우회 코드는 감독 기기의 '활성화 잠금 삭제' 명령을 이용해서 원격으로 전송할 수 있습니다. 그러나 기기를 다시 활성화하거나 내 기기 찾기 기능을 끌 때는 코드를 직접 입력해야 합니다.

> 모든 공간에 대해 하나의 활성화 잠금 구성만 만들 수 있습니다.

## 감독 기기에서 iOS 활성화 잠금 기능 활성화

**절차**

1. 기기에서 **내 찾기** 기능을 활성화합니다.
2. **구성**으로 이동합니다.
3. 기존 구성 목록에서 **Apple 활성화 잠금** 구성을 선택합니다.
4. **편집**을 클릭합니다.
5. iOS 7+ 감독 섹션에서 **활성화 잠금 활성화**를 클릭합니다.
6. **완료**를 클릭하세요.
7. 기기를 등록합니다.

## macOS 활성화 잠금 활성화

**적용 대상:** macOS 10.15+ 감독 기기

이 구성은 감독 기기 macOS 10.15 이상에 적용됩니다. macOS의 활성화 잠금은 Apple T2 보안 칩이 있는 Mac에만 적용됩니다. 업그레이드되거나 새로 설치되었는지 여부에 관계없이 감독 기기 및 현재 등록된 업데이트 기기에서 활성화 잠금은 기본적으로 해제되어 있습니다. 내 기기 찾기를 활성화해도 이 기기에서 활성화 잠금이 자동으로 활성화되지 않습니다.

관리자나 다른 사용자가 기기를 삭제하거나, 활성화하거나, 내 찾기 기능을 비활성화하려고 시도할 경우 Apple 활성화 잠금 화면이 표시됩니다. 진행하려면 iTunes 자격 증명이나 우회 코드를 입력해야 합니다. 감독 기기의 우회 코드는 활성화와 함께 저장되며 기기 세부 정보에서 확인할 수 있습니다. 우회 코드는 감독 기기의 '활성화 잠금 삭제' 명령을 이용해서 원격으로 전송할 수 있습니다. 그러나 기기를 다시 활성화하거나 내 찾기 기능을 끌 때는 코드를 직접 입력해야 합니다.

> 모든 공간에 대해 하나의 활성화 잠금 구성만 만들 수 있습니다.

## 감독 기기에서 macOS 활성화 잠금 기능 활성화

**절차**

1. 기기에서 내 찾기 기능을 활성화합니다.
2. **구성**으로 이동합니다.
3. 기존 구성 목록에서 **Apple 활성화 잠금** 구성을 선택합니다.
4. **편집**을 클릭합니다.
5. macOS 10.15+ 감독 섹션에서 **활성화 잠금 활성화**를 클릭합니다.
6. **완료**를 클릭하세요.
7. 기기를 등록합니다.

## iOS 활성화 잠금 우회 코드 사용

iOS 활성화 잠금이 활성화된 상태에서 기기가 지워지는 경우, 우회 코드가 Apple 활성화 서버 및 MDM용 Ivanti Neurons 관리자 인터페이스에 유지됩니다.

**절차**

1. **기기**로 이동합니다.
2. 원하는 장치를 선택하세요.
3. **작업 > 지우기**를 클릭합니다. 기기를 다시 시작하는 데 몇 분이 소요될 수 있습니다.

4. 기기에서 Apple ID와 비밀번호를 입력하라는 메시지가 표시되면 **Apple ID**를 비워둡니다.
5. **비밀번호** 필드에 우회 코드를 입력합니다.
6. **다음**을 클릭합니다.
7. 설정으로 진행합니다.

## iOS 활성화 잠금 우회 코드 삭제

iOS 활성화 잠금이 MDM용 Ivanti Neurons 관리자 인터페이스에서 삭제되면 우회 코드가 Apple 활성화 서버에서 제거되지만, MDM용 Ivanti Neurons 관리자 인터페이스의 기기 세부 정보에는 여전히 남아 있습니다.

**절차**

1. **기기**로 이동합니다.
2. 원하는 장치를 선택하세요.
3. **구성**을 선택합니다.
4. **Apple 활성화 잠금**을 선택합니다.
5. **편집**을 클릭합니다.
6. iOS 7+ 감독 섹션에서 **활성화 잠금 활성화**를 비활성화합니다.
7. **완료**를 클릭하세요.
8. **기기**로 이동합니다.
9. 원하는 장치를 선택하세요.
10. **작업 > 지우기**를 클릭합니다. 기기를 다시 시작하는 데 몇 분이 소요될 수 있습니다. 이제 새 사용자의 AppleID와 비밀번호로 기기가 설정될 수 있습니다.
11. 설정으로 진행합니다.

iOS 활성화 잠금 삭제 상태가 다음과 같이 인터페이스에 표시됩니다.

| 상태 | 결과 |
| --- | --- |
| 보류 중 | • 서버가 활성화 잠금 삭제 코드를 Apple에 전송하고 있습니다. |
| 보냄 | • Apple이 활성화 잠금 삭제 코드 확인을 승인합니다. |
| 실패함 | • 서버가 Apple에 코드를 전송하지 못했습니다.<br>• Apple이 오류를 보고했습니다. |

# 10.10.4.24. iOS 사용자 지정 구성

iOS 사용자 지정 구성을 하면 Apple의 아이폰 구성 유틸리티 등 다른 앱에서 생성된 iOS 구성 프로필을 업로드하고 배포할 수 있습니다.

## iOS 사용자 지정 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 파일 데이터 | 해당 구성 파일을 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택할 수 있습니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.25. 인텔리전스 설정

인텔리전스 설정을 사용하여 감독 모드 기기에서 Apple Intelligence 설정을 구성합니다. 이 선언을 통해 관리자는 기기가 Apple Intelligence 기능에 액세스하고 이를 사용하는 방식을 관리하는 일관된 정책 기반 제어를 적용할 수 있습니다.

**적용 대상**:

- iOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- macOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- visionOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **인텔리전스 설정** 구성을 검색하여 선택합니다.
3. 다음 표에 따라 **인텔리전스 설정**을 구성합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| Apple Intelligence 보고서 허용 | 확인란을 선택하여 Apple Intelligence 보고서를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 Apple Intelligence 보고서를 활성화합니다. |
| 젠모지 허용 | 확인란을 선택하여 젠모지를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 젠모지를 활성화합니다. |
| 이미지 플레이그라운드 허용 | 확인란을 선택하여 이미지 플레이그라운드를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 이미지 플레이그라운드를 활성화합니다. |
| 이미지 완드 허용 | 확인란을 선택하여 이미지 완드를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 이미지 완드를 활성화합니다.<br>이 설정은 macOS 기기에는 적용되지 않습니다. |
| 개인 맞춤 손글씨 결과 허용 완드 | 확인란을 선택하여 개인화된 필기 결과 완드를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 개인화된 필기 결과 완드를 활성화합니다.<br>이 설정은 macOS 및 visionOS 기기에는 적용되지 않습니다. |
| 비주얼 인텔리전스 요약 허용 | 확인란을 선택하여 비주얼 인텔리전스 요약을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 비주얼 인텔리전스 요약을 활성화합니다.<br>이 설정은 macOS 및 visionOS 기기에는 적용되지 않습니다. |
| 쓰기 도구 허용 | 확인란을 선택하여 쓰기 도구를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 쓰기 도구를 활성화합니다. |
| 기기 내 전용 받아쓰기 강제 | 확인란을 선택하여 기기 내 전용 받아쓰기를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 기기 내 전용 받아쓰기를 활성화합니다. |
| 기기 내 전용 번역 강제 | 확인란을 선택하여 기기 내 전용 번역을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 기기 내 전용 번역을 활성화합니다.<br>이 설정은 macOS 및 visionOS 기기에는 적용되지 않습니다. |
| **앱**<br><br>**달력**<br><br>자연어 편집 허용<br><br>**메일**<br><br>스마트 회신 허용 | <br><br><br><br>확인란을 선택하여 달력 및 미리 알림에서 자연어 편집을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기의 달력 및 미리 알림에서 자연어 편집을 활성화합니다.<br><br><br>확인란을 선택하여 스마트 회신을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 스마트 회신을 활성화합니다. |
| 요약 허용 | 확인란을 선택하여 요약을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 요약을 활성화합니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| **메모** | |
| 전사 허용 | 확인란을 선택하여 전사를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 전사를 활성화합니다.<br>이 설정은 visionOS 기기에는 적용되지 않습니다. |
| 전사 요약 허용 | 확인란을 선택하여 전사 요약을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 전사 요약을 활성화합니다.<br>이 설정은 visionOS 기기에는 적용되지 않습니다. |
| **Safari** | |
| 요약 허용 | 확인란을 선택하여 요약을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 요약을 활성화합니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **인텔리전스 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.26. iOS 제한

iOS 제한은 기기의 기본 사용자가 iOS, watchOS 및 visionOS 기기에서 다른 사용자가 수행할 수 있는 작업을 제어하는 데 도움이 되는 설정입니다. 이러한 설정은 Apple이 정의하고 MDM용 Ivanti Neurons에서 관리합니다.

이 구성을 **공유 iPad**로 배포하는 동안 기기 채널 또는 사용자 채널을 선택할 수 있습니다. 이는 별도의 구성을 배포하고 기기나 사용자 채널에만 해당되는 제한을 실행하기에 유용합니다.

전역 관리자는 공간 관리자에게 **모든 장치 및 사용자 지정 배포** 옵션 구성을 편집하도록 위임할 수 있습니다. iOS 제한 구성의 경우 **이 구성을 모든 공간에서 사용할 수 있도록 허용** 옵션을 선택할 수 있습니다.

> 배포 변경 사항은 특정 공간에만 적용됩니다. 기타 모든 공간은 계속 기본 공간 배포 설정을 상속합니다.

## iOS 제한 설정

| 범주 | 설정 항목 | 수행 작업 |
|---|---|---|
| | 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| | 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 기기 기능 | **모든 iOS 버전** | **기기 기능 사용을 활성화합니다.** |
| | 스크린샷 및 화면 녹화 허용 | 기기 사용자가 내장 iOS 화면 캡처 기능을 이용해 화면 캡처를 할 수 있도록 설정할 수 있습니다. |
| | 원격 화면 관찰 허용 (iOS 9.3 이상) | 사용자가 원격 화면을 관찰할 수 있도록 설정할 수 있습니다. |
| | 요청하지 않은 관리되는 교실 화면 관찰 강제 허용(감독 전용 - iOS 10.3+) | (iPad에만 적용) 감독 iPad가 관리되는 수업으로 구성되었을 때 화면에 표시하지 않은 메시지를 표시하도록 허용하려면 선택합니다. |
| | 로밍하는 동안 자동 동기화 허용 | 기기가 해외에서 사용될 때 메일 계정 동기화가 허용되도록 설정할 수 있습니다. |
| | Siri 허용 | 지원 기기에서 PA(개인비서 기능) 앱이 허용되도록 설정할 수 있습니다. |
| | 기기가 잠겨 있는 동안 Siri 허용 | 기기가 잠금 설정된 상태에서도 PA 앱에서 작업 수행이 허용되도록 설정할 수 있습니다. |
| | Siri 불경 필터를 활성화합니다(감독 전용). | Siri 불경 필터를 활성화하도록 설정할 수 있습니다. |
| | 음성 다이얼링 허용 | 사용자가 음성으로 기기에 연락처나 전화번호를 불러 전화를 걸 수 있도록 설정할 수 있습니다. |
| | 앱에서 구매 허용 | 사용자가 기기에 실행 중인 앱을 통해 구매를 할 수 있도록 설정할 수 있습니다. |
| | 기기가 잠겨 있는 동안 패스북 허용 | 기기가 잠금 설정 상태일 때 패스북 알림 표시가 허용되도록 설정할 수 있습니다. |
| | 잠금 화면 제어 센터 허용 | 잠금 화면에서 제어 센터 접속이 허용되도록 설정할 수 있습니다. |
| | 잠금 화면 알림 보기 허용 | 잠금 화면에 알림 표시가 허용되도록 설정할 수 있습니다. |
| | 잠금 화면 오늘 보기 허용 | 잠금 화면에서 오늘 보기 접속이 허용되도록 설정할 수 있습니다. |
| | 관리되는 앱에서 관리되지 않는 앱으로 열기 허용 | **Gold 라이센스가 필요합니다.**<br>관리 상태인 앱과 계정의 문서가 비관리 상태인 앱과 계정에서 열리도록 설정할 수 있습니다. 이 옵션을 해제하면 관리 상태인 앱 및 계정과 비관리 상태인 앱 및 계정 간 문서 전송이 차단됩니다. 예를 들어, 개인 앱을 통해 회사 문서가 열리는 것을 원하지 않는 경우 이 옵션(사용 안 함)을 관리되는 도메인 구성과 함께 사용하여 관리되는 도메인에서 다운로드된 데이터가 관리 앱에서만 열리도록 할 수 있습니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 관리되지 않는 앱에서 관리되는 앱으로 열기 허용 | **Gold 라이센스가 필요합니다.**<br>비관리 상태인 앱과 계정의 문서를 관리 상태인 앱과 계정에서 열리도록 설정할 수 있습니다. 이 옵션을 해제하면 관리 상태인 앱 및 계정과 비관리 상태인 앱 및 계정 간 문서 전송이 차단됩니다. 예를 들어, 사용자가 회사 이메일로 개인 문서를 보내지 않도록 하려면 이 옵션(끄기)을 관리되는 도메인 구성과 함께 사용하여 관리되지 않는 도메인에서 다운로드된 데이터가 관리되는 앱에서 열리지 않도록 할 수 있습니다. |
| | 최초 AirPlay 페어링에서 암호 요구 | 기기의 초기 페어링 권한을 부여하기 위해 사용자가 iOS 기기에 입력해야 하는 암호를 Apple TV에서 나타내도록 설정할 수 있습니다. |
| | AirPlay 수신 요청 시 비밀번호 강요(tvOS 최대 10.1) | 모든 AirPlay 수신 요청 시 사용자가 비밀번호를 입력하도록 설정할 수 있습니다.<br>기본값: 선택 해제 |
| | **iOS 26+** | |
| | 등급 제한에서 제외된 앱(iOS 26.1+ 기기에 적용) | 연령 기반 등급 제한에서 제외할 앱 목록은 번들 ID가 여러 페이로드의 모든 예외 목록과, 화면 시간제한과 같은 자녀 보호 앱의 교집합에 포함된 경우에만 입력해야 합니다.<br>기본값: 선택됨 |
| | **모든 iOS 버전 감독** | |
| | Apple Books 허용 | 사용자가 Apple Books 앱에 액세스할 수 있도록 설정할 수 있습니다. |
| | iBooks Store에서 노골적인 성적 컨텐츠 허용(iOS 및 tvOS 11.3 이상) | 사용자가 iBooks store 도서 중 외설서로 표시된 도서를 다운로드할 수 있도록 설정할 수 있습니다. |
| | 계정 수정 허용 | 관리 상태인 iOS 7 기기 사용자가 이메일 계정을 추가로 등록하고 기존 이메일 구성을 변경할 수 있도록 설정할 수 있습니다. |
| | 앱 휴대폰 데이터 수정 허용 | 사용자가 앱의 휴대폰 데이터 설정을 변경할 수 있도록 설정할 수 있습니다. |
| | 내 친구 찾기 수정 허용 | 사용자가 내 친구 찾기 앱 설정을 변경할 수 있도록 설정할 수 있습니다. |
| | 비 구성자 호스트와 연결 허용 | iTunes 동기화를 위해 호스트 페어링이 허용되도록 설정할 수 있습니다. 이 옵션을 설정하면 관리 상태인 기기가 관리 호스트 이외 Mac의 iTunes와의 동기화가 가능해집니다. 이 옵션을 해제하면 관리 호스트를 제외한 모든 호스트 페어링이 불가능해집니다. 구성된 관리 호스트 인증서가 없는 경우에는 모든 페어링이 불가능합니다. |
| | AirDrop 허용 | 기기에서 AirDrop 사용이 허용되도록 설정할 수 있습니다. AirDrop은 가까운 위치에 있는 사용자와 파일을 공유할 수 있는 Apple의 Ad Hoc Wi-Fi 시스템입니다. 이 기능을 제한하면 민감한 문서가 인가되지 않은 기기나 보안 설정이 되지 않은 기기에 노출되는 것을 방지할 수 있습니다. |
| | 기기 잠금 해제 시 터치 ID/Face ID 허용 | 기기 잠금 해제 시 터치 ID/Face ID를 허용하도록 설정할 수 있습니다. |

| 범주 | 설정 항목 | 수행 작업 |
|---|---|---|
| | Spotlight 검색으로 인터넷 검색 결과 반환 허용 | 내부 검색으로 인터넷 검색 결과를 리턴할 수 있도록 설정할 수 있습니다. |
| | 단일 앱 모드에서 앱 허용 | iOS 감독 기기에서 자동으로 단일 앱 모드로 진입할 수 있는 앱의 번들 ID 목록을 쉼표로 구분하여 입력합니다. 예를 들어, 학생용 커스텀 시험 앱을 설정할 수 있습니다. 학생이 앱을 실행하면 앱은 바로 단일 앱 모드로 진입하므로 시험을 치르는 동안 다른 리소스를 사용할 수 없습니다. 이 기능은 자동 단일 앱 모드용으로 개발된 앱에 적용됩니다. 관리 설정은 Apple Configurator로 이루어집니다. |
| | **iOS 8+** | |
| | 엔터프라이즈 도서 백업 허용 | MDM을 사용하여 기기에 푸시되는 iBooks, ePub, PDF 문서의 개인 백업을 허용하도록 설정할 수 있습니다. |
| | 엔터프라이즈 도서 메모 및 하이라이트 표시 동기화 허용 | 엔터프라이즈 도서에 추가된 메모와 하이라이트 표시를 iTunes에 동기화하도록 설정할 수 있습니다. |
| | 강제 Apple Watch 손목 감지 | 누군가 Apple Watch를 사용하고 있지 않는 한, 화면 알림에 숨길 수 있도록 설정할 수 있습니다. |
| | **iOS 8+ 감독** | |
| | 키 입력 예측 허용 | 사용자가 입력하고 있는 단어의 iOS 예측을 활성화하도록 허용하여, 사용자가 세 개의 예측 중 한 개를 눌러 단어를 완성하도록 설정할 수 있습니다. |
| | 키보드 자동 수정 허용 | 사용자가 블루투스 키보드로 자동 수정을 사용하도록 설정할 수 있습니다. |
| | 키보드 철자 확인 허용 | 사용자가 블루투스 키보드로 철자 확인을 사용하도록 설정할 수 있습니다. |
| | 키보드 정의 검색 허용 | 사용자가 블루투스 키보드로 정의 검색이 가능하도록 설정할 수 있습니다. |
| | 터치 ID 지문/Face ID 얼굴 수정 허용 | 사용자가 터치 ID 또는 Face ID 설정을 변경할 수 있도록 설정할 수 있습니다. |
| | **iOS 9+ 감독** | |
| | iPad의 키보드 바로 가기 허용 | iPad에서 키보드 바로 가기 사용이 허용되도록 설정할 수 있습니다. |
| | 배경화면 수정 허용 | 사용자가 배경화면 이미지를 변경할 수 있도록 설정할 수 있습니다. |
| | Apple Watch와의 페어링 허용 | 사용자가 iPhone과 Apple Watch 페어링을 사용할 수 있도록 하려면 선택합니다. |
| | 기기 이름 수정 허용 | 사용자가 기기 이름을 변경할 수 있도록 설정할 수 있습니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 엔터프라이즈 앱 신뢰 설정 수정 허용 | 사용자가 엔터프라이즈 앱 신뢰 설정을 변경할 수 있도록 설정할 수 있습니다. |
| | **iOS 9.3+ 감독** | |
| | 알림 설정 수정 허용 | 사용자가 알림 설정을 변경할 수 있도록 설정할 수 있습니다. |
| | **iOS 9.3.2+ 감독** | |
| | 진단 전송 수정 허용 | 사용자가 Apple에 진단 데이터 전송 관련 설정을 변경할 수 있도록 설정할 수 있습니다. |
| | **iOS 10+ 감독** | |
| | Bluetooth 수정 허용 | 사용자가 감독 기기에서 Bluetooth 설정을 수정하도록 설정할 수 있습니다. 앱을 실행할 때 블루투스가 필요한 교육용 Classroom 앱에 공유 iPad를 사용하는 등의 경우에 유용합니다. |
| | **iOS 10.3+ 감독** | |
| | 받아쓰기 허용 | 사용자가 입력 대신 말로 iPhone이나 iPad에 지시를 내리게 하려면 선택합니다. |
| | **iOS 11+ 감독** | |
| | AirPrint 허용 | 무선 인쇄에 대해 AirPrint 기능을 허용하도록 설정할 수 있습니다. |
| | AirPrint 자격 증명 저장 | AirPrint에 대한 사용자 이름 및 비밀번호의 키체인 저장을 허용하도록 설정할 수 있습니다. |
| | Airprint iBeacon 검색 허용 | 사용자가 AirPrint 프린터의 iBeacon 검색을 설정하도록 설정할 수 있습니다. |
| | VPN 구성 추가 허용 | 사용자가 VPN 구성을 생성할 수 있도록 선택합니다. |
| | Airprint 신뢰할 수 있는 TLS 요구 사항 강제 | TLS 인쇄 통신에 대해 신뢰할 수 있는 인증서를 허용하도록 설정할 수 있습니다.<br>기본값: 선택 해제 |
| | 시스템 앱 제거 허용 | 시스템 앱을 제거할 수 있도록 선택합니다. |
| | 요금제 설정 수정 허용 | 사용자가 휴대폰 요금제 설정을 수정할 수 있도록 선택합니다. |
| | 새 주변 기기 설정 허용 | 사용자가 새 인접 기기를 설정할 수 있도록 선택합니다. |
| | 메시지를 표시하지 않고 Classroom 수업에 자동으로 참여 | 메시지를 표시하지 않고 사용자가 Classroom 수업에 자동으로 참여할 수 있도록 선택합니다.<br>기본값: 선택 해제 |
| | 메시지를 표시하지 않고 앱 잠금 및 기기 잠금에 Classroom 허용 | 사용자에게 메시지를 표시하지 않고 앱 잠금 및 기기 잠금에 Classroom을 허용하도록 선택합니다.<br>기본값: 선택 해제 |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | Safari 및 앱에서 암호 또는 신용카드 정보를 자동 완성하기 전에 사용자 강제 인증 | 장치 소유자가 Safari 브라우저와 애플리케이션에서 암호나 신용카드 정보를 자동 입력하려면 우선 인증을 완료해야 합니다.<br>기본값: False |
| | **iOS 11.3+** | |
| | Remote 앱과의 페어링 허용(tvOS 11.3 이상) | 사용자가 기기와 원격 앱 페어링을 사용할 수 있도록 설정할 수 있습니다. |
| | AirPlay 수신 요청 허용(tvOS 11.3 이상) | AirPlay 수신 요청을 허용하도록 설정할 수 있습니다. |
| | **iOS 11.3+ 감독** | |
| | USB 제한 모드 허용 | 사용자가 USB 제한 모드를 액세스할 수 있도록 설정할 수 있습니다. |
| | 30일 동안 소프트웨어 업데이트 연기(iOS 11.3, tvOS 12.2 이상 감독 기기 전용인 경우) | 선택하여 소프트웨어 업데이트를 연기할 일수를 입력합니다. 기본값은 30일이며 최대 90일까지 가능합니다.<br>기본값: 선택 해제 |
| | Classroom 비관리 수업을 나가려면 교사 권한 필요 | Classroom 비관리 수업을 나가기 위해 사용자에게 필요한 교사 권한을 부여하도록 선택합니다. |
| | iOS 12+ 감독 | |
| | 강제 자동 날짜 및 시간(iOS 12.0 및 tvOS 12.2 이상) | 날짜 및 시간 "자동 설정" 기능 켜기를 선택합니다. 사용자가 끌 수 없습니다.<br>기본값: False |
| | eSIM 설정 수정 허용(iPhone XS, iPhone XS Max 및 iPhone XR - iOS 12.1 이상 버전) | 사용자가 지원되는 기기에서 eSim 구성을 수정하도록 설정할 수 있습니다. 이 옵션은 사용자가 기기의 설정에서 요금제 설정을 추가 또는 제거하지 못하도록 차단하기도 합니다.<br>기본: True |
| | **iOS 12.2+ 감독** | |
| | 개인 핫스팟 설정 수정 허용 | 사용자가 개인 핫스팟 설정을 수정하도록 설정할 수 있습니다.<br>기본: True |
| | **iOS 13.0+** | |
| | 파일 앱 네트워크 드라이브 액세스 허용 | 사용자가 Files 앱의 네트워크 드라이브에 연결할 수 있도록 설정할 수 있습니다.<br>기본: True |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 파일 USB 드라이브 액세스 허용 | 사용자가 Files 앱의 연결된 USB 기기에 연결할 수 있도록 설정할 수 있습니다.<br>기본: True |
| | **iOS 13.0+ 감독** | |
| | 연속 경로 키보드 허용 | 연속 경로 키보드를 활성화하려면 선택합니다(스와이프 또는 입력 추적).<br>기본: True |
| | 기기 절전 허용 | 기기 절전 기능을 활성화하려면 선택합니다.<br>기본: True |
| | 기기 찾기 허용 | 내 앱 찾기에서 내 기기 찾기를 활성화하려면 선택합니다.<br>기본: True |
| | 내 친구 찾기 허용 | 내 앱 찾기에서 내 친구 찾기를 활성화하려면 선택합니다.<br>기본: True |
| | WiFi 전원 강제 켜기 | Wi-Fi 전력이 켜진 상태로 유지하려면 선택합니다.<br>기본값: False |
| | **iOS 13.4+** | |
| | 공유 iPad에 대한 게스트 세션 허용 | false인 경우 공유 iPad에서 임시 세션을 사용할 수 없습니다.<br>기본: True |
| | **iOS 14.0+** | |
| | Apple 맞춤 광고 허용 | False인 경우 Apple 맞춤 광고를 제한합니다. 이로 인해 Apple은 광고를 목적으로 사용자 정보를 사용할 수 없습니다. 이로써 수신되는 광고 수가 줄어드는 것이 아니라 광고와 사용자 간 관련성이 줄어들 수 있습니다.<br>기본: True |
| | **iOS 14.0+ 감독** | |
| | 앱 클립 허용 | false인 경우 사용자가 앱 클립을 추가할 수 없으며 기기에 있는 기존의 앱 클립이 제거됩니다.<br>기본: True |
| | **iOS 14.2+ 감독** | |
| | NFC 허용 | false인 경우 NFC를 비활성화합니다. 감독 기기가 필요합니다. iOS 14.2 이상에서 사용 가능합니다.<br>기본: True |
| | **iOS 14.5+** | |
| | 자동 잠금 해제 허용 | 관리자는 기존 allowAutoUnlock 제한을 사용하여 이 기능을 관리할 수 있습니다. False인 경우 자동 잠금 해제를 허용하지 않습니다. macOS 10.12 이상 및 iOS 14.5 이상에서 사용 가능합니다.<br>기본: True |
| | 강제 기기 전용 받아쓰기 | True인 경우 받아쓰기 목적으로 Siri 서버에 연결할 수 없습니다.<br>기본: False |

| 범주 | 설정 항목 | 수행 작업 |
|---|---|---|
| | **iOS 14.5+ 감독** | |
| | 복구를 위한 페어링되지 않은 외부 부팅 허용 | True인 경우 페어링되지 않은 기기를 통해 기기를 부팅하여 복구할 수 있습니다.<br>기본: False |
| | 허용된 네트워크에만 Wi-Fi 강제 연결 | True인 경우 구성 프로필을 통해 Wi-Fi 네트워크 설정만 조인하도록 기기를 제한합니다.<br>기본: False<br>**허용된 네트워크에만 Wi-Fi 강제 연결** 제한이 활성화되고 Wi-Fi 구성이 기기에 배포되지 않은 경우 Wi-Fi 연결이 해제됩니다. |
| | **iOS 15+** | |
| | 강제 기기 전용 번역 | True인 경우 기기는 번역 목적을 위해 Siri 서버에 연결되지 않습니다.<br>기본: False |
| | 관리 임시 보드 필요 | True인 경우 복사 및 붙여넣기 기능은 allowOpenFromManagedToUnmanaged 및 allowOpenFromUnmanagedToManaged 제한을 사용합니다.<br>기본: False |
| | **iOS 15.2+** | |
| | 메일 개인 정보 보호 허용 | false인 경우 기기의 메일 개인 정보 보호를 비활성화합니다. iOS 15.2 이상에서 사용 가능합니다.<br>메일 개인 정보 보호 허용 구성이 MDM용 Ivanti Neurons 관리 포털에서 설치 및 활성화된 경우 기기에서 메일 활동 보호 토글이 활성화되며 다음 옵션이 표시됩니다.<br>• **IP 주소 숨기기** - 이메일 발신자가 이메일을 사용자의 온라인 활동에 연결하거나 사용자의 위치를 파악할 수 없습니다<br>• **모든 원격 콘텐츠 차단** - 이메일 발신자가 사용자의 이메일 활동을 볼 수 없습니다<br>기본: True |
| | **iOS 15.4+** | |
| | Apple TV의 자동 화면 보호기 허용(tvOS 15.4 이상) | false일 경우 Apple TV의 자동 화면 보호기가 비활성화됩니다. tvOS 15.4 이상에서 사용 가능합니다.<br>기본: True |
| | **iOS 16.0~26.0** | |
| | 백그라운드 보안 개선 설치 허용 | 응답을 비활성화합니다. 사용자가 백그라운드 보안 개선을 설치할 수 없습니다. |
| | 백그라운드 보안 개선 제거 허용 | 사용자가 응답의 실행을 취소할 수 없도록 차단합니다. 사용자가 백그라운드 보안 개선을 제거할 수 없습니다. |
| | **iOS 17.0+ 감독됨** | |
| | Mac 기기에서 iPhone 위젯 허용 | 두 기기 모두에서 iCloud용 iPhone의 동일한 AppleID를 사용하는 Mac 기기에 iPhone 위젯이 표시되도록 허용하려면 선택합니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | **iOS 17.2 이상 감독 대상 기기** | |
| | 실시간 음성 메일 허용 | 기기에서 실시간 음성 메일을 활성화하려면 선택합니다. |
| | 지울 때 ESIM 강제 보존 | 비밀번호 시도 실패 횟수가 너무 많거나 **설정** > **일반** > **재설정**에서 모든 콘텐츠 및 설정 지우기 옵션으로 인해 시스템이 기기를 지울 때 eSIM을 보존하려면 선택합니다.<br>**내 기기/정보 찾기**가 기기 지우기를 시작하는 경우 시스템은 eSIM을 보존하지 않습니다. |
| | **iOS 17.4 이상 감독 대상 기기** | |
| | Marketplace 앱 설치 허용 | 사용자가 대체 마켓플레이스에서 앱을 다운로드할 수 있도록 허용하려면 선택합니다. 이 제한을 false로 설정하면 사용자가 새로운 대체 마켓플레이스 앱과 해당 마켓플레이스에서 설치된 앱을 설치할 수 없습니다. |
| | 자동 밝기 조절 허용 | OLED 디스플레이가 탑재된 iPad에서 자동 밝기 조절 옵션을 허용하려면 선택합니다. |
| | **iOS 17.5 이상 감독 대상 기기** | |
| | 웹 배포 앱 설치 허용 | 이 **allowWebdistributionAppInstallation** 제한을 false로 설정하면 사용자가 새로운 대체 웹사이트에서 직접 앱을 설치할 수 없게 됩니다. 이는 감독 대상 기기에만 적용됩니다. |
| | **iOS 18.0 이상 감독 대상 기기** | |
| | eSIM 발신 전송 허용 | 제한이 설치된 기기가 아닌 다른 기기로 eSIM 전송을 허용하려면 선택합니다. |
| | 젠모지 허용 | 젠모지 생성을 허용하려면 선택합니다. |
| | 이미지 플레이그라운드 허용 | 이미지 생성의 사용을 허용하려면 선택합니다. |
| | 이미지 완드 허용 | 이미지 완드의 사용을 허용하려면 선택합니다. |
| | iPhone 미러링 허용 | iPhone이 macOS 기기에서 미러링하도록 허용하려면 선택합니다. |
| | 개인화된 손글씨 결과 허용 | 사용자의 필기를 사용하여 시스템이 텍스트를 생성하도록 허용하려면 선택합니다. |
| | 쓰기 도구 허용 | Apple Intelligence 쓰기 도구를 활성화하려면 선택합니다. |
| | 앱 숨김 허용 | 선택하여 앱 숨김을 허용합니다. |
| | 앱 잠금 허용 | 선택하여 앱 잠금을 허용합니다. |
| | **감독 대상인 iOS 18.1+** | |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 통화 녹음 허용 | 선택하여 통화 녹음을 허용합니다.<br>기본: True |
| | 메일 요약 허용 | 선택하여 이메일 메시지 요약을 수동으로 생성합니다.<br>기본: True |
| | RCS 메시징 허용<br><br>**감독 대상인 iOS 18.2+** | 선택하여 RCS 메시징을 허용합니다.<br>기본: True<br>iOS 26 기기와 iPadOS 26을 사용하는 셀룰러 iPad 모델에서 셀룰러 요금제가 ICCID와 연동된 기기의 경우 RCS Messaging 사용이 제한될 수 있습니다. |
| | 외부 인텔리전스 통합 허용 | 선택하여 Siri에서 외부 클라우드 기반 인텔리전스 서비스를 사용하도록 설정합니다. |
| | 외부 인텔리전스 통합 로그인 허용 | 선택하여 외부 인텔리전스 제공자를 익명 모드로 전환할 수 있도록 합니다. 사용자가 이미 외부 인텔리전스 제공자에 로그인한 경우 이 제한을 적용하면 로그아웃됩니다. |
| **애플리케이션** | 기본 브라우저 수정 허용<br><br>**모든 iOS 버전** | 선택하여 기본 브라우저 환경 설정 수정을 활성화합니다. MDM용 Ivanti Neurons 설정에서 기본 웹 브라우저를 설정할 수 있습니다.<br><br>기기의 애플리케이션에 대한 액세스를 활성화합니다. |
| | 앱 설치 허용 | 사용자가 Apple App Store에서 애플리케이션을 설치할 수 있도록 설정할 수 있습니다. 이 옵션을 선택 해제하면 App Store 기능이 해제되고 해당 아이콘이 홈 화면에서 제거됩니다. |
| | 카메라 사용 허용<br><br>Safari 사용 허용 | 사용자가 카메라 기능을 이용할 수 있도록 설정할 수 있습니다. 이 옵션을 선택 해제하면 카메라 기능이 해제되고 해당 아이콘이 홈 화면에서 제거됩니다.<br>iOS 26 이상 기기에서 앱이 예외 목록에 추가되면 카메라 허용 제한은 적용되지 않습니다.<br><br>Safari 웹 브라우저 사용이 허용되도록 설정할 수 있습니다. 이 옵션을 선택 해제하면 Safari 웹 브라우저 기능이 해제되고 해당 아이콘이 홈 화면에서 제거됩니다. 사용자들은 웹 클립을 실행할 수 없게 됩니다. |
| | 자동 채우기 활성화 | Safari에 표시되는 항목의 자동 채우기 기능을 설정할 수 있습니다. |
| | 사기 경고 강제 | 사기성이 있거나 손상된 것으로 인식되는 웹사이트를 사용자가 방문하지 못하도록 유도하는 메시지가 Safari에 표시되도록 설정할 수 있습니다. |
| | JavaScript 활성화 | Safari의 JavaScript 지원 기능을 설정할 수 있습니다. |
| | 팝업 차단 | Safari의 팝업이 차단되도록 설정할 수 있습니다. |
| **Safari** | **감독 모드 전용 - 버전 26 이상** | |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | Safari 기록 지우기 허용 | 사용자가 브라우징 기록을 지울 수 있도록 선택합니다. |
| | Safari 비공개 브라우징 허용 | 비공개 브라우징을 사용하도록 선택합니다. |
| | **모든 iOS 버전 감독** | |
| | 앱 제거 허용 | 사용자가 기기에서 앱을 제거하도록 설정할 수 있습니다. |
| | Game Center 사용 허용 | 게임 센터 접속이 허용되도록 설정할 수 있습니다. |
| | 게임 센터 친구 추가 허용 | 사용자가 게임 센터에 친구를 추가할 수 있도록 설정할 수 있습니다. |
| | 멀티플레이어 게임 허용 | 사용자가 여러 사용자가 참여하는 게임을 할 수 있도록 설정할 수 있습니다. |
| | iMessage 허용 | iMessage 사용이 허용되도록 설정할 수 있습니다.<br>iOS 26 기기와 iPadOS 26을 사용하는 셀룰러 iPad 모델의 경우는 기기가 거부된 목록에 추가되면 iMessage 사용을 제한할 수 있습니다. |
| | 쿠키 허용 | 항상 금지, 항상 허용, 방문 이력이 있는 사이트를 선택할 수 있습니다. |
| | FaceTime 허용 | 카메라 기능이 설정된 경우 사용자가 FaceTime을 실행할 수 있도록 설정할 수 있습니다.<br>iOS 26 기기와 iPadOS 26을 사용하는 셀룰러 iPad 모델의 경우는 기기가 거부된 목록에 추가되면 FaceTime을 제한할 수 있습니다. |
| | **iOS 8+** | |
| | 관리 중인 애플리케이션의 클라우드 동기화 사용 허용 | 관리되는 앱이 클라우드 동기화를 사용하도록 설정할 수 있습니다. |
| | 작업 지속 허용 | Handoff를 지원하는 앱에서 작업을 지속하도록 설정할 수 있습니다. |
| | **iOS 8+ 감독** | |
| | 팟캐스트 이용 허용 | 팟캐스트 사용이 허용되도록 설정할 수 있습니다. |
| | **iOS 9+** | |
| | 새 엔터프라이즈 앱 작성자 신뢰 허용 | 사용자가 새 엔터프라이즈 앱에 액세스할 수 있도록 설정할 수 있습니다. |
| | **iOS 9+ 감독** | |
| | App Store 허용 | 사용자가 Apple App Store에 액세스할 수 있도록 설정할 수 있습니다. |
| | 자동 앱 다운로드 허 | 사용자에게 메시지를 표시하여 앱이 파일, 데이터, 업데이트를 다운로드하도록 설정할 수 있습니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 용 | |
| | 새로운 앱 허용 | 새로운 앱의 사용을 허용하도록 설정할 수 있습니다. |
| | **iOS 9.3+ 감독** | |
| | iTunes Radio 허용 | iTunes Radio 사용이 허용되도록 설정할 수 있습니다. |
| | Apple Music 허용 | Apple Music 사용이 허용되도록 설정할 수 있습니다. |
| | 열거된 앱 번들 ID 허용 | 배열에 열거된 번들 ID만 표시되거나 시작할 수 있도록 허용합니다. 모든 웹클립을 허용하도록 com.apple.webapp 값을 포함합니다. |
| | 앱 번들 ID 차단 | 배열에 열거된 번들 ID가 표시되거나 시작하지 못하도록 방지합니다. 모든 웹클립을 제한하도록 com.apple.webapp 값을 포함합니다. |
| | **iOS 13.0+ 감독** | |
| | iTunes Store 사용 허용 | 사용자가 iTunes Music Store 기능을 이용할 수 있도록 설정할 수 있습니다. 이 옵션을 선택 해제하면 iTunes Music Store 기능이 해제되고 해당 아이콘이 홈 화면에서 제거됩니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| iCloud | 모든 iOS 버전 | iCloud 서비스에 대한 액세스를 활성화합니다. |
| | 백업 허용 | 기기가 Apple의 iCloud 서비스를 통해 데이터를 백업할 수 있도록 설정할 수 있습니다. |
| | 문서 동기화 허용 | Apple의 iCloud 서비스를 통해 문서 동기화가 허용되도록 설정할 수 있습니다. |
| | 사진 스트림 허용 | Apple iCloud를 통한 다른 iOS 기기와의 사진 동기화가 허용되도록 설정할 수 있습니다. |
| | 공유 사진 스트림 허용(허용하지 않을 경우 데이터가 손실될 수 있음) | 공유 사진 동기화가 허용되도록 설정할 수 있습니다.<br>이 옵션을 선택 해제하면 사진이 손실될 수 있습니다. |
| | 키체인 동기화 허용 | 키체인 동기화가 허용되도록 설정할 수 있습니다. |
| | **iOS 9+** | |
| | iCloud 포토 라이브러리 허용 | iCloud 포토 라이브러리에 대한 액세스를 허용하도록 설정할 수 있습니다. |
| | **iOS 15+ 감독** | |
| | Cloud 비공개 릴레이 허용 | False인 경우 iCloud 비공개 릴레이를 비활성합니다. 기본: True |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| **보안 및 개인정보 보호** | **모든 iOS 버전** | 보안 및 개인 정보 보호 정책을 활성화합니다. |
| | 무선 인증서 업데이트 허용 | 루트 인증서 무선 업데이트가 허용되도록 설정할 수 있습니다. |
| | 광고 추적 제한 강제 | 광고 추적 제한 기능 사용이 필요하도록 설정할 수 있습니다. |
| | **모든 iOS 버전 감독** | |
| | 구성 프로필 설치 허용 | 사용자가 구성 프로필과 인증서를 한번에 연동 설치할 수 있도록 설정할 수 있습니다. |
| | 지원 사용자 생성 컨텐츠 허용 | 웹에서 Siri가 사용자 생성 컨텐츠에 대해 쿼리를 실행할 수 있도록 설정할 수 있습니다. |
| | **iOS 8+ 감독** | |
| | 사용자가 초기화 UI의 컨텐츠 및 설정 값을 삭제하도록 허용 | 기기의 iOS 재설정 UI에서 "모든 컨텐츠 및 설정 삭제" 옵션을 활성화하도록 설정할 수 있습니다. |
| | 스크린 타임 허용 | 스크린 타임을 허용하려면 선택하십시오(설정 > 스크린 타임). |
| | 진단 데이터를 Apple에 전송 허용 | 진단 데이터가 자동으로 Apple에 전송되도록 설정할 수 있습니다. |
| | 사용자에게 신뢰할 수 없는 TLS 인증서 수용 허용 | 기기 사용자가 신뢰할 수 없는 HTTPS 인증서를 수락하도록 설정할 수 있습니다. 이 옵션을 선택하지 않으면 해당 기기는 신뢰할 수 없는 HTTPS 인증서를 사용자에게 알리지 않고 자동으로 거절하게 됩니다. |
| | 암호화된 백업 강제 | iTunes를 통한 암호화 백업이 필요하도록 설정할 수 있습니다. 이 옵션은 SCEP 규격에 따라 자동으로 선택됩니다. |
| | 사용자의 모든 거래에 대해 iTunes Store 비밀번호 입력 강제 | 기기 사용자가 App Store 거래마다 iTunes 비밀번호를 입력해야 하도록 설정할 수 있습니다. 이 옵션을 선택하지 않으면 기기 사용자는 단일 인증으로 여러 번의 거래를 할 수 있게 됩니다. |
| | **iOS 9+** | |
| | AirDrop을 미관리 대상으로 취급 | AirDrop 파일 공유에 대한 사용자 액세스를 허용하도록 설정할 수 있습니다.<br>기본값: False |
| | **iOS 9+ 감독** | |
| | 기기 암호 수정 허용 | 사용자가 기기의 암호를 변경할 수 있도록 설정할 수 있습니다. |
| | iOS 12+ | |
| | 관리되는 앱이 관리되지 않는 연락처 계정에 연락처를 쓸 수 있도록 허용 | 관리되는 앱이 관리되지 않는 연락처 계정에 연락처를 쓸 수 있게 허용하도록 선택합니다.<br>기본값: False |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | iOS 12+ 감독 | |
| | 비밀번호 자동 채우기 허용 | 사용자가 iOS에서 비밀번호 자동 입력 기능을 사용하고 Safari 또는 앱에서 저장된 비밀번호를 사용할 수 있게 지시를 받을 수 있게 허용하도록 선택합니다. |
| | 주변 기기의 비밀번호 요청 공유 허용 | 사용자의 기기가 주변 기기의 비밀번호를 요청할 수 있게 허용하도록 선택합니다. |
| | 비밀번호 공유 허용 | 사용자가 AirDrop 비밀번호 기능으로 비밀번호를 공유할 수 있게 허용하도록 선택합니다. |
| | 관리되지 않는 앱이 관리되는 연락처 계정에서 연락처를 읽을 수 있도록 허용 | 관리되지 않는 앱이 관리되는 연락처 계정에서 읽을 수 있게 허용하도록 선택합니다.<br>기본값: False |
| | iOS 18.3 | |
| | 외부 인텔리전스 작업 영역 ID 허용 | 외부 인텔리전스 작업 영역 ID를 입력합니다. |
| | 메모 받아쓰기 요약 허용 | 대화 기록에서 요약 생성을 활성화하려면 선택합니다.<br>기본: True |
| | 비주얼 인텔리전스 요약 허용 | Apple의 Visual Intelligence에서 이미지나 시각적 콘텐츠를 사용하여 요약 생성을 활성화하려면 선택합니다.<br>기본: True |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| **컨텐츠 등급** | | 앱 및 미디어에 대한 액세스를 제어합니다. |
| | 유해 음악, 팟캐스트 및 iTunes U 미디어 재생 허용(iOS 13+ 감독 전용 및 tvOS 11.3 이상) | 명시적(노골적) 컨텐츠는 iTunes Store를 통해 판매될 경우 음반 업체 등 해당 컨텐츠 제공업체가 해당 표시를 하도록 되어 있습니다. |
| | 등급 영역 | 드롭다운 목록에서 원하는 지역을 선택해 애플리케이션 및 TV 프로그램, 영화 관련 등급 선정 기준 지역을 변경할 수 있습니다. |
| | 동영상 | 기기에 저장된 영화의 등급 제한을 설정할 수 있습니다.<br>• 영화 비허용<br>• G<br>• PG<br>• PG-13<br>• R<br>• NC-17<br>• 모든 영화 허용 |
| | TV 프로그램 | 기기에 저장된 TV 프로그램의 등급 제한을 설정할 수 있습니다.<br>• TV 프로그램 비허용<br>• TV-Y<br>• TV-Y7<br>• TV-G<br>• TV-PG<br>• TV-14<br>• TV-MA<br>• 모든 TV 프로그램 허용 |
| | 앱 | 기기 애플리케이션의 등급 제한을 설정할 수 있습니다.<br>• 앱 비허용<br>• 4+<br>• 9+<br>• 12+<br>• 17+<br>• 모든 앱 허용 |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.27. 회의실 디스플레이

**적용 대상:** tvOS 10.2 및 지원되는 최신 버전.

이 구성은 Apple TV에서 회의실 디스플레이 모드를 켭니다. 회의실 디스플레이 모드에서는 Apple TV가 이 모드로 고정되므로 다른 종류의 사용이 금지됩니다.

tvOS 10.2부터는 관리 상태인 Apple TV 기기를 회의실 디스플레이 모드로 설정할 수 있습니다. 배경 이미지와 화면 보호기를 Apple TV 기기 설정에서 수동으로 정의하지 않은 한 회의실 디스플레이는 범위가 지정된 Apple TV 기기를 검정색 배경화면으로 고정하고 기본 화면 보호기를 다운로드합니다. 이 모드는 회의실 디스플레이 구성에서 구성한 대로 메시지를 표시할 수도 있습니다.

기기가 이 모드일 때는 회의실 디스플레이 구성이 자동으로 배포될 수 있고 앱이 설치될 수 있습니다. 재부팅하면 홈 화면이 먼저 나타나지 않고 잠금 화면을 자동으로 재개하는 회의실 디스플레이 모드로 설정된 기기입니다.

> Apple TV 기기가 단일 앱 모드로 실행되고 있거나 단일 앱 모드가 회의실 디스플레이와 함께 전개되는 경우에는 회의실 디스플레이가 단일 앱 모드를 재정의합니다. 또한, Apple TV 기기가 이더넷을 통해 네트워크에 연결된 경우 회의실 디스플레이는 AirPlay 공유를 위해 Wi-Fi 네트워크를 자동으로 표시하지 않습니다. 이러한 지침은 회의실 디스플레이 구성의 사용자 지정 메시지 필드를 사용하여 화면에 표시될 수 있습니다.

## 회의실 디스플레이 구성 만들기

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **회의**를 입력한 다음, **회의실 디스플레이** 구성을 클릭합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. **사용자 지정 메시지**를 지정합니다. 이것은 회의실 디스플레이 모드의 화면에 표시되는 사용자 지정 메시지입니다.
6. **다음**을 클릭해 배포 설정을 구성합니다.
7. **완료**를 클릭하세요.

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.4.28. 키보드 설정

**키보드 설정**을 사용하여 감독 모드 기기에서 키보드 설정을 구성합니다. 이 선언을 통해 관리자는 키보드 동작, 입력 옵션 및 관련 사용자 경험 설정을 관리하는 일관된 정책 기반 제어를 적용할 수 있습니다.

**적용 대상**:

- iOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- macOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **키보드 설정** 구성을 검색하여 선택합니다.
3. 다음 표에 따라 **키보드 설정**을 구성합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 자동 수정 허용 | 확인란을 선택하여 자동 수정을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 자동 수정을 활성화합니다.<br>이 설정은 macOS 기기에는 적용되지 않습니다. |
| 정의 조회 허용 | 확인란을 선택하여 정의 조회를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 정의 조회를 활성화합니다. |
| 받아쓰기 허용 | 확인란을 선택하여 받아쓰기를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 받아쓰기를 활성화합니다. |
| 수학 키보드 제안 허용 | 확인란을 선택하여 수학 키보드 제안을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 수학 키보드 제안을 활성화합니다. |
| 예측 텍스트 허용 | 확인란을 선택하여 예측 텍스트를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 예측 텍스트를 활성화합니다.<br>이 설정은 macOS 기기에는 적용되지 않습니다. |
| 슬라이드 입력 허용 | 확인란을 선택하여 슬라이드 입력을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 슬라이드 입력을 활성화합니다.<br>이 설정은 macOS 기기에는 적용되지 않습니다. |
| 맞춤법 검사 허용 | 확인란을 선택하여 맞춤법 검사를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 맞춤법 검사를 활성화합니다.<br>이 설정은 macOS 기기에는 적용되지 않습니다. |
| 텍스트 대체 허용 | 확인란을 선택하여 텍스트 대체를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 텍스트 대체를 활성화합니다.<br>이 설정은 macOS 기기에는 적용되지 않습니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **키보드 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.29. 잠금 및 키오스크: Android 기기 관리 모드

락다운 및 키오스크: Android 관리자 모드 구성은 Android 장치의 특정 기능을 비활성화하며 키오스크 모드에서 사용자가 사용할 수 있는 앱의 허용 목록을 생성합니다.

> Android 장치 관리 모드 구성은 더 이상 사용되지 않으며 Android 8 이상 버전의 장치에서 지원되지 않습니다. Android 8 이상 버전에서 키오스크 잠금에 Android Enterprise 잠금을 사용하는 것이 좋습니다.

Android 기기가 키오스크 모드일 때 설정 또는 앱을 수정하는 옵션을 제한할 수 있습니다.

- 잠금 및 키오스크 생성에서 앱을 추가하고 설정을 선택합니다. Android 기기 관리자 모드 구성 페이지.
- 설정 아이콘으로 설정을 변경하는 기능을 키오스크에서 이용할 수 있습니다.
- 설정 구성 옵션을 선택하지 않고 앱을 선택하면 설정 아이콘이 키오스크 모드에 표시되지 않습니다.
- 구성에 아무 앱도 추가하지 않기로 했다면 설정 아이콘이 표시됩니다.

| 설정 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **잠금 설정:** 모든 Android 기기용 기능을 비활성화합니다. | |
| Wi-Fi 비활성화 | 무선 랜 기능을 끌 수 있습니다. |
| 카메라 비활성화 | 카메라 기능을 끌 수 있습니다. |
| Bluetooth 비활성화 | Bluetooth 기능을 끌 수 있습니다.<br>이 기능을 사용할 때는 주의가 필요합니다. Ivanti에서는 핸즈프리 Bluetooth 기능이 지원되지 않으므로 오디오를 끄지 않는 것이 좋습니다. 운전 중 핸즈프리 기기 사용과 관련한 법적 요건의 적용 범위가 더욱 확대되고 있습니다. |
| **키오스크 모드 설정:** 기기를 키오스크로 사용할 수 있게 허용하며 기능은 일부 앱으로 제한됩니다.<br>키오스크 모드 설정은 Android 8.0 이상의 기기에는 적용되지 않습니다. 이런 기기의 경우 기기 상세 정보 페이지에 키오스크 상태가 UNSUPPORTED_ON_DEVICE로 보고됩니다. | |
| 키오스크 모드 활성화 | Android 기기의 키오스크 모드를 설정할 수 있습니다. |
| 빠른 설정 비활성화 | 키오스크 모드에서 빠른 설정을 비활성화할 수 있습니다. |
| 사용자의 Wi-Fi 설정 허용 | 사용자가 Wi-Fi 설정을 변경하고 선호하는 무선 네트워크에 액세스할 수 있도록 선택합니다. |
| Bluetooth 설정에 대한 사용자 액세스 허용 | 사용자가 Bluetooth 설정을 변경하고 별도의 Bluetooth 기기를 페어링할 수 있도록 선택합니다. |
| 위치 설정에 대한 사용자 액세스 허용 | 사용자가 위치 설정 기능에 액세스하도록 허용합니다. |
| 사용자의 애플리케이션 업데이트 지연 허용 | 사용자가 애플리케이션 업데이트를 지연할 수 있도록 선택합니다. |
| 키오스크 종료 PIN | 최종 사용자가 키오스크 모드 종료 시 입력해야 하는 4자리 코드를 입력할 수 있습니다. |
| **앱 허용 목록 생성:** 이것은 허용된 앱 목록에 앱을 추가해 키오스크 모드에서 사용자 접근이 가능한 앱입니다. 앱을 드래그해서 키오스크 모드 런처에 표시되는 앱의 배열 순서를 설정할 수 있습니다.<br>허용 앱 목록에 애플리케이션을 등록해도 해당 앱이 기기에 설치되지는 않습니다. 반드시 각 앱을 App Catalog에 포함되어 있는 적절한 사용자와 사용자 그룹에 배포하시기 바랍니다. | |
| 빌트인 앱 | +추가를 클릭하면 기본 내장 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다. |

| 설정 | 설정하기 |
| --- | --- |
| | 위 잠금 설정에서 다이얼러 또는 카메라를 비활성화한 경우 이를 허용 앱 목록에 추가할 수 없습니다. |
| 앱 카탈로그 | +추가를 클릭하면 앱 카탈로그의 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다. |
| 기타 앱 | +추가를 클릭하면 Google Play Store에서 이용할 수 없는 앱의 패키지 이름를 추가할 수 있습니다. |
| 키오스크 모드 허용 앱 | X를 클릭하면 키오스크 모드 시 허용되는 앱 그룹에서 원하는 앱을 삭제할 수 있습니다. 앱을 드래그해서 키오스크 기기에서 나타나는 순서를 변경할 수 있습니다. |

> Knox Standard 4.0 이상 Samsung 기기의 경우 키오스크 모드에서 다중 사용자 기능을 자동으로 잠급니다.

사용하는 기기가 Samsung 기기가 아닌 경우 Android 8.0 이상에서 키오스크 모드가 지원되지 않습니다. Android 8.0 이상에서 키오스크 모드는 Android Enterprise 잠금을 사용하는 것이 좋습니다.

**관련 주제:**

- **Android용 키오스크 모드 설정**
- 구성을 생성하는 방법

# 10.10.4.30. Android용 키오스크 모드 설정

이 섹션에는 다음 주제가 포함됩니다.

- 키오스크 모드 원격 시작
- 키오스크 모드 종료

**라이센스: Silver**

Android 기기용 키오스크 모드를 통해 기기 사용을 특정 앱으로 제한할 수 있습니다. 키오스크 모드를 이용하여 업무 전용 앱만 사용하는 직원용 기기 설정을 할 수 있습니다.

Android 기기를 키오스크 모드에 대하여 또는 키오스크 모드로 기기 소유자를 준비할 때, 키오스크 모드에서 사용자가 사용할 수 있도록 하려는 앱의 허용 목록을 만들어야 합니다. 기기 소유자를 사용하는 기기의 경우 앱을 허용되는 앱 목록으로 드래그 앤 드롭하여 추가함으로써 앱을 구성할 때 키오스크 모드 런처에 표시되는 앱의 배열 순서를 설정할 수 있습니다. 자세한 정보는 잠금 및 키오스크 구성을 참조하십시오.

**필수 조건**

Android 기기의 키오스크 모드를 구성하려면 다음 작업을 먼저 완료해야 합니다.

- 기기에 Go 설치
- 키오스크 구성에 필요한 앱으로 앱 카탈로그 구성.
- 키오스크 모드로 실행될 기기에 앱 카탈로그 배포.

> SonimXP5S 기기에서는 키오스크 모드가 지원되지 않습니다.

- 키오스크 구성에 필요한 앱 설치.
- (선택 사항) Android 키오스크 브랜딩을 설정합니다.

> 키오스크 모드는 Android 5.1 및 6.0에서 지원됩니다. 원치 않는 애플리케이션의 사용을 방지하려면 Samsung 이외 Knox를 기기 소유자 모드로 설정해야 합니다.

**중요:** 일부 기기의 기능 때문에 화면이 가려지거나 키오스크 모드가 종료될 수 있습니다. Samsung Galaxy S6 Edge의 People Edge 기능이 그 중 한 예입니다. 기기를 배포하기 전 관리자가 이러한 유형의 기능을 끄는 것이 좋습니다.

**절차**

1. **구성**으로 이동합니다.
2. **+추가**를 클릭합니다.
3. **잠금 및 키오스크: Android 기기 관리 모드**를 클릭합니다.
4. **설정 생성** 화면에서 최소 **키오스크 모드 설정** 섹션을 완료하십시오.
5. **배포** 화면에서, 해당 구성을 배포할 기기 그룹을 선택하세요.
6. **완료**를 클릭하세요.
7. 사용하는 기기가 삼성 기기가 아닌 경우에는 다음 순서에 따라 진행하세요.
    1. **기기** > **기기**로 이동합니다.
    2. 키오스크 모드로 설정할 기기를 선택하십시오.
    3. **작업 강제 체크인**을 선택합니다.

4. 기기에서 **키오스크 모드** 버튼을 누릅니다.
5. 기기의 **홈** 버튼을 누릅니다.
6. **시작 관리자 선택** 대화 상자가 표시되면 **Go 키오스크 시작 관리자**를 누르고 **항상**을 선택합니다. 이 단계는 해당 기능에 맞는 런처를 사용하기 위해 필요합니다. 해당 설정을 하지 않을 경우, 사용자에게 런처를 선택하라는 메시지가 표시됩니다.

## 키오스크 모드 원격 시작

**절차**

1. **장치 > 장치**를 선택하세요.
2. 키오스크 모드 열을 추가하여 표시합니다.
3. 키오스크 모드를 활성화했지만 현재 키오스크 모드가 아닌 기기를 선택하세요.
4. **작업 > 키오스크 모드 시작**을 선택합니다.

## 키오스크 모드 종료

구성에 PIN을 설정하면 기기의 키오스크 모드를 종료할 수 있습니다.

**절차**

1. **설정** 아이콘을 누르세요.
2. **키오스크 모드 종료**를 선택하세요.
3. **키오스크 PIN** 입력 필드가 표시되면 해당 필드를 누르세요.
4. 키오스크 PIN을 입력하세요.

포털에서 특정 장치의 키오스크 모드를 종료할 수 있습니다.

**절차**

1. **장치 > 장치**를 선택하세요.
2. 장치 정보를 확인하세요.
3. **작업 > 키오스크 모드 종료**를 선택합니다.

다음 방법으로도 키오스크 모드를 종료할 수 있습니다.

- 구성 삭제
- 구성 설정 해제
- 구성에서 해당 장치 그룹 삭제

# 10.10.4.31. Android 공유 기기 키오스크 설정

작업자를 배치하기 위해 회사는 특정 사용자 역할이 지정된 전용 Android 기기를 제공할 수 있습니다. 사용자 프로필에 따라 기기에 앱과 구성이 다르게 나타날 수 있습니다. 예를 들어 기술 담당자 역할의 사용자에는 그 일에 대한 특정 앱 세트가 주어지고, 유지 관리 역할의 다른 사용자는 다른 앱 세트를 이용할 수 있습니다.

Android 공유 장치 키오스크 모드는 장치를 공유하는 다양한 사용자 그룹에 대한 앱 필터 역할을 합니다. 공유 기기 키오스크에 로그인한 사용자는 주어진 역할에 적합한 앱들만 볼 수 있습니다. 공유 기기 키오스크의 가장 큰 장점 중 하나는 다른 사용자 그룹에게 동일한 기기 내에서 다른 앱 세트에 접근할 수 있게 해준다는 점입니다. 사용자가 Android 공유 장치 키오스크 모드에서 로그아웃하면 해당 앱과 기록을 포함한 사용자 데이터가 장치에 로그인한 다음 사용자의 표시에서 지워집니다(표시된 앱이 재설치인 경우). 공유 기기 키오스크는 관리되는 Google Play 계정의 Android 엔터프라이즈 배포에 한해 지원됩니다.

공유 기기 키오스크에는 두 유형의 사용자(준비 사용자와 공유 키오스크 사용자)와 이 사용자에게 해당하는 최소 두 개의 정책이 필요합니다. 준비 사용자는 공유 기기에 나타나는 로그인 화면을 표시하는 데 사용됩니다. 또한, 준비 사용자는 실제 키오스크 기기에 다른 사용자들이 로그인할 수 있게 하는 특정 유형의 관리자입니다. 공유 기기 키오스크 사용자가 성공적으로 로그인하면 준비 정책이 공유 키오스크 정책으로 대체됩니다. 키오스크 사용자는 기기에 할당된 정책에 따라 설치된 앱에 접속할 수 있습니다. 여러 개의 공유 키오스크 정책을 생성하더라도 키오스크 기기에는 한 번에 하나의 키오스크 정책만 활성화됩니다. 키오스크 사용자가 공유 키오스크에서 로그아웃하면 기기는 준비 사용자로 되돌아가고 그 결과 준비 정책으로 되돌아갑니다.

준비 사용자는 로그인 페이지에 접근할 수 있는 기능만 가지고 있습니다. 따라서 준비 사용자 전용 준비 정책을 생성해야 합니다. 이와 대조적으로 공유 기기 키오스크 사용자는 해당 정책에서 정의하는 앱 세트에만 접근할 수 있습니다 (기본적으로, 공유 기기 키오스크 기기에 허용된 앱도 설치해야 합니다.) 공유 기기 키오스크 정책을 사용하면 이전에 설치한 모든 앱에서 허용된 앱의 필터를 만들 수 있습니다. Android 공유 키오스크 정책에 바로 앱을 업로드할 수 없습니다. 종종 조직에 따라 공유 키오스크 사용자의 유형 또는 사용자 그룹에 공유 키오스크 정책을 한정하려는 경우가 있습니다. 예를 들어 회사에 각기 다른 역할의 주간 근무자와 야간 근무자가 있으면 서로 다른 앱 세트 액세스가 필요할 수 있습니다. 이 경우 주간근무 정책과 야간근무 정책을 생성해야 합니다.

공유 기기 키오스크 활성화에 대한 자세한 내용은 **잠금 및 키오스크: Android Enterprise**를 참조하십시오.

# 10.10.4.32. 잠금 및 키오스크: Android Enterprise

락다운 & 키오스크: Android Enterprise 구성은 Android Enterprise 기기의 특정 기능을 비활성화하며 키오스크 모드에서 사용자가 사용할 수 있는 앱의 허용 목록을 생성합니다.

이 섹션에는 다음 주제가 포함됩니다.


- 잠금 설정
- 작업 프로필
- 업무 관리 기기(기기 소유자 및 키오스크 모드 설정)
- 작업 프로필이 있는 관리되는 기기/회사 소유 기기의 작업 프로필 잠금 설정


## 잠금 설정

| 설정 | 설명 |
| --- | --- |
| 이름<br><br>설명 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다.<br><br>현재 설정에 대한 간략한 설명을 입력합니다. |
| 잠금 유형 선택 | 구성하고자 하는 잠금 설정 유형을 설정할 수 있습니다.<br>• 작업 프로필<br>• 업무 관리 기기(기기 소유자 및 키오스크 모드 설정)<br>• 작업 프로필이 있는 관리되는 기기/회사 소유 기기의 작업 프로필 잠금 설정<br>회사 소유 기기의 작업 프로필 잠금 설정은 Android 11+ 기기에만 적용됩니다.<br>구성당 한 개 유형만 가능합니다. 선택하는 유형에 따라 표시되는 옵션이 달라집니다.<br>업무 관리 기기(기기 소유자) 및 회사 소유 기기의 작업 프로필이 있는 관리되는 기기 구성이 동일한 기기로 배포될 경우 작업 프로필이 있는 관리되는 기기가 우선합니다. |

## 작업 프로필

Android Enterprise 기기의 특정 기능을 비활성화합니다.

| 설정 항목 | 수행 작업 | 기기 대상 |
| --- | --- | --- |
| 화면 캡처 비활성화 | 기기에 내장된 화면 캡처 기능을 끌 수 있습니다. | • Android 5.0+ |
| 앱 제어 금지 | 사용자가 설정 또는 런처에서 애플리케이션을 수정하지 못하도록 설정할 수 있습니다. | • Android 5.0+ |
| 구성 자격 증명 금지 | 사용자가 사용자 자격 증명을 구성하지 못하도록 설정할 수 있습니다. | • Android 5.0+ |
| 교차 프로필 복사 붙여넣기 금지 | 프로필 간 정보의 복사/붙여놓기를 금지하도록 설정할 수 있습니다. | • Android 5.0+ |
| 계정 수정 금지 | 사용자가 계정을 추가 또는 제거하지 못하도록 설정할 수 있습니다. | • Android 5.0+ |
| 플래시 불빛 금지 | 사용자가 NFC를 이용해 앱 데이터를 전송하지 못하도록 하려면 이 옵션을 선택합니다. | • Android 5.1+ |
| 위치 공유 금지 | 사용자가 기기 위치를 앱에 나타내지 못하도록 설정할 수 있습니다. | • Android 5.0+ |
| 디버깅 기능 허용 불가 | 기기에서 디버깅 기능을 비활성화하도록 설정할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다. | • Android 5.0+ |
| 앱 확인 | 기기에서 애플리케이션 검증 기능을 허용하려면 선택합니다. 기본적으로 이 옵션은 켜져 있습니다.<br>이 옵션이 꺼져 있으면 기기가 기본 동작(기기마다 다를 수 있음)으로 돌아갑니다. | • Android 5.0+ |
| 기기에서 알 수 없는 소스 비활성화 | 기기가 알 수 없는 소스의 앱을 설치하지 못하도록 설정할 수 있습니다.<br>이 설정은 기기에 적용되기 위해 Google Play 업데이트에 종속되어 이 기능을 활성화합니다. | • Android 5.0+ |
| 입력 방법 제한 | **패키지 이름** 필드를 통해 허용 패키지 이름 목록을 지정하여 허용되는 IME 패키지 이름을 제한하도록 선택할 수 있습니다. 기기에서는 허용 패키지 입력 방법 및 기본 시스템 입력 방법 둘 다를 사용할 수 있게 됩니다.<br>사용자는 기본 시스템 입력 방법과 허용 목록에 있는 패키지 입력 방법 사이에서 전환할 수 있습니다.<br>Android 10+의 경우에는 작업 프로필 공간에서만 허용 목록을 적용할 수 있습니다. 이전 Android 버전의 경우에는 기기 전체(작업 프로필 내부 및 외부)에서 IME 앱에 대한 허용 목록을 적용할 수 있습니다. | • Android 5.0+ |

| 설정 항목 | 수행 작업 | 기기 대상 |
| --- | --- | --- |
| 접근성 서비스 제한 | **패키지 이름** 필드를 통해 허용 패키지 이름 목록을 지정하여 작업 앱의 접근성 서비스를 제한하도록 선택할 수 있습니다. 허용 목록 패키지가 없는 경우에는 시스템 접근성 서비스만 허용됩니다. | • Android 5.0+ |
| 작업 프로필 내에서 알 수 없는 소스 비활성화 | 작업 프로필 내에서 알 수 없는 소스로부터의 다운로드를 허용하지 않으려면 선택합니다. | • Android 5.0+ |
| 시스템 앱 활성화/비활성화 | **시스템 앱 패키지 이름** 필드를 통해 2개의 패키지 이름 목록을 지정하여 시스템 애플리케이션 배포를 활성화 및 비활성화하려면 선택합니다.<br>이 기능을 사용하여 Google Play에 게시되지 않은 시스템 애플리케이션에 대한 액세스 권한을 관리할 수 있습니다.<br>App Catalog에 앱을 추가하고 시스템 앱에도 추가하는 작업은 지원되지 않습니다. | • Android 5.0+ |
| 발신자 ID 비활성화 | 작업 프로필의 발신자 ID 정보가 전화 수신 시 기기에 표시될지 여부를 설정합니다. | • Android 6.0+ |
| Bluetooth를 통한 연락처 공유 비활성화 | 기기가 Bluetooth를 통해 다른 기기와 연락처를 공유하지 못하도록 하려면 선택합니다. | • Android 6.0+ |
| 검색을 통한 연락처 공유 비활성화 | 사용자가 개인 폰 다이얼러에서 회사 연락처를 검색하지 못하도록 하려면 선택합니다. | • Android 7.0+ |
| 자동 채우기 허용 불가 | 자동 채우기를 허용하지 않으려면 선택합니다. | • Android 8.0+ |
| 개인 프로필에서 작업 앱 알림 허용 불가 | 작업 프로필 알림을 제한하려면 선택합니다. | • Android 8.0+ |
| 인쇄 허용 불가 | 모든 앱에서 인쇄를 제한하려면 선택합니다. | • Android 9.0+ |
| 프로필에서 공유 허용 불가 | 기기의 작업 프로필에서 사용자들이 개인 데이터를 공유하지 못하도록 하려면 선택합니다. | • Android 9.0+ |
| 작업 프로필 일정에 대한 액세스 허용 | 다음 옵션 중 어느 것이든 선택하여 모든 앱을 허용하거나 개인 공간의 앱 집합을 선택하여 작업 프로필에 있는 캘린더 정보에 액세스합니다.<br>• **개인 프로필의 모든 앱** - 모든 앱이 작업 프로필에 있는 캘린더 정보에 액세스할 수 있도록 허용<br>• **개인 프로필의 다음 앱만** - 아래 텍스트 필드에서, 쉼표로 구분한 앱의 번들 ID 입력. 개인 공간에서 선택한 이 앱만 작업 프로필에 있는 캘린더 정보에 액세스할 수 있게 됩니다.<br>개인 공간의 앱은 공유 캘린더에 액세스할 수 있도록 특정 API를 구현해야 합니다. | • Android 10.0+ |
| 앱의 교차 프로필 허용 목록 적용 설정 | 사용자가 작업 프로필 내의 특정 앱에 있는 정보를 기기의 개인 공간으로 가져와 공유할 수 있게 하려면 이 체크박스를 선택합니다.<br>**허용 목록에 등록된 앱** 필드에서 허용 목록에 등록할 앱의 패키지 ID를 쉼표로 구분하여 입력합니다.<br>기본적으로 이 옵션은 비활성화되어 있습니다. | • Android 11.0+ |

| 설정 항목 | 수행 작업 | 기기 대상 |
| --- | --- | --- |
| 5G 네트워크 슬라이싱 활성화 | 회사 소유 기기의 작업 프로필에 5G 네트워크 슬라이싱 옵션을 제공하려면 선택합니다.<br>기본적으로 이 옵션은 비활성화되어 있습니다. | • Android 12.0+ |
| 관리자가 구성한 Wi-Fi 공유 금지 | 관리자가 설정한 Wi-Fi 구성을 사용자가 공유하지 못하도록 하려면 선택합니다. | • Android 13.0+ |
| AI 지원 비활성화 | 사용자가 AI Assist 기능을 사용하지 못하도록 하려면 선택합니다.<br>기본적으로 이 옵션은 비활성화되어 있습니다. | • Android 15.0+ |

## 업무 관리 기기(기기 소유자 및 키오스크 모드 설정)

Android 5.0 이상에서 업무 관리 기기(기기 소유자)의 특정 기능을 비활성화합니다.

| 설정 | 설명 |
| --- | --- |
| Wi-Fi 비활성화 | 무선 랜 기능을 끌 수 있습니다. |
| Wi-Fi 설정 비활성화 | 무선 기능을 끌 수 있습니다. |
| 카메라 비활성화 | 카메라 기능을 끌 수 있습니다. |
| Bluetooth 비활성화<br>(Android 8.0+) | Bluetooth 기능을 끌 수 있습니다.<br>이 기능을 사용할 때는 주의가 필요합니다. Ivanti에서는 핸즈프리 Bluetooth 기능이 지원되지 않으므로 오디오를 끄지 않는 것이 좋습니다. 운전 중 핸즈프리 기기 사용과 관련한 법적 요건의 적용 범위가 더욱 확대되고 있습니다. |
| Bluetooth 설정 허용 불가<br>(Android 8.0+) | Bluetooth 기능을 끌 수 있습니다. |
| 화면 캡처 비활성화 | 기기에 내장된 화면 캡처 기능을 끌 수 있습니다. |
| 네트워크 재설정 비활성화 | 네트워크 재설정을 방지하려면 선택하세요. (Android 7.0 이상 장치에 해당하며 회사 소유 장치 모드의 작업 프로필에서는 지원되지 않음). |
| 마스터 볼륨 음소거 | 마스터 볼륨을 음소거할 수 있습니다. |
| 앱 제어 금지 | 사용자가 설정 또는 런처에서 애플리케이션을 수정하지 못하도록 설정할 수 있습니다. |
| 자격 증명 허용 불가 | 사용자가 사용자 자격 증명을 구성하지 못하도록 설정할 수 있습니다. |
| 긴급 방송 허용 불가 | 긴급 방송을 허용하지 않을 수 있습니다. |
| 모바일 네트워크 허용 불가 | 모바일 네트워크 기능을 끌 수 있습니다.<br>Wi-Fi가 꺼져 있으면 비활성화가 불가합니다. |
| 테더링 허용 불가 | 기기 1대에 인터넷을 연결한 후 해당 기기에 연결된 다른 기기에서도 인터넷을 이용할 수 있는 테더링 기능을 끌 수 있습니다. |
| VPN 허용 불가 | VPN 기능을 끌 수 있습니다. |
| 공장 초기화 허용 불가 | 사용자가 장치 설정을 기본값으로 초기화할 수 없도록 차단할 수 있습니다. |
| 공장 초기화 보호 활성화 | 사용자가 장치 설정을 기본값으로 초기화할 수 있도록 허용할 수 있습니다.<br>필요에 따라 공장 초기화 후 기기를 프로비저닝할 수 있는 공인 Google 계정 ID(정수 값) 목록을 지정하거나 도움말 아이콘을 마우스로 가리켜서 공인 계정 ID 검색을 위한 도움말을 볼 수 있습니다. |
| 계정 수정 금지 | 사용자가 계정을 추가 또는 제거하지 못하도록 설정할 수 있습니다. |
| NFC(플래시 불빛) 금지 | 사용자가 NFC를 이용해 앱 데이터를 전송하지 못하도록 하려면 이 옵션을 선택합니다. |
| 발신 전화 허용 불가 | 사용자가 발신 전화를 하지 못하도록 설정할 수 있습니다. |
| 안전 모드 허용 불가(Android 6.0+) | 사용자가 기기를 안전 모드로 재부팅하지 못하도록 설정할 수 있습니다. |
| 위치 공유 금지 | 사용자가 기기 위치를 앱에 나타내지 못하도록 설정할 수 있습니다. |

| 설정 | 설명 |
| --- | --- |
| 디버깅 기능 허용 불가 | 기기에서 디버깅 기능을 비활성화하도록 설정할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다. |
| 앱 확인 | 기기에서 애플리케이션 검증 기능을 허용하려면 선택합니다. 기본적으로 이 옵션은 켜져 있습니다.<br>이 옵션이 꺼져 있으면 기기가 기본 동작(기기마다 다를 수 있음)으로 돌아갑니다. |
| SMS 허용 불가 | 사용자가 SMS 메시지를 송수신하지 못하도록 설정할 수 있습니다. |
| 마이크 음소거 해제 허용 불가 | 사용자가 기기의 마이크 음소거 해제를 하지 못하도록 설정할 수 있습니다. |
| 자동 시간 비활성화 | 사용자가 자동 시간 변경을 활성화할 수 없도록 설정할 수 있습니다. |
| 자동 표준 시간대 비활성화 | 사용자가 표준 시간대 변경으로 자동 기기 시간 조정을 활성화하지 못하도록 설정할 수 있습니다. |
| 서버와의 동기화 시간(Android 9.0+) | 기기가 처음에는 등록 시에, 그 이후에는 매번 체크인 후 24시간마다 MDM용 Ivanti Neurons와 시간을 동기화할 수 있도록 선택합니다. 이 옵션은 **자동 시간 비활성화**를 선택할 경우에만 사용할 수 있게 됩니다. |
| 시간대 설정(Android 9.0+) | 시간대 문자열을 Olson Time Zone ID 형식(예: Pacific/Midway)으로 지정합니다. |
| 데이터 로밍 비활성화 | 기기 로밍 중 데이터 전송 기능을 끌 수 있습니다. |
| Wi-Fi 절전 모드 비활성화 | 기기가 절전 모드일 때 Wi-Fi를 유지할 수 있습니다. |
| 입력 방법 제한 | **패키지 이름** 필드를 통해 허용 패키지 이름 목록을 지정하여 허용되는 IME 패키지 이름을 제한하도록 선택할 수 있습니다. 기기에서는 허용 패키지 입력 방법 및 기본 시스템 입력 방법 둘 다를 사용할 수 있게 됩니다.<br>사용자는 기본 시스템 입력 방법과 허용 목록에 있는 패키지 입력 방법 사이에서 전환할 수 있습니다.<br>Android 10+의 경우에는 기기 공간에서만 IME 앱에 대한 허용 목록을 적용할 수 있습니다. 이전 Android 버전의 경우에는 기기 전체에서 IME 앱에 대한 허용 목록을 적용할 수 있습니다. |
| 접근성 서비스 제한 | **패키지 이름** 필드를 통해 허용 패키지 이름 목록을 지정하여 작업 앱의 접근성 서비스를 제한하도록 선택할 수 있습니다. 허용 목록 패키지가 없는 경우에는 시스템 접근성 서비스만 허용됩니다. |
| USB 파일 전송 비활성화 | USB 파일 전송을 비활성화하도록 설정합니다. |
| 외부 미디어 비활성화 | 외부 미디어를 비활성화하도록 설정합니다. |
| Keyguard 비활성화(PIN/비밀번호가 설정되어 있는 경우 효과 없음) | Keyguard 비활성화하도록 설정합니다. 이 옵션은 비밀번호, PIN, 또는 패턴이 현재 설정되어 있는 경우 효과가 없습니다.<br>비밀번호, PIN 또는 패턴이 Keyguard가 비활성화된 후 설정될 경우 Keyguard 비활성화가 정지됩니다. |
| 전원에 연결되어 있는 동안 화면 켜기를 유지합니다. | 전원에 연결되어 있는 동안 화면 켜기를 유지하도록 설정합니다. 기기가 전원에 연결되어 있는 동안 화면이 흐릿해질 수 있으나 꺼지지는 않습니다. |

| 설정 | 설명 |
| --- | --- |
| | 이 설정은 시간 제한 설정을 위해 암호 구성의 자동 잠금 또는 비활성 시간 제한이 사용되지 않을 경우에만 적용됩니다. |
| 창 생성을 허용하지 않음 | 앱이 알림 및 토스트와 같이 특정 유형의 오버레이를 표시하지 않도록 설정합니다. |
| 최초 사용 힌트 건너뛰기 | 앱에 대한 시스템 권장사항이 최초 시작 시 사용자 튜토리얼 및 기타 소개 힌트를 건너뛰도록 활성화합니다. |
| 기기에서 알 수 없는 소스를 허용하지 않기 | 사용자가 알 수 없는 소스의 앱을 설치하는 것을 허용하지 않으려면 선택합니다. |
| 잠금 화면 메시지 설정(Android 7.0+) | 기기에 표시될 잠금 화면 메시지 설정을 선택합니다. 텍스트 필드에 잠금 화면 메시지(최대 256자)를 입력합니다. 이 옵션을 활성화하면, 사용자가 설정에서 메시지를 설정할 수 없으며 관리자가 설정하는 메시지가 사용자에게 표시됩니다.<br>관리자가 '잠금 화면 메시지 설정'을 활성화한 후 잠금 화면 메시지도 제공하지 않을 경우 사용자는 설정에서 메시지를 설정할 수는 없으나, 어떠한 메시지도 사용자에게 표시되지 않습니다. |
| 화면 밝기 설정 | 기기 화면의 밝기를 설정하려면 선택합니다.<br>• 수동 - 수동으로 숫자 입력(0~255)<br>• 적응 - 기기에서 자동으로 밝기 설정<br>기기 화면의 밝기를 설정하기 전에 '밝기 구성 허용 안 함'을 활성화하는 것이 좋습니다. |
| 화면 시간제한 설정 | 화면 시간제한(초)을 설정하려면 선택합니다.<br>기기 화면의 밝기를 설정하기 전에 '화면 시간제한 구성 허용 안 함'을 활성화하는 것이 좋습니다. |
| 화면 방향 설정 | 화면 방향을 설정하려면 선택합니다. 화면 방향을 드롭다운 목록에서 0, 90, 180, 270도로 설정할 수 있습니다.<br>기본적으로 이 옵션은 선택되지 않았습니다. Go 앱 89 이후 버전의 경우 키오스크에서 장치를 세로 모드로 유지하려면 이 옵션을 선택하고 값을 0으로 설정해야 합니다. |
| 시스템 앱 활성화/비활성화 | **시스템 앱 패키지 이름** 필드를 통해 2개의 패키지 이름 목록을 지정하여 시스템 애플리케이션 배포를 활성화 및 비활성화하려면 선택합니다. 이 기능을 사용하여 Google Play에 게시되지 않은 시스템 애플리케이션에 대한 액세스 권한을 관리할 수 있습니다.<br>앱 카탈로그와 시스템 앱 목록에 앱 추가하기는 지원하지 않습니다. |
| **Android 8.0+** | |
| 자동 채우기 허용 불가 | 사용자가 자동 채우기 서비스를 사용하지 못하도록 합니다. |
| Bluetooth 공유 허용 불가 | 사용자가 기기의 발신 Bluetooth를 공유하지 못하도록 합니다. |
| 백업 서비스 비활성화 | 백업 서비스를 사용하지 못하도록 합니다. |
| **Android 9.0+** | |
| 인쇄 허용 불가 | 사용자가 인쇄하지 못하도록 합니다. |
| 비행기 모드 허용 불가 | 전체 기기에서 비행기 모드를 사용하지 못하도록 합니다. |

| 설정 | 설명 |
| --- | --- |
| 주변 표시 허용 불가 | 사용자의 주변 표시를 못하도록 합니다. |
| 구성 밝기 허용 불가<br><br>구성 날짜 시간 허용 불가<br><br>구성 위치 허용 불가<br><br>구성 화면 시간 제한 허용 불가<br><br>**Android 12.0+**<br><br>충전 전용 USB 활성화<br><br>**Android 13.0+** | 사용자가 밝기를 구성하지 못하도록 합니다.<br>이 옵션을 선택하기 전에 '화면 밝기 모드 설정' 모드를 정의하는 것이 좋습니다.<br><br>날짜, 시간 및 시간대를 구성하지 못하도록 합니다.<br><br>사용자가 위치 공급자를 사용하지 못하도록 합니다.<br><br>사용자가 화면 꺼짐 시간 제한을 변경하지 못하도록 합니다.<br>이 옵션을 선택하기 전에 '화면 시간제한 설정' 값을 정의하는 것이 좋습니다.<br><br>USB 포트를 충전 전용으로 활성화하려면 선택합니다. |
| 필요한 최소 Wi-Fi 보안 설정<br><br>관리자가 구성한 Wi-Fi 공유 금지<br><br>**Android 15.0+** | 이 옵션을 이용해 다음과 같이 필요한 최소 Wi-Fi 보안을 설정하십시오.<br>• 최소 보안이 필요하지 않음 – 최소 보안이 필요하지 않은 경우 선택<br>• 개인 네트워크 기반 보안 – WEP, WPA/WPA2/WPA3 등의 개인 Wi-Fi 네트워크 차단<br>• Enterprise EAP 네트워크 기반 보안 – EAP 프로토콜 기반 Wi-Fi 네트워크 차단<br>• Enterprise 192 네트워크 기반 보안 - EAP 회사 기반 Wi-Fi 네트워크 차단<br>최소 기준을 충족하지 않는 기존 기기의 연결을 모두 해제합니다.<br>기기 세부 정보에서 **일반 > Wi-Fi 보안 수준** 아래에 필요한 최소 Wi-Fi 보안 수준(해당하는 경우)이 표시됩니다.<br><br>관리자가 설정한 Wi-Fi 구성을 사용자가 공유하지 못하도록 하려면 선택합니다. |
| AI 지원 비활성화 | 사용자가 AI Assist 기능을 사용하지 못하도록 하려면 선택하세요.<br>기본적으로 이 옵션은 비활성화되어 있습니다. |
| **키오스크 모드 설정:** 키오스크 모드에는 사용자 지정 런처를 통한 앱 접근 제한 등 기기에 추가적인 제한이 설정됩니다. | |
| 키오스크 모드 활성화<br><br>작업 잠금 모드 활성화 | Android 기기의 키오스크 모드를 설정할 수 있습니다.<br>• 사용자가 공유 키오스크 모드에 로그인했다가 로그아웃하면 나중에 로그인할 때 사용자 이름을 Go 클라이언트에서 계속 사용할 수 있습니다. 공유 키오스크 모드에서는 Go 클라이언트가 최근에 사용된 7개의 사용자 이름을 보유합니다.<br>• 현재 공유 키오스크 모드는 IDP 인증을 지원합니다. 따라서 MDM용 Ivanti Neurons를 IDP로 구성하면 공유 키오스크 모드를 IDP 인증으로 사용할 수 있습니다.<br><br>Android 기기에서 잠금 작업 모드를 활성화하도록 설정합니다. 활성화되면 기기가 Keyguard, 상태 표시줄 및 안전 모드를 표시할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.<br>Android 9 또는 지원되는 최신 버전에 대한 작업 잠금 모드가 활성화되면 다음 설정이 추가 |

| 설정 | 설명 |
| --- | --- |
| | 로 표시됩니다.<br>**설정 아이콘** - 앱이 기기 설정 앱에 종속된 시스템 기능에 액세스할 수 있도록 허용합니다. 기기 설정을 허용하면 앱에서 Bluetooth를 페어링하는 경우와 같은 시나리오에서 작업 잠금 모드 위반을 방지하는 데 도움이 됩니다. 특정 앱에 대해서는 이 설정을 활성 상태로 유지하는 것이 좋습니다.<br>**시스템 정보** - 날짜/시간, 연결성, 배터리, 진동 모드 등을 상태 표시줄에 표시합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.<br>**Keyguard**(기본적으로 활성화됨) - 작업 잠금 모드 동안 Keyguard를 활성화합니다.<br>**전역 작업**(기본적으로 활성화됨) - 사용자가 전원 버튼을 길게 누르는 경우에 표시되는 메뉴를 활성화합니다. 이 옵션이 비활성화되면 사용자는 기기 전원을 끄지 못할 수도 있습니다.<br>**홈 버튼** - 홈 버튼을 활성화합니다. 이 옵션은 기본적으로 비활성화되어 있습니다. 활성화되면 다음 하위 옵션이 표시됩니다.<br>• **개요 버튼**(기본적으로 비활성화됨) - 작업 잠금 모드일 때 개요 버튼과 개요 화면을 활성화합니다.<br>• **알림**(비활성화됨) - 작업 잠금 모드일 때 알림을 활성화합니다. 여기에는 상태 표시줄, 미리 알림, 확장 가능한 알림 쉐이드에 있는 알림 아이콘이 포함됩니다.<br>홈 버튼 옵션이 활성화되지 않은 경우 사용자는 다중 창 기능을 사용할 수 없게 됩니다. |
| 자동으로 키오스크 입력(최초 설정 시에만)<br><br>정책 업데이트 후 키오스크 모드 유지 | 구성이 적용될 때 키오스크 모드를 자동으로 허용하도록 설정합니다.<br><br>잠금 정책 업데이트가 적용된 후 기기가 자동으로 키오스크 모드로 돌아가도록 하려면 선택합니다. 이 설정은 중단 없는 키오스크 작동을 유지하고 정책 변경 후 수동 개입의 필요성을 줄이는 데 도움이 됩니다. 이전에는 잠금 정책을 업데이트하면 기기가 키오스크 모드를 종료하는 경우가 있었습니다. 활성화하면 업데이트된 정책이 처리된 후 기기가 자동으로 키오스크 모드로 다시 전환됩니다. |
| Android 5 기기의 빠른 설정 비활성화<br><br>Android 6+ 및 모든 Samsung 기기의 빠른 설정 비활성화 | Android 5에서 실행되는 기기에 대해 키오스크 모드에서 빠른 설정을 비활성화할 수 있습니다.<br><br>가장 최신 릴리스 버전을 통한 버전 6의 Android Enterprise 기기 및 모든 Samsung 기기에 대해 키오스크 모드에서 빠른 설정을 비활성화하려면 선택합니다.<br>이 설정을 비활성화하더라도 기기의 알림 아이콘 및 사운드는 차단되지 않습니다. |
| 사용자의 Wi-Fi 설정 허용 | 사용자가 Wi-Fi 설정을 변경하고 선호하는 무선 네트워크에 액세스할 수 있도록 선택합니다. |
| Bluetooth 설정에 대한 사용자 액세스 허용<br><br>위치 설정에 대한 사용자 액세스 허용<br><br>사용자의 애플리케이션 업데이트 지연 허용<br><br>날짜 및 시간 설정에 대한 사용자 액세스 허용 | 사용자가 Bluetooth 설정을 변경하고 별도의 Bluetooth 기기를 페어링할 수 있도록 선택합니다.<br><br>사용자가 위치 설정 기능에 액세스하도록 허용합니다.<br><br>사용자가 애플리케이션 업데이트를 지연할 수 있도록 선택합니다.<br><br>사용자가 날짜 및 시간 설정 기능에 액세스하도록 허용합니다. |

| 설정 | 설명 |
| --- | --- |
| 모바일 네트워크 설정에 대한 사용자 액세스 허용 | 사용자가 모바일 네트워크 설정 기능에 액세스하도록 허용합니다. |
| 사용자가 언어를 선택할 수 있음 | 사용자가 언어 설정에 액세스하도록 허용합니다. |
| 공유 기기 활성화 | 공유 기기 키오스크에서는 여러 최종 사용자들 간에 기기가 공유됩니다. 이 옵션을 설정하면 기기가 키오스크 모드에 있는 동안 기기 공유가 가능합니다.<br>• **로그인 활성화**: 키오스크 관리자를 위한 옵션입니다. 이 옵션으로 기기를 구성하면 보여지는 사용자 로그인 공유된 키오스크 기기에 최종 사용자가 로그인할 수 있습니다. 로그인 옵션 활성화는 사용자가 Android Enterprise 기기 계정 사용자(준비 사용자)로 생성된 경우에만 나타납니다.<br>도메인 대체 사용을 선택하고 도메인을 적절히 입력합니다.<br>이 옵션은 도메인 접미사를 위해 사용자 이름을 확인합니다. 도메인 접미사가 누락되어 있을 경우 시스템이 도메인 접미사를 사용자 이름에 자동으로 추가합니다.<br>• **로그아웃 활성화**: 이 옵션으로 기기를 구성하면 로그인된 최종 사용자는 허용된 앱 목록에 액세스할 수 있습니다. 이 사용자는 로그아웃 옵션은 볼 수 있지만 키오스크를 종료할 수 없습니다. 사용자가 공유 키오스크 기기에서 로그아웃할 때 추가 사용자가 공유 키오스크 기기로 로그인하여 관리자가 구성한 앱을 볼 수 있습니다.<br>• 앱에 로그인할 때마다 재설치 실행에 사용되는 재활용 아이콘이 앱과 함께 나타납니다. 이 옵션은 로컬로 캐시된 데이터 앱에서 사용할 수 있습니다.<br>관리자가 키오스크 종료 PIN을 제공하는 경우 사용자는 키오스크 모드를 종료할 수 있습니다.<br>• **시간 제한**: 시간 단위로 시간 제한을 지정합니다. 예를 들어 시간 제한이 2시간 간격으로 구성되어 있고 최종 사용자가 공유 키오스크 기기에 로그아웃을 실패한 경우 2시간 후에 기기가 자동으로 로그아웃을 수행합니다.<br>**로그아웃 활성화** 옵션이 선택된 경우에만 **시간 제한** 필드가 보여집니다. 이는 선택 사항입니다.<br>기기 상세 페이지에서 **Android 엔터프라이즈 키오스크 로그아웃** 옵션을 클릭하여 최종 사용자를 공유 키오스크 모드에서 로그아웃시킬 수 있습니다. |
| FIDO 인증 허용(장치에 Google Chrome 앱 필요)<br><br>사용자가 밝기 및 자동 회전을 구성할 수 있음 | 공유 키오스크 사용 시 사용자에 대해 FIDO 인증을 사용하려면 이 옵션을 선택합니다. 사용자가 FIDO 키를 사용하여 장치에 로그인하는 것을 허용합니다.<br>유일하게 지원되는 브라우저는 Google Chrome으로, 공유 키오스크에서 FIDO 인증을 사용하려면 장치에 Google Chrome이 있어야 합니다.<br><br>사용자가 밝기 및 자동 회전을 구성할 수 있도록 합니다. |
| 다중 창 활성화 | Samsung 기기(기기 소유자 키오스크)와 동시에 둘 이상의 앱 표시를 허용하려면 선택하십시오.<br>작업 잠금 모드에서 다중 창을 허용하려면 다음 작업 잠금 모드 옵션도 활성화해야 합니다.<br>• **홈 버튼**<br>• **개요 버튼** |

| 설정 | 설명 |
| --- | --- |
| 비활성 보호 활성화 | 키오스크 모드에서 비활성 보호를 활성화하려면 선택합니다. 선택할 경우 기본값은 30초입니다. 그때까지 키오스크 화면이 활성 상태로 유지됩니다. 30~3600 사이의 값을 설정할 수 있습니다. |
| 키오스크 브랜딩 | 드롭다운 목록에서 기본 또는 사용자 지정 브랜딩 옵션을 선택합니다. |
| 키오스크 종료 PIN | 키오스크 모드를 종료하기 위해 사용자가 입력해야 하는 6자리수 PIN을 입력합니다. PIN은 최소 6자리수, 최대 10자리수여야 합니다. 이 PIN은 키오스크 모드인 모든 기기에 적용됩니다.<br>이전의 키오스크 PIN 길이는 4자리수였습니다. 사용자는 이전 버전에서 MDM용 Ivanti Neurons 82로 업그레이드한 후에도 4자리수 PIN을 계속 사용할 수 있습니다. 그러나 구성이 변경된 경우에는 PIN 길이를 새로운 요구 사항에 맞게 설정해야 합니다(예: 최소 6자리수 및 최대 10자리수).<br>Go 앱은 악의적 공격으로부터 기기를 보호합니다. 자세한 내용은 Android용 Go 문서를 참조하십시오. |
| 단일 앱 실행기 키오스크 활성화 | 선택하면 키오스크 모드를 사용하여 GMS 및 비GMS 기기의 전경에 앱을 유지합니다. 앱 카탈로그에서 앱을 선택하거나 패키지 ID를 입력해야 합니다. |
| Ivanti Agent 설정에 대한 사용자 액세스 허용 | 기기가 **단일 앱 키오스크 모드**로 유지되는 동안 **Ivanti 에이전트 설정**에 액세스하려면 선택합니다. 이전에는 관리자가 에이전트 설정에 액세스하려면 키오스크 모드를 종료해야 했습니다. 설정을 활성화하고 기기에 배포한 후 사용자는 볼륨 높이기 및 볼륨 낮추기 버튼을 동시에 길게 눌러 Ivanti 에이전트 설정 페이지를 열 수 있습니다.<br>이 기능은 업무 관리형 기기 모드로 등록된 Android 기기에서만 지원됩니다. |
| 드라이버 안전 활성화 | 키오스크 모드 허용 앱 섹션에 있는 모든 앱에 대해 운전자 안전 아이콘 을 활성화하려면 선택합니다. 제한 속도를 넘으면 운전자 안전 아이콘을 클릭하여 앱을 비활성화하세요. |
| **앱 허용 목록 생성:** 이것은 허용된 앱 목록에 앱을 추가해 키오스크 모드에서 사용자 접근이 가능한 앱입니다. 앱을 드래그해서 키오스크 모드 런처에 표시되는 앱의 배열 순서를 설정할 수 있습니다.<br>허용 앱 목록에 애플리케이션을 등록해도 해당 앱이 기기에 설치되지는 않습니다. 반드시 각 앱을 App Catalog에 포함되어 있는 적절한 사용자와 사용자 그룹에 배포하시기 바랍니다. | |
| 빌트인 앱 | +추가를 클릭하면 기본 내장 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.<br>키오스크 모드 허용 앱 설정에서는 다음 옵션을 사용할 수 있습니다.<br>• **앱 사용자 데이터 지우기**: 이 옵션을 활성화하면 사용자가 키오스크에서 로그아웃할 때 어떤 메시지도 없이 모든 애플리케이션 데이터가 자동으로 지워집니다.<br>키오스크 모드 설정에서 공유 기기 활성화를 선택하면 이 옵션을 애플리케이션에서 사용할 수 있습니다. |

| 설정 | 설명 |
| --- | --- |
| | ◦ Google Chrome 및 Web View 패키지의 앱 데이터는 사용자 데이터 지우기 활성화 상태로 앱 허용 목록에 추가되어 있는 경우에도 지워지지 않습니다. 이러한 두 패키지의 앱 데이터가 지워질 경우 키오스크가 충돌할 수도 있기 때문입니다.<br>◦ 앱 런처를 사용할 수 없는 시스템 앱의 앱 데이터는 지워지지 않습니다(키오스크 내부 및 외부).<br>• **숨기기**: 이 옵션을 활성화하면 다른 앱에서 해당 앱에 액세스할 수 있지만 키오스크 런처에서는 사용할 수 없게 됩니다.<br>위 잠금 설정에서 다이얼러 또는 카메라를 비활성화한 경우 이를 허용 앱 목록에 추가할 수 없습니다. |
| 앱 카탈로그<br><br>기타 앱 | +추가를 클릭하면 앱 카탈로그의 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.<br><br>+추가를 클릭하면 Google Play Store에서 이용할 수 없는 앱의 패키지 이름를 추가할 수 있습니다.<br>Samsung 기기의 경우 관리자는 키오스크 모드에서 다이얼러 기능을 활성화하기 위해 키오스크 모드에서 기능할 수 있도록 다음 다이얼러/시스템 패키지를 허용 목록에 지정해야 합니다.<br>• 호출 - com.samsung.android.incallui<br>• 전화 - com.samsung.android.dialer(이에 대한 허용 목록을 지정해야 하며 관리자는 사용자에 대한 두 가지 다이얼러 옵션으로 인한 오류를 피하기 위해 숨김 옵션을 선택해야 함)<br>• 호출 - com.sec.phone<br>• 호출 설정 - com.samsung.android.app.telephonyui<br>• 지원된 전화 걸기 – com.sec.providers.assisteddialing<br>• 호출 로그 백업 및 복원 – com.android.calllogbackup<br>• 다이얼러 저장소 – com.android.providers.telephony<br>• 전화 – com.android.server.telecom<br>• 전화 - com.android.phone<br>• 스마트 호출 – com.samsung.android.smartcallprovider<br>• Wi-Fi 호출 – com.sec.unifiedwfc |
| 키오스크 모드 허용 앱 | X를 클릭하면 키오스크 모드 시 허용되는 앱 그룹에서 원하는 앱을 삭제할 수 있습니다. 앱을 드래그해서 키오스크 기기에서 나타나는 순서를 변경할 수 있습니다.<br>**폴더 추가** - 이 옵션을 사용하여 이 섹션 아래에 폴더를 만들고 하나 이상의 앱을 이 폴더로 이동할 수 있습니다. 최대 2단계까지 폴더를 만들 수 있습니다. 한 폴더에 복사된 앱은 다른 폴더에 복사할 수 없습니다. 폴더 내에서 25개의 앱만 지원됩니다. |
| **앱 허용 목록 생성:** 이것은 허용된 앱 목록에 앱을 추가해 키오스크 모드에서 사용자 접근이 가능한 앱입니다. 앱을 드래그해서 키오스크 모드 런처에 표시되는 앱의 배열 순서를 설정할 수 있습니다. | |

| 설정 | 설명 |
| --- | --- |
| 허용 앱 목록에 애플리케이션을 등록해도 해당 앱이 기기에 설치되지는 않습니다. 반드시 각 앱을 App Catalog에 포함되어 있는 적절한 사용자와 사용자 그룹에 배포하시기 바랍니다. | |
| 빌트인 앱 | +추가를 클릭하면 기본 내장 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.<br>키오스크 모드 허용 앱 설정에서는 다음 옵션을 사용할 수 있습니다.<br>• **앱 사용자 데이터 지우기**: 이 옵션을 활성화하면 사용자가 키오스크에서 로그아웃할 때 어떤 메시지도 없이 모든 애플리케이션 데이터가 자동으로 지워집니다.<br>키오스크 모드 설정에서 공유 기기 활성화를 선택하면 이 옵션을 애플리케이션에서 사용할 수 있습니다.<br>◦ Google Chrome 및 Web View 패키지의 앱 데이터는 사용자 데이터 지우기 활성화 상태로 앱 허용 목록에 추가되어 있는 경우에도 지워지지 않습니다. 이러한 두 패키지의 앱 데이터가 지워질 경우 키오스크가 충돌할 수도 있기 때문입니다.<br>◦ 앱 런처를 사용할 수 없는 시스템 앱의 앱 데이터는 지워지지 않습니다(키오스크 내부 및 외부).<br>• **숨기기**: 이 옵션을 활성화하면 다른 앱에서 해당 앱에 액세스할 수 있지만 키오스크 런처에서는 사용할 수 없게 됩니다.<br>위 잠금 설정에서 다이얼러 또는 카메라를 비활성화한 경우 이를 허용 앱 목록에 추가할 수 없습니다. |
| 앱 카탈로그<br><br>기타 앱 | +추가를 클릭하면 앱 카탈로그의 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.<br><br>+추가를 클릭하면 Google Play Store에서 이용할 수 없는 앱의 패키지 이름를 추가할 수 있습니다.<br>Samsung 기기의 경우 관리자는 키오스크 모드에서 다이얼러 기능을 활성화하기 위해 키오스크 모드에서 기능할 수 있도록 다음 다이얼러/시스템 패키지를 허용 목록에 지정해야 합니다.<br>• 호출 - com.samsung.android.incallui<br>• 전화 - com.samsung.android.dialer(이에 대한 허용 목록을 지정해야 하며 관리자는 사용자에 대한 두 가지 다이얼러 옵션으로 인한 오류를 피하기 위해 숨김 옵션을 선택해야 함)<br>• 호출 - com.sec.phone<br>• 호출 설정 - com.samsung.android.app.telephonyui<br>• 지원된 전화 걸기 – com.sec.providers.assisteddialing<br>• 호출 로그 백업 및 복원 – com.android.calllogbackup<br>• 다이얼러 저장소 – com.android.providers.telephony<br>• 전화 – com.android.server.telecom<br>• 전화 - com.android.phone<br>• 스마트 호출 – com.samsung.android.smartcallprovider |

| 설정 | 설명 |
| --- | --- |
| | • Wi-Fi 호출 – com.sec.unifiedwfc |
| 키오스크 모드 허용 앱 | X를 클릭하면 키오스크 모드 시 허용되는 앱 그룹에서 원하는 앱을 삭제할 수 있습니다. 앱을 드래그해서 키오스크 기기에서 나타나는 순서를 변경할 수 있습니다.<br>**폴더 추가** - 이 옵션을 사용하여 이 섹션 아래에 폴더를 만들고 하나 이상의 앱을 이 폴더로 이동할 수 있습니다. 최대 2단계까지 폴더를 만들 수 있습니다. 한 폴더에 복사된 앱은 다른 폴더에 복사할 수 없습니다. 폴더 내에서 25개의 앱만 지원됩니다. |
| 단일 앱 실행기 키오스크 활성화 | 선택하면 키오스크 모드를 사용하여 GMS 및 비GMS 기기의 전경에 앱을 유지합니다. 앱 카탈로그에서 앱을 선택하거나 패키지 ID를 입력해야 합니다. |
| **앱 허용 목록 생성:** 이것은 허용된 앱 목록에 앱을 추가해 키오스크 모드에서 사용자 접근이 가능한 앱입니다. 앱을 드래그해서 키오스크 모드 런처에 표시되는 앱의 배열 순서를 설정할 수 있습니다.<br>허용 앱 목록에 애플리케이션을 등록해도 해당 앱이 기기에 설치되지는 않습니다. 반드시 각 앱을 App Catalog에 포함되어 있는 적절한 사용자와 사용자 그룹에 배포하시기 바랍니다. | |
| 빌트인 앱 | +추가를 클릭하면 기본 내장 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.<br>키오스크 모드 허용 앱 설정에서는 다음 옵션을 사용할 수 있습니다.<br>• **앱 사용자 데이터 지우기**: 이 옵션을 활성화하면 사용자가 키오스크에서 로그아웃할 때 어떤 메시지도 없이 모든 애플리케이션 데이터가 자동으로 지워집니다.<br>키오스크 모드 설정에서 공유 기기 활성화를 선택하면 이 옵션을 애플리케이션에서 사용할 수 있습니다.<br>◦ Google Chrome 및 Web View 패키지의 앱 데이터는 사용자 데이터 지우기 활성화 상태로 앱 허용 목록에 추가되어 있는 경우에도 지워지지 않습니다. 이러한 두 패키지의 앱 데이터가 지워질 경우 키오스크가 충돌할 수도 있기 때문입니다.<br>◦ 앱 런처를 사용할 수 없는 시스템 앱의 앱 데이터는 지워지지 않습니다(키오스크 내부 및 외부).<br>• **숨기기**: 이 옵션을 활성화하면 다른 앱에서 해당 앱에 액세스할 수 있지만 키오스크 런처에서는 사용할 수 없게 됩니다.<br>위 잠금 설정에서 다이얼러 또는 카메라를 비활성화한 경우 이를 허용 앱 목록에 추가할 수 없습니다. |
| 앱 카탈로그 | +추가를 클릭하면 앱 카탈로그의 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다. |
| 기타 앱 | +추가를 클릭하면 Google Play Store에서 이용할 수 없는 앱의 패키지 이름를 추가할 수 있습니다.<br>Samsung 기기의 경우 관리자는 키오스크 모드에서 다이얼러 기능을 활성화하기 위해 키오 |

| 설정 | 설명 |
| --- | --- |
| | 스크 모드에서 기능할 수 있도록 다음 다이얼러/시스템 패키지를 허용 목록에 지정해야 합니다.<br>• 호출 - com.samsung.android.incallui<br>• 전화 - com.samsung.android.dialer(이에 대한 허용 목록을 지정해야 하며 관리자는 사용자에 대한 두 가지 다이얼러 옵션으로 인한 오류를 피하기 위해 숨김 옵션을 선택해야 함)<br>• 호출 - com.sec.phone<br>• 호출 설정 - com.samsung.android.app.telephonyui<br>• 지원된 전화 걸기 – com.sec.providers.assisteddialing<br>• 호출 로그 백업 및 복원 – com.android.calllogbackup<br>• 다이얼러 저장소 – com.android.providers.telephony<br>• 전화 – com.android.server.telecom<br>• 전화 - com.android.phone<br>• 스마트 호출 – com.samsung.android.smartcallprovider<br>• Wi-Fi 호출 – com.sec.unifiedwfc |
| 키오스크 모드 허용 앱 | X를 클릭하면 키오스크 모드 시 허용되는 앱 그룹에서 원하는 앱을 삭제할 수 있습니다. 앱을 드래그해서 키오스크 기기에서 나타나는 순서를 변경할 수 있습니다.<br>**폴더 추가** - 이 옵션을 사용하여 이 섹션 아래에 폴더를 만들고 하나 이상의 앱을 이 폴더로 이동할 수 있습니다. 최대 2단계까지 폴더를 만들 수 있습니다. 한 폴더에 복사된 앱은 다른 폴더에 복사할 수 없습니다. 폴더 내에서 25개의 앱만 지원됩니다. |
| 단일 앱 실행기 키오스크 활성화 | 선택하면 키오스크 모드를 사용하여 GMS 및 비GMS 기기의 전경에 앱을 유지합니다. 앱 카탈로그에서 앱을 선택하거나 패키지 ID를 입력해야 합니다. |
| **앱 허용 목록 생성:** 이것은 허용된 앱 목록에 앱을 추가해 키오스크 모드에서 사용자 접근이 가능한 앱입니다. 앱을 드래그해서 키오스크 모드 런처에 표시되는 앱의 배열 순서를 설정할 수 있습니다.<br>허용 앱 목록에 애플리케이션을 등록해도 해당 앱이 기기에 설치되지는 않습니다. 반드시 각 앱을 App Catalog에 포함되어 있는 적절한 사용자와 사용자 그룹에 배포하시기 바랍니다. | |
| 빌트인 앱 | +추가를 클릭하면 기본 내장 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.<br>키오스크 모드 허용 앱 설정에서는 다음 옵션을 사용할 수 있습니다.<br>• **앱 사용자 데이터 지우기**: 이 옵션을 활성화하면 사용자가 키오스크에서 로그아웃할 때 어떤 메시지도 없이 모든 애플리케이션 데이터가 자동으로 지워집니다.<br>키오스크 모드 설정에서 공유 기기 활성화를 선택하면 이 옵션을 애플리케이션에서 사용할 수 있습니다. |

| 설정 | 설명 |
| --- | --- |
| | ◦ Google Chrome 및 Web View 패키지의 앱 데이터는 사용자 데이터 지우기 활성화 상태로 앱 허용 목록에 추가되어 있는 경우에도 지워지지 않습니다. 이러한 두 패키지의 앱 데이터가 지워질 경우 키오스크가 충돌할 수도 있기 때문입니다.<br>◦ 앱 런처를 사용할 수 없는 시스템 앱의 앱 데이터는 지워지지 않습니다(키오스크 내부 및 외부).<br>• **숨기기**: 이 옵션을 활성화하면 다른 앱에서 해당 앱에 액세스할 수 있지만 키오스크 런처에서는 사용할 수 없게 됩니다.<br>위 잠금 설정에서 다이얼러 또는 카메라를 비활성화한 경우 이를 허용 앱 목록에 추가할 수 없습니다. |
| 앱 카탈로그<br><br>기타 앱 | +추가를 클릭하면 앱 카탈로그의 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.<br><br>+추가를 클릭하면 Google Play Store에서 이용할 수 없는 앱의 패키지 이름를 추가할 수 있습니다.<br>Samsung 기기의 경우 관리자는 키오스크 모드에서 다이얼러 기능을 활성화하기 위해 키오스크 모드에서 기능할 수 있도록 다음 다이얼러/시스템 패키지를 허용 목록에 지정해야 합니다.<br>• 호출 - com.samsung.android.incallui<br>• 전화 - com.samsung.android.dialer(이에 대한 허용 목록을 지정해야 하며 관리자는 사용자에 대한 두 가지 다이얼러 옵션으로 인한 오류를 피하기 위해 숨김 옵션을 선택해야 함)<br>• 호출 - com.sec.phone<br>• 호출 설정 - com.samsung.android.app.telephonyui<br>• 지원된 전화 걸기 – com.sec.providers.assisteddialing<br>• 호출 로그 백업 및 복원 – com.android.calllogbackup<br>• 다이얼러 저장소 – com.android.providers.telephony<br>• 전화 – com.android.server.telecom<br>• 전화 - com.android.phone<br>• 스마트 호출 – com.samsung.android.smartcallprovider<br>• Wi-Fi 호출 – com.sec.unifiedwfc |
| 키오스크 모드 허용 앱 | X를 클릭하면 키오스크 모드 시 허용되는 앱 그룹에서 원하는 앱을 삭제할 수 있습니다. 앱을 드래그해서 키오스크 기기에서 나타나는 순서를 변경할 수 있습니다.<br>**폴더 추가** - 이 옵션을 사용하여 이 섹션 아래에 폴더를 만들고 하나 이상의 앱을 이 폴더로 이동할 수 있습니다. 최대 2단계까지 폴더를 만들 수 있습니다. 한 폴더에 복사된 앱은 다른 폴더에 복사할 수 없습니다. 폴더 내에서 25개의 앱만 지원됩니다. |

Knox Standard 4.0 이상 Samsung 기기의 경우 키오스크 모드에서 다중 사용자 기능을 자동으로 잠급니다.

## 작업 프로필이 있는 관리 장치

Android 8.0+용 작업 프로필이 있는 관리되는 기기에서 특정 기능을 비활성화합니다.

회사 소유 기기의 작업 프로필에 대해 특정 기능을 비활성화할 수 있습니다(Android 11+ 기기에만 적용).

| 설정 | 설명 |
| --- | --- |
| **관리 기기 잠금 설정** | |
| Wi-Fi 비활성화 | 무선 LAN에 대한 액세스를 끄려면 선택합니다(Android 11+ 기기에는 적용되지 않음). |
| Wi-Fi 설정 비활성화 | 무선 기능을 끌 수 있습니다. |
| 카메라 비활성화 | 카메라 기능을 끌 수 있습니다. |
| Bluetooth 비활성화 | Bluetooth 기능을 끌 수 있습니다.<br>이 기능을 사용할 때는 주의가 필요합니다. Ivanti에서는 핸즈프리 Bluetooth 기능이 지원되지 않으므로 오디오를 끄지 않는 것이 좋습니다. 운전 중 핸즈프리 기기 사용과 관련한 법적 요건의 적용 범위가 더욱 확대되고 있습니다. |
| Bluetooth 설정 허용 불가 | Bluetooth 기능을 끌 수 있습니다. |
| 네트워크 재설정 비활성화 | 네트워크 재설정을 방지하려면 선택하세요(Android 7.0 이상 버전의 장치에 해당). |
| 마스터 볼륨 음소거 | 마스터 볼륨을 음소거할 수 있습니다. (Android 11+ 기기에는 적용되지 않음) |
| 긴급 방송 허용 불가 | 긴급 방송을 허용하지 않을 수 있습니다. |
| 모바일 네트워크 허용 불가 | 모바일 네트워크 기능을 끌 수 있습니다.<br>Wi-Fi가 꺼져 있으면 비활성화가 불가합니다. |
| 테더링 허용 불가 | 기기 1대에 인터넷을 연결한 후 해당 기기에 연결된 다른 기기에서도 인터넷을 이용할 수 있는 테더링 기능을 끌 수 있습니다. |
| VPN 허용 불가 | VPN 연결을 끌 수 있습니다. (Android 11+ 기기에는 적용되지 않음) |
| 공장 초기화 비활성화 | 사용자가 기기 설정을 기본값으로 초기화할 수 없도록 차단할 수 있습니다. (Android 11+ 기기에는 적용되지 않음) |
| 공장 초기화 보호 활성화 | 사용자가 기기 설정을 기본값으로 초기화할 수 있도록 허용할 수 있습니다.<br>필요에 따라 공장 초기화 후 기기를 프로비저닝할 수 있는 공인 Google 계정 ID(정수 값) 목록을 지정하거나 도움말 아이콘을 마우스로 가리켜서 공인 계정 ID 검색을 위한 도움말을 볼 수 있습니다. |
| 발신 전화 허용 불가 | 사용자가 발신 전화를 하지 못하도록 설정할 수 있습니다. |
| 안전 모드 허용 불가 (Android 6.0+) | 사용자가 기기를 안전 모드로 재부팅하지 못하도록 설정할 수 있습니다. |
| 디버깅 기능 허용 불가 | 기기에서 디버깅 기능을 비활성화하도록 설정할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다. |
| 앱 확인 | 기기에서 애플리케이션 검증 기능을 허용하려면 선택합니다. 기본적으로 이 옵션은 켜져 있습니다.<br>이 옵션이 꺼져 있으면 기기가 기본 동작(기기마다 다를 수 있음)으로 돌아갑니다. |
| SMS 허용 불가 | 사용자가 SMS 메시지를 송수신하지 못하도록 설정할 수 있습니다. |
| 마이크 음소거 해제 허 | 사용자가 기기의 마이크 음소거 해제를 하지 못하도록 설정할 수 있습니다. |

| 설정 | 설명 |
| --- | --- |
| 용 불가 | |
| 자동 시간 비활성화 | 사용자가 자동 시간 변경을 활성화할 수 없도록 설정할 수 있습니다. |
| 자동 표준 시간대 비활성화 | 사용자가 표준 시간대 변경으로 자동 기기 시간 조정을 활성화할 수 없도록 설정할 수 있습니다. |
| 데이터 로밍 비활성화 | 기기 로밍 중 데이터 전송 기능을 끌 수 있습니다. |
| 서버와의 동기화 시간(Android 9.0+) | 기기가 처음에는 등록 시에, 그 이후에는 매번 체크인 후 24시간마다 MDM용 Ivanti Neurons와 시간을 동기화할 수 있도록 선택합니다. 이 옵션은 **자동 시간 비활성화**를 선택할 경우에만 사용할 수 있게 됩니다. |
| 시간대 설정(Android 9.0+) | 시간대 문자열을 Olson Time Zone ID 형식(예: Pacific/Midway)으로 지정합니다. |
| Wi-Fi 절전 모드 비활성화 | 기기가 절전 모드일 때 Wi-Fi를 유지할 수 있습니다. (Android 11+ 기기에는 적용되지 않음) |
| 입력 방법 제한 | **패키지 이름** 필드를 통해 허용 목록에 있는 패키지 이름 목록을 지정하여 작업 앱의 입력 방법을 제한하려면 선택합니다(Android 11+ 기기에는 적용되지 않음).<br>기기에서는 허용 패키지 입력 방법 및 기본 시스템 입력 방법 둘 다를 사용할 수 있게 됩니다.<br>사용자는 기본 시스템 입력 방법과 허용 목록에 있는 패키지 입력 방법 사이에서 전환할 수 있습니다.<br>Android 10+에서는 입력 방법이 기기 쪽에만 적용되고 그 외 경우에는 전체 기기로 제한됩니다. |
| 접근성 서비스 제한 | **패키지 이름** 필드를 통해 허용 패키지 이름 목록을 지정하여 작업 앱의 접근성 서비스를 제한하도록 선택할 수 있습니다. 허용 목록 패키지가 없는 경우에는 시스템 접근성 서비스만 허용됩니다.<br>Android 10+에서는 입력 방법이 Work Apps로만 제한되고 그 외 경우에는 전체 기기로 제한됩니다. |
| USB 파일 전송 비활성화 | USB 파일 전송을 비활성화하도록 설정합니다. |
| 외부 미디어 비활성화 | 외부 미디어를 비활성화하도록 설정합니다. |
| 기기에서 알 수 없는 소스 허용 안 함 | 기기가 알 수 없는 소스의 앱을 설치하지 못하도록 설정할 수 있습니다.<br>이 설정은 기기에 적용되기 위해 Google Play 업데이트에 종속되어 이 기능을 활성화합니다. |
| 잠금 화면 메시지 설정(Android 7.0+) | 기기에 표시될 잠금 화면 메시지 설정을 선택합니다. 텍스트 필드에 잠금 화면 메시지(최대 256자)를 입력합니다. 이 옵션을 활성화하면, 사용자가 설정에서 메시지를 설정할 수 없으며 관리자가 설정하는 메시지가 사용자에게 표시됩니다.<br>관리자가 '잠금 화면 메시지 설정'을 활성화한 후 잠금 화면 메시지도 제공하지 않을 경우 사용자는 설정에서 메시지를 설정할 수는 없으나, 어떠한 메시지도 사용자에게 표시되지 않습니다. |
| 화면 밝기 설정 | 기기 화면의 밝기를 설정하려면 선택합니다.<br>• 수동 - 수동으로 숫자 입력(0~255)<br>• 적응 - 기기에서 자동으로 밝기 설정<br>기기 화면의 밝기를 설정하기 전에 '밝기 구성 허용 안 함'을 활성화하는 것이 좋습니다.<br>이 사용자의 변경이 허용되는 경우 이러한 설정은 다음 체크인 시 관리자 지정 설정으로 재설정됩니다.<br>Android 11 이상 버전의 기기에서는 회사 소유 기기의 직장 프로필 모드에 대한 이러한 설정을 지원하지 않습니다. |

| 설정 | 설명 |
| --- | --- |
| 화면 시간제한 설정 | 화면 시간제한(초)을 설정하려면 선택합니다.<br>기기 화면의 밝기를 설정하기 전에 '화면 시간제한 구성 허용 안 함'을 활성화하는 것이 좋습니다.<br>이 사용자의 변경이 허용되는 경우 이러한 설정은 다음 체크인 시 관리자 지정 설정으로 재설정됩니다.<br>Android 11 이상 버전의 기기에서는 회사 소유 기기의 직장 프로필 모드에 대한 이러한 설정을 지원하지 않습니다. |
| 화면 방향 설정 | 화면 방향을 설정하려면 선택합니다. 화면 방향을 드롭다운 목록에서 0, 90, 180, 270도로 설정할 수 있습니다.<br>Android 11 이상 버전의 기기에서는 회사 소유 기기의 직장 프로필 모드에 대한 이러한 설정을 지원하지 않습니다. |
| 자동 채우기 허용 불가(Android 8.0+) | 자동 채우기를 허용하지 않으려면 선택합니다. (Android 11+ 기기에는 적용되지 않음) |
| Bluetooth 공유 허용 불가(Android 8.0+) | 사용자가 기기의 발신 Bluetooth를 공유하지 못하도록 합니다. |
| 백업 서비스 비활성화(Android 8.0+) | 백업 서비스를 사용하지 못하도록 합니다. (Android 11+ 기기에는 적용되지 않음) |
| 인쇄 허용 불가(Android 9.0+) | 모든 앱에서 인쇄를 제한하려면 선택합니다(Android 11+ 기기에는 적용되지 않음). |
| 비행기 모드 허용 불가(Android 9.0+) | 전체 기기에서 비행기 모드를 사용하지 못하도록 합니다. |
| 주변 표시 허용 불가(Android 9.0+) | 사용자의 주변 표시를 못하도록 합니다. (Android 11+ 기기에는 적용되지 않음) |
| 밝기 구성 허용 불가(Android 9.0+) | 사용자의 밝기 구성을 허용하지 않으려면 선택합니다(Android 11+ 기기에는 적용되지 않음).<br>이 옵션을 선택하기 전에 '화면 밝기 모드 설정'을 정의하는 것이 좋습니다. |
| 날짜/시간 구성 허용 불가(Android 9.0+) | 날짜, 시간 및 시간대를 구성하지 못하도록 합니다. |
| 위치 구성 허용 불가(Android 9.0+) | 사용자가 위치 공급자를 사용하지 못하도록 합니다. |
| 화면 시간 제한 구성 허용 불가(Android 9.0+) | 사용자의 화면 끄기 시간제한 변경을 허용하지 않으려면 선택합니다. (Android 11+ 기기에는 적용되지 않음)<br>이 옵션을 선택하기 전에 '화면 시간제한 설정' 값을 설정하는 것이 좋습니다. |
| 시스템 오류 대화 상자 허용 불가(Android 9.0+) | 시스템 오류 대화 상자를 허용하지 않으려면 선택합니다(Android 11+ 기기에는 적용되지 않음). |
| 화면 캡처 비활성화(Android 11.0+)<br>**Android 12.0+** | 기기에 내장된 화면 캡처 기능을 끌 수 있습니다. 선택하면 기기의 개인 공간에서 화면 캡처가 비활성화됩니다. |

| 설정 | 설명 |
| --- | --- |
| 충전 전용 USB 활성화 | USB 포트를 충전 전용으로 활성화하려면 선택합니다. |
| **Android 13.0+** | |
| 필요한 최소 Wi-Fi 보안 설정 | 이 옵션을 이용해 다음과 같이 필요한 최소 Wi-Fi 보안을 설정하십시오.<br>• 최소 보안이 필요하지 않음 – 최소 보안이 필요하지 않은 경우 선택<br>• 개인 네트워크 기반 보안 – WEP, WPA/WPA2/WPA3 등의 개인 Wi-Fi 네트워크 차단<br>• Enterprise EAP 네트워크 기반 보안 – EAP 프로토콜 기반 Wi-Fi 네트워크 차단<br>• Enterprise 192 네트워크 기반 보안 - EAP 회사 기반 Wi-Fi 네트워크 차단<br>최소 기준을 충족하지 않는 기존 기기의 연결을 모두 해제합니다.<br>기기 세부 정보에서 **일반 > Wi-Fi 보안 수준** 아래에 필요한 최소 Wi-Fi 보안 수준(해당하는 경우)이 표시됩니다. |
| 관리자가 구성한 Wi-Fi 공유 금지 | 관리자가 설정한 Wi-Fi 구성을 사용자가 공유하지 못하도록 하려면 선택합니다. |
| **작업 프로필 잠금 설정** | |
| 화면 캡처 비활성화 | 기기에 내장된 화면 캡처 기능을 끌 수 있습니다. |
| 앱 제어 금지 | 사용자가 설정 또는 런처에서 애플리케이션을 수정하지 못하도록 설정할 수 있습니다. |
| 구성 자격 증명 금지 | 사용자가 사용자 자격 증명을 구성하지 못하도록 설정할 수 있습니다. |
| 교차 프로필 복사 붙여넣기 금지 | 프로필 간 정보의 복사/붙여놓기를 금지하도록 설정할 수 있습니다. |
| 계정 수정 금지 | 사용자가 계정을 추가 또는 제거하지 못하도록 설정할 수 있습니다. |
| NFC(플래시 불빛) 금지 (Android 5.1+) | 사용자가 NFC를 이용해 앱 데이터를 전송하지 못하도록 하려면 이 옵션을 선택합니다. |
| 위치 공유 금지 | 웹사이트 및 앱에서 기기 사용자가 기기 위치를 공유하지 못하도록 하려면 이 옵션을 선택합니다. |
| 디버깅 기능 허용 불가 | 기기에서 디버깅 기능을 비활성화하도록 설정할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다. |
| 앱 확인 | 기기에서 애플리케이션 검증 기능을 허용하려면 선택합니다. 기본적으로 이 옵션은 켜져 있습니다.<br>이 옵션이 꺼져 있으면 기기가 기본 동작(기기마다 다를 수 있음)으로 돌아갑니다. |
| 작업 프로필 내에서 알 수 없는 소스 비활성화 | 작업 프로필 내에서 알 수 없는 소스로부터의 다운로드를 허용하지 않으려면 선택합니다. |
| 시스템 앱 활성화/비활성화 | **시스템 앱 패키지 이름** 필드를 통해 2개의 패키지 이름 목록을 지정하여 시스템 애플리케이션 배포를 활성화 및 비활성화하려면 선택합니다. 이 기능을 사용하여 Google Play에 게시되지 않은 시스템 애플리케이션에 대한 액세스 권한을 관리할 수 있습니다.<br>App Catalog에 앱을 추가하고 시스템 앱에도 추가하는 작업은 지원되지 않습니다. |
| 발신자 ID 비활성화 (Android 6.0 이상) | 작업 프로필의 발신자 ID 정보가 전화 수신 시 기기에 표시될지 여부를 설정합니다. |

| 설정 | 설명 |
| --- | --- |
| Bluetooth를 통한 연락처 공유 비활성화 (Android 6.0+) | 기기가 Bluetooth를 통해 다른 기기와 연락처를 공유하지 못하도록 하려면 선택합니다. |
| 검색을 통한 연락처 공유 비활성화(Android 7.0+) | 사용자가 개인 폰 다이얼러에서 회사 연락처를 검색하지 못하도록 하려면 선택합니다. |
| 자동 채우기 허용 불가 (Android 8.0+) | 자동 채우기를 허용하지 않으려면 선택합니다. (Android 11+ 기기에는 적용되지 않음) |
| 개인 프로필에서 작업 앱 알림 허용 불가 (Android 8.0+) | 작업 프로필 알림을 제한하려면 선택합니다. |
| 인쇄 허용 불가(Android 9.0+) | 모든 앱에서 인쇄를 제한하려면 선택합니다. (Android 11+ 기기에는 적용되지 않음) |
| 프로필에서 공유 허용 불가(Android 9.0+) | 기기의 작업 프로필에서 사용자들이 개인 데이터를 공유하지 못하도록 하려면 선택합니다. |
| 입력 방법 제한(Android 10.0+) | **패키지 이름** 필드를 통해 허용 패키지 이름 목록을 지정하여 허용되는 IME 패키지 이름을 제한하도록 선택할 수 있습니다(Android 11+ 기기에는 적용되지 않음).<br>기기에서는 허용 패키지 입력 방법 및 기본 시스템 입력 방법 둘 다를 사용할 수 있게 됩니다.<br>사용자는 기본 시스템 입력 방법과 허용 목록에 있는 패키지 입력 방법 사이에서 전환할 수 있습니다.<br>작업 프로필 공간에 설치된 IME 앱에 대한 입력 방법이 적용됩니다. 이 기기 공간에 설치된 앱이 이 잠금에 대해 허용 목록으로 지정되었다고 하더라도 작업 프로필 공간에서 사용하는 앱에서 사용할 수 없습니다. |
| 작업 프로필 캘린더에 대한 액세스 허용 (Android 10.0+) | 다음 옵션 중 어느 것이든 선택하여 모든 앱을 허용하거나 개인 공간의 앱 집합을 선택하여 작업 프로필에 있는 캘린더 정보에 액세스합니다.<br>• **개인 프로필의 모든 앱** - 모든 앱이 작업 프로필에 있는 캘린더 정보에 액세스할 수 있도록 허용<br>• **개인 프로필의 다음 앱만** - 아래 텍스트 필드에서, 쉼표로 구분한 앱의 번들 ID 입력. 개인 공간에서 선택한 이 앱만 작업 프로필에 있는 캘린더 정보에 액세스할 수 있게 됩니다.<br>개인 공간의 앱은 공유 캘린더에 액세스할 수 있도록 특정 API를 구현해야 합니다. |
| 앱의 교차 프로필 허용 목록 적용 설정(Android 11.0+) | 사용자가 작업 프로필 내의 특정 앱에 있는 정보를 기기의 개인 공간으로 가져와 공유할 수 있게 하려면 이 체크박스를 선택합니다.<br>**허용 목록에 등록된 앱** 필드에서 허용 목록에 등록할 앱의 패키지 ID를 쉼표로 구분하여 입력합니다.<br>기본적으로 이 옵션은 비활성화되어 있습니다. |
| 최대 프로필 시간 제한 활성화(Android 11.0+) | 최대 시간 창 설정을 선택하면 MDM용 Ivanti Neurons가 기기에서 개인 앱을 일시 중지하기 전에 작업 프로필을 끌 수 있습니다. 72 ~ 8,760시간으로 시간을 설정할 수 있습니다. 8,760시간은 1년입니다.<br>옵션을 선택할 경우 기본 값은 72시간으로 설정됩니다.<br>기기 사용자는 일시 중지된 앱을 활성화하기 위해 작업 프로필을 켜라는 메시지를 봅니다. 회사 소유 기기의 작업 프로필에 있는 Android 11+ 기기에 대해 이용할 수 있습니다.<br>프로필이 장시간 꺼져 있으면 기기에서 개인 앱이 중단됩니다. |

| 설정 | 설명 |
| --- | --- |
| 5G 네트워크 슬라이싱 활성화(Android 12.0+) | 회사 소유 장치의 작업 프로필에 5G 네트워크 슬라이싱 옵션을 제공하려면 선택합니다.<br>기본적으로 이 옵션은 비활성화되어 있습니다. |
| AI 지원 비활성화 (Android 15.0+) | 사용자가 AI Assist 기능을 사용하지 못하도록 하려면 선택합니다.<br>기본적으로 이 옵션은 비활성화되어 있습니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.33. 잠금 및 키오스크: Samsung Knox 표준

잠금 및 키오스크: Samsung Knox Standard 구성은 Samsung Knox Standard 기기의 특정 기능을 비활성화하고 키오스크 모드에서 사용자가 이용할 수 있는 앱의 허용 목록을 생성합니다.

> Samsung KNOX 표준 구성은 더 이상 사용되지 않으며 Android 9 이상 버전이 있는 장치에서 지원되지 않습니다.

## 잠금 설정

**설정**

**설정하기**

이름

현재 설정을 식별할 수 있는 고유한 이름을 입력합니다.

설명

현재 설정에 대한 간략한 설명을 입력합니다.

**Samsung Knox 잠금 설정:** Samsung Knox 기기의 특정 기능만 비활성화합니다.

Wi-Fi 비활성화

무선 랜 기능을 끌 수 있습니다.

카메라 비활성화

카메라 기능을 끌 수 있습니다.

Bluetooth 비활성화

Bluetooth 기능을 끌 수 있습니다.

Bluetooth 오디오에만 허용

Bluetooth 오디오 기능만 켜도록 선택합니다.

모바일 데이터 비활성화

기기 간 터치를 통한 데이터 전송 기능을 끌 수 있습니다.

Wi-Fi가 꺼져 있으면 비활성화가 불가합니다.

GPS 비활성화

GPS 기능을 끌 수 있습니다.

폰 다이얼러 기능 비활성화

전화 앱 기능을 끌 수 있습니다.

SD 카드 비활성화

SD 카드 기능을 끌 수 있습니다.

Google 백업 비활성화

Google 서버 백업 기능을 끌 수 있습니다.

복사/붙여넣기 비활성화

복사/붙여넣기 기능을 끌 수 있습니다.

NFC 비활성화

기기 간 터치를 통한 NFC(근거리 무선통신) 데이터 전송 기능을 끌 수 있습니다.

마이크 비활성화

기기 마이크 앱 연결 기능을 끌 수 있습니다.

화면 캡처 비활성화

기기에 내장된 화면 캡처 기능을 끌 수 있습니다. 이 옵션을 켜면 Go의 화면 캡처 기능이 허용되지 않습니다. 이러한 화면 캡처 기능은 허용되지 않습니다.

Bluetooth 테더링 비활성화

장치 1대에 인터넷을 연결한 후 해당 장치에 연결된 다른 장치에서도 인터넷을 이용할 수 있는 Bluetooth 테더링 기능을 끌 수 있습니다.

USB 디버그 비활성화

USB 디버깅 기능을 끌 수 있습니다.

USB 테더링 비활성화

장치 1대에 인터넷을 연결한 후 해당 장치에 연결된 다른 장치에서도 인터넷을 이용할 수 있는 Bluetooth 테더링 기능을 끌 수 있습니다.

Wi-Fi 테더링 비활성화

장치 1대에 인터넷을 연결한 후 해당 장치에 연결된 다른 장치에서도 인터넷을 이용할 수 있는 Wi-Fi 테더링 기능을 끌 수 있습니다.

기본 브라우저 비활성화

사용자의 Android 브라우저 이용을 차단할 수 있습니다.

YouTube 비활성화

사용자의 YouTube 이용을 차단할 수 있습니다.

공장 초기화 비활성화

사용자가 장치 설정을 기본값으로 초기화할 수 없도록 차단할 수 있습니다.

OTA 업그레이드 비활성화

장치 펌웨어 무선 업그레이드 기능을 끌 수 있습니다.

경고: **OTA 업그레이드**가 활성화된 경우 **설정 변경 비활성화**를 비활성화하지 마십시오. **OTA 업그레이드**가 설정된 상태에서 **설정 변경 비활성화**를 진행할 경우 기기의 기능에 영향을 줄 수 있습니다. 업그레이드를 위해서는 설정을 변경해야 하기 때문입니다.

음성 로밍 비활성화

기기 로밍 중 음성 전화 기능을 끌 수 있습니다.

USB Media Player 비활성화

USB 미디어 플레이어 기능을 끌 수 있습니다.

Google Play 비활성화

Google Play 기능을 끌 수 있습니다.

데이터 로밍 비활성화

기기 로밍 중 데이터 전송 기능을 끌 수 있습니다.

알 수 없는 소스 비활성화

모든 곳에서 앱 설치를 비활성화합니다. 단, Go 앱을 제외한 Google Play Store는 예외입니다.

기기 관리자 권한 제거 비활성화

Go에서 사용자가 기기 관리자 권한을 끄지 못하게 하려면 이 옵션을 선택합니다.

설정 변경 비활성화

장치 설정 앱 기능을 끌 수 있습니다.

경고: **OTA 업그레이드**가 활성화된 경우 **설정 변경 비활성화**를 비활성화하지 마십시오. **OTA 업그레이드**가 설정된 상태에서 **설정 변경 비활성화**를 진행할 경우 기기의 기능에 영향을 줄 수 있습니다. 업그레이드를 위해서는 설정을 변경해야 하기 때문입니다.

**키오스크 모드 설정:** 키오스크 모드에는 사용자 지정 런처를 통한 앱 접근 제한 등 기기에 추가적인 제한이 설정됩니다.

Android 버전 8.1까지 적용 가능합니다. Android 버전 9.0의 경우 Android Enterprise 관리 기기 키오스크 구성을 사용합니다.

키오스크 모드 활성화

Android 기기의 키오스크 모드를 설정할 수 있습니다.

사용자의 Wi-Fi 설정 허용

사용자가 Wi-Fi 설정을 변경하고 선호하는 무선 네트워크에 액세스할 수 있도록 선택합니다.

Bluetooth 설정에 대한 사용자 액세스 허용

사용자가 Bluetooth 설정을 변경하고 별도의 Bluetooth 기기를 페어링할 수 있도록 선택합니다.

사용자의 애플리케이션 업데이트 지연 허용

사용자가 애플리케이션 업데이트를 지연할 수 있도록 선택합니다.

GPS 위치 설정

다음의 GPS 위치 중 하나를 선택합니다.

- 위치 비활성화
- 위치 활성화
- 사용자가 선택할 수 있음

키오스크 종료 PIN

최종 사용자가 키오스크 모드 종료 시 입력해야 하는 4자리 코드를 입력할 수 있습니다.

**앱 허용 목록 생성:** 이것은 허용된 앱 목록에 앱을 추가해 키오스크 모드에서 사용자 접근이 가능한 앱입니다. 앱을 드래그해서 키오스크 모드 런처에 표시되는 앱의 배열 순서를 설정할 수 있습니다.

허용 앱 목록에 애플리케이션을 등록해도 해당 앱이 기기에 설치되지는 않습니다. 반드시 각 앱을 App Catalog에 포함되어 있는 적절한 사용자와 사용자 그룹에 배포하시기 바랍니다.

빌트인 앱

+추가를 클릭하면 기본 내장 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.

위 잠금 설정에서 다이얼러 또는 카메라를 비활성화한 경우 이를 허용 앱 목록에 추가할 수 없습니다.

앱 카탈로그

+추가를 클릭하면 앱 카탈로그의 앱 목록을 키오스크 모드 시 허용되는 앱 그룹에 추가할 수 있습니다.

기타 앱

+추가를 클릭하면 Google Play Store에서 이용할 수 없는 앱의 **패키지 이름**를 추가할 수 있습니다.

키오스크 모드 허용 앱

X를 클릭하면 키오스크 모드 시 허용되는 앱 그룹에서 원하는 앱을 삭제할 수 있습니다. 앱을 드래그해서 키오스크 기기에서 나타나는 순서를 변경할 수 있습니다.

> Android 4.4 또는 지원되는 최신 버전에서 키오스크 모드를 사용했을 때 다중 사용자를 지원하는 Samsung 기기는 키오스크 모드에서 다중 사용자 기능을 자동으로 잠급니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.34. 로컬 관리자 암호 솔루션 구성

**로컬 관리자 암호 솔루션(LAPS)** 구성 설정을 사용하면 MDM용 Ivanti Neurons 관리자가 관리형 macOS 기기에서 로컬 관리자 비밀번호를 설정된 간격으로 자동 재생성할 수 있습니다. LAPS에 대한 자세한 내용은 **LAPS(로컬 관리 비밀번호 솔루션)**을 참조하십시오.

**적용 대상**: 자동화된 기기 등록을 통해 등록 및 관리되는 macOS 기기.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **로컬 관리자 암호 솔루션(LAPS)** 구성을 검색하여 선택합니다.
3. 다음 표에 따라 **LAPS** 설정을 구성합니다.

| 설정 항목 | 설명 |
|---|---|
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **플랫폼** | 드롭다운에서 macOS를 선택합니다. |
| **변경 주기** | 드롭다운 목록에서 다음 옵션 중 하나를 선택하여 비밀번호의 자동 회전을 정의합니다.<br>• 회전 안 함(**기본값**)<br>• 15일<br>• 30일<br>• 60일<br>• 90일<br>• 120일<br>• 180일 |
| **조회 후 변경 간격** | 드롭다운 목록에서 다음 옵션 중 하나를 선택하여 **기기 상세 정보** 페이지에서 비밀번호를 확인한 후 자동으로 비밀번호를 회전합니다.<br>• 1~24시간<br>• 36시간<br>• 48시간<br>기본값은 **2시간**으로 설정되어 있습니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. **로컬 관리자 암호 솔루션(LAPS)** 구성을 설정하려면 배포 옵션 중 하나를 선택합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.35. macOS 방화벽

**라이센스:** Gold

macOS 방화벽이 macOS 기기의 보안 기본 설정 창에서 액세스할 수 있는 애플리케이션 방화벽 설정을 관리합니다.

**적용 대상**: macOS 12.3+

- **들어오는 연결을 내장 소프트웨어에서 수신하도록 허용** - true일 경우 내장 소프트웨어가 들어오는 연결을 수신하도록 허용합니다.
- **들어오는 연결을 다운로드되어 서명된 소프트웨어에서 수신하도록 허용** - true일 경우 다운로드되어 서명된 소프트웨어가 들어오는 연결을 수신하도록 허용합니다.

**적용 대상**: macOS 12.0+

- **로깅 활성화** - true일 경우 로깅을 활성화합니다
- **로깅 유형 지정**
  - **제한**
  - **간략**
  - **세부 정보**

**적용:** macOS 10.12+

**방화벽 활성화**를 클릭하면 다음 옵션 중 하나 이상을 선택할 수 있습니다.

- **모든 수신 차단** - macOS 장치에서 화면 공유나 파일 공유 등 모든 공유 서비스가 수신 연결을 수신하지 않게 방지하려면 선택합니다. 다음 시스템 서비스는 여전히 수신 연결을 받을 수 있습니다.
  - configd(DHCP 및 기타 네트워크 구성 서비스 구현)
  - mDNSResponder(Bonjour 구현)
  - racoon(IPSec 구현)
- **은폐 모드 사용** - macOS 장치가 조사 요청에 응답하지 못하도록 하려면 선택합니다. 관리되는 macOS 장치는 승인된 앱에 대한 수신 요청에는 여전히 응답하지만, ICMP(ping)와 같은 예상치 못한 요청은 무시합니다.
- **애플리케이션** - 방화벽으로 연결이 제어되는 애플리케이션 목록입니다 macOS 장치에서 수신 연결을 받으려는 특정 앱을 선택합니다.

**추가+**를 선택하여 앱 목록에 한 행을 추가합니다. **번들 ID** 아래의 셀을 선택하여 수신 연결을 명시적으로 허용할 앱을 선택합니다. **연결 허용** 셀에서 확인란을 선택하여 선택한 앱에서 수신되는 연결을 허용합니다.

> 구성이 시스템 범위 프로필에 존재해야 합니다. 두 개 이상의 프로필에 이 구성이 포함되어 있는 경우 가장 제한적인 설정 조합이 사용됩니다.

> **서명되어 다운로드된 소프트웨어 자동 허용** 및 **내장 소프트웨어 자동 허용** 옵션은 지원되지 않습니다. 그러나 이 구성을 사용할 수 있으면 두 옵션 모두 강제로 켜집니다.

> 관리자는 Ping 명령으로 발견할 수 없는 기기를 지정하여 은폐 모드를 활성화할 수 있습니다.

# 10.10.4.36. macOS 제한

**라이센스:** Gold

macOS 제한은 macOS 기기에서 활성화되는 제한을 결정합니다.

macOS 기기에서 다음 기능을 활성화 또는 비활성화하도록 설정할 수 있습니다.

| macOS 버전 | 기능 |
| --- | --- |
| **macOS 10.11+** | • 카메라 허용<br>• iCloud 문서 동기화 허용<br>**감독 전용:**<br>• Spotlight 인터넷 결과 허용 |
| **macOS 10.11.2+** | • 정의 조회 허용 |
| **macOS 10.12+** | • iCloud 키체인 동기화 허용<br>• 내 Mac으로 돌아가기 허용<br>• 내 Mac 찾기 허용<br>• 메모, 알림 또는 LinkedIn에 공유 허용<br>• 북마크 동기화 허용<br>• macOS 메일 iCloud 서비스 허용<br>• macOS iCloud 달력 서비스 허용<br>• macOS iCloud 주소록 서비스 허용<br>• iCloud 알림 서비스 허용<br>• 자동 잠금 해제 허용<br>**감독 전용:**<br>• Apple Music 허용 |
| **macOS 10.12.4+** | • 잠금 해제를 위해 지문 허용 |
| **macOS 10.13+** | • iTunes 파일 공유 허용<br>• 콘텐츠 캐싱 허용<br>• 배경화면 수정 허용<br>**감독 전용:**<br>• AirPrint 허용<br>• AirPrint iBeacon 탐색 허용 |

| macOS 버전 | 기능 |
| --- | --- |
| | • AirPrint에서 신뢰할 수 있는 TLS 강제 요구 사항<br>• AirDrop 허용<br>• 게임 센터 허용 |
| **macOS 10.13 4+** | **감독 전용:**<br>일정 기간(30일에서 90일) 동안 소프트웨어 업데이트<br>기본값: 30일. |
| **macOS 10.14+** | |
| **macOS 10.14.4+** | **감독 전용:**<br>주변 장치의 암호 요청 공유 허용<br>• 스크린샷 허용<br>• 원격 화면 관찰 허용<br>**감독 전용:**<br>• Classroom에 자동으로 참여 허용<br>• Classroom이 수업에서 나갈 권한 요청 허용<br>• 메시지를 표시하지 않고 앱 잠금 및 기기 잠금에 Classroom 허용<br>• 요청하지 않은 관리되는 교실 화면 관찰 강제 허용 |
| **macOS 11.0+** | |
| **macOS 11.3+** | **감독 전용:**<br>앱 소프트웨어 업데이트 강제 지연 허용<br>적용된 지문 시간 제한<br>기본: 48시간<br>필수 구성 요소: 장치에서 터치 ID가 구성되어 있어야 합니다. |
| **macOS 11.3+** | **감독 전용:**<br>• 강제적 소프트웨어 업데이트 주요 OS 지연된 설치 지연 |

| macOS 버전 | 기능 |
| --- | --- |
| | • 강제적 소프트웨어 업데이트 부 OS 지연된 설치 지연<br>• 강제적 소프트웨어 업데이트 비 OS 지연된 설치 지연<br>• 강제 지연된 주요 소프트웨어 업데이트 |
| **macOS 12+** | |
| | • allowCloudPrivateRelay: macOS 장치에서 비공개 릴레이를 켜짐으로 설정한 경우 네트워크 트래픽을 암호화하여 인터넷 활동을 비공개로 유지하고 보호합니다. 이 제한에는 감독 중인 장치가 필요합니다.<br>• iCloud 포토 라이브러리 허용<br>**감독 대상만 해당**:<br>• 콘텐츠 및 설정 지우기 허용 |
| **macOS 13.0~26.0** | |
| | • 백그라운드 보안 개선 설치 허용: 응답을 비활성화합니다. 사용자가 백그라운드 보안 개선을 설치할 수 없습니다.<br>• 백그라운드 보안 개선 제거 허용: 사용자가 응답의 실행을 취소할 수 없도록 차단합니다. 사용자가 백그라운드 보안 개선을 제거할 수 없습니다.<br>• 범용 제어 허용:<br>◦ **참**이면 구성에서 기본 기기의 입력 기기를 사용하여 보조 디스플레이 기기를 제어할 수 있습니다.<br>◦ **거짓**이면 보조 디스플레이 기기를 추가할 수 있지만 기본 입력 기기로 제어할 수는 없습니다.<br>**감독 대상만 해당**:<br>• UI 구성 프로필 설치 허용 - 거짓이면 구성에서 macOS 기기에 프로필, 구성, 인증서의 설치가 허용되지 않습니다.<br>• USB 제한 모드 허용 - 참이면 구성에서 원격으로 연결된 입력 기기를 사용할 수 없도록 기기를 잠급니다. 장치에서 액세서리 연결 허용 옵션이 회색으로 표시됩니다. |
| **macOS 14.0+** | |
| | • ARD 원격 관리 수정 허용<br>◦ 거짓인 경우 시스템 설정에서 원격 관리 공유 설정을 수정할 수 없습니다.<br>◦ 기본: True<br>• Bluetooth 공유 수정 허용<br>◦ 거짓인 경우 시스템 설정에서 Bluetooth 설정을 수정할 수 없습니다.<br>◦ 기본: True<br>• 클라우드 자유형 허용<br>◦ 거짓인 경우 iCloud Freeform 서비스를 허용하지 않습니다.<br>◦ 기본: True<br>• 파일 공유 수정 허용<br>◦ 거짓인 경우 시스템 설정에서 파일 공유 설정을 수정할 수 없습니다. |

| macOS 버전 | 기능 |
| --- | --- |
| | ◦ 기본: True<br>• 인터넷 공유 수정 허용<br>◦ 거짓인 경우 시스템 설정에서 인터넷 공유 설정을 수정할 수 없습니다.<br>◦ 기본: True<br>• 로컬 사용자 생성 허용<br>◦ 거짓인 경우 시스템 설정에서 새 사용자를 생성할 수 없습니다.<br>◦ 기본: True<br>• 프린터 공유 수정 허용<br>◦ 거짓인 경우 시스템 설정에서 프린터 공유 설정을 수정할 수 없습니다.<br>◦ 기본: True<br>• 원격 Apple 이벤트 수정 허용<br>◦ 거짓인 경우 시스템 설정에서 원격 Apple 이벤트 공유 설정을 수정할 수 없습니다.<br>◦ 기본: True<br>• Siri 허용<br>◦ 기본: True<br>• 시동 디스크 수정 허용<br>◦ 거짓인 경우 시스템 설정에서 시동 디스크 설정을 수정할 수 없습니다.<br>◦ 기본: True<br>• Time Machine 백업 허용<br>◦ 거짓인 경우 시스템 설정에서 Time Machine 설정을 수정할 수 없습니다.<br>◦ 기본: True<br>**감독 대상만 해당**:<br>• 계정 수정 허용<br>◦ False인 경우 계정 수정을 방지합니다.<br>◦ 기본: True<br>• 장치 이름 수정 허용<br>◦ False인 경우 장치 이름이 변경되지 않습니다.<br>◦ 기본: True<br>• TouchID 지문 수정 허용<br>◦ False인 경우 Touch ID 지문이 수정되지 않습니다.<br>◦ 기본: True |
| **macOS 15.0+** | **감독 대상만 해당**:<br>• 젠모지 허용 |

| macOS 버전 | 기능 |
| --- | --- |
| | ◦ 젠모지 생성을 허용하려면 선택합니다.<br>◦ 기본: True<br>• 이미지 플레이그라운드 허용<br>◦ 이미지 생성의 사용을 허용하려면 선택합니다.<br>◦ 기본: True<br>• iPhone 미러링 허용<br>◦ iPhone이 macOS 기기에서 미러링하도록 허용하려면 선택합니다.<br>◦ 기본: True<br>• 쓰기 도구 허용<br>◦ Apple Intelligence 쓰기 도구를 활성화하려면 선택합니다.<br>◦ 기본: True |
| **macOS 15.1+** | **감독 대상만 해당**:<br>• 메일 요약 허용<br>◦ 선택하여 이메일 메시지 요약을 수동으로 생성합니다.<br>◦ 기본: True<br>• 미디어 공유 수정 허용<br>◦ 선택하여 미디어 공유 설정을 수정합니다.<br>◦ 기본: True |
| **macOS 15.2+** | **감독 대상만 해당**:<br>• 외부 인텔리전스 통합 허용<br>◦ 선택하여 Siri에서 외부 클라우드 기반 인텔리전스 서비스를 사용하도록 설정합니다.<br>◦ 기본: True<br>• 외부 인텔리전스 통합 로그인 허용<br>◦ 선택하여 기본 브라우저 환경 설정 수정을 활성화합니다. 기본 브라우저 환경 설정을 지정하는 MDM용 Ivanti Neurons 설정 명령은 이 설정이 적용되어도 계속 작동합니다.<br>◦ 기본: True |
| **macOS 15.3** | **보안 및 개인 정보 보호**:<br>• 외부 인텔리전스 작업 영역 ID 허용 |

| macOS 버전 | 기능 |
| --- | --- |
| | ◦ 허용되는 외부 인텔리전스 작업 영역 ID 입력<br>• 메모 받아쓰기 요약 허용<br>◦ 대화 기록에서 요약 생성을 활성화하려면 선택합니다.<br>◦ 기본값: 참 |

# 10.10.4.37. macOS 앱스토어 제한 사항

**라이센스:** Gold

macOS AppStore 제한 사항은 macOS AppStore에서 활성화되는 제한을 정의합니다.

다음과 같은 옵션을 설정할 수 있습니다.

| **설정** | **설정하기** |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **구성 설정** | |
| **macOS 버전** | **기능** |
| 10.9+ | 앱 설치를 관리자로 제한합니다. |
| 10.10+ | • 앱 설치를 소프트웨어 업데이트로만 제한합니다.<br>• 사용자가 앱 채택을 비활성화합니다.<br>• 소프트웨어 업데이트 알림을 비활성화합니다. |
| 10.11+ | 앱 설치를 MDM-설치 앱 및 소프트웨어 업데이트로 제한합니다. |

## 구성 배포 중

**절차**

1. 이전 표를 사용하여 옵션을 설정합니다.
2. **다음**을 클릭하세요.
3. **이 구성 활성화** 옵션을 선택합니다.
4. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정

**완료**를 클릭하세요.

# 10.10.4.38. macOS 디스크 굽기 제한 사항

**라이센스:** Gold

macOS의 디스크 굽기 제한 사항은 macOS의 디스크 굽기 제한 사항을 관리합니다. macOS의 Finder 앱에서 디스크 굽기 옵션을 활성화 또는 비활성화하도록 **macOS Finder 설정**을 구성할 수 있습니다.

다음과 같은 옵션을 설정할 수 있습니다.

| **설정** | **설정하기** |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **구성 설정** | |
| **설정 항목** | **수행 작업** |
| 디스크 굽기 허용 | • 설정<br>• 해제<br>• 인증 필요 |

## 구성 배포 중

**절차**

1. 이전 표를 사용하여 옵션을 설정합니다.
2. **다음**을 클릭하세요.
3. **이 구성 활성화** 옵션을 선택합니다.
4. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정

**완료**를 클릭합니다.

# 10.10.4.39. 허용된 미디어 제어(더 이상 사용되지 않음)

**라이센스:** Gold

허용 미디어 제어 구성은 로그아웃 시 macOS에 있는 다양한 실제 미디어에 대한 마운팅, 마운팅 해제 및 추출을 관리합니다.

다음과 같은 옵션을 설정할 수 있습니다.

| 설정 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **구성 설정** | |
| **미디어 유형에 대한 마운트 제어**<br>각 미디어 유형에 대한 마운트 제어를 켜고 마운트 설정을 지정합니다. 마운트 제어를 끄면, OS 기본 설정이 적용됩니다. | |
| **미디어 유형** | **마운트 설정** |
| • CD<br>• DVD<br>• BD | • 읽기 전용(인증 포함)<br>• 마운트 거부<br>• 미디어 꺼내기 |
| • 빈 CD<br>• 빈 DVD<br>• 빈 BD<br>• DVD-RAM<br>• 디스크 이미지<br>• 내장 하드 디스크<br>• 외장 하드 디스크<br>• 네트워크 디스크 | • 읽기 전용<br>• 마운트 거부<br>• 미디어 꺼내기<br>• 인증 |
| • 외장 하드 디스크에는 USB HDD, USB 플래시 드라이브 스토리지 및 SD 카드가 있습니다.<br>• CD, DVD 및 BD와 같은 읽기 전용 미디어는 기본적으로 읽기 전용으로 마운트됩니다. | |
| **미디어 유형에 대한 언마운트 제어**<br>각 미디어 유형에 대한 언마운트 제어를 켜고 언마운트 설정을 지정합니다. 언마운트 제어를 끄면, OS 기본 설정이 적용됩니다. 미디어 유형에 대한 언마운트 거부는 주의해서 설정하십시오. | |
| **미디어 유형** | **마운트 설정** |
| • CD<br>• DVD<br>• BD<br>• 빈 CD<br>• 빈 DVD<br>• 빈 BD<br>• DVD-RAM | • 마운트 해제 거부<br>• 인증 |

| 설정 | 설정하기 |
| --- | --- |
| • 디스크 이미지<br>• 내장 하드 디스크<br>• 외장 하드 디스크<br>• 네트워크 디스크 | |
| **로그아웃 시 꺼내기 설정** | |
| 사용자가 로그아웃할 때 자동으로 꺼내기가 수행되는 미디어 유형입니다. | |
| **미디어 유형** | |
| • CD<br>• DVD<br>• BD<br>• 빈 CD<br>• 빈 DVD<br>• 빈 BD<br>• DVD-RAM<br>• 디스크 이미지<br>• 외장 하드 디스크<br>• 네트워크 디스크 | |

## 구성 배포 중

**절차**

1. 이전 표를 사용하여 옵션을 설정합니다.
2. **다음**을 클릭하세요.
3. **이 구성 활성화** 옵션을 선택합니다.
4. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정

**완료**를 클릭하세요.

# 10.10.4.40. macOS 파인더 설정

**라이센스:** Gold

macOS Finder 설정은 macOS의 Finder 앱 설정을 관리합니다.

다음과 같은 옵션을 설정할 수 있습니다.

| **설정** | **설정하기** |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **구성 설정** | |
| **설정 항목** | **수행 작업** |
| 파인더에서 디스크 굽기 지원 비활성화 | • 켜기<br>• 끄기 |

## 구성 배포 중

**절차**

1. 이전 표를 사용하여 옵션을 설정합니다.
2. **다음**을 클릭하세요.
3. **이 구성 활성화** 옵션을 선택합니다.
4. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정

**완료**를 클릭합니다.

# 10.10.4.41. macOS 커널 확장 정책

**적용 대상:** macOS 10.13.2 또는 지원되는 최신 버전.

사용자 승인 커널 확장 로드를 위한 제한 및 설정 제어

## macOS 커널 확장 정책 구성 생성하기

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **커널**을 입력한 다음, **macOS 커널 확장 정책** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. **사용자 오버라이드 허용** 옵션을 선택하여 사용자가 다음 구성에 의해 명시적으로 허용되지 않는 추가 커널 확장을 승인할 수 있도록 허용합니다.
6. 허용되는 팀 식별자 및 커널 확장 섹션에서 **+ 추가**를 클릭하여 허용되는 팀 식별자 및 커널 확장을 추가합니다. 커널 확장은 패키지의 번들 식별자입니다. 각 팀 식별자의 경우, 팝업 창에 여러 개의 유효 서명된 커널 확장 이름을 추가할 수 있습니다.
7. **추가**를 클릭합니다.
8. **다음**을 클릭해 배포 설정을 구성합니다.
9. **완료**를 클릭합니다.

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.4.42. macOS용 Mobile@Work

이 섹션에는 다음 주제가 포함됩니다.

- macOS용 Mobile@Work 구성 및 스크립트 실행 워크플로우
- macOS용 Mobile@Work 구성 생성
- macOS 기기에 대한 사용자 온보딩 활성화
- macOS용 Mobile@Work 스크립트 구성 생성
- macOS용 Mobile@Work의 깨끗한 설치 해제 수행
- macOS Mobile@Work를 통해 스크립트 적용

MDM용 Ivanti Neurons 를 통해 자신만의 macOS 쉘 스크립트를 생성할 수 있으며 그런 다음, 이를 MDM용 Ivanti Neurons에 업로드하여 관리되는 macOS 기기에서 실행할 수 있습니다. 스크립트 리포지토리 생성, 업로드 및 관리에 대한 자세한 내용은 모든 스크립트를 참조하십시오.

macOS 기기 사용자는 macOS용 Mobile@Work 1.1 이상을 사용하여 기기 폐기를 시작할 수 있습니다. 폐기 옵션은 Mobile@Work 정보 화면에서 **설치 해제**를 클릭하면 사용할 수 있습니다. MDM용 Ivanti Neurons에서는 **기기** 페이지와 기기 상세 정보 페이지를 통해 기기의 상태를 확인할 수 있습니다.

macOS용 Mobile@Work 1.5 이상인 경우에는 MDM 등록이 완료될 때까지 기다릴 필요 없이 등록 직후 Apps@Work가 열립니다.

macOS용 Mobile@Work에서 애플리케이션 타일을 클릭하면 해당 애플리케이션의 앱 상세 정보 페이지가 표시됩니다. 이 페이지에는 앱 설명, 스크린샷, 등급 및 평가가 포함됩니다.

macOS용 Mobile@Work는 Packager 인하우스 macOS 앱이 설치되었는지를 인벤토리 보고서에서 MDM용 Ivanti Neurons 서버에 알립니다.

**필수 조건**

앱 카탈로그에서 macOS용 Mobile@Work 클라이언트를 비즈니스 앱으로 사용할 수 있습니다. macOS 기기에서 셸 스크립트를 실행하기 전에 사용자에게 macOS용 Mobile@Work를 사용하여 MDM용 Ivanti Neurons에서 기기를 등록하도록 지시합니다.

**절차**

1. macOS 애플리케이션에 대한 Mobile@Work를 다운로드합니다. https://support.mobileiron.com/support/CDL.html에서 PKG 파일로 사용할 수 있습니다. 다운로드 사이트의 자격 증명을 얻는 방법에 대한 정보는 이 Ivanti 고객 포럼 기술 자료를 참조하십시오.
2. macOS용 Mobile@Work에 대한 PKG 파일을 보안 서버로 업로드하십시오. 이 서버는 기기 사용자가 액세스할 수 있어야 합니다.
3. macOS용 Mobile@Work에 대한 설치 파일 URL을 이메일 또는 메시지를 통해 기기 사용자와 공유하십시오.
4. 사용자에게 다음을 지시하십시오.
    1. 다른 기기에 macOS용 Mobile@Work를 다운로드하여 설치하십시오.
    2. macOS용 Mobile@Work를 사용하여 MDM용 Ivanti Neurons에서 기기를 등록합니다.

## macOS용 Mobile@Work 구성 및 스크립트 실행 워크플로우

**절차**

1. macOS용 Mobile@Work 구성을 설정하고 배포합니다.
2. macOS용 Mobile@Work 스크립트 구성을 설치하고 배포하여 다음으로 스크립트를 업로드합니다MDM용 Ivanti Neurons. 스크립트는 테넌트에 대해 고유한 서명 인증서를 사용하여 암호화, 서명되었습니다. 스크립트 암호화 해제를 위한 키는 암호화, 서명된 스크립트에 대한 다운로드 URL과 함께 기기로 전송됩니다.

3. MDM용 Ivanti Neurons 는 macOS용 Mobile@Work를 사용하여 macOS 기기의 스크립트를 실행합니다. macOS용 Mobile@Work는 MDM용 Ivanti Neurons에 정기적으로 폴링하여 실행 대기 중인 스크립트가 있는지 확인합니다. 대기열에 스크립트가 있을 경우, Mobile@Work는 MDM용 Ivanti Neurons에서 정의하는 설정에 따라 macOS 기기의 스크립트를 다운로드, 실행합니다.
4. macOS용 Mobile@Work는 스크립트 실행 결과를 MDM용 Ivanti Neurons에 반환하며, 이는 기기 로그에 표시됩니다. **로그** 탭의 macOS의 기기 상세 정보 페이지에서 기기 로그를 확인할 수 있습니다.

## macOS용 Mobile@Work 구성 생성

macOS용 Mobile@Work 구성을 위한 기본 시스템 구성을 사용할 수 있습니다. 그러나 기본적으로는 어떠한 기기에도 배포되지 않습니다.

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **work**를 입력한 다음, **macOS용 Mobile@Work** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. **최대 실행 시간**을 초 단위로 입력하여 스크립트가 실행될 수 있는 시간을 지정합니다. 기본값은 60초입니다.
6. **최대 응답 크기**를 킬로바이트(KB) 단위로 입력하여 MDM용 Ivanti Neurons로 반환되는 스크립트 출력의 최대 응답 크기 제한을 지정합니다. 이는 스크립트 실행 시 반환되는 stdout 또는 stderr 데이터입니다. 기본값은 1KB입니다.
7. **체크인 빈도**를 분 단위로 입력하여 macOS용 Mobile@Work 앱이 MDM용 Ivanti Neurons(으)로 체크인해야 하는 빈도를 지정합니다. 기본값은 15분으로 설정되어 있습니다.
8. (선택 사항) macOS 기기에 대한 사용자 온보딩 활성화 섹션을 사용하여 macOS 기기에 대한 사용자 온보딩을 활성화할 수 있습니다.
9. **다음**을 클릭해 배포 설정을 구성합니다.
    1. 배포 수준 선택:
    2. **전체 사용자 대상** - 모든 사용자의 호환 기기에 앱이 추가됩니다.
    3. **배포하지 않음** - 앱을 추후에 배포하도록 준비합니다.
    4. **사용자 지정 배포** - 다음 옵션 중에서 선택합니다.
        - **사용자/사용자 그룹** - 선택한 사용자 또는 사용자 그룹에게만 앱이 배포됩니다.
          사용자를 선택하려면 **사용자** 탭을 클릭합니다.
          사용자 그룹을 선택하려면 **사용자 그룹** 탭을 클릭합니다.
        - **기기/기기 그룹** - 선택한 기기 또는 기기 그룹에게만 앱이 배포됩니다.
          기기를 선택하려면 **기기** 탭을 클릭합니다.
          기기 그룹을 선택하려면 **기기 그룹** 탭을 클릭합니다.
10. **완료**를 클릭합니다.

## macOS 기기에 대한 사용자 온보딩 활성화

다음과 같이 자동화된 기기 등록 프로세스 중에 macOS 기기에 대한 사용자 온보딩을 활성화할 수 있습니다.

- 기기 등록이 완료되자마자 macOS용 Mobile@Work(버전 1.68 이상 필요)가 프로필, 구성 및 앱과 함께 기기로 푸시됩니다.
- macOS용 Mobile@Work 클라이언트 및 기타 앱은 다음과 같은 경우에만 기기에 푸시됩니다.
    - 앱은 인하우스 PKG 앱 또는 Apple Apps 및 Books 공개 앱입니다.
    - 앱의 자동 설치 설정은 true로 설정되어 있습니다. 설정은 **앱** > 앱 상세 정보 > **앱 구성** > **기기에 설치** 페이지에서 사용할 수 있습니다.

    - 앱의 우선 순위가 높음으로 설정되어 있습니다. 기본적으로 macOS용 Mobile@Work 클라이언트 앱의 우선순위는 높음으로 설정되어 있으며(수정 불가), **이 설정이 없으면 사용자 온보딩 프로세스가 실패할 수 있습니다**.
    - 앱은 기기, 사용자 그룹 또는 기기 그룹에 배포되도록 구성되어 있습니다.
- macOS용 Mobile@Work가 설치되어 등록된 후 남아 있는 프로필, 구성 및 앱이 구성 및 설치될 때까지 macOS 기기가 키오스크 모드로 들어갑니다(사용자가 기기를 제어할 수 없음). 진행 상태가 단계적으로 표시됩니다.

MDM용 Ivanti Neurons에서 지원되는 macOS 1.73 이상 버전용 Mobile@Work의 경우 다음과 같은 추가 기능이 지원됩니다.

- 사용자 온보딩 프로세스는 기기에 대한 기기 등록이 완료되는 직후에 완료됩니다. 사용자 온보딩 프로세스는 사용자 온보딩을 트리거할 시간 창이 만료된 후(일반적으로 기기 등록 후 20분)에는 관리자가 Mobile@Work 구성에서 사용자 온보딩을 활성화하더라도 시작하지 않습니다. 이는 기기가 일반 사용 중일 때 기기가 사용자 온보딩 키오스크 모드로 들어가지 않도록 해줍니다.
- 사용자 온보딩 프로세스는 macOS용 Mobile@Work 클라이언트에 단계적으로 표시됩니다. 구성은 첫 번째 단계의 일부로 설치됩니다.
- 우선순위가 높은 앱이 처음에 설치됩니다. 우선순위가 높은 각 앱은 한 단계로 카운트됩니다. Packager 앱은 진행 단계의 일부로 카운트되지 않습니다.
- 나머지 앱은 사용자 온보딩이 완료된 후에도 백그라운드에서 계속 설치됩니다. 기기에서 설치가 시작된 후 또는 기기에서 애플리케이션이 실제 설치된 후에는 애플리케이션이 설치됨으로 표시됩니다.
- 사용자 온보딩 후에는 기기 상세 정보 페이지로 가서 각 기기에 푸시된 구성과 앱을 검증할 수 있습니다. 추가 정보는 로그에서 확인할 수 있습니다.

**절차**

1. macOS용 Mobile@Work 구성 생성을 사용하여 macOS용 Mobile@Work 구성을 생성합니다.
2. **사용자 온보딩 활성화** 옵션을 선택합니다.
3. 다음 상세 정보를 입력합니다.
    - **사용자 온보딩 시간 제한 값** - 처음 기기를 설정하는 동안 기기가 앱 및 구성을 설치하는 데 걸리는 대략적인 시간을 입력합니다. 기본적으로 macOS 기기의 사용자 온보딩 프로세스는 120초 이내에 시간 제한이 종료되며, 이는 필요에 따라 변경할 수 있습니다.
    - **사용자 랜딩 페이지 URL** - 온보딩이 완료된 후 사용자에게 표시된 랜딩 페이지 URL을 제공합니다.
4. **다음**을 클릭해 배포 설정을 구성합니다.
5. **완료**를 클릭합니다.

## macOS용 Mobile@Work 스크립트 구성 생성

macOS용 Mobile@Work 스크립트 구성을 기기에 여러 개 생성하고 배포할 수 있습니다. 이 구성을 사용하면 저장소(**관리 > 스크립트 및 파일 > 모든 스크립트**)에서 스크립트를 선택하여 Mobile@Work for macOS로 배포할 수 있습니다.

macOS용 Mobile@Work 1.66 이상 버전을 사용하여 기기에 스크립트 실행을 예약할 수 있습니다. 버전이 1.66 미만인 macOS용 Mobile@Work 클라이언트로 기기에 스크립트 실행을 예약할 경우 스크립트가 한 번만 실행됩니다. macOS용 Mobile@Work 클라이언트를 1.4에서 1.66으로 업그레이드하면 macOS 클라이언트의 모든 구성이 기기에 다시 배포됩니다.

**필수 조건**

- **관리 > 스크립트 및 파일 > 모든 스크립트**로 이동하여 해당 구성에 사용하고 기기에 배포할 수 있는 스크립트를 업로드 및 관리합니다.
- 기기에 macOS용 Mobile@Work 구성을 구성하고 배포합니다. 그러지 않으면 macOS용 Mobile@Work 스크립트 구성이 오류 상태가 됩니다.

**절차**

1. **구성**을 선택합니다.

2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **work**를 입력한 다음, **macOS용 Mobile@Work 스크립트** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. **스크립트 선택** 필드에서 찾으려는 스크립트 이름을 입력하고 드롭다운 목록에서 스크립트를 선택합니다.
6. 스크립트 입력 섹션에 스크립트와 관련된 스크립트 입력 레이블과 스크립트 변수가 표시됩니다. 이를 재정의해야 할 경우 대체 스크립트 변수(예: {$userWorkEmailAddress})와 그 대체 기본 값(예: john.doe@company.com)을 입력하십시오.
7. 스크립트 실행 섹션에서 다음 예약 옵션 중 하나를 선택합니다.
   - 배포 시 한 번 실행
   - 반복 실행
8. 반복 실행을 선택할 경우 다음 세부 정보를 지정합니다.
   - 사용할 시간대 - 기기의 현지 시간 또는 UTC 시간을 선택합니다. 이 필드에 선택한 시간에 스크립트가 실행됩니다.
   - 실행 시작일 - 시작 날짜를 선택합니다.
   - 실행 종료일 - 종료 날짜를 선택합니다(시작 날짜보다 크거나 같음).
   - 스크립트 실행 - 매일 또는 매주를 선택하고 해당하는 시간(24시간 형식), 분 및 일수를 선택합니다.
9. **다음**을 클릭해 배포 설정을 구성합니다.
10. **완료**를 클릭합니다.

## macOS용 Mobile@Work의 깨끗한 설치 해제 수행

macOS용 Mobile@Work 설치 중 **미등록 앱 제거(관리형 앱에만 적용됨)** 옵션을 활성화하고 MDM용 Ivanti Neurons 관리자 포털에서 폐기될 기기를 시작하는 경우, macOS용 Mobile@Work 애플리케이션 및 설치 해제 스크립트가 기기에서 삭제됩니다. 프로세스 및 스크립트가 백엔드에서 실행되지 않도록 하려면, 신규 사용자의 기기 등록이나 기존 사용자의 폐기 중에 설치 해제 스크립트가 실행되어 백엔드에서 관련 프로세스와 스크립트를 삭제하도록 MDM용 Ivanti Neurons 관리자 포털에서 다음 옵션을 선택 해제합니다.

**절차**

1. MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **앱** > **Mobile@Work** > **앱 구성** > **앱 구성 요약 목록** > **Apple 앱 설정** > **Apple 애플리케이션 관리 구성 설정**으로 이동합니다.
3. **구성 설정** 페이지에서 다음 옵션의 선택을 해제합니다.
   - **미등록 앱 제거(관리되는 앱에만 적용)**

## macOS Mobile@Work를 통해 스크립트 적용

**macOS Mobile@Work를 통해 스크립트 적용**은 관리자가 관리형 macOS 기기에 셸 스크립트를 원격으로 배포하고 실행할 수 있도록 합니다. 이를 통해 작업 자동화, 문제 해결 적용, 정책 시행, 구성 간소화를 사용자 개입 없이 수행할 수 있어 기기 관리를 규모에 따라 일관되고 효율적으로 유지할 수 있습니다.

**전제 조건**:

- 기기는 macOS를 실행 중이어야 합니다.
- macOS용 Mobile@Work가 기기에 이미 설치되어 있어야 합니다.
- macOS용 Mobile@Work 구성이 올바르게 생성, 배포 및 할당되었는지 확인하십시오. 자세한 내용은 **macOS용 Mobile@Work 구성 생성**을 참조하십시오.

기기에 Mobile@Work 클라이언트가 설치 및 구성되어 있지 않거나, 기기 플랫폼이 스크립트 실행을 지원하지 않는 경우 macOS Mobile@Work를 통한 스크립트를 적용할 수 없습니다. macOS 클라이언트가 활성 상태인지 확인하고, 지원되는 macOS 기기만 선택하십시오.

**절차**

1. MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **기기**로 이동하여 스크립트를 실행하려는 macOS 기기 목록을 선택합니다.
3. **기기** 페이지에서 **작업** > **macOS** > **macOS Mobile@Work를 통해 스크립트 적용**으로 이동합니다.
   **macOS Mobile@Work를 통해 스크립트 적용** 창이 나타납니다.
4. 스크립트를 적용하려면 **스크립트 선택** 필드에 스크립트 이름을 입력하고 선택합니다.
   스크립트 생성에 대한 자세한 내용은 모든 스크립트를 참조하십시오.
5. **확인**을 선택하여 기기에서 스크립트를 실행합니다.

**관련 주제:**

- 관리 > 스크립트 및 파일 > 모든 스크립트
- 구성을 생성하는 방법

# 10.10.4.43. macOS 소프트웨어 업데이트 규칙 구성

관리자는 **macOS 소프트웨어 업데이트 규칙**을 정의하여 기기의 소프트웨어 업데이트 정책을 구성할 수 있습니다.

**적용 대상**: macOS 10.7~26.0.

1. 구성 > +추가로 이동합니다.
2. 검색 필드에 macOS를 입력한 다음, macOS 소프트웨어 업데이트 설정 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. **macOS 소프트웨어 업데이트 규칙**에서 필요한 구성을 선택합니다.
5. 다음을 클릭하세요.
6. 이 구성 활성화 옵션을 선택합니다.
7. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
8. 완료를 클릭하세요.

## macOS 소프트웨어 업데이트 규칙

관리자는 다음과 같이 규칙 목록에서 선택할 수 있습니다.

> 사용자는 기기에서 이러한 규칙이 적용될 때는 이 설정을 변경할 수 없습니다.

- 릴리스 전 소프트웨어 설치 허용.
- 자동:
    - 업데이트 확인
    - 이용 가능 시 새로운 업데이트 다운로드
    - macOS 업데이트 설치
    - App Store에서 앱 업데이트 설치
    - 시스템 데이터 파일 및 보안 업데이트를 설치합니다.
- 앱 설치를 관리 사용자로 제한합니다.
- 소프트웨어 업데이트 카탈로그의 URL을 추가하기 위한 옵션(macOS 11+에서는 지원되지 않음).

# 10.10.4.44. 인증서 환경설정

**적용 대상**:

- Ivanti Neurons for MDM는 macOS 10.12 이상 최신 버전까지 지원합니다.

동일 프로필에 포함된 인증서 페이로드를 참조하는 사용자의 키체인에서 인증서 환경설정 항목을 확인합니다.

이 구성은 이메일 주소 또는 URL에 인증서를 바인딩하기 위해 사용합니다. 인증서를 이메일 주소에 바인딩하고 나면 메일 앱에서 해당하는 이메일 계정에 대해 구성한 환경을 사용합니다. 웹 사이트용 SSL 인증서를 신뢰할 수 없는 경우 인증서 환경설정을 추가하여 웹사이트에 액세스하고자 할 때 브라우저에 경고 메시지가 나타나지 않도록 합니다.

> 관리자는 반드시 인증서를 보유해야 합니다. 인증서를 추가하고 배포하는 방법에 대한 자세한 내용은 인증서 구성을 참조하십시오.

## 인증 환경설정 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **환경설정**을 입력한 다음, **인증서 환경설정** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. 구성 설정 섹션의 **이름** 필드에 기본 설정 인증서가 필요한 이메일 ID 또는 이름을 입력합니다.
6. **인증서 UUID** 필드에서 인증서를 선택합니다.
7. **다음**을 클릭해 배포 설정을 구성합니다.
8. **완료**를 클릭합니다.

**관련 주제:**

- ID 환경설정
- 인증서 구성
- 구성을 생성하는 방법

# 10.10.4.45. 활성 디렉토리(macOS)

**적용 대상:** macOS 10.9 또는 지원되는 최신 버전.

인증 및 보안을 위해 활성 디렉토리(AD)를 사용하는 소프트웨어 서비스에 액세스하려면 macOS 기기를 AD 도메인에 바인딩하도록 고급 옵션을 구성합니다.

이 섹션에는 다음 주제가 포함됩니다.


- Active Directory 구성 생성
- Active Directory 설정


## Active Directory 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **개인정보 보호**를 입력한 다음, **활성 디렉토리** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. 다음 활성 디렉토리 설정 표의 설명대로 설정을 입력합니다.
6. **다음**을 클릭해 배포 설정을 구성합니다.
7. **완료**를 클릭하세요.

## Active Directory 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| 활성 디렉토리 설정 - 기본 | |
| 호스트 이름 | (필수) 가입할 활성 디렉토리 도메인인 호스트 이름을 입력합니다. |
| 사용자 이름 | 도메인 가입에 사용되는 계정의 사용자 이름을 입력합니다. |
| 비밀번호 | 도메인 가입에 사용되는 계정의 비밀번호를 입력합니다. |
| AD 조직 단위 | 가입 컴퓨터 개체가 추가되는 조직 단위(OU)를 입력합니다. |
| AD 마운트 스타일 | 사용할 네트워크 홈 프로토콜을 표시할 다음 옵션 중 하나를 선택합니다.<br>• AFP<br>• SMB |
| 활성 디렉토리 설정 - 고급 | |
| ADCreateMobileAccountAtLogin 키 활성화 | ADCreateMobileAccountAtLogin 키를 활성화 또는 비활성화합니다.<br>추가 옵션: 로그인 시 모바일 계정을 생성합니다. |
| ADWarnUserBeforeCreatingMA 키 활성화 | ADWarnUserBeforeCreatingMA 키를 활성화 또는 비활성화합니다.<br>추가 옵션: 모바일 계정을 생성하기 전 사용자에게 경고합니다. |
| ADForceHomeLocal 키 활성화 | ADForceHomeLocal 키를 활성화 또는 비활성화합니다.<br>추가 옵션: 강제 로컬 홈 디렉토리 |
| ADUseWindowsUNCPath 키 활성화 | ADUseWindowsUNCPath 키를 활성화 또는 비활성화합니다.<br>추가 옵션: 네트워크 홈 위치를 파생할 AD에서 UNC 경로를 사용합니다. |
| ADAllowMultiDomainAuth 키 활성화 | ADAllowMultiDomainAuth 키를 활성화 또는 비활성화합니다.<br>추가 옵션: 포리스트의 어느 도메인에서든 인증을 허용합니다. |
| 기본 사용자 쉘 | /bin/bash와 같은 기본 사용자 쉘을 입력합니다. |
| 사용자 UID를 속성으로 매핑 | 사용자 UID를 지정된 속성으로 매핑하도록 설정합니다. |
| 사용자 GID를 속성으로 매핑 | 사용자 GID를 지정된 속성으로 매핑하도록 설정합니다. |
| 그룹 GID를 속성으로 매핑 | 그룹 GID를 지정된 속성으로 매핑하도록 설정합니다. |
| 선호하는 도메인 서버 | 이 도메인 서버를 선호합니다. |
| 명칭 공간 규칙 | 다음 사용자 명명 규칙 중 하나를 선택합니다.<br>• 도메인(기본)<br>• 포리스트 |
| 패킷 서명 | 다음 패킷 서명 옵션 중 하나를 선택합니다.<br>• 허용(기본)<br>• 비활성화<br>• 필수 |

| 설정 항목 | 수행 작업 |
| --- | --- |
| 패킷 암호화 | 다음 패킷 암호화 옵션 중 하나를 선택합니다.<br>• 허용(기본)<br>• 비활성화<br>• 필수<br>• SSL |
| 지정된 활성 디렉토리 그룹에 의한 관리 허용 | 지정된 활성 디렉토리 그룹에 의한 관리를 허용하도록 설정합니다.<br>하나 이상의 그룹을 추가하려면 **추가**를 클릭합니다. |
| 동적 DNS 제한 | 동적 DNS 업데이트를 지정된 인터페이스(예: en0, en1 등)로 제한하도록 설정합니다.<br>하나 이상의 인터페이스 이름을 추가하려면 **추가**를 클릭합니다. |
| 비밀번호 변경 주기 | 컴퓨터 신뢰 계정 비밀번호의 변경 주기(일)를 지정합니다. 0 값은 비활성화되어 있습니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.46. ID 환경설정

**적용 대상:** macOS 10.12 또는 지원되는 최신 버전.

동일 프로필에 포함된 ID 페이로드를 참조하는 사용자의 키체인에서 ID 환경설정 항목을 확인합니다.

macOS 기기에서 ID 환경설정을 통해 웹사이트와 함께 사용하고자 하는 ID(키 값 쌍)를 선택할 수 있습니다. ID 환경설정(URL 및 ID로 구성)을 기기에 적용하면 **키체인 액세스 > 모든 항목**에 환경설정이 나타납니다("종류"는 "ID 환경설정"). 다음에 Safari에서 해당 URL에 연결할 때 기기가 구성된 인증서를 제시합니다.

MDM용 Ivanti Neurons 에서 사용할 AppStore URL 및 인증서에 대한 페이로드를 통해 기본 시스템의 ID 환경설정을 구성합니다.

macOS 10.12 이상에서 Safari를 사용해 macOS App Catalog에 액세스하면 사용자에게 ID 인증서를 캐시하라는 시스템 비밀번호 메시지가 표시됩니다. 사용자가 macOS App Catalog에 처음으로 액세스할 때 '항상 허용'을 선택해야 다음부터 메시지가 표시되지 않습니다.

macOS 버전 10.12 미만인 Safari와 다른 브라우저에서는 macOS 기기에서 새 브라우저 세션에 macOS App Catalog에 액세스할 때 인증서 및 시스템 비밀번호 메시지가 표시됩니다.

## ID 환경설정 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **환경설정**을 입력한 다음, **ID 환경설정** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. 구성 설정 섹션의 **이름** 필드에 서비스를 고유하게 식별하는 이메일 ID, DNS 호스트 이름 또는 이름을 입력합니다.
6. **인증서 UUID** 필드에서 인증서를 선택합니다.
7. **다음**을 클릭해 배포 설정을 구성합니다.
8. **완료**를 클릭합니다.

**관련 주제:**

- 인증서 환경설정
- 구성을 생성하는 방법

# 10.10.4.47. Office 365 자동 계정 생성(macOS)

**적용 가능 운영 체제:**

- 지원되는 macOS 기기.
- 권장 Microsoft Office 365 앱 버전 16.13.x 이상

사용자 정보 및 옵션을 구성하여 모든 Microsoft Office 365 애플리케이션에 대한 최초 구성을 설정합니다.

이 섹션에는 다음 주제가 포함됩니다.


- Office 365 자동 계정 생성 구성 생성
- Office 365 자동 계정 생성 설정


## Office 365 자동 계정 생성 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **office**를 입력한 다음, **Office 365 자동 계정 생성** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. 다음 Office 365 자동 계정 생성 설정 표의 설명대로 설정을 입력합니다.
6. **다음**을 클릭해 배포 설정을 구성합니다.
7. **완료**를 클릭하세요.

## Office 365 자동 계정 생성 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| Office 활성화 이메일 주소 | 사용자 이메일 주소를 입력합니다. |
| Office 자동 로그인 | 최초 실행 창을 건너뛰도록 설정합니다. O365 인증과 같은 필수 정보에 대해서만 사용자에게 메시지를 표시합니다. |
| 로컬 열기/저장을 기본값으로 설정 | '온라인 위치' 대신 '내 Mac에서' 패널을 강제로 열도록/저장하도록 설정합니다. |
| 실행 시 새로운 기능 표시 | 실행 시 새로운 기능 정보를 표시하도록 설정합니다. |
| 비주얼 베이직 매크로 실행 상태 | 다음 옵션 중 하나를 선택합니다.<br>• 경고로 비활성화됨<br>• 경고 없이 비활성화됨<br>• 경고 없이 활성화됨 |
| 비주얼 베이직 외부 Dylib 비활성화 | 비주얼 베이직 외부 종속성을 비활성화하도록 설정합니다. |
| 시스템을 바인딩할 비주얼 베이직 허용 | 매크로가 DECLARE를 사용하여 시스템() OS API로 바인딩할 수 있도록 설정합니다. 이 API를 통해 매크로가 임의의 외부 프로세스를 실행하고 이를 명령 줄의 임의 데이터로 넘겨줄 수 있습니다. |
| Popen으로 바인딩할 비주얼 베이직 비활성화 | 매크로가 DECLARE를 사용하여 popen() OS API로 바인딩할 수 있도록 설정합니다. 이 API를 통해 매크로가 임의의 외부 프로세스를 실행하고 이를 명령 줄의 임의 데이터로 넘겨줄 수 있습니다. |
| 비주얼 베이직 Mac 스크립트 비활성 | 매크로가 Apple 스크립트 비주얼 베이직 API를 호출할 수 있도록 설정합니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.49. Apple 앱 카탈로그

**해당 대상:** iOS 및 macOS

Apple 앱 카탈로그 구성은 웹 클립을 통해 Apple 앱 카탈로그에 대한 접근권한을 관리합니다. MDM용 Ivanti Neurons 릴리스 83부터 Go 애플리케이션에서 Apps@Work 기본 환경으로 전환할 수 있습니다. 새로 생성된 테넌트의 경우 iReg 또는 클라이언트를 통해 설치된 iOS 기기에 대해 Apps@Work Webclip 구성이 기본적으로 배포되지 않습니다. 관리자는 iReg 또는 클라이언트를 통해 등록된 기기에 webclip 구성을 수동으로 배포해야 합니다.

> Apps@Work webclip 검색 결과는 검색 요청에 10개 이상의 행 매개변수가 있는 경우에도 iOS 및 iPad 기기에서 10개의 애플리케이션만 표시합니다.

**절차**

관리자는 이 시스템 정의 구성 배포를 다음과 같이 편집할 수 있습니다.

1. **구성**으로 이동합니다.
2. **Apple App Catalog**를 클릭합니다.
3. **배포 편집**을 클릭합니다.
4. 다음 배포 옵션 중 하나를 선택합니다.
    - 전체 기기 - 호환되는 모든 기기가 이러한 구성을 전송하게 됩니다.
    - 배포 안함 - Apple 앱 카탈로그에 대한 접근권한을 비활성화하거나 나중에 이 구성을 배포하도록 준비합니다. 이 구성을 이후에 배포할 수 있도록 준비
    - 맞춤 설정 - 이 구성을 전송할 특정 기기 그룹을 정의합니다.

**저장**을 클릭하세요.

# 10.10.4.50. 관리되는 도메인

**라이센스**: Silver

관리형 도메인 구성을 사용하면 iOS 8 이상 및 visionOS 1.1 이상 기기의 Mail 및 Safari에 대해 신뢰할 수 있는 도메인을 지정할 수 있습니다. 일단 구성이 기기에 적용되고 나면 구성에 지정되지 않은 도메인이 기기의 Mail 및 Safari에 신뢰할 수 없음으로 강조 표시됩니다. 이 구성을 **제한 구성**과 결합하여 사용하면 Safari에서 허용하는 데이터 다운로드를 제어할 수 있습니다.

## 관리되는 도메인 설정

| 설정 | 설정하기 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 관리되는 이메일 도메인 | **+추가**를 클릭하여 도메인을 입력합니다(예: mycompany.com). |
| 관리되는 웹 도메인 | **+추가**를 클릭하여 도메인을 입력합니다(예: mycompany.com). |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.51. 암호 구성

MDM용 Ivanti Neurons에서(시작 마법사를 사용하여) 먼저 설정하는 것 중 하나는 암호 구성입니다. 암호 설정을 통해 장치의 화면 잠금 기능을 설정할 수 있습니다.

## 암호 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 단일 값 허용 | 문자 또는 숫자를 순서대로 포함하는 PIN 또는 비밀번호를 제한합니다.<br><br>**iOS, macOS, watchOS, Android의 경우:** 반복, 오름차순 또는 내림차순 문자 시퀀스가 포함되어 보안 수준이 낮은 핀 또는 암호를 허용하도록 선택합니다.<br>예: 1111, 1234, abcd.<br><br>Android 기기의 경우 이 옵션을 선택 해제하면 복잡한 PIN으로 암호를 시행합니다. 예를 들어 사용자는 오름차순 또는 내림차순이나 반복되는 문자를 구성할 수 없습니다.<br>**Windows 10 이상의 경우** : 반복 또는 오름차순 숫자 시퀀스가 포함되어 보안 수준이 낮은 암호를 허용하도록 선택합니다.<br>예: 1111, 1234 |
| 영숫자 값 필요 | 암호에는 최소 한 개의 문자와 한 개의 숫자를 포함해야 합니다.<br><br>**iOS 및 Android의 경우**: 암호에 글자와 숫자가 포함되도록 하려면 선택합니다.<br>**Windows 10 이상의 경우** : Microsoft 표준을 기반으로 강력한 비밀번호만 허용하도록 선택합니다. |
| 최소 암호 길이 | 최소 암호 길이를 목록에서 선택해 설정할 수 있습니다.<br>**Windows 10 Desktop의 경우:** 로컬 계정은 최소 암호 길이 6자가 적용됩니다. |
| 최소 복잡한 문자 수 | **iOS 및 Android의 경우**: 목록에서 숫자를 선택하여 숫자나 글자가 아닌 문자의 최소 개수를 설정합니다.<br>**Windows 10 이상의 경우** : 로컬 계정은 무조건 3개의 복합 문자를 적용합니다. |
| 최대 암호 사용기간 | 암호 설정 후 암호 재설정을 해야 하는 주기를 입력해 설정할 수 있습니다. 암호 재설정 주기 설정을 원하지 않을 경우 해당 항목을 빈칸으로 남기시기 바랍니다. |
| 자동 잠금 | 장치에 일정 시간 입력이 없을 경우 화면 잠금이 실행되는 주기를 목록에서 선택해 설정할 수 있습니다. |
| 모든 잠금 방법 | **Android 전용**. 사용자가 패턴 잠금 해제 등의 모든 잠금 방식을 선택할 수 있습니다. 위의 암호 설정은 이 기기에 적용되지 않습니다. |
| 암호 이력 | 사용자가 암호를 재사용하기 전에 입력해야 하는 고유 암호 개수를 입력해 설정할 수 있습니다. 예를 들어, 해당 항목을 4로 설정할 경우, 사용자가 첫 번째 암호를 재사용하려면 암호 4개를 먼저 설정해야 합니다. |
| 기기 잠금의 유예 기간 | 잠금화면 실행 후 사용자가 암호를 입력해야 잠금 해제를 할 수 있는 기준 경과시간을 목록에서 선택해 설정할 수 있습니다. |
| 최대 실패 시도 횟수 | 기기가 재설정되고 지워지기 전에 최대 허용되는 연속 암호 입력 횟수를 목록에서 선택해 설정할 수 있습니다.<br>**경고:** 사용자가 비밀번호 최대 시도 횟수를 초과할 경우 기기가 지워집니다. 이 옵션을 사용할 때는 주의해야 합니다. |
| (macOS 전용)<br>암호 정규식 활성화 (macOS 14+) | 암호와 일치하는 표현식 문자열을 지정하여 정책과 일치하는지 확인하세요. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| (macOS 전용)<br>언어<br><br>(macOS 전용)<br>설명 | 설명의 언어를 지정합니다.<br><br>암호의 복잡성을 설명하세요. 예를 들어 숫자, 특수 문자, 문자열 등이 있습니다. |
| (macOS 전용)<br>다음 로그인 시 암호 규칙 적용<br><br>(macOS 전용)<br>로그인 실패 후 재설정되기까지 남은 시간(분) | 다음번에 사용자가 로그인할 때 비밀번호 정책을 준수하는 비밀번호를 만들 수 있도록 macOS가 사용자에게 비밀번호 변경을 지시할 수 있게 활성화하도록 설정합니다.<br>이 옵션은 기본적으로 선택되지 않습니다.<br>macOS 10.13 이상 버전에 적용됩니다.<br><br>최대 로그인 시도 실패 횟수에 도달한 후 로그인이 재설정되기까지 남은 시간(분)을 지정합니다.<br>이 필드의 최대 시도 실패 횟수가 활성화되었습니다. macOS 10.10 이상에서 사용할 수 있습니다. |
| SmartLock | **Android 엔터프라이즈 작업 프로필을 제외한 Android 5.0 기기:**<br>**Android 6.0 이상:**<br>사용자가 SmartLock 기능을 선택하여 기기 잠금을 해제하도록 허용 또는 금지할 수 있습니다. SmartLock 기능은 사용자가 기기에 가까이 있거나 기기가 위치에 있거나 기기가 신뢰할 수 있는 기기와 페어링되는 등의 특정 환경에서 기기 잠금을 자동으로 해제합니다. |
| 지문 잠금 해제<br><br>잠금 화면 알림 (Android 엔터프라이즈만 해당) | **Android 엔터프라이즈 작업 프로필을 제외한 Android 5.0 기기:**<br>**Android 6.0 이상:**<br>사용자가 지문 기능을 선택하여 기기 잠금을 해제하도록 허용 또는 금지할 수 있습니다.<br><br>**작업 관리 기기에 대한 알림 활성화(기기 소유자용)**<br>작업 관리 기기의 잠금 화면 알림 허용 또는 허용 금지<br><br>**작업 프로필에 대한 수정하지 않은 알림 활성화**<br>**Android 6.0 이상:**<br>작업 프로필 기기의 잠금 화면 수정되지 않은 알림 허용 또는 허용 금지<br>이 설정을 활성화한 후에는 알림을 수신하지만 콘텐츠는 '정책에 따라 콘텐츠 숨김'으로 표시됩니다. 콘텐츠(메일/푸시 알림)는 앱에서만 볼 수 있습니다. |

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.4.52. 개인정보 보호 환경 설정(macOS)

**적용 대상:** macOS 10.14 또는 지원되는 최신 버전.

시스템 서비스, 시스템 파일 및 시스템 리소스에 대한 액세스를 얻기 위해 어떤 애플리케이션이 허용되는지 구성합니다. 이 구성은 시스템 환경설정 > 보안 및 개인 정보 보호 > 개인 정보 보호에서 macOS 기기에 대한 설정을 제어합니다.

## 개인 정보 보호 환경설정 구성 생성

**Procedure**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **개인 정보 보호**를 입력한 다음, **개인 정보 보호 환경설정** 구성을 클릭합니다.
4. 구성의 이름 및 설명을 입력합니다.
5. 페이지에 열거된 애플리케이션 중 하나를 탐색합니다. 관련 정보는 **Apple 문서**를 참조하십시오.
    1. macOS 10.14+의 경우 구성에 사용할 수 있는 애플리케이션 및 설정은 다음과 같습니다.
        - 접근성 - 접근성 하위 시스템을 통해 앱에 대한 정책을 지정합니다.
        - 주소록 - Contacts.app에서 관리하는 연락처 정보에 대한 정책을 지정합니다.
        - Apple 이벤트 - 제한된 Apple 이벤트를 다른 프로세스에 전송하는 앱에 대한 정책을 지정합니다.
        - 캘린더 - Calendar.app에서 관리하는 캘린더 정보에 대한 정책을 지정합니다.
        - 카메라 - 시스템 카메라. 프로필에서는 카메라에 액세스할 수 없습니다. 거부만 가능합니다.
        - 마이크 - 시스템 마이크. 프로필에서는 마이크에 액세스할 수 없습니다. 거부만 가능합니다.
        - 사진 - ~/Pictures/.photoslibrary에 있는 사진 앱에서 관리하는 사진
        - 게시 이벤트 - CoreGraphics API를 사용하여 시스템 이벤트 스트림에 CGEvents를 전송하는 애플리케이션에 대한 정책을 지정합니다.
        - 미리 알림 - 미리 알림 앱에서 관리하는 미리 알림 정보에 대한 정책을 지정합니다.
        - 시스템 정책(모든 파일) - 시스템 관리 파일을 포함한 모든 보호 파일에 대한 애플리케이션 액세스를 허용합니다.
        - 시스템 정책(관리 파일) - 시스템 관리에 사용되는 일부 파일에 대한 애플리케이션 액세스를 허용합니다.
    2. macOS 10.15+의 경우 구성에 사용할 수 있는 애플리케이션 및 설정은 다음과 같습니다.
        - 파일 사용 - 파일 제공자가 관리하는 파일을 사용자가 사용할 때 파일 제공자 애플리케이션이 이를 알 수 있게 합니다.
        - 모든 프로세스에서 이벤트 수신 - 애플리케이션이 CoreGraphics 및 HID API를 사용하여 모든 프로세스에서 CGEvents 및 HID 이벤트를 수신할 수 있도록 합니다. 프로필에서는 이러한 이벤트에 액세스할 수 없습니다. 거부만 가능합니다. 허용됨 옵션을 선택 취소합니다.
        - 미디어 라이브러리 액세스 - 애플리케이션이 Apple Music, 음악 및 동영상 활동, 미디어 라이브러리에 액세스할 수 있도록 허용합니다.
        - 시스템 디스플레이의 화면 캡처 - 애플리케이션이 시스템 디스플레이의 콘텐츠를 캡처(읽기)할 수 있도록 합니다. 프로필에서는 콘텐츠에 액세스할 수 없습니다. 거부만 가능합니다. 허용됨 옵션을 선택 취소합니다.
        - 음성 데이터 인식 및 Apple로 전송 - 애플리케이션이 시스템 음성 인식 기능을 사용하고 음성 데이터를 Apple로 전송할 수 있도록 합니다.
        - 사용자의 데스크톱 폴더의 파일 액세스 - 애플리케이션이 사용자의 데스크톱 폴더의 파일에 액세스할 수 있도록 합니다.

- 사용자의 도큐멘트 폴더의 파일에 액세스 - 애플리케이션이 사용자의 도큐멘트 폴더의 파일에 액세스할 수 있도록 합니다.
- 사용자의 다운로드 폴더의 파일에 액세스 - 애플리케이션이 사용자의 다운로드 폴더의 파일에 액세스할 수 있도록 합니다.
- 네트워크 볼륨의 파일에 액세스 - 애플리케이션이 네트워크 볼륨의 파일에 액세스할 수 있도록 합니다.
- 제거 가능한 볼륨의 파일에 액세스 - 애플리케이션이 제거 가능한 볼륨의 파일에 액세스할 수 있도록 합니다.

6. 구성하고자 하는 각 애플리케이션에 대해 **작업 > 추가**를 클릭합니다.
7. 다음 ID 사전 키에 대한 값을 입력합니다.
    - 식별자 - 설정 이름 예: "us.zoom.ZoomPresence."
    - 식별자 유형 - 번들 ID 또는 경로 선택. 예: "Bundle ID".
    - 코드 요구 사항 - 번들 ID 또는 경로에 대한 값 지정. 예: "identifier "us.zoom.ZoomPresence" 및 anchor apple generic."
    - 정적 코드(True 또는 False)
    - 허용됨(True 또는 False)
    - 설명
8. **저장**을 클릭하세요.
9. (선택 사항) 어느 애플리케이션에서든 기존 개인 정보 보호 환경설정을 삭제하려면 **작업 > 삭제**를 클릭하십시오.
10. **다음**을 클릭해 배포 설정을 구성합니다.
11. **완료**를 클릭하세요.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.53. 개인정보 보호 설정

개인 정보는 다음과 같이 구성되는지 여부를 정의합니다.

- 위치 데이터는 기기에서 수집되어 기기 관리 시스템으로 전송
- 관리자가 기기를 지울 수 있는지 여부
- 앱 인벤토리를 모든 앱에 대해 수집할 것인지 아니면 앱 카탈로그에 나타나는 앱에 대해서만 수집할 것인지 여부

## 개인정보 보호 설정

> 사용자 등록 기기에서는 기기 지우기 및 기기의 모든 앱용 인벤토리 수집이 적용되지 않습니다.

| 설정 | 설정하기 |
| --- | --- |
| **이름** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **위치 데이터 수집** | 위치 데이터 수집 기능을 선택할 수 있습니다. 기기 페이지에서 기기 위치를 확인합니다.<br>• iOS 기기의 경우 기기에 표시된 위치는 네트워크 위치만을 기반으로 합니다.<br>• A ndroid 기기의 경우 위치는 네트워크 위치와 GPS 위치(해당할 경우) 모두를 기반으로 합니다.<br>• Windows 기기의 경우 위치는 기기 체크인 시 구한 경도와 위도 값을 기반으로 합니다.<br>장치에 위치 데이터 수집 기능이 설정되면, 현재 위치가 4시간 간격으로 업데이트됩니다. 위치 데이터는 해당 장치가 폐기되거나 개인정보 보호 설정이 해제 또는 삭제되는 경우 장치 관리 시스템에서 삭제됩니다.<br>기기 사용자는 기기에서 위치 데이터의 수집을 끌 수 있습니다. |
| **기기 지우기 작업 비활성화** | 관리자가 기기를 지우지 못하게 합니다. 사용자가 소유하고 있는(직원 소유) 기기에 대해 이 옵션을 선택할 것을 고려하십시오. |
| **사용자에게 위치 서비스 활성화 메시지 표시** | 이 옵션을 선택하면 사용자는 선택적으로 장치, Wi-Fi, MTD 찾기를 비롯하여 위치 서비스의 사용을 허용하거나 허용하지 않을 수 있습니다. 완전 관리 장치의 경우 관리자가 이 옵션을 비활성화할 경우 자동으로 권한이 부여될 수 있습니다. |
| **앱 인벤토리 수집** | **앱 인벤토리 수집**을 선택하면 기기에 설치된 모든 앱의 정보를 수집할 수 있습니다. 여기에는 앱 카탈로그에 포함된 앱과 포함되지 않은 앱이 모두 적용됩니다.<br>기기에 설치되어 있고 앱 카탈로그에 포함된 앱의 정보만 수집하려면 **앱 카탈로그에 있는 기기의 모든 앱용**을 선택합니다.<br>기기에 있는 모든 앱에 대한 정보를 수집하려면 **기기의 모든 앱용**을 선택합니다. 이 옵션은 Windows 10+ 기기에 적용됩니다. 다음 앱 소스 유형 인벤토리가 표시되고 기본적으로 선택됩니다.<br>• **비 App Store 인벤토리 활성화** - MDM을 통해 푸시되거나 최종 사용자가 앱을 수동으로 언팩한 후 로컬에서 설치하는 방법으로 기기에 직접 설치한 인하우스 앱(범용 앱)의 경우<br>• **App Store 인벤토리 활성화** - Microsoft Store에서 수동으로 또는 Apps@work 스토어를 통해 설치한 앱의 경우<br>• **시스템 인벤토리 활성화** - Microsoft가 Windows 10 OS와 함께 미리 설치한 것으로 보고한 앱의 경우<br>• **Win32 인벤토리 사용** - MSI, EXE, Win32 스토어 앱 등과 같은 앱처럼 MDM을 통해 설치되거나 최종 사용자가 장치에 직접 설치하는 시스템 32 기반 앱에 사용됩니다.<br>선택한 앱에 대한 정보를 수집하기 위해 그러한 앱 소스 유형 인벤토리만 선택할 수도 있습니다. Non App Store 또는 Win32 앱 인벤토리를 선택하지 않은 경우에도 MDM이 설치된 앱은 앱 인벤토리에 나타납니다.<br>.EXEs 인벤토리는 개인 정보 구성이 기본 구성을 사용하여 AppCatalog에 대해서만 앱 인벤토리를 수집하는 경우에도 수집됩니다. AppCatalog 앱에 대해서만 수집할 때 모든 앱에 대해 인벤토리를 일관되게 수집해야 합니다.<br>앱 카탈로그에서 사용할 수 있는 Modern, MSI, EXE 앱의 인벤토리는 이러한 각 유형에 속한 앱이 하나 이상 배포된 경우에만 가져옵니다. |

| 설정 | 설정하기 |
| --- | --- |
| **Android Enterprise 장치(7.0+) 설정**<br><br>아래 설정을 구성하여 Android Enterprise 장치의 개인 정보 정책을 설정합니다. | |
| **조직 이름** | 기기를 관리하는 조직의 이름을 입력하십시오. |
| **조직 색상** | 사용자 화면 배경에 표시될 조직 색상을 선택하십시오. |
| **짧은 메시지** | 사용자가 관리자에 의해 잠금 처리된 기능을 사용하려 할 경우 표시될 짧은 메시지를 입력합니다. |
| **긴 메시지** | 사용자가 짧은 메시지를 클릭할 때 표시될 긴 메시지를 입력하십시오. 이 메시지는 사용자에게 제한 사항에 대해 자세한 내용을 제공합니다. |
| **Go 앱 화면 숨기기** | 목록에서 참 또는 거짓을 선택합니다.<br>• **참** - 원격 공유 중에는 Ivanti Go 앱 화면이 표시되지 않습니다.<br>• **거짓** - 원격 공유 중에 Ivanti Go 앱 화면이 표시되어 문제 해결에 도움을 주고 문서도 볼 수 있습니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.4.54. 클라이언트 개인정보 보호방침 정보

**적용 대상:** Android, Android Enterprise, iOS 기기 또는 지원되는 최신 버전.

Go 클라이언트에서 사용자에게 개인 정보 보호 방침 정보를 배포하기 위한 구성. 이것은 배포 설정만 구성할 수 있는 시스템 정의 구성입니다.

사용자에게 표시되는 정보에는 다음 구성의 일부로 설정된 상세 정보가 포함됩니다.

- 개인 정보
  - 위치 데이터 수집
  - 앱 인벤토리 수집
  - Android 7.0+:
    - 조직 이름
    - 조직 색상
    - 짧은 메시지
    - 긴 메시지
- 클라이언트 개인정보 보호
  - SLC - 정기적으로 기기의 절전 모드를 해제하는 중요한 위치 변경
  - 최소 위치 기반 절전 모드 해제 간격
  - MixPanel 상태 활성화
- 모바일 기기 관리 - MDM 액세스 권한(사용자 등록 기기에는 적용되지 않음)
  - 기기 잠금 및 암호 제거
  - 기기 삭제
  - 네트워크 정보(전화/SIM 번호, MAC 주소)

# 10.10.4.55. Ivanti Go Client 설정

제품의 문제를 파악하고 높은 서비스 품질을 보장하기 위해 기기, 사용 정보를 포함한 익명의 최종 사용자 데이터 수집을 구성합니다. 이 설정을 통해 지원 연락처 구성 옵션도 사용할 수 있습니다.

## Ivanti Go Client 설정 구성 만들기

**적용 가능 운영 체제:**

- macOS용 Mobile@Work 1.67 또는 지원되는 최신 버전.
- iOS용 Go 3.5.0 또는 지원되는 최신 버전.
- Mobile@Work for Android 12.9.0.0 또는 지원되는 최신 버전.
- Go for Android 124 또는 지원되는 최신 버전.

**절차**

1. **구성** > **구성 추가** > **Ivanti Go Client 설정**으로 이동합니다. 그러면 **Ivanti Go Client 설정 구성 만들기** 페이지가 나타납니다.
2. **이름** 상자에 구성의 이름을 입력합니다.
3. 구성의 **설명**을 입력합니다.
4. 위치 기반 절전 모드에서 SLC 활성화 옵션을 선택합니다. 중요 위치 변경 서비스는 최소 15분 후(기본 간격)에 사용자의 위치가 크게 변화하였을 경우에만 위치 업데이트를 iOS용 Go 앱에 전달하여 전력 소비를 절약하는 대안을 제공합니다. 이 서비스를 활성화할 경우 위치 변경 시 배경에 Go 앱이 실행되며 체크인됩니다.
5. **고객용 분석을 통한 데이터 수집**에서 **분석 활성화** 옵션이 비활성화되어 있으면 이를 선택합니다. 기본적으로 이 옵션은 활성화되어 있습니다.
6. **다음**을 클릭해 배포 설정을 구성합니다.
7. **완료**를 클릭합니다.

## 지원 탭 설정 구성

**적용 가능 운영 체제:**

- macOS용 Mobile@Work 1.67 또는 지원되는 최신 버전.
- iOS용 Go 3.5.0 또는 지원되는 최신 버전.
- Mobile@Work for Android 12.9.0.0 또는 지원되는 최신 버전.
- Go for Android 124 또는 지원되는 최신 버전.

**절차**

1. **구성** > **구성 추가** > **Ivanti Go Client 설정**으로 이동합니다. 그러면 **Ivanti Go Client 설정 구성 만들기** 페이지가 나타납니다.
2. **이름** 상자에 구성의 이름을 입력합니다.
3. 구성의 **설명**을 입력합니다.
4. **플랫폼** 옵션에서 해당 플랫폼을 선택합니다.
5. **지원 탭 설정 구성** 섹션에서 **지원 탭 활성화**를 클릭합니다.

> **지원 탭 활성화** 필드는 iOS 기기에만 적용됩니다.

> **지원 탭**은 iOS용 Go 버전 118.0.0 이상 및 Android용 Go 버전 124 이상에서 활성화할 수 있습니다. 이전 버전이 설치된 기기의 경우 이 기능이 표시되지 않거나 지원되지 않습니다.

**지원 연락처 구성** 섹션에서 다음 세부 정보를 입력합니다.

- **탭 이름** - Ivanti 앱 탐색 창에 표시되는 탭 이름을 입력합니다. 기본값은 '지원'입니다. (최대 10자)
- **최종 사용자 지침** - 지원 연락처 사용 방법에 대한 지침을 입력합니다. (최대 40자)
- **연락처 추가** - **+추가**를 클릭하여 연락처를 추가합니다. (최대 연락처 수: 5)
  - **이름** - 연락처 이름을 입력합니다. (최대 20자)
  - **전화번호** - 유효한 전화번호를 입력합니다. (국가 전화 코드 포함)
- **URL 추가** - **+추가**를 클릭하여 URL을 추가합니다. (최대 URL 수: 5)
  - **URL 이름** - URL 이름을 입력합니다. (최대 20자)
  - **URL** - 유효한 URL을 입력합니다.
- **추가 정보** - 여기에 표시할 추가적인 지원 관련 메시지가 있다면 입력합니다. (최대 120자)
- **이메일 보내기** - 지원 이메일을 보낼 수 있는 이메일을 입력합니다. (최대 40자)

  > alias@domainname.com 형식의 유효한 이메일 주소를 입력해야 합니다

- **지원 티켓 시스템 URL** - **iOS용 Ivanti Go** 및 **Android용 Ivanti Go** 앱에서 **지원** 탭에 '**지원 티켓 생성**' 버튼을 추가합니다. 토글을 활성화하여 지원 탭에 버튼을 표시하고, 제공된 필드에 적절한 URL을 입력하여 사용자를 지원 시스템으로 리디렉션합니다.

  > 이 URL은 Ivanti Go **지원 탭**에서 사용자를 지정된 지원 시스템으로 리디렉션하는 데 사용됩니다. 보안을 강화하려면 *http://*대신 *https://*를 시작하는 URL 사용이 권장됩니다.

**다음**을 클릭해 배포 설정을 구성합니다.

8. **완료**를 클릭합니다.

자세한 내용은 구성을 참조하십시오.

# 10.10.4.56. Siri 설정

**Siri 설정**을 사용하여 감독 모드 기기에서 Siri 설정을 구성합니다. 이 구성 통해 관리자는 기기가 Siri 기능에 액세스하고 이를 사용하는 방식을 관리하는 일관된 정책 기반 제어를 적용할 수 있습니다.

**적용 대상**:

- iOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- macOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- watchOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- visionOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지의 tvOS 27+ 감독 모드 기기.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **Siri 설정** 구성을 검색하여 선택합니다.
3. 다음 표에 따라 **Siri 설정**을 구성합니다.

| 설정 항목 | 수행 작업 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 활성화됨 | 확인란을 선택하여 Siri를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 Siri를 활성화합니다. |
| Siri AI 허용 | 확인란을 선택하여 **Siri AI** 전용 기능을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 **Siri AI** 전용 기능을 활성화합니다. |
| 사용자 생성 콘텐츠 허용 | 확인란을 선택하여 사용자 생성 콘텐츠를 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 사용자 생성 콘텐츠를 활성화합니다.<br>이 설정은 macOS 및 visionOS 기기에는 적용되지 않습니다. |
| 잠겨 있는 동안 | 확인란을 선택하여 잠겨 있는 동안을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 잠겨 있는 동안 허용을 활성화합니다.<br>이 설정은 macOS 및 visionOS 기기에는 적용되지 않습니다. |
| 욕설 필터 강제 적용 | 확인란을 선택하여 욕설 필터 강제 적용을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 욕설 필터 강제 적용을 활성화합니다.<br>이 설정은 visionOS 기기에는 적용되지 않습니다. |
| 민감한 컨텐츠 줄이기 강제 적용 | 확인란을 선택하여 Siri가 민감한 컨텐츠를 줄이도록 강제 적용합니다.<br>**기기로 푸시** 버튼을 전환하여 감독 모드 기기에서 Siri가 민감한 컨텐츠를 줄이도록 강제 적용합니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. **Siri 설정** 구성을 설정하려면 배포 옵션 중 하나를 선택합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.57. 서비스 구성 파일 설정

**서비스 구성 파일** 구성은 관리자가 등록된 기기에서 다양한 시스템 서비스에 대한 구성 파일을 중앙에서 관리하고 배포할 수 있게 합니다. 또한, 관리자는 변조 방지 환경에서 서비스별 보안 디렉토리에 파일을 배포함으로써, 서비스 설정이 일관되게 유지되고 무단 수정으로부터 보호되도록 설계할 수 있습니다.

**적용 대상**: macOS 기기

**시작하기 전에**:

- 다양한 구성을 *ZIP* 파일 형식으로 업로드할 수 있습니다. 파일 추가에 대한 자세한 내용은 **파일**을 참조하십시오.
- 확장된 보관 내의 모든 파일은 *-r–r–r– unix* 파일 권한으로 설정됩니다. 보관 내의 모든 링크는 서비스별 위치 내의 파일만 참조하도록 제한됩니다.
- ZIP 아카이브에 포함된 파일은 파일 시스템의 루트부터 시작하여 서비스에서 필요로 하는 폴더 구조 및 구성 파일을 그대로 반영해야 합니다. 서비스는 선언에서 제공된 파일만 사용하며, 기본 디렉토리에 있는 파일은 무시합니다.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **서비스 구성 파일** 구성을 검색하여 선택합니다.
3. 다음 표에 따라 **서비스 구성 파일** 설정을 구성합니다:

| 설정 항목 | 설명 |
| --- | --- |
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **파일 선택** | 파일 이름을 입력합니다. |
| **서비스 유형 선택** | 다음 드롭다운 목록에서 **서비스 유형** 중 하나를 선택합니다:<br>• SSHD<br>• SUDO<br>• PAM<br>• CUPS<br>• HTTP_D<br>• BASH<br>• ZSH |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **서비스 구성 파일** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 **구성 작업**을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.58. 소프트웨어 업데이트

**적용 가능 운영 체제:**

- iOS 10.3~26.0 및 tvOS 12.0~26.0 감독 모드 기기
- macOS 장치
- Windows 10+ 기기

OS 업데이트를 위한 규칙을 생성하고 배포합니다.

이 섹션에는 다음 주제가 포함됩니다.

- iOS/tvOS 기기의 소프트웨어 업데이트 구성
- DEP 외 기기 및 DEP macOS 기기의 소프트웨어 업데이트 구성
- Windows 기기의 소프트웨어 업데이트 구성
- 선언적 기기 관리(DDM)를 사용한 소프트웨어 업데이트 적용

## iOS/tvOS 기기의 소프트웨어 업데이트 구성

**절차**

감독 모드일 때 iOS/tvOS 기기에 OS 업데이트를 전송하는 방법:

1. **구성**으로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **소프트웨어 업데이트**를 클릭합니다.
4. **iOS/tvOS**를 클릭하여 구성 설정 섹션을 확인합니다.
5. **감독 대상 기기에 OS 업데이트를 자동으로 설치하도록 허용** 옵션을 선택합니다.
6. 다음 옵션 중 하나를 선택합니다.
    - 최신 버전으로 업데이트
    - 특정 버전으로 업데이트 - iOS 버전을 입력합니다(예: 11.3.0).
7. 다음 설치 작업 중 하나를 선택하십시오.
    - 기본
    - 다운로드만
    - 최대한 빨리 설치
8. 업데이트를 실행하기 위한 시간 옵션을 선택합니다.
    - 시작 시간
    - 종료 시간
    - 시간대
9. **다음**을 클릭하세요.
10. **이 구성 활성화** 옵션을 선택합니다.
11. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기

    - 배포 안 함(기본값)
    - 사용자 지정
12. **완료**를 클릭합니다.

- iOS 기기에 대해 특정 버전의 OS 업데이트를 설치할 때는 기기에 사용할 수 있는 버전을 선택해야 합니다. 유효하지 않거나 사용할 수 없는 버전을 선택할 경우 기기의 소프트웨어 업데이트가 무시됩니다.
- 기기에 암호가 있는 경우 MDM이 기기에 업데이트를 전송한 후, 기기에서 대기열에 업데이트를 추가하며, 사용자에게 설치를 시작하려면 암호를 입력하라는 메시지가 표시됩니다.
- iOS 제한에서 `enforcedSoftwareUpdateDelay`를 활성화하여 소프트웨어 업데이트에 대한 기기의 수동 검색이 이 구성에서 다운로드한 특정 버전을 삭제하지 않도록 합니다.

## DEP 외 기기 및 DEP macOS 기기의 소프트웨어 업데이트 구성

Apple Business Manager의 일부인 기기 등록 프로필을 통해 고객은 기기를 대량으로 구매하고, 활성화하는 동안 해당 기기를 MDM에 자동으로 등록할 수 있습니다. 자세한 내용은 기기 등록을 참조하십시오.

다음 절차는 DEP 외 기기 및 DEP macOS 기기에 OS 업데이트를 전송하는 데 도움이 됩니다.

**절차**

1. **구성**으로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **소프트웨어 업데이트**를 클릭합니다.
4. **macOS**를 클릭하여 구성 설정 섹션을 확인합니다.
5. **macOS 소프트웨어 업데이트 활성화** 옵션을 선택합니다.
6. 기기에 대한 업데이트 유형을 선택합니다. 이들 업데이트 각각에 대해 다시 시작하지 않아도 되는 업데이트를 선택할 수도 있습니다.
    - OS 업데이트
    - 중요 업데이트
    - 구성 데이터 업데이트
    - 펌웨어 업데이트
    - 중요하지 않은 업데이트

    > 관리자는 **중요하지 않은 업데이트 활성화**를 사용 설정하여 중요하지 않은 macOS 업데이트를 관리(설치/예약)할 수 있습니다. 기존 테넌트에 대해서는 이 옵션이 기본적으로 비활성화되므로 필요한 경우 관리자의 명시적 사후 업그레이드로 활성화해야 합니다.

    > **OS 업데이트**에서 관리자는 기기를 macOS의 특정 버전으로 업데이트할 수 있습니다.

    > 모든 macOS 업데이트는 다음과 같이 작업과 함께 구성할 수 있습니다.

        - 기본
        - 알림만
        - 나중에 설치
        - 강제 다시 시작 설치

        - 다운로드만
        - 최대한 빨리 설치
    -

가능한 값 - 낮음, 높음

기본값 - 낮음

우선 순위

    - 최대 사용자 지연
      가능한 값 - 정수
      나중에 설치 옵션이 선택된 경우에만 지원됩니다.
7. 업데이트를 실행하기 위한 시간 옵션을 선택합니다.
    - 시작 시간
    - 종료 시간
    - 시간대
8. **다음**을 클릭하세요.
9. **이 구성 활성화** 옵션을 선택합니다.
10. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
11. **완료**를 클릭합니다.

## Windows 기기의 소프트웨어 업데이트 구성

**절차**

Windows 설치 업데이트 일정을 설정하려면:

1. **구성**으로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **소프트웨어 업데이트**를 클릭합니다.
4. **Windows**를 클릭하여 구성 설정 섹션을 확인합니다.
5. Windows 기기 버전에 따라 다음 옵션을 입력합니다.
6. **다음**을 클릭하세요.
7. **이 구성 활성화** 옵션을 선택합니다.
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정

**완료**를 클릭합니다.

## Windows 10+ 기기의 소프트웨어 업데이트

- 업데이트 소스 - 다음 소스 중 하나를 선택합니다.
  - Enterprise WSUS
  - Microsoft 업데이트 및/또는 Enterprise WSUS

드라이버 업데이트 소스

- 기능 업데이트 소스
- 기타 업데이트 소스
- 품질 업데이트 소스
- Enterprise WSUS Server URL
- 대체 인트라넷 Microsoft 업데이트 서버
- '신뢰하는 게시자'에서 업데이트 허용 - 신뢰하는 게시자로만 업데이트 소스를 제한합니다.
- 자동 업데이트 전략 - 풀다운 메뉴에서 옵션 중 하나를 선택합니다.
- 예정 설치일 - 업데이트 빈도를 설정합니다.
- 예정 설치 시간 - 업데이트 설치 시간을 선택합니다.
- 업데이트가 계량된 연결에 따라 자동으로 다운로드되도록 허용 – 옵션을 활성화 또는 비활성화합니다.
- Windows 업데이트에 대해 스캔을 유발하는 유예 정책 업데이트 허용 불가 – 옵션을 활성화 또는 비활성화합니다.
- 약속된 데드라인 재시작 – 데드라인을 다시 시작할 기간(일)을 선택합니다.
- 약속된 데드라인 재시작 다시 알림 – 약속된 데드라인 재시작을 다시 알릴 기간(일)을 선택합니다.
- 약속된 전환 일정 재시작 – 전환 일정을 다시 시작할 기간(일)을 선택합니다.
- 빈 콘텐츠 URL 업데이트/채우기.
- MO App 다운로드 제한 – 다음 옵션 중 하나를 선택합니다.
  - 앱과 업데이트의 MO 다운로드 제한을 무시하지 마십시오
  - 앱과 업데이트의 MO 다운로드 제한을 무시하십시오(무제한 다운로드 허용)
- MO 업데이트 다운로드 제한 – 다음 옵션 중 하나를 선택합니다.
  - OS 업데이트의 MO 다운로드 제한을 무시하지 마십시오
  - OS 업데이트의 MO 다운로드 제한을 무시하십시오(무제한 다운로드 허용)
- Preview 빌드 관리 – 다음 옵션 중 하나를 선택합니다.
  - Preview 빌드 사용 안 함
  - 다음 릴리스가 공개되면 Preview 빌드 사용 안 함
  - Preview 빌드 사용
- 업데이트용 자동 재시작 경고 알림 일정 – 자동 재시작 경고 알림에 소요될 시간(분)을 선택합니다.
- 재시작 경고 알림 – 재시작 경고 알림을 설정할 시간을 선택합니다.
- 자동 업데이트 일정 – 자동 업데이트 빈도를 선택합니다.
- 업데이트용 자동 재시작 알림-– 업데이트용 자동 재시작 알림을 켭니다.
- 제품 버전 - Windows 업데이트 버전 페이지(URL: aka.ms/WindowsTargetVersioninfo)에 나열된 제품 버전을 입력합니다. 예를 들어 "Windows 11", "11" 또는 "Windows 10"입니다.
- 대상 릴리스 버전 - Windows 업데이트 버전 페이지에 대상 릴리스 버전을 입력합니다.

- 사용 시간 시작 - 이 옵션을 활성화하면 사용 시간 동안 업데이트 후 PC가 자동으로 다시 시작되지 않습니다. 사용 시간 외에는 PC가 다시 시작을 시도합니다.
- 사용 시간 종료 - 이 옵션을 활성화하면 사용 시간 동안 업데이트 후 PC가 자동으로 다시 시작되지 않습니다. 사용 시간 외에는 PC가 다시 시작을 시도합니다.
- 사용 시간 최대 범위 – 사용자가 사용 시간을 설정할 수 있는 시작 시간부터 최대 시간을 나타내려면 이 옵션을 활성화합니다.
- 사용 시간 동안 업데이트 알림 없음 - 업데이트 알림 옵션은 다음과 같습니다.
  - 기본 Windows 업데이트 알림
  - 다시 시작 경고를 제외한 모든 알림 해제
  - 다시 시작 경고를 포함한 모든 알림 해제
- 드라이버 업데이트 비활성화 – Windows 품질 업데이트에서 드라이버를 제외하려면 이 옵션을 활성화합니다. 이 옵션을 비활성화하거나 구성하지 않으면 드라이버 분류가 포함된 업데이트가 Windows 업데이트에 포함됩니다.
- 품질 업데이트 기한 – 품질 업데이트가 장치에 자동으로 설치되기까지의 일수는 사용 시간과 별개입니다.
- 품질 업데이트 기한 유예 기간 – 업데이트 설치부터 품질 업데이트를 위해 자동으로 다시 시작될 때까지의 최소 일수입니다.
- 기능 업데이트 기한 유예 기간 – 사용 시간과 관계없이 기능 업데이트가 장치에 자동으로 배포될 때까지의 일수입니다.
- 기능 업데이트 기한 유예 기간 – 사용 시간과 관계없이 기능 업데이트가 장치에 자동으로 배포될 때까지의 최소 일수입니다.
- 유예 기간이 끝날 때까지 자동으로 다시 시작하지 않음 – 활성화하면 업데이트를 다시 시작할 준비가 된 경우에도 기한과 유예 기간이 지날 때까지 사용 시간 외에 장치가 자동으로 다시 시작되지 않습니다. 비활성화하면 기한 이전에 업데이트를 다시 시작할 수 있는 경우 사용 시간 외에 자동 다시 시작이 시도될 수 있습니다.

### Windows 10.0.14393 이전 기기의 소프트웨어 업데이트

다음 설정은 기기에서 원격 분석 제한이 비활성화되면 작동하지 않습니다.

- 업그레이드/업데이트 일시 정지 – 변경 사항을 나중으로 미룹니다.
- 업데이트 연기 기간 – 최대 4주까지 연기할 수 있습니다.
- 업그레이드 연기 – 업그레이드를 연기합니다.
- 업그레이드 연기 기간 – 최대 8개월까지 연기할 수 있습니다.

### Windows 10.0.14393+ 기기의 소프트웨어 업데이트

- 업데이트를 설치할 분기 - IT 관리자가 장치가 업데이트를 받을 분기를 설정할 수 있습니다. 업데이트를 설치할 분기 필드에는 다음 옵션이 포함됩니다.
  - Windows 참가자 빌드 - 빠름
  - Windows 참가자 빌드 - 느림
  - Windows 참가자 빌드 릴리스
  - 연 2회 채널(타겟티드)
  - 연 2회 채널
  - 품질 업데이트만 릴리스 미리보기
  - Canary 채널

기능 업데이트(업그레이드) - Windows Professional, Windows Enterprise, Windows Education에서만 지원됩니다.

  - 업데이트 일시 중지

- 연기 기간 - 최대 180일까지 연기할 수 있습니다.

품질 업데이트(업데이트) - Windows Professional, Windows Enterprise, Windows Education에서만 지원됩니다.

- 업데이트 일시 중지
- 연기 기간 - 최대 30일까지 연기할 수 있습니다.

### Windows 10.0.17083+ 기기의 소프트웨어 업데이트

- 기능 업데이트:
  - 기능 업데이트 설치 해제 기간 – 기능 업데이트 설치 해제에 소요될 기간(일)을 선택합니다.

### Windows 10.0.17763+ 기기의 소프트웨어 업데이트

- 사용자별 "업데이트 일시 중지" 액세스 사용 안 함
- 사용자별 UXWU 액세스 사용 안 함(Windows 업데이트 검사, 다운로드 및 설치)
- 업데이트 알림 수준 – 다음 옵션 중 하나를 선택합니다.
  - 기본 Windows 업데이트 알림 사용
  - 다시 시작 경고를 제외한 모든 알림 해제
  - 다시 시작 경고를 포함한 모든 알림 해제
- 기능 업데이트:
  - 업데이트 설치를 위한 자동 재시작 전 데드라인 – 업데이트 설치를 위한 자동 재시작 전 데드라인을 위한 기간(일)을 선택합니다.
  - 약속된 데드라인 재시작 – 약속된 데드라인 재시작을 위한 기간(일)을 선택합니다.
  - 약속된 데드라인 재시작 다시 알림 – 약속된 데드라인 재시작을 다시 알릴 기간(일)을 선택합니다.
  - 약속된 전환 일정 재시작 – 전환 일정을 다시 시작할 기간(일)을 선택합니다.

## DDM을 사용한 소프트웨어 업데이트 적용

관리자는 DDM을 사용하여 iOS, macOS, iPadOS 기기에 소프트웨어 업데이트 설치를 적용할 수 있습니다.

지원:

- iOS 17+
- iPadOS 17+
- macOS 14+

**절차**

1. 구성 섹션에서 **소프트웨어 업데이트 적용** 구성을 새로 만듭니다.
2. 강제 체크인을 수행하여 소프트웨어 업데이트 적용 구성이 기기에 설치되어 있는지 확인하십시오.

장치를 열면 버전 번호, 필요한 날짜 등과 같은 세부 정보가 포함된 필수 소프트웨어 업데이트에 대한 알림이 표시됩니다.

> 소프트웨어 업데이트를 적용하지 않으려면 구성 배포 옵션을 **없음**으로 설정해야 합니다.

### 소프트웨어 업데이트 적용에 조건자 배포 구성

1. 소프트웨어 업데이트 적용 구성을 만듭니다.

2. 토글 스위치 "조건자를 사용한 활성화"를 ON으로 설정하고 + 버튼을 눌러 (필요에 따라) 조건자를 포함합니다.




조건자를 편집하거나 삭제하려면 **관리자** > **Apple** > **조건자**로 이동합니다. 이 페이지에서 사용 가능한 조건자 목록을 확인할 수 있습니다. **편집**을 클릭하여 기존 조건자를 변경하고 저장할 수 있습니다. 마찬가지로, 기존 조건자를 삭제하려면 조건자를 선택하고 **삭제**를 클릭합니다.

> 구성과 연관된 조건자는 삭제할 수 없습니다.

# 10.10.4.59. 소프트웨어 업데이트 설정 구성

MDM용 Ivanti Neurons 을 사용하여 소프트웨어 업데이트 적용 설정을 생성하고 최종 사용자에게 적용되는 업데이트의 케이던스 및 연기 동작을 정의할 수 있습니다.

**적용 대상**:

- 감독 대상인 iOS 18.0부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- 감독 대상인 macOS 15.0부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **소프트웨어 업데이트 설정** 구성을 검색하고 선택합니다.
3. 다음 표에 따라 **소프트웨어 업데이트 설정**을 구성합니다.

| 설정 항목 | 설명 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **iOS 18+ 감독 대상** 및 **macOS15+**<br><br>베타 등록<br><br>프로그램 등록(선택 사항) | 다음 옵션 중 하나를 선택합니다.<br>• **허용됨**: 사용자는 로그인한 Apple 계정과 연결된 해당 베타 프로그램에 등록할 수 있습니다.<br>• **항상 켜짐**: 조직에서 지정한 베타 프로그램이 사용되며, 사용자는 로그인한 Apple 계정을 사용하여 베타 프로그램에 등록할 수 없습니다.<br>**프로그램 제공** - 프로그램 제공을 이용하면 필요한 프로그램을 시행할 수 있습니다. 적용할 때 iOS 및 macOS 장치에 필요한 버전을 설정할 수 있습니다.<br>**필수 프로그램**: 기기가 이 베타 프로그램에 자동으로 등록됩니다.<br>• **항상 꺼짐**: 기기를 어떤 베타 프로그램에도 등록할 수 없습니다. 기기가 이미 등록되어 있다면 시스템이 베타 프로그램에서 기기를 제거합니다. |
| **감독 대상인 iOS 18+** 및 **감독 대상인 macOS15+** | |
| 알림 | **알림** 확인란과 **모든 소프트웨어 업데이트 적용 알림 표시** 확인란을 선택하여 사용자 기기에 모든 소프트웨어 업데이트 적용 알림을 표시합니다.<br>**알림** 확인란만 선택하면, 기기는 적용 마감 시간 1시간 전에 단일 적용 알림을 표시합니다.<br>두 확인란 중 어느 것도 선택하지 않으면, 기기에는 사용자의 기기에서 모든 소프트웨어 업데이트 적용 알림을 표시하도록 트리거된 알림이 표시됩니다. |
| 자동 작업 | |
| 다운로드<br><br><br><br>OS 업데이트 설치<br><br><br><br>백그라운드 보안 개선<br><br>백그라운드 보안 개선<br><br><br><br>**감독 대상인 iOS 18+** | 다음 옵션 중 하나를 선택합니다.<br>• **허용됨**: 사용자는 자동 다운로드에 대해 "켜짐" 또는 "꺼짐"을 설정할 수 있습니다.<br>• **항상 켜짐**: 자동 다운로드가 사용자에게 항상 "켜짐" 상태입니다.<br>• **항상 꺼짐**: 자동 다운로드가 사용자에게 항상 "꺼짐" 상태입니다.<br><br>다음 옵션 중 하나를 선택합니다.<br>• **허용됨**: 사용자는 OS 업데이트를 자동으로 설치하기 위해 "켜짐" 또는 "꺼짐"을 설정할 수 있습니다.<br>• **항상 켜짐**: OS 업데이트 자동 설치가 사용자에게 항상 "켜짐" 상태입니다.<br>• **항상 꺼짐**: OS 업데이트 자동 설치가 사용자에게 항상 "꺼짐" 상태입니다.<br><br><br><br>**백그라운드 보안 개선** 확인란을 선택하여 업데이트 설치 및 롤백을 제어합니다. 다음 옵션을 선택합니다.<br>• **활성화**: 이 옵션을 선택하면 **백그라운드 보안 개선** 설치가 사용자에게 제공됩니다.<br>• **롤백 활성화**: 이 옵션을 선택하면 **백그라운드 보안 개선** 롤백이 사용자에게 제공됩니다. |

| 설정 항목 | 설명 |
| --- | --- |
| 권장 케이던스 | 두 개 이상의 업데이트가 있는 경우 다음 옵션 중 하나를 선택하여 사용자에게 소프트웨어 업데이트를 표시합니다.<br>• **모두**: 모든 소프트웨어 업데이트 버전을 보여줍니다.<br>• **가장 오래된 순**: 가장 오래된(낮은 번호) 소프트웨어 업데이트 버전만 표시합니다.<br>• **최신순**: 최신(가장 높은 번호) 소프트웨어 업데이트 버전만 표시합니다. |
| 연기 | 모든 감독 대상 기기에 대해 소프트웨어 업데이트를 연기하도록 선택할 수 있습니다.<br>**백그라운드 보안 개선**은 연기할 수 없습니다. |
| 결합 기간(일수)<br><br>**감독 대상인 macOS 15+** | 장치의 주요 또는 경미한 시스템 업데이트를 연기할 일수를 설정합니다. 구성이 완료되면, 주요 또는 경미한 소프트웨어 업데이트는 릴리스 후 지정된 일수 후에 나타납니다.<br>1~90일 사이의 값을 설정할 수 있습니다. |
| 표준 사용자 OS 업데이트 허용 | **표준 사용자 OS 업데이트 허용** 확인란을 선택하여 사용자가 OS 업데이트를 수행할 수 있도록 허용합니다.<br>**표준 사용자가 주요 및 경미한 소프트웨어 업데이트를 수행하도록 허용** 확인란을 선택하여 표준 사용자가 경미한 소프트웨어 업데이트와 주요 소프트웨어 업데이트를 수행할 수 있도록 허용합니다.<br>확인란을 선택하지 않으면 관리자만 경미한 소프트웨어 업데이트와 주요 소프트웨어 업데이트를 수행할 수 있습니다. |
| 연기 | |
| 주요 업데이트 기간(일수) | 장치의 주요 OS 소프트웨어 업데이트를 연기할 일수를 설정합니다. 구성이 완료되면, 주요 소프트웨어 업데이트는 출시 후 지정된 날짜 이후에 나타납니다.<br>1~90일 사이의 값을 설정할 수 있습니다. |
| 경미한 업데이트 기간(일수) | 기기에서 경미한 OS 소프트웨어 업데이트를 연기할 일수를 설정합니다. 구성이 완료되면, 주요 소프트웨어 업데이트는 출시 후 지정된 날짜 이후에 나타납니다.<br>1~90일 사이의 값을 설정할 수 있습니다. |
| 시스템 업데이트 기간(일수) | 기기에서 시스템 OS 업데이트를 연기할 일수를 설정합니다. 구성이 완료되면, 주요 소프트웨어 업데이트는 출시 후 지정된 날짜 이후에 나타납니다.<br>1~90일 사이의 값을 설정할 수 있습니다. |
| 자동 작업 | |
| 보안 업데이트 설치 | 다음 옵션 중 하나를 선택합니다.<br>• **허용됨**: 사용자는 보안 업데이트 설치를 "켜짐" 또는 "꺼짐"으로 전환할 수 있습니다.<br>• **항상 켜짐**: 보안 업데이트 설치가 사용자에게 항상 "켜짐" 상태로 유지됩니다.<br>• **항상 꺼짐**: 보안 업데이트 설치가 사용자에게 항상 "꺼짐" 상태로 설정됩니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **소프트웨어 업데이트 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.4.60. 보안 기본 설정 구성

관리자는 보안 기본 설정 구성을 통해 방화벽 설정 사용자 변경, 잠금 메시지 및 기기 비밀번호 변경을 관리, 제어할 수 있습니다.

적용 대상: macOS 10.10+

**Procedure**

1. 구성 > +추가로 이동합니다.
2. 검색 필드에 보안을 입력한 다음, 보안 기본 설정 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. 필요한 구성을 선택합니다.
    - 방화벽 설정 변경 비활성화
    - 잠금 메시지 변경 비활성화
    - 비밀번호 변경 비활성화
5. 다음을 클릭하세요.
6. 이 구성 활성화 옵션을 선택합니다.
7. 구성을 적용하기 위해 다음 채널 옵션 중 하나를 선택합니다.
    - 기기 채널(가장 일반적)
    - 사용자 채널(현재 등록 사용자)
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
9. 완료를 클릭하세요.

# 10.10.4.61. 시간 서버

**적용 대상:** macOS 10.12.4 또는 지원되는 최신 버전.

장치가 사용자 지정 시간 서버에 연결될 수 있도록 시간 서버 구성을 생성합니다.

## 시간 서버 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **시간**을 입력한 다음, **시간 서버** 구성을 클릭합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. **NTP 서버**를 지정합니다.
6. **시간대** 문자열을 Olson 표준 시간대 ID 형식으로 지정합니다(예: Pacific / Midway). Olson Time Zone 형식을 가져오려면 관리자의 macOS 기기에서 `"/usr/sbin/systemsetup -listtimezones"` 명령을 실행합니다.
7. **다음**을 클릭해 배포 설정을 구성합니다.
8. **완료**를 클릭하세요.

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.4.62. 웹 컨텐츠 필터

**라이센스:** Silver

웹 콘텐츠 필터 구성은 iOS 7 이상, macOS 10.15 이상, visionOS 1.1 이상 기기에 대한 웹 액세스를 제한합니다.

## 웹 컨텐츠 필터 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 허용된 웹 사이트 | **제한된 성인 콘텐츠:** iOS 자동 필터에 기반하여 웹 사이트 액세스를 차단하려면 이 옵션을 선택합니다. 해당 필터 기능은 유해 컨텐츠를 제공하는 웹 사이트를 높은 정확도로 차단합니다.<br>**특정 웹 사이트만:** 액세스 가능한 웹 사이트의 목록을 수동으로 작성하려면 이 옵션을 선택합니다.<br>**플러그인(감독 대상 iOS 8, macOS 10.15 이상에만 해당)**: 타사 플러그인을 사용하려면 이 옵션을 선택합니다. |
| 허용된 URL | 이 옵션은 성인 컨텐츠 제한이 선택된 경우에 한해 지원됩니다.<br>허용된 URL을 입력할 수 있습니다. 각 URL은 반드시 다음 값 중 하나로 시작해야 합니다.<br>• http://<br>• https://<br>동일 사이트에 http:// 및 https://를 둘 다 허용하려면 2개의 URL을 포함하십시오.<br>지정한 허용 URL과 시작 글자가 일치하는 모든 URL은 접속이 가능합니다.<br>예: http://www.someCompanySite.com은 다음과 같은 사이트 접속을 허용합니다.<br>• http://www.someCompanySite.com<br>• http://www.someCompanySite.com/jobs<br>이런 URL은 iOS 자동 필터 기능으로 차단을 해도 접속이 가능합니다. |
| 거부 목록 URL 사용 | 이 옵션은 성인 컨텐츠 제한이 선택된 경우에 한해 지원됩니다.<br>허용 목록으로 지정된 URL을 입력합니다. 각 URL은 반드시 다음 값 중 하나로 시작해야 합니다.<br>• http://<br>• https://<br>동일 사이트에 http:// 및 https://를 둘 다 차단하려면 각 URL의 행을 포함하십시오.<br>지정한 차단 목록에 포함된 URL과 시작 글자가 일치하는 URL은 모두 차단됩니다.<br>예: http://www.someCompanySite.com은 다음과 같은 사이트 접속을 차단합니다.<br>• http://www.someCompanySite.com<br>• http://www.someCompanySite.com/jobs<br>이런 URL은 iOS 자동 필터 기능으로 허용을 해도 접속이 차단되기 때문입니다. |
| 허용 목록에 있는 북마크 | 이 옵션은 특정 웹 사이트만 선택한 경우에 한해 지원됩니다.<br>필요한 경우 Safari에 북마크 추가가 필요한 폴더를 입력할 수 있습니다(선택 사항).<br>예:<br>/Sales/Products/<br>빈칸으로 남길 경우 북마크는 기본 북마크 디렉토리로 추가됩니다. |
| 필터 이름 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>이 필터를 식별하도록 표시할 내용을 입력할 수 있습니다. |
| 식별자 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>필터링 서비스를 제공하는 플러그인의 번들 ID를 입력할 수 있습니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| 서비스 주소 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>선택 사항: 플러그인 사용에 필요한 서버 주소를 입력할 수 있습니다. 플러그인 관련 문서를 참고하여 이 값이 필요한지 여부를 결정할 수 있습니다. |
| 조직 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>선택 사항: 플러그인이 요구하는 조직 문자열을 입력할 수 있습니다. 플러그인 관련 문서를 참고하여 이 값이 필요한지 여부를 결정할 수 있습니다. |
| 사용자 이름 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>선택 사항: 플러그인 서비스가 요구하는 모든 사용자 이름을 입력할 수 있습니다. 플러그인 관련 문서를 참고하여 이 값이 필요한지 여부를 결정할 수 있습니다. |
| 비밀번호 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>선택 사항: 플러그인 서비스가 요구하는 모든 비밀번호를 입력할 수 있습니다. 플러그인 관련 문서를 참고하여 이 값이 필요한지 여부를 결정할 수 있습니다. |
| 인증서 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>선택 사항: 플러그인 서비스가 요구하는 모든 인증서를 입력하여 사용자를 인증할 수 있습니다. 플러그인 관련 문서를 참고하여 이 값이 필요한지 여부를 결정할 수 있습니다. |
| 필터 Webkit 트래픽 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>필터에 Webkit 트래픽을 포함하도록 선택할 수 있습니다. |
| 필터 소켓 트래픽 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>필터에 소켓 트래픽을 포함하도록 선택할 수 있습니다. |
| 사용자 지정 데이터 | 이 옵션은 플러그인을 선택한 경우에 한해 지원됩니다.<br>선택 사항: 플러그인 서비스가 요구하는 모든 키/값 쌍을 추가할 수 있습니다. 플러그인 관련 문서를 참고하여 이 값이 필요한지 여부를 결정할 수 있습니다. |

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.4.63. Windows 방화벽

Windows 방화벽 구성은 Windows 방화벽 프로필 설정을 구성하고 기기에 원하는 사용자 지정 규칙을 시행할 수 있게 합니다. 이 구성을 사용하여 비관리 기기를 관리하고 기업 네트워크에 연결된 모든 시스템의 네트워크 보안 위협 위험을 감소시킬 수 있습니다.

## Windows 방화벽 구성 설정

**절차**

1. **구성 > +추가**로 이동합니다.
2. **방화벽** 구성을 선택합니다.
3. **Windows** 아이콘을 클릭합니다.
4. 구성 이름을 입력합니다.
5. 방화벽 구성의 설명을 입력합니다.
6. 구성 설정 섹션에서 다음 표에 설명된 바와 같이 남은 설정을 지정합니다.

| 설정 | 설정하기 |
| --- | --- |
| **프로필** | |
| 활성화 | 프로필을 활성화하려면 스위치를 켜기로 밉니다. |
| 유형 | 프로필의 유형을 표시합니다.<br>예: 도메인 |
| 기본 인바운드 조치 | 인바운드 트래픽에서 수행되어야 할 기본 조치 옵션을 선택합니다.<br>**허용**: 트래픽을 허용합니다.<br>**차단**: 트래픽을 차단합니다. |
| 기본 아웃바운드 조치 | 아웃바운드 트래픽에서 수행되어야 할 기본 조치 옵션을 선택합니다.<br>**허용**: 트래픽을 허용합니다.<br>**차단**: 트래픽을 차단합니다. |

7. 규칙을 추가하려면 **+추가**를 클릭하고 다음 설정을 구성합니다.

| 설정 | 설정하기 |
| --- | --- |
| **규칙** | |
| 설정 | 프로필을 활성화하려면 스위치를 밉니다. |
| 규칙 이름 | 현재 규칙을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 규칙에 대한 간략한 설명을 입력합니다. |
| 지시 | 규칙이 적용되어야 할 트래픽의 방향을 선택합니다.<br>• **인**: 인바운드 트래픽의 경우<br>• **아웃**: 아웃바운드 트래픽의 경우<br>• **모두**: 양방향 |
| 작업 | 수행할 작업을 선택합니다.<br>• **허용**: 트래픽을 허용합니다.<br>• **차단**: 트래픽을 차단합니다. |
| 프로필 | 규칙이 적용되어야 할 프로필을 선택합니다.<br>• **모두**<br>• **도메인**<br>• **개인용**<br>• **공용** |
| 앱 | 실행 앱에 패키지 패밀리 이름(PFN) 또는 전체 경로를 입력합니다. |
| 프로토콜 | 다음 중 규칙이 적용되어야 할 프로토콜을 선택합니다.<br>• **TCP**<br>• **UDP**<br>• **ICMP** |
| 로컬 주소 범위 | 로컬 IPv4/IPv6 주소 범위 또는 서브넷 마스크를 입력합니다. |
| 로컬 포트 범위 | 쉼표로 구분된 로컬 포트 또는 포트 범위 목록을 입력합니다.<br>예: 20,50,100-120 |
| 원격 주소 범위 | 원격 IPv4/IPv6 주소 범위 또는 서브넷 마스크를 입력합니다. |
| 원격 포트 범위 | 쉼표로 구분된 로컬 포트 또는 포트 범위 목록을 입력합니다.<br>예: 20,50,100-120 |
| 인터페이스 유형 | 다음 인터페이스 유형 옵션 중 하나를 선택합니다.<br>• **모두**<br>• **원격 액세스**<br>• **무선**<br>• **LAN** |

| 설정 | 설정하기 |
| --- | --- |
| | • **모바일 광대역**<br>인터페이스 유형 옵션을 선택하지 않은 경우에는 기본 옵션인 **모두**가 적용됩니다. |

8. **다음**을 클릭하세요.
9. 다음 배포 옵션 중 하나를 선택합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정
10. **완료**를 클릭하세요.

# 10.10.4.64. Windows 정보 보호

**라이센스: Gold**

**적용 가능 운영 체제: Windows 10+**

WIP(Windows 정보 보호) 구성은 WIP 설정을 정의하여 엔터프라이즈 데이터를 보호합니다. 이 구성은 관리에 등록된 기기에 적용할 수 있습니다. 또한 해당 장치의 개요 페이지에서 구성된 장치에 대한 WIP 상세 정보를 확인할 수 있습니다.

## Windows용 Windows 정보 보호 설정

**절차**

1. **구성 > +추가**로 이동합니다.
2. **Windows 정보 보호** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 표에 설명된 바와 같이 남은 설정을 지정합니다.
6. **다음**을 클릭하세요.
7. 이 구성에 대한 배포를 선택합니다.

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| | 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 엔터프라이즈 정보 | **모든 버전(Windows 10+)** | |
| | 보호되는 도메인 이름 | 데이터 보호 정책을 구성할 ID 목록을 지정합니다. 이러한 ID와 관련된 이메일 및 기타 데이터는 엔터프라이즈용으로 간주되어 보호됩니다.<br>• \|으로 구분하는 도메인 목록으로, 목록의 첫 번째 도메인은 Windows UI를 위한 기본 ID로 간주합니다.<br>• 예: "domain1.com\|domain2.co.uk" |
| | 네트워크 도메인 이름 | 엔터프라이즈의 경계를 구성하는 도메인 목록을 지정합니다. 기기로 전송되는 이러한 도메인 중 하나의 데이터는 엔터프라이즈 데이터로 간주되어 보호됩니다.<br>• 이 위치는 엔터프라이즈 데이터를 공유하기에 안전한 대상으로 간주됩니다.<br>• 도메인을 쉼표로 구분한 목록입니다.<br>• 예: "mail.domain3.com, domain4.com" |
| | 클라우드 리소스 | 보호해야 할 클라우드에서 호스팅되는 엔터프라이즈 리소스 도메인 목록입니다. 이런 리소스와의 연결은 엔터프라이즈 데이터로 간주합니다. 괄호 안에 선택적 프록시 주소가 있는 하나 이상의 도메인 이름을 지정합니다.<br>• 예: "domainname1.com, domainname2 (10.0.0.1)".<br>• 프록시가 클라우드 리소스와 페어링되면 클라우드 리소스로의 트래픽이 지정된 프록시 서버(포트 80)를 통해 엔터프라이즈 네트워크로 라우팅됩니다.<br>• 이 필드에 지정된 모든 프록시 주소를 다음 내부 프록시 서버 필드에도 입력해야 합니다. |
| | IP 범위 | 엔터프라이즈 네트워크에서 컴퓨터를 정의하는 엔터프라이즈 IP 범위를 설정합니다. 이런 컴퓨터에서 나오는 데이터는 엔터프라이즈의 일부로 간주하고 보호합니다. 이 위치는 엔터프라이즈 데이터를 공유하기에 안전한 대상으로 간주됩니다. IPv4와 IPv6 범위를 쉼표로 구분한 목록입니다.<br>• IPv4와 IPv6 범위를 쉼표로 구분한 목록입니다.<br>• 클라이언트가 구성된 목록을 받아들이고 탐색 방법을 사용하여 다른 서브넷을 찾지 말아야 할 경우 **IP 범위를 신뢰할 수 있음** 옵션을 선택합니다. |
| | 중립 리소스 | 작업 또는 개인 리소스로 사용할 수 있는 도메인 이름 목록을 지정합니다. |
| | 프록시 서버 | 프록시 서버의 쉼표로 구분한 목록을 지정합니다. 이 목록에 있는 모든 서버는 엔터프라이즈가 아닌 것으로 간주합니다.<br>• 예: “157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59"<br>• 클라이언트가 프록시 구성 목록을 받아들이고 다른 작업 프록시를 감지하지 말아야 할 경우 **프록시 서버를 신뢰할 수 있음** 옵션을 선택합니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 내부 프록시 서버 | 내부 프록시 서버의 쉼표로 구분한 목록을 지정합니다.<br>• 예: "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59"<br>• 이런 프록시는 인터넷의 특정 리소스와 연결되도록 관리자가 구성합니다. 엔터프라이즈 네트워크 위치로 간주합니다. 프록시는 EnterpriseCloudResources 정책을 구성하는 데만 활용하여 트래픽이 이런 프록시를 통해 클라우드 리소스와 일치하도록 강제합니다. |
| 데이터 보호 | **모든 버전(Windows 10+)** | |
| | 적용 수준 | 다음 적용 수준 중 한 가지를 선택합니다.<br>• 꺼짐 - 보호 없음(이전의 암호화된 데이터에 암호화가 적용되지 않습니다).<br>• 자동 - 데이터가 보호된 후 기기에서 데이터와 감사 활동을 암호화합니다. 사용자는 계정에서 부정적인 데이터/앱 정보를 받지 않습니다.<br>• 재정의 - 자동 모드와 유사합니다. 또한 앱이나 데이터가 잘못 사용되고 있다면 사용자가 현재 수행 중인 작업을 진행하거나 취소할지 사용자에게 묻습니다.<br>• 차단 - 자동 모드와 유사합니다. 또한, 앱이나 데이터가 잘못 사용되고 있다면 현재 사용자가 수행하는 작업이 차단되고 사용자에게는 작업 차단 이유를 경고합니다.<br>꺼짐 모드를 제외하고는 엔터프라이즈 데이터나 리소스를 사용할 수 없는 데이터나 앱은 기기에 기록됩니다. 이 데이터는 다른 CSP(구성 서비스 제공자)를 사용하여 장치에서 제거할 수 있습니다. |
| RMS | 데이터 복구 인증서 | 암호화된 파일의 데이터 복구에 사용할 수 있는 복구 인증서를 지정합니다.<br>• EFS(암호화 파일 시스템)의 DRA(데이터 복구 에이전트) 인증서와 동일합니다. 그러나 이 인증서는 그룹 정책이 아니라 MDM에서 파생됩니다.<br>또한 다음 옵션 중 하나를 선택할 수 있습니다.<br>• 사용자 암호 해독 허용<br>• 등록 취소 시 철회<br>• EDP 아이콘 표시<br>• 잠금 상태에서 보호 필요(Windows 10 Mobile 전용) |
| | **모든 버전(Windows 10+)** | |
| | Azure RMS 허용 | WIP에 대해 Azure RMS(Azure 권한 관리) 암호화 허용 여부를 설정합니다. |
| | RMS 템플릿 ID | RMS 암호화용으로 사용할 TemplateID GUID를 지정합니다. RMS 템플릿을 사용하면 관리자가 RMS 보호 파일에 액세스할 수 있는 사람과 액세스 시간에 관한 상세 정보를 구성할 수 있습니다. |
| 앱 컨트롤 | **모든 버전(Windows 10+)** | |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | WIP 값으로 **앱 > App Catalog** 페이지에서 빌드된 앱 컬렉션을 지정합니다. 다음 매개 변수 세트를 사용하여 앱에 대한 규칙 정의를 지정합니다. | |
| | 앱 유형 | 다음 앱 유형 중 하나를 선택합니다.<br>• 게시자/PFN 같음 - PFN을 지원하는 Windows 10 이상에 적용됩니다.<br>• EXE/Win32 같음 - Windows 데스크톱에만 적용됩니다. |
| | 앱 식별자 | 표시된 선택에서 앱을 선택하여 앱 식별자에 추가합니다. **앱 검색**을 클릭할 수도 있습니다. |
| | 앱 설명 | 앱 설명을 입력합니다. |

# 10.10.4.65. Windows 제한

Windows 제한 사항은 Windows 10 이상 장치에서 활성화되는 기능을 결정합니다.

## Windows 제한 설정

| 범주 | 설정 항목 | 수행 작업 |
|---|---|---|
| | 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| | 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 기기 성능 | **모든 버전(Windows 10+)** | |
| | Wi-Fi 오프로딩 비활성화 | 기기가 권한이 있는 무선 네트워크의 데이터를 운반하는 호환 가능한 네트워크에 액세스하는 것을 막으려면 이 옵션을 선택합니다. |
| | 인터넷 공유 비활성화 | 기기가 다른 무선 기기로 인터넷에 액세스하는 것을 막으려면 이 옵션을 선택합니다. |
| | 위치 비활성화 | 위치 서비스를 비활성화하려면 이 옵션을 선택합니다. |
| | 휴대폰 데이터 로밍 비활성화 | 기기가 휴대폰 모드일 때 데이터 로밍을 비활성화하려면 이 옵션을 선택합니다. |
| | Bluetooth 비활성화 | 기기가 블루투스 연결을 설정하지 못하게 하려면 이 옵션을 선택합니다. |
| | 로밍 중이거나 휴대폰 네트워크에 있을 때 VPN 비활성화 | 기기가 Wi-FI를 사용하지 않을 때 VPN 연결을 설정하지 못하게 하려면 이 옵션을 선택합니다. |
| | Wi-Fi 수동 구성 비활성화 | 사용자가 장치에서 Wi-Fi 설정을 수동으로 구성하지 못하도록 하려면 선택합니다. |
| | Wi-Fi 비활성화 | WiFi 연결을 허용하거나 거부하려면 선택하세요. |
| 원격 분석<br>- 기기가 진단 및 사용량 원격 측정 데이터를 보내도록 허용합니다. | **Windows 10만 해당** | |
| | 원격 분석 수준 | 다음의 데이터 보고 원격 분석 수준에서 하나를 선택합니다.<br>• **보안** - 연결된 사용자 경험, 원격 분석 구성 요소 설정, 악성 소프트웨어 제거 도구 및 Windows Defender에 관한 정보를 전송합니다.<br>• **기본** - 품질 관련 데이터, 앱 호환성, 앱 사용 데이터, 보안 수준의 데이터를 비롯한 기본적인 기기 정보를 전송합니다.<br>• **향상** - Windows, Windows Server, System Center 및 앱의 사용 및 성능을 포함하는 자세한 정보를 제공합니다. 고급 안정성 데이터, 기본 및 보안 수준 모두의 데이터도 포함합니다.<br>• **전체(기본)** - 문제 해결을 식별하고 지원하는 모든 데이터와 보안, 기본 및 향상 수준의 데이터를 전송합니다. |
| 데이터 손실 방지(DLP) | **모든 버전(Windows 10+)** | |
| | 카메라 비활성화 | 최종 사용자가 카메라 앱을 사용하지 못하게 하려면 이 옵션을 선택합니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 스토리지(SD) 카드 액세스 비활성화 | 기기가 스토리지 카드에 액세스하지 못하게 하려면 이 옵션을 선택합니다. |
| | 화면 캡처 비활성화(데스크톱에만 해당) | 기기 내 화면 캡처 앱을 사용하여 화면을 캡처하지 못하게 하려면 선택하세요. |
| | USB 대용량 저장소 비활성화(HoloLens에만 해당) | HoloLens가 대용량 저장 장치에 액세스하지 못하도록 하려면 선택합니다. |
| 데이터 사용량 | **Windows 10+** | |
| Defender | 3G 연결 비용 | 다음 옵션 중 하나를 선택합니다.<br>• **제한 없음** - 연결에 사용 요금 및 용량 제한으로 인한 한도 및 제한이 없습니다.<br>• **고정** - 연결에 특정 데이터 제한을 초과하면 사용 요금 및 용량 제한으로 인한 제한이 있습니다.<br>• **변수** - 연결은 1바이트당 요금이 부과됩니다. |
| | 4G 연결 비용 | |
| | **Windows 10+** | |
| | Defender 실시간 모니터링 기능 비활성화 | Windows Defender 실시간 모니터링 기능을 비활성화하려면 선택합니다. |
| DeviceGuard | **Windows 10+** | |
| | 가상화 기반 보안(VBS) 비활성화 | 가상화 기반 보안이 보안 서비스 지원을 제공하지 못하게 하려면 선택합니다. |
| | 가상화 기반 보안이 있는 Credential Guard | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화됨** - 가상화 기반 보안이 있는 Credential Guard를 비활성화합니다.<br>• **UEFI 잠금을 사용하여 활성화됨** - 가상화 기반 보안이 있는 Credential Guard를 UEFI(Unified Extensible Firmware Interface) 잠금을 사용하여 활성화합니다.<br>• **잠금을 사용하지 않고 활성화됨** - 가상화 기반 보안이 있는 Credential Guard를 UEFI 잠금을 사용하지 않고 활성화합니다. |
| | 플랫폼 보안 수준(플랫폼 보안 기능 필요) | 다음 옵션 중 하나를 선택합니다.<br>• **보안 부팅 포함 VBS** - 보안 부팅을 포함한 가상화 기반 보안을 활성화하려면 이 옵션을 선택합니다.<br>• **보안 부팅 및 직접 메모리 액세스 포함 VBS** - 보안 부팅 및 직접 메모리 액세스(DMA)를 포함한 가상화 기반 보안을 활성화하려면 이 옵션을 선택합니다. |
| 개인 정보 | **Windows 10+** | |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | 광고 ID 비활성화 | 광고 ID를 비활성화하려면 선택합니다. |
| Windows 및 애플리케이션 | 앱/OS에 의한 작업 피드 게시 비활성화<br>**모든 버전(Windows 10+)** | 앱/OS이 작업 피드로 게시되지 못하게 하려면 선택합니다. |
| | 이메일 이외의 서비스에 대해 Microsoft 계정 비활성화 | 최종 사용자가 이메일 이외 서비스에 인증하는 데 Microsoft 계정을 사용하지 못하게 하려면 이 옵션을 선택합니다. |
| | Microsoft 계정 이외의 계정 비활성화 | 최종 사용자가 Microsoft 이외의 계정으로 이메일을 구성하지 못하게 하려면 이 옵션을 선택합니다. |
| | Cortana 개인 비서 비활성화 | 최종 사용자가 Microsoft의 개인 비서에 액세스하지 못하게 하려면 이 옵션을 선택합니다. |
| | 위치 기반 검색 비활성화 | 기기 위치를 활용한 검색을 막으려면 이 옵션을 선택합니다. |
| | 개발자 잠금 해제 비활성화 | 최종 사용자가 앱의 테스트용 로드를 활성화하지 못하게 하려면 이 옵션을 선택합니다. 기기가 MDM에 등록될 때 기본 모드로 테스트용 로드가 활성화됩니다. |
| | **11+ 지원 에디션만** | |
| | 작업 표시줄의 Teams 채팅 아이콘 구성<br>**Windows 10+ 지원 버전만** | 다음 옵션 중 하나를 선택합니다.<br>• **보이기:** 채팅 아이콘이 작업 표시줄에 기본적으로 나타납니다. 사용자는 설정에서 아이콘을 표시하거나 숨길 수 있습니다.<br>• **숨기기:** 채팅 아이콘이 기본적으로 숨겨집니다. 사용자는 설정에서 아이콘을 표시하거나 숨길 수 있습니다.<br>• **비활성화됨:** 채팅 아이콘이 표시되지 않으며, 사용자는 설정에서 아이콘을 표시하거나 숨길 수 없습니다.<br>• **구성되지 않음:** 채팅 아이콘이 Windows 에디션의 기본 설정에 따라 동작합니다.<br>Windows 기기를 재시작하기 전에는 변경 사항이 적용되지 않습니다. |
| | Microsoft Store에서 앱 자동 업데이트 비활성화 | 최종 사용자가 Microsoft 앱 스토어에 액세스하지 못하도록 하려면 선택합니다. |
| | Microsoft Store에서 사전 설치되거나 다운로드된 모든 앱 실행 비활성화 | Microsoft Store에서 사전 설치되거나 다운로드된 모든 앱을 최종사용자가 실행하지 못하도록 하려면 선택합니다.<br>Enterprise 및 Education Windows 에디션에서만 지원됩니다. |
| | 앱의 백그라운드 실행 허용 | 다음 옵션 중 하나를 선택합니다. |

| 범주 | 설정 항목 | 수행 작업 |
| --- | --- | --- |
| | | • **관리 중인 사용자**: 사용자는 배경에서 실행되고 있는 앱을 제어할 수 있습니다.<br>• **강제 허용**: 배경에서 앱들이 실행될 수 있습니다.<br>• **강제 거부**: 배경에서 앱들이 실행되지 않도록 할 수 있습니다. |
| 기타 제한 | **모든 버전(Windows 10+)**<br><br>UEM에서의 등록 취소 기능을 비활성화하고 작업 공간 계정 삭제<br><br>사용자가 장치 잠금 유예 기간을 설정할 수 없도록 설정합니다(HoloLens에만 해당). | <br><br>최종 사용자가 UEM에서 등록을 취소하고 기업 계정 이미지를 삭제하지 못하도록 하려면 이 옵션을 선택합니다.<br><br>사용자가 장치 잠금 유예 기간을 설정하지 못하도록 하려면 선택합니다. |
| | **Windows 10+ 지원 버전만** | |
| | 제어판과 하드웨어 키 조합을 사용하여 사용자가 기기를 공장 초기화하도록 비활성화<br><br>기기 설정 중에 사용자가 네트워크에 연결해야 함(Autopilot 프로필 필요) | 사용자가 기기 잠금 유예 기간을 설정할 수 없도록 하려면 이 옵션을 선택합니다.<br><br>TenantLockdown을 통해 Autopilot 기능을 사용하여 등록되는 모든 Windows 기기를 잠그도록 하려면 이 옵션을 선택하십시오. |
| | **Windows 11+ 지원되는 버전만** | |
| | 사용자가 사용자 인터페이스를 통해 eSIM을 변경할 수 없도록 합니다. | 이 옵션을 선택하면 사용자의 eSIM 프로필 변경이 제한됩니다. |

# 10.10.4.66. Windows 데스크톱 제한

**적용 가능 운영 체제: Windows 10 데스크톱**

이 섹션에는 다음 주제가 포함됩니다.

- Windows 데스크톱 제한 구성
- 제거 가능한 스토리지 기기의 허용 목록 생성

관리자는 다음으로의 사용자 액세스를 제한하여 관리되는 Windows 10 데스크톱 기기의 OS 정보를 제어할 수 있습니다.

- 제어 패널
- 작업 관리자
- 파일 탐색기
- 레지스트리 편집기

위의 기능을 사용하는 경우 사용자가 기기를 크게 변경할 수 있습니다. 이 기능을 사용하여 관리자는 이러한 시스템 수준 제어로의 액세스를 제한하고 보안할 수 있습니다.

이 기능을 사용하려면 Bridge가 필요합니다. 자세한 내용은 Ivanti Bridge를 참조하십시오.

## Windows 데스크톱 제한 구성

**절차**

1. **구성 > +추가**로 이동합니다.
2. **Windows 데스크톱 제한** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 표에 설명된 바와 같이 남은 설정을 지정합니다.

| 설정 항목 | 수행 작업 |
|---|---|
| **작업 관리자** | 액세스를 거부하고자 하는 설정의 **액세스 거부** 체크박스를 선택합니다. |
| **제어 패널** | |
| **레지스트리 편집기** | |
| **파일 탐색기** | **기능 제한** 체크박스를 선택하여 파일 탐색기의 기능을 제한합니다. 예: 네트워크 드라이브 매핑 제거<br>제공된 링크를 클릭하면 제한되어 있는 기능 목록을 볼 수 있습니다. |
| **제거 가능한 스토리지** | |
| 제거 가능한 스토리지에 대한 액세스 모드 | • **읽기 액세스 제한**: 모든 액세스를 방지하며 가장 제한이 큰 구성입니다.<br>• **쓰기 액세스 제한**: 제한적인 액세스를 허용하지만 인가되지 않은 데이터 삭제 또는 기기에 바이러스를 추가하는 기능 등을 방지합니다. |

6. **다음**을 클릭하세요.

7. 다음 배포 옵션 중 하나를 선택합니다.
- 모든 기기
- 배포 안 함(기본값)
- 사용자 지정
8. **완료**를 클릭하세요.

> 구성이 완전한 효과를 발휘하려면 구성 적용 후 기기를 재부팅 해야 합니다.

## 제거 가능한 스토리지 기기의 허용 목록 생성

허가된 스토리지 기기의 허용 목록을 생성하려면 먼저 다음 단계를 완료하십시오.

- PC에 허용하고자 하는 USB 스토리지 기기를 연결합니다.
- 기기 관리자를 열고 USB 컨트롤러를 클릭합니다.
- 기기 정보의 각 컨트롤러 설정을 확인합니다.
- 허용 목록을 생성할 때 사용할 수 있도록 기기 정보를 저장합니다.

제거 가능한 스토리지 기기의 허용 목록 생성 방법:

**절차**

1. **Windows 데스크톱 제한** 구성 페이지의 **허용 목록에 있는 제거 가능한 스토리지** 섹션에서 **+추가**를 클릭합니다.
2. **하드웨어 ID 추가** 창에서 허용 목록에서 제거하고 저장 기기로서 차단하려는 하나 이상의 기기에 대한 하드웨어 ID를 입력합니다.
3. **하드웨어 ID 추가**를 클릭합니다. **허용 목록에 있는 제거 가능한 스토리지** 섹션에 허용 목록에 있는 하드웨어 ID 목록이 표시됩니다.

> 목록에서 하드웨어 ID를 편집하거나 삭제하려면 **작업** 열의 편집 또는 삭제 옵션을 선택합니다.
>
> 구성이 완전한 효과를 발휘하려면 구성 적용 후 기기를 재부팅 해야 합니다.

# 10.10.4.67. Windows 10 데스크톱 설정

Windows 10 데스크톱 설정을 통해 데스크톱 설정을 사용자 지정하고 이를 Windows 10 기기로 푸시할 수 있습니다. 이 구성을 사용하여 다음 데스크톱 설정을 구성할 수 있습니다.

- 데스크톱 배경화면 이미지
- 잠금 화면 이미지
- 사용자 지정 화면 보호기 업로드
- 데스크톱 바로가기

> 이 기능을 사용하려면 Bridge가 필요합니다. 자세한 내용은 **Ivanti Bridge**를 참조하십시오.

**절차**

1. **구성**에서 **+추가**를 클릭합니다.
2. **Windows 10 데스크톱 설정** 구성을 선택합니다.**Windows 10 데스크톱 설정** 창이 표시됩니다.
3. **이름** 필드에 적절한 설정 이름을 입력합니다.
4. **+설명 추가** 링크를 클릭하여 구성에 대한 설명을 추가합니다(선택 사항).
5. **구성 설정** 섹션에서 다음 설정을 구성합니다.

| 설정 | 설명 |
| --- | --- |
| 파일 전달 | 데스크톱 설정에 대해 다음 파일 전송 옵션 중 하나를 선택합니다.<br>• **파일 업로드** - MDM용 Ivanti Neurons에 설정을 업로드합니다.<br>• **오버라이드 URL** - 다운로드할 설정 파일과 함께 오버라이드 URL을 제공합니다. |
| 데스크톱 배경화면 설정 | **파일 선택**을 클릭하여 배경화면 이미지를 찾아 업로드합니다. 지원되는 파일 형식은 BMP, JPG, JPEG, PNG입니다. |
| 잠금 화면 배경화면 설정<br>(잠금 화면 배경화면 설정은 Windows 10 Pro 기기에서 지원되지 **않음**) | **파일 선택**을 클릭하여 배경화면 이미지의 위치를 확인하고 업로드합니다.<br>지원 파일 형식은 BMP, JPG, JPEG, PNG. |
| 화면 보호기 설정 | **파일 선택**을 클릭하여 화면 보호기 파일을 찾아 업로드합니다.<br>Windows 호환 .SCR 파일만 업로드합니다.<br>화면 보호기 모드의 잠금을 해제하기 위해 비밀번호를 설정하려면 **화면 보호기에 대한 비밀번호 보호**를 선택합니다.<br>**화면 보호기 시간 초과** 시간(분)을 선택합니다. |
| 데스크톱 바로가기 | **바로가기 추가**를 클릭하여 기기 데스크톱에 추가할 데스크톱 바로가기를 설정합니다. **바로가기 추가** 창이 표시됩니다. 다음 옵션을 사용하여 표를 채웁니다.<br>• **위치** - Windows 기기에서 바로가기가 표시될 위치를 입력합니다.<br>• **대상 경로** – 로컬 경로 또는 UNC나 바로 가기가 이끄는 구동장치 표시 글자를 입력합니다. 대상 경로는 URL이 될 수도 있습니다.<br>• **인수** - 대상 파일을 열 때 사용될 인수를 입력합니다.<br>• **작업 디렉토리** - 대상에 필요한 파일이 담긴 폴더 경로를 입력합니다.<br>• **아이콘 파일** - 유효한 Windows .ico 파일을 업로드합니다.<br>옵션을 구성한 후 **바로가기 추가**를 클릭합니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정
8. **완료**를 클릭하세요.

# 10.10.4.68. Windows Hello for Business 구성

이 구성을 통해 관리자는 기기에 Windows Hello를 설정할 수 있습니다. Windows Hello를 설정하려면 기기에 로그인할 PIN을 설정해야 합니다.

적용 가능 운영 체제: Windows 10

**Procedure절차**

1. 구성 > +추가로 이동합니다.
2. 검색 필드에 Windows를 입력한 다음, Windows Hello for Business 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. Windows 10 기기에 대한 Windows Hello for Business 활성화/비활성화를 켜짐으로 토글합니다.

> 토글은 기본적으로 켜짐으로 설정되어 있습니다. Windows Hello for Business를 비활성화해도 기기에서 PIN이 제거되지 않습니다.

5. PIN 복잡도를 설정합니다.
6. 필요한 구성을 선택합니다.
    - Windows Hello for Business를 위한 TPM(신뢰 플랫폼 모듈) 필요
    - Windows Hello for Business 인증서를 스마트 카드 인증서로 사용
    - 얼굴 및 지문과 같은 생체 표시를 Windows Hello for Business에 대한 PIN 표시의 대안으로 사용
    - Windows Hello 안면 인증 시 얼굴 특징 인식에 강화된 스푸핑 방지 기능 필요
    - 동적 잠금
    - 사용자가 FIDO2 보안 키로 로그인할 수 있습니다.
7. 다음을 클릭하세요.
8. 이 구성 활성화 옵션을 선택합니다.
9. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
10. 완료를 클릭하세요.

# 10.10.4.69. Windows AI Management 구성

MDM용 Ivanti Neurons 에서는 관리자가 Windows AI 설정 및 구성을 관리할 수 있습니다. Windows AI Management는 강력한 AI 도우미의 도움으로 창의성과 생산성을 향상할 수 있습니다. **Windows AI 관리** 구성을 사용하여 등록된 Windows 기기의 Windows AI 기능을 관리합니다. 이 구성을 통해 관리자는 Windows AI 구성 서비스 공급자(CSP) 정책을 사용하여 Microsoft Copilot, Windows Recall 및 Microsoft Paint AI 기능을 제어할 수 있습니다.

관리자는 선택한 AI 기능을 비활성화하고, Copilot 기능에 대한 액세스를 제거하고, Windows Recall 동작을 제어하고, Microsoft Paint의 AI 기반 이미지 생성 기능을 관리할 수 있습니다.

**적용 대상**: Windows 10+

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **Windows AI Management** 구성을 검색하고 선택합니다.
3. 구성의 **이름** 및 **설명**을 입력합니다.
4. **구성 설정** 섹션에서 다음 옵션 중에 선택합니다. ### Copilot 설정

| 설정 | 설명 |
|---|---|
| Windows Copilot 비활성화 | 사용자가 Windows Copilot에 액세스하지 못하도록 합니다. |
| Copilot 하드웨어 키 비활성화 | 지원되는 기기에서 전용 Copilot 하드웨어 키를 비활성화합니다. |
| Microsoft Copilot 앱 제거 | 기기에서 Microsoft Copilot 애플리케이션을 제거합니다. |

## Recall 설정

| 설정 | 설명 |
|---|---|
| AI 데이터 분석 비활성화 | Windows Recall에서 사용하는 AI 기반 데이터 분석을 비활성화합니다. |
| Recall 스냅샷의 최대 저장 공간 설정(GB) | Windows Recall에서 스냅샷을 저장하는 데 사용할 수 있는 최대 저장 공간을 지정합니다. |

## Paint AI 설정

| 설정 | 설명 |
|---|---|
| Image Creator 비활성화 | Microsoft Paint의 Image Creator 기능을 비활성화합니다. |
| Cocreator 비활성화 | Microsoft Paint의 Cocreator 기능을 비활성화합니다. |
| 생성형 채우기 비활성화 | Microsoft Paint의 생성형 채우기 기능을 비활성화합니다. |

**Microsoft**는 이 구성에서 사용하는 **TurnOffWindowsCopilot** 정책을 더 이상 추천하지 않습니다. 그 결과 이 구성은 더 이상 기기에 설치된 Copilot 앱에 영향을 미치지 않습니다.

**Windows Copilot 비활성화** 확인란을 선택하지 않으면 구성이 장치의 이전 구성 선택을 재정의하여 Windows AI Management를 활성화합니다.

5. **다음**을 클릭해 배포 설정을 구성합니다.
6. 배포 옵션 중 하나를 선택하여 **Windows AI Management** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
7. **완료**를 클릭하세요.

# 10.10.4.70. Play Integrity(구 SafetyNet Attestation)

Play Integrity(구 SafetyNet)는 Google의 Play Integrity API를 사용하여 Android 기기의 보안 및 호환성을 평가하는 데 도움이 됩니다. 이 기능을 설정하면, 일정 시간 간격마다 장치를 분석하여 장치가 조작되었는지 여부를 확인할 수 있습니다.

> 이제 모든 Android 버전에서 Play Integrity를 지원합니다.

**절차**

1. **구성** 탭에서 **+추가**를 클릭합니다.
2. **Play Integrity** 구성을 선택합니다.**Play Integrity 구성** 페이지가 표시됩니다.
3. Play Integrity 구성의 **이름** 필드에 적절한 이름을 입력합니다.
4. **+설명 추가** 링크를 클릭하여 구성에 대한 설명을 추가합니다. 이 필드는 선택 사항입니다
5. **구성 설정** 섹션에 최소 시간 간격(단위: 시간)을 입력합니다. 이 값은 장치의 보안 및 호환성 검사 평가에 적용됩니다. 값은 1~24로 지정해야 합니다.
6. **다음**을 클릭하고 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정

**완료**를 클릭하세요.

> Play Integrity 및 SafetyNet nonce가 장치로 전송되는 경우 Play Integrity nonce가 SafetyNet nonce보다 우선 순위로 지정됩니다.

# 10.10.4.71. 고급 Android 암호 및 잠금 화면

Couldn't convert your doc.

# 10.10.4.72. 엔드포인트용 Microsoft Defender

이전에 Windows Advanced Threat Protection으로 알려진 MDE(Microsoft Defender for Endpoint) 구성을 통해 고객은 기기를 MDE 서비스에 온보딩 및 오프보딩할 수 있습니다.

**절차**

1. **구성 > +추가**로 이동합니다.
2. **엔드포인트용 Microsoft Defender**를 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 표에 설명된 바와 같이 남은 설정을 지정합니다.

| 설정 | 설명 |
| --- | --- |
| **온보딩 또는 오프보딩 Blob** | 엔드포인트용 Microsoft Defender Security Center 사이트에서 온보딩 또는 오프보딩 Blob을 붙여넣습니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.

- 모든 기기
- 배포 안 함(기본값)
- 사용자 지정

8. **완료**를 클릭하세요.

# 10.10.4.73. 인증서 기반 인증

MDM용 Ivanti Neurons은(는) 관리자가 디지털 인증서와 테넌트 지정(베니티) 호스트 이름을 사용하여 로그인할 수 있도록 하는 인증서 기반 인증을 지원합니다. 활성화 및 구성될 때 관리자는 기본 인증(사용자 이름과 비밀번호) 대신 디지털 인증서를 사용하여 로그인할 수 있습니다.

> 이 기능은 기본으로 비활성화되었습니다. 관리자는 지원팀에 문의하여 테넌트에서 이 기능을 활성화해야 합니다. 이 기능은 지원팀이 활성화하는 경우 NA3 클러스터 환경에서만 이용할 수 있습니다. 슈퍼 관리자 사용자 이름 및 비밀번호를 테스트하여 준비했는지 확인해 주십시오. 왜냐하면 일단 인증서 기반 인증이 활성화되면 이는 베니티 도메인을 성공적으로 구성할 때까지 로그인하기 위해 사용할 수 있는 유일한 자격 증명이기 때문입니다.

**절차**

1. **관리** 탭에서 **Vanity 호스트 구성**을 선택합니다.
2. 베니티 호스트 구성 페이지에서 다음 옵션을 구성합니다.
3. **저장**을 클릭하세요.
   베니티 호스트가 액세스할 수 있으려면 수 분이 소요될 수 있습니다.

| 설정 | 설정하기 |
| --- | --- |
| 베니티 도메인 만들기 | 베니티 도메인 이름을 입력합니다. 이는 기업의 CI(Corporate Identity)에 더 잘 어울리고 디지털 인증서를 사용해 로그인할 수 있는 도메인 이름입니다. |
| 신뢰할 수 있는 발급 CA 인증서 업로드 | 관리자에게 인증서를 발행하는 CA 인증서를 선택하여 업로드하려면 **파일 선택**을 클릭합니다.<br>인증서 해지 확인을 활성화하려면 **이 인증서에 대한 인증서 상태 검증 설정 활성화**를 선택합니다(선택 사항).<br>이 옵션은 기본적으로 활성화되어 있습니다. 인증서 해지를 비활성화하려면 이 옵션을 선택 취소합니다.<br>더 많은 인증서를 추가하려면 **더 추가**를 클릭합니다.<br>인증서 형식이 .p7b, .pem, .der, .crt 또는 .cer인지 확인하십시오. |
| 인증서 속성 매핑 | 인증서 속성 매핑은 관리자의 계정 속성에 인증서 ID 요소의 매핑을 구성합니다.<br>**인증서** 필드에서 다음 인증서 요소 중 하나를 선택합니다.<br>• **NTPrincipalName**<br>• **RFC 822 이름**<br>**변수** 필드에서 관리자의 다음 계정 속성 중 하나를 선택합니다.<br>• **UserUPN**<br>• **$UserEmailAddress**<br>• **$EDIPI** |

# 10.10.5. 사용자 리소스 구성

이 섹션에는 다음 주제가 포함됩니다.

- CalDAV 설정
- CardDAV 설정
- Google 구성
- 이메일 설정
- Exchange 구성
- 폰트 설정
- 구독한 달력 설정
- 웹 클립 구성 만들기
- Office 365 설치
- Windows GPO 설정
- BitLocker 암호화 구성

# 10.10.5.1. CalDAV 설정

CalDAV 인터넷 표준으로 웹 달력을 사용하는 데 필요한 CalDAV 설정을 할 수 있습니다.

## CalDAV 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 호스트 이름 및 포트 | 해당 달력 서버의 호스트 이름과 포트를 입력할 수 있습니다. |
| 기본 URL | 달력 서비스를 이용할 URL을 입력할 수 있습니다. |
| 사용자 | 접속 시 사용할 사용자 이름을 입력할 수 있습니다. |
| 비밀번호 | 접속 시 사용할 비밀번호를 입력할 수 있습니다. |
| SSL 사용 | 장치와 서버 간 통신에 보안 소켓 레이어만 사용하도록 설정할 수 있습니다. |
| 퍼앱 VPN | **전제 조건**: CalDAV 구성에서 퍼앱 VPN을 구성하기 전에 Tunnel 또는 퍼앱 VPN 구성을 설정하십시오.<br>드롭다운 메뉴에서 사전 구성된 퍼앱 VPN 구성을 선택하십시오.<br>**적용 가능 운영 체제**: iOS 14+ |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.5.2. CardDAV 설정

CardDAV 인터넷 표준으로 웹 주소록을 사용할 수 있는 CardDAV 설정을 할 수 있습니다.

## CardDAV 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 호스트 이름 및 포트 | 해당 주소록 서버에 사용할 호스트 이름과 포트를 입력할 수 있습니다. |
| 기본 URL | 주소록 서비스를 이용할 URL을 입력할 수 있습니다. |
| 사용자 이름 | 접속 시 사용할 사용자 이름을 입력할 수 있습니다. |
| 비밀번호 | 접속 시 사용할 비밀번호를 입력할 수 있습니다. |
| SSL 사용 | 장치와 서버 간 통신에 보안 소켓 레이어만 사용하도록 설정할 수 있습니다. |
| 퍼앱 VPN<br><br><br><br>**iOS 10+** | **전제 조건**: CardDAV 구성에서 퍼앱 VPN을 구성하기 전에 Tunnel 또는 퍼앱 VPN 구성을 설정하십시오.<br>드롭다운 메뉴에서 사전 구성된 퍼앱 VPN 구성을 선택하십시오.<br>**적용 가능 운영 체제**: iOS 14+ |
| 통신 서비스 규칙 | CardDAV 시스템에서 연락처에 음성 전화를 거는 데 사용하는 기본 앱을 선택합니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.5.3. Google 구성

Google 계정 구성은 iOS 9.3.2와 visionOS 1.1 또는 Android 6.0 이상 기기 또는 지원되는 최신 버전을 Google 계정에 연결합니다. Google 계정에는 Android 엔터프라이즈가 필요합니다. 이 구성은 여러 개의 Google 이메일 주소와 사용자가 인증 후 활성화하는 다른 Google 서비스를 설정할 수 있습니다.

**절차**

1. **구성 > +추가**로 이동합니다.
2. **Google 계정** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 표에 설명된 바와 같이 남은 설정을 지정합니다.

| 설정 항목 | 수행 작업 |
|---|---|
| **iOS 9.3.2+ , Android 6.0+** | |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 계정 설명 | 계정의 표시 이름을 입력합니다. |
| 계정 이름 | 계정의 사용자 이름 전체를 입력합니다. |
| 이메일 주소 | 계정의 Google 이메일 주소를 입력합니다. |
| 퍼앱 VPN | **전제 조건**: Google 계정 구성에서 퍼앱 VPN을 구성하기 전에 Tunnel 또는 퍼앱 VPN 구성을 설정하십시오. 드롭다운 메뉴에서 사전 구성된 퍼앱 VPN 구성을 선택하십시오.<br>**적용 가능 운영 체제**: iOS 14+ |
| **iOS 10+** | |
| **통신 서비스 규칙** | 다음 옵션 중 어느 것이든 선택하여 Google 시스템에서 연락처에 음성 전화를 거는 데 사용하는 기본 앱을 선택합니다.<br>• **App Catalog 및 시스템 앱에서**: 앱 이름의 첫 번째 몇 글자를 입력하여 앱을 검색합니다.<br>• **번들 ID 입력(Apple 시스템 앱만 해당)**: 시스템 앱 번들 ID를 입력합니다. 번들 ID는 'com.apple'로 시작해야 합니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.

- 모든 기기
- 배포 안 함(기본값)
- 사용자 지정

8. **완료**를 클릭하세요.

기기에 Google 계정 구성이 적용되면 Go 클라이언트가 사용자에게 Google에 로그인하라는 메시지를 표시합니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.5.4. 이메일 설정

장치에 POP 또는 IMAP 이메일 설정을 할 수 있습니다.

## 이메일 설정

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 계정 설명 | 현재 이메일의 고유 정보를 입력할 수 있습니다. |
| 계정 유형 | IMAP와 POP 중 원하는 계정 유형을 선택할 수 있습니다. IMAP를 선택하면 경로 접두어도 입력할 수 있습니다. 지원되는 계정 유형은 인터넷 서비스 제공업체(ISP)에서 확인 가능합니다. 일반적으로 접두어는 모든 IMAP 폴더 목록이 받은편지함에 위치할 때 필요합니다. 접두어가 필요한 ISP는 보통 설정할 접두어 정보를 알려줍니다. |
| 사용자 표시 이름 | 이메일 계정 사용자의 고유 이름을 입력할 수 있습니다. 이 항목은 사용자가 직접 장치에서 설정할 수도 있습니다. |
| 이메일 주소 | 변수를 입력해 계정 이메일 주소를 지정할 수 있습니다. |
| 이동 허용 | 현재 계정에서의 이메일 이동이 차단되지 않도록 설정할 수 있습니다. |
| S/MIME 활성화 | S/MIME 암호화 지원 기능을 켤 수 있습니다. 그리고 서명 및 암호화 인증서를 선택할 수 있습니다.<br>인증서 캐싱이 필요합니다. ID 인증서 구성에서 사용하는 인증서 권한에 캐싱이 활성화되었는지 확인하십시오.<br>**iOS 10.3+:**<br>**S/MIME 서명** 및 **S/MIME 암호화** 필드에 대해 다음 옵션 중 하나를 선택합니다.<br>• 끄기<br>• 켜기<br>• 사용자가 선택<br>**iOS 12.0+:**<br>• 사용자가 S/MIME 서명 설정을 재정의하도록 활성화<br>• 사용자가 S/MIME 서명 ID를 선택하도록 활성화<br>• 사용자가 S/MIME 암호화 설정을 재정의하도록 활성화<br>• 사용자가 S/MIME 암호화 ID를 선택하도록 활성화<br>필요 시 **S/MIME 메시지별 서명 및 암호화를 활성화**합니다. |
| 메일 드롭 허용 | 이 계정에 대한 메일 드롭을 허용하도록 선택합니다. 메일 드롭을 통해 사용자는 첨부파일을 iCloud에 저장하고 이메일로 링크를 전송하여 대용량 첨부파일이 있는 이메일을 발송할 수 있습니다. 메일 드롭에 대한 자세한 내용은 다음 사이트를 참조하십시오. https://support.apple.com/ |
| 퍼앱 VPN | 메일 도메인에서 다수의 퍼앱 VPN 프로필을 연결하는 기능은 Apple에서 지원됩니다. 이제는 퍼앱 VPN에서 IMAP 및 POP3 이메일 구성이 지원됩니다.<br>**전제 조건**: 이메일 구성에서 퍼앱 VPN을 구성하기 전에 Tunnel 또는 퍼앱 VPN 구성을 설정하십시오.<br>드롭다운 메뉴에서 **퍼앱 VPN 구성 선택**을 선택합니다. |

## 수신 메일

| 설정 항목 | 수행 작업 |
| --- | --- |
| 메일 서버 및 포트 | 이 주소는 인터넷 서비스 제공업체(ISP)에서 확인 가능합니다. |
| 사용자 이름 | 수신 메일 서버 접속에 사용할 사용자 이름을 입력할 수 있습니다. 보통 이메일 주소와 동일합니다. 해당 형식은 ISP에서 지정합니다. |
| 인증 유형 | ISP에서 지정한 인증 유형을 선택할 수 있습니다. |
| 비밀번호 | 수신 메일 서버 접속에 사용할 비밀번호를 입력할 수 있습니다. |
| SSL 사용 | 장치와 서버 간 통신에 보안 소켓 레이어만 사용하도록 설정할 수 있습니다. |

## 송신 메일

| 설정 항목 | 수행 작업 |
| --- | --- |
| 메일 서버 및 포트 | 이 주소는 인터넷 서비스 제공업체(ISP)에서 확인 가능합니다. |
| 사용자 이름 | 송신 이메일 서버 접속에 사용할 사용자 이름을 입력할 수 있습니다. 보통 이메일 주소와 동일합니다. 해당 형식은 ISP에서 지정합니다. |
| 인증 유형 | ISP에서 지정한 인증 유형을 선택할 수 있습니다. |
| 비밀번호 | 송신 이메일 서버 접속에 사용할 비밀번호를 입력할 수 있습니다. |
| 수신과 동일한 송신 비밀번호 | SMTP 인증에 POP/IMAP와 동일한 비밀번호가 사용될 경우 해당 항목을 선택합니다. |
| 메일에서만 사용 | 현재 구성을 이메일 클라이언트만 사용하도록 설정할 수 있습니다. 이메일을 보내는 다른 앱(예: 네이티브 이메일 클라이언트를 이용해 컨텐츠를 보내는 앱)은 이 구성을 사용할 수 없습니다. |
| SSL 사용 | 장치와 서버 간 통신에 보안 소켓 레이어만 사용하도록 설정할 수 있습니다. |

# 10.10.5.5. Exchange 구성

Exchange 구성은 Android, iOS 및 visionOS 기기에 ActiveSync 기반 이메일을 설정하고 macOS 기기에 Exchange Web Services(EWS) 기반 이메일을 설정합니다.

> Exchange 구성은 Android 9에서 Samsung에 의해 더 이상 사용되지 않습니다. Android 9 이상 버전의 Samsung 장치의 경우 장치 관리 모드에서 Exchange 구성이 지원되지 않습니다.

## Exchange 설정

| 설정 | 설정 방법 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| Exchange 호스트 | 사용자가 Sentry를 사용하여 이메일 액세스를 제어하는 경우 Sentry 서버 호스트 이름을 입력합니다. 그렇지 않은 경우, ActiveSync 서버 주소를 입력합니다.* |
| 이동 허용 | **iOS 및 Android:** 이 계정에서 이메일 이동이 차단되지 않게 하려면 선택합니다.<br>**Windows 10의 경우:** 해당 없음. |
| S/MIME 활성화 | S/MIME 암호화 지원 기능을 켤 수 있습니다. 그리고 서명 및 암호화 인증서를 선택할 수 있습니다.<br>인증서 캐싱이 필요합니다. ID 인증서 구성에서 사용하는 인증서 권한에 캐싱이 활성화되었는지 확인하십시오.<br>**iOS 10.3+:**<br>**S/MIME 서명** 및 **S/MIME 암호화** 필드에 대해 다음 옵션 중 하나를 선택합니다.<br>• 끄기<br>• 켜기<br>• 사용자가 선택<br>**iOS 12.0+:**<br>• 사용자가 S/MIME 서명 설정을 재정의하도록 활성화<br>• 사용자가 S/MIME 서명 ID를 선택하도록 활성화<br>• 사용자가 S/MIME 암호화 설정을 재정의하도록 활성화<br>• 사용자가 S/MIME 암호화 ID를 선택하도록 활성화<br>필요 시 **S/MIME 메시지별 서명 및 암호화를 활성화**합니다. |
| 최근 이메일 주소 동기화 | 기기와 서버 간 최근 서로 접속한 이메일 주소가 동기화되도록 설정할 수 있습니다. |
| 메일에서만 사용 | 현재 구성을 이메일 클라이언트만 사용하도록 설정할 수 있습니다. 이메일을 보내는 다른 앱(예: 네이티브 이메일 클라이언트를 이용해 컨텐츠를 보내는 앱)은 이 구성을 사용할 수 없습니다. |
| SSL 사용 | 장치와 서버 간 통신에 보안 소켓 레이어만 사용하도록 설정할 수 있습니다. |
| 교환 페이로드를 위해 OAuth 활성화 | iOS 12.0+ 및 macOS 10.14+:<br>OAuth를 사용하여 인증을 사용 가능하도록 설정합니다.<br>이 옵션이 활성화되면 OAuth를 사용한 인증을 지원하는 이메일 앱에 대해 다음과 같은 추가 설정을 사용할 수 있습니다.<br>• OAuth 로그인 URL<br>• OAuth 토큰 요청 URL |
| 도메인 | 현재 이메일 계정의 도메인을 입력해 해당 사용자가 도메인을 입력하지 않도록 설정할 수 있습니다. |
| 사용자 | 이 계정의 이메일 주소를 나타내는 변수를 입력하십시오.* |
| 계정 비밀번호 | 현재 계정의 비밀번호를 입력해 해당 사용자가 비밀번호를 입력하지 않도록 설정할 수 있습니다. |
| 이메일 주소 | 이 계정의 이메일 주소를 나타내는 변수를 입력하십시오.* |

| 설정 | 설정 방법 |
| --- | --- |
| 동기화할 메일의 이전 일 수 | 기기와 서버 간 이메일을 동기화할 기준 기간을 선택할 수 있습니다. |
| 퍼앱 VPN | **전제 조건**: Exchange Active Sync 구성에서 퍼앱 VPN을 구성하기 전에 Tunnel 또는 퍼앱 VPN 구성을 설정하십시오.<br>드롭다운 메뉴에서 사전 구성된 퍼앱 VPN 구성을 선택하십시오.<br>**적용 가능 운영 체제**: iOS 14+ |
| **Android 및 Windows** | |
| 달력 동기화 | **Android 및 Windows 10의 경우:** 기기와 서버 간에 일정 항목을 동기화하려면 선택합니다.<br>**Samsung 기기의 경우:** 이 설정은 사용되지 않습니다(기본값으로 ON 상태).<br>**Android Email+ 앱의 경우:** 이 설정이 사용됩니다. |
| 연락처 동기화 | **Android 및 Windows 10의 경우:** 기기와 서버 간에 연락처를 동기화하려면 선택합니다.<br>**Samsung 기기의 경우:** 이 설정은 사용되지 않습니다(기본값으로 ON 상태).<br>**Android Email+ 앱의 경우:** 이 설정이 사용됩니다. |
| 이메일 동기화 | **Android 및 Windows 10의 경우:** 기기와 서버 간에 이메일을 동기화하려면 선택합니다.<br>**Samsung 기기의 경우:** 이 설정은 사용되지 않습니다(기본값으로 ON 상태).<br>**Android Email+ 앱의 경우:** 이 설정은 사용되지 않습니다(기본값으로 ON 상태). |
| 작업 동기화 | **Android 및 Windows 10의 경우:** 기기와 서버 간에 작업을 동기화하려면 선택합니다.<br>**Samsung 기기의 경우:** 이 설정은 사용되지 않습니다(기본값으로 ON 상태).<br>**Android Email+ 앱의 경우:** 적용되지 않습니다. |
| **iOS 13.0+** | |
| • 달력 동기화<br>• 연락처 동기화<br>• 메일 동기화<br>• 메모 동기화<br>• 알림 동기화 | 캘린더, 연락처, 메일, 메모, 알림 등의 Outlook Exchange 항목을 개별적으로 동기화하도록 지정합니다.<br>각 항목에 대해 **활성화** 및 **사용자 재정의 허용** 옵션을 선택 또는 선택 취소합니다.<br>이들 항목 중 적어도 하나에 대해 동기화를 활성화해야 합니다. 옵션 중 하나에 대해 동기화를 비활성화했지만 사용자가 재정의할 수 있게 허용한 경우 사용자는 계속해서 해당 기능을 활성화할 수 있습니다. |
| ID 인증서<br><br>**안드로이드**<br><br>인증서 기반 인증만 사용 | 목록에서 ID 인증서를 선택해 기기가 인증서로 서버에 인증되도록 설정할 수 있습니다. ID 인증서 구성으로 설정되어 있는 경우에 한해 해당 목록에 인증서가 표시됩니다.<br><br>선택된 ID 인증서만 Exchange 서버에 대한 인증 수단으로 사용할 수 있습니다. |
| 모든 SSL 인증서 허용 | Android 기기가 모든 SSL 인증서를 허용하도록 설정할 수 있습니다. 이 설정은 Android Email+ 및 Samsung Knox Email에 적용됩니다.<br>• 이 기능 설정 시 기기 사용자들이 자신도 모르게 사용 기기를 공격에 노출시킬 수 있으므로 주의하시기 바랍니다.<br>• Sentry 인증서가 자체 서명 인증서 또는 알 수 없는 인증서인 경우 이 옵션을 활성화해야 합니다. |

| 설정 | 설정 방법 |
| --- | --- |
| Exchange 앱 우선 순위<br><br>**iOS 10+**<br><br>통신 서비스 규칙<br><br>**Windows 10+만**<br><br>Outlook 구성 | Android 기기에 기본으로 설정될 이메일 클라이언트를 선택할 수 있습니다(Android Email+ 및 Samsung Email).<br>Email+ 앱은 Exchange 앱 우선순위를 활성화한 모든 테넌트의 App Catalog에 추가됩니다.<br><br>CardDAV 시스템에서 연락처에 음성 전화를 거는 데 사용하는 기본 앱을 선택합니다.<br><br>Microsoft Outlook을 기기에 구성하려면 이 옵션을 선택합니다.<br>이 옵션은 Bridge가 활성화되어 있을 경우에만 지원됩니다. |

*$를 입력하면 현재 칸에 해당하는 지원 변수 목록을 확인할 수 있습니다.

# 10.10.5.6. 폰트 설정

폰트 설정을 하면 iOS 7 기기에 TrueType 또는 OpenType 폰트 파일을 추가로 제공할 수 있습니다. 다음 표에 글꼴 설정 설명이 제공됩니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 글꼴 업로드 | 글꼴 파일을 점선 박스로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다. 지원되는 폰트 파일은 .otf 또는 .ttf 형식 파일입니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.5.7. 구독한 달력 설정

공용 웹 달력을 이용하는 데 필요한 설정을 할 수 있습니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| URL | 달력 이용을 위한 URL을 입력합니다.* |
| 사용자 | 접속 시 사용할 사용자 이름을 입력할 수 있습니다.* |
| 비밀번호 | 접속 시 사용할 비밀번호를 입력할 수 있습니다. |
| SSL 사용 | 장치와 서버 간 통신에 보안 소켓 레이어만 사용하도록 설정할 수 있습니다. |

$를 입력하면 현재 필드에 해당하는 지원 변수 목록을 확인할 수 있습니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.5.8. 웹 클립 구성 만들기

웹 클립은 iOS 기기에서 웹사이트나 웹 페이지로 접속하는 바로가기 아이콘입니다. 웹 클립 설정을 통해 기기에 표준 웹 클립을 생성할 수 있습니다. iOS 장치에 특정 웹 사이트를 실행하는 웹 클립 아이콘을 추가할 수 있습니다. 웹 클립을 사용하면 장치의 홈 화면에서 북마크를 빠르게 찾고 사용할 수 있습니다. 사이트의 Mobile Safari 보기 환경의 일부 매개 변수를 제어할 수도 있습니다.

> 이 구성에는 사용자 지정 배포 옵션을 사용한 위임을 사용할 수 있습니다. 자세한 정보는 구성 작업에서 *구성 배포* 항목을 참조하십시오.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**을 클릭합니다.
3. **+추가**를 클릭합니다.
4. 웹 클립 구성을 검색하고 선택합니다.
5. 이 페이지에서 설정을 구성합니다. 값에 대한 안내는 **웹 클립 구성 설정** 항목의 표를 참조하십시오.
6. **다음**을 클릭해 배포 설정을 구성합니다.
7. **사용자 지정**과 **장치/장치 그룹**을 차례로 선택합니다.
8. **완료**를 클릭하세요.

## 웹 클립 구성 설정

다음 표는 웹 클립 구성 설정 목록을 나타냅니다.

| 설정 항목 | 설정하기 |
|---|---|
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **레이블** | 장치 화면의 바로가기 아이콘 하단에 표시할 내용을 입력할 수 있습니다.* |
| **URL** | 웹 클립이 접속할 URL을 입력할 수 있습니다.* |
| **제거 가능** | 장치 사용자가 웹 클립을 삭제할 수 있도록 허용하려면 체크박스를 선택합니다. |
| **아이콘** | 아이콘 파일을 점선 박스로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다. |
| **사전 구성된 아이콘** | Safari 최신 버전으로 추가된 특수효과가 제거되도록 설정할 수 있습니다. |
| **전체 화면** | 웹 클립이 브라우저 컨텐츠로 표시되지 않고 전체 화면으로 표시되도록 설정할 수 있습니다. |
| **매니페스트 범위 무시** | Safari 브라우저를 표시하지 않고 외부 웹 사이트 탐색을 허용하려면 선택합니다. 전체 화면이 선택되지 않은 상태에서는 이 옵션의 효과가 나타나지 않습니다. |
| **대상 애플리케이션 번들 식별자** | URL을 여는 애플리케이션을 지정하는 애플리케이션 번들 식별자입니다. **예시**: com.google.chrome.ios |

> $를 입력하면 현재 필드에 해당하는 지원 변수 목록을 확인할 수 있습니다.

관련 주제:

- iOS용 다중 사용자 보안 로그인
- 구성을 생성하는 방법

# 10.10.5.9. Office 365 설치

**라이센스: Silver**

**적용 가능 운영 체제: Windows 10+**

## Office 365 설치 설정

Office 365 설치는 Office 365 설치 또는 제거를 위해 선택한 기기에 적용할 수 있는 구성 설정입니다. 구성 설정을 Microsoft Office 배포 도구를 사용하여 xml 형식으로 정의한 다음 해당 파일을 업로드하면 됩니다. 파일을 업로드한 후에는 선택한 기기로 구성 옵션을 푸시할 수 있습니다.

**절차**

1. **구성** 탭에서 **+추가**를 클릭합니다.
2. **Office 365 설치**를 선택합니다. **Office 365 설치** 페이지가 표시됩니다.
3. **이름** 필드에 적절한 구성 이름을 입력합니다.
4. **+설명 추가** 링크를 클릭하여 구성에 대한 설명을 추가합니다. 이 필드는 선택 사항입니다.
5. **구성 설정** 섹션에서 다음 필드를 업데이트합니다.

| 필드 이름 | 설명 |
| --- | --- |
| **Office 365 설치를 위한 구성 파일** | **파일 선택** 버튼을 클릭하여 Office 365 설치를 위해 정의된 설정이 포함된 XML 형식의 구성 파일을 찾아 선택합니다. 예: <Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration><br>구성 설정 파일을 추가한 후 구성 파일이 xml 형식인지, 그리고 녹색 체크 표시가 표시되어 있는지 확인합니다. |
| **Office 365 제거를 위한 구성 파일** | **파일 선택** 버튼을 클릭하여 Office 365 제거를 위해 정의된 설정이 포함된 XML 형식의 xml 구성 파일에서 구성 파일을 찾아 선택합니다. 예: <Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration><br>구성 설정 파일을 추가한 후 구성 파일이 xml 형식인지, 그리고 녹색 체크 표시가 표시되어 있는지 확인합니다. |

6. **다음**을 클릭합니다.
7. 다음 옵션 중 하나를 선택하여 기기에 설정을 배포합니다.

| 옵션 | 설명 |
| --- | --- |
| **이 구성 활성화** | 이 체크박스를 선택하면 선택한 기기에 이 구성을 적용할 수 있습니다. 이 체크박스를 선택 해제하면 구성이 제거됩니다(이미 기기에 적용된 경우). |
| **모든 기기** | 해당 설정을 모든 기기에 배포합니다. |
| **기기 없음** | 기기에 설정을 배포하지 않습니다. |
| **사용자 지정** | 해당 설정을 정의된 기기 그룹에 배포합니다. 설정을 배포할 기기 유형 옆에 있는 체크박스를 선택합니다. **기기 그룹 검색** 필드에 기기 그룹 이름을 입력하여 기기 그룹을 검색할 수도 있습니다. 새 기기 그룹을 생성하려면 페이지 하단에 있는 **새 기기 그룹 생성** 링크를 클릭합니다. 자세한 내용은 기기 그룹을 참조하십시오.<br>기기 범주를 선택하면 **배포 요약** 섹션에서 선택한 기기 범주의 기기 사용자 목록에 대한 상세 사항(**이름**, **전화번호**, **기기 유형**)을 확인할 수 있습니다. |

8. **완료**를 클릭하여 선택한 기기에 설정을 푸시합니다.

# 10.10.5.10. Windows GPO 설정

**라이센스: Bridge**

**적용 가능 운영 체제: Windows Desktop**

## Windows GPO 설정 지정

GPO(그룹 정책 객체)는 기기에서 허용되거나 허용되지 않는 작업 권한을 정의하는 설정 모음입니다. GPO 설정을 관리하려면 먼저 Bridge를 설정해야 합니다. 자세한 내용은 Ivanti Bridge를 참조합니다.

GPO 메타데이터가 데이터베이스에 업로드되지 않는 경우 사이트 관리자에게 문의하십시오. GPO 구성이 PowerShell 스크립트에 의해서 Bridge를 통해 기기에 전개됩니다. GPO 설정을 사용하면 특정 설정을 구성하여 기기에 푸시할 수 있습니다.

**절차**

1. **구성** 탭에서 **+추가**를 클릭합니다.
2. **Windows GPO 설정** 구성을 선택합니다. **Windows GPO 설정** 페이지가 표시됩니다.
3. **이름** 필드에 Windows GPO 설정에 적절한 이름을 입력합니다.
4. **+설명 추가** 링크를 클릭하여 구성에 대한 설명을 추가합니다. 이 필드는 옵션 사항입니다.
5. **구성 설정** 섹션에서 **+추가**를 클릭합니다. **Windows 그룹 정책 객체(GPO) 추가** 창이 표시됩니다.
6. 왼쪽 창에 있는 GPO 계층 트리에서 관련 구성 요소를 클릭하여 GPO를 검색한 후 선택합니다. GPO 계층 트리는 정책 설정 경로를 나타냅니다. 검색 필드에 GPO 설정 이름을 입력하여 특정 GPO 설정을 검색할 수도 있습니다.
   GPO 설정을 선택한 후에는 오른쪽 창에서 선택한 GPO 설정의 상세 정보를 볼 수 있습니다.
7. **설정 상태** 필드에서 다음과 같은 설정 옵션을 사용할 수 있습니다.

| 옵션 | 설명 |
| --- | --- |
| **구성되지 않음** | 기존 GPO 설정을 제거합니다. |
| **활성화됨** | GPO 설정을 활성화합니다. |
| **비활성화됨** | GPO 설정을 비활성화합니다. |

8. **설정값** 필드에 GPO의 적절한 이름을 입력합니다.
   설정 값을 추가하려면 **+** 아이콘을 클릭합니다. 설정 값 추가에 일부 GPO 설정이 필요하지 않을 수 있습니다. 텍스트 값 형식으로 설정 값 아래에 추가 데이터를 지정해야 할 수도 있습니다. 그러한 설정의 드롭다운 값에서 아무 값이나 선택합니다.

> 이 필드는 **설정 상태**에서 **활성화됨** 옵션이 선택된 경우에만 편집할 수 있습니다.

9. **저장 및 닫기**를 클릭하여 GPO를 저장하고 창을 닫습니다. 다른 GPO를 추가하려는 경우에는 **저장 후 다른 항목 추가**를 클릭하여 저장하고 GPO 창이 열린 상태로 둡니다.
   추가된 GPO 설정이 **구성 설정** 섹션에 표시됩니다.

> **작업** 열의 관련 아이콘을 클릭하여 GPO 설정을 편집하거나 삭제합니다.

**옵션설명이 구성 활성화**이 체크박스를 선택하면 선택한 기기에 이 구성을 적용할 수 있습니다. 이 체크박스를 선택 해제하면 구성이 제거됩니다(이미 기기에 적용된 경우).**모든 기기**해당 설정을 모든 기기에 배포합니다.**기기 없음**기기에 설정을 배포하지 않습니다.**사용자 지정**해당 설정을

정의된 기기 그룹에 배포합니다. 설정을 배포할 기기 유형 옆에 있는 체크박스를 선택합니다. **기기 그룹 검색** 필드에 기기 그룹 이름을 입력하여 기기 그룹을 검색할 수도 있습니다. 새 기기 그룹을 생성하려면 페이지 하단에 있는 **새 기기 그룹 생성** 링크를 클릭합니다. 자세한 내용은 기기 그룹을 참조하십시오.

기기 범주를 선택하면 **배포 요약** 섹션에서 선택한 기기 범주의 기기 사용자 목록에 대한 상세 사항(**이름**, **전화번호**, **기기 유형**)을 확인할 수 있습니다.

10. **완료**를 클릭하여 선택한 기기에 GPO 설정을 푸시합니다.

# 10.10.5.11. BitLocker 암호화 구성

**라이센스: Bridge**

**적용 가능 운영 체제: Windows Desktop**

이 섹션에는 다음 주제가 포함됩니다.

- BitLocker 암호화 설정
- BitLocker 설정 보기

## BitLocker 암호화 설정

BitLocker 암호화는 하드 드라이브 및 기기의 이동식 드라이브에서 암호화를 강화하여 데이터를 보호하는 기능입니다. BitLocker 암호화를 관리하려면 먼저 Bridge를 설정해야 합니다. 자세한 내용은 **Bridge**를 참조하십시오. BitLocker 암호화 구성으로 기기의 암호화 설정을 구성할 수 있습니다.

**절차**

1. **구성** 탭에서 **+추가**를 클릭합니다.
2. **BitLocker 암호화** 구성을 선택합니다. **BitLocker 암호화** 페이지가 나타납니다.
3. **이름** 필드에 BitLocker 암호화에 적합한 이름을 입력합니다.
4. **+설명 추가** 링크를 클릭하여 구성에 대한 설명을 추가합니다. 이 필드는 옵션 사항입니다.
5. 구성 설정 섹션에서 다음 설정을 구성합니다.

| 설정 | 설명 |
| --- | --- |
| **암호화 방법 및 유형** | 암호화 키 사이즈에 따른 암호화 알고리즘 유형을 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.<br>• **AES-CBL 128비트**<br>• **AES-CBL 256비트** |
| 모든 하드웨어 드라이브 암호화 | 토글 버튼을 클릭하여 **켜기** 또는 **끄기**로 설정하여 모든 하드웨어 드라이브를 암호화합니다.<br>기기에서 하드웨어 드라이브가 이미 암호화되어 있는 경우 암호화 과정이 편집을 통해 복구 불가능하기 때문에 이 구성을 편집하는 것이 적용되지 않습니다. |
| 드라이브 선택 | 암호화가 필요한 드라이브를 선택합니다. 예: **C:**<br>더 많은 드라이브를 추가하려면 **+추가**를 클릭합니다.<br>이 필드는 **모든 하드웨어 드라이브 암호화**를 켜기로 설정한 경우 표시되지 않습니다. |
| 드라이브 유형에 대한 하드웨어 기반 암호화 | TPM(신뢰 플랫폼 모듈)이란 컴퓨터 마더보드에 있는 칩으로, 무단 변형 억제 암호화를 지원합니다. TPM을 갖춘 컴퓨터에서 BitLocker 암호화 또는 기기 암호화를 이용하는 경우, 키의 일부가 TPM에 저장됩니다. 드롭다운 목록에서 다음과 같은 하드웨어 기반 암호화 설정 옵션을 선택할 수 있습니다.<br>• **시작 시 TPM 필요**<br>• **TPM으로 PIN을 시작해야 함**<br>• **TPM 사용 안 함**<br>TPM 옵션은 OS 드라이브 및 TPM 1.2 이상 버전에서만 이용할 수 있습니다.<br>기기에 하드웨어 기반 암호화 설정을 적용하는 경우 기기에 해당 설정을 더 이상 수정할 수 없습니다.<br>기기에 BitLocker 구성이 이미 설정되어 있는 경우 TPM 옵션이 있는 두 번째 BitLocker 구성을 푸시할 수 없습니다. |
| 구성 확인란 옵션 선택(선택 사항):<br>• **BitLocker로 보호되지 않는 고정 드라이브로의 쓰기 액세스를 거부합니다.**<br>• **BitLocker로 보호되지 않는 이동식 드라이브로의 쓰기 액세스를 거부합니다.** | |
| 미리 암호화된 기기 작업 | 다음 옵션 중에서 선택하여 암호가 완전히 해독되지 않았거나 이미 키 보호기가 있는 드라이브를 처리하는 방법을 정의하십시오.<br>• 암호화 중지 - 선택한 드라이브가 이미 암호화된 경우에는 암호화를 중지합니다.<br>• MDM용 Ivanti Neurons에 복구 비밀번호 저장소가 없는 드라이브를 선택하여 암호 해독 - 이 옵션을 선택하면 에 복구 비밀번호가 없는 드라이브에만 적용합니다.MDM용 Ivanti Neurons |

| 설정 | 설명 |
| --- | --- |
| 복구 옵션 | 사용자가 비밀번호를 잊을 경우 복구 옵션이 사용됩니다. 기기 상세 정보 페이지에서 검색할 수 있습니다. 다음과 같은 복구 옵션을 구성할 수 있습니다.<br>• **복구 비활성화**<br>• **비밀번호 사용 및 AD에 저장**<br>• **비밀번호 사용 및 AD와 MobileIron에 저장** |
| 재시작 간격 | 구성이 기기에 푸시된 후에는 재시작 메시지가 표시됩니다. 재시작 후 암호화가 시작됩니다. 재시작 간격을 구성하려면 드롭다운 목록에서 기기 재시작에 소요되는 시간을 선택하십시오. 최소 재시작 간격은 1분이며 최대 재시작 간격은 120분(2시간)입니다. |
| 다시 시작 메시지 | 기기에 표시되어야 하는 재시작 메시지를 입력합니다.<br>해당되는 경우 시작 비밀번호 또는 시작 PIN도 사용자에게 표시됩니다. 사용자는 재시작 후 메시지가 표시될 때 입력할 수 있도록 시작 비밀번호 또는 시작 PIN을 메모할 수 있습니다. |

6. **다음**을 클릭하세요.
7. 다음 옵션 중 하나를 선택하여 기기에 설정을 배포합니다.

| 설정 | 설명 |
| --- | --- |
| **이 구성 활성화** | 이 체크박스를 선택하면 선택한 기기에 이 구성을 적용할 수 있습니다. 이 체크박스를 선택 해제하면 구성이 제거됩니다(이미 기기에 적용된 경우). |
| **모든 기기** | 해당 설정을 모든 기기에 배포합니다. |
| **기기 없음** | 기기에 설정을 배포하지 않습니다. |
| **사용자 지정** | 해당 설정을 정의된 기기 그룹에 배포합니다. 설정을 배포할 기기 유형 옆에 있는 체크박스를 선택합니다. **기기 그룹 검색** 필드에 기기 그룹 이름을 입력하여 기기 그룹을 검색할 수도 있습니다. 새 기기 그룹을 생성하려면 페이지 하단에 있는 **새 기기 그룹 생성** 링크를 클릭합니다. 자세한 내용은 기기 그룹을 참조하십시오.<br>기기 범주를 선택하면 **배포 요약** 섹션에서 선택한 기기 범주의 기기 사용자 목록에 대한 상세 사항(**이름**, **전화번호**, **기기 유형**)을 확인할 수 있습니다. |

8. **완료**를 클릭하여 선택한 기기에 설정을 푸시합니다.

## BitLocker 설정 보기

**BitLocker 설정** 섹션의 기기 상세 정보 페이지(**기기 > 기기 > [기기 이름]**)에서 기기의 BitLocker 설정을 확인할 수 있습니다. 상세 정보는 기본적으로 숨겨져 있습니다.

각 필드 옆의 보기(눈 모양)를 클릭하면 세부 정보가 보입니다.

| 설정 | 설명 |
| --- | --- |
| **복구 비밀번호** | 해당 옵션을 선택하면, BitLocker 구성을 푸시한 후 Windows에서 복구 비밀번호를 생성하고 MDM용 Ivanti Neurons으로 반환합니다. 기기가 복구 모드에 들어가면 해당 비밀번호를 입력하라는 메시지가 사용자에게 표시됩니다.<br>여러 개의 드라이브가 암호화되어 있을 경우 같은 복구 비밀번호를 사용해야 합니다.<br>**비밀번호 저장 및 AD와 MobileIron에 저장** 복구 옵션을 선택한 경우 복구 비밀번호만 게시됩니다. |
| **PIN** | 6자리 시작 PIN을 표시합니다. PIN은 BitLocker 구성 설정에서 **TPM으로 PIN을 시작해야 함** 옵션을 선택한 경우에만 표시됩니다. |
| **시작 비밀번호** | 기기에 설정된 시작 비밀번호입니다. 해당 옵션을 선택한 경우에만 시작 비밀번호가 표시됩니다. BitLocker 구성 설정에서 **TPM을 사용하지 마십시오**. |
| **TPM 버전** | TPM 구성 버전을 표시합니다. |

BitLocker 구성 설정에서 구성한 설정을 기반으로 일부 필드에서 **해당 없음**을 표시할 수 있습니다.

- 기기 상세 정보 페이지의 기기 암호화 상태 아래에 암호화 상태가 표시됩니다.
- BitLocker가 적용되는 기기의 모든 드라이브에 동일한 시작 비밀번호 또는 PIN이 사용됩니다.
- 드라이브가 이미 암호화되고 복구 비밀번호가 저장된 기기의 두 번째 드라이브를 암호화하는 구성을 생성하는 경우 기존의 비밀번호는 덮어쓰기됩니다. 따라서 기기에 드라이브가 한 개가 있는 경우에만 복구 비밀번호 옵션을 사용할 것을 권장합니다.

# 10.10.6. 엔터프라이즈 네트워크 액세스 구성

이 섹션에는 다음 주제가 포함됩니다.

- AirPlay 설정
- AirPrint 설정
- Always On VPN 구성
- 기본 앱 런타임 권한
- 교육
- 글로벌 프록시 설정
- LDAP 설정
- macOS 서버 구성
- 네트워크 릴레이 구성
- Tunnel
- AppTunnel 설정
- 퍼앱 VPN 구성
- Single Sign-On 설정
- iOS용 다중 사용자 보안 로그인
- Android APN 설정 구성
- VPN 구성
- VPN(요청 시)
- Wi-Fi 구성

# 10.10.6.1. AirPlay 설정

**라이센스:** Silver

AirPlay 설정을 통해 미디어 디스플레이용 대체 기기 사용 환경을 설정할 수 있습니다. 다음 표에 AirPlay 설정 목록이 제공됩니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 목록 허용 | 허용된 각 AirPlay 저장 위치의 기기 ID를 입력할 수 있습니다. ID를 지정하지 않으면 AirPlay 저장 위치가 제한되지 않습니다.<br>**적용 가능 운영 체제**: iOS 7.0+ 및 macOS 10.10+(감독됨) |
| 기기 설정 | 확인된 각 AirPlay 저장 위치의 기기 ID(macOS)나 기기 이름(iOS) 및 비밀번호를 입력할 수 있습니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.6.2. AirPrint 설정

**라이센스:** Silver

AirPrint 구성을 통해 무선 인쇄 환경을 설정할 수 있습니다. 다음 표에 AirPrint 설정 목록이 제공됩니다.

| 설정 | 설정 방법 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| AirPrint 설정 | **IP 주소**: AirPrint 프린터의 IP 주소를 입력합니다.<br>**리소스 경로**: AirPrint 프린터와 연결된 리소스 경로를 입력합니다. 이 경로는 _ipps.tcp Bonjour 기록의 rp 매개변수에 해당합니다.<br>예:<br>• printers/Canon_MG5300_series<br>• printers/Xerox_Phaser_7600<br>• ipp/print<br>• Epson_IPP_Printer.<br>리소스 경로는 대소문자를 구분합니다.<br>**포트:** AirPrint 대상의 수신 포트를 입력합니다.<br>포트를 지정하지 않으면 AirPrint는 기본 포트를 사용합니다. Apple 표준 포트에 대한 자세한 내용은 https://support.apple.com/en-us/HT202944를 방문하십시오.<br>**강제 TLS:** TLS(Transport Layer Security)에 의해 보호되도록 연결할 수 있습니다. 기본적으로 비활성화되어 있습니다. |

macOS에 **AirPrint** 구성이 설치된 후 프린터 상세 정보가 **AirPrint** 구성을 통해 기기로 푸시됩니다. 사용자는 시스템 환경설정 > 프린터 & 스캐너 > +를 클릭하여 자동으로 채워진 프린터 상세 정보를 볼 수 있습니다. **추가** 화면에서 사용자는 **기본값**을 선택하고 필수 인쇄 프로필을 선택해야 합니다. 이로써 필요한 프린터가 **프린터 & 스캐너**에 추가됩니다.

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.6.3. Always On VPN 구성

**라이센스:**

- **Android Enterprise의 골드**
- **iOS: Silver**

Always On VPN 구성을 사용하면 사용자는 어떠한 조치 없이 사용 가능한 VPN에 자동으로 연결됩니다. 이 기능을 사용하려면 Android 7.0 이상 또는 iOS 8 이상은 물론 IKEv2 프로토콜을 지원하는 VPN 제공자가 필요합니다.

## Android용 Always On VPN 설정

Always On VPN 구성은 Android 7.0 이상이 설치된 Android Enterprise 기기로 전송됩니다. 작업 프로필이 있는 관리되는 기기(Android 8.0 이상)에서는 작업 프로필에서 VPN 구성이 적용됩니다.

> 기기가 **COSU** 모드에서 기기 등록 유형 **AMA**으로 배포되고 **Always On**이 구성된 앱이 기기에 푸시될 경우 **Always On** 구성도 기기에 푸시됩니다.

이 구성을 활성화하려면 앱 카탈로그에서 앱을 선택하거나 패키지 이름을 입력합니다.

## iOS의 Always On VPN 설정

| 설정 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 휴대폰과 Wi-Fi에 같은 터널 구성을 사용합니다.<br><br>서버<br><br>로컬 식별자 | 휴대폰이나 Wi-Fi 네트워크를 통해 연결이 설정되는지 여부와 관계없이 VPN 연결을 위한 서버 식별자 한 쌍을 지정하도록 선택합니다.<br><br>VPN 서버의 호스트 이름이나 IP 주소를 입력합니다.<br><br>다음의 형식 중 하나로 된 IKEv2 클라이언트의 식별자:<br>• FQDN<br>• UserFQDN<br>• 주소<br>• ASN1DN |
| 원격 식별자 | 다음 형식 중 하나로 된 원격 식별자:<br>• FQDN<br>• UserFQDN<br>• 주소<br>• ASN1DN |
| EAP 활성화 | 확장된 인증을 활성화하도록 선택합니다. |
| 시스템 인증<br><br>EAP 인증 | EAP 활성화가 선택되지 않은 경우에만 사용 가능합니다.<br>다음 중 하나를 선택합니다.<br>• 인증서<br>• 공유 비밀<br><br>EAP 활성화가 선택된 경우에만 사용 가능합니다.<br>다음 중 하나를 선택합니다.<br>• 인증서<br>• 사용자 이름/비밀번호 |
| 공유 비밀<br><br>자격 증명 | 시스템 인증을 위한 공유 비밀이 선택되어 있는 경우에만 사용 가능합니다. 연결하려면 공유 비밀을 입력합니다.<br><br>시스템 인증을 위한 인증서가 선택된 경우에만 사용 가능합니다. 사용할 인증서를 선택합니다. 이 인증서가 IKE 클라이언트 인증을 위해 전송됩니다. 확장된 인증을 사용하는 경우 이 인증서를 EAP-TLS용으로 사용할 수 있습니다. |
| 계정 | EAP 인증을 위한 사용자 이름/비밀번호가 선택된 경우에만 사용 가능합니다. VPN 서버의 계정 ID를 입력합니다. |
| 비밀번호 | EAP 인증을 위한 사용자 이름/비밀번호가 선택된 경우에만 사용 가능합니다. VPN 서버의 비밀번호를 입력합니다. |
| 정지 피어 감시 주기 | 다음 중 하나를 선택합니다. |

| 설정 | 설정하기 |
| --- | --- |
| | • 없음(비활성화)<br>• 낮음(킵얼라이브가 1시간마다 전송됨)<br>• 중간(킵얼라이브가 30분마다 전송됨)<br>• 높음(킵얼라이브가 10분마다 전송됨) |
| 암호화 알고리즘 | 다음 중 하나를 선택합니다.<br>• DES<br>• 3DES<br>• AES-128<br>• AES-256<br>• AES-128-GCM<br>• AES-256-GCM<br>• ChaCha20-Poly1305 |
| 무결성 알고리즘 | 다음 중 하나를 선택합니다.<br>• SHA1-96<br>• SHA1-160<br>• SHA2-256<br>• SHA2-384<br>• SHA2-512 |
| 디피 헬만 그룹 | D-H 키 익스체인지 그룹을 선택합니다. |
| 분 단위 수명 | 분 단위 SA 수명(re-key 주기)을 입력합니다. 유효한 값은 10 ~ 1440입니다. |
| 음성 메일 | 터널을 통한 트래픽 허용을 선택하여 Always On VPN에 대해 음성 메일을 제외합니다. 예외가 되지 않도록 하려면 트래픽 드롭을 선택합니다. |
| Airprint | 터널을 통한 트래픽 허용을 선택하여 Always On VPN에 대해 AirPrint 트래픽을 제외합니다. 예외가 되지 않도록 하려면 트래픽 드롭을 선택합니다. |
| 셀룰러 서비스 | 터널을 통한 트래픽 허용을 선택하여 Always On VPN에 대해 셀룰러 서비스 트래픽을 제외합니다. 예외가 되지 않도록 하려면 트래픽 드롭을 선택합니다. |
| VPN 터널 외부에 있는 캡티브 웹 시트에서의 트래픽 허용 | VPN 터널 외부에 있는 캡티브 웹 시트에서의 트래픽 허용을 선택합니다. |
| VPN 터널 외부에 있는 모든 캡티브 네트워킹 앱에서의 트래픽 허용 | VPN 터널 외부에 있는 모든 캡티브 네트워킹 앱에서의 트래픽 허용을 선택하여 캡티브 네트워크 처리를 수행합니다. |
| 캡티브 네트워킹 앱 번들 식별자 | VPN 터널 외부에 트래픽이 허용된 캡티브 네트워킹 앱에 대한 번들 ID를 나열하여 캡티브 네트워크 처리를 수행합니다. 캡티브 환경에서 작동하기 위해 캡티브 네트워킹 앱이 추가 권한을 요구할 수 있습니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.6.4. 기본 앱 런타임 권한

**적용 대상:** Android API 23 이상을 대상으로 개발되었고 Android Enterprise 기기에서 Android 6.0 이상을 실행하는 앱.

관리자는 Android 엔터프라이즈 기기에 배포된 앱의 런타임 권한 구성을 설정할 수 있습니다. API 23(또는 이상)을 대상으로 개발되었고 Android 6.0 이상을 실행하는 앱은 런타임 시 사용자에게 권한을 요청할 수 있습니다. 기본 앱 런타임 권한 구성은 앱 런타임 권한의 기본값을 설정합니다. MDM용 Ivanti Neurons는 이 구성을 기본값으로 생성합니다. 이 기본 시스템 구성을 편집하거나 요구 사항에 따라 새 구성을 생성할 수 있습니다.

앱별 권한이 전역 앱 권한 구성보다 우선합니다. 인하우스 앱은 전역 권한이 적용됩니다. 인하우스 앱은 앱별 권한을 설정할 수 없습니다.

## 전역 런타임 권한 설정

관리자는 기본 앱 런타임 권한과 구성 배포를 다음과 같이 편집할 수 있습니다.

**Procedure절차**

1. **구성**으로 이동합니다.
2. 다음 작업 중 하나를 수행합니다.
   - 기본 시스템 구성을 편집하려면 **기본 앱 런타임 권한**을 클릭한 다음, **편집**을 클릭합니다.
   - 새 구성을 추가하려면 **추가 > 기본 앱 런타임 권한**을 클릭합니다.

구성 이름을 입력합니다.

4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 기본 런타임 권한 중 하나를 선택합니다.
   - 사용자 프롬프트(기본 옵션)
   - 자동 권한 부여
   - 자동 거부(주의해서 사용)

**다음**을 클릭하세요.

7. **이 구성 활성화 옵션**을 선택합니다.

> 이 옵션을 취소하면 기기에 구성이 적용되지 않습니다. 이전에 적용된 경우 모든 기기에서 제거됩니다.

8. 다음 배포 옵션 중 하나를 선택합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정

**완료**를 클릭합니다.

## 앱별 런타임 권한 설정

관리자는 다음과 같이 개별 애플리케이션에 대해 기본 런타임 권한을 설정할 수 있습니다.

**절차**

1. **앱**으로 이동합니다.

2. 앱 이름을 클릭합니다.
3. **앱 구성 > Android 엔터프라이즈**를 클릭합니다.
4. **추가**를 클릭하거나 구성 이름을 클릭하여 기존 구성을 편집합니다.
5. 이름, 설명, 제한 등의 구성 옵션을 설정합니다.
6. 런타임 권한 섹션에서 **권한 관리**를 클릭합니다.
7. 표시된 창에서 권한을 선택하고 **선택**을 클릭합니다.
   특정 애플리케이션에 적용 가능한 위험한 권한만 선택을 위해 나열됩니다. 위험한 권한(예: 연락처 읽기, 기기에서 계정 찾기, 호출 로그 쓰기 등)의 전체 목록은 https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups에서 확인할 수 있습니다.
   - 권한은 애플리케이션이 권한을 요청하는 경우에만 적용됩니다.
   - 사용자가 이전에 권한을 수락했거나 거부한 경우에는 권한이 적용되지 않습니다.

런타임 권한 섹션에서 다음 기본 런타임 권한 중 하나를 선택합니다.

- 기본/전역(기본 옵션)
- 자동 권한 부여
- 자동 거부(주의해서 사용)

이 앱 구성 배포 섹션에서 다음 배포 옵션 중 하나를 선택합니다.

- 앱을 소유한 모든 사람
- 대상 없음
- 사용자 지정

**저장**을 클릭합니다.

# 10.10.6.5. 교육

**라이센스:** Gold

**적용 대상:** 관리 상태인 iOS 9.3+

Apple Education 페이로드 및 리더 및 구성원용 Classroom 앱을 구성할 수 있습니다. 다음 표에 Education 설정 목록이 제공됩니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 구성 유형 | 다음 중 하나를 선택합니다.<br>• 리더<br>• 구성원 |
| 이 구성 활성화 | • 이 옵션을 선택하면 구성을 선택한 기기에 적용할 수 있습니다.<br>• 이 옵션을 해제하면 이 구성이 이전에 적용된 경우 구성을 삭제합니다. |
| 배포 | 다음 배포 옵션 중 하나를 선택합니다.<br>• 모든 기기<br>• 기기 없음<br>• 사용자 지정 |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.6.6. 글로벌 프록시 설정

**라이센스**: Silver

글로벌 프록시를 설정하면 기기에서 프록시 서버로 HTTP 트래픽이 전달되도록 설정됩니다. 다음 표에 글로벌 프록시 설정 목록이 제공됩니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 유형 | **수동** 또는 **자동**을 선택하세요. **수동**을 선택한 경우 프록시 서버 호스트 이름과 포트가 필요하며, 상황에 따라 프록시 서버의 사용자 이름과 비밀번호가 필요할 수도 있습니다. **자동**을 선택하면 프록시 자동 구성(PAC) URL을 입력할 수 있습니다. |
| 호스트 이름 및 포트 | **수동**을 선택한 경우 해당 프록시 서버의 호스트 이름과 포트 번호를 입력할 수 있습니다. |
| 사용자 | (선택사항) 프록시 서버 접속 시 사용할 사용자 이름* |
| 비밀번호 | (선택사항) 프록시 서버 접속 시 사용할 비밀번호 |
| PAC URL | (선택사항) **자동**을 선택했다면, 해당 프록시 구성을 정의하는 PAC 파일의 URL을 입력할 수 있습니다. 이 항목을 공란으로 비워둘 경우, 장치에서 웹 프록시 자동검색 프로토콜(WPAD)을 통해 프록시가 검색됩니다. |
| PAC에 연결할 수 없는 경우 직접 연결 허용 | (iOS 7 이상) 어떤 이유에서건 장치에서 PAC 파일 액세스가 불가능한 경우 직접 연결이 허용되도록 설정할 수 있습니다. |
| 캡티브 네트워크에 액세스하는 데 프록시 바이패스 허용 | (iOS 7 이상) 캡티브 네트워크 로그인 페이지를 표시하는 데 프록시 바이패스가 허용되도록 설정할 수 있습니다. |

$를 입력하면 현재 필드에 해당하는 지원 변수 목록을 확인할 수 있습니다.

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.6.7. 전역 프록시 구성(Android)

> 기기 소유자 및 AOSP 모드에서 Android 기기에만 적용됩니다.

글로벌 프록시를 설정하면 기기에서 프록시 서버로 HTTP 트래픽이 전달되도록 설정됩니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**을 클릭합니다.
3. **+추가**를 클릭합니다.
4. 검색 필드에 **전역**을 입력한 다음 **전역 프록시**를 클릭합니다.
   전역 프록시 구성 세부 정보 페이지가 표시됩니다.
5. **이름** 상자에 구성 이름을 입력합니다.
6. 필요에 따라 구성에 대한 설명을 일부 추가할 수 있습니다.
7. **플랫폼** 목록에서 **Android**를 선택합니다. **구성 설정** 섹션이 표시됩니다.
8. 유형에서 **수동** 또는 **자동**을 선택합니다.
   - **수동**
     - **호스트 이름**(도메인 이름/IP 주소) 및 **포트** 상세 정보를 입력합니다.
     - **제외 항목 추가**에서 제외 목록에 포함해야 하는 여러 호스트 이름(도메인 이름/와일드카드)을 추가할 수 있습니다.
   - **자동**
     - PAC URL을 입력합니다.
9. **다음**을 클릭해 배포 설정을 구성한 다음 **완료**를 클릭합니다.

# 10.10.6.8. LDAP 설정

LDAP 설정을 통해 회사 디렉토리 사용 환경을 설정할 수 있습니다. 다음 표에 LDAP 설정 목록이 제공됩니다.

| 설정 항목 | 설정하기 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 호스트 이름 | LDAP 서버의 호스트 이름을 입력합니다.* |
| 사용자 | LDAP 계정 접속에 사용할 사용자 이름을 입력합니다.* |
| 비밀번호 | LDAP 계정 접속에 사용할 비밀번호를 입력합니다. |
| SSL 사용 | SSL을 사용해 LDAP 서버에 연결할 수 있습니다. |
| 검색 설정 | 각 계정에 대해 반드시 1개 이상 항목을 입력해야 합니다. 각 항목은 검색이 시작되는 LDAP 트리의 노드를 의미합니다. + 버튼을 클릭하면 신규 항목 추가 후 해당 항목 수정이 가능합니다.<br>각 항목은 다음 값으로 구성됩니다.<br>설명: 해당 검색 설정에 대한 설명을 제공합니다.<br>범위: **베이스나 하위 트리**, **한 수준**을 선택해 검색 범위를 표시할 수 있습니다. **베이스**는 노드 수준을 나타내며, **하위 트리**는 노드와 모든 하위 요소를 의미합니다. 그리고 **한 수준**은 노드와 하위 요소의 수준을 의미합니다.<br>검색 기준: 지정된 노드의 개념 경로(예: ou=people, o=mycorp). |
| 퍼앱 VPN | **전제 조건**: LDAP 구성에서 퍼앱 VPN을 구성하기 전에 Tunnel 또는 퍼앱 VPN 구성을 설정하십시오.<br>드롭다운 메뉴에서 사전 구성된 퍼앱 VPN 구성을 선택하십시오.<br>**적용 가능 운영 체제**: iOS 14+ |
| **iOS 10+** | |
| 통신 서비스 규칙 | LDAP 시스템에서 연락처에 음성 전화를 거는 데 사용하는 기본 앱을 선택합니다. |

$를 입력하면 현재 필드에 해당하는 지원 변수 목록을 확인할 수 있습니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.6.9. macOS 서버 구성

macOS 서버 구성은 구성된 계정 유형과 설정으로 macOS 서버 계정을 정의합니다. 이 구성을 통해 사용자는 서버에서 파일 공유를 활성화할 수 있습니다.

**적용 가능 운영 체제:** iOS 10+

## macOS 서버 구성

**절차**

1. **구성 > +추가**로 이동합니다.
2. **macOS 서버** 구성을 선택하여 **macOS 서버 구성 생성** 페이지를 표시합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. **호스트 이름**을 입력하여 서버 주소를 지정합니다.
6. **사용자 이름**을 입력하여 사용자 로그인 이름을 지정합니다.
7. (선택 사항) 사용자 **비밀번호**를 입력합니다.
8. (선택 사항) 계정 **설명**을 입력합니다.
9. 구성된 계정에서 문서 사전 계정의 서버를 연결할 때 사용할 **포트** 번호를 입력합니다(선택 사항). 포트 번호를 지정하지 않으면 기본 포트 번호가 사용됩니다.
10. **다음**을 클릭하세요.
11. 이 구성에 대한 배포를 선택합니다.

# 10.10.6.10. Tunnel

Ivanti Tunnel은 iOS, Android, Windows 장치에서 VPN 기능을 활성화합니다. Ivanti Tunnel은 UEM(Unified Endpoint Management) 플랫폼, Standalone Sentry, Access와 상호 작용하여 엔터프라이즈 네트워크 외부에서 엔터프라이즈 리소스 액세스를 보호합니다. 엔터프라이즈 리소스는 온프레미스 또는 클라우드에 있을 수 있습니다. UEM 플랫폼은 Ivanti EPMM 및 MDM용 Ivanti Neurons입니다.

> 앱별 구성은 Android Enterprise 기기에서 더 이상 사용되지 않습니다. 앱 카탈로그에서 Ivanti Tunnel용 관리형 구성을 사용해야 합니다.

## Ivanti Tunnel 구성 정보

Ivanti Tunnel에 대한 구성은 UEM(Unified Endpoint Management) 플랫폼에서 생성합니다. Ivanti Tunnel은 UEM 클라이언트로부터 구성을 받습니다. Ivanti EPMM의 클라이언트는 Mobile@Work이고 MDM용 Ivanti Neurons의 클라이언트는 Go입니다.

### 최신 문서

최신 Tunnel 지침은 제품 문서를 확인하십시오.

- Android용 Tunnel은 **Android용 Ivanti Tunnel 가이드** 참조
- iOS용 Tunnel은 **iOS용 Ivanti Tunnel 가이드** 참조
- macOS용 Tunnel은 **macOS용 Ivanti Tunnel 가이드** 참조
- Windows Tunnel은 **Windows용 Ivanti Tunnel 가이드**를 참조하십시오

> Windows용 Ivanti Tunnel은 사용 중지되어 더 이상 MDM용 Ivanti Neurons에서 지원되지 않습니다.

# 10.10.6.11. AppTunnel 설정

AppTunnel은 각 앱 컨테이너와 기업 네트워크 사이에 앱별 세션 보안을 제공하여 앱 데이터를 보호합니다.

이 섹션에는 다음 주제가 포함됩니다.


- Sentry를 인증서가 포함된 AppTunnel을 사용하도록 설정
- Sentry 인증서 업로드
- AppTunnel을 사용하도록 앱 설정
- AppTunnel 서비스 이름 정보


## Sentry를 인증서가 포함된 AppTunnel을 사용하도록 설정합니다.

> Standalone Sentry를 처음 설치하면 자체 서명된 인증서도 설치됩니다. Ivanti는 기본 인증서를 공개적으로 신뢰할 수 있는 타사 인증서로 교체할 것을 강력히 권장합니다.

**필수 조건**

- AppTunnel은 Sentry의 최신 지원 버전에 따라 달라집니다. AppTunnel 설정 작업을 시작하기 전에 Sentry 설치를 완료하십시오.
- SCEP ID를 사용할 경우:
  - 로컬 또는 외부 인증기관을 추가합니다. Connector 설치가 필요합니다.
  - 앱 ID 인증서 설정을 추가합니다. AppTunnel 구성 시 사용할 동적 배포입니다.

프로필에 할당된 Sentry 서버를 사용하도록 인증을 위한 X.509 인증서를 사용하여 ActiveSync 및/또는 AppTunnel을 구성할 수 있습니다.

**절차**

1. **관리 > Sentry**로 이동합니다.
2. **+ Sentry 프로필 추가**를 클릭합니다.
3. **ActiveSync 및/또는 인증서 포함 AppTunnel**을 클릭합니다.
4. **다음**을 클릭하세요.
5. 다음 표의 가이드라인을 사용하여 **글로벌 설정** 페이지를 완료합니다.

| 표: 관리 > Sentry를 위한 글로벌 설정 | |
|---|---|
| 설정 | **수행 작업** |
| **Windows** | 이 프로파일을 식별할 수 있는 이름을 입력합니다. |
| **설명** | 현재 프로파일에 대한 간략한 설명을 입력합니다. |
| **외부 호스트 이름 및 포트** | Sentry의 호스트 이름과 포트를 입력합니다. |
| **기기 인증 모드** | |
| **2단계 인증에 단일 인증서 사용** | 인증에 단일 인증서를 사용할 경우 이 옵션을 선택합니다. **업로드한 인증서**가 없을 경우, 아래 선택한 옵션에 표시된 영역에서 인증서를 업로드할 수 있습니다. |
| **인증서 선택** | 기기 인증에 필요한 그룹 인증서 업로드 방법:<br>1. **추가**를 클릭합니다. **인증서 추가** 창이 표시됩니다.<br>2. **인증서 이름** 필드에 인증서 이름을 입력합니다.<br>3. PKCS12 파일을 보호하는 비밀번호를 입력합니다.<br>4. **파일 선택**을 클릭하여 그룹 인증서를 업로드합니다.파일 형식이 .p7b, .p12, .pfx, .pem, .der, .crt 또는 .cer인지 확인하십시오. |
| **인증서 폐기 목록(CRL) 활성화** | CA가 게시한 인증서 폐기 목록(CRL)에 대해 기기에서 제시한 인증서를 검증하려면 이 옵션을 선택합니다. |
| **비관리 기기 기본 동작** | |
| **비관리 기기의 이메일 및 데이터 수신 허용** | MDM용 Ivanti Neurons에서 관리되지 않는 기기의 데이터 액세스를 차단하지 않으려면 선택합니다. |

6. **다음**을 클릭하세요.
7. **Sentry 서버 구성** 페이지에서 다음 필드를 구성합니다.
8. **다음**을 클릭하세요.

| 표: 관리 > Sentry에 대한 Sentry 서버 구성 | |
|---|---|
| 설정 | 설정하기 |
| **리스너 프로토콜** | 다음 프로토콜 옵션 중 하나를 선택합니다.<br>• **HTTPS 전용**<br>• **HTTP 전용**<br>• **HTTPS 및 HTTP** |
| **Https 포트** | Https 포트 번호를 입력합니다. 이 필드는 리스너 프로토콜이 HTTP 전용으로 선택될 경우 표시되지 않습니다. |
| **Http 포트** | Http 포트 번호를 입력합니다. 이 필드는 리스너 프로토콜이 HTTPS 전용으로 선택될 경우 표시되지 않습니다. |
| **Sentry TLS 서버 인증서/키** | |
| **Sentry의 자체 서명 인증서 사용** | MDM용 Ivanti Neurons 서비스에서 생성되어 현재 프로필의 일부로 Sentry에 전송된 자체 서명 인증서를 사용하려면 선택합니다. 이 인증서는 Sentry와 모바일 기기 간 통신에 사용됩니다. |
| **추가** | 인증에 필요한 자체 인증서 업로드 방법:<br>1. **추가**를 클릭합니다. **인증서 추가** 창이 표시됩니다.<br>**Sentry의 자체 서명 인증서 사용** 옵션을 선택 해제해야 이 옵션이 표시됩니다.<br>2. **인증서 이름** 필드에 인증서 이름을 입력합니다.<br>3. PKCS12 파일을 보호하는 비밀번호를 입력합니다.<br>4. **파일 선택**을 클릭하고 인증서를 업로드합니다.파일 형식은 .p12 파일이어야 합니다.<br>5. **추가**를 클릭합니다.<br>업로드된 모든 TLS 서버 인증서(Sentry 메인 페이지 및 다른 프로필에서 업로드된 인증서 포함)가 Sentry TLS 서버 인증서/키 섹션에 표시됩니다. 인증에 필요한 TLS 인증서를 선택하려면 인증서 옆의 라디오 버튼을 클릭하십시오. |
| **두 번째 인증서 추가** | 두 번째 인증서를 활성화하려면 선택합니다. 기본 인증서가 만료되면 관리자의 개입 없이 Sentry가 자동으로 예비 인증서로 전환합니다.<br>Tunnel에는 이미 두 인증서 모두 저장되어 있어 어느 인증서와도 일치시킬 수 있으므로 연결이 중단되지 않도록 합니다. |
| **프로토콜** | 필요한 수신 및 발신 프로토콜을 선택합니다. |
| **암호 스위트** | Sentry와 SSL 암호화 통신 시에는 암호가 사용됩니다. 보안성이 높은 암호를 사용하는 것이 좋습니다. 구식 기기의 경우 보안 수준이 낮은 암호를 사용하기도 합니다. 기본적으로 보안 수준이 높은 암호가 선택됩니다. 사용할 추가 암호를 선택할 수 있습니다. 반드시 1개 이상 암호를 선택해야 합니다. |

9. 표시된 서버스를 한 개 이상 추가합니다.
10. **저장**을 클릭합니다.

Sentry가 등록되면 미설정 Sentry 서버 섹션의 Sentry 페이지에 나타납니다. Sentry에 대한 프로필을 할당하려면 **작업** 열의 **할당**을 클릭하십시오.

# Sentry 인증서 업로드

MDM용 Ivanti Neurons 은(는) Sentry 프로필을 생성할 때 TLS 서버 인증서 및 그룹 인증서를 업로드합니다. **Sentry 인증서** 섹션의 **Sentry** 페이지에서 이 인증서를 업로드할 수도 있습니다.

Ivanti Neurons는 업로드 시 Sentry 인증서의 유효성을 검사하여 인증서에 나온 조건에 따라 다음 유형의 정보를 반환합니다.

| 조건 | 정보 유형 |
| --- | --- |
| 리프 인증서에 인증 기관에 대한 체인이 포함되어 있지 않거나 업로드된 파일에 인증 기관이 없습니다. | 오류 |
| 사용 가능한 루트 인증 기관이 없습니다. | 경고 |
| 루트 인증 기관이 리프 인증서에 대한 중간 인증 기관을 승인하지 않았습니다. | 경고 |

MDM용 Ivanti Neurons 도 본 조항의 규칙에 대해 유효성을 검사합니다.

**절차**

1. **TLS 서버 인증서** 섹션에서 **추가**를 클릭합니다. **인증서 추가** 창이 표시됩니다.
2. **인증서 이름** 필드에 인증서 이름을 입력합니다.
3. PKCS12 파일을 보호하는 비밀번호를 입력합니다.
4. **파일 선택**을 클릭하여 그룹 인증서를 업로드합니다. 파일 형식이 .p7b, .p12, .pfx, .pem, .der, .crt 또는 .cer인지 확인하십시오.
5. **추가**를 클릭합니다. 업로드된 인증서가 표에 표시됩니다.
6. TLS 서버 인증서를 삭제하려면 **작업** 열의 삭제 아이콘을 클릭하십시오.

> Sentry 프로필에 TLS 서버 인증서가 사용된 경우 해당 인증서를 삭제할 수 없습니다. 삭제 작업이 수행되면 오류 메시지가 표시됩니다.

## 그룹 인증서 추가

**절차**

1. **그룹 인증서** 섹션에서 **추가**를 클릭합니다. **인증서 추가** 창이 표시됩니다.
2. **인증서 이름** 필드에 인증서 이름을 입력합니다.
3. PKCS12 파일을 보호하는 비밀번호를 입력합니다.
4. **파일 선택**을 클릭하여 그룹 인증서를 업로드합니다. 파일 형식이 .p7b, .p12, .pfx, .pem, .der, .crt 또는 .cer인지 확인하십시오.
5. **추가**를 클릭합니다.

업로드된 그룹 인증서를 삭제하려면 **작업** 열의 삭제 아이콘을 클릭하십시오.

## Sentry 루트 인증서 편집

관리자는 Sentry 루트 인증서 구성의 배포를 편집할 수 있습니다. 구성을 다른 공간에 위임하여 사용자 지정 공간 관리자에게 편집 권한을 제공할 수도 있습니다.

1. **구성**으로 이동합니다.
2. **Sentry 루트 인증서**를 검색합니다.
3. 편집 아이콘을 클릭합니다.

4. 인증서를 배포할 기기 또는 기기 그룹에 해당하는 확인란을 선택합니다. 또는 기기 또는 기기 그룹에 해당하는 확인란의 선택을 취소합니다.
5. 해당하는 경우 배포 요약 섹션에서 다음 옵션 중 하나를 선택합니다.
    - **다른 공간에 적용하지 않음**
    - **다른 공간의 장치에 적용**
6. (선택 사항) **공간 관리자가 배포를 편집하도록 허용** 확인란을 클릭합니다.
7. **저장**을 클릭하세요.
8. 경고 메시지가 나타납니다. **예**를 눌러 확인합니다.

## AppTunnel을 사용하도록 앱 설정

최신 Sentry 지침을 보려면 제품 문서에서 Sentry를 클릭하십시오. Sentry 버전에 적합한 문서를 선택하십시오.

## AppTunnel 서비스 이름 정보

AppTunnel 서비스는 AppConnect 앱에서 터널링하는 백 엔드 서비스를 정의합니다.

최신 지침의 경우 제품 문서에 방문하여 **Sentry** 및 **AppConnect** 버전에 적합한 문서를 선택하십시오.

# 10.10.6.12. 퍼앱 VPN 구성

**라이센스:** Silver

**적용 대상:** iOS, watchOS, visionOS, tvOS 기기

퍼앱 VPN 구성은 다음과 같은 특정 앱의 가상 사설 네트워크 액세스에 필요한 설정을 정의합니다.

- 퍼앱 VPN 설정
- Psec(Cisco)
- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- 사용자 지정 SSL
- Palo Alto Networks GlobalProtect

> 퍼앱 VPN 구성은 앱 구성에 의존합니다. 퍼앱 VPN 구성은 앱 구성 설정 중에 생성됩니다. 퍼앱 VPN 구성이 삭제 또는 배포 취소되면 앱 연결이 네트워크에서 끊어져 앱 구성이 오작동합니다.

## 구성 배포 중

MDM용 Ivanti Neurons 릴리스 91부터 전역 관리자는 모든 기기 및 사용자 지정 배포 옵션에서 앱별 VPN 인증서 구성을 편집할 권한을 공간 관리자에게 위임할 수 있습니다. 앱별 VPN 구성의 경우 이 구성을 모든 공간에서 사용할 수 있도록 허용 옵션을 선택적으로 선택할 수 있습니다.

> 배포 변경 사항은 특정 공간에만 적용됩니다. 기타 모든 공간은 계속 기본 공간 배포 설정을 상속합니다.

해당하는 경우 다음 표의 정보를 사용하여 필드에 구성 설정을 지정한 다음 구성을 배포합니다.

**자세한 정보는 구성 작업에서 *구성 배포* 항목을 참조하십시오.**

## 퍼앱 VPN 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 연결 유형<br><br>요청 시 VPN 활성화<br><br>iOS 규칙 활성화<br>(요청 시 VPN 활성화를 선택한 경우 적용)<br><br>요청 시 일치 앱이 활성화됨 | 설정할 VPN 유형을 선택할 수 있습니다.<br>선택한 유형에 따라 나머지 설정 항목이 달라집니다.<br><br>요청 시 VPN을 설정하는 도메인 및 호스트 이름에 현재 설정을 사용하도록 설정할 수 있습니다.<br><br>iOS 및 macOS의 경우 다음을 설정할 수 있습니다.<br>• 진짜로 확인된 네트워크 연결을 허용/금지하거나 해당 네트워크를 허용/무시하는 네트워크 규칙입니다.<br>• 필요에 따라 진짜로 확인된 네트워크를 허용하거나 금지하거나 연결하는 연결 규칙입니다.<br>네트워크 규칙에서 지정할 수 있는 매개 변수 유형:<br>• DNS 도메인 일치<br>• DNS 서버 주소 일치<br>• SSID 일치<br>• URL 문자열 검색<br>• 인터페이스 유형 일치<br>연결 규칙에서 지정할 수 있는 매개 변수 유형:<br>• DNS 도메인 일치<br>• DNS 서버 주소 일치<br>• SSID 일치<br>• URL 문자열 검색<br>• 인터페이스 유형 일치<br>• 도메인<br>• DNS 서버<br>• URL 조사<br><br>요청 시 퍼앱 VPN을 활성화하려면 선택합니다. |
| 5G 네트워크 슬라이싱 활성화 | 특정 셀룰러 슬라이스 VPN을 대상으로 터널링하기 위해 네트워크 제공자가 제공한 **DNN**(데이터 네트워크 이름)을 선택합니다.<br>**앱 카테고리**(네트워크 제공자가 제공)를 선택하여 터널링할 셀룰러 슬라이스의 유형을 식별합니다. |
| **도메인** | |
| Safari 도메인(iOS)<br><br>**iOS 14.0+ 및 macOS 11.0+**<br><br>연결된 도메인 | 항목이 Safari에서 VPN 연결을 트리거하는 도메인을 각각 지정해야 하는 배열입니다. 각 엔트리는 www.apple.com 형식입니다.<br><br>하나 이상의 연결된 도메인을 지정합니다. 이들 도메인 중 하나에 있는 서버에 연결하면 퍼앱 VPN과 연결됩니다. |

| 설정 항목 | 설정하기 |
| --- | --- |
| 제외된 도메인 | 하나 이상의 제외된 도메인을 지정합니다. 이들 도메인 중 하나에 있는 서버에 연결하면 퍼앱 VPN에서 제외됩니다. |
| **iOS 13+ 및 macOS 10.15+** | |
| 메일 도메인 | **+ 추가**를 클릭하여 메일에서 이 VPN 연결을 트리거할 하나 이상의 도메인을 입력합니다. 각 엔트리는 www.apple.com 형식입니다. |
| 연락처 도메인 | **+ 추가**를 클릭하여 연락처에서 이 VPN 연결을 트리거할 하나 이상의 도메인을 입력합니다. 각 엔트리는 www.apple.com 형식입니다. |
| 달력 도메인 | **+추가**를 클릭하여 달력에서 이 VPN 연결을 트리거할 하나 이상의 도메인을 입력합니다. 각 엔트리는 www.apple.com 형식입니다. |
| **iOS 9 이상** | |
| 제공자 유형(iOS 9+) | 다음 터널 제공자 중 하나를 선택합니다.<br>• 앱 프록시 - 앱 레이어에서 터널 트래픽. 앱 프록시 제공자 개요는 Apple 문서를 참조하십시오.<br>• 패킷 터널 - IP 레이어에서 터널 트래픽. 패킷 터널 제공자 개요는 Apple 문서를 참조하십시오. |

## IPsec (Cisco)

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 시스템 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 사용자 PIN 포함 | 사용자가 PIN을 입력하도록 설정할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## Cisco AnyConnect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 그룹 | 연결 인증에 사용할 그룹을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### Juniper SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 영역 | 연결 인증에 사용될 인증 영역을 입력할 수 있습니다. |
| 역할 | 연결 인증에 사용될 인증 역할을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### NetMotion VPN

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | **인증서**는 사용할 사용자 인증 방법입니다. 다음 항목을 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. 사용자가 제공한 인증서는 iOS 기기에 대해서만 지원됩니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다.<br>다음 옵션을 선택합니다.<br>• 요청 시 VPN 활성화 - 요청 시 VPN을 설정하는 도메인 또는 호스트 이름 추가합니다.<br>• iOS 규칙을 활성화합니다.<br>• 요청 시 일치 앱이 활성화됨. |
| Safari 도메인 | **+ 추가**를 클릭하여 Safari 도메인을 추가할 수 있습니다. |
| 제공자 유형(iOS 9.0+) | **패킷 터널**은 기본적으로 터널 제공자 유형으로 선택됩니다.<br>패킷 터널 제공자 개요는 Apple 문서를 참조하십시오. |

## F5 SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## SonicWALL Mobile Connect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 로그인 그룹 또는 도메인 | 연결 인증에 사용될 로그인 그룹이나 도메인을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## Aruba VIA

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## 사용자 지정 SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 식별자 | 역방향 DNS 형식(예: com.mycompany.myserver)인 현재 사용자 지정 SSL VPN의식별자를 입력할 수 있습니다. |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 지정 데이터 | 현재 VPN의 사용자 지정 데이터를 정의하는 키- 값 쌍을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |
| (iOS 9.0+) 기본 및 하위 VPN 사전에 ProviderType 포함 | plist(사전 정의된 구성 파일)를 생성하는 동안 공급자 유형을 포함하도록 선택합니다. |
| 번들 식별자 제공 | VPN 제공업체의 번들 식별자를 입력하세요. 서로 다른 공급자 번들 식별자를 사용하여 동일한 앱에 대해 여러 앱 구성을 유지할 수 있습니다. |

## Palo Alto Networks GlobalProtect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다. * |
| 사용자 지정 데이터 | 현재 VPN의 사용자 지정 데이터를 정의하는 키- 값 쌍을 입력할 수 있습니다. |
| 사용자 인증 | 인증서는 사용자 인증 방법입니다.<br>**자격 증명** 필드에서 사용할 ID 인증서를 선택합니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

$를 입력하면 현재 필드에 해당하는 지원 변수 목록을 확인할 수 있습니다.

**관련 항목**:

구성을 생성하는 방법

# 10.10.6.13. Single Sign-On 설정

MDM용 Ivanti Neurons 는 확장형 SSO 및 확장형 SSO Kerberos 구성으로 확장형 Single Sign-On(SSO)을 활성화합니다. 구현하려면 ID 공급자의 앱 확장(예: Microsoft Authenticator)이 필요합니다. 확장형 SSO 구현과 함께 사용자는 엔터프라이즈 리소스에 액세스할 때 1번만 인증해야 합니다. 사용자에게 다음 로그인을 위해 인증하라는 메시지가 표시되지 않습니다. 대상 ID 공급자의 설정 정보에 대한 정보는 **ID 제공자 구성**을 참조하십시오.

이 섹션에는 다음 주제가 포함됩니다.

- **Single Sign-On 계정 설정**
- **확장형 Single Sign-On 계정 설정**
- **확장형 Single Sign-On Kerberos 계정 설정**

## Single Sign-On 계정 설정

**적용 가능 운영 체제:**

- iOS 7.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- visionOS 1.1부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

다음 설정을 사용하여 관리되는 앱과 Apple Safari 브라우저용 Kerberos 기반 엔터프라이즈 SSO를 iOS 기기에 구성합니다.

> 이 구성을 위해서는 Tunnel과 Sentry가 필요합니다. 자세한 내용은 *iOS용 Tunnel 가이드*의 "Kerberos로 싱글 사인온(SSO) 설정"을 참조하십시오.

| 설정 항목 | 설명 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 사용자 이름 | Kerberos 주요 이름을 입력합니다. |
| Kerberos 영역 이름 | Kerberos 영역 이름을 입력합니다. |
| 인증서 | **iOS 8, 골드 라이센스의 경우:** Kerberos 자격 증명을 갱신하려면 사용할 인증서를 선택합니다. |
| URL 접두사 일치 | 현재 계정을 이용해 HTTP로 Kerberos 인증을 하기 위해 반드시 일치해야 하는 URL 접두사 목록입니다. |
| SSO용 애플리케이션 허용 목록 지정 | App Catalog에서 앱을 추가하여 SSO에 대한 허용 목록으로 지정합니다.<br>예를 들어 "Safari"를 입력하여 Apple Safari를 추가하십시오.<br>이 구성 유형을 사용하는 SSO에 대해 허용 목록으로 지정된 앱이 없는 경우 기본 제공 iOS 앱을 포함해 iOS SSO를 지원하는 모든 앱은 SSO를 이용할 수 있습니다. |

## 확장형 Single Sign-On 계정 설정

**적용 가능 운영 체제:**

- iOS 13.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- macOS 10.15부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

- visionOS 1.1부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

다음 설정을 사용하여, 다양한 인증 방법으로 기본 앱과 웹 사이트에 대한 SSO를 활성화하도록 일반 확장 유형으로 SSO 확장 프로필을 구성합니다.

> 확장형 SSO는 macOS 10.15.x 기기에 대해 사용자 채널에서 구성이 푸시되는 경우 작동하지 않습니다.

| 설정 항목 | 설명 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| SSO 유형 선택 | 다음 SSO 유형 중 하나를 선택합니다.<br>• **자격 증명**<br>◦ 앱 확장을 통해 인증될 수 있는 하나 이상의 **호스트** 이름 또는 도메인 이름을 입력합니다. 호스트 또는 도메인 이름은 일치하는 대/소문자를 구분하지 않고 설치된 모든 확장형 SSO 페이로드의 모든 호스트/도메인 이름은 고유해야 합니다. "."로 시작하는 호스트 와일드카드 접미사이며 모든 하위 도메인과 일치합니다. 그렇지 않으면 호스트가 정확히 일치해야 합니다.<br>◦ **영역** 이름을 입력합니다. 이 값은 적절하게 대문자로 표기되어야 합니다.<br>• **리디렉션**<br>◦ 앱 확장이 SSO를 수행하는 ID 공급자의 **URL** 접두사 하나 이상을 입력합니다. URL은 http:// 또는 https://로 시작해야 하고, 체계와 호스트 이름은 일치하는 대/소문자를 구분하지 않으며, 쿼리 매개변수와 URL 조각은 허용되지 않고, 설치된 모든 확장형 SSO 페이로드의 URL은 고유해야 합니다. |
| 확장 식별자 | 지정된 URL에 대해 SSO를 수행하는 앱 확장의 번들 식별자를 입력합니다. |
| 팀 식별자 | 앱 확장의 팀 식별자.<br>이 키는 macOS에 필요하고 그 외에는 무시됩니다. |
| 사용자 지정 데이터 | 하나 이상의 사용자 지정 데이터를 키-값 쌍으로 입력합니다. |
| 인증 방법 (macOS 13 이상에만 적용 가능) | • 비밀번호<br>• 사용자 보안 엔클레이브 키 |
| 등록 토큰 | 토큰을 입력합니다.<br>인증 방법 중 하나를 선택하면 이 필드가 활성화됩니다. |
| 화면 잠금 동작 (iOS 15.0+ 및 macOS 12.0+에 적용) | 다음 옵션 중 하나를 선택합니다.<br>• **취소**: 화면이 잠기면 시스템이 인증 요청을 취소합니다.<br>• **취급 안 함**: 화면이 잠겨 있으면 SSO 없이 인증 요청이 계속됩니다. |
| 거부된 번들 식별자 (iOS 15.0+ 및 macOS 12.0+에 적용) | 이 확장 프로그램에서 제공하는 SSO를 사용하지 않는 앱의 여러 번들 식별자를 추가합니다. 예: *com.company.appname.www.* |

**적용 대상:** iOS 14.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

| 설정 항목 | 설명 |
| --- | --- |
| 계정 표시 이름 | 알림 및 인증 요청에 표시될 계정의 이름을 입력하십시오. |
| 추가 그룹 | 관리자 액세스 권한을 부여하지 않을 그룹의 이름을 입력하십시오. |
| 관리자 그룹 | 관리자 액세스 권한이 있는 그룹의 이름을 입력하십시오. |
| 인증 방법 | 드롭다운 목록에서 인증 방법 중 하나를 선택합니다.<br>• 비밀번호<br>• 사용자 보안 엔클레이브 키<br>• 스마트 카드 |
| 승인 그룹 | 그룹 이름에 대한 승인 권한을 입력하십시오. |
| 승인 활성화 | 관리자 그룹, 인증 그룹 또는 추가 그룹에 대한 인증 프롬프트를 활성화하려면 확인란을 선택합니다. |
| 로그인 시 사용자 생성 활성화 | 비밀번호나 스마트 카드를 인증 방법으로 사용하여 로그인 중에 신규 사용자를 생성하려면 확인란을 선택합니다. |
| 로그인 빈도 | 시스템에서 새로 고침 대신 전체 로그인이 필요할 때까지의 기간(초)입니다.<br>기본값은 64,800(18시간)입니다. 최소값은 3600(1시간)입니다. |
| 새로운 사용자 인증 모드 | 드롭다운 목록에서 신규 사용자에 대한 인증 모드 중 하나를 선택합니다.<br>• 표준: 계정은 표준 사용자를 위한 것입니다.<br>• 관리자: 시스템이 로컬 관리자 그룹에 계정을 추가합니다.<br>• 그룹: 시스템이 관리자 그룹, 인증 그룹 또는 추가 그룹 아래에 신규 사용자를 자동으로 그룹화합니다. |
| 토큰-사용자 간 매핑 | 인증을 위해 매핑할 신규 사용자의 계정 이름과 전체 이름을 입력합니다. |
| 사용자 인증 모드 | 드롭다운 목록에서 사용자에 대한 인증 모드 중 하나를 선택합니다.<br>• 표준: 계정은 표준 사용자를 위한 것입니다.<br>• 관리자: 시스템이 로컬 관리자 그룹에 계정을 추가합니다.<br>• 그룹: 시스템이 관리자 그룹, 인증 그룹 또는 추가 그룹 아래에 신규 사용자를 자동으로 그룹화합니다. |
| 공유 장치 키 사용 | 모든 사용자에게 동일한 로그인 및 암호화 키를 활성화하려면 확인란을 선택합니다. |

**적용 대상**: macOS 15.4부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

| 설정 항목 | 설명 |
| --- | --- |
| 장치 식별자 증명 허용 | 플랫폼 SSO 증명에 기기의 UDID와 일련 번호를 포함하려면 확인란을 선택하여 등록된 기기의 백엔드 추적을 허용합니다. |

**적용 대상:** iOS 14.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

확장형 싱글 사인온(SSO) 계정 설정을 보려면 **인증 방법** 필드에서 드롭다운 옵션을 **비밀번호**로 선택하십시오

| 설정 항목 | 설명 |
| --- | --- |
| FileVault 정책 | 다음 설정을 보려면 정책을 활성화합니다.<br>• 인증 시도<br>• 인증 필요<br>추가 구성 설정을 활성화하려면 **인증 필요** 확인란을 선택합니다.<br>• 오프라인 유예 기간 허용<br>• 인증 유예 기간 허용 |
| 로그인 정책 | 다음 설정을 보려면 정책을 활성화합니다.<br>• 인증 시도<br>• 인증 필요<br>추가 구성 설정을 활성화하려면 **인증 필요** 확인란을 선택합니다.<br>• 오프라인 유예 기간 허용<br>• 인증 유예 기간 허용 |
| 잠금 해제 정책 | 다음 설정을 보려면 정책을 활성화합니다.<br>• 인증 시도<br>• 인증 필요<br>추가 구성 설정을 활성화하려면 **인증 필요** 확인란을 선택합니다.<br>• 오프라인 유예 기간 허용<br>• 인증 유예 기간 허용<br>• TouchID 허용 또는 잠금 해제 감시 |
| 인증 유예 기간 | 등록되지 않은 로컬 계정을 사용하기 위해 정책 중 하나를 선택한 후 시간을 입력합니다.<br>정책 중에서 **인증 유예 기간 허용** 확인란을 선택하면 필수 필드가 됩니다. |
| 오프라인 유예 기간 | 플랫폼 SSO에 무사히 로그인한 후 오프라인 로컬 계정 비밀번호를 사용하기 위해 정책 중 하나를 선택한 후 시간을 입력합니다.<br>정책 중에서 **오프라인 유예 기간 허용** 확인란을 선택하면 필수 필드가 됩니다. |
| 비 플랫폼 SSO 계정 | **+추가**를 선택하여 FileVault, 로그인 또는 잠금 해제 정책이 적용되지 않는 사용자 이름 목록을 입력합니다. |

## 확장형 Single Sign-On Kerberos 계정 설정

**적용 가능 운영 체제:**

- iOS 13.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- macOS 10.15부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- visionOS 1.1부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

Kerberos 확장으로 SSO를 수행하는 앱 확장을 구성하려면 다음 설정을 사용합니다.

> 확장형 SSO Kerberos는 macOS 10.15.x 기기용 사용자 채널에서 구성이 푸시될 때 작동하지 않습니다.

| 설정 항목 | 설명 |
| --- | --- |
| **기본 설정** | |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 사용자 이름 | Kerberos 주요 이름을 입력합니다. |
| 영역 | Kerberos 영역 이름을 입력합니다. |
| 인증서 | Kerberos 자격 증명을 갱신하려면 사용할 자격 증명을 선택합니다. |
| URL 접두사 | 현재 계정을 이용해 HTTP로 Kerberos 인증을 하기 위해 반드시 일치해야 하는 URL 접두사 목록입니다. |
| **고급 설정** | |
| 자동 로그인 허용 | False인 경우에는 키체인에 비밀번호를 저장할 수 없습니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 사용자 설정 지연 | True인 경우에는 관리자가 앱 SSO 도구로 활성화하거나 Kerberos 챌린지가 수신될 때까지 Kerberos 확장을 설정하도록 사용자에게 요구하지 않습니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 11 이상 최신 버전에 적용됩니다. |
| 사용자 현재 상태 요구 | True인 경우에는 키체인 항목에 액세스하려면 Touch ID, Face ID 또는 암호를 입력할 것을 사용자에게 요구합니다. |
| 자격 증명 캐시 모니터링 | False인 경우에는 다음으로 일치하는 Kerberos 챌린지 또는 네트워크 상태 변경에서 자격 증명이 요청됩니다. 자격 증명이 만료 또는 분실된 경우에는 새 자격 증명이 생성됩니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 11 이상 최신 버전에 적용됩니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 캐시 이름 | 사용할 Kerberos 캐시의 일반 보안 서비스(GSS) 이름을 입력합니다. 이제 이 옵션은 사용하지 않습니다. |
| 도메인 영역 매핑 | 영역 이름을 키로 입력합니다. 값은 영역에 매핑되는 DNS 접미사의 배열입니다.<br>하나 이상의 키-값 쌍을 추가하려면 **+추가**를 클릭합니다. |
| 기본 영역 | 이 속성은 Kerberos 확장 구성이 여러 개인 경우 기본 영역을 지정합니다. |
| 사이트 자동 검색 사용 | False인 경우 Kerberos 확장은 AD 사이트 이름을 결정하기 위해 LDAP 및 DNS를 자동으로 사용하지 않습니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 사이트 코드 | Kerberos 확장이 사용해야 하는 Active Directory 사이트의 이름을 입력합니다. |
| 복제 시간 | Active Directory 도메인에서 변경 사항을 복제하는 데 필요한 초 단위 시간을 입력합니다. Kerberos 확장은 변경 후 비밀번호 사용기간을 확인할 때 이 값을 사용합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 11 이상 최신 버전에 적용됩니다. 이제 이 옵션은 사용하지 않습니다. |
| 자격 증명 번들 ID ACL | 인증을 위해 Ticket Granting Ticket(TGT)에 액세스할 수 있는 번들 ID 목록을 추가하려면 **+추가**를 클릭합니다. |
| 번들 ID ACL에 관리 앱 포 | True인 경우 Kerberos 확장은 관리 앱에만 액세스 및 자격 증명 사용을 허용합니다. 자격 증명 번들 ID ACL도 포함됩니 |

| 설정 항목 | 설명 |
| --- | --- |
| 함 | 다(지정된 경우). 이 옵션은 iOS 14에 적용되거나 MDM용 Ivanti Neurons 새로운 버전을 지원합니다. |
| 번들 ID ACL에 Kerberos 앱 포함 | true인 경우 Kerberos 확장자는 자격 증명 액세스 및 사용을 위해 Ticket Viewer 및 klist를 포함한 표준 Kerberos 유틸리티를 허용합니다. macOS 12 이상에서 사용 가능. |
| 사용자 지정 사용자 이름 레이블 | '사용자 이름' 대신 Kerberos 확장자에 사용된 사용자 정의 사용자 이름 레이블을 입력합니다(예: '회사 ID'). 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 11 이상 최신 버전에 적용됩니다. |
| 도움말 텍스트 | 사용자의 Kerberos 로그인 창 하단에 표시되는 텍스트를 입력합니다. 도움말 정보 또는 법적 고지 텍스트를 표시하는 데 사용할 수 있습니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 iOS 14 및 macOS 11 이상 최신 버전에 적용됩니다. |
| 자격 증명 사용 모드 | 이 설정은 다른 프로세스에서 Kerberos 확장 자격 증명을 사용하는 방식에 영향을 미칩니다. 다음 중 하나를 사용합니다.<br>• 항상(기본값) - 확장 자격 증명은 서비스 사용자 이름(SPN)이 Kerberos 확장 호스트 배열과 일치하는 경우 항상 사용됩니다. 자격 증명은 호출하는 앱이 credentialBundleIDACL에 있지 않은 경우 사용되지 않습니다.<br>• 지정되지 않을 때 - 자격 증명은 호출자가 다른 자격 증명을 지정하지 않았고 SPN이 Kerberos 확장 호스트 배열과 일치하는 경우에만 사용됩니다. 자격 증명은 호출하는 앱이 credentialBundleIDACL에 있지 않은 경우 사용되지 않습니다.<br>• Kerberos 기본값 - 자격 증명을 선택하는 기본 Kerberos 프로세스가 사용되는데, 이 프로세스는 보통 기본 Kerberos 자격 증명을 사용합니다. 이는 이 기능을 끄는 것과 동일합니다.<br>(선택 사항) **LDAP용 TLS 필요**를 선택합니다. |
| 선호하는 키 배포 센터 | 선호하는 키 배포 센터를 추가합니다.<br>선호하는 KDC를 추가하려면 **+추가**를 클릭합니다. |
| | **플랫폼 SSO 인증 폴백 허용** - 이를 True로 설정하고 플랫폼 SSO TGT 사용이 True로 설정됐다면 사용자가 수동으로 로그인할 수 있습니다. macOS 13 이상에서 사용 가능<br><br>**Kerberos만 수행** - True로 설정할 경우 Kerberos 확장이 Kerberos 요청만 처리합니다. macOS 13 이상에서 사용할 수 있습니다.<br><br>**플랫폼 SSO TGT 사용** - True로 설정할 경우 이 구성이 플랫폼 SSO에서 신규 요청 대신 TGT를 사용합니다. macOS 13 이상에서 사용할 수 있습니다. |
| 비밀번호 모드로 전환 구성 | True인 경우 사용자가 사용자 인터페이스를 비밀번호 모드로 전환할 수 있습니다. macOS 15 이상에서 사용할 수 있습니다. |
| 스마트카드 모드로 전환 구성 | True인 경우 사용자가 사용자 인터페이스를 스마트 카드 모드로 전환할 수 있습니다. macOS 15 이상에서 사용할 수 있습니다. |
| 스마트카드 모드로 시작 구성 | True인 경우사용자 인터페이스가 스마트 카드 모드에서 시작됩니다. macOS 15 이상에서 사용할 수 있습니다. |

| 설정 항목 | 설명 |
| --- | --- |
| ID 발급자 자동 선택 필터 | 사용 가능한 스마트 카드 목록을 필터링합니다. macOS 15 이상에서 사용할 수 있습니다. |
| **비밀번호 설정** | |
| 비밀번호 변경 허용 | False인 경우 비밀번호 변경을 비활성화합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 비밀번호 변경 URL | 이 URL을 입력하면 이 URL이 비밀번호 변경을 초기화할 때 사용자의 기본 웹 브라우저에서 실행됩니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. |
| 비밀번호 복잡도 허용 | true인 경우 비밀번호는 Active Directory의 '복잡함' 정의를 충족해야 합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. |
| 최소 비밀번호 길이 | 도메인에서 비밀번호의 최소 길이(단위: 문자)를 입력합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. |
| 비밀번호 만료 알림 | 비밀번호 만료 알림이 사용자에게 전송되는 비밀번호 만료 날짜까지 남은 일 수를 입력합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다.<br>기본값은 15일입니다. |
| 비밀번호 만료 재정의 | 비밀번호를 이 도메인에서 사용할 수 있는 일 수를 입력합니다. 대부분의 도메인에서 이 일 수는 자동으로 계산될 수 있습니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. (이 옵션은 서비스 중단되었습니다.) |
| 비밀번호 필수 텍스트 | 도메인의 비밀번호 요구 사항 텍스트 버전을 입력합니다. pwReqComplexity 또는 pwReqLength가 지정되지 않은 경우에만 사용 가능합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. |
| 비밀번호 히스토리 수 | 이 도메인에서 사용할 수 없는 이전 비밀번호 수를 입력합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. |
| 비밀번호 최소 기간 | 비밀번호를 이 도메인에서 변경할 수 있기까지 사용해야 하는 최소 기간(단위: 일수)을 입력합니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. |
| 로컬 비밀번호 동기화 허용 | False인 경우 비밀번호 동기화를 비활성화합니다.<br>이는 사용자가 모바일 계정으로 로그인되는 경우 작동하지 않습니다. 이 옵션은 MDM용 Ivanti Neurons에서 지원하는 macOS 10.15 이상 최신 버전에 적용됩니다. |
| 비밀번호 요구 사항 RTF 데이터 | 도메인의 비밀번호 요건에 대한 RTF 파일 형식 버전입니다. macOS 15 이상에서 사용할 수 있습니다.<br>pwReqComplexity 또는 pwReqLength가 지정되지 않은 경우에만 사용 가능합니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.6.14. 네트워크 릴레이 구성

MDM용 Ivanti Neurons 는 VPN이나 터널의 필요 없이 사설 리소스에 액세스하기 위해 장치나 애플리케이션의 릴레이 설정 구성에 사용하는 페이로드에 네트워크 릴레이 구성을 이용합니다.

**적용 대상**

- iOS 17.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- macOS 14부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- visionOS 1.1부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **네트워크 릴레이** 구성을 검색하고 선택합니다.
3. 다음 표에 따라 **네트워크 릴레이** 설정을 구성합니다.

| 설정 항목 | 설명 |
|---|---|
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **HTTP/3 릴레이 URL** | 이 구성에서 HTTP 필드 값으로 사용할 URL 값을 지정합니다.<br>HTTP/2 릴레이 URL 또는 HTTP/3 릴레이 URL 중 어느 하나 혹은 둘 다 포함할 수 있습니다. |
| **HTTP/2 릴레이 URL** | 이 구성에서 HTTP 필드 값으로 사용할 URL 값을 지정합니다.<br>HTTP/2 릴레이 URL 또는 HTTP/3 릴레이 URL 중 어느 하나 혹은 둘 다 포함할 수 있습니다. |
| **추가 HTTP 헤더 필드** | 해당 헤더 필드 이름에 대한 HTTP 헤더 필드 값을 지정합니다. |
| **인증서** | 드롭다운 목록에서 생성한 ID 인증서 중 하나를 선택합니다. |
| **원시 공개 키** | 네트워크 연결 도중에 서버를 인증하기 위한 원시 공개 키를 지정합니다. |
| **+ 추가** | 여러 네트워크 릴레이 구성을 추가하려면 **+ 추가**를 선택합니다. |
| **도메인 일치** | 릴레이에서 서버를 통해 라우팅할 연결을 결정하려면 도메인 목록을 지정합니다. |
| **도메인 제외** | 릴레이에서 서버를 통해 피해야 할 연결을 결정하려면 도메인 목록을 지정합니다. |
| **FQDN 일치**(iOS 18.4 이상, macOS 15.4 이상 기기에서 지원됨) | 호스트 이름이라고도 알려진 정규화된 도메인 이름(FQDN) 목록을 지정합니다. 이는 릴레이에 포함된 서버를 통해 라우팅되어야 합니다. 정확히 이 FQDN 또는 호스트 이름과 일치하는 연결은 릴레이를 사용합니다. 목록에 FQDN 및 'MatchDomains'가 없으면, 제외된 도메인 또는 제외된 FQDN과 일치하는 도메인을 제외한 모든 도메인 대상 트래픽은 릴레이 서버로 라우팅됩니다. |
| **FQDN 제외**(iOS 18.4 이상, macOS 15.4 이상 기기에서 지원됨) | 호스트 이름이라고도 알려진 정규화된 도메인 이름(FQDN) 목록을 지정합니다. 이는 릴레이에 포함된 서버를 통해 라우팅되지 **않아야** 합니다. FQDN과 정확하게 일치하는 연결은 릴레이 서버를 사용하지 않습니다.<br>'MatchDomains'도 지정되어 있다면, 'ExcludedFQDNs'에 나열된 FQDN은 하나 이상의 MatchDomain의 하위 도메인이어야 합니다. 그렇지 않으면 이는 적용되지 않습니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. **네트워크 릴레이** 구성을 설정하려면 배포 옵션 중 하나를 선택하십시오. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.6.15. iOS용 다중 사용자 보안 로그인

다중 사용자 웹 클립을 활용하면 사용자는 MDM용 Ivanti Neurons에 등록된 iOS 기기에서 로그인 및 로그아웃할 수 있습니다. 사용자가 처음으로 로그인하는 경우 그 사용자와 연관된 프로필, 앱 및 구성이 기기에 푸시됩니다. 작업을 마치면 웹 클립을 열어 "로그아웃" 기능을 선택할 수 있습니다. 이는 구성과 앱이 Nobody 사용자에게 배포되지 않는다면 기기를 Nobody 사용자에 할당하고 처음에 로그인했던 사용자와 연관된 프로필, 앱 및 구성을 제거합니다. 로그아웃 이후 웹 클립은 다음 사용자가 로그인하여 사용자 지정 구성, 앱 및 정책을 받을 수 있도록 재설정됩니다. 기기 감독은 다중 사용자 보안 로그인 기능을 사용할 필요가 없습니다. 다중 사용자 로그인 기능을 자세히 살펴보려면 지원팀 기술 자료 문서, **MDM용 Ivanti Neurons: iOS용 다중 사용자 보안 로그인**을 참조하십시오.

**적용 대상:** iOS 기기(사용자 등록 기기에는 적용되지 않음)

이 섹션에는 다음 주제가 포함됩니다.

- 지원되는 자격 증명
- Nobody 사용자에 대한 이해
- 기기 로그인
- 기기 로그아웃

## 지원되는 자격 증명

다중 사용자 보안 웹 클립에 로그인하려면 사용자 이름과 비밀번호를 사용해야 합니다. 다중 사용자 보안 웹 클립에서는 PIN 기반 등록을 지원하지 않습니다.

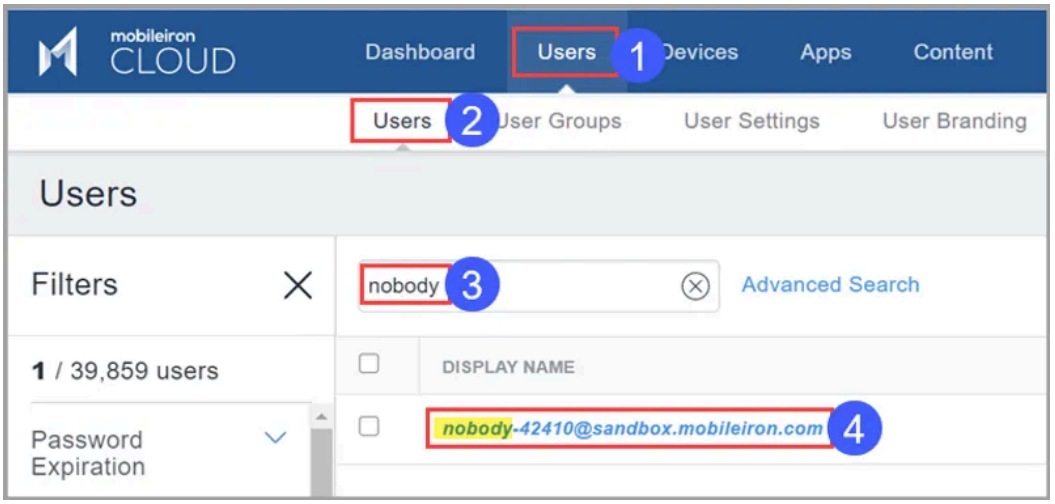
**절차**

1. **구성**으로 이동합니다.
2. **iOS용 다중 사용자 보안 로그인**을 클릭합니다. 여러 페이지의 구성이 있는 경우 이를 찾으려면 검색 기능을 사용해야 할 수 있습니다. 이 구성은 **+추가**를 선택하여 액세스되지 않습니다.
3. 웹 클립을 적합한 기기 그룹에 배포하려면 **배포 편집** 또는 관련 아이콘을 클릭합니다.
   
   이를 사용자 그룹에 배포하고자 하면 사용자 그룹과 연결된 동적 기기 그룹을 만들 수 있습니다.
4. 웹 클립을 항상 Nobody 사용자에 배포하거나 Nobody 사용자가 연결되어 있는 기기 그룹에 배포해야 한다는 것을 유념하면서 다음 배포 옵션 중 하나를 선택합니다. 이는 기본적으로 발생하지 않으므로 Nobody 사용자에 배포되는지 확인해야 합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정

**저장**을 클릭합니다.

## *Nobody* 사용자에 대한 이해

웹 클립을 통해 기기에서 로그아웃한 경우, Nobody 사용자라고 불리는 특수 사용자로 MDM용 Ivanti Neurons에 등록된 상태로 남게 됩니다. 사용자 로그아웃 시 기기에서 앱과 구성을 제거하고자 하는 경우 이 앱과 구성이 Nobody 사용자에게 배포되어 있지 않은지 확인해야 합니다. 사용자가 보안 로그인 웹 클립에서 로그아웃할 때 기기에 계속 남을 수 있도록 Wi-Fi 같은 특정 구성을 원하는 경우 이 구성이 Nobody 사용자에게도 배포되어 있는지 확인해야 합니다.




즉 앱과 구성을 배포하는 사용자 그룹과 기기 그룹에 주의를 기울여야 합니다. 앱을 모두에 배포 중이고 기기에서 로그아웃 시 이를 삭제하고자 한다면 Nobody 사용자를 포함하지 않는 사용자 그룹을 만드는 것이 최선의 방법입니다. 사용자 지정 속성 덕분에 "다중 사용자"인 사용자 그룹과 Nobody 사용자로만 구성된 다른 사용자 그룹을 만드는 것이 훨씬 더 쉽습니다. "다중 사용자 소유자"라고 불리는 관리 > 시스템 > 속성을 통해 사용자 속성을 만든 후 "Yes" 또는 "True" 값을 Nobody 사용자에게 할당할 수 있습니다. 그 다음에 속성 값에 기반하여 사용자 그룹과 기기 그룹을 만들 수 있습니다. 그 다음에 속성 값에 기반하여 사용자 그룹과 기기 그룹을 만들 수 있습니다.

## 기기 로그인

사용자는 iOS 기기에 로그인하여 자신에게 기기를 지정할 수 있습니다. 로그인하면 관련 애플리케이션, 정책, 구성, 인증서가 모두 이 기기로 푸시됩니다.

> 보안상의 이유로, iDP 사용자는 기기에 이미 로그인되어 있더라도 로그인할 때마다 재인증을 해야 합니다.

## 기기 로그아웃

사용 후 iOS 기기에서 로그아웃할 수 있습니다. 로그아웃 하면 기기에서 관련 애플리케이션, 정책, 구성, 인증서가 모두 삭제되어 기기가 로그인 전 상태로 복구됩니다. 이후 다른 사용자가 로그인할 수 있습니다.

> 다중 사용자 웹 클립에서 로그아웃하기 전에 모든 Microsoft 앱에서 로그아웃하세요.

자세한 내용은 **다중 사용자 로그인 브랜딩**을 참조하십시오.

# 10.10.6.16. Android APN 설정 구성

Android APN 설정 구성을 통해 공개 네트워크 상의 기기에서 필요한 액세스 지점 이름(APN) 설정을 설정할 수 있습니다. 이 구성은 Android Enterprise 업무 관리 기기 및 회사 소유 기기에 작업 프로필이 있는 관리 기기(Android 버전 9.0 또는 지원되는 최신 버전)에 적용됩니다.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **Android APN 설정** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 옵션을 구성합니다.
6. **다음**을 클릭하세요.

| 설정 | 설명 |
| --- | --- |
| **엔트리 이름** | 액세스 지점 설정 이름을 입력합니다. |
| **액세스 지점 이름** | 액세스 지점 이름을 입력합니다. |
| **액세스 지점 유형** | 다음 옵션에서 액세스 지점 유형을 선택합니다.<br>• **기본**<br>• **DUN**<br>• **IMS**<br>• **긴급**<br>• MMS<br>• **HIPRI**<br>• **CBS**<br>• **MCX**<br>• **SUPL**<br>• **FOTA**<br>• **IA** |
| **MVNO 유형** | 다음 옵션에서 모바일 가상 네트워크 운영자 유형을 선택합니다.<br>• **없음**<br>• **SPN**<br>• **IMSI**<br>• **GID**<br>• **ICCID** |
| **Bearer** | 다음 옵션에서 데이터 전송에 사용되는 서비스 전달자 유형을 선택합니다.<br>• **1xRTT**<br>• **CDMA**<br>• **EDGE**<br>• **EHRPO**<br>• **EVDO**<br>• **EVDO A**<br>• **EVDO B**<br>• **GPRS**<br>• **GSM**<br>• **HSDPA**<br>• **HASP**<br>• **HSPAP**<br>• **HSUPA**<br>• **IDEN** |

| 설정 | 설명 |
| --- | --- |
| | • **IWLAN**<br>• **LTE**<br>• **NR**<br>• **TD_SCDMA**<br>• **UMTS** |
| **APN 프로토콜** | APN에 필요한 APN 프로토콜을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.<br>• **없음**<br>• **IPV4**<br>• **IPV6**<br>• **IPV4/IPV6**<br>• **NON_IP**<br>• **PPP**(지점간 프로토콜)<br>• **비정형** |
| **APN 로밍 프로토콜** | APN에 필요한 APN 로밍 프로토콜을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.<br>• **없음**<br>• **IPV4**<br>• **IPV6**<br>• **IPV4/IPV6**<br>• **NON_IP**<br>• **PPP**(지점간 프로토콜)<br>• **비정형** |
| **APN 활성화/비활성화** | APN 구성을 켭니다. |
| **통신사 ID** | 통신사 ID의 숫자 값을 입력합니다. |
| **인증 유형** | 다음 옵션에서 인증 프로토콜 유형을 선택합니다.<br>• **없음**<br>• **PAP**(암호 인증 프로토콜)<br>• **CHAP**(Challenge-Handshake 인증 프로토콜)<br>• **PAP 또는 CHAP** |
| **사용자 이름** | 로그인 사용자 이름을 입력합니다. |
| **비밀번호** | 로그인 비밀번호를 입력합니다. |
| **비밀번호 확인** | 확인을 위해 비밀번호를 다시 입력합니다. |
| **포트 번호** | 포트 번호를 입력합니다(1 ~ 65535의 숫자값). |
| **프록시 주소** | 프록시 주소를 입력합니다. |

| 설정 | 설명 |
| --- | --- |
| **모바일 국가 코드** | 모바일 국가 코드를 입력합니다. |
| **모바일 네트워크 코드** | 모바일 네트워크 코드를 입력합니다. |
| **MMS 프록시 주소** | MMS 프록시 주소를 입력합니다. |
| **MMS 포트 번호** | MMS 포트 번호를 입력합니다(1 ~ 65535의 숫자값). |
| **MMS 서버 주소(mmsc)** | MMS 서버 주소를 입력합니다. |

7. 다음 배포 옵션 중 하나를 선택합니다.
8. **완료**를 클릭하세요.

- **모든 기기**
- 배포 안 함(기본값)
- **사용자 지정**

> 기기에 대해 이 값을 가진 기존 APN 구성이 있을 경우에는 다음 필드에 대해 동일한 값의 또 다른 APN 구성을 추가할 수 없습니다.

- 모바일 국가 코드
- 모바일 네트워크 코드
- 액세스 지점 이름
- 프록시 주소
- 포트 번호
- MMS 프록시 주소
- MMS 포트 번호
- MMS 서버 주소
- APN 활성화/비활성화
- MVNO 유형
- APN 프로토콜
- APN 로밍 프로토콜

Android APN 설정 구성은 수동으로, 또는 네트워크 운영자에 의해 기기에 이미 구성되어 있는 경우 APN 설정을 재정의합니다.

# 10.10.6.17. VPN 구성

**적용 가능 운영 체제:**

- Android(Android Enterprise 기기에서는 더 이상 사용되지 않음. 앱 카탈로그에서 특정 VPN에 대한 관리형 구성을 사용해야 합니다.)
- Windows
- iOS
- macOS
- tvOS
- visionOS

가상 사설 네트워크 접속에 필요한 VPN 설정을 할 수 있습니다.

> 이 구성에는 사용자 지정 배포 옵션을 사용한 위임을 사용할 수 있습니다. 자세한 정보는 구성 작업에서 *구성 배포* 항목을 참조하십시오.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **VPN** 구성을 선택합니다.
3. 구성 **이름**을 입력합니다.
4. 설명을 입력합니다.
5. 다음 설명에 따라 VPN 설정을 구성합니다.
6. (iOS 9.0+ 전용) 일치 도메인 섹션에서 **+추가**를 클릭하여 하나 이상의 일치 도메인(예: company.com)으로 들어갑니다. 도메인이 지정된 도메인 중 하나일 경우 프록시 연결을 사용합니다.
7. **다음**을 클릭하세요.
8. (macOS 전용) 배포 페이지에서 다음 배포 옵션 중 하나를 선택합니다.
    - 기기 채널 - 구성은 기기의 모든 사용자에게 효과적이며 일반적인 옵션입니다.
    - 사용자 채널 - 구성은 기기에 현재 등록된 사용자에게만 효과적입니다.
9. 이 구성의 나머지 배포 옵션을 선택합니다.
10. **완료**를 클릭하세요.

## VPN 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| **이름** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **연결 유형** | 설정할 VPN 유형을 선택할 수 있습니다.<br>선택한 유형에 따라 나머지 설정 항목이 달라집니다. |

프로토콜 및 그 설정은 다음과 같습니다.

- L2TP(Ivanti Go에서 지원되지 않음)

- PPTP(Ivanti Go에서 지원되지 않음)
- IPsec(Cisco)(Ivanti Go에서 지원되지 않음)
- Cisco AnyConnect(Ivanti Go에서 지원됨)
- Juniper SSL(Ivanti Go에서 지원되지 않음)
- NetMotion VPN(Ivanti Go에서 지원되지 않음)
- Pulse Secure(Ivanti Go에서 지원)
- F5 SSL(Ivanti Go에서 지원되지 않음)
- SonicWALL Mobile Connect(Ivanti Go에서 지원되지 않음)
- Aruba VIA(Ivanti Go에서 지원되지 않음)
- 사용자 지정 SSL(Ivanti Go에서 지원되지 않음)
- Palo Alto Networks GlobalProtect(Ivanti Go에서 지원)
- KEv2(Windows 전용)(Ivanti Go에서 지원되지 않음)
- IKEv2(Ivanti Go에서 지원되지 않음)

## L2TP

| 설정 항목 | 설정하기 |
|---|---|
| **서버** | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| **계정** | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| **사용자 인증** | 사용할 인증 방법으로 **비밀번호** 또는 **RSA SecurID** 중 하나를 선택합니다. |
| **공유 비밀** | 필요한 경우 연결 초기화 시 공유 비밀 암호를 입력할 수 있습니다. |
| **모든 트래픽 보내기** | 모든 네트워크 트래픽에 현재 연결을 사용하도록 설정할 수 있습니다. 이 항목을 설정하면 특히 공개 네트워크 상에서의 데이터 손상을 방지할 수 있습니다. |
| **프록시 설정** | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## PPTP

| 설정 항목 | 설정하기 |
| --- | --- |
| **서버** | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| **계정** | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| **사용자 인증** | 사용할 인증 방법으로 **비밀번호** 또는 **RSA SecurID** 중 하나를 선택합니다. |
| **암호화 레벨**<br><br>**모든 트래픽 보내기** | 연결에 사용할 데이터 암호화 수준을 **없음, 자동** 또는 **최대(128비트)**로 설정할 수 있습니다.<br><br>모든 네트워크 트래픽에 현재 연결을 사용하도록 설정할 수 있습니다. 이 항목을 설정하면 특히 공개 네트워크 상에서의 데이터 손상을 방지할 수 있습니다. |
| **프록시 설정** | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## IPsec (Cisco)

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 시스템 인증 | 사용할 인증 방법을 **공유 비밀/그룹 이름** 또는 **인증서**로 설정할 수 있습니다. |
| 그룹 이름<br><br><br><br>공유 비밀 | 공유 비밀/그룹 이름 인증.<br>사용할 그룹의 이름을 지정할 수 있습니다. 하이브리드 인증을 사용할 경우에는 문자열을 반드시 â€œ[hybrid]â€로 종료해야 합니다.<br><br>공유 비밀/그룹 이름 인증.<br>공유 비밀 암호를 입력할 수 있습니다. |
| 하이브리드 인증 사용<br><br><br>비밀번호 확인<br><br><br>자격 증명 | 공유 비밀/그룹 이름 인증.<br>하이브리드 인증 관련 설정을 할 수 있습니다(예: 서버가 인증서를 제공하고 클라이언트가 사전 공유 키를 제공하도록 설정).<br><br>공유 비밀/그룹 이름 인증.<br>연결 시 사용자가 비밀번호를 입력해야 할지 여부를 설정할 수 있습니다.<br><br>*인증서 인증*<br>사용할 ID 인증서를 선택할 수 있습니다. |
| 사용자 PIN 포함 | *인증서 인증*<br>사용자가 PIN을 입력하도록 설정할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## Cisco AnyConnect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 그룹 | 연결 인증에 사용할 그룹을 입력할 수 있습니다. |
| 사용자 인증 | 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 설정할 수 있습니다.<br>**인증서**를 선택하면 다음과 같은 필드를 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### Juniper SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 영역 | 연결 인증에 사용될 인증 영역을 입력할 수 있습니다. |
| 역할 | 연결 인증에 사용될 인증 역할을 입력할 수 있습니다. |
| 사용자 인증 | 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 설정할 수 있습니다.<br>**인증서**를 선택하면 다음과 같은 필드를 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### NetMotion VPN

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 설정할 수 있습니다. **인증서**를 선택하면 다음과 같은 필드를 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### F5 SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다. * |
| 사용자 인증 | 사용할 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 입력합니다.<br>**인증서**를 선택하면 다음과 같은 필드를 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | 수동 또는 자동을 선택해 프록시 설정을 할 수 있습니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### SonicWALL Mobile Connect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 로그인 그룹 또는 도메인 | 연결 인증에 사용될 로그인 그룹이나 도메인을 입력할 수 있습니다. |
| 사용자 인증 | 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 설정할 수 있습니다.<br>인증서로 설정하면 다음과 같은 항목을 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## Aruba VIA

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 설정할 수 있습니다.<br>**인증서**를 선택하면 다음과 같은 필드를 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | 수동 또는 자동을 선택해 프록시 설정을 할 수 있습니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## 사용자 지정 SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 식별자 | 역방향 DNS 형식(예: com.mycompany.myserver)인 현재 사용자 지정 SSL VPN의식별자를 입력할 수 있습니다. |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 지정 데이터 | 현재 VPN의 사용자 지정 데이터를 정의하는 키- 값 쌍을 입력할 수 있습니다. |
| 사용자 인증 | 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 설정할 수 있습니다.<br>인증서로 설정하면 다음과 같은 항목을 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## Palo Alto Networks GlobalProtect

> Android 기기에는 적용되지 않습니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다. * |
| 사용자 지정 데이터 | 현재 VPN의 사용자 지정 데이터를 정의하는 키- 값 쌍을 입력할 수 있습니다. |
| 사용자 인증 | 사용자 인증 방법을 **비밀번호** 또는 **인증서**로 설정할 수 있습니다.<br>인증서로 설정하면 다음과 같은 항목을 설정할 수 있습니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## IKEv2(Windows 전용)

| 설정 항목 | 수행 작업 |
| --- | --- |
| 서버 | VPN 서버의 호스트 이름이나 IP 주소를 입력합니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### IKEv2

| 설정 항목 | 수행 작업 |
| --- | --- |
| **서버** | VPN 서버의 호스트 이름이나 IP 주소를 입력합니다. |
| **로컬 식별자** | 다음 형식 중 하나로 된 IKEv2 클라이언트의 식별자:<br>• FQDN<br>• UserFQDN<br>• 주소<br>• ASN1DN |
| **원격 식별자** | 다음 형식 중 하나로 된 원격 식별자:<br>• FQDN<br>• UserFQDN<br>• 주소<br>• ASN1DN |
| **시스템 인증** | **EAP 활성화**가 선택되지 않은 경우에만 사용 가능합니다.<br>다음 중 하나를 선택합니다.<br>• 인증서<br>• 공유 비밀 |
| **EAP 인증** | **EAP 활성화**가 선택된 경우에만 사용 가능합니다.<br>다음 중 하나를 선택합니다.<br>• 인증서<br>• 사용자 이름/비밀번호 |
| **공유 비밀** | 시스템 인증을 위한 공유 비밀이 선택되어 있는 경우에만 사용 가능합니다. 연결하려면 공유 비밀을 입력합니다. |
| **자격 증명** | 시스템 인증을 위한 인증서가 선택된 경우에만 사용 가능합니다. 사용할 인증서를 선택합니다. 이 인증서가 IKE 클라이언트 인증을 위해 전송됩니다. 확장된 인증을 사용하는 경우 이 인증서를 EAP-TLS용으로 사용할 수 있습니다. |
| **EAP 활성화** | 확장된 인증을 활성화하도록 선택합니다. |
| **계정** | EAP 인증을 위한 사용자 이름/비밀번호가 선택된 경우에만 사용 가능합니다. VPN 서버의 계정 ID를 입력합니다. |
| **비밀번호** | EAP 인증을 위한 사용자 이름/비밀번호가 선택된 경우에만 사용 가능합니다. VPN 서버의 비밀번호를 입력합니다. |
| **정지 피어 감시 주기** | 다음 옵션 중 하나를 선택합니다.<br>• 없음(비활성화)<br>• 낮음(킵얼라이브가 1시간마다 전송됨)<br>• 중간(킵얼라이브가 30분마다 전송됨)<br>• 높음(킵얼라이브가 10분마다 전송됨) |

| 설정 항목 | 수행 작업 |
| --- | --- |
| **서버 인증서 발급자 공통 이름** | (선택 사항) - 서버 인증서 발급자의 일반 이름으로, IKE 서버가 인증서 발급자를 기반으로 인증서 요청을 서버로 보냅니다. |
| **서버 인증서 공통 이름** | (선택 사항) - IKEv2 서버에서 보낸 인증서의 유효성을 검사하는 데 사용되는 서버 인증서의 일반 이름입니다. |
| **IP4와 IP6 서브넷 속성 사용** | (선택 사항) IP4 및 IP6 서브넷 속성을 사용하려면 선택합니다. |
| **IKEv2 모빌리티와 멀티호밍 프로토콜(MOBIKE) 활성화** | (선택 사항) 기본 설정은 0입니다. MOBIKE(Wi-Fi와 여러 IP 주소의 휴대폰 링크에 연결되는 경우 멀티 홈 모바일 기기를 지원하는 기능)가 활성화됩니다. 이것은 기본적으로 활성화됩니다. 1로 설정하면 MOBIKE가 비활성화됩니다. |
| **완벽한 전달 기밀(PFS) 활성화** | (선택 사항) 1로 설정하면 IKEv2 연결에 대해 PFS를 활성화합니다. 기본 설정은 0입니다. |
| **IKEv2 리디렉션 활성화** | (선택 사항) 기본 설정은 0입니다. 서버에서 리디렉트 요청을 수신하면 IKEv2 연결이 리디렉션됩니다. 이것은 기본적으로 활성화됩니다. 1을 설정해 IKEv2 리디렉션을 비활성화합니다. |
| **NAT keepalive 활성화** | IKE 피어 사이에 NAT가 있는 경우 트래픽 부재 시 NAT 입력의 삭제를 방지하도록 네트워크 주소 번역 킵얼라이브를 활성화합니다. |
| **NAT keepalive 간격** | NAT keepalive가 활성화된 경우 기기에 대한 keepalive 패킷이 전송되는 시간(초)입니다. |
| **PPK** | RFC 8784를 지원하는 VPN 서버에 포스트 퀀텀 사전 공유 키(PPK)를 입력합니다. 이 키가 있으면 PPK 식별자도 있어야 합니다. |
| **PPK 식별자** | PPK 식별자를 입력합니다. |
| **PPK 필수** | 다음 드롭다운 옵션 중 하나를 선택합니다.<br>• **위임**: 서버가 RFC 8784를 지원하거나 PPK 식별자에 지정된 PPK 식별자를 허용하는 경우 VPN 연결이 성공적으로 설정됩니다.<br>• **비위임**: 서버가 RFC 8784를 지원하지 않거나 PPK 식별자에 지정된 PPK 식별자를 허용하지 않으면 VPN 연결에 실패합니다. |
| **암호화 알고리즘** | 다음 옵션 중 하나를 선택합니다.<br>• **DES**<br>• **3DES**<br>• **AES-128**<br>• **AES-256**(기본)<br>• **AES-128 GCM**<br>• **AES-256 GCM** |

| 설정 항목 | 수행 작업 |
| --- | --- |
| **무결성 알고리즘** | 다음 옵션 중 하나를 선택합니다.<br>• **SHA2-256**(기본)<br>• **SHA2-384**<br>• **SHA2-512** |
| **디피 헬만 그룹** | 다음 옵션 중 하나를 선택합니다.<br>• **1**<br>• **2**(기본)<br>• **5**<br>• **14**<br>• **15**<br>• **16**<br>• **17**<br>• **18** |
| **분 단위 수명** | 분 단위 SA 수명(re-key 주기)을 입력합니다. 유효한 값은 10 ~ 1440입니다. |
| **프록시 설정** | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

*$를 입력하면 현재 칸에 해당하는 지원 변수 목록을 확인할 수 있습니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.6.18. VPN(요청 시)

**적용 가능 대상:** iOS 기기

요청 시 VPN 설정을 하면 도메인, 호스트 이름 등을 기준으로 원하는 VPN 서버에 접속할 수 있습니다.

## 요청 시 VPN 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 연결 유형 | 설정할 VPN 유형을 선택할 수 있습니다.<br>선택한 유형에 따라 나머지 설정 항목이 달라집니다. |
| 요청 시 VPN 활성화 | 요청 시 VPN을 설정하는 도메인 및 호스트 이름에 현재 설정을 사용하도록 설정할 수 있습니다. |
| iOS 규칙 활성화<br>(요청 시 VPN 활성화를 선택한 경우 적용) | iOS 및 macOS의 경우 다음을 설정할 수 있습니다.<br>• 진짜로 확인된 네트워크 연결을 허용/금지하거나 해당 네트워크를 허용/무시하는 네트워크 규칙입니다.<br>• 필요에 따라 진짜로 확인된 네트워크를 허용하거나 금지하거나 연결하는 연결 규칙입니다.<br>네트워크 규칙에서 지정할 수 있는 매개 변수 유형:<br>• DNS 도메인 일치<br>• DNS 서버 주소 일치<br>• SSID 일치<br>• URL 문자열 검색<br>• 인터페이스 유형 일치<br>연결 규칙에서 지정할 수 있는 매개 변수 유형:<br>• DNS 도메인 일치<br>• DNS 서버 주소 일치<br>• SSID 일치<br>• URL 문자열 검색<br>• 인터페이스 유형 일치<br>• 도메인 이름<br>• DNS 서버<br>• URL 조사 |
| 제공자 유형(iOS 9+) | 다음 터널 제공자 중 하나를 선택합니다.<br>• 앱 프록시 - 앱 레이어에서 터널 트래픽. 앱 프록시 제공자 개요는 **Apple 문서**를 참조하십시오.<br>• 패킷 터널 - IP 레이어에서 터널 트래픽. 패킷 터널 제공자 개요는 **Apple 문서**를 참조하십시오. |
| EnforceRoutes | 이 기능을 활성화하면, VPN의 기본이 아닌 경로가 로컬에서 정의된 모든 경로보다 우선합니다.<br>• IncludeAllNetworks가 활성화된 경우, 시스템은 EnforceRoutes 설정을 무시합니다.<br>• iOS 14.2 이상에서 사용 가능합니다. |
| ExcludeLocalNetworks | IncludeAllNetworks와 함께 이 기능을 활성화하면, 모든 로컬 네트워크 트래픽이 VPN 외부로 라우팅됩니다. |
| IncludeAllNetworks | 이 기능을 활성화하면 모든 트래픽이 VPN을 통해 라우팅됩니다. |

프로토콜 및 그 설정은 다음과 같습니다.

- IPsec (Cisco)
- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- 사용자 지정 SSL
- Palo Alto Networks GlobalProtect

## IPsec (Cisco)

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 시스템 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 사용자 PIN 포함 | 사용자가 PIN을 입력하도록 설정할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## Cisco AnyConnect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 그룹 | 연결 인증에 사용할 그룹을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### Juniper SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 영역 | 연결 인증에 사용될 인증 영역을 입력할 수 있습니다. |
| 역할 | 연결 인증에 사용될 인증 역할을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### NetMotion VPN

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | 인증서는 사용자 인증 방법입니다.<br>**자격 증명**: 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>**프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### F5 SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### SonicWALL Mobile Connect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 로그인 그룹 또는 도메인 | 연결 인증에 사용될 로그인 그룹이나 도메인을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## Aruba VIA

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

## 사용자 지정 SSL

| 설정 항목 | 설정하기 |
| --- | --- |
| 식별자 | 역방향 DNS 형식(예: com.mycompany.myserver)인 현재 사용자 지정 SSL VPN의식별자를 입력할 수 있습니다. |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다.* |
| 사용자 지정 데이터 | 현재 VPN의 사용자 지정 데이터를 정의하는 키- 값 쌍을 입력할 수 있습니다. |
| 사용자 인증 | 인증서 인증만 지원됩니다. |
| 자격 증명 | 사용할 ID 인증서를 선택할 수 있습니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

### Palo Alto Networks GlobalProtect

| 설정 항목 | 설정하기 |
| --- | --- |
| 서버 | VPN 서버의 IP 주소 또는 호스트 이름을 입력합니다. |
| 계정 | 연결 인증에 사용될 사용자 계정을 입력할 수 있습니다. * |
| 사용자 지정 데이터 | 현재 VPN의 사용자 지정 데이터를 정의하는 키- 값 쌍을 입력할 수 있습니다. |
| 사용자 인증 | 인증서는 사용자 인증 방법입니다.<br>**자격 증명** 필드에서 사용할 ID 인증서를 선택합니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>**자동을 선택하면** 다음과 같은 필드를 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |

$를 입력하면 현재 필드에 해당하는 지원 변수 목록을 확인할 수 있습니다.

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.6.19. Wi-Fi 구성

**적용 가능 운영 체제:**

- Android
- Windows
- iOS
- macOS
- watchOS
- visionOS
- tvOS

이 섹션에는 다음 주제가 포함됩니다.

**Wi-Fi 설정**

- **WEP, WPA/WPA2/WPA3, 임의(개인) 설정**
- **WEP 엔터프라이즈, WPA/WPA2/WPA3 엔터프라이즈, 임의(엔터프라이즈) 설정**
- **iOS, macOS, visionOS**

## Wi-Fi 설정

무선 네트워크 연결에 필요한 Wi-Fi 환경을 설정할 수 있습니다.

> 사용자는 기기에서 일부 Wi-Fi 설정을 수정할 수 있습니다. 단, MDM 서버는 기기 OS를 기반으로 한 변경 사항과 관련한 정보를 수신할 수도 있고 수신하지 않을 수도 있습니다. 따라서 자동으로 기기에 구성이 다시 푸시되어 기기 구성이 서버 구성으로 재정의되지 않습니다.

> 이 구성에는 사용자 지정 배포 옵션을 사용한 위임을 사용할 수 있습니다. 자세한 정보는 구성 작업에서 *구성 배포* 항목을 참조하십시오.

> 일부 특정 버전의 Android 장치에서는 관리자가 TLS, TTLS, PEAP 등에 연결하기 위해 도메인 및 추가 정보를 입력해야 할 수 있습니다. (WPA2) 네트워크. 더 큰 장치 집합에서 이러한 변경을 수행하기 전에 선택한 장치에서 Wi-Fi 구성을 변경했는지 확인하는 것이 좋습니다.

> 94 이전 MDM용 Ivanti Neurons 버전에 등록된 Android 14.x 장치는 '설치 보류 중' 상태의 구성 상태를 갖습니다. Wi-Fi 구성을 편집하지 않고 MDM용 Ivanti Neurons에서 94로 업그레이드하면 구성 상태가 '설치 보류 중' 상태로 유지됩니다. EAP_PEAP에 대한 도메인 필드를 활성화하고 구성에서 도메인 및 인증서를 업데이트하여 상태를 '설치됨' 상태로 업데이트해야 합니다.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **Wi-Fi** 구성을 선택합니다.
3. 구성 **이름**을 입력합니다.
4. 설명을 입력합니다.
5. 다음 설명에 따라 Wi-Fi 설정을 구성합니다.

6. **다음**을 클릭하세요.
7. (macOS 전용) 배포 페이지에서 다음 배포 옵션 중 하나를 선택합니다.
    - 기기 채널 - 구성은 기기의 모든 사용자에게 효과적이며 일반적인 옵션입니다.
    - 사용자 채널 - 구성은 기기에 현재 등록된 사용자에게만 효과적입니다.
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
9. **완료**를 클릭하세요.

다음 표에는 Wi-Fi 설정이 나열되어 있습니다.

| 설정 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 서비스 세트 식별자 (SSID) | 현재 설정이 적용될 무선 네트워크 이름을 입력할 수 있습니다. 이 항목은 대소문자를 구분합니다. |
| 자동 참여 | 기기가 해당 Wi-Fi 네트워크에 자동으로 접속하도록 설정할 수 있습니다. 이 항목을 선택하지 않을 경우, 사용자가 직접 기기에서 네트워크 이름을 터치해야 해당 네트워크에 접속할 수 있습니다. |
| 숨겨진 네트워크 | 사용할 네트워크가 숨겨져 있을 경우 이 항목을 선택합니다. |
| 캡티브 네트워크 감지 (iOS 10+) 비활성화 | 관리자는 Wi-Fi 캡티브 우회 모드를 활성화/비활성화할 수 있습니다. Apple이 캡티브 포털의 존재를 감지하면 액세스를 요청하는 로그인 화면이 열립니다. 캡티브 포털 감지를 비활성화하고 사용자가 캡티브 네트워크의 포털 로그인을 실행하는 웹브라우저를 수동으로 열 수 있습니다. 이 새로운 설정은 ISE 캡티브 포털로 인해 로그인 화면이 팝업으로 나타나지 않아서, 사용자들은 연결되지 않은 기기가 실제로는 인터넷에 연결되어 있다고 생각합니다. |
| 프록시 설정 | **수동** 또는 **자동**을 선택해 프록시를 설정합니다.<br>**수동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **서버 및 포트**: 해당 프록시 서버의 네트워크 주소와 포트 번호를 입력합니다.*<br>• **인증**: 프록시 연결에 필요할 경우 유효한 사용자 이름을 입력합니다.*<br>• **비밀번호**: 프록시 연결에 필요할 경우 유효한 비밀번호를 입력합니다.<br>추가된 호스트 이름을 제거하려면 '빼기' 아이콘을 클릭합니다.<br>**자동**을 선택하면 다음과 같은 항목을 추가로 설정할 수 있습니다.<br>• **프록시 서버 URL**: 사용할 프록시의 정규화된 URL을 입력합니다. |
| 보안 유형 | 네트워크 접속에 필요한 보안 방법을 선택할 수 있습니다.<br>• 임의(개인)<br>• 모두(엔터프라이즈)<br>• WEP<br>• WEP 엔터프라이즈<br>• WPA<br>• WPA 엔터프라이즈<br>• WPA2<br>• WPA2 엔터프라이즈<br>• WPA3<br>• WPA3 Enterprise<br>WPA3/WPA3 엔터프라이즈는 iOS 13+에 적용됩니다.<br>Windows에서는 WPA, WPA 엔터프라이즈, WPA2 및 WPA2 엔터프라이즈를 지원합니다. |

## WEP, WPA/WPA2/WPA3, 임의(개인) 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 비밀번호 | (선택사항) 현재 네트워크 접속 시 사용될 비밀번호를 입력할 수 있습니다. 비밀번호를 설정하지 않으면 장치 사용자가 해당 네트워크를 접속할 때 필요한 임의 비밀번호를 입력하라는 메시지가 표시됩니다. |

### WEP 엔터프라이즈, WPA/WPA2/WPA3 엔터프라이즈, 임의(엔터프라이즈) 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| **프로토콜** | |
| 허용된 EAP 유형 | 현재 네트워크 연결에 사용 가능한 EAP 유형을 선택할 수 있습니다.<br>• TLS<br>• TTLS - 내부 ID 필드에서 OS 기본 설정, PAP, CHAP, MSCHAP, MSCHAPv2 및 EAP와 같은 인증 프로토콜 중 하나를 선택합니다.<br>• PEAP<br>• LEAP(AMAPI 등록 기기에 지원되지 않음)<br>• EAP-SIM<br>• EAP-AKA<br>• EAP-FAST(AMAPI 등록 기기에 지원되지 않음) |
| EAP-FAST | 인증 방법을 설정할 EAP-FAST 옵션을 선택할 수 있습니다.<br>• **PAC 사용:**프록시 자동 설정(PAC)을 사용하도록 설정할 수 있습니다.<br>• **PAC 제공:** PAC 제공을 허용하도록 설정할 수 있습니다. 이 옵션을 설정하지 않으면, 장치에 이미 제공되는 PAC만 사용할 수 있습니다. PAC 사용 옵션을 선택한 경우에 한해 설정 가능한 옵션입니다.<br>• **익명으로 PAC 제공:** 서버 인증 없이 PAC 제공이 허용되도록 설정할 수 있습니다. PAC 제공 옵션을 선택한 경우에 한해 설정 가능한 옵션입니다. |
| **인증** | |
| 사용자 이름 | 네트워크 접속에 필요한 사용자 이름을 지정할 수 있습니다. 해당 항목을 지정하지 않고 비워두면, 장치 사용자에게 이름을 지정하라는 메시지가 표시됩니다.* |
| 연결별 비밀번호 사용 | 장치 사용자가 연결을 시도할 때마다 비밀번호를 입력하라는 메시지가 표시되도록 설정할 수 있습니다. 해당 기기가 동일한 네트워크에 재접속할 경우 기기 사용자에게 해당 네트워크에 접속하려면 재인증이 필요하다는 메시지가 표시됩니다. 이 옵션은 AMAPI 등록 기기에 지원되지 않습니다. |
| 비밀번호 | (선택사항) 현재 네트워크 접속 시 사용될 비밀번호를 입력할 수 있습니다. 비밀번호를 설정하지 않으면 장치 사용자가 해당 네트워크를 접속할 때 필요한 임의 비밀번호를 입력하라는 메시지가 표시됩니다. |
| ID 인증서 | (선택사항) 신원 증명에 사용할 인증서를 선택할 수 있습니다. ID 인증서 구성은 사용 가능한 각 ID 인증서를 정의합니다. |
| 인증서(Windows 기기만 사용 가능) | 다음 인증서 저장소 3개 중 하나를 선택하고 Wi-Fi 네트워크에 연결합니다.<br>• 컴퓨터 또는 사용자: 이 옵션을 선택하고 사용자가 로그인하지 않을 경우 컴퓨터 스토어의 인증서가 선택됩니다. 사용자가 로그인하면 사용자 저장소의 특정 인증서가 선택됩니다.<br>• 컴퓨터: 이 옵션을 선택하면 컴퓨터 스토어의 인증서가 선택됩니다.<br>• 사용자: 이 옵션을 선택하면 사용자 스토어의 인증서가 선택됩니다.<br>기본값으로 선택된 것은 사용자 옵션입니다. |
| 외부 ID | (선택 사항) TLS, TTLS, PEAP 및 EAP-FAST의 경우 장치 사용자가 자신의 ID를 숨길 수 있도록 선택합니다. 이 옵션을 설정하면 사용자의 실명이 암호화된 터널 내부에서만 표시됩니다. 이 옵션을 사용하면 공격자가 인증 사용자의 이름을 확인할 수 없으므로 보안을 강화할 수 있습니다. |

| 설정 항목 | 설정하기 |
| --- | --- |
| 도메인 | EAP 유형이 TLS 및 TTLS인 경우 지원됩니다. |
| **신뢰** | |
| 신뢰할 수 있는 인증서 (AMAPI 등록 기기에 지원되지 않음) | 목록에서 여러 인증서를 선택하려면 확인란을 선택합니다. |
| 신뢰할 수 있는 서버 인증서 이름 | **+ 추가**를 클릭하여 하나 이상의 신뢰할 수 있는 서버 인증서 이름을 입력합니다.<br>**신뢰 예외 허용**을 선택하면 대화 상자를 통해 사용자가 내린 의사결정을 신뢰하도록 허용합니다(선택 사항). |

### iOS, macOS, visionOS

| 설정 항목 | 설정하기 |
| --- | --- |
| **모든 버전** | |
| 네트워크 유형 | 네트워크가 다음과 같이 취급되어야 한다면 선택하십시오.<br>• 표준<br>• 레거시 핫스팟<br>• Passpoint |
| Proxy PAC 폴백 허용 | (선택사항) PAC 파일 접근이 불가능한 경우 장치가 바로 해당 네트워크에 연결될 수 있도록 설정할 수 있습니다. |
| 설정 모드(선택사항) | 연결할 연결 모드 유형을 포함하고 있는 문자열 배열입니다.<br>• 시스템: 사용자가 기기에 로그인하기 전에 Wi-Fi가 연결됩니다.<br>• 로그인 창: 사용자가 기기에 로그인한 후에 Wi-Fi를 사용할 수 있습니다.<br>현재 설정 모드는 시스템 및 로그인 창 모드를 모두 활성화한 경우에만 사용할 수 있습니다. |
| **Passpoint 설정** | 네트워크 유형에 맞는 Passpoint를 선택했다면 이 섹션의 설정이 나타납니다. |
| 도메인 이름 | Passpoint 협상에 사용할 도메인 이름을 입력합니다. |
| 로밍 파트너 Passpoint 네트워크에 연결 | (선택사항) 로밍 서비스 제공자 연결이 허용되도록 설정할 수 있습니다. |
| 로밍 컨소시엄 조직 식별자 | (선택사항) 현재 Wi-Fi 프로필이 지원하는 항목에 IEEE가 할당한 식별자를 입력할 수 있습니다. |
| 네트워크 액세스 식별자 영역 이름 | (선택사항) Passpoint 협상에 사용할 네트워크 액세스 영역 이름을 입력하십시오. |
| MCC 및 MNC 쌍 | (선택 사항) Passpoint 협상에 사용할 모바일 국가 코드(MCC)/모바일 네트워크 코드(MNC) 쌍을 입력합니다. 각 문자열은 6개 숫자로만 구성되어야 합니다. |
| 표시된 연산자 이름 | (선택사항) 표시할 네트워크 연산자 이름을 입력할 수 있습니다. |
| **Cisco QoS 고속선** | 이 섹션의 설정은 Cisco 고속선 구성에 적용됩니다. 설정에는 L2 및 L3 표시를 위한 허용 목록 앱을 비롯하여, FaceTime이나 Wi-Fi 호출 등 기본 제공되는 오디오 및 비디오 서비스의 오디오/비디오 트래픽을 허용 목록에 등록할지 여부가 포함됩니다. |
| QoS 마킹 제한 | 선택이 해제되어 있다면 네트워크가 Cisco QoS 고속선을 지원할 경우, 모든 앱이 L2와 L3 마킹을 할 수 있습니다. 선택되어 있을 경우, 나타나는 **앱 선택** 설정을 사용하여 L2와 L3 마킹에 포함할 앱을 추가합니다. 선택되지 않은 앱은 L2와 L3 마킹을 사용하지 않습니다. |
| QoS 마킹 활성화 | L3 마킹을 비활성화하고 L2 마킹만 사용하여 트래픽을 Wi-Fi 네트워크에 전송합니다. 선택을 해제한 상태에서 시스템은 Wi-Fi를 Cisco QoS 고속선 네트워크와 관련이 없는 것으로 취급합니다. |

| 설정 항목 | 설정하기 |
| --- | --- |
| Apple 오디오/비디오 호출 허용 목록<br><br>앱 선택<br><br>**iOS 10+** | FaceTime이나 Wi-Fi 호출 등 기본 제공되는 오디오/비디오 서비스의 오디오 및 비디오 트래픽을 허용 목록에 등록할지 여부를 지정합니다.<br><br>L2와 L3 마킹에 포함하고 싶은 앱을 추가합니다. 선택되지 않은 앱은 L2와 L3 마킹을 사용하지 않습니다. |
| **Cisco QoS 고속선** | 이 섹션의 설정은 Cisco 고속선 구성에 적용됩니다. 설정에는 L2 및 L3 표시를 위한 허용 목록 앱을 비롯하여, FaceTime이나 Wi-Fi 호출 등 기본 제공되는 오디오 및 비디오 서비스의 오디오/비디오 트래픽을 허용 목록에 등록할지 여부가 포함됩니다. |
| QoS 마킹 제한<br><br>QoS 마킹 활성화 | 선택이 해제되어 있다면 네트워크가 Cisco QoS 고속선을 지원할 경우, 모든 앱이 L2와 L3 마킹을 할 수 있습니다. 선택되어 있을 경우, 나타나는 **앱 선택** 설정을 사용하여 L2와 L3 마킹에 포함할 앱을 추가합니다. 선택되지 않은 앱은 L2와 L3 마킹을 사용하지 않습니다.<br><br>L3 마킹을 비활성화하고 L2 마킹만 사용하여 트래픽을 Wi-Fi 네트워크에 전송합니다. 선택을 해제한 상태에서 시스템은 Wi-Fi를 Cisco QoS 고속선 네트워크와 관련이 없는 것으로 취급합니다. |
| Apple 오디오/비디오 호출 허용 목록<br><br>앱 선택<br><br>**iOS 10.3+ 감독**<br><br>Wi-Fi 허용 목록 지정 활성화<br><br>**iOS 14.0+ 및 macOS 15.0+** | FaceTime이나 Wi-Fi 호출 등 기본 제공되는 오디오/비디오 서비스의 오디오 및 비디오 트래픽을 허용 목록에 등록할지 여부를 지정합니다.<br><br>L2와 L3 마킹에 포함하고 싶은 앱을 추가합니다. 선택되지 않은 앱은 L2와 L3 마킹을 사용하지 않습니다.<br><br>기기에서 연결을 허용할 Wi-Fi 네트워크를 지정합니다. Wi-Fi 구성이 여러 개인 경우 가장 제한적인 구성이 적용됩니다. |
| MAC 주소 임의 지정 비활성화 | iOS 14.0+ 및 macOS 15.0+에서 Apple은 장치가 Wi-Fi MAC 주소를 보고하는 기본 동작을 변경하여 장치의 실제 Wi-Fi MAC 주소 대신 새 연결에 대해 임의의 주소를 보고하도록 설정했습니다. 결과적으로 이 기능은 캡티브 포털 또는 MAC 주소 필터링을 사용하는 엔터프라이즈에 예기치 않은 동작을 일으킬 수 있습니다.<br>관리자는 연결된 Wi-Fi 설정을 편집하고 이 옵션을 켜서(기본값은 False) Wi-Fi 네트워크에 대한 **MAC 주소 임의 지정을 비활성화**할 수 있습니다. 이렇게 하면 Wi-Fi 설정이 모든 기기에 다시 푸시됩니다. 이 옵션은 네트워크가 개인정보 보호 수준을 낮추었음을 나타내는 개인정보 보호 경고를 기기 설정에 표시합니다.<br>기기 사용자는 기기 설정을 통해 이 설정을 여전히 수동으로 켜거나 끌 수 있습니다. |
| **Android 11+** | |
| MAC 주소 임의 지정 | • 사용 안 함: 사용자가 장치에 로그인하기 전에 Wi-Fi가 연결됩니다.<br>• 사용 - 자동: 사용자가 장치에 로그인한 후 Wi-Fi를 사용할 수 있습니다.<br>• 사용 - 비영구적<br>• 사용 - 영구적 |

$를 입력하면 현재 필드에 해당하는 지원 **변수** 목록을 확인할 수 있습니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.7. 셀룰러 네트워크 구성

이 섹션에는 다음 주제가 포함됩니다.

- APN 설정
- 휴대폰
- Cellular Private Network Configuration.htm셀룰러 사설 네트워크 구성
- iOS 텔레콤 사전 설정 구성
- eSIM 구성

# 10.10.7.1. APN 설정

APN 구성은 기기에 대한 셀룰러 액세스 포인트 이름을 설정합니다. iOS 7의 경우 **휴대폰 설정** 메뉴를 이용합니다.

## APN 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 액세스 지점 이름 | 해당 액세스 지점 이름을 입력할 수 있습니다. 액세스 지점 이름은 보통 통신 서비스 제공업체가 설정합니다. |
| 액세스 지점 사용자 이름 | 현재 액세스 지점에 대해 권한이 있는 사용자 이름을 입력할 수 있습니다.* |
| 액세스 지점 비밀번호 | 입력한 사용자 이름에 해당하는 비밀번호를 입력할 수 있습니다. |
| 프록시 서버 및 포트 | APN 프록시의 IP 주소 또는 URL과 포트 번호를 입력할 수 있습니다. |
| EnableXLAT464 | 액세스 포인트 이름(APN)을 활성화하려면 체크박스를 선택합니다. 이 옵션은 IPv6 전용 네트워크를 통해 IPv4 서비스를 제공합니다. |

$를 입력하면 현재 필드에 해당하는 지원 **변수** 목록을 확인할 수 있습니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.7.2. 휴대폰

**적용 대상:** iOS 7.0 이상, watchOS 10.0 이상

이 섹션에는 다음 주제가 포함됩니다.

- 기본 APN의 셀룰러 설정
- 데이터 APN의 셀룰러 설정
- 로밍 중 휴대폰 액세스 제어
- 휴대폰 액세스 제어

휴대폰 설정은 기기의 휴대폰 프로필을 설정합니다. iOS 7.0+ 또는 watchOS 10.0+를 실행하는 장치에서 셀룰러 네트워크 설정을 구성합니다. 일부 회사는 원격 네트워크 액세스 또는 특수한 청구 계획을 위해 고유 APN(Access Point Name)에 대한 액세스 권한을 부여하는 무선 통신 운영자와 계약이 체결되어 있습니다. 구성 매개 변수는 무선 통신 운영자에게 문의하십시오.

- 휴대폰 프로필 설치는 1개까지만 가능합니다.
- **APN 프로필**이 이미 설치되어 있는 경우에는 휴대폰 프로필을 설치할 수 없습니다.

**구성된 APN 유형** 드롭다운 상자에서 다음 APN 유형의 휴대폰 설정을 구성할 수 있습니다.

- 기본 및 데이터 APN
- 기본 APN
- 데이터 APN

모든 구성에서 구성을 식별하는 이름을 입력하고, 필요한 경우 설명도 입력합니다.

## 기본 APN의 셀룰러 설정

| 기본 APN 설정 | 설정하기 |
|---|---|
| APN 이름 | 해당 액세스 지점 이름을 입력할 수 있습니다. 액세스 지점 이름은 보통 통신 서비스 제공업체가 설정합니다. |
| APN 인증 유형 | (선택 사항) 다음 중 하나를 선택합니다.<br>• CHAP(challenge handshake authentication protocol)<br>• PAP(password authentication protocol) |
| 사용자 이름 | (선택사항) 인증에 사용될 사용자 이름을 입력할 수 있습니다. |
| 비밀번호 | (선택사항) 인증에 사용될 비밀번호를 입력할 수 있습니다. |

## 데이터 APN의 셀룰러 설정

| 데이터 APN 설정 | 설정하기 |
| --- | --- |
| APN 이름 | 해당 액세스 지점 이름을 입력할 수 있습니다. 액세스 지점 이름은 보통 통신 서비스 제공업체가 설정합니다. |
| APN 인증 유형 | (선택 사항) 다음 중 하나를 선택합니다.<br>• CHAP(challenge handshake authentication protocol)<br>• PAP(password authentication protocol) |
| 사용자 이름 | (선택사항) 인증에 사용될 사용자 이름을 입력할 수 있습니다. |
| 비밀번호 | (선택사항) 인증에 사용될 비밀번호를 입력할 수 있습니다. |
| 프록시 서버 | 프록시 서버를 지정합니다. |
| 프록시 서버 포트 | 프록시 서버 포트를 지정합니다. |
| **10.3+** | |
| 허용되는 프로토콜 마스크 | IPv4, IPv6 또는 두 가지 모두 선택합니다. |
| 국내 로밍에서 허용되는 프로토콜 마스크 | IPv4, IPv6 또는 두 가지 모두 선택합니다. |
| 로밍에서 허용되는 프로토콜 마스크 | IPv4, IPv6 또는 두 가지 모두 선택합니다. |

## 로밍 중 휴대폰 액세스 제어

기기가 로밍 상태일 때 휴대폰 데이터에서 관리된 앱의 일부 또는 전체에 대한 액세스를 제한할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 주 탐색 메뉴에서 **구성** 탭으로 이동합니다.
2. **+추가**를 클릭하고
3. 검색 필드에 **네트워크**를 입력한 다음 **네트워크 사용** 구성을 클릭합니다.
4. **모든 관리되는 앱에 대해 허용 안 함** 체크박스를 선택하면 관리되는 앱이 로밍 상태 또는 항상 휴대폰 데이터에 액세스할 수 없도록 차단합니다.
5. 체크박스를 해제하여 관리된 앱을 이름 또는 번들 ID로 명시하여 휴대폰 데이터의 수신을 차단할 수 있습니다.
6. 앱 필드에서 풀다운 메뉴를 이용하여 앱을 이름 또는 번들 ID별로 검색합니다.

## 휴대폰 액세스 제어 중

언제든 관리된 앱 일부 또는 전체의 휴대폰 데이터 액세스를 제한할 수 있습니다. 앱은 기준을 제한한 상태에서도 사용될 수 있지만 휴대폰 데이터에는 액세스할 수 없습니다.

**절차**

1. MDM용 Ivanti Neurons 주 탐색 메뉴에서 **구성** 탭으로 이동합니다.
2. **+추가**를 클릭하고
3. 검색 필드에 **네트워크**를 입력한 다음 **네트워크 사용** 구성을 클릭합니다.

4. **모든 관리된 앱에 대해 허용 안 함** 체크박스을 선택하여 로밍 시 또는 항상 휴대폰 데이터에 관리된 앱의 액세스를 차단합니다.
5. 필요에 따라 체크박스를 해제하면 휴대폰 데이터 수신을 차단하게 될 관리된 앱을 지정할 수 있습니다.
6. 앱 필드에서 풀다운 메뉴를 이용하여 앱을 이름 또는 번들 ID별로 검색합니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.7.3. 셀룰러 사설 네트워크 구성

MDM용 Ivanti Neurons 를 통해 셀룰러 사설 네트워크 구성 페이로드가 지리적 위치, Wi-Fi에 대한 기본 설정, 네트워크 배포 유형 등 사설 네트워크 배포에 대한 장치 정보를 제공할 수 있습니다.

**적용 대상**

iOS 17.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **셀룰러 사설 네트워크** 구성을 검색하고 선택합니다.
3. 다음 표에 따라 **셀룰러 사설 네트워크** 설정을 구성합니다.

| 설정 항목 | 설명 |
|---|---|
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **셀룰러 데이터 우선** | Wi-Fi를 통해 셀룰러 데이터를 활성화하고 사용하려면 확인란을 선택합니다. |
| **NR 독립형** | 셀룰러 데이터 네트워크에 NR 5G 독립형이 있는 경우 확인란을 선택합니다. |
| **데이터 세트 이름** | 이 구성으로 식별되는 데이터 세트 이름을 지정하십시오. |
| **버전 번호** | 시스템 업데이트를 추적하려면 데이터 세트의 버전 번호를 지정하십시오. |
| **지오펜스** | 각 지오 ID에 대한 위도, 경도, 반경을 지정하여 지리적 위치에 사설 네트워크를 배포합니다.<br>사설 네트워크에 최대 1,000개의 지오펜스 목록을 만들 수 있습니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **셀룰러 사설 네트워크** 구성을 설정하십시오. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.7.4. iOS 텔레콤 사전 설정 구성

iOS 텔레콤 사전 설정을 통해 로밍 제한 및 핫스팟 제한 기본값을 설정할 수 있습니다.

## iOS 텔레콤 사전 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 로밍 중 기기에 음성 서비스 사용 허용 | 음성 로밍 기능을 설정할 수 있습니다. 음성 로밍 기능 사용 가능 여부는 연산자에 따라 다릅니다. |
| 로밍 중 기기에 데이터 서비스 사용 허용 | 데이터 로밍 기능을 설정할 수 있습니다.<br>데이터 로밍을 활성화하면 기기의 음성 로밍도 활성화됩니다. |
| 사용자에게 개인 핫스팟 활성화 허용 | 개인 핫스팟 기능을 설정할 수 있습니다. 해당 기능의 사용 가능 여부는통신사에 따라 다릅니다. |

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.7.5. 향상된 5G 네트워크 슬라이싱 구성

MDM용 Ivanti Neurons는 안드로이드에 5G 네트워크 슬라이스를 설정할 수 있도록 향상된 5G 네트워크 슬라이싱 구성을 제공합니다. 그러면 모바일 네트워크 사업자는 전용 5G 네트워크 구간, 즉 '슬라이스'를 할당하여 특정 슬라이스에서 낮은 지연 시간이나 높은 대역폭과 같이 요구 사항이 유사한 애플리케이션끼리 그룹으로 묶을 수 있어 네트워크 리소스를 더욱 최적으로 사용할 수 있습니다. 이를 통해 MDM 관리자와 네트워크 제공자가 슬라이스를 직접 관리하게 되므로 앱 성능이 향상됩니다.

## 주요 특징

1. **전용 네트워크**: 모든 애플리케이션이 단일 네트워크 슬라이스를 공유하는 대신, 네트워크 슬라이싱을 통해 다양한 애플리케이션이 각자의 요건에 맞게 조정한 자체 네트워크 슬라이스를 사용할 수 있습니다.

2. **사용자 정의**: 관리자는 앱이 특정 네트워크 슬라이스에 할당되는 방식을 개별 요건에 따라 구성할 수 있습니다. 예를 들어 실시간 커뮤니케이션 앱에는 낮은 지연 시간을 보장하고, YouTube와 같은 스트리밍 서비스에는 높은 대역폭을 보장할 수 있습니다. 고성능 게임에 할당된 슬라이스는 낮은 지연 시간을 우선시하고, 미디어 스트리밍에 할당된 슬라이스는 높은 대역폭에 최적화할 수 있습니다.

3. **파트너 참여**: 이 기능을 사용하려면 슬라이스를 정의하고 MDM 관리자에게 슬라이스 목록과 그 중요성을 알려주는 네트워크 제공자와의 협업이 필요한 경우가 많습니다.

## 향상된 5G 네트워크 슬라이싱 구성 만들기

### 절차

1. **구성 추가**

- **구성 >> +추가**로 이동합니다. **구성 추가** 페이지가 표시됩니다.
- 검색 창에 **향상된 네트워크 슬라이싱**을 입력하고 향상된 네트워크 슬라이싱을 구성하세요. **향상된 네트워크 슬라이싱 구성 만들기** 페이지가 표시됩니다.
- **+설명 추가**를 클릭하여 구성에 대한 설명을 입력합니다.

2. **애플리케이션 구성**

- **구성 설정 >> 앱 카탈로그** 아래에 원하는 애플리케이션 이름을 입력합니다.
- 해당 애플리케이션이 Play Store 또는 App Store에서 제공되지 않는 경우 **수동으로 추가**를 클릭합니다.
- **패키지 ID**를 입력하고 드롭다운 메뉴에서 적절한 **네트워크 슬라이스**를 선택합니다.
- **슬라이스 선택** 드롭다운에서 원하는 슬라이스를 선택합니다.
- **추가**를 클릭합니다.이제 선택한 네트워크 슬라이스 아래의 **네트워크 슬라이스 구성**에 애플리케이션이 나타납니다.
- 애플리케이션을 제거하려면 **네트워크 슬라이스 구성** 섹션 아래에서 **제거**를 클릭합니다.

3. **구성 배포**

- **다음**을 클릭하여 "**이 구성 활성화**" 확인란에 체크하거나 체크를 해제하고, 배포 옵션(모든 장치, 장치 없음, 사용자 지정)을 선택합니다.
- **완료**를 클릭하여 구성을 마칩니다.

## 잠금 및 키오스크를 위한 향상된 네트워크 슬라이싱 구성

향상된 5G 네트워크 슬라이싱 구성 만들기에서 장치가 제한된 방식으로 작동하도록 구성하면 사용자가 지정된 애플리케이션과 설정에만 액세스하도록 할 수 있습니다.

다음 잠금 아래에 "**5G 네트워크 슬라이싱 활성화**" 확인란이 있습니다.

- **업무 프로필** - Android Enterprise 버전 12.0으로 업무 프로필을 구성한 직원 소유 장치에서 "5G 네트워크 슬라이싱 활성화" 확인란은 다음 아래에 있습니다.
  **구성 설정 > 업무 프로필 잠금 설정**.
- **업무 프로필이 있는 관리형 기기/회사 소유 기기의 업무 프로필** - Android 12.0 버전이 설치된 업무 프로필이 있는 관리형 기기/회사 소유 기기의 업무 프로필 아래에 "5G 네트워크 슬라이싱 활성화" 확인란이 있습니다.

이는 기기가 5G 네트워크 슬라이싱을 사용할 수 있도록 허용하는 레거시 설정입니다. 새로운 향상된 5G 네트워크 슬라이싱 구성과의 상관관계는 다음과 같습니다.

위의 잠금 중 하나라도 장치에 적용되고 *5G 네트워크 슬라이싱 활성화* 옵션이 선택되지 **않은** 경우, *향상된 5G 네트워크 슬라이싱* 구성은 오류로 인해 실패합니다.

### 예

- **사례 1**: 장치 잠금이 배포되지 않고 향상된 네트워크 슬라이싱 구성이 배포되면 향상된 구성이 활성화됩니다.
- **사례 2**: 장치 잠금이 배포되었지만 5G 확인란이 선택되지 않은 경우(거짓), 향상된 5G 네트워크 구성에서 오류가 발생합니다.
- **사례 3**: 향상된 네트워크 슬라이싱이 먼저 배포되고 그다음에 확인란이 활성화된 상태에서 장치 잠금이 배포되면, 향상된 네트워크 슬라이싱 구성이 계속 작동합니다. 그렇지 않으면 오류가 발생합니다.

## 구성 세부 정보:

- 장치 잠금이 분산되고 향상된 네트워크 슬라이싱 구성이 푸시/분산되는 경우, 오류를 방지하기 위해 사용자는 5G 네트워크 슬라이싱 활성화 확인란이 활성화되어 있는지 확인해야 합니다.
- 확인란이 활성화되어 있지 않은 상태에서 구성을 전송하면 장치에서 오류가 발생합니다.

# 10.10.7.6. eSIM 구성

eSIM 구성은 RefreshCellularPlans 명령으로 기기의 셀룰러 네트워크를 구성합니다. 관리자는 셀룰러 네트워크를 기기로 매핑하기 전에 먼저 eSIM 통신사 URL을 획득해야 합니다.

적용 대상: Android 15+, iOS, iPadOS, Windows 11

**Android 15 + 기기의 절차**

1. **구성** >**+추가**로 이동합니다.
2. 검색 필드에 eSIM을 입력한 다음, **eSIM** 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. **플랫폼** 목록에서 **Android**를 선택합니다.
5. **구성 설정** 섹션에서 **통신사 URL**을 입력합니다.
6. **자동 활성화** - 이 옵션을 선택하면 eSIM 프로필을 다운로드하고 기기에서 자동으로 활성화합니다. 이 옵션을 선택하지 않으면 eSIM 프로필은 다운로드되지만 기기에서 자동으로 활성화되지는 않습니다.

> 이 옵션은 작업 프로필 모드의 기기에서는 사용할 수 없습니다.

7. 다음 배포 옵션 중 하나를 사용하여 구성을 선택하고 배포합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정
8. **완료**를 클릭하세요.

**Android 13+ 기기용 EID**

**EID 요청** 옵션은 이제 기기 세부 사항 페이지와 기기 목록 페이지에서 사용할 수 있습니다. 이 옵션은 작업 프로필, 업무 관리형 기기, 회사 소유 기기의 작업 프로필 모드에서 eSIM과 호환되는 기기에서만 사용할 수 있습니다. 기기가 등록되어 있으면 등록된 기기의 EID가 자동으로 선택되어 기기 세부 사항 페이지에 표시됩니다. 그렇지 않은 경우 이 필드는 활성화되며, **EID 요청**을 클릭하여 EID를 요청할 수 있습니다. 기기 목록 페이지의 **CSV로 내보내기** 옵션을 사용하여 EID를 내보낼 수도 있습니다.

> **기기 세부 사항** 페이지에서 **EID 요청** 옵션은 Ivanti Go R122 이상 버전이 설치된 Android 13+ 기기에서 사용할 수 있습니다.

**eSIM 데이터 플랜 유지(iOS 11+ 및 Android 15.0+에 적용)**: eSIM 구성으로 등록된 기기를 지우려고 하면, **기기 지우기** 작업에서 데이터 플랜을 유지하는 추가 옵션이 제공됩니다. **eSIM 데이터 플랜 유지(iOS 11+ 및 Android 15.0+에 적용)**를 선택한 후 **지우기**를 클릭하면, 기존 eSIM 데이터 플랜은 유지되고 기기의 다른 모든 데이터는 삭제됩니다. **기기 상세 정보** 페이지에서 이 옵션에 액세스하거나, 기기를 선택한 뒤 **작업** 메뉴를 열고 **지우기**를 클릭하여 액세스할 수 있습니다.

**iOS 및 iPadOS 장치의 절차**

1. **구성** > **추가**로 이동합니다.
2. 검색 필드에 eSIM을 입력한 다음, eSIM 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. **iOS/iPadOS**를 선택합니다.
5. 통신사 URL을 입력합니다.

6. **다음**을 클릭하세요.
7. 이 구성 활성화 옵션을 선택합니다.
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
9. 완료를 클릭하세요.

**Windows 11 장치의 절차**

1. **구성** > **추가**로 이동합니다.
2. 검색 필드에 eSIM을 입력한 다음, eSIM 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. OS 선택 섹션에서 **Windows**를 클릭하세요.
5. 구성 설정 섹션에서 서버 이름 텍스트 상자에 통신사 URL을 입력합니다(FQDN 형식).
    - 검색 서버 - 서버를 검색 가능으로 표시하려면 선택합니다.
    - 자동 활성화 - 다운로드한 후 장치에서 프로필을 활성화하려면 선택합니다.
6. **다음**을 클릭하세요.
7. 이 구성 활성화 옵션을 선택합니다.
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
9. **완료**를 클릭하세요.

**eSIM을 공장 초기화(Windows 11 장치에만 해당)**

이 옵션은 모든 장치의 장치 세부 정보 섹션에서 사용할 수 있습니다. 이 옵션을 클릭하면 장치에 다운로드된 모든 eSIM 프로필이 삭제됩니다.

**중요 참고 사항 - Windows eSIM 구성에만 적용**

- 기기가 등록되면 **기기 상세 정보** 섹션의 **eSIM 지원** 아래에 기기의 eSIM 지원 여부가 표시됩니다. eSIM을 지원하는 기기의 경우 해당 eSIM ID 상세 정보도 **eSIM 식별자** 아래에 표시됩니다.
- MDM용 Ivanti Neurons 등록 장치를 삭제했다가 다시 등록할 때, 다시 등록된 장치에서 eSIM 구성과 관련된 프로비저닝 문제를 방지하기 위해 장치 페이지에서 이 장치의 이전 기록(삭제됨 상태)을 삭제해야 합니다.
- 이미 프로필을 다운로드한 장치에 동일한 구성을 다시 푸시하면 프로필을 다시 다운로드할 수 없습니다. 관리자가 장치에서 프로필을 새로 다운로드하도록 하려면 먼저 eSIM 모듈을 공장 초기화한 다음 eSIM 구성을 푸시/다시 푸시하는 것이 좋습니다.
- 장치에 eSIM 구성이 성공적으로 프로비저닝되면 장치를 폐기하기 전에 관리자가 eSIM 삭제 작업을 수행하여 다운로드한 eSIM 프로필을 장치에서 지워야 합니다.
- eSIM 구성을 제거하면 장치에서 구성만 삭제됩니다. eSIM 프로필을 찾아 기기에 다운로드하고 활성화한 경우, 해당 eSIM 프로필은 eSIM이 삭제될 때까지 활성 상태를 유지합니다.

- eSIM을 삭제하면 다운로드한 모든 eSIM 프로필이 장치에서 제거됩니다. 그러나 설치된 상태의 eSIM 구성은 장치에 그대로 유지됩니다. 기기에서 구성을 제거하려면 관리자가 eSIM 구성의 배포를 해제해야 합니다.

# 10.10.8. 기타 구성

이 섹션에는 다음 주제가 포함됩니다.


- 관련 도메인 구성
- Android 파일 전송 구성
- Apple TV 설정
- AirPlay 설정
- AirPlay 미러링
- 브라우저 설정
- iOS에서 단일 앱 모드 구성
- iOS MDM 프로필 구성
- macOS MDM 프로필 구성
- 콘텐츠 캐싱
- Android 바로가기 생성
- 기기 이름 설정
- 이더넷 구성(macOS)
- EMA 서버 통합 구성
- 기기 배경화면 설정
- 잠금 화면 메시지 구성
- 화면 보호기 구성 생성
- 사용자 화면 보호기 구성
- macOS 시스템 확장 구성
- MAM 전용
- 관리되는 Google Play 구성
- 마이그레이션 지원 설정
- 알림 구성
- 프린터 설정
- 블로트웨어 제거 구성
- Samsung Phone 제한 구성
- Single App 모드 설정
- 시작 메뉴 및 작업 표시줄
- 시스템 업데이트 구성
- Windows 업데이트 관리
- Windows 앱 일정 설정
- Windows BIOS 구성
- Windows BitLocker
- Windows 키오스크 구성

- Windows 라이선스 구성
- 소프트웨어 업데이트 권장 케이던스 구성

# 10.10.8.1. 관련 도메인 구성

**라이센스**: Gold

관련 도메인 구성은 연결된 도메인에 앱을 매핑하는 사전입니다. 관련 도메인은 Extensible AppSSO, 유니버설 링크, 암호 자동 완성과 같은 기능과 함께 사용할 수 있습니다.

관련 도메인 설정은 다음과 같습니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 애플리케이션 식별자 | (필수) 도메인을 연결할 앱 식별자. |
| 연결된 도메인 | (필수) 앱과 연결할 도메인. 각 문자열은 "service:domain" 형식입니다. 도메인은 정규화된 호스트 이름이어야 합니다(예: www.example.com). |
| 직접 다운로드 활성화 | true인 경우 이 도메인의 데이터는 CDN을 통하지 않고 직접 다운로드해야 합니다. 이 도메인의 권한 값은 service:domain?mode=managed로 설정해야 하며, 그렇지 않을 경우 이 값은 무시됩니다. macOS 11 이상에서 사용할 수 있습니다.<br>**기본**: false |

# 10.10.8.2. Android 파일 전송 구성

Android 11의 일부로 Google은 앱에서 기기의 저장소 액세스를 크게 변경했으며, 이는 기업이 이러한 기기의 특정 앱으로 파일을 전송하는 방식에도 영향을 미쳤습니다. 이러한 변경으로 인해 많은 대기업은 기기가 Android 11 이상으로 업그레이드됨에 따라 기기와 앱에 파일을 배포하는 데 어려움을 겪고 있습니다. 하드웨어 공급업체의 특정 API에 의존하는 모든 접근 방식은 기업이 서로 다른 제조업체 기기와 OS 버전 사이에서 동일한 접근 방식을 사용하는 데 제한을 가합니다.

Ivanti는 Android 버전과 하드웨어 공급업체에 구애받지 않는 파일 전송 솔루션을 개발했습니다. 이 솔루션은 Android의 표준 *콘텐츠 제공자* 기능에 의존합니다. *콘텐츠 제공자*를 사용하면 Ivanti의 Go 앱이 UEM을 통해 푸시된 각 파일에 대해 고유한 기기 내 위치를 생성할 수 있습니다.

파일 전송 구성은 완전 관리형 기기 모드의 Android 기기에서 사용할 수 있습니다. 관리자는 이 구성을 사용하여 동일한 장치에 있는 여러 허용된 앱 간에 공유할 파일을 전송하는 옵션을 제공할 수 있습니다. 다른 앱은 필요한 이유가 무엇이든 파일을 사용할 수 있습니다. 사용 사례의 예는 JavaScript를 사용하여 앱 구성을 초기화하거나 PDF 또는 비디오를 사용하여 회사 정보를 표시하는 것입니다. Ivanti의 파일 전송 구성에 업로드된 모든 파일은 해당 구성과 관련 파일을 수신할 때 Ivanti Go에서 다운로드합니다. 파일은 Ivanti Go 내에 안전하게 저장됩니다.

다른 앱은 이 파일에 임의로 접근할 수 없습니다.

앱 샌드박스 내에 다운로드된 모든 파일은 *ContentURI* 또는 *URI*라고도 하는 고유한 위치로 참조됩니다. 사용자 지정 속성은 기기의 모든 파일에 대해 서버에서 ContentURI 값을 유지하는 데 사용되며 관리자가 기기에서 파일의 가용성을 확인하고 동적 기기 그룹을 형성하는 데 도움이 될 수 있으며 관리형 앱 구성 등을 사용하여 대상 앱에 ContentURI를 전달하는 데 필요합니다.

> 비 Ivanti 앱의 경우 관리자는 일반적으로 “Consuming FileProvider based ContentURI”라고 하는 이 접근 방식에 대한 지원이 되는지 타사 앱 개발자에게 확인해야 합니다.

**전제 조건**:

- 파일 전송 작업에 사용할 새 기기 기반 사용자 지정 속성을 추가합니다. 모든 파일 전송 구성에 대해 고유한 사용자 지정 속성을 생성해야 합니다. 각 사용자 지정 기기 속성은 구성당 하나의 파일에 대한 기기의 contentURI(파일 위치)만 저장할 수 있습니다.

**절차**

1. **구성** > **구성 추가** > **파일 전송**으로 이동합니다. **파일 전송 구성 만들기** 페이지가 열립니다.
2. **이름** 상자에 구성의 이름을 입력합니다.
3. 구성의 **설명**을 입력합니다.
4. **구성 설정**
   **전송할 파일** 섹션에서 전송할 파일을 끌어다 놓거나 **파일 선택** 옵션으로 파일을 찾아보고 선택합니다. 기본적으로 파일 크기의 상한선은 50MB입니다.
5. 다음 **기기로 다운로드** 옵션을 하나 이상 선택합니다(선택 사항).
   - **데이터 통신 연결 네트워크를 통한 다운로드 허용** - 데이터 통신 연결 네트워크에서도 계속해서 파일을 다운로드하려면 선택
   - **충전 필요** - 파일 전송 프로세스 중 장치를 충전하려면 선택
   - **장치 유휴 상태 필요** - 파일 전송 프로세스 중 장치의 유휴 상태를 유지하려면 선택
6. 다음 두 가지 옵션 중 하나를 사용하여 다른 앱과 파일을 공유합니다.
   - **Android 관리형 앱 구성을 사용하여 전송** - 대상 앱이 해당 관리형 앱 구성을 사용하여 콘텐츠 URI를 사용할 수 있는 경우에만 이 옵션을 사용합니다.
   - **온디바이스 인텐트를 사용하여 전송** - 인텐트는 앱별로 다릅니다. 이 옵션을 사용하여 파일을 공유하려면 대상 앱의 설명서를 참조하고 아래 인텐트 섹션에 정보를 제공하십시오. 인텐트는 파일을 앱과 공유할 수 있게 되면 Ivanti Go 앱이 기기에서 메시지를 브로드캐스트하도록 허용합니다.

## Android 관리형 앱 구성을 사용하여 전송

**절차**

1. **이 파일을 다른 앱과 공유할 기존 장치 기반 사용자 지정 속성 선택** 필드에 기존 속성 이름(예: **Custom-Filename)**을 입력합니다. 자세한 내용은 장치에 사용자 지정 속성 할당을 참조하십시오.
2. 사용자 지정 속성 이름은 이 파일 전송 작업에만 사용되는 새롭고 고유한 속성이어야 합니다. 각 사용자 지정 기기 속성은 구성당 하나의 파일에 대한 기기의 contentURI(파일 위치)만 저장할 수 있습니다.
   **다음 앱 및/또는 패키지 이름에 대한 액세스 제공**: 앱 이름 선택기에서 앱 이름을 선택하고 패키지 이름을 추가할 수 있습니다.

> 이러한 패키지는 파일에 액세스할 수 있는 유일한 인증 패키지입니다.

   - **앱 이름** - 앱 이름 선택기에서 앱 이름을 선택할 수 있습니다.
   - **패키지 이름** - 이 영역에 번들 ID를 입력할 수 있습니다. 예:여러 패키지 이름을 세미콜론(;)으로 구분합니다.

```bash
com.mobileiron.filetransfer.android3.
```

**저장**을 클릭합니다. 새 파일 전송 구성이 구성 페이지에 나타납니다.

## 대상 앱 구성

**절차**

1. **앱 > 앱 카탈로그**로 이동합니다.
2. 파일을 받을 대상 앱을 선택합니다.
3. **앱 구성 > Android용 관리형 구성**으로 이동합니다.
4. 새 구성을 생성하거나 기존 구성을 사용합니다.
5. 앱에는 관리자가 대체 변수를 정의하고 파일 위치를 대상 앱에 전달할 수 있는 "매니페스트 정보" 또는 기타 속성과 같은 설정이 있을 수 있습니다. 예를 들어 Ivanti Velocity 앱의 경우, 앱 구성 대화 상자 > **구성 가져오기 > 매니페스트 정보** 필드에 대체 변수를 입력합니다. 예: $Custom-File-Name$.
   배포를 선택합니다.
6. **저장**을 클릭하세요.

## 온디바이스 인텐트를 사용하여 전송

**절차**

1. **인텐트 엑스트라에서 파일 경로를 전달할 기존 기기 속성 선택** 필드에 새 사용자 지정 속성 이름(예: deviceIntentURI)을 입력합니다.
2. 사용자 지정 속성은 모든 기기에 대한 서버의 위치(URI / ContentURI) 값을 유지하는 데 사용되며 관리자가 기기에서 파일의 가용성을 결정하는 데 도움을 줄 수 있습니다. 자세한 내용은 장치에 사용자 지정 속성 할당을 참조하십시오.
   **특정 앱 또는 패키지 이름에 대한 액세스 제공** 필드에 **앱 이름** 또는 **패키지 이름**(예: Velocity)을 입력합니다.

> 이러한 패키지는 파일에 액세스할 수 있는 유일한 인증 패키지입니다.

3. 인텐트 표준 섹션에서 다음 세부 정보를 제공합니다.

- **작업 유형** - 드롭다운 목록에서 **활동 시작 / 서비스 시작** 또는 앱에 따라 다른 유사한 항목을 선택합니다. 대상 앱 개발자의 지침에 따라 이 필드에 적합한 값을 선택하거나 대상 앱 설명서를 참조하십시오.
- **클래스 이름**(선택 사항) - 대상 앱 개발자의 지침에 따라 이 필드에 적합한 값을 선택하거나 대상 앱 설명서를 참조하십시오.
- **작업** - 작업을 다음으로 설정합니다.또는 앱에 따라 이와 유사하게 지정합니다.

```
Bash

com.wavelink.nameofapp.action.INSTALL_CONFIG
```

- **범주** - 세미콜론(;)으로 구분된 값을 입력합니다.
- **MIME 유형**(선택 사항) - 관리자의 호스트 서버에서 custom.mobileconfig 파일을 애플리케이션/구성의 MIME 유형으로 설정해야 기기에 대한 MDM 프로필이 다운로드되어 기기에 설치됩니다. 대상 앱 개발자의 지침에 따라 이 필드에 적합한 값을 선택하거나 대상 앱 설명서를 참조하십시오.
- **플래그**(선택 사항) - 사용할 플래그 수를 선택합니다. 대상 앱 개발자의 지침에 따라 이 필드에 적합한 값을 선택합니다.

KEY, TYPE, VALUE에 **인텐트 - 엑스트라** 값을 입력합니다(선택 사항). 보다 구체적인 매개변수는 OEM 앱 설명서를 참조하십시오. 대상 앱 개발자의 지침에 따라 이 필드에 적합한 값을 선택하거나 대상 앱 설명서를 참조하십시오.

5. **저장**을 클릭하세요.
6. 구성 페이지에서 새 파일 전송 구성을 선택한 다음 **작업** > **레이블에 적용**을 선택합니다. **레이블에 적용** 대화 상자가 열립니다.
7. 적합한 레이블을 선택한 다음 **적용**을 클릭합니다.
   다른 앱과의 파일 전송/공유는 대상 앱 또는 기기에서 로그를 수집해야만 확인할 수 있습니다.

## 파일 다운로드 상태 확인

사용자 지정 속성은 각 기기의 모든 파일에 대한 서버의 위치(ContentURI) 값을 유지하는 데 사용되며 관리자가 기기에서 파일의 가용성을 결정하는 데 도움을 줄 수 있습니다.

**절차**

1. **기기** > **기기**로 이동합니다.
2. 파일 전송 구성이 배포된 특정 기기를 선택합니다.
3. 기기 세부 정보 페이지에서 기기를 선택한 다음 **작업** > **강제 기기 체크인**을 선택합니다.
4. 구성 탭에서 파일 전송 구성이 **적용됨** 상태로 표시되는지 확인합니다.
5. 사용자 지정 속성 탭에서 관련 값과 함께 새 사용자 지정 속성의 이름이 표시되는지 확인합니다(예: “Custom-File-Name$”). 이것은 기기에 있는 파일의 저장 위치 정보를 제공하고 파일이 Ivanti Go 앱 샌드박스 내에서 사용 가능한 기기에 로컬로 다운로드되었음을 보여줍니다.
   다른 앱과의 파일 전송/공유는 대상 앱 또는 기기에서 로그를 수집해야만 확인할 수 있습니다.

# 10.10.8.3. Apple TV 설정

**라이센스**: Silver

Apple TV 설정을 통해 Apple TV의 언어 및 로캘을 설정할 수 있습니다.

Apple TV 설정은 다음과 같습니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 언어 | 두 글자로 이루어진 언어 코드를 입력해 UI 언어를 설정합니다. |
| 로캘 | 로캘 ID를 입력해 UI를 사용할 국가/언어를 설정합니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.8.4. AirPlay 미러링

**라이센스:** Gold

AirPlay 미러링은 iOS 기기의 화면을 Apple TV를 사용하는 모니터에 보여주는 기능입니다. Apple TV와 iOS 기기가 동일한 Wi-Fi 네트워크에 연결되어야 합니다. 이 기능을 사용하려면 다음 기기가 필요합니다.

- iOS 7 이상 기기 - 감독됨
- macOS 10.10 이상 기기 - 감독됨
- Apple TV 버전 - 감독됨
- AirPlay

> iOS가 아닌 기기의 관리를 포함하도록 전환하면 이것을 번복할 수 없습니다.

이 섹션에는 다음 주제가 포함됩니다.

- **Apple AirPlay 구성**
- **모바일 기기에 AirPlay 설정**
- **Apple TV와 함께 사용할 모니터 설정**
- **iOS 기기와 Apple TV 연결**

## Apple AirPlay 구성

AirPlay 구성 설정에 대한 자세한 내용은 **AirPlay 구성**을 참조하십시오.

**절차**

1. **구성**으로 이동합니다.
2. **+추가**를 클릭합니다.
3. **AirPlay**를 클릭합니다.
4. 해당 필드에 구성 이름 및 설명을 입력합니다.
5. 지원되는 모든 iOS 버전은 기기 이름과 비밀번호를 입력합니다.
6. 필요한 경우 + **추가**를 클릭하여 다른 기기를 추가합니다.
7. 필요할 경우 관리 상태인 iOS 7+ 기기나 macOS 10.10+에서 허용 목록에 기기 ID를 추가합니다.
8. **다음**을 클릭하세요.
9. 배포 수준을 선택합니다.
10. **완료**를 클릭하세요.

## 모바일 기기에 AirPlay 설정

**절차**

1. **Apple Configurator**를 설치합니다.
2. **기기 > 기기**로 이동합니다.
3. 해당 기기에 대한 상세 정보 페이지를 표시할 iOS 기기의 이름을 클릭합니다.

4. ⋮ 아이콘을 클릭합니다.
5. **AirPlay 미러링**을 선택하여 AirPlay 미러링 대화 상자를 표시합니다.
6. 풀다운 메뉴에서 Apple TV 기기를 선택합니다.
7. 검색 시간 (초)을 입력해 선택한 기기를 검색하는 시간 제한을 지정합니다.
8. Apple TV 기기의 비밀번호를 입력합니다.
9. **요청 보내기**를 클릭합니다.

## Apple TV와 함께 사용할 모니터 설정

**절차**

1. Apple TV에 연결된 모니터에서, **설정 > 프로필**로 이동합니다.
2. **MDM용 Ivanti Neurons Apple Configurator**를 선택합니다.
3. **프로필 추가**를 클릭합니다.
4. ⋮ 아이콘을 클릭합니다.
5. **AirPlay 미러링**을 선택하여 AirPlay 미러링 대화 상자를 표시합니다.
6. 풀다운 메뉴에서 Apple TV 기기를 선택합니다.
7. 검색 시간 (초)을 입력해 선택한 기기를 검색하는 시간 제한을 지정합니다.
8. Apple TV 기기의 비밀번호를 입력합니다.
9. **요청 보내기**를 클릭합니다.

## iOS 기기와 Apple TV 연결

**절차**

1. Apple TV 기기를 모니터에 연결합니다.
2. 원격 Apple TV를 사용해 **설정 > 계정 > 홈 공유**로 이동하여 홈 공유를 켭니다.
3. **Apple TV 기기**와 동일한 Wi-Fi 네트워크에 **iOS 기기를 연결합니다**.
4. 원격 앱을 **iOS** 기기에서 엽니다.
5. **원격 설정** 화면에서 **홈 공유**를 활성화합니다.

# 10.10.8.5. 브라우저 설정

브라우저 설정을 사용하면 Windows 10 기기에서 Google Chrome, Mozilla Firefox, Microsoft Edge 및 Internet Explorer에 대한 설정 및 제한을 구성할 수 있습니다.

이 기능을 사용하려면 Bridge가 필요합니다. 자세한 내용은 **Ivanti Bridge**를 참조하십시오.

> 브라우저 설정을 적용하기 전에 브라우저가 기기에 설치되어 있는지 확인하십시오.

브라우저 설정을 구성하려면

1. **구성 > +추가**로 이동합니다.
2. **브라우저 설정** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 표에 설명된 바와 같이 남은 설정을 지정합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| **브라우저** | 설정이 필요한 브라우저 유형을 선택합니다.<br>• **Chrome**<br>• **Firefox**<br>• **Microsoft Edge**<br>• **Internet Explorer** |
| **브라우저 설정** | 다음 옵션을 구성하십시오.<br>**브라우저 허용**:<br>• 비밀번호 저장 허용<br>• 안전 탐색 모드 허용<br>• 브라우저에 오래된 플러그인 유지 허용<br>**Chrome 및 Firefox**:<br>• **브라우저 기록 삭제 허용**<br>**Chrome 및 Internet Explorer**:<br>• **브라우저 인쇄 허용**<br>• **새 탭 페이지 URL**<br>**Chrome에만 해당**:<br>• **북마크 표시줄에 앱 바로가기 표시**<br>• **홈 버튼 표시**<br>• **Google과의 데이터 동기화 허용**<br>• **Chrome을 닫아도 계속해서 백그라운드 앱 실행**<br>**Firefox에만 해당**:<br>• **설치 확장자 허용**<br>**Internet Explorer에만 해당**:<br>• **웹 사이트에서 데이터 다운로드 허용** |
| **브라우저 즐겨찾기** | **+추가**를 클릭합니다.<br>**브라우저 즐겨찾기 추가** 창이 표시됩니다. 다음 필드를 구성하십시오.<br>• **표시 이름**: 즐겨찾기에 대한 표시 이름 입력<br>• **URL**: 브라우저 즐겨찾기 URL 입력<br>**추가**를 클릭합니다.<br>추가된 브라우저 즐겨찾기 상세 정보가 페이지에 표시됩니다. **작업** 열에서, 편집 아이콘을 클릭하여 설정을 편집합니다. 브라우저 즐겨찾기를 삭제하려면 삭제 아이콘을 클릭합니다.<br>**브라우저 즐겨찾기 폴더 이름**: 즐겨찾기를 열거해야 하는 브라우저 즐겨찾기 폴더 이름의 이름을 입력합니다.<br>CSV 형식으로 브라우저 즐겨찾기를 추가할 수도 있습니다. CSV 형식으로 업로드하는 방법:<br>1. CSV 파일 업로드를 클릭합니다. 업로드할 CSV 파일을 탐색, 선택합니다.<br>2. **업로드**를 클릭하세요.<br>CSV 파일의 상세 정보가 다음 형식으로 추가되어야 합니다.<br>• 첫 번째 열(표시 이름)은 즐겨찾기의 표시 이름을 지정해야 합니다. 예: "쇼핑".<br>• 두 번째 열(URL)은 즐겨찾기의 URL을 지정해야 합니다. 예: "https://amazon.com". |

| 설정 항목 | 수행 작업 |
| --- | --- |
| **웹 사이트 보안** | 다음의 웹 사이트 보안 설정을 구성하십시오.<br>**모든 웹 사이트(Chrome 및 Firefox)**<br>• **쿠키 차단**<br>• **Javascript 차단**<br>• **플러그인 차단**<br>• **팝업 차단**<br>특정 웹 사이트(Chrome에만 해당)<br>**차단된 웹사이트(Chrome 및 Edge)**: 차단 목록에 추가하려는 웹사이트를 추가합니다.<br>**+추가**를 클릭합니다. **차단 목록 웹 사이트 추가** 창이 표시됩니다.<br>**웹 사이트 URL**에서 차단 목록에 등록할 웹 사이트의 URL을 입력합니다.<br>**액세스** 필드에서 **차단**을 선택하여 웹 사이트를 차단 목록에 등록합니다. 기본 옵션은 **허용**입니다.<br>**추가**를 클릭합니다. |
| **브라우저 확장자** | **허용되는 확장 유형(Chrome에만 해당)**: 다음 옵션 중 하나를 선택합니다.<br>• **확장자**<br>• **사용자 스크립트**<br>• **주제**<br>• **패키징 앱**<br>• **호스팅된 앱**<br>• **플랫폼 앱**<br>**브라우저 확장 소스(Chrome만 해당)**:<br>브라우저 확장자 소스를 추가하려면 **+추가**를 클릭합니다. 브라우저 확장자 소스가 추가된 후, **작업** 열에서 관련 옵션을 클릭하여 소스를 편집 또는 삭제할 수 있습니다.<br>**확장 프로그램 강제 설치(Chrome만 해당)**:<br>강제 설치 확장자를 추가하려면 **+추가**를 클릭합니다.<br>강제 설치 확장자가 추가된 후, **작업** 열에서 관련 옵션을 클릭하여 소스를 편집 또는 삭제할 수 있습니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정
8. **완료**를 클릭하세요.

# 10.10.8.6. iOS에서 단일 앱 모드 구성

**라이센스: Silver**

단일 앱 모드는 iOS 및 tvOS 기기가 지정된 앱만 사용하도록 제한합니다. 예를 들어 사용자의 조직이 개발한 맞춤형 앱만 사용하도록 기기를 설정할 수 있습니다.

**절차**

1. **구성 > 추가 > 단일 앱 모드**로 이동합니다.
2. 다음 지침을 사용하여 앱과 관련 설정을 정의하세요.
3. **다음**을 클릭하세요.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 앱 선택 | 앱 선택을 위해 사용할 방법을 선택합니다.<br>• **앱 카탈로그 및 시스템 앱:** MDM용 Ivanti Neurons 앱 카탈로그 및 시스템 앱(Apple 기기에 기본값으로 사전 설치)을 검색하도록 선택합니다.<br>• 앱 이름을 입력하고 앱 목록에 표시되면 선택합니다.<br>• **번들 ID 입력:** 선택할 시스템 앱의 고유 식별자를 입력하도록 선택합니다. **App Catalog 및 시스템 앱에서** 옵션으로 시스템 앱을 찾을 수 없을 경우 이 옵션을 사용합니다. |
| 터치 비활성화 | 터치 화면 기능을 해제할 수 있습니다. |
| 기기 회전 비활성화 | 기기 회전 감지 기능을 해제할 수 있습니다. |
| 볼륨 버튼 비활성화 | 기기의 음량 버튼 기능을 해제할 수 있습니다. |
| 링거 스위치 비활성화 | 기기의 링거 스위치 기능을 해제할 수 있습니다. |
| 절전 모드 해제 버튼 비활성화 | 기기의 절전 모드 설정/해제 버튼(기기 가장자리 우측 상단) 기능을 해제할 수 있습니다. |
| 자동 잠금 비활성화 | 일정 시간 입력이 없을 때 기기가 절전 모드로 진입하는 것을 차단할 수 있습니다. |
| 보이스 오버 활성화 | 보이스오버 화면 낭독 기능을 설정할 수 있습니다(접근성 기능). |
| 확대/축소 활성화 | 확대/축소 기능을 설정할 수 있습니다(접근성 기능). |
| 색상 반전 활성화 | 색상 반전 조절 기능을 설정할 수 있습니다(접근성 기능). |
| 보조 터치 활성화 | 보조 터치 기능을 설정할 수 있습니다(접근성 기능). |
| 말하기 선택 활성화 | 말하기 선택 기능을 설정할 수 있습니다(접근성 기능). |
| 모노 오디오 활성화 | 스테레오에서 모노 오디오 모드로 전환할 수 있습니다(접근성 기능). |
| 보이스 오버 조정 | 기기 사용자의 보이스 오버 설정 변경이 허용되도록 설정할 수 있습니다. |
| 확대/축소 조정 | 기기 사용자의 확대/축소 설정 변경이 허용되도록 설정할 수 있습니다. |
| 색상 반전 조정 | 기기 사용자의 색상 반전이 허용되도록 설정할 수 있습니다. |
| 보조 터치 조정 | 사용자의 보조 터치 설정 변경이 허용되도록 설정할 수 있습니다. |

4. **배포** 화면에서, 해당 구성을 배포할 기기 그룹을 선택하세요.
5. **완료**를 클릭하세요.

> 사용할 앱으로 전화 걸기를 구성한 경우 기기가 단일 앱 모드로 들어가면 홈 버튼이 작동합니다.

# 10.10.8.7. iOS MDM 프로필 구성

iOS MDM 구성은 MDM용 Ivanti Neurons에 대한 액세스 제한을 정의합니다. iOS MDM 구성에는 두 가지 유형이 있습니다.

- **iOS MDM - 대량 제공:** 엔터프라이즈가 구매하고 대량 배포의 일환으로 제공된 기기용입니다.
- **iOS MDM - 개별 제공:** 하나씩 제공된 기기용입니다. 감독 기기 및 사용자 등록 기기에는 적용되지 않습니다.

모든 공간에서 각 유형 중 하나만 제공되고 허용됩니다.

## iOS MDM 구성 편집

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**으로 이동합니다.
3. 편집할 iOS MDM 구성을 선택합니다.
4. 연필(편집) 아이콘을 클릭하여 구성을 편집합니다.
5. 다음 지침을 사용하여 변경합니다.
6. **완료**를 클릭하세요.

| 설정 항목 | 설정하기 |
| --- | --- |
| MDM 액세스 권한 | |
| 기기 잠금 및 암호 제거 허용 | 암호 준수 구성의 실행을 방지하는 설정을 해제합니다. |
| 기기 삭제 허용 | 기기 지우기 작업의 실행을 방지하는 설정을 해제합니다. |
| 네트워크 정보 쿼리(전화/SIM 번호, MAC 주소) 허용 | 기기를 네트워킹 정보 보고에서 배제하는 설정을 해제합니다.<br>이 옵션을 선택 취소하면 기기 목록 보기 및 기기 상세 정보 보기에는 더 이상 보고되지 않는 네트워크 정보가 N/A로 표시됩니다. 또한, 해당 기기에서는 로밍 정책을 실행할 수 없습니다. |
| **프로필 제거 암호** | |
| 프로필 제거를 위한 암호 | 비밀번호를 지정합니다. 기기에서 프로필을 삭제하는 동안 비밀번호를 입력하라는 메시지가 표시됩니다. |
| 필수 앱 추가(iOS 15+) | |
| 조회로 추가 | App Store에서 앱 이름을 입력하여 앱을 검색하고 필수 앱을 선택합니다.<br>한 번에 한 앱만 추가할 수 있습니다. 한 앱을 선택하면 다른 앱이 비활성화됩니다. |
| 수동 추가 | 앱의 iTunes ID를 입력합니다. |

변경 사항은 변경한 후에 프로비저닝된 기기에만 적용됩니다.

# 10.10.8.8. macOS MDM 프로필 구성

macOS MDM 구성은 MDM용 Ivanti Neurons에 대한 액세스 제한을 정의합니다. macOS MDM 구성은 개별적으로 프로비저닝되므로 기기는 하나씩 프로비저닝됩니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**으로 이동합니다.
3. 편집할 macOS MDM 구성을 선택합니다.
4. 연필(편집) 아이콘을 클릭하여 구성을 편집합니다.
5. 다음 지침을 사용하여 변경합니다.
6. **완료**를 클릭하세요.

| 설정 항목 | 설정하기 |
| --- | --- |
| 기기 잠금 및 암호 제거 허용 | 암호 준수 구성의 실행을 방지하는 설정을 해제합니다. |
| 기기 삭제 허용 | 기기 지우기 작업의 실행을 방지하는 설정을 해제합니다. |
| 네트워크 정보 쿼리(전화/SIM 번호, MAC 주소) 허용 | 기기를 네트워킹 정보 보고에서 배제하는 설정을 해제합니다.<br>이 옵션을 선택 취소하면 기기 목록 보기 및 기기 상세 정보 보기에는 더 이상 보고되지 않는 네트워크 정보가 N/A로 표시됩니다. 또한, 해당 기기에서는 로밍 정책을 실행할 수 없습니다. |
| **프로필 제거 암호** | |
| 프로필 제거를 위한 암호 | 비밀번호를 지정합니다. 기기에서 프로필을 삭제하는 동안 비밀번호를 입력하라는 메시지가 표시됩니다. |

변경 사항은 변경한 후에 프로비저닝된 기기에만 적용됩니다.

# 10.10.8.9. 콘텐츠 캐싱

**라이센스:** Gold

**적용 대상:** macOS 10.13.4 또는 지원되는 최신 버전.

App Store 소프트웨어의 로컬 사본을 활성화하고 연결된 클라이언트가 소프트웨어 및 앱 다운로드를 더 빠르게 할 수 있도록 콘텐츠 캐싱 서비스를 구성합니다.

## 콘텐츠 캐싱 구성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **캐싱**을 입력한 다음, **콘텐츠 캐싱** 구성을 클릭합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. 콘텐츠 캐싱 구성 설정을 입력합니다.
6. **다음**을 클릭하세요.
7. **이 구성 활성화** 옵션을 선택합니다.
8. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
9. **완료**를 클릭합니다.

## 콘텐츠 캐싱 구성 설정

다음 표의 설정을 사용하여 콘텐츠 캐싱을 구성합니다. 이 설정에 대한 자세한 내용은 **Apple 문서**를 참조하십시오.

| 설정 항목 | 설명 |
| --- | --- |
| 시스템이 캐시에서 콘텐츠를 자동으로 제거하도록 허용<br>(macOS 10.15 또는 지원되는 최신 버전에서 사용 가능.) | 다른 앱을 위한 디스크 공간이 필요할 때 시스템이 캐시에서 콘텐츠를 자동으로 제거하도록 허용합니다(예: 컴퓨터의 여유 디스크 공간이 부족할 경우).<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 개인 캐싱 허용 | 사용자의 iCloud 데이터를 캐시합니다. 클라이언트가 이 설정에 대한 변경사항에 반응하는 데 약간의 시간(몇 시간 또는 며칠)이 소요될 수 있으므로, 즉각적인 효과는 없습니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 공유 캐싱 허용 | 앱 및 소프트웨어 업데이트와 같은 비-iCloud 콘텐츠를 캐시합니다. 클라이언트가 이 설정에 대한 변경사항에 반응하는 데 약간의 시간(몇 시간, 며칠)이 소요될 수 있으므로, 즉각적인 효과는 없습니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 콘텐츠 캐시 자동 활성화 허용 | 가능할 때 콘텐츠 캐시를 자동으로 활성화하여 비활성화되지 않도록 합니다. |
| 테더링 캐싱 자동 활성화 허용<br>(macOS 10.15.4 또는 지원되는 최신 버전에서 사용 가능) | 가능할 때 인터넷 연결 공유를 자동으로 활성화하여 인터넷 연결 공유가 비활성화되지 않도록 합니다. |
| 테더링 캐싱 비활성화 | 테더링 캐싱을 비활성화합니다. 테더링 캐싱 비활성화 옵션은 테더링 캐싱 자동 활성화 허용 옵션을 재정의합니다. |
| 캐시 한계 | 콘텐츠 캐시에 사용될 디스크 공간의 최대 바이트 수입니다. 0의 값은 무제한 디스크 공간을 의미합니다.<br>기본값: 0 |
| 데이터 경로 | 캐시된 콘텐츠를 저장하는 데 사용되는 디렉토리 경로입니다. 이 설정을 수동으로 변경하면 기존 위치에서 새 위치로 캐시된 콘텐츠가 자동으로 이동하지 않습니다. 콘텐츠를 자동으로 이동하려면 공유 환경설정의 콘텐츠 캐싱 창을 사용하십시오.<br>값은 /Library/Application Support/Apple/AssetCache/Data여야(또는 로 끝나야) 합니다. |
| 알림 표시 허용<br>(macOS 10.15 또는 지원되는 최신 버전에서 사용 가능.) | 콘텐츠 캐싱에는 화면 상단 모서리의 시스템 알림으로 예외적인 조건(경보)이 표시됩니다. |
| 기기 절전 해제 유지<br>(macOS 10.15 또는 지원되는 최신 버전에서 사용 가능.) | 콘텐츠 캐싱이 켜져 있는 동안은 컴퓨터가 절전되지 않도록 합니다(시스템 환경설정 > 공유 > 콘텐츠 캐싱 켜짐). |
| **범위 수신** | 서브할 다양한 클라이언트 IP 주소를 설명하는 사전의 배열입니다. |
| 첫 번째 IP 주소 | 수신 범위 내 클라이언트의 IP 주소입니다. |

| 설정 항목 | 설명 |
| --- | --- |
| 마지막 IP 주소 | 수신 범위 내 클라이언트의 마지막 IP 주소입니다. |
| IP 주소 유형 | 다음 옵션 중 하나를 선택합니다.<br>• IPv4(기본)<br>• IPv6 |
| 범위만 수신 허용 | 콘텐츠 캐시는 수신 범위 내의 클라이언트에만 콘텐츠를 제공합니다. |
| 피어 및 상위에서 수신 허용 | 콘텐츠 캐시는 수신 범위, 피어 수신 범위, 그리고 상위의 연합에서 클라이언트에 콘텐츠를 제공합니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 로컬 서브넷만 허용 | 콘텐츠 캐시는 동일한 인접 로컬 네트워크에서만 클라이언트에 콘텐츠를 제공합니다. 콘텐츠 캐시에 의해 도달 가능한 다른 네트워크에서는 클라이언트에 아무런 콘텐츠도 제공되지 않습니다. 이 옵션이 활성화되면 수신 범위는 무시됩니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 클라이언트 ID 로깅 | 콘텐츠 캐시는 IP 주소와 콘텐츠를 요청하는 클라이언트의 포트 번호를 기록합니다. |
| 상위 선택 정책 | 다음 정책 옵션 중 하나를 선택합니다.<br>• 첫 번째 사용 가능<br>• URL 경로 해시<br>• 라운드 로빈(기본)<br>• 랜덤<br>• 스티커 - 이용 가능 |
| 상위 | Apple에서 직접 다운로드하거나 Apple에 직접 업로드하는 대신 이 캐시가 다운로드하거나 업로드해야 하는 다른 콘텐츠 캐시의 로컬 IP 주소 배열입니다.<br>하나 이상의 IP 주소를 추가하려면 **+추가**를 클릭합니다. |
| 피어 로컬 서브넷만 허용 | 콘텐츠 캐시는 동일한 공용 IP 주소를 기기로 사용하는 콘텐츠 캐시를 통해서보다는 동일한 인접 로컬 네트워크의 다른 콘텐츠 캐시를 통해서만 피어링합니다.<br>기본적으로 이 옵션은 활성화되어 있습니다. |
| 포트 | 콘텐츠 캐시가 업로드 또는 다운로드에 대해 요청하는 TCP 포트 번호입니다. 임의로 이용 가능한 포트를 선택하려면 포트를 0으로 설정하십시오.<br>기본값: 0 |
| **공개 범위** | MDM용 Ivanti Neurons 서버가 클라이언트를 콘텐츠 캐시에 매칭하는 데 사용해야 하는 다양한 공개 IP 주소를 설명하는 사전의 배열입니다. |
| 첫 번째 IP 주소 | 공개 범위 내 서버의 첫 번째 IP 주소입니다. |
| 마지막 IP 주소 | 공개 범위 내 서버의 마지막 IP 주소입니다. |
| IP 주소 유형 | 다음 옵션 중 하나를 선택합니다.<br>• IPv4(기본)<br>• IPv6 |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.8.10. Android 바로가기 생성

바로가기는 허용 목록으로 설정된 브라우저를 사용해 키오스크 모드에서만 사용할 수 있습니다. 브라우저는 잠금 및 키오스크 구성에서 허용 목록으로

설정되어야 합니다. MDM용 Ivanti Neurons 키오스크 시작 관리자에 바로 가기가 나타납니다.

**절차**

1. **구성**으로 이동합니다. **> +추가**
2. **Android 바로 가기**를 클릭하여 **Android 바로 가기 구성 생성** 페이지를 표시합니다.
3. **이름** 필드에 구성의 이름을 입력합니다.
4. **설명** 필드에 구성의 설명을 입력합니다.
5. **레이블** 필드에 바로 가기의 고유 레이블을 입력합니다.
6. **URL** 필드에 바로 가기 대상의 URL을 입력합니다.
7. 선택에 따라 아이콘 필드에 파일을 끌어다 놓거나 **파일 선택**을 클릭하여 바로 가기 아이콘으로 선택할 파일을 찾아볼 수 있습니다.
8. **다음**을 클릭하세요.

# 10.10.8.11. 접근성 설정 구성 생성

이 구성을 통해 기업은 Apple 장치에서 접근성 설정을 제한, 변경 또는 구성할 수 있습니다.

**절차**

1. **구성**으로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **접근성 설정 구성**을 클릭합니다.
4. 다음 표에 지정된 설정을 구성합니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 접근성 설정 중 하나 선택<br><br>**접근성 설정** | • **접근성 설정**: macOS 장치에서 접근성 설정을 구성하는 데 사용합니다.<br>• **접근성 설정 제한**: iOS 장치의 접근성 설정 변경을 제한할 때 사용합니다.<br><br>**구성 설정** |
| 원거리 지점 닫기 | 확대/축소 설정에서 최소 확대/축소 레벨 |
| 근거리 지점 닫기 | 확대/축소 설정에서 최대 확대/축소 레벨 |
| | 확대/축소 옵션에서 '스크롤 제스처 사용' 활성화 |
| | 확대/축소 옵션에서 '부드러운 이미지' 활성화 |
| 대비 값 | 값 지정 |
| | 확인란 선택 - 오디오 옵션에서 "화면 깜박임" 활성화 |
| | 확인란 선택 - 마우스 및 트랙패드 옵션에서 마우스 키 활성화 |
| 커서 크기 | 값 지정 |
| | 체크박스 선택 - 내장 트랙패드 무시 |
| 마우스 드라이버 초기 지연 | 값 지정 |
| 마우스 드라이버 최대 속도 | 값 지정 |
| 키보드 옵션에서 '느린 키' 활성화 | 확인란 선택 |
| 느린 키에 '클릭 키 소리' 활성화 | 확인란 선택 |
| 느린 키 지연 | 확인란 선택 |
| 값을 밀리초 단위로 지정 | 확인란 선택 |
| 확인란 선택 - 스테레오 오디오를 모노로 재생 | 확인란 선택 |
| 키보드 옵션에서 고정 키 활성화 | 확인란 선택 |
| 수정자 키가 고정 키로 설정된 경우 신호음 활성화 | 확인란 선택 |
| 고정 키에 대해 화면에서 누른 키 표시 활성화 | 확인란 선택 |
| 보이스 오버 활성화 | 확인란 선택 |
| 디스플레이 조정에서 색상 반전 활성화 | 확인란 선택 |
| **접근성 제한** | **구성 설정** |

| 설정 항목 | 설정하기 |
| --- | --- |
| 굵은 텍스트 활성화 | 확인란 선택 |
| 대비 증가 활성화 | 확인란 선택 |
| 모션 감소 활성화 | 확인란 선택 |
| 투명성 감소 활성화 | 확인란 선택 |
| 동적 텍스트 사용을 지원하는 접근성 텍스트 크기 앱 | 드롭다운 목록에서 옵션 선택 |
| 터치 조정 활성화 | 확인란 선택 |
| 보이스 오버 활성화 | 확인란 선택 |
| 확대/축소 활성화 | 확인란 선택 |

5. 배포 옵션을 선택하고 해당하는 경우 필요한 세부 정보를 지정합니다.
6. **완료**를 클릭하세요.

# 10.10.8.12. 화면 보호기 구성 생성

화면 보호기 구성을 사용하면 비밀번호, 유휴 시간, 모듈 경로, 이름과 같은 옵션을 추가할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**을 클릭합니다.
3. **+추가**를 클릭합니다.
4. 검색 필드에 화면을 입력하고 **화면 보호기**를 클릭합니다.
   화면 보호기 구성 생성 세부 정보 페이지가 나타납니다.
5. 이 페이지에서 설정을 구성합니다. 값에 대한 안내는 **화면 보호기 구성 설정** 항목의 표를 참조하십시오.
6. **다음**을 클릭해 배포 설정을 구성한 다음 **완료**를 클릭합니다.

## 화면 보호기 구성 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| **이름**(필수) | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 비밀번호 확인 체크박스 | 체크박스를 선택하면 화면 보호기가 잠금 해제되거나 중지될 때 기기 사용자에게 비밀번호를 입력하라는 메시지가 표시됩니다. (macOS 10.13 이상에서 사용 가능) |
| **비밀번호 지연 확인** | 지연 시간을 초 단위로 지정합니다. |
| **로그인 창 유휴 시간** | 화면 보호기가 표시될 유휴 시간을 초 단위로 지정합니다. |
| **화면 보호기 모듈 경로** | 화면 보호기 모듈의 경로를 지정합니다. |
| **화면 보호기 모듈 이름**(필수) | 화면 보호기의 이름을 입력합니다. |

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.8.13. 사용자 화면 보호기 구성

사용자 화면 보호기 구성을 사용하면 비밀번호, 유휴 시간, 모듈 경로, 이름과 같은 옵션을 추가할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **구성**을 클릭합니다.
3. **+추가**를 클릭합니다.
4. 검색 필드에 화면을 입력하고 **사용자 화면 보호기**를 클릭합니다.
   사용자 화면 보호기 구성 생성 세부 정보 페이지가 나타납니다.
5. 이 페이지에서 설정을 구성합니다. 값에 대한 안내는 **사용자 화면 보호기 구성 설정** 항목의 표를 참조하십시오.
6. **다음**을 클릭해 배포 설정을 구성한 다음 **완료**를 클릭합니다.

## 사용자 화면 보호기 구성 설정

| 설정 항목 | 설정하기 |
|---|---|
| **이름**(필수) | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **유휴 시간** | 화면 보호기가 표시될 유휴 시간을 초 단위로 지정합니다. |
| **화면 보호기 모듈 경로** | 화면 보호기 모듈의 경로를 지정합니다. |
| **화면 보호기 모듈 이름**(필수) | 화면 보호기의 이름을 입력합니다. |

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.8.14. 기기 이름 설정

## 라이센스: Silver

기본 기기 이름 구성을 사용하면 등록 또는 사후 등록 수준에서 기기로 푸시다운되고 기기 이름 지정을 허용하는 새 구성을 생성할 수 있습니다. 관리자는 **감독 대상 iOS 8 기기**에 대해서만 기본 기기 이름을 정의할 수 있습니다. 다음 변수를 사용하여 기기 이름을 생성할 수 있습니다.

- 장치 일련 번호
- 장치 IMEI
- 기기 모델
- MDM용 Ivanti Neurons 사용자 이름(로컬 사용자 한정)
- LDAP 조직 단위(OU)
- LDAP 공통 이름(CN)

예를 들어, LDAP에 지정되었듯이 기기 일련 번호로 시작하고 사용자 조직으로 끝나는 기기 이름에 $-$를 입력합니다.

**기본 기기 이름 설정(iOS용)**

| 설정 항목 | 설정하기 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 기기 이름<br><br><br>설명 | 사용 가능한 기기와 LDAP 속성을 비롯한 기본값 기기 이름의 형식을 입력합니다.<br>기기 이름이 63자를 초과할 경우 기기에 올바르게 표시하기 위해 잘립니다.<br><br>현재 설정에 대한 간략한 설명을 입력합니다. |

> $를 입력하면 현재 필드에 해당하는 지원 변수 목록을 확인할 수 있습니다.

**기기 이름 설정(Android)**

Android 장치 이름은 Go app에서 검색할 수 있습니다. 관리자가 기기 세부 정보 보고서를 생성할 때 실제 기기 이름이 기기 모델 또는 제조업체 이름 대신 표시됩니다. 사용자가 기기 이름을 변경하는 경우 다음에 보고서가 생성될 때 새 이름이 표시됩니다. 각 기기 이름은 **기기** > **설정** > **기기 이름**에서 볼 수 있습니다.

# 10.10.8.15. 기기 배경화면 설정

## 라이센스: Silver

기기 배경화면 구성은 기기 소유자 모드의 Android 7.0 기기 또는 COPE(회사 소유 개인 지원) 기기(Android 11 EPO 모드 기기 제외)의 홈 화면 및 잠금 화면에 대한 기본 배경화면 이미지를 정의합니다.

## Android 배경화면 설정

Android 기기용 기본 배경 이미지를 정의하려면:

1. **구성**으로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **기기 배경화면**을 클릭합니다.
4. Android 구성 설정 섹션을 보려면 Android 아이콘을 클릭하고 다음의 설정을 구성합니다.
5. **다음**을 클릭합니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **Android 배경화면 업로드** | |
| 홈 화면과 잠금 화면에 동일한 이미지 사용 | 두 화면에 하나의 이미지를 업로드하려면 선택합니다. |
| **홈 화면** | 원하는 이미지 파일을 드래그하거나 **파일 선택**을 클릭해 해당 파일을 선택합니다. |
| **잠금 화면** | 원하는 이미지 파일을 드래그하거나 **파일 선택**을 클릭해 해당 파일을 선택합니다. |

6. 다음 배포 옵션 중 하나를 선택합니다.

- **모든 기기**
- **배포 안 함**(기본값)
- **사용자 지정**

7. **완료**를 클릭하세요.

> 업로드한 이미지는 .jpg 또는 .png 형식이어야 합니다.

## iOS 배경화면 설정

iOS 기기의 기본 배경화면 이미지를 설정할 수 있습니다.

> 이 설정은 감독 대상 기기에만 적용됩니다.

1. **구성**으로 이동합니다.
2. **+ 추가**를 클릭합니다.

3. **기기 배경화면**을 클릭합니다.
4. iOS 구성 설정 섹션을 보려면 iOS 아이콘을 클릭하고 다음의 설정을 구성합니다.
5. **다음**을 클릭하세요.

| 설정 항목 | 설정하기 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| iPhone 배경화면 업로드 | |
| 홈 화면과 잠금 화면에 동일한 이미지 사용 | 아이폰용 단일 이미지를 업로드할 수 있습니다. |
| 홈 화면 | 원하는 이미지 파일을 드래그하거나 **파일 선택**을 클릭해 해당 파일을 선택합니다. |
| 잠금 화면 | 원하는 이미지 파일을 드래그하거나 **파일 선택**을 클릭해 해당 파일을 선택합니다. |
| iPad 배경화면 업로드 | |
| 홈 화면과 잠금 화면에 동일한 이미지 사용 | 아이패드용단일 이미지를 업로드할 수 있습니다. |
| 홈 화면 | 원하는 이미지 파일을 드래그하거나 **파일 선택**을 클릭해 해당 파일을 선택합니다. |
| 잠금 화면 | 원하는 이미지 파일을 드래그하거나 **파일 선택**을 클릭해 해당 파일을 선택합니다. |

6. 다음 옵션 중 하나를 선택합니다.
- **모든 기기**
- **배포 안 함**(기본값)
- **사용자 지정**
7. **완료**를 클릭하세요.

> 업로드한 이미지는 640W x 1136H 크기이고 .jpg 또는 .png 형식이어야 합니다.

## macOS 배경화면 설정

macOS 기기용 기본 배경 이미지를 정의하려면:

1. **구성**으로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **기기 배경화면**을 클릭합니다.
4. macOS 아이콘을 클릭하여 macOS용 구성 설정 섹션을 표시합니다.
5. 데스크톱 그림 경로를 입력합니다.
6. **다음**을 클릭하세요.
7. 다음 옵션 중 하나를 선택합니다.
    - **모든 기기**
    - **배포 안 함**(기본값)

- **사용자 지정**

8. **완료**를 클릭합니다.

> 제한을 기반으로 배경화면을 변경할 수 있습니다. macOS 제한 구성 **배경화면 수정 허용**이 활성화된 경우 배경화면을 수정할 수 있습니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.8.16. EMA 서버 통합 구성

EMA 서버 통합 구성으로 Windows 10 기기를 구성된 Intel EMA 서버에 연결할 수 있습니다. 구성된 Intel EMA 서버에 기기를 연결하려면 원본 EMA 에이전트의 설치 디렉터리를 제공하고 새 EMA 서버에서 EMA 에이전트 .msh 파일을 업로드해야 합니다.

이 기능을 사용하려면 Bridge가 필요합니다. 자세한 내용은 **Bridge**를 참조하십시오.

**절차**

1. **구성 > +추가**로 이동합니다.
2. **EMA 서버 통합** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 구성 설정 섹션에서 **파일 선택**을 클릭하여 EMA 에이전트 .msh 파일을 선택합니다.

> msh 파일은 EMA 서버에서 다운로드할 수 있는 에이전트 정책 파일입니다.

5. 원본 **EMA 에이전트 설치 디렉터리** 필드에서 원본 EmaAgent.exe 파일을 설치할 위치를 입력합니다.
6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
8. **완료**를 클릭하세요.

# 10.10.8.17. 절전 구성

MDM용 Ivanti Neurons 은(는) Windows 및 macOS 기기에서 에너지 세이버 설정을 구성하는 데 사용하는 페이로드에 대해 에너지 세이버 구성을 활성화합니다.

**적용 대상**:

- Windows 10부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.
- macOS 10.7부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **절전** 구성을 검색하고 선택합니다.
3. OS 선택 섹션에서 **Windows** 또는 **macOS**를 선택하고 **다음**을 클릭합니다.
4. **+설명 추가**를 클릭하여 구성에 대한 간단한 설명을 입력합니다.
5. Windows의 경우 다음 **에너지 세이버** 설정을 구성합니다:
   - 배터리가 있는 기기
   - 기기 연결됨
6. 다음 **절전** 설정을 구성합니다.
   - 데스크톱 AC 절전 설정
   - 컴퓨터 시작 또는 종료 일정 설정
   - 노트북 AC 절전 설정
   - 노트북 배터리 절전 설정
7. **다음**을 클릭해 배포 설정을 구성합니다.
8. 배포 옵션 중 하나를 선택하여 **절전** 구성을 설정하십시오. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
9. **완료**를 클릭하세요.

## Windows 절전 구성

새로운 에너지 세이버 구성이 기기에 적용되거나 기존 에너지 세이버 구성 설정이 수정된 경우 변경 사항을 적용하려면 기기를 재부팅해야 합니다.

### 배터리가 있는 기기

기기가 배터리 전원을 사용하는 경우 표에 있는 다음의 에너지 세이버 설정을 사용합니다:

| 설정 항목 | 설명 |
| --- | --- |
| **에너지 세이버 기능을 켜기 위한 배터리 제한 수준** | 기기가 배터리 전원을 사용하는 경우 배터리 충전 수준을 입력하여 에너지 세이버 기능을 켭니다. 0~100 사이의 값을 입력할 수 있습니다. 배터리 충전 수준을 나타내는 백분율 값을 입력합니다. 예를 들어, 80으로 설정하면 배터리 잔량이 80% 이하일 때 에너지 세이버 기능이 켜집니다.<br>값을 입력하지 않으면 MDM용 Ivanti Neurons에서 이 설정을 변경하거나 업데이트하지 않습니다. 기본적으로 Windows에서는 이 값을 70%로 설정합니다. |
| **뚜껑을 닫았을 때** | • **아무런 조치도 취하지 않음**: 기기가 켜져 있고 배터리 전원을 계속 사용합니다.<br>• **절전**: 기기가 절전 모드로 전환되어 소량의 배터리가 소모됩니다. 컴퓨터는 여전히 켜져 있으며 열려 있는 앱과 파일은 RAM(Random Access Memory)에 저장됩니다.<br>• **최대 절전 상태**: 기기가 최대 절전 모드로 전환됩니다. 열려 있는 앱과 파일은 하드 디스크에 저장되며, 기기가 꺼집니다.<br>• **종료**: 기기가 종료됩니다. 열려 있는 앱과 파일이 저장되지 않고 닫힙니다. |
| **전원 버튼을 선택한 경우** | • **아무런 조치도 취하지 않음**: 기기가 켜져 있고 배터리 전원을 계속 사용합니다.<br>• **절전**: 기기가 절전 모드로 전환되어 소량의 배터리가 소모됩니다. 컴퓨터는 여전히 켜져 있으며 열려 있는 앱과 파일은 RAM에 저장됩니다.<br>• **최대 절전 상태**: 기기가 최대 절전 모드로 전환됩니다. 열려 있는 앱과 파일은 하드 디스크에 저장되며, 기기가 꺼집니다.<br>• **종료**: 기기가 종료됩니다. 열려 있는 앱과 파일이 저장되지 않고 닫힙니다. |
| **절전 버튼을 선택한 경우** | • **아무런 조치도 취하지 않음**: 기기가 켜져 있고 배터리 전원을 계속 사용합니다.<br>• **절전**: 기기가 절전 모드로 전환되어 소량의 배터리가 소모됩니다. 컴퓨터는 여전히 켜져 있으며 열려 있는 앱과 파일은 RAM에 저장됩니다.<br>• **최대 절전 상태**: 기기가 최대 절전 모드로 전환됩니다. 열려 있는 앱과 파일은 하드 디스크에 저장되며, 기기가 꺼집니다.<br>• **종료**: 기기가 종료됩니다. 열려 있는 앱과 파일이 저장되지 않고 닫힙니다. |
| **하이브리드 절전 모드 켜기** | • **참**: 기기가 하이브리드 절전 모드로 진입할 수 있습니다. 열려 있는 앱과 파일은 RAM과 하드 디스크에 저장됩니다. 소량의 배터리 충전량을 사용합니다.<br>• **거짓**: 기기가 하이브리드 절전 모드로 전환되지 않도록 합니다. |

## 기기 연결됨

기기가 외부 전원의 전원을 사용하는 경우 표에 있는 다음의 설정을 사용합니다:

| 설정 항목 | 설명 |
| --- | --- |
| **에너지 세이버 기능을 켜기 위한 배터리 제한 수준** | 기기가 연결되면 배터리 충전 수준을 입력하여 에너지 세이버를 켭니다. 0부터 100까지의 값을 입력할 수 있습니다. 배터리 충전 수준을 나타내는 백분율 값을 입력합니다. 예를 들어, 80으로 설정하면 배터리 잔량이 80% 이하일 때 에너지 세이버 기능이 켜집니다.<br>값을 입력하지 않으면 MDM용 Ivanti Neurons에서 이 설정을 변경하거나 업데이트하지 않습니다. 기본적으로 Windows에서는 이 값을 70%로 설정합니다. |
| **뚜껑을 닫았을 때**<br><br>**전원 버튼을 선택한 경우** | • **아무런 조치도 취하지 않음**: 기기가 켜져 있고 외부 전원을 계속 사용합니다.<br>• **절전**: 기기가 절전 모드로 전환되고 소량의 외부 전원을 사용합니다. 컴퓨터는 여전히 켜져 있으며 열려 있는 앱과 파일은 RAM에 저장됩니다.<br>• **최대 절전 상태**: 기기가 최대 절전 모드로 전환됩니다. 열려 있는 앱과 파일은 하드 디스크에 저장되며, 기기가 꺼집니다.<br>• **종료**: 기기가 종료됩니다. 열려 있는 앱과 파일이 저장되지 않고 닫힙니다.<br><br>• **아무런 조치도 취하지 않음**: 기기가 켜져 있고 외부 전원을 계속 사용합니다.<br>• **절전**: 기기가 절전 모드로 전환되고 소량의 외부 전원을 사용합니다. 컴퓨터는 여전히 켜져 있으며 열려 있는 앱과 파일은 RAM에 저장됩니다.<br>• **최대 절전 상태**: 기기가 최대 절전 모드로 전환됩니다. 열려 있는 앱과 파일은 하드 디스크에 저장되며, 기기가 꺼집니다.<br>• **종료**: 기기가 종료됩니다. 열려 있는 앱과 파일이 저장되지 않고 닫힙니다. |
| **절전 버튼을 선택한 경우**<br><br>**하이브리드 절전 모드 켜기** | • **아무런 조치도 취하지 않음**: 기기가 켜져 있고 외부 전원을 계속 사용합니다.<br>• **절전**: 기기가 절전 모드로 전환되고 소량의 외부 전원을 사용합니다. 컴퓨터는 여전히 켜져 있으며 열려 있는 앱과 파일은 RAM에 저장됩니다.<br>• **최대 절전 상태**: 기기가 최대 절전 모드로 전환됩니다. 열려 있는 앱과 파일은 하드 디스크에 저장되며, 기기가 꺼집니다.<br>• **종료**: 기기가 종료됩니다. 열려 있는 앱과 파일이 저장되지 않고 닫힙니다.<br><br>• **참**: 기기가 하이브리드 절전 모드로 진입할 수 있습니다. 열려 있는 앱과 파일은 RAM과 하드 디스크에 저장됩니다. 소량의 외부 전원을 사용합니다.<br>• **거짓**: 기기가 하이브리드 절전 모드로 전환되지 않도록 합니다. |

# macOS 절전 구성

## 데스크톱 AC 절전 설정

macOS 데스크톱 장치의 AC 절전 설정을 구성하려면 다음 설정을 사용합니다.

| 설정 항목 | 설명 |
| --- | --- |
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **정전 후 자동 시작** | 정전 후 자동으로 장치 시작을 활성화합니다. |
| **다음 이후에 하드 디스크를 절전 모드로 전환**<br><br>**다음 이후에 디스플레이 끄기** | 1분~180분 사이의 고정 간격으로 하드 디스크를 절전 모드로 전환하려면 확인란을 활성화합니다.<br>0분으로 설정하면 하드 디스크가 절전 모드로 전환되지 않습니다.<br><br>1~180분 사이의 고정 간격으로 디스플레이를 끄려면 확인란을 활성화합니다.<br>0분으로 설정하면 디스플레이가 절대 꺼지지 않습니다. |
| **동적 전력 단계** | 동적 전력 단계를 활성화하려면 확인란을 선택합니다. |
| **프로세서 속도 감소** | 프로세서 속도를 줄이려면 확인란을 선택합니다. |
| **다음 이후에 컴퓨터를 절전 모드로 전환** | 1~180분 사이의 고정 간격으로 컴퓨터를 절전 모드로 전환하려면 확인란을 선택합니다.<br>0분으로 설정하면 컴퓨터가 절전 모드로 전환되지 않습니다. |
| **네트워크 액세스를 위해 절전 모드 해제**<br><br>**모뎀 벨소리 절전 모드 해제** | 네트워크 액세스를 위해 컴퓨터의 절전 모드를 해제하려면 확인란을 선택합니다.<br><br>모뎀 벨소리에 대한 컴퓨터의 절전 모드를 해제하려면 확인란을 선택합니다. |

## 컴퓨터 시작 또는 종료 일정 설정

다음 설정을 사용하여 macOS 장치의 시작 또는 종료 예약 시간을 구성합니다.

## 장치 설정 끄기

고정 간격으로 장치를 종료하려면 **장치 끄기** 확인란을 선택합니다.

| 설정 항목 | 설명 |
| --- | --- |
| **이벤트 유형** | 드롭다운 목록에서 이벤트 유형을 한 가지 선택합니다.<br>• 절전 모드<br>• 재시작<br>• 종료 |
| **시기** | 이벤트 유형을 예약할 요일을 하나 이상 선택하십시오. |
| **시간** | 이벤트 유형을 예약할 시간을 선택하십시오. |

## 장치 설정 시작 또는 절전 모드 해제

고정 간격으로 장치 절전 모드를 해제하려면 **장치 시작 또는 절전 모드 해제** 확인란을 선택합니다.

| 설정 항목 | 설명 |
| --- | --- |
| **이벤트 유형** | 드롭다운 목록에서 이벤트 유형을 한 가지 선택합니다.<br>• 절전 모드 해제<br>• 시작/절전 모드 해제 |
| **시기** | 이벤트 유형을 예약할 요일을 하나 이상 선택하십시오. |
| **시간** | 이벤트 유형을 예약할 시간을 선택하십시오. |

## 노트북 AC 절전 설정

다음 설정을 사용하여 macOS 노트북 장치의 AC 절전 설정을 구성합니다.

| 설정 항목 | 설명 |
| --- | --- |
| **정전 후 자동 시작** | 정전 후 자동으로 장치 시작을 활성화합니다. |
| **다음 이후에 하드 디스크를 절전 모드로 전환** | 1분~180분 사이의 고정 간격으로 하드 디스크를 절전 모드로 전환하려면 확인란을 활성화합니다.<br>0분으로 설정하면 하드 디스크가 절전 모드로 전환되지 않습니다. |
| **다음 이후에 디스플레이 끄기** | 1~180분 사이의 고정 간격으로 디스플레이를 끄려면 확인란을 활성화합니다.<br>0분으로 설정하면 디스플레이가 절대 꺼지지 않습니다. |
| **동적 전력 단계** | 동적 전력 단계를 활성화하려면 확인란을 선택합니다. |
| **프로세서 속도 감소** | 프로세서 속도를 줄이려면 확인란을 선택합니다. |
| **다음 이후에 노트북을 절전 모드로 전환** | 1~180분 사이의 고정 간격으로 노트북을 절전 모드로 전환하려면 확인란을 활성화합니다.<br>0분으로 설정하면 노트북이 절전 모드로 전환되지 않습니다. |
| **네트워크 액세스를 위해 절전 모드 해제** | 네트워크 액세스를 위해 노트북의 절전 모드를 해제하려면 확인란을 선택합니다. |
| **모뎀 벨소리 절전 모드 해제** | 모뎀 벨소리에 대한 노트북 절전 모드를 해제하려면 확인란을 선택합니다. |

## 노트북 배터리 절전 설정

다음 설정을 사용하여 macOS 노트북 배터리 절전 설정을 구성합니다.

| 설정 항목 | 설명 |
| --- | --- |
| **정전 후 자동 시작** | 정전 후 자동으로 장치 시작을 활성화합니다. |
| **다음 이후에 하드 디스크를 절전 모드로 전환** | 1분~180분 사이의 고정 간격으로 하드 디스크를 절전 모드로 전환하려면 확인란을 활성화합니다.<br>0분으로 설정하면 하드 디스크가 절전 모드로 전환되지 않습니다. |
| **다음 이후에 디스플레이 끄기** | 1~180분 사이의 고정 간격으로 디스플레이를 끄려면 확인란을 활성화합니다.<br>0분으로 설정하면 디스플레이가 절대 꺼지지 않습니다. |
| **동적 전력 단계** | 동적 전력 단계를 활성화하려면 확인란을 선택합니다. |
| **프로세서 속도 감소** | 프로세서 속도를 줄이려면 확인란을 선택합니다. |
| **다음 이후에 컴퓨터를 절전 모드로 전환** | 1~180분 사이의 고정 간격으로 노트북 배터리를 절전 모드로 전환하려면 확인란을 활성화합니다.<br>0분으로 설정하면 노트북 배터리가 절전 모드로 전환되지 않습니다. |
| **네트워크 액세스를 위해 절전 모드 해제** | 네트워크 액세스를 위해 노트북 배터리의 절전 모드를 해제하려면 확인란을 선택합니다. |
| **모뎀 벨소리 절전 모드 해제** | 모뎀 벨소리를 위해 노트북 배터리의 절전 모드를 해제하려면 확인란을 선택합니다. |

# 10.10.8.18. 이더넷 구성(macOS)

**라이센스:** Gold

**적용 대상:** macOS 10.13+ 또는 지원되는 최신 버전.

관리자는 이더넷 인터페이스를 다양하게 구성할 수 있습니다. 다음 페이로드를 사용하여 이더넷을 구성할 수 있습니다.

- 글로벌 이더넷
- 첫 번째 활성 이더넷
- 첫 번째 이더넷
- 두 번째 활성 이더넷
- 두 번째 이더넷
- 세 번째 활성 이더넷
- 세 번째 이더넷

> 이더넷을 구성하는 다양한 페이로드로 기본 대체 글로벌, 첫 번째, 첫 번째 활성, 두 번째, 두 번째 활성, 세 번째, 세 번째 활성 이더넷 인터페이스가 있습니다. Apple에는 첫 번째, 첫 번째 활성, 두 번째, 두 번째 활성, 세 번째, 세 번째 활성 이더넷 인터페이스와 관련하여 기존의 알려진 문제가 있습니다.

## 이더넷 구성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.
3. 검색 필드에 **이더넷**을 입력한 다음 **이더넷** 구성을 선택합니다.
4. 구성에 대한 이름 및 설명을 입력합니다.
5. 드롭다운 목록에서 구성 설정을 선택합니다.
6. 이더넷 구성 설정을 입력합니다.
7. **다음**을 클릭하세요.
8. **이 구성 활성화** 옵션을 선택합니다.
9. 구성을 적용하기 위해 다음 채널 옵션 중 하나를 선택합니다.
    - 기기 채널(가장 일반적)
    - 사용자 채널(현재 등록 사용자)
10. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
11. **완료**를 클릭합니다.

## 이더넷 구성 설정

다음 표의 설정을 사용하여 이더넷을 구성합니다. 이 설정에 대한 자세한 내용은 **Apple 문서**를 참조하십시오.

| 설정 항목 | 설명 |
| --- | --- |
| **프로토콜** | |
| **허용된 EAP 유형** | 현재 네트워크 연결에 사용 가능한 EAP 유형을 선택할 수 있습니다.<br>• TLS(Transport Layer Security): TLS는 인터넷의 두 컴퓨터 간 암호화 세션을 설정하는 프로토콜입니다. 이는 서버 ID를 검증하고 해커가 데이터를 가로채지 못하도록 합니다.<br>• TTLS: **내부 ID** 필드에서 OS 기본값, PAP, CHAP, MSCHAP, MSCHAPv2 및 EAP와 같은 인증 프로토콜 중 하나를 선택합니다.<br>• PEAP<br>• LEAP<br>• EAP-SIM: **RAND의 EAP SIM 번호** 필드의 드롭다운 목록에서 RAND 번호를 선택합니다.<br>• EAP-AKA<br>• EAP-FAST: 다음과 같이 인증 방법을 정의하는 EAP-FAST 옵션을 선택할 수 있습니다.<br>  ◦ **PAC 사용**: 프록시 자동 설정(PAC)을 사용하도록 설정할 수 있습니다.<br>  ◦ **PAC 제공**: PAC 제공을 허용하도록 설정할 수 있습니다. 이 옵션을 설정하지 않으면, 장치에 이미 제공되는 PAC만 사용할 수 있습니다. PAC 사용 옵션을 선택한 경우에 한해 설정 가능한 옵션입니다.<br>  ◦ **익명으로 PAC 제공**: 서버 인증 없이 PAC 제공이 허용되도록 설정할 수 있습니다. PAC 제공 옵션을 선택한 경우에 한해 설정 가능한 옵션입니다. |
| **인증** | **사용자 이름**: 네트워크 접속에 필요한 사용자 이름을 지정할 수 있습니다. 해당 항목을 지정하지 않고 비워두면, 장치 사용자에게 이름을 지정하라는 메시지가 표시됩니다.<br>• 연결별 비밀번호 사용: 기기 사용자가 연결을 시도할 때마다 비밀번호를 입력하라는 메시지가 표시되도록 설정할 수 있습니다. 해당 기기가 동일한 네트워크에 재접속할 경우 기기 사용자에게 해당 네트워크에 접속하려면 재인증이 필요하다는 메시지가 표시됩니다. 연결을 시작할 때마다 비밀번호를 재요청합니다.<br>• **네트워크에 연결되면 일회용 비밀번호 메시지 표시**: 구성이 기기로 푸시될 때 한 번만 비밀번호를 요청합니다. 네트워크를 연결하고 해제할 때마다 어떤 비밀번호도 요청하지 않습니다.<br>**비밀번호**: (선택 사항) 현재 네트워크 접속 시 사용될 비밀번호를 입력할 수 있습니다. 비밀번호를 설정하지 않으면 장치 사용자가 해당 네트워크를 접속할 때 필요한 임의 비밀번호를 입력하라는 메시지가 표시됩니다.<br>**외부 ID**: (선택 사항) TTLS, PEAP 및 EAP-FAST의 경우, 기기 사용자가 신원을 숨길 수 있도록 설정할 수 있습니다. 이 옵션을 설정하면 사용자의 실명이 암호화된 터널 내부에서만 표시됩니다. 이 옵션을 사용하면 공격자가 인증 사용자의 이름을 확인할 수 없으므로 보안을 강화할 수 있습니다.<br>**시스템 모드 자격 증명 소스 ID**: 시스템 모드가 컴퓨터 인증에 사용됩니다. 시스템 모드를 사용한 인증은 사용자가 컴퓨터에 로그인하기 전에 발생합니다. 일반적으로 시스템 모드는 로컬 인증 기관에서 발급한 컴퓨터 X.509 인증서 (EAP-TLS)로 인증을 제공하도록 구성됩니다. |
| **신뢰** | **신뢰할 수 있는 인증서:** 목록에서 여러 인증서를 선택하려면 확인란을 선택합니다.<br>**신뢰할 수 있는 서버 인증서 이름**: 인증서 이름을 추가합니다.<br>• **신뢰 예외 허용**: 사용자가 신뢰 결정(대화 상자를 통해)을 수행하도록 허용합니다.<br>• **TLS 인증서 필요**<br>**EAP 인증으로 허용된 최대 TLS 버전** |

| 설정 항목 | 설명 |
| --- | --- |
| | **EAP 인증으로 허용된 최소 TLS 버전**<br>**TLS 신뢰할 수 있는 인증서: MobileIron 에이전트 CA 인증서** |

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.8.19. Google BeyondCorp 구성

MDM용 Ivanti Neurons 은(는) 조건부 액세스를 위해 Google BeyondCorp와 통합될 수 있습니다. MDM용 Ivanti Neurons는 기기 규정 준수 상태 신호를 Google BeyondCorp로 전송합니다. 이렇게 하면 N-MDM을 준수하는 기기만 Google Workspace 애플리케이션에 액세스할 수 있습니다.

**적용 대상**

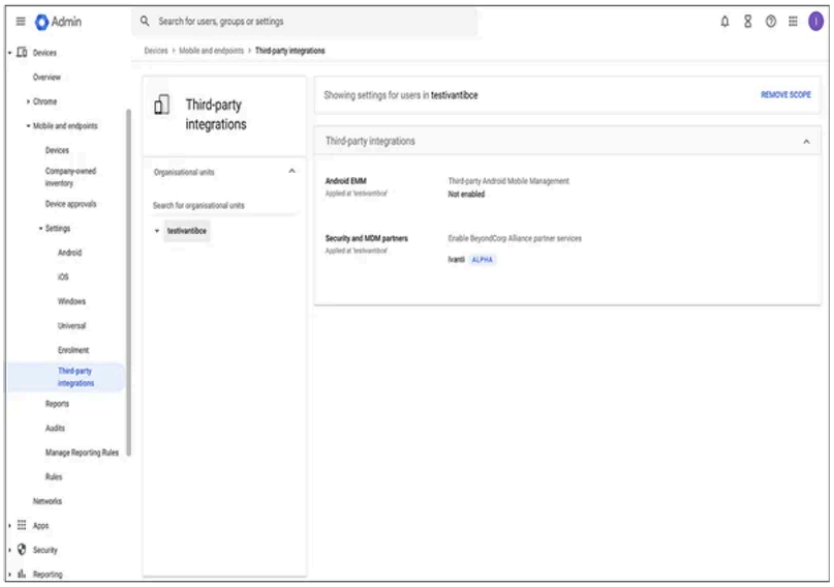
- iOS
- Android
- Windows

**필수 조건**

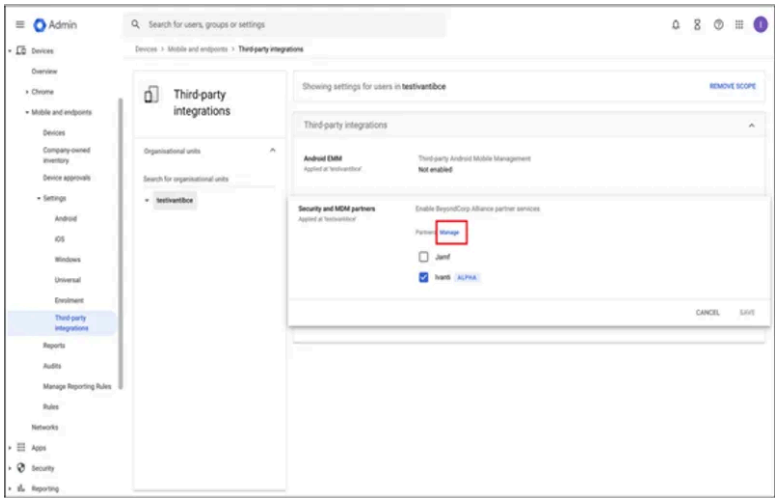
- MDM용 Ivanti Neurons의 경우, Ivanti Professional Plus/Premium 라이선스가 있어야 합니다.
- Google의 경우 BeyondCorp Enterprise, Google Workspace Enterprise 또는 Cloud Identity Premium 라이선스가 있어야 합니다.
- Windows의 경우, 기기에 다음 항목이 설치되어 있어야 합니다.
  - Ivanti Bridge
  - Google Chrome

**절차(Google)**

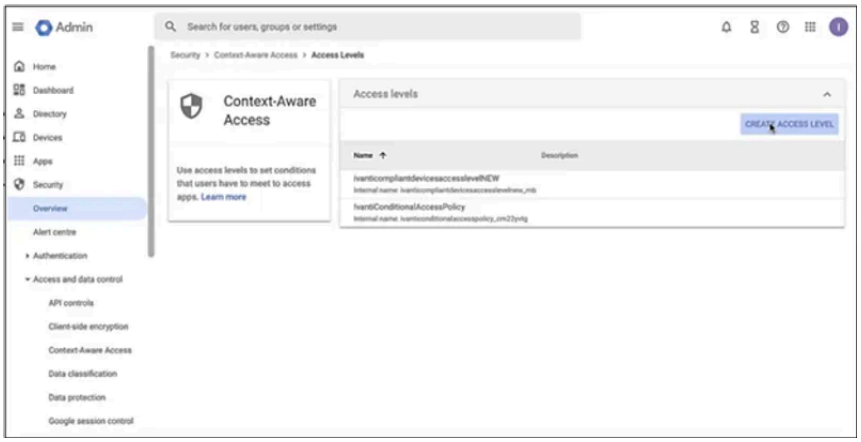
1. **Google 관리 콘솔**에 관리자 자격 증명으로 로그인합니다.
2. **기기** > **모바일 및 엔드포인트** > **설정** > **타사 통합**으로 이동합니다.



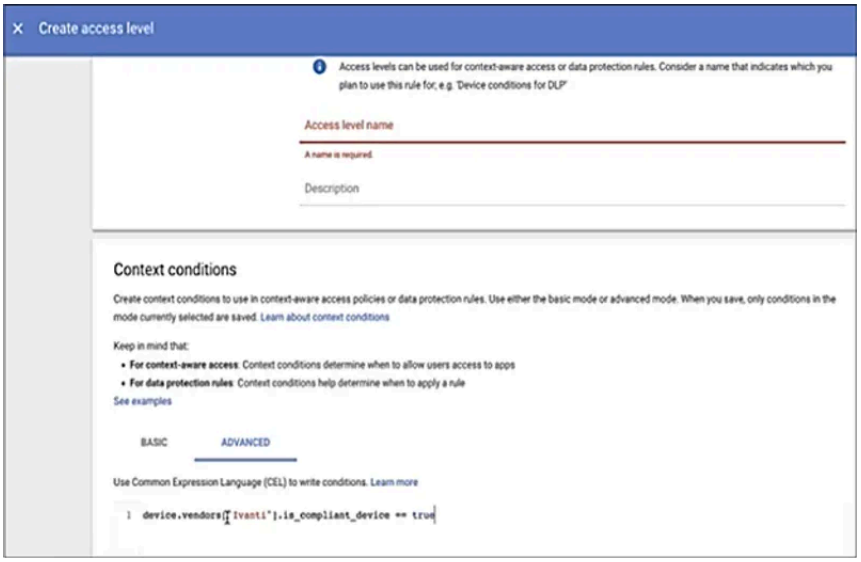

3. **보안 및 MDM 파트너** > **관리**를 클릭합니다.



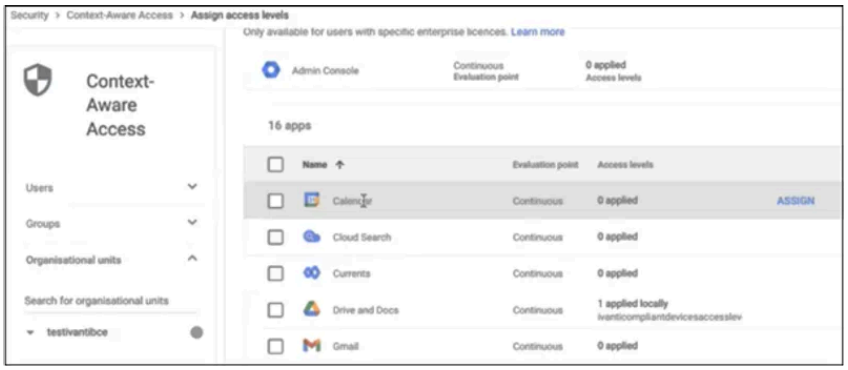

4. **파트너 연결 관리** 창에서 **Ivanti**를 선택합니다.
5. **연결 열기**를 클릭합니다.
   MDM용 Ivanti Neurons 로그인 페이지로 리디렉션되면 테넌트 관리자 자격 증명을 입력합니다. 테넌트에 로그인하면 **Google BeyondCorp**가 활성화되어 Google 계정에 자동으로 연결되는 것을 알 수 있습니다.
6. Google 관리 콘솔에서 **보안** > **컨텍스트 인식 액세스** > **액세스 수준**으로 이동합니다.



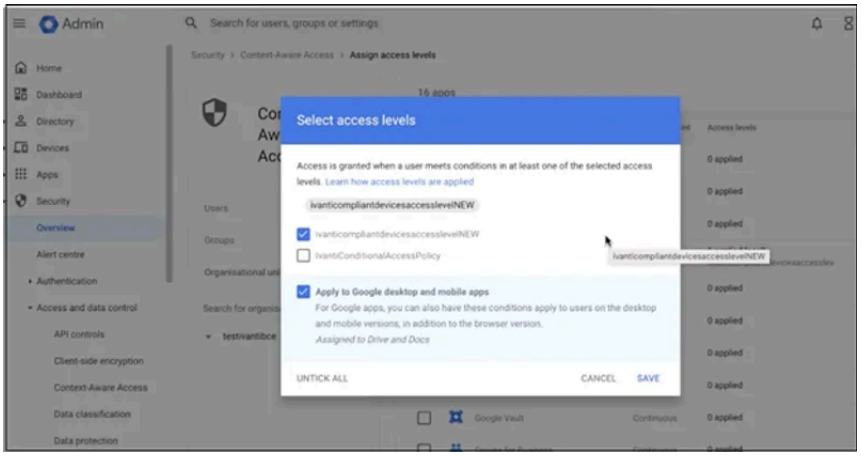

7. **액세스 수준 생성**을 클릭합니다.
   액세스 수준 생성 창의 컨텍스트 조건 섹션에서 **고급**을 클릭하고 필요한 정보를 제공합니다.




8. **보안** > **컨텍스트 인식 액세스** > **액세스 수준**으로 이동하여 정책을 할당하려는 애플리케이션을 선택합니다.




9. **할당**을 클릭합니다.
10. **액세스 수준 선택** 창에서 할당하려는 정책을 선택하고 **저장**을 클릭합니다.




위 설정이 완료되면 **Google BeyondCorp**를 사용하여 파트너 기기 규정 준수 구성을 생성할 수 있습니다.

**절차 (**MDM용 Ivanti Neurons**)**:

1. **구성** > **구성 추가**로 이동합니다.

2. **파트너 기기 규정 준수** 구성을 선택합니다.
3. 화면에 파트너 기기 규정 준수 구성 생성 페이지가 표시됩니다.
   구성 이름을 입력합니다.
4. 파트너 선택 목록에서 **Google BeyondCorp**를 선택합니다.
5. 구성 설정 섹션이 화면에 표시됩니다. iOS 및 Android 기기에 대한 규정 준수 상태 보고 옵션이 ON으로 설정되어 있는지 확인합니다.
   **다음**을 클릭하세요.
6. **이 구성 활성화**를 선택합니다.
7. 배포 옵션으로 **사용자 지정**을 선택합니다.
8. **맞춤형 배포** 옵션 아래의 **사용자/사용자 그룹**을 선택합니다.
9. **이 구성을 배포하려면 아래를 선택하세요** 섹션의 목록에서 사용자/사용자 그룹을 선택합니다.
10. **완료**를 클릭하세요.

> Google BeyondCorp 서버는 앱에서 관리되는 구성 P-List를 통해 각 기기를 고유하게 식별할 수 있습니다.
> 

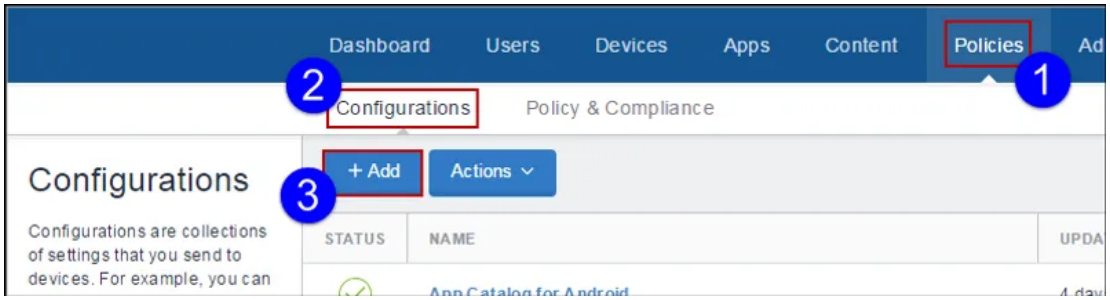
# 10.10.8.20. 잠금 화면 메시지 구성

로그인 및 잠금 화면에 메시지 및 자산 태그 정보를 표시합니다. 이것은 iOS 9.3 또는 지원되는 최신 버전을 사용하는 감독 기기를 위한 옵션입니다.

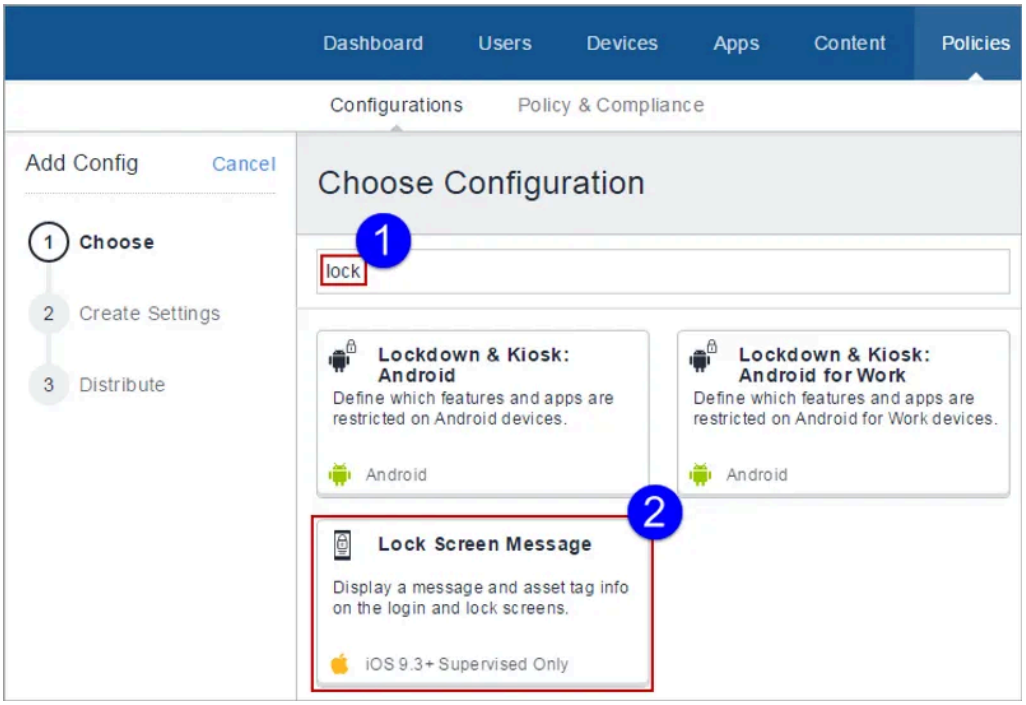
## 잠금 화면 메시지 구성 생성

**절차**

1. **구성**을 선택합니다.
2. **+ 추가**를 클릭합니다.




검색 필드에 **알림**을 입력한 다음 **앱 알림** 구성을 클릭합니다.




잠금 화면 메시지 구성 상세 정보 페이지가 나타납니다.
이 페이지에서 설정을 구성합니다. 값에 대한 안내는 잠금 화면 메시지 구성 설정 섹션의 표를 참조하십시오.

5. **다음**을 클릭해 배포 설정을 구성한 다음 **완료**를 클릭합니다.

## 잠금 화면 메시지 구성 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 잠금 화면 각주 | 이 텍스트가 로그인 창과 잠금 화면에 나타납니다. |
| 자산 태그 정보 | 이 텍스트가 로그인 창과 잠금 화면의 하단에 나타납니다. |

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.8.21. 로그인 창 구성 - macOS

**절차**

1. MDM용 Ivanti Neurons에 로그인합니다.
2. **구성** > **구성 추가**로 이동합니다.
3. **로그인 창**을 클릭(또는 선택)합니다.
4. **이름** 필드에 로그인 창 구성의 이름을 입력합니다.
5. 세부 사항을 추가하려면 **+ 설명 추가**를 클릭합니다.
6. **구성 설정** 섹션에서 다음의 필드를 입력합니다:
   - **관리자 호스트 정보**: 호스트 이름이나 IP 주소 또는 SystemVersion을 입력합니다.
   - **허용 목록**: 시스템에서 사용자가 로그인할 수 있도록 허용하는 사용자 GUID 또는 그룹 GUID 목록입니다. 별표('*') 문자열은 모든 사용자 또는 그룹을 지정합니다.
   - **자동 로그인 비밀번호**: 자동 로그인을 위한 비밀번호를 입력합니다.
   - **거부 목록**: 시스템에서 로그인을 허용하지 않는 사용자의 사용자 GUID 또는 그룹 GUID 목록입니다. 이 목록은 'AllowList' 키의 목록보다 우선순위가 높습니다.
   - **로그인 창 텍스트**: 로그인 창 텍스트를 입력합니다.
   - 추가 옵션의 확인란을 선택하세요. 예:
     - **콘솔 액세스 비활성화**
     - **FDE 자동 로그인 비활성화(FileVault 디스크 암호화)**
     - **즉시 화면 잠금 기능 비활성화**
     - **사용자 목록 표시하는 동안 관리자인 사용자 숨기기**
     - **네트워크 및 시스템 사용자만 표시**
     - **모바일 계정 숨김**
     - **네트워크 사용자 표시**
     - **로그아웃 메뉴 항목 비활성화**
     - **사용자 로그인 시 전원 끄기 비활성화**
     - **사용자 로그인 시 재시작 메뉴 항목을 비활성ㅎ와**
     - **다시 시작 항목 비활성화**
     - **이름 및 비밀번호 대화 상자 표시**
     - **다른 사용자 표시 - 관리형**
     - **입력 메뉴 표시**
     - **종료 버튼 비활성화**
     - **절전 버튼 비활성화**
     - **종료 메뉴 항목 비활성화**
7. **완료**를 클릭하세요.

# 10.10.8.22. macOS 시스템 확장 구성

시스템 확장 구성을 통해 커널 수준 액세스 없이 드라이버 확장, 네트워크 확장, 엔드포인트 보안 확장 등의 확장 유형을 설치할 수 있습니다.

**절차**

**적용 대상**: macOS 10.15+

1. **구성** > **+추가**로 이동합니다.
2. 검색 필드에 **확장자**를 입력한 다음, **시스템 확장** 구성을 클릭합니다.
3. 구성의 **이름** 및 **설명**을 입력합니다.
4. **허용된 시스템 확장**에서 **허용된 팀 식별자** 및 **허용된 시스템 확장**을 **+추가**합니다.
5. **허용된 시스템 확장 유형**에서 **허용된 팀 식별자** 및 **허용된 시스템 유형**을 **+추가**합니다.
6. **사용자 재정의 허용** 옵션을 체크 표시합니다.
7. **다음**을 클릭하세요.
8. **이 구성 활성화** 옵션을 선택합니다.
9. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
10. **완료**를 클릭하세요.

> macOS 12에서 RemovableSystemExtensions를 사용하면 애플리케이션 제거 중에 관리자 승인 없이 애플리케이션에서 시스템 확장을 비활성화할 수 있습니다.

# 10.10.8.23. MAM 전용

MDM용 Ivanti Neurons 을(를) 통해 iOS 및 Android 기기를 MAM-only로 지정하고 해당 기기에 모바일 앱 관리(MAM)를 제공할 수 있습니다. MAM-only를 배포하면 기기를 관리할 필요 없이 앱을 배포하고 관리할 수 있습니다.

## MAM 전용 솔루션 - Ivanti AppStation 대안

Ivanti는 Ivanti AppStation의 대체 솔루션으로써 Ivanti Go Client를 사용하는 유연한 최신 MAM(모바일 애플리케이션 관리) 솔루션을 제공하며, iOS와 Android 플랫폼에서 모두 사용 가능합니다.

새 MAM 전용 솔루션은 통합 앱 카탈로그와 MDM용 Ivanti Neurons 웹 클립 기능을 도입하여, 이전에 앱 스테이션이 담당했던 핵심 사용 사례를 충족하며 사용자와 관리자 모두에게 보다 간편하고 안전하며 통합된 앱 관리 환경을 제공합니다.

### 핵심 기능

- **앱 내 앱 카탈로그**: 승인된 관리형 앱을 Go Client 내에 직접 호스트 및 배포합니다.
- **앱 구성 및 업데이트**: MAM 정책을 통해 강제 적용되는 애플리케이션 수준의 구성 및 버전 업데이트를 지원합니다.
- MDM용 Ivanti Neurons **요구 사항**: MDM용 Ivanti Neurons 등록이 가능하지 않은 BYOD 및 계약자 시나리오에 이상적입니다.

### 접근성 향상을 위한 웹 클립 사용

- **앱 카탈로그에 직접 액세스**: MDM용 Ivanti Neurons을(를) 통해 웹 클립을 배포하여 앱 카탈로그 또는 특정 웹 기반 엔터프라이즈 앱 바로 가기를 제공합니다.
- **사용자 정의 앱 바로 가기**: 사용자가 홈 화면에서 자주 사용하는 리소스를 빠르게 실행할 수 있습니다.

### 관리자 및 사용자 환경 향상

- **통합 인터페이스**: 앱 카탈로그, 웹 액세스, 규정 준수 메시징을 하나의 환경으로 결합합니다.
- **관리 간소화**: 별도의 솔루션(예: 앱 스테이션)을 유지할 필요가 없어 복잡성과 구성 드리프트의 위험이 줄어듭니다.

### 유연성 및 사용자 지정

- **카탈로그 뷰 사용자 지정**: 사용자 역할, 지리적 위치, 조직 단위를 기반으로 앱 카탈로그 콘텐츠를 사용자 지정합니다.
- **기존 인프라 사용**: 기존 MDM용 Ivanti Neurons / MAM 투자를 활용합니다(별도의 인프라가 필요하지 않음).

### 이중 역할 사용자 지원

Ivanti MAM 전용 솔루션은 이중 역할을 지닌 사용자를 포함하여 최신 작업 시나리오를 지원하도록 설계되었습니다.

- **정규 직원 - 조직 A**: MDM용 Ivanti Neurons(으)로 배포된 웹 클립(예: Apps@Work)을 통해 엔터프라이즈 앱에 액세스할 수 있습니다.
- **계약자 - 조직 B**: MDM용 Ivanti Neurons에 기기를 등록할 필요 없이 MAM 전용 모드로 Ivanti Go Client를 사용하여 관리형 앱에 안전하게 액세스할 수 있습니다.

이를 통해 프로필 충돌 또는 기기 관리 중첩 문제 없이 역할에 기반하여 필요한 앱에 원활하게 액세스할 수 있습니다.

### 마이그레이션 안내

Ivanti는 앱 스테이션 고객에게 Go Client 기반의 MAM 전용 솔루션으로 전환할 것을 계획하고 실행하도록 강력히 권장합니다. 단계별 마이그레이션 지원은 다음 리소스를 참조하십시오.

- Ivanti MAM 전용 솔루션
- **Go Client에서 앱 카탈로그 구성**
- **웹 클립 구성 만들기**

질문이 있거나 마이그레이션 지원이 필요하다면 **Ivanti 지원** 또는 고객 성공 매니저에게 문의하십시오.

# 10.10.8.24. 관리되는 Google Play 구성

관리자는 Google Play 스토어가 Android Enterprise 기기에서 앱을 업데이트할 때 사용하는 자동 업데이트 설정을 구성할 수 있습니다.

자동 업데이트 설정 구성 방법:

1. **구성** > **+추가**로 이동합니다.
2. **관리되는 Google Play** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서, Google Play에서 앱 업데이트 옵션을 선택합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| **사용자 정의됨** | 기기 사용자는 자동 업데이트 앱 유지보수 창 설정을 설정하여 앱을 업데이트해야 할 때를 정의할 수 있습니다.<br>1. **시작 시간** 필드에서 앱 업데이트를 수행할 시간을 선택합니다.<br>2. **기간** 필드에서 업데이트를 수행해야 하는 최대 기간(단위: 시간)을 선택합니다. 최소 및 최대 범위는 1 ~ 24시간입니다. 앱은 시작 시간에서 선택한 기간 사이의 어느 때든 업데이트할 수 있습니다. 예를 들어, '시작 시간'이 오후 6시로 설정되고 '기간'이 12시간으로 설정되어 있는 경우, 앱은 오후 6시에서 오전 6시 사이의 어느 때든 업데이트될 수 있습니다. |
| **없음** | Google Play Store는 절대로 기기에서 자동으로 앱을 업데이트하지 않습니다. |
| **Wi-Fi 전용** | Google Play Store는 휴대폰 연결이 아닌 Wi-Fi를 사용해서만 기기에서 자동으로 앱을 업데이트합니다. |
| **항상** | Google Play Store는 Wi-Fi 또는 휴대폰 연결을 사용하여 기기에서 자동으로 앱을 업데이트합니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.

- 모든 기기
- 배포 안 함(기본값)
- 사용자 지정

8. **완료**를 클릭하세요.

# 10.10.8.25. 마이그레이션 지원 설정

**마이그레이션 지원 설정**을 사용하여 감독 모드 기기에서 마이그레이션 지원 설정을 구성합니다. 이 구성을 통해 관리자는 기기 설정 또는 마이그레이션 중 사용자가 데이터, 앱 및 설정을 전송하는 방식을 관리하는 일관된 정책 기반 제어를 적용할 수 있습니다.

**적용 대상**:

- macOS 26.4+ 감독 모드부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **마이그레이션 지원 설정** 구성을 검색하여 선택합니다.
3. 아래 표에 따라 **마이그레이션 지원 설정**을 구성합니다:

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 관리형 마이그레이션 수행 여부 | 확인란을 선택하여 기기 마이그레이션을 활성화하고 관리합니다.<br>**기기로 푸시** 버튼을 전환하여 기기 마이그레이션을 활성화합니다. |
| 제외된 계정 | 마이그레이션에서 제외할 계정 이름을 입력합니다.<br>**기기로 푸시** 버튼을 전환하여 계정 제외를 활성화합니다. |
| 제외 경로 | 마이그레이션에서 제외할 경로 이름을 입력합니다.<br>**기기로 푸시** 버튼을 전환하여 경로 제외를 활성화합니다. |
| 필수 경로 | 마이그레이션에 포함할 경로 이름을 입력합니다.<br>**기기로 푸시** 버튼을 전환하여 경로 포함을 활성화합니다. |
| 보안 개인정보 보호 설정의 마이그레이션 여부 | 확인란을 선택하여 기기에서 보안 개인정보 보호 설정의 마이그레이션을 활성화합니다.<br>**기기로 푸시** 버튼을 전환하여 보안 개인정보 보호 설정의 마이그레이션을 활성화합니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **마이그레이션 지원 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.8.26. 알림 구성

알림 구성을 사용하여 관리자는 iOS 기기에 대해 무음 및 표시 알림을 예약할 수 있습니다. 알림 구성은 복제, 내보내기 또는 삭제할 수도 있습니다.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **알림** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음과 같은 **알림 일정** 옵션 중 하나를 선택하거나 두 개 모두 선택합니다:
    - 무음 알림 일정 - 무음 알림은 MDM용 Ivanti Neurons에서 시작된 백그라운드 기기 관리 작업을 지원하는 데 사용됩니다. 사용자 상호작용 없이 규정 준수 확인, 정책 업데이트, 앱 업데이트와 같은 자동 작업을 수행할 수 있도록 합니다. MDM용 Ivanti Neurons 은(는) 구성된 수준에 따라 기기로 무음 알림을 전송합니다.
    - 시각 알림 일정 - 시각 알림은 기기 규정 준수, 보안 또는 기능 유지를 위해 사용자 인식 또는 조치가 필요한 경우 사용됩니다. 시각 알림은 지정된 간격 이후에만 트리거되며, 해당 기간 동안 여러 작업이나 이벤트가 발생하더라도 동일하게 적용됩니다. 시각 알림은 시각 알림 간격 동안 무음 알림이 전송되지 않은 경우에만 기기에 표시됩니다.
6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
8. **완료**를 클릭하세요.

MTD 기기용 시각 알림 내용 - 기기가 위협에 노출될 수 있습니다. Ivanti Go 애플리케이션을 실행하고 위협 방어 상태를 확인합니다.

MTD 미적용 기기의 시각 알림 내용 - 향상된 보안 기능을 제공받고 최신 보호 조치를 보장할 수 있도록, 보다 안전한 사용자 경험을 위해 기기에서 앱을 실행합니다.

# 10.10.8.27. 프린터 설정

MDM용 Ivanti Neurons에서는 프린터 프로필을 생성하여 이를 기기에 추가할 수 있습니다. 이 기능을 사용하려면 Bridge가 필요합니다. 자세한 내용은 **Bridge**를 참조하십시오.

> 프린터 프로필을 기기에 전송할 때는 프린터가 활성 상태여야 합니다. 그렇지 않으면 기기가 발견할 수 없습니다.

**Windows 기기의 프린터 설정 구성을 설정하려면:**

1. **구성 > +추가**로 이동합니다.
2. **프린터 설정** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. **Windows** 옵션을 선택합니다.
5. **구성 설정** 섹션에서 다음 설정을 구성합니다.

| 설정 항목 | 설정하기 |
|---|---|
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **Windows 프린터 설정**<br><br>**공유 프린터** | **공유 프린터** 옵션이 선택될 경우, 프린터가 다른 기기와 공유됩니다. 다음 필드를 구성하십시오.<br>**이름**: 프린터 구성 이름을 입력하십시오.<br>**설명**: 프린터 설명을 입력하십시오.<br>**인쇄 서버**: 인쇄 서버의 IP 주소를 입력하십시오.<br>**공유 프린터 이름**: 프린터 이름을 입력하십시오. |
| **네트워크 연결 프린터** | **네트워크 연결** 옵션이 선택된 경우 연결된 네트워크 내부의 기기만 프린터에 액세스할 수 있습니다. 다음 필드를 구성하십시오.<br>**이름**: 프린터 구성 이름을 입력하십시오.<br>**설명**: 프린터 설명을 입력하십시오.<br>**인쇄 이름**: 네트워크의 프린터 이름을 입력하십시오.<br>**프린터 호스트 주소**: 프린터의 호스트 IP 주소를 입력하십시오.<br>**프린터 포트 번호**: 네트워크 프린터의 포트 번호를 선택하십시오.<br>**프린터 드라이버 이름**: 프린터 드라이버의 이름을 입력하십시오.<br>**프린터 드라이버 URL**: 프린터 드라이버의 URL을 입력하십시오.<br>프린터 드라이버의 경우, 필수 파일이 포함된 ZIP 아카이브를 업로드해야 합니다. ZIP 보관에는 다음 파일이 포함되어야 합니다:<br>• .inf 파일(드라이버 정보)<br>• .cat 파일(카탈로그/서명)<br>• INF에서 참조되는 추가 드라이버 2진 파일(.dll, .sys 등) |

6. **다음**을 클릭하세요.

7. 다음 배포 옵션 중 하나를 선택합니다.
- 모든 기기
- 배포 안 함(기본값)
- 사용자 지정
8. **완료**를 클릭하세요.

**macOS 기기의 프린터 설정 구성을 설정하려면:**

1. **구성 > +추가**로 이동합니다.
2. **프린터 설정** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. **macOS** 옵션을 선택합니다.
5. **프린터 구성 생성** 섹션에서 다음 설정을 구성합니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **구성 설정** | 다음 필드를 업데이트하여 macOS 기기용 프린터를 설정합니다.<br>• 로컬 프린터 허용<br>• 기본 프린터 표시 이름<br>• 바닥글 글꼴 이름<br>• 바닥글 글꼴 크기<br>• 사용자 프린터 목록<br>• + 프린터 추가 |

6. **다음**을 클릭합니다.
7. 다음 배포 옵션 중 하나를 선택합니다.
- 모든 기기
- 배포 안 함(기본값)
- 사용자 지정
8. **완료**를 클릭하세요.

# 10.10.8.28. 블로트웨어 제거 구성

Bloatware 제거 구성을 사용하면 강제로 제거해야 하는 기기에 설치된 애플리케이션 목록을 선택할 수 있습니다. 이 구성을 사용하려면 Bridge를 설정해야 합니다. 자세한 내용은 Bridge를 참조하십시오.

앱을 실행하거나 제거하는 방법:

1. **구성** 탭에서 **+추가**를 클릭합니다.
2. **블로트웨어 제거** 구성을 선택합니다. **Bloatware 제거 구성** 페이지가 표시됩니다.
3. **이름** 필드에 적절한 구성 이름을 입력합니다.
4. **+설명 추가** 링크를 클릭하여 구성에 대한 설명을 추가합니다. 이 필드는 선택 사항입니다.
5. **구성 설정** 섹션에서 제거하거나 삭제할 앱을 선택합니다. 또는 데스크톱 앱 목록에 표시되는 앱 이름을 사용하여 검색 필드에서 앱을 검색할 수도 있습니다.

> **블로트웨어 제거** 구성을 생성하기 전에 **앱 > 데스크톱 앱 > 앱 가져오기**로 이동하여 앱을 가져와야 합니다.그러지 않을 경우 **블로트웨어 제거** 구성을 생성할 때 검색하거나 선택할 수 있는 애플리케이션이 없을 것입니다.

파일 유형 .appx, .appxbundles, .xap 및 .msi는 제거할 수 있지만 파일 유형은 .exe는 제거할 수 없습니다.

6. 고급 옵션에서 다음 옵션을 구성합니다.

| 옵션 | 설명 |
| --- | --- |
| **다음 간격마다 이 구성 실행:** | 구성을 실행해야 하는 간격(분 단위)을 설정합니다. |
| **로그온 시 실행** | 로그온할 때 구성을 실행하려면 이 체크박스를 선택합니다. |
| **제거 후 강제 재시작 건너뛰기** | 앱을 제거한 후에 강제 재시작을 방지하려면 이 체크박스를 선택합니다. |

# 10.10.8.29. Safari 확장 및 설정 구성

## Safari 확장 프로그램

MDM용 Ivanti Neurons 을 사용하면 감독 대상인 iOS 및 macOS 기기에서 Safari 확장을 관리할 수 있습니다. 관리자는 Safari 확장을 효과적으로 관리하여 표준 및 비공개 브라우징을 수행할 수 있습니다.

**적용 대상**:

- 감독 대상인 iOS 18.0부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.
- 감독 대상인 macOS 15.0부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **Safari 확장 설정** 구성을 검색하고 선택합니다.
3. 다음 표에 따라 **Safari 확장 설정**을 구성합니다.

| 설정 항목 | 설명 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 확장 ID | 구성된 확장 식별자를 입력합니다. 예를 들어, "*식별자(TeamIdentifier)*"와 같이 입력합니다.<br>모든 확장에 "*"를 입력합니다.<br>이 문자열을 생성하려면 *-dv <path_to_appex>* 코드 기호를 사용합니다. 브라우저 확장은 앱 번들 내의 플러그인 폴더에 있습니다. 예상되는 형식은 "*식별자(TeamIdentifier)*"입니다. macOS에서 사용할 수 없는 확장의 경우 앱 개발자가 이 정보를 제공해야 합니다. |
| 확장 상태 | 다음 옵션 중 하나를 선택합니다.<br>• **허용됨**: 사용자는 확장을 켜거나 끌 수 있습니다.<br>• **항상 켜짐**: 사용자에 대해 확장이 항상 "켜짐" 상태입니다.<br>• **항상 꺼짐**: 사용자에 대해 확장이 항상 "꺼짐" 상태입니다. |
| 비공개 브라우징 상태 | 다음 옵션 중 하나를 선택합니다.<br>• **허용됨**: 사용자는 비공개 브라우징에서 확장을 켜거나 끌 수 있습니다.<br>• **항상 켜짐**: 이 확장은 비공개 브라우징 중에도 사용자에게 항상 "켜짐" 상태로 유지됩니다.<br>• **항상 꺼짐**: 확장을 현재 사용할 수 없습니다. |
| 허용된 도메인 | Safari 확장에 액세스 권한을 부여하려면 도메인 또는 하위 도메인 값을 입력합니다.<br>여러 개의 도메인이나 하위 도메인 값을 입력할 수 있습니다.<br>확장 ID 필드에 "*"를 입력하면 허용된 도메인 설정이 해당 장치에 적용되지 않습니다. |
| 거부된 도메인 | Safari 확장 액세스를 제한하려면 도메인이나 하위 도메인 값을 입력합니다.<br>여러 개의 도메인이나 하위 도메인 값을 입력할 수 있습니다.<br>확장 ID 필드에 "*"를 입력하면 거부된 도메인 설정이 장치에 적용되지 않습니다. |

4. 여러 개의 **확장**을 추가하려면 **+추가**를 클릭합니다.

5. **다음**을 클릭해 배포 설정을 구성합니다.
6. 배포 옵션 중 하나를 선택하여 **Safari 확장 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
7. **완료**를 클릭하세요.

## Safari 설정

MDM용 Ivanti Neurons 을(를) 사용하면 감독 모드인 iOS 및 macOS 기기에서 Safari 설정을 관리할 수 있습니다. 관리자는 Safari 확장을 효과적으로 관리하여 표준 및 비공개 브라우징을 수행할 수 있습니다.

**적용 대상**:

- iOS 26.0+, iPad 26.0+, macOS 26.0+, visionOS 26.0+ 베타 버전부터 MDM용 Ivanti Neurons에서 지원하는 최신 출시 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **Safari 확장 및 설정** 구성을 검색하고 선택합니다.
3. **Safari 설정**을 클릭합니다.
4. 다음 표에 따라 **Safari 설정**을 구성합니다.

| 설정 항목 | 설명 |
|---|---|
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 구성 설정 | 시작 페이지 유형을 설정하려면 다음 옵션 중 하나를 선택합니다:<br>• **시작**: 기본 시작 페이지를 사용합니다. Safari가 기존 홈페이지를 비활성화합니다.<br>• **홈페이지**: 지정된 HomePage URL을 사용합니다. Safari는 이를 홈페이지로 설정합니다.<br>• **확장**: 식별자가 ExtensionIdentifier인 Safari 확장 기능에서 지정한 페이지를 사용합니다. Safari가 기존 홈페이지를 비활성화합니다. |

5. **다음**을 클릭해 배포 설정을 구성합니다.
6. 배포 옵션 중 하나를 선택하여 **Safari 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
7. **완료**를 클릭하세요.

## Safari 개인정보 보호 설정

**Safari 개인정보 보호 설정**을 통해 관리자는 선언적 기기 관리(DDM)를 사용하여 Safari의 특정 웹 사이트에 대한 기본 카메라 및 마이크 권한을 정의할 수 있습니다. 이 기능을 통해 조직은 웹 사이트 개인정보 보호 권한을 중앙에서 관리하고 관리되는 Apple 기기에서 보다 일관된 브라우징 환경을 제공할 수 있습니다.

**적용 대상**:

- iOS 27.0+ 및 macOS 27.0+ 버전부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지.

**절차**

1. **구성** > **+추가**로 이동합니다.

2. **Safari 확장 및 설정** 구성을 검색하고 선택합니다.
3. **Safari 개인정보 보호 설정**을 클릭합니다.
4. 다음 표에 따라 **Safari 개인정보 보호 설정**을 구성합니다.

| 설정 항목 | 설명 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 구성 설정 | • **URL 추가**: 설정을 적용할 URL을 입력합니다.<br>• **+기본값 추가**: 이 설정에 적용할 기본값을 지정합니다.<br>  ◦ 카메라 - 허용/거부<br>  ◦ 마이크 - 허용/거부<br>  ◦ 조직 사유(필수 입력) |

5. **다음**을 클릭해 배포 설정을 구성합니다.
6. 배포 옵션 중 하나를 선택하여 **Safari 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
7. **완료**를 클릭하세요.

# 10.10.8.30. Samsung Phone 제한 구성

구성

Samsung Phone 제한 구성에서 Samsung 기기에서 통화 제한 및 예외를 설정할 수 있습니다. 이러한 제한은 사용자가 생성 또는 수신할 수 있는 전화번호를 한정합니다.

**적용 대상:** Knox SDK 2.0+가 탑재된 모든 Samsung 기기

Samsung Phone 제한 사항 구성 방법

1. **구성** 탭에서 **+추가**를 클릭합니다.
2. **Samsung 휴대폰 제한 사항** 구성을 선택합니다. **Samsung Phone 제한 사항 구성** 페이지가 표시됩니다.
3. **이름** 필드에 적절한 구성 이름을 입력합니다.
4. **+설명 추가** 링크를 클릭하여 구성에 대한 설명을 추가합니다. 이 필드는 선택 사항입니다.
5. **구성 설정** 섹션에서 다음 옵션을 구성합니다.
   **옵션**
   **설명**
   **수신 전화**
   **차단된 번호**
   추가 아이콘을 클릭하여 번호와 Java 정규 표현식을 추가하고 수신 통화 제한을 정의합니다.
   **허용 목록에 있는 번호**
   추가 아이콘을 클릭하여 번호와 Java 정규 표현식을 추가하고 전화 수신 시 더 큰 차단된 번호 집합에서 허용된 번호들을 정의합니다. 차단된 번호가 없으면 해당 옵션은 아무런 영향이 없습니다.
   **발신 전화**
   **차단된 번호**
   추가 아이콘을 클릭하여 번호와 Java 정규 표현식을 추가하고 수신 통화 제한을 정의합니다.
   **허용 목록에 있는 번호**
   추가 아이콘을 클릭하여 번호와 Java 정규 표현식을 추가하고 전화 발신 시 더 큰 차단된 번호 집합에서 허용된 번호들을 정의합니다. 차단된 번호가 없으면 해당 옵션은 아무런 영향이 없습니다.
6. **완료**를 클릭하여 선택한 기기에 설정을 푸시합니다.

> 기기를 폐기하면 모든 통화 제한이 기기에서 삭제됩니다.

자세한 내용은 **구성을 생성하는 방법**을 참조하십시오.

# 10.10.8.31. 기본 브라우저 구성 - iOS 및 visionOS

iOS 및 visionOS 기기의 기본 애플리케이션 설정을 변경하기 위한 구성입니다.

**필수 조건**

- iOS(18.2+) 및 visionOS 2.2 버전에만 적용됩니다.
- 이 앱은 iOS 기기의 **설정** - **앱** - **기본 앱**에서 설정할 수 있습니다.

**절차**

1. **기기** 페이지에서 iOS(18.2 이상) 기기 또는 visionOS 2.2 기기를 등록합니다.
2. **구성** > **구성 추가** > **기본 애플리케이션 설정**으로 이동하여 iOS 기기에서 기본 브라우저를 설정합니다.
3. **구성** > **설정 생성** > **기본 애플리케이션 설정 구성 생성**을 클릭합니다.
4. 구성 세부 정보 섹션에서 **이름** 및 **설명**을 입력합니다.
5. 구성 설정 > 앱 추가 > 조회로 추가에서 원하는 브라우저를 검색합니다. 사용자 목록이 표시됩니다.
6. 목록에서 원하는 브라우저를 선택합니다.
7. **기본 애플리케이션 설정 구성 생성** 페이지에서 **사용자 지정**을 클릭하여 특정 장치 또는 장치 그룹이나 사용자 또는 사용자 그룹에 구성을 배포합니다.
8. **이 사용자 지정 배포 옵션 중 하나 선택**에서 원하는 옵션을 선택하여 이 구성을 사용자/사용자 그룹 또는 기기/기기 그룹에 배포하도록 지정합니다.
9. **모두 사용 가능**에서 원하는 옵션을 선택하여 이 구성을 배포합니다.
10. **완료**를 클릭하세요.

# 10.10.8.32. 화면 공유 호스트 설정 구성

**화면 공유 호스트 설정** 구성을 통해 관리자는MDM용 Ivanti Neurons을(를) 사용하여 관리형 macOS 기기 전반에서 macOS 화면 공유 기능을 안전하게 제어할 수 있습니다. 이 기능은 승인된 사용자, 인증 방법 및 서비스 제한 사항을 지정할 수 있도록 하여 규정을 준수하고 안전한 원격 액세스를 보장합니다.

**적용 대상:** iOS 14.0부터 MDM용 Ivanti Neurons에서 지원되는 가장 최신 릴리스 버전까지.

**시작하기 전에**: **화면 공유 호스트 설정** 구성을 원활하게 통합하려면, 사용자는 자신의 기기에서 '**원격 관리**'를 활성화해야 합니다. 기기에서 **설정** > **원격 관리** > **원격 관리 활성화**로 이동합니다.

**절차**

1. **구성** > **+추가**로 이동합니다.
2. **화면 공유 호스트 설정** 구성을 검색하여 선택합니다.
3. 아래 표에 따라 **화면 공유 호스트 설정**을 구성합니다:

| 설정 항목 | 설명 |
|---|---|
| **Windows** | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| **설명** | 현재 설정에 대한 간략한 설명을 입력합니다. |
| **포트 기준값** | 호스트에 연결하기 위한 초기 UDP 포트 번호를 입력합니다. 화면 공유에는 여러 연결이 필요하므로, 추가 연결 시마다 시스템은 이 값을 1씩 증분합니다.<br>이는 시스템이 호스트와의 초기 연결을 설정할 때 사용하는 포트 번호에는 영향을 주지 않으며, 초기 연결은 항상 TCP 포트 5900을 사용합니다.<br>**최소 포트 기준값**: 1024<br>**최대 포트 기준값**: 65535 |
| **최대 가상 디스플레이 수** | 최대 두 개의 가상 디스플레이를 사용할 수 있습니다. |
| **호스트에서 파일 복사 방지** | 확인란을 선택하여 사용자가 화면 공유 호스트에서 파일을 복사하지 못하도록 합니다. |
| **호스트로 파일 복사 방지** | 확인란을 선택하여 사용자가 화면 공유 호스트로 파일을 복사하지 못하도록 합니다. |
| **고성능 연결 방지** | 확인란을 선택하여 사용자가 호스트에 고성능 연결을 설정하지 못하도록 합니다. |

4. **다음**을 클릭해 배포 설정을 구성합니다.
5. 배포 옵션 중 하나를 선택하여 **화면 공유 호스트 설정** 구성을 설정합니다. 구성 배포 옵션에 대한 자세한 내용은 구성 작업을 참조하십시오.
6. **완료**를 클릭하세요.

# 10.10.8.33. Single App 모드 설정

구성

## 라이센스: Silver

단일 앱 모드는 iOS 기기가 특정 앱을 사용하도록 제한합니다. 예를 들어 사용자의 조직이 개발한 맞춤형 앱만 사용하도록 기기를 설정할 수 있습니다.

## Single App 모드 설정

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 설정을 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 설정에 대한 간략한 설명을 입력합니다. |
| 앱 선택 | 앱 선택을 위해 사용할 방법을 선택합니다.<br>• **앱 카탈로그 및 시스템 앱:** MDM용 Ivanti Neurons 앱 카탈로그 및 시스템 앱(Apple 기기에 기본값으로 사전 설치)을 검색하도록 선택합니다.<br>• 앱 이름을 입력하고 앱 목록에 표시되면 선택합니다.<br>• **번들 ID 입력:** 선택할 시스템 앱의 고유 식별자를 입력하도록 선택합니다. **App Catalog 및 시스템 앱에서** 옵션으로 시스템 앱을 찾을 수 없을 경우 이 옵션을 사용합니다. |
| 터치 비활성화 | 터치 화면 기능을 해제할 수 있습니다. |
| 기기 회전 비활성화 | 기기 회전 감지 기능을 해제할 수 있습니다. |
| 볼륨 버튼 비활성화 | 기기의 음량 버튼 기능을 해제할 수 있습니다. |
| 링거 스위치 비활성화 | 기기의 링거 스위치 기능을 해제할 수 있습니다. |
| 절전 모드 해제 버튼 비활성화 | 기기의 절전 모드 설정/해제 버튼(기기 가장자리 우측 상단) 기능을 해제할 수 있습니다. |
| 자동 잠금 비활성화 | 일정 시간 입력이 없을 때 기기가 절전 모드로 진입하는 것을 차단할 수 있습니다. |
| 보이스 오버 활성화 | 보이스오버 화면 낭독 기능을 설정할 수 있습니다(접근성 기능). |
| 확대/축소 활성화 | 확대/축소 기능을 설정할 수 있습니다(접근성 기능). |
| 색상 반전 활성화 | 색상 반전 조절 기능을 설정할 수 있습니다(접근성 기능). |
| 보조 터치 활성화 | 보조 터치 기능을 설정할 수 있습니다(접근성 기능). |
| 말하기 선택 활성화 | 말하기 선택 기능을 설정할 수 있습니다(접근성 기능). |
| 모노 오디오 활성화 | 스테레오에서 모노 오디오 모드로 전환할 수 있습니다(접근성 기능). |
| 보이스 오버 조정 | 기기 사용자의 보이스 오버 설정 변경이 허용되도록 설정할 수 있습니다. |
| 확대/축소 조정 | 기기 사용자의 확대/축소 설정 변경이 허용되도록 설정할 수 있습니다. |
| 색상 반전 조정 | 기기 사용자의 색상 반전이 허용되도록 설정할 수 있습니다. |
| 보조 터치 조정 | 사용자의 보조 터치 설정 변경이 허용되도록 설정할 수 있습니다. |

자세한 내용은 구성을 생성하는 방법을 참조하십시오.

# 10.10.8.34. 소프트웨어 업데이트 권장 케이던스 구성

관리자는 사용자가 기기를 확인하고 번호가 높은(가장 최신) 릴리스 또는 번호가 낮은(오래된) 릴리스 또는 둘 모두로 업데이트할 수 있게 허용하는 옵션이 있습니다.

적용 대상: iOS 및 iPadOS 14.5~26.0(감독 모드)

**절차**

1. 구성 > +추가로 이동합니다.
2. 검색 필드에서소프트웨어 업데이트 권장을 입력한 다음, 소프트웨어 업데이트 권장 케이던스 구성을 클릭합니다.
3. 구성의 이름 및 설명을 입력합니다.
4. 드롭다운에서 필요한 구성 설정을 선택합니다.
    - 소프트웨어 업데이트 버전 둘 모두 제공
    - 번호가 낮은(오래된) 소프트웨어 업데이트 버전 제공
    - 번호가 높은(최신) 소프트웨어 업데이트 버전만 제공
5. 다음을 클릭하세요.
6. 이 구성 활성화 옵션을 선택합니다.
7. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정.
8. 완료를 클릭하세요.

# 10.10.8.35. 시작 메뉴 및 작업 표시줄

사용자의 시작 메뉴 레이아웃을 정의하여 안전하게 사용 가능한 애플리케이션을 정의하고 필요하지 않은 애플리케이션을 삭제할 수 있습니다. Windows 10과 Windows 11 버전은 시작 메뉴 레이아웃이 다르기 때문에 서로 다른 기능을 지원합니다.

시작 메뉴 및 작업 표시줄 구성을 설정하려면:

1. **구성 > +추가**로 이동합니다.
2. **Windows 시작 메뉴 및 작업 표시줄** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 해당하는 Windows 버전을 선택합니다.
5. **Windows 10 장치**:
   **구성 설정** 섹션에서 다음 설정을 구성합니다.
   **설정**
   **설정하기**
   **Windows**
   현재 설정을 식별할 수 있는 고유한 이름을 입력합니다.
   **설명**
   현재 설정에 대한 간략한 설명을 입력합니다.**표준 기기 선택**
   시작 메뉴와 작업 표시줄에 앱이 프로비저닝된 Windows 10 장치를 선택합니다.
6. **기기에서 시작 메뉴 레이아웃 가져오기**를 클릭하고 다음 옵션을 구성합니다.
7. **설정**
   **설정하기시작 메뉴 및 작업 표시줄 레이아웃**
   앱 목록을 숨기기 위해 다음 옵션 중 어느 것이든 선택합니다.
   - 없음
   - 모든 앱 목록 숨기기
   - 모든 앱 목록을 숨기고 설정 앱에서 "시작 메뉴에 앱 목록 표시" 비활성화
   - 모든 앱 목록을 숨기고 모든 앱 버튼을 제거한 후 설정 앱에서 "시작 메뉴에 앱 목록 표시" 비활성화

**시작 메뉴 레이아웃시작 메뉴 사용자 지정**
**예**를 클릭하여 시작 메뉴와 레이아웃 매개 변수를 사용자 지정합니다.**작업 표시줄작업 표시줄 사용자 지정예**를 클릭하여 작업 표시줄 사용자 지정**기존에 고정된 작업 표시줄 바로 가기를 제거하고 새로운 작업 표시줄을 추가합니다.예**를 클릭하여 기존에 고정된 작업 표시줄 바로 가기를 제거하고 새로운 작업 표시줄을 추가합니다.**앱 유형**앱 유형을 지정합니다.**앱**앱 ID를 지정합니다.**복구**
**복원** 링크를 클릭하여 기존 Golden 장치 작업 표시줄의 작업 표시줄을 복원합니다.
행의 화살표 아이콘을 클릭 후 드래그하여 특정 행의 위치를 변경합니다(위/아래).
삭제 아이콘을 클릭하여 행을 삭제합니다.
**새로 추가** 버튼을 클릭하여 새 행을 추가합니다.

8. **Windows 11 장치**
   **구성 설정** 섹션에서 다음 설정을 구성합니다.
   **설정**
   **설정하기**
   **Windows**
   현재 설정을 식별할 수 있는 고유한 이름을 입력합니다.
   **설명**

현재 설정에 대한 간략한 설명을 입력합니다.**표준 기기 선택**
시작 메뉴의 고정됨 섹션에서 앱이 구성된 Windows 11 장치를 선택합니다.**시작 메뉴 및 작업 표시줄 레이아웃시작 메뉴 및 작업 표시줄 레이아웃**
작업 표시줄에서 검색 옵션을 보려면 다음 옵션 중 하나를 선택하세요.

- **숨기기**
- **검색 아이콘**
- **검색 아이콘 및 레이블**
- **검색창(기본값)**

작업 보기를 숨기려면 **작업 보기 숨기기** 확인란을 선택하세요.**가장 많이 사용한 앱**
시작 메뉴에서 가장 많이 사용한 앱을 구성하려면 다음 옵션 중 하나를 선택하세요.

- **시작에서 가장 많이 사용한 앱 목록 표시를 강제 적용하지 않음.**
- **시작에서 가장 많이 사용한 앱 목록 강제 표시.**
- **시작에서 가장 많이 사용한 앱 목록을 강제로 숨기기.**

**작업 표시줄에 고정 허용** 확인란이 기본적으로 선택되어 있습니다.
모든 권장 섹션을 숨기려면 **추천 섹션 숨기기** 확인란을 선택하세요.
판매자 문제로 인해 **추천 섹션 숨기기** 확인란은 사용자가 로그오프하거나 로그인한 후에도 장치에 눈에 띄는 영향을 미치지 않습니다. 현재는 추천 섹션을 숨길 수 없습니다.**작업 표시줄앱 유형**
앱 유형을 지정하려면 다음 옵션 중 하나를 선택하십시오.

- **앱 사용자 모델 ID**
- **데스크톱 애플리케이션 링크 경로**

**앱**앱 ID 또는 경로를 지정합니다.**복구**
**복원** 링크를 클릭하여 기존 Golden 장치 작업 표시줄의 작업 표시줄을 복원합니다.
행의 화살표 아이콘을 클릭 후 드래그하여 특정 행의 위치를 변경합니다(위/아래).
삭제 아이콘을 클릭하여 행을 삭제합니다.
**새로 추가** 버튼을 클릭하여 새 행을 추가합니다.

9. **장치에서 시작 메뉴 레이아웃 가져오기**를 클릭합니다.
10. Golden 장치의 설정을 가져오면 시작 메뉴의 고정됨 섹션에서 구성된 모든 앱이 표시되므로 관리자가 검토할 수 있습니다.
    **다음**을 클릭하고 해당하는 모든 장치 및 사용자 그룹에 구성을 배포합니다.

> 공급업체 문제로 구성이 배포되지 않을 경우 고정된 앱은 기존 구성과 같이 유지됩니다. 하지만 새로운 구성이 배포되면 기존 레이아웃을 덮어쓰고 새로운 레이아웃이 적용됩니다.

# 10.10.8.36. 시스템 업데이트 구성

관리자는 Android 6.0 기기나 지원되는 최신 버전에서 기기 사용자가 시스템 업데이트를 관리하는 것을 제한할 수 있습니다. 이 기능은 Android Enterprise 기기에만 적용됩니다.

구성하려면

1. **구성** > **+추가**로 이동합니다.
2. **시스템 업데이트** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 옵션을 구성합니다.

| 설정 | 설명 |
| --- | --- |
| 자동 | 새 펌웨어를 사용할 수 있을 때마다 시스템 업데이트를 자동으로 적용합니다. |
| 연기<br><br>창 형식(지역 시간)<br><br>**수동 OS 업데이트 (Android 10+)**<br>Samsung 및 Zebra 기기에는 적용 또는 지원되지 않습니다. | 30일 동안 시스템 업데이트 설치를 연기합니다. 30일이 지나면 업데이트를 설치하기 위해 시스템이 기기 사용자를 표시합니다.<br><br>시스템 업데이트를 자동으로 적용할 기간 일정을 예약합니다.<br>**시작 시간** 및 **종료 시간**을 선택합니다.<br><br>모든 기기에 업데이트를 적용하기 전에, 제한된 수의 기기에서 수동으로 OS 업데이트를 수행하도록 선택합니다.<br>**펌웨어 파일** - **사용자 지정 속성** 또는 **HTTPS 주소** 옵션을 선택합니다.<br>다음 세부 정보를 입력합니다.<br>• 펌웨어 위치 - **사용자 지정 속성**을 펌웨어 파일 옵션으로 선택하면, 파일 전송에 사용된 사용자 지정 속성을 제공해야 합니다. 펌웨어 파일은 자체 호스팅되거나 파일 전송 구성을 사용하여 MDM용 Ivanti Neurons에 업로드될 수 있습니다. 자세한 내용은 **파일 전송 구성**을 참조하십시오. 50MB 이상의 파일을 MDM용 Ivanti Neurons에 업로드하려면 추가 라이선스가 필요합니다.<br>• 설명(선택 사항)<br>• 지문(필수) - 해당 OS 버전이 장치에 설치되어 있는지 확인하는 용도입니다.<br>OTA 폴더의 압축을 풀고 /META-INF/com/android/metadata 파일을 열면 OTA 파일에서 지문을 찾을 수 있습니다. 아래와 유사한 항목을 검색합니다:<br>"post-build=google/xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxxxx:user/release-keys"<br>위의 항목에서, **google/ xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxx:user/release-keys**는 지문이고 TQ3A.230805.001.S1은 빌드 ID입니다(빌드 ID는 지문에서 '/'로 구분된 값의 왼쪽에서 4번째 값임).<br>• 체크섬(선택 사항)<br>**업데이트 설정** -> **OS 업데이트 요청** - 이 섹션의 설정은 Zebra 펌웨어 구성과 동일합니다. 이 표의 *Zebra 펌웨어 구성* 섹션을 참조하십시오.<br>**HTTPS 주소**를 펌웨어 파일 옵션으로 선택하는 경우 다음 정보를 제공해야 합니다:<br>• 펌웨어 위치 - 인증할 필요 없이 펌웨어를 다운로드할 수 있는 경로를 입력합니다.<br>설명(선택 사항)<br>• 지문(필수) - 해당 OS 버전이 장치에 설치되어 있는지 확인하는 용도입니다.<br>• 체크섬(선택 사항)<br>"**OS 업데이트 요청**" 섹션 외에도 **다운로드 요청 시작** 및 **다운로드 중 조건** 섹션이 제공됩니다. **다운로드 요청 시작** 및 **다운로드 중 조건** 섹션에서 사용 가능한 옵션은 **Zebra 펌웨어 구성** 섹션 아래에 있는 옵션과 동일합니다.<br>기기에서 시스템 업데이트가 다운로드 후 시작되면, 업데이트 중에 기기를 재시작할 경우 업데이트 과정이 중단됩니다. |
| 동결 기간 | 지정된 기간에 대해 시스템 업데이트를 동결합니다.<br>이 옵션은 Android 9.0+ 기기에 적용됩니다.<br>**동결 기간 추가**를 클릭합니다.<br>동결 기간에 대한 **시작일** 및 **종료일**을 선택합니다.<br>동결 기간은 90일을 넘을 수 없으며 여러 동결 기간을 추가할 수 있습니다. 다음 동결 기간은 이전 종료일로부터 60일 후에만 선택할 수 있습니다.<br>동결 기간을 삭제하려면 삭제 아이콘을 클릭합니다. |
| **Zebra 펌웨어 구** | Zebra 기기(Android 8.0 또는 지원되는 최신 버전에서 실행되는)의 작동 펌웨어를 업그레이드 또는 업데이트하려면 **Zebra OTA 구성**을 선택하십시오. 이는 기기 소유자 모드에만 적용됩니다. |

| 설정 | 설명 |
| --- | --- |
| 성 | Zebra OTA 업데이트를 구성하려면 **관리자 > 펌웨어 관리 > Zebra OTA**에서 MDM용 Ivanti Neurons OTA 서비스를 활성화하고 MDM용 Ivanti Neurons에 Zebra 기기가 있어야 합니다. 팝업에 Zebra 자격 증명을 입력해야 합니다. 자격 증명을 다시 만들려면 Zebra에 직접 문의하십시오.<br>이 옵션을 선택하면 등록된 Zebra 기기 목록이 표시됩니다.<br>펌웨어를 선택하여 기기 모델에 적용하는 방법:<br>1. Zebra 기기에 대한 **작업** 열에서 다음 작업을 수행합니다.<br>◦ **없음**: 기기 모델에 대해 아무 작업도 수행되지 않습니다.<br>◦ **전체 업그레이드**. **대상 Zebra 펌웨어** 창에서 기기 모델에 적용될 전체 업그레이드 펌웨어 버전을 선택합니다.<br>**전체 업그레이드** 프로세스 중에는 포트 443만 필요합니다.<br>**검색** 필드에서 빌드 ID의 문자를 입력하여 빌드 ID에 기반한 업그레이드를 검색할 수 있습니다. 빌드 ID가 분류되어 내림차순(최신이 맨 상단)으로 표시됩니다.<br>**패치 업그레이드** 옵션은 Android 11+ 장치에서 사용할 수 **없습니다**.<br>2. 다음 옵션 중 하나를 구성합니다.<br>**다운로드 요청 시작** - 이 조건은 Go app에서 평가합니다.<br>◦ **필요한 최소 배터리 수준**: 슬라이더를 이동하여 사용 가능한 범위에서 필요한 최소 배터리 수준을 설정합니다.<br>◦ **장치 충전 필요**: 프로세스 중에 장치를 충전 모드로 유지하려면 이 옵션을 선택합니다.<br>◦ **다운로드 일정**: 다운로드 요청 및 파일 다운로드를 시작하는 일정을 생성하려면 이 옵션을 선택합니다.<br>◦ **유휴 장치 필요**, **충전 필요**, **요금제 네트워크를 통한 다운로드 허용**은 Android Download Manager로 전달됩니다. Go app 은(는) 언급된 창에서 위와 같은 매개 변수로 Android Download Manager에 다운로드 요청을 추가합니다.<br>**다운로드 일정 적용** - 다운로드를 예약하려면 **요일**, **시작 시간** 및 **종료 시간**을 선택합니다. 여러 요일을 선택하여 다운로드를 예약할 수도 있습니다. 예를 들어 토요일과 일요일을 선택하고 시작 시간과 종료 시간을 오전 12시에서 오후 11시까지로 하면, 선택한 요일의 해당 시간 동안에만 Zebra 기기에서 다운로드가 수행됩니다.<br>Go app에서 장치에 구성이 적용되면 예정대로 다운로드가 시작됩니다. 다운로드 종료 시간 제한은 없으며 예정된 종료 시간을 넘는 시간에 완료될 수 있습니다.<br>◦ 업데이트 일정 적용 - 펌웨어 업데이트 설치를 예약하려면 **요일**, **시작 시간** 및 **종료 시간**을 선택합니다.<br>기기 배터리 수준이 32 미만일 경우 설치가 연기됩니다.<br>업데이트 일정이 구성되지 않은 경우 펌웨어 다운로드 완료 직후에 설치가 시작됩니다.<br>3. 다음 옵션 중 하나를 구성합니다.<br>**다운로드 중 조건** - 이 조건은 다운로드 관리자에 의해 평가됩니다. 선택은 기준에 따라 결정할 수 있습니다.<br>◦ **기기 유휴 필요**(기본으로 선택): 기기가 유휴 상태일 때 기기에서 펌웨어 업데이트를 허용합니다.<br>◦ **충전 필요**(기본적으로 선택): 충전 모드일 때 기기에서 펌웨어 업데이트를 허용합니다.<br>◦ **데이터 통신 네트워크를 통한 다운로드 허용**: Wi-Fi 모드에서 다운로드를 허용하려면 이 옵션을 선택합니다. 이 옵션은 기본으로 선택 해제되어 있습니다.<br>◦ **유휴 장치 필요**, **충전 필요**, **요금제 네트워크를 통한 다운로드 허용**은 Android Download Manager로 전달됩니다.Go app 은(는) 언급된 창에서 위와 같은 매개 변수로 Android Download Manager에 다운로드 요청을 추가합니다.<br>**지정된 "다운로드 일정"을 초과해도 다운로드되도록 허용**: 지정된 다운로드 일정을 초과해도 다운로드되 |

| 설정 | 설명 |
| --- | --- |
| | 도록 허용하려면 이 옵션을 선택합니다.<br>**OS 업데이트 요청**<br>◦ **필요한 최소 배터리 수준** - OS 업데이트를 요청하는 데 사용할 수 있어야 하는 최소 배터리 수준을 설정하려면 이 옵션을 선택합니다.<br>◦ **장치 충전 필요** - 프로세스 중에 장치를 충전 모드로 유지하려면 이 옵션을 선택합니다.<br>◦ **기기에서 OS 업데이트 시작 일정 만들기** - 기기에서 OS 업데이트가 시작되는 일정을 설정하려면 이 옵션을 선택합니다.<br>Go app에서 장치에 구성이 적용되면 예정대로 다운로드가 시작됩니다. 다운로드 종료 시간 제한은 없으며 예정된 종료 시간을 넘는 시간에 완료될 수 있습니다.<br>**적용**을 클릭합니다. |
| Samsung e-FOTA 구성 | Samsung 기기의 작동 펌웨어를 업그레이드 또는 업데이트하려면 **Samsung e-FOTA 구성**을 선택합니다(Knox 버전 2.7.1 이상에서). 이는 회사 소유 기기의 관리되는 기기 모드에만 적용됩니다.<br>Samsung e-FOTA가 지원되는 기기를 등록하지 않은 경우에는 이러한 정보를 알리는 메시지가 페이지에 표시됩니다.<br>Samsung e-FOTA 업데이트를 구성하려면 **관리 > 펌웨어 관리 > Samsung E-FOTA**에서 Samsung E-FOTA 라이센스를 활성화해야 합니다. 이 옵션을 선택하면 등록된 Samsung 기기 목록이 표시됩니다.<br>펌웨어를 선택하여 기기 모델에 적용하는 방법:<br>1. Samsung 기기에 대한 **작업** 열에서 다음 작업을 수행합니다.<br>◦ **최신**: 최신 펌웨어 버전이 적용됩니다. 이 옵션은 기본으로 선택되어 있습니다.<br>◦ **강제**: 대상 Samsung 펌웨어 선택 창에서 기기 모델에 강제 적용할(사용자 개입 없이) 특정 펌웨어 버전을 선택합니다. 이 작업이 수행되면 15분 안에 펌웨어 다운로드가 시작됩니다.<br>◦ **대상**: 대상 Samsung 펌웨어 선택 창에서 기기 모델에 적용할 특정 펌웨어 버전을 선택합니다.<br>'강제' 또는 '대상' 작업을 수행할 때 기기에 해당하는 펌웨어가 목록에 없는 경우에는 이러한 정보를 알리는 메시지가 페이지에 표시됩니다.<br>2. **디버그 FW 활성화**(선택 사항): **디버그 FW 활성화** 옵션이 활성화되고 구성이 적용되면 기기가 더미 펌웨어로 업그레이드됩니다. Samsung 기기 펌웨어의 더미 펌웨어를 이용해 실제로 기기를 수정하지 않고도 관리자가 기기에서 시스템 업데이트 구성 동작을 테스트할 수 있습니다.<br>더미 펌웨어가 아닌 실제 펌웨어 업데이트로 업그레이드할 경우 관리자는 구성을 적용하기 전에 **디버그 FW 활성화** 옵션이 비활성화되어 있는지 확인해야 합니다.<br>3. **적용**을 클릭합니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정
8. **완료**를 클릭하세요.

## 삼성 E-FOTA 구성(지원 중단)

삼성 E-FOTA 구성은 2022년 7월부터 지원이 중단되었습니다. 따라서 이 구성은 신규 기기에 사용할 수 없습니다. 기존 구성된 기기의 경우 이 구성의 비활성화만 가능합니다.

# 10.10.8.37. Windows 10 업데이트 관리

관리자는 Windows 10 업데이트 관리를 사용하여 업데이트하려는 Windows 10 기기에서 보고된 업데이트를 확인하고 승인할 수 있습니다. 이 기능을 사용하면 불필요하거나 테스트 되지 않은 업데이트가 기기에 설치되는 것을 방지할 수 있습니다.

업데이트 관리 기능을 사용하려면 **업데이트 승인 필요** 옵션이 활성화된 상태에서 **소프트웨어 업데이트** 구성으로 설정된 기기가 필요합니다. 기기에 이 구성을 적용해야만 기기가 업데이트 설치 준비를 보고하고 승인을 기다릴 수 있습니다.

## 업데이트 관리

1. **관리 > Windows > Windows 업데이트**로 이동합니다. 페이지에 업데이트에 관한 다음 상세 정보가 표시됩니다.
   **생성 날짜**: 업데이트가 생성된 날짜**제목**: 기술 자료 정보 번호와 함께 업데이트 유형을 설명합니다.

> 업데이트를 클릭하면 설명이 표시됩니다.

**분류**: 업데이트 유형을 다음 중 하나로 분류합니다.

- 중요 업데이트
- 정의 업데이트
- 드라이버 업데이트
- 보안 업데이트
- 업데이트
- 업그레이드
- 업데이트 롤업

**배포**: 업데이트를 위해 수행되는 배포 예를 들어, 업데이트가 모든 기기에 배포되면 **모두**를 표시합니다.

> 업데이트가 특정 수의 그룹에 배포되면 배포 수가 표시됩니다. 예를 들어 세 그룹에게 배포가 수행된 경우 3을 표시합니다.

2. 또한, 필요한 기기에 업데이트가 배포되었는지 여부를 확인할 수 있습니다. 다음 열에 표시된 숫자는 업데이트의 여러 카테고리에 속한 기기 수를 나타냅니다.
   - 해당하는 기기
   - 설치된 기기
   - 실패한 기기
   - 재부팅 보류 중 기기

이러한 숫자 중 하나를 클릭하면 기기 페이지의 필터링 보기로 이동하여 업데이트 상태를 확인하고 필요한 작업을 수행할 수 있습니다.
업데이트를 검토한 후 업데이트 체크박스를 클릭하여 기기에 배포하고 싶은 업데이트를 선택합니다.

3. **작업**에서 **배포 설정**을 클릭합니다.
4. **Windows 업데이트 배포** 창에서 다음 배포 옵션 중 하나를 선택합니다.
   **모든 기기**: 모든 기기에 업데이트를 배포합니다.
   **배포 안함**: 기기에 업데이트를 배포하지 않습니다.**사용자 지정**: 특정 기기 그룹에 업데이트를 배포합니다.
5. **저장**을 클릭하세요.

## 업데이트 검색 및 필터링

다음과 같은 기준을 기반으로 업데이트를 검색하고 필터링할 수 있습니다.

- 기술 자료 ID
- 구성된 배포

기술 자료 ID에 기반한 필터링:

1. **Windows 10 업데이트 관리** 페이지에서 빠른 검색 필드에 기술 자료 ID를 입력합니다(검색 필드에는 숫자만 사용).
   예: KB4056892의 경우, 4056892만 입력합니다. 검색 기준과 맞는 업데이트가 페이지에 표시됩니다.

> **지원** 및 **추가 정보** 링크를 클릭하여 업데이트의 추가적인 정보를 확인할 수 있습니다.**지원**링크는 업데이트를 위한 제품 지원 정보를 제공하는 Microsoft 웹 페이지로 연결되며 **자세한 내용**링크는 기술자료와 같은 업데이트에 관한 자세한 정보를 보여주는 Microsoft 웹 페이지로 연결됩니다.

구성된 배포를 기반으로 필터링:

**Windows 10 업데이트 관리** 페이지에서 구성된 배포에 따라 다음 필터링 옵션 중 하나를 선택합니다.

- **모두**: 모든 업데이트를 표시합니다.
- **구성됨**: 기기에 배포된 업데이트 목록을 표시합니다.
- **구성되지 않음**: 배포가 특정하지 않은 업데이트 목록을 표시합니다.

> 구성된 필터와 구성되지 않은 필터는 배포 상태에 따라 결정되며, 배포는 **없음**으로 설정할 수도 있습니다.

## 기기에 대한 업데이트 검토

기기별 업데이트 세부 정보 검토 방법:

1. **장치 > 장치**를 선택하세요.
2. 세부 정보 페이지를 표시할 기기 이름을 클릭합니다.
3. **업데이트** 탭으로 이동합니다. 기기에 지연(관리자가 업데이트를 승인했지만 기기에 설치됨으로 보고되지 않은 경우), 실패, 설치된 업데이트가 보여집니다.

> 대시보드의 알림 페이지에서 새 Windows 업데이트에 대한 알림을 볼 수도 있습니다. 알림에는 알림 생성 날짜, 사용 가능한 알림 개수 및 알림 목적이 포함됩니다. Windows 업데이트 알림은 관리자 포털의 상단 우측 모서리에서도 볼 수 있습니다.

# 10.10.8.38. Windows 앱 일정 설정

Windows 데스크톱 앱의 크기가 클 경우 엔터프라이즈의 주요 사용 시간 동안 네트워크 및 서버에 길고 추가적인 부하를 줄 수 있습니다. Windows 앱 일정 설정 기능은 사용자가 선택한 시간 동안 기기에 특히 크기가 큰 앱을 설치하도록 설정할 수 있도록 합니다.

앱 설정을 구성하려면 다음 단계를 수행합니다.

1. **앱 > 앱 카탈로그**를 선택하세요.
2. **추가**를 클릭하고 Windows 앱을 선택한 후 **앱 추가** 마법사에서 다음 단계를 계속합니다.
3. 5단계(구성)에서 **애플리케이션 구성 설정 설치**를 클릭하여 **구성 설정** 페이지를 확인합니다.
4. **설치 예약** 체크박스를 선택합니다.

> **일정 설치** 체크박스가 자동 설치가 활성화된 경우에만 표시됩니다.

5. **시작 시간** 및 **종료 시간**을 선택하여 앱 설치 시간을 예약합니다.
6. **시작일**과 **종료일**을 선택하여 앱을 설치할 날짜를 예약합니다.

> 예약된 날짜를 놓치면 수행해야 하는 두 작업(**다음 체크인 중 설치** 또는 **설치 안 함**) 중 하나를 선택할 수도 있습니다.

7. 앱 구성 배포 옵션(**앱이 있는 모든 사람**, **없음**, 또는 **사용자 지정**)을 선택합니다.
8. **완료**를 클릭하세요.

> 예약이 필요한 앱은 Apps@Work에 추가해서는 안 됩니다.
> Store 앱은 자동 설치를 지원하지 않기 때문에 Store 앱에서는 앱 일정 설정을 적용할 수 없습니다.

# 10.10.8.39. Windows BIOS 구성

관리자는 Lenovo 기기에서 Windows BIOS 설정을 구성할 수 있습니다. 이 구성을 설정하려면 BIOS 설정을 지원하는 Lenovo 기기가 하나 이상 등록되어 있어야 합니다.

구성하려면

1. **구성** > **+추가**로 이동합니다.
2. **Windows BIOS** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. Choose device model 섹션의 드롭다운 목록에서 기기 모델을 선택합니다.
6. 구성 설정 섹션에서 다음 옵션을 구성합니다.

> 설정 목록은 등록된 특정 기기 모델에 사용할 수 있는 옵션에 따라 다릅니다. 자세한 내용은 해당 기기 웹사이트를 참조하십시오.

| 설정 항목 | 설정하기 |
| --- | --- |
| AMT 제어 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| Adaptive Thermal Management(적응성 열 관리) AC | 다음 옵션 중 하나를 선택합니다.<br>• **밸런스 조정**<br>• **성능 극대화** |
| Adaptive Thermal Management(적응성 열 관리) 배터리 | 다음 옵션 중 하나를 선택합니다.<br>• **밸런스 조정**<br>• **성능 극대화** |
| 올웨이즈온 USB | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| BIOSPasswordAtBootDeviceList | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 재부팅 시 BIOS 비밀번호 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 무인 부팅 시 BIOS 비밀번호 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 최종 사용자에 의한 BIOS 업데이트 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| Bluetooth 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 부팅 기기 목록 F12 옵션 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |

| 설정 항목 | 설정하기 |
| --- | --- |
| 부팅 표시 기기 | 다음 옵션 중 하나를 선택합니다.<br>• **DisplayPort**<br>• **디스플레이 독**<br>• **HDMI**<br>• **LCD** |
| 부팅 모드 | 다음 옵션 중 하나를 선택합니다.<br>• **진단**<br>• **빠른** |
| 부팅 순서 잠금 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| BootTimeExtension | 다음 옵션 중 하나를 선택합니다.<br>• **1**<br>• **10**<br>• **2**<br>• **3**<br>• **5**<br>• **비활성화** |
| 하단 커버 변형 감지 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| CPU 전력 관리 | 다음 옵션 중 하나를 선택합니다.<br>• **자동**<br>• **비활성화** |
| Computrace 모듈 활성화 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 데이터 실행 방지 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 이더넷 LAN 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 이더넷 LAN 옵션 ROM | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화** |

| 설정 항목 | 설정하기 |
| --- | --- |
| | • **활성화** |
| 지문 비밀번호 인증 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 지문 프리 데스크톱 인증 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 지문 판독기 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 지문 판독기 우선순위 | 다음 옵션 중 하나를 선택합니다.<br>• **외부**<br>• **내부 전용** |
| 지문 보안 모드 | 다음 옵션 중 하나를 선택합니다.<br>• **높음**<br>• **보통** |
| Fn Ctrl 키 교체 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| FnKeyAsPrimary | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| FnSticky | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| IPv4 네트워크 스택 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| IPv6 네트워크 스택 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 통합 카메라 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |

| 설정 항목 | 설정하기 |
| --- | --- |
| InternalStorageTamper | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 키보드 비프음 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| BIOS 설정 잠금 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 메모리 카드 슬롯 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 마이크 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 최소 비밀번호 길이 | 다음 옵션 중 하나를 선택합니다.<br>• 4<br>• 5<br>• 6<br>• 7<br>• 8<br>• 9<br>• 10<br>• 11<br>• 12<br>• **비활성화** |
| NFFControl | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| NFC 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| AC 부착으로 전원 켜짐 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |

| 설정 항목 | 설정하기 |
| --- | --- |
| PasswordBeep | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| PasswordCountExceededError | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| TPM 삭제용 물리적 실재 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| TPM 프로비저닝용 물리적 실재 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 신속 시작 기술 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 안전 부팅 | **활성화** 선택 |
| 안전 롤백 방지 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 보안 칩 | 다음 옵션 중 하나를 선택합니다.<br>• **활성**<br>• **비활성화**<br>• **활성화**<br>• **비활성** |
| 스마트 카드 슬롯 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| SpeedStep | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 시작 옵션 키 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| TXT 기능 | 다음 옵션 중 하나를 선택합니다. |

| 설정 항목 | 설정하기 |
| --- | --- |
| | • **비활성화**<br>• **활성화** |
| 총 그래픽 메모리 | 다음 옵션 중 하나를 선택합니다.<br>• **256MB**<br>• **512MB** |
| 터치패드 | 다음 옵션 중 하나를 선택합니다.<br>• **자동**<br>• **비활성화** |
| TrackPoint | 다음 옵션 중 하나를 선택합니다.<br>• **자동**<br>• **비활성화** |
| USB30 모드 | 다음 옵션 중 하나를 선택합니다.<br>• **자동**<br>• **비활성화**<br>• **활성화** |
| USB BIOS 지원 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| USB 포트 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| Uefi Pxe 부팅 우선순위 | 다음 옵션 중 하나를 선택합니다.<br>• **IPv4 우선**<br>• **IPv6 우선** |
| VTd 기능 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 가상화 기술 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |

| 설정 항목 | 설정하기 |
| --- | --- |
| Wake On LAN | 다음 옵션 중 하나를 선택합니다.<br>• **AC 전용**<br>• **AC 및 배터리**<br>• **비활성화**<br>• **활성화** |
| 무선 LAN 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |
| 무선 WAN 액세스 | 다음 옵션 중 하나를 선택합니다.<br>• **비활성화**<br>• **활성화** |

7. **다음**을 클릭하세요.
8. 다음 배포 옵션 중 하나를 선택합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정
9. **완료**를 클릭하세요.

# 10.10.8.40. Windows BitLocker

관리자로서, 기기 GUID 및 복구 비밀번호로 Excel 파일을 업로드하여 일련의 암호화된 Windows 10 기기에 대해 복구 키를 대량 업데이트할 수 있습니다.

복구 키의 대량 업데이트를 위한 Excel 파일 업로드 방법:

1. **관리자>Windows BitLocker**로 이동합니다.
2. .csv 파일의 예를 다운로드하여 보려면 **샘플 csv 파일**을 클릭하여 샘플 CSV 파일을 다운로드합니다.
3. BitLocker 복구 키 .csv 파일에 대한 기록을 생성하고 추가합니다.
4. **복구 비밀번호 업로드**를 클릭합니다.
5. **파일 선택**을 클릭하여 생성한 .csv 파일을 업로드합니다.
6. **업로드**를 클릭합니다. 이전에 업로드된 키로 새 파일을 업로드하면 기존 항목을 덮어쓰게 됩니다.

> 각 업로드마다 최대 1,000개의 기록을 제출할 수 있습니다. 업로드 성공 후, 특정 기기의 기기 상세 정보에서 개별 키를 볼 수 있습니다.

# 10.10.8.41. Windows 키오스크 구성

Windows 키오스크 구성을 사용하여 Windows 10 기기에서 단일 또는 다중 앱 키오스크를 구성할 수 있습니다. 이 구성을 적용함으로써 키오스크 사용자는 키오스크 앱 이외의 어떠한 기능에도 액세스가 제한됩니다. 이 구성은 Windows Bridge가 활성화되어야 합니다.

다음은 구성이 적용될 수 있는 세 가지 모드입니다.

- 단일 애플리케이션
- 다중 애플리케이션(Windows 기기에서 애플리케이션 목록 가져오기)
- 다중 애플리케이션(시작 메뉴 구성에서 기존 레이아웃 선택)

> Windows 키오스크 구성에 사용되는 애플리케이션은 구성된 Windows 키오스크 모드로 들어가기 전에 이미 기기에 존재해야 합니다.

Windows 키오스크 구성을 구성하려면 다음 단계를 수행합니다.

1. **구성** > **+추가**로 이동합니다.
2. **Windows 키오스크** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 구성 설정 섹션에서 다음 표에 설명된 바와 같이 남은 설정을 지정합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| **키오스크 모드 선택**: 다음 세 가지 옵션 중 선택합니다. | |
| **단일 애플리케이션** | 이 옵션을 선택하여 기기에 대한 단일 애플리케이션 키오스크 모드를 구성합니다.<br>1. **Windows 기기 선택(선택 사항)** 섹션에서 Windows 10 기기를 선택합니다. **기기에서 앱 가져오기**를 클릭하여 기기에서 앱 목록을 가져옵니다. 선택한 기기는 사용자의 감독하에 있어야 하며 앱 데이터를 가져오려면 체크인이 필요합니다.<br>이 단계를 건너뛰려면 **이 단계 건너뛰기를 선택합니다. 원할 경우 나중에 마음을 바꿀 수 있습니다.** 체크박스를 선택하십시오.<br>2. **가져온 앱 목록에서 추가**를 클릭하여 가져온 목록에서 앱을 추가합니다.<br>3. 앱의 **이름** 열에서 라디오 버튼을 클릭하여 단일 앱을 선택합니다. **새로 추가**를 클릭하여 목록에 새 앱을 추가합니다. 목록에서 앱을 삭제하려면 삭제 아이콘을 클릭하십시오. |
| **다중 애플리케이션 (Windows 기기에서 애플리케이션 목록 가져오기)** | 이 옵션을 선택하여 기기에 대한 다중 애플리케이션 키오스크 모드를 구성합니다.<br>1. **Windows 기기 선택(선택 사항)** 섹션에서 Windows 10 기기를 선택합니다. **기기에서 앱 가져오기**를 클릭하여 기기에서 앱 목록을 가져옵니다. 선택한 기기는 사용자의 감독하에 있어야 하며 앱 데이터를 가져오려면 체크인이 필요합니다.<br>이 단계를 건너뛰려면 **이 단계 건너뛰기를 선택합니다. 원할 경우 나중에 마음을 바꿀 수 있습니다.** 체크박스를 선택하십시오.<br>2. **키오스크 앱 및 시작 메뉴 레이아웃**에서 **가져온 앱 목록에서 추가**를 클릭합니다. **키오스크 앱 선택** 창이 표시됩니다. 가져온 목록에서 앱을 선택하고 **선택한 앱 사용**을 클릭합니다.<br>3. 추가 허용된 앱 섹션에서 **가져온 앱 목록에서 추가**를 클릭합니다. **키오스크 앱 선택** 창이 표시됩니다. 가져온 목록에서 앱을 선택하고 **선택한 앱 사용**을 클릭합니다.<br>추가 허용된 앱은 **키오스크 앱 및 시작 메뉴 레이아웃**에서 선택된 앱에 대한 종속 항목으로 간주되는 앱입니다. '허용된 앱'이 없을 경우 OS는 시작 메뉴에 애플리케이션 아이콘이 표시되더라도 이 애플리케이션의 실행을 허용하지 않습니다.<br>4. **새로 추가**를 클릭하여 목록에 새 앱을 추가합니다. 목록에서 앱을 삭제하려면 삭제 아이콘을 클릭하십시오. 목록의 앱을 끌어 목록의 어느 위치로든 이동할 수 있습니다.<br>5. **다중 앱 기타 설정**에서 필요한 옵션을 선택하십시오.<br>◦ **전원 버튼 숨기기**<br>◦ **사용자 타일 숨기기**<br>◦ **작업 표시줄 숨기기**<br>Microsoft Windows 11에서는 다중 앱 키오스크 모드 옵션인 "**작업 표시줄 숨기기**"는 지원되지 않습니다. |
| **다중 애플리케이션(시작 메뉴 구성에서 기존 레이아웃 선택)** | 시작 메뉴 레이아웃 구성을 생성한 경우, 구성을 가져오고 이 옵션을 선택하여 다중 애플리케이션 모드를 구성하는 데 이를 사용할 수 있습니다.<br>1. **레이아웃 선택** 섹션에서 이미 시작 메뉴 구성으로 설정된 레이아웃을 선택합니다. 해당 레이아웃 매개변수로 이전에 생성된 구성이 아래의 드롭다운 목록에 표시됩니다.<br>2. 다중 앱 기타 설정에서 필요한 옵션을 선택하십시오.<br>◦ **전원 버튼 숨기기**<br>◦ **사용자 타일 숨기기** |

| 설정 항목 | 수행 작업 |
| --- | --- |
| | ◦ **작업 표시줄 숨기기**<br>Microsoft Windows 11에서는 다중 앱 키오스크 모드 옵션인 "**작업 표시줄 숨기기**"는 지원되지 않습니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.
   - 모든 기기
   - 배포 안 함(기본값)
   - 사용자 지정
8. **완료**를 클릭하세요.

> 구성이 완전한 효력을 발휘하려면 Windows 키오스크 구성을 적용 또는 업데이트한 후 기기를 재부팅해야 합니다. 다중 앱 키오스크 구성을 위한 애플리케이션에 따라 기기를 두 번째로 재부팅해야 합니다. 최초 로그인 시 일부 아이콘이 누락될 수 있으나 누락된 아이콘은 두 번째 재부팅 후 로그인 시 표시됩니다.

기기는 키오스크 구성을 적용, 삭제, 또는 업데이트한 후 재부팅해야 합니다. 이는 기기 작업 메뉴에서 다시 시작/종료 기기 명령으로 수행할 수 있습니다. 재부팅을 하지 않을 경우:

- 키오스크 구성을 적용한 후 기기가 키오스크 모드로 자동으로 들어가지 않습니다.
- 적용된 키오스크 구성을 삭제한 후 기기가 키오스크 모드에서 자동으로 빠져나오지 않습니다.
- 기기는 실행 키오스크 구성을 변경하지 않습니다.

키오스크 구성이 적용된 기기가 업데이트된 구성을 받을 경우 기기의 Windows OS가 기존 키오스크 사용자를 제거하고 새 키오스크 구성의 새 키오스크 사용자를 다시 생성합니다. 현재 사용자에 대한 세션은 기기 재부팅을 통해 확실히 종료되어야 합니다.

다중 앱 키오스크 구성에는 '.lnk' 파일, Single-App 키오스크 구성에는 '.exe' 파일로 구성하는 것이 좋습니다. 기기에서 가져온 시작 메뉴 구성은 '.lnk' 형식을 사용합니다. '.exe' 애플리케이션을 위해 수동으로 생성된 시작 메뉴 항목은 때로 '.exe' 애플리케이션에 따라 다중 앱 키오스크 구성의 시작 메뉴에 표시되지 않을 수 있습니다.

예를 들어 Windows Media Player는 다음 '.lnk' 파일 중 하나를 사용하여 시작 메뉴에 추가할 수 있습니다.

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

이 앱이 다음 '.exe' 파일을 통해 직접 추가될 경우 해당 아이콘이 표시되지 않으며 첫 번째 '.exe' 경로도 위의 '.lnk' 파일에서 내부적으로 사용됩니다.

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

단일 앱 키오스크 구성의 경우 exe 파일에 인수를 추가할 수 있습니다. E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'. 그러나 인수가 있는 exe 앱에 대한 아이콘은 다중 앱 구성의 경우 시작 메뉴에 표시되지 않습니다. 다중 앱 키오스크 구성에서 인수가 있는 exe 앱이 필요할 경우, 내부적으로 인수를 가질 수 있는 '.lnk' 파일을 사용하십시오. '.lnk'는 단일 앱 키오스크 구성의 경우 작동하지 않습니다.

# 다중 앱 키오스크 모드의 종속성

Win32/64 애플리케이션은 다중 앱 키오스크 모드의 경우 종속성이 추가 허용된 앱 섹션에 추가되어야 할 수 있습니다. '추가 허용된 앱'은 단일 앱 키오스크 모드에는 필요하지 않습니다.

**예 1**: Windows Media Player 앱의 경우 다중 앱 키오스크 모드에서는 다음과 같은 종속성이 필요합니다.

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

첫 번째 종속성은 해당 ".lnk" 파일에서 부르는 앱 바이너리입니다. 두 번째는 첫 번째 종속성에서 부르는 1회용 마법사입니다.

'허용된 앱'이 없으면 OS는 시작 메뉴에 애플리케이션 아이콘이 표시되어도 이 애플리케이션 실행을 허용하지 않습니다.

**예 2**: Internet Explorer의 경우 다음 목록의 항목을 통해 구성될 경우 그 아이콘이 시작 메뉴에 표시됩니다.

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- C:\Program Files\internet explorer\iexplore.exe
- %ProgramFiles%\Internet Explorer\iexplore.exe

Internet Explorer에는 다음과 같은 종속성이 필요합니다.

- C:\Program Files (x86)\Internet Explorer\iexplore.exe
- C:\Program Files (x86)\Internet Explorer\ExtExport.exe
- C:\Program Files (x86)\Internet Explorer\ieinstal.exe
- C:\Program Files (x86)\Internet Explorer\ielowutil.exe

첫 번째 종속성은 '.lnk' 항목에만 필요한 앱 바이너리이며 다른 종속성은 1회용 마법사에 필요합니다. 첫 번째 종속성이 없으면 OS가 팝업으로 앱을 차단합니다. 다른 종속성이 없으면 애플리케이션은 OS의 추가 알림 없이 시작 직후 닫힙니다.

# 10.10.8.42. Windows 라이선스 구성

Windows 라이선스 구성은 기기의 운영 체제를 업그레이드합니다(예: Windows 10 Pro에서 Windows 10 Enterprise로) 또한 이 구성은 Windows 10 데스크톱 기기의 제품 키를 활성화 또는 변경할 수 있는 기능을 제공합니다.

Windows 라이선스를 업그레이드하려면 다음을 수행합니다.

1. **구성 > +추가**로 이동합니다.
2. **Windows 라이선스** 구성을 선택합니다.
3. 구성 이름을 입력합니다.
4. **구성 설정** 섹션에서 Windows **제품 키**를 입력합니다.
5. **다음**을 클릭하세요.
6. 다음 배포 옵션 중 하나를 선택합니다.
    - 모든 기기
    - 배포 안 함(기본값)
    - 사용자 지정
7. **완료**를 클릭하세요.

# 11. 정책

정책 메뉴에서는 기기 요건을 비롯해 기기가 요건을 충족하지 않을 경우 발생하는 결과값을 설정할 수 있습니다. 각 정책은 하나의 규칙과 컴플라이언스 조치(규칙을 위반한 경우 결과)로 구성됩니다. **정책** 페이지에서 정책을 선택하고 설정, 배포할 수 있습니다.

> 자동화된 기기 체크인 프로세스와 관련하여 다음 변경 사항에 유의하십시오:

- 최근 90일 이내에 체크인한 기기만 평가 대상이 됩니다.
- 90일 이후~1년 이내에 체크인한 기기에는 강제 체크인 명령만 트리거됩니다.
- 최근 1년 동안 체크인하지 않은 기기에는 아무 작업도 수행되지 않습니다.

이 섹션에는 다음 주제가 포함됩니다.

- 정책 작업
- 사용자 지정 정책
- 허용 앱 모니터링 및 제어
- 정책 우선순위 지정
- Windows 하드웨어 정책

# 11.1. 정책 작업

이 섹션에는 다음 주제가 포함됩니다.


- 정책 구현
- 컴플라이언스 조치
- 기존 정책 찾기
- 정책 추가
- 정책 편집
- 정책 삭제


## 정책 구현

정책 메뉴에서는 기기 요건을 비롯해 기기가 요건을 충족하지 않을 경우 발생하는 결과값을 설정할 수 있습니다. 각 정책은 하나의 규칙과 컴플라이언스 조치(규칙을 위반한 경우 결과)로 구성됩니다. **정책** 페이지에서 정책을 선택하고 설정, 배포할 수 있습니다.

사용 가능한 정책 유형은 다음과 같습니다.

| 유형 | 상세 기능 |
| --- | --- |
| 손상된 기기 | 우선순위(1 = 가장 높음)<br>위반<br>1 플러그인 손상됨<br>2 클라이언트 변경됨<br>3<br>알 수 없는 기기 제조업체: 알 수 없음<br>4 의심되는 폴더 감지됨: [경로]<br>5 의심되는 바이너리가 다음에서 발견됨: [경로]<br>6 /data 폴더를 검색할 수 있거나 /data/data 폴더 검색 가능<br>7 /system/app/Superuser.apk 발견됨<br>8 패키지 관리자 손상됨<br>9 의심되는 앱 발견됨: [패키지]<br>탈옥(iOS) 또는 루팅된 기기(Android)는 플래그로 표시됩니다.<br>시스템에서 Android 기기를 루팅으로 인해 손상되었다고 표시하는 위반 이유를 보려면:<br>1. **정책** 탭을 클릭합니다<br>2. **손상된 기기** 링크를 클릭합니다.<br>3. **활성 위반** 탭을 클릭합니다.<br>4. 위반 열에서 위반 이유를 점검합니다.<br>시스템에서 Android 기기를 루팅으로 인해 손상되었다고 표시하는 위반 이유를 보려면:<br>5. **정책** 탭을 클릭합니다.<br>6. **손상된 기기** 링크를 클릭합니다.<br>7. **활성 위반** 탭을 클릭합니다.<br>8. **위반** 열에서 위반 이유를 점검합니다. 다음 이유 중 하나가 될 수 있습니다. |
| 데이터 보호/암호화 비활성화됨(macOS 전용) | 암호가 없거나 암호화가 활성화된 macOS 장치에 플래그로 표시됩니다. |
| 국제 로밍 | 국제 로밍 요금이 부과될 기기를 플래그로 표시합니다. 해당 기기가 체크인을 하면 상태가 새로고침 됩니다.<br>iOS의 경우, iOS에서 설정하고 리포팅한 대로 로밍 플래그가 사용됩니다. 규정 준수 조치는 첫 번째 위반 시에만 실행됩니다. |
| MDM/기기 관리가 비활성화됨 | 기기에서 MDM을 사용할 수 없는 경우에는 체크인하는 동안 다른 정책 또는 구성이나 앱의 델타 처리에 대한 평가가 이루어지지 않습니다. |
| 연결 안 됨 | 지정된 시간 범위 동안 MDM용 Ivanti Neurons와 연결되지 않은 기기를 플래그로 표시합니다.<br>지정된 시간(2~3시간에서 23~24시간)이나 일수 동안 기기를 체크인하지 않은 경우 취할 조치를 선택합니다. |
| MI 클라이언트가 연결되지 않음(iOS만 해당) | 지정된 시간 범위 동안 MDM용 Ivanti Neurons와 연결되지 않은 MDM용 Ivanti Neurons 클라이언트를 플래그로 표시합니다.<br>지정된 시간(2~3시간에서 23~24시간)이나 일수 동안 체크인하지 않은 경우 취할 조치를 선택합니다.<br>이는 iReg를 통해 등록된 기기에만 적용됩니다. 정책은 클라이언트가 없거나 클라이언트가 정의된 기간 동안 체크인하지 않은 경우 기기를 미준수로 표시합니다. |

| 유형 | 상세 기능 |
| --- | --- |
| 허용된 앱 | 허용된 앱이나 필수 앱 선택에 관한 규칙을 위반한 기기를 플래그로 표시합니다. |
| 사용자 지정 정책 | 사용자가 지정한 조건과 관련 작업에 기초하여 사용자 지정 정책을 만듭니다. |

## 컴플라이언스 조치

다음과 같은 규정 준수 작업을 진행할 수 있습니다.

| 컴플라이언스 조치 | 상세 기능 |
| --- | --- |
| 모니터 | MDM용 Ivanti Neurons 기기 페이지에서 기기에 플래그를 지정합니다. 기본적으로 이 작업은 켜져 있습니다. |
| 차단 | 마지막 체크인 세부 정보를 기준으로 정책을 위반한 후 장치가 Sentry 또는 Access를 통해 리소스에 액세스하려 할 경우 Access 및/또는 Sentry에 장치를 차단하도록 지시합니다. |
| 사용자에게 메시지 보내기 | • MDM용 Ivanti Neurons 기기 페이지에서 기기에 플래그를 지정합니다.<br>• 장치 소유주에게 이메일이 발송됩니다.<br>• 기존 정책 외에 "**규정 준수 정책 이메일 템플릿 사용**" 토글은 이제 다음 정책에도 사용할 수 있습니다:<br>◦ 데이터 보호/암호화 비활성화됨<br>◦ 국제 로밍<br>◦ MDM/기기 관리가 비활성화됨<br>◦ 연결 안 됨<br>◦ MI 클라이언트 연결 끊김<br>장치에 푸시 알림이 발송됩니다. |
| 격리 | • 장치의 설정값이 대부분 삭제됩니다.<br>◦ 예외: 암호 구성, Wi-Fi 전용 기기의 경우 Wi-Fi 구성, 제한 구성(iOS)<br>• MDM용 Ivanti Neurons에서 설치된 모든 앱을 제거합니다.<br>• iBook 및 ePub 파일을 포함하여 MDM용 Ivanti Neurons가 배포하는 모든 콘텐츠를 제거합니다.<br>• MDM용 Ivanti Neurons 카탈로그에 대한 액세스를 차단합니다.<br>• 추가 앱 설치 프롬프트가 중지됩니다.<br>• AppConnect 지원 앱에 대한 액세스를 차단합니다.<br>• AppConnect 지원 앱 지원을 포함합니다.<br>• 켜져 있으면, 격리된 기기의 개인 공간에서 개인 앱을 일시 중지하여, 기능하게 하려면 사용자가 기기에서 컴플라이언스 문제를 해결해야 한다는 점을 나타냅니다. 회사 소유 기기에서 작업 프로필로 프로비저닝된 Android 11+ 기기에서 지원됩니다. |
| 추가 격리 실행(선택 사항): | **새로운 앱 다운로드 차단** - 장치에 새로운 앱을 다운로드하지 못하도록 차단합니다.<br>**관리형 앱 격리** - MDM용 Ivanti Neurons 관리형 앱을 장치에서 제거하고 새로운 앱 다운로드 차단 옵션을 활성화하여 앱이 장치에 재설치되지 않도록 차단합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 애플리케이션을**<br>• **다음을 제외한 모든 앱 제거** - 애플리케이션 목록에 추가된 애플리케이션을 제외한 모든 애플리케이션을 제거합니다.<br>• **지정된 애플리케이션** - 조회하거나 수동으로 하나 이상의 앱을 추가합니다(번들 ID 또는 패키지 이름 사용). **앱 보기** 탭을 클릭하여 추가된 앱 목록을 검토합니다. App Store 액세스 차단 기본 격리 조치는 더 이상 사용할 수 없습니다. 특정 기기에서는 특정 기기 제한으로 인해 격리 작업으로 기기에서 애플리케이션을 제거하지 못합니다.<br>세 가지(모든 애플리케이션, 다음을 제외한 모든 애플리케이션 제거, 지정된 애플리케이션) 모두에 대해 기본적으로 이 옵션이 선택되며 선택을 취소할 수 없습니다. 이로써 기기에 앱이 다시 설치되는 것이 차단됩니다. |

| 컴플라이언스 조치 | 상세 기능 |
| --- | --- |
| | **구성 제거** - 장치에서 MDM용 Ivanti Neurons 구성을 제거합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 구성**<br>• **지정된 구성** - 목록에서 하나 이상의 구성을 선택하거나 검색합니다. **선택한 구성** 탭을 클릭하여 선택한 구성 목록을 검토합니다.<br>**지정된 구성 푸시** - 사용자 지정 규정 준수의 일환으로 지정된 구성을 배포합니다.<br>이 목록에는 다음 기준을 충족하는 구성이 포함되어 있습니다.<br>• 활성화된 구성<br>• 비시스템 구성<br>• 격리 가능한 구성<br>• 현재 공간에 생성되었거나 기본 공간에서 위임된 구성<br>격리 불가능한 구성 목록의 경우에는 격리 불가능한 구성을 참조하십시오.<br>**콘텐츠 제거** - MDM용 Ivanti Neurons에서 배포한 앱과 관련한 모든 콘텐츠 및 미디어를 장치에서 제거합니다.<br>**개인 앱 일시 중지** - 격리된 장치의 개인 공간에서 앱을 일시 중지하여 장치 사용자가 장치의 규정 준수 문제를 해결해야 사용할 수 있다는 점을 나타냅니다. 회사 소유 기기에서 작업 프로필로 프로비저닝된 Android 11+ 기기에서 지원됩니다. |

## 기존 정책 찾기

정책 페이지의 검색 기능과 필터를 사용하여 하나 이상의 기존 정책을 찾을 수 있습니다.

**절차**

1. **정책**으로 이동합니다.
2. 특정 기준과 일치하는 정책 목록을 필터링하려면 **필터**를 클릭합니다.
3. 하나 이상의 필터 기준을 선택합니다.
4. 기존 정책을 이름으로 검색하려면 **검색** 필드에 정책 이름을 입력합니다.

## 정책 추가

**절차**

1. **정책**으로 이동합니다.
2. +**추가**(우측 상단)를 클릭합니다.
3. 정책 유형을 선택하세요.
4. 설정을 완료하세요.
5. 해당 정책을 수신할 장치 그룹을 선택하세요.

> 한 번에 최대 100개의 구성 파일로 배포할 수 있습니다.

6. **완료**를 클릭하세요.

## 정책 편집

**절차**

1. **정책**으로 이동합니다.
2. 필수 정책인 경우에는 작업 열 아래에서 **편집**(연필) 아이콘을 클릭합니다.
3. 원하는 속성을 수정하세요.
4. 변경 사항을 저장합니다.

## 정책 삭제

**절차**

1. **정책**으로 이동합니다.
2. 필수 정책인 경우에는 작업 열 아래에서 **제거**를 클릭합니다.
3. **예**를 눌러 확인합니다.

정책 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 기기 관리
- 장치 읽기 전용

자세한 내용은 **정책 우선순위 지정**을 참조하십시오.

# 11.2. 사용자 지정 정책

정책

**라이센스:** Platinum

**적격 기기:** Android, iOS, macOS, Windows.

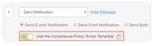
지정하는 기기 및 사용자 속성, 섹션 기준, 값 및 컴플라이언스 조치를 바탕으로 사용자 지정 정책을 생성할 수 있습니다.

> 사용자 지정 정책 정의 시 Android 보안 패치 수준 설정도 사용할 수 있습니다.

## 사용자 지정 정책 추가

1. **정책**으로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **사용자 지정 정책**을 선택합니다.
4. 사용자 지정 정책의 이름을 입력합니다.
5. **+ 설명 추가**를 클릭한 후 원하는 경우 상세 사항을 추가로 입력합니다.
6. 규칙 작성기를 사용하여 조건이 충족될 때 작업을 트리거하는 조건을 정의합니다. 조건 생성 지침은 조건 설정 이해를 참조하십시오. MDM용 Ivanti Neurons 관리자는 규칙 작성기에서 사용자 그룹 이름 속성을 선택할 때 중복 그룹을 식별할 수 있도록 중복 사용자 그룹 수 및 해당 GUID 수를 표시합니다. 또한 이 규칙 아래에 있는 표에는 중복 사용자 그룹 목록과 사용자 그룹 이름, GUID, 소스, 배포된 이름(DN)과 같은 세부 정보가 표시됩니다.
7. 지정한 조건이 충족될 때 적용할 규정 준수 조치(아래의 기본 조치 참조) 중 하나를 선택합니다. 다른 작업 사이에 "**대기**" 작업을 추가하면 새로운 작업을 시작하기 전에 기기 사용자가 기기를 복구하고 준수 작업을 할 수 있습니다. 예를 들어, 격리 조치를 적용하기 전에 경고 메시지를 전송하여 24시간 동안 기다릴 수 있습니다.
8. 기본적으로 꺼져 있는 **기기가 다시 규정 준수 상태가 되면 알림 보내기** 옵션을 선택합니다.

- **이메일 알림 보내기** - 장치가 다시 규정을 준수하게 되면 이를 알리는 이메일을 장치 사용자의 이메일 주소로 보냅니다.
  - 여기에서 구성하는 메시지를 구성 중인 정책 알림 이메일 템플릿에 삽입하려면 이메일 템플릿 브랜딩이메일 템플릿 사용자 정의하기에서 설명한 것처럼 **규정 준수 정책 이메일 템플릿 사용** 옵션을 켭니다.개요는 정책 규정 준수 알림 이메일 구성 및 사용을 참조하십시오.

    
  - 선택 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 수신자에게 보다 자세한 정책 위반 사항 및 기타 관련 정보 등을 제공할 수 있습니다. 다음 속성 유형을 클릭하여 전체 변수 목록을 표시합니다.
    - $, $ 및 $을 포함한 정책 속성
    - $, $ 및 $을 포함한 사용자 속성
    - $, $ 및 $을 포함한 기기 속성
    - **관리 > 속성** 페이지에서 생성되는 사용자 지정 기기/사용자/LDAP 속성
- **푸시 알림 보내기** - 기기가 다시 규정 준수 상태가 되면 푸시 알림을 기기에 전송합니다.
- **둘 다 보내기** - 기기가 다시 규정 준수 상태가 되면 이를 알리는 푸시 알림과 이메일을 각각 기기와 사용자 이메일 주소로 전송합니다. 옵션 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 이메일 보내기 작업 이전에 설명한 자세한 정보를 수신자에게 제공할 수 있습니다.

9. 장치 소유자가 정책 규칙을 위반하는 경우 관리자와 등록된 장치 소유자에게 알리려면 표에서 다음 옵션을 지정하십시오.

| 옵션 | 설명 |
| --- | --- |
| 주제 | 제목 텍스트를 입력하세요. 예를 들면 '정책을 위반했습니다!'라고 입력합니다. |
| 본문 | 필요에 따라 메시지를 입력하세요. 예를 들면 '조치가 필요합니다!'라고 입력합니다. |
| 관리자에게만 이메일 알림을 보냅니다.<br><br>관리자에게 참조<br><br>관리자의 이메일 주소 입력 | 이 옵션은 관리자에게만 이메일 알림을 보내는 경우 선택합니다.<br><br>"관리자에게만 이메일 알림을 보냅니다." 옵션을 선택한 경우에는 이 텍스트 상자를 사용할 수 없습니다.<br><br>관리자의 이메일 ID를 입력하세요. 이메일 주소가 여러 개인 경우 구분 기호로 세미콜론(;)을 입력하세요. |
| 이메일 미리보기 | **이메일 미리보기** 버튼을 누르면 이메일 주소가 보입니다. |

10. **다음**을 클릭하여 정책 세부 정보를 저장합니다.

**기본 조치:**

1. **예** 체크박스를 클릭하여 해당 정책이 이전에 기기에서 트리거된 적이 있는 경우 계층화된 정책을 추가하면 기존에 적용된 정책 및 컴플라이언스 조치를 초기화한다는 사실을 이해했음을 확인합니다. 새 사용자 지정 정책은 다음 기기 체크인 시 적용됩니다. 폐기 조치를 선택한 경우 **예**를 클릭하여 해당 조치를 실행 취소할 수 없다는 사실을 이해했음을 확인합니다.

- **모니터** - 현재는 항상 선택되어 있습니다. 계층화된 컴플라이언스 조치를 이용하려면 Sentry 버전 9.0.0 이상이 필요합니다.
- **아무 것도 하지 않습니다.**
- **알림 보내기**
- **이메일 보내기** - 장치가 규정을 어기면 이를 알리는 이메일을 장치 사용자의 이메일 주소로 보냅니다.
  - 위의 설명과 같이 정책 알림 이메일 템플릿을 사용할 수 있습니다.
  - 선택 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 수신자에게 보다 자세한 정책 위반 사항 및 기타 관련 정보 등을 제공할 수 있습니다. 이는 규정 미준수 기기의 사용자에게 정책 위반에 관한 관련 정보를 제공하여 시정 조치를 취할 수 있도록 합니다. 다음 속성 유형을 클릭하여 전체 변수 목록을 표시합니다.
    - $, $ 및 $을 포함한 정책 속성
    - $, $ 및 $을 포함한 사용자 속성
    - $, $ 및 $을 포함한 기기 속성
    - **관리 > 속성** 페이지에서 생성되는 사용자 지정 기기/사용자/LDAP 속성
- **푸시 알림 보내기** – 기기가 규정을 벗어났음을 알리는 푸시 알림을 기기에 전송합니다.
- **둘 다 보내기** – 기기가 규정을 벗어났음을 알리는 푸시 알림과 이메일을 각각 기기와 사용자 이메일 주소에 전송합니다. 옵션 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 이메일 보내기 작업 이전에 설명한 자세한 정보를 수신자에게 제공할 수 있습니다.
- **Block** - Sentry를 이용해 관리되는 기기의 이메일 및 AppConnect 지원 애플리케이션 액세스를 차단합니다. 차단 작업을 이용하려면 Sentry 버전 9.0.0 이상이 필요합니다.
- **폐기** - 기기를 폐기합니다. **이 작업은 실행 취소할 수 없습니다**. 예를 들어 사용자 활성화 조건을 사용하여 비활성화된 모든 사용자의 기기를 폐기하는 규칙이 있을 수 있습니다.
- **대기** – 기기가 미준수 상태인 경우 지정한 시간(시간 또는 일) 동안 작업을 지연시키면 사용자는 추가 조치를 취하기 전에 위반 사항을 해결할 수 있습니다.

- **격리** – 다음 실행에 따라 앱, 콘텐츠 및 서버 액세스를 제거합니다.

| (선택 사항) 추가 격리 실행 | 설명 |
| --- | --- |
| 관리되는 애플리케이션 격리 | MDM용 Ivanti Neurons 관리형 앱을 기기에서 제거하고 새로운 앱 다운로드 차단 옵션을 활성화하여 앱이 기기에 재설치되지 않도록 차단합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 애플리케이션을**<br>• **지정된 애플리케이션** - 조회하거나 수동으로 하나 이상의 앱을 추가합니다(번들 ID 또는 패키지 이름 사용). **앱 보기** 탭을 클릭하여 추가된 앱 목록을 검토합니다. App Store 액세스 차단 기본 격리 조치는 더 이상 사용할 수 없습니다.<br>특정 기기에서는 특정 기기 제한으로 인해 격리 작업으로 기기에서 애플리케이션을 제거하지 못합니다. |
| 새로운 앱 다운로드 차단 | 기기에 새로운 앱을 다운로드하지 못하도록 차단합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 애플리케이션을**<br>• **지정된 애플리케이션** - 조회하거나 수동으로 하나 이상의 앱을 추가합니다(번들 ID 또는 패키지 이름 사용). **앱 보기** 탭을 클릭하여 추가된 앱 목록을 검토합니다. App Store 액세스 차단 기본 격리 조치는 더 이상 사용할 수 없습니다.<br>이 옵션은 모든 애플리케이션 및 지정된 애플리케이션에 대해 기본적으로 선택되며 선택을 취소할 수 없습니다. 이로써 기기에 앱이 다시 설치되는 것이 차단됩니다. |
| 구성 제거 | 기기에서 MDM용 Ivanti Neurons 구성을 제거합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 구성**<br>• **지정된 구성** - 목록에서 하나 이상의 구성을 선택하거나 검색합니다. **선택한 구성** 탭을 클릭하여 선택한 구성 목록을 검토합니다. |
| 지정된 구성 푸시 | 사용자 지정 규정 준수의 일환으로 지정된 구성을 배포합니다.<br>이 목록에는 다음 기준을 충족하는 구성이 포함되어 있습니다.<br>• 활성화된 구성<br>• 비시스템 구성<br>• 격리 가능한 구성<br>• 현재 공간에 생성되었거나 기본 공간에서 위임된 구성<br>격리 불가능한 구성 목록의 경우에는 격리 불가능한 구성을 참조하십시오.<br>자세한 정보를 보려면 이 절차를 진행한 후 지정된 구성 푸시 섹션을 살펴보십시오. |
| 컨텐츠 제거 | MDM용 Ivanti Neurons에서 배포한 앱과 관련한 모든 콘텐츠 및 미디어를 기기에서 제거합니다. |
| 개인 앱 일시 중지 | 격리된 기기의 개인 공간에서 앱을 일시 중지하여 기능하게 하려면 사용자가 기기에서 컴플라이언스 문제를 해결해야 한다는 점을 나타냅니다. 회사 소유 기기에서 작업 프로필로 프로비저닝된 Android 11+ 기기에서 지원됩니다. |
| **기본 격리 작업** - 해당 작업을 항상 수행합니다. | |

| (선택 사항) 추가 격리 실행 | 설명 |
| --- | --- |
| App Store 액세스 차단 | MDM용 Ivanti Neurons를 통한 기기의 앱 스토어 액세스를 방지합니다. |
| 컨텐츠 스토어 액세스 차단 | MDM용 Ivanti Neurons를 통한 기기의 콘텐츠 스토어 액세스를 방지합니다. |
| AppConnect 차단 | 기기의 AppConnect 기능 사용을 차단합니다. |
| AppTunnel 차단 | AppTunnel을 통한 기기 애플리케이션의 컨텐츠 및 서버 액세스를 차단합니다. |
| ActiveSync 차단 | ActiveSync 서버를 통한 기기의 이메일 액세스를 차단합니다. |

2. **다음**을 클릭하여 어떤 기기에 정책 및 실행을 적용할지 여부를 구성합니다.
3. **완료**를 클릭합니다.

MDM용 Ivanti Neurons가 격리 작업의 시작자일 경우 다양한 Android 기기에 대한 격리 방법이 다음 표에 나와 있습니다.

| 결정합니다. | 격리 방법 |
| --- | --- |
| Go 클라이언트 앱을 통해 기기 관리자 모드인 Samsung 기기 | • 관리되는 공개 앱과 인하우스 앱 모두 제거<br>• 특정 프로필 제거(모바일 위협 방어 및 기타 제외) |
| Go 클라이언트 앱을 통해 기기 관리자 모드인 Samsung 기기가 아닌 기기<br>AppStation 앱을 통한 MAM | • 관리되는 공개 앱과 인하우스 앱 모두에 대해 제거나 숨기기를 지원하지 않음<br>• 특정 프로필 제거(모바일 위협 방어 및 기타 제외) |
| Go 클라이언트 앱을 통한 Android Enterprise | • 관리되는 공개 앱과 인하우스 앱 모두 숨기기<br>• 특정 프로필 제거(모바일 위협 방어 및 기타 제외) |

## 지정된 구성 푸시

사용자 지정 규정 준수의 일환으로 지정된 구성을 배포합니다. 기기가 규정을 벗어날 경우 구성 집합을 배포하기 위한 사용자 지정 정책을 구성합니다. 기기 상태가 규정 미준수에서 규정 준수 상태로 바뀔 경우 해결 조치의 일환으로 기기를 이전 상태로 재설정합니다.

> 관리자가 위임되지 않은 구성이 있는 사용자 지정 정책을 지정된 구성 푸시 탭 아래에 위임하려고 하면 오류가 발생합니다.

다음은 특정 조건에서 사용자 지정 정책을 통해 구성을 푸시할 경우의 동작입니다.

| 조건 | 동작 |
| --- | --- |
| 우선 순위가 설정된 동일한 유형의 두 가지 구성이 선택됩니다. | 우선 순위가 더 높은 구성이 기기로 푸시됩니다. |
| 우선 순위가 설정되지 않은 동일한 유형의 두 가지 구성이 선택됩니다. | 두 가지 구성이 모두 기기에 적용됩니다. 예기치 않은 동작이 발생할 수 있습니다. |
| 사용자 지정 정책에 정의된 우선 순위를 지원하는 동일한 유형의 구성이 이미 기기에 있는 경우 | 사용자 지정 정책에 정의된 구성이 우선적으로 기기로 푸시됩니다. 기기의 기존 구성은 (사용자 지정 정책에 정의된 구성보다 우선 순위가 더 높더라도) 우선 순위에 상관없이 제거됩니다. |
| 사용자 지정 정책에 정의된 우선 순위를 지원하지 않는 동일한 유형의 구성이 이미 기기에 있는 경우 | 사용자 지정 정책에 정의된 구성이 기기로 푸시됩니다. 두 가지 구성이 모두 기기에 존재하게 됩니다. 예기치 않은 동작이 발생할 수 있습니다. |
| 사용자 지정 정책이 만들어진 후 구성 우선 순위가 변경된 경우 | 기기 체크인 시, 사용자 지정 정책의 일부인 경우 우선 순위가 가장 높은 구성이 적용됩니다. |
| 두 조건이 모두 충족되는 경우:<br>• 조건 A: 위반이 있는 기기에 사용자 지정 정책의 일부로 푸시된 구성이 존재했으며, 해당 구성이 기기 상 동일한 유형의 구성보다 우선한 경우.<br>• 조건 B: 위반이 다시 해결되었으며 기기의 격리가 해제된 경우. | 사용자 지정 정책에 정의된 구성이 제거되고 격리 전 장치에 있던 동일한 유형의 구성이 기존 기기 그룹의 애플리케이션을 통해 적용되면서 기기가 원래 상태로 돌아가게 됩니다. |

격리 조치에서 지정된 구성 푸시와 함께 구성 제거를 선택할 경우 다음 규칙에 주의하십시오.

- 모든 구성 제거 + 지정된 구성 푸시: 이 시나리오에서는 기기의 모든 구성이 제거되며 지정된 구성 푸시에서 선택한 구성이 기기로 푸시됩니다.
- 지정된 구성 제거(하나의 사용자 지정 정책에서) + 두 가지 모두 선택 시 공통 구성을 사용하여 지정된 구성(다른 사용자 지정 정책에서) 푸시: 두 가지 다른 규정 준수 정책에서 구성이 선택되기 때문에 가장 제한적인 접근 방식이 취해질 것입니다(예: 구성이 기기에서 삭제됨).

기본 공간에서 사용자 지정 공간으로 사용자 지정 정책을 위임할 수 있습니다. 위임할 사용자 지정 정책을 공간에 위임하는 데 필요한 구성은 지정된 구성 푸시 탭 아래의 사용자 지정 정책에 나와 있습니다.

기기 페이지에서 기기 이름을 클릭하면 기기 상세 정보 페이지로 이동할 수 있습니다. 구성 탭 아래의 구성 방법 열에 기기에 푸시되는 구성의 배포 방법이 나와 있으며 "기기 그룹" 또는 "규정 준수 조치" 중에서 선택할 수 있습니다.

구성 페이지의 MDM용 Ivanti Neurons에는 기기 그룹 및 규정 준수 조치를 통해 각 구성을 수신하는 기기 수가 표시됩니다.

## 조건 설정 이해

다음 표에는 규칙 작성에 사용 가능한 몇 가지 필드가 나와 있습니다.

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| APNS 가능 | 이 필드는 기기가 APNS를 지원하는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS/Android |
| 피싱 방지 기본 상태 | 이 필드에는 피싱 방지 기본 상태가 표시됩니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값<br>:<br>• 활성화 안 됨<br>• 해당 없음<br>• 활성화됨<br>• 알 수 없음 | iOS/Android |
| 피싱 방지 상태 | 이 필드에는 피싱 방지 상태가 표시됩니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 활성화 안 됨<br>• 해당 없음<br>• 활성화됨<br>• 알 수 없음 | iOS/Android |
| 피싱 방지 VPN 상태 | 이 필드에는 피싱 방지 VPN 상태가 표시됩니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 활성화 안 됨<br>• 해당 없음<br>• 활성화됨<br>• 알 수 없음 | iOS/Android |
| 배터리 정보 | 이 필드에는 다음과 같은 속성이 있습니다.<br>• 배터리 수준 - Android OS에서 보고하는 현재 배터리 충전 수준을 표시합니다<br>• 배터리 성능 상태 - Android OS에서 보고하는 상태를 표시합니다 | 가능한 값에 대한 자세한 내용은 고급 검색 사용을 참조하십시오. | 안드로이드 |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | • 배터리 충전 상태 - Android OS에서 보고하는 상태를 표시합니다<br>• 배터리 성능 백분율(OEM별) - Zebra 기기와 같이 지원되는 기기 제조업체의 배터리 성능을 백분율로 표시합니다<br>• 배터리 제조일자(OEM) - Zebra 기기와 같이 지원되는 기기 제조업체의 배터리 제조일자를 표시합니다<br>• 배터리 충전 주기(OEM) - Zebra 기기와 같이 지원되는 기기 제조업체의 완료된 총 주기 수를 표시합니다 | | |
| 베이스밴드 상태 | 이 필드는 기기의 베이스밴드 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 확인 또는 오류입니다. | iOS 27.0+ 감독 모드 기기 |
| 부트스트랩 토큰 사용 가능 | 이 필드는 기기에 대해 부트스트랩 토큰을 사용할 수 있는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | macOS |
| Autopilot 등록됨 | 이 필드는 장치가 Autopilot에 등록되었는지 여부를 나타냅니다. | • 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | Windows |
| Bridge Last Check-in | 이 필드는 클라이언트의 Bridge 마지막 체크인 시간을 나타냅니다. | 가능한 연산자:<br>• 보다 작음<br>• 보다 작거나 같음<br>• 보다 큼<br>• 보다 크거나 같음<br>• 범위에 있음<br>• 범위 내에 없음<br>Bridge 마지막 체크인 시간의 숫자값을 입력하세요.<br>해당 기간에 대해 다음 옵션 중 하나를 선택하십시오.<br>• 시간<br>• 일<br>예: Bridge 마지막 체크인 시간이 12시간 미만입니다. | Windows |
| 카메라 상태 | 이 필드는 기기의 카메라 상태를 나타냅니다. | 가능한 연산자:<br>• 같음 | iOS 27.0+ 감독 모드 기기 |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | | • 같지 않음<br>가능한 값:<br>• 확인<br>• 오류<br>• 비정품(정품 Apple 구성요소가 아닌 경우) | |
| 클라이언트 마지막 체크인 | 이 필드는 클라이언트의 마지막 체크인 시간을 나타냅니다. | 가능한 연산자:<br>• 보다 작음<br>• 보다 큼<br>마지막 체크인 시간의 숫자 값을 입력합니다. 지속 시간에 대한 다음 옵션 중 어느 것이든 선택합니다.<br>• 시간<br>• 일<br>예: 클라이언트 마지막 체크인은 12시간 전 미만입니다. | iOS/macOS/Android |
| 등록된 클라이언트 | 이 필드는 등록된 클라이언트의 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS/Android |
| 손상됨 | 이 필드는 기기가 루팅/손상되었는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 탈옥 또는 루팅<br>• 손상되지 않음 | iOS/Android |
| 현재 국가 이름 | 이 필드는 기기가 현재 연결되어 있음을 알려주는 모바일 국가 코드(MCC) 또는 모바일 네트워크 코드(MNC)에 해당하는 현재 국가의 이름을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 홈 국가 이름을 나타내는 드롭다운 목록 값입니다. | iOS/macOS/Android |
| 현재 MCC | 이 필드는 현재 모바일 국가 코드를 나타냅니다. | 확인할 속성의 값을 입력합니다. 가능한 연산자:<br>• 같음<br>• 같지 않음 | iOS/macOS/Android |
| 현재 MNC | 이 필드는 현재 모바일 네트워크 코드를 나타냅니다. | 확인할 속성의 값을 입력합니다. 가능한 연산자:<br>• 같음<br>• 같지 않음 | iOS/macOS/Android |
| 사용자 지정 기 | 이 필드는 값을 확인하는 규칙 조건으로 기존의 사용자 지정 기기 속성 추가하기 | 확인할 속성의 값을 입력합니다. 가능한 연산자:<br>• 같음 | iOS/macOS/Android/Windows |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| 기 속성 | 를 활성화합니다. | • 같지 않음<br>• 포함<br>• 포함되지 않음<br>값은 공백과 유니코드 문자를 포함한 ASCII 문자로 이루어진 문자열이 될 수 있습니다. | |
| 사용자 지정 LDAP 속성 | 이 필드는 값을 확인하는 규칙 조건으로 기존의 사용자 지정 LDAP 속성 추가하기를 활성화합니다. | 확인할 속성의 값을 입력합니다. 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 포함<br>• 포함되지 않음<br>값은 공백과 유니코드 문자를 포함한 ASCII 문자로 이루어진 문자열이 될 수 있습니다. | iOS/macOS/Android/Windows |
| 사용자 지정 사용자 속성 | 이 필드는 값을 확인하는 규칙 조건으로 기존의 사용자 지정 사용자 속성 추가를 활성화합니다. | 확인할 속성의 값을 입력합니다. 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 포함<br>• 포함되지 않음<br>값은 공백과 유니코드 문자를 포함한 ASCII 문자로 이루어진 문자열이 될 수 있습니다. | iOS/macOS/Android/Windows |
| 데이터 로밍 | 이 필드에서 값을 확인하는 규칙 조건으로 사용할 데이터 로밍을 활성화합니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다.<br>지원 기기가 이 필드에 대한 정보를 보고하지 않으면 기본값은 '아니요'입니다. | iOS/Android |
| 기기 유형 | 이 필드는 기기 모델을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 시작<br>• 끝<br>가능한 값은 텍스트 값입니다. | iOS/macOS/Android/Windows |
| 디바이스 유형 (Apple) | 이 필드는 장치 모델의 듣기 좋은 이름을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 시작<br>• 끝<br>가능한 값은 텍스트 값입니다. | iOS/macOS |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| 디스플레이 상태 | 이 필드는 기기의 디스플레이 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 확인<br>• 오류<br>• 비정품(정품 Apple 구성요소가 아닌 경우) | iOS 27.0+ 감독 모드 기기 |
| 암호화 활성화됨 | 이 필드는 기기에 암호화/데이터 보호가 활성화되었는지 여부를 나타냅니다. | 예 - 기기에서 암호화/데이터 보호가 활성화되었습니다.<br>아니요 - 장치에서 암호화/데이터 보호가 활성화되지 않았습니다. | iOS/Android/Windows |
| GUID | 이 필드는 기기 GUID를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 시작<br>• 끝 | iOS/macOS/Android/Windows |
| Face ID 상태 | 이 필드는 기기의 Face ID 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 확인 또는 오류입니다. | iOS 27.0+ 감독 모드 기기 |
| 주요 국가 이름 | 이 필드는 기기의 SIM 또는 eSIM에 프로그래밍된 모바일 국가 코드(MCC) 또는 모바일 네트워크 코드(MNC)에 해당하는 홈 국가의 이름을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 홈 국가 이름을 나타내는 드롭다운 목록 값입니다. | iOS/Android/Windows |
| Windows 업데이트 실패함 | 이 필드는 기기가 최신 업데이트 규칙 미준수 상태인지 여부 나타냅니다. | 예 - 기기가 최신 업데이트를 준수하지 않습니다.<br>아니요 - 기기가 최신 업데이트를 준수합니다. | Windows |
| 홈 MCC | 이 필드는 자국 모바일 국가 코드를 나타냅니다. | 확인할 속성의 값을 입력합니다. 가능한 연산자:<br>• 같음<br>• 같지 않음 | iOS/macOS/Android |
| 홈 MNC | 이 필드는 자국 모바일 네트워크 코드를 나타냅니다. | 확인할 속성의 값을 입력합니다. 가능한 연산자:<br>• 같음<br>• 같지 않음 | iOS/macOS/Android |
| IMEI | 이 필드는 첫 번째 SIM 슬롯의 IMEI 번호를 나타냅니다. | 가능한 연산자:<br>• 같음 | iOS/Android/Windows |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
|---|---|---|---|
| | | • 같지 않음<br>• 시작<br>• 끝 | |
| IMEI2 | 이 필드는 두 번째 SIM 슬롯의 IMEI 번호를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 시작<br>• 끝 | Android |
| IMSI | 이 필드는 SIM 카드의 IMSI 번호를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 시작<br>• 끝 | Android/Windows |
| 기관 복구 키 활성화됨 | 이 필드는 기기에서 기관 복구 키가 활성화되어 있는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음 | macOS |
| 마지막 체크인 | 이 필드에서는 MDM 채널을 통해 관리되는 기기의 마지막 체크인 시간과 관련된 조건을 설정할 수 있습니다. | 가능한 연산자:<br>• 보다 작음<br>• 보다 큼<br>• 공백임<br>마지막 체크인 시간의 숫자 값을 입력합니다. 지속 시간에 대한 다음 옵션 중 어느 것이든 선택합니다.<br>• 시간<br>• 일<br>예: 마지막 체크인 시간이 12시간 이상 전입니다. | iOS/macOS/Android/Windows |
| 마지막 핫픽스 ID | 이 필드에서는 마지막 핫픽스 ID와 관련된 조건을 설정할 수 있습니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 보다 작음<br>• 보다 작거나 같음<br>• 보다 큼<br>• 보다 크거나 같음<br>• 포함<br>• 포함되지 않음<br>• 시작 | Windows |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | | • 다음으로 시작하지 않음<br>• 끝<br>• 다음으로 끝나지 않음 | |
| 마지막 핫픽스 설치 시간 | 이 필드에서는 마지막으로 설치된 핫픽스와 관련된 조건을 설정할 수 있습니다. | 가능한 연산자:<br>• 보다 작음<br>• 보다 큼 | Windows |
| 로케이터 서비스 활성화됨 | 이 필드는 기기에서 로케이터 서비스(예: Find My iPhone)가 활성화되었는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS |
| 제조업체 | 이 필드에서는 기기 제조업체에 관련한 조건을 설정할 수 있습니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• Samsung<br>• NOKIA<br>• HTC<br>• LGE<br>• Apple Inc | iOS/macOS/Android/Windows |
| MTD 활성화 상태 | 이 필드는 MTD 활성화 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 해당 없음<br>• 오류<br>• 보류 중<br>• 보호됨 | iOS/Android |
| 관리되는 MDM | 이 필드는 기기에서 MDM/기기 관리자가 활성화되었는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS/Android |
| MDM 등록 유형 | 이 필드는 기기의 등록 유형을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값: | iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+ 및 watchOS 27.0+ |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | | • 사용자<br>• 기기<br>• 감독됨<br>• 없음 | |
| MDM 서비스 복귀 | 이 필드는 앱 보존을 통한 MDM 서비스 복귀에 대한 기기 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 True 또는 False입니다. | iOS 27.0+ 및 visionOS 27.0+ |
| 다중 사용자 모드 | 이 필드는 기기(iPad)가 다중 사용자 모드를 사용하는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예 또는 아니요입니다. | iOS 27.0+ |
| 근거리 무선 통신 상태 | 이 필드는 NFC 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 확인 또는 오류입니다. | iOS 27.0+ 감독 모드 기기 |
| OS | 이 필드는 기기의 OS 유형을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• macOS<br>• Android<br>• iOS<br>• Windows<br>• visionOS | iOS/macOS/visionOS/Android/Windows |
| OS 빌드 버전 | 이 필드는 기기의 OS 빌드 버전을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 보다 작음<br>• 보다 작거나 같음<br>• 보다 큼<br>• 보다 크거나 같음<br>• 포함<br>• 포함되지 않음<br>• 시작<br>• 다음으로 시작하지 않음 | iOS/macOS/visionOS/Android/Windows |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | | • 공백이 아님<br>• 공백임<br>• 끝<br>• 다음으로 끝나지 않음 | |
| OS 버전 | 이 필드는 기기의 OS 버전을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 보다 작음<br>• 보다 작거나 같음<br>• 보다 큼<br>• 보다 크거나 같음<br>• 범위에 있음<br>• 범위 내에 없음<br>가능한 값은 텍스트입니다. | iOS/macOS/visionOS/Android/Windows |
| 버전이 있는 OS | 이 필드는 장치의 OS 및 OS 버전을 나타냅니다 | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 보다 작음<br>• 보다 작거나 같음<br>• 보다 큼<br>• 보다 크거나 같음<br>• 범위에 있음<br>• 범위 내에 없음<br>가능한 값은 텍스트입니다. | iOS/macOS/visionOS/Android/Windows |
| 소유권 | 이 필드는 기기의 소유권 유형을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 사용자 소유<br>• 설정되지 않음<br>• 회사 소유 | iOS/macOS/Android/Windows |
| 개인 복구 키 활성화됨 | 이 필드는 개인 복구 키가 활성화되어 있는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음 | macOS |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| 프로필과 호환되는 암호 | 이 필드는 기기의 프로필 암호 준수 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS/Android |
| 개인 핫스팟 활성화됨 | 이 필드는 기기에서 개인 핫스팟 기능이 활성화되었는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다.<br>개인 핫스팟 설정은 특정 통신사에서만 제공합니다. | iOS |
| 전화 번호 | 이 필드는 기기 전화 번호를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 포함<br>• 시작<br>• 끝 | iOS/Android/Windows |
| 공용 IP 주소 | 이 필드는 공용 IP 주소를 나타냅니다. 장치가 VPN 연결 또는 프록시 서버를 사용하여 MDM용 Ivanti Neurons에 연결하는 경우 프록시 WAN IP 주소가 표시됩니다. | 가능한 연산자:<br>• 범위에 있음<br>• 범위 내에 없음<br>• 공백이 아님<br>• 공백임 | Android/ChromeOS |
| 로밍 | 이 필드는 기기의 로밍 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/Android/Windows |
| 보안 잠금 모드 | 이 필드는 기기에서 잠금 모드가 활성화됨 또는 비활성화됨으로 되어 있는지를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 True 또는 False입니다. | iOS 27.0+ 및 macOS 27.0+ |
| Sentry 차단됨 | Sentry의 장치 차단 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS/Android/Windows |
| 상태 | 이 필드는 등록 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>기본값은 '활성'이지만<br>사용자 정의 정책에서는 장치가 활성, 사용 중지 보 | iOS/macOS/Android |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | | 류, 초기화 보류 상태를 체크인할 때 정책 평가가 발생하고 체크인 시 장치의 정책 평가가 이루어지기 때문에 다른 모든 잠재적 값을 제거하여 장치 상태를 활성으로 제한합니다. | |
| 일련 번호 | 이 필드는 기기 일련 번호를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 시작<br>• 끝 | iOS/macOS/Android/Windows |
| 감독됨 | 이 필드는 기기가 감독되는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS |
| 추가 빌드 버전 | 이 필드는 기기의 추가 빌드 버전을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 보다 작음<br>• 보다 작거나 같음<br>• 보다 큼<br>• 보다 크거나 같음<br>• 포함<br>• 포함되지 않음<br>• 시작<br>• 다음으로 시작하지 않음<br>• 끝<br>• 다음으로 끝나지 않음<br>• 공백이 아님<br>• 공백임 | iOS/macOS |
| 추가 OS/버전 기타 | 이 필드는 기기의 추가 OS 빌드 버전을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>• 보다 작음<br>• 보다 작거나 같음<br>• 보다 큼<br>• 보다 크거나 같음<br>• 포함 | iOS/macOS |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | | • 포함되지 않음<br>• 시작<br>• 다음으로 시작하지 않음<br>• 끝<br>• 다음으로 끝나지 않음<br>• 공백이 아님<br>• 공백임 | |
| Touch ID 상태 | 이 필드는 기기의 Touch ID 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값:<br>• 확인<br>• 오류<br>• N/A(iPhone인 경우) | iOS 27.0+ 감독 모드 기기 |
| 사용자 활성화됨 | 이 필드는 사용자가 활성화되었는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS/Android/Windows |
| 사용자 그룹 | 이 필드는 사용자 그룹을 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음 | iOS/macOS/Android/Windows |
| 초광대역 상태 | 이 필드는 기기의 초광대역 상태를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 확인 또는 오류입니다. | iOS 27.0+ 감독 모드 기기 |
| 음성 로밍 | 이 필드는 기기에 음성 로밍이 활성화되었는지 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다.<br>음성 로밍 설정은 특정 통신사에서만 제공합니다.<br>음성 로밍을 비활성화하면 데이터 로밍도 비활성화됩니다.<br>지원 기기가 해당 필드에 관한 정보를 보고하지 않는 경우 기본값이 동일하지 않습니다. | iOS |
| 액세스 차단됨 | Access의 장치 차단 여부를 나타냅니다. | 가능한 연산자:<br>• 같음 | iOS/macOS/Android/Windows |

| UI 필드 | 설명 | 가능한 값 | 지원 플랫폼 |
| --- | --- | --- | --- |
| | | • 같지 않음<br>가능한 값은 예와 아니요입니다. | |
| 컴플라이언스 | 장치의 규정 준수 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 규정 준수함과 규정 준수 안 함 입니다. | iOS/macOS/Android/Windows |
| 정책 준수 활동 차단됨 | 장치의 차단 여부를 나타냅니다. | 가능한 연산자:<br>• 같음<br>• 같지 않음<br>가능한 값은 예와 아니요입니다. | iOS/macOS/Android/Windows |

## 격리 불가능한 구성

다음 표는 격리 불가능한 구성 목록을 보여줍니다.

| OS | 격리 불가능한 구성 |
| --- | --- |
| **Android** | • Android 앱 카탈로그<br>• Android 암호화<br>• Android Enterprise<br>• Android Enterprise 앱<br>• Android Zebra<br>• 피싱 방지 보호<br>• Android 작업 챌린지<br>• 장치 암호<br>• 파일 다운로드<br>• 잠금 및 키오스크: Android 기기 관리 모드<br>• 잠금 및 키오스크: Samsung Knox 표준<br>• MAM 전용<br>• 작업 프로필이 있는 관리되는 기기/회사 소유 기기의 작업 프로필<br>• 업무 관리형 기기(기기 소유자)<br>• Samsung 휴대폰 제한 사항<br>• SafetyNet 인증<br>• 회사 소유 기기의 작업 프로필 |
| **iOS 및 macOS** | • 피싱 방지 보호(iOS)<br>• 앱 알림(iOS)<br>• AppStation 사이트(iOS)<br>• FileVault 복구 키(macOS)<br>• Filevault 2(macOS)<br>• 전역 프록시(iOS 및 tvOS)<br>• 홈 화면 배치(iOS 및 tvOS)<br>• iOS 앱 제어<br>• iOS 제한<br>• iOS 소프트웨어 업데이트(iOS)<br>• macOS 방화벽<br>• macOS 소프트웨어 업데이트<br>• MAM Only(iOS)<br>• MI 클라이언트 개인정보(iOS/macOS)<br>• 네트워크 사용량(iOS)<br>• Office 365 계정 생성(macOS)<br>• 단일 앱 모드(iOS 및 tvOS)<br>• 시스템 정책 제어(macOS) |

| OS | 격리 불가능한 구성 |
| --- | --- |
| | • 시스템 정책 관리(macOS)<br>• 시스템 정책 규칙 옵션(macOS)<br>• 시간 서버(macOS)<br>• 웹 콘텐츠 필터(iOS) |
| **Windows** | • Windows 앱 제어<br>• Windows 제한 DDF(데이터 정의 파일)<br>• Windows 방화벽<br>• Windows 네트워크 프록시<br>• Windows 제한<br>• Windows 업데이트 |
| **모두** | • 활성 디렉토리<br>• 클라이언트 서비스<br>• 모바일 기기 관리<br>• 모바일 위협 방어 활성화<br>• 모바일 위협 방어 로컬 작업<br>• 암호<br>• 개인 정보<br>• 개인 정보 보호 방침<br>• ServiceConnect<br>• 동기화 |

정책 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 기기 관리
- 장치 읽기 전용

# 11.3. 허용 앱 모니터링 및 제어

**라이센스:** Silver

기기에 어떤 앱을 설치할지 제어하려면 허용 앱 정책을 생성합니다. 이 정책은 MIP(MobileIron Packager) 인하우스 macOS 앱도 지원합니다. 이 정책에는 다음 정보가 포함되어 있습니다.

- {{허용 목록 앱}}
- {{차단 목록 앱}}
- {{필수 앱}}
- {{컴플라이언스 조치}}

앱이 필수 목록과 차단 목록에 모두 포함되어 있으면 필수 목록보다 앱 평가가 우선합니다. 예를 들어, 앱 A1이 필수 목록과 차단 목록에 모두 포함되어 있으면 이 기기에 대한 앱 정책 평가는 다음과 같이 동작합니다.

- A1이 기기에 설치되어 있으면 기기가 정책을 준수합니다.
- A1이 기기에 설치되어 있지 않으면 기기가 정책을 준수하지 않습니다.

## 지원되는 기기

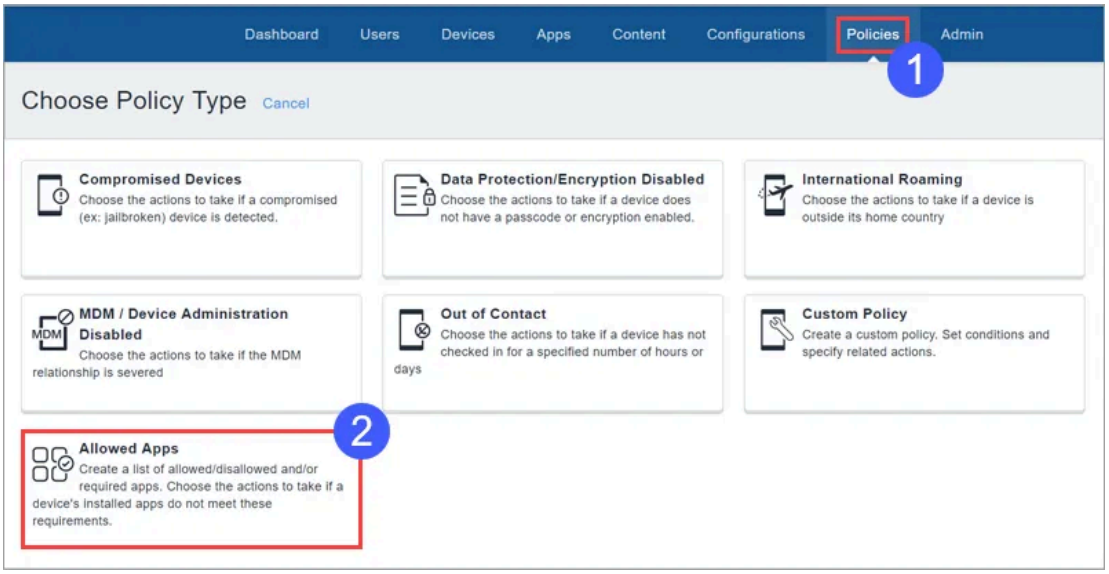
- Android 4.2 또는 지원되는 최신 버전
- iOS 8.0 또는 지원되는 최신 버전
- macOS 10.12 또는 지원되는 최신 버전
- Windows 10 또는 지원되는 최신 버전

**필수 조건**

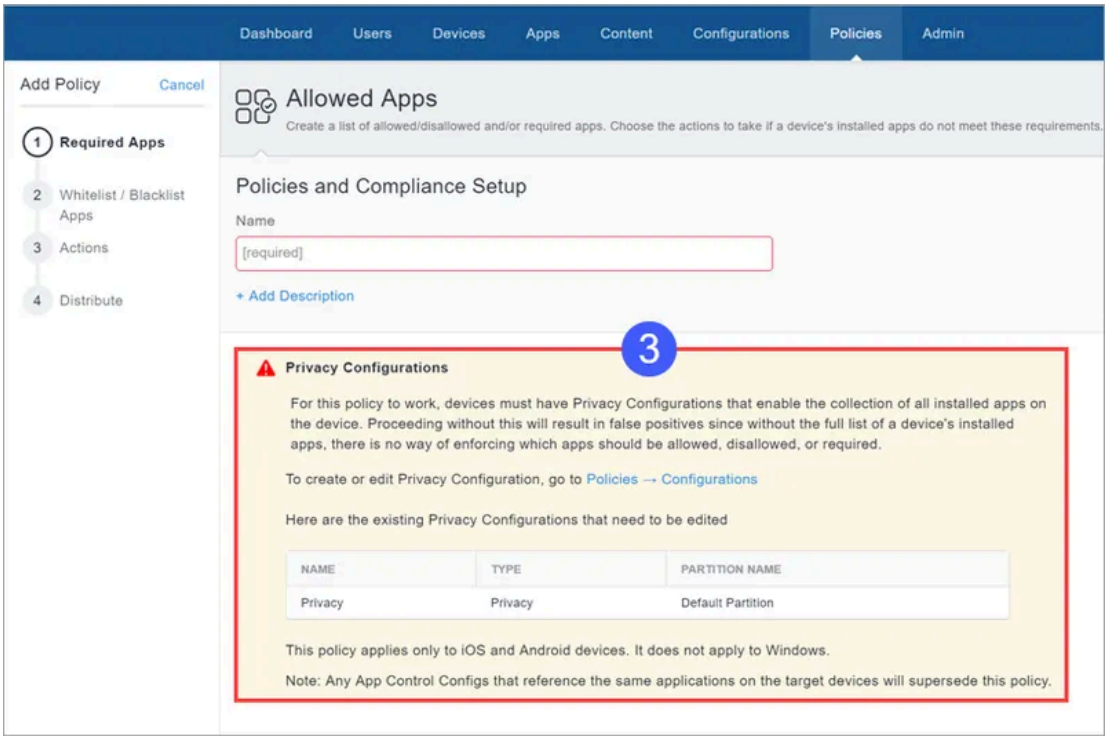
- 허용된 앱 정책이 올바르게 작동하려면 기기에 할당된 개인정보 보호 설정에서 앱 정보 수집을 허용해야 합니다. 허용된 앱 정책을 적용할 기기에 할당된 개인정보 보호 설정을 확인합니다.

어떤 설정이 영향을 받는지 잘 모를 경우:

1. **정책**으로 이동합니다.



**허용된 앱**을 클릭합니다.




3. **정책 구성**에서 편집이 필요한 구성을 확인합니다.
4. **구성**으로 이동합니다.
5. 각각의 메모한 개인정보 보호 설정:
    1. 원하는 구성을 선택하세요.
    2. **편집**을 클릭합니다.
    3. **앱 인벤토리 수집**에서 **기기의 모든 앱**을 선택합니다.
    4. **완료**를 클릭하세요.

# 허용된 앱 정책 생성

### 필수 조건

- Android Enterprise를 활성화하여 Google Play Store에 액세스하고 허용 앱 정책에 새로운 애플리케이션을 추가합니다.

### 절차

1. **정책**으로 이동하여 **+추가**를 클릭합니다.

2. **허용된 앱**을 클릭합니다.

3. **이름** 필드에서 현재 정책의 이름을 입력하세요.
4. **설명** 필드에서 현재 정책의 목적에 관한 간략한 설명을 입력하세요.
5. 다음 탭 중 하나 또는 두 개 모두를 클릭하여 허용 목록 또는 차단 목록에 등록할 앱을 선택합니다.

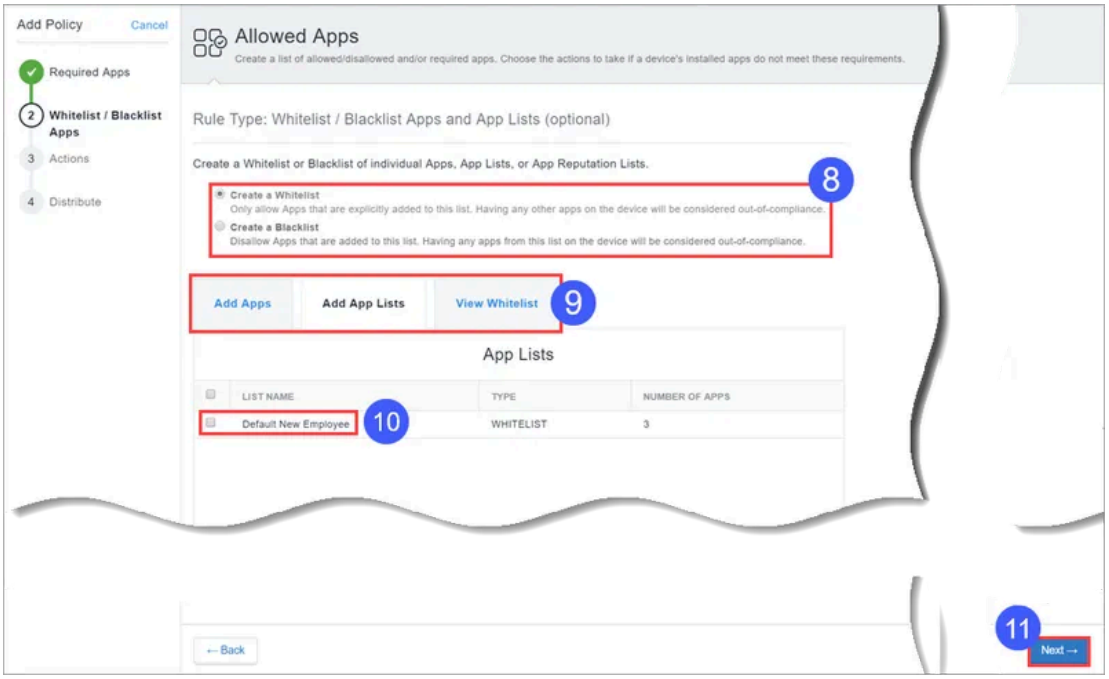
- 조회로 추가를 클릭하여 App Store 또는 App Catalog에서 앱을 검색하고 선택합니다.
  Android Enterprise 활성화를 확인하고 Google Play Store에 액세스합니다.
  
- Android, Windows, iOS, macOS 시스템 앱의 번들 ID를 입력하여 앱을 선택하려면 **수동으로 추가**를 클릭하세요.

**앱 목록 추가** 탭을 선택한 후 원하는 필수 앱 목록을 선택합니다.

6. 결과 필드를 사용하여 필수 앱이나 앱 목록을 선택합니다.
7. **다음**을 클릭합니다.

> **필요한 목록 보기** 탭을 클릭하여 지금까지 선택한 앱 목록을 확인합니다.

8. 만들고자 하는 허용 목록 또는 차단 목록을 선택합니다.



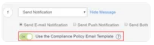

9. **허용 목록/차단 목록 앱 및 앱 목록** 섹션을 이용해 앱 및 앱 목록을 선택합니다.

> 기기에 대한 허용 목록과 차단 목록을 동시에 보유할 수는 없습니다. 허용 목록을 생성하면 다른 모든 앱은 차단 목록으로 등록됩니다.

10. 결과 필드를 사용하여 필수 앱이나 앱 목록을 선택합니다.
    - **앱 목록 추가** 탭을 선택한 후 원하는 앱 목록을 선택합니다.
11. **다음**을 클릭하세요.

> **허용 목록 또는 차단 목록 보기** 탭을 클릭하여 지금까지 선택한 앱 목록을 확인합니다.

12. 기기가 정책을 벗어났을 때 수행할 작업을 선택합니다.

| 작업 | 설정하기 |
| --- | --- |
| **모니터** | 현재는 항상 선택되어 있습니다. 계층화된 컴플라이언스 조치를 이용하려면 Sentry 버전 9.0.0 이상이 필요합니다. |
| 아무것도 안 함 | 기기가 정책을 벗어났을 때 아무런 조치를 취하지 않으려면 선택합니다. |
| **알림 보내기** | |
| 이메일 보내기 | 이메일 보내기를 선택해 기기 사용자의 이메일 주소로 기기가 규정을 벗어났음을 알리는 이메일을 전송합니다.<br>• 여기에서 구성하는 메시지를 구성 중인 정책 알림 이메일 템플릿에 삽입하려면 이메일 템플릿 브랜딩이메일 템플릿 사용자 정의하기에서 설명한 것처럼 **규정 준수 정책 이메일 템플릿 사용** 옵션을 켭니다.개요는 정책 규정 준수 알림 이메일 구성 및 사용을 참조하십시오.<br><br>• 선택 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 수신자에게 보다 자세한 정책 위반 사항 및 기타 관련 정보 등을 제공할 수 있습니다. 이는 규정 미준수 기기의 사용자에게 정책 위반에 관한 관련 정보를 제공하여 시정 조치를 취할 수 있도록 합니다. 다음 속성 유형을 클릭하여 전체 변수 목록을 표시합니다.<br>◦ $, $, $을 포함한 정책 속성.<br>◦ $, $ 및 $을 포함한 사용자 속성<br>◦ $, $ 및 $을 포함한 기기 속성 |
| 푸시 알림 보내기 | 푸시 알림 보내기를 선택해 기기가 규정을 벗어났음을 알리는 푸시 알림을 기기에 전송합니다. |
| 둘 다 보내기 | 기기가 규정을 벗어났음을 알리는 푸시 알림과 이메일을 각각 기기와 사용자 이메일 주소에 전송합니다. 옵션 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 이메일 보내기 작업 이전에 설명한 자세한 정보를 수신자에게 제공할 수 있습니다. |
| **대기**<br><br>**차단**<br><br>**격리**<br><br>**기기가 다시 규정 준수 상태가 되면 알림 보내기** | 선택하여 기기가 미준수 상태인 경우 지정한 시간 동안 작업을 지연시키면 사용자는 추가 조치를 취하기 전에 위반 사항을 해결할 수 있습니다.<br><br>Sentry를 이용해 관리되는 기기의 이메일 및 AppConnect 지원 애플리케이션 액세스를 차단합니다.<br><br>선택하여 다음 표에 따라 앱, 컨텐츠 및 서버 액세스를 제거합니다. 작업이 허용되지 않는 모든 앱을 제거합니다. |
| 이메일 보내기 | 기기가 규정을 벗어났을 때 기기 사용자의 이메일 주소로 이를 알리는 이메일을 전송합니다.<br>• 위의 설명과 같이 정책 알림 이메일 템플릿을 사용할 수 있습니다.<br>• 선택 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 수신자에게 보다 자세한 정책 위반 사항 및 기타 관련 정보 등을 제공할 수 있습니다. 다음 속성 유형을 클릭하여 전체 변수 목록을 표시합니다.<br>◦ $, $ 및 $을 포함한 정책 속성<br>◦ $, $ 및 $을 포함한 사용자 속성<br>◦ $, $ 및 $을 포함한 기기 속성<br>◦ **관리 > 속성** 페이지에서 생성되는 사용자 지정 기기/사용자/LDAP 속성 |
| 푸시 알림 보내기 | 기기가 다시 규정 준수 상태가 되면 기기에 푸시 알림을 보냅니다. |

| 작업 | 설정하기 |
| --- | --- |
| 둘 다 보내기 | 기기가 다시 규정 준수 상태가 되면 이를 알리는 푸시 알림과 이메일을 각각 기기와 사용자 이메일 주소로 전송합니다. 옵션 사항인 대체 변수를 추가하여 메시지를 원하는 대로 바꾸어 이메일 보내기 작업 이전에 설명한 자세한 정보를 수신자에게 제공할 수 있습니다. |

Platinum 라이센스가 있으면 허용 앱 정책은 **계층화된 컴플라이언스 조치**를 지원합니다.

| (선택 사항) 추가 격리 실행 | 설명 |
| --- | --- |
| 관리되는 애플리케이션 격리 | MDM용 Ivanti Neurons 관리형 앱을 기기에서 제거하고 새로운 앱 다운로드 차단 옵션을 활성화하여 앱이 기기에 재설치되지 않도록 차단합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 애플리케이션을**<br>• **지정된 애플리케이션** - 조회하거나 수동으로 하나 이상의 앱을 추가합니다(번들 ID 또는 패키지 이름 사용). **앱 보기** 탭을 클릭하여 추가된 앱 목록을 검토합니다. App Store 액세스 차단 기본 격리 조치는 더 이상 사용할 수 없습니다.<br>특정 기기에서는 특정 기기 제한으로 인해 격리 작업으로 기기에서 애플리케이션을 제거하지 못합니다. |
| 새로운 앱 다운로드 차단 | 기기에 새로운 앱을 다운로드하지 못하도록 차단합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 애플리케이션을**<br>• **지정된 애플리케이션** - 조회하거나 수동으로 하나 이상의 앱을 추가합니다(번들 ID 또는 패키지 이름 사용). **앱 보기** 탭을 클릭하여 추가된 앱 목록을 검토합니다. App Store 액세스 차단 기본 격리 조치는 더 이상 사용할 수 없습니다. |
| 구성 제거 | 기기에서 MDM용 Ivanti Neurons 구성을 제거합니다.<br>다음 옵션 중 하나를 선택합니다.<br>• **모든 구성**<br>• **지정된 구성** - 목록에서 하나 이상의 구성을 선택하거나 검색합니다. **선택한 구성** 탭을 클릭하여 선택한 구성 목록을 검토합니다. |
| 컨텐츠 제거 | MDM용 Ivanti Neurons에서 배포한 앱과 관련한 모든 콘텐츠 및 미디어를 기기에서 제거합니다. |
| 개인 앱 일시 중지 | 격리된 기기의 개인 공간에서 앱을 일시 중지하여 기능하게 하려면 사용자가 기기에서 컴플라이언스 문제를 해결해야 한다는 점을 나타냅니다. 회사 소유 기기에서 작업 프로필로 프로비저닝된 Android 11+ 기기에서 지원됩니다. |
| **기본 격리 작업** - 해당 작업을 항상 수행합니다. | |
| App Store 액세스 차단 | MDM용 Ivanti Neurons를 통한 기기의 앱 스토어 액세스를 방지합니다. |
| 컨텐츠 스토어 액세스 차단 | MDM용 Ivanti Neurons를 통한 기기의 콘텐츠 스토어 액세스를 방지합니다. |
| AppConnect 차단 | 기기의 AppConnect 기능 사용을 차단합니다. |
| AppTunnel 차단 | AppTunnel을 통한 기기 애플리케이션의 컨텐츠 및 서버 액세스를 차단합니다. |
| ActiveSync 차단 | ActiveSync 서버를 통한 기기의 이메일 액세스를 차단합니다. |

**다음**을 클릭하세요.

14. 배포를 구성합니다.

15. **완료**를 클릭하세요.

허용 앱 정책에 더 높거나 낮은 우선순위를 설정하는 것과 관련한 자세한 내용은 **정책 우선순위 지정**을 참조하십시오.

# 11.4. 정책 우선순위 지정

허용된 앱 정책은 구성과 유사한 우선순위를 지원합니다. 우선순위를 사용하여 동일한 유형의 어떤 정책이 여러 기기 그룹으로 배포되는지, 그리고 동일한 기기가 여러 기기 그룹에 나타나는 사례를 결정합니다. 예를 들어, 정책 우선순위는 다음과 같은 경우에 정책 배포를 결정하는 데 유용합니다.

- "필수 앱 A"는 기기 그룹 1로 배포해야 하고,
- "필수 앱 B"는 기기 그룹 2로 배포해야 하며,
- 사용자의 기기는 두 기기 그룹 모두의 구성원입니다.

다음과 같이 정책의 우선순위를 지정할 수 있습니다.

1. **정책 > 정책 & 규정 준수**로 이동합니다.
2. **작업 > 정책 우선순위 지정**을 선택합니다. **작업**이 표시되지 않으면, 우선 순위 지정이 필요한 여러 정책이 존재하지 않는 것입니다.
3. 화살표를 사용하여 높은 것(상단)에서 낮은 것(하단) 순으로 우선 순위를 목록화합니다. 잠금 아이콘은 정책 내의 모든 기기 배포 설정을 편집해야 정책의 우선순위를 변경할 수 있다는 것을 의미합니다.
4. **저장**을 클릭하세요.

# 11.5. Windows 하드웨어 정책

Couldn't convert your doc.

# 12. 관리

관리 섹션은 MDM용 Ivanti Neurons 포털에서 사용자, 기기, 구성을 관리하는 데 도움이 됩니다. 다음 섹션에는 관리자로서 수행할 수 있는 모든 작업 목록이 포함되어 있습니다.

- 시스템
- 인프라
- 설정(Apple)
- Windows 기기 사용 작업
- Microsoft Azure 설정
- Google Apps와 연결
- ChromeOS 장치 작업
- 펌웨어 관리
- 테넌트 정지
- 스크립트 및 파일 관리
- 브랜딩
- 비 iOS 기기 관리 추가

# 12.1. 시스템

이 섹션에는 다음 주제가 포함됩니다.

- 속성
- 장치 정리 설정
- GDPR 프로필
- 알림 이메일
- 역할 관리
- 공간
- 지원 관리자
- 관리 > 시스템 사용 알림

# 12.1.1. 속성

속성 페이지에서 다음과 같은 작업을 진행할 수 있습니다.

- 사용자, 장치, 앱에 대해 기록할 수 있는 정보 유형을 관리합니다.
- MDM용 Ivanti Neurons에서 추적하는 정보의 표준 유형을 확인합니다.

사용자 지정 사용자 속성에는 부서 또는 내부 ID와 같은 정보가 포함됩니다. 각 속성에는 해당하는 변수가 있으며, 이를 사용하여 그룹을 구축하거나 구성을 배포할 수 있습니다.

> 사용자 규칙 그룹 기준을 만드는 동안 고객 속성이 숫자 값을 가질 경우 MDM용 Ivanti Neurons은(는) 정수 연산을 지원하지 않습니다.

## 사용자 지정 속성 만들기

MDM용 Ivanti Neurons 관리 포털에서 사용자 지정 속성을 생성할 수 있습니다.

**절차**

1. 관리 포털에 로그인합니다.
2. **관리** > **시스템** > **속성**으로 이동합니다.
3. **사용자 지정 속성**에 있는 **+추가**를 클릭합니다.
4. **속성 이름** 필드에 속성을 나타내는 텍스트를 입력합니다.

> 입력하는 내용은 **사용** 필드에 해당 변수를 생성하는 데 사용됩니다.

다음 **속성 유형** 옵션에서 속성 유형을 선택합니다.

   - **사용자**
   - **기기**
   - **앱**
   - **IDP**(자세한 내용은 **SCIM을 사용한 사용자 프로비저닝** 또는 **Entra ID 사용자 소스로 MDM용 Ivanti Neurons 연결** 참조)

속성 유형이 장치인 경우 다음 **데이터 유형** 옵션 중 하나를 선택합니다.

   - **숫자**
   - **텍스트**

7. **속성 보존**(선택 사항): 이 옵션은 속성 유형이 **기기**인 경우에만 사용할 수 있습니다. 기기에서 지우기/폐기 작업이 수행되더라도 사용자 정의 속성을 유지하려면 이 옵션을 선택합니다.
8. **추가**를 클릭합니다.
   생성된 사용자 지정 사용자 속성은 속성 페이지의 **관리자가 추가됨** 섹션에 표시됩니다.

> 사용자 지정 속성 조합 $ + $ + $ + ${Static String}이(가) 어떤 순서로든 지원됩니다.

## 사용자 지정 속성 이름 변경

사용자 지정 속성의 이름을 변경하면 다음 항목에서 사용되는 해당 사용자 지정 속성에 대한 모든 참조의 이름이 변경됩니다.

- 사용자 지정 정책
- 사용자 그룹
- 기기 그룹
- 앱 배포 필터
- 공간

> 구성, 초대 이메일 템플릿, 정책 규정 준수 조치의 이메일 및 푸시 메시지 등 다른 항목에 있는 사용자 지정 속성의 참조는 업데이트되지 않습니다.

**절차**

1. **관리자가 추가됨** 아래에서 이름을 변경할 속성 옆의 **+편집**을 클릭합니다.
2. **속성 이름** 필드에 속성을 나타내는 새 이름을 입력합니다.

> 입력하는 내용은 **사용** 필드에 해당 변수를 생성하는 데 사용됩니다.

**저장**을 클릭하세요.

## 사용자 지정 속성 삭제

사용자 지정 속성을 삭제하면 연결된 모든 사용자 또는 기기에서 해당 값이 제거됩니다. 이 작업은 번복할 수 없습니다.

사용자 지정 속성은 다음 항목에서 사용되지 않는 경우에 삭제할 수 있습니다.

- 사용자 지정 정책
- 사용자 그룹
- 기기 그룹
- 앱 배포 필터
- 공간

사용자 지정 속성을 삭제하기 전에 엔터티에서 사용자 지정 속성을 제거하십시오.

삭제하려는 속성 안에 위 항목에 대한 참조가 없는 경우에는 속성 옆의 **삭제**를 클릭하면 작업을 확인하는 팝업 창이 표시됩니다. 작업을 확인하고 **삭제**를 클릭합니다.

> 다음 사용자 지정 속성의 필드 이름은 해당 규칙 빌더에서 정렬됩니다.

- 사용자 지정 LDAP 속성
- 사용자 지정 사용자 속성
- 사용자 지정 기기 속성
- 사용자 지정 IdP 속성
- 사용자 지정 앱 속성

## 시스템 속성 보기

시스템 속성은 구성에서 변수로 사용할 수 있도록 사전 정의된 속성입니다. 전체 목록은 **관리자** > **시스템** > **속성** 페이지의 **시스템 속성** 섹션에서 확인할 수 있습니다. 시스템 속성은 다음 유형의 속성을 포함하고 있습니다.

- 사용자 속성
- 기기 속성
- 이메일 템플릿 속성
- 시스템 속성
- 타임스탬프 속성
- Entra ID 사용자 지정 사용자 속성
- 정책 속성

## 사용자 속성

사용자 속성을 사용하여 사용자에 대한 정보를 지정합니다.

| 키 | 설명 |
| --- | --- |
| $ | 부서 속성(Entra ID 필요) |
| $ | 전자 데이터 교환-개인 식별자 |
| $ | 사용자의 관리되는 Apple ID |
| $ | sAMAccountName 속성(Active Directory 필요) |
| $ | 고유 이름에서 추출된 공통 이름(CN) 속성(LDAP 필요) |
| $ | 표시 이름 |
| $ | 고유 이름(LDAP 필요) |
| $ | 이메일 주소의 도메인 부분('@' 이후 부분) |
| $> | 이메일 주소의 로컬 부분('@' 이전 부분) |
| $ | 이메일 주소 |
| $ | 이름 |
| $ | 성 |
| $ | 로캘 |
| $ | 고유 이름에서 추출된 조직 단위(OU) 속성(LDAP 필요) |
| $ | Kerberos 영역 정보(Active Directory 필요) |
| $ | 로그인 ID의 도메인 부분('@' 이후 부분) |
| $ | 로그인 ID의 로컬 부분('@' 이전 부분) |
| $ | 로그인 ID(이메일 주소 형식) |
| $ | userPrincipalName 속성(Active Directory 필요) |

## 기기 속성

사용자 속성을 사용하여 모바일 기기에 대한 정보를 지정합니다.

| 키 | 설명 |
| --- | --- |
| $ | 클라이언트가 마지막으로 체크인한 날짜(가장 최근 체크인 - MDM 또는 클라이언트) |
| $ | 대체 일련 번호 |
| $ | 클라이언트 애플리케이션에 사용하는 식별자 |
| $ | 전역 고유 기기 식별자 |
| $ | ICCID |
| $ | IMEI2 |
| $ | IMEI |
| $ | IMSI |
| $ | 기기가 마지막으로 체크인된 날짜(가장 최근 체크인 - MDM 또는 클라이언트) |
| $ | 내부 기기 식별자 |
| $ | MDM에 사용되는 식별자 |
| $ | MEID |
| $ | 모델 |
| $ | 기기 이름 |
| $ | 기기 전화 번호 |
| $ | 클러스터 고유 기기 식별자 |
| $ | 일련번호 |
| $ | iOS UDID |
| $ | Wi-Fi MAC 주소 |
|  | 전화 번호 2 |
|  | ICCID 2 |

사용자 지정 특성을 만들고 관리 앱 구성에서 이 특성을 참조할 경우 특성 값이 업데이트되면 관리 앱 구성에서 참조된 특성 또한 업데이트되며, 관리 앱 구성이 장치로 다시 푸시됩니다.

사용자 지정 또는 장치 속성이 업데이트되고 구성이 장치로 푸시되면 Android 키오스크 브랜딩 구성도 업데이트되어야 합니다.

## 앱 속성

앱 속성을 사용하여 애플리케이션에 대한 정보를 지정하고 사용자 지정 애플리케이션 그룹을 만듭니다.

| 키 | 설명 |
| --- | --- |
| $ | AppCatalog에 날짜 애플리케이션이 추가되었습니다 |
| $ | 애플리케이션 이름 |
| $ | 애플리케이션 운영 체제 |
| $ | 애플리케이션 번들 또는 패키지 ID |
| $ | 애플리케이션을 가져온 소스를 설명합니다 |
| $ | iOS 또는 macOS 애플리케이션이 VPP인지 여부를 설명합니다 |

## 이메일 템플릿 속성

| 키 | 설명 |
| --- | --- |
| $ | 이메일 본문 |
| $ | 이메일 제목 |

## 타임스탬프 속성

| 변수 키 | 설명 |
| --- | --- |
| $ | 현재 타임스탬프(Epoch 이후 밀리초) |

## 정책 템플릿 속성

| 키 | 설명 |
| --- | --- |
| $ | 정책 이름 위반 |
| $ | 메시지를 보낸 후 수행할 다음 계층화된 규정 준수 작업(대기 및 사용 중지와 다름) |
| $ | 기기가 비준수 상태였던 기간(일) |
| $ | 정책 위반이 처음 트리거된 타임스탬프(UTC DD-MM-YYYY 형식) |
| $ | 규칙 정의(지금 표시되는 쿼리 문자열) |

**관련 주제:**

- 사용자에게 사용자 지정 속성 할당
- 장치에 사용자 지정 속성 할당
- 사용자에게서 사용자 지정 속성 제거
- 장치에서 사용자 지정 속성 제거
- 변수

# 12.1.2. 장치 정리 설정

장치 정리는 미사용 장치에 대한 장치 수명 주기를 자동화합니다. 지정한 일 수 동안 연결되지 않은 장치를 사용 중지할 수 있습니다. 지정한 일 수 동안 사용 중지된 장치를 삭제할 수 있습니다. 감사 추적 페이지는 기기 사용 중지, 기기 삭제 및 지워진 기기 삭제 설정을 캡처합니다.

다음 표는 장치 정리 설정을 지원하는 Android 장치에 대한 정보를 제공합니다.

| 모드 | 규정 미준수 시 사용 중지 | 사용 중지 삭제 | 강제 중지 또는 중지 보류 중 | 지워짐 삭제 | 지우기 보류 삭제 |
|---|---|---|---|---|---|
| Android 직장 프로필(프로필 소유자) | 예 | 예 | 예 | 아니요 | 아니요 |
| 기기 관리자/회사 소유 기기의 작업 프로필 | 예 | 예 | 예 | 예 | 예 |
| 업무 관리형 기기/작업 프로필이 있는 Android 관리형 기기 | 아니요 | 아니요 | 아니요 | 예 | 예 |

**필수 조건**

이 설정에 액세스하려면 시스템 관리 역할 권한이 있어야 합니다.

## 장치 사용 중지

**절차**

1. **관리 > 시스템 > 장치 정리**로 이동합니다. 장치 정리 페이지가 열립니다.
2. **기기 사용 중지**를 선택합니다.
3. **장치 사용 중지** 테이블을 사용하여 세부 정보를 지정합니다.
4. **체크인되지 않은 장치 목록 표시**를 클릭합니다. 지정된 일 수 동안 체크인하지 않은 장치 목록을 표시합니다.
5. **지금 기기 사용 중지**를 클릭하거나 기기 사용 중지를 예약할 수 있습니다.
6. **MDM용 Ivanti Neurons** 관리 포털은 지정된 장치를 사용 중지합니다.
7. **저장**을 클릭하여 설정을 저장합니다.
8. (선택 사항) 값을 업데이트하는 경우 **재설정**을 클릭하여 설정을 초기 설정으로 다시 재설정할 수 있습니다.

### 장치 사용 중지

| 필드 | 설명 |
| --- | --- |
| **플랫폼 선택** | 기기 정리 설정을 적용할 플랫폼을 선택합니다. 현재 이 옵션은 **기기 폐기** 및 **폐기 보류 중인 기기 폐기** 설정에서만 사용할 수 있습니다. |
| **(일) 넘게 체크인되지 않은 기기 사용 중지** | 일수: 기본값은 30일이고, 최대 허용 일수는 365일입니다. |
| **각 세션에서 사용 중지할 최대 장치 수** | 100, 500 또는 1000을 선택합니다(기본값: 100). |
| **일정에 따라 기기 자동 사용 중지** | 미리 설정된 일정에 따라 기기를 사용 중지하려면 확인란을 선택합니다. |
| **일정 구성 사용 중지** | 사용 중지 빈도를 설정하려면 다음 옵션 중 하나를 선택하십시오.<br>• **매일** - 기기를 매일 사용 중지하도록 설정합니다.<br>• **매주** - 사용 중지를 예약할 요일을 지정합니다.<br>• **매월** - 매월 1일에 기기를 사용 중지하도록 설정합니다. |

# 사용 중지된 기기 삭제

**절차**

1. **관리** > **시스템** > **장치 정리**로 이동합니다. 장치 정리 페이지가 열립니다.
2. **사용 중지된 기기 삭제**를 선택합니다.
3. **사용 중지된 기기 삭제** 테이블을 사용하여 세부 정보를 지정합니다.
4. **사용 중지된 장치 목록 표시**를 클릭합니다. 지정된 일수 동안 사용 중지된 장치의 목록을 표시합니다.
5. **지금 사용 중지된 기기 삭제**를 클릭하거나 기기 삭제를 예약할 수 있습니다.
6. MDM용 Ivanti Neurons 관리 포털은 지정된 장치를 삭제합니다.
7. **저장**을 클릭하여 설정을 저장합니다.
8. (선택 사항) 값을 업데이트하는 경우 **재설정**을 클릭하여 설정을 초기 설정으로 다시 재설정할 수 있습니다.

## 사용 중지된 기기 삭제

| 필드 | 설명 |
| --- | --- |
| **(일) 넘게 사용 중지된 장치 삭제** | 일수: 기본값은 30일이고, 최대 허용 일수는 365일입니다. |
| **각 세션에서 삭제할 사용 중지된 최대 장치 수** | 100, 500 또는 1000을 선택합니다(기본값: 100) |
| **일정에 따라 사용 중지된 기기 자동 삭제** | 미리 설정된 일정에 따라 기기를 사용 중지하려면 확인란을 선택합니다. |
| **일정 구성 삭제** | 삭제 빈도를 설정하려면 다음 옵션 중 하나를 선택하십시오.<br>• **매일** - 기기를 매일 삭제하도록 설정합니다.<br>• **매주** - 삭제를 예약할 요일을 지정합니다.<br>• **매월** - 매월 1일에 사용 중지된 기기를 삭제하도록 설정합니다. |

## 지워진 기기 삭제

**절차**

1. **관리** > **시스템** > **장치 정리**로 이동합니다. 장치 정리 페이지가 열립니다.
2. **지워진 기기 삭제**를 선택합니다.
3. **지워진 기기 삭제** 테이블을 사용하여 세부정보를 지정합니다.
4. **지워진 기기 목록 표시**를 클릭합니다. 지정된 일수 동안 사용 중지된 장치의 목록을 표시합니다.
5. **지금 지워진 기기 삭제**를 클릭하거나 지워진 기기 삭제를 예약할 수 있습니다.
6. MDM용 Ivanti Neurons 관리 포털은 지정된 장치를 삭제합니다.
7. **저장**을 클릭하여 설정을 저장합니다.
8. (선택 사항) 값을 업데이트하는 경우 **재설정**을 클릭하여 설정을 초기 설정으로 다시 재설정할 수 있습니다.

### 지워진 기기 삭제

| 필드 | 설명 |
| --- | --- |
| **(일) 넘게 지워진 기기 삭제** | 일수: 기본값은 30일이고, 최대 허용 일수는 365일입니다. |
| **각 세션에서 최대 삭제할 수 있는 지워진 기기 수** | 100, 500 또는 1000을 선택합니다(기본값: 100) |
| **일정에 따라 지워진 기기 자동 삭제** | 미리 설정된 일정에 따라 지워진 기기를 삭제하려면 이 확인란을 선택합니다. |
| **지워진 일정 구성 삭제** | 삭제 빈도를 설정하려면 다음 옵션 중 하나를 선택하십시오.<br>• **매일** - 지워진 기기를 매일 삭제하도록 설정합니다.<br>• **매주** - 삭제를 예약할 요일을 지정합니다.<br>• **매월** - 매월 1일에 지워진 기기를 삭제하도록 설정합니다. |

# 지우기 보류 중인 기기 삭제

**절차**

1. **관리** > **시스템** > **장치 정리**로 이동합니다. 장치 정리 페이지가 열립니다.
2. **지우기 보류 중인 기기 삭제**를 선택합니다.
3. **지우기 보류 중인 기기 삭제** 테이블을 사용하여 세부 정보를 지정합니다.
4. **지우기 보류 중인 기기 목록 표시**를 클릭합니다. 지정된 일 수 동안 지울 예정인 기기 목록을 표시합니다.
5. **지금 지우기 보류 중인 기기 삭제**를 클릭하거나 지우기 보류 중인 기기의 삭제를 예약할 수 있습니다.
6. MDM용 Ivanti Neurons 관리 포털은 지정된 장치를 삭제합니다.
7. **저장**을 클릭하여 설정을 저장합니다.
8. (선택 사항) 값을 업데이트하는 경우 **재설정**을 클릭하여 설정을 초기 설정으로 다시 재설정할 수 있습니다.

### 지우기 보류 중인 기기 삭제

| 필드 | 설명 |
| --- | --- |
| **(일) 넘게 지우기 보류 중인 기기 삭제** | 일수: 기본값은 30일이고, 최대 허용 일수는 365일입니다. |
| **지우기 보류 중인 기기를 각 세션에서 삭제할 수 있는 최대 수** | 100, 500 또는 1000을 선택합니다(기본값: 100) |
| **일정에 따라 지우기 보류 중인 기기 자동 삭제** | 미리 설정된 일정에 따라 지워진 기기를 삭제하려면 이 확인란을 선택합니다. |
| **지우기 보류 중인 일정 구성 삭제** | 삭제 빈도를 설정하려면 다음 옵션 중 하나를 선택하십시오.<br>• **매일** - 지우기 보류 중인 기기를 매일 삭제하도록 설정합니다.<br>• **매주** - 삭제를 예약할 요일을 지정합니다.<br>• **매월** - 매월 1일에 지우기 보류 중인 기기를 삭제하도록 설정합니다. |

# 사용 중지 보류 중인 기기 사용 중지

**절차**

1. **관리** > **시스템** > **장치 정리**로 이동합니다. 장치 정리 페이지가 열립니다.
2. **사용 중지 보류 중인 기기 사용 중지**를 선택합니다.
3. **사용 중지 보류 중인 기기 삭제** 테이블을 사용하여 세부 정보를 지정합니다.
4. **사용 중지 보류 중인 기기 목록 표시**를 클릭합니다. 지정된 일 수 동안 사용 중지 예정인 기기 목록을 표시합니다.
5. **사용 중지 보류 중인 기기를 지금 강제 사용 중지**를 클릭하거나 보류 중인 기기의 사용 중지 일정을 정할 수 있습니다.
6. MDM용 Ivanti Neurons 관리 포털은 지정된 장치를 사용 중지합니다.
7. **저장**을 클릭하여 설정을 저장합니다.
8. (선택 사항) 값을 업데이트하는 경우 **재설정**을 클릭하여 설정을 초기 설정으로 다시 재설정할 수 있습니다.

## 사용 중지 보류 중인 기기 사용 중지

| 필드 | 설명 |
| --- | --- |
| **(일) 넘게 체크인하지 않은 사용 중지 보류 상태의 기기 사용 중지** | 일수: 기본값은 30일이고, 최대 허용 일수는 365일입니다. |
| **각 세션에서 사용 중지할 최대 사용 중지 보류 상태의 기기 수** | 100, 500 또는 1000을 선택합니다(기본값: 100) |
| **일정에 따라 사용 중지 보류 중인 기기 자동 사용 중지** | 미리 설정된 일정에 따라 사용 중지 보류 중인 기기를 사용 중지하려면 확인란을 선택합니다. |
| **사용 중지 보류 중인 일정 구성 사용 중지** | 삭제 빈도를 설정하려면 다음 옵션 중 하나를 선택하십시오.<br>• **매일** - 보류 중인 기기를 매일 사용 중지하도록 설정합니다.<br>• **매주** - 보류 중인 기기의 사용 중지를 예약할 요일을 지정합니다.<br>• **매월** - 매월 1일에 보류 중인 기기를 사용 중지하도록 설정합니다. |

기기가 폐기되고 체크인이 오래 전에 이루어진 경우, 마지막 체크인 시간이 기기 삭제를 결정하는 데 사용됩니다. 예를 들어, 기기가 마지막으로 30일 전에 체크인되었고, 오늘 기기가 폐기된 경우('(일) 넘게 체크인되지 않은 기기 사용 중지' 옵션으로 인해 발생했을 수 있음)' 및 '(일) 넘게 사용 중지된 기기 삭제'가 30일로 설정된 경우, 기기는 '사용 중지된 기기 삭제' 작업이 실행되는 즉시 삭제됩니다.

# 12.1.3. GDPR 프로필

이제 MDM용 Ivanti Neurons 관리 포털에 GDPR 프로필 페이지가 포함되어 사용자 그룹에 GDPR 프로필을 할당할 수 있습니다. GDPR 프로필은 개별 사용자가 아닌 사용자 그룹에만 할당할 수 있습니다.

참고:

- 특정 사용자 그룹에 할당하려면 먼저 GDPR 프로필을 활성화해야 합니다.
- GDPR 프로필을 비활성화할 경우 사용자 그룹에 이미 할당된 프로필 제한이 모두 풀립니다.
- GDPR 프로필을 활성화한 후 일부 필드의 편집 기능이 제한되거나 비활성화됩니다.

## GDPR 프로필 할당 후 숨겨진 필드

사용자에게 GDPR 프로필이 있는 경우 사용자 정보를 표시할 때 MDM용 Ivanti Neurons에서 다음 필드를 기본적으로 숨깁니다.

- **사용자 ID**
- **사용자 이름**
- **이메일 주소**
- **일련 번호**
- **ICCID**
- **IMSI**
- **MEID**
- **IP 주소**
- **전화번호**
- **IMEI**
- **eSIM 식별자**
- **위치**

> 위치가GDPR프로필에 추가되면 장치 위치 필드 마지막 위치, 위도 및 경도가 GDPR 프로필에 할당된 사용자의 장치 세부 정보에서 마스킹됩니다.

## GDPR 프로필 활성화

GDPR 프로필을 활성화하고 MDM용 Ivanti Neurons 관리 포털과 기기에서 숨겨야 하는 필드를 선택할 수 있습니다.

**Procedure절차**

| | | |
|---|---|---|
| | 1. | **MDM용 Ivanti Neurons 관리 포털로 로그인합니다.** |
| | 2. | **관리 > 시스템 > GDPR 프로필로 이동합니다.** |
| | 3. | **활성화를 클릭합니다.** |

| | |
|---|---|
| 4. | 편집(연필) 아이콘을 클릭합니다. |

| | |
|---|---|
| 5. | 숨겨야 하는 필드를 선택합니다. |

| |
|---|
| 6. 저장을 클릭합니다. 선택한 필드가 마스킹 처리되고 해당 사용자의 값으로 표시되지 않습니다. |

## 사용자 그룹에 GDPR 프로필 할당

GDPR 프로필을 활성화한 후 특정 사용자 그룹에 할당할 수 있습니다.

**Procedure절차**

| | | |
|---|---|---|
| | 1. | MDM용 Ivanti Neurons 관리 포털로 로그인합니다. |

| | |
|---|---|
| | 2. 사용자 > 사용자 그룹으로 이동합니다. |

| | |
|---|---|
| 3. | 목록에서 사용자 그룹을 선택합니다. |

| | |
|---|---|
| 4. | 작업 드롭다운 목록을 클릭하고 **GDPR 프로필 할당**을 선택합니다. GDPR 프로필이 해당 그룹의 모든 사용자에게 할당되고 선택한 모든 값이 마스킹 처리되어 관리 포털과 사용자 기기에서 보이지 않습니다.<br><br>모든 사용자 그룹에는 관리자도 포함되므로 GDPR 프로필을 모든 사용자 그룹에 할당하지 마십시오. |

# 12.1.4. 알림 이메일

라이센스: Silver

알림의 심각도에 따라 이메일 알림을 받아야 하는 사용자의 이메일 주소 목록을 구성할 수 있습니다.

알림 이메일 기능은 선택사항이며 필요할 때 이 기능을 켜고 끌 수 있습니다. 시스템 관리 역할을 지정 받은 사람만 이 기능을 사용할 수 있습니다.

1. **관리 > 시스템 > 알림 이메일**을 선택합니다. **알림 이메일** 페이지가 표시됩니다.
2. 알림 이메일 설정 섹션에서 **켜기**를 클릭하여 알림 이메일 기능을 활성화합니다.
3. **수신자 추가**를 클릭합니다. **수신자 추가** 팝업 창이 표시됩니다.
4. **수신자 추가** 팝업 창에서 다음 필드를 업데이트합니다.
    - 수신자 이메일 ID – 알림을 받아야 할 수신자의 이메일 ID를 입력합니다.
    - 보낼 알림 유형 – 체크박스를 선택하여 알림 유형을 선택합니다. 알림 유형 옵션은 다음과 같습니다. **위험 알림**, **경고 알림**, **정보 알림**.
5. **확인**을 클릭합니다. 설정 상세 정보가 표에 표시됩니다.
6. 변경 사항을 적용하려면 **저장**을 클릭합니다.

# 12.1.5. 역할 관리

역할은 특정 기능 영역 제어에 대한 액세스를 제한하면서 관리자 역할을 하는 사용자에게 일련의 권한을 허용하는 패키지 형태의 권한 그룹입니다. MDM용 Ivanti Neurons는 할당(또는 편집)할 수 있는 일련의 시스템 역할과 사용자 지정 역할을 생성하는 기능을 제공합니다. 카테고리를 기준으로 특정 권한을 검색할 수 있으며, UI 내 특정 역할 또는 권한과 관련된 모든 옵션이 표시됩니다. 종속 권한으로서 추가되는 권한에 대한 툴팁이 표시됩니다.

> 역할 관리 페이지 및 관련 옵션은 UEM용 Ivanti Neurons 및 MDM용 Ivanti Neurons에 모두 액세스할 수 있는 컨버지드 테넌트에 대해 숨겨집니다.

두 가지 종류의 권한을 사용할 수 있으므로 역할 종류도 두 가지입니다.

- **공간별 역할** - 권한은 공간별로 다르므로 특정 공간에만 적용됩니다. 기기 관리, 공간 안에서의 앱 관리를 예로 들 수 있습니다.
- **공간 교차 역할** - 특성상 권한을 모든 역할에 적용할 수 있습니다. MDM 인증서, App Catalog 설정처럼 테넌트 수준 설정을 예로 들 수 있습니다.

## 사용자 지정 역할 생성

사용자 지정 공간 교차 또는 공간별 역할을 생성할 수 있습니다. 권한을 선택하면 종속된 권한이 자동으로 선택됩니다. 이에 따라, 사용자 지정 역할이 할당된 사용자는 사용자가 기기 페이지 또는 기기 상세 정보 페이지를 방문하면 사용할 수 있는 특정 작업(폐기, 지우기 등)만 수행할 수 있습니다.

보기 사용자 등록 PIN 사용자 지정 역할을 적용하면 사용자는 액세스 수준이 같거나 권한이 더 낮은 다른 사용자의 PIN을 볼 수 있으며 사용자는 다른 사용자의 PIN을 만들 수 없습니다.

> 새로 생성된 사용자 지정 역할은 아무에게나 자동으로 할당할 수 없습니다. 테넌트 슈퍼 관리자는 나중에 필요할 때 다른 사용자에게 사용자 지정 역할을 할당할 수 있는 필수 관리 사용자에게 이 역할을 할당해야 합니다.

**절차**

1. **관리자** > **역할 관리**로 이동합니다.
2. **+사용자 지정 역할 추가**를 클릭합니다.
3. **역할 생성** 페이지에서 새 역할의 **이름**을 입력합니다.
4. (선택 사항) 새로운 역할에 대한 설명을 추가합니다.
5. **역할 유형**에서 다음 역할 유형 중 하나를 선택합니다.
   - **공간 교차 역할**
   - **공간별 역할**
6. **권한**에서 필요한 상세 권한을 선택합니다.
7. 관리자 및 사용자 권한은 다음 표를 참조하십시오.
   **저장**을 클릭하세요.

다음 표에는 사용자 지정 역할을 생성하는 데 사용할 수 있는 권한, 역할, 속성이 열거되어 있습니다.

| 역할 유형 | 권한 범주 | 상세 권한 |
| --- | --- | --- |
| **공간 교차 역할** | | |
| **관리** | | |
| | 사용자 지정 속성 관리 | • 사용자 지정 속성 추가<br>• 사용자 지정 속성 제거<br>• 사용자 지정 속성 편집<br>• 사용자 지정 속성 보기 |
| | 지원 관리자 | • 지원 관리자 추가<br>• 지원 관리자 삭제<br>• 지원 관리자 비활성화<br>• 지원 관리자 보기 및 로그인 기록 표시 |
| | 인증서 권한 | • 인증서 권한 추가<br>• 인증서 권한 삭제 |
| | Connector | • Connector 로그 추가<br>• Connector 로그 삭제<br>• Connector 보기<br>• Connector 업데이트 |
| | LDAP 관리 | • 사용자/그룹/OU 추가<br>• 서버 추가<br>• 서버 탐색<br>• 서버 삭제<br>• 서버 검색<br>• 서버 동기화<br>• 사용자/그룹/OU 제거<br>• 서브 보기<br>이 섹션의 모든 LDAP 권한에는 Connector 보기 권한이 필요합니다. 이는 이 LDAP 권한 중 어느 것이든 선택하면 Connector 섹션에서 자동으로 선택됩니다. |
| | 라이선싱 관리 | 라이선스 보기 |
| | 앱 배포 관리 | **앱 배포 업데이트**<br>이제 **앱 배포 업데이트** 권한을 **앱 배포 관리**의 사용자 정의 역할에서 설정할 수 있습니다. 시스템 관리 역할을 가진 사용자는 이 권한이 기본적으로 자동 부여됩니다. 이제 앱 배포 페이지에 **공간 관리자가 배포를 편집하도록 허용** 확인란이 추가되었으며, 새로운 앱 버전에서 기본적으로 활성화되어 있습니다. 이 새로운 권한이 포함된 사용자 정의 역할을 |

| 역할 유형 | 권한 범주 | 상세 권한 |
| --- | --- | --- |
| | | 할당받은 사용자와 시스템 관리 권한 없이 앱 관리 역할을 가진 사용자도 이 설정을 수정할 수 있습니다. 각 애플리케이션 버전에 대해 앱 배포 잠금 설정의 사용 가능 여부가 배포 페이지에 표시되며, 모든 디스코핑 시도가 감사 로그에 기록됩니다. |
| **사용자** | | |
| | 사용자 관리 작업 | • 사용자 보기<br>• 사용자 업데이트<br>• 사용자에게 메시지 보내기<br>• 사용자에게 역할 추가/할당<br>• 사용자 생성<br>• 사용자 삭제<br>• 사용자 초대<br>• 사용자 등록 PIN 보기 |
| | 사용자 지정 사용자 속성 할당 | • 속성 삭제<br>• 속성 보기<br>• 속성 추가/편집 |
| | 사용자 그룹 | • 사용자 그룹 보기<br>• 사용자 그룹 편집<br>• 사용자 그룹에 역할 추가/할당<br>• 사용자 그룹 만들기<br>• 사용자 그룹 삭제 |
| | 보고서 관리 | • 보고서 만들기<br>• 보고서 편집<br>• 보고서 실행<br>• 보고서 기록 삭제<br>• 보고서 보기<br>• 보고서 삭제<br>• 보고서 기록 다운로드 |
| **결정합니다.** | | |
| | 대량 등록 | • 대량 등록 생성<br>• 대량 등록 업데이트 |

| 역할 유형 | 권한 범주 | 상세 권한 |
| --- | --- | --- |
| | | • 대량 등록에 사용자 할당<br>• 대량 등록 보기<br>• 대량 등록 삭제 |
| **공간별 역할**<br><br>**결정 합니다.** | | |
| | 기기 작업 | • 사용자에게 기기 할당<br>• 기기 활성화 잠금 삭제<br>• 기기 삭제<br>• 기기 분실 모드 비활성화<br>• 기기 분실 모드 활성화<br>• 기기 강제 체크인<br>• 장치 잠금 설정<br>• 장치 잠금 해제<br>• 기기 강제 로그아웃<br>• 기기 시스템 앱 재설치<br>• 기기 다시 시작<br>• iOS 기기 업데이트 일정 설정<br>• 기기 소유권 포기<br>• 장치 폐기<br>• 기기 폐기 취소<br>• 기기 종료<br>• 기기 보기<br>• 기기 지우기<br>• 기기 지우기 취소<br>• 기기 OS 버전 업데이트<br>• 업로드를 통한 대량 할당<br>• TeamViewer 세션 시작<br>• 키오스크 모드 입력<br>• Kiosk 모드 나가기 |
| | 사용자 지정 기 | • 기기 사용자 지정 속성 추가/편집 |

| 역할 유형 | 권한 범주 | 상세 권한 |
| --- | --- | --- |
| | 기 속성 할당 | • 기기 사용자 지정 속성 삭제<br>• 기기 사용자 지정 속성 보기<br>이 섹션의 사용자 지정 기기 속성 모두 할당 권한에는 기기 읽기 권한이 필요합니다. 이는 이 사용자 지정 기기 속성 할당 권한 중 어느 것이든 선택하면 기기 작업 섹션에서 자동으로 선택됩니다. |
| | 기기 구성 | • 프로필 제외<br>• 프로필 푸시<br>• 제외된 프로필 푸시<br>• 오류 발생 시 설치 재시도 |
| | 기기 그룹 | • 기기 그룹 추가<br>• 기기 그룹 삭제<br>• 기기 그룹 편집<br>• 기기 그룹 보기 |
| | 대량 등록 | • 대량 등록 생성<br>• 대량 등록 업데이트<br>• 대량 등록에 사용자 할당<br>• 대량 등록 보기<br>• 대량 등록 삭제 |
| | 앱 인벤토리 | • 앱 인벤토리 보기 |
| **구성** | | |
| | 구성 | • 구성 보기/내보내기<br>• 구성 편집/우선순위 지정<br>• 구성 추가/복제<br>• 구성 삭제 |
| **정책** | | |
| | 정책 | • 정책 보기<br>• 정책 편집/우선순위 지정<br>• 정책 추가/복제<br>• 정책 삭제 |

역할을 편집하려면 관리자, 역할 관리 페이지로 이동해 역할 이름에 대한 **작업**에서 편집 아이콘을 클릭합니다. 사용자는 공간 교차 역할을 공간별 역할로, 또 그 반대로도 편집할 수 없습니다.

**관련 항목**:

- 사용자에게 사용자 지정 역할을 할당하려면 **역할 할당**을 참조하십시오.
- 기본 역할 목록은 **사용자 역할**을 참조하십시오.
- **사용자 지정 보고서 사용**
- **정기 보고서 사용**

# 12.1.6. 공간

이 섹션에는 다음 주제가 포함됩니다.


- 공간
- 공간 관리
- 공간 예
- 기기 위임
- 앱 위임

# 12.1.6.1. 공간

**라이센스:** Silver

공간은 위임된 관리를 위해 UEM(통합 엔드포인트 관리) 시스템을 독립적으로 관리되는 엔티티로 분리하는 데 사용됩니다. 조직 계층을 반영하기 위해 공간을 생성할 수 있습니다. MDM용 Ivanti Neurons는 기본 공간이라고 하는 중앙 관리 엔터티와 위임된 공간이라고 하는 다수의 종속 관리 엔터티를 사용하여 단일 수준 위임을 지원합니다. 모든 UEM 시스템은 기본 공간과 함께 생성됩니다.

> 간격 페이지 및 관련 옵션은 UEM용 Ivanti Neurons 및 MDM용 Ivanti Neurons에 모두 액세스할 수 있는 컨버지드 테넌트에 대해 숨겨집니다.

공간은 다음 시스템 구성 요소의 위임된 관리를 허용합니다. 사용자 및 사용자 그룹은 현재 위임할 수 없습니다.

- 기기
- 구성
- 정책
- 기기 그룹
- 애플리케이션
- 앱 카탈로그
- Apple Apps 및 Books 토큰

관리자가 하나 이상의 위임된 공간으로 테넌트의 MDM용 Ivanti Neurons 관리자 포털에 로그인하면 관리자에게 관리자 포털 로그인 프로모 팝업이 나타납니다. 위임된 공간 생성 이후 및 위임된 공간이 이미 생성된 경우 사용자 로그인 중에는 프로모 팝업이 표시되지 않습니다.

## 전역 관리자 및 위임된 공간 관리자의 역할

기본 공간에 액세스할 수 있는 적절한 역할을 보유한 관리자를 전역 관리자라고 합니다. 기본 공간에 대한 액세스는 읽기 전용 또는 읽기-쓰기 권한일 수 있습니다. 적절한 관리 역할을 보유한 전역 관리자는 위임된 공간을 생성하고 이를 관리하기 위한 위임된 관리자를 할당할 수 있습니다. 하나 이상의 위임된 공간을 관리하도록 위임된 관리자를 할당할 수 있습니다.

해당 관리자가 액세스할 수 있는 공간은 기기 및 앱 탭의 왼쪽 상단 모서리에 있는 공간 선택기 드롭다운에 나열됩니다. 공간을 보고 관리하려면 공간 드롭다운을 사용하여 원하는 공간으로 전환하십시오.

전역 관리자는 기본 공간 외에 모든 위임된 공간을 보고 제어할 수 있습니다. 위임된 관리자는 전역 관리자로부터 할당받은 공간만 보고 제어할 수 있습니다. 전역 관리자는 위임된 공간에 대한 중앙 제어권을 유지하는 반면, 위임된 관리자는 위임받은 공간을 자율적으로 관리할 수 있습니다. 관리 자율성은 위임이 기본 공간에서 상속된 것인지 아니면 복사된 것인지에 따라 다릅니다.

다음은 다양한 사용자 역할 그리고 이들이 수행할 수 있는 작업입니다.

### 위임된 공간에 있는 상속된 앱

- 위임 당시의 기존 등급이나 평가는 상속되며, 위임된 공간에서 사용자에게 표시됩니다(작성자 사용자 이름 포함).
- 위임된 관리자는 상속된 앱에 대한 등급/평가를 삭제할 수 없습니다.
- 위임된 관리자는 상속된 앱에 대한 등급/평가를 내보낼 수 있습니다.
- 위임된 공간에 있는 사용자는 상속된 앱에 등급/평가를 추가할 수 있습니다.
- 위임된 공간에 있는 사용자는 위임된 공간에서 사용자가 추가한 등급/평가를 볼 수 있습니다(작성자 사용자 이름 포함).

### 위임된 공간에 있는 앱(추가됨, 상속되지 않음)

- 전역 관리자만 **앱 > 카탈로그 설정 > 등급 및 평가**에서 평가를 활성화하거나 비활성화할 수 있습니다.
- 위임된 공간에 있는 사용자는 등급/평가를 추가할 수 있습니다.
- 위임된 관리자는 같은 위임된 공간에서 사용자가 추가한 평가를 삭제할 수 있습니다.
- 기본 공간을 비롯한 다른 위임된 공간에 있는 사용자는 각 위임된 공간에 있는 사용자가 추가한 등급이나 평가를 볼 수 없습니다.
- 위임된 관리자는 모든 사용자가 추가한 평가를 내보낼 수 있습니다(사용자 이름 포함).

### 기본 공간에 있는 위임된 앱

- 전역 관리자는 위임된 공간에서 사용자가 추가한 등급이나 평가를 삭제할 수 있습니다.
- 전역 관리자는 위임된 공간에서 사용자가 추가한 등급 및 평가를 포함하여 모든 등급이나 평가를 내보낼 수 있습니다.
- 기본 공간에 있는 사용자는 위임된 공간에서 사용자가 추가한 등급이나 평가를 볼 수 있습니다(사용자 이름 포함).

## 위임된 공간의 우선순위

UEM 시스템에 있는 기본 공간은 언제나 우선순위가 가장 낮습니다. 다른 위임된 공간과 관련된 위임된 공간의 우선순위는 전역 관리자에 의해 설정되며 언제든지 변경될 수 있습니다. 위임된 공간은 관리 포털의 관리 탭 아래에 있는 공간 페이지에서 가장 높은 우선 순위부터 가장 낮은 우선 순위 순으로 나열됩니다.

## 상속 또는 복사를 통한 위임

위임된 관리에서의 핵심 개념은 시스템 구성 요소가 기본 공간으로부터 상속되는지 아니면 복사되는지의 여부입니다.

# 12.1.6.2. 공간 관리

공간을 사용하면 여러 관리자가 관리(위임 관리)할 기기 그룹을 지정할 수 있습니다. 공간 관리자는 공간에 있는 기기에 적용되는 {{구성}} 및 {{정책}}을 정의할 수 있습니다. 공간을 만든 후 각 공간을 관련되거나 적합한 관리자에게 할당할 수 있습니다.

이 공간 페이지에는 다음이 포함됩니다.

- 공간을 빠르게 찾을 수 있는 검색 기능.
- 많은 수의 공간을 탐색하기 위한 페이지 매김 제어 기능.
- 위임된 공간 순서를 관리하기 위한 공간 우선순위 지정 제어 기능.
- 여러 공간을 선택하고 삭제할 수 있는 옵션.

> 기본 공간은 삭제할 수 없습니다.

- 공간의 알파벳순 정렬.
- 공간 선택기에서 최근 조회된 공간 목록.
- 기기, 구성, 정책 및 콘텐츠 페이지 전반에서 공간 선택이 유지되어 페이지 간 이동 시 다시 선택해야 하는 필요성 감소.

> 사용자는 사용 가능한 모든 공간이 아닌 할당된 공간만 확인할 수 있습니다. 현재로서 이 설정은 **장치**, **장치 그룹**, **앱**, **앱 인벤토리**, **콘텐츠**, **구성**, **정책**, **인증서 관리** 모듈에만 적용됩니다. 이러한 모듈을 보면서 스페이스 목록에서 선택한 스페이스는 해당 모듈에 대한 관리자 기본 설정 선택 사항으로 저장됩니다. 이러한 기본 설정은 현재 로그인 세션뿐 아니라 이후의 세션에 대해서도 저장됩니다.

사용자가 생성하는 공간은 기본 공간의 구성을 그대로 상속합니다. 따라서 사용자가 차후 기본 공간에 구성을 생성할 경우 해당 구성은 모두 다른 공간에도 적용될 수 있습니다. 단, 기존 설정에서 변경되는 내용은 상속되지 않습니다.

사용자가 생성하는 공간에는 생성 당시 기본 공간에 존재하는 정책의 복사본만 수신됩니다. 차후 기본 공간에 생성하는 정책은 기본 공간에만 적용됩니다.

해당 공간의 소속 기기를 정할 규칙을 생성합니다. 이러한 규칙은 "다음으로 시작", "다음으로 끝", "포함", "미포함", "다음으로 시작하지 않음", "다음으로 끝나지 않음", "보다 작음", "보다 큼", "범위에 있음", "다음과 같음", "다음과 같지 않음" 연산자를 사용하여 필터링할 수 있습니다. 규칙은 ANY(OR) 또는 ALL(AND) 옵션을 사용하여 중첩될 수 있습니다. 규칙의 정확도는 규칙 끝에 나타나는 텍스트를 사용하여 검토할 수 있습니다.

규칙 작성기에서 사용자 그룹 이름 속성을 선택하면 MDM용 Ivanti Neurons 관리자 포털에 중복 사용자 그룹의 수와 중복 그룹을 식별하기 위한 해당 GUID 수가 표시됩니다. 또한 이 규칙 아래에 있는 표에는 중복 사용자 그룹 목록과 사용자 그룹 이름, GUID, 소스, 배포된 이름(DN)과 같은 세부 정보가 표시됩니다.

다음 기준으로 규칙을 통해 기기를 확인합니다.

- Entra ID 등록됨
- APNS 가능
- 대체 일련 번호(Android 전용 - 기기 관리자 또는 기기 소유자 모드에서 Samsung 기기에 해당됨)
- Android 5G 네트워크 슬라이싱 활성화됨
- Android 엔터프라이즈 업무 관리형 기기 비 GMS 모드(AOSP) 활성화됨
- Android 전용 기기
- Android 엔터프라이즈 지원

- 작업 프로필이 있는 Android 관리 기기
- Android SafetyNet 인증 유형
- Android Work 활성화됨
- Android 보안 패치 수준(Android 기기)
- Android 업무 관리 기기(기기 소유자)가 활성화됨
- Android 작업 프로필 활성화됨
- 활성화된 회사 소유 기기에서 Android 작업 프로필 활성화됨
- 피싱 방지 기본 상태
- 피싱 방지 상태
- 피싱 방지 VPN 상태
- 자동화된 기기 등록 등록됨
- 자동화된 기기 등록 활성화됨
- Autopilot 등록됨
- Azure 클라이언트 상태 코드
- Azure 기기 컴플라이언스 보고서 시간
- Azure 기기 컴플라이언스 상태
- Azure 기기 식별자
- Sentry 차단됨
- 액세스 차단됨
- 부트스트랩 토큰 사용 가능
- 대량 제공 유형(Apple Configurator 또는 없음)
- 통신사
- 클라이언트 마지막 체크인
- 등록된 클라이언트
- 컴플라이언스
- 정책 준수 활동 차단됨
- 현재 국가 이름(드롭다운 목록에서 국가 이름 선택)
- 현재 MCC
- 현재 MNC
- 사용자 지정 기기 속성
- 사용자 지정 LDAP 속성
- 사용자 지정 사용자 속성
- 데이터 로밍
- 기기 소스
- 기기 유형
- 디바이스 유형(Apple)
- 표시 이름

- 암호화 활성화됨
- 자국 이름(드롭다운 목록에서 자국 선택)
- 홈 MCC
- 홈 MNC
- IMEI
- IMEI2(듀얼 SIM 포트가 있는 Android 장치에만 해당되고 Android 8.0 이상 장치에 적용 가능)
- 기관 복구 키 활성화됨
- IP 주소
- Kiosk 모드
- 마지막 체크인
- 분실 모드 활성화됨
- MAM 전용
- 제조업체
- MTD 활성화 상태
- 다중 사용자 모드
- OS
- OS 버전
- 버전이 있는 OS
- 소유권
- 개인 복구 키 활성화됨
- 전화 번호
- 격리됨
- 복구 잠금 활성화됨
- 로밍
- Secure Apps 상태
- 일련 번호
- 상태
- 감독됨
- 추가 빌드 버전
- 추가 OS/버전 기타
- 토큰 잠금 해제 사용 가능(iOS)
- 사용자 등록 등록됨
- 사용자 그룹
- 사용자 이름
- 음성 로밍
- macOS 개인 복구 키 에스크로됨
- macOS 복구 키 유형

> 이러한 규칙은 **실버** 라이센스 이상에서만 사용 가능합니다.

## 공간 생성

**절차**

1. **관리** > **시스템** > **공간**으로 이동합니다.
2. **공간 만들기**를 클릭합니다.
3. 공간 이름을 입력합니다.
4. 공간에 적절한 규칙 및 설정을 구성합니다.
5. **저장**을 클릭하세요.

## 공간 우선순위 지정

MDM용 Ivanti Neurons는 모양 순서대로 공간을 평가합니다.

**절차**

1. **공간 우선순위 지정**을 클릭합니다.
2. 공간 옆에 있는 위쪽 또는 아래쪽 아이콘을 선택하여 우선순위를 조정합니다.
3. **저장**을 클릭하세요.

## 공간 삭제하기

1. **관리** > **시스템** > **공간**으로 이동합니다.
2. 확인란을 사용하여 하나 이상의 공간을 선택합니다.
3. **삭제**를 클릭하세요. 메시지가 표시되면 삭제 확인

## 공간 관리자 지정

**절차**

1. **사용자**를 선택하세요.
2. 관리자로 지정할 사용자를 검색하세요.
3. 세부정보를 표시할 사용자 링크를 클릭하세요.
4. **작업** > **역할 할당**을 선택합니다.
5. **장치 관리**를 선택하세요.
6. **기기 관리** 메뉴에서 해당 관리자의 공간을 선택합니다.
7. **완료**를 클릭하세요.

해당 관리자가 로그인하면 소속 공간의 기기와 구성, 정책만 화면에 표시됩니다.

## 구성 또는 정책 복제하기

몇 가지의 차이를 두고 구성이나 정책을 복제해야 할 경우 이를 복제할 수 있습니다. 복제된 구성이나 정책을 다른 기기 그룹으로 연동할 수도 있습니다. 모든 정책은 공간 안에서 복제할 수 있습니다. 사용자 제공 ID 인증서 및 Threat Defense를 제외한 모든 구성은 공간 안에서 복제할

수 있습니다. 다음 구성 또한 기본 공간의 공간 전체에 걸쳐 복제할 수 있습니다.

- iOS 제한
- 웹 클립
- 인증서
- 암호
- SCEP(iOS 및 Windows)
- ID 인증서(동적으로 생성됨)

- 구성 또는 정책 유형 이름은 공간 안에서 고유해야 합니다. 구성 또는 정책의 기타 모든 속성은 복제할 수 있습니다.
- 구성은 관리자가 액세스할 수 있는 모든 공간으로 복제됩니다. 구성을 복제하기 위해 전역 관리자가 될 필요는 없습니다.

**절차**

1. 복제하고자 하는 것에 따라 **구성** 또는 **정책**으로 이동합니다.
2. 구성 또는 정책 링크를 클릭하여 상세 내용을 표시합니다.
3. **복제** 아이콘을 클릭합니다.
4. 팝업 창에서 **이름** 및 필요한 경우 **설명**을 입력합니다.
5. **다음**을 클릭하세요.
6. 요구 사항에 따라 구성 또는 정책을 수정합니다.
7. **다음**을 클릭하세요.
8. 배포를 구성합니다.
9. **완료**를 클릭하세요.

자세한 내용은 공간 예를 참조하십시오.

# 12.1.6.3. 공간 예

이 주제는 관리자가 공간을 사용할 수 있는 방식과 관련된 예를 제공합니다.

## 위치별 관리자

ACME, Inc.는 북미와 유럽에 지사를 두고 있습니다. ACME에서는 언어와 시차 문제로 미국에서 북미 지역 장치를 관리할 관리자 한 명과 독일에서 유럽 지역 장치를 관리할 관리자 한 명을 필요로 합니다.

이러한 공간을 구성하기 위해 ACME는 다음과 같은 사항을 변경했습니다.

1. MDM용 Ivanti Neurons에 유럽 지역 사용자를 위한 사용자 그룹을 생성했습니다.
2. MDM용 Ivanti Neurons에 북미 지역 사용자를 위한 사용자 그룹을 생성했습니다.
3. 다음 규칙에 따라 유럽 공간을 생성했습니다.
4. 사용자 그룹 = 유럽
   다음 규칙에 따라 북미 공간을 생성했습니다.
5. 사용자 그룹 = 북미
   각 공간의 기기 관리 역할을 적절한 관리자에게 할당했습니다.

현재 ACME의 공간:

- 유럽
- 북미
- 기본

## 각 위치의 OS별 관리자

ACME는 Android 전문가만 Android 기기를 관리하도록 하기로 결정했습니다. 북미 그룹과 유럽 그룹에 Android 전문가가 각각 한 명씩 추가되었습니다. 따라서 신규 공간이 두 개 필요합니다.

해당 공간을 추가하기 위해 ACME는 다음과 같은 사항을 변경했습니다.

1. 다음 규칙에 따라 유럽-Android 공간을 생성했습니다.
2. 사용자 그룹 = 유럽
   OS = Android
   다음 규칙에 따라 북미-Android 공간을 생성했습니다.
3. 사용자 그룹 = 북미
   OS = Android
   각 공간의 기기 관리 역할을 적절한 관리자에게 할당했습니다.

현재 ACME의 공간:

- 유럽-Android
- 북미-Android
- 유럽
- 북미
- 기본

## 경영진 관리자

ACME 경영진은 전문 관리자의 전문적인 서비스가 필요하다는 결정을 내렸습니다. 현재 목록에는 가장 중요한 경영진만 포함되어 있습니다.

해당 공간을 추가하기 위해 ACME는 다음과 같은 사항을 변경했습니다.

1. 다음 규칙에 따라 경영진 공간을 생성했습니다.
2. 사용자 이름 = jdoe@acme.com
   사용자 이름 = gkunz@acme.com
   사용자 이름 = prizzo@acme.com
   사용자 이름 = fvanhoff@acme.com
   해당 공간을 **공간** 페이지 목록 맨 위로 이동했습니다.
3. 그렇지 않을 경우, Android 기기를 사용하는 경영진에게 잘못된 관리자가 배정될 수 있습니다.
   해당 공간의 기기 관리 역할을 전문 관리자에게 할당했습니다.

현재 ACME의 공간:

- 경영진
- 유럽-Android
- 북미-Android
- 유럽
- 북미
- 기본

## 기타 장치 관리자

ACME가 일본 지사를 개사하면 일본 공간이 생성되기 전까지 추가되는 기기는 기본 공간 관리자에게 할당될 예정입니다.

# 12.1.6.4. 기기 위임

공간은 기기를 독립적으로 관리되는 엔티티로 분리하는 데 사용됩니다. 공간의 구성원 자격은 생성한 규칙에 의해 결정됩니다. 기기 위임을 통해 전역 관리자가 UEM 시스템에서 기기를 분할하여 독립적으로 관리할 수 있습니다. 기기가 위임되면 해당 기기에 대한 액세스 권한을 하위 집단인 위임 관리자에게 할당하여 관리 책임을 분산할 수 있습니다.

위임된 기기를 기기 그룹으로 그룹화하고, 기본 공간이나 다른 공간에 있는 기기에 영향을 주지 않으면서 서로 다른 사용자 지정 구성을 기기 그룹에 적용할 수 있습니다.

## 기기를 위임하기 위한 규칙 생성

공간 규칙에 따라 해당 공간에 소속될 기기가 정해집니다. 기기가 소속될 수 있는 공간은 1개로 제한됩니다. 생성하는 공간 규칙과 일치하지 않는 기기는 자동으로 기본 공간에 소속됩니다.

1. 규칙 중 하나라도 충족하는 장치는 해당 정의에 포함되도록 설정하려면 **일부**를 선택하세요.
2. 규칙을 모두 충족하는 장치만 해당 정의에 포함되도록 설정하려면 **전체**를 선택하세요.
3. 드롭다운 목록의 다음 규칙 유형 중 원하는 유형을 선택하세요.
   - **사용자 지정 LDAP 속성:** LDAP 속성에 기반한 규칙.
   - **OS**: 기기의 운영 체제에 기반한 규칙.
   - **사용자 그룹**: 기기의 사용자 그룹에 기반한 규칙(기기 관리 서비스에서 설정됨).
   - **사용자 이름**: 기기와 연결된 사용자 이름에 기반한 규칙.
4. 선택한 규칙 유형의 기준을 설정하세요.
   - **사용자 지정 LDAP 속성**: LDAP 설정에서 구성된 사용자 지정 LDAP 속성의 이름을 입력합니다.
   - **OS**: Android, iOS, macOS 또는 Windows를 선택합니다.
   - **사용자 그룹**: 드롭다운 목록의 사용자 그룹 중 원하는 그룹을 선택합니다. 이 목록의 사용자 그룹은 **사용자 > 사용자 그룹** 메뉴에서 설정된 그룹입니다.
   - **사용자 이름**: 사용자 이름을 입력합니다.
5. 공간에 규칙을 추가하려면 바로 앞 규칙 옆의 + 표시를 클릭하십시오.
6. **미리보기**를 클릭하면 해당 공간에 할당될 기기를 미리 확인할 수 있습니다.
7. 미리보기로 확인한 기기를 해당 공간에 최종 할당하려면 **저장**을 클릭합니다.

공간 규칙과 일치하지 않는 기기는 일치하는 다음 공간으로 자동 이동됩니다. 기존 공간 규칙과 일치하지 않는 기기는 자동으로 기본 공간으로 이동됩니다. 예를 들어, 사용자 그룹에서 사용자를 삭제하면 해당 사용자의 기기가 다른 공간으로 이동됩니다. 다른 공간으로 이동할 경우 정책과 구성까지 변경됩니다.

# 12.1.6.5. 앱 위임

앱 위임을 통해 전역 관리자가 MDM용 Ivanti Neurons에서 앱을 분할하여 독립적으로 관리할 수 있습니다. 전역 관리자는 위임된 공간을 통한 분리와 제어를 유지하면서 공개 및 인하우스 앱을 중앙 집중식으로 소싱하고 배포할 수 있습니다.

앱을 중앙 집중식으로 배포함으로써 전역 관리자는 앱 구성은 물론 앱의 배포 규칙을 통해서도 앱의 관리 동작을 사전 정의할 수 있습니다. 그런 다음에 위임된 공간의 App Catalog에서 앱을 위임하고 사용 가능하도록 할 수 있습니다.

그러면 위임된 앱이 해당 위임된 공간 내에서 사용자에게 배포됩니다. 애플리케이션이 위임되면 해당 애플리케이션에 대한 액세스 권한을 하위 집단인 위임 관리자에게 할당함으로써 관리 책임을 분산할 수 있습니다.

앱 위임을 사용하려면 먼저 하나 이상의 위임된 공간을 정의해야 합니다. 애플리케이션은 위임될 때 모든 공간에 할당됩니다. 앱 위임 공간은 다음과 같이 분류됩니다.

- 기본 공간
- 위임된 공간

## 위임된 공간에 앱 추가

위임 관리자 또는 전역 관리자가 위임된 공간에 애플리케이션을 추가할 수 있습니다. 앱은 해당 앱이 추가된 위임된 공간의 App Catalog에만 나타납니다. 이미 위임된 앱을 기본 공간에서 위임된 공간으로 추가하면 오류가 발생합니다. 이 경우에는 먼저 기본 공간에서 앱에 대한 상속을 비활성화해야 위임된 공간에 추가할 수 있습니다. 자세한 내용은 구성 작업에서 **구성 추가**를 참조하십시오.

## 위임된 공간에서의 앱 배포

앱이 기본 공간으로부터 위임될 때 해당 배포 규칙이 상속됩니다. 이 앱은 앱의 배포 규칙에 맞는 위임된 공간에 할당된 모든 기기에 배포됩니다.

전역 관리자는 공간 관리자에게 모든 장치 및 사용자 지정 배포 옵션에 대해 동적으로 생성된 ID 인증서를 편집하도록 위임할 수 있습니다.

> 배포 변경 사항은 특정 공간에만 적용 가능합니다. 기타 모든 공간은 계속 기본 공간 배포 설정을 상속합니다.

> Android 앱에 대한 앱 승인 설정: Android 앱에 대해서는 공간별 앱 승인 설정을 지원하지 않습니다. 사용자 정의 공간에서 승인된 앱은 모든 공간에 적용됩니다.

> 기존 Android 카탈로그 앱: 공용 Android 앱이 기본 공간에 이미 추가된 테넌트에서 해당 공용 앱을 기본이 아닌 다른 공간에 추가하려면 먼저 앱의 위임을 취소해야 합니다.

> Android Enterprise 앱은 테넌트 수준 관리자만 추가할 수 있으며, 공간 수준 관리자는 추가할 수 **없습니다**. 관리형 Google Play는 위임된 공간별이 아니라 조직 수준에서 구성됩니다. 그 결과, 새로운 Android Enterprise 앱은 기본 공간에서만 승인할 수 있습니다. 위임된 관리자는 자신의 공간에서 이미 승인된 앱을 할당하고 관리할 수 있지만, 위임된 공간 내에서는 새로운 Android Enterprise 앱을 승인하거나 추가할 수 없습니다. 모든 새로운 앱은 먼저 기본 공간에서 승인되어야 하며, 이후에 적절한 그룹에 할당할 수 있습니다.

자세한 내용은 구성 작업에서 **구성 추가**를 참조하십시오.

# 12.1.7. 지원 관리자

임시 지원 관리자를 생성해 서비스 지원 팀이 사용자의 역할과 권한으로 로그인하도록 합니다. 이 사용자 계정은 7일 후 자동 만료되며, 필요한 경우 만료 전에 언제든 직접 삭제할 수 있습니다. 지원 관리자 계정을 생성하면 지원 팀의 장치 문제 해결이 더 용이해집니다.

## 지원 관리자 생성

**절차**

1. **지원 관리자** 페이지에서 **지원 사용자 추가**를 클릭합니다.
2. **사용자 생성**을 클릭하면 승인이 요청됩니다.

장치 관리 서비스 지원 팀에 승인 요청 이메일이 바로 발송됩니다.

> 지원 팀원이 새 계정을 승인하기 전까지는 **표시 이름** 필드에 "(비활성화)"가 표시됩니다. 생성된 계정이 화면에 표시되는 형식:

support-[random_ID]-[your_username]@[your_company].com

지원 관리자 계정 생성 후 **관리 > 지원 관리자**를 선택하면 기존 지원 관리자 목록이 바로 나타납니다. 따라서 지원 관리자 계정을 추가로 생성하려면 바로 2단계를 진행하시기 바랍니다.

> 새로 생성된 지원 관리자 계정은 기본적으로 읽기 전용입니다. 사용자 정의 역할은 자동으로 할당되지 않으므로 의도하지 않은 구성 변경의 위험을 줄일 수 있습니다. 관리자는 필요에 따라 나중에 역할 및 권한을 추가할 수 있습니다.

## 사용자 내역 보기

**지원 관리자** 페이지에서 **사용자 기록**을 클릭하여 지원 관리자의 로그인 기록을 확인합니다. 지원 관리자 페이지의 로그인 기록 데이터는 최근 90일 동안의 데이터까지만 사용할 수 있습니다.

## 지원 관리자 액세스 종료

**절차**

1. **지원 관리자** 페이지에서 삭제할 계정 우측의 **삭제** 링크를 클릭합니다.
2. 메시지가 표시되면 **사용자 제거**를 클릭하고 확인합니다.

## 지원 관리자 액세스 중지

**지원 관리자** 페이지에서 일시 중단할 계정 우측의 **비활성화** 링크를 클릭합니다.

# 12.1.8. 관리 > 시스템 사용 알림

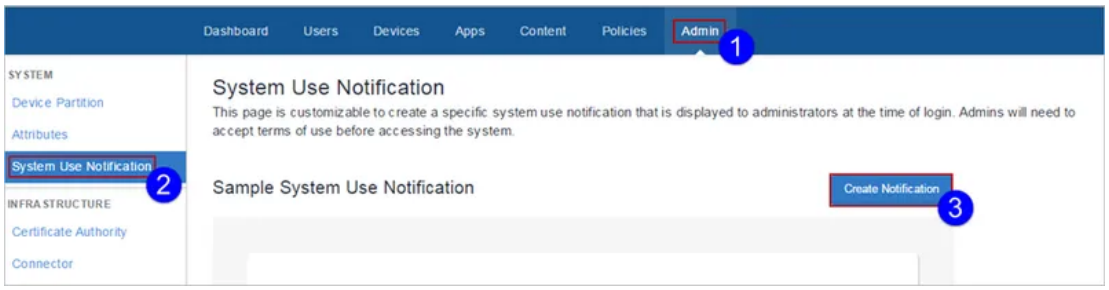
**라이센스:** Silver

시스템 사용 알림 기능을 사용해 사용자 지정 시스템 사용 알림을 만들 수 있습니다. 이 알림은 로그인 시 관리자에게 나타나며 관리자가 시스템에 액세스하기 전 사용 조건을 수락해야 합니다.

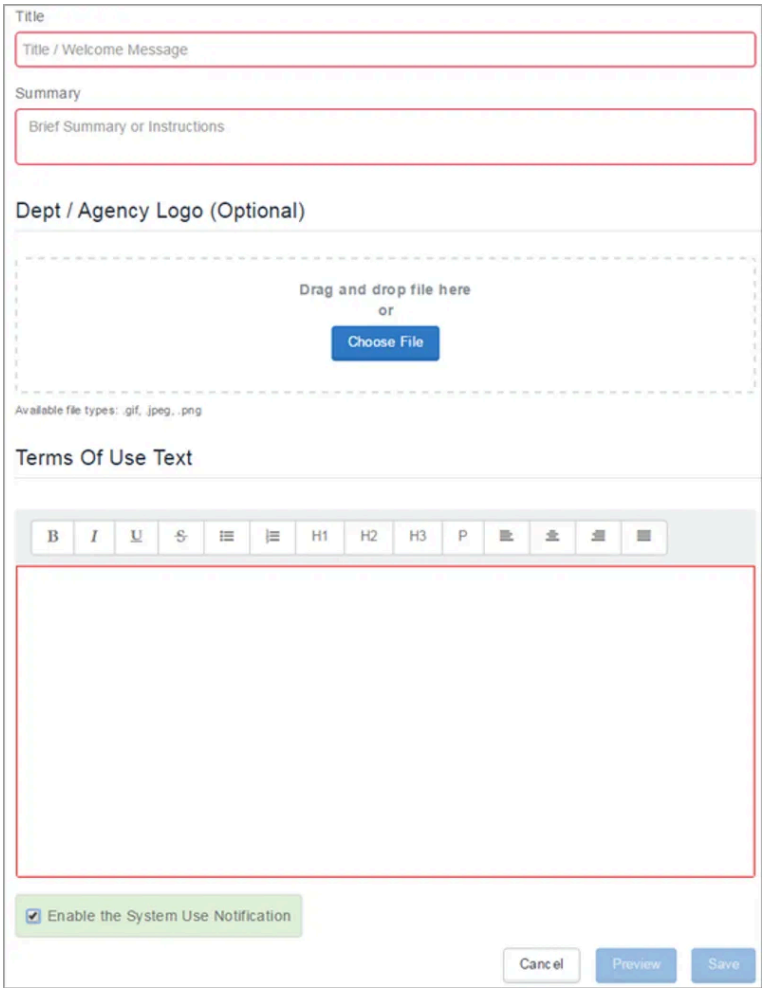
## 시스템 사용 알림 생성

**절차**

1. **관리 > 시스템 사용 알림**을 선택합니다.
2. **알림 생성**을 클릭합니다.




시스템 사용 알림 상세 정보 페이지가 나타납니다.




**제목** 필드에 제목을 입력합니다.

4. **요약** 필드에 요약 또는 지침을 입력합니다.
5. 원하는 경우 로고를 선택합니다.
6. **텍스트 사용 조건** 필드에서 텍스트 사용 조건을 입력합니다. 이것은 로그인 시 관리자가 수락해야 하는 텍스트입니다.
7. **시스템 사용 알림 활성화** 체크 박스에 체크 표시를 하여 알림을 켭니다.
8. **미리 보기**를 클릭하여 시스템 사용 알림의 미리 보기를 불러옵니다.
9. 시스템 사용 알림에 만족하는 경우 **저장**을 클릭합니다.

# 12.2. 인프라

이 섹션에는 다음 주제가 포함됩니다.

- 액세스
- 앱 목록
- 감사 내역 내보내기
- 인증서 관리
- 외부 인증기관용 SCEP 구성
- 파생된 자격 증명 제공자
- Connector
- Connector용 httpproxy 명령 사용
- Help@Work
- 인프라 ID
- LDAP 서버 구성
- Sentry
- MDM용 Ivanti Neurons 및 SCEP 서버 사이에 Kerberos 인증 활성화

# 12.2.1. 액세스

**적용 대상:** iOS 및 Android 기기

Access는 모든 기기 또는 앱에서 원활하고 생산적인 사용자 환경을 활성화하면서 비즈니스 데이터를 안전하게 보호합니다. Access는 사용자가 보안되지 않은 기기, 앱 또는 클라우드 서비스의 엔터프라이즈 클라우드 서비스에 액세스하지 못하도록 하는 데이터 경계를 설정합니다.

## 최신 문서

Access 및 Access 설정 방법에 대한 자세한 내용을 보려면 **제품 설명서**를 방문하고 Access를 클릭하십시오. 액세스 버전에 적합한 문서를 선택하십시오.

# 12.2.2. 앱 목록

**라이센스: Silver**

필수 앱, 허용 목록에 등록된 앱, 차단 목록에 등록된 앱 목록을 생성할 수 있으며, **허용된 앱 정책**과 함께 사용합니다. 기기에 설치한 앱이 앱 목록에서 암시한 요구 사항을 충족하지 않을 때 이 목록을 사용하여 수행할 작업을 지정할 수 있습니다. 앱 목록을 생성하면 편집할 수 없습니다. 앱 목록이 **허용된 앱 정책**에 참조될 수 있기 때문입니다. 마찬가지로 허용된 앱 정책에서 참조한 앱 목록은 삭제할 수 없습니다.

## 앱 목록 생성

**절차**

1. **관리 > 인프라 > 앱 목록**을 클릭합니다.
2. **새 목록 생성**을 클릭합니다.
3. **앱 목록 이름** 상자 아래에서 목록 이름을 입력합니다.
4. 목록 유형을 **화이트리스트**, **블랙리스트** 또는 **필수** 중에서 선택합니다.
5. **앱 추가** 섹션에서 앱 유형을 **App Store**, **OS X 스토어**, **Google Play**, **앱 카탈로그** 중에서 선택합니다.
6. 검색 기준을 입력하여 범위를 좁힙니다.
7. 체크박스를 사용하여 앱을 선택합니다. 복합 검색을 사용하고 하나 이상의 체크박스를 활성화할 수 있습니다.
8. **앱 보기** 탭을 클릭하여 지금까지 선택한 앱 목록을 확인합니다.
   **저장**을 클릭하세요.

이제 **허용된 앱 정책**을 구성할 때 이 목록을 사용할 수 있습니다.

**앱 목록** 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 시스템 읽기 전용

# 12.2.3. 감사 내역 내보내기

감사 내역 내보내기는 모든 감사 내역 정보를 특정 서버 위치로 내보내거나 업로드하기 위한 기능입니다. 서버는 기본 포트에서 액세스 되어야 합니다. 사용자는 매일 자동으로 특정 위치에 업로드된 감사 내역 아카이브를 얻기 위해 감사 내역 내보내기 설정을 구성할 수 있습니다.

> 감사 내역 내보내기는 Linux 및 Windows 기반 SFTP 서버에서 지원됩니다.

감사 내역 내보내기 설정 구성을 위해:

1. **관리자 > 인프라 > 감사 내역**을 선택합니다. **감사 내역** 페이지가 표시됩니다.
2. **감사 내역**페이지에서, 감사 내역 내보내기 활성화를 위해 **켜기**를 클릭합니다.
3. **내보내기** 섹션에서 다음 필드를 업데이트합니다.

| 기능 | 설명 |
| --- | --- |
| **형식 내보내기** | 감사 내역 데이터를 내보내야 하는 다음 형식 중 하나를 선택하십시오.<br>• **JSON**<br>• **CEF**(공통 이벤트 형식)<br>CEF 로그 메시지에는 다음의 기본값이 포함됩니다.<br>◦ 버전: CEF 형식 버전 번호. v25는 현재 지원되는 버전입니다.<br>◦ 기기 공급업체: Ivanti Inc<br>◦ 기기 제품: MDM용 Ivanti Neurons<br>◦ 기기 버전: 이벤트 생성 시의 최신 MDM용 Ivanti Neurons 버전.<br>◦ 기기 이벤트 등급 ID: 감사당 고유한 엔티티 ID<br>◦ 이름: 감사당 엔티티 이름 및 작업. 예: 프로모션 배포 구성 설정 생성.<br>◦ 심각도: 이벤트의 중요성 지정. 예: 낮음.<br>CEF 로그 메시지에는 다음의 키 값 쌍의 컬렉션인 확장 필드도 포함됩니다.<br>◦ CS1 및 CS1라벨: createdAt, entityType, entityName, and actionType과 같은 감사 내역 메타 데이터.<br>◦ CS2 & CS2 라벨: 행위자 정보.<br>◦ CS3 & CS3라벨: 작업 이전 상태.<br>◦ CS4 & CS4라벨: 작업 이후 상태.<br>CEF 내보내기에서는 지정된 제한을 초과하는 필드가 있을 경우(예: CS3 또는 CS4 키), 실제 값이 텍스트 “이 키에 대한 값이 매핑된 사전 키 허용 길이를 초과합니다”로 교체됩니다. |
| **서버** | 감사 내역 내보내기를 위해 서버 이름을 입력합니다. |
| **사용자** | 서버에 로그인하기 위해 사용자 이름을 입력합니다. |
| **비밀번호** | 서버 로그인 비밀번호를 입력합니다. |
| **서버 경로** | 서버 경로를 입력하고 주어진 경로가 서버에 존재하는지 확인합니다. 예: /사용자/테스트/내보내기 |
| **키 교환 알고리즘** | 송신 SFTP 구성에 대한 감사 로그를 내보내려면 키 교환 알고리즘 목록을 선택합니다.<br>다음은 기본적으로 선택된 키 교환 알고리즘입니다.<br>• **diffie-hellman-group-exchange-sha1**<br>• **diffie-hellman-group14-sha1**<br>• **curve25519-sha256**<br>• **diffie-hellman-group-exchange-sha256**(기본값으로 선택됨) |
| **암호** | 송신 SFTP 구성에 대한 감사 로그를 내보내려면 암호화 암호 목록을 선택합니다. 다음은 기본적으로 선택된 암호화 암호입니다.<br>• **aes128-ctr**<br>• **aes192-ctr**<br>• **aes256-ctr**(기본값으로 선택됨) |
| **HMAC** | 송신 SFTP 구성에 대한 감사 로그를 내보내려면 HMAC 알고리즘 목록을 선택합니다.<br>• **hmac-sha1 (기본적으로 선택되어 있음)** |

| 기능 | 설명 |
| --- | --- |
| | • **hmac-sha2-256**<br>• **hmac-sha2-512** |

필드가 이미 구성되었을 경우 위에 언급된 필드는 읽기 전용 모드 상태입니다. 구성된 필드를 수정하려면 **편집** 버튼을 클릭하십시오. 관리자가 이미 SFTP 내보내기를 설정했다면 업데이트된 후 모든 키 알고리즘이 선택됩니다.

서버 연결을 테스트하고 감사 내역 내보내기 구성을 저장하려면 **연결 테스트와 저장**을 클릭하십시오.

아카이빙된 감사 내역 파일들은 .zip파일 형태의 JSON 포맷으로 이용 가능합니다.

감사 내역 내보내기 설정을 저장하기 전 모든 필드의 구성 설정을 확인하십시오. 필드에 입력된 값이 하나라도 유효하지 않으면 오류 메시지가 표시됩니다.

## 공간에서 기기 등록 및 등록 해제에 대한 감사 내역 활성화

활성화하면 기기 등록, 기기 삭제, 공간 업데이트 또는 삭제로 인해 발생한 이벤트를 포함하여 공간 간 기기 이동이 감사 내역에 기록됩니다. 공간 관리자는 영향을 받는 기기를 식별하고, 공간 및 활동 유형별로 로그를 필터링하고, 감사 기록을 CSV로 내보낼 수 있습니다.

# 12.2.4. 인증서 관리

## 라이센스: Silver

인증서를 통해 인증하면 효과적으로 모바일 기기의 보안을 유지할 수 있습니다. 인증서는 비밀번호보다 더 안전한 데다, 자격 하나로 VPN(가상 사설 네트워크), 무선 네트워크, 이메일 등을 보호할 수 있기 때문입니다. 외부 인증기관 이용자는 Connector를 통해 해당 인증서 사용이 가능합니다. 따로 이용하는 인증 기관이 없는 사용자는 MDM용 Ivanti Neurons를 인증 기관으로 이용할 수 있습니다. 또한 Anyware를 다른 인증기관 이용을 위한 중간 인증기관으로 이용할 수도 있습니다. MDM용 Ivanti Neurons에서 발행되는 인증서는 자체 서명 인증서라고 합니다.

- SHA-1 인증서는 ID 인증서를 생성하는 동안 사용되지 않습니다. 다른 알고리즘을 선택할 수 있습니다. 인증서를 업데이트하는 동안 이전 인증서에서 SHA-1을 사용하는 경우 동일한 SHA-1 알고리즘을 사용할 수 있습니다. 이전 인증서에서 SHA-1 위의 알고리즘을 사용하는 경우 SHA-1로의 전환이 허용되지 않습니다.
- 로컬 또는 외부 인증 기관 구성 중 MDM용 Ivanti Neurons**의 캐시 ID** 옵션을 선택하여 MDM용 Ivanti Neurons 서비스를 통해 인증서를 저장합니다. 필요에 따라 매번 인증서를 생성해 캐시를 제거합니다.
- 인증서는 자동으로 재발급됩니다.
- 시스템 효율성을 높이기 위해 FIFO(처음 들어간 것부터 사용) 대기열을 사용하여 관리자가 만든 구성을 위한 인증서가 오프라인에서 생성됩니다. 오프라인에서 구성을 생성하는 기간 동안 구성 상태는 **기기 상세 정보** 페이지의 **구성** 탭에 있는 **상태** 열의 **인증서 생성 보류 중**이 됩니다. 인증서가 생성되면 구성은 **설치 보류** 상태로 이동하며, 자동 강제 체크인을 통해 인증서와 함께 기기로 푸시됩니다.
- DigiCert PKI 플랫폼 또는 GlobalSign 외부 인증 기관에서 서명한 인증서를 비롯한 모든 인증 기관 인증서는 기기가 폐기 및 삭제될 때, 그리고 인증서가 재생성될 때 해지됩니다.

관리자는 스마트 카드 로그온과 사용자 지정 개체 ID(OID)에 대해 MDM용 Ivanti Neurons 인증서를 생성할 수 있습니다. 다음 인증 옵션에 대해 인증서를 생성할 수 있습니다.

  - 클라이언트 인증 - 기본적으로 활성화됨
  - IPSEC – 선택 사항, 관리자가 활성화할 수 있음
  - 스마트 카드 로그온 - 선택 사항, 관리자가 활성화할 수 있음
  - 사용자 지정 OID - 선택 사항, 관리자가 활성화할 수 있음

> 이 기능은 다음 인증 기관에 대해서만 해당됩니다.
>
>  - 로컬 인증 기관
>  - 중간 인증 기관
>  - 외부 인증 기관 - IPSEC, 스마트 카드 로그온 및 사용자 지정 OID를 지원하도록 NDES 서버에서 CA 템플릿의 애플리케이션 정책 구성

> 장치 관리, 앱 스테이션 또는 기타 비 Android Enterprise 모드에서 Samsung API를 사용하는 Samsung 장치에서는 인증서 관리가 지원되지 않습니다. Samsung 권장 사항을 기반으로 Android Keystore로의 전환을 확인하는 것이 좋습니다.

자세한 내용은 인증서 구성을 참조하십시오.

## 온프레미스 SCEP 인증 기관에 연결

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.

2. 커넥터를 설치하고 구성하십시오(**관리자 > 커넥터**). 자세한 내용은 **Connector**를 참조하십시오.
3. **관리자** > **인프라** > **인증서 관리**로 이동합니다.
4. **인증서 권한** 섹션에서 **추가**를 클릭합니다.
5. **온프레미스 SCEP 인증 기관 추가**를 선택하고 **계속**을 클릭합니다.
6. 구성을 식별할 수 있는 이름을 입력합니다.
7. 다음 인증 기관 유형 중 하나를 선택합니다.
   - Microsoft
   - EJBCA
   - 일반 SCEP 서버
     일반 SCEP 서버 항목은 고정 챌린지 비밀번호를 갖는 대부분의 SCEP 서버에 사용할 수 있습니다.

화면에 표시된 양식을 작성하세요.

9. **완료**를 클릭하세요.

# 외부 인증 기관 생성

타사의 인증 기관을 사용하려면 이 옵션을 선택하십시오.

**절차**

1. **인증 관리** 페이지의 **인증 기관**섹션에서 **추가**를 클릭합니다.
2. 외부 인증 기관 생성의 인증 기관 추가 페이지에서 **계속**을 클릭합니다.
3. GlobalSign 또는 DigiCert PKI 플랫폼을 외부 인증 기관으로 선택합니다.
4. 표시된 양식에서 나머지 필드를 완료합니다.
5. **완료**를 클릭하세요.

## 외부 인증 기관의 인증서 보기

기존에 보관된 사본을 교체하기 위해 인증서의 세부 사항을 보고 이 인증 기관의 중간/대체 루트 인증서를 업로드할 수 있습니다.

**절차**

1. **인증 관리** 페이지의 **인증 기관**에서 외부 인증 기관 옆에 있는 **작업**을 클릭합니다. 그리고 **인증서 보기**를 클릭합니다. **인증서 보기** 창이 나타납니다.
2. **인증서 보기** 창에서 **인증서 업로드**를 클릭합니다. **인증서 업로드: 외부 인증 기관** 창이 표시됩니다.
3. **파일 선택**을 클릭하여 업로드할 인증서를 선택합니다.
4. **완료**를 클릭하세요.

# 중간 인증 기관 생성

- 인증서가 필요한 경우에는 CSR을 생성해 서명기관에 제출합니다. 서명기관으로부터 인증서를 받으면 해당 인증서를 업로드하시기 바랍니다.
- 필수 인증서가 이미 있는 경우 해당 인증서를 업로드하십시오.

## CSR(인증서 서명 요청서) 생성

**절차**

1. **인증 관리** 페이지의 **인증 기관** 섹션에서 **추가**를 클릭합니다
2. 인증 기관 추가 섹션의 중간 인증 기관 생성에서 **CSR 생성**을 클릭합니다.
3. 화면에 표시된 양식을 작성하세요.
4. **생성**을 클릭합니다.
5. 인증서 요청 시작(BEGIN CERTIFICATE REQUEST)과 인증서 요청 종료(END CERTIFICATE REQUEST) 사이의 내용을 텍스트 파일로 저장하세요.
6. 인증 기관에 텍스트 파일을 업로드합니다.
7. **완료**를 클릭하세요.

## 서명한 인증서 업로드하기

인증 기관으로부터 서명된 인증서를 받으면 서명된 인증서를 업로드할 수 있습니다.

**절차**

1. **인증 관리** 페이지의 **인증 기관** 섹션에서 생성했던 CSR에 대한 항목을 찾습니다.
2. 섹션에서 **작업 > 서명된 신규 인증서 업로드**를 선택합니다.
3. **파일 선택**을 클릭합니다.
4. 업로드할 서명된 신규 인증서를 선택하세요.
5. **완료**를 클릭하세요.

## 기존 인증서 업로드하기

이 토픽은 서명된 인증서를 업로드하는 방법을 설명합니다.

**절차**

1. **인증 관리** 페이지의 **인증 기관** 섹션에서 **추가**를 클릭합니다.
2. 인증 기관 추가 섹션의 중간 인증 기관 생성에서 **기존 ID 업로드**를 클릭합니다.
3. **이름** 필드에 이 인증서의 이름을 입력해 다른 인증서와 구별할 수 있도록 합니다.
4. **업로드**를 클릭하세요.
5. 업로드할 인증서를 선택하세요.
6. 업로드할 인증서의 비밀번호를 입력하세요.
7. **업로드**를 클릭하세요.

## 중간 인증 기관의 인증서 보기

인증서 상세 정보를 확인하고 인증 기관의 CRL(인증서 폐기 목록) URL을 얻을 수 있습니다.

**절차**

1. **인증 기관** 섹션에서 인증 기관 옆의 **작업**을 선택하고 **인증서 보기**를 클릭합니다. **인증서 보기** 창이 나타납니다.
2. **인증서 보기** 창에 있는 **CRL URL** 필드에서 URL을 볼 수 있습니다.
3. **복사**를 클릭하여 URL을 클립보드에 복사하고 다른 애플리케이션에 붙여넣기합니다. 해당 URL을 사용하여 인증 기관이 발행한 인증서를 수락하도록 Office 365를 구성할 수 있습니다.

# 독립 실행형 인증서 권한 생성

새로운 완전한 독립(로컬 및 자체 서명) 인증 기관을 생성하고자 하는 경우 이 옵션을 선택합니다.

**절차**

1. **인증 관리** 페이지의 **인증 기관** 섹션에서 **추가**를 클릭합니다.
2. 인증 기관 추가 페이지의 독립 인증 기관 생성에서 **계속**을 클릭합니다.
3. 화면에 표시된 양식을 작성하세요.
4. **생성**을 클릭합니다.

# 독립 실행형 인증 기관 만료 알림

독립 실행형(로컬) 인증 기관의 만료 정보는 인증서 만료일까지 30일 미만 남은 경우 이제 **만료 날짜** 열에 만료 정보가 툴팁으로 표시됩니다.

만료일까지 365일 미만 남은 경우,전송되는 알림 외에도 이 정보는 **대시보드** > **알림**에서 확인할 수 있습니다. **만료**를 필터로 선택합니다.

## 독립 실행형 인증 기관에서 발급한 인증서의 만료 기간 구성

독립(로컬) 인증 기관의 만료 기간을 구성할 수 있습니다.

**절차**

1. **인증 관리** 페이지의 **인증 기관** 섹션에서 독립 인증 기관 옆에 있는 **작업**을 클릭합니다.
2. **편집**을 클릭합니다.
   **인증 기관 편집** 창이 표시됩니다.
3. 클라이언트 인증서 템플릿 섹션의 **인증서 수명** 필드에서 새 만료 기간을 일 단위로 입력합니다.
4. **저장**을 클릭하세요.

로컬 인증 기관이 발행한 인증서가 곧 만료되거나 이미 만료된 경우 알림 및 이메일(옵션으로 설정 가능)을 받을 수 있습니다.

- 인증서 만료까지 남은 날짜 알림 - 인증서 만료 창에 미리 지정한 간격으로 알림이 생성됩니다. 첫 번째 알림은 만료되기 365일 전에 발생되며 이어서 180일, 60일, 45일, 7일 전에 각각 추가로 알림이 발생됩니다. **관리 > 인증서 관리 > 작업 > 새 서명 인증서 업로드**로 이동하여 인증서를 교체하기 전까지는 이 알림이 계속 표시됩니다.
- 인증서 만료 알림 - 인증서가 만료되면 알림이 발송됩니다. 정상 서비스를 재개하려면 인증서를 교체해야 합니다.
- 새 유효 인증서 업로드 시 알림 - 서명된 신규 인증서가 업로드되면 알림이 발송됩니다.

## 독립 인증 기관의 인증서 보기

인증서 상세 정보를 확인하고 로컬 인증 기관의 인증서 폐기 목록(CRL) URL을 얻을 수 있습니다.

**절차**

1. **인증 관리** 페이지의 **인증 기관** 섹션에서 로컬 인증 기관 옆에 있는 **작업** 클릭합니다. 그리고 **인증서 보기**를 클릭합니다. **인증서 보기** 창이 나타납니다.
2. **인증서 보기** 창에 있는 **CRL URL** 필드에서 URL을 볼 수 있습니다.
3. **복사**를 클릭하여 URL을 클립보드에 복사하고 다른 애플리케이션에 붙여넣기합니다. 해당 URL을 사용하여 로컬 인증 기관이 발행한 인증서를 수락하도록 Office 365를 구성할 수 있습니다.

# 인증 기관의 CRL 수명 보기

로컬 또는 중간 인증 기관의 CRL 수명을 보기 및 수정할 수 있습니다.

**절차**

1. **인증 관리** 페이지의 **인증 기관** 섹션에서 로컬 인증 기관 옆에 있는 **작업**을 클릭하고 **편집**을 클릭합니다. **인증 기관 편집** 창이 표시됩니다.
2. **인증서 권한 편집** 창에서 CRL 수명 값을 확인할 수 있습니다. 최소 기본값은 24시간입니다. 입력할 수 있는 최대값은 10,950시간입니다.
3. CRL 수명 값을 수정한 후 **저장**을 클릭합니다.

# 클라우드 인증 기관 생성

클라우드 인증 기관을 사용하려면 이 옵션을 선택하십시오.

**절차**

1. **관리자** > **인프라** > **인증서 관리**로 이동합니다.
2. **인증서 관리** 페이지의 **인증 기관** 섹션에서 **추가**를 클릭합니다.
3. **인증 기관 추가** 페이지의 **공개적으로 신뢰할 수 있는 클라우드 인증 기관에 연결** 아래에서 **계속**을 클릭합니다.
4. **이름** 칸에 이름을 입력합니다.
5. 다음 옵션 중에서 클라우드 인증 기관을 선택합니다.
   - **Atos IDnomic CMS**
   - **DigiCert One PKI 플랫폼**
   - **DigiCert PKI Platform**
   - **Entrust**
   - **GlobalSign**
6. 기본 URL을 입력하고 인증서 데이터를 업로드하세요.
7. **완료**를 클릭하세요.

# 인증서에 대해 고급 검색 사용

특정 기준에 따라 인증서를 식별하고 보려면 고급 검색 옵션을 사용하여 규칙 기반으로 발행된 인증서를 검색할 수 있습니다. 이러한 규칙은 "다음으로 시작", "다음으로 끝", "포함", "미포함", "다음으로 시작하지 않음", "다음으로 끝나지 않음", "보다 작음", "보다 큼", "범위에 있음", "다음과 같음", "다음과 같지 않음" 연산자를 사용하여 구성할 수 있습니다. 규칙 옵션은 임의(OR) 또는 모두(AND) 옵션을 사용하여 중첩될 수 있습니다. 섹션 하단에 발행된 인증서 중 규칙과 일치하는 것이 표시됩니다. MDM용 Ivanti Neurons 릴리스 76부터 모든 인증서 관리 템플릿에 대한 연산자는 표준 연산자를 갖습니다. 다음 템플릿의 운영자는 이 릴리스에서 표준화됩니다.

- 관리 > 인증서 관리 > 발행된 인증서 > 고급 검색

## 발행된 인증서 고급 검색

**절차**

1. **인증서 관리** 페이지의 **발행된 인증서** 섹션에서 **고급 검색** 링크를 클릭합니다.
2. 사용자가 규칙 중 하나 이상을 충족해야 할 경우에는 **일부**를 선택하고, 인증서가 모든 규칙을 충족해야 할 경우에는 **모두**를 클릭합니다.
3. 다음 속성에 대해 검색 기준을 정의하는 규칙을 생성합니다.
   - **CA**
   - **구성 이름**

- **만료**
- **비공개 키임**
- **OS**
- **일련 번호**
- **상태**
- **사용 유형**
- **사용자**

4. (선택 사항) 필요할 경우 +를 클릭하여 추가 규칙을 생성할 수 있습니다.
5. (선택 사항) 쿼리를 저장하려면 **저장**을 클릭합니다.
6. **검색**을 클릭합니다. 검색 기준에 부합하는 사용자 목록이 페이지에 표시됩니다.

### 사용자 제공 인증서 고급 검색

**절차**

1. **인증서 관리** 페이지의 **사용자 제공 인증서** 섹션에서 **고급 검색** 링크를 클릭합니다.
2. 사용자가 규칙 중 하나 이상을 충족해야 할 경우에는 **일부**를 선택하고, 인증서가 모든 규칙을 충족해야 할 경우에는 **모두**를 클릭합니다.
3. 다음 속성에 대해 검색 기준을 정의하는 규칙을 생성합니다.
   - **인증서 이름**
   - **만료 날짜**
   - **발급자**
   - **다음에 업로드됨**
4. (선택 사항) 필요할 경우 +를 클릭하여 추가 규칙을 생성할 수 있습니다.
5. (선택 사항) 쿼리를 저장하려면 **저장**을 클릭합니다.
6. **검색**을 클릭합니다. 검색 기준에 부합하는 사용자 목록이 페이지에 표시됩니다.

## 발행된 인증서에 대한 검색 쿼리 로드

저장된 검색 쿼리 목록을 볼 수 있습니다.

**절차**

1. **인증서 관리** 페이지의 **발행된 인증서** 섹션에서 **고급 검색** 링크를 클릭합니다.
2. '폴더' 아이콘을 클릭합니다. **고급 검색** 창이 표시됩니다. 생성된 검색 쿼리 목록이 **쿼리 로드** 섹션에 표시됩니다. 이 섹션에 다음 상세 정보가 표시됩니다.
   - **쿼리 이름** - 로드된 쿼리 이름.
   - **쿼리 콘텐츠** - 검색 쿼리를 정의하는 규칙에 콘텐츠를 표시합니다.
   - **작업** - 쿼리에서 수행할 작업을 선택합니다.
3. 로드된 쿼리에 정의된 기준에 부합하는 발행된 인증서 목록을 보려면 **작업** 열에서 **쿼리 로드**를 클릭합니다.
   로드된 쿼리를 삭제하려면 삭제 아이콘을 클릭합니다.

> **CSV로 내보내기**를 클릭하고 CSV 파일로 검색 결과 보고서 콘텐츠를 다운로드하여 이후 참조나 분석에 활용합니다.

### 발행된 인증서의 만료 기간 보기

**발행된 인증서** 섹션의 **만료(일)** 열에서 30일 내에 만료될 인증서의 남은 일수를 확인할 수 있습니다. 마지막 30일 내에 인증서가 이미 만료된 경우 인증서의 **만료(일 기준)** 열에는 만료일 이후 경과된 일 수가 표시됩니다.

자세한 내용은 **외부 인증 기관용 SCEP 구성**을 참조하십시오.

## CSV로 내보내기

인증서를 CSV 파일로 내보내면 추후 참조하거나 분석할 수 있습니다.

**절차**

1. **인증서 관리** 페이지에서 다음 탭 중 하나로 이동합니다.
    - **인증서 권한**
    - **발행된 인증서**
    - **사용자 제공 인증서**
2. **CSV로 내보내기**를 클릭합니다.
3. **다운로드**를 클릭합니다.
4. (선택 사항) 보고서를 삭제하려면 **삭제**를 클릭합니다.

# 12.2.5. 외부 인증기관용 SCEP 구성

이 기능을 사용하면 Windows 10 장치의 외부 인증 기관에 대한 SCEP(단순 인증서 등록 프로토콜) 구성을 지원할 수 있습니다.

> 이 구성에는 사용자 지정 배포 옵션을 사용한 위임을 사용할 수 있습니다. 자세한 정보는 구성 작업에서 *구성 배포* 항목을 참조하십시오.

## 외부 인증서 권한 설정

먼저 외부 CA를 설정해야 합니다. 이미 외부 CA가 있는 경우 다음 섹션으로 건너뛸 수 있습니다.

1. **관리자 > 인프라 > 인증서 관리**로 이동합니다.
2. **+추가**를 클릭합니다.
3. 인증서 권한의 이름을 입력합니다.
4. 풀다운 메뉴를 사용하여 Microsoft를 **인증 기관 유형**으로 선택합니다.
5. **SCEP URL**을 입력합니다.
6. **사용자 이름**과 **비밀번호**를 입력합니다.
7. **챌린지 URL**을 입력합니다.
8. **저장**을 클릭하세요.

## SCEP 구성

이제 SCEP 구성으로 진행할 수 있습니다.

1. **구성 > +추가**로 이동합니다.
2. Windows 아이콘을 선택합니다.
3. **ID 인증서**를 선택하여 **ID 인증서 구성 생성** 페이지로 이동합니다.
4. 구성 이름을 입력합니다.
5. **인증서 배포** 풀다운 메뉴의 SCEP 구성 목록에서 **Windows 구성**을 선택합니다.
6. 외부 CA를 선택합니다.
7. 인증서 배포 상세 정보를 입력합니다.
   - 소유자를 입력합니다. 예: CN=$
   - **재시도** 풀다운 메뉴에서 재시도 횟수를 선택합니다.
   - **재시도 지연** 풀다운 메뉴의 각 입력 전에 기다려야 하는 시간(초)을 선택합니다.
   - **키 길이** 풀다운 메뉴에서 키 크기를 선택합니다.
   - 최소한 한 개의 인증서 사용 옵션을 선택합니다.
   - **유효성** 필드 및 풀다운 메뉴에 기간을 입력합니다.
   - CA 지문을 입력합니다.
   - SCEP 챌린지 URL로 이동한 후 CA 지문을 복사하여 이곳에 붙여넣거나 **인증서에서 생성**을 클릭하여 CA Thumbprint를 생성할 수 있는 인증서를 업로드합니다.
     **해시 알고리즘군** 옵션에서 하나 이상의 해시 알고리즘을 선택합니다.
8. **다음**을 클릭하세요.

# 12.2.6. 파생된 자격 증명 제공자

파생 자격 증명 제공자 페이지에서 인증서 배포에 사용된 파생 자격 증명 제공자 목록을 볼 수 있습니다. 어떤 파생 자격 증명 제공자를 기본값으로 설정할지 지정할 수 있으며, 사용하고 있는 다른 사용자 지정 파생 자격 증명 제공자를 추가할 수도 있습니다.

파생 자격 증명 제공자를 기본값으로 설정하는 방법:

1. **관리 > 파생 자격 증명 제공자**로 이동합니다. 다음 파생 자격 증명 제공자 목록이 페이지에 나타납니다.
    - **Entrust**
    - **Intercede**
    - **Purebred**
2. 기본값으로 설정할 공급자의 경우 **작업** 열에서 **기본값으로 설정**을 클릭합니다. 설정하면 제공자가 기본 자격 증명 제공자임을 나타내는 확인 표시 아이콘이 제공자의 **기본 제공자** 열 아래에 표시됩니다.

사용자 지정 파생 자격 증명 제공자를 추가하는 방법:

1. **관리 > 파생 자격 증명 제공자**로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. **이름** 열 아래의 텍스트 필드에 파생 자격 증명 제공자의 이름을 입력합니다.
4. **저장**을 클릭합니다.
   추가되면 ID 인증서 구성에서 파생 자격 증명 배포를 구성하는 동안 이 사용자 지정 파생 자격 증명 제공자를 **브랜드** 필드에서 선택 옵션으로 사용할 수 있습니다.

파생 자격 증명 제공자를 삭제하려면 **작업** 열에서 **삭제**를 클릭합니다.

> 기본값으로 설정된 파생 자격 증명 제공자는 삭제할 수 없습니다.

# 12.2.7. Connector

**라이센스:** Silver

MDM용 Ivanti Neurons Connector는 MDM용 Ivanti Neurons 서비스에서 LDAP 서버 또는 인증 기관(CA)과 같은 회사 리소스에 대한 액세스를 제공합니다. 액세스하고자 하는 리소스마다 하나의 Connector를 설정하십시오.

Microsoft Active Directory 또는 AWS(Amazon Web Service)에서 호스트하는 LDAP 서버를 사용한다면 AWS에서 MDM용 Ivanti Neurons Connector를 호스트할 수 있습니다. 온-프레미스 Connector가 필요하지 않습니다.

Connector는 최신 버전의 소프트웨어로 자동 업데이트됩니다.

최신 MDM용 Ivanti Neurons Connector 설치 안내서를 보려면 **https://help.ivanti.com/#106**에서 "Connector"를 검색하십시오.

## Connector 호스팅 옵션

데이터센터 또는 AWS(Amazon Web Service)에서 MDM용 Ivanti Neurons Connector 온프레미스를 호스트할 수 있습니다.

- AWS가 호스트하는 Microsoft Active Directory를 사용하거나 AWS에서 자체 관리되는 Microsoft Active Directory를 사용하는 경우 AWS에서 Connector를 호스트하십시오. 이 경우 Connector 온-프레미스가 필요하지 않습니다.
- LDAP 서버 또는 CA 같은 온-프레미스 리소스를 액세스하려면 Connector 온-프레미스를 설정하십시오.

### AWS에서 Connector 호스팅

고객은 다음과 같이 AWS가 호스트하는 Microsoft Active Directory 옵션을 사용하여 AWS에서 Connector를 호스트할 수 있습니다.

- Microsoft Active Directory용 AWS 디렉터리 서비스
- Amazon VPC에서 고객이 관리하는 Microsoft Active Directory

Microsoft Active Directory용 AWS 디렉터리 서비스에 대한 자세한 내용은 다음을 참조하십시오. **Https://aws.amazon.com/directoryservice**. Amazon VPC에서 Microsoft Windows Server 및 Microsoft Active Directory를 호스팅하는 것에 대한 AWS 문서를 참조하십시오. MDM용 Ivanti Neurons Connector는 Windows Server 2012, 2012 R2, 2015를 지원합니다.

### AWS에서 MDM용 Ivanti Neurons Connector AMI 설정

MDM용 Ivanti Neurons Connector AMI 설정 방법:

1. 관리자 자격 증명으로 AWS에 로그인합니다.
2. AWS 서비스 페이지에서 **컴퓨팅**의 **EC2**를 선택합니다.
3. **이미지**를 확장하고 좌측 창에서 **AMI**를 선택합니다.
4. 우측 창의 드롭다운 목록에서 **공용 이미지**를 선택합니다.
5. "mobileiron-kocab" 같은 키워드를 사용하여 MDM용 Ivanti Neurons 커넥터를 검색합니다.
6. 목록에서 최신 버전의 Connector를 선택하고 **실행**을 클릭합니다.
7. *MDM용 Ivanti Neurons Connector 설치 안내서*(https://help.ivanti.com/mi/help/en_us/cld/*<version>*/inst/default.htm에서 확인 가능, *버전*은 설치 중인 MDM용 Ivanti Neurons Connector의 버전을 말함)에서 "AWS에 MDM용 Ivanti Neurons Connector 배포" 섹션의 Connector 설치 지침을 따릅니다. 예를 들어, MDM용 Ivanti Neurons Connector 버전 74의 경우 https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm에서 가이드를 확인할 수 있습니다.

### Connector 온-프레미스 호스팅

데이터센터에서 MDM용 Ivanti Neurons Connector를 온프레미스로 호스트하려면 **Connector 다운로드**를 클릭하여 MDM용 Ivanti Neurons Connector를 다운로드하고 설치합니다. 다운로드한 패키지 콘텐츠의 압축을 풀고 패키지에 포함된 MDM용 Ivanti Neurons Connector 설치 가이드의 설정 지침을 따릅니다.

## Connector 로그 액세스

Connector 서비스에서 Connector 로그에 액세스하여 Connector 관련 문제를 해결하는 데 도움을 받을 수 있습니다. 시스템 관리자 또는 시스템 읽기 전용 역할을 가지고 있어야 합니다.

1. **관리 > 커넥터**로 이동하여 커넥터 페이지를 확인합니다.
   Connector 인터페이스는 Connector 상태(활성화 또는 비활성화), Connector 이름, 연결(연결됨 또는 연결되지 않음), 버전 번호, 로깅 레벨, 작업(Connector 비활성화 또는 제거)을 표시합니다.
2. **로깅 수준** 풀다운 메뉴를 이용해 수준을 선택합니다.
   이용 가능한 로깅 레벨은 풀다운 메뉴에 가장 낮은 로깅 레벨부터 가장 높은 로깅 레벨 순으로 표시됩니다.
   - 오류
   - 경고
   - 정보
   - 디버그
   - 추적

정보 레벨은 기본 로깅 레벨 설정입니다. 다른 로깅 레벨을 선택하는 경우, 회전하는 동기화 아이콘()이 나타나 선택한 로깅 레벨에서 정보가 수집되고 있음을 표시합니다. 한 시간 후 로깅 레벨이 정보 레벨로 재설정됩니다. 추적 레벨은 가장 높은 로깅 레벨 설정입니다. 이 레벨을 사용해 모든 다른 레벨의 메시지를 수집합니다. 요청 기간 동안 동기화 아이콘이 표시됩니다.

3. 필요한 경우 동기화 아이콘 을 마우스로 가리키면 취소 아이콘 이 표시됩니다. 취소 아이콘을 클릭하여 로깅 레벨 변경을 취소합니다.
4. 요청 아이콘을 마우스로 가리켜 요청 정보를 확인합니다. 요청 아이콘()을 클릭해 현 로그 폴더의 파일을 .zip 파일로 요청합니다.
   요청에 성공하면 로그 파일이 .zip 파일에 추가됩니다.  새 요청이 이루어지면 이전 요청의 .zip 파일은 삭제됩니다.
5. 필요한 경우 요청 아이콘()을 마우스로 가리키면 취소 아이콘()이 됩니다. 취소 아이콘을 클릭해 요청을 중지합니다.
   요청이 완료되기 전에 취소하면, 이전 로그 .zip 파일이 서버에서 삭제되므로 다운로드 아이콘 이 표시되지 않습니다. Connector의 원래 로그 파일을 여전히 요청에 사용할 수 있습니다.
6. 요청이 완료되면 다운로드 아이콘()을 클릭해 최신 요청에서 수집된 로그 파일을 포함한 로그 .zip 파일을 다운로드합니다.
   로그 파일의 이름은 kocab.log와 같은 형식입니다. 다운로드한 zip 파일의 이름에는 서버 이름과 연결 버전, 연, 월, 일, 시간을 포함한 타임스탬프로 구성되며 그 형식은 <Connector_Hostname>_<Connector_Version>_<TimeStamp>.zip과 같습니다. 보관된 .zip 파일 이름의 형식은 kocab.yyyy-mm-dd.0.log.gz와 같습니다.
7. 필요 시 **작업** 풀다운 메뉴를 이용해 커넥터를 비활성화하거나 삭제합니다.

**커넥터** 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 시스템 읽기 전용

자세한 내용은 **Connector용 httpproxy 명령 사용**을 참조하십시오.

# 12.2.8. Connector용 httpproxy 명령 사용

MDM용 Ivanti Neurons 설치를 위해 Connector 구성을 편집할 수 있도록 klish 쉘 명령이 새로 생성되었습니다. 이 명령으로 로그인 정보 및 다른 매개변수를 변경하여 커넥터를 구성할 수 있습니다.

현재 릴리즈에서는 이 요건과 함께 httpproxy 명령을 사용할 수 있습니다.

- klish 쉘

Connector 구성 방법

1. klish 쉘에 로그인합니다.
2. 사용할 수 있는 klish 쉘 명령 목록에 대해 ?를 입력합니다.
3. **httpproxy**를 입력하여 이 매개 변수의 현재 값을 표시합니다.
    1. 활성화됨
    2. 체계
    3. 서버
    4. 인증 유형
    5. 사용자 이름
    6. 비밀번호
4. **httpproxy ?**를 입력하여 httpproxy와 함께 사용할 수 있는 명령 목록을 확인합니다.
    1. 인증 유형 - http 프록시의 인증 유형을 NONE, BASIC 또는 NTLM으로 설정
    2. 비활성화 - http 프록시 비활성화
    3. 활성화 - http 프록시 활성화
    4. 호스트 - http 프록시 호스트 설정 - FQDN 또는 IP이거나 http 또는 https이어야 합니다.
    5. 비밀번호 - http 프록시의 인증 비밀번호 설정
    6. 포트 - http 프록시의 포트 설정
    7. 체계 - http 프록시의 체계 설정 - http 또는 https이어야 합니다.
    8. 표시 - 현재 http 프록시 설정 표시
    9. 사용자 이름 - http 프록시의 인증 사용자 이름 설정
5. 위에 나열된 명령을 사용하여 Connector 인스턴스를 설정합니다.

# 12.2.9. Help@Work

**라이센스:** Platinum

**지원되는 기기:** MDM용 Ivanti Neurons에서 지원하는 Android 및 iOS 기기

Android/iOS용 Help@Work를 사용하여 Android 및 iOS 기기 사용자에게 원격 지원을 제공합니다. Android/iOS용 Help@Work는 TeamViewer QuickSupport 앱을 기반으로 합니다. Android/iOS용 Help@Work를 사용하려면 TeamViewer 계정이 필요합니다. 계정이 없는 경우, teamviewer.com을 방문하여 세부 정보를 확인하십시오.

Help@Work는 사용자가 클릭 한 번으로 도움을 요청하고 헬프 데스크 에이전트로 화면을 공유하도록 하여 iOS 11.0+ 및 Android 기기의 헬프 데스크 경험을 변화시킵니다. 사용자는 문제를 말하는데 소중한 시간을 버리지 않아도 되며, IT 직원은 더 효율적으로 기기 문제를 해결할 수 있습니다. 이는 MAM-only iOS 기기에서는 지원되지 않습니다.

> TeamViewer는 Android 기기 소유자 기기에서 키오스크 모드로 지원됩니다.

> 앱이 종료되거나 기기가 재부팅되면 TeamViewer 시작 명령이 더 이상 존재하지 않습니다.

> Android 기기에 TeamViewer QuickSupport 앱이 설치되어 있지 않으면 앱을 다운로드하라는 메시지가 표시됩니다. iOS 기기에서는 App Catalog를 통해 앱 푸시 요청을 해야 하며, 기기에 이미 설치되어 있는 경우에는 관리되는 앱으로 변환시켜야 합니다.

> 세션이 애플리케이션에 적용되도록 하려면 TeamViewer QuickSupport 앱이 포그라운드에 있어야 합니다. 무인 모드에는 TeamViewer 호스트 앱이 필요합니다.

> 원격 세션을 지원하려면 관리자가 설치하는 데스크톱 애플리케이션이 클라이언트 기기에 설치된 QuickSupport 버전과 호환되어야 합니다.

## Android 또는 iOS용 Help@Work 설정

다음은 Android 또는 iOS용 Help@Work의 브랜딩 및 배포를 위한 원스탑 설정 단계입니다.

1. **관리자** 탭으로 이동합니다.
2. 인프라에서 **Help@Work**를 클릭합니다.
3. **Help@Work**에는 TeamViewer가 필요합니다. TeamViewer 활성화 섹션에서 **지금 활성화** 버튼을 클릭하여 **TeamViewer 참석** 또는 **TeamViewer 무인(Android 전용)** 옵션을 활성화합니다.
4. TeamViewer 라이센스 계약서를 검토하고 계속하려면 **동의**를 클릭합니다. 이제 엔터프라이즈 라이센스가 활성화되었습니다. 이 과정은 TeamViewer에서 Ivanti 고객을 식별하여 액세스가 허용되도록 합니다.

> TeamViewer를 활성화하면 **활성화 제거** 옵션을 사용할 수 있습니다. **TeamViewer 활성화** 섹션 아래의 **활성화 제거**를 클릭하면 화면에 **활성화 제거 확인** 창이 표시됩니다. TeamViewer 활성화를 제거하려면 **활성화 제거**를 클릭합니다. 클릭하면 지원되는 모든 기기에서 Help@Work 기능이 제거됩니다. 하지만 기존 계정이나 다른 계정을 사용하여 나중에 언제든지 다시 활성화할 수 있습니다.

> 무인 모드에서 **TeamViewer** 계정을 삭제하고 싶은 경우에는 무인 모드가 활성화된 연결 기기의 프로비저닝을 해제해야 합니다. 연결 기기의 프로비저닝을 해제하려면 연결 기기에서 **TeamViewer** 앱의 배포를 해제하고 강제 체크인해야 합니다. 모든 기기에서 TeamViewer 앱을 삭제한 후 관리 콘솔에서 계정 바인딩을 삭제하십시오.

기본 앱 배포 워크플로우를 사용하여 원격 세션을 시작하려는 사용자에게 TeamViewer 앱을 배포합니다. 이는 **참석** 및 **무인** 모드에만 해당됩니다. 관리자가 기기를 제어하려면 TeamViewer의 범용 추가 기능 또는 OEM/모델별 추가 기능도 기기에 배포해야 합니다. 자세한 지침은 앱 구성을 참조하십시오.

## Android 또는 iOS용 Help@Work를 사용하여 원격 세션 시작하기

일반적인 Android 또는 iOS용 Help@Work 세션은 도움이 필요한 최종 사용자로 시작합니다.

사용자 기기에서 Help@Work 세션을 시작하는 방법:

1. MDM용 Ivanti Neurons에서 **기기**로 이동합니다.
2. 기기 목록 페이지에서 지원이 필요한 기기를 클릭합니다.
3. 작업 메뉴에서 Android 기기인 경우 **TeamViewer 원격 제어 시작**, iOS 기기인 경우 **원격 디스플레이**를 클릭합니다. 두 가지 옵션이 표시됩니다.
    - 참석 모드(기본값) - 대상 기기에 **TeamViewer 빠른 지원** 앱을 설치하고 허용 목록에 추가해야 합니다.
    - 무인 모드(Android 기기에서만 사용 가능) - 대상 기기에 **TeamViewer 호스트** 앱을 설치하고 허용 목록에 추가해야 합니다.

> 호스트 이름을 화이트리스트에 추가하거나 콘텐츠 보안 정책을 재정의하려면 지원 팀에 문의하십시오.

> 무인 모드 옵션은 키오스크 모드에서도 작동합니다. 또한, TeamViewer 통합 페이지에서 활성화해야 합니다. 무인 원격 제어를 사용하려면 기기의 TeamViewer 호스트 앱, 기기의 1회 활성화 및 MI 추가 기능 라이선스가 필요합니다. 일회성 활성화의 경우 TeamViewer 호스트 앱을 설치하고 처음 실행할 때 권한 프롬프트가 표시됩니다. 원할 경우 관리자는 설치 후 "자동 시작(관리 앱 구성의 설정)" TeamViewer 앱을 사용할 수 있습니다. 라이선스 수는 TeamViewer 호스트 앱 배포를 기준으로 계산됩니다. TeamViewer 호스트 앱이 기기에 배포되는 경우 하나의 무인 원격 호스트 세션 라이선스가 사용됩니다. TeamViewer 호스트 앱 외에도 다른 추가 기능 앱이 필요할 수 있으며 키오스크 또는 공유 키오스크 모드에서 허용되어야 합니다. 장치 모델 및 제조업체에 따라 다른 추가 기능이 필요할 수 있습니다.

> Google Pixel 장치는 이 권한 승인을 유지하지 않으며, 세션마다 매번 권한에 동의해야 합니다.

관리자에게 유효한 TeamViewer 토큰이 있는 경우 데스크톱 클라이언트가 기기에 대한 지원 세션을 시작합니다. 그렇지 않으면 관리자가 TeamViewer에 로그인하여 권한을 부여해야 합니다.

제거 세션을 빠르게 시작하기 위해 관리자가 미리 데스크톱 애플리케이션에 로그인할 수 있습니다.

## TeamViewer 설치하기

TeamViewer 앱을 데스크톱에 설치하여 사용자의 원격 기기에 액세스하여 이에 대한 지원을 제공합니다. TeamViewer를 설치하려면

1. 다음 사이트에서 Mac, Windows 또는 Android용 TeamViewer 풀버전용 설치 패키지를 다운로드해야 합니다. https://www.teamviewer.com/en/download/
2. TeamViewer 설치 프로그램을 시작합니다.
3. **기본 설치**를 선택합니다.
4. **회사/상업용**을 선택합니다.

5. **수락 - 완료**를 클릭합니다.

## TeamViewer 계정 요청하기

TeamViewer를 이용하여 지원을 제공하려면 TeamViewer 계정이 있어야 합니다. TeamViewer 계정을 얻으려면

1. https://login.teamviewer.com/으로 이동합니다.
2. 이메일, 이름 및 비밀번호를 입력합니다.
3. **가입**을 클릭합니다.
4. 2단계에서 입력한 이메일 계정을 이용하여 TeamViewer 계정 활성화 이메일을 받습니다.
5. 이메일에 기재된 지침에 따라 TeamViewer 계정을 활성화합니다.

## TeamViewer 세션 ID 확인하기

관리자의 컴퓨터와 사용자의 모바일 기기가 연결되면 TeamViewer가 세션 ID를 생성합니다.

1. 세션 ID가 생성되면 MDM용 Ivanti Neurons가 관리되는 앱 구성을 사용하여 생성된 세션 ID를 TeamViewer QuickSupport 앱에 전송하고, 이 세션 ID를 이용해 기기에 TeamViewer 클라이언트를 호출합니다. iOS의 경우 세션 ID는 30분 후에 만료됩니다.
2. TeamViewer EULA 동의 메시지가 표시됩니다.

# 12.2.10. 인프라 ID

이 섹션에는 다음 주제가 포함됩니다.

# 12.2.10.1. ID 제공자 구성

**라이센스:**Silver

ID 제공자(IdP)를 구성하여 MDM용 Ivanti Neurons에 기기 등록을 원하는 사용자를 인증하거나 이 관리자 포털 또는 셀프 서비스 포털에 액세스합니다. 사내 LDAP 호환 사용자 디렉터리가 필요합니다. MDM용 Ivanti Neurons는 모든 SAML 2.0 호환 IdP에서 작동합니다. Microsoft Entra ID 인증(Entra ID), Microsoft ADFS(Active Directory Federation Services), Okta, OneLogin, PingOne, Ping ID의 PingFederate는 MDM용 Ivanti Neurons와 호환되는 것으로 확인되었습니다.

이전에는 SAML 인증/IdP를 설정할 경우 기기 등록 및 포털 인증에 모두 SAML 인증이 사용되었습니다. 이제 관리자 포털 액세스 및 장치 등록을 위한 다양한 인증 방법을 선택할 수 있는 토글 버튼이 프로비저닝됩니다. 바이패스 토글은 장치 등록에만 적용 가능합니다.

기기 등록 중에 관리자는 ID 제공자 옵션을 무시하고 ID 제공자 페이지를 사용한 인증 대신 PIN을 사용하여 인증하는 옵션을 사용자에게 제공할 수 있습니다.

## 개요

- Microsoft AD 또는 다른 온프레미스 LDAP 디렉토리를 사용 중인 경우, Connector를 설정하여 사용자와 연결하고 사용자를 MDM용 Ivanti Neurons에 가져와야 합니다. 이미 완료하지 않았다면 Connector 또는 **LDAP**를 설정합니다.
- ID 제공자를 추가하면 사용자 인증이 LDAP에서 ID 제공자로 자동 전환됩니다.
- ID 제공자는 1개만 허용됩니다.
- IdP에 액세스할 수 없는 경우에는 MDM용 Ivanti Neurons 테넌트 관리자(TA) 계정으로 이 관리자 포털에 액세스하여 문제를 해결할 수 있습니다. TA는 로컬 계정이므로 외부 인증이 필요 없습니다. TA 계정은 MDM용 Ivanti Neurons가 프로비저닝되고 있으며 정보를 조직의 기술 담당자 또는 그에 준하는 담당자에게 제공했을 경우 생성됩니다. TA 계정 정보가 없다면 지원 담당자에게 문의하십시오.
- MDM용 Ivanti Neurons는 Windows 10 기기 등록 시 사용자 인증에 Microsoft Entra ID(Entra ID)를 지원합니다.

> IdP 공급업체가 제공한 도구로 LDAP 사용자의 인증 유형을 설정합니다. IdP 인증 체계는 MDM용 Ivanti Neurons 설정보다 우선합니다. MDM용 Ivanti Neurons 인증 설정은 **사용자 > 사용자 설정 > 기기 등록 설정 > 기기 등록 인증 유형**에서 확인할 수 있습니다.

- Apple 기기 등록과 Configurator 기기 등록은 사용자 인증에 IdP를 사용하지 않습니다.
- Apple Business Manager iOS 및 macOS 기기 등록을 위해 작동하도록 ID 공급자를 구성하려면 **관리 > Apple > 기기 등록 >** *기기 등록 프로필 편집*에 있는 **사용자 지정 등록 활성화** 및 관련 **Ivanti 호스팅 웹페이지** 설정을 활성화해야 합니다.자세한 내용은 **기기 등록**을 참조하십시오.



## IdP 설정 유형

MDM용 Ivanti Neurons ID 페이지에서 다음의 IdP 제공자 유형 설정에 대해 안내합니다.

- **MDM용 Ivanti Neurons IdP 설정** - 지원되는 MDM용 Ivanti Neurons IdP 제공자는 Entra ID, OneLogin, Okta, PingOne입니다.
- **온 프레미스 IdP 설정** - 지원되는 온 프레미스 IdP 제공자는 ADFS 3.0, PingFederate 8.2.1 및 PingFederate 8.1.3입니다.
- **일반 IdP 설정** - 이는 Microsoft ADFS, Okta, OneLogin 또는 PingFederate를 사용하지 않는 경우 사용할 수 있는 일반 설정 경로입니다.

## ID 제공자(IdP) 구성

**절차**

1. **관리** > **ID** > **SAML 인증**으로 이동합니다.

2. ID 공급자 설정 유형을 클릭합니다.
    - **MDM용 Ivanti Neurons IDP 설정**
    - **온-프레미스 IDP 설정**
    - **일반 IDP 설정**
3. 해당하는 IdP를 선택합니다. 3단계에서 **일반 IDP 설정**을 선택한 경우 이 단계를 건너뛰고 5단계로 넘어갑니다.
4. 선택한 IdP에 대해 화면에 표시되는 지침을 따릅니다.
5. **완료**를 클릭하세요.

> 관리자는 IdP를 통한 최초 인증 후 최대 2시간까지 Single Sign-On이 허용됩니다.

## 완료해야 하는 작업 설정

선택한 IdP에 따라 다음 관련 페이지 및 단계로 이동하게 됩니다.

| ID 제공자 | 절차 |
| --- | --- |
| • Entra ID<br>• Okta<br>• OneLogin<br>• PingOne | • IdP에 업로드할 키 생성하기.<br>• IdP에 로그인하여 생성된 키 업로드하기.<br>• IdP에서 메타데이터 파일을 내보내고 이를 MDM용 Ivanti Neurons로 가져옵니다. |
| • ADSF 3.0<br>• PingFederate 8.2.1<br>• PingFederate 8.1.3 | • MDM용 Ivanti Neurons에서 메타데이터 파일을 다운로드합니다.<br>• ADFS에서 "신뢰 당사자 트러스트"를 설정하거나 PingFederate에서 “SP 연결”을 설정하고 MDM용 Ivanti Neurons 메타데이터 파일을 가져옵니다.<br>• IdP에서 메타데이터 파일을 내보내고 이를 MDM용 Ivanti Neurons로 가져옵니다. |
| • 일반 IdP | 1. MDM용 Ivanti Neurons에서 메타데이터 파일을 다운로드합니다.<br>2. IdP 공급업체가 제공한 지침에 따라 IdP 서버 또는 서비스가 "서비스 공급자"로 MDM용 Ivanti Neurons 서비스와 통신하도록 구성합니다. 여기에는 다음이 포함될 수 있습니다.<br>1. 위의 1단계에서 받은 메타데이터 파일을 IdP로 업로드합니다. 이 구성 파일에는 SAML 2.0 서비스 공급자인 MDM용 Ivanti Neurons에서 SAML 2.0 ID 공급자와 통신할 수 있는 필수 정보가 포함되어 있습니다. 표준 SAML 2.0 URL, 인증서 및 설정은 메타데이터 파일에 포함되어 있습니다.<br>MDM용 Ivanti Neurons 은(는) SAML 2.0 호환 IdP에는 서비스 공급자에서 내보낸 XML 메타데이터를 가져와서 처리할 수 있는 기능이 있을 것으로 예상합니다.<br>2. IdP를 구성하여 SAML 인증 요청을 서명하기 위해 RSA-SHA1 사용하기. 인증 요청을 확인하는 데 사용되는 서명 인증서에 관한 정보는 1단계에서 다운로드한 메타데이터 파일에 포함되어 있습니다.<br>3. MDM용 Ivanti Neurons(으)로 전송한 SAML 응답에 사용자 이름을 포함하도록 IdP를 구성합니다. IdP의 SAML 응답의 [Name ID] 요소에서 사용자 이름을 지정합니다.<br>IdP에서 메타데이터 파일을 내보내고 이를 MDM용 Ivanti Neurons(으)로 가져옵니다.<br>3. (선택 사항) - SAML 인증 요청에 사용자 이름 포함: 인증 요청에 인증하려는 사용자의 사용자 이름을 포함하고 IdP를 통한 인증 시 추가 사용자 입력을 제거합니다. 이 옵션을 활성화하면 인증 실패가 발생할 수 있습니다. IdP 유효성 검사에 대해 확신하는 경우, **이 변경으로 인한 영향을 이해합니다** 옵션을 선택하고 **SAML 인증 요청에 사용자 이름 포함** 설정을 **ON**으로 토글합니다.<br>Ivanti Access는 이 설정에 대해 유효성 검사된 IdP입니다. |

## 로컬 사용자가 IdP 인증을 우회할 수 있도록 지원

IdP 또는 MDM용 Ivanti Neurons 연결이 중지되어 MDM용 Ivanti Neurons 측에서 문제 해결이 필요한 경우, 특정 관리자는 인증을 위해 LDAP 또는 IdP와 같은 외부 시스템에 의존하지 않고 MDM용 Ivanti Neurons에 로그인할 수 있는 권한이 필요합니다. 시스템 관리 역할을 가진 로컬 사용자만 IdP 인증을 우회할 수 있습니다.

IdP 인증을 우회할 로컬 사용자 목록을 생성합니다.

**절차**

1. **관리 > ID**를 클릭합니다.
2. IdP 인증을 우회할 로컬 사용자 섹션 아래에서 **+사용자 추가**를 클릭합니다.
3. 시스템 관리 역할을 가진 로컬 사용자만 표시하는 목록에서 일부 사용자를 선택합니다.
4. **저장**을 클릭하세요.

> IdP 인증을 우회하는 로컬 사용자 목록에서 사용자를 삭제하려면 삭제하려는 항목 옆의 삭제 아이콘을 클릭합니다.

ID 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 시스템 읽기 전용

# 12.2.10.2. SCIM을 사용한 사용자 프로비저닝

이 섹션에는 다음 주제가 포함됩니다.


- 사용자 프로비저닝
- 에서 토큰 생성 MDM용 Ivanti Neurons
- 토큰 상태 변경
- 감사 추적에서 토큰 상태 보기
- SCIM 프로비저닝에서 속성 구성


## 사용자 프로비저닝

사용자 프로비저닝은 SCIM 프로토콜을 사용하여 IDP를 MDM용 Ivanti Neurons에 동기화하고 부분 사용자 및 그룹 동기화를 허용합니다. 사용자 프로비저닝은 SCIM 프로토콜을 사용하여 IDP에서 MDM용 Ivanti Neurons에 소싱된 사용자 및 그룹 객체를 자동으로 만들고 업데이트합니다. Entra ID, Okta와의 현재 통합과 마찬가지로 사용자 및 그룹 프로비저닝 프로세스가 자동화됩니다. IDP에서 사용자 또는 그룹이 변경되면 동일한 변경사항이 MDM용 Ivanti Neurons에 반영됩니다.

> SCIM을 통해 프로비저닝된 사용자의 사용자 이름은 사용자 이름이 MDM용 Ivanti Neurons에서 고유한 경우 ID 공급자(IdP)에서 이름을 변경할 수 있습니다.

> SCIM 사용자와 그룹은 이제 해당 외부 ID를 사용하여 검색할 수 있습니다.

## 에서 토큰 생성 MDM용 Ivanti Neurons

IDP에 대한 사용자 프로비저닝을 시작하려면 MDM용 Ivanti Neurons에서 토큰과 대상 URL을 생성합니다.

> 토큰과 대상 URL을 저장했는지 확인하십시오.

> 언제든 최대 2개의 토큰을 생성할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **관리** > **ID** > **사용자 프로비저닝**으로 이동합니다.
3. 드롭다운 목록에서 ID 공급자(IDP)를 선택합니다.
4. 새 토큰을 생성하려면 **생성**을 클릭합니다. 알림 메시지가 나타나면 **생성**을 클릭합니다. 토큰과 대상 SCIM URL의 세부 정보가 포함된 새 페이지가 열립니다.
5. **복사**를 클릭하여 토큰 또는 SCIM URL을 복사합니다.
6. 페이지를 새로 고칩니다. **사용자 프로비저닝** 페이지에 토큰 상태 테이블이 표시됩니다.

## 토큰 상태 변경

기존 토큰의 상태를 변경할 수 있습니다.

**절차**

1. **사용자 프로비저닝 Entra ID** 페이지에서 **선택** 드롭다운 메뉴를 클릭합니다.
2. **선택**을 클릭하여 토큰을 다음과 같이 변경합니다.
    - **활성으로 설정**
    - **비활성으로 설정**
    - **갱신**
    - **제거**

## 감사 추적에서 토큰 상태 보기

감사 추적 섹션에서 SCIM 토큰에 발생한 작업/이벤트 로그를 볼 수 있습니다. SCIM 토큰은 다음 상태 중 하나일 수 있습니다.

- SCIM 토큰 생성됨 - SCIM 토큰이 생성되었습니다.
- SCIM 토큰 활성화됨 - SCIM 토큰이 활성화되었습니다.
- SCIM 토큰 비활성화됨 - SCIM 토큰이 비활성화되었습니다.
- SCIM 토큰 갱신됨 - SCIM 토큰이 갱신되었습니다.
- SCIM 토큰 삭제됨 - SCIM 토큰이 삭제되었습니다.

DETAILS 열에는 Azure, Okta 등과 같은 SCIM 공급업체 이름(IDP)도 나열됩니다. 이로써 MDM용 Ivanti Neurons 간의 통신이 용이해집니다.

## SCIM 프로비저닝에서 속성 구성

이 섹션에서는 사용자 프로비저닝 중에 IDP에 대한 사용자 지정 및 엔터프라이즈 속성을 만드는 방법을 설명합니다.

## 매핑 속성

연결이 설정된 후 IDP와 MDM용 Ivanti Neurons 간에 속성을 매핑할 수 있습니다. MDM용 Ivanti Neurons 은(는) 다음과 같은 사용자 속성을 지원합니다:

### 주요 속성

- id
- userName
- displayname
- active
- givenName
- familyName
- emails

> Entra ID IDP의 경우 외부 IDP가 지원됩니다.

### 업데이트 작업이 허용되는 속성 목록

- userName
- displayName
- emails

- givenName
- familyName
- active
- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

## 사용자 지정 속성

**스키마** - urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

## 엔터프라이즈 속성

현재 부서 특성만 지원됩니다.

**스키마** - urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

# 12.2.10.2.1. Entra ID IDP의 사용자 프로비저닝

이 섹션에는 다음 주제가 포함됩니다.


- MDM용 Ivanti Neurons와(과) 연결 설정와(과) 연결 설정
- 할당된 사용자 및 그룹 프로비저닝
- 모든 사용자 및 그룹 프로비저닝
- 할당된 사용자 프로비저닝 확인
- Entra ID IDP의 사용자 프로비저닝
- 설정 편집
- 사용자 정의 및 엔터프라이즈 속성 구성
- 마이그레이션 고려 사항 - Entra ID 사용자 소스에서 사용자 프로비저닝 SCIM으로
- 마이그레이션 고려 사항 - LDAP에서 사용자 프로비저닝 SCIM으로
- 중요 사항 - SCIM


## MDM용 Ivanti Neurons와(과) 연결 설정

Entra ID Enterprise 애플리케이션에서 사용자와 그룹을 생성한 후에는 Entra ID와 MDM용 Ivanti Neurons 간의 연결을 구축할 수 있습니다.

**절차**

1. Entra ID 포털로 로그인합니다.
2. **엔터프라이즈 애플리케이션**으로 이동하여 **+ 나만의 애플리케이션 만들기**를 클릭합니다. 나만의 애플리케이션 만들기 창이 열립니다.
3. 앱 이름(**기본값: 비갤러리**)을 지정하고 **만들기**를 클릭합니다. MDM용 Ivanti Neurons 사용자 프로비저닝을 예로 들 수 있습니다.
4. **프로비저닝** > **프로비저닝 편집** > **관리자 자격 증명**으로 이동합니다.
5. MDM용 Ivanti Neurons 관리 포털에서 대상 SCIM URL을 복사하여 Entra ID 포털의 **테넌트 URL** 필드에 붙여 넣습니다.
6. MDM용 Ivanti Neurons에서 토큰을 복사하여 Entra ID 포털의 **보안 토큰** 필드에 붙여 넣습니다.
7. 다음 작업 중 하나를 수행합니다.
   - **할당된 사용자 및 그룹만 동기화**를 선택합니다. 자세한 내용은 할당된 사용자 및 그룹 프로비저닝을 참조하십시오.
   - **모든 사용자 및 그룹 동기화**를 선택합니다. 자세한 내용은 모든 사용자 및 그룹 프로비저닝을 참조하십시오.

   > 사용자를 마이그레이션하려면 모든 사용자 및 그룹 동기화 옵션을 선택합니다.

**테스트 연결**을 클릭합니다. 연결되었음을 알려주는 초록색 체크 표시가 있는 팝업 상자가 나타납니다.

9. **저장**을 클릭하세요.
10. Entra ID 포털의 **프로비저닝** 페이지에서 **매핑**을 확장합니다.
11. **Entra ID 사용자 프로비저닝**을 클릭합니다. 속성 매핑 페이지가 열립니다.
12. **삭제**를 클릭하여 지원되지 않는 속성을 삭제합니다.

## 할당된 사용자 및 그룹 프로비저닝

Entra ID와 MDM용 Ivanti Neurons 간에 연결이 설정된 후 사용자 또는 그룹을 프로비저닝할 수 있습니다.

그룹을 프로비저닝할 때 Entra ID는 선택한 그룹에 중첩된 그룹의 구성원을 추가하지 않습니다. Entra ID는 동기화 프로세스 중에 하위 그룹 구성원이 아닌 그룹에만 직속 구성원 및 그룹 이름을 추가합니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. 애플리케이션에서 **사용자 및 그룹**으로 이동하여 **+ 사용자/그룹 추가**를 클릭합니다. 할당 추가 페이지가 열립니다.
3. **검색** 필드에서 사용자 또는 그룹을 검색하고 **선택**을 클릭한 다음 **할당**을 클릭합니다. 사용자 및 그룹 페이지가 열립니다.
4. 해당 사용자 또는 그룹 확인란을 선택합니다.
5. **프로비저닝**을 클릭한 다음 **프로비저닝 시작**을 클릭합니다. 성공한 구성의 세부 정보가 표시됩니다.

## 모든 사용자 및 그룹 프로비저닝

Entra ID와 MDM용 Ivanti Neurons 간의 연결이 구축된 후 사용자 또는 그룹을 프로비저닝할 수 있습니다.

**절차**

- **프로비저닝**을 클릭한 다음 **프로비저닝 시작**을 클릭합니다. 성공적인 프로비저닝의 세부 정보가 포함된 페이지가 열리고, 사용자는 MDM용 Ivanti Neurons에 프로비저닝됩니다.

## 할당된 사용자 프로비저닝 확인

할당된 사용자가 Entra ID 포털에서 프로비저닝된 후 MDM용 Ivanti Neurons 관리 포털에서 프로비저닝을 확인합니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. 주 메뉴에서 **사용자** 탭으로 이동합니다. 프로비저닝된 사용자가 이 페이지의 사용자 목록에 나타납니다.

프로비저닝 프로세스는 최대 1시간이 소요될 수 있습니다.

## 그룹 프로비저닝 확인

Entra ID 포털에서 그룹을 프로비저닝한 후 MDM용 Ivanti Neurons에서 프로비저닝을 확인합니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **사용자** 탭 > **사용자 그룹**으로 이동합니다. 프로비저닝된 그룹이 이 페이지의 그룹 목록에 나타납니다.

프로비저닝 프로세스는 최대 1시간이 소요될 수 있습니다.

## 설정 편집

본 항목은 Entra ID 설정을 구성하는 데 도움이 됩니다.

**절차**

1. **관리자 > Microsoft Azure > 사용자 프로비저닝 Entra ID**로 이동합니다.

2. **토큰 생성**을 클릭하고 토큰을 복사합니다.
3. 페이지를 새로 고칩니다. Entra ID 설정 페이지가 열립니다.
4. **설정 편집**을 클릭합니다.
5. **Entra ID에서 불러온 사용자를 자동으로 초대** 설정 - Entra ID에서 MDM용 Ivanti Neurons(으)로 불러온 사용자에게 자동으로 등록 초대 이메일을 보낼지 여부를 관리합니다.
6. **관리되는 Apple ID** 설정 - 이 옵션은 기본적으로 비활성화되어 있습니다. 토글 버튼을 클릭하여 활성화합니다. 관리되는 Apple ID는 프로비저닝 중에 다음 방법으로 설정할 수 있습니다:
   - **사용자 이메일 주소**
     - (선택 사항) "appleid" 하위 도메인 포함 옵션을 선택하여 기존 Apple ID와의 충돌을 방지합니다.
   - **사용자 정의 속성**으로 매핑

     > 사용자 정의 속성은 고유한 이메일 주소로 평가되어야 합니다.
7. (선택 사항) **사용자 지정 속성 추가** 클릭 - 장치 관리에 적용할 디렉터리 서비스의 사용자 지정 속성을 지정합니다. 이후 각 속성은 변수를 지원하는 구성 필드에서 ${속성이름}으로 지칭될 수 있습니다. 이 옵션을 사용하려면 Entra ID 서버 전체에 사용자 지정 속성을 일관적으로 구현해야 합니다. 구현에 포함된 Entra ID 서버가 이 속성을 사용하지 않을 경우 이 속성에 종속된 기능이 예상한 바와 같이 작동하지 않을 수 있습니다. **설정 편집** 섹션에 포함된 **사용자 지정 특성** 표에서 **특성 유형** 열에 **IDP** 특성이 표시됩니다.
8. Entra ID 설정을 수정한 후 변경사항 저장을 클릭합니다.

## 사용자 정의 및 엔터프라이즈 속성 구성

**절차**

1. **관리** > **ID** > **사용자 프로비저닝**으로 이동합니다.
2. **설정 편집**에서 **+사용자 지정 속성 추가**를 클릭합니다.
3. **속성 이름** 필드에 이름을 입력하고(예: custAttr1) **변경사항 저장**을 클릭하세요. 속성은 **관리** > **시스템** > **속성** 페이지에 나열되어 있어 이것을 사용하면 됩니다. 속성은 IDP 속성으로 표시되며 삭제 작업만 수행할 수 있습니다.
4. **Entra ID** 포털로 로그인합니다.
5. **홈** > **엔터프라이즈 애플리케이션**에서 SCIM 애플리케이션을 클릭합니다.
6. **매핑** 섹션에서 **Entra ID 사용자 프로비저닝**을 클릭합니다.
7. **고급 옵션 표시** 확인란을 선택합니다.
8. **customappsso에 대한 속성 목록 편집**을 클릭합니다.
9. MDM용 Ivanti Neurons UI에서 생성한 사용자 지정 속성에 새 항목을 입력합니다.
10. 다음과 같이 사용자 지정/엔터프라이즈(부서) 특성에 대한 스키마를 추가합니다.
    사용자 지정 속성 - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custAttr1> -** 3단계를 참조하십시오.
    엔터프라이즈 속성 - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
11. **변경사항 저장**을 클릭합니다.
12. **새 매핑 추가**를 클릭하고 드롭다운 메뉴에서 소스 및 대상 특성을 선택합니다.
13. **확인**을 클릭하고 **매핑 저장**을 클릭합니다.
14. **홈** > **엔터프라이즈 애플리케이션**에서 SCIM 애플리케이션 > **사용자 및 그룹**을 클릭합니다.
15. 사용자 이름을 클릭합니다. 프로필 페이지가 열립니다.
16. 속성과 연결된 값이 프로필 페이지에 나타나는지 확인합니다.

17. (선택 사항) SCIM 애플리케이션 > 프로비저닝 > 주문형 프로비저닝을 클릭하고 특정 사용자를 검색한 다음 프로비저닝을 클릭합니다. 이전 단계에서 수행된 새 속성 매핑의 유효성을 확인합니다.
18. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
19. **사용자** > **사용자**> 사용자 선택으로 이동합니다
20. **속성** 탭을 클릭한 후 속성 값을 확인합니다. 속성은 특정 사용자에 대해 매핑됩니다.

## 마이그레이션 고려 사항 - Entra ID 사용자 소스에서 사용자 프로비저닝 SCIM으로

- Entra ID 사용자 소스에서 사용자 프로비저닝 Entra ID(SCIM)로 마이그레이션할 때 모든 사용자 및 그룹 동기화를 선택합니다.
- 사용자 및 그룹이 SCIM Entra ID 소스로 업데이트된 후에는 Azure에서 Azure 프로비저닝 페이지로 돌아가서 할당된 사용자 및 그룹만 동기화 옵션을 통해 사용자 프로비저닝 Entra ID에서 관리할 특정 사용자 및 그룹을 설정합니다.
- 동기화가 완료되면 Azure에 정의되지 않은 사용자 및 그룹을 MDM용 Ivanti Neurons 사용자 및 그룹 목록에서 제거할 수 있습니다.
- 마이그레이션이 시작되면 Entra ID 사용자 소스 페이지에 읽기 전용 상태로 액세스할 수 있습니다.

## 마이그레이션 고려 사항 - LDAP에서 사용자 프로비저닝 SCIM으로

**전제 조건**:

1. **이 LDAP 서버 활성화** 옵션이 기본적으로 선택되어 있습니다. 마이그레이션하기 전에 이 옵션을 선택 취소해야 합니다.
2. Entra ID에서 Enterprise 앱을 만들고 동기화된 LDAP 사용자/그룹(Ivanti에 있는 동일한 LDAP 사용자/그룹)을 SCIM 앱에 추가합니다. 프로비저닝을 시작합니다.

**LDAP에서 SCIM으로 마이그레이션에 대한 주요 고려 사항**

- LDAP는 동기화된 사용자/그룹에 대한 모든 정보를 캡처하지 않는 반면, SCIM은 감사 로그에 사용자/그룹 이벤트를 기록합니다.
- 사용자 정의 속성이 있는 LDAP 사용자는 유형이 정의된 ldap을 가지며, SCIM의 경우 IdP입니다. 따라서 사용자 정의 속성이 있는 사용자가 LDAP에서 SCIM으로 마이그레이션되면 해당 IdP 사용자 정의 속성이 SCIM 앱에서 생성되어야 사용자가 마이그레이션됩니다. 사용자가 나중에 ldap 사용자 정의 속성을 업데이트하려는 경우 마이그레이션 후 MDM에서 ldap.custom 속성 값이 업데이트되지 않습니다. IdP 속성 값이 업데이트됩니다.
- 하나 이상의 사용자 정의 속성, 특히 "ldap.custAttr1"과 연결된 LDAP 사용자를 마이그레이션합니다. 이는 LDAP 기기 등록 및 LDAP 사용자 정의 속성 값에 해당하는 SAN 유형을 사용하여 기기에 푸시된 구성(ID 인증서 구성)을 나타냅니다.
- 이메일 주소와 연결된 관리되는 Apple ID가 있는 LDAP 사용자를 마이그레이션하려면 - LDAP에서 SCIM으로 마이그레이션하기 전에, LDAP 사용자의 관리되는 Apple ID 값을 유지하려면 SCIM 설정에서 관리되는 Apple ID를 활성화하고 해당 설정을 저장해야 합니다.
- LDAP 사용자가 LDAP 서버에서 제거되면 사용자는 여전히 활성 상태이지만 특정 동기화된 LDAP 사용자에 대해 동기화 플래그는 true로 설정되지 않습니다. SCIM의 경우 프로비저닝된 사용자 1명이 삭제되면 사용자 상태가 비활성화됩니다.
- SCIM 사용자의 ID 공급자(IdP)에 대해 SAML이 구성되면 로컬 및 LDAP와 같은 다양한 소스의 모든 사용자가 SAML을 통해 인증됩니다. IdP 인증 흐름을 우회하기 위해 로컬 사용자만 예외 목록에 추가할 수 있습니다. 이 구성은 **관리자** > **ID** > **SAML** 아래의 SAML 페이지에서 관리할 수 있습니다.
- 마이그레이션된 IDP(SCIM) 사용자에 대해 SAML이 구성되면 로컬 및 LDAP와 같은 다른 소스의 다른 사용자에 대해 기기 등록을 우회할 수 있습니다(IDP를 통하지 않음). 이는 **사용자** > **사용자 설정**에서 관리될 수 있습니다.
- LDAP에서는 사용자, 그룹, OU가 지원되는 반면, SCIM에서는 사용자와 그룹은 지원되지만 OU는 지원되지 않습니다.
- SCIM에서는 중첩된 그룹 프로비저닝 프로세스가 지원되지 않습니다.

## 중요 사항 - SCIM

- 이메일 주소는 사용자 또는 구성원을 프로비저닝하고 마이그레이션하기 위한 필수 필드입니다.

- SCIM은 Microsoft Entra ID에서 MDM용 Ivanti Neurons로 단방향 프로비저닝을 제공합니다. MDM용 Ivanti Neurons는 동기화 옵션을 제공하지 않습니다. MDM용 Ivanti Neurons에서 SCIM 프로비저닝된 그룹 또는 사용자를 삭제한 경우, Microsoft Entra ID에서도 사용자 또는 그룹을 제거해야 합니다.
- Microsoft Entra ID의 SCIM 애플리케이션 매핑 창에서 하나의 속성(소스 또는 대상)을 한 번만 사용할 수 있습니다. 동일한 소스를 특정 대상 속성에 두 번 매핑할 수 없습니다.
- 비활성 사용자는 SCIM을 사용하여 프로비저닝하거나 MDM용 Ivanti Neurons로 마이그레이션할 수 없습니다.
- 현재 MDM용 Ivanti Neurons는 SCIM 이벤트 알림을 지원하지 않습니다.
- 마이그레이션 또는 프로비저닝 기간은 관련된 사용자 또는 그룹의 수에 따라 다릅니다.
- Microsoft Azure는 프로비저닝 간격을 제어하며 약 40분 이상입니다.
- 다시 프로비저닝하는 동안 Microsoft Entra ID는 실패한 항목만 다시 시도합니다. 프로비저닝 로그를 다운로드하여 Microsoft Entra ID에서 프로비저닝에 성공하거나 실패한 사용자를 확인할 수 있습니다.
- 다른 소스의 중복 그룹은 SCIM에서 허용되지 않습니다.
- 프로비저닝된 사용자가 Microsoft Entra ID에서 영구 삭제되면 사용자는 MDM용 Ivanti Neurons에서 비활성화됩니다.
- 프로비저닝된 사용자 그룹이 Microsoft Entra ID에서 삭제되면 해당 그룹은 MDM용 Ivanti Neurons에서 삭제되며 삭제된 그룹에 속한 독립 구성원은 비활성화되고 모든 사용자 그룹에 연결됩니다.
- 프로비저닝된 그룹의 프로비저닝된 구성원이 Microsoft Entra ID에서 영구 삭제되면 구성원이 MDM용 Ivanti Neurons에서 비활성화되지만 구성원은 여전히 MDM용 Ivanti Neurons의 그룹에 연결됩니다.
- 속성(엔터프라이즈 속성 또는 사용자 지정 속성) 매핑이 앱에서 제거되면 제거된 속성 값이 여전히 MDM용 Ivanti Neurons에 반영됩니다.
- 프로비저닝된 사용자의 사용자 속성이 비어 있거나 빈 값으로 업데이트되면 업데이트된 속성 값이 MDM용 Ivanti Neurons에 반영되지 않습니다.
- Microsoft Entra ID에서 SCIM으로 마이그레이션 또는 업데이트하는 동안 사용자 속성 FName 및 LName(name.formatted)이 비어 있으면 마이그레이션 또는 업데이트가 실패합니다.
- Entra ID에서 사용자를 삭제하면 해당 SCIM API는 사용자를 영구적으로 삭제하는 대신 일시 삭제를 수행하고 사용자 상태를 활성에서 비활성으로 변경합니다. 사용자를 영구적으로 삭제하려면 MDM용 Ivanti Neurons 관리 포털에 로그인하고 비활성 사용자를 수동으로 삭제합니다.
- 로컬 사용자가 이미 특정 사용자 ID를 가지고 MDM용 Ivanti Neurons에 존재하는 경우, 동일한 사용자 ID를 가진 유사한 사용자가 Entra ID에서 MDM으로 프로비저닝되고 사용자 소스는 로컬에서 SCIM Entra ID로 업데이트됩니다.
- "Entra ID Premium P1" 구독이 포함된 Entra ID에는 할당 및 프로비저닝할 필수 그룹을 프로비저닝할 수 있는 권한이 있습니다.

# 12.2.10.2.2. Okta IDP의 사용자 프로비저닝

이 섹션에는 다음 주제가 포함됩니다.


- MDM용 Ivanti Neurons와(과) 연결 설정와(과) 연결 설정
- 사용자 및 그룹 프로비저닝
- 할당된 사용자 프로비저닝 확인
- 그룹 프로비저닝 확인
- 설정 편집
- SCIM 사용자 프로비저닝에서 사용자 지정 / 엔터프라이즈 속성 구성


## MDM용 Ivanti Neurons와(과) 연결 설정

**Okta** 애플리케이션에서 사용자와 그룹을 생성한 후 **Okta**와 MDM용 Ivanti Neurons 간의 연결을 설정할 수 있습니다.

**절차**

1. **Okta**에 로그인합니다.
2. **애플리케이션** > **애플리케이션** > **앱 카탈로그 찾아보기**로 이동합니다.
3. **SCIM 2.0 테스트 앱 추가**(OAuth 전달자 토큰)로 검색하고 앱을 설치합니다.
4. 앱을 클릭하고 **프로비저닝** > **통합**으로 이동합니다.
5. **편집**을 클릭하고 기본 URL을 입력한 후 생성된 토큰을 붙여 넣습니다.
6. **저장**을 클릭하세요.
7. **프로비저닝**으로 이동하여 **편집**을 클릭합니다.
8. 필요한 사용자 작업을 활성화하고 **저장**을 클릭합니다.

## 사용자 및 그룹 프로비저닝

**Okta**와 MDM용 Ivanti Neurons 간에 연결이 설정된 후 사용자 또는 그룹을 프로비저닝할 수 있습니다.

**절차**

1. **할당** > **할당** > **사람에게 할당** 또는 **그룹에 할당**으로 이동합니다.
2. 2. 기존 사용자 또는 그룹을 선택하거나 검색하고 **할당**을 클릭합니다.
3. **사용자** 또는 **그룹**을 더 추가하려면 이 과정을 반복하세요.
4. **완료**를 클릭하세요.
5. 그룹을 선택하고 **이름으로 그룹 푸시**를 클릭하여 저장하고 그룹을 동기화합니다.

## 할당된 사용자 프로비저닝 확인

할당된 사용자가 Okta 포털에서 프로비저닝된 후 MDM용 Ivanti Neurons 관리 포털에서 사용자 프로비저닝을 확인합니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. 주 메뉴에서 **사용자** 탭으로 이동합니다. 프로비저닝된 사용자가 이 페이지의 사용자 목록에 나타납니다.

## 그룹 프로비저닝 확인

Okta 포털에서 그룹을 프로비저닝한 후 MDM용 Ivanti Neurons에서 프로비저닝을 확인합니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털로 로그인합니다.
2. **사용자** 탭으로 이동하여 **사용자 그룹**을 클릭합니다. 프로비저닝된 사용자가 이 페이지의 그룹 목록에 나타납니다.

## 설정 편집

이 토픽은 Okta 설정을 구성하는 데 도움이 됩니다.

**절차**

1. **관리** > **ID** > **사용자 프로비저닝 Okta**로 이동합니다.
2. **설정 편집**을 클릭합니다.
3. **Okta에서 불러온 사용자를 자동으로 초대** 설정 - Okta에서 MDM용 Ivanti Neurons(으)로 불러온 사용자에게 자동으로 등록 초대 이메일을 보낼지 여부를 관리합니다.
4. (선택 사항) **사용자 지정 속성 추가** 클릭 - 장치 관리에 적용할 디렉터리 서비스의 사용자 지정 속성을 지정합니다. 변수를 지원하는 구성 필드에서 $을(를) 사용하여 각 속성을 참조할 수 있습니다. 이 옵션을 사용하려면 Okta 서버 전체에 사용자 지정 속성을 일관적으로 구현해야 합니다. 구현에 포함된 Okta 서버가 사용자 지정 속성을 사용하지 않을 경우 사용자 지정 속성에 종속된 기능이 예상한 바와 같이 작동하지 않을 수 있습니다. **설정 편집** 섹션에 포함된 **사용자 지정 특성** 표에서 **특성 유형** 열에 **IDP** 특성이 표시됩니다.
5. Okta 설정을 수정한 후 **변경사항 저장**을 클릭합니다.

## SCIM 사용자 프로비저닝에서 사용자 지정 / 엔터프라이즈 속성 구성

**절차**

1. **관리** > **ID** > **사용자 프로비저닝**으로 이동합니다.
2. **설정 편집**을 클릭합니다.
3. 사용자 지정 속성(예: custAttr1)을 입력하고 **변경사항 저장**을 클릭합니다.
4. Okta 포털에서 **디렉터리** > **프로필 편집기**를 클릭합니다.
5. **SCIM 2.0 테스트 앱(OAuth 전달자 토큰) User**을 클릭합니다.
6. **속성 추가**를 클릭합니다.
7. 다음 예시와 같은 사용자 지정 속성 값을 추가합니다.
    - 표시 이름(N-MDM에서 제공한 것과 동일한 사용자 지정 속성 값, 3단계 참조).
    - 변수 이름: custAttr1
    - 외부 이름: custAttr1
    - 외부 네임스페이스: **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User**
    - 사용자 권한: (읽기/쓰기)
8. **속성 저장**을 클릭합니다.
9. **프로필 편집기** > **매핑**을 클릭합니다. 매핑의 두 섹션(SCIM, Okta)이 표시됩니다.
10. N-MDM에서 생성된 사용자 지정 속성을 Okta에 정의된 속성에 매핑하고 매핑을 저장합니다.
11. **사용자**로 이동하여 필요한 사용자에 대고 클릭합니다.

12. **프로필** > **편집**을 클릭하고 속성을 편집합니다.
13. **애플리케이션** > **SCIM 2.0 테스트 앱(OAuth 전달자 토큰)** 앱으로 이동합니다.
14. **할당** 탭 아래에서 **할당**을 클릭하고 **사람에게 할당**을 선택합니다.
    **사람에게 SCIM 2.0 테스트 앱(OAuth 전달자 토큰) 할당** 창이 화면에 나타납니다.
15. 필요한 사용자를 선택하고 **할당**을 클릭합니다.
16. **완료**를 클릭하세요.

MDM용 Ivanti Neurons에서 사용자 지정 속성과 해당 매핑 확인하기:

- **사용자** > **사용자**(특정 사용자) > **속성**으로 이동합니다. Okta에 매핑된 사용자 지정 속성이 사용자 속성 섹션에 표시되는지 확인하세요.

# 12.2.11. LDAP 서버 구성

## 라이센스: Silver

LDAP 서버와 Connector를 설정해 회사 디렉토리에서 사용자와 그룹을 불러올 수 있습니다. 1개 이상 Connector를 설치하면 여러 대의 LDAP 서버를 추가할 수 있습니다.

LDAP 서버를 추가하면 다음 항목을 설정해야 합니다.

- LDAP 서버 *연결*
- 대상 디렉토리 데이터 확인에 필요한 *검색 용어*
- *가져올* 디렉토리의 일부분
- 선택한 디렉토리 부분에서 *사용자 초대*를 자동으로 실행할지 여부

LDAP 서버를 추가한 후 이 페이지로 돌아와 **LDAP 서버 정보를 편집**하거나 선택한 **LDAP 사용자를 변경**할 수 있습니다.

> LDAP 사용자는 반드시 LDAP 사용자를 구성한 후에 불러와야 합니다. **LDAP 사용자 불러오는 방법**을 참고하십시오.
> 로컬 사용자 이름과 동일하게, LDAP 사용자 이름 또한 전역적으로 고유해야 합니다. 사용자가 이미 같은 사용자 이름의 로컬 계정을 가지고 있지 않은지, 또는 하나 이상의 테넌트가 있는 조직의 경우, 사용자 이름이 이미 다른 테넌트와 연결되지 않았는지 확인하십시오.

## LDAP 서버 추가

**절차**

1. **+서버 추가**를 클릭합니다.
2. 다음 정보를 설정하세요.
3. **테스트 접속 및 계속하기**를 클릭합니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 이름 | 현재 서버를 식별할 수 있는 고유한 이름을 입력합니다. |
| 설명 | 현재 서버에 대한 간략한 정보를 입력합니다. |
| 디렉토리 URL | 해당 디렉토리 URL을 입력할 수 있습니다. 다음 형식 중 하나를 사용하세요.<br>ldap://IP 주소 또는<br>ldaps://IP 주소 또는<br>예: ldap://myserver1.mycompany.com:389 |
| 사용자 ID | 다음 특징을 갖는 계정의 사용자 ID를 입력할 수 있습니다.<br>• LDAP 서버로 관리되는 계정<br>• LDAP 서버와 연동되어 사용자 및 그룹, 조직 구성 단위 하위 트리를 검색할 수 있는 계정<br>보통 이 계정에는 디렉토리 관리자 자격(DN 또는 고유 이름 및 비밀번호)이 부여됩니다. |
| 비밀번호 | 현재 계정의 비밀번호를 입력합니다. |
| 비밀번호 확인 | 현재 계정의 비밀번호를 한 번 더 입력합니다. |
| 디렉토리 유형 | 지원 디렉토리 목록에서 해당 디렉토리 유형을 선택할 수 있습니다.<br>• Microsoft 활성 디렉토리<br>• LDAP 열기<br>• 기타(Open LDAP 호환) |

4. 이 단계에서는 현재까지 설정한 정보를 확인할 수 있습니다.

- 설정한 정보가 유효한 것으로 확인되면, LDAP 이름 지정 컨텍스트가 조회되며, 조회된 값은 다음 페이지의 일부 항목 설정에 사용됩니다.
- LDAP URL이 연결되지 않을 시에도 다음 단계로 진행할 수 있습니다. 단, 이 경우 연결될 시까지 기능이 제한될 수 있습니다.

남은 설정을 완료하세요.

5. **다음**을 클릭하세요.

| 설정 | 설정하기 |
| --- | --- |
| 디렉토리 페일오버 URL | 보조 디렉토리 URL을 입력할 수 있습니다. 다음 중 원하는 형식으로 입력하세요.<br>ldap://IP 주소 또는<br>예: ldap://myserver2.mycompany.com:389 |
| 동기화 간격 | LDAP 서버에서 시도되는 LDAP 데이터 동기화 주기를 입력할 수 있습니다. 기본값은 15분으로 설정되어 있습니다. 원하는 모든 LDAP 데이터가 성공적으로 동기화되어 해당 LDAP 설정이 원하는 값을 충족하는 것으로 확인되면 동기화 주기를 느리게 변경해도 됩니다. |
| 동기화 무시 활성화 | 다시 로딩한 데이터 세트가 현저하게 감소할 경우 해당 LDAP 동기화 데이터가 자동 폐기되도록 설정할 수 있습니다. 이 옵션을 설정하면 LDAP 시스템 부분에 비정상적인 동작이 발생하더라도 해당 서비스에 불필요한 업데이트나 등록된 장치의 설정 삭제 등이 발생하지 않습니다. LDAP 설정이나 LDAP 서버 관련 중요한 사항을 변경해야 할 경우에는 이 옵션을 선택하지 마시기 바랍니다. |
| 이 LDAP 서버 활성화 | 현재 LDAP 서버로 서비스를 이용하도록 설정할 수 있습니다. 현재 LDAP 서버를 폐기하거나 서비스에서 제외시키려면, 이 항목을 선택 해제하세요. 설정된 시스템 대체 작동 실행 시 현재 서버가 자동으로 보조 LDAP 서버로 교체되더라도, 이 옵션을 설정하면 사전 계획을 통해 대체 작동 중 연결 끊김 문제를 방지할 수 있습니다. |
| 불러올 때마다 자동으로 사용자를 초대합니다. | 사용자를 LDAP 서버에서 불러올 시마다 사용자에게 초대를 보내려면 선택하십시오. |
| CA 인증서 업로드 | 이 LDAP 서버에 설치된 CA가 발급한 TLS 인증서를 업로드하려면 **파일 선택**을 클릭합니다. 여러 개의 CA 인증서를 업로드할 수 있습니다. |
| 조회 추적 | 다중 포리스트 도메인을 사용 중인 경우에 한해 적용됩니다. 타겟 도메인 컨트롤러가 요청된 오브젝트 복사본을 갖고 있지 않을 경우 대체 도메인 컨트롤러 사용 여부를 표시하는 옵션입니다.<br>• 조회를 사용하려면 **따르기**를 선택하세요.<br>• 대체 도메인 컨트롤러 사용을 원하지 않는 경우에는 **무시하기**를 선택하세요.<br>• 현재는 **버리기**가 **무시하기**와 같은 기능을 하고 있습니다.<br>**팔로우**를 선택하면 LDAP 인증이 지연됩니다. |
| 검색 결과 시간 초과 | LDAP 서버에서 동기화된 데이터 탐색 중 성능 문제나 불완전한 결과가 발생할 경우 이 시간 초과값을 늘릴 수 있습니다. |
| 검색 결과 개수 | 한 번에 LDAP 서버에서 리턴될 레코드 개수를 최대로 설정할 수 있습니다. 다음과 같은 경우에는 성능 개선을 위해 이 설정을 변경해야 할 수 있습니다.<br>• LDAP 서버가 멀리 떨어져 있거나 대기시간이 긴 링크 뒤에 위치한 경우입니다. 이런 경우 검색 범위가 넓을수록 조회하는 데 시간이 더 오래 걸리므로 검색 범위를 좁혀야 업데이트되는 데이터의 부분 집합을 조금 더 신속히 확인할 수 있습니다.<br>• LDAP가 방대하고, 검색 결과 집합 역시 항상 방대한 경우입니다. 이런 경우 성능이 문제 되지 않는다면 결과 집합을 넓게 설정해야 적은 검색으로 모든 데이터가 반환될 수 있습니다. |

Sandbox 환경에서는 LDAP 동기화 간격을 8시간 미만으로 예약할 수 없습니다.

6. 아래 내용을 참고로 LDAP 서버와의 연동 설정을 하세요.

7. **탐색** 또는 **검색**을 클릭합니다.

| 설정 항목 | 설정하기 |
| --- | --- |
| 그룹 구성원 형식 | **DN** 또는 **UID**를 선택해 검색에서 고유한 이름과 사용자 ID 중 어떤 것을 사용할지 표시할 수 있습니다. |
| *OU 검색 속성* | 조직 단위 레벨로 검색할 기준을 설정할 수 있습니다. |
| 기본 DN | 검색을 시작할 시작 레벨에 해당하는 고유 이름을 입력할 수 있습니다. 선택한 내용에 따라 다른 여러 항목의 기본값이 달라집니다. 해당 항목들은 필요 시 변경이 가능합니다. |
| 개체 GUID | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. 이 속성은 OU 이름 변경 및 시간에 따라 고유하게 조직 구성 단위를 식별합니다. |
| 속성 이름 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 설명 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 속성 DN | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 검색 필터 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 검색 범위 | 다음 중 원하는 LDAP 계층 구조 범위를 선택할 수 있습니다.<br>• **베이스**(베이스 검색 입력 수준만)<br>• **한 수준**(베이스 검색 미만의 수준)<br>• **하위 트리**(베이스 검색 DN 미만인 디렉토리 정보 트리의 하위 트리) |
| *사용자 검색 속성* | 주어진 디렉토리 레벨로 사용자를 검색할 기준을 설정할 수 있습니다. |
| 기본 DN | 검색할 시작 레벨의 고유 이름을 입력할 수 있습니다. |
| 속성 UID | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 개체 GUID | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. 이 속성은 사용자 이름 변경 및 시간에 따라 고유하게 사용자를 식별할 수 있습니다. |
| 속성 DN | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 이름 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 성 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 표시 이름 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 이메일 주소 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 기본 이름 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 로캘 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 구성원 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |

| 설정 항목 | 설정하기 |
| --- | --- |
| 검색 필터 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 검색 범위 | 다음 중 원하는 LDAP 계층 구조 범위를 선택할 수 있습니다.<br>• **베이스**(베이스 검색 입력 수준만)<br>• **한 수준**(베이스 검색 미만의 수준)<br>• **하위 트리**(베이스 검색 DN 미만인 디렉토리 정보 트리의 하위 트리) |
| 관리되는 Apple ID | LDAP 사용자에 대한 관리되는 Apple ID를 동기화하려면 선택합니다.<br>• **없음**<br>• **패턴** -<br>◦ **사용자 이메일 주소**<br>◦ **userUPN**<br>필요에 따라 기존 Apple ID와의 충돌을 피하기 위해 **"appleid" 서브도메인 포함**을 선택하십시오. |
| +사용자 지정 속성 추가 | (선택사항) 디렉토리 서비스에서 기기 관리에 적용할 커스텀 사용자 속성을 최대 7개까지 지정합니다. 이후 각 속성은 변수를 지원하는 구성 필드에서 ${속성이름}으로 지칭될 수 있습니다.<br>**중요:** 이 옵션을 사용하려면 LDAP 서버 전체에 사용자 지정 속성을 일관적으로 구현해야 합니다. 사용자의 구현에 포함된 LDAP 서버가 이 속성을 사용하지 않는 경우, 이 속성에 종속된 기능이 예상처럼 작동하지 않을 수 있습니다. |
| *그룹 검색 속성* | |
| 기본 DN | 검색할 시작 레벨의 고유 이름을 입력할 수 있습니다. |
| 개체 GUID | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. 이 속성은 그룹 이름 변경 및 시간에 따라 고유하게 그룹을 식별합니다. |
| 속성 DN | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 속성 이름 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 설명 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 구성원 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 검색 필터 | 필요 시 현재 LDAP 환경과 일치하도록 기본값을 수정할 수 있습니다. |
| 검색 범위 | 다음 중 원하는 LDAP 계층 구조 범위를 선택할 수 있습니다.<br>• **베이스**(베이스 검색 입력 수준만)<br>• **한 수준**(베이스 검색 미만의 수준)<br>• **하위 트리**(베이스 검색 DN 미만인 디렉토리 정보 트리의 하위 트리) |

8. 현재 설정이 예상 데이터를 리턴하는지 확인하세요.
9. 해당 디렉토리 내 알려진 항목을 탐색 또는 검색해 확인할 수 있습니다.

**다음**을 클릭하세요.

# 사용자 지정 LDAP 속성 삭제

사용자 지정 LDAP 속성을 삭제하고 연결된 사용자 또는 기기에서 해당 값을 제거할 수 있습니다.

**절차**

1. **관리 > 속성**으로 이동합니다.
2. **사용자 지정 속성** 섹션에서 삭제할 LDAP 속성 옆에 있는 **삭제** 링크를 클릭합니다. 확인 창이 표시됩니다.
3. **삭제**를 눌러 삭제를 확인합니다.

> 기본값으로 **삭제** 버튼이 비활성화되어 있습니다. **삭제** 버튼을 활성화하려면 **사용자 지정 속성을 삭제하면 되돌릴 수 없음을 알고 있습니다** 옵션에 있는 체크박스를 선택해야 합니다.

# LDAP 서버 정보 수정

**절차**

1. **관리 > LDAP**로 이동합니다.
2. LDAP 서버 항목에서 **작업** 열에서 **편집** 아이콘을 선택하면 LDAP 서버 페이지 연결을 볼 수 있습니다.
3. 필요한 설정을 수정하세요.
4. **테스트 접속 및 계속하기**를 클릭합니다.
   LDAP URL이 연결되지 않을 시에도 다음 단계로 진행할 수 있습니다. 단, 이 경우 연결될 시까지 기능이 제한될 수 있습니다.
5. **탐색** 또는 **검색**을 클릭합니다.
6. 현재 설정이 예상 데이터를 리턴하는지 확인하세요.
   해당 디렉토리 내 알려진 항목을 탐색 또는 검색해 확인할 수 있습니다.
7. **완료**를 클릭하세요.

# LDAP 사용자 불러오기

**절차**

1. **사용자**를 선택하세요.
2. **+추가 > LDAP에서 사용자 초대**를 클릭합니다.
3. LDAP 서버 항목에서 **사용자 선택**을 클릭합니다.
4. LDAP 사용자 추가 페이지에서 사용자, 그룹 또는 OU를 검색 필드에 입력합니다.
5. 새 사용자 또는 그룹을 추가하려면 추가하려는 항목 옆의 **+추가**를 클릭합니다.
6. **다음**을 클릭하세요.
7. 초대장 발송 여부를 선택합니다.
   - 아무도 초대하지 않음
     초대장을 나중에 보내려면 **사용자 > 사용자**로 이동한 다음 **작업 > 초대 보내기**를 선택해 초대를 보냅니다.
   - 모두 초대

**완료**를 클릭하세요.

# 선택한 사용자나 그룹 또는 조직 구성 단위 업데이트

**절차**

1. **관리 > LDAP**로 이동합니다.
2. LDAP 서버 항목에서, LDAP 사용자 추가 페이지를 보려면 **작업** 열에서 **사용자 관리** 아이콘을 선택합니다.
3. 새로운 사용자 또는 그룹을 추가하려면 검색 필드에 사용자 또는 그룹의 이름을 입력합니다.
4. 추가할 항목 옆의 **+추가**를 클릭합니다.
5. 사용자, 그룹, 조직단위를 삭제하려면 삭제하려는 항목 옆의 삭제 아이콘을 클릭하십시오.
6. **완료**를 클릭하세요.

## LDAP 동기화 무시 알림 활성화

LDAP 동기화 무시 알림을 활성화하면 LDAP 환경에 의도치 않은 대규모 변경 사항으로 인해 발생하는 중단을 막을 수 있습니다.

**절차**

1. **관리 > LDAP**로 이동합니다.
2. LDAP 서버 항목에서 **작업** 열에서 **편집** 아이콘을 선택하면 LDAP 서버 페이지 연결을 볼 수 있습니다.
3. **동기화 무시 활성화** 체크박스를 확인합니다.
4. 다시 로딩되는 LDAP 데이터의 퍼센트 값을 입력하여 동기화 무시를 트리거합니다.
5. **테스트 접속 및 계속하기**를 클릭합니다.
   LDAP URL이 연결되지 않을 시에도 다음 단계로 진행할 수 있습니다. 단, 이 경우 연결될 시까지 기능이 제한될 수 있습니다.
6. **완료**를 클릭하세요.
7. LDAP 서버 항목에서 **지금 동기화** 아이콘을 클릭하십시오.
   LDAP에서 MDM용 Ivanti Neurons로 동기화될 변경 차이가 설정된 무시 비율 이상인 경우, 경고 알림이 생성됩니다. 변경 사항을 설정한 비율 아래의 값으로 되돌리면 알림이 사라집니다.

| 트리거 | 심각도 | 알림 유형 | 구성요소 유형 | 구성요소 |
|---|---|---|---|---|
| LDAP 동기화 무시 | 경고 | 데이터 동기화 | LDAP | LDAP 서버 이름 |
| LDAP 동기화 복원 | 정보 | 데이터 동기화 | LDAP | LDAP 서버 이름 |

하나 이상의 사용자 기록이 LDAP에서 동기화하지 못하면 동기화 알림 일부 무시가 생성됩니다. 이런 경우 CSV 파일이 동기화에 실패한 사용자 목록의 첨부파일로 포함됩니다. 사용자가 속성 누락으로 인해 무시된 경우 누락된 속성의 목록 또한 내보낸 CSV 파일에 포함됩니다.

## LDAP 서버에서 변경 사항 동기화

LDAP 페이지에서 LDAP 서버 항목의 **지금 동기화** 아이콘을 클릭하십시오.

> 표시 이름이 128자를 초과할 경우, LDAP 동기화는 해당 사용자를 무시하고 다른 사용자 또는 사용자 그룹 동기화를 진행합니다.

## LDAPS 서버의 연결 문제 해결

LDAPS(SSL을 통한 LDAP) 서버에 연결하는 데 문제가 발생하는 경우, 인증서에 문제가 있을 수 있습니다.

이 문제를 해결하려면:

- LDAPS 서버에 자체 서명 인증서를 사용하고 있지 않은지 확인합니다.
- LDAPS 인증서가 만료 또는 철회되지 않았는지 확인합니다. 호스트 이름이 일치하지 않는지도 확인합니다.

확인한 후 자동 LDAP 동기화를 기다리거나 LDAP 서버 항목의 **관리 > LDAP > 지금 동기화** 아이콘으로 직접 동기화할 수 있습니다.

LDAP 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 **역할** 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 시스템 읽기 전용

# 12.2.12. Sentry

Sentry는 ActiveSync가 설정된 이메일 시스템과 모바일 기기 간 게이트웨이 역할을 하는 구성요소입니다. Sentry를 이용해 이메일 접근을 허용할 기기를 관리할 수 있습니다. Sentry는 ISO 파일로 다운로드한 후 가상 시스템에 설치할 수 있습니다. 기업에서는 로드 밸런서를 이용하면 여러(이중) Sentry를 유지관리할 수 있습니다.

**라이센스:** Silver

## 최신 문서

최신 Sentry 지침을 보려면 **제품 문서**에서 Sentry를 클릭하십시오.

최신 Sentry 설치 지침은 *Standalone Sentry 온프레미스 설치 가이드*의 적합한 버전을 선택하십시오.

Sentry 업그레이드 지침은 *Sentry 가이드*의 적합한 버전을 선택하십시오. Sentry 가이드에서 다음 섹션을 확인하십시오.

- Standalone Sentry System Manager UI를 사용한 업그레이드 지침은 "Standalone Sentry 소프트웨어 업데이트"를 참조하십시오.
- Standalone Sentry 명령줄 인터페이스(CLI)를 사용한 업그레이드 안내는 "CLI를 사용한 업그레이드"를 참조하십시오.

업그레이드 전에 Standalone Sentry 릴리스 노트에서 업그레이드할 버전을 확인하십시오.

# 12.3. Apple 설정

이 섹션에는 다음 주제가 포함됩니다.

- Apple Configurator
- 기기 등록
- 설정 도우미 구성
- MDM 인증서 설치
- 기업용 공유 iPad 기기
- School Manager
- 설정(Apple)

# 12.3.1. Apple Configurator

이 페이지에서는 iOS 기기의 MDM용 Ivanti Neurons 기기 관리 설정을 위해 Apple Configurator를 구성할 수 있습니다. Apple Configurator를 사용하면 대량으로 iOS 기기를 매우 쉽게 배포할 수 있습니다. 또한 구성자를 사용하여 관리자는 iOS 기기를 감독할 수 있으며 이렇게 하면 구성 및 관리 기능을 더 높은 수준으로 사용할 수 있습니다. Apple Configurator에 관한 자세한 정보는 Mac App Store를 참조하십시오.

기본 단계는 다음과 같습니다.

1. MDM용 Ivanti Neurons 테넌트에서 MDM 프로필을 내보냅니다.
2. 해당 MDM 프로필을 Configurator로 불러옵니다.
3. 테더링으로 연결된 장치에 Configurator를 이용해 MDM 프로필을 적용합니다.

## 기기에 기본 사용자 정의

다른 사용자를 선택하지 않는 한, Apple Configurator를 통해 구성된 기기는 MDM용 Ivanti Neurons에서 그 어느 사용자에게도 할당되지 않습니다.

1. **구성된 기기 할당** 필드를 클릭합니다.
2. 선택하고자 하는 MDM용 Ivanti Neurons 사용자 이름을 입력합니다.
3. 드롭다운 목록에 해당 사용자 이름이 표시되면 선택합니다.
4. **저장**을 클릭하세요.

## Apple Configurator를 사용한 앱 설치

Apple Configurator를 사용하여 앱을 설치하기 전에:

- Apple 앱 스토어의 액세스가 기기 구성에 의해 제한됩니다.
- 앱 설치는 기기 구성에 의해 허용됩니다.
- Apple Configurator는 기기를 구성하는 데 사용되는 컴퓨터에 설치되어 있어야 합니다.

Apple Configurator를 사용하여 앱을 설치하려면:

1. MDM용 Ivanti Neurons에서 **관리자 > Apple Configurator**로 이동합니다.
2. 등록된 기기 토글 스위치를 켭니다.
3. 다음 중 하나를 클릭합니다.
    - **기본 사용자의 plist**
    - **특정 사용자의 plist** - 특정 사용자의 사용자 이름이나 이메일 ID를 입력합니다.

Apple Configurator에서 **준비 > 앱**으로 이동합니다.

5. **준비 > 설정하고 감독을 비활성화**로 이동합니다.
6. iOS 업데이트에서 **기기를 업데이트하지 않음** 옵션을 선택합니다.
7. **준비**를 클릭합니다(Apple Configurator의 하단).
   기기 체크인 후 기기에 설치된 앱의 목록에 앱이 보입니다.

## UEM 서버를 사용하여 앱 설치

UEM 서버를 사용하여 앱을 설치하려면:

1. 앱 탭의 사내 스토어에서 앱을 업로드합니다.
2. 앱을 선택합니다.
3. **앱 구성** 탭을 클릭합니다.
4. **기기에 설치**를 선택합니다.
   구성 설정을 완료합니다.
5. **동작 > 강제 체크인**을 선택하세요.

## 최종 사용자가 해야 할 일

Apple은 최종 사용자가 Go을(를) 최소 1회 실행할 것을 요구합니다. 그렇지 않은 경우 MDM용 Ivanti Neurons 위치 확인 기능이 제대로 작동하지 않습니다. 이것은 자신의 위치가 추적되고 있음을 최종 사용자가 인식하기 위한 것입니다.

**주의:** Configurator를 통해 단일 앱 모드로 기기를 배포하는 경우에는 이 방법을 사용할 수 없습니다.

**Apple Configurator 설치** 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 시스템 읽기 전용

# 12.3.2. 계정 기반 등록

이 섹션은 계정 기반 사용자와 계정 기반 기기 등록에 해당합니다.

**지원 기기**

- (계정 기반 사용자 등록 시) iOS 15 이상, (계정 기반 기기 등록 시) iOS17 이상이 설치된 기기
- macOS 14 이상이 설치된 장치
- visionOS 1.1 이상이 설치된 기기

**필수 조건:**

**계정 기반 사용자 등록**

- 관리형 Apple ID(Apple Business Manager 또는 Apple School Manager 사용자)가 있는 MDM용 Ivanti Neurons 사용자 계정.
- **Apple 등록** 섹션 아래에 있는 **Apple 등록 유형 선택** 드롭다운 목록에서 **사용자 등록**을 선택하십시오.
- **사용자** -> **사용자 설정** -> **기기 소유자 설정**을 **ON**으로 설정 -> **사용자 소유** 옵션 선택.

**계정 기반 기기 등록**

- 관리형 Apple ID(Apple Business Manager 또는 Apple School Manager 사용자)를 가진 MDM용 Ivanti Neurons 사용자 계정.
- **Apple 등록** 섹션 아래에 있는 **Apple 등록 유형 선택** 드롭다운 목록에서 **기기 등록**을 선택합니다.
- **사용자** -> **사용자 설정** -> **기기 소유자 설정**을 **ON**으로 설정 -> **회사 소유** 옵션을 선택합니다.

iOS 15+, macOS 14+, visionOS 1.1+ 기기의 **계정 기반 사용자 등록**은 BYOD(Bring Your Own Device)를 실행하는 회사를 위해 설계된 등록 옵션입니다. 계정 기반 사용자 등록은 사용자 개인 정보에 더욱 초점을 맞춰 기업에서 필요로 하는 보안 수준을 구현한 수정된 버전의 MDM 프로토콜이자 Apple Business Manager를 이용하는 사용자 등록 옵션입니다.

iOS 17+, macOS 14+, visionOS 1.1+ 기기의 **계정 기반 기기 등록**은 회사 소유/법인 기기를 등록하는 회사를 위해 설계된 등록 옵션입니다. 계정 기반 기기 등록은 사용자 개인정보 보호에 더욱 초점을 맞춰 기업에서 필요로 하는 보안 수준을 구현하고자 MDM 프로토콜과 Apple Business Manager를 이용하는 기기 등록을 활용합니다. 최종 사용자는 설정의 회사 계정 기능을 이용해 기기를 등록할 수 있습니다.

## 검색 서비스 설정

기업에 acme.com과 같은 기업 도메인 이름이 있는 경우 사용자의 이메일 ID는 devicename@acme.com입니다.

1. 사용자가 username@acme.com을 입력하여 회사 또는 학교 계정에 로그인하면 기기에서 URL에 대한 HTTP GET 요청 호출을 수행합니다.
   https://acme.com/.well-known/com.apple.remotemanagement?user-identifier=user@acme.com
   자세한 내용은 https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers를 참조하십시오.
2. acme.com 도메인에서 URI - /.well-known/com.apple.remotemanagement에 대한 리디렉션 규칙을 구성하여 이를 다음 URL로 리디렉션합니다.
   https://<n-MDM cluster>/.well-known/com.apple.remotemanagement

## 계정 기반 기기 등록을 위한 간소화된 서비스 검색

> iOS 18.2 이상, macOS 15.2 이상, visionOS 2.2 이상 기기에 적용됩니다.

계정 기반 등록의 경우, 사용자가 조직 이메일을 입력하여 직장이나 학교 계정에 로그인하면 기기는 먼저 조직 도메인에서 잘 알려진 HTTP 리소스를 검색합니다. 이 리소스에는 MDM 등록 URL에 대한 링크가 포함되어 있습니다.

**절차**

1. 직장이나 학교 계정에 로그인합니다.
2. **Apple Business Manager** 및 **Apple School Manager**에서 도메인 검증 - Apple Business Manager 또는 Apple School Manager 내에서 검증된 도메인에만 적용됩니다. 도메인이 검증되면 해당 기기는 Apple Business Manager/Apple School Manager에 확인하여 대체 MDM 등록 URL을 얻을 수 있습니다.
3. **Mac**, **Apple Vision Pro**, **iPhone** 및 **iPad** 플랫폼 유형에 대한 기본 MDM용 Ivanti Neurons 할당을 설정합니다.
   기본 기기 할당을 설정하려면 아래 단계를 따르십시오:
   1. **Apple Business Manager**/**Apple School Manager**에서 관리자 또는 기기 등록 관리자 역할을 가진 사용자로 로그인합니다.
   2. 사이드바 하단에서 자신의 이름을 선택하고 기본 설정을 선택한 후, 다음 중 하나를 수행합니다:
      - 기기 관리 서비스 아래에서 기기 관리 서비스 할당을 선택한 후, 기본 기기 관리 서비스 할당 옆의 편집을 선택합니다.
      - 기기 관리 서비스 아래에서 기존 서비스를 선택한 후, 기본 기기 할당 아래의 변경을 선택합니다.
   3. 다른 구성된 기기 관리 서비스가 없는 경우, 선택한 서비스로 모든 자동 기기 할당을 변경한 후 **저장**을 선택합니다.
4. MDM용 Ivanti Neurons 콘솔에서 **관리자** > **Apple** > **장치 등록**으로 이동합니다. **장치 등록** 화면에 **ADDE URL** 및 **ADDE URL SET TIME** 열이 추가됩니다.

> **첫 번째 기본 설정**: 기기는 조직의 도메인에서 잘 알려진 HTTP 리소스를 확인합니다.

**대체 옵션**: 첫 번째 방법이 실패하면 기기는 Apple ABM/ASM에 연결하여 MDM용 Ivanti Neurons에서 지정한 대체 대상을 가져옵니다.

5. **작업** 아래의 **ADDE URL 구성**을 선택합니다.
6. 페이지를 새로 고칩니다.

## 기기 사용자 지침

이 항목은 계정 기반 사용자 등록 또는 계정 기반 기기 등록 시 기기 사용자가 취해야 할 작업에 대해 다룹니다.

**절차**

1. 기기에서 다음 중 하나로 이동합니다.
   - **iOS** 장치의 경우 - **설정** > **일반** > **VPN** 및 **장치 관리**.
   - **macOS** 장치의 경우 - **시스템 설정** > **개인정보 보호 및 보안** > **프로필**.
   - **visionOS** 기기의 경우 - **설정** > **일반** > **VPN** 및 **기기 관리**.
2. **회사 또는 학교 계정에 로그인**으로 이동합니다.
3. 회사 또는 학교 계정 이메일 주소를 입력합니다. 이메일 주소는 다음 형식을 따라야 합니다.
   username@<enterprise domain name>, 예: username@acme.com.
4. 로그인 페이지에 자동으로 관리되는 Apple ID가 표시되고 사용자를 iReg 플로우로 안내합니다. MDM용 Ivanti Neurons 자격 증명을 입력했는지 확인하십시오.
5. 회사 또는 학교 계정 자격 증명을 입력하고 **계속**을 클릭합니다.
6. 2단계 인증 후 기기 등록이 완료됩니다.

# 12.3.3. 기기 등록

Apple Business Manager의 일부인 기기 등록을 통해 고객은 기기를 대량으로 구매하고, 활성화하는 동안 해당 기기를 MDM에 자동으로 등록할 수 있습니다. 참여하기로 선택하면 MDM용 Ivanti Neurons(을)를 기기 관리용 MDM 서버로 사용할 수 있습니다. 자세한 내용은 https://business.apple.com/을 참조하십시오.

## 기기 등록에 MDM용 Ivanti Neurons 연결하기

MDM용 Ivanti Neurons(을)를 기기 등록용 MDM 서버로 사용하려면 MDM용 Ivanti Neurons에서 Apple Business Manager 서버 토큰을 설정합니다.

각 Apple Business Manager 서버에 대해 MDM용 Ivanti Neurons에서 다음 작업을 사용할 수 있습니다.

- 테스트 연결
- 기기 등록 프로필 추가
- 공개 키 다운로드
- 기기 등록 전체 동기화 - 전체 동기화 시작. 완료하는 데 약간의 시간이 소요될 수 있습니다. 동기화가 완료되면 마지막 동기화 열에서 정보를 볼 수 있습니다. 이미 진행 중일 경우에는 전체 동기화를 시작할 수 없습니다.

> MDM용 Ivanti Neurons DEP 서버 동기화에 실패하면 에서 관리자에게 알림을 보내 문제를 더 쉽게 식별할 수 있습니다. DEP 서버를 삭제하면 시스템은 관련된 알림도 함께 삭제합니다.

- 새 토큰 업로드
- 삭제

> **인증 편집** 및 **기기 등록 기기 속성 할당** 작업은 이제 기기 등록 대신 기기 등록 프로필에 대해 이용 가능합니다(MDM 서버).

**절차**

1. **관리** > **Apple** > **기기 등록**으로 이동합니다.
2. **키 다운로드**를 클릭하세요.
3. MDM용 Ivanti Neurons 키를 저장합니다.
4. **business.apple.com**을 클릭합니다.
5. 기기 등록을 이용할 수 있는 Apple 사용자 정보로 로그인합니다.
6. Apple 기기 등록 사이트에서:
7. MDM용 Ivanti Neurons에서 **업로드**를 클릭합니다.
8. **시작하기**를 클릭합니다.
9. Apple 서비스 인증에 사용할 신뢰할 수 있는 휴대전화를 선택합니다.
10. 선택한 전화번호로 전송된 인증 코드를 입력합니다.
11. **MDM 서버 추가**를 클릭합니다.
12. 서비스에 이용될 가상 MDM 서버의 고유 이름을 입력합니다.
13. **다음**을 클릭하세요.
14. 다운로드해 놓은 공개 키를 업로드합니다.

15. **다음**을 클릭합니다.
16. **내 서버 토큰**을 클릭해 토큰을 다운로드합니다.
17. **완료**를 클릭하세요.
18. **다음**을 클릭하세요.
19. 인증 옵션을 선택하세요.

- **사용자 등록/로그인 메시지 표시**

> visionOS 플랫폼으로 작동하는 장치는 지원하지 않습니다. 대신 장치를 등록할 때 **사용자 로그인 건너뛰기**를 사용합니다.

> 사용자 이름과 비밀번호를 사용자에게 표시합니다. 사용자는 비밀번호 필드에 비밀번호나 PIN을 입력할 수 있습니다. macOS 15 이상의 기기에서는 암호 키 지원 ID 제공자를 사용하는 iDP 사용자에게는 **페이스 ID**, **터치 ID**, **보안 키**와 같은 추가 옵션도 제공됩니다. 비밀번호 및 PIN 기본 설정은 인증과 관련된 **사용자** > 사용자 설정에서 구성할 수 있습니다.

- **사용자 로그인 건너뛰기**

> Nobody 사용자(익명)나 정의된 사용자에게 할당된 기기는 나중에 **기기** 페이지에서 특정 사용자에게 할당할 수 있습니다.

다음 옵션 중 하나를 선택합니다.

  - **모든 기기를 할당할 한 명의 사용자 정의**
  - **모든 기기를 익명의 사용자에게 할당**

10. 이때 선택한 옵션이 사용자 설정에 선택된 설정보다 우선적으로 적용됩니다.

**업로드**를 클릭하여 3단계에서 수신한 키를 설치합니다.

11. 화면에 표시된 양식을 작성해 사용할 기기 등록 기기의 프로필을 설정합니다.
12. 다음 설정 옵션을 위한 장치 활성화 도중 사용자가 건너뛸 수 있는 단계를 정의합니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| 이름 | 해당 기기 등록 프로필의 고유한 이름을 입력합니다. |
| 설명 | 프로필 설명을 입력합니다. |
| 부서 | 현재 프로필과 연동되어 있는 소속 조직의 부서를 입력할 수 있습니다. |
| 감독 모드 | 구성 및 제한에 대한 관리 제어 기능을 추가로 활성화합니다. iOS 13+ 및 macOS 10.15+ 기기의 경우 이 옵션이 기본적으로 활성화됩니다. |
| iOS 17+ | **등록용 OS 버전**<br>• **등록 시 최소 OS 버전 필요**: 관리자는 장치 등록을 위한 최소 필수 OS 버전을 설정할 수 있습니다. 장치가 최소 OS 버전 기준을 충족하지 않는 경우 시스템은 사용자에게 필요한 버전으로 업그레이드하라는 메시지를 표시합니다. 사용자가 업그레이드를 거부하면 등록이 차단됩니다.<br>**최신 버전**: 관리자는 기기 등록에 사용할 최신 OS 버전을 설정할 수 있습니다. 장치가 최신 OS 버전 기준을 충족하지 않는 경우 시스템은 필요한 버전으로 업그레이드하라는 메시지를 사용자에게 표시합니다. 사용자가 업그레이드를 거부하면 등록이 차단됩니다.<br>**특정 버전**: 관리자는 기기 등록 시 필요한 최소 OS 버전을 설정할 수 있습니다. 장치가 최소 OS 버전 기준을 충족하지 않는 경우 시스템은 사용자에게 필요한 버전으로 업그레이드하라는 메시지를 표시합니다. 사용자가 업그레이드를 거부하면 등록이 차단됩니다.<br>• **최소 iOS**: 빌드 버전이 '**OSVersion**' 키에 지정된 OS 버전과 일치하지 않는 경우 이 OS 버전이 우선 적용됩니다.<br>• **최소 빌드 버전**: 빌드 버전이 **'OSVersion**' 키에 지정된 OS 버전과 일치하지 않는 경우 이 OS 버전이 우선 적용됩니다.<br>잘못된 빌드 번호를 입력한 경우 이 필드는 선택 사항입니다.<br>• **메시지**: 사용자에게 표시하기에 적합한 오류에 대한 설명입니다. 필요한 경우,<br>◦ 클라이언트는 메시지를 표시하기 위해 최선을 다하지만 현지 사정에 따라<br>◦ 그렇게 하지 못할 수도 있습니다.<br>관행에 따라 메시지를 추가해야 합니다.<br>• **기기를 베타 프로그램에 추가**<br>**iOS용 베타 프로그램**: 자동 기기 등록 중 iOS에 베타 소프트웨어 버전을 강제 적용합니다. |
| macOS 14+ | **등록용 OS 버전**<br>• **등록 시 최소 OS 버전 필요**: 관리자는 장치 등록을 위한 최소 필수 OS 버전을 설정할 수 있습니다. 장치가 최소 OS 버전 기준을 충족하지 않는 경우 시스템은 사용자에게 필요한 버전으로 업그레이드하라는 메시지를 표시합니다. 사용자가 업그레이드를 거부하면 등록이 차단됩니다.<br>**최신 버전**: 관리자는 기기 등록에 사용할 최신 OS 버전을 설정할 수 있습니다. 장치가 최신 OS 버전 기준을 충족하지 않는 경우 시스템은 필요한 버전으로 업그레이드하라는 메시지를 사용자에게 표시합니다. 사용자가 업그레이드를 거부하면 등록이 차단됩니다.<br>**특정 버전**: 관리자는 기기 등록 시 필요한 최소 OS 버전을 설정할 수 있습니다. 장치가 최소 OS 버전 기준을 충족하지 않는 경우 시스템은 사용자에게 필요한 버전으로 업그레이드하라는 메시지를 표시합니다. 사용자가 업그레이드를 거부하면 등록이 차단됩니다.<br>• **최소 macOS**: 빌드 버전이 '**OSVersion**' 키에 지정된 OS 버전과 일치하지 않는 경우 이 OS 버전이 우선 적용됩니다.<br>• **최소 빌드 버전**: 빌드 버전이 **'OSVersion**' 키에 지정된 OS 버전과 일치하지 않는 경우 이 OS 버전이 우선 적용됩니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| | 잘못된 빌드 번호를 입력한 경우 이 필드는 선택 사항입니다.<br>• **메시지**: 사용자에게 표시하기에 적합한 오류에 대한 설명입니다. 필요한 경우,<br>◦ 클라이언트는 메시지를 표시하기 위해 최선을 다하지만 현지 사정에 따라<br>◦ 그렇게 하지 못할 수도 있습니다.<br>관행에 따라 메시지를 추가해야 합니다.<br>• **기기를 베타 프로그램에 추가**<br>**macOS용 베타 프로그램**: 자동 기기 등록 중 macOS에 베타 소프트웨어 버전을 강제 적용합니다. |
| iOS 업데이트 자동 다운로드 및 설치 | (iOS 9.0+ 전용) **설정 > iTunes & App Store**에서 장치의 자동 다운로드 옵션을 선택한 경우 OS 업데이트는 자동 다운로드되지만 설치되지는 않습니다. 이는 장치 등록 프로필 옵션이 꺼져 있더라도 같습니다.<br>이 설정은 관리 상태인 기기 등록 등록 기기에 적용되는 iOS 소프트웨어 업데이트 구성이 있을 때 우선합니다.<br>이 설정이 변경되면 기기를 재설정하지 않아도 관리 상태인 기기 등록 등록 기기에 적용됩니다. |
| MDM 제거 가능 | 기기가 등록된 후 사용자가 MDM에서 등록 해제를 못하도록 할지 여부를 정의합니다.<br>공유 iPad에는 이 설정이 적용되지 않습니다. |
| MDM 필수 | 사용자가 활성화 프로세스 중 MDM 설치 건너뛰기를 못하도록 할지 여부를 정의합니다. iOS 13+ 및 macOS 10.15+ 기기의 경우 이 옵션이 기본적으로 활성화됩니다. |
| 백업에서 프로필 사용 안 함 | 활성화된 경우, 기기를 백업에서 복원할 때 이 프로필을 사용하지 않습니다.<br>iOS 26 이상 및 visionOS 26 이상 기기에만 적용됩니다. |
| 페어링 허용 | (iOS 13+ 및 macOS 10.15+에는 해당되지 않음) iTunes 동기화와 같은 호스트 페어링 기능을 허용합니다.<br>유효한 페어링 인증서가 있는 호스트에는 항상 페어링이 허용됩니다. |
| 서비스로 복귀 | **서비스 복귀**를 **True**로 설정하면 **서비스 복귀** 작업 실행 시 애플리케이션이 유지됩니다. 이를 통해 기기가 애플리케이션의 스냅샷을 생성하고 서비스 복귀 과정에서 더 빠른 환경을 제공할 수 있습니다. 비활성화된 경우에도 기기는 서비스 복귀를 수행할 수 있지만, 재등록 과정에서 애플리케이션을 다시 다운로드해야 합니다.<br>**Apple Migration ABM** 기능을 활용하려면 이 기능을 비활성화해야 합니다.<br>**서비스로 복귀**가 **True**로 설정된 경우 기기를 마이그레이션할 수 없습니다.<br>iOS 26 이상 및 visionOS 26 이상 기기에만 적용됩니다. |
| 인증서 | **+추가**를 클릭하여 인증서를 업로드합니다. |
| 지원 전화 번호 | 기기 사용자가 도움이 필요할 때 연락할 수 있는 전화번호를 제공할 수 있습니다. |
| 이메일 주소 지원 | 기기 사용자가 도움이 필요할 때 연락할 수 있는 이메일 주소가 제공됩니다. |
| 사용자 지정 등록 | (iOS 13.0+ 및 macOS 10.15+) 사용자 지정 등록 웹 페이지를 만듭니다. 기기 등록 중에 사용자를 인증하려면 사용자 지정 웹 페이지(웹 뷰)를 지정합니다.<br>이 페이지를 사용하여 인증 유형, 브랜딩, 동의 텍스트, 개인정보 보호정책 등의 사용자 지정 정보를 표시할 수 있습니다.<br>자세한 내용은 이 절차 다음에 나오는 "*사용자 지정 기기 등록 웹 페이지 추가하기*" 섹션을 참조하십시오.<br>• **사용자 지정 등록 활성화**를 선택하여 이 기능을 활성화합니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| | • **URL**(예: https://mycustomweburl.com)을 입력합니다. 이 URL은 사용자 지정 URL 값이 웹 뷰를 통해 사용자에게 표시되도록 정의합니다. |
| 다중 사용자 | (iOS 13.4+) 비즈니스용 공유 iPad<br>기업은 여러 직원들 간에 기기를 공유하도록 하면서 개인화된 환경을 제공할 수 있습니다.<br>공유 iPad를 기기에서 사용 설정하려면 **다중 사용자 모드**를 선택하십시오. 자세한 내용은 **비즈니스용 공유 iPad**를 참조하십시오.<br>• Apple Education에는 이 설정이 적용되지 않습니다.<br>• 다중 사용자 설정을 수정하려면 **감독 모드** 설정을 선택하십시오. |
| 할당량 크기 | (iOS 13.4+) 비즈니스용 공유 iPad.<br>값은 장치에서 사용자에게 할당된 저장소를 나타내는 메가바이트(MB) 단위입니다.<br>값이 너무 작으면 장치에서 기본 할당량 크기를 할당합니다. |
| 거주 사용자 | (iOS 13.4+) 비즈니스용 공유 iPad<br>값은 기기에서 지속되거나 있을 수 있는 사용자 수를 나타냅니다. 값이 기기가 지원하는 최대 사용자 수의 값보다 클 경우 MDM 서버가 해당 값(최대 사용자 수)을 기본값으로 사용합니다.<br>관리자는 할당량 크기 또는 거주 사용자 값을 제공할 수 있습니다. 두 값이 모두 제공될 경우 MDM 서버는 할당량 크기를 기본값으로 사용합니다. |
| 사용자 세션 시간제한 | (iOS 14.5+) 비즈니스용 공유 iPad<br>사용자 세션에 대한 시간제한을 표시합니다(초). 사용자 세션은 지정된 비활성 시간이 지나면 자동으로 로그아웃됩니다.<br>최소 값은 30초입니다. 이 값을 0으로 지정하면 시간제한이 사라지며 기기 기본 시간제한으로 설정됩니다.<br>1~29 값은 유효하지 않습니다. 설정되면 기기가 기본 시간제한으로 설정됩니다. |
| 임시 세션 시간제한 | (iOS 14.5+) 비즈니스용 공유 iPad<br>게스트 또는 임시 세션에 대한 시간제한을 표시합니다(초). 임시 세션은 지정된 비활성 시간이 지나면 자동으로 로그아웃됩니다. 최소 값은 30초입니다. 이 값을 0으로 지정하면 시간제한이 사라지며 기기 기본 시간제한으로 설정됩니다.<br>1~29 값은 유효하지 않습니다. 설정되면 기기가 기본 시간제한으로 설정됩니다. |
| 임시 세션만 | (iOS 14.5+) 비즈니스용 공유 iPad<br>True인 경우 사용자는 게스트 환영 창만 볼 수 있으며 게스트 사용자로만 로그인할 수 있습니다.<br>False인 경우 사용자는 관리되는 Apple ID로 로그인할 수 있습니다(기존 동작).<br>기본: False |
| 관리형 Apple ID 기본 도메인 | (iOS 16.0+) 비즈니스용 공유 iPad<br>도메인 목록을 지정합니다. 사용자는 QuickType 키보드의 도메인 목록에서 계정 도메인을 선택할 수 있습니다. |
| 온라인 인증 유예 기간 | (iOS 16.0+) 비즈니스용 공유 iPad<br>네트워크에 연결하지 않고 사용자가 로그인할 수 있는 기간을 지정합니다(단위: 일).<br>값을 영(0)으로 지정하면 매번 온라인 인증을 수행합니다.<br>**기본값**: 0 |
| 자동 잠금 시간 | (iOS 17.0+)<br>장치가 절전 모드로 전환되는 시간(초)을 지정합니다. 최소값은 120초입니다. |

| 설정 항목 | 수행 작업 |
| --- | --- |
| 암호 잠금 유예 기간 | 장치 사용자가 장치 암호를 입력해야 잠금이 해제되는 시간(초)을 지정할 수 있습니다. 최소값은 0초이고 최대값은 14400초입니다. |
| 표준 시간대 | 장치가 속한 시간대를 지정합니다.<br>**예:** Pacific/Midway |

**설정 옵션**

- 암호 입력 건너뛰기 - 선택하면 Apple Pay 설정 건너뛰기 및 Touch ID 건너뛰기가 자동으로 활성화됩니다.
- 위치 서비스 건너뛰기
- 백업에서 복원 건너뛰기
- Android에서 "iOS로 이동" 건너뛰기
- 서비스 조건 건너뛰기
- Apple ID 및 iCloud에 로그인 건너뛰기 - 선택하면 Apple Pay 설정 건너뛰기가 자동으로 활성화됩니다.
- Touch ID 설정 건너뛰기(iPhone 5s, 6, 6+, iPad Air 2, iPad Mini 3 전용) – 선택하면 Apple Pay 설정 건너뛰기가 자동으로 활성화됩니다.
- Apple Pay 설정 건너뛰기(iPhone 6, 6+, iPad Air 2, iPad Mini 3 전용)
- 확대/축소 설정 건너뛰기
- Siri 건너뛰기
- 인텔리전스 건너뛰기(iOS 18+ 및 macOS 15+)
- 진단 정보 자동 전송 건너뛰기
- Cloud Storage(iOS 10.3+ 및 macOS 10.13.4+) 건너뛰기
- 표시 톤 설정 건너뛰기(iOS 9+ 및 macOS 10.14+)
- 홈 버튼 감도 건너뛰기
- 키보드 선택 화면 건너뛰기
- 온보딩 정보 화면 건너뛰기 – 이 정보는 사용자 교육을 위한 것입니다. 예: 커버 시트, 멀티태스킹 및 제어 센터
- Apple Watch 마이그레이션 화면 건너뛰기
- 스타일 고르기 화면 건너뛰기(iOS 13.0+ 및 macOS 10.14+)
- 스크린 타임(iOS 12.0+ 및 macOS 10.15+) 건너뛰기
- 개인 정보 보호(macOS 10.13.4+ 및 tvOS 11.3+) 건너뛰기
- 잠금 모드 활성화 건너뛰기(iOS 17.1+ 및 macOS 14.0+)
- 소프트웨어 업데이트 건너뛰기(iOS 12.0+ 및 macOS 15.4+)
- 요금제 설정 창 추가 건너뛰기(iPhone Xs, iPhone Xs Max, iPhone XR)
- 로그인 페이지에 사용자 지정 텍스트 표시 - 텍스트 박스에 사용자 지정 텍스트 메시지를 입력하려면 이 옵션을 선택합니다. 기기 등록 설정 중 기기의 로그인 페이지에 이 메시지가 표시되어 과정을 통해 최종 사용자에게 도움이 되도록 추가 지침을 제공합니다.
- 자동 넘어가기 설정 - 이 옵션을 선택하여 기기 설정 화면을 통해 자동으로 넘어가는 지원을 설정할 수 있습니다. 기본은 False로 설정되어 있습니다. tvOS 및 macOS 11 이상 버전 지원. 자동 넘어가기 설정은 Wi-Fi 연결에서 작동하지 않으므로 기기를 이더넷으로 연결해야 합니다.
- 주소 조건 - 주소 조건 창을 건너뜁니다. (iOS 16+)
- Liquid Glass 창 건너뛰기(iOS 27.0+ 및 macOS 27.0+)

**iOS**

- 시작하기 창 건너뛰기(13.0+)
- iMessage 및 FaceTime 건너뛰기(12.0+)
- 음성 언어 건너뛰기(13.0+)

**설정 옵션**

- 복원 완료(14.0+) 건너뛰기
- 업데이트 완료(14.0+) 건너뛰기
- 보안 건너뛰기(16.0+)
- 작업 버튼 설정 창 건너뛰기(17.0+)
- 웹 콘텐츠 필터링 창 건너뛰기(18.2+)
- 안전 및 취급 창 건너뛰기(18.4+)
- 멀티태스킹 창 건너뛰기(26.0+)
- OS 쇼케이스 창 건너뛰기(26.0+)
- 접근성 표시 창 건너뛰기(27.0+)

**macOS**

- iCloud Analytics 화면 건너뛰기
- True Tone 디스플레이 화면 건너뛰기(10.13.6+) - (선택 사항) 이 옵션을 선택하면 True Tone 디스플레이 창을 건너뛰게 됩니다.
- 접근성 건너뛰기(11.0+)
- Watch에서 잠금 해제 건너뛰기(12.0+)
- 잠금 모드 활성화 건너뛰기(14.0+)
- 배경화면 선택 건너뛰기(14.1+)
- 추가 개인정보 보호 설정 창 건너뛰기(26.0+)
- 업데이트 완료(26.0+) 건너뛰기

**tvOS**

- Apple TV 홈 화면 레이아웃 동기화 화면 건너뛰기
- Apple TV 공급업체 로그인 화면 건너뛰기
- 탭하여 설정 옵션 건너뛰기
- 항공촬영 화면보호기 설정 건너뛰기

**macOS 계정 설정 지원 옵션**

- 관리자 계정 생성 건너뛰기
- 기본 설정 계정 생성 건너뛰기
- 기본 계정을 일반 사용자로 생성(체크 표시되지 않은 경우 관리자로 생성)

기기 등록 설정 중 기기 구성 대기

- 구성 및 우선순위가 높은 애플리케이션이 기기로 푸시될 때까지 대기 - 나머지 기기 등록 설정 화면을 계속하기 전에 구성 및 우선순위가 높은 애플리케이션을 기기로 푸시하려면 선택합니다. 이 설정은 필요한 구성 및 우선순위가 높은 애플리케이션이 기기에 푸시되기 전에 최종 사용자가 기기를 사용하지 못하게 합니다.
- 시간 제한 - 기본 시간 제한은 3분입니다. 최대 시간은 10분입니다.
  이 기능을 활성화하려면 기기 등록 프로필을 편집하는 동안 **감독 모드** 옵션을 선택합니다.

**저장**을 클릭합니다.

다음 표는 **관리자** > **Apple** > **기기 등록** 페이지에서 채워집니다.

| 설정 항목 | 수행 작업 |
| --- | --- |
| **Windows**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.)<br>검색 필드를 사용하여 이 열의 항목을 검색합니다 | MDM 서버 이름 |
| **Apple 계정 이름**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.)<br>검색 필드를 사용하여 이 열의 항목을 검색합니다 | 관리되는 Apple ID |
| **기기 수**<br><br>**등록 프로필**<br><br>**마지막 동기화**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.) | 할당된 기기 수<br><br>할당된 기기 등록 프로필 수<br><br>마지막 접속 시간 |
| **토큰 만료**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.) | 토큰 만료 날짜 |

- 새 기기를 Apple 기기 등록에 추가하면 MDM용 Ivanti Neurons에서 새 기기를 발견하기까지 최대 15분이 소요될 수 있습니다. 그런 다음 새 기기가 등록 프로필에 할당됩니다. 새 기기를 기기 등록에 추가할 수 없는 경우 **대시보드 > 알림**으로 이동하여 기기 등록용 Apple 알림을 확인합니다. EULA에 업데이트가 있는 경우 이메일을 통해 새 EULA를 수신하는 단계에 관한 알림을 받습니다.
- Apple 기기 등록을 통한 등록 시 테넌트에 있는 모든 사용자 지정 기기 속성을 확인하고 기기에 할당할 수 있습니다.
- 공유 macOS 기기에서 ListUsers 명령은 기기의 모든 로컬 사용자 목록과 기기를 등록한 사용자의 마지막 체크인 세부 정보만 표시합니다.

## 기기 등록 프로필 편집하기

**절차**

1. **관리** > **Apple** > **기기 등록**으로 이동합니다.
2. Apple 계정 이름 열에서 Apple Business Manager 서버의 이름(Apple 사이트에서 만든)을 찾습니다.
3. 등록 프로필 열에서 숫자 링크를 클릭합니다.
4. 특정 프로필에 대해 **작업** > **기기 등록 프로필 편집**을 선택합니다.
5. 프로필을 업데이트하고 저장합니다.

- 기기 등록 프로필이 편집되면, 수정된 프로필의 기기 수가 곧 업데이트됩니다.
- Apple 사이트에서 서버 토큰을 새로 고치면 기존 토큰이 유효하지 않게 됩니다. 그러나 토큰 만료일 등 기기 등록 페이지에 표시되는 내용은 신규 토큰이 업로드될 때까지 유지됩니다.
- 기기 등록 프로필이 생성되거나 편집되면, 프로필에 대해 변경된 사항을 감사 추적 섹션에서 확인할 수 있습니다. 상세 정보 아래의 링크를 클릭하면, 이전 및 이후 열에서 속성에 대해 변경된 내용을 볼 수 있습니다. 각 기기 등록 프로필의 상태는 생성됨(새 프로필용), 업데이트됨(기존 프로필 편집용), 삭제됨(기존 프로필 삭제용)으로 표시되는 것을 확인할 수 있습니다. 감사 내역에서 기기 등록 프로필을 필터링하려면 관리 시스템을 범주로 선택하고, 자동화된 기기 등록 유형을 유형으로 선택해야 합니다.

기기 등록 프로필에는 다음 세부 정보가 포함되어 있습니다.

| 설정 항목 | 수행 작업 |
|---|---|
| **프로필 이름**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.) | 해당 기기 등록 프로필의 고유한 이름을 입력합니다. |
| **설명**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.) | 프로필 설명을 입력합니다. |
| **부서**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.) | 현재 프로필과 연동되어 있는 소속 조직의 부서를 입력할 수 있습니다. |
| **지원 전화 번호**<br>(영숫자 순으로 정렬하려면 열 제목을 클릭합니다.) | 기기 사용자가 도움이 필요할 때 연락할 수 있는 전화번호를 제공할 수 있습니다. |
| **기기 수** | 프로필의 기기 수 표시 |
| **작업** | 프로필 관리 |

## 여러 기기 등록 프로필 관리

각 Apple Business Manager 서버에 대해 여러 개의 기기 등록 프로필을 만들 수 있습니다. 이렇게 하면 기기 세트마다 서로 다른 구성을 수신할 수 있습니다. 또한 기기를 한 기기 등록 프로필에서 다른 기기 등록 프로필로 옮길 수도 있습니다.

**절차**

1. **관리** > **Apple** > **기기 등록**으로 이동합니다.
2. Apple 계정 이름 열에서 Apple Business Manager 서버의 이름을 찾습니다.
3. 등록 프로필 열에서 숫자 링크를 클릭합니다.
4. 선택한 서버와 연결할 기기 등록 프로필을 새로 만들려면 **프로필 새로 만들기**를 클릭합니다. 프로필을 만들어 저장합니다.
5. 각 프로필을 관리하려면 **작업**을 클릭하고 다음 옵션 중 하나를 선택합니다.
   - **기본 프로필로 설정** - 프로필을 동일한 가상 서버 내의 기본 프로필로 설정합니다. 새 기기 등록에서 이 기본 프로필을 수신하게 됩니다.
   - **프로필 편집** - 기존 프로필을 업데이트합니다.

- **인증 편집** - 기기 등록 인증 설정을 편집합니다.
- **기기 등록 기기 속성 할당** - 관리자는 기기에 대한 사용자 지정 속성을 사용해서 추가 속성을 이 개체에 연결할 수 있습니다. 그 다음 이 속성을 사용해서 그룹을 만들거나 구성을 배포할 수 있습니다.
- **삭제** - 기본 프로필은 삭제할 수 없습니다. 기본값이 아닌 프로필이 삭제되면 연결된 모든 기기가 기본 프로필에 재할당됩니다.

6. 등록된 기기를 한 프로필에서 동일한 가상 서버 내의(서로 다른 Apple Business Manager 서버 간 아님) 다른 프로필로 옮기려면 기기 수 열 아래에 있는 숫자 링크를 클릭합니다. 프로필 재할당은 앞으로 등록할 기기에 적용됩니다.
   1. 단일 기기를 옮기려면 특정 기기에 대한 **등록 프로필 할당**을 클릭하고 드롭다운 목록에서 프로필을 선택한 다음, **할당**을 클릭합니다.
   2. 여러 기기를 이동하려면 기기를 선택한 후 **작업** > **등록 프로필 할당**을 클릭합니다. 드롭다운 목록에서 프로필을 선택하고 **할당**을 클릭합니다.

- 기기 등록 프로필이 편집되면 수정된 프로필의 기기 수가 곧바로 업데이트됩니다.
- Apple 사이트에서 서버 토큰을 새로 고치면 기존 토큰이 유효하지 않게 됩니다. 그러나 토큰 만료일 등 기기 등록 페이지에 표시되는 내용은 신규 토큰이 업로드될 때까지 유지됩니다.

## 사용자 지정 기기 등록 웹 페이지 추가하기

**적용 대상:** iOS 13.0과 macOS 10.15 및 지원되는 최신 버전

사용자 지정 등록 섹션에서 사용자 지정 웹 페이지(웹 뷰)를 지정하여 기기 등록 중에 사용자를 인증할 수 있습니다. 이 페이지를 사용하여 인증 유형, 브랜딩, 동의 텍스트, 개인정보 보호정책 등의 사용자 지정 정보를 표시할 수 있습니다.

**절차**

1. **관리** > **Apple** > **기기 등록**으로 이동합니다.
2. Apple 사이트에 생성한 서버 이름을 확인하세요.
3. **작업** > **기기 등록 프로필 편집**을 선택합니다.
4. 사용자 지정 등록 섹션에서 **사용자 지정 등록 활성화**를 선택합니다.
5. 다음 옵션 중 하나를 선택합니다.
   - **MobileIron에 호스팅된 웹페이지** - 등록이 ID 공급자(예: Microsoft Active Directory Federation Services(ADFS), Okta)를 사용하는 경우 ID 공급자(IDP)로 리디렉션됩니다. 또한 이는 비-IDP 기반 인증을 활용하여 MDM용 Ivanti Neurons 사용자용 셀프 서비스 포털로 리디렉션될 수 있습니다.
   - **사용자 지정 URL** - https://mycustomweburl.com 같은 URL을 입력합니다. 이 URL은 새로운 기기 등록 기기 또는 삭제된 기기를 처음 설정할 때 로드되는 웹 뷰를 통해 사용자 지정 URL 값이 사용자에게 표시되도록 정의합니다. 이 필드를 사용하여 인증 방법으로 자체 인증 UI를 정의하십시오. 사용자가 인증된 후 MDM 등록 프로필이 다운로드됩니다.

### 사용자 지정 기기 등록 웹 페이지의 워크플로

이 섹션에서는 사용자 지정 기기 등록 웹 페이지의 동작 및 사용자 지정 웹 페이지(웹 뷰)를 만드는 절차에 대해 설명합니다.

**URL** 필드에 지정된 사용자 지정 웹 페이지가 처음 로드되는 경우:

- 구성 웹 URL은 **https** 체계를 사용하며 **GET** 요청입니다. 웹 페이지는 공개적으로 신뢰할 수 있는 인증서를 사용해야 합니다.
- 등록이 초기화된 Apple 기기에 의해 사용자 지정 헤더 **x-apple-aspen-deviceinfo**가 GET 요청에 추가됩니다. 여기에는 기기 속성과 함께 plist를 포함하는 CMS(Cryptographic Message Syntax) 엔벨로프의 base64 인코딩이 포함됩니다. 이것은 토큰 기반의 기기 등록으로 초기 POST 요청에서 제공된 것과 동일한 형식의 동일한 정보입니다.

사용자 지정 웹 페이지가 나중에 로드되는 경우:

- 기기 사용자는 관리자의 호스트 서버가 **custom.mobileconfig** 파일을 클라이언트에게 제공할 때까지 웹 페이지(웹 뷰)와 상호작용합니다. MDM용 Ivanti Neurons 서버는 MDM 프로필의 바이트 코드를 반환합니다. 관리자의 호스트 서버에서는 기기의 MDM 프로필이 다운로드되어 기기에 설치되도록 MIME 유형의 **application/x-apple-aspen-config**으로 custom.mobileconfig 파일이 설정되어야 합니다.
- MDM용 Ivanti Neurons의 인증을 위해서는 웹 페이지에 인증 사용자 이름과 비밀번호 자격 증명이 포함되어야 합니다. MDM용 Ivanti Neurons에서 별도의 사용자를 만들고 MDM용 Ivanti Neurons 서버 URL(예: https://micloudDomain.com/c/i/dep/custom.mobileconfig)로 MDM 프로필을 가져와 사용자 지정 등록 역할을 할당하는 것이 좋습니다.
- 기기 등록 및 MDM용 Ivanti Neurons에서 MDM 프로필 가져오기를 위해 관리자의 호스트 웹 서버는 MDM용 Ivanti Neurons 서버 URL에 POST 호출을 해야 합니다. 또한, 기기가 GET URL을 통해 사용자 지정 웹 페이지를 로드할 때 기기가 제공하는 값과 함께 헤더 x-apple-aspen-deviceinfo도 전달해야 합니다. 등록 사용자 ID가 제공되지 않으면 기기는 Nobody 사용자로 등록됩니다. 다음은 추가 정보입니다.
  - 기기가 기기 등록 프로필에 구성된 사용자 지정 웹 URL에 연결되면 관리자의 호스트 웹 서버는 기기가 제공하는 헤더 "x-apple-aspen-deviceinfo"를 캡처해야 합니다.
  - 해당 기기의 MDM 프로필 및 관련 사용자를 가져오려면 관리자의 호스트 웹 서버는 헤더 x-apple-aspen-deviceinfo인 MDM용 Ivanti Neurons 서버 URL로 POST 호출을 수행해야 합니다. MDM용 Ivanti Neurons 사용자 ID를 요청 매개 변수(예: https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com)로 사용하는 기본 인증을 포함해야 합니다. 사용자에게는 사용자 지정 등록 역할이 할당되어야 합니다.
  - 관리자의 호스트 웹 서버가 바이트 코드를 수신한 후에는 응답 헤더 Content-Disposition = attachment;filename="profile.mobileconfig" 및 Content-Type = application/x-apple-aspen-config를 설정하여 바이트 코드를 기기로 다운로드해야 합니다.
- 웹 뷰가 종료되고, OS는 MDM 등록 프로필이어야 하는 프로필의 설치를 시도합니다.

> MDM용 Ivanti Neurons 는 MDM 프로필이 반환된 사용자 ID를 인증하지 않습니다. 따라서 관리자는 MDM 프로필을 요청하기 전에 사용자 ID에 필요한 인증을 수행해야 합니다.

iOS의 경우에는 삭제된 기기를 처음 설정하는 동안 이 워크플로가 지원됩니다. macOS의 경우에는 설정 지원 내에서 그리고 프로필 환경설정 창을 통해서(설정 지원에서 기기 등록을 건너뛴 경우) 이 워크플로가 지원됩니다.

사용자 지정 웹 페이지 만들기와 관련된 개발자 정보를 보려면 다음 Apple 참조 문서를 확인하십시오.

- 웹 뷰
- 웹 뷰를 통한 인증
- 웹 사이트의 데스크톱 또는 모바일 버전을 볼 수 있는 간단한 iPad 웹 브라우저를 구현하기 위한 샘플 코드

## 기기 등록 인증 설정 편집하기

**절차**

1. **관리** > **Apple** > **기기 등록**으로 이동합니다.
2. Apple 사이트에 생성한 서버 이름을 확인하세요.
3. **작업** > **인증 편집**을 선택합니다.

## 모바일 계정에 대한 부트스트랩 토큰 관리

**적용 대상:** Apple School Manager 또는 Apple Business Manager를 통해 MDM에 등록된 macOS 10.15 기기 및 지원되는 최신 버전.

MDM용 Ivanti Neurons 에서는 모바일 계정에 대한 부트스트랩 토큰 관리를 지원합니다. 부트스트랩 토큰을 사용하면 FileVault를 사용하는 macOS 기기에 모바일 계정으로 로그인할 수 있습니다. 이 기능을 사용하면 로그인한 모든 모바일 계정이 SecureToken을 자동으로 받게 됩니다. 이 기능은 여러 사용자가 암호화된 컴퓨터에 로그인하는 경우에 유용합니다.

관리되는 관리자 계정으로 기기에 로그인을 시도하는 경우:

- 첫 번째 로그인인 경우, MDM 서버에서 부트스트랩 토큰을 요청합니다.
- MDM 서버가 부트스트랩 토큰을 제공하는 경우 기기는 계정에 대한 SecureToken을 자동으로 생성합니다.
- 기기 사용자는 FileVault를 사용할 수 있게 됩니다.

부트스트랩 토큰 사용 가능은 새 기기 그룹 또는 사용자 지정 정책을 만드는 동안 기기 상세 정보 페이지에서 필터 속성으로 사용할 수 있는 필드입니다.

문제 해결 및 검증이 목적인 경우 기기의 기기 상세 정보 페이지로 이동합니다. 부트스트랩 토큰 설정 및 부트스트랩 토큰 받기와 같이 작업 이름에 따른 필터를 사용하여 기기 로그를 구체화하려면 로그 페이지를 사용합니다.

## 기기 등록을 사용하여 관리되는 macOS 관리자 계정 설정

MDM용 Ivanti Neurons 는 공장 기본값으로 초기화되거나 처음 활성화되는 기기에 대한 기기 등록 등록을 지원합니다. 기기 등록을 사용하면 macOS 기기에서 관리자 계정을 만들 수 있습니다. MDM용 Ivanti Neurons 에서는 macOS에 대한 선택적 등록만 지원합니다. 따라서 MDM용 Ivanti Neurons에서는 기기 등록 프로필의 **MDM 필수** 필드가 iOS 기기에만 적용되므로 이 필드를 무시합니다.

**절차**

1. **관리 > Apple > 기기 등록**으로 이동합니다.
2. Apple 사이트에 생성한 서버 이름을 확인하세요.
3. **작업 > 기기 등록 프로필 편집**을 선택합니다.
4. macOS 계정 설정에서 다음 지원 옵션 중 하나를 선택합니다.
    - **관리자 계정 생성 건너뛰기** – 관리자 계정(표시 또는 숨김) 생성을 금지하려면 이 옵션을 선택합니다. **관리되는 macOS 관리자 계정 설정** 섹션에서 관리자 계정 생성을 허용하려면 이 옵션을 선택 취소합니다(아래 참조).
    - **기본 설정 계정 생성 건너뛰기** – macOS 기기에서 기본 계정 설정을 건너뛰려면 이 옵션을 선택합니다. 관리자 계정 외에 다른 사용자 계정을 생성하지 않습니다. 추가 섹션인 **관리되는 macOS 관리자 계정 설정**이 표시됩니다(아래 참조). 여기서 관리되는 macOS 관리자 계정을 생성할 수 있습니다. 계정은 사용자 및 그룹에 숨길 수 있습니다.
    - **기본 계정을 일반 사용자로 생성(선택하지 않은 경우 관리자로)** - 등록의 일부로 비관리 표준 계정을 생성하려면 이 옵션을 선택합니다. 관리자 계정은 여전히 관리자가 생성하고 기기에 푸시합니다. 추가 섹션인 **관리되는 macOS 관리자 계정 설정**이 표시됩니다(아래 참조). 여기서 관리되는 macOS 관리자 계정을 생성할 수 있습니다. 계정은 사용자 및 그룹에 숨길 수 있습니다.

위 옵션 중 하나를 선택한 후, 관리되는 macOS 관리자 계정을 생성하고 싶다면 **관리되는 macOS 관리자 계정 설정** 섹션에서 다음 세부 정보를 입력합니다.

- 성명
- 계정 이름
- 비밀번호
- 비밀번호 확인
- (선택 사항) 관리되는 관리자 계정을 사용자 및 그룹에 숨기기

**기본 설정 계정 생성 건너뛰기**를 선택하지 않는 경우 **기본 계정 설정** 섹션에서 다음 상세 정보를 입력합니다. 이는 관리되는 로컬 사용자 바로 가기 이름을 관리자의 바로 가기 이름으로 설정하여 관리되는 관리 계정에 대한 사용자 채널 지원을 추가합니다.

- **전체 이름**
- **약식 이름**
- (선택 사항) **최종 사용자의 수정 방지** - '전체 이름' 및/또는 '약식 이름'에 대체 변수가 있고 비어 있는 것으로 평가되면 이 설정이 재정의됩니다. 이 옵션을 선택하면 이 기본 관리 계정 설정은 아래 옵션 중 하나가 올바로 설정된 경우에만 적용 가능하다는 것을 이해해야 합니다.
  1. 인증 설정 보기에서 사용자 등록/로그인 메시지 표시가 선택된 경우.
  2. 사용자 지정 등록에 대해 MobileIron에 호스팅된 웹페이지가 선택된 경우.

7. 관리되는 관리 계정에 대한 사용자 채널 지원을 활성화하려면 **기본 설정 계정 생성 건너뛰기**를 선택하십시오. 관리되는 로컬 사용자 바로 가기 이름을 관리자의 바로 가기 이름으로 설정할 수 있습니다.
8. **저장**을 클릭하세요.

### 로컬 macOS 관리자 계정 비밀번호 변경

관리자는 기기 등록 동안 설정 지원에서 만들어진 로컬 macOS 관리자 계정의 로컬 비밀번호를 변경할 수 있습니다.

**적용 대상:** macOS 10.11 또는 지원되는 최신 버전.

**절차**

1. **기기**로 이동합니다.
2. 기기 상세 정보 페이지를 보려면 기기와 연결된 사용자 이름을 클릭합니다.
3. 작업 메뉴에서 **macOS 관리자 비밀번호 설정**을 클릭합니다. 기기 목록 페이지에서 하나 이상의 기기를 선택하여 이 작업을 진행할 수도 있습니다.
4. 비밀번호를 입력합니다.
5. **저장**을 클릭하세요.

## CSV로 내보내기

MDM용 Ivanti Neurons 을(를) 사용하면 등록된 기기를 CSV 파일로 내보낼 수 있습니다.

**절차**

1. **관리** > **Apple** > **기기 등록**으로 이동합니다.
2. **기기 수** 열에서 특정 기기 수 링크를 클릭합니다.
3. **CSV로 내보내기** 옵션을 클릭하여 기기 목록과 관련 세부 정보를 CSV 파일로 내보냅니다. 보고서가 준비되면 보고서를 다운로드하거나 삭제하라는 메시지가 표시됩니다. 또한 관리자는 보고서 다운로드 링크가 포함된 이메일을 수신하게 됩니다.
4. **다운로드**를 클릭합니다.
5. (선택 사항) 보고서를 삭제하려면 **삭제**를 클릭합니다.

# 12.3.4. 베타 등록

MDM용 Ivanti Neurons 는 장치가 감독 대상이고 iOS 18, iPadOS 18, macOS 15 이상을 실행하는 경우 나중에 원격으로 장치를 자동으로 등록할 수 있습니다. 필요한 경우, 감독 대상 장치를 베타 프로그램에서 제거하고 사용자가 수동으로 등록하지 않도록 제한할 수 있습니다. 이렇게 되면 사용자가 수동 단계를 수행할 필요가 없어 베타 테스트 라이프사이클 전반의 프로세스가 간소해집니다.

**필수 조건**

- 장치 등록은 베타 등록에 필수적입니다 장치 등록에 대한 자세한 내용은 기기 등록을 참조하세요.
- Apple 계정 없이도 IT용 AppleSeed 베타 버전을 제공하려면 Apple Business Manager 또는 Apple School Manager의 관리자가 IT용 AppleSeed 포털에 로그인하고 현재 베타 기간 동안 조직을 대신하여 이용 약관에 동의해야 합니다.

## 베타 등록에 MDM용 Ivanti Neurons 연결하기

MDM용 Ivanti Neurons(을)를 베타 등록용 MDM 서버로 사용하려면 MDM용 Ivanti Neurons에서 Apple Business Manager 또는 Apple School Manager 서버 토큰을 설정합니다.

**베타 등록 섹션**

| 이름 | 설명 |
| --- | --- |
| **조직 이름** | 조직의 이름입니다. |
| **마지막 동기화** | 동기화가 수행된 날짜와 시간입니다. |
| **상태** | 동기화 상태입니다. |
| **베타 등록 토큰 동기화** | 베타 업데이트를 위해 새 베타 등록 토큰을 동기화하려면 **동기화**를 클릭합니다. |

# 12.3.5. 설정 도우미 구성

구성 설정 도우미를 사용하면 iOS 및 macOS 기기에 대한 기기 설정 중에 건너뛰거나 포함할 설정 화면을 선택할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리 콘솔로 로그인합니다.
2. **구성**으로 이동합니다.
3. **설정 도우미**를 선택합니다.
4. 연필(편집) 아이콘을 클릭합니다.
5. 기기에서 특정 설정 화면을 건너뛰려면 확인란을 선택합니다.
6. **완료**를 클릭하세요.
7. **기기 채널**을 선택합니다.
8. **모든 기기**를 선택합니다. 설정 지원 구성이 기기로 푸시되고 기기 세부 정보 페이지의 구성 탭에 설치됨 상태가 표시됩니다.
9. 기기에 로그인합니다. 모든 초기 설정 화면을 건너뜁니다.

# 12.3.6. MDM 인증서 설치

iOS 기기를 관리하려면 Apple MDM 인증서를 요청해 설치해야 합니다. 또한 설치한 인증서는 매년 갱신해야 합니다. (인증서 생성에 사용된 Apple 계정은 만료 날짜가 가까워지면 Apple 사이트에서 알림을 받습니다.) MDM 인증서 페이지를 사용하여 이 인증서를 추가하거나 갱신합니다.

## MDM 인증서 요청 및 설치

**절차**

1. **MDM 인증서** 페이지를 사용하여 MDM용 Ivanti Neurons 테넌트에서 인증서 서명 요청(CSR)을 다운로드합니다.
2. CSR을 Apple에 업로드해 새 인증서를 생성할 수 있습니다.
3. Apple 사이트에서 인증서의 용도를 표시하는 메모를 추가할 수 있습니다. 해당 메모를 통해 인증서를 갱신할 시기를 확인할 수 있습니다. 발급된 인증서를 저장하세요.
4. MDM용 Ivanti Neurons 테넌트의 인증서를 설치합니다.

## MDM 인증서 갱신

**절차**

1. **인증서 갱신**을 클릭합니다.
2. MDM용 Ivanti Neurons 테넌트에서 인증서 서명 요청(CSR)을 다운로드합니다.
3. CSR을 Apple에 업로드하여 해당 인증서를 갱신합니다.
4. Apple 사이트에서 갱신할 인증서가 맞는지 반드시 확인 후 갱신하시기 바랍니다. MDM용 Ivanti Neurons에 다른 인증서를 업로드할 경우 등록된 iOS 기기가 모두 자동 폐기됩니다.
   MDM용 Ivanti Neurons 테넌트의 인증서를 설치합니다.

잘못된 인증서 업로드를 시도할 경우 경고 메시지가 표시됩니다.

**MDM 인증서 설치** 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.

- 시스템 관리
- 시스템 읽기 전용

# 12.3.7. 기업용 공유 iPad 기기

기업용 공유 iPad 기기는 iOS 13.4 또는 지원되는 최신 버전의 Apple Business Manager에서 생성된 관리되는 Apple ID에 사용할 수 있습니다.

- 공유 iPad 기기를 사용하면 기업에서 여러 직원 간에 기기를 공유하는 동시에 맞춤식 경험을 제공할 수 있습니다.
- 직원은 관리되는 Apple ID로 로그인하여 메일 계정, 파일, iCloud 사진 보관함, 앱 데이터 등을 포함한 데이터 로드를 시작할 수 있습니다.
- 데이터는 iCloud에 저장되므로 직원은 조직에 속한 모든 공유 iPad 기기에 로그인할 수 있습니다.

공유 iPad 기기는 의료, 소매 및 산업 응용 프로그램에서 사용할 수 있습니다. 예를 들어 의사와 간호사는 각각 고유하게 설계된 사용자 프로필에 안전하게 액세스할 수 있으므로 하나의 iPad 기기를 공유할 수 있습니다. 소매점의 일선 작업자는 제품 정보, 리소스, 전문 기술 등에 액세스하여 고객을 만족시키고 보다 나은 쇼핑 경험을 제공할 수 있습니다.

**작동 원리**

- iPad 기기가 Apple Business Manager에 추가되고 공유 모드가 켜진 상태에서 자동화된 등록 프로필을 사용하여 등록됩니다.
- 직원은 회사에서 제공한 관리형 Apple ID 및 비밀번호를 사용하여 공유 iPad 기기에 로그인합니다. Apple Business Manager 관리자는 사용자에 대한 계정을 수동으로 생성하거나 계정 생성을 Entra ID와 같은 ID 제공자와 연동할 수 있습니다.
- 각 사용자는 공유 iPad 기기에 로그인할 때 사용자 지정 프로필을 가질 수 있습니다. 관리자는 사용자의 역할, 책임, 부서에 따라 앱을 배포할 수 있습니다.
- 사용자는 공유 iPad 기기에서 게스트 사용자로 로그인할 수 있습니다. 게스트 사용자 로그인은 기본적으로 활성화되어 있습니다. 게스트 사용자는 관리되는 Apple ID 및 비밀번호로 로그인할 필요가 없습니다. **iOS 제한** 구성에서 **공유 iPad에 대한 게스트 세션 허용** 옵션을 **False**로 설정하여 게스트 사용자 로그인을 비활성화할 수 있습니다.
- MDM용 Ivanti Neurons **> 기기**로 이동하고 공유 iPad 기기 이름을 클릭한 후 **사용자** 탭을 클릭하여 기기의 사용자 목록과 세부 정보(예: 관리형 Apple ID, 사용 가능한 데이터(바이트), 사용된 데이터(바이트), MDM용 Ivanti Neurons에 동기화할 데이터 있음)을 확인합니다.
- **로그** 탭으로 이동하여 필터에서 **사용자 목록 보고** 작업을 선택하여 추가 사용자 세부 정보를 확인합니다.
- 공유 iPad 기기의 게스트 사용자 로그인은 MDM용 Ivanti Neurons의 게스트 사용자 관리와 다릅니다. MDM용 Ivanti Neurons에서는 기본적으로 게스트 사용자 계정이 비활성화됩니다. 공유 iPad 기기에서 게스트 사용자를 관리하려면 게스트 사용자 계정을 활성화합니다.
- 화면 녹화는 공유 iPad 기기의 제어 센터에서 사용할 수 있습니다.
- MDM용 Ivanti Neurons 는 관리되는 Apple ID, `${managedAppleID}` 에 대한 대체 변수를 지원합니다. 이 시스템 변수는 시스템 속성 섹션 및 기기 속성 섹션에 표시됩니다.
- MDM용 Ivanti Neurons 은(는) 관리자가 현재 로그인한 사용자와 함께 과거에 공유 iPad 기기에 로그인했던 상주 사용자의 관리되는 Apple ID를 변경하지 못하도록 제한합니다. 관리되는 Apple ID를 변경하려 시도하면 사용자가 공유 iPad 기기를 사용하고 있기 때문에 사용자의 관리되는 Apple ID를 변경할 수 없다는 오류 메시지가 표시됩니다.
- **Apple Apps and Books**의 경우 기기 기반 라이선스 선택 여부와 관계없이 공유 iPad 기기에 Apps and Books가 기기 기반 라이선스 기반으로 설치됩니다.

**필수 조건**

다음 필수 조건이 충족되어야 합니다.

- 공유 iPad 기기에는 관리형 Apple ID가 필요합니다. 관리자는 계정을 수동으로 만들거나 Entra ID와 같은 ID 제공자와 연동할 수 있습니다.
- 공유 iPad 기기에는 iOS 13.4 또는 지원되는 최신 버전이 포함되어야 합니다.
- 기기는 Apple Business Manager 계정과 연결되어 있어야 합니다.
- 기기에는 32GB 이상의 저장 공간이 있어야 합니다.

참고:

- MDM용 Ivanti Neurons 은(는) Apple에서 지원하지 않으므로 공유 iPad 기기에 대해 암호와 같은 특정 구성을 제한합니다. 그러한 구성은 기기로 푸시되지 않습니다(기기 > 기기 이름 링크 클릭 > 구성 탭).
- 암호 구성은 공유 iPad 기기에는 적용되지 않습니다. 공유 iPad 기기에는 암호가 아닌 비밀번호와 연결된 관리형 Apple ID가 필요하기 때문입니다. MDM용 Ivanti Neurons 관리 포털의 잠금 해제 작업은 공유 iPad 기기의 암호를 지우지 않습니다.
- iOS 제한 구성을 공유 iPad 기기에 배포하는 동안 기기 채널 또는 사용자 채널 중 하나를 선택합니다. 별도의 구성을 배포하고 기기나 사용자 채널에만 해당되는 제한을 실행할 수 있습니다.
- MDM용 Ivanti Neurons 은(는) 만료된 계정을 확인하고 만료된 계정을 사용하는 기기를 소유자로서 사용 중지합니다. 그러나 공유 iPad 기기의 경우 기기 소유자는 마지막으로 로그인한 사용자이며 법적 소유자가 아닐 수 있습니다. 소유자 계정이 만료되면, 공유 iPad 기기가 사용 중지되지 않도록 MDM용 Ivanti Neurons은(는) 제외됩니다.
- iOS용 Go 클라이언트는 공유 iPad 기기에 대해 지원되지 않습니다.
- 사용자는 공유 iPad 기기에서 사용 중지 및 지우기와 같은 작업을 수행할 수 없습니다. 오직 관리자만이 MDM용 Ivanti Neurons 관리 포털에서 사용 중지 및 지우기 작업을 수행할 수 있습니다.
- 관리자는 MDM용 Ivanti Neurons 관리 포털에서 공유 iPad 기기의 소유자를 변경할 수 없습니다.
- 공유 iPad 기기에는 Zero Sign-On이 지원되지 않습니다.
- ListUsers 명령이 활성화되면 모든 관리 사용자 ID와 해당 체크인 시간이 **관리** 탭 아래의 기기 등록(Apple Business Manager의 일부)에 표시됩니다.

## 공유 iPad 기기 구성

공유 iPad 기기를 설정하고 해당 설정을 구성할 수 있습니다.

**절차**

1. **관리** > **Apple** > **기기 등록**으로 이동합니다.
2. 자동화된 기기 등록 프로필을 사용하여 기기를 등록하여 기기를 Apple Business Manager에 추가합니다. 이 절차에 대한 자세한 내용은 기기 등록을 참조하십시오.
3. 기기 등록 설정에서 다음을 활성화합니다.
   - **감독 모드**.
   - **기업용 공유 iPad 기기**의 **다중 사용자 모드**.
4. (선택 사항) 로컬 사용자 계정을 만듭니다. 기기가 이 사용자에게 등록됩니다. 이 사용자에 대한 인증은 등록 중 단 한 번만 이루어집니다.
5. 공유 iPad를 재설정합니다.

> 등록 프로세스는 재설정 후에 시작됩니다. 기기를 공유 iPad 기기로 등록하고 구성하는 데는 몇 분 정도 소요됩니다.

6. 법적 소유자는 기기를 등록한 사용자 계정에 할당됩니다. 관리자는 **기기** 페이지에서 법적 소유자를 변경할 수 있습니다.
7. 기기 로그인 화면에서 사용자의 관리되는 Apple ID 자격 증명을 입력합니다.
   - macOS 기기와 유사하게 기기 및 사용자 채널을 통해 공유 iPad 기기의 구성을 푸시할 수 있습니다.
   - 사용자 대체 변수는 기기 채널에 푸시된 구성(관리 앱 구성 포함)을 대체하지 않습니다.
   - 공유 iPad 기기에 로그인한 사용자가 관리되는 사용자가 아닌 경우 관리되는 Apple ID는 MDM용 Ivanti Neurons 관리 포털의 어떤 사용자에게도 속하지 않으며 기기는 누구에게도 할당되지 않습니다. 사용자는 관리되지 않음 - 관리자는 MDM용 Ivanti Neurons에서 사용자 채널 구성을 푸시할 수 없습니다.

- MDM용 Ivanti Neurons에 의해 생성된 기본값 게스트 사용자의 기본 상태는 비활성화되어 있습니다. 게스트 사용자가 로그인하면 기기가 사용자에게 할당되지 않고 사용자는 관리되지 않습니다. 게스트 사용자를 관리해야 하는 경우 MDM용 Ivanti Neurons에서 생성된 기본 게스트 사용자를 활성화해야 하며 게스트 사용자가 로그인한 후 기기는 기본 게스트 사용자에게 할당됩니다. 그런 다음 사용자를 관리할 수 있습니다.
- 기기 소유자 정보는 MDM용 Ivanti Neurons > **기기** 페이지 및 기기 로그(기기 세부 정보 페이지 > **로그**)에 표시됩니다.

## 공유 iPad의 법적 소유자 관리

기기 목록 페이지에서 이메일 ID를 사용하여 공유 iPad 기기의 법적 소유자를 검색하고 볼 수 있습니다. 기존 법적 소유자를 새로운 법적 소유자에게 재할당하여 공유 iPad 기기의 법적 소유자를 변경할 수 있습니다. 공유되지 않은 iPad 기기의 법적 소유자가 재할당된 경우 MDM용 Ivanti Neurons은(는) 할당을 무시합니다.

**절차**

1. **기기**로 이동합니다.
2. 톱니바퀴 아이콘을 클릭하여 **법적 소유자** 열을 선택하고 기기 목록 페이지에 추가합니다.
3. 공유 iPad 기기를 선택합니다.
4. **작업 > 법적 소유자에게 할당**을 클릭합니다.

## 공유 iPad 기기의 법적 소유자에게 이메일 보내기

공유 iPad 기기의 법적 소유자에게 이메일을 보낼 수 있습니다.

**절차**

1. **기기**로 이동합니다.
2. 공유 iPad 기기의 이름을 클릭합니다.
3. **이메일** 아이콘을 클릭합니다.
4. 이메일을 작성합니다.
5. **보내기**를 클릭하세요.

## 다중 사용자 모드 속성 사용

MDM용 Ivanti Neurons에서 공유 iPad 기기의 다중 사용자 모드 속성을 사용할 수 있습니다.

**절차**

1. **기기** 페이지에서 **다중 사용자 모드** 속성을 사용합니다.
2. **고급 검색**을 클릭하고 **다중 사용자 모드** 속성을 사용하여 기기를 찾는 규칙을 만듭니다.
3. **기기 > 기기 그룹** 페이지에서 **다중 사용자 모드** 속성을 사용하여 공유 iPad 기기에 대한 동적 기기 그룹을 만듭니다. 예를 들어 이 그룹을 배포 필터로 사용하여 구성을 배포할 수 있습니다.
4. **정책** 페이지에서 **다중 사용자 모드** 속성을 사용하여 공유 iPad 기기에 대한 사용자 지정 정책을 생성합니다.
5. **앱 > 배포 필터**에서 **다중 사용자 모드** 속성을 사용하여 설치에 사용할 수 있는 애플리케이션 수를 제한합니다.

- MDM용 Ivanti Neurons 는 Apple School Manager 기기에 대해 다중 사용자 모드를 지원하지 않습니다. 설정을 활성화하여 기기 등록 프로필을 Apple School Manager 기기에 푸시하는 것은 바람직하지 않습니다.

- iOS용 다중 사용자 보안 로그인 구성은 공유 iPad 기기에 적용할 수 없습니다.

## 공유 iPad 기기에서 사용자 삭제

공유 iPad 기기에서 사용자 또는 여러 사용자 계정을 삭제할 수 있습니다. 사용자 목록 탭에 현재 로그인한 사용자의 **활성** 레이블이 표시됩니다. 삭제 옵션은 공유 iPad 기기에서 현재 로그인한 사용자에게는 적용할 수 없습니다. 사용자는 **기기** 또는 **사용자** 탭에서 삭제할 수 있습니다.

**기기 탭에서 사용자 삭제**

**절차**

1. **기기** 탭 > **기기 세부 정보**로 이동합니다.
2. **사용자** 탭으로 이동합니다. 사용자 목록이 표시됩니다.
3. **모든 사용자 삭제**를 클릭합니다.
4. 특정 사용자를 삭제하려면 "-" 빼기 기호를 클릭합니다.
    - (선택 사항) **사용자 삭제** 창에서 **MDM용 Ivanti Neurons에 대한 데이터 동기화가 보류 중인 경우에도 사용자 강제 삭제** 옵션을 선택하고 **예**를 클릭합니다.

      > **MDM용 Ivanti Neurons에 대한 데이터 동기화가 보류 중인 경우에도 사용자 강제 삭제**를 선택하면 데이터가 MDM용 Ivanti Neurons 관리 포털에 아직 동기화되지 않은 경우에도 사용자가 강제로 삭제됩니다.

**사용자 탭에서 사용자 삭제**

**절차**

1. **사용자** 탭으로 이동합니다.
2. 사용자 또는 여러 사용자를 선택하고 **작업** 드롭다운 메뉴로 이동하여 **삭제**를 클릭합니다. 확인 메시지가 나타납니다. 확인 후 사용자 삭제 명령이 기기에 실행됩니다.
3. 기기 세부 정보에서 **기기 로그**로 이동하고 사용자 삭제 명령이 공유 iPad 기기의 선택된 사용자에게 전송되었는지 확인합니다.

## 공유 iPad 기기에서 사용자 로그아웃

관리자는 공유 iPad 기기에서 사용자를 로그아웃시킬 수 있습니다.

**절차**

1. **기기** 페이지에서 공유 iPad 기기를 선택합니다.
2. **작업** 메뉴에서 **강제 로그아웃**을 선택합니다. 공유 iPad 기기에서 사용자를 로그아웃시킬지 확인하는 팝업 창이 나타납니다.
3. 강제 로그아웃을 승인하려면 **확인**을 클릭합니다.

# 12.3.8. School Manager

## 라이센스: Gold

**적용 대상:** 관리 상태인 iOS 9.3+

Apple School Manager는 교육 기관 전용 Apple 클라우드 서비스로서 Apple Apps 및 Books의 애플리케이션 구입, Apple 기기 등록을 통한 iPad 등록, 관리되는 Apple ID 만들기와 같은 서비스를 제공합니다. Apple School Manager와 완전 통합된 MDM용 Ivanti Neurons UEM 솔루션을 사용하면 교사와 학생에게 지정된 iPad를 완전히 관리하여 Classroom과 같은 앱과 School Manager 에코시스템을 원활하게 활용할 수 있습니다.

> Apple Books는 지원되지 않습니다.

## School Manager 구성

1. **관리 > School Manager**로 이동합니다.
2. **Education 설정** 옵션이 비활성화되어 있으면 이를 클릭합니다.
3. 다음 옵션 중 하나를 선택합니다.
   - **Apple School Manager 계정과 동기화하여 학교 정보 가져오기**:
     1. **관리 > Apple > 기기 등록**으로 이동하여 사용자 조직의 주요 파일을 다운로드합니다.
     2. 주요 파일을 Apple School Manager 계정으로 업로드하여 암호화 키를 생성합니다.
     3. Apple School Manager에서 암호화 키를 다운로드하여 MDM용 Ivanti Neurons에 업로드합니다(**관리자 > Apple > 기기 등록**).

        > 기존 Apple 기기 등록 계정으로 Apple Education을 이용할 수도 있습니다. Apple에서는 기기 등록 계정을 업그레이드하여 Apple School Manager에 액세스할 시 Education 기능을 이용할 수 있는 옵션을 제공합니다. 자세한 업그레이드 관련 설명은 https://support.apple.com/en-in/HT206960에서 볼 수 있습니다.

     암호화 키가 통과되면 **지금 동기화** 버튼이 나타납니다.

     4. **지금 동기화**를 클릭하여 Apple School Manager와 데이터 동기화를 시작합니다.
   - **CSV 파일에서 데이터 가져오기**:
     1. (선택 사항) **CSV 템플릿 ZIP 파일 다운로드**을 클릭하여 전체 데이터 유형의 템플릿이 들어있는 zip 파일을 다운로드합니다.
     2. **파일 선택...**을 클릭합니다.
     3. 다음의 6가지 CSV 파일을 추가합니다.
        - 학생 데이터 파일(students.csv)
        - 명단 데이터 파일(roster.csv)
        - 직원 데이터 파일(staff.csv)
        - 수업 데이터 파일(classes.csv)
        - 과정 데이터 파일(courses.csv)
        - 위치 데이터 파일 (locations.csv)

        > 업로드하기 전 매번 반드시 이 여섯 가지 CSV 파일을 모두 선택해야 합니다.

**업로드**를 클릭합니다.

4. (선택 사항) CSV 파일을 수정해야 할 시에는 이전에 업로드한 6개 파일 전체의 필요한 모든 데이터를 그대로 유지해야 합니다. 필요한 내용을 편집하고 다시 모두 업로드합니다.

**클래스** 및 **개인** 탭에서 데이터를 검색합니다.

> 개인(학생 및 교직원)도 MDM용 Ivanti Neurons의 **사용자** 페이지에 나타납니다.

5. 다음과 같이 학생과 교직원이 교육에 사용할 기기에 대해 두 개의 기기 그룹을 만듭니다.
    1. **관리 > 사용자 지정 속성**으로 이동합니다.
    2. 동적으로 관리되는 기기 그룹을 생성하는 데 사용할 학생 및 직원의 사용자 지정 속성을 생성합니다.
    3. **기기 > 기기 그룹**으로 이동합니다.
    4. **추가+**를 클릭합니다.
    5. 앞서 생성한 사용자 지정 속성을 필터로 이용하여 학생과 직원을 위한 각 동적 관리 기기 그룹을 생성합니다.
6. **기기** 페이지에서 **작업 > 사용자에 할당** 옵션을 이용하여 학생 및 직원에게 등록된 기기를 할당합니다.
7. **구성 >** 교육 페이로드를 추가하여 리더(직원) 구성과 구성원(학생) 구성을 생성합니다.
8. 리더(직원) 구성 및 구성원(학생) 구성을 직원과 학생 기기 그룹에 배포합니다.
   이 배포를 통해 구성 및 설치 인증서를 각 기기에 푸시할 수 있습니다.

> **관리 > School Manager** 페이지에서 수업 이름의 값이 없다면 이 값은 수업 시스템 소스 식별자 및 과정 식별자 필드에서 파생됩니다.이 필드는 Apple School Manager 또는 CSV 파일에서 선택 사항입니다. 다만 수업 이름이 없을 시 이 합계를 기본 식별자로 사용하게 되므로 항상 값을 입력하는 것이 좋습니다.

## Classroom 앱을 교사에게 푸시하기

Classroom 앱을 이용하여 교사(리더)들은 다음과 같은 상황을 관리할 수 있습니다.

- iPad 및 앱을 원격으로 제어할 수 있는 교실 관리 기능.
- 수업 그룹 생성 기능
- 교사가 그룹 내 학생 구성원을 볼 수 있는 기능.
- 교사가 그룹 내 학생에게 컨텐츠를 발송할 수 있는 기능.
- 학생이 볼 수 있는 앱과 컨텐츠 제한.

Apple App Store에서 클래스룸 앱을 푸시할 수 있습니다.

**절차**

1. **앱 > App Catalog** 페이지로 이동합니다.
2. **+추가** 버튼을 클릭합니다.
3. Apple의 Classroom 앱을 검색하여 선택합니다.
4. **다음**을 클릭하세요.
5. 카테고리와 설명을 입력합니다.
6. **다음**을 클릭하세요.
7. 이전에 생성된 교사 기기 그룹에 앱을 배포합니다.

8. 앱 구성 페이지에서 앱 설정을 구성합니다.
9. **완료**를 클릭하세요.

## School Manager 비활성화

School Manager를 비활성화하면 현재 데이터가 모두 삭제됩니다. 주의해서 실행해 주십시오.

1. **관리 > School Manager**로 이동합니다.
2. **Education 설정** 옵션이 활성화되어 있으면 이를 클릭합니다.
3. **예**를 클릭합니다.

# 12.3.9. 설정(Apple)

관리자는 Apple 기기의 다양한 설정을 구성, 활성화 및 비활성화할 수 있습니다.

## 자동 등록(macOS만 해당)

macOS 기기용 자동 등록은 활성화 상태로 잠겨 있습니다. 이것은 테넌트의 모든 새 기기 등록에 해당되며 Mobile@Work 1.4 또는 지원되는 최신 버전에서 지원됩니다.

## 일반 설정

**기기 조정 비활성화** - 관리자는 동일한 기기를 다시 등록하려는 경우 기기 항목을 유지할 수 있습니다. 기본적으로 이 옵션은 선택되지 않았습니다. 이 옵션을 선택하면 비활성 기기 세부 사항을 유지할 수 있습니다.

> 기기 조정 비활성화가 활성화되지 않은 상태에서 기기를 동일한 사용자로 다시 등록하면, 새 항목이 생성됩니다. 그렇지 않으면, 기기 항목이 새로운 등록 정보로 업데이트됩니다.

## 프로필 설정

관리자는 MDM 프로필이 설치되지 않은 경우 최종 사용자에게 이메일 보내기 및 macOS와 iOS용 Go에 알림 보내기를 활성화 또는 비활성화할 수 있습니다. MDM 프로필 알림 기능이 기본적으로 활성화됩니다.

**절차**

1. **관리 > 설정**으로 이동합니다.
2. **MDM 프로필이 설치되지 않은 경우 사용자에게 이메일 보내기 및 클라이언트에게 알림 보내기** 옵션을 선택 또는 취소합니다.
3. 최대 이메일/알림 수를 1 ~ 4 중에서 선택합니다.
4. **저장**을 클릭하세요.

## 자동 기기 등록에 대한 OS 업데이트(iOS만 해당)

관리자는 자동 기기 등록에 대한 iOS 운영 체제 업데이트를 켤 수 있습니다. 이 옵션이 활성화되면 기기 등록 기기가 기기 등록 프로필의 OS 업데이트 일정 설정 대신 **소프트웨어 업데이트** 구성을 사용하게 됩니다.

이 옵션은 기본으로 비활성화되며 이 경우 기기 등록 프로필의 OS 업데이트 일정 설정이 사용됩니다. 이 설정을 켜는 것은 영구적이며 끌 수 없습니다. 이 설정은 사용 가능한 모든 기기 등록 프로필의 OS 업데이트 일정 설정을 제거하게 됩니다.

> 감독 비 기기 등록 기기는 소프트웨어 업데이트 구성을 사용합니다.

**절차**

1. **관리 > 설정**으로 이동합니다.
2. **자동 기기 등록에 대해 소프트웨어 업데이트 구성 사용** 옵션을 선택하거나 선택 해제합니다.
3. **예**를 눌러 확인합니다.
4. **저장**을 클릭하세요.

## 다중 사용자 보안 로그인

관리자는 관리 > Apple > 설정의 "**다중 사용자 보안 로그인**" 섹션에서 "**사용자 로그아웃 후 암호 지우기**" 옵션을 선택하여 사용자가 iOS 공유 기기의 다중 사용자 보안 로그인 웹 클립에서 로그아웃하면 기기 비밀번호를 지울 수 있습니다.

## 제한 구성을 위한 우선순위 설정

관리자는 **관리 > Apple > 설정**의 **제한 구성을 위한 우선순위 설정** 섹션에서 **iOS 제한 구성** 또는 **macOS 제한 구성** 옵션을 선택하여 복수의 iOS 및 macOS에 대해 우선순위를 활성화할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다. 우선 순위의 작동에 대한 자세한 내용은 구성 우선순위 지정을 참조하십시오.

**절차**

1. **관리자 > Apple > 설정**으로 이동합니다.
2. **제한 구성을 위한 우선순위 설정** 섹션에서 **iOS 제한 구성** 또는 **macOS 제한 구성** 옵션을 선택합니다.
3. **저장**을 클릭하여 우선순위를 활성화합니다. "**제한 구성을 위한 우선순위 설정(iOS 또는 macOS)이 활성화되었습니다**" 배너가 표시됩니다. 우선순위가 **승인**되기 전:
    - **배포 요약 편집(해당하는 경우)**: 우선순위 설정이 활성화되면 선택한 제한 구성의 배포 요약이 기본적으로 "**다른 공간에 있는 기기에 적용**"에서 "**다른 기기 공간에 있는 모든 기기에 가장 높은 우선순위로 적용**"으로 변경됩니다.
    - **기본 우선순위가 생성 순서대로 할당됨**: 선택한 제한 유형 구성의 경우 생성된 순서대로 기존의 기본 우선순위가 할당됩니다.
    - **구성 관리 일시 중지**: 선택한 제한 구성(예: iOS 제한 구성)의 관리가 우선순위를 승인할 때까지 일시 중지됩니다.

> 우선순위가 활성화되면 제한 변경 사항이 승인될 때까지는 처리되지 않습니다. 승인 전에 관리자는 **구성** 섹션에서 제한 구성에 대한 배포, 배포 요약 또는 우선순위를 편집할 수 있습니다.

4. **승인** 옵션을 선택하여 우선순위를 발효합니다.
5. **저장**을 클릭하세요.

> iOS 또는 macOS 제한 구성 옵션을 선택 취소하면 **승인** 옵션을 사용할 수 없으며, 변경 사항이 즉시 적용됩니다.

우선순위 설정이 비활성화되면 구성과 연결된 우선순위는 취소됩니다. 해당되는 경우 모든 제한 구성이 기기에 푸시됩니다(다음 기기 동기화 시).

- **배포 요약(해당하는 경우): 제한 구성에 대한 우선순위 설정이 비활성화되면 배포 요약은 다른 기기 공간에 있는 모든 기기에 가장 높은 우선순위로 적용 또는 다른 기기 공간에 있는 모든 기기에 가장 낮은 우선순위로 적용에서 "다른 공간에 있는 기기에 적용"으로 변경됩니다.**
- **우선순위가 할당되지 않음**: 선택한 제한 구성에 대해 할당된 우선순위가 제거됩니다.

# 12.4. Windows 기기 사용 작업

이 섹션에는 다음 주제가 포함됩니다.

- Windows Autopilot 프로필 구성
- Windows Autopilot 프로필의 감사 추적
- TenantLockdown CSP
- ADMX(GPO) 브라우저
- 앱 인벤토리 간격 설정
- 하드웨어 인벤토리

# 12.4.1. Windows Autopilot 프로필 구성

Windows Autopilot은 관리자가 새로운 기기로 언제든 비즈니스를 수행할 수 있도록 설정하고 사전 구성하는 데 도움을 주는 Microsoft 기능입니다. Autopilot 기능은 Windows Desktop 또는 HoloLens2 기기를 빠르고 안정적이며 원활하게 프로비저닝하는 데 유용합니다. 뿐만 아니라 Autopilot 기능은 다음 작업을 수행하는 데 도움을 줍니다.

- Entra ID(Entra ID)에 기기 자동 연결
- 기기를 MDM 서비스에 자동으로 등록합니다.
- 기기 프로필을 기반으로 기기를 생성하여 구성 그룹에 자동 할당합니다.
- 등록 환경을 사용자 정의합니다.
- 구성 및 정책을 적용합니다.
- 필수 애플리케이션을 설치합니다.

## 필수 조건

Windows Autopilot 페이지를 작동하려면 MDM용 Ivanti Neurons 파트너 단계 및 Azure 라이선싱 요구 사항을 검토하십시오. Autopilot 기능이 예상대로 작동하려면 다음 전제 조건이 충족되는지 확인하십시오.

- **Autopilot 요구 사항에 대한 Azure 라이선싱**: "Windows Autopilot 라이선싱 요구 사항"을 확인합니다.
- **Azure Windows Autopilot 장치 등록**: "Windows Autopilot 등록 개요"를 확인합니다.
- **고객 계정에 장치를 추가하는 리셀러**: "새 장치에서 Windows Autopilot 프로필을 사용하여 고객의 초기 경험 사용자 지정"을 확인합니다.

## 추가 요구 사항

1. Entra ID 테넌트 및 MDM용 Ivanti Neurons를 통합합니다. 자세한 내용은 **Microsoft Azure 설정**을 참조하십시오.
2. MDM용 Ivanti Neurons 및 Entra ID에 관리자 계정이 있는지 확인하십시오.
3. 자체 배포 프로필을 활용하려면 MDM용 Ivanti Neurons에서 사용자가 없는 자체 배포 장치를 등록하기 위한 가짜 사용자를 만드십시오.
4. Entra ID 기본 도메인에서 더미 사용자 fooUser@Entra IDPrimaryDomain.com을 만들고 동기화합니다.

> 더미 사용자를 만들고 동기화하는 데 Microsoft 라이선스가 필요하지 않습니다.

5. Entra ID의 "사용자 지정 도메인 이름" 페이지에 Entra ID 환경의 기본 도메인이 표시됩니다.
6. 사용자가 장치를 등록할 수 있고 비활성화되지 않았는지 확인하십시오. 예를 들어 기본 도메인이 contoso.com인 경우 그 결과로 나온 사용자는 fooUser@contoso.com이 됩니다. 기본 도메인이 contoso.onmicrosoft.com인 경우 그 결과로 나온 사용자는 fooUser@contoso.onmicrosoft.com이 됩니다.
7. SCIM이 있는 사용자를 MDM용 Ivanti Neurons에 프로비저닝하려면 Entra ID에서 사용자 세부 정보를 편집하고 이메일 주소를 추가합니다. 일반적으로 이메일 주소는 UPN과 동일합니다.
8. fooUser를 포함한 모든 사용자가 Azure 및 MDM용 Ivanti Neurons에 있는지 확인합니다.
9. 관리자는 비즈니스용 Microsoft Store 또는 MDM용 Ivanti Neurons를 사용하여 Autopilot 프로필을 만들 수 있습니다. MDM용 Ivanti Neurons 관리자로 프로필을 만들려면 글로벌 Entra ID 관리자 및 Intune 관리자 권한이 필요합니다.

> 관리자에게는 Azure P1 또는 P2가 필요하고 MDM Secure UEM용 Ivanti Neurons 또는 Secure UEM Premium 라이선스가 필요합니다. Intune 라이선스는 관리자에게 필요하지 않습니다.

MDM용 Neurons에서 Autopilot 프로필 생성 기능은 아직 베타 버전인 Autopilot용 Microsoft Graph API를 활용합니다.

## Autopilot 등록 모드

기기를 특정 사용자 프로필 그룹과 연결한 후 기기 용도에 따라 사용자가 자신의 기기를 빠르게 시작할 수 있도록 Autopilot 등록 모드를 구성할 수 있습니다. MDM용 Ivanti Neurons는 다음과 같은 Autopilot 등록 모드를 제공합니다.

- 자체 배포 모드
- 사용자 주도(사전 프로비저닝된 모드)
- 사용자 주도

**자체 배포 Autopilot 모드** - 자체 배포 Autopilot 장치 등록 모드는 초기 장치 설정을 우회하고 장치가 안전하게 시작하는 데 필요한 모든 필수 구성 파일을 푸시하여 사용자를 위한 엔터프라이즈 장치가 원활하게 배포되도록 합니다. 이 모드는 하드웨어를 보호하고, 기기를 엔터프라이즈 네트워크에 연결하며, 더미 사용자 ID를 사용하여 기기를 Entra ID(Entra ID), MDM 서비스, MDM용 Ivanti Neurons 관리자 포털에 등록하고, 사용자가 로그인하기 전에 모든 필수 구성 파일을 기기에 푸시합니다. 필수 구성 파일이 기기에 푸시된 후 기기는 재시작되어 엔터프라이즈 사용자가 시작할 수 있는 로그인 화면을 표시합니다. 자체 배포 모드는 키오스크 또는 디지털 서명된 기기로 사용할 수 있는 기기에 사용할 수 있습니다.

**사용자 기반 사전 프로비저닝 프로필 모드** – 관리자가 사용자 기반 사전 프로비저닝 프로필을 생성하면 관리자가 프로필을 사용자 그룹에 할당하고 기기 하드웨어 ID가 업로드되어 Entra ID 그룹에 할당됩니다. 기기는 사용자 주도의 사전 프로비저닝된 프로필에 연결됩니다. 이 모드는 장치가 엔터프라이즈 사용자에게 전달되기 전에 관리자가 장치를 설정하는 데 사용됩니다.

### 절차

사전 프로비저닝된 배포를 위한 단계를 따르십시오.

1. 새 하드웨어 기기를 LAN에 연결하고 Windows 버튼을 5회 누릅니다.
2. 기기에 질문 프롬프트가 표시됩니다. Windows Autopilot 프로비저닝 옵션을 선택하고 계속을 클릭합니다. Entra ID가 사용자 기반 사전 프로비저닝 프로필 모드를 감지하고 모든 기본 구성 설정이 기기에 배포됩니다. Windows Autopilot 구성 화면이 표시됩니다.
3. 계속을 클릭합니다. 기기는 다음 단계로 가서 하드웨어를 보호하고, 기기를 엔터프라이즈 네트워크에 연결하며, 더미 사용자 ID를 사용하여 기기를 Entra ID(Entra ID), MDM 서비스, MDM용 Ivanti Neurons 관리자 포털에 등록하고, 모든 필수 구성 파일을 기기에 푸시하며 확인 메시지가 나타납니다.
4. 이제 기기를 사용자에게 인도할 수 있습니다. 사용자가 기기에 로그인하면 사용자 ID가 기기 세부 정보와 함께 MDM용 Ivanti Neurons 관리자 포털에 등록됩니다.

사용자가 기기에 로그인하기 전에 다음 구성이 자동으로 푸시됩니다.

ID 인증서

Wi-Fi

Windows Hello For Business

Windows 제한

보류 중 상태의 나머지 구성은 사용자가 이메일 주소를 사용하여 기기에 로그인한 후 푸시됩니다.

셀프 배포 및 사용자 주도(사전 프로비저닝) 모드의 Autopilot 등록 프로세스에서 할당된 .MSI 및 .EXE 앱이 기기에 설치되면 등록 프로세스가 완료됩니다. Autopilot 등록 프로세스에서 .MSI 및 .EXE 앱을 설치할 경우, 앱이 설치 중 보고하거나 보고에 실패하면 Autopilot 프로세스가 완료되고 다시 봉인 버튼이 활성화됩니다.

## Windows Autopilot 사용자 프로필 생성

Entra ID(Entra ID) 사용자 소스를 구성하고 사용자와 Entra ID 사용자 그룹을 MDM용 Ivanti Neurons 테넌트와 동기화한 후, Autopilot 프로필을 생성할 수 있습니다.

**절차**

1. MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **관리 > Microsoft Azure > Windows 장치 관리**로 이동합니다.

Entra ID 사용자 소스가 구성되지 않은 경우에는 **추가** 버튼이 비활성화됩니다. **Microsoft Azure** 섹션의 **Windows 장치 관리** 옵션을 사용하여 사용자 소스를 구성해야 합니다.

3. **추가**를 클릭합니다.
   **Windows Autopilot 프로필 추가** 페이지가 화면에 나타납니다.
4. **이름** 상자에 프로필 이름을 입력합니다.
5. 이 절차 하단에 있는 표를 사용하여 **프로필 설정**을 완료합니다.
6. **다음**을 클릭하세요.
   화면에 모든 Entra ID 기기 그룹이 표시된 새 페이지가 나타납니다.
7. Autopilot 프로필을 할당할 Entra ID 기기 그룹을 하나 이상 선택합니다.
8. Entra ID 기기 그룹을 만들고 이 새로 생성된 그룹에 Autopilot 프로필을 할당할 수도 있습니다. 자세한 내용은 을 참조하십시오.
   Autopilot 프로필을 모든 Entra ID 그룹에 할당하려는 경우 **모든 Entra ID 그룹에 할당** 옵션을 선택하십시오.

Microsoft 측의 제한으로 인해 하나 이상의 프로필을 “모든 그룹”에 할당할 수는 없습니다.

9. **완료**를 클릭하세요.

| 설정 | 설명 |
| --- | --- |
| **기기 유형** | 기기에 따라 다음 두 가지 옵션 중 하나를 선택합니다.<br>• **Windows PC**<br>• **HoloLens** - 이 옵션을 선택하면 기본 배포 모드가 **자체 배포** 모드로 설정됩니다.<br>Autopilot을 사용하여 HoloLens 2 기기를 등록할 때 '기기 작동 설정' 화면에서 등록 절차가 진행되지 않는 경우가 드물게 있습니다. 그런 경우에는 전원 버튼을 눌러 기기를 껐다가 다시 켜야 합니다. 그러면 기기에 로그인 화면이 나타나며, 여기에 Entra ID 자격 증명을 입력하면 등록이 완료됩니다. |
| **배포 모드**<br><br>**사용자 계정 유형**<br><br>**언어**<br><br>**모든 대상 기기를 Autopilot으로 변환** | • **자체 배포**: 이 모드에서는 수동 개입을 거의 또는 전혀 하지 않아도 기기 배포가 이루어집니다.<br>• **사용자 주도**: 관리자는 기기를 사용자에게 인도하기 전에 이 옵션을 사용하여 새 기기를 구성하기 위한 등록 모드를 선택할 수 있습니다.<br><br>• **관리자**: 기기가 배포된 후 사용자의 완전한 제어가 필요한 경우 이 옵션을 선택합니다.<br>• **표준**: 기기가 배포된 후 사용자가 기본 옵션에 대한 권한을 필요로 하는 경우 이 옵션을 선택합니다.<br><br>기본적으로 언어는 운영 체제에 따라 다릅니다. 목록에서 다른 언어로 변경할 수 있습니다.<br><br>할당된 그룹의 모든 기기를 Autopilot으로 변환하려면 이 옵션을 선택합니다. |
| **사전 프로비저닝 허용** | 정상 등록 프로세스를 통해 Autopilot에 기기를 등록하려면 이 옵션을 선택합니다. **자체 배포** 옵션을 선택하면 이 옵션을 사용할 수 없습니다. |
| **키보드 자동 구성**<br><br>**기기 이름 템플릿**<br><br>**Microsoft 소프트웨어 라이선스 조건** | **언어** 옵션을 기본값과 다른 값으로 설정한 경우 키보드 선택을 건너뛰려면 **예**를 선택합니다.<br><br>기기 등록 과정에서 사용할 템플릿 이름을 입력합니다.<br><br>사용자 주도 배포 모드에서만 이 옵션을 보이거나 숨길 수 있습니다. |
| **개인정보 보호 설정**<br><br>**계정 옵션 변경** | 사용자 주도 배포 모드에서만 이 옵션을 보이거나 숨길 수 있습니다.<br><br>사용자 주도 배포 모드에서 그리고 사용자 계정 유형이 표준 유형인 경우에만 이 옵션을 보이거나 숨길 수 있습니다. |

**Windows 장치 관리**

관리자는 신규 옵션인 Windows 기기 관리를 사용하여 테넌트에서 Autopilot 기능을 구성할 수 있습니다. 사용자에게 Entra ID 환경이 있을 경우 이 옵션을 활용하면 MDM용 Ivanti Neurons와의 통합을 보다 쉽게 진행할 수 있습니다.

이 옵션에 액세스하려면 **관리자** > **Microsoft Azure** > **Windows 장치 관리**로 이동합니다.

이 통합을 통해 MDM용 Ivanti Neurons는 기기 관리, Autopilot 프로필, Windows 기기 규정 준수 확인, Azure 테넌트 확인을 위한 권한을 얻게 됩니다.

**관련 주제**

- TenantLockdown CSP

## Entra ID 기기 그룹 생성

관리자는 필요시 Entra ID 기기 그룹 섹션에서 Entra ID 기기 그룹을 생성할 수 있습니다. Entra ID 기기 그룹을 생성하기 위해서는 기기 규정 준수 섹션에서 Entra ID 테넌트 확인이 구성되었어야 합니다.

**절차**

1. **관리** > **Microsoft Azure** > **Entra ID 기기 그룹**으로 이동합니다.
2. 화면에 **Entra ID 기기 그룹** 페이지가 표시됩니다.
   **ADD**를 클릭합니다.
3. 화면에 **그룹 설정** 페이지가 표시됩니다.
   다음 세부 정보를 입력합니다.
   - 그룹 이름
   - 그룹 설명
   - 멤버십 유형
     - 정적 기기 - 관리자는 **그룹에 구성원 할당** 창에서 사용 가능한 정적 기기의 목록을 확인할 수 있습니다. 필요한 기기를 선택하고 **저장**을 클릭합니다.
     - 동적 기기 - 관리자는 **동적 쿼리** 창에서 특정 조건을 입력해야 합니다.

새 Entra ID 기기 그룹이 생성되며 관리자는 새로 생성된 그룹에 기기를 추가할 수 있습니다.

> 동적 그룹이 생성되면 일정 시간이 지난 후 특정 기기 그룹의 기기 탭에 추가된 기기가 표시됩니다.

## Autopilot 기기 편집

사용자는 MDM용 Ivanti Neurons 관리 포털에서 Autopilot 기기를 편집할 수 있습니다.

**필수 조건**

다음 전제 조건이 충족되는지 확인하십시오.

- IT 관리자 사용자에게는 Azure 글로벌 관리자 및 Intune 관리자 권한이 있어야 합니다.
- 사용자에게 친숙한 이름은 사용자가 설정된 경우에만 설정할 수 있습니다.
- 장치 이름은 한 번 설정하면 해제할 수 없습니다.

**절차**

1. MDM용 Ivanti Neurons 관리 포털에 로그인합니다.
2. **관리** > **Windows** > **Autopilot**으로 이동합니다. Autopilot 기기는 Autopilot 기기 탭 아래에 열거됩니다.
3. **편집**(연필 아이콘)을 클릭합니다. 편집 페이지가 나타납니다.
4. 다음 상세 정보를 편집합니다.
   - **사용자**
   - **사용자에게 친숙한 이름**
   - **기기 이름**
   - **그룹 태그**

**저장**을 클릭합니다. 기기 상세 정보가 업데이트됩니다.

## Autopilot 기기 삭제

사용자는 MDM용 Ivanti Neurons 관리 포털에서 Autopilot 기기를 삭제할 수 있습니다.

1. MDM용 Ivanti Neurons 관리 포털에 로그인합니다.
2. **관리** > **Windows** > **Autopilot**으로 이동합니다. Autopilot 기기는 Autopilot 기기 탭 아래에 열거됩니다.
3. **삭제**를 클릭하세요. 기기 상세 정보가 삭제됩니다.

# 12.4.2. Windows Autopilot 프로필의 감사 추적

감사 내역은 MDM용 Ivanti Neurons 내의 모든 엔터티에서 수행된 활동을 모두 추적합니다. 이러한 활동에는 새 기기 추가, 삭제, 업데이트 등이 포함됩니다.

자세한 내용은 감사 추적을 참조하십시오.

관리자는 Autopilot 모드에 등록된 모든 Windows 기기에서 감사 추적을 사용하여 다음 활동을 수행할 수 있습니다.

**Autopilot 프로필**

- 만들기
- 편집
- 삭제
- 그룹에 프로필 할당

**Autopilot 기기**

- CSV 업로드
- 편집
- 삭제

# 12.4.3. TenantLockdown CSP

관리자는 TenantLockdown CSP 기능을 사용하여 테넌트에 대해 모든 Windows 기기를 잠글 수 있습니다. 이 기능을 사용하려면 Autopilot 옵션을 사용하여 기기를 등록해야 합니다. 이 구성은 기기 수준에서 수행할 수 있습니다.

Autopilot 자체 배포 및 사용자 주도 모드에서 관리자는 테넌트에 대해 직접 기기를 잠글 수 있습니다. 이것은 기기를 분실 또는 도난당했을 때 유용한 방법입니다. 그런 경우에는 기기를 리셋하더라도 사용자는 테넌트에 강제로 연결되며, 자체 배포 모드에서는 로컬 계정 생성이 지원되지 않습니다. 그러나 사용자 주도 모드에서 계정 생성을 금지해야 하는 경우, 관리자는 Autopilot 프로필 구성 중에 **계정 옵션 변경** 설정에서 **숨기기** 옵션을 활성화해야 합니다.

관리자는 Windows 제한 구성을 생성하고 **기타 제한** 아래에서 **사용자는 기기 설정 중에 네트워크에 연결해야 합니다(Autopilot 프로필 필요)** 옵션을 선택하여 TenantLockdown CSP를 활성화할 수 있습니다.

TenantLockdown CSP에서 기기를 제거하려면 관리자는 기기를 그룹에서 수동으로 제거하거나 제한 사항을 변경해야 합니다.

# 12.4.4. ADMX(GPO) 브라우저

ADMX(GPO) 브라우저를 사용하여 테넌트에 존재하는 ADMX 객체를 기반으로 구성된 GPO 설정을 볼 수 있습니다. 기본 ADMX 객체를 검색하고 볼 수 있으며 GPO 설정 표시를 정의하기 위해 XML 기반 구조를 제공하는 사용자 지정 ADMX 파일을 추가(업로드)할 수도 있습니다.

사용자 지정 ADMX 객체를 업로드하려면

1. **관리자 > ADMX(GPO) 브라우저**를 선택합니다. **ADMX(GPO) 브라우저** 페이지가 표시됩니다.
2. **추가**를 클릭합니다. **사용자 지정 ADMX(GPO) 객체 추가** 창이 표시됩니다.
3. **파일 선택**을 클릭하여 업로드할 ADMX 파일을 선택합니다.

> ADMX 파일이 zip 파일인지 확인하세요.

4. **추가**를 클릭합니다. 업로드 성공 확인 메시지가 표시됩니다.

> zip 파일의 압축을 푼 후 루트 폴더에 *.admx* 확장자 파일이 포함되어 있는지 확인하세요.

## GPO 설정 검색

ADMX(GPO) 브라우저의 왼쪽 창에 있는 GPO 계층 구조 트리에서 관련 구성 요소를 클릭하면 GPO를 검색하고 선택할 수 있습니다. GPO 계층 트리는 정책 설정 경로를 나타냅니다. 검색 필드에 GPO 이름이나 ADMX 파일 이름을 입력하여 특정 GPO 설정을 검색할 수도 있습니다. 선택한 GPO 설정의 상세 정보가 오른쪽 창에 표시됩니다.

# 12.4.5. 앱 인벤토리 간격 설정

여러 앱 소스 유형 인벤토리에 대해 Windows 10 애플리케이션 인벤토리 수집 간격을 설정할 수 있습니다. 간격은 개인정보 보호 설정이 기기에서 모든 앱을 수집하도록 설정된 경우에 사용됩니다.

1. **관리 > 앱 인벤토리 간격**으로 이동합니다.
2. 드롭다운 목록에서 다음 앱 소스 유형에 대한 앱 인벤토리를 수집하는 간격(시간 단위)을 선택합니다.
   - **비 App Store 인벤토리 간격**
   - **App Store 인벤토리 간격**
   - **시스템 인벤토리 간격**
   - **Win32 인벤토리 간격**
     Windows 앱 인벤토리를 수집하는 간격 옵션은 **24**~**48**시간입니다. 기본값은 **24**시간입니다.

# 12.4.6. 하드웨어 인벤토리

Windows 10 기기에서 하드웨어 정보 수집을 활성화할 수 있습니다. 하드웨어 인벤토리 상세 정보는 Bridge를 사용하여 검색됩니다.

1. **관리 > 하드웨어 인벤토리**로 이동합니다.
2. **하드웨어 인벤토리 수집 활성화** 옵션을 활성화합니다.
3. **인벤토리 간격**에서 하드웨어 인벤토리 수집 빈도를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
    - **하루에 한 번**(기본)
    - **1주일에 한 번**
    - **30일에 한 번**

하드웨어 인벤토리 옵션이 활성화되면 기기 상세 정보 페이지에 있는 **하드웨어** 탭에서 기기의 하드웨어 상세 정보를 확인할 수 있습니다.

# 12.5. Microsoft Azure 설정

이 섹션에는 다음 주제가 포함됩니다.

- Microsoft Azure 사용하기
- Entra ID Windows 10 통합 엔드포인트 관리 설정
- Entra ID UEM 앱 할당
- Entra ID 사용자 소스로 MDM용 Ivanti Neurons 연결
- Azure 테넌트
- 관리 > Microsoft Azure > Office 365 앱 보호

# 12.5.1. Microsoft Azure 사용하기

MDM용 Ivanti Neurons 은(는) Microsoft Azure로 설정할 수 있어 Windows 데스크톱 및 Windows 10에서 실행되는 태블릿 기기의 사용자가 원활하게 등록할 수 있습니다. 아래의 단계를 따라 인스턴스를 구성하고 연결하십시오.

이 섹션에는 다음 주제가 포함됩니다.

## Entra ID 계정 설정

Entra ID 설정:

1. https://azure.microsoft.com/en-in/pricing/purchase-options/로 이동하여 Azure 계정을 구입합니다.
2. 기존의 Hotmail 또는 Outlook.com 계정을 이용하거나 새로운 계정을 생성하여 새로운 사용자로 등록합니다.
3. 다음 중 한 가지 지불 옵션을 사용하고 검증 단계를 따라서 Azure 계정을 구입합니다.
4. Microsoft에 MDM용 Ivanti Neurons 테넌트를 허용 목록에 추가할 것을 요청합니다.
5. 2단계에서 사용한 것과 동일한 Hotmail 또는 Outlook.com 계정을 사용하여 https://manage.windowsazure.com/https://manage.windowsazure.com/에서 관리자로 Entra ID에 로그인합니다.
6. **도메인** 탭으로 이동합니다.
   기본적으로 계정에 대한 도메인 TestMiBGLRoutlook.onmicrosoft.com이 생성되며 생성된 모든 사용자는 이 도메인에 속하게 됩니다. 필요한 경우 사용자 정의 도메인을 재생성할 수 있습니다.

## Entra ID에서 사용자 생성

Entra ID에서 사용자 생성하기:

1. 활성 디렉터리 > **기본 디렉터리 > 사용자**로 이동합니다.
2. 사용자 추가 옵션 > 소속 조직의 새로운 사용자 선택을 선택합니다.
3. 사용자 이름을 입력합니다. 다음**(->)**을 클릭합니다.
   **사용자 프로필** 페이지가 표시됩니다.
4. 성을 포함한 이름과 표시 이름 등 사용자 정보를 추가합니다.
5. 드롭다운 메뉴를 사용하여 사용자에게 적절한 역할을 할당합니다.
6. 임시 비밀번호를 생성합니다.
   사용자는 처음 로그인 시 이 비밀번호를 변경해야 합니다.

## Windows 10 기기용 UEM에 Entra ID 연결

Entra ID를 UEM에 연결하기:

1. **관리 > Microsoft Azure > Entra ID를 사용하여 Windows 등록 및 규정 준수로 이동합니다.**
2. Entra ID Windows 10 통합 엔드포인트 관리 설정 섹션에서 설명한 UEM 설정 단계를 완료합니다.
3. Azure 포털에서 Entra ID UEM 앱 할당 설정을 완료합니다.
4. MDM용 Ivanti Neurons 관리 포털에 Entra ID 계정의 도메인 이름을 입력하고 Azure 포털에 연결을 클릭한 후 확인란을 선택합니다.
5. 로그인에 성공했으면 MobileIron AD 테넌트 확인 앱을 허용하는 동의를 수락하여 MDM용 Ivanti Neurons UEM 앱이 설정되었음을 확인합니다. 연결에 성공했음을 알리는 메시지가 나타납니다.

### Windows 10 기기용 Microsoft Passport for Work

Microsoft Passport for Work가 Windows Hello for Business로 교체됩니다. 자세한 내용은 **Windows Hello for Business 구성**을 참조하십시오.

### Windows 기기 Entra ID 등록

**필수 조건**

사용자는 반드시 MDM용 Ivanti Neurons에 등록되어야 합니다.

Windows 10 이상 장치에 사용자를 등록하려면 도메인을 연결하세요.

1. **Entra ID 가입**을 클릭합니다.
2. 사용자 이름과 비밀번호를 입력합니다.
3. **로그인**을 클릭합니다.
4. EULA를 허용합니다
5. **PIN 생성**을 클릭합니다.
   - Microsoft Passport for Work PIN 복잡도를 사용하도록 설정했다면 설정된 정책에 따라 복잡한 PIN을 설정하라는 메시지가 표시됩니다.
   - Entra ID는 사용자를 인증하고 JWT(JSON 웹 토큰)를 기기로 다운로드합니다.
   - 이제 기기가 등록됩니다.
   - 사용자는 검증을 위해 기기를 통해 접촉합니다.
6. PIN을 입력하고 확인합니다.
7. **확인**을 클릭하세요.

## Windows 기기의 다중 사용자 지원

MDM용 Ivanti Neurons 은(는) Windows 10 Entra ID 등록 기기에서 다중 사용자 기능을 지원합니다. 이 기능에는 VPN, Wi-Fi, 기본 이메일 클라이언트 프로필 및 인증서와 같은 일부 프로필을 기기가 아닌 개별 사용자에게 푸시하는 것이 포함됩니다. 이 기능은 또한 로그인한 사용자에 대해 인하우스 및 공개 앱의 배포를 지원합니다. 신규 Entra ID 사용자가 기기에 로그인할 때마다 MDM용 Ivanti Neurons에서 기기와 사용자를 함께 평가합니다. 신규 사용자일 경우 MDM용 Ivanti Neurons은(는) 해당 사용자의 기기를 업데이트합니다. 사용자가 기기의 기존 사용자일 경우에는 마지막 로그인 후 업데이트해야 하는 기기 및 사용자 설정에 변화가 있을 경우 평가됩니다.

기기에 로그인한 Entra ID 사용자의 세부 정보는 MDM용 Ivanti Neurons 관리 포털에 보고됩니다. 사용자가 기기에서 로그아웃하고 두 번째 사용자가 기기에 로그인하면 두 번째 사용자의 상세 정보가 기기 상세 정보 페이지에 업데이트됩니다.

## UEM이 있는 비즈니스용 Microsoft Store 설정

비즈니스용 Microsoft Store는 Azure의 일환으로 Microsoft에서 제공하는 포털입니다. 관리자는 이 포털에 로그인하여 앱을 구매하고 이를 관리되는 모든 기기로 배포할 수 있습니다. MDM용 Ivanti Neurons 은(는) 비즈니스용 Microsoft Store로 설정하여 다음 단계의 설정을 통해 MDM용 Ivanti Neurons 관리 포털 내에서 애플리케이션을 관리할 수 있습니다.

### 1단계: Microsoft Azure 포털에서 Entra ID 애플리케이션 등록

1. 첫 번째 브라우저를 열고 Microsoft Azure 포털(**https://portal.azure.com/https://portal.azure.com/**)에 로그인합니다.
2. 왼쪽 창에 있는 **앱 등록**을 클릭합니다.
3. **+새 애플리케이션 등록**을 클릭합니다.

4. 다음 정보를 입력하여 MobileIron을 Azure 앱으로 등록합니다.
    - **이름**: MobileIron 앱의 이름을 입력합니다. (이 필드는 최소 4개 문자를 입력해야 합니다.)
    - **애플리케이션 유형:** 웹 앱/API를 선택합니다.
    - **로그인 URL:** MobileIron에 로그인할 URL 기기 사용자 액세스를 입력합니다(필수).
5. **생성**을 클릭하여 앱을 추가하고 Azure 홈페이지로 돌아갑니다.
6. 설정으로 이동하여 새 키를 생성합니다.

## 2단계: 애플리케이션을 관리 도구로 추가

1. 비즈니스용 Microsoft Store 설정에서 관리를 클릭합니다.
2. 배포 설정
3. 관리 도구 추가에서 생성된 애플리케이션을 활성화합니다.

## 관리자 포털에서 계정 연결

1. **관리 > Microsoft Azure > 비즈니스용 Microsoft Store**로 이동합니다.
2. 1단계의 **Entra ID 애플리케이션 등록**에서 **예, 이 단계를 완료했습니다** 확인란을 선택합니다.
3. 2단계, **관리 도구 추가**에서 체크박스 **예, 이 단계를 완료했습니다**를 선택합니다.
4. 3단계, 계정 연결에서 다음 필드를 업데이트합니다.
    - Entra ID 도메인
    - 애플리케이션 식별자
    - 애플리케이션 키
    - 동기화 간격(시간)
5. **연결**을 클릭합니다. 비즈니스용 MobileIron 스토어가 성공적으로 설치되었다는 확인 메시지를 보게 됩니다.
6. **앱 동기화**를 클릭합니다. 동기화에 성공하면 상태가 **애플리케이션 동기화 성공**으로 표시됩니다.

앱용 Microsoft Store가 기기로 푸시되면 기기 상세 정보의 **설치된 앱** 탭에서 앱 상세 정보를 사용할 수 있습니다. 기기에서 보고된 각각의 비즈니스용 Microsoft Store는 **소스** 열에서 **비즈니스용 Microsoft Store**로 식별할 수 있습니다.

# 12.5.2. Entra ID Windows 10 통합 엔드포인트 관리 설정

Windows 10 통합 엔드포인트 관리(UEM) 설정 방법:

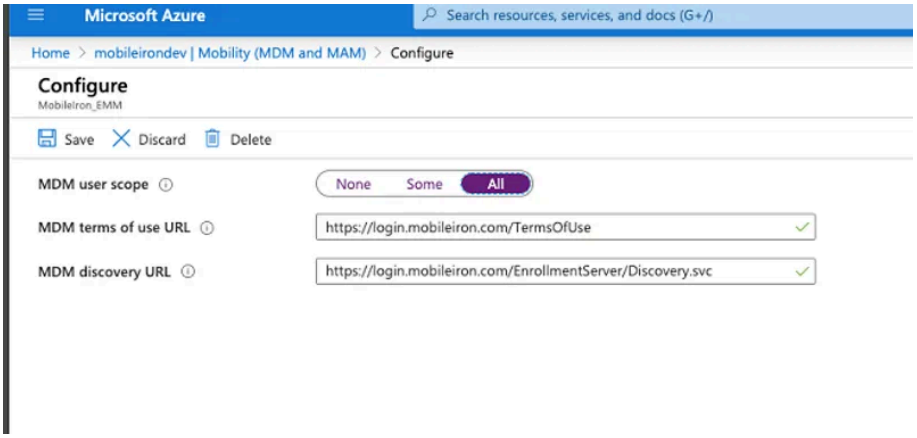
1. https://portal.azure.com/에서 관리 사용자로 로그인하고 Entra ID를 선택합니다.
2. 좌측 패널에서 "모빌리티(MDM 및 MAM)"를 선택한 다음, **+ 애플리케이션 추가**를 클릭합니다.

3. 앱 갤러리에서 MobileIron_UEM 애플리케이션을 선택하고 **추가**를 클릭합니다.


# 12.5.3. Entra ID UEM 앱 할당

사용자 할당 설정을 완료하려면:

1. **Entra ID Windows 10 통합 엔드포인트 관리 설정**의 2단계에서 만든 MobileIron UEM 앱을 클릭합니다.
2. MDM 사용자 범위에서 사용자 지정 사용자 그룹에 할당하거나 **모두** 선택합니다.



# 12.5.4. Entra ID 사용자 소스로 MDM용 Ivanti Neurons 연결

Entra ID(Entra ID)로 작업하려면 Microsoft Entra ID 계정의 상세 정보로 MDM용 Ivanti Neurons을(를) 구성해야 합니다. 구성 완료된 기존 Microsoft Entra ID 계정이 필요합니다. 이 솔루션은 온프레미스 커넥터나 LDAP를 필요로 하지 않습니다.

이 섹션에는 다음 주제가 포함됩니다.


- 사용 사례
- Entra ID 사용
- Entra ID 설정


## 사용 사례

다음 사용 사례 중 하나에 대해 MDM용 Ivanti Neurons와(과) Entra ID를 연결할 수 있습니다.

- Microsoft Office 365 작업
- 사용자 인증을 위해 Microsoft Entra ID, Microsoft ADFS, 또는 기타 SAML 2.0 ID 제공자(IDP) 설정
- 사용자 소스로 Microsoft Entra ID 설정
- Microsoft Entra ID에서 사용자를 동기화하고 시작합니다. Entra ID 도메인의 모든 사용자 및 그룹과 MDM용 Ivanti Neurons 인스턴스 동기화
  다음과 같은 이유로 Entra ID 동기화에 오류가 발생한 경우에는 **알림** 페이지에 알림이 표시됩니다.
  - Entra ID 서비스에 연결할 수 없음
  - 모든 사용자 속성이 Entra ID와 동기화되지 않음
  - 일부 사용자 속성이 Entra ID와 동기화되지 않음
- 여러 개의 IdP가 있는 환경은 현재 지원되지 않습니다.
- Microsoft Entra ID를 사용자 소스로 사용하지 않는 경우에는 로컬 계정 또는 LDAP의 소스 사용자를 사용할 수 있습니다. 이를 위해서는 MDM용 Ivanti Neurons 커넥터가 온프레미스에서 LDAP 리소스에 액세스할 수 있도록 설정해야 합니다.
- Microsoft Entra ID를 사용자 인증에만 사용하고 온프레미스 LDAP를 사용자 디렉터리로 사용하는 기능은 현재 지원되지 않습니다.

## Entra ID 사용

Entra ID를 사용하려면 다음 방법 중 하나를 활용하여 사용자 인증을 위한 ID 제공자를 설정합니다.

- 사용자 소스와 사용자 인증 모두에 Microsoft Entra ID를 사용하려면 Entra ID를 IDP로 설정하십시오. **관리자 > ID > MDM용 Ivanti Neurons IDP 설정**으로 이동하여 메뉴에서 **Entra ID**를 선택합니다.
- 사용자 소스에 Microsoft Entra ID를 사용하고 사용자 인증에 ADFS를 사용하려면 ADFS를 IDP로 설정하십시오. **관리 > ID > 온-프레미스 IdP 설정**으로 이동하여 메뉴에서 ADFS를 선택합니다.
- Entra ID 이외의 SAML 2.0 IdP를 사용하고 사용자 인증에 ADFS를 사용하려면 **관리자 > ID > 일반 IDP 설정**으로 이동하여 해당 페이지에 표시된 지침을 따릅니다.

자세한 내용은 ID 제공자 구성을 참조하십시오.

## Entra ID 설정

본 항목은 Entra ID 설정을 구성하는 데 도움이 됩니다.

**절차**

1. **관리자 > Microsoft Azure > Entra ID 사용자 소스**로 이동합니다.
2. 다음 세부 정보를 지정합니다.
    1. **Entra ID 이름**.
    2. **동기화 간격** - MDM용 Ivanti Neurons이(가) Entra ID의 사용자 데이터를 동기화하는 빈도를 수정합니다.
    3. **이 Entra ID 활성화** - 이 옵션을 사용하여 Entra ID 인스턴스를 활성화하거나 비활성화합니다.
    4. **Entra ID에서 불러온 사용자를 자동으로 초대** 선택 - Entra ID에서 MDM용 Ivanti Neurons(으)로 불러온 사용자에게 자동으로 등록 초대 이메일을 보낼지 여부를 관리합니다.
    5. **관리형 Apple ID** 선택 - Entra ID 사용자에 대한 관리 Apple ID 동기화를 선택합니다.
        - **없음**
        - **패턴** -
            - **사용자 이메일 주소**
            - **userUPN**
            - (선택 사항) "appleid" 하위 도메인 포함 옵션을 선택하여 기존 Apple ID와의 충돌을 방지합니다.
    6. (선택 사항) **사용자 지정 속성 추가** 클릭 - 장치 관리에 적용할 디렉터리 서비스의 사용자 지정 속성을 지정합니다. 이후 각 속성은 변수를 지원하는 구성 필드에서 ${속성이름}으로 지칭될 수 있습니다. 이 옵션을 사용하려면 Entra ID 서버 전체에 사용자 지정 속성을 일관적으로 구현해야 합니다. 구현에 포함된 Entra ID 서버가 이 속성을 사용하지 않을 경우 이 속성에 종속된 기능이 예상한 바와 같이 작동하지 않을 수 있습니다.

Entra ID 설정을 수정한 후 **저장**을 클릭합니다.

# 12.5.5. Azure 테넌트

이 섹션에는 다음 주제가 포함됩니다.


- 요건
- 기기 사용자에 Intune 라이센스 적용
- 규정 준수 파트너로 MobileIron 추가하기
- Microsoft Endpoint Manager에서 조건부 액세스 정책 만들기
- Microsoft Azure와 MDM용 Ivanti Neurons 연결 중
- 파트너 기기 컴플라이언스 정책 만들기
- MDM용 Ivanti Neurons에서 Azure로 기기 상태 보고
- Azure 테넌트의 프로비저닝 해제

# 12.5.5.1. Azure Tenant Requirements

이 섹션에서는 Microsoft Azure 테넌트와 함께 MDM용 Ivanti Neurons를 설정하는 것에 대해 설명합니다.

## 요건

### Microsoft

MDM용 Ivanti Neurons 고객은 Microsoft Intune에 대한 유효한 구독이 있어야 하며 Microsoft Intune 라이선스를 기기 사용자에게 할당해야 합니다.

### MobileIron

- MDM용 Ivanti Neurons - MDM용 Ivanti Neurons 버전 75부터 최신 버전까지 MobileIron에서 지원됩니다.
- 추가 라이센스 - Azure 기기 컴플라이언스는 Premium 혜택이며 **Secure UEM Premium** 및 Platinum 고객이 이용할 수 있습니다. 기존 고객의 경우 Platinum 라이센스로도 충분합니다.
- MobileIron에서 지원하는 iOS용 Go(클라이언트) 또는 Android용 Go(클라이언트) 버전 75.0 이상 최신 버전.

### 여러 MDM용 Ivanti Neurons 지원

동일한 Azure 테넌트에 연결된 다중 MDM용 Ivanti Neurons가 있을 경우, 기기 데이터를 Azure로 업로드하지 않도록 모든 MDM용 Ivanti Neurons에서 연결을 해제하거나 특정(단일) MDM용 Ivanti Neurons에서 Entra ID 규정 준수 통합에 대한 규정 준수 정책을 비활성화합니다.

> MDM용 Ivanti Neurons를 연결 해제하기 전에 반드시 규정 준수 정책을 비활성화하십시오.

## MDM용 Ivanti Neurons 관리자 프로세스

MDM용 Ivanti Neurons 관리자 관점에서의 프로세스:

1. 관리자가 Intune 라이센스를 기기 사용자에게 적용합니다. **기기 사용자에 Intune 라이센스 적용**을 참조하십시오.
2. 관리자가 Azure 포털로 로그인합니다.
3. 관리자가 Azure 규정 준수 파트너로 MobileIron을 추가합니다. **규정 준수 파트너로 MobileIron 추가하기**를 참조하십시오.
4. 관리자가 앱에 대해 조건부 액세스 정책을 만듭니다. **Microsoft Endpoint Manager에서 조건부 액세스 정책 만들기**를 참조하십시오.
5. 관리자가 MobileIron과 Azure 간에 연결을 설정합니다. **Microsoft Azure와 MDM용 Ivanti Neurons 연결 중**를 참조하십시오.
6. 관리자가 MDM용 Ivanti Neurons에서 기기 규정 준수 정책을 만듭니다. **파트너 기기 컴플라이언스 정책 만들기**를 참조하십시오.
7. 조건부 액세스 정책이 발효됩니다. 기기가 규정을 준수하는지 여부에 따라 앱에 대한 액세스 권한이 승인되거나 거부됩니다.

> 관리자가 각 Microsoft 앱에서 테스트를 실행하는 것이 좋습니다.

# 12.5.5.2. 기기 사용자에 Intune 라이센스 적용

- 다음의 경우에는 이 기능을 사용하지 마십시오.
  - 사용자가 바뀔 것 같은 상황에서 사용자를 변경하거나 상황을 관리하는 경우
  - 기기를 여러 명의 사용자가 소유하는 경우
- 사용자에게 할당을 수행하지 않고, 또한 기기 컴플라이언스 구성을 다음과 같은 다중 사용자 기기로 배포하지 않는 것이 좋습니다.
  - Secure Sign-In WebClip이 있는 기기
  - 공유 iPad 기기
  - Android 키오스크 모드 기기

## MDM용 Ivanti Neurons 라이선스 요건

기기 컴플라이언스는 Premium 혜택이며 Secure UEM Premium 및 Platinum 고객이 이용할 수 있습니다. 기존 고객의 경우 Platinum 라이센스로도 충분합니다.

## 기기 사용자에게 대량 라이센스 할당

기존 기기 사용자에게 라이센스를 대량 할당하는 방법:

### 그룹 기반 할당

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

### PowerShell 기반 할당

https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide

# 12.5.5.3. 규정 준수 파트너로 MobileIron 추가하기

**필수 조건**

- Microsoft Intune 라이센스 설치. 기기 사용자에 Intune 라이센스 적용을 참조하십시오.
- Microsoft Azure에서 사용자 만들기
- Microsoft Azure에서 그룹 만들기

**절차**

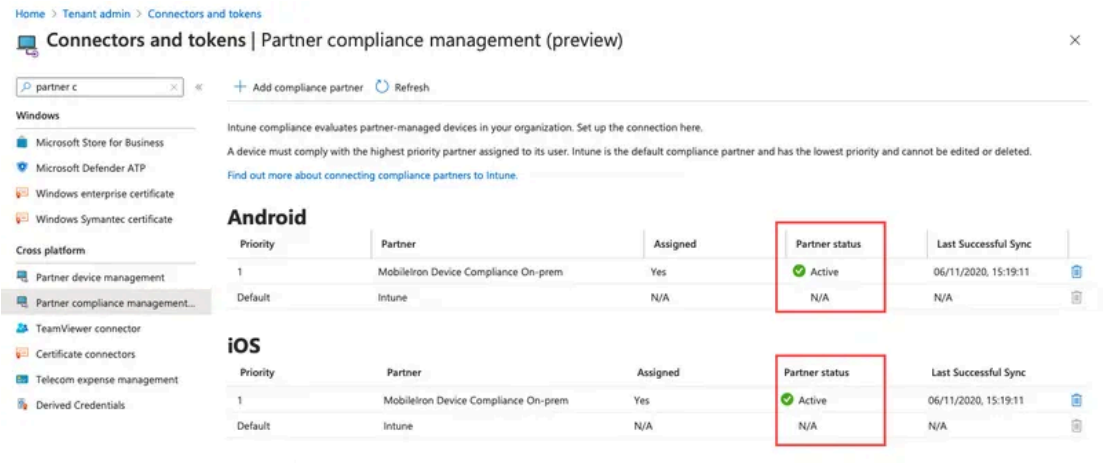
1. 로그인: https://endpoint.microsoft.com.
2. Microsoft Endpoint Manager 관리 센터 페이지의 좌측 패널에서 테넌트 관리자를 클릭합니다. 커넥터 및 토큰 > 파트너 규정 준수 관리를 클릭하십시오.

3. 오른쪽의 검색 필드에서 + 규정 준수 파트너 추가를 클릭합니다.

4. 기본 탭에서 규정 준수 파트너 필드의 드롭다운에서 MobileIron 기기 컴플라이언스 클라우드를 선택합니다.

5. 플랫폼 필드에서 iOS 또는 Android를 선택한 다음, 다음을 클릭합니다.
6. 정책 탭을 클릭합니다. 드롭다운으로 할당에서 컴플라이언스 상태에 해당하는 사용자/기기 사용자 그룹을 선택하십시오. 라이센스가 있는 사용자/그룹을 선택하십시오.

7. 다음을 선택합니다.
8. 생성을 클릭합니다. 새 규정 준수 파트너가 파트너 규정 준수 관리 페이지에 나타납니다.



# 12.5.5.4. Microsoft Endpoint Manager에서 조건부 액세스 정책 만들기

**절차**

1. Microsoft Endpoint Manager https://endpoint.microsoft.com에 로그인합니다.
2. Microsoft Endpoint Manager 관리 센터 페이지에서 홈 > Endpoint Security > 조건부 액세스로 이동합니다.
3. 정책을 클릭한 다음, + 새 정책을 클릭합니다.

4. 조건부 액세스 정책의 이름을 입력합니다.

5. 할당에서, 클릭하여 정책을 사용자와 그룹에 할당합니다.

6. 클라우드 앱 또는 작업을 클릭한 다음 선택을 클릭합니다. 검색하여 보호받아야 할 앱을 선택하십시오.

7. 조건을 클릭한 다음, 기기 플랫폼을 클릭합니다. 적절한 기기 플랫폼을 선택하십시오.

8. 새 조건부 액세스 정책 페이지 > 액세스 제어에서, 승인을 클릭하고 액세스 및 차단 선택을 합니다.

9. 새 정책을 활성화하려면, 켜기를 클릭합니다.

10. 생성을 클릭합니다.

# 12.5.5.5. Microsoft Azure와 MDM용 Ivanti Neurons 연결 중

**절차**

1. MDM용 Ivanti Neurons에 로그인하고 **관리자** > **Microsoft Azure**로 이동합니다.
2. 왼쪽 탐색 창에서 **Microsoft Azure** > **장치 규정 준수**를 클릭합니다.
3. 계정 연결 섹션에서 다음 세부 정보를 입력합니다.
   - **Azure 테넌트 ID** - Microsoft Azure 인스턴스에서 찾으십시오.
   - **등록 URL(선택 사항)** - 장치가 MDM 등록되지 않은 경우 등록을 위해 장치 사용자가 이 URL로 안내됩니다. 구성할 때는 HTTPS 형식을 사용하십시오. 등록 정보를 위해 기기 사용자를 리디렉션할 조직에서 페이지를 호스팅할 경우 해당 링크를 여기에 추가하십시오.
   - **해결 URL(선택 사항)** - 장치가 규정을 준수하지 않을 경우 해결을 위해 사용자가 해결을 위해 이 URL로 안내됩니다. 구성할 때는 HTTPS 형식을 사용하십시오. 수정 정보를 위해 기기 사용자를 리디렉션할 조직에서 페이지를 호스팅할 경우 해당 링크를 여기에 추가하십시오.
4. **계정 연결**을 클릭합니다. Azure 테넌트 검사 대화 상자가 열립니다.

> 현재 Azure에 연결되어 있고 macOS 장치의 장치 규정 준수를 추가하려는 테넌트는 계정 연결을 끊은 다음 연결을 다시 설정해야 합니다.

5. Azure 테넌트 확인 대화 상자에서 대화 상자에서 1단계에 있는 **링크**를 클릭합니다.
6. **로그인합니다**.
7. 권한을 검토한 다음, **허용**을 클릭합니다.

> 로그인했는데 페이지에 다시 로그인하라는 메시지가 표시되면 브라우저 탭/창을 닫으십시오.

8. MDM용 Ivanti Neurons(으)로 돌아갑니다. Azure 계정 연결 대화 상자에서 **동의를 제공했습니다** 체크박스를 선택하십시오. **확인**을 클릭합니다.

- 계정을 편집하려면 **계정 편집**을 클릭합니다.
- 계정을 연결 해제하려면 **계정 연결 해제**를 클릭합니다. 추가 지침은 **Azure 테넌트의 프로비저닝 해제**를 참조하십시오.
- 계정을 추가, 편집, 비활성화하는 모든 활동이 로그에 기록됩니다.

# 12.5.5.6. 파트너 기기 컴플라이언스 정책 만들기

MDM용 Ivanti Neurons에서 파트너 장치 규정 준수 정책을 만들고 원하는 레이블을 적용합니다. 파트너 규정 준수 정책은 조건부 액세스를 위해 장치 규정 준수 상태를 Azure 또는 BeyondCorp에 보고합니다.

### 적용 대상

- iOS
- Android
- Windows

### 필수 조건

Azure 테넌트 ID 또는 Google BeyondCorp ID가 설정되어 있어야 합니다. Azure 파트너 장치 규정 준수에 대한 자세한 내용은 **Microsoft Azure와 MDM용 Ivanti Neurons 연결 중**를 참조하세요.



### 절차

1. MDM용 Ivanti Neurons에 로그인하고 **구성**으로 이동합니다.
2. **추가**를 클릭하고 **파트너 장치 규정 준수** 구성을 검색합니다.
3. **파트너 장치 규정 준수 구성 만들기** 페이지에 다음 세부 정보를 입력합니다.

| 항목 | 설명 |
|---|---|
| **Windows** | 이름을 입력합니다. |
| **+ 설명 추가** | 설명을 입력합니다. |
| **파트너 선택** | **Microsoft Azure 규정 준수**를 선택합니다. 또는 **Google BeyondCorp 규정 준수 - 베타**를 선택합니다. |
| **구성 설정**<br>iOS, macOS, Android 장치에 대한 규정 준수 상태 보고 | 기본적으로 켜져 있습니다. 이 필드가 표시되지 않으면 Azure 테넌트 ID를 설정해야 합니다.<br>iOS, macOS, Android 장치에 대한 규정 준수 상태 보고 옵션이 활성화되어 있고 규정 준수 정책이 클라이언트에 적용되는 경우, 클라이언트는 장치의 설정 아래에 'Microsoft 365 Access'를 표시합니다. 기기의 컴플라이언스 상태는 다음과 같은 경우에 보고됩니다.<br>• 기기가 규정을 준수하지 않을 때<br>• 기기가 규정을 준수할 때<br>• 기기가 규정 준수로 돌아올 때<br>• 24시간이 경과했을 때. 상태에 변화가 없으면 일주일/7일에 한 번 보고서가 전송됩니다. |
| iOS, macOS, Android 및 Windows 기기에 대해 Google BeyondCorp로 규정 준수 상태 보고 | 기본적으로 켜져 있습니다.<br>기기의 컴플라이언스 상태는 다음과 같은 경우에 보고됩니다.<br>• 기기가 규정을 준수하지 않을 때<br>• 기기가 규정을 준수할 때<br>• 기기가 규정 준수로 돌아올 때<br>• 24시간이 경과했을 때. 상태에 변화가 없으면 24시간에 한 번 보고서가 전송됩니다. |

4. **다음**을 클릭합니다.
5. **이 구성 활성화**가 기본으로 선택되어 있습니다.
6. 구성의 배포 수준을 선택합니다. 구성 배포에 대한 자세한 내용은 **구성 추가**를 참조하세요.
7. **완료**를 클릭하세요.

# 12.5.5.7. MDM용 Ivanti Neurons에서 Azure로 기기 상태 보고

다음과 같은 경우, MDM용 Ivanti Neurons에서 기기 인벤토리와 규정 준수 상태를 보고합니다.

- 온 디바이스(On-device) 컴플라이언스 상태 변경
- 온 디바이스(On-device) 인벤토리 변경
- 일주일에 한 번, MDM용 Ivanti Neurons에서 규정 준수와 인벤토리 상태 보고

컴플라이언스 정책에서 선택한 작업에 따라 다음과 같은 기기 상태가 전송됩니다.

| 작업<br>(가장 제한적인 작업 적용) | MDM용 Ivanti Neurons 전송 내용 |
| --- | --- |
| 이메일 차단, AppConnect 앱, 격리 | 기기가 규정을 준수하지 않음 |
| 경보 전송 | Azure 규정 준수 |
| 기기 폐기 | Azure 플랫폼에서 제거된 기기 데이터 |

## 기기 상세 정보 페이지

기기에 관한 Azure 정보를 보려면 기기 상세 정보 페이지로 이동하십시오. 필드와 가능한 값에 대한 설명:

| 필드 | 설명 |
| --- | --- |
| Azure 기기 식별자 | Microsoft에서 iOS 또는 Android 기기로 보고한 기기 ID. 예: 007c8232-9489-4074-9b35-345b16f0a72d. 이 기능을 사용하려면 기기 사용자가 Microsoft Authenticator 애플리케이션에 등록해야 하므로 MDM용 Ivanti Neurons에서 이 기기 ID를 수신합니다.<br>기기 ID를 검색할 수 없는 경우 이 필드가 공백으로 남습니다. |
| Azure 기기 컴플라이언스 상태 | Azure에 기기의 컴플라이언스 상태를 열거합니다. 가능한 값:<br>• 진행 중<br>• 성공<br>• 실패함 |
| Azure 클라이언트 상태 코드 | 기기가 Azure에 연결되어 있는지 여부를 나타냅니다. 가능한 값:<br>• Success - 기기 ID를 검색할 수 있음.<br>• Internal_Error - 클라이언트 내 또는 서버 쪽에서 발생한 복구 불가능한 오류.<br>• Workplace_Join_Required - 기기 등록 필요. 기기 사용자가 이 상태를 완화할 수 있습니다.<br>• Interaction_Required - 상호 작용 로그인이 필요합니다. 기기 사용자가 이 상태를 완화할 수 있습니다.<br>• Server_Declined_Scopes - 일부 범위에 대해 액세스 권한이 승인되지 않았습니다.<br>• Server_Protection_Policies_Required - 요청 받은 리소스가 Intune 조건부 액세스 정책에 의해 보호됩니다.<br>• User_Canceled - 기기 사용자가 웹 브라우저에서 "완료" 또는 "취소" 버튼을 눌러 웹 인증 세션을 취소했습니다.<br>• Account_logged_out - 계정 로그아웃됨. |
| Azure 기기 컴플라이언스 보고서 시간 | MDM용 Ivanti Neurons에서 Microsoft Intune으로 기기 규정 준수 상태를 보고한 시간. 공백 필드는 다음 중 하나를 나타냅니다.<br>• 해당 기능이 비활성화됨<br>• MDM용 Ivanti Neurons에서 데이터를 수신했으나 아직 Microsoft API를 호출하지 못함<br>• user_Cancelled 또는 내부 오류와 같은 오류가 존재함 |

# 12.5.5.8. Azure 테넌트의 프로비저닝 해제

다중 MDM용 Ivanti Neurons가 동일한 Azure 테넌트를 사용하도록 활성화되어 있다면 모든 MDM용 Ivanti Neurons에서 프로비전을 해제합니다. 단일 MDM용 Ivanti Neurons가 Azure 사용을 중단해야 할 경우, 해당 MDM용 Ivanti Neurons에 대해서만 파트너 규정 준수 정책을 비활성화할 수 있습니다.

관리자가 MDM용 Ivanti Neurons에서 연결 해제를 수행할 경우, MDM용 Ivanti Neurons는 Azure에 기기 인벤토리 및 규정 준수 상태를 보고하는 것을 중단합니다.

**필수 조건**

- 모든 기기를 비관리로
- 모든 기기를 비준수로

**절차**

## Microsoft

1. Microsoft Azure로 로그인합니다.
2. Intune > 조건부 액세스로 이동합니다. 조건부 액세스 정책이 비활성화되어 있는지 확인하십시오.

## MDM용 Ivanti Neurons

1. MDM용 Ivanti Neurons에 로그인하고 관리로 이동합니다.
2. 좌측 탐색 패널에서 Microsoft Azure > iOS 및 Android용 기기 컴플라이언스를 클릭합니다.
3. 계정 연결 해제를 클릭합니다.

4. 예를 클릭합니다.

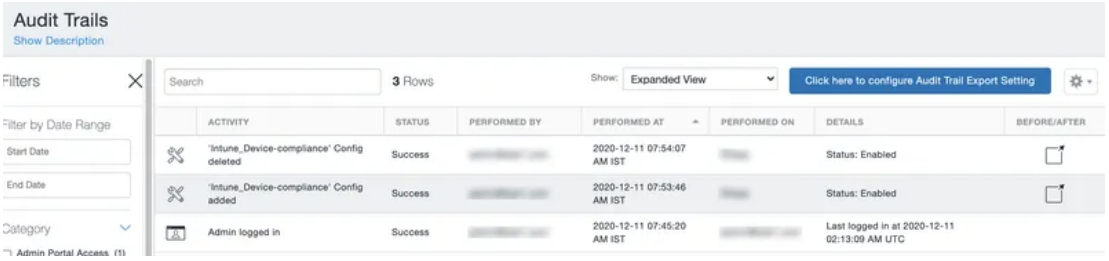
## Azure에서 기기 폐기하기

기기를 폐기하자마자 MDM용 Ivanti Neurons에서 Azure로 기기가 더 이상 관리되지 않으며 미준수 상태라고 보고합니다.

Azure는 90일 후 폐기된 기기 항목을 삭제합니다.

## 로그에 기록된 Azure 계정 활동

모든 활동이 로그에 기록됩니다.



# 12.5.6. 관리 > Microsoft Azure > Office 365 앱 보호

**라이센스: Gold**

Office 365 앱 보호 정책을 설정하여 회사 데이터를 보호하는 데 도움이 될 수 있습니다. 정책은 Microsoft Graph API를 사용한 Microsoft Office 365에 대한 데이터 손실 방지(DLP) 제어를 시행합니다. 그래프 API 중 일부는 관리자가 그래프 SDK를 활용하는 네이티브 iOS 및 Android 앱 보호를 실행하도록 합니다.

이 기능을 사용하여 정책을 다음과 같이 적용합니다.

- Office 365 앱에서 사용자 인쇄 금지.
- Office 365 앱에서 아웃바운드 데이터 공유 금지.
- Office 365 앱에서 PIN 실행.
- Office 365 앱에서 연락처 동기화 비활성화.

## Office 365 앱 보호 사용 필수 조건

Office 365 앱 보호를 사용하려면 다음이 있어야 합니다.

- 유효한 MobileIron 라이센스.
- MDM용 Ivanti Neurons에서 활성화되는 Office 365 앱 보호 기능
- Intune 구독 또는 Intune을 포함하는 Microsoft EMS 구독.
    - 그러나 통합을 활성화하고 시험하기 위해 라이선스를 요구하는 정책이 적용되는 각 사용은 단 하나의 라이선스를 요구합니다.
- 유효한 Office Enterprise 또는 Business 구독(모바일 기기의 Office 365 앱 액세스 포함).
- 1개 이상의 Office 365 앱.
- Active Directory 사용자를 Entra ID와 동기화했습니다.
- Word, Excel 및 PowerPoint 데이터를 보호하도록 기기에 설치된 One Drive for Business. 이는 필수가 아닙니다.
- Microsoft Azure 포털(https://portal.azure.com/)에 액세스하여 Intune 앱 보호 정책을 구성합니다.
- Android 기기에 설치된 Intune 회사 포털 앱입니다.
  기기 사용자는 로그인할 필요가 없습니다. 하지만 기기의 데이터를 보호하려면 이 앱이 설치되어야 합니다. 보호 기능은 사용자가 앱에 로그인했을 때 사용할 수 있습니다.

## Azure 앱으로 MobileIron 등록

이 항목은 MDM용 Ivanti Neurons 소프트웨어를 통해 Azure 테넌트 자격 증명을 등록 및 저장하는 방법과 Android 및iOS Office 365 앱용 Microsoft Azure 클라우드의 앱 보호 정책을 원격으로 관리하는 방법을 설명합니다. 필요하지는 않지만 2개의 브라우저를 열어 다음과 같은 절차에서 단계를 수행할 수 있습니다. 첫 번째 브라우저를 사용하여 Microsoft Azure 포털에 로그인합니다. 두 번째 브라우저를 사용하여 MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.

### Microsoft Azure 포털에 대한 절차

> Microsoft는 때때로 Azure 포털 사용자 인터페이스를 변경할 수 있습니다. 이 지침은 사용자가 Microsoft Azure 포털에 익숙하고 MobileIron을 Azure 앱으로 등록하면서 필요한 조정을 할 수 있다는 것을 가정합니다.

1. 첫 번째 브라우저를 열고 Microsoft Azure 포털(https://portal.azure.com/)에 로그인합니다.

2. 왼쪽 창에 있는 **앱 등록**을 클릭합니다.
3. **+새 애플리케이션 등록**을 클릭합니다.
4. 다음 정보를 입력하여 MobileIron을 Azure 앱으로 등록합니다.
    - **이름:** MobileIron 앱의 이름을 입력합니다. (이 필드는 최소 4개 문자를 입력해야 합니다.)
    - **애플리케이션 유형:** 웹 앱/API를 선택합니다.
    - **로그인 URL:** MobileIron에 로그인할 URL 기기 사용자 액세스를 입력합니다(필수).

창 하단에 있는 **생성**을 클릭하여 앱을 추가하고 Azure 홈페이지로 돌아갑니다.

6. Azure 홈페이지에서 새로 생성된 MobileIron 앱을 클릭합니다.
7. Azure 홈 페이지로 돌아가 MobileIron Azure 앱에 권한을 할당합니다.
8. 새로 생성되는 MobileIron 앱에 필요한 API 권한을 설정하려면 앱 등록에서 앱 이름을 클릭합니다.
9. **API 권한** > **권한 추가**를 클릭합니다.
10. **Microsoft Graph > 위임된 권한 > 기기 관리 앱** 섹션에서 **DeviceManagementApps.Read.All** 권한을 선택한 후 **저장**을 클릭합니다. 기본적으로 user.Read 권한은 앱에 대해 활성화되어 있습니다.
11. 액세스를 부여하려면 **MobileIron에 대한 관리 동의 부여**를 클릭합니다.
12. MDM용 Ivanti Neurons 관리 포털에 대해 다음 절차를 수행합니다.

## MDM용 Ivanti Neurons 관리자 포털 절차

1. 두 번째 브라우저를 열고 MDM용 Ivanti Neurons 관리자 포털에 로그인합니다.
2. **관리 > Microsoft Azure > Office 365 앱 보호**로 이동합니다.
3. MDM용 Ivanti Neurons 관리자 포털에 **애플리케이션 ID**를 붙여넣습니다.
4. **절차**
    1. Azure 포털로 이동합니다.
    2. MobileIron 앱 > **속성**을 선택합니다.
    3. **애플리케이션 ID**를 복사합니다.
    4. 관리 포털에서 **관리 > Microsoft Azure > Office 365 앱 보호**로 돌아갑니다.
    5. **애플리케이션 ID** 필드에 붙여 넣습니다.

MDM용 Ivanti Neurons 관리자 포털에 **애플리케이션 암호**(클라이언트 암호)를 붙여넣습니다.

5. **절차**
    1. Azure 포털로 이동합니다.
    2. MobileIron 앱을 선택합니다.
    3. **키**를 클릭하고 **키 설명**에 이름을 입력한 다음 **기간**에서 만료 기간을 선택합니다.
    4. **저장**을 클릭하고 **키** 값을 복사합니다.
    5. 관리 포털에서 **관리 > Microsoft Azure > Office 365 앱 보호**로 돌아갑니다.
    6. **애플리케이션 비밀**(클라이언트 암호) 필드에 붙여넣습니다.

MDM용 Ivanti Neurons 관리자 포털에 **테넌트 ID**를 붙여넣습니다.

6. **절차**

1. Azure 포털로 이동합니다.
2. 왼쪽 창에서 Entra ID를 클릭한 다음 속성을 클릭합니다.
3. 디렉토리 ID를 복사합니다.
4. 관리 포털에서 **관리 > Microsoft Azure > Office 365 앱 보호**로 돌아갑니다.
5. **테넌트 ID** 필드에 붙여 넣습니다.

Intune 관리 **사용자 이름**과 **비밀번호**를 입력합니다.

- Azure 계정에는 글로벌 관리 권한 또는 제한적인 관리 + Intune 서비스 관리 권한이 있어야 합니다.
- Intune 서비스 관리 권한으로만 로컬 Azure 계정을 생성하는 것이 좋습니다. Microsoft는 Graph API를 활용한 인증에 대하여 ID 공급자에 연합되는 사용자 계정을 지원하지 않습니다.

**인증 및 저장**을 클릭합니다.
제출한 날짜가 잘못된 경우 오류 메시지가 표시됩니다.

# Office 365 앱 보호 정책

Microsoft Graph 자격 증명을 구성한 이후 **앱 > Office 365 앱 보호**로 이동하여 각기 다른 사용자 그룹에 대한 iOS또는 Android기기용 Office 365 앱 보호 정책을 새로 추가합니다.

정책은 **앱 정책** 탭 아래에 **앱 > Office 365 보호** 페이지 나열되어 있습니다. 정책 목록은 업데이트된 시간 스탬프, 플랫폼, 할당된 앱, 배포된 사용자 그룹과 같은 상세 정보를 표로 제공합니다.

## iOS 기기용 Office 365 앱 보호 정책 추가

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **앱 정책 > + 추가**를 클릭합니다.
3. 정책에 대한 **이름** 및 필요한 경우 **설명**을 입력합니다.
4. OS 선택에서 **iOS**를 클릭합니다.
5. **데이터 재배치**에서 다음 설정 및 옵션을 선택합니다.
   - iTunes 및 iCloud 백업 방지
   - 앱에서 다른 앱으로 데이터를 전송할 수 있도록 허용 - 모든 앱(기본값), 정책 관리된 앱, 없음
   - 앱에서 다른 앱의 데이터를 받을 수 있도록 허용 - 모든 앱(기본값), 정책 관리된 앱, 없음
   - “다음으로 저장” 방지
   - 다른 앱에서 잘라내기, 복사 및 붙여넣기 제한 - 모든 앱(기본값), 차단됨, 정책 관리된 앱, 붙여넣기로 정책 관리됨
   - 관리되는 브라우저에서 웹 콘텐츠 표시 제한
   - 앱 데이터 암호화 - 기기가 잠겼을 때(기본값), 기기가 잠기고 열린 파일이 있을 때, 기기 재시작 이후, 기기 설정 사용
   - 연락처 동기화 비활성화
   - 인쇄 비활성화
6. **액세스**에서 다음 설정 및 옵션을 선택합니다.
   - 액세스에 PIN 필요
   - PIN 재설정 이전 시도 횟수(기본값 5)

- 단일 PIN 허용
- PIN 길이(기본값 4)
- PIN 대신 지문 허용(iOS 8+)
- 기기 PIN 관리 시 앱 PIN 비활성화
- 액세스를 위해 기업 자격 증명 필요
- 무단 해제되거나 루팅된 기기에서 관리되는 앱 실행 차단
- (분) 후 액세스 요구 사항 재확인
  - 시간 제한 - 1~65535 사이의 값이어야 함(기본값 30)
  - 오프라인 - 유예 기간으로 1~65535 사이의 값이어야 함(기본값 720)
  - 앱 데이터 삭제 전 오프라인 간격(일) - 1~65535 사이의 값이어야 함(기본값 90)

최소 iOS 운영 체제 필요

- 최소 iOS 운영 체제 요구 사항(경고만)
- 최소 앱 버전 필요
- 최소 앱 버전 요구 사항(경고만)
- 최소 Intune 앱 보호 정책 SDK 버전 필요

**다음**을 클릭하세요.

8. 이 정책을 적용할 앱을 선택하고 할당합니다.
9. **다음**을 클릭하세요.
10. 이 정책을 적용할 사용자 그룹을 선택합니다.
11. **완료**를 클릭하세요.

## Android 기기용 Office 365 앱 보호 정책 추가

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **앱 정책 > + 추가**를 클릭합니다.
3. 정책에 대한 **이름** 및 필요한 경우 **설명**을 입력합니다.
4. OS 선택에서 **Android**를 클릭합니다.
5. **데이터 재배치**에서 다음 설정 및 옵션을 선택합니다.
   - Android 백업 방지
   - 앱에서 다른 앱으로 데이터를 전송할 수 있도록 허용 - 모든 앱(기본값), 정책 관리된 앱, 없음
   - 앱에서 다른 앱의 데이터를 받을 수 있도록 허용 - 모든 앱(기본값), 정책 관리된 앱, 없음
   - “다음으로 저장” 방지
   - 다른 앱에서 잘라내기, 복사 및 붙여넣기 제한 - 모든 앱(기본값), 차단됨, 정책 관리된 앱, 붙여넣기로 정책 관리됨
   - 관리되는 브라우저에서 웹 콘텐츠 표시 제한
   - 앱 데이터 암호화
   - 기기 암호화가 활성화된 경우 앱 암호화 비활성화

- 연락처 동기화 비활성화
- 인쇄 비활성화

6. **액세스**에서 다음 설정 및 옵션을 선택합니다.
   - 액세스에 PIN 필요
   - PIN 재설정 이전 시도 횟수(기본값 5)
   - 단일 PIN 허용
   - PIN 길이(기본값 4)
   - PIN 대신 지문 허용(Android 6+)
   - 기기 PIN 관리 시 앱 PIN 비활성화
   - 액세스를 위해 기업 자격 증명 필요
   - 무단 해제되거나 루팅된 기기에서 관리되는 앱 실행 차단
   - (분) 후 액세스 요구 사항 재확인
     - 시간 제한 - 1~65535 사이의 값이어야 함(기본값 30)
     - 오프라인 - 유예 기간으로 1~65535 사이의 값이어야 함(기본값 720)
     - 앱 데이터 삭제 전 오프라인 간격(일) - 1~65535 사이의 값이어야 함(기본값 90)
   - 화면 캡처 및 Android 길잡이 차단
   - 최소 Android 운영 체제 필요
   - 최소 Android 운영 체제 요구 사항(경고만)
   - 최소 앱 버전 필요
   - 최소 앱 버전 요구 사항(경고만)
   - 최소 Intune 앱 보호 정책 SDK 버전 필요
7. **다음**을 클릭하세요.
8. 이 정책을 적용할 앱을 선택하고 할당합니다.
9. **다음**을 클릭하세요.
10. 이 정책을 적용할 사용자 그룹을 수정합니다.
11. **완료**를 클릭하세요.

## Office 365 앱 보호 정책 수정

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **앱 정책**을 클릭합니다.
3. 수정하고자 하는 정책의 이름을 클릭합니다.
4. 정책 상세 정보 페이지에서 **편집**을 클릭합니다.
5. 정책 구성 설정을 수정합니다.
6. **다음**을 클릭하세요.
7. 이 정책을 적용할 앱의 목록을 수정합니다.
8. **다음**을 클릭하세요.

9. 이 정책을 적용할 사용자 그룹을 수정합니다.
10. **완료**를 클릭하세요.

### Office 365 앱 보호 정책 삭제

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **앱 정책**을 클릭합니다.
3. **작업** 열에서 삭제하고자 하는 정책 이름에 대해 삭제 아이콘을 클릭합니다.
4. **예**를 눌러 확인합니다.

## Office 365 앱 구성

**앱 구성** 탭 아래 **앱 > Office 365 앱 보호** 페이지로 이동하여 각기 다른 사용자 그룹에 대한 Office 365 앱 구성을 추가, 수정, 삭제할 수 있습니다. 이 앱 구성에서 관리자는 키-값 쌍의 목록을 추가할 수 있습니다. 또한 하나 이상의 Office 365 앱에 구성을 할당할 수 있습니다. 앱 구성 탭은 업데이트된 시간 스탬프, 할당된 앱, 배포 상태 등을 표로 정리된 세부정보를 구성과 함께 나열합니다.

### Office 365 앱 구성 추가하기

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **앱 구성 > + 추가**를 클릭합니다.
3. 구성에 대한 **이름** 및 필요한 경우 **설명**을 입력합니다.
4. 키-값 쌍을 입력합니다.
5. **다음**을 클릭하세요.
6. 이 구성을 적용할 앱을 선택합니다.
7. **다음**을 클릭하세요.
8. 이 구성을 적용할 사용자 그룹을 선택합니다.
9. **완료**를 클릭하세요.

### Office 365 앱 구성 수정하기

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **앱 구성**을 클릭합니다.
3. 수정하고자 하는 구성의 이름을 클릭합니다.
4. 구성 상세 정보 페이지에서 **편집**을 클릭합니다.
5. 또는, **앱 배포** 또는 **사용자 그룹 배포** 탭을 클릭합니다. **편집**을 클릭하여 설정을 수정하고 **저장**을 클릭합니다.
6. 구성 설정을 수정합니다.
7. **다음**을 클릭하세요.
8. 이 구성을 적용할 앱의 목록을 수정합니다.
9. **다음**을 클릭하세요.

10. 이 구성을 적용할 사용자 그룹을 수정합니다.
11. **완료**를 클릭하세요.

### Office 365 앱 구성 삭제하기

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **앱 구성**을 클릭합니다.
3. **작업** 열에서 삭제하고자 하는 구성 이름에 대해 삭제 아이콘을 클릭합니다.
4. **예**를 눌러 확인합니다.

## 컴플라이언스 위반 Office 365 앱 사용자

관리자는 컴플라이언스 위반 사용자 및 사용 기기 목록을 검토할 수 있습니다. 이 페이지를 사용하여 이처럼 표시된 기기의 Office 365 앱을 지웁니다.

### Office 365 앱 지우기

**절차**

1. **앱 > Office 365 앱 보호**로 이동합니다.
2. **컴플라이언스 위반 사용자**를 클릭합니다.
3. 다음 작업 중 하나를 수행합니다.
    - 목록에서 사용자를 선택하고 **Office 365 앱 지우기**를 클릭합니다.
    - 사용자 이름을 클릭하여 컴플라이언스 위반 앱이 있는 기기 목록을 표시합니다. **작업**열 아래에서 특정 기기에 대해 **Office 365 앱 지우기** 아이콘을 클릭합니다.
    - 사용자 이름을 클릭하여 컴플라이언스 위반 앱이 있는 기기 목록을 표시합니다. 특정 기기 이름을 클릭하여 번들 ID/패키지 이름 목록으로 된 앱과 표시된 이유를 검토합니다. **Office 365 앱 지우기**를 클릭합니다.
4. **예**를 클릭해 작업을 확인합니다.

또는, 다음 단계를 수행합니다.

1. **사용자**를 선택하세요.
2. 사용자 이름을 클릭하여 사용자 상세 정보 페이지를 엽니다.
3. **작업 > Office 365 앱 지우기**를 클릭합니다.
4. Office 365 앱을 지워야 하는 기기를 선택합니다.
5. **확인**을 클릭해 작업을 확인합니다.

### Office 365 앱 지우기 요청 취소하기

**절차**

1. **사용자**를 선택하세요.
2. 사용자 이름을 클릭하여 사용자 상세 정보 페이지를 엽니다.
3. **Office 365 보호** 탭을 클릭합니다.
4. **보고서 유형 선택** 드롭다운 박스에서 **지우기 요청** 보고서를 선택하여 해당 정보를 나타냅니다.

5. 지우기 요청을 취소해야 하는 기기를 선택합니다. 지우기 보류 상태인 기기만 선택할 수 있습니다.
6. **지우기 취소**를 클릭합니다.
7. **확인**을 클릭해 작업을 확인합니다.

## Office 365 앱 보호 사용자를 위한 앱 보고서

관리자는 다음 보고서 중 하나를 선택하여 Office 365 앱 보호 사용자 및 관련 정보를 검토할 수 있습니다.

- 앱 정책 보고서
- 앱 구성 보고서
- 요청 지우기

앱 보고서의 정보에는 번들 ID/패키지 이름, 기기 이름, 기기 유형, 정책 또는 기기에 배포된 구성, 상태(동기화됨, 동기화되었지만 최신 버전이 아님, 또는 동기화되지 않음), 마지막 체크인 시간이 포함됩니다. 앱 보고서의 정보는 CSV 파일로 내보내지며 이후 참조나 분석에 활용할 수 있습니다.

지우기 요청 보고서의 정보에는 표시 이름, 사용자 이름, 기기 이름, 기기 유형 및 지우기 상태(지우기 보류 또는 지우기 완료)가 포함됩니다.

원하는 보고서의 검토하려면 다음 단계를 수행합니다.

1. **사용자**를 선택하세요.
2. 사용자 이름을 클릭하여 사용자 상세 정보 페이지를 엽니다.
3. **Office 365 보호** 탭을 클릭합니다.
4. **보고서 유형 선택** 드롭다운 박스에서 보고서 중 하나를 선택하여 해당 정보를 표시합니다.
5. (선택 사항) 지우기 요청 보고서에서 지우기 요청을 취소해야 하는 기기를 선택하고 **지우기 취소**를 클릭합니다. 지우기 보류 상태인 기기만 선택할 수 있습니다.
6. (선택 사항) **CSV로 내보내기**를 클릭하고 CSV 파일로 보고서 콘텐츠를 다운로드하여 이후 참조나 분석에 활용합니다.

# 12.6. Google Apps와 연결

이 섹션에는 다음 주제가 포함됩니다.

- 관리되는 Google Play 계정(Android Enterprise 계정)
- Android 기기 등록
- Android 관리 API
- Google Apps API
- 관리 - Android Enterprise

# 12.6.1. 관리되는 Google Play 계정(Android Enterprise 계정)

**라이센스: Silver**

관리되는 Google Play 계정은 Android Enterprise 기기를 사용하고 구성해야 합니다. Google 앱 디렉토리 동기화(GADS)를 사용하거나 Google 계정을 사용하여 기기를 등록할 필요가 없습니다.

**중요:** 이미 Android Enterprise를 설정한 경우 먼저 해당 기기를 폐기해야 이 기능을 사용할 수 있습니다.

## 관리되는 Google Play 계정을 사용하여 Android Enterprise 구성

**절차**

1. MDM용 Ivanti Neurons 포털에 로그인합니다.
2. **관리자 > Google > Android Enterprise**로 이동합니다.
3. **관리되는 Google Play 계정**에서 **Google에 권한 부여**를 클릭하면 **회사용 Google Play** 페이지가 표시됩니다.
4. **Google Play 계정 이메일 ID**를 입력합니다.
5. **시작하기**를 클릭합니다.
6. Android Enterprise 계약에 동의합니다.
7. **확인**을 클릭합니다.
8. **등록 완료**를 클릭합니다.
   **Android Enterprise 구성됨** 섹션에 다음 정보가 표시됩니다:
   - **상태**
   - **관리자 이메일**
   - **기업 유형**
   - **Google Enterprise ID**

관리되는 Google Play 계정을 사용하여 Android Enterprise가 설정될 때 사용자당 등록되는 기기의 수에 제한이 있습니다. 이 제한을 넘어서려면 새 사용자를 생성하는 동안 **Android Enterprise 기기 계정** 옵션을 선택하여 이 계정에 연결된 Android Enterprise 작업 관리 기기 등록이 Google 기기 계정에 자동으로 할당되도록 합니다.

기기 계정은 COSU(일회용) 배포(예: 키오스크 모드 포함)를 위해 사용됩니다. 기기 계정이 있는 사용자는 Google Play 액세스가 제한될 수 있습니다.

인증 토큰이 만료되거나 계정 또는 엔터프라이즈가 삭제되는 등의 다양한 이유로 가끔씩 관리되는 Google Play 계정 또는 해당 토큰이 만료됩니다. 이러한 경우 Google Play 서비스는 기존 계정을 제거하고 UEM 서버에서 얻은 새 토큰으로 계정을 추가하여 기기가 다시 프로비저닝되도록 클라이언트를 트리거하는 브로드캐스트 작업을 통해 클라이언트에 알립니다.

이때 이전 계정을 제거할 수 없거나 다시 프로비저닝할 때 여러 번 시도하면 계정 재프로비저닝이 실패하며, 기기가 작업 프로필 모드인지 관리형 기기 모드인지에 따라 사용자에게 클라이언트를 폐기하거나 기기를 공장 초기화하여 다시 시작하라는 알림이 각각 표시됩니다.

## 기존 관리되는 Google Play 계정을 관리형 Google 도메인 계정으로 마이그레이션(BTE)

이 기능을 사용하면 Android Enterprise 계정 및 기기를 **관리되는 Google Play 계정**에서 **관리형 Google 도메인 계정**으로 마이그레이션할 수 있습니다.

마이그레이션은 다음으로 구성됩니다:

- 계정 업그레이드
- 기기 마이그레이션

### 필수 조건

- 기기는 업무 관리형 기기 또는 작업 프로필 모드 중 하나로 등록되어야 하며, 회사 소유 기기의 작업 프로필(WPCOD) 모드로 등록된 기기는 Android 12 이상을 실행해야 합니다.
- 기기에 유효한 회사 또는 비즈니스 이메일 ID가 할당되어 있습니다.

> 기기에 회사 이메일 ID가 아닌 이메일 ID가 할당된 경우, 관리자는 기기가 마이그레이션 대상이 되도록 유효한 회사 이메일 ID를 다시 할당해야 합니다.

## Android Enterprise 계정 업그레이드

Android Enterprise 계정을 관리되는 Google Play 계정에서 관리형 Google 도메인 계정으로 업그레이드합니다.

### 절차

1. **관리** -> **Google** → **Android Enterprise**로 이동합니다.
2. **계정 업그레이드**를 클릭합니다.
3. 유효한 회사 또는 비즈니스 이메일 ID를 사용하여 로그인합니다.
4. 업그레이드 프로세스를 완료합니다.
5. 페이지를 새로 고칩니다.

## 기기 마이그레이션 구성 적용

### 절차

1. 구성으로 이동합니다.
2. **Android Enterprise: 관리형 Google Play에서 관리형 Google 계정으로 기기 마이그레이션** 구성 > **편집** > **다음** > **모든 기기 또는 사용자 정의** > **점진적 롤아웃 배포** 선택 – 기본적으로 **수동 롤아웃** 옵션 > 드롭다운에서 선택 **선택 요약에 포함된 사용자 정의 기기 %(점진적 롤아웃)** 또는 **선택 요약에 포함된 모든 기기**를 선택합니다.
3. **완료**를 클릭하세요.

## 기기 마이그레이션 완료

### 절차

1. 기기에서 "업무용 계정 추가" 메시지가 표시되면 **계속**을 탭합니다.
2. **회사 이메일 ID**를 확인합니다.
3. **비밀번호**를 입력합니다.
4. 사용 가능한 경우 **2단계 인증(2FA)**을 완료합니다.
5. 계정 설정 프로세스를 완료합니다.

## 마이그레이션 확인

**기기에서**

1. **Google Play 스토어**를 엽니다.
2. 계정 유형이 업무 계정에서 회사 도메인 계정으로 변경되었는지 확인합니다.

**관리 콘솔에서**

- **Android Enterprise: 관리형 Google Play에서 관리형 Google Play 계정으로 기기 마이그레이션** 구성 상태를 보려면 **기기** > **기기** > **기기 상세 정보** > **구성** > **Android Enterprise: 관리형 Google Play에서 관리형 Google 계정으로 기기 마이그레이션**으로 이동합니다. 구성 상태가 설치됨 상태인지 확인합니다.

## 마이그레이션 상태 모니터링

관리자는 다음을 사용하여 마이그레이션(**관리형 Google 계정으로 마이그레이션됨**) 진행 상황을 추적할 수 있습니다.

- **기기 상세 정보** – 기기별 마이그레이션 상태 보기
- **고급 검색** – 마이그레이션된 기기와 마이그레이션되지 않은 기기 필터링
- **기기 그룹** – 마이그레이션된 기기와 마이그레이션되지 않은 기기 그룹화

이러한 옵션은 추가 조치가 필요한 기기를 식별하는 데 도움이 됩니다.

## 관리형 Google 도메인 계정을 사용한 새 등록(BTE)

Android Enterprise는 Google 인증 사용 여부와 관계없이 **관리형 Google 도메인 계정**을 사용하여 구성할 수 있습니다.

### 절차

1. 포털에 로그인합니다.
2. **관리** > **Google** > **Android Enterprise**로 이동합니다.
3. **관리되는 Google Play 계정**에서 **권한 부여**를 클릭합니다.
4. **회사** 또는 **비즈니스 이메일 ID**를 입력하고 **다음**을 클릭합니다.
5. **새 바인딩 만들기..**를 선택합니다 **바인딩 옵션 선택** 페이지에서
6. **확인**을 클릭합니다. **건너뛰기** 및 **활성화** 옵션이 표시됩니다.
- **건너뛰기**- 인증 없이 진행합니다.
- **활성화** – 인증을 진행합니다.

Android Enterprise 섹션에 다음 정보가 표시됩니다.

- **상태**: 연결 상태를 표시합니다.
- **관리자 이메일**: 회사 또는 비즈니스 이메일 ID를 표시합니다.
- **기업 유형**: 기업 유형을 표시합니다.
- **Google 인증 설정**: 인증 필요에 따라 아니요/예를 표시합니다.
- **Google Enterprise ID**: 고유한 Google Enterprise ID를 표시합니다.
- **기업 이름**: 기업 이름을 표시합니다.

# 12.6.2. Android 기기 등록

Android 기기 등록 도중 등록 완료를 위해 IMEI에 보고해야 하는 전화기 권한, 전화번호 및 기타 전화기 식별자가 필요한 경우 이 옵션을 구성할 수 있습니다. 구성되면 기기 사용자에게 Go 클라이언트의 기기 식별자 액세스 권한 부여 메시지가 표시됩니다.

> 이 구성은 Android 버전 6.0 이상의 모든 Android 기기의 새 등록에만 해당됩니다.

1. **관리자 > Google > 등록**을 선택합니다.
2. **등록 시 Android 장치 식별자 필요(직장 프로필 및 장치 관리자)**를 선택합니다.
3. **저장**을 클릭하세요.

분실 모드에 대한 자세한 내용은 **분실 모드에서 Android 기기 관리하기**를 참조하십시오.

# 12.6.3. Android 관리 API

Android 관리 API(AMAPI)는 Google Android UEM 기능을 MDM용 Ivanti Neurons에 통합하는 Google의 Cloud 플랫폼 API입니다. Android Enterprise 설정에서 기기 관리를 위해 기기에 클라이언트 앱을 설치할 필요 없이 Android Enterprise 기기를 관리하도록 Android 관리 API 프레임워크를 활성화할 수 있습니다. 현재 MTD와 같은 다른 기능을 위해 Go app을(를) 장치에 푸시하는 기능은 지원되지 않습니다.

설정에서 Android Enterprise 계정을 구성하면 Android 관리 API 프레임워크를 활성화하여 사용할 수 있습니다. 사용할 수 있게 된 후에는 다음과 같이 할 수 있습니다.

- 등록 프로필을 추가하여 QR 코드를 기기 등록에 사용할 수 있습니다.
- 특정 목적을 위해 등록된 기기에 대해 전용 기기 구성(기업 소유의 일회용 기기, COSU)을 생성할 수 있습니다.

현재 Android 관리 API는 전용 모드에 Google Play가 설치되고 프로비저닝되어 있는 Android 버전 9 이상에서 작동하는 기기에서만 지원됩니다. 기업 전용 모드는 기업 소유의 일회용 기기(COSU) 모드라고도 하며, 기기 소유자 모드의 일종입니다. 또한, 이 기능은 다음과 같은 기기 작업을 지원합니다.

- 잠금
- 재부팅
- 서버와 동기화
- 지우기

기기 체크인 일정은 규칙적으로(시간별로) 수립됩니다. 그러나 즉각적인 조치가 필요한 경우 기기 상세 정보 페이지에서 '서버와 동기화' 기기 작업을 사용하십시오. AMAPI 장치는 MDM용 Ivanti Neurons에 필수 체크인을 전송하지 않습니다. 인벤토리 업데이트는 기기에서 활동이 있을 때 수행됩니다.

## Android 관리 API 활성화

Android Management API를 활성화하려면 **관리자 > Android Enterprise > Google에 권한 부여(유효한 Google 주소 필요) > Android Enterprise 활성화**로 이동합니다.

Android Management API 기능의 활성 상태(**예**는 활성, **아니요**는 비활성) 역시 기기 세부 정보 페이지에 표시됩니다.

> GSuite 계정은 COSU에서 현재 지원되지 않습니다.

## 등록 프로필 추가

QR 코드 스캔 또는 토큰의 영숫자 문자열을 사용하여 Android 기기를 등록하려면 등록 프로필을 생성해야 합니다. 등록 프로필은 Android 관리 API가 활성화된 경우에만 생성할 수 있습니다. 등록 프로필과 연결할 사용자 지정 기기 속성도 생성할 수 있습니다.

1. **관리 > Android 엔터프라이즈 > 등록 프로필**을 선택합니다.
2. **등록 프로필 - 기업 소유 전용 기기** 창에서 다음 설정을 구성합니다.
3. **저장**을 클릭합니다. **프로필 요약** 창에 다음과 같은 토큰 상세 정보가 표시됩니다.

| 설정 | 설명 |
| --- | --- |
| **Windows** | 이 등록 프로필의 이름을 입력합니다. |
| **설명** | 이 등록 프로필의 목적에 대한 명백한 설명을 입력합니다. |
| **사용자 이름** | 유효한 사용자 이름의 처음 몇 자를 입력하면 표시되는 일치하는 결과 중 하나를 선택합니다.<br>유효한 사용자 이름은 로컬 사용자 또는 LDAP 사용자에 있을 수 있습니다.<br>등록 프로필은 프로필의 QR 코드를 사용하여 등록된 기기에 태그를 지정하여, 등록된 프로필의 대상 사용자에게 속한 기기로 표시되도록 합니다. |
| **토큰 유효성** | 인증 토큰 QR 코드 스캔의 유효성을 나타내는 일 수를 입력합니다. 입력한 숫자는 1~30여야 합니다. 만료 기간 이후의 토큰 또는 등록 프로필을 사용하는 경우 기기가 재설정됩니다. |
| **사용자 지정 기기 속성** | 작업 열에서 **+새로 추가**를 클릭하여 등록 프로필과 연결할 사용자 지정 기기 속성을 추가합니다.<br>1. 드롭다운 목록의 **속성 이름** 열에서 사용자 지정 기기 속성을 선택합니다.<br>2. **값** 열에서 사용자 지정 속성의 값을 입력합니다.<br>3. **저장**을 클릭합니다. 추가된 사용자 지정 기기 속성이 표에 표시됩니다. 삭제하려면 작업 열에서 **삭제** 옵션을 클릭합니다.<br>사용자 지정 속성은 프로필 생성 중 등록 프로필에만 추가할 수 있습니다. 프로필 생성 후에는 속성 필드를 편집할 수 없습니다. |

- 이름
- 설명
- 사용자 이름
- 토큰 생성 날짜
- 토큰 만료 날짜
- 토큰 값
- QR 코드
- 사용자 지정 기기 속성.

> 등록 후 10분 이내로 기기의 적절한 구성이 확보되지 않으면 기기는 재설정됩니다. 그런 경우에는 등록 토큰/QR 코드를 사용하여 다시 등록해야 합니다.

등록 프로필이 생성되면 **등록 프로필** 페이지에 열거됩니다. **작업** 열에서 다음 작업을 수행할 수 있습니다.

- 프로필 요약 창에서 등록 프로필의 상세 정보를 보려면 보기 아이콘을 클릭합니다. QR 코드도 이 창에 표시됩니다.
- 등록 프로필의 상세 정보를 편집하려면 편집 아이콘을 클릭합니다.

> 토큰 유효성만 편집할 수 있습니다. 기타 속성은 편집할 수 없습니다.

등록 프로필을 삭제하려면 삭제 아이콘을 클릭합니다.

## COSU 구성 생성

관리자는 전용 기기(기업 소유의 일회용 기기 또는 COSU 기기)를 사용하여 Android Enterprise를 사용하는 고유의 목적에 사용할 수 있는 전용 기기를 구성할 수 있습니다. COSU 구성은 사용자가 키오스크 모드에서 사용할 수 있는 유일한 앱을 제공하기 위해 업무 관리 기기(기기 소유자 모드)에 배포됩니다. 회사 소유 기기의 작업 프로필에 있는 기기는 지원되지 않습니다.

이 구성을 사용하면 관리자는 앱을 화면에 고정시킴으로써 Kiosk 모드 사용자가 이 앱을 고정 취소하고 앱에서 벗어나 기기의 다른 화면으로 이동하거나 기기의 다른 앱을 사용하지 못하도록 기기를 구성할 수 있습니다.

> 고급 옵션 및 앱 구성에서 "기기에 설치" 옵션을 선택하여 AMA 기기에 다른 앱도 강제로 설치할 수 있지만, 키오스크 앱이 구성을 통해 스크린에 고정되는 동안에는 이 앱과 상호작용할 수 없습니다. 다중 앱 키오스크의 경우에는 업무 관리 기기의 키오스크 기능(기기 소유자 모드)을 사용하는 것이 좋습니다. 그러면 앱과 기기의 설정을 보다 잘 제어할 수 있으며, 다중 사용자 모드로 확장할 수도 있습니다.

관리자는 필요에 따라 다양한 옵션을 검토하여 최종 사용자에게 Google DPC를 통해서 시스템 탐색을 하도록 허용하거나 기기에 푸시된 다른 앱을 사용할 수 있도록 허용하는 등의 구성 변경을 수행할 수 있습니다.

COSU 구성은 할당된 우선순위에 따라 결정됩니다. 우선순위가 가장 높은 구성은 정책 구성을 Google에 푸시하는 데 사용됩니다. COSU 구성은 정해진 공간 내의 기기에 적용됩니다. 기본 공간에서 정의된 경우에는 다른 공간에 위임할 수 있습니다.

구성하려면,

1. **구성 > +추가**로 이동합니다.
2. **잠금 및 키오스크: Android Enterprise 구성**에서 **전용 기기(기업 소유의 일회용 기기, COSU)**를 클릭합니다.
3. 구성 이름을 입력합니다.
4. 설명을 입력합니다.
5. 관련 탭을 클릭하여 다음 설정을 구성할 수 있습니다.

- **앱 설정**
- **일반 잠금**
- **키오스크 사용자 지정**
- **시스템 설정**

다음 표는 구성 가능한 필드의 상세 정보를 보여줍니다.

| 설정 | 설명 |
| --- | --- |
| **앱 설정** | |
| **앱 이름** | 드롭다운에 원하는 앱이 표시될 때까지 앱 이름의 앞 글자를 입력하여 기기에 고정할 앱을 선택합니다. 원하는 앱이 드롭다운에 표시되지 않으면 배포하려는 앱이 Play Store에 있는 공개/비공개 앱인지 그리고 App Catalog에 추가되어 있는지 확인합니다.<br>이 필드는 필수입니다. 이 필드에 추가할 앱을 선택하지 않으면 구성을 생성할 수 없습니다. 공개 및 비공개 앱만 추가할 수 있습니다. 인하우스 앱과 웹 앱(비공개)은 추가할 수 없습니다. |
| **일반 잠금** | |
| **디스플레이 켜짐 유지**<br><br>**키오스크 사용자 지정**<br><br>**상태 표시줄 사용자 지정** | 기기가 켜져 있도록 할 배터리 연결 모드를 구성합니다. 다음 옵션 중 하나를 선택합니다.<br>• **AC** - 전원 소스는 AC 충전기입니다.<br>• **무선**<br>• **USB** - 전원 소스는 USB 포트입니다.<br>• **모두** - 전원 소스는 AC 충전기, USB 포트 또는 무선 충전기입니다.<br><br>대상 기기의 상태 표시줄을 사용자 지정하려면 다음 옵션 중 하나를 선택합니다.<br>• **알림 및 시스템 정보 사용 설정** - 상태 표시줄에 시스템 정보 및 알림을 표시합니다.<br>• **시스템 정보만 사용 설정** - 상태 표시줄에 시스템 정보만 표시합니다. |
| **시스템 탐색 사용자 지정**<br><br>**전역 작업 활성화** | Kiosk 모드에서 다음 옵션 중 하나를 선택하여 탐색 기능(홈, 개요 버튼)에 대한 액세스를 지정합니다.<br>• **활성화** - 홈 및 개요 버튼 탐색을 활성화합니다. 이 옵션을 선택하면 사용자는 지정된 앱 중에서 탐색할 수 있습니다.<br>• **비활성화** - 홈 및 개요 버튼 탐색을 비활성화합니다.<br>• **홈 버튼 전용** - 홈 버튼만 탐색을 활성화합니다.<br>뒤로 가기 버튼은 모든 옵션에서 사용 가능합니다.<br><br>키오스크 모드에서 전역 작업을 활성화하려면 선택합니다. 전원 버튼과 연결된 재시작 및 종료 기능은 이 옵션을 통해 제어됩니다. |
| **시스템 오류 대화 상자 활성화**<br><br>**시스템 설정**<br><br>**시스템 업데이트 설정** | 키오스크 모드에서 충돌하거나 반응이 없는 앱에 대한 오류 대화 상자를 활성화하려면 선택합니다.<br><br>시스템 업데이트를 관리하려면 다음 설정을 구성합니다.<br>• **시스템 업데이트** - 필요한 시스템 업데이트 유형을 선택합니다.<br>  ◦ **자동** - 업데이트가 가능하면 즉시 자동으로 설치합니다.<br>  ◦ **연기** - 자동 설치를 최장 30일까지 연기합니다.<br>  ◦ **창** - 일상적 유지 관리 창에서 자동으로 설치합니다. 유지 관리 창 기간의 시작 시간 및 종료 시간을 설정합니다. |

| 설정 | 설명 |
| --- | --- |
| | 기기에 설치되는 업데이트는 지원되는 기능 세트, Android 버전, 및 기기에 설치되는 Google DPC 버전에 따라 다를 수 있습니다.<br>• **동결 기간** - 기기가 동결 기간 내에 설정되면 수신되는 시스템 업데이트는 모두 차단되어 설치되지 않습니다. 동결 기간의 **시작 날짜** 및 **종료 날짜**를 설정하려면 **동결 기간 추가**를 클릭합니다.<br>기기가 동결 기간에 포함되지 않으면 정상적인 업데이트 작업이 적용됩니다. 종료 날짜가 시작 날짜 이전인 경우에는 동결 기간이 현재 연도와 다음 연도 사이로 연장됩니다.<br>동결 기간은 최장 90일까지로 설정할 수 있습니다. 연속된 2개의 동결 기간은 최소 60일 단위로 분리해야 합니다. |

6. **다음**을 클릭하세요.
7. 다음 배포 옵션 중 하나를 선택합니다.

- **모든 기기**
- **배포 안 함**(기본값)
- **사용자 지정**

8. **완료**를 클릭하세요.

## AMAPI 기기에서 앱 관리

COSU 구성이 기기에 배포되는 경우 앱이 푸시되어 AMA 기기의 스크린에 고정됩니다. 기기에 푸시되는 COSU 구성과 관계없이, AMA 기기에 설치된 앱을 여전히 관리할 수 있습니다. 다음은 이러한 기기의 앱 관리에 대한 상세 정보입니다.

- 공개 및 비공개 앱만 지원되고, 인하우스 앱과 웹 클립은 지원되지 않습니다.
- 앱은 설치 설정의 "기기에 설치" 또는 "자동 설치" 옵션이 활성화되는 경우에만 푸시됩니다. 이러한 옵션 중 어떤 것도 활성화되지 않은 상태로 사용자/기기에 할당되는 앱은 기기 또는 기기의 Play Store에 나타나지 않고, 사용자 조치가 필요합니다.
- 지원되는 앱 구성은 관리되는 Google Play 및 작업 관리 기기(Android for Work) 설정입니다. OEMConfig 앱의 관리형 구성 지원을 포함한 앱의 관리형 구성이 지원됩니다.

> 구성의 설치/제거 완료 시기는 원하는 작업 수행 여부에 관한 Google(메시징 서비스) 알림에 따라 다를 수 있습니다.

- 이제 AMA 기기 등록의 일부로써 Go app(이)가 기본값으로 설치됩니다. 등록 중에는 앱이 화면에 고정되며, 설정이 완료되면 백그라운드에서 실행됩니다.

> 제조업체, OS 버전 및 보안 패치 수준에 기반한 기기 등록 요구 사항 적용의 경우를 제외한 정책은 지원되지 않습니다. 허용 목록에 있는 기기만 MDM용 Ivanti Neurons에 등록할 수 있는 기기 허용 목록 기능이 지원됩니다.

## AMAPI 기기에서 앱 피드백 지원 관리하기

앱 피드백 지원은 AMAPI(COSU) 기기에서 관리할 수 있습니다. AMAPI(COSU) 모드에서 기기를 등록하면 Go app의 개입 없이 관리형 앱 구성이 Google에서 바로 MDM용 Ivanti Neurons(으)로 푸시됩니다. 관리형 앱 피드백 정보를 기기 수준에서 보려면 **기기 세부 정보 > 설치된 앱 > 피드백 보기**에서 확인할 수 있으며, 개별 앱 수준에서 보려면 '앱 구성 피드백' 탭 아래 앱 카탈로그에서 특정 Android 앱을 찾으면 모든 기기의 전체 보고서를 확인할 수 있습니다. 앱 피드백 방식에 대한 정보는 앱 피드백 동기화 및 가져오기를 확인하십시오.

## AMAPI 제한

현재 AMAPI에는 다음 제한이 있습니다.

- 전용 기기(COSU 모드)만 지원됩니다.

## 지원되는 구성

AMAPI에는 다음 구성이 지원됩니다.

- 앱 배포(단일 또는 다중 앱)
- 기기로 푸시되는 앱에 대한 관리 앱 구성
- Wi-Fi 구성
- Android Enterprise 잠금 전용(COSU) 구성
- Always On VPN 구성

# 12.6.4. Google Apps API

Single Sign On(SSO)를 이용해 Google Apps 서비스 이용 인증을 받는 Google 사용자의 경우, SSO 구동을 통한 외부 인증 서비스로의 리디렉트를 기기가 지원하지 못하도록 하는 프로토콜 제한으로 인해 Exchange를 통한 이메일 및 연락처, 일정 등의 사용자 연동이 불가능할 수 있습니다. 이 서비스는 ActiveSync 연결 계정 비밀번호를 생성 및 관리함으로써 이 문제를 해결합니다.

**필수 조건**

Google Apps API 기능을 구성하기 전:

- https://console.developers.google.com/의 계정에 관리자로 액세스해야 합니다.
- https://admin.google.com의 계정에 관리자로 액세스해야 합니다.

## Google Apps API 기능 활성화

**절차**

1. **관리 > Google > Google Apps API**를 선택합니다.
2. 1로 표시된 왼쪽 직사각형 하단에서 **1단계: Google Dev**를 클릭합니다.
3. 1단계: Google Dev 페이지가 나타납니다.
   1단계: Google Dev 페이지에 표시된 지침에 따라 진행한 다음 **완료**를 클릭합니다.
4. 2로 표시된 중앙 직사각형 하단에서 **2단계: Google 관리자**를 클릭합니다.
5. 2단계: Google 관리자 페이지가 나타납니다.
   2단계: Google 관리 페이지에 표시된 지침에 따라 진행한 다음 **완료**를 클릭합니다.
6. 우측의 3으로 라벨링된 작사각형의 **Google 관리자 이름** 필드에 Google 관리자 이름을 입력합니다.
7. 같은 사각형의 **파일 선택**을 클릭하여 1단계에서 다운로드한 JSON 에이전트 파일을 업로드합니다.
8. **저장**을 클릭합니다.
9. Google Apps API 페이지를 볼 수 없는 경우 필요한 권한이 없는 것일 수 있습니다. 다음 역할 권한 중 하나로 설정되어 있어야 합니다.
   - 시스템 관리
   - 시스템 읽기 전용

# 12.6.5. 관리 - Android Enterprise

**라이센스: Silver**

- Email+, Docs@Work, Web@Work와 같이 Android Enterprise를 활성화한 Ivanti, Inc 생산성 앱에는 골드 라이선스가 필요합니다.
- Tunnel for Android Enterprise에는 플래티넘 라이선스가 필요합니다.

Android Enterprise를 통해 Android Enterprise 앱을 사용하고 구성할 수 있습니다. Android Enterprise 사용자는 앱 카탈로그나 Google Play를 통해 앱을 확인하고 설치할 수 있습니다.

새 고객일 경우 앱 배포는 기본적으로 기기별로 설정되어 있습니다. 이 설정은 변경할 수 없습니다. 고객 업그레이드의 경우 사용자별 또는 기기별 앱 배포 중 선택할 수 있습니다. 또한 고객 업그레이드의 경우 기본적으로 사용자별 앱 배포가 선택되어 있습니다. 많은 사용자에게는 여러 기기가 있습니다. 사용자에게 여러 기기가 있을 경우 앱 배포가 기기별로 설정되어 있으면 각 기기에서 사용 가능한 다른 앱 세트를 만들 수 있습니다.

이 섹션에는 다음 주제가 포함됩니다.


- Android Enterprise 구성
- Android Enterprise 작업 프로필 구성


## Android Enterprise 구성

1. MDM용 Ivanti Neurons 포털에서 **관리자 > Google > Android Enterprise**를 클릭합니다.
2. 다음 옵션 중 하나를 선택합니다.
    - **관리형 Google Play 계정:** G Suite를 구독하지 않은 기업의 경우 이 방법을 활용하면 사용자는 개인 정보를 전송하지 않고도(Google에 이메일 주소 전송) Android Enterprise에 등록할 수 있습니다. MDM용 Ivanti Neurons는 Google을 통해 사용자를 자동으로 프로비저닝 및 관리합니다. 관리자 Google 계정으로 Android Enterprise를 승인하라는 메시지가 표시됩니다.
    - **관리형 Google 계정:** G Suite를 구독하는 기업의 경우 이 방법을 활용하면 사용자는 본인의 Google 계정으로 Android Enterprise에 등록할 수 있습니다. Android Enterprise에 등록하려면 사용자의 Google 계정이 필요합니다.

화면상의 지침에 따라 구성 절차를 완료합니다.

4. 자동 실행 방법:
    - UEM API 활성화 및 엔터프라이즈 자격 증명 생성.
    - 통합 소유자를 승인하여 Google에 등록. 개인 계정이 아니라 IT 부서 계정이어야 합니다.
    - 서비스 계정 JSON 클라이언트 ID를 끌어다 놓는 방법으로 자격 증명 설정.

그 외의 다른 방법:

    - 아래 섹션의 CLIENT ID를 참조하여 Google Admin에 추가하세요.
    - Google Admin의 MDM 토큰과 Google Cloud 콘솔의 서비스 계정을 확인합니다.
    - MDM용 Ivanti Neurons에서 MDM 토큰, Enterprise Google 도메인, Enterprise 관리자 이메일 주소를 입력하여 Google 서비스에 연결합니다.
    - MDM용 Ivanti Neurons에서 서비스 계정 JSON 클라이언트 ID를 끌어다 놓습니다.
    - MDM용 Ivanti Neurons에서 **승인**을 클릭하여 MDM용 Ivanti Neurons를 승인하고 Google 사용자를 확인 및/또는 관리합니다.

MDM용 Ivanti Neurons 사용자 인터페이스에서 이 단계를 안내합니다.

### MDM용 Ivanti Neurons와 관리형 Google 계정의 바인딩을 위한 클라이언트 ID

관리자 콘솔에서 클라이언트 ID를 **140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com**으로 추가하고 MDM용 Ivanti Neurons 테넌트와 관리형 Google 계정을 바인딩합니다.

## Android Enterprise 작업 프로필 구성

1. MDM용 Ivanti Neurons 포털에서 **구성**으로 이동합니다.
2. **+추가**를 클릭합니다.
3. **잠금 및 키오스크: Android Enterprise** 구성을 선택합니다.
4. 구성 이름 및 설명을 입력합니다.
5. **작업 프로필** 잠금 유형을 클릭합니다.
   대상 기기에 적용하려는 **잠금 설정**을 선택합니다.
   **중요:** 사용자가 설정에 있는 계정 추가를 사용하여 Google 계정을 추가하면 Google 인증 서버에서 해당 계정의 도메인이 UEM에서 관리되는 도메인으로 등록되었는지 확인합니다. **Android 기기에서 UEM 정책 적용**을 선택했는지 확인합니다. 표시되었다면 Go 클라이언트가 자동으로 설치되거나 업데이트된 다음(이미 기기에 설치되지 않았을 경우), 시작됩니다. 사용자가 등록 절차를 완료하면 사용자에게 작업 프로필을 생성하라는 메시지가 표시되고 Google 계정이 자동으로 작업 프로필에 마이그레이션됩니다.

# 12.7. ChromeOS 장치 작업

이 섹션에는 다음 주제가 포함됩니다.

- ChromeOS 및 MDM용 Ivanti Neurons
- ChromeOS 장치에 Android 앱 배포
- ChromeOS Blueprint 구성
- 기기 작업
- FAQ
- 평가를 위한 권장 단계

# 12.7.1. ChromeOS 및 MDM용 Ivanti Neurons

ChromeOS는 Google에서 만들고 배포하는 Linux 기반 운영 체제입니다. MDM용 Ivanti Neurons 에서는 Android, Windows, iOS 및 macOS에서 작동하는 장치를 지원합니다. 이 지원은 이제 ChromeOS 장치로도 확장되었습니다. MDM용 Ivanti Neurons 에서는 ChromeOS 장치 구성 및 관리를 위한 통합된 간단한 이동성 관리 솔루션을 제공합니다. Ivanti는 MDM용 Ivanti Neurons의 iOS, Android, Windows 및 Mac에서 사용할 수 있는 관리 워크플로와 유사한 ChromeOS 장치를 위한 통합되고 단순하며 기능이 풍부한 솔루션을 제공합니다. 관리자는 **관리자 > Google > ChromeOS 관리**에서 간단한 통합을 사용하여 Google Cloud(Google 관리 콘솔이라고도 함)와 MDM용 Ivanti Neurons에 간단히 연결할 수 있습니다.

## 필수 조건

1. 관리형 Google 관리 계정이 있어야 합니다.
2. LDAP 사용자 및 OU는 Google 관리 콘솔에서 가져와야 합니다. MDM용 Ivanti Neurons 에서는 LDAP 소스에서 가져온 OU만 지원합니다. 로컬 OU는 지원되지 않습니다.
3. 관리자는 조직 단위(사용자 그룹)를 MDM용 Ivanti Neurons에 동기화해야 합니다. 이는 LDAP 서버를 구성하고 조직 단위를 추가하여 수행할 수 있습니다.

## Google 승인

Google 관리 콘솔에서 사용할 수 있는 ChromeOS 장치는 MDM용 Ivanti Neurons에 직접 등록할 수 없습니다. 대신, 이 장치는 Google에 등록되고 이 장치에 대한 정보는 Google과 MDM용 Ivanti Neurons 간에 동기화됩니다. 관리자는 Google이 장치를 가져오고 앱 할당, 구성 등과 같은 기타 작업을 수행하도록 승인해야 합니다.

**절차**

1. **관리자 > Google > ChromeOS > 관리**로 이동합니다.
2. **Google 승인**을 클릭합니다.
3. 승인하려는 Google 관리 계정을 선택합니다.
4. **계속**을 클릭하여 필수 서비스를 제공하는 권한을 수락합니다.
   **ChromeOS가 성공적으로 설정**되었다는 확인 메시지가 화면에 나타납니다. 확인 아래에서 도메인 정보를 찾을 수도 있습니다.

## Google에서 ChromeOS 장치 동기화

관리자는 Google 관리 콘솔에서 ChromeOS 장치를 동기화해야 합니다. Google 관리 콘솔을 사용하여 처음으로 ChromeOS 장치에 액세스하는 경우 관리자는 ChromeOS 관리 페이지에서 지금 동기화 옵션을 사용하여 수동으로 장치를 동기화해야 합니다.

> 장치를 처음으로 수동으로 동기화한 후 후속 동기화는 매시간 자동으로 수행됩니다.

## MDM용 Ivanti Neurons와 Google 관리 콘솔 통합 삭제

통합을 삭제하면 Google 리소스에 액세스하기 위해 Google로부터 받은 OAuth 토큰이 취소됩니다. ChromeOS 기기, Blueprint 구성 및 앱 구성과 연결된 인벤토리, 등록 메타데이터가 삭제됩니다. Blueprint 구성과 업로드된 앱은 삭제되지 않습니다.

테넌트 등록이 삭제되지 않은 경우 문의하여 문제를 확인할 수 있습니다.

**절차**

1. **관리자 > Google > ChromeOS > 관리**로 이동합니다.

2. ChromeOS MDM용 Ivanti Neurons 등록 섹션에서 **삭제**를 클릭합니다.
   삭제 작업의 진행 여부를 나타내는 팝업이 화면에 나타나고 이 통합과 관련된 모든 장치가 삭제됩니다. **확인**을 선택합니다.

# 12.7.2. ChromeOS 장치에 Android 앱 배포

관리자는 앱 카탈로그에서 ChromeOS 장치로 Android 앱을 배포할 수 있습니다.

**필수 조건**

1. Android Enterprise를 구성해야 합니다. Android Enterprise 설정에 대한 자세한 내용은 **Android Enterprise 설정**을 참조하십시오.
2. Android 앱은 앱 카탈로그에 있어야 합니다.
3. Android 앱 및 ChromeOS Blueprint 구성을 배포하기 전에 ChromeOS 장치(Chromebook) 사용자가 사용자 그룹(조직 단위라고도 함)의 일부인지 확인합니다.

Android 앱이 확인되었으면, 다른 앱을 배포할 때 따르는 유사한 프로세스에 따라 앱을 배포해야 합니다. Android 앱을 배포할 때 앱을 배포할 사용자 그룹을 선택하고 장치에서 자동 설치를 수행해야 합니다.

> 기존 Android 앱 배포가 장치/장치 그룹 또는 사용자에게 배포되도록 설정된 경우 배포를 사용자 그룹을 기반으로 변경해야 합니다. 이는 앱이 이미 사용 중인 경우 기존 배포에 영향을 줄 수 있습니다. 이 작업은 완전히 새로운 앱에서 먼저 수행하는 것이 좋습니다.

> 설치 설정을 통해 관리자는 최종 자동 설치를 제어할 수 있고 ChromeOS 장치에 앱을 푸시하는 데 필요합니다. 사용자 그룹은 여기에서 선택해야 합니다.

# 12.7.3. ChromeOS 확장 앱 추가 및 배포

관리자는 앱 카탈로그에 ChromeOS 확장 앱을 추가하고 이러한 앱을 ChromeOS 장치에 배포할 수 있습니다.

**절차**

1. **앱** > **앱 카탈로그**로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. 목록에서 **ChromeOS**를 선택합니다. 화면에 **ChromeOS 앱 세부 정보 추가** 페이지가 표시됩니다.
4. 다음 세부 정보를 제공하십시오. **앱 이름** - ChromeOS 확장 앱의 이름, **확장 ID** - 이 정보는 Chrome 웹 스토어에서 얻을 수 있습니다.
5. **다음**을 클릭합니다. 화면에 **앱 구성** 페이지가 표시됩니다. 다음 기기 체크인 시 즉시 업데이트를 선택하거나 새 버전이 나왔을 때 자동으로 앱을 업데이트하도록 선택할 수 있습니다.
6. 앱 배포 옵션 중 하나를 선택하고 필요한 세부 정보를 입력합니다.

> ChromeOS 앱 배포는 LDAP 사용자 그룹에 대해서만 지원됩니다.

ChromeOS 확장 앱이 확인되었으면, 다른 앱을 배포할 때 따르는 유사한 절차에 따라 앱을 배포해야 합니다. ChromeOS 확장 앱을 배포할 때 앱을 배포할 사용자 그룹을 선택하고 장치에서 자동 설치를 수행해야 합니다.

> 설치 설정을 통해 관리자는 최종 자동 설치를 제어할 수 있고 ChromeOS 장치에 앱을 푸시하는 데 필요합니다. 사용자 그룹은 여기에서 선택해야 합니다.

ChromeOS 확장 앱에 대한 정보를 편집하거나 앱 카탈로그에서 ChromesOS 확장 앱을 삭제할 수 있습니다. 앱 카탈로그에서 다른 앱을 편집하거나 삭제할 때 따르는 과정과 유사한 절차를 따라야 합니다.

## ChromeOS 확장 앱 편집

1. **앱 > 앱 카탈로그 > 세부 정보**로 이동합니다.
2. **편집**을 클릭합니다. 필요한 사항을 변경하고 **저장**을 클릭합니다.

앱 삭제에 대한 자세한 내용은 앱 카탈로그에서 앱 삭제를 참조하십시오.

# 12.7.4. ChromeOS Blueprint 구성

ChromeOS Blueprint 구성에 있는 설정은 다음과 같습니다.

- 장치 설정
- 사용자 및 브라우저 설정
- 관리형 게스트 세션 설정

특정 사용자 그룹(조직 단위라고도 함)에 ChromeOS 구성을 적용할 수 있습니다. ChromeOS Blueprint 구성을 배포하려고 하면 사용자 그룹 섹션만 사용할 수 있고, 승인된 Google 관리 콘솔과도 연결된 모든 LDAP 사용자 그룹이 섹션 아래에 열거됩니다. 열거된 그룹에서 하나 이상을 선택하고 구성을 적용할 수 있습니다.

**절차**

1. **구성 > 추가**로 이동합니다.
2. OS 섹션에서 **Google ChromeOS**를 선택합니다. **ChromeOS Blueprint 구성** 탭이 화면에 나타납니다.
3. **ChromeOS Blueprint**를 클릭합니다. 화면에 **ChromeOS Blueprint 구성 만들기** 페이지가 표시됩니다.
4. **이름** 상자에 구성의 이름을 입력합니다.
5. 구성 설정에서 필요에 따라 장치 설정, 사용자 및 브라우저 설정, 관리형 게스트 세션 설정을 수정하고 "장치로 푸시" 버튼을 토글하여 수정된 설정을 적용할 수 있습니다.
6. **다음**을 클릭하세요.
7. 배포 옵션에 대해 **사용자 지정**을 선택합니다.

> LDAP 사용자 그룹만 구성을 배포하는 데 사용할 수 있습니다.

> 구성을 모든 사람에게 배포하는 경우, MDM용 Ivanti Neurons 및 Google 관리 콘솔에서 사용할 수 있는 LDAP 사용자 그룹에 대해서만 수행할 수 있습니다.

하나 이상의 그룹을 선택하고 **완료**를 클릭합니다.

> 배포된 설정이 배포되지 않은 경우 적용된 설정은 되돌릴 수 없습니다.

> ChromeOS Blueprint 구성에서 파일을 업로드할 수 있습니다.

# 12.7.5. 기기 작업

ChromeOS 장치에서는 다음 작업이 지원됩니다.

- **지우기** - 지우기 작업은 장치에서 모든 데이터를 삭제하고 장치는 공장 설정으로 재설정됩니다. 자세한 내용은 **장치 지우기**를 참조하십시오.
- **잠금** - 잠금 작업은 장치에서 추가 작업을 수행할 수 없도록 제한합니다. 자세한 내용은 **장치 잠금 설정하기**을 참조하십시오.
- **잠금 해제** - 잠금 해제 작업은 추가 사용을 위해 장치를 해제합니다. 자세한 내용은 **장치 잠금 해제하기**를 참조하십시오.

# 12.7.6. FAQ

이 섹션에는 MDM용 Ivanti Neurons에서 ChromeOS 장치를 사용할 때 있을 수 있는 몇 가지 일반 FAQ가 열거되었습니다.

- Chromebook 관리는 다른 OS와 어떻게 다른가요?
- Google은 현재 LDAP 사용자 그룹 기반 구성 배포만 허용하기 때문에, 관리자는 구성 또는 앱으로 작업할 때 배포가 LDAP 사용자 그룹을 기반으로 하는지 확인해야 합니다. ChromeOS 장치 관리에는 로컬 사용자 그룹 및 장치 그룹이 지원되지 않습니다.
  ChromeOS 장치를 관리하려면 Ivanti에 어떤 라이선스가 필요한가요?
- ChromeOS 장치에는 Chrome Enterprise 업그레이드 또는 Chrome Education 업그레이드 등의 라이선스가 있어야 합니다. 이는 하드웨어의 일부 또는 독립 실행형 라이선스로 리셀러로부터 구매할 수 있습니다. 자세한 내용은 Google 설명서를 참조하십시오. Chrome 장치 관리를 시작하려면 Ivanti에 보안 UEM(통합 엔드포인트 관리) 라이선스가 필요합니다.
  MTD(Mobile Threat Defense) 또는 유사한 솔루션을 사용할 수 있나요? MTD에 대한 별도의 라이선스가 필요한가요?
- 지금은 이 제품에서 해당 라이선스를 사용할 수 없습니다. 최신 제한 사항을 참조하십시오. 기능 변경에 대한 세부 정보는 FAQ 및 릴리스 발표를 통해 제공할 예정입니다.
  구성 및 앱 탭에 다른 장치의 경우와 달리 세부 정보가 없는데 왜 그런 걸까요?
- 구성은 사용자 그룹에 배포되고 로그인한 사용자를 기반으로 적용되지 않으므로 현재는 구성이 장치 세부 정보에 표시되지 않습니다. 앱은 동일한 배포 논리를 따르고 동일한 제한이 있습니다. 이 제한 사항의 변경에 대한 세부 정보는 FAQ 및 릴리스 발표를 통해 제공할 예정입니다.
  ChromeOS에는 현재 몇 가지 구성이 지원되나요?
- ChromeOS를 사용하여 사용 가능한 구성 타일 수를 줄이고 구성과 관련된 관리 작업을 줄였습니다. 이 구성을 "ChromeOS Blueprint"라고 합니다. ChromeOS Blueprint는 이 장치에서 700개에 가까운 구성을 지원합니다. 구성 옵션은 Google 문서를 참조하십시오.
  모든 장치에 대해 하나의 구성을 관리하기가 얼마나 쉬운가요?
- 관리자는 단순히 기존 구성을 복제하고 해당 사용자 그룹에 맞게 수정할 수 있습니다(필요한 경우). 처음부터 시작하지 않아도 됩니다.
  Chrome 장치에 VPN 구성을 추가하려면 어떻게 하나요?
- Android 앱을 통해 가능하고 기본 VPN은 없어도 됩니다.
  이 장치에서 사용 중지 및 지우기 등의 기능도 되나요?
- Enterprise의 Chromebook은 항상 조직에서 관리하며 이러한 장치의 데이터는 완전히 조직적인 것으로 간주됩니다. 유의할 사항:
  - 사용 중지 차단됨
  - 지우기 허용됨
  - 잠금 허용됨
  - 잠금 해제 허용됨
  - 기타 작업 – 지원되지 않음

Ivanti는 하드웨어 측면에서 어떤 Chromebook을 지원하나요?

- Google Cloud 장치 관리 솔루션에서 지원하는 장치는 기본으로 Ivanti에서 지원해야 합니다. Ivanti는 현재 Ivanti 솔루션에서 지원하는 특정 하드웨어 목록을 게시하지 않습니다.
  어떤 버전의 Chrome OS가 지원되나요?
- Google Cloud는 ChromeOS의 최신 안정 버전만 지원하고 Ivanti의 지원은 백엔드 통합의 특성상 Google에서 지원하는 모델을 따릅니다.
  이 기능의 첫 출시이므로 현재 당면한 제한 사항 목록은 무엇인가요?

새로운 Chrome OS 지원을 통해 고객이 간절히 바라는 기능을 제공하고자 노력하고 있습니다. 관리자가 주의해야 할 몇 가지 제한 사항은 다음과 같습니다.

- Chrome OS 확장 프로그램(브라우저 앱)은 현재 배포용("앱")이 지원되지 않습니다.

- Android 앱용 관리형 앱 구성은 현재 지원되지 않습니다.
- Wi-Fi 구성 API는 최근 출시되었고 현재 지원되지 않습니다.
- 인증서 배포는 현재 지원되지 않습니다.
- Ivanti Go(구 MobileIron Go) Android 앱 배포는 현재 지원되지 않습니다.
- Ivanti Tunnel(VPN) 앱은 현재 지원되지 않습니다.
- 공간 및 공간 위임은 현재 지원되지 않습니다.
- 모바일 위협 방어 솔루션은 현재 지원되지 않습니다.
- 이 장치에서는 비관리형 장치로 분류되는 Ivanti의 Zero Sign-On 솔루션이 지원됩니다.
- 정책 작업은 완전히 지원되지 않습니다.

# 12.7.7. 평가를 위한 권장 단계

솔루션의 유효성을 확인하려면 다음 단계를 수행하는 것이 좋습니다.

1. 디렉터리 소스(예: Active Directory)에 테스트 사용자가 있는 별도의 OU(사용자 그룹)를 만듭니다. 이렇게 하면 활성 조직 단위에 미치는 영향을 방지할 수 있습니다.
2. Ivanti, Google 및 디렉터리 소스(LDAP) 간에 사용자를 동기화합니다. 사용자 그룹에서 "테스트 OU"를 사용할 수 있는지 확인합니다.
3. 위의 단계에서 강조 표시된 대로 MDM용 Ivanti Neurons를 Google과 통합합니다.
4. ChromeOS Blueprint 구성을 생성하고 "테스트 OU" 사용자 그룹에만 배포합니다.
5. Chromebook을 부팅합니다(기본 제공 또는 이전에 등록됨). 장치 목록에서 사용할 수 있는지 확인합니다.
6. 장치에서 ChromeOS Blueprint 설정을 사용할 수 있는지 확인합니다.
7. Android 앱 배포와 유사한 단계를 따릅니다.

# 12.8. 펌웨어 관리

이 섹션에는 다음 주제가 포함됩니다.

- Zebra OTA 서비스에 등록
- 삼성 E-FOTA 라이선스 관리(지원 중단)

# 12.8.1. Zebra OTA 서비스에 등록

Zebra OTA(무선) 서비스에 등록하면 Zebra OTA 구성을 활성화하여 MDM용 Ivanti Neurons에 등록된 Zebra 기기의 펌웨어 세부 정보를 수신 및 업데이트할 수 있습니다.

**절차**

1. **관리자 > 인프라 > Zebra OTA**로 이동합니다. **Zebra OTA 서비스** 페이지가 표시됩니다.
2. **Zebra의 OTA 서비스 링크** 아래에서 **시작**을 클릭합니다.
3. Zebra OTA 자격 증명을 입력하여 로그인한 후 Zebra 서비스 이용을 위한 승인 요청 단계를 수행합니다.
4. **확인 완료**를 클릭하여 Zebra 서비스 연결에 대한 확인을 받습니다. 연결이 확인되면 Zebra OTA 서비스 페이지에 등록 성공 상태가 표시됩니다.

등록을 취소하려면 **작업** 열 아래에서 **취소**를 클릭하세요. **취소** 작업은 기존 구성에서 모든 Zebra OTA 구성을 제거합니다. Zebra OTA로 다시 등록하려면, **새로 고침**을 클릭합니다. 새로 고침 작업은 기존 구성에는 아무런 영향을 주지 않습니다.

등록 후, 기기 소유자 모드에서 Go 클라이언트가 수신하여 Zebra 기기(Android 버전 8.0 또는 지원되는 최신 버전)에 적용하는 Zebra 펌웨어 구성을 활성화할 수 있습니다. 구성이 적용되면 펌웨어가 다운로드되어 구성에서 예약한 대로 기기에 설치됩니다. Zebra 펌웨어 구성 활성화에 대한 자세한 내용은 시스템 업데이트 구성을 참조하십시오.

펌웨어 업데이트를 완료하면 기기 페이지의 **시스템 업데이트** 열에서 Zebra 기기의 펌웨어 업데이트 상태를 확인할 수 있습니다. 다음은 나타날 수 있는 상태입니다.

- **알 수 없음** - 클라이언트 또는 OS에서 지원하지 않음
- **최신** - 기기에 사용할 수 있는 최신 업데이트가 있음
- **보류 중** - 시스템 업데이트 구성이 적용되었으나 업데이트가 다운로드 또는 적용되지 않았음
- **다운로드 중** - 시스템 업데이트가 클라이언트에 다운로드되는 중
- **사용 가능** - 현재 시스템 업데이트를 기기에 사용할 수 있음
- **오류** - 다운로드 또는 설치 시 오류

기기 페이지의 **Zebra 패치 버전** 열에는 기기의 Zebra 패치 정보가 표시됩니다.

> **Zebra 패치 버전**은 Android 11 이상의 장치에서 지원되지 않습니다. **Zebra 전체 업그레이드**만 지원됩니다.

# 12.8.2. 삼성 E-FOTA 라이선스 관리(지원 중단)

삼성 E-FOTA 서비스는 2022년 7월부터 지원이 중단됩니다. 자세한 내용은 삼성 발표 사항을 참조하십시오.

> 이제 삼성 E-FOTA 서비스를 구성할 수 없습니다. 하지만 기존 E-FOTA 구성이 있을 경우 **관리** > **펌웨어 관리** > **삼성 E-FOTA**으로 이동하여 **비활성화** 옵션을 클릭하면 구성을 비활성화할 수 있습니다.

# 12.9. 스크립트 및 파일 관리

관리자는 구성에 사용하고 기기로 푸시할 수 있는 스크립트 및 파일을 관리할 수 있습니다.

이 섹션에는 다음 주제가 포함됩니다.

모든 스크립트

파일

# 12.9.1. 모든 스크립트

**적용 대상:** macOS 및 Windows 기기

**관리 > 스크립트 및 파일 > 모든 스크립트** 페이지의 MDM용 Ivanti Neurons에서는 시스템 관리 역할을 가진 사용자가 구성에서 사용할 수 있는 스크립트를 생성, 업로드, 관리하고 기기에 배포할 수 있습니다. 사용자 지정 속성을 스크립트와 연결하고 결과 값을 구성한 기기에 할당할 수 있습니다. 감사 내역을 사용하여 스크립트 변경 로그를 확인하고, 장치 세부 사항 페이지에서 실행 결과를 확인할 수 있습니다.

기기 설정을 구성하는 스크립트를 쓸 수 있습니다. 예를 들어 다음 스크립트를 실행할 수 있습니다.

- 기기 사용자가 매월 비밀번호를 강제로 변경하도록 하거나
- 유휴 시간 5분이 지나면 화면을 잠그거나 또는
- 보안 Wi-Fi 네트워크를 구성하는 스크립트

이 섹션에는 다음 주제가 포함됩니다.


- 스크립트 추가하기
- 스크립트 수정
- 스크립트 변수 사용(Windows 및 macOS에 적용 가능)
- 스크립트 테스트
- 스크립트 실행 결과 확인


## 스크립트 추가하기

bash 스크립트(macOS용) 및 ps1 스크립트(Windows용)의 저장소를 생성하거나 업로드할 수 있습니다. 이 저장소는 구성에서 스크립트를 선택하고 구성에 지정된 일정에 따라 장치에서 실행되도록 배포하는 데 사용할 수 있습니다.

예를 들어 기기에 실행할 쉘 스크립트를 작성할 수 있습니다. 필요할 경우 래퍼를 사용할 수 있습니다. 쉘 스크립트 내에서부터 바이너리 파일을 실행하는 것은 지원되지 않습니다.

> 쉘 스크립트를 해당 기기에서 실행하기 전 먼저 테스트하여 견고성 및 품질을 확인하는 것이 좋습니다. 스크립트를 로컬로 실행하고 결과로 나타나는 오류를 수정하십시오.

**절차**

1. **관리 > 스크립트 > 모든 스크립트**로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. 스크립트의 이름과 설명을 입력합니다.
4. 플랫폼 유형에서 macOS 또는 Windows를 선택합니다.
5. 다음 **스크립트 유형** 중 하나를 선택합니다.
   - **bash**
   - **zsh**
   - **python**
   - **swift**
   - **ps1**
6. **루트로 실행** 체크박스를 선택하여 기기에서 스크립트를 루트로 실행합니다. 기본적으로 이 옵션은 해제되어 있습니다.

7. **스크립트 편집기**에서 텍스트 상자에 스크립트를 입력하고 끌어다 놓거나 복사하여 붙여넣을 수 있습니다.
8. 또는, **스크립트에서 코드 가져오기**를 클릭하여 기존 스크립트 파일을 끌어다 놓거나 파일 선택을 클릭하여 MDM용 Ivanti Neurons로 업로드할 스크립트 파일을 찾아 선택합니다. 스크립트 편집기의 기존 스크립트가 대체됩니다. 이 작업은 실행 취소할 수 없습니다. **가져오기**를 클릭합니다. 업로드한 스크립트의 코드가 스크립트 편집기에 표시됩니다.
9. (선택 사항) **사용 가능한 사용자 지정 속성** 섹션에서 스크립트와 연결할 표시된 기기 사용자 지정 속성을 하나 이상 선택합니다. 선택한 속성을 사용해 구성한 기기의 기기 사용자 지정 속성에 결과 스크립트 실행 값을 할당할 수 있습니다. **사용자 지정 속성의 샘플 코드**를 클릭하여 스크립트의 사용자 지정 속성을 사용해 샘플 코드를 봅니다.
10. **저장**을 클릭하세요.

스크립트의 사용자 지정 속성 이름은 소문자이어야 합니다. 사용자 지정 속성이 다른 스크립트에 참조될 경우 속성을 제거할 수 없습니다. 사용자 지정 속성(예: 사용자 지정 속성의 이름)을 수정하고 수정한 이름을 스크립트와 연결할 경우 연결 스크립트에 해당 사항을 변경해야 합니다.

## 스크립트 수정

스크립트를 편집하거나 제거하려면 다음을 수행합니다.

1. **관리 > 스크립트 > 모든 스크립트**로 이동합니다.
2. 스크립트의 **작업** 열 아래에서 편집 또는 삭제 작업에 해당하는 아이콘을 클릭합니다.
3. 화면의 지침에 따라 작업을 완료합니다.

스크립트(콘텐츠, 이름, 설명)이 변경되면 스크립트와 연결된 모든 구성이 기기에 다시 배포됩니다.

## 스크립트 변수 사용(Windows 및 macOS에 적용 가능)

환경 및 대체 변수와 같은 스크립트 입력 사항을 정의하고 스크립트 리포지토리에 저장합니다. macOS용 Mobile@Work 스크립트 구성 또는 Windows용 Ivanti Bridge 스크립트 및 작업 구성에서는 연결된 스크립트에 따라 관련 스크립트 변수를 필요 시 사용할 수 있습니다. macOS의 경우, 이 기능을 사용하려면 **macOS용 Mobile@Work** 1.71.0부터 MDM용 Ivanti Neurons에서 지원하는 최신 릴리스 버전까지의 범위에 해당해야 합니다. Windows의 경우, 이 기능을 사용하려면 **Ivanti Bridge**가 필요합니다.

변수를 사용하여 실행할 때마다 다른 값의 스크립트로 실행합니다. 예를 들어 관리자는 스크립트를 생성하여 스크립트 변수로 $ 환경 변수를 사용하고 이를 macOS용 Mobile@Work 스크립트 또는 Windows 구성과 연결할 수 있습니다. 구성이 배포되고 각 사용자 기기에 설치되면, MDM용 Ivanti Neurons에서 각 기기가 특정 조치를 취할 수 있도록 서로 다른 등록 사용자 이메일 주소를 전송합니다. MDM용 Ivanti Neurons 관리 포털은 사용자 지정 변수를 지원합니다.

스크립트 변수 추가 방법:

1. **관리 > 스크립트 > 모든 스크립트**로 이동합니다.
2. 스크립트 입력 섹션에서 **+추가**를 클릭합니다.
3. 스크립트 입력 추가 - 환경 변수 팝업 페이지에서, 다음과 같은 세부 사항을 입력합니다.
    - 표시할 레이블 - 이 텍스트는 macOS용 Mobile@Work 스크립트 구성 페이지에 레이블로 표시됩니다. 예를 들어 OS 폴더 입력, Apache 번호 입력 등입니다.
    - 환경 변수 이름 - 예를 들어 JAVA_HOME, OS_VERSION 등입니다. MDM용 Ivanti Neurons 는 값이 데이터베이스에서 지속되면서 구성 세부 사항을 대상 기기로 보내는 한편 스크립트 변수에 대한 값을 대체합니다.
    - 환경 변수 기본 값 - 예를 들어 1024, bin/java, $ 등입니다. 입력 변수는 관리자가 업로드하거나 편집한 스크립트에서 사용됩니다. 다음 참고 사항도 확인하십시오.

미리 보기 영역에서 환경 변수 값이 구성 페이지에서 어떻게 스크립트 입력으로 표시되는지 검토합니다.

5. **저장**을 클릭하세요.

이러한 방법으로 구성에는 레이블과 기본 값만 사용할 수 있으며 추상적 개념의 레이어를 제공하는 환경 변수 이름은 사용할 수 없습니다.

- 영숫자 값(예: 1024, bin/java, root@localhost) 또는 시스템 속성(예: $)은 환경 변수 값으로 허용 가능합니다.
- 환경 변수 값은 구성 페이지에서 배포 중에 수정 또는 삭제될 수 있습니다.
- 환경 변수 값이 제공되지 않을 경우 스크립트 배포 중 값이 제공되는지 확인하십시오. 그렇지 않으면 빈 값이 스크립트에 전달됩니다.
- 스크립트 구성이 배포되어 기기에 설치된 이후에는**관리 > 스크립트 및 파일 > 모든 스크립트** 페이지에서 환경 변수를 편집하더라도 해당 스크립트와 연결된 기존 구성에는 영향을 주지 않습니다. **macOS용 Mobile@Work 스크립트 구성**도 참조하십시오. Windows에 대한 자세한 내용은 **Windows용 Ivanti Bridge 스크립트 및 작업 구성**을 참조하십시오.

### 스크립트 변수 편집

스크립트 변수를 편집하려면 변수에 대고 편집(연필) 아이콘을 클릭하여 변경 사항을 저장합니다.

스크립트 구성이 스크립트 변수를 가진 스크립트를 가리킬 경우 기존 스크립트 변수의 레이블을 편집하면 스크립트 구성에서도 반영이 됩니다. 그러나,

- 스크립트 변수 기본 값의 변경은 기존 구성에 반영되지 않습니다.
- 스크립트 변수 기본 값의 변경은 선행 스크립트로 생성된 모든 새 구성에 반영됩니다.

### 스크립트 변수 삭제

스크립트 변수를 삭제하려면 변수에 삭제(마이너스) 아이콘을 클릭하고 확인합니다.

새로 생성된 스크립트 변수, 또는 기존 스크립트 변수의 삭제는 기존 구성에서도 반영됩니다.

## 스크립트 테스트

스크립트를 저장할 필요 없이 기기에서 테스트하기 전에 먼저 신속하게 디버그 툴에서 테스트를 실행합니다.

필수 조건

- macOS의 경우, 이 기능을 사용하려면 **macOS용 Mobile@Work** 1.67부터 MDM용 Ivanti Neurons에서 지원하는 최신 버전까지의 범위에 해당해야 합니다.
- Windows의 경우, 이 기능을 사용하려면 **Windows용 Ivanti Bridge 스크립트 및 작업 구성**이 필요합니다.

**절차**

1. **관리 > 스크립트 > 모든 스크립트**로 이동합니다.
2. 스크립트 편집기에서 스크립트를 추가하거나 가져옵니다.
3. 테넌트에 여러 공간이 있을 경우, 공간을 선택합니다.
4. 스크립트 테스트 섹션에서 플랫폼으로 **macOS** 또는 **Windows**를 선택합니다.
5. **기기 찾기** 텍스트 필드에서, 스크립트를 테스트할 수 있는 기기를 찾아 선택합니다. 기기는 일련 번호, 사용자 이름, 기기 이름 및 OS 버전으로 검색할 수 있습니다.
6. **지금 테스트**를 클릭합니다. 이 방법을 사용하면 환경 변수를 추가, 편집 및 삭제할 수 있으며, (변경 사항을 저장하지 않고도) 해당 상태로 스크립트를 테스트할 수 있습니다. **Windows** 스크립트의 경우, 스크립트 실행이 시작된다는 팝업 창이 화면에 나타나고, 일정 시간이 지난 후 장치 세부 사항 로그 탭에서 실행 상태를 확인할 수 있습니다.
7. **저장**을 클릭하세요.
8. macOS의 경우, 스크립트가 기기에 푸시되어 실행될 때까지 기다립니다.

9. 스크립트 입력(환경 변수 세부 사항 포함), 스크립트 출력 및 사용자 지정 속성 섹션에서 게시된 테스트 결과를 검토합니다. 환경 변수의 기본값 또한 표시됩니다.

## 스크립트 실행 결과 확인

스크립트 실행 결과 로그를 보려면 다음을 수행합니다.

1. **기기**로 이동합니다.
2. 기기 이름을 클릭합니다.
3. **로그** 탭을 클릭합니다.
4. 스크립트 실행 작업을 표시하는 열에서 확인할 수 있는 정보는 다음과 같습니다.
    - 세부 정보 열의 스크립트 이름
    - 상태 열의 스크립트 실행 상태
    - 날짜 열의 스크립트 실행 날짜 및 시간
    - 작업 열 아래의 눈 모양 아이콘 클릭 시 스크립트 실행 로그(기기 로그 plist)

필터를 사용하여 **스크립트 실행** 행을 표시합니다. 해당 행의 로그에는 스크립트의 표준 출력 및 표준 오류에 대한 출력(plist)이 포함되어 있습니다.

6. 필터를 사용하여 **스크립트 실행 결과 처리** 행을 표시합니다. 해당 행의 로그에는 결과 처리에 대한 세부 정보(plist)가 포함되어 있습니다.
    - 스크립트에 연결된 사용자 지정 속성이 없을 경우 처리할 결과가 없게 됩니다. 이러한 스크립트는 필터링된 열의 목록에 표시되지 않습니다.
    - 스크립트에 연결된 사용자 지정 속성이 있고 해당 속성이 예상 형식일 경우 결과의 사용자 지정 속성이 매핑되며 상태가 성공으로 표시됩니다. 매핑된 사용자 지정 속성과 해당 값은 **속성** 탭에서 확인할 수 있습니다.
    - 스크립트에 연결된 사용자 지정 속성이 있지만 해당 속성이 예상 형식일 아닐 경우 결과의 사용자 지정 속성이 매핑되지 않으며 상태가 오류로 표시됩니다.
    - 결과 형식이 올바르지만 연결된 사용자 지정 속성이 모두 결과에 전송되지 않을 경우 상태가 오류로 표시됩니다.
    - 스크립트와 함께 스크립트 변수가 전송될 경우 스크립트 실행 결과 처리 로그에 스크립트 변수에 대한 세부 사항(plist)이 포함됩니다.

**관련 주제:**

- macOS 스크립트용 Mobile@Work 구성
- 구성을 생성하는 방법
- Windows용 Ivanti Bridge 스크립트 및 작업 구성

# 12.9.2. 파일

**적용 가능 대상:** macOS 기기

MDM용 Ivanti Neurons에서는 시스템 관리 역할을 가진 사용자가 기기를 구성하고 기기에 배포하는 데 사용되는 파일을 생성하거나 업로드하고 관리할 수 있도록 합니다.

**절차**

1. **관리** > **스크립트 및 파일** > **파일**로 이동합니다.
2. **파일** 페이지에서 **+ 추가**를 클릭합니다.
3. **파일 생성** 창에서 다음 세부 정보를 입력합니다:
    1. **이름** 필드에 파일 식별할 수 이름을 입력합니다.
    2. **설명** 필드에 이 파일의 목적을 명확히 설명하는 내용을 입력합니다.
    3. **파일 업로드** 창에서 **파일 선택**을 클릭하여 .zip 파일을 업로드합니다. 또는 기기에서 파일을 끌어다 놓을 수도 있습니다.
4. **저장**을 클릭하세요.
   새로 추가된 파일은 **파일** 페이지에 표시됩니다.

## 파일 편집하기

1. **관리** > **스크립트 및 파일** > **파일**로 이동합니다.
2. 편집하려는 파일을 선택하고 **편집**을 클릭합니다.
   **파일 편집** 창이 표시됩니다.
3. (선택 사항) **이름** 및 **설명** 필드를 편집할 수 있습니다.
4. **파일 업로드** 창에서 **다른 파일 선택**을 클릭하여 .zip 파일을 업로드합니다. 또는 기기에서 파일을 끌어다 놓을 수도 있습니다.
5. **업데이트**를 클릭합니다.

## 파일 삭제하기

기존 **파일**을 삭제하려면 **관리** > **스크립트 및 파일** > **파일**로 이동하여 삭제하려는 파일을 모두 선택한 후 **+ 삭제**를 클릭합니다.

**파일**이 구성과 연결된 경우, MDM용 Ivanti Neurons에 **"다른 정책에서 사용 중이므로 파일을 삭제할 수 없습니다."**라는 **경고** 메시지를 표시합니다.

# 12.10. 브랜딩

이 섹션에는 다음 주제가 포함됩니다.

- 관리 > Apple 앱 카탈로그(브랜딩)
- Android App Catalog 브랜딩
- 관리 > Android 키오스크 브랜딩
- 이메일 템플릿 브랜딩
- 셀프 서비스 포털
- 셀프 서비스 포털(브랜딩)
- 다중 사용자 로그인(웹 클립) 브랜딩
- 조직

# 12.10.1. 관리 > Apple 앱 카탈로그(브랜딩)

**라이센스:** Gold

Apple {{App Catalog}}를 브랜딩할 수 있어 iPhone, iPad, Mac 기기의 최종 사용자에게 더 친근한 카탈로그를 제작할 수 있습니다. Apple 앱 카탈로그에서 사용자 지정할 수 있는 항목은 다음과 같습니다.

- 앱 아이콘(PNG, 360px 정방형)
- 앱 이름
- 앱 배너 이미지(PNG, 360x64)
- 텍스트 색상

> Apple App Catalog에 액세스할 수 있는 모드는 표준 App Catalog 및 통합 App Catalog 두 가지입니다. 독립 실행형 App Catalog는 iPhone, iPad 및 Mac 기기에서 사용 가능합니다. 통합 앱 카탈로그는 iOS 및 Mac 기기에서 사용 가능합니다.

## Apple 앱 카탈로그 브랜딩

이 페이지의 변경 사항은 홈 화면, 시작 화면, 그리고 앱 홈 화면에 영향을 미칩니다. 독립 실행형 App Catalog와 통합 App Catalog 둘 모두에 대해 절차는 유사합니다.

**절차**

1. **Apple App Catalog 브랜딩** 페이지에서 **사용자 지정**(우측 상단)을 클릭합니다.
2. **앱 아이콘** 섹션에서 로고 파일을 점선 박스에 끌어 놓거나 **파일 선택**을 클릭하여 파일 시스템에서 선택합니다. 앱 아이콘이 iOS 홈 화면에 표시됩니다.
3. **앱 이름** 섹션에서 **App Catalog 이름** 텍스트를 편집하여 시작 화면에 표시된 라벨을 변경합니다.
4. 홈 화면 배너에 이름 및 아이콘이 적용됩니다. 사용자 지정 배너 이미지를 변경하려면 **홈 화면 배너에 이름 및 아이콘 적용** 옵션을 선택 해제합니다. **앱 배너 이미지** 섹션이 표시됩니다.
5. 앱 배너 이미지를 변경하려면 새 배너 이미지 파일을 점선 박스로 끌어다 놓거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다. 앱 홈 화면 상단 표시줄에 앱 배너 이미지가 나타납니다.
6. **텍스트 색상** 섹션에서 16진수 색상 코드 상자란을 클릭하여 색상을 선택하거나 16진수 색상 코드를 입력합니다. 이는 시작 화면의 텍스트, 앱 이름, 배너 및 작업 버튼에 적용됩니다.
7. **변경사항 저장**을 클릭하세요.

입력한 App Catalog 이름은 Android, iOS, macOS에 적용됩니다.

# 12.10.2. Android App Catalog 브랜딩

**라이센스:** Gold

Android {{App Catalog}}를 브랜딩하여 최종 사용자에게 더 친근한 카탈로그를 제작할 수 있습니다. Android 앱 카탈로그에서 다음 항목을 맞춤 설정할 수 있습니다.

- 카탈로그 로고(PNG, 360x64)
- 카탈로그 이름
- 작업 표시줄 색상
- 바로가기 아이콘
- 바로가기 이름

## Android 앱 카탈로그 브랜딩

**절차**

1. **Android App Catalog 브랜딩**화면에서 **사용자 설정**(우측 상단)을 클릭합니다.
2. 앱 카탈로그 로고를 변경하려면 로고 파일을 점선 박스에 끌어 놓거나 **파일 선택**을 클릭하여 파일 시스템에서 선택합니다.
3. **작업 표시줄 색상** 필드를 클릭하여 색상표가 나타나면 원하는 색상을 선택하거나 원하는 색상에 해당하는 16진수 숫자를 입력합니다.
4. **앱 카탈로그 이름**을 수정해 카탈로그 레이블을 변경하세요.
5. 입력한 App Catalog 이름은 Android, iOS, macOS에 적용됩니다.
   바로가기 아이콘을 변경하려면 아이콘 파일을 점선 박스에 끌어 놓거나 **파일 선택**을 클릭하여 파일 시스템에서 선택합니다.
6. **바로가기 이름** 텍스트를 편집하여 앱 바로가기 레이블을 변경합니다.
7. **변경사항 저장**을 클릭하세요.

# 12.10.3. 관리 > Android 키오스크 브랜딩

라이센스: Silver

Android 키오스크 브랜딩을 통해 사용자들에게 더 친근한 카탈로그를 제공할 수 있습니다. 다음과 같은 항목의 사용자 설정이 가능합니다.

- 배너 로고(PNG, 840x114) 또는 텍스트
- 배너 테두리 색
- 배너 배경색
- 화면 배경색
- 화면 배경 이미지(1280x800)
- 화면 배경 형식

## Android 키오스크 화면 브랜딩

**절차**

1. **관리 > Android 키오스크**를 탐색하세요.
2. **키오스크 모드 브랜딩** 페이지에서 **브랜딩 생성**을 클릭합니다.
3. **이름** 필드에서, 키오스크 모드 브랜딩의 이름을 입력하세요.
4. 배너를 끄려면, **상단 배너 설정**을 선택 해제하세요.
5. **배너 배경색** 필드를 클릭하여 색상표가 나타나면 원하는 색상을 선택하거나 원하는 색상에 해당하는 16진수 숫자를 입력합니다.
6. **배너 테두리 색** 필드를 클릭하여 색상표가 나타나면 원하는 색상을 선택하거나 원하는 색상에 해당하는 16진수 숫자를 입력합니다.
7. **이미지/로고** 또는 **텍스트**를 선택해 배너 내용을 설정하세요.
8. **이미지/로고**를 선택한 경우 이미지 파일을 끌어다 놓거나 **파일 선택**을 클릭하여 이미지 파일을 선택합니다.
9. **텍스트**를 선택한 경우, 배너에 표시할 문구를 입력합니다.
10. **배경** 탭을 클릭하세요.
11. **배경색** 필드를 클릭하여 색상표가 나타나면 원하는 색상을 선택하거나 원하는 색상에 해당하는 16진수 숫자를 입력합니다.
12. 배경 이미지 변경 방법
13. a. 기본 이미지를 삭제합니다.
    b. 원하는 이미지를 드래그하거나 **파일 선택**을 클릭해 파일을 선택합니다.
    c. 선호하는 레이아웃을 선택합니다.
    **변경사항 저장**을 클릭하세요.
    **키오스크 모드 브랜딩** 페이지에 생성된 키오스크 모드 브랜딩이 표시됩니다. 사용자 지정 브랜딩을 추가로 편집하려면 **작업** 열의 편집 아이콘을 클릭하세요. 사용자 지정 브랜딩을 삭제하려면 삭제 아이콘을 클릭합니다. 사용자 지정 키오스크 브랜딩을 삭제하면 브랜딩을 사용하는 구성이 기본 브랜딩으로 되돌아갑니다.

# 12.10.4. 이메일 템플릿 브랜딩

최종 사용자 이메일 초대 브랜딩을 통해 최종 사용자에게 더 친근한 카탈로그를 제공할 수 있습니다. **기본값 설정으로 되돌리기**를 클릭하여 사용자 지정 사항을 삭제합니다.

지원되는 모든 언어로 다음의 이메일 템플릿을 사용자 지정할 수 있습니다.

- **최종 사용자 초대** - 앱과 구성에 액세스할 수 있도록 기기를 연결하라는 초대를 사용자에게 보냅니다.
- **비밀번호 재설정 알림** - 시스템에서 로컬 계정의 비밀번호가 만료되기 7일 및 24시간 전에 알림 이메일을 보냅니다. 이 옵션은 LDAP 계정에 적용되지 않습니다.
- **등록 확인** - 사용자가 등록을 완료한 후 발송하는 이메일입니다. 이를 사용하여 등록하고 더 많은 학습 리소스로 안내해준 사용자에게 감사를 표할 수 있습니다.
- **정책 규정 준수 알림** - 기기가 규정을 준수하지 않을 때 발송하는 이메일입니다.

이 섹션에는 다음 주제가 포함됩니다.


- 이메일 템플릿 미리보기 및 테스트
- 메시지 헤더 맞춤형 수정
- 이메일 템플릿 사용자 정의하기
- 지원되는 메일 변수


## 이메일 템플릿 미리보기 및 테스트

이메일 템플릿을 미리 확인하고 테스트할 수 있습니다. 이메일 템플릿 테스트에서는 지정한 이메일 주소로 템플릿을 사용한 이메일을 보낼 수 있습니다.

이메일 템플릿 미리보기 및 테스트

1. **관리**를 클릭합니다.
2. 이메일 템플릿에서 **최종 사용자 초대**, **비밀번호 재설정 알림**, **등록 확인** 또는 **정책 규정 준수 알림**을 클릭합니다.
3. 미리 보기와 테스트를 수행할 대상 이메일 템플릿과 연결된 **미리 보기 및 테스트** 링크를 클릭합니다.
4. 렌더링된 템플릿 창에서 렌더링된 템플릿을 봅니다.
5. 테스트 이메일을 전송할 테스트 이메일 주소를 지정합니다.
   지정한 이메일 주소가 현재 사용자에 속한다면 테스트 이메일이 이메일 템플릿 변수 값 대부분을 대체하여 이메일의 매우 정확한 사용자 환경을 제공합니다. 그러나 테스트 이메일은 실제 이메일 초대 생성 시 MDM용 Ivanti Neurons가 생성하는 변수 값을 대체하지 않습니다.
6. **테스트 이메일 전송**을 클릭합니다.

## 메시지 헤더 맞춤형 수정

1. **관리**를 클릭합니다.
2. **이메일 템플릿**을 클릭합니다.
3. 편집할 이메일 템플릿에 연결된 **편집**아이콘 링크(작업 열 아래)를 클릭합니다.
4. **이메일 표시 이름**, **발송 이메일 주소**, **회신 이메일 주소**, **SMTP 이메일 구성 설정**에 원하는 대로 신규 설정을 입력합니다.
5. 보낸 사람 및 받는 사람 이메일 주소를 사용자 지정하는 경우 이메일 릴레이 서비스를 허용 목록으로 설정하여 이메일 스팸 필터링 서비스에서 사용자의 이메일을 차단하지 않도록 하는 것이 좋습니다. 자세한 내용은 이 문서를 참조하십시오.
   **저장**을 클릭하세요.

6. 이메일 템플릿을 검토하고 미리 본 후 **저장**을 클릭합니다.

## SMTP 구성 사용

관리자가 아웃바운드 알림에 이용할 자체 이메일 서버 통합을 구성할 수 있도록 **SMTP 이메일 구성 설정**이 추가되었습니다.

1. **관리 > 브랜딩 > 이메일 설정**으로 이동하여 **SMTP 이메일 구성 설정** 옵션을 활성화하십시오.
2. 다음 필드를 업데이트합니다.
   - SMTP 서버
   - SMTP 서버 포트
   - 프로토콜
   - 사용자 이름
   - 비밀번호
3. **테스트**를 클릭하여 테스트 메일을 보내면 **테스트 이메일** 팝업 화면이 표시됩니다.
4. **수신자** 이름과 메시지 **본문**을 입력하고 **저장**을 클릭합니다.

> 자격 증명이 올바르지 않으면 오류 메시지가 표시됩니다.

5. **저장**을 클릭합니다.

다음 표에 SMTP 구성 창의 필드와 설명이 요약되어 있습니다.

| 필드 | 설명 |
| --- | --- |
| SMTP 서버 | MDM 서버용 Ivanti Neurons가 사용할 SMTP 서버의 IP 주소 또는 정규화된 호스트 이름을 지정합니다. |
| SMTP 서버 포트 | SMTP 서버에 구성된 포트를 지정합니다. |
| 프로토콜 | 구성 중인 SMTP 서버가 보안 서버인 경우, 즉 SMTPS 프로토콜을 사용하는 경우 SMTPS 버튼을 선택하십시오. 그렇지 않으면 SMTP가 선택된 상태로 둡니다. |
| 사용자 이름 | SMTP 인증에 필요한 사용자 이름을 입력하십시오. |
| 비밀번호 | SMTP 인증에 필요한 비밀번호를 입력하십시오. |

## 이메일 템플릿 사용자 정의하기

1. **관리 > 브랜딩 > 이메일 템플릿**을 선택합니다.
2. 편집할 템플릿, **최종 사용자 초대**, **비밀번호 재설정 알림**, **등록 확인** 또는 **정책 규정 준수 알림**을 선택합니다.
3. 수정하려는 메일 템플릿 옆에 있는 펜 아이콘을 클릭합니다.



4. 필요 시 제목을 수정합니다.
5. 본문 창에서 HTML 요소를 포함한 이메일 템플릿을 수정하여 메시지 내용을 사용자 정의합니다.

메일 본문 우측에 표시된 변수도 사용할 수 있습니다. 지원되는 메일 변수를 참고하십시오.

6. **미리 보기**를 클릭하여 이메일 템플릿을 미리 확인하면서 만족스러운 정도까지 템플릿을 반복 생성합니다.
7. 템플릿을 저장하려면 **미리 보기**를 클릭합니다. 미리보기가 렌더링되면서 저장 기능을 제공합니다.



8. 미리보기에 만족하는 경우 **저장**을 클릭합니다.

## 사용자 정의된 사용자 초대의 허용 목록 및 차단 목록 콘텐츠

**최종 사용자 초대**에서 사용자 초대 이메일 템플릿을 사용자 지정할 경우 허용되는 HTML 태그와 속성 집합이 있습니다. 교차 사이트 스크립팅(XSS) 취약성을 방지하기 위해 사용자 초대에서 허용되지 않는 차단 문자열 목록도 있습니다.

초대 이메일에서는 허용 목록에 등록된 태그와 속성만 사용할 수 있습니다. 다음 표는 허용 목록에 있는 허용되는 태그와 해당 속성을 열거한 것입니다.

> 일부 허용 목록 태그(예: <big>)에는 허용 목록 속성이 없어야 하므로 공백으로 표시됩니다.

| 허용 목록 태그 | 허용 목록 속성 |
| --- | --- |
| <big> | [] |
| <img> | ["id","label","editable","height","border","src","style","width", "align", "class","cellpadding","alt","title","data-max-width","data-default"] |
|  | [] |
| <singleline> | ["label"] |
| <tbody> | [] |
| <!DOCTYPE> | [] |
| <h1> | ["style"] |
| <h2> | ["style"] |
| <hr> | ["noshade","style"] |
| <h3> | [] |
| <body> | ["style", "class", "bgcolor", "paddingwidth", "paddingheight", "offset", "toppadding", "leftpadding", "lang","link","vlink","border","cellspacing","cellpadding"] |
| <title> | ["id"] |
| <head> | [] |
|  | ["style","class","width","align","id"] |
| <br> | [] |
| <path> | ["d"] |
| <ul> | ["style"] |
| <html> | ["xmlns","xmlns:mso","xmlns:msdt"] |
| <ol> | ["start"] |
| <table> | ["class","width","border","cellspacing","cellpadding","style","height","bgcolor", "align","background"] |
| <a> | ["href","style","target","rel","class","title"] |
| <b> | [] |
| <o:p> | [] |
| <svg> | ["xmlns","class","viewbox","width","height","role","aria-labelledby"] |

| 허용 목록 태그 | 허용 목록 속성 |
| --- | --- |
|  | [] |
|  | [] |
| <i> | [] |
| <label> | ["style"] |
| <td> | ["valign","width","height","class", "cellpadding", "cellspacing","border","bgcolor","align", "style","colspan","id"] |
| <p> | ["style","class","align"] |
| <u> | [] |
| <meta> | ["name","content","http-equiv","charset"] |
| <multiline> | ["label"] |
| <style> | ["type","id"] |
| <li> | ["style"] |
| <tr> | ["style"] |
|  | ["style","class","lang"] |
| <font> | ["color"] |

다음은 사용자 정의된 사용자 초대에서 허용되지 않는 차단 목록 문자열 목록입니다.

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4-,+ADw-/SCRIPT+AD4-, xml:base
- 특수 문자 및 javascript 또는 스크립트 검색
- "url="을 포함한 메타 콘텐츠 속성(대소문자 구분)
- .svg를 포함하지 않는 img src
- "\00"을 포함하는 속성 값

위의 차단 목록 문자열 중 하나라도 최종 사용자 초대의 HTML 콘텐츠에 사용된 경우 **미리 보기**를 클릭하면 오류 메시지가 표시됩니다. 이 오류 메시지에는 최종 사용자 초대에 허용되지 않는 HTML 컨텐츠가 열거됩니다. 허용되지 않는 HTML 컨텐츠를 수정 및 제거한 다음, **미리 보기**를 클릭하여 계속합니다.

> 차단 목록 HTML 콘텐츠가 포함된 수정한 템플릿은 저장할 수 없습니다.

## 지원되는 메일 변수

MDM용 Ivanti Neurons는 이메일 템플릿 사용자 지정 시 사용할 수 있는 다양한 변수를 제공합니다.

## 최종 사용자 초대 변수

| 변수 | 설명 |
| --- | --- |
| $ | 사용자 활성화 URL - $ 텍스트 주변 하이퍼링크 |
| $ | 클러스터 등록 URL - 기본 템플릿에서는 찾을 수 없지만 간접적으로 참조됨($ 변수를 통해) |
| $ | 제품 브랜드 이름 - 기본 템플릿 헤더의 <title> 태그로 정의됩니다. |
| $ | 회사 로고 URL - 기본 템플릿에 있는 하나의 이미지(MobileIron CDN에 있는 이미지를 가리킴). **사용자 브랜딩** 설정을 업데이트하면 **$**에서 참조하는 값이 변경됩니다. |
| ${message:$ | 사용자 기기 제목 등록 |
| ${message:$} | 이메일 초대 제목 |
| ${message:$} | 사용자가 기기를 사용 중인지 확인 |
| ${message:$} | 이메일 초대 시작하기 텍스트 |
| ${message:$} | 로그인 및 등록 지침 |
| ${message:$} | 기기 정보로 푸시된 이메일 및 앱 |
| ${message:$} | 사용자가 기기를 사용하고 있지 않은 경우 등록 정보(클러스터 등록 URL 포함) |
| ${message:$} | 회사 웹 사이트 레이블이 포함된 이메일 초대 바닥글 |
| $ | 회사 웹 사이트 레이블 - 기본 템플릿에서는 찾을 수 없지만 간접적으로 참조됨($ 변수를 통해) |

## 비밀번호 만료 알림 변수

| 변수 | 설명 |
| --- | --- |
| $ | 비밀번호 재설정 URL |
| $ | 제품 브랜드 이름 - 기본 템플릿 헤더의 <title> 태그로 정의됩니다. |
| $ | 회사 로고 URL - 기본 템플릿에 있는 하나의 이미지(MobileIron CDN에 있는 이미지를 가리킴). **사용자 브랜딩** 설정을 업데이트하면 **$**에서 참조하는 값이 변경됩니다. |
| ${message:$} | 비밀번호 만료 알림 제목입니다. |
| ${message:$} | 비밀번호 만료 알림 소개 단락입니다. |
| ${message:$} | 비밀번호 재설정 URL 이름입니다. |
| ${message:$} | 회사 웹 사이트 레이블이 포함된 이메일 초대 바닥글 |
| $ | 회사 웹 사이트 레이블 - 기본 템플릿에서는 찾을 수 없지만 간접적으로 참조됨($ 변수를 통해) |

## 등록 확인 변수

| 변수 | 설명 |
| --- | --- |
| $ | 제품 브랜드 이름 - 기본 템플릿 헤더의 <title> 태그로 정의됩니다. |
| $ | 회사 로고 URL - 기본 템플릿에 있는 하나의 이미지(MobileIron CDN에 있는 이미지를 가리킴). **사용자 브랜딩** 설정을 업데이트하면 **$**에서 참조하는 값이 변경됩니다. |
| ${message:$} | 등록 확인 제목 |
| ${message:$} | 등록 확인 소개 단락 |

## 정책 규정 준수 변수

| 변수 | 설명 |
| --- | --- |
| $ | 이 변수는 정책 내에서 이메일 전송 컴플라이언스 조치의 제목 줄에 입력된 내용으로 대체됩니다. |
| $ | 이 변수는 정책 내에서 이메일 전송 컴플라이언스 조치의 메시지 부분에 입력된 내용으로 대체됩니다. |
| $ | 제품 브랜드 이름 - 기본 템플릿 헤더의 <title> 태그로 정의됩니다. |
| $ | 회사 로고 URL - 기본 템플릿에 있는 하나의 이미지(MobileIron CDN에 있는 이미지를 가리킴). **사용자 브랜딩** 설정을 업데이트하면 **$**에서 참조하는 값이 변경됩니다. |
| ${message:$} | 회사 웹 사이트 레이블이 포함된 이메일 초대 바닥글 |
| $ | 회사 웹 사이트 레이블 - 기본 템플릿에서는 찾을 수 없지만 간접적으로 참조됨($ 변수를 통해) |

## 사용자 지정 사용자 속성 변수

관리자는 다음 조건에서 **사용자 지정 사용자 속성**을 사용자 지정 이메일 템플릿의 이메일 변수로 사용할 수 있습니다.

- 사용자 지정 사용자 속성은 **관리 > 속성** 페이지에서 확인할 수 있습니다.
- 관리자는 **사용자를 대상으로 사용자 지정 사용자 속성을 할당했으며**, 각 사용자에 대해 사용자 지정 사용자 속성 값이 지정되었습니다.

# 12.10.5. 셀프 서비스 포털

등록 초대에는 자체 서비스 포털 링크가 포함됩니다. 최종 사용자는 이 포털을 이용해 다음 기능을 이용할 수 있습니다.

- 잠금
- 잠금 해제
- 위치 보기(개인정보보호 구성에서 활성화된 경우)
- 지우기
- 폐기
- 계정 정보(이름, 비밀번호, 이메일 주소) 변경
- 강제 체크인
- 암호화 및 서명 인증서 추가

추가 기기를 등록하려면, 최종 사용자는 자체 서비스 포털에 표시된 등록 포털 링크를 클릭하십시오.

최종 사용자가 셀프 서비스 포털의 URL을 잃어버릴 경우 최종 사용자를 **https://mydevices.mobileiron.com/user/login.html**로 보냅니다. iOS 사용자는 자체 서비스 포털 **웹 클릭 구성**을 생성할 수 있습니다.

## 서명 및 암호화 인증서 업로드

최종 사용자가 사용자 제공 인증서 구성 내에서 자체 서비스 포털에 이메일 서명 및 암호화 인증서를 업로드하도록 허용할 수 있습니다. 이 설정은 사용자 제공 인증서 구성을 사용하여 구성할 수 있습니다. 이 설정을 구성하면 최종 사용자가 자신의 이메일 서명 및 암호화 인증서를 업로드할 수 있습니다.

1. **내 인증서** 탭에서 **인증서 추가**를 클릭합니다. **인증서 추가** 창이 표시됩니다.
2. 다음 필드를 업데이트합니다.

| 필드 이름 | 설명 |
| --- | --- |
| 인증서 유형 | 업로드할 인증서 유형을 선택합니다. 옵션은 다음과 같습니다.<br>• **암호화 인증서**<br>• **서명 인증서**<br>이러한 옵션은 MDM용 Ivanti Neurons 관리 포털에서 생성됩니다. 자세한 내용은 **ID 인증서 구성**을 참조하십시오. |
| 업로드할 인증서 | **파일 선택**을 클릭하고 업로드할 인증서 파일을 선택합니다.<br>파일이 PKCS12 형식인지 확인하십시오. |
| 비밀번호 | 파일에 사용되는 비밀번호를 입력합니다. |

3. **업로드**를 클릭하세요.

업로드 후에는 다음 상세 정보를 표시하는 인증서 목록을 표에서 볼 수 있습니다.

| 필드 이름 | 설명 |
| --- | --- |
| 인증서 이름 | 인증서 유형을 **암호화** 또는 **서명**으로 지정합니다. |
| 발급자 | 발급된 인증서의 상세 정보입니다. |
| 다음에 업로드됨 | 인증서가 업로드된 날짜입니다. |
| 만료 날짜 | 인증서의 만료 날짜입니다. |
| 작업 | 다음과 같은 작업을 수행할 수 있습니다.<br>• **인증서 편집** - 인증서 상세 정보를 편집합니다.<br>• **개인 키 삭제** - 인증서 패키지(PKCS#12)에서 개인 키를 삭제합니다.<br>• **인증서 삭제** – MDM용 Ivanti Neurons 서버에서 인증서를 삭제합니다. |

사용자가 인증서 구성을 업로드할 때 서버는 인증서를 사용하고 있는 구성을 다시 푸시합니다.

> 사용자가 비공개 키를 삭제하거나 지울 때는 구성이 다시 푸시되지 않습니다.

자세한 내용은 **셀프 서비스 포털 브랜딩**을 참조하십시오.

# 12.10.6. 셀프 서비스 포털(브랜딩)

**라이센스:** Silver

사용자 소속 조직 로고를 이용해 **자체 서비스 포털**을 맞춤설정할 수 있습니다. 로고를 따로 등록하지 않을 경우, 자체 서비스 포털에는 기본 서비스 로고가 표시됩니다.

## 셀프 서비스 포털 브랜딩

**절차**

1. 자체 서비스 포털 브랜딩 화면에서 **사용자 설정**(우측 상단)을 클릭하세요.
2. 로고 파일(PNG, 182x34)을 점선 박스로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다.
3. **변경사항 저장**을 클릭하세요.

# 12.10.7. 다중 사용자 로그인(웹 클립) 브랜딩

새 제목 및 웹 클립 아이콘을 추가하여 iOS용 다중 사용자 보안 로그인을 사용자 지정합니다.

**절차**

1. **관리 > 다중 사용자 로그인(웹 클립)**으로 이동합니다.
2. 다중 사용자 로그인(웹 클립) 화면에서 **사용자 지정**을 클릭합니다.
3. 로고 파일을 점선 박스로 드래그하거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다.
4. 레이블을 변경하려면 **보안 로그인** 텍스트를 편집합니다.
5. 웹 클립 아이콘을 변경하려면 웹 클립 파일을 점선 박스로 끌어다 놓거나 **파일 선택**을 클릭해 파일 시스템에서 해당 파일을 선택합니다.
6. 업데이트를 미리 보기한 다음 **변경 저장**을 클릭합니다.

iPhone 및 iPod touch 기기의 경우 120 x 120픽셀 또는 60 x 60픽셀(표준 해상도) 크기의 아이콘을 생성합니다.

iPad 기기의 경우 152 x 152픽셀 또는 76 x 76픽셀(표준 해상도) 크기의 아이콘을 생성합니다.

자세한 내용은 **iOS용 다중 사용자 보안 로그인**을 참조하십시오.

# 12.10.8. 조직

조직에 브랜딩 이름을 지정하거나, 이메일 제목 줄에 테넌트별 식별자(예: 고객 이름)를 포함하여 시스템 알림 이메일 제목 줄을 개인화할 수 있습니다. 조직 이름을 업데이트하지 않으면, 조직 화면에는 기본값이 표시됩니다.

## 조직 브랜드 지정

**절차**

1. 조직 화면의 **이름** 필드에 원하는 이름을 입력합니다.
2. 접두사를 추가하려면, **편집**을 클릭하고 **시스템에서 생성된 모든 이메일(예: 라이선스 만료)에 조직 이름을 접두사로 추가** 옵션을 활성화하세요.
3. 변경 사항을 적용하려면 **저장**을 클릭하세요.

# 12.11. 비 iOS 기기 관리 추가

**라이센스: Gold**

현재 iOS 기기에 최적화된 MDM용 Ivanti Neurons 버전을 사용하고 있습니다. 이 섹션에서는 iOS가 아닌 기기의 관리를 허용하도록 전환하는 방법을 설명합니다. 전환한 후에는 다음 기기를 관리할 수도 있습니다.

- Android 5.0 또는 지원되는 최신 버전
- Windows 10+

iOS가 아닌 기기의 관리를 포함하도록 전환하면 이것을 번복할 수 없습니다.

iOS가 아닌 기기를 포함하도록 전환하려면:

1. **관리 > 허용된 플랫폼**을 클릭합니다.
2. **모든 플랫폼 허용** 버튼을 클릭합니다.
3. **이 작업을 실행 취소할 수 없다는 것을 이해했습니다**를 선택하여 이 작업을 취소할 수 없음을 인지하고 이해했음을 확인합니다.
4. **모든 플랫폼 허용** 버튼을 클릭합니다.

# 13. 패키지

이 섹션에는 다음 주제가 포함됩니다.


- 업그레이드하기
- 보안 UEM 및 보안 UEM 프리미엄 패키지
- 기존의 브론즈, 실버, 골드 패키지
  - 라이센스
  - 업그레이드
  - Platinum
- 미리보기 또는 테스트용 샌드박스


## 보안 UEM 및 보안 UEM 프리미엄 패키지

보안 UEM 및 보안 UEM 프리미엄 패키지는 다음과 같은 기능을 제공합니다.

| | Secure UEM | Secure UEM Premium |
|---|---|---|
| **Device management and security** | | |
| Easy on-boarding | ✓ | ✓ |
| Multi-OS security and management | ✓ | ✓ |
| Secure email gateway | ✓ | ✓ |
| App distribution and configuration | ✓ | ✓ |
| Mobile application management (MAM) | ✓ | ✓ |
| **Scale IT operations** | | |
| Helpdesk tools | ✓ | ✓ |
| Reporting | ✓ | ✓ |
| **Secure connectivity** | | |
| Per app VPN | | ✓ |
| Conditional Access | | ✓ |
| **Secure productivity** | | |
| Secure email and personal information management (PIM) app | | ✓ |
| Secure web browsing | | ✓ |
| Secure content collaboration | | ✓ |
| Mobile app containerization | | ✓ |
| Derived Credentials | | ✓ |
| **Zero Sign-On** | | |
| Passwordless user authentication (single app) | | ✓ |

패키지는 변경될 수 있습니다. **Ivanti 세일즈**에 문의하여 현재 구성을 확인하십시오.

## 기존의 브론즈, 실버, 골드 패키지

이 섹션은 기존의 브론즈, 실버, 골드 패키지를 설명합니다. 이 패키지는 현재 **보안 UEM 및 보안 UEM 프리미엄** 구성으로 업그레이드됐습니다.

### 브론즈

Bronze 패키지에는 MDM용 Ivanti Neurons 기본 기능이 제공됩니다. Bronze 패키지 확장 방법:

- 장치 추가
- Silver 추가
- Gold 추가
- 다음 라이센스 추가: Platinum

이렇게 기기 등의 항목을 추가하면 모바일 솔루션 사용 범위를 기본 기기 구성 이상으로 확장할 수 있습니다.

관리자는 테넌트에 기본적으로 비활성화된 하나 이상의 주문형 기능을 활성화하는 데 관심이 있는 경우 지원에 문의할 수 있습니다.

## 라이센스

Silver로 업그레이드하면 다음 기능이 추가됩니다.

- **LDAP 및 Connector:** MDM용 Ivanti Neurons에 회사 디렉토리 및 인증 기관 추가를 지원합니다.
- **Sentry:** 이메일 접근 제어를 지원합니다.
- **공간:** 여러 관리자가 관리할(위임 관리) 장치 지정을 지원합니다.
- **감독 모드:** 단일 앱(Single-app) 모드 등 세분화된 설정에 대해 장치별로 지원합니다.
- **셀프 서비스 포털 브랜딩:** 셀프 서비스 포털에서 로고를 사용합니다.
- **인증 기관:** MDM용 Ivanti Neurons를 인증 기관으로 사용합니다.
- **자동 앱 설치/제거:** 모바일 기기에서 앱을 자동으로 배포하거나 제거할 수 있습니다.
- **앱 허용/차단/필수 앱:** 기기에 설치되는 앱을 모니터링 및 제어합니다.
- **웹 콘텐츠 필터:** 모든 웹 브라우저에 허용 목록/차단 목록 정책을 적용할 수 있습니다.
- **Apple 전용 기능:** AirPlay 및 AirDrop, iOS 배경화면 배포, Apple TV 설정/제한 가능
- **오픈인 관리:** 어떤 모바일 앱이 어떤 엔터프라이즈 콘텐츠를 열 수 있는지 관리합니다.
- **Apple Apps 및 Books:** 모바일 앱 라이센스를 기기에 배포하고 기기가 폐기되는 경우 해당 라이센스를 회수 및 재할당할 수 있습니다.
- **Android 엔터프라이즈(Android for Work) 지원**
- **기기 등록:** 고객이 대량으로 기기를 구매하고 이를 활성화하는 동안 MDM에 Apple 기기를 자동으로 등록할 수 있습니다.
- **퍼앱 구성:** 구성된 모바일 앱을 최종 사용자의 별도 작업 없이 수준에 맞게 배포할 수 있습니다.
- **제3자 퍼앱 VPN:** VPN 보안이 이제는 모바일 앱 전용으로 즉각적이고 무형으로 이루어집니다.
- **계층화된 정책 작업**
- 앱 배포 필터
- **감사 내역**
- **Android 키오스크 모드:** 키오스크 모드에 작동될 Android 기기 구성 지원
- **Android 키오스크 브랜딩:** 기기가 키오스크 모드로 작동 중일 때 나타나는 키오스크 화면의 배경 및 배너를 변경할 수 있습니다.
- **Microsoft Graph API를 사용한 Office 365 데이터 손실 방지 (DLP)**: 그래프 API를 통해 Office 365 앱에 대한 DLP 제어를 실행합니다.

## 업그레이드

Gold로 업그레이드하면 Silver가 제공하는 기능에 더해 다음 기능이 추가됩니다.

- **싱글 사인온(SSO):** 1회의 인증을 거치면 다른 엔터프라이즈 모바일 앱에도 자동으로 로그인됩니다.
- **iOS 및 Android App Catalog 사용자 지정 브랜딩:** App Catalog에 회사 로고를 표시합니다.
- **콘텐츠 한도 증가**: 파일 50개, 파일당 25MB
- **iOS용 AppConnect:** AppConnect 활성화 앱을 보안 및 구성할 수 있습니다.
- **iOS용 AppTunnel:** 엔터프라이즈 리소스에 대한 보안 앱 액세스입니다.
- **iOS용 Docs@Work:** 사용자에게 문서 보기, 저장, 공유 권한을 부여합니다.
- **iOS 8 인증 기반 SSO**

- **iOS 8 iBook/ePub 관리**
- **macOS 지원**
- **사용자 브랜딩**
- **AppConnect를 통한 모바일 애플리케이션 관리(MAM: Mobile Application Management)**
- **파생 자격 증명**
- **Windows 10(Bridge 포함) 지원**

### Platinum

Platinum으로 업그레이드하면 Gold가 제공하는 기능에 더해 다음 기능이 추가됩니다.

- **Tunnel:** 엔터프라이즈 데이터에 앱별 액세스 구성
- **Help@Work**
- **모니터**
- **ServiceConnect(ServiceNow, Splunk)**

## 미리보기 또는 테스트용 샌드박스

**프리미엄 플러스** 지원을 구입한 경우 MDM용 Ivanti Neurons 고객은 샌드박스 테넌트를 사용하여 생산을 시작하기 전에 새 릴리스를 미리 보고 테스트할 수 있습니다.

# 13.1. 업그레이드하기

이 섹션에는 다음 주제가 포함됩니다.


- 라이센스 업그레이드
- 업그레이드 요청
- 이전 릴리스에서 업그레이드


## 라이센스 업그레이드

Bronze 패키지에는 기본 기능이 제공됩니다. Bronze 패키지 확장 방법:

- 장치 추가
- Silver 추가
- Gold 추가
- 다음 라이센스 추가: Platinum

이렇게 장치 등의 항목을 추가하면 모바일 솔루션 사용 범위를 기본 장치 설정 이상으로 확장할 있습니다.

## 업그레이드 요청

**절차**

1. 관리 드롭다운 메뉴에서**업그레이드 옵션**을 선택합니다.
2. **업그레이드 요청 / 기기 추가**(우측 상단)를 클릭하세요.
3. 추가할 항목을 선택한 후 연락 가능한 전화번호를 입력하세요.

24시간 내에 담당자가 연락해 자세한 사항을 안내해 드립니다.

## 이전 릴리스에서 업그레이드

이전 릴리스에서 업그레이드하는 경우 **기기 등록 프로필 편집** 페이지의 설정이 유지되지 않습니다. 업그레이드하기 전에 옵션 설정에 주의하십시오.

- 업그레이드 전에 **AppleID 및 iCloud에 로그인 건너뛰기**가 활성화된 경우, 업그레이드 후 **Apple Pay 설정 건너뛰기**가 활성화됩니다.
- 업그레이드 전에 **암호 입력 건너뛰기**가 활성화된 경우, 업그레이드 후 **터치 ID 건너뛰기** 및 **Apple Pay 설정 건너뛰기**가 활성화됩니다.

**절차**

1. 업그레이드가 완료된 후 **기기 등록 프로필 편집** 페이지로 돌아가 기기 등록 프로필을 편집하여 원하는 설정을 복원합니다.
2. **저장**을 클릭하세요.

업그레이드한 후에는 일부 구성 설정이 영향을 받습니다.

- 프로모션 옵션이 **사용 안함**으로 설정됩니다.
  설치 설정이 **설치 안함**으로 설정됩니다.
  **App Catalog에 다시 표시하지 않음** 옵션이 더 이상 선택되지 않습니다.
  **Android Samsung Knox에 자동 설치**가 False로 설정됩니다.

iOS 관리 플래그가 다음과 같이 설정됩니다.

- iCloud에 백업.
- 등록 해제 시 제거.

이 iOS 관리 플래그 설정은 각 앱에 대해 개별적으로 선택할 수 있습니다.

앱 설정:

- 앱 설정을 이제 구성이라고 합니다.
- 모든 다른 앱 설정은 업그레이드 전과 동일합니다.

자세한 내용은 **패키지**를 참조하십시오.

# 14. 장치 라이센스

MDM용 Ivanti Neurons 기기 기반 라이선스는 등록 가능한 기기 수, 기기 배포용으로 구성 가능한 콘텐츠 양, 사용 가능한 기능을 정의합니다. 장치 개수가 지정된 최대 한계에 도달하면 관리 페이지에 적색 삼각형이 표시됩니다. 컨텐츠 양이 지정된 최대 한계에 도달하면 컨텐츠 추가가 차단되면서 지정된 최대 한계에 도달했다는 메시지가 표시됩니다.

# 14.1. 테넌트 정지

평가 라이선스 또는 프로덕션 라이선스와 함께 사용된 테넌트에 대한 액세스는 MDM용 Ivanti Neurons에 의해 일시 정지될 수 있습니다. 평가 라이센스는 평가 기간이 만료되거나 사용 허용량이 초과된 경우 정지될 수 있습니다. 프로덕션 라이센스는 구독 기간이 만료되거나 사용 허용량이 초과된 경우 정지될 수 있습니다. 기간이 만료된 경우, 라이선스를 갱신하거나 추가 라이선스를 구매하면 MDM용 Ivanti Neurons는 일시 정지된 테넌트를 복원합니다.

### 테넌트 라이센스가 일시 정지된 경우:

- 기존 등록 기기는 계속 정상적으로 작동합니다.
- 관리자가 관리 포털에 로그인할 수 없습니다.
- 새 기기를 등록할 수 없습니다.
- 테넌트의 API 액세스가 차단됩니다.
- 최종 사용자는 계속 자체 서비스 포털에 액세스할 수 있습니다.

### 테넌트 정지 조치 및 오류 메시지

| 정지 조치 | 오류 | 표시되는 오류 메시지 | 위치 |
|---|---|---|---|
| 최종 고객 통합 API 액세스가 차단됩니다. | API 호출에 실패했습니다. | 액세스가 거부되었습니다. 평가 라이센스가 만료되었습니다. API 액세스를 다시 활성화하도록 라이센스를 갱신하십시오. 자세한 내용은 시스템 관리자에게 문의하십시오. | API 오류 401. |
| 새 기기의 등록이 차단되었습니다. | 오류 메시지가 등록 화면에 표시됩니다. | 기기를 등록할 수 없습니다. 시스템에 대한 라이센스가 만료되었습니다. 자세한 내용은 시스템 관리자에게 문의하십시오. 이전에 등록한 기기는 계속해서 정상적으로 작동합니다. | 후속 비밀번호 검증. |
| 관리자의 관리 포털 로그인이 차단됩니다. | 오류 메시지가 로그인 화면에 표시됩니다. | 로그인할 수 없습니다. 라이센스가 만료되었습니다. 관리자 포털에 다시 액세스하고 새 기기를 등록하려면 라이센스를 갱신하십시오. 이전에 등록된 기기는 정상적으로 작동합니다. 라이센스를 갱신하려면 담당 영업 사원에게 문의하십시오. 관리자 비밀번호는 1년(365일) 이후 만료됩니다. | 후속 비밀번호 검증. |

# 15. 지원 티켓 열기

지원 티켓을 열려면 **Ivanti 지원 포털**을 방문하십시오.

# 16. 타사 속성

MDM용 Ivanti Neurons에는 타사에서 개발한 구성 요소가 포함되어 있습니다. 목록은 여기에서 볼 수 있습니다.

# 17. Apps@Work

MDM용 Ivanti Neurons 릴리스 83부터 Go 애플리케이션에서 Apps@Work 기본 환경으로 전환할 수 있습니다. 새로 생성된 테넌트의 경우 iReg 또는 클라이언트를 통해 설치된 iOS 기기에 대해 Apps@Work Webclip 구성이 기본적으로 배포되지 않습니다. 관리자는 iReg 또는 클라이언트를 통해 등록된 기기에 webclip 구성을 수동으로 배포해야 합니다. 참고:

MDM용 Ivanti Neurons **관리 포털**:

- 기본적으로 새 테넌트만 iOS 기기에 배포된 네이티브 클라이언트용 앱 카탈로그 구성을 가져옵니다.
- 기존 테넌트의 경우 기본적으로 Apps@Work Native 애플리케이션이 배포되지 않습니다.
- 기본 앱스토어 환경에서 Apps@Work를 사용할 수 있도록 하려면 관리자가 네이티브 클라이언트용 앱 카탈로그 구성을 기기에 푸시해야 합니다.

**클라이언트**:

- 이제 Go 애플리케이션에 Apps@Work용 탭이 표시됩니다.
- 네이티브 클라이언트용 앱 카탈로그 구성에는 네이티브 클라이언트용 앱 카탈로그 ID 인증서와 App Station ID 인증서가 있습니다. MDM용 Ivanti Neurons 은(는) 네이티브 클라이언트용 앱 카탈로그 구성과 함께 인증서를 푸시합니다.

## Apps@Work 기능

Apps@Work 탭에는 다음과 같은 기능이 있습니다.

- Go 애플리케이션에서 **Go 애플리케이션에서 Apps@Work 탭에 액세스**
- **검색**
- **앱 설치 - 버튼 상태**
- **추천 애플리케이션 및 배너**
- **애플리케이션 업데이트 알림**
- **애플리케이션 업데이트 알림**

### Go 애플리케이션에서 Apps@Work 탭에 액세스

- 새 탭이 Apps@Work용 Go app에 추가됩니다.
- Apps@Work-All 앱 및 카테고리에서 두 개의 기본 탭을 사용할 수 있습니다.
- 모든 앱 탭에는 모든 앱이 알파벳 순서로 나열됩니다.
- 범주 탭에는 애플리케이션이 포함된 범주만 표시됩니다.
- 각 범주는 해당 범주에 있는 애플리케이션의 수를 표시합니다.
- 범주 아래의 MyApps는 설치된 모든 애플리케이션을 포함하는 목록 항목입니다. MyApps는 항상 첫 번째 범주가 되며 나머지 범주는 알파벳순으로 나열됩니다.
- 설치된 애플리케이션이 없으면 MyApps 목록에 없음이 표시됩니다.
- 범주를 클릭하면 해당 범주와 관련된 모든 애플리케이션이 설치 옵션과 함께 나열됩니다. 마법사를 사용하여 각 애플리케이션을 개별적으로 설치하거나 모두 설치를 클릭하여 범주 내 모든 애플리케이션을 설치할 수 있습니다. 각 애플리케이션에 대한 설치를 허용할지 묻는 메시지가 표시됩니다.

### 검색

- 검색(렌즈) 아이콘을 눌러 다음을 검색합니다.
  - 새 릴리스-검색창에 텍스트를 입력하지 않으면 새로 출시된 앱 목록 표시
  - 텍스트를 입력하면 일치하는 해당 애플리케이션을 검색 필드에서 동적으로 예측하고 표시합니다.
  - 검색 결과 개수가 부제목으로 표시
  - 세부 정보 페이지로 이동하지 않고 설치 버튼을 눌러 애플리케이션을 설치할 수 있습니다.

## 앱 설치 - 버튼 상태

- 앱 설치는 서버에서 요청을 처리하고 앱을 기기에 푸시해야 하기 때문에 설치 버튼이 실시간으로 진행 상황을 표시하지 않음
- 설치 버튼은 설치 > 요청됨 > 설치됨에서 상태를 변경합니다.
- 처음에는 설치가 요청되었음을 나타내는 경고 메시지가 나타납니다.
- "요청됨" 버튼을 누를 때도 경고가 나타납니다.
- 설치됨 상태는 버튼이 아닙니다.

## 추천 애플리케이션 및 배너

- 추천 탭은 관리자 구성에 따라 표시됩니다.
- 추천 탭은 사용 가능한 업데이트가 없을 때 표시되는 기본 랜딩 페이지입니다.
- 추천 앱 배너는 배너에 하나의 애플리케이션을 표시합니다.
- 추천 앱에는 모든 추천 애플리케이션 목록이 포함되어 있습니다.

## 애플리케이션 업데이트 알림

- Go는 애플리케이션 업데이트가 있을 때 알림을 보냅니다. 알림에는 애플리케이션 이름이 표시되지 않습니다.
- 애플리케이션 업데이트 알림을 누르면 Apps@Work의 모든 앱 페이지로 리디렉션됩니다.
- Go 애플리케이션에서 Apps@Work 탭 아이콘은 보류 중인 업데이트가 있는 애플리케이션 수의 배지 개수를 표시합니다.
- Apps@Work 탭에서 모든 앱 탭 아래에 사용 가능한 업데이트 하위 섹션이 나타나고 업데이트에 사용할 수 있는 애플리케이션 수가 표시됩니다.
- 업데이트가 필요한 모든 애플리케이션에 대해 빨간색 점 아이콘이 표시됩니다.

## 설정-내 기기

- 이제 내 기기 탭이 설정 아래로 이동되었습니다.
- 애플리케이션 업데이트 알림을 누르면 Apps@Work의 모든 앱 페이지로 리디렉션됩니다.
- Go 애플리케이션에서 Apps@Work 탭 아이콘은 보류 중인 업데이트가 있는 애플리케이션 수의 배지 개수를 표시합니다.
- Apps@Work 탭에서 모든 앱 탭 아래에 사용 가능한 업데이트 하위 섹션이 나타나고 업데이트에 사용할 수 있는 애플리케이션 수가 표시됩니다.
- 업데이트가 필요한 모든 애플리케이션에 대해 빨간색 점 아이콘이 표시됩니다.

# 18. MDM용 Ivanti Neurons 및 SCEP 서버 사이에 Kerberos 인증 활성화

MDM용 Ivanti Neurons 및 SCEP 간 통신에 Kerberos 인증을 사용할 수 있습니다. 다음 섹션에서 SCEP 서버 및 MDM용 Ivanti Neurons에서 Kerberos 인증을 활성화하는 방법을 다룹니다.

> 이 기능은 MDM용 Ivanti Neurons 커넥터 93 버전을 사용할 수 있는 경우에 작동합니다.

## 사전 구성 단계

1. SCEP 서버에서 SCEP 서비스에 사용 중인 서비스 계정을 확인하세요.
2. SCEP 서버에서 서비스 계정이 로컬 IIS_USRS 그룹의 구성원인지 확인합니다.
3. 프로비저닝 중인 CA 서버 인증서 템플릿에서 서비스 계정에 등록 권한이 있는지 확인하세요.

## Windows 서버 구성

1. 도메인 컨트롤러에서 다음 명령을 실행합니다.
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
2. **Active Directory 사용자 및 컴퓨터**에서 서비스 계정의 **위임** 탭을 클릭합니다.
   1. **지정 서비스 위임에 한하여 이 사용자 신뢰**에서 **Kerberos만 사용**을 선택합니다.
   2. **추가**를 클릭하고 SCEP 서버 이름을 추가합니다.
   3. HTTP 서비스를 선택합니다.
   4. **확인**을 클릭하세요.
3. Kerberos 티켓을 해독하는 데 응용 프로그램 풀 자격 증명이 사용되는지 확인하려면 IIS 서버에서 다음을 수행하십시오.
   1. 앞서 확인한 서비스 계정에서 SCEP 응용 프로그램 풀이 실행되고 있는지 확인하세요.
   2. useAppPoolCredentials를 활성화하려면 Microsoft SCEP 관리(mscep_admin) 또는 Microsoft SCEP(mscep) 웹페이지에서 **구성 편집기 > System.webServer > 보안 > 인증 > Windows 인증**을 선택하고 값을 useAppPoolCredentials=참으로 설정합니다.
4. **인증 > 익명 인증**을 선택하고 **비활성화**를 클릭하여 Microsoft SCEP 관리 웹페이지(mscep_admin)에서 **익명 인증**을 비활성화합니다.
5. Windows 인증 고급 설정에서 커널 모드 인증을 비활성화합니다.

> 인증 서비스의 첫 번째 옵션으로 **협상**을 사용해야 합니다.

6. Windows 인증 고급 설정 웹페이지에서 커널 모드 인증을 비활성화합니다.
7. IIS 서비스를 다시 시작합니다.

## Kerberos 구성

이 섹션에서는 MDM용 Ivanti Neurons 서버에서 Kerberos를 구성하는 방법에 대해 설명합니다.

### MDM용 Ivanti Neurons에서 Kerberos 설정 구성

**관리 > 인프라 > Kerberos**로 이동하여 표에 나온 대로 다음 설정을 입력합니다.

| UI 섹션 | 보기 |
| --- | --- |
| Active Directory의 Kerberos 영역 | IVANTI.COM |
| 해당 KDC(키 배포 센터) 서버 | kdc.ivanti.com |
| 서비스 사용자 자격 증명 | user@realm<br>예:<br>serviceuser@IVANTI.COM |
| Microsoft AD 인증서 서비스와의 아웃바운드 통신을 위한 도메인(호스트 이름은 대소문자를 구분하지 않으며 .ivanti.com 또는 .IVANTI.COM으로 끝나야 함)<br>SCEP 또는 NDES 서버: ndes.ivanti.com 또는 scep.ivanti.com과 같은 호스트 이름을 사용할 수도 있음 | |

## 기존 인증 기관의 Microsoft SCEP 인증서 등록 구성에서 Kerberos 인증 활성화

기존 인증 기관에서 Kerberos 인증을 활성화하려면 다음 단계를 수행하십시오.

1. MDM용 Ivanti Neurons에서 **관리자 > 인프라 > 인증서 관리**를 선택합니다.
2. **외부** 옵션으로 인증 기관 유형을 선택합니다.

> 이러한 외부 인증 기관 유형이 Microsoft로 표시되어야 합니다.

3. **작업** 드롭다운에서 **편집**을 선택합니다.
4. **외부 CA 편집** 창에서 **Kerberos 인증 선호** 확인란을 선택하여 Kerberos 인증을 활성화합니다.

## 새 인증 기관에 대한 Microsoft SCEP 인증서 등록 구성에서 Kerberos 인증 활성화

새 인증 기관에 대해 Kerberos 인증을 활성화하려면 다음 단계를 수행하십시오.

1. MDM용 Ivanti Neurons에서 **관리자 > 인프라 > 인증서 관리**를 선택합니다.
2. **+추가** 옵션을 선택합니다.
3. **인증 기관 추가** 창에서 **온프레미스 SCEP 인증 기관에 연결** 옵션을 선택합니다.
4. 계속을 클릭하세요.
5. **외부 인증 기관 추가** 창에서 다음 단계를 수행하십시오.
    1. **인증 기관 유형** 드롭다운에서 **Microsoft** 옵션을 선택합니다.
    2. Kerberos 인증을 활성화하려면 **Kerberos 인증 선호** 확인란을 선택합니다.
    3. 필수 입력란을 모두 입력하세요.
    4. **완료**를 클릭하세요.

# 19. MDM용 Ivanti Neurons 127 관리자 가이드

## 2026년 9월

최신 모바일 보안 접근 방법인 MDM용 Ivanti Neurons는 고도로 확장 가능하고 안전하며 쉽게 업데이트할 수 있는 인프라를 통해 UEM(통합 엔드포인트 관리) 솔루션을 제공하며 전 세계의 수백만 기기를 지원합니다.

{{원하는 언어를 사용할 수 없는 경우}}

새 기능 요약

PDF로 보기

비디오

# 20. Welcome

# 21. Welcome CSH

# 22. Windows 업데이트 관리

관리자는 Windows 업데이트 관리를 사용하여 업데이트하려는 Windows 장치에서 보고된 업데이트를 확인하고 승인할 수 있습니다. 이 기능을 사용하면 불필요하거나 테스트 되지 않은 업데이트가 기기에 설치되는 것을 방지할 수 있습니다.

업데이트 관리 기능을 사용하려면 **업데이트 승인 필요** 옵션이 활성화된 상태에서 **소프트웨어 업데이트** 구성으로 설정된 기기가 필요합니다. 기기에 이 구성을 적용해야만 기기가 업데이트 설치 준비를 보고하고 승인을 기다릴 수 있습니다.

## 업데이트 관리

1. **관리자>Windows 업데이트**로 이동합니다. 페이지에 업데이트에 관한 다음 상세 정보가 표시됩니다.
   **생성 날짜**: 업데이트가 생성된 날짜**제목**: 기술 자료 정보 번호와 함께 업데이트 유형을 설명합니다.

> 업데이트를 클릭하면 설명이 표시됩니다.

**분류**: 업데이트 유형을 다음 중 하나로 분류합니다.

- 중요 업데이트
- 정의 업데이트
- 드라이버 업데이트
- 보안 업데이트
- 업데이트
- 업그레이드
- 업데이트 롤업

**배포**: 업데이트를 위해 수행되는 배포 예를 들어, 업데이트가 모든 기기에 배포되면 **모두**를 표시합니다.

> 업데이트가 특정 수의 그룹에 배포되면 배포 수가 표시됩니다. 예를 들어 세 그룹에게 배포가 수행된 경우 3을 표시합니다.

2. 또한, 필요한 기기에 업데이트가 배포되었는지 여부를 확인할 수 있습니다. 다음 열에 표시된 숫자는 업데이트의 여러 카테고리에 속한 기기 수를 나타냅니다.
   - 해당하는 기기
   - 설치된 기기
   - 실패한 기기
   - 재부팅 보류 중 기기

이러한 숫자 중 하나를 클릭하면 기기 페이지의 필터링 보기로 이동하여 업데이트 상태를 확인하고 필요한 작업을 수행할 수 있습니다.
업데이트를 검토한 후 업데이트 체크박스를 클릭하여 기기에 배포하고 싶은 업데이트를 선택합니다.

3. **작업**에서 **배포 설정**을 클릭합니다.
4. **Windows 업데이트 배포** 창에서 다음 배포 옵션 중 하나를 선택합니다.
   **모든 기기**: 모든 기기에 업데이트를 배포합니다.
   **배포 안함**: 기기에 업데이트를 배포하지 않습니다.**사용자 지정**: 특정 기기 그룹에 업데이트를 배포합니다.
5. **저장**을 클릭하세요.

## 업데이트 검색 및 필터링

다음과 같은 기준을 기반으로 업데이트를 검색하고 필터링할 수 있습니다.

- 기술 자료 ID
- 구성된 배포

기술 자료 ID에 기반한 필터링:

1. **Windows 업데이트 관리** 페이지에서 빠른 검색 필드에 기술 자료 ID를 입력합니다(검색 필드에는 숫자만 사용).
   예: KB4056892의 경우, 4056892만 입력합니다. 검색 기준과 맞는 업데이트가 페이지에 표시됩니다.

> **지원** 및 **추가 정보** 링크를 클릭하여 업데이트의 추가적인 정보를 확인할 수 있습니다.**지원**링크는 업데이트를 위한 제품 지원 정보를 제공하는 Microsoft 웹 페이지로 연결되며 **자세한 내용**링크는 기술자료와 같은 업데이트에 관한 자세한 정보를 보여주는 Microsoft 웹 페이지로 연결됩니다.

구성된 배포를 기반으로 필터링:

**Windows 업데이트 관리** 페이지에서 구성된 배포에 따라 다음 필터링 옵션 중 하나를 선택합니다.

- **모두**: 모든 업데이트를 표시합니다.
- **구성됨**: 기기에 배포된 업데이트 목록을 표시합니다.
- **구성되지 않음**: 배포가 특정하지 않은 업데이트 목록을 표시합니다.

> 구성된 필터와 구성되지 않은 필터는 배포 상태에 따라 결정되며, 배포는 **없음**으로 설정할 수도 있습니다.

## 기기에 대한 업데이트 검토

기기별 업데이트 세부 정보 검토 방법:

1. **장치 > 장치**를 선택하세요.
2. 세부 정보 페이지를 표시할 기기 이름을 클릭합니다.
3. **업데이트** 탭으로 이동합니다. 기기에 지연(관리자가 업데이트를 승인했지만 기기에 설치됨으로 보고되지 않은 경우), 실패, 설치된 업데이트가 보여집니다.

> 대시보드의 알림 페이지에서 새 Windows 업데이트에 대한 알림을 볼 수도 있습니다. 알림에는 알림 생성 날짜, 사용 가능한 알림 개수 및 알림 목적이 포함됩니다. Windows 업데이트 알림은 관리자 포털의 상단 우측 모서리에서도 볼 수 있습니다.