



XenMobile Server 현재 릴리스

Contents

롤링 패치에 대한 릴리스 정보	10
XenMobile Server 10.15 롤링 패치 5 릴리스에 대한 릴리스 정보	11
XenMobile Server 10.15 롤링 패치 4 릴리스에 대한 릴리스 정보	13
XenMobile Server 10.15 롤링 패치 3 릴리스에 대한 릴리스 정보	14
XenMobile Server 10.15 롤링 패치 2 릴리스에 대한 릴리스 정보	14
XenMobile Server 10.15 롤링 패치 1 릴리스에 대한 릴리스 정보	15
XenMobile Server 10.14 롤링 패치 12 릴리스에 대한 릴리스 정보	16
XenMobile Server 10.14 롤링 패치 11 릴리스에 대한 릴리스 정보	16
XenMobile Server 10.14 롤링 패치 10 릴리스에 대한 릴리스 정보	17
XenMobile Server 10.14 롤링 패치 9 릴리스에 대한 릴리스 정보	18
XenMobile Server 10.14 롤링 패치 8 릴리스에 대한 릴리스 정보	19
XenMobile Server 10.14 롤링 패치 7 릴리스에 대한 릴리스 정보	19
XenMobile Server 10.14 롤링 패치 6 릴리스에 대한 릴리스 정보	21
XenMobile Server 10.14 롤링 패치 5 릴리스에 대한 릴리스 정보	21
XenMobile Server 10.14 롤링 패치 4 릴리스에 대한 릴리스 정보	22
XenMobile Server 10.14 롤링 패치 3 릴리스에 대한 릴리스 정보	23
XenMobile Server 10.14 롤링 패치 2 릴리스에 대한 릴리스 정보	23
XenMobile Server 10.14 롤링 패치 1 릴리스에 대한 릴리스 정보	23
XenMobile Server 10.13 롤링 패치 10 릴리스에 대한 릴리스 정보	24
XenMobile Server 10.13 롤링 패치 9 릴리스에 대한 릴리스 정보	25
XenMobile Server 10.13 롤링 패치 8 릴리스에 대한 릴리스 정보	26
XenMobile Server 10.13 롤링 패치 7 릴리스에 대한 릴리스 정보	27
XenMobile Server 10.13 롤링 패치 6 릴리스에 대한 릴리스 정보	27

XenMobile Server 10.13 롤링 패치 4 릴리스에 대한 릴리스 정보	27
XenMobile Server 10.13 롤링 패치 3 릴리스에 대한 릴리스 정보	28
XenMobile Server 10.12 롤링 패치 11 릴리스에 대한 릴리스 정보	29
XenMobile Server 10.12 롤링 패치 10 릴리스에 대한 릴리스 정보	29
XenMobile Server 10.12 롤링 패치 9 릴리스에 대한 릴리스 정보	29
XenMobile Server 10.12 롤링 패치 8 릴리스에 대한 릴리스 정보	30
XenMobile Server 10.15 의 새로운 기능	31
XenMobile Server 10.14 의 새로운 기능	36
XenMobile Server 10.13 의 새로운 기능	41
XenMobile Server 10.12 의 새로운 기능	51
XenMobile Server 10.11 의 새로운 기능	58
타사 고지 사항	68
사용 중단	68
수정된 문제	79
알려진 문제	80
아키텍처	81
시스템 요구 사항 및 호환성	84
XenMobile 호환성	87
지원되는 장치 운영 체제	89
포트 요구 사항	90
확장성 및 성능	97
라이센싱	100
FIPS 140-2 준수	106
언어 지원	107

설치 및 구성	109
XenMobile 을 사용하여 FIPS 구성	122
클러스터링 구성	125
재해 복구 가이드	135
프록시 서버 사용	136
SQL Server 구성	139
서버 속성	142
명령줄 인터페이스 옵션	155
XenMobile 콘솔에 대한 워크플로 시작하기	172
인증서 및 인증	176
Citrix Gateway 및 XenMobile	189
도메인 인증 또는 도메인 및 보안 토큰 인증	199
클라이언트 인증서 인증 또는 인증서와 도메인 인증	206
PKI 엔터티	227
자격 증명 공급자	232
APNs 인증서	238
Citrix Files 의 SSO(Single Sign-on) 용 SAML	246
IdP 역할을 하는 Azure Active Directory	256
업그레이드	268
사용자 계정, 역할 및 등록	272
등록 프로필	287
RBAC 를 사용하여 역할 구성	291
알림	307
장치	318

ActiveSync Gateway	325
장치 관리에서 Android Enterprise 로 마이그레이션	328
Android Enterprise	333
Android Enterprise 앱 배포	379
Google Workspace 고객을 위한 레거시 Android Enterprise (이전 명칭 G Suite)	405
iOS	441
macOS	457
Apple 장치의 대량 등록	464
클라이언트 속성	470
Apple 배포 프로그램을 통한 장치 배포	480
장치 등록	491
Firebase Cloud Messaging	511
Apple 교육 기능과 통합	517
Apple 앱 배포	554
네트워크 액세스 제어	579
Samsung Knox	585
Samsung Knox 대량 등록	588
보안 동작	593
XenMobile AutoDiscovery Service	606
장치 정책	610
플랫폼별 장치 정책	623
AirPlay 미러링 장치 정책	624
AirPrint 장치 정책	627
Android Enterprise 앱 권한	627

APN 장치 정책	629
앱 액세스 장치 정책	631
앱 특성 장치 정책	632
앱 구성 장치 정책	633
앱 인벤토리 장치 정책	634
앱 잠금 장치 정책	635
앱 네트워크 사용 장치 정책	638
앱 알림 장치 정책	638
터널 장치 정책	639
앱 제거 장치 정책	641
관리되는 앱 자동 업데이트 장치 정책	642
BitLocker 장치 정책	643
캘린더 (CalDav) 장치 정책	646
셀룰러 장치 정책	648
연결 예약 장치 정책	649
연락처 (CardDAV) 장치 정책	650
OS 업데이트 제어 장치 정책	652
자격 증명 장치 정책	656
사용자 지정 XML 장치 정책	661
Defender 장치 정책	662
장치 상태 증명 장치 정책	664
장치 이름 장치 정책	665
교육 구성 장치 정책	666
Exchange 장치 정책	668

파일 장치 정책	675
FileVault 장치 정책	676
글꼴 장치 정책	678
홈 화면 레이아웃 장치 정책	679
iOS 및 macOS 프로필 장치 정책 가져오기	681
Keyguard 관리 장치 정책	682
키오스크 장치 정책	685
Launcher 구성 장치 정책	686
LDAP 장치 정책	687
위치 장치 정책	689
메일 장치 정책	695
관리되는 구성 정책	697
관리되는 도메인 장치 정책	707
MDM 옵션 장치 정책	708
조직 정보 장치 정책	709
암호 장치 정책	710
개인 핫스팟 장치 정책	719
프로필 제거 장치 정책	719
프로비전 프로필 장치 정책	720
프로비전 프로필 제거 장치 정책	721
프록시 장치 정책	722
제한 장치 정책	723
로밍 장치 정책	756
SCEP 장치 정책	757

Siri 및 받아쓰기 정책	760
SSO 계정 장치 정책	762
스토어 장치 정책	763
구독 캘린더 장치 정책	763
약관 장치 정책	764
VPN 장치 정책	765
배경 화면 장치 정책	793
웹 콘텐츠 필터 장치 정책	794
웹 클립 장치 정책	796
Wi-Fi 장치 정책	797
Windows Information Protection 장치 정책	808
XenMobile 옵션 장치 정책	812
XenMobile 제거 장치 정책	814
앱 추가	815
앱 커넥터 유형	850
MDX 또는 엔터프라이즈 앱 업그레이드	851
Citrix Launcher	852
Apple 볼륨 구매	855
Citrix Secure Hub 를 통한 Virtual Apps and Desktops	858
XenMobile 에서 ShareFile 사용	859
HDX 앱용 SmartAccess	874
미디어 추가	892
리소스 배포	896
매크로	911

자동화된 동작	943
모니터링 및 지원	950
지원 번들의 데이터 익명화	953
연결 확인	954
사용자 환경 개선 프로그램	957
로그	958
모바일 서비스 공급자	965
보고서	966
SNMP 모니터링	971
지원 번들	978
지원 옵션 및 원격 지원	987
Syslog	993
XenMobile 에서 로그 파일 보기	994
REST API	996
Exchange ActiveSync 용 Endpoint Management 커넥터	998
Exchange ActiveSync 용 Citrix Gateway 커넥터	1044
고급 개념	1057
온-프레미스 XenMobile 과 Active Directory 상호 작용	1057
XenMobile 배포	1061
관리 모드	1062
장치 요구 사항	1068
보안 및 사용자 환경	1068
앱	1083
사용자 커뮤니티	1089

전자 메일 전략	1095
XenMobile 통합	1102
다중 사이트 요구 사항	1110
Citrix Gateway 및 Citrix ADC 통합	1111
MDX 앱에 대한 SSO 및 프록시 고려 사항	1121
인증	1126
온-프레미스 배포용 참조 아키텍처	1137
서버 속성	1148
장치 및 앱 정책	1152
사용자 등록 옵션	1161
XenMobile 작업 조정	1163
앱 프로비전 및 프로비전 해제	1170
대시보드 기반 작업	1173
역할 기반 액세스 제어 및 XenMobile 지원	1174
시스템 모니터링	1176
재해 복구	1184
Citrix 지원 프로세스	1187
XenMobile 에서 그룹 등록 초대 보내기	1188
온-프레미스 장치 상태 증명 서버 구성	1190
Secure Mail 푸시 알림을 통한 EWS 의 인증서 기반 인증 구성	1200
XenMobile MDM (모바일 기기 관리) 을 Cisco ISE (ID 서비스 엔진) 와 통합	1203

롤링 패치에 대한 릴리스 정보

November 27, 2023

이 섹션에는 최신 XenMobile Server 롤링 패치에 대한 릴리스 정보가 포함되어 있습니다. 아래 링크를 클릭하여 해결된 문제 및 알려진 문제, 기능 변경 사항, 필요한 작업을 확인하십시오.

최신 롤링 패치에는 동일한 릴리스에 대한 이전 롤링 패치의 모든 수정 사항이 포함되어 있습니다.

현재 릴리스의 패치에 대한 릴리스 정보	게시 날짜	지원 문서
10.15 롤링 패치 5	Nov 13, 2023	CTX583748
10.15 롤링 패치 4	Sep 18, 2023	CTX579528
10.15 롤링 패치 3	Jul 19, 2023	CTX565649
10.15 롤링 패치 2	Apr 26, 2023	CTX546782
10.15 롤링 패치 1	Feb 23, 2023	CTX478719

이전 릴리스의 패치에 대한 릴리스 정보	게시 날짜	지원 문서
10.14 롤링 패치 12	Oct 19, 2023	CTX582535
10.14 롤링 패치 11	May 31, 2023	CTX558678
10.14 롤링 패치 10	Mar 23, 2023	CTX491036
10.14 롤링 패치 9	Dec 20, 2022	CTX477055
10.14 롤링 패치 8	Sep 22, 2022	CTX464099
10.14 롤링 패치 7	Aug 18, 2022	CTX463691
10.14 롤링 패치 6	May 23, 2022	CTX459871
10.14 롤링 패치 5	Mar 30, 2022	CTX399411
10.14 롤링 패치 4	Jan 26, 2022	CTX339069
10.14 롤링 패치 3	Dec 22, 2021	CTX335897
10.14 롤링 패치 2	Dec 15, 2021	CTX335763
10.14 롤링 패치 1	Nov 19, 2021	CTX335342
10.13 롤링 패치 10	Sep 8, 2022	CTX463922
10.13 롤링 패치 9	Jun 14, 2022	CTX460128
10.13 롤링 패치 8	Apr 12, 2022	CTX447596

이전 릴리스의 패치에 대한 릴리스 정보	게시 날짜	지원 문서
10.13 롤링 패치 7	Mar 1, 2022	CTX341602
10.13 롤링 패치 6	Dec 21, 2021	CTX335875
10.13 롤링 패치 5	Dec 15, 2021	CTX335753
10.13 롤링 패치 4	Aug 11, 2021	CTX324159
10.13 롤링 패치 3	May 13, 2021	CTX315034
10.13 롤링 패치 2	Feb 25, 2021	CTX296934
10.13 롤링 패치 1	Jan 8, 2021	CTX289495
10.12 롤링 패치 11	Dec 21, 2021	CTX335861
10.12 롤링 패치 10	Dec 16, 2021	CTX335785
10.12 롤링 패치 9	Oct 8, 2021	CTX331040
10.12 롤링 패치 8	Jun 2, 2021	CTX316910
10.12 롤링 패치 7	Mar 29, 2021	CTX309096
10.12 롤링 패치 6	Jan 26, 2021	CTX292680
10.11 롤링 패치 7	Nov 18, 2020	CTX286435
10.10 롤링 패치 6	Jul 22, 2020	CTX279101

XenMobile Server 10.15 롤링 패치 5 릴리스에 대한 릴리스 정보

November 27, 2023

이 릴리스 노트에서는 XenMobile Server 10.15 롤링 패치 5의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **Android Enterprise** 용 **802.1x** 설정에 새로운 필수 필드 ‘도메인’을 추가했습니다.

802.1x EAP 인증 유형의 Android Enterprise 플랫폼 네트워크 정책 설정 페이지에 새 필드 도메인이 추가되었습니다. 자세한 내용은 [Android Enterprise 용 802.1x 설정](#)을 참조하십시오.

XenMobile Server에는 **Android Enterprise** 용 **802.1x** 설정에 도메인필드를 추가하는 새 `afw.network.domain.support` 속성이 추가되었습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 [서버 속성](#)을 참조

하십시오.

- **iOS** 용 **OS** 업데이트 제어 정책에 새 옵션 '**OS** 업데이트 버전' 이 추가되었습니다.

iOS 플랫폼용 **OS** 업데이트 제어 정책에서 **OS** 업데이트 빈도 필드 뒤에 새 옵션인 **OS** 업데이트 버전이 추가됩니다. 이 옵션을 사용하면 감독되는 iOS 장치를 업데이트하는 데 사용할 OS 버전을 지정할 수 있습니다. 자세한 내용은 [iOS 설정](#)을 참조하십시오.

- **iOS** 용 제한 정책 및 **Exchange** 정책에 새 설정이 추가되었습니다.
 - iOS 용 Exchange 정책에 새 설정 **Mail Drop** 허용이 추가되었습니다. 자세한 내용은 [Exchange 장치 정책 - iOS 설정](#)을 참조하십시오.
 - iOS 용 제한 정책에 다음과 같은 새 설정을 추가했습니다.
 - * 페어링되지 않은 장치로 부팅하여 복구 허용
 - * 신속 보안 대응 설치
 - * 신속 보안 대응 제거
 - * 메일 프라이버시 보호 허용
 - * NFC
 - * 앱 클립 허용
 - * Apple 개인 맞춤형 광고 허용
 - * 자동 잠금 해제

자세한 내용은 [제한 장치 정책 - iOS 설정](#)을 참조하십시오.

- **OS** 업데이트
 - **Android 14** 지원: XenMobile Server 및 Citrix 모바일 생산성 앱은 이제 Android 14 로의 Android Enterprise 장치 업데이트를 지원합니다. 보안 및 개인 정보 보호 혜택에 대한 자세한 내용은 [Android 문서](#)를 참조하십시오.
 - **iOS 17** 지원: XenMobile Server 및 Citrix 모바일 생산성 앱은 이제 iOS 17 과 호환되지만 현재는 새로운 iOS 17 기능을 지원하지 않습니다.

수정된 문제

- XenMobile Server 10.15 RP3 또는 10.15 RP4 로 업그레이드한 후에는 구성 > **Android Enterprise** 용 앱 페이지 > 관리되는 **Google Playstore** 앱에서 앱 구성 버튼을 사용할 수 없습니다. [CXM-112124]
- XenMobile Server 10.15 RP3 또는 10.15 RP4 로 업그레이드한 후 **Android Enterprise** 플랫폼에 대한 Wi-Fi 정책을 구성하는 동안 **CA** 인증서 드롭다운 메뉴에서 어떤 값도 볼 수 없습니다. 인증서 선택 옵션만 표시됩니다. [CXM-112269]

XenMobile Server 10.15.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.15 롤링 패치 4 릴리스에 대한 릴리스 정보

September 26, 2023

이 릴리스 노트에서는 XenMobile Server 10.15 롤링 패치 4의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- 장치 및 앱 보고서에 액세스

이전에는 장치 및 앱 보고서 페이지에 역할 기반 액세스 제어 (RBAC)가 적용되더라도 사용자 그룹에 관계없이 모든 사용자의 모든 장치 및 앱에 대한 정보가 표시되었습니다.

XenMobile Server 10.15 Rolling Patch 4 릴리스부터 장치 및 앱 보고서 페이지에는 RBAC 역할에 관리 권한이 있는 대상 사용자 그룹 구성에 정의된 사용자 그룹과 관련된 장치 및 앱이 표시됩니다. RBAC를 사용하여 역할을 구성하는 방법에 대한 자세한 내용은 [RBAC를 사용한 역할 구성](#)을 참조하십시오.

- **OS 업데이트 제어** 장치 정책을 시스템 기본값으로 재설정하기 위한 지원

XenMobile Server 10.15 롤링 패치 4 릴리스부터 Android Enterprise의 **OS 업데이트 제어** 페이지에 있는 시스템 업데이트 정책 드롭다운 목록에 기본값이라는 새 값이 추가되었습니다. 이 기능을 사용하면 시스템 업데이트 정책을 시스템 기본값으로 재설정할 수 있습니다. 자세한 내용은 [OS 업데이트 제어 장치 정책](#)을 참조하십시오.

- **iOS용 Exchange** 장치 정책 설정에 새 필드 **OAuth 로그인 URL** 및 **OAuth 토큰 요청 URL** 추가

XenMobile Server 10.15 롤링 패치 4 릴리스부터 **OAuth 로그인 URL** 및 **OAuth 토큰 요청 URL** 필드가 **Exchange** 정책 > **iOS** > **OAuth** 사용 라디오 버튼 아래에 추가되었습니다. 자세한 내용은 [Exchange 장치 정책](#)을 참조하십시오.

- **iOS용 Synced Exchange** 서비스 동기화 또는 재정의 지원

XenMobile Server 10.15 롤링 패치 4 릴리스부터 관련 설정을 활성화하여 다음과 같이 iOS용 Synced Exchange 서비스를 동기화할지 아니면 재정의할지 선택할 수 있습니다.

- 일정
- 연락처
- 메일
- 참고
- 미리 알림

자세한 내용은 [Exchange 장치 정책](#)을 참조하십시오.

- **iOS 장치의 eSIM** 지원

XenMobile Server에는 새로운 `ios.esim.support` 속성이 있습니다. 이 속성을 사용하면 XenMobile Server가 iOS 장치에서 eSIM 정보를 가져오고 사용자 인터페이스에 eSIM 관련 장치 속성을 표시할 수 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.15 롤링 패치 3 릴리스에 대한 릴리스 정보

March 15, 2024

이 릴리스 노트에서는 XenMobile Server 10.15 롤링 패치 3의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **XenMobile Server**를 통해 혼합 라이선스 유형을 지원합니다. 이 기능은 고객이 XenMobile Server 또는 Citrix 라이선스 서버를 사용하여 XenMobile 라이선스 유형과 에디션을 혼합하여 활성화할 수 있도록 합니다. 자세한 내용은 [다른 라이선스 활성화하기](#)를 참조하십시오.
- **macOS** 장치에서 엔터프라이즈 앱을 지원합니다. XenMobile Server에는 macOS를 실행하는 장치에서 엔터프라이즈 앱을 지원할 수 있는 새로운 `mac.app.push` 속성이 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.

수정된 문제

- 관리되는 **Google Play** 계정에서 앱을 다운로드할 수 없습니다. [CXM-109786]
- XenMobile Server 콘솔에서는 RSR(신속 보안 대응) 버전을 볼 수 없습니다. [CXM-109928]
- Android 장치에서 사용자가 기존 MDX 톨킷에서 MAM SDK로 전환하면 Secure Mail 앱이 Secure Hub 저장소에서 제거됩니다. [CXM-110266]
- XenMobile Server 10.15 RP2로 업그레이드한 후, 기존 iOS 제한 장치 정책이 “제한된 앱 사용”을 사용하는 경우 해당 정책은 iOS 장치에 배포되지 않습니다. [CXM-110585]

XenMobile Server 10.15 롤링 패치 2 릴리스에 대한 릴리스 정보

September 13, 2023

이 릴리스 노트에서는 XenMobile Server 10.15 롤링 패치 2의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

XenMobile Analyzer 도구의 지원이 중단되었습니다. 릴리스가 안정적인 주기로 자주 이루어지기 때문에 XenMobile Analyzer 도구는 더 이상 필요하지 않습니다. Citrix 는 2023 년 3 월 31 일부터 이 서비스를 중단했습니다. Citrix XenMobile 콘솔 또는 Citrix NetScaler Gateway 에서 제공되는 연결 검사를 사용하는 것이 좋습니다. 자세한 내용은 [연결 검사](#)를 참조하십시오.

수정된 문제

- 알고리즘 APK 서명 체계 v2 이상을 사용하여 Android 플랫폼에서 엔터프라이즈 앱을 구성할 수 없습니다. [CXM-108603]
- NetScaler 에서 nFactor 인증 정책을 사용하는 경우 Android 및 iOS 장치에서 MAM 에 액세스할 수 없습니다. [CXM-108759]
- XenMobile Server 버전 10.14 이상에서 Citrix Gateway 인증의 구성 스크립트를 내보내는 경우 스크립트가 잘려서 작동하지 않습니다. [CXM-108918]
- XenMobile Server 에서는 설명에 **\b** 가 포함되어 있는 동기화된 VPP 앱을 다시 편집할 수 없습니다. [CXM-109029]
- XenMobile Server 버전 10.15 이상에서는 OCSP(온라인 인증서 상태 프로토콜) 가 요청에 응답하지 않습니다. [CXM-109145]
- XenMobile Server 서버에서는 Windows 11 을 실행하는 장치를 등록할 수 없습니다. [CXM-109349]

XenMobile Server 10.15 롤링 패치 1 릴리스에 대한 릴리스 정보

March 2, 2023

이 릴리스 노트에서는 XenMobile Server 10.15 롤링 패치 1 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- 네트워크 액세스 제어 NAC(네트워크 액세스 제어) 솔루션을 사용하여 Android 및 Apple 장치에 대한 XenMobile 장치 보안 평가를 확장할 수 있습니다. NAC 솔루션에서 XenMobile 보안 평가를 사용하여 인증 의사 결정을 지원하고 처리할 수 있습니다. NAC 장비를 구성한 후 XenMobile 에서 구성된 장치 정책 및 NAC 필터가 적용됩니다. 자세한 내용은 [네트워크 액세스 제어](#)를 참조하십시오.
- Secure Hub APN** 인증서 갱신. XenMobile Server 10.15 에 대한 Secure Hub Apple 푸시 알림 서비스 (APN) 인증서가 2023 년 4 월 8 일에 만료됩니다. 이 업데이트는 Secure Hub APN 인증서를 갱신하며, 이 인증서는 2024 년 3 월 12 일에 만료됩니다.

수정된 문제

- Android Enterprise 장치에서 관리형 구성 정책을 편집하거나 배포할 때 오류가 발생합니다. [CXM-107297]
- MAM 전용 모드로 등록된 iOS 장치에서는 Secure Hub 스토어에서 엔터프라이즈 또는 MDX 앱을 설치할 수 없습니다. [CXM-107515]
- 앱의 트랙 ID 를 구성한 후에는 XenMobile Server 콘솔에서 앱의 예상 미리 보기 버전을 볼 수 없습니다. 대신 앱의 프로덕션 버전이 표시됩니다. [CXM-107517]
- Provisioning 프로파일 장치 정책이 보류 상태일 때는 XenMobile Server 에서 Secure Hub 저장소의 MDX 래핑된 앱을 설치할 수 없습니다. [CXM-107573]
- MDM 프로필 갱신 후 ABM 공유 iPad 는 관리되지 않는 상태로 전환됩니다. [CXM-107908]

XenMobile Server 10.14 롤링 패치 12 릴리스에 대한 릴리스 정보

November 1, 2023

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 12 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

수정된 문제

- 관리되는 **Google Play** 계정에서 앱을 다운로드할 수 없습니다. [CXM-110411]
- XenMobile Server 10.14 RP11 로 업그레이드한 후 기존 iOS 제한 정책이 장치에 배포되지 않습니다. [CXM-110596]
- Secure Hub 에 모바일 장치를 등록하면 Secure Hub 스토어 및 관리되는 Google Play 스토어에 앱이 표시되지 않습니다. [CXM-111982]

XenMobile Server 10.14.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.14 롤링 패치 11 릴리스에 대한 릴리스 정보

September 13, 2023

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 11 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

수정된 문제

- 알고리즘 APK 서명 체계 v2 이상을 사용하여 Android 플랫폼에서 엔터프라이즈 앱을 구성할 수 없습니다. [CXM-108605]
- XenMobile Server에서는 설명에 b 가 포함되어 있는 동기화된 VPP 앱을 다시 편집할 수 없습니다. [CXM-109030]
- XenMobile Server 버전 10.14 RP9 이상에서는 OCSP(온라인 인증서 상태 프로토콜)가 요청에 응답하지 않습니다. [CXM-109150]
- XenMobile Server 서버에서는 Windows 11을 실행하는 장치를 등록할 수 없습니다. [CXM-109373]
- XenMobile Server 콘솔에서는 RSR(신속 보안 대응) 버전을 볼 수 없습니다. [CXM-109927]

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.14 롤링 패치 10 릴리스에 대한 릴리스 정보

April 28, 2023

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 10의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **Secure Hub APN** 인증서 갱신. XenMobile Server 10.14에 대한 Secure Hub Apple 푸시 알림 서비스 (APN) 인증서가 2023년 4월 8일에 만료됩니다. 이 업데이트는 Secure Hub APN 인증서를 갱신하며, 이 인증서는 2024년 3월 12일에 만료됩니다.
- **XenMobile Analyzer** 도구의 지원이 중단되었습니다. 릴리스가 안정적인 주기로 자주 이루어지기 때문에 XenMobile Analyzer 도구는 더 이상 필요하지 않습니다. Citrix는 2023년 3월 31일부터 이 서비스를 중단하기로 결정했습니다. Citrix XenMobile 콘솔 또는 Citrix NetScaler Gateway에서 제공되는 연결 검사를 사용하는 것이 좋습니다. 자세한 내용은 [연결 검사](#)를 참조하십시오.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- MDM 프로필 갱신 후 ABM 공유 iPad는 관리되지 않는 상태로 전환됩니다. [CXM-107909]
- MAM 전용 모드로 등록된 iOS 장치에서는 Secure Hub 스토어에서 엔터프라이즈 또는 MDX 앱을 설치할 수 없습니다. [CXM-107939]
- NetScaler에서 nFactor 인증 정책을 사용하는 경우 Android 및 iOS 장치에서 MAM에 액세스할 수 없습니다. [CXM-108747]

- XenMobile Server 버전 10.14 이상에서 Citrix Gateway 인증의 구성 스크립트를 내보내는 경우 스크립트가 잘려서 작동하지 않습니다. [CXM-108919]

XenMobile Server 10.14 롤링 패치 9 릴리스에 대한 릴리스 정보

December 22, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 9의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

네트워크 액세스 제어 NAC(네트워크 액세스 제어) 솔루션을 사용하여 Android 및 Apple 장치에 대한 XenMobile 장치 보안 평가를 확장할 수 있습니다. NAC 솔루션에서 XenMobile 보안 평가를 사용하여 인증 의사 결정을 지원하고 처리할 수 있습니다. NAC 장비를 구성한 후 XenMobile에서 구성된 장치 정책 및 NAC 필터가 적용됩니다. 자세한 내용은 [네트워크 액세스 제어](#)를 참조하십시오.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- XenMobile Server 버전 10.14에서는 라이선스 만료 날짜가 알림 기간에 해당하지 않더라도 라이선스 만료 알림을 받게 됩니다. [CXM-106593]
- 일부 앱에서는 설치된 버전이 최신 버전이더라도 Secure Hub 앱 스토어에 업데이트 보류 중 상태가 표시됩니다. [CXM-106594]
- XenMobile Server에서는 독일어 로케일에서 제한 장치 정책을 만들거나 편집할 수 없습니다. [CXM-106749]
- XenMobile Server 버전 10.14에서는 DEP가 아닌 iOS 장치의 경우 소유자 탭이 공백으로 표시됩니다. [CXM-106762]
- 주체 대체 이름 유형이 없음이 아닌 경우 SCEP 장치 정책이 실패합니다. [CXM-106850]
- Android Enterprise 장치에서 관리형 구성 정책을 편집하거나 배포할 때 오류가 발생합니다. [CXM-107296]
- MAM 전용 모드로 등록된 iOS 장치에서는 Secure Hub 앱 스토어에서 엔터프라이즈 또는 MDX 앱을 설치할 수 없습니다. [CXM-107513]
- 앱의 트랙 ID를 구성한 후에는 XenMobile Server 콘솔에서 앱의 예상 미리 보기 버전을 볼 수 없습니다. 대신 앱의 프로덕션 버전이 표시됩니다. [CXM-107514]
- Provisioning 프로필 장치 정책이 보류 상태일 때는 XenMobile Server에서 Secure Hub 저장소의 MDX 래핑된 앱을 설치할 수 없습니다. [CXM-107570]

XenMobile Server 10.14 롤링 패치 8 릴리스에 대한 릴리스 정보

November 1, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 8의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

Windows Information Protection 정책에 대한 지원이 중단되었습니다. Windows [발표](#)에 따라 XenMobile Server는 Windows Information Protection(WIP)에 대한 지원을 중단했습니다. **windows.wip.deprecation**이라는 서버 속성을 추가하여 WIP에 대한 지원을 중단했으며, 이 속성은 기본적으로 **True**로 설정되어 있습니다. 자세한 내용은 [서버 속성](#)을 참조하십시오. [CXM-106445]

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- XenMobile Server에서는 독일어 로케일로 관리되는 앱 자동 업데이트 정책을 만들거나 편집할 수 없습니다. [CXM-106562]

XenMobile Server 10.14 롤링 패치 7 릴리스에 대한 릴리스 정보

August 24, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 7의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **OS 업데이트**
 - **iOS 16** 지원. XenMobile Server 및 Citrix 모바일 생산성 앱은 iOS 16과 호환되지만 현재는 새로운 iOS 16 기능을 지원하지 않습니다.
 - **Android 13** 지원. 이제 XenMobile Server에서 Android 13에 대한 Android Enterprise 장치 업데이트를 지원합니다. 보안 및 개인 정보 보호 혜택에 대한 요약은 [Android 문서](#)를 참조하십시오.
- 사용되지 않는 기능. 이제 다음 기능이 지원되지 않습니다.

- RBAC 역할 - 공유 및 COSU 장치 등록자 [CXM-104826]
- Android - Sony 및 HTC [CXM-104827]
- 높은 보안 등록 모드 [CXM-104828]
- 파생된 자격 증명 [CXM-104829]
- SEAMS [CXM-104833]
- Windows Phone 장치 [CXM-104834], [CXM-104835]
- 일반, DigiCert 관리형 및 Entrust 어댑터 PKI 엔터티. [CXM-104990]

자세한 내용은 [지원 중단](#)을 참조하십시오.

- 모바일 서비스 공급자 (**MSP**) 인터페이스에 대한 지원이 중단되었습니다. 콘솔에서 MSP 인터페이스를 제거하는 새로운 서버 속성 (`deprecate.mobile.service.provider`) 을 추가하고 MSP 에 대한 지원은 중단했으며, 이 속성은 기본적으로 **True** 로 설정되어 있습니다. 자세한 내용은 [서버 속성](#)을 참조하십시오. [CXM-104836]
- **Windows 10** 장치에 대한 **Wi-Fi** 감지 핫스팟 자동 연결 제한 허용 지원을 제거합니다. 자세한 내용은 [Windows 데스크톱/태블릿 설정](#)을 참조하십시오. [CXM-104839]
- **Nexmo SMS** 게이트웨이에 대한 지원이 중단되었습니다. 새로운 서버 속성 (`deprecate.carrier.sms.gateway`) 을 추가하고 Nexmo SMS 에 대한 지원은 중단했으며, 이 속성은 기본적으로 **True** 로 설정되어 있습니다. Nexmo SMS 는 자가 지원 포털에서도 더 이상 사용되지 않습니다. 자세한 내용은 [알림](#)을 참조하십시오. [CXM-104840]
- **Google** 의 **API** 지원 중단. Google 은 XenMobile Server 에서 앱 카테고리 및 라이선스에 사용되는 여러 API 를 더 이상 지원하지 않습니다. 다음과 같은 변경 사항이 적용됩니다.
 - 이제 승인하지 않고 추가할 앱을 선택합니다. [관리되는 앱 스토어 앱](#)을 참조하십시오.
 - 이제 앱을 카테고리가 아닌 컬렉션으로 구성할 수 있습니다. [앱 구성](#)을 참조하십시오.
 - 더 이상 사용자로부터 앱 라이선스를 분리할 수 없습니다. [앱 추가](#)를 참조하십시오. [CXM-105835]
- **Android Enterprise** 관리형 앱을 자동으로 업데이트하도록 우선 순위를 구성합니다. Android Enterprise 관리형 앱을 낮은 우선 순위로 자동 업데이트할지 아니면 높은 우선 순위로 업데이트할지를 지정합니다. 자동 업데이트를 연기할 수도 있습니다. 자세한 내용은 [관리되는 앱 자동 업데이트 장치 정책](#)을 참조하십시오. [CXM-105837]

XenMobile Server 10.14.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- Google Play 에서 일부 공용 앱을 사용할 수 없는 경우 Android 를 실행하는 일부 기기에서는 Secure Hub 에 액세스할 수 없습니다. [CXM-105492]
- SSL 인증서 갱신 후 특정 macOS 장치에서는 설치된 프로필 및 인증서가 자동으로 제거됩니다. [CXM-105759]
- XenMobile Server 콘솔에서는 이름에 / 기호가 있는 제한 장치 정책을 편집할 수 없습니다. [CXM-105828]
- 출시된 DEP 장치는 XenMobile Server 콘솔에 계속 표시됩니다. [CXM-105905]

- Secure Hub 스토어에 액세스할 수 없습니다. 다음 오류가 발생합니다. 로그인에 만료되었습니다. 계속하려면 다시 로그인하십시오. [CXM-106054]

XenMobile Server 10.14 롤링 패치 6 릴리스에 대한 릴리스 정보

May 26, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 6의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

새 제한 정책이 추가되었습니다. 작업 프로필에서 복사 및 붙여넣기 허용 및 개인 프로필에서 데이터 공유 허용을 제한 정책에 추가했습니다. 개인 프로필에서 작업 프로필로 복사, 붙여넣기 및 가져오기를 제한하려면 이러한 정책을 꺼짐으로 설정합니다. 자세한 내용은 [제한 장치 정책](#)을 참조하십시오. [CXM-104599]

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- XenMobile Server에서 일부 VPP 앱의 올바른 버전이 자동으로 업데이트되지 않습니다. [CXM-104329]
- XenMobile Server 버전 10.14에서는 특정 Active Directory 사용자를 삭제할 수 없습니다. [CXM-105176]
- iOS 15를 실행하는 장치를 새로 등록할 때 연결 유형이 **AlwaysOn IKEv2** 이중 구성으로 설정된 경우 VPN 정책 배포가 실패합니다. [CXM-105181]

XenMobile Server 10.14 롤링 패치 5 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 5의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **Google Analytics**를 활성화합니다. XenMobile Server에서 Google Analytics를 활성화하려면 **xms.ga.enabled** 서버 속성의 값을 **True**로 설정합니다. 기본값은 **True**입니다. [CXM-104006]

- **Secure Hub APN** 인증서 갱신. XenMobile Server 10.14 에 대한 Secure Hub Apple 푸시 알림 서비스 (APN) 인증서가 2022 년 5 월 7 일에 만료됩니다. 이 업데이트는 Secure Hub APN 인증서를 갱신하며, 이 인증서는 2023 년 4 월 8 일에 만료됩니다. [CXM-104194]

XenMobile Server 10.14.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- 장치의 CA 갱신 이후 XenMobile Server 에서 장치 인증서 발급자 CA 가 업데이트되지 않습니다. [CXM-104234]
- 일부 장치의 SQL 데이터베이스에는 두 개의 인증서 항목이 있어 오류가 발생합니다. [CXM-104296]
- XenMobile Server 버전 10.14 에서는 프로필 장치 프로비저닝 정책을 편집할 수 없습니다. [CXM-104461]
- XenMobile Server 에서 ShareFile Enterprise 를 커넥터로 변경할 때 배달 그룹 아래에서 GUI 가 업데이트되지 않습니다. [CXM-104470]

XenMobile Server 10.14 롤링 패치 4 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 4 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

WSDL 서비스를 사용하도록 설정합니다. XenMobile 서버에서 WSDL 서비스를 사용하도록 설정하려면 서버 속성 값 `wSDL.service.enabled`을 **True** 로 설정합니다. ActiveSync 게이트웨이 커넥터를 사용할 때 필요합니다. 기본값은 **False** 입니다. [CXM-103017]

XenMobile Server 10.14.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- 일부 Android Enterprise 장치에서는 배달 그룹 및 할당된 정책 또는 앱이 간헐적으로 적용되지 않습니다. [CXM-102044]
- XenMobile Server 버전 10.13 에서는 StorageZone 커넥터만 사용하여 StorageZone 컨트롤러를 연결하고 구성할 수 없습니다. [CXM-102661]
- MDM 전용 모드로 등록된 iOS 장치에서는 Secure Hub 가 App Store 에서 연 브라우저를 통해 앱을 추가할 수 없습니다. 다음 오류가 발생합니다. 로그인이 만료되었습니다. 계속하려면 다시 로그인하십시오. [CXM-102664]

- XenMobile Server 버전 10.13 RP1 이상에서는 SNMP 모니터링의 XenMobile 노드 간 연결 트랩이 작동하지 않습니다. [CXM-102753]
- XenMobile Server 에서 잘못된 시간이 W-SU 시간대에 표시됩니다. [CXM-102856]

XenMobile Server 10.14 롤링 패치 3 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 3 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

이 릴리스에는 버그 수정이 포함되어 있습니다.

XenMobile Server 10.14.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.14 롤링 패치 2 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 2 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

XenMobile Server 10.14.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

해결된 문제

XenMobile Server 에서는 사용량이 많은 시간에 서버 노드의 높은 CPU 사용률을 확인할 수 있습니다. [CXM-102568]

XenMobile Server 10.14 롤링 패치 1 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.14 롤링 패치 1 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **Windows 10** 장치를 지원합니다. 이제 XenMobile 을 사용하여 Windows 11 장치를 관리할 수 있습니다. 자세한 내용은 [운영 체제 지원 목록](#)을 참조하십시오. [CXM-99999]
- **macOS** 의 연결 모드 및 네트워크 우선 순위를 구성합니다. Wi-Fi 장치 정책에서 macOS 장치에 대한 연결 모드 설정을 활성화하여 사용자가 네트워크에 참여하는 방법을 선택합니다. 장치는 로그인 창에 입력한 시스템 자격 증명 또는 자격 증명을 통해 사용자를 인증할 수 있습니다. 네트워크가 여러 개인 경우 우선 순위 필드에 숫자를 입력하여 네트워크 연결의 우선 순위를 설정합니다. 장치는 번호가 가장 낮은 네트워크를 선택합니다. 자세한 내용은 [Wi-Fi 장치 정책](#)의 macOS 설정을 참조하십시오. [CXM-100879]
- Google 의 Android Enterprise 장치에서 그룹 라이선스에 대한 지원이 중단되므로 XenMobile Server 에서 그룹 라이선스를 Google 에 동기화할 수 없습니다. 자세한 내용은 [이 문서](#)를 참조하십시오. [CXM-101209]

알려진 문제

등록된 장치 중 macOS 11 이전 버전에서 macOS 12 로 업그레이드된 장치 또는 macOS 12 에 새로 등록된 장치는 장치의 시스템 환경설정 > 프로필에 “확인되지 않음” 으로 표시될 수 있습니다. 자세한 내용과 해결 방법은 이 [지원 문서](#)를 참조하십시오. [CXM-101843]

수정된 문제

- iOS 15 또는 macOS 12 장치를 등록한 후 MDM 구성 프로필에 확인되지 않음으로 표시됩니다. [CXM-99379]
- XenMobile Server 콘솔에서 앱의 설정을 수정하여 모든 플랫폼의 선택을 취소하고 저장하면 해당 앱이 구성 > 앱에 나열되지 않습니다. [CXM-99851]
- Android Enterprise 플랫폼에서 Citrix Launcher 를 종료할 수 없습니다. 다음 오류가 발생합니다. 암호가 잘못되었습니다. [CXM-100975]
- XenMobile Server 버전 10.14 에서는 iOS 및 macOS 프로필 가져오기 정책을 편집할 수 없습니다. [CXM-102393]

XenMobile Server 10.13 롤링 패치 10 릴리스에 대한 릴리스 정보

November 1, 2022

이 릴리스 노트에서는 XenMobile Server 10.13 롤링 패치 10 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **OS 업데이트**
 - **iOS 16** 지원. XenMobile Server 및 Citrix 모바일 생산성 앱은 iOS 16 과 호환되지만 현재는 새로운 iOS 16 기능을 지원하지 않습니다.
 - **Android 13** 지원. 이제 XenMobile Server 에서 Android 13 에 대한 Android Enterprise 장치 업데이트를 지원합니다. 보안 및 개인 정보 보호 혜택에 대한 요약은 [Android 문서](#)를 참조하십시오.
- **Google 의 API** 지원 중단. Google 은 XenMobile Server 에서 앱 카테고리 및 라이선스에 사용되는 여러 API 를 더 이상 지원하지 않습니다. 다음과 같은 변경 사항이 적용됩니다.
 - 이제 승인하지 않고 추가할 앱을 선택합니다. [관리되는 앱 스토어 앱](#)을 참조하십시오.
 - 이제 앱을 카테고리가 아닌 컬렉션으로 구성할 수 있습니다. [앱 구성](#)을 참조하십시오.
 - 더 이상 사용자로부터 앱 라이선스를 분리할 수 없습니다. [앱 추가](#)를 참조하십시오. [CXM-105986]

XenMobile Server 10.13.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- SSL 인증서 갱신 후 특정 macOS 장치에서는 설치된 프로필 및 인증서가 자동으로 제거됩니다. [CXM-105813]
- XenMobile Server 콘솔에서는 이름에 / 기호가 있는 제한 장치 정책을 편집할 수 없습니다. [CXM-105834]
- 출시된 DEP 장치는 XenMobile Server 콘솔에 계속 표시됩니다. [CXM-105906]
- Secure Hub 스토어에 액세스할 수 없습니다. 다음 오류가 발생합니다. 로그인에 만료되었습니다. 계속하려면 다시 로그인하십시오. [CXM-106062]

XenMobile Server 10.13 롤링 패치 9 릴리스에 대한 릴리스 정보

June 17, 2022

이 릴리스 노트에서는 XenMobile Server 10.13 롤링 패치 9 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- 새 제한 정책이 추가되었습니다. 작업 프로필에서 복사 및 붙여넣기 허용 및 개인 프로필에서 데이터 공유 허용을 제한 정책에 추가했습니다. 개인 프로필에서 작업 프로필로 복사, 붙여넣기 및 가져오기를 제한하려면 이러한 정책을 꺼짐으로 설정합니다. 자세한 내용은 [제한 장치 정책](#)을 참조하십시오. [CXM-104600]

XenMobile Server 10.13.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- XenMobile Server 에서 ShareFile Enterprise 를 커넥터로 변경할 때 배달 그룹 아래에서 GUI 가 업데이트되지 않습니다. [CXM-104476]
- 장치의 CA 갱신 이후 XenMobile Server 에서 장치 인증서 발급자 CA 가 업데이트되지 않습니다. [CXM-104545]
- XenMobile Server 버전 10.13 에서는 특정 Active Directory 사용자를 삭제할 수 없습니다. [CXM-105177]
- iOS 15 를 실행하는 장치를 새로 등록할 때 연결 유형이 **AlwaysOn IKEv2** 이중 구성으로 설정된 경우 VPN 정책 배포가 실패합니다. [CXM-105195]

XenMobile Server 10.13 롤링 패치 8 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.13 롤링 패치 8 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- 로컬 사용자가 약한 암호를 사용하지 못하도록 암호 유효성 검사를 활성화합니다. `enable.password.strength.validation` 을 `true` 로 설정하면 약한 암호를 사용하는 로컬 사용자를 추가할 수 없습니다. `false` 로 설정하면 약한 암호로 로컬 사용자를 만들 수 있습니다. 기본값은 `true` 입니다. [CXM-104085]
- **Secure Hub APN** 인증서 갱신. XenMobile Server 10.13 에 대한 Secure Hub Apple 푸시 알림 서비스 (APN) 인증서가 2022 년 5 월 7 일에 만료됩니다. 이 업데이트는 Secure Hub APN 인증서를 갱신하며, 이 인증서는 2023 년 4 월 8 일에 만료됩니다. [CXM-104195]

XenMobile Server 10.13.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#) 를 참조하십시오.

수정된 문제

- 일부 장치의 SQL 데이터베이스에는 두 개의 인증서 항목이 있어 오류가 발생합니다. [CXM-104297]
- XenMobile Server 에서 일부 VPP 앱의 올바른 버전이 자동으로 업데이트되지 않습니다. [CXM-104330]
- XenMobile Server 버전 10.13 에서는 프로필 장치 프로비저닝 정책을 편집할 수 없습니다. [CXM-104464]

XenMobile Server 10.13 롤링 패치 7 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.13 롤링 패치 7의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

- **WSDL** 서비스를 사용하도록 설정합니다. XenMobile 서버에서 WSDL 서비스를 사용하도록 설정하려면 서버 속성 값 `wSDL.service.enabled`을 **True**로 설정합니다. ActiveSync 게이트웨이 커넥터를 사용할 때 필요합니다. 기본값은 **False**입니다. [CXM-103131]
- **Google Analytics**를 활성화합니다. XenMobile Server에서 Google Analytics를 활성화하려면 `xms.ga.enabled` 서버 속성의 값을 **True**로 설정합니다. 기본값은 **True**입니다. [CXM-103823]

XenMobile Server 10.13.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

XenMobile Server에서 잘못된 시간이 W-SU 시간대에 표시됩니다. [CXM-102922]

XenMobile Server 10.13 롤링 패치 6 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.13 롤링 패치 6의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

이 릴리스에는 버그 수정이 포함되어 있습니다.

XenMobile Server 10.13.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.13 롤링 패치 4 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.13 롤링 패치 4의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

Android 12 를 지원합니다. 이제 XenMobile Server 에서 Android 12 에 대한 Android Enterprise 장치 업데이트를 지원합니다. 보안 및 개인 정보 보호 혜택에 대한 요약은 [Android 문서](#)를 참조하십시오.

XenMobile Server 10.13.0 의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

수정된 문제

- APN 용 HTTP/2 기반 API 로 전환하면 `ios.mdm.apns.connectionPoolSize` 서버 속성이 숨겨집니다. [CXM-95479]
- XenMobile Server 버전 10.12 에서는 특정 앱의 VPP 속성을 수정할 수 없습니다. [CXM-96854]
- 필요한 웹 앱이 MDM 전용 장치에 자동으로 설치되지 않습니다. [CXM-97477]
- XenMobile Server 버전 10.13 에서는 **CLI** 아래에서 프록시 서버를 구성할 때 iOS 장치에서 실행 중인 Secure Hub 로 알림을 보낼 수 없습니다. [CXM-97807]
- XenMobile Server 버전 10.13 에서 장치 세부 정보에 액세스하는 동안 오류가 발생합니다. 이 오류는 장치 속성에 ” “의 값이 있는 경우 발생합니다. [CXM-97951]

XenMobile Server 10.13 롤링 패치 3 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.13 롤링 패치 3 의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

Secure Hub APN 인증서 갱신. XenMobile Server 10.13 에 대한 Secure Hub APNs(Apple 푸시 알림 서비스) 인증서가 2021 년 6 월 17 일에 만료됩니다. 이 업데이트는 Secure Hub APN 인증서를 갱신하며, 이 인증서는 2022 년 5 월 7 일에 만료됩니다. [CXM-94070]

APN 알림에 대한 대체 포트. 이제 XenMobile Server 포트 443 의 대안으로 포트 2197 을 사용할 수 있도록 지원합니다. 포트 2197 을 사용하여 `api.push.apple.com`에 APN 알림을 보내고 이로부터 피드백을 받을 수 있습니다. 포트는 HTTP/2 기반 APN 공급자 API 를 사용합니다. 서버 속성 `apns.http2.alternate.port.enabled`의 기본 값은 `false`입니다. 대체 포트를 사용하려면 서버 속성을 업데이트한 다음 서버를 다시 시작하십시오. [CXM-93911]

수정된 문제

macOS 10.14 이상을 실행하는 장치를 등록한 직후 XenMobile Server 콘솔에 장치 속성이 항상 채워지는 것은 아닙니다. 장치를 다시 시작하고 나면 장치 속성이 예상대로 나타납니다. [CXM-94150]

제한 정책에서 동일한 앱에 대해 시스템 앱 활성화 및 애플리케이션 비활성화 설정을 모두 활성화하면 앱이 작업 프로필에 나타납니다. [CXM-94097]

XenMobile Server 콘솔에 SNMP 사용자를 추가하면 **SNMP** 모니터링 사용자 목록에 사용자가 나타나지 않거나 SNMP 에이전트가 비활성화됩니다. [CXM-93199]

XenMobile Server에서 NetScaler Gateway 연결 확인에 결과가 표시되지 않습니다. [CXM-93134]

XenMobile Server 콘솔에 올바른 루트 인증서 만료 날짜가 표시되지 않습니다. [CXM-93133]

XenMobile Server 10.12 롤링 패치 11 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.12 롤링 패치 11의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

이 릴리스에는 버그 수정이 포함되어 있습니다.

XenMobile Server 10.12.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.12 롤링 패치 10 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.12 롤링 패치 10의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

이 릴리스에는 버그 수정이 포함되어 있습니다.

XenMobile Server 10.12.0의 이전 롤링 패치에 대한 자세한 내용은 [롤링 패치에 대한 릴리스 정보](#)를 참조하십시오.

XenMobile Server 10.12 롤링 패치 9 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.12 롤링 패치 9의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

Android 12를 지원합니다. XenMobile Server는 Android Enterprise 장치에서 Android 12를 지원합니다. 보안 및 개인 정보 보호 혜택에 대한 요약은 [Android](#)에 대한 Google 설명서를 참조하십시오. [CXM-97765]

Windows 10 장치를 지원합니다. 이제 XenMobile Server를 사용하여 Windows 11 장치를 관리할 수 있습니다. 자세한 내용은 [운영 체제 지원 목록](#)을 참조하십시오. [CXM-99995]

수정된 문제

앱 자동 업데이트 설정이 비활성화되면 기기에 설치된 Apple 볼륨 구매 앱이 최신 버전으로 자동 업데이트됩니다. [CXM-95985]

XenMobile Server 버전 10.12에서 장치 세부 정보에 액세스하는 동안 오류가 발생합니다. 이 오류는 장치 속성에 ”의 값이 있는 경우 발생합니다. [CXM-97953]

XenMobile Server 콘솔에서 앱의 설정을 수정하여 모든 플랫폼의 선택을 취소하고 저장하면 해당 앱이 구성 > 앱에 나열되지 않습니다. [CXM-99708]

XenMobile Server 10.12 롤링 패치 8 릴리스에 대한 릴리스 정보

May 6, 2022

이 릴리스 노트에서는 XenMobile Server 10.12 롤링 패치 8의 향상된 기능 및 해결된 문제와 알려진 문제에 대해 설명합니다.

새로운 항목

Secure Hub APN 인증서 갱신. XenMobile Server 10.12에 대한 Secure Hub APNs(Apple 푸시 알림 서비스) 인증서가 2021년 6월 17일에 만료됩니다. 이 업데이트는 Secure Hub APN 인증서를 갱신하며, 이 인증서는 2022년 5월 7일에 만료됩니다. [CXM-94513]

수정된 문제

- macOS 10.14 이상을 실행하는 장치를 등록한 직후 XenMobile Server 콘솔에 장치 속성이 항상 채워지는 것은 아닙니다. 장치를 다시 시작하고 나면 장치 속성이 예상대로 나타납니다. [CXM-94221]

- XenMobile Server 10.12 에서 ShareFile 가 간헐적으로 연결을 설정하는 데 실패합니다. [CXM-95419]

XenMobile Server 10.15 의 새로운 기능

March 15, 2024

Citrix ADC 에서 지원 중단되는 클래식 정책에 대한 지속적인 지원

Citrix 는 최근 Citrix ADC 12.0 빌드 56.20 부터 클래식 정책 기반 기능의 일부를 지원 중단한다고 발표했습니다. Citrix ADC 지원 중단 고지는 Citrix Gateway 와의 기존 XenMobile Server 통합에는 영향을 주지 않습니다. XenMobile Server 는 클래식 정책을 계속 지원하므로 별도의 작업이 필요하지 않습니다.

XenMobile 마이그레이션 서비스

XenMobile Server 를 온-프레미스에서 사용하는 경우 무료 XenMobile 마이그레이션 서비스를 사용하여 Endpoint Management 를 시작할 수 있습니다. XenMobile Server 에서 Citrix Endpoint Management 로 마이그레이션할 때 장치를 재등록할 필요는 없습니다.

마이그레이션을 시작하려면 해당 지역의 Citrix 영업 사원 또는 Citrix 파트너에게 문의하십시오. [XenMobile 마이그레이션 서비스](#)를 참조하십시오.

사용 중단 발표

단계적으로 중단되는 Citrix XenMobile 기능에 대한 고급 알림은 [사용 중단](#)을 참조하십시오.

엔드포인트를 iOS 14.5 로 업그레이드하기 전에

Citrix 는 엔드포인트를 iOS 14.5 로 업그레이드하기 전에 다음 작업을 수행하여 앱 충돌을 완화할 것을 권장합니다.

- Citrix Secure Mail 및 Secure Web 을 21.2.X 이상으로 업그레이드합니다. [MDX 또는 엔터프라이즈 앱 업그레이드](#)를 참조하십시오.
- MDX Toolkit 을 사용하는 경우 MDX Toolkit 21.3.X 이상으로 모든 타사 iOS 애플리케이션을 래핑합니다. 최신 버전은 MDX Toolkit [다운로드 페이지](#)를 확인하십시오.

온-프레미스 Citrix ADC 를 업그레이드하기 전에

온-프레미스 Citrix ADC 를 특정 버전으로 업그레이드하면 Single Sign-on 오류가 발생할 수 있습니다. 회사 직원 로그인 옵션이 있는 브라우저에서 Citrix Files 또는 ShareFile 도메인 URL 에 Single Sign-on 으로 인해 오류가 발생합니다. 사용자가 로그인할 수 없습니다.

이 문제의 해결 방법: Citrix Gateway 의 ADC CLI 에서 다음 명령을 아직 실행하지 않은 경우 명령을 실행하여 전역 SSO 를 사용하도록 설정합니다.

```
1 `set vpn parameter SSO ON`  
2 `bind vpn vs <vsName> -portalTheme X1`
```

자세한 내용은 다음을 참조하십시오.

- [Citrix ADC 릴리스 \(Feature Phase\) 13.1 빌드 33.52](#)
- [영향을 받는 SSO 구성](#)

문제 해결을 완료한 후 사용자는 회사 직원 로그인 옵션이 제공되는 브라우저에서 SSO 를 사용하여 Citrix Files 또는 ShareFile 도메인 URL 에 인증할 수 있습니다. [CXM-88400]

XenMobile 10.15 로 업그레이드하기 전에 (온-프레미스)

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 [시스템 요구 사항 및 호환성](#)과 [XenMobile 호환성](#)을 참조하십시오.

1. 업그레이드할 XenMobile Server 를 실행하는 가상 컴퓨터의 RAM 이 8GB 미만인 경우 8GB 이상으로 RAM 을 늘리는 것이 좋습니다.
2. 최신 버전의 XenMobile Server 10.15 로 업데이트하기 전에 Citrix License Server 를 11.17 이상으로 업데이트하십시오.

최신 버전의 XenMobile 에는 Citrix License Server 11.17(최소 버전) 이 필요합니다.

참고:

XenMobile 10.15 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2022 년 11 월 15 일입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 이후여야 합니다.

날짜는 라이선스 서버의 라이선스 옆에서 볼 수 있습니다. 최신 버전의 XenMobile 을 이전 버전의 라이선스 서버 환경에 연결하면 연결 확인이 실패하고 라이선스 서버를 구성할 수 없게 됩니다.

라이선스의 날짜를 갱신하려면 Citrix 포털에서 최신 라이선스 파일을 다운로드하고 라이선스 서버에 파일을 업로드하십시오. [Customer Success Services](#)를 참조하십시오.

3. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 iOS 정책 및 앱을 배포하려면 다음과 같은 요구 사항이 충족되어야 합니다. Citrix Gateway 에 SSL 지속성이 구성되어 있으면 모든 XenMobile Server 노드에서 포트 80 을 열어야 합니다.

4. XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

이번 릴리스에서 XenMobile은 VMware ESXi 7.0을 지원합니다. ESXi 7.0을 설치하거나 업그레이드하기 전에 10.14 이상으로 업그레이드해야 합니다.

XenMobile 10.14.x 또는 10.13.x에서 직접 XenMobile 10.15로 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 이진 파일을 다운로드합니다. <https://www.citrix.com/downloads>로 이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server > 제품 소프트웨어 > XenMobile Server 10**으로 이동합니다. 해당하는 하이퍼바이저에 대한 XenMobile Server 소프트웨어 타일에서 파일 다운로드를 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다. [릴리스 관리 페이지를 사용하여 업그레이드하려면](#)을 참조하십시오.

업그레이드 후

연결 구성을 변경하지 않았는데도 발신 연결이 관련된 기능이 작동을 중지하는 경우 XenMobile Server 로그에 다음과 같은 오류가 있는지 확인하십시오. “VPP Server에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’이 피어가 제공한 인증서 제목과 일치하지 않습니다.”

- 이 인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 유효성 검사를 비활성화해야 함을 나타냅니다.
- 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다.
- 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 `disable.hostname.verification`을 `true`로 변경하십시오. 이 속성의 기본값은 `false`입니다.

플랫폼 업데이트

iOS 16 지원. XenMobile Server 및 Citrix 모바일 생산성 앱은 iOS 16과 호환되지만 현재는 새로운 iOS 16 기능을 지원하지 않습니다.

Android 13 지원. XenMobile Server는 Android 13에 대한 Android Enterprise 장치 업데이트를 지원합니다. 보안 및 개인 정보 보호 혜택에 대한 요약은 [Android 문서](#)를 참조하십시오.

Windows 10 장치를 지원합니다. 이제 XenMobile을 사용하여 Windows 11 장치를 관리할 수 있습니다. 자세한 내용은 [운영 체제 지원 목록](#)을 참조하십시오.

macOS의 연결 모드 및 네트워크 우선 순위 구성

Wi-Fi 장치 정책에서 macOS 장치에 대한 연결 모드 설정을 활성화하여 사용자가 네트워크에 참여하는 방법을 선택합니다. 장치는 로그인 창에 입력한 시스템 자격 증명 또는 자격 증명을 통해 사용자를 인증할 수 있습니다. 네트워크가 여러 개인 경우 우선

순위 필드에 숫자를 입력하여 네트워크 연결의 우선 순위를 설정합니다. 장치는 번호가 가장 낮은 네트워크를 선택합니다. 자세한 내용은 [Wi-Fi 장치 정책](#)의 macOS 설정을 참조하십시오.

Android Enterprise 관리형 앱을 자동으로 업데이트하도록 우선 순위를 구성합니다

Android Enterprise 관리형 앱을 낮은 우선 순위로 자동 업데이트할지 아니면 높은 우선 순위로 업데이트할지를 지정합니다. 자동 업데이트를 연기할 수도 있습니다. 자세한 내용은 [관리되는 앱 자동 업데이트 장치 정책](#)을 참조하십시오.

Citrix Hypervisor 버전 8.2 CU1 이상에서 하드웨어 가상화 모드 (HVM) 이미지 사용

Citrix Hypervisor 버전 8.2 CU1 이상에서는 더 이상 반가상화 (PV) VM 을 지원하지 않습니다. 자세한 내용은 [누적 업데이트 1](#)을 참조하십시오.

XenMobile Server 버전 10.15 부터 하드웨어 가상화 모드 (HVM) 가 지원됩니다. XenMobile Server 를 새로 설치하려면 citrix.com 에서 HVM xva 이미지를 다운로드하십시오. 기존 XenMobile Server 환경의 경우 PV 에서 HVM 게스트로 마이그레이션하는 단계를 따르십시오. HVM 게스트 이미지는 XenMobile Server 버전 10.15 이상에서 citrix.com 을 통해 사용할 수 있습니다.

사전 요구 사항

- 클러스터가 활성화되어 있고 데이터베이스가 원격인지 확인합니다.
- 백업으로 이전 PV 노드를 유지하거나 스냅샷을 저장합니다. PV 노드가 XenMobile Server 버전 10.14 또는 10.13 에 있는 경우 데이터베이스도 백업합니다.
- 마이그레이션하기 전에 새 HVM 노드로 이전되지 않는 이전 PV 노드에서 지원 번들을 다운로드합니다.

마이그레이션 단계

1. XenMobile Server 10.15 HVM xva 이미지를 다운로드합니다.
2. 기존 PV 게스트 노드를 종료합니다.
3. Citrix Hypervisor 에서 새 HVM 노드를 부팅합니다.
4. 기존 클러스터의 서버 PKI 키 저장소 암호와 함께 이전 노드와 동일한 데이터베이스 설정을 사용하여 XenMobile Server 10.15 노드를 구성합니다.
5. 필요한 경우 Citrix Gateway 설정을 업데이트합니다.

참고:

마이그레이션 중에 오류가 발생하면 동일한 버전 데이터베이스를 사용하여 이전 PV 노드를 부팅합니다.

중요:

XenMobile PV 게스트에 대해서는 `/opt/xensource/bin/pv2hvm` 명령을 실행하지 마십시오. 이로 인해 VM 부팅이 실패합니다.

Google Analytics 사용

XenMobile Server 에서 Google Analytics 를 활성화하려면 `xms.ga.enabled` 서버 속성의 값을 **True** 로 설정합니다. 기본값은 **True** 입니다.

새 제한 정책 추가됨

작업 프로필에서 복사 및 붙여넣기 허용 및 개인 프로필에서 데이터 공유 허용을 제한 정책에 추가했습니다. 개인 프로필에서 작업 프로필로 복사, 붙여넣기 및 가져오기를 제한하려면 이러한 정책을 꺼짐으로 설정합니다. 자세한 내용은 [제한 장치 정책](#)을 참조하십시오.

Secure Hub APN 인증서 갱신

XenMobile Server 에 대한 Secure Hub Apple 푸시 알림 서비스 (APN) 인증서가 2022 년 5 월 7 일에 만료됩니다. 이 업데이트는 Secure Hub APN 인증서를 갱신하며, 이 인증서는 2023 년 4 월 8 일에 만료됩니다.

지원 중단 및 제거

- **Google 의 API** 지원 중단. Google 은 XenMobile Server 에서 앱 카테고리 및 라이선스에 사용되는 여러 API 를 더 이상 지원하지 않습니다. 다음과 같은 변경 사항이 적용됩니다.
 - 이제 승인하지 않고 추가할 앱을 선택합니다. [관리되는 앱 스토어 앱](#)을 참조하십시오.
 - 이제 앱을 카테고리가 아닌 컬렉션으로 구성할 수 있습니다. [앱 구성](#)을 참조하십시오.
 - 더 이상 사용자로부터 앱 라이선스를 분리할 수 없습니다. [앱 추가](#)를 참조하십시오.
- **Windows Information Protection** 정 책 에 대 한 지 원 이 중 단 되 었 습 니 다. Windows [발 표](#)에 따라 XenMobile Server 는 Windows Information Protection(WIP) 에 대 한 지 원 을 중 단 했 습 니 다. `windows.wip.deprecation` 이라는 서버 속성을 추가하여 WIP 에 대 한 지 원 을 중 단 했 으며, 이 속성은 기본적으로 **True** 로 설정되어 있습니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.
- 모바일 서비스 공급자 (**MSP**) 인터페이스에 대한 지원이 중단되었습니다. 콘솔에서 MSP 인터페이스를 제거하는 새로운 서버 속성 `deprecate.mobile.service.provider` 를 추가하여 MSP 에 대 한 지 원 을 중 단 했 으며, 이 속성은 기본적으로 **True** 로 설정되어 있습니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.
- **Nexmo SMS** 게이트웨이에 대한 지원이 중단되었습니다. 새로운 서버 속성 `deprecate.carrier.sms.gateway` 를 추가하여 Nexmo SMS 에 대 한 지 원 을 중 단 했 으며, 이 속성은 기본적으로 **True** 로 설정되어 있습니다. Nexmo SMS 는 자가 지원 포털에서도 더 이상 사용되지 않습니다. 자세한 내용은 [알림](#)을 참조하십시오.

- **Windows 10** 장치에 대한 **WiFi** 감지 핫스팟 자동 연결 제한 허용 의 지원이 중단되었습니다. 자세한 내용은 [Windows 데스크톱/태블릿 설정](#)을 참조하십시오.
- 등록 초대 설정. 장치 IMEI, 일련 번호 및 UDID 를 사용하여 등록 초대를 만드는 지원은 더 이상 사용되지 않습니다. 등록 초대를 만들 때 XenMobile Server 콘솔의 관리 > 등록 초대에서 사용 가능한 설정을 구성합니다.
- 이제 다음 기능이 지원되지 않습니다.
 - Android - Amazon
 - Android - Sony 및 HTC
 - Zebra 장치의 사용자 지정 XML
 - 파생된 자격 증명
 - 일반, DigiCert 관리형 및 Entrust 어댑터 PKI 엔터티.
 - 높은 보안 등록 모드
 - RBAC 역할 - 공유 및 COSU 장치 등록자
 - Samsung SAFE 및 KNOX
 - SEAMS
 - Windows Phone 장치

자세한 내용은 [지원 중단](#)을 참조하십시오.

XenMobile Server 10.14 의 새로운 기능

November 21, 2022

[XenMobile Server 10.14](#)(PDF 다운로드)

Citrix ADC 에서 지원 중단되는 클래식 정책에 대한 지속적인 지원

Citrix 는 최근 Citrix ADC 12.0 빌드 56.20 부터 클래식 정책 기반 기능의 일부를 지원 중단한다고 발표했습니다. Citrix ADC 지원 중단 고지는 Citrix Gateway 와의 기존 XenMobile Server 통합에는 영향을 주지 않습니다. XenMobile Server 는 클래식 정책을 계속 지원하므로 별도의 작업이 필요하지 않습니다.

XenMobile 마이그레이션 서비스

XenMobile Server 를 온-프레미스에서 사용하는 경우 무료 XenMobile 마이그레이션 서비스를 사용하여 Endpoint Management 를 시작할 수 있습니다. XenMobile Server 에서 Citrix Endpoint Management 로 마이그레이션할 때 장치를 재등록할 필요는 없습니다.

마이그레이션을 시작하려면 해당 지역의 Citrix 영업 사원 또는 Citrix 파트너에게 문의하십시오. [XenMobile 마이그레이션 서비스](#)를 참조하십시오.

사용 중단 발표

단계적으로 중단되는 Citrix XenMobile 기능에 대한 고급 알림은 [사용 중단](#)을 참조하십시오.

엔드포인트를 iOS 14.5 로 업그레이드하기 전에

Citrix 는 엔드포인트를 iOS 14.5 로 업그레이드하기 전에 다음 작업을 수행하여 앱 충돌을 완화할 것을 권장합니다.

- Citrix Secure Mail 및 Secure Web 을 21.2.X 이상으로 업그레이드합니다. [MDX 또는 엔터프라이즈 앱 업그레이드](#)를 참조하십시오.
- MDX Toolkit 을 사용하는 경우 MDX Toolkit 21.3.X 이상으로 모든 타사 iOS 애플리케이션을 래핑합니다. 최신 버전은 MDX Toolkit [다운로드 페이지](#)를 확인하십시오.

온-프레미스 Citrix ADC 를 업그레이드하기 전에

온-프레미스 Citrix ADC 를 특정 버전으로 업그레이드하면 Single Sign-on 오류가 발생할 수 있습니다. 회사 직원 로그인 옵션이 있는 브라우저에서 Citrix Files 또는 ShareFile 도메인 URL 에 Single Sign-on 으로 인해 오류가 발생합니다. 사용자가 로그인할 수 없습니다.

이 문제의 해결 방법: Citrix Gateway 의 ADC CLI 에서 다음 명령을 아직 실행하지 않은 경우 명령을 실행하여 전역 SSO 를 사용하도록 설정합니다.

```
1 `set vpn parameter SSO ON`  
2 `bind vpn vs <vsName> -portalTheme X1`
```

자세한 내용은 다음을 참조하십시오.

- [Citrix ADC 릴리스 \(Feature Phase\) 13.0 빌드 67.39/67.43](#)
- [영향을 받는 SSO 구성](#)

문제 해결을 완료한 후 사용자는 회사 직원 로그인 옵션이 제공되는 브라우저에서 SSO 를 사용하여 Citrix Files 또는 ShareFile 도메인 URL 에 인증할 수 있습니다. [CXM-88400]

XenMobile 10.14 로 업그레이드하기 전에 (온-프레미스)

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 [시스템 요구 사항 및 호환성](#)과 [XenMobile 호환성](#)을 참조하십시오.

1. 업그레이드할 XenMobile Server 를 실행하는 가상 컴퓨터의 RAM 이 8GB 미만인 경우 8GB 이상으로 RAM 을 늘리는 것이 좋습니다.
2. 최신 버전의 XenMobile Server 10.14 로 업데이트하기 전에 Citrix License Server 를 11.16 이상으로 업데이트하십시오.

최신 버전의 XenMobile 에는 Citrix License Server 11.16(최소 버전) 이 필요합니다.

참고:

XenMobile 10.14 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2021 년 9 월 15 일입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 이후여야 합니다.

날짜는 라이선스 서버의 라이선스 옆에서 볼 수 있습니다. 최신 버전의 XenMobile 을 이전 버전의 라이선스 서버 환경에 연결하면 연결 확인이 실패하고 라이선스 서버를 구성할 수 없게 됩니다.

라이선스의 날짜를 갱신하려면 Citrix 포털에서 최신 라이선스 파일을 다운로드하고 라이선스 서버에 파일을 업로드하십시오. [Customer Success Services](#)를 참조하십시오.

- 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 iOS 정책 및 앱을 배포하려면 다음과 같은 요구 사항이 충족되어야 합니다. Citrix Gateway 에 SSL 지속성이 구성되어 있으면 모든 XenMobile Server 노드에서 포트 80 을 열어야 합니다.
- XenMobile 업데이트를 설치하기 전에 VM 의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

이번 릴리스에서 XenMobile 은 VMware ESXi 7.0 을 지원합니다. ESXi 7.0 를 설치하거나 업그레이드하기 전에 10.14 로 업그레이드해야 합니다.

XenMobile 10.13.x 또는 10.12.x 에서 직접 XenMobile 10.14 로 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 이진 파일을 다운로드합니다. <https://www.citrix.com/downloads>로 이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server > 제품 소프트웨어 > XenMobile Server 10** 으로 이동합니다. 해당하는 하이퍼바이저에 대한 XenMobile Server 소프트웨어 타일에서 파일 다운로드를 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다. [릴리스 관리 페이지를 사용하여 업그레이드하려면](#)을 참조하십시오.

업그레이드 후

연결 구성을 변경하지 않았는데도 발신 연결이 관련된 기능이 작동을 중지하는 경우 XenMobile Server 로그에 다음과 같은 오류가 있는지 확인하십시오. “VPP Server 에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’ 이 피어가 제공한 인증서 제목과 일치하지 않습니다.”

- 이 인증서 유효성 검사 오류는 XenMobile Server 에서 호스트 이름 유효성 검사를 비활성화해야 함을 나타냅니다.
- 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다.
- 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 `disable.hostname.verification`을 `true`로 변경하십시오. 이 속성의 기본값은 `false`입니다.

플랫폼 지원 업데이트

- **iOS 15:** XenMobile Server 및 Citrix 모바일 생산성 앱은 iOS 15 와 호환되지만 현재는 새로운 iOS 15 기능을 지원하지 않습니다.
- **Android 12:** XenMobile Server 는 Android 12 를 지원합니다. Google Device Administration API 의 지원 중단이 Android 10 이상을 실행하는 장치에 미치는 영향에 대해서는 [장치 관리에서 Android Enterprise 로 마이그레이션](#)을 참조하십시오. 이 [Citrix 블로그](#)도 참조하십시오.

장치 정책

- Google 설정과 더욱 가깝게 일치하고 구성을 단순화하도록 모든 Android Enterprise 등록 모드에 두 가지 설정을 추가했습니다.

- **Bluetooth** 공유 허용: 선택을 취소할 경우 사용자가 장치에서 나가는 Bluetooth 공유를 설정할 수 없습니다.
- 앱 제거 허용: 사용자가 관리되는 Google Play 스토어 내에서 앱을 제거하도록 허용합니다.

또한 무선 업그레이드 허용 설정을 제한 정책에서 OS 업데이트 정책으로 이동했습니다.

이러한 변경 사항에 대한 자세한 내용은 [제한 장치 정책](#) 및 [OS 업데이트 장치 정책](#)을 참조하십시오.

- Android Enterprise 에 대한 제한 설정이 명확하게 재구성되었습니다. 때로는 설정 이름이 약간 변경되는 경우가 있습니다. 재구성에 대한 자세한 내용은 [Android Enterprise 설정](#)을 참조하십시오.
- 이제 Android Enterprise 장치에서 관리되는 앱을 자동으로 업데이트할 수 있습니다. 자세한 내용은 [관리되는 앱 자동 업데이트 장치 정책](#)을 참조하십시오.
- Files 장치 정책을 사용하여 업로드 가능한 파일 형식 목록을 구성할 수 있습니다. 다음 파일 유형은 이 허용 목록에 추가해도 업로드할 수 없습니다.

- .cab
- .appx
- .ipa
- .apk
- .xap
- .mdx
- .exe

자세한 내용은 [서버 속성](#)을 참조하십시오.

장치 등록

- 이제 iOS 및 Android 장치에 대해 서로 다른 등록 프로필을 만들 수 있습니다. XenMobile Server 는 등록 유형이 서로 다른 여러 등록 프로필을 지원합니다. 자세한 내용은 [등록 프로필](#)을 참조하십시오.

- 완전 관리형 Android 11 이상 장치는 회사 소유 장치 모드로 작업 프로필에 등록됩니다. 새로운 모드는 장치에서 개인 프로필과 직장 프로필을 추가로 구분합니다. 이 변경 사항을 통해 조직은 관리되는 프로필을 보다 효과적으로 제어할 수 있으며 사용자에게 개인 프로필에 대한 더 효과적인 개인 정보 보호를 제공할 수 있습니다. 자세한 내용은 [Android Enterprise](#) 및 [서버 속성](#)을 참조하십시오.
- 이제 사용자가 iOS 또는 macOS 장치를 설정할 때 건너뛴 설정 화면을 추가로 지정할 수 있습니다.
 - iOS
 - * 복원 완료: 설치 중에 복원이 완료되었는지 여부가 사용자에게 표시되지 않습니다. iOS 14.0 에 해당합니다.
 - * 업데이트 완료: 설치 중에 소프트웨어 업데이트가 완료되었는지 여부가 사용자에게 표시되지 않습니다. iOS 14.0 에 해당합니다.
 - macOS
 - * 접근성: 사용자가 Voice Over 를 자동으로 들을 수 없습니다. 장치가 이더넷에 연결된 경우에만 사용할 수 있습니다. macOS 11 이상에 해당합니다.
 - * 생체 인식: 사용자가 Touch ID 및 Face ID 를 설정할 수 없습니다. macOS 10.12.4 이상에 해당합니다.
 - * **True Tone**: 사용자가 4 채널 센서를 설정해 디스플레이의 화이트 밸런스를 동적으로 조정할 수 없습니다. macOS 10.13.6 이상에 해당합니다.
 - * **Apple Pay**: 사용자가 Apple Pay 를 설정할 수 없습니다. 이 설정을 선택 취소하면 사용자는 Touch ID 및 Apple ID 를 설정해야 합니다. **Apple ID** 및 생체 인식 설정이 선택 취소되었는지 확인합니다. macOS 10.12.4 이상에 해당합니다.
 - * 스크린 타임: 사용자가 스크린 타임을 활성화할 수 없습니다. macOS 10.15 이상에 해당합니다.

설정 옵션 구성에 대한 자세한 내용은 [Apple 배포 프로그램을 통한 장치 배포](#)를 참조하십시오.

업데이트 로그 파일 표시

업데이트 로그 파일 표시라는 새 옵션은 문제 해결 메뉴의 로그 명령줄 인터페이스에서 사용할 수 있습니다. 이 옵션을 사용하면 업데이트 로그 목록의 내용을 볼 수 있으며 문제 해결의 효율성을 높일 수 있습니다. 명령줄 인터페이스 도구에 대한 자세한 내용은 [명령줄 인터페이스 옵션](#)을 참조하십시오.

오류 로그 파일

문제 해결 및 지원 > 로그에서 로그를 확인할 때 이제 디버그 로그에서 필터링된 오류가 표시된 로그를 확인할 수 있습니다. 자세한 내용은 [XenMobile 에서 로그 파일 보기](#)를 참조하십시오.

서버 속성

- `afw.allow.legacy.apps` 서버 속성을 구성하여 레거시 Android 앱을 Android Enterprise 앱에 제공할지 여부를 결정할 수 있습니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.

- 이제 XenMobile Server 포트 443의 대안으로 포트 2197을 사용할 수 있도록 지원합니다. 포트 2197을 사용하여 [api.push.apple.com](#)에서 APN 알림을 보내고 받을 수 있습니다. 포트는 HTTP/2 기반 APN 공급자 API를 사용합니다. 서버 속성 [apns.http2.alternate.port.enabled](#)의 기본값은 **false**입니다. 포트 2197을 사용하려면 서버 속성을 업데이트한 다음 서버를 다시 시작하십시오.
- 암호 유효성 검사는 사용자가 약한 암호를 사용하지 못하도록 합니다. [enable.password.strength.validation](#) 속성을 **true**로 설정하면 약한 암호를 사용하는 로컬 사용자를 만들 수 없습니다.

VPN 가상 서버 목록 개선

VPN 서버 이름에 [_XM_XenMobileGetway](#)가 포함되어 있지 않으면 XenMobile Server는 목록에서 사용 가능한 첫 번째 VPN 가상 서버를 선택합니다.

Citrix Launcher 지원

XenMobile Server는 Android Enterprise 장치에서 Citrix Launcher를 지원합니다. 자세한 내용은 [Launcher 구성 장치 정책](#)을 참조하십시오.

XenMobile Server 색상 개편

XenMobile Server는 Citrix 브랜드 색상 업데이트를 준수합니다.

XenMobile Server 10.13의 새로운 기능

May 6, 2022

[XenMobile Server 10.13](#)(PDF 다운로드)

Citrix ADC에서 지원 중단되는 클래식 정책에 대한 지속적인 지원

Citrix는 최근 Citrix ADC 12.0 빌드 56.20부터 클래식 정책 기반 기능의 일부를 지원 중단한다고 발표했습니다. Citrix ADC 지원 중단 고지는 Citrix Gateway와의 기존 XenMobile Server 통합에는 영향을 주지 않습니다. XenMobile Server는 클래식 정책을 계속 지원하므로 별도의 작업이 필요하지 않습니다.

XenMobile 마이그레이션 서비스

XenMobile Server 를 온-프레미스에서 사용하는 경우 무료 XenMobile 마이그레이션 서비스를 사용하여 Endpoint Management 를 시작할 수 있습니다. XenMobile Server 에서 Citrix Endpoint Management 로 마이그레이션할 때 장치를 재등록할 필요는 없습니다.

마이그레이션을 시작하려면 해당 지역의 Citrix 영업 사원 또는 Citrix 파트너에게 문의하십시오. [XenMobile 마이그레이션 서비스를](#) 참조하십시오.

사용 중단 발표

단계적으로 중단되는 Citrix XenMobile 기능에 대한 고급 알림은 [사용 중단](#)을 참조하십시오.

엔드포인트를 iOS 14.5 로 업그레이드하기 전에

Citrix 는 엔드포인트를 iOS 14.5 로 업그레이드하기 전에 다음 작업을 수행하여 앱 충돌을 완화할 것을 권장합니다.

- Citrix Secure Mail 및 Secure Web 을 21.2.X 이상으로 업그레이드합니다. [MDX 또는 엔터프라이즈 앱 업그레이드를](#) 참조하십시오.
- MDX Toolkit 을 사용하는 경우 MDX Toolkit 21.3.X 이상으로 모든 타사 iOS 애플리케이션을 래핑합니다. 최신 버전은 MDX Toolkit [다운로드 페이지](#)를 확인하십시오.

온-프레미스 Citrix ADC 를 업그레이드하기 전에

온-프레미스 Citrix ADC 를 특정 버전으로 업그레이드하면 Single Sign-on 오류가 발생할 수 있습니다. 회사 직원 로그인 옵션이 있는 브라우저에서 Citrix Files 또는 ShareFile 도메인 URL 에 Single Sign-on 으로 인해 오류가 발생합니다. 사용자가 로그인할 수 없습니다.

이 문제의 해결 방법: Citrix Gateway 의 ADC CLI 에서 다음 명령을 아직 실행하지 않은 경우 명령을 실행하여 전역 SSO 를 사용하도록 설정합니다.

```
1 `set vpn parameter SSO ON`  
2 `bind vpn vs <vsName> -portalTheme X1`
```

자세한 내용은 다음을 참조하십시오.

- [Citrix ADC 릴리스 \(Feature Phase\) 13.0 빌드 67.39/67.43](#)
- [영향을 받는 SSO 구성](#)

문제 해결을 완료한 후 사용자는 회사 직원 로그인 옵션이 제공되는 브라우저에서 SSO 를 사용하여 Citrix Files 또는 ShareFile 도메인 URL 에 인증할 수 있습니다. [CXM-88400]

XenMobile 10.13 로 업그레이드하기 전에 (온-프레미스)

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 [시스템 요구 사항 및 호환성](#)과 [XenMobile 호환성](#)을 참조하십시오.

1. 업그레이드할 XenMobile Server 를 실행하는 가상 컴퓨터의 RAM 이 8GB 미만인 경우 8GB 이상으로 RAM 을 늘리는 것이 좋습니다.
2. 최신 버전의 XenMobile Server 10.13 으로 업데이트하기 전에 Citrix License Server 를 11.16 이상으로 업데이트하십시오.

최신 버전의 XenMobile 에는 Citrix License Server 11.16(최소 버전) 이 필요합니다.

참고:

XenMobile 10.13 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2020 년 9 월 29 일입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 이후여야 합니다.

날짜는 라이선스 서버의 라이선스 옆에서 볼 수 있습니다. 최신 버전의 XenMobile 을 이전 버전의 라이선스 서버 환경에 연결하면 연결 확인이 실패하고 라이선스 서버를 구성할 수 없게 됩니다.

라이선스의 날짜를 갱신하려면 Citrix 포털에서 최신 라이선스 파일을 다운로드하고 라이선스 서버에 파일을 업로드하십시오. [Customer Success Services](#)를 참조하십시오.

3. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 iOS 정책 및 앱을 배포하려면 다음과 같은 요구 사항이 충족되어야 합니다. Citrix Gateway 에 SSL 지속성이 구성되어 있으면 모든 XenMobile Server 노드에서 포트 80 을 열어야 합니다.
4. XenMobile 업데이트를 설치하기 전에 VM 의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터 베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

이번 릴리스에서 XenMobile 은 VMware ESXi 7.0 을 지원합니다. ESXi 7.0 를 설치하거나 업그레이드하기 전에 10.13 으로 업그레이드해야 합니다.

XenMobile 10.12.x 또는 10.11.x 에서 직접 XenMobile 10.13 으로 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 이진 파일을 다운로드합니다. <https://www.citrix.com/downloads>로 이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server > 제품 소프트웨어 > XenMobile Server 10** 으로 이동합니다. 해당하는 하이퍼바이저에 대한 XenMobile Server 소프트웨어 타일에서 파일 다운로드를 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다. [릴리스 관리 페이지를 사용하여 업그레이드하려면](#)을 참조하십시오.

업그레이드 후

연결 구성을 변경하지 않았는데도 발신 연결이 관련된 기능이 작동을 중지하는 경우 XenMobile Server 로그에 다음과 같은 오류가 있는지 확인하십시오. “VPP Server 에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’ 이 피어가 제공한 인증서 제목과 일치하지 않습니다.”

- 이 인증서 유효성 검사 오류는 XenMobile Server 에서 호스트 이름 유효성 검사를 비활성화해야 함을 나타냅니다.
- 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다.
- 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 `disable.hostname.verification`을 `true`로 변경하십시오. 이 속성의 기본값은 `false`입니다.

플랫폼 지원 업데이트

- **iOS 14:** XenMobile Server 및 Citrix 모바일 생산성 앱은 iOS 14 와 호환되지만 현재는 새로운 iOS 14 기능을 지원하지 않습니다. MDX Toolkit 20.8.5 이상을 사용하거나 MAM SDK 를 사용하여 앱을 준비합니다.
- **Android 11:** XenMobile Server 는 Android 11 을 지원합니다. Google Device Administration API 의 지원 중단이 Android 10 이상을 실행하는 장치에 미치는 영향에 대해서는 [장치 관리에서 Android Enterprise 로 마이그레이션](#)을 참조하십시오. 이 [Citrix 블로그](#)도 참조하십시오.

단일 환경에서 여러 장치 및 앱 관리 모드 구성

이제 하나의 XenMobile 사이트를 구성하여 여러 등록 구성을 지원할 수 있습니다. 등록 프로필의 역할이 장치 및 앱 관리를 위한 등록 설정을 포함하도록 확장되었습니다.

등록 프로필은 단일 XenMobile 콘솔 내에서 여러 사용 사례와 장치 마이그레이션 경로를 지원합니다. 사용 사례에는 다음이 포함됩니다.

- Mobile Device Management(MDM 전용)
- MDM+MAM(Mobile Application Management)
- MAM 전용
- 회사 소유 등록
- BYOD 등록 (MDM 등록 취소 기능)
- Android Enterprise 등록으로 Android 장치 관리자 등록 마이그레이션 (완전 관리됨, 작업 프로필, 전용 장치)

등록 프로필은 이제 지원 중단된 `xms.server.mode` 서버 속성을 대체합니다. 이러한 변경은 기존 배달 그룹과 등록된 장치에 영향을 미치지 않습니다.

전용 장치를 등록하지 않아도 된다면 `enable.multimode.xms`을 `false`로 설정하여 이 기능을 비활성화하면 됩니다. [서버 속성](#)을 참조하십시오.

다음 표는 기존 서버 모드에서 새 등록 프로필 기능으로 자동화된 마이그레이션 경로를 보여줍니다.

기존 서버 속성

새 관리 모드

ENT 모드 (iOS)

Citrix MAM 을 활용하는 Apple 장치 등록

ENT 모드 (Android)

Citrix MAM 을 활용하는 레거시 장치 관리자

ENT 모드 (Android Enterprise)

Citrix MAM 을 활용하는 완전 관리형 장치 (이전의 COPE)의 작업 프로필

MAM 모드 (iOS 및 Android)

Citrix MAM

MDM 모드 (iOS)

Apple 장치 등록

MDM 모드 (Android)

레거시 장치 관리자

MDM 모드 (Android Enterprise)

완전 관리형 장치의 작업 프로필

배달 그룹을 만들면 해당 그룹에 등록 프로필을 첨부할 수 있습니다. 등록 프로필을 첨부하지 않으면 XenMobile 이 전역 등록 프로필을 첨부합니다.

등록 프로필은 다음 장치 관리 기능을 제공합니다.

- **Android** 장치 관리자 (**DA**) 모드를 **Android Enterprise** 로 더 쉽게 마이그레이션할 수 있습니다. **Android Enterprise** 장치의 경우 설정에 완전 관리형 장치, 완전 관리형 장치의 작업 프로필, 전용 장치와 같은 장치 소유자 모드가 포함됩니다. [Android Enterprise](#)를 참조하십시오.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ⓘ Management <ul style="list-style-type: none"> <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ Device owner mode <ul style="list-style-type: none"> <input checked="" type="radio"/> Company-owned device ⓘ <input type="radio"/> Fully managed with work profile ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ BYOD work profile <input checked="" type="checkbox"/> ⓘ Application management ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ User consent <ul style="list-style-type: none"> Allow users to decline device management <input checked="" type="checkbox"/> ⓘ
Android	
iOS	
3 Assignment (optional)	

이 업그레이드의 경우 서버 모드에 대한 현재 XenMobile 구성과 설정 > **Android Enterprise** 가 다음과 같이 새로운 등록 프로필 설정에 매핑됩니다.

현재 구성	관리 설정	장치 소유자 모드 설정	Citrix MAM 설정
MDM. 관리되는 Google Play(Android Enterprise)	Android Enterprise	완전 관리형 장치의 작업 프로 필	꺼짐
MDM, G Suite(레거시 DA)	레거시 DA	해당 없음	꺼짐
MAM	장치 관리 안 함	해당 없음	켜짐
MDM+MAM. 관리되는 Google Play(Android Enterprise)	Android Enterprise*	완전 관리형 장치의 작업 프로 필	켜짐
MDM+MAM, G Suite(레 거시 DA)	레거시 DA*	해당 없음	켜짐

* 등록이 필요한 경우 사용자의 장치 관리 거부를 허용을 꺼짐으로 설정합니다.

업그레이드하고 나면 현재 등록 프로필에 이러한 매핑이 반영됩니다. 신규 사용 사례를 레거시 DA로부터의 전환으로 처리하려면 다른 등록 프로필 생성 여부를 고려해 보십시오.

- 더 간편해진 **iOS** 관리. iOS 장치의 경우 설정에서 장치를 관리되는 장치 또는 관리되지 않는 장치로 등록할지를 선택할 수 있습니다.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	<p>Specify device management settings for this enrollment profile.</p> <p>Device management ⓘ</p> <p>Management <input checked="" type="radio"/> Device enrollment ⓘ <input type="radio"/> Do not manage devices ⓘ</p> <p>Application management ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
2 Platforms	
Android	
iOS	
3 Assignment (optional)	

이 업그레이드의 경우 이전 구성이 새 등록 프로필에 다음과 같이 매핑됩니다.

서버 모드	관리 설정	Citrix MAM 설정
MDM	장치 등록	꺼짐
MAM	장치 관리 안 함	켜짐

서버 모드	관리 설정	Citrix MAM 설정
MDM+MAM	장치 등록	켜짐

등록이 필요한 경우 사용자의 장치 관리 거부를 허용을 꺼짐으로 설정합니다.

강화된 등록 프로필에 다음과 같은 제한이 존재합니다.

- 일회용 PIN 또는 2 단계 인증 등록 초대에는 강화된 등록 프로필 기능을 사용할 수 없습니다.

[등록 프로필](#)을 참조하십시오.

최신 HTTP/2 기반 APN 제공업체 API 지원

Apple의 Apple 푸시 알림 서비스 레거시 바이너리 프로토콜 지원이 2021년 3월 31일에 종료됩니다. Apple에서는 HTTP/2 기반 APN 제공업체 API를 대신 사용하도록 권장합니다. XenMobile Server에서는 이제 HTTP/2 기반 API를 지원합니다. 자세한 정보는 <https://developer.apple.com/>에서 뉴스 업데이트 “Apple 푸시 알림 서비스 업데이트”를 참고하십시오. APN 연결 확인과 관련된 지원은 [연결 확인](#)을 참조하십시오.

다음 XenMobile Server 버전에서 기본적으로 HTTP/2 기반 API를 지원합니다.

- XenMobile Server 10.13
- XenMobile Server 10.12 롤링 패치 5 이상

다음 XenMobile Server 버전을 사용하는 경우 지원을 이용하려면 **apple.apns.http2** 서버 속성을 추가해야 합니다.

- XenMobile Server 10.12 롤링 패치 2-4 이상
- XenMobile Server 10.11 롤링 패치 5 이상

XenMobile Server 10.11은 더 이상 지원되지 않으므로 최신 릴리스로 업그레이드하는 것이 좋습니다.

여러 iOS 장치에 장치 인증서 기반 IPsec VPN 사용

장치 인증서 기반 IPsec VPN이 필요한 iOS 장치마다 VPN 장치 정책과 자격 증명 장치 정책을 구성하는 대신 프로세스를 자동화해 보십시오.

1. 연결 유형이 **IKEv2** 항상 켜짐인 상태로 iOS VPN 장치 정책을 구성합니다.
2. 장치 ID 기반 장치 인증서를 장치 인증 방법으로 선택합니다.
3. 사용할 장치 ID 유형을 선택합니다.
4. REST API를 사용하여 장치 인증서를 일괄적으로 가져옵니다.

VPN 장치 정책 구성에 대한 자세한 내용은 [VPN 장치 정책](#)을 참조하십시오. 인증서 일괄 가져오기에 대한 자세한 내용은 [REST API로 인증서 일괄 업로드](#)를 참조하십시오.

Apple 볼륨 구매 앱 자동 업데이트

볼륨 구매 계정을 추가하면 (설정 > iOS 설정) 이제 모든 iOS 앱을 자동으로 업데이트할 수 있습니다. [Apple 볼륨 구매](#)에서 앱 자동 업데이트 설정을 참고하십시오.

로컬 사용자 계정의 암호 요구 사항

XenMobile 콘솔에서 로컬 사용자 계정을 추가하거나 편집할 경우 최신 암호 요구 사항을 따라야 합니다.

자세한 내용은 [로컬 사용자 계정을 추가하려면](#)을 참조하십시오.

- **암호 요구 사항:** XenMobile Server 콘솔에서 로컬 사용자 계정을 추가하거나 편집할 경우 최신 암호 요구 사항을 따르십시오. [로컬 사용자 계정을 추가하려면](#)을 참조하십시오.
- **로컬 사용자 계정 잠금:** 사용자가 유효하지 않은 로그인 시도를 연속으로 할 수 있는 최대 횟수에 도달한 경우 로컬 사용자 계정이 30 분 간 잠깁니다. 잠금 기간이 만료될 때까지 시스템에서는 모든 인증 시도를 거부합니다. XenMobile Server 콘솔에서 계정의 잠금을 해제하려면 관리 > 사용자로 이동한 다음 사용자 계정을 선택하고 로컬 사용자 잠금 해제를 클릭합니다. [로컬 사용자 계정을 잠금 해제하려면](#)을 참조하십시오.

장치 정책

Android Enterprise 장치의 신규 장치 정책 및 장치 정책 설정이 추가되었습니다.

Android Enterprise 장치에서 트레이 도구 모음 아이콘 숨기기

이제 Android Enterprise 장치에서 트레이 도구 모음 아이콘을 숨기거나 표시할지 여부를 선택할 수 있습니다. [XenMobile 옵션 장치 정책](#)을 참조하십시오.

작업 프로필 모드 또는 완전 관리형 장치 모드의 **Android Enterprise** 장치에 대한 추가 인증서 관리 기능

관리되는 키 저장소에서 인증 기관을 설치할 뿐 아니라 이제 다음 기능도 관리할 수 있습니다.

- 특정 관리되는 앱을 사용하는 인증서를 구성합니다. Android Enterprise의 인증서 장치 정책에 이제 인증서를 사용할 앱 설정이 포함됩니다. 이 정책에서 선택한 자격 증명 공급자가 발행한 사용자 인증서를 사용할 앱을 지정할 수 있습니다. 런타임 중에 인증서에 대한 액세스 권한이 자동으로 앱에 부여됩니다. 모든 앱에 인증서를 사용하려면 앱 목록을 비워 두십시오. [자격 증명 장치 정책](#)을 참조하십시오.
- 관리되는 키 저장소에서 인증서를 자동으로 삭제하거나 비시스템 CA 인증서를 제거하십시오. [자격 증명 장치 정책](#)을 참조하십시오.
- 사용자가 관리되는 키 저장소에 저장된 자격 증명을 수정할 수 없게 합니다. Android Enterprise의 제한 장치 정책에 이제 사용자가 사용자 자격 증명을 구성하도록 허용 설정이 포함됩니다. 기본적으로 이 설정은 켜짐입니다. [제한 장치 정책](#)을 참조하십시오.

관리되는 구성에서 더 간편하게 사용하는 인증서 별칭

관리되는 구성 장치 설정이 포함된 자격 증명 장치 정책에서 새 인증서 별칭 설정을 사용합니다. 이렇게 하면 사용자 작업 없이도 앱이 VPN에서 인증할 수 있습니다. 앱 로그에서 자격 증명 별칭을 찾는 대신 자격 증명 별칭을 만듭니다. 관리되는 구성 장치 정책의 인증서 별칭 필드에 입력하여 별칭을 만듭니다. 자격 증명 장치 정책의 인증서 별칭 설정에 동일한 인증서 별칭을 입력합니다. [관리되는 구성 정책](#) 및 [자격 증명 장치 정책](#)을 참조하십시오.

Android Enterprise 장치의 “한 번 잠금 사용” 설정 제어

암호 장치 정책의 새로운 통합 암호 사용 설정을 사용하면 장치에 별도의 암호와 작업 프로필이 필요한지 여부를 제어할 수 있습니다. 이 설정 전에는 사용자가 장치의 한 번 잠금 사용 설정으로 이 동작을 제어했습니다. 통합 암호 사용이 켜지면 사용자는 장치에 작업 프로필과 동일한 암호를 사용할 수 있습니다. 통합 암호 사용이 꺼지면 사용자는 장치에 작업 프로필과 동일한 암호를 사용할 수 없습니다. 기본값은 꺼짐입니다. Android 9.0 이상을 실행하는 Android Enterprise 장치에 통합 잠금 사용 설정을 사용할 수 있습니다. [암호 장치 정책](#)을 참조하십시오.

규정을 준수하지 않는 **Android Enterprise** 장치의 앱과 바로 가기 표시

Android Enterprise의 암호 장치 정책에는 새로운 설정인 암호가 규정을 준수하지 않는 경우 앱 및 바로 가기 표시가 있습니다. 이 설정을 사용하여 장치 암호가 더 이상 규정을 준수하지 않을 경우 앱과 바로가기를 계속 표시할 수 있습니다. Citrix에서는 암호가 규정을 준수하지 않는 경우 규정을 준수하지 않는 장치로 표시하도록 자동화된 작업을 만드는 것을 권장합니다. [암호 장치 정책](#)을 참조하십시오.

Android Enterprise 작업 프로필 장치 또는 완전히 관리되는 장치에서 인쇄하는 기능 비활성화

제한 장치 정책에서 인쇄 허용 안 함 설정을 사용하면 사용자가 Android Enterprise 장치에서 액세스할 수 있는 프린터로 인쇄할 수 있는지 여부를 지정할 수 있습니다. [Android Enterprise 설정](#)을 참조하십시오.

키오스크 정책에서 패키지 이름을 추가하여 전용 장치의 앱 허용

이제 Android Enterprise 플랫폼에서 허용할 패키지 이름을 입력할 수 있습니다. [Android Enterprise 설정](#)을 참조하십시오.

Android Enterprise 작업 프로필 및 완전히 관리되는 장치에 대한 **Keyguard** 관리

Android Keyguard는 장치 및 Work Challenge 잠금 화면을 관리합니다. 다음과 같은 Keyguard 관리 장치 정책을 사용하여 제어합니다.

- 작업 프로필 장치의 Keyguard 관리. 사용자가 장치 Keyguard 와 Work Challenge Keyguard 의 잠금을 해제하기 전에 사용할 수 있는 기능을 지정할 수 있습니다. 예를 들어, 기본적으로 사용자는 지문 잠금 해제를 사용하고 잠금 화면에서 수정되지 않은 알림을 확인할 수 있습니다. Keyguard 관리 정책을 사용하여 Android 9.0 이상을 실행하는 장치에 대해 모든 생체 인증을 비활성화할 수도 있습니다.
- 완전 관리형 전용 장치의 Keyguard 관리. Keyguard 화면의 잠금을 해제하기 전에 신뢰할 수 있는 에이전트, 보안 카메라와 같이 사용할 수 있는 기능을 지정할 수 있습니다. 또는 모든 Keyguard 기능을 사용하지 않도록 선택할 수 있습니다.

[Keyguard 관리 장치 정책](#)을 참조하십시오.

XenMobile 콘솔에서 **Android Enterprise** 의 엔터프라이즈 앱 게시

Android Enterprise 개인 앱을 추가할 때 더 이상 Google Play 개발자 계정을 등록하지 않아도 됩니다. XenMobile 콘솔에서 APK 파일을 업로드하고 게시할 수 있도록 관리되는 Google Play 스토어 UI 가 열립니다. 자세한 내용은 [엔터프라이즈 앱 추가](#)를 참조하십시오.

XenMobile 콘솔에서 **Android Enterprise** 의 웹 앱 게시

이제 관리되는 Google Play 또는 Google 개발자 포털로 이동하지 않고도 XenMobile 용 Android Enterprise 웹 앱을 게시할 수 있습니다. 구성 > 앱 > 웹 링크에서 업로드를 클릭하면 파일을 업로드하고 저장할 수 있도록 관리되는 Google Play 스토어 UI 가 열립니다. 약 10 분 안에 앱을 승인하고 게시할 수 있습니다. 자세한 내용은 [웹 링크 추가](#)를 참조하십시오.

XenMobile Server REST API 로 **iOS** 장치에 인증서 일괄 업로드

한 번에 인증서 하나를 업로드하는 것이 실용적이지 않다면 XenMobile Server REST API 를 사용하여 iOS 장치에 인증서를 일괄 업로드할 수 있습니다.

1. 연결 유형이 **IKEv2** 항상 켜짐인 상태로 iOS VPN 장치 정책을 구성합니다.
2. 장치 **ID** 기반 장치 인증서를 장치 인증 방법으로 선택합니다.
3. 사용할 장치 **ID** 유형을 선택합니다.
4. REST API 를 사용하여 장치 인증서를 일괄적으로 가져옵니다.

VPN 장치 정책 구성에 대한 자세한 내용은 [VPN 장치 정책](#)을 참조하십시오. 인증서 일괄 가져오기에 대한 자세한 내용은 [REST API 로 iOS 장치에 인증서 일괄 업로드](#)를 참조하십시오.

암호화 키 새로고침

XenMobile CLI 의 고급 설정에서 암호화 키 새로고침 옵션이 추가됩니다. 이 옵션을 사용하여 암호화 키를 한 번에 한 노드씩 새로 고칠 수 있습니다. [시스템 옵션](#)을 참조하십시오.

ESXi 7.0 지원

이번 릴리스에서 XenMobile은 VMware ESXi 7.0을 지원합니다. ESXi 7.0을 설치하거나 업그레이드하기 전에 10.13으로 업그레이드해야 합니다.

새 서버 속성

이제 다음 서버 속성이 제공됩니다.

- **iOS App Store** 링크에 호스트 이름 허용: 콘솔이 아닌 공개 API를 사용하여 iOS용 공개 앱 스토어 앱을 추가하려면 원할 경우 허용된 호스트 이름 목록을 구성합니다.
- 로컬 사용자 계정 잠금 한도: 계정이 잠기기 전에 로컬 사용자에게 허용되는 로그인 시도 횟수를 구성합니다.
- 로컬 사용자 계정 잠금 시간: 로그인 시도가 너무 많이 실패한 경우 로컬 사용자가 잠기는 시간의 길이를 구성합니다.
- 설정된 파일 업로드 최대 크기 제한: 업로드한 파일에 대한 최대 파일 크기를 제한할 수 있습니다.
- 허용되는 파일 업로드 최대 크기: 업로드된 파일의 최대 파일 크기를 설정합니다.

이러한 속성에 대한 자세한 내용은 [서버 속성](#)을 참조하십시오.

셀프 서비스 디스크 정리 수행

디스크 사용량이라는 새 명령줄 인터페이스를 문제 해결 메뉴에서 사용할 수 있습니다. 이 옵션을 사용하면 코어 덤프 파일과 지원 번들 파일 목록을 볼 수 있습니다. 목록을 확인한 후 명령줄을 통해 이러한 파일을 모두 삭제하도록 선택할 수 있습니다. 명령줄 인터페이스 도구에 대한 자세한 내용은 [명령줄 인터페이스 옵션](#)을 참조하십시오.

XenMobile Server 10.12의 새로운 기능

January 5, 2022

[XenMobile Server 10.12](#)(PDF 다운로드)

XenMobile 마이그레이션 서비스

XenMobile Server를 온-프레미스에서 사용하는 경우 무료 XenMobile 마이그레이션 서비스를 사용하여 Endpoint Management를 시작할 수 있습니다. XenMobile Server에서 Citrix Endpoint Management로 마이그레이션할 때 장치를 재등록할 필요는 없습니다.

마이그레이션을 시작하려면 해당 지역의 Citrix 영업 사원 또는 Citrix 파트너에게 문의하십시오. 자세한 내용은 [XenMobile 마이그레이션 서비스](#)를 참조하십시오.

사용 중단 발표

단계적으로 중단되는 Citrix XenMobile 기능에 대한 고급 알림은 [사용 중단](#)을 참조하십시오.

예정된 변경 사항에 대한 **Android** 장치 준비

이전에 발표된 사용 중단은 Android 및 Android Enterprise 장치에 영향을 미칩니다.

- Android 10 에 대한 DA(장치 관리) 등록:
 - **2020 년 7 월 31 일:** 레거시 Android 장치 관리 모드에 대한 신규 등록이 중단됩니다.
 - **2020 년 11 월 1 일:** Google 의 레거시 장치 관리 API 사용이 중단됩니다. 레거시 장치 관리 모드에서 실행되는 Android 10 장치는 더 이상 작동하지 않습니다.
- MDX 암호화:
 - **2020 년 8 월 1 일:** Citrix 모바일 생산성 및 타사 MDX 앱에 대한 MDX 암호화가 플랫폼 암호화로 마이그레이션됩니다.
 - **2020 년 9 월 1 일:** MDX 암호화가 수명 종료에 도달합니다.

레거시 **DA** 에서 등록된 장치의 경우

- MDX 암호화를 사용하지 않는 경우 별도의 조치가 필요하지 않습니다.
- MDX 암호화를 사용하는 경우 2020 년 7 월 31 일 이전에 Android 장치를 Android Enterprise 로 마이그레이션하십시오. Android 10 을 실행하는 장치는 Android Enterprise 를 사용하여 등록하거나 재등록해야 합니다. 이 요구 사항에는 MAM 전용 모드의 Android 장치가 포함됩니다. [장치 관리에서 Android Enterprise 로 마이그레이션](#)을 참조하십시오.

7 월 31 일을 기준으로 **Android Enterprise** 에 이미 등록된 장치의 경우

- Android Enterprise 플랫폼을 사용하여 앱을 게시한 경우 Android Enterprise 를 통해 암호화가 이미 처리되었습니다. 작업이 필요하지 않습니다.
- 레거시 Android 플랫폼을 사용하여 앱을 게시한 경우 2020 년 7 월 31 일 이전에 Android Enterprise 를 사용하여 앱을 다시 게시합니다.

XenMobile 10.12 로 업그레이드하기 전에 (온-프레미스)

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 [시스템 요구 사항 및 호환성](#)과 [XenMobile 호환성](#)을 참조하십시오.

1. 최신 버전의 XenMobile Server 10.12 로 업데이트하기 전에 Citrix License Server 를 11.16 이상으로 업데이트하십시오.
최신 버전의 XenMobile 에는 Citrix License Server 11.16(최소 버전) 이 필요합니다.

참고:

미리 보기에 자체 라이선스를 사용하려는 경우 XenMobile 10.12의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜)는 2020년 1월 20일이라는 점을 숙지하십시오. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 이후여야 합니다.

날짜는 라이선스 서버의 라이선스 옆에서 볼 수 있습니다. 최신 버전의 XenMobile을 이전 버전의 라이선스 서버 환경에 연결하면 연결 확인이 실패하고 라이선스 서버를 구성할 수 없게 됩니다.

라이선스의 날짜를 갱신하려면 Citrix 포털에서 최신 라이선스 파일을 다운로드하고 라이선스 서버에 파일을 업로드하십시오. 자세한 내용은 [Customer Success Services](#)를 참조하십시오.

- 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 iOS 정책 및 앱을 배포하려면 다음과 같은 요구 사항이 충족되어야 합니다. Citrix Gateway에 SSL 지속성이 구성되어 있으면 모든 XenMobile Server 노드에서 포트 80을 열어야 합니다.
- 업그레이드할 XenMobile Server를 실행하는 가상 컴퓨터의 RAM이 4GB 미만인 경우 4GB 이상으로 RAM을 늘리십시오. 프로덕션 환경에 권장되는 최소 RAM은 8GB입니다.
- XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

XenMobile 10.11.x 또는 10.10.x에서 직접 XenMobile 10.12로 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 이진 파일을 다운로드합니다. <https://www.citrix.com/downloads>로 이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server > 제품 소프트웨어 > XenMobile Server 10**으로 이동합니다. 해당하는 하이퍼바이저에 대한 XenMobile Server 소프트웨어 타일에서 파일 다운로드를 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다. 자세한 내용은 [릴리스 관리 페이지를 사용하여 업그레이드하려면](#)을 참조하십시오.

업그레이드 후

XenMobile 10.12로 업그레이드한 후 (온-프레미스):

연결 구성을 변경하지 않았는데도 발신 연결이 관련된 기능이 작동을 중지하는 경우 XenMobile Server 로그에 다음과 같은 오류가 있는지 확인하십시오. “VPP Server에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’이 피어가 제공한 인증서 제목과 일치하지 않습니다.”

이 인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 유효성 검사를 비활성화해야 함을 나타냅니다. 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다. 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 `disable.hostname.verification`을 `true`로 변경하십시오. 이 속성의 기본값은 `false`입니다.

iOS 13 에 대한 추가 지원

XenMobile Server 는 iOS 13 으로 업그레이드된 장치를 지원합니다. 업그레이드는 사용자에게 다음과 같은 영향을 미칩니다.

- 등록하는 동안 몇 개의 새로운 iOS Setup Assistant(설정 도우미) 옵션 화면이 나타납니다. Apple 은 iOS 13 에 새로운 iOS Setup Assistant(설정 도우미) 옵션 화면을 추가했습니다. 새 옵션은 이 릴리스의 설정 > **Apple DEP**(장치 등록 프로그램) 페이지에 포함되어 있습니다. 이러한 화면을 건너뛰도록 XenMobile Server 를 구성할 수 없습니다. 이러한 페이지는 iOS 13 장치 사용자에게 나타납니다.
- iOS 13 이상에서는 이전 버전의 iOS 에 대한 감독 또는 감독되지 않은 장치에서 사용할 수 있었던 일부 제한 장치 정책 설정을 감독되는 장치에서만 사용할 수 있습니다. 현재 XenMobile Server 콘솔의 도구 설명에는 이러한 설정이 iOS 13 이상에서 감독되는 장치 전용이라는 설명이 표시되지 않습니다.
 - 하드웨어 제어 허용:
 - * FaceTime
 - * 앱 설치
 - 앱 허용:
 - * iTunes 스토어
 - * Safari
 - * Safari > 자동 채우기
 - 네트워크 - iCloud 동작 허용:
 - * iCloud 문서 및 데이터
 - 감독되는 경우에만 해당되는 설정 - 허용:
 - * 게임 센터 > 친구 추가
 - * 게임 센터 > 멀티플레이 게임
 - 미디어 콘텐츠 - 허용:
 - * 음악, 팟캐스트 및 iTunes U 의 성인 등급 자료

이러한 제한은 다음과 같이 적용됩니다.

- iOS 12 이하 장치가 이미 XenMobile Server 에 등록되어 있는 상태에서 iOS 13 으로 업그레이드하는 경우 위의 제한 사항은 감독되지 않는 장치 및 감독되는 장치에 적용됩니다.
- 감독되지 않는 iOS 13 이상 장치를 XenMobile Server 에 등록하는 경우 위의 제한 사항은 감독되는 장치에만 적용됩니다.
- 감독되는 iOS 13 이상 장치를 XenMobile Server 에 등록하는 경우 위의 제한 사항은 감독되는 장치에만 적용됩니다.

Apple Volume Purchase Program 을 ABM(Apple Business Manager) 및 ASM(Apple School Manager) 으로 마이그레이션

Apple VPP(Volume Purchase Program) 를 사용하는 회사 및 교육 기관에서는 2019 년 12 월 1 일 전에 Apple Business Manager 또는 Apple School Manager 의 앱 및 서적으로 마이그레이션해야 합니다.

XenMobile 에서 VPP 계정을 마이그레이션하기 전에 이 [Apple 지원 문서](#)를 참조하십시오.

조직 또는 학교에서 VPP(Volume Purchase Program) 만 사용하는 경우 ABM/ASM 에 등록한 다음 기존 VPP 구매자를 새 ABM/ASM 계정으로 초대할 수 있습니다. ASM 의 경우 <https://school.apple.com>으로 이동합니다. ABM 의 경우 <https://business.apple.com>으로 이동합니다.

XenMobile 에서 VPP 계정을 업데이트하려면:

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. **iOS** 설정을 클릭합니다. **Volume Purchase Program** 구성 페이지가 나타납니다.
3. ABM 또는 ASM 계정에 이전 VPP 계정과 동일한 앱 구성이 있는지 확인합니다.
4. ABM 또는 ASM 포털에서 업데이트된 토큰을 다운로드합니다.
5. XenMobile 콘솔에서 다음을 수행합니다.
 - a) 해당 위치에 대한 업데이트된 토큰 정보로 기존 볼륨 구매 계정을 편집합니다.
 - b) ABM 또는 ASM 자격 증명을 편집합니다. 접미사를 변경하지 마십시오.
 - c) 저장을 두 번 클릭합니다.

자세한 내용은 다음을 참조하십시오.

- [Apple 배포 프로그램](#)
- [Apple 장치의 대량 등록](#)

Android Enterprise COPE 장치에 대한 지원

XenMobile Server 는 작업 프로필이 있는 완전 관리형 Android Enterprise 장치 (이전의 COPE(회사 소유의 개인 사용) 장치) 를 지원합니다. 이러한 장치는 완전 관리형 Android Enterprise 장치의 한 유형으로, 작업 프로필이 있는 장치를 말합니다. 다. 장치와 작업 프로필에 개별 정책 설정을 적용할 수 있습니다. 이 릴리스의 경우:

- 자격 증명, 암호 및 제한 장치 정책을 사용하여 장치와 작업 프로필에 개별 설정을 적용할 수 있습니다.
- 위치 장치 정책의 위치 모드 설정을 COPE 장치 자체에 적용할 수 있지만 COPE 장치의 작업 프로필에는 적용할 수 없습니다. 위치 장치 정책의 다른 설정은 COPE 에서 사용할 수 없습니다.
- 장치 또는 작업 프로필에 잠금 보안 동작을 개별적으로 적용할 수 있습니다.

장치 정책

작업 프로필이 있는 완전 관리형 Android Enterprise 장치 (COPE 장치) 의 경우 일부 장치 정책의 개별 설정을 전체 장치와 작업 프로필에 적용할 수 있습니다. XenMobile Server 콘솔에서 일부 장치 정책의 개별 설정을 적용할 수 있습니다. 다른 장치 정책을 사용하여 전체 장치에만 설정을 적용하거나 작업 프로필로 완전히 관리되는 장치의 작업 프로필에만 설정을 적용할 수 있습니다.

보안 동작

작업 프로필이 있는 완전 관리형 Android Enterprise 장치 (COPE devices) 의 경우 다음을 적용할 수 있습니다.

- 잠금 보안 동작을 장치 또는 작업 프로필에 개별적으로 적용.
- 다른 모든 보안 동작을 장치에 적용.

등록 프로필을 사용하여 **Android** 장치의 등록 옵션 제어

XenMobile 배포에서 Android Enterprise 를 사용하도록 설정한 경우 이제 등록 프로필을 사용하여 Android 장치의 등록 방법을 제어할 수 있습니다. 등록 프로필은 Android 장치를 기본 Android Enterprise 모드 (완전 관리형 또는 작업 프로필) 로 등록할지, 아니면 레거시 (장치 관리자) 모드로 등록할지를 결정합니다.

기본적으로 글로벌 등록 프로필은 신규 및 공장 기본값으로 재설정된 Android Enterprise 장치를 완전 관리형 장치로 등록하고, BYOD Android Enterprise 장치를 작업 프로필 장치로 등록합니다. 자세한 내용은 [Android Enterprise](#)를 참조하십시오.

Android Enterprise 를 기본 등록으로 사용하도록 레거시 **Android** 장치 준비

Google 은 장치 관리의 장치 관리자 모드 사용을 중단하고 장치 소유자 모드 또는 프로필 소유자 모드에서 모든 Android 장치를 관리할 것을 권장하고 있습니다. Google Android Enterprise 개발자 가이드의 [장치 관리자 사용 중단](#)을 참조하십시오. 이 변경 사항을 지원하기 위해 이제 Android 장치의 기본 등록 옵션이 Android Enterprise 로 변경되었습니다.

따라서 XenMobile 배포에서 Android Enterprise 를 사용하도록 설정한 경우 새로 등록되거나 다시 등록되는 모든 Android 장치는 Android Enterprise 장치로 등록됩니다.

이 변경 사항을 준비하기 위해 이제 XenMobile 에서 Android 장치의 등록 방법을 제어하는 등록 프로필을 생성할 수 있습니다.

조직이 레거시 Android 장치를 장치 소유자 모드 또는 프로필 소유자 모드에서 관리할 준비가 되지 않았을 수 있습니다. 이러한 장치를 장치 관리자 모드에서 계속해서 관리할 수 있습니다. 레거시 장치에 대한 등록 프로필을 만들고 등록된 모든 레거시 장치를 재등록하십시오.

레거시 장치에 대한 등록 프로필을 만들려면:

1. XenMobile 콘솔에서 구성 > 등록 프로필로 이동합니다.
2. 등록 프로필을 추가하려면 추가를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다.
3. 다음을 클릭하거나 플랫폼에서 **Android Enterprise** 를 선택합니다. 등록 구성 페이지가 나타납니다.
4. 관리를 레거시 (장치 관리) 로 설정합니다. 다음을 클릭하거나 할당 (옵션) 을 선택합니다. 배달 그룹 할당 화면이 나타납니다.

Enrollment Profile	Enrollment Type
1 Enrollment Info	Select the enrollment type for Android devices
2 Platforms	<input type="radio"/> Fully managed/Work profile <input type="radio"/> COPE/Work profile <input checked="" type="radio"/> Legacy (device administrator)
Android Enterprise	
3 Assignment (optional)	

5. 전용 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장을 클릭합니다.

장치 관리자 모드에서 레거시 장치 관리를 계속하려면 이 프로필을 사용하여 등록하거나 재등록합니다. 사용자로 하여금 Secure Hub 를 다운로드하고 등록 서버 URL 을 제공하도록 하면 작업 프로필 장치와 유사하게 장치 관리자 장치를 등록할 수 있습니다.

Android Enterprise 로의 전환에 대한 Endpoint Management 지원에 대한 자세한 내용은 블로그 [Android Enterprise](#) 를 기본 Citrix Endpoint Management 서비스로 설정을 참조하십시오.

Android Enterprise 의 간소화된 앱 관리

이제 관리되는 Google Play 또는 Google 개발자 포털로 이동하지 않고도 XenMobile Server 용 앱을 승인하거나 게시할 수 있습니다. 따라서 몇 시간이 아닌 약 10 분 안에 앱을 승인하고 게시할 수 있습니다.

XenMobile Server 콘솔에서 공용 앱 스토어용 **Android Enterprise** 앱 승인. 이제 XenMobile Server 콘솔을 종료하지 않고도 관리되는 Google Play Store 앱을 승인할 수 있습니다. 검색 필드에 앱 이름을 입력하면 관리되는 Google Play Store UI 가 열리고 앱 승인 및 저장에 대한 지침이 표시됩니다. 결과에 앱이 표시되면 앱 세부 정보를 구성할 수 있습니다. [공용 앱 스토어 앱 추가](#)를 참조하십시오.

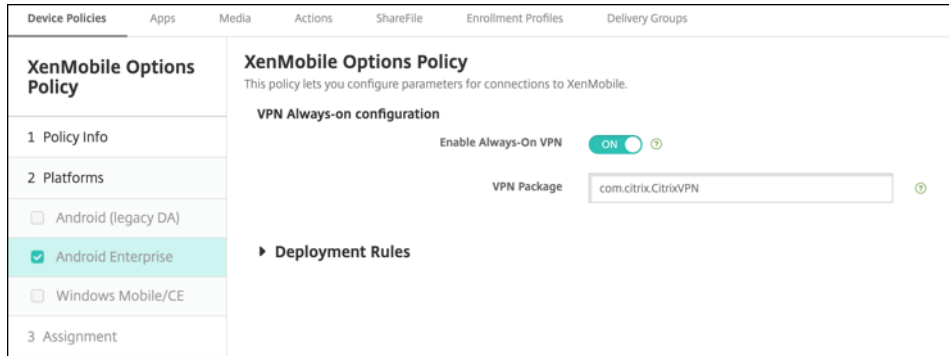
Android Enterprise 용 **MDX** 앱 추가. 이제 XenMobile Server 콘솔에서 Android Enterprise 가 MDX 앱 배포 플랫폼으로 지원됩니다. [MDX 앱 추가](#)를 참조하십시오.

XenMobile Server 콘솔에서 **Android Enterprise** 용 **MDX** 앱 승인. 이제 XenMobile Server 콘솔을 종료하지 않고도 Android Enterprise 용 관리되는 Google Play Store 앱을 승인할 수 있습니다. MDX 파일을 업로드하면 관리되는 Google Play Store UI 가 열리고 앱 승인 및 저장에 대한 지침이 표시됩니다. [MDX 앱 추가](#)를 참조하십시오.

Android Enterprise 에 대한 항상 VPN 연결 지원

이제 XenMobile Server 옵션 장치 정책에서 Android Enterprise 에 대해 항상 VPN 연결을 사용하도록 설정할 수 있습니다.

Android Enterprise ○에 대한 VPN 프로필을 구성할 때 기본 **VPN** 프로필에 VPN 프로필의 이름을 입력합니다. XenMobile 은 사용자가 특정 프로필을 누르지 않고 Citrix SSO 앱의 사용자 인터페이스에서 연결 스위치를 누를 때 이 프로필을 사용합니다. 이 필드를 비워 두면 기본 프로필이 연결에 사용됩니다. 하나의 프로필만 구성된 경우 기본 프로필로 표시됩니다. 항상 VPN 연결의 경우 항상 VPN 연결을 설정하는 데 사용할 VPN 프로필의 이름으로 이 필드를 설정해야 합니다.



Android Enterprise 앱에 대한 제품 트랙 구성

Android Enterprise 에 대한 공용 앱 스토어 앱 또는 MDX 앱을 추가할 때 사용자 장치에 표시할 제품 트랙을 구성할 수 있습니다. 예를 들어 테스트용으로 설계된 추적이 있는 경우 해당 추적을 선택하여 특정 배달 그룹에 할당할 수 있습니다. 릴리스 롤아웃에 대한 자세한 내용은 [Google Play 도움말 센터](#)를 참조하십시오. 제품 트랙 구성에 대한 자세한 내용은 [MDX 앱 추가](#) 또는 [공용 앱 스토어 앱 추가](#)를 참조하십시오.

macOS 사용자에게 대한 암호 재설정 강제

macOS 장치에 암호 정책이 포함된 구성 프로필이 수신되는 경우 사용자는 정책 설정을 충족하는 암호를 제공해야 합니다. 이제 사용자의 다음 인증 시에 암호 재설정을 강제할 수 있습니다. macOS(10.13 이상) 에 대한 암호 장치 정책에서 새로운 설정인 **Force passcode reset**(암호 재설정 강제 적용) 을 사용하도록 설정합니다. 암호 정책에 대한 자세한 내용은 [암호 장치 정책](#)을 참조하십시오.

XenMobile Server 10.11 의 새로운 기능

May 6, 2022

[XenMobile Server 10.11](#)(PDF 다운로드)

XenMobile 마이그레이션 서비스

XenMobile Server 를 온-프레미스에서 사용하는 경우 무료 XenMobile 마이그레이션 서비스를 사용하여 Endpoint Management 를 시작할 수 있습니다. XenMobile Server 에서 Citrix Endpoint Management 로 마이그레이션할 때

장치를 재등록할 필요는 없습니다.

마이그레이션을 시작하려면 해당 지역의 Citrix 영업 사원 또는 Citrix 파트너에게 문의하십시오. 자세한 내용은 [XenMobile 마이그레이션 서비스](#)를 참조하십시오.

Apple Volume Purchase Program 을 ABM(Apple Business Manager) 및 ASM(Apple School Manager) 으로 마이그레이션

Apple VPP(Volume Purchase Program) 를 사용하는 회사 및 교육 기관에서는 2019 년 12 월 1 일 전에 Apple Business Manager 또는 Apple School Manager 의 앱 및 서적으로 마이그레이션해야 합니다.

XenMobile 에서 VPP 계정을 마이그레이션하기 전에 이 [Apple 지원 문서](#)를 참조하십시오.

조직 또는 학교에서 VPP(Volume Purchase Program) 만 사용하는 경우 ABM/ASM 에 등록된 다음 기존 VPP 구매자를 새 ABM/ASM 계정으로 초대할 수 있습니다. ASM 의 경우 <https://school.apple.com>으로 이동합니다. ABM 의 경우 <https://business.apple.com>으로 이동합니다.

XenMobile 에서 볼륨 구매 (이전 VPP) 계정을 업데이트하려면:

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 볼륨 구매를 클릭합니다. 볼륨 구매 구성 페이지가 나타납니다.
3. ABM 또는 ASM 계정에 이전 VPP 계정과 동일한 앱 구성이 있는지 확인합니다.
4. ABM 또는 ASM 포털에서 업데이트된 토큰을 다운로드합니다.
5. XenMobile 콘솔에서 다음을 수행합니다.
 - a) 해당 위치에 대한 업데이트된 토큰 정보로 기존 볼륨 구매 계정을 편집합니다.
 - b) ABM 또는 ASM 자격 증명을 편집합니다. 접미사를 변경하지 마십시오.
 - c) 저장을 두 번 클릭합니다.

iOS 13 에 대한 추가 지원

중요:

iOS 12 이상으로 장치를 업그레이드하기 위한 준비: iOS 용 VPN 장치 정책의 Citrix VPN 연결 유형은 iOS 12 이상을 지원하지 않습니다. VPN 장치 정책을 삭제하고 Citrix SSO 연결 유형으로 새 VPN 장치 정책을 만듭니다.

VPN 장치 정책을 삭제한 후 Citrix VPN 연결은 이전에 배포된 장치에서 계속 작동합니다. 새 VPN 장치 정책 구성은 사용자 등록 중에 XenMobile Server 10.11 에서 적용됩니다.

XenMobile Server 는 iOS 13 으로 업그레이드된 장치를 지원합니다. 업그레이드는 사용자에게 다음과 같은 영향을 미칩니다.

- 등록하는 동안 몇 개의 새로운 iOS Setup Assistant(설정 도우미) 옵션 화면이 나타납니다. Apple 은 iOS 13 에 새로운 iOS Setup Assistant(설정 도우미) 옵션 화면을 추가했습니다. 새 옵션은 이 릴리스의 설정 > **Apple DEP**(장치 등록 프로그램) 페이지에 포함되지 않습니다. 따라서 이러한 화면을 건너뛰도록 XenMobile Server 를 구성할 수 없습니다. 이러한 페이지는 iOS 13 장치 사용자에게 나타납니다.
- iOS 13 이상에서는 이전 버전의 iOS 에 대한 감독 또는 감독되지 않은 장치에서 사용할 수 있었던 일부 제한 장치 정책 설정을 감독되는 장치에서만 사용할 수 있습니다. 현재 XenMobile Server 콘솔의 도구 설명에는 이러한 설정이 iOS 13 이상에서 감독되는 장치 전용이라는 설명이 표시되지 않습니다.
 - 하드웨어 제어 허용:
 - ★ FaceTime
 - ★ 앱 설치
 - 앱 허용:
 - ★ iTunes 스토어
 - ★ Safari
 - ★ Safari > 자동 채우기
 - 네트워크 - iCloud 동작 허용:
 - ★ iCloud 문서 및 데이터
 - 감독되는 경우에만 해당되는 설정 - 허용:
 - ★ 게임 센터 > 친구 추가
 - ★ 게임 센터 > 멀티플레이 게임
 - 미디어 콘텐츠 - 허용:
 - ★ 음악, 팟캐스트 및 iTunes U 의 성인 등급 자료

이러한 제한은 다음과 같이 적용됩니다.

- iOS 12 이하 장치가 이미 XenMobile Server 에 등록되어 있는 상태에서 iOS 13 으로 업그레이드하는 경우 위의 제한 사항은 감독되지 않는 장치 및 감독되는 장치에 적용됩니다.
- 감독되지 않는 iOS 13 이상 장치를 XenMobile Server 에 등록하는 경우 위의 제한 사항은 감독되는 장치에만 적용됩니다.
- 감독되는 iOS 13 이상 장치를 XenMobile Server 에 등록하는 경우 위의 제한 사항은 감독되는 장치에만 적용됩니다.

iOS 13 및 macOS 15 의 신뢰할 수 있는 인증서에 대한 요구 사항

Apple 은 TLS 서버 인증서에 대한 새로운 요구 사항을 도입했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는지 확인하십시오. Apple 게시물 <https://support.apple.com/en-us/HT210176>를 참조하십시오. 인증서 관리에 대한 도움말은 [XenMobile 에서 인증서 업로드](#)를 참조하십시오.

GCM 에서 FCM 으로 업그레이드

2018 년 4 월 10 일을 기준으로 Google 은 GCM(Google Cloud Messaging) 을 더 이상 사용하지 않습니다. Google 은 2019 년 5 월 29 일에 GCM 서버 및 클라이언트 API 를 제거했습니다.

중요 요구 사항:

- 최신 버전의 XenMobile Server 로 업그레이드하십시오.
- 최신 버전의 Secure Hub 로 업그레이드하십시오.

Google 에서는 FCM 의 새로운 기능을 활용할 수 있도록 즉시 FCM(Firebase Cloud Messaging) 으로 업그레이드 할 것을 권장합니다. Google 의 자세한 내용은 <https://developers.google.com/cloud-messaging/faq> 및 <https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html> 을 참조하십시오.

Android 장치로의 푸시 알림에 대한 지원을 계속하려면: XenMobile Server 에서 GCM 을 사용하는 경우 FCM 으로 마이그레이션합니다. 그런 다음 Firebase Cloud Messaging 콘솔에서 제공되는 새 FCM 키를 사용하여 XenMobile Server 를 업데이트합니다.

다음 단계는 신뢰할 수 있는 인증서를 사용할 때의 등록 워크플로에 대한 것입니다.

업그레이드 단계:

1. Google 의 정보에 따라 GCM 에서 FCM 으로 업그레이드합니다.
2. Firebase Cloud Messaging 콘솔에서 새 FCM 키를 복사합니다. 이 키는 다음 단계를 수행하는 데 필요합니다.
3. XenMobile Server 콘솔에서 설정 > **Firebase Cloud Messaging** 으로 이동하고 설정을 구성합니다.

다음에 XenMobile Server 로 체크인하고 정책 새로 고침을 수행하면 장치가 FCM 으로 전환됩니다. Secure Hub 에서 장치를 새로 고치려면: Secure Hub 에서 기본 설정 > 장치 정보로 이동하고 정책 새로 고침을 누릅니다.

FCM 구성에 대한 자세한 내용은 [Firebase Cloud Messaging](#) 을 참조하십시오.

XenMobile 마이그레이션 서비스

XenMobile Server 를 온-프레미스에서 사용하는 경우 XenMobile 마이그레이션 서비스를 사용하여 Endpoint Management 를 시작할 수 있습니다. XenMobile Server 에서 Citrix Endpoint Management 로 마이그레이션할 때 장치를 재등록할 필요는 없습니다.

자세한 내용은 해당 지역의 Citrix 영업 사원, 시스템 엔지니어 또는 Citrix 파트너에게 문의하십시오. 다음 블로그에 XenMobile 마이그레이션 서비스에 대한 자세한 내용이 나와 있습니다.

[New XenMobile Migration Service\(새로운 XenMobile 마이그레이션 서비스\)](#)

[Making the Case for XenMobile in the Cloud\(클라우드에서 XenMobile 용 사례 만들기\)](#)

XenMobile 10.11 로 업그레이드하기 전에 (온-프레미스)

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 [시스템 요구 사항 및 호환성](#) 과 [XenMobile 호환성](#) 을 참조하십시오.

1. 최신 버전의 XenMobile Server 10.11 로 업데이트하기 전에 Citrix License Server 를 11.15 이상으로 업데이트 하십시오.

최신 버전의 XenMobile 에는 Citrix License Server 11.15(최소 버전) 가 필요합니다.

참고:

미리 보기에 자체 라이선스를 사용하려는 경우 XenMobile 10.11 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2019 년 4 월 9 일이라는 점을 숙지하십시오. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 이후여야 합니다.

날짜는 라이선스 서버의 라이선스 옆에서 볼 수 있습니다. 최신 버전의 XenMobile 을 이전 버전의 라이선스 서버 환경에 연결하면 연결 확인이 실패하고 라이선스 서버를 구성할 수 없게 됩니다.

라이선스의 날짜를 갱신하려면 Citrix 포털에서 최신 라이선스 파일을 다운로드하고 라이선스 서버에 파일을 업로드하십시오. 자세한 내용은 [Customer Success Services](#)를 참조하십시오.

2. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 iOS 정책 및 앱을 배포하려면 다음과 같은 요구 사항이 충족되어야 합니다. Citrix Gateway 에 SSL 지속성이 구성되어 있으면 모든 XenMobile Server 노드에서 포트 80 을 열어야 합니다.
3. 업그레이드할 XenMobile Server 를 실행하는 가상 컴퓨터의 RAM 이 4GB 미만인 경우 4GB 이상으로 RAM 을 늘리십시오. 프로덕션 환경에 권장되는 최소 RAM 은 8GB 입니다.
4. XenMobile 업데이트를 설치하기 전에 VM 의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

XenMobile 10.10.x 또는 10.9.x 에서 XenMobile 10.11 로 직접 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 이진 파일을 다운로드합니다. <https://www.citrix.com/downloads>로 이동하십시오. **Citrix Endpoint Management(및 Citrix XenMobile Server) > XenMobile Server(온-프레미스) > 제품 소프트웨어 > XenMobile Server 10** 으로 이동합니다. 해당하는 하이퍼바이저에 대한 XenMobile Server 소프트웨어 타일에서 파일 다운로드를 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다. 자세한 내용은 [릴리스 관리 페이지를 사용하여 업그레이드하려면](#)을 참조하십시오.

업그레이드 후

XenMobile 10.11 으로 업그레이드한 후 (온-프레미스):

연결 구성을 변경하지 않았는데도 발신 연결이 관련된 기능이 작동을 중지하는 경우 XenMobile Server 로그에 다음과 같은 오류가 있는지 확인하십시오. “VPP Server 에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’ 이 피어가 제공한 인증서 제목과 일치하지 않습니다.”

이 인증서 유효성 검사 오류는 XenMobile Server 에서 호스트 이름 유효성 검사를 비활성화해야 함을 나타냅니다. 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다. 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 `disable.hostname.verification`을 `true`로 변경하십시오. 이 속성의 기본값은 `false`입니다.

Android Enterprise 장치의 신규 및 업데이트된 장치 정책 설정

Samsung Knox 와 **Android Enterprise** 정책 통합. Samsung Knox 3.0 이상과 Android 8.0 이상을 실행하는 Android Enterprise 장치의 경우: Knox 와 Android Enterprise 가 통합 장치 및 프로필 관리 솔루션으로 결합됩니다. 다음 장치 정책의 Android Enterprise 페이지에서 Knox 설정을 구성합니다.

- **OS 업데이트 장치 정책.** Samsung Enterprise FOTA 업데이트에 대한 설정이 포함되어 있습니다.
- **암호 장치 정책.**
- **Samsung MDM 라이선스 키 장치 정책.** Knox 라이선스 키를 구성합니다.
- **제한 장치 정책 설정.**

The screenshot shows the 'Restrictions Policy' configuration page in the XenMobile Server console. The left sidebar lists various policies, with 'Android Enterprise' selected. The main area displays the configuration for this policy, including sections for 'Allow USB actions', 'Network', 'Security', and 'Assignment'. Each section contains several settings with toggle switches.

Section	Setting	Value
Allow USB actions	Debugging	OFF
	File transfer	OFF
Network	Allow VPN Configuration	ON
	Android beam	ON
	Allow configuring location provider	ON
Security	Allow use of the status bar	OFF
	Keep the keyguard from locking the device	OFF
	Allow Account Management	OFF
	Keep the device screen on	OFF
Assignment	Allow cross profile copy and paste	OFF

Android Enterprise 의 앱 인벤토리 장치 정책. 이제 관리되는 장치에서 Android Enterprise 앱의 인벤토리를 수집할 수 있습니다. [앱 인벤토리 장치 정책](#)을 참조하십시오.

관리되는 **Google Play Store** 의 모든 **Google Play** 앱에 액세스. 관리되는 **Google Play Store** 의 모든 앱에 액세스

서버 속성을 사용하면 관리되는 Google Play Store 에서 공용 Google Play Store 의 모든 앱에 액세스할 수 있습니다. 이 속성을 **true** 로 설정하면 모든 Android Enterprise 사용자에게 대한 공용 Google Play Store 앱이 허용됩니다. 이후 관리자는 [제한 장치 정책](#)을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다.

Android Enterprise 장치에서 시스템 앱 사용. Android Enterprise 작업 프로필 모드 또는 완전 관리형 모드에서 사용자가 앱에 미리 설치된 시스템 앱을 실행할 수 있도록 하려면 [제한 장치 정책](#)을 구성합니다. 이 구성은 카메라, 갤러리 및 기타 기본 장치 앱에 대한 액세스 권한을 사용자에게 부여합니다. 특정 앱에 대한 액세스를 제한하려면 [Android Enterprise 앱 권한 장치 정책](#)을 사용하여 앱 권한을 설정합니다.

Android Enterprise 전용 장치에 대한 지원. 이제 XenMobile 이 COSU(회사 소유 일회 사용) 장치라고 하는 전용 장치의 관리를 지원합니다.

전용 Android Enterprise 장치는 단일 사용 사례를 이행하는 데 전용으로 사용되는 완전 관리형 장치입니다. 이러한 장치는 이 사용 사례에 필요한 작업을 수행하는 데 필요한 단일 앱 또는 소수의 앱으로 제한되어야 합니다. 또한 사용자가 장치에서 다른 앱을 사용하도록 설정하거나 다른 작업을 수행하지 못하도록 차단해야 합니다.

Android Enterprise 장치 프로비저닝에 대한 자세한 내용은 [전용 Android Enterprise 장치 프로비저닝](#)을 참조하십시오.

정책 이름 변경. Google 용어에 맞추기 위해 Android Enterprise 앱 제한 장치 정책의 이름이 이제 관리되는 구성 장치 정책으로 변경되었습니다. [관리되는 구성 장치 정책](#)의 내용을 참조하십시오.

Android Enterprise 의 잠금 및 암호 재설정

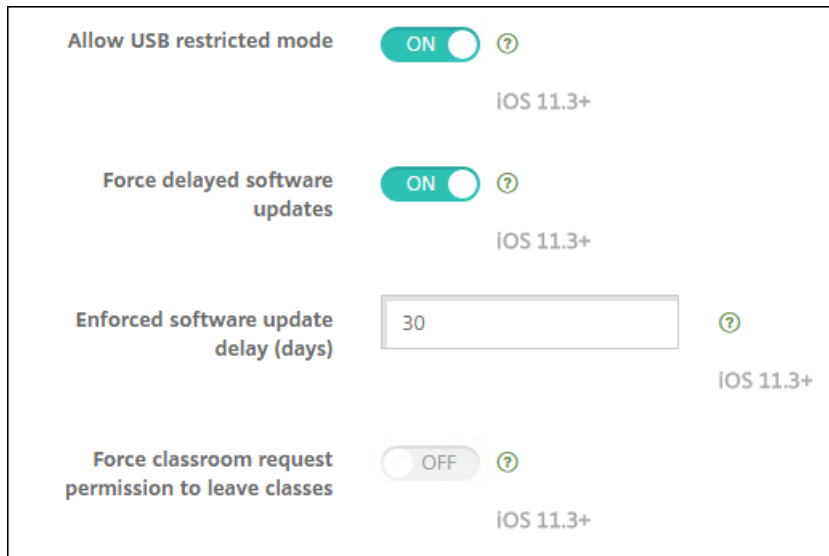
XenMobile 은 이제 Android Enterprise 장치에 대한 잠금 및 암호 재설정 보안 동작을 지원합니다. 이러한 장치는 Android 8.0 이상을 실행하는 작업 프로필 모드에 등록되어야 합니다.

- 전송된 암호로 작업 프로필이 잠깁니다. 장치는 잠기지 않습니다.
- 암호가 전송되지 않았거나 전송된 암호가 암호 요구 사항을 충족하지 않는 경우:
 - 작업 프로필에 암호가 이미 설정되어 있지 않으면 장치가 잠깁니다.
 - 작업 프로필에 암호가 이미 설정되어 있으면 작업 프로필은 잠기지만 장치는 잠기지 않습니다.

잠금 및 암호 재설정 보안 동작에 대한 자세한 내용은 [보안 동작](#)을 참조하십시오.

iOS 또는 macOS 의 새로운 제한 장치 정책 설정

- **관리되지 않는 앱이 관리되는 연락처 읽기:** 선택 사항. 관리되지 않는 앱에 있는 관리되는 앱의 문서가 사용되지 않는 경우에만 사용할 수 있습니다. 사용하도록 설정하면 관리되지 않는 앱이 관리되는 계정의 연락처에서 데이터를 읽을 수 있습니다. 기본값은 꺼짐입니다. iOS 12 부터 사용할 수 있습니다.
- **관리되는 앱이 관리되지 않는 연락처 쓰기:** 선택 사항. 사용하도록 설정하면 관리되는 앱에서 관리되지 않는 계정의 연락처에 연락처를 쓸 수 있습니다. 관리되지 않는 앱에 있는 관리되는 앱의 문서를 사용하는 경우 이 제한은 영향을 미치지 않습니다. 기본값은 꺼짐입니다. iOS 12 부터 사용할 수 있습니다.
- **암호 자동 채우기:** 선택 사항입니다. 사용하지 않는 경우 사용자는 암호 자동 채우기 또는 강력한 자동 암호 기능을 사용할 수 없습니다. 기본값은 켜짐입니다. iOS 12 및 macOS 10.14 부터 사용할 수 있습니다.
- **암호 근접 요청:** 선택 사항입니다. 사용하지 않는 경우 사용자의 장치는 주변 장치에서 암호를 요청하지 않습니다. 기본값은 켜짐입니다. iOS 12 및 macOS 10.14 부터 사용할 수 있습니다.
- **암호 공유:** 선택 사항입니다. 사용하지 않는 경우 사용자는 AirDrop 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 켜짐입니다. iOS 12 및 macOS 10.14 부터 사용할 수 있습니다.
- **자동 날짜 및 시간 적용:** 감독되는 장치. 사용하는 경우 사용자는 일반 > 날짜 및 시간 > 자동 설정 옵션을 사용하지 않도록 설정할 수 없습니다. 기본값은 꺼짐입니다. iOS 12 부터 사용할 수 있습니다.
- **USB 제한 모드 허용:** 감독되는 장치에서만 사용할 수 있습니다. 꺼짐인 경우 장치가 잠겨 있는 동안 항상 USB 액세서리에 연결할 수 있습니다. 기본값은 켜짐입니다. iOS 11.3 부터 사용할 수 있습니다.
- **소프트웨어 업데이트 강제 지연:** 감독되는 장치에서만 사용할 수 있습니다. 켜짐으로 설정하면 사용자에게 소프트웨어 업데이트 표시가 지연됩니다. 이 제한을 적용하면 소프트웨어 업데이트 릴리스 날짜로부터 지정된 기간 (일) 까지 소프트웨어 업데이트가 표시되지 않습니다. 기본값은 꺼짐입니다. iOS 11.3 및 macOS 10.13.4 부터 사용할 수 있습니다.
- **소프트웨어 업데이트 시행 지연 (일):** 감독되는 장치에서만 사용할 수 있습니다. 관리자는 이 제한을 사용하여 장치의 소프트웨어 업데이트를 지연할 일 수를 설정할 수 있습니다. 최대값은 90 일이고 기본값은 **30** 입니다. iOS 11.3 및 macOS 10.13.4 부터 사용할 수 있습니다.
- **교실에서 클래스를 나갈 때 허가 요청 시행:** 감독되는 장치에서만 사용할 수 있습니다. 켜짐으로 설정하면 교실 앱을 통해 관리되지 않는 과정에 등록한 학생이 과정을 나가려면 교사의 허가를 요청해야 합니다. 기본값은 꺼짐입니다. iOS 11.3 부터 사용할 수 있습니다.



제한 장치 정책을 참조하십시오.

iOS 또는 macOS 에 대한 Exchange 장치 정책 업데이트

iOS 12 이상의 추가 **S/MIME Exchange** 서명 및 암호화 설정. 이제 Exchange 장치 정책에 S/MIME 서명 및 암호화를 구성하는 설정이 포함됩니다.

S/MIME 서명의 경우:

- 서명 **ID** 자격 증명: 사용할 서명 자격 증명을 선택합니다.
- **S/MIME** 서명 사용자 재정의의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다.
- **S/MIME** 서명 인증서 **UUID** 사용자 재정의의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 꺼짐입니다.

S/MIME 암호화의 경우:

- 암호화 **ID** 자격 증명: 사용할 암호화 자격 증명을 선택합니다.
- 메시지별 **S/MIME** 전환 사용: 켜짐으로 설정하면 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션이 표시됩니다. 기본값은 꺼짐입니다.
- 기본적으로 **S/MIME** 암호화 사용자 재정의의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 를 기본적으로 켜지 여부를 선택할 수 있습니다. 기본값은 꺼짐입니다.
- **S/MIME** 암호화 인증서 **UUID** 사용자 재정의의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다.

iOS 12 이상의 **Exchange OAuth** 설정. 이제 인증에 OAuth 를 사용하도록 Exchange 연결을 구성할 수 있습니다.

macOS 10.14 이상의 **Exchange OAuth** 설정. 이제 인증에 OAuth 를 사용하도록 Exchange 연결을 구성할 수 있습니다. OAuth 를 사용한 인증의 경우 자동 검색을 사용하지 않는 설정에 대한 로그인 URL 을 지정할 수 있습니다.

[Exchange 장치 정책](#)을 참조하십시오.

iOS 용 메일 장치 정책 업데이트

iOS 12 이상의 추가 **S/MIME Exchange** 서명 및 암호화 설정. 메일 장치 정책에 S/MIME 서명 및 암호화를 구성하는 추가 설정이 포함됩니다.

S/MIME 서명의 경우:

- **S/MIME 서명 사용:** 이 계정이 S/MIME 서명을 지원하는지 여부를 선택합니다. 기본값은 켜짐입니다. 켜짐으로 설정하면 다음 필드가 나타납니다.
 - **S/MIME 서명 사용자 재정의 가능:** 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
 - **S/MIME 서명 인증서 UUID 사용자 재정의 가능:** 켜짐으로 설정하면 사용자가 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

S/MIME 암호화의 경우:

- **S/MIME 암호화 사용:** 이 계정이 S/MIME 암호화를 지원하는지 여부를 선택합니다. 기본값은 꺼짐입니다. 켜짐으로 설정하면 다음 필드가 나타납니다.
 - 메시지별 **S/MIME** 전환 사용: 켜짐으로 설정하면 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션이 표시됩니다. 기본값은 꺼짐입니다.
 - 기본적으로 **S/MIME** 암호화 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 를 기본적으로 켜지 여부를 선택할 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
 - **S/MIME** 암호화 인증서 **UUID** 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

[메일 장치 정책](#)을 참조하십시오.

iOS 용 앱 알림 장치 정책 업데이트

다음 앱 알림 설정은 iOS 12 부터 사용할 수 있습니다.

- **CarPlay** 로 표시: 켜짐인 경우 Apple CarPlay 에 알림이 표시됩니다. 기본값은 켜짐입니다.
- **중요 알림 사용:** 켜짐인 경우 앱이 방해 금지 및 벨소리 설정을 무시하는 중요 알림으로 알림을 표시할 수 있습니다. 기본값은 꺼짐입니다.

[앱 알림 장치 정책](#)을 참조하십시오.

Apple Education 에 사용되는 공유 iPad 지원

XenMobile 과 Apple Education 통합 기능에서 이제 공유 iPad 가 지원됩니다. 한 교실에 있는 여러 학생이 한 명 또는 여러 명의 강사가 가르치는 다양한 과목에서 iPad 를 공유할 수 있습니다.

관리자 또는 강사는 공유 iPad 를 등록한 다음 장치 정책, 앱 및 미디어를 장치에 배포합니다. 그런 다음 수강생은 관리되는 Apple ID 자격 증명을 제공하여 공유 iPad 에 로그인합니다. 이전에 교육 구성 정책을 학생에게 배포한 경우 학생은 장치를 공유할 때 “기타 사용자” 로 로그인하지 않습니다.

공유 iPad 에 대한 사전 요구 사항:

- 모든 iPad Pro, iPad 5 세대, iPad Air 2 이상 및 iPad 미니 4 이상
- 최소 32GB 의 스토리지
- 감독됨

자세한 내용은 [공유 iPad 구성](#)을 참조하십시오.

RBAC(역할 기반 액세스 제어) 권한 변경

로컬 사용자 추가/삭제 RBAC 권한이 로컬 사용자 추가와 로컬 사용자 삭제의 두 가지 권한으로 분할되었습니다.

자세한 내용은 [RBAC 를 사용하여 역할 구성](#)을 참조하십시오.

타사 고지 사항

January 5, 2022

XenMobile 의 이 릴리스에는 다음 문서에 정의된 약관에 따라 사용이 허가된 타사 소프트웨어가 포함될 수 있습니다.

[XenMobile 타사 고지 사항](#)

사용 중단

April 14, 2023

이 문서의 발표 내용은 단계적으로 중단되는 XenMobile Server 기능에 대한 사전 알리를 제공하기 위한 것입니다. 회사에서 적시에 의사 결정을 내릴 수 있도록 돕기 위해 이 정보를 제공합니다. Citrix 는 고객의 사용 및 피드백을 모니터링하여 이러한 중단 시기를 결정합니다. 발표 내용은 후속 릴리스에서 변경될 수 있으며 사용되지 않는 모든 기능이 발표에 포함되지 않을 수 있습니다. 제품 수명 주기 지원에 대한 자세한 내용은 [제품 수명 주기 지원 정책](#) 문서를 참조하십시오.

지원 중단 및 제거

다음 목록에는 사용되지 않거나 제거된 XenMobile Server 기능이 나와 있습니다.

사용되지 않는 항목은 즉시 제거되지 않습니다. Citrix 는 사용되지 않는 항목이 향후 릴리스에서 제거되기 전까지 이러한 항목에 대한 지원을 계속합니다.

제거된 항목은 XenMobile Server 에서 제거되거나 더 이상 지원되지 않습니다.

수명 종료에 도달한 모바일 생산성 앱에 대한 자세한 내용은 [EOL 및 사용되지 않는 앱](#)을 참조하십시오.

항목	설명	사용 중단 발표	제거됨	대체
Zebra 용 사용자 지정 XML	Zebra 장치의 사용자 지정 XML 에 대한 지원 중단됨	January 2022	Target: June 2022	Android Enterprise 관리되는 구성을 사용합니다.
Windows Information Protection(WIP)	Microsoft 의 발표 (여기) 에 따라 Windows Information Protection 은 더 이상 지원되지 않습니다.	August 2022	목표: 2022 년 10 월	대체 없음
Xenmobile Analyzer	Xenmobile Analyzer 도구에 대한 지원이 중단되었습니다.	July 2022	목표: March 31, 2023	대체 없음
PKI ID: 일반, Symantec PKI, DigiCert, Entrust 어댑터	일반, DigiCert 관리 형 및 Entrust 어댑터 PKI 엔터티는 더 이상 지원되지 않습니다.	June 2021	January 2022	대체 없음
등록 초대 설정	장치 IMEI, 일련 번호 및 UDID 를 사용하여 등록 초대를 만드는 지원은 더 이상 사용되지 않습니다.	January 2022	May 2022	등록 초대를 만들 때 XenMobile 콘솔의 관리 > 등록 초대에서 사용 가능한 설정을 구성합니다.
이동 통신 사업자 SMS 게이트웨이	Nexmo SMS 게이트웨이 알림에 대한 지원이 중단됨	January 2022	April 2022	SMTP 서버 알림 사용

항목	설명	사용 중단 발표	제거됨	대체
모바일 서비스 공급자 (MSP)	BlackBerry 및 기타 Exchange ActiveSync 장치를 쿼리하고 작업을 실행하는 MSP 인터페이스에 대한 지원이 중단됨	January 2022	April 2022	대체 없음
Samsung 키오스크 모드	장치 관리자 (DA) 모드에 기반한 레거시 Samsung 키오스크 모드의 지원을 중단합니다.	January 2022	March 2022	Android Enterprise(AE) 키오스크 모드를 사용합니다.
Windows 장치에 대한 Wi-Fi 감지 핫스팟 자동 연결 제한을 허용합니다.	Windows 10 장치에 대한 Wi-Fi 감지 핫스팟 자동 연결 제한 허용 지원을 제거합니다. Windows 10 은 더 이상 이 기능을 지원하지 않습니다. 자세한 내용은 Microsoft 설명서 를 참조하십시오.	October 2021	February 2022	대체 없음
Samsung SAFE/Samsung Knox 플랫폼	SAFE 및 Knox 플랫폼에 대한 지원이 중단되었습니다.	January 2022	June 2022	Android Enterprise 로 Knox 정책을 설정하려면 관리형 앱 구성 정책을 통해 Knox 서비스 플러그인을 사용합니다.
높은 보안 등록 모드	높은 보안 등록 보안 모드를 사용한 등록 초대 생성은 더 이상 지원되지 않습니다.	July 2021	February 2022	지원되는 등록 보안 모드 목록은 장치 등록 을 참조하십시오.
RBAC 역할 - 공유 장치 등록자 및 COSU 장치 등록자	공유 장치 등록자와 COSU 장치 등록자 모두에 미리 정의된 역할 기반 액세스 제어 설정의 지원을 중단합니다.	July 2021	December 2021	지원되는 등록 방법 을 통해 iOS 장치를 구성합니다. 등록 프로파일 을 통해 Android COSU (전용) 장치를 구성합니다.

항목	설명	사용 중단 발표	제거됨	대체
Knox Mobile Enrollment(레거시 DA)	모든 Android 버전에서 레거시 장치 관리자 모드인 KME(Knox Mobile Enrollment)에 대한 지원이 사용되지 않습니다.	May 2021	June 2021	KME 를 사용하여 Android Enterprise 모드로 등록합니다. Android 9, 10, 11 은 Android Enterprise 를 지원 합니다.
Android 7.x 및 iOS 12.x 용 Citrix 모바일 앱 및 Workspace 앱	Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱의 Android 7.x 및 iOS 12.x 버전에 대한 지원이 중단되었습니다.	2021 년 4 월	June 2021	최소한 각 주요 운영 체제 플랫폼의 현재 및 이전 버전을 사용합니다. 이전 장치는 등록된 상태로 유지됩니다. 그러나 Citrix 는 레거시 장치를 테스트하거나 지원하지 않습니다.
파생된 자격 증명	파생된 자격 증명 및 Citrix Derived Credential Manager 앱에 대한 지원이 중단되었습니다.	March 2021	December 2021	iOS 에서 지원되는 인증 유형 목록은 iOS 를 참조하십시오.
Internet Explorer 11	XenMobile Server 콘솔에서는 Internet Explorer 사용이 더 이상 지원되지 않습니다.	January 2021	January 2021	Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari 중 하나의 최신 버전을 사용 하십시오.
Android 용 RSA 소프트웨어 토큰 지원	Android 용 Secure Hub 에 RSA 소프트웨어 토큰 직접 가져오는 더 이상 지원되지 않습니다.	January 2021	February 2021	Google Play 에서 제공되는 RSA 보안 ID 앱 내부에서 RSA 소프트웨어 토큰을 가져올 수 있습니다. 그런 다음 Citrix Gateway 인증에 토큰을 사용할 수 있습니다.

항목	설명	사용 중단 발표	제거됨	대체
Android - Sony	Android Sony 장치 및 Sony 관련 정책에 대한 지원은 중단되었습니다.	January 2021	February 2022	Android Enterprise 사용
Android - HTC	Android HTC 장치 및 HTC 관련 정책에 대한 지원은 중단되었습니다.	January 2021	February 2022	Android Enterprise 사용
Android - Amazon	Android Amazon 장치 및 Amazon 관련 정책에 대한 지원은 중단되었습니다.	January 2021	February 2022	Android Enterprise 사용
XenMobile 대시보드의 타사 구성 요소	XenMobile 대시보드의 일부로 사용되는 타사 구성 요소는 사용 중단될 예정입니다.	December 2020	January 2021	대시보드를 계속 사용하려면 XenMobile 10.12 이상으로 업그레이드하십시오.
Android Enterprise 장치에서 레거시 장치 관리자 모드에 대해 게시된 앱	Android Enterprise에 등록된 장치에 레거시 DA 플랫폼용으로 게시된 앱은 더 이상 제공되지 않습니다.	October 2020	November 2020	Android Enterprise 장치의 경우 Android Enterprise 플랫폼용으로 앱을 게시합니다. DA 모드인 장치에 레거시 DA 앱을 계속 게시하려면 이러한 앱에 대해 별도의 배달 그룹을 만듭니다.

항목	설명	사용 중단 발표	제거됨	대체
APNs 송신 포트	<p>APN 레거시 바이너리 프로토콜에 대한 Apple 의 지원은 2021 년 3 월 31 일부로 종료됩니다.</p> <p>Apple 에서는 HTTP/2 기반 APN 제공업체 API 를 대신 사용하도록 권장합니다. 이 변경의 일환으로 APN 알림을 *.push.apple.com에 보내는 데 사용되는 포트 2195 및 2196 이 더 이상 지원되지 않습니다.</p>	October 2020	March 2021	대신 포트 443 또는 2197 을 사용하십시오. 장치 관리를 위한 XenMobile 포트 열기 를 참조하십시오.
Samsung SEAMS 컨테이너	Samsung SEAMS 컨테이너에 대한 지원이 중단되었습니다.	June 2020	August 2020	<p>Android Enterprise 용 Samsung Knox 서비스 플러그인 (KSP) 앱을 사용합니다.</p> <p>Knox 서비스 플러그인 앱 추가를 참조하십시오.</p>
자체 서명된 SSL(Secure Sockets Layer) 인증서	모든 장치 플랫폼에서 자체 서명된 SSL 인증서 지원이 사용 중단되었습니다.	May 2020		이 SSL 인증서를 잘 알려진 CA(인증 기관)의 신뢰할 수 있는 SSL 인증서로 교체합니다.

항목	설명	사용 중단 발표	제거됨	대체
인증서 기반 인증 서명 알고리즘 (비 FIPS 및 약한 암호화)	다음 서명 알고리즘에 대한 지원이 사용 중단되었습니다. SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	May 2020	June 2021	XenMobile 콘솔에서 자격 증명 공급자의 CSR 을 만들 때 (설정 > 자격 증명 공급자 > 인증서 서명 요청 (CSR)) 더 강력한 암호화를 선택합니다.
데이터베이스 서버	Microsoft SQL Server 2014 이하에 대한 지원이 중단됩니다.	October 2021	August 2022	지원되는 다음 버전 중 하나로 시스템을 업데이트하십시오. Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 또는 Microsoft SQL Server 2019 CTP 3.2. 시스템 요구 사항 및 호환성 에서 지원되는 서버 목록을 참조하십시오.

항목	설명	사용 중단 발표	제거됨	대체
하이퍼바이저	Citrix XenServer 6.5.x 이전 버전과 VMware ESXi 5.5 업데이트 3 이전 버전, Hyper-V 2012 에 대한 지원이 중단되었습니다.	May 2020	August 2020	지원되는 다음 버전 중 하나로 시스템을 업데이트하십시오. Citrix Hypervisor 8.0 이상, Citrix XenServer 7.0 이상, VMware (ESXi 6.0, ESXi 6.5.0 업데이트 3, ESXi 6.7 업데이트 2 패치 10 또는 ESXi 7.0) 또는 Hyper-V (Windows Server 2016 또는 Windows Server 2019).
Citrix Launcher	레거시 Citrix Launcher 앱에 대한 지원이 중단되었습니다.	May 2020	August 2020 (앱 스토어에서 제거)	프로비저닝 장치를 키오스크 (전용 장치) 및 Android Enterprise 용 Citrix Launcher 로 사용할 수 있습니다. 자세한 내용은 Citrix Launcher 대체 를 참조하십시오.
Android 6.x 및 iOS 11.x 용 Citrix 모바일 앱 및 Workspace 앱	Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱의 Android 6.x 및 iOS 11.x 버전에 대한 지원이 중단되었습니다.	April 2020	June 2020	최소한 각 주요 운영 체제 플랫폼의 현재 및 이전 버전을 사용합니다.

항목	설명	사용 중단 발표	제거됨	대체
MDX Toolkit 및 MDX Service	MAM(모바일 애플리케이션 관리) SDK를 위해 MDX Toolkit 및 MDX Service에 대한 지원이 중단되었습니다. 전환 기간 동안 MDX 래핑 앱과 MAM SDK 개발 앱을 모두 사용할 수 있습니다.	March 2020	Target: July 2023	엔터프라이즈 응용 프로그램을 계속 관리하려면 MAM SDK를 사용합니다.
MDX: 대체 게이트웨이 서버	iOS 및 Android 장치에 대한 상위 단계 인증이 사용되지 않습니다.	March 2020	September 2021	대체 없음
MDX: Micro VPN(전체 터널 모드)	iOS 및 Android 장치에 대한 전체 VPN(가상 사설망) 터널이 사용되지 않습니다.	March 2020	September 2021	MAM SDK 웹 SSO 모드를 사용하거나 Citrix SSO 연결 유형을 사용하여 앱별 VPN 정책을 만듭니다.
MDX: PAC 파일 지원	iOS 및 Android 장치에 대한 전체 VPN 터널 배포에 사용되는 PAC(Proxy Automatic Configuration) 파일이 더 이상 지원되지 않습니다.	March 2020	September 2021	프록시 서버 연결을 통해 내부 네트워크에 액세스하려면 Citrix Gateway를 사용합니다.
MDX 공유 장치 지원	MDX 앱에 대한 공유 장치 지원이 중단되었습니다.	March 2020	September 2021	Android Enterprise의 경우 MDM에 대한 공유 장치 지원을 사용합니다. iOS의 경우 Apple School Manager 또는 GroundControl을 사용합니다.

항목	설명	사용 중단 발표	제거됨	대체
Android 10 의 신규 장치 관리자 등록	Android 10 장치에서 레거시 장치 관리자 모드에 대한 신규 등록 또는 재등록 지원이 중단되었습니다. 이미 등록된 장치는 계속 작동합니다.	February 2020	September 2020	Android 10 이상인 신규 장치를 Android Enterprise 에 등록합니다.
Android 10 장치의 레거시 장치 관리자 모드	Google 에서 일부 Device Administrator API 의 사용을 중단했습니다. Citrix 는 Citrix Secure Hub 를 대상 Android API 수준 29 로 업그레이드한 이후로 장치 관리자 모드에 등록된 Android 10 장치를 지원하지 않습니다.	February 2020	November 2020	Android 10 장치를 Android Enterprise 로 마이그레이션합니다.
MDX 암호화	XenMobile 콘솔에서 MDX 암호화 및 MDX 암호화 기능이 사용되지 않습니다.	October 2019	September 2020	규정 준수 확인이 추가된 암호화 관리 기능을 사용하여 iOS 또는 Android 플랫폼 암호화를 사용하도록 설정합니다. 2020 년 7 월까지 MDX 암호화 마이그레이션을 테스트하고 계획해야 합니다.
암호 장치 정책: Android Enterprise 에 대한 제한 없음 설정	Android 7 이상을 실행하는 Android Enterprise 장치에서 문자 제한이 있는 암호 생성만 지원됩니다. 이전에 필수 문자를 제한 없음으로 설정한 경우 이번 업데이트 이후 해당 값은 숫자만으로 변경됩니다.	February 2019	April 2019	이 변경 사항은 현재 사용자 로그인 환경에 영향을 주지 않습니다.

항목	설명	사용 중단 발표	제거됨	대체
원격 지원	클러스터링된 온-프레미스 XenMobile Server 배포에 대한 원격 지원 클라이언트가 더 이상 지원되지 않습니다.	January 2019	August 2020	대체 없음
iOS 용 Secure Hub 네트워크 확장	Secure Hub release 20.3.0 이후로 iOS 장치의 네트워킹 기능 사용자 지정을 허용하는 네트워크 확장 프레임워크가 사용되지 않습니다.	October 2018	March 2020	대체 없음
TLS 버전 1.0 및 1.1	XenMobile의 보안을 개선하기 위해 Citrix는 이제 TLS(전송 계층 보안) 1.0 및 1.1을 통한 모든 통신을 차단합니다. PCI 보안표준 위원회에서는 보안 약화를 이유로 TLS 1.0 및 TLS 1.1의 사용을 중단하고 있습니다.	June 2018	March 2019	TLS 1.2로 업그레이드합니다.
Windows Mobile/CE	Windows Mobile/CE 장치가 더 이상 지원되지 않습니다.	April 2018	September 2020	Windows 10 데스크톱 및 랩톱을 사용합니다.
Android TouchDown	DigiCert는 Android TouchDown 지원을 중단했습니다. Citrix는 Exchange 장치 정책에서 Android TouchDown 플랫폼 페이지를 삭제할 예정입니다.	2018년 7월	2021	권장 사항: Citrix Secure Mail을 사용하십시오.

수정된 문제

December 26, 2022

XenMobile 10.15 에서는 다음과 같은 문제가 수정되었습니다.

- iOS 15 또는 macOS 12 장치를 등록한 후 MDM 구성 프로필에 확인되지 않음으로 표시됩니다. [여기](#)에서 지원 문서를 참조하십시오. [CXM-98525]
- XenMobile Server 콘솔에서 앱의 설정을 수정하여 모든 플랫폼의 선택을 취소하고 저장하면 해당 앱이 구성 > 앱에 나열되지 않습니다. [CXM-99849]
- Android Enterprise 플랫폼에서 Citrix Launcher 를 종료할 수 없습니다. 다음 오류가 발생합니다. 암호가 잘못되었습니다. [CXM-100039]
- 일부 Android Enterprise 장치에서는 배달 그룹 및 할당된 정책 또는 앱이 간헐적으로 적용되지 않습니다. [CXM-102020]
- XenMobile Server 버전 10.14 에서는 iOS 및 macOS 프로필 가져오기 정책을 편집할 수 없습니다. [CXM-102420]
- XenMobile Server 에서는 사용량이 많은 시간에 서버 노드의 높은 CPU 사용률을 확인할 수 있습니다. [CXM-102651]
- XenMobile Server 버전 10.13 에서는 StorageZone 커넥터만 사용하여 StorageZone 컨트롤러를 연결하고 구성할 수 없습니다. [CXM-102662]
- MDM 전용 모드로 등록된 iOS 장치에서는 Secure Hub 가 App Store 에서 연 브라우저를 통해 앱을 추가할 수 없습니다. 다음 오류가 발생합니다. 로그인이 만료되었습니다. 계속하려면 다시 로그인하십시오. [CXM-102665]
- XenMobile Server 버전 10.13 RP1 이상에서는 SNMP 모니터링의 XenMobile 노드 간 연결 트랩이 작동하지 않습니다. [CXM-102791]
- XenMobile Server 에서 잘못된 시간이 W-SU 시간대에 표시됩니다. [CXM-102885]
- 장치의 CA 갱신 이후 XenMobile Server 에서 장치 인증서 발급자 CA 가 업데이트되지 않습니다. [CXM-104235]
- 일부 장치의 SQL 데이터베이스에는 두 개의 인증서 항목이 있어 오류가 발생합니다. [CXM-104298]
- XenMobile Server 에서 일부 VPP 앱의 올바른 버전이 자동으로 업데이트되지 않습니다. [CXM-104327]
- XenMobile Server 버전 10.14 에서는 프로필 장치 프로비저닝 정책을 편집할 수 없습니다. [CXM-104463]
- XenMobile Server 에서 ShareFile Enterprise 를 커넥터로 변경할 때 배달 그룹 아래에서 GUI 가 업데이트되지 않습니다. [CXM-104475]
- DEP 장치에서 Secure Hub 를 업데이트하면 보류 중 상태로 새 등록 초대가 생성됩니다. [CXM-104799]
- iOS 15 를 실행하는 장치를 새로 등록할 때 연결 유형이 **AlwaysOn IKEv2** 이중 구성으로 설정된 경우 VPN 정책 배포가 실패합니다. [CXM-105182]

- 일부 기존 사용자는 XenMobile Server 에 다시 등록할 수 없습니다. [CXM-105185]
- XenMobile Server 버전 10.14 에서는 특정 Active Directory 사용자를 삭제할 수 없습니다. [CXM-105346]
- Google Play 에서 일부 공용 앱을 사용할 수 없는 경우 Android 를 실행하는 일부 기기에서는 Secure Hub 에 액세스할 수 없습니다. [CXM-105493]
- SSL 인증서 갱신 후 특정 macOS 장치에서는 설치된 프로필 및 인증서가 자동으로 제거됩니다. [CXM-105755]
- XenMobile Server 콘솔에서는 이름에 / 기호가 있는 제한 장치 정책을 편집할 수 없습니다. [CXM-105827]
- 출시된 DEP 장치는 XenMobile Server 콘솔에 계속 표시됩니다. [CXM-105892]
- Secure Hub 스토어에 액세스할 수 없습니다. 다음 오류가 발생합니다. 로그인에 만료되었습니다. 계속하려면 다시 로그인하십시오. [CXM-106057]
- XenMobile Server 에서는 독일어 로케일로 관리되는 앱 자동 업데이트 정책을 만들거나 편집할 수 없습니다. [CXM-106565]
- XenMobile Server 버전 10.13 에서는 라이선스 만료 날짜가 알림 기간에 해당하지 않더라도 라이선스 만료 알림을 받게 됩니다. [CXM-106581]
- 일부 앱에서는 설치된 버전이 최신 버전이더라도 Secure Hub 앱 스토어에 업데이트 보류 중 상태가 표시됩니다. [CXM-106583]
- XenMobile Server 버전 10.14 에서는 DEP 가 아닌 iOS 장치의 경우 소유자 탭이 공백으로 표시됩니다. [CXM-106586]
- XenMobile Server 에서는 독일어 로케일에서 제한 장치 정책을 만들거나 편집할 수 없습니다. [CXM-106748]
- 주체 대체 이름 유형이 없음이 아닌 경우 SCEP 장치 정책이 실패합니다. [CXM-106847]
- 버전 10.14.0 롤링 패치 릴리스의 수정된 문제는 다음을 참조하십시오.
 - [XenMobile Server 10.14 롤링 패치 8 에 대한 릴리스 정보](#)
 - [XenMobile Server 10.14 롤링 패치 7 에 대한 릴리스 정보](#)
 - [XenMobile Server 10.14 롤링 패치 6 에 대한 릴리스 정보](#)

관련 정보

[XenMobile Support Knowledge Center](#)

알려진 문제

November 21, 2022

XenMobile 10.15 에는 알려진 문제가 없습니다.

- 모바일 생산성 앱과 관련된 알려진 문제에 대해서는 [Secure Hub](#), [Secure Mail](#) 및 [Secure Web](#)을 참조하십시오.
- 최신 버전 10.14.0 롤링 패치 릴리스의 알려진 문제에 대해서는 [XenMobile Server 10.14 롤링 패치 8의 릴리스 노트](#)를 참조하십시오.

관련 정보

[XenMobile Support Knowledge Center](#)

아키텍처

March 15, 2024

조직의 장치 및 앱 관리 요구 사항에 따라 XenMobile 아키텍처의 XenMobile 구성 요소가 결정됩니다. XenMobile의 구성 요소는 모듈식이며 상호 기반하여 구축됩니다. 예를 들어, 배포에는 Citrix Gateway가 포함됩니다.

- Citrix Gateway를 통해 사용자는 모바일 앱에 원격으로 액세스하고 사용자 장치 유형을 추적할 수 있습니다.
- XenMobile에서는 이러한 앱과 장치를 관리할 수 있습니다.

XenMobile 구성 요소 배포: XenMobile을 배포하여 사용자가 다음과 같은 방법으로 내부 네트워크의 리소스에 연결하도록 할 수 있습니다.

- 내부 네트워크로의 연결. 원격 사용자의 경우 Citrix Gateway를 통해 VPN 또는 Micro VPN 연결을 사용하여 연결할 수 있습니다. 이 연결은 내부 네트워크의 앱 및 데스크톱에 대한 액세스를 제공합니다.
- 장치 등록. 사용자가 XenMobile에서 모바일 장치를 등록할 수 있으므로 네트워크 리소스에 연결하는 장치를 XenMobile 콘솔에서 관리할 수 있습니다.
- 웹, SaaS 및 모바일 앱. 사용자는 XenMobile에서 Secure Hub를 통해 웹, SaaS 및 모바일 앱에 액세스할 수 있습니다.
- Windows 기반 앱 및 가상 데스크톱. 사용자는 Citrix Receiver 또는 웹 브라우저에 연결하여 StoreFront 또는 Web Interface에서 Windows 기반 앱 및 가상 데스크톱에 액세스할 수 있습니다.

온-프레미스 XenMobile Server에 대해 이러한 기능을 수행하려면 XenMobile 구성 요소를 다음 순서로 배포하는 것이 좋습니다.

- Citrix Gateway. Quick Configuration(빠른 구성) 마법사를 통해 Citrix Gateway의 설정을 구성하여 XenMobile, StoreFront 또는 Web Interface와의 통신을 설정할 수 있습니다. Citrix Gateway에서 Quick Configuration(빠른 구성) 마법사를 사용하기 전에 XenMobile, StoreFront 또는 Web Interface 중 하나를 설치하여 통신을 설정해야 합니다.
- XenMobile. XenMobile을 설치한 후 XenMobile 콘솔에서 사용자의 모바일 장치 등록을 허용하는 정책 및 설정을 구성할 수 있습니다. 또한 모바일, 웹 및 SaaS 앱을 구성할 수 있습니다. 모바일 앱에는 Apple App Store 또는

Google Play 앱이 포함될 수 있습니다. 또한 사용자는 MDX Toolkit 을 사용하여 래핑되고 콘솔에 업로드된 모바일 앱에 연결할 수 있습니다.

- MAM SDK 또는 MDX Toolkit. MDX 래핑 기술은 2023 년 7 월에 EOL(수명 종료) 에 도달할 예정입니다. 엔터프라이즈 응용 프로그램을 계속 관리하려면 MAM SDK 를 포함해야 합니다.

MAM(모바일 응용 프로그램 관리) SDK 는 iOS 및 Android 플랫폼에서 제공되지 않는 MDX 기능을 제공합니다. iOS 또는 Android 앱을 보호하고 MDX 를 사용 설정할 수 있습니다. 내부 스토어 또는 공개 앱 스토어를 통해 이러한 앱을 제공합니다. [MDX 앱 SDK](#)를 참조하십시오.

- StoreFront(선택 사항). Receiver 연결을 통해 StoreFront 의 Windows 기반 앱 및 가상 데스크톱에 대한 액세스를 제공할 수 있습니다.
- Citrix Files(선택 사항). Citrix Files 를 배포하는 경우 XenMobile 을 통해 엔터프라이즈 디렉터리를 통합하여 SAML(Security Assertion Markup Language) ID 공급자로 사용할 수 있습니다. ShareFile 에 대한 ID 공급자 구성에 대한 자세한 내용은 ShareFile 지원 사이트를 참조하십시오.

XenMobile 은 XenMobile 콘솔을 통해 장치 관리 및 앱 관리를 제공합니다. 이 섹션에서는 XenMobile 배포의 참조 아키텍처를 설명합니다.

프로덕션 환경에서는 확장성 및 서버 중복성을 위해 XenMobile 솔루션을 클러스터 구성으로 배포하는 것이 좋습니다. 또한 Citrix ADC SSL 오프로드 기능을 사용하면 XenMobile Server 의 부하가 줄고 처리량이 늘어납니다. Citrix ADC 에 부하 분산을 위한 가상 IP 주소 2 개를 구성하여 XenMobile 클러스터를 설정하는 방법에 대한 자세한 내용은 [클러스터링](#)을 참조하십시오.

재해 복구 배포용으로 XenMobile 을 구성하는 방법에 대한 자세한 내용은 배포 안내서의 [재해 복구](#) 문서를 참조하십시오. 이 문서에는 아키텍처 다이어그램이 포함되어 있습니다.

다음 섹션에서는 XenMobile 배포의 다양한 참조 아키텍처를 설명합니다. 참조 아키텍처 다이어그램은 XenMobile 배포 안내서 문서인 [온-프레미스 배포용 참조 아키텍처](#) 및 [아키텍처](#)를 참조하십시오. 전체 포트 목록은 [포트 요구 사항](#)(온-프레미스) 및 [포트 요구 사항](#)(클라우드) 을 참조하십시오.

MDM(모바일 기기 관리) 모드

중요:

MDM 모드를 구성하고 나중에 ENT 모드로 변경하는 경우 동일한 인증 (Active Directory) 을 사용해야 합니다. XenMobile 은 사용자 등록 후의 인증 모드 변경을 지원하지 않습니다. 자세한 내용은 [XenMobile MDM Edition 에서 Enterprise Edition 으로 업그레이드](#)를 참조하십시오.

XenMobile MDM Edition 은 모바일 기기 관리를 제공합니다. 플랫폼 지원은 [지원되는 장치 운영 체제](#)를 참조하십시오. XenMobile 의 MDM 기능만 사용하려는 경우 XenMobile 을 MDM 모드로 배포합니다. 예를 들어 다음을 수행할 수 있습니다.

- 장치 정책 및 앱 배포
- 자산 인벤토리 검색

- 장치에서 장치 초기화와 같은 동작 수행

권장 모델에서 XenMobile Server 는 DMZ 에 배치되며 XenMobile 의 보호를 개선하는 Citrix ADC 를 선택적으로 그 앞에 배포할 수 있습니다.

MAM(모바일 앱 관리) 모드

MAM 또는 MAM 전용 모드는 모바일 앱 관리를 제공합니다. 플랫폼 지원은 [지원되는 장치 운영 체제](#)를 참조하십시오. XenMobile 의 MAM 기능만 사용하고 MDM 에 장치를 등록하지 않으려는 경우 XenMobile 을 MAM 모드로 배포합니다. 예를 들어 다음을 수행할 수 있습니다.

- BYO 모바일 장치의 앱 및 데이터 보안
- 엔터프라이즈 모바일 앱 제공
- 앱 잠금 및 데이터 초기화

장치를 MDM 에 등록할 수 없습니다.

이 배포 모델에서 XenMobile Server 는 XenMobile 의 보호를 개선하는 Citrix Gateway 다음에 배치됩니다.

MDM+MAM 모드

MDM 과 MAM 모드를 함께 사용하면 모바일 앱 및 데이터 관리 기능과 모바일 기기 관리 기능을 사용할 수 있습니다. 플랫폼 지원은 [지원되는 장치 운영 체제](#)를 참조하십시오. XenMobile 의 MDM 기능과 MAM 기능을 사용하려는 경우 XenMobile 을 ENT(엔터프라이즈) 모드로 배포합니다. 예를 들어 다음을 수행할 수 있습니다.

- MDM 을 사용하여 회사에서 발급한 장치 관리
- 장치 정책 및 앱 배포
- 자산 인벤토리 검색
- 장치 초기화
- 엔터프라이즈 모바일 앱 제공
- 장치의 앱 잠금 및 데이터 초기화

권장 배포 모델에서 XenMobile Server 는 DMZ 에 배치되며 XenMobile 의 보호를 개선하는 Citrix Gateway 를 그 앞에 배포합니다.

내부 네트워크의 **XenMobile** - 다른 배포 옵션은 온-프레미스 XenMobile Server 를 DMZ 가 아닌 내부 네트워크에 배치하는 것입니다. 이 배포는 보안 정책에 따라 DMZ 에 네트워크 장비만 배치해야 하는 경우 사용됩니다. 이 배포에서 XenMobile Server 는 DMZ 에 배치되지 않습니다. 따라서 DMZ 의 SQL Server 및 PKI 서버에 대한 액세스를 허용하기 위해 내부 방화벽의 포트를 열 필요가 없습니다.

시스템 요구 사항 및 호환성

November 21, 2022

참고:

이 문서에서는 XenMobile Server 10.15 의 시스템 요구 사항 및 호환성에 대해 다룹니다. Endpoint Management 의 시스템 요구 사항에 대해서는 [시스템 요구 사항](#)을 참조하십시오.

추가 요구 사항 및 호환성 정보는 다음 문서를 참조하십시오.

- [XenMobile 호환성](#)
- [지원되는 장치 운영 체제](#)
- [포트 요구 사항](#)
- [확장성](#)
- [라이선싱](#)
- [FIPS 140-2 준수](#)
- [언어 지원](#)

XenMobile 10.15 를 실행하려면 다음과 같은 최소 시스템 요구 사항이 필요합니다.

- 다음 중 하나:
 - Citrix Hypervisor 8.2 CU1 또는 Citrix XenServer(지원되는 버전: 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2), 자세한 내용은 [XenServer](#)를 참조하십시오.
 - VMware(지원되는 버전: ESXi 6.0, ESXi 6.5.0 Update 3 또는 ESXi 6.7 Update 2 패치 10, ESXi 7.0 Update 3g), 자세한 내용은 ESXi 6.7 해결 방법 및 [VMware](#)를 참조하십시오.
 - Hyper-V(지원되는 버전: Windows Server 2016 및 Windows Server 2019), 자세한 내용은 [Hyper-V](#)를 참조하십시오.
- Exchange ActiveSync 10.1.10 용 Endpoint Management 커넥터 또는 Exchange ActiveSync 8.5.3.19 용 Citrix Gateway 커넥터
- 듀얼 코어 프로세서
- 가상 CPU 4 개
- 프로덕션 환경의 경우 8GB RAM. POC 및 테스트 환경의 경우 4GB RAM
- 50GB 의 디스크 공간
- Citrix License Server 11.16.

XenMobile Server 를 업그레이드하기 전에 라이선스 서버를 업데이트하십시오.

ESXi 6.7 해결 방법

ESXi 6.7 이 작동하려면 다음 해결 방법을 수행해야 합니다.

1. VMware 에서 제공하는 OVF 도구를 사용하여 citrix.com 에서 다운로드한 OVA 파일을 추출합니다. VMware 페이지 (<https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491>) 에서 OVF 도구를 얻습니다.
2. 추출된 세 개 파일 중에서.vmdk 파일을 데이터 저장소에 업로드합니다.
3. 새 가상 컴퓨터를 만듭니다.
 - a) 가상 컴퓨터 이름을 지정하고 호환성 옵션으로 **ESX/ESXi 4.x virtual machine(ESX/ESXi 4.x 가상 컴퓨터)** 을 선택합니다.
 - b) Guest OS family(게스트 OS 제품군) 에서 **Linux** 를 선택합니다.
 - c) Guest OS version(게스트 OS 버전) 에서 **Other 2.6.x Linux (64-bit)(기타 2.6.x Linux(64 비트))** 를 선택합니다.
 - d) 데이터 저장소에서 **Default(기본값)** 를 선택합니다.
 - e) 사용자 지정하는 동안 기본 하드 디스크, USB 컨트롤러 및 CD/DVD 드라이브를 제거합니다.
 - f) Network(네트워크) 에서 어댑터 유형으로 **VMXNET3** 을 선택합니다.
 - g) ESXi 에서 디스크가 로컬인 경우 **SCSI Controller(SCSI 컨트롤러)** 및 **LSI Logic Parallel(LSI Logic 병렬)** 을 선택합니다. 공유 디스크를 사용하는 경우 **VMware Paravirtual(VMware 반가상화)** 을 선택합니다.
 - h) Next(다음) 를 클릭하여 VM 생성을 마칩니다.
4. 데이터 저장소로 이동하고 앞서 업로드한.vmdk 파일을 복사합니다. XenMobile 용으로 만든 VM 디렉터리에 붙여 넣습니다.
5. ESXi 웹 인터페이스에서 VM 을 선택하고 설정을 편집합니다.
6. **Add Hard disk(하드 디스크 추가)** 를 클릭합니다.
7. 앞서 복사한.vmdk 파일을 선택하고 VM 에 파일을 연결합니다.
8. 저장을 클릭합니다.
9. VM 의 전원을 켭니다.

Citrix Gateway 시스템 요구 사항

XenMobile 10.15 와 함께 Citrix Gateway 를 실행하려면 다음과 같은 최소 시스템 요구 사항이 필요합니다.

- Citrix Gateway(온프레미스). 지원되는 버전: 12.1 이상
- 또한 Active Directory 와 통신하기 위한 서비스 계정이 있어야 합니다. 쿼리 및 읽기 권한만 있으면 됩니다.

XenMobile 10.15 데이터베이스 요구 사항

XenMobile 에는 다음 데이터베이스 중 하나가 필요합니다.

- Microsoft SQL Server

XenMobile 은 지원되는 다음 버전 중 하나를 실행하는 Microsoft SQL Server 데이터베이스를 지원합니다. SQL Server 데이터베이스 및 해당 하드웨어 요구 사항에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

- Microsoft SQL Server 2016 SP3
- Microsoft SQL Server 2017 CU 31
- Microsoft SQL Server 2019 CU 18
- Microsoft SQL Server 2022

Microsoft SQL Server 데이터베이스 요구 사항은 배포 크기에 따라 다릅니다. 배포 규모에 따른 Microsoft SQL Server 데이터베이스 요구 사항에 대한 자세한 내용은 [확장성](#)을 참조하십시오.

XenMobile 은 데이터베이스 고가용성을 위한 SQL Basic 가용성 그룹 (Always On 가용성 그룹) 및 SQL 클러스터링을 지원합니다.

Microsoft SQL 은 원격으로 사용하는 것이 좋습니다.

Microsoft SQL 업그레이드에 대한 자세한 내용은 Microsoft 문서 [SQL Server 업그레이드](#)를 참조하십시오.

- PostgreSQL(테스트 환경 전용). PostgreSQL 은 XenMobile 에 포함되어 있으며 테스트 환경에서 로컬 또는 원격으로 사용할 수 있습니다. 데이터베이스 마이그레이션은 지원되지 않습니다. 테스트 환경에서 만든 데이터베이스를 프로덕션 환경으로 이동할 수 없습니다.

모든 XenMobile 버전은 Windows 용 원격 PostgreSQL 9.5.1 및 9.5.11 을 지원할 때 다음과 같은 제한 사항이 있으므로 프로덕션 환경에는 권장되지 않습니다. 최대 300 개 장치 지원 장치 개수가 300 개가 넘을 경우 온-프레미스 SQL Server 사용 클러스터링 지원 안 함

SQL Server 서비스 계정 요구 사항

XenMobile 에 사용할 SQL Server 서비스 계정에 [DBcreator](#) 역할 권한이 있는지 확인합니다. XenMobile Server 설치 중에 지정하는 SQL Server 계정 암호를 기록합니다. XenMobile Server 복구 중에 XenMobile 데이터베이스를 복제해야 하는 경우 이 암호가 필요합니다.

TDE(Transparent Data Encryption) 를 사용하여 SQL Server 데이터베이스를 보호합니다. [온-프레미스 배포용 참조 아키텍처](#)의 참조 아키텍처에 표시된 대로 SQL Server 포트에 대한 외부 액세스를 허용하지 마십시오.

SQL Server 서비스 계정에 대한 자세한 내용은 Microsoft 설명서 사이트의 다음 페이지를 참조하십시오. 이러한 링크는 SQL Server 2014 에 대한 정보를 가리킵니다. 다른 버전을 사용하는 경우 **Other Versions(다른 버전)** 목록에서 서버 버전을 선택하십시오.

- [Windows 서비스 계정 및 권한 구성](#)
- [서버 수준 역할](#)

Virtual Apps and Desktops 호환성

- Virtual Apps and Desktops 7.15 LTSR CU3
- Virtual Apps and Desktops 7.1811
- Virtual Apps and Desktops 7 1906
- Virtual Apps and Desktops 7 1909
- Virtual Apps and Desktops 7 2006

StoreFront 호환성

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

기타 호환성

- Exchange ActiveSync 10.1.10 용 Endpoint Management 커넥터
 - 이전 버전은 테스트되지 않았습니다.
- Exchange ActiveSync 8.5.3.19 용 Citrix Gateway 커넥터
 - 이전 버전은 테스트되지 않았습니다.

XenMobile 호환성

November 21, 2022

참고:

이 문서에서는 XenMobile Server의 호환성에 대해 다룹니다. Endpoint Management에서 테스트된 구성 요소에 대해서는 [Endpoint Management 호환성](#)을 참조하십시오.

새로운 기능, 수정 사항 및 정책 업데이트를 사용하려면 Citrix 권장 사항에 따라 다음의 최신 버전을 설치하는 것이 좋습니다.

- Citrix에서는 Mobile Application Management(MAM) SDK를 엔터프라이즈 iOS 및 Android 앱과 통합하여 MDX 기능을 앱에 적용하도록 권장합니다.

MDX Toolkit은 2023년 7월에 EOL(수명 종료)에 도달할 예정입니다. 엔터프라이즈 앱을 계속 관리하면 MAM SDK를 통합해야 합니다.

이 문서에서는 통합이 가능한 지원되는 XenMobile 구성 요소의 버전을 요약하여 보여 줍니다.

호환성 및 업그레이드 경로

Secure Hub, MDX Toolkit 및 모바일 생산성 앱의 최신 버전은 XenMobile Server의 현재 및 이전 버전과 호환됩니다.

최신 버전의 모바일 생산성 앱에는 최신 버전의 Secure Hub가 필요합니다. 이전 두 버전의 앱은 최신 Secure Hub와 호환됩니다. 자세한 내용은 [Citrix Product Matrix\(Citrix 제품 매트릭스\)](#)를 참조하십시오.

Citrix는 공용 앱 스토어에서만 XenMobile 생산성 앱의 배포를 지원합니다.

XenMobile Server(온-프레미스)

- 이전 두 버전의 XenMobile Server에서 업그레이드할 수 있습니다.
- 최신 버전의 XenMobile Server: XenMobile Server 10.15
- 업그레이드 원본:
 - XenMobile Server 10.14.x
 - XenMobile Server 10.13.x

모바일 생산성 앱

사용자는 공용 앱 스토어에서 모바일 생산성 앱에 액세스할 수 있습니다. 최신 버전의 모바일 생산성 앱에는 최신 버전의 Secure Hub가 필요합니다. 이전 두 버전의 앱은 최신 Secure Hub와 호환됩니다.

릴리스 케이던스가 2 주인 모바일 생산성 앱에 대한 자세한 정보는 [릴리스 타임라인](#)을 참조하십시오. 지원에 대한 자세한 내용은 [모바일 생산성 앱 지원](#)을 참조하십시오.

MAM SDK

MAM SDK는 iOS 및 Android 플랫폼에서 제공되지 않는 MDX 기능을 제공합니다. 내부 스토어 또는 공개 앱 스토어를 통해 이러한 앱을 제공합니다. [MDX 앱 SDK](#)를 참조하십시오.

MDX Toolkit

MDX 래핑 기술은 2023년 7월에 EOL(수명 종료)에 도달할 예정입니다. 엔터프라이즈 응용 프로그램을 계속 관리하려면 MAM SDK를 포함해야 합니다.

Citrix는 MDX Toolkit의 최신 릴리스 3개(n.n.n)를 지원합니다. [MDX Toolkit의 새로운 기능](#)을 참조하십시오.

브라우저 지원

XenMobile Server 콘솔에는 지원되는 다음 웹 브라우저 중 하나가 필요합니다.

- Google Chrome 최신 버전
- Mozilla Firefox 최신 버전
- Microsoft Edge 최신 버전
- Apple Safari 최신 버전

지원되는 장치 운영 체제

November 21, 2022

참고:

이 문서에서는 XenMobile Server 10.13 에서 지원되는 장치 운영 체제에 대해 다룹니다. Endpoint Management 에 지원되는 운영 체제는 [지원되는 장치 운영 체제](#)를 참조하십시오.

XenMobile 은 앱, 장치 관리 등 엔터프라이즈 모바일 관리를 위한 다음 플랫폼 및 운영 체제를 실행하는 장치를 지원합니다. 플랫폼 제한 및 보안 기능으로 인해 XenMobile 에서 일부 플랫폼의 일부 기능이 지원되지 않을 수 있습니다.

이 문서에 포함된 지원되는 장치 플랫폼 정보는 Exchange ActiveSync 용 Citrix Gateway 커넥터 및 Exchange ActiveSync 용 XenMobile 커넥터에도 적용됩니다.

모바일 생산성 앱의 최신 버전과 MDX 암호화가 지원되는 장치는 [모바일 생산성 앱 지원](#)을 참조하십시오.

참고:

Citrix 는 최소한 각 주요 운영 체제 플랫폼의 현재 및 이전 버전을 지원합니다. 최신 Endpoint Management 버전의 일부 기능은 이전 플랫폼 릴리스에서 작동하지 않을 수 있습니다.

지원 중단 발표는 [사용 중지](#)를 참조하십시오.

운영 체제 지원 목록

Citrix XenMobile 은 다음 운영 체제를 지원합니다.

- **Android:** 10.x, 11.x, 12.x, 13.x

Android 10 이상에 대해서는 [Android 고려사항](#)을 참조하십시오.

- **iOS:** 13.x, 14.x, 15.x, 16.x

XenMobile 및 Citrix 모바일 앱은 iOS 14.x 와 호환되지만 현재는 모든 새로운 iOS 14.x 기능을 지원하지 않습니다. iOS 14.x 용 사내 엔터프라이즈 앱을 래핑하려면 MDX Toolkit 21.8.5 이상을 사용하거나 MAM SDK 를 사용하여 앱을 준비합니다.

- **iPadOS:** 13.x, 14.x, 15.x, 16.x

XenMobile 및 Citrix 모바일 앱은 iPadOS 14.x 와 호환되지만 현재는 모든 새로운 iPadOS 14.x 기능을 지원하지 않습니다.

- **macOS:** 10.13x, 10.14x, 10.15x, 11.x, 12.x, 13.x

XenMobile 및 Citrix 모바일 앱은 macOS 11 과 호환되지만 현재는 모든 새로운 macOS 11 기능을 지원하지 않습니다.

- **Windows** 데스크톱 및 태블릿: (MDM에만 해당). Windows 10 및 Windows 11

Android 고려 사항

중요:

장치 관리 모드는 더 이상 지원되지 않습니다. 자세한 내용은 [장치 관리에서 Android Enterprise 로 마이그레이션](#)을 참조하십시오.

- Citrix에서는 Android 장치를 레거시 장치 관리 모드에서 등록하지 않을 것을 권장합니다. Google에서는 Device Administration API의 지원을 중단했으며, 이는 Android 10 이상을 실행하는 장치에 영향을 미칩니다. 레거시 장치 관리 모드에서 Android 장치를 등록할 수 없습니다. Citrix는 장치 관리 모드에서 Android 11 장치 등록을 지원하지 않습니다.
- Citrix에서는 Android 10 장치에 Android Enterprise를 사용할 것을 권장합니다. 자세한 내용은 [장치 관리에서 Android Enterprise 로 마이그레이션](#)을 참조하십시오.
- Google API 변경은 MAM 전용 모드에서 등록된 장치에는 영향을 주지 않습니다.

업그레이드 전에:

- 서버 인프라가 subjectAltName(SAN) 확장에 일치하는 호스트 이름을 가진 보안 인증서와 호환되는지 확인하십시오.
- 호스트 이름을 확인하려면 서버가 일치하는 SAN이 포함된 인증서를 제공해야 합니다. Citrix는 호스트 이름과 일치하는 SAN이 포함된 인증서만 신뢰합니다.

포트 요구 사항

September 13, 2023

장치 및 앱에서 XenMobile과 통신할 수 있도록 하려면 방화벽에서 특정 포트를 열어야 합니다. 열어야 하는 포트가 다음 표에 나열되어 있습니다.

Citrix Gateway 및 XenMobile의 앱 관리를 위한 포트 열기

Citrix Secure Hub, Citrix Receiver 및 Citrix Gateway 플러그인 사용자가 Citrix Gateway를 통해 다음 구성 요소에 연결할 수 있도록 하려면 다음 포트를 열어야 합니다.

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- Exchange ActiveSync 용 Citrix Gateway 커넥터
- 인트라넷 웹 사이트와 같은 다른 내부 네트워크 리소스

Citrix ADC 에서 Launch Darkly 로의 트래픽을 활성화하려면 이 [Support Knowledge Center 문서](#)에 나와 있는 IP 주소를 사용할 수 있습니다.

Citrix Gateway 에 대한 자세한 내용은 Citrix Gateway 설명서를 참조하십시오. 이 설명서에 NSIP(Citrix ADC IP), VIP(가상 서버 IP) 및 SNIP(서브넷 IP) 주소에 대한 정보가 포함되어 있습니다.

TCP 포트	설명	원본	대상
21 또는 22	FTP 또는 SCP 서버로 지원 번들을 보내는 데 사용됩니다.	XenMobile	FTP 또는 SCP 서버
53(TCP 및 UDP)	DNS 연결에 사용됩니다.	Citrix Gateway, XenMobile	DNS 서버
80	Citrix Gateway 가 두 번째 방화벽을 통해 VPN 연결을 내부 네트워크 리소스에 전달합니다. 이 상황은 일반적으로 사용자가 Citrix Gateway 플러그인으로 로그인한 경우 발생합니다.	Citrix Gateway	인트라넷 웹 사이트
80 또는 8080, 443	열거, 티켓 생성 및 인증에 사용되는 XML 및 STA(Secure Ticket Authority) 포트입니다. 포트 443 을 사용할 것을 권장합니다.	StoreFront 및 Web Interface XML 네트워크 트래픽, Citrix Gateway STA	Virtual Apps 또는 Desktops
123(TCP 및 UDP)	NTP(Network Time Protocol) 서비스에 사용됩니다.	Citrix Gateway, XenMobile	NTP 서버
389	보안되지 않은 LDAP 연결에 사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증 서버 또는 Microsoft Active Directory

TCP 포트	설명	원본	대상
443	Citrix Receiver 의 StoreFront 연결 또는 Receiver for Web 의 Virtual Apps and Desktops 연결에 사용됩니다.	인터넷	Citrix Gateway
443	웹, 모바일 및 SaaS 앱 제공을 위해 XenMobile 에 연결할 때 사용됩니다.	인터넷	Citrix Gateway
443	일반 장치와 XenMobile Server 의 통신에 사용됩니다.	XenMobile	XenMobile
443	등록을 위해 모바일 장치에서 XenMobile 에 연결할 때 사용됩니다.	인터넷	XenMobile
443	XenMobile 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터로의 연결에 사용됩니다.	XenMobile	Exchange ActiveSync 용 Citrix Gateway 커넥터
443	Exchange ActiveSync 용 Citrix Gateway 커넥터에서 XenMobile 로의 연결에 사용됩니다.	Exchange ActiveSync 용 Citrix Gateway 커넥터	XenMobile
443	인증서 인증을 사용하지 않는 배포의 콜백 URL 에 사용됩니다.	XenMobile	Citrix Gateway
514	XenMobile 과 syslog 서버 간의 연결에 사용됩니다.	XenMobile	Syslog 서버
636	보안 LDAP 연결에 사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증 서버 또는 Active Directory
1494	내부 네트워크의 Windows 기반 응용 프로그램에 대한 ICA 연결에 사용됩니다. 이 포트는 열어 두는 것이 좋습니다.	Citrix Gateway	Virtual Apps 또는 Desktops
1812	RADIUS 연결에 사용됩니다.	Citrix Gateway	RADIUS 인증 서버

TCP 포트	설명	원본	대상
2598	세션 안정성을 사용한 내부 네트워크의 Windows 기반 응용 프로그램에 대한 연결에 사용됩니다. 이 포트는 열어 두는 것이 좋습니다.	Citrix Gateway	Virtual Apps 또는 Desktops
3268	Microsoft 글로벌 카탈로그의 보안되지 않은 LDAP 연결에 사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증 서버 또는 Active Directory
3269	Microsoft 글로벌 카탈로그의 보안 LDAP 연결에 사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증 서버 또는 Active Directory
9080	Citrix ADC 와 Exchange ActiveSync 용 Citrix Gateway 커넥터 간의 HTTP 트래픽에 사용됩니다.	Citrix ADC	Exchange ActiveSync 용 Citrix Gateway 커넥터
30001	HTTPS 서비스의 초기 스테이징을 위한 관리 API	내부 LAN	XenMobile Server
9443	Citrix ADC 와 Exchange ActiveSync 용 Citrix Gateway 커넥터 간의 HTTPS 트래픽에 사용됩니다.	Citrix ADC	Exchange ActiveSync 용 Citrix Gateway 커넥터
45000; 80	클러스터에 배포된 두 XenMobile VM 간의 통신에 사용됩니다. 포트 80 은 노드 간 통신 및 SSL 오프로드에 사용됩니다.	XenMobile	XenMobile
8443	등록, XenMobile Store 및 MAM(모바일 앱 관리)에 사용됩니다.	XenMobile, Citrix Gateway, 장치, 인터넷	XenMobile
4443	관리자가 브라우저를 통해 XenMobile 콘솔에 액세스할 때 사용됩니다. 또한 모든 XenMobile 클러스터 노드의 로그 및 지원 번들을 한 노드에서 다운로드하는 데 사용됩니다.	액세스 지점 (브라우저), XenMobile	XenMobile

TCP 포트	설명	원본	대상
27000	외부 Citrix License Server 에 액세스할 때 사용되는 기본 포트입니다.	XenMobile	Citrix License Server
7279	들어오고 나가는 Citrix 라이선스를 확인할 때 사용되는 기본 포트입니다.	XenMobile	Citrix 공급업체 데몬
161	UDP 프로토콜을 사용하는 SNMP 트래픽에 사용됩니다.	SNMP 관리자	XenMobile
162	XenMobile 의 SNMP 트랩 알림을 SNMP 관리자로 보내는 데 사용됩니다. 원본은 XenMobile 이고 대상은 SNMP 관리자입니다.	XenMobile	SNMP 관리자

장치 관리를 위한 **XenMobile** 포트 열기

XenMobile 이 네트워크에서 통신할 수 있도록 하려면 다음 포트를 엽니다.

TCP 포트	설명	원본	대상
25	XenMobile 알림 서비스의 기본 SMTP 포트입니다. SMTP 서버가 다른 포트를 사용하는 경우 방화벽이 해당 포트를 차단하지 않는지 확인하십시오.	XenMobile	SMTP 서버

TCP 포트	설명	원본	대상
80 및 443	Apple iTunes App Store 또는 Google Play(80 을 사용해야 함) 에 대한 엔터프 라이즈 앱 스토어 연결입니다. Apple 볼륨 구매에 사용됩 니다. iOS 또는 Android 용 Secure Hub 에서 앱 스토 어의 앱을 게시하는 데 사용됩 니다.	XenMobile	ax.apps.apple.com 및 *.mzstatic.com , vpp.itunes.apple.com , login.live.com , *.notify.windows.com play.google.com , android.clients.google.com , android.l.google.com
80 또는 443	XenMobile 과 Nexmo SMS 알림 릴레이 간의 아웃 바운드 연결에 사용됩니다.	XenMobile	Nexmo SMS 릴레이 서버
389	보안되지 않은 LDAP 연결에 사용됩니다.	XenMobile	LDAP 인증 서버 또는 Active Directory
443	Android 의 등록 및 상담원 설정에 사용됩니다.	인터넷	XenMobile
443	Android 및 Windows 장 치 및 MDM 원격 지원 클라 이언트의 등록 및 에이전트 설 정에 사용됩니다.	인터넷 LAN 및 Wi-Fi	XenMobile
1433	원격 데이터베이스 서버에 대 한 연결에 기본적으로 사용됩 니다 (선택 사항).	XenMobile	SQL Server
443 또는 2197	APNs 알림을 * . push.apple.com 으로 전송하 는 데 사용됩니다.	XenMobile	인터넷 (공용 IP 주소 17.0.0.0/8 을 사용하는 APNs 호스트)
5223	iOS 장치에서 * . push.apple.com 으로 APNs 아웃바운드 연결에 사 용됩니다.	iOS 장치	인터넷 (공용 IP 주소 17.0.0.0/8 을 사용하는 APNs 호스트)
8081	선택적 MDM 원격 지원 클라 이언트의 앱 터널에 사용됩 니다. 기본값은 8081 입니다.	원격 지원 클라이언트	XenMobile

TCP 포트	설명	원본	대상
8443	iOS 장치 등록에 사용됩니다.	인터넷, LAN 및 Wi-Fi	XenMobile

자동 검색 서비스 연결을 위한 포트 요구 사항

이 포트 구성은 Android 용 Secure Hub 로부터 연결되는 Android 장치가 내부 네트워크 내에서 Citrix ADS(자동 검색 서비스)에 액세스할 수 있도록 합니다. ADS를 통해 제공되는 보안 업데이트를 다운로드하려면 ADS에 액세스해야 합니다.

참고:

ADS 연결에서 프록시 서버가 지원되지 않을 수 있습니다. 이 시나리오에서는 ADS 연결이 프록시 서버를 우회할 수 있게 허용합니다.

인증서 고정을 사용하려는 경우 다음 사전 요구 사항을 수행합니다.

- **XenMobile Server** 및 **Citrix ADC** 인증서를 수집합니다. 인증서는 PEM 형식이어야 하고 공용 인증서여야 하며 개인 키가 아니어야 합니다.
- **Citrix** 지원 팀에 연락하여 인증서 고정을 사용하기 위한 요청을 제출하십시오. 이 과정에서 인증서를 요구받게 됩니다.

인증서 고정을 사용하려면 장치 등록 전에 장치가 ADS에 연결되어야 합니다. 그렇게 해야 최신 보안 정보가 Secure Hub에 제공됩니다. Secure Hub에서 장치를 등록하려면 장치가 ADS에 연결되어야 합니다. 그러므로 내부 네트워크 내에서 ADS 액세스를 열어야 장치를 등록할 수 있습니다.

Android 또는 iOS 용 Secure Hub에 대해 ADS 액세스를 허용하려면 다음 FQDN으로 포트 443을 엽니다.

FQDN	포트	IP 및 포트 사용
<code>discovery.cem.cloud.us</code>	443	Secure Hub - CloudFront를 통한 ADS 통신

지원되는 IP 주소에 대한 정보는 [AWS의 클라우드 기반 Storage Center](#)를 참고하십시오.

Android Enterprise 네트워크 요구 사항

Android Enterprise를 위한 네트워크 환경을 설정할 때 고려해야 할 아웃바운드 연결에 대한 자세한 내용은 Google 지원 문서 [Android Enterprise 네트워크 요구사항](#)을 참조하십시오.

XenMobile의 포트 요구 사항 관리형 Google Play Enterprise를 만들고 [관리형 Google Play iFrame](#)에 액세스하려면 네트워크에서 다음 대상 호스트에 연결할 수 있어야 합니다.. Google은 앱 검색 및 승인을 간소화하기 위해 EMM 개발자

가 관리형 Play iFrame 을 사용할 수 있도록 했습니다. 관리형 Play iFrame 을 사용하려면 XenMobile 콘솔에 액세스하는 브라우저에 Google Play 에 대한 액세스 권한이 있어야 합니다.

대상 호스트	포트	설명
play.google.com	TCP/443	Google Play 스토어, Play Enterprise 가입에 사용
*.googleapis.com	TCP/443	Google Mobile Management, Google API, Google Play 스토어 API, FCM 에 사용
accounts.youtube.com , accounts.google.com	TCP/443	계정 인증에 사용
apis.google.com	TCP/443	Google 웹 서비스에 사용
ogs.google.com	TCP/443	iFrame UI 요소에 사용
notifications.google.com	TCP/443	데스크톱 및 모바일 알림에 사용
fonts.googleapis.com , *.gstatic.com , *.googleusercontent.com	TCP/443	Google Fonts 사용자 생성 콘텐츠에 사용. 예: 스토어의 앱 아이콘
cri.pki.goog , ocsp.pki.goog	TCP/443	인증서 유효성 검사에 사용

확장성 및 성능

November 27, 2023

XenMobile 인프라의 규모를 이해하는 것은 XenMobile 을 어떻게 배포하고 구성할지 결정하는 데 있어 중요합니다. 이 문서에는 확장성 테스트 데이터와 소규모에서 대규모에 이르는 온-프레미스 XenMobile 엔터프라이즈 배포의 성능과 확장성을 위한 인프라 요구 사항을 결정하는 지침이 포함되어 있습니다.

여기서 확장성은 배포에 이미 등록된 장치가 해당 배포에 동시에 다시 연결되는 능력의 관점에서 정의됩니다.

- 확장성은 배포에 등록된 최대 장치 수로 정의됩니다.
- 로그인 속도는 기존 장치가 배포에 다시 연결될 수 있는 최대 속도로 정의됩니다.

이 문서에 나온 데이터는 10,000~75,000 개 장치 규모의 배포에 대한 테스트 결과입니다. 알려진 작업 부하를 사용하여 모바일 장치를 테스트했습니다.

모든 테스트는 XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드) 에서 수행되었습니다.

테스트는 Citrix Gateway 8200 을 사용하여 수행되었습니다. 비슷하거나 더 큰 용량의 Citrix ADC 장비에서는 비슷한 수준 또는 더 뛰어난 확장성과 성능이 나타날 수 있습니다.

확장성 테스트 결과의 요약은 다음과 같습니다.

최대 **75,000** 개 장치의 배포에 대한 확장성 테스트 결과 요약

로그인 속도 (기존 사용자의 다시 연결 속도) - 시간당 최대 9,375 개 장치

사용된 구성:

- Citrix Gateway
- MPX 8200
- XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드)
- XenMobile Server 7 노드 클러스터
- 데이터베이스: Microsoft SQL Server 외부 데이터베이스

장치 모집단 및 하드웨어 구성을 사용한 테스트 결과

장치 수	12,500	30,000	60,000	75,000
시간당 기존 장치의 다시 연결 속도	1,250	3,750	7,500	9,375
XenMobile Server - 모드	독립 실행형	클러스터	클러스터	클러스터
XenMobile Server - 클러스터	해당 없음	3	5	7
XenMobile Server - 가상 장비	메모리 = 8GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 6	메모리 = 24GB RAM, vCPU = 8	메모리 = 24GB RAM, vCPU = 8
Active Directory	메모리 = 4GB RAM, vCPU = 2	메모리 = 8GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 4
Microsoft SQL Server 외부 데이터베이스	메모리 = 8GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 8	메모리 = 24GB RAM, vCPU = 16	메모리 = 24GB RAM, vCPU = 16

확장성 프로필

Active Directory 구성	사용된 프로필
사용자	100,000
그룹	200,000
중첩 수준	5

XenMobile Server 구성	합계	사용자당
정책	20	20
앱	270	50
공용 앱	200	0
MDX	50	30
웹 및 SaaS	20	20
동작	50	
배달 그룹	20	
배달 그룹당 Active Directory 그룹	10	
SQL		
데이터베이스 개수	1	

장치 연결 및 앱 작업

이러한 확장성 테스트를 통해 배포에 등록된 장치가 8 시간 내에 다시 연결될 수 있는지에 대한 데이터를 수집했습니다.

이 테스트에서 시뮬레이션한 다시 연결 간격 동안에는 다시 연결되는 장치에 모든 해당 보안 정책이 적용되기 때문에 XenMobile Server 노드의 부하 상태가 일반적인 수준보다 높아집니다. 이후에 다시 연결할 때에는 변경된 정책 또는 새로운 정책만 iOS 장치로 푸시되므로 XenMobile Server 노드의 부하가 줄어듭니다.

이러한 테스트에서는 iOS 장치와 Android 장치를 50% 씩 섞어서 사용했습니다.

이러한 테스트에서는 다시 연결되는 Android 장치가 사전 GCM 알림을 받은 것으로 가정합니다.

8 시간의 테스트 기간 동안 다음과 같은 앱 관련 작업이 이루어졌습니다.

- 권한이 부여된 앱을 열거하기 위해 Secure Hub 가 한 번 열림
- 2 개의 SAML 웹 앱이 열림

- 4 개의 MAM 앱이 다운로드됨
- Secure Mail 에서 사용하도록 1 개의 STA 가 생성됨
- Micro VPN 을 통한 Secure Mail 다시 연결 이벤트당 하나씩 240 개의 STA 티켓 유효성 검사가 수행됨

참조 아키텍처

이러한 확장성 테스트에 사용되는 배포의 참조 아키텍처에 대한 자세한 내용은 [온-프레미스 배포용 참조 아키텍처](#)의 “핵심 MAM + MDM 참조 아키텍처”를 참조하십시오.

주의 사항 및 제한 사항

이 문서에 나온 확장성 테스트 결과를 고려할 때 다음 사항에 유의하십시오.

- Windows 플랫폼은 테스트되지 않았습니다.
- iOS 와 Android 장치에 대한 정책 푸시를 테스트했습니다.
- 각 XenMobile Server 노드는 동시에 최대 12,000 개의 장치를 지원합니다.

라이선싱

July 26, 2023

중요:

Citrix 라이선스 반환 및 수정 프로세스가 2020 년 11 월 4 일부터 변경되었습니다. 자세한 내용은 다음 문서를 참조하십시오.

- [내 계정을 사용하여 라이선스를 반환하는 방법](#)
- [라이선스 파일 재할당 방법](#)

XenMobile 은 Citrix Licensing 을 사용하여 라이선스를 관리합니다. XenMobile Server 및 Citrix Gateway 를 사용하려면 라이선스가 필요합니다.

Citrix Gateway 라이선스에 대한 자세한 내용은 Citrix Gateway 설명서를 참조하십시오. Citrix Licensing 에 대한 자세한 내용은 [The Citrix Licensing System\(Citrix Licensing 시스템\)](#)을 참조하십시오.

XenMobile Server 를 구입하면 라이선스 활성화 지침이 포함된 주문 확인 전자 메일 메시지가 전송됩니다. 신규 고객은 주문을 제출하기 전에 라이선스 프로그램에 등록해야 합니다. XenMobile 라이선스 모델 및 프로그램에 대한 자세한 내용은 [XenMobile licensing\(XenMobile 라이선스\)](#)을 참조하십시오.

요구 사항

- 최신 버전의 XenMobile Server 로 업데이트하기 전에 Citrix License Server 를 11.16.x 이상으로 업데이트하십시오. 이전 라이선스 서버 버전은 최신 버전의 XenMobile 을 지원하지 않습니다.
- XenMobile 라이선스를 다운로드하기 전에 Citrix Licensing 을 설치해야 합니다. 라이선스 파일을 생성하려면 Citrix Licensing 을 설치한 서버의 이름이 필요합니다. XenMobile 을 설치하면 Citrix Licensing 이 기본적으로 이 서버에 설치됩니다. 또는 기존 Citrix Licensing 배포를 사용하여 XenMobile 라이선스를 관리할 수 있습니다. Citrix Licensing 설치, 배포 및 관리에 대한 자세한 내용은 [제품 라이선스](#)를 참조하십시오.
- XenMobile 의 노드 또는 인스턴스를 클러스터하려는 경우 원격 서버에서 Citrix Licensing 을 사용해야 합니다.
- 받은 모든 라이선스 파일의 로컬 복사본을 유지하는 것이 좋습니다. 구성 파일의 백업 복사본을 저장하면 모든 라이선스 파일이 백업에 포함됩니다. 그러나 구성 파일을 먼저 백업하지 않고 XenMobile 을 다시 설치하는 경우 원래 라이선스 파일이 필요합니다.

XenMobile 라이선스 고려 사항

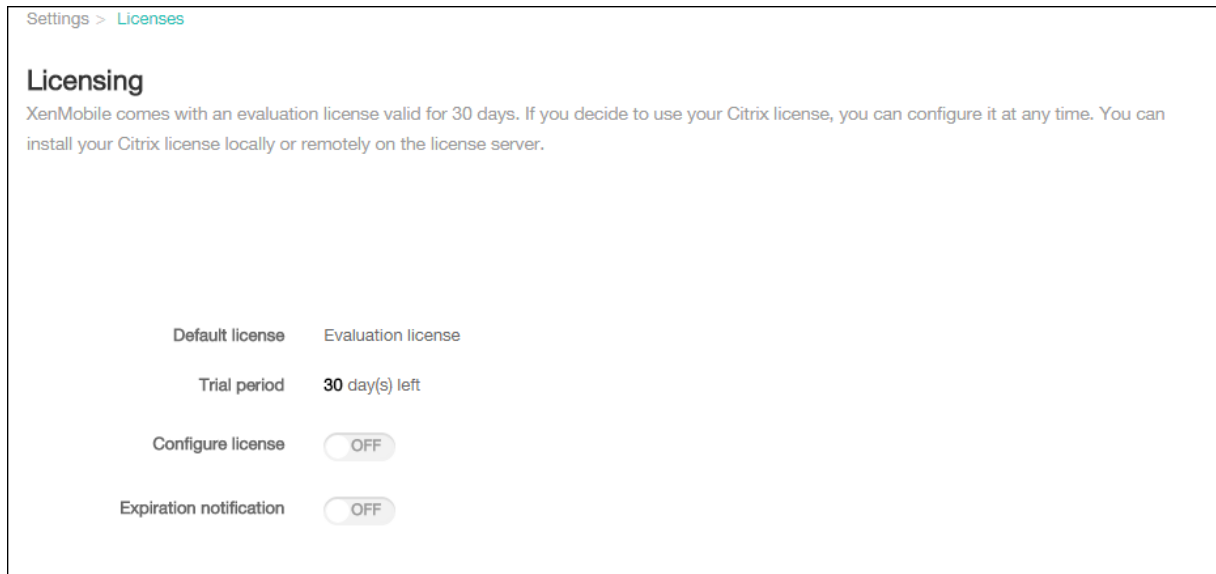
라이선스가 없는 경우 평가 모드에서 30 일의 유예 기간 동안 XenMobile 의 모든 기능을 사용할 수 있습니다. 이 평가 모드는 한 번만 사용할 수 있으며 XenMobile 을 설치한 날부터 30 일간 유효합니다. 유효한 XenMobile 라이선스가 있는지 여부와 관계없이 XenMobile 웹 콘솔에 대한 액세스는 차단되지 않습니다. XenMobile 콘솔에서 평가 기간이 얼마나 남았는지를 확인할 수 있습니다.

XenMobile 에서 다수의 라이선스를 업로드할 수 있지만 한 번에 하나의 라이선스만 활성화할 수 있습니다.

XenMobile 라이선스가 만료되면 더 이상 장치 관리 기능을 수행할 수 없습니다. 예를 들어 새 사용자 또는 장치를 등록할 수 없고 등록된 장치에 배포한 앱 및 구성을 업데이트할 수 없습니다. XenMobile 라이선스 모델 및 프로그램에 대한 자세한 내용은 [XenMobile licensing\(XenMobile 라이선스\)](#)을 참조하십시오.

XenMobile 콘솔에서 라이선스 페이지를 찾으려면

XenMobile 을 설치한 후 라이선스 페이지가 처음으로 나타날 때 라이선스는 기본 30 일 평가 모드로 설정되고 아직 구성되지 않은 상태로 표시됩니다. 이 페이지에서 라이선스를 추가하고 구성할 수 있습니다.



1. XenMobile 콘솔에서 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 라이선스를 클릭합니다. 라이선스 페이지가 나타납니다.

로컬 라이선스를 추가하려면

새 라이선스를 추가하면 테이블에 새 라이선스가 나타납니다. 추가한 첫 번째 라이선스가 자동으로 활성화됩니다. 동일한 범주(예: Enterprise)와 유형의 여러 라이선스를 추가하는 경우 이러한 라이선스가 테이블의 한 행에 나타납니다. 이 경우 공통 라이선스의 결합된 양이 총 라이선스 수 및 사용된 수에 반영됩니다. 만료 날짜에는 공통 라이선스 중에서 가장 빠른 만료 날짜가 표시됩니다.

모든 로컬 라이선스는 XenMobile 콘솔을 통해 관리합니다.

1. Simple License Service 에서 License Administration Console 을 통해 라이선스 파일을 가져오거나 Citrix.com 계정에서 직접 가져옵니다. 자세한 내용은 Citrix Licensing 설명서를 참조하십시오.
2. XenMobile 콘솔에서 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
3. 라이선스를 클릭합니다. 라이선스 페이지가 나타납니다.
4. 라이선스 구성을 커짐으로 설정합니다. 라이선스 유형 목록, 추가 단추 및 라이선스 테이블이 표시됩니다. 라이선스 테이블에는 XenMobile 에서 사용한 라이선스가 포함됩니다. Citrix 라이선스를 추가하지 않은 경우 테이블이 비어 있습니다.

Settings > Licenses

Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

Default license: Evaluation license

Trial period: 30 day(s) left

Configure license: ☒

License type: Local license

Add

Product Name	Active	Total number of licenses	Number used	Type	Expires on
No results found.					

Expiration notification: ☐

5. 라이선스 유형이 로컬 라이선스로 설정되어 있는지 확인하고 추가를 클릭합니다. 새 라이선스 추가 대화 상자가 나타납니다.

Add New License

License File: No file chosen

6. 새 라이선스 추가 대화 상자에서 파일 선택을 클릭하고 라이선스 파일의 위치를 찾습니다.
7. 업로드를 클릭합니다. 라이선스가 로컬로 업로드되고 테이블에 나타납니다.

License type: Local license

Add | Delete All

Product Name	Active	Total number of licenses	Number used	Type	Expires on
Citrix XenMobile Enterprise Edition Device	✓	15002	0	Retail	01-DEC-2015

Showing 1 - 1 of 1 items

Expiration notification: OFF

8. 라이선스 페이지의 테이블에 나타난 라이선스를 활성화합니다. 테이블의 첫 번째 라이선스인 경우 해당 라이선스가 자동으로 활성화됩니다.

원격 라이선스를 추가하려면

원격 Citrix Licensing 서버를 사용하는 경우 Citrix Licensing 서버를 사용하여 모든 라이선스 작업을 관리합니다. 자세한 내용은 [제품 라이선스](#)를 참조하십시오.

1. 라이선스 서버 인증서를 XenMobile Server 로 가져옵니다 (설정 > 인증서).
2. 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다. 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 **disable.hostname.verifcation** 을 **true** 로 변경하십시오. 이 속성의 기본값은 **false** 입니다.

호스트 이름 유효성 검사가 실패하면 서버 로그에 다음과 같은 오류가 포함됩니다. “볼륨 구매 서버에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’ 은 피어가 제공한 인증서 주체와 일치하지 않습니다.”

3. 라이선스 페이지에서 라이선스 구성을 커짐으로 설정합니다. 라이선스 유형 목록, 추가 단추 및 라이선스 테이블이 표시됩니다. 라이선스 테이블에는 XenMobile 에서 사용한 라이선스가 포함됩니다. Citrix 라이선스를 추가하지 않은 경우 테이블이 비어 있습니다.
4. 라이선스 유형을 원격 라이선스로 설정합니다. 추가 단추가 라이선스 서버 및 포트 필드와 연결 테스트 단추로 바뀝니다.

License type: Remote license

License server*:

Port*:

Product name	Active	Total number of licenses	Number used	Type	Expires on
		1001	0	Retail	01-DEC-2015

5. 다음 설정을 구성합니다.

- 라이선스 서버: 원격 라이선스 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름) 을 입력합니다.
- 포트: 기본 포트를 사용하거나 라이선스 서버와의 통신에 사용할 포트 번호를 입력합니다.

6. 연결 테스트를 클릭합니다. 연결이 성공적인 경우 XenMobile 이 라이선스 서버에 연결하고 라이선스 테이블이 사용 가능한 라이선스로 채워집니다. 테이블에 라이선스가 하나만 있는 경우 자동으로 활성화됩니다.

연결 테스트를 클릭하면 XenMobile 이 다음을 확인합니다.

- XenMobile 에서 라이선스 서버와 통신할 수 있습니다.
- 라이선스 서버의 라이선스가 유효합니다.
- 라이선스 서버가 XenMobile 과 호환됩니다.

연결이 실패한 경우 표시된 오류 메시지를 검토하고 필요한 사항을 수정한 후 연결 테스트를 클릭합니다.

Perform various connectivity checks for XenMobile. A complete check might take several minutes to run before results appear. If you are not using selected features within the console, clear the selections to speed the process.

Perform connectivity checks for ☒ Cluster

☐ .15

☒ .18

☐ Connectivity to IP address or FQDN .18

☐ License Server .22

Showing 1 - 1 of 1 items

Successful Connection

Connectivity results for ".18"

.22

Server is reachable.
Port 27000/TCP is open.
The server is a valid license server.

Clear Results Test Connectivity

서로 다른 라이선스를 활성화하려면

라이선스가 여러 개인 경우 활성화할 라이선스를 선택할 수 있습니다.

1. 라이선스 페이지의 라이선스 테이블에서 활성화할 라이선스를 선택합니다. 목록에서 아무 행이나 클릭하면 활성화 대화 상자가 나타납니다.

<input type="checkbox"/>	Product name	Status	Active	Total number of licenses	Number used	Type	Expires on
<input type="checkbox"/>	Citrix XenMobile Enterprise Edition User	Up to date	✓	1001	12	Retail	12/1/23
<input checked="" type="checkbox"/>	Citrix XenMobile Enterprise Edition Device	Up to date		1001	6	Retail	12/1/23
<input type="checkbox"/>	Citrix XenMobile Advanced Edition User	Up to date		1001	0	Retail	12/1/23
<input checked="" type="checkbox"/>	Citrix XenMobile Advanced Edition Device	Up to date		1011	4	Eval	12/1/23
<input type="checkbox"/>	Citrix XenMobile Advanced Edition Device	Up to date		1011	0	Retail	12/1/23
<input type="checkbox"/>	Citrix XenMobile MDM Edition User	Up to date		1001	1	Retail	
<input type="checkbox"/>	Citrix XenMobile MDM Edition Device	Up to date		1001	0	Retail	

✓

Activate

2. 활성화를 클릭합니다.
3. 활성 행에 라이선스에 대한 확인 표시가 보이면 저장을 클릭합니다.

중요:

- 사용자별 라이선스와 장치별 라이선스는 상호 배타적이며 동시에 활성화할 수 없습니다.

- ADV 에디션과 ENT 에디션 라이선스만 함께 사용할 수 있습니다. MDM 에디션 라이선스는 ADV 에디션 또는 ENT 에디션 라이선스와 함께 사용할 수 없습니다.
- 동일한 에디션의 라이선스 파일이 동일한 상태인지 확인하십시오. 예를 들어, 하나의 ADV 에디션 파일이 활성화되면 나머지 ADV 파일도 자동으로 활성화됩니다.
- XenMobile Server 10.15 롤링 패치 3 이전 버전의 경우 한 번에 하나의 라이선스만 활성화할 수 있습니다. 선택한 라이선스를 활성화하면 현재 라이선스가 비활성화됩니다.

만료 알림을 자동화하려면

원격 또는 로컬 라이선스를 활성화한 후 라이선스 만료 날짜가 가까워질 때 알림을 보내도록 XenMobile 을 구성할 수 있습니다.

1. 라이선스 페이지에서 만료 알림을 켜짐으로 설정합니다. 새 알림 관련 필드가 나타납니다.

Expiration notification ☒

Notify every* 7 day(s) 60 day(s) before expiration

Recipient* Enter email address(es)

Content* License expiry notice

2. 다음 설정을 구성합니다.

- 알림 간격: 유형:
- 알림을 보낼 빈도 (예: **7** 일마다) 입니다.
- 알림 전송을 시작할 시기 (예: 라이선스 만료 60 일 전) 입니다.
- 받는 사람: 자신의 전자 메일 주소 또는 라이선스 담당자의 전자 메일 주소를 입력합니다.
- 내용: 받는 사람이 알림에서 볼 만료 알림 메시지를 입력합니다.

3. 저장을 클릭합니다. 설정을 기반으로 XenMobile 이 내용에 입력된 텍스트가 포함된 전자 메일 메시지를 받는 사람에 입력된 받는 사람에게 보내기 시작합니다. 알림은 설정한 빈도로 전송됩니다.

FIPS 140-2 준수

January 5, 2022

미국 NIST(표준 기술 연구소) 에서 발행한 FIPS(Federal Information Processing Standard) 는 보안 시스템에 사용되는 암호화 모듈의 보안 요구 사항을 지정합니다. FIPS 140-2 는 이 표준의 두 번째 버전입니다. NIST 가 검증한 FIPS 140 모듈에 대한 자세한 내용은 [NIST Computer Security Resource Center](#)를 참조하십시오.

중요:

- XenMobile FIPS 모드는 초기 설치 중에만 설정할 수 있습니다.
- XenMobile 모바일 기기 관리 전용, XenMobile 모바일 앱 관리 전용 및 XenMobile MDM+MAM 은 모두 HDX 앱을 사용하지 않는 한 FIPS 를 준수합니다.

iOS 의 모든 저장 데이터 및 전송 중 데이터 암호화 작업에는 Citrix 및 Apple 에서 제공하는 FIPS 검증 암호화 모듈이 사용됩니다. Android 의 모든 저장 데이터 암호화 작업에는 FIPS 검증 암호화 모듈 또는 장치 제조업체에서 제공하는 플랫폼 암호화 모듈이 사용됩니다. 장치 제조업체의 모듈에 대한 자세한 정보는 Citrix 담당자에게 문의하십시오.

지원되는 Windows 장치의 MDM(모바일 기기 관리) 에 대한 모든 저장 데이터 및 전송 중 데이터 암호화 작업에는 FIPS 검증 암호화 모듈이 사용됩니다.

XenMobile MDM 의 모든 저장 데이터 및 전송 중 데이터 암호화 작업에는 FIPS 검증 암호화 모듈이 사용됩니다. MDM 흐름의 모든 저장된 데이터와 전송 중 데이터에는 FIPS 준수 암호화 모듈이 사용됩니다. 이 보안에는 위에서 설명한 모바일 장치에 대한 암호화 작업에 더해 모바일 장치와 Citrix Gateway 간의 암호화 작업이 포함됩니다.

MDX Vault 는 iOS 및 Android 장치의 MDX 래핑된 앱 및 연관된 저장 데이터를 FIPS 인증 암호화 모듈을 사용하여 암호화합니다.

언어 지원

December 1, 2020

모바일 생산성 앱 및 XenMobile 콘솔은 영어 이외의 언어로 사용하기 적합합니다. 앱이 사용자의 기본 설정 언어로 현지화되지 않은 경우에도 영어 이외의 문자 및 키보드 입력이 지원됩니다. 모든 Citrix 제품의 국제화 지원에 대한 자세한 내용은 <https://support.citrix.com/article/CTX119253>을 참조하십시오.

이 문서에서는 XenMobile 의 최신 릴리스에서 지원되는 언어를 나열합니다.

XenMobile 콘솔 및 자가 지원 포털

- 프랑스어
- 독일어
- 스페인어
- 일본어
- 한국어
- 포르투갈어
- 중국어 (간체)

모바일 생산성 앱

X 는 해당 언어로 앱을 사용할 수 있음을 나타냅니다.

iOS 및 Android

언어	Secure Hub	Secure Mail	Secure Web	QuickEdit
일본어	X	X	X	X
중국어 (간체)	X	X	X	X
중국어 (번체)	X	X	X	X
프랑스어	X	X	X	X
독일어	X	X	X	X
스페인어	X	X	X	X
한국어	X	X	X	X
포르투갈어	X	X	X	X
네덜란드어	X	X	X	X
이탈리아어	X	X	X	X
덴마크어	X	X	X	X
스웨덴어	X	X	X	X
히브리어	X	X	X	iOS 만 해당
아랍어	X	X	X	X
러시아어	X	X	X	X
터키어	X	X	Android 전용	-
폴란드어	X	X	X	-

Windows

언어	Secure Hub	Secure Mail	Secure Web
프랑스어	X	X	X
독일어	X	X	X

언어	Secure Hub	Secure Mail	Secure Web
스페인어	X	X	X
이탈리아어	X	X	X
덴마크어	X	X	X
스웨덴어	X	X	X

오른쪽에서 왼쪽으로 읽는 언어 지원

다음 표는 각 앱의 중동 언어 텍스트 지원을 요약한 것입니다. X는 해당 플랫폼에서 기능을 사용할 수 있음을 나타냅니다. Windows 장치에서는 오른쪽에서 왼쪽으로 읽는 언어가 지원되지 않습니다.

앱	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
QuickEdit	X	X

설치 및 구성

March 15, 2024

시작하기 전에

다음 사전 설치 체크리스트를 사용하여 온-프레미스에 XenMobile을 설치하기 위한 사전 요구 사항과 설정을 확인할 수 있습니다. 각 작업 또는 메모에는 요구 사항이 적용되는 구성 요소 또는 기능을 나타내는 열이 포함되어 있습니다.

XenMobile 배포를 계획할 때는 많은 요소를 고려해야 합니다. 전체 XenMobile 환경에 대한 권장 사항, 일반적인 질문 및 사용 사례는 [XenMobile 배포 안내서](#)를 참조하십시오.

설치 단계는 이 문서 뒷부분의 [XenMobile 설치](#) 섹션을 참조하십시오.

사전 설치 체크리스트

기본 네트워크 연결

다음은 XenMobile 솔루션에 필요한 네트워크 설정입니다.

- | 사전 요구 사항 또는 설정 | 구성 요소 또는 기능 | 설정 메모 |
- | ————| ————| ————|
- | 원격 사용자가 연결하는 FQDN(정규화된 도메인 이름) 을 적어 둡니다. | XenMobile 및 Citrix Gateway |
- | 공용 및 로컬 IP 주소를 적어 둡니다. |
- | 방화벽을 구성하여 NAT(Network Address Translation) 를 설정하려면 이러한 IP 주소가 필요합니다. | XenMobile 및 Citrix Gateway | |
- | 서브넷 마스크를 적어 둡니다. | XenMobile 및 Citrix Gateway | |
- | DNS IP 주소를 적어 둡니다. | XenMobile 및 Citrix Gateway | |
- | WINS 서버 IP 주소 (해당하는 경우) 를 적어 둡니다. | Citrix Gateway | |
- | Citrix Gateway 호스트 이름을 식별하고 적어 둡니다. | Citrix Gateway | 이 항목은 FQDN 이 아닙니다. FQDN 은 가상 서버에 바인딩되어 있고 사용자가 연결하는 서명된 서버 인증서에 포함되어 있습니다. Citrix Gateway 에서 설치 마법사를 사용하여 호스트 이름을 구성할 수 있습니다. | Citrix Gateway | |
- | XenMobile 의 IP 주소를 적어 둡니다. XenMobile 의 인스턴스 하나를 설치하는 경우 IP 주소 하나를 예약합니다. 클러스터를 구성하는 경우 필요한 모든 IP 주소를 적어 둡니다. | XenMobile | |
- | Citrix Gateway 에 구성된 공용 IP 주소 1 개 | Citrix Gateway | |
- | Citrix Gateway 에 대한 외부 DNS 항목 1 개 | Citrix Gateway |
- | 웹 프록시 서버 IP 주소, 포트, 프록시 호스트 목록 및 관리자 사용자 이름/암호를 적어 둡니다. 회사 네트워크 (해당하는 경우) 에 프록시 서버를 배포하는 경우 이러한 설정은 선택 사항입니다. | Citrix Gateway | 웹 프록시에 대한 사용자 이름을 구성할 때 sAMAccountName 또는 UPN(사용자 계정 이름) 을 사용할 수 있습니다. | XenMobile 및 Citrix Gateway | |
- | 기본 게이트웨이 IP 주소를 적어 둡니다. | XenMobile 및 Citrix Gateway | |
- | 시스템 IP(NSIP) 주소 및 서브넷 마스크를 적어 둡니다. | Citrix Gateway | |
- | 서브넷 IP(SNIP) 주소 및 서브넷 마스크를 적어 둡니다. | Citrix Gateway | |
- | 인증서에서 Citrix Gateway 가상 서버 IP 주소 및 FQDN 을 적어 둡니다. 다수의 가상 서버를 구성하려면 인증서의 모든 가상 IP 주소 및 FQDN 을 적어 둡니다. | Citrix Gateway | |
- | 사용자가 Citrix Gateway 를 통해 액세스할 수 있는 내부 네트워크를 적어 둡니다. 예: 10.10.0.0/24. 분할 터널링이 켜짐으로 설정된 경우 사용자가 Secure Hub 또는 Citrix Gateway 플러그인에 연결할 때 액세스해야 하는 모든 내부 네트워크 및 네트워크 세그먼트를 입력합니다. | Citrix Gateway | |
- | XenMobile Server, Citrix Gateway, 외부 Microsoft SQL Server 및 DNS 서버 간의 네트워크 연결이 접속 가능한지 확인합니다. | XenMobile 및 Citrix Gateway | |

라이센싱

XenMobile 을 사용하려면 Citrix Gateway 및 XenMobile 에 대한 라이선스 옵션을 구입해야 합니다. Citrix Licensing 에 대한 자세한 내용은 [The Citrix Licensing System\(Citrix Licensing 시스템\)](#)을 참조하십시오.

사전 요구 사항	구성 요소	위치 메모
Citrix 웹 사이트에서 범용 라이선스를 구입합니다. 자세한 내용은 Citrix Gateway 설명서에서 Licensing(라이선스)을 참조하십시오.	Citrix Gateway, XenMobile 및 Citrix License Server	

인증서

XenMobile 및 Citrix Gateway를 사용자 장치의 다른 Citrix 제품 및 앱과 연결하려면 인증서가 필요합니다. 자세한 내용은 XenMobile 설명서의 [인증서 및 인증](#) 섹션을 참조하십시오.

| 사전 요구 사항 | 구성 요소 | 참고 |

| ——— | ——— | — |

| 필요한 인증서를 받아서 설치합니다. | XenMobile 및 Citrix Gateway |

포트

XenMobile 구성 요소와 통신할 수 있도록 포트를 엽니다.

사전 요구 사항	구성 요소	참고
XenMobile 포트를 엽니다.	XenMobile 및 Citrix Gateway	

데이터베이스

XenMobile에 데이터베이스 연결을 구성해야 합니다. XenMobile 저장소에는 [시스템 요구 사항 및 호환성](#)에 명시된 지원되는 버전 중 하나에서 실행되는 Microsoft SQL Server 데이터베이스가 필요합니다. Microsoft SQL은 원격으로 사용하는 것이 좋습니다. PostgreSQL은 XenMobile에 포함되어 있으며 테스트 환경에서만 로컬 또는 원격으로 사용할 수 있습니다.

기본적으로 XenMobile은 JTDS 데이터베이스 드라이버를 사용합니다. XenMobile Server의 온-프레미스 설치에 Microsoft JDBC 드라이버를 사용하려면 [SQL Server 드라이버](#)를 참조하십시오.

사전 요구 사항	구성 요소	참고
Microsoft SQL Server, IP 주소 및 포트. XenMobile에 사용할 SQL Server 서비스 계정에 DBcreator 역할 권한이 있는지 확인합니다.	XenMobile	

Active Directory 설정

- | 사전 요구 사항 | 구성 요소 | 참고 |
- | ————| ————| ————|
- | 주 서버와 보조 서버의 Active Directory IP 주소 및 포트를 적어 둡니다. 포트 636 을 사용하는 경우 XenMobile 에서 CA 의 루트 인증서를 설치하고 보안 연결 사용 옵션을 예로 변경합니다.| XenMobile 및 Citrix Gateway|
- | Active Directory 도메인 이름을 적어 둡니다.| XenMobile 및 Citrix Gateway|
- | Active Directory 서비스 계정을 사용자 ID, 암호 및 도메인 별칭을 포함하여 적어 둡니다. |
- | Active Directory 서비스 계정은 XenMobile 이 Active Directory 에 쿼리할 때 사용하는 계정입니다. | XenMobile 및 Citrix Gateway| |
- | 사용자가 위치한 디렉터리 수준을 나타내는 사용자 기본 DN 을 적어 둡니다. 예: `cn=users,dc=ace,dc=com`. Citrix Gateway 및 XenMobile 은 사용자 기본 DN 을 사용하여 Active Directory 에 쿼리합니다. | XenMobile 및 Citrix Gateway| |
- | 그룹이 위치한 디렉터리 수준을 나타내는 그룹 기본 DN 을 적어 둡니다. Citrix Gateway 및 XenMobile 은 이 DN 을 사용하여 Active Directory 에 쿼리합니다. | XenMobile 및 Citrix Gateway| |

XenMobile 과 Citrix Gateway 간 연결

사전 요구 사항	구성 요소	설정 메모
XenMobile 호스트 이름을 적어 둡니다.	XenMobile	
XenMobile 의 FQDN 또는 IP 주소를 적어 둡니다.	XenMobile	
사용자가 액세스할 수 있는 앱을 파악합니다.	Citrix Gateway	
콜백 URL 을 적어 둡니다.	XenMobile	

사용자 연결: Citrix Virtual Apps and Desktops 및 Citrix Secure Hub 액세스

Citrix ADC 의 Quick Configuration(빠른 구성) 마법사를 사용하여 XenMobile 과 Citrix Gateway 간의 연결 설정 및 XenMobile 과 Secure Hub 간의 연결 설정을 구성하는 것이 좋습니다. 두 번째 가상 서버를 생성하여 Citrix Receiver 와 웹 브라우저에서 사용자 연결을 사용하도록 설정합니다. 이러한 연결은 Virtual Apps and Desktops 에 있는 Windows 기반 응용 프로그램과 가상 데스크톱에 대한 연결입니다. 이러한 설정도 Citrix ADC 의 Quick Configuration(빠른 구성) 마법사를 사용하여 구성하는 것이 좋습니다.

사전 요구 사항	구성 요소	설정 메모
Citrix Gateway 호스트 이름 및 외부 URL 을 적어 둡니다. 외부 URL 은 사용자가 연결하는 웹 주소입니다.	XenMobile	
Citrix Gateway 콜백 URL 을 적어 둡니다.	XenMobile	
가상 서버의 IP 주소와 서브넷 마스크를 적어 둡니다.	Citrix Gateway	
Program Neighborhood Agent 또는 Virtual Apps and Desktops 사이트의 경로를 적어 둡니다.	Citrix Gateway 및 XenMobile	
STA(Secure Ticket Authority) 를 실행하는 Virtual Apps and Desktops 서버의 FQDN 또는 IP 주소를 적어 둡니다 (ICA 연결에만 해당).	Citrix Gateway	
XenMobile 의 공용 FQDN 을 적어 둡니다.	Citrix Gateway	
Secure Hub 의 공용 FQDN 을 적어 둡니다.	Citrix Gateway	

XenMobile 배포 순서도

이 순서도에서는 XenMobile 을 배포하는 주요 단계를 안내합니다. 각 단계에 대한 항목으로 연결되는 링크가 그림 다음에 옵니다.

- 1: [시스템 요구 사항 및 호환성](#)
- 2: [설치 및 구성](#)
- 3 및 4: 사전 설치 체크리스트 (이 문서)
- 5: 명령 프롬프트 창에서 XenMobile 구성 (이 문서)
- 6: 웹 브라우저에서 XenMobile 구성 (이 문서)
- 7: [XenMobile 환경에 대한 설정 구성](#)
- 8: [포트 요구 사항](#)

XenMobile 설치

XenMobile VM(가상 컴퓨터) 은 Citrix XenServer, VMware ESXi 또는 Microsoft Hyper-V 에서 실행됩니다. XenCenter 또는 vSphere 관리 콘솔을 사용하여 XenMobile 을 설치할 수 있습니다.

참고:

NTP 서버 또는 수동 구성을 사용하여 하이퍼바이저에 정확한 시간이 구성되어 있는지 확인합니다. XenMobile 에서 해당 시간을 사용합니다. XenMobile 시간을 하이퍼바이저와 동기화할 때 표준 시간대 관련 문제가 나타나는 경우 XenMobile 이 NTP 서버를 가리키도록 하면 이 문제를 방지할 수 있습니다. 이렇게 하려면 [CLI 옵션](#)에 나온 대로 XenMobile CLI 를 사용합니다.

XenServer 또는 **VMware ESXi** 사전 요구 사항. XenServer 또는 VMware ESXi 에 XenMobile 를 설치하기 전에 다음을 수행해야 합니다. 자세한 내용은 [XenServer](#) 또는 [VMware](#) 설명서를 참조하십시오.

- 적절한 하드웨어 리소스가 있는 컴퓨터에 XenServer 또는 VMware ESXi 를 설치합니다.
- XenCenter 또는 vSphere 를 별도의 컴퓨터에 설치합니다. XenCenter 또는 vSphere 를 호스트하는 컴퓨터는 네트워크를 통해 XenServer 또는 VMware ESXi 호스트에 연결합니다.

Hyper-V 관련 사전 요구 사항. Hyper-V 에 XenMobile 을 설치하기 전에 다음을 수행해야 합니다. 자세한 내용은 [Hyper-V](#) 설명서를 참조하십시오.

- 충분한 시스템 리소스를 보유하고 있는 컴퓨터에서 Hyper-V 와 역할을 활성화한 상태로 Windows Server 2016 또는 Windows Server 2019 를 설치하십시오. Hyper-V 역할을 설치할 때 Hyper-V 에서 가상 네트워크를 만드는 데 사용할 서버에서 NIC 를 지정해야 합니다. 일부 NIC 는 호스트용으로 남겨 둘 수 있습니다.
- Virtual Machines/<build-specific UUID>.xml 파일을 삭제합니다.
- Legacy/<build-specific UUID>.exp 파일을 Virtual Machines 로 이동합니다.

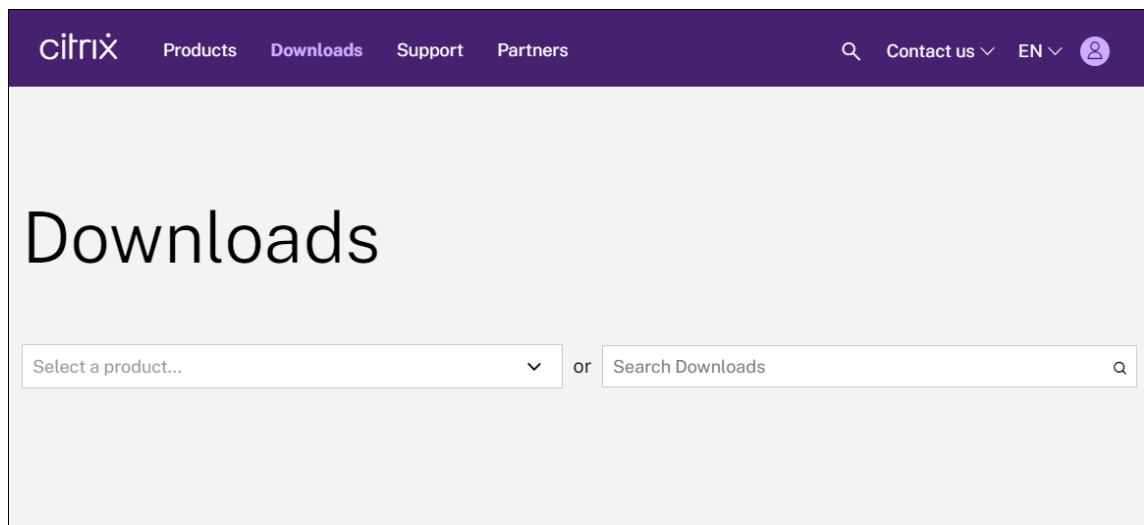
FIPS 140-2 모드. XenMobile Server 를 FIPS 모드로 설치하려는 경우 [XenMobile](#) 을 사용하여 **FIPS** 구성에 나온 일련의 사전 요구 사항을 완료합니다.

XenMobile 제품 소프트웨어 다운로드

[Citrix 웹 사이트](#)에서 제품 소프트웨어를 다운로드할 수 있습니다. 사이트에 로그인한 후 Download(다운로드) 링크를 사용하여 다운로드할 소프트웨어가 있는 페이지로 이동합니다.

XenMobile 소프트웨어를 다운로드하려면

1. [Citrix 웹 사이트](#)로 이동합니다.
2. Search(검색) 상자 옆에 있는 **Log On(로그온)** 을 클릭하여 계정에 로그인합니다.
3. **Downloads(다운로드)** 탭을 클릭합니다.
4. 다운로드 페이지의 제품 선택 목록에서 **Citrix Endpoint Management(및 Citrix XenMobile Server)** 를 선택합니다. Citrix Endpoint Management(및 Citrix XenMobile Server) 페이지가 자동으로 나타납니다.



5. **XenMobile Server**(온-프레미스) 를 확장합니다.
6. **Product Software**(제품 소프트웨어) 를 확장합니다.
7. **XenMobile Server 10** 을 클릭합니다.
8. **Jump to Download**(다운로드로 이동) 메뉴를 클릭하고 XenMobile 을 설치할 때 사용할 가상 이미지를 선택합니다. 또는 페이지를 아래로 스크롤하여 설치할 이미지에 대한 **Download File**(파일 다운로드) 단추를 찾습니다.
9. 화면의 지침을 따라 소프트웨어를 다운로드합니다.

Citrix Gateway 소프트웨어를 다운로드하려면 Citrix Gateway 가상 장비 또는 소프트웨어 업그레이드를 기존 Citrix Gateway 장비에 다운로드하려면 다음 절차를 사용합니다.

1. [Citrix 웹 사이트](#)로 이동합니다.
2. Citrix 웹 사이트에 아직 로그인하지 않은 경우 Search(검색) 상자 옆에 있는 **Log On**(로그온) 을 클릭하여 계정에 로그인합니다.
3. **Downloads**(다운로드) 탭을 클릭합니다.
4. 다운로드 페이지의 제품 선택 목록에서 **Citrix Gateway** 를 클릭합니다.
5. **Go**(이동) 를 클릭합니다. Citrix Gateway 페이지가 나타납니다.
6. Citrix Gateway 페이지에서 실행 중인 Citrix Gateway 버전을 확장합니다.
7. **Firmware**(펌웨어) 아래에서 다운로드할 장비 소프트웨어 버전을 클릭합니다.

참고:

Virtual Appliances(가상 장비) 를 클릭하여 Citrix ADC VPX 를 다운로드할 수도 있습니다. 이 옵션을 선택하면 각 하이퍼바이저에 대한 가상 컴퓨터용 소프트웨어 목록이 나타납니다.

8. 다운로드하려는 장비 소프트웨어 버전을 클릭합니다.

9. 다운로드하려는 버전의 장비 소프트웨어 페이지에서 해당 가상 장비에 대해 **Download(다운로드)** 를 클릭합니다.
10. 화면의 지침을 따라 소프트웨어를 다운로드합니다.

처음 사용을 위한 **XenMobile** 구성

1. XenMobile 에 대한 IP 주소와 서브넷 마스크, 기본 게이트웨이, DNS 서버 등을 구성하려면 XenCenter 또는 vSphere 명령줄 콘솔을 사용합니다.

참고:

vSphere 웹 클라이언트를 사용하는 경우 **Customize template(사용자 지정 템플릿)** 페이지에서 OVF 템플릿을 배포할 때 네트워킹 속성을 구성하지 않는 것이 좋습니다. 이렇게 하면 고가용성 구성에서 복제 후 두 번째 XenMobile 가상 컴퓨터를 다시 시작할 때 발생하는 IP 주소 관련 문제를 방지할 수 있습니다.

2. XenMobile Server 의 정규화된 도메인 이름 또는 노드의 IP 주소를 통해서만 XenMobile 관리 콘솔에 액세스합니다.
3. 로그인한 후 초기 로그인 화면의 단계를 수행합니다.

명령 프롬프트 창에서 **XenMobile** 구성

1. XenMobile 가상 컴퓨터를 Citrix XenServer, Microsoft Hyper-V 또는 VMware ESXi 로 가져옵니다. 자세한 내용은 [XenServer](#), [Hyper-V](#) 또는 [VMware](#) 설명서를 참조하십시오.
2. 하이퍼바이저에서, 가져온 XenMobile 가상 컴퓨터를 선택하고 명령 프롬프트 보기를 시작합니다. 자세한 내용은 해당 하이퍼바이저의 설명서를 참조하십시오.
3. 하이퍼바이저의 콘솔 페이지에서 명령 프롬프트 창에 관리자의 사용자 이름 및 암호를 입력하여 XenMobile 의 관리자 계정을 만듭니다.

명령 프롬프트 관리자 계정, PKI(공개 키 인프라) 서버 인증서 및 FIPS 의 암호를 만들거나 변경하는 경우 XenMobile 외부에서 암호가 관리되는 Active Directory 사용자를 제외한 모든 사용자에게 다음 규칙이 적용됩니다.

- 암호는 8 자 이상이어야 합니다.
- 암호는 다음 복잡성 기준 중 최소 3 개를 충족해야 합니다.
 - 대문자 (A ~ Z)
 - 소문자 (a ~ z)
 - 숫자 (0 ~ 9)
 - 특수 문자 (예: ! # \$ %)

```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through the
initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password: █
```

새 암호를 입력할 때 별표와 같은 문자는 표시되지 않습니다.

4. 다음 네트워크 정보를 입력한 후 **y** 를 입력하여 설정을 적용합니다.

- a) XenMobile Server 의 IP 주소
- b) 넷마스크
- c) 기본 게이트웨이 - DMZ 에 있는 기본 게이트웨이의 IP 주소
- d) 주 DNS 서버 - DNS 서버의 IP 주소
- e) 보조 DNS 서버 (선택 사항)

```
Network settings:
IP address: 192.0.2.0
Netmask: 225.225.225.128
Default gateway: 203.0.113.3
Primary DNS server: 192.0.2.4
Secondary DNS server [optional]: 192.0.2.5

Commit settings [y/n]: y█
```

참고:

이 이미지와 다음 이미지에 표시된 주소는 작동하지 않는 주소이며 예를 위해서만 제공되었습니다.

5. 무작위 암호화 암호를 생성하여 보안을 강화하려면 **y** 를 입력하고 고유한 암호를 제공하려면 **n** 을 입력합니다. **y** 를 입력하여 무작위 암호를 생성하는 것이 좋습니다.

암호는 중요한 데이터를 보호하는 데 사용되는 암호화 키의 보호 차원에서 사용됩니다. 데이터의 암호화 및 암호 해독 시 서버 파일 시스템에 저장된 암호 해시를 사용하여 키가 검색됩니다. 암호는 볼 수 없습니다.

참고:

환경을 확장하고 추가 서버를 구성하려는 경우 고유한 암호를 제공합니다. 무작위 암호를 선택하는 경우 암호를 볼 수 없습니다.

```
Encryption passphrase:
Generate a random passphrase to secure the server data? [y/n]: y
```

6. 필요한 경우 FIPS(Federal Information Processing Standard) 를 사용하도록 설정합니다. FIPS 에 대한 자세한 내용은 [FIPS](#)를 참조하십시오. 또한 [XenMobile](#) 을 사용하여 [FIPS 구성](#)에 설명된 대로 일련의 사전 요구 사항을 충족해야 합니다.

```
Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]:
```

7. 다음 정보를 제공하여 데이터베이스 연결을 구성합니다.

```
Database connection:
Local or remote [l/r]: r
Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
Use SSL [y/n]: n
Server: .10
Port: 5432
Username: postgres
Password:
```

- 데이터베이스는 로컬 또는 원격일 수 있습니다. 로컬인 경우 **l** 을 입력하고 원격인 경우 **r** 을 입력합니다.
- 데이터베이스 유형을 선택합니다. Microsoft SQL 인 경우 **mi** 를 입력하고 PostgreSQL 인 경우 **p** 를 입력합니다.

중요:

- Microsoft SQL 은 원격으로 사용하는 것이 좋습니다. PostgreSQL 은 XenMobile 에 포함되어 있으며 테스트 환경에서만 로컬 또는 원격으로 사용할 수 있습니다.
- 데이터베이스 마이그레이션은 지원되지 않습니다. 테스트 환경에서 만든 데이터베이스를 프로덕션 환경으로 이동할 수 없습니다.

- 필요한 경우 **y** 를 입력하여 데이터베이스에 대한 SSL 인증을 사용합니다.
- XenMobile 을 호스트하는 서버의 FQDN(정규화된 도메인 이름) 을 입력합니다. 이 하나의 호스트 서버에서 장치 관리와 앱 관리 서비스를 모두 제공합니다.
- 기본 포트 번호와 다른 경우 해당 데이터베이스 포트 번호를 입력합니다. Microsoft SQL 의 기본 포트는 1433 이고 PostgreSQL 의 기본 포트는 5432 입니다.
- 데이터베이스 관리자의 사용자 이름을 입력합니다.
- 데이터베이스 관리자의 암호를 입력합니다.
- 데이터베이스 이름을 입력합니다.
- **Enter** 키를 눌러 데이터베이스 설정을 적용합니다.

8. 필요한 경우 **y** 를 입력하여 XenMobile 노드 또는 인스턴스의 클러스터를 사용하도록 설정합니다.

중요:

XenMobile 클러스터를 사용하도록 설정하는 경우 시스템 구성이 완료된 후 클러스터 구성원 간의 실시간 통신이 가능하도록 포트 80 을 열어야 합니다. 모든 클러스터 노드에 대해 이 설정을 완료합니다.

9. XenMobile Server 의 FQDN(정규화된 도메인 이름) 을 입력합니다.

```
XenMobile hostname:  
Hostname: justan.example.com
```

10. **Enter** 키를 눌러 설정을 적용합니다.

11. 통신 포트를 확인합니다. 포트와 용도에 대한 자세한 내용은 [포트 요구 사항](#)을 참조하십시오.

참고:

Enter(Mac 의 경우 Return) 키를 눌러 기본 포트를 적용합니다.

```
HTTP [80]: 80  
HTTPS with certificate authentication [443]: 443  
HTTPS with no certificate authentication [8443]: 8443  
HTTPS for management [4443]: 4443
```

12. XenMobile 을 처음으로 설치하는 것이므로 이전 XenMobile 릴리스에서의 업그레이드에 대한 다음 질문은 건너뛰니다.
13. 각 PKI(공개 키 인프라) 인증서에 동일한 암호를 사용하려면 **y** 를 입력합니다. XenMobile PKI 기능에 대한 자세한 내용은 [인증서 업로드](#)를 참조하십시오.

```
The wizard will now generate an internal Public Key Infrastructure (PKI):  
- A root certificate  
- An intermediate certificate to issue device certificates during enrollment  
- An intermediate certificate to issue an SSL certificate  
- An SSL certificate for your connectors  
Do you want to use the same password for all the certificates of the PKI [y]:  
New password:  
Re-enter new password:
```

중요:

XenMobile 의 노드 또는 인스턴스를 함께 클러스터링하려는 경우 후속 노드에 동일한 암호를 제공합니다.

14. 새 암호를 입력한 다음, 확인을 위해 새 암호를 다시 입력합니다.

새 암호를 입력할 때 별표와 같은 문자는 표시되지 않습니다.

15. **Enter** 키를 눌러 설정을 적용합니다.

16. 웹 브라우저에서 XenMobile 콘솔에 로그인할 때 사용할 관리자 계정을 만듭니다. 이러한 자격 증명을 기록하여 나중에 사용할 수 있도록 하십시오.

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile console through a web browser.
Username [administrator]: administrator
Password:
Re-enter new password:
```

참고:

새 암호를 입력할 때 별표와 같은 문자는 표시되지 않습니다.

17. **Enter** 키를 눌러 설정을 적용합니다. 초기 시스템 구성이 저장됩니다.
18. 새로운 설치이므로 업그레이드 중인지 묻는 메시지가 나타나면 **n** 을 입력합니다.
19. 화면에 나타나는 전체 URL 을 복사하고 웹 브라우저에서 이 초기 XenMobile 구성을 계속합니다.

```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
Upgrade from previous release (y/n) [n]:

Stopping configuration app... [ OK ]
Starting configuration app...
application started successfully [ OK ]
Stopping main app... [ OK ]
Starting main app...
this may take a few minutes.....
application started successfully [ OK ]

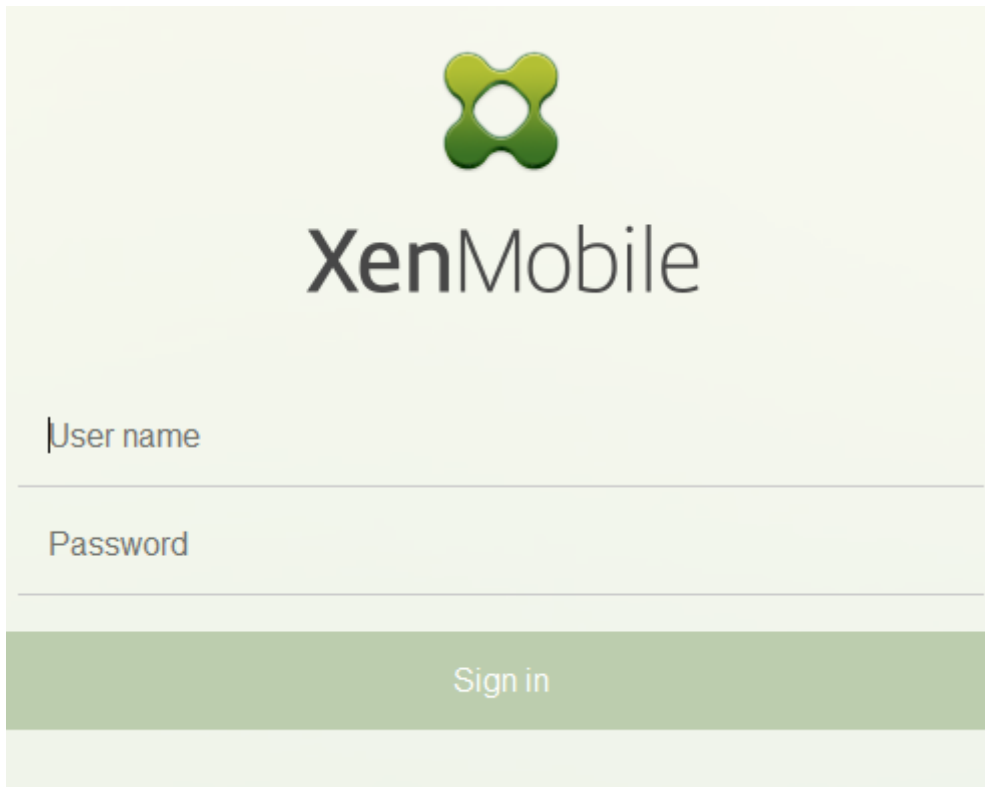
To access the console, from a web browser, go to the following location and
log on with your console credentials:
https://203.0.113.8:4443/

Starting monitoring... [ OK ]
```

웹 브라우저에서 XenMobile 구성

하이퍼바이저 명령 프롬프트 창에서 XenMobile 구성의 초기 부분을 완료한 후 웹 브라우저에서 프로세스를 완료합니다.

1. 웹 브라우저에서, 명령 프롬프트 창 구성의 마지막 부분에 제공된 위치로 이동합니다.
2. 명령 프롬프트 창에서 만든 XenMobile 콘솔 관리자 계정의 사용자 이름 및 암호를 입력합니다.

The image shows the XenMobile login interface. At the top center is the XenMobile logo, which consists of a green four-lobed shape above the word "XenMobile" in a dark grey sans-serif font. Below the logo are two input fields: the first is labeled "User name" and the second is labeled "Password". Both labels are in a light grey font. Below these fields is a green rectangular button with the text "Sign in" in white. The entire login area is set against a light green background.

3. 시작 페이지에서 시작을 클릭합니다. 라이선스 페이지가 나타납니다.
4. 라이선스를 구성합니다. 라이선스를 업로드하지 않는 경우 30 일 동안 유효한 평가 라이선스를 사용합니다. 라이선스를 추가 및 구성하고 만료 알림을 구성하는 방법에 대한 자세한 내용은 [라이선스](#)를 참조하십시오.

중요:

XenMobile의 클러스터 노드 또는 인스턴스를 추가하여 XenMobile 클러스터링을 사용하려는 경우 원격 서버에서 Citrix Licensing을 사용해야 합니다.

5. 인증서 페이지에서 가져오기를 클릭합니다. 가져오기 대화 상자가 나타납니다.
6. APNs 및 SSL 수신기 인증서를 가져옵니다. iOS 장치를 관리하려면 APNs 인증서가 필요합니다. 인증서 사용 방법에 대한 자세한 내용은 [인증서](#)를 참조하십시오.

참고:

이 단계를 수행하려면 서버를 다시 시작해야 합니다.

7. 환경에 해당되는 경우 Citrix Gateway를 구성합니다. Citrix Gateway를 구성하는 방법에 대한 자세한 내용은 [Citrix Gateway 및 XenMobile과 XenMobile 환경에 대한 설정 구성](#)을 참조하십시오.

참고:

- 내부 네트워크 경계 (또는 인트라넷)에 Citrix Gateway를 배포할 수 있습니다. 이 배포는 내부 네트워크에 있는 서버, 앱 및 기타 네트워크 리소스에 대한 안전한 단일 지점 액세스를 제공합니다. 이 배포에서는 모든

원격 사용자가 내부 네트워크의 리소스에 액세스하기 위해 먼저 Citrix Gateway 에 연결해야 합니다.

- Citrix Gateway 는 선택적인 설정이지만 이 페이지에서 데이터를 입력한 후에 페이지에서 나가려면 모든 필수 필드를 지우거나 작성해야 합니다.

8. Active Directory 에서 사용자 및 그룹에 액세스하려면 LDAP 구성을 완료합니다. LDAP 연결을 구성하는 방법에 대한 자세한 내용은 [LDAP 구성](#)을 참조하십시오.

9. 사용자에게 메시지를 보낼 수 있도록 알림 서버를 구성합니다. 알림 서버 구성에 대한 자세한 내용은 [알림](#)을 참조하십시오.

사후 요구 사항. XenMobile Server 를 다시 시작하여 인증서를 활성화합니다.

XenMobile 을 사용하여 FIPS 구성

September 13, 2023

XenMobile 의 FIPS(Federal Information Processing Standard) 모드는 모든 암호화 작업에 FIPS 140-2 인증 라이선스만 사용하여 미국 연방 정부 고객을 지원합니다. FIPS 모드를 사용하여 XenMobile Server 를 설치하면 XenMobile 클라이언트와 서버의 모든 데이터가 FIPS 140-2 를 완벽하게 준수합니다. 이러한 준수는 저장된 데이터와 전송 중 데이터에 적용됩니다.

FIPS 모드로 XenMobile Server 를 설치하기 전에 다음과 같은 사전 요구 사항을 충족합니다.

- XenMobile 데이터베이스에 외부 SQL Server 2014 를 사용합니다. 또한 보안 SSL 통신을 사용하도록 SQL Server 를 구성해야 합니다. SQL Server 에 대한 보안 SSL 통신을 구성하는 방법에 대한 자세한 내용은 [데이터베이스 엔진에 대한 암호화된 연결 사용 \(SQL Server Configuration Manager\)](#)을 참조하십시오.
- 보안 SSL 통신을 사용하려면 SQL Server 에 잘 알려진 CA(인증 기관)의 신뢰할 수 있는 SSL 인증서를 설치해야 합니다. SQL Server 2014 에는 와일드카드 인증서를 사용할 수 없습니다. 따라서 SQL Server FQDN 을 사용하여 SSL 인증서를 요청하는 것이 좋습니다.

FIPS 모드 구성

FIPS 모드는 XenMobile Server 를 처음 설치하는 동안에만 사용하도록 설정할 수 있습니다. 설치가 완료된 후에는 FIPS 를 사용하도록 설정할 수 없습니다. 따라서 FIPS 모드를 사용하려는 경우 처음부터 FIPS 모드로 XenMobile Server 를 설치해야 합니다. 또한 XenMobile 클러스터의 경우 모든 클러스터 노드에서 FIPS 를 사용해야 합니다. FIPS 와 비 FIPS XenMobile Server 를 동일한 클러스터에 혼합하여 배치할 수 없습니다.

XenMobile 명령줄 인터페이스에 **Toggle FIPS mode(FIPS 모드 전환)**가 있지만 이는 프로덕션 용도가 아닙니다. 이 옵션은 비프로덕션 및 진단 용도로 제공되며 프로덕션 XenMobile Server 에서 지원되지 않습니다.

1. 초기 설정 시 **FIPS** 모드를 사용하도록 설정합니다.
2. SQL Server 에 대한 루트 CA 인증서를 업로드합니다.

3. SQL Server 의 서버 이름 및 포트, SQL Server 에 로그인하는 데 사용할 자격 증명, XenMobile 에 대해 만들 데이터베이스 이름을 지정합니다.

참고:

SQL 로그인 또는 Active Directory 계정을 사용하여 SQL Server 에 액세스할 수 있지만 사용하는 로그인 계정이 DBcreator 역할을 보유해야 합니다.

4. Active Directory 계정을 사용하려면 도메인\사용자 이름 형식으로 자격 증명을 입력합니다.
5. 이러한 단계를 완료한 후에는 XenMobile 초기 설정을 진행합니다.

FIPS 모드가 성공적으로 구성되었는지 확인하려면 XenMobile 명령줄 인터페이스에 로그인합니다. 로그인 배너에 **In FIPS Compliant Mode(FIPS 준수 모드)** 가 표시됩니다.

인증서 가져오기

다음 절차는 인증서를 가져와서 XenMobile 에서 FIPS 를 구성하는 방법을 설명합니다.

SQL 사전 요구 사항

1. XenMobile 에서 SQL 인스턴스로의 연결은 보안되어야 하며 SQL Server 2012 또는 SQL Server 2014 버전이어야 합니다. 연결 보안에 대한 자세한 내용은 [Microsoft Management Console 을 사용하여 SQL Server 인스턴스에 대해 SSL 암호화를 활성화하는 방법](#)을 참조하십시오.
2. 서비스가 제대로 다시 시작되지 않으면 다음을 확인합니다. **Services.msc** 를 엽니다.
 - a) SQL Server 서비스에 사용되는 로그인 계정 정보를 복사합니다.
 - b) SQL Server 에서 MMC.exe 를 엽니다.
 - c) 파일 > 스냅인 추가/제거로 이동한 후 해당 인증서 항목을 두 번 클릭하여 인증서 스냅인을 추가합니다. 마법사의 두 페이지에서 컴퓨터 계정과 로컬 컴퓨터를 선택합니다.
 - d) 확인을 클릭합니다.
 - e) 인증서 (로컬 컴퓨터) > 개인 > 인증서를 확장하여 가져온 SSL 인증서를 찾습니다.
 - f) 가져온 인증서를 마우스 오른쪽 단추로 클릭한 후 (SQL Server 구성 관리자에서 선택) 모든 작업 > 개인 키 관리를 클릭합니다.
 - g) 그룹 또는 사용자 이름 아래에서 추가를 클릭합니다.
 - h) 앞 단계에서 복사한 SQL 서비스 계정 이름을 입력합니다.
 - i) 모든 권한 허용 옵션을 선택 취소합니다. 기본적으로 서비스 계정은 모든 권한과 읽기 권한을 둘 다 갖지만 개인 키를 읽는 권한만 필요합니다.
 - j) **MMC** 를 닫고 SQL 서비스를 시작합니다.

3. SQL 서비스가 제대로 시작되는지 확인합니다.

IIS(인터넷 정보 서비스) 사전 요구 사항

1. 루트 인증서 (base 64) 를 다운로드합니다.
2. 루트 인증서를 IIS 서버의 기본 사이트 (C:\inetpub\wwwroot) 로 복사합니다.
3. 기본 사이트에 대해 인증 확인란을 선택합니다.
4. 익명을 사용으로 설정합니다.
5. 실패한 요청 추적 규칙 확인란을 선택합니다.
6. .cer 이 차단되지 않았는지 확인합니다.
7. 로컬 서버의 웹 브라우저에서.cer 위치로 이동합니다 (<https://localhost/certname.cer>). 루트 인증서 텍스트가 브라우저에 나타납니다.
8. 사용 중인 웹 브라우저에 루트 인증서가 표시되지 않을 경우 다음과 같이 IIS 서버에서 ASP 를 사용하도록 설정되어 있는지 확인합니다.
 - a) 서버 관리자를 엽니다.
 - b) 관리 > 역할 및 기능 추가에서 마법사로 이동합니다.
 - c) 서버 역할에서 웹 서버 (**IIS**), 웹 서버, 응용 프로그램 개발을 차례로 확장한 후 **ASP** 를 선택합니다.
 - d) 설치가 완료될 때까지 다음을 클릭합니다.

9. <https://localhost/cert.cer>로 이동합니다.

자세한 내용은 [웹 서버 \(IIS\)](#)를 참조하십시오.

참고:

이 절차에 CA 의 IIS 인스턴스를 사용할 수 있습니다.

초기 **FIPS** 구성 시 루트 인증서 가져오기

명령줄 콘솔에서 처음으로 XenMobile 구성 단계를 완료하는 경우 다음 설정을 완료하여 루트 인증서를 가져와야 합니다. 설치 단계에 대한 자세한 내용은 [XenMobile 설치](#)를 참조하십시오.

- Enable FIPS: Yes
- Upload Root Certificate: Yes
- Copy(c) or Import(i): i
- Enter HTTP URL to import: <https://<FQDN of IIS server>/cert.cer>
- Server: SQL Server 의 FQDN
- Port: 1433

- User name: 데이터베이스를 만들 수 있는 서비스 계정 (`domain\username`)
- Password: 서비스 계정의 암호
- Database Name: 원하는 이름

모바일 장치에서 **FIPS** 모드 사용

기본적으로 모바일 장치에서는 FIPS 모드가 사용되지 않습니다. FIPS 모드를 사용하려면 설정 > 클라이언트 속성으로 이동하고 **FIPS** 모드 사용 속성을 편집하여 값을 **true** 로 설정합니다. 자세한 내용은 [클라이언트 속성](#)을 참조하십시오.

클러스터링 구성

March 19, 2021

클러스터링을 구성하려면 Citrix ADC 에 다음 두 부하 분산 가상 IP 주소를 구성합니다.

- **MDM**(모바일 기기 관리) 부하 분산 가상 IP 주소: 클러스터로 구성된 XenMobile 노드와 통신하려면 MDM 부하 분산 가상 IP 주소가 필요합니다. 이 부하 분산은 SSL 브리지 모드에서 수행됩니다.
- **MAM**(모바일 앱 관리) 부하 분산 가상 IP 주소: Citrix Gateway 에서 클러스터로 구성된 XenMobile 노드와 통신하려면 MAM 부하 분산 가상 IP 주소가 필요합니다. XenMobile 에서는 기본적으로 Citrix Gateway 의 모든 트래픽이 포트 8443 의 부하 분산 가상 IP 주소로 전달됩니다.

이 문서에 나와 있는 절차는 새로운 XenMobile VM(가상 컴퓨터) 을 만들고 새 VM 을 기존 VM 에 연결하는 방법을 설명합니다. 이러한 단계를 수행하면 클러스터 설정이 만들어집니다.

사전 요구 사항

- 필요한 XenMobile 노드가 완전히 구성되어 있어야 합니다.
- 모든 클러스터 노드와 XenMobile 데이터베이스에 NTP 를 구성합니다. 클러스터링이 올바르게 작동하려면 이러한 모든 서버의 시간이 동일해야 합니다.
- MDM 부하 분산 장치용 공용 IP 주소 하나와 MAM 용 사설 IP 주소 하나
- 서버 인증서
- Citrix Gateway 가상 IP 주소에 사용할 가용 IP 주소 하나
- 클러스터 설치 및 MDM 전용 또는 엔터프라이즈 모드 (MDM+MAM) 에서 XenMobile 을 배포한 경우: 모든 Citrix ADC MDM 부하 분산 장치, 즉 포트 8443 및 443 에 대해 설정된 가상 서버에 **Source IP persistence**(소스 IP 지속성) 를 사용하도록 Citrix ADC 부하 분산 장치 구성을 수정합니다. 이 구성은 사용자 장치를 iOS 11 로 업그레이드하기 전에 완료되어야 합니다. 자세한 내용은 이 Citrix Knowledge Center 문서 (<https://support.citrix.com/article/CTX227406>) 를 참조하십시오.
- iOS 11 장치의 XenMobile Store 에서 앱을 설치하려면 XenMobile Server 에서 포트 80 을 사용하도록 설정해야 합니다.

클러스터링된 구성의 XenMobile 10.x 에 대한 참조 아키텍처 다이어그램은 [아키텍처](#)를 참조하십시오.

XenMobile 클러스터 노드 설치

필요한 노드 수에 따라 XenMobile VM 을 만듭니다. 새 VM 이 동일한 데이터베이스를 가리키도록 하고 동일한 PKI 인증서 암호를 제공합니다.

1. 새 VM 의 명령줄 콘솔을 열고 관리자 계정에 대한 새 암호를 입력합니다.
2. 다음 그림에 표시된 것과 같이 네트워크 구성 세부 정보를 제공합니다.

```
Network settings:
IP address [l]: 10.147.75.51
Netmask [l]: 255.255.255.0
Default gateway [l]: 10.147.75.1
Primary DNS server [l]: 10.147.75.240
Secondary DNS server (optional) [l]:

Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps
```

3. 데이터 보호를 위해 기본 암호를 사용하려면 **y** 를 입력합니다. 또는 **n** 을 입력한 후 새 암호를 입력합니다.

```
Encryption passphrase:
Generate a random passphrase to secure the server data (y/n) [y]:
```

4. FIPS 를 사용하려면 **y** 를 입력하고 그렇지 않으면 **n** 을 입력합니다.

```
Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]:
```

5. 이전에 완벽하게 구성된 VM 이 가리키는 동일한 데이터베이스를 가리키도록 데이터베이스를 구성합니다. “Database already exists(데이터베이스가 이미 있습니다)” 라는 메시지가 표시됩니다.

```
Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mil]:
Use SSL (y/n) [n]:

Server [l]: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..
```

6. 첫 번째 VM에 대해 제공한 것과 동일한 인증서 암호를 입력합니다.

```
Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:

Server []: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
```

- 암호를 입력하면 두 번째 노드에 대한 초기 구성이 완료됩니다.

```
Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
y
New password:
Re-enter new password:
Saving server and client certs password...

Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
this may take a few seconds..... [ OK ]
application started
Stopping main app... [ OK ]
Starting main app...
this may take a few minutes....._
```

7. 구성이 완료되면 서버가 다시 시작되고 로그인 대화 상자가 나타납니다.

```

Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
  this may take a few seconds.....
  application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
  this may take a few minutes.....^I.....
  application started [ OK ]

To access the console, from a web browser, go to the following location and
log on with your console credentials:
  https://10.147.75.59:4443/

Starting monitoring... [ OK ]
xms51.wg.lab login:

```

참고:

로그온 대화 상자는 첫 번째 VM 의 로그인 대화 상자와 동일합니다. 두 대화 상자가 일치하는 것을 통해 두 VM 이 동일한 데이터베이스 서버를 사용한다는 것을 확인할 수 있습니다.

8. XenMobile 의 FQDN(정규화된 도메인 이름) 을 사용하여 웹 브라우저에서 XenMobile 콘솔을 엽니다.
9. XenMobile 콘솔에서 오른쪽 위 모서리의 런치 아이콘을 클릭합니다.



지원 페이지가 열립니다.

10. 고급 아래에서 클러스터 정보를 클릭합니다.

Support		
Diagnostics	Support Bundle	Links
NetScaler Gateway Connectivity Checks	Create Support Bundles	Citrix Product Documentation
XenMobile Connectivity Checks		Citrix Knowledge Center
Log Operations	Advanced	Tools
Logs	Cluster Information	APNs Signing Utility
Log Settings	Garbage Collection	Citrix Insight Services
	Java Memory Properties	Device NetScaler Connector Status
	Macros	
	PKI Configuration	
	Anonymization and De-anonymization	

클러스터 구성원, 장치 연결 정보, 작업 등을 포함하여 클러스터에 대한 모든 정보가 나타납니다. 이제 새 노드가 클러스터의 구성원이 됩니다.

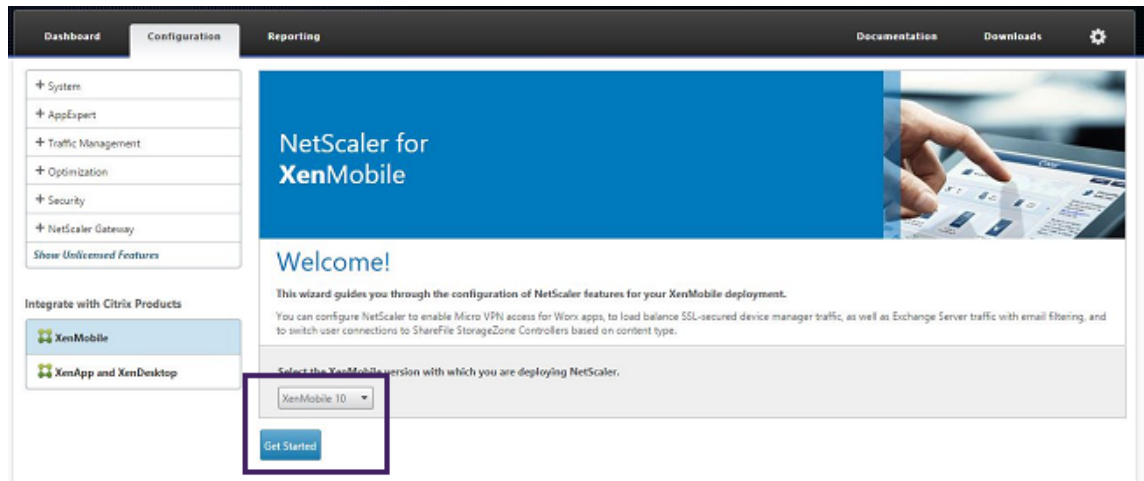
Support > Cluster Information						
Cluster Information						
Provides information about each of the nodes in the cluster.						
▼ Cluster Members						
Node ID	Node name	Status	Role	First check-in	Next check-in	
177425211		ACTIVE	null	2019-04-22 14:40:34.877	2019-04-22 01:52:56.293	
177425203		ACTIVE	OLDEST	2019-04-22 14:30:06.47	2019-04-22 02:09:02.61	
Showing 1 - 2 of 2 items						

동일한 단계를 수행하여 다른 노드를 추가할 수 있습니다. 클러스터에 추가된 첫 번째 노드는 **OLDEST** 역할을 갖습니다. 그 후에 추가된 노드에는 **NONE** 또는 **null** 역할이 표시됩니다.

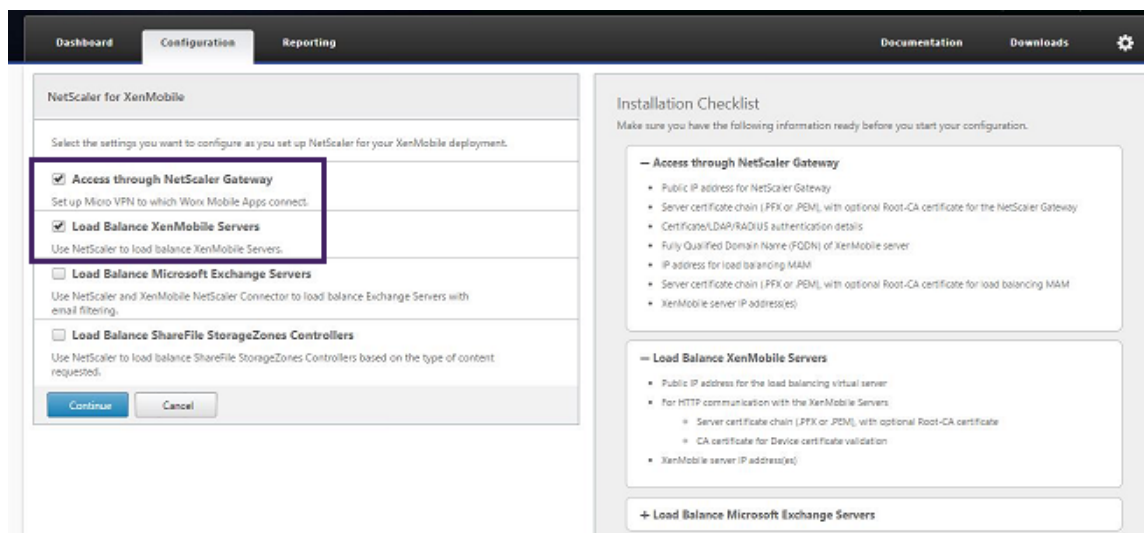
Citrix ADC 에서 XenMobile 클러스터에 대한 부하 분산을 구성하려면

필요한 노드를 XenMobile 클러스터의 구성원으로 추가한 후에는 노드가 클러스터에 액세스할 수 있도록 부하를 분산합니다. 부하 분산을 수행하려면 Citrix ADC 에서 사용할 수 있는 XenMobile 마법사를 실행합니다. 다음 단계는 마법사를 실행하여 XenMobile 의 부하를 분산하는 방법을 설명합니다.

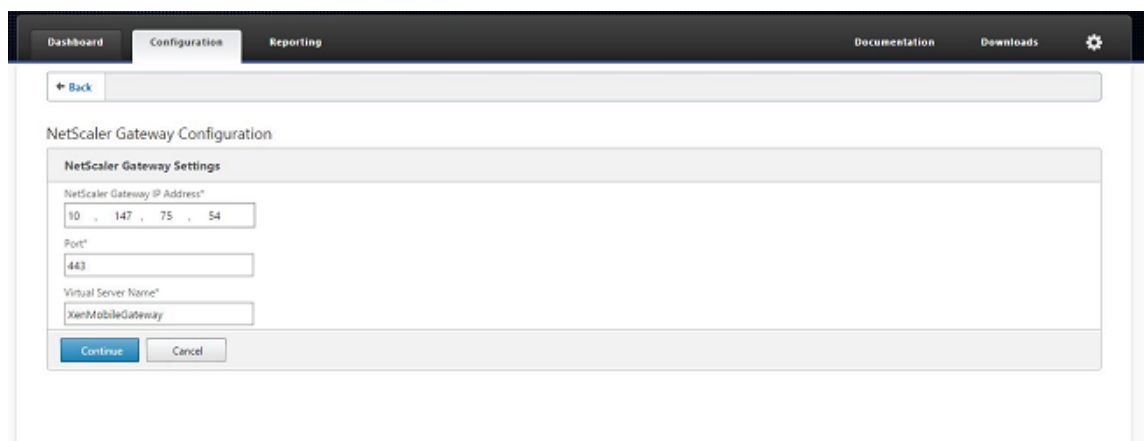
1. Citrix ADC 에 로그인합니다.
2. Configuration(구성) 탭에서 **XenMobile** 을 클릭하고 **Get Started(시작)** 를 클릭합니다.



3. **Citrix Gateway** 를 통해 액세스 확인란과 **XenMobile Server** 부하 분산 확인란을 선택한 후 **계속**을 클릭합니다.



4. Citrix Gateway 의 IP 주소를 입력하고 **Continue(계속)** 를 클릭합니다.



5. 다음 중 하나를 수행하여 서버 인증서를 Citrix Gateway 가상 IP 주소에 바인딩한 후 **Continue(계속)** 를 클릭합니다.

- **Use existing certificate**(기존 인증서 사용) 에서, 목록에서 해당 서버 인증서를 선택합니다.
- **Install Certificate**(인증서 설치) 탭을 클릭하여 새 서버 인증서를 업로드합니다.

The screenshot shows the 'NetScaler Gateway Configuration' page. Under the 'Server Certificate for NetScaler Gateway' section, the 'Use existing certificate' radio button is selected. A dropdown menu shows 'wildcert-wg-lab.pem_CERT_KEY' as the chosen certificate. The 'Continue' button is visible at the bottom.

6. 인증 서버 세부 정보를 입력하고 **Continue**(계속) 를 클릭합니다.

The screenshot shows the 'Authentication Settings' page. The 'Primary authentication method' is set to 'Active Directory/LDAP'. The 'IP Address' is 10.147.75.240. The 'Port' is 389. The 'Base DN' is dc=wg,dc=lab. The 'Service account' is administrator@wg.lab. The 'Password' and 'Confirm Password' fields are masked with asterisks. The 'Time out (seconds)' is 3. The 'Server Logon Name Attribute' is userPrincipalName. The 'Secondary authentication method' is set to 'None'. The 'Continue' button is visible at the bottom.

참고:

Server Logon Name Attribute(서버 로그인 이름 특성) 가 XenMobile LDAP 구성에서 지정한 것과 동일해야 합니다.

7. XenMobile settings(XenMobile 설정) 아래에서 Load Balancing FQDN for MAM(MAM 의 FQDN 부하 분산) 을 입력하고 **Continue**(계속) 를 클릭합니다.

참고:

MAM 부하 분산 가상 IP 주소의 FQDN 과 XenMobile 의 FQDN 이 동일해야 합니다.

8. SSL 브리지 모드 (HTTPS) 를 사용하려는 경우 **HTTPS communication to XenMobile Server(XenMobile 서버에 대한 HTTPS 통신)** 를 선택합니다. 그러나 SSL 오프로드를 사용하려는 경우 앞의 그림에 나온 것처럼 **HTTP communication to XenMobile Server(XenMobile Server 에 대한 HTTP 통신)** 를 선택합니다. 이 문서에서는 SSL 브리지 모드 (HTTPS) 를 선택했습니다.
9. MAM 부하 분산 가상 IP 주소에 대한 서버 인증서를 바인딩하고 Continue(계속) 를 클릭합니다.

10. XenMobile Servers 아래에서 **Add Server(서버 추가)** 를 클릭하고 XenMobile 노드를 추가합니다.

11. XenMobile 노드의 IP 주소를 입력하고 Add(추가) 를 클릭합니다.

12. 10-11 단계를 반복하여 XenMobile 클러스터의 일부인 XenMobile 노드를 추가합니다. 추가한 모든 XenMobile 노드가 표시됩니다. Continue(계속) 을 클릭합니다.

IP Address	Port
10.147.75.51	8443
10.147.75.59	8443

13. **Load Balance Device Manager Servers**(부하 분산 장치 관리자 서버) 를 클릭하여 MDM 부하 분산 구성을 계속합니다.

14. MDM 부하 분산 IP 주소에 사용할 IP 주소를 입력하고 **Continue**(계속) 를 클릭합니다.

Dashboard Configuration Reporting Documentation Downloads

Back

Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration

Enter a public IP address and a name for the load balancing virtual server.

IP Address*
10 . 147 . 75 . 56

Name*
XenMobileMDM

SSL Traffic Configuration
HTTPS communication to XenMobile Server

Continue Cancel

15. XenMobile 노드가 목록에 표시되면 **Continue**(계속) 를 누른 다음 **Done**(완료) 을 클릭하여 프로세스를 마칩니다.

Dashboard Configuration Reporting Documentation Downloads

Back

Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration

Name	IP Address	Port	SSL Traffic Configuration
MDM_XenMobileMDM	10.147.75.56	443,8443	HTTPS communication to XenMobile Server

XenMobile Servers

Add Server Remove Server

IP Address	Port
10.147.75.51	443, 8443
10.147.75.59	443, 8443

Continue

XenMobile 페이지에 가상 IP 주소 상태가 표시됩니다.

Dashboard Configuration Reporting Documentation Downloads

System AppExpert Traffic Management Optimization Security NetScaler Gateway Show Unlicensed Features

Integrate with Citrix Products

XenMobile XenApp and XenDesktop

NetScaler Gateway

Universal Licenses

Current Universal Licenses: 0

MDX Sessions

Current MDX Sessions: 0

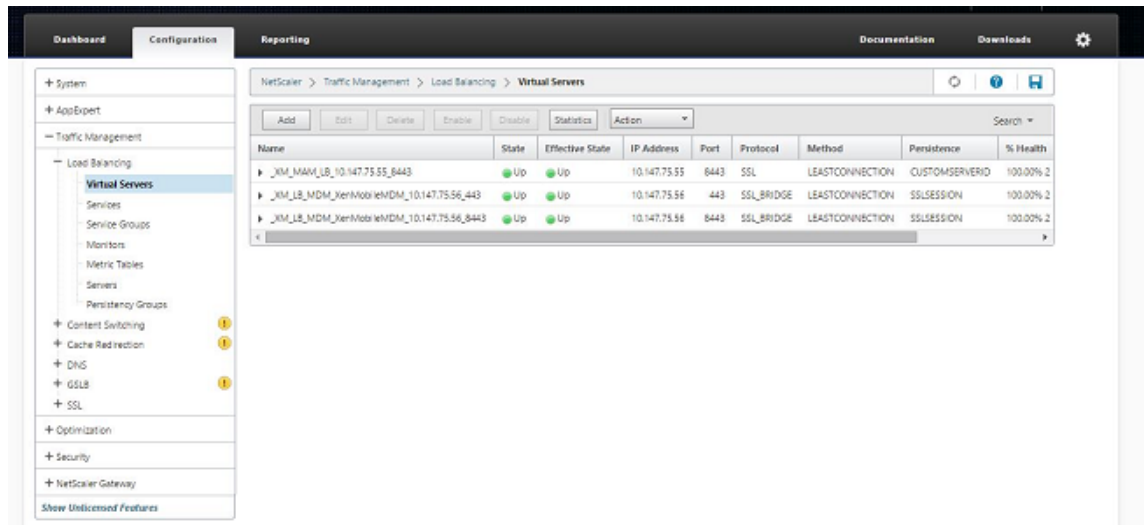
XenMobile Server Load Balancing

IP Address	Port	Status
10.147.75.56	443	Up
10.147.75.59	8443	Up

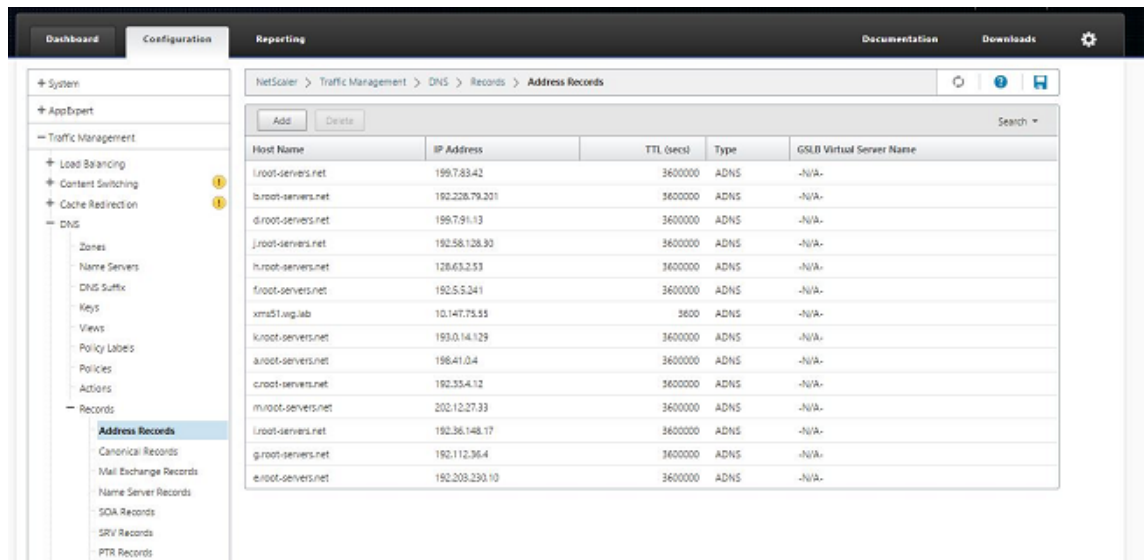
Microsoft Exchange Load Balancing with Email Security Filtering

Not Configured

16. 가상 IP 주소가 제대로 작동하는지 확인하기 위해 Configuration(구성) 탭을 클릭하고 **Traffic Management**(트래픽 관리) > **Load Balancing**(부하 분산) > **Virtual Servers**(가상 서버) 로 이동합니다.



Citrix ADC의 DNS 항목이 MAM 부하 분산 가상 IP 주소를 가리키는 것을 볼 수 있습니다.



재해 복구 가이드

January 5, 2022

재해 복구를 위해 활성/수동 장애 조치 (failover) 전략을 사용하여 여러 사이트가 포함된 XenMobile 배포를 설계하고 구성할 수 있습니다. 자세한 내용은 XenMobile 배포 안내서 [재해 복구](#) 문서를 참조하십시오.

프록시 서버 사용

January 5, 2022

아웃바운드 인터넷 트래픽을 제어하려면 XenMobile 에서 해당 트래픽을 처리할 프록시 서버를 설정하면 됩니다. 프록시 서버는 CLI(명령줄 인터페이스) 를 통해 설정합니다. 프록시 서버를 설정하려면 시스템을 다시 시작해야 합니다.

1. XenMobile CLI 메인 메뉴에서 **2** 를 입력하여 시스템 메뉴를 선택합니다.
2. 시스템 메뉴에서 **6** 을 입력하여 프록시 서버 메뉴를 선택합니다.

```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
Choice: [0 - 5] 2
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] Admin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----
```

3. 프록시 구성 메뉴에서 **1** 을 입력하여 SOCKS 를 선택합니다.

이 설정을 저장하기 전에 HTTPS 도 구성해야 합니다. 동일한 구성에서 SOCKS 및 HTTPS 설정을 저장하지 않으면 프록시가 작동하지 않습니다.

```
-----
Choice: [0 - 10] 6
-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
```

4. 프록시 서버 IP 주소, 포트 번호 및 대상을 입력합니다. 각 프록시 서버 유형에 대해 지원되는 대상 유형은 다음 표를 참조하십시오.

프록시 유형	지원되는 대상
SOCKS	APNS
HTTP	APNS, 웹, PKI
HTTPS	웹, PKI
인증을 사용하는 HTTP	웹, PKI
인증을 사용하는 HTTPS	웹, PKI


```

-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 1

Enter socks proxy information
Address [1]: 203.0.113.23
Port[1]: 1080
Target - APNS
Proxy configuration updated successfully.
Please restart all nodes in the cluster for the changes to take effect
Are you sure to restart the system? [y/n]: █

```

5. **n**을 입력하고 **2**를 입력하여 HTTPS를 선택한 다음 프록시 서버 IP 주소, 포트 번호 및 대상을 입력합니다.
6. 프록시 서버 인증에 사용할 사용자 이름과 암호를 구성하도록 선택하는 경우 **y**를 입력한 후 사용자 이름과 암호를 입력합니다.

```

[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 2

Enter https proxy information
Address [1]: 203.0.113.23
Port[1]: 4443
Configure username & password [y/n]: y
Username: Justaname
Password:
Target - WEB
WEB proxy configured. Override proxy settings?[y/n]: █

```

7. **y**를 입력하여 설정을 저장합니다.

SQL Server 구성

January 5, 2022

온-프레미스 XenMobile Server 에서 SQL Server 에 연결하는 경우 다음 드라이버 중 하나를 사용할 수 있습니다.

- 기본 드라이버
- jTDS
- Microsoft JDBC(Java Database Connectivity) 드라이버

다음의 경우 jTDS 드라이버가 기본 드라이버입니다.

- XenMobile Server 를 온-프레미스로 설치합니다.
- jTDS 드라이버를 사용하도록 구성된 XenMobile Server 에서 업그레이드합니다.

XenMobile 은 두 드라이버에 대해 SQL Server 인증 또는 Windows 인증을 지원합니다. 이러한 인증 및 드라이버 조합에 대해 SSL 을 켜거나 끌 수 있습니다.

Windows 인증과 함께 Microsoft JDBC 드라이버를 사용하는 경우 드라이버에 Kerberos 통합 인증이 사용됩니다. XenMobile 은 Kerberos 에 접속하여 Kerberos KDC(키 배포 센터) 세부 정보를 가져옵니다. 필요한 세부 정보가 제공되지 않는 경우 XenMobile CLI 에 Active Directory 서버의 IP 주소를 입력하라는 메시지가 표시됩니다.

jTDS 드라이버를 JDBC 드라이버로 전환하려면 모든 XenMobile Server 노드에 SSH 로 연결한 후 XenMobile CLI 를 사용하여 구성합니다. 단계는 다음과 같이 현재 jTDS 드라이버 구성에 따라 다릅니다.

Microsoft JDBC 로 전환 (SQL Server 인증)

이러한 단계를 완료하려면 SQL Server 사용자 이름과 암호가 필요합니다.

1. 모든 XenMobile Server 노드에 SSH 로 연결합니다.
2. XenMobile CLI 메인 메뉴에서 **2** 를 입력하여 시스템 메뉴를 선택합니다.
3. **12** 를 입력하여 고급 설정을 선택합니다.
4. **7** 을 입력하여 JDBC 드라이버 전환을 선택한 후 **m** 을 입력하여 Microsoft 를 선택합니다.

```
[12] Advanced Settings
-----
Choice: [0 - 12] 12

***** WARNING *****
Please only modify these options if you are
in contact with Citrix Support
*****

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
[7] Switch JDBC driver
-----
Choice: [0 - 7] 7
JDBC driver type (JTDS or Microsoft) []:
```

5. 메시지가 표시되면 **y** 를 입력하여 SQL 인증을 선택하고 SQL Server 사용자 이름과 암호를 입력합니다.
6. 각 XenMobile Server 노드에 대해 단계를 반복합니다.
7. 각 XenMobile Server 노드를 다시 시작합니다.

Microsoft JDBC 로 전환 (SSL 꺼짐, Windows 인증)

이러한 단계를 완료하려면 Active Directory 사용자 이름 및 암호 Kerberos KDC 영역 및 KDC 사용자 이름이 필요합니다.

1. 모든 XenMobile Server 노드에 SSH 로 연결합니다.
2. XenMobile CLI 메인 메뉴에서 **2** 를 입력하여 시스템 메뉴를 선택합니다.
3. **12** 를 입력하여 고급 설정을 선택합니다.
4. **7** 을 입력하여 JDBC 드라이버 전환을 선택한 후 **m** 을 입력합니다.
5. SQL Server 인증의 사용 여부를 묻는 메시지가 표시되면 **n** 을 입력합니다.
6. 메시지가 표시되면 SQL Server 에 구성된 Active Directory 사용자 이름과 암호를 입력합니다.
7. XenMobile 에서 Kerberos KDC 영역이 자동으로 검색되지 않으면 SQL Server FQDN 을 비롯한 KDC 세부 정보를 묻는 메시지가 표시됩니다.
8. SSL 사용 여부를 묻는 메시지가 표시되면 **n** 을 입력합니다. XenMobile 구성 XenMobile 에서 오류로 인해 구성이 저장되지 않으면 오류 메시지와 입력한 세부 정보가 표시됩니다.

9. 각 XenMobile Server 노드에 대해 단계를 반복합니다.
10. 각 XenMobile Server 노드를 다시 시작합니다.

XenMobile 데이터베이스 암호를 변경하려면

다음 지침에 따라 XenMobile 데이터베이스 암호를 변경합니다. 예를 들어 Citrix 지원에서 암호 변경을 요청하는 경우 암호를 변경해야 합니다.

SQL Server 에서 Windows 인증을 사용하는 경우 Windows Active Directory 에서 데이터베이스 암호를 변경해야 합니다. 그런 다음 데이터베이스 서버의 데이터베이스 관리자 계정을 새로 고쳐 암호 변경을 동기화합니다. 그러면 다음과 같이 XenMobile 에서 암호를 변경할 수 있습니다.

중요:

- XenMobile 의 데이터베이스 암호 변경을 위해 예약된 유지 관리 기간을 계획합니다. 암호는 시스템 중단 시간에 변경해야 합니다.
- 암호를 변경할 때는 모든 XenMobile 노드가 네트워크에 연결되어 있는지 확인하십시오. 암호를 변경한 후 XenMobile 을 다시 시작합니다.

If you don't restart XenMobile after a password change, XenMobile goes into recovery mode. In that case, revert to the old password in SQL server, restart XenMobile, and change the password again.

1. 모든 XenMobile Server 노드가 실행 중인지 확인합니다. 클러스터링된 환경의 경우 모든 노드를 가동합니다.
2. Citrix ADC 부하 분산 장치에서 가상 서버를 사용하지 않도록 설정하여 XenMobile 에 대한 수신 장치 트래픽을 차단합니다.
3. SQL Server 에서 데이터베이스 암호를 변경하려면: XenMobile CLI 에 로그인하고 **Configuration > Database** 로 이동한 다음 메시지가 표시되면 변경된 암호를 입력합니다.

```
1 Server []: <ipAddress>
2 Port [1433]: 1433
3 Username [sa]: <userName>
4 Password: <*****>
5 <!--NeedCopy-->
```

4. **Y** 를 입력하여 서버를 다시 시작합니다.
5. 클러스터의 다른 모든 노드에 대해 3 단계와 4 단계를 반복합니다.
6. Citrix ADC 부하 분산 장치에서 가상 서버를 사용하도록 설정하여 수신 장치 트래픽의 차단을 해제합니다.

서버 속성

November 27, 2023

XenMobile에는 서버 전체 작업에 적용되는 다수의 속성이 있습니다. 이 문서에서는 여러 서버 속성을 설명하고 서버 속성을 추가, 편집 또는 삭제하는 방법을 자세히 설명합니다.

일부 속성은 사용자 지정 키입니다. 사용자 지정 키를 추가하려면 추가를 클릭한 다음 키에서 사용자 지정 키를 선택합니다.

일반적으로 구성되는 속성에 대한 자세한 내용은 XenMobile 가상 안내서에서 [서버 속성](#)을 참조하십시오.

서버 속성 정의

Add Device Always(항상 장치 추가)

- **true** 인 경우 XenMobile이 등록에 실패한 장치도 XenMobile 콘솔에 추가합니다. 따라서 등록을 시도한 장치를 볼 수 있습니다. 기본값은 **false**입니다.

AG Client Cert Issuing Throttling Interval(AG 클라이언트 인증서 발급 제한 간격)

- 인증서 생성 사이의 유예 기간입니다. 이 간격은 XenMobile이 짧은 기간에 장치용 인증서를 여러 개 생성하는 것을 방지합니다. 이 값은 변경하지 않는 것이 좋습니다. 기본값은 **30** 분입니다.

Audit Log Cleanup Execution Time(감사 로그 정리 실행 시간)

- 감사 로그 정리를 시작하는 시간이며 HH:MM AM/PM 형식을 사용합니다. 예: 04:00 AM. 기본값은 **02:00 AM**입니다.

Audit Log Cleanup Interval (in Days)(감사 로그 정리 간격 (일))

- XenMobile에 감사 로그가 유지되는 일 수입니다. 기본값은 **1**입니다.

Audit Logger(감사 로거)

- **False**인 경우 UI(사용자 인터페이스) 이벤트를 기록하지 않습니다. 기본값은 **False**입니다.

Audit Log Retention (in Days)(감사 로그 유지 (일))

- XenMobile에 감사 로그가 유지되는 일 수입니다. 기본값은 **7**입니다.

auth.ldap.connect.timeout and auth.ldap.read.timeout

- 느린 LDAP 응답을 보완하려면 다음 사용자 지정 키의 서버 속성을 추가하는 것이 좋습니다.
 - 키: 사용자 지정 키
 - 키: **auth.ldap.connect.timeout**
 - 값: **60000**
 - 표시 이름: **auth.ldap.connect.timeout**
 - 설명: **LDAP** 연결 시간 초과
 - 키: 사용자 지정 키
 - 키: **auth.ldap.read.timeout**
 - 값: **60000**
 - 표시 이름: **auth.ldap.read.timeout**
 - 설명: **LDAP** 읽기 시간 제한

인증서 갱신 (초)

- XenMobile 이 인증서 갱신을 시작하는 인증서가 만료되기 전의 시간 (초) 입니다. 예를 들어 인증서가 12 월 30 일에 만료될 예정이고 이 속성이 30 일로 설정된 경우 장치가 12 월 1 일에서 12 월 30 일 사이에 연결하면 XenMobile 이 인증서 갱신을 시작합니다. 기본값은 **2592000** 초 (30 일) 입니다.

연결 시간 제한

- XenMobile 이 장치에 대한 TCP 연결을 종료하기 전까지의 세션 비활성 시간 제한 (분) 입니다. 세션은 열린 상태로 유지됩니다. Android 장치 및 원격 지원에 적용됩니다. 기본값은 **5** 분입니다.

Microsoft 인증 서버에 대한 연결 시간 제한

- XenMobile 이 인증서 서버의 응답을 대기하는 시간 (초) 입니다. 인증서 서버가 느리고 트래픽이 많은 경우 이 값을 60 초 이상으로 늘립니다. 120 초 후에 응답하지 않는 인증서 서버는 유지 관리가 필요합니다. 기본값은 **15000** 밀리초 (15 초) 입니다.

기본 배포 채널

- XenMobile 이 리소스를 장치에 배포하는 방법을 사용자 수준 (**DEFAULT_TO_USER**) 또는 장치 수준에서 결정합니다. 기본값은 **DEFAULT_TO_DEVICE** 입니다.

Deploy Log Cleanup (in Days)(배포 로그 정리 (일))

- XenMobile 에 배포 로그가 유지되는 일 수입니다. 기본값은 **7** 입니다.

호스트 이름 확인 사용 안 함

- 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다. 호스트 이름 유효성 검사가 실패하면 서버 로그에 다음과 같은 오류가 포함됩니다. “볼륨 구매 서버에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’ 은 피어가 제공한 인증서 주체와 일치하지 않습니다.” 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 이 속성을 **true** 로 변경하십시오. 기본값은 **false** 입니다.

SSL 서버 확인 사용 안 함

- **True** 인 경우 다음 모든 조건이 충족되면 SSL 서버 인증서 유효성 검사가 사용되지 않습니다.
 - XenMobile Server 에서 인증서 기반 인증을 사용합니다.
 - Microsoft CA 서버가 인증서 발급자입니다.
 - XenMobile Server 가 루트를 신뢰하지 않는 내부 CA 에서 인증서를 서명했습니다.

기본값은 **true** 입니다.

Enable Console(콘솔 사용)

- **true** 인 경우 사용자가 자가 지원 포털 콘솔에 액세스할 수 있습니다. 기본값은 **true** 입니다.

Enable Crash Reporting(크래시 보고 사용)

- **true** 인 경우 Citrix 는 iOS 및 Android 용 Secure Hub 의 문제를 해결하는 데 도움이 되는 충돌 보고서 및 진단을 수집합니다. **false** 인 경우 데이터가 수집되지 않습니다. 기본값은 **true** 입니다.

Enable/Disable Hibernate statistics logging for diagnostics(진단에 Hibernate 통계 로깅 사용/사용 안 함)

- **True** 인 경우 Hibernate 통계 로깅을 사용하여 응용 프로그램 성능 문제 해결을 지원합니다. Hibernate 는 XenMobile 에서 Microsoft SQL Server 에 연결할 때 사용되는 구성 요소입니다. 기본적으로 로깅은 응용 프로그램 성능에 영향을 미치므로 사용하지 않도록 설정됩니다. 매우 큰 로그 파일이 만들어지는 것을 방지하려면 짧은 기간 동안만 로깅을 사용하십시오. XenMobile 은 /opt/sas/logs/hibernate_stats.log 에 로그를 기록합니다. 기본값은 **False** 입니다.

Enable macOS OTAE(macOS OTAE 사용)

- **false** 인 경우 macOS 장치에 대한 등록 링크의 사용을 차단합니다. 즉, macOS 사용자는 등록 초대를 통해서만 등록할 수 있습니다. 기본값은 **true** 입니다.

Enable Notification Trigger(알림 트리거 사용)

- Secure Hub 클라이언트 알림을 사용하거나 사용하지 않도록 설정합니다. **true** 값은 알림을 사용합니다. 기본값은 **true** 입니다.

force.server.push.required.apps

- 다음과 같은 경우에 Android 및 iOS 장치에서 필수 앱의 강제 배포를 사용하도록 설정합니다.
 - 사용자가 새 앱을 업로드하고 필수 앱으로 표시합니다.
 - 사용자가 기존 앱을 필수 앱으로 표시합니다.
 - 사용자가 필수 앱을 삭제합니다.
 - Secure Hub 업데이트가 제공됩니다.

필수 앱의 강제 배포는 기본적으로 **false** 로 설정됩니다. 강제 배포를 사용하도록 설정하려면 사용자 지정 키를 만들고 값을 **true** 로 설정하십시오. 강제 배포 중에는 엔터프라이즈 앱 및 공용 앱 스토어 앱을 포함한 MDX 지원 필수 앱이 즉시 업그레이드됩니다. 관리자가 앱 업데이트 유예 기간에 대한 MDX 정책을 구성하고 사용자가 앱을 나중에 업그레이드하도록 선택하는 경우에도 업그레이드가 수행됩니다.

- 키: 사용자 지정 키
- 키: **force.server.push.required.apps**
- 값: **false**
- 표시 이름: **force.server.push.required.apps**
- 설명: 필수 앱을 강제로 배포

ActiveSync 가 허용 및 거부된 사용자 전체 목록 끌어오기

- XenMobile 이 ActiveSync 가 허용 및 거부한 사용자의 전체 목록 (기준) 을 가져오는 간격 (초) 입니다. 기본값은 **28800** 초입니다.

hibernate.c3p0.idle_test_period

- XenMobile Server 속성인 사용자 지정 키는 연결 유효성이 자동으로 검사되기까지의 유효 시간 (초) 을 결정합니다. 다음과 같이 키를 구성합니다. 기본값은 **30** 입니다.
- 키: 사용자 지정 키

- 키: **hibernate.c3p0.idle_test_period**
- 값: **30**
- 표시 이름: **hibernate.c3p0.idle_test_period=nnn**
- 설명: **Hibernate** 유휴 테스트 기간

hibernate.c3p0.max_size

- 이 사용자 지정 키는 XenMobile 에서 SQL Server 데이터베이스에 대해 열 수 있는 최대 연결 수를 결정합니다. XenMobile 은 이 사용자 지정 키에 지정한 값을 상한으로 사용합니다. 필요한 경우에만 연결이 열립니다. 데이터베이스 서버의 용량에 따라 설정을 결정합니다. 자세한 내용은 [XenMobile 작업 조정](#)을 참조하십시오. 다음과 같이 키를 구성합니다. 기본값은 **1000** 입니다.
- 키: **hibernate.c3p0.max_size**
- 값: **1000**
- 표시 이름: **hibernate.c3p0.max_size**
- 설명: **SQL** 에 대한 **DB** 연결

hibernate.c3p0.min_size

- 이 사용자 지정 키는 XenMobile 에서 SQL Server 데이터베이스에 대해 여는 최소 연결 수를 결정합니다. 다음과 같이 키를 구성합니다. 기본값은 **100** 입니다.
- 키: **hibernate.c3p0.min_size**
- 값: **100**
- 표시 이름: **hibernate.c3p0.min_size**
- 설명: **SQL** 에 대한 **DB** 연결

hibernate.c3p0.timeout

- 이 사용자 지정 키는 유휴 시간 초과 (초) 를 결정합니다. 기본값은 **120** 입니다.
- 키: 사용자 지정 키
- 키: **hibernate.c3p0.timeout**
- 값: **120**
- 표시 이름: **hibernate.c3p0.timeout**
- 설명: 데이터베이스 유휴 시간 초과

원격 분석의 사용 여부를 식별합니다

- 원격 분석 (사용자 환경 개선 프로그램 또는 CEIP) 이 사용되는지 여부를 식별합니다. XenMobile 을 설치하거나 업그레이드할 때 CEIP 에 참여할 수 있습니다. XenMobile 서 15 번 연속으로 업로드에 실패할 경우 원격 분석이 사용되지 않습니다. 기본값은 **false** 입니다.

Inactivity Timeout in Minutes(비활성 시간 제한 (분))

- 웹 서비스 시간 제한 유형 서버 속성이 **INACTIVITY_TIMEOUT** 인 경우: 이 속성은 XenMobile 이 다음을 수행한 비활성 관리자를 로그아웃하기 전까지의 시간 (분) 을 정의합니다.
 - REST 서비스에 대한 XenMobile 공용 API 를 사용한 XenMobile 콘솔 액세스
 - REST 서비스에 대한 XenMobile 공용 API 를 사용하여 타사 앱에 액세스. 시간 제한이 **0** 인 경우 비활성 사용자가 로그인한 상태로 유지됩니다.

기본값은 **5** 입니다.

iOS Device Management Enrollment Auto-Install Enabled(iOS 장치 관리 등록 자동 설치 사용)

- true 인 경우 이 속성은 장치 등록 시 필요한 사용자 상호 작용의 수를 줄입니다. 사용자는 **Root CA install(루트 CA 설치)**(필요한 경우) 및 **MDM Profile install(MDM 프로필 설치)** 을 클릭해야 합니다.

iOS Device Management Enrollment First Step Delayed(iOS 장치 관리 등록의 첫 번째 단계 지연)

- 장치 등록 시 사용자가 자격 증명을 입력한 후 루트 CA 에 대한 메시지에 응답하기까지 대기해야 하는 시간을 지정합니다. 이 속성은 네트워크 대기 시간 또는 속도 문제가 있는 경우에만 편집하는 것이 좋습니다. 이 경우 5000 밀리초 (5 초) 를 초과하는 값을 설정하지 마십시오. 기본값은 **1000** 밀리초 (1 초) 입니다.

iOS Device Management Enrollment First Step Delayed(iOS 장치 관리 등록의 마지막 단계 지연)

- 이 속성 값은 장치 등록 중에 MDM 프로필이 설치된 후 장치의 에이전트가 시작되기까지 대기해야 하는 시간을 지정합니다. 이 속성은 네트워크 대기 시간 또는 속도 문제가 있는 경우에만 편집하는 것이 좋습니다. 이 경우 5000 밀리초 (5 초) 를 초과하는 값을 설정하지 마십시오. 기본값은 **1000** 밀리초 (1 초) 입니다.

iOS Device Management Identity Delivery Mode(iOS 장치 관리 ID 배달 모드)

- XenMobile 이 장치에 MDM 인증서를 배포할 때 **SCEP**(보안상의 이유로 권장됨) 또는 **PKCS12** 를 사용할지 여부를 지정합니다. PKCS12 모드에서는 서버에 키 쌍이 생성되고 협상이 수행되지 않습니다. 기본값은 **SCEP** 입니다.

iOS Device Management Identity Key Size(iOS 장치 관리 ID 키 크기)

- MDM ID, iOS 프로필 서비스 및 XenMobile iOS 에이전트 ID 에 대한 개인 키의 크기를 정의합니다. 기본값은 **1024** 입니다.

iOS Device Management Identity Renewal Days(iOS 장치 관리 ID 갱신 일 수)

- XenMobile 이 인증서 갱신을 시작하는 인증서가 만료되기 전의 시간 (일) 을 지정합니다. 예를 들어 인증서가 10 일 후에 만료되고 이 속성이 **10** 일인 경우 장치가 만료 9 일 전에 연결하면 XenMobile 이 새 인증서를 발급합니다. 기본값은 **30** 일입니다.

iOS MDM APNS Private Key Password(iOS MDM APNS 개인 키 암호)

- 이 속성에는 XenMobile 에서 Apple 서버로 알림을 푸시할 때 필요한 APNs 암호가 포함됩니다.

Length of Inactivity Before Device Is Disconnected(장치 연결을 해제하기 전 비활성 시간)

- XenMobile 이 연결을 해제하기 전에 장치가 마지막 인증부터 비활성 상태로 있을 수 있는 시간을 지정합니다. 기본값은 **7** 일입니다.

MAM Only Device Max

- 이 사용자 지정 키는 각 사용자가 등록할 수 있는 MAM 전용 장치의 수를 제한합니다. 다음과 같이 키를 구성합니다. 값이 **0** 이면 장치를 무제한 등록할 수 있습니다.
- 키 = **number.of.mam.devices.per.user**
- 값 = **5**
- 표시 이름 = **MAM Only Device Max**
- 설명 = 각 사용자가 등록할 수 있는 **MAM** 장치 수를 제한합니다.

MaxNumberOfWorker

- 많은 수의 볼륨 구매 라이선스를 가져올 때 사용되는 스레드 수입니다. 기본값은 **3** 입니다. 추가 최적화가 필요한 경우 스레드 수를 늘릴 수 있습니다. 그러나 예를 들어 6 과 같이 스레드 수가 커지면 볼륨 구매를 가져올 때 CPU 사용량이 높아 집니다.

Citrix ADC Single Sign-On

- **False** 인 경우 Citrix ADC 에서 XenMobile 로의 SSO 중에 XenMobile 콜백 기능이 사용되지 않습니다. Citrix Gateway 구성에 콜백 URL 이 포함되는 경우 XenMobile 이 콜백 기능을 사용하여 Citrix Gateway 세션 ID 를 확인합니다. 기본값은 **False** 입니다.

Number of consecutive failed uploads(연속 업로드 실패 수)

- CEIP(사용자 환경 개선 프로그램) 업로드 중에 연속적으로 실패한 횟수를 표시합니다. 업로드가 실패하면 값이 증가합니다. 업로드가 15 회 실패하면 XenMobile 이 원격 분석이라고도 하는 CEIP 를 사용하지 않도록 설정합니다. 자세한 내용은 원격 분석의 사용 여부를 식별합니다 서버 속성을 참조하십시오. 업로드가 성공하면 값이 **0** 으로 재설정됩니다.

Number of Users Per Device(장치당 사용자 수)

- 동일한 장치를 MDM 에 등록할 수 있는 사용자의 최대 수입니다. **0** 값은 무제한의 사용자가 동일한 장치를 등록할 수 있음을 의미합니다. 기본값은 **0** 입니다.

Pull of Incremental Change of Allowed and Denied Users(허용 및 거부된 사용자의 증분 변경 끌어오기)

- XenMobile 이 PowerShell 명령을 실행하여 ActiveSync 장치의 델타를 가져올 때 도메인의 응답을 대기하는 시간 (초) 입니다. 기본값은 **60** 초입니다.

Read Timeout to Microsoft Certification Server(Microsoft 인증 서버에 대한 읽기 시간 제한)

- XenMobile 이 읽기를 수행할 때 인증서 서버의 응답을 대기하는 시간 (초) 입니다. 인증서 서버가 느리고 트래픽이 많은 경우 이 값을 60 초 이상으로 늘릴 수 있습니다. 120 초 후에 응답하지 않는 인증서 서버는 유지 관리가 필요합니다. 기본값은 **15000** 밀리초 (15 초) 입니다.

REST Web Services(REST 웹 서비스)

- REST 웹 서비스를 사용합니다. 기본값은 **true** 입니다.

지정된 크기의 청크로 장치 정보를 검색합니다

- 이 값은 장치 내보내기 중 내부적으로 다중 스레드 처리에 사용됩니다. 값이 클수록 단일 스레드가 더 많은 장치를 구문 분석합니다. 값이 작을수록 더 많은 스레드가 장치를 가져옵니다. 값을 줄이면 내보내기 및 장치 목록 가져오기 성능이 향상되지만 사용 가능한 메모리가 줄어들 수 있습니다. 기본값은 **1000** 입니다.

Session Log Cleanup (in Days)(세션 로그 정리 (일))

- XenMobile 에 세션 로그가 유지되는 일 수입니다. 기본값은 **7** 입니다.

Server Mode(서버 모드)

- XenMobile 이 앱 관리, 장치 관리 또는 앱 및 장치 관리에 해당하는 MAM, MDM 또는 ENT(엔터프라이즈) 모드에서 실행되는지 확인합니다. Server Mode(서버 모드) 속성은 아래 표에 설명된 것과 같이 장치 등록 방법에 따라 설정합니다. 서버 모드의 기본값은 라이선스 유형에 관계없이 **ENT** 입니다.

XenMobile MDM Edition 라이선스가 있는 경우 유효한 서버 모드는 서버 속성에서 설정한 서버 모드와 관계없이 항상 MDM 입니다. MDM Edition 라이선스가 있는 경우 서버 모드를 MAM 또는 ENT 로 설정하여 앱 관리를 사용할 수 없습니다.

라이선스 버전	장치 등록에 사용할 모드	Server Mode(서버 모드) 속성을 다음으로 설정
Enterprise/Advanced	MDM 모드	MDM
Enterprise/Advanced	MDM+MAM 모드	ENT
MDM	MDM 모드	MDM

유효한 서버 모드는 라이선스 유형과 서버 모드의 조합입니다. MDM 라이선스에 유효한 서버 모드는 서버 모드 설정과 관계없이 항상 MDM 입니다. Enterprise 및 Advanced 라이선스의 경우 유효한 서버 모드는 서버 모드가 **ENT** 또는 **MDM** 인 경우 서버 모드와 일치합니다. 서버 모드가 **MAM** 인 경우 유효한 서버 모드는 ENT 입니다.

XenMobile 은 라이선스 활성화, 라이선스 삭제 및 서버 속성에서 서버 모드 변경 작업에 대한 서버 로그에 서버 모드를 추가합니다. 로그 파일 만들기 및 보기에 대한 자세한 내용은 [로그](#)와 [XenMobile 의 로그 파일 보기 및 분석](#)을 참조하십시오.

ShareFile configuration type(ShareFile 구성 유형)

- Citrix Files 스토리지 유형을 지정합니다. **ENTERPRISE** 는 Citrix Files Enterprise 모드를 사용합니다. **CONNECTORS** 는 XenMobile 콘솔을 통해 만든 StorageZone 커넥터에 대한 액세스만 제공합니다. 기본값은 **NONE** 이며 구성 > **ShareFile** 화면의 초기 보기에서 Citrix Files Enterprise 와 커넥터 중에서 선택할 수 있습니다. 기본값은 **NONE** 입니다.

Static Timeout in Minutes(정적 시간 제한 (분))

- 웹 서비스 시간 제한 유형 서버 속성이 **STATIC_TIMEOUT** 인 경우: 이 속성은 XenMobile 이 다음을 사용한 후 관리자를 로그아웃하기 전의 시간 (분) 을 정의합니다.

- REST 서비스에 대한 XenMobile 공용 API 를 사용하여 XenMobile 콘솔에 액세스
- REST 서비스에 대한 XenMobile 공용 API 를 사용하여 타사 앱에 액세스.

기본값은 **60** 입니다.

Trigger Agent Message Suppression(에이전트 메시지 트리거 억제)

- Secure Hub 클라이언트 메시지를 사용하거나 사용하지 않도록 설정합니다. **false** 값은 메시지를 사용합니다. 기본값은 **true** 입니다.

Trigger Agent Sound Suppression(에이전트 사운드 트리거 억제)

- Secure Hub 클라이언트 사운드를 사용하거나 사용하지 않도록 설정합니다. **false** 값은 사운드를 사용합니다. 기본값은 **true** 입니다.

Unauthenticated App Download for Android Devices(Android 장치에 대한 인증되지 않은 앱 다운로드)

- **True** 인 경우 자체 호스팅된 앱을 Android Enterprise 를 실행하는 Android 장치에 다운로드할 수 있습니다. 이 속성은 Google Play Store 의 다운로드 URL 을 정적으로 제공하는 Android Enterprise 옵션이 사용되는 경우 필요합니다. 이 경우 다운로드 URL 에는 인증 토큰이 있는 일회용 티켓 (**XAM One-Time Ticket server(XAM 일회용 티켓 서버)** 속성으로 정의됨) 이 포함될 수 없습니다. 기본값은 **False** 입니다.

Unauthenticated App Download for Windows Devices(Windows 장치에 대한 인증되지 않은 앱 다운로드)

- 일회용 티켓의 유효성을 검사하지 않는 이전 버전의 Secure Hub 에만 사용됩니다. **False** 인 경우 XenMobile 에서 인증되지 않은 앱을 Windows 장치에 다운로드할 수 있습니다. 기본값은 **False** 입니다.

Use ActiveSync ID to Conduct an ActiveSync Wipe Device(ActiveSync ID 를 사용하여 ActiveSync 장치 초기화 수행)

- **true** 인 경우 Exchange ActiveSync 용 Endpoint Management 커넥터가 ActiveSync 식별자를 asWipeDevice 메서드의 인수로 사용합니다. 기본값은 **false** 입니다.

Exchange 의 사용자만

- **true** 인 경우 ActiveSync Exchange 사용자에게 대한 사용자 인증을 사용하지 않습니다. 기본값은 **false** 입니다.

VP 기준 간격

- XenMobile 이 Apple 에서 볼륨 구매 라이선스를 다시 가져오는 최소 간격입니다. 라이선스 정보를 새로 고치면 볼륨 구매에서 가져온 앱을 수동으로 삭제하는 것과 같은 모든 변경 내용을 XenMobile 에 반영할 수 있습니다. 기본적으로 XenMobile 에서 볼륨 구매 라이선스 기준은 최소 **720** 분마다 새로 고쳐집니다.

설치된 볼륨 구매 라이선스가 많은 경우 (예: 50,000 개 초과) Citrix 에서는 라이선스 가져오기의 빈도 및 오버헤드가 줄도록 값을 늘릴 것을 권장합니다. Apple 에서 볼륨 구매 라이선스가 자주 변경될 것으로 예상되는 경우 Citrix 에서는 XenMobile 에 변경 내용이 업데이트되도록 값을 낮출 것을 권장합니다. 두 기준 사이의 최소 간격은 60 분입니다. 또한 XenMobile 은 60 분마다 델타 가져오기를 수행하여 마지막 가져오기 이후의 변경 내용을 캡처합니다. 그러므로 볼륨 구매 기준 간격이 60 분인 경우 기준 사이의 간격이 최대 119 분까지 지연될 수 있습니다.

웹 서비스 시간 제한 유형

- 공용 API 에서 검색되는 인증 토큰의 만료 방법을 지정합니다. **STATIC_TIMEOUT** 인 경우 정적 시간 제한 (분) 서버 속성에 지정된 값이 지나면 인증 토큰이 만료된 것으로 간주합니다.

INACTIVITY_TIMEOUT 인 경우 비활성 시간 제한 (분) 서버 속성에 지정된 값 동안 비활성 상태이면 인증 토큰이 만료된 것으로 간주합니다. 기본값은 **STATIC_TIMEOUT** 입니다.

Windows WNS 채널 - 갱신 전 일 수

- ChannelURI 의 갱신 빈도입니다. 기본값은 **10** 일입니다.

Windows WNS 하트비트 간격

- XenMobile 이 3 분마다 5 번 장치에 연결한 후 장치에 연결하기 전까지 기다릴 시간입니다. 기본값은 **6** 시간입니다.

XAM 일회용 티켓

- OTT(일회용 인증 토큰) 로 앱을 다운로드할 수 있는 시간 (밀리초) 입니다. 이 속성은 **Android** 장치의 인증되지 않은 앱 다운로드 및 **Windows** 장치의 인증되지 않은 앱 다운로드 속성과 함께 사용됩니다. 이러한 속성은 인증되지 않은 앱 다운로드를 허용할지 여부를 지정합니다. 기본값은 **3600000** 입니다.

XenMobile MDM Self-Help Portal console max inactive interval (minutes)(XenMobile MDM 자가 지원 포털 콘솔 최대 비활성 간격 (분))

- XenMobile 자가 지원 포털에서 비활성 사용자가 로그아웃되기까지의 시간 (분) 입니다. 시간 제한이 **0** 인 경우 비활성 사용자가 로그인 상태로 유지됩니다. 기본값은 **30** 입니다.

서버 속성 추가, 편집 또는 삭제

XenMobile 에서 서버에 속성을 적용할 수 있습니다. 변경한 후에는 모든 노드에서 XenMobile 을 다시 시작하여 변경 내용을 커밋하고 활성화해야 합니다.


참고:

XenMobile 을 다시 시작하려면 하이퍼바이저를 통해 명령 프롬프트를 사용합니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 서버 속성을 클릭합니다. 서버 속성 페이지가 나타납니다. 이 페이지에서 서버 속성을 추가, 편집 또는 삭제할 수 있습니다.

Settings > [Server Properties](#)

Server Properties
You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

 Add

<input type="checkbox"/>	Display name	Key	Value	Default value	Description
<input type="checkbox"/>	NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
<input type="checkbox"/>	Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
<input type="checkbox"/>	Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata.id, url	odata.metadata, id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
<input type="checkbox"/>	Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE
<input type="checkbox"/>	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
<input type="checkbox"/>	Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
<input type="checkbox"/>	Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
<input type="checkbox"/>	User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

Showing 1 - 10 of 111 items Showing 1 of 12

서버 속성을 추가하려면

1. 추가를 클릭합니다. 새 서버 속성 추가 페이지가 나타납니다.

2. 다음 설정을 구성합니다.

- 키: 목록에서 해당하는 키를 선택합니다. 키는 대/소문자를 구분합니다. 속성 값을 편집하기 전 또는 특수 키를 요청하려는 경우 Citrix 지원에 문의하십시오.
- 값: 선택한 키에 따른 값을 입력합니다.
- 표시 이름: 서버 속성 테이블에 표시되는 새 속성 값의 이름을 입력합니다.
- 설명: 필요한 경우 새 서버 속성의 설명을 입력합니다.

3. 저장을 클릭합니다.

서버 속성을 편집하려면

1. 서버 속성 테이블에서 편집할 서버 속성을 선택합니다.

서버 속성 옆의 확인란을 선택하면 서버 속성 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하여 목록 오른쪽의 옵션 메뉴를 엽니다.

2. 편집을 클릭합니다. 새 서버 속성 편집 페이지가 나타납니다.

Settings > Server Properties > Edit New Server Property

Edit New Server Property

Key

Value*

Display name*

Description

3. 다음 정보를 적절하게 변경합니다.

- 키: 이 필드는 변경할 수 없습니다.
- 값: 속성 값입니다.
- 표시 이름: 속성 이름입니다.
- 설명: 속성 설명입니다.

4. 저장을 클릭하여 변경 내용을 저장하거나 취소를 클릭하여 속성을 변경하지 않고 그대로 유지합니다.

서버 속성을 삭제하려면

1. 서버 속성 테이블에서 삭제할 서버 속성을 선택합니다.

각 속성 옆에 있는 확인란을 선택하여 삭제할 속성을 둘 이상 선택할 수 있습니다.

2. 삭제를 클릭합니다. 확인 대화 상자가 나타납니다. 삭제를 다시 클릭합니다.

명령줄 인터페이스 옵션

November 27, 2023

XenMobile Server 온-프레미스 설치의 경우 다음과 같은 방법으로 CLI 옵션에 액세스할 수 있습니다.

- **XenMobile** 을 설치한 하이퍼바이저에서는 하이퍼바이저에서 가져온 XenMobile 가상 컴퓨터를 선택하고 명령 프롬프트 보기를 시작한 다음 XenMobile 의 관리자 계정에 로그인합니다. 자세한 내용은 해당 하이퍼바이저의 설명서를 참조하십시오.
- **SSH** 를 사용하여 방화벽에서 **SSH** 를 사용하도록 설정한 경우 XenMobile 의 관리자 계정에 로그인합니다.

CLI 를 사용하여 다양한 구성 및 문제 해결 작업을 수행할 수 있습니다. 다음 그림은 CLI 의 최상위 메뉴를 보여줍니다.

```
-----
Main Menu
-----
[0] Configuration
[1] Clustering
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
```

구성 옵션

다음은 구성 메뉴의 샘플과 각 옵션에 표시되는 설정입니다.

```
-----
Configuration Menu
-----
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----
```

[1] 네트워크

```
Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: y
IP address [10.207.87.75]: 10.200.87.75
Netmask [255.255.254.0]: 255.255.254.0
Default gateway [10.207.86.1]: 10.200.86.1
Primary DNS server [10.207.86.50]: 10.200.86.50
Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]: █
```

[2] 방화벽

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
- comma separated list of hosts or networks
- e.g. 10.20.5.3, 10.20.6.0/24
- an empty value means no access restriction
- enter c as value to clear list

HTTP service
Port: 80
Enable access (y/n) [y]: y
Access white list []:

Management HTTPS service
Port: 4443
Enable access (y/n) [y]:
Access white list []:

SSH service
Port [22]:
Enable access (y/n) [y]:
Access white list []:

Management API (for initial staging) HTTPS service
Port [30001]:
Enable access (y/n) [n]:

Remote support tunnel
Port [8081]:
Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```

[3] 데이터베이스

```
Type: [mi]
Use SSL (y/n) [n]:
Server [10.207.86.64]:
Port [1433]:
Username [sa]:
Password:
Database name [RC]:

Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: █
```

[4] 수신기 포트

```

Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]: █

```

클러스터링 옵션

다음은 클러스터링 메뉴의 샘플과 각 옵션에 표시되는 설정입니다.

```

-----
Clustering Menu
-----
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----

```

[1] 클러스터 상태 표시

```

Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE

```

[2] 클러스터 활성화/비활성화

클러스터링을 사용하도록 선택할 경우 다음과 같은 메시지가 나타납니다.

To enable real-time communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings **for** restricted access.

클러스터링을 사용하지 않도록 선택할 경우 다음과 같은 메시지가 나타납니다.

You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.

[3] 클러스터 구성원 화이트 리스트

```
Current White List:
- comma separated list of hosts or networks
- e.g. 10.20.5.3, 10.20.6.0/24
- an empty value means no access restriction

Please enter hosts or networks to be white listed:
```

[4] SSL 오프로드 활성화 또는 비활성화

SSL 오프로딩을 사용할지 여부를 선택하면 다음과 같은 메시지가 나타납니다.

Enabling SSL offload opens port 80 **for** everyone. Please configure Access white list under Firewall settings **for** restricted access.

[5] Hazelcast 클러스터 표시

Hazelcast 클러스터를 표시하도록 선택하면 다음과 같은 옵션이 나타납니다.

Hazelcast Cluster Members:

[나열된 IP 주소]

참고:

구성된 노드가 클러스터의 일부가 아닌 경우 해당 노드를 다시 시작합니다.

시스템 옵션

System Menu에서는 시스템 수준 정보를 표시 또는 설정하거나, 서버를 다시 시작 또는 종료하거나, **Advanced Settings**에 액세스할 수 있습니다.

```
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----
```

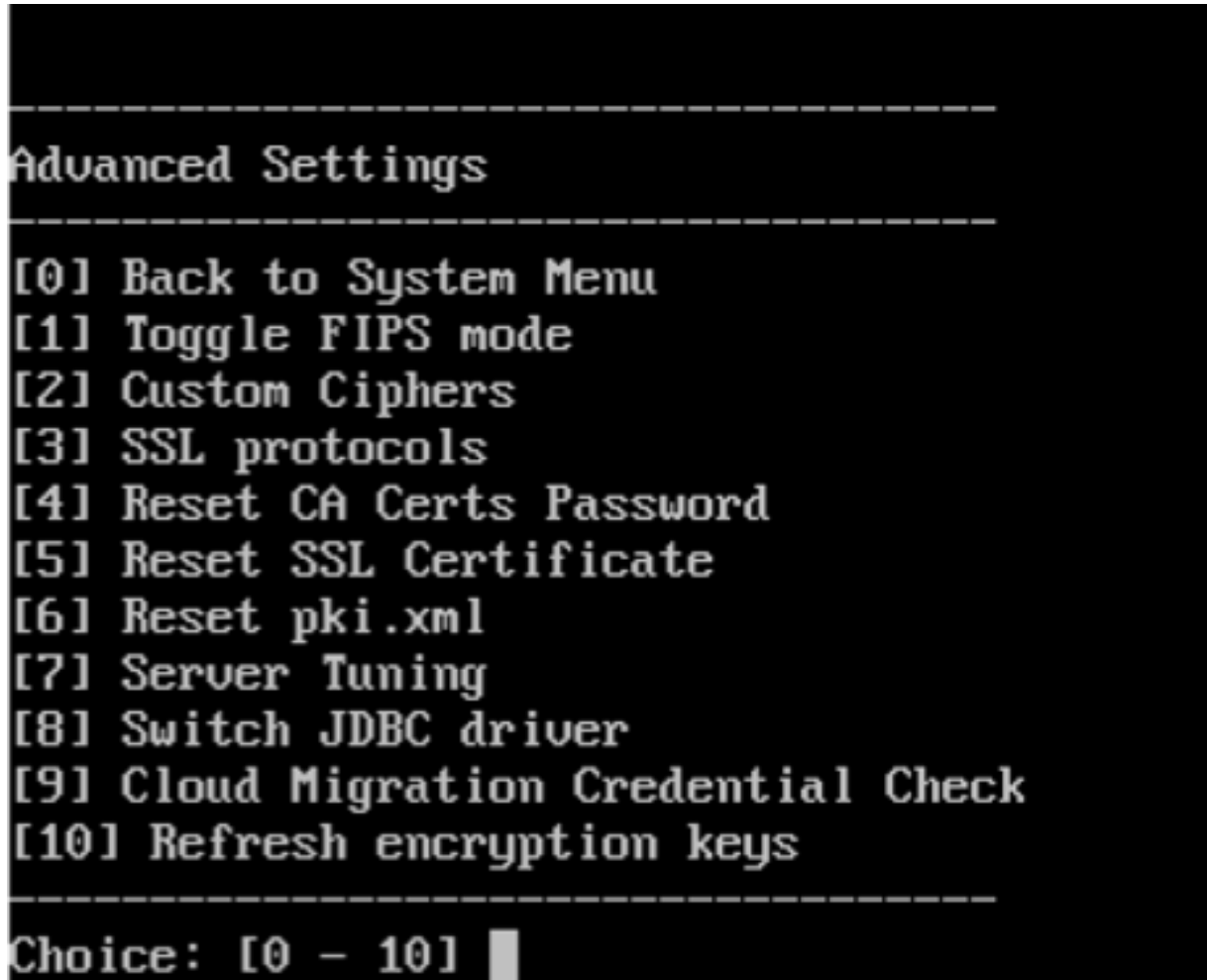
NTP 서버 설정을 통해 NTP 서버 정보를 지정할 수 있습니다. XenMobile 시간을 하이퍼바이저와 동기화할 때 표준 시간대 관련 문제가 나타나는 경우 XenMobile 이 NTP 서버를 가리키도록 하면 이 문제를 방지할 수 있습니다. 이 옵션을 변경한 후에 모든 클러스터 서버를 다시 시작합니다.

[5] 시스템 디스크 사용량 표시 메뉴 항목을 확인하여 디스크 공간을 확인할 수도 있습니다.

서버 노드 종료 정보

클러스터에서 단일 서버 노드를 종료하는 경우 일반적으로 [확장성 및 성능](#)에 설명된 요구 사항을 충족하는 다른 노드에서 작업 부하를 처리할 수 있습니다. 영향은 동시에 종료된 노드 수, 총 사용자 수 및 노드가 종료된 시간에 따라 다를 수 있습니다.

- 사용자는 여전히 Secure Hub 및 스토어에 액세스할 수 있습니다.
- 사용 가능한 노드에서 사용자 수를 처리할 수 있는 경우 사용자는 배포된 관리되는 앱에 액세스하고 이러한 앱을 시작할 수 있습니다. 연결이 느려져 장치 체크인 속도가 느려질 수 있습니다.
- 장치 정책은 모든 노드가 종료되지 않는 한 계속해서 작동합니다. 리소스와 장치 수에 따라 정책 배포 속도가 더 느려질 수 있습니다.

[12] 고급 설정

SSL protocols 옵션은 기본적으로 허용된 모든 프로토콜로 설정됩니다. **New SSL protocols to enable** 프롬프트가 표시되면 사용할 프로토콜을 입력합니다. XenMobile은 응답에 포함되지 않은 모든 프로토콜을 사용하지 않습니다. 예를 들어 TLSv1을 사용하지 않으려면 **TLSv1.2**, **TLSv1.1**을 입력한 다음 **y**를 입력하여 XenMobile Server를 다시 시작합니다.

Server Tuning 옵션에는 서버 연결 시간 초과, 최대 연결 수 (포트별) 및 최대 스레드 수 (포트별)가 포함됩니다.

Switch JDBC driver 옵션은 **jTDS**와 **Microsoft** JDBC입니다. 기본 드라이버는 jTDS입니다. Microsoft JDBC 드라이버 전환에 대한 자세한 내용은 [SQL Server 드라이버](#)를 참조하십시오.

문제 해결 옵션

다음은 **Troubleshooting Menu**의 샘플과 각 옵션에 대해 표시되는 설정입니다.


```
-----  
Troubleshooting Menu  
-----
```

```
[0] Back to Main Menu  
[1] Network Utilities  
[2] Logs  
[3] Support Bundle  
[4] Disk Usage  
-----
```

```
Choice: [0 - 4] 4
```

[1] 네트워크 유틸리티

```
-----  
Network Menu  
-----
```

```
[0] Back to Troubleshooting Menu  
[1] Network Information  
[2] Show Routing Table  
[3] Show Address Resolution Protocol (ARP) Table  
[4] PING  
[5] Traceroute  
[6] DNS Lookup  
[7] Network Trace  
-----
```

[2] 로그

```
-----  
Logs Menu  
-----
```

```
[0] Back to Troubleshooting Menu  
[1] Display debug log file  
[2] Display update log file
```

[3] 지원 번들

```
-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----
```

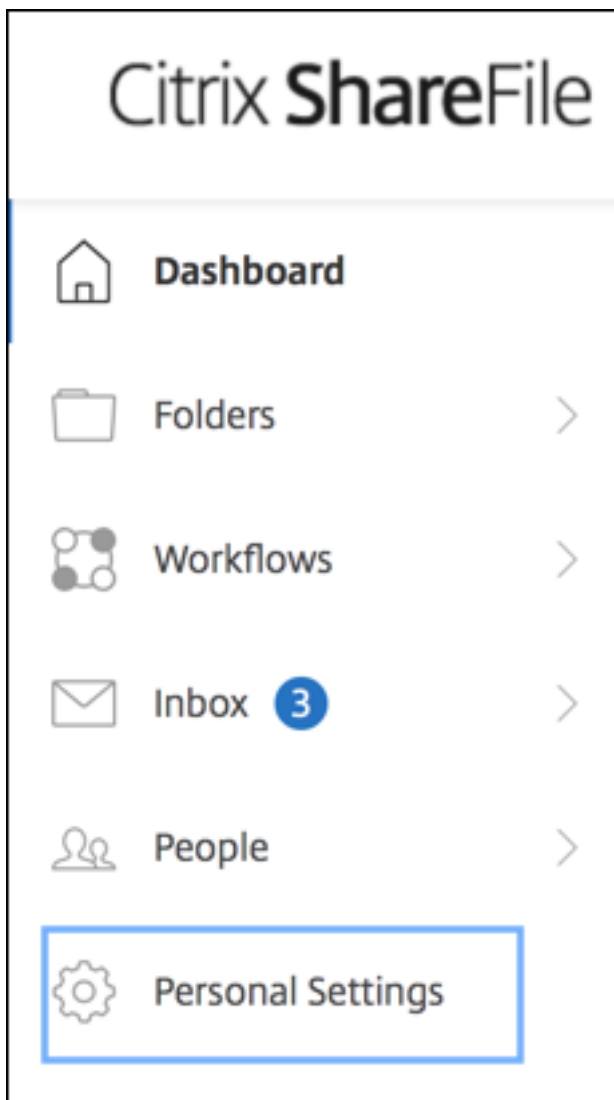
[4] 디스크 사용량

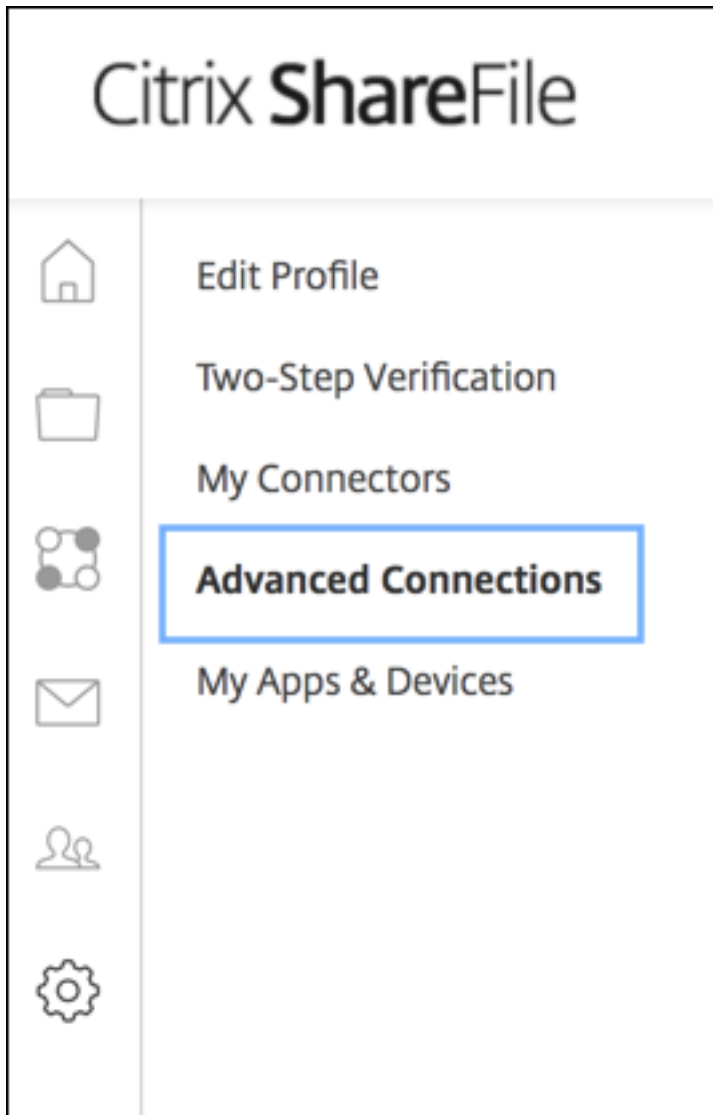
```
-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----
Choice: [0 - 4] 4
```

Citrix Files 를 **FTP** 사이트로 사용하여 지원 번들을 업로드하려면

지원 번들 업로드를 시작하기 전에 Citrix Files 에서 다음 필수 구성 요소를 구성합니다.

1. FTP 로그인 세부 정보를 확인합니다.
 - a. 웹 브라우저에서 <https://citrix.sharefile.com>을 엽니다.
 - b. **Personal Settings**(개인 설정) 를 클릭한 후 **Advanced connections**(고급 연결) 를 클릭합니다.





c. FTP 서버 정보에서 사용자 이름에 대한 영숫자 사용자 ID 가 기본 하위 도메인/사용자 이름 세부 정보와 함께 나타나는지 확인합니다.

You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the / and @ characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

[Detailed Set-up Instructions](#)

FTP Server Information

Security: Standard (Port 21) or Implicit SSL/TLS (Port 990)

FTP Server: citrite.sharefileftp.com

User name: [redacted].com or [redacted]

Password: (your ShareFile password)

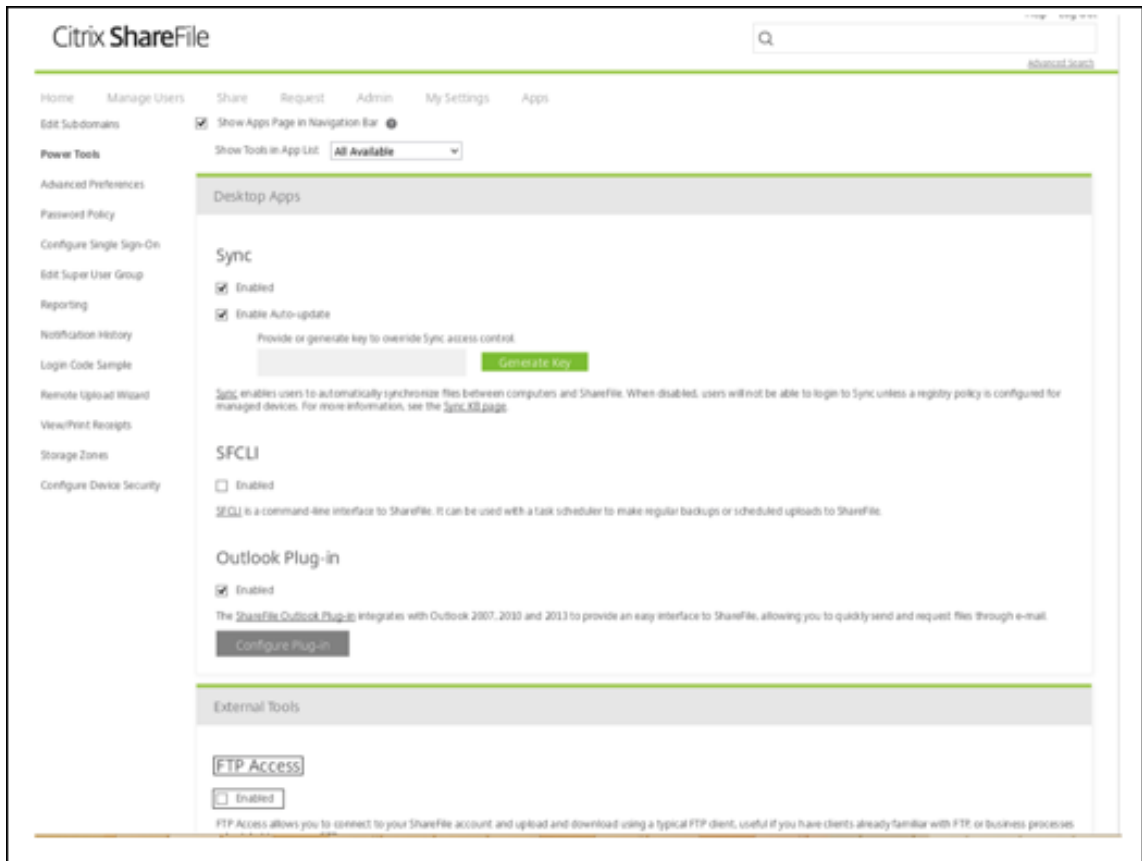
Both secure and standard FTP are enabled for your account.

참고:

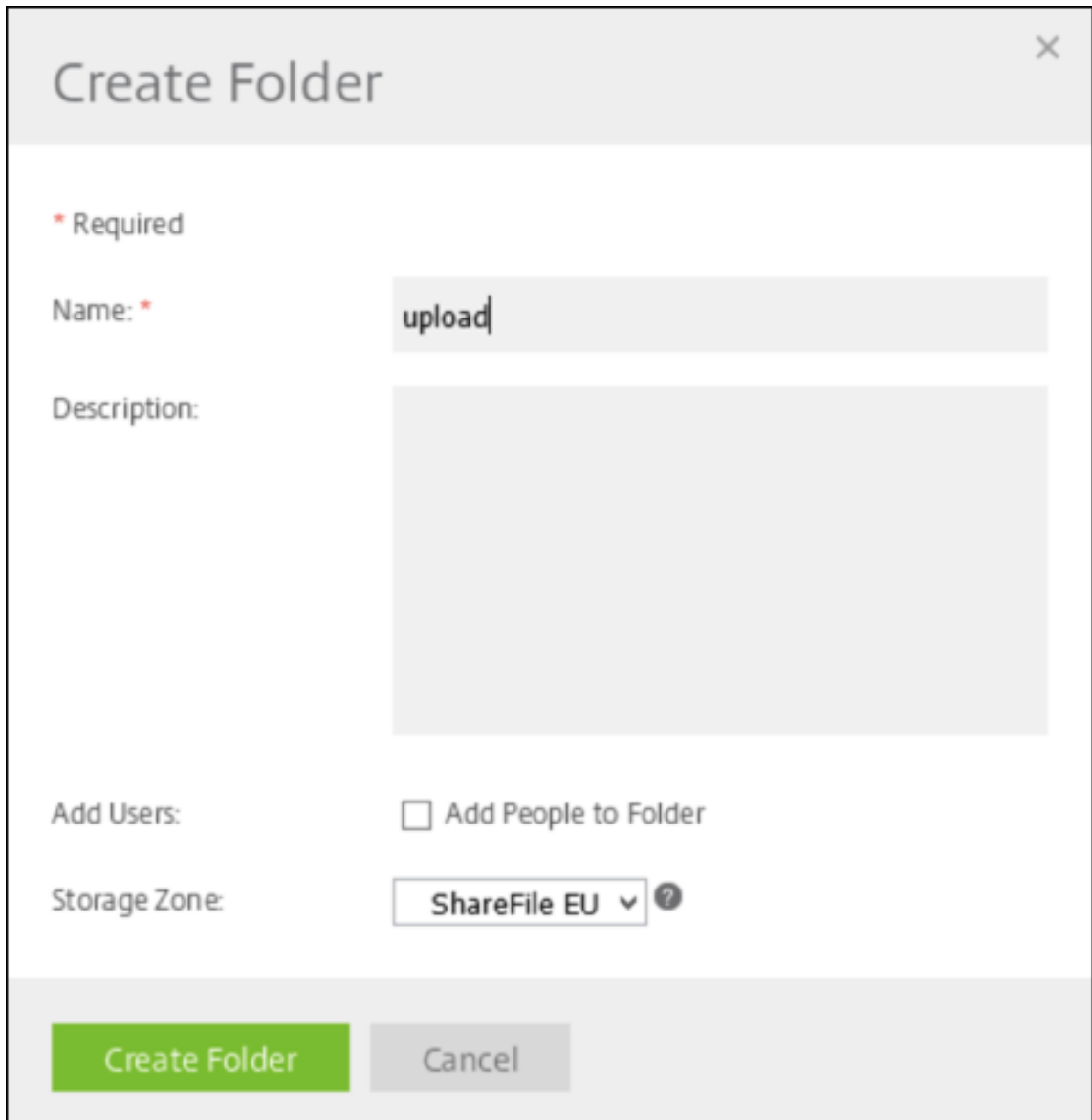
- XenMobile 에서 업로드하는 파일은 Linux CLI 기반 FTP 클라이언트입니다. 따라서 사용자 이름의 일부로 백슬래시 (\) 및 기호 (@) 문자를 입력할 수 없습니다.
- 영숫자 사용자 ID 가 보이지 않으면 ShareFile 관리자 또는 ShareFile 지원으로부터 이 사용자 ID 를 요청할 수 있습니다.

2. Citrix Files 서버에서 FTP 통신 및 FTPS 를 사용할 수 있는지 확인합니다. 이상적으로는 ShareFile 관리자가 FTP 통신에서 사용자 계정을 여는 것을 허용합니다. 그러나 가끔은 FTPS 통신만 허용됩니다.

관리자 권한이 있는 사용자는 설정, 관리 설정, 고급 기본 설정을 클릭한 후 **ShareFile** 도구 사용을 클릭하여 이 설정을 확인하고 사용하도록 설정할 수 있습니다. 외부 앱, **FTP** 액세스에서 사용 확인란을 선택해야 합니다.



3. FTP 클라이언트에서 파일 업로드에 대한 디렉터리로 사용할 공유 폴더를 만듭니다. 홈, 폴더를 차례로 클릭한 후 개인 폴더를 클릭합니다.
4. 맨 오른쪽에서 더하기 (+) 아이콘을 클릭하고 **Create Folder(폴더 만들기)** 를 클릭한 다음 폴더 이름을 입력합니다.



The image shows a 'Create Folder' dialog box with a close button (X) in the top right corner. The dialog has a light gray header and footer. The main content area is white. It contains the following fields and controls:

- * Required** (indicated by a red asterisk)
- Name: *** (text input field containing 'upload')
- Description:** (large text area)
- Add Users:** (checkbox labeled 'Add People to Folder')
- Storage Zone:** (dropdown menu showing 'ShareFile EU' with a question mark icon)
- Create Folder** (green button)
- Cancel** (gray button)

5. XenMobile Server CLI 의 **Main Menu**(메인 메뉴) 에서 **Troubleshooting**(문제 해결) > **Support Bundle**(지원 번들) 을 선택합니다. 그런 다음 **Support Bundle Menu**(지원 번들 메뉴) 에서 **Generate Support Bundle**(지원 번들 생성) 을 선택합니다.

```

-----
Main Menu
-----
[0] Configuration
[1] Clustering
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
Choice: [0 - 5] 3

```

```

-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----
Choice: [0 - 3] 3

```

```

-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----
Choice: [0 - 3] 1
Support bundle exists. Overwrite it? [y/n]: y

Support Bundle generation is in progress. This could take a while

Support_Bundle successfully generated: 201511123_1450866290591_22.17%_58.17%_37%_37%_37%.zip

```

참고:

지원 번들이 있는 경우 메시지가 표시되면 **y** 를 입력하여 번들을 재정의합니다.

6. 지원 번들을 FTP 서버에 업로드합니다.

- a. **Upload Support Bundle by using FTP**(FTP 를 사용하여 지원 번들 업로드) 를 선택합니다.
- b. **Enter remote host**(원격 호스트 입력): 메시지가 표시되면 FTP 서버 이름을 입력합니다. Citrix Files 가 FTP 서버로 사용되는 경우 회사 이름 다음에 Citrix Files FTP 사이트 이름을 입력합니다. 예: citrix.sharefileftp.com
- c. **Enter remote user name**(원격 사용자 이름 입력): 메시지가 표시되면 영숫자 사용자 ID 를 입력합니다.

d. **Enter remote user password**(원격 사용자 암호 입력): 메시지가 표시되면 암호를 입력합니다.

e. **Enter remote directory**(원격 디렉터리 입력): 메시지가 표시되면 Citrix Files 에서 만든 공유 폴더 이름을 입력한 후 **Enter** 키를 누릅니다.

```

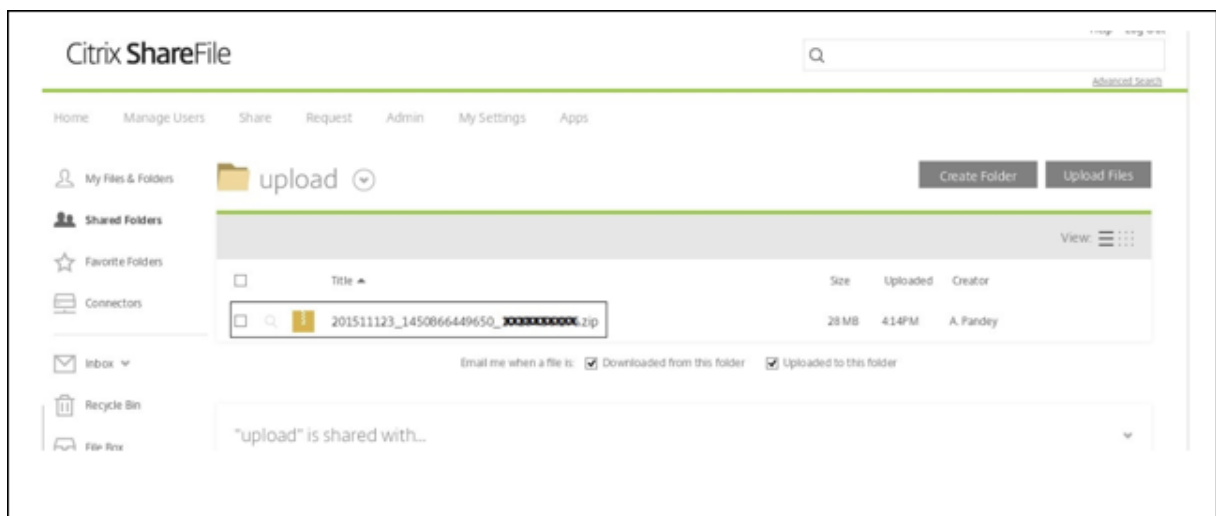
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----
Choice: [0 - 3] 3

Current support bundle: 201511123_1450866449650_XXXXXXXXXX.zip

Enter remote host: XXXXX.sharefileftp.com
Enter remote user name: XXXXX
Enter remote user password:
Enter remote directory
(Note: Do not use ftp://, http:// or host name. Path should be relative to ftp root location.): /upload

Connected to eu-XXXXX.eu-west-1.compute.amazonaws.com.
Remote system type is UNIX.
230-Connection established from (unknown) [XXXXX]
230-You are connected as (XXXXX) (XXXXX@XXXXX.citrix.com).
230>Welcome to the XXXXX Test Account FTP site.
250 "/upload" is the current directory.
125 Data connection open; transfer starting.
226-Received 29050517 bytes.
226 Transfer Complete.
29050517 bytes sent in 16.3 seconds (1779137 bytes/s)
221-Sent: 550 bytes Rcvd: 29,050,639 bytes Billable: 1 operations Time: 27s
  
```

업로드한 지원 번들을 Citrix Files 에서 만든 공유 폴더에서 볼 수 있습니다.



Citrix Files FTP 에 대한 자세한 내용은 이 [Citrix Support Knowledge Center 문서](#)를 참조하십시오.

디스크 공간을 확인하려면

CLI 에서 다음과 같이 시스템 디스크 공간을 확인할 수 있습니다.

1. 메인 메뉴에서 **System** 메뉴를 선택합니다.
2. **System** 메뉴에서 **Display System Disk Usage** 옵션을 선택합니다.

파일 시스템 정보가 나타납니다.

```
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----
Choice: [0 - 12] 5

filesystem      1K-blocks      Used Available Use% Mounted on
dev/             49431012 3786556 43133500   9% /
mpfs             8191176      156 8191020    1% /run
devtmpfs         8190888        0 8190888    0% /dev
dev/             101086      10094 85773     11% /boot
```

셀프 서비스 디스크 정리 수행

다음과 같이 CLI 에서 디스크를 정리할 수 있습니다.

1. 문제 해결 메뉴에서 디스크 사용량을 선택합니다. 디스크 사용량 메뉴에는 다음과 같은 옵션이 있습니다.

```

-----
Disk Usage Menu (Core dump and Support Bundle)
-----
[0] Back to Troubleshooting Menu
[1] Display Disk Usage
[2] Clean
-----
[Choice: [0 - 2] 1

No core dump and support bundle found.

```

2. 유형 1 은 코어 덤프 파일과 지원 번들 파일 유형을 나열합니다. 파일이 존재하지 않으면 다음 메시지가 표시됩니다. 코어 덤프 및 지원 번들이 없습니다.
3. 유형 2 는 검사된 코어 덤프 파일과 지원 번들 파일을 정리합니다.

XenMobile 콘솔에 대한 워크플로 시작하기

March 15, 2024

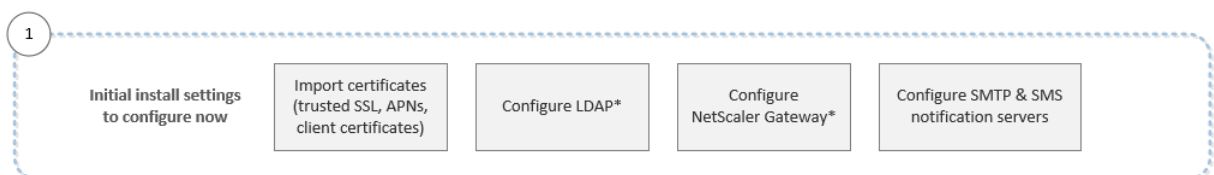
XenMobile 콘솔은 XenMobile 의 통합된 관리 도구입니다. 이 문서에서는 XenMobile 를 설치했고 콘솔에서 작업할 수 있는 상태인 것으로 가정합니다. XenMobile 을 아직 설치하지 않은 경우 [XenMobile 설치](#)를 참조하십시오. XenMobile 콘솔의 브라우저 지원에 대한 자세한 내용은 XenMobile 호환성 문서를 참조하십시오.

초기 설정 워크플로

명령줄 콘솔과 XenMobile 콘솔에서 차례로 XenMobile 을 구성하고 나면 대시보드가 열립니다. 초기 구성 화면으로 돌아갈 수 없습니다. 일부 설치 구성을 건너뛴 경우 콘솔에서 다음 설정을 구성할 수 있습니다. 사용자, 앱 및 장치를 추가하기 전에 다음 설치 설정을 완료해야 합니다. 먼저 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다.

참고:

별표가 있는 항목은 선택적 요소입니다.



각 설정에 대한 자세한 내용과 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

- [인증](#)
- [Citrix Gateway 및 XenMobile](#)
- [알림](#)

Android, iOS 및 Windows 플랫폼을 지원하려면 다음과 같은 계정 관련 설정을 완료해야 합니다.

Android

- Google Play 자격 증명을 만듭니다. 자세한 내용은 [Google Play Launch\(시작\)](#)를 참조하십시오.
- Android Enterprise 관리자 계정을 만듭니다. 자세한 내용은 [Android Enterprise](#)를 참조하십시오.
- Google 의 도메인 이름을 확인합니다. 자세한 내용은 [Google Workspace 도메인 확인](#)을 참조하십시오.
- API 를 사용하도록 설정하고 Android Enterprise 의 서비스 계정을 만듭니다. 자세한 내용은 [Android Enterprise 도움말](#)을 참조하십시오.

iOS

- Apple ID 와 개발자 계정을 만듭니다. 자세한 내용은 [Apple Developer Program](#) 웹 사이트를 참조하십시오.
- APNs(Apple 푸시 알림 서비스) 인증서를 만듭니다. XenMobile Server 배포를 사용하여 iOS 장치를 관리하려는 경우 Apple APNs 인증서가 필요합니다. Secure Mail 배포에 푸시 알림을 사용하는 경우 Apple APNs 인증서도 필요합니다. Apple APNs 인증서를 얻는 방법에 대한 자세한 내용은 [Apple Push Certificates Portal](#)을 참조하십시오. XenMobile 및 APNs 에 대한 자세한 내용은 [APNs 인증서](#) 및 [iOS 용 Secure Mail 의 푸시 알림](#)을 참조하십시오.
- 볼륨 구매 회사 토큰을 만듭니다. 자세한 내용은 [Apple Volume Purchasing Program](#)을 참조하십시오.

Windows

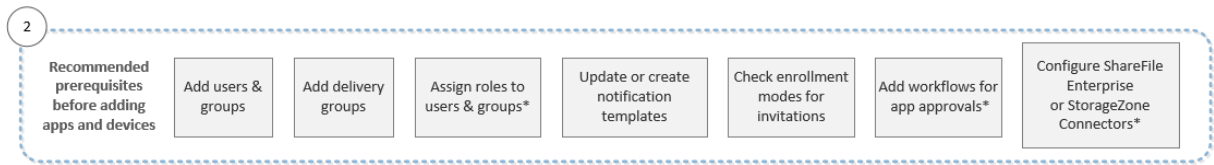
- Microsoft Windows 스토어 개발자 계정을 만듭니다. 자세한 내용은 [계정 유형, 위치 및 수수료](#)를 참조하십시오.
- Microsoft Windows 스토어 게시자 ID 를 가져옵니다. 자세한 내용은 [계정 설정 및 프로필 정보 관리](#)를 참조하십시오.
- Windows 장치 등록에 XenMobile 자동 검색을 사용하려는 경우 공용 SSL 인증서를 사용할 수 있는지 확인합니다. 자세한 내용은 [XenMobile 자동 검색 서비스](#)를 참조하십시오.

콘솔 사전 요구 사항 워크플로

이 워크플로에서는 앱 및 장치를 추가하기 전에 구성해야 할 사전 요구 사항을 보여 줍니다.

참고:

별표가 있는 항목은 선택적 요소입니다.



각 설정에 대한 자세한 내용과 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

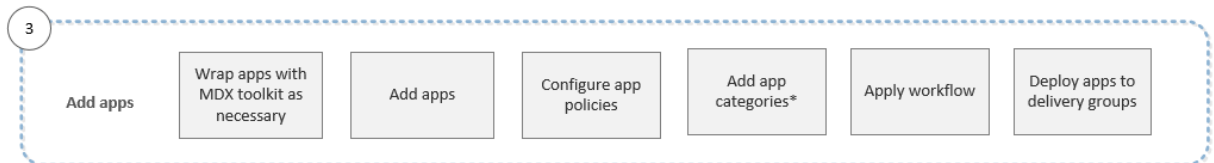
- [사용자 계정, 역할 및 등록](#)
- [리소스 배포](#)
- [RBAC 를 사용하여 역할 구성](#)
- [알림](#)
- [워크플로 적용](#)
- [XenMobile 에서 ShareFile 사용](#)

앱 워크플로 추가

이 워크플로는 XenMobile 에 앱을 추가하는 경우 따라야 할 권장 순서를 보여 줍니다.

참고:

별표가 있는 항목은 선택적 요소입니다.



각 설정에 대한 자세한 내용과 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

- [MDX Toolkit 정보](#)
- [앱 추가](#)
- [MDX 정책 요약](#)
- [워크플로 적용](#)
- [리소스 배포](#)

장치 워크플로 추가

이 워크플로는 XenMobile 에서 장치를 추가하고 등록하는 경우 따라야 할 권장 순서를 보여 줍니다.

참고:

별표가 있는 항목은 선택적 요소입니다.

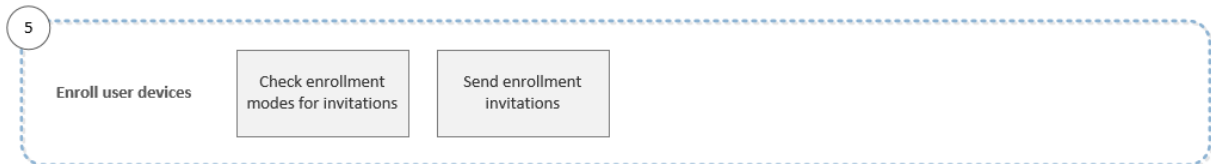


각 설정에 대한 자세한 내용과 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

- [장치](#)
- [지원되는 장치 운영 체제](#)
- [리소스 배포](#)
- [모니터링 및 지원](#)
- [자동화된 동작](#)

사용자 장치 워크플로 등록

이 워크플로는 XenMobile 에서 사용자 장치를 등록하는 경우 따라야 할 권장 순서를 보여 줍니다.



각 설정에 대한 자세한 내용과 단계별 절차는 다음 Citrix 제품 설명서 문서를 참조하십시오.

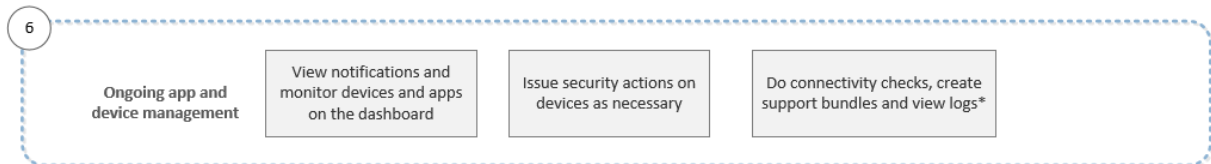
- [사용자 계정, 역할 및 등록](#)
- [알림](#)

진행 중인 앱 및 장치 관리 워크플로

이 워크플로는 콘솔에서 수행할 수 있는 앱 및 장치 관리 작업을 보여 줍니다.

참고:

별표가 있는 항목은 선택적 요소입니다.



콘솔의 오른쪽 위 모서리에 있는 렌치 아이콘을 클릭하면 표시되는 지원 옵션에 대한 자세한 내용은 [모니터링 및 지원](#)을 참조하십시오.

인증서 및 인증

July 11, 2023

XenMobile 작동 중에 다음과 같은 다양한 구성 요소가 인증에 관여합니다.

- **XenMobile Server:** XenMobile Server 는 등록 보안 및 등록 환경을 정의하는 위치입니다. 사용자 등록에 대한 옵션은 다음과 같습니다.
 - 등록을 모두에게 공개할지 초대 전용으로 할지 여부.
 - 2 단계 인증을 요구할지 3 단계 인증을 요구할지 여부. XenMobile 의 클라이언트 속성을 통해 Citrix PIN 인증 을 사용하도록 설정하고 PIN 의 복잡성과 만료 시간을 구성합니다.
- **Citrix ADC:** Citrix ADC 는 Micro VPN SSL 세션을 종료할 수 있는 기능을 제공합니다. 또한 Citrix ADC 는 네트워크 전송 중 보안 기능을 제공하며 사용자가 앱에 액세스할 때마다 사용되는 인증 환경을 정의할 수 있게 해 줍니다.
- **Secure Hub:** 등록 작업에서 Secure Hub 와 XenMobile Server 가 함께 작동합니다. Secure Hub 는 장치에서 Citrix ADC 와 통신하는 엔터티입니다. 세션이 만료되면 Secure Hub 가 Citrix ADC 로부터 인증 티켓을 받아 MDX 앱에 해당 티켓을 전달합니다. Citrix 는 인증서 고정을 권장하며, 이 방식은 메시지 가로채기 (man-in-the-middle) 공격을 방지해 줍니다. 자세한 내용은 Secure Hub 문서에서 [인증서 고정](#) 섹션을 참조하십시오.

또한 Secure Hub 를 통해 MDX 보안 컨테이너를 쉽게 사용할 수 있습니다. Secure Hub 는 정책을 푸시하고 앱이 시간 초과되면 Citrix ADC 를 통해 세션을 만들며 MDX 시간 초과 및 인증 환경을 정의합니다. 또한 Secure Hub 는 탈옥 감지, 지오로케이션 확인 및 사용자가 적용한 모든 정책을 관리합니다.
- **MDX 정책:** MDX 정책은 장치에서 데이터 저장소를 만듭니다. MDX 정책은 Micro VPN 연결을 다시 Citrix ADC 로 리디렉션하고 오프라인 모드 제한과 시간 초과 같은 클라이언트 정책을 적용합니다.

1 단계 인증 및 2 단계 인증 방법의 개요를 비롯한 인증 구성에 대한 자세한 내용은 배포 안내서에서 [인증](#) 문서를 참조하십시오.

XenMobile 의 인증서를 사용하여 보안 연결을 만들고 사용자를 인증할 수 있습니다. 이 문서의 나머지 부분에서 인증서에 대해 설명합니다. 다른 구성 세부 정보에 대해서는 다음과 같은 문서를 참조하십시오.

- [도메인 인증 또는 도메인 및 보안 토큰 인증](#)
- [클라이언트 인증서 인증 또는 인증서와 도메인 인증](#)
- [PKI 엔터티](#)
- [자격 증명 공급자](#)
- [APNs 인증서](#)
- [Citrix Files 의 SSO\(Single Sign-on\) 용 SAML](#)
- [Microsoft Azure Active Directory 서버 설정](#)
- [Wi-Fi 서버 인증을 위한 인증서를 장치로 보내려면: Wi-Fi 장치 정책](#)
- [내부 루트 인증 기관 \(CA\) 인증서와 같이 인증에 사용되지 않는 독특한 인증서 또는 특정 정책을 푸시하려면 자격 증명 장치 정책을 수행합니다.](#)

인증서

XenMobile 은 서버로 전달되는 통신을 보호하기 위해 자체 서명된 SSL(Secure Sockets Layer) 인증서를 설치 중에 생성합니다. 이 SSL 인증서를 잘 알려진 CA 의 신뢰할 수 있는 SSL 인증서로 교체해야 합니다.

또한 XenMobile 은 자체 PKI(공개 키 인프라) 서비스를 사용하거나 클라이언트 인증서에 대한 CA 로부터 인증서를 가져옵니다. 모든 Citrix 제품은 와일드카드 인증서와 SAN(주체 대체 이름) 인증서를 지원합니다. 대부분의 배포에서 와일드카드 또는 SAN 인증서 두 개만 있으면 됩니다.

클라이언트 인증서 인증에는 모바일 앱을 위한 추가 보안 계층이 제공되기 때문에 사용자가 HDX 앱에 원활하게 액세스할 수 있습니다. 클라이언트 인증서 인증이 구성된 경우 사용자가 XenMobile 지원 앱에 액세스하려면 SSO(Single Sign-on) 용 Citrix PIN 을 입력해야 합니다. 또한 Citrix PIN 은 사용자 인증 환경을 간소화합니다. Citrix PIN 은 클라이언트 인증서를 보호하거나 Active Directory 자격 증명을 장치에 로컬로 저장하는 데 사용됩니다.

XenMobile 에서 iOS 장치를 등록하고 관리하려면 Apple 에서 APNs(Apple 푸시 알림 서비스) 인증서를 설정하고 만드십시오. 단계에 대해서는 [APNs 인증서](#)를 참조하십시오.

다음 표에서는 각 XenMobile 구성 요소에 대한 인증서 형식 및 유형을 보여 줍니다.

XenMobile 구성 요소	인증서 형식	필요한 인증서 유형
Citrix Gateway	PEM(BASE64), PFX(PKCS #12)	SSL, 루트 (Citrix Gateway 가 PFX 를 자동으로 PEM 으로 변환함)
XenMobile Server	.p12(Windows 기반 컴퓨터의 경우.pfx)	SSL, SAML, APNs(XenMobile 이 설치 프로세스 중에 전체 PKI 도 생성함) 중요: XenMobile Server 는.pem 확장자의 인증서를 지원하지 않습니다. .pem 인증서를 사용하려면.pem 파일을 인증서와 키로 분할하고 각각을 XenMobile Server 로 가져옵니다.
StoreFront	PFX(PKCS #12)	SSL, 루트

XenMobile 은 비트 길이가 4096, 2048 및 1024 인 SSL 수신기 인증서 및 클라이언트 인증서를 지원합니다. 1024 비트 인증서는 공격 받기 쉽습니다.

Citrix Gateway 및 XenMobile Server 의 경우 Verisign, DigiCert, Thawte 등과 같은 공용 CA 로부터 서버 인증서를 받는 것이 좋습니다. Citrix Gateway 또는 XenMobile 구성 유틸리티에서 CSR(인증서 서명 요청) 을 만들 수 있습니다. CSR 을 만든 후 CA 에 제출하여 서명을 받을 수 있습니다. CA 가 서명된 인증서를 반환하면 해당 인증서를 Citrix Gateway 또는 XenMobile 에 설치할 수 있습니다.

중요: iOS, iPadOS 및 macOS 의 신뢰할 수 있는 인증서에 대한 요구 사항

Apple 은 TLS 서버 인증서에 대한 새로운 요구 사항을 도입했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는지 확인하십시오. Apple 게시물 <https://support.apple.com/en-us/HT210176>를 참조하십시오.

Apple 은 TLS 서버 인증서의 최대 허용 수명을 줄이는 중입니다. 이 변경 사항은 2020 년 9 월 이후에 발급된 서버 인증서에만 영향을 줍니다. Apple 게시물 <https://support.apple.com/en-us/HT211025>를 참조하십시오.

XenMobile 에서 인증서 업로드

업로드하는 인증서에는 인증서 콘텐츠를 포함하여 인증서 테이블의 항목이 포함됩니다. 인증서가 필요한 PKI 통합 구성 요소를 구성할 때 컨텍스트에 종속적인 조건을 충족하는 서버 인증서를 선택하십시오. 예를 들어 Microsoft 인증 기관 (CA) 과 통합되도록 XenMobile 을 구성한다고 가정합니다. Microsoft CA 에 대한 연결은 클라이언트 인증서를 사용하여 인증되어야 합니다.

이 섹션에서는 인증서를 업로드하는 일반적인 절차를 제공합니다. 클라이언트 인증서 만들기, 업로드 및 구성에 대한 자세한 내용은 [클라이언트 인증서 인증 또는 인증서와 도메인 인증](#)을 참조하십시오.

개인 키 요구 사항 XenMobile 은 지정된 인증서에 대한 개인 키를 소유하거나 소유하지 않을 수 있습니다. 마찬가지로 XenMobile 에서 사용자가 업로드한 인증서에 개인 키를 요구하거나 요구하지 않을 수 있습니다.

인증서 업로드 다음과 같은 두 가지 옵션으로 인증서를 업로드할 수 있습니다.

- 인증서를 콘솔에 개별적으로 업로드합니다.
- REST API 로 iOS 장치에 인증서를 일괄 업로드합니다.

콘솔에 인증서를 업로드할 때 주요 옵션 두 가지가 있습니다.

- 키 저장소 가져오기를 클릭합니다. PKCS #12 형식을 업로드하려는 경우가 아니라면 계속해서 설치하려는 키 저장소의 항목을 식별합니다.
- 클릭하여 인증서를 가져옵니다.

CA 가 요청에 서명하기 위해 사용하는 CA 인증서 (개인 키 포함 안 함) 를 업로드할 수 있습니다. 또한 클라이언트 인증을 위해 SSL 클라이언트 인증서 (개인 키 포함) 를 업로드할 수 있습니다.

Microsoft CA 엔터티를 구성할 때 CA 인증서를 지정합니다. CA 인증서인 모든 서버 인증서 목록에서 CA 인증서를 선택합니다. 마찬가지로, 클라이언트 인증을 구성할 때 XenMobile 에 개인 키가 있는 모든 서버 인증서의 목록에서 선택할 수 있습니다.

키 저장소를 가져오려면 보안 인증서 저장소인 키 저장소는 여러 항목을 포함할 수 있도록 설계되어 있습니다. 따라서 키 저장소에서 로드할 경우 로드할 항목을 식별하는 항목 별칭을 지정하라는 메시지가 나타납니다. 별칭을 지정하지 않으면 저장소의 첫 번째 항목이 로드됩니다. PKCS #12 파일은 대개 항목 하나만 포함하기 때문에 PKCS #12 를 키 저장소 유형으로 선택하면 별칭 필드가 나타나지 않습니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 인증서를 클릭합니다. 인증서 페이지가 나타납니다.

Settings > Certificates

Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import

Add

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key	▼
<input type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2015-11-16	2025-11-13	SAML	✓	
<input type="checkbox"/>	*.agsag.com		⚠ Expired	2013-10-23	2015-10-23	SSL Listener	✓	
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2015-11-16	2035-11-14	Devices CA		
<input type="checkbox"/>	ent-root-ca		Up to date	2012-02-22	2017-02-21	Root or intermediate		
<input type="checkbox"/>	APSP:3623302e-7c6e-4df8-aa9a		🕒 22 days left	2015-09-30	2016-09-29	APNs	✓	

Showing 1 - 5 of 5 items

3. 가져오기를 클릭합니다. 가져오기 대화 상자가 나타납니다.
4. 다음 설정을 구성합니다.
- 가져오기:

목록에서 키 저장소를 클릭합니다. 가져오기 대화 상자가 변경되어 사용 가능한 키 저장소 옵션이 나타납니다.

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import

Keystore

Keystore type

PKCS#12

Use as

Server

Keystore file*

Browse

Password*

Description

Cancel

Import

- 키 저장소 유형: 목록에서 **PKCS #12** 를 클릭합니다.
- 용도: 목록에서 인증서 사용 방법을 클릭합니다. 사용 가능한 옵션은 다음과 같습니다.
 - 서버. 서버 인증서는 XenMobile 웹 콘솔에 업로드되어 XenMobile Server 에서 기능적으로 사용되는 인증서입니다. 여기에는 CA 인증서, RA 인증서 및 클라이언트 인증용 인증서와 인프라의 다른 구성 요소가 포함됩니다. 또한 서버 인증서를 장치에 배포할 인증서의 저장소로 사용할 수 있습니다. 이 용도는 특히 장치에서 신뢰를 형성하는 데 사용되는 CA 에 적용됩니다.
 - **SAML**. SAML(Security Assertion Markup Language) 인증을 사용하면 서버, 웹 사이트 및 앱에 대한 SSO 액세스를 제공할 수 있습니다.
 - **APNs**. Apple 의 APNs 인증서를 사용하면 Apple Push Network 를 통해 모바일 장치를 관리할 수 있습니다.
 - **SSL** 수신기. SSL(Secure Sockets Layer) 수신기는 XenMobile 에 SSL 암호화 활동을 알립니다.
- 키 저장소 파일: 찾아보기로 가져올.p12(또는 Windows 기반 컴퓨터의 경우.pfx) 파일 형식의 키 저장소를 찾습니다.
- 암호: 인증서에 할당된 암호를 입력합니다.
- 설명: 필요한 경우 서로 다른 키 저장소를 구분하는 데 도움이 되는 설명을 입력합니다.

5. 가져오기를 클릭합니다. 키 저장소가 인증서 테이블에 추가됩니다.

인증서를 가져오려면 파일 또는 키 저장소 항목에서 인증서를 가져오면 XenMobile 이 입력에서 인증서 체인을 구성합니다. XenMobile 은 해당 체인의 모든 인증서를 가져와 각 인증서에 대한 서버 인증서 항목을 만듭니다. 이 작업은 파일 또는 키 저장소 항목의 인증서가 체인을 형성하는 경우에만 작동합니다. 예를 들어 체인의 각 후속 인증서가 이전 인증서의 발급자여야 합니다.

필요한 경우 가져온 인증서에 대한 설명을 추가할 수 있습니다. 설명은 체인의 첫 번째 인증서에만 첨부됩니다. 나중에 나머지 인증서의 설명을 업데이트할 수 있습니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭한 다음 인증서를 클릭합니다.
2. 인증서 페이지에서 가져오기를 클릭합니다. 가져오기 대화 상자가 나타납니다.
3. 가져오기 대화 상자의 가져오기에서 인증서가 선택되어 있지 않은 경우 인증서를 클릭합니다.
4. 가져오기 대화 상자가 변경되어 사용 가능한 인증서 옵션이 나타납니다. 용도에서 키 저장소를 사용할 방법을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - 서버. 서버 인증서는 XenMobile 웹 콘솔에 업로드되어 XenMobile Server 에서 기능적으로 사용되는 인증서입니다. 여기에는 CA 인증서, RA 인증서 및 클라이언트 인증용 인증서와 인프라의 다른 구성 요소가 포함됩니다. 또한 서버 인증서를 장치에 배포할 인증서의 저장소로 사용할 수 있습니다. 이 옵션은 특히 장치에서 신뢰를 형성하는 데 사용되는 CA 에 적용됩니다.
 - **SAML**. SAML(Security Assertion Markup Language) 인증을 사용하면 서버, 웹 사이트 및 앱에 대한 SSO(Single Sign-On) 액세스를 제공할 수 있습니다.
 - **SSL** 수신기. SSL(Secure Sockets Layer) 수신기는 XenMobile 에 SSL 암호화 활동을 알립니다.
5. 찾아보기로 가져올.p12(또는 Windows 기반 컴퓨터의 경우.pfx) 파일 형식의 키 저장소를 찾습니다.
6. 찾아보기로 인증서에 대한 선택적인 개인 키 파일을 찾습니다. 개인 키는 인증서의 암호화 및 암호 해독에 사용됩니다.
7. 필요한 경우 서로 다른 인증서를 구분할 때 도움이 되도록 인증서에 대한 설명을 입력합니다.
8. 가져오기를 클릭합니다. 인증서가 인증서 테이블에 추가됩니다.

REST API 로 iOS 장치에 인증서를 일괄 업로드합니다 한 번에 인증서 하나를 업로드하는 것이 실용적이지 않다면 REST API 를 사용하여 iOS 장치에 일괄 업로드할 수 있습니다. 이 방식은.p12 형식의 인증서를 지원합니다. REST API 에 대한 자세한 정보는 [REST API](#)를 참조하십시오.

1. `device_identity_value.p12` 형식으로 각 인증서 파일의 이름을 변경합니다. `device_identity_value` 는 각 장치의 IMEI, 일련 번호 또는 MEID 일 수 있습니다.
 일례로, 일련 번호를 인증 방식으로 사용하기로 선택합니다. 한 장치의 일련 번호가 `A12BC3D4EFGH`이므로 해당 장치에 설치될 것으로 예상되는 인증서 파일에 `A12BC3D4EFGH.p12`라는 이름을 지정합니다.
2. .p12 인증서의 암호를 저장할 텍스트 파일을 만듭니다. 해당 파일의 새 줄에 각 장치의 장치 식별자와 암호를 입력합니다. `device_identity_value=password` 형식을 사용합니다. 다음을 참조하십시오.

```
1 A12BC3D4EFGH.p12=password1!
2 A12BC3D4EFGH.p12=password2@
```

```

3 A12BC3D4EFL.p12=password3#
4 <!--NeedCopy-->

```

3. 생성한 모든 인증서와 텍스트 파일을.zip 파일에 담습니다.
4. REST API 클라이언트를 실행하고 XenMobile 에 로그인한 다음 인증 토큰을 가져옵니다.
5. 인증서를 가져와서 다음 내용을 본문에 입력합니다.

```

1 {
2
3     "alias": "",
4     "useAs": "device",
5     "uploadType": "keystore",
6     "keystoreType": "PKCS12",
7     "identityType": "SERIAL_NUMBER",           # identity type can be
8     "credentialFileName": "credential.txt"      # The credential file
9     }                                           name in .zip
10
11 <!--NeedCopy-->

```

POST https:// /xenmobile/api/v1/certificates/import/keystore/device

Params Authorization Headers (11) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> uploadFile	cert_p12.zip X	
<input checked="" type="checkbox"/> certImportData	{ "alias": "", "useAs": "device", "uploadType": "keystore", "keystoreType": "PKCS12", "identityType": "SERIAL_NUMBER", "credentialFileName": "credential.txt" }	
<input type="checkbox"/> useAs		
<input type="checkbox"/> uploadType		
<input type="checkbox"/> description		
Key		Description

Body Cookies Headers (4) Test Results

Status: 200 OK Time: 366 ms

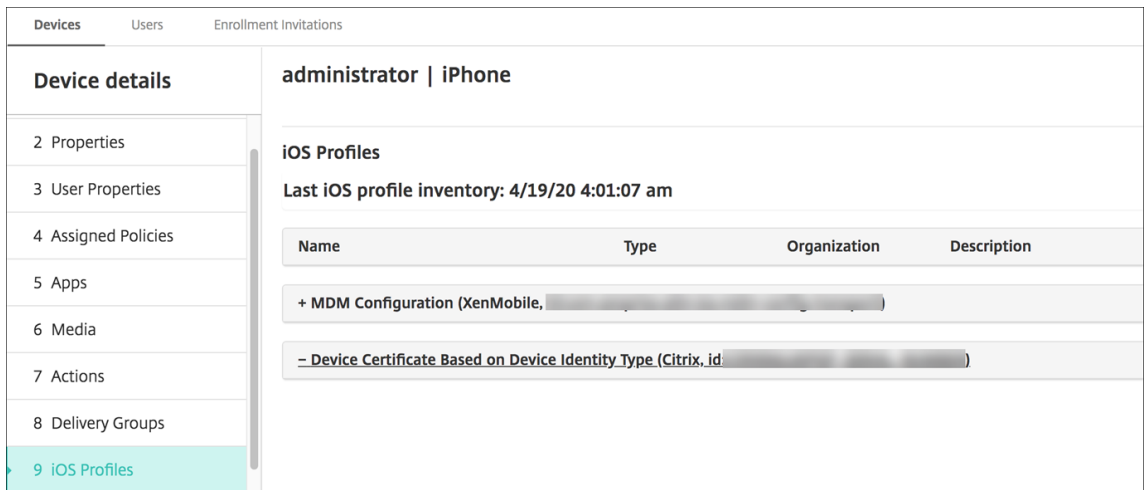
Pretty Raw Preview Visualize JSON

```

1 {
2   "status": 0,
3   "message": "Success",
4   "successCount": 3,
5   "failedCount": 0,
6   "skipCount": 0
7 }

```

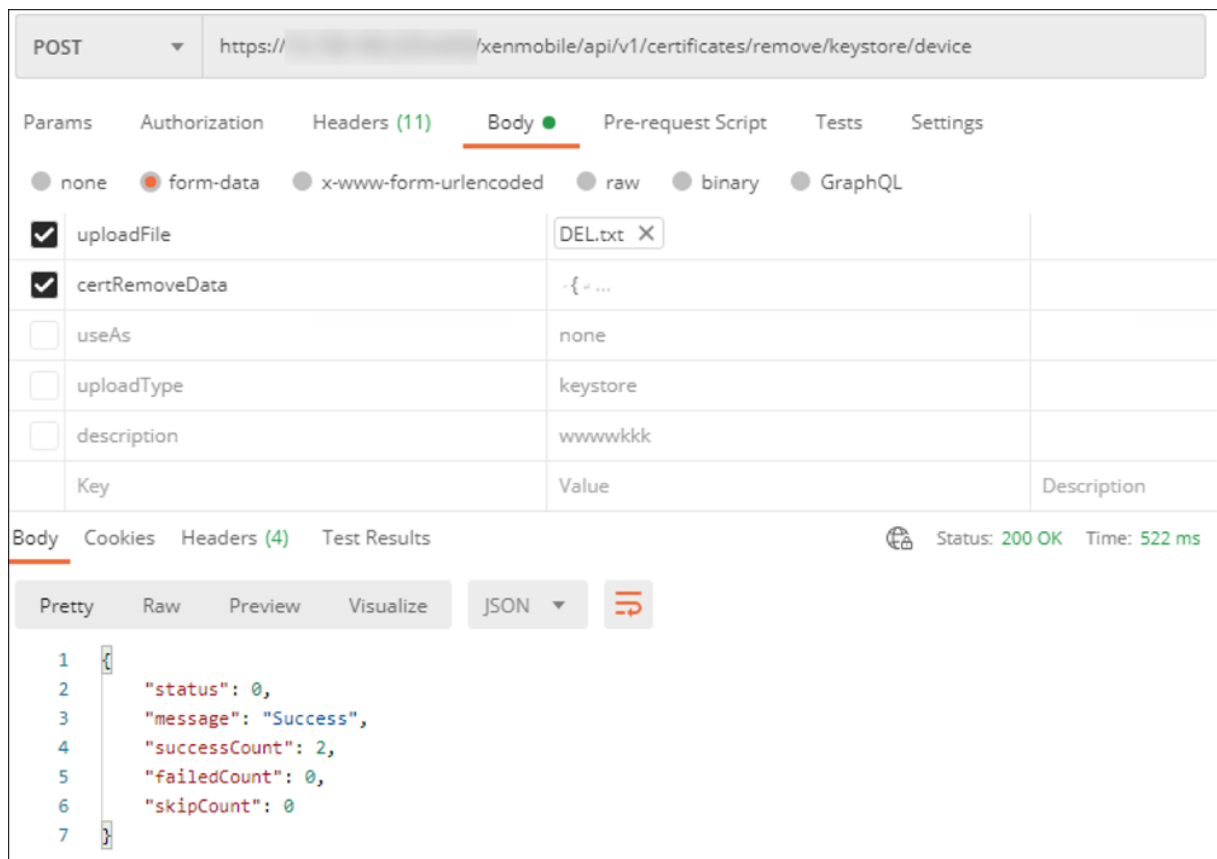
6. 인증서 유형이 **IKEv2** 항상 켜짐이고 장치 인증 방식이 장치 ID 기반 장치 인증서인 VPN 정책을 만듭니다. 인증서 파일 이름에 사용한 장치 ID 유형을 선택합니다. [VPN 장치 정책](#)을 참조하십시오.
7. iOS 장치를 등록하고 VPN 정책이 배포되기를 기다립니다. 장치의 MDM 구성을 확인하여 인증서 설치를 확인합니다. XenMobile 콘솔에서도 장치 세부 정보를 확인할 수 있습니다.



삭제할 각 인증서에 나열된 `device_identity_value`로 텍스트 파일을 만들어서 인증서를 일괄 삭제할 수도 있습니다. REST API 에서 삭제 API 를 호출하고 다음 요청을 사용하여 `device_identity_value`를 적절한 식별자로 대체합니다.

```

1  ``
2  {
3
4      "identityType"="device_identity_value"
5  }
6
7  <!--NeedCopy-->  ``
    
```



인증서 업데이트 XenMobile 은 특정 시점에 공개 키당 하나의 인증서만 시스템에 존재하도록 허용합니다. 이미 가져온 인증서와 동일한 키 쌍의 인증서를 가져오려고 하면 기존 항목을 바꾸거나 항목을 삭제할 수 있습니다.

인증서를 가장 효과적으로 업데이트하려면 XenMobile 콘솔에서 다음을 수행하십시오. 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭하여 설정 페이지를 연 다음 인증서를 클릭합니다. 가져오기 대화 상자에서 새 인증서를 가져옵니다.

서버 인증서를 업데이트할 경우 이전 인증서를 사용하는 구성 요소가 자동으로 새 인증서를 사용하도록 전환됩니다. 마찬가지로, 장치에 서버 인증서를 배포한 경우 인증서가 다음 번 배포에서 자동으로 업데이트됩니다.

인증서 갱신 XenMobile Server 는 PKI: 루트 CA, 장치 CA 및 서버 CA 에 대해 내부적으로 다음과 같은 인증 기관을 사용합니다. 이러한 CA 는 논리적 그룹으로 분류되며 그룹 이름이 제공됩니다. 새 XenMobile Server 인스턴스를 프로비저닝하면 세 개의 CA 가 생성되고 그룹 이름 “default(기본)” 가 지정됩니다.

XenMobile Server 콘솔 또는 공용 REST API 를 사용하여 지원되는 iOS, macOS 및 Android 장치에 대한 CA 를 갱신할 수 있습니다. 등록된 Windows 장치의 경우 새 장치 CA 를 받으려면 사용자가 장치를 재등록해야 합니다.

XenMobile Server 에서 내부 PKI CA 를 갱신하거나 다시 생성하고 이러한 인증 기관에서 발급한 장치 인증서를 갱신하는 데 다음과 같은 API 를 사용할 수 있습니다.

- 새 그룹 CA(인증 기관) 를 만듭니다.
- 새 CA 를 활성화하고 이전 CA 를 비활성화합니다.

- 구성된 장치 목록에서 장치 인증서를 갱신합니다. 이미 등록된 장치는 중단 없이 계속 작동합니다. 장치가 서버에 다시 연결되면 장치 인증서가 발급됩니다.
- 여전히 이전 CA 를 사용 중인 장치의 목록을 반환합니다.
- 모든 장치가 새 CA 를 사용하게 되면 이전 CA 를 삭제합니다.

자세한 내용은 [Public API for REST Services\(REST 서비스에 대한 공용 API\)](#) PDF 에서 다음 섹션을 참조하십시오.

- 섹션 3.16.58, Renew Device Certificate(장치 인증서 갱신)
- 섹션 3.23, Internal PKI CA Groups(내부 PKI CA 그룹)

장치 관리 콘솔에는 장치에서 등록 인증서를 갱신하는 데 사용된 보안 조치인 인증서 갱신이 포함됩니다.

사전 요구 사항

- 기본적으로 이 인증서 새로 고침 기능은 사용되지 않도록 설정됩니다. 인증서 새로 고침 기능을 활성화하려면 **refresh.internal.ca** 서버 속성 값을 **True** 로 설정하십시오.

중요:

Citrix ADC 에 SSL 오프로드가 설정된 경우 새 인증서를 생성할 때 새 cacert.perm 으로 부하 분산 장치를 업데이트해야 합니다. Citrix Gateway 설정에 대한 자세한 내용은 [NetScaler VIP 에 대해 SSL 오프로드 모드 사용](#)을 참조하십시오.

클러스터 노드에 대한 서버 **CA** 인증서 암호를 재설정하는 **CLI** 옵션 한 XenMobile Server 노드에서 서버 CA 인증서를 생성한 후 XenMobile CLI 를 사용하여 다른 클러스터 노드의 인증서 암호를 재설정합니다. CLI 기본 메뉴에서 시스템 > 고급 설정 > **CA** 인증서 암호 재설정을 선택합니다. 새 CA 인증서가 없는 경우 암호를 재설정하면 XenMobile 이 암호를 재설정하지 않습니다.



XenMobile 인증서 관리

특히 만료 날짜와 관련 암호에 대해, XenMobile 배포에서 사용하는 인증서를 기록해 두는 것이 좋습니다. 이 섹션에서는 XenMobile 에서 인증서를 보다 쉽게 관리할 수 있도록 도와 줍니다.

환경에 다음과 같은 인증서 중 일부 또는 전체가 포함될 수 있습니다.

- XenMobile Server
 - MDM FQDN 에 대한 SSL 인증서
 - SAML 인증서 (Citrix Files 용)
 - 이전 인증서 및 다른 모든 내부 리소스 (StoreFront/프록시 등) 에 대한 루트 및 중간 CA 인증서
 - iOS 장치 관리용 APN 인증서
 - XenMobile Server Secure Hub 알림을 위한 내부 APNs 인증서
 - PKI 연결을 위한 PKI 사용자 인증서
- MDX Toolkit

- Apple Developer 인증서
- Apple 프로비전 프로파일 (응용 프로그램별)
- Apple APNs 인증서 (Citrix Secure Mail 용)
- Android 키 저장소 파일

MAM SDK 는 앱을 래핑하지 않으므로 인증서가 필요하지 않습니다.

- Citrix ADC
 - MDM FQDN 에 대한 SSL 인증서
 - Gateway FQDN 에 대한 SSL 인증서
 - ShareFile SZC FQDN 에 대한 SSL 인증서
 - Exchange 부하 분산에 대한 SSL 인증서 (오프로드 구성)
 - StoreFront 부하 분산에 대한 SSL 인증서
 - 이전 인증서에 대한 루트 및 중간 CA 인증서

XenMobile 인증서 만료 정책

인증서가 만료되도록 허용하는 경우 인증서가 무효화됩니다. 더 이상 환경에서 보안 트랜잭션을 실행할 수 없으며 XenMobile 리소스에 액세스할 수 없습니다.

참고:

만료 날짜 전에 CA(인증 기관) 에서 SSL 인증서를 갱신하라는 메시지를 표시합니다.

Citrix Secure Mail 용 **APNs** 인증서

APNs(Apple 푸시 알림 서비스) 인증서는 매년 만료됩니다. 인증서가 만료되기 전에 APNs SSL 인증서를 만들고 Citrix 포털에서 업데이트하십시오. 인증서가 만료되면 Secure Mail 푸시 알림에서 불일치가 발생합니다. 또한 더 이상 앱에 대한 푸시 알림을 보낼 수 없습니다.

iOS 장치 관리용 **APNs** 인증서

XenMobile 에서 iOS 장치를 등록하고 관리하려면 Apple 에서 APNs 인증서를 설정하고 만드십시오. 인증서가 만료되면 사용자가 XenMobile 에 등록할 수 없으며 사용자의 iOS 장치를 관리할 수 없게 됩니다. 자세한 내용은 [APNs 인증서](#)를 참조하십시오.

Apple Push Certificates Portal 에 로그인하여 APNs 인증서 상태 및 만료 날짜를 확인할 수 있습니다. 인증서를 만든 동일 사용자로 로그인해야 합니다.

또한 만료 날짜 30 일 전과 10 일 전에 Apple 로부터 전자 메일 알림을 받게 됩니다. 알림에는 다음 정보가 포함되어 있습니다.

```
1 The following Apple Push Notification Service certificate, created for
  Apple ID CustomerID will expire on Date. Revoking or allowing this
  certificate to expire will require existing devices to be re-
  enrolled with a new push certificate.
2
3 Please contact your vendor to generate a new request (a signed CSR),
  then visit https://identity.apple.com/pushcert to renew your Apple
  Push Notification Service certificate.
4
5 Thank You,
6
7 Apple Push Notification Service
8 <!--NeedCopy-->
```

MDX Toolkit(iOS 배포 인증서)

물리적 iOS 장치에서 실행되는 앱 (Apple App Store 의 앱 제외) 은 다음과 같은 서명 요구 사항을 충족해야 합니다.

- 프로비전 프로파일로 앱을 서명합니다.
- 해당하는 배포 인증서로 앱을 서명합니다.

유효한 iOS 배포 인증서가 있는지 확인하려면 다음을 수행하십시오.

1. Apple Enterprise Developer 포털에서 MDX Toolkit 으로 래핑할 각 앱에 대한 명시적 앱 ID 를 만듭니다. 사용할 수 있는 앱 ID 의 예는 다음과 같습니다. `com.CompanyName.ProductName`.
2. Apple Enterprise Developer 포털에서 **Provisioning Profiles(프로비전 프로파일) > Distribution(배포)** 으로 이동하고 사내 프로비전 프로파일 을 만듭니다. 이전 단계에서 만든 각 앱 ID 에 대해 이 단계를 반복합니다.
3. 모든 프로비전 프로파일 을 다운로드합니다. 자세한 내용은 [iOS 모바일 앱 래핑](#) 을 참조하십시오.

모든 XenMobile Server 인증서가 유효한지 확인하려면 다음을 수행하십시오.

1. XenMobile 콘솔에서 설정 > 인증서를 클릭합니다.
2. APNs, SSL 수신기, 루트 및 중간 인증서를 비롯한 모든 인증서가 유효한지 확인합니다.

Android 키 저장소

키 저장소는 Android 앱에 서명하는 데 사용된 인증서가 들어 있는 파일입니다. 키 유효 기간이 만료되면 사용자가 더 이상 새 버전의 앱으로 원활하게 업그레이드할 수 없습니다.

Citrix ADC

Citrix ADC 에서 인증서 만료를 처리하는 방법에 대한 자세한 내용은 Citrix Support Knowledge Center 에서 [How to handle certificate expiry on NetScaler\(NetScaler 에서 인증서 만료를 처리하는 방법\)](#) 를 참조하십시오.

만료된 Citrix ADC 인증서를 통해서도 사용자가 스토어에 등록 및 액세스할 수 없습니다. 또한 만료된 인증서로 인해 Secure Mail 사용 시 Exchange Server에 연결할 수 없습니다. 또한 사용자가 HDX 앱을 나열하고 열 수 없습니다 (만료된 인증서에 따라 다름).

Expiry Monitor 및 Command Center를 사용하면 Citrix ADC 인증서를 추적할 수 있습니다. 인증서 만료 시 Center로부터 알림을 받게 됩니다. 이러한 도구를 사용하여 다음과 같은 Citrix ADC 인증서를 모니터링할 수 있습니다.

- MDM FQDN에 대한 SSL 인증서
- Gateway FQDN에 대한 SSL 인증서
- ShareFile SZC FQDN에 대한 SSL 인증서
- Exchange 부하 분산에 대한 SSL 인증서 (오프로드 구성)
- StoreFront 부하 분산에 대한 SSL 인증서
- 이전 인증서에 대한 루트 및 중간 CA 인증서

Citrix Gateway 및 XenMobile

July 18, 2022

XenMobile을 사용하여 Citrix Gateway를 구성할 때 내부 네트워크에 대한 원격 장치 액세스를 위한 인증 메커니즘을 설정합니다. 이 기능을 사용하면 모바일 장치의 앱이 인트라넷의 회사 서버에 액세스할 수 있습니다. XenMobile은 장치의 앱에서 Citrix Gateway로 Micro VPN을 만들 수 있습니다.

Citrix Gateway에서 실행되는 XenMobile에서 스크립트를 내보내어 XenMobile과 함께 사용할 Citrix Gateway를 구성합니다.

Citrix Gateway 구성 스크립트 사용을 위한 필수 구성 요소

Citrix ADC 요구 사항:

- Citrix ADC(최소 버전 11.0, 빌드 70.12).
- LDAP가 부하 분산되는 경우 이외에는 Citrix ADC IP 주소가 구성되고 LDAP 서버에 연결됩니다.
- Citrix ADC 서브넷 (SNIP) IP 주소가 구성되어 있고 필요한 백엔드 서버에 연결되며 포트 8443/TCP를 통해 공용 네트워크 액세스가 가능합니다.
- DNS가 공용 도메인을 확인할 수 있습니다.
- Citrix ADC가 플랫폼/범용 또는 평가판 라이선스로 라이선스 허가되었습니다. 자세한 내용은 <https://support.citrix.com/article/CTX126049>에서 참조하십시오.
- Citrix Gateway SSL 인증서가 Citrix ADC에 업로드되고 설치되었습니다. 자세한 내용은 <https://support.citrix.com/article/CTX136023>에서 참조하십시오.

XenMobile 요구 사항:

- XenMobile Server(최소 버전 10.6).
- LDAP 서버가 구성되었습니다.

내부 네트워크에 대한 원격 장치 액세스를 위한 인증 구성

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 **Citrix Gateway** 를 클릭합니다. **Citrix Gateway** 페이지가 나타납니다. 다음 예제에서는 Citrix Gateway 인스턴스가 존재합니다.

	Name	Default	External URL	Logon Type	# of Callback URLs
<input checked="" type="checkbox"/>	testGateway	✓	https://testGateway.domain.com	Domain	0

3. 다음 설정을 구성합니다.
 - 인증: 인증을 사용하도록 설정하지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 인증을 위한 사용자 인증서 제공: Citrix Gateway 에서 클라이언트 인증서 인증을 처리할 수 있도록 XenMobile 에서 Secure Hub 와 인증 인증서를 공유하기를 원하는지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 자격 증명 공급자: 목록에서 사용할 자격 증명 공급자를 클릭합니다. 자세한 내용은 [자격 증명 공급자](#)를 참조하십시오.
4. 저장을 클릭합니다.

Citrix Gateway 인스턴스 추가

인증 설정을 저장한 후 Citrix Gateway 인스턴스를 XenMobile 에 추가합니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 열립니다.
2. 서버 아래에서 **Citrix Gateway** 를 클릭합니다. **Citrix Gateway** 페이지가 나타납니다.
3. 추가를 클릭합니다. 새 **Citrix Gateway** 추가 페이지가 나타납니다.

Settings > Citrix Gateway > Add New Citrix Gateway

Add New Citrix Gateway

Name *

Alias

External URL *

Logon Type

Password Required ☒

Set as Default ☐

[Export Configuration Script](#)

Callback URL *	Virtual IP *	
<input type="text"/>	<input type="text"/>	Add

4. 다음 설정을 구성합니다.

- 이름: Citrix Gateway 인스턴스의 이름을 입력합니다.
- 별칭: 원하는 경우 Citrix Gateway 의 별칭 이름을 포함합니다.
- 외부 URL: Citrix Gateway 의 공개적으로 액세스 가능한 URL 을 입력합니다. 예를 들어, <https://receiver.com>입니다.
- 로그인 유형: 로그인 유형을 선택합니다. 유형에는 도메인만, 보안 토큰만, 도메인 및 보안 토큰, 인증서, 인증서 및 도메인, 인증서 및 보안 토큰이 포함됩니다. 암호 필요 필드의 기본 설정은 선택한 로그인 유형에 따라 달라집니다. 기본값은 도메인만입니다.

여러 개의 도메인이 있는 경우 인증서 및 도메인을 사용합니다. XenMobile 및 Citrix Gateway 를 통한 여러 도메인 인증 구성에 대한 자세한 내용은 여러 도메인에 대한 인증 구성을 참조하십시오.

인증서 및 보안 토큰을 사용하는 경우 Secure Hub 를 지원하기 위해 Citrix Gateway 에서 몇 가지 추가 구성이 필요합니다. 자세한 내용은 [Configuring XenMobile for Certificate and Security Token Authentication\(인증서 및 보안 토큰 인증을 사용하기 위한 XenMobile 구성\)](#)을 참조하십시오.

자세한 내용은 배포 안내서의 [인증](#)을 참조하십시오.

- 암호 필요: 암호 인증을 요구할지 여부를 선택합니다. 기본값은 선택한 로그인 유형에 따라 달라집니다.
- 기본값으로 설정: 이 Citrix Gateway 를 기본값으로 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 구성 스크립트 내보내기: 단추를 클릭하면 Citrix Gateway 에 업로드하는 구성 번들을 내보내서 XenMobile 설정으로 구성할 수 있습니다. 자세한 내용은 이 단계 뒤의 “XenMobile Server 와 함께 사용할 온-프레미스 Citrix Gateway 구성” 을 참조하십시오.
- 콜백 URL 및 가상 IP: 이러한 필드를 추가하기 전에 설정을 저장하십시오. 자세한 내용은 이 문서의 콜백 URL 및 Citrix Gateway VPN 가상 IP 추가를 참조하십시오.

5. 저장을 클릭합니다.

새 Citrix Gateway 가 추가되고 테이블에 나타납니다. 인스턴스를 편집하거나 삭제하려면 목록에서 이름을 클릭합니다.

XenMobile Server 와 함께 사용할 Citrix Gateway 구성

XenMobile 과 함께 사용할 온-프레미스 Citrix Gateway 를 구성하려면 이 문서에서 자세히 설명하는 다음 일반 단계를 수행하십시오.

1. XenMobile Server 에서 스크립트 및 관련 파일을 다운로드합니다. 최신의 상세 지침을 보려면 스크립트와 함께 제공되는 추가 정보 파일을 참조하십시오.
2. 환경이 필수 구성 요소를 충족하는지 확인합니다.
3. 스크립트를 환경에 맞게 업데이트합니다.
4. Citrix ADC 에서 스크립트를 실행합니다.
5. 구성을 테스트합니다.

이 스크립트로 XenMobile 에 필요한 Citrix Gateway 설정을 구성합니다.

- MDM 및 MAM 에 필요한 Citrix Gateway 가상 서버
- Citrix Gateway 가상 서버의 세션 정책
- XenMobile Server 세부 정보
- Citrix Gateway 가상 서버의 인증 정책 및 동작
스크립트에 LDAP 구성 설정이 설명됩니다.
- 프록시 서버의 트래픽 동작 및 정책
- 클라이언트 없는 액세스 프로필
- Citrix ADC 의 정적 로컬 DNS 레코드
- 기타 바인딩: 서비스 정책, CA 인증서

다음 구성은 스크립트에서 처리되지 않습니다.

- Exchange 부하 분산
- Citrix Files 부하 분산
- ICA 프록시 구성
- SSL 오프로드

스크립트를 다운로드, 업데이트 및 실행하려면

1. Citrix Gateway 를 추가하는 경우 새 **Citrix Gateway** 추가 페이지에서 구성 스크립트 내보내기를 클릭합니다.

Settings > Citrix Gateway > Add New Citrix Gateway

Add New Citrix Gateway

Name *

Alias

External URL *

Logon Type

Password Required ☒

Set as Default ☐

[Export Configuration Script](#)

Callback URL * Virtual IP * [Add](#)

또는 Citrix Gateway 인스턴스를 추가하고 스크립트를 내보내기 전에 저장을 클릭하는 경우: 설정 > **Citrix Gateway** 로 돌아가서 Citrix ADC 를 선택한 다음 구성 스크립트 내보내기와 다운로드를 차례로 클릭합니다.

Settings > Citrix Gateway

Citrix Gateway

When you configure Citrix Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use Citrix Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication ☒

Deliver user certificate for authentication ☒

Credential provider

[Save](#)

[Add](#) | [Edit](#) | [Export Configuration Script](#)

	Name	Default	External URL	Logon Type	# of Callback URLs
<input checked="" type="checkbox"/>	testGateway	✓	https://testGateway.domain.com	Domain	0

구성 스크립트 내보내기를 클릭하면 XenMobile 에서.tar.gz 스크립트 번들이 만들어집니다. 스크립트 번들에는 다음 이 포함됩니다.

- 상세 지침이 포함된 추가 정보 파일
- Citrix ADC 에서 필요한 구성 요소를 구성하는 데 사용되는 Citrix ADC CLI 명령이 포함된 스크립트
- 공용 루트 CA 인증서와 XenMobile Server 의 중간 CA 인증서 (현재 릴리스에서는 SSL 오프로드에 대해 이러한 인증서가 필요하지 않음)
- Citrix ADC 구성을 제거하는 데 사용되는 Citrix ADC CLI 명령이 포함된 스크립트

2. 스크립트 (NSGConfigBundle_CREATESCRIPT.txt) 를 편집하여 모든 자리 표시자를 환경의 세부 정보로 바꿉니다.


```

# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <MSG_ROOT_CA_CERT_TAG> -- NetScaler ROOT CA Tag.
# <RADIUS_KEY> -- Radius Key.
# <XMS_CERT_TAG> -- XenMobile Certificate Tag.
# <MAM_LB_IP> -- Virtual IP Address to be assigned for MAM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <MDM_LB_IP> -- Virtual IP Address to be assigned for MDM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <MSG_UIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reacha
ble from your devices either directly or via a NAT.

```

3. 스크립트 번들에 포함된 추가 정보 파일의 설명에 따라, 편집된 스크립트를 Citrix ADC 배시 셸 (shell) 에서 실행합니다.
예:

```

/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler
Management Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.
txt"

```

```

login as: nsroot
#####
#
#      WARNING: Access to this system is for authorized users only      #
#      Disconnect IMMEDIATELY if you are not an authorized user!      #
#
#####
Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"

```

스크립트가 완료되면 다음 줄이 나타납니다.

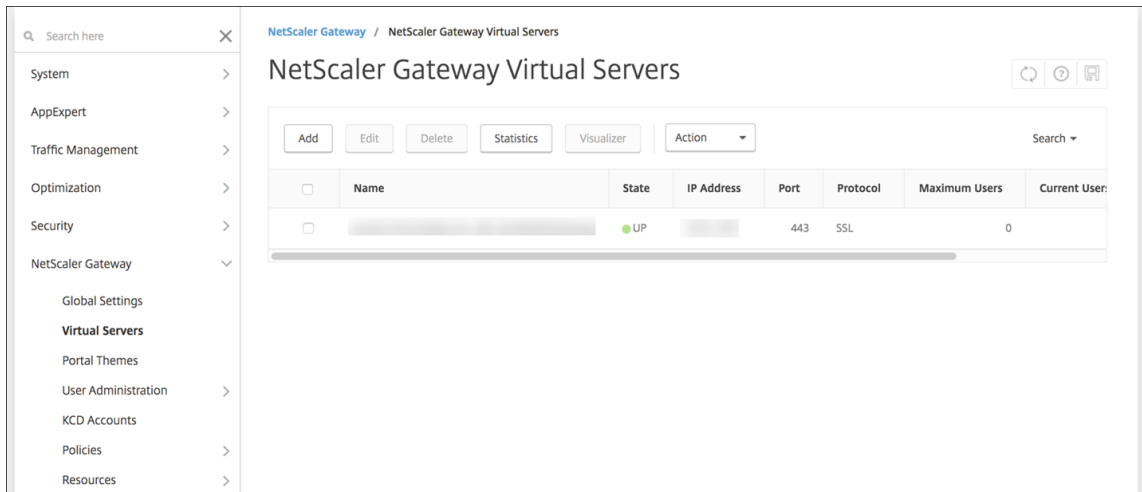
```

exec: save ns config
Done
Done
root@ns#

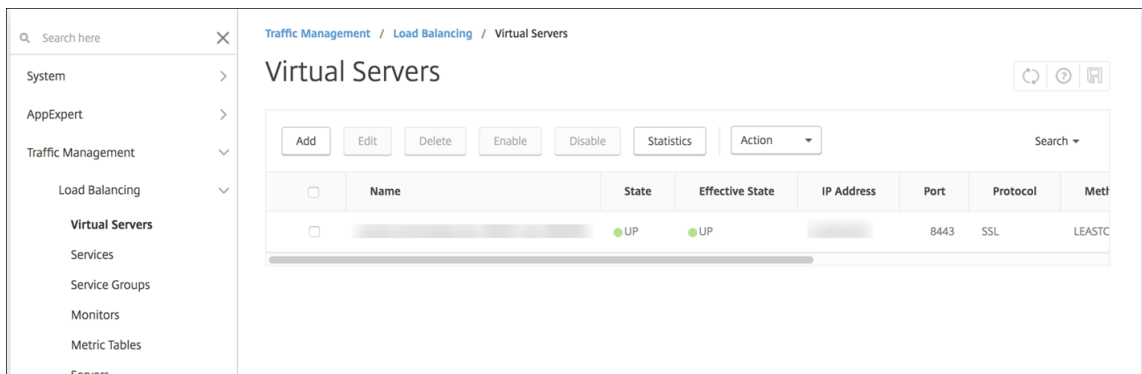
```

구성 테스트

1. Citrix Gateway 가상 서버의 상태가 작동인지 확인합니다.



2. 프록시 부하 분산 가상 서버의 상태가 작동인지 확인합니다.



3. 웹 브라우저를 열고 Citrix Gateway URL 에 연결하여 인증을 시도합니다. 인증이 실패하면 HTTP 상태 404 - 찾을 수 없음 메시지가 나타납니다.
4. 장치를 등록하고 MDM 및 MAM 모두에 등록되었는지 확인합니다.

콜백 URL 및 Citrix Gateway VPN 가상 IP 추가

Citrix Gateway 인스턴스를 추가한 후 콜백 URL 을 추가하고 Citrix Gateway 가상 IP 주소를 지정할 수 있습니다. 이 설정은 선택 사항이지만 특히 XenMobile Server 가 DMZ 에 있는 경우 보안을 강화하기 위해 구성할 수 있습니다.

1. 설정 > **Citrix Gateway** 에서 Citrix Gateway 를 선택하고 편집을 클릭합니다.
2. 테이블에서 추가를 클릭합니다.
3. 콜백 **URL** 로 FQDN(정규화된 도메인 이름) 을 입력합니다. 콜백 URL 은 요청이 Citrix Gateway 에서 온 요청인지 확인합니다.

콜백 URL 이 XenMobile Server 에서 연결 가능한 IP 주소로 확인되는지 확인합니다. 콜백 URL 은 외부 Citrix Gateway URL 또는 다른 URL 일 수 있습니다.

4. Citrix Gateway 가상 **IP** 주소를 입력한 다음 저장을 클릭합니다.

여러 도메인에 대한 인증 구성

테스트, 개발 및 프로덕션 환경을 위한 다수의 XenMobile Server 인스턴스가 있는 경우 추가 환경에 대한 Citrix Gateway를 수동으로 구성합니다. XenMobile 용 Citrix ADC 마법사는 한 번만 사용할 수 있습니다.

Citrix Gateway 구성

여러 도메인 환경에 대한 Citrix Gateway 인증 정책 및 세션 정책을 구성하려면:

1. Citrix Gateway 구성 유틸리티의 구성 탭에서 **Citrix Gateway > 정책 > 인증**을 확장합니다.
2. 탐색 창에서 **LDAP**를 클릭합니다.
3. LDAP 프로필을 클릭하여 편집합니다. 서버 로그인 이름 특성을 **userPrincipalName** 또는 검색에 사용하려는 특성으로 변경합니다. XenMobile 콘솔에서 LDAP 설정 구성 시 사용할 수 있도록 지정한 특성을 메모해 둡니다.

The screenshot shows the 'Other Settings' section of the Citrix Gateway LDAP configuration. It contains four fields with dropdown menus:

- Server Logon Name Attribute:** sAMAccountName
- Search Filter:** (empty)
- Group Attribute:** memberOf
- Sub Attribute Name:** cn

4. 각 LDAP 정책에 대해 이러한 단계를 반복합니다. 각 도메인에는 개별 LDAP 정책이 필요합니다.
5. Citrix Gateway 가상 서버에 바인딩된 세션 정책에서 **Edit session profile(세션 프로필 편집) > Published Applications(게시된 응용 프로그램)**로 이동합니다. **Single Sign-On Domain(Single Sign-On 도메인)**이 비어 있는지 확인합니다.

XenMobile Server 구성

여러 도메인의 XenMobile 환경에 대한 LDAP를 구성하려면:

1. XenMobile 콘솔에서 설정 > **LDAP**로 이동하고 디렉터리를 추가하거나 편집합니다.

Settings > LDAP

LDAP
Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups ☐ NO

Add

<input type="checkbox"/>	Directory Type	Domain Name	Server/Port	User Base DN	Group Base DN	Default
<input type="checkbox"/>	Microsoft Active Directory	Araujo.local	10.25.213.2389	dc=araujo,dc=local	dc=araujo,dc=local	✓

Showing 1 - 1 of 1 items

2. 다음 정보를 제공합니다.

- 도메인 별칭에서 사용자 인증에 사용할 각 도메인을 지정합니다. 도메인을 쉼표로 구분하십시오. 도메인 사이에 공백을 사용하지 마십시오. 예: `domain1.com, domain2.com, domain3.com`
- 사용자 검색 기준 필드가 Citrix Gateway LDAP 정책에서 지정한 **Server Logon Name Attribute**(서버 로그인 이름 특성)와 일치하는지 확인합니다.

Directory type*	Microsoft Active Directory	
Primary server*	10.	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*	Araujo.local	
User base DN*	dc=Araujo,dc=local	?
Group base DN*	dc=Araujo,dc=local	?
User ID*	Administrator@Araujo.local	
Password*		
Domain alias*	Araujo.local,Araujo.com,Araujo.net	
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

특정 URL에 대한 인바운드 연결 요청 삭제

사용자 환경의 Citrix Gateway에 SSL 오프로드가 구성된 경우 게이트웨이에서 특정 URL에 대한 인바운드 연결 요청을 삭제하는 것이 좋습니다.

추가 보안을 원하는 경우 Citrix Gateway 에서 두 개의 MDM 부하 분산 장치 가상 서버 (포트 443 용 및 포트 8443 용) 를 구성합니다. 설정 시 다음 정보를 템플릿으로 활용합니다.

중요:

다음 업데이트는 SSL 오프로드가 구성된 Citrix Gateway 에만 적용됩니다.

1. XMS_DropURLs라는 이름의 패턴 집합을 만듭니다.

```
1 add policy patset XMS_DropURLs
2 <!--NeedCopy-->
```

2. 이 새로운 패턴 집합에 다음 URL 을 추가합니다. 필요에 따라 이 목록을 사용자 지정합니다.

```
1 bind policy patset XMS_DropURLs /zdm/shp/console -index 6
2
3 bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5
4
5 bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4
6
7 bind policy patset XMS_DropURLs /zdm/log.jsp -index 3
8
9 bind policy patset XMS_DropURLs /zdm/login.jsp -index 2
10
11 bind policy patset XMS_DropURLs /zdm/console -index 1
12 <!--NeedCopy-->
```

3. 연결 요청이 지정된 서브넷에서 시작되지 않는 한 이러한 URL 에 대한 모든 트래픽을 삭제하는 정책을 만듭니다.

```
1 add responder policy XMS_DROP_pol "CLIENT.IP.SRC.IN_SUBNET
(192.168.0.0/24).NOT &&
2 HTTP.REQ.URL.CONTAINS_ANY(" XMS_DropURLs ") " DROP -comment "Allow
only subnet 192.168.0.0/24 to access these URLs. All other
connections are DROPed"
3 <!--NeedCopy-->
```

4. 새 정책을 두 MDM 부하 분산 장치 가상 서버 (포트 443 및 8443) 에 바인딩합니다.

```
1 bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
REQUEST
2
3 bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
REQUEST
4 <!--NeedCopy-->
```

5. 브라우저를 통한 MAM URL 액세스 차단

브라우저를 통해 MAM URL 에 직접 액세스하면 사용자에게 Active Directory 자격 증명을 입력하라는 메시지가 표시 됩니다. 이는 사용자가 자격 증명의 유효성을 검사하는 도구 역할을 하지만 일부 사용자는 이를 보안 위반으로 간주할 수 있습니다. 다음 섹션은 NetScaler 의 응답자 정책 기능을 사용하여 MAM URL(NetScaler Gateway VIP) 에 대한 브라우저 액세스를 제한하는 데 도움이 됩니다.

다음 응답자 정책 중 하나를 만들어 NetScaler Gateway 가상 서버에 바인딩합니다.

- `add responder policy Resp_Brow_Pol "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"Mozilla\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")"DROP`
- `add responder policy Resp_Brow_Pol_CR "!HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")"DROP`
- `add responder policy Resp_Brow_Pol_CR "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")"DROP`

`bind vpn vserver _XM_XenMobileGateway -policy Resp_Brow_Pol_CR -priority 100 -gotoPriorityExpression END -type REQUEST`를 사용하여 NetScaler Gateway 가상 서버에 바인딩

참고:

`_XM_XenMobileGateway`는 NetScaler Gateway 가상 서버의 예제 이름입니다.

도메인 인증 또는 도메인 및 보안 토큰 인증

January 5, 2022

XenMobile은 LDAP(Lightweight Directory Access Protocol)와 호환되는 하나 이상의 디렉터리에 대한 도메인 기반 인증을 지원합니다. XenMobile에서 하나 이상의 디렉터리에 대한 연결을 구성한 다음 LDAP 구성을 사용하여 그룹, 사용자 계정 및 관련 속성을 가져올 수 있습니다.

LDAP는 IP(인터넷 프로토콜) 네트워크를 통한 분산 디렉터리 정보 서비스 액세스 및 유지 관리를 지원하는 공급업체 중립적인 오픈소스 응용 프로그램 프로토콜입니다. 디렉터리 정보 서비스는 네트워크에서 사용 가능한 사용자, 시스템, 네트워크, 서비스 및 응용 프로그램에 대한 정보를 공유하는 데 사용됩니다.

LDAP는 일반적으로 다수의 서비스에서 하나의 암호(사용자당)를 공유하는 SSO(Single Sign-on)를 사용자에게 제공할 때 사용됩니다. SSO(Single Sign-on)를 사용하면 사용자가 회사 웹 사이트에 한 번 로그인하여 회사 인트라넷에 대한 액세스를 인증할 수 있습니다.

클라이언트는 DSA(Directory System Agent)라고 하는 LDAP 서버에 연결하여 LDAP 세션을 시작합니다. 그런 다음 클라이언트는 서버에 작업 요청을 보내고 서버는 적절한 인증으로 응답합니다.

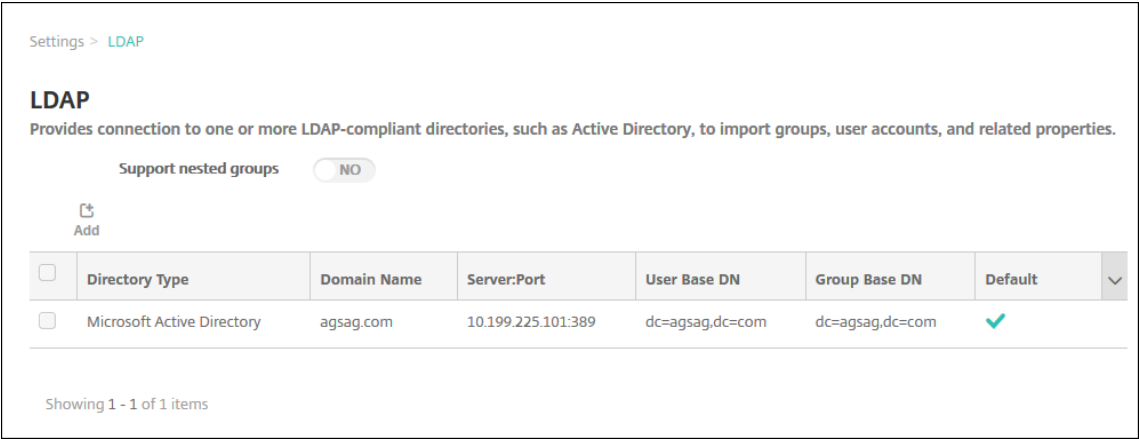
중요:

XenMobile은 사용자가 XenMobile에서 장치를 등록한 후 도메인 인증에서 다른 인증 모드로의 인증 모드 변경을 지

원하지 않습니다.

XenMobile에서 **LDAP** 연결을 추가하려면

- 1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
- 2. 서버에서 **LDAP**를 클릭합니다. **LDAP** 페이지가 나타납니다. 이 문서에 설명된 대로 LDAP 호환 디렉터리를 추가, 편집 또는 삭제할 수 있습니다.



LDAP 호환 디렉터리를 추가하려면

- 1. **LDAP** 페이지에서 추가를 클릭합니다. **LDAP** 추가 페이지가 나타납니다.

Settings > LDAP > Add LDAP

Add LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	IP Address or FQDN	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*		
User base DN*	dc=example,dc=com	?
Group base DN*	dc=example,dc=com	?
User ID*		
Password*		
Domain alias*		
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	NO	

Cancel Save

2. 다음 설정을 구성합니다.

- **디렉터리 유형:** 목록에서 적절한 디렉터리 유형을 클릭합니다. 기본값은 **Microsoft Active Directory**입니다.
- **주 서버:** LDAP에 사용되는 주 서버를 입력합니다. IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력할 수 있습니다.
- **보조 서버:** 보조 서버가 구성된 경우 선택적으로 보조 서버의 IP 주소 또는 FQDN을 입력합니다. 이 서버는 주 서버에 연결할 수 없을 때 사용되는 장애 조치 (failover) 서버입니다.
- **포트:** LDAP 서버가 사용하는 포트 번호를 입력합니다. 기본적으로 포트 번호는 보안되지 않은 LDAP 연결의 경우 **389**로 설정됩니다. 보안 LDAP 연결에는 포트 번호 **636**을 사용하고, Microsoft 비보안 LDAP 연결에는 **3268**을 사용하고, Microsoft 보안 LDAP 연결에는 **3269**를 사용하십시오.
- **도메인 이름:** 도메인 이름을 입력합니다.
- **사용자 기본 DN:** 고유 식별자를 통해 Active Directory의 사용자 위치를 입력합니다. 구문의 예로는 `ou=users,dc=example` 또는 `dc=com`이 있습니다.

- 그룹 기본 **DN**: Active Directory의 그룹 위치를 입력합니다. 예를 들어 **cn=users**, **dc=domain**, **dc=net**를 입력합니다. 여기서, **cn=users**는 그룹의 컨테이너 이름을 나타내고 **dc**는 Active Directory의 도메인 구성 요소를 나타냅니다.
- 사용자 **ID**: Active Directory 계정과 연관된 사용자 ID를 입력합니다.
- 암호: 사용자와 연관된 암호를 입력합니다.
- 도메인 별칭: 도메인 이름의 별칭을 입력합니다. 등록 후 도메인 별칭 설정을 변경하는 경우 사용자가 다시 등록해야 합니다.
- **XenMobile** 잠금 제한: 실패한 로그인 시도 횟수를 **0**에서 **999** 사이의 숫자로 입력합니다. **0** 값은 XenMobile이 실패한 로그인 시도를 기준으로 사용자를 잠그지 않음을 의미합니다.
- **XenMobile** 잠금 시간: 잠금 제한을 초과한 후 사용자가 대기해야 하는 시간 (분)을 나타내는 **0**에서 **99999** 사이의 숫자를 입력합니다. **0** 값은 잠금 후 사용자가 대기하지 않아도 됨을 의미합니다.
- 글로벌 카탈로그 **TCP** 포트: 글로벌 카탈로그 서버의 TCP 포트 번호를 입력합니다. 기본적으로 TCP 포트 번호는 **3268**로 설정됩니다. SSL 연결의 경우 포트 번호 **3269**를 사용하십시오.
- 글로벌 카탈로그 루트 컨텍스트: 필요한 경우 Active Directory의 글로벌 카탈로그 검색을 사용하도록 설정하는 데 사용되는 글로벌 루트 컨텍스트 값을 입력합니다. 이 검색은 실제 도메인 이름을 지정할 필요가 없는 모든 도메인에서 표준 LDAP 검색에 추가됩니다.
- 사용자 검색 기준: 목록에서 **userPrincipalName** 또는 **sAMAccountName**을 클릭합니다. 기본값은 **userPrincipalName**입니다. 등록 후 사용자 검색 기준 설정을 변경하는 경우 사용자가 다시 등록해야 합니다.
- 보안 연결 사용: 보안 연결을 사용할지 여부를 선택합니다. 기본값은 아니요입니다.

3. 저장을 클릭합니다.

LDAP 호환 디렉터리를 편집하려면

1. **LDAP** 테이블에서 편집하려는 디렉터리를 선택합니다.

디렉터리 옆에 있는 확인란을 선택하면 LDAP 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하면 목록의 오른쪽에 옵션 메뉴가 나타납니다.

2. 편집을 클릭합니다. **LDAP** 편집 페이지가 나타납니다.

Directory type*	Microsoft Active Directory	
Primary server*	10.61.	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*	.net	
User base DN*	dc=.dc=.net	?
Group base DN*	dc=.dc=.net	?
User ID*	administrator@.net	
Password*		
Domain alias*	.net	
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	NO	

3. 다음 정보를 적절하게 변경합니다.

- 디렉터리 유형: 목록에서 적절한 디렉터리 유형을 클릭합니다.
- 주 서버: LDAP 에 사용되는 주 서버를 입력합니다. IP 주소 또는 FQDN(정규화된 도메인 이름) 을 입력할 수 있습니다.
- 보조 서버: 필요한 경우 보조 서버의 IP 주소 또는 FQDN 을 입력합니다 (보조 서버가 구성된 경우).
- 포트: LDAP 서버가 사용하는 포트 번호를 입력합니다. 기본적으로 포트 번호는 보안되지 않은 LDAP 연결의 경우 **389** 로 설정됩니다. 보안 LDAP 연결에는 포트 번호 **636** 을 사용하고, Microsoft 비보안 LDAP 연결에는 **3268** 을 사용하고, Microsoft 보안 LDAP 연결에는 **3269** 를 사용하십시오.
- 도메인 이름: 이 필드를 편집할 수 없습니다.
- 사용자 기본 **DN**: 고유 식별자를 통해 Active Directory 의 사용자 위치를 입력합니다. 구문의 예로는 **ou=users,dc=example** 또는 **dc=com**이 있습니다.
- 그룹 기본 **DN**: **cn=groupname** 형식으로 지정된 그룹 기본 DN 그룹 이름을 입력합니다. 예를 들어 **cn=users**가 그룹 이름인 경우 **cn=users, dc=servername, dc=net**입니다. **DN** 및 **servername**은 Active Directory 를 실행하는 서버의 이름을 나타냅니다.
- 사용자 **ID**: Active Directory 계정과 연관된 사용자 ID 를 입력합니다.
- 암호: 사용자와 연관된 암호를 입력합니다.
- 도메인 별칭: 도메인 이름의 별칭을 입력합니다. 등록 후 도메인 별칭 설정을 변경하는 경우 사용자가 다시 등록해야 합니다.
- **XenMobile** 잠금 제한: 실패한 로그인 시도 횟수를 **0** 에서 **999** 사이의 숫자로 입력합니다. **0** 값은 XenMobile 이 실패한 로그인 시도를 기준으로 사용자를 잠그지 않음을 의미합니다.

- **XenMobile 잠금 시간:** 잠금 제한을 초과한 후 사용자가 대기해야 하는 시간 (분) 을 나타내는 **0** 에서 **99999** 사이의 숫자를 입력합니다. **0** 값은 잠금 후 사용자가 대기하지 않아도 됨을 의미합니다.
- **글로벌 카탈로그 TCP 포트:** 글로벌 카탈로그 서버의 TCP 포트 번호를 입력합니다. 기본적으로 TCP 포트 번호는 **3268** 로 설정됩니다. SSL 연결의 경우 포트 번호 **3269** 를 사용하십시오.
- **글로벌 카탈로그 루트 컨텍스트:** 필요한 경우 Active Directory 의 글로벌 카탈로그 검색을 사용하도록 설정하는 데 사용되는 글로벌 루트 컨텍스트 값을 입력합니다. 이 검색은 실제 도메인 이름을 지정할 필요가 없는 모든 도메인에서 표준 LDAP 검색에 추가됩니다.
- **사용자 검색 기준:** 목록에서 **userPrincipalName** 또는 **sAMAccountName** 을 클릭합니다. 등록 후 사용자 검색 기준 설정을 변경하는 경우 사용자가 다시 등록해야 합니다.
- **보안 연결 사용:** 보안 연결을 사용할지 여부를 선택합니다.

4. 저장을 클릭하여 변경 내용을 저장하거나 취소를 클릭하여 속성을 변경하지 않고 그대로 유지합니다.

LDAP 호환 디렉터리를 삭제하려면

1. **LDAP** 테이블에서 삭제하려는 디렉터리를 선택합니다.

각 속성 옆에 있는 확인란을 선택하여 삭제할 속성을 둘 이상 선택할 수 있습니다.

2. 삭제를 클릭합니다. 확인 대화 상자가 나타납니다. 삭제를 다시 클릭합니다.

여러 도메인에 대한 인증 구성

LDAP 구성에서 여러 도메인 접미사를 사용하도록 XenMobile Server 를 구성하려면 Citrix Endpoint Management 설명서에서 [여러 도메인에 대한 인증 구성](#)의 절차를 참조하십시오. 이러한 단계는 온-프레미스 버전의 XenMobile Server 와 Endpoint Management 클라우드 릴리스에서 동일합니다.

도메인과 보안 토큰 인증 구성

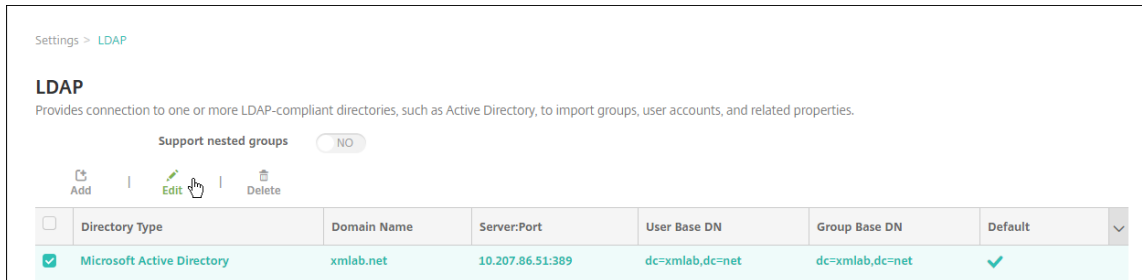
RADIUS 프로토콜을 사용하여 사용자가 LDAP 자격 증명과 일회용 암호를 사용하여 인증하도록 XenMobile 을 구성할 수 있습니다.

사용 편의성을 최적화하기 위해 이 구성을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다. 이 구성에서는 사용자가 LDAP 사용자 이름과 암호를 반복적으로 입력하지 않아도 됩니다. 등록, 암호 만료 및 계정 잠금의 경우 사용자가 사용자 이름과 암호를 입력합니다.

LDAP 설정 구성

인증에 LDAP 를 사용하려면 XenMobile 에 인증 기관에서 발급한 SSL 인증서를 설치해야 합니다. 자세한 내용은 [XenMobile 에서 인증서 업로드](#)를 참조하십시오.

1. 설정에서 **LDAP** 를 클릭합니다.
2. **Microsoft Active Directory** 를 선택한 다음 편집을 클릭합니다.

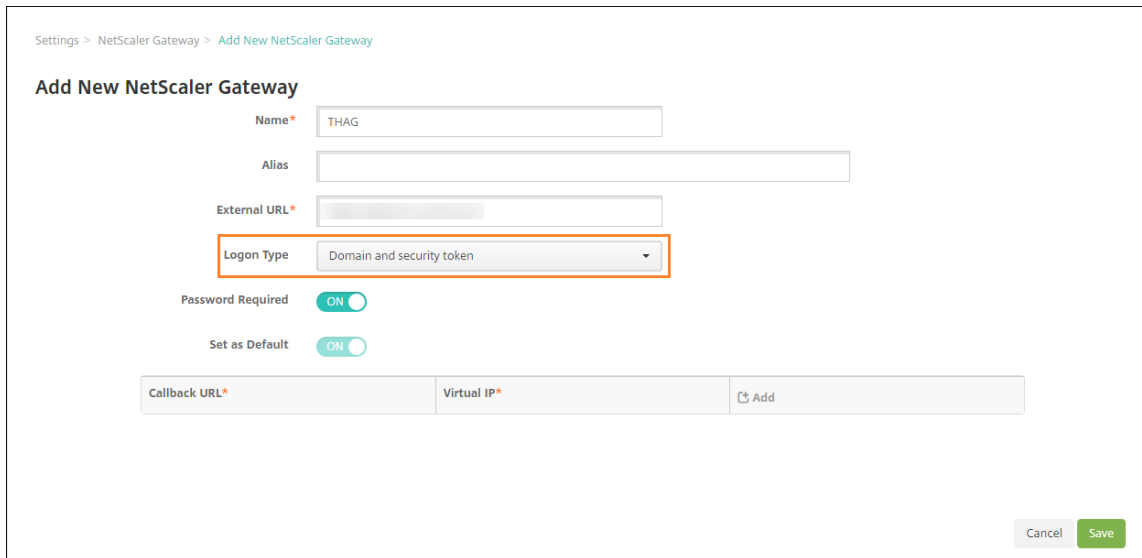


3. 포트가 **636**(보안 LDAP 연결의 경우) 또는 **3269**(Microsoft 보안 LDAP 연결의 경우) 인지 확인합니다.
4. 보안 연결 사용을 예로 변경합니다.

Citrix Gateway 설정 구성

다음 단계에서는 이미 Citrix Gateway 인스턴스를 XenMobile 에 추가했다고 가정합니다. Citrix Gateway 인스턴스를 추가하려면 [Citrix Gateway 인스턴스 추가](#)를 참조하십시오.

1. 설정에서 **Citrix Gateway** 를 클릭합니다.
2. **Citrix Gateway** 를 선택하고 편집을 클릭합니다.
3. 로그인 유형에서 도메인 및 보안 토큰을 선택합니다.



Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name * THAG

Alias

External URL *

Logon Type Domain and security token

Password Required ON

Set as Default ON

Callback URL * Virtual IP * Add

Cancel Save

Citrix PIN 및 사용자 암호 캐싱 사용

Citrix PIN 및 사용자 암호 캐싱을 사용하도록 설정하려면 설정 > 클라이언트 속성으로 이동하여 **Enable Citrix PIN Authentication(Citrix PIN 인증 사용)** 및 **Enable User Password Caching(사용자 암호 캐싱 사용)** 확인란을 선택합니다. 자세한 내용은 [클라이언트 속성](#)을 참조하십시오.

도메인 및 보안 토큰 인증을 위해 Citrix Gateway 구성

XenMobile 과 함께 사용되는 가상 서버에 대한 Citrix Gateway 세션 프로필 및 정책을 구성합니다. 자세한 내용은 Citrix Gateway 설명서를 참조하십시오.

클라이언트 인증서 인증 또는 인증서와 도메인 인증

November 1, 2023

XenMobile 에 대한 기본 구성은 사용자 이름 및 암호 인증입니다. XenMobile 환경에 대한 등록 및 액세스 시 추가 보안 계층을 추가하려면 인증서 기반 인증을 사용하는 것이 좋습니다. XenMobile 환경에서 이 구성은 보안과 사용자 환경을 모두 고려한 최고의 조합입니다. 인증서 인증과 도메인 인증을 함께 사용하면 SSO 를 사용하는 동시에 Citrix ADC 의 2 단계 인증을 통해 강화된 보안이 적용됩니다.

사용 편의성을 최적화하기 위해 인증서 및 도메인 인증을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다. 그러면 사용자가 LDAP 사용자 이름과 암호를 반복적으로 입력하지 않아도 됩니다. 등록, 암호 만료 및 계정 잠금의 경우 사용자가 사용자 이름과 암호를 입력합니다.

중요:

XenMobile 은 사용자가 XenMobile 에서 장치를 등록한 후 도메인 인증에서 다른 인증 모드로의 인증 모드 변경을 지원하지 않습니다.

LDAP 를 허용하지 않고 스마트 카드 또는 유사한 방법을 사용하는 경우 인증서를 구성하면 XenMobile 에 스마트 카드를 나타낼 수 있습니다. 그런 다음 사용자는 XenMobile 에서 생성된 고유한 PIN 을 사용하여 등록합니다. 사용자가 액세스 권한을 획득하면 XenMobile 이 XenMobile 환경에 인증하는 데 사용될 인증서를 만들어 배포합니다.

Citrix ADC 인증서 전용 인증 또는 인증서 및 도메인 인증을 사용하는 경우 XenMobile 용 Citrix ADC 마법사를 통해 XenMobile 에 필요한 구성을 수행할 수 있습니다. XenMobile 용 Citrix ADC 마법사는 한 번만 실행할 수 있습니다.

보안이 매우 중요한 환경에서는 조직 외부의 공용 네트워크 또는 보안되지 않은 네트워크에서 LDAP 자격 증명을 사용하는 것이 조직에 큰 보안 위협으로 간주됩니다. 이러한 환경에서는 클라이언트 인증서와 보안 토큰을 사용하는 2 단계 인증을 선택할 수 있습니다. 자세한 내용은 [Configuring XenMobile for Certificate and Security Token Authentication\(인증서 및 보안 토큰 인증을 사용하기 위한 XenMobile 구성\)](#)을 참조하십시오.

클라이언트 인증서 인증은 XenMobile MAM 모드 (MAM 단독) 및 ENT 모드 (사용자가 MDM 으로 등록 시) 에 사용할 수 있습니다. 하지만 사용자가 레거시 MAM 모드로 등록하는 경우 클라이언트 인증서 인증을 XenMobile ENT 모드에 사용할 수 없습니다. XenMobile ENT 및 MAM 모드로 클라이언트 인증서 인증을 사용하려면 Microsoft 서버와 XenMobile Server 를 구성한 후 Citrix Gateway 를 구성해야 합니다. 이 문서에 설명된 대로 다음의 일반적인 단계를 따릅니다.

Microsoft 서버:

1. Microsoft Management Console 에 인증서 스냅인을 추가합니다.
2. CA(인증 기관) 에 템플릿을 추가합니다.
3. CA 서버에서 PFX 인증서를 만듭니다.

XenMobile Server:

1. XenMobile 에 인증서를 업로드합니다.
2. 인증서 기반 인증을 위한 PKI 엔터티를 만듭니다.
3. 자격 증명 공급자를 구성합니다.
4. 인증을 위한 사용자 인증서를 제공하도록 Citrix Gateway 를 구성합니다.

Citrix Gateway 구성에 대한 자세한 내용은 Citrix ADC 설명서의 다음 문서를 참조하십시오.

- [Client authentication\(클라이언트 인증\)](#)
- [SSL profile infrastructure\(SSL 프로파일 인프라\)](#)
- [Configuring and Binding a Client Certificate Authentication Policy\(클라이언트 인증서 인증 구성 및 바인딩\)](#)

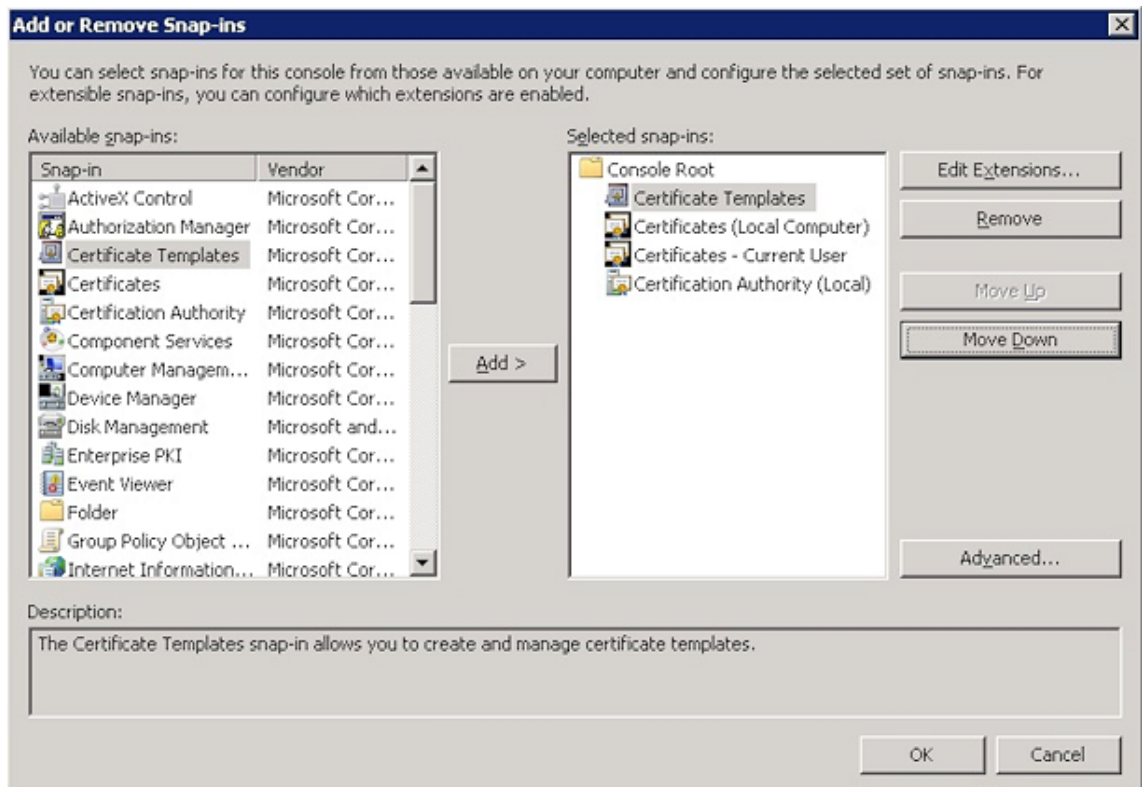
사전 요구 사항

- Microsoft 인증서 서비스 엔터티 템플릿을 생성할 때는 특수 문자를 제외하여 등록된 장치와 관련된 인증 문제를 방지하십시오. 예를 들어 템플릿 이름에 다음 문자를 사용하지 마십시오. : ! \$ () # % + * ~ ? | { } []

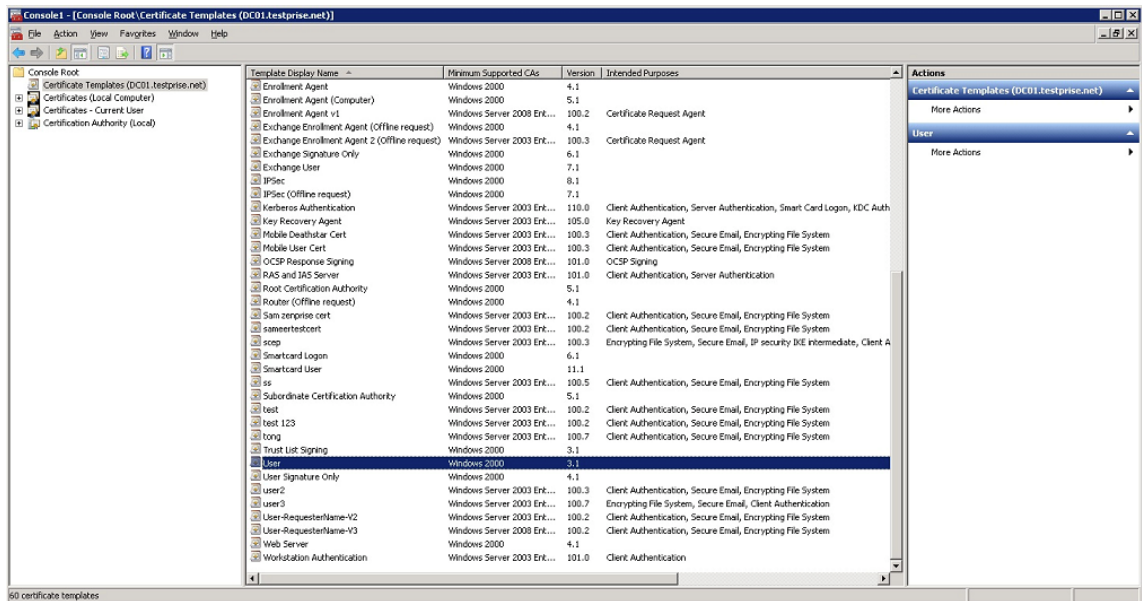
- Exchange ActiveSync 에 대한 인증서 기반 인증을 구성하려면 이 [Microsoft 블로그](#)를 참조하십시오. 클라이언트 인증서를 요구하도록 Exchange ActiceSync 의 인증 기관 (CA) 서버 사이트를 구성합니다..
- Exchange Server 로의 ActiveSync 트래픽을 보안하기 위해 개인 서버 인증서를 사용하는 경우, 필요한 모든 루트 및 중간 인증서가 모바일 장치에 있어야 합니다. 그렇지 않으면 Secure Mail 에서 사서함을 설정하는 동안 인증서 기반 인증이 실패합니다. Exchange IIS 콘솔에서 다음 작업을 수행해야 합니다.
 - Exchange 와 함께 XenMobile 을 사용하기 위한 웹 사이트를 추가하고 웹 서버 인증서를 바인딩합니다.
 - 포트 9443 을 사용합니다.
 - 해당 웹 사이트에 대해 “Microsoft Server ActiveSync” 용 하나와 “EWS” 용 하나의 두 가지 응용 프로그램을 추가해야 합니다. 이러한 응용 프로그램 모두에 대해 **SSL** 설정 아래에서 **SSL** 필요를 선택합니다.

Microsoft Management Console 에 인증서 스냅인을 추가합니다

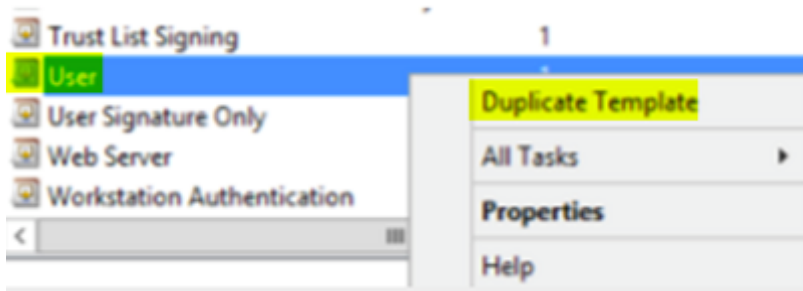
1. 콘솔을 열고 스냅인 추가/제거를 클릭합니다.
2. 다음과 같은 스냅인을 추가합니다.
 - 인증서 템플릿
 - 인증서 (로컬 컴퓨터)
 - 인증서 - 현재 사용자
 - 인증 기관 (로컬)



3. 인증서 템플릿을 확장합니다.



4. 사용자 템플릿과 템플릿 복제를 선택합니다.



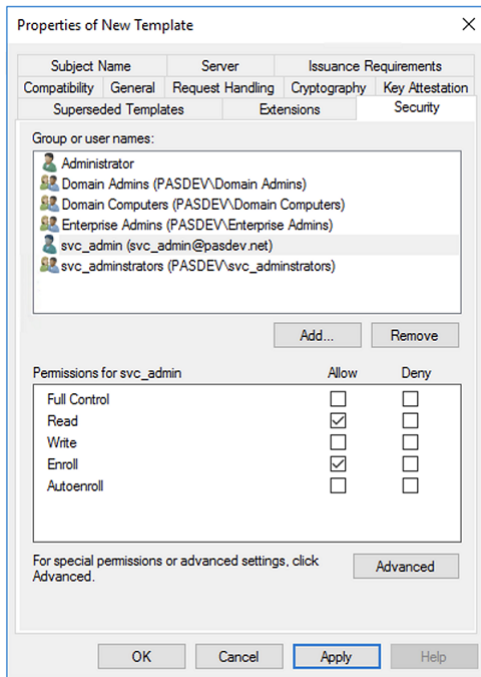
5. 템플릿 표시 이름을 제공합니다.

중요:

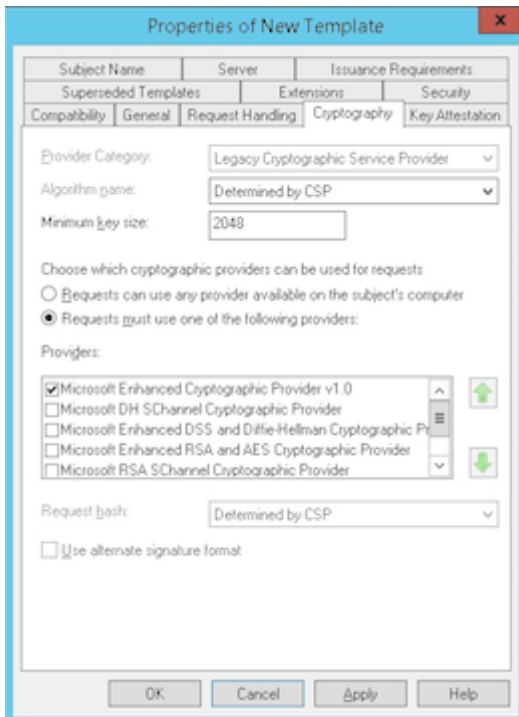
필요한 경우에만 **Active Directory**에 인증서 게시 확인란을 선택합니다. 이 옵션을 선택하면 모든 사용자 클라이언트 인증서가 Active Directory에서 생성되어 Active Directory 데이터베이스가 복잡해질 수 있습니다.

6. 템플릿 유형으로 **Windows 2003 Server**를 선택합니다. Windows 2012 R2 서버에서 호환성 아래에 있는 인증 기관을 선택하고 받는 사람을 **Windows 2003**으로 설정합니다.

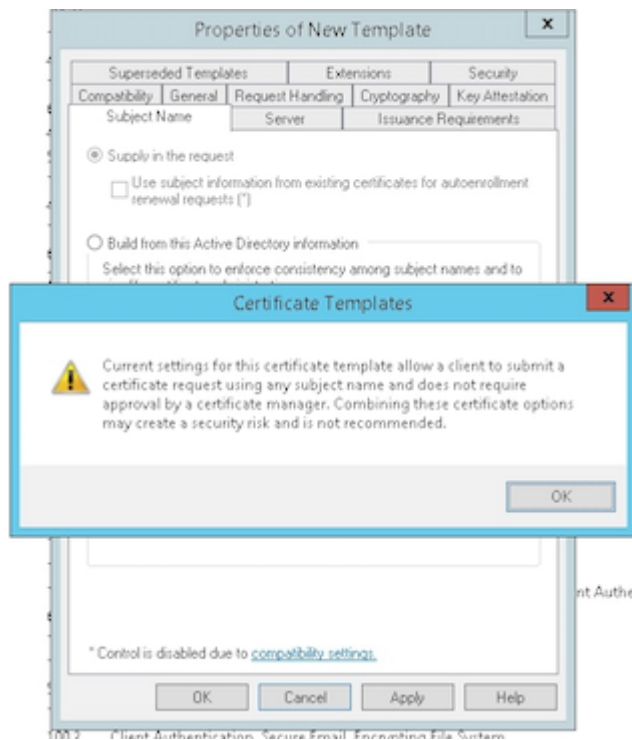
7. 보안에서 XenMobile Server용 PKI 엔티티 설정으로 구성된 특정 사용자 또는 PKI 엔티티 설정으로 구성된 사용자가 있는 사용자 그룹에 대해 허용 열의 등록 옵션을 선택합니다.



8. 암호화 아래에서 키 크기를 제공하는지 확인합니다. 키 크기는 나중에 XenMobile 을 구성할 때 입력합니다.

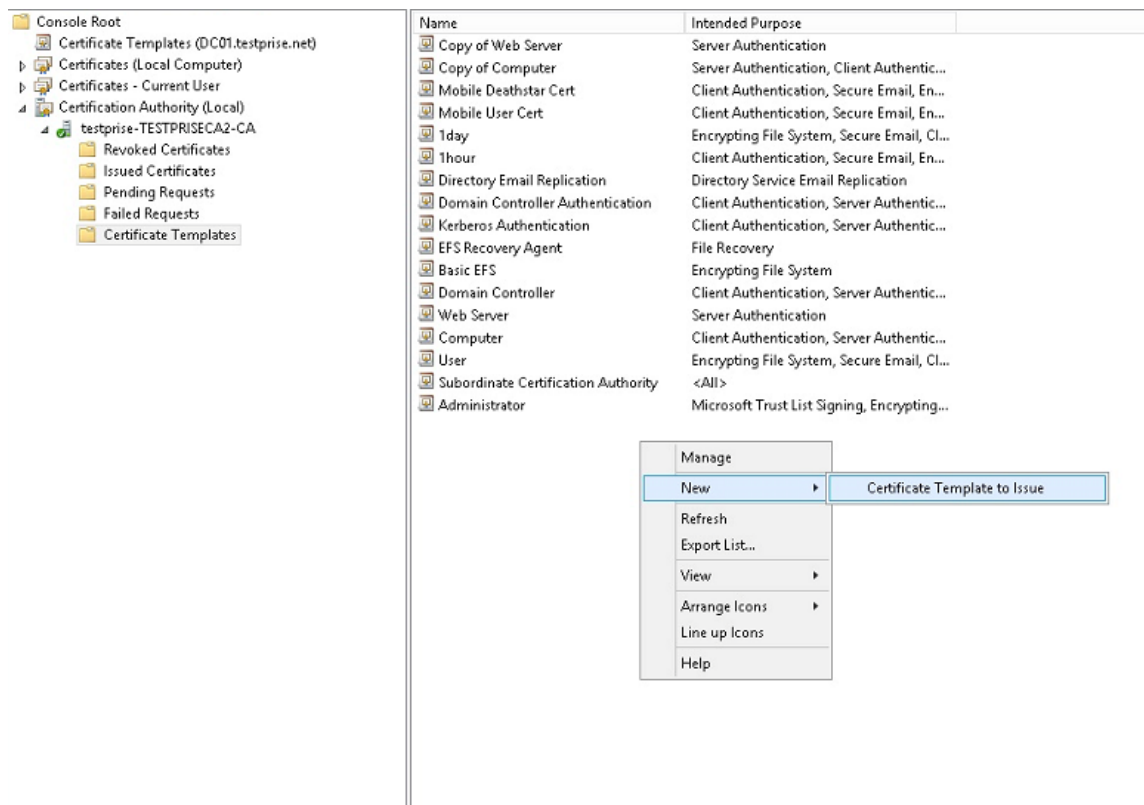


9. 주체 이름 아래에서 요청에서 제공을 선택합니다. 변경 내용을 적용한 후 저장합니다.

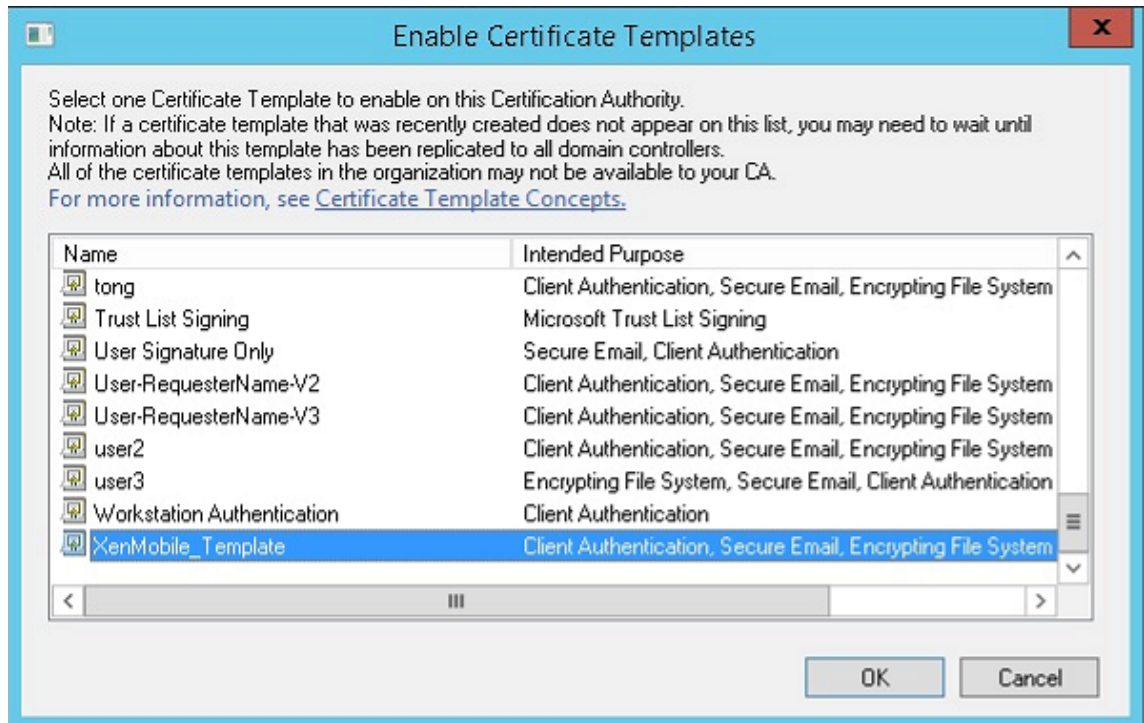


인증 기관에 템플릿 추가

1. 인증 기관으로 이동하여 인증서 템플릿을 선택합니다.
2. 오른쪽 창에서 마우스 오른쪽 단추를 클릭한 후 새로 만들기 > 발급할 인증서 템플릿을 선택합니다.

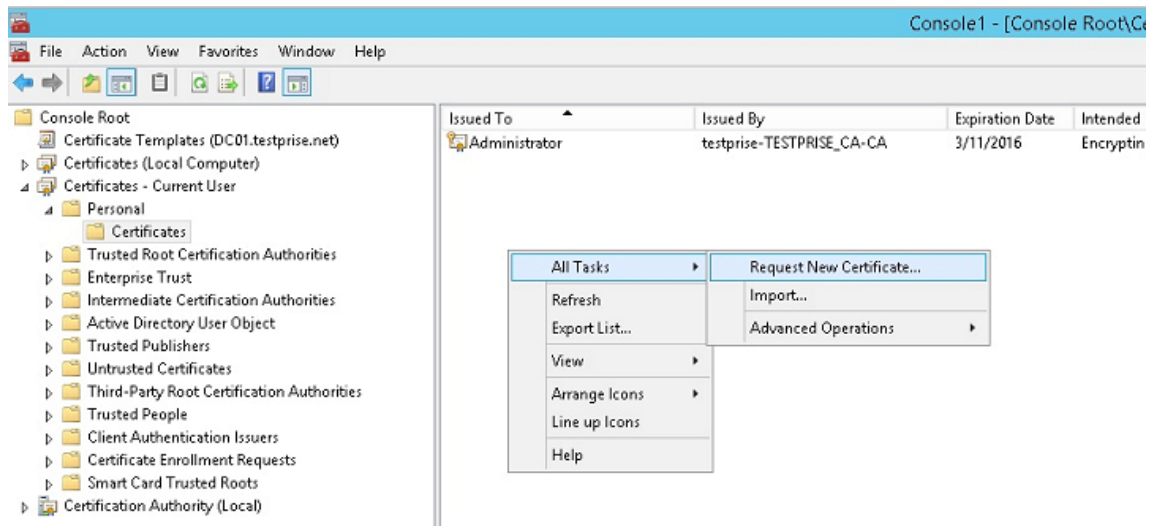


- 이전 단계에서 만든 템플릿을 선택한 다음 확인을 클릭하여 인증 기관에 추가합니다.

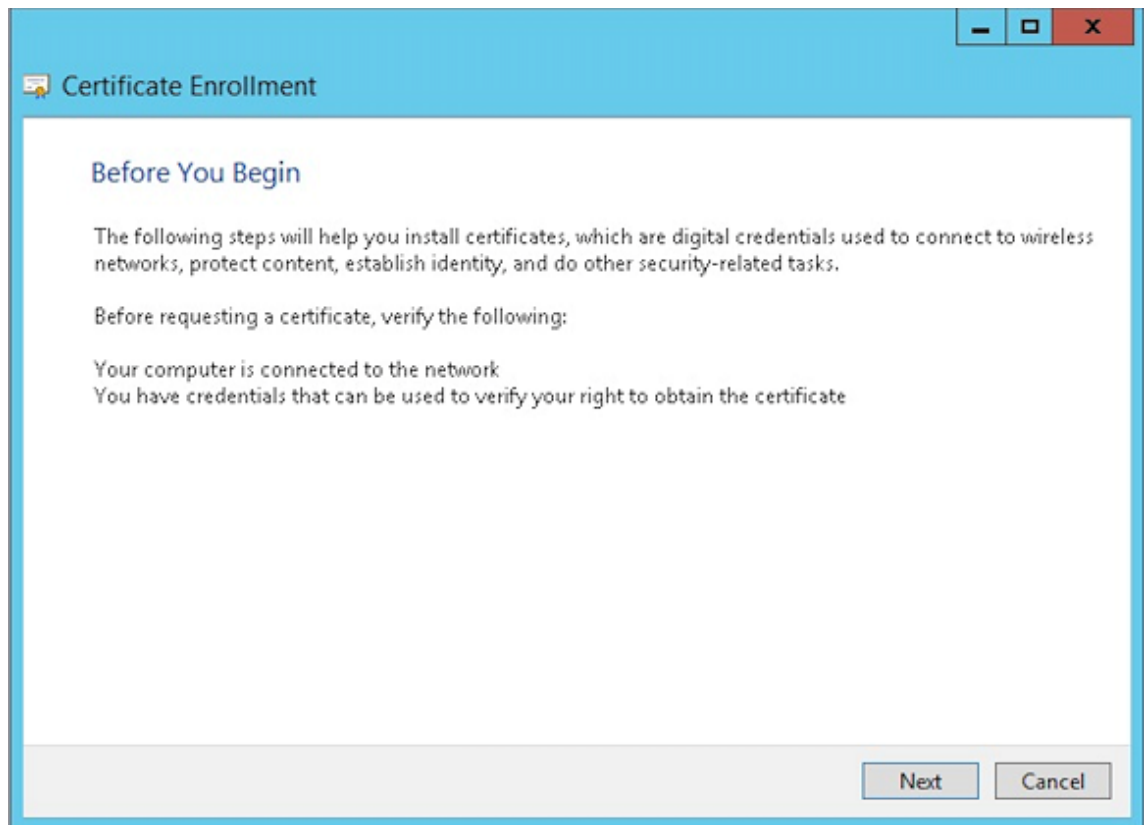


CA 서버에서 PFX 인증서 만들기

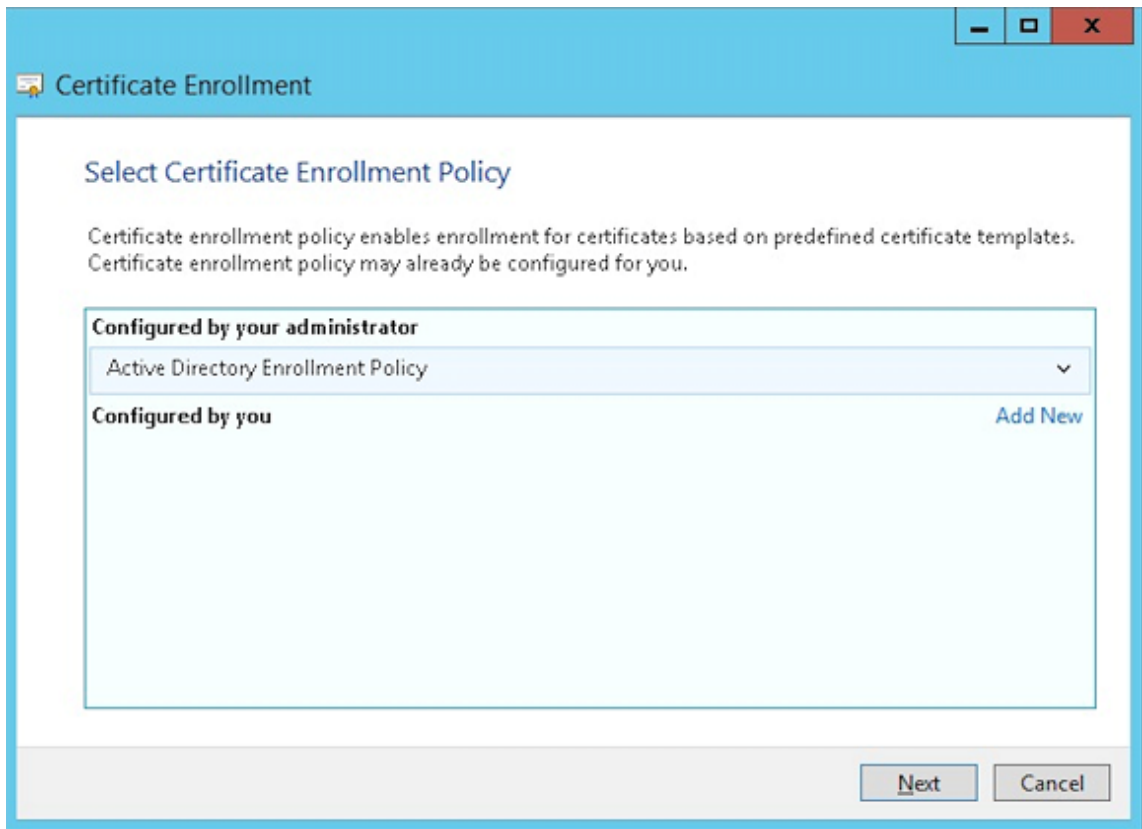
1. 로그인한 서비스 계정을 사용하여 사용자.pfx 인증서를 만듭니다. .pfx 를 XenMobile 에 업로드하면 XenMobile 이 장치를 등록하는 사용자에게 사용자 인증서를 요구하게 됩니다.
2. 현재 사용자 아래에서 인증서를 확장합니다.
3. 오른쪽 창을 마우스 오른쪽 단추로 클릭하고 새 인증서 요청을 클릭합니다.



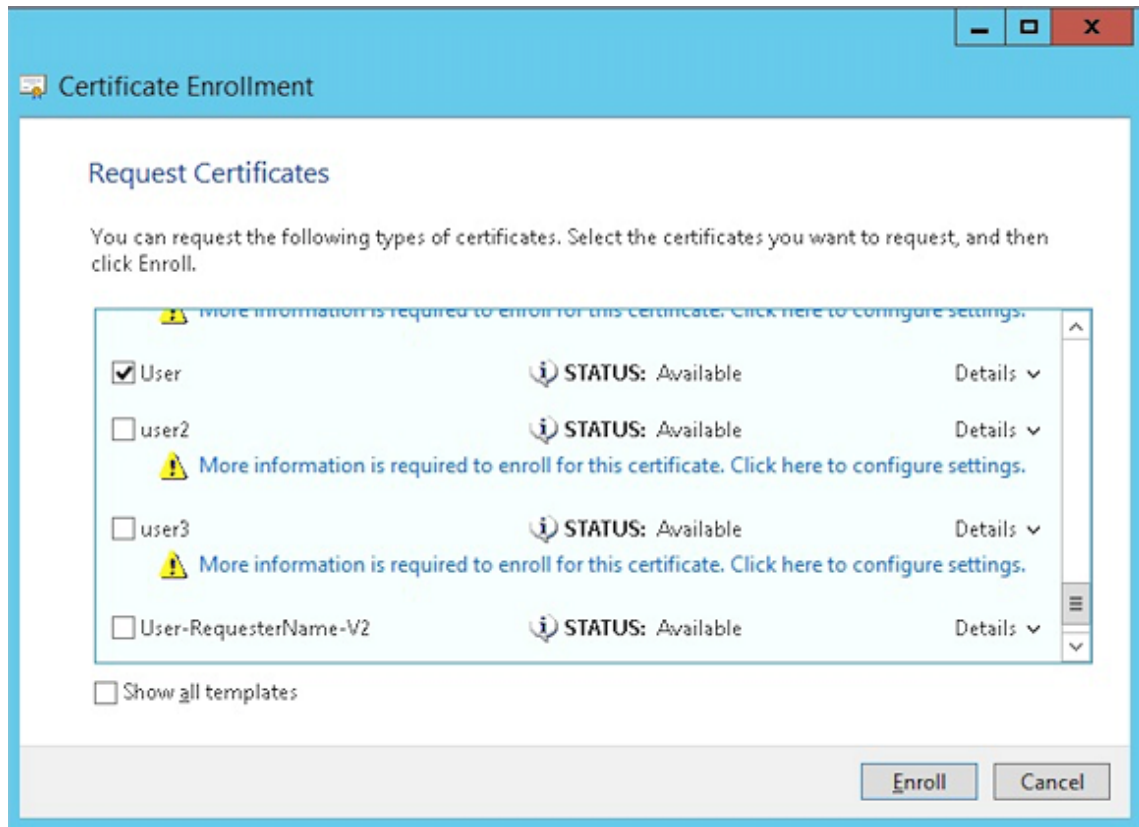
4. 인증서 등록 화면이 나타납니다. 다음을 클릭합니다.



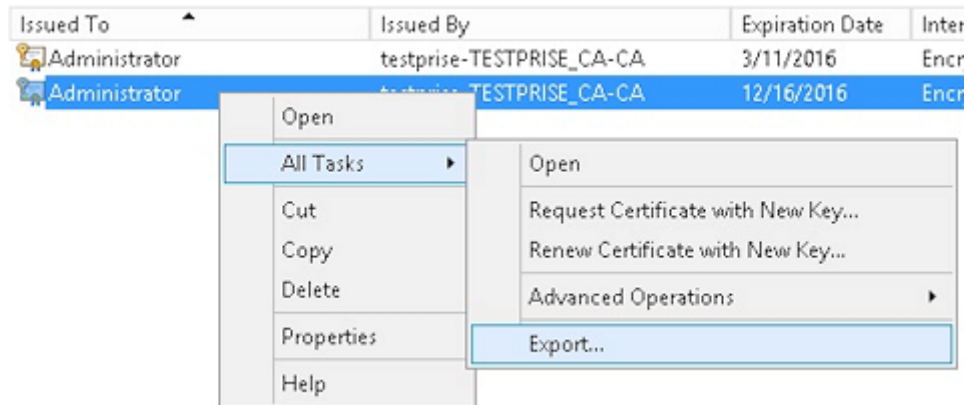
5. **Active Directory** 등록 정책을 선택하고 다음을 클릭합니다.



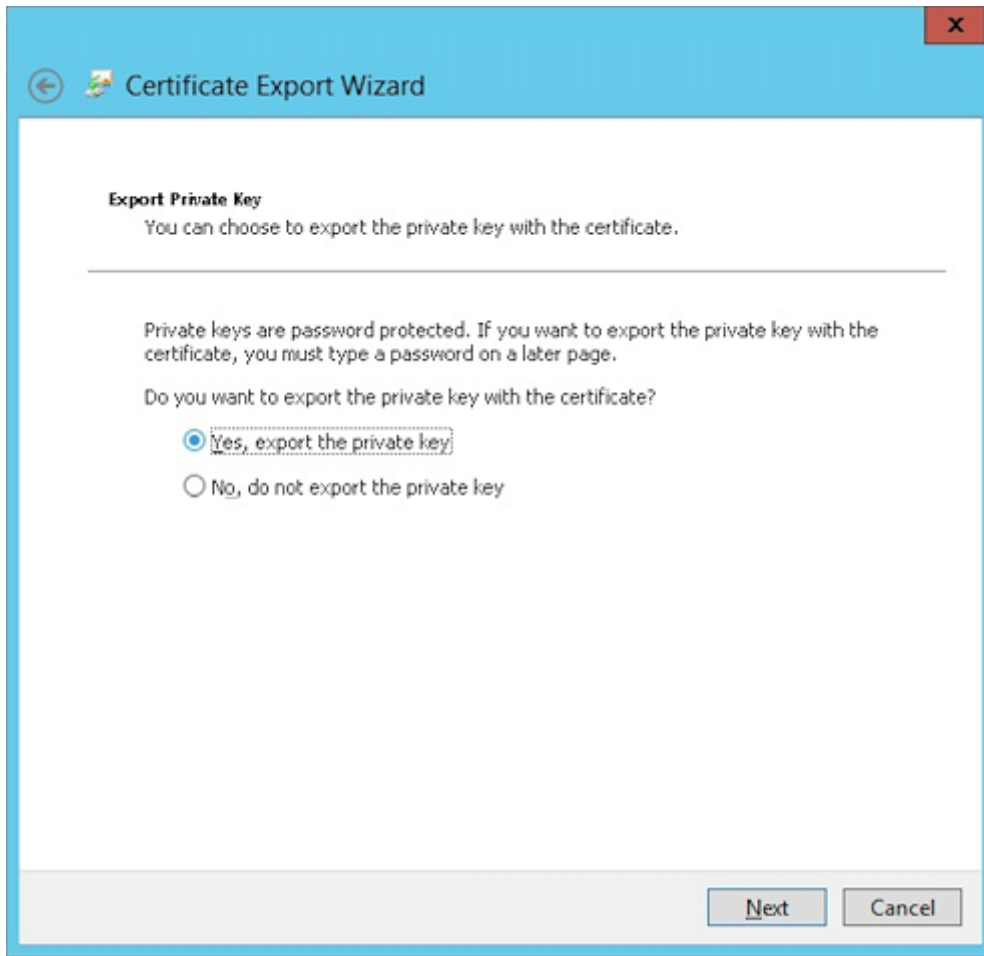
6. 사용자 템플릿을 선택한 후 등록을 클릭합니다.



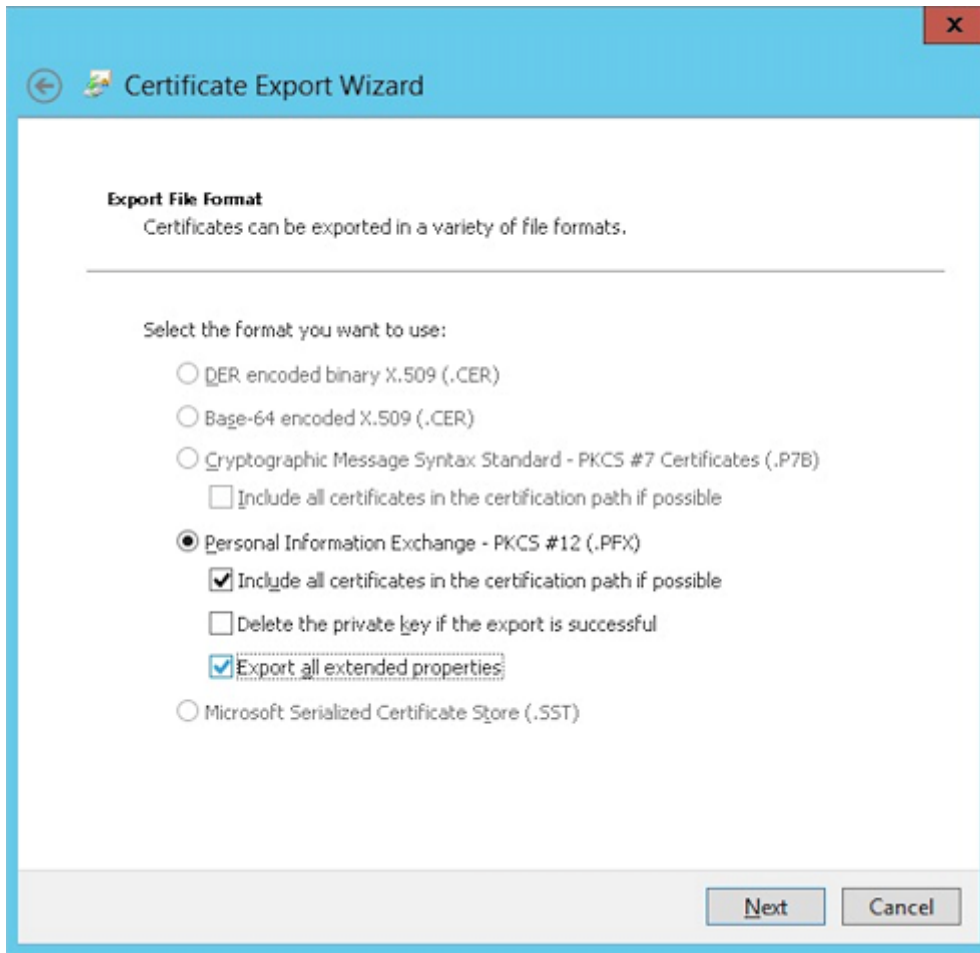
7. 이전 단계에서 만든.pfx 파일을 내보냅니다.



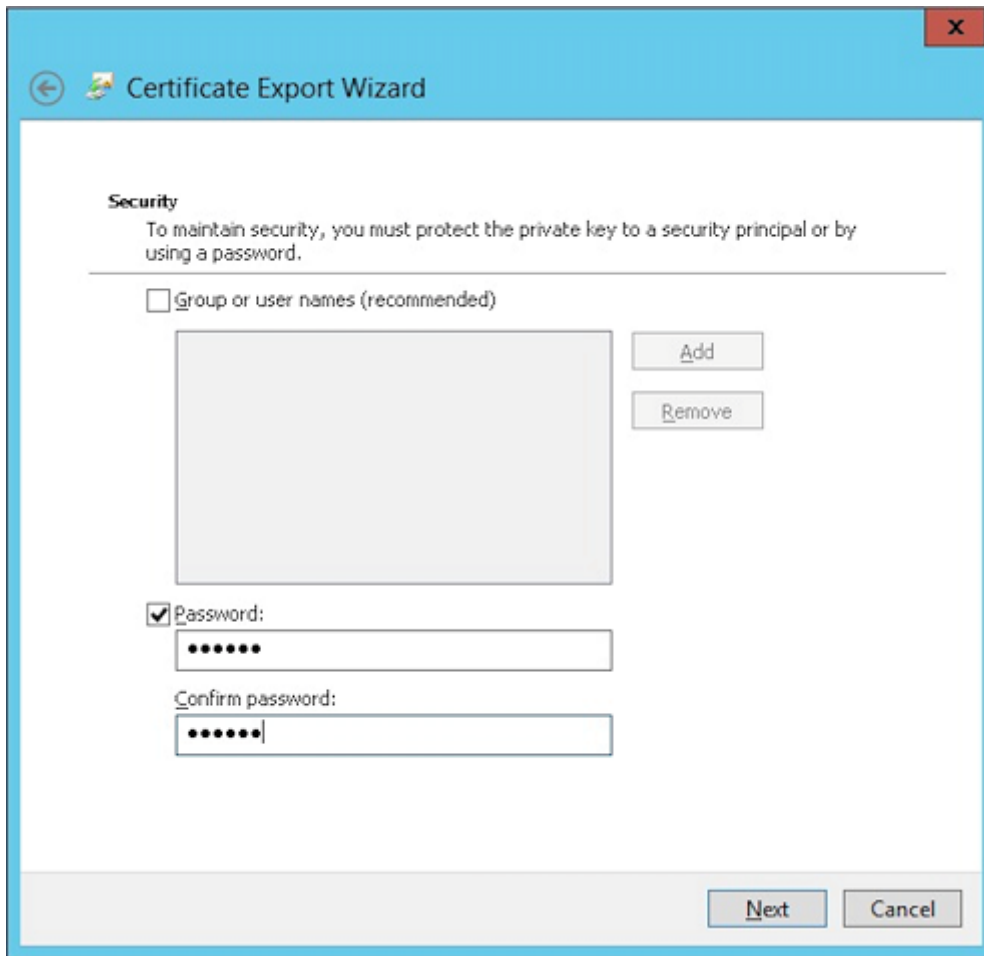
8. 예, 개인 키를 내보냅니다를 클릭합니다.



9. 가능하면 인증 경로에 있는 인증서 모두 포함 및 확장 속성 모두 내보내기 확인란을 선택합니다.



10. XenMobile 에 이 인증서를 업로드할 때 사용할 암호를 설정합니다.



11. 하드 드라이브에 인증서를 저장합니다.

XenMobile 에 인증서 업로드

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 화면이 나타납니다.
2. 인증서를 클릭한 후 가져오기를 클릭합니다.
3. 다음 매개 변수를 입력합니다.
 - 가져오기: 키 저장소
 - 키 저장소 유형: PKCS #12
 - 용도: 서버
 - 키 저장소 파일: 찾아보기를 클릭하여 만들어 둔 .pfx 인증서를 선택합니다.
 - 암호: 이 인증서에 대해 만든 암호를 입력합니다.

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import

Keystore

Keystore type

PKCS#12

Use as

Server

Keystore file*

Browse

Password*

Description

Cancel

Import

4. 가져오기를 클릭합니다.

5. 인증서가 올바르게 설치되었는지 확인합니다. 올바르게 설치된 인증서가 사용자 인증서로 표시됩니다.

인증서 기반 인증을 위한 **PKI** 엔터티 만들기

1. 설정에서 자세히 > 인증서 관리 > **PKI** 엔터티로 이동합니다.
2. 추가를 클릭한 후 **Microsoft** 인증서 서비스 엔터티를 클릭합니다. **Microsoft** 인증서 서비스 엔터티: 일반 정보 화면이 나타납니다.
3. 다음 매개 변수를 입력합니다.
 - 이름: 원하는 이름을 입력합니다.
 - 웹 등록 서비스 루트 **URL**: **https://RootCA-URL/certsrv/** URL 경로에서 마지막 슬래시 (/) 를 반드시 추가해야 합니다.
 - **certnew.cer** 페이지 이름: certnew.cer(기본값)
 - **certfnsh.asp**: certfnsh.asp(기본값)
 - 인증 유형: 클라이언트 인증서
 - **SSL** 클라이언트 인증서: XenMobile 클라이언트 인증서를 발급하는 데 사용할 사용자 인증서를 선택합니다.

Settings > PKI Entities > Microsoft Certificate Services Entity

Microsoft Certificate Services Entity

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

Microsoft Certificate Services Entity: General Information

Name* test

Web enrollment service root URL* https:// /certsrv/

certnew.cer page name* certnew.cer

certfnsh.asp* certfnsh.asp

Authentication type Client certificate

SSL client certificate Select an option

Import SSL certificate

4. 템플릿 아래에서 Microsoft 인증서를 구성할 때 만든 템플릿을 추가합니다. 공백을 추가하지 마십시오.

Microsoft Certificate Services Entity

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

Microsoft Certificate Services Entity: Templates

Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.

Templates	
Templates*	⚙ Add
XVTemplate	

5. HTTP 매개 변수를 생략하고 **CA** 인증서를 클릭합니다.
6. 사용자 환경에 해당하는 루트 CA 이름을 선택합니다. 이 루트 CA 는 XenMobile 클라이언트 인증서에서 가져온 체인의 일부입니다.

Microsoft Certificate Services Entity

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

Microsoft Certificate Services Entity: CA Certificates

Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

<input type="checkbox"/>	Name	Serial number	Valid from	Valid to
<input checked="" type="checkbox"/>	training-AD-CA		02/22/2013	02/22/2023

7. 저장을 클릭합니다.

자격 증명 공급자 구성

- 설정에서 자세히 > 인증서 관리 > 자격 증명 공급자로 이동합니다.
- 추가를 클릭합니다.
- 일반 아래에서 다음 매개 변수를 입력합니다.
 - 이름: 원하는 이름을 입력합니다.
 - 설명: 원하는 설명을 입력합니다.
 - 발급 엔터티: 이전에 만든 PKI 엔터티를 선택합니다.
 - 발급 방법: 서명

- 템플릿: PKI 엔터티 아래에서 추가한 템플릿을 선택합니다.

Credential Providers	Credential Providers: General Information
1 General	<p>You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.</p> <p>Name* <input type="text" value="XenMobile_PKI"/></p> <p>Description <input type="text" value="XenMobile PKI Configuration"/></p> <p>Issuing entity <input type="text" value="MS PKI"/></p> <p>Issuing method <input type="text" value="SIGN"/></p> <p>Templates <input type="text" value="XMTemplates"/></p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	
5 Revocation PKI	
6 Renewal	

4. CSR 을 클릭한 후 다음 매개 변수를 입력합니다.

- 키 알고리즘: RSA
- 키 크기: 2048
- 서명 알고리즘: SHA256withRSA
- 주체 이름 `cn=$user.username`

주체 대체 이름에 대해 추가를 클릭한 후 다음 매개 변수를 입력합니다.

- 유형: 사용자 계정 이름
- 값: `$user.userprincipalname`

Credential Providers	Credential Providers: Certificate Signing Request						
1 General	<p>Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.</p> <p>Key algorithm <input type="text" value="RSA"/></p> <p>Key size* <input type="text" value="2048"/></p> <p>Signature algorithm <input type="text" value="SHA1withRSA"/></p> <p>Subject name* <input type="text" value="cn=\$user.username"/></p> <p>Subject alternative names</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Value*</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>User Principal name</td> <td>\$user.userprincipalname</td> <td><input type="button" value="Add"/></td> </tr> </tbody> </table>	Type	Value*	Add	User Principal name	\$user.userprincipalname	<input type="button" value="Add"/>
Type		Value*	Add				
User Principal name		\$user.userprincipalname	<input type="button" value="Add"/>				
2 Certificate Signing Request							
3 Distribution							
4 Revocation XenMobile							
5 Revocation PKI							
6 Renewal							

5. 배포를 클릭한 후 다음 매개 변수를 입력합니다.

- CA 인증서 발급: XenMobile 클라이언트 인증서에 서명한 발급 CA 를 선택합니다.
- 배포 모드 선택: 중앙 집중식 선호: 서버측 키 생성을 선택합니다.

Credential Providers	Credential Providers: Distribution
1 General	<p>Issuing CA certificate <input type="text" value="CN=training-AD-CA, Serial:"/></p> <p>Select distribution mode</p> <p><input checked="" type="radio"/> Prefer centralized: Server-side key generation</p> <p><input type="radio"/> Prefer distributed: Device-side key generation</p> <p><input type="radio"/> Only distributed: Device-side key generation</p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	

6. 그 다음의 두 섹션, 즉 해지 **XenMobile** 및 해지 **PKI** 에 대해 필요에 따라 매개 변수를 설정합니다. 이 예에서는 두 옵션을 모두 건너뜁니다.
7. 갱신을 클릭합니다.
8. 인증서가 만료될 때 갱신에 대해 커짐을 선택합니다.
9. 다른 모든 설정을 기본값으로 그대로 두거나 필요에 따라 변경합니다.

Credential Providers	Credential Providers: Renewal
1 General	Renew certificates when they expire <input checked="" type="checkbox"/>
2 Certificate Signing Request	Renew when the certificate comes within* <input type="text" value="30"/> days of expiration
3 Distribution	<input type="checkbox"/> Do not renew certificates that have already expired
4 Revocation XenMobile	Send notification <input type="checkbox"/>
5 Revocation PKI	Notify when the certificate nears expiration <input type="checkbox"/>
6 Renewal	

10. 저장을 클릭합니다.

인증서 기반 인증을 사용하도록 **Secure Mail** 구성

Secure Mail 을 XenMobile 에 추가할 경우, 앱 설정 아래에서 Exchange 설정을 구성해야 합니다.

MDX	
1 App Information	App Interaction
2 Platform	Explicit logoff notification <input type="text" value="Shared devices only"/>
<input checked="" type="checkbox"/> iOS	App Settings
<input checked="" type="checkbox"/> Android	WorxMail Exchange Server <input type="text" value="mail.testlab.com:9443"/>
<input checked="" type="checkbox"/> Windows Phone	WorxMail user domain <input type="text" value="testlab.com"/>
3 Approvals (optional)	Background network services <input type="text" value="mail.testlab.com:443.ap-southeast-1.pushre"/>
4 Delivery Group Assignments (optional)	Background services ticket expiration <input type="text" value="168"/>

XenMobile 에서 **Citrix ADC** 인증서 제공 구성

1. XenMobile 콘솔에 로그인하고 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 화면이 나타납니다.
2. 서버 아래에서 **Citrix Gateway** 를 클릭합니다.
3. Citrix Gateway 가 아직 추가되지 않은 경우 추가를 클릭하고 설정을 지정합니다.

- 외부 **URL**: <https://YourCitrixGatewayURL>
- 로그인 유형: 인증서 및 도메인

- 암호 필요: 꺼짐
- 기본값으로 설정: 켜짐

4. 인증을 위한 사용자 인증서 제공에서 켜짐을 선택합니다.

The screenshot shows the 'NetScaler Gateway' configuration page. The 'Authentication' toggle is turned ON. Below it, the 'Deliver user certificate for authentication' toggle is also turned ON and is highlighted with a red rectangle. A 'Credential provider' dropdown menu is set to 'Select provid...'. A green 'Save' button is visible. At the bottom, there is a table with columns: Name, Default, External URL, Logon Type, and # of Callback URLs. The table is currently empty.

5. 자격 증명 공급자에서 공급자를 선택한 다음 저장을 클릭합니다.

6. 사용자 인증서에서 UPN(사용자 계정 이름) 대신 sAMAccount 특성을 사용하려면 XenMobile 에서 LDAP 커넥터를 다음과 같이 구성합니다. 설정 > **LDAP** 로 이동한 후 디렉터리를 선택하고 편집을 클릭한 다음 사용자 검색 기준에서 **sAMAccountName** 을 선택합니다.

User base DN*	<input type="text"/>	?
Group base DN*	<input type="text"/>	?
User ID*	<input type="text"/>	
Password*	<input type="password"/>	
Domain alias*	<input type="text"/>	
XenMobile Lockout Limit	<input type="text" value="0"/>	?
XenMobile Lockout Time	<input type="text" value="1"/>	?
Global Catalog TCP Port	<input type="text" value="3268"/>	?
Global Catalog Root Context	<input type="text" value="dc=example,dc=com"/>	?
User search by	<input type="text" value="sAMAccountName"/>	
Use secure connection	<input type="checkbox"/> NO	

Citrix PIN 및 사용자 암호 캐싱 사용

Citrix PIN 및 사용자 암호 캐싱을 사용하도록 설정하려면 설정 > 클라이언트 속성으로 이동하여 **Enable Citrix PIN Authentication(Citrix PIN 인증 사용)** 및 **Enable User Password Caching(사용자 암호 캐싱 사용)** 확인란을 선택합니다. 자세한 내용은 [클라이언트 속성](#)을 참조하십시오.

클라이언트 인증서 구성 문제 해결

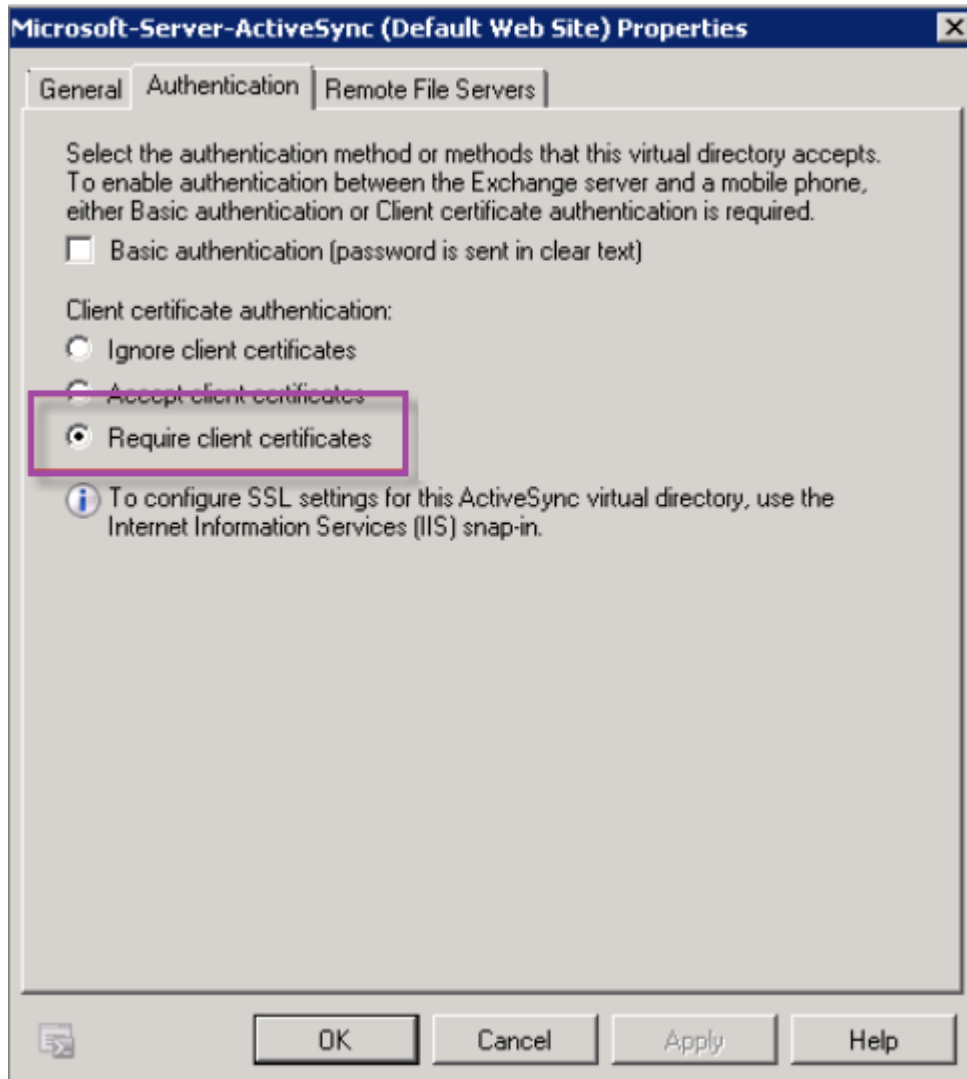
위의 구성과 Citrix Gateway 구성을 성공적으로 완료한 후 사용자 워크플로는 다음과 같습니다.

1. 사용자가 모바일 장치를 등록합니다.
2. XenMobile 에서 Citrix PIN 을 만들라는 메시지를 사용자에게 표시합니다.
3. 그런 다음 사용자가 XenMobile Store 로 리디렉션됩니다.
4. 사용자가 Secure Mail 을 시작할 때는 XenMobile 이 사서함 구성을 위한 사용자 자격 증명을 입력하라는 메시지를 표시하지 않습니다. 대신 Secure Mail 이 Secure Hub 에서 클라이언트 인증서를 요청하고 인증을 위해

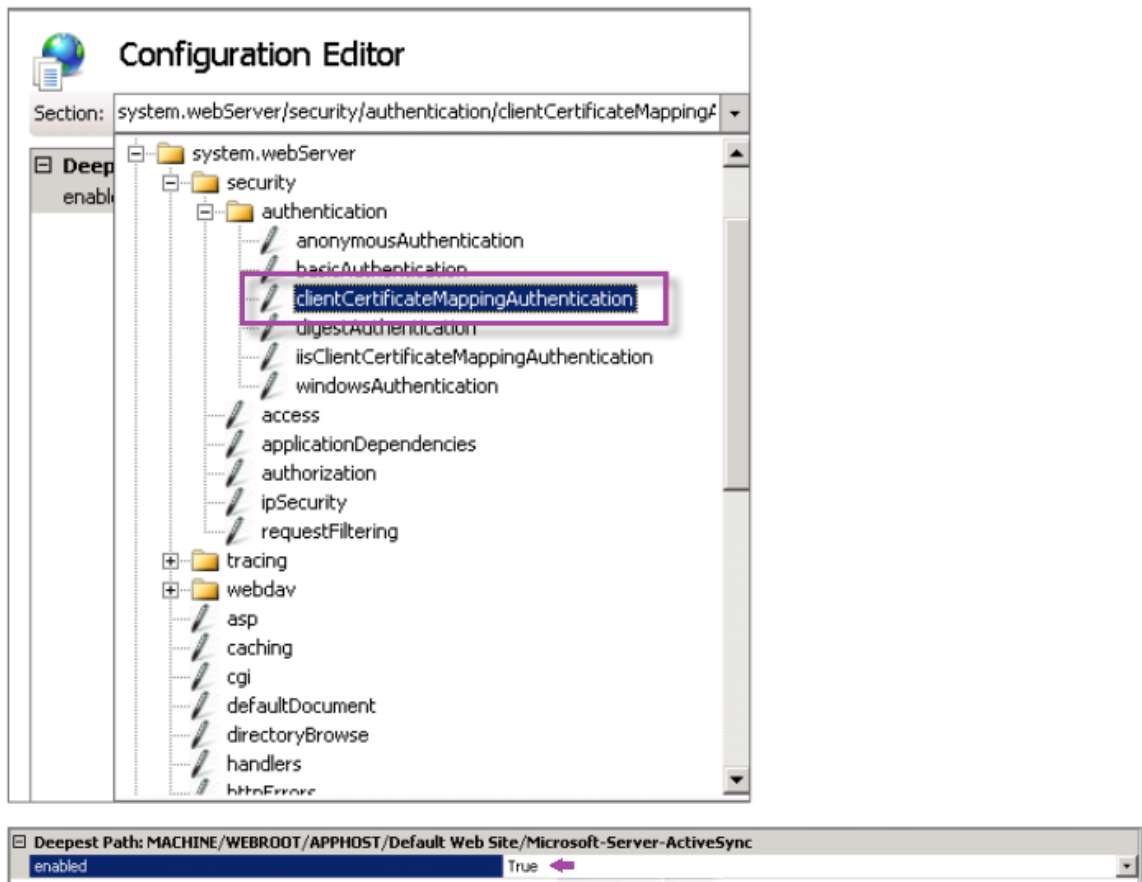
Microsoft Exchange Server 에 제출합니다. 사용자가 Secure Mail 을 시작할 때 자격 증명을 입력하라는 메시지가 XenMobile 에 표시될 경우 구성을 확인하십시오.

사용자가 Secure Mail 을 다운로드하고 설치할 수 있지만 사서함 구성 중에 Secure Mail 이 구성을 완료하지 못할 경우:

1. Microsoft Exchange Server ActiveSync 에서 트래픽을 보안하기 위해 개인 SSL 서버 인증서를 사용하는 경우, 모든 루트 및 중간 인증서가 모바일 장치에 설치되어 있는지 확인합니다.
2. ActiveSync 에 대해 선택한 인증 유형이 클라이언트 인증서 필요인지 확인합니다.



3. Microsoft Exchange Server 에서 **Microsoft-Server-ActiveSync** 사이트를 확인하여 클라이언트 인증서 매핑 인증이 사용하도록 설정되어 있는지 검토합니다. 기본적으로 클라이언트 인증서 매핑은 사용되지 않습니다. 이 옵션은 구성 편집기 > 보안 > 인증 아래에 있습니다.



True 를 선택한 후에 적용을 클릭해야 변경 내용이 적용됩니다.

4. XenMobile 콘솔에서 Citrix Gateway 설정을 확인합니다. 인증을 위한 사용자 인증서 제공이 켜짐이고 자격 증명 공급자에 올바른 프로필이 선택되어 있는지 확인합니다.

클라이언트 인증서가 모바일 장치에 제공되었는지 확인하려면

1. XenMobile 콘솔에서 관리 > 장치로 이동하여 장치를 선택합니다.
2. 편집 또는 자세히 표시를 클릭합니다.
3. 배달 그룹 섹션으로 이동하여 다음 항목을 검색합니다.

Citrix Gateway Credentials: Requested credential, CertId=

클라이언트 인증서 협상을 사용하도록 설정했는지 확인하려면

1. 다음 `netsh` 명령을 실행하여 IIS 웹 사이트에 바인딩된 SSL 인증서 구성을 표시합니다.

```
netsh http show sslcert
```

2. 클라이언트 인증서 협상의 값이 사용 안 함인 경우 다음 명령을 실행하여 사용하도록 설정합니다.

```
netsh http delete sslcert ipport=0.0.0.0:443

netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash
appid={ app_id } certstorename=store_name verifyclientcertrevocation
=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck
=Enable clientcertnegotiation=Enable
```

예:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb71
appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=
ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWit
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

PKI 엔터티

December 8, 2023

XenMobile PKI(공개 키 인프라) 엔터티 구성은 실제 PKI 작업 (발급, 해지 및 상태 정보) 을 수행하는 구성 요소를 나타냅니다. 이러한 구성 요소는 XenMobile 의 내부 또는 외부 구성 요소입니다. 내부 구성 요소는 임의 구성 요소라고 합니다. 외부 구성 요소는 기업 인프라의 일부입니다.

XenMobile 은 다음과 같은 PKI 엔터티 유형을 지원합니다.

- Microsoft 인증서 서비스
- 임의의 CA(인증 기관)

XenMobile 은 다음과 같은 CA 서버를 지원합니다.

- Windows Server 2019
- Windows Server 2016

참고:

Windows Server 2012 R2, 2012 및 2008 R2 는 수명이 다하여 더 이상 지원되지 않습니다. 자세한 내용은 [Microsoft 제품 수명 주기 설명서](#)를 참조하십시오.

일반적인 PKI 개념

유형에 관계없이 모든 PKI 엔터티는 다음과 같은 하위 집합의 기능을 갖습니다.

- 서명: CSR(인증서 서명 요청) 을 기반으로 새 인증서 발급

- 가져오기: 기존 인증서 및 키 쌍 복구
- 해지: 클라이언트 인증서 해지

CA 인증서 정보

PKI 엔터티를 구성하는 경우 해당 엔터티에 의해 발급 (또는 복구) 되는 인증서의 서명자가 어느 CA 인증서인지를 XenMobile 에 알립니다. 이 PKI 엔터티는 개수에 제한 없이 서로 다른 CA 가 서명한 (가져오거나 새로 서명된) 인증서를 반환할 수도 있습니다.

PKI 엔터티 구성의 일환으로 이러한 각 CA 의 인증서를 제공합니다. 이를 위해 인증서를 XenMobile 에 업로드한 후 PKI 엔터티에서 참조해야 합니다. 임의 discretionary CA 의 경우 인증서는 묵시적으로 서명 CA 인증서이지만 외부 엔터티의 경우 인증서를 수동으로 지정해야 합니다.

중요:

Microsoft 인증서 서비스 엔터티 템플릿을 생성할 때 등록된 장치와 관련된 인증 문제를 방지하려면 특수 문자를 템플릿 이름에 사용하지 마십시오. 예를 들어 다음을 사용하지 마십시오. ! : \$ () # % + * ~ ? | { } []

Microsoft 인증서 서비스

XenMobile 은 웹 등록 인터페이스를 통해 Microsoft 인증서 서비스와 상호 작용합니다. XenMobile 은 그 인터페이스를 통해 새 인증서 발급만 지원합니다. Microsoft CA 에서 Citrix Gateway 사용자 인증서를 생성하면 Citrix Gateway 가 해당 인증서의 갱신과 해지를 지원합니다.

XenMobile 에서 Microsoft CA PKI 엔터티를 만들려면 인증서 서비스 웹 인터페이스의 기본 URL 을 지정해야 합니다. 원할 경우 SSL 클라이언트 인증을 사용하여 XenMobile 과 인증서 서비스 웹 인터페이스 간의 연결을 보호할 수 있습니다.

Microsoft 인증서 서비스 엔터티 추가

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭하고 **PKI** 엔터티를 클릭합니다.

2. **PKI** 엔터티 페이지에서 추가를 클릭합니다.

PKI 엔터티 유형에 대한 메뉴가 나타납니다.

3. **Microsoft** 인증서 서비스 엔터티를 클릭합니다.

Microsoft 인증서 서비스 엔터티: 일반 정보 페이지가 나타납니다.

4. **Microsoft** 인증서 서비스 엔터티: 일반 정보 페이지에서 다음 설정을 구성합니다.

- 이름: 나중에 엔터티를 참조하는 데 사용할 새 엔터티 이름을 입력합니다. 엔터티 이름은 고유해야 합니다.
- 웹 등록 서비스 루트 **URL**: Microsoft CA 웹 등록 서비스의 기본 URL(예: <https://192.0.2.13/certsrv/>) 을 입력합니다. URL 은 일반 HTTP 또는 HTTP-over-SSL 을 사용할 수 있습니다.

- **certnew.cer** 페이지 이름: certnew.cer 페이지의 이름입니다. 어떤 이유로 이름을 변경한 경우가 아니면 기본 이름을 사용합니다.
 - **certfnsh.asp**: certfnsh.asp 페이지의 이름입니다. 어떤 이유로 이름을 변경한 경우가 아니면 기본 이름을 사용합니다.
 - 인증 유형: 사용하려는 인증 방법을 선택합니다.
 - 없음
 - **HTTP** 기본: 연결하는 데 필요한 사용자 이름 및 암호를 입력합니다.
 - 클라이언트 인증서: 올바른 SSL 클라이언트 인증서를 선택합니다.
5. 연결 테스트를 클릭하여 서버에 액세스할 수 있는지 확인합니다. 액세스할 수 없는 경우 연결에 실패했음을 알리는 메시지가 나타납니다. 구성 설정을 확인합니다.
6. 다음을 클릭합니다.
- Microsoft** 인증서 서비스 엔터티: 템플릿 페이지가 나타납니다. 이 페이지에서는 해당 Microsoft CA 가 지원하는 템플릿의 내부 이름을 지정합니다. 자격 증명 공급자를 만들 때 여기에 정의된 목록에서 템플릿을 선택합니다. 이 엔터티를 사용하는 모든 자격 증명 공급자가 해당 템플릿 하나만 사용합니다.
- Microsoft 인증서 서비스 템플릿 요구 사항은 해당 Microsoft 서버 버전에 대한 Microsoft 설명서를 참조하십시오. XenMobile 에는 [인증서](#)에 명시된 인증서 형식을 제외하고 배포하는 인증서에 대한 요구 사항이 없습니다.
7. **Microsoft** 인증서 서비스 엔터티: 템플릿 페이지에서 추가를 클릭하고 템플릿 이름을 입력한 후 저장을 클릭합니다. 추가할 각 템플릿에 대해 이 단계를 반복합니다.
8. 다음을 클릭합니다.
- Microsoft** 인증서 서비스 엔터티: **HTTP** 매개 변수 페이지가 나타납니다. 이 페이지에서는 XenMobile 이 Microsoft 웹 등록 인터페이스에 대한 HTTP 요청에 추가해야 하는 사용자 지정 매개 변수를 지정합니다. 사용자 지정 매개 변수는 CA 에서 실행되는 사용자 지정 스크립트에만 유용합니다.
9. **Microsoft** 인증서 서비스 엔터티: **HTTP** 매개 변수 페이지에서 추가를 클릭하고 추가할 HTTP 매개 변수의 이름과 값을 입력한 후 다음을 클릭합니다.
- Microsoft** 인증서 서비스 엔터티: **CA** 인증서 페이지가 나타납니다. 이 페이지에서는 시스템이 이 엔터티를 통해 얻는 인증서의 서명자를 XenMobile 에 알려야 합니다. CA 인증서가 갱신되면 XenMobile 에서 인증서를 업데이트합니다. XenMobile 이 변경 내용을 투명하게 엔터티에 적용합니다.
10. **Microsoft** 인증서 서비스 엔터티: **CA** 인증서 페이지에서 엔터티에 사용할 인증서를 선택합니다.
11. 저장을 클릭합니다.
- PKI 엔터티 테이블에 해당 엔터티가 나타납니다.

Citrix ADC CRL(인증서 해지 목록)

XenMobile 은 타사 인증 기관에 대해서만 CRL(인증서 해지 목록) 을 지원합니다. Microsoft CA 가 구성된 경우 XenMobile 은 Citrix ADC 를 사용하여 인증서 해지를 관리합니다.

클라이언트 인증서 기반 인증을 구성하는 경우 Citrix ADC CRL(인증서 해지 목록) 설정인 **Enable CRL Auto Refresh(CRL 자동 새로 고침 사용)** 를 구성할지 여부를 고려합니다. 이 단계는 MAM 전용 모드의 장치 사용자가 장치의 기존 인증서를 사용하여 인증할 수 없도록 합니다.

XenMobile에서는 인증서가 해지된 경우 사용자가 사용자 인증서를 생성할 수 있으므로 새 인증서가 다시 발급됩니다. 이 설정을 사용하면 CRL이 만료된 PKI 엔터티를 확인하는 경우 PKI 엔터티의 보안이 강화됩니다.

임의의 CA

임의의 CA는 CA 인증서와 연결된 개인 키를 XenMobile에 제공하는 경우 만들어집니다. XenMobile은 지정된 매개 변수에 따라 인증서 발급, 해지 및 상태 정보를 내부적으로 처리합니다.

임의의 CA를 구성하는 경우 해당 CA에 대한 OCSP(온라인 인증서 상태 프로토콜) 지원을 활성화할 수 있습니다. OCSP 지원을 사용하도록 설정한 경우에 한해 CA는 **id-pe-authorityInfoAccess** 확장을 CA가 발급한 인증서에 추가합니다. 이 확장은 다음 위치의 XenMobile 내부 OCSP Responder를 가리킵니다.

<https://<server>/<instance>/ocsp>

OCSP 서비스를 구성하는 경우 해당 임의의 엔터티에 대한 OCSP 서명 인증서를 지정합니다. CA 인증서 자체를 서명자로 사용할 수 있습니다. CA 개인 키의 불필요한 노출을 방지하려면 (권장) CA 인증서로 서명된 위임자 OCSP 서명 인증서를 만들고 **id-kp-OCSPSigning extendedKeyUsage** 확장을 포함합니다.

XenMobile OCSP 응답자 서비스는 기본 OCSP 응답과 다음 해시 알고리즘을 요청에 지원합니다.

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

응답은 SHA-256 및 서명 인증서 키 알고리즘 (DSA, RSA 또는 ECDSA)으로 서명됩니다.

임의의 CA 추가

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭하고 자세히 > **PKI** 엔터티를 클릭합니다.
2. **PKI** 엔터티 페이지에서 추가를 클릭합니다.
PKI 엔터티 유형에 대한 메뉴가 나타납니다.
3. 임의의 **CA**를 클릭합니다.
임의의 **CA**: 일반 정보 페이지가 나타납니다.
4. 임의의 **CA**: 일반 정보 페이지에서 다음을 수행합니다.
 - 이름: 임의의 CA를 설명하는 이름을 입력합니다.

- 인증서 요청에 서명할 **CA 인증서**: 인증서 요청에 서명하는 데 사용할 임의의 CA 용 인증서를 클릭합니다.

XenMobile 에서 구성 > 설정 > 인증서를 통해 업로드한 개인 키를 사용하여 CA 인증서에서 인증서 목록이 생성됩니다.

5. 다음을 클릭합니다.

임의의 **CA**: 매개 변수 페이지가 나타납니다.

6. 임의의 **CA**: 매개 변수 페이지에서 다음을 수행합니다.

- 일련 번호 생성기: 임의의 CA 가 발급한 인증서에 대한 일련 번호를 생성합니다. 이 목록에서 순차적 또는 비순차적을 클릭하여 숫자가 생성되는 방식을 지정합니다.
- 다음 일련 번호: 다음번 발급될 번호를 지정하는 값을 입력합니다.
- 인증서 유효 기간: 인증서가 유효한 일 수를 입력합니다.
- 키 사용: 해당 키를 커짐으로 설정하여 임의의 CA 에서 발급하는 인증서의 용도를 지정합니다. 이 항목을 설정하면 해당 CA 가 지정된 용도로만 인증서를 발급할 수 있게 됩니다.
- 확장 키 사용: 매개 변수를 더 추가하려면 추가를 클릭하고 키 이름을 입력한 후 저장을 클릭합니다.

7. 다음을 클릭합니다.

임의의 **CA**: 배포 페이지가 나타납니다.

8. 임의의 **CA**: 배포 페이지에서 배포 모드를 선택합니다.

- 중앙 집중식: 서버측 키 생성. 중앙 집중식 옵션을 사용하는 것이 좋습니다. 개인 키가 생성되어 서버에 저장되고 사용자 장치에 배포됩니다.
- 분산: 장치측 키 생성. 개인 키가 사용자 장치에 생성됩니다. 이 분산 모드에서는 SCEP 를 사용하며 **keyUsage keyEncryption** 확장의 RA 암호화 인증서와 **keyUsage digitalSignature** 확장의 RA 서명 인증서가 필요합니다. 암호화와 서명에 모두 동일한 인증서를 사용할 수 있습니다.

9. 다음을 클릭합니다.

임의의 **CA: OCSP**(온라인 인증서 상태 프로토콜) 페이지가 나타납니다.

임의의 **CA: OCSP**(온라인 인증서 상태 프로토콜) 페이지에서 다음을 수행합니다.

- 이 CA 가 서명한 인증서에 **AuthorityInfoAccess**(RFC2459) 확장을 추가하려면 이 **CA** 에 **OCSP** 지원 사용을 커짐으로 설정합니다. 이 확장은 CA OCSP Responder(<https://<server>/<instance>/ocsp>) 를 가리킵니다.
- OCSP 지원을 사용하도록 설정한 경우 OCSP 서명 CA 인증서를 선택합니다. XenMobile 에 업로드한 CA 인증서에서 인증서 목록이 생성됩니다.

10. 저장을 클릭합니다.

PKI 엔터티 테이블에 임의의 CA 가 나타납니다.

자격 증명 공급자

March 15, 2024

자격 증명 공급자는 XenMobile 시스템의 다양한 부분에서 사용하는 실제 인증서 구성입니다. 자격 증명 공급자는 인증서의 원본, 매개 변수 및 수명 주기를 정의합니다. 이러한 작업은 인증서가 장치 구성의 일부인지 독립 실행형 (즉, 있는 그대로 장치에 푸시됨) 인지에 따라 발생합니다.

장치 등록은 인증서 수명주기를 제한합니다. 즉, XenMobile 은 등록 과정에서 일부 인증서를 발급할 수 있지만 등록 전에는 인증서를 발급하지 않습니다. 또한 등록이 해지되면 하나의 등록 컨텍스트 내에서 내부 PKI 에 의해 발급된 인증서가 해지됩니다. 관리 관계가 종료된 후에는 유효한 인증서가 남아 있지 않습니다.

단일 구성이 동시에 여러 개의 인증서를 관리할 수 있도록 여러 곳에서 단일 자격 증명 공급자 구성을 사용할 수 있습니다. 통일성은 배포 리소스 및 배포에 기반합니다. 예를 들어 자격 증명 공급자 P 가 구성 C 의 일부로 장치 D 에 배포된 경우 P 에 대한 발급 설정은 D 에 배포된 인증서를 결정합니다. 마찬가지로 D 에 대한 갱신 설정은 C 가 업데이트될 때 적용됩니다. D 에 대한 해지 설정도 C 가 삭제되거나 D 가 해지될 때 적용됩니다.

이 규칙에 따라 XenMobile 의 자격 증명 공급자 구성은 다음을 결정합니다.

- 인증서의 원본.
- 인증서를 얻는 방법: 새 인증서에 서명하거나 기존 인증서 및 키 쌍을 가져옵니다 (복구).
- 발급 또는 복구를 위한 매개 변수. 예: 키 크기, 키 알고리즘 및 인증서 확장 같은 CSR(인증서 서명 요청) 매개 변수.
- 인증서가 장치로 전달되는 방식.
- 해지 조건. XenMobile 에서 관리 관계가 끊어지면 모든 인증서가 해지되지만 구성에서 만료 이전에 해지되도록 지정할 수 있습니다. 예를 들어 연결된 장치 구성이 삭제된 경우 인증서가 해지되도록 구성할 수 있습니다. 또한 특정 조건에서는 XenMobile 에서 관련 인증서의 해지가 백엔드 PKI(공개 키 인프라) 로 전송될 수 있습니다. 즉, XenMobile 에서 인증서가 해지되면 PKI 에서 인증서가 해지될 수 있습니다.
- 갱신 설정. 지정된 자격 증명 공급자를 통해 받은 인증서는 만료 날짜가 가까워질 때 자동으로 갱신될 수 있습니다. 또는 이러한 상황과 별개로 만료 날짜가 다가올 때 알림을 실행할 수 있습니다.

사용 가능한 구성 옵션은 주로 자격 증명 공급자에 대해 선택한 PKI 엔터티 및 발급 방법의 유형에 따라 다릅니다.

인증서 발급 방법

서명을 통해 발급 방법이라고 하는 인증서를 얻을 수 있습니다.

이 방법을 사용할 경우 발급에 새 개인 키를 만들고, CSR 을 만들고, 서명을 위해 CSR 을 CA(인증 기관) 에 제출하는 과정이 포함됩니다. XenMobile 은 MS 인증서 서비스 엔터티와 임의의 CA 엔터티 모두에 대한 서명 방법을 지원합니다.

자격 증명 공급자는 서명 발급 방법을 사용합니다.

인증서 제공

XenMobile에서는 중앙 집중식 모드와 분산 모드의 두 가지 인증서 전달 모드를 사용할 수 있습니다. 분산 모드는 SCEP(단순 인증서 등록 프로토콜)를 사용하여 클라이언트가 프로토콜을 지원하는 경우에만 사용할 수 있습니다(iOS만 해당). 일부 상황에서는 분산 모드가 필수입니다.

자격 증명 공급자가 분산(SCEP 지원) 전달을 지원하려면 RA(등록 기관) 인증서 설정이라는 특수한 구성 단계가 필요합니다. SCEP 프로토콜을 사용하는 경우 XenMobile이 실제 인증 기관의 대리인(등록 기관) 역할을 하기 때문에 RA 인증서가 필요합니다. XenMobile은 클라이언트에게 인증 기관의 역할을 수행할 권한이 있음을 입증해야 합니다. 이 권한은 앞서 언급한 인증서를 XenMobile에 업로드하여 설정됩니다.

단일 인증서로 두 가지 요구 사항을 모두 충족시킬 수 있지만, 두 가지 고유한 인증서 역할(RA 서명 및 RA 암호화)이 필요합니다. 이러한 역할에 대한 제약 조건은 다음과 같습니다.

- RA 서명 인증서에는 X.509 키 사용 디지털 서명이 있어야 합니다.
- RA 암호화 인증서에는 X.509 키 사용 키 암호화가 있어야 합니다.

자격 증명 공급자 RA 인증서를 구성하려면 XenMobile에 인증서를 업로드한 다음 자격 증명 공급자에서 인증서에 연결합니다.

자격 증명 공급자는 인증서 역할에 대해 구성된 인증서가 있는 경우에만 분산 전달을 지원하는 것으로 간주됩니다. 중앙 집중식 모드를 선호하거나, 분산 모드를 선호하거나 또는 분산 모드를 요구하도록 각 자격 증명 공급자를 구성할 수 있습니다. 실제 결과는 컨텍스트에 따라 달라집니다. 컨텍스트가 분산 모드를 지원하지 않지만 자격 증명 공급자가 이 모드를 요구하면 배포가 실패합니다. 마찬가지로 컨텍스트에서 분산 모드를 요구하지만 자격 증명 공급자가 분산 모드를 지원하지 않으면 배포가 실패합니다. 다른 모든 경우에는 기본 설정이 적용됩니다.

다음 표에서는 XenMobile의 SCEP 배포를 보여 줍니다.

컨텍스트	SCEP 지원	SCEP 필요
iOS 프로파일 서비스	예	예
iOS 모바일 기기 관리 등록	예	아니요
iOS 구성 프로파일	예	아니요
SHTP 등록	아니요	아니요
SHTP 구성	아니요	아니요
Windows 태블릿 등록	아니요	아니요
Windows 태블릿 구성	아니요 (Windows 10 및 Windows 11 릴리스에서 지원되는 Wi-Fi 장치 정책 제외)	아니요

인증서 해지

해지에는 세 가지 유형이 있습니다.

- **내부적 해지:** 내부적 해지는 XenMobile 에서 유지 관리하는 인증서 상태에 영향을 줍니다. XenMobile 은 제시된 인증서를 평가하거나 인증서에 대한 OCSP 상태 정보를 제공할 때 이 상태를 고려합니다. 자격 증명 공급자 구성에 따라 다양한 조건에서 이러한 상태가 영향을 받는 방식이 결정됩니다. 예를 들어 자격 증명 공급자는 인증서가 장치에서 삭제된 경우 인증서에 해지 플래그를 지정하도록 지정할 수 있습니다.
- **외부에서 전파된 해지:** 해지 XenMobile 이라고 알려진 이 해지 유형은 외부 PKI 에서 취득한 인증서에 적용됩니다. 자격 증명 공급자 구성에 정의된 조건에 따라 XenMobile 에서 내부적으로 인증서가 해지되는 경우 PKI 에서 인증서가 해지됩니다.
- **외부에서 유도된 해지:** 해지 PKI 라고 알려진 이 해지 유형도 외부 PKI 에서 취득한 인증서에만 적용됩니다. XenMobile 이 지정된 인증서 상태를 평가할 때마다 XenMobile 은 해당 상태에 대해 PKI 를 쿼리합니다. 인증서가 해지된 경우에는 XenMobile 이 내부적으로 인증서를 해지합니다. 이 메커니즘에서 OCSP 프로토콜을 사용합니다.

이 세 가지 유형은 배타적이지 않으며 함께 적용됩니다. 외부 해지 또는 독립적 결과로 인해 내부 해지가 발생할 수 있습니다. 내부 해지는 외부 해지에 영향을 미칠 수 있습니다.

인증서 갱신

인증서 갱신은 기존 인증서의 해지와 다른 인증서 발급의 조합입니다.

XenMobile 은 발급 실패로 인한 서비스 중단을 방지하기 위해 이전 인증서를 해지하기 전에 먼저 새 인증서를 얻으려고 시도합니다. 분산 (SCEP 지원) 제공자의 경우 해지는 인증서가 장치에 설치된 후에만 발생합니다. 그렇지 않은 경우 해지는 새 인증서가 장치에 전송되기 전에 발생합니다. 이 해지는 인증서 설치의 성공 또는 실패와 관계가 없습니다.

해지 구성에서 특정 기간 (일) 을 지정해야 합니다. 장치가 연결되면 서버는 인증서 **NotAfter** 날짜가 현재 날짜에서 지정된 기간을 뺀 날짜보다 이후인지 여부를 확인합니다. 인증서가 조건을 충족하면 XenMobile 이 인증서 갱신을 시도합니다.

자격 증명 공급자 생성

자격 증명 공급자 구성은 주로 자격 증명 공급자에 대해 선택한 발급 엔터티 및 발급 방법의 요인에 따라 달라집니다. 내부 엔터티 또는 외부 엔터티를 사용하는 자격 증명 공급자를 구분할 수 있습니다.

- XenMobile 에 대해 내부인 임의의 엔터티는 내부 엔터티입니다. 임의의 엔터티에 대한 발급 방법은 항상 서명입니다. 서명은 발급 작업을 수행할 때마다 XenMobile 이 엔터티에 대해 선택된 CA 인증서로 새 키 쌍을 서명한다는 것을 의미합니다. 키 쌍이 장치에서 생성되는지, 아니면 서버에서 생성되는지는 선택한 배포 방법에 따라 다릅니다.
- 회사 인프라의 일부인 외부 엔터티에는 Microsoft CA 가 포함됩니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭하고 설정 > 자격 증명 공급자를 클릭합니다.

2. 자격 증명 공급자 페이지에서 추가를 클릭합니다.

자격 증명 공급자: 일반 정보 페이지가 나타납니다.

3. 자격 증명 공급자: 일반 정보 페이지에서 다음을 수행합니다.

- 이름: 새 공급자 구성의 고유한 이름을 입력합니다. 이 이름은 나중에 XenMobile 콘솔의 다른 부분에서 구성을 식별할 때 사용됩니다.
 - 설명: 자격 증명 공급자를 설명합니다. 이 필드는 선택 사항이지만 설명을 사용하면 이 자격 증명 공급자에 대한 유용한 세부 정보를 제공할 수 있습니다.
 - 발급 엔터티: 인증서 발급 엔터티를 클릭합니다.
 - 발급 방법: 시스템이 구성된 엔터티에서 인증서를 가져올 때 사용할 방법으로 서명 또는 가져오기를 클릭합니다. 클라이언트 인증서 인증의 경우 서명을 사용합니다.
 - 템플릿 목록을 사용할 수 있는 경우 자격 증명 공급자에 대한 PKI 엔터티 아래에 추가한 템플릿을 선택합니다.
- 설정 > PKI 엔터티에서 Microsoft 인증서 서비스 엔터티를 추가하면 이러한 템플릿을 사용할 수 있게 됩니다.

4. 다음을 클릭합니다.

자격 증명 공급자: **CSR** 페이지가 나타납니다.

5. 자격 증명 공급자: **CSR** 페이지에서 인증서 구성에 따라 다음을 구성합니다.

- 키 알고리즘: 새 키 쌍에 대한 키 알고리즘을 선택합니다. 사용 가능한 값은 **RSA**, **DSA** 및 **ECDSA** 입니다.
 - 키 크기: 키 쌍의 크기 (비트) 를 입력합니다. 이것은 필수 필드입니다.
- 허용되는 값은 키 유형에 따라 다릅니다. 예를 들어 DSA 키의 최대 크기는 1024 비트입니다. 기본 하드웨어 및 소프트웨어에 따라 달라질 수 있는 거짓 음성 반응을 방지하기 위해 XenMobile 은 키 크기를 강제하지 않습니다. 자격 증명 공급자 구성을 프로덕션 환경에서 활성화하기 전에 항상 테스트 환경에서 테스트해야 합니다.
- 서명 알고리즘: 새 인증서에 대한 값을 클릭합니다. 값은 키 알고리즘에 따라 달라집니다.
 - 주체 이름: 필수 항목입니다. 새 인증서 주체의 DN(고유 이름) 을 입력합니다. 예: `CN=${ user . username } , OU=${ user . department } , O=${ user . companyname } , C=${ user . c } \endquotation`

예를 들어 클라이언트 인증서 인증의 경우 다음 설정을 사용합니다.

- 키 알고리즘: RSA
 - 키 크기: 2048
 - 서명 알고리즘: SHA256withRSA
 - 주체 이름 `cn=${user}.username`
- 주체 대체 이름 테이블에 항목을 추가하려면 추가를 클릭합니다. 대체 이름의 유형을 선택하고 두 번째 열에 값을 입력합니다.
- 클라이언트 인증서 인증의 경우 다음을 지정합니다.
- 유형: 사용자 계정 이름

- 값: `$user.userprincipalname`

주체 이름과 마찬가지로 값 필드에 XenMobile 매크로를 사용할 수 있습니다.

6. 다음을 클릭합니다.

자격 증명 공급자: 배포 페이지가 나타납니다.

7. 자격 증명 공급자: 배포 페이지에서 다음을 수행합니다.

- **CA** 인증서 발급 목록에서 제공된 CA 인증서를 클릭합니다. 자격 증명 공급자가 임의의 CA 엔터티를 사용하기 때문에 자격 증명 공급자에 대한 CA 인증서는 항상 엔터티 자체에서 구성된 CA 인증서입니다. 여기에 나온 CA 인증서는 외부 엔터티를 사용하는 구성과의 일관성을 위한 것입니다.
- 배포 모드 선택에서 다음과 같은 키 생성 및 배포 방법 중 하나를 클릭합니다.
 - 중앙 집중식 선호: 서버 측 키 생성: 이 중앙 집중식 옵션을 사용하는 것이 좋습니다. 이 옵션은 XenMobile에서 지원하는 모든 플랫폼을 지원하며 Citrix Gateway 인증을 사용할 때 필요합니다. 개인 키가 생성되어 서버에 저장되고 사용자 장치에 배포됩니다.
 - 분산식 선호: 장치측 키 생성: 개인 키가 생성되고 사용자 장치에 저장됩니다. 이 분산 모드에서는 SCEP를 사용하며 keyUsage keyEncryption이 포함된 RA 암호화 인증서와 KeyUsage digitalSignature가 포함된 RA 서명 인증서가 필요합니다. 암호화와 서명에 모두 동일한 인증서를 사용할 수 있습니다.
 - 분산 전용: 장치측 키 생성: 이 옵션은 “선호”가 아닌 “전용”이기 때문에 장치 측 키 생성이 실패하거나 사용할 수 없는 경우 사용할 수 있는 옵션이 없다는 것을 제외하면 분산식 선호: 장치측 키 생성과 동일하게 작동합니다.

분산식 선호: 장치측 키 생성 또는 분산 전용: 장치측 키 생성을 선택한 경우 RA 서명 인증서 및 RA 암호화 인증서를 클릭합니다. 둘 모두에 동일한 인증서를 사용할 수 있습니다. 인증서에 대한 새 필드가 나타납니다.

8. 다음을 클릭합니다.

자격 증명 공급자: 해지 **XenMobile** 페이지가 나타납니다. 이 페이지에서 XenMobile이 이 공급자 구성을 통해 발급된 인증서를 어떤 조건일 때 내부적으로 해지된 것으로 플래그 지정해야 하는지를 구성합니다.

9. 자격 증명 공급자: 해지 **XenMobile** 페이지에서 다음을 수행합니다.

- 발급된 인증서 해지에서 인증서를 해지할 시기를 나타내는 옵션 중 하나를 선택합니다.
- 인증서가 해지될 때 XenMobile의 알림을 받으려면 알림 보내기의 값을 커짐으로 설정하고 알림 템플릿을 선택합니다.
- XenMobile에서 인증서가 해지될 때 PKI에서 인증서를 해지하려면 **PKI**에 대한 인증서 해지를 커짐으로 설정하고 엔터티 목록에서 템플릿을 클릭합니다. 엔터티 목록에 해지 기능이 있는 모든 사용 가능한 엔터티가 표시됩니다. XenMobile에서 인증서가 해지되면 해지 요청이 엔터티 목록에서 선택된 PKI로 전송됩니다.

10. 다음을 클릭합니다.

자격 증명 공급자: 해지 **PKI** 페이지가 나타납니다. 이 페이지에서 인증서가 해지된 경우 PKI에서 수행할 동작을 식별합니다. 알림 메시지를 생성하는 옵션도 사용할 수 있습니다.

11. PKI 에서 인증서를 해지하려면 자격 증명 공급자: 해지 **PKI** 페이지에서 다음을 수행합니다.

- 외부 해지 확인 사용 설정을 켜짐으로 변경합니다. 해지 **PKI** 와 관련된 추가 필드가 나타납니다.
- **OCSP** 응답자 **CA** 인증서 목록에서 인증서 주체의 DN(고유 이름) 을 클릭합니다.
DN 필드 값에 XenMobile 매크로를 사용할 수 있습니다. 예: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`
- 인증서가 해지된 경우 목록에서 다음 동작 중 하나를 클릭하여 인증서가 해지될 때 PKI 엔터티에서 수행되게 합니다.
 - 아무 작업도 하지 않습니다.
 - 인증서를 갱신합니다.
 - 장치를 해지 및 초기화합니다.
- 인증서가 해지될 때 XenMobile 의 알림을 받으려면 알림 보내기의 값을 켜짐으로 설정합니다.
두 알림 옵션 중에서 선택할 수 있습니다.
- 알림 템플릿 선택을 선택한 경우 미리 작성된 알림 메시지를 선택하여 사용자 지정할 수 있습니다. 이러한 템플릿은 알림 템플릿 목록에 있습니다.
- 알림 세부 정보 입력을 선택한 경우 고유한 알림 메시지를 작성할 수 있습니다. 받는 사람의 전자 메일 주소와 메시지를 제공하는 것 외에도 알림을 보내는 빈도를 설정할 수 있습니다.

12. 다음을 클릭합니다.

자격 증명 공급자: 갱신 페이지가 나타납니다. 이 페이지에서 다음을 수행하도록 XenMobile 을 구성할 수 있습니다.

- 인증서를 갱신합니다. 필요한 경우 갱신 시 알림을 보내고, 이미 만료된 인증서를 필요에 따라 작업에서 제외할 수 있습니다.
- 만료가 임박한 인증서에 대한 알림을 실행합니다 (갱신 전 알림).

13. 인증서가 만료될 경우 인증서를 갱신하려면 자격 증명 공급자: 갱신 페이지에서 다음을 수행합니다.

인증서가 만료될 때 갱신에 대해 켜짐을 선택합니다. 추가 필드가 나타납니다.

- 인증서가 다음 기간 내에 있는 경우 갱신 필드에 인증서를 갱신해야 하는 만료 전까지 남은 일 수를 입력합니다.
- 필요한 경우 이미 만료된 인증서는 갱신하지 않음을 선택합니다. 이 경우 “이미 만료” 되었다는 의미는 인증서가 해지되었다는 것이 아니라 **NotAfter** 날짜가 지났다는 것입니다. XenMobile 은 내부적으로 해지된 인증서를 갱신하지 않습니다.

인증서가 갱신되었을 때 XenMobile 의 알림을 받으려면 알림 보내기를 켜짐으로 설정합니다. 인증서의 만료가 임박한 경우 XenMobile 의 알림을 받으려면 인증서 만료가 다가오면 알림을 켜짐으로 설정합니다.

어느 항목을 선택하든 두 알림 옵션 중에서 선택할 수 있습니다.

- 알림 템플릿 선택: 미리 작성된 알림 메시지를 선택한 후 사용자 지정합니다. 이러한 템플릿은 알림 템플릿 목록에 있습니다.

- 알림 세부 정보 입력: 고유한 알림 메시지를 작성합니다. 받는 사람의 전자 메일 주소, 메시지 및 알림을 보낼 빈도를 제공합니다.

인증서가 다음 기간 내에 있는 경우 알림 필드에 알림을 보낼 인증서의 만료 전 일 수를 입력합니다.

14. 저장을 클릭합니다.

자격 증명 공급자가 자격 증명 공급자 테이블에 표시됩니다.

APNs 인증서

March 15, 2024

중요:

APN 레거시 바이너리 프로토콜에 대한 Apple의 지원은 2021년 3월 31일부터 종료됩니다. Apple에서는 HTTP/2 기반 APN 제공업체 API를 대신 사용하도록 권장합니다. 릴리스 10.13.0부터 XenMobile Server에서는 HTTP/2 기반 API를 지원합니다. 자세한 정보는 <https://developer.apple.com/>에서 뉴스 업데이트 “Apple 푸시 알림 서비스 업데이트”를 참조하십시오. APN 연결 확인과 관련된 지원은 [연결 확인](#)을 참조하십시오.

XenMobile에서 iOS 및 macOS 장치를 등록하고 관리하려면 Apple의 APNs(Apple 푸시 알림 서비스) 인증서를 설정합니다.

워크플로 요약:

- **1 단계:** 다음 방법 중 하나를 통해 CSR(인증서 서명 요청) 만들기
 - macOS에서 키체인 접근을 사용하여 CSR 만들기 (Citrix에서 권장)
 - Microsoft IIS를 사용하여 CSR 만들기
 - OpenSSL을 사용하여 CSR 만들기
- **2 단계:** XenMobile Tools에서 CSR에 서명
- **3 단계:** 서명된 CSR을 Apple에 제출하고 APNs 인증서 얻기
- **4 단계:** 1 단계에서 사용한 것과 동일한 컴퓨터를 사용하여 CSR을 완료하고 PKCS #12 파일 내보내기
 - macOS에서 키체인 접근을 사용하여 PKCS #12 파일 만들기
 - Microsoft IIS를 사용하여 PKCS #12 파일 만들기
 - OpenSSL을 사용하여 PKCS #12 파일 만들기
- **5 단계:** XenMobile로 APNs 인증서 가져오기
- **6 단계:** APN 인증서 갱신

CSR 만들기

macOS에서는 키체인 접근을 사용하여 CSR을 만드는 것이 좋습니다. Microsoft IIS 또는 OpenSSL을 사용하여 CSR을 만들 수도 있습니다.

중요:

- 인증서를 만드는 데 사용된 Apple ID의 경우:
 - The Apple ID must be a corporate ID and not a personal ID.
 - Record the Apple ID that you use to create the certificate.
 - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate requires device re-enrollment.
- 실수로 또는 의도적으로 인증서를 해지하면 장치를 관리할 수 없게 됩니다.
- iOS 개발자 기업 프로그램을 사용하여 Mobile Device Manager 푸시 인증서를 만든 경우 Apple Push Certificates Portal에서 마이그레이션 인증서에 대한 작업을 처리해야 합니다.

macOS에서 키체인 접근을 사용하여 CSR 만들기

1. macOS를 실행하는 컴퓨터의 응용 프로그램 > 유틸리티에서 키체인 접근 앱을 시작합니다.
2. 키체인 접근 메뉴를 열고 인증 지원 > 인증 기관에서 인증서 요청을 클릭합니다.
3. 다음과 같은 정보를 입력하라는 메시지가 나타납니다.
 - 전자 메일 주소: 인증서 관리를 담당하는 개인 또는 역할 계정의 전자 메일 주소입니다.
 - 일반 이름: 인증서 관리를 담당하는 개인 또는 역할 계정의 일반 이름입니다.
 - **CA** 전자 메일 주소: 인증 기관의 전자 메일 주소입니다.
4. 디스크에 저장됨 및 본인이 키 쌍 정보 지정 옵션을 선택하고 계속을 클릭합니다.
5. CSR 파일의 이름을 입력하고 컴퓨터에 파일을 저장한 다음 저장을 클릭합니다.
6. 키 쌍 정보를 지정합니다. 2048 비트의 키 크기와 **RSA** 알고리즘을 선택한 다음 계속을 클릭합니다. APNs 인증서 프로세스의 일부로 CSR 파일을 업로드할 준비가 되었습니다.
7. 인증 지원의 CSR 프로세스가 완료되면 완료를 클릭합니다.
8. 계속하려면 CSR에 서명합니다.

Microsoft IIS를 사용하여 CSR 만들기

APNs 인증서 요청을 생성하기 위한 첫 번째 단계는 CSR(증서 서명 요청)을 만드는 것입니다. Windows의 경우 Microsoft IIS를 사용하여 CSR을 만듭니다.

1. Microsoft IIS를 엽니다.
2. IIS에 대한 서버 인증서 아이콘을 두 번 클릭합니다.
3. 서버 인증서 창에서 인증서 요청 만들기를 클릭합니다.

4. 해당하는 DN(고유 이름) 정보를 입력하고 다음을 클릭합니다.
5. 암호화 서비스 공급자로 **Microsoft RSA SChannel Cryptographic Provider** 를 선택하고 비트 길이로 **2048** 을 선택한 후 다음을 클릭합니다.
6. 파일 이름을 입력하고 CSR 을 저장할 위치를 지정한 다음 마침을 클릭합니다.
7. 계속하려면 CSR 에 서명합니다.

OpenSSL 을 사용하여 CSR 만들기

macOS 장치 또는 Microsoft IIS 를 사용하여 CSR 을 생성할 수 없는 경우 OpenSSL 을 사용합니다. OpenSSL 웹 사이트에서 OpenSSL 을 다운로드하여 설치할 수 있습니다.

1. OpenSSL 을 설치한 컴퓨터의 명령 프롬프트 또는 셸에서 다음 명령을 실행합니다.

```
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate
.csr -newkey rsa:2048
```

2. 인증서 이름 지정 정보에 대한 다음과 같은 메시지가 나타납니다. 요청에 따라 정보를 입력합니다.

```
1 You are about to be asked to enter information that will be
   incorporated into your certificate request.
2 What you are about to enter is what is called a Distinguished Name
   or a DN.
3 There are quite a few fields but you can leave some blank
4 For some fields there will be a default value,
5 If you enter '.', the field will be left blank.
6 -----
7 Country Name (2 letter code) [AU]:US
8 State or Province Name (full name) [Some-State]:CA
9 Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    Customer
11 Organizational Unit Name (eg, section) [:Marketing
12 Common Name (eg, YOUR name) []:John Doe
13 Email Address []:john.doe@customer.com
14 <!--NeedCopy-->
```

3. 다음 메시지가 나타나면 CSR 개인 키의 암호를 입력합니다.

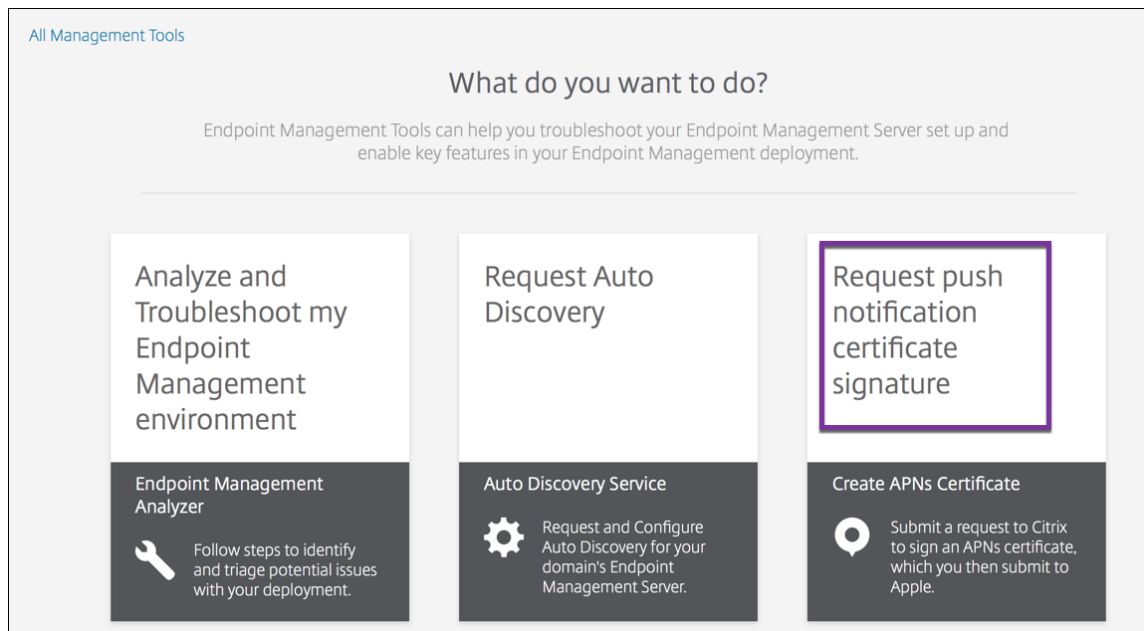
```
1 Please enter the following 'extra' attributes
2 to be sent with your certificate request
3 A challenge password []:
4 An optional company name []:
5 <!--NeedCopy-->
```

4. 계속하려면 다음 섹션에 설명된 대로 CSR 에 서명합니다.

CSR 서명

XenMobile 에서 인증서를 사용하려면 서명을 위해 Citrix 에 인증서를 제출합니다. Citrix 는 모바일 기기 관리 서명 인증서로 CSR 에 서명하고 서명된 파일을 `.plist` 형식으로 반환합니다.

1. 브라우저에서 [Endpoint Management Tools](#) 웹 사이트로 이동한 다음 **Request push notification certificate signature**(푸시 알림 인증서 서명 요청) 을 클릭합니다.



2. 새 인증서 만들기 페이지에서 **CSR** 업로드를 클릭합니다.



3. 인증서를 찾아 선택합니다.

인증서는.pem/txt 형식이어야 합니다.

4. **Endpoint Management APNs CSR** 서명 페이지에서 서명을 클릭합니다. CSR 이 서명되고 구성된 다운로드 폴더에 자동으로 저장됩니다.
5. 계속하려면 다음 섹션에 설명된 대로 서명된 CSR 을 제출합니다.

Apple 에 서명된 **CSR** 을 제출하여 **APNs** 인증서 받기

Citrix 에서 서명된 CSR(증서 서명 요청) 을 받았으면 Apple 에 CSR 을 제출하여 XenMobile 로 가져오는 데 필요한 APNs 인증서를 받습니다.

참고:

일부 사용자가 Apple Push Portal 로그인과 관련된 문제를 보고했습니다. 또는 [Apple 개발자 포털](#)에 로그인한 후 다음 단계를 따르십시오.

1. 브라우저에서 [Apple Push Certificates Portal](#)로 이동합니다.

2. **Create a Certificate**(인증서 생성) 를 클릭합니다.
3. Apple 에서 인증서를 만드는 것이 처음이라면 **I have read and agree to these terms and conditions**(이용 약관을 읽었고 이에 동의합니다.) 확인란을 선택하고 **Accept**(동의) 를 클릭합니다.
4. **Choose File**(파일 선택) 을 클릭하고 컴퓨터에서 서명된 CSR 을 찾아 선택한 다음 **Upload**(업로드) 를 클릭합니다. 업로드가 성공했다는 확인 메시지가 나타납니다.
5. **Download**(다운로드) 를 클릭하여.pem 인증서를 검색합니다.
6. 계속하려면 CSR 을 완료하고 다음 섹션에 설명된 대로 PKCS #12 파일을 내보냅니다.

CSR 을 완료하고 PKCS #12 파일 내보내기

Apple 에서 APNs 인증서를 받은 후 키체인 접근, Microsoft IIS 또는 OpenSSL 로 돌아가서 인증서를 PCKS #12 파일로 내보냅니다.

PKCS #12 파일에는 APNS 인증서 파일과 개인 키가 들어 있습니다. PFX 파일의 확장자는 일반적으로.pfx 또는.p12 입니다. .pfx 및.p12 파일을 서로 바꿔서 사용할 수 있습니다.

중요:

로컬 시스템에서 개인 및 공개 키를 저장하거나 내보내는 것이 좋습니다. 재사용을 위해 APNs 인증서에 액세스하려면 키가 필요합니다. 동일한 키가 없으면 인증서가 유효하지 않으므로 전체 CSR 및 APNs 프로세스를 반복해야 합니다.

macOS 에서 키체인 접근을 사용하여 PKCS #12 파일 만들기

중요:

이 작업에는 CSR 을 생성할 때 사용한 것과 동일한 macOS 장치를 사용합니다.

1. 장치에서 Apple 에서 받은 프로덕션 ID(.pem) 인증서를 찾습니다.
2. 키체인 접근 응용 프로그램을 시작하고 **Login**(로그인) > **My Certificates**(내 인증서) 탭으로 이동합니다. 제품 ID 인증서를 열려 있는 창으로 끌어다 놓습니다.
3. 인증서를 클릭하고 왼쪽 화살표를 확장하여 인증서에 연결된 개인 키가 포함되어 있는지 확인합니다.
4. 인증서를 PKCS #12(.pfx) 인증서로 내보내려면 인증서와 개인 키를 선택하고 마우스 오른쪽 단추로 클릭한 다음 **Export 2 items**(2 개 항목 내보내기) 를 선택합니다.
5. 인증서 파일에 XenMobile 에서 사용할 고유 이름을 지정합니다. 이름에 공백 문자를 사용하지 마십시오. 저장된 인증서의 폴더 위치를 선택하고.pfx 파일 형식을 선택한 후 저장을 클릭합니다.
6. 인증서를 내보낼 암호를 입력합니다. 고유하고 강력한 암호를 사용하는 것이 좋습니다. 또한 나중에 사용하고 참조할 수 있도록 인증서와 암호를 안전하게 보관하십시오.
7. 키체인 접근 앱에 로그인 암호 또는 선택한 키체인을 묻는 메시지가 나타납니다. 암호를 입력한 다음 **OK**(확인) 를 클릭합니다. 이제 저장된 인증서를 XenMobile Server 에서 사용할 수 있습니다.
8. 계속하려면 XenMobile 로 APN 인증서 가져오기를 참조하십시오.

Microsoft IIS 를 사용하여 PKCS #12 파일 만들기

중요:

이 작업에는 CSR 을 생성하는 데 사용한 IIS 서버와 동일한 서버를 사용합니다.

1. Microsoft IIS 를 엽니다.
2. 서버 인증서 아이콘을 클릭합니다.
3. 서버 인증서 창에서 인증서 요청 완료를 클릭합니다.
4. Apple 의 Certificate.pem 파일을 찾아 선택합니다. 그런 다음 친숙한 이름이나 인증서 이름을 입력하고 확인을 클릭합니다. 이름에 공백 문자를 사용하지 마십시오.
5. 4 단계에서 식별한 인증서를 선택하고 내보내기를 클릭합니다.
6. .pfx 인증서의 위치 및 파일 이름과 암호를 지정한 다음 확인을 클릭합니다.
인증서를 XenMobile 로 가져오려면 해당 인증서의 암호가 필요합니다.
7. XenMobile 을 설치할 서버에.pfx 인증서를 복사합니다.
8. 계속하려면 XenMobile 로 APN 인증서 가져오기를 참조하십시오.

OpenSSL 을 사용하여 PKCS #12 파일 만들기

OpenSSL 을 사용하여 CSR 을 만드는 경우 OpenSSL 을 사용하여.pfx APNs 인증서도 만들 수 있습니다.

1. 명령 프롬프트 또는 셸에서 다음 명령을 실행합니다. `Customer.privatekey.pem`은 CSR 의 개인 키이고 `APNs_Certificate.pem`은 방금 Apple 에서 받은 인증서입니다.

```
openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
```
2. .pfx 인증서 파일의 암호를 입력합니다. XenMobile 에 인증서를 업로드할 때 암호를 다시 사용하므로 이 암호를 기억하고 있어야 합니다.
3. .pfx 인증서 파일의 위치를 기록합니다. 콘솔을 사용하여 파일을 업로드할 수 있도록 파일을 XenMobile Server 에 복사합니다.
4. 계속하려면 다음 섹션에 설명된 대로 APNs 인증서를 XenMobile 로 가져옵니다.

XenMobile 로 APNs 인증서 가져오기

새 APNs 인증서를 받은 후 APNs 인증서를 XenMobile 로 가져와 인증서를 처음으로 추가하거나 인증서를 바꿉니다.

1. XenMobile 콘솔에서 설정 > 인증서로 이동합니다.
2. 가져오기 > 키 저장소를 클릭합니다.

3. 용도에서 **APNs** 를 선택합니다.
4. 컴퓨터에서.pfx 또는.p12 파일을 찾습니다.
5. 암호를 입력하고 가져오기를 클릭합니다.

XenMobile 의 인증서에 대한 자세한 내용은 [인증서 및 인증](#)을 참조하십시오.

APNs 인증서 갱신

중요:

갱신 프로세스에 다른 Apple ID 를 사용하는 경우 사용자 장치를 다시 등록해야 합니다.

APNs 인증서를 갱신하려면 인증서를 만드는 단계를 수행한 다음 [Apple Push Certificates Portal](#)로 이동합니다. 포털을 사용하여 새 인증서를 업로드합니다. 로그인하면 기존 인증서 또는 이전 Apple Developers 계정에서 가져온 인증서가 표시됩니다.

Certificates Portal 에서 인증서를 갱신할 때 유일한 차이점은 **Renew(갱신)** 를 클릭한다는 것입니다. 사이트에 액세스하려면 Certificates Portal 에 개발자 계정이 있어야 합니다. 인증서를 갱신하려면 동일한 조직 이름과 Apple ID 를 사용합니다.

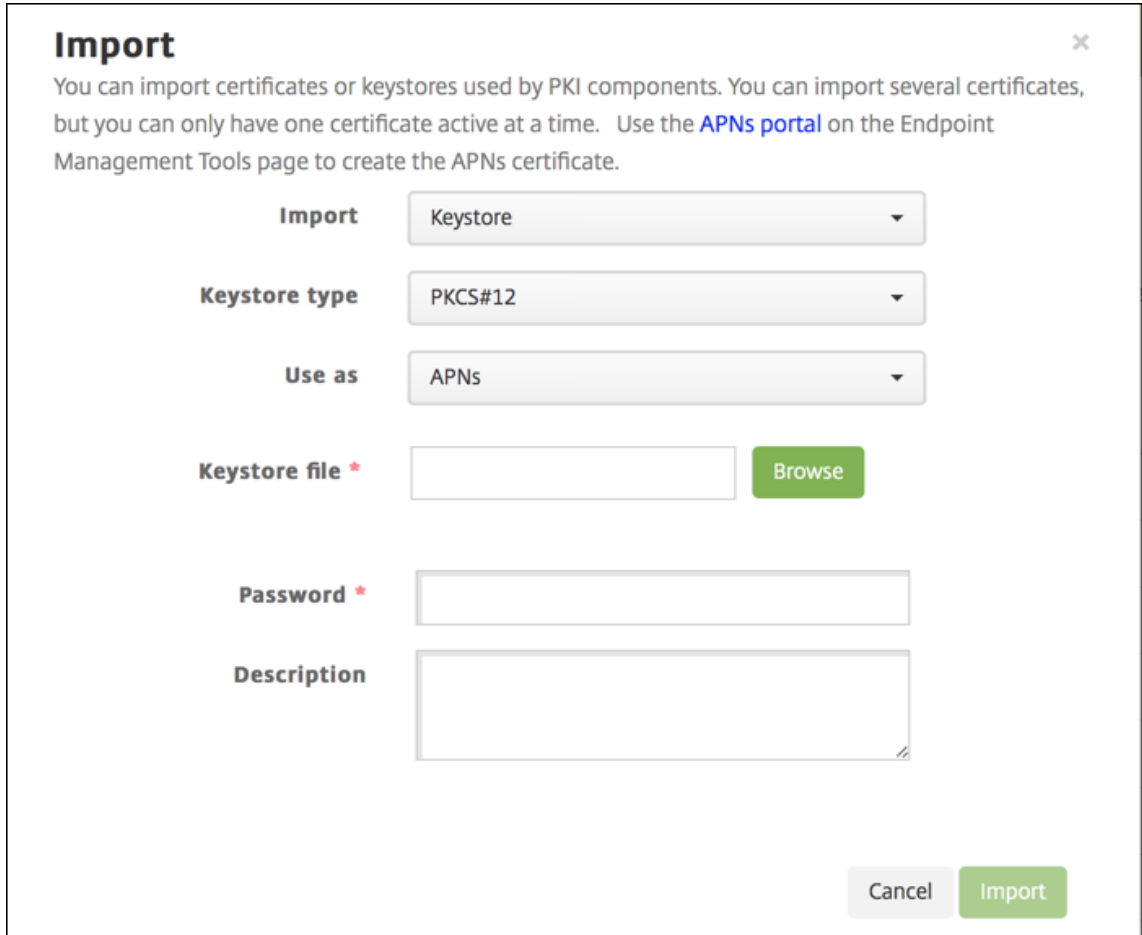
APNs 인증서 만료 시기를 확인하려면 XenMobile 콘솔에서 설정 > 인증서로 이동합니다. 인증서가 만료된 경우 해지하지 마십시오.

1. Microsoft IIS, 키체인 접근 (macOS) 또는 OpenSSL 을 사용하여 CSR 을 생성합니다. CSR 생성에 대한 자세한 내용은 인증서 서명 요청 만들기를 참조하십시오.
2. 브라우저에서 [Endpoint Management 도구](#)로 이동합니다. 그런 다음 **Request push notification certificate signature(푸시 알림 인증서 서명 요청)** 를 클릭합니다.
3. **+ Upload the CSR(+ CSR 업로드)** 을 클릭합니다.
4. 대화 상자에서 CSR 로 이동한 후 **Open(열기)** 을 클릭하고 **Sign(서명)** 을 클릭합니다.
5. **.plist** 파일이 표시되면 저장합니다.
6. 3 단계 제목에서 **Apple Push Certificates Portal** 을 클릭하고 로그인합니다.
7. 갱신할 인증서를 선택하고 **Renew(갱신)** 를 클릭합니다.
8. **.plist** 파일을 업로드합니다. **.pem** 파일이 출력으로 표시됩니다. **.pem** 파일을 저장합니다.
9. 이.pem 파일을 사용하여 CSR 을 완료합니다 (1 단계에서 CSR 을 생성할 때 사용한 방법에 따라).
10. 인증서를.pfx 파일로 내보냅니다.

XenMobile 콘솔에서.pfx 파일을 가져오고 다음과 같이 구성을 완료합니다.

1. 설정 > 인증서 > 가져오기로 이동합니다.

2. 가져오기 메뉴에서 키 저장소를 선택합니다.
3. 키 저장소 유형 메뉴에서 **PKCS#12** 를 선택합니다.
4. 용도에서 **APNs** 를 선택합니다.



The image shows a modal dialog box titled "Import" with a close button (X) in the top right corner. Below the title is a descriptive text: "You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate." Below this text are four rows of form controls: 1. "Import" label followed by a dropdown menu showing "Keystore". 2. "Keystore type" label followed by a dropdown menu showing "PKCS#12". 3. "Use as" label followed by a dropdown menu showing "APNs". 4. "Keystore file *" label followed by a text input field and a green "Browse" button. Below these are two more rows: "Password *" followed by a text input field, and "Description" followed by a larger text area. At the bottom right of the dialog are two buttons: a grey "Cancel" button and a green "Import" button.

5. 키 저장소 파일에 대해 찾아보기를 클릭하고 해당 파일로 이동합니다.
6. 암호에 인증서 암호를 입력합니다.
7. 필요한 경우 설명을 입력합니다.
8. 가져오기를 클릭합니다.

XenMobile 의 인증서 페이지로 리디렉션됩니다. 이름, 상태, 유효 기간 시작일 및 유효 기간 종료일 필드가 업데이트됩니다.

Citrix Files 의 **SSO(Single Sign-on)** 용 **SAML**

December 8, 2023

SAML(Security Assertion Markup Language) 을 사용하여 Citrix Files 모바일 응용 프로그램에 대한 SSO(Single Sign-On) 액세스를 제공하도록 XenMobile 및 ShareFile 을 구성할 수 있습니다. 이 기능에는 다음이 포함됩니다.

- MDX Toolkit 을 통해 MAM SDK 를 사용하거나 래핑된 Citrix Files 앱
- 웹사이트, Outlook 플러그인 또는 동기화 클라이언트와 같이 래핑되지 않은 Citrix Files 클라이언트
- 래핑된 **Citrix Files** 앱의 경우. Citrix Files 모바일 앱을 통해 Citrix Files 에 로그인하는 사용자는 사용자 인증과 SAML 토큰 획득을 위해 Secure Hub 로 리디렉션됩니다. 인증이 성공하면 Citrix Files 모바일 응용 프로그램이 SAML 토큰을 ShareFile 로 전송합니다. 초기 로그인 후 사용자는 SSO 를 통해 Citrix Files 모바일 앱에 액세스할 수 있습니다. 또한 매번 로그인하지 않고도 ShareFile 의 문서를 Secure Mail 메일에 첨부할 수 있습니다.
- 래핑되지 않은 **Citrix Files** 클라이언트의 경우. 웹 브라우저 또는 다른 Citrix Files 클라이언트를 사용하여 Citrix Files 에 로그인하는 사용자가 XenMobile 로 리디렉션됩니다. XenMobile 이 사용자를 인증하면 인증된 사용자가 받은 SAML 토큰이 ShareFile 로 전송됩니다. 초기 로그인 후 사용자는 매번 로그인하지 않고 SSO 를 통해 Citrix Files 클라이언트에 액세스할 수 있습니다.

XenMobile 을 ShareFile 에 대한 SAML IdP(ID 공급자) 로 사용하려면 이 문서에 설명된 대로 Enterprise 계정과 사용하도록 XenMobile 을 구성해야 합니다. 또한 StorageZone 커넥터에서만 작동하도록 XenMobile 을 구성할 수 있습니다. 자세한 내용은 [XenMobile 에서 ShareFile 사용](#)을 참조하십시오.

자세한 참조 아키텍처 다이어그램은 [아키텍처](#)를 참조하십시오.

사전 요구 사항

XenMobile 및 Citrix Files 앱에서 SSO 를 구성하려면 먼저 다음과 같은 사전 요구 사항을 충족해야 합니다.

- MAM SDK 또는 호환되는 버전의 MDX Toolkit(Citrix Files 모바일 응용)
자세한 내용은 [XenMobile 호환성](#)을 참조하십시오.
- 호환되는 버전의 Citrix Files 모바일 앱 및 Secure Hub.
- ShareFile 관리자 계정.
- XenMobile 과 ShareFile 간의 연결이 확인됨

ShareFile 액세스 구성

ShareFile 를 위한 SAML 을 설정하기 전에 다음과 같이 ShareFile 액세스 정보를 제공합니다.

1. XenMobile 웹 콘솔에서 구성 > **ShareFile** 을 클릭합니다. **ShareFile** 구성 페이지가 나타납니다.

Content Collaboration ▼

Configure settings to connect to the Content Collaboration and administrator service accounts for user account management.

Domain *

Assign to delivery groups

- ☐ AllUsers
- ☐ Local Policy
- ☐ o87
- ☐ Local

Content Collaboration Administrator Account Logon

User name *

Password *

User account provisioning ☐ OFF

App internal name

SAML certificate

Name

Advanced Content Collaboration Configuration

2. 다음 설정을 구성합니다.

- 도메인: ShareFile 하위 도메인 이름을 입력합니다. 예: `example.sharefile.com`.
- 배달 그룹에 할당: ShareFile 에서 SSO 를 사용할 수 있게 하려는 배달 그룹을 선택하거나 검색합니다.
- **ShareFile** 관리자 계정 로그인
- 사용자 이름: ShareFile 관리자 사용자 이름을 입력합니다. 이 사용자는 관리자 권한을 가지고 있어야 합니다.
- 암호: ShareFile 관리자 암호를 입력합니다.
- 사용자 계정 프로비저닝: 이 설정을 사용하지 않도록 설정합니다. ShareFile 사용자 관리 도구를 사용자 프로비전에 사용합니다. [사용자 계정 및 메일 그룹 프로비전](#)을 참조하십시오.

3. 연결 테스트를 클릭하여 ShareFile 관리자 계정이 지정된 ShareFile 계정으로 인증하는 사용자 이름과 암호를 확인합니다.

4. 저장을 클릭합니다.

- XenMobile 이 ShareFile 과 동기화되고 ShareFile 설정인 **ShareFile** 발급자/엔터티 ID 및 로그인 URL 이 업데이트됩니다.
- 구성 > **ShareFile** 페이지에 앱 내부 이름이 표시됩니다. Citrix Files.com SSO 설정 수정의 뒷부분에 설명된 단계를 완료하려면 이 이름이 필요합니다.

래핑된 **Citrix Files MDX** 앱을 위한 **SAML** 설정

래핑된 Citrix Files MDX 앱의 Single Sign-on 구성에 Citrix Gateway 를 사용하지 않아도 됩니다. 웹사이트, Outlook 플러그인 또는 동기화 클라이언트와 같이 래핑되지 않은 Citrix Files 클라이언트에 대한 액세스를 구성하려면 [다른 Citrix Files 클라이언트에 대한 Citrix Gateway 구성](#)을 참조하십시오.

다음 단계는 iOS 및 Android 앱 및 장치에 적용됩니다. 래핑된 Citrix Files MDX 앱에 대해 SAML 을 구성하려면 다음을 수행합니다.

1. MDX Toolkit 을 사용하여 Citrix Files 모바일 앱을 래핑합니다. MDX Toolkit 으로 앱을 래핑하는 것에 대한 자세한 내용은 [Wrapping Apps with the MDX Toolkit\(MDX Toolkit 으로 앱 래핑\)](#)을 참조하십시오.
2. XenMobile 콘솔에서 래핑된 Citrix Files 모바일 앱을 업로드합니다. MDX 앱 업로드에 대한 자세한 내용은 [XenMobile 에 MDX 앱을 추가하려면](#)을 참조하십시오.
3. 위에서 구성한 관리자 사용자 이름과 암호로 ShareFile 에 로그인하여 SAML 설정을 확인합니다.
4. ShareFile 및 XenMobile 이 동일한 표준 시간대로 구성되어 있는지 확인합니다. XenMobile 이 구성된 표준 시간대를 기준으로 정확한 시간을 표시하는지 확인합니다. 그렇지 않은 경우 SSO 가 실패할 수 있습니다.

Citrix Files 모바일 앱의 유효성 검사

1. 사용자 장치에서 Secure Hub 를 설치하고 구성합니다.
2. XenMobile Store 에서 Citrix Files 모바일 앱을 다운로드하고 설치합니다.
3. Citrix Files 모바일 앱을 시작합니다. Citrix Files 는 사용자 이름이나 암호를 묻지 않고 시작됩니다.

Secure Mail 로 유효성 검사

1. 아직 완료하지 않은 경우 사용자 장치에서 Secure Hub 를 설치하고 구성합니다.
2. XenMobile Store 에서 Secure Mail 을 다운로드하여 설치하고 설정합니다.
3. 새 전자 메일 양식을 열고 **Citrix Files** 에서 첨부을 누릅니다. 사용자 이름이나 암호를 묻지 않고 전자 메일에 첨부할 수 있는 파일이 표시됩니다.

다른 **Citrix Files** 클라이언트에 대한 **Citrix Gateway** 구성

웹 사이트, Outlook 플러그인 또는 동기화 클라이언트와 같이 래핑되지 않은 Citrix Files 클라이언트에 대한 액세스 권한을 구성하려면 다음과 같이 XenMobile 을 SAML ID 공급자로 사용하는 것을 지원하도록 Citrix Gateway 를 구성합니다.

- 홈 페이지 리디렉션을 사용하지 않도록 설정합니다.
- Citrix Files 세션 정책 및 프로필을 만듭니다.
- Citrix Gateway 가상 서버에서 정책을 구성합니다.

홈 페이지 리디렉션 사용 안 함

/cginfra 경로를 통해 수신되는 요청의 기본 동작을 사용하지 않도록 설정합니다. 이렇게 하면 사용자가 구성된 홈 페이지 대신 원래 요청된 내부 URL 을 볼 수 있습니다.

1. XenMobile 로그인에 사용되는 Citrix Gateway 가상 서버의 설정을 편집합니다. Citrix ADC 에서 **Other Settings**(기타 설정) 로 이동한 다음 **Redirect to Home Page**(홈 페이지로 리디렉션) 확인란을 선택 취소합니다.

The screenshot shows the 'Other Settings' configuration page in Citrix ADC. The 'Redirect to Home page' checkbox is checked. Under the 'ShareFile' section, the 'Citrix Endpoint Management' option is highlighted with a red box. The 'L2 Connection' checkbox is unchecked. The 'OK' button is at the bottom.

2. **ShareFile**(현재 ShareFile) 에서 XenMobile 내부 서버의 이름과 포트 번호를 입력합니다.
3. **Citrix Endpoint Management** 아래에 XenMobile URL 을 입력합니다. 사용 중인 Citrix Gateway 버전에 이전 제품 이름인 **AppController** 가 표시될 수 있습니다.

이 구성은 /cginfra 경로를 통해 입력된 URL 에 대한 요청을 인증합니다.

Citrix Files 세션 정책 및 요청 프로필 만들기

다음과 같은 설정을 구성하여 Citrix Files 세션 정책 및 요청된 프로필을 만듭니다.

1. Citrix Gateway 구성 유틸리티의 왼쪽 탐색 창에서 **Citrix Gateway > 정책 > 세션**을 클릭합니다.
2. 세션 정책을 만듭니다. 정책 탭에서 추가를 클릭합니다.
3. 이름 필드에 **ShareFile_Policy** 를 입력합니다.
4. + 단추를 클릭하여 동작을 만듭니다. 세션 프로필 만들기 페이지가 나타납니다.

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Accounting Policy
None

Override Global

☐ Display Home Page ☒ Home Page
none

URL for Web-Based Email
None

Split Tunnel*
OFF

Session Time-out (mins)
1

Client Idle Time-out (mins)
None

Clientless Access*
Allow

Clientless Access URL Encoding*
Obscure

Clientless Access Persistent Cookie*
DENY

Plug-in Type*
Windows/MAC OS X

☒ Single Sign-on to Web Applications ☒ Credential Index*
PRIMARY

KCD Account
None

다음 설정을 구성합니다.

- **Name(이름):** **ShareFile_Profile** 을 입력합니다.
- **Client Experience(클라이언트 환경)** 탭을 클릭하고 다음과 같은 설정을 구성합니다.
 - **Home Page(홈 페이지):** **none** 을 입력합니다.
 - **Session Time-out (mins)(세션 시간 제한 (분)):** **1** 을 입력합니다.
 - **Single Sign-on to Web Applications(웹 응용 프로그램에 대한 SSO):** 이 설정을 선택합니다.
 - **Credential Index(자격 증명 색인):** 목록에서 **PRIMARY** 를 클릭합니다.
- **Published Applications(게시된 응용 프로그램)** 탭을 클릭합니다.

Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security **Published Applications**

Override Global

ICA Proxy*
ON ☒

Web Interface Address
https://xms.citrix.lab:8443 ☒ ?

Web Interface Address Type*
IPV4

Web Interface Portal Mode*
NORMAL ☐

Single Sign-on Domain
citrix ☒

Citrix Receiver Home Page
☐

Account Services Address
☐

OK Close

다음 설정을 구성합니다.

- **ICA Proxy(ICA 프록시): ON(켜짐)** 을 클릭합니다.
- **Web Interface Address(웹 인터페이스 주소):** XenMobile Server URL 을 입력합니다.
- **Single Sign-on Domain(SSO 도메인):** Active Directory 도메인 이름을 입력합니다.

Citrix Gateway 세션 프로필을 구성할 때 **Single Sign-on Domain(SSO 도메인)** 의 도메인 접미사는 LDAP 에 정의된 XenMobile 도메인 별칭과 일치해야 합니다.

5. **Create(만들기)** 를 클릭하여 세션 프로필을 정의합니다.
6. **Expression Editor(식 편집기)** 를 클릭합니다.

다음 설정을 구성합니다.

- **Value(값):** NSC_FSRD 를 입력합니다.
- **Header Name(헤더 이름):** COOKIE 를 입력합니다.

7. **Create(만들기)** 를 클릭한 다음 **Close(닫기)** 를 클릭합니다.

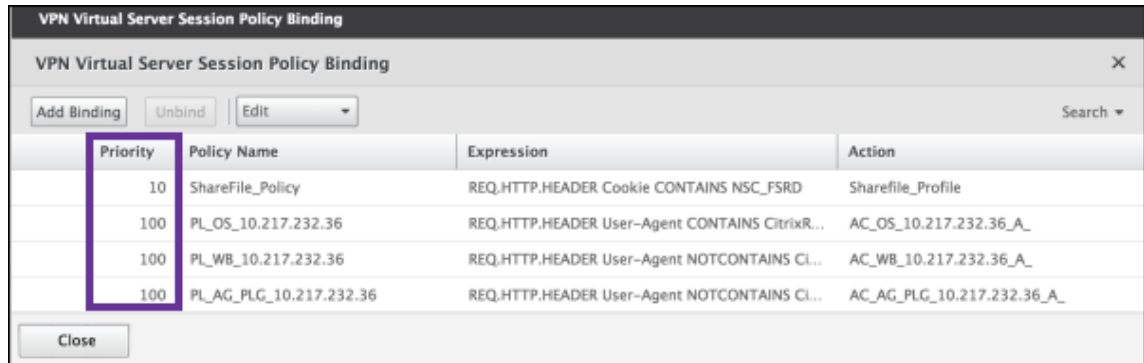
Citrix Gateway 가상 서버에서 정책 구성

Citrix Gateway 가상 서버에서 다음과 같은 설정을 구성합니다.

1. Citrix Gateway 구성 유틸리티의 왼쪽 탐색 창에서 **Citrix Gateway >** 가상 서버를 클릭합니다.
2. **Details(세부 정보)** 창에서 Citrix Gateway 가상 서버를 클릭합니다.
3. 편집을 클릭합니다.
4. **Configured policies(구성된 정책) > Session policies(세션 정책)** 를 클릭한 다음 **Add binding(바인딩 추가)** 을 클릭합니다.

5. **ShareFile_Policy** 를 선택합니다.

6. 선택한 정책의 자동 생성된 **Priority(우선 순위)** 번호를 편집하여 나열된 다른 정책과 비교하여 가장 높은 우선 순위 (가장 작은 숫자) 를 갖도록 설정합니다. 예:



Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_AG_PLG_10.217.232.36_A_

7. **Done(완료)** 을 클릭한 다음 실행 중인 Citrix ADC 구성을 저장합니다.

Citrix Files.com SSO 설정 수정

MDX 및 비 MDX Citrix Files 앱을 다음과 같이 변경합니다.

중요:

다음과 같은 경우 내부 응용 프로그램 이름에 새 번호가 추가됩니다.

- Citrix Files 앱을 수정 또는 재생성할 때마다
- XenMobile 에서 ShareFile 설정을 변경할 때마다

그러므로 Citrix Files 웹 사이트에서 로그인 URL 을 업데이트하여 업데이트된 앱 이름을 반영해야 합니다.

1. ShareFile 계정 (<https://<subdomain>.sharefile.com>) 에 ShareFile 관리자로 로그인합니다.
2. ShareFile 웹 인터페이스에서 관리를 클릭한 다음 **Single Sign-On** 설정 구성을 선택합니다.
3. **Login URL(로그인 URL)** 을 다음과 같이 편집합니다.

다음은 편집 전의 로그인 **URL** 샘플입니다. https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.

- XenMobile Server FQDN 앞에 Citrix Gateway 가상 서버 외부 FQDN 과 **/cginfra/https/**를 삽입한 다음 XenMobile FQDN 뒤에 **8443** 을 추가합니다.

다음은 편집된 URL 의 샘플입니다. `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

- `&app=ShareFile_SAML_SP` 매개 변수를 내부 Citrix Files 응용 프로그램 이름으로 변경합니다. 내부 이름은 기본적으로 `ShareFile_SAML`입니다. 그러나 구성을 변경할 때마다 내부 이름에 번호가 추가됩니다 (`ShareFile_SAML_2`, `ShareFile_SAML_3` 등). 구성 > **ShareFile** 페이지에서 앱 내부 이름을 찾을 수 있습니다.

다음은 편집된 URL 의 샘플입니다. `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- URL 끝에 `&nssso=true`를 추가합니다.

다음은 최종 URL 의 샘플입니다. `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. 옵션 설정에서 웹 인증 사용 확인란을 선택합니다.

Optional Settings

Require SSO Login: ☐ ?

SSO IP Range: ?

SP-Initiated SSO certificate: HTTP Redirect with no signature ?

Enable Web Authentication: ☒ ?

SP-Initiated Auth Context: User Name and Password Minimum ?

Active Profile Cookies: ?

☒ Save Cancel

구성 유효성 검사

다음을 수행하여 구성의 유효성을 검사합니다.

1. 브라우저를 <https://<subdomain>sharefile.com/saml/login>으로 가리킵니다.

Citrix Gateway 로그인 양식으로 리디렉션됩니다. 리디렉션되지 않으면 이전 구성 설정을 확인하십시오.

2. 구성된 Citrix Gateway 및 XenMobile 환경의 사용자 이름과 암호를 입력합니다.

<subdomain>.sharefile.com의 Citrix Files 폴더가 나타납니다. Citrix Files 폴더가 보이지 않으면 적절한 로그인 자격 증명을 입력했는지 확인하십시오.

IdP 역할을 하는 Azure Active Directory

May 6, 2022

Azure Active Directory(ADD) 를 IdP(ID 공급자) 로 구성하면 사용자가 Azure 자격 증명을 사용하여 XenMobile 에 등록할 수 있습니다.

iOS, Android, Windows 10, Windows 11 장치가 지원됩니다. iOS 및 Android 장치는 Secure Hub 를 통해 등록됩니다. 이 인증 방법은 Citrix Secure Hub 를 통해 MDM 에 등록하는 사용자만 사용할 수 있습니다. MAM 에 등록하는 장치는 AAD 자격 증명을 사용하여 인증할 수 없습니다. MDM+MAM 을 통해 Secure Hub 를 사용하려면 MAM 등록에 Citrix Gateway 를 사용하도록 XenMobile 을 구성합니다. 자세한 내용은 [Citrix Gateway 및 XenMobile](#)을 참조하십시오.

설정 > 인증 > **IDP** 에서 Azure 를 IdP 로 구성합니다. **IDP** 페이지는 이 버전의 XenMobile 에 새롭게 추가된 페이지입니다. 이전 버전의 XenMobile 에서는 설정 > **Microsoft Azure** 에서 Azure 를 추가했습니다.

요구 사항

- 버전 및 라이선스
 - iOS 또는 Android 장치를 등록하려면 Secure Hub 10.5.5 가 필요합니다.
 - Windows 10 및 Windows 11 장치를 등록하려면 Microsoft Azure Premium 라이선스가 필요합니다.
- 디렉터리 서비스 및 인증
 - XenMobile Server 가 인증서 기반 인증을 사용하도록 구성해야 합니다.
 - Citrix ADC 를 인증에 사용 중인 경우 인증서 기반 인증을 사용하도록 Citrix ADC 를 구성해야 합니다.
 - Secure Hub 인증은 Azure AD 를 사용하여 Azure AD 에서 정의된 인증 모드를 따릅니다.
 - XenMobile Server 는 LDAP 를 사용하여 Windows AD(Active Directory) 에 연결해야 합니다. 로컬 LDAP 서버가 Azure AD 와 동기화되도록 구성합니다.

인증 흐름

장치가 Secure Hub 를 통해 등록되며 XenMobile 이 Azure 를 IdP 로 사용하도록 구성된 경우:

1. 사용자가 자신의 장치를 사용하여 Secure Hub 에서 표시되는 Azure AD 로그인 화면에 Azure Active Directory 사용자 이름과 암호를 입력합니다.
2. Azure AD 가 사용자를 확인하고 ID 토큰을 보냅니다.
3. Secure Hub 는 ID 토큰을 XenMobile Server 와 공유합니다.
4. XenMobile 이 ID 토큰 및 ID 토큰에 있는 사용자 정보를 확인합니다. XenMobile 이 세션 ID 를 반환합니다.

Azure 계정 설정

Azure AD 를 IdP 로 사용하려면 먼저 Azure 계정에 로그인하고 다음과 같이 변경합니다.

1. 사용자 지정 도메인을 등록하고 도메인을 확인합니다. 자세한 내용은 [Azure Active Directory 에 사용자 지정 도메인 이름 추가](#)를 참조하십시오.
2. 디렉터리 통합 도구를 사용하여 온-프레미스 디렉터리를 Azure Active Directory 로 확장합니다. 자세한 내용은 [디렉터리 통합](#)을 참조하십시오.

Azure AD 를 사용하여 Windows 10 및 Windows 11 장치를 등록하려면 Azure 계정을 다음과 같이 변경합니다.

1. MDM 을 Azure AD 의 신뢰할 수 있는 당사자로 설정합니다. 이를 위해 **Azure Active Directory > 응용 프로그램**을 클릭한 다음 추가를 클릭합니다.
2. 갤러리에서 응용 프로그램 추가를 선택합니다. 모바일 기기 관리로 이동하고 온-프레미스 **MDM** 응용 프로그램을 선택합니다. 설정을 저장합니다.

Citrix XenMobile Cloud 에 등록된 경우에도 온-프레미스 응용 프로그램을 선택합니다. Microsoft 용어에서 다중 테넌트가 아닌 모든 응용 프로그램은 온-프레미스 MDM 응용 프로그램입니다.

3. 응용 프로그램에서 XenMobile Server 검색, 사용 약관 끝점, 앱 ID URI 를 구성합니다.

- **MDM 검색 URL:** <https://<FQDN>:8443/<instanceName>/wpe>
- **MDM 사용 약관 URL:** <https://<FQDN>:8443/<instanceName>/wpe/tou>
- **앱 ID URI:** <https://<FQDN>:8443/>

4. 2 단계에서 만든 온-프레미스 MDM 응용 프로그램을 선택합니다. 이 사용자의 장치 관리 옵션을 선택하여 모든 사용자 또는 특정 사용자 그룹에 대한 MDM 관리를 사용하도록 설정합니다.

Windows 10 및 Windows 11 장치에 Azure AD 를 사용하는 방법에 대한 자세한 내용은 Microsoft 문서 [Azure Active Directory](#) 와 [MDM 통합](#)을 참조하십시오.

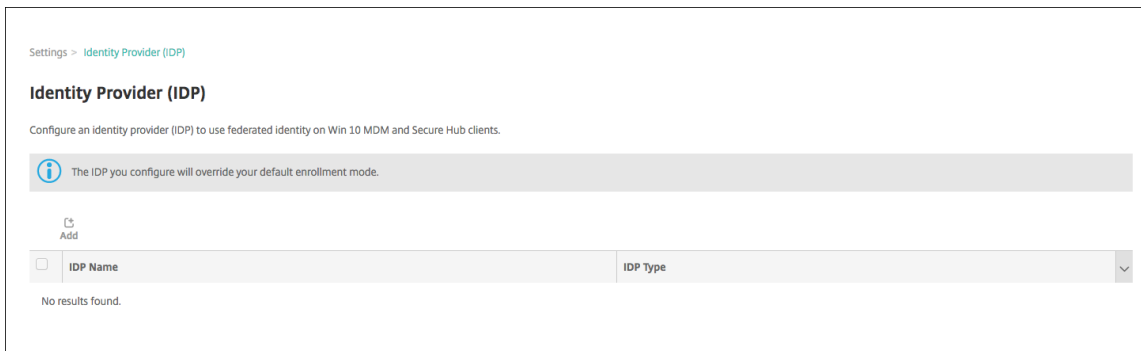
Azure AD 를 IdP 로 구성

1. Azure 계정에서 필요한 다음 정보를 찾거나 메모합니다.

- Azure 응용 프로그램 설정 페이지의 테넌트 ID.
- Azure AD 를 사용하여 Windows 10 및 Windows 11 장치를 등록하려는 경우 다음도 필요합니다.
 - **앱 ID URI:** XenMobile 을 실행하는 서버의 URL 입니다.
 - **클라이언트 ID:** Azure 구성 페이지에서 앱의 고유 식별자입니다.
 - **키:** Azure 응용 프로그램 설정 페이지에서 확인할 수 있습니다.

2. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.

3. 인증 아래에서 **IDP(ID 공급자)** 를 클릭합니다. **ID** 공급자 페이지가 나타납니다.



4. 추가를 클릭합니다. **IDP** 구성 페이지가 나타납니다.

5. IdP 에 대한 다음 정보를 구성합니다.

- **IDP 이름:** 만들려는 IdP 연결의 이름을 입력합니다.
- **IDP 유형:** Azure Active Directory 를 IdP 유형으로 선택합니다.

- **테넌트 ID:** Azure 응용 프로그램 설정 페이지에서 이 값을 복사합니다. 브라우저 주소 표시줄에서 숫자와 문자로 구성된 섹션을 복사합니다.

예 를 들 어 <https://manage.windowsazure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...>에서 테넌트 ID 는 **abc123-abc123-abc123**입니다.

6. 나머지 필드는 자동으로 입력됩니다. 입력되면 다음을 클릭합니다.

7. MDM 등록에 대해 Azure AD 를 사용하여 Windows 10 및 Windows 11 장치를 등록하도록 XenMobile 을 구성하려면 다음 설정을 구성하십시오. 이 선택적 단계를 건너뛰려면 **Windows MDM** 을 선택 취소합니다.

- **앱 ID URI:** Azure 설정을 구성할 때 입력한 XenMobile Server 의 URL 을 입력합니다.
- **클라이언트 ID:** Azure 구성 페이지에서 이 값을 복사하여 붙여 넣습니다. 클라이언트 ID 는 앱의 고유 식별자입니다.
- **키:** Azure 응용 프로그램 설정 페이지에서 이 값을 복사합니다. 키 아래에 있는 목록에서 기간을 선택하고 설정을 저장합니다. 그런 다음 키를 복사하여 이 필드에 붙여 넣을 수 있습니다. 앱이 Microsoft Azure AD 에서 데이터를 읽거나 쓸 때 키가 필요합니다.

Settings > Identity Provider (IDP) > Add IDP

Identity Provider (IDP)

- 1 Discovery URL
- 2 Client Type
- ☒ Win 10 MDM
- ☒ Secure Hub
- 3 IDP Claims Usage
- 4 Summary

Win 10 MDM Info
Integrate XenMobile with Azure Active Directory to let devices running Windows 10, enroll with Azure as a federated means of Active Directory authentication

App ID URI * ⓘ

Client ID * ⓘ

Key * ⓘ

Back Next >

8. 다음을 클릭합니다.

Citrix 는 Secure Hub 를 Microsoft Azure 에 등록했으며 정보를 유지합니다. 이 화면에는 Secure Hub 가 Azure Active Directory 와 통신하는 데 사용하는 세부 정보가 표시됩니다. 이 페이지는 향후 이러한 정보를 변경해야 할 때 사용됩니다. Citrix 에서 편집하도록 안내하는 경우에만 이 페이지를 편집하십시오.

9. 다음을 클릭합니다.

Settings > Identity Provider (IDP) > Add IDP

Identity Provider (IDP)

- 1 Discovery URL
- 2 Client Type
- ☒ Win 10 MDM
- ☒ Secure Hub
- 3 IDP Claims Usage
- 4 Summary

Secure Hub Info
Configure details that Secure Hub mobile client in Android and iOS platforms can use to authenticate using Azure AD.

Citrix has provided this information for Secure Hub to use to authenticate with Azure Active Directory.

Client ID * ⓘ Edit

Redirect_URI * ⓘ

Scopes * ⓘ

Back Next >

10. IdP 가 제공하는 사용자 식별자 유형을 구성합니다.

- 사용자 식별자 유형: 드롭다운 목록에서 **userPrincipalName** 을 선택합니다.
- 사용자 식별자 문자열: 이 필드는 자동으로 입력됩니다.

11. 다음을 클릭합니다.

Settings > Identity Provider (IDP) > Add IDP

Identity Provider (IDP)

- 1 Discovery URL
- 2 Client Type
 - ☒ Win 10 MDM
 - ☒ Secure Hub
 - 3 IDP Claims Usage**
 - 4 Summary

IDP Claims Usage

Choose the type of user identifier that IDP is providing.

XenMobile uses the 'upn' key to retrieve the user information from the jwt token provided by Azure Active Directory.

User Identifier type*

User Identifier string*

Back **Next >**

12. 요약 페이지를 검토하고 저장을 클릭합니다.

Identity Provider (IDP)

- 1 Discovery URL
- 2 Client Type
 - ☒ Win 10 MDM
 - ☒ Secure Hub
 - 3 IDP Claims Usage
 - 4 Summary**

Token endpoint (URL)

Jwks_uri (JSON Web Key Set URI)

End Session endpoint (URL)

Win 10 MDM

App ID URI

Client ID

Key

Secure Hub Info

Client ID

Client Secret (optional)

Redirect_URI

Scopes

IDP Claims Usage

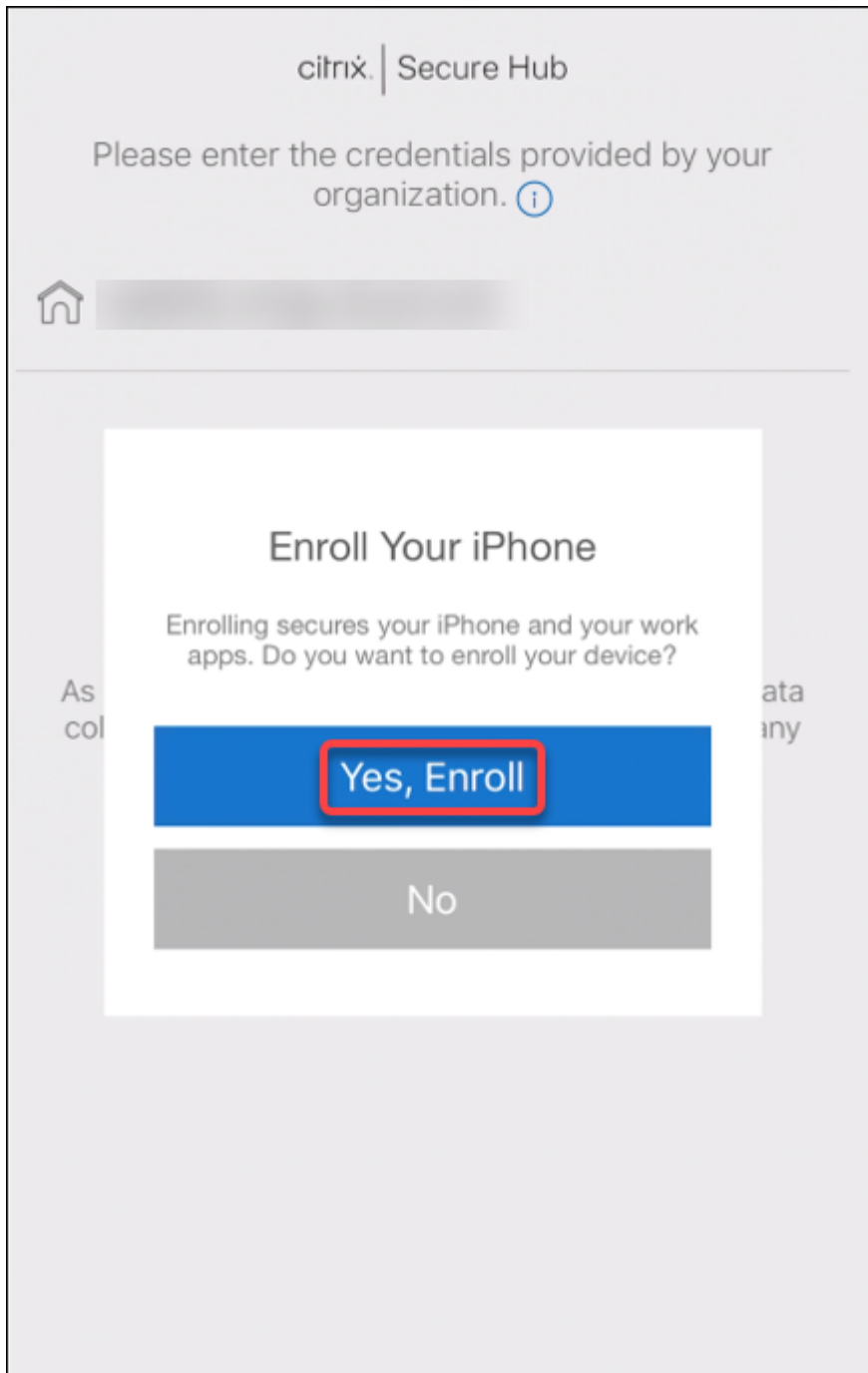
User Identifier type

User Identifier string

Back **Save**

사용자가 경험하는 환경

1. 사용자가 Secure Hub 를 시작합니다. 그런 다음 사용자는 XenMobile Server 의 FQDN(정규화된 도메인 이름), UPN(사용자 계정 이름) 또는 전자 메일 주소를 입력합니다.



2. 그리고 예. 등록하겠습니다를 클릭합니다.

No SIM

10:20 AM

Cancel

Sign On

xmslab

Sign in with your organizational account

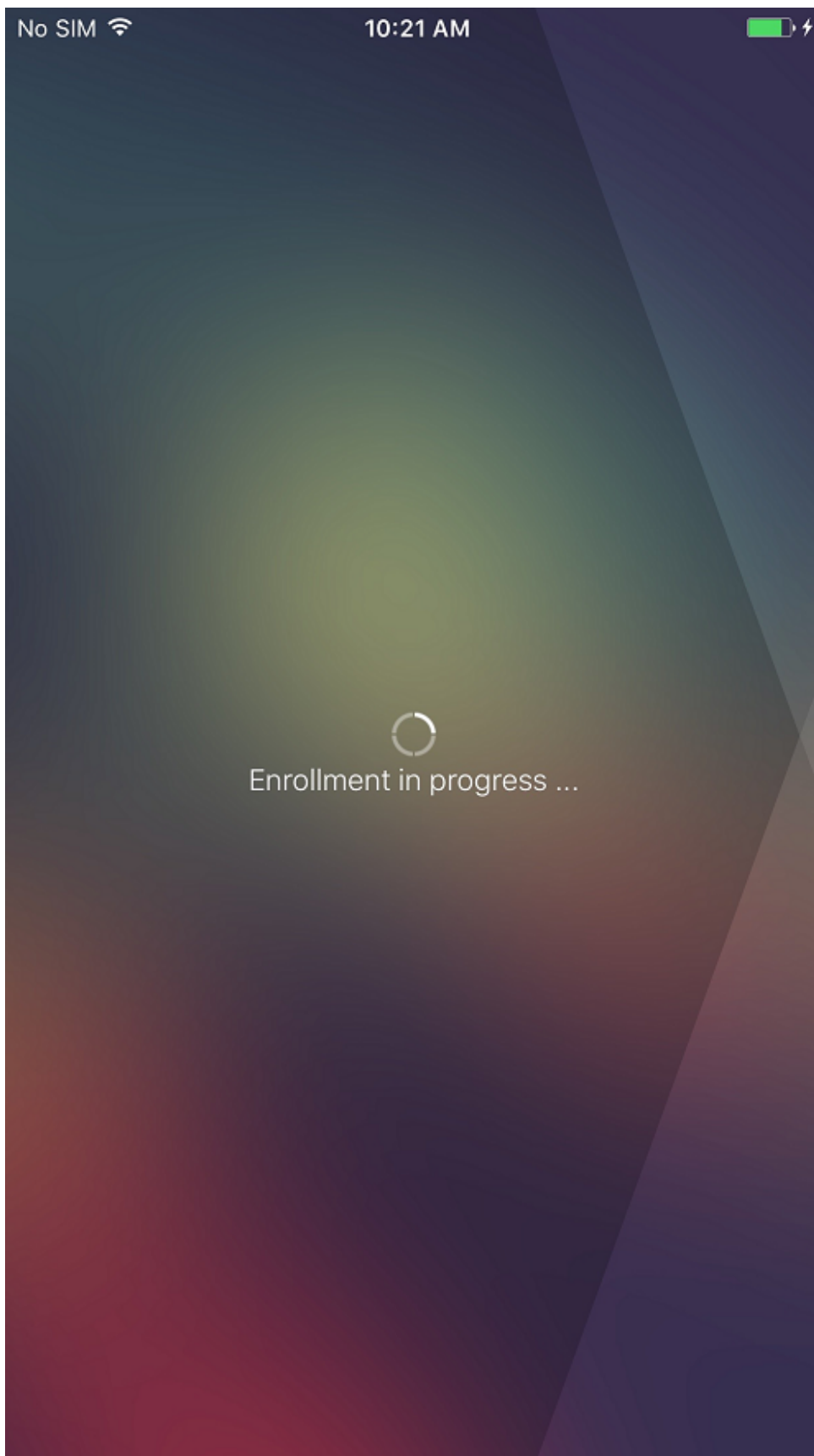
someone@example.com

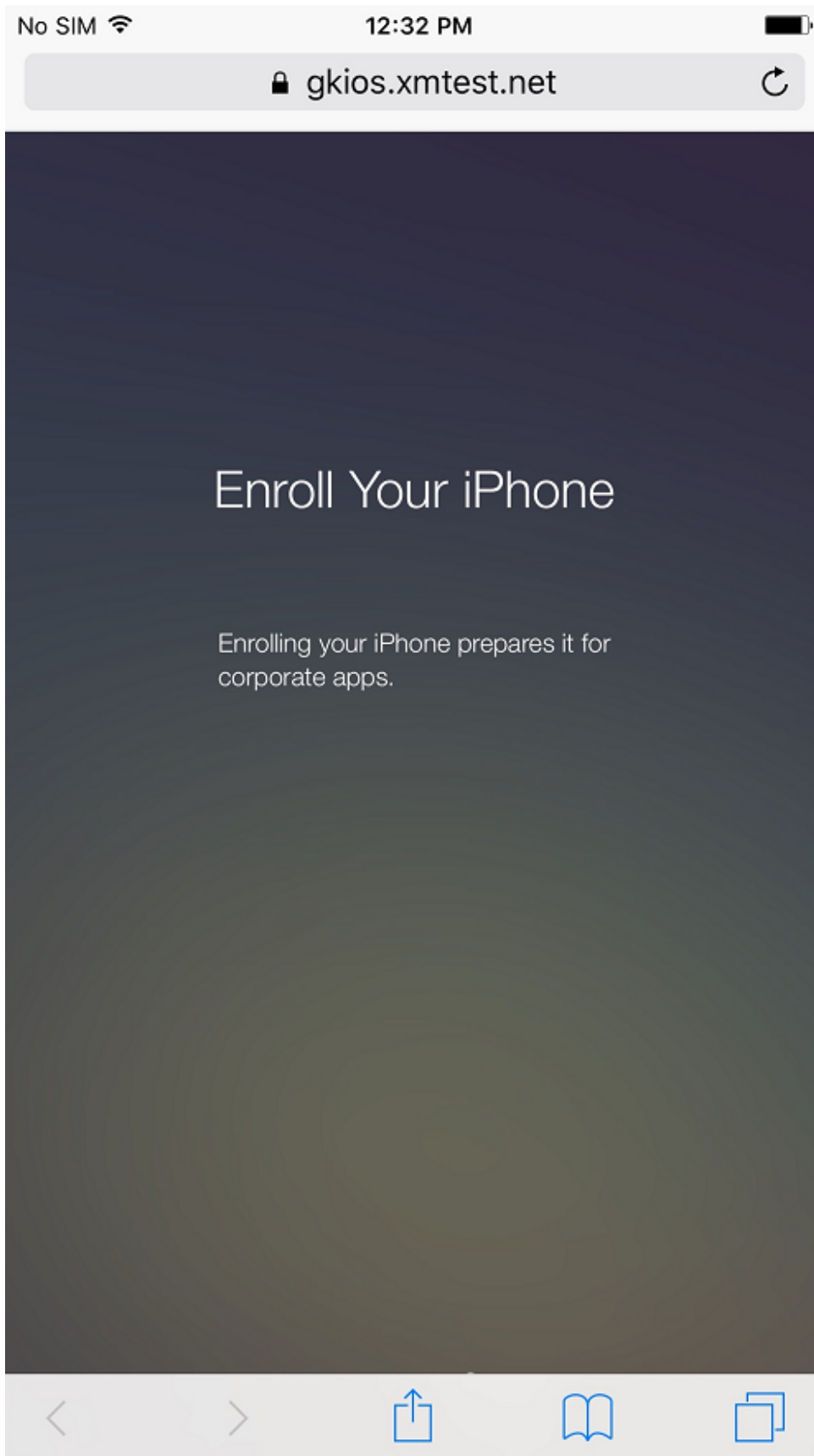
Password

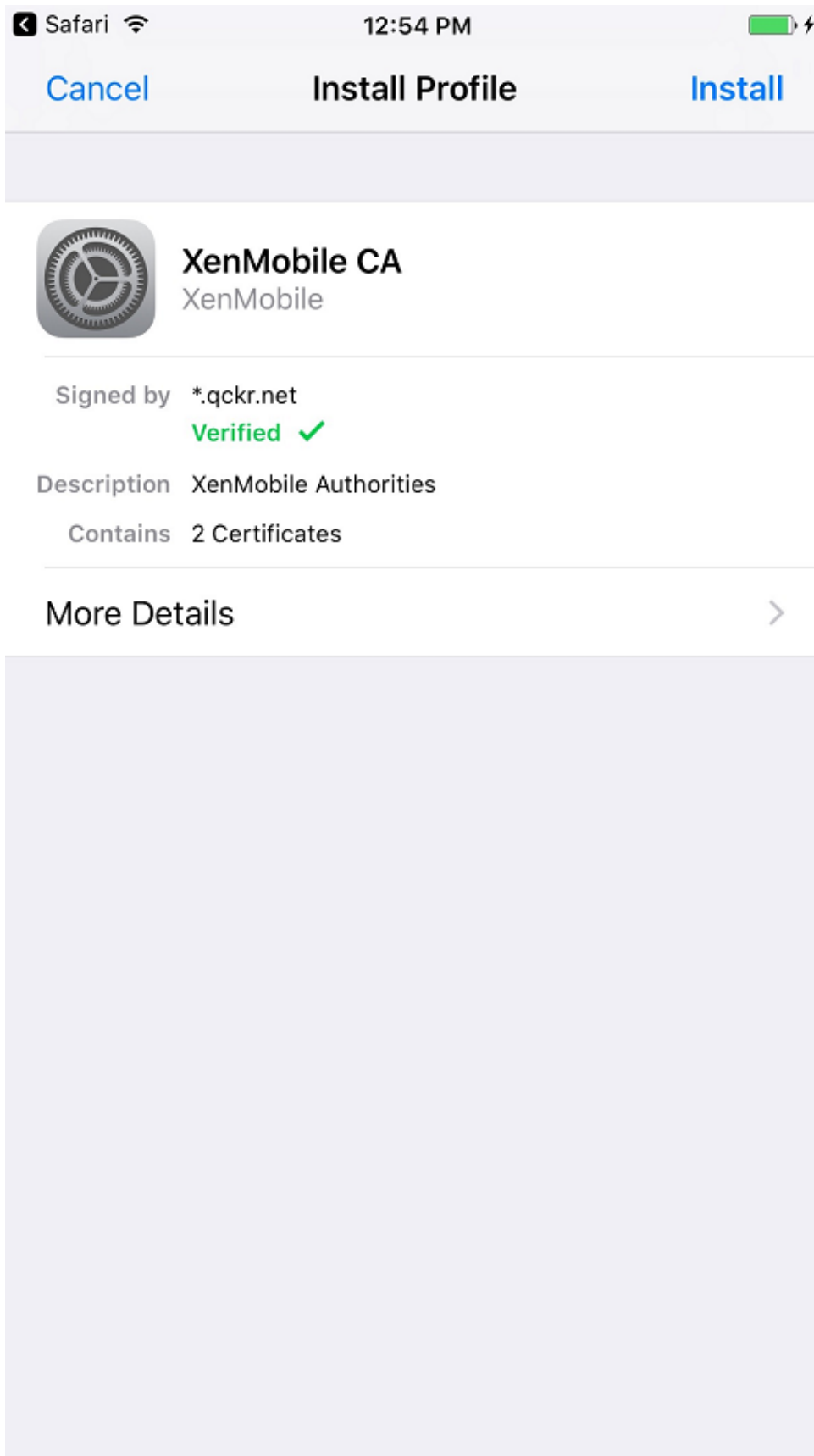
Sign in

© 2016 Microsoft

3. 사용자는 자신의 Azure AD 자격 증명을 사용하여 로그인합니다.







4. 사용자는 Secure Hub 를 통한 다른 등록과 동일한 방법으로 등록 단계를 완료합니다.

참고:

XenMobile 은 등록 초대에 대해 Azure AD 를 통한 인증을 지원하지 않습니다. 사용자에게 등록 URL 이 포함된 등록 초대를 보내는 경우 사용자는 Azure AD 대신 LDAP 를 통해 인증합니다.

업그레이드

March 15, 2024

팁: XenMobile Migration Service

XenMobile Server 를 온-프레미스에서 사용하는 경우 무료 XenMobile 마이그레이션 서비스를 사용하여 Endpoint Management 를 시작할 수 있습니다. XenMobile Server 에서 Citrix Endpoint Management 로 마이그레이션할 때 장치를 재등록할 필요는 없습니다.

자세한 내용은 해당 지역의 Citrix 영업 사원, 시스템 엔지니어 또는 Citrix 파트너에게 문의하십시오. 다음 블로그에 XenMobile 마이그레이션 서비스에 대한 자세한 내용이 나와 있습니다.

[New XenMobile Migration Service\(새로운 XenMobile 마이그레이션 서비스\)](#)

[Making the Case for XenMobile in the Cloud\(클라우드에서 XenMobile 용 사례 만들기\)](#)

XenMobile 10.15 로 업그레이드하기 전에

1. 최신 버전의 XenMobile Server 10.15 로 업데이트하기 전에 Citrix License Server 를 11.17 이상으로 업데이트 하십시오.

최신 버전의 XenMobile 에는 Citrix License Server 11.17(최소 버전) 이 필요합니다.

XenMobile 10.15 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2022 년 11 월 15 일입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 이후여야 합니다. 날짜는 라이선스 서버의 라이선스 옆에서 볼 수 있습니다. 최신 버전의 XenMobile 을 이전 버전의 라이선스 서버 환경에 연결하면 연결 확인이 실패하고 라이선스 서버를 구성할 수 없게 됩니다.

라이선스의 날짜를 갱신하려면 Citrix 포털에서 최신 라이선스 파일을 다운로드하고 라이선스 서버에 파일을 업로드하십시오. 자세한 내용은 [Customer Success Services](#)를 참조하십시오.

2. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 iOS 정책 및 앱을 배포하려면 다음과 같은 요구 사항이 충족되어야 합니다. Citrix Gateway 에 SSL 지속성이 구성되어 있으면 모든 XenMobile Server 노드에서 포트 80 을 열어야 합니다.
3. 업그레이드할 XenMobile Server 를 실행하는 가상 컴퓨터의 RAM 이 8GB 미만인 경우 8GB 이상으로 RAM 을 늘리는 것이 좋습니다.

4. XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

XenMobile 10.14.x 또는 10.13.x에서 직접 XenMobile 10.15로 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 이진 파일을 다운로드합니다. <https://www.citrix.com/downloads>로 이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server > 제품 소프트웨어 > XenMobile Server 10**으로 이동합니다. 해당하는 하이퍼바이저에 대한 XenMobile Server 소프트웨어 타일에서 파일 다운로드를 클릭합니다. 업그레이드를 업로드하려면 XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다.

릴리스 관리 페이지를 사용하여 업그레이드하려면

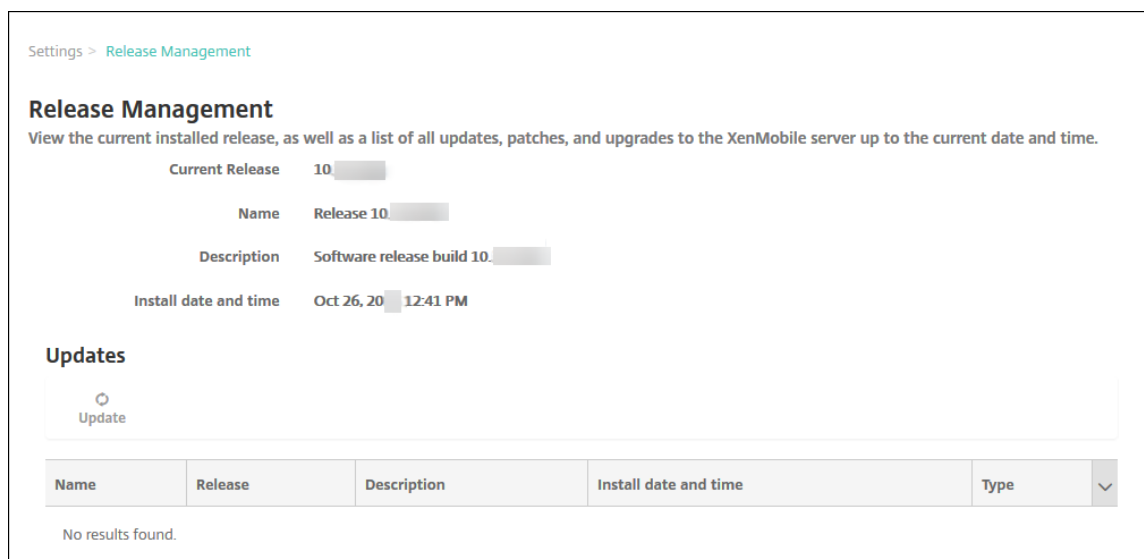
릴리스 관리 페이지를 사용하여 최신 버전의 XenMobile Server로 업그레이드합니다.

필수 구성 요소:

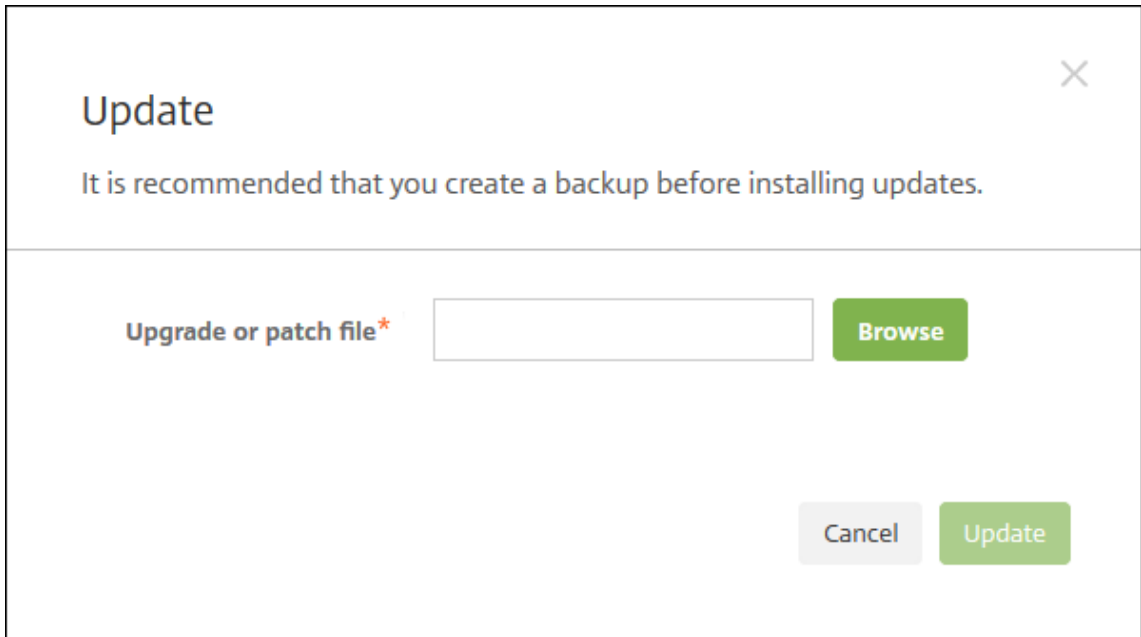
- [시스템 요구 사항](#)을 검토합니다.

클러스터링된 배포의 경우 이 문서의 끝 부분에 나오는 지침을 참조하십시오.

1. 최신 이진 파일을 다운로드합니다. <https://www.citrix.com/downloads>로 이동하십시오. **Citrix Endpoint Management(및 Citrix XenMobile Server) > XenMobile Server(온-프레미스) > 제품 소프트웨어 > XenMobile Server 10**으로 이동합니다. 해당하는 하이퍼바이저에 대한 XenMobile Server 소프트웨어 타일에서 파일 다운로드를 클릭합니다.
2. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
3. 릴리스 관리를 클릭합니다. 릴리스 관리 페이지가 나타납니다.



4. 업데이트 아래에서 업데이트를 클릭합니다. 업데이트 대화 상자가 나타납니다.



5. 찾아보기를 클릭하고 파일 위치로 이동하여 Citrix.com 에서 다운로드한 XenMobile 업그레이드 파일을 선택합니다.
6. 업데이트를 클릭한 후 메시지가 표시되면 XenMobile 을 다시 시작합니다.

몇 가지 이유로 업데이트를 성공적으로 완료할 수 없는 경우 문제를 나타내는 오류 메시지가 표시됩니다. 그런 다음 업데이트 시도 이전의 상태로 시스템이 되돌려집니다.

업그레이드 후

업그레이드한 후 XenMobile 을 다시 시작해야 합니다. XenMobile CLI 를 사용하여 XenMobile Server 를 다시 시작합니다. 시스템을 다시 시작한 후에는 브라우저 캐시를 지워야 합니다.

연결 구성을 변경하지 않았는데도 발신 연결이 관련된 기능이 작동을 중지하는 경우 **XenMobile Server** 로그 에 다음과 같은 오류가 있는지 확인하십시오. “VPP Server 에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’ 이 피어가 제공한 인증서 제목 과 일치하지 않습니다.”

이 인증서 유효성 검사 오류는 XenMobile Server 에서 호스트 이름 유효성 검사를 비활성화해야 함을 나타냅니다. 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외한 발신 연결에 대해 활성화됩니다. 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 **disable.hostname.verification** 을 **true** 로 변경하십시오. 이 속성의 기본값은 **false** 입니다.

Citrix 는 XenMobile 의 최신 버전 또는 중요 업데이트를 Citrix.com 에 게시합니다. 또한 각 고객의 기록된 연락처로 알림을 전송합니다.

클러스터된 **XenMobile** 배포를 업그레이드하려면

중요:

XenMobile 업데이트를 설치하기 전에 VM(가상 컴퓨터)의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

시스템이 클러스터 모드로 구성된 경우 다음 단계에 따라 XenMobile 10 릴리스의 각 노드를 업데이트합니다.

1. 설정 > 릴리스 관리에서 모든 노드에 .bin 파일을 업로드합니다.
2. CLI의 시스템 메뉴에서 모든 노드를 종료합니다.
3. CLI의 시스템 메뉴에서 노드 하나를 시작하고 서비스가 실행되는지 확인합니다.
4. 다른 노드를 하나씩 시작합니다.

XenMobile에서 업데이트를 성공적으로 완료할 수 없는 경우 문제를 나타내는 오류 메시지가 표시됩니다. 그런 다음 XenMobile이 업데이트 시도 이전의 상태로 시스템을 되돌립니다.

XenMobile MDM Edition에서 Enterprise Edition으로 업그레이드

XenMobile MDM Edition을 iOS 및 Android 장치용 XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드)로 업그레이드할 수 있습니다.

사전 요구 사항

- 올바른 Enterprise 라이선스.
- Citrix Gateway가 구성되어 있습니다.

업그레이드하려면

1. 설정 > 라이선스로 이동하고 올바른 Enterprise Edition 라이선스 유형이 업로드되었는지 확인합니다.
2. 설정 > 서버 속성으로 이동하고 서버 모드 속성을 **MDM**에서 **ENT**로 변경합니다.
3. 설정 > **Citrix Gateway**로 이동하고 Citrix Gateway 세부 정보를 구성합니다. 인증 모드를 MDM Edition과 동일한 모드, 즉 도메인 인증 (Active Directory)으로 설정합니다. XenMobile은 사용자 등록 후의 인증 모드 변경을 지원하지 않습니다.
4. 선택 사항: 설정 > 클라이언트 속성으로 이동하고 Citrix PIN 인증을 사용하도록 설정합니다.

이 단계를 완료한 후에는 사용자가 다음 단계를 수행하여 장치를 엔터프라이즈 모드로 전환해야 합니다.

iOS 사용자

1. Secure Hub 닫기: 장치 홈 단추를 빠르게 두 번 누르고 Secure Hub 앱을 위로 밀니다.
2. Secure Hub를 엽니다.

Android 사용자

1. Secure Hub 를 엽니다.
2. 기본 설정 > 장치 정보로 이동합니다.
3. 정책 새로 고침을 클릭합니다.

Citrix PIN 인증을 사용하도록 설정한 경우 Secure Hub 가 PIN 을 만들라는 메시지를 사용자에게 표시합니다. 사용자가 PIN 을 생성하면 XenMobile 이 장치를 엔터프라이즈 모드로 구성합니다. 그러면 XenMobile 콘솔의 관리 > 장치 페이지에 MDM 과 MAM 이 장치의 활성 모드로 표시됩니다.

사용자 계정, 역할 및 등록

September 29, 2021

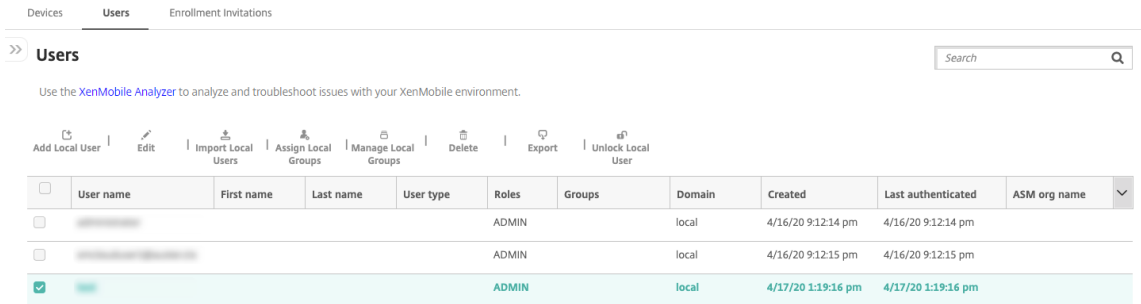
XenMobile 콘솔의 관리 탭 및 설정 페이지에서 사용자 계정, 역할 및 등록을 구성합니다. 별도로 지정되지 않는 한, 다음 작업에 대한 단계는 이 문서에서 제공됩니다.

- 사용자 계정 및 그룹:
 - 관리 > 사용자에서 수동으로 사용자 계정을 추가하거나.csv 프로비저닝 파일을 사용하여 계정을 가져오고 로컬 그룹을 관리합니다.
 - 설정 > 워크플로에서 워크플로를 사용하여 사용자 계정의 생성 및 제거를 관리합니다.
- 사용자 계정 및 그룹의 역할
 - 설정 > 역할 기반 액세스 제어에서 미리 정의된 역할 또는 권한 집합을 사용자 및 그룹에 할당합니다. 이러한 권한은 시스템 기능에 대한 사용자 액세스 수준을 제어합니다. 자세한 내용은 [RBAC 를 사용하여 역할 구성](#)을 참조하십시오.
 - 설정 > 알림 템플릿에서 자동화 동작, 등록 및 사용자에게 보내는 표준 알림 메시지에 사용할 알림 템플릿을 만들거나 업데이트합니다. 세 가지 채널 (Secure Hub, SMTP 또는 SMS) 을 통해 메시지를 보내는 알림 템플릿을 구성합니다. 자세한 내용은 [알림 템플릿 만들기 및 업데이트](#)를 참조하십시오.
- 등록 보안 모드 및 초대
 - 설정 > 등록에서 최대 7 개 등록 보안 모드를 구성하고 등록 초대를 보냅니다. 각 등록 보안 모드별로 사용자가 장치를 등록할 때 수행해야 하는 보안 수준과 단계가 다릅니다.
 - [XenMobile 에서 사용자 등록에 AutoDiscovery 사용](#)

로컬 사용자 계정을 추가, 편집, 잠금 해제 또는 삭제하려면

로컬 사용자 계정을 XenMobile 에 수동으로 추가하거나 프로비저닝 파일을 사용하여 계정을 가져올 수 있습니다. 프로비저닝 파일에서 사용자 계정을 가져오는 단계는 사용자 계정 가져오기를 참조하십시오.

1. XenMobile 콘솔에서 관리 > 사용자를 클릭합니다. 사용자 페이지가 나타납니다.



2. 필터 표시를 클릭하여 목록을 필터링합니다.

로컬 사용자 계정을 추가하려면

1. 사용자 페이지에서 로컬 사용자 추가를 클릭합니다. 로컬 사용자 추가 페이지가 나타납니다.

2. 다음 설정을 구성합니다.

- 사용자 이름: 이름을 입력합니다. 필수 필드입니다. 이름에 공백과 대/소문자를 포함할 수 있습니다.
- 암호: 선택적 사용자 암호를 입력합니다. 암호는 14 자 이상이어야 하며 다음 기준을 모두 충족해야 합니다.
 - 숫자 2 개 이상 포함
 - 대문자와 소문자 각각 1 개 이상 포함
 - 특수 문자 1 개 이상 포함
 - 사전에 등재된 단어, Citrix 사용자 이름 또는 전자 메일 주소와 같이 제한된 단어를 포함하지 마십시오.
 - 1111, 1234, asdf 와 같이 3 개 이상 이어지거나 반복되는 문자 또는 키보드 패턴을 포함하지 마십시오.

- **역할:** 목록에서 사용자 역할을 클릭합니다. 역할에 대한 자세한 내용은 [RBAC 를 사용하여 역할 구성](#)을 참조하십시오. 사용 가능한 옵션은 다음과 같습니다.
 - ADMIN
 - DEVICE_PROVISIONING
 - SUPPORT
 - USER
- **구성원 자격:** 목록에서 사용자를 추가할 그룹을 클릭합니다.
- **사용자 속성:** 선택적 사용자 속성을 추가합니다. 추가할 각 사용자 속성에 대해 추가를 클릭하고 다음을 수행합니다.
 - 사용자 속성: 목록에서 속성을 클릭하고 속성 옆의 필드에 사용자 속성 특성을 입력합니다.
 - 완료를 클릭하여 사용자 속성을 저장하거나 취소를 클릭합니다.

기존 사용자 속성을 삭제하려면 속성이 포함된 줄 위로 마우스 포인터를 이동하고 오른쪽의 X 아이콘을 클릭합니다. 속성이 즉시 삭제됩니다.

기존 사용자 속성을 편집하려면 속성을 클릭하고 변경합니다. 완료를 클릭하여 변경된 목록을 저장하거나 취소를 클릭하여 목록을 변경되지 않은 상태로 유지합니다.

3. 저장을 클릭합니다.

로컬 사용자 계정을 편집하려면

1. 사용자 페이지의 사용자 목록에서 사용자를 선택한 후 편집을 클릭합니다. 로컬 사용자 편집 페이지가 나타납니다.

Edit Local User

User name*

Password

Role*

ADMIN

Membership

☐ local\Device Enrollment Program Group
 ☐ local\MSP

Manage Groups

- User Properties

Add

2. 다음 정보를 적절하게 변경합니다.

- 사용자 이름: 사용자 이름은 변경할 수 없습니다.
- 암호: 사용자 암호를 변경하거나 추가합니다.
- 역할: 목록에서 사용자 역할을 클릭합니다.
- 구성원 자격: 목록에서 사용자 계정을 추가하거나 편집할 그룹을 클릭합니다. 그룹에서 사용자 계정을 제거하려면 그룹 이름 옆의 확인란을 선택 취소합니다.
- 사용자 속성: 다음 중 하나를 수행합니다.
 - 변경하려는 각 사용자 속성에 대해 속성을 클릭하고 변경합니다. 완료 버튼을 클릭하여 변경된 목록을 저장하거나 취소를 클릭하여 목록을 변경되지 않은 상태로 유지합니다.
 - 추가할 각 사용자 속성에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 사용자 속성: 목록에서 속성을 클릭하고 속성 옆의 필드에 사용자 속성 특성을 입력합니다.
 - ★ 완료를 클릭하여 사용자 속성을 저장하거나 취소를 클릭합니다.
 - 삭제할 각 기존 사용자 속성에 대해 속성이 포함된 줄 위로 마우스 포인터를 이동하고 오른쪽의 **X** 아이콘을 클릭합니다. 속성이 즉시 삭제됩니다.

3. 저장을 클릭하여 변경 내용을 저장하거나 취소를 클릭하여 사용자를 변경되지 않은 상태로 유지합니다.

로컬 사용자 계정을 잠금 해제하려면

1. 사용자 페이지의 사용자 목록에서 사용자 계정을 클릭하여 선택합니다.
2. 로컬 사용자 잠금 해제를 클릭합니다. 확인 대화 상자가 나타납니다.
3. 잠금 해제를 클릭하여 사용자 계정을 잠금 해제하거나 취소를 클릭하여 사용자를 변경하지 않은 상태로 둡니다.

로컬 사용자 계정을 삭제하려면

1. 사용자 페이지의 사용자 목록에서 사용자 계정을 클릭하여 선택합니다.

각 사용자 계정 옆의 확인란을 선택하여 둘 이상의 사용자 계정을 선택하고 삭제할 수 있습니다.

1. 삭제를 클릭합니다. 확인 대화 상자가 나타납니다.
2. 삭제를 클릭하여 사용자 계정을 삭제하거나 취소를 클릭합니다.

Active Directory 사용자 삭제

한 번에 한 명 이상의 Active Directory 사용자를 삭제하려면 사용자를 선택하고 삭제를 클릭합니다.

장치가 등록되어 있는 사용자를 삭제한 후 해당 장치를 재등록하려면 재등록하기 전에 해당 장치를 삭제하십시오. 장치를 삭제하려면 관리 > 장치에서 장치를 선택한 다음 삭제를 클릭합니다.

사용자 계정 가져오기

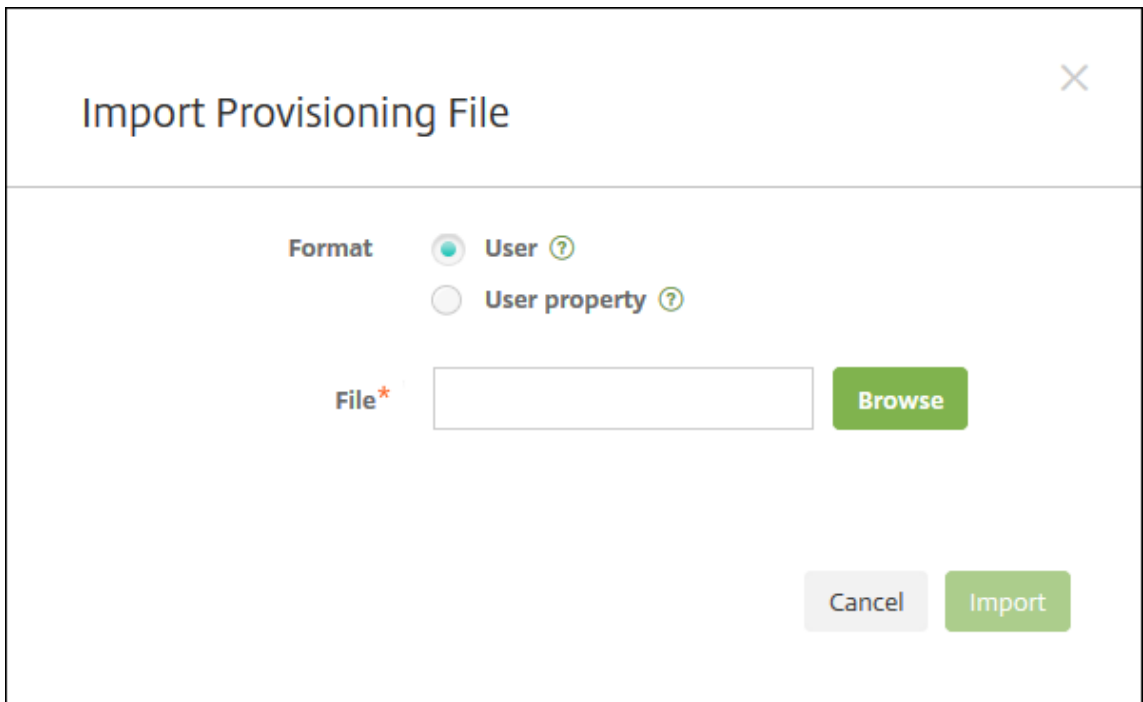
프로비저닝 파일이라고 하는.csv 파일을 수동으로 만들어 로컬 사용자 계정 및 속성을 가져올 수 있습니다. 프로비저닝 파일 형식에 대한 자세한 내용은 프로비저닝 파일 형식을 참조하십시오.

참고:

- 로컬 사용자의 경우 가져오기 파일에 사용자 이름과 함께 도메인 이름을 사용합니다. 예를 들어 `username@domain` 을 지정합니다. 만들거나 가져오는 로컬 사용자가 XenMobile 에서 관리되는 도메인에 대한 사용자인 경우 해당 사용자는 해당하는 LDAP 자격 증명을 사용하여 등록할 수 없습니다.
- XenMobile 내부 사용자 디렉터리로 사용자 계정을 가져오는 경우 기본 도메인을 사용하지 않으면 가져오기 프로세스 속도가 빨라집니다. 도메인을 사용하지 않도록 설정하면 등록에 영향을 미치므로 내부 사용자 가져오기가 완료된 후 기본 도메인을 다시 사용하도록 설정합니다.
- 로컬 사용자는 UPN(사용자 계정 이름) 형식을 사용할 수 있습니다. 그러나 관리되는 도메인은 사용하지 않는 것이 좋습니다. 예를 들어 `example.com` 이 관리되는 경우 이 UPN 형식 (`user@example.com`) 으로 로컬 사용자를 만들지 마십시오.

프로비저닝 파일을 준비한 후 다음 단계에 따라 XenMobile 로 파일을 가져옵니다.

1. XenMobile 콘솔에서 관리 > 사용자를 클릭합니다. 사용자 페이지가 나타납니다.
2. 로컬 사용자 가져오기를 클릭합니다. 프로비저닝 파일 가져오기 대화 상자가 나타납니다.

A screenshot of the 'Import Provisioning File' dialog box. The dialog has a title bar with a close button (X). Below the title, there is a 'Format' section with two radio buttons: 'User' (selected) and 'User property'. Below this is a 'File*' label next to a text input field, with a green 'Browse' button to its right. At the bottom right, there are two buttons: 'Cancel' and 'Import'.

3. 가져오는 프로비저닝 파일의 형식으로 사용자 또는 속성을 선택합니다.
4. 찾아보기를 클릭하고 파일 위치로 이동하여 사용할 프로비저닝 파일을 선택합니다.
5. 가져오기를 클릭합니다.

프로비저닝 파일 형식

프로비저닝 파일을 수동으로 만들어서 사용자 계정과 속성을 XenMobile 로 가져올 수 있습니다. 유효한 형식은 다음과 같습니다.

- 사용자 프로비저닝 파일 필드: `user;password;role;group1;group2`
- 사용자 특성 프로비저닝 파일 필드: `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

참고:

- 프로비저닝 파일 내의 필드는 세미콜론 (;) 으로 구분합니다. 필드 자체에 세미콜론이 포함되는 경우 백슬래시 문자 (\) 로 이스케이프 처리합니다. 예를 들어 `propertyV;test;1;2` 속성을 프로비저닝 파일에 `propertyV\\;test\\;1\\;2`로 입력합니다.
- 역할의 유효한 값은 미리 정의된 USER, ADMIN, SUPPORT 및 DEVICE_PROVISIONING 과 정의된 다른 역할입니다.
- 그룹 계층을 만들 때는 마침표 문자 (.) 를 구분 기호로 사용합니다. 그룹 이름에는 마침표를 사용하지 마십시오.
- 특성 프로비저닝 파일의 속성 특성에는 소문자를 사용합니다. 데이터베이스는 대/소문자를 구분합니다.

사용자 프로비저닝 콘텐츠의 예 `user01;pwd\\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` 항목은 다음을 의미합니다.

- 사용자: `user01`
- 암호: `pwd;01`
- 역할: `USER`
- 그룹:
 - `myGroup.users01`
 - `myGroup.users02`
 - `myGroup.users.users.users01`

또 다른 예로 `AUser0;1.password;USER;ActiveDirectory.test.net`은 다음을 의미합니다.

- 사용자: `AUser0`
- 암호: `1.password`
- 역할: `USER`
- 그룹: `ActiveDirectory.test.net`

사용자 특성 프로비저닝 콘텐츠의 예 `user01;propertyN;propertyV\\;test\\;1\\;2;prop 2;prop2 value` 항목은 다음을 의미합니다.

- 사용자: `user01`
- 속성 **1**

- 이름: `propertyN`
- 값: `propertyV;test;1;2`
- 속성 2:
 - 이름: `prop 2`
 - 값: `prop2 value`

등록 보안 모드 구성

XenMobile 에서 장치 등록 보안 모드를 구성하여 장치 등록을 위한 보안 수준과 알림 템플릿을 지정합니다.

XenMobile 은 사용자가 장치를 등록할 때 수행해야 하는 보안 수준과 단계가 다른 7 가지 등록 보안 모드를 제공합니다. XenMobile Server 콘솔의 설정 > 등록 페이지에서 등록 보안 모드를 구성할 수 있습니다.

일부 모드는 자가 지원 포털에서 사용할 수 있도록 제공할 수 있습니다. 사용자는 포털에서 장치를 등록하는 데 사용하는 등록 링크를 생성합니다. iOS, iPadOS, macOS, Android Enterprise 및 레거시 Android 사용자는 포털에서 본인에게 등록 초대 보내도록 선택할 수 있습니다. Windows 장치에서는 등록 초대를 사용할 수 없습니다.

등록 초대는 관리 > 등록 초대 페이지에서 보낼 수 있습니다. 자세한 내용은 [등록 초대 보내기](#)를 참조하십시오.

참고:

사용자 지정 알림 템플릿을 사용하려는 경우 등록 모드를 구성하기 전에 템플릿을 설정해야 합니다. 알림 템플릿에 대한 자세한 내용은 [알림 템플릿 만들기 또는 업데이트](#)를 참조하십시오.

1. XenMobile 콘솔에서 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 등록을 클릭합니다. 사용 가능한 모든 등록 보안 모드 테이블이 포함된 등록 페이지가 나타납니다. 기본적으로 모든 등록 보안 모드가 사용됩니다.
3. 목록에서 등록 보안 모드를 선택하여 편집합니다. 그런 다음 모드를 기본값으로 설정하거나 모드를 사용하지 않도록 설정하거나 자가 지원 포털을 통한 사용자 액세스를 허용합니다.

참고:

등록 보안 모드 옆의 확인란을 선택하면 등록 보안 모드 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하면 목록의 오른쪽에 옵션 메뉴가 나타납니다.

Settings > Enrollment

Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Worx Home and enroll their devices, or to send themselves an enrollment invitation.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates	▼
<input type="checkbox"/>	User name + Password	✓	✓							
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL	✓			1 day(s)					
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3				
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric		

Showing 1 - 7 of 7 items

다음 등록 보안 모드 중에서 선택합니다.

- 사용자 이름 + 암호
- 높은 수준의 보안
- 초대 URL
- 초대 URL + PIN
- 초대 URL + 암호
- 2 단계 인증
- 사용자 이름 + PIN

등록 초대를 사용하여 초대를 받은 사용자로 등록을 제한할 수 있습니다. 등록 초대를 보내기 위해서는 초대 **URL**, 초대 **URL + PIN** 또는 초대 **URL + 암호** 등록 보안 모드만 사용할 수 있습니다. 사용자 이름 + 암호, **2** 단계 인증 또는 사용자 이름 + PIN 으로 등록하는 장치의 경우 사용자는 Secure Hub 에서 자격 증명을 수동으로 입력해야 합니다.

OTP(일회용 PIN) 등록 초대를 2 단계 인증 솔루션으로 사용할 수 있습니다. OTP 등록 초대는 사용자가 등록할 수 있는 장치의 수를 제어합니다. Windows 장치에서는 OTP 초대를 사용할 수 없습니다.

등록 보안 모드를 편집하려면

1. 등록 목록에서 등록 보안 모드를 선택한 후 편집을 클릭합니다. 등록 모드 편집 페이지가 나타납니다. 선택한 모드에 따라 표시되는 옵션이 결정됩니다.

Settings > Enrollment > Edit Enrollment Mode

Edit Enrollment Mode

Name High Security

Expire after* **Days** ⓘ

Maximum attempts* ⓘ

PIN Length* **Numeric** ▾

Notification templates

Template for enrollment URL -- SELECT ONE -- ▾

Template for Enrollment PIN -- SELECT ONE -- ▾

Template for enrollment confirmation -- SELECT ONE -- ▾

Cancel **Save**

2. 다음 정보를 적절하게 변경합니다.

- 다음 이후에 만료: 사용자가 장치를 등록할 수 없는 만료 기한을 입력합니다. 이 값은 사용자 및 그룹 등록 초대 구성 페이지에 나타납니다.

초대가 만료되지 않도록 하려면 **0** 을 입력하십시오.

- 일: 목록에서 다음 이후에 만료에 입력한 만료 기한에 해당하는 일 또는 시간을 클릭합니다.
 - 최대 시도 횟수: 등록 프로세스가 잠기기 전까지 사용자가 등록을 시도할 수 있는 횟수를 입력합니다. 이 값은 사용자 및 그룹 등록 초대 구성 페이지에 나타납니다.
- 시도 횟수를 제한하지 않으려면 **0** 을 입력하십시오.

- **PIN 길이:** 생성된 PIN 의 길이를 설정할 숫자를 입력합니다.
- **숫자:** 목록에서 숫자 또는 영숫자를 PIN 유형으로 클릭합니다.
- **알림 템플릿:**
 - 등록 **URL** 용 템플릿: 목록에서 등록 URL 에 사용할 템플릿을 클릭합니다. 예를 들어 등록 초대 템플릿은 사용자에게 전자 메일 또는 SMS 를 보냅니다. 방법은 사용자가 XenMobile 에 장치를 등록할 때 사용할 수 있는 템플릿의 구성 방법에 따라 다릅니다. 알림 템플릿에 대한 자세한 내용은 [알림 템플릿 만들기 또는 업데이트](#)를 참조하십시오.
 - 등록 **PIN** 용 템플릿: 목록에서 등록 PIN 에 사용할 템플릿을 클릭합니다.
 - 등록 확인용 템플릿: 목록에서 사용자가 성공적으로 등록되었음을 알릴 때 사용할 템플릿을 클릭합니다.

3. 저장을 클릭합니다.

등록 보안 모드를 기본값으로 설정하려면

등록 보안 모드를 기본값으로 설정하면 다른 등록 보안 모드를 선택하지 않는 한 모든 장치 등록 요청에 해당 모드가 사용됩니다. 기본값으로 설정된 등록 보안 모드가 없는 경우 장치를 등록할 때마다 등록 요청을 만들어야 합니다.

참고:

사용자 이름 + 암호, **2** 단계 또는 사용자 이름 + **PIN** 등록 보안 모드만 기본값으로 사용할 수 있습니다.

1. 사용자 이름 + 암호, **2** 단계 또는 사용자 이름 + **PIN** 중에서 기본 등록 보안 모드를 선택합니다.

모드를 기본값으로 사용하려면 먼저 사용하도록 설정해야 합니다.

2. 기본값을 클릭합니다. 이제 선택한 모드가 기본값입니다. 이전에 기본값으로 설정된 다른 등록 보안 모드는 더 이상 기본값이 아닙니다.

등록 보안 모드를 사용하지 않도록 설정하려면

등록 보안 모드를 사용하지 않도록 설정하면 그룹 등록 초대와 자가 지원 포털에서 등록 모드를 사용할 수 없게 됩니다. 한 등록 보안 모드를 사용하지 않도록 설정하고 다른 등록 보안 모드를 사용하도록 설정하여 사용자가 장치를 등록하는 방법을 변경할 수 있습니다.

1. 등록 보안 모드를 선택합니다.

기본 등록 보안 모드는 사용하지 않도록 설정할 수 없습니다. 기본 등록 보안 모드를 사용하지 않도록 설정하려면 먼저 기본값 상태를 제거해야 합니다.

2. **Disable** 을 클릭합니다. 등록 보안 모드가 더 이상 사용되지 않습니다.

자가 지원 포털에서 등록 보안 모드를 사용하도록 설정하려면

자가 지원 포털에서 등록 보안 모드를 사용하도록 설정하면 사용자가 개별적으로 XenMobile 에 장치를 등록할 수 있습니다.

참고:

- 등록 보안 모드를 자가 지원 포털에서 사용할 수 있으려면 등록 모드를 사용하도록 설정하고 알림 템플릿에 연결해야 합니다.
- 자가 지원 포털에는 한 번에 하나의 등록 보안 모드만 사용하도록 설정할 수 있습니다.

1. 등록 보안 모드를 선택합니다.

2. 자가 지원 포털을 클릭합니다. 이제 사용자가 자가 지원 포털에서 선택한 등록 보안 모드를 사용할 수 있습니다. 자가 지원 포털에 사용하도록 설정된 다른 모드는 더 이상 사용자에게 제공되지 않습니다.

그룹 추가 또는 제거

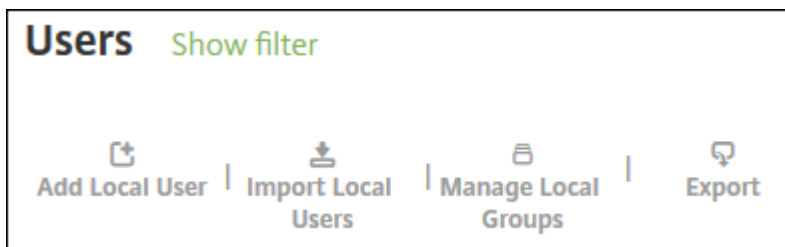
XenMobile 콘솔에서 사용자, 로컬 사용자 추가, 로컬 사용자 편집 페이지의 그룹 관리 대화 상자에서 그룹을 관리할 수 있습니다. 그룹 편집 명령은 없습니다.

그룹을 제거하는 경우 그룹 제거가 사용자 계정에 영향을 주지 않는다는 점을 기억하십시오. 그룹을 제거하면 해당 그룹에 대한 사용자 연결만 제거됩니다. 또한 사용자가 해당 그룹에 연결된 배달 그룹에서 제공하는 앱 또는 프로필에 액세스할 수 없게 됩니다. 그러나 다른 모든 그룹 연결은 그대로 유지됩니다. 다른 로컬 그룹에 연결되지 않은 사용자는 상위 수준에 연결됩니다.

로컬 그룹을 추가하려면

1. 다음 중 하나를 수행합니다.

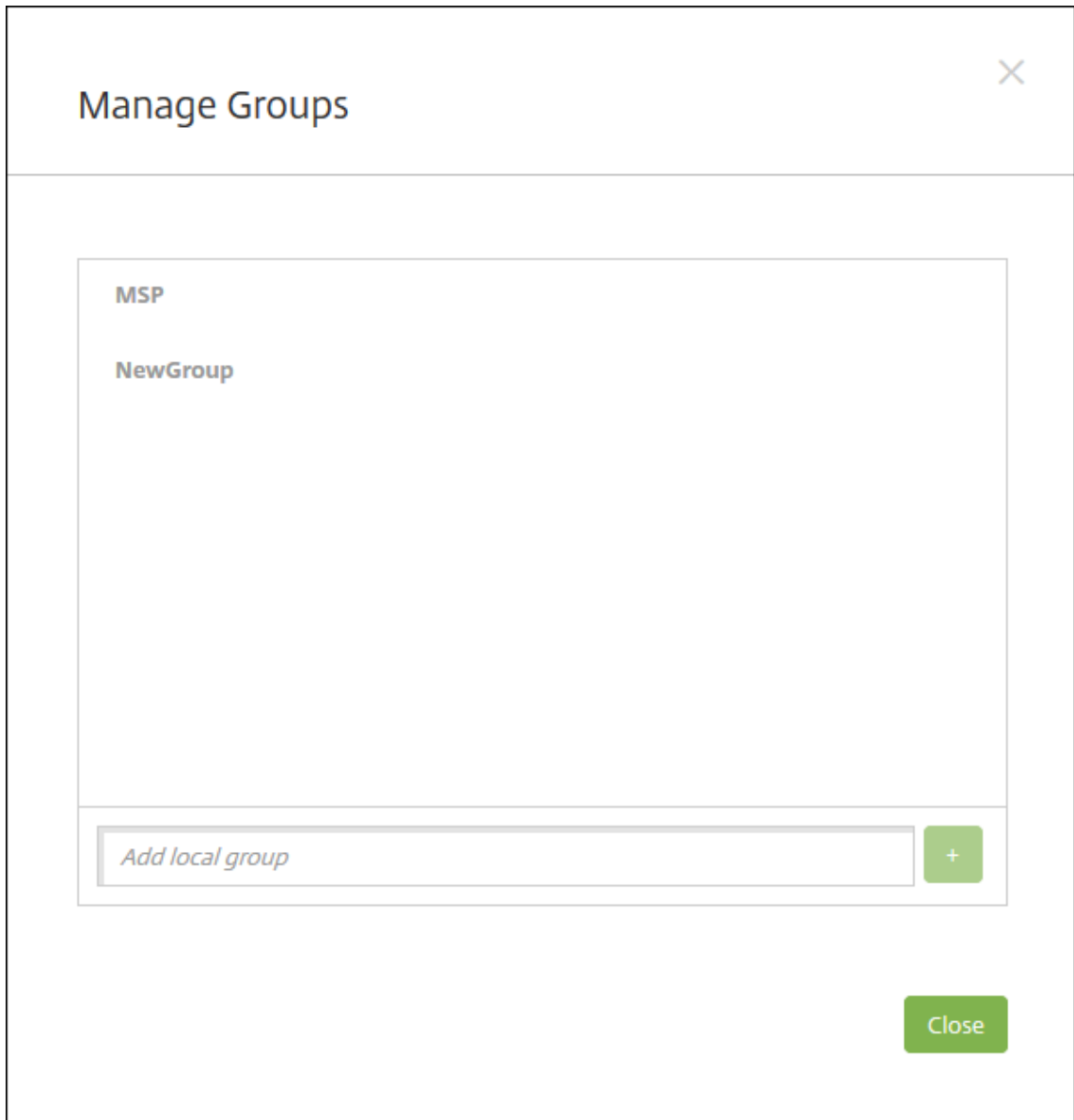
- 사용자 페이지에서 로컬 그룹 관리를 클릭합니다.



- 로컬 사용자 추가 페이지 또는 로컬 사용자 편집 페이지에서 그룹 관리를 클릭합니다.

 A screenshot of the 'Add Local User' or 'Edit Local User' form. It contains several input fields: 'User name*' with the value 'User01', 'Password' with the placeholder 'Enter new password', and 'Role*' with a dropdown menu showing 'SUPPORT'. Below these is the 'Membership' section, which shows a list of groups with a checkbox next to 'local\MSP' that is currently checked. To the right of the membership list is a blue button labeled 'Manage Groups'.

그룹 관리 대화 상자가 나타납니다.



2. 그룹 목록 아래에 새 그룹 이름을 입력한 후 더하기 기호 (+) 를 클릭합니다. 사용자 그룹이 목록에 추가됩니다.
3. **Close**(닫기) 를 클릭합니다.

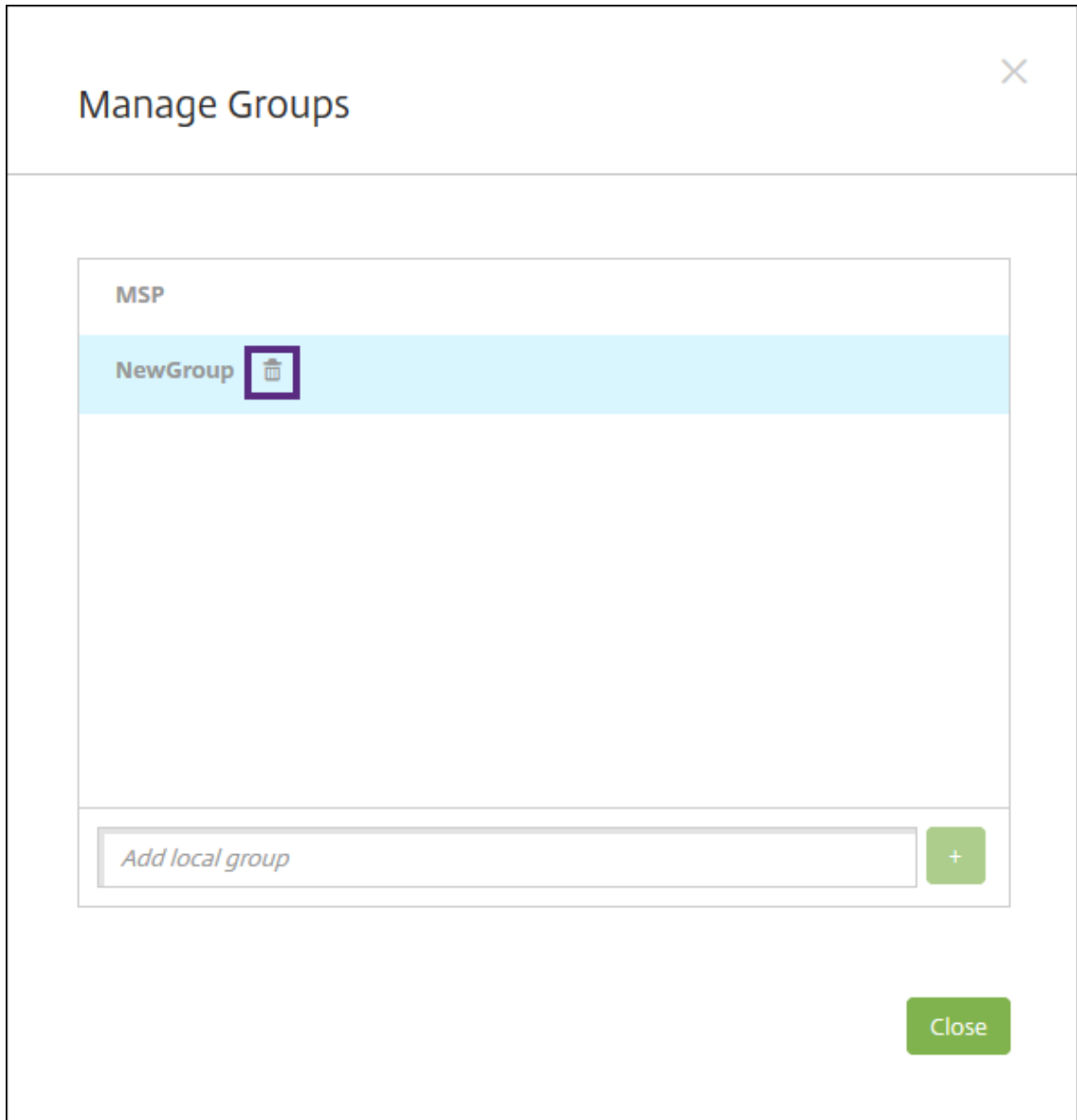
그룹을 제거하려면

그룹을 제거해도 사용자 계정에는 영향을 주지 않습니다. 그룹을 제거하면 해당 그룹에 대한 사용자 연결만 제거됩니다. 또한 사용자가 해당 그룹에 연결된 배달 그룹에서 제공하는 앱 또는 프로필에 액세스할 수 없게 됩니다. 그러나 다른 모든 그룹 연결은 그대로 유지됩니다. 다른 로컬 그룹에 연결되지 않은 사용자는 상위 수준에 연결됩니다.

1. 다음 중 하나를 수행합니다.
 - 사용자 페이지에서 로컬 그룹 관리를 클릭합니다.

- 로컬 사용자 추가 페이지 또는 로컬 사용자 편집 페이지에서 그룹 관리를 클릭합니다.

그룹 관리 대화 상자가 나타납니다.



2. 그룹 관리 대화 상자에서 삭제할 그룹을 클릭합니다.
3. 그룹 이름 오른쪽의 휴지통 아이콘을 클릭합니다. 확인 대화 상자가 나타납니다.
4. 삭제를 클릭하여 작업을 확인하고 그룹을 제거합니다.

중요:

이 작업은 실행 취소할 수 없습니다.

5. 그룹 관리 대화 상자에서 닫기를 클릭합니다.

워크플로 만들기 및 관리

워크플로를 사용하여 사용자 계정의 생성 및 제거를 관리할 수 있습니다. 워크플로를 사용하려면 먼저 조직에서 사용자 계정 요청을 승인할 권한이 있는 담당자를 식별합니다. 그런 다음 워크플로 템플릿을 사용하여 사용자 계정 요청을 만들고 승인할 수 있습니다.

XenMobile 을 처음으로 설정하는 경우 워크플로를 사용하기 전에 먼저 워크플로 전자 메일 설정을 구성해야 합니다. 워크플로 전자 메일 설정은 언제든지 변경할 수 있습니다. 이러한 설정에는 전자 메일 서버, 포트, 전자 메일 주소 및 사용자 계정 생성 요청에 승인이 필요한지 여부가 포함됩니다.

XenMobile 의 두 위치에서 워크플로를 구성할 수 있습니다.

- XenMobile 콘솔의 워크플로 페이지와 워크플로 페이지에서 앱 구성에 사용할 여러 워크플로를 구성할 수 있습니다. 워크플로 페이지에서 워크플로를 구성하는 경우 앱을 구성할 때 워크플로를 선택할 수 있습니다.
- 앱의 응용 프로그램 커넥터를 구성할 때 워크플로 이름을 입력한 다음 사용자 계정 요청을 승인할 수 있는 사용자를 구성합니다. [XenMobile 에 앱 추가](#)를 참조하십시오.

사용자 계정에 대한 관리자 승인을 최대 3 개 수준까지 할당할 수 있습니다. 사용자 계정을 승인할 다른 사용자가 필요한 경우 해당 사용자의 이름 또는 전자 메일 주소를 사용하여 검색하고 선택할 수 있습니다. XenMobile 에서 해당 사용자가 검색되면 워크플로에 추가하면 됩니다. 새 사용자 계정에 대한 승인 또는 거부를 위한 전자 메일이 워크플로의 모든 사용자에게 전송됩니다.


1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 워크플로를 클릭합니다. 워크플로 페이지가 나타납니다.
3. 추가를 클릭합니다. 워크플로 추가 페이지가 나타납니다.

Settings > Workflows > Add Workflow

Add Workflow


Name*

Description

Email Approval Templates Workflow Approval Request 

Levels of manager approval 1 level

Select Active Directory domain agsag.com

Find additional required approvers  Search

Selected additional required approvers

Cancel Save

4. 다음 설정을 구성합니다.

- **이름:** 워크플로의 고유한 이름을 입력합니다.
- **설명:** 필요한 경우 워크플로의 설명을 입력합니다.
- **전자 메일 승인 템플릿:** 목록에서 할당할 전자 메일 승인 템플릿을 선택합니다. XenMobile 콘솔의 설정 아래에 있는 알림 템플릿 섹션에서 전자 메일 템플릿을 만듭니다. 이 필드의 오른쪽에 있는 눈 아이콘을 클릭하면 구성 중인 템플릿의 미리 보기가 표시됩니다.
- **관리자 승인 수준:** 목록에서 이 워크플로에 필요한 관리자 승인 수준의 번호를 선택합니다. 기본값은 **1** 수준입니다. 사용 가능한 옵션은 다음과 같습니다.
 - 필요 없음
 - 1 수준
 - 2 수준
 - 3 수준
- **Active Directory 도메인 선택:** 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
- **추가로 필요한 승인자 찾기:** 검색 필드에 이름을 입력하고 검색을 클릭합니다. 이름은 Active Directory 에서 가져옵니다.

- 필드에 이름이 나타나면 해당하는 이름 옆의 확인란을 선택합니다. 이름과 전자 메일 주소가 추가로 필요한 승인자 선택됨 목록에 나타납니다.
 - 목록에서 이름을 제거하려면 다음 중 하나를 수행합니다.
 - ★ 검색을 클릭하여 선택한 도메인의 모든 사용자 목록을 표시합니다.
 - ★ 검색 결과를 제한하려면 검색 상자에 이름 전체 또는 일부를 입력한 다음 검색을 클릭합니다.
 - ★ 추가로 필요한 승인자 선택됨 목록에 있는 사용자는 검색 결과 목록에서 해당 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하고 제거할 각 이름 옆의 확인란을 선택 취소합니다.

5. 저장을 클릭합니다. 생성된 워크플로가 워크플로 페이지에 표시됩니다.

워크플로를 만든 후 워크플로 세부 정보를 보거나 워크플로에 연결된 앱을 보거나 워크플로를 삭제할 수 있습니다. 워크플로를 만든 후에는 워크플로를 편집할 수 없습니다. 승인 수준 또는 승인자가 다른 워크플로가 필요한 경우 다른 워크플로를 만듭니다.

세부 정보를 보고 워크플로를 삭제하려면

1. 워크플로 페이지의 기존 워크플로 목록에서 특정 워크플로를 선택합니다. 이렇게 하려면 테이블의 행을 클릭하거나 워크플로 옆의 확인란을 선택합니다.
2. 워크플로를 삭제하려면 삭제를 클릭합니다. 확인 대화 상자가 나타납니다. 삭제를 다시 클릭합니다.

중요:

이 작업은 실행 취소할 수 없습니다.

등록 프로필

January 5, 2022

등록 프로필은 다음을 지정합니다.

- Android 및 iOS 장치에 대한 장치 관리 등록 옵션. Android의 경우 MDM+MAM(ENT) 서버 모드에 제공되는 등록 옵션은 MDM 모드의 옵션과 다릅니다.
- Android 및 iOS 장치에 대한 앱 관리 등록 옵션.
- 기타 등록 옵션:
 - 사용자가 등록할 수 있는 장치 수를 제한할지 여부.
장치 제한에 도달하면 사용자에게 장치 등록 제한이 초과되었음을 설명하는 오류 메시지가 표시됩니다.
 - 사용자가 장치 관리를 거부할 수 있는지 여부.

등록 프로필을 사용하여 단일 XenMobile Server 콘솔 내에서 여러 사용 사례와 장치 마이그레이션 경로를 결합할 수 있습니다. 일부 사용 사례에는 다음이 포함됩니다.

- Mobile Device Management(MDM 전용)
- MDM+MAM(Mobile Application Management)
- MAM 전용
- 회사 소유 등록
- BYOD 등록 (MDM 등록 취소 기능)
- Android Enterprise 등록으로 Android 장치 관리자 등록 마이그레이션 (완전 관리됨, 작업 프로필, 전용 장치)

배달 그룹을 만들 때 Global 이라는 기본 등록 프로필을 사용하거나 다른 등록 프로필을 지정할 수 있습니다.

플랫폼별 등록 프로필 기능에는 다음이 포함됩니다.

- **Android 장치:** 장치 소유자 모드를 지정합니다. 완전히 관리, 작업 프로필로 완전히 관리, BYOD 업무 프로필을 예로 들 수 있습니다. 전용 장치 옵션은 XenMobile 용 엔터프라이즈 또는 고급 라이선스가 있는 경우에만 나타납니다. 기본적으로 Android Enterprise 및 앱 관리에서 새 장치를 등록합니다. 등록 보안 모드 사용자 이름 + PIN, 초대 URL, 초대 URL + PIN, 초대 URL + 암호는 Android Enterprise 에 사용할 수 없습니다.
- **iOS 장치:** 장치 등록 유형: 장치 등록을 지정하거나 장치를 관리하지 않습니다. iOS 설정은 XenMobile 엔터프라이즈 또는 고급 라이선스가 있는 경우에만 표시됩니다. 기본적으로 Apple 장치 관리 및 앱 관리에서 새 장치를 등록합니다.

Android 장치에 대한 전용 장치 등록이나 Android 또는 iOS 장치에 대한 MAM 전용 등록이 필요하지 않은 경우 [enable.multimode.xml](#) 서버 속성을 비활성화해도 됩니다. 그러나 이 속성을 계속 활성화해 두면 모든 유형의 등록 프로필을 처리하는 데 XenMobile Server 하나만 있으면 됩니다. [서버 속성](#)을 참조하십시오.

[enable.multimode.xml](#)를 비활성화할 경우 아래 스크린샷에 있는 설정만 사용할 수 있습니다.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ? Management <ul style="list-style-type: none"> <input checked="" type="radio"/> Android Enterprise ? <input type="radio"/> Legacy device administration (not recommended) ?
Android	Device owner mode <ul style="list-style-type: none"> <input checked="" type="radio"/> Company-owned device ? <input type="radio"/> Fully managed with work profile ?
3 Assignment (optional)	BYOD work profile <ul style="list-style-type: none"> <input checked="" type="checkbox"/> On ?

이러한 설정에 대한 자세한 내용은 [Android Enterprise](#)를 참조하십시오.

Global 등록 프로필

기본 등록 프로필의 이름은 Global 입니다. Global 프로필은 등록 프로필을 만들 기회가 생길 때까지 테스트하는 데 유용합니다.

다음 스크린샷은 Global 등록 프로필의 기본 설정을 보여줍니다.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

Enrollment Profile

1 Enrollment Info

2 Platforms

Android

iOS

3 Assignment (optional)

Enrollment Info

Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices.

Enrollment profile name *

Total number of devices a user can enroll

unlimited

Enrollment Profile

1 Enrollment Info

2 Platforms

Android

iOS

3 Assignment (optional)

Enrollment Configuration

Specify device management settings for this enrollment profile.

Device management ?

Management

☒ Android Enterprise ?

☐ Legacy device administration (not recommended) ?

☐ Do not manage devices ?

Device owner mode

☒ Company-owned device ?

☐ Fully managed with work profile ?

☐ Dedicated device ?

☐ None ?

BYOD work profile

☒ On ?

Application management ?

Citrix MAM

☒ On ?

User consent

Allow users to decline device management

☒ On ?

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	<p>Specify device management settings for this enrollment profile.</p> <p>Device management ?</p> <p>Management <input checked="" type="radio"/> Device enrollment ? <input type="radio"/> Do not manage devices ?</p> <p>Application management ?</p> <p>Citrix MAM <input checked="" type="checkbox"/> On ?</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> On ?</p>
2 Platforms	
Android	
iOS	
3 Assignment (optional)	

등록 프로필, 배달 그룹 및 등록

등록 프로필과 배달 그룹은 다음과 같이 상호 작용합니다.

- 하나 이상의 배달 그룹에 등록 프로필을 연결할 수 있습니다.
- 사용자가 등록 프로필이 다른 여러 배달 그룹에 속하는 경우 사용되는 등록 프로필은 배달 그룹의 이름에 따라 결정됩니다. XenMobile Server 는 사전순으로 표시된 배달 그룹 목록의 마지막에 나타나는 배달 그룹을 선택합니다. 예를 들어 다음과 같은 항목이 있다고 가정합니다.
 - “EP1” 과 “EP2” 라는 등록 프로필 2 개
 - “DG1” 과 “DG2” 라는 배달 그룹 2 개
 - “DG1” 은 “EP1” 에 연결되어 있습니다.
 - “DG2” 는 “EP2” 에 연결되어 있습니다.

등록 사용자가 “DG1” 및 “DG2” 배달 그룹에 모두 있는 경우 XenMobile Server 는 “EP2” 등록 프로필을 사용하여 사용자의 등록 유형을 결정합니다.

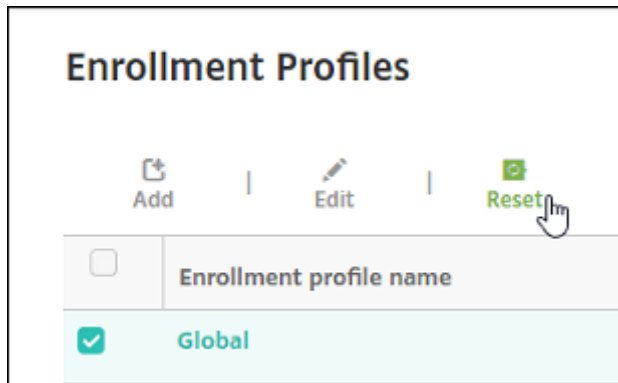
- 배포 순서는 MDM(장치 관리)에 대해 구성된 등록 프로필이 있는 배달 그룹의 장치에만 적용됩니다.
- 장치가 등록된 후 등록 프로필을 일부 변경하려면 다시 등록해야 합니다.
 - MDM에 대해 구성된 등록 프로필에 MAM 추가.
 - MDM에 등록된 장치를 MDM+MAM에 대해 구성된 배달 그룹으로 이동. 이러한 변경 사항은 새 장치 등록에만 영향을 미칩니다. 기존 장치 등록은 영향을 받지 않습니다.
 - MAM에 대해 구성된 등록 프로필에 MDM 추가.
- 다른 등록 프로필로 전환해도 기존의 등록된 장치에는 영향을 주지 않습니다. 그러나 변경 내용을 적용하려면 사용자가 해당 장치를 등록 취소했다가 다시 등록해야 합니다.

등록 프로필을 만들려면

1. XenMobile Server 콘솔에서 구성 > 등록 프로필로 이동합니다.
2. 등록 정보 페이지에서 프로필을 설명하는 이름을 입력합니다. 기본적으로 사용자는 무제한 장치를 등록할 수 있습니다. 사용자당 장치 수를 제한하는 값을 선택합니다. 이 제한은 사용자가 등록하는 MAM 또는 MDM 관리형 Android 및 iOS 장치의 합계에 적용됩니다.
3. 플랫폼 페이지를 작성합니다. 플랫폼별 등록 설정에 대한 정보는 다음에서 확인하십시오.
 - [Android Enterprise](#)
 - iOS: [지원되는 등록 방법](#)
4. 할당 페이지에서 하나 이상의 배달 그룹을 등록 프로필에 연결합니다.

사용자는 서로 다른 등록 프로필이 있는 여러 배달 그룹에 속할 수 있습니다. 이 경우 사용되는 등록 프로필은 배달 그룹의 이름에 따라 결정됩니다. XenMobile 은 사전순으로 표시된 배달 그룹 목록의 마지막에 나타나는 배달 그룹을 선택합니다. 배달 그룹을 만들려면 구성 > 배달 그룹으로 이동합니다.

등록 프로필 목록이 구성 > 등록 프로필 페이지에 나타납니다. Global 프로필을 편집하거나 원래 기본 설정으로 재설정하려면 Global 프로필의 열을 선택하고 재설정을 클릭합니다. Global 프로필은 삭제할 수 없습니다.



RBAC 를 사용하여 역할 구성

November 27, 2023

사전 정의된 각 RBAC(역할 기반 액세스 제어) 역할에는 특정 액세스 및 기능 권한이 연결되어 있습니다. 이 문서에서는 각 사용 권한이 수행하는 작업에 대해 설명합니다. 각 기본 제공 역할에 대한 기본 사용 권한의 전체 목록을 보려면 [Role-Based Access Control Defaults\(역할 기반 액세스 제어 기본값\)](#)를 다운로드하십시오.

사용 권한을 적용할 때 RBAC 역할에 관리 권한이 있는 사용자 그룹을 정의합니다. 기본 관리자는 적용된 사용 권한 설정을 변경할 수 없습니다. 기본적으로, 적용된 사용 권한은 모든 사용자 그룹에 적용됩니다.

할당을 수행할 때 RBAC 역할을 그룹에 할당하면 사용자 그룹이 RBAC 관리자 권한을 소유하게 됩니다.

중요:

설정 권한에서 RBAC 권한은 관리자 사용자에게 자신의 권한을 할당할 수 있는 기능을 포함하여 모든 권한을 부여합니다. Endpoint Management 시스템의 모든 항목을 조작할 수 있는 기능을 제공하려는 사용자에게만 이 액세스 권한을 부여하시기 바랍니다.

이 문서의 섹션은 다음과 같습니다.

- [관리 역할](#)
- [지원 역할](#)
- [사용자 역할](#)
- [RBAC 를 사용하여 역할 구성](#)

관리 역할

미리 정의된 관리자 역할을 가진 사용자는 XenMobile 에서 다음 기능에 액세스하거나 액세스할 수 없습니다. 기본적으로, 허가된 액세스 (자가 지원 포털 제외), 콘솔 기능 및 권한 적용을 사용할 수 있습니다.

허가된 액세스

관리자 콘솔 액세스	관리자는 XenMobile 콘솔의 모든 기능에 액세스할 수 있습니다.
자가 지원 포털 액세스	관리자에게는 자가 지원 포털 액세스 권한이 없습니다.
공유 장치 등록자	관리자에게는 공유 장치 등록자 액세스 권한이 없습니다. 이 기능은 공유 장치를 등록해야 하는 사용자를 위한 것입니다.
원격 지원 액세스	관리자는 원격 지원 액세스를 소유합니다.*
공용 API 액세스	관리자는 공용 API 에 액세스하여 XenMobile 콘솔에서 사용할 수 있는 동작을 프로그래밍 방식으로 수행할 수 있습니다. 이러한 동작에는 인증서, 앱, 장치, 배달 그룹 및 로컬 사용자 관리가 포함됩니다.
COSU 장치 등록자	이 기능이 등록 프로필로 구성되지 않은 경우 관리자가 전용 Android Enterprise 장치 (COSU 장치라고도 함) 를 등록하는 방법을 제공합니다.

* 원격 지원을 사용하면 지원 센터 담당자가 관리되는 Android 모바일 장치를 원격으로 제어할 수 있습니다. 스크린캐스트는 Samsung Knox 장치에서만 지원됩니다. 원격 지원은 클러스터링된 온-프레미스 XenMobile Server 배포에서 지원되지 않습니다. 2019 년 1 월 1 일부터 신규 고객에게는 더 이상 원격 지원이 제공되지 않습니다. 기존 고객은 제품을 계속 사용할 수 있지만 Citrix 는 개선 사항이나 수정 사항을 제공하지 않습니다.

콘솔 기능

관리자는 XenMobile 콘솔에 대한 무제한 액세스 권한을 갖습니다.

|||

|-----|-----|

-|

| 대시보드 | ** 대시보드 ** 는 관리자가 XenMobile 콘솔에 로그인한 후 표시되는 첫 번째 페이지입니다. ** 대시보드 ** 에는 알림 및 장치에 대한 기본 정보가 표시됩니다. |

| 보고 | ** 분석 > 보고 ** 페이지에는 앱 및 장치 배포를 분석할 수 있는 미리 정의된 보고서가 제공됩니다. |

| 장치 | ** 관리 > 장치 ** 페이지에서는 사용자 장치를 관리할 수 있습니다. 관리자는 페이지에서 개별 장치를 추가하거나 장치 프로비저닝 파일을 가져와 한 번에 여러 장치를 추가할 수 있습니다. |

| 로컬 사용자 및 그룹 | ** 관리 > 사용자 ** 페이지에서는 로컬 사용자 및 로컬 사용자 그룹을 추가, 편집 또는 삭제할 수 있습니다. |

| 등록 | ** 관리 > 등록 초대 ** 페이지는 XenMobile 에 장치를 등록할 사용자를 초대하는 방법을 관리하는 곳입니다. |

| 정책 | ** 구성 > 장치 정책 ** 페이지는 VPN 및 Wi-Fi 와 같은 장치 정책을 관리하는 위치입니다. |

| 앱 | ** 구성 > 앱 ** 페이지는 관리자가 사용자가 장치에 설치할 수 있는 다양한 앱을 관리하는 곳입니다. |

| 미디어 | ** 구성 > 미디어 ** 페이지는 관리자가 사용자가 장치에 설치할 수 있는 다양한 미디어를 관리하는 곳입니다. |

| 동작 | ** 구성 > 동작 ** 페이지는 이벤트를 트리거하는 응답을 관리하는 곳입니다. |

| 등록 프로필 | ** 구성 > 등록 프로필 ** 페이지에서 관리자는 사용자가 장치를 등록할 때 사용할 등록 프로필 (모드) 을 구성할 수 있습니다. |

| 배달 그룹 | ** 구성 > 배달 그룹 ** 페이지는 관리자가 배달 그룹 및 배달 그룹과 관련된 리소스를 관리하는 곳입니다. |

| 설정 | 설정 페이지에서는 클라이언트 및 서버 속성, 인증서 및 자격 증명 공급자 같은 시스템 설정을 관리할 수 있습니다. 중요: 이러한 설정에는 RBAC 권한이 포함됩니다. RBAC 권한은 사용자에게 자신의 권한을 할당할 수 있는 기능을 포함하여 모든 권한을 부여합니다. Endpoint Management 시스템의 모든 항목을 조작할 수 있는 기능을 제공하려는 사용자에게만 이 액세스 권한을 부여하시기 바랍니다. ||

| 지원 | 문제 해결 및 지원 페이지에서 진단 실행, 로그 생성 같은 문제 해결 활동을 수행할 수 있습니다. |

장치 관리자는 장치 제한 사항을 설정하고, 장치에 대한 알림을 설정 및 전송하고, 장치의 앱을 관리하는 등 콘솔을 통해 장치 기능에 액세스합니다.

장치 전체 초기화

장치에서 모든 데이터와 앱을 초기화하며, 장치에 메모리 카드가 있는 경우 메모리 카드도 초기화합니다.

제한 사항 지우기

하나 이상의 장치 제한 사항을 제거합니다.

장치 선택적 초기화

개인 데이터 및 앱은 그대로 유지하고 장치에서 모든 회사 데이터 및 앱을 초기화합니다.

위치 보기	장치의 위치를 확인하고 지리적 제한 사항을 설정합니다. 포함 사항: 장치 찾기, 장치의 위치 보기, 장치 추적, 시간대별 장치 위치 추적
장치 잠금	사용자가 장치를 사용할 수 없도록 원격으로 장치를 잠급니다.
장치 잠금 해제	사용자가 장치를 사용할 수 있도록 원격으로 장치의 잠금을 해제합니다.
컨테이너 잠금	장치에서 회사 컨테이너를 원격으로 잠급니다.
컨테이너 잠금 해제	장치에서 회사 컨테이너를 원격으로 잠금 해제합니다.
컨테이너 암호 재설정	회사 컨테이너 암호를 재설정합니다.
ASM DEP 사용/활성화 잠금 바이패스	활성화 잠금을 사용하면 감독되는 iOS 장치에 바이패스 코드가 저장됩니다. 장치를 지워야 하는 경우 이 코드를 사용하여 활성화 잠금을 자동으로 지웁니다.
장치 벨 울림	원격으로 Windows 장치의 벨을 5 분 동안 최대 볼륨으로 울립니다.
장치 다시 부팅	XenMobile 콘솔에서 Windows 장치를 다시 시작합니다.
장치에 배포	장치에 앱, 알림, 제한 사항 등을 보냅니다.
장치 편집	장치의 설정을 변경합니다.
장치에 알림	장치에 알림을 보냅니다.
장치 추가/삭제	XenMobile 에서 장치를 추가하거나 제거합니다.
장치 가져오기	파일에서 XenMobile 로 장치 그룹을 가져옵니다.
장치 테이블 내보내기	장치 페이지에서 장치 정보를 수집하여.csv 파일로 내보냅니다.
장치 해지	장치가 XenMobile 에 연결하는 것을 금지합니다.
앱 잠금	장치의 모든 앱에 대한 액세스를 거부합니다. Android 에서는 사용자가 XenMobile 에 로그인할 수 없습니다. iOS 에서는 사용자가 로그인할 수는 있지만 앱에 액세스할 수는 없습니다.
앱 초기화	Android 에서는 이 작업으로 사용자의 XenMobile 계정이 삭제됩니다. iOS 에서는 이 작업으로 XenMobile 기능에 액세스하는 데 필요한 암호화 키가 삭제됩니다.
소프트웨어 인벤토리 보기	어떤 소프트웨어가 장치에 설치되어 있는지 확인합니다.
AirPlay 미러링 요청	AirPlay 스트리밍을 시작하도록 요청합니다.
AirPlay 미러링 중지	AirPlay 스트리밍을 중지합니다.

분실 모드 활성화	관리 > 장치에서 감독되는 장치를 분실 모드로 설정하여 잠금 화면에서 감독되는 장치를 차단할 수 있습니다. 분실 모드를 사용하면 장치가 분실 또는 도난 당했을 때 장치를 찾을 수도 있습니다.
분실 모드 비활성화	관리 > 장치에서 분실 모드로 설정된 장치의 분실 모드를 비활성화할 수 있습니다.
OS 업데이트 장치	OS 업데이트 제어 장치 정책을 장치에 배포할 수 있습니다.
장치 종료	XenMobile 콘솔에서 iOS 장치를 종료합니다.
장치 다시 시작	XenMobile 콘솔에서 iOS 장치를 다시 시작합니다.

로컬 사용자 및 그룹 관리자는 XenMobile 의 관리 > 사용자 페이지에서 로컬 사용자 및 로컬 사용자 그룹을 관리합니다.

로컬 사용자 추가
로컬 사용자 삭제
로컬 사용자 편집
로컬 사용자 가져오기
로컬 사용자 내보내기
로컬 사용자 그룹
로컬 사용자 잠금 ID 받기
로컬 사용자 잠금 삭제

등록 관리자는 등록 초대장을 추가 및 삭제하고, 사용자에게 알림을 보내고, 등록 테이블을.csv 파일로 내보낼 수 있습니다.

등록 추가/삭제	사용자 또는 사용자 그룹에 대한 등록 초대장을 추가하거나 제거합니다.
사용자 알림	사용자 또는 사용자 그룹에 대한 등록 초대장을 보냅니다.
등록 초대 테이블 내보내기	등록 페이지에서 등록 정보를 수집하여.csv 파일로 내보냅니다.

정책

정책 추가/삭제	장치 또는 앱 정책을 추가하거나 제거합니다.
정책 편집	장치 또는 앱 정책을 변경합니다.
정책 업로드	장치 또는 앱 정책을 업로드합니다.
정책 복제	장치 또는 앱 정책을 복사합니다.
정책 사용 안 함	기존 앱 정책을 사용하지 않도록 설정합니다.
정책 내보내기	장치 정책 페이지에서 장치 정책 정보를 수집하여.csv 파일로 내보냅니다.
정책 할당	장치 정책을 하나 이상의 배달 그룹에 할당합니다.

앱 관리자는 XenMobile 의 구성 > 앱 페이지에서 앱을 관리합니다.

앱 스토어 또는 엔터프라이즈 앱 추가/삭제	공용 앱 스토어 앱 또는 엔터프라이즈 앱 (MDX 지원 아님) 을 추가하거나 제거합니다.
앱 스토어 또는 엔터프라이즈 앱 편집	공용 앱 스토어 앱 또는 엔터프라이즈 앱 (MDX 지원 아님) 을 변경합니다.
MDX, 웹, SaaS 앱 추가/삭제	MDX 지원 앱, 내부 네트워크의 앱 (웹 앱) 또는 공용 네트워크 (SaaS) 의 앱을 XenMobile 에 추가하거나 제거합니다.
MDX, 웹 및 SaaS 앱 편집	MDX 지원 앱, 내부 네트워크의 앱 (웹 앱) 또는 공용 네트워크 (SaaS) 의 앱을 XenMobile 에서 변경합니다.
범주 추가/삭제	XenMobile Store 에서 앱을 표시할 수 있는 범주를 추가하거나 삭제합니다.
공용/엔터프라이즈 앱을 배달 그룹에 할당	배포를 위해 공용 앱 스토어 앱 또는 MDX 지원 앱을 배달 그룹에 할당합니다.
MDX/WebLink/SaaS 앱을 배달 그룹에 할당	Single Sign-on(WebLink) 이 필요하지 않거나 공용 네트워크 (SaaS) 에 있는 MDX 지원 앱을 배달 그룹에 할당합니다.
앱 테이블 내보내기	앱 페이지에서 앱 정보를 수집하여.csv 파일로 내보냅니다.

참고:

콘솔 기능 > 앱을 선택하면 API 엔드포인트 GET <https://XMS_IP:4443/controlpoint/rest/ad>에서 설계상 LDAP 정보를 반환합니다.

미디어 공용 앱 스토어 또는 볼륨 구매 라이선스를 통해 취득한 미디어를 관리합니다.

앱 스토어 또는 엔터프라이즈 서적 추가/삭제

공용/엔터프라이즈 서적을 배달 그룹에 할당

앱 스토어 또는 엔터프라이즈 서적 편집

동작

작업 추가/삭제

트리거 (이벤트, 장치/사용자 속성 또는 설치된 앱 이름) 및 관련 응답에 의해 정의된 동작을 추가하거나 제거합니다.

작업 편집

트리거 (이벤트, 장치/사용자 속성 또는 설치된 앱 이름) 및 관련 응답에 의해 정의된 동작을 변경합니다.

작업을 배달 그룹에 할당

사용자 장치에 배포하기 위해 배달 그룹에 동작을 할당합니다.

작업 내보내기

동작 페이지에서 동작 정보를 수집하여.csv 파일로 내보냅니다.

배달 그룹 관리자는 구성 > 배달 그룹 페이지에서 배달 그룹을 관리합니다.

배달 그룹 추가/삭제

지정된 사용자 및 선택적인 정책, 앱 및 동작을 추가하는 배달 그룹을 만들거나 제거합니다.

배달 그룹 편집

기존 배달 그룹을 변경하여, 사용자 및 선택적인 정책, 앱 및 동작을 수정합니다.

배달 그룹 배포

배달 그룹을 사용할 수 있게 만듭니다.

배달 그룹 내보내기

배달 그룹 페이지에서 배달 그룹 정보를 수집하고 이를.csv 파일로 내보냅니다.

등록 프로필 등록 프로필을 관리합니다.

등록 프로필 추가/삭제

등록 프로필 편집

배달 그룹에 등록 프로필 할당

설정 관리자는 설정 페이지에서 다양한 설정을 구성합니다.

RBAC	RBAC 할당, 역할을 할당합니다. 중요: 이 권한은 사용자에게 자신의 권한을 할당할 수 있는 기능을 포함하여 모든 권한을 부여합니다. Endpoint Management 시스템의 모든 항목을 조작할 수 있는 기능을 제공하려는 사용자에게만 이 액세스 권한을 부여하시기 바랍니다.
LDAP	그룹, 사용자 계정 및 관련 속성을 가져올 수 있도록 하나 이상의 LDAP 호환 디렉터리 (예: Active Directory) 를 관리합니다.
라이선스	온-프레미스 XenMobile Server 에 해당합니다. Citrix 라이선스를 관리합니다.
등록	사용자 및 자가 지원 포털에 대해 등록 보안 모드를 사용하도록 설정합니다.
릴리스 관리	현재 설치된 릴리스를 확인합니다. 포함 사항: 릴리스 관리 업데이트
인증서	APNS 인증서 편집, 인증서 SSL 수신기
알림 템플릿	자동화 동작이나 등록에서, 아니면 사용자에게 표준 알림 메시지를 제공할 때 사용할 알림 템플릿을 만듭니다.
워크플로	앱 구성에 사용할 수 있도록 사용자 계정의 만들기, 승인 및 제거를 관리합니다.
자격 증명 공급자	장치 인증서를 발급하도록 승인된 하나 이상의 자격 증명 공급자를 추가합니다. 자격 증명 공급자는 인증서 형식과 인증서를 갱신하거나 해지하기 위한 조건을 제어합니다.
PKI 엔터티	공개 키 인프라 엔터티 (일반, Microsoft 인증서 서비스 또는 임의의 CA) 를 관리합니다.
PKI 연결 테스트	설정 > PKI 엔터티 페이지의 연결 테스트 단추를 사용하여 서버에 액세스할 수 있는지 확인합니다.
클라이언트 속성	암호 유형, 강도 또는 만료와 같은 사용자 장치의 다양한 속성을 관리합니다.

클라이언트 지원	사용자가 지원 서비스에 연락할 수 있는 방법 (전자 메일, 전화 또는 지원 티켓 전자 메일) 을 설정합니다.
클라이언트 브랜딩	XenMobile Store 의 사용자 지정 스토어 이름과 기본 스토어 보기를 생성합니다. XenMobile Store 또는 Secure Hub 에 표시되는 사용자 지정 로고를 추가합니다.
이동 통신 사업자 SMS 게이트웨이	이동 통신 사업자의 SMS 게이트웨이를 설정하여 이동 통신 사업자의 SMS 게이트웨이를 통해 XenMobile 이 전송하는 알림을 구성합니다.
알림 서버	사용자에게 전자 메일을 보내도록 SMTP 게이트웨이 서버를 설정합니다.
ActiveSync Gateway	규칙 및 속성을 통해 사용자 및 장치에 대한 사용자 액세스를 관리합니다.
Apple 배포 프로그램	XenMobile 에 Apple 배포 프로그램 계정을 추가합니다.
Apple Configurator 장치 등록	XenMobile 에서 Apple Configurator 설정을 구성합니다.
iOS/볼륨 구매 설정	Apple 볼륨 구매 계정을 추가합니다.
모바일 서비스 공급자	모바일 서비스 공급자 인터페이스를 사용하여 BlackBerry 및 기타 Exchange ActiveSync 장치를 쿼리하고 작업을 실행합니다.
Citrix Gateway	온-프레미스 XenMobile Server 에 해당합니다. Citrix Gateway 를 추가합니다. 인증을 사용할지 여부와 인증 시 사용자 인증서를 푸시할지 여부를 선택합니다. 자격 증명 공급자를 선택합니다.
네트워크 액세스 제어	장치가 규정을 준수하지 않는지 확인하고 네트워크에 대한 액세스를 거부하는 조건을 설정합니다.
Samsung Knox	XenMobile 이 Samsung Knox 증명 서버 REST API 를 쿼리하거나 쿼리하지 않도록 설정합니다.
서버 속성	서버 속성을 추가하거나 수정합니다. 모든 노드에서 XenMobile 을 다시 시작해야 합니다.
Syslog	온-프레미스 XenMobile Server 에 해당합니다. 서버 호스트 이름 또는 IP 주소를 사용하여 시스템 로그 (syslog) 서버로 로그 파일을 보냅니다.
XenApp 및 XenDesktop	사용자가 Citrix Secure Hub 를 통해 Virtual Apps and Desktops 를 추가할 수 있습니다.

Citrix Files	XenMobile 을 Enterprise 계정과 사용할 경우: ShareFile 계정 및 관리자 서비스 계정에 연결하여 사용자 계정을 관리하는 설정을 구성합니다. 기존 Citrix Files 도메인 및 관리자 자격 증명이 필요합니다. XenMobile 과 함께 StorageZone 커넥터를 사용하는 경우: StorageZone 커넥터에 정의된 네트워크 공유 및 SharePoint 위치를 가리키도록 XenMobile 을 구성합니다.
환경 개선 프로그램	온-프레미스 XenMobile Server 에 해당합니다. Citrix 로 익명 통계 및 사용 현황 정보를 보내거나 보내지 않도록 선택합니다.
Microsoft Azure	온-프레미스 XenMobile Server 에 해당합니다. XenMobile 과 Microsoft Azure 를 통합합니다.
Android Enterprise	Android Enterprise 서버 설정을 구성합니다.
IdP(ID 공급자)	ID 공급자를 구성합니다.
XenMobile Tools	XenMobile Tools 페이지에 액세스합니다.
SNMP 구성	XenMobile Server 노드에 대해 SNMP 를 사용하도록 설정합니다. 모니터링 사용자를 편집 또는 추가하고, 트랩 알림이 나타나는 SNMP 관리자를 설정하고, 트랩 간격과 임계값을 구성합니다.

지원 관리자는 다양한 지원 작업을 수행할 수 있습니다.

Citrix Gateway 연결 확인	IP 주소로 Citrix Gateway 에 대한 다양한 연결 확인을 수행합니다. 사용자 이름 및 암호가 필요합니다.
XenMobile 연결 확인	선택한 XenMobile 기능 (예: 데이터베이스, DNS 또는 Google Plan) 에 대한 연결 확인을 수행합니다.
지원 번들 만들기	온-프레미스 XenMobile Server 에 해당합니다. 문제 해결을 위해 Citrix 지원에 보낼 파일을 생성합니다. XenMobile 또는 Citrix Gateway 에 대한 시스템 정보, 로그, 데이터베이스 정보, 핵심 정보, 추적 파일 및 최신 구성 정보가 포함됩니다.
Citrix 제품 설명서	공개 Citrix XenMobile 설명서 사이트에 액세스합니다.
Citrix Knowledge Center	Citrix 지원 사이트에 액세스하여 기술 자료 문서를 검색합니다.

로그	디버그, 관리자 감사 및 사용자 감사에 대한 로그 파일 세부 정보에 액세스하고 분석합니다.
클러스터 정보	온-프레미스 XenMobile Server 에 해당합니다. 클러스터된 환경의 각 노드에 대한 정보에 액세스합니다.
가비지 수집	온-프레미스 XenMobile Server 에 해당합니다. 더 이상 사용하지 않는 메모리 개체에 대한 정보에 액세스합니다.
Java 메모리 속성	온-프레미스 XenMobile Server 에 해당합니다. Java 메모리 사용 현황, 메모리 세부 정보 및 메모리 풀 세부 정보의 스냅샷에 액세스합니다.
매크로	프로필, 정책, 알림 또는 등록 템플릿의 텍스트 필드에 사용자 또는 장치 속성 데이터를 채웁니다. 단일 정책을 구성하여 대규모 사용자 기반에 정책을 배포하고 각 대상 사용자에게 사용자 관련 값이 표시되게 합니다.
PKI 구성	PKI 구성 정보를 가져오고 내보냅니다.
APNS 서명 유틸리티	APNs(Apple Push Network signing) 인증서에 대한 요청을 제출하거나 iOS 용 Secure Mail APNs 인증서를 업로드합니다.
Citrix Insight Services	다양한 문제에 대한 도움을 받으려면 CIS(Citrix Insight Services) 에 로그를 업로드하십시오.
Exchange ActiveSync 용 Citrix Gateway 커넥터 장치 상태	장치 ActiveSync ID 를 기반으로 Exchange ActiveSync 용 Citrix Gateway 커넥터로 전송된 장치의 상태를 XenMobile 에 쿼리합니다.
익명화 및 익명화 취소	온-프레미스 XenMobile Server 에 해당합니다. XenMobile 에서 지원 번들을 만드는 경우 중요한 사용자, 서버 및 네트워크 데이터가 기본적으로 익명으로 만들어집니다. 고급 아래의 지원 > 익명화 및 익명화 취소에서 이 동작을 변경할 수 있습니다.
로그 설정	로그 수준을 사용자 지정하거나 사용자 지정 로거를 추가합니다.

그룹 액세스 제한

관리 사용자는 모든 사용자 그룹에 권한을 적용할 수 있습니다.

지원 역할

지원 역할이 있는 사용자는 원격 지원에 액세스할 수 있습니다. 이 권한은 기본적으로 모든 사용자에게 적용되며 이 설정을 편집할 수 없습니다.

사용자 역할

사용자 역할을 가진 사용자는 다음과 같이 XenMobile 에 제한적으로 액세스할 수 있습니다.

허가된 액세스

자가 지원 포털	사용자는 XenMobile 에서 자가 지원 포털에만 액세스할 수 있습니다.
----------	---

콘솔 기능

사용자는 XenMobile 콘솔에 대해 다음과 같은 제한적인 액세스 권한을 갖습니다.

장치

장치 전체 초기화	장치에서 모든 데이터와 앱을 초기화하며, 장치에 메모리 카드가 있는 경우 메모리 카드도 초기화합니다.
장치 선택적 초기화	개인 데이터 및 앱은 그대로 유지하고 장치에서 모든 회사 데이터 및 앱을 초기화합니다.
위치 보기	장치의 위치를 확인하고 지리적 제한 사항을 설정합니다. 포함 사항: 장치 찾기, 장치의 위치 보기, 장치 추적, 시간대별 장치 위치 추적
장치 잠금	장치를 원격으로 잠가 사용할 수 없게 만듭니다.
장치 잠금 해제	장치를 원격으로 잠금 해제하여 사용할 수 있게 만듭니다.
컨테이너 잠금	장치에서 회사 컨테이너를 원격으로 잠급니다.
컨테이너 잠금 해제	장치에서 회사 컨테이너를 원격으로 잠금 해제합니다.
컨테이너 암호 재설정	회사 컨테이너 암호를 재설정합니다.

ASM DEP 사용/활성화 잠금 바이패스

활성화 잠금을 사용하면 감독되는 iOS 장치에 바이패스 코드가 저장됩니다. 장치를 지워야 하는 경우 이 코드를 사용하여 활성화 잠금을 자동으로 지웁니다.

장치 벨 울림

원격으로 Windows 장치의 벨을 5 분 동안 최대 볼륨으로 울립니다.

장치 다시 부팅

Windows 장치를 다시 시작합니다.

소프트웨어 인벤토리 보기

어떤 소프트웨어가 장치에 설치되어 있는지 확인합니다.

등록

등록 추가/삭제

사용자 또는 사용자 그룹에 대한 등록 초대를 추가하거나 제거합니다.

사용자 알림

사용자 또는 사용자 그룹에 대한 등록 초대를 보냅니다.

그룹 액세스 제한

네 가지 기본 역할 모두에 대해 이 권한은 기본적으로 설정되며 모든 사용자 그룹에 적용할 수 있습니다. 이 역할은 편집할 수 없습니다.

RBAC 를 사용하여 역할 구성

XenMobile 의 RBAC(역할 기반 액세스 제어) 를 사용하여 미리 정의된 역할 또는 권한 집합을 사용자 및 그룹에 할당할 수 있습니다. 이러한 권한은 시스템 기능에 대한 사용자 액세스 수준을 제어합니다.

XenMobile 은 네 가지 기본 사용자 역할을 구현하여 시스템 기능에 대한 액세스 권한을 논리적으로 분리합니다.

- 관리자: 전체 시스템 액세스 권한을 부여합니다.
- 지원: 원격 지원에 대한 액세스 권한을 부여합니다.
- 사용자: 장치를 등록할 수 있고 자가 지원 포털에 액세스할 수 있는 사용자가 사용됩니다.

사용자 역할을 만들기 위해 사용자 지정하는 템플릿으로 기본 역할을 사용할 수도 있습니다. 기본 역할에 정의된 기능 이외의 특정 시스템 기능에 액세스할 수 있는 권한이 있는 새로운 사용자 역할을 만들 수 있습니다.

역할은 로컬 사용자 (사용자 수준) 또는 Active Directory 그룹 (해당 그룹의 모든 사용자가 동일한 권한을 가짐) 에 할당할 수 있습니다. 사용자가 여러 Active Directory 그룹에 속하는 경우 모든 권한이 병합되어 해당 사용자의 권한을 정의합니다. 예를 들어 ADGroupA 사용자는 관리자 장치를 찾을 수 있고 ADGroupB 사용자는 직원 장치를 초기화할 수 있습니다. 이 경우, 두 그룹 모두에 속하는 사용자는 관리자와 직원의 장치를 찾고 초기화할 수 있습니다.

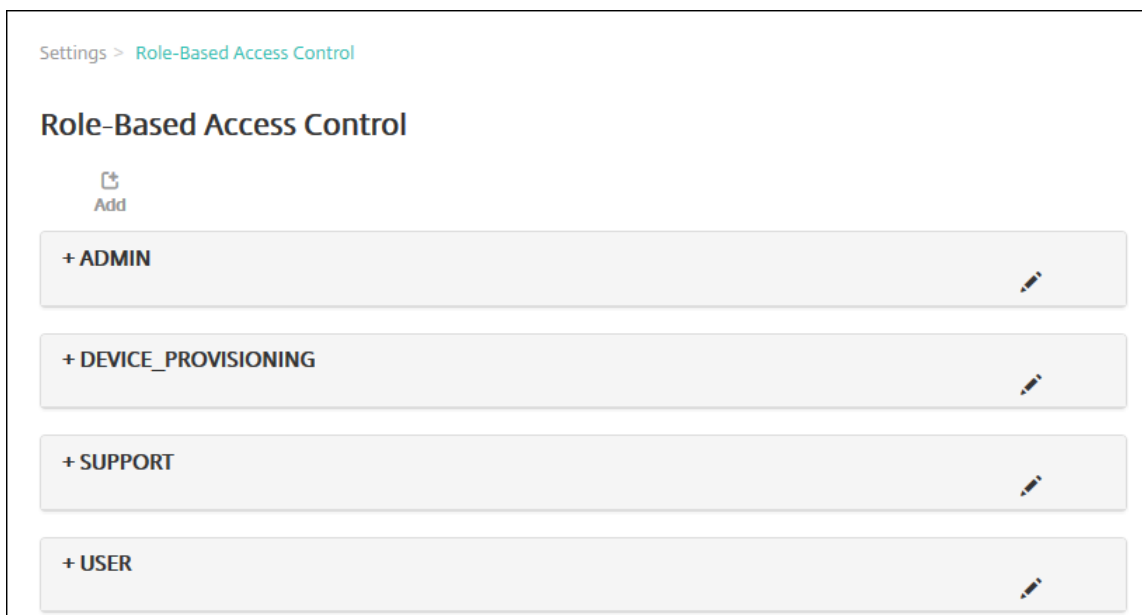
참고:

로컬 사용자에게는 하나의 역할만 할당될 수 있습니다.

XenMobile 의 RBAC 기능을 사용하여 다음을 수행할 수 있습니다.

- 역할을 만듭니다.
- 역할에 그룹을 추가합니다.
- 로컬 사용자를 역할에 연결합니다.

1. XenMobile 콘솔에서 설정 > 역할 기반 액세스 제어로 이동합니다. 역할 기반 액세스 제어 페이지가 나타납니다. 이 페이지에는 네 개의 기본 사용자 역할과 앞서 추가한 모든 역할이 표시됩니다.



역할 옆에 있는 더하기 기호 (+) 를 클릭하면 다음 그림과 같이 역할이 확장되어 해당 역할에 대한 모든 권한이 표시됩니다.



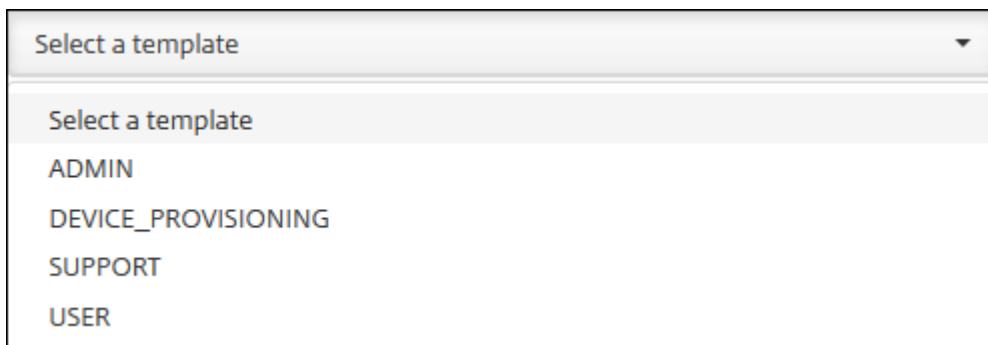
2. 새 사용자 역할을 추가하려면 추가를 클릭합니다. 역할을 편집하려면 기존 역할 오른쪽에 있는 펜 아이콘을 클릭합니다. 역할을 삭제하려면 역할 오른쪽에 있는 휴지통 아이콘을 클릭합니다. 기본 사용자 역할은 삭제할 수 없습니다.

- 추가 또는 연필 아이콘을 클릭하면 역할 추가 또는 역할 편집 페이지가 나타납니다.
- 휴지통 아이콘을 클릭하면 확인 대화 상자가 나타납니다. 선택한 역할을 제거하려면 삭제를 클릭합니다.

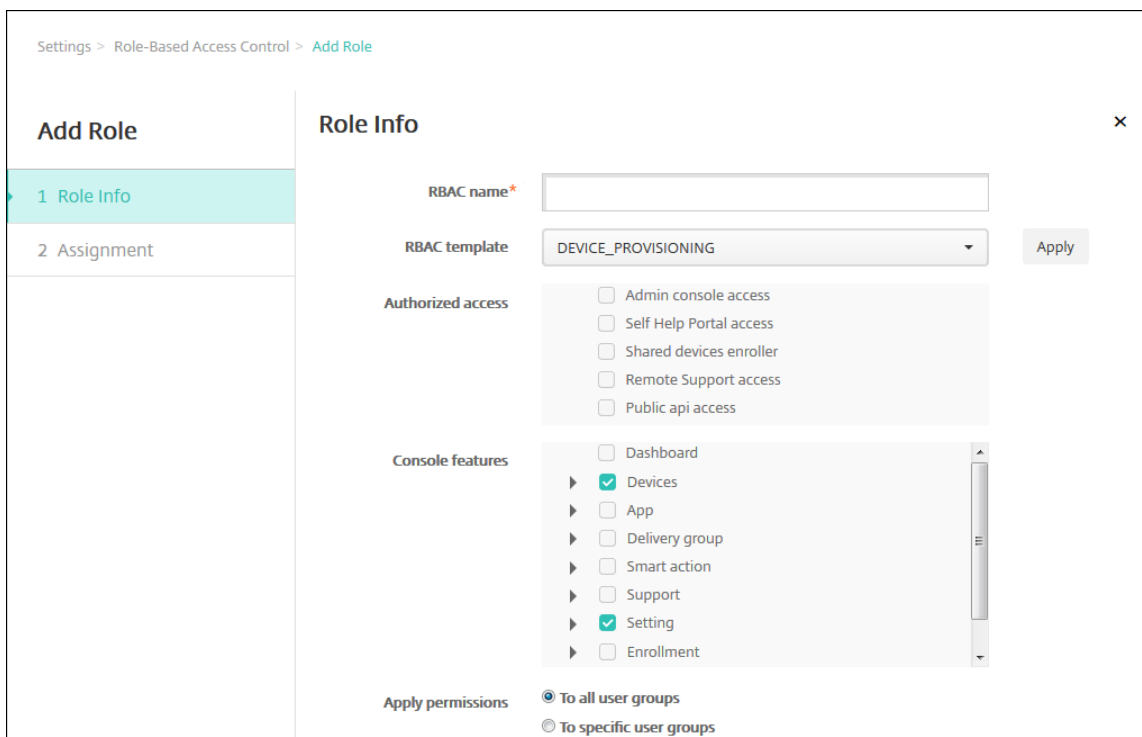
3. 다음 정보를 입력하여 사용자 역할을 만들거나 편집합니다.

- **RBAC 이름:** 새 사용자 역할을 설명하는 이름을 입력합니다. 기존 역할의 이름은 변경할 수 없습니다.
- **RBAC 템플릿:** 선택적으로, 새 역할의 시작점으로 사용할 템플릿을 클릭합니다. 기존 역할을 편집하는 경우 템플릿을 선택할 수 없습니다.

RBAC 템플릿은 기본 사용자 역할입니다. 이러한 템플릿은 해당 역할과 연결된 사용자가 갖는 시스템 기능에 대한 액세스 권한을 정의합니다. RBAC 템플릿을 선택한 후 허가된 액세스 및 콘솔 기능 필드에서 해당 역할과 연결된 모든 권한을 확인할 수 있습니다. 템플릿 사용은 선택 사항입니다. 허가된 액세스 및 콘솔 기능 필드에서 역할에 할당할 옵션을 직접 선택할 수 있습니다.



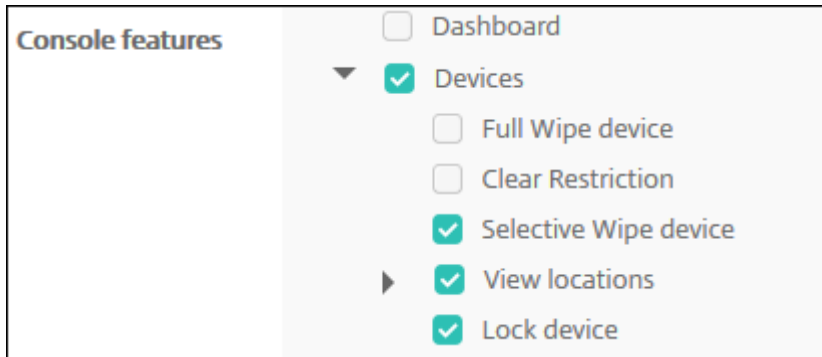
4. **RBAC** 템플릿 필드 가까이에 있는 적용을 클릭하여 허가된 액세스 및 콘솔 기능을 미리 정의된 액세스 권한과 기능 권한으로 채웁니다.



5. 허가된 액세스 및 콘솔 기능의 확인란을 선택하고 선택 취소하여 역할을 사용자 지정합니다.

콘솔 기능 옆에 있는 삼각형을 클릭하면 해당 기능과 관련된 권한이 선택하거나 선택 취소할 수 있도록 나타납니다. 최상

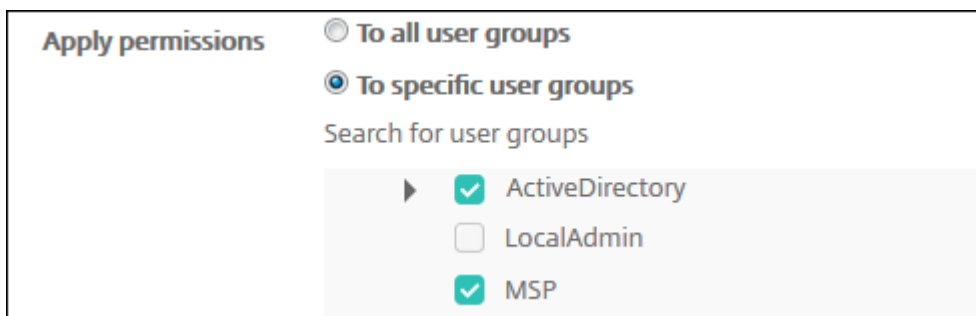
위 확인란을 클릭하면 해당 콘솔 영역에 대한 액세스가 금지됩니다. 이러한 옵션을 활성화하려면 최상위 아래에 있는 개별 옵션을 선택합니다. 예를 들어 다음 그림에서 역할에 할당된 사용자에게 장치 전체 초기화 및 제한 사항 지우기 옵션은 나타나지 않습니다. 선택된 옵션이 나타납니다.



6. 권한 적용: 하나 이상의 사용자 그룹을 선택하여 관리자가 관리할 수 있는 그룹을 제한합니다. 특정 사용자 그룹을 클릭하면 하나 이상의 그룹을 선택할 수 있는 그룹 목록이 나타납니다.

예를 들어 RBAC 관리자에게 ActiveDirectory 및 MSP 사용자 그룹에 대한 권한이 있는 경우:

- 관리자는 ActiveDirectory 그룹, MSP 그룹 또는 두 그룹 모두에 있는 사용자에게 정보에만 액세스할 수 있습니다.
- 관리자는 다른 로컬 또는 AD 사용자를 볼 수 없습니다. 관리자는 이러한 그룹 중 하나의 하위 그룹에 속하는 사용자를 볼 수 있습니다.
- 관리자는 다음으로 초대장을 보낼 수 있습니다.
 - 권한 그룹 및 해당 하위 그룹
 - 권한 그룹 및 하위 그룹의 구성원인 사용자



7. 다음을 클릭합니다. 할당 페이지가 나타납니다.

Settings > Role-Based Access Control > Add Role

Add Role

- 1 Role Info
- 2 Assignment

Assignment
Assign the RBAC role to user groups

Select domain: testprise.net

Include user groups: Search

Selected user groups:

8. 다음 정보를 입력하여 사용자 그룹에 역할을 할당합니다.

- 도메인 선택: 목록에서 도메인을 클릭합니다.
- 사용자 그룹 포함: 검색을 클릭하여 사용 가능한 모든 그룹의 목록을 보거나, 그룹 이름 전체 또는 일부를 입력하여 해당 이름을 포함하는 그룹으로만 목록을 제한합니다.
- 나타나는 목록에서 역할을 할당할 사용자 그룹을 선택합니다. 사용자 그룹을 선택하면 해당 그룹이 선택된 사용자 그룹 목록에 나타납니다.

Settings > Role-Based Access Control > Add Role

Add Role

- 1 Role Info
- 2 Assignment

Assignment
Assign the RBAC role to user groups

Select domain: testprise.net

Include user groups: user Search

Selected user groups:

- testprise.net
 - Remote Desktop Users
 - Performance Monitor Users

참고:

선택된 사용자 그룹 목록에서 사용자 그룹을 제거하려면 사용자 그룹 이름 옆에 있는 X를 클릭합니다.

9. 저장을 클릭합니다.

알림

June 10, 2022

XenMobile 에서 다음과 같은 용도로 알림을 사용할 수 있습니다.

- 선택적인 사용자 그룹에게 여러 가지 시스템 관련 기능을 전달합니다. 특정 사용자를 대상으로 이러한 알림을 보낼 수도 있습니다. 예를 들어 모든 iOS 장치 사용자, 장치가 규정 위반 상태인 사용자, 직원 소유의 장치 사용자 등을 대상으로 할 수 있습니다.
- 사용자 및 장치를 등록합니다.
- 특정 조건이 충족될 때 사용자에게 자동으로 알림을 보냅니다 (자동화 동작 사용). 예:
 - 규정 문제로 인해 기업 도메인에서 사용자 장치를 차단할 예정인 경우
 - 장치가 탈옥 또는 루팅된 경우

자동화 동작에 대한 자세한 내용은 [자동화된 동작](#)을 참조하십시오.

XenMobile 에서 알림을 보내려면 게이트웨이 및 알림 서버를 구성해야 합니다. XenMobile 에서 알림 서버를 설정하고 SMTP(Simple Mail Transfer Protocol) 및 SMS(Short Message Service) 게이트웨이 서버를 구성하여 사용자에게 전자 메일 및 텍스트 (SMS) 알림을 보낼 수 있습니다. 알림을 사용하여 SMTP 또는 SMS 의 두 개 채널로 메시지를 보낼 수 있습니다.

- SMTP 는 연결 지향적인 텍스트 기반 프로토콜로, 일반적으로 TCP(Transmission Control Protocol) 연결을 통해 명령 문자열을 실행하고 필요한 데이터를 제공하는 방식으로 메일을 보낸 사람과 메일을 받는 사람이 통신합니다. SMTP 세션은 SMTP 클라이언트 (메시지를 보내는 사람) 에서 시작된 명령과 이에 대한 SMTP 서버의 응답으로 구성됩니다.
- SMS 는 전화, 웹 또는 모바일 통신 시스템의 문자 메시지 서비스 구성 요소입니다. SMS 는 표준화된 통신 프로토콜을 사용하여 유선 전화 또는 휴대폰 장치에서 SMS 를 교환할 수 있도록 합니다.

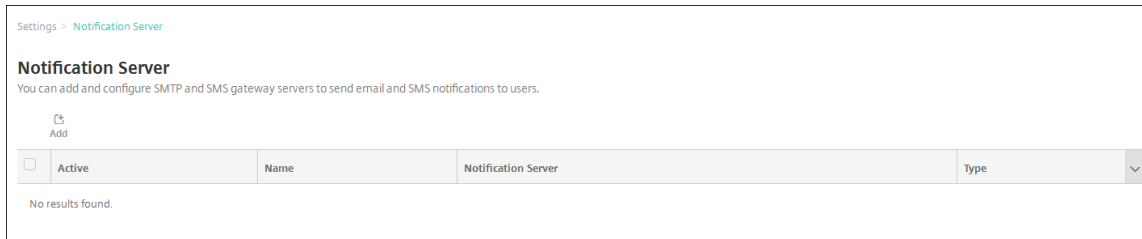
또한 XenMobile 에서 이동 통신 사업자 SMS 게이트웨이를 설정하여 이동 통신 사업자의 SMS 게이트웨이를 통해 전송되는 알림을 구성할 수 있습니다. 이동 통신 사업자는 통신 네트워크를 통한 SMS 전송의 송수신에 SMS 게이트웨이를 사용합니다. 이러한 텍스트 기반 메시지는 표준화된 통신 프로토콜을 사용하여 유선 전화 또는 휴대폰 장치에서 SMS 를 교환할 수 있도록 합니다.

사전 요구 사항

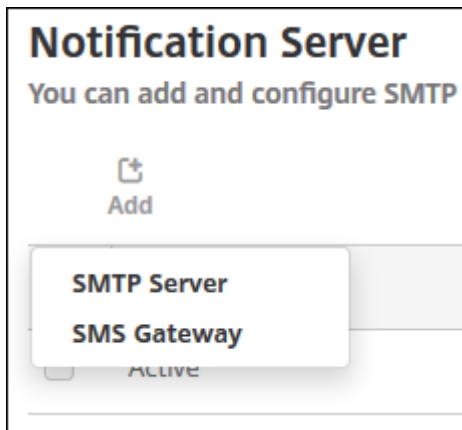
- SMS 게이트웨이를 구성하기 전에 시스템 관리자에게 문의하여 서버 정보를 확인하십시오. SMS 서버가 내부 회사 서버에서 호스트되는지, 호스트되는 전자 메일 서비스의 일부인지를 확인해야 합니다. 후자의 경우 서비스 공급자의 웹 사이트에서 정보를 얻어야 합니다.
- 사용자에게 메시지를 보내도록 SMTP 알림 서버를 구성합니다. 서버가 내부 서버에서 호스트되는 경우 시스템 관리자에게 구성 정보를 문의하십시오. 서버가 호스트되는 전자 메일 서비스인 경우 서비스 공급자의 웹 사이트에서 해당하는 구성 정보를 찾으십시오.
- 하나의 활성 SMTP 서버와 하나의 활성 SMS 서버를 동시에 사용할 수 있습니다. 두 통신 채널 모두 하나의 활성 구성을 허용합니다.
- 네트워크 DMZ 에 위치한 XenMobile 에서 포트 25 를 열어 내부 네트워크의 SMTP 서버를 다시 가리키도록 합니다. 이렇게 하면 XenMobile 에서 성공적으로 알림을 보낼 수 있습니다.

SMTP 서버 및 SMS 게이트웨이 구성

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 알림에서 알림 서버를 클릭합니다. 알림 서버 페이지가 나타납니다.



3. 추가를 클릭합니다. SMTP 서버 또는 SMS 게이트웨이를 구성하는 옵션이 포함된 메뉴가 나타납니다.



- SMTP 서버를 추가하려면 **SMTP** 서버를 클릭하고 [SMTP 서버를 추가하려면](#)의 단계에 따라 이 설정을 구성합니다.
- SMS 게이트웨이를 추가하려면 **SMS** 게이트웨이를 클릭하고 [SMS 게이트웨이를 추가하려면](#)의 단계에 따라 이 설정을 구성합니다.

SMTP 서버 추가

Settings > Notification Server > Add SMTP Server

Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*

Description

SMTP Server*

Secure channel protocol None ▼

SMTP server port*

Authentication OFF

Microsoft Secure Password Authentication (SPA) OFF

From name*

From email*

Test Configuration

► Advanced Settings

Cancel Add

1. 다음 설정을 구성합니다.

- **이름:** SMTP 서버 계정에 연결된 이름을 입력합니다.
- **설명:** 필요한 경우 서버의 설명을 입력합니다.
- **SMTP 서버:** 서버의 호스트 이름을 입력합니다. 호스트 이름은 FQDN(정규화된 도메인 이름) 또는 IP 주소일 수 있습니다.
- **보안 채널 프로토콜:** 목록에서 서버가 사용하는 보안 채널 프로토콜에 대해 **SSL**, **TLS** 또는 없음을 클릭합니다 (보안 인증을 사용하도록 서버가 구성된 경우). 기본값은 없음입니다.
- **SMTP 서버 포트:** SMTP 서버에서 사용하는 포트를 입력합니다. 기본적으로 포트는 25로 설정됩니다. SMTP 연결에 SSL 보안 채널 프로토콜이 사용되는 경우 포트는 465로 설정됩니다.
- **인증:** 켜짐 또는 꺼짐을 선택합니다. 기본값은 꺼짐입니다.

- 인증을 사용하는 경우 다음 설정을 구성합니다.
 - 사용자 이름: 인증에 사용할 사용자 이름을 입력합니다.
 - 암호: 인증 사용자의 암호를 입력합니다.
 - **Microsoft SPA(보안 암호 인증):** SMTP 서버에서 SPA 를 사용하는 경우 커짐을 클릭합니다. 기본값은 꺼짐입니다.
 - 발신자 이름: 클라이언트에서 이 서버의 알림 전자 메일을 수신할 때 보낸 사람 상자에 표시되는 이름을 입력합니다. 예를 들어, 회사 IT 를 입력합니다.
 - 발신자 전자 메일: 전자 메일 받는 사람이 SMTP 서버에서 보낸 알림에 회신할 때 사용하는 전자 메일 주소를 입력합니다.
2. 구성 테스트를 클릭하여 테스트 전자 메일 알림을 보냅니다.
3. 고급 설정을 확장하고 다음 설정을 구성합니다.
- **SMTP 재시도 횟수:** SMTP 서버에서 보낸 실패한 메시지를 재시도할 횟수를 입력합니다. 기본값은 5 입니다.
 - **SMTP 시간 제한:** SMTP 요청을 보낼 때 대기할 기간 (초) 을 입력합니다. 시간 제한으로 인해 메시지 전송이 지속적으로 실패하는 경우 이 값을 늘립니다. 이 값을 줄일 때는 주의하십시오. 시간 초과로 인해 배달되지 않은 메시지의 수가 늘어날 수 있습니다. 기본값은 30 초입니다.
 - **최대 SMTP 받는 사람 수:** SMTP 서버에서 보내는 전자 메일 메시지당 최대 받는 사람 수를 입력합니다. 기본값은 100 입니다.
4. 추가를 클릭합니다.

SMS 게이트웨이 추가

Settings > Notification Server > Add SMS Gateway

Add SMS Gateway

Please consult with your IT department about the server info if the SMS server is hosted on internal corporate server; if this is a hosted email service, the info is available from the service provider's website. Only one SMS server is activated at one time.

Name*

Description

Key*

Secret*

Virtual phone number*

HTTPS ☐ OFF

Country code

Use Carrier Gateway ☒ ON

메모:

XenMobile 은 Nexmo SMS 메시지만 지원합니다. Nexmo 메시지 사용을 위한 계정이 없는 경우 [웹 사이트](#)를 방문하여 계정을 만드십시오.

1. 다음 설정을 구성합니다.

- **이름:** SMS 게이트웨이 구성의 이름을 입력합니다. 이것은 필수 필드입니다.
- **설명:** 필요한 경우 구성의 설명을 입력합니다.
- **키:** 계정을 활성화할 때 시스템 관리자가 제공한 숫자 식별자를 입력합니다. 이것은 필수 필드입니다.
- **암호:** 암호 분실 또는 도난 시 계정에 액세스하는 데 사용할 시스템 관리자가 제공한 암호를 입력합니다. 이것은 필수 필드입니다.
- **가상 전화 번호:** 이 필드는 북미 전화 번호 (+1 접두사 사용) 로 보낼 때 사용합니다. 이 필드에는 Nexmo 가상 전화 번호를 입력해야 하며 숫자만 사용해야 합니다. Nexmo 웹 사이트에서 가상 전화 번호를 구입할 수 있습니다.
- **HTTPS:** SMS 요청을 Nexmo 에 전송할 때 HTTPS 를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다.

중요:

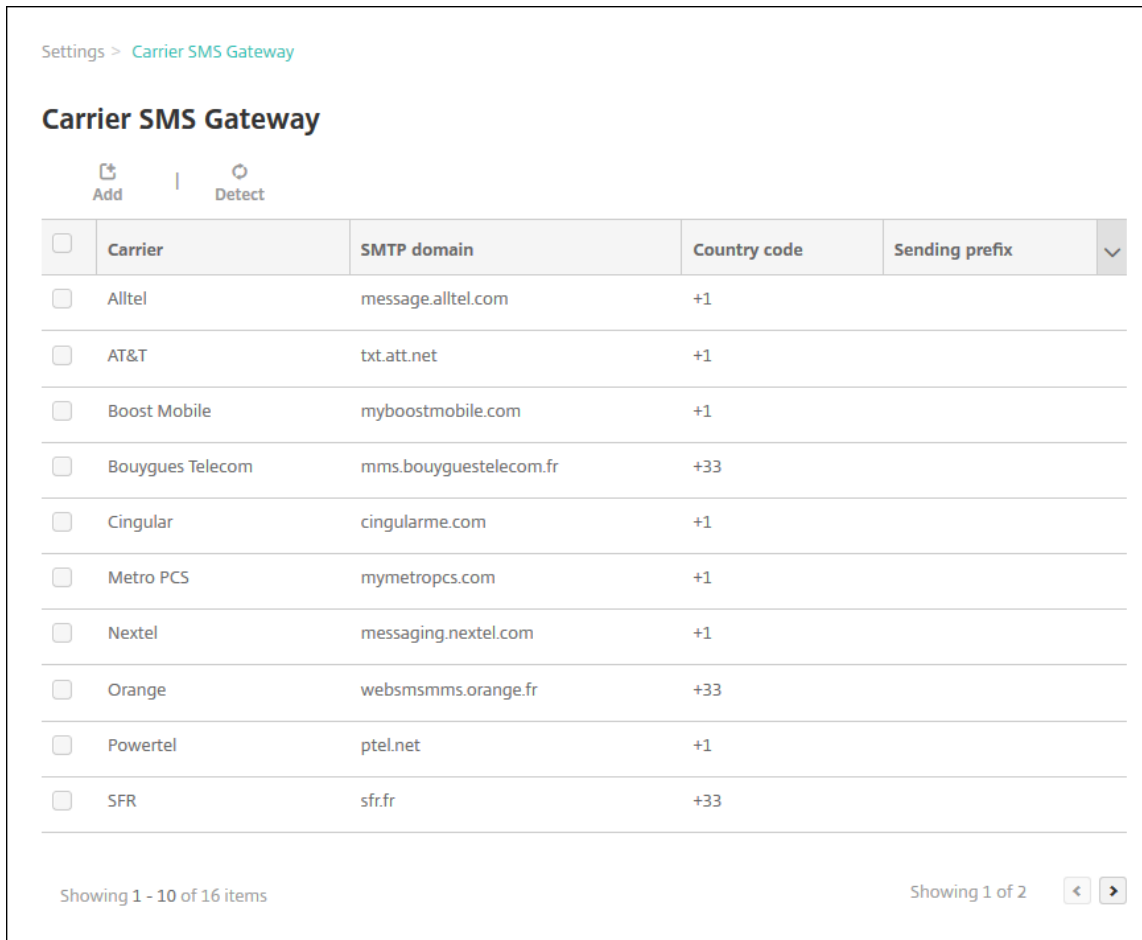
HTTPS 는 꺼짐으로 설정하라는 Citrix 지원의 지침이 없는 한 켜짐으로 설정하십시오.

- 국가 코드: 목록에서 조직의 받는 사람에 대한 기본 SMS 국가 코드 접두사를 클릭합니다. 이 필드는 항상 + 기호로 시작됩니다. 기본값은 아프가니스탄 **+93** 입니다.
2. 구성 테스트를 클릭하여 현재 구성으로 테스트 메시지를 보냅니다. 인증, 가상 전화 번호 오류 등과 같은 연결 오류는 즉시 감지되고 표시됩니다. 휴대폰 간에 전송된 메시지와 같은 시간 내에 메시지가 수신됩니다.
 3. 추가를 클릭합니다.

이동 통신 사업자 **SMS** 게이트웨이 추가

XenMobile 에서 이동 통신 사업자의 SMS 게이트웨이를 설정하여 이동 통신 사업자의 SMS 게이트웨이를 통해 전송되는 알림을 구성할 수 있습니다. 이동 통신 사업자는 SMS(Short Message Service) 게이트웨이를 사용하여 통신 네트워크에서 SMS 전송을 보내거나 받습니다. 이러한 텍스트 기반 메시지는 표준화된 통신 프로토콜을 사용하여 유선 전화 또는 휴대폰 장치에서 SMS 를 교환할 수 있도록 합니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 알림에서 이동 통신 사업자 **SMS** 게이트웨이를 클릭합니다. 이동 통신 사업자 **SMS** 게이트웨이 페이지가 열립니다.



3. 다음 중 하나를 수행합니다.

- 검색을 클릭하여 자동으로 게이트웨이를 검색합니다. 새로운 이동 통신 사업자가 검색되지 않았음을 나타내거나 등록된 장치 중에서 검색된 새 이동 통신 사업자를 나열하는 대화 상자가 나타납니다.
- 추가를 클릭합니다. 이동 통신 사업자 **SMS** 게이트웨이 추가 대화 상자가 나타납니다.

Add a Carrier SMS Gateway

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

Carrier*

Gateway SMTP domain*

Country code*

United States +1 ▼

Email sending prefix

Cancel

Add

메모:

XenMobile 은 Nexmo SMS 메시지만 지원합니다. Nexmo 메시지 사용을 위한 계정이 없는 경우 [웹 사이트](#)를 방문하여 계정을 만드십시오.

4. 다음 설정을 구성합니다.

- 이동 통신 사업자: 이동 통신 사업자의 이름을 입력합니다.
- 게이트웨이 **SMTP** 도메인: SMTP 게이트웨이에 연결된 도메인을 입력합니다.
- 국가 코드: 목록에서 이동 통신 사업자의 국가 코드를 클릭합니다.
- 전자 메일 전송 접두사: 필요한 경우 전자 메일 전송 접두사를 지정합니다.

5. 추가를 클릭하여 새 이동 통신 사업자를 추가하거나 취소를 클릭하여 새 이동 통신 사업자를 추가하지 않습니다.

알림 템플릿 만들기 및 업데이트

XenMobile 에서 자동화 동작, 등록 및 사용자에게 보내는 표준 알림 메시지에 사용할 알림 템플릿을 만들거나 업데이트할 수 있습니다. 세 가지 채널 (Secure Hub, SMTP 또는 SMS) 을 통해 메시지를 보내는 알림 템플릿을 구성합니다.

XenMobile 에는 시스템의 모든 장치에 자동으로 응답하는 서로 다른 이벤트 유형을 반영하는 다수의 미리 정의된 알림 템플릿이 있습니다.

메모:


SMTP 또는 SMS 채널을 사용하여 사용자에게 알림을 보내려는 경우 채널을 설정한 후 활성화해야 합니다. 채널이 설정되지 않은 경우 알림 템플릿을 추가할 때 채널을 설정하라는 메시지가 표시됩니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 알림 템플릿을 클릭합니다. 알림 템플릿 페이지가 나타납니다.

Settings > Notification Templates



Notification Templates

Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

 Add

<input type="checkbox"/>	Name	Channels	Type	Deletable	Manual sending supported	
<input type="checkbox"/>	ActiveSync Gateway Blocked	Worx Home	ActiveSync Gateway blocked device			
<input type="checkbox"/>	Android Download Link	SMTP, SMS	Android Download Link			
<input type="checkbox"/>	APNS cert expiration	SMTP	APNS Cert Expiration			
<input type="checkbox"/>	Certificate renewal	Worx Home	Certificate is renewed			
<input type="checkbox"/>	Enrollment	SMTP, SMS	Enrollment Notification			
<input type="checkbox"/>	Enrollment Confirmation	SMTP, SMS	Enrollment Confirmation			
<input type="checkbox"/>	Enrollment Invitation	SMTP, SMS	Enrollment Invitation			
<input type="checkbox"/>	Enrollment PIN	SMTP, SMS	Enrollment PIN			
<input type="checkbox"/>	Failed Samsung KNOX attestation	Worx Home	Failed Samsung KNOX attestation			✓
<input type="checkbox"/>	iOS Download Link	SMTP, SMS	iOS Download Link			

Showing 1 - 10 of 25 items

Showing 1 of 3  

알림 템플릿 추가

1. 추가를 클릭합니다. SMS 게이트웨이 또는 SMTP 서버가 설정되지 않은 경우 SMS 및 SMTP 알림의 사용에 관한 메시지가 표시됩니다. SMTP 서버 또는 SMS 게이트웨이를 지금 설정하거나 나중에 설정하도록 선택할 수 있습니다.

SMS 또는 SMTP 서버 설정을 지금 설정하도록 선택하는 경우 설정 페이지의 알림 서버 페이지로 리디렉션됩니다. 사용할 채널을 설정한 후 알림 템플릿 페이지로 돌아가서 알림 템플릿 추가 또는 수정을 계속할 수 있습니다.

중요:

SMS 또는 SMTP 서버 설정을 나중에 설정하도록 선택하는 경우 알림 템플릿을 추가하거나 편집할 때 이러한 채널을 활성화할 수 없으므로 사용자 알림을 보낼 때 이러한 채널을 사용할 수 없게 됩니다.

2. 다음 설정을 구성합니다.

- **이름:** 템플릿에 대한 설명적 이름을 입력합니다.
- **설명:** 템플릿에 대한 설명을 입력합니다.
- **유형:** 목록에서 알림 유형을 클릭합니다. 선택한 유형에 대해 지원되는 채널만 표시됩니다. 미리 정의된 템플릿인 APNS 인증서 만료 템플릿만 허용됩니다. 즉, 이 유형의 새 템플릿을 추가할 수 없습니다.

메모:

일부 템플릿 유형의 경우 유형 아래에 ‘수동 보내기 지원’이라는 구가 표시됩니다. 이 구는 대시보드 및 장치 페이지의 알림 목록에 있는 템플릿을 사용하여 사용자에게 수동으로 알림을 보낼 수 있음을 의미합니다. 모든 채널에서 제목 또는 메시지 필드에 다음 매크로를 사용하는 템플릿에는 수동 보내기를 사용할 수 없습니다.

- `${outofcompliance.reason(allowlist_blocklist_apps_name)}`
- `${outofcompliance.reason(smg_block)}`

3. 채널에서 이 알림에 사용할 각 채널에 대한 정보를 구성합니다. 일부 또는 모든 채널을 선택할 수 있습니다. 알림을 보내는 방법에 따라 다른 채널을 선택합니다.

- **Secure Hub** 를 선택하는 경우 iOS 및 Android 장치만 알림을 수신하며 장치의 알림 트레이에 표시됩니다.
- **SMTP** 를 선택하는 경우 전자 메일 주소를 등록한 대부분의 사용자가 메시지를 수신합니다.
- **SMS** 를 선택하는 경우 SIM 카드가 있는 장치를 사용하는 사용자만 알림을 수신합니다.

Secure Hub:

- **활성화:** 알림 채널을 사용하려면 클릭합니다.
- **메시지:** 사용자에게 보낼 메시지를 입력합니다. **Secure Hub** 를 사용하는 경우 필수 필드입니다. 메시지에서 매크로를 사용하는 방법에 대한 자세한 내용은 [매크로](#)를 참조하십시오.
- **사운드 파일:** 목록에서 알림이 수신될 때 울릴 알림 사운드를 클릭합니다.

SMTP:

- **활성화:** 알림 채널을 사용하려면 클릭합니다.

SMTP 서버를 설정한 후에만 SMTP 알림을 활성화할 수 있습니다.

- **보낸 사람:** 알림을 보낸 사람을 선택적으로 입력합니다. 이름, 전자 메일 주소 또는 둘 다를 입력할 수 있습니다.
- **받는 사람:** 이 필드에는 올바른 SMTP 받는 사람 주소로 알림이 전송되도록 임시 알림을 제외한 모든 알림에 대해 미리 작성된 매크로가 포함됩니다. 템플릿의 매크로는 수정하지 않는 것이 좋습니다. 세미콜론 (;) 으로 주소를 구분하여 사용자 외에 받는 사람을 추가할 수 있습니다 (예: 회사 관리자). 임시 알림을 보내려면 이 페이지에서 특정 받는 사람을 입력하거나 관리 > 장치 페이지에서 장치를 선택하고 거기에서 알림을 보낼 수 있습니다. 자세한 내용은 [장치](#)를 참조하십시오.

- **제목:** 알림에 대한 설명적인 제목을 입력합니다. 이것은 필수 필드입니다.
- **메시지:** 사용자에게 보낼 메시지를 입력합니다. 메시지에서 매크로를 사용하는 방법에 대한 자세한 내용은 [매크로](#)를 참조하십시오.

SMS:

- **활성화:** 알림 채널을 사용하려면 클릭합니다.
SMTP 서버를 설정한 후에만 SMTP 알림을 활성화할 수 있습니다.
 - **받는 사람:** 이 필드에는 올바른 SMS 받는 사람 주소로 알림이 전송되도록 임시 알림을 제외한 모든 알림에 대해 미리 작성된 매크로가 포함됩니다. 템플릿의 매크로는 수정하지 않는 것이 좋습니다. 임시 알림을 보내려면 특정 받는 사람을 입력하거나 관리 > 장치 페이지에서 장치를 선택할 수 있습니다.
 - **메시지:** 사용자에게 보낼 메시지를 입력합니다. 이것은 필수 필드입니다. 메시지에서 매크로를 사용하는 방법에 대한 자세한 내용은 [매크로](#)를 참조하십시오.
4. 추가를 클릭합니다. 모든 채널이 올바르게 구성되면 알림 템플릿 페이지에 SMTP, SMS 및 Secure Hub 순서로 표시됩니다. 올바르게 구성되지 않은 채널은 올바르게 구성된 채널 뒤에 표시됩니다.

알림 템플릿 편집

1. 알림 템플릿을 선택합니다. 해당 템플릿에 관련된 편집 페이지가 나타나고 거기에서 유형 필드를 제외한 모든 항목을 변경할 수 있으며 채널을 활성화하거나 비활성화할 수 있습니다.
2. 저장을 클릭합니다.

알림 템플릿 삭제

자신이 추가한 알림 템플릿만 삭제할 수 있습니다. 미리 정의된 알림 템플릿은 삭제할 수 없습니다.

1. 기존의 알림 템플릿을 선택합니다.
2. 삭제를 클릭합니다. 확인 대화 상자가 나타납니다.
3. 삭제를 클릭하여 알림 템플릿을 삭제하거나 취소를 클릭하여 알림 템플릿 삭제를 취소합니다.

장치

March 15, 2024

Citrix XenMobile 은 단일 관리 콘솔에서 다양한 유형의 장치를 프로비저닝, 관리, 보안 및 인벤토리를 수행할 수 있습니다.

XenMobile 서버 데이터베이스는 모바일 장치 목록을 저장합니다. 고유 일련 번호 또는 IMEI(International Mobile Station Equipment Identity)/MEID(Mobile Equipment Identifier)가 각 모바일 장치를 고유하게 정의합니다. XenMobile 콘솔에 장치를 채우려면 수동으로 장치를 추가하거나 파일에서 장치 목록을 가져올 수 있습니다. 장치 프로비저닝 파일 형식에 대한 자세한 내용은 이 문서 뒷부분에서 장치 프로비저닝 파일 형식을 참조하십시오.

XenMobile 콘솔의 장치 페이지에는 각 장치와 다음과 같은 정보가 나열됩니다.

- **상태:** 장치의 탈옥 상태, 관리되는 상태, Active Sync Gateway를 사용할 수 있는지 여부 및 배포 상태가 아이콘으로 나타납니다.
- **모드:** 장치 모드가 MDM 또는 MAM 인지, 아니면 둘 모두인지.
- **사용자 이름, 장치 플랫폼, 운영 체제 버전, 장치 모델, 마지막 액세스 및 비활성 일 수** 같은 장치에 대한 기타 정보. 이러한 머리글은 기본적으로 표시됩니다.

장치테이블을 사용자 지정하려면 마지막 머리글의 아래쪽 화살표를 클릭하십시오. 그런 다음 테이블에 표시할 추가 머리글을 선택하거나 제거할 머리글을 선택 취소합니다.

Last access	Inactivity days	▼
	<div> <div>✓ Status</div> <div>✓ Mode</div> <div>✓ User name</div> <div>Serial number</div> <div>IMEI/MEID</div> <div>ActiveSync ID</div> <div>WiFi MAC address</div> <div>Bluetooth MAC address</div> <div>✓ Device platform</div> <div>✓ Operating system version</div> <div>✓ Device model</div> <div>✓ Last access</div> <div>✓ Inactivity days</div> <div>Shareable</div> <div>Shared status</div> <div>DEP registered</div> </div>	

수동으로 장치를 추가하고, 장치 프로비저닝 파일에서 장치를 가져오고, 장치 세부 정보를 편집하고, 보안 작업을 수행하고, 장치에 알림을 보낼 수 있습니다. 모든 장치 테이블 데이터를.csv 파일로 내보내 사용자 지정 보고서를 만들 수도 있습니다. 서버는 모든 장치 특성을 내보냅니다. 필터를 적용한 경우.csv 파일을 만들 때 XenMobile이 필터를 사용합니다.

수동으로 장치 추가

1. XenMobile 콘솔에서 관리 > 장치를 클릭합니다. 장치 페이지가 나타납니다.

Status	Mode	User name	Device platform	Operating system version
	MDM MAM	[Redacted]	Android	5.0.2
	MDM MAM	[Redacted]	iOS	8.4.1

2. 추가를 클릭합니다. 장치 추가페이지가 나타납니다.

3. 다음 설정을 구성합니다.

- 플랫폼 선택: **iOS** 또는 **Android** 를 클릭합니다.
- 일련 번호: 장치 일련 번호를 입력합니다.
- **IMEI/MEID**: Android 장치에만 해당하며, 필요한 경우 장치 IMEI/MEID 정보를 입력합니다.

4. 추가를 클릭합니다. 장치 테이블이 나타나고 목록 맨 아래에 장치가 추가되어 있습니다. 추가한 장치를 선택한 다음 나타나는 메뉴에서 편집을 클릭하여 장치 세부 정보를 보고 확인합니다.

참고:

장치 옆에 있는 확인란을 선택하면 장치 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하면 목록의 오른쪽에 옵션 메뉴가 나타납니다.

- 엔터프라이즈 (XME) 또는 MDM 모드로 구성된 XenMobile Server
- 구성된 LDAP
- 로컬 그룹 및 로컬 사용자를 사용 중인 경우:
 - 하나 이상의 로컬 그룹.
 - 로컬 그룹에 할당된 로컬 사용자.
 - 배달 그룹은 로컬 그룹과 연결됩니다.
- Active Directory 를 사용 중인 경우:
 - 배달 그룹은 Active Directory 그룹과 연결됩니다.

5. 일반 페이지에는 일련 번호, ActiveSync ID 및 플랫폼 유형에 대한 기타 정보 같은 장치 식별자가 나열됩니다. 장치 소유권의 경우 회사 또는 **BYOD** 를 선택합니다.

일반 페이지에는 강력한 ID, 장치 잠금, 활성화와 잠금 바이패스 및 플랫폼 유형에 대한 기타 정보 같은 장치 보안 속성도 나열됩니다. 장치 전체 초기화 필드에는 사용자 PIN 코드가 포함됩니다. 장치가 초기화된 후 사용자는 이 코드를 입력해야 합니다. 사용자가 코드를 잊은 경우 여기서 코드를 조회할 수 있습니다.

6. 속성 페이지에는 XenMobile 이 프로비저닝할 장치 속성이 나열됩니다. 이 목록에는 장치를 추가하는 데 사용된 프로비저닝 파일에 포함된 모든 장치 속성이 표시됩니다. 속성을 추가하려면 추가를 클릭한 다음 목록에서 속성을 선택합니다. 각 속성에 유효한 값에 대해서는 [장치 속성 이름 및 값 PDF](#) 를 참조하십시오.

속성을 추가하면 처음에는 속성을 추가한 범주 아래에 나타납니다. 다음을 클릭한 후 속성 페이지로 돌아가면 속성이 해당 목록에 나타납니다.

속성을 삭제하려면 목록 위에 마우스 포인터를 이동하고 오른쪽에 있는 **X** 를 클릭합니다. 항목이 즉시 삭제됩니다.

7. 나머지 장치 세부 정보 섹션에는 장치에 대한 요약 정보가 포함되어 있습니다.

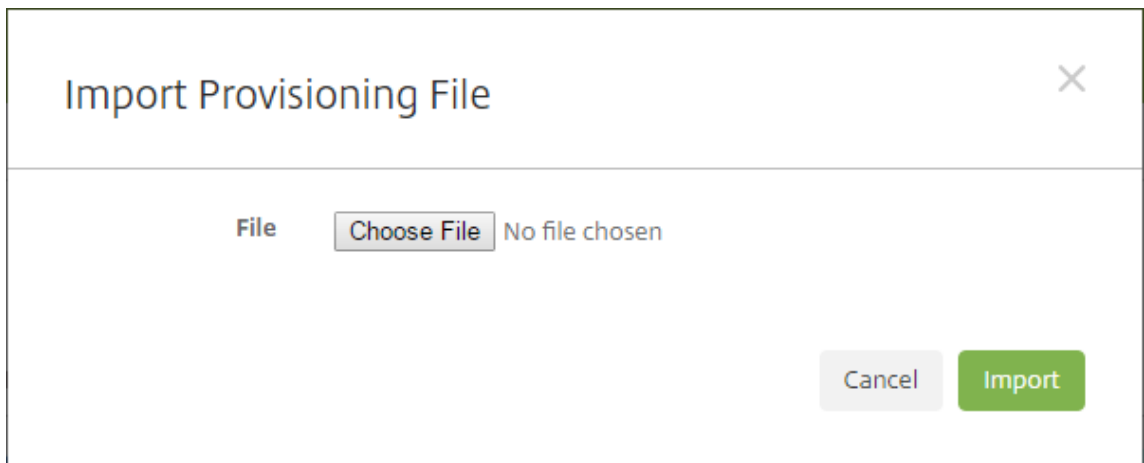
- 사용자 속성: RBAC 역할, 그룹 구성원 자격, 볼륨 구매 계정 및 사용자 속성을 표시합니다. 이 페이지에서 볼륨 구매 계정을 사용 중지할 수 있습니다.
- 할당된 정책: 배포된 정책, 보류 중인 정책 및 실패한 정책의 수를 포함하여 할당된 정책의 수를 표시합니다. 각 정책에 대해 정책 이름, 유형 및 마지막 배포 정보를 제공합니다.
- 앱: 마지막 인벤토리에 대한 설치된 앱 배포, 보류 중인 앱 배포 및 실패한 앱 배포의 수를 표시합니다. 앱 이름, 식별자, 유형 및 기타 정보를 제공합니다.
- 미디어: 마지막 인벤토리에 대해 배포된 미디어 배포, 보류 중인 미디어 배포 및 실패한 미디어 배포의 수를 표시합니다.
- 동작: 배포된 동작, 보류 중인 동작 및 실패한 동작의 수를 표시합니다. 마지막 배포의 동작 이름 및 시간을 제공합니다.

- **배달 그룹:** 성공한 배달 그룹, 보류 중인 배달 그룹 및 실패한 배달 그룹의 수를 표시합니다. 각 배포에 대해 배달 그룹 이름 및 배포 시간을 제공합니다. 배달 그룹을 선택하여 상태, 동작 및 채널 또는 사용자를 비롯한 자세한 정보를 확인합니다.
- **iOS 프로파일:** 이름, 유형, 조직 및 설명을 비롯한 마지막 iOS 프로파일 인벤토리를 표시합니다.
- **iOS 프로비전 프로파일:** UUID, 만료 날짜 및 관리 여부와 같은 엔터프라이즈 배포 프로비전 프로파일 정보를 표시합니다.
- **인증서:** 유효하거나, 만료되거나, 해지된 인증서에 대해 유형, 공급자, 발급자, 일련 번호 및 만료 전까지 남은 날짜와 같은 정보를 표시합니다.
- **연결:** 첫 번째 연결 상태 및 마지막 연결 상태를 표시합니다. 각 연결에 대해 사용자 이름, 마지막 두 번째 (끝에서 두 번째) 인증 시간 및 마지막 인증 시간을 제공합니다.
- **MDM 상태:** MDM 상태, 마지막 푸시 시간 및 마지막 장치 회신 시간 같은 정보를 표시합니다.

프로비저닝 파일에서 장치 가져오기

이동 통신 사업자 또는 장치 제조업체가 제공한 파일을 가져오거나 고유한 장치 프로비저닝 파일을 만들 수 있습니다. 자세한 내용은 이 문서 뒷부분에서 장치 프로비저닝 파일 형식을 참조하십시오.

1. 관리 > 장치로 이동하여 가져오기를 클릭합니다. 프로비저닝 파일 가져오기 대화 상자가 나타납니다.



2. 파일 선택을 클릭한 다음 가져오려는 파일을 찾습니다.
3. 가져오기를 클릭합니다. 장치 테이블에 가져온 파일이 나열됩니다.
4. 장치 정보를 편집하려면 장치를 선택한 다음 편집을 클릭합니다. 장치 세부 정보 페이지에 대한 자세한 내용은 수동으로 장치 추가를 참조하십시오.

장치에 알림 보내기

장치 페이지에서 장치에 알림을 보낼 수 있습니다. 알림에 대한 자세한 내용은 [알림](#)을 참조하십시오.

1. 관리 > 장치 페이지에서 알림을 보낼 하나 이상의 장치를 선택합니다.

- 알림을 클릭합니다. 알림 대화 상자가 나타납니다. 받는 사람 필드에 알림을 받을 모든 장치가 나열됩니다.

The image shows a 'Notification' dialog box with a close button (X) in the top right corner. The dialog is divided into several sections:

- Recipients:** A text field containing the value 'CMVVXKX06J6A'.
- Templates:** A dropdown menu currently showing 'Ad Hoc'.
- Channels:** Two checkboxes, 'SMTP' and 'SMS', both of which are checked.
- Message Composition:** A section with two tabs, 'SMTP' and 'SMS'. The 'SMTP' tab is active, showing three input fields: 'Sender', 'Subject', and 'Message'.
- Buttons:** At the bottom right, there are two buttons: 'Cancel' (light gray) and 'Notify' (green).

- 다음 설정을 구성합니다.

- **템플릿:** 목록에서 보내려는 알림을 유형을 클릭합니다. 임시 템플릿을 제외한 각 템플릿의 경우 제목 및 메시지 필드에 선택한 템플릿에 구성된 텍스트가 표시됩니다.
- **채널:** 메시지를 보내는 방법을 선택합니다. 기본값은 **SMTP** 및 **SMS**입니다. 각 채널의 메시지 형식을 확인하려면 탭을 클릭합니다.
- **보낸 사람:** 선택적 보낸 사람을 입력합니다.
- **제목:** 임시 메시지의 경우 제목을 입력합니다.
- **메시지:** 임시 메시지의 경우 메시지를 입력합니다.

- 알림을 클릭합니다.

장치 테이블 내보내기

1. 내보내기 파일에 나타날 항목에 따라 장치 테이블을 필터링합니다.
2. 장치 테이블 위에서 내보내기 단추를 클릭합니다. 필터링된 장치 테이블의 정보가 추출되어.csv 파일로 변환됩니다.
3. 메시지가 표시되면.csv 파일을 열거나 저장합니다.

사용자 장치에 수동으로 태그 지정

다음과 같은 방법으로 XenMobile 에서 장치에 수동으로 태그를 지정할 수 있습니다.

- 초대 기반 등록 프로세스 도중
- 자가 지원 포털 등록 프로세스 도중
- 장치 소유권을 장치 속성으로 추가

장치에 회사 소유 또는 직원 소유 태그를 지정하는 옵션도 있습니다. 자가 지원 포털을 사용하여 장치를 자가 등록할 때 장치에 회사 소유 또는 직원 소유 태그를 지정할 수 있습니다. 다음과 같이 장치에 수동으로 태그를 지정할 수도 있습니다.

1. XenMobile 콘솔의 장치 탭에서 장치에 속성을 추가합니다.
2. 이름이 소유자인 속성을 추가하고 회사 또는 **BYOD**(직원 소유) 중에서 선택합니다.

장치 프로비저닝 파일 형식

여러 모바일 운영자 또는 장치 제조업체에서 인증된 모바일 장치의 목록을 제공합니다. 이러한 목록을 사용하면 긴 모바일 장치 목록을 수동으로 입력할 필요가 없습니다. XenMobile 은 지원되는 세 가지 장치 유형 (Android, iOS 및 Windows) 모두에 공통되는 가져오기 파일 형식을 지원합니다.

수동으로 만들며 장치를 XenMobile 로 가져오기 위해 사용하는 프로비저닝 파일은 다음과 같은 형식이어야 합니다.

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2;
...propertyNameN;propertyValueN
```

다음 사항에 유의하십시오.

- 각 속성에 유효한 값에 대해서는 [장치 속성 이름 및 값](#) PDF 를 참조하십시오.
- UTF-8 문자 집합을 사용합니다.
- 프로비저닝 파일 내에서 필드를 구분하려면 세미콜론 (;) 을 사용합니다. 필드 자체에 세미콜론이 포함되는 경우 백슬래시 문자 (\) 로 이스케이프 처리합니다.

다음 속성을 예로 들겠습니다.

```
propertyV;test;1;2
```

이 경우 다음과 같이 이스케이프 처리합니다.

```
propertyV\;test\;1\;2
```

- 일련 번호는 iOS 장치 식별자이므로 iOS 장치에는 일련 번호가 필수입니다.
- 다른 장치 플랫폼의 경우 일련 번호 또는 IMEI 를 포함해야 합니다.
- **OperatingSystemFamily** 의 유효한 값은 **WINDOWS**, **ANDROID** 또는 **iOS** 입니다.

장치 프로비저닝 파일의 예:

```
1 `1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2 2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;
   propertyV$*&&ééétest
3 3050BF3F517301081610065510590393;35244201625379903;iOS;test;
4 4050BF3F517301081610065510590393;;iOS;test;
5 ;55244201625379903;ANDROID;test.testé;value;`
```

파일의 각 줄은 장치 하나를 기술합니다. 위 샘플에서 첫 번째 항목은 다음과 같은 의미입니다.

- SerialNumber: 1050BF3F517301081610065510590391
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

ActiveSync Gateway

March 15, 2024

ActiveSync 는 Microsoft 에서 개발한 모바일 데이터 동기화 프로토콜입니다. ActiveSync 는 핸드헬드 장치 및 데스크톱 (또는 랩톱) 컴퓨터와 데이터를 동기화합니다.

XenMobile 에서 ActiveSync Gateway 규칙을 구성할 수 있습니다. 이러한 규칙에 따라 장치에서 ActiveSync 데이터에 대한 액세스를 허용하거나 거부할 수 있습니다. 예를 들어 누락된 필수 앱 규칙을 활성화하면 XenMobile 은 필수 앱에 대해 앱 액세스 정책을 확인하고 필수 앱이 누락된 경우 ActiveSync 데이터에 대한 액세스를 거부합니다. 각 규칙에 대해 허용 또는 거부 중 하나를 선택할 수 있습니다. 기본 설정은 허용으로 설정되어 있습니다.

앱 액세스 장치 정책에 대한 자세한 내용은 [앱 액세스 장치 정책](#)을 참조하십시오.

XenMobile 은 다음 규칙을 지원합니다.

익명 장치: 장치가 익명 모드인지 확인합니다. 이 확인은 장치가 다시 연결할 때 XenMobile 이 사용자를 다시 인증할 수 없는 경우 사용할 수 있습니다.

Samsung KNOX 증명 실패: 장치가 Samsung KNOX 증명 서버의 쿼리에 실패했는지 확인합니다.

금지된 앱: 장치에 앱 액세스 정책에 정의된 금지된 앱이 있는지 확인합니다.

암시적 허용 및 거부: 이 동작이 ActiveSync Gateway 의 기본값입니다. 게이트웨이는 다른 필터 규칙 기준을 충족시키지 않는 모든 장치의 장치 목록을 만들고 해당 목록을 기반으로 연결을 허용하거나 거부합니다. 일치하는 규칙이 없으면 기본값은 암시적 허용입니다.

비활성 장치: 서버 속성의 장치 비활성 일 수 임계값 설정에 정의된 대로 장치가 비활성 상태인지 확인합니다.

누락된 필수 앱: 앱 액세스 정책에 정의된 대로, 장치에 필수 앱이 누락되었는지 확인합니다.

비추천 앱: 앱 액세스 정책에 정의된 대로, 장치에 비추천 앱이 있는지 확인합니다.

규정을 준수하지 않는 암호: 사용자 암호가 규정을 준수하는지 확인합니다. iOS 및 Android 장치에서 XenMobile 은 현재 장치에 있는 암호가 장치로 보낸 암호 정책을 준수하는지 여부를 확인할 수 있습니다. 예를 들어 iOS 에서는 XenMobile 이 암호 정책을 장치에 보내는 경우 60 분 내에 암호를 설정해야 합니다. 사용자가 암호를 설정하기 전에 암호가 규정을 준수하지 않을 수 있습니다.

규정 위반 장치: 규정 위반 장치 속성에 따라 장치가 규정을 위반하는지 여부를 확인합니다. 이 속성은 대개 자동화된 동작이나 XenMobile API 를 활용하는 제 3 자에 의해 변경됩니다.

해지된 상태: 장치 인증서가 해지되었는지 여부를 확인합니다. 해지된 장치는 다시 권한이 부여될 때까지 다시 등록할 수 없습니다.

루팅된 Android 및 탈옥 iOS 장치: Android 또는 iOS 장치가 탈옥되어 있는지 확인합니다.

관리되지 않는 장치: 장치가 여전히 XenMobile 제어 하에 관리되는 상태에 있는지 확인합니다. 예를 들어 MAM 로 등록된 장치나 등록되지 않은 장치는 관리되지 않습니다.

Android 도메인 사용자를 ActiveSync Gateway 로 보내기: XenMobile 이 Android 장치 정보를 ActiveSync Gateway 로 보내도록 하려면 예를 클릭합니다.

ActiveSync Gateway 설정을 구성하려면

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 **ActiveSync Gateway** 를 클릭합니다. **ActiveSync Gateway** 페이지가 나타납니다.

Settings > ActiveSync Gateway

ActiveSync Gateway

Allows or denies access to devices and users based on rules and properties.

All devices

Activate the following rule(s)

☐ Anonymous Devices

☐ Failed Samsung KNOX attestation

☐ Forbidden Apps

☐ Implicit Allow and Deny

☐ Inactive Devices

☐ Missing Required Apps

☐ Non-Suggested Apps

☐ Noncompliant Password

☐ Out of Compliance Devices

☐ Revoked Status

☐ Rooted Android and Jailbroken iOS Devices

☐ Unmanaged Devices

Send Android domain users to ActiveSync Gateway

YES

?

1. **Activate the following rules**(다음 규칙 활성화) 에서 활성화하려는 하나 이상의 규칙을 선택합니다.
2. **Android** 만의 **Android** 도메인 사용자를 **ActiveSync Gateway** 로 보내기에서 예를 클릭하여 XenMobile 이 Android 장치 정보를 ActiveSync Gateway 로 보내도록 합니다.
3. 저장을 클릭합니다.

장치 관리에서 **Android Enterprise** 로 마이그레이션

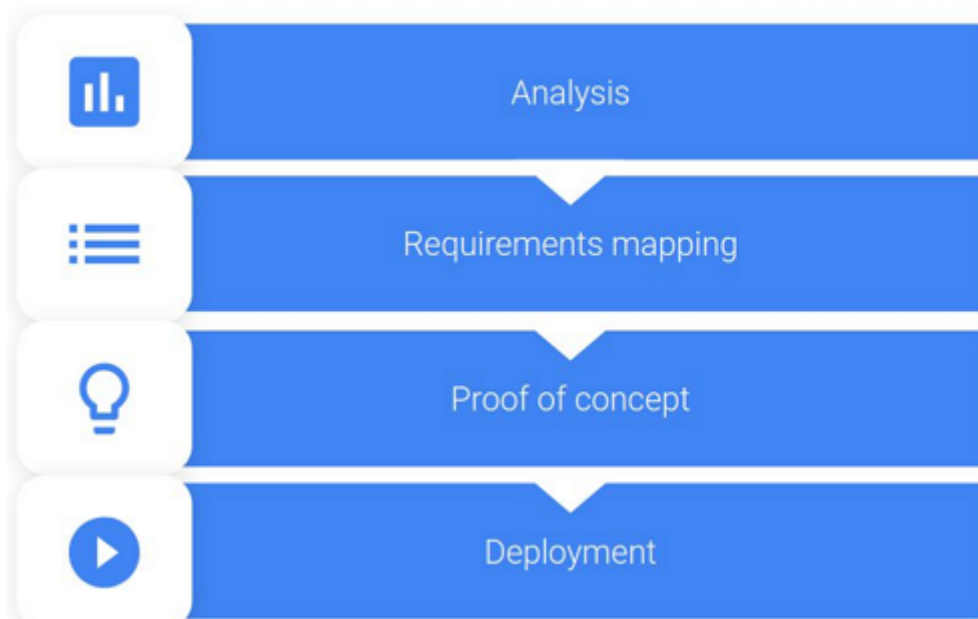
January 5, 2022

이 문서에서는 레거시 Android 장치 관리에서 Android Enterprise 로 마이그레이션할 때의 고려 사항 및 권장 사항에 대해 설명합니다. Google 은 Android 장치 관리 API 를 더 이상 사용하지 않습니다. 이 API 는 Android 장치에서 엔터프라이즈 앱을 지원했습니다. Android Enterprise 는 Google 과 Citrix 가 권장하는 최신 관리 솔루션입니다.

XenMobile 은 Android Enterprise 를 Android 장치에 대한 기본 등록 방법으로 변경하는 중입니다. Google 에서 이 API 의 사용을 중단한 후에는 장치 등록 모드에서 Android Q 장치에 대한 등록이 실패합니다.

Android Enterprise 에는 완전 관리되는 장치 및 작업 프로필 장치 모드에 대한 지원이 포함됩니다. Google 게시물 [Android Enterprise 마이그레이션 지침서](#)에 레거시 장치 관리와 Android Enterprise 의 차이점이 자세히 설명되어 있습니다. Google 에서 마이그레이션 정보를 읽어보시기 바랍니다.

또한 이 게시물은 장치 관리 마이그레이션의 4 단계에 대해 설명하며 다음 다이어그램을 포함하고 있습니다. 이 문서에는 마이그레이션 단계에서 XenMobile 과 관련된 권장 사항이 포함되어 있습니다.



[Android Enterprise 마이그레이션](#)

[지침서](#)의 다이어그램.

Google 의 허가 하에 다시 게시되었습니다.

장치 관리 사용 중단의 영향

Google 은 다음 장치 관리 API 의 사용을 중단할 예정입니다. Android Q API 수준을 대상으로 Secure Hub 를 업그레이드 한 후에는 Android Q 를 실행하는 장치에서 이러한 API 가 작동하지 않습니다.

- 카메라 사용 안 함: 장치 카메라에 대한 액세스를 제어합니다.
- 암호 만료: 구성 가능한 기간이 지난 후 사용자에게 암호를 변경하도록 강제합니다.
- 암호 제한: 제한적인 암호 요구 사항을 설정합니다.

API 사용 중단은 Citrix MAM 전용 모드에 등록된 장치에는 영향을 주지 않습니다.

권장 사항

다음은 Android 레거시 장치 관리 모드에 이미 등록된 장치, 등록되지 않은 장치 및 Citrix MAM 전용 모드에 등록된 장치에 대한 권장 사항입니다.

장치 등록 상태	권장 작업
기존 장치가 장치 관리 모드에 등록되었으며 Android Q 로 업그레이드할 수 있습니다.	장치를 Android Q 로 업그레이드하기 전에 장치 관리 모드에서 Android Enterprise 로 마이그레이션하십시오.
기존 장치가 장치 관리 모드로 등록되어 있습니다. 장치를 Android Q 로 업그레이드할 수 없습니다.	장치를 장치 관리 모드로 유지할 수 있습니다. 그러나 장치 새로 고침 시 Android Enterprise 로 장치를 이동할 계획을 세우십시오.
기존 장치가 장치 관리 모드에 등록되었으며 Android Q 로 업그레이드되었습니다.	Google 이 API 의 사용을 중단하기 전에 장치 관리 모드에서 Android Enterprise 로 마이그레이션하십시오. XenMobile 콘솔에 이러한 장치에 대한 경고 메시지가 나타납니다.
새로운 장치가 Android Q 와 함께 제공되었고 장치 관리 모드에 등록되었습니다.	Google 이 API 의 사용을 중단하기 전에 장치 관리 모드에서 Android Enterprise 로 마이그레이션하십시오. XenMobile 콘솔에 이러한 장치에 대한 경고 메시지가 나타납니다.
Android Q 와 함께 제공되거나 업그레이드할 수 있는 새 장치입니다. 장치는 등록되지 않았습니다.	모든 새로운 장치에 대해 Android Enterprise 를 사용하십시오.
Android Q 의 새 장치 또는 기존 장치는 Google 이 API 의 사용을 중단한 후 장치 관리 모드에 등록됩니다.	Google API 사용 중단에 영향을 방지하려면 Google 에서 API 사용을 중단하기 전에 Android Enterprise 로 마이그레이션하는 것이 좋습니다. 이 날짜 이후에는 이러한 장치의 등록이 실패합니다.
Citrix MAM 전용 모드에 등록된 새 장치 또는 기존 장치	따로 수행해야 할 작업은 없습니다. Google API 사용 중단은 MAM 전용 모드의 장치에는 영향을 주지 않습니다.

분석

마이그레이션의 분석 단계는 다음으로 구성됩니다.

- 레거시 Android 설정 파악
- 레거시 기능을 Android Enterprise 기능에 매핑할 수 있도록 레거시 설정 문서화

권장되는 분석

1. XenMobile 에서 Android Enterprise 평가: 완전 관리되는 장치, 작업 프로파일로 완전 관리되는 장치, 더 이상 사용되지 않는 장치, 작업 프로파일 (BYOD).
2. Android Enterprise 를 기준으로 현재 장치 관리 기능을 분석합니다.
3. 장치 관리 사용 사례를 문서화합니다.

장치 관리 사용 사례를 문서화하려면:

1. 스프레드시트를 만들고 XenMobile 콘솔에서 현재 정책 그룹을 나열합니다.
2. 기존 정책 그룹을 기반으로 별도의 사용 사례를 생성합니다.
3. 각 사용 사례에 대해 다음을 문서화합니다.

- 이름
- 비즈니스 소유자
- 사용자 ID 모델
- 장치 요구 사항
 - 보안
 - 관리
 - 유용성
- 장치 인벤토리
 - 제조사 및 모델
 - OS 버전
- 앱

4. 각 앱에 대해 다음을 나열합니다.

- 앱 이름
- 패키지 이름
- 호스팅 방법
- 앱이 공개 또는 비공개인지 여부
- 앱이 필수인지 여부 (true/false)

요구 사항 매핑

완료된 분석을 바탕으로 Android Enterprise 기능 요구 사항을 결정합니다.

권장되는 요구 사항 매핑

1. 관리 모드 및 등록 방법을 결정합니다.

- 작업 프로필 (BYOD): 재등록이 필요합니다. 공장 기본값으로 재설정할 필요가 없습니다.
 - 완전 관리형: 공장 기본값으로 재설정해야 합니다. QR 코드, NFC(근거리 통신) 범프, DPC(장치 정책 컨트롤러) 식별자, 제로 터치를 사용하여 장치를 등록합니다.
2. 앱 마이그레이션 전략을 만듭니다.
 3. 사용 사례 요구 사항을 Android Enterprise 기능에 매핑합니다. 요구 사항 및 해당 Android 버전과 가장 일치하는 각 장치 요구 사항에 대한 기능을 문서화합니다.
 4. 기능 요구 사항에 따라 최소 Android OS(7.0, 8.0, 9.0)를 결정합니다.
 5. ID 모델을 선택합니다.
 - 권장: 관리되는 Google Play 계정
 - Google Cloud Identity 고객인 경우에만 Google G-Suite 계정 사용
 6. 장치 전략 만들기:
 - 작업 없음: 장치가 최소 OS 수준을 충족하는 경우
 - 업그레이드: 장치가 지원되고 지원되는 OS로 업데이트할 수 있는 경우
 - 교체: 장치를 지원되는 OS 수준으로 업데이트할 수 없는 경우

권장되는 앱 마이그레이션 전략

요구 사항 매핑을 완료한 후 Android 플랫폼에서 Android Enterprise 플랫폼으로 앱을 이동합니다. 앱 게시에 대한 자세한 내용은 [앱 추가](#)를 참조하십시오.

- 공용 스토어 앱
 1. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 Google Play 설정을 지우고 **Android Enterprise**를 플랫폼으로 선택합니다.
 2. 배달 그룹을 선택합니다. 앱이 필수인 경우 앱을 배달 그룹의 필수 앱 목록으로 이동합니다.

앱을 저장하면 Google Play Store에 나타납니다. 작업 프로필이 있는 경우 Google Play Store의 작업 프로필에 앱이 표시됩니다.
- 비공개 (엔터프라이즈) 앱

비공개 앱은 사내에서 개발하거나 타사 개발자가 개발합니다. Google Play를 사용하여 비공개 앱을 게시하는 것이 좋습니다.

 1. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 **Android Enterprise**를 플랫폼으로 선택합니다.
 2. APK 파일을 업로드한 다음 앱 설정을 구성합니다.
 3. 앱을 필수 배달 그룹에 게시합니다.

- MDX 앱

1. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 **Android Enterprise** 를 플랫폼으로 선택합니다.
2. MDX 파일을 업로드합니다. 앱 승인 프로세스를 진행합니다.
3. MDX 정책을 선택합니다.

Enterprise MDX 앱의 경우 MDX SDK 모드 래핑된 앱으로 변경하는 것이 좋습니다.

- 옵션 1: 조직에 비공개로 할당된 개발자 계정을 사용하여 Google Play 에서 APK 를 호스팅합니다. MDX 파일을 XenMobile 에 게시합니다.
- 옵션 2: XenMobile 에서 엔터프라이즈 앱으로 앱을 게시합니다. XenMobile 에서 APK 를 게시하고 MDX 파일에 대해 **Android Enterprise** 플랫폼을 선택합니다.

Citrix 장치 정책 마이그레이션

Android 및 Android Enterprise 플랫폼 모두에 사용할 수 있는 정책의 경우: 정책을 편집하고 **Android Enterprise** 플랫폼을 선택합니다.

Android Enterprise 의 경우 등록 모드를 고려하십시오. 일부 정책 옵션은 작업 프로필 모드 또는 완전 관리되는 모드의 장치에만 사용할 수 있습니다.

개념 증명

앱을 Android Enterprise 로 마이그레이션한 후 마이그레이션 테스트를 설정하여 기능이 의도한 대로 작동하는지 확인할 수 있습니다.

권장되는 개념 증명 설정

1. 배포 인프라 설정:
 - Android Enterprise 테스트를 위한 배포 그룹을 만듭니다.
 - XenMobile 에서 Android Enterprise 를 구성합니다.
2. 사용자 앱을 설정합니다.
3. Android Enterprise 기능을 구성합니다.
4. Android Enterprise 배포 그룹에 정책을 할당합니다.
5. 기능을 테스트하고 확인합니다.
6. 각 사용 사례에 대해 장치 설정 연습을 완료합니다.
7. 사용자 설정 단계를 문서화합니다.

배포

이제 Android Enterprise 설정을 배포하고 사용자 마이그레이션을 준비할 수 있습니다.

권장되는 배포 전략

Citrix 에서 권장하는 배포 전략은 Android Enterprise 의 모든 프로덕션 시스템을 테스트한 다음 나중에 장치 마이그레이션을 완료하는 것입니다.

- 이 시나리오에서 사용자는 현재 구성으로 계속해서 레거시 장치를 사용합니다. 관리자는 Android Enterprise 관리를 위한 새 장치를 설정합니다.
- 기존 장치는 업그레이드 또는 교체가 필요한 경우에만 마이그레이션합니다.
- 일반적인 수명 주기가 끝나면 기존 장치를 Android Enterprise 관리로 마이그레이션합니다. 또는 손실이나 파손으로 인해 교체가 필요한 경우 이러한 장치를 마이그레이션할 수 있습니다.

Android Enterprise

March 15, 2024

Android Enterprise 는 Google 이 Android 장치를 위한 엔터프라이즈 관리 솔루션으로 제공하는 도구 및 서비스 집합입니다. Android Enterprise 에서:

- XenMobile 을 사용하여 회사 소유의 Android 장치와 BYOD(bring your own device) Android 장치를 관리합니다.
- 전체 장치를 관리하거나 장치의 개별 프로필을 관리할 수 있습니다. 개별 프로필은 개인 계정, 앱 및 데이터로부터 비즈니스 계정, 앱 및 데이터를 분리합니다.
- 또한 인벤토리 관리와 같은 일회성 전용 장치를 관리할 수도 있습니다. Google 의 Android Enterprise 기능에 대한 개요는 [Android Enterprise 관리](#)를 참조하십시오.

리소스:

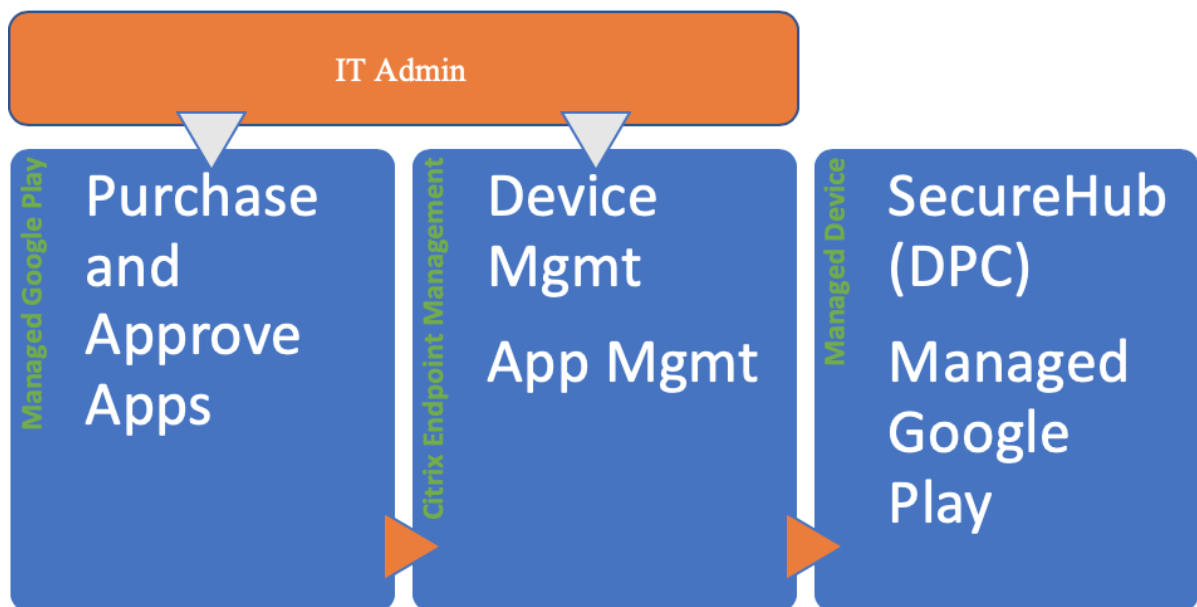
- Android Enterprise 와 관련된 용어 및 정의 목록은 Google Android Enterprise 개발자 가이드에서 [Android Enterprise 용어](#)를 참조하십시오. Google 은 이러한 용어를 자주 업데이트합니다.
- XenMobile 에 대해 지원되는 Android 운영 체제는 [지원되는 기기 운영 체제](#)를 참조하십시오.
- Android Enterprise 를 위한 네트워크 환경을 설정할 때 고려해야 할 아웃바운드 연결에 대한 자세한 내용은 Google 지원 문서 [Android Enterprise 네트워크 요구사항](#)을 참조하십시오.

XenMobile 을 관리되는 Google Play 와 통합하여 Android Enterprise 를 사용하는 경우 엔터프라이즈를 만들게 됩니다. Google 에서의 엔터프라이즈를 조직과 EMM(엔터프라이즈 모바일 관리) 솔루션 간의 바인딩으로 정의합니다. 조직에서 솔루션을 통해 관리하는 모든 사용자 및 장치는 해당 엔터프라이즈에 속합니다.

Android Enterprise 의 엔터프라이즈에는 EMM 솔루션, DPC(장치 정책 컨트롤러) 앱 및 Google 엔터프라이즈 앱 플랫폼의 세 가지 구성 요소가 있습니다. XenMobile 을 Android Enterprise 와 통합하는 경우 전체 솔루션에는 다음과 같은 구성 요소가 포함됩니다.

- **XenMobile:** Citrix EMM 입니다. XenMobile 은 안전한 디지털 작업 공간을 위한 통합 XenMobile 솔루션입니다. XenMobile 은 IT 관리자가 조직의 장치 및 앱을 관리할 수 있는 수단을 제공합니다.
- **Citrix Secure Hub:** Citrix DPC 앱입니다. Secure Hub 는 XenMobile 의 실행 패드입니다. Secure Hub 는 장치에서 정책을 적용합니다.
- 관리되는 **Google Play:** XenMobile 과 통합되는 Google 엔터프라이즈 앱 플랫폼입니다. Google Play EMM API 는 앱 정책을 설정하고 앱을 배포합니다.

다음 그림은 관리자가 이러한 구성 요소와 상호 작용하는 방식과 구성 요소가 서로 상호 작용하는 방식을 보여줍니다.



XenMobile 에서 관리되는 Google Play 사용

참고:

관리형 Google Play 또는 Google Workspace 를 사용하여 Citrix 를 EMM 공급자로 등록할 수 있습니다. 이 문서에서는 관리되는 Google Play 와 함께 Android Enterprise 를 사용하는 방법에 대해 설명합니다. 조직에서 Google Workspace 를 사용하여 앱에 대한 액세스를 제공하는 경우 Android Enterprise 를 함께 사용할 수 있습니다. [Google Workspace](#) 고객을 위한 레거시 Android Enterprise(이전 명칭 G Suite)를 참조하십시오.

관리되는 Google Play 를 사용하는 경우 장치와 최종 사용자에게 관리형 Google Play 계정을 프로비전합니다. 관리되는

Google Play 계정을 통해 사용자가 관리되는 Google Play 에 액세스하여 제공되는 앱을 설치하고 사용할 수 있습니다. 조직에서 타사 ID 서비스를 사용하는 경우 관리형 Google Play 계정을 기존 ID 계정과 연결할 수 있습니다.

이 유형의 엔터프라이즈는 도메인에 연결되지 않으므로 단일 조직에 대해 둘 이상의 엔터프라이즈를 만들 수 있습니다. 예를 들어 조직 내의 각 부서 또는 리전을 서로 다른 엔터프라이즈로 등록하여 별도의 장치 및 앱 집합을 관리할 수 있습니다.

관리되는 Google Play 는 XenMobile 관리자에게 Google Play 의 사용자 환경 및 앱 스토어 기능과 함께 기업을 위해 설계된 관리 기능을 제공합니다. 관리형 Google Play 를 사용하여 장치의 Android Enterprise 작업 공간에 배포할 앱을 추가, 구매 및 승인합니다. Google Play 를 사용하여 공용 앱, 개인 앱 및 타사 앱을 배포할 수 있습니다.

관리되는 장치의 사용자에게 있어서 관리되는 Google Play 는 엔터프라이즈 앱 스토어입니다. 사용자는 앱을 탐색하고, 앱 세부 정보를 보고, 앱을 설치할 수 있습니다. 공개 버전의 Google Play 와 달리 관리형 Google Play 에서는 사용자에게 별도로 제공되는 앱만 설치할 수 있습니다.

장치 배포 시나리오 및 작동 모드

장치 배포 시나리오는 배포한 장치의 소유자와 장치의 관리 방법을 나타냅니다. 장치 프로파일은 DPC 가 장치에서 정책을 관리하고 실행하는 방식을 나타냅니다.

작업 프로파일은 개인 계정, 앱 및 데이터로부터 비즈니스 계정, 앱 및 데이터를 분리합니다. 작업 프로파일에 대한 자세한 내용은 Google Android Enterprise 도움말 항목 [작업 프로파일이란 무엇인가요](#)를 참조하십시오.

중요:

Android 11 으로 Android Enterprise 장치를 업데이트할 경우 Google 은 “작업 프로파일로 완전히 관리” 로 관리되는 장치를 보안이 강화된 신규 작업 프로파일 환경으로 마이그레이션합니다. 자세한 내용은 [Android Enterprise 의 작업 프로파일로 완전히 관리에 예정된 변경 사항](#)을 참조하십시오.

장치 관리	사용 사례	작업 프로파일	개인 프로파일	참고
기업 소유 장치 (완전 관리형)	작업 전용인 기업 소유 장치	아니요	예. DPC 는 장치 전체 연결 구성, 글로벌 설정 구성 및 공장 기본값으로 재설정과 같은 장치 전체 작업을 수행할 수 있습니다.	신규 또는 공장 기본값 재설정 장치 전용입니다.

장치 관리	사용 사례	작업 프로필	개인 프로필	참고
작업 프로필로 완전히 관리	작업 및 개인용 기업 소유 장치	예	예. 이러한 장치에서는 DPC의 복사본 2 개가 실행됩니다. 하나는 장치 소유자 모드에서 장치를 관리하고 다른 하나는 프로필 소유자 모드에서 작업 프로필을 관리합니다. 장치와 작업 프로필에 개별 정책을 적용할 수 있습니다.	이전에는 COPE(회사 소유의 개인 사용) 장치라고 했습니다.
전용 장치 *	디지털 사이니지 또는 티켓 인쇄와 같이 단일 사용 사례를 위해 구성된 회사 소유 장치	아니요	예. 필수 앱만 제공하고 사용자가 다른 앱을 추가하지 못하도록 합니다.	이전에는 COSU(회사 소유 일회 사용) 장치라고 했습니다.
BYOD 작업 프로필 **	작업 프로필 모드로 등록된 개인 장치 (이전에는 프로필 소유자 모드로도 함)	예	예. DPC는 전체 장치가 아닌 작업 프로필만 관리합니다.	이러한 장치가 새 장치이거나 공장 기본값으로 재설정될 필요는 없습니다.

* 사용자는 전용 장치를 공유할 수 있습니다. 사용자가 전용 장치에서 앱에 로그인하면 작업 상태는 장치가 아닌 앱에 대한 상태가 됩니다.

** XenMobile은 BYOD 작업 프로필 모드에서와 같이 Zebra 장치를 지원하지 않습니다. XenMobile은 Zebra 장치를 완전 관리형 장치 및 장치 레거시 모드 (장치 관리 모드로도 함) 로 지원합니다.

레거시 모드에서 장치 소유자 또는 프로필 소유자 모드로 마이그레이션하는 방법에 대한 자세한 내용은 [기기 관리에서 Android Enterprise](#) 로 마이그레이션을 참조하십시오.

인증 방법

등록 프로필은 사용자가 MDM 을 취소할 수 있는 옵션과 함께 Android 장치가 MAM, MDM 또는 MDM+MAM 으로 등록되는지 여부를 결정합니다.

보안 수준 및 필요한 등록 단계에 대한 정보는 [등록 보안 모드 구성](#)을 참조하십시오.

XenMobile은 MDM+MAM 으로 등록된 Android 장치에 대해 다음과 같은 인증 방법을 지원합니다. 자세한 내용은 [인증서 및 인증](#)에 있는 문서를 참조하십시오.

- 도메인
- 도메인 및 보안 토큰

- 클라이언트 인증서
- 클라이언트 인증서와 도메인
- ID 공급자:
 - Azure Active Directory
 - Citrix ID 공급자

거의 사용되지 않는 또 다른 인증 방법은 클라이언트 인증서와 보안 토큰입니다. 자세한 내용은 <https://support.citrix.com/article/CTX215200>에서 참조하십시오.

요구 사항

Android Enterprise 사용을 시작하기 전에 다음이 필요합니다.

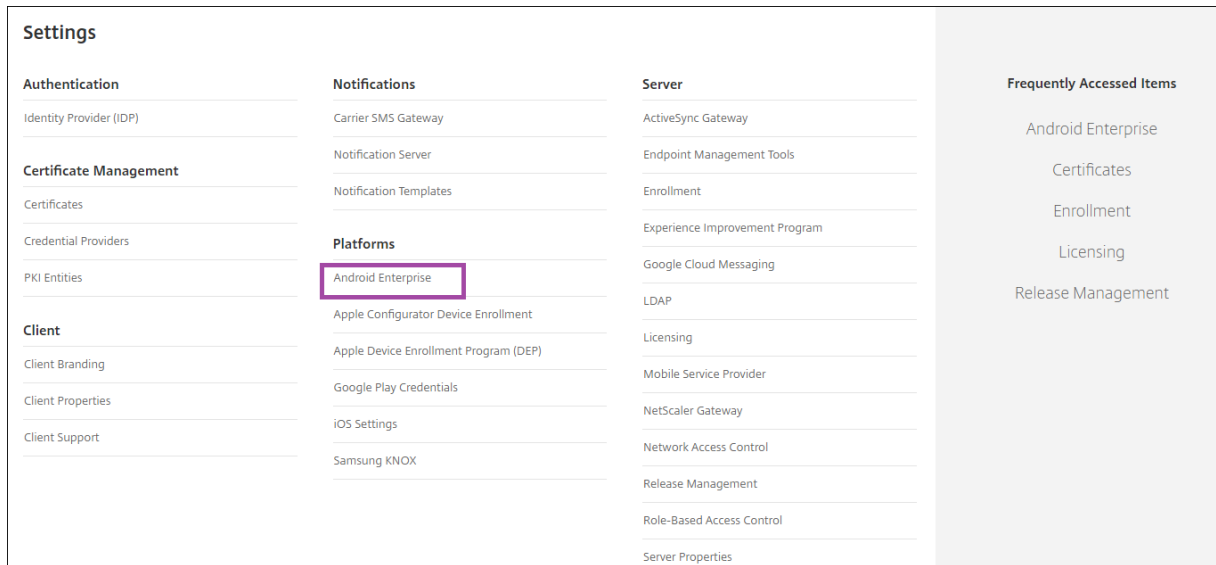
- 계정 및 자격 증명:
 - 관리되는 Google Play 로 Android Enterprise 를 설정하려면 회사의 Google 계정
 - 최신 MDX 파일을 다운로드하려면 Citrix 고객 계정
 - 개인 앱을 배포하려면 (선택 사항) Google 개발자 계정
- XenMobile 에 대해 구성된 Firebase Cloud Messaging(FCM) 지침은 [Firebase Cloud Messaging](#)을 참조하십시오.
- Samsung Knox 모바일 등록 (선택 사항) 의 경우 Knox 프리미엄 라이선스

Google Play 에 XenMobile 연결

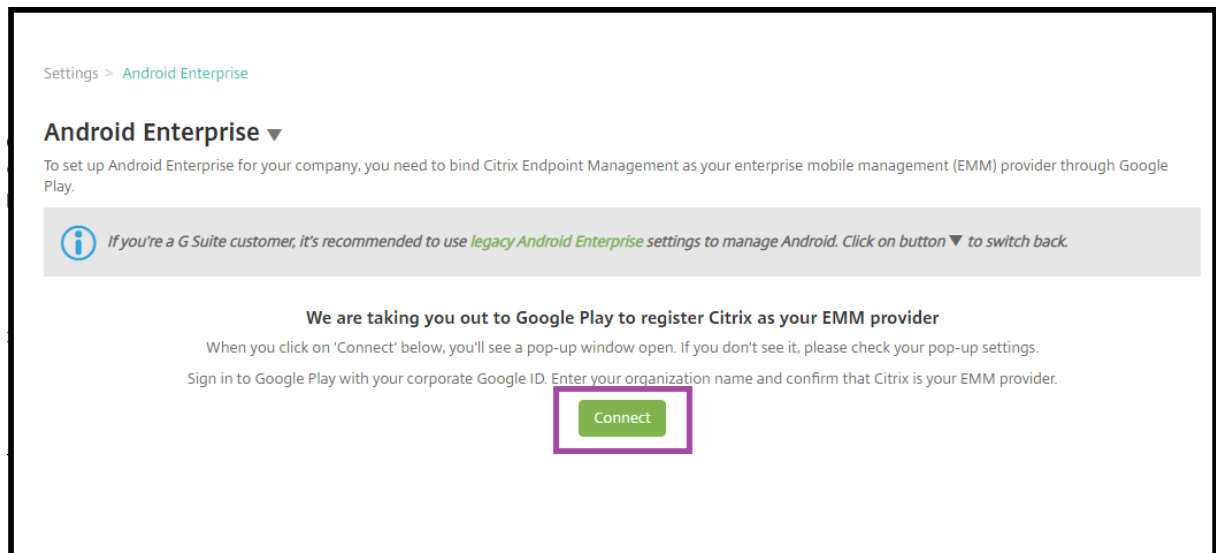
조직에 대한 Android Enterprise 를 설정하려면 관리되는 Google Play 를 통해 Citrix 를 EMM 공급자로 등록합니다. 이 설정은 관리되는 Google Play 를 XenMobile 에 연결하고 XenMobile 에 Android Enterprise 의 엔터프라이즈를 만듭니다.

Google Play 에 로그인하려면 회사 Google 계정이 필요합니다.

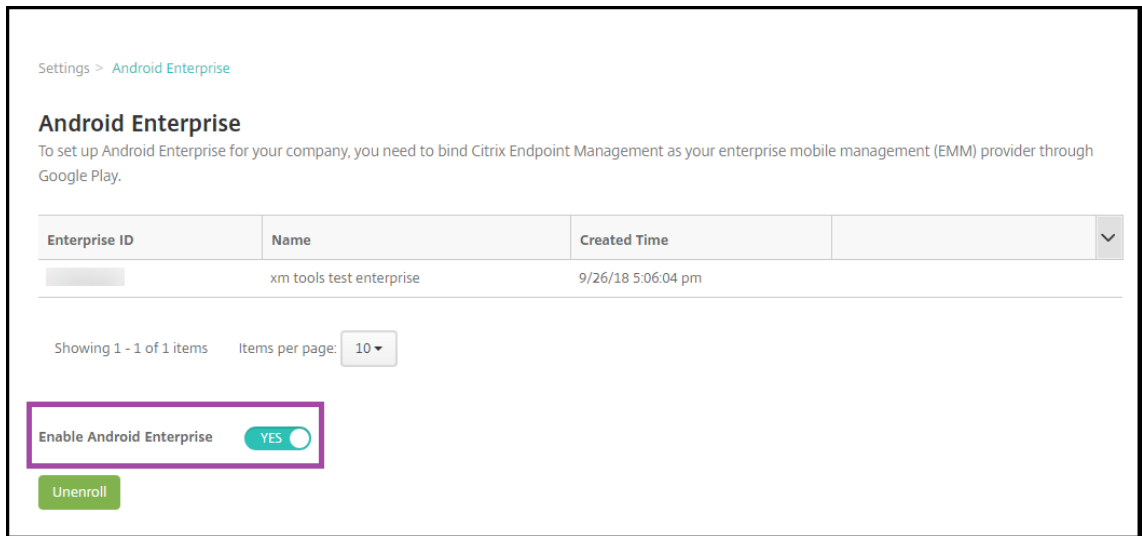
1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 설정 > **Android Enterprise** 로 이동합니다.



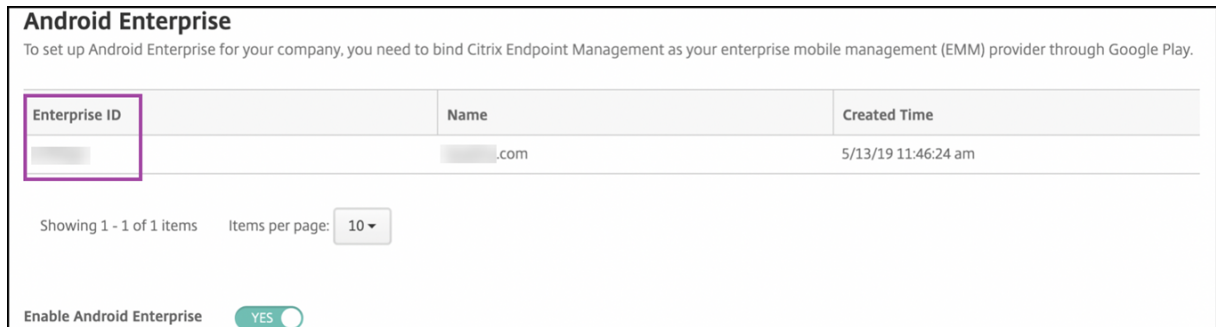
1. 연결을 클릭합니다. Google Play 가 열립니다.



1. 회사 Google 계정 자격 증명을 사용하여 Google Play 에 로그인합니다. 조직 이름을 입력하고 Citrix 가 EMM 공급자인지 확인합니다.
2. Android Enterprise 에 대한 엔터프라이즈 ID 가 추가되었습니다. Android Enterprise 를 사용하려면 **Android Enterprise** 사용을 예로 합니다.



엔터프라이즈 ID 가 XenMobile 콘솔에 나타납니다.



환경이 Google 에 연결되었고 장치를 관리할 준비가 되었습니다. 이제 사용자를 위한 앱을 제공할 수 있습니다.

XenMobile 을 사용하여 사용자에게 Citrix 모바일 생산성 앱, MDX 앱, 공용 앱 스토어 앱, 웹 및 SaaS 앱, 엔터프라이즈 앱 및 웹 링크를 제공할 수 있습니다. 이러한 유형의 앱 및 사용자에게 제공하는 방법에 대한 자세한 내용은 [앱 추가](#)를 참조하십시오.

다음 섹션에서는 모바일 생산성 앱을 제공하는 방법을 보여줍니다.

Android Enterprise 사용자에게 Citrix 모바일 생산성 앱 제공

Android Enterprise 사용자에게 Citrix 모바일 생산성 앱을 제공하려면 다음 단계가 필요합니다.

1. 앱을 MDX 앱으로 게시합니다. 앱을 MDX 앱으로 구성을 참조하십시오.
2. 사용자가 장치의 작업 프로필에 액세스할 때 사용할 보안 챌린지에 대한 규칙을 구성합니다. 보안 챌린지 정책 구성을 참조하십시오.

게시한 앱은 Android Enterprise 엔터프라이즈에 등록된 장치에 제공됩니다.

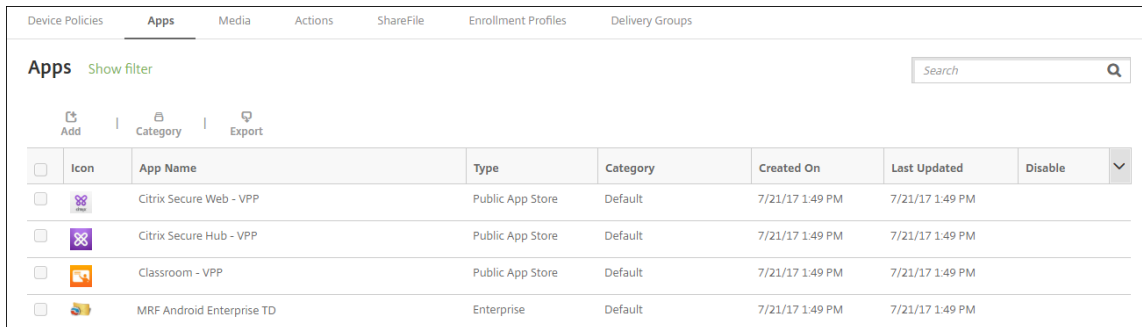
참고:

Android Enterprise 공용 앱 스토어 앱을 Android 사용자에게 배포할 경우 해당 사용자는 Android Enterprise에 자동으로 등록됩니다.

앱을 MDX 앱으로 구성

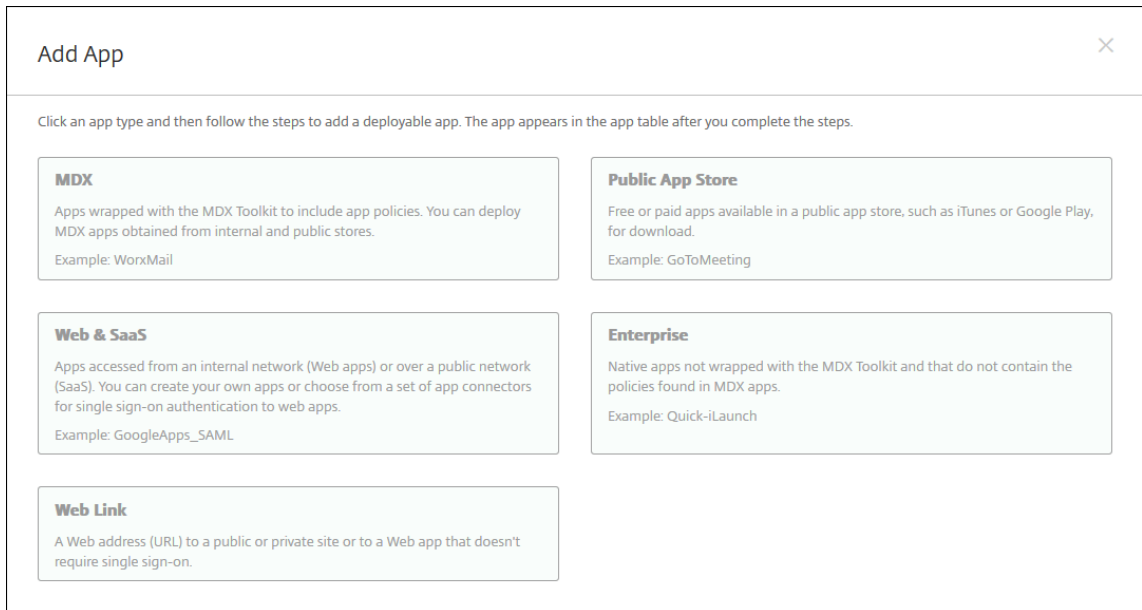
Citrix 생산성 앱을 Android Enterprise 용 MDX 앱으로 구성하려면:

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 나타납니다.



Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
	Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
	Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
	MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	

2. 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

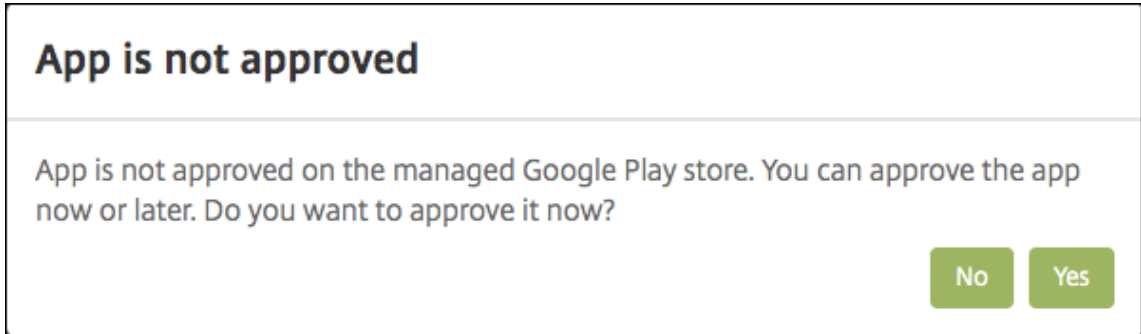
Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

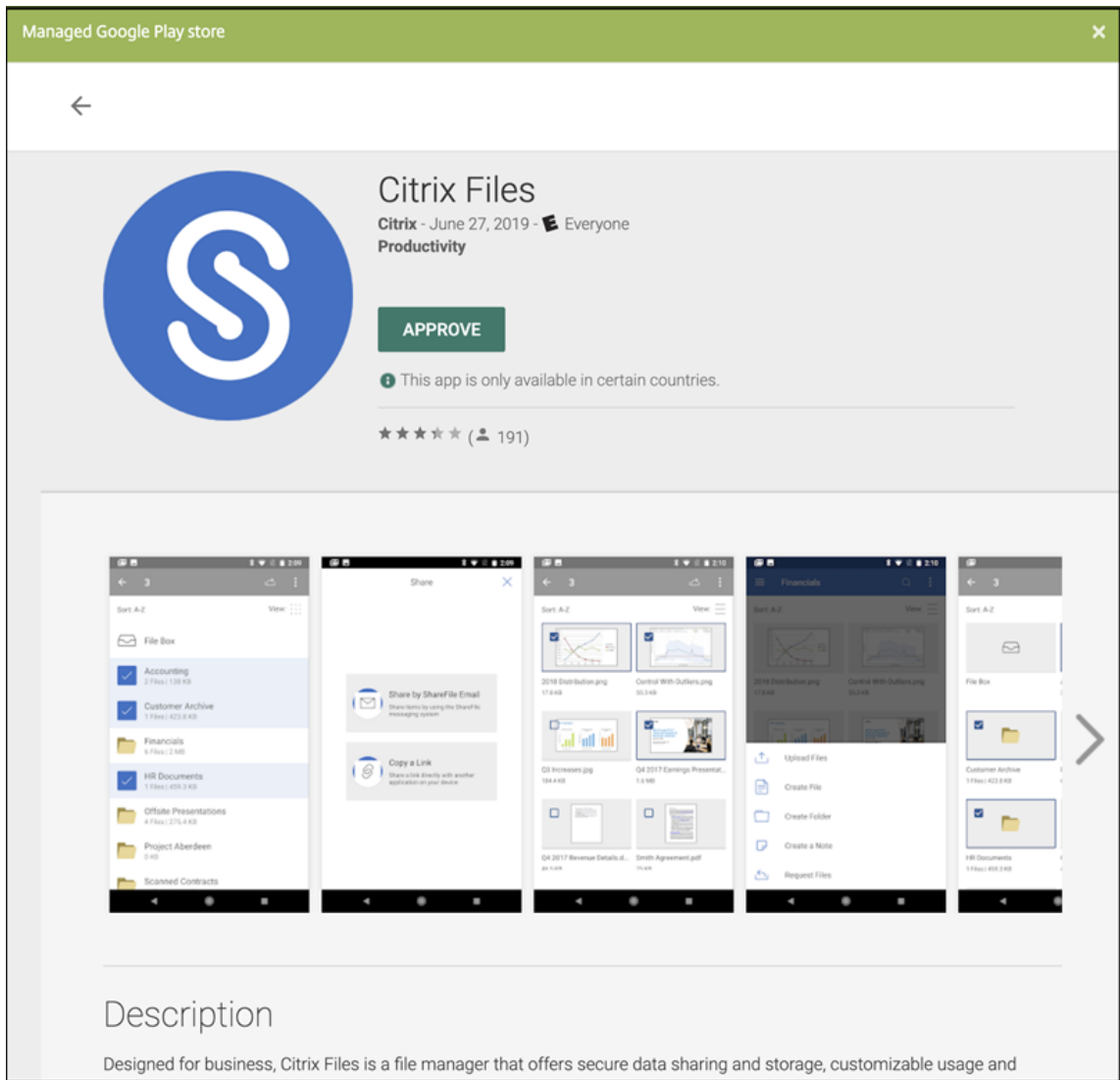
3. MDX를 클릭합니다. 앱 정보 페이지가 나타납니다.
4. 페이지 왼쪽에서 **Android Enterprise**를 플랫폼으로 선택합니다.
5. 앱 정보 페이지에서 다음 정보를 입력합니다.

- 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 표시됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.

- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 정보](#)를 참조하십시오.
6. 다음을 클릭합니다. **Android Enterprise MDX** 앱 페이지가 나타납니다.
 7. 업로드를 클릭하고 앱의.mdx 파일이 있는 파일 위치로 이동합니다. 파일을 선택하고 열기를 클릭합니다.
 8. 연결된 응용 프로그램에 관리되는 Google Play Store의 승인이 필요한 경우 UI에 알림이 표시됩니다. XenMobile 콘솔을 종료하지 않고 응용 프로그램을 승인하려면 예를 클릭합니다.




9. 관리되는 Google Play Store 페이지가 열리면 승인을 클릭합니다.



10. **Approve(승인)** 를 다시 클릭합니다.
11. **Keep approved when app requests new permissions(앱이 새 권한을 요청할 때 승인된 상태로 유지)** 를 선택합니다. 저장을 클릭합니다.

APPROVAL SETTINGS

NOTIFICATIONS



Citrix Files

Citrix

How would you like to handle new app permission requests?

☒ **Keep approved when app requests new permissions.**
 Users will be able to install the updated app.

☐ **Revoke app approval when this app requests new permissions.**
 App will be removed from the store until it is reapproved.

CANCEL

SAVE

12. 앱이 승인되고 저장되면 페이지에 더 많은 설정이 나타납니다. 다음 설정을 구성합니다.

- **파일 이름:** 앱에 연결된 파일 이름을 입력합니다.
- **앱 설명:** 앱에 대한 설명을 입력합니다.
- **제품 트랙:** 사용자 장치로 푸시할 제품 트랙을 지정합니다. 테스트용으로 설계된 추적이 있는 경우 해당 추적을 선택하여 사용자에게 할당할 수 있습니다. 기본값은 프로덕션입니다.
- **앱 버전:** 필요한 경우 앱 버전 번호를 입력합니다.
- **패키지 ID:** Google Play Store에 있는 앱의 URL입니다.
- **최소 OS 버전:** 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
- **최대 OS 버전:** 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
- **제외된 장치:** 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

13. **MDX** 정책을 구성합니다. MDX 앱의 앱 정책에 대한 자세한 내용은 [MDX 정책 요약](#) 및 [MAM SDK 개요](#)를 참조하십시오.

14. 배포 규칙을 구성합니다. 자세한 내용은 [리소스 배포](#)를 참조하십시오.

15. 스토어 구성을 확장합니다. 이 설정은 Android Enterprise 앱에 적용되지 않으며, 이러한 앱은 관리되는 Google Play에만 나타납니다.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

ON

Allow app comments

ON

필요한 경우 앱 스토어에 나타나는 앱 또는 화면 캡처에 대한 FAQ를 추가할 수 있습니다. 또한 사용자의 앱 평가 또는 설명 추가를 허용할지 여부를 설정할 수 있습니다.

- 다음 설정을 구성합니다.
 - 앱 **FAQ**: 앱에 대한 FAQ(질문과 답변)를 추가합니다.
 - 앱 스크린샷: 앱 스토어의 앱을 분류하는 데 도움이 되는 화면 캡처를 추가합니다. 업로드하는 그래픽은 PNG여야 합니다. GIF 또는 JPEG 이미지는 업로드할 수 없습니다.
 - 앱 등급 허용: 사용자의 앱 평가를 허용할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 앱 설명 허용: 선택한 앱에 대한 사용자의 설명을 허용할지 여부를 선택합니다. 기본값은 켜짐입니다.

16. 다음을 클릭합니다. 승인 페이지가 나타납니다.

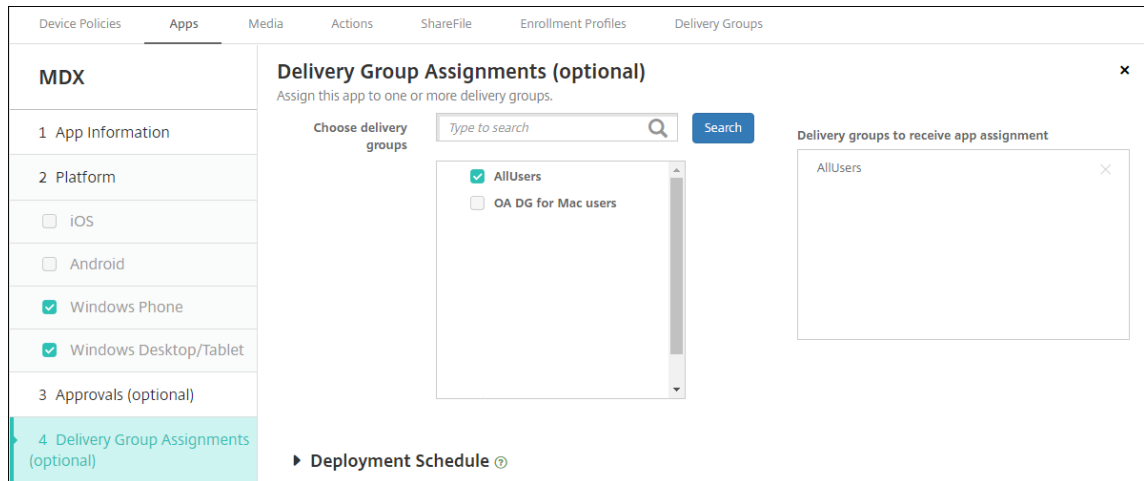
MDX	Approvals (optional) ×
1 App Information	Apply an existing workflow or create a new workflow to require approval before allowing users to access the app. Workflow to Use: None
2 Platform	
<input type="checkbox"/> iOS	
<input type="checkbox"/> Android	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Approvals (optional)	
4 Delivery Group Assignments (optional)	

사용자 계정을 만들 때 승인이 필요한 경우 워크플로를 사용합니다. 승인 워크플로를 설정하지 않으려는 경우 15 단계로 건너뛸 수 있습니다.

다음 설정을 구성하여 워크플로를 할당하거나 만듭니다.

- **사용할 워크플로:** 목록에서 기존 워크플로를 클릭하거나 새 워크플로 만들기를 클릭합니다. 기본값은 없음입니다.
- **새 워크플로 만들기를 선택하는 경우** 다음 설정을 구성합니다. 자세한 내용은 [워크플로 적용](#)을 참조하십시오.
- **이름:** 워크플로의 고유한 이름을 입력합니다.
- **설명:** 필요한 경우 워크플로의 설명을 입력합니다.
- **전자 메일 승인 템플릿:** 목록에서 할당할 전자 메일 승인 템플릿을 선택합니다. 이 필드 오른쪽에 있는 눈 모양 아이콘을 클릭하면 템플릿을 미리 볼 수 있는 대화 상자가 나타납니다.
- **관리자 승인 수준:** 목록에서 이 워크플로에 필요한 관리자 승인 수준의 번호를 선택합니다. 기본값은 1 수준입니다. 사용 가능한 옵션은 다음과 같습니다.
 - 필요 없음
 - 1 수준
 - 2 수준
 - 3 수준
- **Active Directory 도메인 선택:** 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
- **추가로 필요한 승인자 찾기:** 검색 필드에 추가로 필요한 사람의 이름을 입력하고 검색을 클릭합니다. 이름은 Active Directory 에서 가져옵니다.
- 필드에 이름이 나타나면 해당하는 이름 옆의 확인란을 선택합니다. 이름과 전자 메일 주소가 추가로 필요한 승인자 선택된 목록에 나타납니다.
 - 추가로 필요한 승인자 선택된 목록에서 사용자를 제거하려면 다음 중 하나를 수행합니다.
 - ★ 선택한 도메인에 있는 모든 사용자의 목록을 표시하려면 검색을 클릭합니다.
 - ★ 검색 결과를 제한하려면 검색 상자에 이름 전체 또는 일부를 입력한 다음 검색을 클릭합니다.
 - ★ 추가로 필요한 승인자 선택된 목록에 있는 사용자는 검색 결과 목록에서 해당 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하고 제거하려는 각 이름 옆에 있는 확인란의 선택을 취소합니다.

17. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.



18. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.

19. 배포 일정을 확장하고 다음 설정을 구성합니다.

- 배포 옆에서 켜짐을 클릭하여 배포를 예약하거나 꺼짐을 클릭하여 배포를 차단합니다. 기본 옵션은 켜짐입니다.
- 배포 일정 옆에서 지금 또는 나중에를 클릭합니다. 기본 옵션은 켜짐입니다.
- 나중에를 클릭하는 경우 달력 아이콘을 클릭하고 배포 날짜와 시간을 선택합니다.
- 배포 조건 옆에서 모든 연결에서를 클릭하거나 이전 배포가 실패한 경우에만을 클릭합니다. 기본 옵션은 모든 연결에서입니다.
- 상시 연결에 대해 배포 옆에 꺼짐이 선택되어 있는지 확인합니다. 기본 옵션은 꺼짐입니다. 버전이 10.18.19 이상인 XenMobile 을 사용하여 시작한 경우 Android Enterprise 에서는 상시 연결을 사용할 수 없습니다. 버전 10.18.19 이하인 XenMobile 을 사용하여 시작한 고객에게는 연결을 권장하지 않습니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우에만 이 옵션이 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 상시 연결에 대해 배포를 제외하고 모든 플랫폼에 적용됩니다.

20. 저장을 클릭합니다.

단계를 반복하여 각 모바일 생산성 앱에 대해 MDX 앱을 구성합니다.

보안 챌린지 정책 구성

XenMobile 암호 장치 정책은 사용자가 자신의 장치 또는 장치의 Android Enterprise 작업 프로필에 액세스하도록 하는 보안 챌린지에 대한 규칙 집합을 구성합니다. 보안 챌린지는 암호 또는 생체 인식일 수 있습니다. 암호 정책에 대한 자세한 내용은 [암호 장치 정책](#)을 참조하십시오.

- Android Enterprise 배포에 BYOD 장치가 포함되는 경우 작업 프로필에 대한 암호 정책을 구성합니다.

- 배포에 회사 소유의 완전 관리형 장치가 포함되는 경우 장치 자체에 대한 암호 정책을 구성합니다.
- 배포에 두 가지 유형의 장치가 모두 포함되는 경우 두 유형의 암호 정책을 모두 구성합니다.

암호 정책을 구성하려면:

1. XenMobile 콘솔에서 구성 > 장치 정책으로 이동합니다.
2. 추가를 클릭합니다.
3. 필터 표시를 클릭하여 정책 플랫폼 창을 표시합니다. 정책 플랫폼 창에서 **Android Enterprise** 를 선택합니다.
4. 오른쪽 창에서 암호를 클릭합니다.

Device Policies		Apps	Media	Actions	ShareFile	Enrollment Profiles
Policy Platform Clear All		Add a New Policy Hide filter				
<input type="checkbox"/>	iOS	10	Policies most often used <hr/> Exchange <hr/> Location <hr/> Passcode <hr/> Restrictions <hr/> Scheduling			
<input type="checkbox"/>	Windows Desktop/Tablet	11				
<input type="checkbox"/>	Android	11				
<input type="checkbox"/>	macOS	8				
<input type="checkbox"/>	Windows Mobile/CE	8				
<input type="checkbox"/>	Windows Phone	9				
<input checked="" type="checkbox"/>	Android Enterprise	17				

1. 정책 이름을 입력합니다. 다음을 클릭합니다.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery
<div> <div> <h2>Passcode Policy</h2> <div> <div>1 Policy Info</div> <div>2 Platforms Clear All</div> <div> <input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Samsung KNOX <input checked="" type="checkbox"/> Android Enterprise </div> </div> <div> <h3>Policy Information</h3> <p>This policy creates a passcode policy based on the standards of your organization rules, such as the grace period before device lock.</p> <div> <div>Policy Name *</div> <div>Passcode - AE</div> </div> <div> <div>Description</div> <div></div> </div> </div> </div> </div>						

2. 암호 정책 설정을 구성합니다.

- 장치 자체의 보안 챌린지에 사용할 수 있는 설정을 보려면 장치 암호 필요를 커짐으로 설정합니다.
- 작업 프로필 보안 챌린지에 사용할 수 있는 설정을 보려면 작업 프로필 보안 챌린지를 커짐으로 설정합니다.

3. 다음을 클릭합니다.

4. 정책을 하나 이상의 배달 그룹에 할당합니다.

5. 저장을 클릭합니다.

등록 프로필 만들기

XenMobile 배포에서 Android Enterprise 를 사용하도록 설정한 경우 등록 프로필을 사용하여 Android 장치의 등록 방법을 제어할 수 있습니다. 등록 프로필을 만들어서 Android Enterprise 장치를 등록할 경우 등록 프로필을 구성하여 새 장치와 공장 기본값으로 재설정된 장치를 다음으로 등록할 수 있습니다.

- 완전히 관리되는 장치
- 전용 장치 (COSU 장치)
- 작업 프로필로 완전히 관리되는 장치 (COPE 장치)

이러한 Android Enterprise 등록 프로필을 각각 구성하여 BYOD Android 장치를 작업 프로필 장치로 등록할 수도 있습니다.

XenMobile 배포에서 Android Enterprise 를 사용하도록 설정한 경우 새로 등록되거나 다시 등록되는 모든 Android 장치는 Android Enterprise 장치로 등록됩니다. 기본적으로 글로벌 등록 프로필은 신규 및 공장 기본값으로 재설정된 Android 장치를 완전 관리형 장치로 등록하고, BYOD Android 장치를 작업 프로필 장치로 등록합니다.

등록 프로필을 만들 경우 배달 그룹을 할당합니다. 사용자가 등록 프로필이 다른 여러 배달 그룹에 속하는 경우 사용되는 등록 프로필은 배달 그룹의 이름에 따라 결정됩니다. XenMobile 은 사전순으로 표시된 배달 그룹 목록의 마지막에 나타나는 배달 그룹을 선택합니다. 자세한 내용은 [등록 프로필](#)을 참조하십시오.

등록 프로필을 사용하여 MDM 전용, MDM+MAM, MAM 전용과 같이 여러 사용 사례를 결합할 수 있습니다. 서버 속성 `xms.server.mode`에 반영된 XenMobile Server 라이선스 유형에 따라 구성 > 등록 프로필에서 제공되는 설정이 결정됩니다.

완전히 관리되는 장치에 대한 등록 프로필 추가

글로벌 등록 프로필은 기본적으로 완전히 관리되는 장치를 등록하지만 완전히 관리되는 장치를 등록할 추가 등록 프로필을 만들 수 있습니다.

1. XenMobile 콘솔에서 구성 > 등록 프로필로 이동합니다.
2. 등록 프로필을 추가하려면 추가를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다.
3. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수를 설정합니다.
4. 플랫폼에서 **Android**를 선택하거나 다음을 클릭합니다. 등록 구성 페이지가 나타납니다.
5. 관리를 **Android Enterprise**로 설정합니다.
6. 장치 소유자 모드를 기업 소유 장치로 설정합니다.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ? Management <ul style="list-style-type: none"> <input checked="" type="radio"/> Android Enterprise ? <input type="radio"/> Legacy device administration (not recommended) ? <input type="radio"/> Do not manage devices ? Device owner mode <ul style="list-style-type: none"> <input checked="" type="radio"/> Company-owned device ? <input type="radio"/> Fully managed with work profile ? <input type="radio"/> Dedicated device ? <input type="radio"/> None ? BYOD work profile <input checked="" type="checkbox"/> On ? Application management ? Citrix MAM <input checked="" type="checkbox"/> On ? User consent Allow users to decline device management <input checked="" type="checkbox"/> On ?
Android	
iOS	
3 Assignment (optional)	

7. **BYOD** 작업 프로필을 사용하면 BYOD 장치를 작업 프로필 장치로 구성하기 위한 등록 프로필을 구성할 수 있습니다. 신규 및 공장 기본값으로 재설정된 장치를 완전히 관리되는 장치로 등록합니다.

- BYOD 장치를 작업 프로필 장치로 등록하도록 허용하려면 **BYOD** 작업 프로필을 켜짐으로 설정합니다. 기본값은 꺼짐입니다.
- 완전히 관리되는 장치에 대한 등록을 제한하려면 **BYOD** 작업 프로필을 꺼짐으로 설정합니다.

8. Citrix MAM 에서 장치 등록 여부를 선택합니다.

9. **BYOD** 작업 프로필을 켜짐으로 설정할 경우 사용자 동의를 구성합니다. BYOD 작업 프로필 장치 사용자가 장치 등록 시 장치 관리를 거부할 수 있도록 허용하려면 사용자의 장치 관리 거부를 허용을 켜짐으로 설정합니다.

BYOD 작업 프로필이 켜짐으로 설정되면 사용자의 장치 관리 거부를 허용의 기본값은 켜짐입니다. **BYOD** 작업 프로필이 꺼짐으로 설정되면 사용자의 장치 관리 거부를 허용이 비활성화됩니다.

10. 할당 (옵션) 을 선택합니다. 배달 그룹 할당 화면이 나타납니다.

11. 완전히 관리되는 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장을 클릭합니다.

추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.

Device Policies

Apps

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

Alexa for Business

Enrollment Profiles

Search

Q

Add

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit	
<input type="checkbox"/>	Fully managed devices	11/19/19 2:19:16 pm	11/19/19 2:19:16 pm	unlimited	
<input type="checkbox"/>	Global	3/7/18 4:08:24 pm	3/7/18 4:08:24 pm	unlimited	

Showing 1 - 2 of 2 items

Items per page: 10

전용 장치 등록 프로필 추가

XenMobile 배포에 전용 장치가 포함되는 경우 단일 XenMobile 관리자 또는 소규모 관리자 그룹이 다수의 전용 장치를 등록합니다. 이러한 관리자가 필요한 모든 장치를 등록할 수 있도록 하려면 사용자당 무제한의 장치가 허용되는 관리자용 등록 프로필을 만듭니다.

1. XenMobile 콘솔에서 구성 > 등록 프로필로 이동합니다.
2. 등록 프로필을 추가하려면 추가를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수가 무제한으로 설정되어 있는지 확인합니다.
3. 플랫폼에서 **Android** 를 선택하거나 다음을 클릭합니다. 등록 구성 페이지가 나타납니다.
4. 관리를 **Android Enterprise** 로 설정합니다.
5. 장치 소유자 모드를 전용 장치로 설정합니다.

6. **BYOD** 작업 프로필을 사용하면 BYOD 장치를 작업 프로필 장치로 구성하기 위한 등록 프로필을 구성할 수 있습니다. 신규 및 공장 기본값으로 재설정된 장치를 전용 장치로 등록합니다. BYOD 장치를 작업 프로필 장치로 등록하도록 허용하려면 **BYOD** 작업 프로필을 켜짐으로 설정합니다. 기업 소유 장치에 대한 등록을 제한하려면 **BYOD** 작업 프로필을 꺼짐으로 설정합니다. 기본값은 켜짐입니다.

7. Citrix MAM 에서 장치 등록 여부를 선택합니다.

8. **BYOD** 작업 프로필을 켜짐으로 설정할 경우 사용자 동의를 구성합니다. BYOD 작업 프로필 장치 사용자가 장치 등록 시 장치 관리를 거부할 수 있도록 허용하려면 사용자의 장치 관리 거부를 허용을 켜짐으로 설정합니다.

BYOD 작업 프로필이 켜짐으로 설정되면 사용자의 장치 관리 거부를 허용의 기본값은 켜짐입니다. **BYOD** 작업 프로필이 꺼짐으로 설정되면 사용자의 장치 관리 거부를 허용이 비활성화됩니다.

9. 할당 (옵션) 을 선택합니다. 배달 그룹 할당 화면이 나타납니다.

10. 전용 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장을 클릭합니다.

추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.

	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	Dedicated devices	11/1/19 3:30:36 pm	11/1/19 3:30:36 pm	unlimited
<input type="checkbox"/>	Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited

작업 프로파일로 완전히 관리되는 장치에 대한 등록 프로파일 추가

1. XenMobile 콘솔에서 구성 > 등록 프로파일로 이동합니다.
2. 등록 프로 파일을 추가하려면 추가를 클릭합니다. 등록 정보 페이지에서 등록 프로파일의 이름을 입력합니다.
3. 이 프로 파일을 가진 구성원이 등록할 수 있는 장치 수를 설정합니다.
4. 플랫폼에서 **Android** 를 선택하거나 다음을 클릭합니다. 등록 구성 페이지가 나타납니다.
5. 관리를 **Android Enterprise** 로 설정합니다. 장치 소유자 모드를 작업 프로파일로 완전히 관리로 설정합니다.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p>Device management ⓘ</p> <p>Management</p> <p><input checked="" type="radio"/> Android Enterprise ⓘ</p> <p><input type="radio"/> Legacy device administration (not recommended) ⓘ</p> <p><input type="radio"/> Do not manage devices ⓘ</p> <p>Device owner mode</p> <p><input type="radio"/> Company-owned device ⓘ</p> <p><input checked="" type="radio"/> Fully managed with work profile ⓘ</p> <p><input type="radio"/> Dedicated device ⓘ</p> <p><input type="radio"/> None ⓘ</p> <p>BYOD work profile <input checked="" type="checkbox"/> ⓘ</p> <p>Application management ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
Android	
iOS	
3 Assignment (optional)	

6. **BYOD** 작업 프로 파일을 사용하면 BYOD 장치를 작업 프로파일 장치로 구성하기 위한 등록 프로 파일을 구성할 수 있습니다. 신규 및 공장 기본값으로 재설정된 장치를 작업 프로파일로 완전히 관리되는 장치로 등록합니다. BYOD 장치를 작업 프로파일 장치로 등록하도록 허용하려면 **BYOD** 작업 프로 파일을 켜짐으로 설정합니다. 전용 장치에 대한 등록을 제한하려면 **BYOD** 작업 프로 파일을 꺼짐으로 설정합니다. 기본값은 꺼짐입니다.
7. Citrix MAM 에서 장치 등록 여부를 선택합니다.
8. **BYOD** 작업 프로 파일을 켜짐으로 설정할 경우 사용자 동의를 구성합니다. BYOD 작업 프로파일 장치 사용자가 장치 등록 시 장치 관리를 거부할 수 있도록 허용하려면 사용자의 장치 관리 거부를 허용을 켜짐으로 설정합니다.
BYOD 작업 프로 파일이 켜짐으로 설정되면 사용자의 장치 관리 거부를 허용의 기본값은 켜짐입니다. **BYOD** 작업 프로 파일이 꺼짐으로 설정되면 사용자의 장치 관리 거부를 허용이 비활성화됩니다.
9. 할당 (옵션) 을 선택합니다. 배달 그룹 할당 화면이 나타납니다.
10. 배달 그룹 또는 작업 프로파일로 완전히 관리되는 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장 을 클릭합니다.
추가한 프로 파일과 함께 등록 프로 파일 페이지가 나타납니다.

Device Policies	Apps	Media	Actions	Content Collaboration	Enrollment Profiles	Delivery Groups
-----------------	------	-------	---------	-----------------------	----------------------------	-----------------

Enrollment Profiles				Search <input type="text"/>
	Add			
<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	COPE devices	11/1/19 1:01:51 pm	11/1/19 1:01:51 pm	unlimited
<input type="checkbox"/>	Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited

Showing 1 - 2 of 2 items Items per page:

레거시 장치에 대한 등록 프로필 추가

Google 은 장치 관리의 장치 관리자 모드를 지원 중단할 예정입니다. Google 은 장치 소유자 모드 또는 프로필 소유자 모드에서 모든 Android 장치를 관리할 것을 권장하고 있습니다. (Google Android Enterprise 개발자 가이드의 [장치 관리 사용 중단 참고](#))

이 변경 사항을 지원하려면:

- Citrix 에서는 Android 장치에 대한 기본 등록 옵션으로 Android Enterprise 를 사용합니다.
- XenMobile 배포에서 Android Enterprise 를 사용하도록 설정한 경우 새로 등록되거나 다시 등록되는 모든 Android 장치는 Android Enterprise 장치로 등록됩니다.

조직이 Android Enterprise 를 사용하여 레거시 Android 장치를 관리할 준비가 되지 않았을 수 있습니다. 이러한 장치를 장치 관리자 모드에서 계속해서 관리할 수 있습니다. 장치 관리자 모드로 이미 등록된 장치의 경우 XenMobile 에서 장치 관리자 모드로 계속 관리합니다.

신규 Android 장치 등록에 장치 관리자 모드를 사용하도록 허용하려면 레거시 장치에 대한 등록 프로필을 만듭니다.

레거시 장치에 대한 등록 프로필을 만들려면:

1. XenMobile 콘솔에서 구성 > 등록 프로필로 이동합니다.
2. 등록 프로필을 추가하려면 추가를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다.
3. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수를 설정합니다.
4. 플랫폼에서 **Android** 를 선택하거나 다음을 클릭합니다. 등록 구성 페이지가 나타납니다.
5. 관리를 레거시 장치 관리 (권장되지 않음) 로 설정합니다. 다음을 클릭합니다.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ? Management <input type="radio"/> Android Enterprise ? <input checked="" type="radio"/> Legacy device administration (not recommended) ? <input type="radio"/> Do not manage devices ?
Android	Application management ? Citrix MAM <input checked="" type="checkbox"/> On ?
iOS	User consent Allow users to decline device management <input checked="" type="checkbox"/> On ?
3 Assignment (optional)	

6. Citrix MAM 에서 장치 등록 여부를 선택합니다.
7. 사용자가 장치 등록 시 장치 관리를 거부할 수 있도록 허용하려면 사용자의 장치 관리 거부를 허용을 켜짐으로 설정합니다. 기본값은 켜짐입니다.
8. 할당 (옵션) 을 선택합니다. 배달 그룹 할당 화면이 나타납니다.
9. 전용 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장을 클릭합니다.

추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.

Device Policies

Apps

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

Alexa for Business

Enrollment Profiles

Search

Add

	Enrollment profile name	Created on	Updated on	Device limit	
<input type="checkbox"/>	Android legacy (DA) devices	11/19/19 1:41:54 pm	11/19/19 1:41:54 pm	unlimited	
<input type="checkbox"/>	Global	3/7/18 4:08:24 pm	3/7/18 4:08:24 pm	unlimited	

Showing 1 - 2 of 2 items

Items per page: 10

장치 관리자 모드에서 레거시 장치 관리를 계속하려면 이 프로필을 사용하여 등록하거나 재등록합니다. 사용자로 하여금 Secure Hub 를 다운로드하고 등록 서버 URL 을 제공하도록 하면 작업 프로필 장치와 유사하게 장치 관리자 장치를 등록할 수 있습니다.

Android Enterprise 작업 프로필 장치 프로비전

Android Enterprise 작업 프로필 장치는 프로필 소유자 모드에서 등록됩니다. 이러한 장치가 새 장치이거나 공장 기본값으로 재설정될 필요는 없습니다. BYOD 장치는 작업 프로필 장치로 등록됩니다. 등록 환경은 XenMobile 의 Android 등록과 비슷합니다. 사용자가 Google Play 에서 Secure Hub 를 다운로드하고 장치를 등록합니다.

Android Enterprise 에서 작업 프로필 장치로 장치를 등록하는 경우 **USB** 디버깅 및 알 수 없는 소스 설정은 장치에서 기본적으로 비활성화됩니다.

Android Enterprise 에서 작업 프로필 장치로 장치를 등록하는 경우 항상 Google Play 로 이동하십시오. 거기서 사용자의 개인 프로필에 Secure Hub 가 표시되도록 설정합니다.

Android Enterprise 완전 관리형 장치 프로비전

이전 섹션에서 설정한 배포에서 완전 관리형 장치를 등록할 수 있습니다. 완전 관리형 장치는 회사 소유의 장치이며 장치 소유자 모드에서 등록됩니다. 장치 소유자 모드에서는 새 장치 또는 공장 기본값으로 재설정된 장치만 등록할 수 있습니다.

다음 등록 방법 중 하나를 사용하여 장치 소유자 모드에서 장치를 등록할 수 있습니다.

- **DPC** 식별자 토큰 이 등록 방법에서는 사용자가 장치를 설정할 때 `afw#xenmobile` 문자를 입력합니다. `afw#xenmobile`은 Citrix DPC 식별자 토큰입니다. 이 토큰은 XenMobile 이 관리하는 장치로 장치를 식별하고 Google Play Store 에서 Secure Hub 를 다운로드합니다. Citrix DPC 식별자 토큰을 사용하여 장치 등록을 참조하십시오.
- **NFC**(근거리 통신) 범프: NFC 범프 등록 방법은 근거리 통신을 사용하여 두 장치 간 데이터를 전송합니다. 새 장치 또는 공장 기본값으로 재설정된 장치에서는 Bluetooth, Wi-Fi 및 기타 통신 모드를 사용할 수 없습니다. NFC 는 이 상태에서 장치 사용 가능한 유일한 통신 프로토콜입니다. NFC 범프를 사용하여 장치 등록을 참조하십시오.
- **QR 코드**: QR 코드 등록은 태블릿과 같이 NFC 를 지원하지 않는 분산된 제품군의 장치를 등록할 때 사용될 수 있습니다. QR 코드 등록 방법은 설치 마법사에서 QR 코드를 스캔하여 장치 프로필 모드를 설정하고 구성합니다. QR 코드를 사용하여 장치 등록을 참조하십시오.
- **제로 터치**: 제로 터치 등록을 사용하면 장치 전원을 처음 켤 때 자동으로 등록하도록 장치를 구성할 수 있습니다. 제로 터치 등록은 Android 9.0 이상을 실행하는 일부 Android 장치에서 지원됩니다. 제로 터치 등록을 참조하십시오.
- **Google 계정**: 사용자가 Google 계정 자격 증명을 입력하여 프로비저닝 프로세스를 시작합니다. 이 옵션은 Google Workspace 를 사용하는 엔터프라이즈용입니다.

Citrix DPC 식별자 토큰을 사용하여 장치 등록

새 장치 또는 공장 기본값으로 재설정된 장치의 초기 설정을 위해 전원을 켜 후 Google 계정을 입력하라는 메시지가 표시되면 `afw#xenmobile`을 입력합니다. 이 동작을 수행하면 Secure Hub 가 다운로드되고 설치됩니다. 그런 다음 사용자는 Secure Hub 설정 메시지에 따라 등록을 완료합니다.

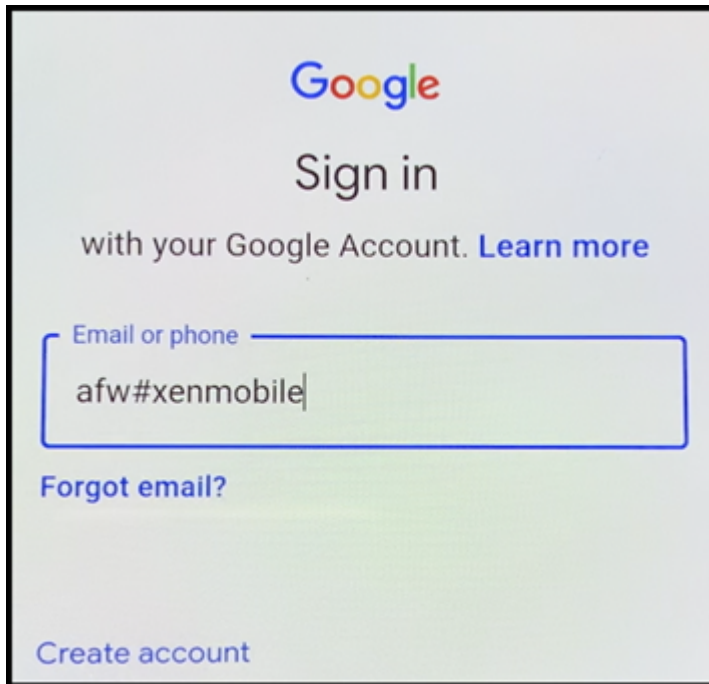
최신 버전의 Secure Hub 가 Google Play Store 에서 다운로드되므로 이 등록 방법이 대부분의 고객에게 권장됩니다. 다른 등록 방법과 달리, XenMobile Server 에서 다운로드하기 위해 Secure Hub 를 제공하지 않습니다.

시스템 요구 사항

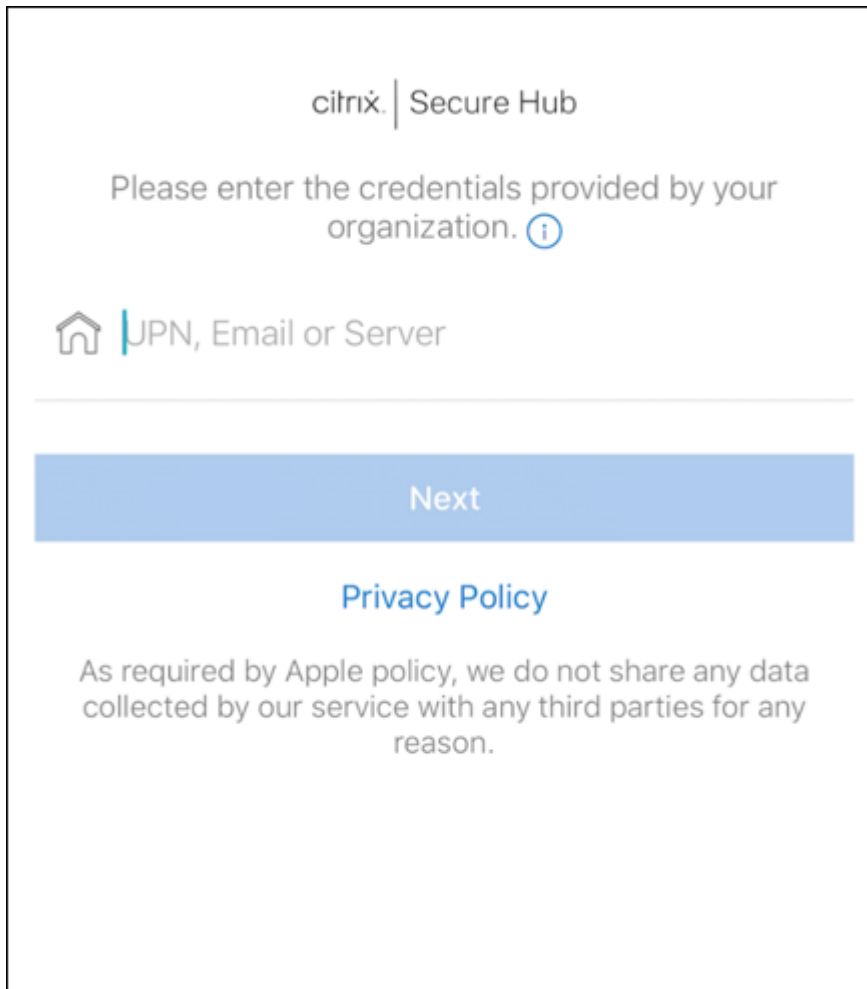
- Android OS 를 실행하는 모든 Android 장치에서 지원됩니다.

장치를 등록하려면

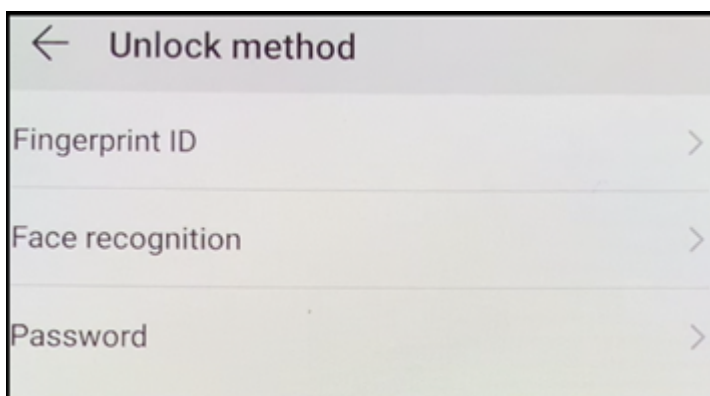
1. 새 장치 또는 공장 기본값으로 재설정된 장치의 전원을 켭니다.
2. 초기 장치 설정이 로드되고 Google 계정을 입력하라는 메시지가 표시됩니다. 장치에 장치의 홈 화면이 로드되는 경우 알림 표시줄에서 설정 완료 알림을 확인합니다.
3. 전자 메일 또는 전화 필드에 `afw#xenmobile`을 입력합니다.



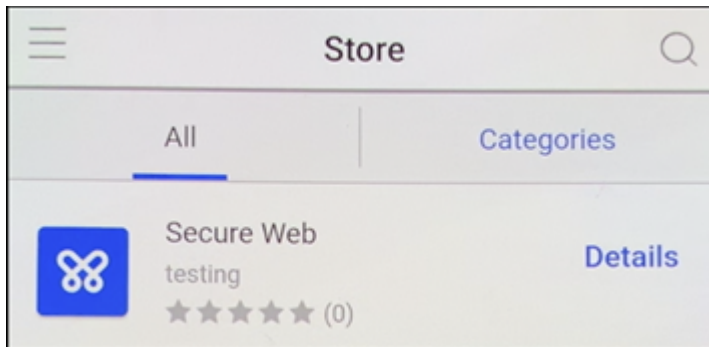
4. Android Enterprise 화면에서 Secure Hub 를 설치하라는 메시지가 표시되면 설치를 누릅니다.
5. Secure Hub 설치 관리자 화면에서 **Install**(설치) 을 누릅니다.
6. 모든 앱 권한 요청에 대해 **Allow**(허용) 를 누릅니다.
7. **Accept & Continue**(동의 및 계속) 를 눌러 Secure Hub 를 설치하고 장치 관리를 허용합니다.
8. 이제 Secure Hub 가 설치되었고 기본 등록 화면에 표시됩니다. 이 예에서는 AutoDiscovery 을 설정하지 않았습니다. 자동 검색을 설정했다면 사용자가 사용자 이름/전자 메일을 입력하고 서버를 찾을 수 있습니다. 대신 환경에 대한 등록 URL 을 입력하고 다음을 누릅니다.



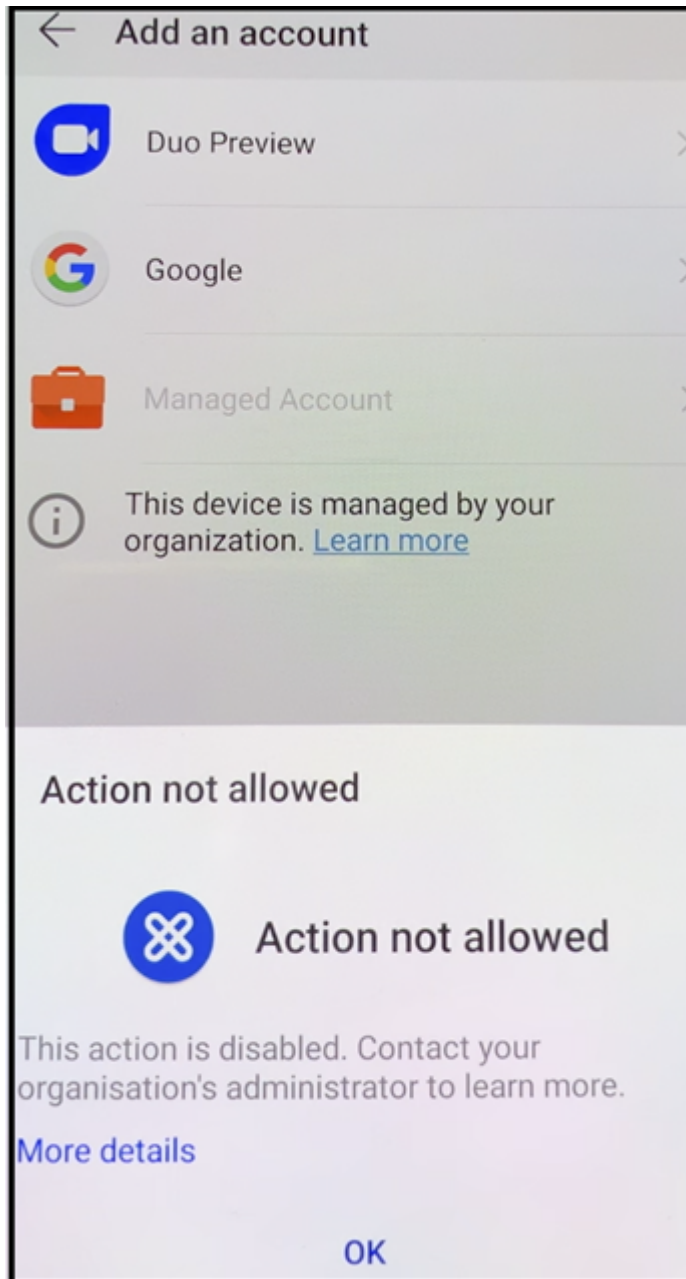
9. XenMobile 의 기본 구성에서는 사용자가 MAM 을 사용할지 아니면 MDM+MAM 을 사용할지를 선택할 수 있습니다. 이와 같은 메시지가 표시되면 예, 등록을 눌러 MDM+MAM 을 선택합니다.
10. 사용자 이름과 암호를 입력하고 다음을 누릅니다.
11. 장치 암호를 구성하라는 메시지가 표시됩니다. 설정을 누르고 암호를 입력합니다.
12. 작업 프로필 잠금 해제 방법을 구성하라는 메시지가 표시됩니다. 이 예에서는 암호를 누르고 **PIN** 을 누른 다음 PIN 을 입력합니다.



13. 이제 Secure Hub **My Apps**(내 앱) 소개 화면에 장치가 표시됩니다. 스토어의 앱 추가를 누릅니다.
14. Secure Web 을 추가하려면 **Secure Web** 을 누릅니다.



15. 추가를 누릅니다.
16. Secure Hub 가 사용자를 Google Play Store 로 보내 Secure Web 을 설치하도록 합니다. 설치를 누릅니다.
17. Secure Web 이 설치된 후 열기를 누릅니다. 주소 표시줄에 내부 사이트의 URL 을 입력하고 페이지가 로드되는지 확인합니다.
18. 장치의 설정 > 계정으로 이동합니다. 관리되는 계정을 수정할 수 없음을 확인합니다. 화면 공유 또는 원격 디버깅을 위한 개발자 옵션도 차단됩니다.



NFC 범프를 사용하여 장치 등록

NFC 범프를 사용하여 완전하게 관리되는 장치로 장치를 등록하려면 두 장치, 즉 출고 기본값으로 재설정된 장치와 XenMobile Provisioning Tool 을 실행하는 장치가 필요합니다.

시스템 요구 사항 및 사전 요구 사항

- 지원되는 Android 장치.

- 완전하게 관리되는 장치로서 Android Enterprise 용으로 프로비전된 새 장치 또는 출고 기본값으로 재설정된 장치. 이 사전 요구 사항을 완료하는 단계는 이 문서의 뒷부분에서 찾을 수 있습니다.
- NFC 호환성이 있으며 구성된 Provisioning Tool 이 실행되고 있는 또 다른 장치. Provisioning Tool 은 Secure Hub 또는 [Citrix 다운로드 페이지](#)에서 사용할 수 있습니다.

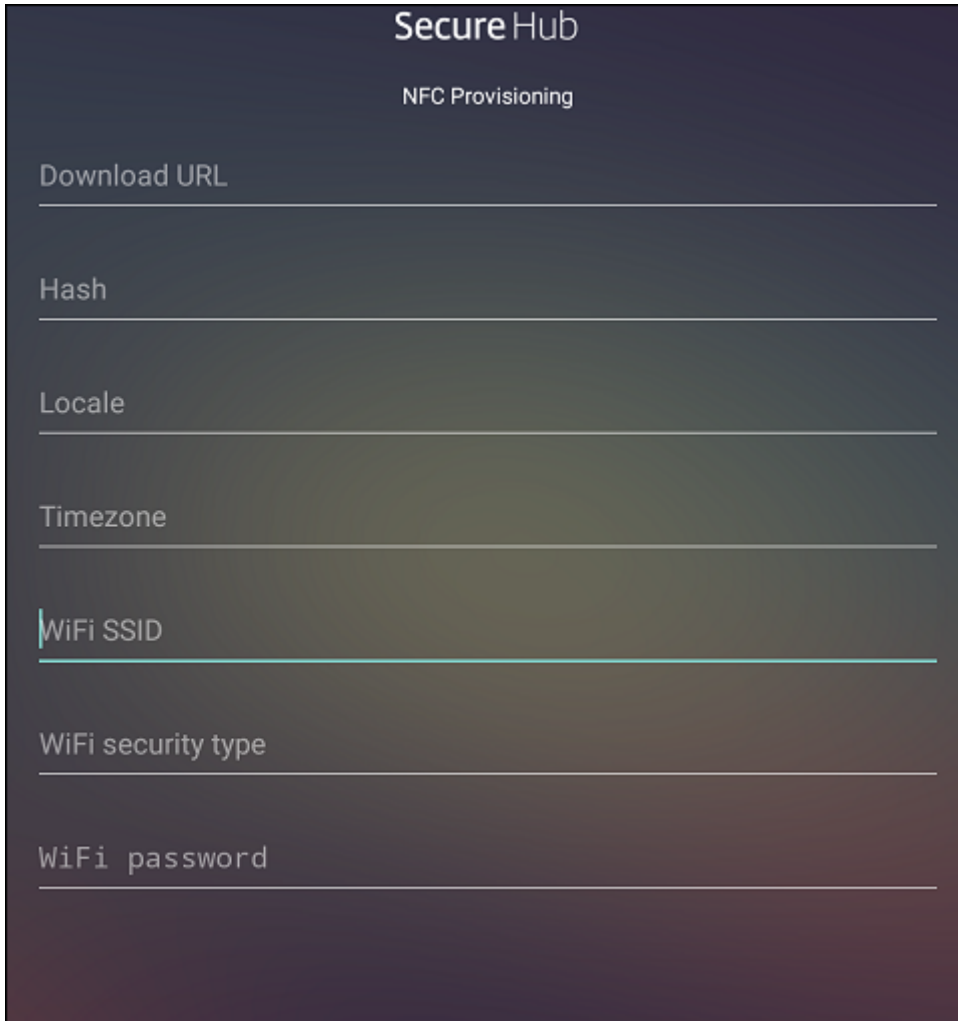
각 장치에는 하나의 Android Enterprise 프로필인 관리되는 Secure Hub 만 있어야 합니다. 각 장치에는 하나의 프로필만 허용됩니다. 두 번째 DPC 앱을 추가하려고 하면 설치된 Secure Hub 가 제거됩니다.

NFC 범프를 통해 전송된 데이터 출고 기본값으로 재설정된 장치를 프로비저닝하려면 NFC 범프를 통해 다음 데이터를 전송하여 Android Enterprise 를 초기화해야 합니다.

- 장치 소유자 (이 경우 Secure Hub) 역할을 하는 DPC 앱의 패키지 이름.
- 장치가 DPC 앱을 다운로드 할 수 있는 인트라넷/인터넷 위치.
- 다운로드가 성공했는지 확인하기 위한 DPC 앱의 SHA1 해시.
- 공장 기본값으로 재설정된 장치가 연결하여 DPC 앱을 다운로드할 수 있는 Wi-Fi 연결 세부 정보. 참고: 이 단계에서 Android 는 802.1x Wi-Fi 를 지원하지 않습니다.
- 장치의 표준 시간대 (선택 사항)
- 장치의 지리적 위치 (선택 사항)

두 장치가 범프되면 Provisioning Tool 의 데이터가 출고 기본값으로 재설정된 장치로 전송됩니다. 이 데이터는 관리자 설정으로 Secure Hub 를 다운로드하는 데 사용됩니다. 표준 시간대 및 위치 값을 입력하지 않으면 Android 가 자동으로 새 장치에서 이러한 값을 구성합니다.

XenMobile Provisioning Tool 구성 NFC 범프를 수행하기 전에 Provisioning Tool 을 구성해야 합니다. 이 구성은 NFC 범프 중에 출고 기본값으로 재설정된 장치로 전송됩니다.



The image shows a mobile application interface titled "Secure Hub" with a subtitle "NFC Provisioning". It contains several text input fields for configuration: "Download URL", "Hash", "Locale", "Timezone", "WiFi SSID" (which has a blue cursor), "WiFi security type", and "WiFi password". Each field is preceded by its label and followed by a horizontal line indicating the input area.

필요한 필드에 데이터를 입력하거나 텍스트 파일을 사용해 데이터를 채울 수 있습니다. 다음 절차의 단계에서는 텍스트 파일을 구성하고 각 필드에 대한 설명을 포함시키는 방법에 대해 설명합니다. 입력한 정보가 앱에 저장되지 않으므로 나중에 사용할 수 있도록 정보를 유지하려면 텍스트 파일을 만들 수 있습니다.

텍스트 파일을 사용하여 **Provisioning Tool** 을 구성하려면 파일의 이름을 `nfcprovisioning.txt` 로 지정하고 장치의 SD 카드에 있는 `/sdcard/` 폴더에 파일을 저장합니다. 그러면 앱에서 텍스트 파일을 읽고 값을 채울 수 있습니다.

텍스트 파일에는 다음과 같은 데이터가 포함되어야 합니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=<download_location>
```

이 줄은 EMM 공급자 앱의 인터넷/인터넷 위치입니다. NFC 범프 후에 출고 기본값으로 재설정된 장치가 Wi-Fi 에 연결되면 장치가 이 위치에 액세스하여 다운로드할 수 있어야 합니다. URL 은 특수한 형식이 필요하지 않은 일반 URL 입니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1
hash>
```


이 줄은 EMM 공급자 앱의 체크섬입니다. 이 체크섬은 다운로드가 성공했는지 확인하는 데 사용됩니다. 체크섬을 얻는 단계에 대해서는 이 문서 뒷부분에서 설명합니다.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

이 줄은 Provisioning Tool 이 실행되고 있는 장치의 연결된 Wi-Fi SSID 입니다.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

지원되는 값은 WEP 및 WPA2 입니다. Wi-Fi 가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Wi-Fi 가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

언어 및 국가 코드를 입력합니다. 언어 코드는 [ISO 639-1](#)에 정의된 대로 소문자 두 자로 구성된 ISO 언어 코드입니다 (예: en). 국가 코드는 [ISO 3166-1](#)에 정의된 대로 대문자 두 자로 구성된 ISO 국가 코드입니다 (예: US). 예를 들어, 미국에서 사용하는 영어의 경우 en_US 를 입력합니다. 코드를 입력하지 않으면 국가 및 언어가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

장치가 실행되는 표준 시간대입니다. [지역/위치 형식의 Olson 이름](#)을 입력합니다. 예를 들어 태평양 표준시의 경우 America/Los_Angeles 를 입력합니다. 이름을 입력하지 않으면 표준 시간대가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

값이 앱에 Secure Hub 로 하드 코딩되어 있기 때문에 이 데이터는 필요하지 않습니다. 여기서는 완결성을 위해 언급되었습니다.

예를 들어 WPA2 를 사용하여 보호되는 Wi-Fi 가 있는 경우 완성된 nfcprovisioning.txt 파일은 다음과 같습니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=
https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

예를 들어 보호되지 않는 Wi-Fi 가 있는 경우 완성된 nfcprovisioning.txt 파일은 다음과 같습니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Citrix Secure Hub 체크섬을 얻으려면 Secure Hub 체크섬은 상수값(qn7oZUtheu3JBainzZRrrjCQv6L006Ll10jcxT3-yKM)입니다. Secure Hub의 APK 파일을 다운로드하려면 다음 Google Play 스토어 링크를 사용하십시오. <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>

앱 체크섬을 얻으려면 필수 구성 요소:

- Android SDK Build Tools의 **apksigner** 도구
- OpenSSL 명령줄

모든 앱의 체크섬을 얻으려면 다음 단계를 따르십시오.

1. Google Play 스토어에서 앱의 APK 파일을 다운로드합니다.
2. OpenSSL 명령줄에서 **apksigner** 도구: `android-sdk/build-tools/<version>/apksigner`로 이동하고 다음 내용을 입력합니다.

```
1 apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
   m{
2   (?<=SHA-256 digest:) .* }
3   ' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
4   <!--NeedCopy-->
```

명령이 유효한 체크섬을 반환합니다.

3. QR 코드를 생성하려면 `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` 필드에 체크섬을 입력합니다. 예:

```
1 {
2
3   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
   zenprise/com.zenprise.configuration.AdminFunction",
4   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "
   qn7oZUtheu3JBainzZRrrjCQv6L006Ll10jcxT3-yKM",
5   "android.app.extra.
   PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
   play.google.com/managed/downloadManagingApp?identifier=xenmobile",
6   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
```

```

7
8     "serverURL": "https://supportability.xm.cloud.com"
9     }
10
11 }
12
13 <!--NeedCopy-->

```

사용된 라이브러리 Provisioning Tool 의 소스 코드에는 다음과 같은 라이브러리가 사용되었습니다.

- Apache 라이선스 2.0 에 따라 Google 이 제작한 v7 appcompat 라이브러리, 디자인 지원 라이브러리 및 v7 [appcompat](#) 라이브러리
자세한 내용은 [지원 라이브러리 기능 가이드](#)를 참조하십시오.
- Apache 라이선스 2.0 에 따라 Jake Wharton 이 제작한 [Butter Knife](#)

QR 코드를 사용하여 장치 등록

QR 코드를 사용하여 완전하게 관리되는 장치를 등록하려면 JSON 을 생성하고 JSON 을 QR 코드로 변환하여 QR 코드를 생성합니다. QR 코드가 장치 카메라로 스캔되어 장치가 등록됩니다.

시스템 요구 사항

- Android 9.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.

JSON 에서 **QR** 코드 생성 다음 필드를 사용하여 JSON 을 생성합니다.

다음 필드는 필수입니다.

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

값: com.zenprise/com.zenprise.configuration.AdminFunction

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

값: qn7oZUtheu3JBainzZRrjCQv6LOO6Ll10jcxT3-yKM

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

값: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>

다음 필드는 선택 사항입니다.

- **android.app.extra.PROVISIONING_LOCALE:** 언어 및 국가 코드를 입력합니다.

언어 코드는 [ISO 639-1](#)에 정의된 대로 소문자 두 자로 구성된 ISO 언어 코드입니다 (예: en). 국가 코드는 [ISO 3166-1](#)에 정의된 대로 대문자 두 자로 구성된 ISO 국가 코드입니다 (예: US). 예를 들어, 미국에서 사용하는 영어의 경우 en_US 를 입력합니다.

- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가 실행되고 있는 표준 시간대입니다.

[지역/위치 형식의 Olson 이름](#)을 입력합니다. 예를 들어 태평양 표준시의 경우 America/Los_Angeles 를 입력합니다. 입력하지 않으면 표준 시간대가 자동으로 입력됩니다.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Epoch 이후의 시간 (밀리초) 입니다.

Unix Epoch(즉 Unix 시간 또는 POSIX 시간 Unix 타임스탬프) 는 1970 년 1 월 1 일 (자정 UTC/GMT) 이후 경과한 시간이며, 윤초는 계산되지 않습니다 (ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 프로필 생성 시 암호화를 건너뛰려면 **true** 로 설정합니다. 프로필 생성 시 암호화를 적용하려면 **false** 로 설정합니다.

일반적인 JSON 은 다음과 같은 형식입니다.

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": " ",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

JSON 유효성 검사 도구 (예: <https://jsonlint.com>) 를 사용하여 생성된 JSON 의 유효성을 검사하고 온라인 QR 코드 생성기 (예: <https://www.qr-code-generator.com>) 를 사용하여 해당 JSON 문자열을 QR 코드로 변환합니다.

이 QR 코드는 공장 기본값으로 재설정된 장치에서 스캔되어 해당 장치를 완전 관리형 장치로 등록하는 데 사용됩니다.

장치를 등록하려면 새 장치 또는 공장 기본값으로 재설정된 장치의 전원을 켜 후:

1. 시작 화면에서 화면을 6 번 눌러 QR 코드 등록 흐름을 시작합니다.
2. 메시지가 표시되면 Wi-Fi 에 연결합니다. QR 코드에 있는 Secure Hub 의 다운로드 위치 (JSON 으로 인코딩됨) 는 이 Wi-Fi 네트워크를 통해 액세스할 수 있습니다.
장치가 Wi-Fi 에 연결되면 Google 에서 QR 코드 판독기를 다운로드하고 카메라를 시작합니다.
3. 카메라로 QR 코드를 가리키고 코드를 스캔합니다.

Android 는 QR 코드에 있는 다운로드 위치에서 Secure Hub 를 다운로드하고 서명 인증서 서명의 유효성을 검사한 후 Secure Hub 를 설치하고 장치 소유자로 설정합니다.

자세한 내용은 Android EMM 개발자용 Google 가이드 (https://developers.google.com/android/work/prov-devices#qr_code_method) 를 참조하십시오.

제로 터치 등록

제로 터치 등록을 사용하면 장치 전원을 처음 켤 때 완전 관리형 장치로 프로비전하도록 설정할 수 있습니다.

장치에 구성을 적용할 때 사용할 수 있는 온라인 도구인 Android 제로 터치 포털에서 장치 리셀러를 통해 계정을 만들 수 있습니다. 그런 다음 Android 제로 터치 포털에서 하나 이상의 제로 터치 등록 구성을 만들고 계정에 할당된 장치에 구성을 적용합니다. 사용자가 이러한 장치의 전원을 켜면 장치가 자동으로 XenMobile 에 등록됩니다. 장치에 할당된 구성에 따라 자동 등록 프로세스가 정의됩니다.

시스템 요구 사항

- 제로 터치 등록에 대한 지원은 Android 9.0 부터 시작됩니다.

리셀러의 장치 및 계정 정보

- 제로 터치 등록이 가능한 장치는 엔터프라이즈 리셀러 또는 Google 파트너로부터 구입할 수 있습니다. Android Enterprise 제로 터치 파트너 목록은 [Android 웹사이트](#)를 참조하십시오.
- 리셀러를 통해 만든 Android Enterprise 제로 터치 포털 계정.
- 리셀러가 제공하는 Android Enterprise 제로 터치 포털 계정 로그인 정보.

제로 터치 구성 만들기 제로 터치 구성을 만들 때는 구성 세부 정보를 지정하는 사용자 지정 JSON 을 포함합니다.

이 JSON 을 사용하여 지정된 XenMobile Server 에 등록할 장치를 구성합니다. 이 예에서는 'URL' 을 서버의 URL 로 대체하십시오.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6              "serverURL": "URL",
7          }
8      }
9
10
11 <!--NeedCopy-->
```

매개 변수가 더 많은 선택적 JSON 을 사용하여 구성을 추가로 사용자 지정할 수 있습니다. 이 예에서는 XenMobile Server 와 이 구성을 사용하는 장치가 서버에 로그인할 때 사용하는 사용자 이름과 암호를 지정합니다.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6              "serverURL": "URL",
```

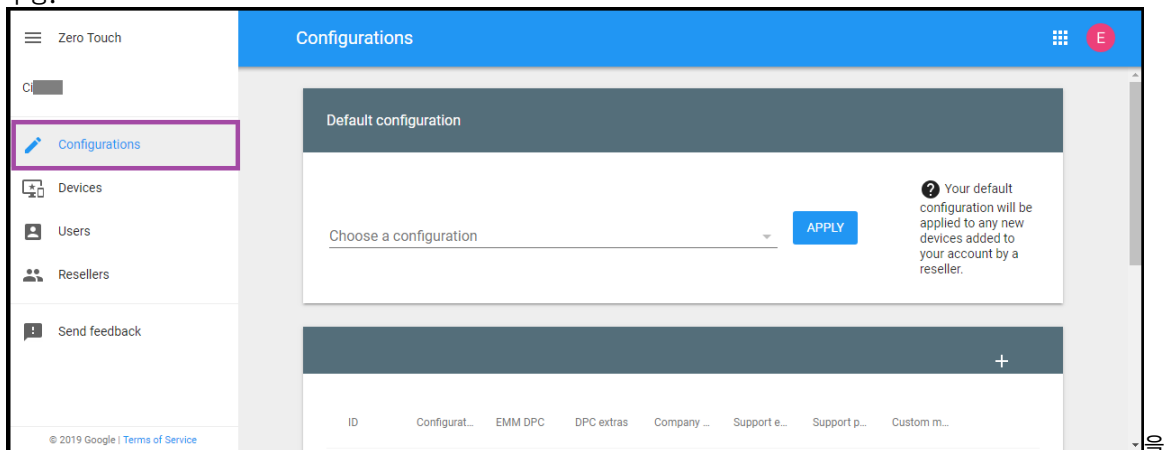
```

7         "xm_username": "username",
8         "xm_password": "password"
9     }
10
11 }
12
13 <!--NeedCopy-->

```

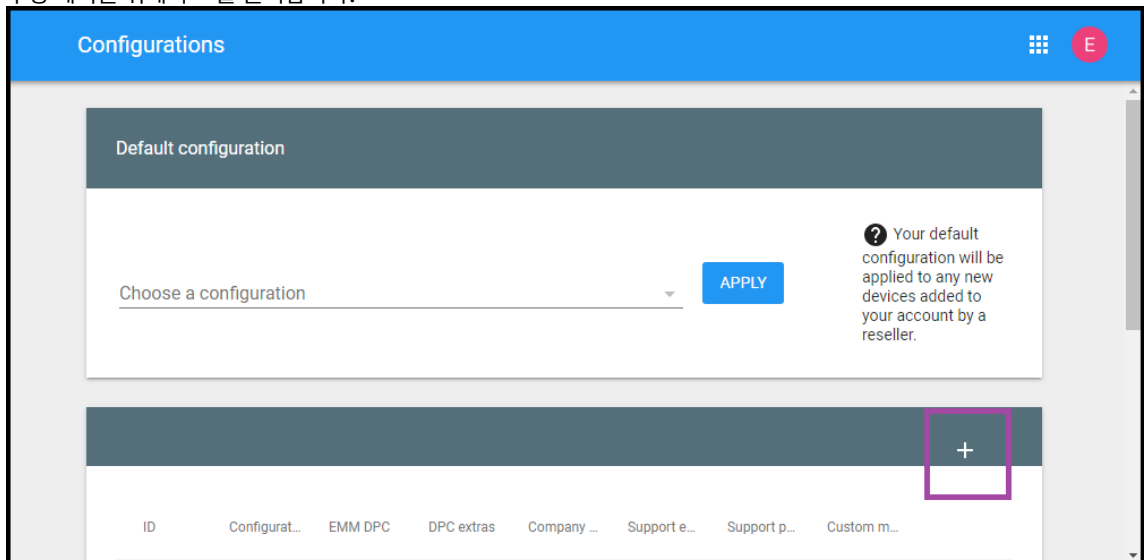
1. <https://partner.android.com/zerotouch>에서 Android 제로 터치 포털로 이동합니다. 제로 터치 장치 리셀러의 계정 정보를 사용하여 로그인합니다.

2. 구성.



클릭합니다.

3. 구성 테이블 위에서 + 를 클릭합니다.



4. 구성 창이 표시되면 구성 정보를 입력합니다.

- **Configuration name**(구성 이름): 이 구성에 대해 선택한 이름을 입력합니다.
- **EMM DPC: Citrix Secure Hub** 를 선택합니다.
- **DPC extras**(DPC 추가 항목): 이 필드에 사용자 지정 JSON 텍스트를 붙여 넣습니다.
- **Company name**(회사 이름): 장치 프로비전 중에 Android Enterprise 제로 터치 장치에 표시할 이름을 입력합니다.
- **Support email address**(지원 전자 메일 주소): 사용자가 지원을 문의할 수 있는 전자 메일 주소를 입력합니다.

다. 이 주소는 장치 프로비전 전에 Android Enterprise 제로 터치 장치에 나타납니다.

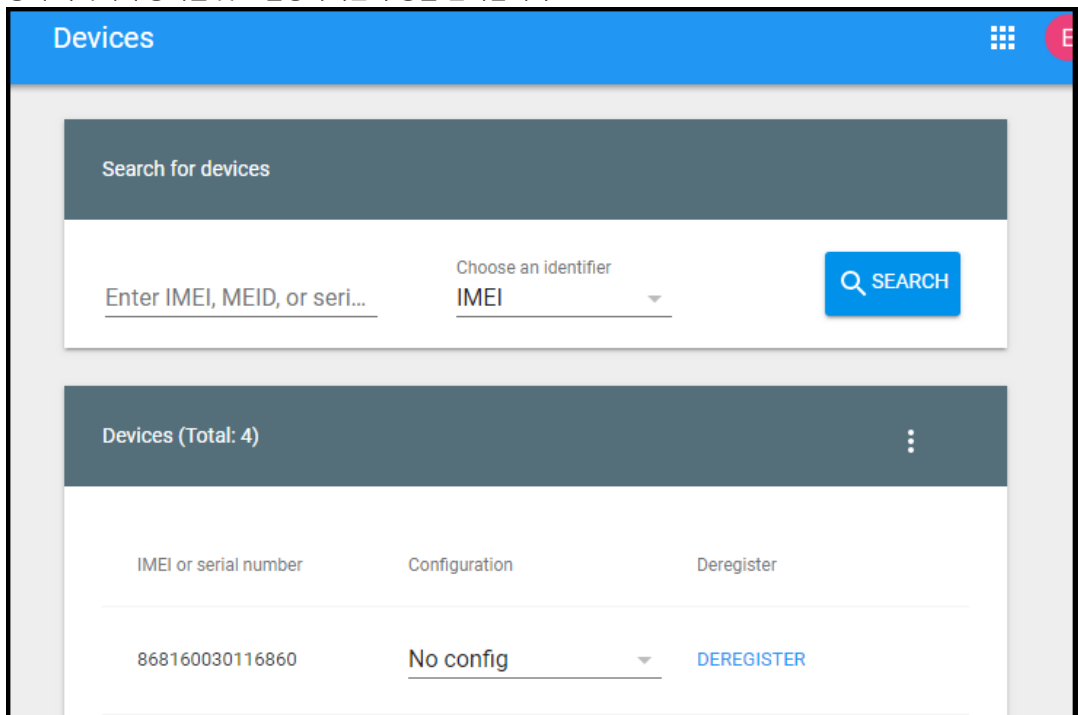
- **Support phone number(지원 전화 번호):** 사용자가 지원을 문의할 수 있는 전화 번호를 입력합니다. 이 전화 번호는 장치 프로비전 전에 Android Enterprise 제로 터치 장치에 나타납니다.
- **Custom Message(사용자 지정 메시지):** 필요에 따라 사용자가 문의하는 데 도움이 되거나 사용자에게 장치에 대한 추가 정보를 제공하는 데 도움이 되는 하나 또는 두 개의 문장을 추가합니다. 이 사용자 지정 메시지는 장치 프로비전 전에 Android Enterprise 제로 터치 장치에 나타납니다.

5. 추가를 클릭합니다.

6. 구성을 추가로 만들려면 2~4 단계를 반복합니다.

7. 장치에 구성을 적용하려면:

- a) Android 제로 터치 포털에서 **Devices(장치)** 를 클릭합니다.
- b) 장치 목록에서 장치를 찾고 할당하려는 구성을 선택합니다.



- c) **Update(업데이트)** 를 클릭합니다.

CSV 파일을 사용하여 여러 장치에 구성을 적용할 수 있습니다.

여러 장치에 구성을 적용하는 방법에 대한 자세한 내용은 Android Enterprise 도움말 항목 [IT 관리자를 위한 제로 터치 등록](#)을 참조하십시오. 이 Android Enterprise 도움말 항목에는 구성을 관리하고 장치에 구성을 적용하는 방법에 대한 자세한 정보가 나와 있습니다.

전용 **Android Enterprise** 장치 프로비전

전용 Android Enterprise 장치는 단일 사용 사례를 이행하는 데 전용으로 사용되는 완전 관리형 장치입니다. 전용 장치를 COSU(회사 소유 일회 사용) 장치라고도 합니다. 이러한 장치는 이 사용 사례에 필요한 작업을 수행하는 데 필요한 단일 앱 또는 소수의 앱으로 제한되어야 합니다. 또한 사용자가 장치에서 다른 앱을 사용하도록 설정하거나 다른 작업을 수행하지 못하도록 차단해야 합니다.

Android Enterprise 로 완전히 관리되는 장치 프로비저닝에 설명된 대로 완전 관리되는 다른 장치에 사용되는 등록 방법 중 하나를 사용하여 전용 장치를 등록합니다. 전용 장치를 프로비전하려면 등록하기 전에 추가 설정이 필요합니다.

전용 장치를 프로비전하려면:

- XenMobile 배포에 전용 장치를 등록할 수 있도록 허용하는 XenMobile 관리자용 등록 프로필을 추가합니다. 등록 프로필 만들기를 참조하십시오.
- 전용 장치에서 액세스할 앱을 허용합니다.
- 필요한 경우 작업 잠금 모드를 허용하도록 허용된 앱을 설정합니다. 앱이 작업 잠금 모드에 있으면 사용자가 앱을 열 때 앱이 장치 화면에 고정됩니다. 홈 단추가 나타나지 않고 뒤로 단추가 비활성화됩니다. 사용자는 로그아웃과 같이 앱에 프로그래밍된 작업을 사용하여 앱을 종료할 수 있습니다.
- 추가한 등록 프로필로 각 장치를 등록합니다.

시스템 요구 사항

- 전용 장치 등록 지원은 Android 6.0 부터 시작됩니다.

앱 허용 및 작업 잠금 모드 설정

키오스크 장치 정책을 사용하면 앱을 허용하고 작업 잠금 모드를 설정할 수 있습니다. 기본적으로 Secure Hub 와 Google Play 서비스는 허용됩니다.

키오스크 정책을 추가하려면:

1. XenMobile 콘솔에서 구성 > 장치 정책을 클릭합니다. 장치 정책 페이지가 나타납니다.
2. 추가를 클릭합니다. 새 정책 추가 대화 상자가 나타납니다.
3. 자세히를 확장한 후 보안 아래에서 키오스크를 클릭합니다. 키오스크 정책 페이지가 나타납니다.
4. 플랫폼에서 **Android Enterprise** 를 선택합니다. 다른 플랫폼을 지웁니다.
5. 정책 정보 창에서 정책 이름과 필요한 경우 설명을 입력합니다.
6. 다음을 클릭한 후 추가를 클릭합니다.
7. 앱을 허용하고 해당 앱에 대한 작업 잠금 모드를 허용 또는 거부하려면:
 - 목록에서 허용할 앱을 선택합니다.

사용자가 앱을 시작할 때 장치 화면에 앱이 고정되도록 설정하려면 허용을 선택합니다. 앱이 고정되지 않도록 설정하려면 거부를 선택합니다. 기본값은 허용입니다.

Kiosk Policy

This policy lets you whitelist apps onto a Kiosk for Corporate Owned Single Use devices. If an app supports lock task mode and when lock task status of that app is set to allow, it will get pinned to the screen on the device.

Allowed apps

Apps to whitelist *	Lock task status	
Cosu App	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

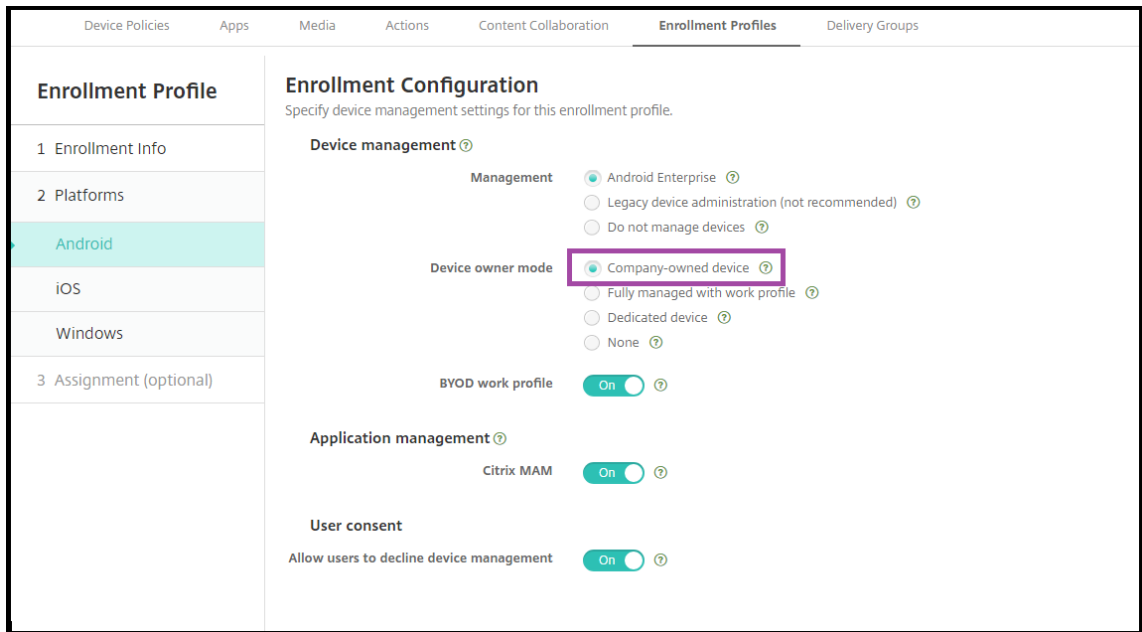
► **Deployment Rules**

Back Next >

8. 저장을 클릭합니다.
9. 다른 앱을 허용하고 해당 앱에 대한 작업 잠금 모드를 허용 또는 거부하려면 추가를 클릭합니다.
10. 배포 규칙을 구성하고 배포 그룹을 선택합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

장치를 등록하려면

1. 다음을 클릭하거나 플랫폼에서 **Android** 를 선택합니다. 등록 구성 페이지가 나타납니다.
2. 관리를 **Android Enterprise** 로 설정합니다.
3. 장치 소유자 모드를 기업 소유 장치로 설정합니다.



4. 할당 (옵션) 을 선택합니다. 배달 그룹 할당 화면이 나타납니다.

5. 전용 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장을 클릭합니다.

등록 프로필에서 **BYOD** 작업 프로필을 설정하면 신규 장치가 아니거나 공장 기본값으로 재설정되지 않은 장치가 작업 프로필 장치로 등록됩니다. [Android Enterprise 작업 프로필 장치 프로비전](#)을 참조하십시오.

작업 프로필이 있는 완전 관리형 **Android Enterprise** 장치 (COPE 장치) 프로비전

작업 프로필로 완전히 관리되는 장치 (이전의 COPE 장치) 는 업무용 및 개인용으로 사용되는 회사 소유의 장치입니다. 전체 장치는 조직에서 관리합니다. 하나의 정책 집합을 장치에 적용하고 개별 정책 집합을 작업 프로필에 적용할 수 있습니다.

XenMobile 콘솔에서 작업 프로필로 완전히 관리되는 장치는 다음과 같은 용어로 표시됩니다.

- 장치 소유권은 “회사” 입니다.
- 장치 Android Enterprise 설치 유형은 “회사 소유 개인 사용” 입니다.

시스템 요구 사항

- 작업 프로필로 완전히 관리되는 장치의 등록은 Android 9.0 부터 Android 10.x 까지 지원됩니다.

작업 프로필로 완전히 관리되는 장치에 대한 등록 프로필 추가

작업 프로필로 완전히 관리되는 장치의 등록을 위한 등록 프로필을 만듭니다. 이 등록 프로필에 할당된 배달 그룹의 관리자는 완전 관리형 장치를 작업 프로필에 등록할 수 있습니다. 이러한 관리자가 필요한 모든 장치를 등록할 수 있도록 하려면 사용자당 무제한

의 장치가 허용되는 관리자용 등록 프로필을 만듭니다. 작업 프로필로 완전히 관리되는 장치를 등록하는 관리자가 포함된 배달 그룹에 이 프로필을 할당합니다.

1. XenMobile 콘솔에서 구성 > 등록 프로필로 이동합니다.
2. 등록 프로필을 추가하려면 추가를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수가 무제한으로 설정되어 있는지 확인합니다.
3. 다음을 클릭하거나 플랫폼에서 **Android Enterprise** 를 선택합니다. 등록 구성 페이지가 나타납니다.
4. 등록 유형을 다음 중 하나로 설정합니다.
 - **완전 관리형 프로필/작업 프로필:** 새 장치 또는 공장 기본값으로 재설정된 장치가 완전 관리형 장치로 등록됩니다. BYOD 장치는 사용자가 관리하는 작업 프로필을 통해서만 등록됩니다.
 - **COPE/작업 프로필:** 새 장치 또는 공장 기본값으로 재설정된 장치가 작업 프로필을 사용하여 완전 관리형 장치로 등록됩니다. BYOD 장치는 사용자가 관리하는 작업 프로필을 통해서만 등록됩니다.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ⓘ Management <ul style="list-style-type: none"> <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ Device owner mode <ul style="list-style-type: none"> <input checked="" type="radio"/> Company-owned device ⓘ <input type="radio"/> Fully managed with work profile ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ BYOD work profile <input checked="" type="checkbox"/> ⓘ Application management ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ User consent <ul style="list-style-type: none"> Allow users to decline device management <input checked="" type="checkbox"/> ⓘ
Android	
iOS	
3 Assignment (optional)	

5. 할당 (선택 사항) 을 선택하거나 다음을 클릭합니다. 배달 그룹 할당 화면이 나타납니다.
 6. 전용 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장을 클릭합니다.
- 추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.

Enrollment Profiles				
Add				
<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	COPE devices	11/1/19 1:01:51 pm	11/1/19 1:01:51 pm	unlimited
<input type="checkbox"/>	Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited

Showing 1 - 2 of 2 items Items per page: 10

사용자가 등록 프로필이 다른 여러 배달 그룹에 속하는 경우 사용되는 등록 프로필은 배달 그룹의 이름에 따라 결정됩니다. XenMobile 은 사전순으로 표시된 배달 그룹 목록의 마지막에 나타나는 배달 그룹을 선택합니다.

장치를 등록하려면

새 장치 또는 공장 기본값으로 재설정된 장치는 DPC 식별자 토큰, NFC(근거리 통신) 범프 또는 QC 코드 방법을 사용하여 작업 프로파일로 완전히 관리되는 장치로 등록됩니다. Citrix DPC 식별자 토큰을 사용하여 장치 등록, NFC 범프를 사용하여 장치 등록 또는 QR 코드를 사용하여 장치 등록을 참조하십시오.

새 장치 또는 공장 기본값으로 재설정된 장치는 [Android Enterprise 작업 프로파일 장치 프로비저닝](#)에 설명된 대로 작업 프로파일 장치로 등록됩니다.

XenMobile 콘솔에서 Android Enterprise 장치 보기

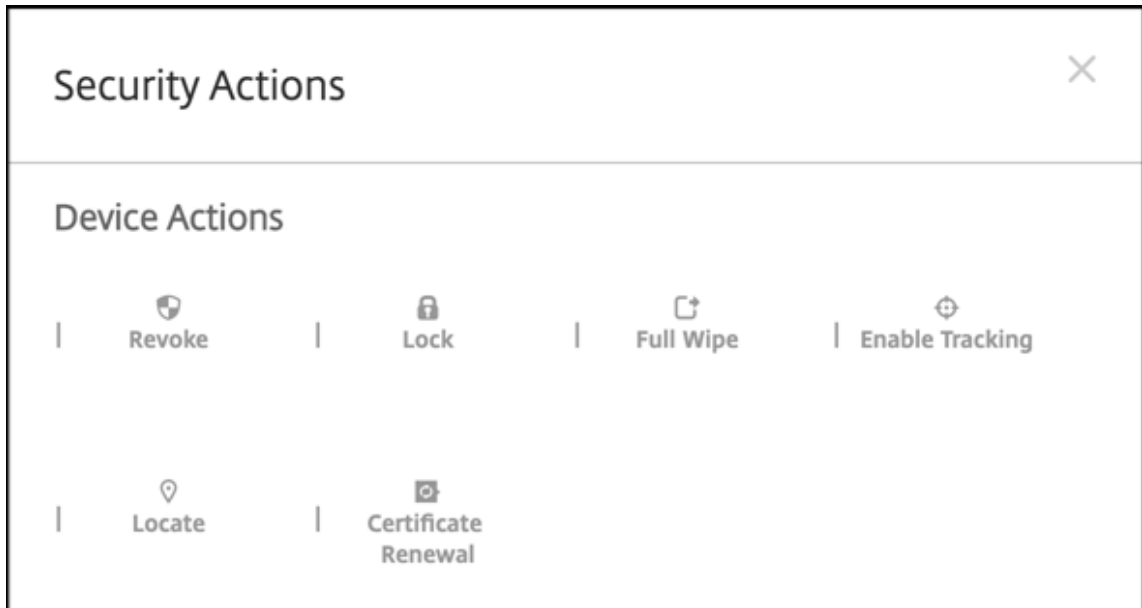
1. XenMobile 콘솔에서 관리 > 장치로 이동합니다.
2. 이 페이지의 테이블 오른쪽에 있는 메뉴를 클릭하여 **Android Enterprise** 에서 활성화된 장치? 열을 추가합니다.

Enrolled Devices Device Whitelist									
Use the Endpoint Management Analyzer to analyze and troubleshoot issues with your Endpoint Management environment.									
Add Import Export Refresh									
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Android Enterprise Enabled Device?
<input type="checkbox"/>		MDM	mbbowlin "mbbowlin"	iOS			5/7/19 1:01:50 pm	33 days	<input checked="" type="checkbox"/> Status <input checked="" type="checkbox"/> Mode <input checked="" type="checkbox"/> User name <input checked="" type="checkbox"/> Inactivity days <input type="checkbox"/> Shareable <input type="checkbox"/> Shared status <input type="checkbox"/> DEP registered <input type="checkbox"/> Apple bulk-enrolled <input type="checkbox"/> ASM DEP device type <input type="checkbox"/> ASM DEP shared <input type="checkbox"/> ASM logged-in user <input type="checkbox"/> ASM resident users <input type="checkbox"/> Administrator disabled <input type="checkbox"/> Amazon MDM API available <input type="checkbox"/> Android Enterprise Device ID <input checked="" type="checkbox"/> Android Enterprise Enabled Device?
<input type="checkbox"/>		MDM MAM	testing2 "testing2"	Android	9	Pixel XL	6/10/19 8:06:51 am	0 day	

Showing 1 - 2 of 2 items Items per page: 10

3. 사용 가능한 보안 동작을 보려면 완전 관리형 장치를 선택하고 보안을 클릭합니다. 장치가 완전 관리형 경우 전체 초기화 작업을 사용할 수 있지만 선택적 초기화는 사용할 수 없습니다. 이 차이는 장치가 관리되는 Google Play Store 의 앱만

허용하기 때문입니다. 사용자가 공용 스토어에서 응용 프로그램을 설치할 수 있는 옵션은 없습니다. 장치의 모든 콘텐츠는 조직에서 관리합니다.



Android Enterprise 장치 및 앱 정책 구성

기기 및 앱 수준 모두에서 제어되는 정책에 대한 개요는 [Android Enterprise](#) 에서 [지원되는 기기 정책](#) 및 [MDX 정책](#) 을 참조하십시오.

정책에 대해 알아야 할 사항:

- **데이터 손실 방지:** XenMobile MAM 컨테이너 기술은 암호화 및 기타 모바일 DLP(데이터 손실 방지) 기술로 앱을 보호합니다. MDX 지원 앱에 대해 Citrix MAM SDK 또는 MDX Toolkit 을 사용합니다.
- **기기 제한:** 수십 가지 기기 제한을 통해 다음과 같은 기능을 제어할 수 있습니다.
 - 장치 카메라의 사용
 - 업무 및 개인 프로필 간 복사 및 붙여넣기 사용
- **앱별 VPN:** 관리되는 구성 장치 정책을 사용하여 Android Enterprise 용 VPN 프로ファイルを 구성합니다.
- **전자 메일 정책:** 관리되는 구성 장치 정책을 사용하여 앱을 구성하는 것이 좋습니다.

다음 표에는 Android Enterprise 장치에 사용할 수 있는 모든 장치 정책이 나열되어 있습니다.

중요:

Android Enterprise 에 등록하고 MDX 앱을 사용하는 장치의 경우: MDX 및 Android Enterprise 를 통해 일부 설정을 제어할 수 있습니다. MDX 에 대해 제한이 최소한인 정책 설정을 사용하고 Android Enterprise 를 통해 정책을 제어합니다.

Android Enterprise 앱 권한	관리되는 구성	앱 인벤토리
앱 제거	관리되는 앱 자동 업데이트	OS 업데이트 제어
자격 증명	사용자 지정 XML	Exchange
파일	Keyguard 관리	키오스크
위치	암호	제한 사항
Samsung MDM 라이선스 키	예약	Wi-Fi

XenMobile 옵션

작업 프로파일로 완전히 관리되는 장치의 장치 정책 (**COPE** 장치)

작업 프로파일로 완전히 관리되는 장치 (COPE 장치) 의 경우 일부 장치 정책을 사용하여 전체 장치와 작업 프로파일에 개별 설정을 적용할 수 있습니다. 다른 장치 정책을 사용하여 전체 장치에만 설정을 적용하거나 작업 프로파일로 완전히 관리되는 장치의 작업 프로파일에만 설정을 적용할 수 있습니다.

정책	적용 대상
Android Enterprise 앱 권한	작업 프로파일
관리되는 구성	작업 프로파일
앱 인벤토리	작업 프로파일
앱 제거	작업 프로파일
관리되는 앱 자동 업데이트	작업 프로파일
OS 업데이트 제어	해당 없음
자격 증명	작업 프로파일
사용자 지정 XML	해당 없음
Exchange	해당 없음
파일	작업 프로파일
Keyguard 관리	장치 및 작업 프로파일
키오스크	해당 없음
위치	장치 (위치 모드만 해당)
암호	장치 및 작업 프로파일

정책	적용 대상
제한 사항	장치 및 작업 프로필 (장치 및 작업 프로필에 대한 개별 정책 만 들기)
Samsung MDM 라이선스 키	해당 없음
예약	작업 프로필
Wi-Fi	장치
XenMobile 옵션	작업 프로필

[Android Enterprise](#) 의 지원되는 장치 정책 및 [MDX 정책](#) 및 [MAM SDK 개요](#)도 참조하십시오.

보안 동작

Android Enterprise 는 다음과 같은 보안 동작을 지원합니다. 각 보안 동작에 대한 설명은 [보안 동작](#)을 참조하십시오.

보안 동작	작업 프로필	완전 관리형
인증서 갱신	예	예
전체 초기화	아니요	예
찾기	예	예
잠금	예	예
Lock and Reset Password(잠금 및 암호 재설정)	아니요	예
Notify (Ring)(알림 (벨 울림))	예	예
해지	예	예
선택적 초기화	예	아니요

보안 동작 참고 사항

- 위치 장치 정책에서 장치에 대한 위치 모드를 높은 정확도 또는 배터리 절약으로 설정하지 않으면 찾기 보안 동작이 실패합니다. [위치 장치 정책](#)을 참조하십시오.
- Android 9.0 이전 버전의 Android 를 실행하는 작업 프로필 장치:
 - 잠금 및 암호 재설정 작업이 지원되지 않습니다.
- Android 9.0 이상인 작업 프로필 장치:

- 전송된 암호로 작업 프로필이 잠깁니다. 장치 자체는 잠기지 않습니다.
- 작업 프로필에 암호가 설정되지 않은 경우:
 - * 암호가 전송되지 않았거나 전송된 암호가 암호 요구 사항을 충족하지 않는 경우: 장치가 잠깁니다.
- 작업 프로필에 암호가 설정된 경우:
 - * 암호가 전송되지 않았거나 전송된 암호가 암호 요구 사항을 충족하지 않는 경우: 작업 프로필은 잠기지만 장치 자체는 잠기지 않습니다.
- 작업 프로파일로 완전히 관리되는 장치 (COPE 장치):
 - 장치 또는 작업 프로필에 잠금 보안 동작을 개별적으로 적용할 수 있습니다.

Android Enterprise 엔터프라이즈 등록 취소

Android Enterprise 엔터프라이즈를 더 이상 사용하지 않으려면 엔터프라이즈 등록을 취소하면 됩니다.

경고:

엔터프라이즈 등록이 취소되면 엔터프라이즈를 통해 이미 등록된 장치의 Android Enterprise 앱이 기본 상태로 재설정됩니다. Google 은 더 이상 장치를 관리하지 않습니다. 새로운 Android Enterprise 에 등록하는 경우 관리되는 Google Play 에서 새 조직의 앱을 승인해야 합니다. 그런 다음에야 XenMobile 콘솔에서 앱을 업데이트할 수 있습니다.

Android Enterprise 엔터프라이즈 등록 취소 후:

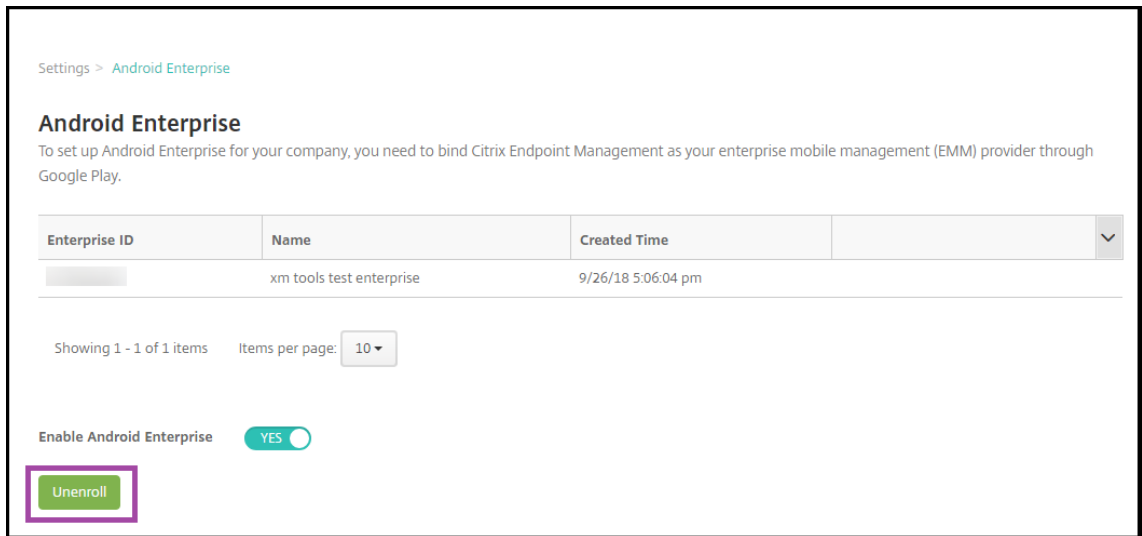
- 엔터프라이즈를 통해 등록된 장치 및 사용자의 Android Enterprise 앱이 기본 상태로 재설정됩니다. 이전에 적용된 관리되는 구성 정책은 더 이상 작업에 영향을 미치지 않습니다.
- XenMobile 은 엔터프라이즈를 통해 등록된 장치를 관리합니다. Google 의 관점에서 이러한 장치는 관리되지 않는 장치입니다. 새로운 Android Enterprise 앱을 추가할 수 없습니다. 관리되는 구성 정책을 적용할 수 없습니다. 예약, 암호 및 제한 같은 다른 정책을 이러한 장치에 적용할 수 있습니다.
- Android Enterprise 에 장치를 등록하려고 하면 Android Enterprise 장치가 아닌 Android 장치로 등록됩니다.

XenMobile Server 콘솔 및 XenMobile Tools 를 사용하여 Android Enterprise 엔터프라이즈를 등록 취소합니다.

이 작업을 수행하면 XenMobile 에서 XenMobile Tools 에 대한 팝업 창이 열립니다. 시작하기 전에 사용하는 브라우저에서 팝업 창을 여는 데 필요한 권한이 XenMobile 에 있는지 확인하십시오. Google Chrome 같은 일부 브라우저의 경우 팝업 차단을 사용하지 않도록 설정하고 XenMobile 사이트 주소를 팝업 차단 허용 목록에 추가해야 합니다.

Android Enterprise 엔터프라이즈를 등록 취소하려면:

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 설정 페이지에서 **Android Enterprise** 를 클릭합니다.
3. 등록 취소를 클릭합니다.



Android Enterprise 앱 배포

March 15, 2024

XenMobile 은 장치에 배포되는 앱을 관리합니다. 다음 유형의 Android Enterprise 앱을 구성하고 배포할 수 있습니다.

- **관리되는 앱 스토어 앱:** 이러한 앱으로는 관리되는 Google Play 스토어에서 이용할 수 있는 무료 앱이 있습니다. 예를 들어 GoToMeeting 이 포함됩니다.
- **MDX:** MAM SDK 로 준비되거나 MDX Toolkit 으로 래핑되는 앱입니다. 이러한 앱에는 MDX 정책이 포함됩니다. 내부 및 공용 스토어에서 MDX 앱을 얻을 수 있습니다. Citrix 모바일 생산성 앱을 MDX 앱으로 배포합니다.
- **Enterprise:** 직접 개발하거나 다른 출처에서 획득한 개인 앱입니다. 이러한 앱은 관리되는 Google Play 스토어를 통해 사용자에게 제공합니다. 관리되는 Google Play 스토어는 Google 엔터프라이즈 앱 스토어입니다.
- **MDX 지원 개인 앱:** MAM SDK 로 준비되거나 MDX Toolkit 으로 래핑된 엔터프라이즈 앱입니다.

엔터프라이즈 앱과 MDX 지원 개인 앱을 두 가지 방식으로 추가할 수 있습니다.

- 이 문서의 엔터프라이즈 앱 및 MDX 지원 개인 앱 섹션에 설명된 대로 XenMobile 콘솔에 앱을 엔터프라이즈 앱으로 추가합니다.
- Google 개발자 계정을 사용하여 관리되는 Google Play 스토어에 앱을 직접 게시합니다. 그런 다음 XenMobile 콘솔에 앱을 관리되는 앱 스토어 앱으로 추가합니다. 관리되는 앱 스토어 앱을 참조하십시오.

Google 개발자 계정을 사용하여 앱을 게시한 다음 XenMobile 콘솔 사용으로 전환할 경우 앱의 소유권이 달라집니다. 이 경우 두 위치 모두에서 앱을 관리합니다. Citrix에서는 한 가지 방법으로 앱을 추가하는 것을 권장합니다.

관리되는 Google Play 스토어에서 자체 관리 앱을 제거해야 하는 경우 Google 에 티켓을 개시합니다. 개발자가 관리되는 Google Play 스토어에서 앱을 비활성화할 수는 있지만 삭제할 수는 없습니다.

다음 섹션에서는 Android Enterprise 앱 구성에 대해 더 자세히 알아봅니다. 앱 배포에 관한 자세한 내용은 [앱 추가](#)를 참조하십시오. 이 문서에는 다음이 포함됩니다.

- 웹 및 SaaS 앱 또는 웹 링크를 추가하는 일반적인 워크플로
- 엔터프라이즈 및 공용 스토어 앱을 위한 필수 앱 워크플로
- 엔터프라이즈 앱용 Citrix CDN(콘텐츠 배달 네트워크)에서 엔터프라이즈 앱을 제공하는 방법

관리되는 앱 스토어 앱

관리되는 Google Play 스토어에서 무료로 제공되는 앱을 XenMobile에 추가할 수 있습니다.

참고:

관리되는 Google Play에서도 Google Play 스토어의 모든 앱에 액세스할 수 있게 만들려면 관리되는 **Google Play** 스토어의 모든 앱에 액세스 서버 속성을 사용합니다. [서버 속성](#)을 참조하십시오. 이 속성을 **true**로 설정하면 모든 Android Enterprise 사용자가 공용 Google Play 스토어 앱에 액세스할 수 있습니다. 이후 [제한 장치 정책](#)을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다.

1 단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 추가를 클릭합니다.
2. 공용 앱 스토어를 클릭합니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

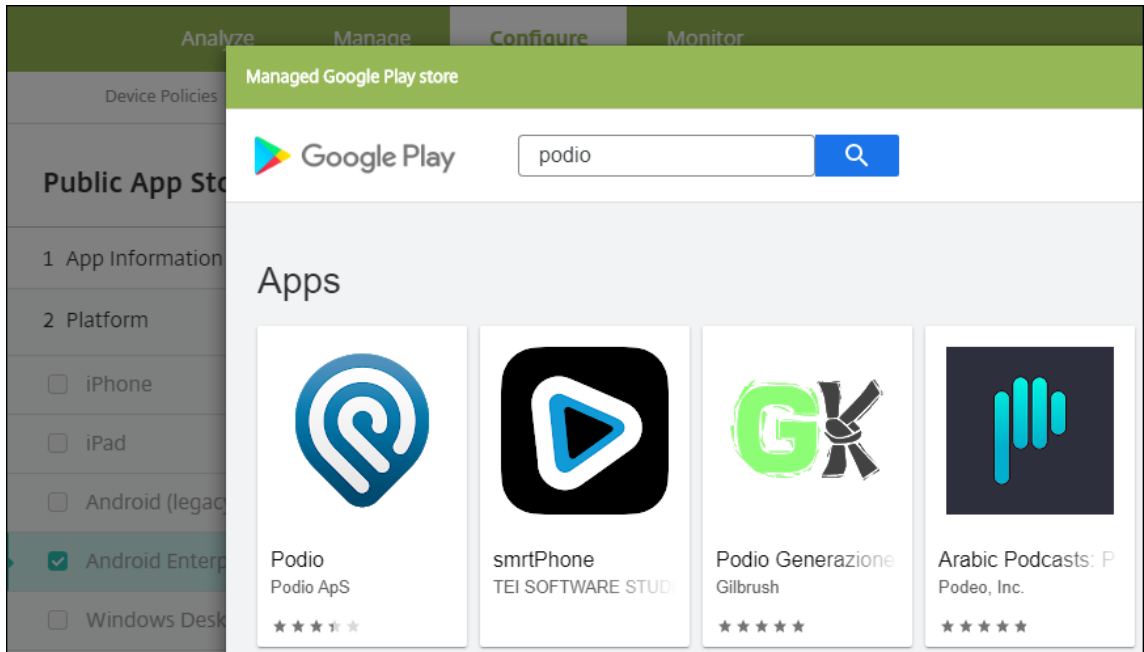
3. 앱 정보 창에서 다음 정보를 입력합니다.

- 이름: 앱을 설명하는 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 표시됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.

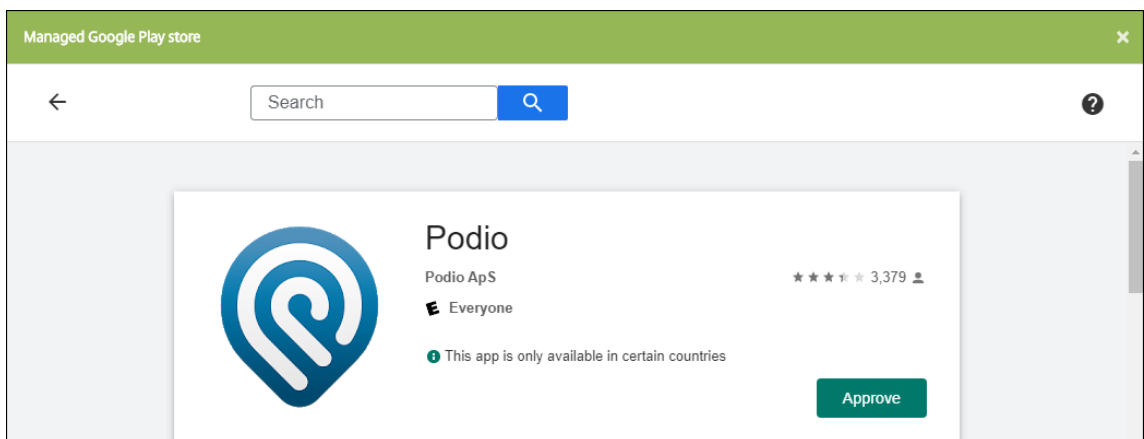
- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 정보](#)를 참조하십시오.

4. 플랫폼으로 **Android Enterprise** 를 선택합니다.

5. 검색 상자에 앱 이름 또는 패키지 ID 를 입력하고 검색을 클릭합니다. Google Play Store 에서 패키지 ID 를 찾을 수 있습니다. ID 는 앱의 URL 에 있습니다. 예를 들어 **com.Slack**은 https://play.google.com/store/apps/details?id=com.Slack&hl=en_US의 패키지 ID 입니다.




6. 검색 기준과 일치하는 앱이 표시됩니다. 원하는 앱을 클릭한 다음 승인을 클릭합니다.



7. **Approve(승인)** 를 다시 클릭합니다.

8. **Keep approved when app requests new permissions(앱이 새 권한을 요청할 때 승인된 상태로 유지)** 를 선택합니다. 저장을 클릭합니다.

APPROVAL SETTINGS
NOTIFICATIONS



Citrix Files
 Citrix

How would you like to handle new app permission requests?

☒ **Keep approved when app requests new permissions.**
Users will be able to install the updated app.

☐ **Revoke app approval when this app requests new permissions.**
App will be removed from the store until it is reapproved.

CANCEL
SAVE

9. 앱 아이콘을 클릭하고 앱 이름 및 설명을 구성합니다.


Public App Store

- 1 App Information
- 2 Platform Clear All
 - ☐ iPhone
 - ☐ iPad
 - ☐ Android (legacy DA)
 - ☒ **Android Enterprise**
 - ☐ Windows Desktop/Tablet
 - ☐ Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

Managed Google Play
Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

Search

Search results for com.podio in Managed Google Play



Podio
Podio ApS

Didn't find the app you were looking for?

App Details

Name *


Description *

Product track

Version

Package ID

Image

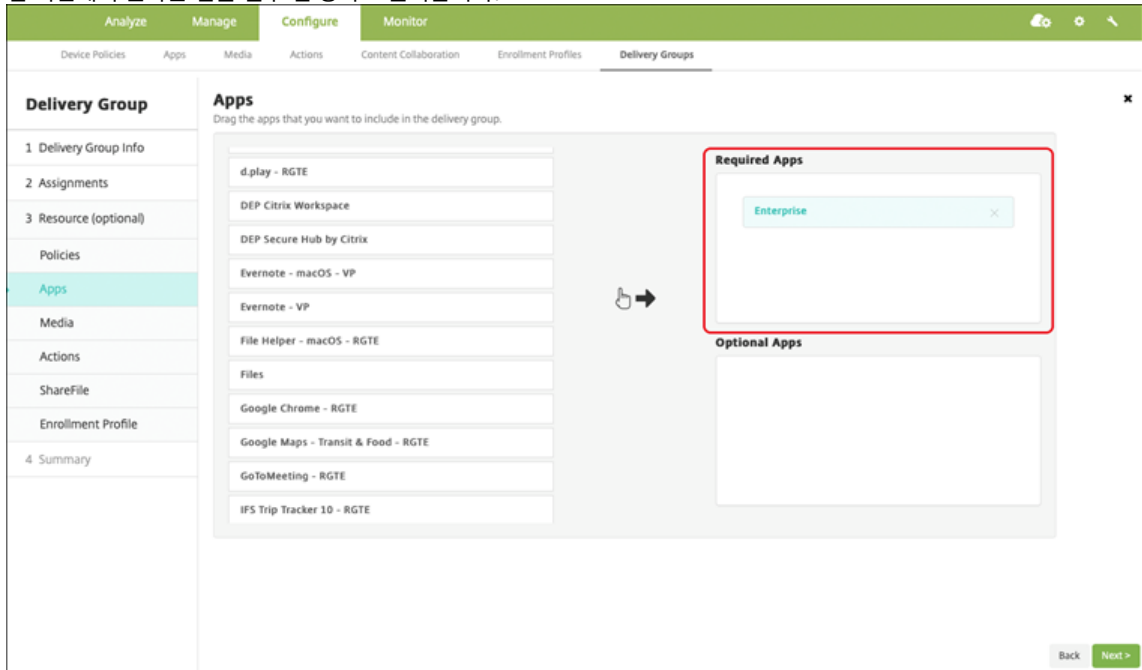


10. 앱에 배달 그룹을 할당하고 저장을 클릭합니다. 자세한 내용은 [리소스 배포](#)를 참조하십시오.

2 단계: 앱 배포 구성

1. 구성 > 배달 그룹으로 이동한 다음 구성한 배달 그룹을 선택합니다. 편집을 클릭합니다.

2. 앱 섹션에서 원하는 앱을 필수 앱 상자로 끌어옵니다.



3. 요약 페이지에서 저장을 클릭합니다.

4. 배달 그룹 페이지에서 배달 그룹을 선택하고 배포를 클릭합니다.

MDX 앱

XenMobile 에 MDX 파일을 추가하고 앱 세부 정보와 정책 설정을 구성합니다. Android Enterprise 에 대해 Citrix 모바일 생산성 앱을 구성하려면 MDX 앱으로 추가합니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

- [MAM SDK Overview\(MAM SDK 개요\)](#)
- [MDX 정책 요약](#)

1 단계: 앱 추가 및 구성

1. Citrix 모바일 생산성 앱의 경우 공용 스토어 MDX 파일을 다운로드하고 <https://www.citrix.com/downloads>로 이동합니다. **Citrix Endpoint Management(XenMobile) > Citrix Endpoint Management** 생산성 앱으로 이동합니다.

다른 MDX 앱 유형의 경우 MDX 파일을 가져옵니다.

2. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. **MDX** 를 클릭합니다. **MDX** 앱 정보 페이지가 나타납니다. 앱 정보 창에서 다음 정보를 입력합니다.

- 이름: 앱을 설명하는 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 표시됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.
- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 정보](#)를 참조하십시오.

4. 플랫폼으로 **Android Enterprise** 를 선택합니다.

5. 업로드를 클릭하고 MDX 파일로 이동합니다. Android Enterprise 는 MAM SDK 또는 MDX Toolkit 으로 준비한 앱만 지원합니다.

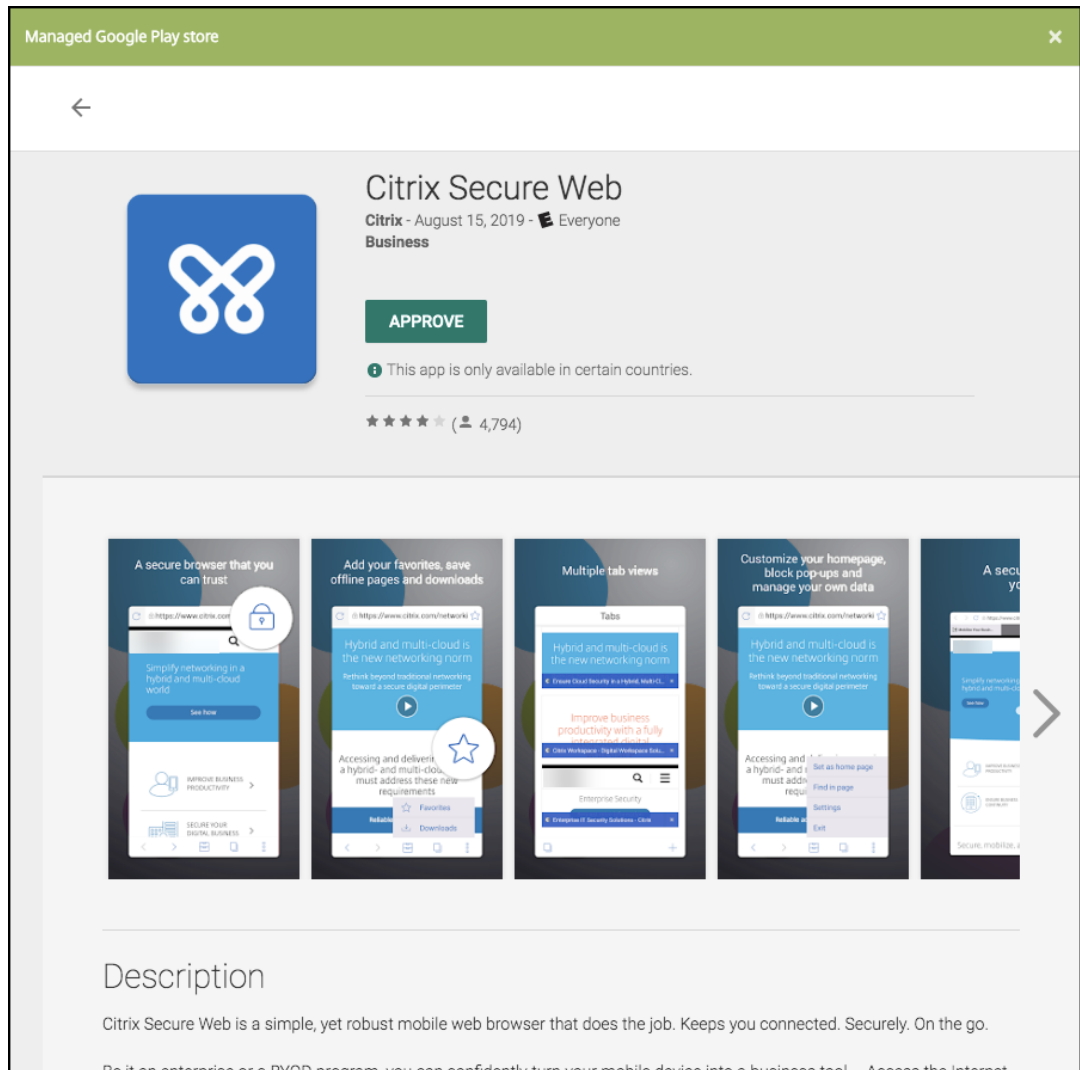
- 연결된 응용 프로그램에 관리되는 Google Play Store 의 승인이 필요한 경우 UI 에 알림이 표시됩니다. XenMobile 콘솔을 종료하지 않고 응용 프로그램을 승인하려면 예를 클릭합니다.

App is not approved

App is not approved on the managed Google Play store. You can approve the app now or later. Do you want to approve it now?

No
Yes

관리되는 Google Play Store 가 열리면 지침에 따라 앱을 승인하고 저장합니다.



앱이 성공적으로 추가되면 앱 세부 정보 페이지가 나타납니다.

6. 다음 설정을 구성합니다.

- **파일 이름:** 앱에 연결된 파일 이름을 입력합니다.
- **앱 설명:** 앱에 대한 설명을 입력합니다.
- **앱 버전:** 필요한 경우 앱 버전 번호를 입력합니다.
- **패키지 ID:** 관리되는 Google Play 스토어에서 가져온 앱의 패키지 ID 를 입력합니다.
- **최소 OS 버전:** 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
- **최대 OS 버전:** 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
- **제외된 장치:** 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

7. MDX 정책을 구성합니다. MDX 정책은 플랫폼별로 다르며 인증, 장치 보안 및 앱 제한 등 정책 영역에 대한 옵션이 포함됩니다. 콘솔에서 각 정책에는 정책을 설명하는 도구 설명이 포함됩니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

- [MAM SDK Overview\(MAM SDK 개요\)](#)
- [MDX 정책 요약](#)

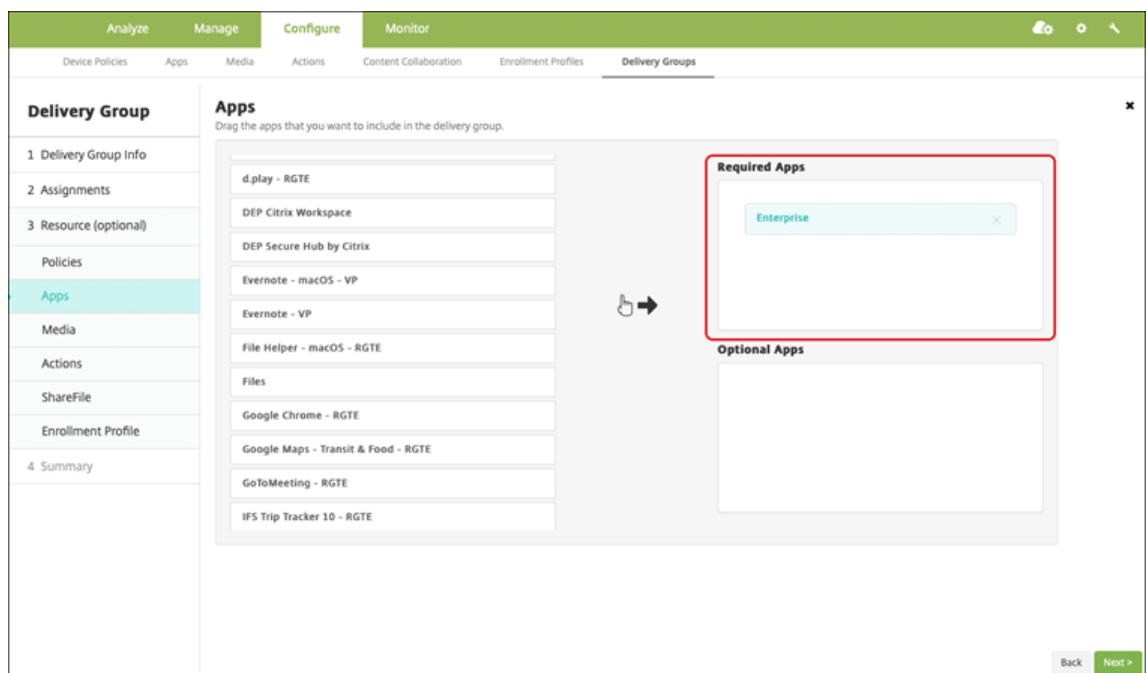
8. 배포 규칙 및 저장소 구성을 구성합니다.

9. 앱에 배포 그룹을 할당하고 저장을 클릭합니다. 자세한 내용은 [리소스 배포](#)를 참조하십시오.

2 단계: 앱 배포 구성

1. 구성 > 배포 그룹으로 이동한 다음 구성한 배포 그룹을 선택합니다. 편집을 클릭합니다.

2. 앱 섹션에서 원하는 앱을 필수 앱 상자로 끌어옵니다.



3. 요약 페이지에서 저장을 클릭합니다.

4. 배포 그룹 페이지에서 배포 그룹을 선택하고 배포를 클릭합니다.

엔터프라이즈 앱

엔터프라이즈 앱은 MAM SDK 또는 MDX Toolkit 으로 준비되지 않은 개인 앱을 나타냅니다. 이러한 앱을 직접 개발하거나 다른 출처에서 직접 획득할 수 있습니다. 엔터프라이즈 앱을 추가하려면 앱과 연결된 APK 파일이 필요합니다. [Google 개인 앱 모범 사례](#)를 따르십시오.

1 단계: 앱 추가 및 구성

다음의 두 가지 방식 중 하나로 앱을 추가합니다.

- 관리되는 Google Play 스토어에 직접 앱을 게시하고 XenMobile 콘솔에 관리되는 Play 스토어 앱으로 추가합니다. [개인 앱 게시](#) 방법에 관한 Google 문서를 따르고 관리되는 앱 스토어 앱 섹션의 단계를 따르십시오.
- 앱을 XenMobile 콘솔에 엔터프라이즈 앱으로 추가합니다. 다음 단계를 수행합니다.

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

Add App [X]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

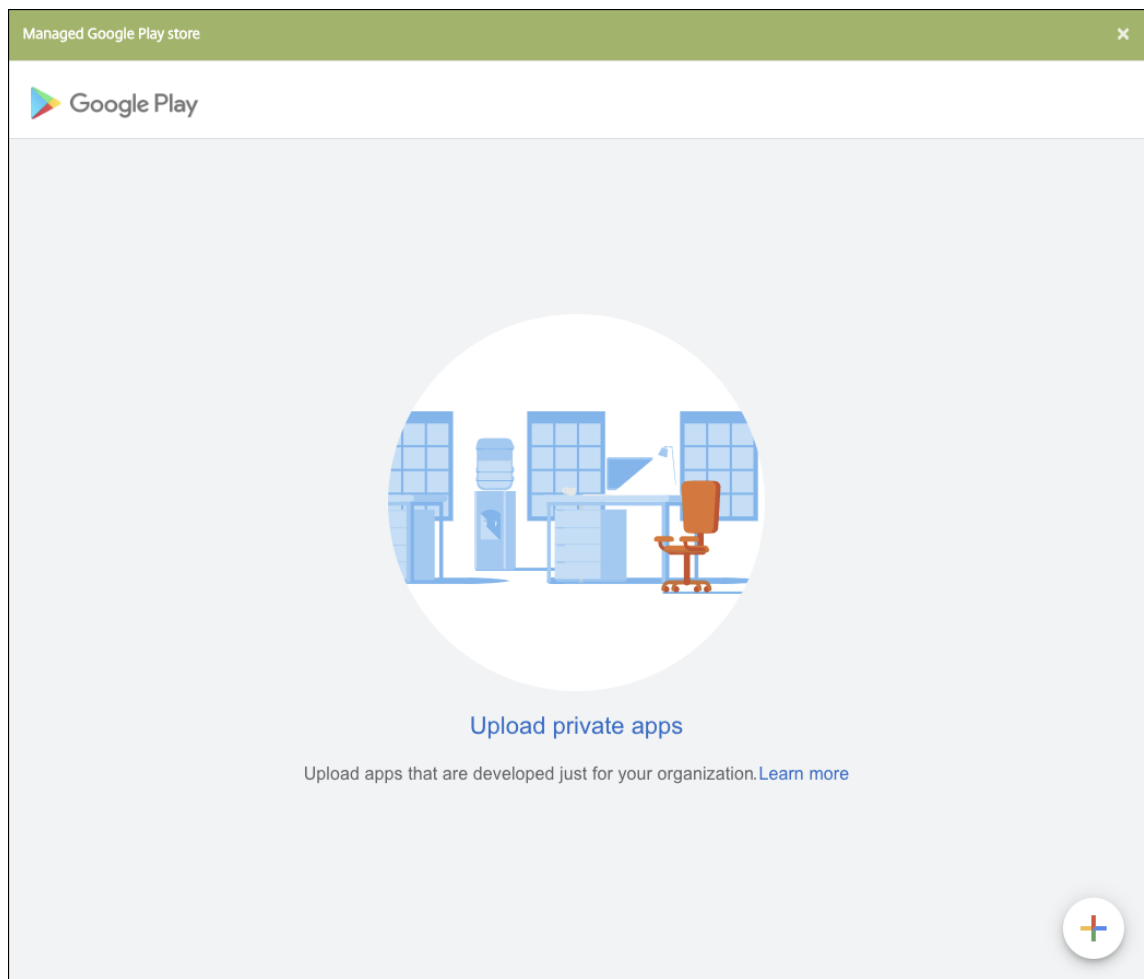
<p>MDX</p> <p>Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.</p> <p>Example: WorxMail</p>	<p>Public App Store</p> <p>Free or paid apps available in a public app store, such as iTunes or Google Play, for download.</p> <p>Example: GoToMeeting</p>
<p>Web & SaaS</p> <p>Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.</p> <p>Example: GoogleApps_SAML</p>	<p>Enterprise</p> <p>Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.</p> <p>Example: Quick-iLaunch</p>
<p>Web Link</p> <p>A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.</p>	

2. 엔터프라이즈를 클릭합니다. 앱 정보 창에서 다음 정보를 입력합니다.

- 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.
- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 정보](#)를 참조하십시오.

3. 플랫폼으로 **Android Enterprise** 를 선택합니다.

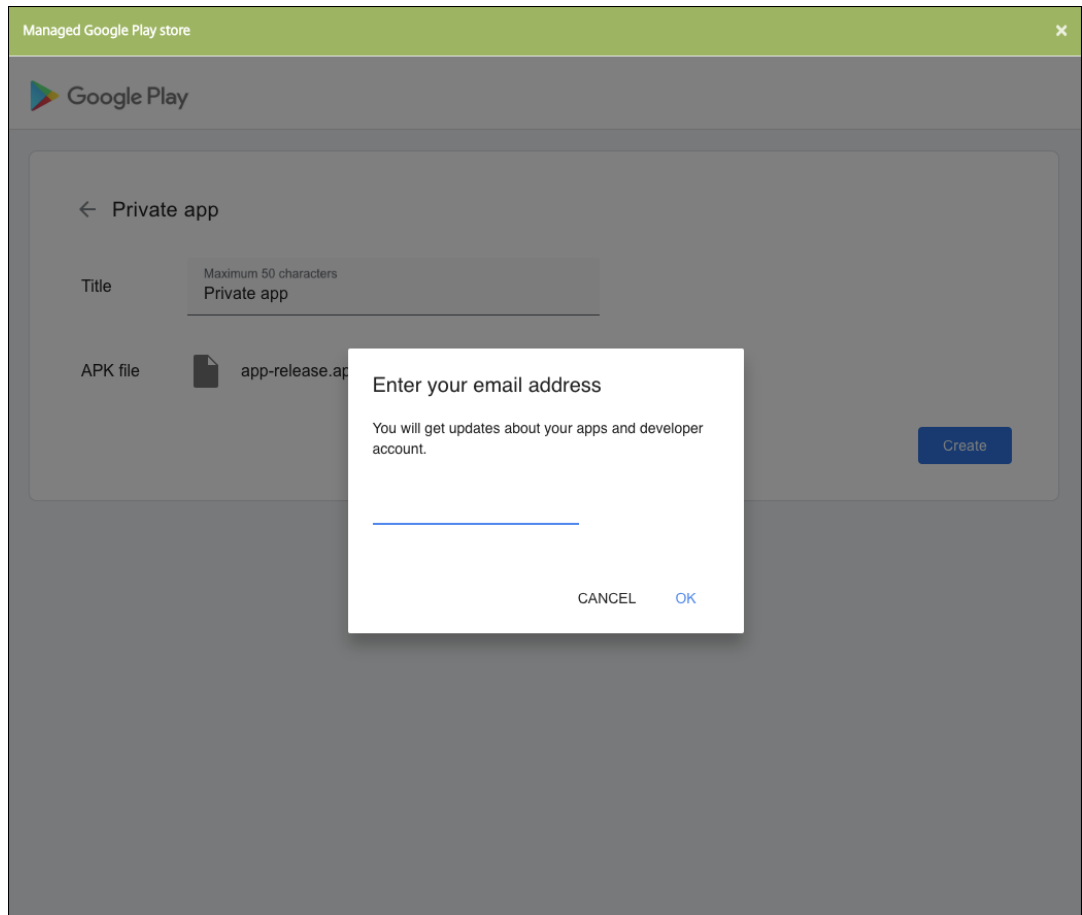
4. 업로드 버튼을 클릭하면 관리되는 Google Play Store 가 열립니다. 개발자 계정을 등록하지 않고도 개인 앱을 게시할 수 있습니다. 계속하려면 오른쪽 아래의 + 아이콘을 클릭합니다.



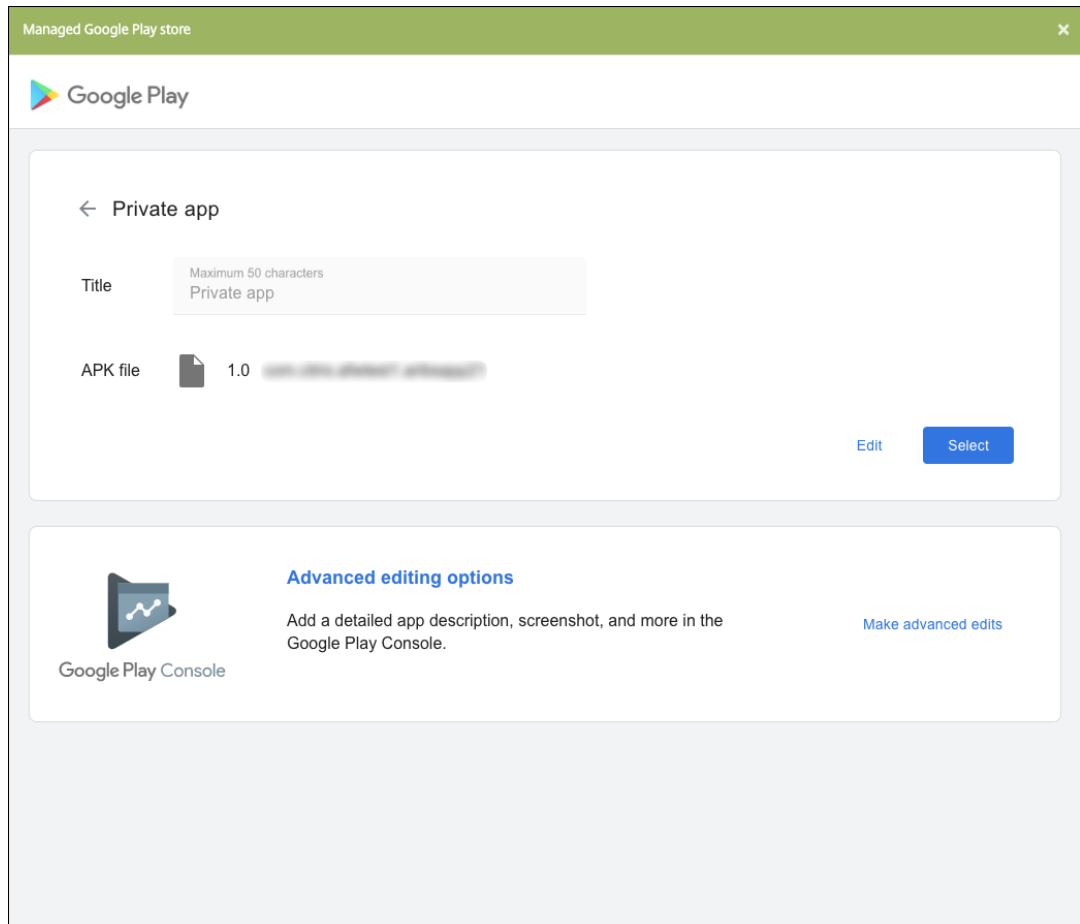
- a) 앱 이름을 입력하고.apk 파일을 업로드합니다. 작업을 마치면 **Create(만들기)** 를 클릭합니다. 개인 앱을 게시하는 데 최대 10 분이 걸릴 수 있습니다.

The screenshot shows a web interface titled "Managed Google Play store" with a close button (X) in the top right corner. Below the title bar is the Google Play logo. The main content area is titled "← Private app". It contains two input fields: "Title" with a placeholder "Maximum 50 characters" and "APK file" with a blue "Upload APK" button. A grey "Create" button is located at the bottom right of the form.

- b) 앱에 대한 업데이트를 받으려면 이메일 주소를 입력합니다.



- c) 애플리케이션이 게시되고 난 후 개인 앱의 아이콘을 클릭합니다. 앱 설명을 추가하거나 앱 아이콘을 변경하는 등 다른 작업을 수행하려면 고급 편집을 클릭합니다. 아니면 선택을 클릭하여 앱 정보 페이지를 엽니다.



5. 다음을 클릭합니다. 플랫폼에 대한 앱 정보 페이지가 나타납니다.

6. 다음과 같은 플랫폼 유형에 대한 설정을 구성합니다.

- 파일 이름: 필요한 경우 앱의 새 이름을 입력합니다.
- 앱 설명: 필요한 경우 앱에 대한 새 설명을 입력합니다.
- 앱 버전: 이 필드는 변경할 수 없습니다.
- 패키지 ID: 앱의 고유 식별자입니다.
- 최소 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
- 최대 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
- 제외된 장치: 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

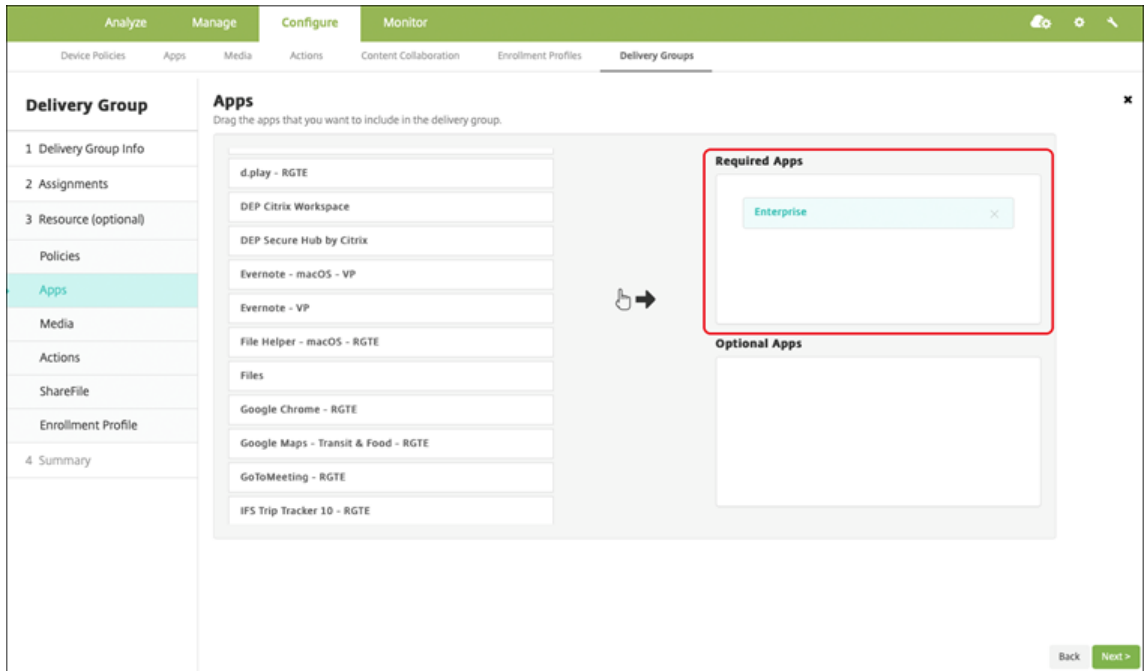
7. 배포 규칙 및 저장소 구성을 구성합니다.

8. 앱에 배달 그룹을 할당하고 저장을 클릭합니다. 자세한 내용은 [리소스 배포](#)를 참조하십시오.

2 단계: 앱 배포 구성

1. 구성 > 배달 그룹으로 이동한 다음 구성한 배달 그룹을 선택합니다. 편집을 클릭합니다.

2. 앱 섹션에서 원하는 앱을 필수 앱 상자로 끌어옵니다.



3. 요약 페이지에서 저장을 클릭합니다.
4. 배달 그룹 페이지에서 배달 그룹을 선택하고 배포를 클릭합니다.

MDX 지원 개인 앱

Android Enterprise 앱을 MDX 지원 엔터프라이즈 앱으로 추가하려면 다음 단계를 따르십시오.

1. 개인 Android Enterprise 앱과 MDX 지원 앱을 만듭니다.
2. XenMobile 콘솔에 앱을 추가합니다.
 - 관리되는 Google Play 스토어에서 앱을 호스팅하고 게시합니다.
 - 앱을 XenMobile 콘솔에 Enterprise 앱으로 추가합니다.
3. MDX 파일을 XenMobile 에 추가합니다.

Google Play Store 를 통해 앱을 호스트하고 게시하기로 했다면 Google 인증서 서명을 선택하지 마십시오. 앱을 MDX 로 지원하는 데 사용한 것과 동일한 인증서로 앱에 서명합니다. 앱 게시에 관한 자세한 정보는 [앱 게시](#) 및 [앱 서명](#)에 관한 Google 문서를 참고하십시오. MAM SDK 는 앱을 래핑하지 않으므로 앱 개발에 사용한 인증서 이외의 인증서가 필요하지 않습니다.

Google Play Console 을 통한 비공개 앱 게시에 관한 자세한 정보는 [Play Console 에서 개인 앱 게시](#) 방법에 관한 Google 문서를 참조하십시오.

XenMobile 을 통해 앱을 게시하려면 다음 섹션을 참조하십시오.

비공개 **Android Enterprise** 앱 준비

비공개 Android Enterprise 앱을 만들 경우 Google [개인 앱 모범 사례](#)를 따라야 합니다.

개인 Android Enterprise 앱을 만든 후 앱과 MAM SDK 를 통합하거나 MDX Toolkit 을 사용하여 앱을 래핑합니다. 그런 다음 결과 파일을 XenMobile 에 추가합니다.

업데이트된 .apk 파일을 업로드하여 앱을 업데이트할 수 있습니다. 다음 단계는 MDX Toolkit 을 통한 앱 래핑에 적용됩니다.

1. 비공개 Android Enterprise 앱을 만들고 서명된.apk 파일을 생성합니다.
2. 다음 예제 파일에는 알려진 모든 정책이 포함되어 있으며 그중 일부는 사용자 환경에 적용되지 않을 수 있습니다. 사용할 수 없는 설정은 무시됩니다. 다음 매개 변수로 XML 파일을 만듭니다.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <MobileAppPolicies>
3      <PolicySchemaVersion>
4          1.0
5      </PolicySchemaVersion>
6      <Policies>
7          <DevicePasscode>false</DevicePasscode>
8          <AppPasscode>false</AppPasscode>
9          <MaxOfflinePeriod>72</MaxOfflinePeriod>
10         <StepupAuthAddress/>
11         <RequireUserEntropy>false</RequireUserEntropy>
12         <BlockRootedDevices>true</BlockRootedDevices>
13         <BlockDebuggerAccess>false</BlockDebuggerAccess>
14         <RequireDeviceLock>false</RequireDeviceLock>
15         <NonCompliantDeviceBehavior>AllowAppAfterWarning</NonCompliantDeviceBehavior>
16         <WifiOnly>false</WifiOnly>
17         <RequireInternalNetwork>false</RequireInternalNetwork>
18         <InternalWifiNetworks/>
19         <AllowedWifiNetworks/>
20         <UpgradeGracePeriod>168</UpgradeGracePeriod>
21         <WipeDataOnAppLock>false</WipeDataOnAppLock>
22         <ActivePollPeriod>60</ActivePollPeriod>
23         <PublicFileAccessLimitsList/>
24         <CutAndCopy>Unrestricted</CutAndCopy>
25         <Paste>Unrestricted</Paste>
26         <DocumentExchange>Unrestricted</DocumentExchange>
27         <OpenInExclusionList/>
28         <InboundDocumentExchange>Unrestricted</InboundDocumentExchange>
29         <InboundDocumentExchangeWhitelist/>
30         <connectionSecurityLevel>TLS</connectionSecurityLevel>
31         <DisableCamera>false</DisableCamera>
32         <DisableGallery>false</DisableGallery>
33         <DisableMicrophone>false</DisableMicrophone>
34         <DisableLocation>false</DisableLocation>
35         <DisableSms>false</DisableSms>
36         <DisableScreenCapture>false</DisableScreenCapture>
37         <DisableSensor>false</DisableSensor>

```



```

38      <DisableNFC>false</DisableNFC>
39      <BlockLogs>false</BlockLogs>
40      <DisablePrinting>false</DisablePrinting>
41      <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
        MvpnNetworkAccess>
42      <MvpnSessionRequired>False</MvpnSessionRequired>
43      <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44      <DisableLocalhostConnections>false</
        DisableLocalhostConnections>
45      <CertificateLabel/>
46      <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47      <DefaultLoggerLevel>15</DefaultLoggerLevel>
48      <MaxLogFiles>2</MaxLogFiles>
49      <MaxLogFileSize>2</MaxLogFileSize>
50      <RedirectSystemLogs>false</RedirectSystemLogs>
51      <EncryptLogs>false</EncryptLogs>
52      <GeofenceLongitude>0</GeofenceLongitude>
53      <GeofenceLatitude>0</GeofenceLatitude>
54      <GeofenceRadius>0</GeofenceRadius>
55      <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56      <Authentication>OfflineAccessOnly</Authentication>
57      <ReauthenticationPeriod>480</ReauthenticationPeriod>
58      <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59    </Policies>
60  </MobileAppPolicies>
61  <!--NeedCopy-->

```

3. MDX Toolkit 을 사용하여 앱을 래핑합니다. MDX Toolkit 사용에 대한 자세한 내용은 [Android 모바일 앱 래핑](#)을 참조하십시오.

apptype 매개 변수를 프리미엄으로 설정합니다. 다음에 설명된 명령에서 이전 단계의 XML 파일을 사용합니다.

앱의 스토어 URL 을 알고 있다면 **storeURL** 매개 변수를 스토어 URL 로 설정합니다. 앱이 게시된 후 사용자는 스토어 URL 에서 앱을 다운로드합니다.

다음은 SampleAEapp 이라는 앱을 래핑하는 데 사용되는 MDX Toolkit 명령의 예입니다.

```

1  ``
2  java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
        Duser.variant
3  -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
4  -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
5  -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
6  -MinPlatform 5.0
7  -keystore /MyKeystore
8  -storepass mystorepwd123
9  -keyalias key0
10 -keypass mykeypwd123
11 -storeURL "https://play.google.com/store/apps/details?id=
        SampleAEAppPackage"
12 -appType Premium
13 -premiumMdxPolicies <Path to Premium policy XML>
14 <!--NeedCopy--> ``

```

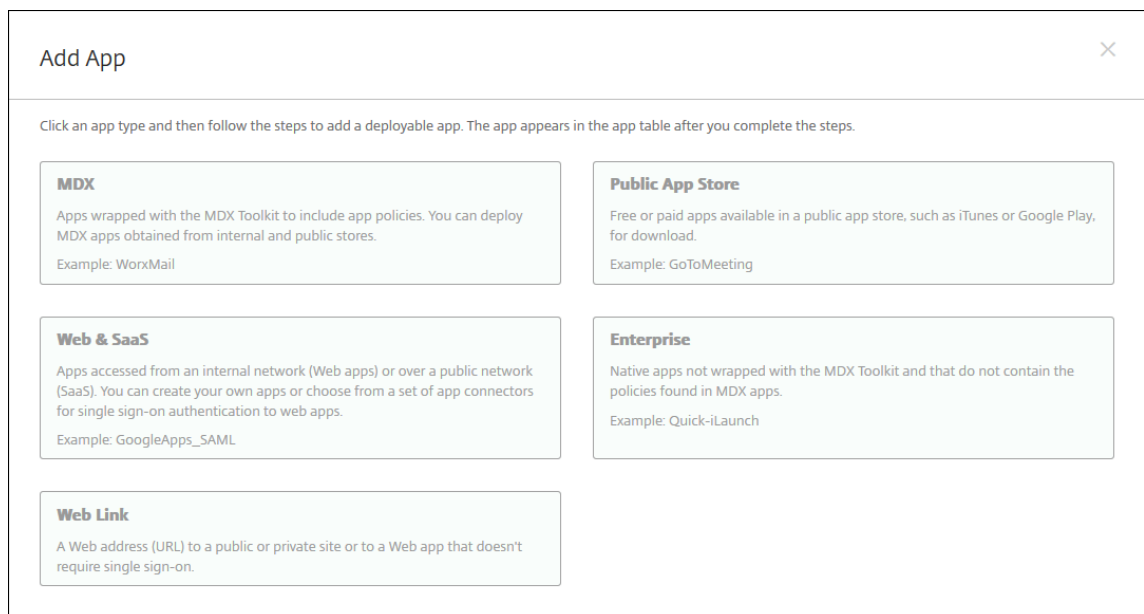
앱을 래핑하면 래핑된.apk 파일과.mdx 파일이 생성됩니다.

래핑된.apk 파일 추가

다음의 두 가지 방식 중 하나로 앱을 추가합니다.

- 관리되는 Google Play 스토어에 직접 앱을 게시하고 XenMobile 콘솔에 관리되는 Play 스토어 앱으로 추가합니다. [개인 앱 게시](#) 방법에 관한 Google 문서를 따르고 관리되는 앱 스토어 앱 섹션의 단계를 따르십시오.
- 앱을 XenMobile 콘솔에 엔터프라이즈 앱으로 추가합니다. 다음 단계를 수행합니다.

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 열립니다.
2. 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

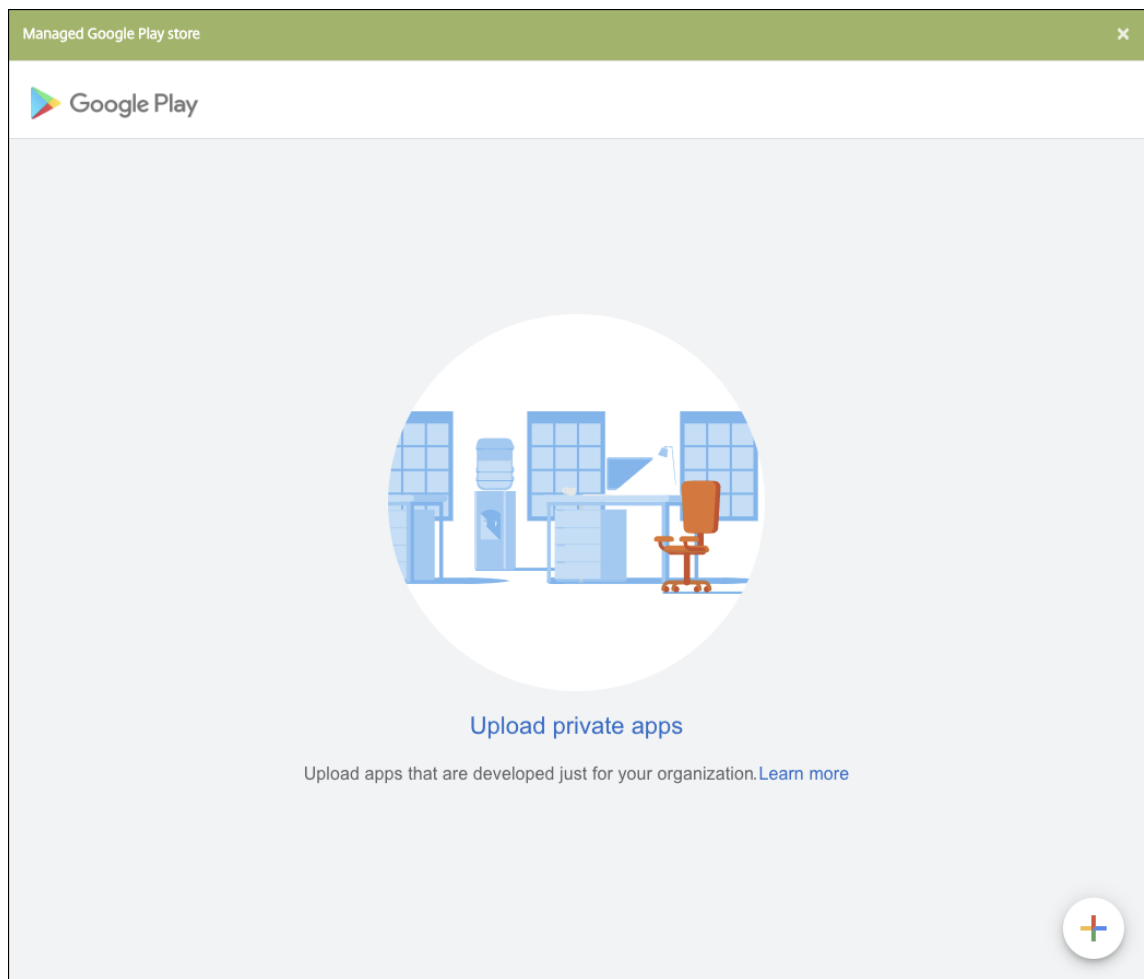


Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.


MDX Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: WorxMail	Public App Store Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
Web & SaaS Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps_SAML	Enterprise Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
Web Link A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.	

3. 엔터프라이즈를 클릭합니다. 앱 정보 창에서 다음 정보를 입력합니다.
 - 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
 - 설명: 앱의 선택적 설명을 입력합니다.
 - 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 정보](#)를 참조하십시오.
4. 플랫폼으로 **Android Enterprise** 를 선택합니다.
5. 업로드 버튼을 클릭하면 관리되는 Google Play Store 가 열립니다. 개발자 계정을 등록하지 않고도 개인 앱을 게시할 수 있습니다. 계속하려면 오른쪽 아래의 + 아이콘을 클릭합니다.



- a) 앱 이름을 입력하고.apk 파일을 업로드합니다. 작업을 마치면 **Create(만들기)** 를 클릭합니다. 개인 앱을 게시하는 데 최대 10 분이 걸릴 수 있습니다.

Managed Google Play store

 Google Play

← Private app

Title

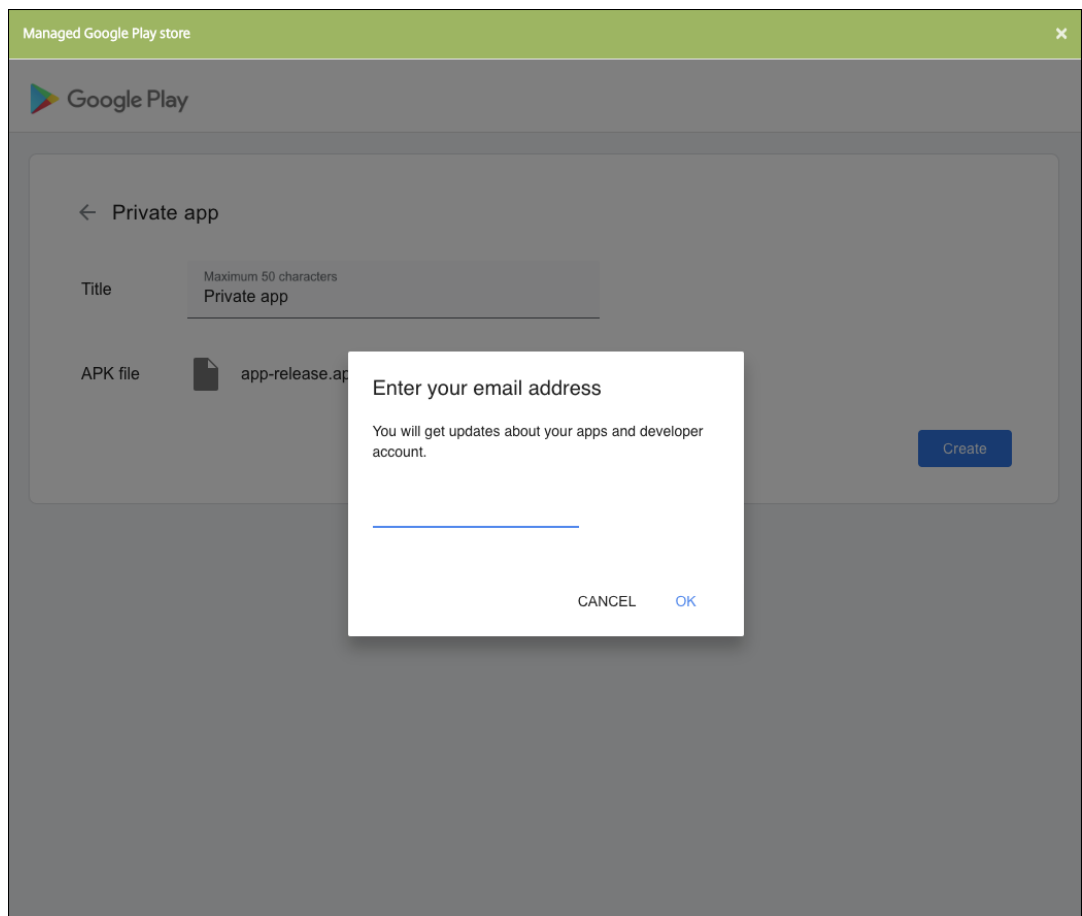
Maximum 50 characters

APK file

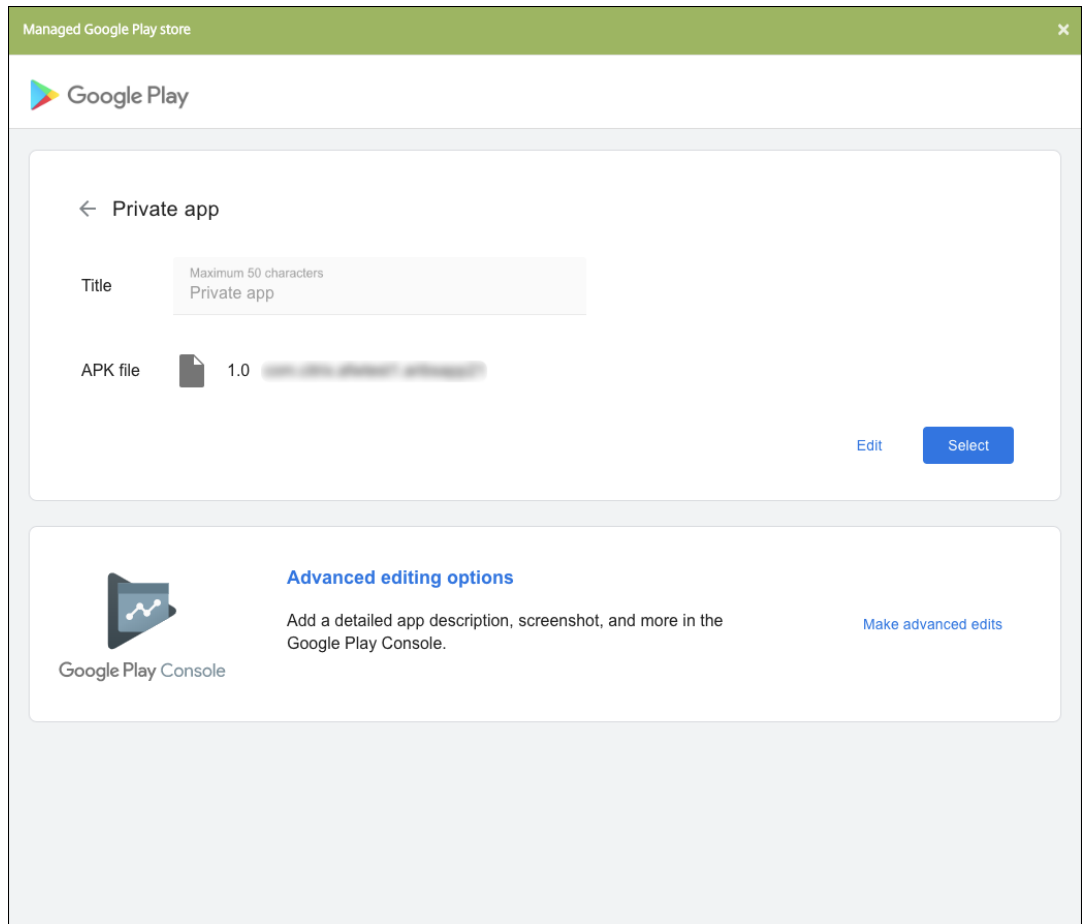
Upload APK

Create

- b) 앱에 대한 업데이트를 받으려면 이메일 주소를 입력합니다.



- c) 응용 프로그램이 게시된 후 개인 앱의 아이콘을 클릭하고 선택을 클릭하여 앱 정보 페이지를 엽니다.



6. 다음을 클릭합니다. 플랫폼에 대한 앱 정보 페이지가 나타납니다.

7. 다음과 같은 플랫폼 유형에 대한 설정을 구성합니다.

- 파일 이름: 필요한 경우 앱의 새 이름을 입력합니다.
- 앱 설명: 필요한 경우 앱에 대한 새 설명을 입력합니다.
- 앱 버전: 이 필드는 변경할 수 없습니다.
- 패키지 ID: 앱의 고유 식별자입니다.
- 최소 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
- 최대 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
- 제외된 장치: 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

8. 배포 규칙 및 저장소 구성을 구성합니다.

9. **Android Enterprise** 엔터프라이즈 앱 페이지에서 다음을 엽니다. 승인 페이지가 나타납니다.

워크플로를 사용하여 사용자의 앱 액세스를 허용하기 전에 승인을 요구하려면 [워크플로 적용](#)을 참조하십시오. 승인 워크플로가 필요하지 않은 경우 13 단계로 건너 뛰어도 됩니다.

10. 다음을 클릭합니다.

11. 배달 그룹 할당 페이지가 나타납니다. 이 페이지에서는 아무 조치도 필요하지 않습니다. .mdx 파일을 추가할 경우 이 앱의 배달 그룹과 배포 일정을 구성합니다. 저장을 클릭합니다.

선택 사항: 스토어 **URL** 을 추가하거나 변경합니다 앱을 래핑했을 때 스토어 URL 을 몰랐다면 지금 스토어 URL 을 추가합니다.

1. 관리되는 Google Play Store 에서 앱을 확인합니다. 앱을 선택하면 스토어 URL 이 브라우저의 주소 표시줄에 표시됩니다. URL 형식에서 앱의 패키지 이름을 복사합니다. 예: <https://play.google.com/store/apps/details?id=SampleAEappPackage>. 복사한 URL 이 <https://play.google.com/work/>으로 시작할 수 있습니다. **work**를 **store**로 변경해야 합니다.
2. MDX Toolkit 을 사용하여 스토어 URL 을.mdx 파일에 추가합니다.

```
1 java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
2 setinfo \
3 -in ~/Desktop/SampleApps/Sample.mdx \
4 -out ~/Desktop/SampleApps/wrapped/Sample.mdx \
5 -storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
6 <!--NeedCopy-->
```

.mdx 파일 추가

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

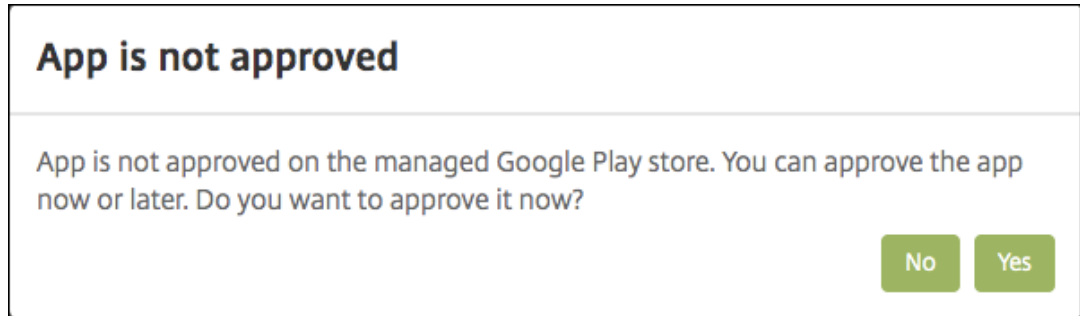
Add App [X]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

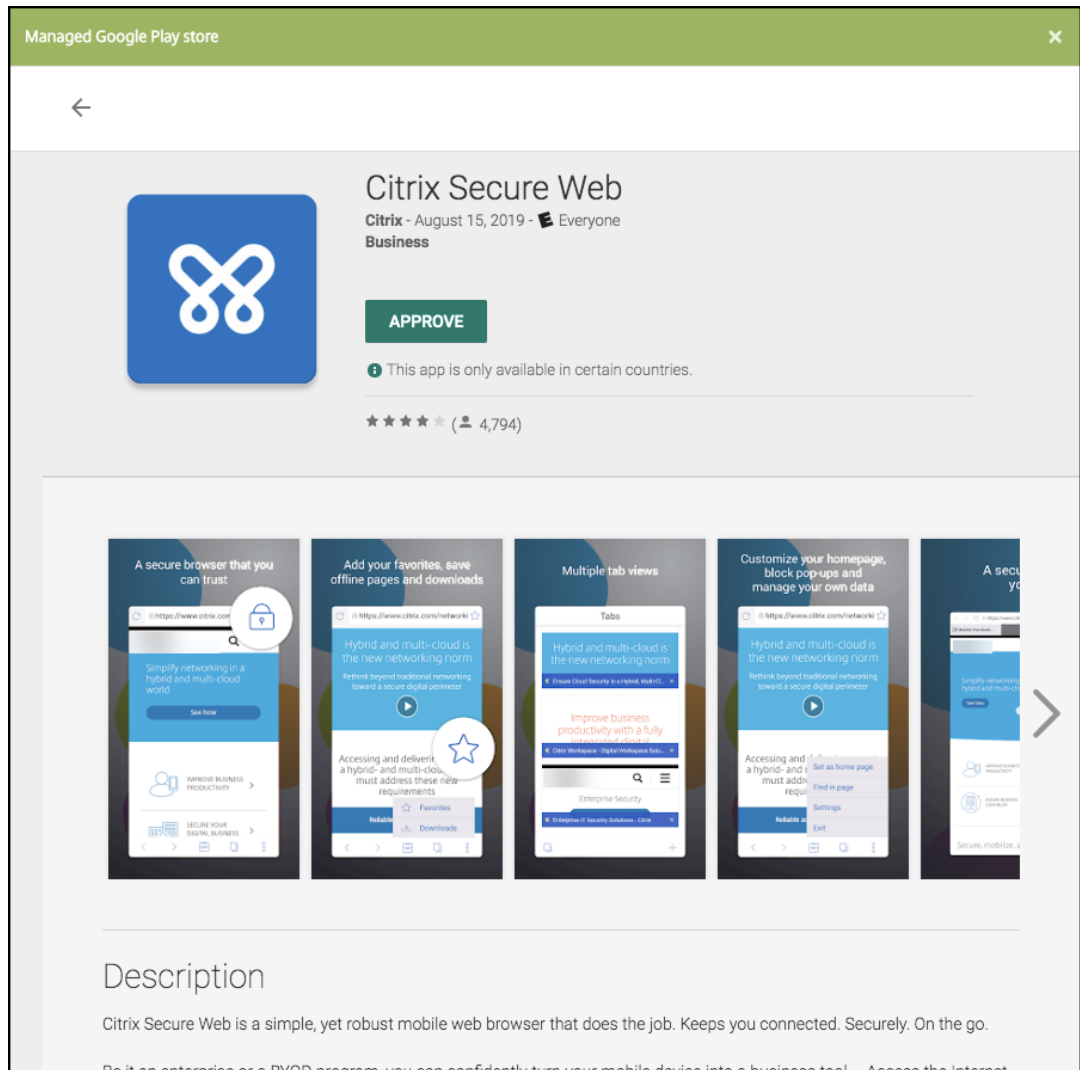
<p>MDX</p> <p>Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.</p> <p>Example: WorxMail</p>	<p>Public App Store</p> <p>Free or paid apps available in a public app store, such as iTunes or Google Play, for download.</p> <p>Example: GoToMeeting</p>
<p>Web & SaaS</p> <p>Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.</p> <p>Example: GoogleApps_SAML</p>	<p>Enterprise</p> <p>Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.</p> <p>Example: Quick-iLaunch</p>
<p>Web Link</p> <p>A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.</p>	

2. **MDX** 를 클릭합니다. **MDX** 앱 정보 페이지가 나타납니다. 앱 정보 창에서 다음 정보를 입력합니다.
 - 이름: 앱을 설명하는 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 표시됩니다.
 - 설명: 앱의 선택적 설명을 입력합니다.

- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 정보](#)를 참조하십시오.
3. 플랫폼으로 **Android Enterprise** 를 선택합니다.
 4. 업로드를 클릭하고 MDX 파일로 이동합니다. Android Enterprise 는 MDX Toolkit 으로 래핑된 앱만 지원합니다.
 - 연결된 응용 프로그램에 관리되는 Google Play Store 의 승인이 필요한 경우 UI 에 알림이 표시됩니다. XenMobile 콘솔을 종료하지 않고 응용 프로그램을 승인하려면 예를 클릭합니다.



관리되는 Google Play Store 가 열리면 지침에 따라 앱을 승인하고 저장합니다.



앱이 성공적으로 추가되면 앱 세부 정보 페이지가 나타납니다.

5. 다음 설정을 구성합니다.

- 파일 이름: 앱에 연결된 파일 이름을 입력합니다.
- 앱 설명: 앱에 대한 설명을 입력합니다.
- 앱 버전: 필요한 경우 앱 버전 번호를 입력합니다.
- 패키지 ID: 관리되는 Google Play 스토어에서 가져온 앱의 패키지 ID 를 입력합니다.
- 최소 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
- 최대 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
- 제외된 장치: 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

6. **MDX** 정책을 구성합니다. MDX 정책은 플랫폼별로 다르며 인증, 장치 보안 및 앱 제한 등 정책 영역에 대한 옵션이 포함됩니다. 콘솔에서 각 정책에는 정책을 설명하는 도구 설명이 포함됩니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

- [MAM SDK Overview\(MAM SDK 개요\)](#)
- [MDX 타사 앱 정책 요약](#)

7. 배포 규칙 및 저장소 구성을 구성합니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우 상시 연결에 대해 배포가 적용됩니다.

상시 연결 옵션:

- 버전 10.18.19 이상으로 Endpoint Management 를 사용하기 시작한 Android Enterprise 고객은 사용할 수 없습니다.
- 버전 10.18.19 이전으로 Endpoint Management 를 사용하기 시작한 Android Enterprise 고객에게는 권장되지 않습니다.

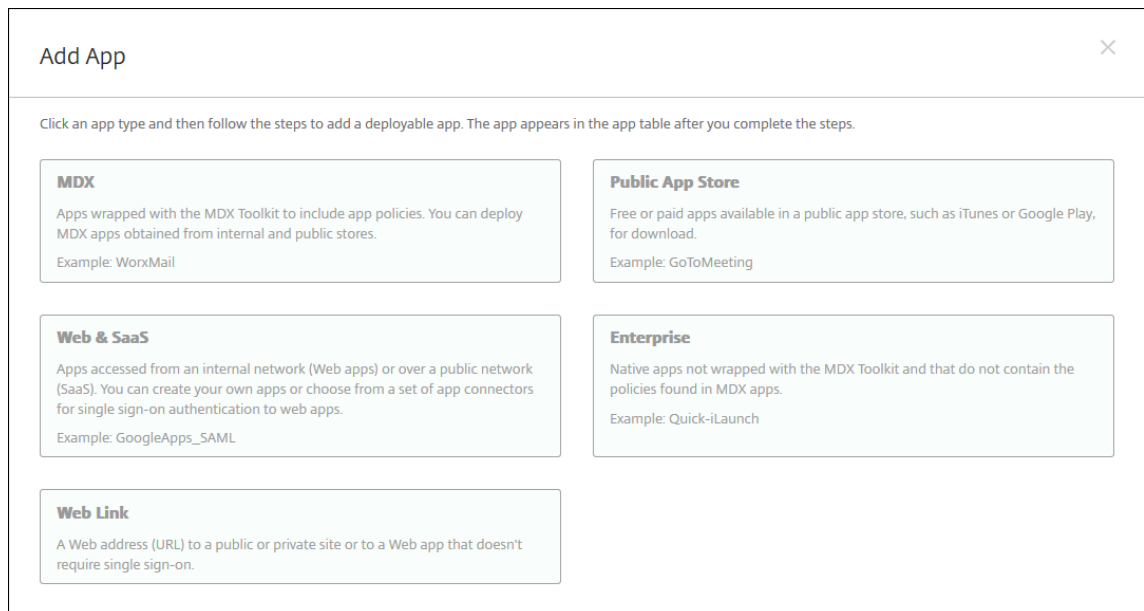
구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 상시 연결에 대해 배포를 제외하고 모든 플랫폼에 적용됩니다.

8. 앱에 배달 그룹을 할당하고 저장을 클릭합니다. 자세한 내용은 [리소스 배포](#)를 참조하십시오.

앱 업데이트

Android Enterprise 앱을 업데이트하려면 업데이트된.apk 파일을 래핑하고 업로드합니다.

1. MAM SDK 또는 MDX Toolkit 을 사용하여 업데이트된 앱의.apk 파일을 래핑합니다.
2. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 열립니다.

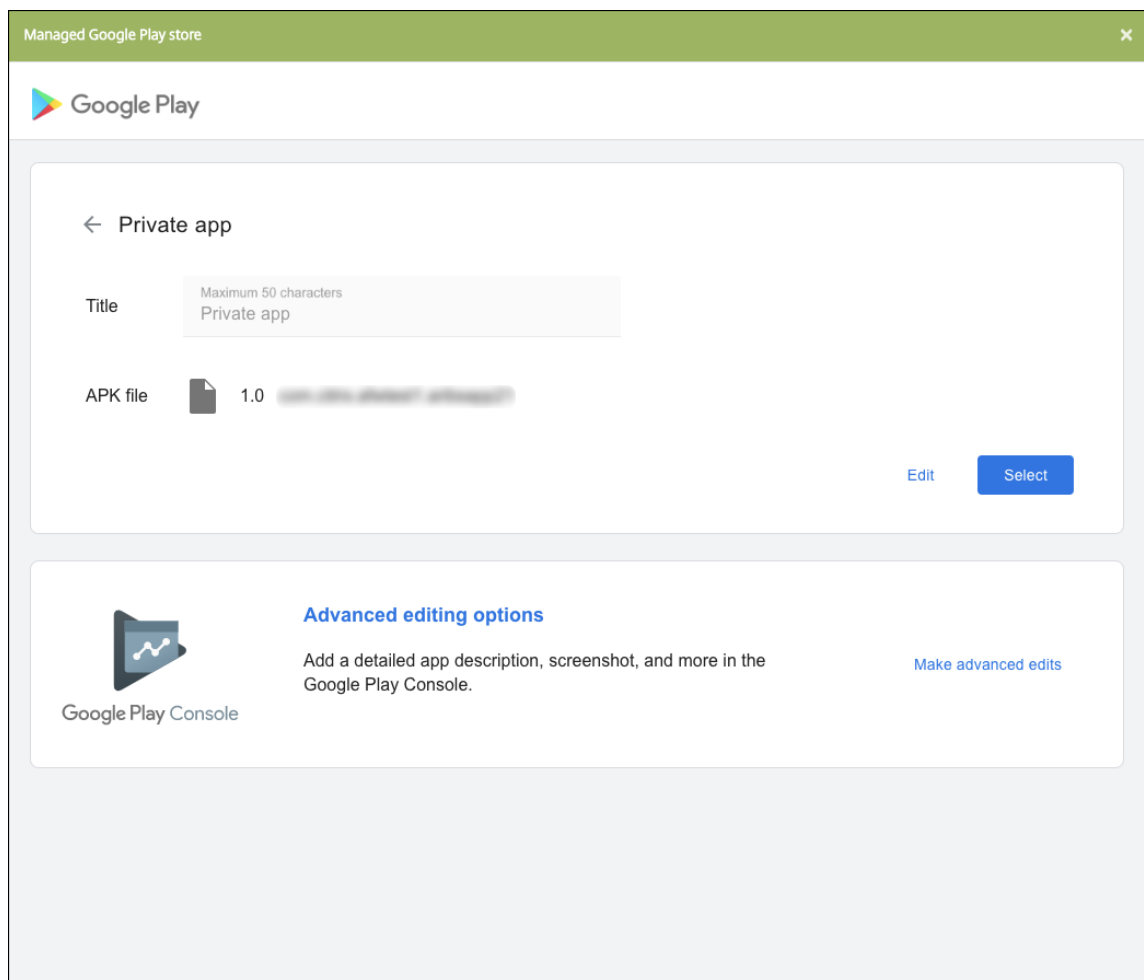


3. 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

4. 엔터프라이즈를 클릭합니다. 앱 정보 창에서 다음 정보를 입력합니다.

- 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.
- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 정보](#)를 참조하십시오.

5. 플랫폼으로 **Android Enterprise** 를 선택합니다.
6. 다음을 클릭합니다. **Android Enterprise** 엔터프라이즈 앱 페이지가 나타납니다.
7. 업로드를 클릭합니다.
8. 관리되는 Google Play 스토어 페이지에서 업데이트할 앱을 선택합니다.
9. 앱 정보 페이지에서.apk 파일 이름 옆에 있는 편집을 클릭합니다.



10. 새.apk 파일로 이동한 다음 업로드합니다.
11. 관리되는 Google Play 스토어 페이지에서 저장을 클릭합니다.

Google Workspace 고객을 위한 레거시 **Android Enterprise**(이전 명칭 **G Suite**)

March 15, 2024

Google Workspace(이전 명칭 G Suite) 고객은 레거시 Android Enterprise 설정을 사용하여 레거시 Android Enterprise 를 구성해야 합니다.

레거시 Android Enterprise 요구 사항:

- 공개적으로 액세스할 수 있는 도메인
- Google 관리자 계정
- 관리되는 프로필을 지원하고 Android 5.0 Lollipop 이상을 실행 중인 장치
- Google Play 가 설치된 Google 계정
- 장치에 설정된 작업 프로필

레거시 Android Enterprise 를 구성하려면 XenMobile 설정의 **Android Enterprise** 페이지에서 레거시 **Android Enterprise** 를 클릭합니다.

Settings > Android for Work

Android for Work ▼

Android for Work To set up Android for Work for your company, you need to bind XenMobile as your enterprise mobile management (EMM) provider through Google Play.

i If you're a G Suite customer, it's recommended to use *legacy Android for Work* settings to manage Android. Click on button ▼ to switch back.

- 1**
We are taking you out to XenMobile Tools to complete a few steps
Once it's done, come back to this page to upload the registration file to XenMobile on step 3.
- 2**
Go to XenMobile Tools and follow steps there
[Go to XenMobile Tools](#)
- 3**
Upload File you just downloaded from XenMobile Tools
Once you download the Google file from XenMobile Tools, upload it here.
[Upload file](#)

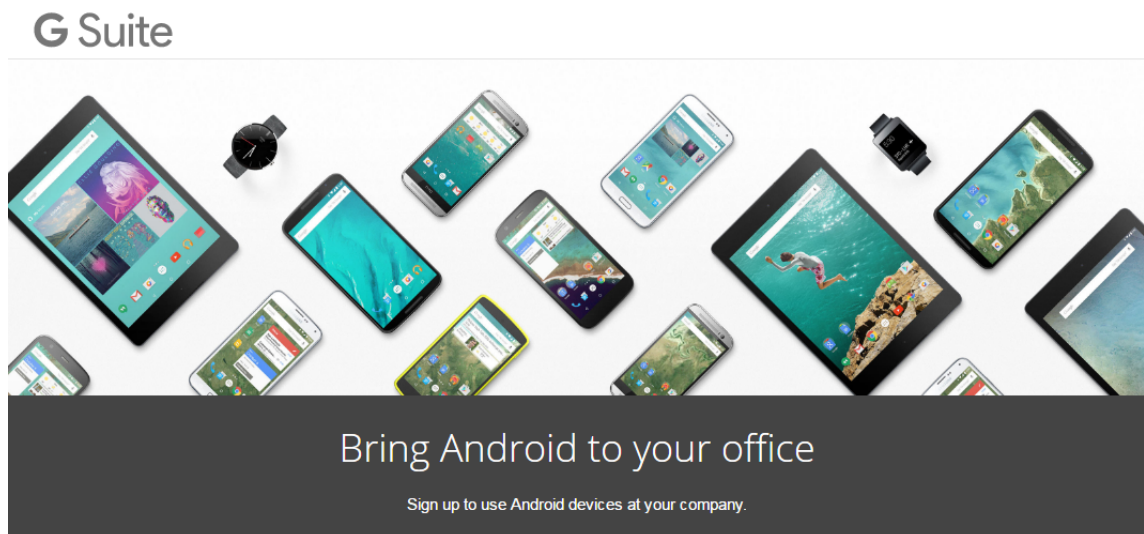
Android Enterprise 계정 만들기

Android Enterprise 계정을 설정하려면 먼저 Google 에서 도메인 이름을 확인해야 합니다.

Google 에서 이미 도메인 이름을 확인한 경우 Android Enterprise 서비스 계정 설정 및 Android Enterprise 인증서 다운로드 단계로 건너뛸 수 있습니다.

1. <https://gsuite.google.com/signup/basic/welcome>로 이동합니다.

관리자 및 회사 정보를 입력하는 다음과 같은 페이지가 표시됩니다.



① About you

Name

First Name

Last Name

Current work email

Doesn't have to be an official business email.

e.g. john@mydomain.com

Phone

+1

2. 관리자 사용자 정보를 입력합니다.

① About you

Name

Justa ✓

User ✓

Current work email

Doesn't have to be an official business email.

justa.user@gmail.com ✓

Phone

+15551234567 ✓

3. 관리자 계정 정보와 더불어 회사 정보를 입력합니다.

2

About your business

Business name

EXAMPLE CORP

✓

Business domain address

example.com

✓

You'll need to verify that you own this domain.

Number of employees

1 employee

Country/Region

United States

3

Your Google admin account [Why do I need this?](#)

Username

justa.user

✓

Create an account to manage Android for Work

@

example.com

Create a password

8-character minimum; case sensitive

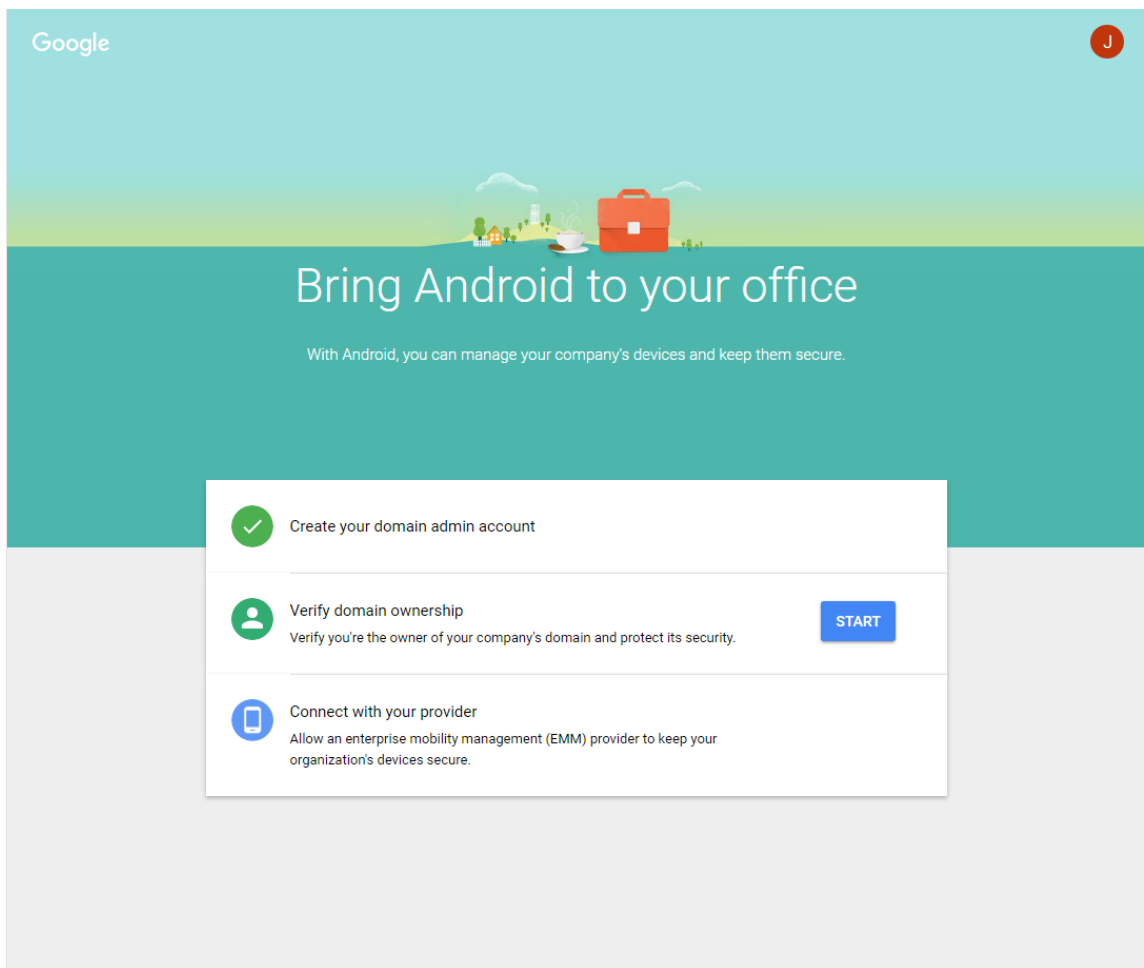
.....

✓

.....

✓

프로세스의 첫 번째 단계가 완료되면 다음 페이지가 표시됩니다.



도메인 소유권 확인


다음 방법 중 하나를 사용하여 Google 이 도메인을 확인할 수 있게 만듭니다.

- TXT 또는 CNAME 레코드를 도메인 호스트의 웹 사이트에 추가합니다.
- 도메인의 웹 서버에 HTML 파일을 업로드합니다.
- 홈 페이지에 `<meta>` 태그를 추가합니다. 첫 번째 방법을 사용하는 것이 좋습니다. 이 문서에서는 도메인 소유권을 확인하는 단계를 다루지 않습니다. 필요한 정보는 <https://support.google.com/a/answer/6248925>에서 찾을 수 있습니다.

1. **Start(시작)** 를 클릭하여 도메인 확인을 시작합니다.

Verify domain ownership(도메인 소유권 확인) 페이지가 나타납니다. 페이지의 지침에 따라 도메인을 확인합니다.

2. **Verify(확인)** 를 클릭합니다.



Verify domain ownership


Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)


After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

Note: Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

VERIFY

 Need help? Search the [Help Center](#) or call 844-390-7627 and provide your unique PIN **12345678**



Verify domain ownership

Verification checklist

Follow these steps to help Google verify that you own the domain **example.com**.

[Learn more](#)

☒ I have successfully logged in.

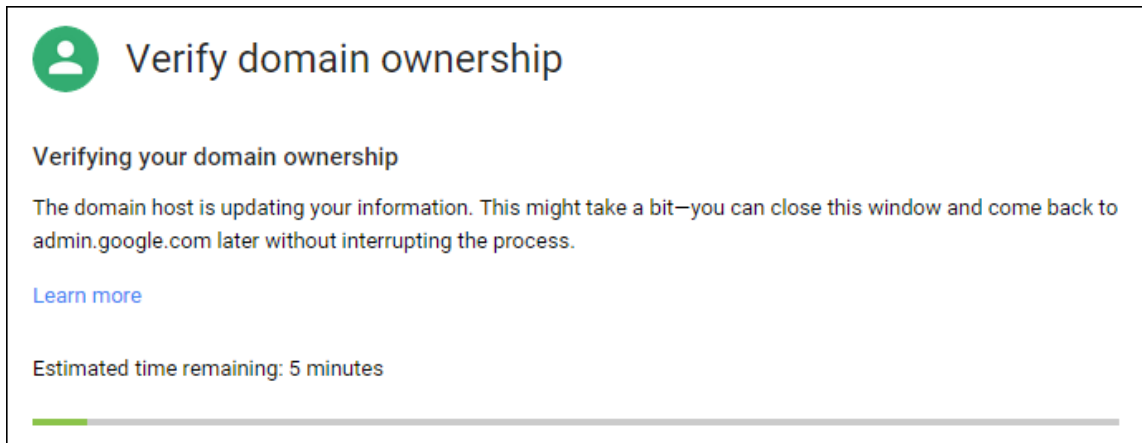
☒ I have opened the control panel for my domain.

☒ I have created the CNAME record.

☒ I have saved the CNAME record.

VERIFY

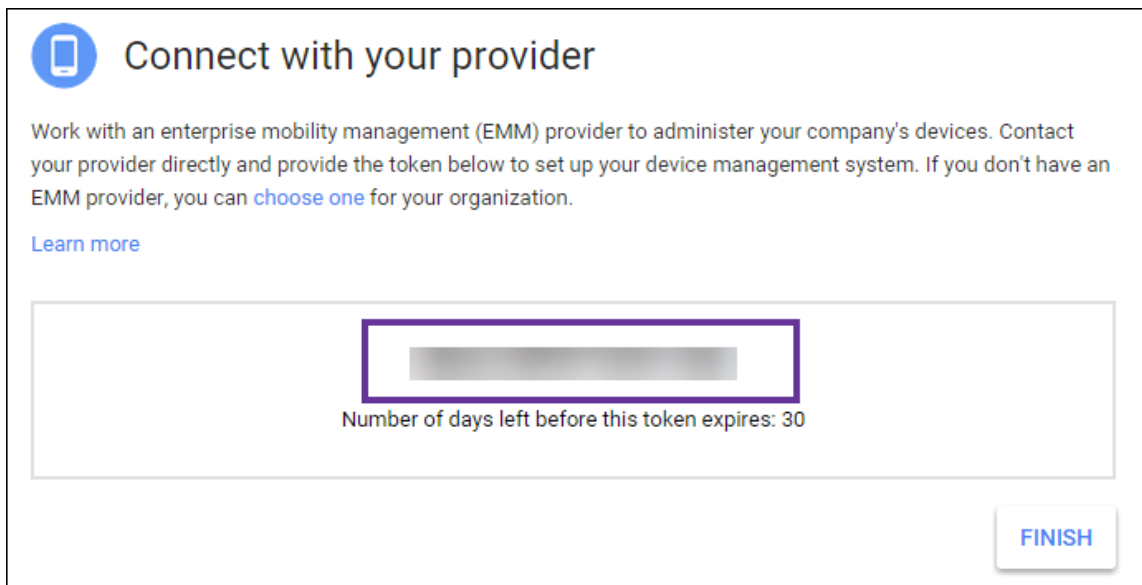
3. Google 이 도메인 소유권을 확인합니다.



4. 확인이 성공하면 다음 페이지가 나타납니다. **Continue**(계속) 를 클릭합니다.



5. Citrix 에 제공하고 Android Enterprise 설정을 구성할 때 사용하는 EMM 바인딩 토큰이 만들어집니다. 토큰을 복사하여 저장합니다. 나중에 설정 절차에서 이 토큰이 필요합니다.



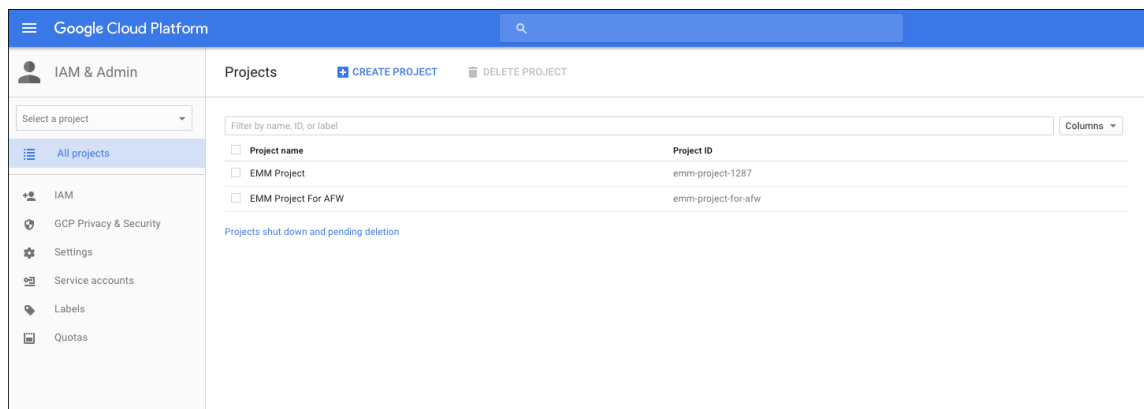
6. **Finish**(마침) 를 클릭하여 Android Enterprise 설정을 완료합니다. 도메인을 확인했음을 나타내는 페이지가 나타납니다.

Android Enterprise 서비스 계정을 만든 후 Google 관리 콘솔에 로그인하여 모바일 관리 설정을 관리할 수 있습니다.

Android Enterprise 서비스 계정 설정 및 Android Enterprise 인증서 다운로드

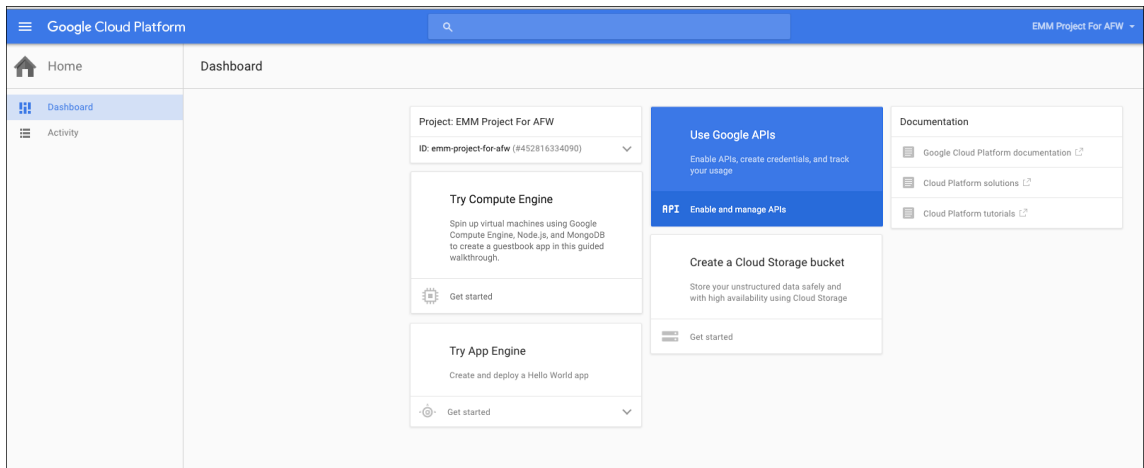
XenMobile 이 Google Play 및 디렉터리 서비스에 액세스할 수 있게 하려면 개발자를 위한 Google 프로젝트 포털을 사용하여 서비스 계정을 만들어야 합니다. 이 서비스 계정은 XenMobile 과 Android 용 Google 서비스 사이의 서버 간 통신에 사용됩니다. 사용되는 인증 프로토콜에 대한 자세한 내용은 <https://developers.google.com/identity/protocols/OAuth2ServiceAccount>를 참조하십시오.

1. 웹 브라우저에서 <https://console.cloud.google.com/project>로 이동하여 Google 관리자 자격 증명으로 로그인합니다.
2. **Projects(프로젝트)** 목록에서 **Create Project(프로젝트 만들기)** 를 클릭합니다.

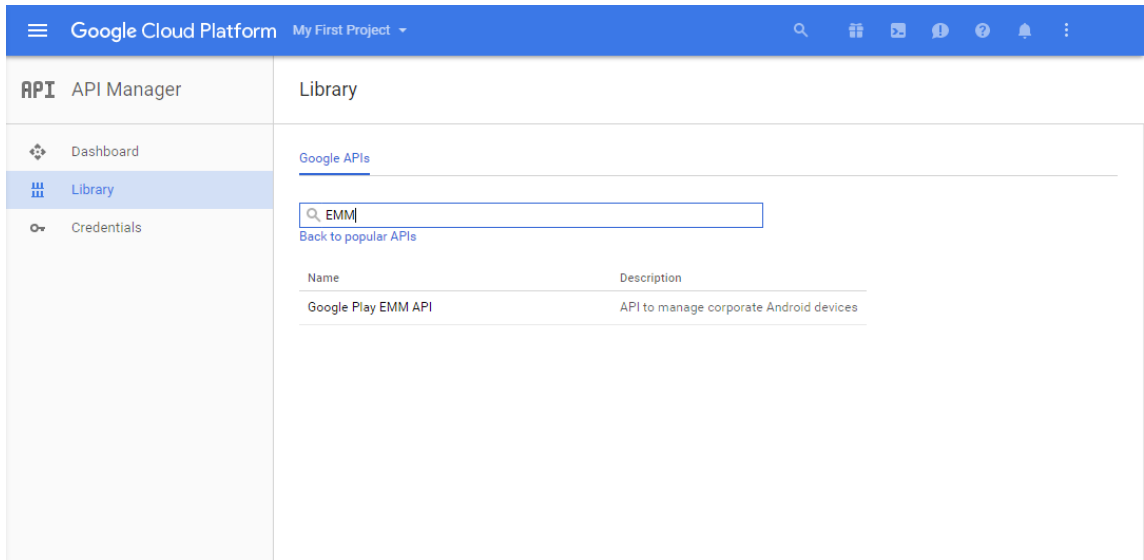


3. **Project name(프로젝트 이름)** 에 프로젝트 이름을 입력합니다.

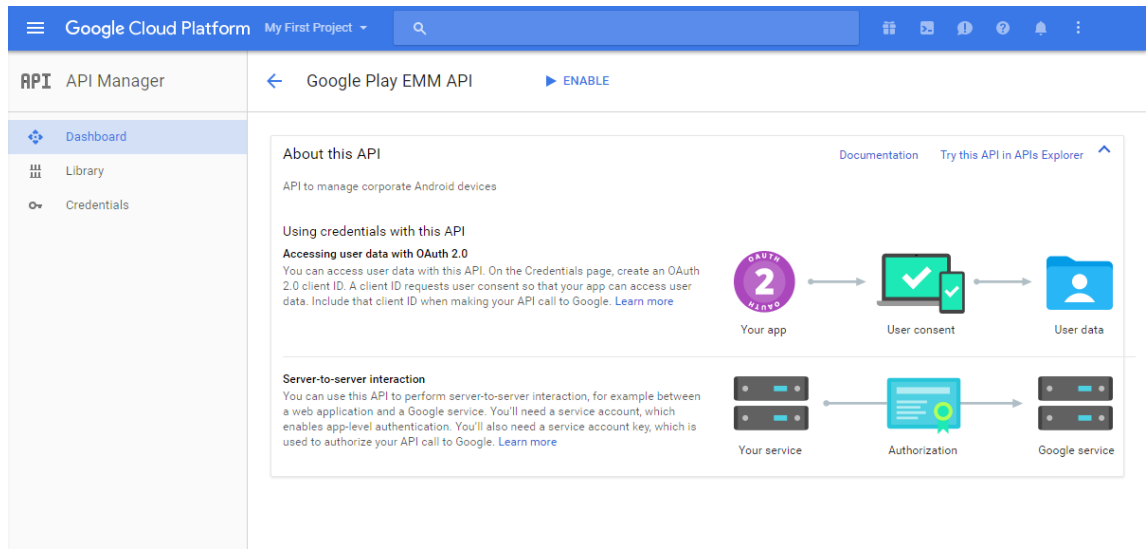
4. 대시보드에서 **Use Google APIs(Google API 사용)** 를 클릭합니다.



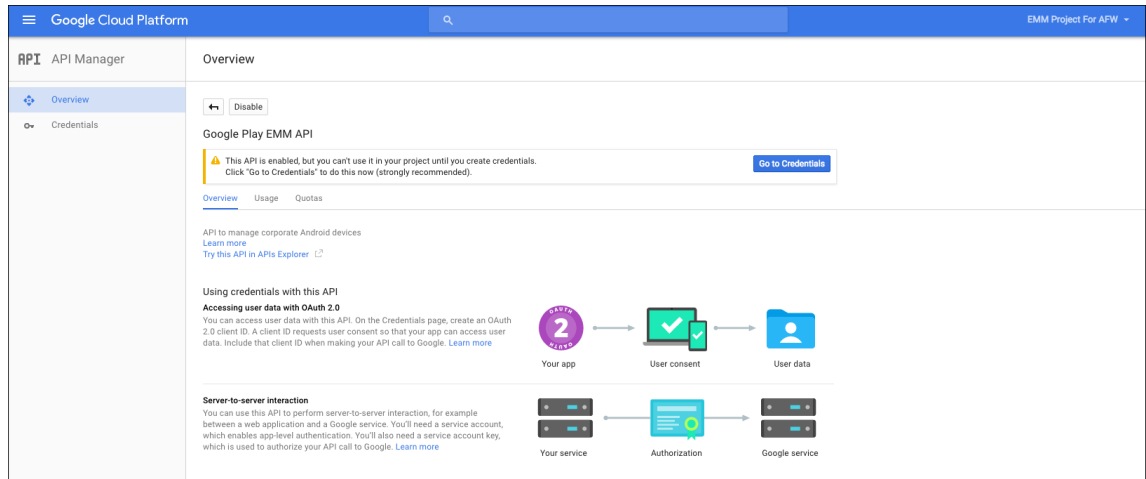
5. **Library**(라이브러리) 를 클릭하고 **Search**(검색) 에 **EMM** 을 입력한 다음 검색 결과를 클릭합니다.



6. **Overview**(개요) 페이지에서 **Enable**(사용) 을 클릭합니다.



7. **Google Play EMM API** 옆에서 **Go to Credentials**(자격 증명으로 이동) 를 클릭합니다.



8. **Add credentials to our project**(프로젝트에 자격 증명 추가) 목록의 1 단계에서 **service account**(서비스 계정) 를 클릭합니다.

9. **Service Accounts(서비스 계정)** 페이지에서 **Create Service Account(서비스 계정 만들기)** 를 클릭합니다.

10. **Create service account(서비스 계정 만들기)** 에서 계정 이름을 지정하고 **Furnish a new private key(새 개인 키 준비)** 확인란을 선택합니다. **P12** 를 클릭하고 **Enable Google Apps Domain-wide Delegation(Google Apps 도메인 전체 위임 사용)** 확인란을 선택한 후 **Create(만들기)** 를 클릭합니다.

Create service account

Service account name [?]
testemmsvcacct

Service account ID
testemmsvcacct @

☒ **Furnish a new private key**
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

☐ JSON
Recommended

☒ **P12**
For backward compatibility with code using the P12 format

☒ **Enable Google Apps Domain-wide Delegation**
Grants a client access to all users' data on a Google Apps domain without manual authorization on their part. [Learn more](#)

To change settings for Google Apps domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.

Product name for the consent screen
anynamewilldo

Create **Configure consent screen** **Cancel**

인증서 (P12 파일) 가 컴퓨터에 다운로드됩니다. 인증서를 안전한 위치에 저장합니다.

11. **Service account created**(서비스 계정 만들어짐) 확인 페이지에서 **Close**(닫기) 를 클릭합니다.

Service account created

The service account "testemmsvcacct" was given editor permission for the project.

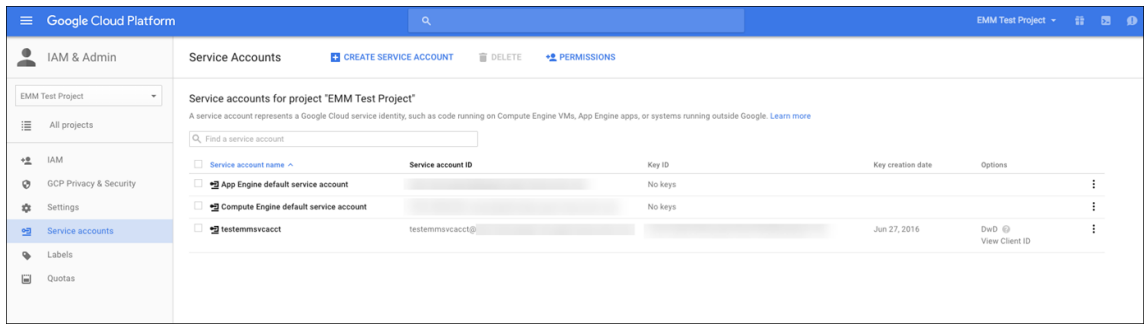
The account's private key **EMM Test Project-37cb73ad0169.p12** has been saved on your computer. This is the only copy of the key, so store it securely.

This is the private key's password. It will not be shown again. You must present this password to use the private key. [Learn more](#)

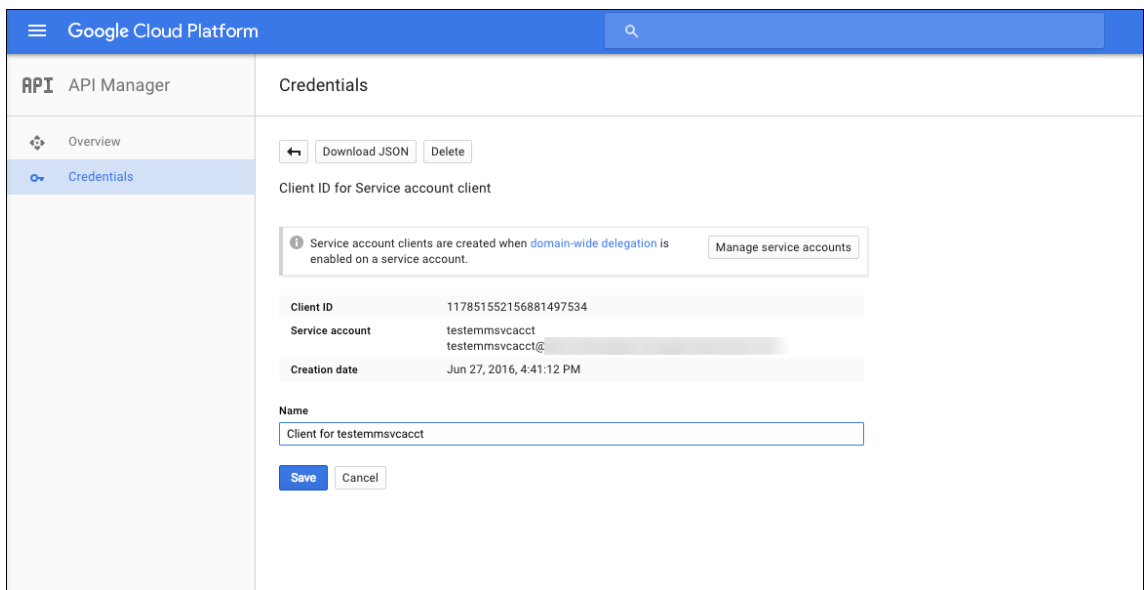
notasecret

Close

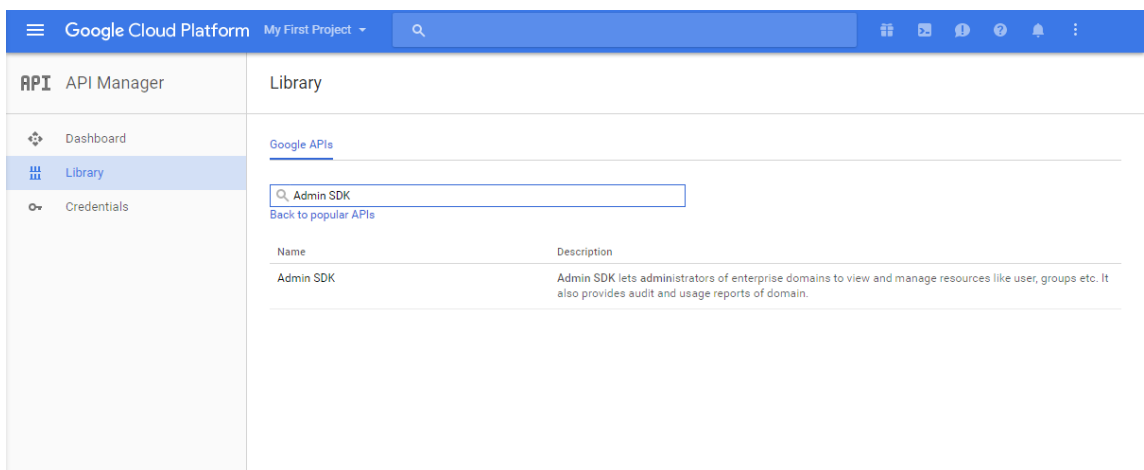
12. **Permissions**(권한) 에서 **Service accounts**(서비스 계정) 를 클릭한 다음 서비스 계정의 **Options**(옵션) 에서 **View Client ID**(클라이언트 ID 보기) 를 클릭합니다.



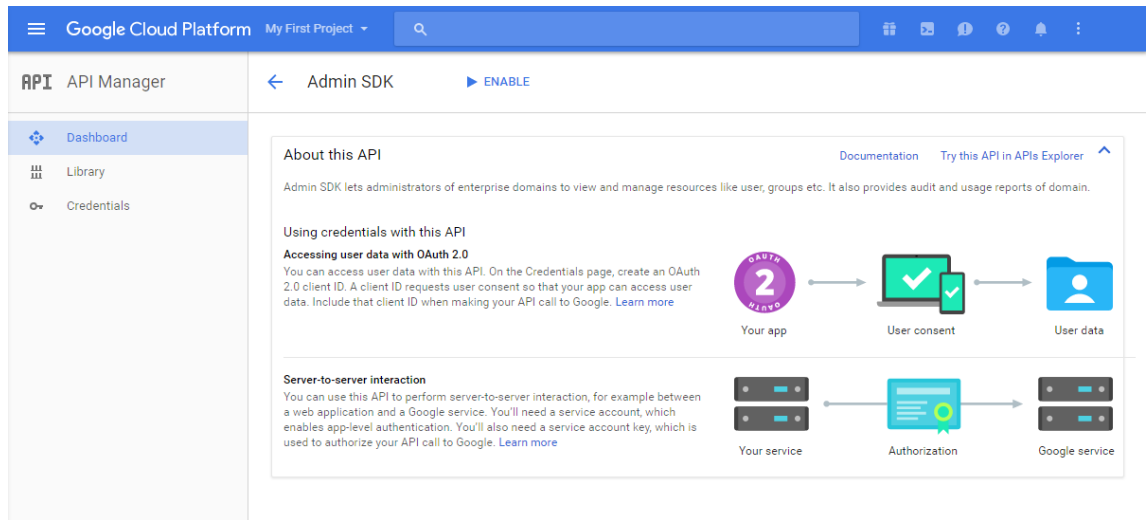
13. Google 관리 콘솔의 계정 승인에 필요한 세부 정보가 표시됩니다. **Client ID(클라이언트 ID)** 및 **Service account ID(서비스 계정 ID)**를 나중에 정보를 검색할 수 있는 위치에 복사합니다. 허용하기 위해 Citrix 지원에 도메인 이름을 보낼 때 이 정보가 필요합니다.



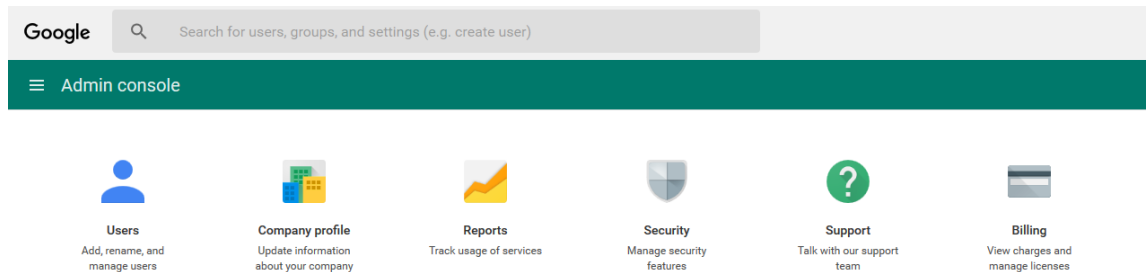
14. **Library(라이브러리)** 페이지에서 **Admin SDK**를 검색한 다음 검색 결과를 클릭합니다.



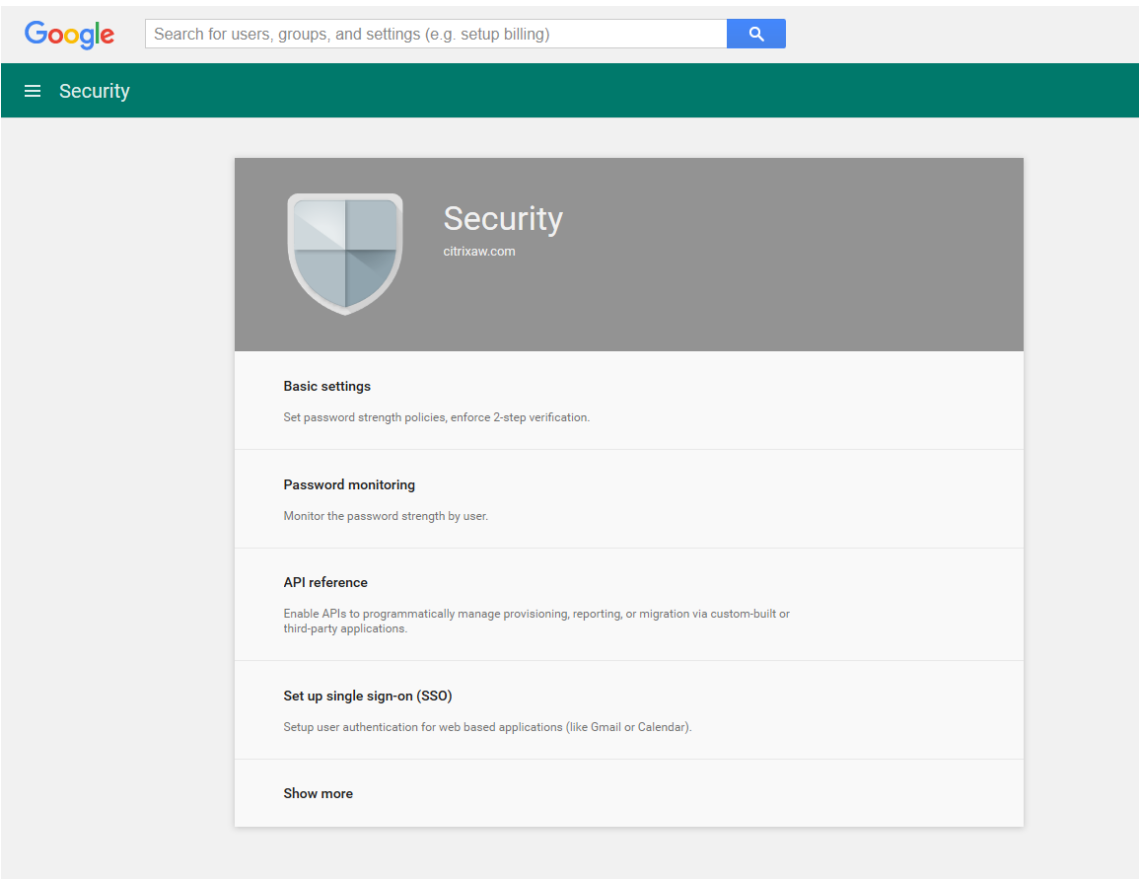
15. **Overview(개요)** 페이지에서 **Enable(사용)**을 클릭합니다.

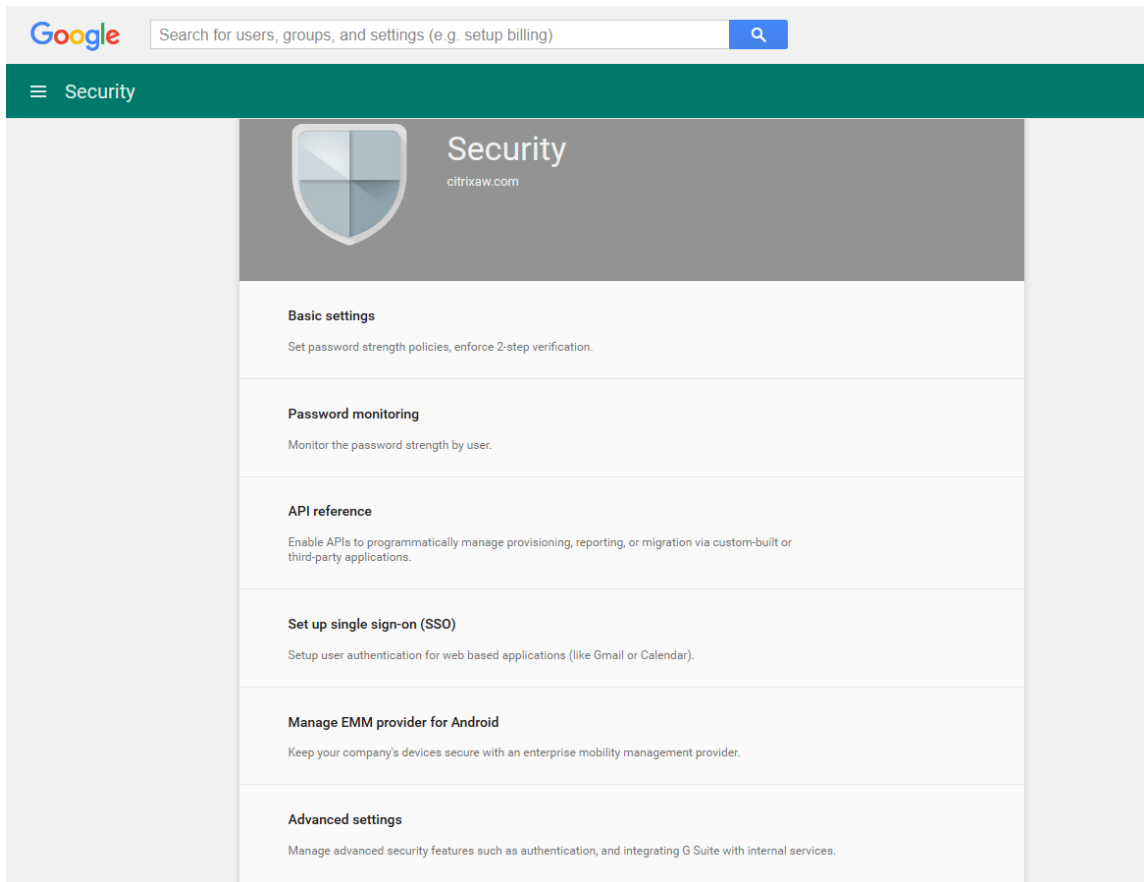


16. 도메인에 대한 Google 관리 콘솔을 연 다음 **Security(보안)** 를 클릭합니다.

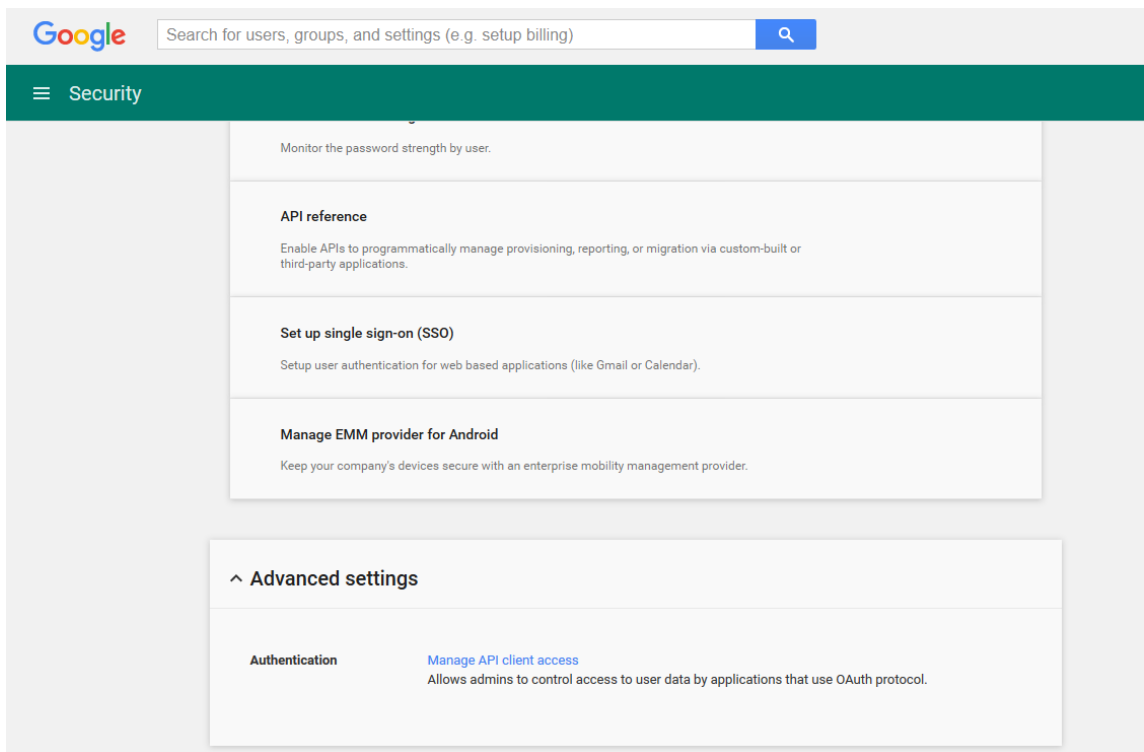


17. **Settings(설정)** 페이지에서 **Show more(자세히 표시)** 를 클릭한 다음 **Advanced settings(고급 설정)** 를 클릭합니다.

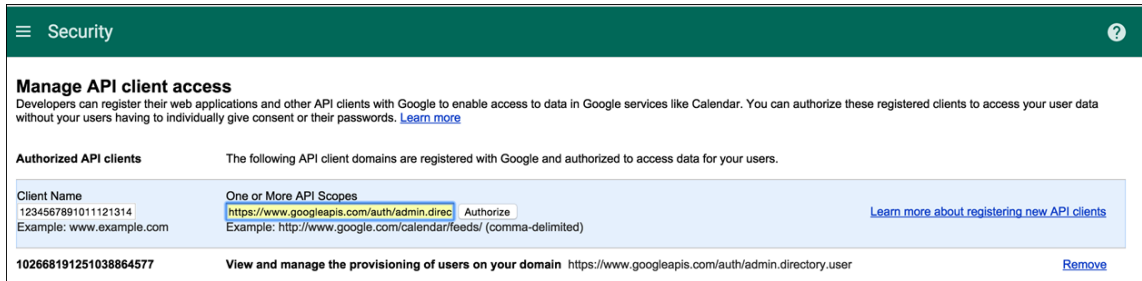




18. **Manage API client access(API 클라이언트 액세스 관리)** 를 클릭합니다.



19. **Client Name**(클라이언트 이름)에 앞서 저장한 클라이언트 ID를 입력하고, **One or More API Scopes**(하나 이상의 API 범위)에 <https://www.googleapis.com/auth/admin.directory.user>를 입력한 다음 **Authorize**(승인)를 클릭합니다.



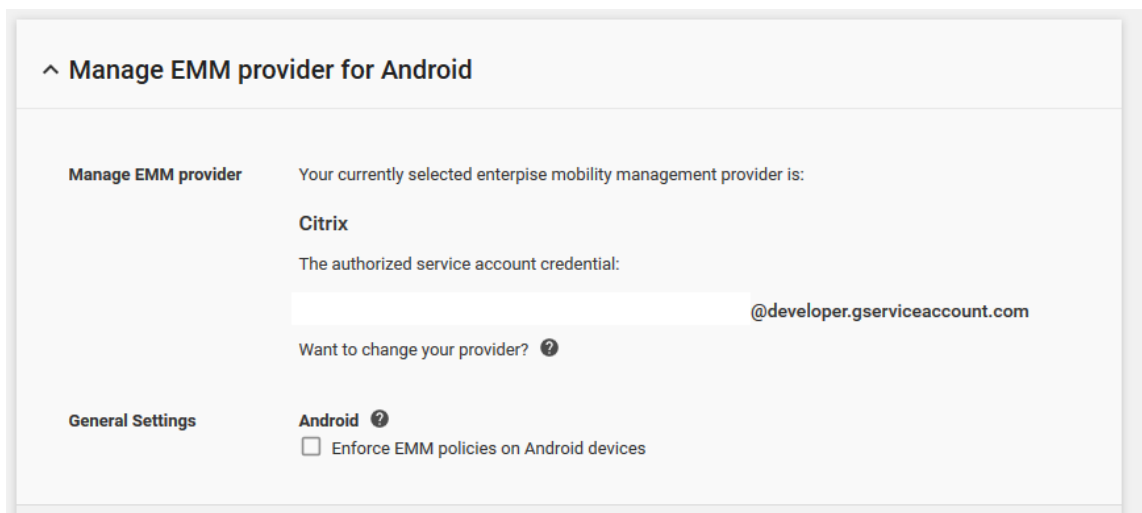
EMM 바인딩

XenMobile을 사용하여 Android 장치를 관리하려면 먼저 Citrix 기술 지원 팀에 연락하여 도메인 이름, 서비스 계정 및 바인딩 토큰을 제공해야 합니다. Citrix는 해당 토큰을 사용자의 EMM(엔터프라이즈 모바일리티 관리) 공급자로 XenMobile에 바인딩합니다. Citrix 기술 지원의 연락처 정보는 [Citrix Technical Support\(Citrix 기술 지원\)](#)를 참조하십시오.

1. 바인딩을 확인하려면 Google Admin 포털에 로그인한 다음 **Security**(보안)를 클릭합니다.
2. **Manage EMM provider for Android(Android용 EMM 공급자 관리)**를 클릭합니다.

Google Android Enterprise 계정이 EMM 공급자로 Citrix에 바인딩되었음을 확인할 수 있습니다.

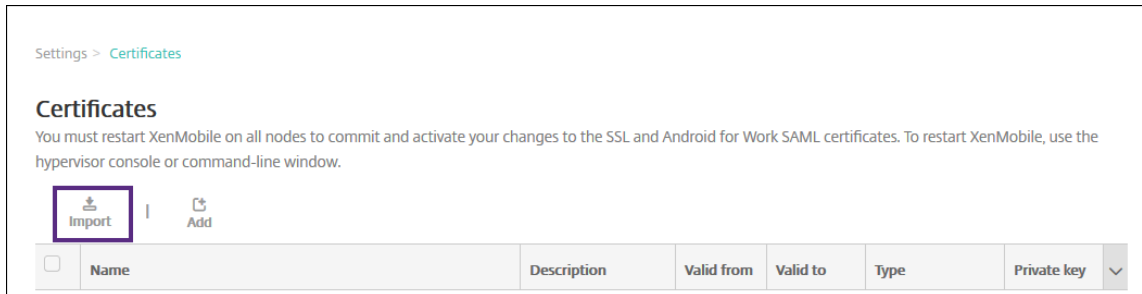
토큰 바인딩을 확인한 후 XenMobile 콘솔을 사용하여 Android 장치를 관리할 수 있습니다. 14 단계에서 생성한 P12 인증서를 가져옵니다. Android Enterprise 서버 설정을 지정하고, SAML 기반 SSO(Single Sign On)를 사용하여 로그인 설정하고, Android Enterprise 장치 정책을 하나 이상 정의합니다.



P12 인증서 가져오기

Android Enterprise P12 인증서를 가져오려면 다음 단계를 따르십시오.

1. XenMobile 콘솔에 로그인합니다.
2. 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭하여 설정 페이지를 연 다음 인증서를 클릭합니다. 인증서 페이지가 나타납니다.



3. 가져오기를 클릭합니다. 가져오기 대화 상자가 나타납니다.

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import

Keystore

Keystore type

PKCS#12

Use as

Server

Keystore file*

A 4d...

Browse

Password*

.....

Description

Cancel

Import

다음 설정을 구성합니다.

- **가져오기:** 목록에서 키 저장소를 클릭합니다.
- **키 저장소 유형:** 목록에서 **PKCS#12** 를 클릭합니다.
- **용도:** 목록에서 서버를 클릭합니다.
- **키 저장소 파일:** 찾아보기를 클릭하고 P12 인증서를 찾아 선택합니다.

- 암호: 키 저장소 암호를 입력합니다.
- 설명: 인증서에 대한 선택적 설명을 입력합니다.

4. 가져오기를 클릭합니다.

Android Enterprise 서버 설정

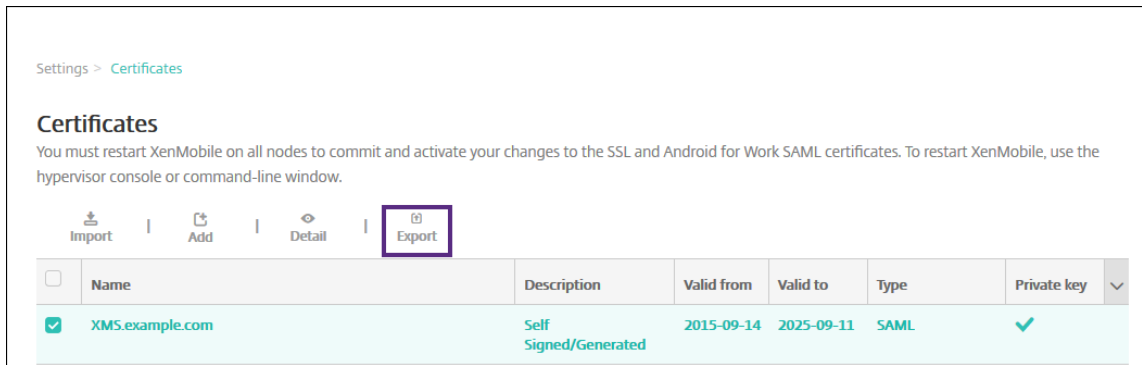
1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 **Android Enterprise** 를 클릭합니다. **Android Enterprise** 페이지가 나타납니다.

다음 설정을 구성한 후 저장을 클릭합니다.

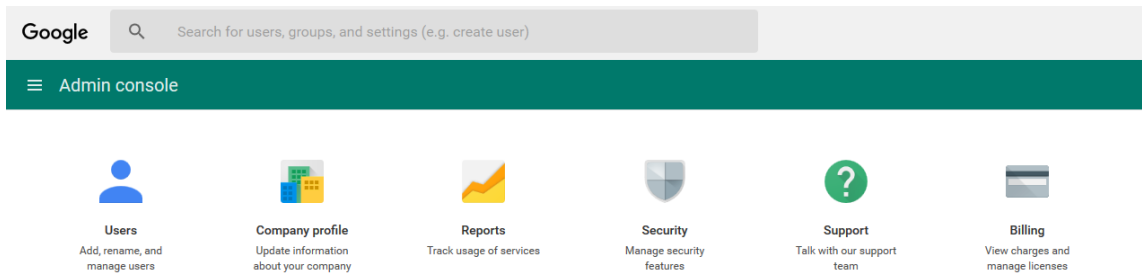
- 도메인 이름: Android Enterprise 도메인 이름을 입력합니다 (예: domain.com).
- 도메인 관리자 계정: 도메인 관리자 사용자 이름을 입력합니다 (예: Google 개발자 포털에 사용되는 전자 메일 계정).
- 서비스 계정 ID: 서비스 계정 ID 를 입력합니다. 예를 들어 Google 서비스 계정에 연결된 전자 메일 (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com) 을 입력합니다.
- 클라이언트 ID: Google 서비스 계정의 클라이언트 ID(숫자) 를 입력합니다.
- **Android Enterprise** 사용: Android Enterprise 를 사용하거나 사용하지 않도록 선택합니다.

SAML 기반 SSO(Single Sign On) 사용

1. XenMobile 콘솔에 로그인합니다.
2. 콘솔 오른쪽 위 모서리에서 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
3. 인증서를 클릭합니다. 인증서 페이지가 나타납니다.



- 인증서 목록에서 SAML 인증서를 클릭합니다.
- 내보내기를 클릭하고 인증서를 컴퓨터에 저장합니다.
- Android Enterprise 관리자 자격 증명을 사용하여 Google Admin 포털에 로그인합니다. 포털 액세스에 대한 자세한 내용은 [Google Admin 포털](#)을 참조하십시오.
- Security(보안)** 를 클릭합니다.



- Security(보안)** 아래에서 **Set up single sign-on (SSO)(SSO(Single Sign-On) 설정)** 을 클릭한 후 다음과 같은 설정을 구성합니다.

^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

☒ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL	<input type="text" value="https://example.com/aw/saml/signin"/>
	URL for signing in to your system and Google Apps
Sign-out page URL	<input type="text" value="https://example.com/aw/saml/signout"/>
	URL for redirecting users to when they sign out
Change password URL	<input type="text" value="https://example.com/aw/saml/changepassword"/>
	URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled
Verification certificate	<div> <div>CHOOSE FILE</div> <div>UPLOAD</div> </div>
	The certificate file must contain the public key for Google to verify sign-in requests. ?
<input type="checkbox"/> Use a domain specific issuer ?	
Network masks	<input type="text"/>
	Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

DISCARD CHANGES [SAVE CHANGES](#)

- **Sign-in page URL(로그인 페이지 URL):** 사용자가 시스템 및 Google Apps 에 로그인할 수 있는 URL 을 입력합니다. 예: <https://<Xenmobile-FQDN>/aw/saml/signin>.
- **Sign out page URL(로그아웃 페이지 URL):** 사용자가 로그아웃한 경우 리디렉션되는 URL 을 입력합니다. 예: <https://<Xenmobile-FQDN>/aw/saml/signout>.
- **Change password URL(암호 변경 URL):** 사용자가 시스템의 암호를 변경할 수 있는 URL 을 입력합니다. 예: <https://<Xenmobile-FQDN>/aw/saml/changepassword>. 이 필드가 정의되어 있으면 SSO 를 사용할 수 없는 경우에도 이 메시지가 표시됩니다.
- **Verification certificate(확인 인증서):** **CHOOSE FILE(파일 선택)** 을 클릭한 다음 XenMobile 에서 내보낸 SAML 인증서를 찾아 선택합니다.

9. **SAVE CHANGES(변경 내용 저장)** 를 클릭합니다.

Android Enterprise 장치 정책 설정

사용자가 처음 등록할 때 장치에 대한 암호를 설정해야 하도록 암호 정책을 설정하십시오.

Passcode Policy	Passcode Policy ✕
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	<div> <div>Passcode Required ON</div> <div> <div>Passcode requirements</div> <div> <div>Minimum length</div> <div>6</div> </div> <div> <div>Biometric recognition</div> <div>OFF</div> </div> <div> <div>Required characters</div> <div>No restriction</div> </div> <div> <div>Advanced rules</div> <div>OFF A 3.0+</div> </div> </div> <div> <div>Passcode security</div> <div> <div>Lock device after (minutes of inactivity) (0-999)</div> <div>None</div> </div> <div> <div>Passcode expiration in days (1-730)</div> <div>0</div> </div> <div> <div>Previous passwords saved (0-50)</div> <div>0</div> <div>?</div> </div> <div> <div>Maximum failed sign-on attempts</div> <div>Not defined</div> <div>?</div> </div> </div> </div>
3 Assignment	<div> <div>Android</div> <div>macOS</div> <div>Android</div> <div>Samsung KNOX</div> <div>Android for Work</div> <div>Windows Phone</div> <div>Windows Desktop/Tablet</div> </div> <div>Deployment Rules</div>

모든 장치 정책을 설정하는 기본 단계는 다음과 같습니다.

1. XenMobile 콘솔에 로그인합니다.
2. 구성을 클릭한 다음 장치 정책을 클릭합니다.
3. 추가를 클릭한 다음 새 정책 추가 대화 상자에서 추가하려는 정책을 선택합니다. 이 예제에서는 암호를 클릭합니다.
4. 정책 정보 페이지를 완성합니다.
5. **Android Enterprise** 를 클릭한 다음 정책에 대한 설정을 구성합니다.
6. 배달 그룹에 정책을 할당합니다.

Android Enterprise 계정 설정 구성

장치에서 Android 앱 및 정책 관리를 시작하려면 먼저 XenMobile 에서 Android Enterprise 도메인 및 계정 정보를 설정해야 합니다. 먼저 Google 에서 Android Enterprise 설정 작업을 완료하여 도메인 관리자를 설정하고 서비스 계정 ID 및 바인딩 토큰을 얻습니다.

1. XenMobile 웹 콘솔에서 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 **Android Enterprise** 를 클릭합니다. **Android Enterprise** 구성 페이지가 나타납니다.

Settings > Android for Work

Legacy Android for Work ▼

Provide Android for Work configuration parameters.

Domain Name * ⓘ

Domain Admin Account * ⓘ

Service Account ID * ⓘ

Client ID * ⓘ

Enable Android for Work ☐ NO

1. **Android Enterprise** 페이지에서 다음 설정을 구성합니다.

- **도메인 이름:** 도메인 이름을 입력합니다.
- **도메인 관리자 계정:** 도메인 관리자 사용자 이름을 입력합니다.
- **서비스 계정 ID:** Google 서비스 계정 ID 를 입력합니다.
- **클라이언트 ID:** Google 서비스 계정의 클라이언트 ID 를 입력합니다.
- **Android Enterprise 사용:** Android Enterprise 를 사용할지 여부를 선택합니다.

2. 저장을 클릭합니다.

XenMobile 에 대한 Google Workspace 파트너 액세스 설정

일부 Chrome 용 엔드포인트 관리 기능은 Google 파트너 API 를 사용하여 XenMobile 과 Google Workspace 도메인 간에 통신합니다. 예를 들어 XenMobile 에는 시크릿 모드와 게스트 모드 같은 Chrome 기능을 관리하기 위한 장치 정책용 API 가 필요합니다.

파트너 API 를 사용하려면 XenMobile 콘솔에서 Google Workspace 도메인을 설정한 다음 Google Workspace 계정을 구성합니다.

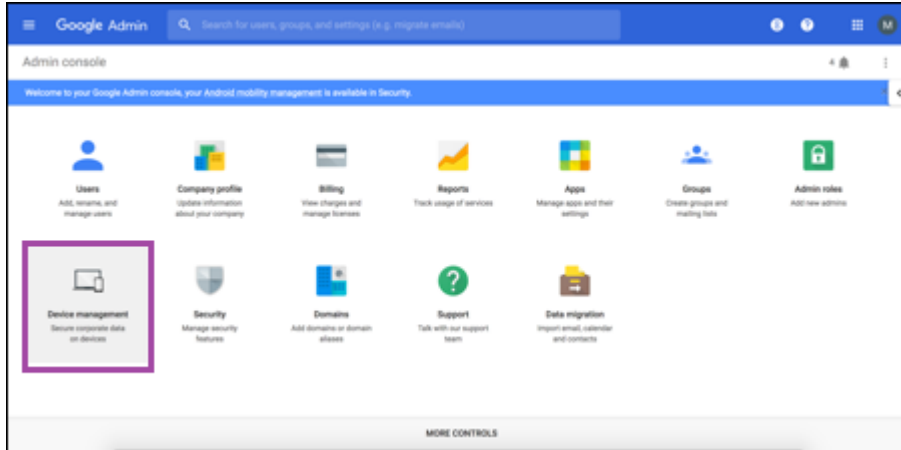
XenMobile 에서 Google Workspace(이전 명칭 G Suite) 도메인 설정

XenMobile 이 Google Workspace 도메인의 API 와 통신하도록 설정하려면 설정 > **Google Chrome** 구성으로 이동하여 설정을 구성합니다.

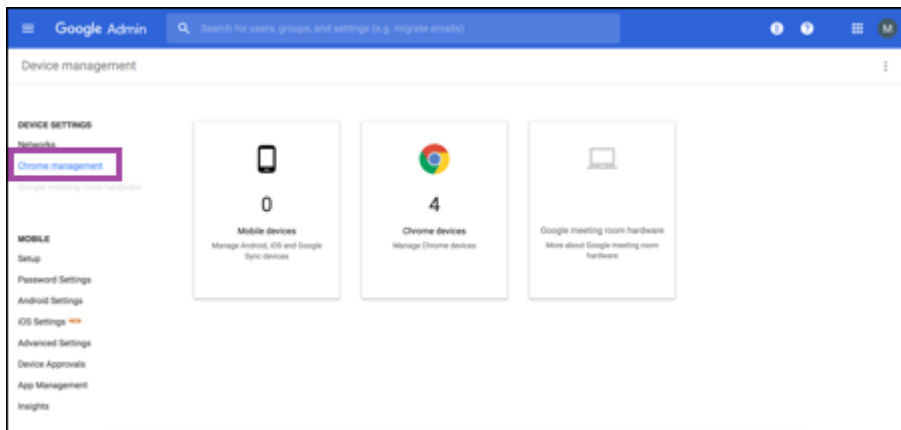
- **G Suite 도메인:** XenMobile 에 필요한 API 를 호스팅하는 Google Workspace 도메인입니다.
- **G Suite 관리 도메인:** G Suite 도메인의 관리자 계정입니다.
- **G Suite 클라이언트 ID:** Citrix 의 클라이언트 ID 입니다. Google Workspace 도메인에 대한 파트너 액세스를 구성하려면 이 값을 사용합니다.
- **G Suite 엔터프라이즈 ID:** 계정의 엔터프라이즈 ID 로, Google Enterprise 계정에서 채워집니다.

Google Workspace 도메인의 장치와 사용자에게 대한 파트너 액세스 설정

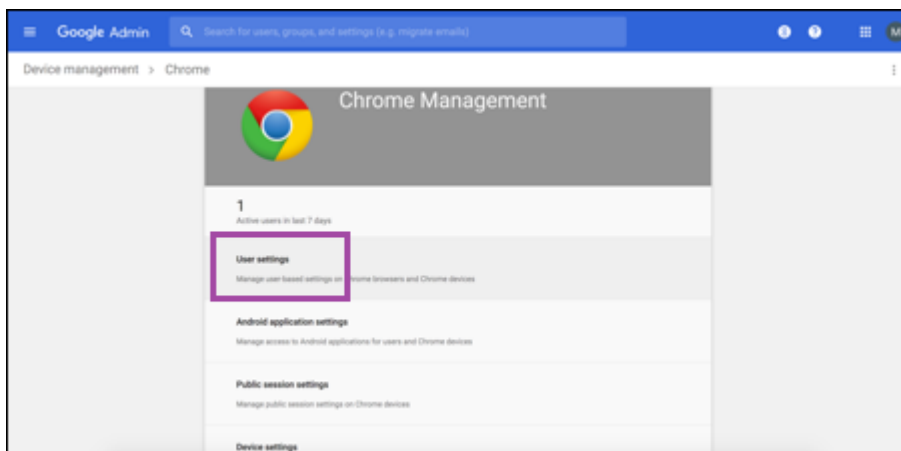
1. Google 관리자 콘솔에 로그인합니다. <https://admin.google.com>
2. **Device Management**(장치 관리) 를 클릭합니다.



3. **Chrome management**(Chrome 관리) 를 클릭합니다.



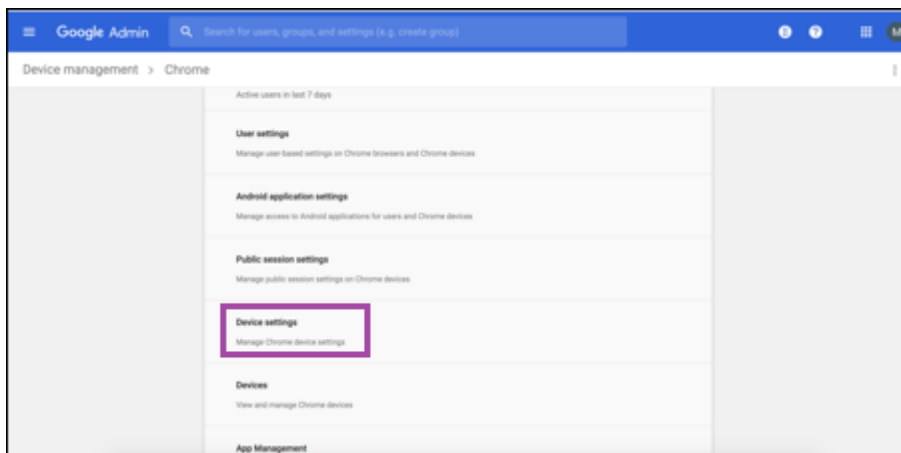
4. **User settings**(사용자 설정) 를 클릭합니다.



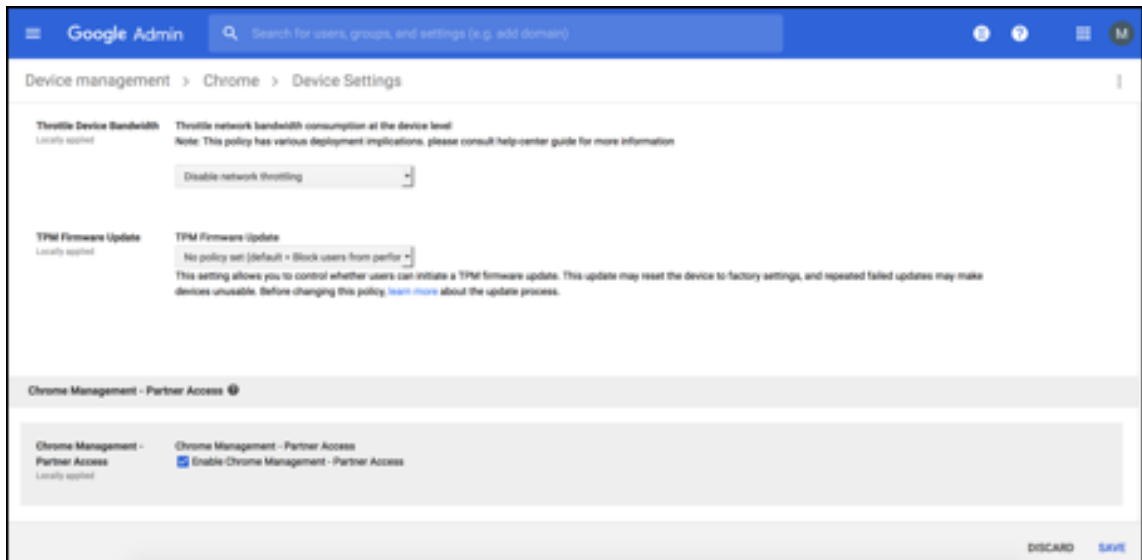
5. **Chrome Management - Partner Access**(Chrome 관리 - 파트너 액세스) 를 검색합니다.



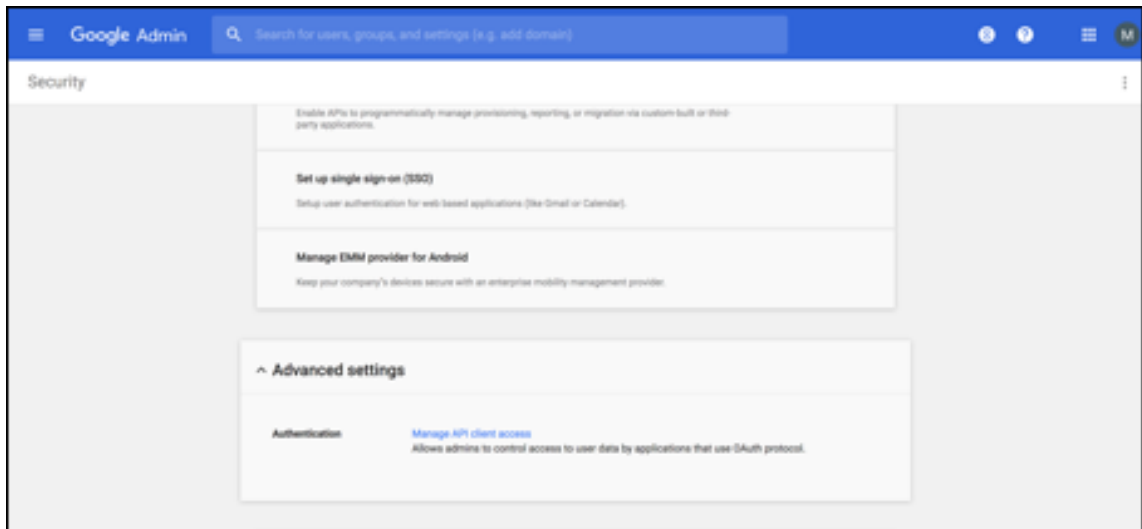
6. **Enable Chrome Management - Partner Access**(Chrome 관리 - 파트너 액세스 사용) 확인란을 선택합니다.
7. 파트너 액세스를 이해하고 사용하길 원한다는 데 동의합니다. 저장을 클릭합니다.
8. Chrome 관리 페이지에서 **Device Settings**(장치 설정) 를 클릭합니다.



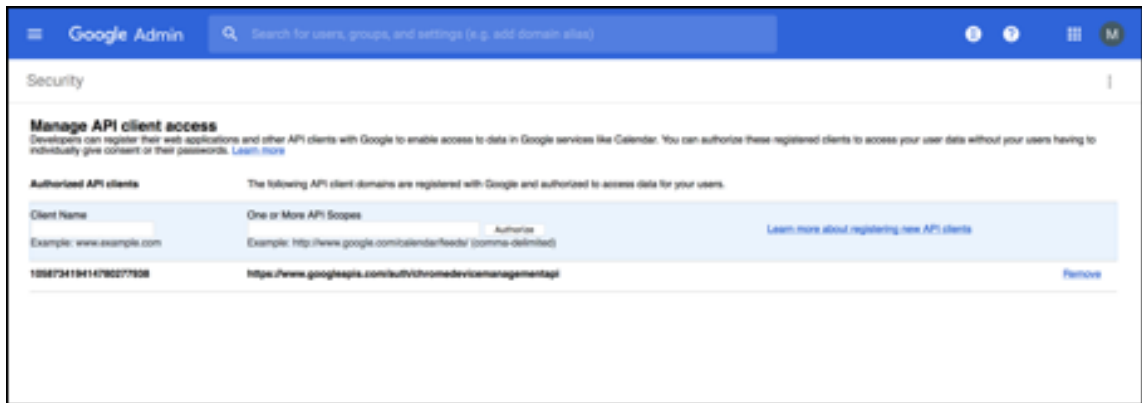
9. **Chrome Management - Partner Access**(Chrome 관리 - 파트너 액세스) 를 검색합니다.



10. **Enable Chrome Management - Partner Access(Chrome 관리 - 파트너 액세스 사용)** 확인란을 선택합니다.
11. 파트너 액세스를 이해하고 사용하길 원한다는 데 동의합니다. 저장을 클릭합니다.
12. **Security(보안)** 페이지로 이동한 다음 **Advanced Settings(고급 설정)** 를 클릭합니다.

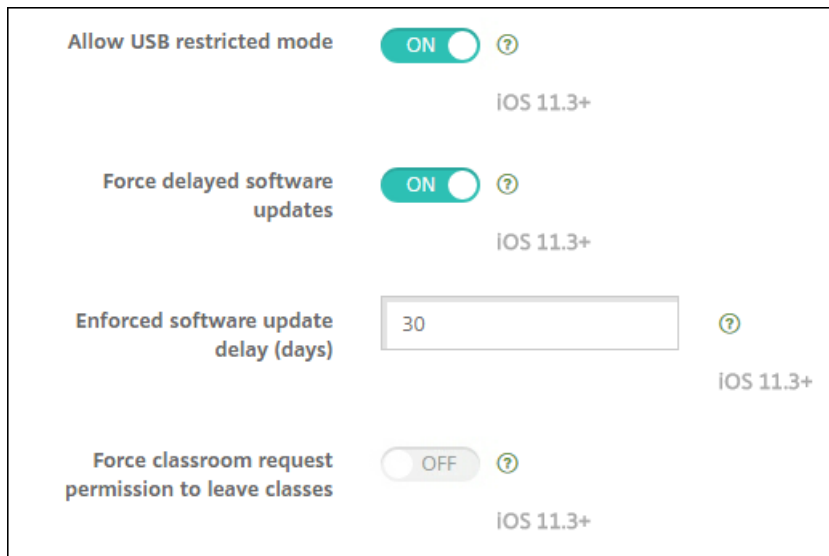


13. **Manage API client access(API 클라이언트 액세스 관리)** 를 클릭합니다.
14. XenMobile 콘솔에서 설정 > **Google Chrome** 구성으로 이동하여 Google Workspace Client ID 의 값을 복사합니다. 그런 다음 **Manage API client Access(API 클라이언트 액세스 관리)** 페이지로 돌아가서 복사한 값을 **Client Name(클라이언트 이름)** 필드에 붙여 넣습니다.
15. **One or More API Scopes(하나 이상의 API 범위)** 에서 URL(<https://www.googleapis.com/auth/chromedevicemanagementapi>) 을 추가합니다.



16. **Authorize(승인)** 을 클릭합니다.

“Your settings have been saved(설정이 저장되었습니다)” 라는 메시지가 표시됩니다.



Android Enterprise 장치 등록

장치 등록 프로세스 동안 사용자가 사용자 이름 또는 사용자 ID 를 입력해야 하는 경우 XenMobile 서버가 무엇 (UPN(사용자 계정 이름) 또는 SAM 계정 이름) 으로 사용자를 검색하도록 구성되었는지에 따라 사용 가능한 형식이 달라집니다.

XenMobile 서버가 UPN 으로 사용자를 검색하도록 구성된 경우 다음 형식으로 UPN 을 입력해야 합니다.

- `username@domain`

XenMobile 서버가 SAM 으로 사용자를 검색하도록 구성된 경우 다음 형식으로 SAM 을 입력해야 합니다.

- `username@domain`
- `domain\username`

XenMobile 서버가 어떤 사용자 이름 유형으로 구성되었는지 확인하려면:

1. XenMobile 서버 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. **LDAP** 를 클릭하여 LDAP 연결 구성을 봅니다.
3. 페이지 하단 가까이에 있는 사용자 검색 기준 필드를 확인합니다.
 - **userPrincipalName** 으로 설정된 경우 XenMobile 서버가 UPN 으로 검색하도록 설정된 것입니다.
 - **sAMAccountName** 으로 설정된 경우 XenMobile 서버가 SAM 으로 검색하도록 설정된 것입니다.

Android Enterprise 엔터프라이즈 등록 취소

XenMobile Server 콘솔 및 XenMobile Tools 를 사용하여 Android Enterprise 엔터프라이즈를 등록 취소할 수 있습니다.

이 작업을 수행하면 XenMobile Server 에서 XenMobile Tools 에 대한 팝업 창이 열립니다. 시작하기 전에 사용하는 브라우저에서 팝업 창을 여는 데 필요한 권한이 XenMobile Server 에 있는지 확인하십시오. Google Chrome 같은 일부 브라우저의 경우 팝업 차단을 사용하지 않도록 설정하고 XenMobile 사이트 주소를 팝업 차단 허용 목록에 추가해야 합니다.

경고:

엔터프라이즈 등록이 취소되면 엔터프라이즈를 통해 이미 등록된 장치의 Android Enterprise 앱이 기본 상태로 재설정됩니다. 장치가 더 이상 Google 을 통해 관리되지 않습니다. Android Enterprise 엔터프라이즈에 다시 등록하는 경우 추가 구성을 수행하지 않으면 이전 기능이 복원되지 않을 수 있습니다.

Android Enterprise 엔터프라이즈 등록 취소 후:

- 엔터프라이즈를 통해 등록된 장치 및 사용자의 Android Enterprise 앱이 기본 상태로 재설정됩니다. 이전에 적용된 Android Enterprise 앱 권한 및 Android Enterprise 앱 제한 정책이 더 이상 유효하지 않습니다.
- 엔터프라이즈를 통해 등록된 장치는 XenMobile 을 통해 관리되지만 Google 측면에서는 관리되지 않습니다. 새로운 Android Enterprise 앱을 추가할 수 없습니다. 새로운 Android Enterprise 앱 권한 또는 Android Enterprise 앱 제한 정책을 적용할 수 없습니다. 예약, 암호 및 제한 같은 다른 정책은 계속해서 이러한 장치에 적용할 수 있습니다.
- Android Enterprise 에 장치를 등록하려고 하면 Android Enterprise 장치가 아닌 Android 장치로 등록됩니다.

Android Enterprise 엔터프라이즈를 등록 취소하려면:

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 설정 페이지에서 **Android Enterprise** 를 클릭합니다.
3. 엔터프라이즈 제거를 클릭합니다.

Settings > Android for Work

Android for Work

Android for Work To set up Android for Work for your company, you need to bind XenMobile as your enterprise mobile management (EMM) provider through Google Play.

Enterprise ID	Name	Created Time	
LC01e0ao50	AFW enterprise	1/8/18 2:26:18 pm	▼

Showing 1 - 1 of 1 items Items per page: 10 ▼

Enable Android for Work ☒

[Remove Enterprise](#)

4. 암호를 지정합니다. 그 다음 단계에서 등록 취소를 완료하려면 암호가 필요합니다. 그런 다음 등록 취소를 클릭합니다.

Settings > Android for Work

Android for Work

Android for Work To set up Android for Work for your company, you need to bind XenMobile as your enterprise mobile management (EMM) provider through Google Play.

Enterprise ID	Name	Created Time	
LC01e0ao50	AFW enterprise	1/8/18 2:26:18 pm	▼

Showing 1 - 1 of 1 items Items per page: 10 ▼

Enable Android for Work ☒

Specify a password then press Unenroll to initiate the process to remove the enterprise. You will need to provide this password in the next step.
Please disable any popup blockers as this step requires opening XenMobile Tools in a new tab.

New password: *

Confirm password: *

[Unenroll](#) [Cancel](#)

5. XenMobile Tools 페이지가 열리면 이전 단계에서 만든 암호를 입력합니다.

All Management Tools > Android for Work

Unenroll Android Enterprise

1

Enter password and press Next to continue unenrollment process.

Password must be least 4 characters.

Next

2

Enter the email address of any administrator for the enterprise and press Unenroll to complete unenrollment.

Unenroll

3

Complete Steps 1 and 2.

6. 등록 취소를 클릭합니다.

All Management Tools > Android for Work

Unenroll Android Enterprise

1

Enter password and press Next to continue unenrollment process.

Password must be least 4 characters.

Next

2

Press Unenroll to complete unenrollment.

AFW enterprise
LC01e0ao50

Unenroll

3

Complete Steps 1 and 2.

Android Enterprise 에서 완전하게 관리되는 장치 프로비전

회사 소유 장치만 Android Enterprise 에서 완전하게 관리되는 장치가 될 수 있습니다. 완전하게 관리되는 장치에서는 작업 프로필뿐만 아니라 전체 장치가 회사 또는 조직에 의해 제어됩니다. 완전하게 관리되는 장치를 작업 관리 장치라고도 합니다.

XenMobile 은 완전하게 관리되는 장치에 대해 다음과 같은 등록 방법을 지원합니다.

- **afw#xenmobile:** 이 등록 방법을 사용하는 경우 사용자가 장치를 설정할 때 “afw#xenmobile” 문자를 입력합니다. 이 토큰은 XenMobile 이 관리하는 장치로 장치를 식별하고 Secure Hub 를 다운로드합니다.
- **QR 코드:** QR 코드 프로비저닝을 통해 태블릿과 같이 NFC 를 지원하지 않는 분산된 제품군의 장치를 간편하게 프로비저닝할 수 있습니다. QR 코드 등록 방법은 출고 기본값으로 재설정된 제품군 장치에 사용할 수 있습니다. QR 코드 등록 방법은 설치 마법사에서 QR 코드를 스캔하여 완전하게 관리되는 장치를 설정하고 구성합니다.
- **NFC(근거리 통신) 범프:** NFC 범프 등록 방법은 출고 기본값으로 재설정된 제품군 장치에 사용할 수 있습니다. NFC 범프는 근거리 통신을 사용하여 두 장치 간 데이터를 전송합니다. 출고 기본값으로 재설정된 장치에서는 Bluetooth, Wi-Fi 및 기타 통신 모드를 사용할 수 없습니다. NFC 는 이 상태에서 장치가 사용할 수 있는 유일한 통신 프로토콜입니다.

afw#xenmobile

이 등록 방법은 새 장치 또는 출고 기본값으로 재설정된 장치의 전원을 켜 후 초기 설정 시 사용됩니다. Google 계정을 입력하라는 메시지가 표시되면 사용자가 “afw#xenmobile” 을 입력합니다. 이 동작을 수행하면 Secure Hub 가 다운로드되고 설치됩니다. 그런 다음 사용자는 Secure Hub 설정 메시지에 따라 등록을 완료합니다.

최신 버전의 Secure Hub 가 Google Play Store 에서 다운로드되므로 이 등록 방법이 대부분의 고객에게 권장됩니다. 다른 등록 방법과 달리, XenMobile Server 에서 다운로드하기 위해 Secure Hub 를 제공하지 않습니다.

필수 구성 요소:

- Android 5.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.

QR 코드

장치 모드에서 QR 코드를 사용하여 장치를 등록하려면 JSON 을 생성하고 JSON 을 QR 코드로 변환하여 QR 코드를 생성합니다. QR 코드가 장치 카메라로 스캔되어 장치가 등록됩니다.

필수 구성 요소:

- Android 7.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.

JSON 에서 **QR** 코드 생성 다음 필드를 사용하여 JSON 을 생성합니다.

다음 필드는 필수입니다.

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

값: com.zenprise/com.zenprise.configuration.AdminFunction

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

값: qn7oZUtheu3JBainzZRrjCQv6LOO6Ll1OjcxT3-yKM

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

값: <https://path/to/securehub.apk>

참고:

Secure Hub 가 엔터프라이즈 앱으로 Citrix XenMobile 서버에 업로드된 경우 https://<fqdn>:4443/*instanceName*/worxhome.apk에서 다운로드할 수 있습니다. Secure Hub APK 의 경로는 프로비저닝 시 장치가 연결되는 Wi-Fi 연결을 통해 액세스할 수 있어야 합니다.

다음 필드는 선택 사항입니다.

- **android.app.extra.PROVISIONING_LOCALE:** 언어 및 국가 코드를 입력합니다.

언어 코드는 [ISO 639-1](#)에 정의된 대로 소문자 두 자로 구성된 ISO 언어 코드입니다 (예: en). 국가 코드는 [ISO 3166-1](#)에 정의된 대로 대문자 두 자로 구성된 ISO 국가 코드입니다 (예: US). 예를 들어, 미국에서 사용하는 영어의 경우 en_US 를 입력합니다.

- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가 실행되고 있는 표준 시간대입니다.

[지역/위치 형식의 Olson 이름](#)을 입력합니다. 예를 들어 태평양 표준시의 경우 America/Los_Angeles 를 입력합니다. 입력하지 않으면 표준 시간대가 자동으로 입력됩니다.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Epoch 이후의 시간 (밀리초) 입니다.

Unix Epoch(즉 Unix 시간 또는 POSIX 시간 Unix 타임스탬프) 는 1970 년 1 월 1 일 (자정 UTC/GMT) 이후 경과한 시간이며, 윤초는 계산되지 않습니다 (ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 프로필 생성 시 암호화를 건너뛰려면 **true** 로 설정합니다. 프로필 생성 시 암호화를 적용하려면 **false** 로 설정합니다.

일반적인 JSON 은 다음과 같은 형식입니다.

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": " ",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

JSON 유효성 검사 도구 (예: <https://jsonlint.com>) 를 사용하여 생성된 JSON 의 유효성을 검사하고 온라인 QR 코드 생성기 (예: <https://goqr.me>) 를 사용하여 해당 JSON 문자열을 QR 코드로 변환합니다.

이 QR 코드는 출고 기본값으로 재설정된 장치에서 스캔되어 해당 장치가 작업 관리 장치 모드로 등록됩니다.

장치를 등록하려면

완전하게 관리되는 장치로 장치를 등록하려면 장치가 출고 기본값으로 재설정된 상태여야 합니다.

1. 시작 화면에서 화면을 6 번 눌러 QR 코드 등록 흐름을 시작합니다.
2. 메시지가 표시되면 Wi-Fi 에 연결합니다. QR 코드에 있는 Secure Hub 의 다운로드 위치 (JSON 으로 인코딩됨) 는 이 Wi-Fi 네트워크를 통해 액세스할 수 있습니다.
장치가 Wi-Fi 에 연결되면 Google 에서 QR 코드 판독기를 다운로드하고 카메라를 시작합니다.
3. 카메라로 QR 코드를 가리키고 코드를 스캔합니다.
Android 는 QR 코드에 있는 다운로드 위치에서 Secure Hub 를 다운로드하고 서명 인증서 서명의 유효성을 검사한 후 Secure Hub 를 설치하고 장치 소유자로 설정합니다.

자세한 내용은 Android EMM 개발자용 Google 가이드 (https://developers.google.com/android/work/prov-devices#qr_code_method) 를 참조하십시오.

NFC 범프

NFC 범프를 사용하여 완전하게 관리되는 장치로 장치를 등록하려면 두 장치, 즉 출고 기본값으로 재설정된 장치와 XenMobile Provisioning Tool 을 실행하는 장치가 필요합니다.

필수 구성 요소:

- Android 5.0, Android 5.1, Android 6.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.
- Android Enterprise 를 사용하도록 설정한 XenMobile Server 버전 10.4
- 완전하게 관리되는 장치로서 Android Enterprise 용으로 프로비전된 새 장치 또는 출고 기본값으로 재설정된 장치. 이 사전 요구 사항을 완료하는 단계는 이 문서의 뒷부분에서 찾을 수 있습니다.
- NFC 호환성이 있으며 구성된 Provisioning Tool 이 실행되고 있는 또 다른 장치. Provisioning Tool 은 Secure Hub 10.4 또는 [Citrix 다운로드 페이지](#)에서 사용할 수 있습니다.

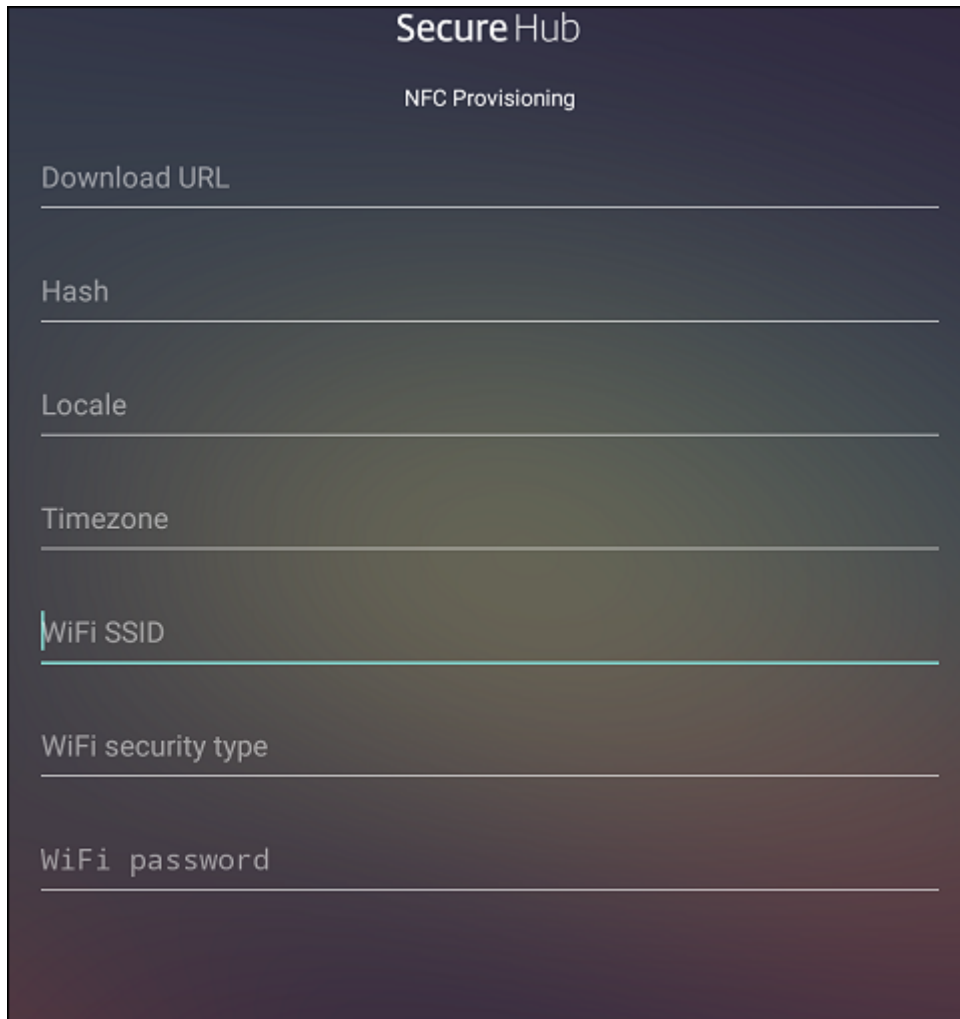
각 장치에는 EMM(엔터프라이즈 모빌리티 관리) 앱으로 관리되는 Android Enterprise 프로필이 하나만 있을 수 있습니다. XenMobile 에서 Secure Hub 는 EMM 앱입니다. 각 장치에는 하나의 프로필만 허용됩니다. 두 번째 EMM 앱을 추가하면 첫 번째 EMM 앱이 제거됩니다.

NFC 범프를 통해 전송된 데이터 출고 기본값으로 재설정된 장치를 프로비저닝하려면 NFC 범프를 통해 다음 데이터를 전송하여 Android Enterprise 를 초기화해야 합니다.

- 장치 소유자 (이 경우 Secure Hub) 역할을 하는 EMM 공급자 앱의 패키지 이름
- 장치가 EMM 공급자 앱을 다운로드 할 수 있는 인트라넷/인터넷 위치
- 다운로드가 성공했는지 확인하기 위한 EMM 공급자 앱의 SHA1 해시
- 출고 기본값으로 재설정된 장치가 연결하여 EMM 공급자 앱을 다운로드할 수 있는 Wi-Fi 연결 세부 정보. 참고: 이 단계에서 Android 는 802.1x Wi-Fi 를 지원하지 않습니다.
- 장치의 표준 시간대 (선택 사항)
- 장치의 지리적 위치 (선택 사항)

두 장치가 범프되면 Provisioning Tool 의 데이터가 출고 기본값으로 재설정된 장치로 전송됩니다. 이 데이터는 관리자 설정으로 Secure Hub 를 다운로드하는 데 사용됩니다. 표준 시간대 및 위치 값을 입력하지 않으면 Android 가 자동으로 새 장치에서 이러한 값을 구성합니다.

XenMobile Provisioning Tool 구성 NFC 범프를 수행하기 전에 Provisioning Tool 을 구성해야 합니다. 이 구성은 NFC 범프 중에 출고 기본값으로 재설정된 장치로 전송됩니다.

The image shows a dark-themed configuration screen for 'SecureHub' under the 'NFC Provisioning' section. It contains several text input fields with labels: 'Download URL', 'Hash', 'Locale', 'Timezone', 'WiFi SSID' (which has a blue vertical bar on its left), 'WiFi security type', and 'WiFi password'. Each field is represented by a horizontal line.

필요한 필드에 데이터를 입력하거나 텍스트 파일을 통해 데이터를 채울 수 있습니다. 다음 절차의 단계에서는 텍스트 파일을 구성하고 각 필드에 대한 설명을 포함시키는 방법에 대해 설명합니다. 입력한 정보가 앱에 저장되지 않으므로 나중에 사용할 수 있도록 정보를 유지하려면 텍스트 파일을 만들 수 있습니다.

텍스트 파일을 사용하여 **Provisioning Tool** 을 구성하려면 파일의 이름을 nfcprovisioning.txt 로 지정하고 장치의 SD 카드에 있는 /sdcard/ 폴더에 파일을 저장합니다. 그러면 앱에서 텍스트 파일을 읽고 값을 채울 수 있습니다.

텍스트 파일에는 다음과 같은 데이터가 포함되어야 합니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=  
=<download_location>
```

이 줄은 EMM 공급자 앱의 인트라넷/인터넷 위치입니다. NFC 범프 후에 출고 기본값으로 재설정된 장치가 Wi-Fi에 연결되면 장치가 이 위치에 액세스하여 다운로드할 수 있어야 합니다. URL은 특수한 형식이 필요하지 않은 일반 URL입니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1  
hash>
```

이 줄은 EMM 공급자 앱의 체크섬입니다. 이 체크섬은 다운로드가 성공했는지 확인하는 데 사용됩니다. 체크섬을 얻는 단계에 대해서는 이 문서 뒷부분에서 설명합니다.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

이 줄은 Provisioning Tool이 실행되고 있는 장치의 연결된 Wi-Fi SSID입니다.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type  
>
```

지원되는 값은 WEP 및 WPA2입니다. Wi-Fi가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Wi-Fi가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

언어 및 국가 코드를 입력합니다. 언어 코드는 [ISO 639-1](#)에 정의된 대로 소문자 두 자로 구성된 ISO 언어 코드입니다 (예: en). 국가 코드는 [ISO 3166-1](#)에 정의된 대로 대문자 두 자로 구성된 ISO 국가 코드입니다 (예: US). 예를 들어, 미국에서 사용하는 영어의 경우 en_US를 입력합니다. 코드를 입력하지 않으면 국가 및 언어가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

장치가 실행되는 표준 시간대입니다. [지역/위치 형식의 Olson 이름](#)을 입력합니다. 예를 들어 태평양 표준시의 경우 America/Los_Angeles를 입력합니다. 이름을 입력하지 않으면 표준 시간대가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package  
name>
```

값이 앱에 Secure Hub로 하드 코딩되어 있기 때문에 이 데이터는 필요하지 않습니다. 여기서는 완결성을 위해 언급되었습니다.

예를 들어 WPA2를 사용하여 보호되는 Wi-Fi가 있는 경우 완성된 nfcprovisioning.txt 파일은 다음과 같습니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION  
=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR  
\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

예를 들어 보호되지 않는 Wi-Fi 가 있는 경우 완성된 nfcprovisioning.txt 파일은 다음과 같습니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJJ72LGR
\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Secure Hub 체크섬을 얻으려면 특정 앱의 체크섬을 얻으려면 앱을 엔터프라이즈 앱으로 추가합니다.

1. XenMobile 콘솔에서 구성 > 앱으로 이동한 후 추가를 클릭합니다.

앱 추가 창이 나타납니다.

2. 엔터프라이즈를 클릭합니다.

앱 정보 페이지가 나타납니다.

3. 다음과 같은 구성을 선택한 후 다음을 클릭합니다.

Android Enterprise 엔터프라이즈 앱 페이지가 나타납니다.

The screenshot shows the 'Enterprise App Information' configuration page. On the left, a sidebar lists the steps: 1. App Information, 2. Platform, 3. Approvals (optional), and 4. Delivery Group Assignments (optional). Under step 2, 'Android for Work' is selected, highlighted with a red box. The main configuration area shows 'Name' as 'Secure Home', 'Description' as an empty text box, and 'App category' as 'All Selected'. A red arrow points to the 'Next >' button at the bottom right.

4. .apk 에 대한 경로를 제공한 후 다음을 클릭하고 파일을 업로드합니다.

업로드가 완료되면 업로드된 패키지의 세부 정보가 나타납니다.

5. 다음을 클릭하여 JSON 파일을 다운로드하는 페이지를 엽니다. 이 파일을 사용하여 Google Play에 업로드할 수 있습니다. Secure Hub의 경우 Google Play에 업로드할 필요가 없지만 SHA1 값을 읽으려면 JSON 파일이 필요합니다.

일반적인 JSON 파일은 다음과 같은 형식입니다.

6. **file_sha1_base64** 값을 복사한 후 Provisioning Tool의 해시 필드에 이 값을 사용합니다.

참고:

해시는 URL로 사용할 수 있는 형식이어야 합니다.

- 모든 + 기호를 -로 변환합니다.
- 모든 / 기호를 _로 변환합니다.
- 끝에 있는 \u003d를 =로 바꿉니다.

장치의 SD 카드에 있는 nfcprovisioning.txt 파일에 해시를 저장하면 앱에서 안전을 위한 변환을 수행합니다. 하지만 수동으로 해시를 입력하는 경우 URL 안전성을 보장하는 것은 사용자의 책임입니다.

사용된 라이브러리 Provisioning Tool의 소스 코드에는 다음과 같은 라이브러리가 사용되었습니다.

- Apache 라이선스 2.0에 따라 Google이 제작한 v7 appcompat 라이브러리, 디자인 지원 라이브러리 및 v7 Palette 라이브러리

자세한 내용은 [지원 라이브러리 기능 가이드](#)를 참조하십시오.

- Apache 라이선스 2.0에 따라 Jake Wharton이 제작한 [Butter Knife](#)

Android Enterprise에서 작업 프로필 장치 프로비전

Android Enterprise에서 작업 프로필 장치에 대해 회사 영역과 개인 영역을 안전하게 분리할 수 있습니다. 예를 들어 BYOD 장치는 작업 프로필 장치가 될 수 있습니다. 작업 프로필 장치의 등록 환경은 XenMobile의 Android 등록과 비슷합니다. 사용자가 Google Play에서 Secure Hub를 다운로드하고 장치를 등록합니다.

Android Enterprise 에서 작업 프로필 장치로 장치를 등록하는 경우 USB 디버깅 및 알 수 없는 소스 설정은 장치에서 기본적으로 비활성화됩니다.

팁:

Android Enterprise 에서 작업 프로필 장치로 장치를 등록하는 경우 항상 Google Play 로 이동하십시오. 거기서 사용자의 개인 프로필에 Secure Hub 가 표시되도록 설정합니다.

iOS

March 15, 2024

XenMobile Server 에서 iOS 장치를 관리하려면 Apple 의 APNs(Apple 푸시 알림 서비스) 인증서를 설정합니다. 자세한 내용은 [APN 인증서](#)를 참조하십시오.

등록 프로필은 사용자가 MDM 을 취소할 수 있는 옵션과 함께 iOS 장치가 MDM+MAM 으로 등록되는지 여부를 결정합니다. XenMobile Server 는 MDM+MAM 에서 iOS 장치에 대해 다음과 같은 인증 유형을 지원합니다. 자세한 내용은 [인증서 및 인증](#)에 있는 문서를 참조하십시오.

- 도메인
- 도메인 및 보안 토큰
- 클라이언트 인증서
- 클라이언트 인증서와 도메인

iOS 13 의 신뢰할 수 있는 인증서에 대한 요구 사항:

Apple 은 TLS 서버 인증서에 대한 새로운 요구 사항을 도입했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는지 확인하십시오. Apple 게시물 <https://support.apple.com/en-us/HT210176>를 참조하십시오. 인증서 관리에 대한 도움말은 [XenMobile Server 에서 인증서 업로드](#)를 참조하십시오.

지원되는 운영 체제에 대해서는 [지원되는 장치 운영 체제](#)를 참조하십시오.

iOS 14 호환 기능

XenMobile Server 및 Citrix 모바일 앱은 iOS 14 와 호환되지만 현재는 새로운 iOS 14 기능을 지원하지 않습니다.

감독되는 iOS 기기의 경우 소프트웨어 업그레이드를 최대 90 일까지 지연시킬 수 있습니다. iOS 에 대한 제한 장치 정책에서 다음 설정을 사용합니다.

- 소프트웨어 업데이트 강제 지연
- 소프트웨어 업데이트 시행 지연

[iOS 설정](#)을 참조하십시오. 사용자 등록 모드 또는 감독되지 않은 (전체 MDM) 모드의 장치에는 이러한 설정을 사용할 수 없습니다.

열린 상태로 유지되어야 하는 **Apple** 호스트 이름

일부 Apple 호스트 이름은 iOS, macOS 및 Apple App Store 의 올바른 작동을 보장하기 위해 열린 상태로 유지되어야 합니다. 이러한 호스트 이름을 차단하면 iOS, iOS 앱, MDM 작업, 장치 및 앱 등록 등의 설치, 업데이트 및 적절한 작동에 영향을 줄 수 있습니다. 자세한 내용은 <https://support.apple.com/en-us/HT201999> 항목을 참조하십시오.

지원되는 등록 방법

등록 프로필의 iOS 장치 관리 방법을 지정합니다. 장치 등록 또는 MDM 등록 안 함을 선택할 수 있습니다.

iOS 장치의 등록 설정을 구성하려면 구성 > 등록 프로필 > **iOS** 로 이동합니다.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ⓘ Management <input checked="" type="radio"/> Device enrollment ⓘ <input type="radio"/> Do not manage devices ⓘ
Android	Application management ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ
iOS	User consent Allow users to decline device management <input checked="" type="checkbox"/> ⓘ
3 Assignment (optional)	

다음 표에는 XenMobile Server 가 iOS 장치에 대해 지원하는 등록 방법이 나와 있습니다.

방법	지원됨
Apple 배포 프로그램	예
Apple School Manager	예
Apple Configurator	예
수동 등록	예
등록 초대	예

Apple 에는 비즈니스 및 교육 계정을 위한 장치 등록 프로그램이 있습니다. 비즈니스 계정의 경우 XenMobile Server 에서 Apple 배포 프로그램을 사용하여 장치를 등록하고 관리하려면 Apple 배포 프로그램에 등록해야 합니다. 이 프로그램은 iOS 및 macOS 장치를 위한 것입니다. [Apple 배포 프로그램을 통한 장치 배포](#)를 참조하십시오.

교육 계정의 경우 Apple School Manager 계정을 생성합니다. Apple School Manager 는 배포 프로그램과 볼륨 구매를 통합합니다. Apple School Manager 는 교육용 Apple 배포 프로그램의 한 유형입니다. [Apple 교육 기능과 통합](#)을 참조하십시오.

Apple 배포 프로그램을 사용하여 iOS 및 macOS 장치를 대량 등록할 수 있습니다. 이러한 장치는 Apple, 참여 Apple 공인 리셀러 또는 이동 통신 사업자에서 직접 구입할 수 있습니다. iOS 장치를 Apple 에서 직접 구매하든 구매하지 않든 Apple Configurator 를 사용하여 이러한 장치를 등록할 수 있습니다. [Apple 장치의 대량 등록](#)을 참조하십시오.

수동으로 iOS 장치 추가

테스트 목적 등으로 iOS 장치를 수동으로 추가하려면 다음 단계를 수행하십시오.

1. XenMobile Server 콘솔에서 관리 > 장치를 클릭합니다. 장치 페이지가 나타납니다.

Status	Mode	User name	Device platform	Operating system version
	MDM MAM	[Redacted]	Android	5.0.2
	MDM MAM	[Redacted]	iOS	8.4.1

2. 추가를 클릭합니다. 장치 추가페이지가 나타납니다.

3. 다음 설정을 구성합니다.

- 플랫폼 선택: **iOS** 를 클릭합니다.
- 일련 번호: 장치 일련 번호를 입력합니다.

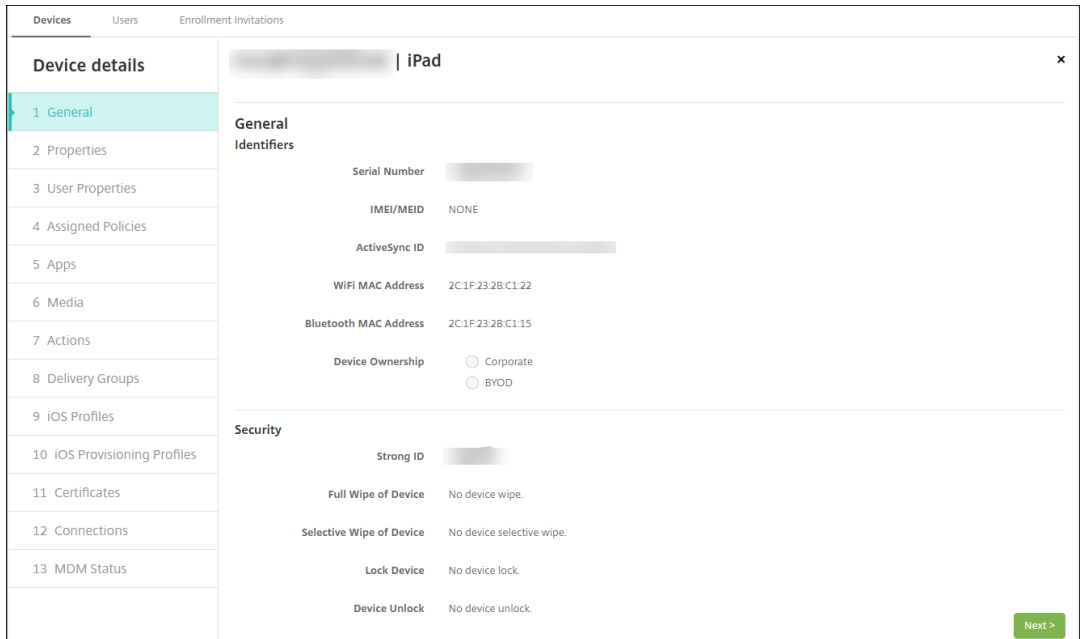
4. 추가를 클릭합니다. 장치 테이블이 나타나고 목록 맨 아래에 장치가 추가되어 있습니다. 장치 세부 정보를 보고 확인하려면: 추가한 장치를 선택한 다음 나타나는 메뉴에서 편집을 클릭합니다.

참고:

장치 옆에 있는 확인란을 선택하면 장치 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하면 목록의 오른쪽에 옵션 메뉴가 나타납니다.

- 구성된 LDAP
- 로컬 그룹 및 로컬 사용자를 사용 중인 경우:
 - 하나 이상의 로컬 그룹.

- 로컬 그룹에 할당된 로컬 사용자.
- 배달 그룹은 로컬 그룹과 연결됩니다.
- Active Directory 를 사용 중인 경우:
 - 배달 그룹은 Active Directory 그룹과 연결됩니다.



5. 일반 페이지에는 일련 번호 및 플랫폼 유형에 대한 기타 정보 같은 장치 식별자가 나열됩니다. 장치 소유권의 경우 회사 또는 **BYOD** 를 선택합니다.

일반 페이지에는 강력한 ID, 장치 잠금, 활성화 잠금 바이패스 및 플랫폼 유형에 대한 기타 정보 같은 장치 보안 속성도 나열됩니다. 장치 전체 초기화 필드에는 사용자 PIN 코드가 포함됩니다. 장치가 초기화된 후 사용자는 이 코드를 입력해야 합니다. 사용자가 코드를 잊은 경우 여기서 코드를 조회할 수 있습니다.

6. 속성 페이지에는 XenMobile Server 가 프로비전할 장치 속성이 나열됩니다. 이 목록에는 장치를 추가하는 데 사용된 프로비저닝 파일에 포함된 모든 장치 속성이 표시됩니다. 속성을 추가하려면 추가를 클릭한 다음 목록에서 속성을 선택합니다. 각 속성에 유효한 값에 대해서는 [장치 속성 이름 및 값 PDF](#) 를 참조하십시오.

속성을 추가하면 처음에는 속성을 추가한 범주 아래에 나타납니다. 다음을 클릭한 후 속성 페이지로 돌아가면 속성이 해당 목록에 나타납니다.

속성을 삭제하려면 목록 위에 마우스 포인터를 이동하고 오른쪽에 있는 **X** 를 클릭합니다. XenMobile Server 에서 항목이 즉시 삭제됩니다.

7. 나머지 장치 세부 정보 섹션에는 장치에 대한 요약 정보가 포함되어 있습니다.

- 사용자 속성: RBAC 역할, 그룹 구성원 자격, 볼륨 구매 계정 및 사용자 속성을 표시합니다. 이 페이지에서 볼륨 구매 계정을 사용 중지할 수 있습니다.
- 할당된 정책: 배포된 정책, 보류 중인 정책 및 실패한 정책의 수를 포함하여 할당된 정책의 수를 표시합니다. 각 정책에 대해 정책 이름, 유형 및 마지막 배포 정보를 제공합니다.

- **앱:** 마지막 인벤토리에 대한 설치된 앱 배포, 보류 중인 앱 배포 및 실패한 앱 배포의 수를 표시합니다. 앱 이름, 식별자, 유형 및 기타 정보를 제공합니다. iOS 및 macOS 인벤토리 키 (예: **HasUpdateAvailable**)에 대한 설명은 [모바일 기기 관리 \(MDM\) 프로토콜](#)을 참조하십시오.
- **미디어:** 마지막 인벤토리에 대해 배포된 미디어 배포, 보류 중인 미디어 배포 및 실패한 미디어 배포의 수를 표시합니다.
- **동작:** 배포된 동작, 보류 중인 동작 및 실패한 동작의 수를 표시합니다. 마지막 배포의 동작 이름 및 시간을 제공합니다.
- **배달 그룹:** 성공한 배달 그룹, 보류 중인 배달 그룹 및 실패한 배달 그룹의 수를 표시합니다. 각 배포에 대해 배달 그룹 이름 및 배포 시간을 제공합니다. 배달 그룹을 선택하여 상태, 동작 및 채널 또는 사용자를 비롯한 자세한 정보를 확인합니다.
- **iOS 프로파일:** 이름, 유형, 조직 및 설명을 비롯한 마지막 iOS 프로파일 인벤토리를 표시합니다.
- **iOS 프로비전 프로파일:** UUID, 만료 날짜 및 관리 상태와 같은 엔터프라이즈 배포 프로비전 프로파일 정보를 표시합니다.
- **인증서:** 유효하거나, 만료되거나, 해지된 인증서에 대해 유형, 공급자, 발급자, 일련 번호 및 만료 전까지 남은 날짜와 같은 정보를 표시합니다.
- **연결:** 첫 번째 연결 상태 및 마지막 연결 상태를 표시합니다. 각 연결에 대해 사용자 이름, 마지막 두 번째 (끝에서 두 번째) 인증 시간 및 마지막 인증 시간을 제공합니다.
- **MDM 상태:** MDM 상태, 마지막 푸시 시간 및 마지막 장치 회신 시간 같은 정보를 표시합니다.

iOS 장치 정책 구성

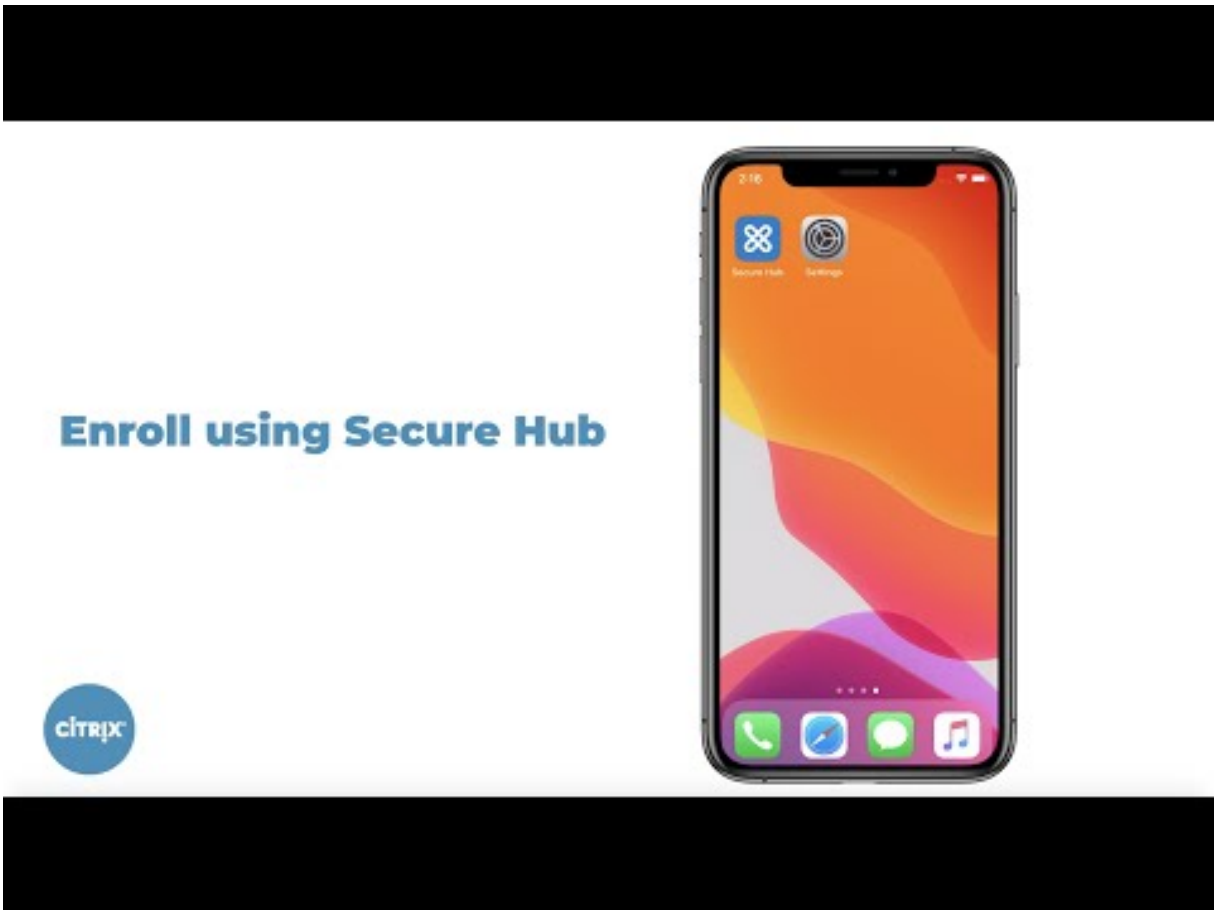
이러한 정책을 사용하여 XenMobile Server가 iOS를 실행하는 장치와 상호 작용하는 방식을 구성할 수 있습니다. 다음 표에는 iOS 장치에 사용할 수 있는 모든 장치 정책이 나열되어 있습니다.

AirPlay 미러링	AirPrint	APN
앱 액세스	앱 특성	앱 구성
앱 인벤토리	앱 잠금	앱 네트워크 사용
앱 제거	앱 알림	일정 (CalDAV)
셀룰러	연락처 (CardDAV)	OS 업데이트 제어
자격 증명	장치 이름	교육 구성
Exchange	글꼴	홈 화면 레이아웃
iOS 및 macOS 프로파일 가져오기	LDAP	위치
메일	관리되는 도메인	MDM 옵션
조직 정보	암호	개인 핫스팟

프로필 제거	프로비전 프로필	프로비전 프로필 제거
프록시	제한 사항	로밍
SCEP	공유 iPad - 최대 상주 사용자 수	공유 iPad - 암호 잠금 유예 기간
SSO 계정	저장소	구독 중인 일정
약관	VPN	배경 화면
웹 콘텐츠 필터	웹 클립	Wi-Fi

iOS 장치 등록

이 섹션에서는 사용자가 iOS 장치 (12.2 이상) 를 XenMobile Server 에 등록하는 방법을 보여 줍니다. iOS 등록에 대한 자세한 내용을 보려면 다음 비디오를 여십시오.



1. iOS 장치의 Apple Store 로 이동하여 Citrix Secure Hub 앱을 다운로드한 후 이 앱을 누릅니다.
2. 앱을 설치하라는 메시지가 표시되면 다음을 누른 후 설치를 누릅니다.

3. Secure Hub 가 설치된 후에 **Open(열기)** 을 누릅니다.
4. XenMobile Server 서버 이름, UPN(사용자 계정 이름) 또는 전자 메일 주소와 같은 회사 자격 증명을 입력합니다. 그리고 **Next(다음)** 를 클릭합니다.

The diagram illustrates the initial login process for Secure Hub. It shows two screens connected by a large blue arrow pointing from left to right.

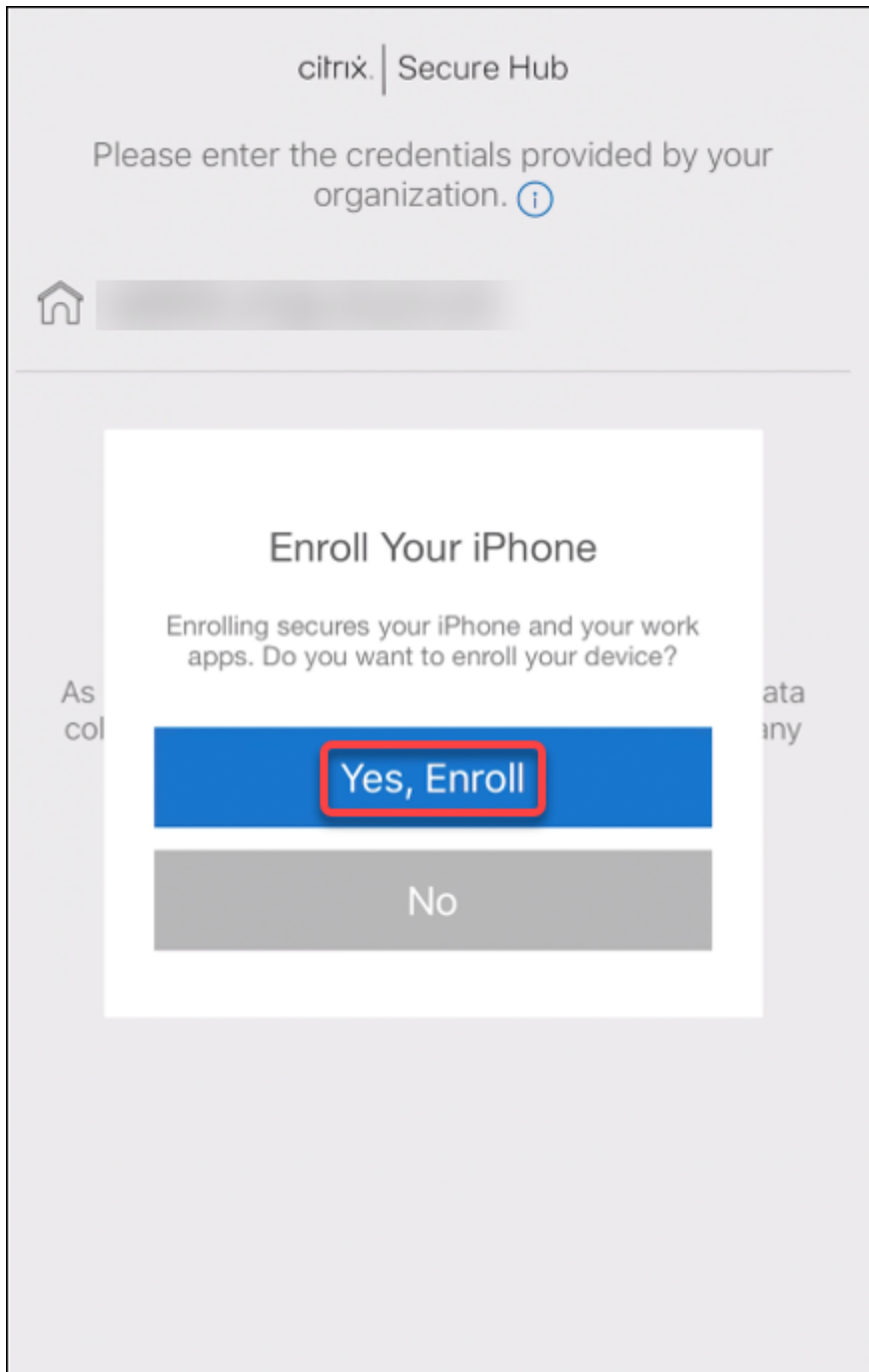
Left Screen (Initial Login):

- Header: citrix | Secure Hub
- Text: Please enter the credentials provided by your organization. ①
- Input field: Home icon | JPN, Email or Server
- Button: Next (large blue button)
- Link: Privacy Policy
- Footnote: As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

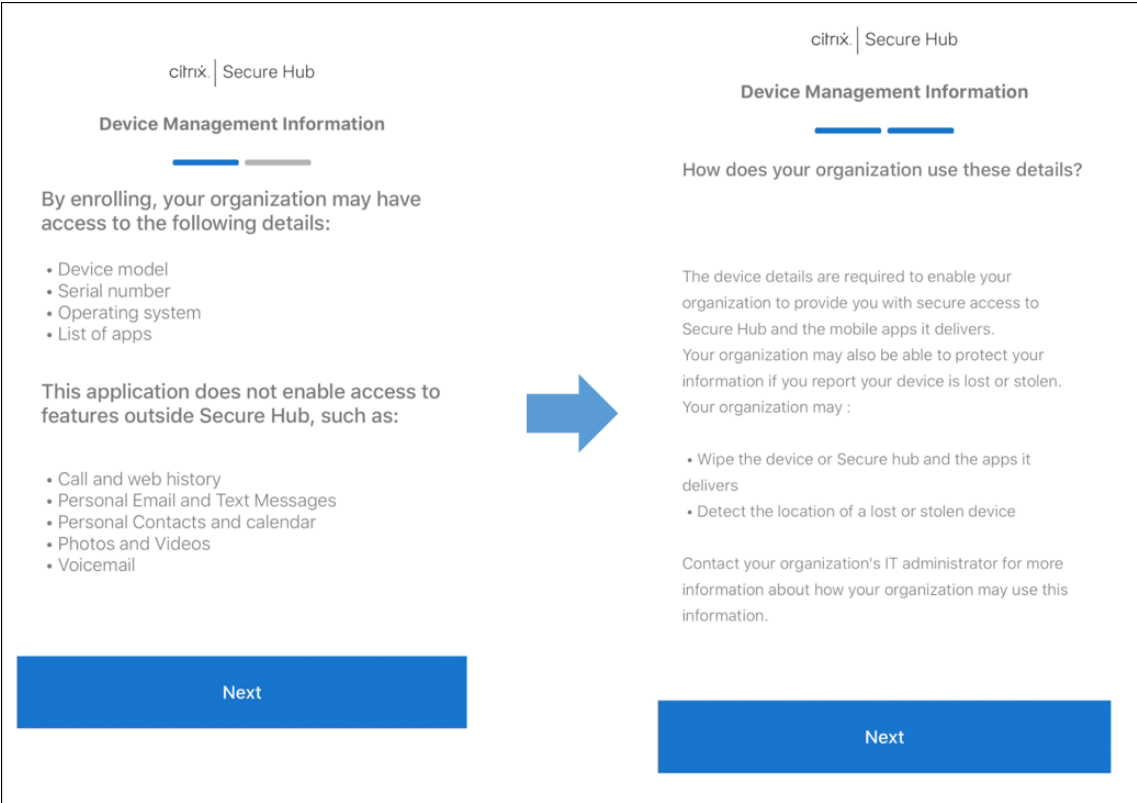
Right Screen (Credential Entry):

- Header: citrix | Secure Hub
- Text: Please enter the credentials provided by your organization.
- Input fields: Username (with person icon), Password (with lock icon)
- Buttons: Back (outlined blue button), Next (solid blue button)
- Link: Privacy Policy
- Footnote: As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

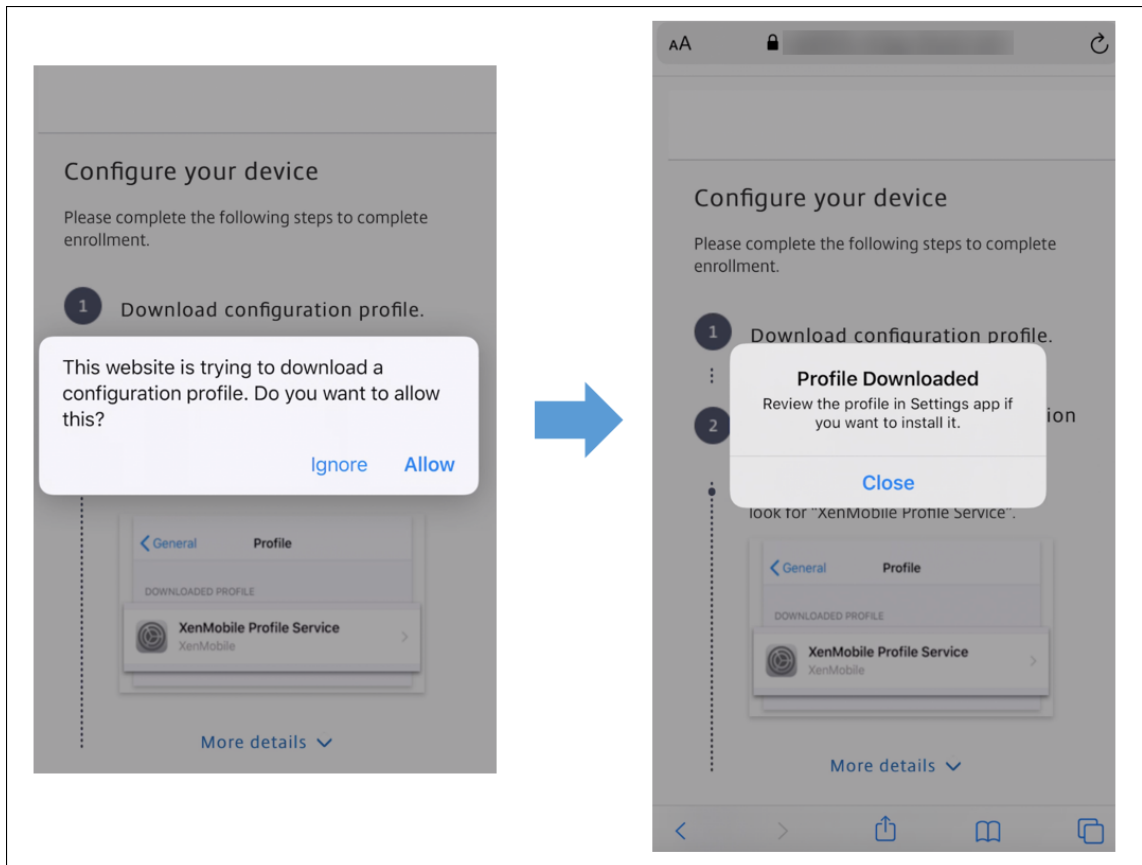
5. 예, 등록을 눌러 iOS 장치를 등록합니다.



6. XenMobile Server 가 수집하는 데이터 목록이 나타납니다. 다음을 클릭합니다. 조직에서 해당 데이터를 사용하는 방법에 대한 설명이 표시됩니다. 다음을 클릭합니다.

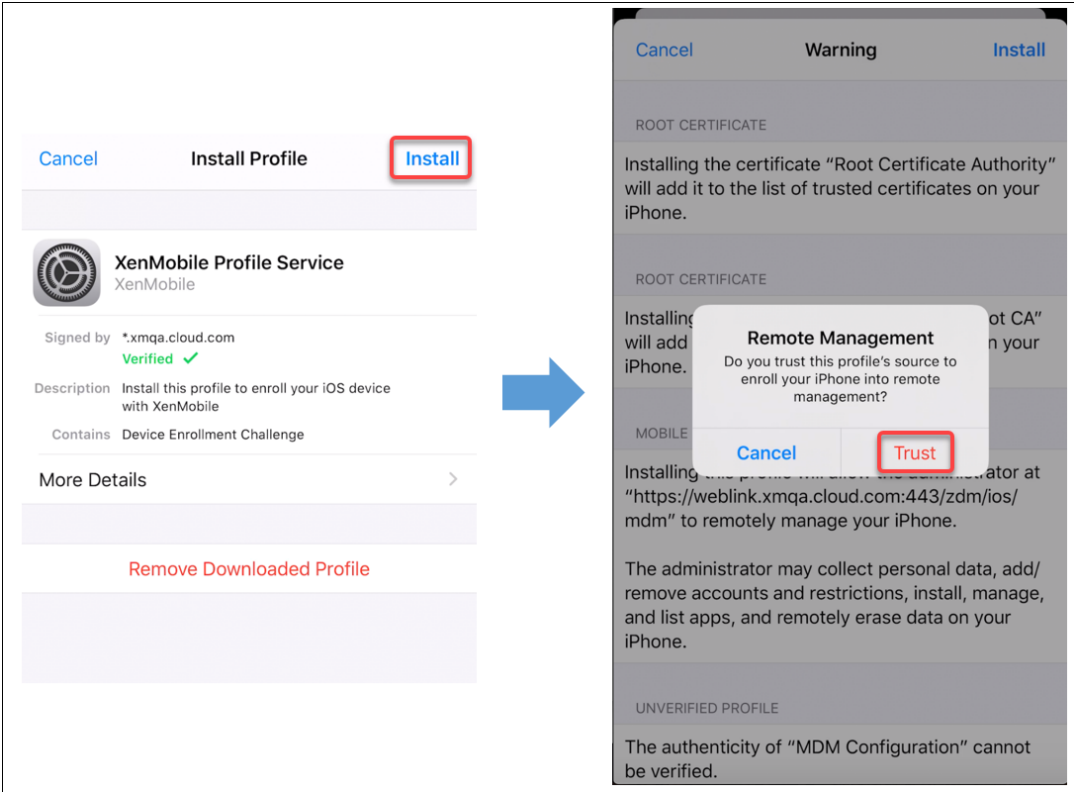


7. 자격 증명을 입력한 후 메시지가 표시되면 허용을 눌러 구성 프로필을 다운로드합니다. 구성 프로필을 다운로드한 후 닫기를 누릅니다.



8. 장치 설정에서 iOS 인증서를 설치하고 장치를 신뢰할 수 있는 목록에 추가합니다.

- 설정 > 일반 > 프로필 > **XenMobile** 프로필 서비스로 이동하고 설치를 눌러 프로필을 추가합니다.
- 알림 창에서 신뢰를 눌러 장치를 원격 관리에 등록합니다.



9. 등록이 성공하면 Secure Hub 를 엽니다. MDM+MAM 에 등록하는 경우: 자격 증명의 유효성이 확인된 후 메시지가 표시되면 Citrix PIN 을 만들고 확인합니다.
10. 워크플로가 완료되면 장치가 등록됩니다. 이제 App Store 에 액세스하여 iOS 장치에 설치할 수 있는 앱을 볼 수 있습니다.

보안 동작

iOS 는 다음과 같은 보안 동작을 지원합니다. 각 보안 동작에 대한 설명은 [보안 동작](#)을 참조하십시오.

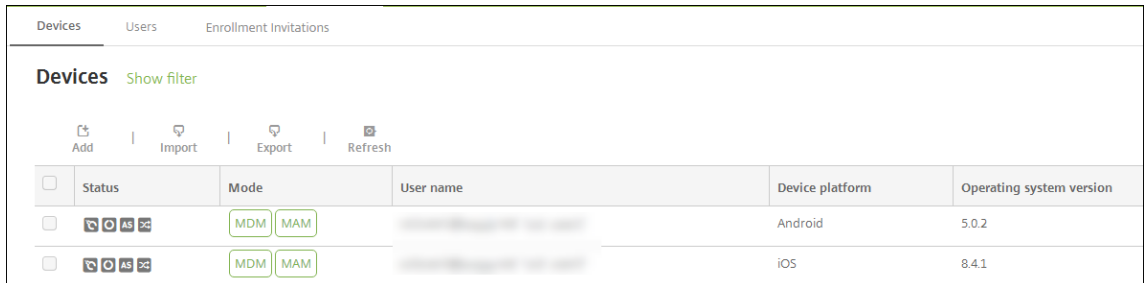
활성화 잠금 바이패스	앱 잠금	앱 초기화
ASM 활성화 잠금	인증서 갱신	제한 사항 지우기
분실 모드 활성화/비활성화	추적 활성화/비활성화	전체 초기화
찾기	잠금	벨 울림
AirPlay 미러링 요청/중지	다시 시작/종료	Revoke/Authorize(해지/권한 부여)
선택적 초기화	잠금 해제	

ios 장치 잠금

분실된 iOS 장치를 잠그고 장치 잠금 화면에 메시지와 전화 번호를 표시할 수 있습니다.

잠겨 있는 장치에 메시지와 전화 번호를 표시하려면 XenMobile Server 콘솔에서 **암호** 정책을 **true** 로 설정합니다. 또는 사용자가 수동으로 장치에서 암호를 사용하도록 설정할 수 있습니다.

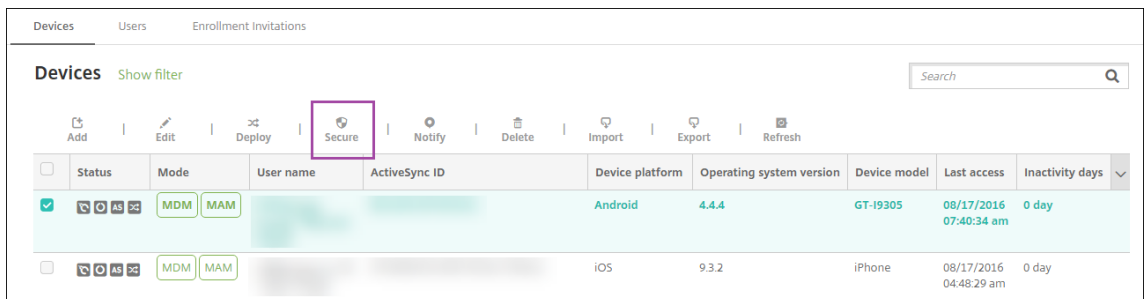
1. 관리 > 장치를 클릭합니다. 장치 페이지가 나타납니다.



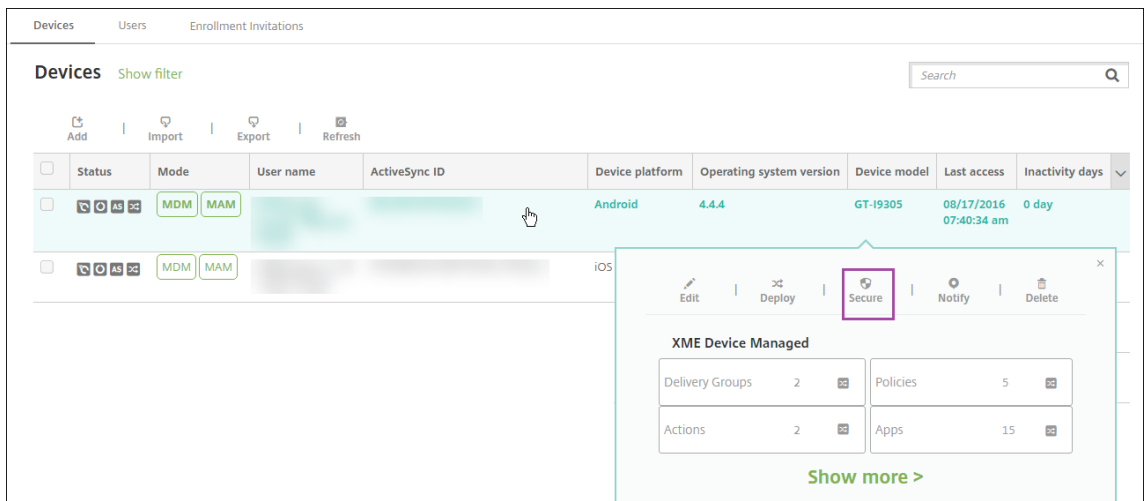
Devices					
	Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>		MDM MAM	[Redacted]	Android	5.0.2
<input type="checkbox"/>		MDM MAM	[Redacted]	iOS	8.4.1

2. 잠글 iOS 장치를 선택합니다.

장치 옆에 있는 확인란을 선택하여 장치 목록 위의 옵션 메뉴를 표시합니다. 목록에서 아무 위치를 클릭하여 목록 오른쪽의 옵션 메뉴를 표시합니다.



Devices									
	Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
<input checked="" type="checkbox"/>		MDM MAM	[Redacted]	[Redacted]	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
<input type="checkbox"/>		MDM MAM	[Redacted]	[Redacted]	iOS	9.3.2	iPhone	08/17/2016 04:48:29 am	0 day



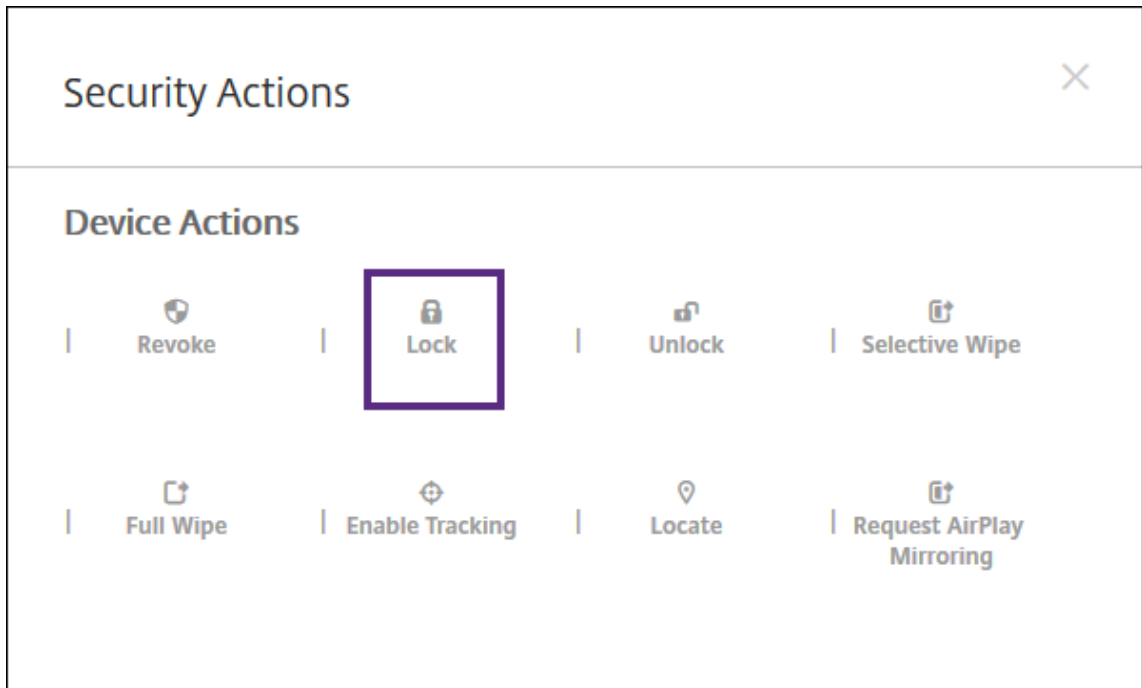
Devices									
	Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
<input checked="" type="checkbox"/>		MDM MAM	[Redacted]	[Redacted]	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
<input type="checkbox"/>		MDM MAM	[Redacted]	[Redacted]	iOS	9.3.2	iPhone	08/17/2016 04:48:29 am	0 day

XME Device Managed

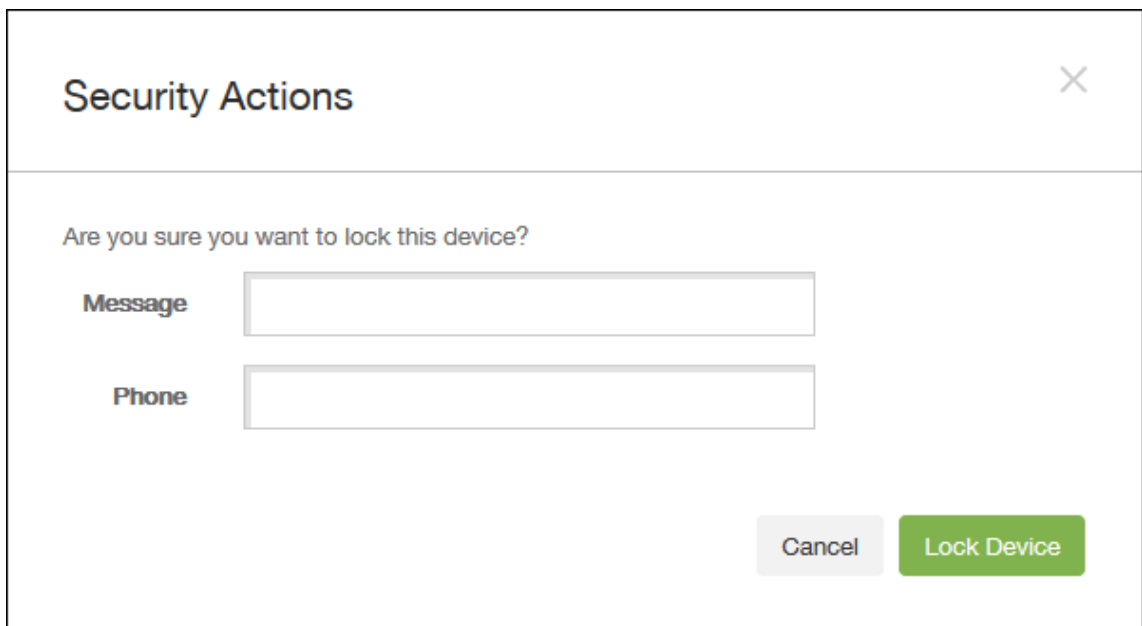
Delivery Groups	2	Policies	5
Actions	2	Apps	15

[Show more >](#)

3. 옵션 메뉴에서 보안을 클릭합니다. 보안 동작 대화 상자가 나타납니다.



4. 잠금을 클릭합니다. 보안 동작 확인 대화 상자가 표시됩니다.



5. 필요에 따라 장치 잠금 화면에 표시되는 메시지와 전화 번호를 입력합니다.

메시지 필드에 입력하는 내용에 “iPad 분실” 이라는 단어가 추가됩니다.

메시지 필드를 비워 두고 전화 번호를 입력할 경우 장치 잠금 화면에 “소유자에게 통화” 라는 메시지가 표시됩니다.

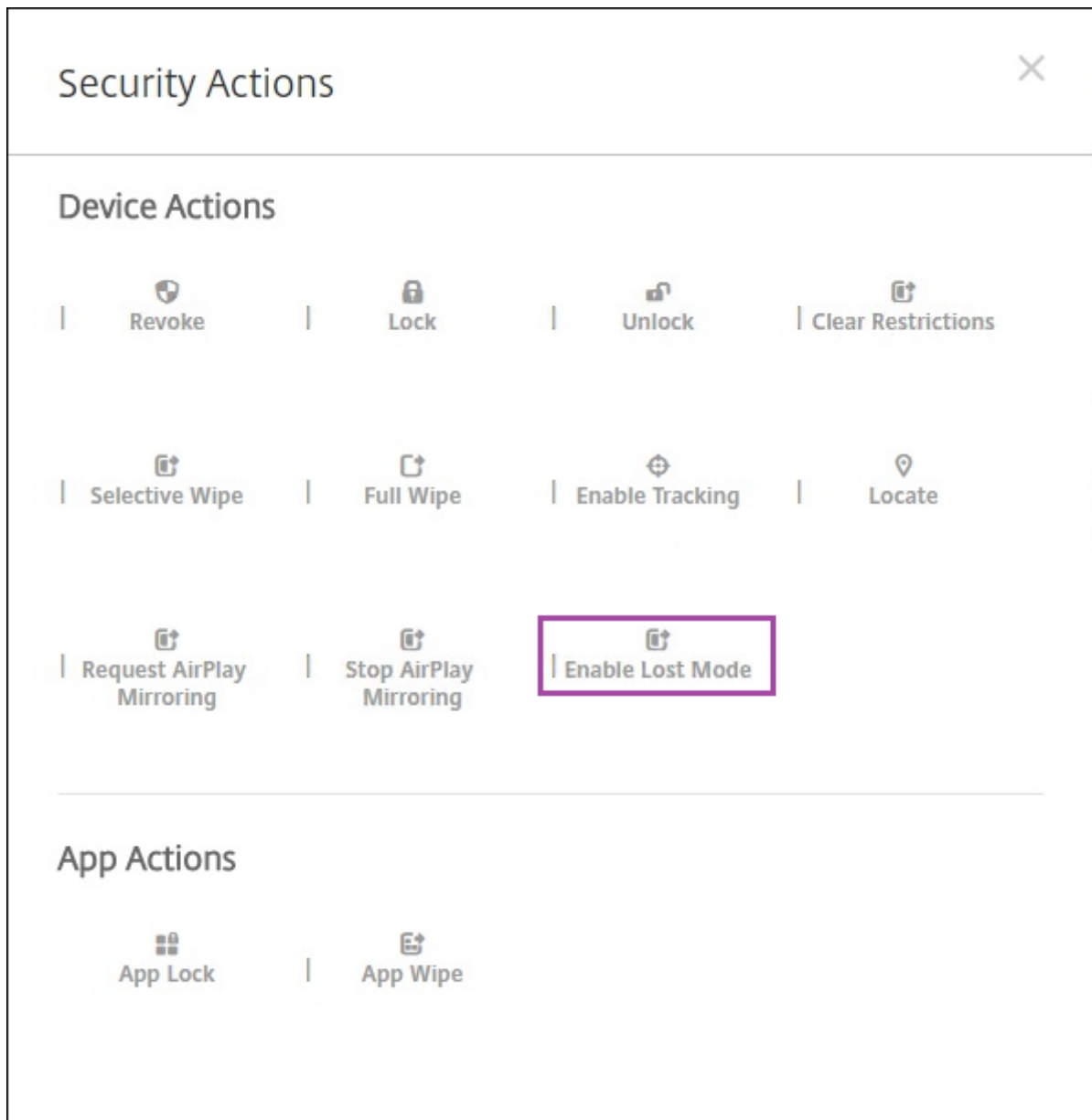
6. 장치 잠금을 클릭합니다.

iOS 장치를 분실 모드로 전환

XenMobile Server 분실 모드 장치 속성은 iOS 장치를 분실 모드로 전환합니다. Apple의 관리되는 분실 모드와 달리 XenMobile Server의 분실 모드에서는 다음 동작 중 하나를 수행하여 사용자가 나의 **iPhone/iPad** 찾기 설정을 구성하거나 Citrix Secure Hub의 위치 서비스를 사용하지 않아도 장치 위치를 찾을 수 있습니다.

XenMobile Server 분실 모드에서는 XenMobile Server만 장치 잠금을 해제할 수 있습니다. 이와 반대로 XenMobile Server 장치 잠금 기능을 사용하는 경우에는 사용자가 제공된 PIN 코드를 사용하여 장치를 직접 잠금 해제할 수 있습니다.

분실 모드를 사용하거나 사용하지 않으려면: 관리 > 장치로 이동하고 감독되는 iOS 장치를 선택한 후 보안을 클릭합니다. 분실 모드 활성화 또는 분실 모드 비활성화를 클릭합니다.



분실 모드 활성화를 클릭하고 장치가 분실 모드가 될 때 장치에 표시할 정보를 입력합니다.

Security Actions

Are you sure you want to enable the lost mode for this device?

Message

?

Phone number

?

Footnote

?

Cancel

Enable Lost Mode

다음 방법 중 하나를 사용하여 분실 모드 상태를 확인합니다.

- 보안 동작 창에서 단추가 분실 모드 비활성화인지 확인합니다.
- 관리 > 장치에서 일반 탭의 보안 아래에서 마지막 분실 모드 활성화 또는 분실 모드 비활성화 동작을 확인합니다.

Devices

Users

Enrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Actions

7 Delivery Groups

8 iOS Profiles

9 iOS Provisioning Profiles

10 Certificates

11 Connections

12 MDM Status

Device Shutdown

No device shutdown.

Device locate

No device locate .

Device Enable Tracking

No device enable tracking.

Device Disown

No device disown.

DEP Activation Lock

No DEP device activation lock.

Activation Lock Bypass

No device activation lock bypass.

Device Clear Restrictions

No Clear Restrictions.

Device App Wipe

No device App Wipe.

Device App Lock

No device App Lock.

Request AirPlay Mirroring

No request AirPlay mirroring.

Stop AirPlay Mirroring

No stop AirPlay mirroring.

Enable Lost Mode

No lost mode enabled.

Disable Lost Mode

No lost mode disabled.

Next >

Next >

- 관리 > 장치의 속성 탭에서 **MDM 분실 모드** 활성화 설정의 값이 올바른지 확인합니다.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div>1 General</div> <div>2 Properties</div> <div>3 User Properties</div> <div>4 Assigned Policies</div> <div>5 Apps</div> <div>6 Actions</div> <div>7 Delivery Groups</div> <div>8 iOS Profiles</div> <div>9 iOS Provisioning Profiles</div> <div>10 Certificates</div> <div>11 Connections</div> <div>12 MDM Status</div>		
Activation lock enabled		No
Hardware encryption capabilities		Block and file levels encryption
Internal storage encrypted		No
Jailbroken/Rooted		No
MDM lost mode enabled		No
Passcode compliant		Yes
Passcode compliant with configuration		Yes
Passcode present		No
Supervised		No
– Storage space		Add
Available storage space		10.92 GB
Total storage space		12.28 GB
– System information		Add
Active iTunes account		Yes
Cloud backup enabled		No
		Back Next >

iOS 장치에서 XenMobile Server 분실 모드를 사용하는 경우 XenMobile Server 콘솔이 다음과 같이 변경됩니다.

- 구성 > 동작에서 동작 목록에 장치 해지, 장치를 선택적으로 초기화 및 장치를 완전히 초기화 자동화 동작이 포함되지 않습니다.
- 관리 > 장치에서 보안 동작 목록에 해지 및 장치 선택적 초기화 동작이 더 이상 포함되지 않습니다. 필요한 경우 보안 동작을 사용하여 전체 초기화를 수행할 수 있습니다.

보안 동작 화면의 메시지에 무엇을 입력하든지 관계없이 끝에 “iPad 분실”이라는 단어가 추가됩니다.

메시지를 비워 두고 전화 번호를 입력할 경우 장치 잠금 화면에 “소유자에게 통화”라는 메시지가 표시됩니다.

iOS 활성화 잠금 바이패스

활성화 잠금은 분실되거나 도난당한 장치의 재활성화를 방지하는 내 iPhone/iPad 찾기 기능입니다. 활성화 잠금은 누군가가 내 iPhone/iPad 찾기를 끄고 장치를 지우거나 장치를 재활성화하여 사용하려고 할 경우 사용자의 Apple ID와 암호를 요구합니다. 조직이 소유한 장치의 경우 예를 들어 장치를 재설정하거나 재활당하기 위해 활성화 잠금을 바이패스해야 합니다.

활성화 잠금을 사용하도록 설정하려면 XenMobile Server MDM 옵션 장치 정책을 구성하고 배포합니다. 그러면 사용자의 Apple 자격 증명 없이도 XenMobile Server 콘솔에서 장치를 관리할 수 있습니다. 활성화 잠금의 Apple 자격 증명 요구 사항을 바이패스하려면 XenMobile Server 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행합니다.

예를 들어 사용자가 분실된 휴대폰을 반환하거나 전체 초기화 전후에 장치를 설정하는 경우 Apple App Store 계정 자격 증명을 묻는 메시지가 표시될 때 XenMobile Server 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행하여 이 단계를 바이패스할 수 있습니다.

활성화 잠금 바이패스를 위한 장치 요구 사항

- Apple Configurator 또는 Apple 배포 프로그램을 통해 감독됨
- iCloud 계정을 사용하여 구성됨
- 내 iPhone/iPad 찾기를 사용하도록 설정됨
- XenMobile Server 에서 등록됨
- 활성화 잠금을 사용하도록 설정된 MDM 옵션 장치 정책이 장치에 배포됨

장치의 전체 초기화를 실행하기 전에 활성화 잠금을 바이패스하려면:

1. 관리 > 장치에서 장치를 선택하고 보안을 클릭한 다음 활성화 잠금 바이패스를 클릭합니다.
2. 장치를 초기화합니다. 장치 설정 중에 활성화 잠금 화면이 표시되지 않습니다.

장치의 전체 초기화를 실행한 후에 활성화 잠금을 바이패스하려면:

1. 장치를 재설정하거나 초기화합니다. 장치 설정 중에 활성화 잠금 화면이 표시됩니다.
2. 관리 > 장치에서 장치를 선택하고 보안을 클릭한 다음 활성화 잠금 바이패스를 클릭합니다.
3. 장치에서 뒤로 단추를 누릅니다. 홈 화면이 나타납니다.

다음 사항에 유의하십시오.

- 사용자에게 내 iPhone/iPad 찾기를 끄지 말라고 알려 두십시오. 장치에서 전체 초기화를 수행하지 마십시오. 두 경우 모두 사용자에게 iCloud 계정 암호를 입력하라는 메시지가 표시됩니다. 계정 유효성 검사 후 모든 콘텐츠와 설정을 지운 다음 사용자에게 iPhone/iPad 활성화 화면이 표시되지 않습니다.
- 활성화 잠금 바이패스 코드가 생성되고 활성화 잠금을 사용하도록 설정한 장치의 경우 전체 초기화 후 iPhone/iPad 활성화 페이지를 바이패스할 수 없으면 XenMobile Server 에서 장치를 삭제할 필요가 없습니다. 관리자 또는 사용자가 Apple 지원 팀에 연락하여 직접 장치의 차단을 해제할 수 있습니다.
- 하드웨어 인벤토리 중에 XenMobile Server 는 장치에서 활성화 잠금 바이패스 코드를 쿼리합니다. 바이패스 코드를 사용할 수 있는 경우 장치가 해당 코드를 XenMobile Server 에 전송합니다. 그런 다음 장치에서 바이패스 코드를 제거하려면 XenMobile Server 콘솔에서 활성화 잠금 바이패스 보안 동작을 전송합니다. 이때 장치의 차단을 해제하려면 XenMobile Server 와 Apple 에 바이패스 코드가 있어야 합니다.
- 활성화 잠금 바이패스 보안 동작은 Apple 서비스의 이용 가용성에 따라 달라집니다. 이 동작이 작동하지 않는 경우 다음과 같이 장치의 차단을 해제할 수 있습니다. 장치에서 수동으로 iCloud 계정의 자격 증명을 입력합니다. 또는 사용자 이름 필드를 비워 두고 암호 필드에 바이패스 코드를 입력합니다. 바이패스 코드를 조회하려면 관리 > 장치로 이동하여 장치를 선택하고 편집, 속성을 차례로 클릭합니다. 활성화 잠금 바이패스 코드는 보안 정보 아래에 있습니다.

macOS

March 15, 2024

XenMobile 에서 macOS 장치를 관리하려면 Apple 의 APNs(Apple 푸시 알림 서비스) 인증서를 설정합니다. 자세한 내용은 [APN 인증서](#)를 참조하십시오.

XenMobile 이 macOS 장치를 MDM 으로 등록합니다. XenMobile 은 MDM 에서 macOS 장치에 대해 다음과 같은 등록 유형을 지원합니다.

- 도메인
- 도메인과 일회용 암호
- 초대 URL 과 일회용 암호

macOS 15 의 신뢰할 수 있는 인증서 요구 사항:

Apple 은 TLS 서버 인증서에 대한 새로운 요구 사항을 도입했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는 지 확인하십시오. Apple 게시물 <https://support.apple.com/en-us/HT210176>를 참조하십시오. 인증서 관리에 대한 도움말은 [XenMobile](#) 에서 [인증서 업로드](#)를 참조하십시오.

macOS 장치 관리를 시작하는 일반적인 워크플로는 다음과 같습니다.

1. macOS 장치 정책 관리.
2. macOS 장치 등록.
3. 장치 및 앱 보안 작업을 설정합니다. 보안 동작을 참조하십시오.

지원되는 운영 체제에 대해서는 [지원되는 장치 운영 체제](#)를 참조하십시오.

열린 상태로 유지되어야 하는 **Apple** 호스트 이름

일부 Apple 호스트 이름은 iOS, macOS 및 Apple App Store 의 올바른 작동을 보장하기 위해 열린 상태로 유지되어야 합니다. 이러한 호스트 이름을 차단하면 iOS, iOS 앱, MDM 작업, 장치 및 앱 등록 등의 설치, 업데이트 및 적절한 작동에 영향을 줄 수 있습니다. 자세한 내용은 <https://support.apple.com/en-us/HT201999> 항목을 참조하십시오.

지원되는 등록 방법

다음 표에는 XenMobile 에서 macOS 장치에 지원하는 등록 방법이 나와 있습니다.

방법	지원됨
Apple 배포 프로그램	예
Apple School Manager	예
Apple Configurator	아니요
수동 등록	예
등록 초대	예

Apple에는 비즈니스 및 교육 계정을 위한 장치 등록 프로그램이 있습니다. 비즈니스 계정의 경우 XenMobile에서 Apple 배포 프로그램을 사용하여 장치를 등록하고 관리하려면 Apple 배포 프로그램에 등록해야 합니다. 이 프로그램은 iOS 및 macOS 장치를 위한 것입니다. [Apple 배포 프로그램을 통한 장치 배포](#)를 참조하십시오.

교육 계정의 경우 Apple School Manager 계정을 생성합니다. Apple School Manager는 배포 프로그램과 볼륨 구매를 통합합니다. Apple School Manager는 교육용 Apple 배포 프로그램의 한 유형입니다. [Apple 교육 기능과 통합](#)을 참조하십시오.

Apple 배포 프로그램을 사용하여 iOS 및 macOS 장치를 대량 등록할 수 있습니다. 이러한 장치는 Apple, 참여 Apple 공인 리셀러 또는 이동 통신 사업자에서 직접 구입할 수 있습니다.

macOS 장치 정책 관리

이러한 정책을 사용하여 XenMobile이 macOS를 실행하는 장치와 상호 작용하는 방식을 구성할 수 있습니다. 다음 표에는 macOS 장치에 사용할 수 있는 모든 장치 정책이 나열되어 있습니다.

AirPlay 미러링	앱 인벤토리	일정 (CalDAV)
연락처 (CardDAV)	OS 업데이트 제어	자격 증명
장치 이름	Exchange	FileVault
방화벽	글꼴	iOS 및 macOS X 프로필 가져오기
LDAP	메일	암호
프로필 제거	제한 사항	SCEP
VPN	웹 클립	Wi-Fi

macOS 장치 등록

XenMobile에서는 macOS를 실행하는 장치를 등록하는 두 가지 방법을 제공합니다. 두 방법 모두 macOS 사용자가 장치에서 직접 온라인으로 등록할 수 있습니다.

- **사용자에게 등록 초대 보내기:** 이 등록 방법을 이용하면 macOS 장치에 대해 다음 등록 모드를 설정할 수 있습니다.
 - 사용자 이름 + 암호
 - 사용자 이름 + PIN
 - 2 단계 인증

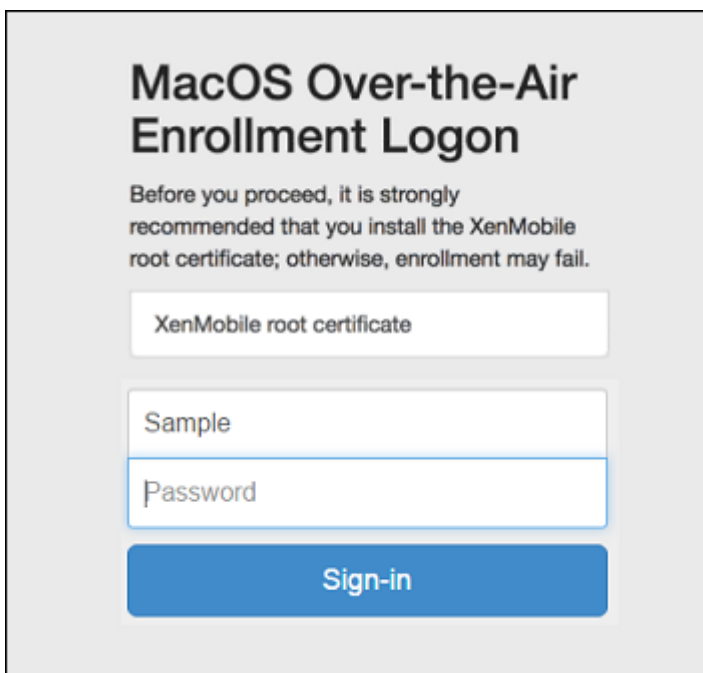
사용자가 등록 초대의 지침을 따르면 사용자 이름이 입력된 로그인 화면이 표시됩니다.

- **사용자에게 등록 링크 보내기:** macOS 장치를 등록하는 이 방법은 사용자에게 등록 링크를 보냅니다. 사용자는 이 링크를 Safari 또는 Chrome 브라우저에서 열 수 있습니다. 그런 다음 사용자 이름과 암호를 제공하여 등록합니다.

서버 속성인 **Enable macOS OTAE** 를 **false** 로 설정하여 macOS 장치에 대한 등록 링크를 사용하지 못하도록 할 수 있습니다. 이렇게 하면 macOS 사용자가 등록 초대만 사용하여 등록할 수 있습니다.

macOS 사용자에게 등록 초대 보내기

1. macOS 사용자 등록을 위한 초대를 추가합니다. [등록 초대 만들기](#)를 참조하십시오.
2. 사용자가 초대를 수신하고 링크를 클릭하면 다음 화면이 Safari 브라우저에 표시됩니다. XenMobile 이 사용자 이름을 채웁니다. 등록 보안 모드를 **2** 단계로 선택한 경우 다른 필드가 나타납니다.

The image shows a login screen for macOS Over-the-Air Enrollment. At the top, it says "MacOS Over-the-Air Enrollment Logon". Below that, a message states: "Before you proceed, it is strongly recommended that you install the XenMobile root certificate; otherwise, enrollment may fail." There are three input fields: "XenMobile root certificate", "Sample", and "Password". Below the input fields is a blue "Sign-in" button.

3. 사용자는 필요에 따라 인증서를 설치합니다. 사용자에게 인증서를 설치할 것인지 묻는 메시지가 표시되는지 여부는 macOS에 대해 공개적으로 신뢰할 수 있는 SSL 인증서와 공개적으로 신뢰할 수 있는 디지털 서명 인증서를 구성했는지 여부에 따라 달라집니다. 인증서에 대한 자세한 내용은 [인증서 및 인증](#)을 참조하십시오.
4. 사용자가 요청된 자격 증명을 제공합니다.

Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하듯이 XenMobile로 macOS 장치를 관리할 수 있습니다.

macOS 사용자에게 설치 링크 보내기

1. Safari 또는 Chrome 브라우저에서 열 수 있는 등록 링크 (<https://serverFQDN:8443/instanceName/macos/otae>)를 사용자에게 보냅니다.

- **serverFQDN**은 XenMobile을 실행하는 서버의 FQDN(정규화된 도메인 이름)입니다.

- 기본 보안 포트는 포트 **8443** 입니다. 다른 포트를 구성한 경우 8443 대신 해당 포트를 사용하십시오.
- 주로 **zdm**으로 표시되는 **instanceName** 은 서버 설치 중에 지정된 이름입니다.

설치 링크를 전송하는 방법에 대한 자세한 내용은 [등록 초대 보내기](#)를 참조하십시오.

2. 사용자는 필요에 따라 인증서를 설치합니다. iOS 와 macOS 에 대해 공개적으로 신뢰할 수 있는 SSL 인증서 및 디지털 서명 인증서를 구성한 경우 사용자에게 인증서를 설치하라는 메시지가 표시됩니다. 인증서에 대한 자세한 내용은 [인증서 및 인증](#)을 참조하십시오.
3. 사용자가 자신의 Mac 에 로그인합니다.

Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하듯이 XenMobile 로 macOS 장치를 관리할 수 있습니다.

보안 동작

macOS 는 다음과 같은 보안 동작을 지원합니다. 각 보안 동작에 대한 설명은 [보안 동작](#)을 참조하십시오.

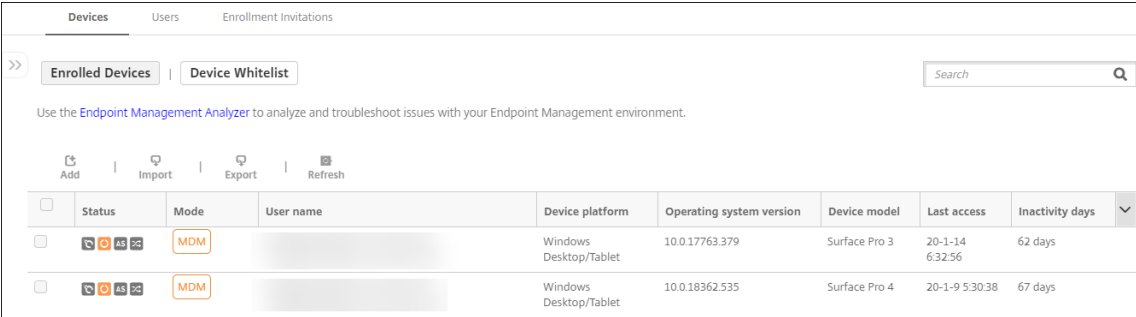
해지	잠금	선택적 초기화
전체 초기화	인증서 갱신	

macOS 장치 잠금

분실한 macOS 장치를 원격으로 잠글 수 있습니다. XenMobile 이 장치를 잠급니다. 그런 다음 PIN 코드를 생성하여 장치에 이 코드를 설정합니다. 장치에 액세스하려면 사용자는 PIN 코드를 입력해야 합니다. 잠금을 제거하려면 XenMobile 콘솔에서 잠금 취소를 사용합니다.

[암호](#) 장치 정책을 사용하여 PIN 코드로 연결된 추가 설정을 구성할 수 있습니다. 자세한 내용은 [macOS 설정](#)을 참조하십시오.

1. 관리 > 장치를 클릭합니다. 장치 페이지가 나타납니다.



2. 잠글 macOS 장치를 선택합니다.

장치 옆에 있는 확인란을 선택하여 장치 목록 위의 옵션 메뉴를 표시합니다. 목록에 나열된 항목 중 아무 위치나 클릭하면 목록 오른쪽에 옵션 메뉴를 표시할 수도 있습니다.

Use the [Endpoint Management Analyzer](#) to analyze and troubleshoot issues with your Endpoint Management environment.

[Add](#) | [Edit](#) | **Secure** | [Notify](#) | [Delete](#) | [Import](#) | [Export](#) | [Refresh](#)

	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.17763.379	Surface Pro 3	20-1-14 6:32:56	62 days
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.18362.535	Surface Pro 4	20-1-9 5:30:38	67 days

Use the [Endpoint Management Analyzer](#) to analyze and troubleshoot issues with your Endpoint Management environment.

[Add](#) | [Import](#) | [Export](#) | [Refresh](#)

	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.17763.379	Surface Pro 3	20-1-14 6:32:56	62 days
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.18362.535	Surface Pro 4	20-1-9 5:30:38	67 days
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.17134.1365	HVM domU	20-3-16 15:38:19	0 day
<input type="checkbox"/>		MDM		Android	10	SM-G970F	20-2-11 19:36:49	34 days
<input type="checkbox"/>		MDM		macOS	10.12.3	MacBook Air	20-2-11 20:15:18	33 days
<input type="checkbox"/>		MDM		Android				
<input type="checkbox"/>		WEM		Windows Desktop/Tablet				
<input type="checkbox"/>		MDM WEM		Windows Desktop/Tablet				

Showing 1 - 8 of 8 items Items per page: 10

[Edit](#) | **Secure** | [Notify](#) | [Delete](#)

Device Unmanaged

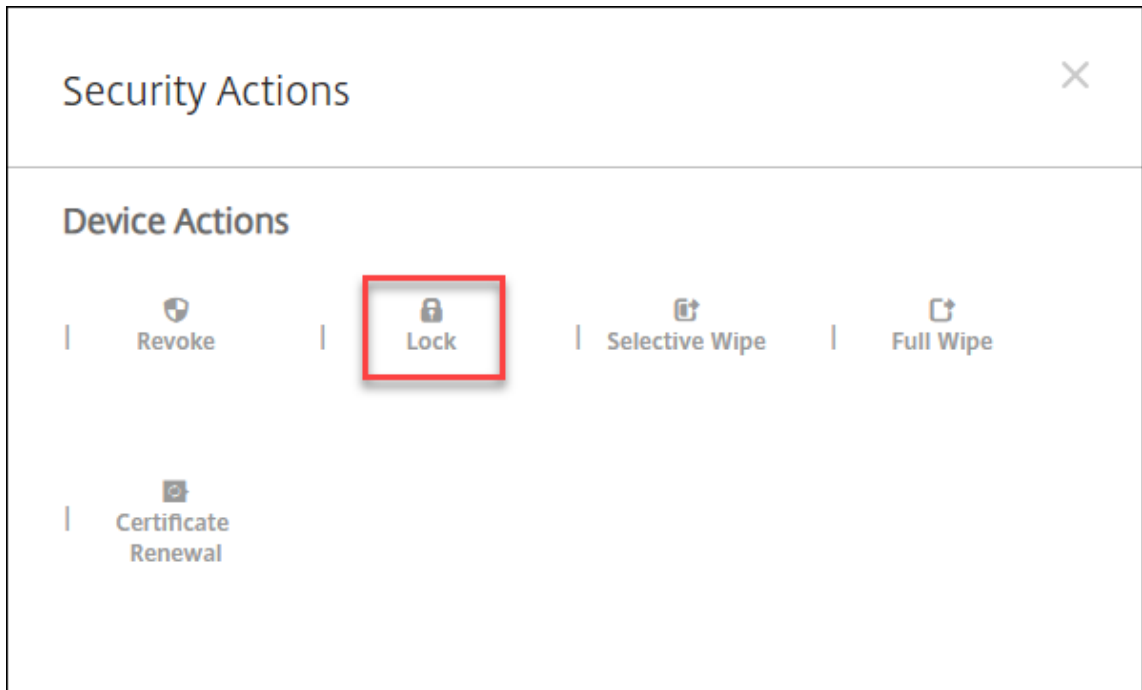
Delivery Groups 0 Policies 0

Actions 0 Apps 0

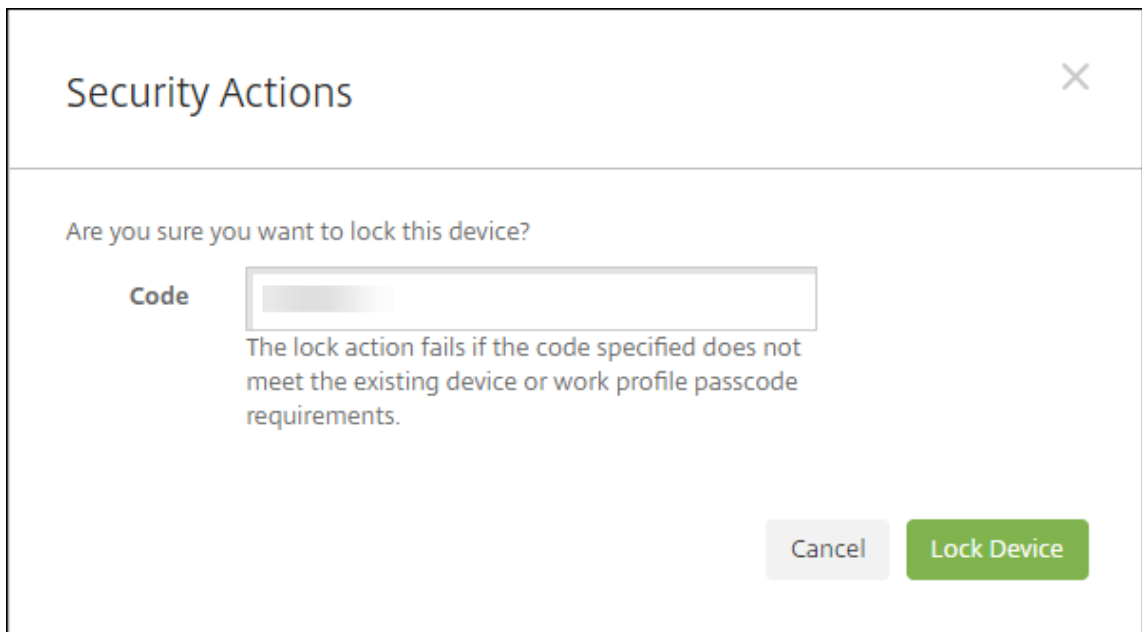
Media 0

[Show more >](#)

3. 옵션 메뉴에서 보안을 클릭합니다. 보안 동작 대화 상자가 나타납니다.



4. 잠금을 클릭합니다. 보안 동작 확인 대화 상자가 표시됩니다.



5. 장치 잠금을 클릭합니다.

중요:

XenMobile 이 생성한 코드를 사용하는 대신 암호를 지정할 수도 있습니다. 지정한 코드가 장치 또는 기존 작업 프로필의 코드 요구 사항을 충족하지 않으면 잠금 동작이 실패합니다.

Apple 장치의 대량 등록

January 5, 2022

XenMobile에서는 두 가지 방법을 사용하여 많은 수의 iOS, iPadOS 및 macOS 장치를 등록할 수 있습니다.

- Apple 배포 프로그램을 사용하여 Apple, 참여 Apple 공인 리셀러 또는 이동 통신 사업자로부터 직접 구입한 iOS, iPadOS 및 macOS 장치를 등록합니다. 이러한 지원에는 공유 iPad도 포함됩니다. XenMobile은 Apple Business Manager(ABM)용 Apple 배포 프로그램과 교육용 Apple School Manager(ASM)를 지원합니다. 이 문서에서는 여러 장치를 ABM 계정과 통합하는 방법에 대해 설명합니다. ABM에 등록하고 ABM 계정을 XenMobile과 연결하는 방법에 대한 자세한 내용은 [Apple 배포 프로그램을 통한 장치 배포](#)를 참조하십시오. Apple School Manager 계정에 대한 자세한 내용은 [Apple 교육 기능과 통합](#)을 참조하십시오.

macOS 장치를 등록하려면 XenMobile에서 해당 장치가 macOS 10.10 이상을 실행해야 합니다.

- Apple Configurator 2를 사용하여 Apple에서 직접 구입했는지 여부와 관계없이 iOS 장치를 등록할 수도 있습니다.

ABM 사용 시:

- 장치를 터치하거나 준비할 필요가 없습니다. 대신, ABM을 통해 장치 일련 번호 또는 구매 주문 번호를 제출하여 장치를 구성하고 등록할 수 있습니다.
- XenMobile에 장치가 등록된 후에는 장치를 사용자에게 제공하여 바로 사용하도록 할 수 있습니다. ABM을 사용하여 장치를 설정하면 장치를 처음 시작할 때 완료해야 하는 설정 도우미의 몇몇 단계를 제거할 수 있습니다.
- ABM 설정에 대한 자세한 정보는 [Apple Business Manager](#)의 설명서를 참고하십시오.

Apple Configurator 2를 사용하는 경우:

- iOS 장치를 macOS 10.7.2 이상을 실행하는 Apple 컴퓨터와 Apple Configurator 2 앱에 연결합니다. Apple Configurator 2를 통해 iOS 장치를 준비하고 정책을 구성할 수 있습니다.
- 필요한 정책으로 장치를 프로비전한 후 장치에서 처음으로 XenMobile에 연결하면 XenMobile의 정책이 장치에 수신됩니다. 그런 다음 장치 관리를 시작할 수 있습니다.
- Apple Configurator 사용에 대한 자세한 내용은 [Apple Configurator 도움말](#)을 참조하십시오.

사전 요구 사항

XenMobile과 Apple 간의 연결에 필요한 포트를 엽니다. 자세한 내용은 [포트 요구 사항](#)을 참조하십시오.

XenMobile와 Apple Business Manager 계정 통합

ABM 계정을 XenMobile로 설정하지 않은 경우 [Apple 배포 프로그램을 통한 장치 배포](#)의 다음 단계를 완료하십시오.

- Apple Business Manager에 등록합니다.
- Apple Business Manager 계정을 XenMobile과 연결합니다.

- 배포 프로그램 지원 장치를 주문합니다.
- 배포 프로그램 지원 장치를 관리합니다.

일괄 등록을 위한 기본 서버 설정

iOS, iPadOS, macOS 장치의 대량 주문을 MDM 서버에 할당하기 위해 XenMobile 을 기본 서버로 설정할 수 있습니다.

1. 관리자 또는 장치 등록 관리자 계정을 사용하여 [Apple Business Manager](#)에 로그인합니다.
2. 사이드바에서 설정 > 장치 관리 설정을 클릭합니다.
3. 기존 MDM 서버를 선택합니다. 기본 장치 할당에서 변경을 클릭합니다. 각 장치 유형에 대해 기본 XenMobile Server 를 선택합니다. 완료를 클릭합니다.

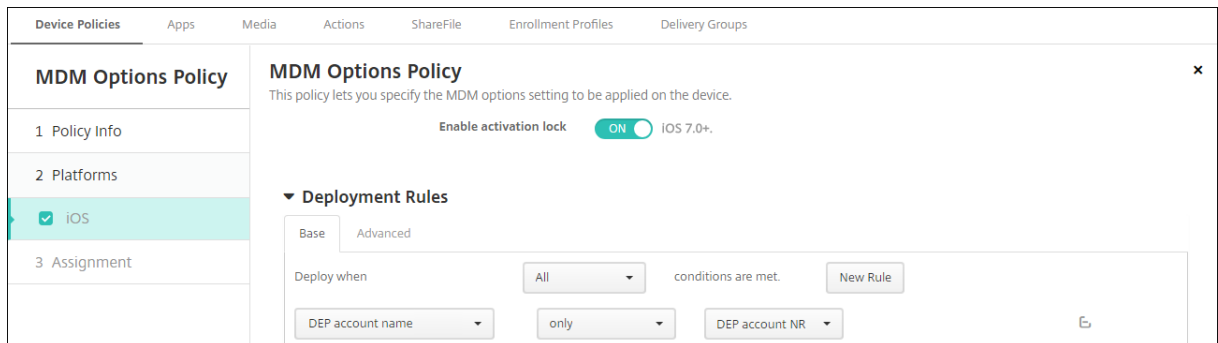
ABM 계정에 대한 장치 정책 및 앱의 배포 규칙 구성

구성 > 장치 정책 및 구성 > 앱 아래의 배포 규칙 섹션을 사용하여 서로 다른 장치 정책 및 앱에 ABM 계정을 연결할 수 있습니다. 다음과 같은 정책 또는 앱을 지정할 수 있습니다.

- 특정 ABM 계정에만 배포합니다.
- 선택한 계정을 제외한 모든 ABM 계정에 배포합니다.

ABM 계정 목록에 상태가 사용 또는 사용 안 함 상태인 계정만 포함됩니다. 사용되지 않는 ABM 계정에는 ABM 장치가 속하지 않습니다. 따라서 XenMobile 에서는 해당 장치에 앱 또는 정책을 배포하지 않습니다.

다음 예에서 장치 정책은 ABM 계정 이름이 “ABM Account NR” 인 장치에만 배포됩니다.



Apple 배포 프로그램 지원 장치 등록 시 사용자 환경

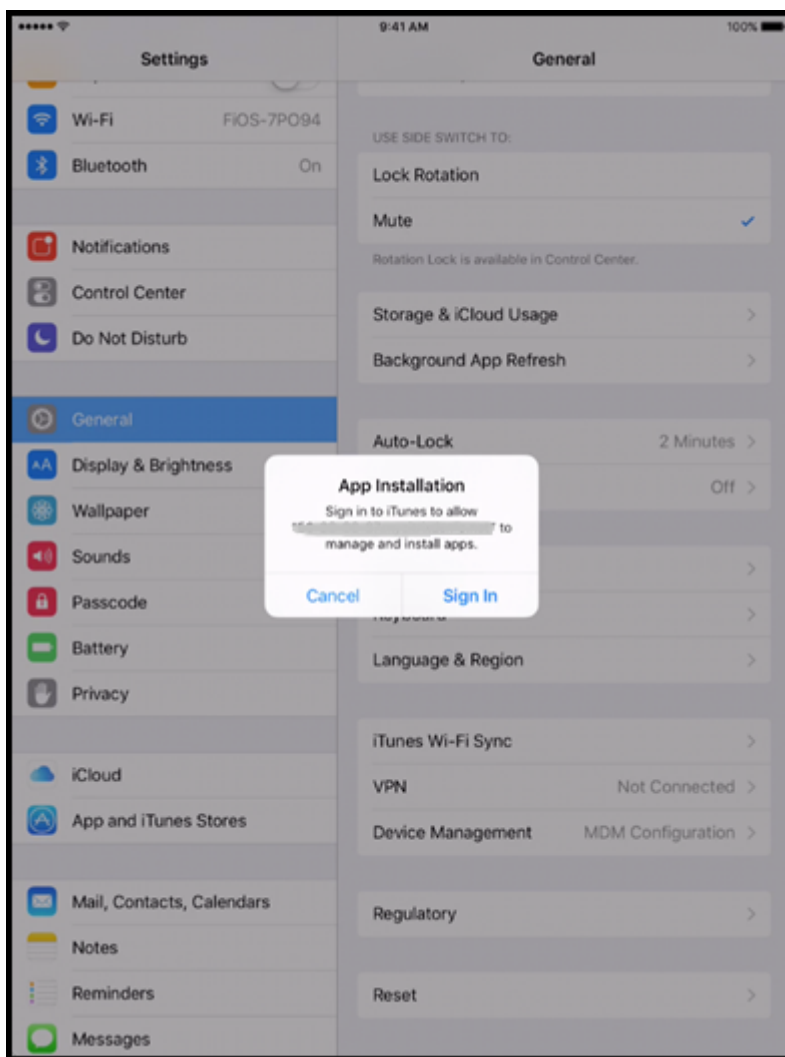
Apple 배포 프로그램 지원 장치를 등록할 때의 사용자 환경은 다음과 같습니다.

1. 사용자가 Apple 배포 프로그램 지원 장치를 시작합니다.
2. XenMobile 은 XenMobile 콘솔에서 구성한 Apple 배포 프로그램 구성을 Apple 배포 프로그램 지원 장치에 제공합니다.

3. 사용자가 장치에서 초기 설정을 구성합니다.
4. 장치에서 XenMobile 장치 등록 프로세스가 자동으로 시작됩니다.
5. 사용자가 장치에서 다른 초기 설정을 계속 구성합니다.
6. 홈 화면에 Citrix Secure Hub 를 다운로드할 수 있도록 Apple App Store 에 로그인하라는 메시지가 나타날 수 있습니다.

참고:

장치 기반 볼륨 구매 앱 할당을 사용하여 Secure Hub 앱을 배포하도록 XenMobile 을 구성할 경우 이 단계는 선택 사항입니다. 이 경우 Apple App Store 계정을 만들거나 기존 계정을 사용할 필요가 없습니다.



7. Secure Hub 를 열고 자격 증명을 입력합니다. 정책에 의해 요구되는 경우 Citrix PIN 을 생성하고 확인하라는 메시지가 표시될 수 있습니다.

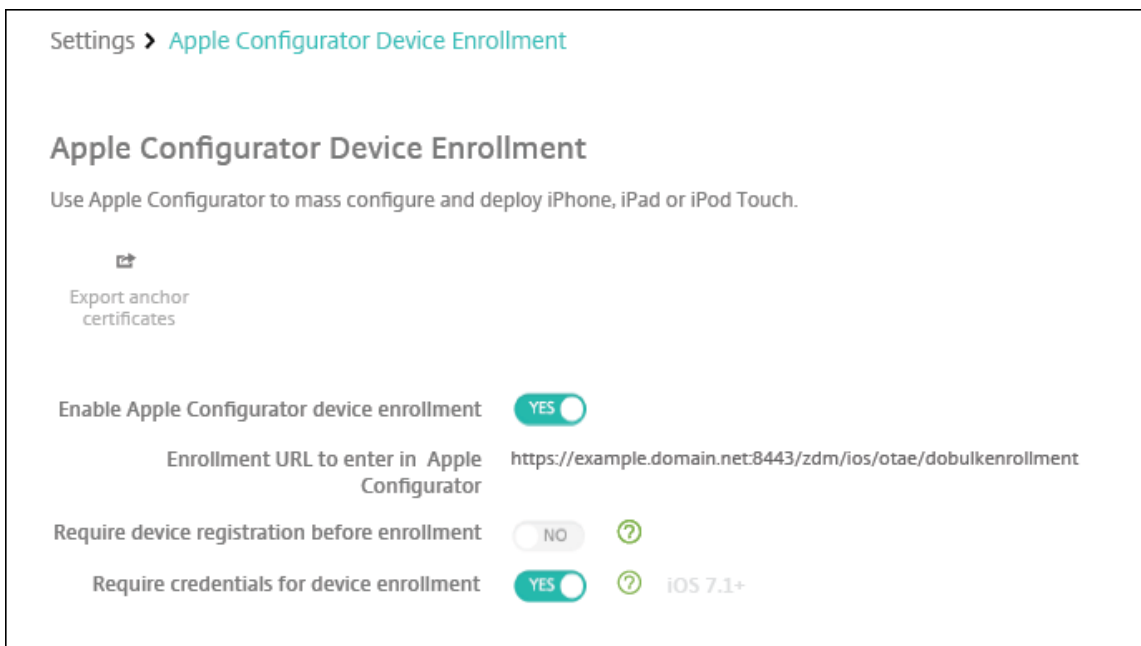
XenMobile 에서 나머지 필수 앱을 장치에 배포합니다.

Apple Configurator 2 설정 구성

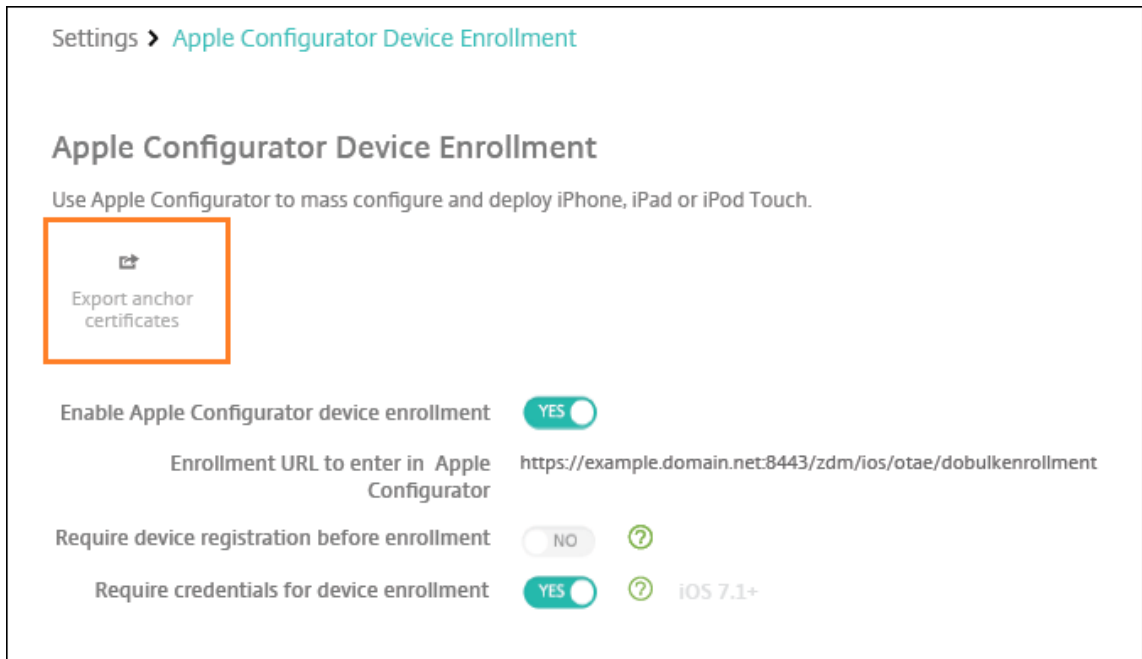
Apple Business Manager 대신 Apple Configurator 2 를 사용하여 iPhone 및 iPad 장치를 일괄 구성하고 배포할 수 있습니다.

1 단계: XenMobile 에서 설정 구성

1. XenMobile 콘솔에서 설정 > **Apple Configurator** 장치 등록으로 이동합니다.



2. **Apple Configurator** 장치 등록 허용을 예로 설정합니다.
3. **Apple Configurator** 에 입력할 등록 **URL** 은 읽기 전용 필드입니다. 이 설정은 Apple 과 통신하는 XenMobile Server 의 URL 을 제공합니다. Apple Configurator 2 에서 설정을 구성할 때 이 URL 을 복사하여 붙여넣습니다. 등록 URL 은 XenMobile Server 의 FQDN(정규화된 도메인 이름)(예: `mdm.server.url.com`) 또는 IP 주소입니다.
4. 알 수 없는 장치의 등록을 방지하려면 등록 전에 장치 등록 필요를 예로 설정합니다. 참고: 이 설정이 예인 경우 등록 전에 구성된 장치를 XenMobile 의 관리 > 장치에 수동으로 추가하거나 CSV 파일을 통해 추가해야 합니다.
5. iOS 장치 사용자가 등록할 때 자격 증명을 입력하도록 하려면 장치 등록에 자격 증명 필요를 예로 설정합니다. 기본값은 등록에 자격 증명을 요구하지 않는 것입니다.
6. 참고: XenMobile 서버에서 신뢰할 수 있는 SSL 인증서를 사용하는 경우 이 단계를 건너뛰십시오. 앵커 인증서 내보내기를 클릭하고 `certchain.pem` 파일을 macOS 키 집합 (로그인 또는 시스템) 에 저장합니다.



2 단계: Apple Configurator 2 에서 설정 구성

1. App Store 에서 Apple Configurator 2 를 설치합니다.
2. 도킹 커넥터-USB 케이블을 사용하여 Apple Configurator 2 를 실행하는 Mac 에 장치를 연결합니다. 연결된 장치는 최대 30 개까지 동시에 구성할 수 있습니다. Dock 커넥터가 없는 경우 전원이 연결된 하나 이상의 USB 2.0 고속 허브를 사용하여 장치에 연결합니다.
3. Apple Configurator 2 를 시작합니다. Configurator 에는 감독을 위해 준비할 수 있는 모든 장치가 표시됩니다.
4. 감독할 장치를 준비하려면:
 - 구성을 정기적으로 다시 적용하여 장치의 제어를 유지하려면 장치 감독을 선택합니다. 다음을 클릭합니다.

중요:

감독 모드로 장치를 설정하면 선택한 버전의 iOS 가 장치에 설치되어 이전에 저장된 사용자 데이터 또는 앱 이 장치에서 완전히 초기화됩니다.
 - iOS 에서 **Latest(최신)** 를 클릭하여 설치할 최신 버전의 iOS 를 검색합니다.
5. **MDM** 서버에서 등록에서 MDM 서버를 선택합니다. 새 서버를 추가하려면 다음을 클릭합니다.
6. **MDM** 서버 정의에서 서버 이름을 제공하고 XenMobile 콘솔에서 MDM 서버 URL 을 붙여 넣습니다.
7. 조직에 할당에서 장치를 감독할 조직을 선택합니다.

Apple Configurator 2 로 장치를 준비하는 방법에 대한 자세한 내용은 Apple Configurator 도움말 페이지 [장치 준비](#)를 참조하십시오.
8. 각 장치를 준비할 때 장치를 켜서 iOS 설정 도우미를 시작하면 장치를 처음으로 사용할 수 있도록 준비됩니다.

Apple Configurator 2 에서 Apple Business Manager 에 장치를 할당하려면

Apple Configurator 2 에서 iPhone 및 iPad 장치를 Apple Business Manager 계정과 연결할 수 있습니다. 장치를 추가하면 장치 섹션에 표시됩니다. 이러한 장치에는 Apple Configurator 2 를 통해 할당된 등록 설정이 더 이상 포함되지 않습니다. 자세한 내용은 [Apple Configurator 2 에서 Apple Business Manager 에 추가된 장치 할당](#)을 참조하십시오.

Apple 배포 프로그램 사용 시 인증서 갱신 또는 업데이트

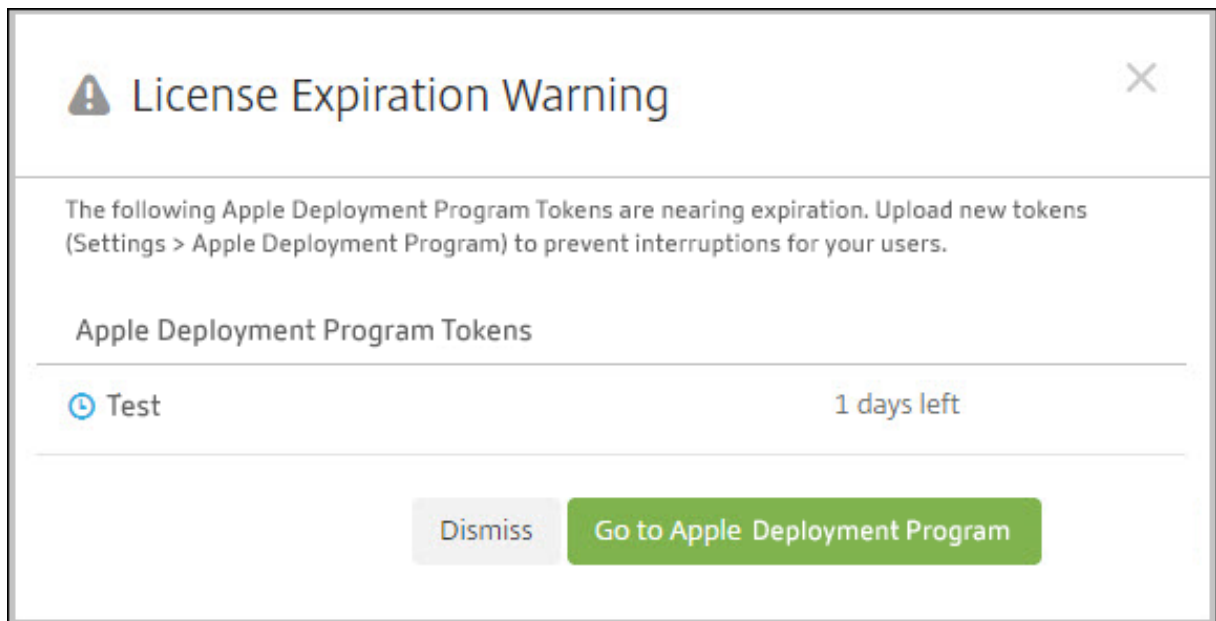
XenMobile SSL(Secure Sockets Layer) 인증서가 갱신되면 XenMobile 콘솔의 설정 > 인증서에서 새 인증서를 업로드합니다. 가져오기 대화 상자의 용도에서 인증서가 SSL 에 사용되도록 **SSL** 수신기를 클릭합니다. 서버를 다시 시작하면 XenMobile 이 새 SSL 인증서를 사용합니다. XenMobile 의 인증서에 대한 자세한 내용은 [XenMobile 의 인증서 업로드](#)를 참조하십시오.

SSL 인증서를 갱신하거나 업데이트할 때 Apple 배포 프로그램과 XenMobile 간의 트러스트 관계를 다시 설정할 필요는 없습니다. 그러나 이 문서의 이전 단계에 따라 언제든지 **Apple** 배포 프로그램 설정을 다시 구성할 수 있습니다.

Apple 배포 프로그램에 대한 자세한 정보는 [Apple 설명서](#)에서 확인하십시오.

Apple 배포 프로그램과 XenMobile 사이의 연결 갱신

XenMobile 은 자동화된 장치 등록 서버 토큰이 만료되면 라이선스 만료 경고를 표시합니다.



Apple School Manager/Apple Business Manager 의 토큰을 교체합니다.

1 단계: XenMobile 서버에서 공개 키 다운로드

1. XenMobile 콘솔에서 설정 > **Apple** 배포 프로그램으로 이동하여 새 공개 키를 다운로드합니다.

2 단계: **Apple** 계정에서 서버 토큰 파일 생성 및 다운로드

1. Apple Business Manager 에 로그인하여 토큰을 다운로드합니다.
2. 설정을 열고 토큰이 필요한 서버를 선택합니다. 편집을 클릭합니다.
3. **MDM** 서버 설정에서 XenMobile 에서 다운로드한 새로운 공개 키를 업로드하고 변경 사항을 저장합니다.
4. 토큰 다운로드를 클릭하여 새 토큰을 다운로드합니다.

3 단계: **XenMobile** 에서 서버 토큰 파일 업로드

1. Citrix XenMobile 에서 설정 > **Apple** 배포 프로그램으로 이동합니다.
2. 배포 프로그램 계정을 선택하고 편집을 클릭한 다음 서버 토큰 파일을 업로드합니다.
3. 다음을 클릭하고 변경 사항을 저장합니다.

클라이언트 속성

December 8, 2023

클라이언트 속성은 사용자 장치에서 Secure Hub 에 직접 제공되는 정보를 포함합니다. 이러한 속성을 사용하여 Citrix PIN 같은 고급 설정을 구성할 수 있습니다. Citrix 지원에서 클라이언트 속성을 가져옵니다.


클라이언트 속성은 Secure Hub 가 릴리스될 때마다 변경될 수 있으며 클라이언트 앱의 경우 가끔 변경될 수 있습니다. 보다 일반적으로 구성된 클라이언트 속성에 대한 자세한 내용은 이 문서 뒷부분에서 클라이언트 속성 참조를 참조하십시오.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 클라이언트에서 클라이언트 속성을 클릭합니다. 클라이언트 속성 페이지가 나타납니다. 이 페이지에서 클라이언트 속성을 추가, 편집 또는 삭제할 수 있습니다.

Settings > Client Properties

Client Properties

To change a property, select the property and then click Edit.

 Add


<input type="checkbox"/>	Name	Key	Value	Description	
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication	
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching	
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password	
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement	
<input type="checkbox"/>	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type	
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement	
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement	
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History	
<input type="checkbox"/>	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer	
<input type="checkbox"/>	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode	

클라이언트 속성을 추가하려면

1. 추가를 클릭합니다. 새 클라이언트 속성 추가 페이지가 나타납니다.

Settings > Client Properties > Add New Client Property

Add New Client Property

Key 

Value*

Name*

Description*

2. 다음 설정을 구성합니다.

- 키: 목록에서 추가하려는 속성을 클릭합니다. 중요: 이 설정을 업데이트하기 전에 Citrix 지원에 문의하십시오. 특수 키를 요청할 수 있습니다.
- 값: 선택한 속성 값입니다.

- 이름: 속성의 이름입니다.
- 설명: 속성의 설명입니다.

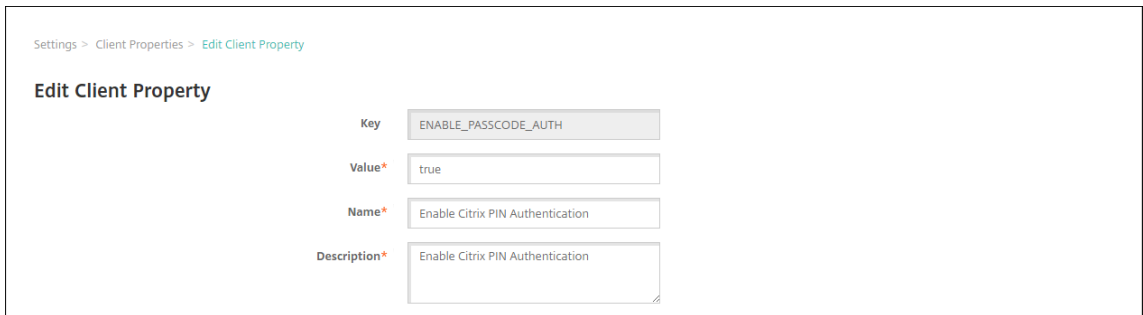
3. 저장을 클릭합니다.

클라이언트 속성을 편집하려면

1. 클라이언트 속성 테이블에서 편집할 클라이언트 속성을 선택합니다.

클라이언트 속성 옆의 확인란을 선택하면 서버 속성 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하면 목록의 오른쪽에 옵션 메뉴가 나타납니다.

2. 편집을 클릭합니다. 클라이언트 속성 편집 페이지가 나타납니다.



3. 다음 정보를 적절하게 변경합니다.

- 키: 이 필드는 변경할 수 없습니다.
- 값: 속성 값입니다.
- 이름: 속성 이름입니다.
- 설명: 속성 설명입니다.

4. 저장을 클릭하여 변경 내용을 저장하거나 취소를 클릭하여 속성을 변경하지 않고 그대로 유지합니다.

클라이언트 속성을 삭제하려면

1. 클라이언트 속성 테이블에서 삭제할 클라이언트 속성을 선택합니다.

각 속성 옆에 있는 확인란을 선택하여 삭제할 속성을 둘 이상 선택할 수 있습니다.

2. 삭제를 클릭합니다. 확인 대화 상자가 나타납니다. 삭제를 다시 클릭합니다.

클라이언트 속성 참조

XenMobile의 미리 정의된 클라이언트 속성과 해당 기본 설정은 다음과 같습니다.

- **CONTAINER_SELF_DESTRUCT_PERIOD**

- 표시 이름: MDX Container Self Destruct Period(MDX 컨테이너 자체 폐기 기간)
- 자체 폐기는 지정된 비활성화 기간 (일) 이 지난 후 Secure Hub 및 관리되는 앱에 액세스할 수 없도록 합니다. 시간 제한 후에는 앱을 더 이상 사용할 수 없습니다. 데이터 초기화에는 설치된 각 앱의 앱 데이터 (앱 캐시 및 사용자 데이터 등) 를 지우는 작업이 포함됩니다.

비활성화 시간은 서버가 특정 시간 동안 사용자 검증을 위한 인증 요청을 수신하지 않는 기간을 의미합니다. 예를 들어 이 속성이 30 일인 경우 사용자가 앱을 30 일 넘게 사용하지 않으면 정책이 적용됩니다.

이 글로벌 보안 정책은 iOS 및 Android 플랫폼에 적용되며 기존의 앱 잠금 및 초기화 정책의 향상된 버전입니다.

- 이 글로벌 정책을 구성하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **CONTAINER_SELF_DESTRUCT_PERIOD** 를 추가합니다.
- 값: 일 수

• DEVICE_LOGS_TO_IT_HELP_DESK

- 표시 이름: 장치 로그를 IT 지원 센터에 보내기
- 이 속성을 사용하여 IT 지원 센터로 로그를 보내는 기능의 사용 여부를 설정합니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

• DISABLE_LOGGING

- 표시 이름: 로깅 사용 안 함
- 사용자가 장치의 로그를 수집하고 업로드할 수 없도록 하려면 이 속성을 사용합니다. 이 속성은 Secure Hub 및 모든 설치된 MDX 앱에 대한 로깅을 사용하지 않도록 설정합니다. 사용자는 지원 페이지에서 앱의 로그를 전송할 수 없습니다. 메일 작성 대화 상자가 표시되지만 로그는 첨부되지 않습니다. 로깅이 비활성화되었다는 메시지가 표시됩니다. 또한 이 설정을 사용하면 XenMobile 콘솔에서 Secure Hub 및 MDX 앱에 대한 로그 설정을 업데이트할 수 없습니다.

이 속성을 **true** 로 설정하면 Secure Hub 에서 **Block application logs**(응용 프로그램 로그 차단) 이 **true** 로 설정됩니다. 따라서 새 정책이 적용될 때 MDX 앱이 로깅을 중지합니다.

- 가능한 값: **true** 또는 **false**
- 기본값: **false**(로깅 사용)

• ENABLE_CRASH_REPORTING

- 표시 이름: Enable Crash Reporting(크래시 보고 사용)
- **true** 인 경우 Citrix 는 iOS 및 Android 용 Secure Hub 의 문제를 해결하는 데 도움이 되는 충돌 보고서 및 진단을 수집합니다. **false** 인 경우 데이터가 수집되지 않습니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **true**

• ENABLE_CREDENTIAL_STORE

- 표시 이름: Enable Credential Store(자격 증명 저장소 사용)
- 자격 증명 저장소를 사용하면 Android 또는 iOS 사용자가 모바일 생산성 앱에 액세스할 때 암호를 한 번만 입력하면 됩니다. Citrix PIN 사용 여부와 상관없이 자격 증명 저장소를 사용할 수 있습니다. Citrix PIN 을 사용하지 않는 경우 사용자는 Active Directory 암호를 입력합니다. XenMobile 은 Secure Hub 및 공용 스토어 앱에 대해서만 자격 증명 저장소와 함께 Active Directory 암호를 사용하도록 지원합니다. 자격 증명 저장소와 함께 Active Directory 암호를 사용하는 경우 XenMobile 에서 PKI 인증을 지원하지 않습니다.
- Secure Mail 에 자동 등록하려면 이 속성을 **true** 로 설정해야 합니다.
- 이 사용자 지정 클라이언트 정책을 구성하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **ENABLE_CREDENTIAL_STORE** 를 추가하고 값을 **true** 로 설정합니다.

• **ENABLE_FIPS_MODE**

- 표시 이름: Enable FIPS Mode(FIPS 모드 사용)
- 이 속성은 모바일 장치에서 FIPS 모드의 사용 여부를 설정합니다. 값을 변경하면 Secure Hub 가 다음번 온라인 인증을 수행할 때 새 값을 장치로 전달합니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

• **ENABLE_PASSCODE_AUTH**

- 표시 이름: Enable Citrix PIN Authentication(Citrix PIN 인증 사용)
- 이 속성을 사용하여 Citrix PIN 기능을 활성화할 수 있습니다. Citrix PIN 또는 암호를 사용하는 경우 Active Directory 암호 대신 사용할 PIN 을 정의하라는 메시지가 나타납니다. 이 설정은 **ENABLE_PASSWORD_CACHING** 이 활성화되거나 XenMobile 이 인증서 인증을 사용하는 경우 자동으로 활성화됩니다.

오프라인 인증의 경우 로컬에서 Citrix PIN 의 유효성이 검사되고 사용자가 요청한 앱이나 콘텐츠에 액세스하도록 허용됩니다. 온라인 인증의 경우 Citrix PIN 또는 암호를 사용하여 Active Directory 암호 또는 인증서를 잠금 해제한 다음 이를 XenMobile 로 전송하여 인증을 수행합니다.

ENABLE_PASSCODE_AUTH 가 true 이고 **ENABLE_PASSWORD_CACHING** 이 false 인 경우 Secure Hub 에 암호가 저장되지 않으므로 온라인 인증 시 항상 암호 입력 메시지가 표시됩니다.

- 가능한 값: **true** 또는 **false**
- 기본값: **false**

• **ENABLE_PASSWORD_CACHING**

- 표시 이름: Enable User Password Caching(사용자 암호 캐싱 사용)
- 이 속성을 사용하면 Active Directory 암호가 모바일 장치에 로컬로 캐싱됩니다. 이 속성을 **true** 로 설정하는 경우 **ENABLE_PASSCODE_AUTH** 속성도 **true** 로 설정해야 합니다. 사용자 암호 캐싱을 사용하도록 설정한 경우 Citrix PIN 또는 암호를 설정하라는 메시지가 나타납니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

- **ENABLE_TOUCH_ID_AUTH**

- 표시 이름: Enable Touch ID Authentication(Touch ID 인증 사용)
- Touch ID 인증을 지원하는 장치의 경우 이 속성은 장치에서 Touch ID 인증의 사용 여부를 설정합니다 요구 사항:

사용자 장치가 Citrix PIN 또는 LDAP 를 사용하도록 설정되어 있어야 합니다. LDAP 인증이 해제된 경우 (예: 인증서 기반 인증만 사용되는 경우) 사용자가 Citrix PIN 을 설정해야 합니다. 이 경우 클라이언트 속성 **ENABLE_PASSCODE_AUTH** 가 **false** 인 경우에도 XenMobile 에 Citrix PIN 이 필요합니다.

사용자가 앱을 시작할 때 Touch ID 를 사용하라는 메시지에 응답해야 하도록 **ENABLE_PASSCODE_AUTH** 를 **false** 로 설정합니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

- **ENABLE_WORXHOME_CEIP**

- 표시 이름: Enable Worx Home CEIP(Worx Home CEIP 사용)
- 이 속성은 CEIP(사용자 환경 개선 프로그램) 를 활성화합니다. 이 기능은 익명의 구성 및 사용 현황 데이터를 Citrix 에 정기적으로 전송합니다. 이 데이터는 Citrix 가 XenMobile 의 품질, 안정성 및 성능을 개선하는 데 도움이 됩니다.
- 값: **true** 또는 **false**
- 기본값: **false**

- **ENCRYPT_SECRETS_USING_PASSCODE**

- 표시 이름: Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)
- 이 속성은 민감한 데이터를 iOS 키 집합과 같은 플랫폼 기반 기본 저장소가 아닌 장치의 기밀 저장소에 저장합니다. 이 속성을 사용하면 키 아티팩트의 암호화가 강화되고 사용자 엔트로피가 추가됩니다. 사용자 엔트로피는 사용자가 생성한 임의의 PIN 코드로, 이 PIN 코드는 사용자만 알고 있습니다.

사용자 장치에서 높은 수준을 보안을 제공하려면 이 속성을 활성화하는 것이 좋습니다. 이 경우 사용자에게 Citrix PIN 에 대한 인증 프롬프트가 더 많이 나타납니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

- **INACTIVITY_TIMER**

- 표시 이름: Inactivity Timer(비활성 타이머)
- 이 속성은 사용자가 장치를 비활성 상태로 둔 후에 Citrix PIN 또는 암호를 입력하라는 메시지 없이 앱에 액세스할 수 있는 시간을 정의합니다. MDX 앱에 대해 이 설정을 사용되도록 설정하려면 앱 암호 설정을 꺼짐으로 설정합니다. 앱 암호 설정이 꺼짐으로 설정된 경우 사용자는 전체 인증을 수행하기 위해 Secure Hub 로 리디렉션됩니다. 이 설정을 변경하면 다음에 사용자에게 인증하라는 메시지가 표시될 때 값이 적용됩니다.

iOS 에서 비활성 타이머는 MDX 및 비 MDX 앱의 Secure Hub 액세스 권한도 제어합니다.

- 가능한 값: 양의 정수
- 기본값: **15** 분

• **ON_FAILURE_USE_EMAIL**

- 표시 이름: On failure Use Email to Send device logs to IT help desk(장애 시 전자 메일을 사용하여 장치 로그를 IT 지원 센터에 보내기)
- 이 속성은 전자 메일을 사용하여 IT 에 장치 로그를 보내는 기능의 사용 여부를 설정합니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **true**

• **PASSCODE_EXPIRY**

- 표시 이름: PIN Change Requirement(PIN 변경 요구 사항)
- 이 속성은 Citrix PIN 또는 암호가 유효한 기간을 정의합니다. 이 기간이 지나면 사용자가 Citrix PIN 또는 암호를 변경하도록 강제합니다. 이 설정을 변경하면 현재 Citrix PIN 또는 암호가 만료된 경우에만 새 값이 설정됩니다.
- 가능한 값: **1 ~ 99**(권장) 입니다. PIN 재설정을 제거하려면 값을 매우 높은 숫자로 설정합니다 (예: 100,000,000,000). 원래 만료 기간을 1 일에서 99 일 사이로 설정한 경우 해당 기간 동안 이 기간을 큰 수로 변경하면 PIN 은 초기 기간이 끝날 때 만료되지만 이후에는 다시 만료되지 않습니다.
- 기본값: **90** 일

• **PASSCODE_HISTORY**

- 표시 이름: PIN History(PIN 기록)
- 이 속성은 사용자가 Citrix PIN 또는 암호를 변경할 때 재사용할 수 없는 이전에 사용된 Citrix PIN 또는 암호의 수를 정의합니다. 이 설정을 변경하면 새 값은 다음번에 사용자가 Citrix PIN 또는 암호를 재설정할 때 설정됩니다.
- 가능한 값: **1~99**
- 기본값: **5**

• **PASSCODE_MAX_ATTEMPTS**

- 표시 이름: PIN Attempts(PIN 시도 횟수)
- 이 속성은 전체 인증 메시지를 표시하기 전에 사용자가 시도할 수 있는 잘못된 Citrix PIN 또는 암호 횟수를 정의합니다. 사용자가 전체 인증을 성공적으로 수행하면 Citrix PIN 또는 암호를 만들라는 메시지가 표시됩니다.
- 가능한 값: 양의 정수
- 기본값: **15**

• **PASSCODE_MIN_LENGTH**

- 표시 이름: PIN Length Requirement(PIN 길이 요구 사항)
- 이 속성은 Citrix PIN 의 최소 길이를 정의합니다.
- 가능한 값: **4 ~ 10**
- 기본값: **6**

• PASSCODE_STRENGTH

- 표시 이름: PIN Strength Requirement(PIN 강도 요구 사항)
- 이 속성은 Citrix PIN 또는 암호의 강도를 정의합니다. 이 설정을 변경하면 사용자가 다음번에 인증을 수행할 때 Citrix PIN 또는 암호를 생성하라는 메시지가 나타납니다.
- 가능한 값: 약함, 중간, 다소 강함 또는 강함
- 기본값: 중간
- PASSCODE_TYPE 설정을 기반으로 각 강도 설정에 대한 암호 규칙은 다음과 같습니다.

숫자 암호에 대한 규칙:

암호 강도	숫자 암호 유형에 대한 규칙	허용	허용 안 함
Low(낮음)	모든 숫자, 모든 순서가 허용 됨	444444, 123456, 654321	
Medium(중간)(기본 설정)	모든 숫자가 동일하거나 연속 해서는 안 됩니다.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
높음	인접한 숫자는 같을 수 없습니 다.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Strong(강함)	같은 숫자를 세 번 이상 사용 하지 마십시오. 세 개 이상의 숫자를 연속으로 사용하지 마 십시오. 세 개 이상의 연속된 숫자를 역순으로 사용하지 마 십시오.	102983, 085085, 824673, 132312	132132, 131313, 902030

영숫자 암호에 대한 규칙:

암호 강도	영숫자 암호 유형에 대한 규칙	허용	허용 안 함
Low(낮음)	하나 이상의 숫자와 하나의 문 자가 있어야 합니다.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
Medium(중간)(기본 설정)	낮음 암호 강도에 대한 규칙에 더해 문자와 모든 숫자가 동일 해서는 안 됩니다. 문자가 연 속해서는 안 되며 숫자가 연속 해서는 안 됩니다.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, or cba123

암호 강도	영숫자 암호 유형에 대한 규칙	허용	허용 안 함
높음	최소한 대문자 하나와 소문자 하나를 포함해야 합니다.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Strong(강함)	최소한 숫자 하나, 특수 기호 하나, 대문자 하나 및 소문자 하나를 포함해야 합니다.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

• PASSCODE_TYPE

- 표시 이름: PIN Type(PIN 유형)
- 이 속성은 사용자가 숫자 Citrix PIN 또는 영숫자 암호를 정의할 수 있는지 여부를 정의합니다. **Numeric(숫자)**를 선택하면 사용자가 숫자만 (Citrix PIN) 사용할 수 있습니다. **Alphanumeric(영숫자)**를 선택하면 사용자가 문자와 숫자 조합 (암호)을 사용할 수 있습니다.
이 설정을 변경하면 사용자가 다음번에 인증을 수행할 때 새 Citrix PIN 또는 암호를 설정해야 합니다.
- 가능한 값: **Numeric(숫자)** 또는 **Alphanumeric(영숫자)**
- 기본값: **Numeric(숫자)**

• REFRESHINTERVAL

- 표시 이름: REFRESHINTERVAL
- 기본적으로 XenMobile 은 3 일마다 고정된 인증서에 대해 ADS(자동 검색 서버)에 ping 을 수행합니다. 새로 고침 간격을 변경하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **REFRESHINTERVAL**를 추가하고 값을 숫자 (시간)로 설정합니다.
- 기본값은 **72** 시간 (3 일)입니다.

• SEND_LDAP_ATTRIBUTES

- Android, iOS 또는 macOS 장치의 MAM 전용 배포의 경우, 전자 메일 자격 증명으로 Secure Hub에 등록된 사용자가 자동으로 Secure Mail에 등록되도록 XenMobile을 구성할 수 있습니다. 이렇게 하면 사용자가 추가 정보를 제공하거나 추가 단계를 수행하지 않고 Secure Mail에 등록할 수 있습니다.
- 이 글로벌 클라이언트 정책을 구성하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **SEND_LDAP_ATTRIBUTES**를 추가하고 값을 다음과 같이 설정합니다.
- 값: `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
- 속성 값은 MDM 정책과 유사하게 매크로로 지정됩니다.
- 다음은 이 속성의 샘플 계정 서비스 응답입니다.

```
<property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,email=user@site.com\,user@site.com"name="SEND_LDAP_ATTRIBUTES"/>
```

- 이 속성의 경우 XenMobile 은 쉼표 문자를 문자열 종결자로 취급합니다. 그러므로 특성 값에 쉼표가 포함되는 경우 그 앞에 백슬래시를 추가해야 합니다. 백슬래시를 추가하면 클라이언트가 포함된 쉼표를 특성 값의 끝으로 해석하지 않습니다. 백슬래시 문자는 "\\\"로 표현합니다.

• HIDE_THREE_FINGER_TAP_MENU

- 이 속성이 설정되지 않거나 **false** 로 설정된 경우 사용자가 장치에서 세 손가락 누르기를 수행하여 숨겨진 기능 메뉴에 액세스할 수 있습니다. 숨겨진 기능 메뉴를 사용하면 사용자가 응용 프로그램 데이터를 재설정할 수 있습니다. 이 속성을 **true** 로 설정하면 사용자가 숨겨진 기능 메뉴에 액세스할 수 없습니다.
- 이 글로벌 클라이언트 정책을 구성하려면 설정 > 클라이언트 속성으로 이동하고 사용자 지정 키 **HIDE_THREE_FINGER_TAP_MENU** 를 추가한 다음 값을 설정합니다.

• TUNNEL_EXCLUDE_DOMAINS

- 표시 이름: Tunnel Exclude Domains
- 기본적으로 MDX 는 Micro VPN 터널링에서 XenMobile SDK 및 앱이 여러 기능에 사용하는 일부 서비스 끝점을 제외합니다. 예를 들어 이러한 끝점에는 Google Analytics, Citrix Cloud Services, Active Directory 서비스 등 엔터프라이즈 네트워크를 통한 라우팅이 필요하지 않은 서비스가 포함됩니다. 제외되는 도메인의 기본 목록을 재정의하려면 이 클라이언트 속성을 사용합니다.
- 이 글로벌 클라이언트 정책을 구성하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **TUNNEL_EXCLUDE_DOMAINS** 를 추가하고 값을 설정합니다.
- 값: 터널링에서 제외할 도메인으로 기본 목록을 바꾸려면 쉼표로 구분된 도메인 접미사 목록을 입력합니다. 터널링에 모든 도메인을 포함하려면 **none** 을 입력합니다. 기본값은 다음과 같습니다.

```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,
cis-test.citrix.com,clientstream,launchdarkly.com,crashlytics
.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.
com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xml.citrix.
com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.
com,ssl.google-analytics.com,stream.launchdarkly.com
```

XenMobile Server 의 사용자 지정 클라이언트 속성은 다음과 같습니다.

ENABLE_MAM_NFACTOR_SSO:

- 이 속성을 사용하면 NetScaler Gateway 에서 고급 인증 정책을 사용하는 상태로 MAM 을 등록하거나 Secure Hub 에 로그인하는 동안 MAM nFactor SSO 를 활성화하거나 비활성화할 수 있습니다. 값을 **true** 로 설정하면 MAM 을 등록하거나 Secure Hub 에 로그인하는 동안 MAM nFactor SSO 가 활성화됩니다.

- 이 속성을 구성하려면 설정 > 클라이언트 속성으로 이동하여 추가를 클릭합니다. 키 드롭다운 메뉴에서 사용자 지정 키를 선택하고 다음 정보를 적절하게 업데이트합니다.

- 키 - ENABLE_MAM_NFACTOR_SSO
- 값 - true 또는 false
- 이름 - ENABLE_MAM_NFACTOR_SSO
- 설명 - 관련 설명을 추가합니다.

Apple 배포 프로그램을 통한 장치 배포

March 15, 2024

Apple에는 비즈니스 및 교육 계정을 위한 장치 등록 프로그램이 있습니다. 비즈니스 계정의 경우 XenMobile에서 Apple Business Manager(ABM) 또는 Apple School Manager(ASM)를 사용하여 장치를 등록하고 관리하려면 Apple 배포 프로그램에 등록해야 합니다. 이 프로그램은 iOS, iPadOS 및 macOS 장치를 위한 것입니다.

Apple 배포 프로그램은 조직을 위한 프로그램이며 개인 사용자는 사용할 수 없습니다. Apple Deployment Program 계정을 만들려면 상당한 양의 회사 세부 정보를 제공해야 합니다. 계정을 요청하고 승인을 받는 데 시간이 걸릴 수 있습니다.

교육 계정의 경우 Apple School Manager 계정을 생성합니다. ASM는 Apple 배포 프로그램과 Apple 볼륨 구매를 통합합니다. Apple School Manager 계정을 생성하려면 [Apple School 사이트](#)로 이동합니다.

Apple 배포 프로그램 등록

Apple Business Manager에 등록하려면 [business.apple.com](#)으로 이동합니다. 지금 등록을 클릭하여 새 계정을 신청합니다. 조직의 전자 메일 주소 (예: [deployment@company.com](#))를 사용하는 것이 가장 좋습니다. 등록 절차에는 며칠이 걸릴 수 있습니다. 로그인 자격 증명을 받은 후 Apple Business Manager에 제공된 단계에 따라 계정을 만듭니다.

참고:

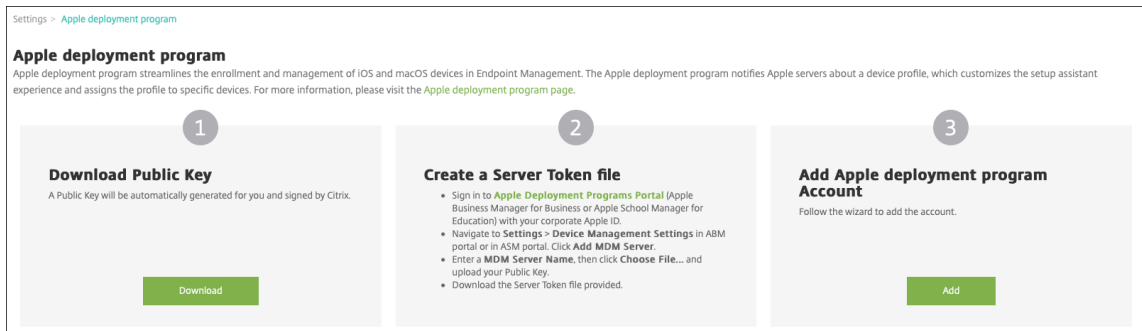
교육 계정의 경우 [Apple 교육 기능과 통합](#)을 참조하십시오.

XenMobile와 Apple Business Manager 계정 연결

Apple Business Manager 계정을 XenMobile 배포와 연결하려면 XenMobile 콘솔과 Apple Business Manager에 정보를 입력합니다. 다음 단계를 따르십시오.

1 단계: XenMobile 서버에서 공개 키 다운로드

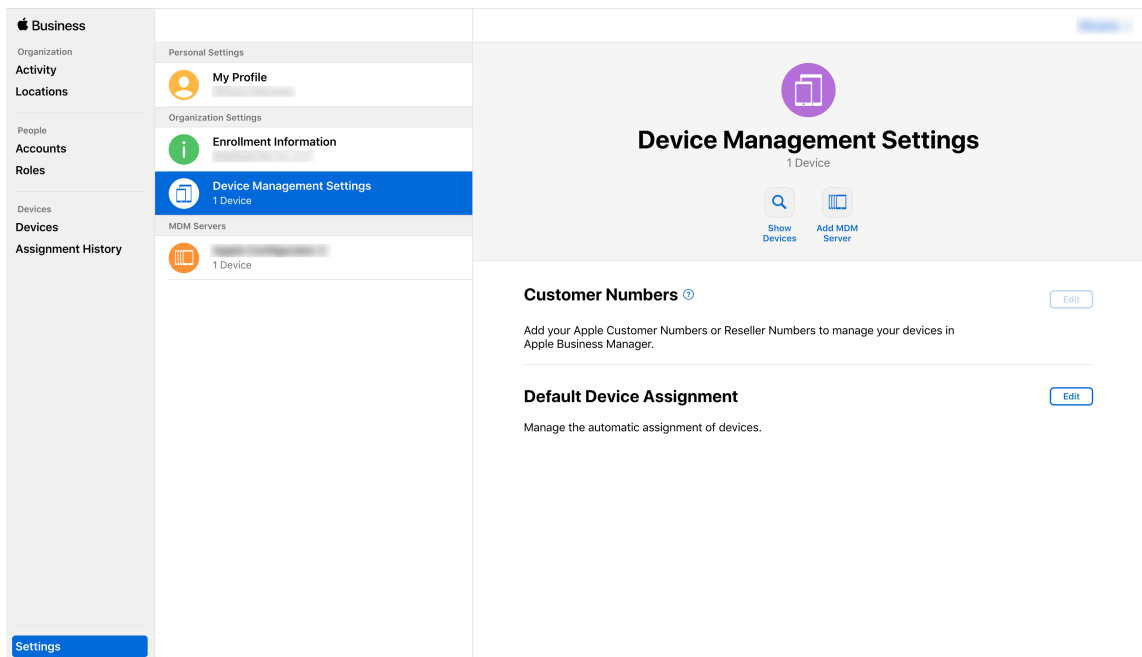
1. XenMobile 콘솔에서 설정 > Apple 배포 프로그램으로 이동합니다.



2. 공개 키 다운로드에서 다운로드를 클릭합니다.

2 단계: Apple 계정에서 서버 토큰 파일 생성 및 다운로드

1. 관리자 또는 장치 등록 관리자 계정을 사용하여 [Apple Business Manager](#)에 로그인합니다.
2. 사이드바 하단에서 설정을 클릭한 다음 장치 관리 설정 > **MDM** 서버 설정을 클릭합니다.



3. **MDM** 서버 이름 설정에서 XenMobile Server의 이름을 입력합니다. 입력하는 서버 이름은 참조용입니다. 서버 URL 또는 이름이 아닙니다.
4. 공개 키 업로드에서 파일 선택을 클릭합니다. XenMobile에서 다운로드한 공개 키를 업로드한 다음 변경 내용을 저장합니다.
5. 토큰 다운로드를 클릭하여 서버 토큰 파일을 컴퓨터에 다운로드합니다.

서버 토큰 파일은 ABM 계정을 XenMobile에 추가할 때 업로드해야 합니다. 토큰 파일을 가져오면 ABM 토큰 정보가 XenMobile 콘솔에 표시됩니다.

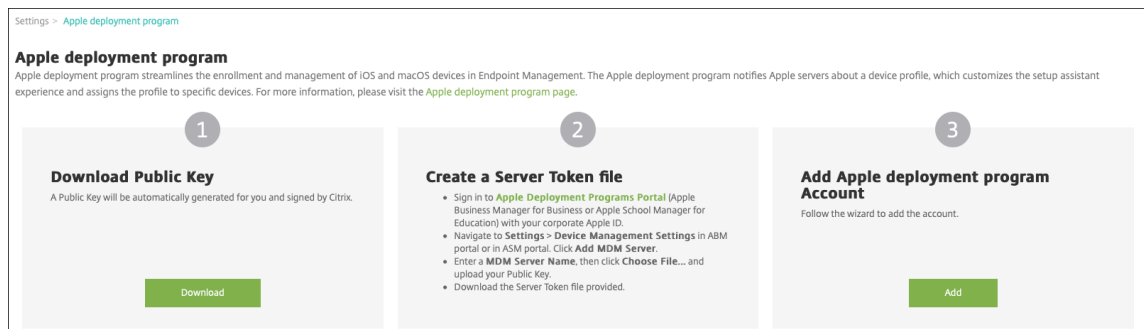
6. 기본 장치 할당에서 변경을 클릭합니다. 장치 할당 방법을 선택한 후 요청된 정보를 제공합니다. 자세한 내용은 [ABM 사용자 가이드](#)를 참조하십시오.

3 단계: XenMobile 에 ABM 계정 추가

여러 개의 ABM 계정을 XenMobile 에 추가할 수 있습니다. 이 기능을 사용하면 서로 다른 등록 설정 및 설정 도우미 옵션을 국가, 부서별로 사용할 수 있습니다. 그런 다음 ABM 계정을 여러 장치 정책에 연결할 수 있습니다.

예를 들어 여러 국가에 있는 동일한 XenMobile 서버의 모든 ABM 계정을 중앙 집중화하여 모든 ABM 장치를 가져오고 감독할 수 있습니다. 등록 설정 및 설정 도우미 옵션을 부서, 조직 계층 또는 다른 구조별로 사용자 지정하면 정책을 통해 조직 전체에 적절한 기능을 제공하고 사용자가 적절한 지원을 받을 수 있습니다.

1. XenMobile 콘솔에서 설정 > **Apple** 배포 프로그램으로 이동한 다음 **Apple** 배포 프로그램 계정 추가에서 추가를 클릭합니다.



2. 서버 토큰 페이지에서 서버 토큰 파일을 지정하고 업로드를 클릭합니다.

Apple deployment program Account	
1 Server Tokens	<h3>Server Tokens</h3> <p>Upload the Server Token file that you downloaded from Apple Business Manager portal or Apple School Manager portal.</p> <p>Select Server Token file <small>*</small> <input type="text" value="untitled_mdm_server_token_..."/> <input type="button" value="Upload"/></p> <p>Consumer key <input type="text"/></p> <p>Consumer secret <input type="text"/></p> <p>Access token <input type="text"/></p> <p>Access secret <input type="text"/></p> <p>Access token expiration 10/30/20 6:25:52 pm</p> <p>Server name Untitled MDM Server</p> <p>Server UUID <input type="text"/></p> <p>Apple admin ID <input type="text"/></p> <p>Organization ID <input type="text"/></p> <p>Organization name <input type="text"/></p> <p>Organization type Education</p> <p>Organization version v2</p> <p>Organization email <input type="text"/></p> <p>Organization phone <input type="text"/></p> <p>Organization address <input type="text"/></p>
2 Account Info	
3 Settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

서버 토큰 정보가 표시됩니다.

3. 계정 정보 페이지에서 다음 설정을 지정합니다.

Apple deployment program Account	
1 Server Tokens	<h3>Account Info</h3> <p>Specify your Apple deployment program account information.</p> <p>Apple deployment program account name <small>*</small> <input type="text" value="ASM Deployment"/></p> <p>Business/Education unit <small>*</small> <input type="text" value="Central High School"/></p> <p>Unique service ID <input type="text" value="2359487"/></p> <p>Support phone number <small>*</small> <input type="text" value="555555555"/></p> <p>Support email address <input type="text"/></p> <p>Education suffix <small>*</small> <input type="text" value="suffix"/></p>
2 Account Info	
3 Settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

- **Apple** 배포 프로그램 계정 이름: 이 Apple 배포 프로그램 계정의 고유한 이름입니다. 국가 또는 조직 계층 구조 별과 같이 Apple 배포 프로그램 계정을 구성하는 방식을 반영하는 이름을 사용합니다.
- **Business/Education unit(비즈니스/교육 단위)**: 장치를 할당할 비즈니스 단위 또는 부서입니다. 이것은 필수 필드입니다.
- 고유 서비스 ID: 계정을 식별하는 데 도움이 되는 선택적 고유 ID 입니다.
- 지원 전화 번호: 사용자가 설정 중에 전화할 수 있는 지원 전화 번호입니다. 이것은 필수 필드입니다.
- 지원 전자 메일 주소: 최종 사용자에게 제공되는 선택적 지원 전자 메일 주소입니다.

4. iOS 설정에서 다음 설정을 지정합니다.

Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account

DEP Account

- 1 Account Info
- 2 Server Tokens
- 3 Settings
- iOS**
- macOS
- 4 Setup Assistant Options
- iOS
- macOS

iOS Settings
Specify the settings to define the enrollment process and the mode of iOS DEP devices.

Enrollment settings

- Require device enrollment: YES
- Require credentials for device enrollment: NO (iOS 7.1+)
- Wait for configuration to complete setup: NO (iOS 9.0+)

Device settings

- Supervised mode: YES
- Allow enrollment profile removal: NO
- Allow device pairing: NO

등록 설정:

- 장치 등록 필요: 사용자가 장치를 등록해야 하는지 여부를 설정합니다. 기본값은 예입니다.
- 장치 등록에 자격 증명 필요: ABM 설정 중에 사용자가 자격 증명을 입력해야 하는지 여부를 설정합니다. 모든 사용자에게 장치 등록 중에 자격 증명을 입력하도록 요구하는 것이 좋습니다. 즉, 권한이 있는 사용자만 장치를 등록할 수 있도록 허용합니다. 기본값은 예입니다.

처음 설정하기 전에 ABM 을 사용 설정하고 이 옵션을 선택하지 않으면 XenMobile 이 ABM 구성 요소를 만듭니다. 이렇게 만들어지는 구성 요소로는 ABM 사용자, Secure Hub, 소프트웨어 인벤토리, ABM 배포 그룹이 있습니다. 이 옵션을 선택하면 XenMobile 이 구성 요소를 만들지 않습니다. 그 결과 나중에 이 옵션을 삭제할 경우 자격 증명을 입력하지 않은 사용자는 ABM 구성 요소가 존재하지 않으므로 ABM 으로 등록할 수 없습니다. ABM 구성 요소를 추가하려면 ABM 계정을 사용하지 않도록 설정한 다음 사용하도록 설정해야 합니다.

- 구성에서 설정을 완료할 때까지 대기: 모든 MDM 리소스가 장치에 배포될 때까지 사용자가 설정 도우미 모드에 있어야 하는지 여부를 설정합니다. 이 옵션은 감독 모드인 장치에서 사용할 수 있습니다. 기본값은 아니요입니다.
- Apple 설명서에 따르면 장치가 설정 도우미 모드에 있는 동안에는 다음 명령이 작동하지 않을 수 있습니다.
 - InviteToProgram
 - InstallApplication
 - ApplyRedemptionCode
 - InstallMedia
 - RequestMirroring
 - DeviceLock

장치 설정:

- 감독 모드: Apple Configurator 를 사용하여 ABM 등록 장치를 관리하거나 구성에서 설정을 완료할 때까지 대기를 사용하는 경우 예로 설정해야 합니다. 기본값은 예입니다. iOS 장치를 감독 모드로 전환하는 방법에 대한 자세한 내용은 [Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 전환](#)을 참조하십시오.
- 등록 프로필 제거 허용: 원격으로 제거할 수 있는 프로필을 장치에서 사용하도록 할지 여부를 설정합니다. 기본값은 아니요입니다.
- 장치 페어링 허용: ABM 을 통해 등록한 장치를 Apple Music 및 Apple Configurator 를 통해 관리할지 여부를 설정합니다. 기본값은 아니요입니다.

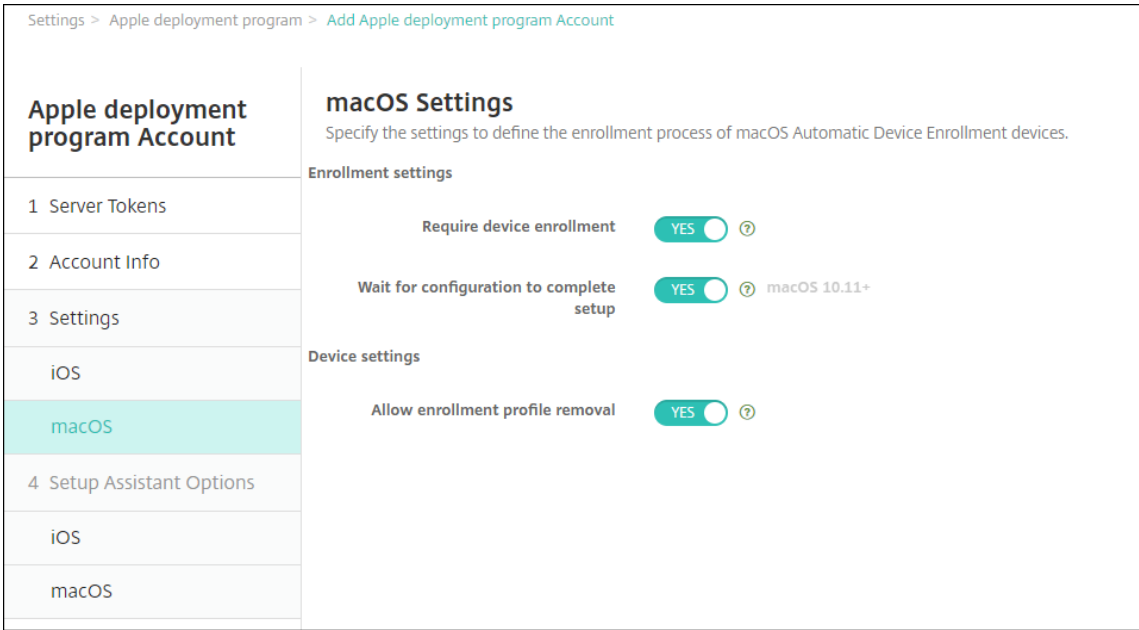
감독 ID

GroundControl 도구를 사용하는 경우 인증서를 추가하여 다음을 수행할 수 있습니다.

- 페어링 제한을 재정의하여 “이 호스트 신뢰” 메시지를 방지합니다.
- USB 로 관리되는 장치 동작을 에스컬레이션하여 사용자 상호 작용 없는 프로필 설치와 같은 활동을 수행합니다. 이렇게 하면 GroundControl 로 체크아웃에 단일 앱 모드와 장치 잠금을 사용할 수 있습니다.
- 백업을 ABM 장치에 복원합니다.

GroundControl 에 대한 자세한 정보는 [GroundControl 웹 사이트](#)를 참조하십시오.

5. macOS 설정에서 다음 설정을 지정합니다.

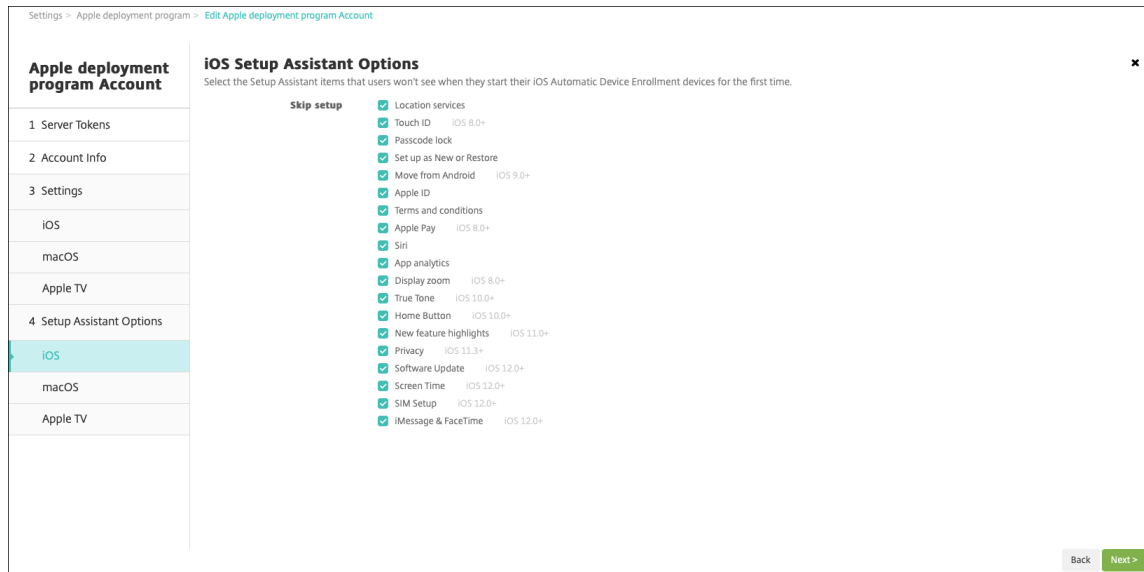


등록 설정:

- **장치 등록 필요:** 사용자가 장치를 등록해야 하는지 여부를 설정합니다. 기본값은 예입니다.
- **구성에서 설정을 완료할 때까지 대기:** 예인 경우 MDM 리소스 암호가 장치에 배포되기 전까지 설정 도우미에서 macOS 장치가 계속되지 않습니다. 해당 배포는 로컬 계정이 만들어지기 전에 발생합니다. 이 설정은 macOS 10.11 이상 장치에서 사용할 수 있습니다. 기본값은 아니요입니다.

장치 설정:

- **등록 프로필 제거 허용:** 원격으로 제거할 수 있는 프로필을 장치에서 사용하도록 할지 여부를 설정합니다. 기본값은 아니요입니다.
6. **ios** 설정 도우미 옵션에서 사용자가 장치를 처음으로 시작할 때 iOS 설정 도우미가 건너뛸 단계를 선택합니다. 화면을 건너뛰면 관련 기능에는 기본 설정이 사용됩니다. 건너뛴 기능에 대한 액세스를 완전히 제한하지 않는 한 사용자는 설정이 완료된 후 해당 기능을 구성할 수 있습니다. 기능 액세스 제한에 대한 자세한 내용은 [제한 장치 정책](#)을 참조하십시오. 모든 항목에 대한 기본값은 선택되어 있지 않습니다. 다음 설명에서는 설정 선택 시 발생하는 결과에 대해 설명합니다.



- **위치 서비스:** 사용자가 장치에서 위치 서비스를 설정할 수 없습니다.
- **Touch ID:** 사용자가 iOS 장치에서 Touch ID 또는 Face ID 를 설정할 수 없습니다.
- **암호 잠금:** 사용자가 장치에 대한 암호를 설정할 수 없습니다. 암호가 없으면 사용자는 Touch ID 또는 Apple Pay 를 사용할 수 없습니다.
- **새로 설정 또는 복원:** 사용자가 장치를 새로 설정하거나 iCloud 또는 Apple App Store 백업에서 설정할 수 없습니다.
- **Android 에서 이동:** 사용자가 Android 장치의 데이터를 iOS 장치로 전송할 수 없습니다. 이 옵션은 새로 설정 또는 복원을 선택한 경우에만 사용할 수 있습니다 (즉, 단계가 생략됨).
- **Apple ID:** 사용자가 장치에 대한 관리형 Apple ID 계정을 설정할 수 없습니다.
- **이용 약관:** 사용자가 장치 사용 약관을 읽고 수락할 수 없습니다.
- **Apple Pay:** 사용자가 Apple Pay 를 설정할 수 없습니다. 이 설정을 선택 취소하면 사용자는 Touch ID 및 Apple ID 를 설정해야 합니다. 이러한 설정이 선택 취소되었는지 확인하시기 바랍니다.
- **Siri:** 사용자가 Siri 를 구성할 수 없습니다.
- **앱 분석:** 사용자가 충돌 데이터 및 사용 현황 통계를 Apple 과 공유할지 여부를 설정할 수 없습니다.
- **표시 확대/축소:** 사용자가 iOS 장치에서 디스플레이 해상도 (표준 또는 확대) 를 설정할 수 없습니다.
- **True Tone:** 사용자가 4 채널 센서를 설정해 디스플레이의 화이트 밸런스를 동적으로 조정할 수 없습니다.
- **홈 버튼:** 사용자가 홈 버튼 스타일의 피드백을 설정할 수 없습니다.
- **새로운 기능 하이라이트:** 사용자에게 Apple 소프트웨어의 새로운 기능에 대한 정보를 보여주는 화면이 표시되지 않습니다.
- **개인 정보 보호:** 사용자에게 데이터 및 개인 정보 보호 패널이 표시되지 않습니다. iOS 11.3 이상에 해당합니다.
- **소프트웨어 업데이트:** 사용자가 iOS 를 최신 버전으로 업데이트할 수 없습니다. iOS 12.0 이상에 해당합니다.
- **스크린 타임:** 사용자가 스크린 타임을 활성화할 수 없습니다. iOS 12.0 이상에 해당합니다.
- **SIM 설정:** 사용자가 셀룰러 요금제를 설정하지 못하도록 합니다. iOS 12.0 이상에 해당합니다.
- **iMessage 및 FaceTime:** 사용자가 iMessage 와 FaceTime 사용 설정하지 못하도록 합니다. iOS 12.0 이상에 해당합니다.
- **모양:** 사용자가 모양 모드를 선택할 수 없습니다. iOS 13.0 이상에 해당합니다.

- **시작:** 사용자에게 시작 화면이 표시되지 않습니다. iOS 13.0 이상에 해당합니다.
- **복원 완료:** 설치 중에 복원이 완료되었는지 여부가 사용자에게 표시되지 않습니다. iOS 14.0 에 해당합니다.
- **업데이트 완료:** 설치 중에 소프트웨어 업데이트가 완료되었는지 여부가 사용자에게 표시되지 않습니다. iOS 14.0 에 해당합니다.

ABM 계정이 설정 > **Apple** 배포 프로그램에 표시됩니다.

7. **macOS** 설정 도우미 옵션에서 사용자가 장치를 처음으로 시작할 때 macOS 설정 도우미가 건너뛴 단계를 선택합니다. 화면을 건너뛰면 관련 기능에는 기본 설정이 사용됩니다. 건너뛴 기능에 대한 액세스를 완전히 제한하지 않는 한 사용자는 설정이 완료된 후 해당 기능을 구성할 수 있습니다. 기능 액세스 제한에 대한 자세한 내용은 [제한 장치 정책](#)을 참조하십시오. 오. 모든 항목에 대한 기본값은 선택되어 있지 않습니다. 다음 설명에서는 설정 선택 시 발생하는 결과에 대해 설명합니다.

- **새 장치로 설정 또는 복원:** 사용자가 장치를 새 장치로 또는 Time Machine 백업에서 장치를 설정하거나 시스템 마이그레이션을 수행할 수 없습니다.
- **위치 서비스:** 사용자가 장치에서 위치 서비스를 설정할 수 없습니다. macOS 10.11 이상에 해당합니다.
- **Apple ID:** 사용자가 장치에 대한 관리형 Apple ID 계정을 설정할 수 없습니다.
- **이용 약관:** 사용자가 장치 사용 약관을 읽고 수락할 수 없습니다.
- **Siri:** 사용자가 Siri 를 구성할 수 없습니다. macOS 10.12 이상에 해당합니다.
- **FileVault:** FileVault 를 사용하여 시동 디스크를 암호화합니다. XenMobile 은 iCloud 에 로그인한 로컬 사용자 계정이 하나인 경우에만 FileVault 설정을 적용합니다.

macOS FileVault 디스크 암호화 기능으로 시스템 볼륨 콘텐츠를 암호화하여 시스템 볼륨을 보호할 수 있습니다 (<https://support.apple.com/en-us/HT204837>). FileVault 가 꺼져 있는 최신 휴대용 Mac 에서 설정

도우미를 실행하면 이 기능을 켜라는 메시지가 표시될 수 있습니다. 새 시스템과 OS X 10.10 또는 10.11 로 업그레이드한 시스템에 메시지가 표시되지만 시스템에 로컬 관리자 계정이 하나이고 이 계정으로 iCloud 에 로그인한 경우에만 표시됩니다.

- **앱 분석:** 사용자가 충돌 데이터 및 사용 현황 통계를 Apple 과 공유할지 여부를 설정할 수 없습니다.
- **개인 정보 보호:** 사용자에게 데이터 및 개인 정보 보호 패널이 표시되지 않습니다. macOS 10.13 이상에 해당합니다.
- **iCloud 분석:** 사용자가 진단 iCloud 데이터를 Apple 에 전송할지 여부를 선택할 수 없습니다. macOS 10.13 이상에 해당합니다.
- **iCloud 문서 및 데스크톱:** 사용자가 iCloud 데스크톱 및 문서를 설정할 수 없습니다. macOS 10.13 이상에 해당합니다.
- **모양:** 사용자가 모양 모드를 선택할 수 없습니다. macOS 10.14 이상에 해당합니다.
- **접근성:** 사용자가 Voice Over 를 자동으로 들을 수 없습니다. 장치가 인터넷에 연결된 경우에만 사용할 수 있습니다. macOS 11 이상에 해당합니다.
- **생체 인식:** 사용자가 Touch ID 및 Face ID 를 설정할 수 없습니다. macOS 10.12.4 이상에 해당합니다.
- **True Tone:** 사용자가 4 채널 센서를 설정해 디스플레이의 화이트 밸런스를 동적으로 조정할 수 없습니다. macOS 10.13.6 이상에 해당합니다.
- **Apple Pay:** 사용자가 Apple Pay 를 설정할 수 없습니다. 이 설정을 선택 취소하면 사용자는 Touch ID 및 Apple ID 를 설정해야 합니다. **Apple ID** 및 생체 인식 설정이 선택 취소되었는지 확인합니다. macOS 10.12.4 이상에 해당합니다.
- **스크린 타임:** 사용자가 스크린 타임을 활성화할 수 없습니다. macOS 10.15 이상에 해당합니다.
- **로컬 계정 설정 옵션:** 장치에서 관리자 계정을 만들 때 사용할 설정을 지정합니다. 사용자는 이 정보로 macOS 장치에 로그인합니다. XenMobile 이 지정된 정보를 사용하여 계정을 만듭니다.
 - **표준 사용자로 기본 계정 생성:** 이 사용자에게 장치의 관리자 권한을 부여하는 대신 XenMobile 에서는 표준 권한이 있는 사용자를 생성합니다. macOS 에는 관리자 계정이 필요하므로 XenMobile 은 관리자 계정을 먼저 만든 다음 새 표준 계정을 만들고 기본으로 설정합니다.
 - **관리자 전체 이름:** 시스템에서 관리자 계정에 대해 표시할 이름을 입력합니다.
 - **관리자 짧은 이름:** 장치에서 홈 폴더에 간략하게 표시할 이름을 입력합니다.
 - **관리자 암호:** 관리자 계정의 보안 암호를 입력합니다.
 - **사용자 및 그룹의 관리자 계정 표시:** 지워질 경우 관리자 계정은 macOS 설정의 관리자 및 그룹에 나타나지 않습니다. 기본 계정을 표준 사용자로 생성할 경우 이 설정을 사용하여 XenMobile 에서 만든 관리자 계정을 먼저 숨깁니다.

배포 프로그램 사용 장치 주문

Apple 또는 배포 프로그램 지원 공인 리셀러 또는 통신사에서 직접 배포 프로그램 지원 장치를 주문할 수 있습니다. Apple 에서 주문하려면 Apple 배포 프로그램 포털에서 Apple 고객 ID 를 제공합니다. 고객 ID 를 통해 구입한 장치가 Apple 배포 프로그

램 계정과 연결될 수 있습니다.

리셀러 또는 이동 통신 사업자에서 주문하려면 Apple 리셀러 또는 이동 통신 사업자에 연락하여 Apple 배포 프로그램에 참여하는지 여부를 문의해야 합니다. 장치를 구입할 때 리셀러의 Apple 배포 프로그램 ID 를 요청하십시오. Apple 배포 프로그램 리셀러를 Apple 배포 프로그램 계정에 추가할 때 이 정보가 필요합니다. 리셀러의 Apple 배포 프로그램 ID 를 추가한 후 배포 프로그램 고객 ID 를 받게 됩니다. 배포 프로그램 고객 ID 를 리셀러에 제공하면 리셀러에서 이 ID 를 사용하여 장치 구매 정보를 Apple 에 제출합니다. 자세한 내용은 [Apple 사용 장치 등록 사이트](#)를 참조하십시오.

배포 프로그램 지원 장치 관리

주문이 배송되면 iOS, iPadOS 및 macOS 장치를 XenMobile Server 에 연결할 수 있습니다.

1. 관리자 또는 장치 등록 관리자 계정을 사용하여 [Apple Business Manager](#)에 로그인합니다.
2. 사이드바에서 장치를 클릭합니다. Apple 에서 직접 구입한 장치는 자동으로 표시됩니다. Apple Configurator 2 에서 Apple Business Manager 로 장치를 할당하려면 [Apple Business Manager 사용자 가이드](#)를 참조하십시오.
3. 목록에서 장치 또는 총 장치 수를 선택하고 장치 관리 편집을 클릭합니다. 다음 두 가지 옵션이 있습니다.
 - MDM 서버에 장치를 할당하려면 서버에 할당에서 XenMobile Server 의 이름을 선택합니다. **Continue(계속)** 를 클릭합니다.
새 장치를 Apple Business Manager 에 일괄 할당하려면 할당할 기본 XenMobile Server 를 설정합니다.
자세한 내용은 [일괄 등록을 위한 기본 서버 설정](#)을 참조하십시오.
 - XenMobile Server 에서 장치 할당을 취소하려면 할당 취소를 선택합니다.

이제 Apple 배포 프로그램 장치가 선택한 XenMobile Server 에 연결됩니다.

서비스를 받기 위해 iOS, iPadOS 또는 macOS 장치를 보낼 경우 Apple Business Manager 에서 장치를 제거해야 합니다. 서비스를 받은 장치를 다시 받으면 장치를 XenMobile Server 에 다시 할당해야 합니다. 장치를 교체할 때 주문 번호를 사용하여 XenMobile Server 에 새 장치를 할당할 수 있습니다.

할당된 장치의 기록을 검토하려면 다음 단계를 따르십시오.

1. 관리자 또는 장치 등록 관리자 계정을 사용하여 [Apple Business Manager](#)에 로그인합니다.
2. 사이드바에서 할당 내역을 클릭합니다. 그런 다음 할당을 선택하여 자세한 정보를 확인합니다.
3. 다운로드를 클릭하여 할당된 장치와 할당되지 않은 장치 모두의 일련 번호가 포함된 CSV 파일을 다운로드합니다.

장치를 판매했거나 도난당했거나 수리할 수 없는 경우 Apple Business Manager 에서 iOS, iPadOS, macOS 장치를 제거할 수 있습니다.

1. 관리자 또는 장치 등록 관리자 계정을 사용하여 [Apple Business Manager](#)에 로그인합니다.
2. 사이드바에서 장치를 클릭하고 장치를 검색합니다.
3. 장치를 선택하고 장치 해제를 클릭합니다. 대화 상자에서 변경 사항을 확인하여 프로그램에서 장치를 제거합니다. iOS 및 iPadOS 장치를 다시 추가하려면 Apple Configurator 2 를 사용합니다. Apple Configurator 2 를 사용하여 macOS 장치를 다시 추가할 수 없습니다.

장치 등록

March 15, 2024

사용자 장치를 원격으로 안전하게 관리하기 위해 사용자 장치를 XenMobile 에 등록합니다. XenMobile 클라이언트 소프트웨어가 사용자 장치에 설치되며 사용자의 ID 가 인증됩니다. 그런 다음 XenMobile 과 사용자 프로필이 설치됩니다. 다음으로, XenMobile 콘솔에서 장치 관리 작업을 수행할 수 있습니다. 정책을 적용하고, 앱을 배포하고, 장치에 데이터를 푸시하고, 분실 또는 도난된 장치를 잠그고 초기화하고 찾을 수 있습니다.

iOS, Android, Windows 10 및 Windows 11 장치에서 Azure Active Directory 등록이 지원됩니다. Azure 를 IdP(ID 공급자) 로 구성하는 방법에 대한 자세한 내용은 [Azure Active Directory 를 IdP 로 XenMobile 과 통합](#)을 참조하십시오.

참고:

iOS 장치 사용자를 등록하려면 APNs 인증서를 요청해야 합니다. 자세한 내용은 [인증서 및 인증](#)을 참조하십시오.

사용자 및 장치에 대한 구성 옵션을 업데이트하려면 관리 > 등록 초대 페이지로 이동합니다. 자세한 내용은 이 문서의 등록 초대 보내기를 참조하십시오.

Android 장치

참고:

Android Enterprise 장치 등록에 대한 자세한 내용은 [Android Enterprise](#)를 참조하십시오.

1. Android 장치의 Google Play 스토어로 이동하여 Citrix Secure Hub 앱을 다운로드한 후 이 앱을 누릅니다.
2. 앱을 설치할 것인지 묻는 메시지가 나타나면 다음을 클릭한 후 설치를 클릭합니다.
3. Secure Hub 가 설치된 후에 **Open(열기)** 을 누릅니다.
4. XenMobile Server 이름, UPN(사용자 계정 이름) 또는 전자 메일 주소와 같은 회사 자격 증명을 입력합니다. 그리고 **Next(다음)** 를 클릭합니다.
5. **Activate device administrator(장치 관리자 활성화)** 화면에서 **Activate(활성화)** 를 누릅니다.
6. 회사 암호를 입력한 다음 **Sign On(로그온)** 을 누릅니다.
7. XenMobile 이 구성된 방식에 따라 Citrix PIN 을 생성하라는 메시지가 나타날 수 있습니다. PIN 을 사용하여 Secure Hub 및 Secure Mail 과 Citrix Files 등의 다른 XenMobile 사용 앱에 로그인할 수 있습니다. Citrix PIN 을 두 번 입력합니다. **Create Citrix PIN(Citrix PIN 만들기)** 화면에서 PIN 을 입력합니다.
8. PIN 을 다시 입력합니다. Secure Hub 가 열립니다. 이제 XenMobile Store 에 액세스하여 Android 장치에 설치할 수 있는 앱을 볼 수 있습니다.
9. 등록 후 앱을 장치에 자동으 푸시하도록 XenMobile 을 구성한 경우 사용자에게 앱을 설치하라는 메시지가 나타납니다. 또한 XenMobile 에서 구성된 정책이 장치에 배포됩니다. 설치를 눌러 앱을 설치합니다.

Android 장치를 등록 취소하고 다시 등록하려면

사용자가 Secure Hub 내에서 등록을 취소할 수 있습니다. 사용자가 다음 절차를 사용하여 등록을 취소하는 경우 XenMobile 콘솔의 장치 인벤토리에 장치가 계속 나타납니다. 하지만 장치에 대한 작업을 수행할 수 없습니다. 장치를 추적하고 장치 규정 준수 여부를 모니터링할 수 없습니다.

1. Secure Hub 앱을 눌러서 엽니다.
2. 휴대폰인지 태블릿인지에 따라 다음 절차를 수행합니다.

휴대폰에서:

- 화면 왼쪽에서 살짝 밀어 설정 창을 엽니다.
- **Preferences**(기본 설정), **Accounts**(계정), **Delete Account**(계정 삭제) 를 차례로 누릅니다.

태블릿에서:

- 오른쪽 맨 위의 전자 메일 주소 옆에 있는 화살표를 누릅니다.
- **Preferences**(기본 설정), **Accounts**(계정), **Delete Account**(계정 삭제) 를 차례로 누릅니다.

3. **Re-Enroll**(재등록) 을 누릅니다. 장치를 재등록할 것인지 확인하는 메시지가 표시됩니다.
4. 확인을 누릅니다.

장치가 등록 취소됩니다.

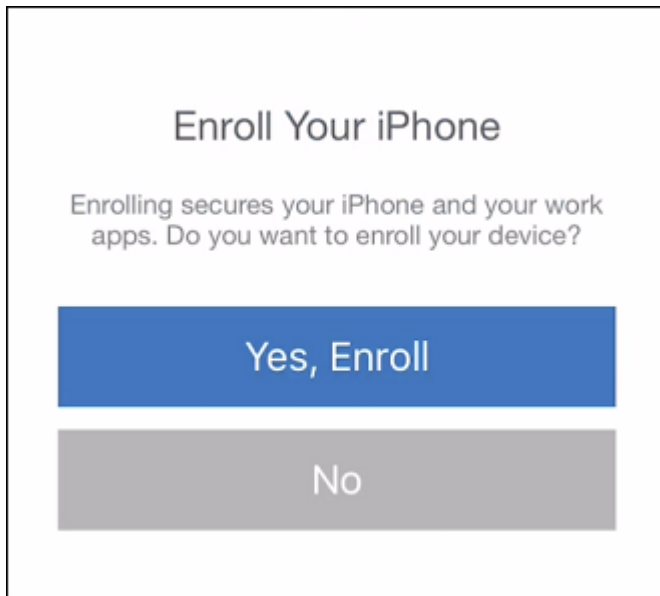
5. 화면의 지침에 따라 장치를 다시 등록합니다.

iOS 장치 등록

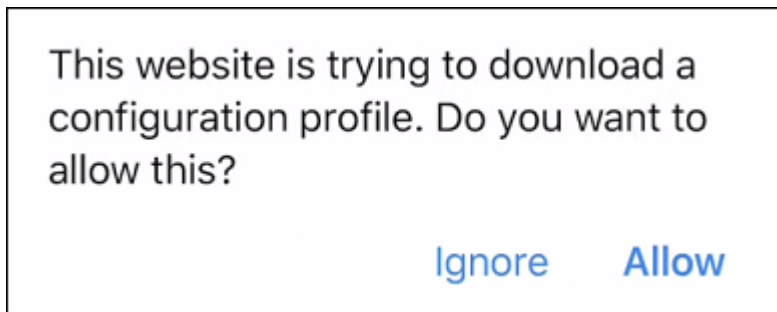
이 섹션에서는 사용자가 iOS 장치 (12.2 이상) 를 XenMobile Server 에 등록하는 방법을 보여 줍니다. iOS 등록에 대한 자세한 내용을 보려면 다음 비디오를 여십시오.



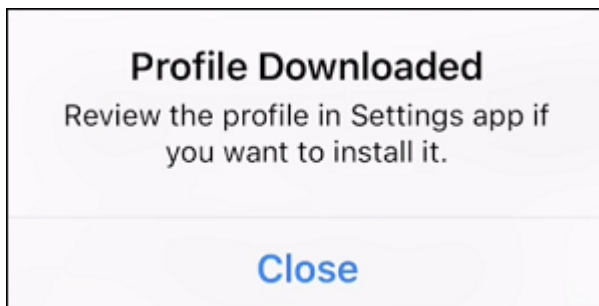
1. iOS 장치의 Apple Store 로 이동하여 Citrix Secure Hub 앱을 다운로드한 후 이 앱을 누릅니다.
2. 앱을 설치하라는 메시지가 표시되면 다음을 누른 후 설치를 누릅니다.
3. Secure Hub 가 설치된 후에 **Open(열기)** 을 누릅니다.
4. XenMobile Server 이름, UPN(사용자 계정 이름) 또는 전자 메일 주소와 같은 회사 자격 증명을 입력합니다. 그리고 **Next(다음)** 를 클릭합니다.
5. 예, 등록을 눌러 iOS 장치를 등록합니다.



6. 자격 증명을 입력한 후 메시지가 표시되면 허용을 눌러 구성 프로필을 다운로드합니다.

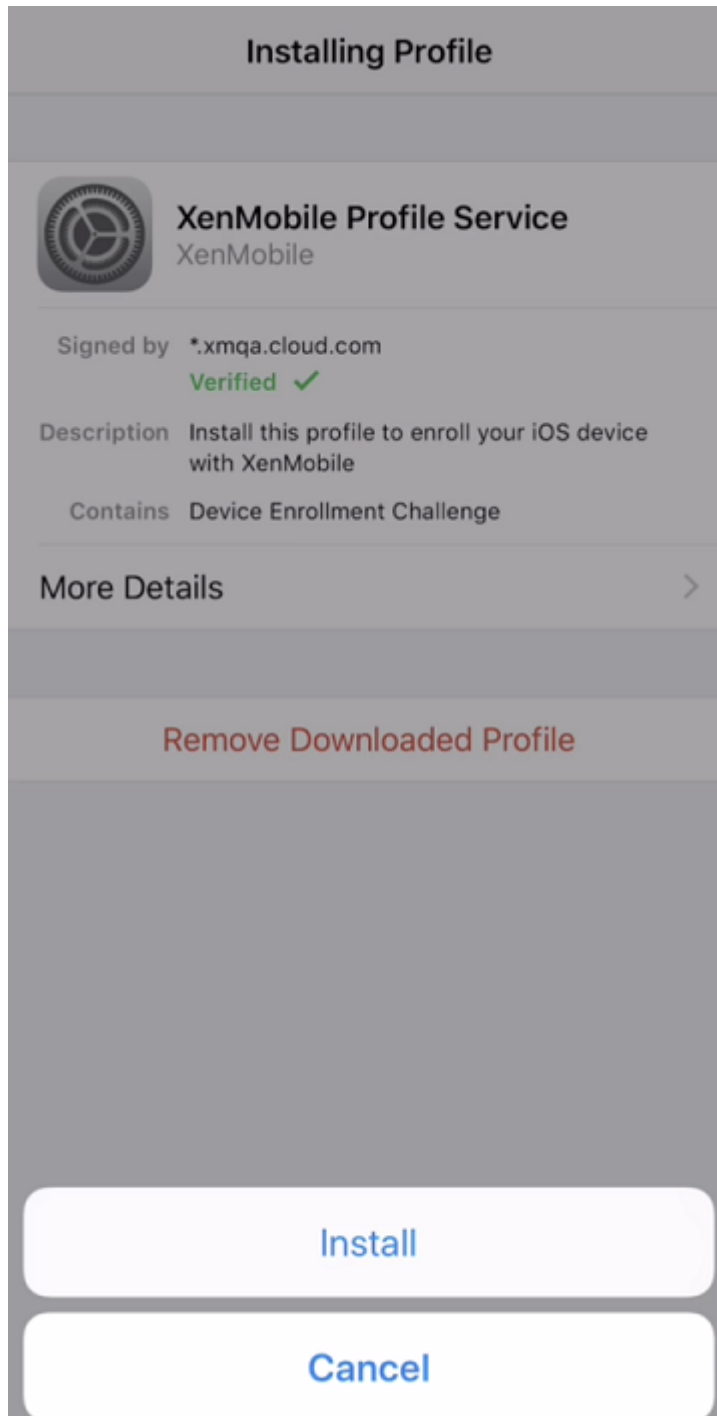


7. 구성 프로필을 다운로드한 후 닫기를 누릅니다.

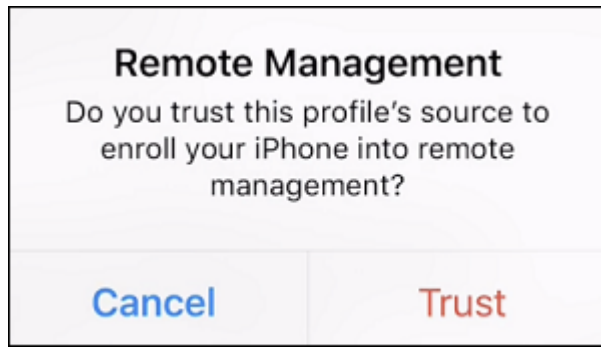


8. 장치 설정에서 iOS 인증서를 설치하고 장치를 신뢰할 수 있는 목록에 추가합니다.

- 설정 > 일반 > 프로필 > **XenMobile** 프로필 서비스로 이동하고 설치를 눌러 프로필을 추가합니다.



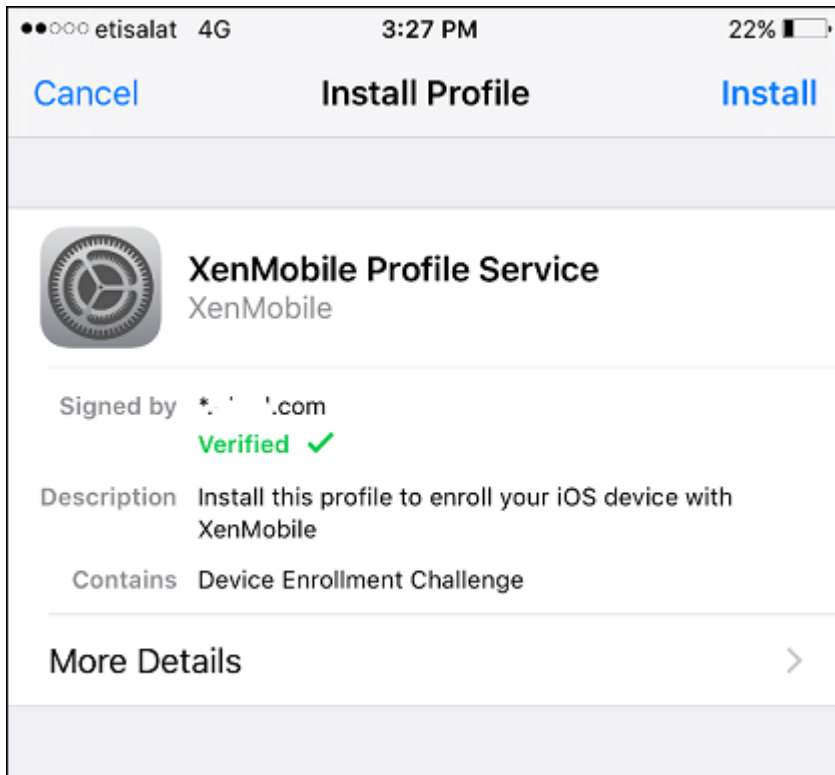
- 알림 창에서 신뢰를 눌러 장치를 원격 관리에 등록합니다.



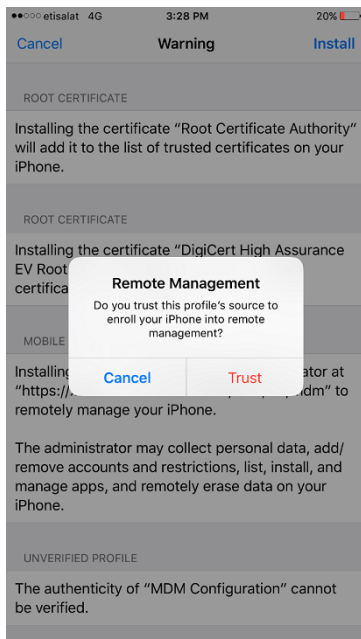
9. Secure Hub 에 로그인합니다. MDM+MAM 에 등록하는 경우: 자격 증명의 유효성이 확인된 후 메시지가 표시되면 Citrix PIN 을 만들고 확인합니다.
10. 워크플로가 완료되면 장치가 등록됩니다. 이제 App Store 에 액세스하여 iOS 장치에 설치할 수 있는 앱을 볼 수 있습니다.

iOS 장치

1. 장치에서 Apple iTunes App Store 로부터 Secure Hub 앱을 다운로드한 후 앱을 설치합니다.
2. iOS 장치의 홈 화면에서 Secure Hub 앱을 누릅니다.
3. Secure Hub 앱이 열리면 지원 센터에서 제공한 서버 주소를 입력합니다.
XenMobile 의 구성 방식에 따라 이러한 예와 다른 화면이 표시될 수 있습니다.
4. 메시지가 표시되면 사용자 이름과 암호 또는 PIN 을 입력합니다. 다음을 클릭합니다.
5. 등록하라는 메시지가 표시되면 **Yes, Enroll**(예, 등록) 을 클릭하고 메시지가 표시되면 자격 증명을 입력합니다.
6. 설치를 눌러 Citrix Profile Services 를 설치합니다.



7. 신뢰를 누릅니다.



8. 열기를 누르고 자격 증명을 입력합니다.

macOS 장치

XenMobile에서는 macOS를 실행하는 장치를 등록하는 두 가지 방법을 제공합니다. 두 방법 모두 macOS 사용자가 장치에서 직접 온라인으로 등록할 수 있습니다.

- 사용자에게 등록 초대 보내기: 이 등록 방법을 이용하면 macOS 장치에 대해 다음 등록 모드를 설정할 수 있습니다.
 - 사용자 이름 + 암호
 - 사용자 이름 + PIN
 - 2 단계

사용자가 등록 초대의 지침을 따르면 사용자 이름이 입력된 로그인 화면이 표시됩니다.

- 사용자에게 설치 링크 보내기: macOS 장치를 등록하는 이 방법은 사용자에게 등록 링크를 보냅니다. 사용자는 이 링크를 Safari 또는 Chrome 브라우저에서 열 수 있습니다. 그런 다음 사용자 이름과 암호를 제공하여 등록합니다.

서버 속성인 **Enable macOS OTAE**를 **false**로 설정하여 macOS 장치에 대한 등록 링크를 사용하지 못하도록 할 수 있습니다. 이렇게 하면 macOS 사용자가 등록 초대만 사용하여 등록할 수 있습니다.

사용자에게 등록 초대 보내기

1. 필요에 따라 XenMobile 콘솔에서 macOS 장치 정책을 설정합니다. 장치 정책에 대한 자세한 내용은 [장치 정책](#)을 참조하십시오.
2. macOS 사용자 등록을 위한 초대를 추가합니다. 자세한 내용은 이 문서에서 사용자에게 등록 초대 보내기를 참조하십시오.
3. 사용자가 초대를 수신하고 링크를 클릭하면 다음 화면이 Safari 브라우저에 표시됩니다. XenMobile이 사용자 이름을 채웁니다. 등록 보안 모드를 **2** 단계로 선택한 경우 다른 필드가 나타납니다.

4. 사용자는 필요에 따라 인증서를 설치합니다. 사용자에게 인증서를 설치할 것인지 묻는 메시지가 표시되는지 여부는 macOS에 대해 공개적으로 신뢰할 수 있는 SSL 인증서와 공개적으로 신뢰할 수 있는 디지털 서명 인증서를 구성했는지 여부에 따라 달라집니다. 인증서에 대한 자세한 내용은 [인증서 및 인증](#)을 참조하십시오.
5. 사용자가 요청된 자격 증명을 제공합니다.

Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하듯이 XenMobile로 Mac을 관리할 수 있습니다.

사용자에게 설치 링크 보내기

1. 필요에 따라 XenMobile 콘솔에서 macOS 장치 정책을 설정합니다. 장치 정책에 대한 자세한 내용은 [장치 정책](#)을 참조하십시오.
2. Safari 또는 Chrome 브라우저에서 열 수 있는 등록 링크 (<https://serverFQDN:8443/instanceName/macos/otae>)를 사용자에게 보냅니다.
 - **serverFQDN**은 XenMobile을 실행하는 서버의 FQDN(정규화된 도메인 이름)입니다.
 - 기본 보안 포트는 포트 **8443**입니다. 다른 포트를 구성한 경우 8443 대신 해당 포트를 사용하십시오.
 - 주로 **zdm**으로 표시되는 **instanceName**은 서버 설치 중에 지정된 이름입니다.

설치 링크를 전송하는 방법에 대한 자세한 내용은 설치 링크를 보내려면을 참조하십시오.

3. 사용자는 필요에 따라 인증서를 설치합니다. iOS와 macOS에 대해 공개적으로 신뢰할 수 있는 SSL 인증서 및 디지털 서명 인증서를 구성한 경우 사용자에게 인증서를 설치하라는 메시지가 표시됩니다. 인증서에 대한 자세한 내용은 [인증서 및 인증](#)을 참조하십시오.
4. 사용자가 자신의 Mac에 로그인합니다.

Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하듯이 XenMobile로 Mac을 관리할 수 있습니다.

Windows 장치

Windows 10 및 Windows 11 장치는 페더레이션된 Active Directory 인증 수단으로 Azure 를 사용하여 등록됩니다. 다음 방법 중 하나로 Windows 10 및 Windows 11 장치를 Microsoft Azure AD 에 가입시킬 수 있습니다.

- 장치의 전원을 처음 켤 때 Azure AD 기본 가입의 일환으로 MDM 에 등록합니다.
- 장치를 구성한 다음 Windows 설정 페이지에서 Azure AD 가입의 일환으로 MDM 에 등록합니다.

XenMobile 에는 다음 Windows 운영 체제를 실행하는 장치를 등록할 수 있습니다.

- Windows 10
- Windows 11

사용자가 자신의 장치를 통해 직접 등록할 수 있습니다.

참고:

Windows 10 RS2 휴대폰 및 태블릿의 경우 재등록 시 사용자에게 서버 URL 을 입력하라는 메시지가 표시되지 않습니다. 이 문제를 해결하려면 장치를 다시 시작하십시오. 또는 전자 메일 주소 화면에서 서비스에 연결하는 중 맞은 편에 있는 X 를 눌러 서버 URL 페이지로 이동합니다. 이것은 타사 문제입니다.

관리자는 지원되는 Windows 장치를 관리할 수 있도록 사용자 등록에 대한 Windows 검색 서비스 및 자동 검색을 구성해야 합니다.

Windows 장치 사용자가 Azure 를 사용하여 등록할 수 있게 하려면 먼저 XenMobile 에서 Microsoft Azure 서버 설정을 구성해야 합니다. 자세한 내용은 [Microsoft Azure Active Directory 서버 설정](#)을 참조하십시오.

자체 검색을 사용하여 **Windows** 장치를 등록하려면

Windows 장치 관리를 사용하려면 자동 검색 서비스 및 Windows 검색 서비스를 구성하는 것이 좋습니다. 자세한 내용은 [XenMobile 자동 검색 서비스](#)를 참조하십시오.

1. 장치에서 사용 가능한 모든 Windows 업데이트를 확인하고 설치합니다.
2. 참 메뉴에서 설정을 누른 후에 계정 > 회사 또는 학교 액세스 > 회사 또는 학교에 연결을 누릅니다.
3. Windows 10 및 Windows 11 의 경우: 회사 이메일 주소를 입력한 다음 계속을 탭합니다. Windows 8.1 의 경우: 장치 관리 사용을 탭합니다. 로컬 사용자로 등록하려면 올바른 도메인 이름을 사용하여 존재하지 않는 전자 메일 주소를 입력합니다 (예: [foo@mydomain.com](#)). 이를 통해 Windows 의 기본 제공 장치 관리를 통해 등록이 수행되는 알려진 Microsoft 제한 사항을 바이패스할 수 있습니다. 서비스에 연결 중 대화 상자에서 로컬 사용자와 연결된 사용자 이름 및 암호를 입력합니다. 장치에서 XenMobile Server 가 자동으로 검색되고 등록 프로세스가 시작됩니다.
4. 암호를 입력합니다. XenMobile 의 사용자 그룹에 속하는 계정과 연결된 암호를 사용합니다.
5. Windows 10 및 Windows 11 의 경우: 사용 약관 대화 상자에서 장치가 관리되는 것에 동의함을 나타내고 동의를 누릅니다. Windows 8.1 의 경우: **IT** 관리자의 앱 및 서비스 허용 대화 상자에서 장치가 관리되는 것에 동의함을 나타내고 여기를 누릅니다.

자체 검색을 사용하지 않고 **Windows** 장치를 등록하려면

자동 검색을 사용하지 않고 Windows 장치를 등록할 수 있습니다. 그러나 자동 검색을 구성하는 것이 좋습니다. 자동 검색을 사용하지 않고 등록하면 원하는 URL에 연결하기 전에 포트 80이 호출됩니다. 따라서 이는 프로덕션 배포를 위한 최선의 방법으로 간주되지 않습니다. 이 프로세스는 테스트 환경과 POC 배포에서만 사용하는 것이 좋습니다.

1. 장치에서 사용 가능한 모든 Windows 업데이트를 확인하고 설치합니다.
2. Windows 10 및 Windows 11의 경우: 참 메뉴에서 설정을 누른 후에 계정 > 회사 또는 학교 액세스 > 회사 또는 학교에 연결을 누릅니다. Windows 8.1의 경우: **PC** 설정 > 네트워크 > 회사를 누릅니다.
3. 회사 전자 메일 주소를 입력합니다.
4. Windows 10 및 Windows 11의 경우: 자동 검색이 구성되지 않은 경우 5 단계에 설명된 대로 서버 세부 정보를 입력할 수 있는 옵션이 표시됩니다. Windows 8.1의 경우: 자동으로 서버 주소 검색이 켜짐으로 설정된 경우 꺼짐 옵션을 눌러서 설정합니다.
5. Windows 10 및 Windows 11의 경우: 서버 주소 입력 필드에 <https://serverfqdn:8443/serverInstance/wpe> 주소를 입력합니다.
8443 이외의 포트가 인증되지 않은 SSL 연결에 사용된 경우 이 주소에서 8443 대신 해당 포트 번호를 사용합니다.
Windows 8.1의 경우: <https://serverfqdn:8443/serverInstance/Discovery.svc> 형식으로 서버 주소를 입력합니다.
8443 이외의 포트가 인증되지 않은 SSL 연결에 사용된 경우 이 주소에서 8443 대신 해당 포트 번호를 사용합니다.
6. 암호를 입력합니다.
7. Windows 10 및 Windows 11의 경우: 사용 약관 대화 상자에서 장치가 관리되는 것에 동의함을 나타내고 동의를 누릅니다. Windows 8.1의 경우: **IT** 관리자의 앱 및 서비스 허용 대화 상자에서 장치가 관리되는 것에 동의함을 나타내고 켜기를 누릅니다.

등록 초대 보내기

XenMobile 콘솔에서 iOS, macOS, Android Enterprise 및 레거시 Android 장치 사용자에게 등록 초대를 보낼 수 있습니다. 또한 iOS, Android Enterprise 또는 레거시 Android 장치 사용자에게 설치 링크도 보낼 수 있습니다.

등록 초대는 다음과 같이 보냅니다.

- 한 명의 로컬 사용자 또는 Active Directory 사용자에게 등록 초대를 보내는 경우: 지정한 휴대폰 번호 및 통신 회사 이름의 SMS를 통해 사용자에게 초대가 발송됩니다.
- 그룹에 대한 등록 초대인 경우: 사용자에게 SMS로 초대가 발송됩니다. Active Directory 사용자에게 Active Directory의 전자 메일 주소 및 휴대폰 번호가 있는 경우 해당 사용자는 초대를 받습니다. 로컬 사용자는 사용자 속성에 지정된 전자 메일 및 전화 번호로 초대를 받습니다.

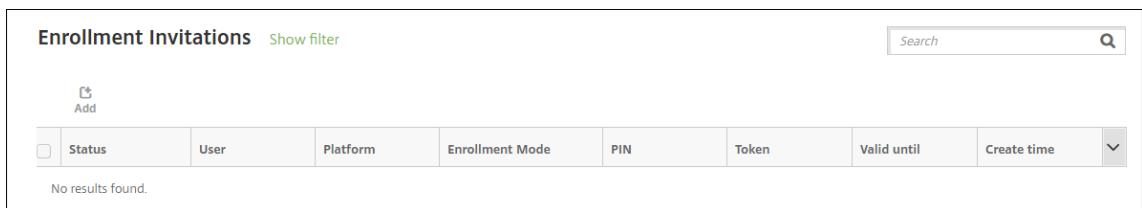
사용자가 등록하면 해당 사용자의 장치는 관리 > 장치에 관리되는 장치로 표시됩니다. 초대 URL의 상태는 상환됨으로 표시됩니다.

사전 요구 사항

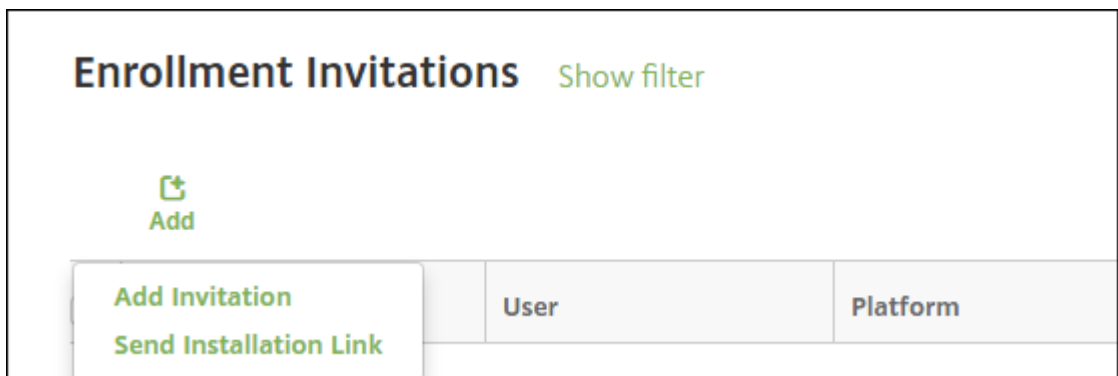
- 엔터프라이즈 (XME) 또는 MDM 모드로 구성된 XenMobile Server
- 구성된 LDAP
- 로컬 그룹 및 로컬 사용자를 사용 중인 경우:
 - 하나 이상의 로컬 그룹.
 - 로컬 그룹에 할당된 로컬 사용자.
 - 배달 그룹은 로컬 그룹과 연결됩니다.
- Active Directory 를 사용 중인 경우:
 - 배달 그룹은 Active Directory 그룹과 연결됩니다.

등록 초대 만들기

1. XenMobile 콘솔에서 관리 > 등록 초대를 클릭합니다. 등록 초대 페이지가 나타납니다.



2. 추가를 클릭합니다. 등록 옵션 메뉴가 나타납니다.



- 사용자 또는 그룹에 등록 초대를 보내려면 초대 추가를 클릭합니다.
- SMTP 또는 SMS 를 통해 받는 사람 목록에 등록 설치 링크를 보내려면 설치 링크 보내기를 클릭합니다.

이후 단계에서는 등록 초대 및 설치 링크 보내기에 대해 설명합니다.

3. 초대 추가를 클릭합니다. 등록 초대 화면이 나타납니다.

Add Invitation	Enrollment Invitation
1 Enrollment Invitation	<p>Recipient* <input type="text" value="Select a recipient type"/></p> <p>Select a platform* <input type="checkbox"/> Android <input type="checkbox"/> iOS <input type="checkbox"/> macOS</p> <p>Device ownership <input type="text" value="Select an ownership type"/></p>

4. 다음 설정을 구성합니다.

- 받는 사람: 그룹 또는 사용자를 선택합니다.
- 플랫폼 선택: 받는 사람이 그룹인 경우 모든 플랫폼이 선택됩니다. 플랫폼 선택은 변경할 수 있습니다. 받는 사람이 사용자인 경우 플랫폼이 선택되지 않습니다. 플랫폼을 선택합니다.

Android Enterprise 장치에 대한 등록 초대를 만들려면 **Android > Android Enterprise** 를 선택합니다.

- 장치 소유권: 회사 또는 직원을 선택합니다.

사용자 또는 그룹에 대한 설정이 나타납니다. 다음 섹션에서 이에 대해 설명합니다.

사용자에게 등록 초대를 보내려면

Add Invitation	Enrollment Invitation
1 Enrollment Invitation	<p>Recipient* <input type="text" value="User"/></p> <p>Select a platform* <input type="checkbox"/> Android <input type="checkbox"/> iOS <input type="checkbox"/> macOS</p> <p>Device ownership <input type="text" value="Select an ownership type"/></p> <p>User name* <input type="text"/> ?</p> <p>Enrollment mode* <input type="text" value="User name + Password"/></p> <p>Template for agent download <input type="text" value="Select a template"/></p> <p>Template for enrollment URL <input type="text" value="Select a template"/></p> <p>Template for enrollment confirmation <input type="text" value="Select a template"/></p> <p>Expire after <input type="text" value="Never"/></p> <p>Maximum Attempts <input type="text" value="0"/></p> <p>Send invitation <input type="button" value="OFF"/></p>

1. 다음 사용자 설정을 구성합니다.

- **사용자 이름:** 사용자 이름을 입력합니다. 사용자는 Active Directory의 사용자 또는 로컬 사용자로 XenMobile Server에 있어야 합니다. 로컬 사용자인 경우 사용자에게 알림을 보낼 수 있도록 사용자의 전자 메일 속성이 설정되어 있는지 확인하십시오. Active Directory 사용자인 경우 LDAP가 구성되어 있는지 확인합니다.
- **장치 정보:** 여러 플랫폼을 선택하거나 macOS만 선택한 경우에는 이 설정이 나타나지 않습니다. 일련 번호, **UDID** 또는 **IMEI**를 선택합니다. 옵션을 선택하면 장치에 대한 해당 값을 입력할 수 있는 필드가 표시됩니다.
- **전화 번호:** 여러 플랫폼을 선택하거나 macOS만 선택한 경우에는 이 설정이 나타나지 않습니다. 필요에 따라 사용자의 전화 번호를 입력합니다.
- **통신 회사:** 여러 플랫폼을 선택하거나 macOS만 선택한 경우에는 이 설정이 나타나지 않습니다. 사용자의 전화 번호에 연결할 통신 회사를 선택합니다.
- **등록 모드:** 사용자의 등록 보안 모드를 선택합니다. 기본값은 사용자 이름 + 암호입니다. 일부 플랫폼에서는 다음 옵션 중 일부를 사용할 수 없습니다.
 - 사용자 이름 + 암호
 - 높은 수준의 보안
 - 초대 URL
 - 초대 URL + PIN
 - 초대 URL + 암호
 - 2 단계
 - 사용자 이름 + PIN

등록 초대를 보내기 위해서는 초대 **URL**, 초대 **URL + PIN** 또는 초대 **URL + 암호** 등록 보안 모드만 사용할 수 있습니다. 사용자 이름 + 암호, 2 단계 또는 사용자 이름 + PIN으로 등록하는 장치의 경우 사용자는 Secure Hub에서 자격 증명을 수동으로 입력해야 합니다.

등록용 PIN을 일회용 PIN이라고도 합니다. 이러한 PIN은 사용자가 등록할 때만 유효합니다.

참고:

PIN이 포함된 등록 보안 모드를 선택하면 등록 **PIN**용 템플릿 필드가 나타납니다. 여기서 등록 **PIN**을 클릭합니다.

- **에이전트 다운로드용 템플릿:** 다운로드 링크라는 이름의 다운로드 링크 템플릿을 선택합니다. 이 템플릿은 지원되는 모든 플랫폼용 템플릿입니다.
- **등록 URL용 템플릿:** 등록 초대를 선택합니다.
- **등록 확인용 템플릿:** 등록 확인을 선택합니다.
- **다음 이후에 만료:** 이 필드는 등록 모드를 구성한 경우 설정되며 등록이 만료되는 시기를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 [등록 보안 모드 구성](#)을 참조하십시오.
- **최대 시도 횟수:** 이 필드는 등록 모드를 구성할 때 설정되며 등록 프로세스가 진행되는 최대 횟수를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 [등록 보안 모드 구성](#)을 참조하십시오.
- **초대 보내기:** 초대를 즉시 보내려면 커짐을 선택합니다. 초대를 등록 초대 페이지의 테이블에 추가되지 보내지 않으려면 꺼짐을 선택합니다.

2. 초대 보내기를 사용하도록 설정한 경우 저장 및 보내기를 클릭합니다. 그렇지 않은 경우 저장을 클릭합니다. 등록 초대 페이지의 테이블에 초대가 표시됩니다.

Enrollment Invitations									
<div> Add Export </div> <div> <div>Search</div> <div>Q</div> </div>									
<input type="checkbox"/>	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time	▼
<input type="checkbox"/>	PENDING		Android	User name + Password				05/03/2017 10:32:24 am	
<input type="checkbox"/>	PENDING		macOS	User name + Password				05/01/2017 07:33:38 pm	
<input type="checkbox"/>	PENDING		iOS	User name + Password				05/01/2017 07:29:02 pm	

그룹에 등록 초대를 보내려면

다음 그림에서는 그룹에 대한 등록 초대를 구성하기 위한 설정을 보여 줍니다.

Add Invitation

1 Enrollment Invitation

Enrollment Invitation

Recipient*

Group

Select a platform*

☒ Android
 ☒ iOS
 ☒ macOS

Device ownership

Select an ownership type

Domain*

Select a domain

Group*

Select a group

Enrollment mode*

User name + Password

Template for agent download

Select a template

Template for enrollment URL

Select a template

Template for enrollment confirmation

Select a template

Expire after

Never

Maximum Attempts

0

Send invitation

OFF

1. 다음 설정을 구성합니다.

- **도메인:** 초대를 받을 그룹의 도메인을 선택합니다.
- **그룹:** 초대를 받을 그룹을 선택합니다.

- **등록 모드:** 그룹의 사용자를 등록할 방식을 선택합니다. 기본값은 사용자 이름 + 암호입니다. 일부 플랫폼에서는 다음 옵션 중 일부를 사용할 수 없습니다.

- 사용자 이름 + 암호
- 높은 수준의 보안
- 초대 URL
- 초대 URL + PIN
- 초대 URL + 암호
- 2 단계
- 사용자 이름 + PIN

등록 초대를 보내기 위해서는 초대 **URL**, 초대 **URL + PIN** 또는 초대 **URL + 암호** 등록 보안 모드만 사용할 수 있습니다. 사용자 이름 + 암호, **2 단계** 또는 사용자 이름 + **PIN** 으로 등록하는 장치의 경우 사용자는 Secure Hub 에서 자격 증명을 수동으로 입력해야 합니다.

선택한 각 플랫폼에 유효한 등록 보안 모드만 표시됩니다.

참고:

PIN 이 포함된 등록 보안 모드를 선택하면 등록 **PIN** 용 템플릿 필드가 나타납니다. 여기서 등록 **PIN** 을 클릭합니다.

- **에이전트 다운로드용 템플릿:** 다운로드 링크: 라는 이름의 다운로드 링크 템플릿을 선택합니다. 이 템플릿은 지원되는 모든 플랫폼용 템플릿입니다.
- **등록 URL 용 템플릿:** 등록 초대를 선택합니다.
- **등록 확인용 템플릿:** 등록 확인을 선택합니다.
- **다음 이후에 만료:** 이 필드는 등록 모드를 구성한 경우 설정되며 등록이 만료되는 시기를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 [등록 보안 모드 구성](#)을 참조하십시오.
- **최대 시도 횟수:** 이 필드는 등록 모드를 구성할 때 설정되며 등록 프로세스가 진행되는 최대 횟수를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 [등록 보안 모드 구성](#)을 참조하십시오.
- **초대 보내기:** 초대를 즉시 보내려면 커짐을 선택합니다. 초대를 등록 초대 페이지의 테이블에 추가하되 보내지 않으려면 꺼짐을 선택합니다.

2. 초대 보내기를 사용하도록 설정한 경우 저장 및 보내기를 클릭합니다. 그렇지 않은 경우 저장을 클릭합니다. 등록 초대 페이지의 테이블에 초대가 표시됩니다.

Devices										
Users										
Enrollment Invitations										
Devices Show filter										
<div> <div>Search</div> </div>										
<div> <div>Add</div> <div>Import</div> <div>Export</div> <div>Refresh</div> </div>										
<input type="checkbox"/>	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name
<input type="checkbox"/>		MDM MAM			iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account
<input type="checkbox"/>		MDM MAM			iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days	
<input type="checkbox"/>		MDM MAM			iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days	
Showing 1 - 3 of 3 items Items per page: <div>10</div>										

설치 링크를 보내려면

등록 설치 링크를 보내기 전에 설정 페이지에서 알림 서버의 채널 (SMTP 또는 SMS) 을 구성해야 합니다. 자세한 내용은 [알림](#)을 참조하십시오.

Send Link	Send Installation Link		
1 Details	<div>Recipients *</div> <div>Email * Phone number * Add</div>		
	<div>Channels ⓘ</div> <div> <div> <div>✉ SMTP</div> <div>⚠ Channel cannot be activated until you define the SMTP server in the Notification Server section in Settings.</div> <div>Sender</div> <div>Subject</div> <div>Message</div> </div> <div> <div>☎ SMS</div> <div>⚠ Channel cannot be activated until you define the SMS server in the Notification Server section in Settings.</div> <div>Message</div> </div> </div>		

1. 다음 설정을 구성한 후 저장을 클릭합니다.

- 받는 사람: 추가하려는 각 받는 사람에 대해 추가를 클릭한 후 다음 작업을 수행합니다.
 - 전자 메일: 받는 사람의 전자 메일 주소를 입력합니다. 이것은 필수 필드입니다.
 - 전화 번호: 받는 사람의 전화 번호를 입력합니다. 이것은 필수 필드입니다.

참고:

기존의 받는 사람을 삭제하려면 목록이 포함된 줄 위로 마우스 포인터를 이동한 후 오른쪽의 휴지통 아이콘을 클릭합니다. 확인 대화 상자가 나타납니다. 삭제를 클릭하여 목록을 삭제하거나 취소를 클릭하여 목록을 유지합니다.

기존의 받는 사람을 편집하려면 목록이 포함된 줄 위로 마우스 포인터를 이동한 후 오른쪽의 펜 아이콘을 클릭합니다. 목록을 업데이트한 후 저장을 클릭하여 변경된 목록을 저장하거나 취소를 클릭하여 목록을 변경되지 않은 상태로 유지합니다.

- 채널: 등록 설치 링크를 보내는 데 사용할 채널을 선택합니다. **SMTP** 또는 **SMS** 를 통해 알림을 보낼 수 있습니다. 설정 페이지의 알림 서버에서 서버 설정을 구성할 때까지 이러한 채널을 활성화할 수 없습니다. 자세한 내용은 [알림](#)을 참조하십시오.
- SMTP:** 다음과 같은 선택적 설정을 구성합니다. 이러한 필드에 아무것도 입력하지 않으면 선택한 플랫폼에 구성된 알림 템플릿에 지정되어 있는 기본값이 사용됩니다.
 - 보낸 사람: 선택적 보낸 사람을 입력합니다.
 - 제목: 선택적 메시지 제목을 입력합니다. 예를 들어, “장치를 등록하십시오.” 를 사용할 수 있습니다.

- 메시지: 받는 사람에게 보낼 선택적인 메시지를 입력합니다. 예를 들어 “조직의 앱과 전자 메일에 대한 액세스 권한을 얻으려면 장치를 등록하십시오.” 를 사용할 수 있습니다.
- **SMS:** 다음 설정을 구성합니다. 이 필드에 아무것도 입력하지 않으면 선택한 플랫폼에 구성된 알림 템플릿에 지정되어 있는 기본값이 사용됩니다.
 - 메시지: 받는 사람에게 보낼 메시지를 입력합니다. 이 필드는 SMS 기반 알림에 필요합니다.

참고: 북미 지역의 경우 160 자를 초과하는 SMS 메시지는 여러 메시지로 배달됩니다.

2. 보내기를 클릭합니다.

참고:

해당 환경에서 sAMAccountName 을 사용하는 경우 초대를 받고 링크를 클릭한 사용자가 사용자 이름을 편집해야 인증이 완료됩니다. 사용자 이름은 sAMAccountName@domainname.com의 형식으로 표시됩니다. 사용자는 @domainname.com 부분을 제거해야 합니다.

플랫폼별 등록 보안 모드

다음 표에는 사용자 장치를 등록하는 데 사용할 수 있는 보안 모드가 나와 있습니다. 표에서 예는 등록 프로필이 다른 특정 등록 및 관리 모드를 지원하는 장치 플랫폼을 나타냅니다.

MDM 등록 보안 모드	Citrix Gate-way의 MAM 등록 보안 모드		다양한 등록 프로파일 지원	Android(레Enterprise)		iOS(사용자 등록 모드)		macOS	Windows
	관리 모드	관리 모드							
Citrix Cloud를 통한 ID 공급자로서의 Azure AD 및 Okta	클라이언트 인증서	MDM+MAM 또는 MDM	예	예	예	예	예	아니요	아니요

Citrix Gate-way 의									
MDM 등 록 보안 모드	MAM 등 록 보안 모드	다양한 등 관리 모드 지원	Android(레 Enterprise)	iOS(사 용자 등록 모드)	iOS	macOS	Windows		
사용자 이 름 + 암호	LDAP, LDAP+ 클라이언 트 인증서 및 클라이 언트 인증 서만	MDM+MAM 또는 MAM(MAM 전용 모드 는 Citrix Gate- way 에 서 클라이 언트 인증 서를 지원 하지 않 음)	예	예	예	예	예	예	
초대 URL	클라이언 트 인증서	MDM+MAM 또는 MDM	예	예	아니요	예	아니요	아니요	
초대 URL + PIN	클라이언 트 인증서	MDM+MAM 또는 MDM	예	예	아니요	예	아니요	아니요	
초대 URL + 암호	LDAP, LDAP+ 클라이언 트 인증서 및 클라이 언트 인증 서만	MDM+MAM 또는 MDM	예	예	아니요	예	아니요	아니요	
2 단계 인 증 (사용 자 이름 + 암호 + PIN)	LDAP, LDAP+ 클라이언 트 인증서 및 클라이 언트 인증 서만	MDM+MAM 또는 MDM	예	예	아니요	예	예	아니요	

Citrix Gate-way 의									
MDM 등 록 보안 모드	MAM 등 록 보안 모드	다양한 등 관리 모드 지원	Android(레 거시)	Android(레 Enterprise)	iOS(사 용자 등록 모드)	iOS	macOS	Windows	
사용자 이 름 + PIN	클라이언 트 인증서	MDM+MAM예 또는 MDM	예	예	아니요	예	예	아니요	

다음은 iOS, Android 및 Android Enterprise 장치에서 등록 보안 모드가 작동하는 방식에 대해 설명합니다.

- **User name + 암호 (기본값)**
 - 사용자에게 등록 URL 이 포함된 단일 알림을 보냅니다. 사용자가 URL 을 클릭하면 Secure Hub 가 열립니다. 그런 다음 사용자가 사용자 이름과 암호를 입력하여 XenMobile 에 장치를 등록합니다.
- **초대 URL**
 - 사용자에게 등록 URL 이 포함된 단일 알림을 보냅니다. 사용자가 URL 을 클릭하면 Secure Hub 가 열립니다. XenMobile 서버 이름 및 예, 등록하겠습니다 단추가 나타납니다. 사용자가 예, 등록하겠습니다를 탭하여 XenMobile 에 장치를 등록합니다.
- **초대 URL + PIN**
 - 사용자에게 다음 전자 메일을 보냅니다.
 - * 등록 URL 이 포함된 전자 메일로, 여기에서 사용자는 Secure Hub 를 통해 XenMobile 에 장치를 등록할 수 있습니다.
 - * 전자 메일에는 장치를 등록할 때 사용자가 입력해야 하는 일회용 PIN 과 사용자의 Active Directory(또는 로컬) 암호가 포함되어 있습니다.
 - 이 모드에서는 사용자가 알림에 있는 등록 URL 을 사용해야만 등록할 수 있습니다. 사용자가 알림 초대장을 분실하면 등록할 수 없습니다. 하지만 다른 초대장을 보낼 수 있습니다.
- **초대 URL + 암호**
 - 사용자에게 등록 URL 이 포함된 단일 알림을 보냅니다. 사용자가 URL 을 클릭하면 Secure Hub 가 열립니다. 사용자가 암호를 입력할 수 있는 필드와 함께 XenMobile 서버 이름이 나타납니다.
- **2 단계**
 - 사용자에게 등록 URL 과 일회용 PIN 이 포함된 단일 알림을 보냅니다. 사용자가 URL 을 클릭하면 Secure Hub 가 열립니다. 사용자가 암호 및 PIN 번호를 입력할 수 있는 두 개의 필드와 함께 XenMobile 서버 이름이 나타납니다.
- **사용자 이름 + PIN**

- 사용자에게 다음 전자 메일을 보냅니다.
 - * 등록 URL 이 포함된 전자 메일로, 여기에서 사용자는 **Secure Hub** 를 다운로드하여 설치할 수 있습니다. **Secure Hub** 가 열리면 사용자 이름과 암호를 입력하여 XenMobile 에 장치를 등록하라는 메시지가 표시됩니다.
 - * 전자 메일에는 장치를 등록할 때 사용자가 입력해야 하는 일회용 PIN 과 사용자의 **Active Directory**(또는 로컬) 암호가 포함되어 있습니다.
- 사용자가 알림 초대를 분실하면 등록할 수 없습니다. 하지만 다른 초대장을 보낼 수 있습니다.

다음은 macOS 장치에서 등록 보안 모드가 작동하는 방식에 대해 설명합니다.

- 사용자 이름 + 암호
 - 사용자에게 등록 URL 이 포함된 단일 알림을 보냅니다. 사용자가 URL 을 클릭하면 Safari 브라우저가 열립니다. 로그인 페이지가 나타나고 XenMobile 에 장치를 등록하려면 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
- **2 단계**
 - 사용자에게 등록 URL 과 일회용 PIN 이 포함된 단일 알림을 보냅니다. 사용자가 URL 을 클릭하면 Safari 브라우저가 열립니다. 사용자가 암호와 PIN 번호를 입력할 수 있는 두 개의 필드가 표시된 로그인 페이지가 나타납니다.
- 사용자 이름 + **PIN**
 - 사용자에게 다음 전자 메일을 보냅니다.
 - * 등록 URL 이 포함된 전자 메일입니다. 사용자가 URL 을 클릭하면 Safari 브라우저가 열립니다. 로그인 페이지가 나타나고 XenMobile 에 장치를 등록하려면 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
 - * 전자 메일에는 장치를 등록할 때 사용자가 입력해야 하는 일회용 PIN 과 사용자의 **Active Directory**(또는 로컬) 암호가 포함되어 있습니다.
 - 사용자가 알림 초대를 분실하면 등록할 수 없습니다. 하지만 다른 초대장을 보낼 수 있습니다.

Windows 장치에는 등록 초대장을 보낼 수 없습니다. Windows 사용자는 장치를 통해 직접 등록할 수 있습니다.

Firebase Cloud Messaging

September 13, 2023

참고:

FCM(Firebase Cloud Messaging) 은 이전의 GCM(Google Cloud Messaging) 입니다. 일부 XenMobile 콘솔 레이블 및 메시지에는 GCM 용어가 사용됩니다.

FCM(Firebase Cloud Messaging) 을 사용하여 Android 장치의 XenMobile 연결 방법 및 시기를 제어하는 것이 좋습니다. FCM 에 구성된 XenMobile 은 FCM 을 사용하도록 설정된 Android 장치에 연결 알림을 전송합니다. 모든 보안 동작 또는 배포 명령이 실행되면 사용자에게 XenMobile 서버에 다시 연결하라는 메시지를 표시하는 푸시 알림이 트리거됩니다.

이 문서의 구성 단계를 완료하고 장치를 체크인하면 장치가 XenMobile Server 의 FCM 서비스에 등록됩니다. 이 연결은 FCM 을 사용하여 XenMobile Service 에서 장치로 거의 실시간 통신을 가능하게 합니다. FCM 등록은 새로운 장치 등록 및 이전에 등록된 장치에서 작동합니다.

장치에 대한 연결을 시작해야 하는 XenMobile 이 FCM 서비스에 연결하면 FCM 서비스가 연결 알림을 장치에 제공합니다. 이 유형의 연결은 Apple 이 푸시 알림 서비스에 사용하는 연결과 유사합니다.

사전 요구 사항

- 최신 Secure Hub 클라이언트
- Google 개발자 계정 자격 증명
- FCM 지원 Android 장치에 설치된 Google Play 서비스

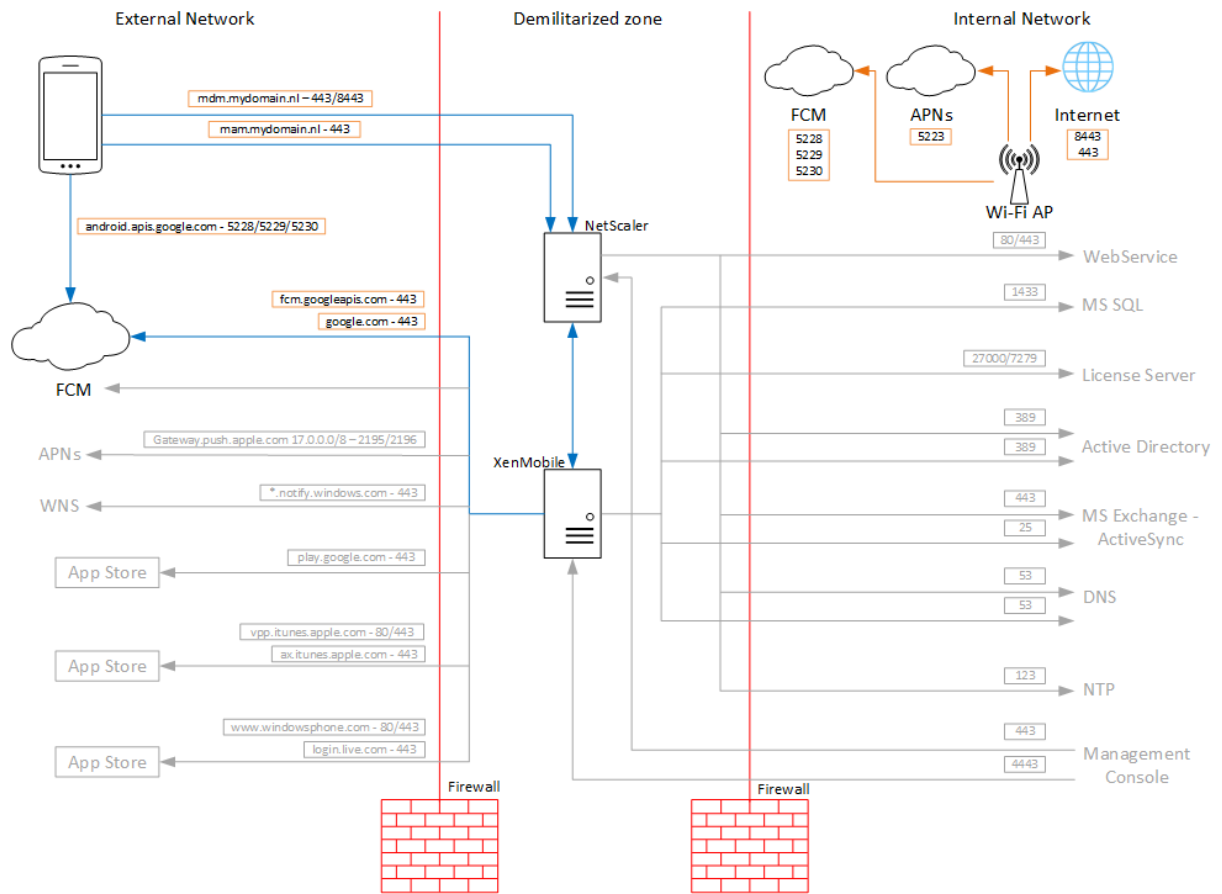
방화벽 포트

- XenMobile 에서 fcm.googleapis.com 및 [Google.com](https://google.com)에 대해 포트 443 을 엽니다.
- 장치 Wi-Fi 에서 나가는 인터넷 통신을 위해 포트 5228, 5229 및 5230 을 엽니다.
- 나가는 연결을 허용하려면 IP 제한 없이 포트 5228~5230 을 허용하는 것이 좋습니다. IP 제한이 필요한 경우에는 IPv4 및 IPv6 블록의 모든 IP 주소를 허용하는 것이 좋습니다. 이러한 블록은 [Google ASN of 15169](#)에 나와 있습니다. 해당 목록을 매월 업데이트하십시오. FCM 포트에 대한 자세한 내용은 [FCM 포트](#)에 대한 Google 설명서를 참조하십시오.

자세한 내용은 [포트 요구 사항](#)을 참조하십시오.

아키텍처

이 다이어그램은 외부 및 내부 네트워크의 FCM 에 대한 통신 흐름을 보여 줍니다.

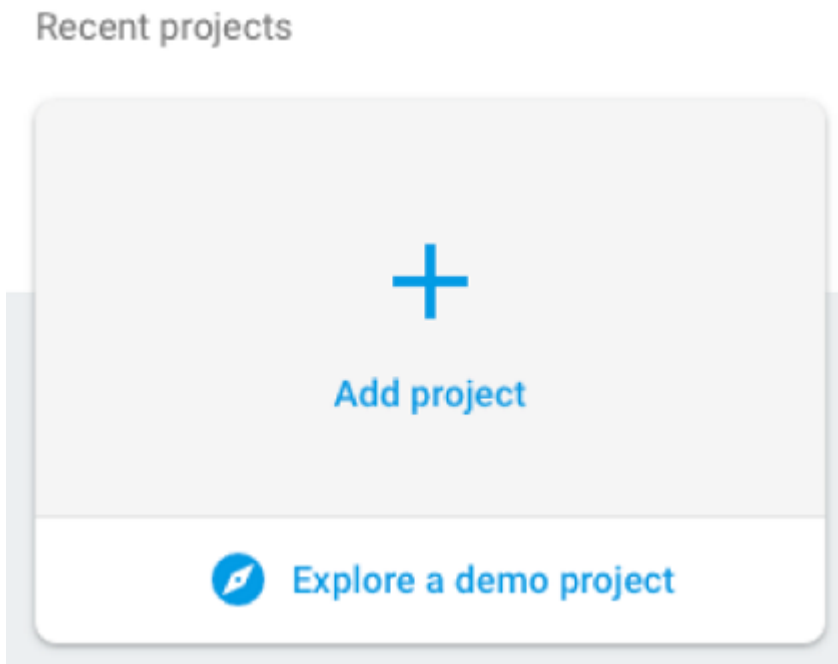


FCM 에 대해 Google 계정을 구성하려면

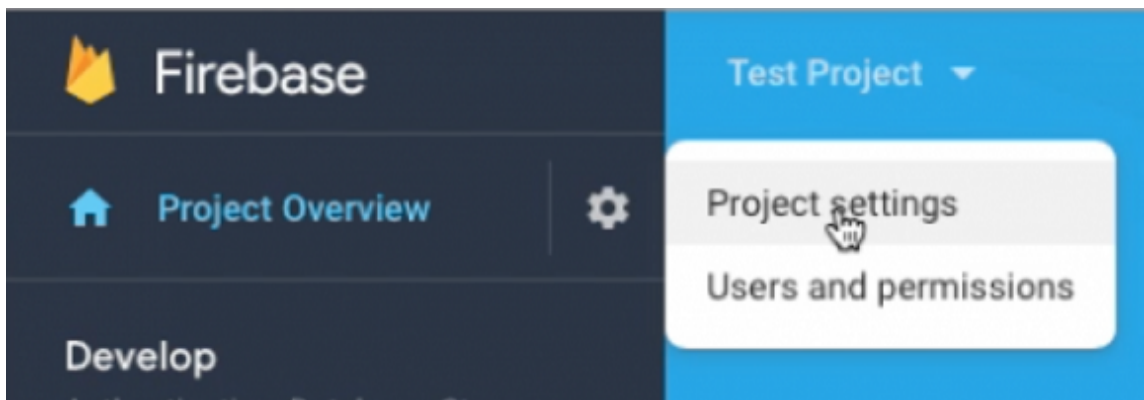
1. Google 개발자 계정 자격 증명을 사용하여 다음 URL 에 로그인합니다.

<https://console.firebase.google.com/>

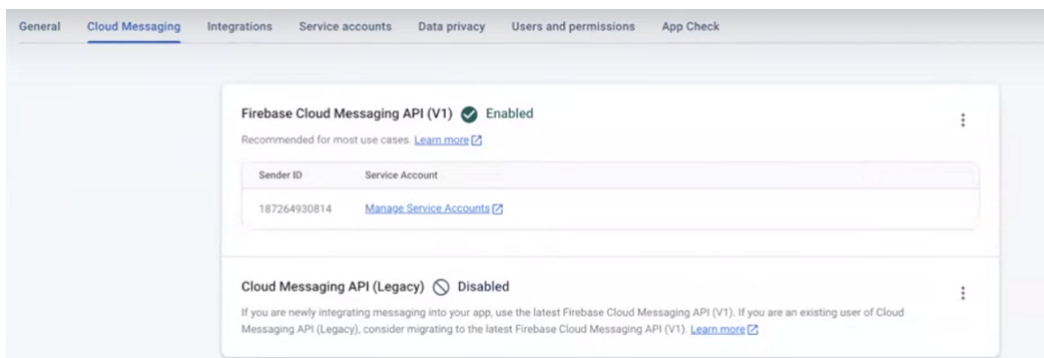
2. **Add project(프로젝트 추가)** 를 클릭합니다.



3. 프로젝트를 만든 후 **Project settings**(프로젝트 설정) 를 클릭합니다.

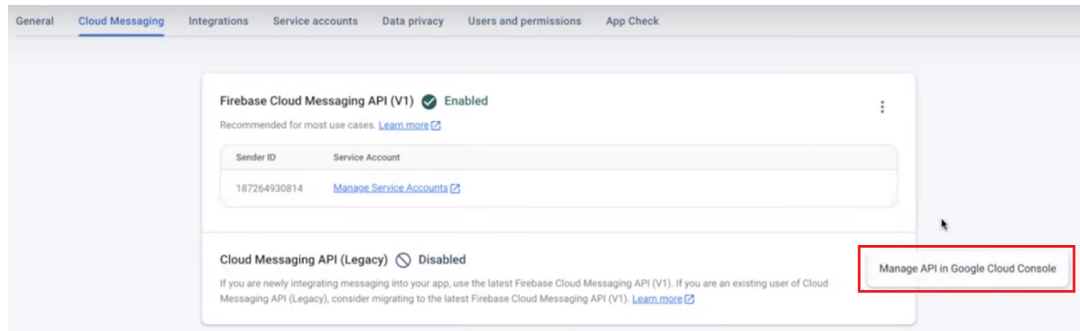


4. **Cloud Messaging**(클라우드 메시징) 탭을 클릭합니다.
5. 클라우드 메시징 **API (레거시)** 가 비활성화되면 서버 키가 표시되지 않습니다.

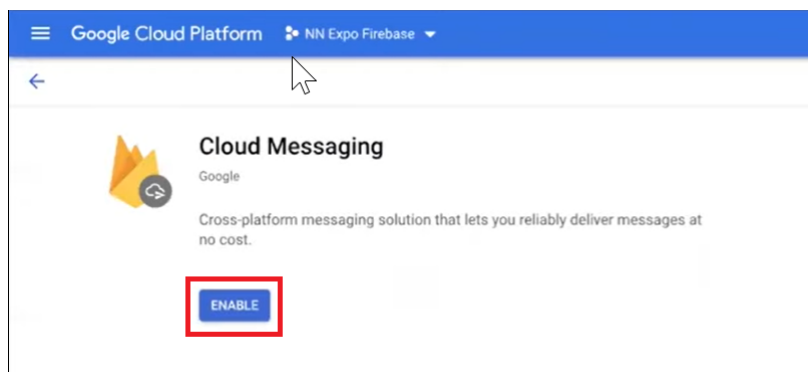


다음과 같이 클라우드 메시징 **API (레거시)** 를 활성화합니다.

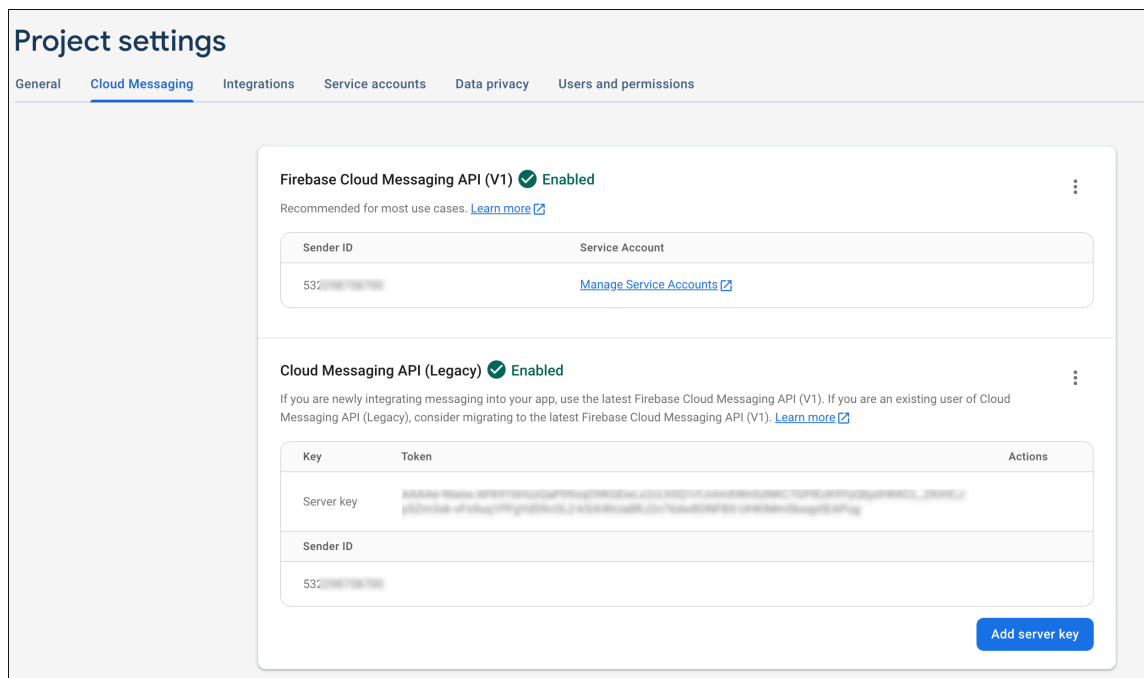
- a) 클라우드 메시징 **API(레거시)** 옆의 줄임표 버튼을 클릭한 다음 **Google Cloud Console** 에서 **API** 관리를 클릭합니다.



- b) **Cloud** 메시징에서 활성화 버튼을 클릭합니다.



6. **Server key**(서버 키) 와 **Sender ID**(보낸 사람 ID) 값을 복사합니다. 다음 절차에서 XenMobile 콘솔에 이러한 값을 붙여 넣습니다. 2016 년 10 월부터는 Firebase 콘솔에서 서버 키를 만들어야 합니다.

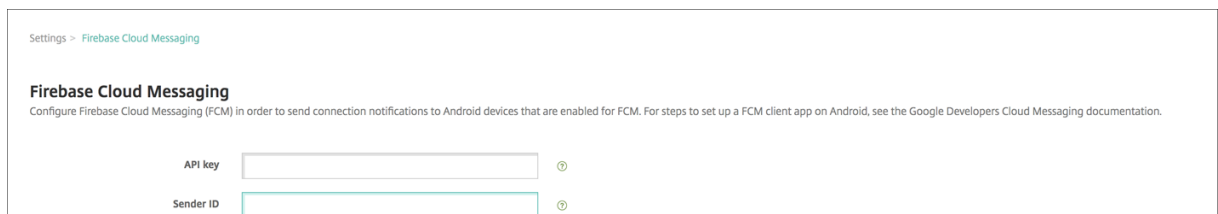


Android 에서 FCM 클라이언트 앱을 설정하는 단계는 이 Google Developers Cloud Messaging 문서 (<https://firebase.google.com/docs/cloud-messaging/android/client>) 를 참조하십시오.

XenMobile 을 FCM 에 대해 구성하려면

XenMobile 콘솔에서 설정 > **Firebase Cloud Messaging** 으로 이동합니다.

- **API** 키를 편집하고 Firebase Cloud Messaging 구성 마지막 단계에서 복사한 Firebase Cloud Messaging 서버 키를 입력합니다.
- 보낸 사람 **ID** 를 편집하고 이전 절차에서 복사한 보낸 사람 **ID** 값을 입력합니다.



Settings > Firebase Cloud Messaging

Firebase Cloud Messaging

Configure Firebase Cloud Messaging (FCM) in order to send connection notifications to Android devices that are enabled for FCM. For steps to set up a FCM client app on Android, see the Google Developers Cloud Messaging documentation.

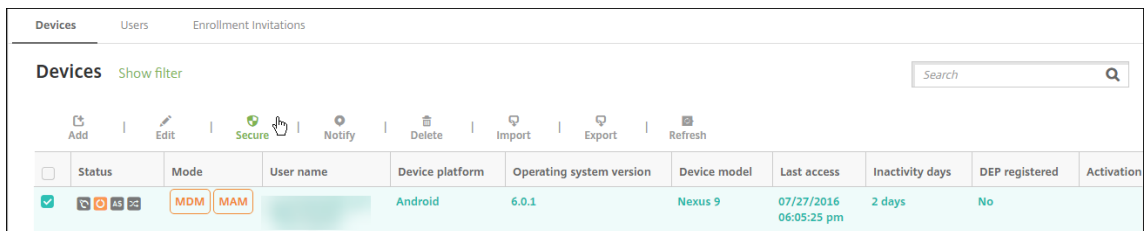
API key ⓘ

Sender ID ⓘ

설정을 완료한 후 예약 장치 정책을 제거하거나 해당 정책을 변경하여 연결 빈도를 줄일 수 있습니다.

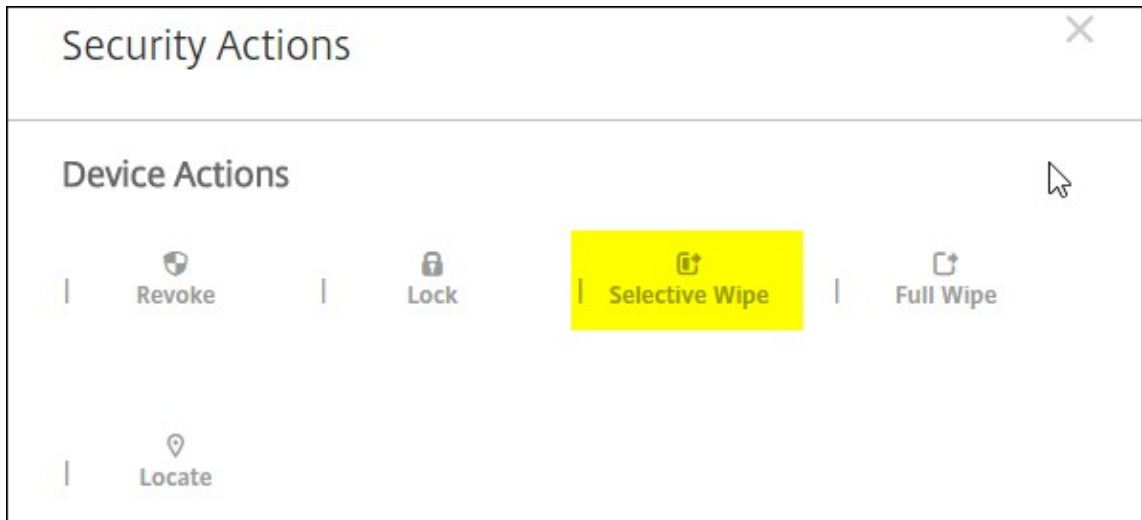
구성을 테스트하려면

1. Android 장치를 등록합니다.
2. XenMobile 에서 연결이 끊기도록 장치를 유휴 상태로 잠시 둡니다.
3. XenMobile 콘솔에 로그인하고 관리를 클릭하고 Android 장치를 선택한 후 보안을 클릭합니다.



Devices										
Users Enrollment Invitations										
Devices <small>Show filter</small>										
<div>Search</div>										
<div>Add Edit Secure Notify Delete Import Export Refresh</div>										
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered	Activation
<input checked="" type="checkbox"/>		MDM MAM		Android	6.0.1	Nexus 9	07/27/2016 06:05:25 pm	2 days	No	

4. 장치 동작에서 선택적 초기화를 클릭합니다.



구성이 성공적인 경우 장치에서 선택적 초기화가 수행됩니다.

Apple 교육 기능과 통합

March 15, 2024

Apple 교육을 사용하는 환경에서 XenMobile 을 MDM(모바일 기기 관리) 솔루션으로 사용할 수 있습니다. XenMobile 지원에는 Apple School Manager(ASM) 및 iPad 용 Classroom 앱이 포함됩니다. XenMobile 교육 구성 장치 정책은 Apple 교육을 사용할 강사 및 학생 장치를 구성합니다.

사전 구성을 마친 감독되는 iPad 를 강사와 학생에게 제공하십시오. 이 구성에는 XenMobile 의 ASM 등록, 새 암호로 구성된 관리되는 Apple ID 계정과 필수 볼륨 구매 앱 및 iBooks 가 포함됩니다.

다음은 Apple 교육 기능에 대한 XenMobile 의 주요 지원입니다.

Apple School Manager

ASM 은 교육 기관에서 사용되는 iOS(iPadOS) 장치와 macOS 노트북을 설정, 배포 및 관리할 수 있도록 하는 서비스입니다. ASM 에는 IT 관리자가 다음을 수행할 수 있는 웹 기반 포털이 포함되어 있습니다.

- Apple 배포 프로그램 장치를 여러 MDM 서버에 할당합니다.
- 앱 및 iBooks 를 위한 볼륨 구매 라이선스를 구매합니다.
- 관리되는 **Apple ID** 를 대량으로 생성합니다. 이 사용자 지정된 Apple ID 를 사용하면 Apple 서비스에 액세스하여 iCloud Drive 에 문서를 저장하고 Apple App Store 교육 과정에 등록하는 등의 작업을 수행할 수 있습니다.

여러 개의 ASM 계정을 XenMobile 에 추가할 수 있습니다. 예를 들어 이 기능을 사용하면 서로 다른 등록 설정 및 설정 도우미 옵션을 교육 단위 또는 부서별로 사용할 수 있습니다. 그런 다음 ASM 계정을 여러 장치 정책에 연결할 수 있습니다.

ASM 계정을 XenMobile 콘솔에 추가하면 XenMobile 이 클래스 및 명단 정보를 검색합니다. 장치 설정 시 XenMobile 은 다음을 수행합니다.

- 장치를 등록합니다.
- 배포에 구성된 리소스를 설치합니다 (예: 장치 정책, 교육 구성, 홈 화면 레이아웃 등).
- 볼륨 구매를 통해 구매한 앱과 iBooks 를 설치합니다.

사전 구성을 마친 장치를 강사와 학생에게 제공합니다. 분실 또는 도난 장치의 경우 MDM 분실 모드 기능을 사용하여 장치를 잠그고 찾을 수 있습니다.

iPad 용 Classroom 앱

iPad 용 Classroom 앱은 강사가 학생 장치에 연결하여 관리할 수 있도록 합니다. 장치 화면을 보고, iPad 에서 앱을 열고, 웹 링크를 공유하고 열 수 있습니다.

Classroom은 App Store 에서 무료로 사용할 수 있습니다. XenMobile 콘솔에 앱을 업로드한 다음 교육 구성 장치 정책을 사용하여 강사 장치에 배포할 Classroom 앱을 구성합니다.

Apple 교육 기능에 대한 자세한 내용은 Apple [교육](#) 사이트와 같은 사이트의 Apple 교육 배포 가이드를 참고하십시오.

사전 요구 사항

- Citrix Gateway
- MDM+MAM 에 대해 구성된 교육 프로필
- Apple iPad 3 세대 (최소 버전) 또는 iPad Mini(iOS 9.3 이상)

참고:

XenMobile 은 LDAP 또는 Active Directory 에 대해 ASM 사용자 계정을 검사하지 않습니다. 그러나 XenMobile 을 LDAP 또는 Active Directory 에 연결하여 ASM 강사나 학생과 관련되지 않는 사용자 및 장치를 관리할 수 있습니다. 예를 들어 Active Directory 를 사용하여 Secure Mail 및 Secure Web 을 다른 ASM 구성원 (예: IT 관리자) 에게 제공할 수 있습니다.

ASM 강사 및 학생은 로컬 사용자이므로 Citrix Secure Hub 를 강사 및 학생의 장치에 배포할 필요가 없습니다.

Citrix Gateway 인증이 포함되는 MAM 등록은 로컬 사용자를 지원하지 않습니다 (Active Directory 사용자만 지원). 따라서 XenMobile 은 필수 볼륨 구매 앱과 iBooks 만 강사와 학생의 장치에 배포합니다.

공유 iPad 에 대한 사전 요구 사항

- 모든 iPad Pro, iPad 5 세대, iPad Air 2 이상 및 iPad 미니 4 이상
- 최소 32GB 의 스토리지
- 감독됨

Apple School Manager 및 XenMobile 구성

Apple 또는 Apple 공인 리셀러/통신사를 통해 iPad 를 구입한 후 이 섹션의 워크플로에 따라 ASM 계정 및 장치를 설정하십시오. 이 워크플로에는 ASM 포털과 XenMobile 콘솔에서 수행하는 단계가 포함되어 있습니다.

다음 지침에 따라 일대일 모델 (학생당 iPad 1 대) 에서 사용하는 모든 iPad 또는 강사 iPad(비공유) 에 대한 통합을 구성합니다. 공유 iPad 를 구성하려면 공유 iPad 구성을 참조하십시오.

1 단계: Apple School Manager 계정 생성 및 설정 도우미 완료

Apple 배포 프로그램에서 업그레이드하려는 경우 Apple 지원 문서, [교육기관을 ASM 으로 업그레이드](#)를 참조하십시오. ASM 계정을 생성하려면 <https://school.apple.com/>으로 이동하고 지침에 따라 등록합니다. ASM 에 처음 로그인하면 설정 도우미가 열립니다.

- Apple School Manager 사전 요구 사항, 설정 도우미 및 관리 작업에 대한 자세한 내용은 [Apple School Manager 사용자 가이드](#)를 참조하십시오.
- ASM 을 설정할 때는 Active Directory 도메인 이름과 다른 도메인 이름을 사용합니다. 예를 들어 ASM 도메인 이름에 `appleid` 같은 접두사를 추가합니다.
- ASM 을 명단 데이터에 연결하면 ASM 이 강사 및 학생이 사용할, 관리되는 Apple ID 를 생성합니다. 명단 데이터에는 강사, 학생 및 클래스가 포함됩니다. ASM 에 명단 데이터 추가에 대한 자세한 정보는 앞서 참고했던 ASM 사용자 가이드에서 확인하십시오.
- 앞서 참고했던 ASM 사용자 가이드의 설명에 따라 관리되는 Apple ID 형식을 해당 교육 기관에 맞게 사용자 지정할 수 있습니다.

중요:

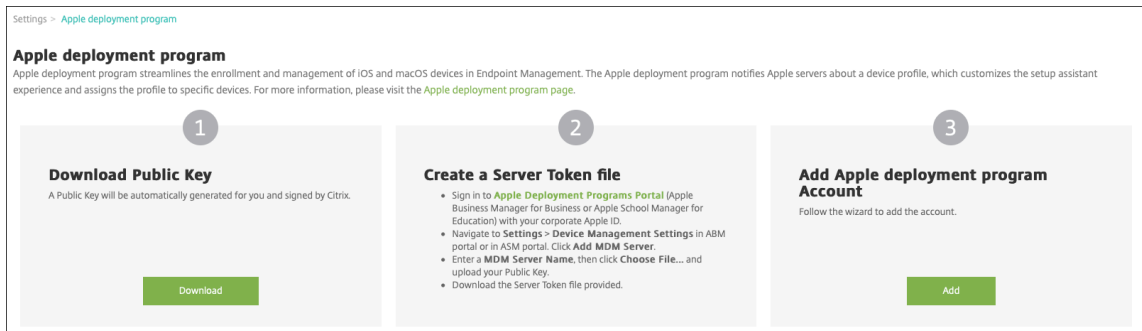
ASM 정보를 XenMobile 로 가져온 후에는 관리되는 Apple ID 를 변경하지 마십시오.

- 리셀러 또는 통신사를 통해 장치를 구매한 경우 이러한 장치를 ASM 에 연결합니다. 자세한 정보는 앞서 참고했던 ASM 사용자 가이드에서 확인하십시오.

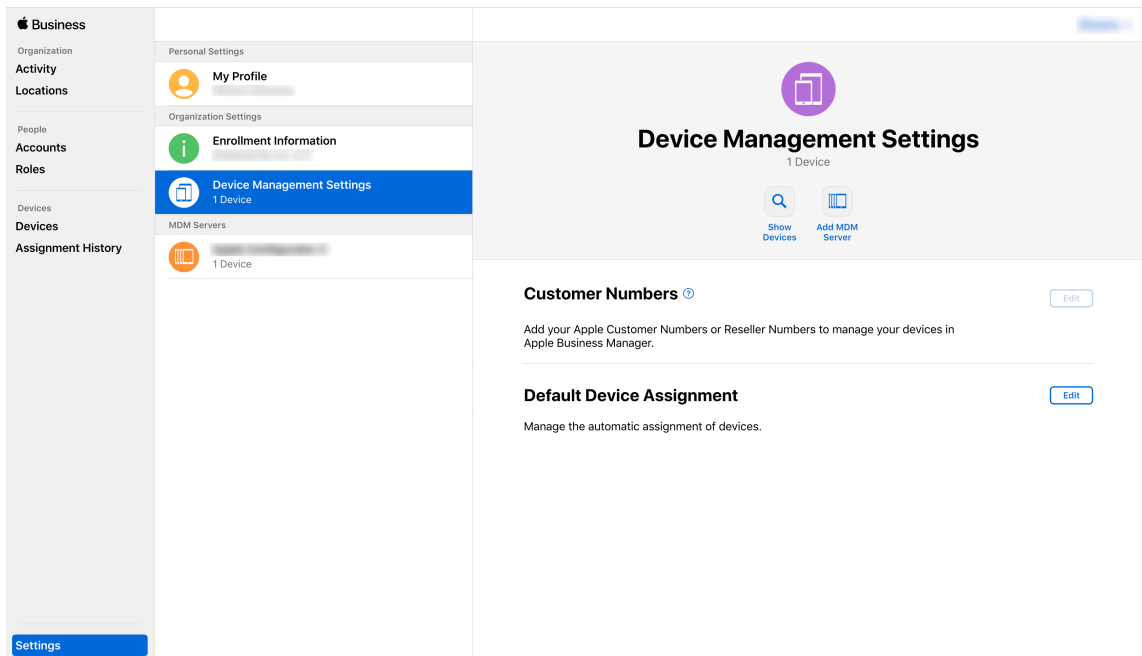
2 단계: XenMobile 을 Apple School Manager 의 MDM 서버로 구성하고 장치 할당 구성

ASM 포털에는 **MDM** 서버 탭이 있습니다. 이 설정을 완료하려면 XenMobile 의 공개 키 파일이 필요합니다.

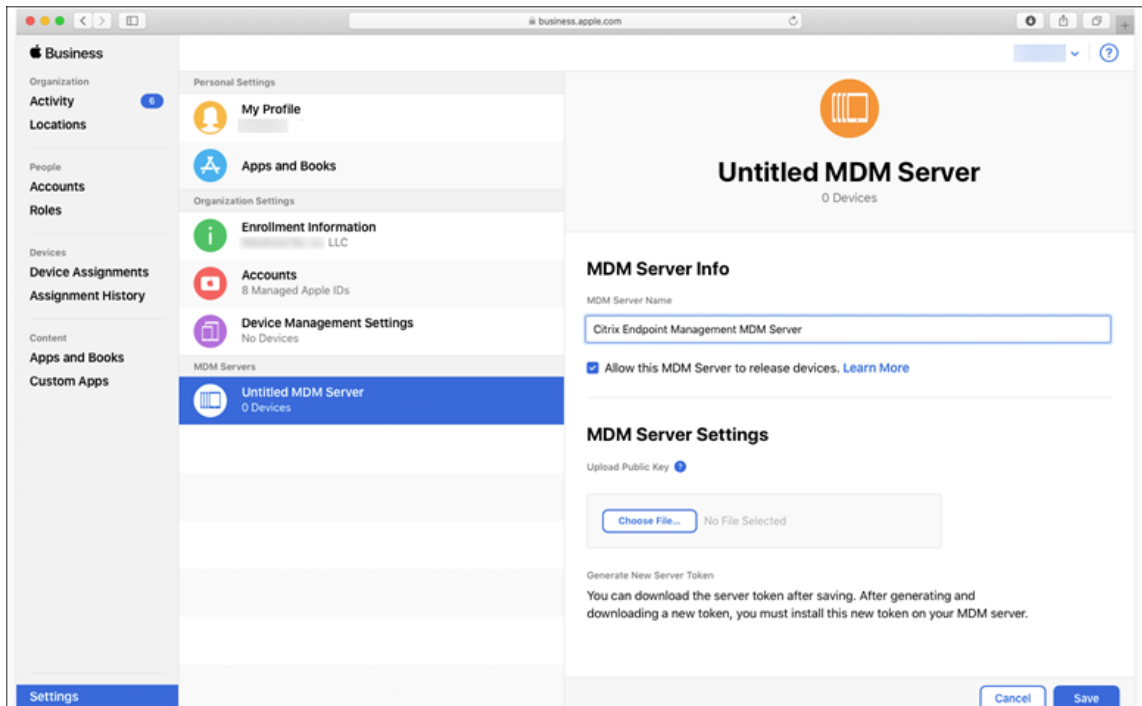
1. XenMobile 의 공개 키를 로컬 컴퓨터에 다운로드합니다. XenMobile 콘솔에서 설정 > **Apple** 배포 프로그램으로 이동합니다.



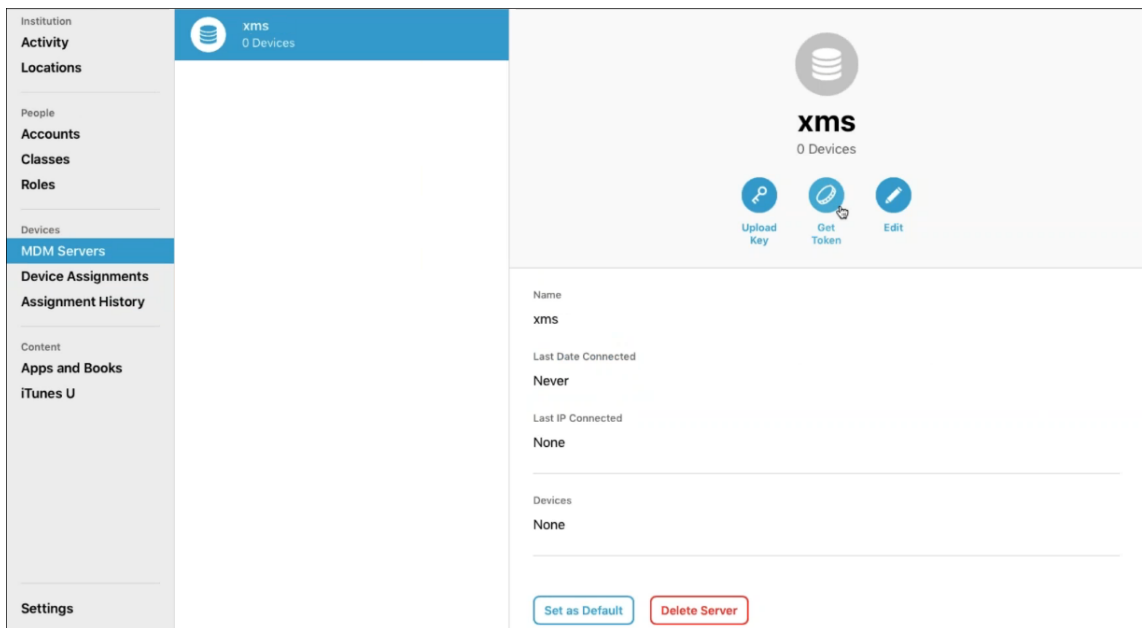
- 공개 키 다운로드에서 다운로드를 클릭하고 PEM 파일을 저장합니다.
- Apple School Manager** 포털에서 설정을 클릭한 다음 장치 관리 설정을 클릭합니다. **MDM** 서버 추가를 클릭합니다.



- XenMobile 이름을 입력합니다. 입력하는 서버 이름은 참조용이며 서버의 URL 또는 이름이 아닙니다. 공개 키 업로드에서 파일 선택을 클릭합니다.



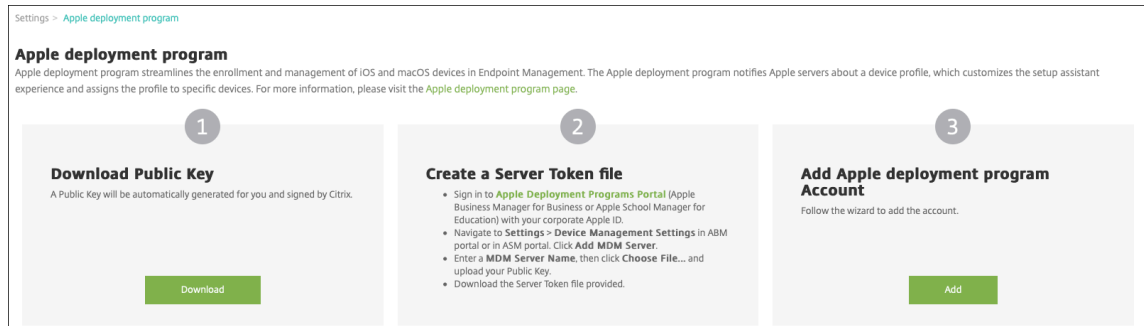
5. XenMobile 에서 다운로드한 공개 키를 업로드하고 저장을 클릭합니다.
6. 서버 토큰을 생성합니다. 토큰 다운로드를 클릭하여 서버 토큰 파일을 컴퓨터에 다운로드합니다.



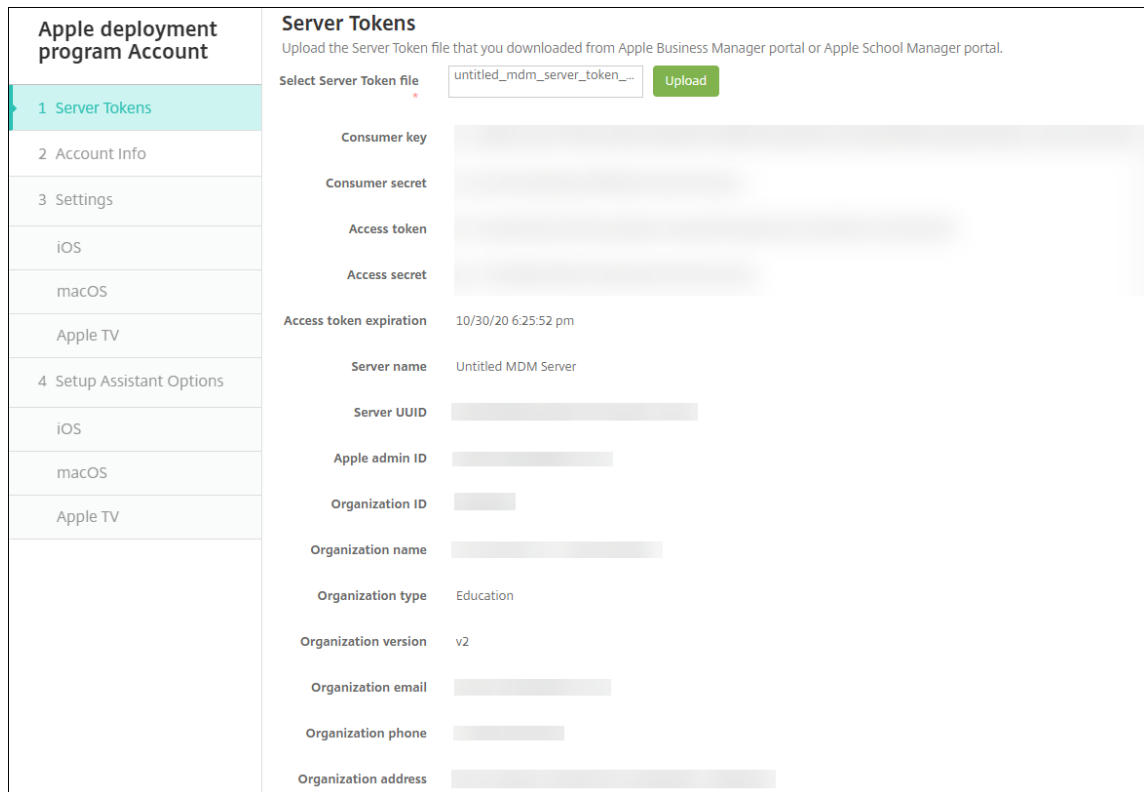
7. 기본 장치 할당에서 변경을 클릭합니다. 장치 할당 방법을 선택한 후 요청된 정보를 제공합니다. 자세한 내용은 [ASM 사용자 가이드](#)를 참조하십시오.

3 단계: XenMobile 에 Apple School Manager 계정 추가

1. XenMobile 콘솔에서 설정 > **Apple** 배포 프로그램으로 이동한 다음 **Apple** 배포 프로그램 계정 추가에서 추가를 클릭합니다.



2. 서버 토큰 페이지에서 업로드를 클릭하고 ASM 포털에서 다운로드한 서버 토큰 파일 (P7M 파일) 을 선택합니다. 토큰 정보 페이지가 나타납니다.



참고:

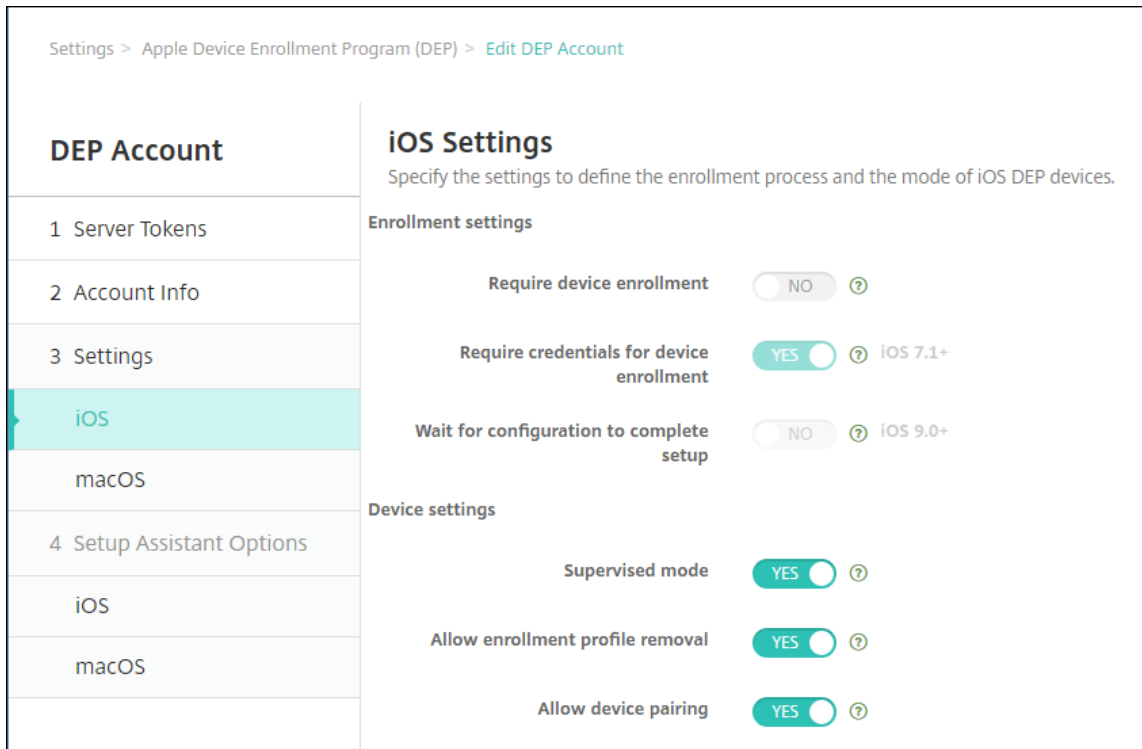
- 조직 **ID** 는 Apple 배포 프로그램의 고객 ID 입니다.
- ASM 계정의 조직 유형은 교육이고 조직 버전은 **v2** 입니다.

3. 계정 정보 페이지에서 다음 설정을 지정합니다.

Apple deployment program Account	Account Info
1 Server Tokens	Specify your Apple deployment program account information.
2 Account Info	<div>Apple deployment program account name * <input type="text" value="ASM Deployment"/></div> <div>Business/Education unit * <input type="text" value="Central High School"/></div> <div>Unique service ID <input type="text" value="2359487"/></div> <div>Support phone number * <input type="text" value="5555555555"/></div> <div>Support email address <input type="text"/></div> <div>Education suffix * <input type="text" value="suffix"/></div>
3 Settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

- **Apple** 배포 프로그램 계정 이름: 이 Apple 배포 프로그램 계정의 고유한 이름입니다. 국가 또는 조직 계층 구조 별과 같이 Apple 배포 프로그램 계정을 구성하는 방식을 반영하는 이름을 사용합니다.
- **Business/Education unit**(비즈니스/교육 단위): 장치를 할당할 교육 단위 또는 부서입니다. 이것은 필수 필드입니다.
- 고유 서비스 ID: 계정을 식별하는 데 도움이 되는 선택적 고유 ID 입니다.
- 지원 전화 번호: 사용자가 설정 중에 전화할 수 있는 지원 전화 번호입니다. 이것은 필수 필드입니다.
- 지원 전자 메일 주소: 최종 사용자에게 제공되는 선택적 지원 전자 메일 주소입니다.
- 교육 접미사: 지정된 ASM 배포 프로그램 계정의 클래스에 플래그를 지정합니다. (볼륨 구매 접미사는 지정된 볼륨 구매 계정의 앱과 iBooks 에 플래그를 지정합니다.) ASM 배포 프로그램과 ASM 볼륨 구매 계정 모두에 동일한 접미사를 사용하는 것이 좋습니다.

4. 다음을 클릭합니다. **iOS** 설정에서 다음 설정을 지정합니다.



- 등록 설정

- 장치 등록 필요: 사용자가 장치를 등록해야 합니다. 이 설정을 아니요로 변경합니다.
- 장치 등록에 자격 증명 필요: Apple 배포 프로그램 설정 중에 사용자가 자격 증명을 입력해야 합니다. XenMobile 과 ASM 의 통합의 경우 이 설정은 기본적으로 예이며 변경할 수 없습니다. Apple 배포 프로그램에는 장치 등록을 위한 자격 증명が必要です.
- 구성에서 설정을 완료할 때까지 대기: 모든 MDM 리소스가 장치에 배포될 때까지 사용자가 설정 도우미 모드에 있어야 하는지 여부를 설정합니다. XenMobile 과 ASM 통합의 경우 이 설정은 기본적으로 아니요입니다. Apple 설명서에 따르면 장치가 설정 도우미 모드에 있는 동안에는 다음 명령이 작동하지 않을 수 있습니다.
 - ★ InviteToProgram
 - ★ InstallApplication
 - ★ InstallMedia
 - ★ ApplyRedemptionCode

- 장치 설정

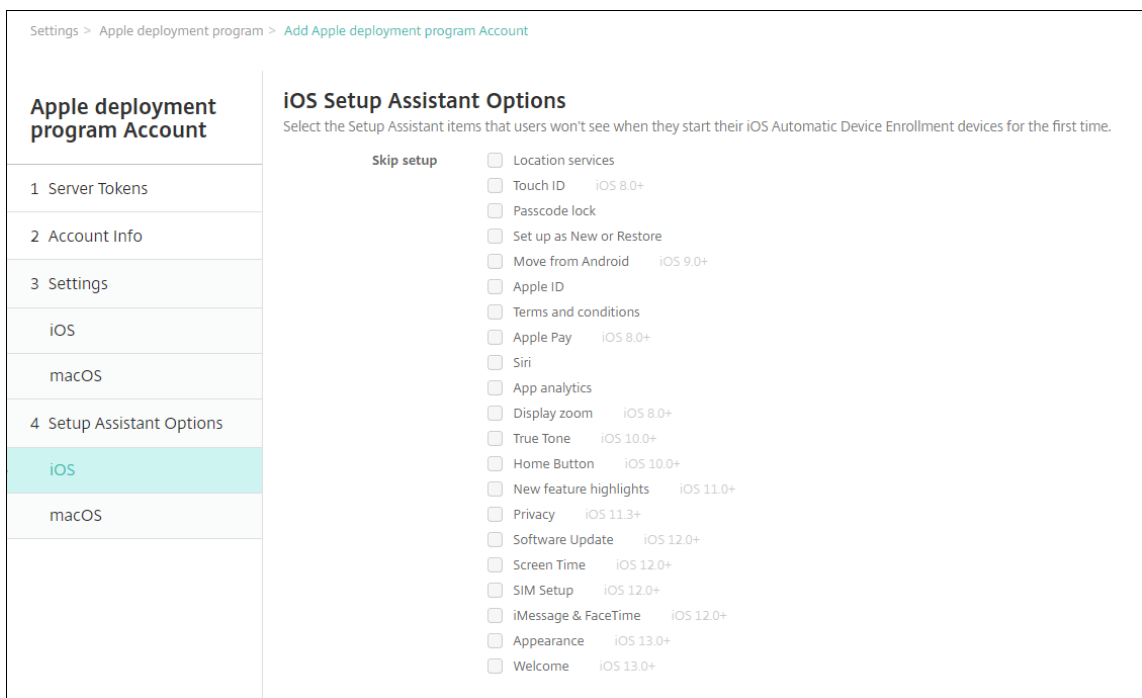
- 감독 모드: iOS 장치를 감독 모드로 전환합니다. 기본값인 예를 변경하지 마십시오. iOS 장치를 감독 모드로 전환하는 방법에 대한 자세한 내용은 [Apple Configurator](#) 를 사용하여 iOS 장치를 감독 모드로 전환을 참조하십시오.
- 공유 모두: iPad 에서 공유 모드를 설정합니다. 최소 요구 사항을 충족하지 않는 장치는 공유할 수 없습니다.

- 등록 프로필 제거 허용: ASM 통합의 경우 사용자가 장치에서 등록 프로필을 제거할 수 있도록 합니다. 이 설정을 예로 변경합니다.
- 장치 페어링 허용: ASM 통합의 경우 App Store 및 Apple Configurator 를 통해 관리할 수 있도록 장치 페어링을 허용합니다. 이 설정을 예로 변경합니다.

5. **iOS** 설정 도우미 옵션에서 사용자가 장치를 처음으로 시작할 때 건너뛴 iOS 설정 도우미 단계를 선택합니다. 기본적으로 설정 도우미에는 모든 단계가 포함됩니다. 설정 도우미에서 단계를 제거하면 사용자 환경이 간소화됩니다.

중요:

Apple ID 및 약관 단계는 포함하는 것이 좋습니다. 이 단계는 강사와 학생이 관리되는 Apple ID 의 새 암호를 입력하고 필수 약관에 동의하는 데 사용됩니다.



- 위치 서비스: 장치에 위치 서비스를 설정합니다.
- **Touch ID:** iOS 장치에서 Touch ID 를 설정합니다.
- 암호 잠금: 장치에 대한 암호를 만듭니다.
- 새로 설정 또는 복원: 장치를 새로 설정하거나 iCloud 또는 Apple App Store 백업에서 복원합니다.
- **Android** 에서 이동: Android 장치의 데이터를 iOS 장치로 전송할 수 있도록 합니다. 이 옵션은 새로 설정 또는 복원을 선택한 경우에만 사용할 수 있습니다 (즉, 단계가 생략됨).
- **Apple ID:** 장치에 대한 Apple ID 계정을 설정합니다. 확인란을 선택하여 이 단계를 포함하는 것이 좋습니다.
- 약관: 사용자가 장치 사용에 대한 약관에 동의해야 합니다. 확인란을 선택하여 이 단계를 포함하는 것이 좋습니다.
- **Apple Pay:** iOS 장치에 Apple Pay 를 설정합니다.
- **Siri:** 장치에서 Siri 를 사용하거나 사용하지 않습니다.
- 앱 분석: 충돌 데이터 및 사용 현황 통계를 Apple 과 공유할지 여부를 설정합니다.

- 표시 확대/축소: iOS 장치에서 디스플레이 해상도 (표준 또는 확대) 를 설정합니다.
- **True Tone:** iOS 장치에서 True Tone 디스플레이를 설정합니다.
- 홈 버튼: 홈 버튼 화면 민감도를 설정합니다.
- 새로운 기능 하이라이트: iOS 11.0 장치 (최소 버전) 에서 어디서든 Dock 에 접근하기와 최근 앱 간 전환이라는 온보딩 정보 제공용 화면을 설정합니다.
- 개인 정보 보호: Apple 배포 프로그램 장치를 설정하는 동안 사용자에게 데이터 및 개인 정보 보호 창을 표시하지 않습니다. iOS 11.3 이상에 해당합니다.
- **SoftwareUpdate:** Apple 배포 프로그램 장치를 설정하는 동안 사용자에게 필수 소프트웨어 업데이트 화면을 표시하지 않습니다. iOS 12.0 이상에 해당합니다.
- **ScreenTime:** Apple 배포 프로그램 장치를 설정하는 동안 사용자에게 Screen Time(화면 시간) 화면을 표시하지 않습니다. iOS 12.0 이상에 해당합니다.
- **SIM Setup(SIM 설정):** Apple 배포 프로그램 장치를 설정하는 동안 사용자에게 Add Cellular Plan(데이터 요금제 추가) 화면을 표시하지 않습니다. iOS 12.0 이상에 해당합니다.
- **iMessage & FaceTime:** Apple 배포 프로그램 장치를 설정하는 동안 사용자에게 iMessage 및 FaceTime 화면을 표시하지 않습니다. iOS 12.0 이상에 해당합니다.

6. 계정이 설정 > **Apple** 배포 프로그램에 표시됩니다. XenMobile 과 ASM 계정 간의 연결을 테스트하려면 계정을 선택하고 연결 테스트를 클릭합니다.

Settings > Apple Deployment Program

Apple Deployment Program

Apple deployment program streamlines the enrollment and management of iOS and macOS devices in Endpoint Management. The Apple deployment program notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. For more information, please visit the [Apple deployment program page](#).

1

Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Download

2

Create a Server Token file

- Sign in to [Apple deployment programs portal](#) (Apple Business Manager for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to Settings > Device Management Settings in ABM portal or in ASM portal. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

3

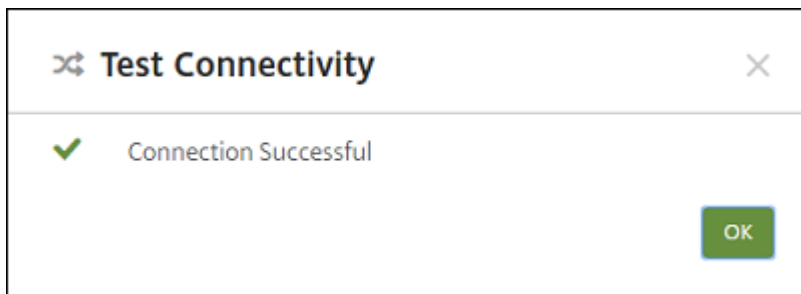
Add Apple Deployment Program Account

Follow the wizard to add the account.

Add

<input type="checkbox"/>	Apple deployment program account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
No results found.							

상태 메시지가 나타납니다.



몇 분 후 ASM 의 사용자 계정이 관리 > 사용자 페이지에 나타납니다. XenMobile 은 각 사용자에게 대해 가져온, 관리되는 Apple ID 를 바탕으로 로컬 사용자 계정을 생성합니다. 다음 예에서 사용자 계정에 대해 사용자 지정된 Apple ID 도 메인 이름 접두사는 **appleid**입니다.

Devices

Users

Enrollment Invitations

Users

Show filter

Search

Add Local User

Import Local Users

Manage Local Groups

Export

<input type="checkbox"/>	User name	First name	Last name	User type	Roles	Groups	Domain	Created	Last authenticated	ASM account name	
<input type="checkbox"/>		Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Lucas	Leong	ASM	USER	SAMPLE-CLASS-1013,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Alex	Mieuli	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Savannah	Cashman	ASM	USER	SAMPLE-CLASS-1010,SAMPLE-CLASS-1011	local	6/6/17 3:21 PM	6/13/17 6:46 PM	US ASM account	
<input type="checkbox"/>		Aiden	Westover	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Ava	Meinerth	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Liam	Willson	ASM	USER	SAMPLE-CLASS-1013,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Brayden	Anderson	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Gabriel	Zeifman	ASM	USER	SAMPLE-CLASS-1012,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	
<input type="checkbox"/>		Gavin	Tien	ASM	USER	SAMPLE-CLASS-1012,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account	

Showing 51 - 60 of 83 items

Items per page: 10

Page: 6 of 9

지정된 ASM 계정에 대한 모든 사용자를 찾으려면 사용자 검색 필터에 계정 이름을 입력합니다.

4 단계: Apple School Manager의 교육 볼륨 구매 계정 구성

이 섹션에서는 앱 및 iBooks 용 볼륨 구매 라이선스를 구매할 때 사용한 볼륨 구매 계정을 XenMobile에 지정합니다.

1. ASM에 대한 교육 볼륨 구매 계정을 구성하려면 [Apple 볼륨 구매](#)의 지침을 따르십시오. 볼륨 구매 계정 추가 화면에서 회사 토큰을 입력해야 합니다. 교육 볼륨 구매 계정에서 직접 토큰을 다운로드하고 볼륨 구매 계정 추가 화면에 붙여 넣습니다.

Settings > [Volume purchase](#)

Volume purchase

Configure these iOS-specific settings. When saved and validated, the Volume purchase apps are added to the table on the Apps tab.

Store user password in Secure Hub

☒

User property for Volume purchase country mapping

c

Volume purchase Accounts

Add

Force synchronization

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login	Last Sync Date	
<input type="checkbox"/>	test	Volume Purchase Acct	Citrix Systems	United States	10/24/20 10:43:54 am		10/28/19 4:00:00 pm	

2. 볼륨 구매 라이선스를 XenMobile 로 가져오는 동안 몇 분 정도 기다리십시오.

5 단계: Apple School Manager 사용자의 암호 추가

ASM 계정을 추가한 후 XenMobile 이 ASM 에서 클래스와 사용자를 가져옵니다. XenMobile 에서 클래스는 로컬 그룹으로 처리되며 콘솔에서 “그룹” 이라는 용어가 사용됩니다. ASM 에 그룹 이름이 있는 클래스의 경우 XenMobile 이 해당 그룹 이름을 클래스에 할당합니다. 그렇지 않은 경우 XenMobile 은 소스 시스템 ID 를 그룹 이름으로 사용합니다. 과정 이름은 ASM 에서 고유하지 않으므로 XenMobile 은 교육 과정 이름을 클래스 이름으로 사용하지 않습니다.

XenMobile 은 관리되는 Apple ID 를 사용하여 사용자 유형이 **ASM** 인 로컬 사용자를 생성합니다. 사용자가 로컬인 이유는 ASM 이 모든 외부 데이터 원본과 별개로 자격 증명을 생성하기 때문입니다. 따라서 XenMobile 은 이러한 사용자를 인증할 때 디렉터리 서버를 사용하지 않습니다.

ASM 은 XenMobile 에 임시 사용자 암호를 보내지 않습니다. CSV 파일로 가져오거나 수동으로 추가해야 합니다. 임시 사용자 암호를 가져오려면:

1. 관리되는 Apple ID 의 임시 암호를 생성할 때 ASM 에서 생성된 CSV 파일을 가져옵니다.
2. CSV 파일을 편집하여 사용자가 XenMobile 에 임시 암호를 등록할 때 제공한 새 암호로 바꿉니다. 이 목적으로 사용하는 암호 유형에는 제약이 없습니다.

CSV 파일의 입력 형식은 다음과 같습니다. `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

여기서:

사용자: `user@appleid.citrix.com`

이름: `Firstname`

중간 이름: `Middle`

성: `Lastname`

암호: `Password123!`

3. XenMobile 콘솔에서 관리 > 사용자를 클릭합니다. 사용자 페이지가 나타납니다.

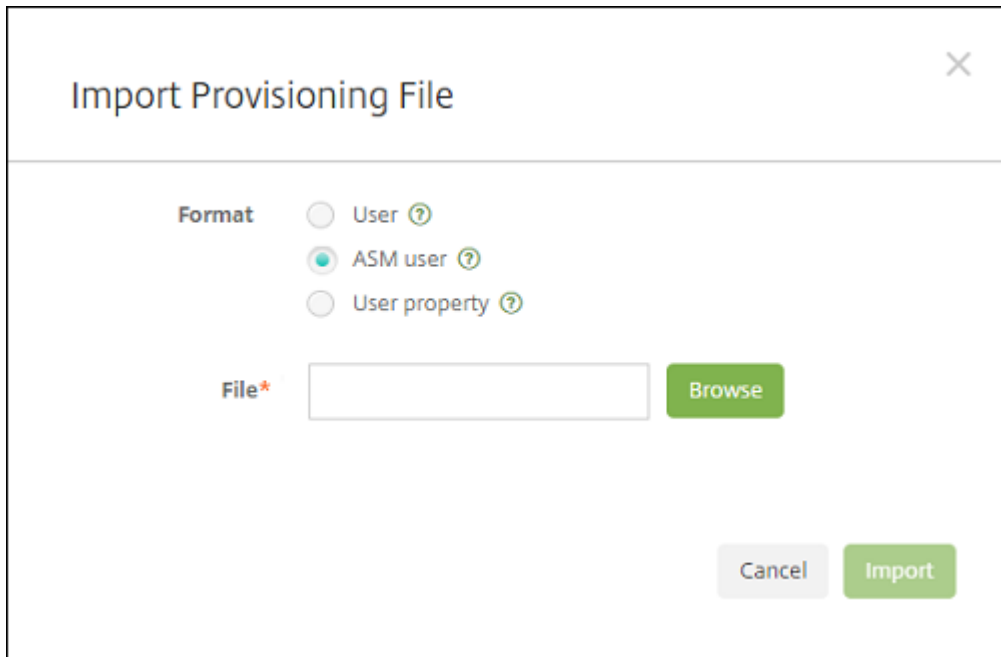
다음 관리 > 사용자 화면 샘플에는 ASM 에서 가져온 사용자 목록이 나와 있습니다. 사용자 목록에서:

- 사용자 이름에는 관리되는 Apple ID 가 표시됩니다.
- 사용자 유형은 **ASM** 이고 ASM 에서 생성된 계정임을 나타냅니다.
- 그룹에는 클래스가 표시됩니다.

Devices Users Enrollment Invitations									
<div> <div>Filters</div> <div> <div>Local groups</div> <div>Role</div> <div>Domain</div> <div>Education title</div> <div>Instructor</div> <div>Student</div> <div>Other</div> </div> <div> <div>Clear All</div> <div>7</div> <div>25</div> <div>0</div> </div> </div>									
<div> <div>Users</div> <div> <div>Add Local User</div> <div>Import Local Users</div> <div>Manage Local Groups</div> <div>Export</div> </div> <div> <div>Hide filter</div> <div>Search</div> </div> </div>									
<input type="checkbox"/>	User name	First name	Last name	User type	Roles	Groups	Domain	Created	
<input type="checkbox"/>		Julia	Romero	ASM	USER	SAMPLE-CLASS-1013 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00	
<input type="checkbox"/>		Kaelyn	Lazzara	ASM	USER	SAMPLE-CLASS-1013 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00	
<input type="checkbox"/>		Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00	

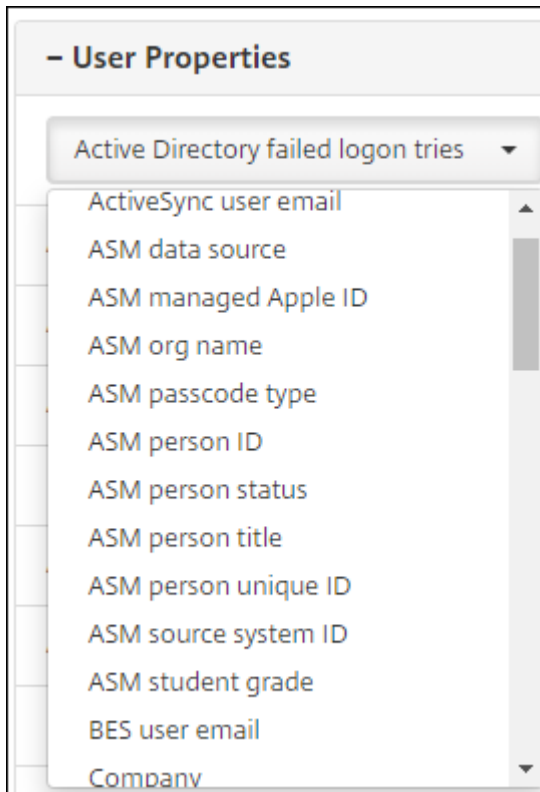
4. 로컬 사용자 가져오기를 클릭합니다. 프로비저닝 파일 가져오기 대화 상자가 나타납니다.

5. 형식으로 **ASM** 사용자를 선택하고, 2 단계에서 준비한 CSV 파일로 이동한 후 가져오기를 클릭합니다.



The dialog box titled "Import Provisioning File" contains a "Format" section with three radio buttons: "User", "ASM user" (which is selected), and "User property". Below this is a "File*" label next to a text input field, with a green "Browse" button to its right. At the bottom right, there are "Cancel" and "Import" buttons.

6. 로컬 사용자의 속성을 보려면 사용자를 선택하고 편집을 클릭합니다.



A dropdown menu titled "- User Properties" is shown. The selected item is "Active Directory failed logon tries". The dropdown list includes the following items: "ActiveSync user email", "ASM data source", "ASM managed Apple ID", "ASM org name", "ASM passcode type", "ASM person ID", "ASM person status", "ASM person title", "ASM person unique ID", "ASM source system ID", "ASM student grade", "BES user email", and "Company".

이름 속성 외에도 다음과 같은 ASM 속성을 사용할 수 있습니다.

- **ASM 데이터 원본:** 클래스의 데이터 원본입니다 (예: **CSV** 또는 **SFTP**).
- **ASM 관리되는 Apple ID:** 관리되는 Apple ID에는 교육 기관 이름과 **appleid**가 포함될 수 있습니다. 예를

들어 ID 는 `johnappleseed@appleid.myschool.edu`과 유사할 수 있습니다. XenMobile 는 인증에 관리되는 Apple ID 를 사용합니다.

- **ASM 조직 이름:** XenMobile 에서 계정에 지정한 이름입니다.
- **ASM 암호 유형:** 사용자의 암호 정책으로, 복합 형식 (학생 암호가 아닌 암호로, 8 자 이상의 숫자 및 문자로 구성 됨), **4**(자리) 또는 **6**(자리) 입니다.
- **ASM 사용자 고유 ID:** 사용자의 식별자입니다.
- **ASM 사용자 상태:** 관리되는 Apple ID 가 활성 또는 비활성인지 여부를 지정합니다. 사용자가 관리되는 Apple ID 계정에 대한 새 암호를 제공하면 이 상태가 활성으로 전환됩니다.
- **ASM 사용자 직위:** 강사, 학생 또는 기타입니다.
- **ASM 사용자 고유 ID:** 사용자의 고유 식별자입니다.
- **ASM 소스 시스템 ID:** 시스템 소스의 식별자입니다.
- **ASM 학생 학년:** 학생의 학년 정보입니다 (강사에게는 사용되지 않음).

6 단계: 학생의 사진 추가 (선택 사항)

각 학생의 사진을 추가할 수 있습니다. 강사가 Apple Classroom 앱을 사용하는 경우 이 앱에 사진이 나타납니다.

사진 권장 사항:

- 해상도: 256 x 256 픽셀 (2x 장치의 경우 512 x 512 픽셀)
- 형식: JPEG, PNG 또는 TIFF

사진을 추가하려면 관리 > 사용자에서 사용자를 선택하고 편집을 클릭한 후 이미지 선택을 클릭합니다.

The screenshot displays the 'Edit Local User' window. It includes input fields for 'User name', 'Password' (with a placeholder 'Enter new password'), and a 'Role' dropdown menu currently set to 'USER'. A 'Membership' section shows a list of groups with checkboxes; 'local\SAMPLE-CLASS-1013 - ASM' and 'local\SAMPLE-CLASS-1014 - ASM' are selected. A 'Manage Groups' button is located to the right of the membership list. Below these fields is a section for 'ASM student image' with a text box and a green 'Choose image' button. At the bottom, there is a table titled '- User Properties' with an 'Add' button. The table contains three rows: 'ASM account name' with the value 'US ASM', 'ASM person title' with the value 'Student', and 'ASM person unique ID' with an empty text box.

- User Properties		Add
ASM account name	US ASM	
ASM person title	Student	
ASM person unique ID		

7 단계: 리소스 및 배달 그룹을 계획하고 **XenMobile** 에 추가

배달 그룹은 사용자 범주에 배포할 리소스를 정의합니다. 예를 들어 강사와 학생에 대한 배달 그룹 하나를 생성하거나 여러 배달 그룹을 생성하여 여러 강사 또는 학생에게 전송되는 앱, 미디어 및 정책을 사용자 지정할 수 있습니다. 클래스당 하나 이상의 배달 그룹을 생성할 수 있습니다. 또한 관리자 (교육 기관의 다른 직원) 를 위한 하나 이상의 배달 그룹을 생성할 수 있습니다.

사용자 장치에 배포하는 리소스에는 장치 정책, 볼륨 구매 앱 및 iBooks 가 포함됩니다.

- 장치 정책:

강사가 Classroom 앱을 사용하는 경우 교육 구성 장치 정책이 필요합니다. 다른 장치 정책을 검토하여 강사 및 학생의 iPad 를 구성하고 제한하는 방법을 결정하십시오.

- 볼륨 구매 앱:

XenMobile 을 사용하려면 볼륨 구매 앱을 교육 사용자의 필수 앱으로 배포해야 합니다. XenMobile 은 볼륨 구매 앱의 선택적 배포를 지원하지 않습니다.

Apple Classroom 앱을 사용하는 경우 강사 장치에만 앱을 배포하십시오.

강사 또는 학생에게 제공하려는 다른 앱을 배포합니다. 이 솔루션은 Citrix Secure Hub 앱을 사용하지 않으므로 강사 또는 학생에게 이 앱을 배포하지 않아도 됩니다.

- 볼륨 구매 iBooks:

XenMobile 이 ASM 계정에 연결하면 구매한 iBooks 가 XenMobile 콘솔의 구성 > 미디어에 나타납니다. 이 페이지에 나열되는 iBooks 는 배달 그룹에 추가할 수 있습니다. XenMobile 은 iBooks 를 필수 미디어로만 지원합니다.

강사 및 학생을 위한 리소스 및 배달 그룹을 계획한 후에는 이러한 항목을 XenMobile 콘솔에서 생성할 수 있습니다.

1. 강사 또는 학생 장치에 배포할 장치 정책을 생성합니다. 교육 구성 장치 정책에 대한 자세한 내용은 [교육 구성 장치 정책](#)을 참조하십시오.

Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS		@appleid.citrix.com, @appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1010 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1011 - HS		@appleid.citrix.com	@appleid.citrix.com	
SAMPLE-CLASS-1012 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	

Allow students to change screen observation permission ☒ ON ⓘ iOS 10.3+

Policy Settings

Remove policy ☒ Select date ☐ Duration until removal (in hours)

장치 정책에 대한 자세한 내용은 [장치 정책](#)과 개별 정책 문서를 참조하십시오.

2. 앱 (구성 > 앱) 과 iBooks(구성 > 미디어) 를 구성합니다.

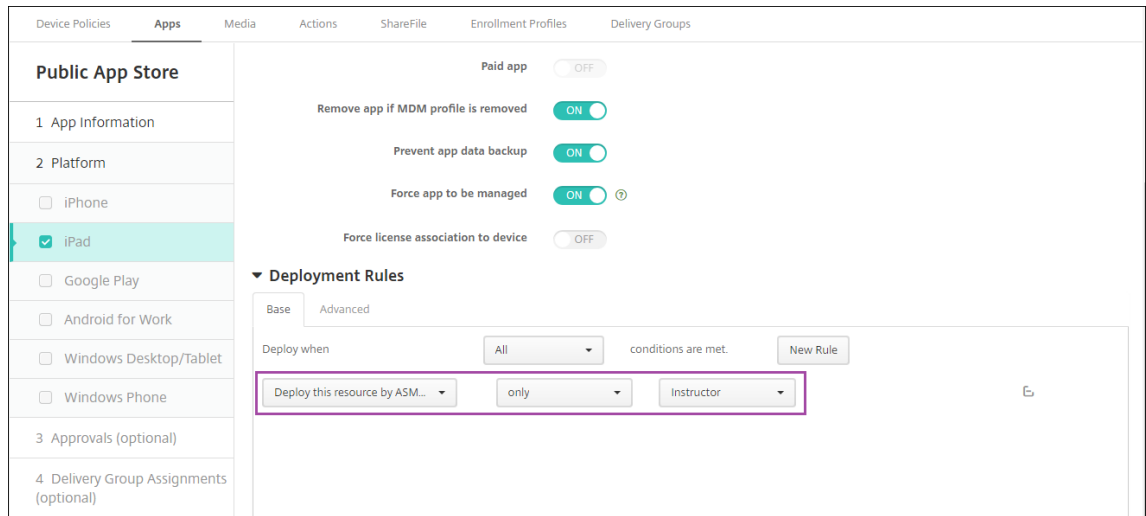
- 기본적으로 XenMobile 은 앱 및 iBooks 를 사용자 수준에서 할당합니다. 첫 배포 시 강사 및 학생에게는 ASM 등록 메시지가 표시됩니다. 사용자가 초대를 수락하면 다음 배포 (6 시간 이내) 시 ASM 앱과 iBooks 가 전송됩니다. Citrix 에서는 새 ASM 사용자에게 앱 및 iBooks 의 배포를 강제하도록 권장합니다. 그러려면 배달 그룹을 선택하고 배포를 클릭합니다.

장치 수준에서 앱 (iBooks 제외) 을 할당하도록 선택할 수 있습니다. 그러려면 장치에 강제로 라이선스 연결 설정을 켜짐으로 변경합니다. 장치 수준에서 앱을 할당하면 사용자에게 Apple 볼륨 구매 가입을 위한 초대가 전송되지 않습니다.

The screenshot displays the 'Apps' configuration page in the XenMobile console. On the left, the 'Public App Store' section is expanded, showing a list of platforms where 'iPad' is selected. The main area shows various app management settings, including 'Paid app' (OFF), 'Remove app if MDM profile is removed' (ON), 'Prevent app data backup' (ON), 'Force app to be managed' (ON), and 'Force license association to device' (OFF), which is highlighted with a red box. Below these, the 'Deployment Rules' section is visible, showing a rule configured to deploy the resource by ASM device type only to the Instructor group.

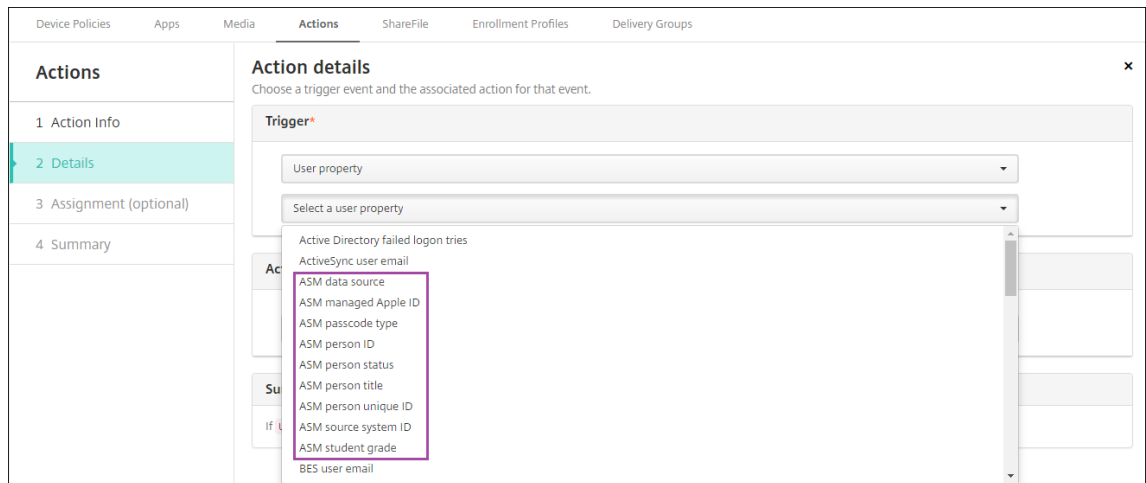
- 강사에게만 앱을 배포하려면 강사만 포함된 배달 그룹을 선택하거나 다음 배포 규칙을 사용합니다.

```
1 Deploy this resource by ASM device type
2 only
3 Instructor
4 <!--NeedCopy-->
```



- 볼륨 구매 앱 추가와 관련된 도움말은 [공용 앱 스토어 앱 추가](#)를 참조하십시오.

3. 선택 사항입니다. ASM 사용자 속성을 기반으로 동작을 생성합니다. 예를 들어 새 앱이 설치될 때 학생 장치에 알림을 보내는 동작을 생성할 수 있습니다. 또는 다음 예제에 표시된 것과 같이 사용자 속성이 트리거하는 동작을 생성할 수 있습니다.



동작을 생성하려면 구성 > 동작으로 이동합니다. 동작 구성에 대한 자세한 내용은 [자동화된 동작](#)을 참조하십시오.

4. 구성 > 배달 그룹에서 강사 및 학생을 위한 배달 그룹을 생성합니다. ASM 에서 가져온 클래스를 선택합니다. 또한 강사 및 학생에 대한 배포 규칙을 생성합니다.

예를 들어 다음은 강사에 대한 사용자 할당입니다. 배포 규칙은 다음과 같습니다.

```

1 Limit by user property
2 ASM person title
3 is equal to
4 Instructor
5 <!--NeedCopy-->
    
```

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

User Assignments

Select domain

local

Include user groups

sample

Search

☒

local\SAMPLE-CLASS-0001 - HS

☒

local\SAMPLE-CLASS-1010 - HS

☒

local\SAMPLE-CLASS-1011 - HS

☒

local\SAMPLE-CLASS-1012 - HS

☒

local\SAMPLE-CLASS-1013 - HS

Selected user groups:

local

SAMPLE-CLASS-1013 - HS

SAMPLE-CLASS-1014 - HS

b8d22143-e8c8-4c30-92db-d0f497151137 - HS

SAMPLE-CLASS-1010 - HS

SAMPLE-CLASS-0001 - HS

SAMPLE-CLASS-1012 - HS

MSP

SAMPLE-CLASS-1011 - HS

☒ Or

☐ And

Deploy to anonymous user

OFF

Deployment Rules

Base

Advanced

Limit by user property

ASM person title

is equal to

Instructor

+

-

AND

OR

NOT

EDIT

New Rule

Delete

다음은 학생에 대한 사용자 할당입니다. 배포 규칙은 다음과 같습니다.

```
1 Limit by user property
2 ASM person title
3 is equal to
4 Student
5 <!--NeedCopy-->
```

Delivery Group

- 1 Delivery Group Info
- 2 User**
- 3 Resource (optional)
- Policies
- Apps
- Media
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

User Assignments

Select domain: local

Include user groups: sample

Selected user groups:

local	
SAMPLE-CLASS-1013 - H5	<input type="button" value="X"/>
SAMPLE-CLASS-1014 - H5	<input type="button" value="X"/>
b8d22143-e8c8-4c30-92db-d0f497151137 - H5	<input type="button" value="X"/>
SAMPLE-CLASS-1010 - H5	<input type="button" value="X"/>
SAMPLE-CLASS-0001 - H5	<input type="button" value="X"/>
SAMPLE-CLASS-1012 - H5	<input type="button" value="X"/>
MSP	<input type="button" value="X"/>
SAMPLE-CLASS-1011 - H5	<input type="button" value="X"/>

☒ Or ☐ And

Deploy to anonymous user:

Deployment Rules

Base Advanced

Limit by user property: ASM person title is equal to Student

ASM 조직 이름에 기반한 배포 규칙을 사용하여 배포 그룹을 필터링할 수도 있습니다.

Delivery Group

- 1 Delivery Group Info
- 2 Assignments**
- 3 Resource (optional)
- Policies
- Apps
- Media
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

☒ Or ☐ And

Deploy to anonymous user:

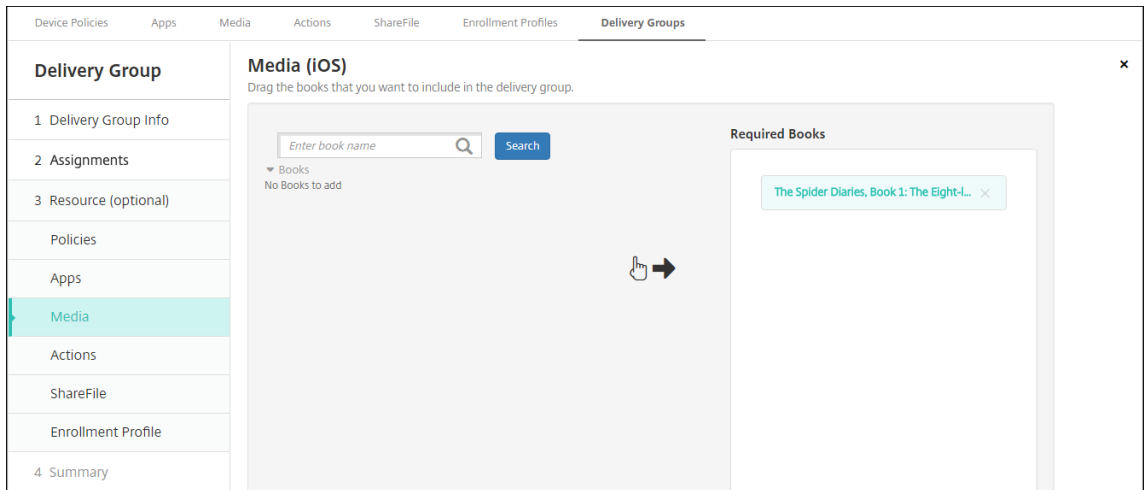
Deployment Rules

Base Advanced

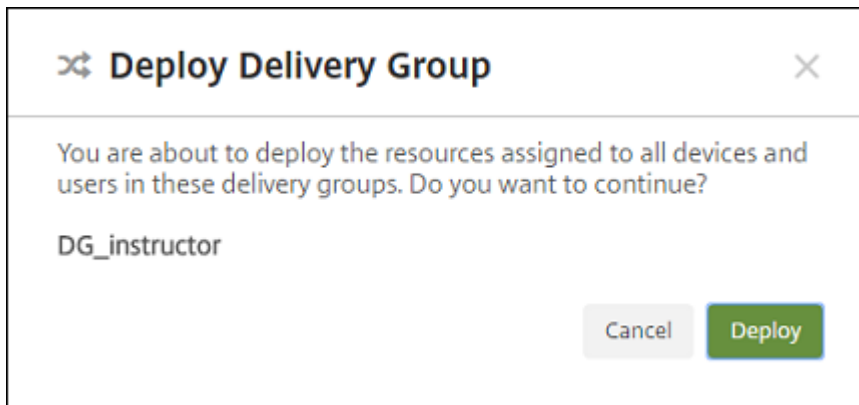
Deploy when: All conditions are met.

ASM org name only ASM

5. 배포 그룹에 리소스를 할당합니다. 다음 예제는 배포 그룹에 포함된 iBooks 를 보여 줍니다.



다음 예제는 배달 그룹을 선택하고 배포를 클릭할 때 표시되는 확인 대화 상자를 보여 줍니다.



자세한 내용은 [리소스 배포](#)의 “배달 그룹을 편집하려면” 과 “배달 그룹을 배포하려면” 을 참조하십시오.

8 단계: 강사 및 학생 장치 등록 테스트

다음 방법 중 하나를 사용하여 장치를 등록할 수 있습니다.

- 학교 관리자는 XenMobile 콘솔에서 설정할 수 있는 사용자 암호를 사용하여 강사 및 학생 장치를 등록할 수 있습니다. 따라서 앱과 미디어가 이미 설정된 장치를 사용자에게 제공할 수 있습니다.
- 사용자는 장치를 받은 후 관리자가 제공한 사용자 암호를 사용하여 등록합니다. 등록이 완료되면 XenMobile 이 장치 정책, 앱 및 미디어를 장치에 전송합니다.

등록을 테스트하려면 ASM 에 연결된 Apple 배포 프로그램 장치를 사용합니다.

1. 장치가 ASM 에 연결되지 않은 경우 하드 리셋을 수행하여 장치 콘텐츠 및 설정을 지웁니다.
2. 강사용 ASM 장치를 등록합니다. 그런 다음 학생용 ASM 장치를 등록합니다.
3. 관리 > 장치 페이지에서 두 ASM 장치가 MDM 전용으로 등록되었는지 확인합니다.

ASM 등록됨, **ASM** 공유됨, 강사, 학생 등의 장치 상태에 따라 장치 페이지를 필터링할 수 있습니다.

Devices

Users

Enrollment Invitations

Filters

Clear All

▶ User Group

Clear

▶ Device Mode

Clear

▶ Device Status

Clear

▶ Platform/Version

Clear

▶ Device Ownership

Clear

▶ Shared Status

Clear

▶ Inactive Time

Clear

▶ User Location

Clear

▶ App Restrictions

Clear

▼ ASM Device Status

Clear

▼

ASM registered

1

✔

Instructor

1

☐

Student

0

Devices

Hide filter

Search

Q

+

Add

+

Import

+

Export

+

Refresh

☐

Status

Mode

User name

Serial number

IMEI/MEID

Operating system version

Device model

Last access

Inactivity days

ASM

☐

🔒

📶

📶

📶

MDM

10.3.2

iPad

06/22/2017
07:00:03 pm

0 day

Instru

Showing 1 - 1 of 1 items

Items per page: 10 ▼

4. 각 장치에 대한 MDM 리소스가 올바르게 배포되었는지 확인하려면: 장치를 선택하고 편집을 클릭한 후 여러 페이지를 확인합니다.

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 iOS Profiles

10 iOS Provisioning Profiles

11 Certificates

12 Connections

13 MDM Status

@appleid.citrix.com | iPad

Success (1)Pending (0)Failed (0)

Delivery Groups

Time

DG_instructor31/07/2017 09:00:11

Showing 1 - 1 of 1 items

- Details

Status	Action	Channel/User	Date
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Book already installed)	@appleid.citrix.com	31/07/2017 09:00:11
Success	Installation result : MY LITTLE PONY: Magic Princess Quests - VPP (No need to install)	@appleid.citrix.com	31/07/2017 09:00:11
Success	Mobileconfig response : EDU (Profile already installed)	@appleid.citrix.com	31/07/2017 09:00:11
Success	Installation result : Classroom - VPP (No need to install)	@appleid.citrix.com	31/07/2017 09:00:11
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Book already installed)	i@appleid.citrix.com	31/07/2017 03:00:11

9 단계: 장치 배포

강사와 학생에게 장치를 배포할 수 있도록 이벤트를 호스트하는 것이 좋습니다.

사전 등록된 장치를 배포하지 않는 경우에는 사용자에게 다음 항목도 제공하십시오.

- 등록용 XenMobile 암호
- 관리되는 Apple ID 에 대한 ASM 임시 암호

첫 번째 사용자 환경은 다음과 같습니다.

1. 하드 리셋 후 사용자가 처음으로 장치를 시작하면 XenMobile 이 장치 등록을 위한 등록 화면을 표시합니다.

2. 사용자는 관리되는 Apple ID 와 인증에 사용되는 XenMobile 암호를 XenMobile 에 제공합니다.
3. Apple ID 설정 단계에서 관리되는 Apple ID 와 ASM 임시 암호를 제공하라는 메시지가 사용자에게 표시됩니다. 이러한 항목은 Apple 서비스에 대해 사용자를 인증하는 데 사용됩니다.
4. 관리되는 Apple ID 의 암호 (iCloud 의 데이터를 보호하는 데 사용됨) 를 생성하라는 메시지가 표시됩니다.
5. 설정 도우미를 마치면 XenMobile 이 장치에 정책, 앱 및 미디어를 설치하기 시작합니다. 사용자 수준에서 할당된 앱 및 iBooks 의 경우 강사 및 학생에게 볼륨 구매 등록 메시지가 표시됩니다. 사용자가 초대를 수락하면 다음 배포 (6 시간 이내) 시 볼륨 구매 앱과 iBooks 가 전송됩니다.

공유 iPad 구성

한 교실에 있는 여러 학생이 한 명 또는 여러 명의 강사가 가르치는 다양한 과목에서 iPad 를 공유할 수 있습니다.

관리자 또는 강사는 공유 iPad 를 등록한 다음 장치 정책, 앱 및 미디어를 장치에 배포합니다. 그런 다음 수강생은 관리되는 Apple ID 자격 증명을 제공하여 공유 iPad 에 로그인합니다. 이전에 교육 구성 정책을 학생에게 배포한 경우 학생은 장치를 공유할 때 “기타 사용자” 로 로그인하지 않습니다.

XenMobile 은 공유 iPad 에서 두 가지 통신 채널을 사용합니다. 장치 소유자 (강사) 에게는 시스템 채널을 사용하고 현재 상주 사용자 (학생) 에게는 사용자 채널을 사용합니다. XenMobile 은 이러한 채널을 사용하여 Apple 이 지원하는 리소스에 적절한 MDM 명령을 보냅니다.

시스템 채널을 통해 배포되는 리소스는 다음과 같습니다.

- 교육 구성, 잠금 화면 메시지, 최대 상주 사용자 수 및 암호 잠금 유예 기간과 같은 장치 정책
- 장치 기반 볼륨 구매 앱

Apple 은 공유 iPad 에서 엔터프라이즈 앱 또는 사용자 기반 볼륨 구매 앱을 지원하지 않습니다. 공유 iPad 에 설치된 앱은 사용자별로 적용되는 것이 아니라 장치에 글로벌로 적용됩니다.

- 사용자 기반 볼륨 구매 iBooks

Apple 은 공유 iPad 의 사용자 기반 볼륨 구매 iBooks 할당을 지원합니다.

사용자 채널을 통해 배포되는 리소스는 다음과 같습니다.

- 장치 정책: 앱 알림, 홈 화면 레이아웃 및 제한 사항

XenMobile 은 사용자 채널을 통해 이러한 장치 정책만 지원합니다.

장치 정책을 구성할 때 정책 설정 프로필 범위에서 배포 채널을 지정합니다.

Policy Settings

Remove policy ☒ Select date ☐ Duration until removal (in hours)

Allow user to remove policy Always

Profile scope User

iOS 9.3+

사용자 채널을 통해 배포한 장치 정책을 제거하려면 프로필 제거 정책에 대해 배포 범위를 사용자로 선택해야 합니다.

일반적인 워크플로

일반적으로 사전 구성을 마친 감독되는 공유 iPad 를 강사에게 제공합니다. 그런 다음 강사가 학생에게 장치를 배포합니다. 강사에게 사전 등록된 공유 iPad 를 배포하지 않는 경우: 강사에게 XenMobile 서버 암호를 제공하여 장치를 등록할 수 있도록 해야 합니다.

공유 iPad 를 구성하고 등록하는 일반적인 워크플로는 다음과 같습니다.

1. XenMobile 서버 콘솔을 사용하여 ASM 계정을 추가하고 (설정 > **Apple** 배포 프로그램) 공유 모드를 사용하도록 설정합니다. 자세한 내용은 다음의 “공유 iPad 에 대한 ASM 계정 관리” 를 참조하십시오.
2. 이 섹션에 설명된 대로 XenMobile 에 필요한 장치 정책, 앱 및 미디어를 추가합니다. 이러한 리소스를 배달 그룹에 할당합니다.
3. 강사로 하여금 공유 iPad 에 대해 하드 리셋을 수행하도록 합니다. 등록에 대한 원격 관리 화면이 나타납니다.
4. 강사가 공유 iPad 를 등록합니다.
XenMobile 이 등록된 각 공유 iPad 에 구성된 리소스를 배포합니다. 자동으로 다시 시작된 후 강사는 학생과 장치를 공유할 수 있습니다. iPad 에 로그인 페이지가 나타납니다.
5. 학생이 클래스를 선택한 다음 관리되는 Apple ID 와 임시 ASM 암호를 입력합니다.
공유 iPad 가 ASM 에 인증하고 학생에게 ASM 암호를 생성하라는 메시지를 표시합니다. 학생은 다음번에 공유 iPad 에 로그인할 때 새 ASM 암호를 제공합니다.
6. iPad 를 공유하는 다른 학생은 이전 단계를 반복하여 로그인할 수 있습니다.

공유 iPad 에 대한 ASM 계정 관리

Apple Education 에서 XenMobile 을 이미 사용하는 경우: 강사가 사용하는 장치와 같이 공유되지 않는 장치에 대한 기존 ASM 계정이 XenMobile 에 구성되어 있습니다. 공유 장치와 비공유 장치 모두에 동일한 ASM 및 동일한 XenMobile 서버를 사용할 수 있습니다.

XenMobile 은 다음과 같은 배포 시나리오를 지원합니다.

- 클래스별 공유 iPad 그룹

이 시나리오에서는 공유 iPad 를 클래스 학생에게 할당합니다. iPad 는 교실에 있습니다. 해당 클래스 다른 과목을 가르치는 강사는 동일한 iPad 세트를 사용합니다.

- 강사별 공유 iPad 그룹

이 시나리오에서는 공유 iPad 를 강사에게 할당합니다. 강사는 강사가 가르치는 다양한 클래스에서 해당 iPad 를 사용합니다.

공유 iPad 를 장치 그룹으로 구성

ASM 을 사용하면 여러 MDM 서버를 만들어 장치를 그룹으로 구성할 수 있습니다. MDM 서버에 공유 iPad 를 할당할 때 공유 iPad 의 각 그룹에 대한 장치 그룹을 클래스별 또는 강사별로 만듭니다.

- 공유 iPad 의 그룹 1 > 장치 그룹 1 MDM 서버
- 공유 iPad 의 그룹 2 > 장치 그룹 2 MDM 서버
- 공유 iPad 의 그룹 N > 장치 그룹 N MDM 서버

각 장치 그룹에 대한 **ASM** 계정 추가

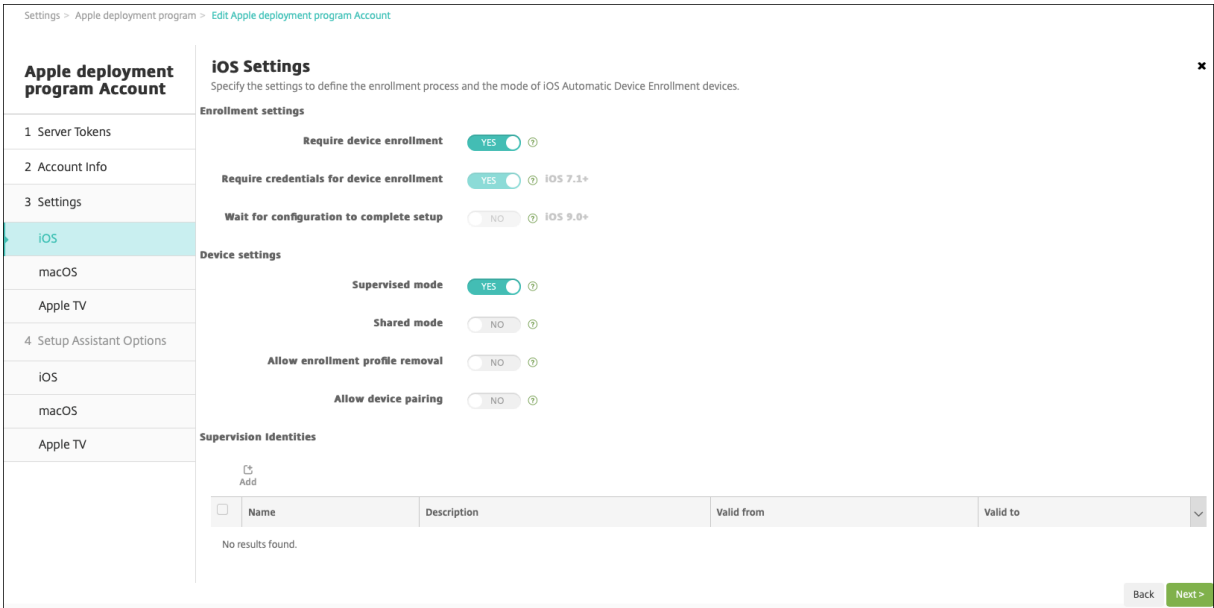
XenMobile 서버 콘솔에서 여러 ASM 계정을 생성하는 경우 공유 iPad 그룹을 자동으로 가져옵니다 (각 클래스 또는 강사당 1 대).

- 장치 그룹 1 MDM 서버 > 장치 그룹 1 계정
- 장치 그룹 2 MDM 서버 > 장치 그룹 2 계정
- 장치 그룹 N MDM 서버 > 장치 그룹 N 계정

공유 iPad 와 관련된 요구 사항은 다음과 같습니다.

- 다음 설정이 사용되는 각 장치 그룹에 대해 ASM 계정 1 개:
 - 장치 등록 필요
 - 감독 모드
 - 공유 모드
- 지정된 교육 조직의 경우 모든 ASM 계정에 동일한 교육 접미사를 사용해야 합니다.

계정을 추가하려면 설정 > **Apple** 배포 프로그램으로 이동합니다.



공유 iPad 의 앱

공유 iPad 는 장치 기반 볼륨 구매 앱 할당을 지원합니다. 공유 iPad 에 앱을 배포하기 전에 XenMobile 은 장치에 볼륨 구매 라이선스를 할당하라는 요청을 Apple 볼륨 구매 서버에 보냅니다. 볼륨 구매 할당을 확인하려면 구성 > 앱 > **iPad** 로 이동하고 볼륨 구매를 확장합니다.

공유 iPad 의 미디어

공유 iPad 는 사용자 기반 볼륨 구매 iBooks 할당을 지원합니다. 공유 iPad 에 iBooks 를 배포하기 전에 XenMobile 은 학생에게 볼륨 구매 라이선스를 할당하라는 요청을 Apple 볼륨 구매 서버에 보냅니다. 볼륨 구매 할당을 확인하려면 구성 > 미디어 > **iPad** 로 이동하고 볼륨 구매를 확장합니다.

Device Policies
Apps
Media
Actions
ShareFile
Enrollment Profiles
Delivery Groups

iBook
1 Book Information
2 Platform
iPhone
iPad
3 Delivery Group Assignments (optional)

Deployment Rules
Base
Advanced
Deploy when
All
conditions are met.
New Rule
Deploy this resource by device model
only
iPad
Device operating system version
is greater than or equal to
9.3
Supervised
True
Apple Deployment Program account name
only
ASM Automated Device Enrollment

Volume Purchase
Volume purchase License
Use Volume purchase company token
Volume purchase Account
test
Volume purchase ID Assignment
License Usage: 2 of 5

	License ID	Usage Status	Associated User
<input type="checkbox"/>	7545903139	Used	
<input type="checkbox"/>	7545903138	Used	

Back
Next >

공유 iPad 에 대한 배포 규칙

공유 iPad 배포의 경우 배달 그룹 수준의 규칙은 사용자 속성과 관련이 있으므로 적용되지 않습니다. 각 장치 그룹에 대한 정책, 앱 및 미디어를 필터링하려면 계정 이름을 기준으로 리소스에 대한 배포 규칙을 추가합니다. 예:

- 장치 그룹 1 계정의 경우 다음 배포 규칙을 설정합니다.

```

1 Apple Deployment Program account name
2 Only
3 Device Group 1 account
4
5 <!--NeedCopy-->

```

- 장치 그룹 2 계정의 경우 다음 배포 규칙을 설정합니다.

```

1 Apple Deployment Program account name
2 Only
3 Device Group 2 account
4
5 <!--NeedCopy-->

```

- 장치 그룹 N 계정의 경우 다음 배포 규칙을 설정합니다.

```

1 Apple Deployment Program account name
2 Only
3 Device Group N account
4
5 <!--NeedCopy-->

```

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Apps Notifications Policy

1 Policy Info

2 Platforms

IOS

3 Assignment

Calendar	True	True	True	True	True	True	None	
Mail	True	True	True	True	True	True	None	
Maps	True	True	True	True	True	True	None	
Wallet	True	True	True	True	True	True	None	

Policy Settings

Remove policy

Select date

Duration until removal (in hours)

Allow user to remove policy

Always

Profile scope

User

IOS 9.3+

Deployment Rules

Base

Advanced

Deploy when

All

conditions are met.

New Rule

Deploy this resource by device model

only

iPad

Device operating system version

is greater than or equal to

9.3

Supervised

True

Apple Deployment Program account name

only

ASM Automated Device Enrollment

Apple 교실 앱을 강사에게만 배포하려면 (공유되지 않는 iPad 사용) 다음 배포 규칙을 사용하여 ‘ASM 에 공유됨’ 상태로 리소스를 필터링합니다.

```
1 Deploy this resource regarding ASM shared mode
2 only
3 unshared
4
5 <!--NeedCopy-->
```

또는:

```
1 Deploy this resource regarding ASM shared mode
2 except
3 shareable
4
5 <!--NeedCopy-->
```

XenMobile Server 현재 릴리스

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

Public App Store

1 App Information

2 Platform

☐ iPhone

☒ iPad

☐ Google Play

☐ Android for Work

☐ Windows Desktop/Tablet

☐ Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Paid app

Remove app if MDM profile is removed

ON

Prevent app data backup

ON

Force app to be managed

ON

Force license association to device

ON

Deployment Rules

Base

Advanced

Deploy when

All

conditions are met.

New Rule

Deploy this resource regarding ASM

except

shareable

Store Configuration

Volume Purchase

Back

Next >

공유 iPad 의 배달 그룹

각 강사의 장치 그룹에 대해

- 하나의 배달 그룹을 구성합니다. 강사의 경우 교육 구성 정책에서 정의하는 모든 클래스를 할당합니다.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

Delivery Group

1 Delivery Group Info

2 Assignments

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

User Assignments

Select domain

testprise.net

Include user groups

Search

Selected user groups:

local

SAMPLE-CLASS-0001 - ASM DEP

SAMPLE-CLASS-1011 - ASM DEP

SAMPLE-CLASS-1010 - ASM DEP

Or

And

Deploy to anonymous user

OFF

Deployment Rules

Base

Advanced

Deploy when

All

conditions are met.

New Rule

ASM org name

only

Citrix Systems

Back

Next >

- 해당 배달 그룹에는 다음과 같은 MDM 리소스가 포함되어야 합니다.

- 장치 정책:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

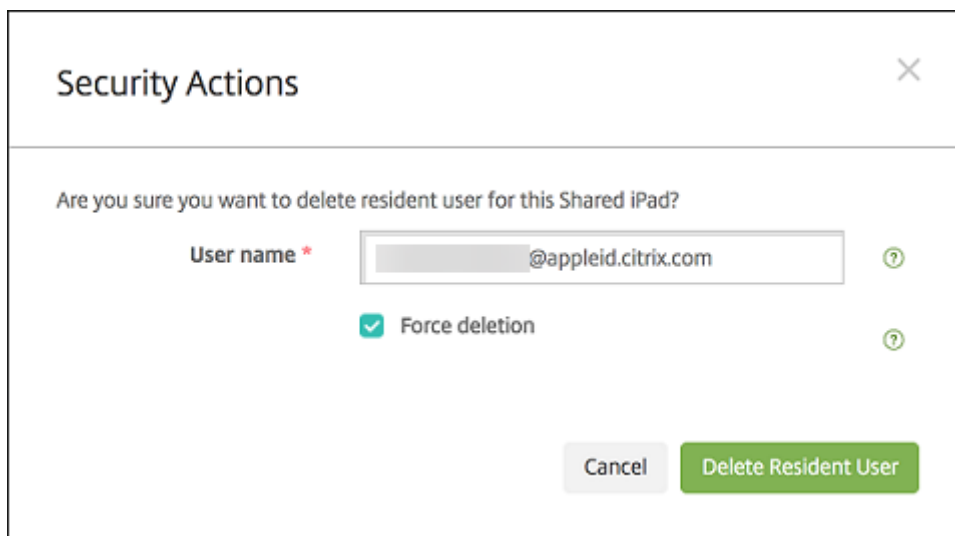
545

- ★ 교육 구성
- ★ 잠금 화면 메시지
- ★ 앱 알림
- ★ 홈 화면 레이아웃
- ★ 제한 사항
- ★ 최대 상주 사용자 수
- ★ 암호 잠금 유예 기간
- 필수 볼륨 구매 앱
- 필수 볼륨 구매 iBooks

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<div> <div> Delivery Group <ul style="list-style-type: none"> 1 Delivery Group Info 2 Assignments 3 Resource (optional) Policies Apps Media Actions ShareFile Enrollment Profile 4 Summary </div> <div> <div> Summary <p>Review the resources you are about to assign to the delivery group.</p> </div> <div> General <p>Name: iOS Education DG</p> <p>Description:</p> </div> <div> User <p>Include local user groups: local\SAMPLE-CLASS-1011 - ASM, local\SAMPLE-CLASS-0001 - ASM, local\SAMPLE-CLASS-1010 - ASM</p> <p>Logic: OR</p> </div> <div> Resource <div> <div> Policies 7 <ul style="list-style-type: none"> DEP Software Inventory Test 1 HSL Test 1 Notifications SAMPLE CLASS 0001 Restrictions Test Maximum Resident Users ASM DEP Edu Config Test Passcode Lock Grace Period </div> <div> Apps 2 <ul style="list-style-type: none"> MY LITTLE PONY: MAGIC PRINCESS - ASM Classroom - ASM </div> <div> Media 2 <ul style="list-style-type: none"> Rome - ASM The Spider Diaries, Book 1: The Eight-leg... - ASM </div> <div> Actions 0 </div> <div> ShareFile Disabled </div> <div> Enrollment Profile Global </div> </div> </div> </div> </div> <div data-bbox="218 1393 458 1429" data-label="Section-Header"> <h2>공유 iPad 의 보안 동작</h2> </div> <div data-bbox="218 1473 963 1509" data-label="Text"> <p>기존 보안 동작 외에 공유 iPad 에 대해 다음 보안 동작을 사용할 수 있습니다.</p> </div> <div data-bbox="268 1541 1457 1704" data-label="List-Group"> <ul style="list-style-type: none"> • 상주 사용자 가져오기: 현재 장치에 활성 계정이 있는 사용자를 나열합니다. 이 동작은 장치와 XenMobile 콘솔 간에 강제로 동기화됩니다. • 상주 사용자 로그아웃: 현재 사용자의 로그아웃을 강제 수행합니다. • 상주 사용자 삭제: 특정 사용자에 대한 현재 세션을 삭제합니다. 사용자는 다시 로그인할 수 있습니다. </div> <div data-bbox="218 2051 954 2094" data-label="Page-Footer"> <p>© 1999–2024 Cloud Software Group, Inc. All rights reserved.</p> </div> <div data-bbox="1394 2051 1457 2089" data-label="Page-Footer"> <p>546</p> </div>						



상주 사용자 삭제를 클릭한 후 사용자 이름을 지정할 수 있습니다.



보안 동작 결과는 관리 > 장치 > 일반 및 관리 > 장치 > 배달 그룹 페이지에 나타납니다.

공유 iPad 에 대한 정보 얻기

관리 > 장치 페이지에서 공유 iPad 와 관련된 정보를 찾습니다.

- 다음을 조회할 수 있습니다.
 - 장치의 공유 여부 (**ASM** 에 공유됨)
 - 공유 장치에 로그인한 사용자 (**ASM** 에 로그인한 사용자)
 - 공유 장치에 할당된 모든 사용자 (**ASM** 상주 사용자)

Devices									
Device Whitelist Users Enrollment Invitations									
<div>></div> <div>Search</div>									
Refresh									
	Serial number	Device platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users	...
leid.citrix.com leid.citrix.com		iOS	11.2.2	iPad	Instructor	Yes			

- **ASM** 장치 상태로 장치 목록을 필터링합니다.

Devices									
Device Whitelist Users Enrollment Invitations									
<div><</div> <div>Search</div>									
<div>▶ Device Status Clear</div> <div>▶ Device Ownership Clear</div> <div>▶ Shared Status Clear</div> <div>▶ Inactive Time Clear</div> <div>▶ User Location Clear</div> <div>▶ App Restrictions Clear</div> <div>▼ ASM Device Status Clear</div> <div><input type="checkbox"/> ASM registered 2</div> <div><input checked="" type="checkbox"/> ASM shared 1</div>									
platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users	...		
	11.2.2	iPad	Instructor	Yes					

- 관리 > 장치 > 로그인한 사용자 속성 페이지에서 공유 iPad 에 로그인한 사용자에 대한 세부 정보를 봅니다.

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

ipad

User Properties

User name

Enter new password

Role *
USER

Membership

local\Android Default Group

local\Android SD Enroller Group

local\Android SD Group

local\Apple Configurator Group

local\CWC GRP

Manage Groups

VPP Accounts

ASM VPP

Retire

Back

Next >

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

- User Properties

Add

ASM DEP org name

Citrix Systems

ASM person title

Student

ASM person unique ID

Name

Brayden Anderson

ASM source system ID

S25-008

ASM person status

Active

First name

Brayden

ASM person ID

SAMPLE-STUDENT-0008

ASM managed Apple ID

Surname

Anderson

ASM student grade

4

ASM passcode type

four

ASM data source

SFTP

Back

Next >

- 관리 > 장치 > 배달 그룹 페이지에서 배달 그룹의 강사 및 사용자에게 리소스를 배포할 때 사용되는 채널을 확인합니다. 채널/사용자 옆에는 유형 (시스템 또는 사용자) 과 받는 사람 (강사 또는 학생) 이 표시됩니다.

Devices

Users

Enrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

Delivery Groups

Success (1) Pending (0) Failed (0)

Delivery Groups

Time

SAMPLE CLASS 0001 DG11/30/17 5:48:04 pm

Showing 1 - 1 of 1 items

~ Details

Status	Action	Channel/User	Date
Failure	NotNow response : SecurityInfo MDM command (PARK)		11/30/17 5:48:04 pm
Success	Mobileconfig response : Test 1 Notifications (Profile already installed)		11/30/17 5:48:04 pm
Success	Package deploy end : SAMPLE CLASS 0001 DG		11/30/17 5:48:04 pm
Success	Mobileconfig response : Test 1 HSL (Profile already installed)		11/30/17 5:48:04 pm
Success	Mobileconfig response : SAMPLE CLASS 0001 Restrictions (Profile already installed)		11/30/17 5:48:03 pm
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Installed)		11/30/17 4:51:22 pm
Success	Installation result : Rome (Installed)		11/30/17 4:51:22 pm
Done	Software inventory requested		11/30/17 4:50:49 pm
Success	Software inventory response		11/30/17 4:50:49 pm
Done	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster - ASM (installing)		11/30/17 4:50:49 pm

BackNext >

- 상주 사용자에게 대한 정보를 확인합니다.
 - 동기화할 데이터 있음: 사용자에게 클라우드에 동기화할 데이터가 있는지 여부를 나타냅니다.
 - 데이터 할당량: 사용자에게 설정된 데이터 할당량 (바이트) 입니다. 사용자 할당량이 일시적으로 꺼져 있거나 사용자에게 적용되지 않는 경우 할당량이 표시되지 않을 수 있습니다.
 - 사용한 데이터: 사용자가 사용한 데이터의 양 (바이트) 입니다. 시스템에서 정보를 수집할 때 오류가 발생하면 값이 나타나지 않을 수 있습니다.
 - 로그인되어 있음: 사용자가 장치에 로그인했는지 여부를 나타냅니다.

Devices

Users

Enrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

Connections

First connection8/30/17 12:42:38 pm

StatusActive

Last connection11/30/17 5:48:04 pm

User name	Penultimate authentication	Last authentication	Has data to sync	Data quota	Data used	Is logged-in
ios	10/12/17 10:15:34 am	10/12/17 10:19:00 am				
	11/23/17 3:45:28 pm	11/23/17 3:45:29 pm				
	11/23/17 5:48:03 pm	11/23/17 5:48:03 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm	Yes			Yes
	11/29/17 7:02:32 pm	11/29/17 7:02:32 pm	No		120.82 MB	No

Showing 1 - 6 of 6 items

BackNext >

- 두 채널의 푸시 상태를 확인합니다.

The screenshot shows the 'Device details' page for an iPad. The left sidebar contains a list of options: 2 Properties, 3 User Properties, 4 Logged-in User Properties, 5 Assigned Policies, 6 Apps, 7 Media, 8 Actions, 9 Delivery Groups, 10 iOS Profiles, 11 iOS Provisioning Profiles, 12 Certificates, 13 Connections, and 14 MDM Status (highlighted). The main content area shows the following data:

System channel	
Push status	Active
Last push initiation	1/24/18 1:00:03 pm
Last notification completion	1/24/18 1:00:03 pm
Last reply time	1/24/18 1:00:03 pm

User channel	
Push status	Active
Last push initiation	1/24/18 1:00:03 pm
Last notification completion	1/24/18 1:00:03 pm
Last reply time	1/24/18 1:00:03 pm

At the bottom of the main content area, there is a 'Refresh' button. At the bottom right of the console, there are 'Back' and 'Save' buttons.

강사, 학생 및 클래스 데이터 관리

강사, 학생 및 클래스 데이터를 관리하는 경우 다음을 참고하십시오.

- ASM 정보를 XenMobile 로 가져온 후에는 관리되는 Apple ID 를 변경하지 마십시오. XenMobile 은 ASM 사용자 식별자를 사용하여 사용자를 식별합니다.
- 하나 이상의 교육 구성 장치 정책을 생성한 후 ASM 의 클래스 데이터를 추가하거나 변경하는 경우: 정책을 편집하고 다시 배포합니다.
- 교육 구성 장치 정책을 배포한 후 클래스의 강사가 변경되는 경우: 정책을 검토하여 XenMobile 콘솔에서 업데이트되는 지 확인한 후 정책을 다시 배포합니다.
- ASM 포털에서 사용자 속성을 업데이트하면 XenMobile 이 이러한 속성을 콘솔에도 업데이트합니다. 그러나 ASM 사용자 직위 속성 (강사, 학생 또는 기타) 은 다른 속성과 같은 방법으로 XenMobile 에 전송되지 않습니다. 그러므로 ASM 에서 ASM 사용자 직위를 변경하는 경우 다음 단계를 수행하여 XenMobile 에 변경 내용이 반영될 수 있도록 하십시오.

데이터를 관리하려면:

1. ASM 포털에서 학생 학년을 업데이트하고 강사 학년을 지웁니다.
2. 학생 계정을 강사 계정으로 변경한 경우 클래스의 학생 목록에서 해당 사용자를 제거합니다. 그런 다음 동일한 클래스 또는 다른 클래스의 강사 목록에 사용자를 추가합니다.

강사 계정을 학생 계정으로 변경한 경우 클래스에서 해당 사용자를 제거합니다. 그런 다음 동일한 클래스 또는 다른 클래스의 학생 목록에 사용자를 추가합니다. 다음 동기화 (기본적으로 5 분마다) 또는 가져오기 (기본적으로 24 시간마다) 중에 업데이트 내용이 XenMobile 콘솔에 표시됩니다.

3. 변경 내용을 적용하도록 교육 구성 장치 정책을 편집하고 다시 배포합니다.

- ASM 포털에서 사용자를 삭제하면 XenMobile 이 가져오기 후 XenMobile 콘솔에서도 해당 사용자를 삭제합니다.

다음 서버 속성 값을 변경하여 두 기준 사이의 간격을 줄일 수 있습니다. **bulk.enrollment.fetchRosterInfoDelay**(기본값은 **1440** 분)

- 리소스 배포 후: 학생이 클래스에 참여하면 해당 학생만 포함된 배달 그룹을 생성하고 리소스를 학생에게 배포합니다.
- 학생 또는 강사가 임시 암호를 잊은 경우 ASM 관리자에게 문의하도록 하십시오. 관리자는 임시 암호를 제공하거나 새 암호를 생성할 수 있습니다.

Apple School Manager Apple 배포 프로그램에 등록된 분실 또는 도난 장치 관리

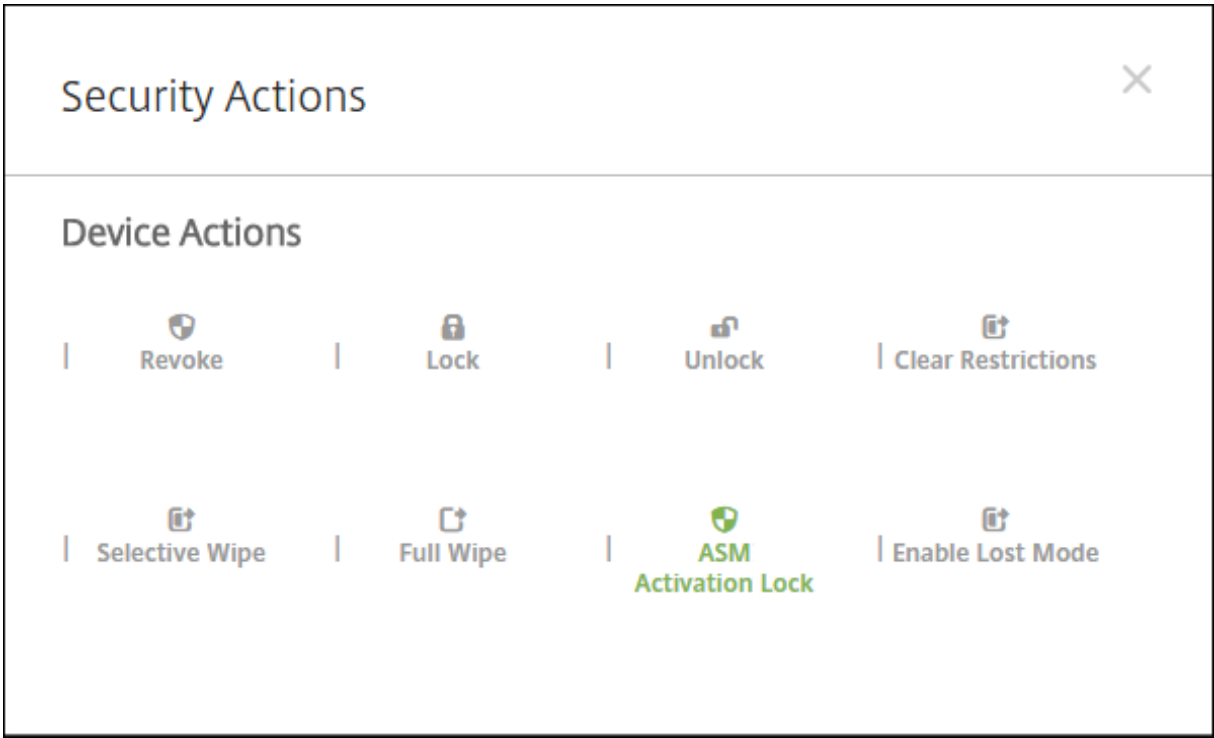
Apple 의 내 iPhone/iPad 찾기 서비스에는 활성화 잠금 기능이 포함되어 있습니다. 활성화 잠금 기능은 권한이 없는 사용자가 Apple 배포 프로그램에 등록된 분실 또는 도난 장치를 사용하거나 재판매할 수 없도록 합니다.

XenMobile 에 포함된 **ASM** 활성화 잠금 보안 동작을 사용하면 ASM Apple 배포 프로그램 등록 장치에 잠금 코드를 전송할 수 있습니다.

ASM 활성화 잠금 보안 동작을 사용하면 사용자가 내 iPhone/iPad 찾기 서비스를 사용하지 않고 XenMobile 을 통해 장치를 찾을 수 있습니다. ASM 장치가 하드 리셋되거나 전체 초기화된 경우 사용자는 관리되는 Apple ID 와 암호를 제공하여 장치 잠금을 해제할 수 있습니다.

콘솔에서 잠금을 해제하려면 활성화 잠금 바이패스 보안 동작을 클릭합니다. 활성화 잠금 바이패스에 대한 자세한 내용은 [iOS 활성화 잠금 바이패스](#)를 참조하십시오. 또한 로그인을 비워 두고 **ASM** 활성화 잠금 바이패스 코드를 암호로 입력할 수도 있습니다. 이 정보는 장치 세부 정보의 속성 탭에 나와 있습니다.

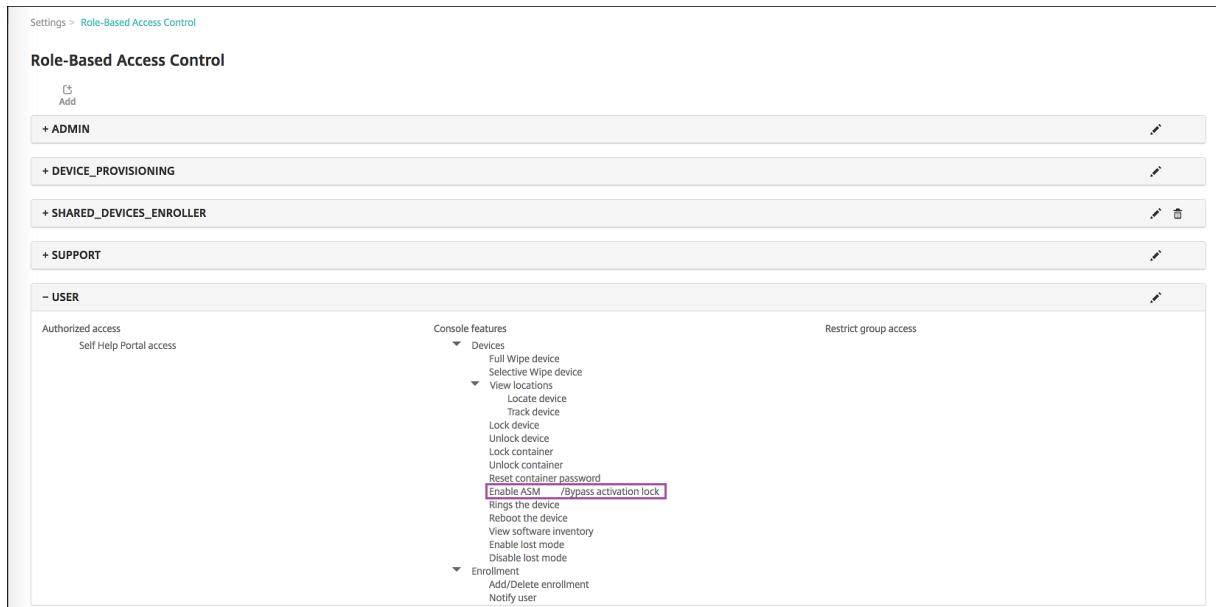
활성화 잠금을 설정하려면 관리 > 장치에서 장치를 선택하고 보안을 클릭한 후 **ASM** 활성화 잠금을 클릭합니다.



ASM 에스크로 키와 **ASM** 활성화 잠금 바이패스 코드 속성은 장치 세부 정보에 표시됩니다.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div>1 General</div> <div>2 Properties</div> <div>3 User Properties</div> <div>4 Assigned Policies</div> <div>5 Apps</div> <div>6 Media</div> <div>7 Actions</div> <div>8 Delivery Groups</div> <div>9 iOS Profiles</div> <div>10 iOS Provisioning Profiles</div> <div>11 Certificates</div> <div>12 Connections</div> <div>13 MDM Status</div>		
<div><div>– Security information</div><div>ASM Automated Device Enrollment escrow key</div><div>ASM Automated Device Enrollment activation lock bypass code</div><div>Activation lock bypass code</div><div>Activation lock enabled</div><div>Hardware encryption capabilities</div><div>Internal storage encrypted</div><div>Jailbroken/Rooted</div><div>MDM lost mode enabled</div><div>Passcode compliant</div><div>Passcode compliant with configuration</div><div>Passcode present</div><div>Supervised</div></div> <div><div>– Storage space</div><div>Available storage space</div><div>Total storage space</div></div>		

ASM 활성화 잠금에 대한 RBAC 권한은 장치 >**ASM** 활성화 잠금 바이패스입니다.



Apple 앱 배포

March 15, 2024

XenMobile 은 장치에 배포되는 앱을 관리합니다. 다음 유형의 iOS/iPadOS 및 macOS 앱을 구성하고 배포할 수 있습니다.

- **공용 앱 스토어 (iOS/iPadOS 전용):** Apple App Store 또는 Google Play 와 같은 공용 앱 스토어에서 무료 또는 유료로 제공되는 앱이 포함됩니다. 예를 들어 GoToMeeting 이 포함됩니다.
- **Enterprise(iOS/iPadOS/macOS):** MDX 가 지원되지 않으며 MDX 앱과 연결된 정책이 포함되지 않는 기본 앱입니다.
- **MDX(iOS/iPadOS 전용):** MAM SDK 로 준비되거나 MDX Toolkit 으로 래핑된 앱입니다. 이러한 앱에는 MDX 정책이 포함됩니다. 내부 및 공용 스토어에서 MDX 앱을 얻을 수 있습니다.
- **볼륨 구매 (iOS/iPadOS/macOS):** Apple 볼륨 구매 프로그램을 통해 관리되는 라이선스가 적용된 앱입니다.
- **iOS 사용자 지정 앱 (iOS/iPadOS 전용):** 사내에서 또는 타사에서 개발한 독점 B2B 앱입니다.

다양한 앱 유형에 관한 정보는 [앱 추가](#)에서 확인하십시오.

배포 중에는 Apple Business Management(ABM) 또는 Apple School Management(ASM) 계정이 필요한 배포가 있습니다. 자세한 내용은 다음 섹션을 참조하십시오.

Citrix 에서는 앱 및 배포 방식의 각 유형에 대해 구성 집합을 사용하기를 권장합니다. 기타 플랫폼의 앱 배포에 관한 정보는 [앱 추가](#)에서 확인하십시오. 다음 섹션에서는 iOS 앱 구성에 관해 더 자세히 알아봅니다.

앱 배포의 일반적인 단계

시나리오	1 단계: 계정 연결	2 단계: 앱 추가 및 구성	3 단계: 배달 그룹 구성 및 앱 배포
공용 앱 스토어 앱, Citrix 이동성 앱 포함	해당 없음	XenMobile 에서: 구성 > 앱으로 이동하여 iPhone 또는 iPad 용 공용 앱 스토어 앱을 추가합니다. 앱을 구성하고 배달 그룹에 할당합니다.	XenMobile 에서: 배달 그룹을 사용하여 앱을 구성하고 배포합니다.
Apple 볼륨 구매를 통해 제공되는 공용 앱 스토어 앱, Citrix 이동성 앱 포함	Apple 배포 프로그램에 등록합니다. XenMobile 에서: 설정 > 볼륨 구매로 이동하여 볼륨 구매 계정을 추가합니다.	ABM 또는 ASM 에서: Apps 및 Books에서 앱을 구매하고 추가합니다. XenMobile 에서: 구성 > 앱으로 이동한 다음 앱을 구성하고 배달 그룹에 할당합니다.	XenMobile 에서: 배달 그룹을 사용하여 앱을 구성하고 배포합니다.
엔터프라이즈 앱	해당 없음	XenMobile 에서: 구성 > 앱으로 이동합니다. 추가를 클릭한 다음 엔터프라이즈를 클릭합니다. IPA 파일을 업로드합니다. 앱을 구성하고 배달 그룹에 할당합니다.	XenMobile 에서: 배달 그룹을 사용하여 앱을 구성하고 배포합니다.
MDX 앱	해당 없음	XenMobile 에서: 구성 > 앱으로 이동합니다. 추가를 클릭한 다음 MDX 를 클릭합니다. 플랫폼에 대해 iPad/iPhone 을 선택해야 합니다. MDX 파일을 업로드합니다. 앱을 구성하고 배달 그룹에 할당합니다.	XenMobile 에서: 배달 그룹을 사용하여 앱을 구성하고 배포합니다.
Apple 볼륨 구매로 배포된 MDX 앱	Apple 배포 프로그램에 등록합니다. XenMobile 에서: 설정 > 볼륨 구매로 이동하여 볼륨 구매 계정을 추가합니다.	ABM 에서: Apps 및 Books에서 앱을 구매하고 추가합니다. ABM 계정에 앱을 연결합니다. XenMobile 에서: 구성 > 앱으로 이동한 다음 앱을 구성하고 배달 그룹에 할당합니다.	XenMobile 에서: 배달 그룹을 사용하여 앱을 구성하고 배포합니다.

시나리오	1 단계: 계정 연결	2 단계: 앱 추가 및 구성	3 단계: 배달 그룹 구성 및 앱 배포
사용자 지정 앱	Apple 배포 프로그램에 등록합니다. XenMobile 에서: 설정 > 볼륨 구매로 이동하여 볼륨 구매 계정을 추가합니다.	ABM 에서: 앱을 App Store 에 비공개 앱으로 추가합니다. 앱을 ABM 계정에 연결합니다. XenMobile 에서: 구성 > 앱으로 이동한 다음 앱을 구성하고 배달 그룹에 할당합니다.	XenMobile 에서: 배달 그룹을 사용하여 앱을 구성하고 배포합니다.
MDX 지원 사용자 지정 앱	Apple 배포 프로그램에 등록합니다. XenMobile 에서: 설정 > 볼륨 구매로 이동하여 볼륨 구매 계정을 추가합니다.	ABM 에서: 앱을 App Store 에 비공개 앱으로 추가합니다. 앱을 ABM 계정에 연결합니다. XenMobile 에서: 구성 > 앱으로 이동한 다음 MDX 파일을 업로드합니다. 앱을 구성하고 배달 그룹에 할당합니다.	XenMobile 에서: 배달 그룹을 사용하여 앱을 구성하고 배포합니다.

공용 앱 스토어 앱

App Store 에서 제공되는 유료 및 무료 앱을 XenMobile 에 추가할 수 있습니다.

기능 가용성

장치 감독 필요	아니요
사용자 등록 모드 제공	아니요
사용 가능한 플랫폼	iOS/iPadOS

1 단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 추가를 클릭합니다.
2. 공용 앱 스토어를 클릭합니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. 플랫폼에 대해 **iPhone** 또는 **iPad** 를 선택합니다.

4. 검색 상자에 앱 이름을 입력하고 검색을 클릭합니다.

Device Policies
Apps
Media
Actions
ShareFile
Enrollment Profiles
Delivery Groups

Public App Store
1 App Information
2 Platform
☒ iPhone
☒ iPad
☒ Google Play
☒ Android for Work
☐ Windows Desktop/Tablet
☐ Windows Phone
3 Approvals (optional)
4 Delivery Group Assignments (optional)

iPhone App Settings
Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

Search results for podio in iPhone apps

Podio Podio

Podio Chat Podio

Didn't find the app you were looking for?

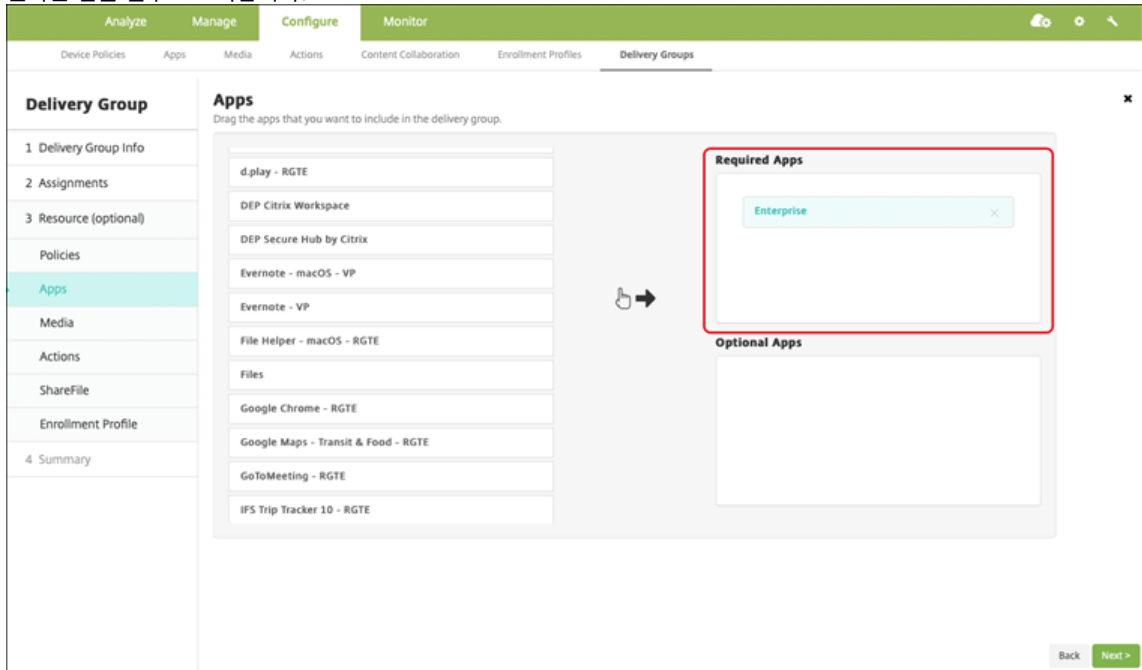
5. 검색 기준과 일치하는 앱이 표시됩니다. 원하는 앱을 클릭합니다.

6. 배달 그룹을 앱에 할당하고 저장을 클릭합니다.

2 단계: 앱 배포 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다.
2. 구성할 앱을 선택하고 편집을 클릭합니다.
3. Citrix 에서는 강제로 앱 관리 기능을 사용하기를 권장합니다.
4. 배달 그룹을 할당하고 저장을 클릭합니다.
5. 구성 > 배달 그룹 > 앱으로 이동합니다.

6. 원하는 앱을 필수로 표시합니다.



7. 구성 > 배달 그룹으로 다시 돌아갑니다.

8. 배달 그룹을 선택하고 배포를 클릭합니다.

9. 사용자는 앱을 설치하라는 요청을 받고 수락 후 앱이 백그라운드에서 설치됩니다.



Apple 볼륨 구매를 통해 제공되는 공용 앱 스토어 앱

Apple 볼륨 구매 프로그램을 통해 iOS/iPadOS 앱 라이선스를 관리할 수 있습니다. XenMobile 에 볼륨 구매 앱을 추가하려면 이러한 단계를 따릅니다.

기능 가용성

장치 감독 필요	아니요
사용자 등록 모드 제공	예
사용 가능한 플랫폼	iOS/iPadOS/macOS

1 단계: 계정 연결

1. Apple Business Manager(ABM) 또는 Apple School Manager(ASM) 에서 설정하고 등록합니다. 이러한 프로그램에 대한 자세한 내용은 [Apple 설명서](#)를 참조하십시오.
2. XenMobile 로 ABM/ASM 계정을 연결합니다. 볼륨 구매 계정 연결에 대한 자세한 내용은 [Apple 볼륨 구매](#)를 참조하십시오.
3. 볼륨 구매 계정을 추가할 경우 앱 자동 업데이트를 활성화합니다. 이 설정을 사용하면 Apple 앱 스토어에 업데이트가 나올 경우 사용자 기기의 앱이 자동으로 업데이트됩니다.

2 단계: Apple 에서 앱과 라이선스 받기

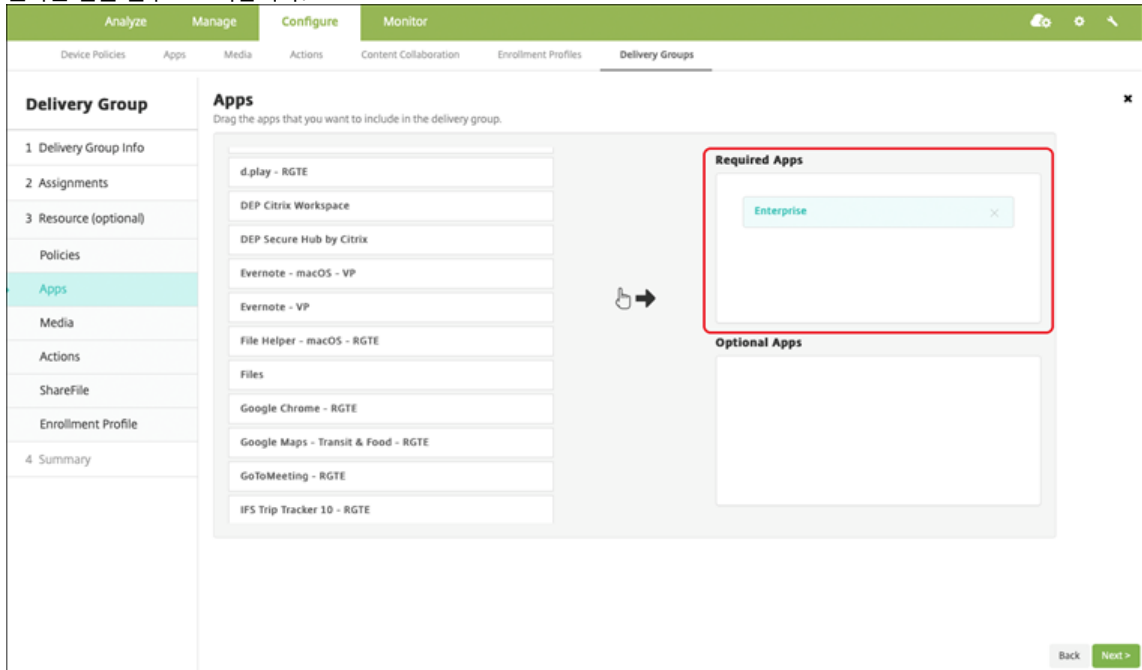
ABM/ASM 계정에서 앱을 추가합니다. Apple App Store 또는 Apple Books(iOS/iPadOS 전용) 에서 구매한 항목을 추가할 수 있습니다. 무료 앱이라도 모두 구매해야 합니다.

앱을 비즈니스에서 사용할 수 있도록 하는 방법은 [Apple 설명서](#)에서 참고하십시오.

3 단계: 앱 배포 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다.
2. 구성할 볼륨 구매 앱을 선택하고 편집을 클릭합니다.
3. **iPhone, iPad** 또는 **macOS** 중에서 플랫폼을 선택합니다.
4. Citrix 에서는 강제로 앱 관리 기능(iOS/iPadOS 전용) 을 사용하기를 권장합니다.
5. 배달 그룹을 할당하고 저장을 클릭합니다.
6. 구성 > 배달 그룹 > 앱으로 이동합니다.

7. 원하는 앱을 필수로 표시합니다.



8. 구성 > 배달 그룹으로 다시 돌아갑니다.

9. 배달 그룹을 선택하고 배포를 클릭합니다.

10. 사용자는 앱을 설치하라는 요청을 받고 수락 후 앱이 백그라운드에서 설치됩니다.



엔터프라이즈 앱

MDX 정책이 연결되어 있지 않은 기본 앱도 추가할 수 있습니다. App Store 에 없는 앱을 추가하려면 이러한 단계를 따릅니다.

기능 가용성

장치 감독 필요	아니요
사용자 등록 모드 제공	예
OS	iOS/iPadOS/macOS

1 단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 추가를 클릭합니다.
2. 엔터프라이즈를 클릭합니다.

Add App [Close]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
 Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
 Example: WorxMail

Public App Store
 Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
 Example: GoToMeeting

Web & SaaS
 Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
 Example: GoogleApps_SAML

Enterprise
 Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
 Example: Quick-iLaunch

Web Link
 A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. 앱 정보 페이지에서 다음을 구성합니다.
 - 이름: 앱을 설명하는 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 표시됩니다.
 - 설명: 앱의 선택적 설명을 입력합니다.
 - 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다.
4. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.
5. **iPhone**, **iPad** 또는 **macOS** 중에서 플랫폼을 선택합니다.
6. IPA 파일 업로드 (iOS/iPadOS) 또는 PKG 파일 업로드 (macOS)
7. 다음을 클릭합니다. 앱 세부 정보 페이지가 나타납니다.
8. 다음 설정을 구성합니다.

- 파일 이름: 필요한 경우 앱의 새 이름을 입력합니다.
- 앱 설명: 필요한 경우 앱에 대한 새 설명을 입력합니다.
- 앱 버전: 이 필드는 변경할 수 없습니다.
- 최소 **OS** 버전: 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
- 최대 **OS** 버전: 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
- 제외된 장치: 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
- **MDM** 프로필이 제거된 경우 앱 제거: MDM 프로필이 제거된 경우 장치에서 앱을 제거할지 여부를 선택합니다. 기본값은 켜짐입니다.(iOS/iPadOS 전용)
- 앱 데이터 백업 방지: 앱이 데이터를 백업하는 것을 방지할지 여부를 선택합니다. 기본값은 켜짐입니다.(iOS/iPadOS 전용)
- 강제로 앱 관리: 관리되지 않는 앱을 설치하는 경우 감독되지 않는 장치의 사용자에게 앱 관리를 허용하라는 메시지를 표시하려면 켜짐을 선택합니다. 사용자가 메시지를 수락하면 앱이 관리됩니다.(iOS/iPadOS 전용)

The screenshot shows the 'Configure' page for an 'iOS Enterprise App'. The left sidebar has a list of platforms: iOS (selected), macOS, Android (legacy DA), Samsung KNOX, Android Enterprise, Windows Phone, Windows Desktop/Tablet, Windows Mobile/CE, and Workspace Hub. The main content area has the following fields and options:

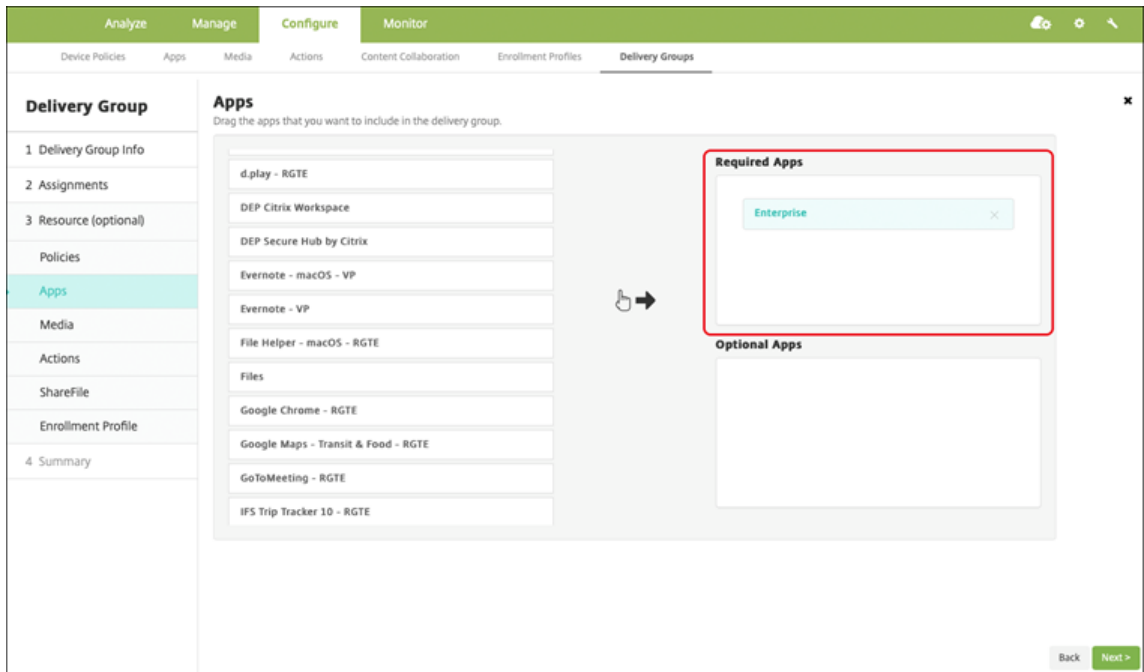
- Upload an .ipa file:** Upload button
- App name:** Hello Cordova
- Description:** Hello Cordova
- App version:** 2.0.0
- Minimum OS version:** 8.0
- Maximum OS version:** (empty)
- Excluded devices:** example: manufacturer or model ..
- Package ID:** com.cbrn.hellocordova
- Remove app if MDM profile is removed:** ON
- Prevent app data backup:** ON
- Force app to be managed:** ON ⓘ
- Deployment Rules** (expandable)
- Store Configuration** (expandable)

At the bottom right are 'Back' and 'Next >' buttons.

9. 배달 그룹을 앱에 할당하고 저장을 클릭합니다.

2 단계: 앱 배포 구성

1. XenMobile 콘솔에서 구성 > 배달 그룹으로 이동합니다. 구성할 배달 그룹을 선택하고 앱 페이지를 클릭합니다.
2. 원하는 앱을 필수로 표시합니다.



3. 구성 > 배달 그룹으로 이동합니다.
4. 배달 그룹을 선택하고 배포를 클릭합니다.
5. 사용자는 앱을 설치하라는 요청을 받고 수락 후 앱이 백그라운드에서 설치됩니다.



MDX 앱

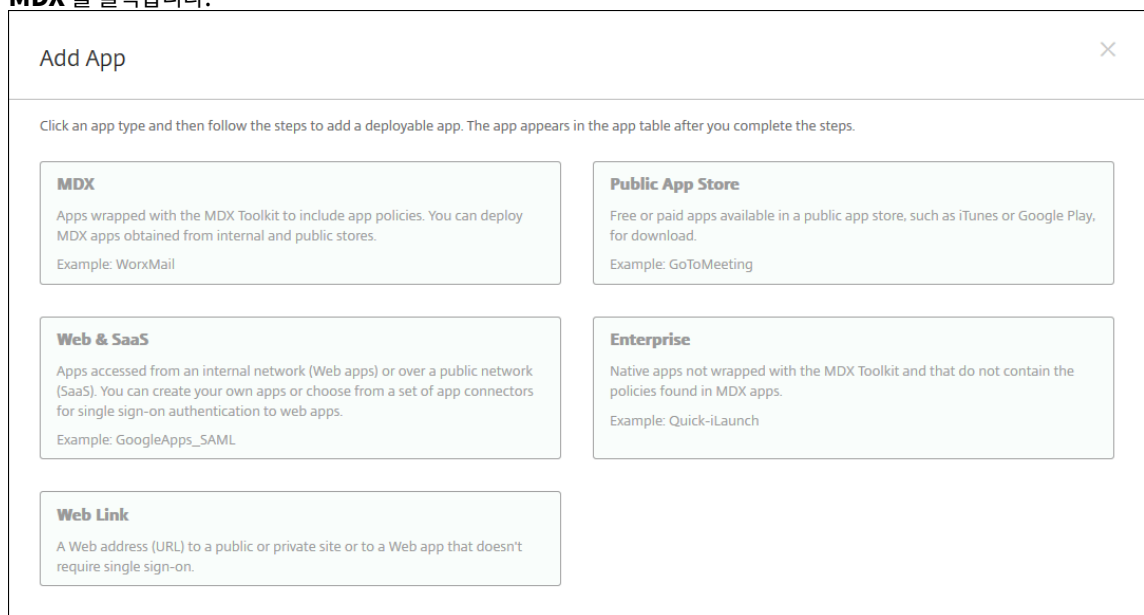
MDX 정책과 보안 기능을 사용하려면 MAM SDK 지원 또는 MDX 래핑 앱을 추가하십시오. 볼륨 구매를 사용하거나 볼륨 구매 없이도 MDX 앱을 배포할 수 있습니다.

기능 가용성

장치 감독 필요	아니요
사용자 등록 모드 제공	예
사용 가능한 플랫폼	iOS/iPadOS

1 단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 추가를 클릭합니다.
2. **MDX** 를 클릭합니다.



3. 플랫폼에 대해 **iPhone** 또는 **iPad** 를 선택합니다.
4. MDX 파일을 업로드합니다.
5. 앱 세부 정보를 구성합니다. 볼륨 구매를 통해 배포된 앱을 꺼짐으로 설정합니다. Citrix 에서는 강제로 앱 관리 기능도 사용하지를 권장합니다.

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

File name *	<input type="text" value="Secure Mail"/>
App Description *	<input type="text" value="Managed Enterprise Application"/>
App version	<input type="text" value="19.3.5"/>
Package ID	<input type="text" value="XGFUKY3NSP.com.citrix.mail.ios"/>
Minimum OS version	<input type="text" value="10.0"/>
Maximum OS version	<input type="text"/>
Excluded devices	<input type="text" value="example: manufacturer or model, ..."/>
Remove app if MDM profile is removed	<input checked="" type="checkbox"/> ON
Prevent app data backup	<input checked="" type="checkbox"/> ON
Force app to be managed	<input checked="" type="checkbox"/> ON ⓘ
App deployed via Volume purchase	<input type="checkbox"/> OFF ⓘ
▼ MDX Policies	
Authentication	
Device passcode	<input type="checkbox"/> OFF ⓘ

6. MDX 정책을 구성합니다. 필수 업그레이드 사용 안 함을 켜짐으로 설정합니다.

Miscellaneous Access

Disable required upgrade

ON

App update grace period (hours)

168

Erase app data on lock

OFF

Active poll period (minutes)

60

Encryption

Enable encryption

On

Database encryption exclusions

File encryption exclusions

App Interaction

Cut and copy

Restricted

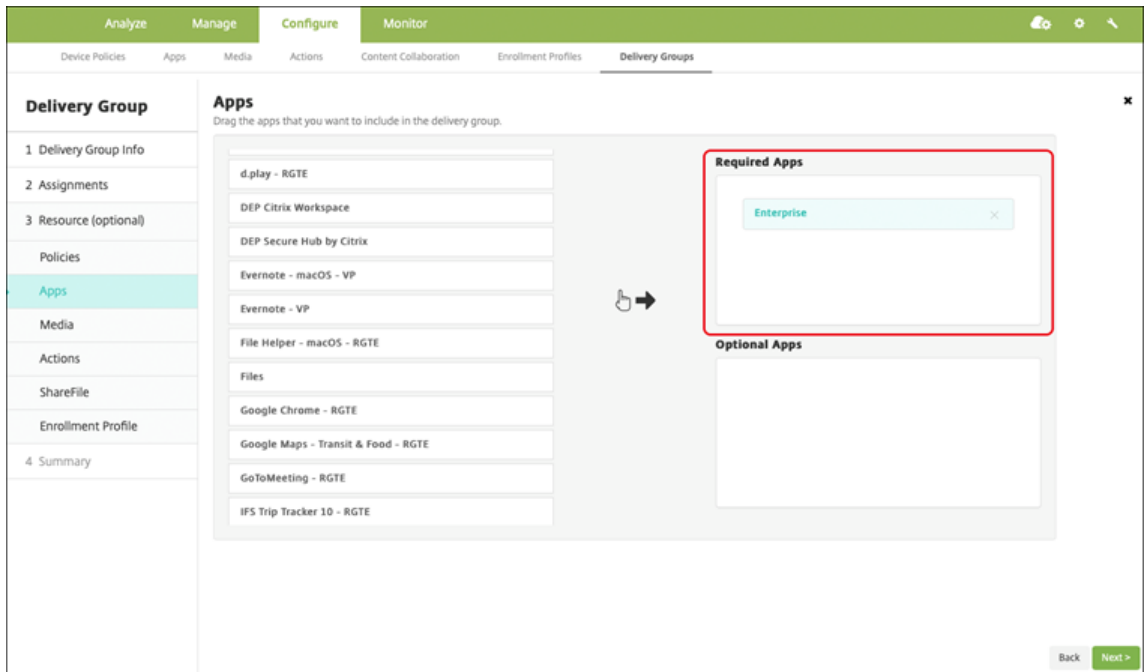
Paste

Unrestricted

7. 배달 그룹을 앱에 할당하고 저장을 클릭합니다.

2 단계: 앱 배포 구성

1. XenMobile 콘솔에서 구성 > 배달 그룹 > 앱으로 이동합니다.
2. 원하는 앱을 필수로 표시합니다.



3. 구성 > 배달 그룹으로 이동합니다.
4. 배달 그룹을 선택하고 배포를 클릭합니다.
5. 사용자는 앱을 설치하라는 요청을 받고 수락 후 앱이 백그라운드에서 설치됩니다.



Apple 볼륨 구매로 배포된 MDX 앱

MDX 정책과 보안 기능을 사용하려면 MAM SDK 지원 또는 MDX 래핑 앱을 추가하십시오. 볼륨 구매를 사용하여 앱을 배포하려면 앱이 앱 스토어에 있어야 합니다.

기능 가용성

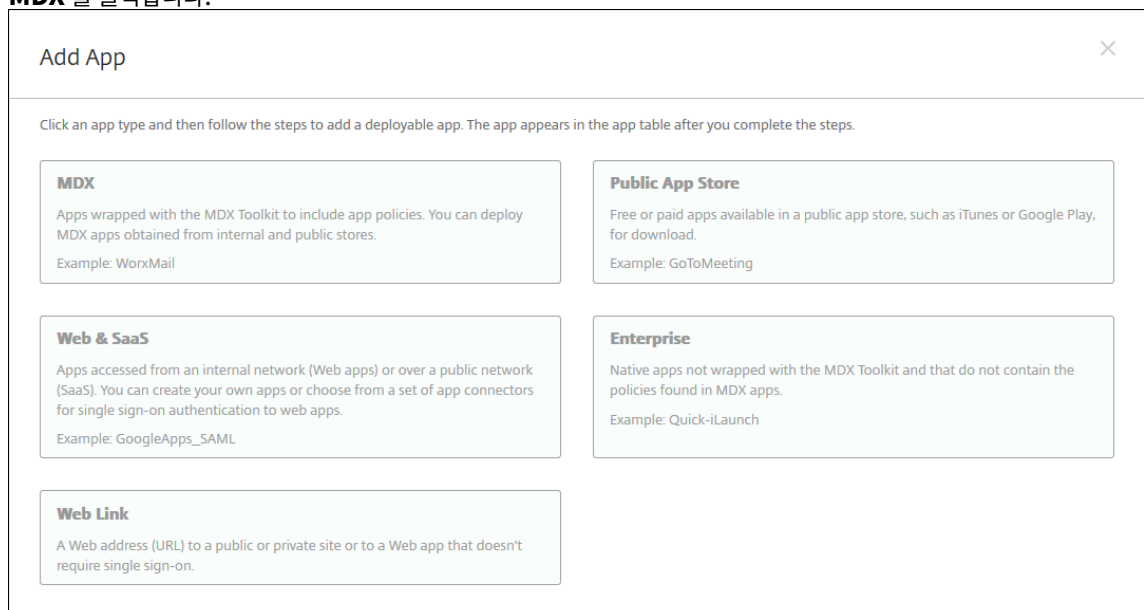
장치 감독 필요	아니요
사용자 등록 모드 제공	예
사용 가능한 플랫폼	iOS/iPadOS

1 단계: 계정 연결

1. Apple Business Manager(ABM) 또는 Apple School Manager(ASM) 에서 설정하고 등록합니다. 이러한 프로그램에 대한 자세한 내용은 [Apple 설명서](#)를 참조하십시오.
2. XenMobile 로 ABM/ASM 계정을 연결합니다. 볼륨 구매 계정 연결에 대한 자세한 내용은 [Apple 볼륨 구매](#)를 참조하십시오.
3. 볼륨 구매 계정을 추가할 경우 앱 자동 업데이트를 활성화합니다. 이 설정을 사용하면 Apple 앱 스토어에 업데이트가 나타날 경우 사용자 기기의 앱이 자동으로 업데이트됩니다.

2 단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 추가를 클릭합니다.
2. **MDX** 를 클릭합니다.



3. 플랫폼에 대해 **iPhone** 또는 **iPad** 를 선택합니다.
4. MDX 파일을 업로드합니다.
5. 앱 세부 정보를 구성합니다. 볼륨 구매를 통해 배포된 앱을 커짐으로 설정합니다. Citrix에서는 강제로 앱 관리 기능도 사용하지하기를 권장합니다.

The screenshot displays the configuration interface for an application in the XenMobile console. The fields and their values are as follows:

- File name ***: Secure Mail
- App Description ***: Managed Enterprise Application
- App version**: 19.3.5
- Package ID**: XGFUKY3N5P.com.citrix.mail.ios
- Minimum OS version**: 10.0
- Maximum OS version**: (empty field)
- Excluded devices**: example: manufacturer or model, ...
- Remove app if MDM profile is removed**: ON (toggle switch)
- Prevent app data backup**: ON (toggle switch)
- Force app to be managed**: ON (toggle switch) with a help icon (i)
- App deployed via Volume purchase**: ON (toggle switch) with a help icon (i)
- ▼ MAM SDK Policies**:
 - Authentication**:
 - Device passcode**: OFF (toggle switch) with a help icon (i)

6. MDX 정책을 구성합니다. 필수 업그레이드 사용 안 함을 커짐으로 설정합니다.

Miscellaneous Access

Disable required upgrade

ON

?

App update grace period (hours)

168

?

Erase app data on lock

OFF

?

Active poll period (minutes)

60

?

Encryption

Enable encryption

On

?

Database encryption exclusions

?

File encryption exclusions

?

App Interaction

Cut and copy

Restricted

?

Paste

Unrestricted

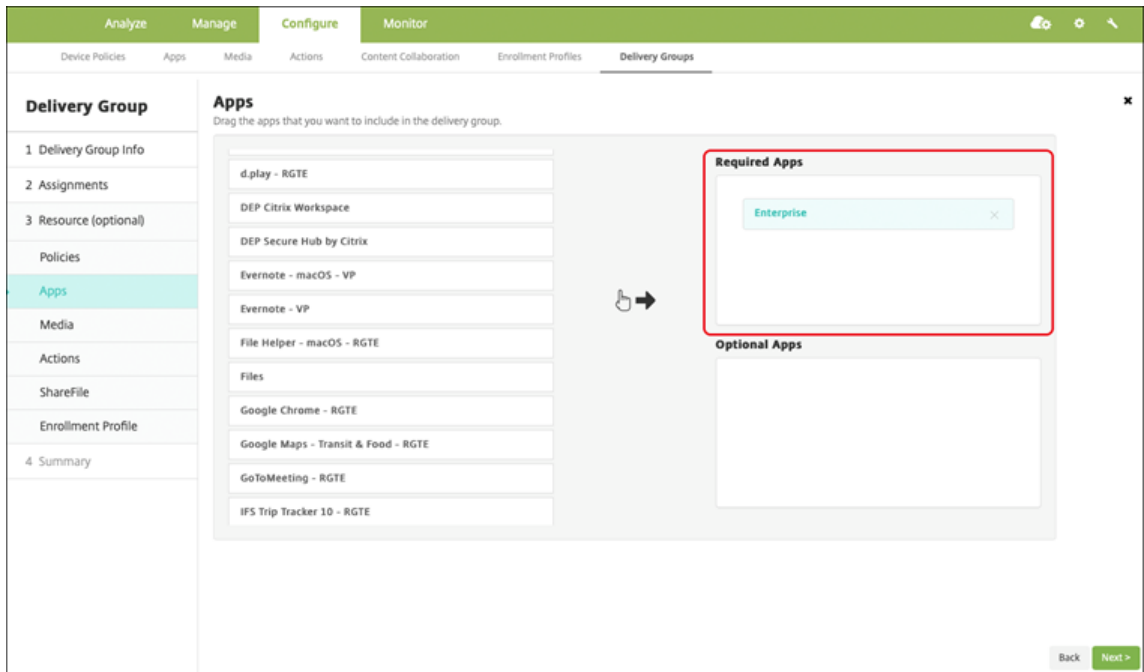
?

7. 각 플랫폼마다 배달 그룹을 앱에 할당하고 저장을 클릭합니다.

이 구성으로 인해 이 앱에 대한 항목 2 개가 앱 목록에 나열됩니다. 구성할 앱을 선택할 경우 유형이 **MDX** 인 앱을 선택합니다.

3 단계: 앱 배포 구성

1. XenMobile 콘솔에서 구성 > 배달 그룹 > 앱으로 이동합니다.
2. 원하는 볼륨 구매 앱을 필수로 표시합니다.



3. 구성 > 배달 그룹으로 이동합니다.
4. 배달 그룹을 선택하고 배포를 클릭합니다.
5. 사용자는 앱을 설치하라는 요청을 받고 수락 후 앱이 백그라운드에서 설치됩니다.



사용자 지정 앱

사용자 지정 앱은 독점적 B2B 앱입니다. XenMobile 및 Apple 볼륨 구매를 사용하여 비공개로 안전하게 독점 앱을 배포할 수 있습니다. 이러한 앱은 특정 파트너, 클라이언트, 프랜차이즈, 내부 직원에게 배포할 수 있습니다.

기능 가용성

장치 감독 필요	아니요
사용자 등록 모드 제공	예
사용 가능한 플랫폼	iOS/iPadOS

사용자 지정 앱에 대한 요구 사항

- Apple Business Manager 또는 Apple School Manager 계정
- Apple 볼륨 구매 계정 (iOS 7 이상인 장치 필요)
- 다음 Apple 등록 모드 중 하나를 사용하여 XenMobile 에서 장치를 등록합니다.
 - 자동화된 장치 등록
 - 장치 등록
 - 사용자 등록

1 단계: 계정 연결

볼륨 구매를 사용하여 사용자 지정 앱을 배포하려면 볼륨 구매 계정을 XenMobile 에 연결합니다.

1. Apple Business Manager(ABM) 에서 설정하고 등록합니다. 이러한 프로그램에 대한 자세한 내용은 [Apple 설명서](#)를 참조하십시오.
2. XenMobile 로 ABM 계정을 연결합니다. 볼륨 구매 계정 연결에 대한 자세한 내용은 [Apple 볼륨 구매](#)를 참조하십시오.
3. 볼륨 구매 계정을 추가할 경우 앱 자동 업데이트를 활성화합니다. 이 설정을 사용하면 Apple 앱 스토어에 업데이트가 나탈 경우 사용자 기기의 앱이 자동으로 업데이트됩니다.

2 단계: ABM 에서 앱 구성

ABM 계정에서 앱을 추가합니다. 자체 사용자 지정 앱을 업로드하고 배포하거나 다른 조직의 사용자 지정 앱에 대한 라이선스를 구매할 수 있습니다. ABM 의 사용자 지정 앱 추가 및 사용에 대한 자세한 정보는 [Apple 설명서](#)에서 확인하십시오.

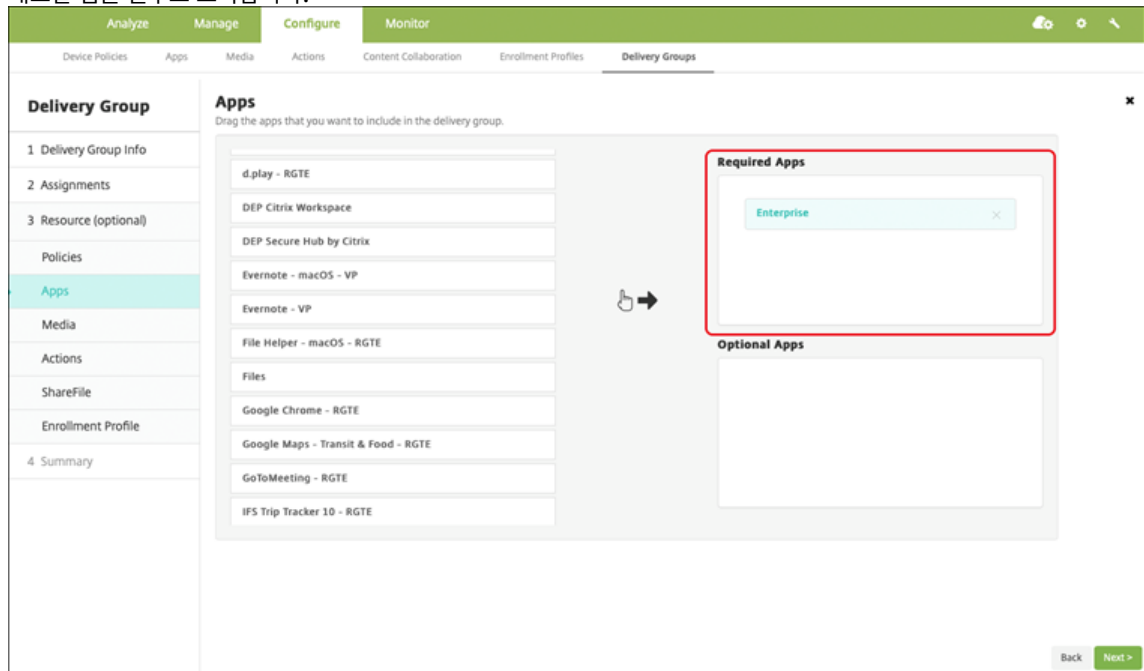
3 단계: XenMobile 에서 앱 추가 및 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 앱 목록에 볼륨 구매 앱이 표시됩니다.

2. 구성할 앱을 선택합니다. 편집을 클릭합니다.
3. **iPhone, iPad** 또는 **macOS** 중에서 플랫폼을 선택합니다.
4. 앱을 배포할 배달 그룹을 선택합니다. 저장을 클릭합니다.

4 단계: 앱 배포 구성

1. XenMobile 콘솔에서 구성 > 배달 그룹 > 앱으로 이동합니다.
2. 배포할 앱을 필수로 표시합니다.



3. 구성 > 배달 그룹으로 다시 돌아갑니다.
4. 배포할 배달 그룹을 선택하고 배포를 클릭합니다.
5. 사용자가 앱 배포 요청을 받습니다. 사용자가 요청을 수락하면 앱이 백그라운드에서 설치됩니다.



MDX 지원 사용자 지정 앱

MDX 정책과 보안 기능을 사용하려면 MAM SDK 지원 또는 MDX 래핑 사용자 지정 앱을 추가하십시오.

기능 가용성

장치 감독 필요	아니요
사용자 등록 모드 제공	예
사용 가능한 플랫폼	iOS/iPadOS

1 단계: 계정 연결

볼륨 구매를 사용하여 사용자 지정 앱을 배포하려면 볼륨 구매 계정을 XenMobile 에 연결합니다.

1. Apple Business Manager(ABM) 에서 설정하고 등록합니다. 이러한 프로그램에 대한 자세한 내용은 [Apple 설명서](#)를 참조하십시오.
2. XenMobile 로 ABM 계정을 연결합니다. 볼륨 구매 계정 연결에 대한 자세한 내용은 [Apple 볼륨 구매](#)를 참조하십시오.
3. 볼륨 구매 계정을 추가할 경우 앱 자동 업데이트를 활성화합니다. 이 설정을 사용하면 Apple 앱 스토어에 업데이트가 나타날 경우 사용자 기기의 앱이 자동으로 업데이트됩니다.

2 단계: ABM 에서 앱 구성

ABM 계정에서 앱을 추가합니다. 자체 사용자 지정 앱을 업로드하고 배포하거나 다른 조직의 사용자 지정 앱에 대한 라이선스를 구매할 수 있습니다. ABM 의 사용자 지정 앱 추가 및 사용에 대한 자세한 정보는 [Apple 설명서](#)에서 확인하십시오.

3 단계: XenMobile 에서 앱 추가 및 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 추가를 클릭합니다.
2. **MDX** 를 클릭합니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. **iPhone** 또는 **iPad** 플랫폼을 선택합니다.
4. 추가할 앱의 MDX 파일을 업로드합니다.
5. 앱 세부 정보를 구성합니다. 볼륨 구매를 통해 배포된 앱을 커짐으로 설정합니다. Citrix에서는 강제로 앱 관리 기능도 사용하지기를 권장합니다.

File name *	Secure Mail
App Description *	Managed Enterprise Application
App version	19.3.5
Package ID	XGFKY3NSP.com.citrix.mail.ios
Minimum OS version	10.0
Maximum OS version	
Excluded devices	example: manufacturer or model, ...
Remove app if MDM profile is removed	ON
Prevent app data backup	ON
Force app to be managed	ON ⓘ
App deployed via Volume purchase	ON ⓘ
▼ MAM SDK Policies	
Authentication	
Device passcode	OFF ⓘ

6. MDX 정책을 구성합니다. 필수 업그레이드 사용 안 함을 켜짐으로 설정합니다.

Miscellaneous Access

Disable required upgrade

ON

?

App update grace period (hours)

168

?

Erase app data on lock

OFF

?

Active poll period (minutes)

60

?

Encryption

Enable encryption

On

?

Database encryption exclusions

?

File encryption exclusions

?

App Interaction

Cut and copy

Restricted

?

Paste

Unrestricted

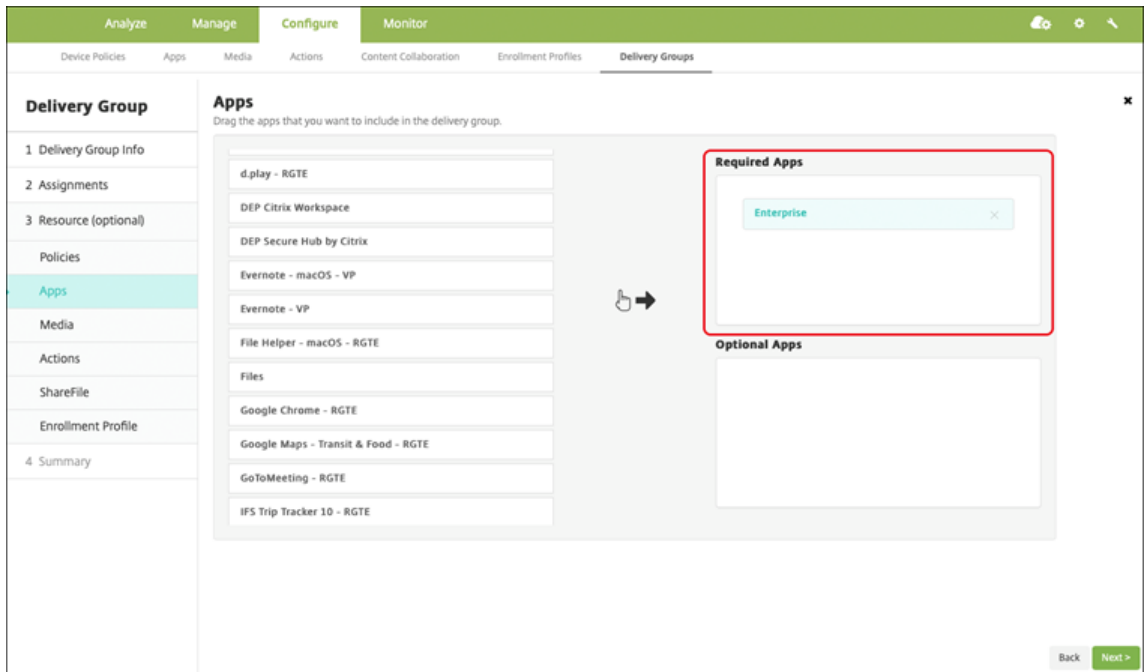
?

7. 배달 그룹을 앱에 할당하고 저장을 클릭합니다.

이 구성으로 인해 이 앱에 대한 항목 2 개가 앱 목록에 나열됩니다. 구성할 앱을 선택할 경우 유형이 **MDX** 인 앱을 선택합니다.

4 단계: 앱 배포 구성

1. XenMobile 콘솔에서 구성 > 앱으로 이동합니다. 앱 목록에 볼륨 구매 앱이 표시됩니다.
2. 구성할 앱을 선택합니다. 편집을 클릭합니다.
3. 각 플랫폼에 앱을 배포할 배달 그룹을 선택합니다. 저장을 클릭합니다.
4. 구성 > 배달 그룹 > 앱으로 다시 돌아갑니다.
5. 배포할 앱을 필수로 표시합니다.



6. 구성 > 배달 그룹으로 다시 돌아갑니다.
7. 배포할 배달 그룹을 선택하고 배포를 클릭합니다.
8. 사용자가 앱 배포 요청을 받습니다. 수락하면 앱이 백그라운드에서 설치됩니다.

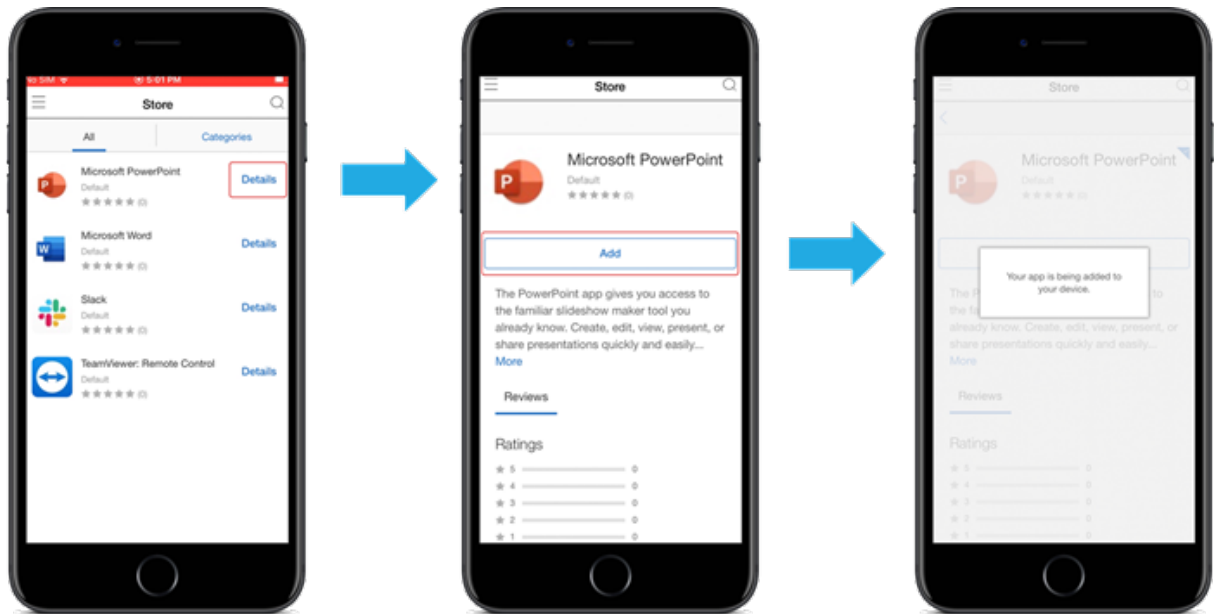


옵션 앱 (iOS/iPadOS 전용)

Citrix에서는 앱을 필수로 배포하기를 권장합니다. 필수 앱은 사용자 장치에 자동으로 설치되므로 상호 작용이 최소화됩니다. 이러한 기능을 사용하면 앱을 자동으로 업데이트할 수도 있습니다.

옵션 앱을 통해 사용자는 설치할 앱을 선택할 수 있지만 사용자는 Secure Hub를 통해 수동으로 설치를 개시해야 합니다.

옵션 앱을 설치하려면 Secure Hub를 실행하고 스토어로 이동한 다음 원하는 앱의 세부 정보를 선택하고 추가를 클릭합니다.



네트워크 액세스 제어

March 15, 2024

NAC(네트워크 액세스 제어) 솔루션을 사용하여 Android 및 Apple 장치에 대한 XenMobile 장치 보안 평가를 확장할 수 있습니다. NAC 솔루션에서 XenMobile 보안 평가를 사용하여 인증 의사 결정을 지원하고 처리할 수 있습니다. NAC 장비를 구성한 후 XenMobile에서 구성한 장치 정책 및 NAC 필터가 적용됩니다.

NAC 솔루션과 함께 XenMobile을 사용하면 QoS를 추가하고 네트워크 내부에 있는 장치를 보다 세밀하게 제어할 수 있습니다. NAC를 XenMobile과 통합하여 얻을 수 있는 장점에 대한 요약은 [액세스 제어](#)에서 확인하십시오.

다음은 XenMobile 통합이 지원되는 솔루션입니다.

- Citrix Gateway
- Cisco Identity Services Engine(ISE)
- ForeScout

다른 NAC 솔루션에 대한 통합은 보장되지 않습니다.

네트워크의 NAC 장비 사용:

- XenMobile 은 iOS, Android Enterprise 및 Android 장치의 엔드포인트 보안 기능으로 NAC 를 지원합니다.
- XenMobile 에서 필터를 사용하여 규칙 또는 속성에 따라 장치를 NAC 준수 또는 비준수 장치로 설정할 수 있습니다. 예:
 - XenMobile 의 관리되는 장치가 지정된 기준을 충족하지 않으면 XenMobile 이 해당 장치를 비준수 장치로 표시합니다. 네트워크에서 규정을 준수하지 않는 장치는 NAC 장비에 의해 차단됩니다.
 - XenMobile 의 관리되는 장치에 비준수 앱이 설치되어 있는 경우 NAC 필터에 의해 VPN 연결이 차단될 수 있습니다. 따라서 비준수 사용자 장치는 VPN 을 통해 앱이나 웹 사이트에 액세스할 수 없습니다.
 - Citrix Gateway 를 NAC 에 사용하는 경우 분할 터널링을 사용하도록 설정하여 Citrix Gateway 플러그인에 서 불필요한 네트워크 트래픽을 Citrix Gateway 로 보내는 것을 방지할 수 있습니다. 분할 터널링에 대한 자세한 내용은 [분할 터널링 구성](#)을 참조하십시오.

지원되는 **NAC** 준수 필터

XenMobile Server 는 다음과 같은 NAC 준수 필터를 지원합니다.

익명 장치: 장치가 익명 모드인지 확인합니다. 이 확인은 장치가 다시 연결할 때 XenMobile 이 사용자를 다시 인증할 수 없는 경우 사용할 수 있습니다.

Samsung Knox 증명 실패: 장치가 Samsung Knox 증명 서버의 쿼리에 실패했는지 확인합니다.

금지된 앱: 장치에 앱 액세스 장치 정책에 정의된 금지된 앱이 있는지 확인합니다. 해당 정책에 대한 자세한 내용은 [앱 액세스 장치 정책](#)을 참조하십시오.

비활성 장치: 서버 속성의 장치 비활성 일 수 임계값 설정에 정의된 대로 장치가 비활성 상태인지 확인합니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.

누락된 필수 앱: 앱 액세스 정책에 정의된 대로, 장치에 필수 앱이 누락되었는지 확인합니다.

비추천 앱: 앱 액세스 정책에 정의된 대로, 장치에 비추천 앱이 있는지 확인합니다.

규정을 준수하지 않는 암호: 사용자 암호가 규정을 준수하는지 확인합니다. iOS 및 Android 장치에서 XenMobile 은 현재 장치에 있는 암호가 장치로 보낸 암호 정책을 준수하는지 여부를 확인할 수 있습니다. 예를 들어 iOS 에서는 XenMobile 이 암호 정책을 장치에 보내는 경우 60 분 내에 암호를 설정해야 합니다. 사용자가 암호를 설정하기 전에 암호가 규정을 준수하지 않을 수 있습니다.

규정 위반 장치: 규정 위반 장치 속성에 따라 장치가 규정을 위반하는지 여부를 확인합니다. 일반적으로 XenMobile API 를 사용하는 자동화된 작업 또는 타사에서는 이 장치 속성을 변경합니다.

해지된 상태: 장치 인증서가 해지되었는지 여부를 확인합니다. 해지된 장치는 다시 권한이 부여될 때까지 다시 등록할 수 없습니다.

루팅된 Android 및 탈옥 iOS 장치: Android 또는 iOS 장치가 탈옥되어 있는지 확인합니다.

관리되지 않는 장치: 장치가 여전히 XenMobile 제어 하에 관리되는 상태에 있는지 확인합니다. 예를 들어 MAM 로 등록된 장치나 등록되지 않은 장치는 관리되지 않습니다.

참고:

묵시적 준수/비준수 필터는 XenMobile 로 관리되는 장치에만 기본값을 설정합니다. 예를 들어 차단된 앱이 설치된 장치 또는 등록되지 않은 장치는 비준수로 표시됩니다. 이러한 장치는 NAC 장비에 의해 네트워크에서 차단됩니다.

구성 개요

NAC 구성 요소를 나열된 순서대로 구성하는 것이 좋습니다.

1. NAC 를 지원하도록 장치 정책 구성:

iOS 장치의 경우:[NAC 를 지원하도록 VPN 장치 정책 구성](#)을 참조하십시오.

Android Enterprise 장치의 경우:[Citrix SSO 에 대한 Android Enterprise 관리되는 구성 만들기](#)를 참조하십시오.

Android 장치의 경우:[Android 용 Citrix SSO 프로토콜 구성](#)을 참조하십시오.

2. XenMobile 에서 NAC 필터 사용.

3. NAC 솔루션 구성:

- Citrix Gateway, NAC 를 지원하도록 Citrix Gateway 정책 업데이트에 자세히 설명되어 있습니다.
장치에 Citrix SSO 를 설치해야 합니다. [Citrix Gateway 클라이언트](#)를 참조하십시오.
- Cisco ISE: Cisco 설명서를 참조하십시오.
- ForeScout: ForeScout 설명서를 참조하십시오.

XenMobile 에서 NAC 필터 사용

1. XenMobile 콘솔에서 설정 > 네트워크 액세스 제어로 이동합니다.

Settings > Network Access Control

Network Access Control

Enables device compliance.

Set as not compliant:

- ☐ Anonymous Devices
- ☐ Failed Samsung KNOX attestation
- ☐ Forbidden Apps
- ☐ Inactive Devices
- ☐ Missing Required Apps
- ☐ Non-Suggested Apps
- ☐ Noncompliant Password
- ☐ Out of Compliance Devices
- ☐ Revoked Status
- ☐ Rooted Android and Jailbroken iOS Devices
- ☐ Unmanaged Devices

Cancel Save

2. 사용하려는 규정 비준수 상태로 설정 필터에 대한 확인란을 선택합니다.

3. 저장을 클릭합니다.

NAC 를 지원하도록 Citrix Gateway 정책 업데이트

VPN 가상 서버에서 고급 (클래식 아님) 인증 및 VPN 세션 정책을 구성해야 합니다.

아래의 단계는 다음과 같은 특성의 Citrix Gateway 를 업데이트합니다.

- XenMobile Server 환경과 통합됩니다.
- 또는 XenMobile Server 환경의 일부가 아닌 VPN 용으로 설정되었고 XenMobile 에 연결할 수 있습니다.

가상 VPN 서버의 콘솔 창에서 다음을 수행합니다. 명령 및 예제의 IP 주소는 가상의 주소입니다.

1. VPN 가상 서버에서 클래식 정책을 사용하는 경우 모든 클래식 정책을 제거하고 바인딩 해제합니다. 확인하려면 다음을 입력합니다.

```
show vpn vserver <VPN_VServer>
```

클래식이라는 단어가 포함된 모든 결과를 제거합니다. 예: VPN Session Policy Name: PL_OS_10 .10.1.1 Type: Classic Priority: 0

정책을 제거하려면 다음을 입력합니다.

```
unbind vpn vsrver <VPN_VServer> -policy <policy_name>
```

2. 다음을 입력하여 해당하는 고급 세션 정책을 만듭니다.

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

예: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. 다음을 입력하여 정책을 VPN 가상 서버에 바인딩합니다.

```
bind vpn vsrver _XM_XenMobileGateway -policy vpn_nac -priority  
100
```

4. 다음을 입력하여 인증 가상 서버를 만듭니다.

```
add authentication vsrver <authentication vsrver name> <service  
type> <ip address>
```

예: `add authentication vsrver authvs SSL 0.0.0.0`

예제에서 0.0.0.0은 인증 가상 서버가 공개되지 않음을 의미합니다.

5. 다음을 입력하여 SSL 인증서를 가상 서버에 바인딩합니다.

```
bind ssl vsrver <authentication vsrver name> -certkeyName <  
Webserver certificate>
```

예: `bind ssl vsrver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. VPN 가상 서버의 인증 가상 서버에 인증 프로필을 연결합니다. 먼저 다음을 입력하여 인증 프로필을 만듭니다.

```
add authentication authnProfile <profile name> -authnVsName <  
authentication vsrver name>
```

예:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. 다음을 입력하여 인증 프로필을 VPN 가상 서버에 연결합니다.

```
set vpn vsrver <vpn vsrver name> -authnProfile <authn profile  
name>
```

예:

```
set vpn vsrver _XM_XenMobileGateway -authnProfile xm_nac_prof
```

8. 다음을 입력하여 Citrix Gateway 에서 장치로의 연결을 확인합니다.

```
curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check  
--header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
```

예를 들어 다음 쿼리는 환경에 등록된 첫 번째 장치 (`deviceid_1`) 의 규정 준수 상태를 확인하여 연결을 확인합니다.

```
curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header
  "X-Citrix-VPN-Device-ID: deviceid_1"
```

성공적인 결과는 다음 예제와 유사합니다.

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. 이전 단계가 성공하면 XenMobile 에 대한 웹 인증 작업을 만듭니다. 먼저 iOS VPN 플러그인에서 장치 ID 를 추출하는 정책 식을 만듭니다. 다음을 입력합니다.

```
add policy expression xm_deviceid_expression "HTTP.REQ.BODY
(10000).TYPECAST_NVLIST_T('=' '\', '& '\').VALUE(\"deviceidvalue\")"
```

10. 다음을 입력하여 요청을 XenMobile 에 보냅니다. 이 예에서 XenMobile ServerIP 는 10.207.87.82, FQDN 은 `example.em.server.com:4443`입니다.

```
add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -
serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP
/1.1\r\n"+ "Host: example.em.server.com:4443\r\n"+ "X-Citrix-VPN-
Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https
-succesRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-
Citrix-Device-State\").EQ(\"Compliant\")"
```

XenMobile NAC 의 성공적인 출력은 HTTP status 200 OK입니다. X-Citrix-Device-State 헤더의 값은 `Compliant`여야 합니다.

11. 다음을 입력하여 작업을 연결할 인증 정책을 만듭니다.

```
add authentication Policy <policy name> -rule <rule> -action <web
authentication action>
```

예: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. 다음을 입력하여 기존 LDAP 정책을 고급 정책으로 변환합니다.

```
add authentication Policy <policy_name> -rule <rule> -action <
LDAP action name>
```

예: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 다음을 입력하여 LDAP 정책을 연결할 정책 레이블을 추가합니다.

```
add authentication policylabel <policy_label_name>
```

예: `add authentication policylabel ldap_pol_label`

14. 다음을 입력하여 LDAP 정책을 정책 레이블에 연결합니다.

```
bind authentication policylabel ldap_pol_label -policyName
ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
```

15. 준수 장치를 연결하여 NAC 테스트를 수행하고 LDAP 인증에 성공하는지 확인합니다. 다음을 입력합니다.

```
bind authentication vserver <authentication vserver> -policy <web
authentication policy> -priority 100 -nextFactor <ldap policy
label> -gotoPriorityExpression END
```

16. 인증 가상 서버에 연결할 UI 를 추가합니다. 다음 명령을 입력하여 장치 ID 를 검색합니다.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule>
-action lschema_single_factor_deviceid
```

17. 다음을 입력하여 인증 가상 서버를 바인딩합니다.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -
priority 100 -gotoPriorityExpression END
```

18. LDAP 고급 인증 정책을 만들어 Secure Hub 연결을 사용하도록 설정합니다. 다음을 입력합니다.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
bind authentication vserver authvs -policy ldap_xm_test_pol -
priority 110 -gotoPriorityExpression NEXT
```

Samsung Knox

July 18, 2022

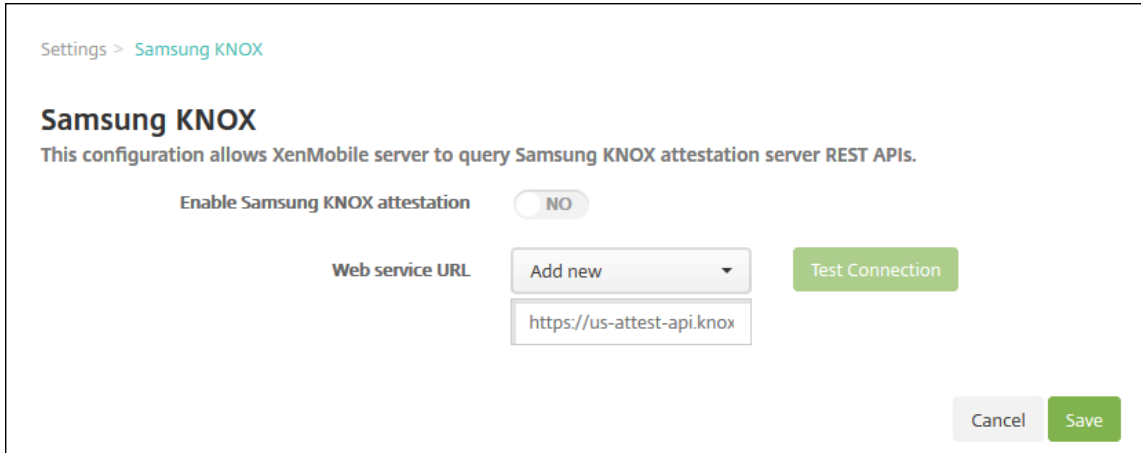
Samsung 은 XenMobile Server 와 호환되는 여러 솔루션을 제공합니다.

- XenMobile 은 호환되는 Samsung 장치에서 Samsung Knox 정책을 지원하고 확장합니다.
- Knox Service 플로그인 (KSP) 은 Knox Platform for Enterprise (KPE) 기능의 하위 집합을 지원하는 앱입니다. KPE 에 대한 Samsung 의 정보는 [엔터프라이즈용 Knox 플랫폼 구성](#) 및 [개요](#)를 참조하십시오.

XenMobile 에서 Samsung Knox 증명 서버 REST API 를 쿼리하도록 구성할 수 있습니다.

Samsung Knox 는 하드웨어 보안 기능을 사용하여 운영 체제 및 응용 프로그램에 대한 여러 수준의 보호를 제공합니다. 이 중 한 수준의 보안 기능이 증명을 통해 플랫폼에서 제공됩니다. 증명 서버는 모바일 장치 핵심 시스템 소프트웨어 (예: 부팅 로더 및 커널) 에 대한 확인을 수행합니다. 확인은 신뢰할 수 있는 부팅 시 수집된 데이터를 기반으로 런타임에 이루어집니다.

1. XenMobile 웹 콘솔에서 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 플랫폼 아래에서 **Samsung KNOX** 를 클릭합니다. **Samsung KNOX** 페이지가 나타납니다.



3. **Samsung Knox** 증명 사용에서 Samsung KNOX 증명을 사용할지 여부를 선택합니다. 기본값은 아니요입니다.
4. **Samsung KNOX** 증명 사용을 예로 설정하는 경우 웹 서비스 **URL** 옵션이 사용됩니다. 그런 다음 목록에서 다음 중 하나를 수행합니다.
 - 적절한 증명 서버를 클릭합니다.
 - 새로 추가를 클릭하고 웹 서비스 URL 을 입력합니다.
5. 연결 테스트를 클릭하여 연결을 확인합니다. 성공 또는 실패 메시지가 나타납니다.
6. 저장을 클릭합니다.

참고:

Samsung Knox Mobile Enrollment 를 사용하여 여러 Samsung Knox 장치를 각 장치에 대한 수동 구성 없이 XenMobile 또는 원하는 모바일 장치 관리자에 등록할 수 있습니다. 자세한 내용은 [Samsung KNOX 대량 등록](#)을 참조하십시오.

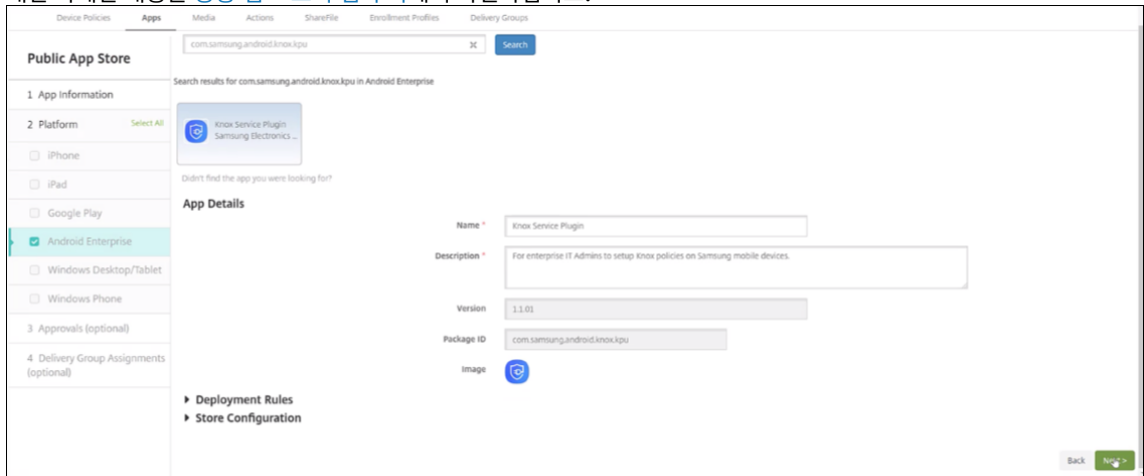
Knox 서비스 플러그인 앱 추가

Knox 와 함께 Android Enterprise 를 사용하려는 경우 KSP(Knox 서비스 플러그인) 를 XenMobile 에 추가합니다. KSP 앱은 AndroidOEMConfig 를 사용하여 보안 정책, 유연한 VPN 구성 및 생체 인증 제어와 같은 기능을 지원합니다. AndroidOEMConfig 를 사용하면 OEM 및 EMM(엔드포인트 모빌리티 관리자) 에서 맞춤형 OEM API 를 지원할 수 있습니다. 이러한 API 는 Android Enterprise 를 통해 지원되지 않는 사용 사례에 적용됩니다.

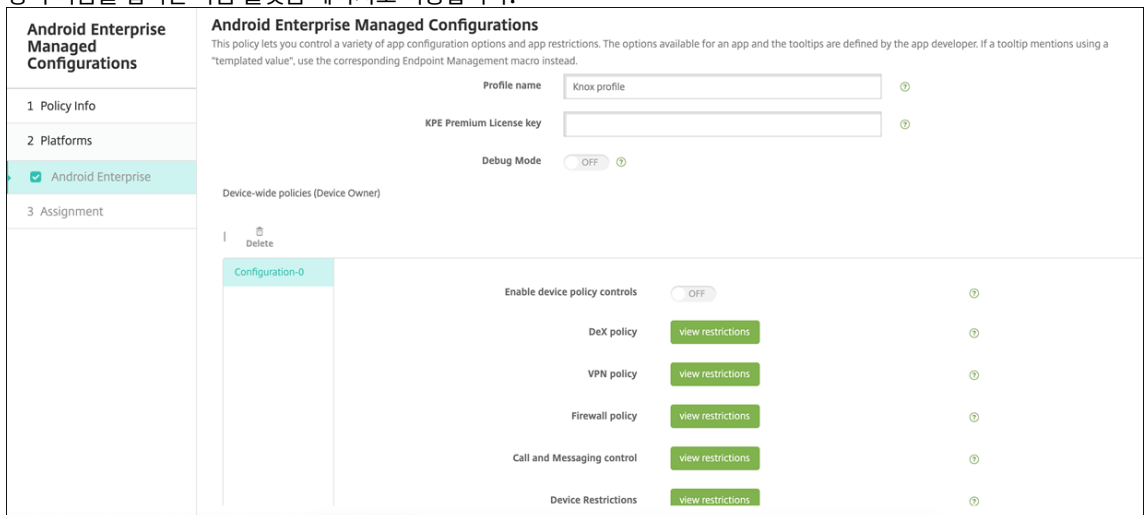
KSP 에 대한 자세한 내용은 [Knox 서비스 플러그인 가이드](#)를 참조하십시오.

1. Google 계정에 로그인하고 <https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu>로 이동합니다. Knox 서비스 플러그인 앱을 승인합니다.

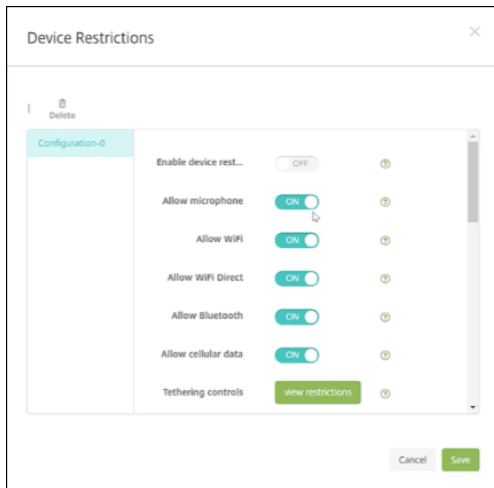
2. XenMobile 콘솔에 로그인하고 Knox 서비스 플러그인을 공용 앱 스토어 앱으로 추가합니다. 공용 앱 스토어 앱 추가에 대한 자세한 내용은 [공용 앱 스토어 앱 추가](#)에서 확인하십시오.



3. XenMobile 콘솔에서 구성 > 장치 정책으로 이동합니다. 추가를 클릭합니다.
4. 관리되는 구성을 클릭합니다. 대화 상자가 나타나면 메뉴에서 **Knox** 서비스 플러그인을 선택합니다. 관리되는 구성 정책에 대한 자세한 내용은 [관리되는 구성 정책](#)을 참조하십시오.
5. 정책 이름을 입력한 다음 플랫폼 페이지로 이동합니다.



6. 플랫폼 페이지에서 Knox 프로파일의 프로필 이름을 입력하고 Samsung의 **KPE Premium** 라이선스 키를 입력합니다. 이러한 필드 아래에 표시되는 정책은 Knox 배포에서 가져온 것입니다. Knox 정책에 대한 자세한 내용은 이 섹션의 앞부분에 참조된 Knox Service Admin Plug-in Guide(Knox 서비스 관리 플러그인 가이드)를 참조하십시오.



7. 다음을 클릭하고 정책에 대한 배포 규칙을 구성합니다.
8. 저장을 클릭합니다.

Samsung Knox 대량 등록

March 15, 2024

여러 Samsung Knox 장치를 각 장치에 대한 수동 구성 없이 XenMobile 또는 Mobile Device Manager 에 등록하려면 Knox Mobile Enrollment 를 사용합니다. 이 등록은 최초 사용 시에 또는 공장 기본값으로 재설정 이후에 발생합니다. 또한 관리자가 장치에 직접 사용자 이름과 암호를 전달할 수 있으므로 사용자가 등록 시 정보를 입력할 필요가 없습니다.

참고:

Knox Mobile Enrollment 설정은 XenMobile Knox 컨테이너와 관련 없습니다. Knox Mobile Enrollment 에 대한 자세한 내용은 [Knox Mobile Enrollment 관리 가이드](#)를 참조하십시오.

Knox Mobile Enrollment 사전 요구 사항

- XenMobile 이 구성되고 (라이선스 및 인증서 포함) 실행 중이어야 합니다.
- Secure Hub APK 파일. Knox Mobile Enrollment 를 설정할 때 이 파일을 업로드합니다.
- KME 요구 사항 목록은 [Knox Mobile Enrollment 소개](#)를 참조하십시오.
- Samsung Knox Platform for Enterprise(PKE) 라이선스는 장치 정책을 적용하는 데 필요합니다. XenMobile 장치 정책인 Knox Platform for Enterprise 에서 라이선스 키를 제공합니다.

Secure Hub APK 파일을 다운로드하려면

Google Play 스토어로 이동하여 Android 용 Citrix Secure Hub 파일을 다운로드합니다.

방화벽 예외 구성

KNOX Mobile Enrollment 에 액세스하려면 다음 방화벽 예외를 구성합니다. 이러한 방화벽 예외 중 일부는 모든 장치에 필요하고 일부는 장치의 특정 지리적 지역에만 필요합니다.

장치 지역	URL	포트	대상
모두	https://gslb.secb2b.com	443	KNOX Mobile Enrollment 초기화를 위한 글로벌 부하 분산 장치
모두	https://gslb.secb2b.com	80	일부 제한된 레거시 장치에서 KNOX Mobile Enrollment 초기화를 위한 글로벌 부하 분산 장치
모두	umc-cdn.secb2b.com	443	Samsung 에이전트 업데이트 서버
모두	bulkenrollment.s3.amazonaws.com	80	KNOX Mobile Enrollment 고객 EULA
모두	eula.secb2b.com	443	KNOX Mobile Enrollment 고객 EULA
모두	us-be-api-mssl.samsungknox.com	443	IMEI 확인을 위한 Samsung 서버
미국	https://us-segd-api.secb2b.com	443	미국 지역용 Samsung 엔터프라이즈 게이트웨이
유럽	https://eu-segd-api.secb2b.com	443	유럽 지역용 Samsung 엔터프라이즈 게이트웨이
중국	https://china-segd-api.secb2b.com	443	중국 지역용 Samsung 엔터프라이즈 게이트웨이

참고:

[Knox Mobile Enrollment 관리 가이드](#)에서 방화벽 예외의 전체 목록을 확인할 수 있습니다.

Knox Mobile Enrollment 액세스 권한 얻기

Knox Mobile Enrollment 액세스 권한을 얻으려면 [KME 로 시작](#)에서 Samsung 설명서를 따르십시오.

Knox Mobile Enrollment 설정

Knox Mobile Enrollment 액세스 권한을 얻은 후 Knox 포털에 로그인합니다.

등록 프로세스는 일반적인 단계를 따릅니다.

1. MDM 콘솔 정보 및 설정으로 MDM 프로필을 생성합니다.

MDM 프로필은 MDM에 연결하는 방법을 장치에 알려 줍니다.

2. 장치를 MDM 프로필에 추가합니다.

장치 정보를 포함하는 CSV 파일을 업로드하거나 Google Play에서 Knox 배포 앱을 설치해서 사용할 수 있습니다.

3. 장치 소유권이 확인되면 Samsung에서 알려줍니다.

4. 사용자에게 MDM 자격 증명을 제공합니다. Wi-Fi를 사용하여 인터넷에 연결하고 메시지에 따라 장치를 등록할 것을 사용자에게 지시합니다.

MDM 프로필을 생성하려면

[Samsung 설명서에 설명된 프로필 구성](#)에 대한 단계를 따릅니다.

다음 필드 또는 단계가 나타나면 설명에 따라 다음과 같이 구성하십시오.

- **MDM 선택:** 메뉴에서 **Citrix**를 선택합니다. 장치 소유자 프로필에만 해당합니다.
- **MDM 에이전트 APK:** 장치 소유자 프로필에만 해당합니다. Secure Hub APK 다운로드 URL(<https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>)을 입력합니다.

APK 파일은 등록 중에 장치가 액세스할 수 있는 서버에 있을 수 있습니다. 등록 중 장치에서는 다음 작업을 수행합니다.

- APK 다운로드 URL에서 Secure Hub를 다운로드합니다.
- Secure Hub를 설치합니다.
- 다음에 설명된 사용자 지정 JSON 데이터로 Secure Hub를 엽니다.

.apk 파일 이름의 대문자 표시는 입력한 URL과 일치해야 합니다. 예를 들어 파일 이름이 모두 소문자이면 URL에서도 모두 소문자여야 합니다.

- **MDM 서버 URI:** MDM 서버 URI를 지정하지 마십시오. XenMobile은 Samsung MDM 프로토콜을 사용하지 않습니다.
- **사용자 지정 JSON 데이터:** Secure Hub에서 등록하려면 XenMobile 서버 주소, 사용자 이름 및 암호가 있어야 합니다. Secure Hub에서 사용자에게 메시지를 표시하지 않도록 JSON에서 해당 데이터를 제공할 수 있습니다. Secure Hub는 JSON에서 이러한 필드가 누락된 경우에만 사용자에게 서버 주소, 사용자 또는 암호를 요청하는 메시지를 표시합니다.

사용자 지정 JSON 데이터의 형식은입니다.

```
{ "serverURL": "URL", "xm_username":"Username", "xm_password":"Password"}
```

일괄 등록에 일반적인 이 예에서 Secure Hub 는 등록하는 중에 사용자에게 서버 주소 또는 자격 증명을 요청하는 메시지를 표시하지 않습니다.

```
{ "serverURL":"https://example.com/zdm", "xm_username":"userN", "xm_password":"password1234"}
{ "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2", "xm_password":"password7890"}
```

키오스크 기반 장치에 일반적인 이 예에서는 Secure Hub 가 사용자에게 다음과 같이 자격 증명을 요청하는 메시지를 표시합니다.

```
{ "serverURL":"https://example.com/zdm"}
```

Android Enterprise 의 제로 터치 등록에 대한 사용자 지정 JSON 을 입력할 수도 있습니다.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6              "serverURL":"URL", "xm_username":"username", "xm_password":"password"
7          }
8      }
9
10
11 <!--NeedCopy-->
```

장치에서 등록을 시작할 때 지정된 URL 에서 Secure Hub 를 다운로드하고 Secure Hub 를 설치한 다음 엽니다.

추가 구성

구성에 대한 자세한 정보는 다음 [Samsung 설명서 페이지](#)에서 확인하십시오.

- **장치 구성:** 장치를 대량으로 추가합니다.
- **Samsung Knox 배포 앱:** Bluetooth, NFC 또는 Wi-Fi Direct 등록을 통해 디바이스를 등록합니다.
- **Knox Mobile Enrollment:** Samsung Knox 에 대한 자세한 내용은 Samsung 설명서를 참조하십시오.

버전 **2.4** 이전의 **Knox API** 를 실행하는 장치를 등록하려면

Knox API 가 버전 2.4 이전인 장치에서는 초기 장치 설정 중 일괄 등록이 시작되지 않습니다. 대신, 사용자는 등록을 시작해야 합니다. 이렇게 하려면 사용자는 Samsung 사이트로 이동하여 새로운 Mobile Enrollment 클라이언트를 다운로드하고 등록을 시작합니다.

다운로드한 등록 클라이언트는 Knox 2.4/2.4.1 장치용으로 Knox 대량 등록 포털에 구성된 것과 동일한 MDM 프로필 및 APK를 사용합니다.

일반적으로 사용자는 다음 단계를 따릅니다.

1. 장치를 켜고 Wi-Fi에 연결합니다. Mobile Enrollment가 시작되지 않거나 Wi-Fi를 사용할 수 없으면 다음을 수행합니다.
 - a) [Samsung Knox Mobile Enrollment](#)로 이동합니다.
 - b) 다음 버튼을 눌러 모바일 데이터로 장치를 등록합니다.
2. **Knox**로 등록 메시지가 나타나면 계속을 누릅니다.
3. EULA(제공되는 경우)를 읽습니다. 다음을 누릅니다.
4. 메시지가 나타나면 IT 관리자가 제공한 사용자 **ID** 및 암호를 입력합니다.

이 시점에서 사용자 자격 증명의 유효성이 검사되고 장치가 조직의 엔터프라이즈 IT 환경에 등록됩니다.

Samsung 장치에 생체 인증을 사용/사용 안 함으로 설정

XenMobile은 생체 인증으로도 알려진 지문 및 홍채 인식 인증을 지원합니다. 사용자 작업이 없어도 Samsung 장치에 대한 생체 인증을 활성화하고 비활성화할 수 있습니다. 관리자가 XenMobile에서 생체 인증을 사용하지 않도록 설정하면 사용자와 타사 앱이 이 기능을 사용하도록 설정할 수 없습니다.

1. XenMobile 콘솔에서 구성 > 장치 정책을 클릭합니다. 장치 정책 페이지가 나타납니다.
2. 추가를 클릭합니다. 새 정책 추가 페이지가 나타납니다.
3. 암호를 클릭합니다. 암호 정책 정보 페이지가 나타납니다.
4. 정책 정보 창에서 다음 정보를 입력합니다.
 - 정책 이름: 정책을 설명하는 이름을 입력합니다.
 - 설명: 필요한 경우 정책의 설명을 입력합니다.
5. 다음을 클릭합니다. 플랫폼 페이지가 나타납니다.
6. 플랫폼에서 **Android** 또는 **Samsung Knox**를 선택합니다.
7. 생체 인증 구성을 켜짐으로 설정합니다.
8. **Android**를 선택한 경우 **Samsung SAFE**에서 지문 허용 또는 홍채 허용 또는 둘 다를 선택합니다.

Passcode Policy	
1 Policy Info	Use same passcode across all users: OFF
2 Platforms	Changed characters: 0
<input type="checkbox"/> iOS	Number of times a character can occur: 0
<input type="checkbox"/> Mac OS X	Alphabetic sequence length: 0
<input checked="" type="checkbox"/> Android	Numeric sequence length: 0
<input type="checkbox"/> Samsung KNOX	Allow users to make password visible: ON
<input type="checkbox"/> Android for Work	Configure biometric authentication: ON
<input type="checkbox"/> Windows Phone	<input type="checkbox"/> Allow fingerprint
	<input checked="" type="checkbox"/> Allow iris
	Forbidden Strings

보안 동작

March 15, 2024

관리 > 장치 페이지에서 장치 및 앱 보안 동작을 수행합니다. 장치 동작에는 해지, 잠금, 잠금 해제 및 초기화가 포함됩니다. 앱 보안 동작에는 앱 잠금 및 앱 초기화가 포함됩니다.

- **활성화 잠금 바이패스:** 장치 활성화 전에 감독되는 iOS 장치에서 활성화 잠금을 제거합니다. 이 명령은 개인 Apple ID 또는 암호가 없어도 사용할 수 있습니다.
- **앱 잠금:** 장치의 모든 앱에 대한 액세스를 거부합니다. Android에서는 앱이 잠기면 사용자가 XenMobile에 로그인할 수 없습니다. iOS에서는 사용자가 로그인할 수 있지만 앱에 액세스할 수는 없습니다.
- **앱 초기화:** Secure Hub에서 사용자 계정을 제거하고 장치를 등록 취소합니다. 사용자는 앱 초기화 취소 작업을 수행할 때까지 다시 등록할 수 없습니다.
- **ASM 배포 프로그램 활성화 잠금:** Apple School Manager DEP에 등록된 iOS 장치에 대한 활성화 잠금 바이패스 코드를 생성합니다.
- **제한 사항 지우기:** 감독되는 iOS 장치에서 이 명령을 사용하면 사용자가 구성한 제한 암호 및 제한 설정을 XenMobile이 지울 수 있습니다.
- **분실 모드 활성화/비활성화:** 감독되는 iOS 장치를 분실 모드로 전환하고 장치에 표시할 메시지, 전화 번호 및 각주를 보냅니다. 이 명령을 두 번째로 보내면 장치가 분실 모드에서 해제됩니다.
- **추적 활성화:** Android 또는 iOS 장치에서 이 명령을 사용하면 XenMobile에서 특정 장치의 위치를 정의된 빈도로 폴링할 수 있습니다. 지도에서 장치의 좌표 및 위치를 보려면 관리 > 장치로 이동하고 장치를 선택한 다음 편집을 클릭합니다. 장치 정보는 일반 탭의 보안 아래에 있습니다. 추적 사용 설정을 사용하여 장치를 지속적으로 추적합니다. Secure Hub는 장치가 실행 중일 때 주기적으로 위치를 보고합니다.
- **전체 초기화:** 모든 메모리 카드를 포함하여 장치에서 모든 데이터와 앱을 즉시 지웁니다.
 - Android 장치의 경우 이 요청에 메모리 카드를 초기화하는 옵션도 포함될 수 있습니다.
 - 작업 프로필로 완전히 관리되는 Android Enterprise 장치 (COPE 장치)의 경우 선택적 초기화로 작업 프로필을 제거한 후 전체 초기화를 수행할 수 있습니다.

- iOS 및 macOS 장치의 경우 장치가 잠겨 있더라도 초기화가 수행됩니다. iOS 11 장치 (최소 버전) 의 경우: 전체 초기화를 확인할 때 장치의 셀룰러 데이터 요금제가 보존되도록 선택할 수 있습니다.
 - 메모리 카드 콘텐츠가 삭제되기 전에 장치 사용자가 장치 전원을 끄면 사용자의 장치 데이터 액세스가 가능할 수 있습니다.
 - 요청이 장치로 전송되기 전까지는 초기화 요청을 취소할 수 있습니다.
- **위치:** 관리 > 장치 페이지의 장치 세부 정보 > 일반에서 장치를 찾고 지도를 포함한 장치 위치를 보고할 수 있습니다. 찾기는 일회성 작업입니다. 찾기 작업을 사용하면 작업을 수행할 때 현재 장치 위치가 표시됩니다. 일정 기간 동안 장치를 지속적으로 추적하려면 추적 사용 설정을 사용합니다.
 - Android(Android Enterprise 제외) 장치 또는 Android Enterprise(회사 소유 또는 BYOD) 장치에 이 작업을 적용하는 경우 다음 동작을 숙지하십시오.
 - ★ 위치 찾기를 사용하려면 사용자가 등록 중에 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 도중 권한을 부여하지 않으면 XenMobile 은 위치 명령을 전송할 때 다시 위치 권한을 요청합니다.
 - iOS 또는 Android Enterprise 장치에 이 기능을 적용할 경우 다음 제한 사항에 유의하십시오.
 - ★ Android Enterprise 장치의 경우 [위치 장치 정책](#)에서 장치에 대한 위치 모드를 높은 정확도 또는 배터리 절약으로 설정하지 않으면 이 요청이 실패합니다.
 - ★ iOS 장치의 경우 이 명령은 장치가 MDM 분실 모드에 있는 경우에만 성공합니다.
- **잠금:** 원격으로 장치를 잠급니다. 이 작업은 장치를 분실한 경우 그리고 장치를 도난당했는지 여부가 불확실한 경우에 유용합니다. 그러면 XenMobile 이 PIN 코드를 생성하여 장치에 이 코드를 설정합니다. 장치에 액세스하려면 사용자는 PIN 코드를 입력해야 합니다. 잠금을 제거하려면 XenMobile 콘솔에서 잠금 취소를 사용합니다.
 - **Lock and Reset Password(잠금 및 암호 재설정):** 원격으로 장치를 잠그고 암호를 재설정합니다.
 - Android 8.0 이전 버전의 Android 버전을 실행하는 작업 프로필 모드에서 Android Enterprise 에 등록된 장치의 경우 지원되지 않습니다.
 - Android 8.0 이상을 실행하는 작업 프로필 모드에서 Android Enterprise 에 등록된 장치에서:
 - ★ 전송된 암호로 작업 프로필이 잠깁니다. 장치는 잠기지 않습니다.
 - ★ 암호가 전송되지 않았거나 전송된 암호가 암호 요구 사항을 충족하지 않고 작업 프로필에 암호가 이미 설정되지 않은 경우 장치가 잠깁니다.
 - ★ 암호가 전송되지 않았거나 전송된 암호가 암호 요구 사항을 충족하지 않지만 작업 프로필에 암호가 이미 설정되어 있는 경우에는 작업 프로필이 잠기지만 장치는 잠기지 않습니다.
 - **Notify (Ring)(알림 (벨 울림)):** Android 장치에서 사운드를 울립니다.
 - **다시 부팅:** Windows 10 및 Windows 11 장치를 다시 시작합니다. Windows 태블릿 및 PC 의 경우 “System will reboot soon(시스템이 곧 다시 부팅됩니다.)” 라는 메시지가 표시되고 5 분 안에 다시 부팅됩니다.
 - **AirPlay** 미러링 요청/중지: 감독되는 iOS 장치에서 AirPlay 미러링을 시작 및 중지합니다.
 - **다시 시작/종료:** 감독되는 iOS 장치를 즉시 다시 시작하거나 종료합니다.

- **해지:** 장치가 XenMobile Server에 연결할 수 없도록 합니다.
- **Revoke/Authorize(해지/권한 부여)(iOS, macOS):** 선택적 초기화와 동일한 동작을 수행합니다. 해지 후에는 장치에 권한을 다시 부여하여 다시 등록할 수 있습니다.
- **벨 울림:** 장치가 분실 모드에 있는 경우 감속되는 iOS 장치의 벨의 사운드가 재생됩니다. 사운드는 장치를 분실 모드에서 제거하거나 사용자가 사운드를 비활성화할 때까지 재생됩니다.
- **선택적 초기화:** 장치에서 모든 회사 데이터 및 앱을 지우고 개인 데이터 및 앱은 그대로 유지합니다. 선택적 초기화 후에는 사용자가 장치를 다시 등록할 수 있습니다.
 - Android 장치의 선택적 초기화가 수행되어도 Device Manager 및 회사 네트워크에서 장치가 분리되지 않습니다. 장치가 Device Manager에 액세스하는 것을 방지하려면 장치 인증서도 해지해야 합니다.
 - Android 장치를 선택적으로 초기화하면 장치도 철회됩니다. 콘솔에서 재인증하거나 삭제한 후에만 장치를 다시 등록할 수 있습니다.
 - 작업 프로필로 완전히 관리되는 Android Enterprise 장치 (COPE 장치)의 경우 선택적 초기화로 작업 프로필을 제거한 후 전체 초기화를 수행할 수 있습니다. 아니면 동일한 사용자 이름으로 장치를 다시 등록할 수 있습니다. 장치를 다시 등록하면 작업 프로필이 다시 생성됩니다.
 - Samsung Knox API를 사용하도록 설정한 경우 장치를 선택적으로 초기화하면 Samsung Knox 컨테이너도 제거됩니다.
 - iOS 및 macOS 장치의 경우 이 명령은 MDM을 통해 설치된 모든 프로필을 제거합니다.
 - Windows 장치에서의 선택적 초기화는 현재 로그인된 모든 사용자의 프로필 폴더 내용도 제거합니다. 선택적 초기화는 구성을 통해 사용자에게 배달하는 웹 클립은 제거하지 않습니다. 웹 클립을 제거하려면 사용자가 자신의 장치를 수동으로 등록 취소해야 합니다. 선택적으로 초기화된 장치를 다시 등록할 수 없습니다.
- **잠금 해제:** 잠겨 있을 때 장치로 전송된 암호를 지웁니다. 이 명령은 장치를 잠금 해제하지 않습니다.

관리 > 장치의 장치 세부 정보 페이지에도 장치 보안 속성이 나열됩니다. 이러한 속성에는 강력한 ID, 장치 잠금, 활성화 잠금 바ypass 및 플랫폼 유형에 대한 기타 정보 등이 포함됩니다. 장치 전체 초기화 필드에는 사용자 PIN 코드가 포함됩니다. 장치가 초기화된 후 사용자는 이 코드를 입력해야 합니다. 사용자가 코드를 잊은 경우 여기서 코드를 조회할 수 있습니다.

Android 장치에 대한 보안 동작

보안 동작	Android(Android Enterprise 장치 제외)	Android Enterprise(BYOD)	Android Enterprise(회사 소유)
앱 잠금	예	아니요	아니요
앱 초기화	예	아니요	아니요
전체 초기화	예	아니요	예

보안 동작	Android(Android Enterprise 장치 제외)	Android Enterprise(BYOD)	Android Enterprise(회사 소유)
찾기	예: Android 6.0 이상을 실행하는 장치의 경우 위치를 사용하려면 사용자가 등록 도중 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 도중 권한을 부여하지 않으면 XenMobile은 위치 명령을 전송할 때 다시 위치 권한을 요청합니다.	예: Android 6.0 이상을 실행하는 장치의 경우 위치를 사용하려면 사용자가 등록 도중 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 도중 권한을 부여하지 않으면 XenMobile은 위치 명령을 전송할 때 다시 위치 권한을 요청합니다.	예: Android 6.0 이상을 실행하는 장치의 경우 위치를 사용하려면 사용자가 등록 도중 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 도중 권한을 부여하지 않으면 XenMobile은 위치 명령을 전송할 때 다시 위치 권한을 요청합니다.
잠금	예	예	예
Lock and Reset Password(잠금 및 암호 재설정)	예	아니요	예
Notify (Ring)(알림 (벨 울림))	예	예	예
해지	예	예	예
선택적 초기화	예	예	아니요

iOS 및 macOS 장치에 대한 보안 동작

보안 동작	iOS	macOS
활성화 잠금 바이패스	예	아니요
앱 잠금	예	아니요
앱 초기화	예	아니요
ASM 배포 프로그램 활성화 잠금	예	아니요
제한 사항 지우기	예	아니요
분실 모드 활성화/비활성화	예	아니요
추적 활성화/비활성화	예	아니요
전체 초기화	예	예
찾기	예	아니요

보안 동작	iOS	macOS
잠금	예	예
벨 울림	예	예
AirPlay 미러링 요청/중지	예	아니요
다시 시작/종료	예	아니요
Revoke/Authorize(해지/권한 부여)	예	예
선택적 초기화	예	예
잠금 해제	예	아니요

Windows 장치에 대한 보안 동작

보안 동작	Windows 태블릿 10
찾기	예
잠금	예
Lock and Reset Password(잠금 및 암호 재설정)	아니요
다시 부팅	예
해지	예
벨 울림	아니요
선택적 초기화	예
초기화	예

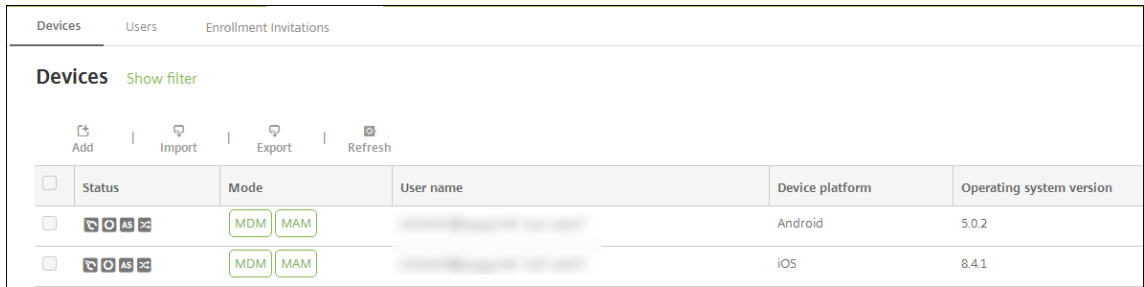
이 문서의 나머지 부분에서는 다양한 보안 동작을 수행하는 단계를 설명합니다. 일부 동작은 자동화할 수도 있습니다. 자세한 내용은 [자동화된 동작](#)을 참조하십시오.

iOS 장치 잠금

분실된 iOS 장치를 잠그고 장치 잠금 화면에 메시지와 전화 번호를 표시할 수 있습니다. 이 기능은 iOS 7 이상을 실행하는 장치에서 지원됩니다.

잠겨 있는 장치에 메시지와 전화 번호를 표시하려면 XenMobile 콘솔에서 [암호](#) 정책을 **true**로 설정합니다. 또는 사용자가 수동으로 장치에서 암호를 사용하도록 설정할 수 있습니다.

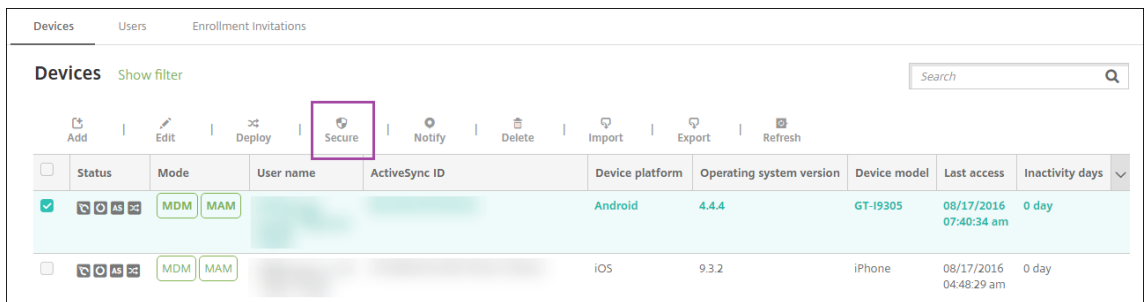
1. 관리 > 장치를 클릭합니다. 장치 페이지가 나타납니다.



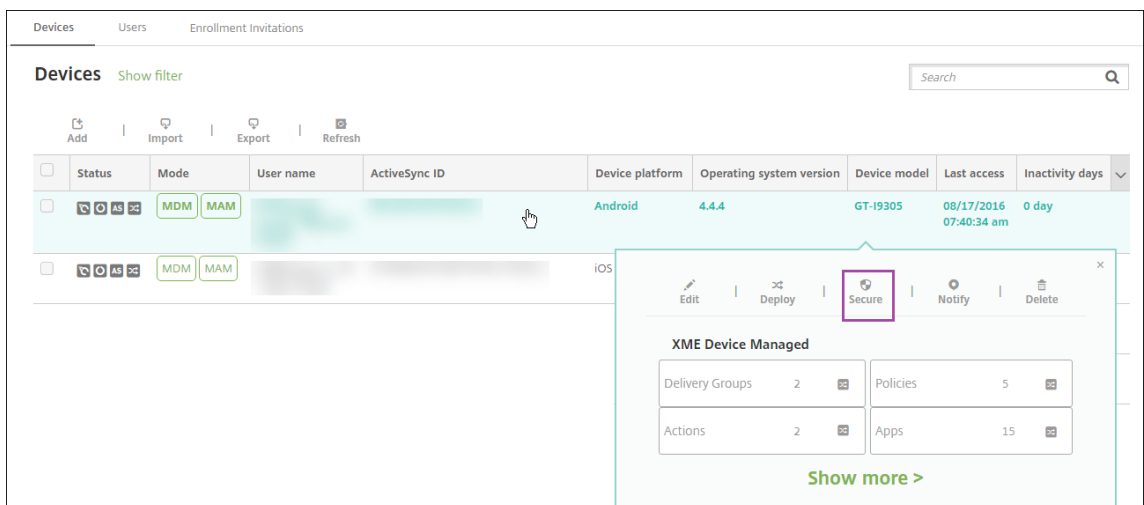
Status	Mode	User name	Device platform	Operating system version
	MDM MAM	[Redacted]	Android	5.0.2
	MDM MAM	[Redacted]	iOS	8.4.1

2. 잠글 iOS 장치를 선택합니다.

장치 옆에 있는 확인란을 선택하면 장치 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하면 목록의 오른쪽에 옵션 메뉴가 나타납니다.



Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
<input checked="" type="checkbox"/>	MDM MAM	[Redacted]	[Redacted]	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
<input type="checkbox"/>	MDM MAM	[Redacted]	[Redacted]	iOS	9.3.2	iPhone	08/17/2016 04:48:29 am	0 day



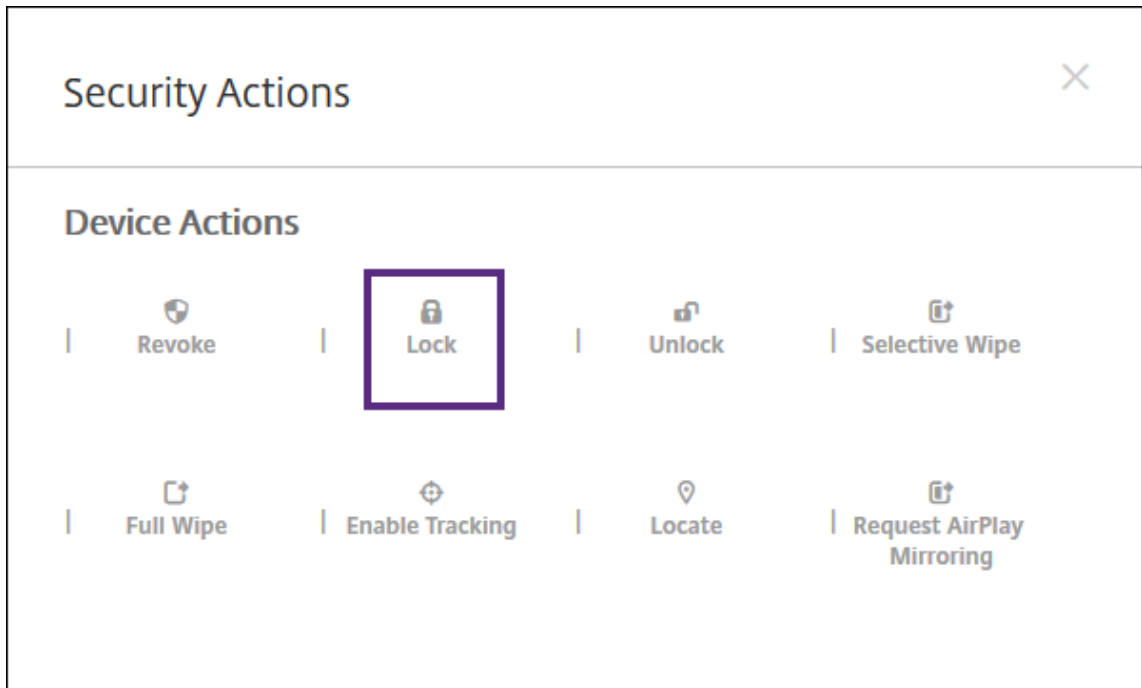
Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
<input checked="" type="checkbox"/>	MDM MAM	[Redacted]	[Redacted]	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
<input type="checkbox"/>	MDM MAM	[Redacted]	[Redacted]	iOS	9.3.2	iPhone	08/17/2016 04:48:29 am	0 day

XME Device Managed

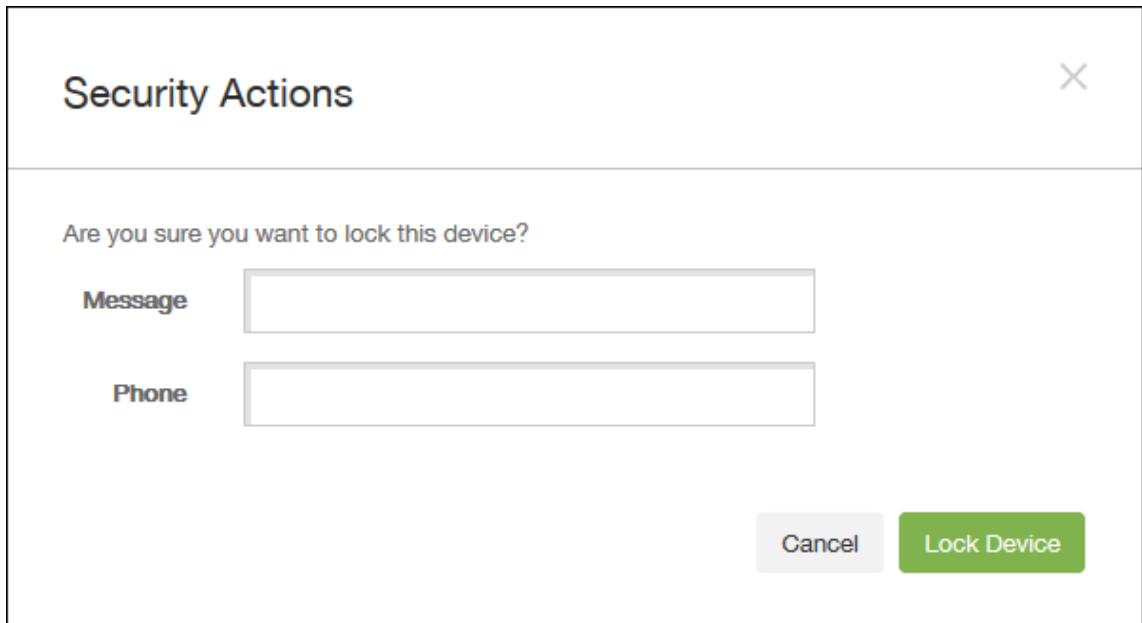
Delivery Groups	2	Policies	5
Actions	2	Apps	15

[Show more >](#)

3. 옵션 메뉴에서 보안을 클릭합니다. 보안 동작 대화 상자가 나타납니다.



4. 잠금을 클릭합니다. 보안 동작 확인 대화 상자가 표시됩니다.



5. 필요에 따라 장치 잠금 화면에 표시되는 메시지와 전화 번호를 입력합니다.

iOS 7 이상을 실행하는 iPad의 경우: 메시지 필드에 입력하는 내용에 “iPad 분실”이라는 단어가 추가됩니다.

iOS 7 이상을 실행하는 iPhone의 경우: 메시지 필드를 비워 두고 전화 번호를 입력할 경우 장치 잠금 화면에 “소유자에게 통화”라는 메시지가 표시됩니다.

6. 장치 잠금을 클릭합니다.

XenMobile 콘솔에서 장치 제거

중요:

XenMobile 콘솔에서 장치를 제거하는 경우 관리되는 앱 및 데이터는 장치에 남습니다. 관리되는 앱 및 데이터를 장치에서 제거하려면 이 문서 뒷부분의 “장치 삭제”를 참조하십시오.

XenMobile 콘솔에서 장치를 제거하려면 관리 > 장치로 이동하여 관리되는 장치를 선택한 다음 삭제를 클릭합니다.

Devices

Users

Enrollment Invitations

Devices

Show filter

Search

Add

Edit

Secure

Notify

Delete

Import

Export

Refresh

<input type="checkbox"/>	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version	
<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div><div></div></div>	<div>MDM</div> <div>MAM</div>			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0	

장치를 선택적으로 초기화

1. 관리 > 장치로 이동하고 관리되는 장치를 선택한 다음 보안을 클릭합니다.
2. 보안 동작에서 선택적 초기화를 클릭합니다.
3. Android 장치의 경우에만 회사 네트워크에서 장치를 분리합니다. 이렇게 하려면 장치가 초기화된 후 보안 동작에서 해지를 클릭하십시오.

초기화가 수행되기 전에 선택적 초기화 요청을 철회하려면 보안 동작에서 선택적 초기화 취소를 클릭합니다.

장치 삭제

이 절차는 관리되는 앱 및 데이터를 장치에서 제거하고 XenMobile 콘솔의 장치 목록에서 장치를 삭제합니다. Endpoint Management Public REST API를 사용하여 장치를 대량으로 삭제할 수 있습니다.

1. 관리 > 장치로 이동하고 관리되는 장치를 선택한 다음 보안을 클릭합니다.
2. 선택적 초기화를 클릭합니다. 메시지가 나타나면 선택적 초기화 수행을 클릭합니다.
3. 초기화 명령이 성공했는지 확인하려면 관리 > 장치를 새로 고치십시오. 모드 열에서 MDM 및 MAM의 색이 황색이면 초기화 명령이 성공한 것입니다.

Devices

Users

Enrollment Invitations

Devices

Show filter





Search?

Add

Import

Export

Refresh

<input type="checkbox"/>	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
<input type="checkbox"/>	   	MDM MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

4. 관리 > 장치에서 장치를 선택한 다음 삭제를 클릭합니다. 메시지가 나타나면 삭제를 다시 클릭합니다.

앱 잠금, 잠금 해제, 초기화 또는 초기화 취소

1. 관리 > 장치로 이동하고 관리되는 장치를 선택한 다음 보안을 클릭합니다.

2. 보안 동작에서 앱 동작을 클릭합니다.

보안 동작 상자를 사용하여 Active Directory 에서 계정이 사용하지 않도록 설정되었거나 삭제된 사용자의 장치 상태를 확인할 수 있습니다. 앱 잠금 해제 또는 앱 초기화 취소 동작이 나타나면 앱이 잠겼거나 초기화되었음을 나타냅니다.

앱 초기화 및 초기화 취소

1. 관리 > 장치로 이동합니다. 장치를 선택합니다.

2. 앱 초기화

- 보안 > 앱 초기화를 클릭합니다. 이 장치를 앱 초기화하시겠습니까? 라는 메시지가 포함된 대화 상자가 나타납니다. 앱 초기화를 클릭합니다.

3. 앱 초기화 취소

- 보안 > 앱 초기화 취소를 클릭합니다. 이 장치의 앱 초기화를 취소하시겠습니까? 라는 메시지가 포함된 대화 상자가 나타납니다. 장치 앱 초기화 취소를 클릭합니다.

4. 장치에서 Secure Hub 를 열고 스토어를 클릭합니다.

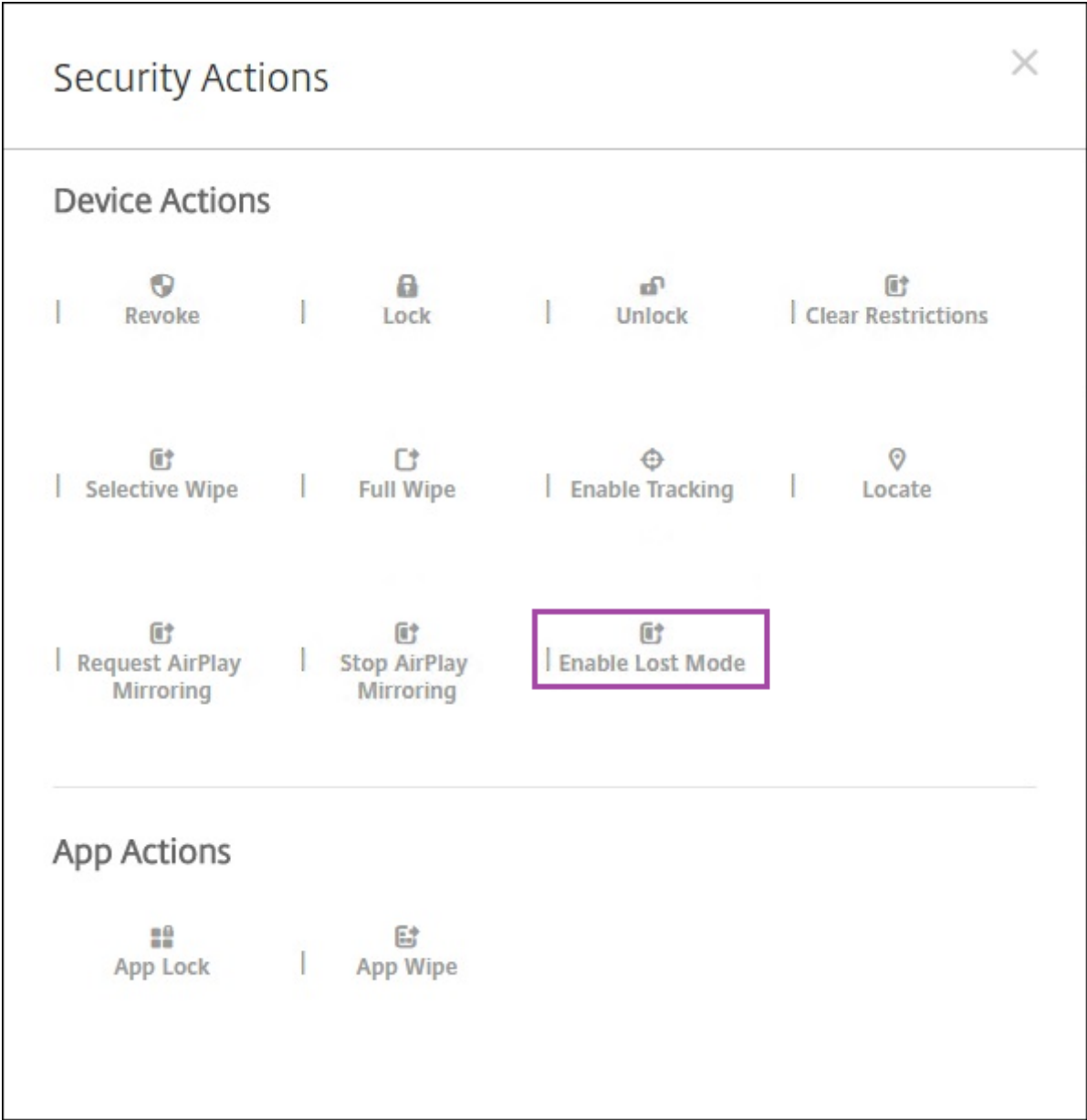
5. Secure Hub 를 실행합니다.

iOS 장치를 분실 모드로 전환

XenMobile 분실 모드 장치 속성은 iOS 장치를 분실 모드로 전환합니다. Apple 의 관리되는 분실 모드와 달리 XenMobile 의 분실 모드에서는 다음 동작 중 하나를 수행하여 사용자가 나의 **iPhone/iPad** 찾기 설정을 구성하거나 Citrix Secure Hub 의 위치 서비스를 사용하지 않아도 장치 위치를 찾을 수 있습니다.

XenMobile 분실 모드에서는 XenMobile Server 만 장치 잠금을 해제할 수 있습니다. 이와 반대로 XenMobile 장치 잠금 기능을 사용하는 경우에는 사용자가 제공된 PIN 코드를 사용하여 장치를 직접 잠금 해제할 수 있습니다.

분실 모드를 사용하거나 사용하지 않으려면: 관리 > 장치로 이동하고 감독되는 iOS 장치를 선택한 후 보안을 클릭합니다. 분실 모드 활성화 또는 분실 모드 비활성화를 클릭합니다.



분실 모드 활성화를 클릭하고 장치가 분실 모드가 될 때 장치에 표시할 정보를 입력합니다.

Security Actions

Are you sure you want to enable the lost mode for this device?

Message

?

Phone number

?

Footnote

?

Cancel

Enable Lost Mode

다음 방법 중 하나를 사용하여 분실 모드 상태를 확인합니다.

- 보안 동작 창에서 단추가 분실 모드 비활성화인지 확인합니다.
- 관리 > 장치에서 일반 탭의 보안 아래에서 마지막 분실 모드 활성화 또는 분실 모드 비활성화 동작을 확인합니다.

Devices

Users

Enrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Actions

7 Delivery Groups

8 iOS Profiles

9 iOS Provisioning Profiles

10 Certificates

11 Connections

12 MDM Status

Device Shutdown

No device shutdown.

Device locate

No device locate .

Device Enable Tracking

No device enable tracking.

Device Disown

No device disown.

DEP Activation Lock

No DEP device activation lock.

Activation Lock Bypass

No device activation lock bypass.

Device Clear Restrictions

No Clear Restrictions.

Device App Wipe

No device App Wipe.

Device App Lock

No device App Lock.

Request AirPlay Mirroring

No request AirPlay mirroring.

Stop AirPlay Mirroring

No stop AirPlay mirroring.

Enable Lost Mode

No lost mode enabled.

Disable Lost Mode

No lost mode disabled.

Next >

Next >

- 관리 > 장치의 속성 탭에서 **MDM 분실 모드** 활성화 설정의 값이 올바른지 확인합니다.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div>1 General</div> <div>2 Properties</div> <div>3 User Properties</div> <div>4 Assigned Policies</div> <div>5 Apps</div> <div>6 Actions</div> <div>7 Delivery Groups</div> <div>8 iOS Profiles</div> <div>9 iOS Provisioning Profiles</div> <div>10 Certificates</div> <div>11 Connections</div> <div>12 MDM Status</div>		
		<div>Activation lock enabled</div> <div>No</div>
		<div>Hardware encryption capabilities</div> <div>Block and file levels encryption</div>
		<div>Internal storage encrypted</div> <div>No</div>
		<div>Jailbroken/Rooted</div> <div>No</div>
		<div>MDM lost mode enabled</div> <div>No</div>
		<div>Passcode compliant</div> <div>Yes</div>
		<div>Passcode compliant with configuration</div> <div>Yes</div>
		<div>Passcode present</div> <div>No</div>
		<div>Supervised</div> <div>No</div>
		<div>- Storage space</div> <div>Add</div>
		<div>Available storage space</div> <div>10.92 GB</div>
		<div>Total storage space</div> <div>12.28 GB</div> <div>×</div>
		<div>- System information</div> <div>Add</div>
		<div>Active iTunes account</div> <div>Yes</div>
		<div>Cloud backup enabled</div> <div>No</div>
		<div>Back</div> <div>Next ></div>

iOS 장치에서 XenMobile 분실 모드를 사용하는 경우 XenMobile 콘솔이 다음과 같이 변경됩니다.

- 구성 > 동작에서 동작 목록에 장치 해지, 장치를 선택적으로 초기화 및 장치를 완전히 초기화 자동화 동작이 포함되지 않습니다.
- 관리 > 장치에서 보안 동작 목록에 해지 및 장치 선택적 초기화 동작이 더 이상 포함되지 않습니다. 필요한 경우 보안 동작을 사용하여 전체 초기화를 수행할 수 있습니다.

iOS 7 이상을 실행하는 iPad의 경우: 보안 동작 화면의 메시지에 무엇을 입력하든지 관계없이 끝에 “iPad 분실”이라는 단어가 추가됩니다.

iOS 7 이상을 실행하는 iPhone의 경우: 메시지를 비워 둔 경우 전화 번호를 입력하면 장치 잠금 화면에 “소유자에게 통화” 메시지가 표시됩니다.

iOS 활성화 잠금 바이패스

활성화 잠금은 분실되거나 도난당한 장치의 재활성화를 방지하는 내 iPhone/iPad 찾기 기능입니다. 활성화 잠금은 누군가가 내 iPhone/iPad 찾기를 비활성화하고 장치를 지우거나 장치를 재활성화하여 사용하려고 할 경우 사용자의 Apple ID와 암호를 요구합니다. 조직이 소유한 장치의 경우 예를 들어 장치를 재설정하거나 재활당하기 위해 활성화 잠금을 바이패스해야 합니다.

활성화 잠금을 사용하도록 설정하려면 XenMobile MDM 옵션 장치 정책을 구성하고 배포합니다. 그러면 사용자의 Apple 자격 증명 없이도 XenMobile 콘솔에서 장치를 관리할 수 있습니다. 활성화 잠금의 Apple 자격 증명 요구 사항을 바이패스하려면 XenMobile 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행합니다.

예를 들어 사용자가 분실된 휴대폰을 반환하거나 전체 초기화 전후에 장치를 설정하는 경우 iTunes 계정 자격 증명을 묻는 메시지가 표시될 때 XenMobile 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행하여 이 단계를 바이패스할 수 있습니다.

활성화 잠금 바이패스를 위한 장치 요구 사항

- iOS 7.1(최소 버전)
- Apple Configurator 또는 Apple DEP 를 통해 감독됨
- iCloud 계정을 사용하여 구성됨
- 내 iPhone/iPad 찾기를 사용하도록 설정됨
- XenMobile 에서 등록됨
- 활성화 잠금을 사용하도록 설정된 MDM 옵션 장치 정책이 장치에 배포됨

장치의 전체 초기화를 실행하기 전에 활성화 잠금을 바이패스하려면:

1. 관리 > 장치에서 장치를 선택하고 보안을 클릭한 다음 활성화 잠금 바이패스를 클릭합니다.
2. 장치를 초기화합니다. 장치 설정 중에 활성화 잠금 화면이 표시되지 않습니다.

장치의 전체 초기화를 실행한 후에 활성화 잠금을 바이패스하려면:

1. 장치를 재설정하거나 초기화합니다. 장치 설정 중에 활성화 잠금 화면이 표시됩니다.
2. 관리 > 장치에서 장치를 선택하고 보안을 클릭한 다음 활성화 잠금 바이패스를 클릭합니다.
3. 장치에서 뒤로 단추를 누릅니다. 홈 화면이 나타납니다.

다음 사항에 유의하십시오.

- 사용자에게 내 iPhone/iPad 찾기를 비활성화하지 말라고 안내하십시오. 장치에서 전체 초기화를 수행하지 마십시오. 두 경우 모두 사용자에게 iCloud 계정 암호를 입력하라는 메시지가 표시됩니다. 계정 유효성 검사 후 모든 콘텐츠와 설정을 지운 다음 사용자에게 iPhone/iPad 활성화 화면이 표시되지 않습니다.
- 활성화 잠금 바이패스 코드가 생성되고 활성화 잠금을 사용하도록 설정한 장치의 경우 전체 초기화 후 iPhone/iPad 활성화 페이지를 바이패스할 수 없으면 XenMobile 에서 장치를 삭제할 필요가 없습니다. 관리자 또는 사용자가 Apple 지원 팀에 연락하여 직접 장치의 차단을 해제할 수 있습니다.
- 하드웨어 인벤토리 중에 XenMobile 은 장치에서 활성화 잠금 바이패스 코드를 쿼리합니다. 바이패스 코드를 사용할 수 있는 경우 장치가 해당 코드를 XenMobile 에 전송합니다. 그런 다음 장치에서 바이패스 코드를 제거하려면 XenMobile 콘솔에서 활성화 잠금 바이패스 보안 동작을 전송합니다. 이때 장치의 차단을 해제하려면 XenMobile Server 와 Apple 에 바이패스 코드가 있어야 합니다.
- 활성화 잠금 바이패스 보안 동작은 Apple 서비스의 이용 가용성에 따라 달라집니다. 이 동작이 작동하지 않는 경우 다음과 같이 장치의 차단을 해제할 수 있습니다. 장치에서 수동으로 iCloud 계정의 자격 증명을 입력합니다. 또는 사용자 이름 필드를 비워 두고 암호 필드에 바이패스 코드를 입력합니다. 바이패스 코드를 조회하려면 관리 > 장치로 이동하여 장치를 선택하고 편집, 속성을 차례로 클릭합니다. 활성화 잠금 바이패스 코드는 보안 정보 아래에 있습니다.

XenMobile AutoDiscovery Service

March 15, 2024

자동 검색 서비스는 전자 메일 기반 URL 검색을 통해 사용자의 등록 프로세스를 간소화합니다. 또한 자동 검색 서비스는 등록 확인, 인증서 고정 같은 기능과 Citrix Workspace 고객을 위한 기타 이점을 제공합니다. Citrix Cloud 에서 호스팅되는 이 서비스는 여러 XenMobile 배포의 중요한 부분입니다.

자동 검색 서비스를 사용하면 다음과 같은 이점이 있습니다.

- 회사 네트워크 자격 증명을 사용하여 장치를 등록할 수 있습니다.
- XenMobile Server 주소에 대한 세부 정보를 입력할 필요가 없습니다.
- 사용자 이름을 UPN(사용자 계정 이름) 형식으로 입력합니다. 예를 들어, user@mycompany.com입니다.

보안 수준이 높은 환경에서는 자동 검색 서비스를 사용하는 것이 좋습니다. 자동 검색 서비스는 중간자 공격을 방지하는 공개 키 인증서 고정을 지원합니다. 인증서 고정을 사용하면 Citrix 클라이언트가 XenMobile 과 통신할 때 회사에서 서명한 인증서가 사용됩니다. XenMobile 사이트에 대한 인증서 고정을 구성하려면 Citrix 지원 서비스에 문의하십시오. 인증서 고정에 대한 자세한 내용은 [인증서 고정](#)을 참조하십시오.

자동 검색 서비스에 액세스하려면 <https://adsui.cloud.com>(상업용) 또는 <https://adsui.cem.cloud.us>(정부) 로 이동합니다.

사전 요구 사항

- Citrix Cloud 의 새로운 자동 검색 서비스를 사용하려면 다음과 같은 Secure Hub 최신 버전이 필요합니다.
 - iOS 의 경우 Secure Hub 버전 21.6.0 이상
 - Android 경우 Secure Hub 버전 21.8.5 이상

이전 버전의 Secure Hub 을 실행하는 장치에서 서비스 중단이 발생할 수 있습니다.

- 새 자동 검색 서비스에 액세스하려면 전체 액세스 권한이 있는 Citrix Cloud 관리자 계정이 있어야 합니다. 자동 검색 서비스는 사용자 지정 액세스 권한이 있는 관리자 계정을 지원하지 않습니다. 계정이 없는 경우 [Citrix Cloud 가입](#)을 참조하십시오.

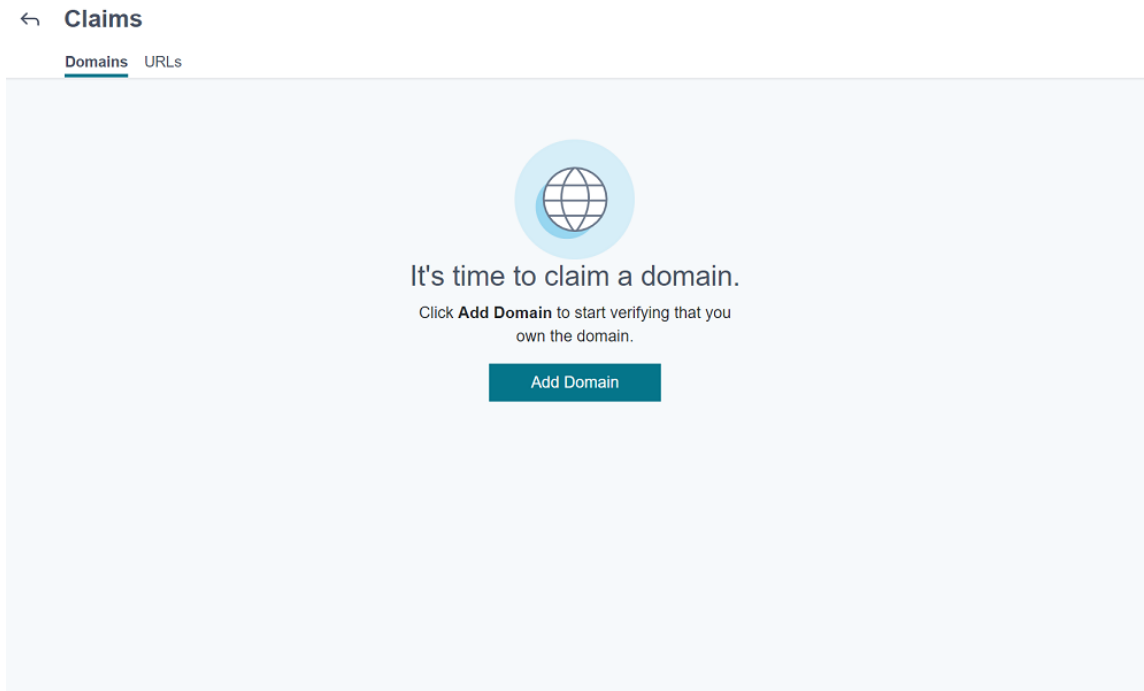
Citrix 는 서비스 중단 없이 기존의 모든 자동 검색 레코드를 Citrix Cloud 로 마이그레이션했습니다. 마이그레이션된 레코드는 새 콘솔에 자동으로 나타나지 않습니다. 소유권을 증명하려면 새 자동 검색 서비스에서 도메인을 회수해야 합니다. 자세한 내용은 [CTX312339](#)를 참조하십시오.

- Endpoint Management 배포에 대해 자동 검색 서비스를 사용하기 전에 도메인을 확인하고 요청합니다. 최대 10 개의 도메인을 요청할 수 있습니다. 요청은 확인된 도메인과 자동 검색 서비스를 연결합니다. 11 개 이상의 도메인을 요청하려면 SRE 티켓을 열거나 Citrix 기술 지원에 문의하십시오.
- Citrix Gateway FQDN 대신 MAM 포트 설정을 사용하여 MAM 트래픽을 데이터 센터로 보낼 수 있습니다. Citrix Gateway 의 포트와 함께 정규화된 도메인 이름을 입력하면 클라이언트 장치는 **MAM** 포트 설정의 구성을 사용합니다.

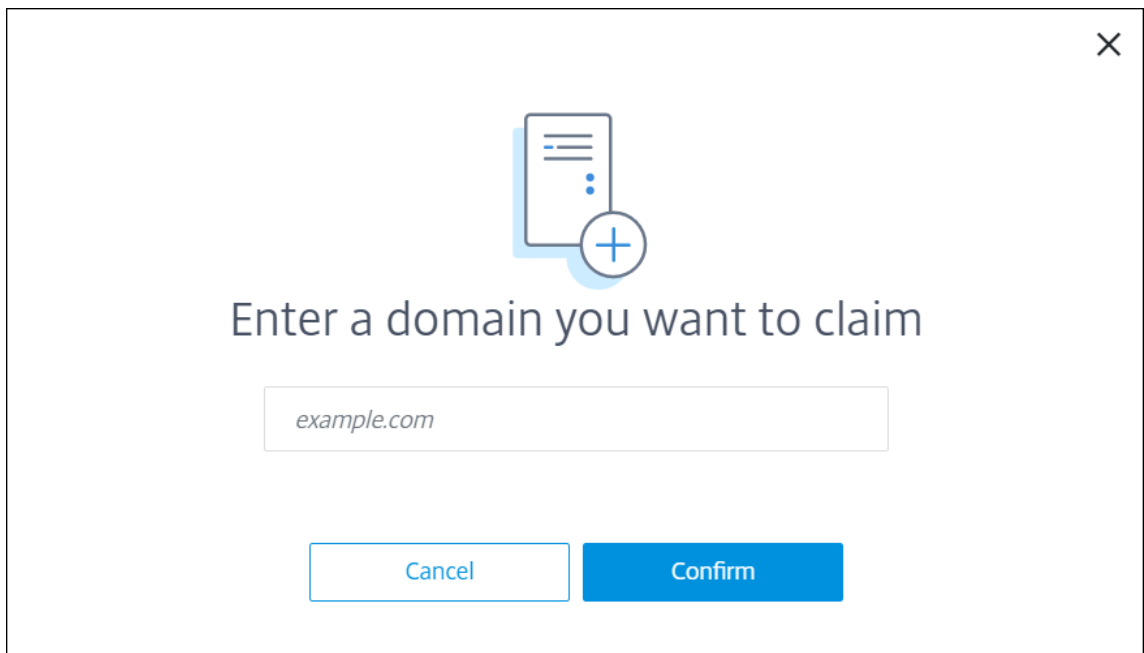
- 광고 차단으로 인해 사이트가 열리지 않는 경우 전체 웹 사이트에 대한 광고 차단기를 비활성화해야 합니다.

도메인 신청

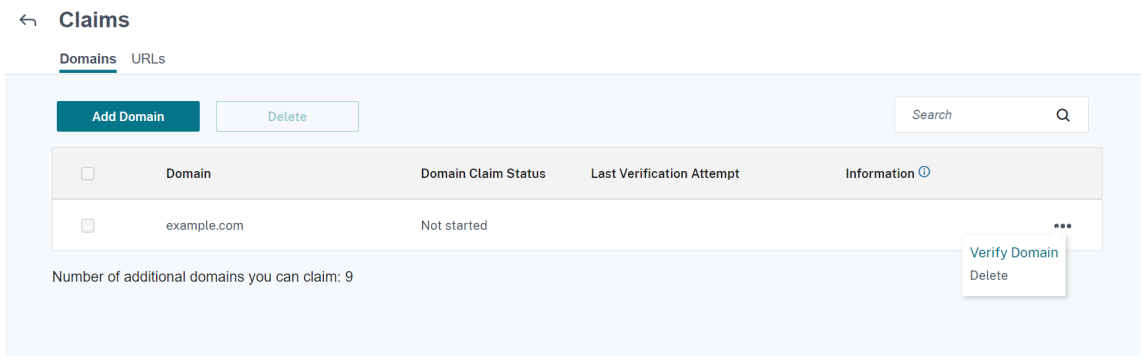
1. 요청 > 도메인 탭에서 도메인 추가를 클릭합니다.



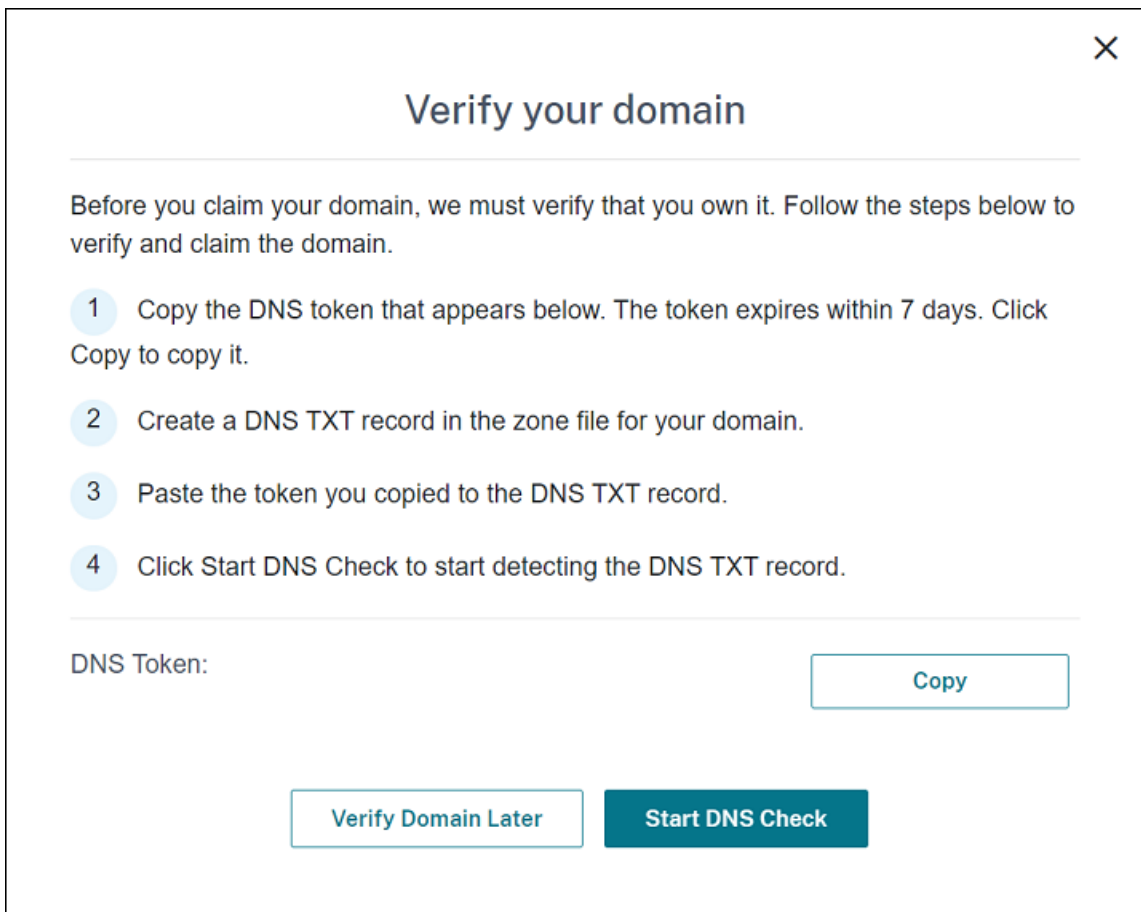
2. 대화 상자가 나타나면 XenMobile 환경의 도메인 이름을 입력하고 확인을 클릭합니다. 도메인이 요청 > 도메인에 나타납니다.



3. 추가한 도메인에서 줄임표 메뉴를 클릭하고 도메인 확인을 선택하여 확인 프로세스를 시작합니다. 도메인 확인 페이지가 나타납니다.



4. 도메인 확인 페이지에서 지침에 따라 도메인을 소유하고 있는지 확인합니다.



- 복사를 클릭하여 DNS 토큰을 클립보드에 복사합니다.
- 도메인의 영역 파일에서 DNS TXT 레코드를 만듭니다. 이렇게 하려면 도메인 호스팅 공급자 포털로 이동하여 복사한 DNS 토큰을 추가합니다.

다음 스크린샷은 도메인 호스팅 공급자 포털을 보여줍니다. 실제 포털은 다르게 보일 수 있습니다.

Dashboard > DNS zones > .cloud.com >

@ .cloud.com

Save Discard Delete Users Metadata

Copy to clipboard

@ .cloud.com

Type

TXT

TTL * TTL unit

5 Minutes

Value

The quick brown fox jumps over the lazy dog.

- c) Citrix Cloud의 도메인 확인 페이지에서 **DNS** 확인 시작을 클릭하여 DNS TXT 레코드 검색을 시작합니다. 나중에 도메인을 확인하려면 나중에 도메인 확인을 클릭합니다.

확인 프로세스에는 보통 약 1 시간 정도가 소요됩니다. 그러나 응답을 반환하는 데 최대 2 일까지 걸릴 수 있습니다. 상태 확인 중에 로그아웃했다가 다시 로그인해도 괜찮습니다.

구성이 완료되면 도메인 상태가 보류 중에서 확인됨으로 변경됩니다.

- 도메인을 요청한 후 자동 검색 서비스에 대한 정보를 제공합니다. 추가한 도메인의 말줄임표 메뉴를 클릭한 다음 **Endpoint Management** 정보 추가를 클릭합니다. 자동 검색 서비스 정보 페이지가 나타납니다.
- 다음 정보를 입력한 다음 저장을 클릭합니다.

- Endpoint Management 서버 FQDN:** XenMobile Server의 정규화된 도메인 이름을 입력합니다. 예: `example.xm.cloud.com`. 이 설정은 MDM 및 MAM 제어 트래픽에 사용됩니다.
- Citrix Gateway FQDN:** Citrix Gateway의 정규화된 도메인 이름을 FQDN 또는 FQDN: 포트 형식으로 입력합니다. 예: `example.com`. 이 설정은 MAM 트래픽을 데이터 센터로 보내는 데 사용됩니다. MDM 전용 배포의 경우 이 필드를 비워 둡니다.

참고:

Citrix는 MAM 트래픽을 제어하기 위해 **Citrix Gateway FQDN** 대신 **MAM** 포트를 사용하기를 권장합니다. Citrix Gateway의 포트와 함께 정규화된 도메인 이름을 입력하면 클라이언트 장치는 **MAM** 포트 설정의 구성을 사용합니다.

- **인스턴스 이름:** 위에서 구성한 XenMobile Server 의 인스턴스 이름을 입력합니다. 인스턴스 이름을 잘 모르는 경우 기본값인 **zdm** 을 그대로 둡니다.
- **MDM 포트:** MDM 제어 트래픽 및 MDM 등록에 사용되는 포트를 입력합니다. 클라우드 기반 서비스의 경우 기본값은 443 입니다.
- **MAM 포트:** MAM 제어 트래픽, MAM 등록, iOS 등록 및 앱 열거에 사용되는 포트를 입력합니다. 클라우드 기반 서비스의 경우 기본값은 8443 입니다.

Windows 장치에 대한 자동 검색 요청

Windows 장치를 등록하려는 경우 다음을 수행합니다.

1. Citrix 지원 서비스에 문의하여 Windows 자동 검색을 사용하도록 설정하는 지원 요청을 만듭니다.
2. enterpriseenrollment.mycompany.com에 대해 공개적으로 서명된 와일드카드가 아닌 SSL 인증서를 얻습니다. 이 [mycompany.com](https://enterpriseenrollment.mycompany.com) 부분은 사용자가 등록하는 데 사용하는 계정이 포함된 도메인입니다. .pfx 형식의 SSL 인증서와 암호를 이전 단계에서 만든 지원 요청에 연결합니다.

두 개 이상의 도메인을 사용하여 Windows 장치를 등록하려면 다음과 같은 구조의 다중 도메인 인증서를 사용할 수도 있습니다.

- SubjectDN 과 기본 도메인을 지정하는 CN(예: enterpriseenrollment.mycompany1.com)
 - 나머지 도메인에 해당하는 SAN(예: enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com 등)
3. DNS 에 CNAME(정식 이름) 레코드를 만들고 SSL 인증서 주소 (enterpriseenrollment.mycompany.com) 를 autodisc.xm.cloud.com 에 매핑합니다.

Windows 장치 사용자가 UPN 을 사용하여 등록하면 Citrix 등록 서버는 다음을 수행합니다.

- XenMobile Server 에 대한 세부 정보를 제공합니다.
- XenMobile 에서 유효한 인증서를 요청하도록 장치에 지시합니다.

이 시점에서 지원되는 모든 장치를 등록할 수 있습니다. 다음 섹션으로 이동하여 장치에 리소스를 제공할 준비를 합니다.

장치 정책

March 15, 2024

정책을 만들어 XenMobile 이 장치와 상호 작용하는 방식을 구성할 수 있습니다. 많은 정책이 모든 장치에 공통적으로 적용되지만 각 장치에 해당 운영 체제와 관련된 일련의 정책이 있습니다. 따라서 플랫폼 간에는 물론 Android 장치 제조업체 사이에서도 차이가 있을 수 있습니다.

각 장치 정책에 대한 요약 설명은 이 문서의 장치 정책 요약을 참조하십시오.

참고:

환경에 GPO(그룹 정책 개체)가 구성되어 있는 경우:

Windows 10 및 Windows 11 용 XenMobile 장치 정책을 구성할 때 다음 규칙을 고려하십시오. 하나 이상의 등록된 장치에서 정책이 충돌하는 경우 GPO와 일치하는 정책이 우선합니다.

Android Enterprise 컨테이너가 지원하는 정책은 [Android Enterprise](#)를 참조하십시오.

사전 요구 사항

- 사용하려는 배달 그룹을 만듭니다.
- 필요한 모든 CA 인증서를 설치합니다.

장치 정책 추가

장치 정책을 만드는 기본 단계는 다음과 같습니다.

1. 정책의 이름을 지정하고 관련 설명을 입력합니다.
2. 하나 이상의 플랫폼에 대한 정책을 구성합니다.
3. 배포 규칙을 만듭니다 (선택 사항).
4. 배달 그룹에 정책을 할당합니다.
5. 배포 일정을 구성합니다 (선택 사항).

장치 정책을 만들고 관리하려면 구성 > 장치 정책으로 이동합니다.

Device Policies Apps Media Actions ShareFile Enrollment Profiles Delivery Groups						
Device Policies Show filter						
<div> <div>Add</div> <div>Export</div> </div> <div> <div>Search</div> <div>Q</div> </div>						
<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	▼
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM		
<input type="checkbox"/>	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM		

정책을 추가하려면:

1. 장치 정책 페이지에서 추가를 클릭합니다. 새 정책 추가 페이지가 나타납니다.

Policy Platform

Clear All

☐ iOS45

☐ Android20

☐ Windows Mobile/CE20

☐ macOS18

☐ Windows Desktop/Tablet17

☐ Windows Phone16

☐ Samsung KNOX10

☐ Samsung SAFE9

☐ Android for Work6

☐ Amazon3

☐ Android HTC1

☐ SEAMS1

☐ Sony1

☐ Zebra1

Add a New Policy

Hide filter

Search policy

Policies most often used

Exchange

Location

Passcode

Restrictions

Scheduling

Terms & Conditions

VPN

WiFi

Network access

APN

Cellular

Connection Manager

Security

Android for Work App Restrictions

App Lock

App Restrictions

BitLocker

Contacts (CardDAV)

Copy Apps to Samsung Container

Credentials

Defender

Kiosk

Managed Domains

SCEP

Samsung MDM License Key

2. 하나 이상의 플랫폼을 클릭하여 선택한 플랫폼에 대한 장치 정책 목록을 봅니다. 정책 추가를 계속하려면 정책 이름을 클릭합니다.

Policy Platform

Clear All

☒ iOS18

☐ Android7

☐ Windows Mobile/CE4

☒ macOS18

☐ Windows Desktop/Tablet8

☐ Windows Phone7

☐ Samsung KNOX4

☐ Samsung SAFE3

☐ Android for Work3

☐ Amazon2

☐ Android HTC1

☐ SEAMS0

☐ Sony0

☐ Zebra0

Add a New Policy

Hide filter

Search policy

Policies most often used

Exchange

Passcode

Restrictions

VPN

WiFi

Apps

App Inventory

Webclip

Removal

Profile Removal

Security

Contacts (CardDAV)

Credentials

SCEP

End user

AirPlay Mirroring

Calendar (CalDav)

Device Name

Font

LDAP

Mail

Custom

검색 상자에 정책 이름을 입력할 수도 있습니다. 입력할 때 잠재적 검색 결과가 나타납니다. 목록에 해당 정책이 있으면 정책을 클릭합니다. 선택한 정책만 결과에 유지됩니다. 해당 정책을 클릭하여 정책에 대한 정책 정보 페이지를 엽니다.

3. 정책에 포함할 플랫폼을 선택합니다. 5 단계에서 선택한 플랫폼에 대한 구성 페이지가 나타납니다.
4. 정책 정보 페이지를 작성한 후 다음을 클릭합니다. 정책 정보 페이지에서는 정책을 식별하고 추적하는 데 도움이 되는 정책 이름과 같은 정보를 수집합니다. 이 페이지는 모든 정책에 대해 유사합니다.
5. 플랫폼 페이지를 작성합니다. 3 단계에서 선택한 각 플랫폼에 대해 플랫폼 페이지에 나타납니다. 이러한 페이지는 각 정책에 따라 다릅니다. 정책은 플랫폼마다 차이가 있을 수 있습니다. 모든 정책이 모든 플랫폼에 적용되는 것은 아닙니다.

일부 페이지에는 항목 표가 포함되어 있습니다. 기존의 항목을 삭제하려면 목록이 포함된 줄 위로 마우스 포인터를 이동한 후 오른쪽의 휴지통 아이콘을 클릭합니다. 확인 대화 상자에서 삭제를 클릭합니다.

기존의 항목을 편집하려면 목록이 포함된 줄 위로 마우스 포인터를 이동한 후 오른쪽의 펜 아이콘을 클릭합니다.

배포 규칙, 할당 및 일정을 구성하려면

배포 규칙을 구성하는 방법에 대한 자세한 내용은 [리소스 배포](#)를 참조하십시오.

1. 플랫폼 페이지에서 배포 규칙을 확장하고 다음 설정을 구성합니다. 기본적으로 기본 탭이 표시됩니다.
 - 목록에서 어떤 경우에 정책을 배포할지 지정하는 옵션을 클릭합니다. 모든 조건이 충족된 경우 또는 조건 중 하나라도 충족된 경우 정책을 배포하도록 선택할 수 있습니다. 기본 옵션은 모두입니다.
 - 조건을 정의하려면 새 규칙을 클릭합니다.
 - 목록에서 장치 소유권 및 **BYOD** 와 같은 조건을 클릭합니다.
 - 조건을 더 추가하려면 새 규칙을 다시 클릭합니다. 원하는 만큼 많은 조건을 추가할 수 있습니다.
2. 고급 탭을 클릭하여 규칙을 부울 옵션과 결합합니다. 기본 탭에서 선택한 조건이 표시됩니다.
3. 추가 고급 부울 논리를 사용하여 규칙을 결합하거나, 편집하거나, 추가할 수 있습니다.
 - 그리고, 또는이나 아님을 클릭합니다.
 - 목록에서 규칙에 추가할 조건을 선택합니다. 그런 다음 오른쪽의 더하기 기호 (+) 를 클릭하여 규칙에 조건을 추가합니다.

언제든지 조건을 클릭하여 선택한 다음 편집을 클릭하여 조건을 변경하거나 삭제를 클릭하여 조건을 제거할 수 있습니다.
 - 새 규칙을 클릭하여 다른 조건을 추가합니다.
4. 다음을 클릭하여 다음 플랫폼 페이지로 이동하거나, 모든 플랫폼 페이지가 완료된 경우 할당 페이지로 이동합니다.
5. 할당 페이지에서 정책을 적용할 배달 그룹을 선택합니다. 배달 그룹을 클릭하면 앱 할당을 받을 배달 그룹 상자에 해당 그룹이 표시됩니다.

앱 할당을 받을 배달 그룹은 배달 그룹을 선택하기 전까지 표시되지 않습니다.

Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Choose delivery groups

☒ AllUsers
☐ sales

Delivery groups to receive app assignment

AllUsers

6. 할당 페이지에서 배포 일정을 확장하고 다음 설정을 구성합니다.

- 배포 옆에서 켜짐을 클릭하여 배포를 예약하거나 꺼짐을 클릭하여 배포를 차단합니다. 기본 옵션은 켜짐입니다.
- 배포 일정 옆에서 지금 또는 나중에를 클릭합니다. 기본 옵션은 켜짐입니다.
- 나중에를 클릭하는 경우 달력 아이콘을 클릭하고 배포 날짜와 시간을 선택합니다.
- 배포 조건 옆에서 모든 연결에서를 클릭하거나 이전 배포가 실패한 경우에만을 클릭합니다. 기본 옵션은 모든 연결에서입니다.
- 상시 연결에 대해 배포 옆에서 켜짐 또는 꺼짐을 클릭합니다. 기본 옵션은 꺼짐입니다.

참고:

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우에만 이 옵션이 적용됩니다. iOS 장치에는 상시 연결 옵션을 사용할 수 없습니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 모든 플랫폼에 적용되지만 상시 연결에 대해 배포를 선택한 경우 iOS 에는 적용되지 않습니다.

Deployment Schedule ?

Deploy

ON

Deployment Schedule

☒ Now
☐ Later

Deployment condition

☒ On every connection
☐ Only when previous deployment has failed

Deploy for always-on connections

OFF

?

7. 저장을 클릭합니다.

장치 정책 테이블에 정책이 표시됩니다.

장치에서 장치 정책 제거

장치에서 장치 정책을 제거하는 단계는 플랫폼에 따라 다릅니다.

- Android

Android 장치에서 장치 정책을 제거하려면 XenMobile 제거 장치 정책을 사용합니다. 자세한 내용은 [XenMobile 제거 장치 정책](#)을 참조하십시오.

- iOS 및 macOS

iOS 또는 macOS 장치에서 장치 정책을 제거하려면 프로필 제거 장치 정책을 사용합니다. iOS 및 macOS 장치에서 모든 정책은 MDM 프로필의 일부입니다. 따라서 제거할 정책에 대해서만 프로필 제거 장치 정책을 만들 수 있습니다. 나머지 정책과 프로필은 장치에 유지됩니다. 자세한 내용은 [프로필 제거 장치 정책](#)을 참조하십시오.

- Windows 10 및 Windows 11

Windows 데스크톱 또는 태블릿 장치에서 장치 정책을 직접 제거할 수는 없습니다. 그러나 다음 방법 중 하나를 사용할 수 있습니다.

- 장치의 등록을 취소한 다음 새 정책 집합을 장치에 푸시합니다. 그런 다음 사용자가 재등록하여 계속합니다.
- 보안 작업을 푸시하여 특정 장치를 선택적으로 초기화합니다. 이렇게 하면 장치에서 모든 회사 앱 및 데이터가 제거됩니다. 그러면 해당 장치만 포함하는 배달 그룹에서 장치 정책을 제거하고 배달 그룹을 장치로 푸시할 수 있습니다. 그런 다음 사용자가 재등록하여 계속합니다.

- Chrome OS

Chrome OS 장치에서 장치 정책을 제거하려면 해당 장치만 포함하는 배달 그룹에서 장치 정책을 제거하면 됩니다. 그런 다음 배달 그룹을 장치에 푸시합니다.

장치 정책 편집

정책을 편집하려면 정책 옆에 있는 확인란을 선택하여 정책 목록 위에 옵션 메뉴를 표시합니다. 또는 목록에서 정책을 클릭하여 목록 오른쪽에 옵션 메뉴를 표시합니다.

Device Policies						
Apps Media Actions ShareFile Enrollment Profiles Delivery Groups						
<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	▼
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input checked="" type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink				
<input type="checkbox"/>	K--Passcode	Password				
<input type="checkbox"/>	K--Wifi	Wifi				
<input type="checkbox"/>	K--T&C	Terms Conditions				
<input type="checkbox"/>	K--Location	Locationservices				
<input type="checkbox"/>	K--EAS	Exchange				
<input type="checkbox"/>	K--AppLock	Applock				

Edit | Delete

Deployment

0
Installed

0
Pending

0
Failed

[Show more >](#)

정책 세부 정보를 보려면 자세히 표시를 클릭합니다.

장치 정책에 대한 모든 설정을 편집하려면 편집을 클릭합니다.

삭제를 클릭하면 확인 대화 상자가 나타납니다. 삭제를 다시 클릭하여 정책을 삭제합니다.

정책 배포 상태 확인

구성 > 장치 정책 페이지에서 정책 행을 클릭하여 배포 상태를 확인합니다.

9/2/19 4:39:39 am

Edit | Delete

Deployment

2
Installed

0
Pending

0
Failed

[Show more >](#)

정책 배포가 보류 중인 경우 사용자는 기본 설정 > 장치 정보 > 정책 새로 고침을 눌러 Secure Hub 에서 정책을 새로 고칠 수 있습니다.

추가된 장치 정책 목록 필터링

추가된 정책 목록을 정책 유형, 플랫폼 및 관련 배달 그룹으로 필터링할 수 있습니다. 구성 > 장치 정책 페이지에서 필터 표시를 클릭합니다. 목록에서 보려는 항목의 확인란을 선택합니다.

Filters

Clear All

► Policy Type

Clear

▼ Policy Platform

Clear

☐ iOS

14

☐ macOS

5

☐ Android

13

☐ Samsung KNOX

3

☐ Android for Work

1

Show more

► Associated Delivery Group

Clear

Device Policies

Hide filter

Search

Q

+

Add

−

Export

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	▼
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input type="checkbox"/>	K--ApplInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM		
<input type="checkbox"/>	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM		

필터를 저장하려면 이 보기 저장을 클릭합니다. 그러면 해당 필터 이름이 이 보기 저장 단추 아래의 단추에 표시됩니다.

장치 정책 요약

장치 정책 이름	장치 정책 설명
AirPlay 미러링	특정 AirPlay 장치 (예: 다른 Mac 컴퓨터) 를 iOS 장치에 추가합니다. 감독되는 장치의 허용 목록에 장치를 추가하는 옵션도 있습니다. 이 옵션은 사용자를 허용 목록의 AirPlay 장치로만 제한합니다.
AirPrint	iOS 장치의 AirPrint 프린터 목록에 AirPrint 프린터를 추가합니다. 이 정책을 사용하면 프린터와 장치가 서로 다른 서브넷에 있는 환경을 보다 쉽게 지원할 수 있습니다.
Android Enterprise 앱 권한	작업 프로필 내의 Android Enterprise 앱에 대한 요청에서 Google 이 “위험한” 권한이라고 하는 권한을 처리하는 방법을 구성합니다.
Android Enterprise 앱 제한	Android 앱과 관련된 제한 사항을 업데이트합니다.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

617

장치 정책 이름	장치 정책 설명
APN	특정 전화 이동 통신 사업자의 GPRS(General Packet Radio Service)에 장치를 연결하는 데 사용되는 설정을 지정합니다. 이 설정은 대부분의 최신 휴대폰에 이미 정의되어 있습니다. 조직이 모바일 장치에서 인터넷에 연결하는 데 소비자 APN을 사용하지 않는 경우 이 정책을 사용합니다.
앱 액세스	장치의 필수 앱, 선택적 앱 또는 차단 앱 목록을 정의합니다. 그런 다음 자동화된 동작을 만들어 장치가 앱 목록을 따르는 데 대응할 수 있습니다.
앱 특성	iOS 장치에 대한 관리되는 앱 번들 ID 또는 앱별 VPN 식별자와 같은 특성을 지정합니다.
앱 구성	관리되는 구성을 지원하는 앱의 다양한 설정 및 동작을 원격으로 구성합니다. 이렇게 하려면 iOS 장치에 XML 구성 파일 (속성 목록 또는 plist)을 배포합니다. 또는 Windows 10 휴대폰, Windows 10 또는 Windows 11을 실행하는 데스크톱, 태블릿 장치에 키/값 쌍을 배포합니다.
앱 인벤토리	관리되는 장치에서 앱의 인벤토리를 수집합니다. 그러면 XenMobile이 해당 장치에 배포된 앱 액세스 정책과 인벤토리를 비교합니다. 이런 방식으로 앱 액세스 허용 또는 차단 목록에 있는 앱을 감지하고 적절한 조치를 수행할 수 있습니다.
앱 잠금	사용자가 iOS 또는 특정 Android 장치에서 실행할 수 있거나 실행할 수 없는 앱의 목록을 정의합니다.
앱 네트워크 사용	iOS 장치에서 관리되는 앱이 셀룰러 데이터 네트워크와 같은 네트워크를 사용하는 방식을 지정하는 네트워크 사용 규칙을 설정합니다. 이러한 규칙은 관리되는 앱에만 적용됩니다. 관리되는 앱은 XenMobile을 통해 사용자 장치에 배포되는 앱입니다.
앱 제거	사용자 장치에서 앱을 제거합니다.
앱 알림	iOS 사용자가 지정된 앱의 알림을 수신하는 방법을 제어합니다.
관리되는 앱 자동 업데이트	Android Enterprise 장치에서 설치되어 있는 관리되는 앱이 업데이트되는 방식을 제어합니다.
BitLocker	Windows 10 및 Windows 11 장치의 BitLocker 인터페이스에서 사용할 수 있는 설정을 구성합니다.
일정 (CalDav)	iOS 또는 macOS 장치에 일정 (CalDAV) 계정을 추가합니다. CalDAV 계정을 사용하면 CalDAV를 지원하는 모든 서버와 일정 데이터를 동기화할 수 있습니다.
셀룰러	셀룰러 네트워크 설정을 구성합니다.

장치 정책 이름	장치 정책 설명
연결 관리자	인터넷 및 사설망에 자동으로 연결되는 앱에 대한 연결 설정을 지정합니다. 이 정책은 Windows Pocket PC에서만 사용할 수 있습니다.
연락처 (CardDAV)	iOS 또는 macOS 장치에 iOS 연락처 (CardDAV) 계정을 추가합니다. CardDAV 계정을 사용하면 CardDAV를 지원하는 모든 서버와 연락처 데이터를 동기화할 수 있습니다.
OS 업데이트 제어	감독되는 지원 장치에 최신 OS 업데이트를 배포합니다.
자격 증명	XenMobile의 PKI 구성에 대한 통합된 인증을 수행할 수 있습니다. 예를 들어 PKI 엔터티, 키 저장소, 자격 증명 공급자 또는 서버 인증서에 대한 인증이 가능합니다.
사용자 지정 XML	장치 프로비전, 장치 기능 사용, 장치 구성 및 장애 관리 같은 기능을 최적화합니다.
Defender	Windows 10 및 Windows 11 데스크톱과 태블릿의 Windows Defender 설정을 구성합니다.
장치 상태 증명	Windows 10 및 Windows 11 장치가 해당 상태를 보고하도록 합니다. 이를 위해 장치에서 특정 데이터 및 런타임 정보를 분석을 위해 HAS(상태 증명 서비스)로 전송합니다. HAS에서 상태 증명 인증서를 생성하고 반환하면 장치가 이를 XenMobile에 보냅니다. XenMobile은 상태 증명 인증서를 받은 후 인증서의 내용에 따라 이전에 구성된 자동 동작을 배포할 수 있습니다.
장치 이름	장치를 식별할 수 있도록 iOS와 macOS 장치에 이름을 설정합니다. 매크로, 텍스트 또는 둘의 조합을 사용하여 장치 이름을 정의할 수 있습니다.
교육 구성	Apple 교육을 사용할 강사 및 학생 장치를 구성합니다. 강사가 Classroom 앱을 사용하는 경우 교육 구성 장치 정책이 필요합니다.
Exchange	장치의 기본 전자 메일 클라이언트에서 ActiveSync 전자 메일을 사용하도록 설정합니다.
파일	사용자에 대한 특정 기능을 수행하는 스크립트 파일을 XenMobile에 추가합니다. 또는 Android 장치 사용자가 장치에서 액세스할 수 있는 문서 파일을 추가할 수 있습니다. 파일을 추가하는 경우 장치에서 파일이 저장될 디렉터리를 지정할 수도 있습니다.
FileVault	이 정책을 사용하면 등록된 macOS 장치에서 FileVault 장치 암호화를 사용하도록 설정할 수 있습니다. 사용자가 로그인할 때 FileVault 설정을 건너뛸 수 있는 횟수를 제어할 수도 있습니다. macOS 10.7 이상에서 사용할 수 있습니다.

장치 정책 이름	장치 정책 설명
글꼴	iOS와 macOS 장치에 추가 글꼴을 추가합니다. 글꼴은 트루타입 (.TTF) 또는 오픈타입 (.OFT) 형식이어야 합니다. XenMobile은 글꼴 모음 (.TTC 또는 .OTC)을 지원하지 않습니다.
홈 화면 레이아웃	iOS 9.3 이상의 감독되는 장치에서 iOS 홈 화면의 앱 및 폴더 레이아웃을 지정합니다.
iOS 및 macOS 프로필 가져오기	XenMobile로 iOS와 macOS 장치를 위한 장치 구성 XML 파일을 가져옵니다. 이 파일에는 Apple Configurator로 작성한 장치 보안 정책 및 제한 사항이 포함되어 있습니다.
Keyguard 관리	장치 Keyguard와 Work Challenge Keyguard의 잠금을 해제하기 전에 사용자에게 제공되는 기능을 제어합니다. 완전 관리형 전용 장치에 대한 장치 Keyguard 기능도 제어할 수 있습니다. 예를 들어 지문 잠금 해제, 신뢰할 수 있는 에이전트, 알림과 같은 잠금 화면 기능을 비활성화할 수 있습니다.
키오스크	Samsung SAFE 장치에서 앱 사용을 제한합니다. 사용 가능한 앱을 하나 이상의 특정 앱으로 제한할 수 있습니다. 이 정책은 특정 유형 또는 클래스의 앱만 실행하도록 마련된 회사 장치에 유용합니다. 또한 이 정책을 사용하면 키오스크 모드의 장치 홈 화면 및 잠금 화면 배경에 대한 사용자 지정 이미지를 선택할 수 있습니다.
Launcher 구성	허용되는 앱 및 Launcher 아이콘의 사용자 지정 로고 이미지 등 Android 장치의 Citrix Launcher에 대한 설정을 지정합니다.
LDAP	LDAP 서버 호스트 이름 등 필요한 모든 계정 정보를 비롯하여 iOS 장치에 사용할 LDAP 서버에 대한 정보를 제공합니다. 또한 LDAP 서버를 쿼리할 때 사용할 LDAP 검색 정책 집합을 제공합니다.
위치	장치에 Secure Hub에 대한 GPS가 설정된 경우 지도에서 장치의 위치를 찾을 수 있습니다. 장치에 이 정책을 배포한 후 XenMobile Server에서 찾기 명령을 보낼 수 있습니다. 그러면 장치가 해당 위치 좌표를 사용하여 응답합니다. 또한 XenMobile은 지오펜스 및 추적 정책을 지원합니다.
메일	iOS 또는 macOS 장치에 대한 전자 메일 계정을 구성합니다.

장치 정책 이름	장치 정책 설명
관리되는 도메인	전자 메일 및 Safari 브라우저에 적용되는 관리되는 도메인을 정의합니다. 관리되는 도메인을 사용하면 Safari 를 사용하여 도메인에서 다운로드한 문서를 열 수 있는 앱을 제어함으로써 회사 데이터를 보호할 수 있습니다. iOS 8 이상의 감독되는 장치의 경우 URL 또는 하위 도메인을 지정하여 사용자가 브라우저에서 문서, 첨부 파일 및 다운로드를 열 수 있는 방법을 제어할 수 있습니다.
MDM 옵션	감독되는 iOS 7.0 이상의 전화 장치에서 내 전화 찾기 및 iPad 활성화 잠금을 관리합니다.
조직 정보	XenMobile 이 iOS 장치에 배포하는 알림 메시지에 대한 조직 정보를 지정합니다.
암호	관리되는 장치에 PIN 코드 또는 암호를 적용합니다. 장치서 암호 복잡성과 시간 초과를 설정할 수 있습니다.
개인 핫스팟	사용자가 WiFi 네트워크 범위 내에 없는 경우 인터넷에 연결할 수 있습니다. 사용자는 개인 핫스팟 기능을 사용하여 iOS 장치에서 셀룰러 데이터 연결을 통해 연결합니다.
프로필 제거	사용자의 iOS 또는 macOS 장치에서 앱 프로필을 제거합니다.
프로비전 프로필	장치에 보낼 엔터프라이즈 배포 프로비전 프로필을 지정합니다. iOS 엔터프라이즈 앱을 개발하고 코드 서명하는 경우 일반적으로 프로비전 프로필을 포함합니다. Apple iOS 장치에서 앱을 실행하려면 이 프로필이 필요합니다. 프로비전 프로필이 누락되었거나 만료된 경우 사용자가 앱을 눌러서 열 때 앱의 작동이 중단됩니다.
프로비전 프로필 제거	iOS 프로비전 프로필을 제거합니다.
프록시	iOS 를 실행하는 장치에 대한 글로벌 HTTP 프록시 설정을 지정합니다. 장치당 하나의 글로벌 HTTP 프록시 정책만 배포할 수 있습니다.
제한 사항	관리되는 장치의 기능을 잠그고 제어하기 위한 수백 개의 옵션을 제공합니다. 제한 옵션의 예로는 카메라 또는 마이크를 사용하지 않도록 설정, 로밍 규칙 적용, 앱 스토어를 비롯한 타사 서비스에 대한 액세스 적용 등이 있습니다.
로밍	iOS 장치에서 음성 및 데이터 로밍을 허용할 것인지 여부를 구성합니다. 음성 로밍을 사용하지 않도록 설정하면 데이터 로밍이 자동으로 비활성화됩니다.

장치 정책 이름	장치 정책 설명
예약	MDM 관리, 앱 푸시 및 정책 배포를 위해 Android 장치에서 XenMobile Server 에 다시 연결하는 데 필요합니다. 이 정책을 장치에 보내지 않고 Google FCM 을 사용하도록 설정하지 않을 경우 장치에서 서버에 다시 연결할 수 없습니다.
SCEP	외부 SCEP 서버에서 인증서를 검색하도록 iOS 및 macOS 장치를 구성합니다. 또한 XenMobile 에 연결되어 있는 PKI 의 SCEP 를 사용하여 장치에 인증서를 제공할 수 있습니다. 이를 위해 분산 모드에서 PKI 엔터티와 PKI 공급자를 만듭니다.
SSO 계정	사용자가 XenMobile 과 회사 내부 리소스에 액세스하기 위해 한 번만 로그인하도록 SSO(Single Sign-On) 계정을 만듭니다. 사용자가 장치에 자격 증명을 저장할 필요가 없습니다. XenMobile 은 App Store 의 앱을 포함한 앱 전반의 SSO 계정에 엔터프라이즈 사용자 자격 증명을 사용합니다. 이 정책은 Kerberos 인증과 호환됩니다. iOS 에서 사용할 수 있습니다.
구독 중인 일정	iOS 장치의 캘린더 목록에 구독 일정을 추가합니다. 사용자 장치의 구독 일정 목록에 추가하기 전에 일정을 구독해야 합니다.
약관	사용자가 회사 네트워크에 대한 연결을 제어하는 특정 회사 정책에 동의하도록 요구합니다. 사용자가 XenMobile 에 장치를 등록할 때 약관에 동의해야만 장치를 등록할 수 있습니다. 약관에 동의하지 않으면 등록 프로세스가 취소됩니다.
터널	원격 지원에만 사용됩니다. 원격 지원을 사용하면 지원 센터 담당자가 관리되는 Windows CE 및 Android 모바일 장치를 원격으로 제어할 수 있습니다. 원격 지원은 클러스터링된 온-프레미스 XenMobile Server 배포에서 지원되지 않습니다. 2019 년 1 월 1 일부터 신규 고객에게는 더 이상 원격 지원이 제공되지 않습니다. 기존 고객은 제품을 계속 사용할 수 있지만 Citrix 는 개선 사항이나 수정 사항을 제공하지 않습니다.
VPN	레거시 VPN 게이트웨이 기술을 사용하는 백엔드 시스템에 대한 액세스를 제공합니다. 이 정책은 장치에 배포할 수 있는 VPN 게이트웨이 연결 세부 정보를 제공합니다. XenMobile 은 Cisco AnyConnect, Juniper, Citrix VPN 을 비롯한 여러 VPN 공급자를 지원합니다. VPN 게이트웨이가 이 옵션을 지원하는 경우 이 정책을 CA 에 연결하고 주문형 VPN 을 사용하도록 설정할 수 있습니다.

장치 정책 이름	장치 정책 설명
배경 화면	iOS 장치 잠금 화면, 홈 화면 또는 둘 다에 배경 화면을 설정하기 위해.png 또는.jpg 파일을 추가합니다. iPad 및 iPhone에서 서로 다른 배경 화면을 사용하려면 서로 다른 배경 화면 정책을 만들어 해당 사용자에게 배포합니다.
웹 콘텐츠 필터	iOS 장치에서 웹 콘텐츠를 필터링합니다. XenMobile은 Apple 자동 필터 기능과 허용 및 차단 목록에 추가된 사이트를 사용합니다. 감독되는 iOS 장치에서만 사용할 수 있습니다.
웹 클립	웹 사이트에 대한 바로 가기 또는 웹 클립을 배치하여 앱과 나란히 사용자 장치에 표시합니다. iOS, macOS X 및 Android 장치의 웹 클립을 나타내는 사용자 지정 아이콘을 지정할 수 있습니다. Windows 태블릿에는 레이블과 URL 만 필요합니다.
Wi-Fi	관리자가 관리되는 장치에 WiFi 라우터 세부 정보를 배포할 수 있습니다. 라우터 세부 정보에는 SSID, 인증 데이터 및 구성 데이터가 포함됩니다.
Windows Information Protection	정책에 대해 설정한 적용 수준에서 Windows Information Protection이 필요한 앱을 지정합니다. 이 정책은 감독되는 Windows 10 및 Windows 11 장치에 대한 것입니다.
XenMobile Store	XenMobile Store 웹 클립을 사용자 장치의 홈 화면에 표시할지 여부를 지정합니다.
XenMobile 옵션	Android 장치에서 XenMobile에 연결할 때 Secure Hub 동작을 구성합니다.
XenMobile 제거	Android 및 Windows Mobile/CE 장치에서 XenMobile을 제거합니다. 이 정책을 배포하면 배포 그룹에 있는 모든 장치에서 XenMobile이 제거됩니다.

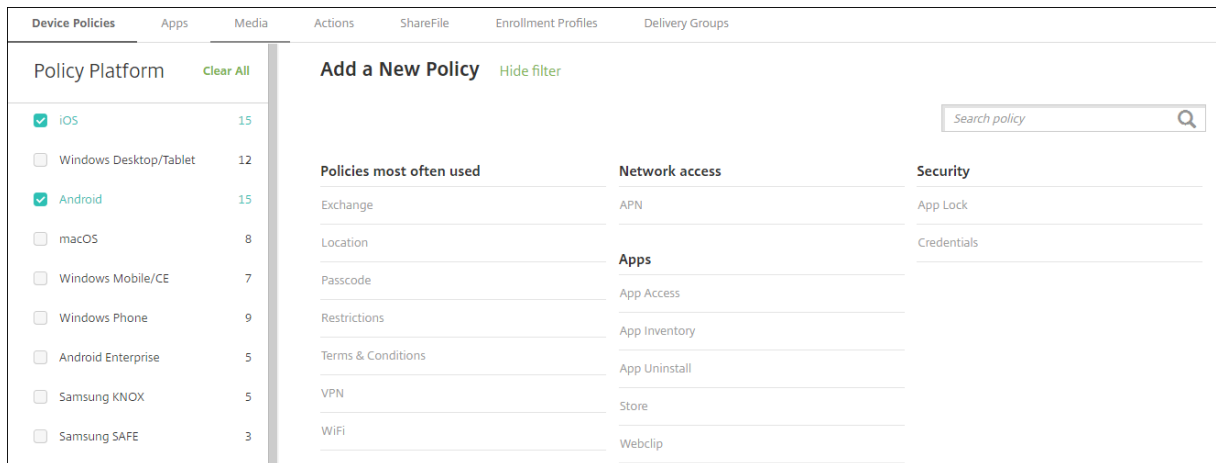
플랫폼별 장치 정책

August 12, 2022

플랫폼별로 사용 가능한 정책을 보려면:

1. XenMobile 콘솔에서 구성 > 장치 정책으로 이동합니다.
2. 추가를 클릭합니다.
3. 정책 플랫폼 창의 목록에 각 장치 플랫폼이 나타납니다. 해당 창이 열리지 않으면 필터 표시를 클릭합니다.

4. 단일 플랫폼에 사용할 수 있는 모든 정책 목록을 보려면 해당 플랫폼을 선택합니다. 여러 플랫폼에 사용할 수 있는 정책 목록을 보려면 각 플랫폼을 선택합니다. 정책은 선택한 각 플랫폼에 적용되는 경우에만 목록에 나타납니다.



XenMobile의 최신 릴리스는 다음과 같은 플랫폼에 대한 장치 정책을 지원합니다.

- Amazon
- Android
- Android Enterprise
- Android Zebra
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Windows 10 및 Windows 11 데스크탑/태블릿

XenMobile의 최신 릴리스에서 지원되는 장치에 대한 자세한 내용은 [지원되는 장치 플랫폼](#)을 참조하십시오.

참고:

환경에 GPO(그룹 정책 개체)가 구성되어 있는 경우:

Windows 10 및 Windows 11용 XenMobile 장치 정책을 구성할 때 다음 규칙을 고려하십시오. 하나 이상의 등록된 장치에서 정책이 충돌하는 경우 GPO와 일치하는 정책이 우선합니다.

AirPlay 미러링 장치 정책

March 15, 2024

Apple AirPlay 기능을 사용하면 장치 디스플레이의 내용을 다른 Mac 컴퓨터로 정확하게 미러링할 수 있습니다.

XenMobile 에서 특정 AirPlay 장치 (예: 다른 Mac 컴퓨터) 를 iOS 장치에 추가하는 장치 정책을 추가할 수 있습니다. 또한 감독되는 장치의 경우 허용 목록에 장치를 추가할 수 있습니다. 그러면 허용 목록에 있는 AirPlay 장치로만 사용자가 제한됩니다. 장치를 감독 모드로 전환하는 방법에 대한 자세한 내용은 [Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 전환](#)을 참조하십시오.

참고:

계속하기 전에 추가할 모든 장치에 대한 장치 ID 와 암호가 있는지 확인하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

AirPlay Mirroring Policy

This policy lets you specify specific AirPlay devices to add to users' iOS and macOS devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.

AirPlay Password

Device Name * Password * Add

Whitelist ID

Device ID * Add

Policy Settings

Remove policy ☒ Select date ☐ Duration until removal (in hours)

Allow user to remove policy Always

- **AirPlay 암호:** 추가할 각 장치에 대해 추가를 클릭하고 다음을 수행합니다.
 - 장치 **ID:** 하드웨어 주소 (MAC 주소) 를 xx:xx:xx:xx:xx:xx 형식으로 입력합니다. 이 필드는 대/소문자를 구분하지 않습니다.
 - 암호: 장치에 대한 선택적 암호를 입력합니다.
 - 추가를 클릭하여 장치를 추가하거나 취소를 클릭하여 장치 추가를 취소합니다.
- 화이트리스트 **ID:** 감독되지 않는 장치의 경우 이 목록이 무시됩니다. 이 목록의 장치 ID 는 사용자 장치에 제공되는 유일한 AirPlay 장치입니다. 목록에 추가할 각 AirPlay 장치에 대해 추가를 클릭하고 다음을 수행합니다.

참고:

XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는 용어가 포함됩니다. 향후 릴리스에서 이러한 용어를 “차단 목록” 및 “허용 목록” 으로 변경하는 중입니다.

- 장치 **ID:** 장치 ID 를 xx:xx:xx:xx:xx:xx 형식으로 입력합니다. 이 필드는 대/소문자를 구분하지 않습니다.
 - 추가를 클릭하여 장치를 추가하거나 취소를 클릭하여 장치 추가를 취소합니다.
- 정책 설정

- 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.

macOS 설정

- **AirPlay 암호:** 추가할 각 장치에 대해 추가를 클릭하고 다음을 수행합니다.
 - 장치 **ID:** 하드웨어 주소 (MAC 주소) 를 xx:xx:xx:xx:xx:xx 형식으로 입력합니다. 이 필드는 대/소문자를 구분하지 않습니다.
 - 암호: 장치에 대한 선택적 암호를 입력합니다.
 - 추가를 클릭하여 장치를 추가하거나 취소를 클릭하여 장치 추가를 취소합니다.
- 화이트리스트 **ID:** 감독되지 않는 장치의 경우 이 목록이 무시됩니다. 이 목록의 장치 ID 는 사용자 장치에 제공되는 유일한 AirPlay 장치입니다. 목록에 추가할 각 AirPlay 장치에 대해 추가를 클릭하고 다음을 수행합니다.
 - 장치 **ID:** 장치 ID 를 xx:xx:xx:xx:xx:xx 형식으로 입력합니다. 이 필드는 대/소문자를 구분하지 않습니다.
 - 추가를 클릭하여 장치를 추가하거나 취소를 클릭하여 장치 추가를 취소합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.
 - 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
 - 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

AirPrint 장치 정책

January 5, 2022

XenMobile 에서 장치 정책을 추가하여 AirPrint 프린터를 iOS 장치에 있는 AirPrint 프린터 목록에 추가할 수 있습니다. 이 정책을 사용하면 프린터와 장치가 서로 다른 서브넷에 있는 환경을 보다 쉽게 지원할 수 있습니다.

이 정책은 iOS 7.0 이상에 적용됩니다.

참고:

각 프린터의 IP 주소와 리소스 경로를 알고 있는지 확인하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- **AirPrint 대상:** 추가하려는 각 AirPrint 대상에 대해 추가를 클릭한 후 다음을 수행합니다.
 - **IP 주소:** AirPrint 프린터 IP 주소를 입력합니다.
 - **리소스 경로:** 프린터와 연결된 리소스 경로를 입력합니다. 이 값은 _ipps.tcp Bonjour 레코드의 매개 변수에 해당합니다. 예를 들어 printers/Canon_MG5300_series 또는 printers/Xerox_Phaser_7600 과 같습니다.
 - 저장을 클릭하여 프린터를 추가하거나 취소를 클릭하여 프린터 추가를 취소합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

Android Enterprise 앱 권한

March 15, 2024

작업 프로필 내의 Android Enterprise 앱에 대한 요청에서 Google 이 “위험한” 권한이라고 하는 권한을 처리하는 방법을 구성할 수 있습니다. 앱의 권한 요청에 대한 부여 또는 거부를 확인하는 메시지를 사용자에게 표시할지 여부를 제어할 수 있습니다. 이 기능은 Android 7.0 이상을 실행하는 장치에 적용됩니다.

Google 에서 위험한 권한이란 사용자의 개인 정보와 관련되거나 사용자의 저장된 데이터 또는 다른 앱의 작동에 영향을 미칠 수 있는 데이터 또는 리소스에 대한 액세스 권한을 앱에 제공하는 권한을 뜻합니다. 예를 들어 사용자의 연락처를 읽을 수 있는 권한은 위험한 권한입니다.

작업 프로필 안에 있는 Android Enterprise 앱에 대한 모든 위험한 권한 요청의 동작을 제어하는 글로벌 상태를 구성할 수 있습니다. 또한 Google 이 정의한 대로 개별 권한 그룹에 대한 위험한 권한 요청의 동작을 각 앱에 대해 제어할 수 있습니다. 이러한 개별 설정은 글로벌 상태를 재정의합니다.

Google 이 권한 그룹을 정의하는 방법에 대한 자세한 내용은 이 [Android 개발자 가이드](#)에서 “권한 그룹” 을 참조하십시오.

기본적으로 위험한 권한 요청을 부여하거나 거부하라는 메시지가 사용자에게 표시됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Android Enterprise 설정

Android for Work App Permissions

This policy lets you specify the behavior when Android for Work apps request dangerous permissions.

Global State * Prompt

Calendar

App *	Grant Status	Add
Gmail	Grant	

Camera

App *	Grant Status	Add
WhatsApp Messenger	Deny	

Contacts

App *	Grant Status	Add
Gmail	Prompt	
WhatsApp Messenger	Deny	

Location

App *	Grant Status	Add
-------	--------------	-----

Microphone

App *	Grant Status	Add
-------	--------------	-----

Back Next >

- **글로벌 상태:** 모든 위험한 권한 요청의 동작을 제어합니다. 목록에서 프롬프트, 부여 또는 거부를 클릭합니다.
 - **프롬프트:** 위험한 권한 요청을 부여하거나 거부하라는 메시지가 사용자에게 표시됩니다.
 - **부여:** 모든 위험한 권한 요청이 부여됩니다. 사용자에게 메시지가 표시되지 않습니다.
 - **거부:** 모든 위험한 권한 요청이 거부됩니다. 사용자에게 메시지가 표시되지 않습니다.

기본값은 프롬프트입니다.

- 앱별로 각 권한 그룹에 대한 개별 동작을 설정합니다. 권한 그룹의 동작을 구성하려면 추가를 클릭합니다. 앱 아래의 목록에서 앱을 선택합니다. Android Enterprise 시스템 앱을 구성하는 경우 새로 추가를 클릭하고 제한 장치 정책에서 사용하도록 설정한 응용 프로그램 패키지 이름을 입력합니다. 부여 상태에서 프롬프트, 부여 또는 거부를 선택합니다. 이 부여 상태는 글로벌 상태를 재정의합니다.

- **프롬프트:** 이 앱의 이 권한 그룹에서 위험한 권한 요청을 부여하거나 거부하라는 메시지가 사용자에게 표시됩니다.
- **부여:** 이 앱의 이 권한 그룹에서 위험한 권한 요청이 부여됩니다. 사용자에게 메시지가 표시되지 않습니다.

참고:

프로필 소유자 모드로 등록된 장치의 경우, Android 12 이상에서는 카메라, 위치, 마이크 및 센서에 대한 권한이 허용되지 않습니다.

- **거부:** 이 앱의 이 권한 그룹에서 위험한 권한 요청이 거부됩니다. 사용자에게 메시지가 표시되지 않습니다.

기본값은 프롬프트입니다.

- 앱 및 부여 상태 옆의 저장을 클릭합니다.
- 권한 그룹의 앱을 추가하려면 추가를 다시 클릭하고 이 단계를 반복합니다.
- 모든 권한 그룹에 대한 부여 상태 설정이 완료되면 다음을 클릭합니다.

APN 장치 정책

March 15, 2024

iOS 및 Android 장치에 대한 사용자 지정 APN(액세스 포인트 이름) 장치 정책을 추가할 수 있습니다. 조직에서 모바일 장치로 부터 인터넷에 연결하는 데 소비자 APN 을 사용하지 않을 경우 이 정책을 사용하십시오. APN 정책은 특정 이동통신 사업자의 GPRS(General Packet Radio Service) 에 장치를 연결하는 데 사용되는 설정을 결정합니다. 이 설정은 대부분의 최신 휴대폰에 이미 정의되어 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

APN Policy	APN Policy
1 Policy Info	This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.
2 Platforms	<div> <div>APN *</div> <div> <div>User name</div> <div>administrator</div> </div> <div> <div>Password</div> <div>*****</div> </div> <div> <div>Server proxy address</div> <div></div> </div> <div> <div>Server proxy port</div> <div></div> </div> </div>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Windows Mobile/CE	<div> <div>Remove policy</div> <div> <input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in hours) </div> <div> <div></div> <div></div> </div> </div>
3 Assignment	<div> <div>Back</div> <div>Next ></div> </div>

- **APN:** 액세스 지점의 이름을 입력합니다. 이 APN 이름은 허용된 iOS APN 과 일치해야 합니다. 그렇지 않으면 정책이 실패합니다.
- **사용자 이름:** 이 문자열은 이 APN 의 사용자 이름을 지정합니다. 사용자 이름이 누락된 경우 프로필 설치 중에 문자열을 입력하라는 메시지가 표시됩니다.
- **암호:** 이 APN 에 대한 사용자의 암호입니다. 쉽게 알 수 없도록 암호는 암호화됩니다. 암호가 페이로드에서 누락된 경우 프로필 설치 중에 암호를 묻는 메시지가 표시됩니다.
- **서버 프록시 주소:** APN 프록시의 IP 주소 또는 URL 입니다.
- **서버 프록시 포트:** APN 프록시의 포트 번호입니다. 서버 프록시 주소를 입력한 경우 이 서버 프록시 포트 번호가 필요합니다.
- 정책 설정의 정책 제거 옆에서 날짜 선택 또는 제거할 때까지의 기간 (시간) 을 클릭합니다.
 - 날짜 선택을 클릭하는 경우 달력을 클릭하여 제거할 날짜를 선택합니다.
 - 사용자가 정책을 제거하도록 허용 목록에서 항상, 암호 필요 또는 안 함을 클릭합니다.
 - 암호 필요를 클릭하는 경우 제거 암호 옆에 필요한 암호를 입력합니다.
- 정책 설정
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

Android 설정

APN Policy	APN Policy
1 Policy Info	This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.
2 Platforms	<div> <div>APN *</div> <div> <div>User name</div> <div>administrator</div> </div> <div> <div>Password</div> <div>.....</div> </div> <div> <div>Server</div> <div></div> </div> <div> <div>APN type</div> <div></div> </div> <div> <div>Authentication type</div> <div>None</div> </div> <div> <div>Server proxy address</div> <div></div> </div> <div> <div>Server proxy port</div> <div></div> </div> <div> <div>MMSC</div> <div></div> </div> </div>
<input type="checkbox"/> iOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	<div>Back</div> <div>Next ></div>

- **APN:** 액세스 지점의 이름을 입력합니다. 이 APN 이름은 허용된 Android APN 과 일치해야 합니다. 그렇지 않으면 정책이 실패합니다.
- **사용자 이름:** 이 문자열은 이 APN 의 사용자 이름을 지정합니다. 사용자 이름이 누락된 경우 프로필 설치 중에 문자열을 입력하라는 메시지가 표시됩니다.

- **암호:** 이 APN 에 대한 사용자의 암호입니다. 쉽게 알 수 없도록 암호는 암호화됩니다. 암호가 페이로드에서 누락된 경우 프로필 설치 중에 암호를 묻는 메시지가 표시됩니다.
- **서버:** 스마트폰을 대상으로 하는 이 설정은 대개 비어 있습니다. 표준 웹 사이트에 액세스할 수 없는 휴대폰의 경우 WAP(Wireless Application Protocol) 게이트웨이 서버를 참조합니다.
- **APN 유형:** 이 설정은 액세스 지점에 대한 이동통신 사업자의 의도된 용도와 일치해야 합니다. 이것은 심표로 구분된 APN 서비스 지정자 문자열이며 이동통신 사업자의 공표된 정의와 일치해야 합니다. 다음 예를 참조하십시오.
 - *: 모든 트래픽은 이 액세스 지점을 통과합니다.
 - mms: 멀티미디어 트래픽은 이 액세스 지점을 통과합니다.
 - default: 멀티미디어를 비롯한 모든 트래픽은 이 액세스 지점을 통과합니다.
 - supl: SUPL(Secure User Plane Location) 은 보조 GPS(A-GPS) 와 연결됩니다.
 - dun: 전화 접속 네트워킹은 시대에 뒤떨어져 거의 사용되지 않습니다.
 - hipri: 우선 순위가 높은 네트워킹입니다.
 - fota: FOTA(Firmware Over The Air) 는 펌웨어 업데이트를 수신하는 데 사용됩니다.
- **인증 유형:** 드롭다운 목록에서 사용할 인증 유형을 클릭합니다. 기본값은 없음입니다.
- **서버 프록시 주소:** 이동 통신 사업자 APN HTTP 프록시의 IP 주소 또는 URL 입니다.
- **서버 프록시 포트:** APN 프록시의 포트 번호입니다. 서버 프록시 주소를 입력한 경우 이 서버 프록시 포트 번호가 필요합니다.
- **MMSC:** 이동통신 사업자가 제공한 MMS 게이트웨이 서버 주소입니다.
- **MMS(멀티미디어 메시징 서버) 프록시 주소:** MMS 트래픽을 위한 멀티미디어 메시징 서비스 서버입니다. MMS 는 SMS 의 후신으로, 사진이나 비디오와 같은 멀티미디어 콘텐츠가 포함된 더 큰 메시지를 보낼 수 있습니다. 이러한 서버에는 특정 프로토콜 (예: MM1, ...MM11).
- **MMS 포트:** MMS 프록시에 사용되는 포트입니다.

앱 액세스 장치 정책

March 15, 2024

XenMobile 의 앱 액세스 장치 정책을 사용하여 다음 사항을 정의할 수 있습니다.

- 장치에 설치해야 하는 앱 목록입니다.
- 장치에 설치할 수 있는 앱 목록입니다.
- 장치에 설치해서는 안 되는 앱 목록입니다.

그런 다음 자동화된 동작을 만들어 장치가 앱 목록을 따르는 데 대응할 수 있습니다. iOS 및 Android 장치에 대한 앱 액세스 정책을 만들 수 있습니다.

한 번에 한 가지 유형의 액세스 정책만 구성할 수 있습니다. 필수 앱, 추천 앱 또는 허용되지 는 앱 목록 중 하나에 대한 정책만 추가할 수 있으며, 동일한 앱 액세스 정책 내에서 목록을 혼합할 수 없습니다. 각 유형의 목록에 대해 정책을 생성하는 경우 각 정책의

이름을 신중하게 지정할 것을 권장합니다. 각 정책의 이름을 신중하게 지정하면 XenMobile 의 어떤 정책이 어떤 앱 목록에 적용되는지 알 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

플랫폼 설정

- 액세스 정책: 필수, 추천 또는 금지를 클릭합니다. 기본값은 필수입니다.
- 하나 이상의 앱을 목록에 추가하려면 추가를 클릭한 후 다음을 수행합니다.
 - 앱 이름: 앱 이름을 입력합니다.
 - 앱 식별자: 선택적인 앱 식별자를 입력합니다.
 - 저장 또는 취소를 클릭합니다.
 - 추가할 각 앱에 대해 이 단계를 반복합니다.

앱 특성 장치 정책

March 15, 2024

앱 특성 장치 정책을 사용하면 iOS 장치에 대한 관리되는 앱 번들 ID 또는 앱별 VPN 식별자와 같은 특성을 지정할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

The screenshot shows the XenMobile 'Configure' page. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, a sub-navigation bar lists 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'App attributes' and includes a sidebar with '1 Policy Info', '2 Platforms', '3 Assignment', and 'iOS' (which is selected). The main panel for 'App attributes' contains the following settings:

- Managed app bundle ID ***: A dropdown menu with the option 'Make a selection'.
- Per-app VPN identifier**: A dropdown menu with the option 'None'.
- Removable app**: A toggle switch set to 'ON'.
- Enable associated domain direct download**: A toggle switch set to 'ON'.
- Associated Domains**: A text input field with an 'Add' button.
- Deployment Rules**: A section header with a right-pointing arrow.

At the bottom right of the configuration panel, there are 'Back' and 'Next >' buttons.

- 관리되는 앱 번들 **ID**: 드롭다운 목록에서 앱 번들 ID 를 클릭하거나 새로 추가를 클릭합니다.
 - 새로 추가를 클릭하는 경우 표시되는 필드에 앱 번들 ID 를 입력 합니다.
- 앱별 **VPN** 식별자: 드롭다운 목록에서 앱별 VPN 식별자를 클릭합니다.

앱 구성 장치 정책

August 12, 2022

다음은 배포하여 관리되는 구성을 지원하는 앱을 원격으로 구성할 수 있습니다.

- iOS 장치에 XML 구성 파일 (속성 목록 또는 plist 라고 함) 을 배포합니다.
- 또는 Windows 10 전화, Windows 10 또는 Windows 11 를 실행하는 태블릿 또는 데스크톱 장치에 대한 키/값 쌍 을 배포합니다.

구성에는 앱의 다양한 설정 및 동작을 지정합니다. 사용자가 앱을 설치하면 XenMobile 이 장치로 구성을 푸시합니다. 구성할 수 있는 실제 설정 및 동작은 앱에 따라 다르며 이 문서에서 다루지 않습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

App Configuration Policy	App Configuration Policy
1 Policy Info	This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed. For iOS devices, after you enter the dictionary content, you can check the syntax.
2 Platforms	Identifier * <input type="text" value="Make a selection"/>
<input checked="" type="checkbox"/> iOS	Dictionary content * <div></div>
<input checked="" type="checkbox"/> Windows Phone	<input type="button" value="Check Dictionary"/>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	
	► Deployment Rules

- 식별자: 목록에서 구성할 앱을 클릭하거나 새로 추가를 클릭하여 새 앱을 목록에 추가합니다.
 - 새로 추가를 클릭하는 경우 표시되는 필드에 앱 식별자를 입력합니다.
- 사전 내용: XML 속성 목록 (plist) 구성 정보를 입력하거나 복사하여 붙여 넣습니다.
- 사전 확인을 클릭합니다. XenMobile 이 XML 을 확인합니다. 오류가 없으면 콘텐츠 상자 아래에 올바른 **XML** 이 표시 됩니다. 콘텐츠 상자 아래에 구문 오류가 표시되면 계속하기 전에 해당 오류를 수정해야 합니다.

Windows 데스크톱/태블릿 설정

App Configuration Policy
1 Policy Info
2 Platforms
☐ iOS
☒ Windows Phone
☒ Windows Desktop/Tablet
3 Assignment

App Configuration Policy
This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed.

Make a selection

Parameter name *	Value *	⚙ Add
------------------	---------	-------

► Deployment Rules

App Configuration Policy
1 Policy Info
2 Platforms
☐ iOS
☐ Windows Phone
☒ Windows Desktop/Tablet
3 Assignment

App Configuration Policy
This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed.

Make a selection

Parameter name *	Value *	⚙ Add
------------------	---------	-------

► Deployment Rules

- 선택 목록에서 구성할 앱을 클릭하거나 새로 추가를 클릭하여 새 앱을 목록에 추가합니다.
 - 새로 추가를 클릭하는 경우 표시되는 필드에 패키지 제품군 이름을 입력합니다.
- 추가할 각 구성 매개 변수에 대해 추가를 클릭하고 다음을 수행합니다.
 - 매개 변수 이름: Windows 장치에 대한 응용 프로그램 설정의 키 이름을 입력합니다. Windows 앱 설정에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.
 - 값: 지정된 매개 변수의 값을 입력합니다.
 - 추가를 클릭하여 매개 변수를 추가하거나 취소를 클릭하여 매개 변수 추가를 취소합니다.

앱 인벤토리 장치 정책

August 12, 2022

앱 인벤토리 정책을 사용하면 관리되는 장치에서 앱의 인벤토리를 수집할 수 있습니다. 그러면 XenMobile 이 해당 장치에 배포된 앱 액세스 정책과 인벤토리를 비교합니다. 이런 방식으로 앱 허용 또는 차단 목록에 표시되는 앱을 감지하고 적절한 조치를 수행할 수 있습니다.

iOS, macOS, Android, Android Enterprise 또는 Windows Desktop/Tablet 장치에 대한 앱 액세스 정책을 만들 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

플랫폼 설정

App Inventory Policy

1 Policy Info

2 Platforms

☒ iOS
☒ macOS
☒ Android
☒ Android Enterprise
☒ Windows Desktop/Tablet
☒ Windows Phone
☒ Windows Mobile/CE

3 Assignment

App Inventory Policy

This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.

ios

ON

Deployment Rules

Back

Next >

- 선택한 각 플랫폼에 대해 기본 설정을 그대로 사용하거나 설정을 꺼짐으로 변경합니다. 기본값은 켜짐입니다.

앱 잠금 장치 정책

January 5, 2022

앱 잠금 장치 정책은 장치에서 실행될 수 있는 앱 목록 또는 장치에서 실행을 차단할 앱 목록을 정의합니다. iOS 및 Android 장치에 대해 이 정책을 구성할 수 있지만 정책이 작동하는 정확한 방식은 각 플랫폼마다 다릅니다. 예를 들어 iOS 장치에서는 여러 앱을 차단할 수 없습니다.

마찬가지로, iOS 장치에서는 정책당 하나의 iOS 앱만 선택할 수 있습니다. 즉, 사용자는 장치를 사용하여 하나의 앱만 실행할 수 있습니다. 앱 잠금 정책이 시행될 때 관리자가 구체적으로 허용한 옵션 외의 다른 어떤 작업도 장치에서 수행할 수 없습니다.

또한 iOS 장치에서 앱 잠금 정책을 푸시하려면 장치가 감독되어야 합니다.

장치 정책은 대부분의 Android L 및 M 장치에서 작동하지만 앱 잠금의 경우 필요한 API 를 Google 이 더 이상 제공하지 않기 때문에 Android N 이상 장치에서 작동하지 않습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

App Lock Policy	App Lock Policy This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.
1 Policy Info	App bundle ID * <input type="text" value="Make a selection"/>
2 Platforms	Options
<input checked="" type="checkbox"/> iOS	<div>Disable touch screen <input checked="" type="checkbox"/> ON iOS 7.0+</div> <div>Disable device rotation sensing <input type="checkbox"/> OFF iOS 7.0+</div> <div>Disable volume buttons <input type="checkbox"/> OFF iOS 7.0+</div> <div>Disable ringer switch <input type="checkbox"/> OFF iOS 7.0+</div> <div>Disable sleep/wake button <input type="checkbox"/> OFF iOS 7.0+</div> <div>Disable auto lock <input type="checkbox"/> OFF iOS 7.0+</div> <div>Enable VoiceOver <input type="checkbox"/> OFF iOS 7.0+</div> <div>Enable zoom <input type="checkbox"/> OFF iOS 7.0+</div>
<input checked="" type="checkbox"/> Android	
3 Assignment	

- 앱 번들 ID: 목록에서 이 정책을 적용할 앱을 클릭하거나 새로 추가를 클릭하여 새 앱을 목록에 추가합니다. 새로 추가를 선택하는 경우 표시되는 필드에 앱 이름을 입력합니다.
- 옵션: 다음 각 옵션은 iOS 7.0 이상에만 적용됩니다. 각 옵션의 기본값은 꺼짐이며 터치 스크린 사용 안 함은 예외적으로 기본값이 켜짐입니다.
 - 터치 스크린 사용 안 함
 - 장치 회전 감지 사용 안 함
 - 볼륨 단추 사용 안 함
 - 벨소리 전환 사용 안 함
벨소리 전환 사용 안 함이 켜짐인 경우 벨소리 동작은 처음 벨소리를 사용 안 함으로 설정할 때 스위치의 위치에 따라 다릅니다.
 - 절전 단추 사용 안 함
 - 자동 잠금 사용 안 함
 - VoiceOver 사용 안 함
 - 확대/축소 사용
 - 색 반전 사용
 - AssistiveTouch 사용
 - 선택 항목 말하기 사용
 - 모노 오디오 사용
- 사용자가 설정할 수 있는 옵션: 다음 각 옵션은 iOS 7.0 이상에만 적용됩니다. 각 옵션의 기본값은 꺼짐입니다.

- VoiceOver 조정 허용
- 확대/축소 조정 허용
- 색 반전 조정 허용
- AssitiveTouch 조정 허용

• 정책 설정

- 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

Android 설정

참고:

앱 잠금 장치 정책을 사용하여 Android 설정 앱을 차단할 수 없습니다.

App Lock Policy

This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.

App Lock parameters

Lock message

Unlock password

Prevent uninstall ☐ OFF

Lock screen Browse

Enforce ☒ Blacklist ☐ Whitelist

Apps

App name *	Add
<input type="text"/>	Add

• 앱 잠금 매개 변수

- 잠금 메시지: 사용자가 잠긴 앱을 열려고 할 때 표시할 메시지를 입력합니다.
- 잠금 해제 암호: 앱 잠금을 해제하는 암호를 입력합니다.
- 제거 금지: 사용자가 앱을 제거하도록 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 잠금 화면: 찾아보기를 클릭하고 파일의 위치로 이동하여 장치의 잠금 화면에 표시할 이미지를 선택합니다.
- 적용: 블랙리스트를 클릭하여 장치에서 실행될 수 없는 앱 목록을 만들거나 화이트리스트를 클릭하여 장치에서 실행될 수 있는 앱 목록을 만듭니다.

참고:

XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는 용어가 포함됩니다. 향후 릴리스에서 이러한 용어를 “차단 목록” 및 “허용 목록” 으로 변경하는 중입니다.

- 앱: 추가를 클릭하고 다음을 수행합니다.
 - 앱 이름: 목록에서 앱 이름을 클릭하여 허용 또는 차단 목록에 추가하거나 새로 추가를 클릭하여 사용 가능한 앱 목록에 새 앱을 추가합니다.
 - 새로 추가를 선택하는 경우 표시되는 필드에 앱 이름을 입력합니다.
 - 저장 또는 취소를 클릭합니다.
 - 허용 또는 차단 목록에 추가할 각 앱에 이러한 단계를 반복합니다.

앱 네트워크 사용 장치 정책

January 5, 2022

iOS 장치에서 관리되는 앱이 셀룰러 데이터 네트워크와 같은 네트워크를 사용하는 방식을 지정하는 네트워크 사용 규칙을 설정할 수 있습니다. 이러한 규칙은 관리되는 앱에만 적용됩니다. 관리되는 앱은 XenMobile 을 통해 사용자 장치에 배포되는 앱입니다. XenMobile 을 통해 배포되지 않고 사용자가 장치에 직접 다운로드한 앱이나 장치를 XenMobile 에 등록할 때 장치에 이미 설치되어 있던 앱은 여기에 해당되지 않습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

ios 설정

- 로밍 셀룰러 데이터 허용: 지정된 앱이 로밍 중에 셀룰러 데이터 연결을 사용할 수 있는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 셀룰러 데이터 허용: 지정된 앱이 셀룰러 데이터 연결을 사용할 수 있는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 앱 식별자 일치: 목록에 추가할 각 앱에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 앱 식별자: 앱 식별자를 입력합니다.
 - 목록에 앱을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.

앱 알림 장치 정책

January 5, 2022

앱 알림 정책을 사용하여 iOS 사용자가 지정된 앱의 알림을 수신하는 방법을 제어할 수 있습니다. 이 정책은 iOS 9.3 이상을 실행하는 장치에서 지원됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

The screenshot displays the 'Apps Notifications Policy' configuration page in the XenMobile console. The left sidebar shows the navigation menu with 'Policy Info', 'Platforms', 'iOS', and 'Assignment'. The main content area is titled 'Apps Notifications Policy' and includes a description: 'Choose how user will receive notifications from the selected apps. It is supported on iOS 9.3 and later.' Below this, there are two sections: 'Notifications Settings' and 'Policy Settings'. The 'Notifications Settings' section contains a table with columns for 'App Bundle Identifier', 'Allow Notifications', 'Show in Notification Center', 'Badge App Icon', 'Sounds', 'Show on Lock Screen', 'Show in Car Play', 'Enable Critical Alert', and 'Unlocked Alert Style'. The 'Policy Settings' section includes options for 'Remove policy' (Select date or Duration until removal), 'Allow user to remove policy' (Always), and 'Profile scope' (System).

- 앱 번들 ID: 이 정책을 적용할 앱을 지정합니다.
- 알림 허용: 알림을 허용하려면 켜짐을 선택합니다.
- 알림 센터에 표시: 사용자 장치의 알림 센터에 알림을 표시하려면 켜짐을 선택합니다.
- 배지 앱 아이콘: 알림과 함께 배지 앱 아이콘을 표시하려면 켜짐을 선택합니다.
- 사운드: 알림과 함께 사운드를 포함하려면 켜짐을 선택합니다.
- 잠금 화면에 표시: 사용자 장치의 잠금 화면에 알림을 표시하려면 켜짐을 선택합니다.
- **CarPlay** 로 표시: 켜짐인 경우 Apple CarPlay 에 알림이 표시됩니다. iOS 12 이상에서 사용할 수 있습니다. 기본값은 켜짐입니다.
- 중요 알림 사용: 켜짐인 경우 앱이 방해 금지 및 벨소리 설정을 무시하는 중요 알림으로 알림을 표시할 수 있습니다. iOS 12 이상에서 사용할 수 있습니다. 기본값은 꺼짐입니다.
- 잠금 해제 경고 스타일: 목록에서 없음, 배너 또는 경고를 선택하여 잠금 해제 경고의 모양을 구성합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.
 - 프로필 범위: 이 정책을 사용자에 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 iOS 9.3 이상에서만 사용할 수 있습니다.

터널 장치 정책

November 1, 2022

응용 프로그램 터널 (앱 터널) 은 모바일 앱의 무중단 서비스 및 데이터 전송 안정성을 개선하도록 설계되었습니다. 앱 터널은 모든 모바일 장치 앱의 클라이언트 구성 요소와 앱 서버 구성 요소 간의 프록시 매개 변수를 정의합니다. Android 장치에 대한 앱 터널 정책을 구성할 수 있습니다.

이 정책에서 정의한 터널을 통해 전송되는 모든 앱 트래픽은 앱을 실행하는 서버로 리디렉션되기 전에 XenMobile 을 통과합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Android 설정

Tunnel Policy	Tunnel Policy
1 Policy Info	This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.
2 Platforms	Use this tunnel for remote support <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> Windows Mobile/CE	Connection configuration
3 Assignment	Connection initiated by <input type="text" value="Device"/> ⓘ Protocol <input type="text" value="Generic TCP"/> Maximum connections per device * <input type="text" value="1"/> ⓘ Define connection time out <input type="checkbox"/> OFF ⓘ Block cellular connections passing by this tunnel <input type="checkbox"/> OFF ⓘ App device parameters Redirect to XenMobile <input type="text" value="Through app settings"/> Client port * <input type="text"/> ⓘ App server parameters IP address or server name * <input type="text"/> Server port * <input type="text"/> ► Deployment Rules

- 연결을 시작한 원본: 장치 또는 서버를 클릭하여 연결을 시작하는 원본을 지정합니다.
- 장치당 최대 연결 수: 숫자를 입력하여 앱에서 설정할 수 있는 동시 TCP 연결 수를 지정합니다. 이 필드는 장치에서 시작된 연결에만 적용됩니다.
- 연결 시간 제한 정의: 터널이 닫히기 전까지 앱이 유휴 상태로 있을 수 있는 시간을 설정할지 여부를 선택합니다.
 - 연결 시간 제한: 연결 시간 제한 정의를 켜짐으로 설정한 경우 터널이 닫히기 전까지 앱이 유휴 상태로 있을 수 있는 시간을 초로 입력합니다.
- 이 터널을 통과하는 셀룰러 연결 차단: 로밍 중에 이 터널을 차단할지 여부를 선택합니다. WiFi 및 USB 연결은 차단되지 않습니다.
- **XenMobile** 로 리디렉션: 앱 설정을 통해 선택합니다.
- 클라이언트 포트: 클라이언트 포트 번호를 입력합니다. 대부분의 경우 이 값은 서버 포트와 동일합니다.
- **IP** 주소 또는 서버 이름: 앱 서버의 IP 주소 또는 이름을 입력합니다. 이 필드는 장치에서 시작된 연결에만 적용됩니다.

- **서버 포트:** 서버 포트 번호를 입력합니다.

앱 제거 장치 정책

August 12, 2022

iOS, Android, Samsung KNOX, Android Enterprise 및 Windows Desktop/Tablet 플랫폼에 대한 앱 제거 정책을 만들 수 있습니다. 앱 제거 정책을 사용하면 여러 가지 이유로 사용자 장치에서 앱을 제거할 수 있습니다. 예를 들어 특정 앱을 더 이상 지원하지 않으려 하거나 회사가 기존 앱을 다른 공급업체의 유사한 앱으로 교체하려고 할 수 있습니다.

이 정책이 사용자 장치에 배포되면 해당 앱이 제거됩니다. Samsung KNOX 장치를 제외하고 사용자에게 앱을 제거할 것인지 묻는 메시지가 표시됩니다. Samsung KNOX 장치 사용자에게는 앱을 제거할 것인지 묻는 메시지가 나타나지 않습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

App Uninstall Policy	App Uninstall Policy
1 Policy Info	This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.
2 Platforms	Managed app bundle ID * <input type="text" value="Make a selection"/>
<input checked="" type="checkbox"/> iOS	► Deployment Rules
<input checked="" type="checkbox"/> Android	
<input checked="" type="checkbox"/> Samsung KNOX	
<input checked="" type="checkbox"/> Android for Work	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- 관리되는 앱 번들 **ID:** 목록에서 기존 앱을 클릭하거나 새로 추가를 클릭합니다. 이 플랫폼에 구성된 앱이 없는 경우 목록은 비어 있을 것이므로 새 앱을 추가해야 합니다.
 - 추가를 클릭하면 앱 이름을 입력할 수 있는 필드가 나타납니다.

다른 모든 플랫폼 설정

- 제거할 앱: 추가하려는 각 앱에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 앱 이름: 목록에서 기존 앱을 클릭하거나 새로 추가를 클릭하여 새 앱 이름을 입력합니다. 이 플랫폼에 구성된 앱이 없는 경우 목록은 비어 있을 것이므로 새 앱을 추가해야 합니다.
 - 추가를 클릭하여 앱을 추가하거나 취소를 클릭하여 앱 추가를 취소합니다.

해당 공용 앱 스토어 앱을 설치한 후 자동으로 엔터프라이즈 앱을 제거합니다

공용 앱 스토어 버전이 설치될 때 Citrix 앱의 엔터프라이즈 버전을 제거하도록 XenMobile 을 구성할 수 있습니다. 이 기능을 사용하면 공용 앱 스토어 버전이 설치된 후 사용자 장치에 두 개의 동일한 앱 아이콘이 나타나는 것이 방지됩니다.

앱 제거 장치 정책의 배포 조건은 새 버전 설치 시 이전 앱을 사용자 장치에서 제거하도록 XenMobile 을 트리거합니다. 이 기능은 XenMobile Server 에 엔터프라이즈 모드 (XME) 로 연결되어 관리되는 iOS 장치에서만 사용할 수 있습니다.

설치된 앱 이름 조건을 사용하여 배포 규칙을 구성하려면:

- 엔터프라이즈 앱에 대한 관리되는 앱 번들 ID 를 지정합니다.
- 규칙 추가: 새 규칙을 클릭한 다음 샘플에 표시된 것과 같이 설치된 앱 이름 및 같음을 선택합니다. 공용 앱 스토어 앱의 앱 번들 ID 를 입력합니다.

예제에서 공용 앱 스토어 앱 (com.citrix.mail.ios) 이 지정된 배달 그룹의 장치에 설치될 때 XenMobile 이 엔터프라이즈 버전 (com.citrix.mail) 을 제거합니다.

관리되는 앱 자동 업데이트 장치 정책

August 24, 2022

이 정책은 Android Enterprise 장치에서 설치되어 있는 관리되는 앱이 업데이트되는 방식을 제어합니다. 사용자가 장치에서 앱을 자동 업데이트하는 기능을 제한할 수 있습니다. 사용자가 기기에서 앱에 대한 자동 업데이트를 제어할 수 있도록 허용할 경우 관리되는 Google Play 스토어에서 자동 앱 업데이트 정책을 설정합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Automatically Update Managed Apps Policy	Automatically Update Managed Apps Policy	
	This policy automatically updates the installed managed apps on the device.	
1 Policy Info	Automatically update managed apps	Always
2 Platforms Clear All	App update priority	<input checked="" type="checkbox"/> ?
<input checked="" type="checkbox"/> Android Enterprise	Set priority for updating apps	
3 Assignment	Available apps *	App auto update priority Add
	Deployment Rules	

- 관리되는 앱 자동 업데이트
 - 항상: 자동 앱 업데이트를 활성화합니다. 항상 기본값입니다.
 - 사용자가 정책을 구성하도록 허용: 사용자가 관리되는 Google Play 스토어에서 기기에 대한 자동 앱 업데이트 정책을 구성하도록 허용합니다.
 - 사용 안 함: 자동 앱 업데이트를 비활성화합니다.
 - 장치가 **Wi-Fi** 에 연결된 경우에만: 장치가 Wi-Fi 에 연결된 경우에만 자동 앱 업데이트를 허용합니다.

- 앱 업데이트 우선 순위: 커짐인 경우 각 관리되는 앱의 업데이트 우선 순위 수준을 구성할 수 있습니다.
- 앱 업데이트 우선 순위 설정: 추가를 클릭하여 앱의 업데이트 우선 순위를 구성합니다.

Available apps *	App auto update priority	
Make a selection ▼	<input checked="" type="radio"/> Auto update low priority <input type="radio"/> Auto update high priority <input type="radio"/> Auto update postponed	Save Cancel

- 사용 가능한 앱: 메뉴에서 앱을 선택하여 업데이트 우선 순위를 구성합니다.
- 앱 자동 업데이트 우선 순위: 다음에서 업데이트 우선 순위를 선택합니다.
 - 낮은 우선 순위 자동 업데이트: 기기가 충전 중이고, 활발하게 사용되고 있지 않으며, 무제한 네트워크에 연결되면 앱이 업데이트됩니다.
 - 높은 우선 순위 자동 업데이트: 제한 없이 최대한 빨리 앱을 업데이트합니다.
 - 자동 업데이트 연기됨: 새 버전을 사용할 수 있게 된 후 최대 90 일 동안 앱이 자동으로 업데이트되지 않습니다. 90 일이 지나면 앱이 낮은 우선 순위로 자동 업데이트됩니다. 앱이 업데이트된 후 90 일 동안 앱이 자동으로 업데이트되지 않습니다. 사용자는 언제든지 앱을 수동으로 업데이트할 수 있습니다.
- 완료되면 저장을 클릭합니다. 연필 아이콘을 클릭하여 구성을 편집할 수 있습니다. 휴지통을 클릭하여 구성을 삭제합니다.

BitLocker 장치 정책

August 12, 2022

Windows 10 및 Windows 11에는 BitLocker라는 디스크 암호화 기능이 포함되어 있습니다. BitLocker는 분실 또는 도난 장치의 파일 및 시스템에 대한 무단 액세스를 추가로 보호합니다. BitLocker를 TPM(신뢰할 수 있는 플랫폼 모듈) 칩 버전 1.2 이상과 함께 사용하면 추가 보호를 적용할 수 있습니다. TPM 칩은 암호화 작업을 처리하고 암호화 키를 생성 및 저장하고 키 사용을 제한합니다.

Windows 10 빌드 1703부터 MDM 정책을 통해 BitLocker를 제어할 수 있습니다. XenMobile에서 BitLocker 장치 정책을 사용하여 Windows 10 및 Windows 11 장치의 BitLocker 마법사에서 제공되는 설정을 구성할 수 있습니다. 예를 들어 BitLocker가 활성화된 장치에서는 시작 시 드라이브 잠금을 해제하는 방법, 복구 키를 백업하는 방법 및 고정 드라이브의 잠금을 해제하는 방법에 대한 메시지를 사용자에게 표시할 수 있습니다. BitLocker 장치 정책 설정을 통해 다음을 구성할 수도 있습니다.

- TPM 칩이 없는 장치에서 BitLocker를 활성화할지 여부
- BitLocker 인터페이스에 복구 옵션을 표시할지 여부
- BitLocker가 활성화되지 않은 경우 고정 또는 이동식 드라이브에 대한 쓰기 액세스를 거부할지 여부

참고:

장치에서 BitLocker 암호화가 시작된 후에는 장치에 업데이트된 BitLocker 장치 정책을 배포하여 BitLocker 설정을 변경할 수 없습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

요구 사항

- BitLocker 장치 정책을 사용하려면 Windows 10 또는 Windows 11 Enterprise 버전이 필요합니다.
- BitLocker 장치 정책을 배포하기 전에 BitLocker 를 사용할 수 있도록 환경을 준비하십시오. BitLocker 시스템 요구 사항 및 설정을 포함한 Microsoft 의 자세한 정보는 [BitLocker](#) 및 해당 노드 아래의 문서를 참조하십시오.

Windows Desktop 및 태블릿 설정

Bitlocker policy	Bitlocker policy
1 Policy Info	This policy lets you enable Bitlocker on an enrolled machine and specify that encryption mechanism to use.
2 Platforms	<p>Bitlocker settings</p> <p>Require device to be encrypted <input type="checkbox"/> OFF</p> <p>Encryption settings</p> <p>Configure encryption methods <input type="checkbox"/> OFF ⓘ</p> <p>OS drive settings</p> <p>Require additional authentication at startup <input type="checkbox"/> OFF ⓘ</p> <p>PIN length</p> <p>Minimum PIN length <input type="text" value="6"/> ⓘ</p> <p>OS drive recovery settings</p> <p>Configure OS drive recovery <input type="checkbox"/> OFF ⓘ</p> <p>Customize preboot recovery message and URL <input type="checkbox"/> OFF ⓘ</p> <p>Fixed drive recovery settings</p> <p>Configure fixed drive recovery <input type="checkbox"/> OFF ⓘ</p> <p>Fixed drive settings</p> <p>Block write access to fixed drives not using BitLocker <input type="checkbox"/> OFF ⓘ</p> <p>Removable drive settings</p> <p>Block write access to removable drives not using BitLocker <input type="checkbox"/> OFF ⓘ</p> <p>Other drive settings</p> <p>Prompt for other disk encryption <input type="checkbox"/> OFF ⓘ</p>
<input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- **장치 암호화 필요:** Windows 데스크톱 또는 태블릿의 BitLocker 암호화 사용 설정에 대한 메시지를 사용자에게 표시할지 여부를 결정합니다. 꺼짐인 경우 등록이 완료되면 장치 암호화가 필요함을 나타내는 메시지가 표시됩니다. 꺼짐인 경우 사용자에게 메시지가 표시되지 않으며 BitLocker에는 정책 설정이 사용됩니다. 기본값은 꺼짐입니다.
- **암호화 방법 구성:** 특정 드라이브 유형에 사용할 암호화 방법을 결정합니다. 꺼짐인 경우 BitLocker 마법사에 드라이브 유형에 사용할 암호화 방법을 선택하라는 메시지가 표시됩니다. 모든 드라이브의 암호화 방법은 기본적으로 XTS-AES

128 비트입니다. 이동식 드라이브의 암호화 방법은 기본적으로 AES-CBC 128 비트입니다. 커짐인 경우 정책에 지정된 암호화 방법이 BitLocker에 사용됩니다. 커짐인 경우 운영 체제 드라이브, 고정 드라이브 및 이동식 드라이브의 추가 설정이 나타납니다. 각 드라이브 유형에 대해 기본 암호화 방법을 선택합니다. 기본값은 꺼짐입니다.

- **시작 시 추가 인증 필요:** 장치 시작 시 추가로 필요한 인증을 지정합니다. TPM 칩이 없는 장치에서 BitLocker를 허용할지 여부도 지정합니다. 꺼짐인 경우 TPM이 없는 장치에서 BitLocker 암호화를 사용할 수 없습니다. TPM에 대한 자세한 내용은 Microsoft 문서 [TPM\(신뢰할 수 있는 플랫폼 모듈\) 기술 개요](#)를 참조하십시오. 커짐인 경우 다음 추가 설정이 나타납니다. 기본값은 꺼짐입니다.

- **TPM 칩이 없는 장치에서 BitLocker 차단:** TPM 칩이 없는 장치에서 BitLocker를 사용하려면 잠금 해제 암호 또는 시작 키를 생성해야 합니다. 시작 키는 USB 드라이브에 저장되며 사용자는 시작 전에 USB 드라이브를 장치에 연결해야 합니다. 잠금 해제 암호는 8자 이상입니다. 기본값은 꺼짐입니다.
- **TPM 시작:** TPM이 있는 장치에는 TPM 전용, TPM + PIN, TPM + 키 및 TPM + PIN + 키의 네 가지 잠금 해제 모드가 있습니다. TPM 시작은 암호화 키가 TPM 칩에 저장되는 TPM 전용 모드를 위한 설정입니다. 이 모드에서는 사용자가 추가 잠금 해제 데이터를 제공하지 않아도 됩니다. 사용자 장치를 다시 시작하면 TPM 칩의 암호화 키를 사용하여 장치가 자동으로 잠금 해제됩니다. 기본값은 **TPM** 허용입니다.
- **TPM 시작 PIN:** 이 설정은 TPM + PIN 잠금 해제 모드입니다. PIN은 최대 20자리일 수 있습니다. 최소 PIN 길이를 지정하려면 최소 **PIN** 길이 설정을 사용합니다. PIN은 BitLocker를 설정할 때 사용자가 구성하며 장치를 시작할 때 이 PIN을 제공해야 합니다.
- **TPM 시작 키:** 이 설정은 TPM + 키 잠금 해제 모드입니다. 시작 키는 USB 또는 기타 이동식 드라이브에 저장되며 사용자는 시작 전에 장치에 드라이브를 연결해야 합니다.
- **TPM 시작 키 및 PIN:** 이 설정은 TPM + PIN + 키 잠금 해제 모드입니다.

잠금 해제에 성공하면 운영 체제가 로딩을 시작합니다. 잠금 해제에 실패하면 장치가 복구 모드로 전환됩니다.

- **최소 PIN 길이:** TPM 시작 PIN의 최소 길이입니다. 기본값은 **6**입니다.
- **OS 드라이브 복구 구성:** 잠금 해제 단계가 실패하면 BitLocker가 구성된 복구 키에 대한 메시지를 표시합니다. 이 설정은 잠금 해제 암호 또는 USB 시작 키가 없는 경우 사용자에게 제공되는 운영 체제 드라이브 복구 옵션을 구성합니다. 기본값은 꺼짐입니다.
 - **인증서 기반 데이터 복구 에이전트 허용:** 인증서 기반 데이터 복구 에이전트를 허용할지 여부를 지정합니다. GPMC(그룹 정책 관리 콘솔) 또는 로컬 그룹 정책 편집기에 위치한 공개 키 정책에서 데이터 복구 에이전트를 추가합니다. 데이터 복구 에이전트에 대한 자세한 내용은 Microsoft 문서 [BitLocker Group Policy settings\(BitLocker 그룹 정책 설정\)](#)를 참조하십시오. 기본값은 꺼짐입니다.
 - **OS 드라이브 복구용 48비트 복구 암호 만들기:** 사용자에게 복구 암호 사용을 허용할지, 아니면 필수로 할지를 지정합니다. BitLocker는 암호를 생성하고 파일 또는 Microsoft Cloud 계정에 저장합니다. 기본값은 **48**비트 암호 허용입니다.
 - **256비트 복구 키 만들기:** 복구 키 사용을 허용할지, 아니면 필수로 할지를 지정합니다. 복구 키는 BEK 파일로, USB 드라이브에 저장됩니다. 기본값은 **256**비트 복구 키 허용입니다.

- **OS** 드라이브 복구 옵션 숨기기: BitLocker 인터페이스에 복구 옵션을 표시할지, 숨길지 여부를 지정합니다. 켜짐인 경우 BitLocker 인터페이스에 복구 옵션이 표시되지 않습니다. 이 경우 장치를 Active Directory에 등록하고 복구 옵션을 Active Directory에 저장하고 **AD DS**에 복구 정보 저장을 켜짐으로 설정하십시오. 기본값은 꺼짐입니다.
 - **AD DS**에 복구 정보 저장: Active Directory 도메인 서비스에 복구 옵션을 저장할지 여부를 지정합니다. 기본값은 꺼짐입니다.
 - **AD DS**에 저장된 복구 정보 구성: BitLocker 복구 암호 또는 복구 암호 및 키 패키지를 Active Directory 도메인 서비스에 저장할지 여부를 지정합니다. 키 패키지를 저장하면 물리적으로 손상된 드라이브에서 데이터를 복구할 수 있습니다. 기본값은 복구 암호 백업입니다.
 - **AD DS**에 복구 정보 저장 후 **BitLocker** 사용: 장치가 도메인에 연결되고 BitLocker 복구 정보가 Active Directory에 백업된 경우에만 BitLocker를 사용할 수 있도록 할지 여부를 지정합니다. 켜짐인 경우 BitLocker를 시작하려면 장치가 도메인에 연결되어 있어야 합니다. 기본값은 꺼짐입니다.
- 사전 부팅 복구 메시지 및 **URL** 사용자 지정: 복구 화면에 BitLocker의 사용자 지정된 메시지 및 URL을 표시할지 여부를 지정합니다. 켜짐인 경우 기본 복구 메시지 및 **URL** 사용, 빈 복구 메시지 및 **URL** 사용, 사용자 지정 복구 메시지 사용 및 사용자 지정 복구 **URL** 사용의 추가 설정이 나타납니다. 꺼짐인 경우 기본 복구 메시지 및 URL이 표시됩니다. 기본값은 꺼짐입니다.
 - 고정 드라이브 복구 구성: BitLocker로 암호화된 고정 드라이브에 대한 사용자 복구 옵션을 구성합니다. BitLocker는 고정 드라이브 암호화에 대한 메시지를 사용자에게 표시하지 않습니다. 시작 시 드라이브 잠금을 해제하려면 사용자가 암호 또는 스마트 카드를 제공해야 합니다. 사용자가 고정 드라이브의 BitLocker 암호화를 사용하도록 설정한 경우 이 정책에 포함되지 않은 시작 잠금 해제 설정이 BitLocker 인터페이스에 표시됩니다. 관련 설정에 대한 자세한 내용은 이 목록의 앞 부분에 있는 **OS** 드라이브 복구 구성을 참조하십시오. 기본값은 꺼짐입니다.
 - **BitLocker**를 사용하지 않는 고정 드라이브에 대한 쓰기 액세스 차단: 켜짐인 경우 BitLocker로 암호화된 고정 드라이브에만 쓰기 작업을 수행할 수 있습니다. 기본값은 꺼짐입니다.
 - **BitLocker**를 사용하지 않는 이동식 드라이브에 대한 쓰기 액세스 차단: 켜짐인 경우 BitLocker로 암호화된 이동식 드라이브에만 쓰기 작업을 수행할 수 있습니다. 이 설정은 조직에서 다른 이동식 드라이브에 대한 쓰기 액세스를 허용하는지 여부에 따라 구성하십시오. 기본값은 꺼짐입니다.
 - 다른 디스크 암호화인 경우 메시지 표시: 장치의 다른 디스크 암호화에 대한 경고 메시지를 표시하지 않도록 설정할 수 있습니다. 기본값은 꺼짐입니다.

캘린더 (CalDav) 장치 정책

January 5, 2022

XenMobile에서 사용자의 iOS 또는 macOS 장치에 캘린더 (CalDAV) 계정을 추가하는 장치 정책을 추가할 수 있습니다. 이 정책을 사용하면 해당 사용자가 CalDAV를 지원하는 모든 서버와 일정 데이터를 동기화할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이것은 필수 필드입니다.
- **호스트 이름:** CalDAV 서버의 주소를 입력합니다. 이것은 필수 필드입니다.
- **포트:** CalDAV 서버에 연결하는 데 사용할 포트를 입력합니다. 이것은 필수 필드입니다. 기본값은 **8443**입니다.
- **보안 주체 URL:** 사용자의 일정에 대한 기본 URL을 입력합니다.
- **사용자 이름:** 사용자의 로그인 이름을 입력합니다. 이것은 필수 필드입니다.
- **암호:** 선택적 사용자 암호를 입력합니다.
- **SSL 사용:** CalDAV 서버에 대한 SSL 연결을 사용할 것인지 여부를 선택합니다. 기본값은 켜짐입니다.
- **정책 설정**
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간)입니다.
 - ★ **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ **제거할 때까지의 기간 (시간):** 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이것은 필수 필드입니다.
- **호스트 이름:** CalDAV 서버의 주소를 입력합니다. 이것은 필수 필드입니다.
- **포트:** CalDAV 서버에 연결하는 데 사용할 포트를 입력합니다. 이것은 필수 필드입니다. 기본값은 **8443**입니다.
- **보안 주체 URL:** 사용자의 일정에 대한 기본 URL을 입력합니다.
- **사용자 이름:** 사용자의 로그인 이름을 입력합니다. 이것은 필수 필드입니다.
- **암호:** 선택적 사용자 암호를 입력합니다.
- **SSL 사용:** CalDAV 서버에 대한 SSL 연결을 사용할 것인지 여부를 선택합니다. 기본값은 켜짐입니다.
- **정책 설정**
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간)입니다.
 - ★ **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ **제거할 때까지의 기간 (시간):** 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.

- 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
- 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

셀룰러 장치 정책

January 5, 2022

이 정책을 사용하면 iOS 장치에 대한 셀룰러 네트워크 설정을 구성할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

• APN 연결

- 이름: 이 구성의 이름입니다.
- 인증 유형: 목록에서 **CHAP**(Challenge Handshake 인증 프로토콜) 또는 **PAP**(암호 인증 프로토콜)를 클릭합니다. 기본값은 **PAP**입니다.
- 사용자 이름 및 암호: 인증에 사용할 사용자 이름과 암호입니다.

• APN

- 이름: APN(액세스 포인트 이름) 구성의 이름입니다.
- 인증 유형: 목록에서 **CHAP** 또는 **PAP**를 클릭합니다. 기본값은 **PAP**입니다.
- 사용자 이름 및 암호: 인증에 사용할 사용자 이름과 암호입니다.
- 프록시 서버: 프록시 서버 네트워크 주소입니다.
- 프록시 서버 포트: 프록시 서버 포트입니다.

• 정책 설정

- 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간)입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

연결 예약 장치 정책

February 2, 2022

중요:

FCM(Firebase Cloud Messaging) 을 사용하여 Android, Android Enterprise 및 Chrome OS 장치의 XenMobile Server 연결을 제어하는 것이 좋습니다. FCM 사용에 대한 자세한 내용은 [Firebase Cloud Messaging](#)을 참조하십시오.

FCM 을 사용하지 않도록 선택한 경우 연결 예약 정책을 만들어 사용자 장치에서 XenMobile Server 에 연결하는 방법과 시기를 제어할 수 있습니다.

사용자가 수동으로 장치에 연결하거나 장치가 정의된 시간 내에 연결하도록 지정할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

플랫폼 설정

- 장치에서 연결하도록 요구: 이 일정에 대해 설정할 옵션을 클릭합니다.
 - **항상:** 연결을 영구적으로 활성 상태로 유지합니다. 네트워크 연결이 끊긴 후 사용자 장치의 XenMobile 이 XenMobile 서버에 다시 연결을 시도하고 제어 패킷을 정기적으로 전송하여 연결을 모니터링합니다. 보안을 최적화하려면 이 옵션을 사용하는 것이 좋습니다. 항상을 선택하는 경우 장치 터널 정책인 연결 시간 제한 정의 설정을 사용하여 연결로 인해 배터리가 소진되지 않도록 하십시오. 연결을 활성 상태로 유지하면 초기화 또는 잠금과 같은 보안 명령을 주문형으로 장치에 푸시할 수 있습니다. 또한 장치에 배포하는 각 정책에서 배포 일정 옵션 상시 연결에 대해 배포를 선택해야 합니다.
 - **안 함:** 수동으로 연결합니다. 사용자가 장치의 XenMobile 에서 연결을 시작해야 합니다. 이 옵션을 사용하면 보안 정책을 장치에 배포할 수 없어 사용자가 새 앱 또는 정책을 받을 수 없으므로 프로덕션 배포에 사용하지 않는 것이 좋습니다.
 - **간격:** 지정된 간격으로 연결합니다. 이 옵션이 적용될 때 잠금 또는 초기화와 같은 보안 정책을 전송하면 다음에 장치가 연결할 때 동작이 처리됩니다. 이 옵션을 선택하면 **N** 분마다 연결 필드가 나타납니다. 이 필드에 장치를 다시 연결하기 전까지의 시간 (분) 을 입력해야 합니다. 기본값은 **20** 입니다.
 - **일정 정의:** 사용하면 네트워크 연결이 끊긴 후 사용자 장치의 XenMobile 이 XenMobile 서버에 다시 연결을 시도하고 제어 패킷을 정의된 시간 내에 정기적으로 전송하여 연결을 모니터링합니다. 연결 시간을 정의하는 방법은 다음에 나오는 연결 시간 정의를 참조하십시오.
 - * 다음 시간 동안 고정된 연결 유지: 사용자 장치가 정의된 시간 동안 연결되어야 합니다.
 - * 다음 각 범위 내에서 연결하도록 요구: 사용자 장치가 정의된 시간 동안 한 번 이상 연결되어야 합니다.
 - * **UTC** 가 아닌 로컬 장치 시간 사용: 정의된 시간을 UTC(협정 세계시) 가 아닌 로컬 장치 시간과 동기화합니다.

XenMobile 에서 장치 정책을 추가하여 iOS 연락처 (CardDAV) 계정을 사용자의 iOS 또는 macOS 장치에 추가하고 이러한 장치의 연락처 데이터를 CardDAV 를 지원하는 모든 서버와 동기화할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이것은 필수 필드입니다.
- **호스트 이름:** CardDAV 서버의 주소를 입력합니다. 이것은 필수 필드입니다.
- **포트:** CardDAV 서버를 연결할 포트를 입력합니다. 이것은 필수 필드입니다. 기본값은 **8443** 입니다.
- **보안 주체 URL:** 사용자의 일정에 대한 기본 URL 을 입력합니다.
- **사용자 이름:** 사용자의 로그인 이름을 입력합니다. 이것은 필수 필드입니다.
- **암호:** 선택적 사용자 암호를 입력합니다.
- **SSL 사용:** CardDAV 서버에 대한 Secure Socket Layer 연결을 사용할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **정책 설정**
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * **제거할 때까지의 기간 (시간):** 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이것은 필수 필드입니다.
- **호스트 이름:** CardDAV 서버의 주소를 입력합니다. 이것은 필수 필드입니다.
- **포트:** CardDAV 서버를 연결할 포트를 입력합니다. 이것은 필수 필드입니다. 기본값은 **8443** 입니다.
- **보안 주체 URL:** 사용자의 일정에 대한 기본 URL 을 입력합니다.
- **사용자 이름:** 사용자의 로그인 이름을 입력합니다. 이것은 필수 필드입니다.
- **암호:** 선택적 사용자 암호를 입력합니다.
- **SSL 사용:** CardDAV 서버에 대한 Secure Socket Layer 연결을 사용할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **정책 설정**

- 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.
- 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
- 프로필 범위: 이 정책을 사용자에 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

OS 업데이트 제어 장치 정책

March 15, 2024

OS 업데이트 제어 장치 정책을 사용하여 다음을 배포할 수 있습니다.

- 감독되는 iOS 장치에 최신 OS 업데이트를 배포할 수 있습니다.
- OS 업데이트 장치 정책은 Apple 배포 프로그램에 등록된 감독되는 장치에 대해서만 작동합니다.
- macOS 10.11.5 이상을 실행하는 DEP 등록 macOS 장치에 최신 OS 및 앱 업데이트를 배포할 수 있습니다.
- 감독되는 Samsung SAFE 장치에 최신 OS 업데이트를 배포할 수 있습니다.

Samsung SAFE 장치의 경우 XenMobile 이 OS 업데이트 제어 정책을 Secure Hub 로 전송하면 Secure Hub 가 장치에 정책을 적용합니다. XenMobile Server 가 정책을 전송하고 장치에 정책이 수신되면 관리 > 장치 페이지가 표시됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<div> <div> OS Update policy </div> <div> <div>1 Policy Info</div> <div>2 Platforms</div> <div> <input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android Enterprise </div> <div>3 Assignment</div> </div> </div>						
<div> <div> Control OS Updates <p>This policy lets you deploy OS updates. For devices running iOS 10.3 and later, this policy works on supervised devices. For devices running a version prior to iOS 10.3, this policy works on devices that are both supervised and Automatic Device Enrollment-enrolled.</p> </div> <div> <div> OS updates options * <input checked="" type="radio"/> Download only ⓘ <input type="radio"/> Download and/or install ⓘ </div> <div> OS updates frequency (1-365 days) * <input type="text" value="7"/> ⓘ </div> <div> OS updates version * <input checked="" type="radio"/> Latest version ⓘ <input type="radio"/> Specified version only ⓘ iOS 11.3+ <input type="text"/> </div> </div> </div>						
<div> <div>▶ Deployment Rules</div> </div>						

- **OS 업데이트 옵션:** 두 옵션 모두 **OS** 업데이트 빈도에 따라 최신 OS 업데이트를 감독되는 장치에 다운로드합니다. 장치에 업데이트를 설치하라는 메시지가 표시됩니다. 장치의 잠금을 해제하면 메시지를 확인할 수 있습니다.
- **OS 업데이트 빈도:** XenMobile 이 장치 OS 를 확인하고 업데이트할 빈도를 결정합니다. 기본값은 **7** 일입니다.
- **OS 업데이트 버전:** 감독되는 iOS 장치를 업데이트하는 데 사용할 OS 버전을 지정합니다. 기본값은 최신 버전입니다.
 - 최신 버전: 최신 OS 버전으로 업데이트하려면 선택합니다.
 - 특정 버전만 해당: 특정 OS 버전으로 업데이트하도록 선택한 다음 버전 번호를 입력합니다. 이 옵션은 iOS 11.3 이상에 적용됩니다.

macOS 설정

Control OS Update	Control OS Update
1 Policy Info	This policy lets you push the latest OS updates to supervised devices and force installation.
2 Platforms	<p>OS update options *</p> <p><input checked="" type="radio"/> Download and/or install ⓘ</p> <p><input type="radio"/> Download only and notify ⓘ</p> <p>OS update frequency (1-365 days) *</p> <p>7 ⓘ</p> <p>► Deployment Rules</p>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Samsung SAFE	
3 Assignment	

- **OS 업데이트 옵션:** 두 옵션 모두 **OS** 업데이트 빈도에 따라 최신 macOS 업데이트를 다운로드합니다. 선택에 따라, 업데이트를 설치하거나 App Store 를 통해 업데이트를 사용할 수 있음을 사용자에게 알릴 수 있습니다.
- **OS 업데이트 빈도:** XenMobile 이 장치 OS 를 확인하고 업데이트할 빈도를 결정합니다. 기본값은 **7** 일입니다.

iOS 및 macOS 업데이트 작업의 상태 확인

iOS 및 macOS 의 경우 XenMobile 이 OS 업데이트 제어 정책을 장치에 배포하지 않습니다. 대신 XenMobile 은 정책을 사용하여 다음과 같은 MDM 명령을 장치에 전송합니다.

- OS 업데이트 검사 예약: OS 업데이트에 대한 백그라운드 검사를 수행하도록 장치에 요청합니다 (iOS 의 경우 선택 사항).
- 사용 가능한 OS 업데이트: 장치를 쿼리하여 사용 가능한 OS 업데이트 목록을 확인합니다.
- OS 업데이트 예약: macOS 업데이트, 앱 업데이트 또는 둘 다를 수행하도록 장치에 요청합니다. OS 및 앱 업데이트를 다운로드하거나 설치하는 시기는 장치 OS 에 따라 결정됩니다.

관리 > 장치 > 장치 세부 정보 (일반) 페이지에 예약된 OS 업데이트 검사와 사용 가능한 OS 업데이트 검사, 예약된 macOS 및 앱 업데이트의 상태가 표시됩니다.

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 Certificates

10 Connections

General Identifiers

Serial Number

IMEI/MEID

ActiveSync ID

WIFI MAC Address

Bluetooth MAC Address

Device Ownership

Corporate

BYOD

Security

Strong ID

Full Wipe of Device

Selective Wipe of Device

Lock Device

Schedule OS Update Scan

Available OS Update

Schedule OS Update

No device wipe.

No device selective wipe.

No device lock.

Schedule OS update scan was done at 10/6/17 1:34:53 pm.

Available OS update was done at 10/6/17 1:35:10 pm.

Schedule OS update was done at 10/6/17 1:35:15 pm with the install action "Download and/or install".

Next >

업데이트 작업의 상태에 대한 자세한 내용을 보려면 관리 > 장치 > 장치 세부 정보 (배달 그룹) 페이지로 이동합니다.

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 Certificates

10 Connections

macos | MacBook

Delivery Groups

Success (1) Pending (0) Failed (0)

Delivery Groups

Time

MacOS DEP DG10/6/17 1:35:28 pm

Showing 1 - 1 of 1 items

-- Details

Status	Action	Channel/User	Date
Success	Get Available OS Update Sent	SYSTEM	10/6/17 1:34:53 pm
Success	Schedule OS Update Scan Acknowledged	SYSTEM	10/6/17 1:34:53 pm
Success	Schedule OS Update Scan Sent	SYSTEM	10/6/17 1:34:53 pm
Success	Software inventory response	macos	10/6/17 1:34:20 pm
Done	Software inventory requested	macos	10/6/17 1:34:20 pm
Success	Mobileconfig response : MacOS DEP Webclip OSX (Profile already installed)	macos	10/6/17 1:34:20 pm

사용 가능한 OS 업데이트 및 마지막 설치 시도 등의 세부 정보를 보려면 관리 > 장치 > 장치 세부 정보 (속성) 페이지로 이동합니다.

XenMobile Server 현재 릴리스

Device details	DEP account name	DEP Account FR
	DEP profile assigned	10/6/17 1:08:16 pm
	DEP profile pushed	10/6/17 1:08:16 pm
	DEP registration by	@outlook.com
	DEP registration date	1/20/17 4:42:06 pm
	Description	MB 12.0 SPACE GRAY/1.1GHZ/8GB/256GB-FRA
	Device model	MacBook
	Device name	FranckD MacBook
	Model ID	MacBook8,1
	OS Update Install Failure Message	
	OS Update Install Status	Success
	OS Update Is Critical	No

1 General	
2 Properties	
3 User Properties	
4 Assigned Policies	
5 Apps	
6 Media	
7 Actions	
8 Delivery Groups	
9 Certificates	
10 Connections	
	Operating system build

	1682657
--	---------

Device details	Properties	
	- Custom	
	Add	
	AutoCheckEnabled	true
	AutomaticAppInstallationEnabled	false
	AutomaticOSInstallationEnabled	false
	AutomaticSecurityUpdatesEnabled	true
	BackgroundDownloadEnabled	true
	CatalogURL	https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
	IsDefaultCatalog	true
	PerformPeriodicCheck	true
	PreviousScanDate	2017-10-06T11:28:41Z

1 General	
2 Properties	
3 User Properties	
4 Assigned Policies	
5 Apps	
6 Media	
7 Actions	
8 Delivery Groups	
9 Certificates	
10 Connections	

	0
--	---

Android Enterprise 설정

XenMobile

Analyze

Manage

Configure

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

OS Update policy

1 Policy Info

2 Platforms

☐ iOS

☐ macOS

☒ Android Enterprise

3 Assignment

Control OS Updates

This policy lets you control OS updates for work managed devices running Android 7.0 or higher.

System update policy

Automatic

Allow over-the-air upgrade

ON

Deployment Rules

- 시스템 업데이트 정책: 시스템 업데이트 시기를 결정합니다. 엔터프라이즈 **FOTA** 제어 설정을 사용하도록 설정하면 이 설정의 구성에 관계없이 업데이트가 자동으로 수행됩니다.

- 자동: 업데이트가 제공되면 설치합니다.
 - 기간 내: 시작 시간과 종료 시간에 지정된 일일 유지 관리 기간 내에 업데이트를 자동으로 설치합니다.
 - * 시작 시간: 유지 관리 기간의 시작 시간으로, 장치의 로컬 시간을 기준으로 자정 이후의 분 수 (**0~1440**) 로 측정됩니다. 기본값은 **0** 입니다.
 - * 종료 시간: 유지 관리 기간의 종료 시간으로, 장치의 로컬 시간을 기준으로 자정 이후의 분 수 (**0~1440**) 로 측정됩니다. 기본값은 **120** 입니다.
 - 연기: 사용자가 최대 30 일까지 업데이트를 연기할 수 있습니다.
 - 기본값: 업데이트 정책을 시스템 기본값으로 설정합니다.
- 무선 업그레이드 허용: 사용하지 않도록 설정하면 사용자 장치에서 소프트웨어 업데이트를 무선으로 수신할 수 없습니다. 기본값은 켜짐입니다.
 - 엔터프라이즈 **FOTA** 제어: 사용하도록 설정하면 Samsung 장치가 최신 업데이트를 확인하고 자동으로 설치합니다. 사용하지 않도록 설정하면 사용자가 직접 업데이트를 확인하고 수동으로 설치할 수 있습니다. Samsung Knox 3.0 이상을 실행하는 Android Enterprise 장치를 위한 설정입니다. 기본값은 꺼짐입니다.
 - 엔터프라이즈 **FOTA** 라이선스 키: 업데이트를 확인할 때 사용할 라이선스 키를 선택합니다. Samsung MDM 라이선스 키 정책에서 이 설정을 구성할 수 있습니다. Samsung Knox 3.0 이상을 실행하는 Android Enterprise 장치를 위한 설정입니다. 기본값은 없음입니다. **Samsung MDM** 라이선스 키 장치 정책을 사용하여 키를 설정할 수 있습니다. [Samsung MDM 라이선스 키 장치 정책](#)을 참조하십시오.

자격 증명 장치 정책

August 12, 2022

자격 증명 장치 정책은 XenMobile 에서 구성된 PKI 를 가리킵니다. 예를 들어, PKI 구성에는 PKI 엔터티, 키 저장소, 자격 증명 공급자 또는 서버 인증서가 포함될 수 있습니다. 자격 증명에 대한 자세한 내용은 [인증서 및 인증](#)을 참조하십시오.

지원되는 각 플랫폼마다 이 문서에서 설명되어 있는 서로 다른 값 집합이 필요합니다.

참고:

이 정책을 만들기 전에 각 플랫폼에 사용할 자격 증명 정보와 모든 인증서 및 암호가 필요합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<div>Credential type: Certificate (.cer, .crt, .der and .pem)</div> <div>Credential name *</div> <div>The credential file path: <input type="text"/> <input type="button" value="Browse"/></div>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Android for Work <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<div>Policy Settings</div> <div>Remove policy: <input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in hours)</div> <div><input type="text"/> <input type="button" value="🗑"/></div> <div>Allow user to remove policy: Always <input type="button" value="🔔"/></div>
3 Assignment	► Deployment Rules

다음 설정을 구성합니다.

- 자격 증명 유형: 목록에서 이 정책에 사용할 자격 증명 유형을 클릭하고 선택한 자격 증명에 대해 다음 정보를 입력합니다.
 - 인증서
 - * 자격 증명 이름: 자격 증명의 고유한 이름을 입력합니다.
 - * 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - 키 저장소
 - * 자격 증명 이름: 자격 증명의 고유한 이름을 입력합니다.
 - * 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - * 암호: 자격 증명에 대한 키 저장소 암호를 입력합니다.
 - 서버 인증서
 - * 서버 인증서: 목록에서 사용할 인증서를 클릭합니다.
 - 자격 증명 공급자
 - * 자격 증명 공급자: 목록에서 자격 증명 공급자의 이름을 클릭합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<div> <div>Credential type</div> <div>Certificate (.cer, .crt, .der and .pem)</div> </div> <div> <div>Credential name *</div> <div></div> </div> <div> <div>The credential file path</div> <div></div> <div>Browse</div> </div>
<input type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Android for Work <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<div>Policy Settings</div> <div> <div>Remove policy</div> <div> <input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in hours) </div> <div></div> </div> <div> <div>Allow user to remove policy</div> <div>Always</div> <div>?</div> </div> <div> <div>Profile scope</div> <div>User</div> <div>macOS 10.7+</div> </div>
3 Assignment	

다음 설정을 구성합니다.

- 자격 증명 유형: 목록에서 이 정책에 사용할 자격 증명 유형을 클릭하고 선택한 자격 증명에 대해 다음 정보를 입력합니다.
 - 인증서
 - 자격 증명 이름: 자격 증명의 고유한 이름을 입력합니다.
 - 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - 키 저장소
 - 자격 증명 이름: 자격 증명의 고유한 이름을 입력합니다.
 - 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - 암호: 자격 증명에 대한 키 저장소 암호를 입력합니다.
 - 서버 인증서
 - 서버 인증서: 목록에서 사용할 인증서를 클릭합니다.
 - 자격 증명 공급자
 - 자격 증명 공급자: 목록에서 자격 증명 공급자의 이름을 클릭합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.
 - 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
 - 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Android 설정

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<div> <div>Credential type</div> <div>Certificate (.cer, .crt, .der and .pem)</div> </div> <div> <div>The credential file path</div> <div><input type="text"/></div> <div>Browse</div> </div>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Android for Work <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<div>► Deployment Rules</div>
3 Assignment	

다음 설정을 구성합니다.

- 자격 증명 유형: 목록에서 이 정책에 사용할 자격 증명 유형을 클릭하고 선택한 자격 증명에 대해 다음 정보를 입력합니다.
 - 인증서
 - ★ 자격 증명 이름: 자격 증명의 고유한 이름을 입력합니다.
 - ★ 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - 키 저장소
 - ★ 자격 증명 이름: 자격 증명의 고유한 이름을 입력합니다.
 - ★ 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - ★ 암호: 자격 증명에 대한 키 저장소 암호를 입력합니다.
 - 서버 인증서
 - ★ 서버 인증서: 목록에서 사용할 인증서를 클릭합니다.
 - 자격 증명 공급자
 - ★ 자격 증명 공급자: 목록에서 자격 증명 공급자의 이름을 클릭합니다.

Android Enterprise 설정

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, certificates such as a certificate for wi-fi authentication can also be used as part of another policy. For Windows phones, only Windows 10 and later supervised devices support the policy.
2 Platforms	<div>Remove credentials <input type="checkbox"/></div> <div>Apply to fully managed devices with a work profile/Work profile on corporate-owned devices <input type="checkbox"/></div> <div>Credential type: Certificate (.cer, .crt, .der and .pem)</div> <div>The credential file path: <input type="text"/> <input type="button" value="Browse"/></div>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android (legacy DA) <input checked="" type="checkbox"/> Android Enterprise <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<div>► Deployment Rules</div>
3 Assignment	

XenMobile 이 자격 증명 설정을 적용하는 방식을 결정하려면 다음 설정을 구성합니다.

- **자격 증명 제거:** 켜짐으로 설정하면 다음 설정이 구성됩니다. 기본값은 꺼짐입니다.
 - 사용자 자격 증명 제거: 관리되는 키 저장소에서 인증서를 삭제합니다. 기본값은 꺼짐입니다.
 - 신뢰할 수 있는 루트 인증서 제거: 비시스템 CA 인증서를 모두 제거합니다. 기본값은 꺼짐입니다.
- **작업 프로필/회사 소유 장치의 작업 프로필을 사용하는 완전 관리형 장치에 적용:** 작업 프로필로 완전히 관리되는 장치에 대해 자격 증명 정책 설정을 구성할 수 있도록 허용합니다. 이 설정이 켜짐인 경우 구성한 자격 증명 설정이 작업 프로필에만 적용됩니다. 이 설정이 꺼짐인 경우 구성하는 자격 증명 설정이 장치에만 적용됩니다. 기본값은 꺼짐입니다.

자격 증명 설정을 구성합니다.

- **자격 증명 유형:** 목록에서 이 정책에 사용할 자격 증명 유형을 클릭하고 선택한 자격 증명에 대해 다음 정보를 입력합니다.
 - 인증서
 - * **자격 증명 파일 경로:** 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - 키 저장소
 - * **자격 증명 파일 경로:** 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - * **인증서 별칭:** 인증서 별칭으로 앱에서 인증서에 액세스하기가 더 간편해집니다. 관리되는 구성 장치 정책에서 인증서 별칭을 구성합니다. 그런 다음 자격 증명 장치 정책의 인증서 별칭 필드에 별칭을 입력합니다. 앱에서 사용자 작업 없이도 인증서를 검색하고 VPN 을 인증합니다.
 - * **암호:** 자격 증명에 대한 키 저장소 암호를 입력합니다.
 - 서버 인증서
 - * **서버 인증서:** 목록에서 사용할 인증서를 클릭합니다.
 - 자격 증명 공급자
 - * **인증서 별칭:** 인증서 별칭으로 앱에서 인증서에 액세스하기가 더 간편해집니다. 관리되는 구성 장치 정책에서 인증서 별칭을 구성합니다. 그런 다음 자격 증명 장치 정책의 인증서 별칭 필드에 별칭을 입력합니다. 앱에서 사용자 작업 없이도 인증서를 검색하고 VPN 을 인증합니다.

- ★ 자격 증명 공급자: 목록에서 자격 증명 공급자의 이름을 클릭합니다.
- ★ 인증서를 사용할 앱: 이 공급자의 자격 증명에 자동으로 액세스하는 앱을 지정하려면 추가를 클릭하고 앱을 선택한 다음 저장을 클릭합니다.

Windows 데스크톱/태블릿 설정

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<div> Certificate Type: <input type="text" value="ROOT"/> </div> <div> Store device: <input type="text" value="root"/> </div> <div> Location: <input type="text" value="System"/> </div> <div> Credential type: <input type="text" value="Certificate (.cer, .crt, .der and .pem)"/> </div> <div> Credential file path: <input type="text"/> <input type="button" value="Browse"/> </div>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Android for Work <input type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	Deployment Rules
3 Assignment	

- 인증서 유형: 목록에서 루트 또는 클라이언트를 클릭합니다.
- 루트를 클릭하는 경우 다음 설정을 구성합니다.
 - 스토어 장치: 목록에서 자격 증명의 인증서 저장소 위치로 루트, 내 또는 **CA**를 클릭합니다. 내의 경우 사용자의 인증서 저장소에 인증서가 저장됩니다.
 - 위치: Windows 10 또는 Windows 11 태블릿의 경우 시스템이 유일한 위치입니다.
 - 자격 증명 유형: Windows 10 및 Windows 11 태블릿의 경우 인증서가 유일한 자격 증명 유형입니다.
 - 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 인증서 파일을 선택합니다.
- 클라이언트를 클릭하는 경우 다음 설정을 구성합니다.
 - 위치: Windows 10 또는 Windows 11 태블릿의 경우 시스템이 유일한 위치입니다.
 - 자격 증명 유형: Windows 10 및 Windows 11 태블릿의 경우 키 저장소가 유일한 자격 증명 유형입니다.
 - 자격 증명 이름: 자격 증명의 이름을 입력합니다. 이것은 필수 필드입니다.
 - 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 인증서 파일을 선택합니다.
 - 암호: 자격 증명과 연관된 암호를 입력합니다. 이것은 필수 필드입니다.

사용자 지정 XML 장치 정책

November 1, 2022

XenMobile 에서 사용자 지정 XML 정책을 만들어 지원되는 Windows 장치에서 다음 기능을 사용자 지정할 수 있습니다.

- 장치 구성을 비롯한 프로비저닝, 기능을 사용하거나 사용하지 않도록 설정
- 사용자가 설정 및 장치 매개 변수를 변경하도록 허용하는 것을 비롯한 장치 구성
- 앱 및 시스템 소프트웨어를 비롯하여 장치에 로드할 새 소프트웨어 또는 버그 수정을 제공하는 것을 포함하는 소프트웨어 업그레이드
- 장치에서 오류 및 상태 보고서를 받는 것을 비롯한 오류 관리

참고:

XML 콘텐츠를 만들 때는 % 문자를 주의해서 사용하십시오. % 문자는 XML 예약 문자로, XML 특수 문자를 이스케이프하는 데만 사용됩니다. 이름에 % 를 사용하려면 %25 로 인코딩합니다.

Windows 장치의 경우: OMA DM(Open Mobile Alliance Device Management) API 를 사용하여 사용자 지정 XML 구성을 만듭니다. OMA DM API 로 사용자 지정 XML 을 만드는 것은 이 항목의 범위를 벗어납니다. OMA DM API 를 사용하는 방법에 대한 자세한 내용은 Microsoft Developer Network 사이트에 있는 [OMA Device Management\(OMA 장치 관리\)](#)를 참조하십시오.

참고:

Windows 10 RS2 휴대폰: Internet Explorer 를 사용하지 않는 사용자 지정 XML 정책 또는 제한 정책을 휴대폰에 배포한 후 브라우저가 사용되는 상태로 유지됩니다. 이 문제를 해결하려면 휴대폰을 다시 시작하십시오. 이것은 타사 문제입니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Windows 데스크톱/태블릿 설정

- **XML 콘텐츠:** 정책에 추가할 사용자 지정 XML 코드를 입력하거나 잘라내 붙여 넣습니다.

다음은 클릭하면 XenMobile 이 XML 콘텐츠 구문을 확인합니다. 모든 구문 오류가 콘텐츠 상자 아래에 나타납니다. 계속하려면 먼저 모든 오류를 해결합니다.

구문 오류가 없으면 사용자 지정 **XML** 정책 할당 페이지가 나타납니다.

Defender 장치 정책

January 5, 2022

Windows Defender 는 Windows 10 및 Windows 11 에 포함된 맬웨어 방지 프로그램입니다. XenMobile 장치 정책인 Defender 를 사용하여 Windows 10 및 Windows 11 데스크톱 및 태블릿에 대한 Microsoft Defender 정책을 구성할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Windows Desktop 및 태블릿 설정

- 보관 파일에 대한 검사 허용: Defender가 보관 파일을 검사하는 것을 허용하거나 허용하지 않습니다. 기본값은 꺼짐입니다.
- 클라우드 보호 허용: Defender가 Microsoft로 맬웨어 활동과 관련된 정보를 보내는 것을 허용하거나 허용하지 않습니다. 기본값은 켜짐입니다.
- 이동식 드라이브에 대한 전체 검사 허용: Defender가 USB 스틱 같은 이동식 드라이브를 검사하는 것을 허용하거나 허용하지 않습니다. 기본값은 켜짐입니다.
- **Windows Defender** 실시간 모니터링 기능 허용: 기본값은 켜짐입니다.
- 네트워크 파일에 대한 검사 허용: Defender가 네트워크 파일을 검사하는 것을 허용하거나 허용하지 않습니다. 기본값은 켜짐입니다.
- **Windows Defender UI**에 대한 사용자 액세스 허용: 사용자가 Windows Defender 사용자 인터페이스에 액세스할 수 있는지 여부를 지정합니다. 이 설정은 다음번에 사용자 장치가 시작될 때 적용됩니다. 이 설정이 꺼짐이면 사용자가 어떠한 Windows Defender 알림도 받지 않습니다. 기본값은 켜짐입니다.
- 제외된 확장명: 실시간 또는 예약 검사에서 제외할 확장명입니다. 확장명을 구분하려면 | 문자를 사용합니다. 예를 들어 “lib|obj”를 사용합니다.
- 제외된 경로: 실시간 또는 예약 검사에서 제외할 경로입니다. 경로를 구분하려면 | 문자를 사용합니다. 예를 들어 “C:\Example\C:\Example1”을 사용합니다.
- 제외된 프로세스: 실시간 또는 예약 검사에서 제외할 프로세스입니다. 프로세스를 구분하려면 | 문자를 사용합니다. 예를 들어 “C:\Example.exe\C:\Example1.exe”를 사용합니다.
- 샘플 동의 제출: 악성인지 확인하려면 추가적인 분석이 필요할 수 있는 파일을 Microsoft로 보낼지 여부를 제어합니다. 옵션: 항상 확인, 안전한 샘플 보내기, 보내지 않음, 모든 샘플 보내기. 기본값은 안전한 샘플 보내기입니다.

장치 상태 증명 장치 정책

January 5, 2022

XenMobile 에서 Windows 10 및 Windows 11 장치가 분석을 위해 특정 데이터 및 런타임 정보를 HAS(상태 증명 서비스)에 전송하여 해당 상태를 보고하도록 할 수 있습니다. HAS 에서 상태 증명 인증서를 생성하고 반환하면 장치가 이를 XenMobile에 보냅니다. XenMobile 은 상태 증명 인증서를 받은 후 상태 증명 인증서의 내용에 따라 이전에 설정된 자동 동작을 배포할 수 있습니다.

HAS 에 의해 확인되는 데이터는 다음과 같습니다.

- AIK 존재
- Bit Locker 상태
- 부팅 디버깅 사용
- 부팅 관리자 수정 목록 버전
- 코드 무결성 사용
- 코드 무결성 수정 목록 버전
- Apple 배포 프로그램 정책
- ELAM 드라이버 로드
- 실행 시간
- 커널 디버깅 사용
- PCR
- 재설정 횟수
- 다시 시작 횟수
- 안전 모드 사용
- SBCP 해시
- 보안 부팅 사용
- 테스트 서명 사용
- VSM 사용
- WinPE 사용

자세한 내용은 Microsoft [장치 HealthAttestation CSP](#) 페이지를 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Microsoft Cloud 를 사용하여 DHA 를 구성하려면

장치 상태 증명 정책을 추가하고 선택한 각 플랫폼에 대해 다음 설정을 구성합니다.

- **장치 상태 증명 사용:** 장치 상태 증명을 요구할 것인지를 선택합니다. 기본값은 꺼짐입니다.

온 프레미스 **Windows DHA** 서버를 사용하여 **DHA** 를 구성하려면

DHA 온-프레미스를 사용하려면 먼저 DHA 서버를 구성해야 합니다. 그런 다음 온-프레미스 DHA 서비스를 활성화하는 XenMobile Server 정책을 생성합니다.

1. DHA 를 구성하려면 Windows Server 2016 Technical Preview 5 이상을 실행하는 컴퓨터에 DHA 서버 역할을 설치해야 합니다. 자세한 내용은 [온 프레미스 장치 상태 증명 서버 구성](#)을 참조하십시오.
2. 장치 상태 증명 정책을 추가하고 다음 설정을 구성합니다.
 - 장치 상태 증명 사용: 켜짐으로 설정합니다.
 - 온 프레미스 **Health Attestation Service** 구성: 켜짐으로 설정합니다.
 - **On-prem DHA Service FQDN**(온-프레미스 **DHA** 서비스 **FQDN**): 설정하는 DHA 서버의 정규화된 도메인 이름을 입력합니다.
 - **On-prem DHA API version**(온-프레미스 **DHA API** 버전): DHA 서버에 설치된 DHA 서비스의 버전을 선택합니다.

장치 이름 장치 정책

January 5, 2022

감독되는 iOS 및 macOS 장치에 장치를 쉽게 식별할 수 있도록 하는 이름을 설정할 수 있습니다. 매크로, 텍스트 또는 둘 다를 사용하여 장치 이름을 정의할 수 있습니다. 예를 들어 장치 일련 번호로 장치 이름을 설정하려는 경우 `${device.serialnumber}` 를 사용할 수 있습니다. 사용자 이름과 도메인의 조합으로 장치 이름을 설정하려면 `${user.username}@example.com` 을 사용할 수 있습니다. 매크로에 대한 자세한 내용은 [XenMobile 의 매크로](#)를 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 및 macOS 설정

Device Name Policy	Device Name Policy
1 Policy Info	This policy lets you apply a name on a supervised device on iOS and macOS devices. Available in iOS 8 and later.
2 Platforms	Device name * <input type="text"/>
<input checked="" type="checkbox"/> iOS	▶ Deployment Rules
<input checked="" type="checkbox"/> macOS	
3 Assignment	

- **장치 이름:** 매크로, 매크로 조합 또는 매크로와 텍스트 조합을 입력하여 각 장치에 고유한 이름을 지정합니다. 예를 들어 `${device.serialnumber}` 를 사용하여 장치 이름을 각 장치의 일련 번호로 설정하거나 `${device.serialnumber}` `${ user.username}` 을 사용하여 장치 이름에 사용자 이름을 포함합니다.

교육 구성 장치 정책

January 5, 2022

교육 구성 장치 정책은 다음을 정의합니다.

- 강사 장치의 Apple Classroom 앱 설정
- 강사 장치와 학생 장치 간의 클라이언트 인증을 수행하는 데 사용되는 인증서

이 정책에서 클래스를 선택하면 XenMobile 콘솔에 Apple School Manager 구성의 강사 및 학생이 입력됩니다. 이 정책의 Apple Classroom 앱 설정이 모든 클래스에 대해 동일한 경우 하나의 정책을 생성합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- **클래스:** 클래스를 추가하려면 추가를 클릭합니다.

Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Display Name*	Description	Instructors*	Students*
			Add

Allow students to change screen observation permission: ☐ OFF ⓘ

iOS 10.3+

그런 다음 표시 이름 목록을 클릭합니다. 연결된 Apple School Manager 계정에서 가져온 클래스 목록이 나타납니다.

Education Configuration Policy

- 1 Policy Info
- 2 Platforms
- 3 Assignment**

Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*
SAMPLE-CLASS-1014 - HS			

Allow students to change screen observation permission ☐ OFF ⓘ

IOS 10.3+

Remove policy ☒ Select date

☐ Duration until removal (in hours)

Allow user to remove policy Always ⓘ

► Deployment Rules

표시 이름에서 클래스를 선택하면 XenMobile 이 강사와 학생을 입력합니다. 클래스 추가를 계속합니다.

Education Configuration Policy

- 1 Policy Info
- 2 Platforms
- 3 Assignment**

Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS		@appleid.citrix.com, @appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1010 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1011 - HS		@appleid.citrix.com	@appleid.citrix.com	
SAMPLE-CLASS-1012 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	

Allow students to change screen observation permission ☒ ON ⓘ

IOS 10.3+

Policy Settings

Remove policy ☒ Select date

☐ Duration until removal (in hours)

- 학생들이 화면 관찰 허가를 변경할 수 있도록 허용: 커짐인 경우 관리되는 클래스에 등록된 학생은 강사가 자신의 장치 화면을 볼 수 있도록 허용할지 여부를 선택할 수 있습니다. 기본값은 꺼짐입니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.

정책의 클래스 정보를 편집하려면

클래스에 설명을 추가할 수 있습니다 (Classroom 앱의 “표시 이름”). 또한 강사와 학생을 추가하거나 제거할 수 있습니다. XenMobile 은 이러한 변경 내용을 Apple School Manager 계정에 저장하지 않습니다. 자세한 내용은 [Apple 교육 기능과 통합](#)의 “강사, 학생 및 클래스 데이터 관리” 를 참조하십시오.

편집할 클래스의 추가 열 위로 마우스를 이동하고 연필 아이콘을 클릭합니다.

Education Configuration Policy		Education Configuration Policy			
1 Policy Info		This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.			
2 Platforms		Classes			
3 Assignment					
iOS		Display Name*	Description	Instructors*	Students*
		SAMPLE-CLASS-0001 - HS		@appleid.citrix.com, pleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, leid.citrix.com, ppleid.citrix.com, appleid.citrix.com, pleid.citrix.com, in@appleid.citrix.com

정책에서 클래스를 삭제하려면 삭제할 클래스의 추가 열 위로 마우스를 이동하고 휴지통 아이콘을 클릭합니다.

Exchange 장치 정책

March 15, 2024

Exchange ActiveSync 장치 정책을 사용하여 Exchange 에서 호스팅되는 회사 전자 메일에 액세스할 수 있도록 사용자 장치의 전자 메일 클라이언트를 구성할 수 있습니다. iOS, macOS, Android Enterprise, Samsung SAFE, Samsung KNOX 및 Windows 태블릿에 대한 정책을 만들 수 있습니다. 각 플랫폼마다 다른 값 집합이 필요합니다. 값 집합에 대해서는 이후 섹션에서 자세히 설명합니다.

이 정책을 만들려면 Exchange Server 의 호스트 이름 또는 IP 주소가 필요합니다. ActiveSync 설정에 대한 자세한 내용은 Microsoft 문서 [ActiveSync CSP](#)를 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

Exchange Policy
This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Exchange ActiveSync account name *

Exchange ActiveSync host name *

Use SSL ☒

Domain

User

Email address

Use OAuth ☐ iOS 12.0+

Password

Email sync interval 3 days

Identity credential (keystore or PKI credential) None

Authorize email move between accounts ☐

Send email only from email app ☐

Disable email recent syncing ☐

Allow Mail Drop ☐

- **Exchange ActiveSync** 계정 이름: 사용자 장치에 표시되는 전자 메일 계정에 대한 설명을 입력합니다.
- **Exchange ActiveSync** 호스트 이름: 전자 메일 서버의 주소를 입력합니다.
- **SSL** 사용: 사용자의 장치와 Exchange Server 간의 연결을 보호할지 여부를 선택합니다. 기본값은 켜짐입니다.
- 도메인: Exchange Server 가 상주하는 도메인을 입력합니다. 이 필드에서 \$user.domainname 시스템 매크로를 사용하여 사용자 도메인 이름을 자동으로 조회할 수 있습니다.
- 사용자: Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 \$user.username 시스템 매크로를 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- 전자 메일 주소: 전체 전자 메일 주소를 지정합니다. 이 필드에서 \$user.mail 시스템 매크로를 사용하여 사용자 전자 메일 계정을 자동으로 조회할 수 있습니다.
- **OAuth** 사용: 켜짐으로 설정된 경우 연결 인증에 OAuth 가 사용됩니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
 - **OAuth** 로그인 URL: 자동 검색 서비스가 사용되지 않을 때 OAuth 를 사용한 인증을 위해 웹뷰에 로드할 URL 을 지정합니다. 이 필드는 **OAuth** 사용이 켜짐으로 설정된 경우 나타납니다.
 - **OAuth** 토큰 요청 URL: 계정이 OAuth 토큰 요청에 사용할 수 있는 URL 을 지정합니다. 이 필드는 **OAuth** 사용이 켜짐으로 설정된 경우 나타납니다.
- 암호: Exchange 사용자 계정에 대한 선택적 암호를 입력합니다. **OAuth** 사용이 켜짐인 경우 이 설정이 나타나지 않습니다.
- 전자 메일 동기화 간격: 목록에서 전자 메일이 Exchange Server 와 동기화되는 빈도를 선택합니다. 기본값은 **3** 일입니다.
- ID 자격 증명 (키 저장소 또는 **PKI**): XenMobile 에 대한 ID 공급자를 구성한 경우 목록에서 선택적인 ID 자격 증명을 클릭합니다. 이 필드는 Exchange 가 클라이언트 인증서 인증을 요구하는 경우에만 필요합니다. 기본값은 없음입니다.
- 계정 간 전자 메일 이동 승인: 사용자가 이 계정에서 다른 계정으로 전자 메일을 이동하고 다른 계정에서 전자 메일을 전달하고 회신할 수 있도록 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.

- 전자 메일 앱에서만 전자 메일 보내기: 전자 메일을 보낼 사용자를 iOS 메일 앱으로 제한할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 최근 전자 메일 동기화 사용 안 함: 사용자가 최근 주소를 동기화하지 못하도록 할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 6.0 이상에만 적용됩니다.
- **Mail Drop** 허용: 계정에서 Mail Drop 을 사용하도록 허용할지 선택합니다. 기본값은 꺼짐입니다.
- **S/MIME** 서명 사용: 이 계정이 S/MIME 서명을 지원하는지 여부를 선택합니다. 기본값은 켜짐입니다. 켜짐으로 설정하면 다음 필드가 나타납니다.
 - 서명 **ID** 자격 증명: 사용할 서명 자격 증명을 선택합니다.
 - **S/MIME** 서명 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
 - **S/MIME** 서명 인증서 **UUID** 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
- **S/MIME** 암호화 사용: 이 계정이 S/MIME 암호화를 지원하는지 여부를 선택합니다. 기본값은 꺼짐입니다. 켜짐으로 설정하면 다음 필드가 나타납니다.
 - 암호화 **ID** 자격 증명: 사용할 암호화 자격 증명을 선택합니다.
 - 메시지별 **S/MIME** 전환 사용: 켜짐으로 설정하면 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션이 표시됩니다. 기본값은 꺼짐입니다.
 - 기본적으로 **S/MIME** 암호화 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 를 기본적으로 켜지 여부를 선택할 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
 - **S/MIME** 암호화 인증서 **UUID** 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

Synced Exchange 서비스

Exchange Policy	
1 Policy Info	
2 Platforms	
<input checked="" type="checkbox"/> iOS	<p>Synced Exchange Services calendars settings</p> <p>Enable calendars <input type="checkbox"/></p> <p>Enable user overridable calendars <input type="checkbox"/></p> <p>Synced Exchange Services contacts settings</p> <p>Enable contacts <input type="checkbox"/></p> <p>Enable user overridable contacts <input type="checkbox"/></p> <p>Synced Exchange Services mail settings</p> <p>Enable mail <input type="checkbox"/></p> <p>Enable user overridable mail <input type="checkbox"/></p> <p>Synced Exchange Services notes settings</p> <p>Enable notes <input type="checkbox"/></p> <p>Enable user overridable notes <input type="checkbox"/></p> <p>Synced Exchange Services reminders settings</p> <p>Enable reminders <input type="checkbox"/></p> <p>Enable user overridable reminders <input type="checkbox"/></p>
<input type="checkbox"/> macOS	
<input type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- 동기화된 **Exchange** 서비스 일정 설정

- 캘린더 활성화: 계정의 일정 서비스를 활성화 또는 비활성화할 수 있습니다. 기본값은 켜짐입니다. 꺼짐으로 설정된 경우 계정에 대한 일정 서비스가 비활성화됩니다. 사용자 재정의 가능한 일정 활성화 버튼이 켜짐으로 설정된 경우에만 설정에서 일정 서비스를 다시 활성화할 수 있습니다.
- 사용자 재정의 가능한 일정 활성화: 설정에서 계정의 일정 서비스 상태를 변경할 수 있습니다. 기본값은 켜짐입니다. 꺼짐으로 설정된 경우 일정 서비스의 상태를 변경할 수 없습니다.

- 동기화된 **Exchange** 서비스 연락처 설정

- 연락처 활성화: 계정의 연락처 서비스를 활성화 또는 비활성화할 수 있습니다. 기본값은 켜짐입니다. 꺼짐으로 설정된 경우 계정에 대한 연락처 서비스가 비활성화됩니다. 연락처 서비스는 사용자 재정의 가능한 연락처 활성화 버튼이 켜짐으로 설정된 경우에만 설정에서 다시 활성화할 수 있습니다.
- 사용자 재정의 가능한 연락처 활성화: 설정에서 계정의 연락처 서비스 상태를 변경할 수 있습니다. 기본값은 켜짐입니다. 꺼짐으로 설정된 경우 일정 서비스의 상태를 변경할 수 없습니다.

- 동기화된 **Exchange** 서비스 메일 설정

- 메일 활성화: 계정의 메일 서비스를 활성화하거나 비활성화할 수 있습니다. 기본값은 켜짐입니다.
꺼짐으로 설정된 경우 계정에 대한 메일 서비스가 비활성화됩니다. 사용자 재정의 가능한 메일 활성화 버튼이 켜짐으로 설정된 경우에만 설정에서 메일 서비스를 다시 활성화할 수 있습니다.
- 사용자 재정의 가능한 메일 활성화: 설정에서 계정의 메일 서비스 상태를 변경할 수 있습니다. 기본값은 켜짐입니다.
꺼짐으로 설정된 경우 메일 서비스의 상태를 변경할 수 없습니다.

• 동기화된 **Exchange** 서비스 메모 설정

- 메모 활성화: 계정에 대한 메모 서비스를 활성화하거나 비활성화할 수 있습니다. 기본값은 켜짐입니다.
꺼짐으로 설정된 경우 계정에 대한 메모 서비스가 비활성화됩니다. 사용자 재정의 가능한 메모 활성화 버튼이 켜짐으로 설정된 경우에만 설정에서 메모 서비스를 다시 활성화할 수 있습니다.
- 사용자 재정의 가능한 메모 활성화: 설정에서 계정의 메모 서비스 상태를 변경할 수 있습니다. 기본값은 켜짐입니다.
꺼짐으로 설정된 경우 메모 서비스의 상태를 변경할 수 없습니다.

• 동기화된 **Exchange** 서비스 미리 알림 설정

- 미리 알림 활성화: 계정에 대한 미리 알림 서비스를 활성화 또는 비활성화할 수 있습니다. 기본값은 켜짐입니다.
꺼짐으로 설정된 경우 계정에 대한 미리 알림 서비스가 비활성화됩니다. 사용자 재정의 가능한 미리 알림 활성화 버튼이 켜짐으로 설정된 경우에만 설정에서 미리 알림 서비스를 다시 활성화할 수 있습니다.
- 사용자 재정의 가능한 미리 알림 활성화: 설정에서 계정의 미리 알림 서비스 상태를 변경할 수 있습니다. 기본값은 켜짐입니다.
꺼짐으로 설정된 경우 미리 알림 서비스의 상태를 변경할 수 없습니다.

macOS 설정

Exchange Policy	Exchange Policy
<p>1 Policy Info</p> <p>2 Platforms</p> <p><input type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> macOS</p> <p><input checked="" type="checkbox"/> Android HTC</p> <p><input checked="" type="checkbox"/> Android TouchDown</p> <p><input checked="" type="checkbox"/> Android for Work</p> <p><input checked="" type="checkbox"/> Samsung SAFE</p> <p><input checked="" type="checkbox"/> Samsung KNOX</p> <p><input checked="" type="checkbox"/> Windows Phone</p> <p><input checked="" type="checkbox"/> Windows Desktop/Tablet</p> <p>3 Assignment</p>	<p>This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.</p> <p>Exchange ActiveSync account name *</p> <p>User *</p> <p>Email address *</p> <p>Password</p> <p>Internal Exchange host</p> <p>Internal server port</p> <p>Internal server path</p> <p>Use SSL for internal Exchange host <input checked="" type="checkbox"/> ON</p> <p>External Exchange host</p> <p>External server port</p> <p>External server path</p>

- **Exchange ActiveSync** 계정 이름: 사용자 장치에 표시되는 전자 메일 계정에 대한 설명을 입력합니다.

- **사용자:** Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 \$user.username 시스템 매크로를 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- **전자 메일 주소:** 전체 전자 메일 주소를 지정합니다. 이 필드에서 \$user.mail 시스템 매크로를 사용하여 사용자 전자 메일 계정을 자동으로 조회할 수 있습니다.
- **OAuth 사용:** 커짐으로 설정된 경우 연결 인증에 OAuth가 사용됩니다. 기본값은 꺼짐입니다. 이 옵션은 macOS 10.14 이상에 적용됩니다.
- **OAuth 로그인 URL:** 자동 검색 서비스가 사용되지 않을 때 OAuth를 사용한 인증을 위해 웹뷰에 로드할 URL을 지정합니다. 이 필드는 OAuth 사용이 커짐으로 설정된 경우 나타납니다.
- **암호:** Exchange 사용자 계정에 대한 선택적 암호를 입력합니다. OAuth 사용이 커짐인 경우 이 설정이 나타나지 않습니다.
- **내부 Exchange 호스트:** 내부 및 외부 Exchange 호스트 이름을 서로 다르게 만들려면 선택적인 내부 Exchange 호스트 이름을 입력합니다.
- **내부 서버 포트:** 내부 및 외부 Exchange Server 포트를 서로 다르게 만들려면 선택적인 내부 Exchange Server 포트 번호를 입력합니다.
- **내부 서버 경로:** 내부 및 외부 Exchange Server 경로를 서로 다르게 만들려면 선택적인 내부 Exchange Server 경로를 입력합니다.
- **내부 Exchange 호스트에 SSL 사용:** 사용자 장치와 내부 Exchange 호스트 간의 연결을 보호할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **외부 Exchange 호스트:** 내부 및 외부 Exchange 호스트 이름을 서로 다르게 만들려면 선택적인 외부 Exchange 호스트 이름을 입력합니다.
- **외부 서버 포트:** 내부 및 외부 Exchange Server 포트를 서로 다르게 만들려면 선택적인 외부 Exchange Server 포트 번호를 입력합니다.
- **외부 서버 경로:** 내부 및 외부 Exchange Server 경로를 서로 다르게 만들려면 선택적인 외부 Exchange Server 경로를 입력합니다.
- **외부 Exchange 호스트에 SSL 사용:** 사용자 장치와 내부 Exchange 호스트 간의 연결을 보호할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **메일 삭제 허용:** 사용자가 기존 네트워크에 연결할 필요 없이 두 대의 Mac 간에 무선으로 파일을 공유하도록 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **정책 설정**
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간)입니다.
 - * **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * **제거할 때까지의 기간 (시간):** 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.

- 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
- 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Windows 데스크톱/태블릿 설정

Exchange Policy	
1 Policy Info	Exchange Policy This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.
2 Platforms	<div> <div>Account name or display name *</div> <input type="text"/> </div> <div> <div>Server name or IP address *</div> <input type="text"/> </div> <div> <div>Domain</div> <input type="text"/> </div> <div> <div>User ID or user name *</div> <input type="text"/> </div> <div> <div>Email address *</div> <input type="text"/> </div> <div> <div>Use SSL connection</div> <input type="checkbox"/> OFF </div> <div> <div>Sync items</div> <div> <div>Past days to sync</div> <input type="text" value="All content"/> </div> </div> <div> <div>Sync scheduling</div> <div> <div>Frequency</div> <input type="text" value="When item arrives"/> </div> <div> <div>Logging level</div> <input type="text" value="Disabled"/> </div> </div>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android HTC <input type="checkbox"/> Android TouchDown <input type="checkbox"/> Android for Work <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung KNOX <input type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet	

참고:

이 정책에서는 사용자 암호를 설정하도록 허용하지 않습니다. 사용자는 정책이 푸시된 후 장치에서 해당 매개 변수를 설정해야 합니다.

- 계정 이름 또는 표시 이름: Exchange ActiveSync 계정 이름을 입력합니다.
- 서버 이름 또는 IP 주소: Exchange Server의 호스트 이름 또는 IP 주소를 입력합니다.
- 도메인: Exchange Server가 상주하는 도메인을 입력합니다. 이 필드에서 \$user.domainname 시스템 매크로를 사용하여 사용자 도메인 이름을 자동으로 조회할 수 있습니다.
- 사용자 ID 또는 사용자 이름: Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 \$user.username 시스템 매크로를 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- 전자 메일 주소: 전체 전자 메일 주소를 지정합니다. 이 필드에서 \$user.mail 시스템 매크로를 사용하여 사용자 전자 메일 계정을 자동으로 조회할 수 있습니다.
- SSL 연결 사용: 사용자 장치와 Exchange Server 간의 연결을 보호할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 동기화할 과거 일 수: 목록에서 장치의 모든 콘텐츠를 Exchange Server와 동기화할 과거 일 수를 클릭합니다. 기본값은 모든 콘텐츠입니다.
- 빈도: 목록에서 Exchange Server에서 장치로 보낸 데이터를 동기화할 때 사용할 일정을 클릭합니다. 기본값은 항목이 도착할 때입니다.
- 로깅 수준: 목록에서 사용 안 함, 기본 또는 고급을 클릭하여 Exchange 활동을 로깅할 때 사용할 세부 정보 수준을 지정합니다. 기본값은 사용 안 함입니다.

파일 장치 정책

November 1, 2022

사용자가 Android 및 Android Enterprise 장치에서 액세스할 수 있도록 파일을 추가하고 배포할 수 있습니다. 장치에 파일을 저장할 디렉토리를 지정합니다. 예를 들어 사용자가 회사 문서 또는 .pdf 파일을 받게 하려고 합니다. 장치에 파일을 배포하고 파일의 위치를 사용자에게 알립니다.

Android 장치는 기본적으로 스크립트 실행을 지원하지 않습니다. 스크립트를 실행하려면 타사 소프트웨어가 필요합니다.

이 정책에는 다음과 같은 파일 형식을 추가할 수 있습니다.

- 텍스트 기반 파일 (.xml, .html, .py 등)
- 문서, 그림, 스프레드시트 또는 프레젠테이션 등의 기타 파일

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Android Enterprise 설정

Files Policy

This policy lets you upload files and executable scripts to devices.

File to be imported *

ChatLog 2016_10_27 21_58.rtf

Browse

File type

☒ File
 ☐ Script

Replace macro expressions

☐ OFF

?

Destination folder

%Flash Storage%\

?

Destination file name

?

If file exists

Copy file only if different

Copy file only if different
Do not copy

► Deployment Rules

- **가져올 파일:** 가져올 파일을 선택하려면 찾아보기를 클릭하고 파일의 위치로 이동합니다.
- **파일 유형:** 파일을 선택합니다.
- **대상 폴더:** 목록에서 업로드된 파일을 저장할 위치를 선택하거나 새로 추가를 클릭하여 나열되지 않은 파일 위치를 선택합니다. %XenMobile Folder%\ 또는 %Flash Storage%\ 매크로를 경로 식별자의 시작 부분으로 사용할 수 있습니다.
- **대상 파일 이름:** 선택 사항입니다. 장치에 배포하기 전에 파일 이름을 변경해야 하는 경우 파일 이름을 입력합니다.
- **파일이 있는 경우:** 목록에서 기존 파일을 복사할지 여부를 선택합니다. 기본값은 파일이 다른 경우에만 복사입니다.

Android 설정

- **가져올 파일:** 찾아보기를 클릭하고 파일의 위치로 이동하여 가져올 파일을 선택합니다.
- **파일 유형:** 파일을 선택합니다.
- **대상 폴더:** 목록에서 업로드된 파일을 저장할 위치를 선택하거나 새로 추가를 클릭하여 나열되지 않은 파일 위치를 선택합니다. 또는 %XenMobile Folder%\ 또는 %Flash Storage%\ 매크로를 경로 식별자의 시작 부분으로 사용할 수 있습니다.
- **대상 파일 이름:** 필요에 따라 장치에 배포하기 전에 이름을 변경해야 할 경우 파일에 다른 이름을 입력합니다.
- **파일이 다른 경우에만 복사:** 목록에서 기존 파일과 다른 경우 파일을 복사할 것인지 여부를 선택합니다. 기본값은 다른 경우에 파일을 복사하는 것입니다.

FileVault 장치 정책

August 24, 2018

macOS FileVault 디스크 암호화 기능은 시스템 볼륨 콘텐츠를 암호화하여 시스템 볼륨을 보호합니다. macOS 장치에서 FileVault 를 사용하도록 설정하면 장치를 시작할 때마다 사용자가 계정 암호를 사용하여 로그인해야 합니다. 사용자가 암호를 잊은 경우 복구 키를 사용하여 디스크 잠금을 해제하고 암호를 재설정할 수 있습니다.

XenMobile 장치 정책인 FileVault 는 FileVault 사용자 설치 화면을 사용하도록 설정하고 복구 키 같은 설정을 구성합니다. FileVault 에 대한 자세한 내용은 Apple 지원 사이트 (<https://support.apple.com>) 를 참조하십시오.

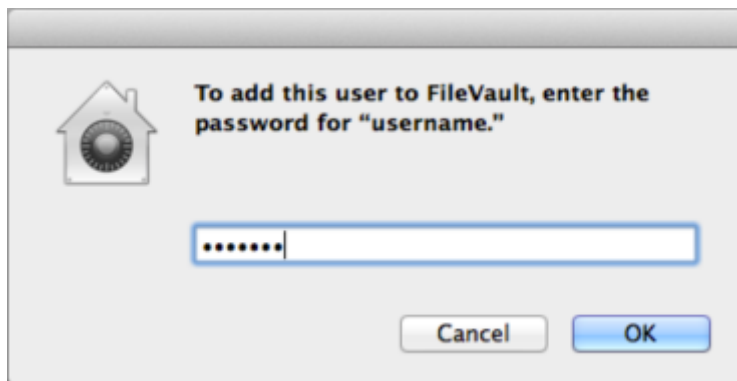
FileVault 정책을 추가하려면 구성 > 장치 정책으로 이동합니다.

macOS 설정

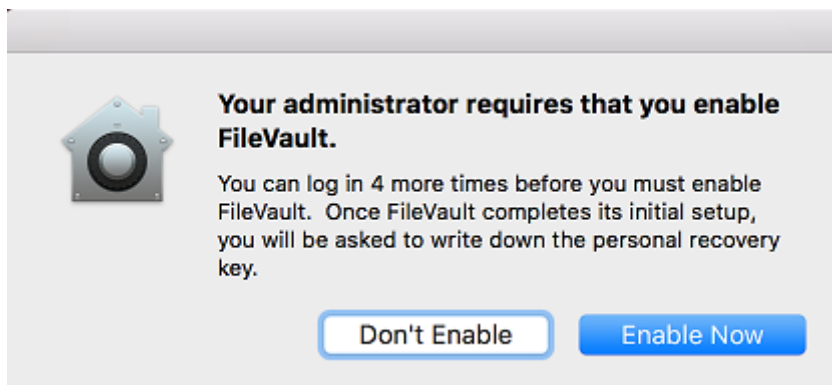
FileVault Policy	FileVault Policy
1 Policy Info	This policy lets you enable FileVault device encryption on enrolled macOS devices.
2 Platforms	<p>Prompt for FileVault setup during logout <input type="checkbox"/> OFF ⓘ</p> <p>Maximum times to skip FileVault setup <input type="text" value="0"/> ⓘ</p> <p>Recovery key type <input type="text" value="Personal recovery key"/> ⓘ</p> <p>Show personal recovery key <input checked="" type="checkbox"/> ON ⓘ</p> <p>► Deployment Rules</p>
<input checked="" type="checkbox"/> macOS	
3 Assignment	

- 로그아웃 도중 **FileVault** 설정에 대해 묻기: 꺼짐인 경우 **FileVault** 설정을 건너뛸 최대 횟수 옵션에 지정된 대로 다음 N 번째 로그아웃 시 FileVault 를 사용할지 여부를 묻는 메시지를 표시합니다. 꺼짐인 경우 FileVault 암호 확인 메시지가 표시되지 않습니다.

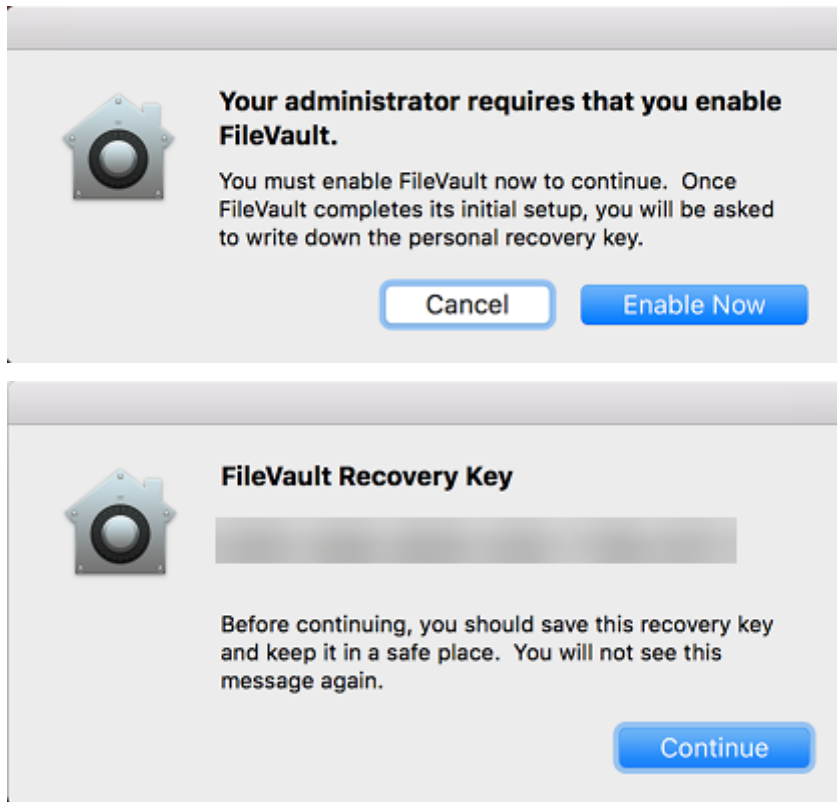
이 설정을 켜고 FileVault 정책을 배포하면 사용자가 장치에서 로그아웃할 때 다음 화면이 나타납니다. 이 화면에는 사용자가 로그오프 전에 FileVault 를 사용하도록 설정할 수 있는 옵션이 표시됩니다.



FileVault 설정을 건너뛸 최대 횟수 값이 0 이 아닌 경우: 이 설정을 끄고 FileVault 정책을 배포하면 사용자가 로그인할 때 다음 화면이 나타납니다.



FileVault 설정을 건너뛸 최대 횟수 값이 0 이거나 사용자가 최대 횟수로 설정을 건너뛴 경우 다음 화면이 나타납니다.



글꼴 장치 정책

January 5, 2022

iOS 및 macOS 장치에 글꼴을 더 추가하는 장치 정책을 XenMobile 에서 추가할 수 있습니다. 글꼴은 트루타입 (.ttf) 또는 오픈타입 (.oft) 형식이어야 합니다. 글꼴 모음 (.ttc 또는.otc) 은 지원되지 않습니다.

iOS 의 경우, 이 정책은 iOS 7.0 이상의 버전에만 적용됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- 사용자에게 표시되는 이름: 글꼴 목록에서 사용자에게 표시되는 이름을 입력합니다.
- 글꼴 파일: 찾아보기를 클릭하고 파일의 위치로 이동하여 사용자 장치에 추가할 글꼴 파일을 선택합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.

- ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
- ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- 사용자에게 표시되는 이름: 글꼴 목록에서 사용자에게 표시되는 이름을 입력합니다.
- 글꼴 파일: 찾아보기를 클릭하고 파일의 위치로 이동하여 사용자 장치에 추가할 글꼴 파일을 선택합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.
 - 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
 - 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

홈 화면 레이아웃 장치 정책

January 5, 2022

iOS 홈 화면의 앱 및 폴더 레이아웃을 지정할 수 있습니다. 홈 화면 레이아웃 장치 정책은 iOS 9.3 이상의 감독되는 장치에 적용됩니다.

중요:

한 장치에 여러 개의 홈 화면 레이아웃 정책을 배포하면 장치에서 iOS 오류가 발생합니다. 이 제한은 이 XenMobile 정책 또는 Apple Configurator 를 통해 홈 화면을 정의할 때 적용됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

Home Screen Layout Policy

This policy defines a layout of apps, folders and web clips for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application, you should enter its bundle identifier. For a folder, you should enter a list of bundle identifiers separated with commas. For a web clip, you should enter its URL.

Dock

Type	Display Name *	Value *	Add
			+

Page 1

Type	Display Name *	Value *	Add
			+

Page 2

Type	Display Name *	Value *	Add
			+

Page 3

Type	Display Name *	Value *	Add
			+

Page 4

Type	Display Name *	Value *	Add
			+

Page 5

Type	Display Name *	Value *	Add
			+

Policy Settings

Back Next > Refresh

- 구성할 각 화면 영역 (예: **Dock** 또는 **1** 페이지)에 대해 추가를 클릭합니다.
- 유형: 응용 프로그램, 폴더 또는 웹 클립을 선택합니다.

제한 장치 정책의 제한된 앱 사용 > 일부 앱만 허용 설정을 사용하면 웹 클립이 홈 화면에 올바르게 표시되지 않을 수 있습니다. 웹 클립이 올바르게 표시되지 않을 경우 다음 중 하나를 수행합니다.

- 제한된 앱 사용을 모든 앱 허용 또는 일부 앱 허용 안 함으로 설정합니다.
- 제한된 앱 사용을 일부 앱만 허용으로 설정한 상태에서 번들 ID `com.apple.webapp`로 앱을 추가하여 웹 클립을 허용합니다.

Home Screen Layout Policy

This policy defines a layout of apps, folders and web clips for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application, you should enter its bundle identifier. For a folder, you should enter a list of bundle identifiers separated with commas. For a web clip, you should enter its URL.

Dock

Type	Display Name *	Value *	
Application			Save Cancel

Page 1

Type	Display Name *	Value *	Add
			+

- 표시 이름: 홈 화면에 표시되는 앱 또는 폴더의 이름입니다.
- 값: 앱의 경우 번들 식별자입니다. 폴더의 경우 쉼표로 구분된 번들 식별자 목록을 입력합니다. 웹 클립의 경우 번들 ID(`com.apple.webClip.managed`)를 입력하고 웹 클립 정책에서 웹 클립 URL을 구성합니다. URL이

동일한 웹 클립 값이 둘 이상인 경우 iOS 11.3 이상인 장치에서 동작이 정의되지 않습니다.

- 정책 설정

- 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간)입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.
- 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 iOS 9.3 이상에서만 사용할 수 있습니다.

iOS 및 macOS 프로필 장치 정책 가져오기

January 5, 2022

XenMobile 로 iOS 와 macOS 장치를 위한 장치 구성 XML 파일을 가져올 수 있습니다. 이 파일에는 Apple Configurator 로 작성한 장치 보안 정책 및 제한 사항이 포함되어 있습니다.

이 문서의 뒷부분에 설명된 대로 Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 설정할 수 있습니다. Apple Configurator 를 사용하여 구성 파일을 만드는 방법에 대한 자세한 내용은 Apple [Configurator 지원](#)을 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 및 macOS 설정

Import iOS & macOS Profile Policy

1 Policy Info

2 Platforms

☒ iOS

☒ macOS

3 Assignment

Import iOS & macOS Profile Policy

This policy lets you import a device configuration XML file for either iOS or macOS. The file contains device security policies and restrictions that you prepare with the Apple Configurator.

iOS configuration profile

Browse

► Deployment Rules

- **iOS** 구성 프로파일 또는 **macOS** 구성 프로파일: 가져올 구성 파일을 선택하려면 찾아보기를 클릭하고 해당 파일 위치로 이동합니다.

Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 설정

Apple Configurator 를 사용하려면 macOS 10.7.2 이상을 실행하는 Apple 컴퓨터가 필요합니다.

중요:

감독 모드로 장치를 설정하면 선택한 버전의 iOS 가 장치에 설치되어 이전에 저장된 사용자 데이터 또는 앱이 장치에서 완전히 초기화됩니다.

1. iTunes 에서 Apple Configurator 를 설치합니다.
2. Apple 컴퓨터에 iOS 장치를 연결합니다.
3. Apple Configurator 를 시작합니다. 감독을 위해 준비할 장치가 있다고 표시됩니다.
4. 감독할 장치를 준비하려면:
 - a) 감독 컨트롤을 켜짐으로 전환합니다. 정기적으로 구성을 다시 적용하여 장치에 대한 제어를 지속적으로 유지하려는 경우 이 설정을 선택하는 것이 좋습니다.
 - b) 필요에 따라 장치에 이름을 지정합니다.
 - c) iOS 에서 최신을 클릭하여 설치할 최신 버전의 iOS 를 검색합니다.
5. 장치를 감독하도록 준비할 수 있는 상태가 되면 **Prepare(준비)** 를 클릭합니다.

Keyguard 관리 장치 정책

January 5, 2022

Android Keyguard 는 장치 및 Work Challenge 잠금 화면을 관리합니다. 이 정책을 통해 Android Enterprise 작업 프로파일 Keyguard 및 고급 장치 Keyguard 기능을 관리할 수 있습니다. 다음을 제어할 수 있습니다.

- 작업 프로파일 장치의 Keyguard 관리. 사용자가 장치 Keyguard 와 Work Challenge Keyguard 의 잠금을 해제하기 전에 사용할 수 있는 기능을 지정할 수 있습니다. 예를 들어, 기본적으로 사용자는 지문 잠금 해제를 사용하고 잠금 화면에서 수정되지 않은 알림을 확인할 수 있습니다.
- 완전 관리형 전용 장치의 Keyguard 관리. Keyguard 화면의 잠금을 해제하기 전에 신뢰할 수 있는 에이전트, 보안 카메라와 같이 사용할 수 있는 기능을 지정할 수 있습니다. 또는 모든 Keyguard 기능을 사용하지 않도록 선택할 수 있습니다.
- 작업 프로파일로 완전히 관리되는 장치의 Keyguard 관리. 하나의 Keyguard Management 정책을 사용하여 장치와 작업 프로파일에 개별 설정을 적용할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Android Enterprise 설정

Keyguard Management Policy	Keyguard Management Policy
1 Policy Info	Android keyguard manages the device and work challenge lock screens. This policy lets you control the features available to users before they unlock the device keyguard and the work challenge keyguard.
2 Platforms	
<input checked="" type="checkbox"/> Android Enterprise	<p>Apply to fully managed devices with a work profile <input type="checkbox"/> OFF</p> <p>Work profile keyguard features</p> <p>Disable trust agents <input type="checkbox"/> OFF ?</p> <p>Disable biometric authentication <input type="checkbox"/> OFF ?</p> <p>Disable fingerprint unlock <input type="checkbox"/> OFF ?</p> <p>Disable face authentication <input type="checkbox"/> OFF ?</p> <p>Disable iris authentication <input type="checkbox"/> OFF ?</p> <p>Disable unredacted notifications <input type="checkbox"/> OFF ?</p> <p>Fully managed device keyguard features</p> <p>Disable all keyguard features <input type="checkbox"/> OFF ?</p> <p>Disable trust agents <input type="checkbox"/> OFF ?</p> <p>Disable biometric authentication <input type="checkbox"/> OFF ?</p> <p>Disable fingerprint unlock <input type="checkbox"/> OFF ?</p> <p>Disable face authentication <input type="checkbox"/> OFF ?</p> <p>Disable iris authentication <input type="checkbox"/> OFF ?</p> <p>Disable all notifications <input type="checkbox"/> OFF ?</p> <p>Disable unredacted notifications <input type="checkbox"/> OFF ?</p> <p>Disable secure camera <input type="checkbox"/> OFF ?</p>
3 Assignment	

- 작업 프로필로 완전히 관리되는 장치에 적용: 작업 프로필로 완전히 관리되는 장치에 대해 Keyguard Management 장치 정책 설정을 구성할 수 있도록 허용합니다.
- 이 설정이 켜짐인 경우 별도의 설정을 장치와 작업 프로필로 완전히 관리되는 장치의 작업 프로필에 적용할 수 있습니다.
- 이 설정이 꺼짐인 경우 작업 프로필 장치와 완전 관리형 장치에 설정을 적용할 수 있습니다. 작업 프로필에 구성된 설정은 작업 프로필 장치에만 적용됩니다. 완전 관리형 장치에 구성된 설정은 완전 관리형 장치에만 적용됩니다.
- 기본값은 꺼짐입니다.
- 작업 프로필 **Keyguard** 기능: 사용자가 작업 프로필 Keyguard(잠금 화면)의 잠금을 해제하기 전에 다음 기능을 사용

할 수 있는지를 제어합니다.

- 신뢰할 수 있는 에이전트 비활성화: 꺼짐인 경우 작업 프로필에 Challenge 가 설정되어 있으면 신뢰할 수 있는 에이전트는 보안 Keyguard 화면에서 작동할 수 있습니다. 켜짐으로 설정하면 작업 프로필의 신뢰할 수 있는 에이전트가 모두 비활성화됩니다. 기본값은 꺼짐입니다.
 - 생체 인증 비활성화: 꺼짐인 경우 작업 프로필에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 생체 인증을 사용할 수 있습니다. 켜짐으로 설정하면 작업 프로필의 생체 인증이 비활성화됩니다. 이 설정은 지문 잠금 해제, 안면 인증, 홍채 인증을 비활성화합니다. 기본값은 꺼짐입니다. Android 9.0 이상에 적용됩니다.
 - 지문 잠금 해제 비활성화: 켜짐인 경우 작업 프로필에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 지문 잠금 해제를 사용할 수 없습니다. 작업 프로필에서 지문 잠금 해제를 사용하려면 꺼짐으로 설정합니다. 기본값은 꺼짐입니다.
 - 안면 인증 비활성화: 꺼짐인 경우 작업 프로필에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 안면 인증을 사용할 수 있습니다. 켜짐으로 설정하면 작업 프로필의 안면 인증이 비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에 적용됩니다.
 - 홍채 인증 비활성화: 꺼짐인 경우 작업 프로필에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 홍채 인증을 사용할 수 있습니다. 켜짐으로 설정하면 작업 프로필의 홍채 인증이 비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에 적용됩니다.
 - 수정되지 않은 알림 비활성화: 꺼짐인 경우 수정된 알림과 수정되지 않은 알림이 모두 보안 Keyguard 화면에 표시됩니다. 켜짐으로 설정하면 수정되지 않은 알림이 비활성화되고 수정된 알림만 표시됩니다. 기본값은 꺼짐입니다.
- 완전 관리형 장치 **Keyguard** 기능: 사용자가 장치 Keyguard(잠금 화면)의 잠금을 해제하기 전에 다음 기능을 사용할 수 있는지를 제어합니다. 이러한 기능은 완전 관리형 장치나 전용 장치에 적용됩니다.
 - 모든 **Keyguard** 기능 비활성화: 꺼짐인 경우 현재 및 향후의 모든 Keyguard 맞춤화를 보안 Keyguard 화면에서 사용할 수 있습니다. 켜짐으로 설정하면 모든 Keyguard 맞춤화가 비활성화됩니다. 기본값은 꺼짐입니다.
 - 신뢰할 수 있는 에이전트 비활성화: 꺼짐인 경우 신뢰할 수 있는 에이전트는 보안 Keyguard 화면에서 작동할 수 있습니다. 켜짐으로 설정하면 신뢰할 수 있는 에이전트가 비활성화됩니다. 기본값은 꺼짐입니다.
 - 생체 인증 비활성화: 꺼짐인 경우 장치에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 생체 인증을 사용할 수 있습니다. 켜짐으로 설정하면 장치에서 생체 인증이 비활성화됩니다. 이 설정은 지문 잠금 해제, 안면 인증, 홍채 인증을 비활성화합니다. 기본값은 꺼짐입니다. Android 9.0 이상에 적용됩니다.
 - 지문 잠금 해제 비활성화: 꺼짐인 경우 장치에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 지문 잠금 해제를 사용할 수 있습니다. 켜짐으로 설정하면 장치에서 지문 잠금 해제가 비활성화됩니다. 기본값은 꺼짐입니다.
 - 안면 인증 비활성화: 꺼짐인 경우 장치에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 안면 인증을 사용할 수 있습니다. 켜짐으로 설정하면 장치에서 안면 인증이 비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에 적용됩니다.
 - 홍채 인증 비활성화: 꺼짐인 경우 장치에 Challenge 가 설정되어 있으면 보안 Keyguard 화면에서 홍채 인증을 사용할 수 있습니다. 켜짐으로 설정하면 장치에서 홍채 인증이 비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에 적용됩니다.
 - 모든 알림 비활성화: 꺼짐인 경우 모든 알림이 보안 Keyguard 화면에 표시됩니다. 켜짐으로 설정하면 모든 알림

이 표시됩니다. 기본값은 꺼짐입니다.

- 수정되지 않은 알림 비활성화: 꺼짐인 경우 수정된 알림과 수정되지 않은 알림이 모두 보안 Keyguard 화면에 표시됩니다. 켜짐으로 설정하면 수정되지 않은 알림이 비활성화되고 수정된 알림만 표시됩니다. 기본값은 꺼짐입니다.
- 보안 카메라 비활성화: 꺼짐인 경우 보안 Keyguard 화면에서 보안 카메라를 사용할 수 있습니다. 켜짐으로 설정하면 보안 카메라가 비활성화됩니다. 기본값은 꺼짐입니다.

키오스크 장치 정책

March 15, 2024

키오스크 정책을 사용하면 실행할 수 있는 앱을 제한하여 장치를 키오스크 모드로 제한할 수 있습니다. 키오스크 모드에서 잠기는 장치의 부분은 XenMobile 을 통해 제어되지 않습니다. 정책을 배포한 후 장치에서 키오스크 모드 설정을 관리할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

키오스크 장치 정책을 추가하려면

키오스크 모드에서 지정하는 모든 앱은 사용자의 장치에 이미 설치되어 있어야 합니다.

일부 옵션은 Samsung MDM(모바일 기기 관리) API 4.0 이상에만 적용됩니다.

Android Enterprise 설정

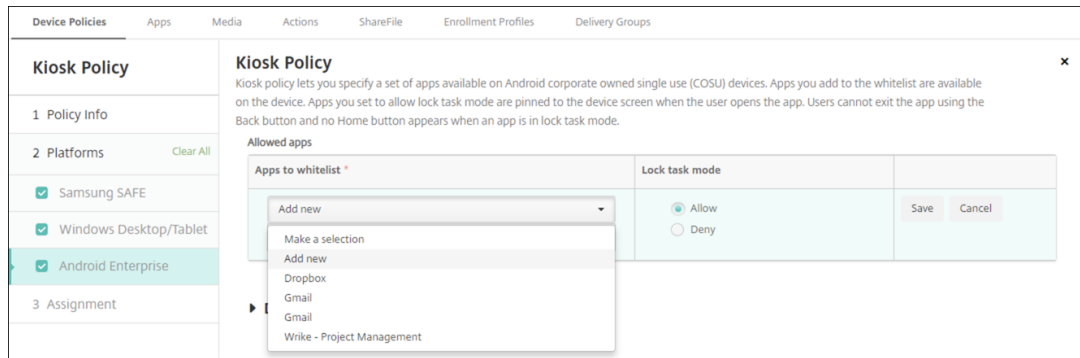
COSU(회사 소유 일회 사용) 장치라고도 하는 전용 Android Enterprise 장치의 경우 앱을 허용하고 작업 잠금 모드를 설정할 수 있습니다. 기본적으로 Secure Hub 와 Google Play 서비스는 허용 목록에 포함됩니다.

앱을 허용하려면 추가를 클릭합니다. 여러 앱을 허용할 수 있습니다. 자세한 내용은 [Android Enterprise](#)를 참조하십시오.

참고:

XenMobile Server 콘솔에는 “블랙리스트” 와 “화이트리스트” 라는 용어가 포함되어 있습니다. 향후 릴리스에서 이러한 용어를 “차단 목록” 및 “허용 목록” 으로 변경하는 중입니다.

- 화이트리스트에 추가할 앱: 화이트리스트에 추가할 앱의 패키지 이름을 입력하거나 목록에서 앱을 선택합니다.
 - 새로 추가를 클릭하여 목록에 표시할 승인된 앱의 패키지 이름을 입력합니다.
 - 목록에서 기존 앱을 선택합니다. 목록에는 XenMobile Server 에 업로드된 앱이 표시됩니다. 기본적으로 Secure Hub 와 Google Play 서비스는 화이트리스트에 포함됩니다.



- **작업 잠금 모드:** 사용자가 앱을 시작할 때 장치 화면에 앱이 고정되도록 설정하려면 허용을 선택합니다. 앱이 고정되지 않도록 설정하려면 거부를 선택합니다. 기본적으로 Secure Hub와 Google Play 서비스는 허용됩니다. 기본값은 허용입니다.

앱이 작업 잠금 모드에 있으면 사용자가 앱을 열 때 앱이 장치 화면에 고정됩니다. 홈 단추가 나타나지 않고 뒤로 단추가 비활성화됩니다. 사용자는 로그아웃과 같이 앱에 프로그래밍된 작업을 사용하여 앱을 종료할 수 있습니다.

Launcher 구성 장치 정책

September 29, 2021

Citrix Launcher를 사용하면 XenMobile에 의해 배포되는 Android 장치의 사용자 환경을 사용자 지정할 수 있습니다. Citrix Launcher 및 Launcher 구성 장치 정책은 Android Enterprise와 호환되지 않습니다.

Launcher 구성 정책을 추가하여 이러한 Citrix Launcher 기능을 제어할 수 있습니다.

- 사용자가 지정된 앱에만 액세스할 수 있도록 Android 장치를 관리합니다.
- 필요에 따라 Citrix Launcher 아이콘의 사용자 지정 로고 이미지와 Citrix Launcher의 사용자 지정 배경 이미지를 지정합니다.
- 사용자가 Launcher를 종료할 때 입력해야 하는 암호를 지정합니다.

Citrix Launcher를 사용하면 이러한 장치 수준 제한을 적용하는 동시에 사용자가 WiFi 설정, Bluetooth 설정 및 장치 암호 설정과 같은 장치 설정에 기본적으로 액세스하여 유연하게 운영할 수 있습니다. Citrix Launcher는 장치 플랫폼이 이미 제공하는 보안에 추가적인 보안 계층을 더하기 위한 것이 아닙니다.

Citrix Launcher를 배포하면 XenMobile이 Launcher를 설치하고 기본 Android Launcher를 대체합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Android(레거시 DA) 및 Android Enterprise 설정

Launcher Configuration Policy	Launcher Configuration Policy This policy lets you define a configuration of an Android device launcher.	
1 Policy Info	Launcher app configuration	
2 Platforms	Define a logo image <input type="checkbox"/> OFF ⓘ	
<input checked="" type="checkbox"/> Android (legacy DA)	Define a background image <input type="checkbox"/> OFF ⓘ	
<input checked="" type="checkbox"/> Android Enterprise	Allowed apps	
3 Assignment	App name	Package name * <input type="text"/> <input type="button" value="Add"/>
	Password	<input type="password"/> ⓘ
	▶ Deployment Rules	

- 로고 이미지 정의: Citrix Launcher 아이콘에 대한 사용자 지정 로고 이미지를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 로고 이미지: 로고 이미지 정의를 사용하는 경우 찾아보기를 클릭하고 파일의 위치로 이동하여 이미지 파일을 선택합니다. 지원되는 파일 형식은 PNG, JPG, JPEG 및 GIF 입니다.
- 배경 이미지 정의: Citrix Launcher 배경에 대한 사용자 지정 이미지를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 배경 이미지: 배경 이미지 정의를 사용하는 경우 찾아보기를 클릭하고 파일의 위치로 이동하여 이미지 파일을 선택합니다. 지원되는 파일 형식은 PNG, JPG, JPEG 및 GIF 입니다.
- 허용되는 앱: Citrix Launcher 에서 허용하려는 각 앱에 대해 추가를 클릭하고 다음을 수행합니다.
 - 추가 할 새 앱: 추가 할 앱의 전체 이름을 입력합니다. 예를 들어 Android 일정 앱의 경우 com.android.calendar 를 입력합니다.
 - 저장을 클릭하여 앱을 추가하거나 취소를 클릭하여 앱 추가를 취소합니다.
- 암호: Citrix Launcher 를 종료할 때 사용자가 입력해야 하는 암호입니다.

LDAP 장치 정책

January 5, 2022

XenMobile 에서 iOS 장치에 대한 LDAP 정책을 만들어 사용할 LDAP 서버에 대한 정보 (예: 필요한 계정 정보 등) 를 제공할 수 있습니다. 또한 LDAP 서버를 쿼리할 때 사용할 LDAP 검색 정책 집합을 제공합니다.

이 정책을 구성하려면 LDAP 호스트 이름이 필요합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#) 을 참조하십시오.

iOS 설정

- **계정 설명:** 선택적 계정 설명을 입력합니다.
- **계정 사용자 이름:** 선택적 사용자 이름을 입력합니다.
- **계정 암호:** 선택적 암호를 입력합니다. 이 필드는 암호화된 프로필에만 사용됩니다.
- **LDAP 호스트 이름:** LDAP 서버 호스트 이름을 입력합니다. 이것은 필수 필드입니다.
- **SSL 사용:** LDAP 서버에 대한 Secure Socket Layer 연결을 사용할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **검색 설정:** LDAP 서버에 쿼리할 때 사용할 검색 설정을 추가합니다. 원하는 수의 검색 설정을 추가할 수 있지만 계정을 유용하게 사용하려면 적어도 하나 이상의 검색 설정을 추가해야 합니다. 추가를 클릭하고 다음을 수행합니다.
 - **설명:** 검색 설정의 설명을 입력합니다. 이것은 필수 필드입니다.
 - **범위:** 기준, 한 수준 또는 하위 트리를 선택하여 검색할 LDAP 트리의 깊이를 정의합니다. 기본값은 기준입니다.
 - * 기준은 검색 기준이 가리키는 노드를 검색합니다.
 - * 한 수준은 기준 노드와 한 수준 아래 노드를 검색합니다.
 - * 하위 트리는 기준 노드와 모든 하위 노드를 깊이에 관계없이 검색합니다.
 - **검색 기준:** 검색을 시작할 노드에 대한 경로를 입력합니다. 예를 들어 ou=people 또는 0=example corp 을 입력합니다. 이것은 필수 필드입니다.
 - 저장을 클릭하여 검색 설정을 추가하거나 취소를 클릭하여 검색 설정 추가를 취소합니다.
 - 추가할 각 검색 설정에 대해 이 단계를 반복합니다.
- **정책 설정**
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- **계정 설명:** 선택적 계정 설명을 입력합니다.
- **계정 사용자 이름:** 선택적 사용자 이름을 입력합니다.
- **계정 암호:** 선택적 암호를 입력합니다. 이 필드는 암호화된 프로필에만 사용됩니다.
- **LDAP 호스트 이름:** LDAP 서버 호스트 이름을 입력합니다. 이것은 필수 필드입니다.
- **SSL 사용:** LDAP 서버에 대한 Secure Socket Layer 연결을 사용할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **검색 설정:** LDAP 서버에 쿼리할 때 사용할 검색 설정을 추가합니다. 원하는 수의 검색 설정을 추가할 수 있지만 계정을 유용하게 사용하려면 적어도 하나 이상의 검색 설정을 추가해야 합니다. 추가를 클릭하고 다음을 수행합니다.
 - **설명:** 검색 설정의 설명을 입력합니다. 이것은 필수 필드입니다.
 - **범위:** 기준, 한 수준 또는 하위 트리를 선택하여 검색할 LDAP 트리의 깊이를 정의합니다. 기본값은 기준입니다.
 - * 기준은 검색 기준이 가리키는 노드를 검색합니다.

- ★ 한 수준은 기준 노드와 한 수준 아래 노드를 검색합니다.
 - ★ 하위 트리는 기준 노드와 모든 하위 노드를 깊이에 관계없이 검색합니다.
 - 검색 기준: 검색을 시작할 노드에 대한 경로를 입력합니다. 예를 들어 ou=people 또는 0=example corp 을 입력합니다. 이것은 필수 필드입니다.
 - 저장을 클릭하여 검색 설정을 추가하거나 취소를 클릭하여 검색 설정 추가를 취소합니다.
 - 추가할 각 검색 설정에 대해 이 단계를 반복합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.
 - 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
 - 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

위치 장치 정책

January 5, 2022

XenMobile 에서 위치 장치 정책을 만들어 지리적 경계를 적용할 수 있습니다. 사용자가 정의된 경계 (지오펜스라고도 함) 를 위반하면 XenMobile 이 특정 동작을 수행할 수 있습니다. 예를 들어 사용자가 정의된 경계를 위반할 경우 사용자에게 경고 메시지를 보내도록 정책을 구성할 수 있습니다. 사용자가 경계를 위반할 경우 즉시 또는 지연 후에 사용자의 회사 데이터를 초기화하는 정책을 구성할 수 있습니다. 장치 추적 및 찾기 사용 여부와 같은 보안 조치에 대한 자세한 내용은 [보안 동작](#)을 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

Location Policy	Location Policy
1 Policy Info	This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.
2 Platforms	Device agent configuration
<input checked="" type="checkbox"/> iOS	<div>Location Timeout: 1 Minutes</div> <div>Tracking duration: 6 Hours</div> <div>Accuracy: 328 Feet</div>
3 Assignment	<div>Report if Location Services are disabled: OFF</div> <div>Geofencing: OFF</div>
	► Deployment Rules

- **위치 시간 제한:** 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 XenMobile 이 장치의 위치를 수정하려고 시도하는 빈도를 설정합니다. 유효한 값은 60~900 초 또는 1~15 분입니다. 기본값은 1 분입니다.
- **추적 기간:** 숫자를 입력한 다음 목록에서 시간 또는 분을 클릭하여 XenMobile 이 장치를 추적하는 기간을 설정합니다. 유효한 값은 1~6 시간 또는 10~360 분입니다. 기본값은 6 시간입니다.
- **정확도:** 숫자를 입력한 다음 목록에서 미터, 피트 또는 야드를 클릭하여 XenMobile 이 장치를 추적하는 정확도를 설정합니다. 유효한 값은 10~5000 야드 (또는 미터) 또는 30~15000 피트입니다. 기본값은 328 피트입니다.
- **위치 서비스가 사용하지 않도록 설정될 경우 보고:** GPS 를 사용하지 않을 때 장치가 XenMobile 에 보고서를 보낼지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **지오펜스**

지오펜스를 사용하도록 설정한 경우 다음 설정을 구성합니다.

- **반경:** 숫자를 입력한 다음 목록에서 반경을 측정하는 데 사용할 단위를 클릭합니다. 기본값은 16,400 피트입니다. 유효한 반경은 다음과 같습니다.
 - 164~164,000 피트
 - 50~50,000 미터
 - 54~54,680 야드
 - 1~31 마일
- **중심점 위도:** 위도 (예: 37.787454) 를 입력하여 지오펜스 중심점의 위도를 정의합니다.
- **중심점 경도:** 경도 (예: 122.402952) 를 입력하여 지오펜스 중심점의 경도를 정의합니다.
- **경계 위반 시 사용자에게 경고 표시:** 사용자가 정의된 경계를 위반할 경우 경고 메시지를 발행할지 여부를 선택합니다. 기본값은 꺼짐입니다. 경고 메시지를 표시하는 데에는 XenMobile 연결이 필요하지 않습니다.
- **경계 위반 시 회사 데이터 초기화:** 사용자의 장치가 경계를 위반한 경우 장치를 초기화할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하도록 설정하면 로컬 초기화 시 지연 필드가 나타납니다.
 - 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 사용자의 장치에서 회사 데이터를 초기화하기 전에 대기 할 기간을 설정합니다. 이 설정은 XenMobile 이 사용자의 장치를 선택적으로 초기화하기 전에 사용자가 허용된 위치로 돌아갈 수 있는 기회를 제공합니다. 기본값은 0 초입니다.

Android 설정

Location Policy	Location Policy
1 Policy Info	This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.
2 Platforms	<p>Device agent configuration</p> <p>Poll interval: 10 Minutes</p> <p>Report if Location Services is disabled: OFF</p> <p>Geofencing: OFF</p> <p>► Deployment Rules</p>
<input type="checkbox"/> iOS <input checked="" type="checkbox"/> Android	
3 Assignment	

- **폴링 간격:** 숫자를 입력한 다음 목록에서 분, 시간 또는 일을 클릭하여 XenMobile 이 장치의 위치를 수정하려고 시도하는 빈도를 설정합니다. 유효한 값은 1~1440 분, 1~24 시간 또는 일 수입니다. 기본값은 10 분입니다. 이 값을 10 분 미만으로 설정하면 장치의 배터리 수명이 저하될 수 있습니다.
- 위치 서비스가 사용하지 않도록 설정될 경우 보고: GPS 를 사용하지 않을 때 장치가 XenMobile 에 보고서를 보낼지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 지오펜스

Geofencing **ON**

Radius: 16400 Feet

Center point latitude*: 0.000000

Center point longitude*: 0.000000

Warn user on perimeter breach: OFF

Device connects to XenMobile for policy refresh

☒ Perform no action on perimeter breach
☐ Wipe corporate data on perimeter breach
☐ Lock device locally

지오펜스를 사용하도록 설정한 경우 다음 설정을 구성합니다.

- **반경:** 숫자를 입력한 다음 목록에서 반경을 측정하는 데 사용할 단위를 클릭합니다. 기본값은 16,400 피트입니다. 유효한 반경은 다음과 같습니다.
 - 164~164,000 피트
 - 1~50 킬로미터
 - 50~50,000 미터
 - 54~54,680 야드
 - 1~31 마일
- **중심점 위도:** 위도 (예: 37.787454) 를 입력하여 지오펜스 중심점의 위도를 정의합니다.

- 중심점 경도: 경도 (예: 122.402952) 를 입력하여 지오펜스 중심점의 경도를 정의합니다.
- 경계 위반 시 사용자에게 경고 표시: 사용자가 정의된 경계를 위반할 경우 경고 메시지를 발행할지 여부를 선택합니다. 기본값은 꺼짐입니다. 경고 메시지를 표시하는 데에는 XenMobile 연결이 필요하지 않습니다.
- 정책 새로 고침을 위해 장치가 **XenMobile** 에 연결: 사용자가 경계를 위반한 경우에 대해 다음 옵션 중 하나를 선택합니다.
 - 경계 위반 시 아무런 동작을 수행하지 않음: 아무 작업도 하지 않습니다. 이 설정은 기본값입니다.
 - 경계 위반 시 회사 데이터 초기화: 지정된 시간이 지난 후 회사 데이터를 초기화합니다. 이 옵션을 사용하도록 설정하면 로컬 초기화 시 지연 필드가 나타납니다.
 - * 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 사용자의 장치에서 회사 데이터를 초기화하기 전에 대기할 기간을 설정합니다. 이 설정은 XenMobile 이 사용자의 장치를 선택적으로 초기화하기 전에 사용자가 허용된 위치로 돌아갈 수 있는 기회를 제공합니다. 기본값은 0 초입니다.
 - 잠금 시 지연: 지정된 시간이 지난 후 사용자의 장치를 잠급니다. 이 옵션을 사용하도록 설정하면 잠금 시 지연 필드가 나타납니다.
 - * 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 사용자의 장치를 잠그기 전에 대기할 기간을 설정합니다. 이 설정은 XenMobile 이 사용자의 장치를 잠그기 전에 사용자가 허용된 위치로 돌아갈 수 있는 기회를 제공합니다. 기본값은 0 초입니다.

Android Enterprise 설정

Android 위치 추적이 작동하려면 다음 요구 사항을 충족해야 합니다.

- Android 8.5 이상
- Android Enterprise 의 제한 장치 정책에서 위치 공유 허용 설정 사용 설정됨
- 연결 예약 (Firebase Cloud Messaging 권장)

Location Policy	Location Policy
1 Policy Info	This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.
2 Platforms	<p>Apply to fully managed devices with a work profile/Work profile on corporate-owned devices <input type="checkbox"/></p> <p>Managed device</p> <p>Location Mode <input type="text" value="Off"/></p> <p>Managed profile</p> <p>Report if Location Services is disabled <input type="checkbox"/></p> <p>Geofencing <input type="checkbox"/></p>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> Android (legacy DA) <input checked="" type="checkbox"/> Android Enterprise	
3 Assignment	

작업 프로필로 완전히 관리되는 장치에 적용

작업 프로필로 완전히 관리되는 장치의 경우 위치 모드 설정을 사용할 수 있습니다.

- **작업 프로필/회사 소유 장치의 작업 프로필을 사용하는 완전 관리형 장치에 적용:** 작업 프로필로 완전히 관리되는 장치에 대해 위치 모드를 구성할 수 있도록 허용합니다. 이 설정이 켜져 있으면 작업 프로필에 대한 위치 모드 설정을 구성합니다.

- 위치 서비스가 사용하지 않도록 설정될 경우 보고: 사용자가 GPS 를 끈 경우 장치에서 XenMobile Server 에 보고서를 보낼지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 지오펜스: 관리되는 장치에서 이 문서의 설정을 참조하십시오.

작업 프로필/회사 소유 장치의 작업 프로필을 사용하는 완전 관리형 장치에 적용이 꺼짐이면 다음 섹션에 표시된 것과 같이 관리되는 장치와 작업 프로필에 설정이 적용됩니다. 기본값은 꺼짐입니다.

관리되는 장치

- **위치 모드:** 사용할 위치 검색의 수준을 지정합니다. 위치 모드가 높은 정확도 또는 배터리 절약으로 설정된 경우에만 찾기 보안 동작을 사용할 수 있습니다. 기본값은 높은 정확도입니다.
 - 높은 정확도: GPS, 네트워크 및 기타 센서를 포함한 모든 위치 검색 방법을 사용하도록 설정합니다.
 - 센서만: GPS 및 기타 센서만 사용하도록 설정합니다.
 - 배터리 절약: 네트워크 위치 공급자만 사용하도록 설정합니다.
 - 꺼짐: 위치 검색을 사용하지 않습니다.
- **지오펜스:**

The screenshot shows the Geofencing configuration page. At the top, the 'Geofencing' toggle is switched to 'ON'. Below it, the 'Poll interval' is set to '10' with a unit dropdown menu currently showing 'Minutes'. The 'Radius' is set to '16400' with a unit dropdown menu showing 'Feet'. The 'Center point latitude' and 'Center point longitude' fields both contain the value '0.000000'. The 'Warn user on perimeter breach' toggle is set to 'OFF'. At the bottom, under the heading 'Device connects to Endpoint Management for policy refresh', there are three radio button options: 'Perform no action on perimeter breach' (which is selected), 'Wipe corporate data on perimeter breach', and 'Lock device locally'.

지오펜스를 사용하도록 설정한 경우 다음 설정을 구성합니다.

- **폴링 간격:** 숫자를 입력한 다음 분, 시간 또는 일을 클릭하여 XenMobile Server가 장치의 위치를 수정하려고 시도하는 빈도를 설정합니다. 유효한 값은 1~1440 분, 1~24 시간 또는 일 수입니다. 기본값은 **10** 분입니다. 이 값을 10 분 미만으로 설정하면 장치의 배터리 수명이 저하될 수 있습니다.
- **반경:** 숫자를 입력한 다음 반경을 측정하는 데 사용할 단위를 클릭합니다. 기본값은 **5,000** 미터 (**16,400** 피트)입니다. 유효한 반경은 다음과 같습니다.
 - 164~164,000 피트
 - 1~50 킬로미터
 - 50~50,000 미터
 - 54~54,680 야드
 - 1~31 마일
- **중심점 위도:** 위도 (예: 37.787454)를 입력하여 지오펜스 중심점의 위도를 정의합니다. 값을 조회하려면 관리 > 장치에서 장치를 선택하고 보안을 클릭한 다음 찾기를 클릭합니다. 장치를 찾은 후 XenMobile Server는 보안 아래의 장치 세부 정보 > 일반 페이지에 장치 위치를 보고합니다.
- **중심점 경도:** 경도 (예: 122.402952)를 입력하여 지오펜스 중심점의 경도를 정의합니다.
- **경계 위반 시 사용자에게 경고 표시:** 사용자가 정의된 경계를 위반할 경우 경고 메시지를 발행할지 여부를 선택합니다. 기본값은 꺼짐입니다. 경고 메시지를 표시하는 데에는 XenMobile Server 연결이 필요하지 않습니다.
- **정책 새로 고침을 위해 장치가 XenMobile Server에 연결:** 사용자가 경계를 위반한 경우에 대해 다음 옵션 중 하나를 선택합니다.
 - 경계 위반 시 아무런 동작을 수행하지 않음: 아무 작업도 하지 않습니다. 이 설정은 기본값입니다.
 - 경계 위반 시 회사 데이터 초기화: 지정된 시간이 지난 후 회사 데이터를 초기화합니다. 이 옵션을 사용하도록 설정하면 로컬 초기화 시 지연 필드가 나타납니다.
 - * 숫자를 입력한 다음 초 또는 분을 클릭하여 사용자의 장치에서 회사 데이터를 초기화하기 전에 초기화를 지연할 기간을 설정합니다. 이 지연 기간은 XenMobile Server가 사용자의 장치를 선택적으로 초기화하기 전에 사용자가 허용된 위치로 돌아갈 수 있는 기회를 제공합니다. 기본값은 **0** 초입니다.
 - 로컬에서 장치 잠금: 지정된 시간이 지난 후 사용자의 장치를 잠급니다. 이 옵션을 사용하도록 설정하면 잠금 시 지연 필드가 나타납니다.
 - * 숫자를 입력한 다음 초 또는 분을 클릭하여 사용자의 장치를 잠그기 전에 잠금을 지연할 기간을 설정합니다. 이 지연 기간은 XenMobile Server가 사용자의 장치를 잠그기 전에 사용자가 허용된 위치로 돌아갈 수 있는 기회를 제공합니다. 기본값은 **0** 초입니다.

관리되는 프로필

- 위치 서비스가 사용하지 않도록 설정될 경우 보고: 사용자가 GPS를 끈 경우 장치에서 XenMobile Server에 보고서를 보낼지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 지오펜스: [관리되는 장치](#)에서 이 문서의 설정을 참조하십시오.

메일 장치 정책

January 5, 2022

XenMobile 에서 메일 장치 정책을 추가하여 iOS 또는 macOS 장치에서 전자 메일 계정을 구성할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 및 macOS 설정

Mail Policy	Mail Policy
1 Policy Info	This configuration allows you to set email parameters. Note that when applied to a supervised device, you need to configure Email address and User name fields.
2 Platforms	<div>Account description *</div> <div>Account type</div> <div>Path prefix</div> <div>User display name *</div> <div>Email address *</div>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS	<div>Incoming email</div> <div>Email server host name *</div> <div>Email server port *</div> <div>User name *</div> <div>Authentication type</div> <div>Password</div>
3 Assignment	

- **계정 설명:** 메일 및 설정 앱에 나타나는 계정 설명을 입력합니다. 이것은 필수 필드입니다.
- **계정 유형:** **IMAP** 또는 **POP** 를 선택하여 사용자 계정에 사용할 프로토콜을 선택합니다. 기본값은 **IMAP** 입니다. **POP** 를 선택하면 다음 경로 접두사 옵션이 사라집니다.
- **경로 접두사:** **INBOX** 또는 IMAP 메일 계정 경로 접두사를 입력합니다. 이것은 필수 필드입니다.
- **사용자 표시 이름:** 메시지 및 기타 용도로 사용할 전체 사용자 이름을 입력합니다. 이것은 필수 필드입니다.
- **전자 메일 주소:** 계정의 전체 전자 메일 주소를 입력합니다. 이것은 필수 필드입니다.
- **들어오는 전자 메일 설정**
 - **전자 메일 서버 호스트 이름:** 들어오는 메일 서버 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - **전자 메일 서버 포트:** 들어오는 메일 서버 포트 번호를 입력합니다. 기본값은 **143** 입니다. 이것은 필수 필드입니다.
 - **사용자 이름:** 전자 메일 계정의 사용자 이름을 입력합니다. 이 이름은 일반적으로 전자 메일 주소에서 @ 문자까지의 부분과 같습니다. 이것은 필수 필드입니다.
 - **인증 유형:** 사용할 인증 유형을 선택합니다. 기본값은 암호입니다. 없음을 선택하면 다음 암호 필드가 사라집니다.
 - **암호:** 들어오는 메일 서버에 대한 선택적 암호를 입력합니다.
 - **SSL 사용:** 들어오는 메일 서버가 SSL(Secure Socket Layer) 인증을 사용하는지 여부를 선택합니다. 기본값은 꺼짐입니다.

- 나가는 전자 메일 설정

- 전자 메일 서버 호스트 이름: 나가는 메일 서버 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
- 전자 메일 서버 포트: 나가는 메일 서버 포트 번호를 입력합니다. 포트가 없는 경우 포트 번호를 입력하지 않으면 지정된 프로토콜의 기본 포트가 사용됩니다.
- 사용자 이름: 전자 메일 계정의 사용자 이름을 입력합니다. 이 이름은 일반적으로 전자 메일 주소에서 @ 문자까지의 부분과 같습니다. 이것은 필수 필드입니다.
- 인증 유형: 사용할 인증 유형을 선택합니다. 기본값은 암호입니다.
- 암호: 나가는 메일 서버에 대한 선택적 암호를 입력합니다.
- 나가는 암호와 들어오는 암호가 같음: 들어오는 암호와 나가는 암호가 같은지 여부를 선택합니다. 기본값은 꺼짐이며, 이는 암호가 다르다는 의미입니다.
- **SSL** 사용: 나가는 메일 서버가 SSL(Secure Socket Layer) 인증을 사용하는지 여부를 선택합니다. 기본값은 꺼짐입니다.

- 정책

- 계정 간 전자 메일 이동 승인: 사용자가 이 계정에서 다른 계정으로 전자 메일을 이동하고 다른 계정에서 전자 메일을 전달하고 회신할 수 있도록 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 메일 앱에서만 전자 메일 보내기: 전자 메일을 보낼 사용자를 iOS 메일 앱으로 제한할지 여부를 선택합니다.
- 최근 메일 동기화 사용 안 함: 사용자가 최근 주소를 동기화하지 못하도록 할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 6.0 이상에만 적용됩니다.
- 메일 삭제 허용: iOS 9.2 이상을 실행하는 장치에서 Apple Mail Drop의 사용을 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **S/MIME** 서명 사용: 이 계정이 S/MIME 서명을 지원하는지 여부를 선택합니다. 기본값은 켜짐입니다. 켜짐으로 설정하면 다음 필드가 나타납니다.
 - * 서명 ID 자격 증명: 사용할 서명 자격 증명을 선택합니다.
 - * **S/MIME** 서명 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
 - * **S/MIME** 서명 인증서 **UUID** 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
- **S/MIME** 암호화 사용: 이 계정이 S/MIME 암호화를 지원하는지 여부를 선택합니다. 기본값은 꺼짐입니다. 켜짐으로 설정하면 다음 필드가 나타납니다.
 - * 암호화 ID 자격 증명: 사용할 암호화 자격 증명을 선택합니다.
 - * 메시지별 **S/MIME** 전환 사용: 켜짐으로 설정하면 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션이 표시됩니다. 기본값은 꺼짐입니다.
 - * 기본적으로 **S/MIME** 암호화 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME를 기본적으로 켜지 여부를 선택할 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
 - * **S/MIME** 암호화 인증서 **UUID** 사용자 재정의 가능: 켜짐으로 설정하면 사용자가 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

- 정책 설정

- 정책 제거: 나중에 정책을 제거하려면 날짜 선택 또는 제거할 때까지의 기간 (시간) 에서 정책을 제거하도록 이 설정을 구성하면 됩니다.
- 사용자가 정책을 제거하도록 허용: 사용자가 메일 정책을 제거하는 것을 항상 허용하거나, 암호 필요로만 허용하거나 안 함으로 설정합니다.
- 프로필 범위: macOS 에 한해 정책을 사용자 수준별로 적용할지 전체 시스템에 적용할지를 선택합니다.

관리되는 구성 정책

February 2, 2023

관리되는 구성 장치 정책은 다양한 앱 구성 옵션과 앱 제한을 제어합니다. 앱 개발자는 앱에서 사용할 수 있는 옵션과 도구 설명을 정의합니다. 도구 설명에 “템플릿 값” 사용이 언급되는 경우 해당하는 XenMobile 매크로를 대신 사용합니다. 자세한 내용은 [원격 구성 개요](#)(Android 개발자 사이트) 및 [매크로](#)를 참조하십시오.

앱 구성 설정에는 다음과 같은 항목이 포함될 수 있습니다.

- 앱 전자 메일 설정
- 웹 브라우저의 URL 허용 또는 차단
- 셀룰러 연결을 통해 또는 Wi-Fi 연결을 통해서만 앱 콘텐츠 동기화를 제어하는 옵션

앱에 대해 표시되는 설정에 대한 자세한 내용은 앱 개발자에게 문의하십시오.

사전 요구 사항

- Google 에서 Android Enterprise 설정 작업을 완료하고 Android Enterprise 를 관리되는 Google Play 에 연결합니다. 자세한 내용은 [Android Enterprise](#)를 참조하십시오.
- XenMobile 에 Android Enterprise 앱을 추가합니다. 자세한 내용은 [XenMobile 에 앱 추가](#)를 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

앱별 VPN 에 대한 요구 사항

AE 에 대한 앱별 VPN 을 만들려면 관리되는 구성 정책을 구성하는 것 외에도 추가 단계를 수행해야 합니다. 또한 다음 사전 요구 사항도 충족하는지 확인해야 합니다.

- 온프레미스 Citrix Gateway
- 다음 응용 프로그램이 장치에 설치됩니다.
 - Citrix SSO
 - Citrix Secure Hub

AE 장치에 대한 앱별 VPN 을 구성하는 일반적인 워크플로는 다음과 같습니다.

1. 이 문서에 설명된 대로 VPN 프로필을 구성합니다.
2. 앱별 VPN 에서 트래픽을 허용하도록 Citrix ADC 를 구성합니다. 자세한 내용은 [Citrix Gateway 에서 전체 VPN 설정](#)을 참조하십시오.

Android Enterprise 설정

관리되는 구성 장치 정책을 추가하도록 선택하면 앱을 선택하라는 메시지가 나타납니다. XenMobile 에 추가된 Android Enterprise 앱이 없는 경우 계속 진행할 수 없습니다.

앱을 선택한 후 정책 설정을 구성합니다. 설정은 각 앱마다 다릅니다.

Android Enterprise Managed Configurations	Android Enterprise Managed Configurations
1 Policy Info	This policy lets you control a variety of app configuration options and app restrictions. The options available for an app and the tooltips are defined by the app developer. If a tooltip mentions using a "templated value", use the corresponding Endpoint Management macro instead.
2 Platforms Clear All	
<input checked="" type="checkbox"/> Android Enterprise	<p>Restrictions for importing documents</p> <p><input type="checkbox"/> Box</p> <p><input type="checkbox"/> DropBox</p> <p><input type="checkbox"/> Drive</p> <p>Restrictions for sharing the DocuSign app</p> <p><input type="checkbox"/> Box</p> <p><input type="checkbox"/> DropBox</p> <p><input type="checkbox"/> Drive</p> <p><input type="checkbox"/> Evernote</p> <p>Restrictions for sharing envelopes and documents</p> <p><input type="checkbox"/> Box</p> <p><input type="checkbox"/> DropBox</p> <p><input type="checkbox"/> Drive</p> <p><input type="checkbox"/> Evernote</p>
3 Assignment	

Android Enterprise 에 대한 VPN 프로필 구성

Citrix SSO 앱과 관리되는 구성 장치 정책을 사용하여 Android Enterprise 장치에서 사용할 수 있는 VPN 프로필을 제공합니다.



먼저 Citrix SSO 를 Google Play Store 앱으로 XenMobile 콘솔에 추가합니다. [공개 앱 스토어 앱 추가](#)를 참조하십시오.

Device Policies **Apps** Media Actions ShareFile Enrollment Profiles Delivery Groups

> **Apps** Search

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

Add | Category | Export

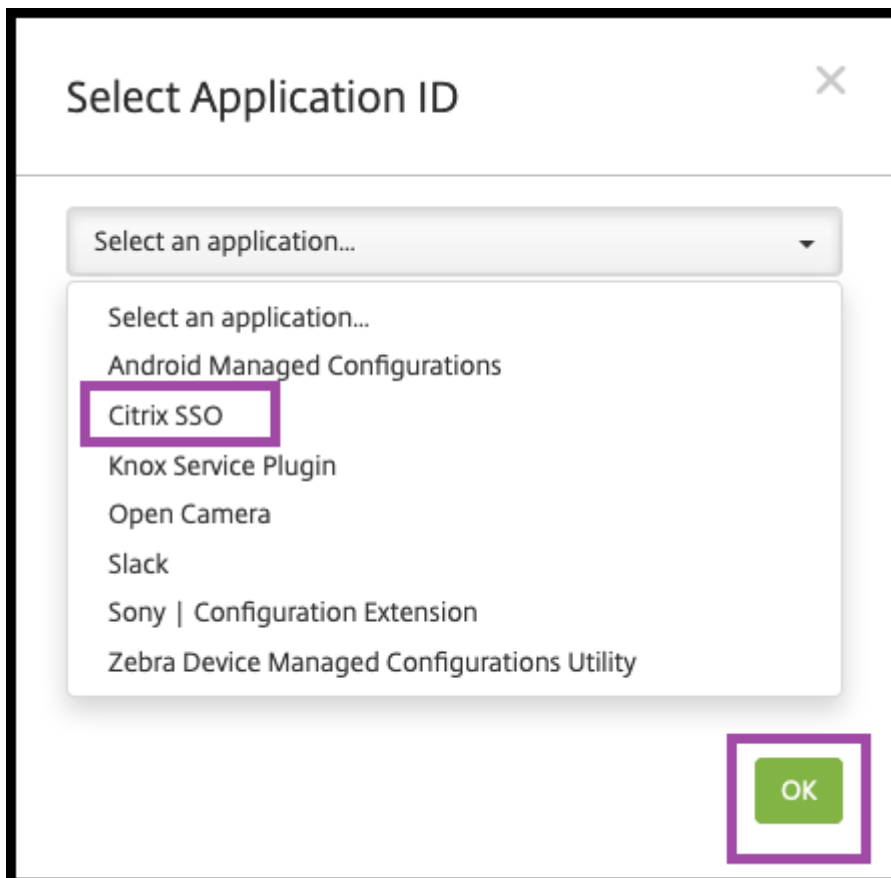
<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated
<input type="checkbox"/>		Citrix SSO	Public App Store	Default	3/19/19 8:36:03 am	4/9/19 3:25:17 pm
<input type="checkbox"/>		E1-GOOGLE	Enterprise	Default	2/14/19 7:33:58 am	2/14/19 7:33:58 am

Citrix SSO 에 대한 **Android Enterprise** 관리되는 구성 만들기

Citrix SSO 에 대한 관리되는 구성 장치 정책을 구성하여 VPN 프로필을 만듭니다. 만든 VPN 프로필에는 Citrix SSO 앱이 설치되고 정책이 배포된 장치에서 액세스할 수 있습니다.

Citrix Gateway FQDN 및 포트가 필요합니다.

1. XenMobile 콘솔에서 구성 > 장치 정책을 클릭합니다. 추가를 클릭합니다.
2. **Android Enterprise** 를 선택합니다. 관리되는 구성을 클릭합니다.
3. 응용 프로그램 ID 선택 창이 나타나면 목록에서 **Citrix SSO** 를 선택하고 확인을 클릭합니다.



4. Citrix SSO VPN 구성에 대한 이름과 설명을 입력합니다. 다음을 클릭합니다.

5. VPN 프로파일 매개 변수를 구성합니다.

- **VPN 프로파일 이름.** VPN 프로파일의 이름을 입력합니다. 둘 이상의 VPN 프로파일을 만드는 경우 각각에 대해 고유한 이름을 사용합니다. 이름을 제공하지 않으면 서버 주소필드에 입력한 주소가 VPN 프로파일 이름으로 사용됩니다.
- **서버 주소 (*).** Citrix Gateway FQDN 을 입력합니다. Citrix Gateway 포트가 443 이 아닌 경우 해당 포트를 입력합니다. URL 형식을 사용합니다. 예: <https://gateway.mycompany.com:8443>.
- **사용자 이름 (선택 사항).** 최종 사용자가 Citrix Gateway 에 인증할 때 사용하는 사용자 이름을 제공합니다. 이 필드에 XenMobile 매크로 {user.username} 을 사용할 수 있습니다. [매크로](#)를 참조하십시오. 사용자 이름을 제공하지 않으면 사용자가 Citrix Gateway 에 연결할 때 사용자 이름을 제공하라는 메시지가 표시됩니다.
- **암호 (선택 사항).** 최종 사용자가 Citrix Gateway 에 인증할 때 사용하는 암호를 제공합니다. 암호를 제공하지 않으면 사용자가 Citrix Gateway 에 연결할 때 암호를 제공하라는 메시지가 표시됩니다.
- **인증서 별칭 (선택 사항).** 인증서 별칭을 입력합니다. 인증서 별칭으로 앱에서 인증서에 액세스하기가 더 간편해집니다. 동일한 인증서 별칭을 자격 증명 장치 정책에 사용할 경우 앱에서 사용자 작업 없이 인증서를 검색하고 VPN 을 인증합니다.
- **앱별 VPN 유형 (선택 사항).** 앱별 VPN 을 사용하여 이 VPN 을 사용하는 앱을 제한하는 경우 이 설정을 구성할 수 있습니다. 허용을 선택하면 **PerAppVPN** 앱 목록에 나열된 앱 패키지 이름에 대한 네트워크 트래픽이 VPN 을 통해 라우팅됩니다. 다른 모든 앱의 네트워크 트래픽은 VPN 외부에서 라우팅됩니다. 허용 안 함을 선택하면 **PerAppVPN** 앱 목록에 나열된 앱 패키지 이름에 대한 네트워크 트래픽이 VPN 외부에서 라우팅됩니다. 다른 모든 앱의 네트워크 트래픽은 VPN 을 통해 라우팅됩니다. 기본값은 허용입니다.
- **PerAppVPN 앱 목록.** 앱별 VPN 유형의 값에 따라 VPN 에서 트래픽이 허용되거나 차단되는 앱의 목록입니다. 쉼표 또는 세미콜론으로 구분하여 앱 패키지 이름을 나열합니다. 앱 패키지 이름은 대소문자를 구분하며 이 목록에 나타나는 이름은 Google Play Store 에 나타나는 것과 정확히 일치해야 합니다. 이 목록은 선택 사항입니다. 장치 전체 VPN 을 프로비전하려면 이 목록을 비워 두십시오.

- 기본 **VPN** 프로파일. 사용자가 특정 프로파일을 누르지 않고 Citrix SSO 앱의 사용자 인터페이스에서 연결 스위치를 누를 때 사용할 VPN 프로파일의 이름을 입력합니다. 이 필드를 비워 두면 기본 프로파일이 연결에 사용됩니다. 하나의 프로파일만 구성된 경우 기본 프로파일로 표시됩니다. 항상 VPN 연결의 경우 항상 VPN 연결을 설정하는 데 사용할 VPN 프로파일의 이름으로 이 필드를 설정해야 합니다.
- 사용자 프로파일 사용 안 함. 이 설정이 켜짐인 경우 사용자는 장치에서 자체 VPN 을 만들 수 없습니다. 이 설정이 꺼짐인 경우 사용자는 장치에서 자체 VPN 을 만들 수 있습니다. 기본값은 꺼짐입니다.
- 신뢰할 수 없는 서버 차단. Citrix Gateway 에 대해 자체 서명된 인증서를 사용하는 경우 또는 Citrix Gateway 인증서를 발급하는 CA 의 루트 인증서가 시스템 CA 목록에 없는 경우 이 설정은 꺼짐입니다. 이 설정이 켜짐인 경우 Android 운영 체제에서는 Citrix Gateway 인증서의 유효성이 검사됩니다. 유효성 검사에 실패하면 연결이 허용되지 않습니다. 기본값은 켜짐입니다.

6. 필요한 경우 사용자 지정 매개 변수를 만듭니다. 사용자 지정 매개 변수 **XenMobileDeviceId** 와 **UserAgent** 가 지원됩니다. 현재 VPN 구성을 선택하고 추가를 클릭합니다.

- a) 사용자 지정 매개 변수를 만듭니다.

- 매개 변수 이름. **XenMobileDeviceId** 를 입력합니다. 이 필드는 XenMobile 의 장치 등록을 기준으로 네트워크 액세스 검사에 사용할 장치 ID 입니다. XenMobile 에서 장치를 등록하고 관리하는 경우 VPN 연결이 허용됩니다. 그렇지 않으면 VPN 설정 시 인증이 거부됩니다.

- 매개 변수 값 XenMobile 에서 장치의 등록 및 관리 상태를 결정하려면 XenMobileDeviceId 의 값을 `DeviceID_${ device.id }` 로 설정합니다.

The screenshot shows the 'Android Enterprise Managed Configurations' interface. On the left, there's a sidebar with '1 Policy Info', '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. The '2 Platforms' section is active, showing 'Android Enterprise' with a checkmark. The main area is titled 'List of additional VPN profiles' and contains a table with two rows: 'Parameter Name' with the value 'XenMobileDeviceId' and 'Parameter Value' with the value 'DeviceID_\${device.id}'. There are 'Add' and 'Delete' buttons at the top of the table.

- 다른 사용자 지정 매개 변수를 만들려면 추가를 다시 클릭합니다. 이 사용자 지정 매개 변수를 만듭니다.
 - 매개 변수 이름. **UserAgent** 를 입력합니다. 이 텍스트는 Citrix Gateway 에서 추가 검사를 수행하기 위해 사용자 에이전트 HTTP 헤더에 추가됩니다. 이 텍스트의 값은 Citrix 게이트웨이와 통신하는 동안 Citrix SSO 앱을 통해 사용자 에이전트 HTTP 헤더에 추가됩니다.
 - 매개 변수 값. 사용자 에이전트 HTTP 헤더에 추가할 텍스트를 입력합니다. 이 텍스트는 HTTP 사용자 에이전트 사양을 준수해야 합니다.
7. 필요한 경우 VPN 프로필 구성을 추가로 만듭니다. 구성 목록에서 추가를 클릭합니다. 새 구성이 목록에 나타납니다. 새 구성을 선택하고 5 단계와 6 단계를 반복합니다 (선택 사항).

The screenshot shows the 'Android Enterprise Managed Configurations' interface. On the left, there's a sidebar with '1 Policy Info', '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. The '2 Platforms' section is active, showing 'Android Enterprise' with a checkmark. The main area is titled 'List of additional VPN profiles' and contains a table with one row: 'VPN Profile Name' with the value 'Profile2'. There are 'Add' and 'Delete' buttons at the top of the table. Below the table, there's a 'Deployment Rules' section. At the bottom right, there are 'Back' and 'Next >' buttons.

- 원하는 VPN 프로필을 모두 만들었으면 다음을 클릭합니다.
- Citrix SSO 의 이 관리되는 구성에 대한 배포 규칙을 구성합니다.
- 저장을 클릭합니다.

이제 Citrix SSO 에 대한 이러한 관리되는 구성이 구성된 장치 정책 목록에 나타납니다.

구성한 VPN 프로필에 대해 항상 커기를 사용하려면 [XenMobile 옵션 장치 정책](#) 을 설정합니다.

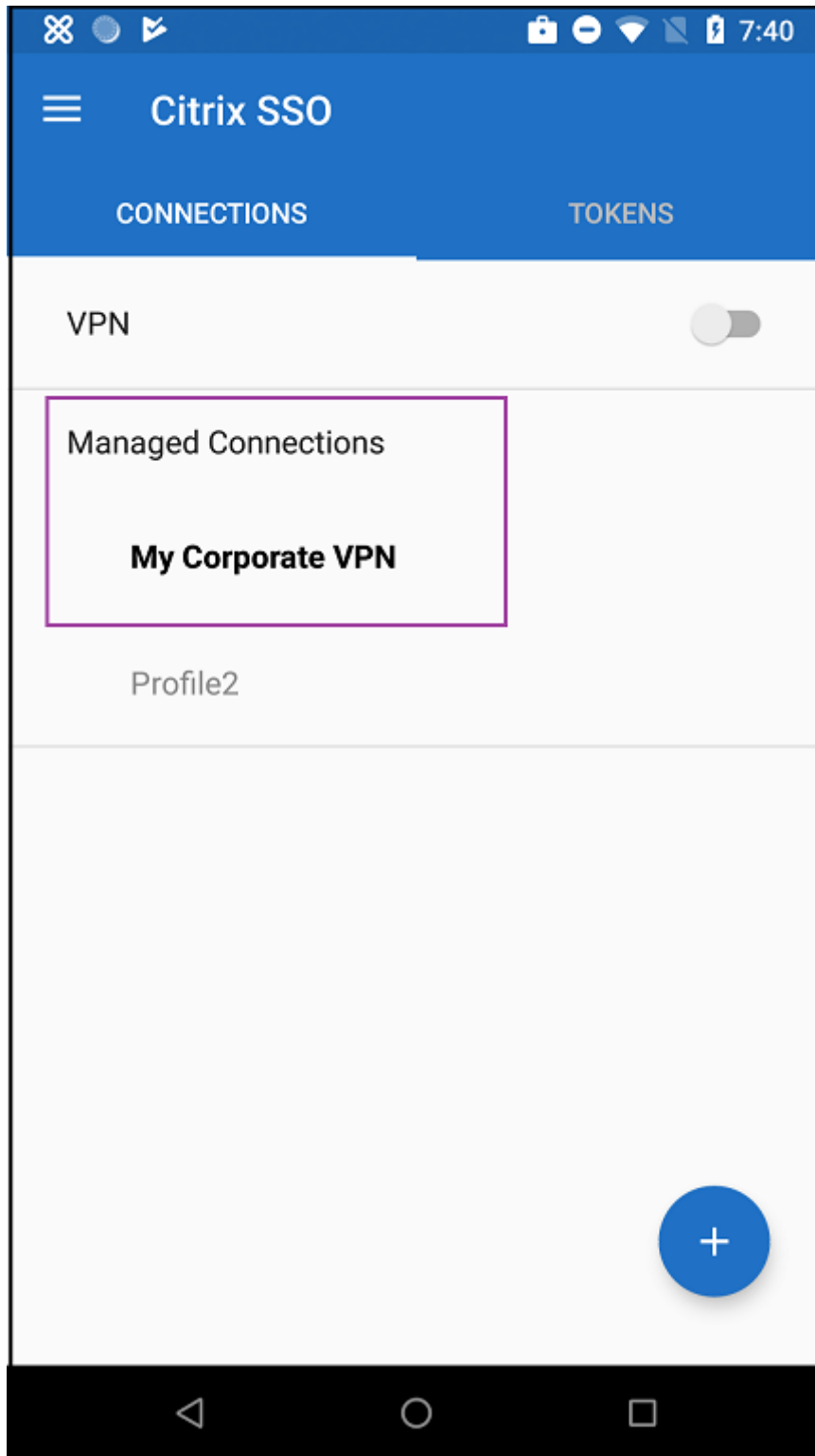
참고:

Android Enterprise 의 항상 VPN 연결에는 Citrix Secure Hub 19.5.5 이상이 필요합니다.

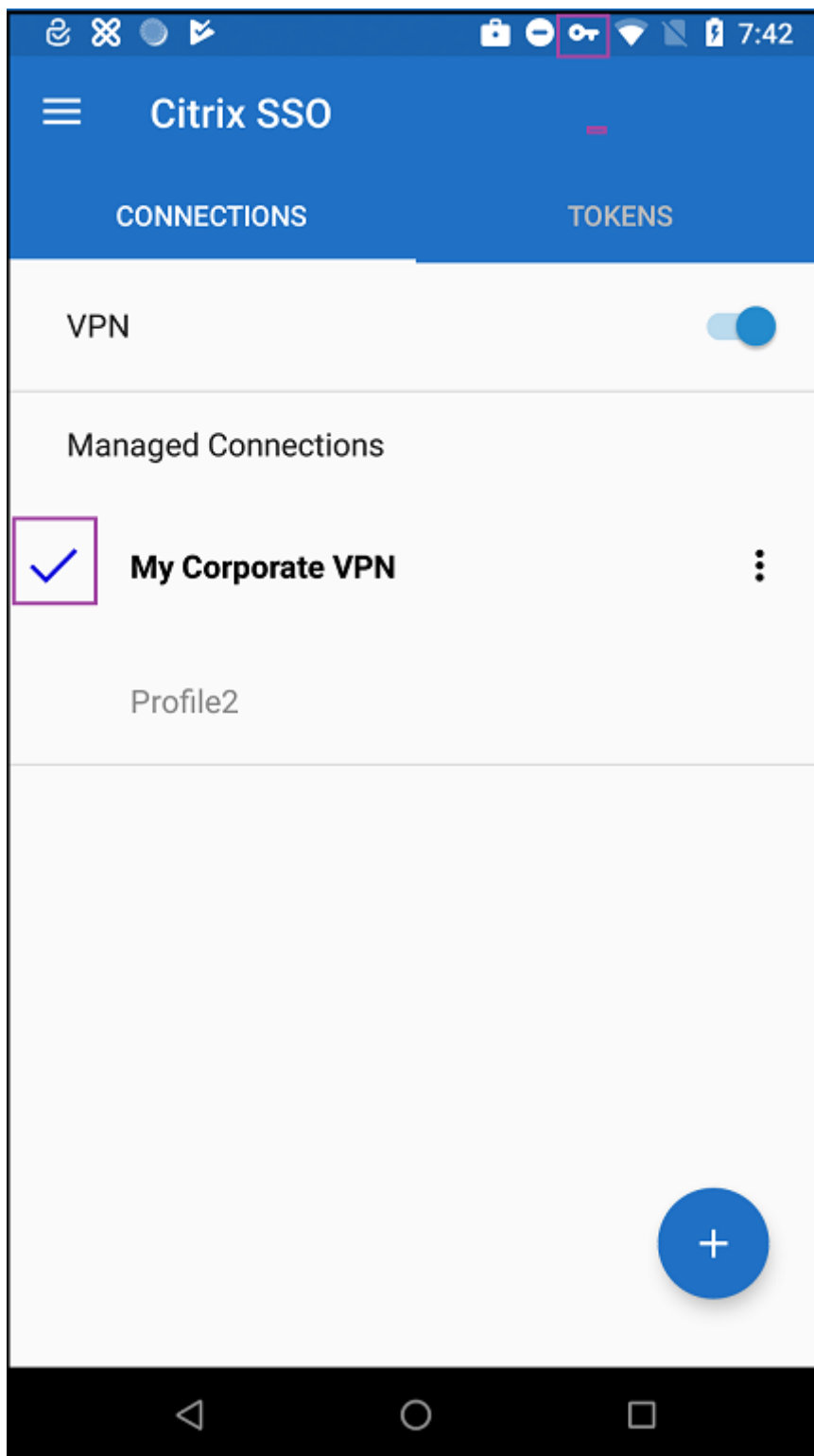
장치에서 **VPN** 프로필에 액세스

만든 VPN 프로필에 액세스하려면 Android Enterprise 사용자가 Google Play Store 에서 Citrix SSO 를 설치해야 합니다.

구성한 VPN 프로필은 앱의 **Managed Connections**(관리되는 연결) 영역에 나타납니다. 사용자는 VPN 프로필을 사용하여 연결하려는 VPN 프로필을 누릅니다.



사용자가 인증되고 연결되면 VPN 프로필 옆에 확인 표시가 나타납니다. 열쇠 아이콘은 VPN 이 연결되어 있음을 나타냅니다.



Zebra OEMConfig를 사용하여 **Zebra Android** 장치 관리

Zebra Technologies OEMConfig 관리 도구를 사용하여 Zebra Android 장치를 관리할 수 있습니다. Zebra OEMConfig 앱에 대한 자세한 내용은 [Zebra Technologies 웹사이트](#)를 참조하십시오.

XenMobile은 Zebra OEMConfig 버전 9.2 이상을 지원합니다. 장치에 Zebra OEMConfig를 설치하기 위한 시스템 요구 사항에 대한 자세한 내용은 Zebra Technologies 웹 사이트에서 [OEMConfig 설정](#)을 참조하십시오.

먼저 Zebra OEMConfig 앱을 Google Play Store 앱으로 XenMobile 콘솔에 추가합니다. [공개 앱 스토어 앱 추가](#)를 참조하십시오.

Zebra OEMConfig 앱에 대한 **Android Enterprise** 관리되는 구성 만들기

Zebra OEMConfig 앱에 대한 관리되는 구성 장치 정책을 구성합니다. 이 정책은 Zebra OEMConfig 앱이 설치되고 정책이 배포된 Zebra 장치에 적용됩니다.

1. XenMobile 콘솔에서 구성 > 장치 정책을 클릭합니다. 추가를 클릭합니다.
2. **Android Enterprise**를 선택합니다. 관리되는 구성을 클릭합니다.
3. 응용 프로그램 ID 선택 창이 나타나면 목록에서 **ZebraOEMConfig powered by MX(MX 기반 ZebraOEM-Config)**를 선택하고 확인을 클릭합니다.
4. Zebra OEMConfig 구성의 이름과 설명을 입력합니다. 다음을 클릭합니다.
5. Zebra OEMConfig 구성의 이름을 입력합니다.
6. 사용 가능한 매개 변수를 구성합니다. 예:
 - 장치 전면의 카메라를 사용하지 않으려면 **Camera Configuration(카메라 구성)**을 선택하고 **Use of Front Camera(전면 카메라 사용)**를 **Off(꺼짐)**로 설정합니다.
 - 장치 시간 형식을 변경하려면 **Clock Configuration(시계 구성)**을 선택하고 **Time Format(시간 형식)**을 **12(12 시간 형식)** 또는 **24(24 시간 형식)**로 설정합니다.

사용 가능한 모든 구성의 목록 및 설명은 Zebra Technologies 웹 사이트에서 [Zebra 관리 구성](#)을 참조하십시오.

1. 필요한 경우 Zebra OEMConfig 구성을 추가로 만들 수 있습니다. 구성 목록에서 추가를 클릭합니다. 새 구성이 목록에 나타납니다. 새 구성을 선택하고 매개 변수를 구성합니다.
2. 원하는 Zebra OEMConfig 구성을 모두 만들었으면 다음을 클릭합니다.
3. Zebra OEMConfig의 이 관리되는 구성에 대한 배포 규칙을 구성합니다.
4. 저장을 클릭합니다.

관리되는 도메인 장치 정책

January 5, 2022

전자 메일 및 Safari 브라우저에 적용되는 관리되는 도메인을 정의할 수 있습니다. 관리되는 도메인을 사용하면 Safari 를 사용하여 도메인에서 다운로드한 문서를 열 수 있는 앱을 제어함으로써 회사 데이터를 보호할 수 있습니다.

iOS 8 이상의 감독되는 장치의 경우 URL 또는 하위 도메인을 지정하여 사용자가 브라우저에서 문서, 첨부 파일 및 다운로드를 열 수 있는 방법을 제어할 수 있습니다. iOS 9.3 이상의 감독되는 장치의 경우 사용자가 Safari 에서 암호를 저장할 수 있는 URL 을 지정할 수 있습니다.

iOS 장치를 감독 모드로 설정하는 단계는 [Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 전환](#)을 참조하십시오.

사용자가 관리되는 전자 메일 도메인 목록에 없는 도메인의 받는 사람에게 전자 메일을 보낼 경우 사용자 장치에서 회사 도메인 외부의 사람에게 메시지를 보낸다는 경고가 표시됩니다.

문서, 첨부 파일 또는 다운로드 등의 항목: 사용자가 관리되는 웹 도메인 목록에 있는 웹 도메인에서 Safari 를 사용하여 항목을 열면 관련 회사 앱에서 항목이 열립니다. 해당 항목이 관리되는 웹 도메인 목록의 웹 도메인에 없는 경우 사용자가 회사 앱으로 항목을 열 수 없고 관리되지 않는 개인 앱을 사용해야 합니다.

감독되는 장치의 경우 Safari 암호 자동 채우기 도메인을 지정하지 않더라도 장치가 임시 다중 사용자로 구성된 경우 사용자가 암호를 저장할 수 없습니다. 그러나 임시 다중 사용자로 구성되지 않은 장치에서는 사용자가 모든 암호를 저장할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

도메인을 지정하려면:

형식	설명
<code>example.com</code>	<code>site.example.com/</code> 을 제외하고, <code>example.com</code> 아래의 모든 경로를 관리되는 경로로 처리
<code>foo.example.com</code>	<code>example.com/</code> 또는 <code>bar.example.com/</code> 을 제외하고, <code>foo.example.com</code> 아래의 모든 경로
<code>*.example.com</code>	<code>example.com/</code> 을 제외하고, <code>foo.example.com</code> 또는 <code>bar.example.com</code> 아래의 모든 경로
<code>example.com/sub</code>	<code>example.com/</code> 을 제외하고, <code>example.com/sub</code> 와 그 아래 모든 경로를 관리되는 경로로 처리
<code>foo.example.com/sub</code>	<code>example.com</code> , <code>example.com/sub</code> , <code>foo.example.com/</code> 또는 <code>bar.example.com</code> 의 모든 경로
<code>*.example.com/sub</code>	<code>example.com</code> 또는 <code>foo.example.com/</code> 을 제외하고, <code>foo.example.com/sub</code> 의 모든 경로

규칙:

- 도메인 비교 시 URL 의 선행 “www” 와 후행 슬래시는 무시됩니다.

- 포트 번호가 포함된 항목의 경우 해당 포트 번호를 지정하는 주소만 관리되는 주소로 간주됩니다. 그 외 항목의 경우 표준 포트 (http 의 경우 포트 80, https 의 경우 포트 443) 만 관리되는 것으로 간주됩니다. 예를 들어 *.example.com:8080 패턴은 <https://site.example.com:8080/page.html>과 일치하지만 <https://site.example.com/page.html>과는 일치하지 않는 한편, *.example.com 패턴은 <https://site.example.com/page.html> 및 <https://site.example.com/page.html>과 일치하지만 <https://site.example.com:8080/page.html>과는 일치하지 않습니다.
- 관리되는 Safari 웹 도메인 정의는 누적됩니다. 관리되는 Safari 웹 도메인 페이로드에 의해 정의되는 패턴은 모두 URL 요청과 일치시키는 데 사용됩니다.

설정:

- 관리되는 도메인
 - 표시되지 않은 전자 메일 도메인: 목록에 포함하려는 각 전자 메일 도메인에 대해 추가를 클릭한 후 다음을 수행합니다.
 - * 관리되는 전자 메일 도메인: 전자 메일 도메인을 입력합니다.
 - * 전자 메일 도메인을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.
 - 관리되는 **Safari** 웹 도메인: 목록에 포함하려는 각 웹 도메인에 대해 추가를 클릭한 후 다음을 수행합니다.
 - * 관리되는 웹 도메인: 웹 도메인을 입력합니다.
 - * 웹 도메인을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.
 - **Safari** 암호 자동 채우기 도메인: 목록에 포함하려는 각 자동 채우기 도메인에 대해 추가를 클릭한 후 다음을 수행합니다.
 - * **Safari** 암호 자동 채우기 도메인: 자동 채우기 도메인을 입력합니다.
 - * 자동 채우기 도메인을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

MDM 옵션 장치 정책

January 5, 2022

감독되는 iOS 7.0 이상의 전화 장치에서 내 전화 찾기 및 iPad 활성화 잠금을 관리하는 장치 정책을 XenMobile 에서 만들 수 있습니다. iOS 장치를 감독 모드로 설정하는 단계는 [Apple Configurator](#) 를 사용하여 **iOS 장치를 감독 모드로 전환**을 참조하십시오.

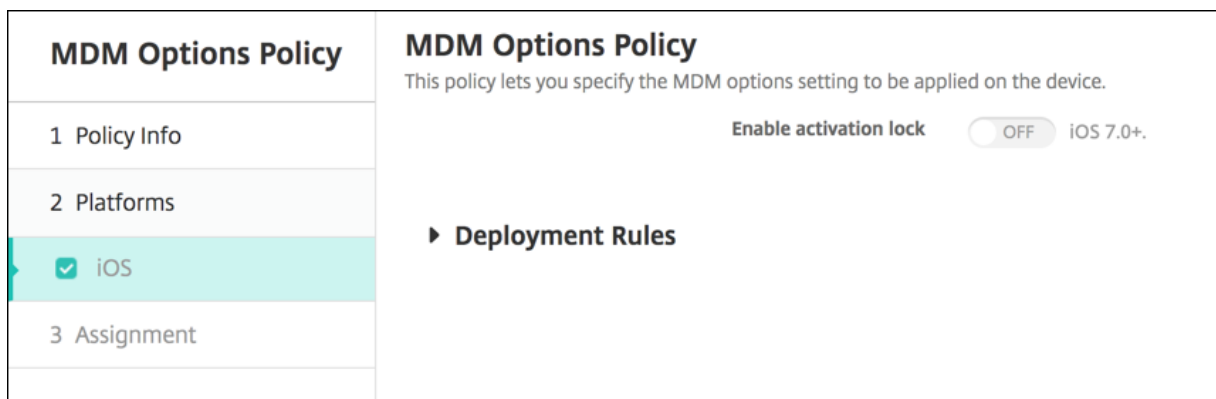
활성화 잠금은 분실되거나 도난당한 장치의 재활성화를 방지하는 내 iPhone/iPad 찾기 기능입니다. 활성화 잠금은 누군가가 내 iPhone/iPad 찾기를 끄고 장치를 지우거나 장치를 재활성화하여 사용하려고 할 경우 사용자의 Apple ID 와 암호를 요구합니다. 조직이 소유한 장치의 경우 예를 들어 장치를 재설정하거나 재활당하기 위해 활성화 잠금을 바이패스해야 합니다.

활성화 잠금을 사용하도록 설정하려면 XenMobile MDM 옵션 장치 정책을 구성하고 배포합니다. 그러면 사용자의 Apple 자격 증명 없이도 XenMobile 콘솔에서 장치를 관리할 수 있습니다. 활성화 잠금의 Apple 자격 증명 요구 사항을 바이패스하려면 XenMobile 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행합니다.

예를 들어 사용자가 분실된 휴대폰을 반환하거나 전체 초기화 전후에 장치를 설정하는 경우 iTunes 계정 자격 증명을 묻는 메시지가 표시될 때 XenMobile 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행하여 이 단계를 바이패스할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정



- **활성화 잠금 사용:** 이 정책을 배포할 장치에서 활성화 잠금을 사용 것인지를 선택합니다. 기본값은 꺼짐입니다.

MDM 옵션 장치 정책을 배포하여 활성화 잠금을 사용하도록 설정하면 관리 > 장치 페이지에서 해당 장치를 선택하고 보안을 클릭할 때 보안 동작 활성화 잠금 바이패스가 표시됩니다. 활성화 잠금 바이패스를 사용하면 장치 사용자의 Apple ID 및 암호를 몰라도 장치 활성화 전에 감독되는 장치에서 활성화 잠금을 해제할 수 있습니다. 전체 초기화 전후에 활성화 잠금 바이패스를 장치에 전송할 수 있습니다. 자세한 내용은 보안 동작 문서에서 [iOS 활성화 잠금 바이패스](#)를 참조하십시오.

조직 정보 장치 정책

January 5, 2022

XenMobile 에서 iOS 장치에 푸시되는 알림 메시지에 대한 조직 정보를 지정하는 장치 정책을 XenMobile 에서 추가할 수 있습니다. iOS 7 이상의 장치에서 이 정책을 사용할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

ios 설정

- 이름: XenMobile 을 실행하는 조직의 이름을 입력합니다.
- 주소: 조직의 주소를 입력합니다.
- 전화: 조직의 지원 전화 번호를 입력합니다.
- 전자 메일: 지원 전자 메일 주소를 입력합니다.
- 매직: 조직에서 관리하는 서비스를 설명하는 단어 나 구절을 입력합니다.

암호 장치 정책

March 15, 2024

조직의 표준에 따라 XenMobile 에서 암호 정책을 만듭니다. 사용자의 장치에 암호를 요구할 수 있으며 다양한 형식 및 암호 규칙을 설정할 수 있습니다. iOS, macOS, Android, Samsung KNOX, Android Enterprise 및 Windows Desktop/Tablet 에 대한 정책을 만들 수 있습니다. 각 플랫폼마다 이 문서에서 설명되어 있는 서로 다른 값 집합이 필요합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

ios 설정

Passcode Policy	Passcode Policy This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
1 Policy Info	
2 Platforms	
<input checked="" type="checkbox"/> iOS	Passcode requirements
<input checked="" type="checkbox"/> macOS	Passcode required <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Android	Minimum length 6
<input checked="" type="checkbox"/> Samsung KNOX	Allow simple passcodes <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Android for Work	Required characters <input type="checkbox"/>
<input checked="" type="checkbox"/> Windows Phone	Minimum number of symbols 0
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Passcode security
3 Assignment	Device lock grace period (minutes of inactivity) None
	Lock device after (minutes of inactivity) (0-999) None
	Passcode expiration in days (1-730) 0
	Previous passcodes saved (0-50) 0

- 암호 필요: 암호를 요구하고 iOS 암호 장치 정책의 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안 및 정책 설정에 대한 설정을 구성할 수 있게 됩니다.
- 암호 요구 사항
 - 최소 길이: 목록에서 최소 암호 길이를 클릭합니다. 기본값은 6 입니다.

- **단순 암호 허용:** 단순 암호를 허용할지 여부를 선택합니다. 단순 암호는 반복적 또는 순차적 문자 집합입니다. 기본값은 켜짐입니다.
- **필수 문자:** 암호에 적어도 문자가 하나 있어야 하는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **최소 기호 개수:** 목록에서 암호에 포함되어야 하는 기호의 수를 클릭합니다. 기본값은 **0** 입니다.

- 암호 보안

- **장치 잠금 유예 기간 (비활성 시간 (분)):** 목록에서 잠긴 장치의 잠금을 해제하려는 사용자가 암호를 입력해야 하는 기간을 클릭합니다. 기본값은 없음입니다.
- **다음의 비활성 시간 (분) 이후 장치 잠금:** 목록에서 장치가 잠기지 않고 비활성 상태를 유지할 수 있는 기간을 클릭합니다. 기본값은 없음입니다.
- **암호 만료 (일)(1-730):** 암호가 만료되기 전까지 남은 일 수를 입력합니다. 유효한 값은 1 부터 730 까지입니다. 기본값은 **0** 이며, 암호가 만료되지 않는다는 의미입니다.
- **이전 암호 저장 (0-50):** 저장할 이전 암호 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0 부터 50 까지입니다. 기본값은 **0** 이며, 사용자가 암호를 재사용할 수 있다는 의미입니다.
- **최대 로그인 시도 실패 횟수:** 목록에서 사용자가 로그인에 실패할 수 있는 횟수를 클릭합니다. 이 횟수를 넘으면 장치가 전체 초기화됩니다. 기본값은 정의되지 않음입니다.

macOS 설정

Passcode Policy	Passcode Policy
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	<div>Passcode required <input type="checkbox"/></div> <div>Passcode security</div> <div>Delay after failed sign-on attempts, in minutes <input type="text"/></div> <div>Policy Settings</div> <div>Profile scope <input type="text" value="User"/> macOS 10.7+</div> <div>► Deployment Rules</div>
<input type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
<input checked="" type="checkbox"/> Android	
<input checked="" type="checkbox"/> Samsung KNOX	
<input checked="" type="checkbox"/> Android for Work	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- **암호 필요:** 암호를 요구하고 iOS 암호 장치 정책의 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안 및 정책 설정에 대한 설정을 구성할 수 있게 됩니다.
- **암호 필요를 사용하지 않으려면** 로그인 시도에 실패한 후 지연 시간 (분) 옆에 사용자가 암호를 다시 입력할 수 있게 될 때까지 대기하는 시간 (분) 을 입력합니다.
- 암호 필요를 사용하도록 설정한 경우 다음 설정을 구성합니다.
- **암호 요구 사항**
 - **최소 길이:** 목록에서 최소 암호 길이를 클릭합니다. 기본값은 **6** 입니다.

- 단순 암호 허용: 단순 암호를 허용할지 여부를 선택합니다. 단순 암호는 반복적 또는 순차적 문자 집합입니다. 기본값은 켜짐입니다.
- 필수 문자: 암호에 적어도 문자가 하나 있어야 하는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 최소 기호 개수: 목록에서 암호에 포함되어야 하는 기호의 수를 클릭합니다. 기본값은 0 입니다.

• 암호 보안

- 장치 잠금 유예 기간 (비활성 시간 (분)): 목록에서 잠긴 장치의 잠금을 해제하려는 사용자가 암호를 입력해야 하는 기간을 클릭합니다. 기본값은 없음입니다.
- 다음의 비활성 시간 (분) 이후 장치 잠금: 목록에서 장치가 잠기지 않고 비활성 상태를 유지할 수 있는 기간을 클릭합니다. 기본값은 없음입니다.
- 암호 만료 (일)(1-730): 암호가 만료되기 전까지 남은 일 수를 입력합니다. 유효한 값은 1 부터 730 까지입니다. 기본값은 0 이며, 암호가 만료되지 않는다는 의미입니다.
- 이전 암호 저장 (0-50): 저장할 이전 암호 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0 부터 50 까지입니다. 기본값은 0 이며, 사용자가 암호를 재사용할 수 있다는 의미입니다.
- 최대 로그인 시도 실패 횟수: 목록에서 사용자가 로그인에 실패할 수 있는 횟수를 클릭합니다. 이 횟수를 넘으면 장치가 잠깁니다. 기본값은 정의되지 않음입니다.
- 로그인 시도에 실패한 후 지연 시간 (분): 사용자가 암호를 다시 입력할 수 있게 될 때까지 대기하는 시간 (분) 을 입력합니다.
- **Force passcode reset**(암호 재설정 강제 적용): 사용자는 다음에 인증할 때 암호를 재설정해야 합니다.

• 정책 설정

- 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Android 설정

Passcode Policy	Passcode Policy
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	<div>Passcode Required <input type="checkbox"/></div> <div>Encryption <input type="checkbox"/></div> <div>Enable encryption <input type="checkbox"/> A 3.0+</div> <div>Samsung SAFE <input type="checkbox"/></div> <div>Use same passcode across all users <input type="checkbox"/></div>
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
<input checked="" type="checkbox"/> Android	
<input checked="" type="checkbox"/> Samsung KNOX	
<input checked="" type="checkbox"/> Android for Work	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	<div>► Deployment Rules</div>

참고:

Android의 기본 설정은 꺼짐입니다.

- **암호 필요:** 암호를 요구하고 Android 암호 장치 정책의 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안, 암호화 및 Samsung SAFE에 대한 설정을 구성할 수 있게 됩니다.
- **암호 요구 사항**
 - **최소 길이:** 목록에서 최소 암호 길이를 클릭합니다. 기본값은 6입니다.
 - **생체 인식:** 생체 인식을 사용할지 여부를 선택합니다. 이 옵션을 사용하도록 설정하면 필수 문자 필드가 숨겨집니다. 기본값은 꺼짐입니다.
 - **필수 문자:** 목록에서 제한 없음, 숫자와 문자 모두, 숫자만 또는 문자만을 클릭하여 암호가 구성되는 방식을 구성합니다. 기본값은 제한 없음입니다.
 - **고급 규칙:** 고급 암호 규칙을 적용할지 여부를 선택합니다. 이 옵션은 Android 3.0 이상에서 사용할 수 있습니다. 기본값은 꺼짐입니다.
 - **고급 규칙을 사용하도록 설정한 경우 다음과 같은 목록 각각에서 암호에 포함되어야 하는 각 문자 유형의 최소 수를 클릭합니다.**
 - ★ **기호:** 기호의 최소 수입니다.
 - ★ **문자:** 문자의 최소 수입니다.
 - ★ **소문자:** 소문자의 최소 수입니다.
 - ★ **대문자:** 대문자의 최소 수입니다.
 - ★ **숫자 또는 기호:** 숫자 또는 기호의 최소 수입니다.
 - ★ **숫자:** 숫자의 최소 수입니다.
- **암호 보안**
 - **다음의 비활성 시간 (분) 이후 장치 잠금:** 목록에서 장치가 잠기지 않고 비활성 상태를 유지할 수 있는 기간을 클릭합니다. 기본값은 없음입니다.
 - **암호 만료 (일)(1-730):** 암호가 만료되기 전까지 남은 일 수를 입력합니다. 유효한 값은 1부터 730까지입니다. 기본값은 0이며, 암호가 만료되지 않는다는 의미입니다.
 - **이전 암호 저장 (0-50):** 저장할 이전 암호 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0부터 50까지입니다. 기본값은 0이며, 사용자가 암호를 재사용할 수 있다는 의미입니다.
 - **최대 로그인 시도 실패 횟수:** 목록에서 사용자가 로그인에 실패할 수 있는 횟수를 클릭합니다. 이 횟수를 넘으면 장치가 초기화됩니다. 기본값은 정의되지 않음입니다.
- **암호화**
 - **암호화 사용:** 암호화를 사용하도록 설정하지 여부를 선택합니다. 이 옵션은 Android 3.0 이상에서 사용할 수 있습니다. 이 옵션은 암호 필요 설정과 관계없이 사용할 수 있습니다.

장치를 암호화하려면 충전된 배터리로 시작하고 암호화가 실행되는 수 시간 동안 장치를 켜둔 상태로 유지해야 합니다. 암호화 프로세스가 중단되면 장치의 데이터 중 일부 또는 전부가 손실될 수 있습니다. 장치를 암호화한 후에는 프로세스를 되돌릴 수 없으며, 암호화를 취소하는 유일한 방법은 장치의 모든 데이터를 지우고 공장 기본값으로 재설정하는 것입니다.

• Samsung SAFE

참고:

Samsung SAFE 장치에서 얼굴 또는 홍채 인식을 사용하지 않도록 설정한 경우 해결 방법: Samsung SAFE 용 제한 장치 정책을 만듭니다. 제한 정책에서 응용 프로그램 사용 안 함을 켜고 테이블에 `com.samsung.android.bio.face.service` 또는 `com.samsung.android.server.iris`를 추가합니다. 그런 다음 제한 정책을 배포합니다.

- 모든 사용자가 동일한 암호 사용: 모든 사용자에게 동일한 암호를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 설정은 Samsung SAFE 장치에만 적용되며 암호 필요 설정과 관계없이 사용할 수 있습니다.
- 모든 사용자가 동일한 암호 사용을 사용하도록 설정한 경우 암호 필드에 모든 사용자가 사용할 암호를 입력합니다.
- 암호 필요를 사용하도록 설정한 경우 다음과 같은 Samsung SAFE 설정을 구성합니다.
 - * 변경된 문자: 사용자가 이전 암호에서 변경해야 하는 문자 수를 입력합니다. 기본값은 0입니다.
 - * 한 문자의 최대 사용 횟수: 한 문자가 암호에서 발생할 수 있는 최대 횟수를 입력합니다. 기본값은 0입니다.
 - * 연속 영문자 길이: 암호에서 연속될 수 있는 영문자의 최대 길이를 입력합니다. 기본값은 0입니다.
 - * 연속 숫자 길이: 암호에서 연속될 수 있는 숫자의 최대 길이를 입력합니다. 기본값은 0입니다.
 - * 사용자에게 암호 표시 허용: 사용자가 암호를 볼 수 있는지 여부를 선택합니다. 기본값은 켜짐입니다.
 - * 생체 인증 구성. 생체 인증을 사용하도록 설정할지 여부를 선택합니다. 기본값은 꺼짐입니다. 켜짐으로 설정하는 경우 다음과 같은 옵션을 설정할 수 있습니다.
 - 지문 허용. 사용자가 지문을 사용하여 인증할 수 있도록 하려면 이 옵션을 선택합니다.
 - 홍채 허용. 사용자가 홍채를 사용하여 인증할 수 있도록 하려면 이 옵션을 선택합니다.
 - * 금지된 문자열: 금지된 문자열을 만들어 사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등과 같이 쉽게 추측할 수 있는 안전하지 않은 문자열을 사용하지 못하게 합니다. 거부하려는 각 문자열에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 금지된 문자열: 사용자가 사용할 수 없는 문자열을 입력합니다.
 - 저장을 클릭하여 문자열을 추가하거나 취소를 클릭하여 문자열 추가를 취소합니다.

Android Enterprise 설정

Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock. Note: When devices running Samsung Knox 3.0 are enrolled in work profile mode, device passcode settings for Knox 3.0 and later do not apply to the device passcode, even if you configure them. The descriptions of these settings tell you which ones these are.

Device passcode required ☒ ON

Show apps and shortcuts while passcode is not in compliance ☐ OFF ⓘ

Passcode requirements for device passcode

Minimum length 6

Allow users to make password visible (Knox 3.0+) ☐ OFF ⓘ

Biometric recognition ☐ OFF

Required characters Numbers only

Forbidden Strings (Knox 3.0+) ⓘ

Back Next >

Android Enterprise 장치의 경우 장치의 암호 또는 Android Enterprise 작업 프로파일의 보안 챌린지를 요구하거나 둘 다를 요구할 수 있습니다.

Android 9.0 이상 및 Samsung Knox 3.0 이상을 실행하는 장치의 경우 **Android Enterprise** 페이지에서 Samsung Knox 에 대한 설정을 구성합니다. 이전 버전의 Android 또는 Samsung Knox 를 실행하는 장치의 경우 **Samsung Knox** 페이지를 사용합니다.

참고:

Samsung Knox 3.0 을 실행하는 장치를 작업 프로파일 장치로 등록한 경우 Knox 3.0 이상에 대한 장치 암호 설정은 구성된 경우라 하더라도 장치 암호에 적용되지 않습니다.

- **장치 암호 필요:** 장치에 암호가 필요합니다. 이 설정이 켜짐인 경우 장치 암호의 암호 요구 사항 및 장치 암호의 암호 보안에서 설정을 구성합니다. 기본값은 꺼짐입니다.
- **암호가 규정을 준수하지 않는 경우 앱 및 바로 가기 표시:** 이 설정이 켜짐이면 암호가 규정을 준수하지 않더라도 장치의 앱과 바로 가기가 숨겨지지 않습니다. 이 설정이 꺼짐이면 암호가 규정을 준수하지 않는 경우 앱과 바로 가기가 숨겨집니다. 이 설정을 사용하면 Citrix 에서는 암호가 규정을 준수하지 않는 경우 규정을 준수하지 않는 장치로 표시하도록 자동화된 작업을 만드는 것을 권장합니다. 기본값은 꺼짐입니다.
- **장치 암호의 암호 요구 사항:**
 - **최소 길이:** 최소 암호 길이를 지정합니다. 기본값은 6 입니다.
 - **사용자에게 암호 표시 허용:** 올바른 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로파일 장치로 등록된 장치에는 적용되지 않습니다. 사용자가 암호를 표시할 수 있습니다. 기본값은 꺼짐입니다.
 - **생체 인식:** 생체 인식을 사용하도록 설정합니다. 이 설정이 켜짐인 경우 필수 문자 필드가 숨겨집니다. 기본값은 꺼짐입니다.
 - **필수 문자:** 암호에 필요한 문자의 유형을 지정합니다. 목록에서 제한 없음, 숫자와 문자 모두, 숫자만 또는 문자만을 선택합니다. 제한 없음은 Android 7.0 을 실행하는 장치에만 사용합니다. Android 7.1 이상은 제한 없음 설정

정을 따르지 않습니다. 기본값은 숫자와 문자 모두입니다.

- **금지된 문자열:** 올바른 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로파일 장치로 등록된 장치에는 적용되지 않습니다. 사용자가 암호로 사용할 수 없는 문자열을 지정합니다. 금지된 문자열을 만들어 사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등과 같이 쉽게 추측할 수 있는 안전하지 않은 문자열을 사용하지 못하게 합니다. 거부할 각 문자열에 대해 추가를 클릭하고 사용 금지하려는 문자열을 입력한 다음 저장을 클릭하여 문자열을 추가하거나 취소를 클릭하여 문자열 추가를 취소합니다.
- **고급 규칙:** 암호에서 발생할 수 있는 문자 유형에 대해 고급 규칙을 적용합니다. 이 설정이 켜짐인 경우 최소 개수 및 최대 개수에서 설정을 구성합니다. Android 5.0 이전의 Android 장치에서는 이 설정을 사용할 수 없습니다. 기본값은 꺼짐입니다.
- **최소 개수:**
 - * **기호:** 기호의 최소 수를 지정합니다. 기본값은 **0** 입니다.
 - * **문자:** 문자의 최소 수를 지정합니다. 기본값은 **0** 입니다.
 - * **소문자:** 소문자의 최소 수를 지정합니다. 기본값은 **0** 입니다.
 - * **대문자:** 대문자의 최소 수를 지정합니다. 기본값은 **0** 입니다.
 - * **숫자 또는 기호:** 숫자 또는 기호의 최소 수를 지정합니다. 기본값은 **0** 입니다.
 - * **숫자:** 숫자의 최소 수를 지정합니다. 기본값은 **0** 입니다.
 - * **변경된 문자:** 올바른 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로파일 장치로 등록된 장치에는 적용되지 않습니다. 사용자가 이전 암호에서 변경해야 하는 문자 수를 지정합니다. 기본값은 **0** 입니다.
- **최대 개수:** 올바른 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로파일 장치로 등록된 장치에는 적용되지 않습니다.
 - * **한 문자의 최대 사용 횟수:** 한 문자가 암호에서 발생할 수 있는 최대 횟수를 지정합니다. 기본값은 **0** 이며 최대 제한이 없음을 의미합니다.
 - * **연속 영문자 길이:** 암호에서 연속될 수 있는 영문자의 최대 길이를 지정합니다. 기본값은 **0** 이며 최대 제한이 없음을 의미합니다.
 - * **연속 숫자 길이:** 암호에서 연속될 수 있는 숫자의 최대 길이를 지정합니다. 기본값은 **0** 이며 최대 제한이 없음을 의미합니다.

• **장치 암호의 암호 보안:**

- **다음 로그인 시도 실패 후 장치 초기화:** 사용자가 로그인에 실패할 수 있는 횟수를 지정합니다. 이 횟수를 넘으면 장치가 전체 초기화됩니다. 기본값은 정의되지 않음입니다.
- **다음의 비활성 시간 (분) 이후 장치 잠금 (0-999):** 장치가 잠기지 않고 비활성 상태를 유지할 수 있는 시간 (분) 을 지정합니다. 기본값은 없음입니다.
- **암호 만료 (일)(1-730):** 암호가 만료되기 전까지 남은 일 수를 지정합니다. 유효한 값은 1 부터 730 까지입니다. 기본값은 **0** 이며, 암호가 만료되지 않는다는 의미입니다.
- **이전 암호 저장 (0-50):** 저장할 이전 암호 수를 지정합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0 부터 50 까지입니다. 기본값은 **0** 이며, 사용자가 암호를 재사용할 수 있다는 의미입니다.
- **다음 로그인 시도 실패 후 장치 잠금** 올바른 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로파일 장치로 등록된 장치에는 적용

되지 않습니다. 사용자가 로그인에 실패할 수 있는 횟수를 지정합니다. 그 후 장치가 잠깁니다. 기본값은 정의되지 않음입니다.

- **작업 프로필 보안 챌린지:** 사용자가 Android Enterprise 작업 프로필에서 실행되는 앱에 액세스할 때 보안 챌린지를 완료하도록 합니다. Android 7.0 이상을 실행하는 장치를 위한 설정입니다. 이 설정이 켜짐인 경우 작업 프로필 보안 과제에 대한 암호 요구 사항 및 작업 프로필 보안 과제에 대한 암호 보안에서 설정을 구성합니다. 기본값은 꺼짐입니다.
- **작업 프로필 보안 과제에 대한 암호 요구 사항:**
 - **최소 길이:** 최소 암호 길이를 지정합니다. 기본값은 6 입니다.
 - **사용자에게 암호 표시 허용:** 올바른 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 사용자가 암호를 표시할 수 있습니다. 기본값은 꺼짐입니다.
 - **생체 인식:** 생체 인식을 사용하도록 설정합니다. 이 설정이 켜짐인 경우 필수 문자 필드가 숨겨집니다. 기본값은 꺼짐입니다.
 - **필수 문자:** 암호에 필요한 문자의 유형을 지정합니다. 목록에서 제한 없음, 숫자와 문자 모두, 숫자만 또는 문자만을 선택합니다. 제한 없음은 Android 7.0 을 실행하는 장치에만 사용합니다. Android 7.1 이상은 제한 없음 설정을 따르지 않습니다. 기본값은 숫자와 문자 모두입니다.
 - **금지된 문자열:** 올바른 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 사용자가 암호로 사용할 수 없는 문자열을 지정합니다. 금지된 문자열을 만들어 사용자가 “password” , “pwd” , “welcome” , “123456” , “111111” 등과 같이 쉽게 추측할 수 있는 안전하지 않은 문자열을 사용하지 못하게 합니다. 거부할 각 문자열에 대해 추가를 클릭하고 사용 금지하려는 문자열을 입력한 다음 저장을 클릭하여 문자열을 추가하거나 취소를 클릭하여 문자열 추가를 취소합니다.
 - **고급 규칙:** 암호에서 발생할 수 있는 문자 유형에 대해 고급 규칙을 적용합니다. 이 설정이 켜짐인 경우 최소 개수 및 최대 개수에서 설정을 구성합니다. Android 5.0 이전의 Android 장치에서는 이 설정을 사용할 수 없습니다. 기본값은 꺼짐입니다.
 - **최소 개수:**
 - * **기호:** 기호의 최소 수를 지정합니다. 기본값은 0 입니다.
 - * **문자:** 문자의 최소 수를 지정합니다. 기본값은 0 입니다.
 - * **소문자:** 소문자의 최소 수를 지정합니다. 기본값은 0 입니다.
 - * **대문자:** 대문자의 최소 수를 지정합니다. 기본값은 0 입니다.
 - * **숫자 또는 기호:** 숫자 또는 기호의 최소 수를 지정합니다. 기본값은 0 입니다.
 - * **숫자:** 숫자의 최소 수를 지정합니다. 기본값은 0 입니다.
 - * **변경된 문자:** 올바른 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 사용자가 이전 암호에서 변경해야 하는 문자 수를 지정합니다. 기본값은 0 입니다.
 - **최대 개수:** 올바른 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치를 위한 설정입니다.
 - * **한 문자의 최대 사용 횟수:** 한 문자가 암호에서 발생할 수 있는 최대 횟수를 지정합니다. 기본값은 0 이며 최대 제한이 없음을 의미합니다.
 - * **연속 영문자 길이:** 암호에서 연속될 수 있는 영문자의 최대 길이를 지정합니다. 기본값은 0 이며 최대 제한이 없음을 의미합니다.

★ 연속 숫자 길이: 암호에서 연속될 수 있는 숫자의 최대 길이를 지정합니다. 기본값은 **0**이며 최대 제한이 없음을 의미합니다.

- 통합 암호 사용: 꺼짐인 경우 사용자는 장치와 작업 프로필에 하나의 암호를 사용합니다. 꺼짐인 경우:

- ★ 사용자는 장치와 작업 프로필에 다른 암호를 사용해야 합니다.
- ★ 사용자가 장치와 작업 프로필에 하나의 암호를 사용하려고 설정한 장치의 한 번 잠금 사용 설정이 비활성화됩니다. 사용자가 활성화할 수 없습니다.
- ★ 작업 프로필 보안 인증 질문에 대한 암호 요건이 장치 암호보다 복잡한 경우: 한 번 잠금 사용 설정을 활성화한 사용자에게 작업 프로필 암호를 변경하라는 메시지가 표시됩니다.

기본값은 꺼짐입니다. Android 9.0 부터 사용할 수 있습니다.

• 작업 프로필 보안 과제에 대한 암호 보안

- 다음 로그인 시도 실패 후 컨테이너 초기화: 사용자가 로그인에 실패할 수 있는 횟수를 지정합니다. 이 횟수를 넘으면 장치에서 작업 프로필 및 해당 데이터가 초기화됩니다. 사용자는 초기화가 발생한 후 작업 프로필을 다시 초기화해야 합니다. 기본값은 정의되지 않음입니다.
- 다음 비활성 시간 (분) 이후 컨테이너 잠금: 작업 프로필이 잠기지 않고 장치가 비활성 상태를 유지할 수 있는 시간 (분) 을 지정합니다. 기본값은 없음입니다.
- 암호 만료 (일)(1-730): 암호가 만료되기 전까지 남은 일 수를 지정합니다. 유효한 값은 1 부터 730 까지입니다. 기본값은 **0**이며, 암호가 만료되지 않는다는 의미입니다.
- 이전 암호 저장 (0-50): 저장할 이전 암호 수를 지정합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0 부터 50 까지입니다. 기본값은 **0**이며, 사용자가 암호를 재사용할 수 있다는 의미입니다.
- 다음 로그인 시도 실패 후 컨테이너 잠금 올바른 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치를 위한 설정입니다. 사용자가 로그인에 실패할 수 있는 횟수를 지정합니다. 그 후 장치가 잠깁니다. 기본값은 정의되지 않음입니다.

Windows 데스크톱/태블릿 설정

Passcode Policy	Passcode Policy This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
1 Policy Info	Passcode required <input checked="" type="checkbox"/>
2 Platforms	Passcode security
<input type="checkbox"/> iOS	Lock device after (minutes of inactivity) (0-999) <input type="text" value="0"/>
<input type="checkbox"/> macOS	Passcode expiration in 0-730 days * <input type="text" value="0"/>
<input type="checkbox"/> Android	Previous passwords saved (0-24) <input type="text" value="0"/>
<input type="checkbox"/> Samsung KNOX	Passcode requirements
<input type="checkbox"/> Android for Work	Minimum length <input type="text" value="6"/>
<input type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	► Deployment Rules
3 Assignment	

- **간편 로그인 허용 안 함:** 사용자가 사진 암호 또는 생체 인식 로그인을 사용하여 장치에 액세스할 수 있도록 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **최소 암호 길이:** 목록에서 최소 암호 길이를 클릭합니다. 기본값은 **6**입니다.
- **초기화하기 전까지의 최대 암호 시도 횟수:** 목록에서 사용자가 로그인에 실패할 수 있는 횟수를 클릭합니다. 이 횟수를 넘으면 장치에서 데이터가 초기화됩니다. 기본값은 **4**입니다.
- **암호 만료 (일)(0-730):** 암호가 만료되기 전까지 남은 일 수를 입력합니다. 유효한 값은 0 부터 730 까지입니다. 기본값은 **0**이며, 암호가 만료되지 않는다는 의미입니다.
- **암호 기록 (1-24):** 저장할 이전 암호 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 1 부터 24 까지입니다. 이 필드에 1 에서 24 사이의 숫자를 입력해야 합니다. 기본값은 **0**입니다.
- **장치를 잠그기 전까지의 최대 비활성 시간 (분)(1-999):** 장치가 잠기지 않고 비활성 상태를 유지할 수 있는 기간 (분) 을 입력합니다. 유효한 값은 1 부터 999 까지입니다. 이 필드에 1 에서 999 사이의 숫자를 입력해야 합니다. 기본값은 **0**입니다.

개인 핫스팟 장치 정책

January 5, 2022

사용자가 WiFi 네트워크 범위 외부에 있을 때 iOS 장치의 개인 핫스팟 기능을 통해 셀룰러 데이터 연결을 사용하여 인터넷에 연결하도록 허용할 수 있습니다. iOS 7.0 이상에서 사용 가능합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- **개인 핫스팟 사용 안 함:** 사용자의 장치에서 개인 핫스팟 기능을 사용하지 않도록 설정할지 여부를 선택합니다. 기본값은 사용자의 장치에서 개인 핫스팟을 끄는 꺼짐입니다. 이 정책은 기능을 사용하지 않도록 설정하지 않습니다. 사용자는 여전히 자신의 장치에서 개인 핫스팟을 사용할 수 있지만 정책이 배포될 때 개인 핫스팟이 해제되어 기본적으로 켜져 있지 않습니다.

프로필 제거 장치 정책

January 5, 2022

XenMobile 에서 앱 프로필 제거 장치 정책을 만들 수 있습니다. 정책을 배포하면 사용자의 iOS 또는 macOS 장치에서 앱 프로필이 제거됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

Profile Removal Policy	Profile Removal Policy This policy lets you remove a profile for iOS or macOS from a device.
1 Policy Info	Profile ID * <input type="text" value="This field is mandatory."/>
2 Platforms	Comment <input type="text"/>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS	Deployment Rules
3 Assignment	

- **프로필 ID:** 목록에서 앱 프로필 ID 를 클릭합니다. 이것은 필수 필드입니다.
- **설명:** 선택적 설명을 입력합니다.

macOS 설정

Profile Removal Policy	Profile Removal Policy This policy lets you remove a profile for iOS or macOS from a device.
1 Policy Info	Profile ID * <input type="text" value="This field is mandatory."/>
2 Platforms	Deployment scope <input type="text" value="User"/> macOS 10.7+
<input type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS	Comment <input type="text"/>
3 Assignment	Deployment Rules

- **프로필 ID:** 목록에서 앱 프로필 ID 를 클릭합니다. 이것은 필수 필드입니다.
- **배포 범위:** 목록에서 사용자 또는 시스템을 클릭합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.
- **설명:** 선택적 설명을 입력합니다.

프로비전 프로필 장치 정책

January 5, 2022

iOS 엔터프라이즈 앱을 개발하고 코드 서명하는 경우 일반적으로 엔터프라이즈 배포 프로비전 프로필을 포함합니다. Apple iOS 장치에서 앱을 실행하려면 이 프로필이 필요합니다. 프로비전 프로필이 누락되었거나 만료된 경우 사용자가 앱을 눌러서 열 때 앱의 작동이 중단됩니다.

프로비전 프로파일의 주요 문제는 Apple Developer Portal 에서 생성된 후 1 년 지나면 만료된다는 것입니다. 따라서 사용자에게 의해 등록된 모든 iOS 장치에서 모든 프로비전 프로파일의 만료 날짜를 추적해야 합니다. 만료 날짜를 추적하는 작업에는 실제 만료 날짜뿐 아니라 어떤 사용자가 어떤 앱 버전을 사용하는지를 지속적으로 파악하는 것도 포함됩니다. 두 가지 해결 방법은 프로비전 프로파일 사용자에게 전자 메일로 보내거나 웹 포털에 게시해 다운로드하여 설치하도록 하는 것입니다. 이러한 해결 방법은 효과가 있지만 오류가 발생하기 쉽습니다. 사용자가 전자 메일의 지침에 대응하거나 웹 포털에서 올바른 프로파일 다운로드하여 설치해야 하기 때문입니다.

이 프로세스를 사용자에게 투명하게 진행하려면 XenMobile 에서 장치 정책을 사용하여 프로비전 프로파일 설치하거나 제거할 수 있습니다. 누락되었거나 만료된 프로파일은 필요에 따라 제거되고 최신 프로파일 사용자의 장치에 설치되므로 앱을 누르기만 하면 열어서 사용할 수 있습니다.

프로비전 프로파일 정책을 만들려면 먼저 프로비전 프로파일 파일을 만들어야 합니다. 자세한 내용은 [Apple Developer 사이트](#)에서 개발 프로비전 프로파일 만드는 방법에 대한 Apple 설명서를 참조하십시오.

iOS 설정

Provisioning Profile Policy	Policy Information This policy lets you upload an iOS provisioning profile.
1 Policy Info	Policy Name * <input type="text"/>
2 Platforms	Description <input type="text"/>
<input checked="" type="checkbox"/> iOS	
3 Assignment	

- **iOS** 프로비전 프로파일: 찾아보기를 클릭하고 파일 위치로 이동하여 가져올 프로비전 프로파일 파일을 선택합니다.

프로비전 프로파일 제거 장치 정책

January 5, 2022

장치 정책을 사용하여 iOS 프로비전 프로파일 제거할 수 있습니다. 프로비전 프로파일 대한 자세한 내용은 [프로비전 프로파일 장치 정책](#)을 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- **iOS** 프로비전 프로파일: 목록에서 제거할 프로비전 프로파일 클릭합니다.
- 설명: 필요한 경우 설명을 추가합니다.

프록시 장치 정책

August 12, 2022

XenMobile 에서 장치 정책을 추가하여 iOS 6.0 이상을 실행하는 장치에 대한 글로벌 HTTP 프록시 설정을 지정할 수 있습니다. 장치당 하나의 글로벌 HTTP 프록시 정책만 배포할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

사전 요구 사항

이 정책을 배포하기 전에 글로벌 HTTP 프록시를 설정할 모든 iOS 장치를 감독 모드로 설정해야 합니다. 자세한 내용은 [Apple Configurator](#)를 사용하여 iOS 장치를 감독 모드로 전환 또는 [Apple 배포 프로그램을 통해 장치 배포](#)를 참조하십시오.

장치로 프록시 정책을 보내기 전에 장치를 등록하기 위한 배포 규칙을 설정합니다.

iOS 설정

- **프록시 구성:** 사용자의 장치에서 프록시를 구성하는 방법에 대해 수동 또는 자동으로 클릭합니다.
 - 수동을 클릭하는 경우 다음 설정을 구성합니다.
 - * **프록시 서버의 호스트 이름 또는 IP 주소:** 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - * **프록시 서버용 포트:** 프록시 서버 포트 번호를 입력합니다. 이것은 필수 필드입니다.
 - * **사용자 이름:** 프록시 서버 인증에 사용할 선택적 사용자 이름을 입력합니다.
 - * **암호:** 프록시 서버 인증에 사용할 선택적 암호를 입력합니다.
 - 자동으로 클릭하는 경우 다음 설정을 구성합니다.
 - * **프록시 PAC URL:** 프록시 구성을 정의하는 PAC 파일의 URL 을 입력합니다.
 - * **PAC** 에 연결할 수 없는 경우 직접 연결 허용: PAC 파일에 연결할 수 없는 경우 대상에 직접 연결할 수 있도록 할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 7.0 이상에서만 사용할 수 있습니다.
- **중속 네트워크에 액세스하기 위한 프록시 바이패스 허용:** 중속 네트워크에 액세스하기 위한 프록시 바이패스를 허용할 것인지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **정책 설정**
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * **제거할 때까지의 기간 (시간):** 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

제한 장치 정책

March 15, 2024

제한 장치 정책은 사용자 장치에서 카메라와 같은 특정 기능을 허용하거나 제한합니다. 또한 보안 제한을 설정하고 미디어 콘텐츠에 대한 제한과 사용자가 설치할 수 있는 앱 유형 및 설치할 수 없는 앱 유형에 대한 제한을 설정할 수 있습니다. 대부분의 제한 설정은 기본적으로 켜짐 또는 허용입니다. 주요 예외 사항은 iOS 보안 - 시행 기능 및 모든 Windows 태블릿 기능입니다. 이러한 기능은 기본적으로 꺼짐 또는 제한으로 설정됩니다.

Windows 10 RS2 휴대폰: Internet Explorer 를 사용하지 않는 사용자 지정 XML 정책 또는 제한 정책을 휴대폰에 배포한 후 브라우저가 사용되는 상태로 유지됩니다. 이 문제를 해결하려면 휴대폰을 다시 시작하십시오. 이것은 타사 문제입니다.

팁:

켜짐을 선택한 모든 옵션은 사용자가 해당 작업을 수행하거나 기능을 사용할 수 있다는 의미입니다. 예:

카메라. 켜짐이면 사용자가 장치에서 카메라를 사용할 수 있습니다. 꺼짐이면 사용자가 장치에서 카메라를 사용할 수 없습니다.

스크린샷. 켜짐이면 사용자가 장치에서 스크린샷을 만들 수 있습니다. 꺼짐이면 사용자가 장치에서 스크린샷을 만들 수 없습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

Restrictions Policy	
1 Policy Info	Restrictions Policy This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install. Allow hardware controls
2 Platforms	<div> <input checked="" type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung KNOX <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Amazon <input type="checkbox"/> Windows Mobile/CE </div>
3 Assignment	<div> <div> <div>Camera</div> <div>ON</div> </div> <div> <div>Screen shots</div> <div>ON</div> </div> <div> <div>Photo streams</div> <div>ON</div> </div> <div> <div>Shared photo streams</div> <div>ON</div> </div> <div> <div>Voice dialing</div> <div>ON</div> </div> <div> <div>Siri</div> <div>ON</div> </div> <div> <div>Installing apps</div> <div>ON</div> </div> <div> <div>Allow global background fetch while roaming</div> <div>ON</div> </div> <div> <div>iTunes Store</div> <div>ON</div> </div> </div> <div> <div> <input checked="" type="checkbox"/> Allow the Classroom app to remotely observe student screens iOS 9.3+ <input type="checkbox"/> Allow the Classroom app to perform AirPlay and View Screen without prompting iOS 10.3+ </div> <div> <input checked="" type="checkbox"/> Allow while device is locked <input type="checkbox"/> Siri profanity filter </div> </div>

일부 iOS 제한 정책 설정은 여기와 XenMobile 콘솔 제한 정책 페이지에 설명된 대로 특정 버전의 iOS에만 적용됩니다.

iOS 제한 정책 설정은 장치가 사용자 등록 모드, 감독되지 않는 모드 (전체 MDM) 또는 감독 모드에서 등록된 경우 적용됩니다. 다음 표에는 iOS 13 이상에 대한 각 제한 정책 설정에 사용할 수 있는 등록 모드가 나와 있습니다.

표에 나와 있듯이 iOS 13 부터는 이전에 감독되지 않은 모드 및 감독 모드에서 사용할 수 있었던 일부 설정을 감독 모드에서만 사용할 수 있습니다. 다음 규칙이 적용됩니다.

- 감독되는 iOS 13 이상 장치를 XenMobile 에 등록하는 경우 설정이 장치에 적용됩니다.
- 감독되지 않는 iOS 13 이상 장치를 XenMobile 에 등록하는 경우 설정이 장치에 적용되지 않습니다.
- iOS 12 이하 장치가 이미 XenMobile 에 등록되었고 iOS 13 으로 업그레이드된 경우 변경 사항은 없습니다. 이 설정은 업그레이드 전과 마찬가지로 장치에 적용됩니다.

iOS 장치를 감독 모드로 설정하는 방법에 관한 정보는 [Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 전환](#)을 참조하십시오.

설정	사용자 등록	감독되지 않음	감독됨
하드웨어 제어 허용			
카메라	아니요	예	예
FaceTime	아니요	아니요 (iOS 13 의 새로운 기능)	예
스크린샷	예	아니요	예
교실 앱이 학생 화면을 원격으로 관찰할 수 있도록 허용	아니요	아니요	예
메시지를 표시하지 않고 교실 앱이 AirPlay 및 화면 보기를 수행할 수 있도록 허용	아니요	아니요	예
사진 스트림	아니요	예	예
공유 사진 스트림	아니요	예	예
음성 전화 걸기	아니요	예	예
Siri	예	예	예
장치가 잠겨 있는 동안 허용	예	예	예
Siri 비속어 필터	아니요	아니요	예
앱 설치	아니요	아니요 (iOS 13 의 새로운 기능)	예
로밍 중에 글로벌 배경 가져오기 허용	아니요	예	예
앱 허용			
iTunes 스토어	아니요	아니요 (iOS 13 의 새로운 기능)	예

설정	사용자 등록	감독되지 않음	감독됨
앱에서 바로 구매	아니요	예	예
구매 시 iTunes 암호 필요	아니요	예	예
Safari	아니요	아니요 (iOS 13의 새로운 기능)	예
자동 채우기	아니요	아니요 (iOS 13의 새로운 기능)	예
부정 행위 경고 시행	예	예	예
JavaScript 사용	아니요	예	예
팝업 차단	아니요	예	예
쿠키 적용	아니요	예	예
네트워크 - iCloud 동작 허용			
iCloud 문서 및 데이터	아니요	아니요 (iOS 13의 새로운 기능)	예
iCloud 백업	아니요	예	예
iCloud 사진 키 집합	아니요	예	예
iCloud 사진 라이브러리	아니요	예	예
보안 - 시행			
암호화된 백업	예	예	예
제한된 AD 추적	아니요	예	예
첫 번째 AirPlay 페어링의 암호	예	예	예
Wrist Detect를 사용하기 위해 페어링된 Apple Watch	예	예	예
AirDrop을 사용하여 관리되는 문서 공유	예	예	예
보안 - 허용			
신뢰할 수 없는 SSL 인증서 수락	아니요	예	예
인증서 신뢰 설정에 대한 자동 업데이트	아니요	예	예
관리되지 않는 앱에 있는 관리되는 앱의 문서	예	예	예

설정	사용자 등록	감독되지 않음	감독됨
관리되지 않는 앱이 관리되는 연락처 읽기	아니요	아니요	예
관리되는 앱이 관리되지 않는 연락처 쓰기	아니요	아니요	예
관리되는 앱에 있는 관리되지 않는 앱의 문서	예	예	예
Apple에 진단 제출	예	예	예
장치의 잠금을 해제하기 위한 Touch ID	아니요	예	예
자동 잠금 해제	아니요	예	예
잠겨 있을 경우 Passbook 알림	아니요	예	예
핸드오프	아니요	예	예
관리되는 앱에 대한 iCloud 동기화	예	예	예
엔터프라이즈 북에 대한 백업	예	예	예
엔터프라이즈 북 동기화에 대한 메모 및 하이라이트	예	예	예
Spotlight에 대한 인터넷 결과	아니요	예	예
엔터프라이즈 앱 신뢰	아니요	예	예
Apple 개인 맞춤형 광고 허용	아니요	예	예
감독되는 경우에만 해당되는 설정 - 허용			
모든 내용 및 설정 지우기	아니요	아니요	예
제한 구성	아니요	아니요	예
팟캐스트	아니요	아니요	예
구성 프로필 설치	아니요	아니요	예
지문 수정	아니요	아니요	예
장치에서 앱 설치	아니요	아니요	예
바로 가기 키	아니요	아니요	예
페어링된 Apple Watch	아니요	아니요	예
암호 수정	아니요	아니요	예

설정	사용자 등록	감독되지 않음	감독됨
장치 이름 수정	아니요	아니요	예
배경 화면 수정	아니요	아니요	예
자동으로 앱 다운로드	아니요	아니요	예
AirDrop	아니요	아니요	예
iMessage	아니요	아니요	예
Siri 사용자 생성 콘텐츠	아니요	아니요	예
iBooks	아니요	아니요	예
앱 제거	아니요	예	예
게임 센터	아니요	아니요 (iOS 13의 새로운 기능)	예
친구 추가	아니요	아니요	예
멀티플레이 게임	아니요	아니요 (iOS 13의 새로운 기능)	예
계정 설정 수정	아니요	아니요	예
앱 셀룰러 데이터 설정 수정	아니요	아니요	예
앱 셀룰러 데이터 설정 수정	아니요	아니요	예
내 친구 찾기 설정 수정	아니요	아니요	예
비 Configurator 호스트와 페어링	아니요	아니요	예
키보드 자동 완성	아니요	아니요	예
키보드 자동 수정	아니요	아니요	예
키보드 맞춤법 검사	아니요	아니요	예
정의 조회	아니요	아니요	예
단일 앱 번들 ID			
뉴스	아니요	아니요	예
Apple Music 서비스	아니요	아니요	예
iTunes Radio	아니요	아니요	예
알림 수정	아니요	아니요	예
제한된 앱 사용	아니요	아니요	예
진단 제출 수정	아니요	아니요	예

설정	사용자 등록	감독되지 않음	감독됨
Bluetooth 수정	아니요	아니요	예
받아쓰기 허용	아니요	아니요	예
Wi-Fi 정책에 따라 설치된	아니요	아니요	예
Wi-Fi 네트워크에만 참가			
메시지를 표시하지 않고 교실	아니요	아니요	예
앱이 AirPlay 및 화면 보기를			
수행할 수 있도록 허용			
메시지를 표시하지 않고 교실	아니요	아니요	예
앱이 앱 및 장치를 잠글 수 있			
도록 허용			
메시지를 표시하지 않고 교실	아니요	아니요	예
앱 클래스에 자동 참가			
AirPrint 허용	아니요	아니요	예
키 집합에 AirPrint 자격 증	아니요	아니요	예
명 저장 허용			
iBeacon 을 사용하여	아니요	아니요	예
AirPrint 프린터 검색 허용			
신뢰할 수 있는 인증서가 있는	아니요	아니요	예
대상에만 AirPrint 허용			
VPN 구성 추가	아니요	아니요	예
셀룰러 요금제 설정 수정	아니요	아니요	예
시스템 앱 제거	아니요	아니요	예
새로운 주변 장치 설정	아니요	아니요	예
USB 제한 모드 허용	아니요	아니요	예
소프트웨어 업데이트 강제 지	아니요	아니요	예
연			
소프트웨어 업데이트 시행 지	아니요	아니요	예
연			
교실에서 클래스를 나갈 때 허	아니요	아니요	예
가 요청 시행			
암호 자동 채우기	아니요	아니요	예
암호 근접 요청	아니요	아니요	예
암호 공유	아니요	아니요	예
자동 날짜 및 시간 적용	아니요	아니요	예

설정	사용자 등록	감독되지 않음	감독됨
페어링되지 않은 장치로 부팅	아니요	아니요	예
하어 복구 허용			
신속 보안 대응 설치	아니요	아니요	예
신속 보안 대응 제거	아니요	아니요	예
메일 프라이버시 보호 허용	아니요	아니요	예
NFC	아니요	아니요	예
앱 클립 허용	아니요	아니요	예
보안 - 잠금 화면에 표시			
제어 센터	예	예	예
알림	예	예	예
오늘의 보기	예	예	예
미디어 콘텐츠 - 허용			
음악, 팟캐스트 및 iTunes U	아니요	아니요 (iOS 13의 새로운 기능)	예
의 성인 등급 자료			
iBooks의 성 관련 성인 등급 콘텐츠	아니요	예	예
평가 지역	아니요	예	예
영화	아니요	예	예
TV 쇼	아니요	예	예
앱	아니요	예	예

- 하드웨어 제어 허용

- 카메라: 사용자가 장치에서 카메라를 사용할 수 있도록 허용합니다.

- ★ **FaceTime:** 사용자가 장치에서 FaceTime을 사용할 수 있도록 허용합니다. 감독되는 iOS 장치를 위한 설정입니다.

- 스크린샷: 사용자가 장치에서 스크린샷을 찍을 수 있도록 허용합니다.

- ★ 교실 앱이 학생 화면을 원격으로 관찰할 수 있도록 허용: 이 제한을 선택 취소하면 강사가 교실 앱을 사용하여 학생 화면을 원격으로 관찰할 수 없습니다. 기본 설정은 선택되어 있으며 강사는 교실 앱을 사용하여 학생 화면을 관찰할 수 있습니다. 메시지를 표시하지 않고 교실 앱이 **AirPlay** 및 화면 보기를 수행할 수 있도록 허용 설정에 따라 강사에게 권한을 제공할지 여부를 묻는 메시지가 학생에게 표시됩니다. 감독되는 iOS 장치를 위한 설정입니다.

- ★ 메시지를 표시하지 않고 교실 앱이 **AirPlay** 및 화면 보기를 수행할 수 있도록 허용: 이 제한을 선택하면 권한에 대한 메시지 표시 없이 강사가 학생 장치에서 AirPlay 및 화면 보기를 수행할 수 있습니다. 기본 설정은

선택 취소되어 있습니다. 감독되는 iOS 장치를 위한 설정입니다.

- 사진 스트림: 사용자가 MyPhotoStream 을 사용하여 iCloud 를 통해 사진을 모든 iOS 장치에 공유할 수 있도록 허용합니다.
- 공유 사진 스트림: 사용자가 iCloud 사진 공유를 사용하여 동료, 친구 및 가족과 사진을 공유할 수 있도록 허용합니다.
- 음성 전화 걸기: 사용자의 장치에서 전화 걸기를 사용하도록 설정합니다.
- **Siri**: 사용자가 Siri 를 사용할 수 있도록 허용합니다.
 - * 장치가 잠겨 있는 동안 허용: 사용자가 장치가 잠겨 있는 동안 Siri 를 사용할 수 있도록 허용합니다.
 - * **Siri** 비속어 필터: Siri 비속어 필터를 사용하도록 설정합니다. 기본값은 이 기능을 제한하는 것이며, 비속어를 필터링하지 않습니다.Siri 및 보안에 대한 자세한 내용은 [Siri 및 받아쓰기 정책](#)을 참조하십시오.
- 앱 설치: 사용자가 앱을 설치하도록 허용합니다. 감독되는 iOS 장치를 위한 설정입니다.
- 로밍 중에 글로벌 배경 가져오기 허용: 장치가 로밍 중인 동안 장치가 iCloud 에 메일 계정을 자동으로 동기화하도록 허용합니다. 꺼짐으로 설정하면 iOS 휴대폰이 로밍 중일 때 배경 가져오기 활동이 비활성화됩니다. 기본값은 켜짐입니다.

• 앱 허용

- **iTunes** 스토어: 사용자가 iTunes 스토어에 액세스할 수 있도록 허용합니다. 감독되는 iOS 장치를 위한 설정입니다.
- 앱에서 바로 구매: 사용자가 앱 내에서 구입할 수 있도록 허용합니다.
 - * 구매 시 **iTunes** 암호 필요: 앱에서 바로 구매 시 암호를 묻습니다. 기본값은 이 기능을 제한하는 것이며, 앱에서 바로 구매 시 암호가 필요하지 않습니다.
- **Safari**: 사용자가 Safari 에 액세스할 수 있도록 허용합니다. 감독되는 iOS 장치를 위한 설정입니다.
 - * 자동 채우기: 사용자가 Safari 에서 사용자 이름 및 암호에 대한 자동 채우기를 설정할 수 있도록 허용합니다.
 - * 부정 행위 경고 시행: 이 설정을 사용하는 경우 사용자가 의심스러운 피싱 웹 사이트를 방문하면 Safari 경고가 나타납니다. 기본값은 이 기능을 제한하는 것이며, 경고가 실행되지 않습니다.
 - * **JavaScript** 사용: Safari 에서 JavaScript 를 실행하도록 허용합니다.
 - * 팝업 차단: 웹 사이트를 보는 동안 팝업을 차단합니다. 기본값은 이 기능을 제한하는 것이며, 팝업을 차단하지 않습니다.
- 쿠키 적용: 쿠키가 허용되는 범위를 설정합니다. 목록에서 쿠키를 허용하거나 제한하는 옵션을 선택합니다. 기본 옵션은 항상이며, Safari 에서 모든 웹 사이트가 쿠키를 저장하도록 허용합니다. 다른 옵션은 현재 웹 사이트만, 안함 및 방문한 웹 사이트에서만입니다.

• 네트워크 - **iCloud** 동작 허용

- **iCloud** 문서 및 데이터: 사용자가 문서 및 데이터를 iCloud 에 동기화하도록 허용합니다. 감독되는 iOS 장치를 위한 설정입니다.
- **iCloud** 백업: 사용자가 장치를 iCloud 에 백업하도록 허용합니다.
- **iCloud** 키 집합: 사용자가 암호, Wi-Fi 네트워크, 신용 카드 및 기타 정보를 iCloud 키 집합에 저장하도록 허용합니다.

- 클라우드 사진 라이브러리: 사용자가 iCloud 사진 라이브러리에 액세스할 수 있도록 허용합니다.

- 보안 - 시행

기본값은 다음과 같은 기능을 제한하는 것이며, 보안 기능이 사용되지 않습니다.

- 암호화된 백업: iCloud에 대한 백업을 암호화합니다.
- 제한된 AD 추적: 표적 광고 추적을 차단합니다.
- 첫 번째 **Airplay** 페어링의 암호: AirPlay 지원 장치는 AirPlay를 사용하기 전에 화면 상의 일회용 코드로 확인을 받아야 합니다.
- **Wrist Detect**를 사용하기 위해 페어링된 **Apple Watch**: 손목 인식을 사용하려면 페어링된 Apple Watch가 있어야 합니다.
- **AirDrop**을 사용하여 관리되는 문서 공유: 이 옵션을 켜짐으로 설정하면 AirDrop이 관리되지 않는 드롭 대상으로 나타납니다.

- 보안 - 허용

- 신뢰할 수 없는 **SSL** 인증서 수락: 사용자가 웹 사이트의 신뢰할 수 없는 SSL 인증서를 수락하도록 허용합니다.
- 인증서 신뢰 설정에 대한 자동 업데이트: 신뢰할 수 있는 인증서가 자동으로 업데이트되도록 허용합니다.
- 관리되지 않는 앱에 있는 관리되는 앱의 문서: 사용자가 관리되는 (기업) 앱에서 관리되지 않는 (개인) 앱으로 데이터를 이동할 수 있도록 허용합니다.
- 관리되는 앱에 있는 관리되지 않는 앱의 문서: 사용자가 관리되지 않는 (개인) 앱에서 관리되는 (회사) 앱으로 데이터를 이동할 수 있도록 허용합니다.
- **Apple**에 진단 제출: 사용자의 장치에 대한 익명의 진단 데이터를 Apple에 보내도록 허용합니다.
- 장치의 잠금을 해제하기 위한 **Touch ID**: 사용자가 지문을 사용하여 장치의 잠금을 해제하도록 허용합니다.
- 자동 잠금 해제: 꺼짐으로 설정되어 있으면 사용자는 Apple Watch를 사용하여 페어링된 iPhone의 잠금을 해제할 수 없습니다. 기본값은 켜짐입니다. iOS 14.5 이상에서 사용할 수 있습니다.
- 잠겨 있을 경우 **Passbook** 알림: 잠금 화면에 Passbook 알림이 표시되도록 허용합니다.
- 핸드오프: 사용자가 한 iOS 장치에서 근처의 다른 iOS 장치로 활동을 전송할 수 있도록 허용합니다.
- 관리되는 앱에 대한 **iCloud** 동기화: 사용자가 관리되는 앱을 iCloud와 동기화하도록 허용합니다.
- 엔터프라이즈 북에 대한 백업: 엔터프라이즈 북을 iCloud에 백업하도록 허용합니다.
- 엔터프라이즈 북 동기화에 대한 메모 및 하이라이트: 사용자가 엔터프라이즈 북에 추가한 메모 및 하이라이트를 iCloud와 동기화할 수 있도록 허용합니다.
- 엔터프라이즈 앱 신뢰: 엔터프라이즈 응용 프로그램을 신뢰할 수 있도록 허용합니다. 엔터프라이즈 앱은 조직에 따라 맞춤 제작된 앱입니다. 이러한 앱은 내부적으로 만들거나 외부 공급업체를 통해 개발 및 구매할 수 있습니다. 자세한 내용은 [iOS에 사용자 지정 엔터프라이즈 앱 설치](#)를 참조하십시오.
- **Spotlight**에 대한 인터넷 결과: Spotlight가 인터넷뿐만 아니라 장치의 검색 결과를 표시하도록 허용합니다.
- 관리되지 않는 앱이 관리되는 연락처 읽기: 선택 사항. 관리되지 않는 앱에 있는 관리되는 앱의 문서가 사용되지 않는 경우에만 사용할 수 있습니다. 사용하도록 설정하면 관리되지 않는 앱이 관리되는 계정의 연락처에서 데이터를 읽을 수 있습니다. 기본값은 꺼짐입니다. iOS 12부터 사용할 수 있습니다.
- 관리되는 앱이 관리되지 않는 연락처 쓰기: 선택 사항. 사용하도록 설정하면 관리되는 앱에서 관리되지 않는 계정의 연락처에 연락처를 쓸 수 있습니다. 관리되지 않는 앱에 있는 관리되는 앱의 문서를 사용하는 경우 이 제한은 영

항을 미치지 않습니다. 기본값은 꺼짐입니다. iOS 12 부터 사용할 수 있습니다.

- **Apple** 개인 맞춤형 광고 허용: 꺼짐으로 설정되어 있으면 Apple 광고 플랫폼에서 개인 맞춤형 광고를 게재하는 데 사용자의 데이터가 사용되지 않습니다. 기본값은 켜짐입니다. iOS 14.0 이상에서 사용할 수 있습니다.

- 감독되는 경우에만 해당되는 설정 - 허용

이러한 설정은 감독되는 장치에만 적용됩니다. iOS 장치를 감독 모드로 설정하는 단계는 [Apple Configurator](#) 를 사용하여 [iOS 장치를 감독 모드로 전환](#)을 참조하십시오.

- 모든 내용 및 설정 지우기: 사용자가 장치에서 모든 콘텐츠 및 설정을 지울 수 있도록 허용합니다.
- 제한 구성: 사용자가 장치에서 자녀 보호 기능을 구성하도록 허용합니다.
- 팟캐스트: 사용자가 팟캐스트를 다운로드하고 동기화하도록 허용합니다.
- 구성 프로필 설치: 사용자가 배포된 구성 프로필과 다른 구성 프로필을 설치하도록 허용합니다.
- 지문 수정: 사용자가 Touch ID 지문을 변경하거나 삭제하도록 허용합니다.
- 장치에서 앱 설치: 사용자가 앱을 설치하도록 허용합니다. 이 설정을 비활성화하면 최종 사용자가 새 앱을 설치하지 못하게 됩니다. App Store 가 비활성화되고 아이콘이 홈 화면에서 제거됩니다.
- 바로 가기 키: 사용자가 자주 사용하는 단어나 구에 대한 사용자 지정 바로 가기 키를 만들 수 있도록 허용합니다.
- 페어링된 **Apple Watch**: 사용자가 Apple Watch 를 감독되는 장치와 페어링할 수 있도록 허용합니다.
- 암호 수정: 사용자가 감독되는 장치에서 암호를 변경할 수 있도록 허용합니다.
- 장치 이름 수정: 사용자가 장치 이름을 변경할 수 있도록 허용합니다.
- 배경 화면 수정: 사용자가 장치에서 배경 화면을 변경할 수 있도록 허용합니다.
- 자동으로 앱 다운로드: 앱 다운로드를 허용합니다.
- **AirDrop**: 사용자가 인접한 iOS 장치와 사진, 비디오, 웹 사이트, 위치 등을 공유할 수 있도록 허용합니다.
- **iMessage**: 사용자가 iMessage 를 사용하여 Wi-Fi 를 통한 텍스트를 사용하도록 허용합니다.
- **Siri** 사용자 생성 콘텐츠: Siri 가 웹에서 사용자 생성 콘텐츠를 쿼리하도록 허용합니다. 전통적인 저널리스트가 아닌 소비자가 사용자 생성 콘텐츠를 제작합니다. 예를 들어 Twitter 또는 Facebook 에서 찾은 콘텐츠가 사용자가 생성한 콘텐츠입니다.
- **iBooks**: 사용자가 iBooks 앱을 사용할 수 있도록 허용합니다.
- 앱 제거: 사용자가 장치에서 앱을 삭제하도록 허용합니다.
- 게임 센터: 사용자가 장치에서 Game Center 를 통해 온라인 게임을 플레이할 수 있도록 허용합니다.
 - ★ 친구 추가: 사용자가 게임을 할 친구에게 알림을 보낼 수 있도록 허용합니다.
 - ★ 멀티플레이 게임: 사용자가 장치에서 멀티플레이 게임을 시작할 수 있도록 허용합니다.
- 계정 설정 수정: 사용자가 장치 계정 설정을 수정할 수 있도록 허용합니다.
- 앱 셀룰러 데이터 설정 수정: 앱이 셀룰러 데이터를 사용하는 방식을 사용자가 수정할 수 있도록 허용합니다.

- 내 친구 찾기 설정 수정: 사용자가 내 친구 찾기 설정을 변경할 수 있도록 허용합니다.
- 비 **Configurator** 호스트와 페어링: 관리자가 사용자 장치가 페어링할 수 있는 장치를 제어할 수 있도록 허용합니다. 이 설정을 사용하지 않도록 설정하면 Apple Configurator 를 실행하는 감독되는 호스트 이외에는 페어링할 수 없습니다. 감독 호스트 인증서가 구성되어 있지 않으면 모든 페어링을 사용할 수 없습니다.
- 키보드 자동 완성: 사용자 장치가 키보드 자동 완성 기능을 사용하여 입력하는 단어를 제안할 수 있도록 허용합니다. 사용자가 추천 단어에 액세스하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 키보드 자동 수정: 사용자 장치가 키보드 자동 수정을 사용할 수 있도록 허용합니다. 사용자가 자동 수정에 액세스하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 키보드 맞춤법 검사: 입력하는 동안 사용자 장치가 맞춤법 검사를 사용할 수 있도록 허용합니다. 사용자가 맞춤법 검사에 액세스하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 정의 조회: 입력하는 동안 사용자 장치가 정의 조회를 사용할 수 있도록 허용합니다. 사용자가 입력하는 동안 정의를 조회하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 단일 앱 번들 ID: 장치에 대한 제어 권한을 유지하고 다른 앱 또는 기능과의 상호 작용을 방지하도록 허용된 앱 목록을 만듭니다.
앱을 추가하려면 추가를 클릭하고 앱 이름을 입력한 후 저장을 클릭합니다. 추가할 각 앱에 대해 이 프로세스를 반복합니다.
- 뉴스: 사용자가 뉴스 앱을 사용할 수 있도록 허용합니다.
- **Apple Music** 서비스: 사용자가 Apple Music 서비스를 사용할 수 있도록 허용합니다. Apple Music 서비스를 허용하지 않는 경우 Music 앱이 클래식 모드에서 실행됩니다.
- **iTunes Radio**: 사용자가 iTunes Radio 를 사용할 수 있도록 허용합니다.
- 알림 수정: 사용자가 알림 설정을 수정할 수 있도록 허용합니다.
- 제한된 앱 사용: 사용자가 제공된 번들 ID 를 기반으로 모든 앱을 사용하거나 일부 앱을 사용하거나 사용하지 않도록 허용합니다. 감독되는 장치에만 적용됩니다. 일부 앱만 허용을 선택할 경우 번들 ID 가 [com.apple.webapp](#)인 앱을 추가하여 웹 클립을 허용합니다.

참고:

iOS 11 부터 앱 제한에서 사용할 수 있는 Apple 정책이 변경되었습니다. Apple 의 경우 더 이상 적절한 iOS 응용 프로그램 번들을 제한하여 설정 앱과 전화 앱에 대한 액세스를 제거할 수 없습니다.

일부 앱을 차단하는 제한 장치 정책을 구성한 후 정책 배포: 나중에 해당 앱 중 일부 또는 전부를 허용하려는 경우 제한 장치 정책을 변경하고 배포해도 제한이 변경되지 않습니다. 이 경우 iOS 가 변경 내용을 iOS 프로필에 적용하지 않습니다. 계속하려면 프로필 제거 정책을 사용하여 iOS 프로필을 제거한 후 업데이트된 제한 장치 정책을 배포해야 합니다.

이 설정을 **Only allow some apps**(일부 앱만 허용) 로 변경하는 경우: 이 정책을 배포하기 전에 Apple 배포 프로그램을 사용하여 등록된 장치의 사용자가 설정 도우미에서 Apple 계정에 로그인할 수 있도록 해당 사용자에게

게 알려줘야 합니다. 그렇지 않으면 사용자가 장치에서 2 단계 인증을 사용하지 않도록 설정해야 Apple 계정으로 로그인하고 허용된 앱에 액세스할 수 있습니다.

- 진단 제출 수정: 사용자가 설정 > 진단 및 사용 현황 창의 설정에서 진단 제출 및 앱 분석 설정을 변경할 수 있도록 허용합니다.
- **Bluetooth** 수정: 사용자가 Bluetooth 설정을 수정할 수 있도록 허용합니다.
- 받아쓰기 허용: 감독되는 경우에만 해당. 이 제한을 꺼짐으로 설정하면 음성 텍스트 변환을 포함한 받아쓰기 입력이 허용되지 않습니다. 기본 설정은 켜짐입니다.
- **WiFi** 정책에 따라 설치된 **WiFi** 네트워크에만 참가: 선택 사항입니다. 감독되는 경우에만 해당. 이 제한을 켜짐으로 설정하면 구성 프로필을 통해 설정된 장치만 Wi-Fi 네트워크에 참여할 수 있습니다. 기본 설정은 꺼짐입니다.
- 메시지를 표시하지 않고 교실 앱이 **AirPlay** 및 화면 보기를 수행할 수 있도록 허용: 이 제한을 선택하면 권한에 대한 메시지 표시 없이 강사가 학생 장치에서 AirPlay 및 화면 보기를 수행할 수 있습니다. 기본 설정은 선택 취소되어 있습니다. 감독되는 iOS 장치를 위한 설정입니다.
- 메시지를 표시하지 않고 교실 앱이 앱 및 장치를 잠글 수 있도록 허용: 이 제한을 켜짐으로 설정하면 교실 앱이 사용자에게 메시지를 표시하지 않고 자동으로 사용자 장치와 앱을 잠급니다. 기본 설정은 꺼짐입니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- 메시지를 표시하지 않고 교실 앱 클래스에 자동 참가: 이 제한을 켜짐으로 설정하면 교실 앱이 사용자에게 메시지를 표시하지 않고 사용자를 자동으로 클래스에 참가시킵니다. 기본 설정은 꺼짐입니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- **AirPrint** 허용: 이 제한을 꺼짐으로 설정하면 사용자가 AirPrint를 사용하여 인쇄할 수 없습니다. 기본 설정은 켜짐입니다. 이 제한이 켜짐인 경우 다음과 같은 추가 제한이 표시됩니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
 - * 키 집합에 **AirPrint** 자격 증명 저장 허용: 이 제한을 선택 취소하면 AirPrint 사용자 이름과 암호가 키 집합에 저장되지 않습니다. 기본 설정은 선택되어 있습니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
 - * **iBeacon**을 사용하여 **AirPrint** 프린터 검색 허용: 이 제한을 선택 취소하면 AirPrint 프린터에 대한 iBeacon 검색이 사용되지 않습니다. 이렇게 하면 위장한 AirPrint Bluetooth 알림의 네트워크 트래픽 피싱이 방지됩니다. 기본 설정은 선택되어 있습니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
 - * 신뢰할 수 있는 인증서가 있는 대상에만 **AirPrint** 허용: 이 제한을 선택하면 사용자가 AirPrint를 사용하여 신뢰할 수 있는 인증서가 있는 대상에만 인쇄할 수 있습니다. 기본 설정은 선택 취소되어 있습니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- **VPN** 구성 추가: 이 제한을 꺼짐으로 설정하면 사용자가 VPN 구성을 만들 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- 셀룰러 요금제 설정 수정: 이 제한을 꺼짐으로 설정하면 사용자가 셀룰러 요금제 설정을 수정할 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.

- **시스템 앱 제거:** 이 제한을 꺼짐으로 설정하면 사용자가 시스템 앱을 장치에서 제거할 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- **새로운 주변 장치 설정:** 이 제한을 꺼짐으로 설정하면 사용자가 새로운 주변 장치를 설정할 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- **USB 제한 모드 허용:** 꺼짐인 경우 장치가 잠겨 있는 동안 항상 USB 액세서리에 연결할 수 있습니다. 기본값은 켜짐입니다. iOS 11.3 이상의 감독되는 장치에서만 사용할 수 있습니다.
- **소프트웨어 업데이트 강제 지연:** 켜짐인 경우 사용자에게 소프트웨어 업데이트 표시가 지연됩니다. 이 제한을 적용하면 소프트웨어 업데이트 릴리스 날짜로부터 지정된 기간 (일) 까지 소프트웨어 업데이트가 표시되지 않습니다. 기본값은 꺼짐입니다. iOS 11.3 이상의 감독되는 장치에서만 사용할 수 있습니다.
- **소프트웨어 업데이트 시행 지연 (일):** 장치에서 소프트웨어 업데이트를 지연할 일 수를 지정할 수 있습니다. 최대 지연은 **90** 일입니다. 기본값은 **30** 일입니다. iOS 11.3 이상의 감독되는 장치에서만 사용할 수 있습니다.
- **교실에서 클래스를 나갈 때 허가 요청 시행:** 켜짐인 경우 교실 앱을 통해 관리되지 않는 과정에 등록된 학생이 과정을 나가려면 교사의 허가를 요청해야 합니다. 기본값은 꺼짐입니다. iOS 11.3 이상의 감독되는 장치에서만 사용할 수 있습니다.
- **암호 자동 채우기:** 선택 사항입니다. 사용하지 않는 경우 사용자는 암호 자동 채우기 또는 강력한 자동 암호 기능을 사용할 수 없습니다. 기본값은 켜짐입니다. iOS 12 부터 사용할 수 있습니다.
- **암호 근접 요청:** 선택 사항입니다. 사용하지 않는 경우 사용자의 장치는 주변 장치에서 암호를 요청하지 않습니다. 기본값은 켜짐입니다. iOS 12 부터 사용할 수 있습니다.
- **암호 공유:** 선택 사항입니다. 사용하지 않는 경우 사용자는 AirDrop 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 켜짐입니다. iOS 12 부터 사용할 수 있습니다.
- **자동 날짜 및 시간 적용:** 감독되는 장치에서 날짜와 시간을 자동으로 설정할 수 있습니다. 켜짐인 경우 장치 사용자는 일반 > 날짜 및 시간에서 자동으로 설정을 끌 수 없습니다. 장치의 표준 시간대는 장치가 해당 위치를 확인할 수 있는 경우에만 업데이트됩니다. 즉, 장치에 위치 서비스가 활성화된 셀룰러 연결 또는 Wi-Fi 연결이 있는 경우입니다. 기본값은 꺼짐입니다. iOS 12 이상의 감독되는 장치에서만 사용할 수 있습니다.
- **페어링되지 않은 장치로 부팅하여 복구 허용:** 꺼짐으로 설정되어 있으면 페어링되지 않은 장치가 복구 모드로 장치를 부팅할 수 있습니다. 기본값은 꺼짐입니다. iOS 14.5 이상에서 사용할 수 있습니다.
- **신속 보안 대응 설치:** 꺼짐으로 설정되어 있으면 신속 보안 대응이 설치되지 않습니다. 기본값은 켜짐입니다.
- **신속 보안 대응 제거:** 꺼짐으로 설정되어 있으면 신속 보안 대응이 제거되지 않습니다. 기본값은 켜짐입니다.
- **메일 개인 프라이버시 보호 허용:** 꺼짐으로 설정되어 있으면 장치에서 메일 프라이버시 보호가 비활성화됩니다. 기본값은 켜짐입니다. iOS 15.2 이상에서 사용할 수 있습니다.
- **NFC:** 꺼짐으로 설정되어 있으면 NFC 가 비활성화됩니다. 기본값은 켜짐입니다. iOS 14.2 이상에서 사용할 수 있습니다.
- **앱 클립 허용:** 꺼짐으로 설정되어 있으면 사용자가 앱 클립을 추가하지 못하게 하고 장치에서 기존 앱 클립을 제거합니다. 기본값은 켜짐입니다. iOS 14.0 이상에서 사용할 수 있습니다.

- 보안 - 잠금 화면에 표시
 - 제어 센터: 잠금 화면에서 제어 센터에 액세스 할 수 있습니다. 사용자는 제어 센터에서 비행기 모드, Wi-Fi, Bluetooth, 방해 금지 모드 및 회전 잠금 설정을 쉽게 수정할 수 있습니다.
 - 알림: 잠금 화면에서 알림을 허용합니다.
 - 오늘의 보기: 날씨 및 오늘 날짜의 일정 항목과 같은 정보를 잠금 화면에 집계하는 [오늘의 보기] 를 허용합니다.
- 미디어 콘텐츠 - 허용
 - 음악, 팟캐스트 및 **iTunes U** 의 성인 등급 자료: 사용자의 장치에 무삭제판 자료를 허용합니다.
 - **iBooks** 의 성 관련 성인 등급 콘텐츠: iBooks 에서 무삭제판 자료를 다운로드하도록 허용합니다.
 - 평가 지역: 유해 콘텐츠 차단 등급을 얻는 지역을 설정합니다. 목록에서 평가 지역을 설정할 국가를 클릭합니다. 기본값은 미국입니다.
 - 영화: 사용자 장치에서 영화를 허용할지 여부를 설정합니다. 영화가 허용된 경우 선택적으로 영화 등급을 설정합니다. 목록에서 장치에 영화를 허용하거나 제한하는 옵션을 선택합니다. 기본값은 모든 영화 허용입니다.
 - **TV 쇼**: 사용자 장치에서 TV 쇼를 허용할지 여부를 설정합니다. TV 쇼가 허용된 경우 선택적으로 TV 쇼 등급을 설정합니다. 목록에서 장치에 TV 쇼를 허용하거나 제한하는 옵션을 선택합니다. 기본값은 모든 TV 쇼 허용입니다.
 - 앱: 사용자 장치에서 앱을 허용할지 여부를 설정합니다. 앱이 허용된 경우 선택적으로 앱 등급을 설정합니다. 목록에서 장치에 앱을 허용하거나 제한하는 옵션을 선택합니다. 기본값은 모든 앱 허용입니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.
 - 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 iOS 9.3 이상에서만 사용할 수 있습니다.

macOS 설정

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	Preferences
<input type="checkbox"/> iOS	Restrict items in System Preferences <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> macOS	Apps
<input checked="" type="checkbox"/> Samsung SAFE	Allow use of Game Center <input checked="" type="checkbox"/> ON macOS 10.11+
<input checked="" type="checkbox"/> Samsung KNOX	Allow adding Game Center friends <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Phone	Allow multiplayer gaming <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Allow Game Center account modification <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Amazon	Allow App Store adoption <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Mobile/CE	Allow Safari AutoFill <input checked="" type="checkbox"/> ON
3 Assignment	Require admin password to install or update apps <input type="checkbox"/> OFF
	Restrict App Store to software update only <input type="checkbox"/> OFF

- 기본 설정
 - 시스템 기본 설정에서 항목 제한: 시스템 기본 설정에 대한 사용자 액세스를 허용하거나 제한합니다. 기본값은 시스템 기본 설정에 대한 사용자의 전체 액세스를 허용하는 꺼짐입니다. 사용하는 경우 다음 설정을 구성합니다.
 - ★ 시스템 기본 설정 창: 선택한 설정을 사용할지 여부를 선택합니다. 기본값은 모든 설정을 사용하도록 설정하는 것이며, 기본적으로 꺼짐입니다.
 - 사용자 및 그룹
 - 일반
 - 내게 필요한 옵션
 - App Store
 - 소프트웨어 업데이트
 - Bluetooth
 - CD 및 DVD
 - 날짜 및 시간
 - 데스크톱 및 화면 보호기
 - 디스플레이
 - 고정
 - 절전
 - 확장
 - FibreChannel
 - iCloud
 - 잉크
 - 인터넷 계정
 - 키보드
 - 언어 및 텍스트

- Mission Control
 - 마우스
 - 네트워크
 - 알림
 - 자녀 보호
 - 프린터 및 스캐너
 - 프로필
 - 보안 및 개인 정보
 - 공유
 - 사운드
 - 받아쓰기 및 음성
 - Spotlight
 - 시동 디스크
 - Time Machine
 - 트랙 패드
 - Xsan
- 앱
 - 게임 센터 사용 허용: 사용자가 Game Center 를 통해 온라인 게임을 할 수 있도록 허용합니다. 기본값은 켜짐입니다.
 - 게임 센터 친구 추가 허용: 사용자가 게임을 할 친구에게 알림을 보낼 수 있도록 허용합니다. 기본값은 켜짐입니다.
 - 멀티 플레이어 게임 허용: 사용자가 멀티 플레이어 게임을 시작할 수 있도록 허용합니다. 기본값은 켜짐입니다.
 - 게임 센터 계정 수정 허용: 사용자가 Game Center 계정 설정을 수정할 수 있도록 허용합니다. 기본값은 켜짐입니다.
 - **App Store** 채택 허용: App Store 에서 OS X 의 기존 앱을 채택하는 것을 허용하거나 제한합니다. 기본값은 켜짐입니다.
 - **Safari** 자동 채우기 허용: Safari 가 암호, 주소 및 다른 저장된 기본 정보로 웹 사이트의 필드를 자동으로 채우도록 허용합니다. 기본값은 켜짐입니다.
 - 앱을 설치 또는 업데이트하려면 관리자 암호가 필요함: 앱을 설치하거나 업데이트하려면 관리자 암호가 필요합니다. 기본값은 꺼짐이며, 관리자 암호가 필요하지 않습니다.
 - **App Store** 를 소프트웨어 업데이트 전용 제한: App Store 를 업데이트 전용으로 제한합니다. 업데이트를 제외한 App Store 의 모든 탭이 비활성화됩니다. 기본값은 전체 App Store 액세스 권한을 허용하는 꺼짐입니다.
 - 열기가 허용된 앱 제한: 사용자가 사용할 수 있는 앱을 제한하거나 허용합니다. 기본값은 모든 앱을 사용하도록 허용하는 꺼짐입니다. 사용하는 경우 다음 설정을 구성합니다.
 - * 허용되는 앱: 추가를 클릭하고 시작하도록 허용된 앱의 번들 ID 와 이름을 입력한 다음 저장을 클릭합니다. 시작하도록 허용할 각 앱에 대해 이 단계를 반복합니다.
 - * 허용되지 않은 폴더: 추가를 클릭하고 사용자 액세스를 제한할 폴더의 파일 경로 (예: /Applications/Utilities) 를 입력한 다음 저장을 클릭합니다. 사용자가 액세스할 수 없게 하려는 모든 폴더에 대해 이 단계를 반복합니다.
 - * 허용되는 폴더: 추가를 클릭하고 사용자에게 액세스하도록 허가할 폴더의 파일 경로를 입력한 다음 저장을 클

립니다. 사용자가 액세스할 수 있게 하려는 모든 폴더에 대해 이 단계를 반복합니다.

- 위젯

- 다음 대시보드 위젯만 실행되도록 허용: 세계 시계 또는 계산기와 같이 사용자에게 실행하도록 허용된 대시보드 위젯을 허용하거나 제한합니다. 기본값은 사용자가 모든 위젯을 실행하도록 허용하는 꺼짐입니다. 사용하는 경우 다음 설정을 구성합니다.
 - ★ 허용되는 위젯: 추가를 클릭하고 실행하도록 허용된 위젯의 이름 및 ID 를 입력한 다음 저장을 클릭합니다. 대시보드에서 실행하려는 각 위젯에 대해 이 단계를 반복합니다.

- 미디어

- **AirDrop** 허용: 사용자가 인접한 iOS 장치와 사진, 비디오, 웹 사이트, 위치 등을 공유할 수 있도록 허용합니다.

- 공유

- 새 공유 서비스를 자동으로 사용: 공유 서비스를 자동으로 사용할지 여부를 선택합니다.
- 메일: 공유 사서함을 허용할지 여부를 선택합니다.
- **Facebook**: 공유 Facebook 계정을 허용할지 여부를 선택합니다.
- 비디오 서비스 - **Flickr, Vimeo, Tudou** 및 **Youku**: 공유 비디오 서비스를 허용할지 여부를 선택합니다.
- **Aperture** 에 추가: Aperture 에 공유 기능을 추가하도록 허용할지 여부를 선택합니다.
- **Sina Weibo**: 공유 Sina Weibo 마이크로 블로그 계정을 허용할지 여부를 선택합니다.
- **Twitter**: 공유 Twitter 계정을 허용할지 여부를 선택합니다.
- 메시지: 메시지에 대한 공유 액세스를 허용할지 여부를 선택합니다.
- **iPhoto** 에 추가: iPhoto 에 공유 기능을 추가하도록 허용할지 여부를 선택합니다.
- 읽기 목록에 추가: 읽기 목록에 공유 기능을 추가하도록 허용할지 여부를 선택합니다.
- **AirDrop**: 공유 AirDrop 계정을 허용할지 여부를 선택합니다.

- 기능

- 데스크톱 바탕 화면 잠금: 사용자가 바탕 화면 사진을 변경할 수 있는지 여부를 선택합니다. 기본값은 사용자가 바탕 화면 사진을 변경할 수 있는 꺼짐입니다.
- 카메라 사용 허용: 사용자가 Mac 에서 카메라를 사용할 수 있는지 여부를 선택합니다. 기본값은 사용자가 카메라를 사용할 수 없는 꺼짐입니다.
- **Apple Music** 허용: 사용자가 Apple Music 서비스를 사용할 수 있도록 허용합니다 (macOS 10.12 이상). Apple Music 서비스를 허용하지 않는 경우 Music 앱이 클래식 모드에서 실행됩니다. 감독되는 장치에만 적용됩니다. 기본값은 꺼짐입니다.
- **Spotlight** 제안 허용: 사용자가 Spotlight 제안을 사용하여 Mac 을 검색하고 인터넷, iTunes 및 App Store 의 Spotlight 제안을 제공할 수 있는지 여부를 선택합니다. 기본값은 사용자가 Spotlight 제안을 사용하지 못하게 하는 꺼짐입니다.
- 조회 허용: 사용자가 상황에 맞는 메뉴 또는 Spotlight 검색 메뉴를 사용하여 단어의 정의를 조회할 수 있는지 여부를 선택합니다. 기본값은 사용자가 Mac 에서 조회를 사용하지 못하게 하는 꺼짐입니다.
- 로컬 계정에 **iCloud** 암호 사용 허용: 사용자가 Apple ID 및 iCloud 암호를 사용하여 Mac 에 로그인할 수 있는지 여부를 선택합니다. 이 정책을 사용하도록 설정하면 사용자가 Mac 의 모든 로그인 화면에서 하나의 ID 와 암호

만 사용하게 됩니다. 기본값은 사용자가 Apple ID 및 iCloud 암호를 사용하여 Mac 에 액세스할 수 있도록 허용하는 켜짐입니다.

- **iCloud** 문서 및 데이터 허용: 사용자가 Mac 에서 iCloud 에 저장된 문서 및 데이터에 액세스할 수 있도록 허용할지 여부를 선택합니다. 기본값은 사용자가 Mac 에서 iCloud 문서 및 데이터를 사용하지 못하게 하는 꺼짐입니다.

★ **iCloud** 바탕 화면 및 문서 허용: (macOS 10.12.4 이상) 기본적으로 선택됩니다.

- **iCloud** 키 집합 동기화 허용: iCloud 키 집합 동기화를 허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 메일 허용: 사용자가 iCloud 메일을 사용할 수 있도록 허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 연락처 허용: 사용자가 iCloud 연락처를 사용할 수 있도록 허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 일정 허용: 사용자가 iCloud 일정을 사용할 수 있도록 허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 미리 알림 허용: 사용자가 iCloud 미리 알림을 사용할 수 있도록 허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 책갈피 허용: 사용자가 iCloud 책갈피를 동기화할 수 있도록 허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 메모 허용: 사용자가 iCloud 메모를 사용할 수 있도록 허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 사진 허용: 이 설정을 꺼짐으로 변경하면 iCloud 사진 라이브러리에서 완벽하게 다운로드되지 않은 모든 사진이 로컬 장치 스토리지에서 제거됩니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- 자동 잠금 해제 허용: 이 옵션 및 Apple Watch 에 대한 자세한 내용은 <https://www.imore.com/auto-unlock>을 참조하십시오 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **Touch ID** 를 통한 **Mac** 잠금 해제 허용: (macOS 10.12.4 이상). 기본값은 켜짐입니다.
- 소프트웨어 업데이트 강제 지연: 켜짐인 경우 사용자에게 소프트웨어 업데이트 표시가 지연됩니다. 소프트웨어 업데이트 릴리스 날짜로부터 지정된 기간 (일) 까지 소프트웨어 업데이트가 표시되지 않습니다. 기본값은 꺼짐입니다. macOS 10.13.4 이상을 실행하는 감독되는 장치에만 사용할 수 있습니다.
- 소프트웨어 업데이트 시행 지연 (일): 장치에서 소프트웨어 업데이트를 지연할 일 수를 지정합니다. 최대값은 90 일입니다. 기본값은 30 입니다. macOS 10.13.4 이상을 실행하는 감독되는 장치에만 사용할 수 있습니다.
- 암호 자동 채우기: 선택 사항입니다. 사용하지 않는 경우 사용자는 암호 자동 채우기 또는 강력한 자동 암호 기능을 사용할 수 없습니다. 기본값은 켜짐입니다. macOS 10.14 부터 사용할 수 있습니다.
- 암호 근접 요청: 선택 사항입니다. 사용하지 않는 경우 사용자의 장치는 주변 장치에서 암호를 요청하지 않습니다. 기본값은 켜짐입니다. macOS 10.14 부터 사용할 수 있습니다.
- 암호 공유: 선택 사항입니다. 사용하지 않는 경우 사용자는 Airdrop 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 켜짐입니다. macOS 10.14 부터 사용할 수 있습니다.

Android 설정

- **카메라:** 사용자가 장치에서 카메라를 사용할 수 있도록 허용합니다. 꺼짐인 경우 카메라가 사용되지 않습니다. 기본값은 켜짐입니다.

Android Enterprise 설정

Apply to fully managed devices with a work profile/Work profile on corporate-owned devices

ON

For fully managed devices with a work profile, apply the policy to

Work profile

Managed device

Security

Allow Account Management

OFF

Allow cross profile copy and paste

OFF

Allow screen capture

OFF

Allow use of camera

OFF

Allow configuring location provider

ON

Allow location sharing

OFF

Allow user to configure user credentials

ON

Allow printing

OFF

새 Android 장치 또는 공장 기본값으로 재설정된 Android 장치가 작업 프로필 모드로 등록되면 Android 9.0-10.x 를 실행하는 장치는 작업 프로필이 있는 완전 관리형 장치로 등록됩니다. Android 11 이상을 실행하는 장치는 회사 소유 장치에서 작업 프로필로 등록됩니다. 제한 정책은 장치 또는 관리되는 장치의 작업 프로필에 적용할 수 있습니다.

회사 소유 장치 모드로 작업 프로필에 등록된 장치에서는 다음 제한을 작업 프로필에만 사용할 수 있습니다.

- 백업 서비스 허용
- 시스템 앱 사용
- Keyguard 가 장치를 잠그지 않도록 방지
- 상태 표시줄의 사용 허용
- 장치 화면을 켜진 상태로 유지
- 응용 프로그램 설정의 사용자 제어 허용
- 사용자가 사용자 자격 증명을 구성하도록 허용
- VPN 구성 허용
- USB 대용량 스토리지 허용
- 공장 기본값으로 재설정 허용
- 앱 제거 허용
- Google Play 이외의 앱 허용
- 상호 프로필 복사 및 붙여넣기 허용
- 앱 확인 사용
- 계정 관리 허용
- 인쇄 허용
- NFC 허용
- 사용자 추가 허용

Android Enterprise 의 작업 프로필 모드에서 장치를 등록하는 경우 **USB** 디버깅 및 알 수 없는 소스 설정은 기본적으로 사용되지 않도록 설정됩니다.

Android 9.0-10.x 및 Samsung Knox 3.0 이상을 실행하는 장치의 경우 **Android Enterprise** 페이지에서 Samsung Knox 및 Samsung SAFE 에 대한 설정을 구성합니다. 이전 버전의 Android 또는 Samsung Knox 를 실행하는 장치의 경우 **Samsung Knox** 페이지 및 **Samsung SAFE** 페이지를 사용합니다.

회사 소유 장치 모드로 작업 프로필에 등록된 장치에는 Samsung 제한이 적용되지 않습니다. Knox 서비스 플러그인 (KSP) 을 사용하여 이러한 장치에 Samsung 제한을 적용합니다. 자세한 내용은 [Samsung 설명서](#)를 참조하십시오.

최신 Samsung Knox 관리 기능에 Samsung Knox 3.4 이상을 사용할 것을 권장합니다.

- 작업 프로필/회사 소유 장치의 작업 프로필을 사용하는 완전 관리형 장치에 적용: 작업 프로필로 완전히 관리되는 장치에 대해 제한 정책 설정이 구성될 수 있도록 허용합니다. 이 설정이 켜짐인 경우 다음 설정 중 하나를 선택합니다.
 - 작업 프로필: 구성하는 제한 설정이 장치의 작업 프로필에만 적용됩니다.
 - 장치 관리: 구성하는 제한 설정이 장치에만 적용됩니다.

이 설정이 꺼짐인 경우 구성하는 자격 증명 설정은 작업 프로필에 명시적으로 적용되는 설정을 제외하고 장치에 적용됩니다. 기본값은 꺼짐입니다.

작업 프로필/회사 소유 장치의 작업 프로필을 사용하는 완전 관리형 장치에 적용이 꺼짐인 경우 다음 설정을 구성합니다.

- 보안

- 계정 관리 허용: 작업 프로필 및 관리되는 장치에 계정을 추가할 수 있습니다. 기본값은 꺼짐입니다.
- 상호 프로필 복사 및 붙여넣기 허용: 커짐일 경우 사용자는 Android Enterprise 프로필의 앱과 개인 영역의 앱 사이에 복사해서 붙여넣을 수 있습니다. 기본값은 꺼짐입니다.
- 화면 캡처 허용: 사용자가 장치 화면의 화면 캡처를 기록하거나 생성할 수 있습니다. 기본값은 꺼짐입니다.
- 카메라 사용 허용: 사용자가 장치 카메라로 사진을 찍고 비디오를 만들 수 있습니다. 기본값은 꺼짐입니다.
- VPN 구성 허용: 사용자가 VPN 구성을 만들 수 있습니다. Android 6 이상을 실행하는 작업 프로필 장치와 완전 관리형 장치를 위한 설정입니다. 기본값은 커짐입니다.
- 백업 서비스 허용: 사용자가 장치에서 응용 프로그램 및 시스템 데이터를 백업할 수 있습니다. 기본값은 커짐입니다.
- NFC 허용: 사용자가 NFC(근거리 통신)를 사용하여 장치의 웹 페이지, 사진, 비디오 또는 기타 콘텐츠를 다른 장치로 보낼 수 있도록 허용합니다. MDM 4.0 이상에 해당합니다. 기본값은 커짐입니다.
- 위치 공급자 구성 허용: 사용자가 자신의 장치에서 GPS를 켤 수 있습니다. Android API 28 이상을 위한 설정입니다. 기본값은 커짐입니다.
- 위치 공유 허용: 관리되는 프로필의 경우 장치 소유자가 이 설정을 재정의할 수 있습니다. 기본값은 꺼짐입니다.

팁:

XenMobile에서 위치 장치 정책을 만들어 지리적 경계를 적용할 수 있습니다. [위치 장치 정책](#)을 참조하십시오.

- 사용자가 사용자 자격 증명을 구성하도록 허용: 사용자가 관리형 키 저장소의 자격 증명을 구성할 수 있는지 여부를 지정합니다. 기본값은 커짐입니다.
- 인쇄 허용: 커짐일 경우 이 설정은 사용자가 사용자 장치에서 액세스할 수 있는 모든 프린터로 인쇄할 수 있도록 허용합니다. 기본값은 꺼짐입니다. Android 9 이상에서 사용할 수 있습니다.
- USB 디버깅 허용: 기본값은 꺼짐입니다.

• 앱

- 시스템 앱 사용: 사용자가 사전 설치된 장치 앱을 실행할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 특정 앱을 사용하려면 시스템 앱 목록 테이블에서 추가를 클릭합니다.
 - * 시스템 앱 목록: 장치에서 사용할 시스템 앱 목록입니다. 시스템 앱 사용을 커짐으로 설정하고 앱 패키지 이름을 추가합니다. 시스템 앱의 패키지 이름을 조회하려면 Android Debug Bridge(adb)를 사용하여 Android 패키지 관리자 (pm) 명령을 호출하면 됩니다. 예: `adb shell "pm list packages -f name"`. 여기서 "name"은 패키지 이름의 일부입니다. 자세한 내용은 <https://developer.android.com/studio/command-line/adb> 항목을 참조하십시오. Android Enterprise 기기의 경우 [Android Enterprise 앱 권한](#) 정책을 사용하여 앱 권한을 제한할 수 있습니다.

- 응용 프로그램 사용 안 함: 장치에서 지정된 목록의 앱이 실행되지 않도록 차단합니다. 기본값은 꺼짐입니다. 설치된 앱을 사용하지 않도록 설정하려면 설정을 켜짐으로 변경한 다음 응용 프로그램 목록 테이블에서 추가를 클릭합니다.
 - * 응용 프로그램 목록: 차단하려는 앱의 목록입니다. 응용 프로그램 사용 안 함을 켜짐으로 설정하고 앱을 추가합니다. 앱 패키지 이름을 입력합니다. 앱 목록을 변경하고 배포하면 이전 앱 목록을 덮어씁니다. 예: com.example1 및 com.example2 를 사용하지 않도록 설정하고 나중에 com.example1 및 com.example3 으로 목록을 변경하는 경우 XenMobile 은 com.example.2 를 사용하도록 설정합니다.
- 앱 확인 사용: OS 에서 앱을 검사하여 악성 동작을 검색할 수 있도록 합니다. 기본값은 켜짐입니다.
- **Google** 앱 사용: 사용자가 Google 모바일 서비스에서 컨테이너로 앱을 다운로드할 수 있습니다. 기본값은 켜짐입니다.
- **Google Play** 이외의 앱 허용: Google Play 이외의 스토어에서 앱을 설치할 수 있습니다. 기본값은 꺼짐입니다.
- 응용 프로그램 설정의 사용자 제어 허용: 사용자가 앱을 제거하고, 앱을 사용하지 않도록 설정하고, 캐시 및 데이터를 지우고, 앱을 강제로 중지하고, 기본값을 지울 수 있습니다. 사용자는 설정 앱에서 이러한 작업을 수행합니다. 기본값은 꺼짐입니다.
- 앱 제거 허용: 사용자가 관리되는 Google Play 스토어 내에서 앱을 제거하도록 허용합니다. 기본값은 꺼짐입니다. 이 설정을 표시하려면 서버 속성 ([afw.restriction.policy.v2](#)) 을 활성화합니다. 서버 속성에 대한 자세한 내용은 [서버 속성](#) 을 참조하십시오.

• BYOD 작업 프로필

- 홈 화면에 작업 프로필 앱 위젯 허용: 이 설정이 켜짐인 경우 사용자가 작업 프로필 앱 위젯을 장치 홈 화면에 배치할 수 있습니다. 이 설정이 꺼짐인 경우 사용자가 작업 프로필 앱 위젯을 장치 홈 화면에 배치할 수 없습니다. 기본값은 꺼짐입니다.
 - * 위젯이 허용되는 앱: 홈 화면에서 허용할 앱 목록입니다. 홈 화면에 작업 프로필 앱 위젯 허용을 켜짐으로 설정하고 앱을 추가합니다. 추가를 클릭하고 목록에서 홈 화면에 허용할 위젯의 앱을 선택합니다. 저장을 클릭합니다. 더 많은 앱 위젯을 허용하려면 이 프로세스를 반복합니다.
- 장치 연락처에 작업 프로필 연락처 허용: 수신 전화에 대해 관리되는 Android Enterprise 프로필에 있는 연락처가 상위 프로필에 표시됩니다 (Android 7.0 이상). 기본값은 꺼짐입니다.

• 완전 관리형 장치만

- 사용자 추가 허용: 사용자가 장치에 새 사용자를 추가할 수 있도록 허용합니다. 기본값은 켜짐입니다.
- 데이터 로밍 허용: 로밍하는 동안 사용자가 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐이며, 사용자의 장치에서 로밍이 비활성화됩니다. 기본값은 꺼짐입니다.
- **SMS** 허용: 사용자가 SMS 메시지를 보내고 받을 수 있습니다. 기본값은 꺼짐입니다.
- 상태 표시줄의 사용 허용: 켜짐인 경우 관리되는 장치 및 전용 장치 (COSU 장치라고도 함) 에서 상태 표시줄이 사용됩니다. 이렇게 설정하면 알림, 빠른 설정 및 전체 화면 모드에서 벗어날 수 있는 기타 화면 오버레이가 사용되지 않습니다. 사용자는 시스템 설정으로 이동하여 알림을 볼 수 있습니다. Android 6.0 이상을 위한 설정입니다. 기본값은 꺼짐입니다.

- **Bluetooth** 허용: 사용자가 Bluetooth 를 사용할 수 있습니다. 기본값은 켜짐입니다.
 - * **Bluetooth** 공유 허용: 선택을 취소할 경우 사용자가 장치에서 나가는 Bluetooth 공유를 설정할 수 없습니다. 기본값은 선택되어 있습니다. 이 설정을 표시하려면 서버 속성 ([afw.restriction.policy.v2](#)) 을 활성화합니다. 서버 속성에 대한 자세한 내용은 [서버 속성](#) 을 참조하십시오.
- 날짜 및 시간 구성 허용: 사용자가 장치에서 날짜 및 시간을 변경할 수 있습니다. 기본값은 켜짐입니다.
- 공장 기본값으로 재설정 허용: 사용자가 장치에서 공장 기본값으로 재설정을 수행할 수 있습니다. 기본값은 켜짐입니다.
- 장치 화면을 켜진 상태로 유지: 이 설정을 켜짐으로 설정하면 장치를 연결할 때 장치 화면이 켜진 상태로 유지됩니다. 기본값은 꺼짐입니다.
- **USB** 대용량 스토리지 허용: USB 연결을 통해 사용자의 장치와 컴퓨터 간에 대용량 데이터 파일을 전송할 수 있습니다. 기본값은 켜짐입니다.
- 마이크 허용: 사용자가 장치에서 마이크를 사용할 수 있습니다. 기본값은 켜짐입니다.
- 테더링 허용: 사용자가 휴대용 핫스팟을 구성하고 데이터를 테더링할 수 있습니다. 기본값은 꺼짐입니다.
- **Keyguard** 가 장치를 잠그지 않도록 방지: 켜짐일 경우 관리되는 장치 및 전용 장치 (COSU 장치라고도 함) 의 잠금 화면에서 Keyguard 가 사용되지 않습니다. 기본값은 꺼짐입니다.
- **Wi-Fi** 변경 허용: 켜짐일 경우 사용자가 Wi-Fi 를 켜거나 끄고 Wi-Fi 네트워크에 연결할 수 있습니다. 기본값은 켜짐입니다.
- 파일 전송 허용: USB 를 통한 파일 전송을 허용합니다. 기본값은 꺼짐입니다.

• Samsung

- **TIMA** 키 저장소 사용: TIMA 키 저장소는 대칭 키에 대한 TrustZone 기반의 보안 키 저장소를 제공합니다. RSA 키 쌍 및 인증서는 저장을 위해 기본 키 저장소 공급자로 라우팅됩니다. 기본값은 꺼짐입니다.
- 공유 목록 허용: 사용자가 공유 방법 목록의 앱 간에 콘텐츠를 공유할 수 있습니다. 기본값은 켜짐입니다.
- 감사 로그 사용: 장치의 법의학 분석을 위한 이벤트 감사 로그 만들기를 사용하도록 설정합니다. 기본값은 꺼짐입니다.

• Samsung: 완전 관리형 장치만

- **ODE** 신뢰할 수 있는 부팅 확인 사용: ODE 신뢰할 수 있는 부팅 확인을 사용하여 bootloader 에서 시스템 이미지까지 신뢰 체인을 설정합니다. 기본값은 켜짐입니다.
- 긴급 호출만 허용: 사용자가 장치에서 긴급 통화 전용 모드를 사용할 수 있습니다. 기본값은 꺼짐입니다.
- 펌웨어 복구 허용: 사용자가 장치에서 펌웨어를 복구할 수 있습니다. 기본값은 켜짐입니다.
- 빠른 암호화 허용: 사용된 메모리 공간의 암호화만 허용합니다. 이 암호화는 모든 데이터를 암호화하는 전체 디스크 암호화와 대조됩니다. 이 데이터에는 설정, 응용 프로그램 데이터, 다운로드한 파일 및 응용 프로그램, 미디어 및 기타 파일이 포함됩니다. 기본값은 켜짐입니다.
- **Common Criteria** 모드 사용: 장치를 Common Criteria 모드로 전환합니다. Common Criteria 구성은 엄격한 보안 프로세스를 적용합니다. 기본값은 켜짐입니다.
- 재부팅 배너 사용: 사용자의 장치가 다시 시작되면 DoD 에서 승인 시스템 사용 알림 메시지 또는 배너를 표시합니다. 기본값은 꺼짐입니다.
- 설정 변경 허용: 사용자가 완전 관리형 장치에서 설정을 변경할 수 있습니다. 기본값은 켜짐입니다.

- 백그라운드 데이터 사용 활성화: 완전히 관리되는 장치의 경우 앱이 백그라운드에서 데이터를 동기화할 수 있습니다. 기본값은 켜짐입니다.
- 클립보드 허용: 사용자가 장치의 클립보드에 데이터를 복사할 수 있도록 허용합니다.
 - * 클립보드 공유 허용: 사용자가 장치와 컴퓨터 간에서 클립보드 콘텐츠를 공유할 수 있도록 허용합니다 (MDM 4.0 이상).
- 홈 키 허용: 사용자가 완전 관리형 장치에서 홈 키를 사용할 수 있습니다. 기본값은 켜짐입니다.
- 모의 위치 허용: 사용자가 GPS 위치를 조작할 수 있습니다. 완전 관리형 장치에 사용할 수 있습니다. 기본값은 꺼짐입니다.
- **NFC**: 사용자가 완전 관리형 장치에서 NFC 를 사용할 수 있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- 전원 끄기 허용: 사용자가 완전 관리형 장치를 끌 수 있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- **Wi-Fi Direct** 허용: 사용자가 Wi-Fi 연결을 통해 다른 장치에 직접 연결할 수 있습니다. 기본값은 켜짐입니다. 켜짐인 경우 **Wi-Fi** 변경 허용 설정을 사용하도록 설정해야 합니다.
- **SD** 카드 허용: 가능한 경우 사용자가 장치에서 SD 카드를 사용할 수 있습니다. 기본값은 켜짐입니다.
- **USB** 호스트 스토리지 허용: USB 장치가 연결될 때 사용자의 장치가 USB 호스트로 작동할 수 있도록 허용합니다. 그러면 사용자의 장치가 USB 장치에 전원을 공급합니다. 기본값은 켜짐입니다.
- 음성 다이얼 허용: 사용자가 장치에서 음성 다이얼을 사용할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **S Beam** 허용: 사용자가 NFC 및 Wi-Fi Direct 를 사용하여 다른 사용자와 콘텐츠를 공유할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **S Voice** 허용: 사용자가 장치에서 지능형 개인 비서 및 지식 탐색기를 사용할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **USB** 테더링 허용: 사용자가 USB 연결을 사용하여 다른 장치와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 테더링 허용 설정도 켜짐이어야 합니다.
- **Bluetooth** 테더링 허용: 사용자가 Bluetooth 연결을 사용하여 다른 장치와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 테더링 허용 설정도 켜짐이어야 합니다.
 - * **Bluetooth** 공유 허용: 선택을 취소할 경우 사용자가 장치에서 나가는 Bluetooth 공유를 설정할 수 없습니다. 기본값은 선택되어 있습니다. 이 설정을 표시하려면 서버 속성 ([afw.restriction.policy.v2](#)) 을 활성화합니다. 서버 속성에 대한 자세한 내용은 [서버 속성](#)을 참조하십시오.
- **Wi-Fi** 테더링 허용: 사용자가 Wi-Fi 연결을 사용하여 다른 장치와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 테더링 허용 설정도 켜짐이어야 합니다.
- 들어오는 **MMS** 허용: 사용자가 MMS 메시지를 받을 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.
- 나가는 **MMS** 허용: 사용자가 MMS 메시지를 보낼 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.
- 들어오는 **SMS** 허용: 사용자가 SMS 메시지를 받을 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.
- 나가는 **SMS** 허용: 사용자가 SMS 메시지를 보낼 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.
- 모바일 네트워크 구성: 사용자가 셀룰러 데이터 연결을 사용할 수 있도록 허용합니다. 기본값은 꺼짐입니다.
- 일별 제한 (**MB**): 사용자가 하루에 사용할 수 있는 모바일 데이터의 양 (MB) 을 입력합니다. 기본값은 이 기능은

비활성화하는 0 입니다 (MDM 4.0 이상).

- 주별 제한 (**MB**): 사용자가 한 주에 사용할 수 있는 모바일 데이터의 양 (MB) 을 입력합니다. 기본값은 이 기능은 비활성화하는 0 입니다 (MDM 4.0 이상).
- 월별 제한 (**MB**): 사용자가 한 달에 사용할 수 있는 모바일 데이터의 양 (MB) 을 입력합니다. 기본값은 이 기능은 비활성화하는 0 입니다 (MDM 4.0 이상).
- 보안 **VPN** 통신만 허용: 사용자가 보안 연결만 사용할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- 오디오 녹음 허용: 사용자가 장치에서 오디오를 녹음할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다. 켜짐인 경우 마이크 허용 설정을 켜야 합니다.
- 비디오 녹화 허용: 사용자가 장치에서 비디오를 녹화할 수 있습니다 (MDM 4.0 이상). 기본값은 꺼짐입니다. 꺼짐인 경우 카메라 사용 허용 설정을 켜야 합니다.
- 로밍 시 푸시 메시지 허용: 사용자가 푸시에 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 데이터 로밍 허용 설정을 사용하도록 설정해야 합니다.
- 로밍 시 자동 동기화 허용: 사용자가 동기화에 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 데이터 로밍 허용 설정을 사용하도록 설정해야 합니다.
- 로밍 시 음성 통화 허용: 사용자가 음성 통화에 셀룰러 데이터를 사용할 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 데이터 로밍 허용 설정을 사용하도록 설정해야 합니다.

• **Samsung: Knox** 컨테이너/완전 관리형 장치

- 해지 확인 사용: 해지된 인증서를 확인할 수 있습니다. 기본값은 꺼짐입니다.

• **Samsung: Knox** 컨테이너만

- 앱을 컨테이너로 이동: 사용자가 Knox 컨테이너와 장치의 개인 영역 간에서 앱을 이동할 수 있습니다. 기본값은 켜짐입니다.
- 다단계 인증 적용: 사용자는 지문과 함께 암호 또는 PIN 과 같은 다른 인증 방법을 사용하여 장치를 열어야 합니다. 기본값은 켜짐입니다.
- 컨테이너에 대한 인증 적용: 장치의 잠금을 해제하는 데 사용되는 방법과 다른 인증 방법을 사용하여 KNOX 컨테이너를 여십시오. 기본값은 켜짐입니다.
- 보안 키패드 사용: 사용자가 Knox 컨테이너 내부의 보안 키보드를 사용하도록 강제합니다. 기본값은 켜짐입니다.

• **Samsung: DeX**

- **Samsung DeX** 사용: 지원되는 Knox 지원 장치가 Samsung DeX 모드에서 실행되도록 합니다. Samsung Knox 3.1(최소 버전) 이 필요합니다. 기본값은 켜짐입니다. Samsung DeX 장치 요구 사항 및 Samsung DeX 설정 방법에 대한 자세한 내용은 Samsung 개발자 문서를 참조하십시오.
 - * **DeX** 모드에서만 인터넷 허용: Samsung DeX 모드에서 인터넷을 사용하도록 설정합니다 DeX 모드에서는 셀룰러 데이터, Wi-Fi, 테더링 (Wi-Fi, Bluetooth 및 USB) 이 제한됩니다. 기본값은 선택되어 있지 않습니다.
 - * **DeX** 로고 이미지 업로드: Samsung DeX 아이콘으로 사용할.png 이미지를 지정하려면 이 설정을 선택합니다.
 - * **DeX** 화면 시간 초과 (초): DeX 화면이 꺼질 때까지의 유효 시간 (초) 을 지정합니다. 시간 초과를 비활성화하려면 0 을 입력합니다. 기본값은 1200 초 (20 분) 입니다.

- ★ **Samsung DeX** 앱에서 앱 바로가기 추가: 앱 패키지 이름을 지정하여 앱 바로 가기를 DeX 파일에 추가합니다. 앱 패키지 이름을 조회하려면 Google Play 로 이동하여 앱을 선택합니다. URL 에는 패키지 이름 (<https://play.google.com/store/apps/details?id=<package.name><!--NeedCopy-->>) 이 포함됩니다.
- ★ **Samsung DeX** 앱에서 앱 바로 가기 제거: 앱 패키지 이름을 지정하여 DeX 에서 바로 가기를 제거합니다. 앱 패키지 이름을 조회하려면 Google Play 로 이동합니다.
- ★ **Samsung DeX** 모드에서 비활성화할 앱 패키지: Samsung DeX 모드에서 차단할 앱 패키지의 심프로 구분된 목록을 지정합니다. 예: `"com.android.chrome"`, `"com.google.android.gm"<!--NeedCopy-->`.

작업 프로필로 완전히 관리되는 장치에 적용이 커짐이고 작업 프로필이 있는 완전히 관리되는 장치의 경우 정책을 다음 항목에 적용이 작업 프로필로 설정된 경우 다음 설정을 구성합니다.

• 보안

- 계정 관리 허용: 작업 프로필 및 관리되는 장치에 계정을 추가할 수 있습니다. 기본값은 꺼짐입니다.
- 상호 프로필 복사 및 붙여넣기 허용: 커짐일 경우 사용자는 Android Enterprise 프로필의 앱과 개인 영역의 앱 사이에 복사해서 붙여넣을 수 있습니다. 기본값은 꺼짐입니다.
- 화면 캡처 허용: 사용자가 장치 화면의 화면 캡처를 기록하거나 생성할 수 있습니다. 기본값은 꺼짐입니다.
- 카메라 사용 허용: 사용자가 장치 카메라로 사진을 찍고 비디오를 만들 수 있습니다. 기본값은 꺼짐입니다.
- 위치 공급자 구성 허용: 사용자가 자신의 장치에서 GPS 를 켤 수 있습니다. Android API 28 이상을 위한 설정입니다. 기본값은 켜짐입니다.
- 위치 공유 허용: 관리되는 프로필의 경우 장치 소유자가 이 설정을 재정의할 수 있습니다. 기본값은 꺼짐입니다.

팁:

XenMobile 에서 위치 장치 정책을 만들어 지리적 경계를 적용할 수 있습니다. [위치 장치 정책](#)을 참조하십시오.

- 사용자가 사용자 자격 증명을 구성하도록 허용: 사용자가 관리형 키 저장소의 자격 증명을 구성할 수 있는지 여부를 지정합니다. 기본값은 켜짐입니다.
- 인쇄 허용: 커짐인 경우 이 설정은 사용자가 사용자 장치에서 액세스할 수 있는 모든 프린터로 인쇄할 수 있도록 허용합니다. 기본값은 꺼짐입니다. Android 9 이상에서 사용할 수 있습니다.

• 앱

- 시스템 앱 사용: 사용자가 사전 설치된 장치 앱을 실행할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 특정 앱을 사용하려면 시스템 앱 목록 테이블에서 추가를 클릭합니다.
 - ★ 시스템 앱 목록: 장치에서 사용할 시스템 앱 목록입니다. 시스템 앱 사용을 커짐으로 설정하고 앱 패키지 이름을 추가합니다. 시스템 앱의 패키지 이름을 조회하려면 Android Debug Bridge(`adb`)를 사용하여 Android 패키지 관리자 (`pm`) 명령을 호출하면 됩니다. 예: `adb shell "pm list packages -f name"`. 여기서 “name” 은 패키지 이름의 일부입니다. 자세한 내용

은 <https://developer.android.com/studio/command-line/adb> 항목을 참조하십시오.
Android Enterprise 기기의 경우 [Android Enterprise 앱 권한](#) 정책을 사용하여 앱 권한을 제한할 수 있습니다.

- 응용 프로그램 사용 안 함: 장치에서 지정된 목록의 앱이 실행되지 않도록 차단합니다. 기본값은 꺼짐입니다. 설치된 앱을 사용하지 않도록 설정하려면 설정을 켜짐으로 변경한 다음 응용 프로그램 목록 테이블에서 추가를 클릭합니다.
 - * 응용 프로그램 목록: 차단하려는 앱의 목록입니다. 응용 프로그램 사용 안 함을 켜짐으로 설정하고 앱을 추가합니다. 앱 패키지 이름을 입력합니다. 앱 목록을 변경하고 배포하면 이전 앱 목록을 덮어씁니다. 예: com.example1 및 com.example2 를 사용하지 않도록 설정하고 나중에 com.example1 및 com.example3 으로 목록을 변경하는 경우 XenMobile 은 com.example.2 를 사용하도록 설정합니다.
- 앱 확인 사용: OS 에서 앱을 검사하여 악성 동작을 검색할 수 있도록 합니다. 기본값은 켜짐입니다.
- **Google** 앱 사용: 사용자가 Google 모바일 서비스에서 컨테이너로 앱을 다운로드할 수 있습니다. 기본값은 켜짐입니다.
- **Google Play** 이외의 앱 허용: Google Play 이외의 스토어에서 앱을 설치할 수 있습니다. 기본값은 꺼짐입니다.
- 응용 프로그램 설정의 사용자 제어 허용: 사용자가 앱을 제거하고, 앱을 사용하지 않도록 설정하고, 캐시 및 데이터를 지우고, 앱을 강제로 중지하고, 기본값을 지울 수 있습니다. 사용자는 설정 앱에서 이러한 작업을 수행합니다. 기본값은 꺼짐입니다.
- 앱 제거 허용: 사용자가 관리되는 Google Play 스토어 내에서 앱을 제거하도록 허용합니다. 기본값은 꺼짐입니다. 이 설정을 표시하려면 서버 속성 ([afw.restriction.policy.v2](#)) 을 활성화합니다. 서버 속성에 대한 자세한 내용은 [서버 속성](#)을 참조하십시오.

• BYOD 작업 프로필

- 홈 화면에 작업 프로필 앱 위젯 허용: 이 설정이 켜짐인 경우 사용자가 작업 프로필 앱 위젯을 장치 홈 화면에 배치할 수 있습니다. 이 설정이 꺼짐인 경우 사용자가 작업 프로필 앱 위젯을 장치 홈 화면에 배치할 수 없습니다. 기본값은 꺼짐입니다.
 - * 위젯이 허용되는 앱: 홈 화면에서 허용할 앱 목록입니다. 홈 화면에 작업 프로필 앱 위젯 허용을 켜짐으로 설정하고 앱을 추가합니다. 추가를 클릭하고 목록에서 홈 화면에 허용할 위젯의 앱을 선택합니다. 저장을 클릭합니다. 더 많은 앱 위젯을 허용하려면 이 프로세스를 반복합니다.
- 장치 연락처에 작업 프로필 연락처 허용: 수신 전화에 대해 관리되는 Android Enterprise 프로필에 있는 연락처가 상위 프로필에 표시됩니다 (Android 7.0 이상). 기본값은 꺼짐입니다.

• Samsung

- **TIMA** 키 저장소 사용: TIMA 키 저장소는 대칭 키에 대한 TrustZone 기반의 보안 키 저장소를 제공합니다. RSA 키 쌍 및 인증서는 저장을 위해 기본 키 저장소 공급자로 라우팅됩니다. 기본값은 꺼짐입니다.
- 공유 목록 허용: 사용자가 공유 방법 목록의 앱 간에서 콘텐츠를 공유할 수 있습니다. 기본값은 켜짐입니다.
- 감사 로그 사용: 장치의 법의학 분석을 위한 이벤트 감사 로그 만들기를 사용하도록 설정합니다. 기본값은 꺼짐입니다.

- **Samsung: Knox** 컨테이너/완전 관리형 장치

- 해지 확인 사용: 해지된 인증서를 확인할 수 있습니다. 기본값은 꺼짐입니다.

- **Samsung: Knox** 컨테이너만

- 앱을 컨테이너로 이동: 사용자가 Knox 컨테이너와 장치의 개인 영역 간에서 앱을 이동할 수 있습니다. 기본값은 꺼짐입니다.
- 다단계 인증 적용: 사용자는 지문과 함께 암호 또는 PIN 과 같은 다른 인증 방법을 사용하여 장치를 열어야 합니다. 기본값은 꺼짐입니다.
- 컨테이너에 대한 인증 적용: 장치의 잠금을 해제하는 데 사용되는 방법과 다른 인증 방법을 사용하여 KNOX 컨테이너를 여십시오. 기본값은 꺼짐입니다.
- 보안 키패드 사용: 사용자가 Knox 컨테이너 내부의 보안 키보드를 사용하도록 강제합니다. 기본값은 꺼짐입니다.

작업 프로파일로 완전히 관리되는 장치에 적용이 꺼짐이고 작업 프로필이 있는 완전히 관리되는 장치의 경우 정책을 다음 항목에 적용이 관리되는 장치로 설정된 경우 다음 설정을 구성합니다.

- 보안

- 계정 관리 허용: 작업 프로필 및 관리되는 장치에 계정을 추가할 수 있습니다. 기본값은 꺼짐입니다.
- 상호 프로필 복사 및 붙여넣기 허용: 꺼짐일 경우 사용자는 Android Enterprise 프로필의 앱과 개인 영역의 앱 사이에 복사해서 붙여넣을 수 있습니다. 기본값은 꺼짐입니다.
- 화면 캡처 허용: 사용자가 장치 화면의 화면 캡처를 기록하거나 생성할 수 있습니다. 기본값은 꺼짐입니다.
- 카메라 사용 허용: 사용자가 장치 카메라로 사진을 찍고 비디오를 만들 수 있습니다. 기본값은 꺼짐입니다.
- VPN 구성 허용: 사용자가 VPN 구성을 만들 수 있습니다. Android 6 이상을 실행하는 작업 프로필 장치와 완전 관리형 장치를 위한 설정입니다. 기본값은 꺼짐입니다.
- 백업 서비스 허용: 사용자가 장치에서 응용 프로그램 및 시스템 데이터를 백업할 수 있습니다. 기본값은 꺼짐입니다.
- NFC 허용: 사용자가 NFC(근거리 통신) 를 사용하여 장치의 웹 페이지, 사진, 비디오 또는 기타 콘텐츠를 다른 장치로 보낼 수 있도록 허용합니다. MDM 4.0 이상에 해당합니다. 기본값은 꺼짐입니다.
- 위치 공급자 구성 허용: 사용자가 자신의 장치에서 GPS 를 켤 수 있습니다. Android API 28 이상을 위한 설정입니다. 기본값은 꺼짐입니다.
- 위치 공유 허용: 관리되는 프로필의 경우 장치 소유자가 이 설정을 재정의할 수 있습니다. 기본값은 꺼짐입니다.

팁:

XenMobile 에서 위치 장치 정책을 만들어 지리적 경계를 적용할 수 있습니다. [위치 장치 정책](#)을 참조하십시오.

- 사용자가 사용자 자격 증명을 구성하도록 허용: 사용자가 관리형 키 저장소의 자격 증명을 구성할 수 있는지 여부를 지정합니다. 기본값은 꺼짐입니다.

- 인쇄 허용: 커짐인 경우 이 설정은 사용자가 사용자 장치에서 액세스할 수 있는 모든 프린터로 인쇄할 수 있도록 허용합니다. 기본값은 꺼짐입니다. Android 9 이상에서 사용할 수 있습니다.
- **USB 디버깅 허용:** 기본값은 꺼짐입니다.

• 앱

- 시스템 앱 사용: 사용자가 사전 설치된 장치 앱을 실행할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 특정 앱을 사용하려면 시스템 앱 목록 테이블에서 추가를 클릭합니다.
 - * 시스템 앱 목록: 장치에서 사용할 시스템 앱 목록입니다. 시스템 앱 사용을 커짐으로 설정하고 앱 패키지 이름을 추가합니다. 시스템 앱의 패키지 이름을 조회하려면 Android Debug Bridge([adb](#))를 사용하여 Android 패키지 관리자 (`pm`) 명령을 호출하면 됩니다. 예: `adb shell "pm list packages -f name"`. 여기서 “name”은 패키지 이름의 일부입니다. 자세한 내용은 <https://developer.android.com/studio/command-line/adb> 항목을 참조하십시오. Android Enterprise 기기의 경우 [Android Enterprise 앱 권한](#) 정책을 사용하여 앱 권한을 제한할 수 있습니다.
- 응용 프로그램 사용 안 함: 장치에서 지정된 목록의 앱이 실행되지 않도록 차단합니다. 기본값은 꺼짐입니다. 설치된 앱을 사용하지 않도록 설정하려면 설정을 커짐으로 변경한 다음 응용 프로그램 목록 테이블에서 추가를 클릭합니다.
 - * 응용 프로그램 목록: 차단하려는 앱의 목록입니다. 응용 프로그램 사용 안 함을 커짐으로 설정하고 앱을 추가합니다. 앱 패키지 이름을 입력합니다. 앱 목록을 변경하고 배포하면 이전 앱 목록을 덮어씁니다. 예: com.example1 및 com.example2를 사용하지 않도록 설정하고 나중에 com.example1 및 com.example3으로 목록을 변경하는 경우 XenMobile은 com.example.2를 사용하도록 설정합니다.
- 앱 확인 사용: OS에서 앱을 검사하여 악성 동작을 검색할 수 있도록 합니다. 기본값은 커짐입니다.
- **Google 앱 사용:** 사용자가 Google 모바일 서비스에서 컨테이너로 앱을 다운로드할 수 있습니다. 기본값은 커짐입니다.
- **Google Play 이외의 앱 허용:** Google Play 이외의 스토어에서 앱을 설치할 수 있습니다. 기본값은 꺼짐입니다.
- 응용 프로그램 설정의 사용자 제어 허용: 사용자가 앱을 제거하고, 앱을 사용하지 않도록 설정하고, 캐시 및 데이터를 지우고, 앱을 강제로 중지하고, 기본값을 지울 수 있습니다. 사용자는 설정 앱에서 이러한 작업을 수행합니다. 기본값은 꺼짐입니다.
- 앱 제거 허용: 사용자가 관리되는 Google Play 스토어 내에서 앱을 제거하도록 허용합니다. 기본값은 꺼짐입니다. 이 설정을 표시하려면 서버 속성 ([afw.restriction.policy.v2](#))을 활성화합니다. 서버 속성에 대한 자세한 내용은 [서버 속성](#)을 참조하십시오.

• 완전 관리형 장치만

- 사용자 추가 허용: 사용자가 장치에 새 사용자를 추가할 수 있도록 허용합니다. 기본값은 커짐입니다.
- 데이터 로밍 허용: 로밍하는 동안 사용자가 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐이며, 사용자의 장치에서 로밍이 비활성화됩니다. 기본값은 꺼짐입니다.
- **SMS 허용:** 사용자가 SMS 메시지를 보내고 받을 수 있습니다. 기본값은 꺼짐입니다.

- 상태 표시줄의 사용 허용: 커짐인 경우 관리되는 장치 및 전용 장치 (COSU 장치라고도 함) 에서 상태 표시줄이 사용됩니다. 이렇게 설정하면 알림, 빠른 설정 및 전체 화면 모드에서 벗어날 수 있는 기타 화면 오버레이가 사용되지 않습니다. 사용자는 시스템 설정으로 이동하여 알림을 볼 수 있습니다. Android 6.0 이상을 위한 설정입니다. 기본값은 꺼짐입니다.
- **Bluetooth** 허용: 사용자가 Bluetooth 를 사용할 수 있습니다. 기본값은 커짐입니다.
 - * **Bluetooth** 공유 허용: 선택을 취소할 경우 사용자가 장치에서 나가는 Bluetooth 공유를 설정할 수 없습니다. 기본값은 선택되어 있습니다. 이 설정을 표시하려면 서버 속성 (`afw.restriction.policy.v2`) 을 활성화합니다. 서버 속성에 대한 자세한 내용은 [서버 속성](#) 을 참조하십시오.
- 날짜 및 시간 구성 허용: 사용자가 장치에서 날짜 및 시간을 변경할 수 있습니다. 기본값은 커짐입니다.
- 공장 기본값으로 재설정 허용: 사용자가 장치에서 공장 기본값으로 재설정을 수행할 수 있습니다. 기본값은 커짐입니다.
- 장치 화면을 켜진 상태로 유지: 이 설정을 커짐으로 설정하면 장치를 연결할 때 장치 화면이 켜진 상태로 유지됩니다. 기본값은 꺼짐입니다.
- **USB** 대용량 스토리지 허용: USB 연결을 통해 사용자의 장치와 컴퓨터 간에 대용량 데이터 파일을 전송할 수 있습니다. 기본값은 커짐입니다.
- 마이크 허용: 사용자가 장치에서 마이크를 사용할 수 있습니다. 기본값은 커짐입니다.
- 테더링 허용: 사용자가 휴대용 핫스팟을 구성하고 데이터를 테더링할 수 있습니다. 기본값은 꺼짐입니다. 이 설정이 켜져 있으면 Samsung 장치에서 다음 설정을 사용할 수 있습니다.
- **Keyguard** 가 장치를 잠그지 않도록 방지: 커짐일 경우 관리되는 장치 및 전용 장치 (COSU 장치라고도 함) 의 잠금 화면에서 Keyguard 가 사용되지 않습니다. 기본값은 꺼짐입니다.
- **Wi-Fi** 변경 허용: 커짐인 경우 사용자가 Wi-Fi 를 켜거나 끄고 Wi-Fi 네트워크에 연결할 수 있습니다. 기본값은 커짐입니다.
- 파일 전송 허용: USB 를 통한 파일 전송을 허용합니다. 기본값은 꺼짐입니다.

• Samsung

- **TIMA** 키 저장소 사용: TIMA 키 저장소는 대칭 키에 대한 TrustZone 기반의 보안 키 저장소를 제공합니다. RSA 키 쌍 및 인증서는 저장을 위해 기본 키 저장소 공급자로 라우팅됩니다. 기본값은 꺼짐입니다.
- 공유 목록 허용: 사용자가 공유 방법 목록의 앱 간에 콘텐츠를 공유할 수 있습니다. 기본값은 커짐입니다.
- 감사 로그 사용: 장치의 법의학 분석을 위한 이벤트 감사 로그 만들기를 사용하도록 설정합니다. 기본값은 꺼짐입니다.

• Samsung: 완전 관리형 장치만

- **ODE** 신뢰할 수 있는 부팅 확인 사용: ODE 신뢰할 수 있는 부팅 확인을 사용하여 bootloader 에서 시스템 이미지까지 신뢰 체인을 설정합니다. 기본값은 커짐입니다.
- 긴급 호출만 허용: 사용자가 장치에서 긴급 통화 전용 모드를 사용할 수 있습니다. 기본값은 꺼짐입니다.
- 펌웨어 복구 허용: 사용자가 장치에서 펌웨어를 복구할 수 있습니다. 기본값은 커짐입니다.
- 빠른 암호화 허용: 사용된 메모리 공간의 암호화만 허용합니다. 이 암호화는 모든 데이터를 암호화하는 전체 디스크 암호화와 대조됩니다. 이 데이터에는 설정, 응용 프로그램 데이터, 다운로드한 파일 및 응용 프로그램, 미디어 및 기타 파일이 포함됩니다. 기본값은 커짐입니다.

- **Common Criteria** 모드 사용: 장치를 Common Criteria 모드로 전환합니다. Common Criteria 구성은 엄격한 보안 프로세스를 적용합니다. 기본값은 켜짐입니다.
- 재부팅 배너 사용: 사용자의 장치가 다시 시작되면 DoD 에서 승인 시스템 사용 알림 메시지 또는 배너를 표시합니다. 기본값은 꺼짐입니다.
- 설정 변경 허용: 사용자가 완전 관리형 장치에서 설정을 변경할 수 있습니다. 기본값은 켜짐입니다.
- 백그라운드 데이터 사용 활성화: 완전히 관리되는 장치의 경우 앱이 백그라운드에서 데이터를 동기화할 수 있습니다. 기본값은 켜짐입니다.
- 클립보드 허용: 사용자가 장치의 클립보드에 데이터를 복사할 수 있도록 허용합니다. 기본값은 켜짐입니다.
 - * 클립보드 공유 허용: 사용자가 장치와 컴퓨터 간에서 클립보드 콘텐츠를 공유할 수 있도록 허용합니다 (MDM 4.0 이상).
- 홈 키 허용: 사용자가 완전 관리형 장치에서 홈 키를 사용할 수 있습니다. 기본값은 켜짐입니다.
- 모의 위치 허용: 사용자가 GPS 위치를 조작할 수 있습니다. 완전 관리형 장치에 사용할 수 있습니다. 기본값은 꺼짐입니다.
- **NFC**: 사용자가 완전 관리형 장치에서 NFC 를 사용할 수 있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- 전원 끄기 허용: 사용자가 완전 관리형 장치를 끌 수 있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- **Wi-Fi Direct** 허용: 사용자가 Wi-Fi 연결을 통해 다른 장치에 직접 연결할 수 있습니다. 기본값은 켜짐입니다. 켜짐인 경우 **Wi-Fi** 변경 허용 설정을 사용하도록 설정해야 합니다.
- **SD** 카드 허용: 가능한 경우 사용자가 장치에서 SD 카드를 사용할 수 있습니다. 기본값은 켜짐입니다.
- **USB** 호스트 스토리지 허용: USB 장치가 연결될 때 사용자의 장치가 USB 호스트로 작동할 수 있도록 허용합니다. 그러면 사용자의 장치가 USB 장치에 전원을 공급합니다. 기본값은 켜짐입니다.
- 음성 다이얼 허용: 사용자가 장치에서 음성 다이얼을 사용할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **S Beam** 허용: 사용자가 NFC 및 Wi-Fi Direct 를 사용하여 다른 사용자와 콘텐츠를 공유할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **S Voice** 허용: 사용자가 장치에서 지능형 개인 비서 및 지식 탐색기를 사용할 수 있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **USB** 테더링 허용: 사용자가 USB 연결을 사용하여 다른 장치와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 테더링 허용 설정도 켜짐이어야 합니다.
- **Bluetooth** 테더링 허용: 사용자가 Bluetooth 연결을 사용하여 다른 장치와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 테더링 허용 설정도 켜짐이어야 합니다.
- **Wi-Fi** 테더링 허용: 사용자가 Wi-Fi 연결을 사용하여 다른 장치와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 테더링 허용 설정도 켜짐이어야 합니다.
- 들어오는 **MMS** 허용: 사용자가 MMS 메시지를 받을 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.
- 나가는 **MMS** 허용: 사용자가 MMS 메시지를 보낼 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.
- 들어오는 **SMS** 허용: 사용자가 SMS 메시지를 받을 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.
- 나가는 **SMS** 허용: 사용자가 SMS 메시지를 보낼 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 **SMS** 허용 설정을 켜야 합니다.

- 모바일 네트워크 구성: 사용자가 셀룰러 데이터 연결을 사용할 수 있도록 허용합니다. 기본값은 꺼짐입니다.
- 일별 제한 (**MB**): 사용자가 하루에 사용할 수 있는 모바일 데이터의 양 (MB) 을 입력합니다. 기본값은 이 기능은 비활성화하는 0 입니다 (MDM 4.0 이상).
- 주별 제한 (**MB**): 사용자가 한 주에 사용할 수 있는 모바일 데이터의 양 (MB) 을 입력합니다. 기본값은 이 기능은 비활성화하는 0 입니다 (MDM 4.0 이상).
- 월별 제한 (**MB**): 사용자가 한 달에 사용할 수 있는 모바일 데이터의 양 (MB) 을 입력합니다. 기본값은 이 기능은 비활성화하는 0 입니다 (MDM 4.0 이상).
- 보안 **VPN** 통신만 허용: 사용자가 보안 연결만 사용할 수 있습니다 (MDM 4.0 이상). 기본값은 꺼짐입니다.
- 오디오 녹음 허용: 사용자가 장치에서 오디오를 녹음할 수 있습니다 (MDM 4.0 이상). 기본값은 꺼짐입니다. 꺼짐인 경우 마이크 허용 설정을 켜야 합니다.
- 비디오 녹화 허용: 사용자가 장치에서 비디오를 녹화할 수 있습니다 (MDM 4.0 이상). 기본값은 꺼짐입니다. 꺼짐인 경우 카메라 사용 허용 설정을 켜야 합니다.
- 로밍 시 푸시 메시지 허용: 사용자가 푸시에 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 데이터 로밍 허용 설정을 사용하도록 설정해야 합니다.
- 로밍 시 자동 동기화 허용: 사용자가 동기화에 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 켜짐인 경우 데이터 로밍 허용 설정을 사용하도록 설정해야 합니다.
- 로밍 시 음성 통화 허용: 사용자가 음성 통화에 셀룰러 데이터를 사용할 수 있습니다. 기본값은 꺼짐입니다. 켜짐인 경우 데이터 로밍 허용 설정을 사용하도록 설정해야 합니다.

- **Samsung: Knox** 컨테이너/완전 관리형 장치

- 해지 확인 사용: 해지된 인증서를 확인할 수 있습니다. 기본값은 꺼짐입니다.

- **Samsung: Knox** 컨테이너만

- 앱을 컨테이너로 이동: 사용자가 Knox 컨테이너와 장치의 개인 영역 간에서 앱을 이동할 수 있습니다. 기본값은 켜짐입니다.
- 다단계 인증 적용: 사용자는 지문과 함께 암호 또는 PIN 과 같은 다른 인증 방법을 사용하여 장치를 열어야 합니다. 기본값은 켜짐입니다.
- 컨테이너에 대한 인증 적용: 장치의 잠금을 해제하는 데 사용되는 방법과 다른 인증 방법을 사용하여 KNOX 컨테이너를 여십시오. 기본값은 켜짐입니다.
- 보안 키패드 사용: 사용자가 Knox 컨테이너 내부의 보안 키보드를 사용하도록 강제합니다. 기본값은 켜짐입니다.

Windows 데스크톱/태블릿 설정

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
Restrictions This policy allows or restricts the use of certain features on user devices, such as the camera. You can also set security restrictions, restrictions on media content, and the types of apps users can and can't install.						
Wi-Fi settings Allow internet sharing <input checked="" type="checkbox"/>						
Connectivity Allow VPN over cellular <input checked="" type="checkbox"/> Allow VPN over cellular while roaming <input checked="" type="checkbox"/> Allow cellular data roaming <input checked="" type="checkbox"/>						
Accounts Allow Microsoft account connection <input type="checkbox"/> Allow non-Microsoft email <input type="checkbox"/>						

• WiFi 설정

- 인터넷 공유 허용: 장치가 WiFi 핫스팟으로 전환되어 다른 장치와 인터넷 연결을 공유할 수 있도록 허용합니다.

• 연결

- 셀룰러를 통한 **VPN** 허용: 장치가 VPN 을 통해 셀룰러 네트워크에 연결할 수 있도록 허용합니다.
- 로밍하는 동안 셀룰러를 통한 **VPN** 허용: 장치가 셀룰러 네트워크를 통해 로밍할 때 장치가 VPN 을 통해 연결할 수 있도록 허용합니다.
- 셀룰러 데이터 로밍 허용: 로밍하는 동안 사용자가 셀룰러 데이터를 사용할 수 있도록 허용합니다.

• 계정

- **Microsoft** 계정 연결 허용: 장치가 전자 메일과 관련이 없는 연결 인증 및 서비스에 대해 Microsoft 계정을 사용할 수 있도록 허용합니다.
- **Microsoft** 이외의 전자 메일 허용: 사용자가 Microsoft 이외의 전자 메일 계정을 추가할 수 있도록 허용합니다.

• 시스템

- 스토리지 카드 허용: 장치가 스토리지 카드를 사용할 수 있도록 허용합니다.
- 원격 분석: 목록에서 옵션을 클릭하여 장치가 원격 분석 정보를 보내는 것을 허용하거나 제한합니다. 기본값은 허용입니다. 다른 옵션은 허용 안 함 및 허용, 보조 데이터 요청 제외입니다.
- 위치 서비스 허용: 위치 서비스를 허용합니다.
- 내부 빌드에 대한 미리 보기 허용: 사용자가 Microsoft 내부 빌드를 미리 볼 수 있도록 허용합니다.

• 카메라:

- 카메라 사용 허용: 사용자가 장치의 카메라를 사용할 수 있도록 허용합니다.

• Bluetooth:

- 검색 가능 모드 허용: Bluetooth 장치가 로컬 장치를 찾을 수 있도록 허용합니다.

- 로컬 장치 이름: 로컬 장치의 이름입니다.
- 경험:
 - **Cortana** 허용: 사용자가 지능형 개인 비서 및 지식 탐색기인 Cortana 에 액세스할 수 있도록 허용합니다.
 - 장치 검색 허용: 네트워크를 통한 장치 검색을 허용합니다.
 - **MDM** 수동 등록 해제 허용: 사용자가 수동으로 XenMobile MDM 에서 장치의 등록을 해제할 수 있도록 허용합니다.
 - 장치 설정 동기화 허용: 로밍 중에 사용자가 Windows 10 및 Windows 11 장치 간에서 설정을 동기화할 수 있도록 허용합니다.
- 위쪽 잠금:
 - 알림 허용: 잠금 화면에 알림 메시지를 허용합니다.
- 앱
 - 앱 스토어 자동 업데이트 허용: 앱 스토어에서 앱이 자동으로 업데이트되도록 허용합니다.
- 개인 정보:
 - 개인 설정 입력 허용: 입력 개인 설정 서비스가 실행되어 사용자의 입력 내용에 따라 펜 및 터치 키보드 등의 예측 입력을 개선할 수 있도록 허용합니다.
- 설정:
 - 자동 재생 허용: 사용자가 자동 재생 설정을 변경할 수 있도록 허용합니다.
 - 데이터 센스 허용: 사용자가 데이터 센스 설정을 변경할 수 있도록 허용합니다.
 - 날짜/시간 허용: 사용자가 날짜 및 시간 설정을 변경할 수 있도록 허용합니다.
 - 언어 허용: 사용자가 언어 설정을 변경할 수 있도록 허용합니다.
 - 절전 모드 허용: 사용자가 전원 및 절전 모드 설정을 변경할 수 있도록 허용합니다.
 - 지역 허용: 사용자가 지역 설정을 변경할 수 있도록 허용합니다.
 - 로그인 옵션 허용: 사용자가 로그인 설정을 변경할 수 있도록 허용합니다.
 - 회사 허용: 사용자가 회사 설정을 변경할 수 있도록 허용합니다.
 - 사용자 계정 허용: 사용자가 계정 설정을 변경할 수 있도록 허용합니다.

로밍 장치 정책

August 12, 2022

사용자의 iOS 장치에서 음성 및 데이터 로밍을 허용할 것인지 여부를 구성하는 장치 정책을 XenMobile 에서 추가할 수 있습니다. 음성 로밍을 사용하지 않도록 설정하면 데이터 로밍이 자동으로 비활성화됩니다. iOS 의 경우 iOS 5.0 이상의 장치에서만 이 정책을 사용할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- 음성 로밍 사용 안 함: 음성 로밍을 사용하지 않을 것인지 여부를 선택합니다. 이 옵션을 사용하도록 설정하면 데이터 로밍이 자동으로 비활성화됩니다. 기본값은 꺼짐, 즉 음성 로밍을 사용하는 것입니다.
- 데이터 로밍 사용 안 함: 데이터 로밍을 사용하지 않을 것인지 여부를 선택합니다. 이 옵션은 음성 로밍이 활성화된 경우에만 사용할 수 있습니다. 기본값은 꺼짐, 즉 데이터 로밍을 사용하는 것입니다.

SCEP 장치 정책

January 5, 2022

이 정책을 사용하면 SCEP(단순 인증서 등록 프로토콜)를 사용하여 외부 SCEP 서버에서 인증서를 검색하도록 iOS 및 macOS 장치를 구성할 수 있습니다. XenMobile 에 연결된 PKI 에서 SCEP 를 사용하여 장치에 인증서를 제공하려면 분산 모드에서 PKI 엔터티 및 PKI 공급자를 만들어야 합니다. 자세한 내용은 [PKI 엔터티](#)를 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

SCEP Policy	SCEP Policy This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.
1 Policy Info	URL base *
2 Platforms	Instance name *
<input checked="" type="checkbox"/> iOS	Subject X.500 name (RFC 2253)
<input checked="" type="checkbox"/> macOS	Subject alternative names type None
3 Assignment	Maximum retries 3
	Retry delay 10
	Challenge password
	Key size (bits) 1024
	Use as digital signature OFF
	Use for key encipherment OFF
	SHA1/MD5 fingerprint (hexadecimal string)

- **URL 기준:** HTTP 또는 HTTPS 를 통해 SCEP 요청을 전송할 SCEP 서버 주소를 입력합니다. 개인 키는 CSR(인증서 서명 요청) 로 전송되지 않으므로 요청을 암호화되지 않은 상태로 보내도 안전할 수 있습니다. 그러나 일회용 암호를 재사용하는 것이 허용되므로 HTTPS 를 사용하여 암호를 보호해야 합니다. 이 단계는 필수 단계입니다.
- **인스턴스 이름:** SCEP 서버가 인식하는 문자열을 입력합니다. 예를 들어 example.org 와 같은 도메인 이름을 입력할 수 있습니다. CA 에 여러 CA 인증서가 있는 경우 이 필드를 사용하여 필요한 도메인을 구분할 수 있습니다. 이 단계는 필수 단계입니다.

- 주체 **X.500** 이름 (**RFC 2253**): OID(개체 식별자) 및 값 배열로 나타나는 X.500 이름의 표현을 입력합니다. 예를 들어 /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 는 [[[“C” , “US”]], [[“O” , “Apple Inc.”]], ..., [[“1.2.5.3” , “bar”]]] 로 변환될 수 있습니다. 국가 (C), 지역 (L), 시/도 (ST), 조직 (O), 조직 구성 단위 (OU) 및 일반 이름 (CN) 에 대한 바로 가기가 포함된 점 형식 숫자로 OID 를 표현할 수 있습니다.
- 주체 대체 이름 유형: 목록에서 대체 이름 유형을 클릭합니다. SCEP 정책은 CA 의 인증서 발급에 필요한 값을 제공하는 선택적 대체 이름 유형을 지정할 수 있습니다. 없음, **RFC 822** 이름, **DNS** 이름 또는 **URI** 를 지정할 수 있습니다.
- 최대 재시도 횟수: SCEP 서버가 PENDING 응답을 보내는 경우 장치에서 재시도할 횟수를 입력합니다. 기본값은 **3** 입니다.
- 재시도 지연: 다음 재시도 전에 대기할 시간을 초로 입력합니다. 첫 번째 재시도는 지연 없이 시도됩니다. 기본값은 **10** 입니다.
- 챌린지 암호: 미리 공유한 암호를 입력합니다.
- 키 크기 (비트): **2048** 이상을 키 크기 (비트 단위) 로 선택합니다.
- 디지털 서명으로 사용: 인증서를 디지털 서명으로 사용할지 여부를 지정합니다. 인증서를 사용하여 디지털 서명을 확인하는 경우, 예를 들어 CA 에서 발급된 인증서인지 여부를 확인하는 경우 SCEP 서버가 공개 키를 사용하여 해시를 해독하기 전에 이 방식으로 인증서를 사용할 수 있는지 여부를 확인합니다.
- 키 암호화에 사용: 인증서를 키 암호화에 사용할지 여부를 지정합니다. 서버에서 클라이언트가 제공한 인증서의 공개 키를 사용하여 데이터가 개인 키를 사용하여 암호화되었는지 확인하는 경우 인증서를 키 암호화에 사용할 수 있는지 여부를 먼저 확인할 수 있습니다. 그렇지 않은 경우 작업에 실패합니다.
- **SHA1/MD5** 지문 (**16** 진수 문자열): CA 에서 HTTP 를 사용하는 경우 이 필드를 사용하여 CA 인증서 지문을 제공합니다. 이 지문은 등록 시 장치에서 CA 응답의 진위를 확인하는 데 사용됩니다. SHA1 또는 MD5 지문을 입력하거나 서명을 가져올 인증서를 선택할 수 있습니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

SCEP Policy

1 Policy Info

2 Platforms

☐ iOS

☒ macOS

3 Assignment

SCEP Policy

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.

URL base *

Instance name *

Subject X.500 name (RFC 2253)

Subject alternative names type

None

Maximum retries

3

Retry delay

10

Challenge password

Key size (bits)

1024

Use as digital signature

OFF

Use for key encipherment

OFF

SHA1/MD5 fingerprint (hexadecimal string)

- **URL 기준:** HTTP 또는 HTTPS 를 통해 SCEP 요청을 전송할 SCEP 서버 주소를 입력합니다. 개인 키는 CSR(인증서 서명 요청) 로 전송되지 않으므로 요청을 암호화되지 않은 상태로 보내도 안전할 수 있습니다. 그러나 일회용 암호를 재사용하는 것이 허용되므로 HTTPS 를 사용하여 암호를 보호해야 합니다. 이 단계는 필수 단계입니다.
- **인스턴스 이름:** SCEP 서버가 인식하는 문자열을 입력합니다. 예를 들어 example.org 와 같은 도메인 이름을 입력할 수 있습니다. CA 에 여러 CA 인증서가 있는 경우 이 필드를 사용하여 필요한 도메인을 구분할 수 있습니다. 이 단계는 필수 단계입니다.
- **주체 X.500 이름 (RFC 2253):** OID(개체 식별자) 및 값 배열로 나타나는 X.500 이름의 표현을 입력합니다. 예를 들어 /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 는 [[[“C” , “US”]], [[“O” , “Apple Inc.”]], …, [[“1.2.5.3” , “bar”]]] 로 변환될 수 있습니다. 국가 (C), 지역 (L), 시/도 (ST), 조직 (O), 조직 구성 단위 (OU) 및 일반 이름 (CN) 에 대한 바로 가기가 포함된 점 형식 숫자로 OID 를 표현할 수 있습니다.
- **주체 대체 이름 유형:** 목록에서 대체 이름 유형을 클릭합니다. SCEP 정책은 CA 의 인증서 발급에 필요한 값을 제공하는 선택적 대체 이름 유형을 지정할 수 있습니다. 없음, **RFC 822** 이름, **DNS** 이름 또는 **URI** 를 지정할 수 있습니다.
- **최대 재시도 횟수:** SCEP 서버가 PENDING 응답을 보내는 경우 장치에서 재시도할 횟수를 입력합니다. 기본값은 **3** 입니다.
- **재시도 지연:** 다음 재시도 전에 대기할 시간을 초로 입력합니다. 첫 번째 재시도는 지연 없이 시도됩니다. 기본값은 **10** 입니다.
- **챌린지 암호:** 미리 공유한 암호를 입력합니다.
- **키 크기 (비트):** **2048** 이상을 키 크기 (비트 단위) 로 선택합니다.
- **디지털 서명으로 사용:** 인증서를 디지털 서명으로 사용할지 여부를 지정합니다. 인증서를 사용하여 디지털 서명을 확인하는 경우, 예를 들어 CA 에서 발급된 인증서인지 여부를 확인하는 경우 SCEP 서버가 공개 키를 사용하여 해시를 해독하기

전에 이 방식으로 인증서를 사용할 수 있는지 여부를 확인합니다.

- 키 암호화에 사용: 인증서를 키 암호화에 사용할지 여부를 지정합니다. 서버에서 클라이언트가 제공한 인증서의 공개 키를 사용하여 데이터가 개인 키를 사용하여 암호화되었는지 확인하는 경우 인증서를 키 암호화에 사용할 수 있는지 여부를 먼저 확인할 수 있습니다. 그렇지 않은 경우 작업에 실패합니다.
- **SHA1/MD5 지문 (16 진수 문자열):** CA 에서 HTTP 를 사용하는 경우 이 필드를 사용하여 CA 인증서 지문을 제공합니다. 이 지문은 등록 시 장치에서 CA 응답의 진위를 확인하는 데 사용됩니다. SHA1 또는 MD5 지문을 입력하거나 서명을 가져올 인증서를 선택할 수 있습니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.
 - 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
 - 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Siri 및 받아쓰기 정책

January 5, 2022

사용자가 Siri 에 무언가를 요청하거나 관리되는 iOS 장치에서 텍스트를 받아쓰면 Apple 이 Siri 를 개선하기 위해 음성 데이터를 수집합니다. 이 음성 데이터는 Apple 의 클라우드 기반 서비스를 통과하므로 보안 XenMobile 컨테이너 외부에 있게 됩니다. 그러나 받아쓰기 결과인 텍스트는 컨테이너 내에서 그대로 유지됩니다.

보안 요구에 따라 XenMobile 에서 Siri 및 받아쓰기 서비스를 차단할 수 있습니다.

MAM 배포에서 각 앱에 대한 받아쓰기 차단 정책은 기본적으로 켜져 있습니다. 즉, 장치의 마이크가 사용되지 않습니다. 받아쓰기를 허용하려면 이 정책을 꺼짐으로 설정합니다. 이 정책은 XenMobile 콘솔의 구성 > 앱에서 찾을 수 있습니다. 앱을 선택하고 편집을 클릭한 후 **iOS** 를 클릭합니다.

MDX	App Restrictions
1 App Information	Block camera <input checked="" type="checkbox"/> ON ?
2 Platform	Block Photo Library <input checked="" type="checkbox"/> ON ?
<input checked="" type="checkbox"/> iOS	Block mic record <input checked="" type="checkbox"/> ON ?
<input type="checkbox"/> Android	Block dictation <input type="checkbox"/> OFF ?
<input type="checkbox"/> Windows Phone	Block location services <input checked="" type="checkbox"/> ON ?
<input type="checkbox"/> Windows Desktop/Tablet	Block SMS compose <input checked="" type="checkbox"/> ON ?
3 Approvals (optional)	
4 Delivery Group Assignments (optional)	

또한 MDM 배포에서 구성 > 장치 정책의 Siri 정책을 통해 Siri 를 사용하지 않도록 설정할 수 있습니다. Siri 사용은 기본적으로 허용됩니다.

Restrictions Policy	Restrictions Policy This policy allows or restricts users from using certain features on their devices, such as the camera media content and on certain types of apps users can and cannot install. Allow hardware controls
1 Policy Info	
2 Platforms	Camera <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> iOS	<input checked="" type="checkbox"/> FaceTime ?
<input checked="" type="checkbox"/> macOS	Screen shots <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Samsung SAFE	Photo streams <input checked="" type="checkbox"/> ON iOS 5.0+
<input checked="" type="checkbox"/> Samsung KNOX	Shared photo streams <input checked="" type="checkbox"/> ON iOS 6.0+
<input checked="" type="checkbox"/> Windows Phone	Voice dialing <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Siri <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Amazon	<input checked="" type="checkbox"/> Allow while device is locked
<input checked="" type="checkbox"/> Windows Mobile/CE	<input type="checkbox"/> Siri profanity filter

Siri 와 받아쓰기를 허용할지 여부를 결정할 때 주의해야 할 몇 가지 사항은 다음과 같습니다.

- Apple 이 공개한 정보에 따르면 Apple 은 Siri 및 받아쓰기 음성 클립 데이터를 최대 2 년간 유지합니다. 이 데이터에는 사용자를 나타내는 무작위 값이 할당되며 이 무작위 번호에 음성 파일이 연결되어 있습니다. 자세한 내용은 [Wired 문서 Apple reveals how long Siri keeps your data\(Apple, Siri 에 사용자 데이터를 유지하는 기간 공개\)](#)를 참조하

십시오.

- iOS 장치에서 설정 > 일반 > 키보드로 이동하고 받아쓰기 활성화 아래의 링크를 눌러 Apple의 개인정보보호정책을 검토할 수 있습니다.

SSO 계정 장치 정책

January 5, 2022

사용자가 다양한 앱에서 XenMobile과 회사 내부 리소스에 액세스하기 위해 한 번만 로그인하도록 XenMobile에서 SSO(Single Sign-On) 계정을 만듭니다. 사용자가 장치에 자격 증명을 저장할 필요가 없습니다. App Store의 앱을 포함하여 앱 전반에 걸쳐 SSO 계정 엔터프라이즈 사용자 자격 증명에 사용됩니다. 이 정책은 Kerberos 인증 백엔드와 함께 작동하도록 설계되었습니다.

이 정책은 iOS 7.0 이상에만 적용됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- **계정 이름:** 사용자의 장치에 나타나는 Kerberos SSO 계정 이름을 입력합니다. 이것은 필수 필드입니다.
- **Kerberos 보안 주체 이름:** Kerberos 보안 주체 이름을 입력합니다. 이것은 필수 필드입니다.
- **ID 자격 증명 (키 저장소 또는 PKI 자격 증명):** 목록에서 사용자 상호 작용 없이 Kerberos 자격 증명을 갱신하는 데 사용할 수 있는 선택적인 ID 자격 증명을 클릭합니다.
- **Kerberos 영역:** 이 정책의 Kerberos 영역을 입력합니다. 일반적으로 도메인 이름은 모두 대문자입니다 (예: EXAMPLE.COM). 이것은 필수 필드입니다.
- **허용 URL:** SSO가 필요한 각 URL에 대해 추가를 클릭한 후 다음을 수행합니다.
 - **허용 URL:** 사용자가 iOS 장치에서 URL을 방문할 때 SSO를 요구할 URL을 입력합니다.

예를 들어 사용자가 사이트를 탐색하려고 할 때 웹 사이트가 Kerberos 챌린지를 시작하는 경우 해당 사이트가 URL 목록에 없으면 iOS 장치는 이전 Kerberos 로그인에서 장치에 캐시되었을 수 있는 Kerberos 토큰을 제공하며 SSO를 시도하지 않습니다. 일치 항목은 URL의 호스트 부분에서 정확히 일치해야 합니다. 예를 들어 <https://shopping.apple.com>은 유효하지만 https://*.apple.com은 유효하지 않습니다.

또한 호스트 일치에 따라 Kerberos가 활성화되지 않는 경우 URL은 여전히 표준 HTTP 호출로 대체됩니다. 이 호출은 URL이 Kerberos를 사용하는 SSO에 대해서만 구성되어 있는 경우 표준 암호 챌린지 또는 HTTP 오류를 포함한 거의 모든 수단을 의미할 수 있습니다.
 - 추가를 클릭하여 URL을 추가하거나 취소를 클릭하여 URL 추가를 취소합니다.
- **앱 식별자:** 이 로그인을 사용하도록 허용된 각 앱에 대해 추가를 클릭한 후 다음을 수행합니다.

- 앱 식별자: 이 로그인을 사용하도록 허용된 앱의 앱 식별자를 입력합니다. 앱 식별자를 추가하지 않으면 이 로그인
은 모든 앱 식별자와 일치합니다.
- 추가를 클릭하여 앱 식별자를 추가하거나 취소를 클릭하여 앱 식별자 추가를 취소합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기
간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만
사용할 수 있습니다.

스토어 장치 정책

January 5, 2022

iOS, Android 또는 Windows 태블릿 장치의 홈 화면에 XenMobile Store 웹 클립을 표시할지 여부를 지정하는 정책을 XenMobile 에서 만들 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

플랫폼 설정

구성하는 각 플랫폼에 대해 XenMobile Store 웹 클립을 사용자 장치에 표시할지 여부를 선택합니다. 기본값은 켜짐입니다.

구독 캘린더 장치 정책

January 5, 2022

XenMobile 에 장치 정책을 추가하여 iOS 장치에 있는 캘린더 목록에 구독 캘린더를 추가할 수 있습니다. 구독할 수 있는 공개
캘린더 목록이 www.apple.com/downloads/macosx/calendars에 나와 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

사전 요구 사항

사용자 장치에 있는 구독 캘린더 목록에 캘린더를 추가하려면 먼저 캘린더를 구독해야 합니다.

iOS 설정

- **설명:** 캘린더의 설명을 입력합니다. 이것은 필수 필드입니다.
- **URL:** 캘린더 URL 을 입력합니다. [webcal://](#) URL 또는 iCalendar 파일 (.ics) 에 대한 [https://](#) 링크를 입력할 수 있습니다. 이것은 필수 필드입니다.
- **사용자 이름:** 사용자의 로그인 이름을 입력합니다. 이것은 필수 필드입니다.
- **암호:** 선택적 사용자 암호를 입력합니다.
- **SSL 사용:** 캘린더에 대한 SSL 연결을 사용할 것인지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **정책 설정**
 - **정책 제거:** 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * **제거할 때까지의 기간 (시간):** 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

약관 장치 정책

August 12, 2022

사용자가 회사 네트워크에 대한 연결을 통제하는 회사의 특정 정책에 동의하도록 하려면 XenMobile 에서 약관 장치 정책을 만듭니다. 사용자가 XenMobile 에 장치를 등록할 때 약관이 표시되며 약관에 동의해야만 장치를 등록할 수 있습니다. 약관에 동의하지 않으면 등록 프로세스가 취소됩니다.

회사에 다양한 국가의 사용자가 있고 사용자의 모국어로 약관에 동의하게 하려면 약관에 대한 정책을 여러 언어로 만들 수 있습니다. 배포하려는 각 플랫폼 및 언어 조합에 대한 파일을 제공해야 합니다. Android 및 iOS 장치의 경우 PDF 파일을 제공해야 합니다. Windows 장치의 경우 텍스트 (.txt) 파일 및 동반 이미지 파일을 제공해야 합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 및 Android 설정

- **가져올 파일:** 찾아보기를 클릭하고 파일의 위치로 이동하여 가져올 약관 파일을 선택합니다.
- **기본 약관:** 이 파일이 서로 다른 약관을 사용하는 여러 그룹의 구성원인 사용자의 기본 문서인지 여부를 선택합니다. 기본값은 꺼짐입니다.

Windows 태블릿 설정

- 가져올 파일: 찾아보기를 클릭하고 파일의 위치로 이동하여 가져올 약관 파일을 선택합니다.
- 이미지: 찾아보기를 클릭하고 파일 위치로 이동하여 가져올 이미지 파일을 선택합니다.
- 기본 약관: 이 파일이 서로 다른 약관을 사용하는 여러 그룹의 구성원인 사용자의 기본 문서인지 여부를 선택합니다. 기본 값은 꺼짐입니다.

VPN 장치 정책

March 15, 2024

VPN 장치 정책은 사용자 장치에서 회사 리소스에 안전하게 연결할 수 있게 하는 VPN(가상 사설망) 설정을 구성합니다. 다음 플랫폼에 대한 VPN 장치 정책을 구성할 수 있습니다. 플랫폼마다 서로 다른 값이 필요합니다. 이에 대해서는 이 문서에 자세히 설명되어 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

앱별 VPN에 대한 요구 사항

VPN 정책을 통해 다음 플랫폼에 대해 앱별 VPN 기능을 구성합니다.

- iOS
- macOS
- Android(레거시 DA)
- Samsung SAFE
- Samsung Knox

Android Enterprise 장치에 대한 VPN을 구성하려면 Citrix SSO 앱에 대한 관리되는 구성 장치 정책을 만듭니다. [Android Enterprise에 대한 VPN 프로필 구성](#)을 참조하십시오.

특정 연결 유형에 대해 앱별 VPN 옵션을 사용할 수 있습니다. 다음 표는 앱별 VPN 옵션이 제공되는 경우를 보여줍니다.

플랫폼	Connection type(연결 유형)	비고
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO 또는 사용자 지정 SSL.	

플랫폼	Connection type(연결 유형)	비고
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA 또는 사용자 지정 SSL.	
Android(레거시 DA)	Citrix SSO	
Samsung SAFE	IPSEC, SSL	VPN 유형이 일반적으로 설정됨
Samsung Knox	IPSEC, SSL	VPN 유형이 일반적으로 설정됨

Citrix SSO 앱을 사용하여 iOS 및 Android(레거시 DA) 장치에 대한 앱별 VPN 을 만들려면 VPN 정책 구성 외에 추가 단계를 수행해야 합니다. 또한 다음 사전 요구 사항도 충족하는지 확인해야 합니다.

- 온프레미스 Citrix Gateway
- 다음 응용 프로그램이 장치에 설치됩니다.
 - Citrix SSO
 - Citrix Secure Hub

Citrix SSO 앱을 사용하여 iOS 및 Android 장치에 대한 앱별 VPN 을 구성하는 일반적인 워크플로는 다음과 같습니다.

1. 이 문서에 설명된 대로 VPN 장치 정책을 구성합니다.

- iOS 의 경우 [iOS 용 Citrix SSO 프로토콜 구성](#)을 참조하십시오. VPN 장치 정책을 통해 iOS 용 Citrix SSO 프로토콜을 구성한 후에는 앱을 앱별 VPN 정책에 연결하는 앱 특성 정책도 만들어야 합니다. 자세한 내용은 [앱별 VPN 구성](#)을 참조하십시오.
 - 연결을 위한 인증 유형 필드에 대해 인증서를 선택할 경우 인증서 기반 Endpoint Management 인증을 먼저 구성해야 합니다. [클라이언트 인증서 인증](#) 또는 [인증서와 도메인 인증](#)을 참조하십시오.
- Android(레거시 DA) 에 대해서는 [Android 용 Citrix SSO 프로토콜 구성](#)을 참조하십시오.
 - 연결을 위한 인증 유형 필드에 대해 인증서 또는 암호 및 인증서를 선택할 경우 인증서 기반 Endpoint Management 인증을 먼저 구성해야 합니다. [클라이언트 인증서 인증](#) 또는 [인증서와 도메인 인증](#)을 참조하십시오.

2. 앱별 VPN 에서 트래픽을 허용하도록 Citrix ADC 를 구성합니다. 자세한 내용은 [Citrix Gateway 에서 전체 VPN 설정](#)을 참조하십시오.

iOS 설정

iOS 12로 장치 업그레이드를 준비하려면:

iOS용 VPN 장치 정책의 Citrix VPN 연결 유형은 iOS 12를 지원하지 않습니다. 다음 단계를 수행하여 기존 VPN 장치 정책을 삭제하고 Citrix SSO 연결 유형으로 VPN 장치 정책을 만듭니다.

1. iOS용 VPN 장치 정책을 삭제합니다.
2. iOS용 VPN 장치 정책을 추가합니다. 중요 설정:
 - **Connection type = Citrix SSO**
 - **Enable per-app VPN = On**
 - **Provider type = Packet tunnel**
3. iOS에 대한 앱 특성 장치 정책을 추가합니다. 앱별 VPN 식별자의 경우 **iOS_VPN**을 선택합니다.

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<div> <div>Connection name</div> <input type="text"/> </div> <div> <div>Connection type</div> <div>L2TP</div> </div> <div> <div>Server name or IP address *</div> <input type="text"/> </div> <div> <div>User account</div> <input type="text"/> </div> <div> <div> <input checked="" type="radio"/> Password authentication <input type="radio"/> RSA SecureID authentication </div> </div> <div> <div>Shared secret</div> <input type="text"/> </div> <div> <div>Send all traffic</div> <div>OFF</div> </div> <div> <div>Proxy configuration</div> <div>None</div> </div>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Samsung SAFE <input checked="" type="checkbox"/> Samsung KNOX <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Amazon	Proxy
3 Assignment	

- **연결 이름:** 연결 이름을 입력합니다.
- **연결 유형:** 목록에서 이 연결에 사용할 프로토콜을 선택합니다. 기본값은 **L2TP**입니다.
 - **L2TP:** 미리 공유한 키 인증을 사용하는 계층 2 터널링 프로토콜입니다.
 - **PPTP:** 지점 간 터널링입니다.
 - **IPSec:** 회사 VPN 연결입니다.
 - **Cisco Legacy AnyConnect:** 이 연결 유형을 사용하려면 Cisco Legacy AnyConnect VPN 클라이언트가 사용자 장치에 설치되어 있어야 합니다. 이제는 사용되지 않는 VPN 프레임워크에 기반하는 Cisco Legacy AnyConnect 클라이언트는 단계적으로 중단됩니다. 자세한 내용은 지원 문서 <https://support.citrix.com/article/CTX227708>에서 참조하십시오.

현재 Cisco AnyConnect 클라이언트를 사용하려면 연결 유형에서 사용자 지정 **SSL**을 선택합니다. 필요한 설정은 이 섹션에서 “사용자 지정 SSL 프로토콜 구성”을 참조하십시오.

- **Juniper SSL:** Juniper Networks SSL VPN 클라이언트입니다.
- **F5 SSL:** F5 Networks SSL VPN 클라이언트입니다.

- **SonicWALL Mobile Connect:** iOS 용 Dell 통합 VPN 클라이언트입니다.
- **Ariba VIA:** Ariba Networks Virtual Internet Access 클라이언트입니다.
- **IKEv2(iOS 에만 해당):** iOS 전용 Internet Key Exchange 버전 2 입니다.
- **AlwaysOn IKEv2:** IKEv2 를 사용하여 상시 액세스를 제공합니다.
- **AlwaysOn IKEv2** 이중 구성: IKEv2 이중 구성을 사용하여 상시 액세스를 제공합니다.
- **Citrix SSO:** iOS 12 이상을 위한 Citrix SSO 클라이언트입니다.
- 사용자 지정 **SSL:** 사용자 지정 Secure Socket Layer 입니다. 이 연결 유형은 번들 ID 가 **com.cisco.anyconnect** 인 Cisco AnyConnect 클라이언트에 필요합니다. 연결 이름을 **Cisco AnyConnect** 로 지정합니다. VPN 정책을 배포하고 iOS 장치에 대해 NAC(네트워크 액세스 제어) 필터를 사용하도록 설정할 수도 있습니다. 이 필터는 호환되지 않는 앱이 설치된 장치에 대한 VPN 연결을 차단합니다. 이 구성에는 다음 iOS 섹션에 설명된 대로 iOS VPN 정책에 대한 특정 설정이 필요합니다. NAC 필터를 사용하는 데 필요한 기타 설정에 대한 자세한 내용은 [네트워크 액세스 제어](#)를 참조하십시오.

다음 섹션에는 이전에 설명한 각 연결 유형에 대한 구성 옵션이 나열되어 있습니다.

iOS 용 L2TP 프로토콜 구성

- 서버 이름 또는 **IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 암호 인증 또는 **RSA SecurID** 인증을 선택합니다.
- 공유 암호: IPsec 공유 암호 키를 입력합니다.
- 모든 트래픽 보내기: VPN 을 통해 모든 트래픽을 보낼 지 여부를 선택합니다. 기본값은 꺼짐입니다.

iOS 용 PPTP 프로토콜 구성

- 서버 이름 또는 **IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 암호 인증 또는 **RSA SecurID** 인증을 선택합니다.
- 암호화 수준: 목록에서 암호화 수준을 선택합니다. 기본값은 없음입니다.
 - 없음: 암호화를 사용하지 않습니다.
 - 자동: 서버에서 지원하는 가장 강력한 암호화 수준을 사용합니다.
 - 최대 (**128 비트**): 항상 128 비트 암호화를 사용합니다.
- 모든 트래픽 보내기: VPN 을 통해 모든 트래픽을 보낼 지 여부를 선택합니다. 기본값은 꺼짐입니다.

iOS 용 IPsec 프로토콜 구성

- 서버 이름 또는 **IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.

- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 공유 암호 또는 인증서를 선택합니다. 기본값은 공유 암호입니다.
- 공유 암호를 사용하는 경우 다음 설정을 구성합니다.
 - 그룹 이름: 선택적 그룹 이름을 입력합니다.
 - 공유 암호: 선택적 공유 암호 키를 입력합니다.
 - 하이브리드 인증 사용: 하이브리드 인증을 사용할지 여부를 선택합니다. 하이브리드 인증을 사용하면 서버가 먼저 클라이언트에서 자체 인증된 후 클라이언트가 서버에서 자체 인증됩니다. 기본값은 꺼짐입니다.
 - 암호 확인: 사용자가 네트워크에 연결할 때 암호 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ID 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - 연결할 때 PIN 확인: 사용자가 네트워크에 연결할 때 PIN 을 입력하도록 할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 주문형 VPN 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 VPN 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.
- 앱별 VPN 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- Safari 도메인: 추가를 클릭하여 Safari 도메인 이름을 추가합니다.

iOS 용 Cisco Legacy AnyConnect 프로토콜 구성

Cisco Legacy AnyConnect 클라이언트에서 새로운 Cisco AnyConnect 클라이언트로 전환하려면 사용자 지정 SSL 프로토콜을 사용합니다.

- 공급자 번들 식별자: Legacy AnyConnect 클라이언트의 번들 ID 는 com.cisco.anyconnect.gui 입니다.
- 서버 이름 또는 IP 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 그룹: 선택적 그룹 이름을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * ID 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 PIN 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.

- ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 공급자 유형: 앱별 VPN 을 앱 프록시로 제공할지, 아니면 패킷 터널로 제공할지를 선택합니다. 기본값은 앱 프록시입니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

iOS 용 Juniper SSL 프로토콜 구성

- 공급자 번들 식별자: 앱별 VPN 프로필에 앱의 번들 식별자와 동일한 유형의 여러 VPN 공급자가 포함되는 경우 여기서 사용할 공급자를 지정합니다.
- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 영역: 선택적 영역 이름을 입력합니다.
- 역할: 선택적 역할 이름을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ★ **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 공급자 유형: 앱별 VPN 을 앱 프록시로 제공할지, 아니면 패킷 터널로 제공할지를 선택합니다. 기본값은 앱 프록시입니다.

- **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.

- ★ 도메인: 추가할 도메인을 입력합니다.
- ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

iOS 용 F5 SSL 프로토콜 구성

- 공급자 번들 식별자: 앱별 VPN 프로필에 앱의 번들 식별자와 동일한 유형의 여러 VPN 공급자가 포함되는 경우 여기서 사용할 공급자를 지정합니다.
- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ★ **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - 공급자 유형: 앱별 VPN 을 앱 프록시로 제공할지, 아니면 패킷 터널로 제공할지를 선택합니다. 기본값은 앱 프록시입니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

iOS 용 SonicWALL 프로토콜 구성

- 공급자 번들 식별자: 앱별 VPN 프로필에 앱의 번들 식별자와 동일한 유형의 여러 VPN 공급자가 포함되는 경우 여기서 사용할 공급자를 지정합니다.
- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.

- 로그인 그룹 또는 도메인: 선택적 로그인 그룹 또는 도메인을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 켜짐으로 설정하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - 공급자 유형: 앱별 VPN 을 앱 프록시로 제공할지, 아니면 패킷 터널로 제공할지를 선택합니다. 기본값은 앱 프록시입니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * 도메인: 추가할 도메인을 입력합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

iOS 용 Ariba VIA 프로토콜 구성

- 공급자 번들 식별자: 앱별 VPN 프로필에 앱의 번들 식별자와 동일한 유형의 여러 VPN 공급자가 포함되는 경우 여기서 사용할 공급자를 지정합니다.
- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.

- **앱별 VPN 사용:** 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

iOS 용 IKEv2 프로토콜 구성

이 섹션에는 IKEv2, AlwaysOn IKEv2 및 AlwaysOn IKEv2 이중 구성 프로토콜에 사용되는 설정이 포함되어 있습니다. AlwaysOn IKEv2 이중 구성 프로토콜의 경우 셀룰러 및 Wi-Fi 네트워크에 대해 이러한 모든 설정을 구성합니다.

- 사용자가 자동 연결을 비활성화하도록 허용: AlwaysOn 프로토콜용입니다. 사용자가 자신의 장치에서 네트워크 자동 연결을 끌 수 있게 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 서버의 호스트 이름 또는 IP 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 로컬 식별자: IKEv2 클라이언트의 FQDN 또는 IP 주소입니다. 이것은 필수 필드입니다.
- 원격 식별자: VPN 서버의 FQDN 또는 IP 주소입니다. 이것은 필수 필드입니다.
- 장치 인증: 이 연결에 대한 인증 유형으로 공유 암호, 인증서 또는 장치 ID 에 기반한 장치 인증서를 선택합니다. 기본값은 공유 암호입니다.
 - 공유 암호를 선택하는 경우 선택적 공유 암호 키를 입력합니다.
 - 인증서를 선택하는 경우 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - 장치 ID 에 기반한 장치 인증서를 선택할 경우 사용할 장치 ID 유형을 선택합니다. 기본값은 IMEI 입니다. 이 옵션을 사용하려면 REST API 를 사용하여 인증서를 일괄적으로 가져옵니다. [REST API 로 iOS 장치에 인증서 일괄 업로드](#)를 참조하십시오. IKEv2 항상 켜짐을 선택한 경우에만 사용할 수 있습니다.
- 확장 인증 사용: EAP(확장 인증 프로토콜) 를 사용할지 여부를 선택합니다. 켜짐을 선택하는 경우 사용자 계정과 인증 암호를 입력합니다.
- 데드 피어 감지 간격: 피어 장치에 접속하여 피어 장치가 연결 가능한 상태로 유지되는지를 확인할 빈도를 선택합니다. 기본값은 없음입니다. 옵션은 다음과 같습니다.
 - 없음: 데드 피어 감지를 사용하지 않습니다.
 - 낮음: 30 분마다 피어에 접속합니다.
 - 중간: 10 분마다 피어에 접속합니다.
 - 높음: 1 분마다 피어에 접속합니다.

- 모바일 및 다중 홈 사용 안 함: 이 기능을 사용하지 않도록 설정할지 여부를 선택합니다.
- **IPv4/IPv6** 내부 서브넷 특성 사용: 이 기능을 사용하도록 설정할지 여부를 선택합니다.
- 리디렉션 사용 안 함: 리디렉션을 사용하지 않도록 설정할지 여부를 선택합니다.
- 장치가 절전 상태일 때 **NAT Keepalive** 사용: AlwaysOn 프로토콜용입니다. Keepalive 패킷에 IKEv2 연결에 대한 NAT 매핑이 유지됩니다. 칩은 장치가 활성 상태일 때 이러한 패킷을 정기적인 간격으로 전송합니다. 이 설정이 켜짐인 경우 장치가 절전 상태일 때도 칩이 Keepalive 패킷을 전송합니다. 기본 간격은 Wi-Fi 를 사용하면 20 초이고 셀룰러를 사용하면 110 초입니다. 간격은 NAT keepalive 간격 매개 변수를 사용하여 변경할 수 있습니다.
- **NAT keepalive** 간격 (초): 기본값은 20 초입니다.
- **PFS(Perfect Forward Secrecy)** 사용: 이 기능을 사용하도록 설정할지 여부를 선택합니다.
- **DNS** 서버 **IP** 주소: 선택 사항입니다. DNS 서버 IP 주소 문자열의 목록입니다. 이러한 IP 주소에는 IPv4 주소 및 IPv6 주소가 혼합되어 포함될 수 있습니다. 추가를 클릭하여 주소를 입력합니다.
- 도메인 이름: 선택 사항입니다. 터널의 기본 도메인입니다.
- 검색 도메인: 선택 사항입니다. 단일 레이블 호스트 이름을 정규화하는 데 사용되는 도메인 문자열의 목록입니다.
- 추가 일치 도메인을 확인자 목록에 추가합니다: 선택 사항입니다. 보조 일치 도메인 목록을 확인자의 검색 도메인 목록에 추가할지 여부를 결정합니다. 기본값은 켜짐입니다.
- 보조 일치 도메인: 선택 사항입니다. DNS 서버 주소에 포함된 DNS 확인자 설정을 사용할 DNS 쿼리를 결정하는 데 사용되는 도메인 문자열 목록입니다. 이 키는 특정 도메인의 호스트만 터널의 DNS 확인자를 사용하여 확인되는 분할 DNS 구성을 생성합니다. 이 목록의 도메인 중 하나에 포함되지 않은 호스트는 시스템의 기본 확인자를 사용하여 확인됩니다.

이 매개 변수에 빈 문자열이 포함된 경우 해당 문자열이 기본 도메인입니다. 분할 터널 구성은 이 방법으로 먼저 모든 DNS 쿼리를 직접 VPN DNS 서버로 전달한 후 기본 DNS 서버로 전달할 수 있습니다. VPN 터널이 네트워크의 기본 경로인 경우 나열된 DNS 서버가 기본 확인자가 됩니다. 이 경우 보조 일치 도메인 목록이 무시됩니다.

- **IKE SA** 매개 변수 및 하위 **SA** 매개 변수. 각 SA(보안 연결) 매개 변수 옵션에 대해 다음 설정을 구성합니다.
 - 암호화 알고리즘: 목록에서 사용할 IKE 암호화 알고리즘을 선택합니다. 기본값은 **3DES** 입니다.
 - 무결성 알고리즘: 목록에서 사용할 무결성 알고리즘을 선택합니다. 기본값은 **SHA1-96** 입니다.
 - **Diffie Hellman** 그룹: 목록에서 Diffie Hellman 그룹 번호를 선택합니다. 기본값은 **2** 입니다.
 - **IKE** 수명 (분): SA 수명 (키 다시 지정 간격) 을 나타내는 10 에서 1440 사이의 정수를 입력합니다. 기본값은 **1440** 분입니다.
- 서비스 예외: AlwaysOn 프로토콜용입니다. 서비스 예외는 AlwaysOn VPN 에서 제외되는 시스템 서비스입니다. 다음 서비스 예외 설정을 구성합니다.
 - 음성 사서함: 목록에서 음성 사서함 예외의 처리 방법을 선택합니다. 기본값은 트래픽이 터널을 통해 전달되도록 허용입니다.

- **AirPrint:** 목록에서 AirPrint 예외의 처리 방법을 선택합니다. 기본값은 트래픽이 터널을 통해 전달되도록 허용입니다.
- 종속 웹 사이트의 트래픽이 **VPN** 터널 외부로 전달되도록 허용: 사용자가 VPN 터널 외부의 공용 핫스팟에 연결할 수 있게 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 모든 종속 네트워킹 앱의 트래픽이 **VPN** 터널 외부로 전달되도록 허용: VPN 터널 외부에 있는 모든 핫스팟 네트워킹 앱을 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 종속 네트워킹 앱 번들 식별자: 사용자 액세스가 허용되는 각 핫스팟 네트워킹 앱 번들 식별자에 대해 추가를 클릭하고 핫스팟 네트워킹 앱 번들 식별자를 입력합니다. 저장을 클릭하여 앱 번들 식별자를 저장합니다.
- **앱별 VPN.** IKEv2 연결 유형에 대한 설정을 구성합니다.
 - **앱별 VPN 사용:** 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **주문형 일치 앱 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 추가를 클릭하여 Safari 도메인 이름을 추가합니다.
- **프록시 구성:** 프록시 서버를 통해 VPN 연결을 라우팅하는 방법을 선택합니다. 기본값은 없음입니다.

iOS 용 Citrix SSO 프로토콜 구성

Citrix SSO 클라이언트는 Apple Store(<https://apps.apple.com/us/app/citrix-ss0/id1333396910>) 에서 제공됩니다.

- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - * **주문형 VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.
- **앱별 VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 켜짐으로 설정하는 경우 다음 설정을 구성합니다.
 - **주문형 일치 앱 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.

- 공급자 유형: 앱별 VPN 을 앱 프록시로 제공할지, 아니면 패킷 터널로 제공할지를 선택합니다. 기본값은 앱 프록시입니다.
- 공급자 유형: 패킷 터널로 설정합니다.
- **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- 사용자 지정 **XML**: 추가할 각 사용자 지정 XML 매개 변수에 대해 추가를 클릭하고 키/값 쌍을 지정합니다. 사용 가능한 매개 변수는 다음과 같습니다.
 - **disableL3**: 시스템 수준 VPN 을 사용하지 않습니다. 앱별 VPN 만 허용합니다. 값이 필요하지 않습니다.
 - **useragent**: 이 장치 정책에 VPN 플러그인 클라이언트를 대상으로 하는 모든 Citrix Gateway 정책을 연결합니다. 플러그인에서 시작된 요청의 경우 이 키의 값이 VPN 플러그인에 자동으로 추가됩니다.

iOS 용 사용자 지정 SSL 프로토콜 구성

Cisco Legacy AnyConnect 클라이언트에서 Cisco AnyConnect 클라이언트로 전환하려면:

1. 사용자 지정 SSL 프로토콜을 사용하여 VPN 장치 정책을 구성합니다. 정책을 iOS 장치에 배포합니다.
2. <https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>에서 Cisco AnyConnect 클라이언트를 업로드하고 앱을 XenMobile 에 추가한 다음 iOS 장치에 앱을 배포합니다.
3. iOS 장치에서 이전 VPN 장치 정책을 제거합니다.

설정:

- 사용자 지정 **SSL** 식별자 (역방향 **DNS** 형식): 번들 식별자로 설정합니다. Cisco AnyConnect 클라이언트의 경우 **com.cisco.anyconnect** 를 사용합니다.
- 공급자 번들 식별자: 사용자 지정 **SSL** 식별자에서 지정한 앱에 동일한 유형 (앱 프록시 또는 패킷 터널) 의 여러 VPN 공급자가 있는 경우 이 번들 식별자를 지정합니다. Cisco AnyConnect 클라이언트의 경우 **com.cisco.anyconnect** 를 사용합니다.
- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ★ **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜진 경우 설정 구성에 대한 자세한 내용은 [iOS 용 주문형 VPN 사용 설정 구성](#)을 참조하십시오.

- **앱별 VPN 사용:** 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 켜짐으로 설정하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - 공급자 유형: 공급자가 VPN 서비스인지 프록시 서비스인지를 나타내는 공급자 유형입니다. VPN 서비스의 경우 패킷 터널을 선택합니다. 프록시 서비스의 경우 앱 프록시를 선택합니다. Cisco AnyConnect 클라이언트의 경우 패킷 터널을 선택합니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * 도메인: 추가할 도메인을 입력합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- 사용자 지정 **XML:** 추가할 각 사용자 지정 XML 매개 변수에 대해 추가를 클릭하고 다음을 수행합니다.
 - 매개 변수 이름: 추가할 매개 변수의 이름을 입력합니다.
 - 값: 매개 변수 이름에 연결된 값을 입력합니다.
 - 저장을 클릭하여 매개 변수를 저장하거나 취소를 클릭하여 매개 변수를 저장하지 않습니다.

NAC 를 지원하도록 VPN 장치 정책 구성

1. NAC 필터를 구성하려면 연결 유형이 사용자 지정 **SSL** 이어야 합니다.
2. **VPN** 의 연결 이름을 지정합니다.
3. 사용자 지정 **SSL** 식별자에는 **com.citrix.NetScalerGateway.ios.app** 를 입력합니다.
4. 공급자 번들 식별자에는 **com.citrix.NetScalerGateway.ios.app.vpnplugin** 을 입력합니다.

3 단계와 4 단계의 값은 NAC 필터링에 필요한 Citrix SSO 설치에서 가져옵니다. 인증 암호는 구성하지 않습니다. NAC 기능 사용에 대한 자세한 내용은 [네트워크 액세스 제어](#)를 참조하십시오.

ios 용 주문형 VPN 사용 옵션 구성

- 주문형 도메인: 각 도메인과 사용자가 연결할 때 수행할 관련 작업에 대해 추가를 클릭하고 다음을 수행합니다.
- 도메인: 추가할 도메인을 입력합니다.
- 동작: 목록에서 가능한 동작 중 하나를 선택합니다.
 - 항상 설정: 도메인에서 항상 VPN 연결이 트리거됩니다.
 - 설정 안 함: 도메인에서 VPN 연결이 트리거되지 않습니다.
 - 필요한 경우 설정: 도메인 이름 확인에 실패하는 경우 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버에서 도메인을 확인할 수 없거나 다른 서버로 리디렉션되거나 시간 초과되는 경우 발생합니다.
 - 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- 주문형 규칙

- 동작: 목록에서 수행할 동작을 선택합니다. 기본값은 **EvaluateConnection** 입니다. 가능한 동작은 다음과 같습니다.
 - * 허용: 트리거 시 주문형 VPN 연결을 허용합니다.
 - * 연결: VPN 연결을 무조건 시작합니다.
 - * 연결 끊기: VPN 연결을 제거하고 규칙이 일치하지 않는 한 주문형 VPN 에 다시 연결하지 않습니다.
 - * **EvaluateConnection**: 각 연결에 대한 ActionParameters 배열을 평가합니다.
 - * 무시: 기존 VPN 연결을 유지하지만 규칙이 일치하지 않는 한 주문형 VPN 에 다시 연결하지 않습니다.
- **DNSDomainMatch**: 장치의 검색 도메인 목록과 일치할 수 있는 추가할 각 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **DNS 도메인**: 도메인 이름을 입력합니다. 와일드카드 “*” 접두사를 사용하여 여러 도메인을 일치할 수 있습니다. 예를 들어 *.example.com 은 mydomain.example.com, yourdomain.example.com 및 herdomain.example.com 과 일치합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- **DNSServerAddressMatch**: 네트워크의 지정된 DNS 서버와 일치할 수 있는 추가할 각 IP 주소에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **DNS 서버 주소**: 추가할 DNS 서버 주소를 입력합니다. 와일드카드 “*” 접미사를 사용하여 DNS 서버를 일치할 수 있습니다. 예를 들어 17.* 는 클래스 A 서브넷의 모든 DNS 서버와 일치합니다.
 - * 저장을 클릭하여 DNS 서버 주소를 저장하거나 취소를 클릭하여 DNS 서버 주소를 저장하지 않습니다.
- **InterfaceTypeMatch**: 목록에서 사용하는 기본 네트워크 인터페이스 하드웨어 유형을 선택합니다. 기본값은 지정되지 않음입니다. 가능한 값은 다음과 같습니다.
 - * 지정되지 않음: 모든 네트워크 인터페이스 하드웨어와 일치합니다. 이 옵션은 기본값입니다.
 - * 이더넷: 이더넷 네트워크 인터페이스 하드웨어만 일치합니다.
 - * **WiFi**: WiFi 네트워크 인터페이스 하드웨어만 일치합니다.
 - * 셀룰러: 셀룰러 네트워크 인터페이스 하드웨어만 일치합니다.
- **SSIDMatch**: 현재 네트워크와 일치할 추가할 각 SSID 에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **SSID**: 추가할 SSID 를 입력합니다. 네트워크가 Wi-Fi 네트워크가 아닌 경우 또는 SSID 가 표시되지 않는 경우 일치이 실패합니다. 모든 SSID 와 일치하려면 이 목록을 비워 둡니다.
 - * 저장을 클릭하여 SSID 를 저장하거나 취소를 클릭하여 SSID 를 저장하지 않습니다.
- **URLStringProbe**: 가져올 URL 을 입력합니다. 이 URL 을 리디렉션 없이 성공적으로 가져온 경우 이 규칙이 일치합니다.
- **ActionParameters : Domains**: EvaluateConnection 이 검사하는 추가할 각 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * 도메인: 추가할 도메인을 입력합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- **ActionParameters : DomainAction**: 목록에서 지정된 **ActionParameters : Domains** 도메인에 대한 VPN 동작을 선택합니다. 기본값은 **ConnectIfNeeded** 입니다. 가능한 동작은 다음과 같습니다.
 - * **ConnectIfNeeded**: 도메인 이름 확인에 실패하는 경우 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버에서 도메인을 확인할 수 없거나 다른 서버로 리디렉션되거나 시간 초과되는 경우 발생합니다.

- ★ **NeverConnect:** 도메인에서 VPN 연결이 트리거되지 않습니다.
- **ActionParameters: RequiredDNSServers:** 지정된 도메인을 확인할 때 사용할 각 DNS 서버 IP 주소에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ **DNS 서버: ActionParameters : DomainAction = ConnectIfNeeded** 인 경우에만 유효합니다. 추가할 DNS 서버를 입력합니다. 이 서버는 장치의 현재 네트워크 구성에 포함된 서버가 아니어도 됩니다. DNS 서버에 연결할 수 없는 경우 VPN 연결이 대신 설정됩니다. 이 DNS 서버는 내부 DNS 서버 또는 신뢰할 수 있는 외부 DNS 서버여야 합니다.
 - ★ 저장을 클릭하여 DNS 서버를 저장하거나 취소를 클릭하여 DNS 서버를 저장하지 않습니다.
- **ActionParameters : RequiredURLStringProbe:** 필요한 경우 GET 요청을 사용하여 검색할 HTTP 또는 HTTPS(기본 설정) URL 을 입력합니다. URL 의 호스트 이름을 확인할 수 없거나 서버에 연결할 수 없거나 서버가 응답하지 않는 경우 VPN 연결이 설정됩니다. **ActionParameters : DomainAction = ConnectIfNeeded** 인 경우에만 유효합니다.
- **OnDemandRules : XML 콘텐츠:** XML 구성 주문형 규칙을 입력하거나 복사 후 붙여 넣습니다.
 - ★ 사전 확인을 클릭하여 XML 코드의 유효성을 검사합니다. XML 이 올바른 경우 **XML** 콘텐츠 텍스트 상자 아래 올바른 XML 이 녹색 텍스트로 표시됩니다. 올바르지 않은 경우 오류를 설명하는 오류 메시지가 주황색 텍스트로 표시됩니다.
- 프록시
 - 프록시 구성: 목록에서 프록시 서버를 통해 VPN 연결을 라우팅하는 방법을 선택합니다. 기본값은 없음입니다.
 - ★ 수동을 사용하는 경우 다음 설정을 구성합니다.
 - 프록시 서버의 호스트 이름 또는 **IP** 주소: 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - 프록시 서버용 포트: 프록시 서버 포트 번호를 입력합니다. 이것은 필수 필드입니다.
 - 사용자 이름: 선택적 프록시 서버 사용자 이름을 입력합니다.
 - 암호: 선택적 프록시 서버 암호를 입력합니다.
 - ★ 자동을 구성하는 경우 다음 설정을 구성합니다.
 - 프록시 서버 **URL**: 프록시 서버의 URL 을 입력합니다. 이것은 필수 필드입니다.
- 정책 설정
 - 정책 설정의 정책 제거 옆에서 날짜 선택 또는 제거할 때까지의 기간 (**시간**) 을 선택합니다.
 - 날짜 선택을 선택하는 경우 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - 사용자가 정책을 제거하도록 허용 목록에서 항상, 암호 필요 또는 안 함을 선택합니다.
 - 암호 필요를 선택하는 경우 제거 암호 옆에 필요한 암호를 입력합니다.

앱별 VPN 구성

iOS 에 대한 앱별 VPN 옵션은 Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO 및 사용자 지정 SSL 연결 유형에 사용할 수 있습니다.

앱별 VPN 을 구성하려면:

1. 구성 > 장치 정책에서 VPN 정책을 생성합니다. 예:

VPN Policy

1 Policy Info
2 Platforms
☒ iOS
☐ macOS
☐ Android
☐ Samsung SAFE
☐ Samsung KNOX
☐ Windows Phone
☐ Windows Desktop/Tablet
☐ Amazon
3 Assignment

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name

XenMobile

Connection type

Custom SSL

Custom SSL identifier (reverse DNS format) *

com.example.custom.identifier

Provider bundle identifier

com.example.bundle.identifier

Server name or IP address *

app-domain.example.com

User account

administrator

Authentication type for the connection

Password

Auth Password

Per-app VPN

Enable per-app VPN

ON

IOS 7.0+

On-demand match app enabled

ON

Provider type

App proxy

Safari domains

Back

Next >

VPN Policy

1 Policy Info
2 Platforms
☒ iOS
☐ macOS
☐ Android
☐ Samsung SAFE
☐ Samsung KNOX
☐ Windows Phone
☐ Windows Desktop/Tablet
☐ Amazon
3 Assignment

Enable per-app VPN

ON

IOS 7.0+

On-demand match app enabled

ON

Provider type

App proxy

Safari domains

Domain *

Add

Custom XML

Custom parameters

Parameter name *

Value

Add

Proxy

Proxy configuration

None

Policy Settings

Remove policy

☒ Select date
☐ Duration until removal (in hours)

Allow user to remove policy

Always

Deployment Rules

Back

Next >

2. 구성 > 장치 정책에서 앱을 앱별 VPN 정책에 연결하는 앱 특성 정책을 생성합니다. 앱별 VPN 식별자에 대해 1 단계에서 생성한 VPN 정책의 이름을 선택합니다. 관리되는 앱 번들 ID에 대해 앱 목록에서 선택하거나 앱 번들 ID를 입력합니다. (iOS 앱 인벤토리 정책을 배포하는 경우 앱 목록에 앱이 포함됩니다.)

App Attributes Policy

1 Policy Info
2 Platforms
☒ iOS
3 Assignment

App Attributes Policy

This policy lets you specify the attributes you want to add to apps on iOS devices.

Managed app bundle ID *

Add new

com.citrixonline.iOS.GoToMeeting

Per-app VPN identifier

PerAppVPN_Policy

Deployment Rules

• 정책 설정

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

780

- 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

1 Policy Info

2 Platforms

- ☐ iOS
- ☒ macOS
- ☐ Android
- ☒ Samsung SAFE
- ☐ Samsung KNOX
- ☐ Windows Phone
- ☐ Windows Desktop/Tablet
- ☐ Amazon

3 Assignment

Connection name

Connection type: L2TP

Server name or IP address *

User account: administrator

☒ Password authentication
☐ RSA SecureID authentication
☐ Kerberos authentication
☐ CryptoCard authentication

Shared secret

Send all traffic: OFF

Proxy configuration: None

Remove policy: ☒ Select date

Back Next >

- 연결 이름: 연결 이름을 입력합니다.
- 연결 유형: 목록에서 이 연결에 사용할 프로토콜을 선택합니다. 기본값은 L2TP 입니다.
 - **L2TP**: 미리 공유한 키 인증을 사용하는 계층 2 터널링 프로토콜입니다.
 - **PPTP**: 지점 간 터널링입니다.
 - **IPSec**: 회사 VPN 연결입니다.
 - **Cisco AnyConnect**: Cisco AnyConnect VPN 클라이언트입니다.
 - **Juniper SSL**: Juniper Networks SSL VPN 클라이언트입니다.
 - **F5 SSL**: F5 Networks SSL VPN 클라이언트입니다.
 - **SonicWALL Mobile Connect**: iOS 용 Dell 통합 VPN 클라이언트입니다.
 - **Ariba VIA**: Ariba Networks Virtual Internet Access 클라이언트입니다.
 - **Citrix VPN**: Citrix VPN 클라이언트입니다.
 - 사용자 지정 **SSL**: 사용자 지정 Secure Socket Layer 입니다.

다음 섹션에는 이전에 설명한 각 연결 유형에 대한 구성 옵션이 나열되어 있습니다.

macOS 용 L2TP 프로토콜 구성

- 서버 이름 또는 **IP 주소**: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 암호 인증, **RSA SecurID** 인증, **Kerberos** 인증 또는 **CryptoCard** 인증을 선택합니다. 기본값은 암호 인증입니다.
- 공유 암호: **IPsec** 공유 암호 키를 입력합니다.
- 모든 트래픽 보내기: VPN 을 통해 모든 트래픽을 보낼 지 여부를 선택합니다. 기본값은 꺼짐입니다.

macOS 용 PPTP 프로토콜 구성

- 서버 이름 또는 **IP 주소**: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 암호 인증, **RSA SecurID** 인증, **Kerberos** 인증 또는 **CryptoCard** 인증을 선택합니다. 기본값은 암호 인증입니다.
- 암호화 수준: 원하는 암호화 수준을 선택합니다. 기본값은 없음입니다.
 - 없음: 암호화를 사용하지 않습니다.
 - 자동: 서버에서 지원하는 가장 강력한 암호화 수준을 사용합니다.
 - 최대 (**128 비트**): 항상 128 비트 암호화를 사용합니다.
- 모든 트래픽 보내기: VPN 을 통해 모든 트래픽을 보낼 지 여부를 선택합니다. 기본값은 꺼짐입니다.

macOS 용 IPsec 프로토콜 구성

- 서버 이름 또는 **IP 주소**: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 공유 암호 또는 인증서를 선택합니다. 기본값은 공유 암호입니다.
 - 공유 암호 인증을 사용하는 경우 다음 설정을 구성합니다.
 - ★ 그룹 이름: 선택적 그룹 이름을 입력합니다.
 - ★ 공유 암호: 선택적 공유 암호 키를 입력합니다.
 - ★ 하이브리드 인증 사용: 하이브리드 인증을 사용할지 여부를 선택합니다. 하이브리드 인증을 사용하면 서버가 먼저 클라이언트에서 자체 인증된 후 클라이언트가 서버에서 자체 인증됩니다. 기본값은 꺼짐입니다.
 - ★ 암호 확인: 사용자가 네트워크에 연결할 때 암호 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 인증서 인증을 사용하는 경우 다음 설정을 구성합니다.
 - ★ ID 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 을 입력하도록 할지 여부를 선택합니다. 기본값은 꺼짐입니다.

- ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 옵션 구성을 참조하십시오.

macOS 용 Cisco AnyConnect 프로토콜 구성

- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 그룹: 선택적 그룹 이름을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ★ ID 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 옵션 구성을 참조하십시오.
 - 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - ★ 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - ★ **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - 도메인: 추가할 도메인을 입력합니다.
 - 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

macOS 용 Juniper SSL 프로토콜 구성

- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 영역: 선택적 영역 이름을 입력합니다.
- 역할: 선택적 역할 이름을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ★ ID 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.

- ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 설정 구성을 참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

macOS 용 F5 SSL 프로토콜 구성

- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ★ **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 설정 구성을 참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

macOS 용 SonicWALL Mobile Connect 프로토콜 구성

- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 로그인 그룹 또는 도메인: 선택적 로그인 그룹 또는 도메인을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 설정 구성을 참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * 도메인: 추가할 도메인을 입력합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

macOS 용 Ariba VIA 프로토콜 구성

- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 설정 구성을 참조하십시오.

- **앱별 VPN 사용:** 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

macOS 용 사용자 지정 SSL 프로토콜 구성

- 사용자 지정 **SSL** 식별자 (역방향 **DNS** 형식): SSL 식별자를 역방향 DNS 형식으로 입력합니다. 이것은 필수 필드입니다.
- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
 - 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - ★ **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - ★ 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - ★ 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜진 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 설정 구성을 참조하십시오.
 - **앱별 VPN:** 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - ★ 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - ★ **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - 도메인: 추가할 도메인을 입력합니다.
 - 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- 사용자 지정 **XML**: 추가할 각 사용자 지정 XML 매개 변수에 대해 추가를 클릭하고 다음을 수행합니다.
 - 매개 변수 이름: 추가할 매개 변수의 이름을 입력합니다.
 - 값: 매개 변수 이름에 연결된 값을 입력합니다.
 - 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.

주문형 VPN 사용 옵션 구성

- 주문형 도메인: 추가할 각 도메인 및 사용자가 도메인에 연결할 때 수행할 동작에 대해 추가를 클릭하고 다음을 수행합니다.
 - 도메인: 추가할 도메인을 입력합니다.
 - 동작: 목록에서 가능한 동작 중 하나를 선택합니다.
 - * 항상 설정: 도메인에서 항상 VPN 연결이 트리거됩니다.
 - * 설정 안 함: 도메인에서 VPN 연결이 트리거되지 않습니다.
 - * 필요한 경우 설정: 도메인 이름 확인에 실패하는 경우 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버에서 도메인을 확인할 수 없거나 다른 서버로 리디렉션되거나 시간 초과되는 경우 발생합니다.
 - 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- 주문형 규칙
 - 동작: 목록에서 수행할 동작을 선택합니다. 기본값은 **EvaluateConnection** 입니다. 가능한 동작은 다음과 같습니다.
 - * 허용: 트리거 시 주문형 VPN 연결을 허용합니다.
 - * 연결: VPN 연결을 무조건 시작합니다.
 - * 연결 끊기: VPN 연결을 제거하고 규칙이 일치하지 않는 한 주문형 VPN 에 다시 연결하지 않습니다.
 - * **EvaluateConnection**: 각 연결에 대한 **ActionParameters** 배열을 평가합니다.
 - * 무시: 기존 VPN 연결을 유지하지만 규칙이 일치하지 않는 한 주문형 VPN 에 다시 연결하지 않습니다.
 - **DNSDomainMatch**: 사용자 장치의 검색 도메인 목록과 일치할 수 있는 추가할 각 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **DNS** 도메인: 도메인 이름을 입력합니다. 와일드카드 "*" 접두사를 사용하여 여러 도메인을 일치할 수 있습니다. 예를 들어 *.example.com 은 mydomain.example.com, yourdomain.example.com 및 herdomain.example.com 과 일치합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
 - **DNSServerAddressMatch**: 네트워크의 지정된 DNS 서버와 일치할 수 있는 추가할 각 IP 주소에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **DNS** 서버 주소: 추가할 DNS 서버 주소를 입력합니다. 와일드카드 "*" 접미사를 사용하여 DNS 서버를 일치할 수 있습니다. 예를 들어 17.* 는 클래스 A 서브넷의 모든 DNS 서버와 일치합니다.
 - * 저장을 클릭하여 DNS 서버 주소를 저장하거나 취소를 클릭하여 DNS 서버 주소를 저장하지 않습니다.
 - **InterfaceTypeMatch**: 목록에서 사용하는 기본 네트워크 인터페이스 하드웨어 유형을 클릭합니다. 기본값은 지정되지 않음입니다. 가능한 값은 다음과 같습니다.
 - * 지정되지 않음: 모든 네트워크 인터페이스 하드웨어와 일치합니다. 이 옵션은 기본값입니다.
 - * 이더넷: 이더넷 네트워크 인터페이스 하드웨어만 일치합니다.
 - * WiFi: WiFi 네트워크 인터페이스 하드웨어만 일치합니다.
 - * 셀룰러: 셀룰러 네트워크 인터페이스 하드웨어만 일치합니다.
 - **SSIDMatch**: 현재 네트워크와 일치할 추가할 각 SSID 에 대해 추가를 클릭하고 다음을 수행합니다.

- ★ **SSID:** 추가할 SSID 를 입력합니다. 네트워크가 Wi-Fi 네트워크가 아닌 경우 또는 SSID 가 표시되지 않는 경우 일치가 실패합니다. 모든 SSID 와 일치하려면 이 목록을 비워 둡니다.
 - ★ 저장을 클릭하여 SSID 를 저장하거나 취소를 클릭하여 SSID 를 저장하지 않습니다.
 - **URLStringProbe:** 가져올 URL 을 입력합니다. 이 URL 을 리디렉션 없이 성공적으로 가져온 경우 이 규칙이 일치합니다.
 - **ActionParameters : Domains:** EvaluateConnection 이 검사하는 추가할 각 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
 - **ActionParameters : DomainAction:** 목록에서 지정된 **ActionParameters : Domains** 도메인에 대한 VPN 동작을 선택합니다. 기본값은 **ConnectIfNeeded** 입니다. 가능한 동작은 다음과 같습니다.
 - ★ **ConnectIfNeeded:** 도메인 이름 확인에 실패하는 경우 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버에서 도메인을 확인할 수 없거나 다른 서버로 리디렉션되거나 시간 초과되는 경우 발생합니다.
 - ★ **NeverConnect:** 도메인에서 VPN 연결이 트리거되지 않습니다.
 - **ActionParameters: RequiredDNSServers:** 지정된 도메인을 확인할 때 사용할 각 DNS 서버 IP 주소에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ **DNS 서버: ActionParameters : DomainAction = ConnectIfNeeded** 인 경우에만 유효합니다. 추가할 DNS 서버를 입력합니다. 이 서버는 장치의 현재 네트워크 구성에 포함된 서버가 아니어도 됩니다. DNS 서버에 연결할 수 없는 경우 VPN 연결이 대신 설정됩니다. 이 DNS 서버는 내부 DNS 서버 또는 신뢰할 수 있는 외부 DNS 서버여야 합니다.
 - ★ 저장을 클릭하여 DNS 서버를 저장하거나 취소를 클릭하여 DNS 서버를 저장하지 않습니다.
 - **ActionParameters : RequiredURLStringProbe:** 필요한 경우 GET 요청을 사용하여 검색할 HTTP 또는 HTTPS(기본 설정) URL 을 입력합니다. URL 의 호스트 이름을 확인할 수 없거나 서버에 연결할 수 없거나 서버가 응답하지 않는 경우 VPN 연결이 설정됩니다. **ActionParameters : DomainAction = ConnectIfNeeded** 인 경우에만 유효합니다.
 - **OnDemandRules : XML 콘텐츠:** XML 구성 주문형 규칙을 입력하거나 복사 후 붙여 넣습니다.
 - ★ 사전 확인을 클릭하여 XML 코드의 유효성을 검사합니다. XML 이 올바른 경우 **XML** 콘텐츠 텍스트 상자 아래 올바른 XML 이 녹색 텍스트로 표시됩니다. 올바르지 않은 경우 오류를 설명하는 오류 메시지가 주황색 텍스트로 표시됩니다.
- 프록시
 - 프록시 구성: 목록에서 프록시 서버를 통해 VPN 연결을 라우팅하는 방법을 선택합니다. 기본값은 없음입니다.
 - ★ 수동을 사용하는 경우 다음 설정을 구성합니다.
 - 프록시 서버의 호스트 이름 또는 IP 주소: 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - 프록시 서버용 포트: 프록시 서버 포트 번호를 입력합니다. 이것은 필수 필드입니다.
 - 사용자 이름: 선택적 프록시 서버 사용자 이름을 입력합니다.
 - 암호: 선택적 프록시 서버 암호를 입력합니다.

★ 자동을 구성하는 경우 다음 설정을 구성합니다.

- 프록시 서버 **URL**: 프록시 서버의 URL 을 입력합니다. 이것은 필수 필드입니다.

Android 설정

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<div> <div>Connection name *</div> <input type="text"/> ⓘ </div> <div> <div>Server name or IP address *</div> <input type="text"/> ⓘ </div> <div> <div>Connection type</div> <div>Cisco AnyConnect</div> </div> <div> <div>Identity credential</div> <div>None</div> ⓘ </div> <div> <div>Cisco AnyConnect VPN</div> <div>Backup VPN server</div> <input type="text"/> ⓘ </div> <div> <div>User group</div> <input type="text"/> ⓘ </div> <div> <div>Trusted Networks</div> <div>Automatic VPN policy</div> <div>OFF ⓘ</div> </div>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Samsung SAFE <input checked="" type="checkbox"/> Samsung KNOX <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Amazon	<div>▶ Deployment Rules</div>
3 Assignment	

Android 용 Cisco AnyConnect VPN 프로토콜 구성

- 연결 이름: Cisco AnyConnect VPN 연결의 이름을 입력합니다. 이것은 필수 필드입니다.
- 서버 이름 또는 IP 주소: VPN 서버의 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
- ID 자격 증명: 목록에서 ID 자격 증명을 선택합니다.
- 백업 VPN 서버: 백업 VPN 서버 정보를 입력합니다.
- 사용자 그룹: 사용자 그룹 정보를 입력합니다.
- 신뢰할 수 있는 네트워크
 - 자동 VPN 정책: 이 옵션을 사용하거나 사용하지 않도록 설정하여 VPN 이 신뢰할 수 있는 네트워크 및 신뢰할 수 없는 네트워크에 반응하는 방법을 설정합니다. 사용하는 경우 다음 설정을 구성합니다.
 - ★ 신뢰할 수 있는 네트워크 정책: 목록에서 원하는 정책을 선택합니다. 기본값은 연결 끊기입니다. 사용 가능한 옵션은 다음과 같습니다.
 - 연결 끊기: 클라이언트가 신뢰할 수 있는 네트워크에서 VPN 연결을 종료합니다. 이 설정은 기본값입니다.
 - 연결: 클라이언트가 신뢰할 수 있는 네트워크에서 VPN 연결을 시작합니다.
 - 아무 작업도 하지 않음: 클라이언트가 아무런 동작을 수행하지 않습니다.
 - 일시 중지: 사용자가 신뢰할 수 있는 네트워크 외부에서 VPN 세션을 설정한 후 신뢰할 수 있는 네트워크로 구성된 네트워크로 들어가면 VPN 세션이 일시 중지됩니다. 사용자가 신뢰할 수 있는 네트워크에서 다시 나가면 세션이 다시 시작됩니다. 이 설정을 사용하면 신뢰할 수 있는 네트워크에서 나간 후 새 VPN 세션을 설정할 필요가 없습니다.

- ★ 신뢰할 수 없는 네트워크 정책: 목록에서 원하는 정책을 선택합니다. 기본값은 연결입니다. 사용 가능한 옵션은 다음과 같습니다.
 - 연결: 클라이언트가 신뢰할 수 없는 네트워크에서 VPN 연결을 시작합니다.
 - 아무 작업도 하지 않음: 클라이언트가 신뢰할 수 없는 네트워크에서 VPN 연결을 시작합니다. 이 옵션을 사용하면 항상 VPN 연결이 사용되지 않습니다.
- 신뢰할 수 있는 도메인: 클라이언트가 신뢰할 수 있는 도메인에 있을 때 네트워크 인터페이스에 포함되는 각 도메인 접미사에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 도메인: 추가할 도메인을 입력합니다.
 - ★ 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- 신뢰할 수 있는 서버: 클라이언트가 신뢰할 수 있는 도메인에 있을 때 네트워크 인터페이스에 포함되는 각 서버 주소에 대해 추가를 클릭하고 다음을 수행합니다.
 - ★ 서버: 추가할 서버를 입력합니다.
 - ★ 저장을 클릭하여 서버를 저장하거나 취소를 클릭하여 서버를 저장하지 않습니다.

Android 용 Citrix SSO 프로토콜 구성

- 연결 이름: VPN 연결의 이름을 입력합니다. 이것은 필수 필드입니다.
 - 서버 이름 또는 IP 주소: Citrix Gateway 의 FQDN 또는 IP 주소를 입력합니다.
 - 연결에 대한 인증 유형: 인증 유형을 선택하고 유형에 대해 나타나는 다음 필드를 모두 작성합니다.
 - 사용자 이름 및 암호: 암호 또는 암호 및 인증서의 인증 유형에 대한 VPN 자격 증명을 입력합니다. 선택 사항입니다. VPN 자격 증명을 입력하지 않으면 Citrix VPN 앱에 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
 - ID 자격 증명: 인증 유형이 인증서 또는 암호 및 인증서인 경우 표시됩니다. 목록에서 ID 자격 증명을 선택합니다.
 - 앱별 VPN 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 앱별 VPN 을 사용하지 않는 경우 모든 트래픽이 Citrix VPN 터널을 통과합니다. 앱별 VPN 을 사용하는 경우 다음 설정을 지정합니다. 기본값은 꺼짐입니다.
 - 화이트리스트 또는 블랙리스트: 화이트리스트인 경우 허용된 모든 앱이 이 VPN 터널을 통과합니다. 블랙리스트인 경우 차단 목록의 앱을 제외한 모든 앱이 이 VPN 터널을 통과합니다.
- 참고:

XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는 용어가 포함됩니다. 향후 릴리스에 이러한 용어를 “차단 목록” 및 “허용 목록” 으로 변경하는 중입니다.
- 응용 프로그램 목록: 허용되거나 차단된 앱을 지정합니다. 추가를 클릭한 다음 앱 패키지 이름의 쉼표로 구분된 목록을 입력합니다.
 - 사용자 지정 XML: 추가를 클릭한 다음 사용자 지정 매개 변수를 입력합니다. XenMobile 은 Citrix VPN 에 대해 다음 매개 변수를 지원합니다.

- **DisableUserProfiles:** 선택 사항입니다. 이 매개 변수를 사용하려면 값에 예를 입력합니다. 사용하도록 설정한 경우 XenMobile 은 사용자가 추가한 VPN 연결을 표시하지 않으며 사용자가 연결을 추가할 수 없습니다. 이 설정은 글로벌 제한이며 모든 VPN 프로필에 적용됩니다.
- **userAgent:** 문자열 값입니다. 각 HTTP 요청에 보낼 사용자 지정 사용자 에이전트 문자열을 지정할 수 있습니다. 지정한 사용자 에이전트 문자열이 기존 Citrix VPN 사용자 에이전트에 추가됩니다.

NAC 를 지원하도록 VPN 구성

1. 연결 유형을 사용자 지정 **SSL** 로 사용하여 NAC 필터를 구성합니다.
2. **VPN** 의 연결 이름을 지정합니다.
3. 사용자 지정 **XML** 에서 추가를 클릭하고 다음을 수행합니다.
 - 매개 변수 이름: **XenMobileDeviceId** 를 입력합니다. 이 필드는 XenMobile 의 장치 등록을 기준으로 NAC 확인에 사용할 장치 ID 입니다. XenMobile 에서 장치를 등록하고 관리하는 경우 VPN 연결이 허용됩니다. 그렇지 않으면 VPN 설정 시 인증이 거부됩니다.
 - 값: **XenMobileDeviceId** 매개 변수의 값인 **DeviceID_\${device.id}** 를 입력합니다.
 - 저장을 클릭하여 매개 변수를 저장합니다.

Android Enterprise 에 대한 VPN 구성

Android Enterprise 장치에 대한 VPN 을 구성하려면 Citrix SSO 앱에 대한 관리되는 구성 장치 정책을 만듭니다. [Android Enterprise 에 대한 VPN 프로필 구성](#)을 참조하십시오.

Windows 데스크톱/태블릿 설정

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<div> <div>Connection name *</div> <input type="text"/> </div> <div> <div>Profile type</div> <div>Native</div> </div> <div> <div>Server address *</div> <input type="text"/> </div> <div> <div>Remember credential</div> <div>OFF</div> </div> <div> <div>DNS suffix</div> <input type="text"/> </div> <div> <div>Tunnel type *</div> <div>L2TP</div> </div> <div> <div>Authentication method *</div> <div>EAP</div> </div> <div> <div>EAP method *</div> <div>TLS</div> </div> <div> <div>Trusted networks</div> <input type="text"/> </div> <div> <div>Require smart card certificate</div> <div>OFF</div> </div> <div> <div>Automatically select client certificate</div> <div>OFF</div> </div> <div> <div>Always-on VPN</div> <div>OFF</div> </div> <div> <div>Reset For Local</div> <div>OFF</div> </div>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung KNOX <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Amazon	
3 Assignment	

Back

Next >

- **연결 이름:** 연결 이름을 입력합니다. 이것은 필수 필드입니다.
- **프로필 유형:** 목록에서 기본 또는 플러그인을 선택합니다. 기본값은 기본입니다.
- **기본 프로필 유형 구성:** 사용자의 Windows 장치에 기본 제공되는 VPN에 적용되는 설정입니다.
 - **서버 주소:** VPN 서버의 FQDN 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - **자격 증명 저장:** 자격 증명을 캐시할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하면 가능한 경우 항상 자격 증명이 캐시됩니다.
 - **DNS 접미사:** DNS 접미사를 입력합니다.
 - **터널 유형:** 목록에서 사용할 VPN 터널 유형을 선택합니다. 기본값은 **L2TP**입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **L2TP:** 미리 공유한 키 인증을 사용하는 계층 2 터널링 프로토콜입니다.
 - * **PPTP:** 지점 간 터널링입니다.
 - * **IKEv2:** Internet Key Exchange 버전 2입니다.
 - **인증 방법:** 목록에서 사용할 인증 방법을 선택합니다. 기본값은 **EAP**입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **EAP:** Extended Authentication Protocol의 약어로 확장 인증 프로토콜을 의미합니다.
 - * **MSChapV2:** Microsoft의 Challenge Handshake 인증을 상호 인증에 사용합니다. **IKEv2**를 터널 유형으로 선택하는 경우 이 옵션을 사용할 수 없습니다.
 - **EAP 방법:** 목록에서 사용할 EAP 방법을 선택합니다. 기본값은 **TLS**입니다. MSChapV2 인증을 사용하는 경우 이 필드를 사용할 수 없습니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **TLS:** 전송 계층 보안
 - * **PEAP:** 보호되는 확장 인증 프로토콜
 - **신뢰할 수 있는 네트워크:** 액세스 시 VPN 연결이 필요하지 않은 네트워크 목록을 심표로 구분하여 입력합니다. 예를 들어 회사 무선 네트워크에 있는 사용자는 보호되는 리소스에 직접 액세스할 수 있습니다.
 - **스마트 카드 인증서 필요:** 스마트 카드 인증서가 필요한지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **자동으로 클라이언트 인증서 선택:** 인증에 사용할 클라이언트 인증서를 자동으로 선택할지 여부를 선택합니다. 기본값은 꺼짐입니다. 스마트 카드 인증서 필요를 사용하는 경우 이 옵션을 사용할 수 없습니다.
 - **항상 VPN 연결:** VPN을 항상 연결할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하는 경우 사용자가 수동으로 연결을 끊기 전까지 VPN 연결이 연결된 상태로 유지됩니다.
 - **로컬에 대해서는 바이패스:** 로컬 리소스의 프록시 서버 바이패스를 허용할 주소 및 포트 번호를 입력합니다.
- **플러그인 프로필 유형 구성:** Windows 스토어에서 가져와 사용자 장치에 설치한 VPN 플러그인에 적용되는 설정입니다.
 - **서버 주소:** VPN 서버의 FQDN 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - **자격 증명 저장:** 자격 증명을 캐시할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하면 가능한 경우 항상 자격 증명이 캐시됩니다.
 - **DNS 접미사:** DNS 접미사를 입력합니다.
 - **클라이언트 앱 ID:** VPN 플러그인의 패키지 제품군 이름을 입력합니다.
 - **플러그인 프로필 XML:** 찾아보기를 클릭하고 파일 위치로 이동하여 사용할 사용자 지정 VPN 플러그인을 선택합니다. 형식 및 세부 정보는 플러그인 공급자에게 문의하십시오.

- 신뢰할 수 있는 네트워크: 액세스 시 VPN 연결이 필요하지 않은 네트워크 목록을 심표로 구분하여 입력합니다. 예를 들어 회사 무선 네트워크에 있는 사용자는 보호되는 리소스에 직접 액세스할 수 있습니다.
- 항상 **VPN 연결**: VPN 을 항상 연결할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하는 경우 사용자가 수동으로 연결을 끊기 전까지 VPN 연결이 연결된 상태로 유지됩니다.
- 로컬에 대해서는 바이패스: 로컬 리소스의 프록시 서버 바이패스를 허용할 주소 및 포트 번호를 입력합니다.

배경 화면 장치 정책

August 18, 2021

iOS 장치 잠금 화면, 홈 화면 또는 둘 다에 배경 화면을 설정할.png 또는.jpg 파일을 추가할 수 있습니다. iOS 7.1.2 이상에서는 감독되는 장치에만 사용할 수 있습니다. iPad 및 iPhone 에서 서로 다른 배경 화면을 사용하려면 서로 다른 배경 화면 정책을 만들어 해당 사용자에게 배포해야 합니다.

다음 표에는 iOS 장치에 대한 Apple 의 권장 이미지 크기가 나와 있습니다.

iPhone

장치	이미지 크기 (픽셀)
iPhone 12 Pro Max	2778 x 1284
iPhone 12 및 iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 2 세대	1334 x 750
iPhone 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 Plus	1334 x 750
iPhone 8	1334 x 750

iPad

장치	이미지 크기 (픽셀)
iPad Pro (1, 2, 3 세대 12.9 인치)	2732 x 2048
iPad Pro 10.5 인치	2224 x 1668
iPad Pro(9.7 인치)	1536 x 2048
iPad Air 2	2048 x 1536

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- 적용 대상: 목록에서 잠금 화면, 홈 (아이콘 목록) 화면 또는 잠금 및 홈 화면을 선택하여 배경 화면이 나타날 위치를 설정합니다.
- 배경 화면 파일: 찾아보기를 클릭하고 파일 위치로 이동하여 배경 화면 파일을 선택합니다.

웹 콘텐츠 필터 장치 정책

January 5, 2022

허용 및 차단 목록에 추가한 특정 사이트와 함께 Apple의 자동 필터 기능을 사용하여 iOS 장치에서 웹 콘텐츠를 필터링하는 장치 정책을 XenMobile에서 추가할 수 있습니다. 감독 모드에서 iOS 7.0 이상의 장치에서만 이 정책을 사용할 수 있습니다. iOS 장치를 감독 모드로 설정하는 방법에 대한 자세한 내용은 [Apple Configurator를 사용하여 iOS 장치를 감독 모드로 전환](#)을 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- 필터 유형: 목록에서 기본 제공 또는 플러그인을 클릭한 후 선택한 옵션에 대한 절차를 따릅니다. 기본값은 기본 제공입니다.

기본 제공 필터 유형

- 웹 콘텐츠 필터

- 자동 필터 사용: **Apple**의 자동 필터 기능을 사용하여 웹 사이트의 부적절한 콘텐츠를 분석할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 허용 **URL**: 자동 필터 사용이 꺼짐으로 설정된 경우 이 목록이 무시됩니다. 자동 필터 사용이 켜짐으로 설정된 경우 자동 필터가 액세스를 허용하는지 여부에 관계없이 항상 이 목록의 항목에 액세스할 수 있습니다. 허용 목록에 추가할 각 URL에 대해 추가를 클릭하여 다음을 수행합니다.
 - * 허용된 웹 사이트의 URL을 입력합니다. 웹 주소 앞에 **http://** 또는 **https://**를 추가해야 합니다.
 - * 웹 사이트를 허용 목록에 저장하려면 저장을 클릭하고, 저장하지 않으려면 취소를 클릭합니다.
 - 블랙리스트 **URL**: 이 목록의 항목은 항상 차단됩니다. 차단 목록에 추가할 각 URL에 대해 추가를 클릭하여 다음을 수행합니다.
 - * 차단할 웹 사이트의 URL을 입력합니다. 웹 주소 앞에 **http://** 또는 **https://**를 추가해야 합니다.
 - * 웹 사이트를 차단 목록에 저장하려면 저장을 클릭하고, 저장하지 않으려면 취소를 클릭합니다.
- 참고:
- XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트”라는 용어가 포함됩니다. 향후 릴리스에서 이러한 용어를 “차단 목록” 및 “허용 목록”으로 변경하는 중입니다.

• 책갈피 화이트리스트

- 책갈피 화이트리스트: 사용자가 액세스할 수 있는 사이트를 지정합니다. 웹 사이트에 액세스할 수 있도록 하려면 해당 웹 사이트의 URL을 추가합니다.
 - * **URL**: 사용자가 액세스할 수 있는 각 웹 사이트의 URL입니다. 예를 들어 Secure Hub 스토어에 액세스할 수 있도록 하려면 **URL** 목록에 XenMobile Server URL을 추가합니다. 웹 주소 앞에 **http://** 또는 **https://**를 추가해야 합니다. 이것은 필수 필드입니다.
 - * 책갈피 폴더: 선택적 책갈피 폴더 이름을 입력합니다. 이 필드를 비워 두면 책갈피가 책갈피 기본 디렉터리에 추가됩니다.
 - * 제목: 웹 사이트를 설명하는 제목을 입력합니다. 예를 들어, URL이 **https://google.com**인 경우 “Google”을 입력합니다.
 - * 웹 사이트를 허용 목록에 저장하려면 저장을 클릭하고, 저장하지 않으려면 취소를 클릭합니다.

플러그인 필터 유형

- 필터 이름: 필터에 대한 고유한 이름을 입력합니다.
- 식별자: 필터링 서비스를 제공하는 플러그인의 번들 ID를 입력합니다.
- 서비스 주소: 선택적 서버 주소를 입력합니다. 올바른 형식은 IP 주소, 호스트 이름 또는 URL입니다.
- 사용자 이름: 서비스에 대한 선택적 사용자 이름을 입력합니다.
- 암호: 서비스에 대한 선택적 암호를 입력합니다.
- 인증서: 목록에서 서비스에 사용자를 인증하는 데 사용할 선택적 ID 인증서를 클릭합니다. 기본값은 없음입니다.
- **WebKit** 트래픽 필터링: WebKit 트래픽을 필터링할 것인지를 선택합니다.
- 소켓 트래픽 필터링: 소켓 트래픽을 필터링할 것인지를 선택합니다.
- 사용자 지정 데이터: 웹 필터에 추가할 각 사용자 지정 키에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 키: 사용자 지정 키를 입력합니다.

- 값: 사용자 지정 키 값을 입력합니다.
- 사용자 지정 키를 저장하려면 저장을 클릭하고, 저장하지 않으려면 취소를 클릭합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

웹 클립 장치 정책

January 5, 2022

웹 사이트에 대한 바로 가기 또는 웹 클립을 배치하여 앱과 나란히 사용자 장치에 표시할 수 있습니다. iOS, iPadOS, macOS X 및 Android 장치의 웹 클립을 나타내는 사용자 지정 아이콘을 지정할 수 있습니다. Windows 태블릿에는 레이블과 URL 만 필요합니다. iOS 및 iPadOS 장치의 경우 만든 웹 클립을 구성하도록 홈 화면 레이아웃 장치 정책을 구성합니다. iOS 에서 앱 액세스를 제한할 경우 웹 클립을 허용하도록 제한 장치 정책을 구성해야 합니다. 이러한 정책 구성에 대한 자세한 내용은 [홈 화면 레이아웃 장치 정책](#) 및 [제한 장치 정책](#)을 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

iOS 설정

- 레이블: 웹 클립과 함께 표시할 레이블을 입력합니다.
- URL: 웹 클립과 연관된 URL 을 입력합니다. URL 은 프로토콜 (예: <https://server>) 로 시작해야 합니다.
- 제거 가능: 사용자가 웹 클립을 제거할 수 있는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 업데이트할 아이콘: 찾아보기를 클릭하고 파일의 위치로 이동하여 웹 클립에 사용할 아이콘을 선택합니다.
- 미리 작성된 아이콘: 아이콘에 적용된 효과 (둥근 모서리, 그림자 및 반사 광택) 가 있는지 여부를 선택합니다. 기본값은 효과를 추가하는 꺼짐입니다.
- 전체 화면: 링크된 웹 페이지를 전체 화면 모드로 열지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- 레이블: 웹 클립과 함께 표시할 레이블을 입력합니다.
- **URL:** 웹 클립과 연관된 URL 을 입력합니다. URL 은 프로토콜 (예: <https://server>) 로 시작해야 합니다.
- 업데이트할 아이콘: 찾아보기를 클릭하고 파일의 위치로 이동하여 웹 클립에 사용할 아이콘을 선택합니다.

Android 설정

- 규칙: 이 정책으로 웹 클립을 추가할지 아니면 제거할지 선택합니다. 기본값은 추가입니다.
- 레이블: 웹 클립과 함께 표시할 레이블을 입력합니다.
- **URL:** 웹 클립과 연관된 URL 을 입력합니다.
- 아이콘 정의: 아이콘 파일 사용 여부를 선택합니다. 기본값은 꺼짐입니다.
- 아이콘 파일: 아이콘 정의가 켜짐인 경우 찾아보기를 클릭하고 파일 위치로 이동하여 사용할 아이콘 파일을 선택합니다.
- 정책 설정
 - 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - * 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - * 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다.
 - 사용자가 정책을 제거하도록 허용: 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 항상, 암호 필요 또는 안 함을 선택합니다. 암호 필요를 선택한 경우 제거 암호필드에 암호를 입력합니다.
 - 프로필 범위: 이 정책을 사용자에게 적용할지, 전체 시스템에 적용할지 선택합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Windows 데스크톱/태블릿 설정

- 이름: 웹 클립과 함께 표시할 레이블을 입력합니다.
- **URL:** 웹 클립과 연관된 URL 을 입력합니다.

Wi-Fi 장치 정책

November 27, 2023

XenMobile 에서 Wi-Fi 장치 정책을 새로 만들거나 기존 Wi-Fi 장치 정책을 편집하려면 구성 > 장치 정책 페이지를 사용합니다. Wi-Fi 정책을 사용하면 다음 항목을 정의하여 사용자가 장치를 Wi-Fi 네트워크에 연결하는 방식을 관리할 수 있습니다.

- 네트워크 이름 및 유형

- 인증 및 보안 정책
- 프록시 서버 사용
- 기타 WiFi 관련 정보

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

사전 요구 사항

정책을 만들려면 먼저 다음 단계를 완료해야 합니다.

- 사용하려는 배달 그룹을 만듭니다.
- 네트워크 이름과 유형을 파악합니다.
- 사용할 인증 또는 보안 유형을 파악합니다.
- 필요할 수 있는 프록시 서버 정보를 파악합니다.
- 필요한 모든 CA 인증서를 설치합니다.
- 필요한 공유 키를 확보합니다.
- 인증서 기반 인증을 위한 PKI 엔터티를 만듭니다.
- 자격 증명 공급자를 구성합니다.

자세한 내용은 [인증](#) 및 그 하위 문서를 참조하십시오.

iOS 설정

WiFi Policy	WiFi Policy
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	<div>Network type: Standard</div> <div>Network name *</div> <div>Hidden network (enable if network is open or off): OFF</div> <div>Auto Join (automatically join this wireless network): ON</div> <div>Disable Captive Network Detection: OFF</div> <div>Use static MAC address: OFF</div> <div>Security type: None</div> <div>Proxy server settings</div> <div>QoS Settings</div> <div>Fast Lane QoS Marking: Do not restrict QoS marking</div> <div>Policy Settings</div> <div>Remove policy: Select date</div> <div>Duration until removal (in hours)</div>
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
<input checked="" type="checkbox"/> Android (legacy DA)	
<input checked="" type="checkbox"/> Android Enterprise	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- 네트워크 유형: 목록에서 표준, 레거시 핫스팟 또는 **Hotspot 2.0** 을 선택하여 사용할 네트워크 유형을 설정합니다.
- 네트워크 이름: 장치의 사용 가능한 네트워크 목록에 표시되는 SSID 를 입력합니다. **Hotspot 2.0** 에는 적용되지 않습니다.
- 숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용): 네트워크를 숨길지 여부를 선택합니다.
- 자동 참가 (이 무선 네트워크에 자동 참가): 네트워크를 자동으로 참가시킬지 여부를 선택합니다. iOS 장치가 이미 다른 네트워크에 연결되어 있으면 이 네트워크에 연결되지 않습니다. 장치가 자동으로 연결되기 전에 사용자가 이전 네트워크와의 연결을 끊어야 합니다. 기본값은 꺼짐입니다.
- 정적 MAC 주소 사용: MAC 주소는 장치가 네트워크 내에서 전송하는 고유 식별자입니다. 개인 정보 보호를 강화하기 위해 iOS 및 iPadOS 장치에서는 네트워크에 연결할 때마다 다른 MAC 주소를 사용할 수 있습니다. 꺼짐인 경우 장치에서 이 네트워크에 연결할 때 항상 동일한 MAC 주소를 사용합니다. 꺼짐인 경우 장치에서 이 네트워크에 연결할 때마다 다른 MAC 주소를 사용합니다. 기본값은 꺼짐입니다.
- 보안 유형: 목록에서 사용하려는 보안 유형을 선택합니다. **Hotspot 2.0** 에는 적용되지 않습니다.
 - 없음 - 추가 구성이 필요 없습니다.
 - WEP
 - WPA/WPA2 개인
 - 임의 (개인)
 - WEP 엔터프라이즈
 - WPA/WPA2 엔터프라이즈: WPA-2 엔터프라이즈를 사용하려면 SCEP(단순 인증서 등록 프로토콜) 을 구성해야 합니다. 그런 다음 XenMobile 에서 장치에 인증서를 보내 Wi-Fi 서버 인증을 수행할 수 있습니다. SCEP 를 구성하려면 설정 > 자격 증명 공급자의 배포 페이지로 이동합니다. 자세한 내용은 [자격 증명 공급자](#)를 참조하십시오.
 - 임의 (엔터프라이즈)

다음 섹션에는 위의 각 연결 유형에 대해 구성하는 옵션이 나열되어 있습니다.

iOS 의 WPA, WPA 개인, 임의 (개인) 설정

암호: 선택적 암호를 입력합니다. 이 필드를 공백으로 두면 사용자가 로그인할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.

iOS 의 WEP 엔터프라이즈, WPA 엔터프라이즈, WPA2 엔터프라이즈, 임의 (엔터프라이즈) 설정

이러한 설정 중 하나를 선택하면 해당 설정이 프록시 서버 설정 뒤에 나열됩니다.

- 프로토콜, 허용되는 EAP 유형: 지원할 EAP 유형을 사용하도록 설정한 후 관련 설정을 구성합니다. 사용 가능한 각 EAP 유형에서 기본값은 꺼짐입니다.
- 내부 인증 (TTLS): TTLS 를 사용하는 경우에만 필요합니다. 목록에서 사용할 내부 인증 방법을 선택합니다. 사용 가능한 옵션은 PAP, CHAP, MSCHAP 또는 MSCHAPv2 입니다. 기본값은 MSCHAPv2 입니다.
- 프로토콜, EAP-FAST: PAC(보호 액세스 자격 증명) 를 사용할지 여부를 선택합니다.

- **PAC** 사용을 선택하는 경우 프로비저닝 PAC 를 사용할지 여부를 선택합니다.
 - * **PAC** 프로비전을 선택하는 경우 최종 사용자 클라이언트와 XenMobile 간에 익명 TLS 핸드셰이크를 허용할 것인지 선택합니다.
 - 익명으로 **PAC** 프로비전
- 인증:
 - 사용자 이름: 사용자 이름을 입력합니다.
 - 연결별 암호: 사용자가 로그인할 때마다 암호를 요구할지 여부를 선택합니다.
 - 암호: 선택적 암호를 입력합니다. 이 필드를 공백으로 두면 사용자가 로그인할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.
 - ID 자격 증명 (키 저장소 또는 **PKI** 자격 증명): 목록에서 ID 자격 증명의 유형을 선택합니다. 기본값은 없음입니다.
 - 외부 ID: **PEAP**, **TTLS** 또는 **EAP-FAST** 를 사용하도록 설정하는 경우에만 필요합니다. 외부에 표시되는 사용자 이름을 입력합니다. 사용자 이름이 표시되지 않도록 “익명” 같은 일반 용어를 입력하여 보안을 강화할 수 있습니다.
 - **TLS** 인증서 필요: TLS 인증서를 요구할지 여부를 선택합니다.
- 신뢰
 - 신뢰할 수 있는 인증서: 신뢰할 수 있는 인증서를 추가하려면 추가를 클릭하고 추가하려는 각 인증서에 대해 다음을 수행합니다.
 - * 응용 프로그램: 목록에서 추가하려는 응용 프로그램을 선택합니다.
 - * 저장을 클릭하여 인증서를 저장하거나 취소를 클릭합니다.
 - 신뢰할 수 있는 서버 인증서 이름: 신뢰할 수 있는 인증서의 일반 이름을 추가하려면 추가를 클릭하고 추가하려는 각 이름에 대해 다음을 수행합니다.
 - * 인증서: 서버 인증서의 이름을 입력합니다. 와일드카드를 사용하여 `wpa*.example.com` 과 같은 이름을 지정할 수 있습니다.
 - * 저장을 클릭하여 인증서 이름을 저장하거나 취소를 클릭합니다.
- 신뢰 예외 허용: 인증서를 신뢰할 수 없는 경우 사용자 장치에 인증서 신뢰 대화 상자를 표시할 것인지 선택합니다. 기본값은 켜짐입니다.
- 프록시 서버 설정
 - 프록시 구성: 목록에서 없음, 수동 또는 자동을 선택하여 VPN 연결이 프록시 서버를 통해 라우팅되는 방법을 설정한 다음 추가적인 옵션을 모두 구성합니다. 기본값은 없음이며 이 경우 추가적인 구성이 필요하지 않습니다.
 - 수동을 선택하는 경우 다음 설정을 구성합니다.
 - * 호스트 이름/IP 주소: 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
 - * 포트: 프록시 서버 포트 번호를 입력합니다.
 - * 사용자 이름: 프록시 서버 인증에 사용할 선택적 사용자 이름을 입력합니다.
 - * 암호: 프록시 서버 인증에 사용할 선택적 암호를 입력합니다.
 - 자동을 선택하는 경우 다음 설정을 구성합니다.

- ★ 서버 **URL**: 프록시 구성을 정의하는 PAC 파일의 URL 을 입력합니다.
- ★ **PAC** 에 연결할 수 없는 경우 직접 연결 허용: PAC 파일에 연결할 수 없는 경우 대상에 직접 연결할 수 있도록 할지 여부를 선택합니다. 기본값은 켜짐입니다. 이 옵션은 iOS 7.0 이상에서만 사용할 수 있습니다.

• 정책 설정

- 정책 제거: 정책 제거를 예약할 때 사용할 방법을 선택합니다. 사용 가능한 옵션은 날짜 선택과 제거할 때까지의 기간 (시간) 입니다.
 - ★ 날짜 선택: 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
 - ★ 제거할 때까지의 기간 (시간): 정책 제거가 발생할 때까지 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

The screenshot displays the 'Wi-Fi' policy configuration interface in the XenMobile Server console. The left sidebar shows the 'Device Policies' section with 'Wi-Fi' selected. The main area shows the 'Wi-Fi' policy settings, including Network type (Standard), Network name, Hide network (OFF), Automatically join this wireless network (ON), Security type (None), Priority (0), Proxy configuration (None), Remove policy (Select date), Allow user to remove policy (Always), and Profile scope (User).

- 네트워크 유형: 목록에서 표준, 레거시 핫스팟 또는 **Hotspot 2.0** 을 선택하여 사용할 네트워크 유형을 설정합니다.
- 네트워크 이름: 장치의 사용 가능한 네트워크 목록에 표시되는 SSID 를 입력합니다. **Hotspot 2.0** 에는 적용되지 않습니다.
- 네트워크 숨기기: 네트워크를 숨길지 여부를 선택합니다.
- 이 무선 네트워크에 자동 참가: 네트워크를 자동으로 참가시킬지 여부를 선택합니다. 장치가 이미 다른 네트워크에 연결되어 있으면 이 네트워크에 연결되지 않습니다. 장치가 자동으로 연결되기 전에 사용자가 이전 네트워크와의 연결을 끊어야 합니다. 기본값은 켜짐입니다.
- 보안 유형: 목록에서 사용하려는 보안 유형을 선택합니다. **Hotspot 2.0** 에는 적용되지 않습니다.

- 없음 - 추가 구성이 필요 없습니다.
 - WEP
 - WPA/WPA2 개인
 - 임의 (개인)
 - WEP 엔터프라이즈
 - WPA/WPA2 엔터프라이즈
 - 임의 (엔터프라이즈)
- **우선 순위:** 네트워크가 여러 개인 경우 우선 순위 필드에 숫자를 입력하여 네트워크 연결의 우선 순위를 설정합니다. 장치는 번호가 가장 낮은 네트워크를 선택합니다.

다음 섹션에는 위의 각 연결 유형에 대해 구성하는 옵션이 나열되어 있습니다.

macOS의 WPA, WPA 개인, WPA2 개인, 임의 (개인) 설정

- **암호:** 선택적 암호를 입력합니다. 이 필드를 공백으로 두면 사용자가 로그인할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.

macOS의 WEP 엔터프라이즈, WPA 엔터프라이즈, WPA2 엔터프라이즈, 임의 (엔터프라이즈) 설정

이러한 설정 중 하나를 선택하면 해당 설정이 프록시 서버 설정 뒤에 나열됩니다.

- **프로토콜, 허용되는 EAP 유형:** 지원할 EAP 유형을 사용하도록 설정한 후 관련 설정을 구성합니다. 사용 가능한 각 EAP 유형에서 기본값은 꺼짐입니다.
- **내부 인증 (TTLS):** TTLS를 사용하는 경우에만 필요합니다. 목록에서 사용할 내부 인증 방법을 선택합니다. 사용 가능한 옵션은 **PAP, CHAP, MSCHAP** 또는 **MSCHAPv2**입니다. 기본값은 **MSCHAPv2**입니다.
- **프로토콜, EAP-FAST:** PAC(보호 액세스 자격 증명)를 사용할지 여부를 선택합니다.
 - **PAC** 사용을 선택하는 경우 프로비저닝 PAC를 사용할지 여부를 선택합니다.
 - ★ **PAC** 프로비전을 선택하는 경우 최종 사용자 클라이언트와 XenMobile 간에 익명 TLS 핸드셰이크를 허용할 것인지 선택합니다.
 - 익명으로 **PAC** 프로비전
- **인증:**
 - **사용자 이름:** 사용자 이름을 입력합니다.
 - **연결별 암호:** 사용자가 로그인할 때마다 암호를 요구할지 여부를 선택합니다.
 - **암호:** 선택적 암호를 입력합니다. 이 필드를 공백으로 두면 사용자가 로그인할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.
 - **ID 자격 증명 (키 저장소 또는 PKI 자격 증명):** 목록에서 ID 자격 증명의 유형을 선택합니다. 기본값은 없음입니다.

- 외부 **ID: PEAP, TTLS** 또는 **EAP-FAST** 를 사용하도록 설정하는 경우에만 필요합니다. 외부에 표시되는 사용자 이름을 입력합니다. 사용자 이름이 표시되지 않도록 “익명” 같은 일반 용어를 입력하여 보안을 강화할 수 있습니다.
 - **TLS** 인증서 필요: TLS 인증서를 요구할지 여부를 선택합니다.
- 신뢰
 - 신뢰할 수 있는 인증서: 신뢰할 수 있는 인증서를 추가하려면 추가를 클릭하고 추가하려는 각 인증서에 대해 다음을 수행합니다.
 - * 응용 프로그램: 목록에서 추가하려는 응용 프로그램을 선택합니다.
 - * 저장을 클릭하여 인증서를 저장하거나 취소를 클릭합니다.
 - 신뢰할 수 있는 서버 인증서 이름: 신뢰할 수 있는 인증서의 일반 이름을 추가하려면 추가를 클릭하고 추가하려는 각 이름에 대해 다음을 수행합니다.
 - * 인증서: 추가할 서버 인증서의 이름을 입력합니다. 와일드카드를 사용하여 `wpa*.example.com` 과 같은 이름을 지정할 수 있습니다.
 - * 저장을 클릭하여 인증서 이름을 저장하거나 취소를 클릭합니다.
 - 신뢰 예외 허용: 인증서를 신뢰할 수 없는 경우 사용자 장치에 인증서 신뢰 대화 상자를 표시할 것인지 선택합니다. 기본값은 켜짐입니다.
 - 로그인 원도 구성으로 사용: 로그인 창에 입력한 자격 증명을 동일하게 사용하여 사용자를 인증할지 여부를 선택합니다.
 - 프록시 서버 설정
 - 프록시 구성: 목록에서 없음, 수동 또는 자동을 선택하여 VPN 연결이 프록시 서버를 통해 라우팅되는 방법을 설정한 다음 추가적인 옵션을 모두 구성합니다. 기본값은 없음이며 이 경우 추가적인 구성이 필요하지 않습니다.
 - 수동을 선택하는 경우 다음 설정을 구성합니다.
 - * 호스트 이름/IP 주소: 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
 - * 포트: 프록시 서버 포트 번호를 입력합니다.
 - * 사용자 이름: 프록시 서버 인증에 사용할 선택적 사용자 이름을 입력합니다.
 - * 암호: 프록시 서버 인증에 사용할 선택적 암호를 입력합니다.
 - 자동을 선택하는 경우 다음 설정을 구성합니다.
 - * 서버 **URL**: 프록시 구성을 정의하는 PAC 파일의 URL 을 입력합니다.
 - * **PAC** 에 연결할 수 없는 경우 직접 연결 허용: PAC 파일에 연결할 수 없는 경우 대상에 직접 연결할 수 있도록 할지 여부를 선택합니다. 기본값은 켜짐입니다. 이 옵션은 iOS 7.0 이상에서만 사용할 수 있습니다.

Android 설정

WiFi Policy	Policy Information
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	<div> <div>Network name*</div> <input type="text"/> </div> <div> <div>Authentication</div> <div>Open</div> </div> <div> <div>Encryption</div> <div>WEP</div> </div> <div> <div>Password</div> <input type="text"/> </div> <div> <div>Hidden network (enable if network is open or off)</div> <div>OFF</div> </div>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> Mac OS X <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Tablet	<div>► Deployment Rules</div>
3 Assignment	

- 네트워크 이름: 사용자 장치의 사용 가능한 네트워크 목록에 있는 SSID 를 입력합니다.
- 인증: 목록에서 Wi-Fi 연결에 사용할 보안 유형을 선택합니다.
 - 공개
 - 공유
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK
 - 802.1x EAP

다음 섹션에는 위의 각 연결 유형에 대해 구성하는 옵션이 나열되어 있습니다.

Android 의 공개, 공유 설정

- 암호화: 목록에서 사용 안 함 또는 **WEP** 를 선택합니다. 기본값은 **WEP** 입니다.
- 암호: 선택적 암호를 입력합니다.

Android 의 WPA, WPA-PSK, WPA2, WPA2-PSK 설정

- 암호화: 목록에서 **TKIP** 또는 **AES** 를 선택합니다. 기본값은 **TKIP** 입니다.
- 암호: 선택적 암호를 입력합니다.

Android의 802.1x 설정

- **EAP 유형:** 목록에서 **PEAP**, **TLS** 또는 **TTLS** 를 선택합니다. 기본값은 **PEAP** 입니다.
- **암호:** 선택적 암호를 입력합니다.
- **인증 단계 2:** 목록에서 없음, **PAP**, **MSCHAP**, **MSCHAPPv2** 또는 **GTC** 를 선택합니다. 기본값은 **PAP** 입니다.
- **ID:** 선택적 사용자 이름 및 도메인을 입력합니다.
- **익명:** 외부에 표시되는 사용자 이름을 입력합니다. 사용자 이름이 표시되지 않도록 “익명” 같은 일반 용어를 입력하여 보안을 강화할 수 있습니다.
- **CA 인증서:** 목록에서 사용할 인증서를 선택합니다.
- **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
- **숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용):** 네트워크를 숨길지 여부를 선택합니다.

Android Enterprise 설정

WiFi Policy	WiFi Policy
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms Clear All	<div> <div>Network name *</div> <input type="text"/> </div> <div> <div>Authentication</div> <div>Open</div> </div> <div> <div>Encryption</div> <div>WEP</div> </div> <div> <div>Password</div> <input type="password"/> </div> <div> <div>Hidden network (enable if network is open or off)</div> <div>OFF</div> </div>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Android Enterprise <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE <input checked="" type="checkbox"/> Chrome OS <input checked="" type="checkbox"/> Workspace Hub	<div>► Deployment Rules</div>
3 Assignment	

- **네트워크 이름:** 사용자 장치의 사용 가능한 네트워크 목록에 있는 SSID 를 입력합니다.
- **인증:** 목록에서 Wi-Fi 연결에 사용할 보안 유형을 선택합니다.
 - 공개
 - 공유
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK

– 802.1x EAP

다음 섹션에는 위의 각 연결 유형에 대해 구성하는 옵션이 나열되어 있습니다.

Android Enterprise 용 공개, 공유 설정

- **암호화:** 목록에서 사용 안 함 또는 **WEP** 를 선택합니다. 기본값은 **WEP** 입니다.
- **암호:** 선택적 암호를 입력합니다.

Android Enterprise 용 WPA, WPA-PSK, WPA2, WPA2-PSK 설정

- **암호화:** 목록에서 TKIP 또는 AES 를 선택합니다. 기본값은 TKIP 입니다.
- **암호:** 선택적 암호를 입력합니다.

Android Enterprise 용 802.1x 설정

- **EAP 유형:** 목록에서 **PEAP**, **TLS** 또는 **TTLS** 를 선택합니다. 기본값은 **PEAP** 입니다.
- **암호:** 선택적 암호를 입력합니다.
- **인증 단계 2:** 목록에서 없음, **PAP**, **MSCHAP**, **MSCHAPPv2** 또는 **GTC** 를 선택합니다. 기본값은 **PAP** 입니다.
- **ID:** 선택적 사용자 이름 및 도메인을 입력합니다.
- **익명:** 외부에 표시되는 사용자 이름을 입력합니다. 사용자 이름이 표시되지 않도록 “익명” 같은 일반 용어를 입력하여 보안을 강화할 수 있습니다.
- **CA 인증서:** 목록에서 사용할 인증서를 선택합니다.
- **도메인:** 필요한 도메인 이름을 입력합니다. 자세한 내용은 [도메인](#) 을 참조하십시오.

참고:

Android 13 이상을 실행하는 장치에서 Wi-Fi 정책을 구성하는 경우 **CA** 인증서 및 도메인 필드를 의무적으로 업데이트해야 합니다. 업데이트되지 않으면 구성이 실패합니다.

- **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
- **숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용):** 네트워크를 숨길지 여부를 선택합니다.

Windows 10 및 Windows 11 설정

WiFi Policy	WiFi Policy
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	<div> <div>Network name *</div> <input type="text"/> </div> <div> <div>Authentication</div> <div>Open</div> </div> <div> <div>Hidden network (enable if network is open or off)</div> <div>OFF</div> </div> <div> <div>Connect automatically</div> <div>OFF</div> </div> <div> <div>Proxy server settings</div> <div> <div>Host name or IP address</div> <input type="text"/> </div> <div> <div>Port</div> <input type="text"/> </div> </div>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<div>► Deployment Rules</div>
3 Assignment	

- 인증: 목록에서 Wi-Fi 연결에 사용할 보안 유형을 클릭합니다.
 - 공개
 - WPA 개인
 - WPA-2 개인
 - WPA 엔터프라이즈
 - WPA-2 엔터프라이즈: WPA-2 엔터프라이즈를 사용하려면 SCEP 를 구성해야 합니다. SCEP 구성을 사용하면 XenMobile 에서 장치에 인증서를 보내 Wi-Fi 서버 인증을 수행할 수 있습니다. SCEP 를 구성하려면 설정 > 자격 증명 공급자의 배포 페이지로 이동합니다. 자세한 내용은 [자격 증명 공급자](#)를 참조하십시오.

다음 섹션에는 위의 각 연결 유형에 대해 구성하는 옵션이 나열되어 있습니다.

Windows 10 및 Windows 11 설정 열기

- 숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용): 네트워크를 숨길지 여부를 선택합니다.
- 자동 연결: 네트워크에 자동으로 연결할지 여부를 선택합니다.

Windows 10 및 Windows 11 의 WPA 개인, WPA-2 개인 설정

- 암호화: 목록에서 **AES** 또는 **TKIP** 를 선택하여 암호화 유형을 설정합니다. 기본값은 **AES** 입니다.
- 숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용): 네트워크를 숨길지 여부를 선택합니다.
- 자동 연결: 네트워크에 자동으로 연결할지 여부를 선택합니다.

Windows 10 및 Windows 11의 WPA-2 엔터프라이즈 설정

- **암호화:** 목록에서 **AES** 또는 **TKIP**를 선택하여 암호화 유형을 설정합니다. 기본값은 **AES**입니다.
- **EAP 유형:** 목록에서 **PEAP-MSCHAPv2** 또는 **TLS**를 선택하여 EAP 유형을 설정합니다. 기본값은 **PEAP-MSCHAPv2**입니다.
- **숨겨진 경우 연결:** 네트워크를 숨길지 여부를 선택합니다.
- **자동 연결:** 네트워크에 자동으로 연결할지 여부를 선택합니다.
- **SCEP**를 통해 인증서 푸시: SCEP(단순 인증서 등록 프로토콜)를 통해 사용자 장치에 인증서를 푸시할지 여부를 선택합니다.
- **SCEP**의 자격 증명 공급자: 목록에서 SCEP 자격 증명 공급자를 선택합니다. 기본값은 없음입니다.

Windows Information Protection 장치 정책

August 12, 2022

이전의 EDP(엔터프라이즈 데이터 보호)인 WIP(Windows Information Protection)는 엔터프라이즈 데이터의 잠재적 유출을 차단하는 Windows 기술입니다. 데이터 유출은 엔터프라이즈에서 보호되지 않는 앱, 앱 간 또는 조직 네트워크 외부로 엔터프라이즈 데이터를 공유하는 과정에서 발생할 수 있습니다. 자세한 내용은 [Protect your enterprise data using Windows Information Protection \(WIP\)](#)(WIP(Windows Information Protection)를 사용하여 엔터프라이즈 데이터 보호)를 참조하십시오.

XenMobile에서 장치 정책을 생성하여 설정한 적용 수준의 Windows Information Protection이 필요한 앱을 지정할 수 있습니다. Windows Information Protection 정책은 감독되는 Windows 10 또는 Windows 11 실행 태블릿 및 데스크톱에 적용됩니다.

XenMobile에는 자주 사용되는 앱 몇 가지가 포함되어 있으며 다른 앱도 추가할 수 있습니다. 사용자 환경에 영향을 미치는 정책 적용 수준을 지정할 수 있습니다. 예를 들어 다음을 수행할 수 있습니다.

- 부적절한 데이터 공유 차단
- 부적절한 데이터 공유에 대해 경고하고 사용자가 정책을 재정의할 수 있도록 허용
- 부적절한 데이터 공유를 로깅하고 허용하는 동안 WIP를 자동으로 실행

Windows Information Protection에서 앱을 제외하려면 Microsoft AppLocker XML 파일에서 앱을 정의한 다음 이 파일을 XenMobile로 가져옵니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Windows 10 및 Windows 11 설정

Windows Information Protection Policy		Windows Information Protection Policy																						
1 Policy Info		<p>This policy lets you specify the apps that require Windows Information Protection at the enforcement level you set. The policy is supported only on Windows 10 (RS1 and above).</p> <p>Desktop App</p> <table border="1"> <thead> <tr> <th>File name *</th> <th>Publisher *</th> <th>Product name *</th> <th>Version *</th> <th>Allowed</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>ieexplore.exe</td> <td>O= [redacted] L= [redacted] S= [redacted]</td> <td>*</td> <td>*</td> <td>Allowed</td> <td></td> </tr> <tr> <td>notepad.exe</td> <td>O= [redacted] L= [redacted] S= [redacted]</td> <td>*</td> <td>*</td> <td>Allowed</td> <td></td> </tr> </tbody> </table>					File name *	Publisher *	Product name *	Version *	Allowed	Add	ieexplore.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed		notepad.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed	
File name *	Publisher *	Product name *	Version *	Allowed	Add																			
ieexplore.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed																				
notepad.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed																				
2 Platforms																								
<input type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet																								
3 Assignment																								

- 데스크톱 앱 (Windows 10 또는 Windows 11 태블릿), 스토어 앱 (Windows 10 및 Windows 11 태블릿): XenMobile 에는 위의 샘플처럼 몇 가지 자주 사용되는 앱이 포함되어 있습니다. 필요에 따라 이러한 앱을 편집하거나 제거할 수 있습니다.

다른 앱을 추가하려면: 데스크톱 앱 또는 스토어 앱 테이블에서 추가를 클릭하고 앱 정보를 제공합니다.

허용되는 앱은 엔터프라이즈 데이터를 읽고, 만들고, 업데이트할 수 있습니다. 거부되는 앱은 엔터프라이즈 데이터에 액세스할 수 없습니다. 예외 앱은 엔터프라이즈 데이터를 읽을 수 있지만 데이터를 만들거나 수정할 수는 없습니다.

- AppLocker XML:** Microsoft 는 WIP 와 호환성 문제가 있는 것으로 알려진 Microsoft 앱의 목록을 제공합니다. 이러한 앱을 WIP 에서 제외하려면 찾아보기를 클릭하고 목록을 업로드합니다. XenMobile 은 업로드된 AppLocker XML 과 구성된 데스크톱 및 스토어 앱을 장치로 전송된 정책에서 결합합니다. 자세한 내용은 [Windows Information Protection 에 대한 권장 거부 목록](#)을 참조하십시오.
- 적용 수준:** Windows Information Protection 이 데이터 공유를 보호하고 관리할 방식을 지정하는 옵션을 선택합니다. 기본값은 꺼짐입니다.
 - ★ **0-꺼짐:** WIP 가 꺼지며 데이터를 보호 또는 감사하지 않습니다.
 - ★ **1-무음:** WIP 가 자동으로 실행되면서 부적절한 데이터 공유를 기록하고 아무것도 차단하지 않습니다. [보고 CSP](#)를 통해 로그에 액세스할 수 있습니다.
 - ★ **2-재정의:** WIP 가 잠재적으로 안전하지 않은 데이터 공유에 대해 사용자에게 경고합니다. 사용자는 경고를 재정의하고 데이터를 공유할 수 있습니다. 이 모드는 사용자 재정의의 포함된 작업을 감사 로그에 기록합니다.
 - ★ **3-차단:** WIP 는 사용자가 안전하지 않을 수 있는 데이터 공유를 수행하는 것을 차단합니다.
- 보호되는 도메인 이름:** 엔터프라이즈가 사용자 ID 에 사용하는 도메인입니다. 관리되는 ID 도메인의 이 목록은 기본 도메인과 함께 관리 엔터프라이즈의 ID 를 구성합니다. 목록에서 첫 번째 도메인은 Windows UI 에 사용되는 기본 회사 ID 입니다. “|”를 사용하여 목록 항목을 구분합니다. 예: [domain1.com](#) | [domain2.com](#)
- 데이터 복구 인증서:** 찾아보기를 클릭한 다음 암호화된 파일의 데이터 복구에 사용할 복구 인증서를 선택합니다. 이 인증서는 그룹 정책이 아니라 MDM 을 통해 배달된다는 점 이외에는 EFS(암호화 파일 시스템) 에 대한 DRA(데이터 복구 에이전트) 와 동일합니다. 복구 인증서를 사용할 수 없는 경우 새로 만듭니다. 자세한 내용은 이 섹션의 “데이터 복구 인증서 만들기” 를 참조하십시오.

- **네트워크 도메인 이름:** 엔터프라이즈의 경계를 구성하는 도메인의 목록입니다. **WIP** 는 목록의 정규화된 도메인에 대한 모든 트래픽을 보호합니다. 이 설정은 **IP** 범위 설정과 함께 사용되어 네트워크 끝점이 엔터프라이즈인지 아니면 사설망의 개인인지를 감지합니다. 심표를 사용하여 목록 항목을 구분합니다. 예: corp.example.com,region.example.com

- **IP 범위:** 엔터프라이즈 네트워크의 컴퓨터를 정의하는 엔터프라이즈 IPv4 및 IPv6 범위의 목록입니다. **WIP** 는 이러한 위치를 엔터프라이즈 데이터를 공유해도 안전한 대상으로 고려합니다. 심표를 사용하여 목록 항목을 구분합니다. 예:

10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff

- **IP 범위 목록을 신뢰할 수 있음:** Windows 에 의한 IP 범위의 자동 감지를 방지하려면 이 설정을 꺼짐으로 변경합니다. 기본값은 켜짐입니다.

- **프록시 서버:** 엔터프라이즈가 회사 리소스에 사용할 수 있는 프록시 서버의 목록입니다. 네트워크에서 프록시를 사용하는 경우 이 설정이 필요합니다. 프록시 서버가 없으면 프록시 뒤에 있는 클라이언트가 엔터프라이즈 리소스를 사용하지 못할 수 있습니다. 예를 들어 호텔 및 식당의 특정 WiFi 핫스팟에서 리소스를 사용하지 못할 수 있습니다. 심표를 사용하여 목록 항목을 구분합니다. 예:

proxy.example.com:80;157.54.11.118:443

- **내부 프록시 서버:** 장치가 클라우드 리소스에 연결하기 위해 통과하는 프록시 서버의 목록입니다. 이 서버 유형을 사용하면, 연결하는 클라우드 리소스가 엔터프라이즈 리소스임을 나타냅니다. 이 목록에 **WIP** 비보호 트래픽에 사용되는 프록시 서버 설정의 서버를 포함하지 마십시오. 심표를 사용하여 목록 항목을 구분합니다. 예:

example.internalproxy1.com;10.147.80.50

- **클라우드 리소스:** **WIP** 로 보호되는 클라우드 리소스의 목록입니다. 원하는 경우 각 클라우드 리소스에 대해, 이 클라우드 리소스에 대한 트래픽을 라우팅할 프록시 서버 목록의 프록시 서버를 지정할 수도 있습니다. 프록시 서버를 통해 라우팅되는 모든 트래픽은 엔터프라이즈 트래픽으로 취급됩니다. 심표를 사용하여 목록 항목을 구분합니다. 예:

domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.domain2.com

- **등록 취소할 때 **WIP** 인증서 해지:** Windows Information Protection 에서 등록 취소될 때 사용자 장치에서 로컬 암호화 키를 해지할지 여부를 지정합니다. 암호화 키가 해지되면 사용자는 암호화된 회사 데이터에 액세스할 수 없습니다. 꺼짐인 경우 키가 해지되지 않으며 사용자는 등록 취소 후에도 보호된 파일에 계속 액세스할 수 있습니다. 기본값은 켜짐입니다.

- **오버레이 아이콘 표시:** 탐색기의 회사 파일 및 시작 메뉴의 엔터프라이즈 전용 앱 타일에 Windows Information Protection 아이콘 오버레이를 포함할지 여부를 지정합니다. 기본값은 꺼짐입니다.

데이터 복구 인증서 만들기

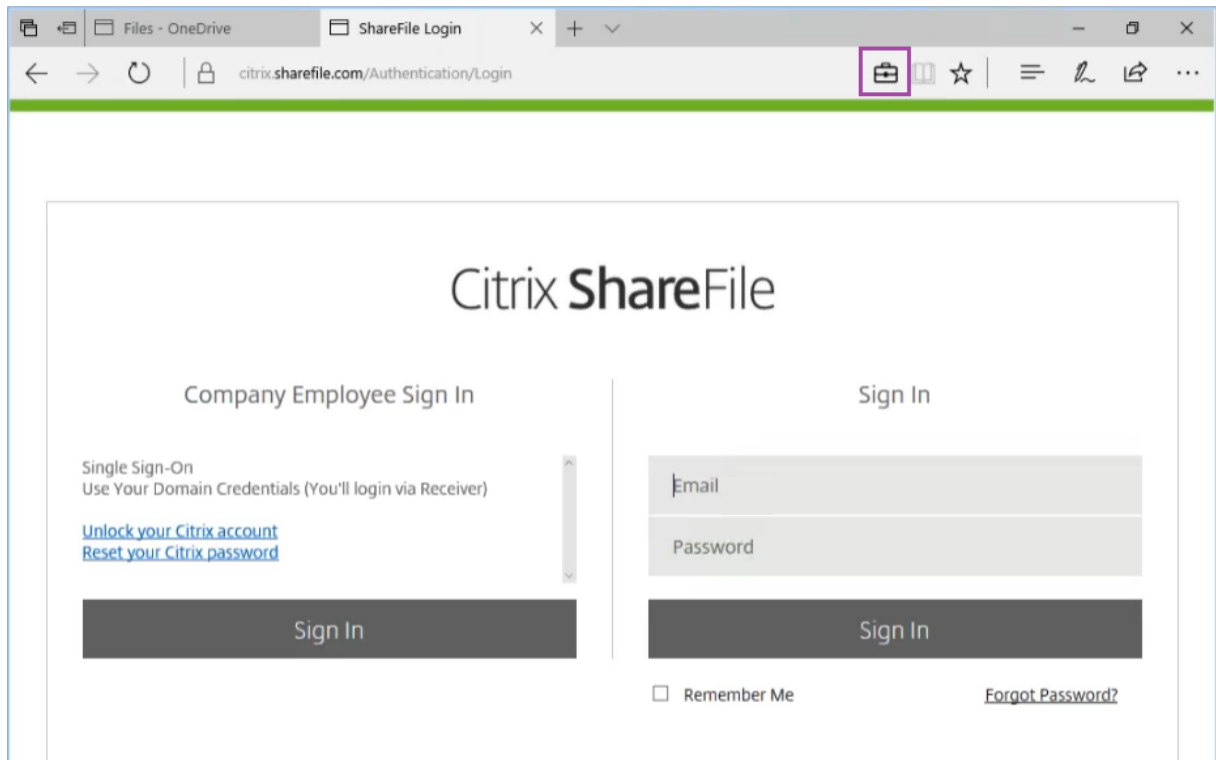
Windows Information Protection 정책을 사용하도록 설정하려면 데이터 복구 인증서가 필요합니다.

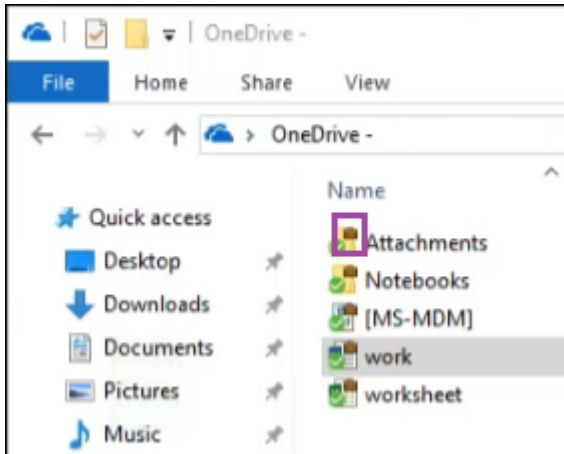
1. XenMobile 콘솔이 실행되는 컴퓨터에서 명령 프롬프트를 열고 인증서를 만들려는 폴더 (Windows\System32 이외의 폴더) 로 이동합니다.
2. 다음 명령을 실행합니다.

```
cipher /r:ESFDRA
```
3. 메시지가 나타나면 개인 키 파일을 보호하기 위한 암호를 입력합니다.
암호화 명령은.cer 및.pfx 파일을 생성합니다.
4. XenMobile 콘솔에서 설정 > 인증서로 이동하고 Windows 10 및 Windows 11 태블릿에 적용되는.cer 파일을 가져옵니다.

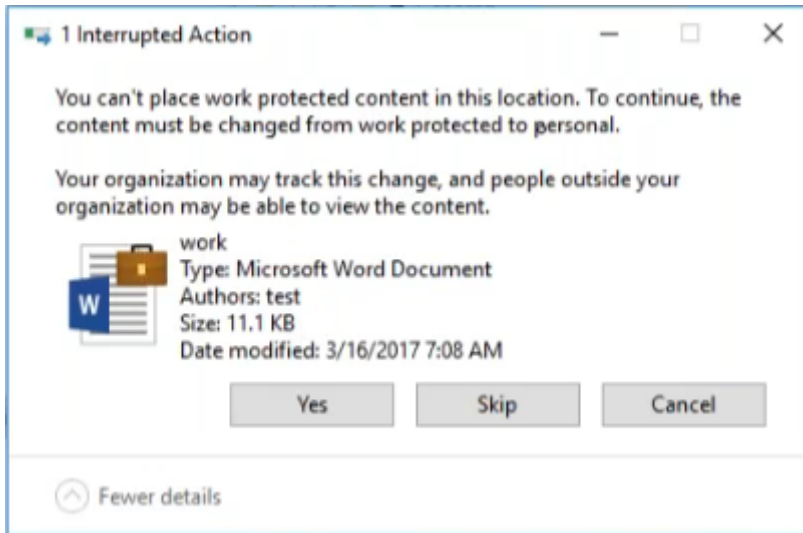
사용자 환경

Windows Information Protection 이 적용될 때는 앱과 파일에 다음 아이콘이 포함됩니다.





사용자가 보호되는 파일을 보호되지 않는 위치로 복사하거나 저장할 경우 구성된 적용 수준에 따라 다음 알림이 나타납니다.



XenMobile 옵션 장치 정책

November 1, 2022

Android 장치에서 XenMobile 에 연결할 때 Secure Hub 동작을 구성하는 XenMobile 옵션 정책을 추가합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Android 설정

XenMobile Options Policy

This policy lets you configure parameters for connections to XenMobile.

Device agent configuration

Traybar notification - hide traybar icon

OFF

Connection time-out(s) *

20

Keep-alive interval(s) *

120

Remote support

Prompt the user before allowing remote control

OFF

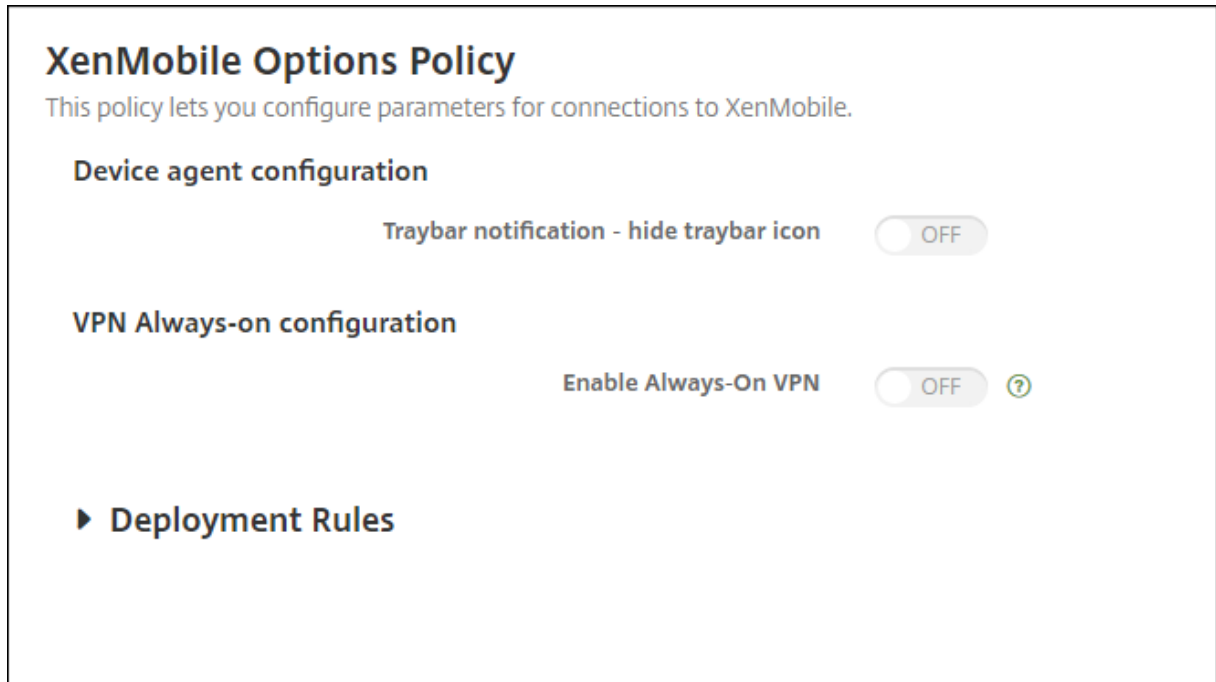
Before a file transfer

Do not warn the user

► Deployment Rules

- **트레이 표시줄 알림 - 트레이 표시줄 아이콘 숨기기:** 트레이 표시줄 아이콘을 표시할지, 아니면 숨길지를 선택합니다. 기본값은 꺼짐입니다.
- **연결 시간 제한:** 연결 시간이 초과되기 전에 연결이 유효 상태로 있을 수 있는 시간 (초) 을 입력합니다. 기본값은 20 초입니다.
- **연결 유지 간격:** 연결을 유지할 시간 (초) 을 입력합니다. 기본값은 120 초입니다.

Android Enterprise 설정



Android 버전 7 부터 지원됩니다.

- 트레이 표시줄 알림 - 트레이 표시줄 아이콘 숨기기: 트레이 표시줄 아이콘을 표시할지, 아니면 숨길지를 선택합니다. 기본값은 꺼짐입니다.
- 항상 **VPN** 연결 사용. 항상 VPN 연결을 사용할지 여부를 선택합니다. 이 설정이 켜짐인 경우 장치의 전원이 켜지면 VPN 서비스가 시작되고 장치가 켜져 있는 동안 계속 실행됩니다. 기본값은 꺼짐입니다.
- **VPN** 패키지. 장치에서 사용하는 VPN 앱의 패키지 이름을 입력합니다. 기본적으로 이 필드에는 Citrix SSO 앱의 패키지 이름인 **com.CitrixVPN** 이 자동으로 채워집니다.

XenMobile 제거 장치 정책

August 12, 2022

XenMobile 에서 장치 정책을 추가하여 Android 장치에서 XenMobile 을 제거할 수 있습니다. 이 정책을 배포하면 배포 그룹에 있는 모든 장치에서 XenMobile 이 제거됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)을 참조하십시오.

Android 설정 구성

- 장치에서 **XenMobile** 제거: 이 정책을 배포할 모든 장치에서 XenMobile 을 제거할지 여부를 선택합니다. 기본값은 꺼짐입니다.

앱 추가

March 15, 2024

XenMobile 에 앱을 추가하면 MAM(모바일 애플리케이션 관리) 기능을 이용할 수 있습니다. XenMobile 은 응용 프로그램 제공, 소프트웨어 라이선스, 구성 및 응용 프로그램 수명 주기 관리를 지원합니다.

MDX 지원 앱은 대부분의 앱 유형을 사용자 장치에 배포하기 위해 준비하는 데 중요한 부분입니다. MDX 에 대한 소개는 [MDX Toolkit 정보 \[및\]\(/en-us/mdx-toolkit/mam-sdk-overview.html\)MAM SDK 개요](#)를 참조하십시오.

- Citrix 에서는 MDX 지원 앱에 MAM SDK 를 사용할 것을 권장합니다. 또는 MDX Toolkit 이 더 이상 사용되지 않을 때까지 MDX 래핑 앱을 계속 사용할 수 있습니다. [사용 중단](#)을 참조하십시오.
- MDX Toolkit 을 사용하여 Citrix 모바일 생산성 앱을 래핑할 수 없습니다. Citrix 다운로드에서 모바일 생산성 앱 MDX 파일을 다운로드하십시오.

XenMobile 콘솔에 앱을 추가하면 다음 작업을 수행할 수 있습니다.

- 앱 설정을 구성합니다.
- 필요에 따라 앱을 범주로 정렬하여 Secure Hub 에서 앱을 구성합니다.
- 필요에 따라 사용자의 앱 액세스를 허용하기 전에 승인이 필요하도록 워크플로를 정의합니다.
- 사용자에게 앱을 배포합니다.

이 문서에서는 앱 추가에 관한 일반적인 워크플로를 설명합니다. 플랫폼별 자세한 내용은 다음 문서를 참조하십시오.

- [Android Enterprise 앱 배포](#)
- [Apple 앱 배포](#)

앱 유형 및 기능

다음 표에는 XenMobile 로 배포할 수 있는 앱 유형이 요약되어 있습니다.

앱 유형	출처	참고	참조
MDX	사용자용으로 개발하는 iOS 및 Android 앱과 Citrix 모바일 생산성 앱입니다.	MAM SDK 로 iOS 또는 Android 앱을 개발하거나 MDX Toolkit 으로 앱을 래핑합니다. 모바일 생산성 앱의 경우 Citrix 다운로드에서 공용 스토어 MDX 파일을 다운로드합니다. 그런 다음 XenMobile 에 앱을 추가합니다.	MDX 앱 추가
공용 앱 스토어	Google Play 또는 Apple App Store 와 같은 공용 앱 스토어의 무료 또는 유료 앱입니다.	앱, MDX 지원 앱을 업로드하고 앱을 XenMobile 에 추가합니다.	공용 앱 스토어 앱 추가
웹 및 SaaS	내부 네트워크 (웹 앱) 또는 공용 네트워크 (SaaS)	Citrix Workspace 는 MDM 에 등록된 iOS 및 Android 장치에서 기본 SaaS 앱에 대한 모바일 Single Sign-on 을 제공합니다. 또는 SAML(Security Assertion Markup Language) 응용 프로그램 커넥터를 사용합니다.	웹 또는 SaaS 앱 추가
Enterprise	Win32 앱 등 MDX 를 지원하지 않는 개인 앱과 MDX 지원 개인 Android Enterprise 앱입니다. Enterprise 앱은 CDN(Content Delivery Network) 위치 또는 XenMobile Server 에 상주합니다.	XenMobile 에 앱을 추가합니다.	엔터프라이즈 앱 추가
웹 링크	Single Sign-On 이 필요하지 않은 인터넷 웹 주소, 인트라넷 웹 주소 또는 웹 앱입니다.	XenMobile 에서 웹 링크를 구성합니다.	웹 링크 추가

앱 배포를 계획할 때는 다음 기능을 고려하십시오.

- 자동 설치 정보
- 필수 앱과 선택적 앱 정보
- 앱 범주 정보
- Microsoft 365 앱 사용
- 워크플로 적용
- 앱 스토어 및 Citrix Secure Hub 브랜딩

자동 설치 정보

Citrix 는 iOS, Android Enterprise 및 Samsung 앱의 자동 설치 및 업그레이드를 지원합니다. 자동 설치에서는 장치에 배포한 앱을 설치하라는 메시지가 사용자에게 표시되지 않습니다. 앱이 백그라운드에서 자동으로 설치됩니다.

자동 설치를 구현하기 위한 필수 구성 요소:

- iOS 의 경우 관리되는 iOS 장치를 감독 모드로 전환합니다. 자세한 내용은 [iOS 및 macOS 프로필 장치 정책 가져오기](#)를 참조하십시오.
- Android Enterprise 경우 앱이 장치의 Android 작업 프로필에 설치됩니다. 자세한 내용은 [Android Enterprise](#)를 참조하십시오.
- Samsung 장치의 경우 장치에서 Samsung Knox 를 사용합니다.
이 작업을 수행하려면 Samsung MDM 라이선스 키 장치 정책을 설정하여 Samsung ELM 및 Knox 라이선스 키를 생성합니다. 자세한 내용은 [Samsung MDM 라이선스 키 장치 정책](#)을 참조하십시오.

필수 앱과 선택적 앱 정보

배달 그룹에 앱을 추가하는 경우 선택적 앱인지, 아니면 필수 앱인지를 선택해야 합니다. Citrix 에서는 앱을 필수로 배포하기를 권장합니다.

- 필수 앱은 사용자 장치에 자동으로 설치되므로 상호 작용이 최소화됩니다. 이러한 기능을 사용하면 앱을 자동으로 업데이트할 수도 있습니다.
- 옵션 앱을 통해 사용자는 설치할 앱을 선택할 수 있지만 사용자는 Secure Hub 를 통해 수동으로 설치를 개시해야 합니다.

필수로 표시된 앱의 경우 사용자는 다음과 같은 경우에 곧바로 업데이트를 받을 수 있습니다.

- 사용자가 새 앱을 업로드하고 필수 앱으로 표시합니다.
- 사용자가 기존 앱을 필수 앱으로 표시합니다.
- 사용자가 필수 앱을 삭제합니다.
- Secure Hub 업데이트가 제공됩니다.

필수 앱의 강제 배포를 위한 요구 사항

- XenMobile Server 10.6(최소 버전)
- Secure Hub 10.5.15(iOS 의 경우) 및 10.5.20(Android 의 경우)(최소 버전)
- MAM SDK 또는 MDX Toolkit 10.6(최소 버전)
- 사용자 지정 서버 속성, **force.server.push.required.apps**.

필수 앱의 강제 배포가 기본적으로 사용되지 않도록 설정됩니다. 이 기능을 사용하도록 설정하려면 사용자 지정 키 서버 속성을 만드십시오. 키 및 표시 이름을 **force.server.push.required.apps** 로 설정하고 값을 **true** 로 설정합니다.

- XenMobile Server 및 Secure Hub 업그레이드 후: 등록된 장치가 있는 사용자는 로그오프 후 Secure Hub 에 로 그온하여 필수 앱 배포 업데이트를 받아야 합니다.

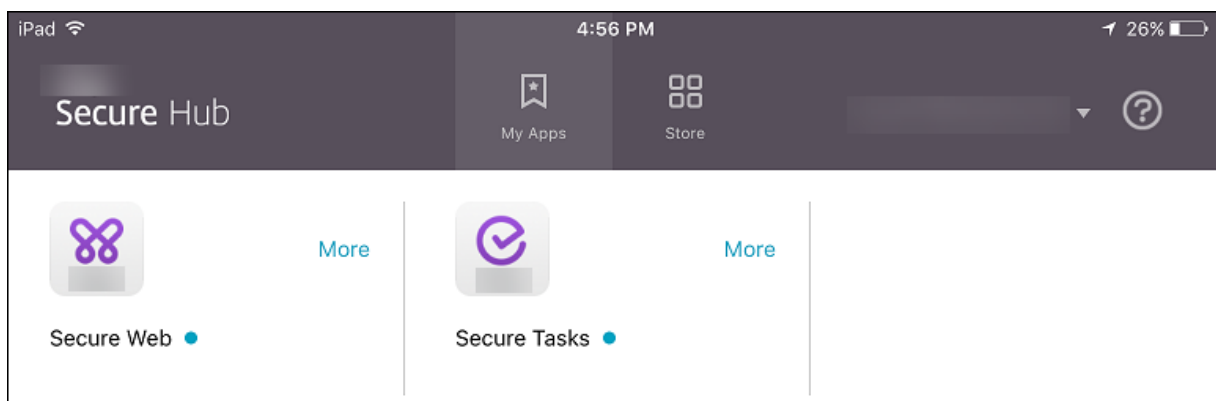
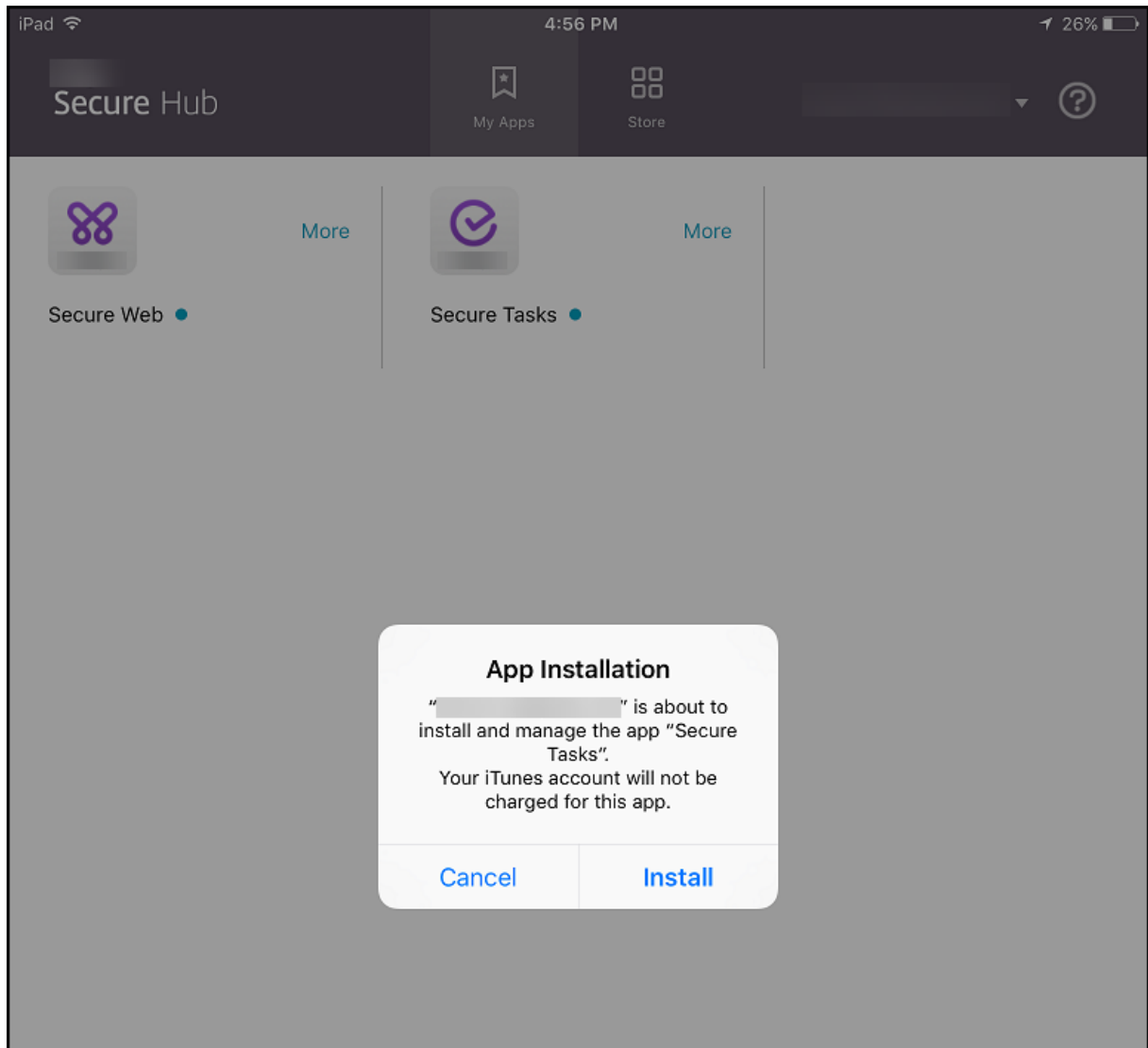
예제

다음 예제에는 Citrix Secure Tasks 로 명명된 앱을 배달 그룹에 추가한 후 배달 그룹을 배포하는 작업의 순서가 나와 있습니다.

The first screenshot shows the 'Delivery Groups' tab in the console. On the left, a sidebar lists 'Delivery Group' options: 1 Delivery Group Info, 2 User, 3 Resource (optional), Policies, Apps (selected), Actions, ShareFile, Enrollment Profile, and 4 Summary. The main area is titled 'Apps' and says 'Drag the apps that you want to include in the delivery group.' It features a search bar and a list of apps: Angry Bird, Box, Fit, and SecureNotes. A hand icon is shown dragging 'SecureTask' from the 'Apps' list to the 'Required Apps' list on the right. The 'Required Apps' list contains SecureWeb, Enterprise-01, GTM, and SecureTask (highlighted with a red box). Below it, the 'Optional Apps' list contains Jira and Office365_SAML.

The second screenshot shows the 'Delivery Groups' list. At the top, there are buttons for Add, Edit, Deploy (highlighted with a red box), Delete, and Export. Below the buttons is a table with columns: Status, Name, Last Updated, and Disabled. The table contains two rows: 'AllUsers' (last updated Apr 18 2017 2:43 AM) and 'DeliveryGroup-01' (last updated Apr 19 2017 8:47 AM, with a green checkmark in the Status column). At the bottom, it says 'Showing 1 - 2 of 2 items' and 'Items per page: 10'.

샘플 앱인 Citrix Secure Tasks 가 사용자 장치에 배포되면 Secure Hub 가 앱을 설치하라는 메시지를 표시합니다.



중요:

엔터프라이즈 앱 및 공용 앱 스토어 앱을 포함한 MDX 지원 필수 앱이 즉시 업그레이드됩니다. 관리자가 앱 업데이트 유예 기간에 대한 MDX 정책을 구성하고 사용자가 앱을 나중에 업그레이드하도록 선택하는 경우에도 업그레이드가 수행됩니다.

엔터프라이즈 및 공용 스토어 앱을 위한 **iOS** 필수 앱 워크플로

1. 초기 등록 중에 XenMobile App 을 배포합니다. 필수 앱이 장치에 설치됩니다.
2. XenMobile 콘솔에서 앱을 업데이트합니다.
3. XenMobile 콘솔에서 필수 앱을 배포합니다.
4. 홈 화면의 앱이 업데이트됩니다. 또한 공용 스토어 앱의 경우 업그레이드가 자동으로 시작됩니다. 사용자에게 업데이트하라는 메시지가 표시되지 않습니다.
5. 사용자가 홈 화면에서 앱을 엽니다. 앱 업데이트 유예 기간을 설정했다라도 사용자가 나중에 앱을 업그레이드하기 위해 누르면 앱이 곧바로 업그레이드됩니다.

엔터프라이즈 앱을 위한 **Android** 필수 앱 워크플로

1. 초기 등록 중에 XenMobile App 을 배포합니다. 필수 앱이 장치에 설치됩니다.
2. XenMobile 콘솔에서 필수 앱을 배포합니다.
3. 앱이 업그레이드됩니다. (Nexus 장치에서는 업데이트를 설치하라는 메시지가 표시되지만 Samsung 장치에서는 자동 설치됩니다.)
4. 사용자가 홈 화면에서 앱을 엽니다. 앱 업데이트 유예 기간을 설정했다라도 사용자가 나중에 앱을 업그레이드하기 위해 누르면 앱이 곧바로 업그레이드됩니다. (Samsung 장치에서는 자동 설치가 수행됩니다.)

공용 스토어 앱을 위한 **Android** 필수 앱 워크플로

1. 초기 등록 중에 XenMobile App 을 배포합니다. 필수 앱이 장치에 설치됩니다.
2. XenMobile 콘솔에서 앱을 업데이트합니다.
3. XenMobile 콘솔에서 필수 앱을 배포합니다. 또는 장치에서 Secure Hub 스토어를 엽니다. 스토어에 업데이트 아이콘이 나타납니다.
4. 앱 업그레이드가 자동으로 시작됩니다. (Nexus 장치에서는 업데이트를 설치하라는 메시지가 표시됩니다.)
5. 홈 화면에서 앱을 엽니다. 앱이 업그레이드됩니다. 유예 기간 동안 사용자에게 메시지가 표시되지 않습니다. (Samsung 장치에서는 자동 설치가 수행됩니다.)

앱이 구성되어 있는 경우 필요에 따라 앱 제거

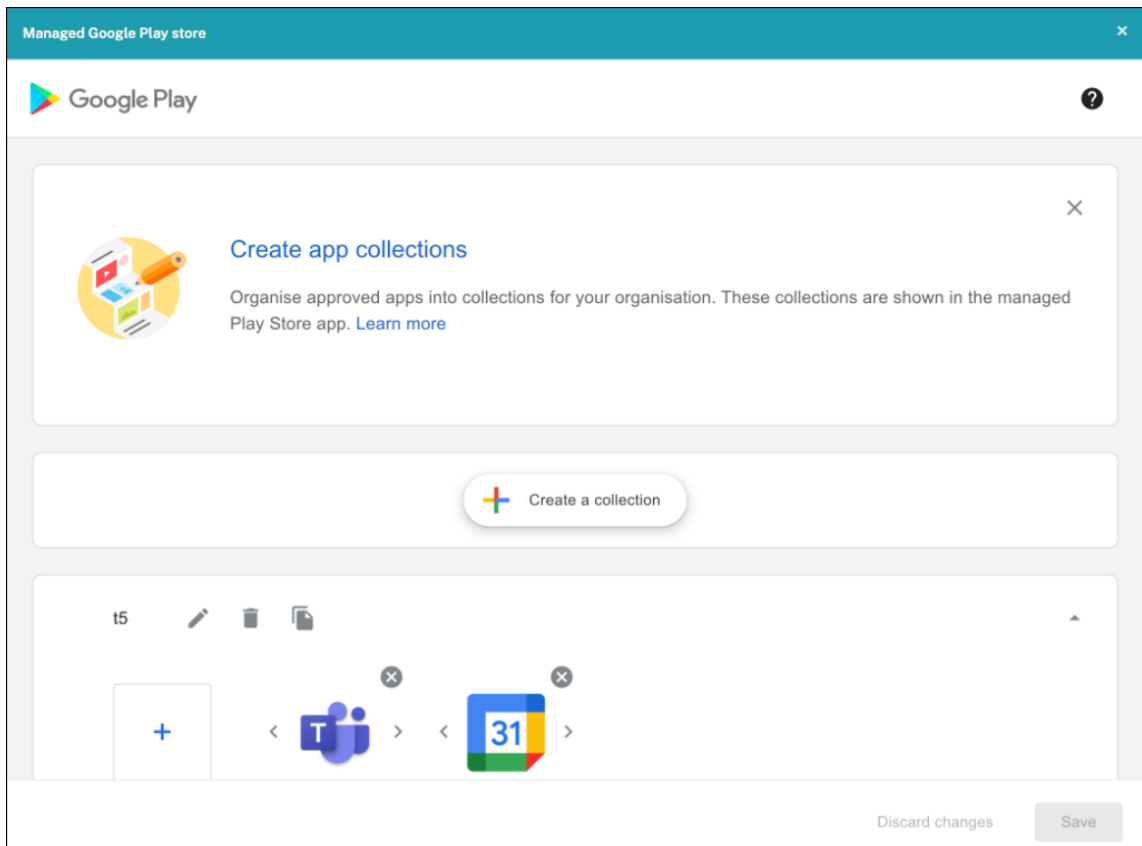
사용자가 구성된 앱을 필요에 따라 제거하도록 허용할 수 있습니다. 구성 > 배달 그룹으로 이동하여 앱을 필수 앱에서 선택적 앱으로 옮깁니다.

권장 사항: 특정 사용자가 앱을 제거할 수 있도록 특수 배달 그룹을 사용하여 앱을 선택사항으로 잠시 변경합니다. 그러면 기존 필수 앱을 선택사항으로 변경하고 해당 배달 그룹으로 앱을 배포한 다음 장치에서 앱을 제거할 수 있습니다. 이후 향후 해당 배달 그룹 등록에 앱이 필요하도록 하려면 다시 앱을 필수로 설정하면 됩니다.

앱 정리하기 (Android Enterprise)

사용자가 Secure Hub 에 로그인하면 XenMobile Server 에서 설정한 앱, 웹 링크 및 스토어 목록이 표시됩니다. Android Enterprise 에서는 사용자가 특정 앱, 스토어 또는 웹 링크에만 액세스할 수 있도록 이러한 앱을 컬렉션으로 정리할 수 있습니다. 예를 들어 금융 컬렉션을 만든 다음 금융 관련 앱만 컬렉션에 추가합니다. 아니면 영업 컬렉션을 구성하여 영업 앱을 할당할 수 있습니다.

1. XenMobile Server 콘솔에서 구성 > 앱 > 앱 구성을 클릭합니다. 관리형 **Google Play Store** 창이 나타납니다.



2. 컬렉션 만들기를 클릭하고 해당 컬렉션에 추가할 앱을 선택합니다.
3. 컬렉션 추가를 완료하면 저장을 클릭합니다.

참고:

IT 관리자는 앱을 승인해야 관리형 Google Play 창에서 컬렉션에 앱을 추가할 수 있습니다. IT 관리자는 <https://play.google.com/work>에서 앱을 승인할 수 있습니다. 향후 릴리스에서는 컬렉션에 앱을 추가하기 전에 앱을 승인할 필요가 없습니다.

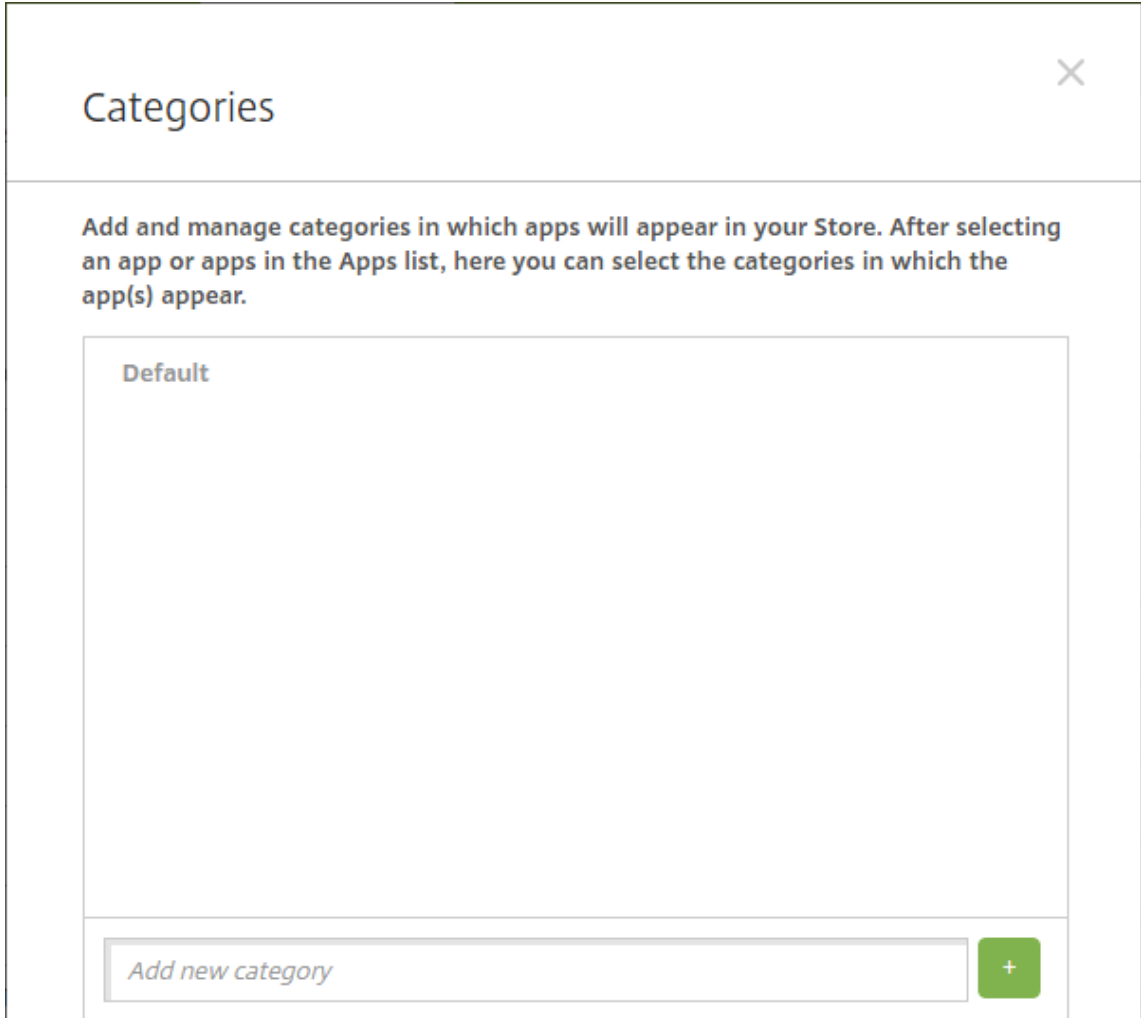
앱 범주 정보

사용자가 Secure Hub 에 로그인하면 XenMobile 에서 설정한 앱, 웹 링크 및 스토어 목록이 표시됩니다. 앱 범주를 사용하면 사용자가 액세스할 수 있는 특정 앱, 스토어 또는 웹 링크를 지정할 수 있습니다. 예를 들어 재무 범주를 만든 후 재무와 관련된 앱

만 범주에 추가할 수 있습니다. 또는 영업 범주를 구성하여 영업 앱을 할당할 수 있습니다.

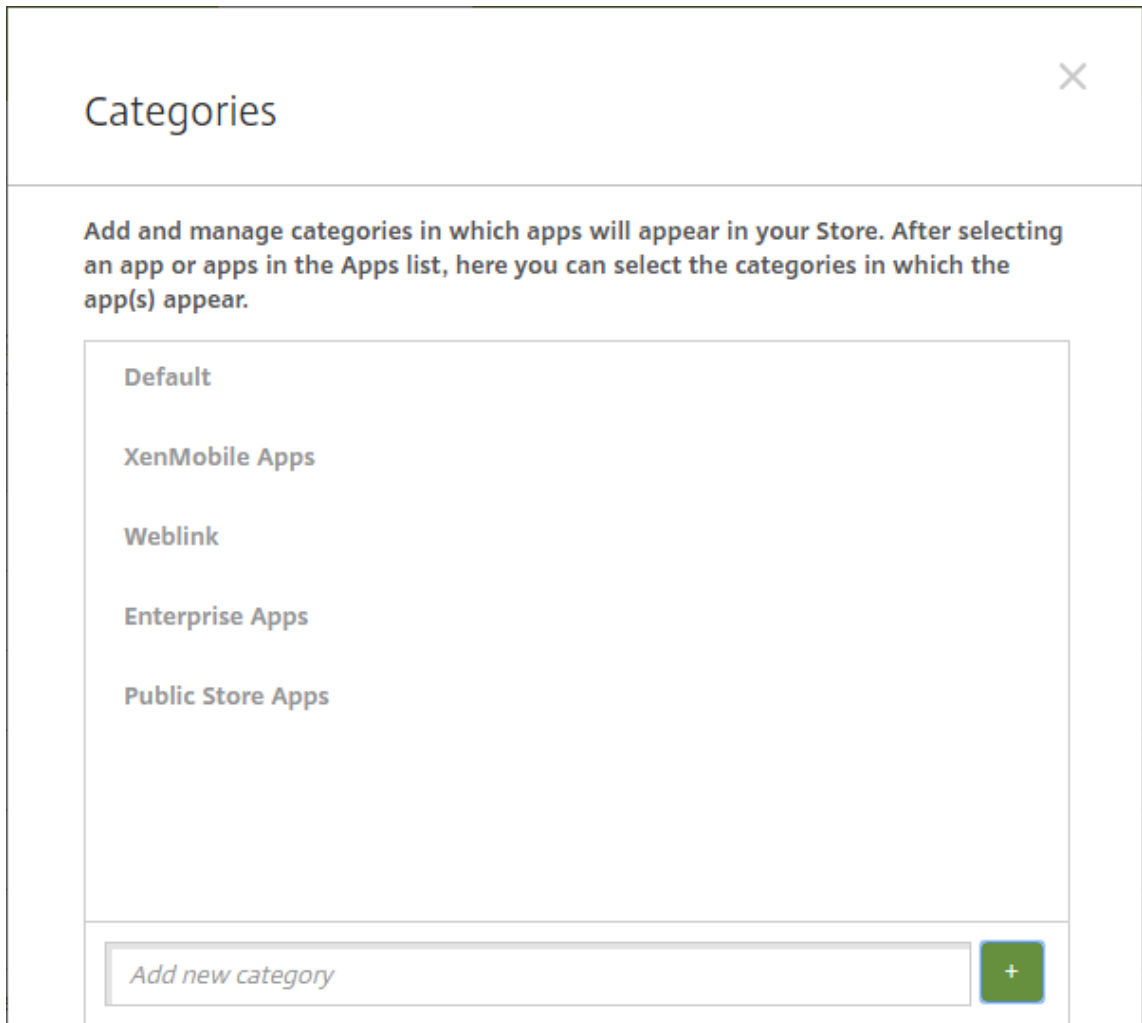
앱, 웹 링크 또는 스토어를 추가하거나 편집할 때 이전에 구성한 하나 이상의 범주에 앱을 추가할 수 있습니다.

1. XenMobile 콘솔에서 구성 > 앱 > 범주를 클릭합니다. 범주 대화 상자가 나타납니다.



2. 추가할 각 범주에 대해 다음을 수행합니다.

- 대화 상자의 맨 아래쪽에 있는 새 범주 추가 필드에 추가할 범주의 이름을 입력합니다. 예를 들어 엔터프라이즈 앱에 대한 범주를 만들려는 경우 엔터프라이즈 앱을 입력할 수 있습니다.
- 더하기 기호 (+) 를 클릭하여 범주를 추가합니다. 새로 만들어진 범주가 추가되고 범주 대화 상자에 표시됩니다.



3. 범주 추가가 완료되면 범주 대화 상자를 닫습니다.

4. 앱 페이지에서 기존 앱을 새 범주에 배치할 수 있습니다.

- 범주로 분류할 앱을 선택합니다.
- 편집을 클릭합니다. 앱 정보 페이지가 나타납니다.
- 앱 범주 목록에서 범주 확인란을 선택하여 새 범주를 적용합니다. 앱에 적용하지 않을 기존 범주에 대한 확인란을 선택 취소합니다.
- 배달 그룹 할당 탭을 클릭하거나 다음 페이지에서 다음을 클릭하여 나머지 앱 설정 페이지 단계를 이동합니다.
- 배달 그룹 할당 페이지에서 저장을 클릭하여 새 범주를 적용합니다. 새 범주가 앱에 적용되고 앱 테이블에 표시됩니다.





MDX 앱 추가

iOS 또는 Android 앱에서 사용할 수 있는 MDX 파일을 받으면 앱을 XenMobile에 업로드할 수 있습니다. 앱을 업로드한 후 앱 세부 정보 및 정책 설정을 구성할 수 있습니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참

조하십시오.

- [MAM SDK Overview\(MAM SDK 개요\)](#)
- [MDX 정책 요약](#)

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 나타납니다.

Apps							
Show filter							
Search							
Add Category Export							
<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
<input type="checkbox"/>		Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
<input type="checkbox"/>		Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	

2. 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. **MDX**를 클릭합니다. **MDX** 앱 정보 페이지가 나타납니다.

4. 앱 정보 창에서 다음 정보를 입력합니다.

- 이름: 앱을 설명하는 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 표시됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.
- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

5. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.

6. 플랫폼 아래에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼에 대해서만 구성하는 경우 다른 플랫폼의 선택을 취소합니다.

7. 업로드할 MDX 파일을 선택하려면 업로드를 클릭하고 파일의 위치로 이동합니다.
8. 앱 정보 페이지에서 다음 설정을 구성합니다.
 - 파일 이름: 앱에 연결된 파일 이름을 입력합니다.
 - 앱 설명: 앱에 대한 설명을 입력합니다.
 - 앱 버전: 필요한 경우 앱 버전 번호를 입력합니다.
 - 패키지 ID: 관리되는 Google Play 스토어에서 가져온 앱의 패키지 ID 를 입력합니다.
 - 최소 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
 - 최대 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
 - 제외된 장치: 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
 - MDM 프로필이 제거된 경우 앱 제거: MDM 프로필이 제거된 경우 iOS 장치에서 앱을 제거할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 앱 데이터 백업 방지: 사용자가 iOS 장치에서 앱 데이터를 백업하는 것을 방지할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 제품 트랙: iOS 장치로 푸시할 제품 트랙을 지정합니다. 테스트용으로 설계된 추적이 있는 경우 해당 추적을 선택하여 사용자에게 할당할 수 있습니다. 기본값은 프로덕션입니다.
 - 강제로 앱 관리: 관리되지 않는 앱으로 설치한 앱의 경우 감독되지 않는 iOS 장치에서 해당 앱의 관리를 허용할 것인지 묻는 메시지를 사용자에게 표시할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 볼륨 구매를 통해 배포된 앱: Apple 볼륨 구매를 사용하여 앱을 배포할지 여부를 선택합니다. 켜짐인 경우 앱의 MDX 버전을 배포하고 볼륨 구매를 사용하여 앱을 배포하면 Secure Hub 에 볼륨 구매 인스턴스만 표시됩니다. 기본값은 꺼짐입니다.
9. MDX 정책을 구성합니다. MDX 정책은 플랫폼별로 다르며 인증, 장치 보안, 앱 제한과 같은 정책 영역에 대한 옵션이 포함됩니다. 콘솔에서 각 정책에는 정책을 설명하는 도구 설명이 포함됩니다.
10. 배포 규칙을 구성합니다. 자세한 내용은 [배포 규칙](#)을 참조하십시오.
11. 스토어 구성을 확장합니다.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

ON

Allow app comments

ON

- 앱 **FAQ**: 새 **FAQ** 질의 응답 추가를 클릭하여 앱에 대한 FAQ 를 만듭니다.
- 휴대폰/태블릿용 스크린샷 추가: 앱 스토어에 표시할 화면 캡처를 추가합니다.
- 앱 평가 허용: 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- 앱 댓글 허용: 사용자가 앱 스토어에서 앱에 관한 댓글을 남길 수 있도록 허용합니다.

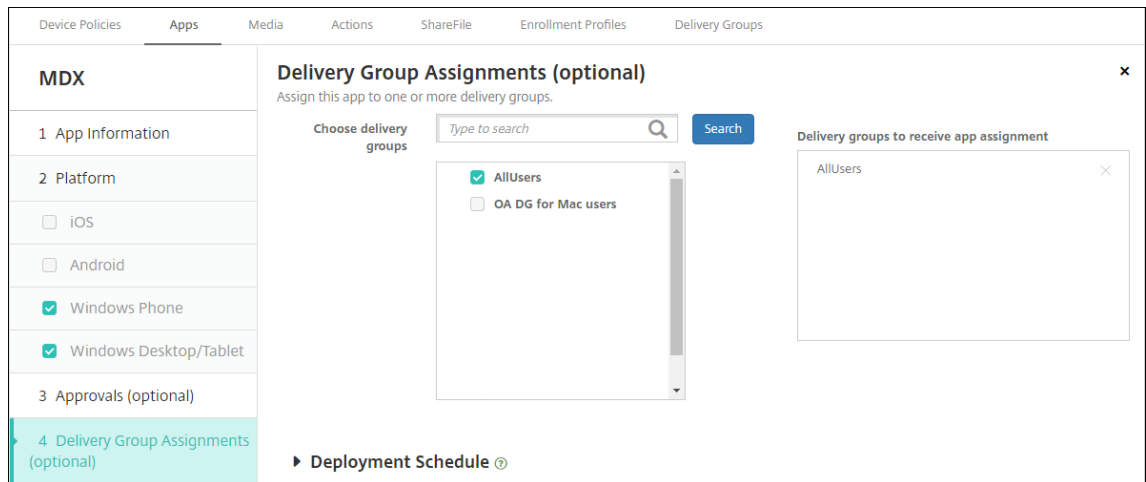
12. 다음을 클릭합니다. 승인 페이지가 나타납니다.

MDX	Approvals (optional) ×
1 App Information	Apply an existing workflow or create a new workflow to require approval before allowing users to access the app. Workflow to Use: None
2 Platform	
<input type="checkbox"/> iOS	
<input type="checkbox"/> Android	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Approvals (optional)	
4 Delivery Group Assignments (optional)	

워크플로를 사용하여 사용자의 앱 액세스를 허용하기 전에 승인을 요구하려면 워크플로 적용을 참조하십시오. 승인 워크

플로를 설정하지 않으려면 다음 단계로 계속 진행합니다.

13. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.



14. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.

15. 배포 일정을 확장하고 다음 설정을 구성합니다.

- 배포: 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 켜짐입니다.
- 배포 일정: 앱을 지금 배포할지 나중에배포할지 선택합니다. 나중에를 선택할 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 지금입니다.
- 배포 조건: 장치를 연결할 때마다 앱을 배포하려면 연결할 때마다를 선택합니다. 장치에서 이전에 앱을 받지 못한 경우 이전 배포가 실패한 경우에만을 선택하여 앱을 배포합니다. 기본값은 연결할 때마다입니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우 상시 연결에 대해 배포가 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 상시 연결에 대해 배포를 제외하고 모든 플랫폼에 적용됩니다.

16. 저장을 클릭합니다.

공용 앱 스토어 앱 추가

Apple App Store 또는 Google Play 와 같은 공용 앱 스토어에서 무료 또는 유료로 제공되는 앱을 XenMobile 에 추가할 수 있습니다.

Apple App Store 에서 앱 이름 및 설명을 검색하는 설정을 구성할 수 있습니다. 스토어에서 앱 정보를 검색하면 XenMobile 이 기존 이름과 설명을 덮어씁니다. Google Play Store 앱 정보를 수동으로 구성합니다.

Android Enterprise 용으로 유료 공용 앱 스토어 앱을 추가할 경우 대량 구매 라이선스 상태를 검토할 수 있습니다. 이 상태는 사용 가능한 총 라이선스 수, 현재 사용 중인 라이선스 수 및 라이선스를 사용하고 있는 각 사용자의 전자 메일 주소입니다. Android Enterprise 의 대량 구매 프로그램은 조직의 앱 및 기타 데이터를 대량으로 찾고, 구입하고, 배포하는 프로세스를 간소화합니다.

앱 정보를 구성하고 앱을 전달할 플랫폼 선택

1. XenMobile 콘솔에서 구성 > 앱 > 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

The 'Add App' dialog box contains the following information:

- MDX**: Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: WorxMail
- Public App Store**: Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
- Web & SaaS**: Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps_SAML
- Enterprise**: Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
- Web Link**: A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

2. 공용 앱 스토어를 클릭합니다. 앱 정보 페이지가 나타납니다.

3. 앱 정보 창에서 다음 정보를 입력합니다.

- 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 표시됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.
- 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

4. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.

5. 플랫폼 아래에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼에 대해서만 구성하는 경우 다른 플랫폼의 선택을 취소합니다.

각 플랫폼에 대한 앱 설정을 구성합니다. 참조:

- Google Play 앱에 대한 앱 설정 구성
- 관리되는 앱 스토어 앱
- iOS 앱에 대한 앱 설정 구성

플랫폼 설정 구성을 마치면 플랫폼 배포 규칙을 설정하고 앱 스토어 구성을 저장합니다.

1. 배포 규칙을 구성합니다. 자세한 내용은 [배포 규칙](#)을 참조하십시오.
2. 스토어 구성을 확장합니다.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

ON

Allow app comments

ON

- 앱 **FAQ**: 새 **FAQ** 질의 응답 추가를 클릭하여 앱에 대한 FAQ 를 만듭니다.
- 휴대폰/태블릿용 스크린샷 추가: 앱 스토어에 표시할 화면 캡처를 추가합니다.
- 앱 평가 허용: 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- 앱 댓글 허용: 사용자가 앱 스토어에서 앱에 관한 댓글을 남길 수 있도록 허용합니다.

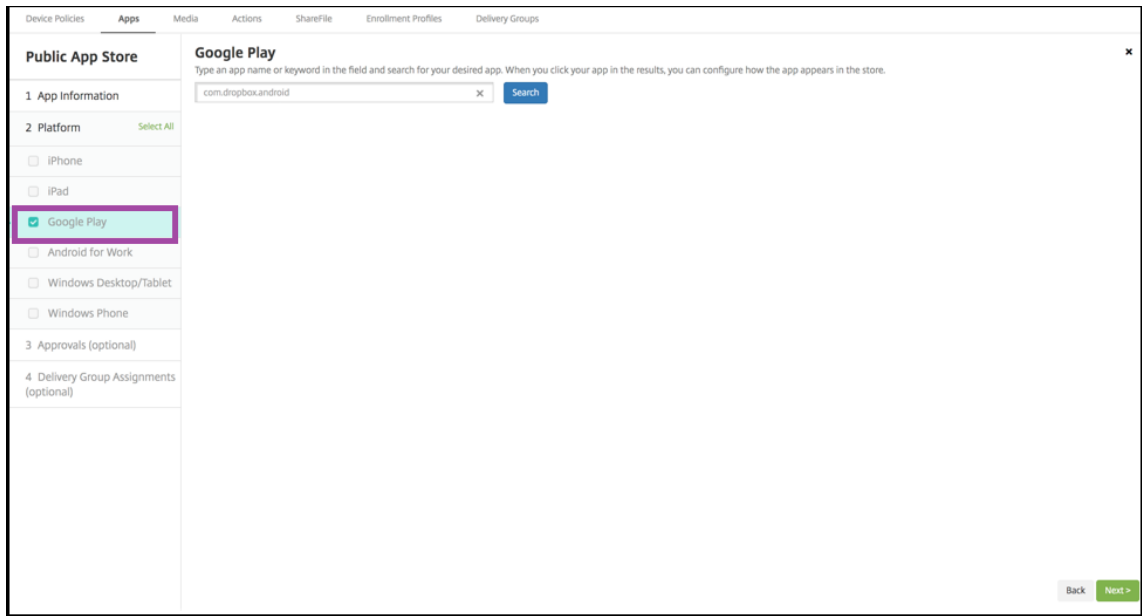
Google Play 앱에 대한 앱 설정 구성

참고:

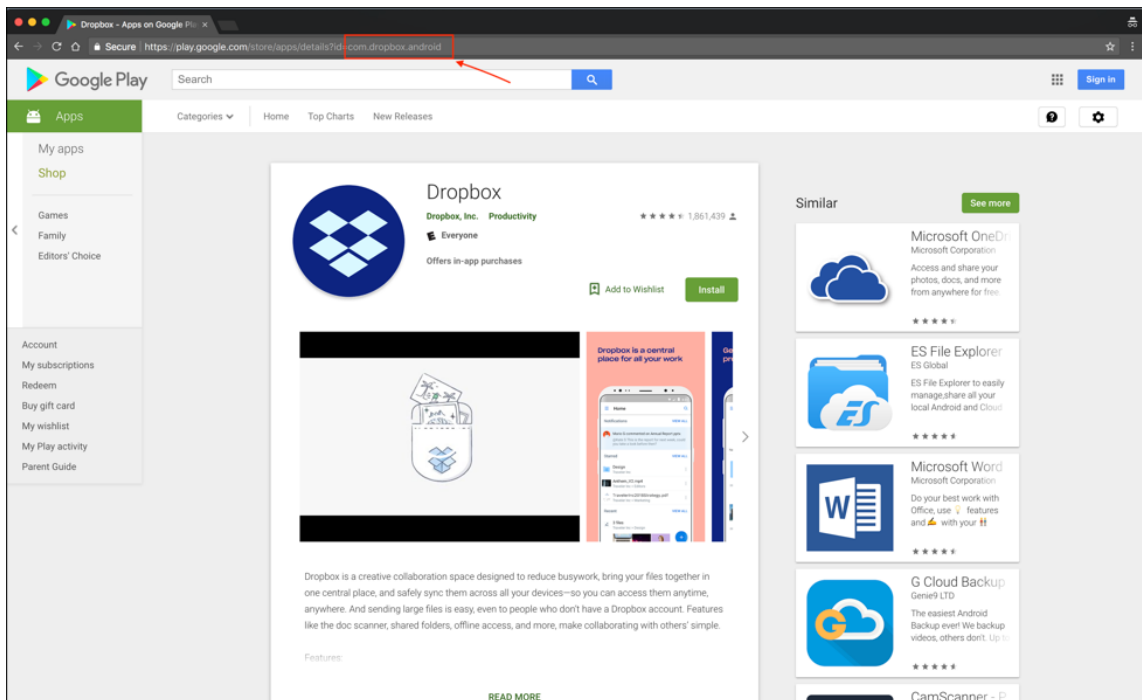
관리되는 Google Play 에서 Google Play Store 의 모든 앱에 액세스하려면 XenMobile Server 속성 관리되는 **Google Play Store** 의 모든 앱에 액세스를 사용합니다. [서버 속성](#)을 참조하십시오. 이 속성을 **true** 로 설정하면 모든 Android Enterprise 사용자에게 대한 공용 Google Play Store 앱이 허용됩니다. 이후 [제한 장치 정책](#)을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다.

Google Play Store 앱 설정을 구성하려면 다른 플랫폼과 다른 단계를 수행해야 합니다. Google Play Store 앱 정보를 수동으로 구성해야 합니다.

1. 플랫폼에서 **Google Play** 가 선택되어 있는지 확인합니다.



2. Google Play Store 로 이동합니다. Google Play Store 에서 패키지 ID 를 복사합니다. ID 는 앱의 URL 에서 찾을 수 있습니다.



3. XenMobile Server 콘솔에서 공용 스토어 앱을 추가할 때 검색 창에 패키지 ID 를 붙여 넣습니다. **Search(검색)** 를 클릭합니다.

4. 패키지 ID 가 유효하면 앱 세부 정보를 입력할 수 있는 UI 가 나타납니다.

5. 스토어의 앱과 함께 표시되도록 이미지의 URL 을 구성할 수 있습니다. Google Play Store 의 이미지를 사용하려면:

- Google Play Store 로 이동합니다. 앱 이미지를 마우스 오른쪽 버튼으로 클릭하고 이미지 주소를 복사합니다.
- Image URL(이미지 URL)** 필드에 이미지 주소를 붙여 넣습니다.
- Upload Image(이미지 업로드)** 를 클릭합니다. **Image(이미지)** 옆에 이미지가 나타납니다.

이미지를 구성하지 않으면 일반 Android 이미지가 앱과 함께 나타납니다.

ios 앱에 대한 앱 설정 구성

1. 검색 상자에 앱 이름을 입력하고 검색을 클릭합니다. 검색 기준과 일치하는 앱이 표시됩니다. 검색 기준과 일치하는 앱이 표시됩니다.

다음 그림은 iPhone 앱에서 **podio**에 대한 검색 결과를 보여 줍니다.

2. 추가할 앱을 클릭합니다.
3. 선택한 앱과 관련된 정보 (이름, 설명, 버전 번호, 관련 이미지 등)로 앱 세부 정보 필드가 채워집니다.

4. 다음 설정을 구성합니다.
 - 필요한 경우 앱의 이름 및 설명을 변경합니다.
 - 유료 앱: 이 필드는 미리 구성되며 변경할 수 없습니다.

- **MDM 프로필이 제거된 경우 앱 제거:** MDM 프로필이 제거된 경우 앱을 제거할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **앱 데이터 백업 방지:** 앱이 데이터를 백업하는 것을 방지할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **제품 트랙:** 사용자 장치로 푸시할 제품 트랙을 지정합니다. 테스트용으로 설계된 추적이 있는 경우 해당 추적을 선택하여 사용자에게 할당할 수 있습니다. 기본값은 프로덕션입니다.
- **강제로 앱 관리:** 앱이 관리되지 않는 앱으로 설치될 경우 감독되지 않는 장치에서 해당 앱의 관리를 허용할 것인지 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다. iOS 9.0 이상에서 사용할 수 있습니다.
- **장치에 강제로 라이선스 연결:** 장치 연결을 사용하는 상태에서 개발된 앱을 사용자가 아닌 장치에 연결할지 여부를 선택합니다. iOS 9 이상에서 사용할 수 있습니다. 선택한 앱이 장치 할당을 지원하지 않는 경우 이 필드를 변경할 수 없습니다.

5. 배포 규칙을 구성합니다. 자세한 내용은 [배포 규칙](#)을 참조하십시오.

6. 스토어 구성을 확장합니다.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

ON

Allow app comments

ON

- **앱 FAQ:** 새 FAQ 질의 응답 추가를 클릭하여 앱에 대한 FAQ 를 만듭니다.
- **휴대폰/태블릿용 스크린샷 추가:** 앱 스토어에 표시할 화면 캡처를 추가합니다.
- **앱 평가 허용:** 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- **앱 댓글 허용:** 사용자가 앱 스토어에서 앱에 관한 댓글을 남길 수 있도록 허용합니다.

7. iPhone 또는 iPad 의 경우 볼륨 구매를 펼칩니다.

a) XenMobile 을 사용하여 앱에 볼륨 구매 라이선스를 적용하려면 볼륨 구매 라이선스 목록에서 볼륨 구매 라이선스 업로드를 클릭합니다.

b) 표시되는 대화 상자에서 라이선스를 가져옵니다.

라이선스 할당 테이블에 사용 가능한 총 라이선스 수와 앱에 사용 중인 라이선스 수가 표시됩니다.

개별 사용자의 볼륨 구매 라이선스 연결을 해제할 수 있습니다. 이렇게 하면 라이선스 할당이 종료되고 라이선스가 확보됩니다.

8. Android Enterprise 의 경우 대량 구매 섹션을 확장합니다.

라이선스 할당 테이블에 사용 가능한 총 라이선스 수와 앱에 사용 중인 라이선스 수가 표시됩니다.

사용자를 선택하고 연결 해제를 클릭하여 라이선스 할당을 종료하고 다른 사용자를 위한 라이선스를 확보할 수 있습니다. 그러나 사용자가 특정 앱이 포함된 배달 그룹에 속하지 않는 경우에만 라이선스 연결을 해제할 수 있습니다.

▼ Bulk Purchase

License Assignment

Disassociate

License Usage: 2 of 3

<input type="checkbox"/>	Associated User	
<input checked="" type="checkbox"/>	@.net	
<input type="checkbox"/>		

Showing 1 - 2 of 2 items

9. 볼륨 구매 또는 대량 구매 설정을 완료한 후 다음을 클릭합니다. 승인 페이지가 나타납니다.

워크플로를 사용하여 사용자의 앱 액세스를 허용하기 전에 승인을 요구하려면 워크플로 적용을 참조하십시오. 승인 워크플로가 필요하지 않은 경우 다음 단계로 계속 진행합니다.

10. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.

11. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.

12. 배포 일정을 확장하고 다음 설정을 구성합니다.

- **배포:** 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **배포 일정:** 앱을 지금 배포할지 나중에배포할지 선택합니다. 나중에를 선택할 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 지금입니다.
- **배포 조건:** 장치를 연결할 때마다 앱을 배포하려면 연결할 때마다를 선택합니다. 장치에서 이전에 앱을 받지 못한 경우 이전 배포가 실패한 경우에만 선택하여 앱을 배포합니다. 기본값은 연결할 때마다입니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우 상시 연결에 대해 배포가 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 상시 연결에 대해 배포를 제외하고 모든 플랫폼에 적용됩니다.

13. 저장을 클릭합니다.

웹 또는 **SaaS** 앱 추가

XenMobile 콘솔에서 사용자에게 모바일, 엔터프라이즈, 웹 및 SaaS 앱에 대한 SSO(Single Sign-On) 인증을 제공할 수 있습니다. 응용 프로그램 커넥터 템플릿을 사용하여 앱에서 SSO를 사용하도록 할 수 있습니다. XenMobile에서 제공되는 커넥터 유형의 목록은 [앱 커넥터 유형](#)을 참조하십시오. XenMobile에서 웹 또는 SaaS 앱을 추가할 때 직접 커넥터를 만들 수도 있습니다.

SSO 전용으로 제공되는 앱의 경우 설정을 저장하면 XenMobile 콘솔의 앱 탭에 앱이 표시됩니다.

1. XenMobile 콘솔에서 구성 > 앱 > 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

- MDX**
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail
- Public App Store**
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting
- Web & SaaS**
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML
- Enterprise**
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch
- Web Link**
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

2. 웹 및 **SaaS**를 클릭합니다. 앱 정보 페이지가 나타납니다.

Web & SaaS

- 1 Web & SaaS App
- 2 Details
- 3 Policies
- 4 Approvals (optional)
- 5 Delivery Group Assignments (optional)

App Information

Add a Web & SaaS app, or choose one from the app index.

App Connector

☒ Choose from existing connectors
☐ Create a new connector

App Connectors

Type to search or type an app

E	1
EchoSign_SAML	
G	3
GoogleApps_SAML	
GoogleApps_SAML_IDP	
Globoforce_SAML	
L	1

3. 다음과 같이 기존 또는 새 앱 커넥터를 구성합니다.

기존 앱 커넥터를 구성하려면

1. 이전에 표시된 것과 같이 앱 정보 페이지에서 기존 커넥터에서 선택이 이미 선택되어 있습니다. 앱 커넥터 목록에서 사용할 커넥터를 클릭합니다. 앱 커넥터 정보 페이지가 나타납니다.
2. 다음 설정을 구성합니다.
 - **앱 이름:** 미리 채워진 이름을 사용하거나 새 이름을 입력합니다.
 - **앱 설명:** 미리 채워진 설명을 사용하거나 직접 설명을 입력합니다.
 - **URL:** 미리 채워진 URL 을 사용하거나 앱의 웹 주소를 입력합니다. 선택한 커넥터에 따라 다음 페이지로 이동하기 전에 바뀌야 하는 자리 표시자가 이 필드에 포함될 수 있습니다.
 - **도메인 이름:** 해당하는 경우 앱의 도메인 이름을 입력합니다. 이 필드는 필수입니다.
 - **앱이 내부 네트워크에서 호스트됨:** 앱이 내부 네트워크의 서버에서 실행되는지 여부를 선택합니다. 원격 위치에 서 내부 앱에 연결하는 사용자의 경우 Citrix Gateway 를 통해 연결해야 합니다. 이 옵션을 켜짐으로 설정하면 VPN 키워드가 앱에 추가되고 사용자가 Citrix Gateway 를 통해 연결할 수 있습니다. 기본값은 꺼짐입니다.
 - **앱 범주:** 목록에서 앱에 적용할 선택적 범주를 클릭합니다.
 - **사용자 계정 프로비전:** 응용 프로그램에 대한 사용자 계정을 만들지 여부를 선택합니다. Globoforce_SAML 커넥터를 사용하는 경우 이 옵션을 사용하여 SSO 가 원활하게 통합되도록 해야 합니다.
 - **사용자 계정 프로비전을 사용하는 경우 다음 설정을 구성합니다.**
 - 서비스 계정
 - ★ **사용자 이름:** 앱 관리자의 이름을 입력합니다. 이것은 필수 필드입니다.
 - ★ **암호:** 앱 관리자 암호를 입력합니다. 이것은 필수 필드입니다.
 - 사용자 계정
 - ★ **사용자 권한 부여가 종료된 경우:** 목록에서 사용자가 앱에 더 이상 액세스할 수 없을 때 수행할 동작을 클릭합니다. 기본값은 계정 사용 안 함입니다.
 - 사용자 이름 규칙
 - ★ **추가할 각 사용자 이름 규칙에 대해 다음을 수행합니다.**
 - **사용자 특성:** 목록에서 규칙에 추가할 사용자 특성을 클릭합니다.
 - **길이 (문자):** 목록에서 사용자 이름 규칙에 사용할 사용자 특성의 문자 수를 클릭합니다. 기본값은 모두입니다.
 - **규칙:** 추가한 각 사용자 특성이 사용자 이름 규칙에 자동으로 추가됩니다.
 - **암호 요구 사항**
 - **길이:** 최소 사용자 암호 길이를 입력합니다. 기본값은 **8** 입니다.
 - **암호 만료**
 - **유효 기간 (일):** 암호가 유효한 일 수를 입력합니다. 유효한 값은 **0~90** 입니다. 기본값은 90 입니다.
 - **만료 후 자동으로 암호 재설정:** 암호 만료 시 암호를 자동으로 재설정할지 여부를 선택합니다. 기본값은 꺼짐 입니다. 이 필드를 사용하지 않는 경우 암호가 만료된 사용자가 앱을 열 수 없습니다.

새 앱 커넥터를 구성하려면

1. 앱 정보 페이지에서 새 커넥터 만들기를 선택합니다. 앱 커넥터 필드가 나타납니다.

Web & SaaS

- 1 Web & SaaS App
- 2 Details
- 3 Policies
- 4 Approvals (optional)
- 5 Delivery Group Assignments (optional)

App Information
Add a Web & SaaS app, or choose one from the app index.

App Connector ☐ Choose from existing connectors ☒ Create a new connector

Name*

Description*

Logon URL*

SAML version ☒ 1.1 ☐ 2.0

Entity ID*

Relay state URL

Name ID format ☒ Email Address ☐ Unspecified

ACS URL*

Image ☒ Use default ☐ Upload your own app image

Add

2. 다음 설정을 구성합니다.

- 이름: 커넥터 이름을 입력합니다. 이것은 필수 필드입니다.
- 설명: 커넥터에 대한 설명을 입력합니다. 이것은 필수 필드입니다.
- 로그인 URL: 사용자가 사이트에 로그인하는 URL 을 입력하거나 복사 후 붙여 넣습니다. 예를 들어 추가하려는 앱에 로그인 페이지가 있는 경우 웹 브라우저를 열고 앱의 로그인 페이지 (예: <https://www.example.com/logon>) 로 이동합니다. 이것은 필수 필드입니다.
- SAML 버전: 1.1 또는 2.0 을 선택합니다. 기본값은 1.1 입니다.
- 엔터티 ID: SAML 앱의 ID 를 입력합니다.
- 릴레이 상태 URL: SAML 응용 프로그램의 웹 주소를 입력합니다. 릴레이 상태 URL 은 앱의 응답 URL 입니다.
- 이름 ID 형식: 전자 메일 주소 또는 지정되지 않음을 선택합니다. 기본값은 전자 메일 주소입니다.
- ACS URL: ID 공급자 또는 서비스 공급자의 Assertion Consumer Service URL 을 입력합니다. ACS URL 은 사용자에게 SSO 기능을 제공합니다.
- 이미지: 기본 Citrix 이미지를 사용할지, 고유한 앱 이미지를 업로드할지 여부를 선택합니다. 기본값은 기본값 사용입니다.
 - 고유한 이미지를 업로드하려면 찾아보기를 클릭하고 파일의 위치로 이동합니다. 파일은 PNG 파일이어야 합니다. JPEG 또는 GIF 파일은 업로드할 수 없습니다. 사용자 지정 그래픽을 추가하면 나중에 변경할 수 없습니다.

3. 완료되면 추가를 클릭합니다. 세부 정보 페이지가 나타납니다.

4. 다음을 클릭합니다. 앱 정책 페이지가 나타납니다.

5. 다음 설정을 구성합니다.

- 장치 보안
- 탈옥 또는 루팅 차단: 탈옥 또는 루팅 장치가 앱에 액세스하는 것을 차단할지 여부를 선택합니다. 기본값은 켜짐입니다.
- 네트워크 요구 사항
- **WiFi 필요:** 앱을 실행하는 데 WiFi 연결이 필요한지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 내부 네트워크 필요: 앱을 실행하는 데 내부 네트워크가 필요한지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 내부 **WiFi** 네트워크: **WiFi** 필요를 사용하는 경우 사용할 내부 WiFi 네트워크를 입력합니다.

6. 배포 규칙을 구성합니다. 자세한 내용은 [배포 규칙](#)을 참조하십시오.

7. 스토어 구성을 확장합니다.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

ON

Allow app comments

ON

- 앱 **FAQ**: 새 **FAQ** 질의 응답 추가를 클릭하여 앱에 대한 FAQ 를 만듭니다.
- 휴대폰/태블릿용 스크린샷 추가: 앱 스토어에 표시할 화면 캡처를 추가합니다.
- 앱 평가 허용: 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- 앱 댓글 허용: 사용자가 앱 스토어에서 앱에 관한 댓글을 남길 수 있도록 허용합니다.

8. 다음을 클릭합니다. 승인 페이지가 나타납니다.

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Web & SaaS

1 Web & SaaS App

2 Details

3 Policies

4 Approvals (optional)

5 Delivery Group Assignments (optional)

Approvals (optional)

Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.

Workflow to Use

None

Back

Next >

워크플로를 사용하여 사용자의 앱 액세스를 허용하기 전에 승인을 요구하려면 워크플로 적용을 참조하십시오.

9. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.
10. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.
11. 배포 일정을 확장하고 다음 설정을 구성합니다.
 - 배포: 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 배포 일정: 앱을 지금 배포할지 나중에배포할지 선택합니다. 나중에를 선택할 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 지금입니다.
 - 배포 조건: 장치를 연결할 때마다 앱을 배포하려면 연결할 때마다를 선택합니다. 장치에서 이전에 앱을 받지 못한 경우 이전 배포가 실패한 경우에만을 선택하여 앱을 배포합니다. 기본값은 연결할 때마다입니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우 상시 연결에 대해 배포가 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 상시 연결에 대해 배포를 제외하고 모든 플랫폼에 적용됩니다.

12. 저장을 클릭합니다.

엔터프라이즈 앱 추가

XenMobile 에서 엔터프라이즈 앱은 MAM SDK 또는 MDX Toolkit 으로 준비되지 않은 기본 앱을 나타냅니다. 이러한 앱에는 MDX 앱에 연결된 정책이 포함되지 않습니다. XenMobile 콘솔의 앱 탭에서 엔터프라이즈 앱을 업로드할 수 있습니다. 엔터프라이즈 앱은 다음 플랫폼 (및 해당하는 파일 형식) 을 지원합니다.

- iOS(.ipa 파일)
- Android(.apk 파일)
- Samsung Knox(.apk 파일)
- Android Enterprise(.apk 파일)
- 참고 항목: [MDX 지원 개인 앱](#)

Google Play Store 에서 엔터프라이즈 앱으로 다운로드한 앱을 추가하는 작업은 지원되지 않습니다. 대신, Google Play Store 의 앱을 공용 앱 스토어 앱으로 추가하십시오. 공용 앱 스토어 앱 추가를 참조하십시오.

1. XenMobile 콘솔에서 구성 > 앱 > 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

2. 엔터프라이즈를 클릭합니다. 앱 정보 페이지가 나타납니다.

3. 앱 정보 창에서 다음 정보를 입력합니다.

- **이름:** 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
- **설명:** 앱의 선택적 설명을 입력합니다.
- **앱 범주:** 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

4. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.

5. 플랫폼 아래에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼에 대해서만 구성하는 경우 다른 플랫폼의 선택을 취소합니다.

6. 선택한 각 플랫폼에 대해 업로드를 클릭하고 파일의 위치로 이동하여 업로드할 파일을 선택합니다.

7. 다음을 클릭합니다. 플랫폼에 대한 앱 정보 페이지가 나타납니다.

8. 다음과 같은 플랫폼 유형에 대한 설정을 구성합니다.

- **파일 이름:** 필요한 경우 앱의 새 이름을 입력합니다.
- **앱 설명:** 필요한 경우 앱에 대한 새 설명을 입력합니다.
- **앱 버전:** 이 필드는 변경할 수 없습니다.
- **최소 OS 버전:** 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영 체제의 가장 이전 버전을 입력합니다.
- **최대 OS 버전:** 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영 체제의 가장 최신 버전을 입력합니다.
- **제외된 장치:** 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
- **패키지 ID:** 앱의 고유 식별자입니다.
- **MDM 프로파일 제거된 경우 앱 제거:** MDM 프로파일 제거된 경우 장치에서 앱을 제거할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **앱 데이터 백업 방지:** 앱이 데이터를 백업하는 것을 방지할지 여부를 선택합니다. 기본값은 켜짐입니다.

- **강제로 앱 관리:** 관리되지 않는 앱을 설치하는 경우 감독되지 않는 장치의 사용자에게 앱 관리를 허용하라는 메시지를 표시하려면 커짐을 선택합니다. 사용자가 메시지를 수락하면 앱이 관리됩니다.

9. 배포 규칙을 구성합니다. 자세한 내용은 [배포 규칙](#)을 참조하십시오.
10. 스토어 구성을 확장합니다.

The screenshot displays the 'Store Configuration' section. It includes an 'App FAQ' section with a button to 'Add a new FAQ question and answer'. Below this is the 'App screenshots' section, which contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

- 앱 **FAQ:** 새 **FAQ** 질의 응답 추가를 클릭하여 앱에 대한 FAQ 를 만듭니다.
- 휴대폰/태블릿용 스크린샷 추가: 앱 스토어에 표시할 화면 캡처를 추가합니다.
- 앱 평가 허용: 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- 앱 댓글 허용: 사용자가 앱 스토어에서 앱에 관한 댓글을 남길 수 있도록 허용합니다.

11. 다음을 클릭합니다. 승인 페이지가 나타납니다.

워크플로를 사용하여 사용자의 앱 액세스를 허용하기 전에 승인을 요구하려면 워크플로 적용을 참조하십시오. 승인 워크플로가 필요하지 않은 경우 다음 단계를 계속 진행합니다.

12. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.

13. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.

14. 배포 일정을 확장하고 다음 설정을 구성합니다.

- 배포: 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 켜짐입니다.
- 배포 일정: 앱을 지금 배포할지 나중에 배포할지 선택합니다. 나중에를 선택할 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 지금입니다.
- 배포 조건: 장치를 연결할 때마다 앱을 배포하려면 연결할 때마다를 선택합니다. 장치에서 이전에 앱을 받지 못한 경우 이전 배포가 실패한 경우에만 선택하여 앱을 배포합니다. 기본값은 연결할 때마다입니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우 상시 연결에 대해 배포가 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 상시 연결에 대해 배포를 제외하고 모든 플랫폼에 적용됩니다.

15. 저장을 클릭합니다.

웹 링크 추가

웹 링크는 인터넷 또는 인트라넷 사이트에 대한 웹 주소입니다. 웹 링크는 SSO가 필요하지 않은 웹 응용 프로그램을 가리킬 수도 있습니다. 웹 링크 구성을 마치면 링크가 앱 스토어에서 아이콘으로 표시됩니다. 사용자가 Secure Hub에 로그인하면 사용 가능한 앱 및 데스크톱의 목록과 함께 링크가 표시됩니다.

XenMobile 콘솔의 앱 탭에서 웹 링크를 구성할 수 있습니다. 웹 링크 구성을 마치면 링크가 앱 테이블의 목록에 링크 아이콘으로 나타납니다. 사용자가 Secure Hub에 로그인하면 사용 가능한 앱 및 데스크톱의 목록과 함께 링크가 표시됩니다.

링크를 추가하려면 다음 정보를 제공합니다.

- 링크 이름
- 링크 설명
- 웹 주소 (URL)
- 범주
- 역할
- .png 형식의 이미지 (선택 사항)

1. XenMobile 콘솔에서 구성 > 앱 > 추가를 클릭합니다. 앱 추가 대화 상자가 나타납니다.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

2. 웹 링크를 클릭합니다. 앱 정보 페이지가 나타납니다.

3. 앱 정보 창에서 다음 정보를 입력합니다.

이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.

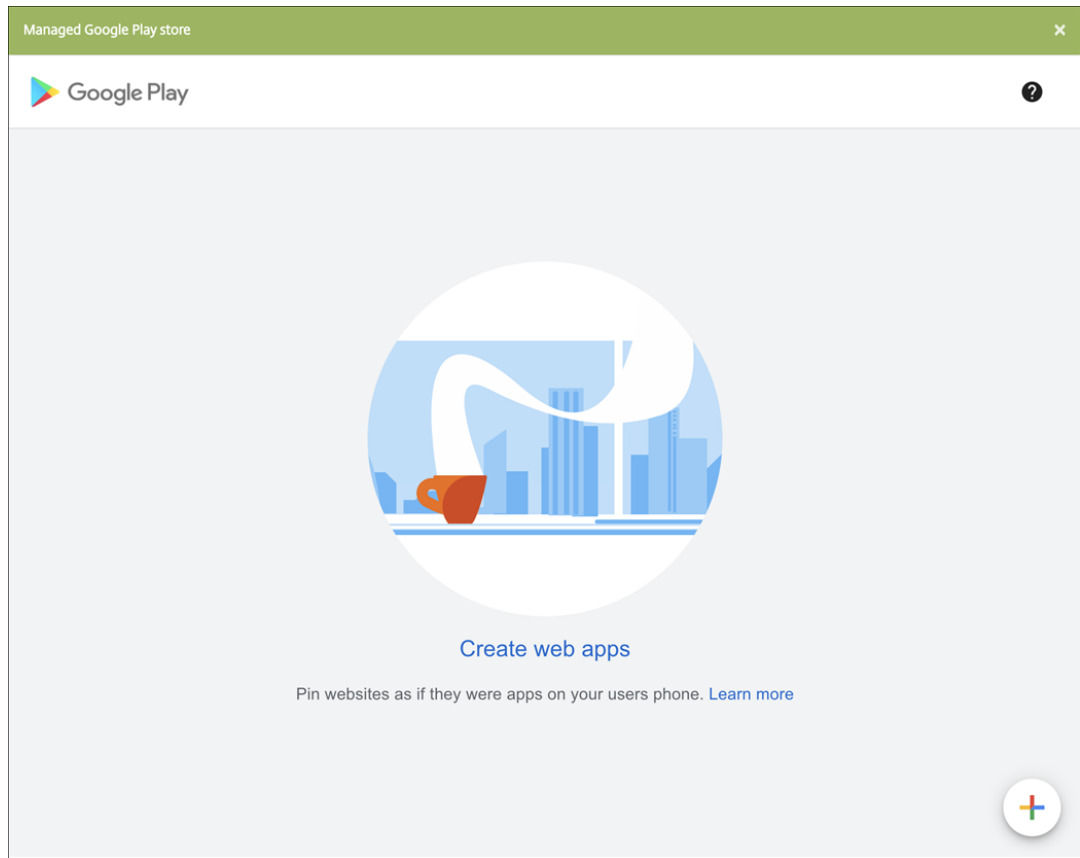
설명: 앱의 선택적 설명을 입력합니다.

앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

4. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.

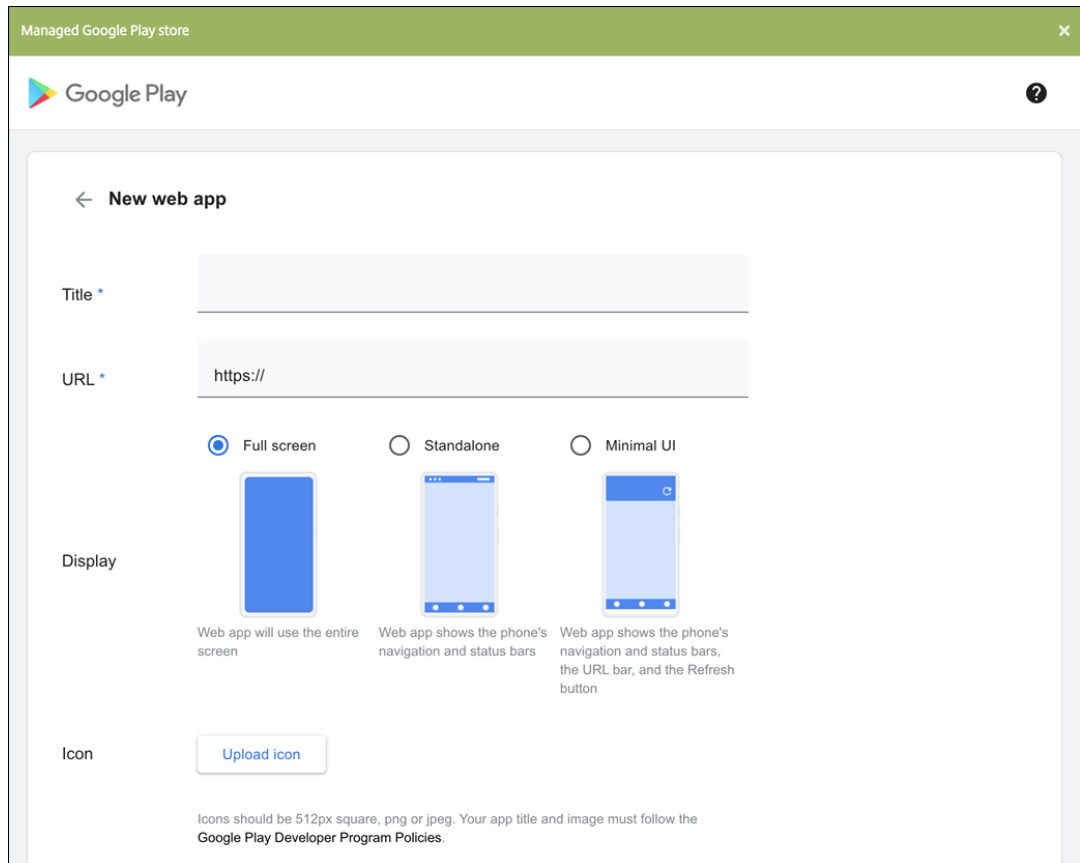
5. 플랫폼에서 iOS 및 Android(레거시 DA)용 웹 앱을 추가할 기타 플랫폼을 선택하거나 **Android Enterprise**를 선택합니다. 추가하지 않을 확인란을 선택 해제합니다.

- 기타 플랫폼을 선택한 경우 다음 단계를 계속 진행하여 설정을 구성합니다.
- Android Enterprise**를 선택할 경우 업로드 버튼을 클릭하여 관리되는 Google Play 스토어를 엽니다. 개발자 계정을 등록하지 않고도 웹 앱을 게시할 수 있습니다. 계속하려면 오른쪽 아래의 + 아이콘을 클릭합니다.



다음 설정을 구성합니다.

- 제목: 웹 앱의 이름을 입력합니다.
- **URL:** 앱의 웹 주소를 입력합니다.
- 표시: 사용자 장치에 웹 앱을 표시하는 방식을 선택합니다. 사용 가능한 옵션은 전체 화면, 독립 실행형, 최소 **UI** 입니다.
- 아이콘: 웹 앱을 나타내는 자체 이미지를 업로드합니다.



작업을 마치면 **Create(만들기)** 를 클릭합니다. 웹 앱을 게시하는 데 최대 10 분이 걸릴 수 있습니다.

6. Android Enterprise 가 아닌 플랫폼에서는 다음 설정을 구성합니다.

- 앱 이름: 미리 채워진 이름을 사용하거나 새 이름을 입력합니다.
- 앱 설명: 미리 채워진 설명을 사용하거나 직접 설명을 입력합니다.
- **URL:** 미리 채워진 URL 을 사용하거나 앱의 웹 주소를 입력합니다. 선택한 커넥터에 따라 다음 페이지로 이동하기 전에 바꿔야 하는 자리 표시자가 이 필드에 포함될 수 있습니다.
- 앱이 내부 네트워크에서 호스트됨: 앱이 내부 네트워크의 서버에서 실행되는지 여부를 선택합니다. 원격 위치에서 내부 앱에 연결하는 사용자의 경우 Citrix Gateway 를 통해 연결해야 합니다. 이 옵션을 켜짐으로 설정하면 VPN 키워드가 앱에 추가되고 사용자가 Citrix Gateway 를 통해 연결할 수 있습니다. 기본값은 꺼짐입니다.
- 앱 범주: 목록에서 앱에 적용할 선택적 범주를 클릭합니다.
- 이미지: 기본 Citrix 이미지를 사용할지, 고유한 앱 이미지를 업로드할지 여부를 선택합니다. 기본값은 기본값 사용입니다.
 - 고유한 이미지를 업로드하려면 찾아보기를 클릭하고 파일의 위치로 이동합니다. 파일은 PNG 파일이어야 합니다. JPEG 또는 GIF 파일은 업로드할 수 없습니다. 사용자 지정 그래픽을 추가하면 나중에 변경할 수 없습니다.

7. 배포 규칙을 구성합니다. 자세한 내용은 [배포 규칙](#)을 참조하십시오.

8. 스토어 구성을 확장합니다.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

ON

Allow app comments

ON

- 앱 **FAQ**: 새 **FAQ** 질의 응답 추가를 클릭하여 앱에 대한 FAQ 를 만듭니다.
- 휴대폰/태블릿용 스크린샷 추가: 앱 스토어에 표시할 화면 캡처를 추가합니다.
- 앱 평가 허용: 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- 앱 댓글 허용: 사용자가 앱 스토어에서 앱에 관한 댓글을 남길 수 있도록 허용합니다.

9. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.

10. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.

11. 배포 일정을 확장하고 다음 설정을 구성합니다.

- 배포: 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 켜짐입니다.
- 배포 일정: 앱을 지금 배포할지 나중에배포할지 선택합니다. 나중에를 선택할 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 지금입니다.
- 배포 조건: 장치를 연결할 때마다 앱을 배포하려면 연결할 때마다를 선택합니다. 장치에서 이전에 앱을 받지 못한 경우 이전 배포가 실패한 경우에만을 선택하여 앱을 배포합니다. 기본값은 연결할 때마다입니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우 상시 연결에 대해 배포가 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 상시 연결에 대해 배포를 제외하고 모든 플랫폼에 적용됩니다.

12. 저장을 클릭합니다.

Microsoft 365 앱 사용

MDX 컨테이너를 열어 Secure Mail, Secure Web 및 Citrix Files 에서 Microsoft Office 365 앱으로 문서 및 데이터를 전송할 수 있습니다. 자세한 내용은 [Office 365 앱](#)과 [Secure 상호 작용 허용](#)을 참조하십시오.

워크플로 적용

다음 설정을 구성하여 워크플로를 할당하거나 만듭니다.

- **사용할 워크플로:** 목록에서 기존 워크플로를 클릭하거나 새 워크플로 만들기를 클릭합니다. 기본값은 없음입니다.

새 워크플로 만들기를 선택하는 경우 다음 설정을 구성합니다.

- **이름:** 워크플로의 고유한 이름을 입력합니다.
- **설명:** 필요한 경우 워크플로의 설명을 입력합니다.
- **전자 메일 승인 템플릿:** 목록에서 할당할 전자 메일 승인 템플릿을 선택합니다. 이 필드 오른쪽에 있는 눈 모양 아이콘을 클릭하면 템플릿을 미리 볼 수 있는 대화 상자가 나타납니다.
- **관리자 승인 수준:** 목록에서 이 워크플로에 필요한 관리자 승인 수준의 번호를 선택합니다. 기본값은 1 수준입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * 필요 없음
 - * 1 수준
 - * 2 수준
 - * 3 수준
- **Active Directory 도메인 선택:** 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
- **추가로 필요한 승인자 찾기:** 검색 필드에 추가로 필요한 사람의 이름을 입력하고 검색을 클릭합니다. 이름은 Active Directory 에서 가져옵니다.
- **필드에 이름이 나타나면 해당하는 이름 옆의 확인란을 선택합니다.** 이름과 전자 메일 주소가 추가로 필요한 승인자 선택된 목록에 나타납니다.

추가로 필요한 승인자 선택된 목록에서 사용자를 제거하려면 다음 중 하나를 수행합니다.

 - * 선택한 도메인에 있는 모든 사용자의 목록을 표시하려면 검색을 클릭합니다.
 - * 검색 결과를 제한하려면 검색 상자에 이름 전체 또는 일부를 입력한 다음 검색을 클릭합니다.
 - * 추가로 필요한 승인자 선택된 목록에 있는 사용자는 검색 결과 목록에서 해당 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하고 제거하려는 각 이름 옆에 있는 확인란의 선택을 취소합니다.

앱 스토어 및 Citrix Secure Hub 브랜딩

앱이 스토어에 나타나는 방식을 설정하고 Secure Hub 및 앱 스토어 브랜드를 나타내는 로고를 추가할 수 있습니다. 이러한 브랜딩 기능은 iOS 및 Android 장치에서 사용할 수 있습니다.

시작하기 전에 사용자 지정 이미지가 준비되었으며 액세스할 수 있는지 확인하십시오.

사용자 지정 이미지는 다음과 같은 요구 사항을 충족해야 합니다.

- 파일은 .png 형식이어야 합니다.
- 72dpi의 투명한 배경에 순수한 흰색 로고 또는 텍스트를 사용합니다.
- 회사 로고는 높이 또는 너비가 170px x 25px(1x) 및 340px x 50px(2x)를 초과해서는 안 됩니다.
- 파일의 이름을 Header.png 및 Header@2x.png로 지정합니다.
- .zip 파일을 만듭니다. 이 파일 내부에 파일이 포함된 폴더가 있어서는 안 됩니다.

1. XenMobile Server 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 클라이언트에서 클라이언트 브랜딩을 클릭합니다. 클라이언트 브랜딩 페이지가 나타납니다.

Settings > Client Branding

Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

Store name* ⓘ

Default store view

☐ Category

☒ A-Z

Device

☒ Phone

☐ Tablet

Branding file

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
- A .zip file should be created from the files, not a folder with the files inside of it.

다음 설정을 구성합니다.

- **스토어 이름:** 사용자 계정 정보에 나타나는 스토어 이름입니다. 이름을 변경하면 스토어 서비스에 액세스하는 데 사용되는 URL도 변경됩니다. 일반적으로 기본 이름을 변경할 필요가 없습니다.

중요:

스토어 이름에는 영숫자만 사용할 수 있습니다.

- **기본 스토어 보기:** 범주 또는 **A-Z**를 선택합니다. 기본값은 **A-Z**입니다.
- **장치 옵션:** 전화 또는 태블릿을 선택합니다. 기본값은 전화입니다.
- **브랜딩 파일:** 찾아보기를 클릭하고 파일 위치로 이동하여 브랜딩에 사용할 이미지 또는 이미지의 .zip 파일을 선택합니다.

3. 저장을 클릭합니다.

앱 커넥터 유형

August 24, 2018

다음 표에는 웹 또는 SaaS 앱을 추가할 때 XenMobile 에서 사용할 수 있는 커넥터와 커넥터 유형이 나와 있습니다. 또한 웹 또는 SaaS 앱을 추가할 때 새 커넥터를 XenMobile 에 추가할 수도 있습니다.

이 표에는 커넥터가 사용자 계정 관리를 지원하는지 여부도 나타나 있습니다. 지원되는 경우 새 계정을 자동으로 또는 워크플로를 사용하여 만들 수 있습니다.

커넥터 이름	SSO SAML	사용자 계정 관리 지원
EchoSign_SAML	예	예
Globoforce_SAML		참고: 이 커넥터를 사용하는 경우 원활한 SSO 통합을 위해 User Management for Provisioning 을 사용하도록 설정해야 합니다.
GoogleApps_SAML	예	예
GoogleApps_SAML_IDP	예	예
Lynda_SAML	예	예
Office365_SAML	예	예
Salesforce_SAML	예	예
Salesforce_SAML_SP	예	예
SandBox_SAML	예	
SuccessFactors_SAML	예	
ShareFile_SAML	예	
ShareFile_SAML_SP	예	
WebEx_SAML_SP	예	예

MDX 또는 엔터프라이즈 앱 업그레이드

January 5, 2022

XenMobile 에서 MDX 또는 엔터프라이즈 앱을 업그레이드하려면 XenMobile 콘솔에서 앱을 비활성화한 다음 새 버전의 앱을 업로드합니다. Citrix Secure Mail 과 같은 공용 앱 스토어 앱은 비활성화하지 않아도 됩니다.

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 나타납니다.
2. 관리되는 장치 (모바일 장치 관리를 위해 XenMobile 에 등록된 장치) 인 경우 3 단계로 건너뛰십시오. 관리되지 않는 장치 (엔터프라이즈 앱 관리 용도로만 XenMobile 에 등록된 장치) 인 경우 다음을 수행하십시오.
 - a) 앱 테이블에서 앱 옆에 있는 확인란을 선택하거나 업데이트하려는 앱이 포함된 라인을 클릭합니다.
 - b) 나타나는 메뉴에서 사용 안 함을 클릭합니다.

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

Add | Category | Export

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input checked="" type="checkbox"/>		Secure Web	MDX	Default	4/3/20 9:42:58 am	4/3/20 9:43:04 am	<input type="checkbox"/>
<input type="checkbox"/>		Secure Mail	MDX	Default			<input type="checkbox"/>
<input type="checkbox"/>		Citrix Files	MDX	Default			<input type="checkbox"/>
<input type="checkbox"/>		AE App add	Public App Store	Default			<input type="checkbox"/>
<input type="checkbox"/>		AE google chrome	Public App Store	Default			<input type="checkbox"/>
<input type="checkbox"/>		Podio	Public App Store	Default			<input type="checkbox"/>
<input type="checkbox"/>		AE App	Public App Store	Default			<input type="checkbox"/>

Showing 1-7 of 7 items Items per page: 10

Deployment Summary: 0 Installed, 0 Pending, 0 Failed. [Show more >](#)

- c) 확인 대화 상자에서 사용 안 함을 클릭합니다. 앱의 사용 안 함 열에 사용 안 함이 나타납니다.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Secure Web	MDX	Default	4/3/20 9:42:58 am	4/3/20 9:43:04 am	Disabled
<input type="checkbox"/>		Secure Mail	MDX	Default	4/3/20 9:43:09 am	4/3/20 9:43:16 am	

참고:

앱을 사용하지 않도록 설정한 동안 로그오프하면 앱에 다시 연결할 수 없습니다. 앱을 사용하지 않도록 설정하는 것은 선택적이지만 앱 기능에 문제가 발생하지 않도록 앱을 사용하지 않도록 설정하는 것이 좋습니다. 예를 들어 사용자가 새 버전을 업로드하는 동시에 앱을 다운로드하도록 요청하는 경우 문제가 발생할 수 있습니다.

3. 앱 테이블에서 앱 옆에 있는 확인란을 클릭하거나 업데이트하려는 앱이 포함된 라인을 클릭합니다.
4. 나타나는 메뉴에서 편집을 클릭합니다. 선택한 앱에 대해 원래 선택한 플랫폼을 보여 주는 앱 정보 페이지가 나타납니다.
5. 다음 설정을 구성합니다.

- 이름: 필요한 경우 앱 이름을 변경합니다.
 - 설명: 필요한 경우 앱 설명을 변경합니다.
 - 앱 범주: 필요한 경우 앱 범주를 변경합니다.
6. 다음을 클릭합니다. 선택한 첫 번째 플랫폼 페이지가 나타납니다. 선택한 각 플랫폼에 대해 다음을 수행합니다.
- a) 업로드를 클릭하고 파일 위치로 이동하여 업로드하려는 대체 파일을 선택합니다. XenMobile 에 앱이 업로드됩니다.
 - Android Enterprise 용 앱을 업로드할 경우 관리되는 Google Play 창이 나타납니다. 여기에 새 버전의 앱을 업로드하십시오. 자세한 내용은 [Android Enterprise 앱 배포](#)를 참조하십시오.
 - b) 필요한 경우 앱 세부 정보 및 플랫폼에 대한 정책 설정을 변경합니다.
 - c) 필요한 경우 배포 규칙 및 XenMobile Store 구성을 구성합니다. 자세한 내용은 [앱 추가](#)에서 MDX 앱 추가를 참조하십시오.
7. 저장을 클릭합니다. 앱 페이지가 나타납니다.
8. 2 단계에서 앱을 사용하지 않도록 설정한 경우 다음을 수행하십시오.
- a) 앱 테이블에서 업데이트한 앱을 클릭하여 선택한 다음 나타나는 메뉴에서 사용을 클릭합니다.
 - b) 나타나는 확인 대화 상자에서 사용을 클릭합니다. 이제 사용자가 앱에 액세스하여 앱을 업그레이드하라는 알림을 받을 수 있습니다.

Citrix Launcher

March 14, 2022

Citrix Launcher 교체

Citrix 는 2020 년 8 월에 Citrix Launcher 를 앱 스토어에서 제거했습니다. Citrix Launcher 대신 이미 제공되는 기능을 사용할 수 있습니다.

장치를 키오스크 (전용 장치) 로 프로비저닝하려면:

1. XenMobile 관리자가 XenMobile 배포에 전용 장치를 등록하는 데 필요한 RBAC 역할을 추가합니다. [전용 Android Enterprise 장치 프로비전](#)을 참조하십시오.
2. 등록 유형이 완전 관리형 프로필/작업 프로필인 등록 프로필을 만듭니다. [등록 프로필을 만들려면](#)을 참조하십시오.
3. 작업 잠금 모드 설정을 사용하도록 설정하여 장치 화면에 앱을 고정하도록 구성하는 키오스크 장치 정책을 만듭니다. [Android Enterprise 설정](#)을 참조하십시오.

Citrix Launcher 정보

Citrix Launcher 를 사용하면 XenMobile 에 의해 배포되는 Android 장치의 사용자 환경을 사용자 지정할 수 있습니다. Citrix Launcher 의 Secure Hub 관리를 위해 지원되는 최소 Android 버전은 Android 4.0.3 입니다. Citrix Launcher 및 Launcher 구성 장치 정책은 Android Enterprise 와 호환되지 않습니다.

이러한 Citrix Launcher 기능을 제어하는 **Launcher** 구성 정책을 추가할 수 있습니다.

- 사용자가 지정된 앱에만 액세스할 수 있도록 Android 장치를 관리합니다.
- 필요에 따라 Citrix Launcher 아이콘의 사용자 지정 로고 이미지와 Citrix Launcher 의 사용자 지정 배경 이미지를 지정합니다.
- 사용자가 Launcher 를 종료할 때 입력해야 하는 암호를 지정합니다.

Citrix Launcher 를 사용하면 이러한 장치 수준의 제한을 적용할 수 있는 동시에 사용자에게 Wi-Fi 설정, Bluetooth 설정 및 장치 암호 설정과 같은 장치 설정에 대한 기본 제공 액세스를 부여할 수 있습니다. Citrix Launcher 는 장치 플랫폼이 이미 제공하는 보안에 추가적인 보안 계층을 더하기 위한 것이 아닙니다.

Android 장치에 Citrix Launcher 를 제공하려면 다음과 같은 일반 단계를 따르십시오.

1. Citrix Launcher 앱을 다운로드하려면: <https://www.citrix.com/downloads>로 이동합니다. **Citrix Launcher** 를 검색합니다. 파일 이름은 CitrixLauncher.apk 입니다. 이 파일은 XenMobile 에 업로드 가능하며 래핑이 필요 없습니다.
2. 장치 정책 **Launcher** 구성 정책을 추가합니다. 구성 > 장치 정책으로 이동한 후 추가를 클릭하고 새 정책 추가 대화 상자에서 **Launcher** 를 입력합니다. 자세한 내용은 [Launcher 구성 정책](#)을 참조하십시오.

3. Citrix Launcher 앱을 XenMobile 에 엔터프라이즈 앱으로 추가합니다. 구성 > 앱에서 추가를 클릭한 후 엔터프라이즈를 클릭합니다. 자세한 내용은 [엔터프라이즈 앱 추가](#)를 참조하십시오.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

4. 구성 > 배달 그룹에서 다음 구성을 사용하여 Citrix Launcher 에 대한 배달 그룹을 만듭니다.

- 정책 페이지에서 **Launcher** 구성 정책을 추가합니다.
- 앱 페이지에서 **Citrix Launcher** 를 필수 앱으로 끌어 옵니다.
- 요약 페이지에서 배포 순서를 클릭하고 **Citrix Launcher** 앱이 **Launcher** 구성 정책보다 앞에 있는지 확인합니다.

Deployment Order

Change the deployment order by dragging the policies, apps and actions into position.

Citrix Launcher

Launcher Configuration

Cancel
Save

자세한 내용은 [리소스 배포](#)를 참조하십시오.

Apple 볼륨 구매

March 15, 2024

Apple iOS 볼륨 구매를 사용하여 iOS 앱 라이선스를 관리할 수 있습니다. 볼륨 구매 솔루션은 조직의 앱 및 기타 데이터를 대량으로 찾고, 구입하고, 배포하는 프로세스를 간소화합니다.

볼륨 구매를 사용하면 XenMobile 에서 공용 앱 스토어 앱을 배포할 수 있습니다.

- MAM 등록에는 볼륨 구매가 지원되지 않습니다. MDM 또는 MDM+MAM 에서 볼륨 구매 장치를 등록해야 합니다.
- Citrix 모바일 생산성 앱에는 볼륨 구매가 지원되지 않습니다.
- XenMobile 공용 스토어 앱을 볼륨 구매로 배포할 수는 있지만 최적화된 배포가 아닙니다. 이러한 제한을 해결하려면 XenMobile 과 Secure Hub 스토어가 개선되어야 합니다.
- 볼륨 구매를 통한 XenMobile 공용 스토어 앱 배포와 관련된 알려진 문제의 목록은 Citrix Knowledge Center 의 [CTX222633](#)를 참조하십시오.

볼륨 구매를 사용하여 해당하는 앱을 장치에 직접 배포할 수 있습니다. 또는 상환 가능한 코드를 사용하여 사용자에게 콘텐츠를 할당할 수 있습니다. XenMobile 에서 iOS 볼륨 구매와 관련된 설정을 구성할 수 있습니다.

XenMobile 은 Apple 에서 볼륨 구매 라이선스를 주기적으로 다시 가져와 해당 라이선스에 모든 변경 내용이 반영되었는지 확인합니다. 볼륨 구매에서 가져온 앱을 수동으로 삭제하는 경우가 이러한 변경에 포함됩니다. 기본적으로 XenMobile 에서 볼륨 구매 라이선스 기준은 최소 1440 분 (24 시간) 마다 새로 고쳐집니다. 새 서버 속성인 [VPP.baseline](#)을 사용하여 볼륨 구매 기준 간격을 변경할 수 있습니다. [서버 속성](#)을 참조하십시오.

앱 자동 업데이트 설정은 [VPP.baseline](#) 서버 속성과 해당 속성에 설정된 동일한 일정의 앱 업데이트에 따라서도 달라집니다.

이 문서에서는 관리되는 라이선스로 볼륨 구매를 사용하여 XenMobile 에서 앱을 배포하는 방법을 집중적으로 설명합니다. 현재 상환 코드를 사용하고 있고 관리되는 배포로 변경하려는 경우 이 Apple 지원 문서 ([볼륨 구입 프로그램을 통해 사용권 코드를 관리 배포로 마이그레이션하기](#)) 를 참조하십시오.

iOS 볼륨 구매에 대한 자세한 내용은 <https://volume.itunes.apple.com/us/store>에서 확인하십시오. 볼륨 구매에 등록하려면 <https://deploy.apple.com/qforms/open/register/index/avs>로 이동하십시오. iTunes 에서 볼륨 구매 스토어에 액세스하려면 <https://volume.itunes.apple.com/?l=en>으로 이동하십시오.

이러한 iOS 볼륨 구매 설정을 XenMobile 에 저장하면 구입한 앱이 XenMobile 콘솔의 구성 > 앱 페이지에 나타납니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 볼륨 구매를 클릭합니다. 볼륨 구매 구성 페이지가 나타납니다.

Settings > Volume purchase


Volume purchase

Configure these iOS-specific settings. When saved and validated, the Volume purchase apps are added to the table on the Apps tab.

Store user password in Secure Hub ☒ ⓘ

User property for Volume purchase country mapping ⓘ

Volume purchase Accounts

 Add

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login
<input type="checkbox"/>	test	Volume Purchase Acct	Citrix Systems	United States	10/24/20 10:43:54 am	

3. 다음 설정을 구성합니다.

- **Secure Hub**에 사용자 암호 저장: XenMobile 인증을 위한 사용자 이름과 암호를 Secure Hub에 저장할지 여부를 선택합니다. 기본값은 이 보안 방법을 사용하여 정보를 저장하는 것입니다.
- 볼륨 구매 국가 매핑을 위한 사용자 속성: 사용자가 국가별 앱 스토어에서 앱을 다운로드할 수 있도록 하는 코드를 입력합니다.

XenMobile은 이 매핑을 사용하여 볼륨 구매의 속성 풀을 선택합니다. 예를 들어 사용자 속성이 미국인 경우 볼륨 구매 코드가 영국과 관련되어 있으면 해당 사용자가 앱을 다운로드할 수 없습니다. 국가 매핑 코드에 대한 자세한 내용은 볼륨 구매 프로그램 관리자에게 문의하십시오.

4. 추가할 각 볼륨 구매 계정에 대해 추가를 클릭합니다. 볼륨 구매 계정 추가 대화 상자가 나타납니다.

5. 추가하는 각 계정에 대해 다음 설정을 구성합니다.

참고:

Apple Configurator 1을 사용하는 경우 라이선스 파일을 업로드합니다. 구성 > 앱으로 이동한 다음 플랫폼 페이지에서 볼륨 구매를 확장합니다.

- **이름:** 볼륨 구매 계정 이름을 입력합니다.
- **접미사:** 볼륨 구매 계정을 통해 받은 앱 이름과 함께 표시할 접미사를 입력합니다. 예를 들어 **VP**를 입력하면 Secure Mail 앱이 앱 목록에 **Secure Mail - VP**로 표시됩니다.
- **회사 토큰:** Apple에서 받은 볼륨 구매 서비스 토큰을 복사하고 붙여 넣습니다. 토큰을 받으려면: Apple 볼륨 구매 포털의 계정 요약 페이지에서 다운로드 단추를 클릭하여 볼륨 구매 파일을 생성하고 다운로드합니다. 이 파일에는 서비스 토큰 및 기타 정보(예: 국가 코드 및 만료일)가 포함되어 있습니다. 파일을 안전한 위치에 저장합니다.
- **사용자 로그인:** 사용자 지정 B2B 앱을 가져올 때 사용할 권한이 있는 볼륨 구매 계정 관리자 이름을 선택적으로 입력합니다.
- **사용자 암호:** 볼륨 구매 계정 관리자 암호를 입력합니다.
- **앱 자동 업데이트:** 켜짐인 경우 Apple 스토어에 업데이트가 있으면 볼륨 구매 앱이 자동으로 업데이트됩니다. 기본값은 꺼짐입니다.

6. 저장을 클릭하여 대화 상자를 닫습니다.

7. 볼륨 구매 구성을 저장하려면 저장을 클릭합니다.

XenMobile의 구성 > 앱 페이지의 목록에 앱이 추가된다는 메시지가 표시됩니다. 이 페이지에서 볼륨 구매 계정의 앱 이름에 이전 구성에 입력한 접미사가 포함된 것을 알 수 있습니다.

이제 볼륨 구매 앱 설정을 구성하고 볼륨 구매 앱에 대한 배달 그룹 및 배달 정책 설정을 조정할 수 있습니다. 이러한 구성이 완료되면 사용자가 장치를 등록할 수 있습니다. 다음 참고는 이러한 프로세스에 대한 고려 사항을 제공합니다.

- 볼륨 구매 앱 설정을 구성할 때 (구성 > 앱) 장치에 강제로 라이선스 연결을 사용합니다.

Apple 볼륨 구매 및 배포 프로그램을 감독되는 장치에서 사용할 경우 XenMobile 을 사용하여 사용자 수준이 아닌 장치 수준에서 앱을 할당할 수 있다는 장점이 있습니다. 따라서 Apple ID 장치를 사용하지 않아도 됩니다. 또한 사용자에게 Apple 볼륨 구매 가입을 위한 초대가 전송되지 않습니다. 사용자 또한 iTunes 계정에 로그인하지 않고 앱을 다운로드할 수 있습니다.

해당 앱에 대한 볼륨 구매 정보를 보려면 볼륨 구매를 확장합니다. 볼륨 구매 라이선스 키 표에서 라이선스가 장치에 연결된 것을 볼 수 있습니다. 사용자가 토큰을 제거한 후 다시 가져오면 Apple 개인 정보 보호 제한으로 인해 일련 번호 대신 숨김 단어가 표시됩니다.

라이선스 연결을 해제하려면 라이선스에 대한 행을 클릭한 후 연결 해제를 클릭합니다.

볼륨 구매 라이선스를 사용자에게 연결하면 XenMobile 에서 사용자를 볼륨 구매 계정에 통합합니다. 또한 iTunes ID 를 볼륨 구매 계정과 연결합니다. 사용자의 iTunes ID 는 회사 또는 XenMobile Server 에 절대 표시되지 않습니다. Apple 은 이 연결을 투명하게 생성하여 사용자 개인 정보를 보호합니다. 사용자의 Apple 볼륨 구매 사용을 중지하여 사용자 계정에서 모든 라이선스 연결을 해제할 수 있습니다. 사용자를 사용 중지하려면 관리 > 장치로 이동합니다.

- XenMobile 에서 앱을 배달 그룹에 할당하면 기본적으로 앱이 선택적 앱으로 식별됩니다. XenMobile 이 앱을 장치에 배포하도록 하려면 구성 > 배달 그룹으로 이동합니다. 앱 페이지에서 앱을 필수 앱 목록으로 이동합니다.
- 공용 앱 스토어 앱에 대한 업데이트가 제공되는 경우: 볼륨 구매에서 앱을 푸시하면 장치에서 앱이 자동으로 업데이트됩니다. 사용자가 아닌 장치에 할당된 Secure Hub 에 대한 업데이트를 푸시하려면 다음을 수행합니다. 구성 > 앱의 플랫폼

페이지에서 업데이트 확인을 클릭하고 업데이트를 적용합니다.

Apple 볼륨 구매가 만료되면 XenMobile 에서 라이선스 만료 경고를 표시합니다.

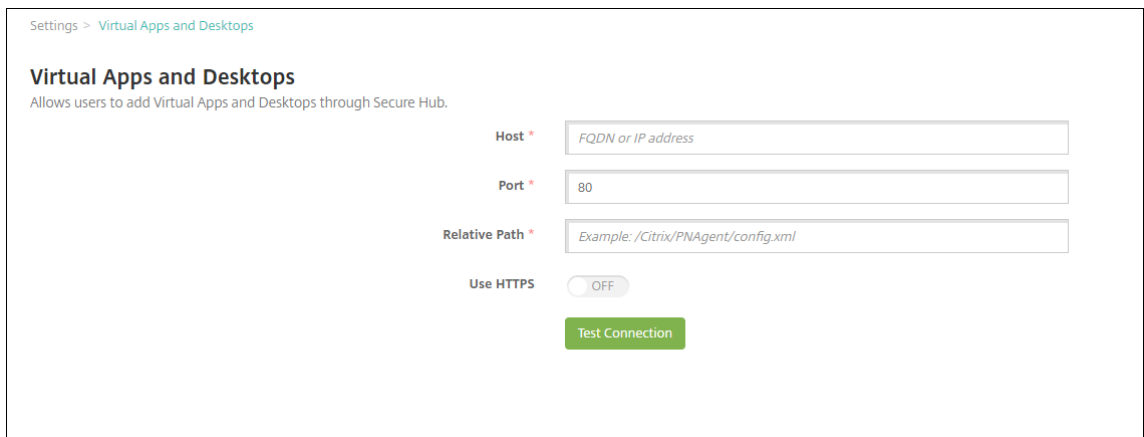
Citrix Secure Hub 를 통한 Virtual Apps and Desktops

December 1, 2020

XenMobile 에서는 Virtual Apps and Desktops 에서 앱을 수집하고 XenMobile Store 를 통해 이러한 앱을 모바일 장치 사용자에게 제공할 수 있습니다. 사용자는 XenMobile Store 내에서 직접 앱을 구독하고 Secure Hub 에서 앱을 시작할 수 있습니다. 앱을 시작하려면 Citrix Receiver 를 사용자 장치에 설치해야 하지만 이를 구성할 필요는 없습니다.

이 설정을 구성하려면 Web Interface 사이트나 StoreFront 의 FQDN(정규화된 도메인 이름) 또는 IP 주소 및 포트 번호가 필요합니다.

1. XenMobile 웹 콘솔에서 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. **Virtual Apps and Desktops** 를 클릭합니다. **Virtual Apps and Desktops** 페이지가 나타납니다.



3. 다음 설정을 구성합니다.
 - **호스트:** Web Interface 사이트나 StoreFront 의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 입력합니다.
 - **포트:** Web Interface 사이트나 StoreFront 의 포트 번호를 입력 합니다. 기본값은 80 입니다.
 - **상대 경로:** 경로를 입력합니다. 예를 들어, /Citrix/PNAgent/config.xml 을 입력할 수 있습니다.
 - **HTTPS 사용:** Web Interface 사이트 또는 StoreFront 와 클라이언트 장치 사이에 보안 인증을 사용할 것인지를 선택합니다. 기본값은 꺼짐입니다.
4. 연결 테스트를 클릭하여 XenMobile 에서 지정된 Virtual Apps and Desktops 서버에 연결할 수 있는지 확인합니다.
5. 저장을 클릭합니다.

XenMobile 에서 ShareFile 사용

March 15, 2024

Citrix Files 와 StorageZone 커넥터라는 두 가지 옵션을 사용하여 XenMobile 을 ShareFile 과 통합할 수 있습니다. Citrix Files 또는 StorageZone 커넥터와 통합하려면 XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드) 가 필요합니다.

Citrix Files

XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드) 를 사용하는 경우 Citrix Files 계정에 대한 액세스를 제공하도록 XenMobile 을 구성할 수 있습니다. 이 구성은 다음과 같습니다.

- 모바일 사용자에게 파일 공유, 파일 동기화 및 StorageZone 커넥터와 같은 전체 Enterprise 기능 집합에 대한 액세스 권한을 부여합니다.
- Citrix Files 에 XenMobile App 사용자의 Single Sign-on 인증과 포괄적인 액세스 제어 정책을 제공할 수 있습니다.
- XenMobile 콘솔을 통해 Citrix Files 구성, 서비스 수준 모니터링 및 라이선스 사용 현황 모니터링을 제공합니다.

Citrix Files 에 대해 XenMobile 을 구성하는 방법에 대한 자세한 내용은 [Citrix Files 를 사용하는 Single Sign-on 을 위한 SAML](#)을 참조하십시오.

StorageZone 커넥터

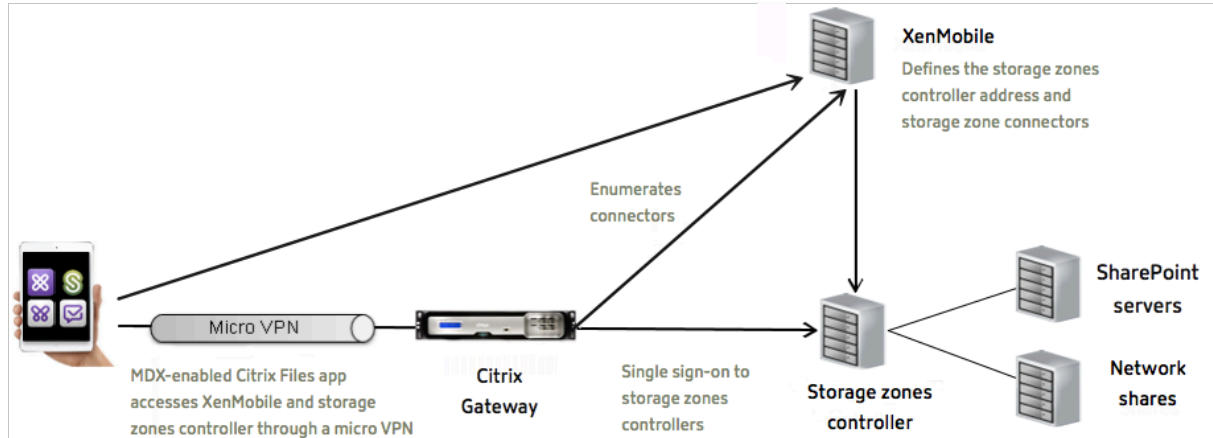
XenMobile 콘솔을 통해 만든 StorageZone 커넥터에 대한 액세스만 제공하도록 XenMobile 을 구성할 수 있습니다. 이 구성은 다음과 같습니다.

- SharePoint 사이트 및 네트워크 파일 공유 등의 기존 온-프레미스 스토리지 저장소에 대한 보안 모바일 액세스를 제공합니다.
- ShareFile 하위 도메인을 설정하거나 Citrix Files 데이터를 호스팅할 필요가 없습니다.
- 사용자가 모바일에서 iOS 및 Android 용 Citrix Files 모바일 생산성 앱을 통해 데이터에 모바일 액세스할 수 있습니다. 사용자가 Microsoft Office 문서를 편집할 수 있습니다. 또한 모바일 장치에서 Adobe PDF 파일을 미리 보고 주석을 달 수 있습니다.
- 사용자 정보가 회사 네트워크 밖으로 유출되지 않도록 하는 보안 제한 사항을 준수합니다.
- XenMobile 콘솔을 통해 StorageZone 커넥터를 간단하게 설치할 수 있습니다. 나중에 전체 Citrix Files 기능을 XenMobile 에서 사용하기로 결정한 경우 XenMobile 콘솔에서 구성을 변경할 수 있습니다.
- XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드) 가 필요합니다.

XenMobile 과 StorageZone 커넥터 전용 통합의 경우:

- ShareFile 은 Citrix Gateway 에 대한 Single Sign-On 구성을 사용하여 StorageZones Controller 에 인증합니다.
- Citrix Files 제어부가 사용되지 않기 때문에 XenMobile 이 SAML 을 통해 인증하지 않습니다.

다음 다이어그램은 XenMobile 과 StorageZone 커넥터를 함께 사용할 때의 아키텍처 개요를 보여 줍니다.



요구 사항

- 최소 구성 요소 버전:
 - XenMobile Server 10.5(온-프레미스)
 - ShareFile for iOS(MDX) 5.3
 - ShareFile for Android(MDX) 5.3
 - StorageZones Controller 5.0

이 문서에는 StorageZones Controller 5.0 구성 방법에 대한 지침이 포함되어 있습니다.
- StorageZones Controller 를 실행하는 서버가 시스템 요구 사항을 충족하는지 확인하십시오. 요구 사항은 [시스템 요구 사항](#)을 참조하십시오.

XenMobile 과 StorageZone 커넥터만 통합하는 경우 Citrix Files 데이터용 StorageZone 및 제한된 StorageZone 에 대한 요구 사항이 적용되지 않습니다.

XenMobile 은 Documentum 커넥터를 지원하지 않습니다.

- PowerShell 스크립트를 실행하려면:
 - 32 비트 (x86) 버전의 PowerShell 에서 스크립트를 실행합니다.

설치 작업

나와 있는 순서대로 다음 작업을 완료하여 StorageZones Controller 를 설치하고 설정합니다. 이러한 단계는 XenMobile 과 StorageZone 커넥터 전용 통합에만 적용됩니다. 이러한 문서 중 일부는 StorageZones Controller 설명서에 포함되어 있습니다.

1. **StorageZones Controller** 를 사용하도록 Citrix ADC 구성

Citrix ADC 를 StorageZones Controller 의 DMZ 프록시로 사용할 수 있습니다.

2. **SSL 인증서 설치**

표준 영역을 호스팅하는 StorageZones Controller 에는 SSL 인증서가 필요합니다. 제한된 영역을 호스팅하고 내부 주소를 사용하는 StorageZones Controller 에는 SSL 인증서가 필요하지 않습니다.

3. **서버 준비**

StorageZone 커넥터에는 IIS 및 ASP.NET 설정이 필요합니다.

4. **StorageZones Controller 설치**

5. **StorageZone 커넥터 전용으로 사용하도록 StorageZones Controller 준비**

6. **StorageZone 에 대한 프록시 서버 지정**

StorageZones Controllers 콘솔을 사용하여 StorageZones Controllers 의 프록시 서버를 지정할 수 있습니다. 다른 방법을 사용하여 프록시 서버를 지정할 수도 있습니다.

7. **위임을 위해 StorageZones Controller 를 신뢰하도록 도메인 컨트롤러 구성**

네트워크 공유 또는 SharePoint 사이트에서 NTLM 또는 Kerberos 인증을 지원하도록 도메인 컨트롤러를 구성합니다.

8. **보조 StorageZones Controller 를 StorageZone 에 연결**

StorageZone 에고가용성을 구성하려면 영역에 적어도 두 개의 StorageZones Controller 를 연결합니다.

StorageZones Controller 설치

1. **StorageZones Controller 소프트웨어 다운로드 및 설치:**

a) <https://www.citrix.com/downloads>로 이동합니다. **ShareFile** 을 검색한 다음 최신 StorageZones Controller 설치 관리자를 다운로드합니다.

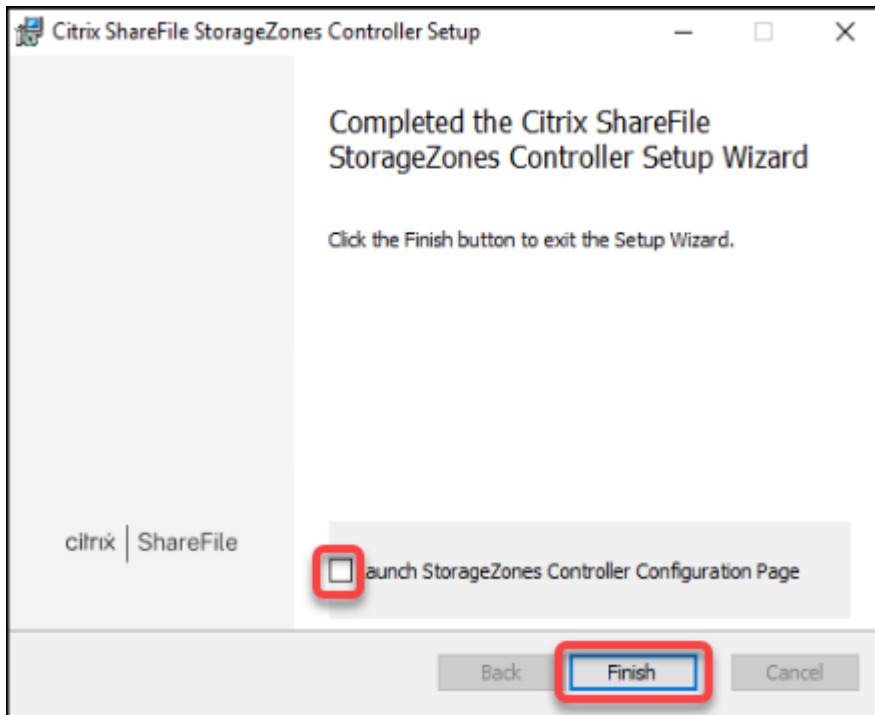
b) StorageZones Controller 를 설치하면 서버의 기본 웹 사이트가 컨트롤러의 설치 경로로 변경됩니다. 기본 웹 사이트에서 익명 인증을 사용하도록 설정합니다.

2. **StorageZones Controller 를 설치하려는 서버에서 StorageCenter.msi 를 실행합니다.**

StorageZones Controller Setup(설치) 마법사가 시작됩니다.

3. **프롬프트에 응답합니다.**

- IIS(Internet Information Services) 가 기본 위치에 설치되어 있는 경우 **Destination Folder**(대상 폴더) 페이지에서 기본값을 그대로 유지합니다. 그렇지 않은 경우 IIS 설치 위치를 찾아 선택합니다.
- 설치가 완료되면 **Launch StorageZones Controller Configuration Page**(StorageZones Controller 구성 페이지 시작) 확인란을 선택 취소한 다음 **Finish**(마침) 를 클릭합니다.



4. 메시지가 나타나면 StorageZones Controller 를 다시 시작합니다.
5. 설치가 성공적이었는지 테스트하려면 <https://localhost/>로 이동합니다. 설치가 성공적이면 Citrix Files 로고가 나타납니다.

Citrix Files 로고가 나타나지 않으면 브라우저 캐시를 지우고 다시 시도하십시오.

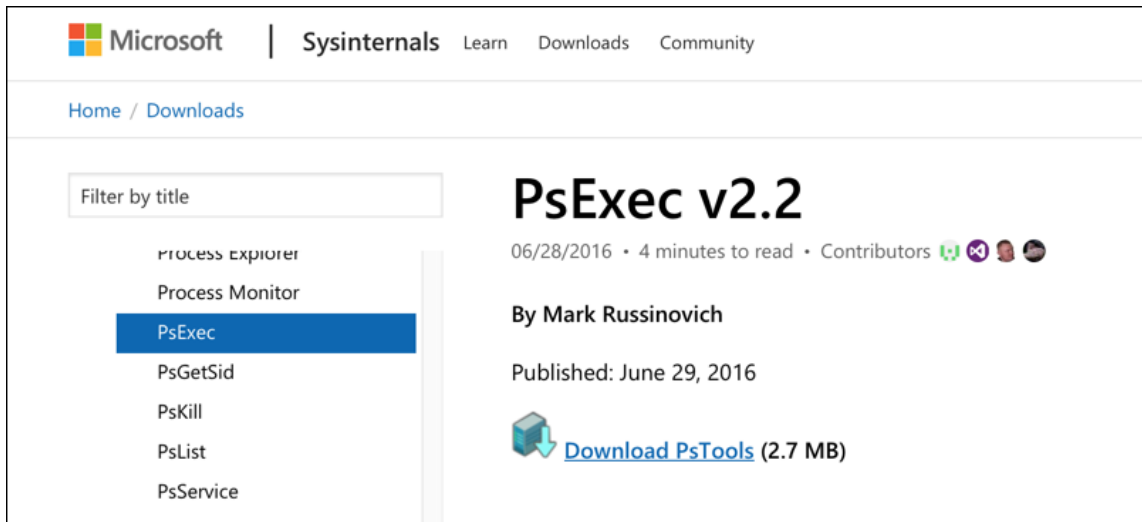
중요:

StorageZones Controller 를 복제하려는 경우 StorageZones Controller 구성을 계속하기 전에 디스크 이미지를 캡처하십시오.

StorageZone 커넥터 전용으로 사용하도록 StorageZones Controller 준비

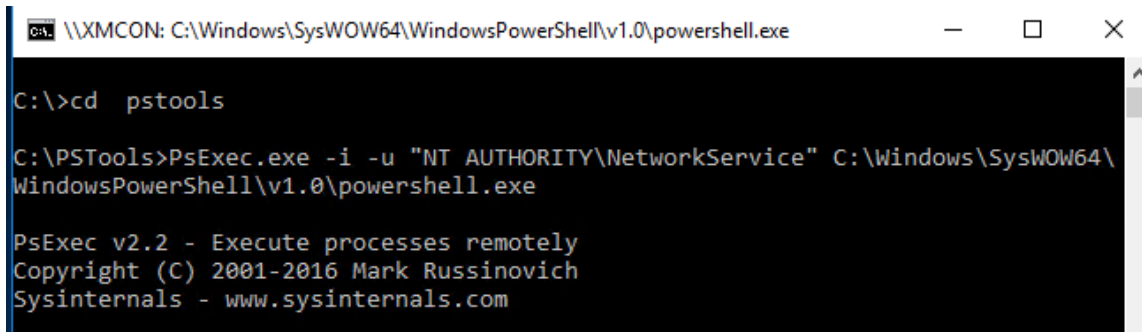
StorageZone 커넥터 전용 통합의 경우 StorageZones Controller 관리 콘솔을 사용하지 않습니다. 이 인터페이스에는 이 솔루션에 필요하지 않은 Citrix Files 관리자 계정이 필요합니다. 따라서 PowerShell 스크립트를 실행하여 Citrix Files 제어 부 없이 사용하도록 StorageZones Controller 를 준비합니다. 스크립트는 다음을 수행합니다.

- 현재 StorageZones Controller 를 기본 StorageZones Controller 로 다시 시작합니다. 나중에 보조 StorageZones Controller 를 기본 컨트롤러에 가입시킬 수 있습니다.
 - 영역을 만들고 사용할 암호를 설정합니다.
1. StorageZone Controller 서버에서 PsExec 도구 다운로드: Microsoft [Windows Sysinternals](#)로 이동한 다음 **Download PsTools(PsTools 다운로드)** 를 클릭합니다. C 드라이브 루트에 도구의 압축을 풉니다.

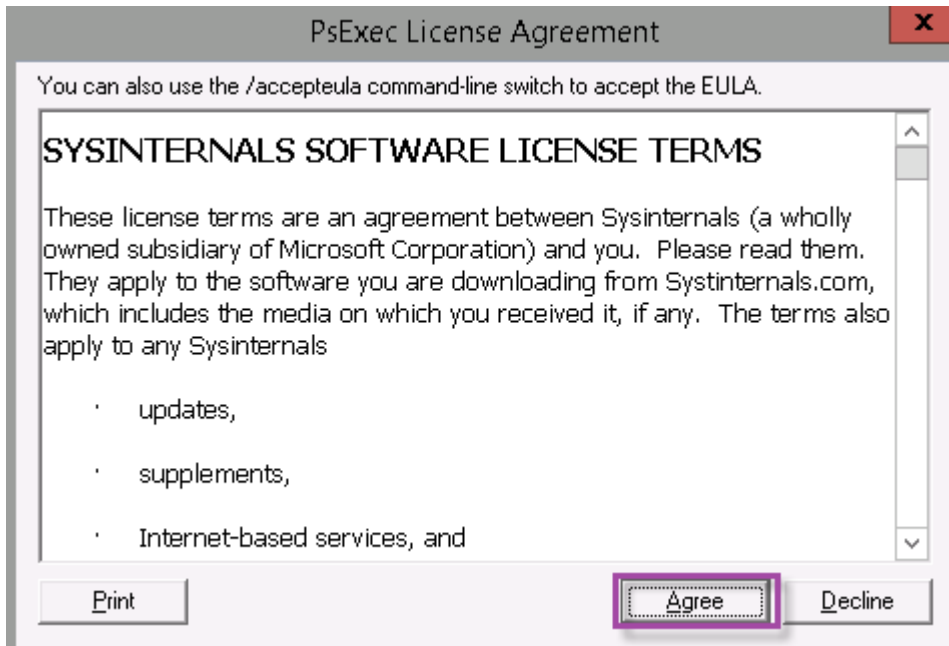


2. PsExec 도구 실행: 관리자 사용자로 명령 프롬프트를 열고 다음을 입력합니다.

```
1 cd c:\pstools
2 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
  \WindowsPowerShell\v1.0\powershell.exe
3 <!--NeedCopy-->
```



3. 메시지가 나타나면 **Agree(동의)** 를 클릭하여 Sysinternals 도구를 실행합니다.



PowerShell 창이 열립니다.

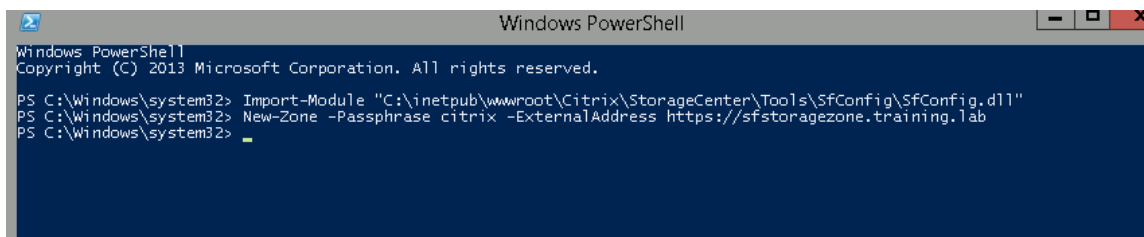
4. PowerShell 창에서 다음을 입력합니다.

```
1 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"
2 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
3 <!--NeedCopy-->
```

여기서:

암호: 사이트에 할당할 암호입니다. 컨트롤러에서 암호를 복구할 수 없으므로 기록해 두십시오. 암호를 분실한 경우 StorageZones Controller 를 다시 설치할 수 없습니다. 추가 StorageZones Controller 를 StorageZone 에 연결하거나 서버에 장애가 발생하는 경우 StorageZone 을 복구해야 합니다.

ExternalAddress: StorageZones Controller 서버의 외부 FQDN(정규화된 도메인 이름)입니다.



이제 기본 StorageZones Controller 가 준비되었습니다.

StorageZone 커넥터를 만들기 위해 XenMobile 에 로그인하기 전: 해당되는 경우 다음 구성을 완료합니다.

[StorageZone 에 대한 프록시 서버 지정](#)

[위임을 위해 StorageZones Controller 를 신뢰하도록 도메인 컨트롤러 구성](#)

보조 StorageZones Controller 를 StorageZone 에 연결

StorageZone 커넥터를 만들려면 XenMobile 에서 StorageZones Controller 연결 정의를 참조하십시오.

보조 **StorageZones Controller** 를 **StorageZone** 에 연결

StorageZone 에고가용성을 구성하려면 영역에 적어도 두 개의 StorageZones Controller 를 연결합니다. 보조 StorageZones Controller 를 영역에 가입시키려면 보조 서버에 StorageZones Controller 를 설치합니다. 그런 다음 해당 컨트롤러를 기본 컨트롤러의 영역에 가입시킵니다.

1. 주 서버에 가입시키려는 StorageZones Controller 서버에서 PowerShell 창을 엽니다.
2. PowerShell 창에서 다음을 입력합니다.

```
Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
```

예:

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

XenMobile 에서 **StorageZones Controller** 연결 정의

StorageZone 커넥터를 추가하기 전에 StorageZone 커넥터에 대해 사용하도록 설정한 각 StorageZone Controller 에 대한 연결 정보를 구성합니다. 이 섹션에 설명된 대로 또는 커넥터를 추가할 때 StorageZones Controller 를 정의할 수 있습니다.

구성 > **ShareFile** 페이지를 처음 방문하면 페이지에 XenMobile 에서 Enterprise 계정을 사용할 때와 StorageZone 커넥터를 사용할 때의 차이점이 요약되어 있습니다.

Choose a method for integrating ShareFile with XenMobile or learn more about which mode to select.

	ShareFile Enterprise	StorageZone Connectors Only
Access network shares and SharePoint data from mobile devices	✓	✓
Edit Microsoft Office documents from mobile devices	✓	✓
Preview and annotate Adobe PDF files from mobile devices	✓	✓
Store data in Citrix-managed or customer-managed StorageZones or both	✓	
Securely share files with people inside and outside the enterprise	✓	
Sync files and data across multiple devices	✓	
Access files through the ShareFile website	✓	
Access Office 365 content and Personal Cloud connectors from mobile devices	✓	
Use auditing and reporting capabilities	✓	

[Configure ShareFile Enterprise](#) [Configure Connectors](#)

커넥터 구성을 클릭하여 이 문서의 구성 단계를 계속 수행합니다.

StorageZone Connectors [Show filter](#)

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

[Add](#) | [Manage StorageZones](#)

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
--------------------------	----------------	------	-------------	----------	-----------------

1. 구성 > **ShareFile** 에서 **StorageZone** 관리를 클릭합니다.

StorageZone Connectors [Show filter](#)

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

[Add](#) | [Manage StorageZones](#)

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
--------------------------	----------------	------	-------------	----------	-----------------

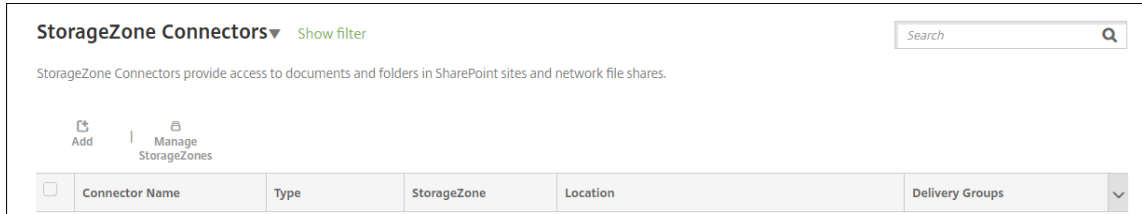
2. **StorageZone** 관리에서 연결 정보를 추가합니다.

- 이름: XenMobile 에서 StorageZone 을 식별하는 데 사용되는 StorageZone 의 설명적인 이름입니다. 이름에 공백이나 특수 문자를 사용하지 마십시오.
 - **FQDN** 및 포트: XenMobile Server 에서 연결할 수 있는 StorageZones Controller 의 FQDN(정규화된 도메인 이름) 및 포트 번호입니다.
 - 보안 연결: StorageZones Controller 에 연결하기 위해 SSL 을 사용하는 경우 기본 설정인 켜짐을 사용합니다. 연결에 SSL 을 사용하지 않는다면 이 설정을 꺼짐으로 변경합니다.
 - 관리자 사용자 이름 및 관리자 암호: 관리자 서비스 계정 사용자 이름 (domain\admin 형식) 및 암호입니다. 또는 StorageZones Controller 에 대한 읽기 및 쓰기 권한이 있는 사용자 계정입니다.
3. 저장을 클릭합니다.
 4. 연결을 테스트하려면 XenMobile Server 가 포트 443 에서 StorageZones Controller 의 FQDN(정규화된 도메인 이름) 에 연결할 수 있는지 확인합니다.
 5. 다른 StorageZones Controller 연결을 정의하려면 **StorageZone** 관리에서 추가 단추를 클릭합니다.

StorageZones Controller 연결에 대한 정보를 편집하거나 삭제하려면 **StorageZone** 관리에서 연결 이름을 선택합니다. 그런 다음 편집 또는 삭제를 클릭합니다.

XenMobile 에서 StorageZone 커넥터 추가

1. 구성 > **ShareFile** 로 이동한 다음 추가를 클릭합니다.



2. 커넥터 정보 페이지에서 다음 설정을 구성합니다.

- 커넥터 이름: XenMobile 에서 StorageZone 커넥터를 식별하는 이름입니다.
- 설명: 이 커넥터에 대한 선택적인 메모입니다.
- 유형: **SharePoint** 또는 네트워크를 선택합니다.
- **StorageZone**: 커넥터와 연결된 StorageZone 을 선택합니다. StorageZone 이 나열되지 않으면 **StorageZone** 관리를 클릭하여 StorageZones Controller 를 정의합니다.
- 위치: SharePoint 의 경우 SharePoint 루트 수준 사이트, 사이트 컬렉션 또는 문서 라이브러리의 URL 을 <https://sharepoint.company.com> 형식으로 지정합니다. 네트워크 공유의 경우 UNC(Uniform Naming Convention) 경로의 정규화된 도메인 이름을 \\server\share 형식으로 지정합니다.

3. 배달 그룹 할당 페이지에서 선택적으로 커넥터를 배달 그룹에 할당합니다. 또는 구성 > 배달 그룹을 사용하여 커넥터를 배달 그룹에 연결할 수 있습니다.

1. 요약 페이지에서 구성된 옵션을 검토할 수 있습니다. 구성을 조정하려면 뒤로를 클릭합니다.
2. 저장을 클릭하여 커넥터를 저장합니다.
3. 커넥터를 테스트합니다.

a) Citrix Files 클라이언트를 래핑하는 경우 다음을 수행합니다.

- 네트워크 액세스 정책을 내부 네트워크로 터널링됨으로 설정합니다.

이 작동 모드에서는 XenMobile MDX 프레임워크가 Citrix Files 클라이언트의 모든 네트워크 트래픽을 가로챍니다. 트래픽은 앱 전용 Micro VPN 을 사용하여 Citrix Gateway 를 통해 리디렉션됩니다.

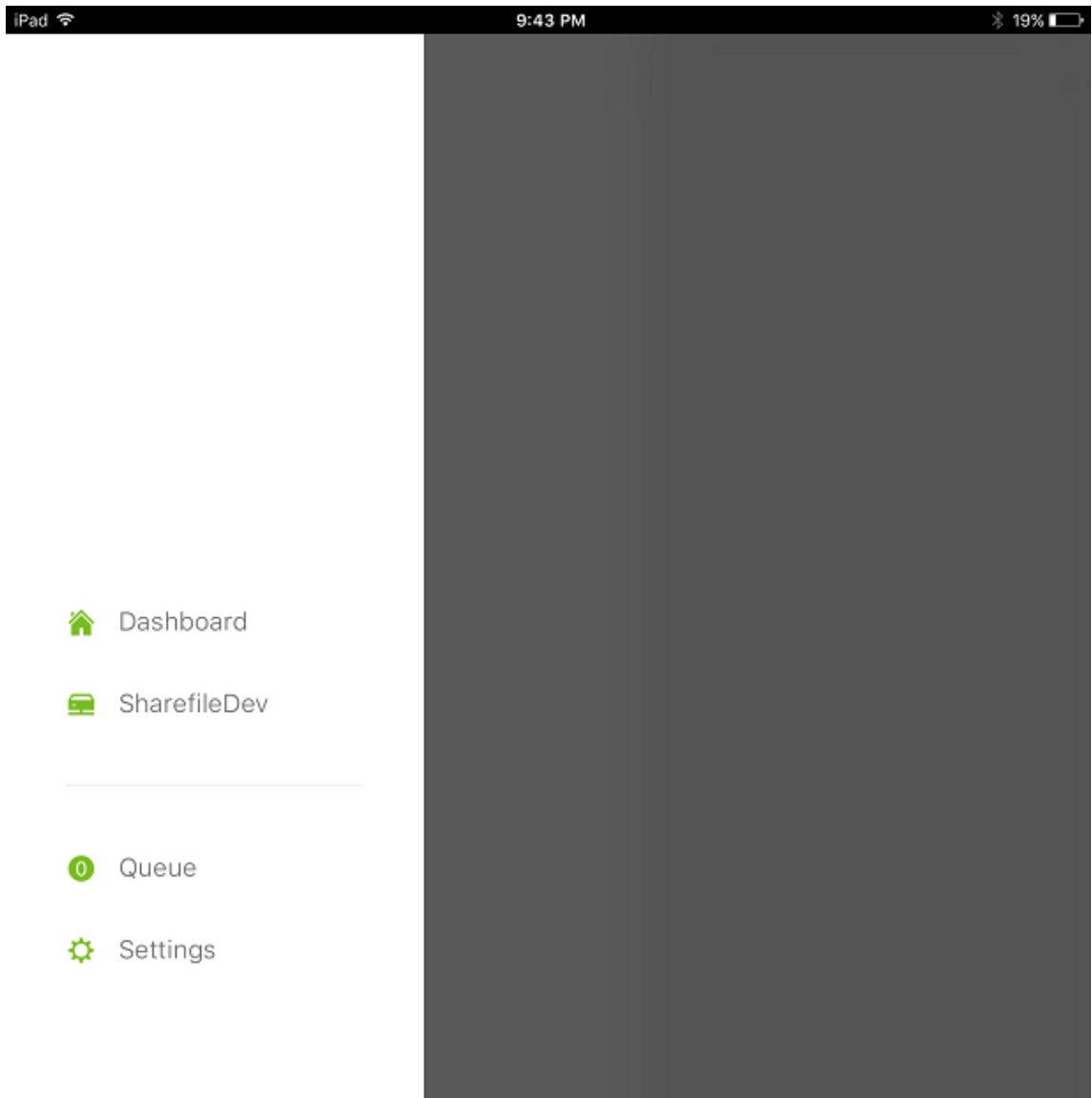
- 기본 설정 VPN 모드 정책을 터널링됨 - 웹 **SSO** 로 설정합니다.

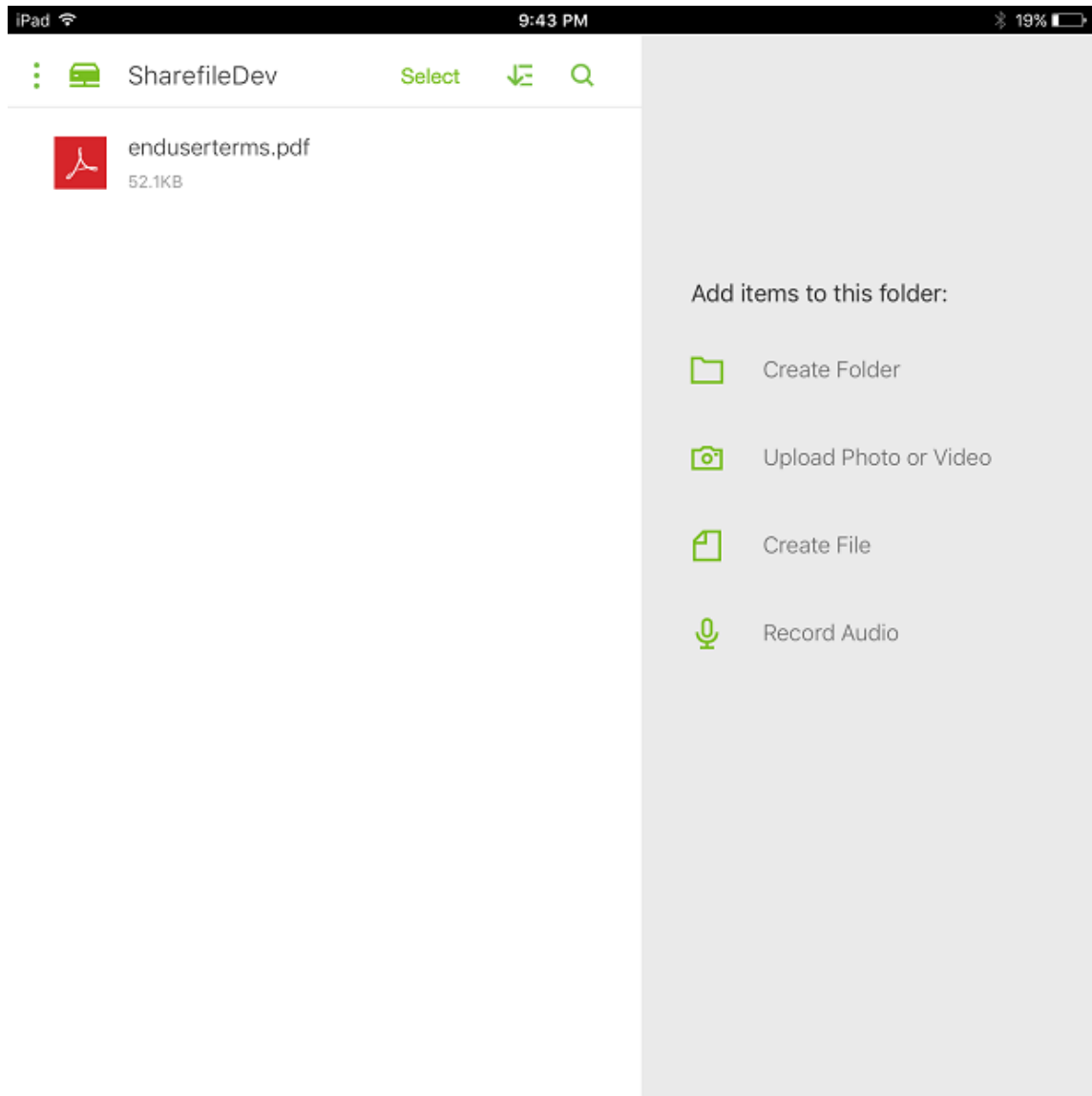
이 터널링 모드에서는 MDX 프레임워크가 MDX 앱의 SSL/HTTP 트래픽을 종료합니다. 그런 다음 MDX 가 사용자 대신 내부 연결로의 새 연결을 시작합니다. 이 정책 설정은 MDX 프레임워크가 웹 서버에서 발행된 인증 챌린지를 감지하고 이에 응답할 수 있게 합니다.

b) Citrix Files 클라이언트를 XenMobile 에 추가합니다. 자세한 내용은 [Citrix Files for Endpoint Management 클라이언트 통합 및 제공](#)을 참조하십시오.

c) 지원되는 장치에서 Citrix Files 및 커넥터에 대한 Single Sign-On 을 확인합니다.

다음 샘플에서 SharefileDev 가 커넥터 이름입니다.





StorageZone 커넥터 목록 필터링

커넥터 유형, 할당된 배달 그룹 및 StorageZone 을 기준으로 StorageZone 커넥터의 목록을 필터링할 수 있습니다.

1. 구성 > **ShareFile** 로 이동한 다음 필터 표시를 클릭합니다.

StorageZone Connectors▼ Show filter

Search

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

Add

Manage StorageZones

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups	▼
<input type="checkbox"/>	TestNS	NetworkFile	iosDev	\\Kylec-az-sz2\DevTestSZ	XM5-users	
<input type="checkbox"/>	TestSP	Sharepoint	iosDev	http://sf-az-sp2013.sfazure.com:80	XM5-users.AllUsers	

Showing 1 - 2 of 2 items

2. 필터 머리글을 확장하여 선택할 수 있게 만듭니다. 필터를 저장하려면 이 보기 저장을 클릭하고 필터 이름을 입력한 다음 저장을 클릭합니다.

Filters

Clear All

▼ Type

Clear

☒ NetworkFile 2

☐ Sharepoint 1

► Assigned Delivery Groups Clear

► StorageZone Clear

StorageZone Connectors▼ Hide filter

Search

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

Add

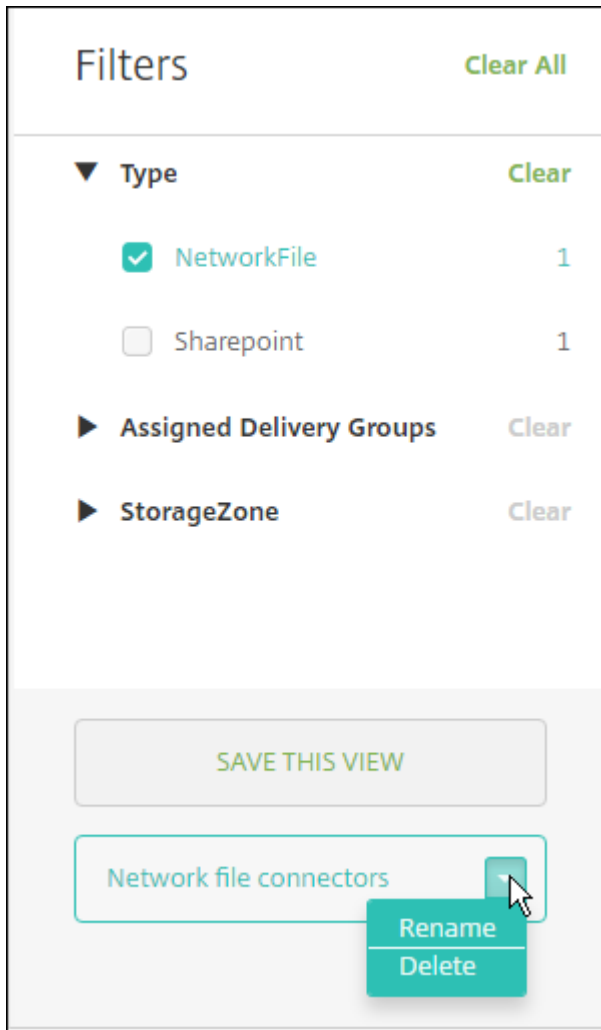
Manage StorageZones

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups	▼
<input type="checkbox"/>	TestNS	NetworkFile	sz2	\\sz2\Storagezone	XM5-users	
<input type="checkbox"/>	testxm	NetworkFile	sz1	\\sz1\Storagezone	XM5-users	

Showing 1 - 2 of 2 items

SAVE THIS VIEW

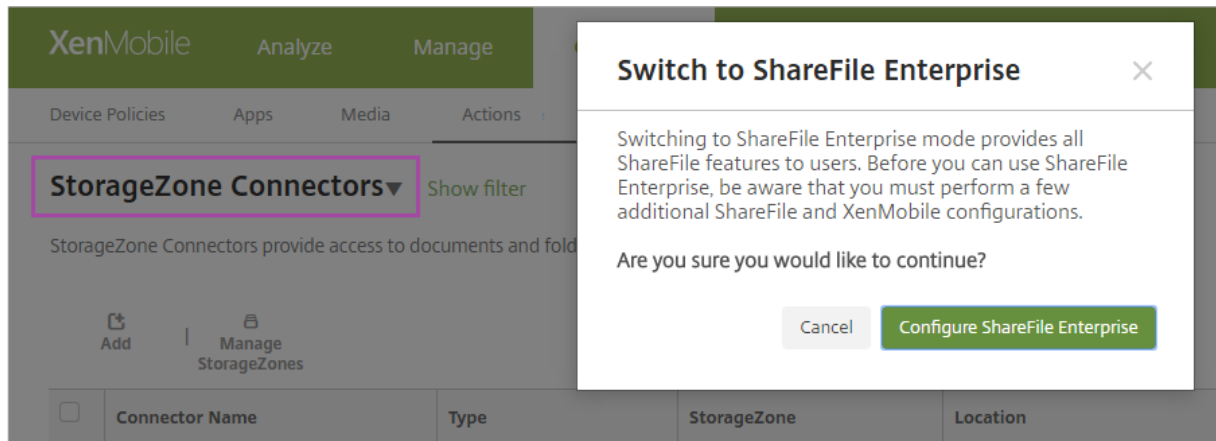
3. 필터 이름을 바꾸거나 필터를 삭제하려면 필터 이름 옆의 화살표 아이콘을 클릭합니다.



Citrix Files 로 전환

StorageZone 커넥터를 XenMobile 과 통합한 후 나중에 전체 Enterprise 기능 집합으로 전환할 수 있습니다. Citrix Files 기능 세트를 사용하려면 XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드)가 필요합니다. XenMobile 은 기존 StorageZone 커넥터 통합 설정을 유지합니다.

구성 > **ShareFile** 로 이동하고 **StorageZone** 커넥터 드롭다운 메뉴를 클릭한 다음 **ShareFile Enterprise** 구성을 클릭합니다.



Citrix Files 를 구성하는 방법에 대한 정보는 [Citrix Files 를 사용하는 Single Sign-on 을 위한 SAML](#)을 참조하십시오.

HDX 앱용 SmartAccess

January 5, 2022

이 기능을 사용하면 장치 속성, 장치의 사용자 속성 또는 장치에 설치된 응용 프로그램을 기반으로 HDX 앱에 대한 액세스 권한을 제어할 수 있습니다. 장치를 규정 위반으로 표시하여 해당 장치 액세스를 거부하는 자동화된 동작을 설정하여 이 기능을 사용합니다. 이 기능과 함께 사용되는 HDX 앱은 Virtual Apps and Desktops 에서 규정 위반 장치에 대한 액세스를 거부하는 SmartAccess 정책을 사용하여 구성됩니다. XenMobile 은 서명되고 암호화된 태그를 사용하여 장치 상태를 StoreFront 에 전달합니다. 그러면 StoreFront 가 앱의 액세스 제어 정책에 따라 액세스를 허용하거나 거부합니다.

이 기능을 사용하려면 배포에 다음이 포함되어야 합니다.

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 또는 3.8
- StoreFront 서버에서 HDX 앱을 집계하도록 구성된 XenMobile Server
- 태그 서명 및 암호화에 사용되는 SAML 인증서가 구성된 XenMobile Server. 동일한 인증서가 개인 키가 없는 상태로 StoreFront 서버에 업로드됩니다.

이 기능을 사용하려면:

- StoreFront 저장소에 대한 XenMobile Server 인증서 구성
- 필요한 SmartAccess 정책을 사용하여 하나 이상의 Virtual Apps and Desktops 배달 그룹 구성
- XenMobile 에서 자동화된 작업 설정

XenMobile Server 인증서를 내보내고 구성하여 StoreFront 저장소에 업로드

SmartAccess 는 서명되고 암호화된 태그를 사용하여 XenMobile 및 StoreFront 서버 간에 통신합니다. 이 통신을 사용하도록 설정하려면 XenMobile Server 인증서를 StoreFront 저장소에 추가합니다.

XenMobile 이 도메인 및 인증서 기반 인증을 사용하도록 설정된 경우 StoreFront 및 XenMobile 의 통합에 대한 자세한 내용은 [Support Knowledge Center](#)를 참조하십시오.

XenMobile Server 에서 SAML 인증서 내보내기

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다. 인증서를 클릭합니다.
2. XenMobile Server 의 SAML 인증서를 찾습니다.

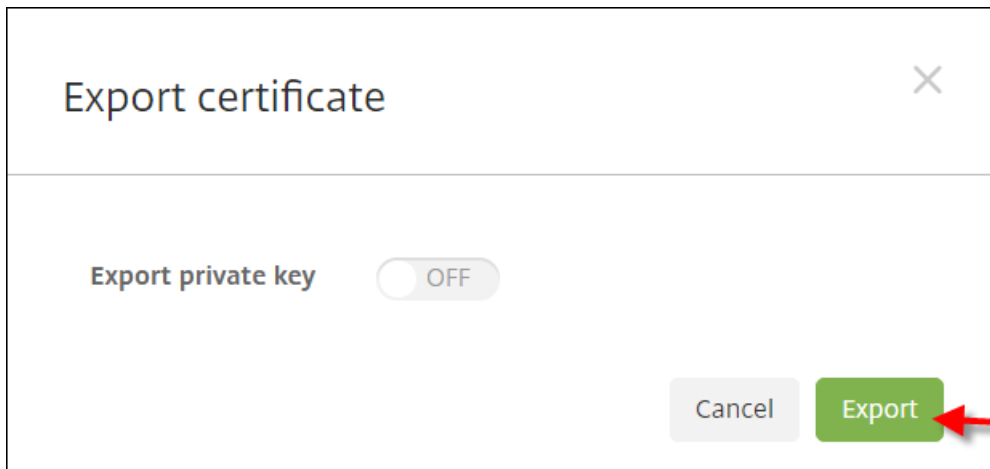
Settings > Certificates

Certificates
You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

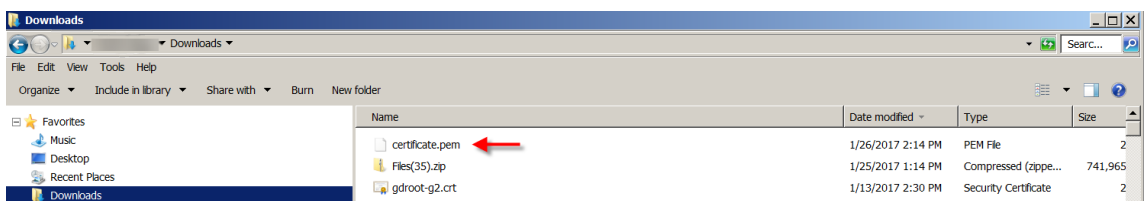
Import | Add | Detail | Export

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input checked="" type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2016-05-23	2026-05-21	SAML	✓
<input type="checkbox"/>	*.mpg.citrix.com		Up to date	2016-04-20	2017-05-27	SSL Listener	✓
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2016-05-23	2036-05-21	Devices CA	
<input type="checkbox"/>	Verizon Public SureServer CA G14-SHA2		Up to date	2014-04-09	2021-04-09	Root or intermediate	
<input type="checkbox"/>	Baltimore CyberTrust Root		Up to date	2000-05-12	2025-05-12	Root or intermediate	

3. 개인 키 내보내기가 꺼짐으로 설정되어 있는지 확인합니다. 내보내기를 클릭하여 인증서를 다운로드 디렉터리로 내보냅니다.

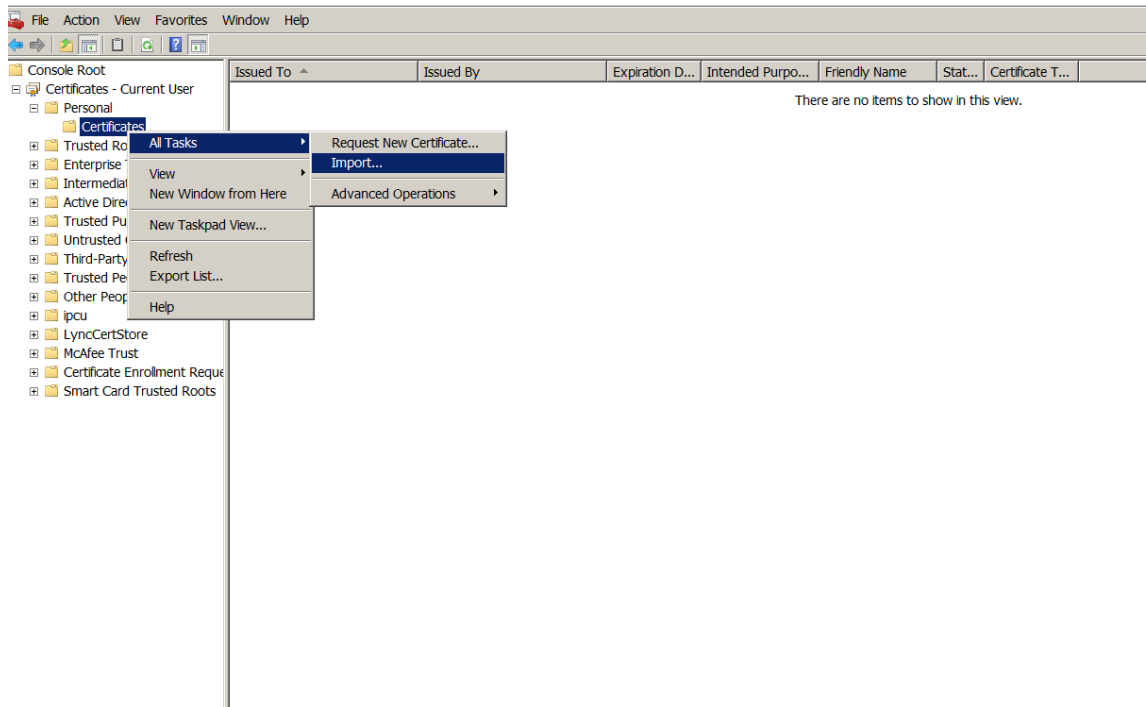


4. 다운로드 디렉터리에서 인증서를 찾습니다. 인증서는 PEM 형식입니다.

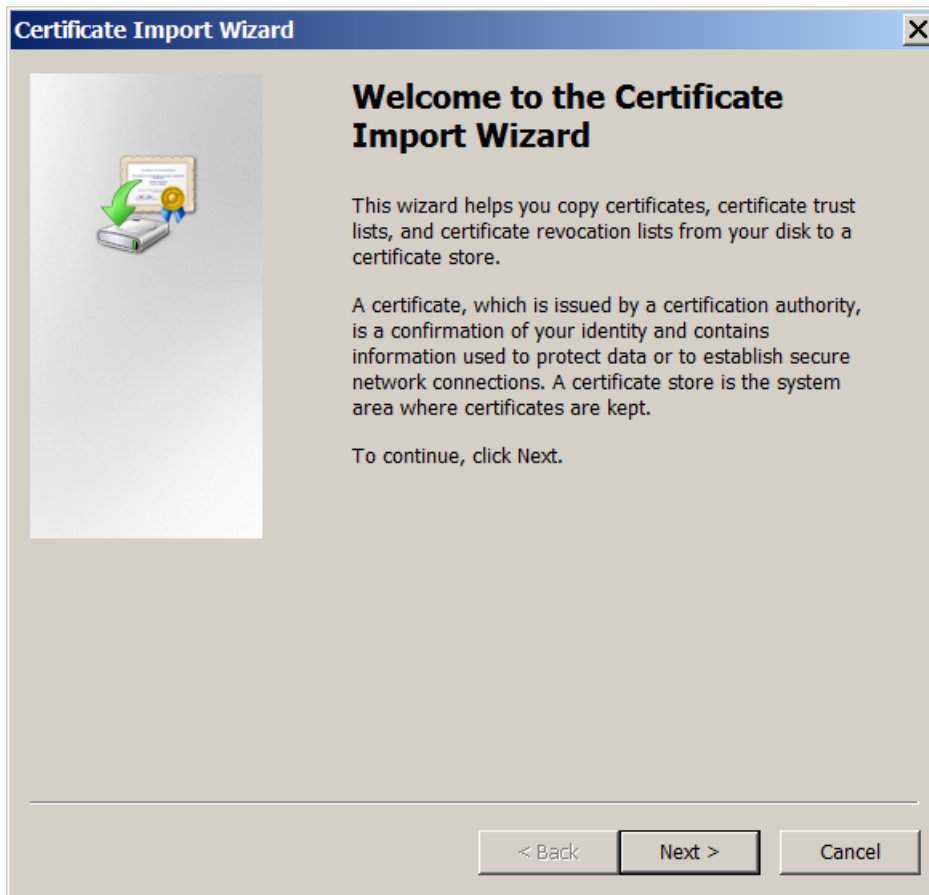


인증서를 **PEM** 에서 **CER** 로 변환

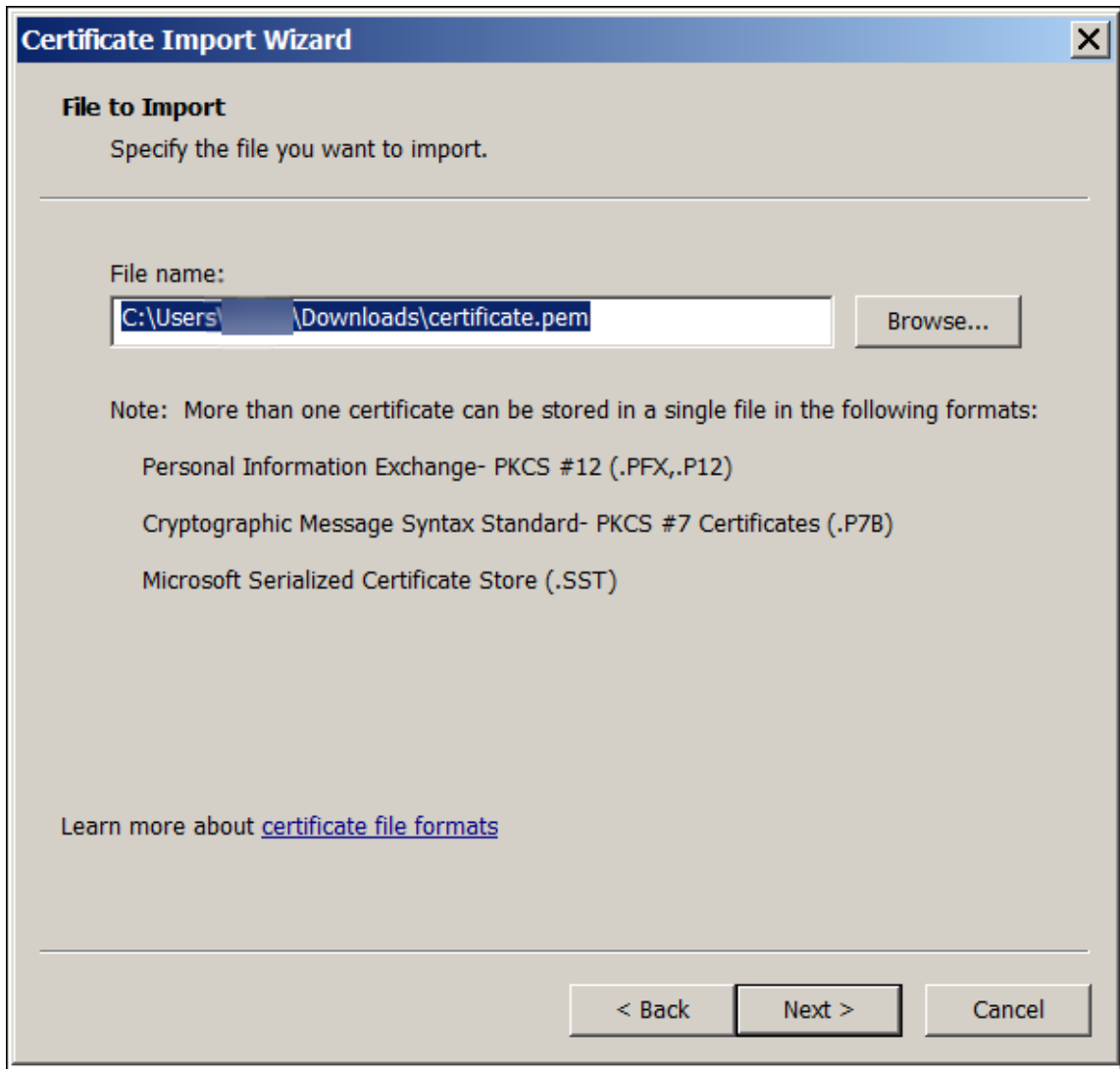
1. MMC(Microsoft Management Console) 를 열고 마우스 오른쪽 단추를 클릭하여 인증서 > 모든 작업 > 가져오기를 선택합니다.



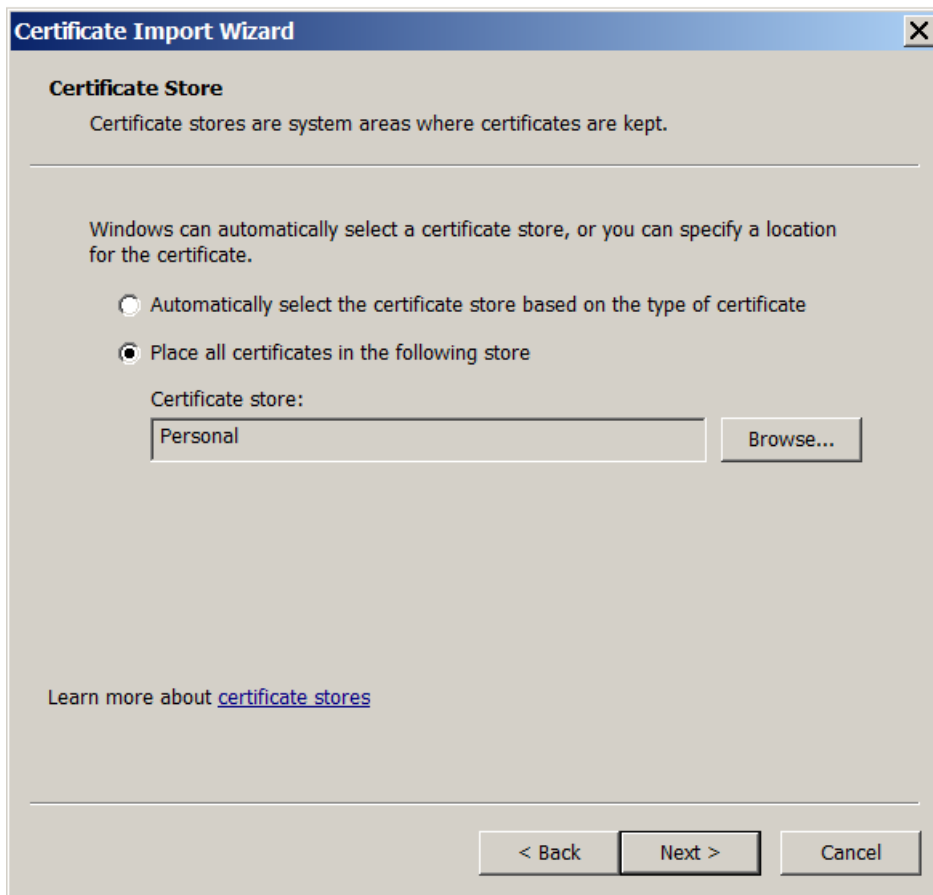
2. 인증서 가져오기 마법사가 나타나면 다음을 클릭합니다.



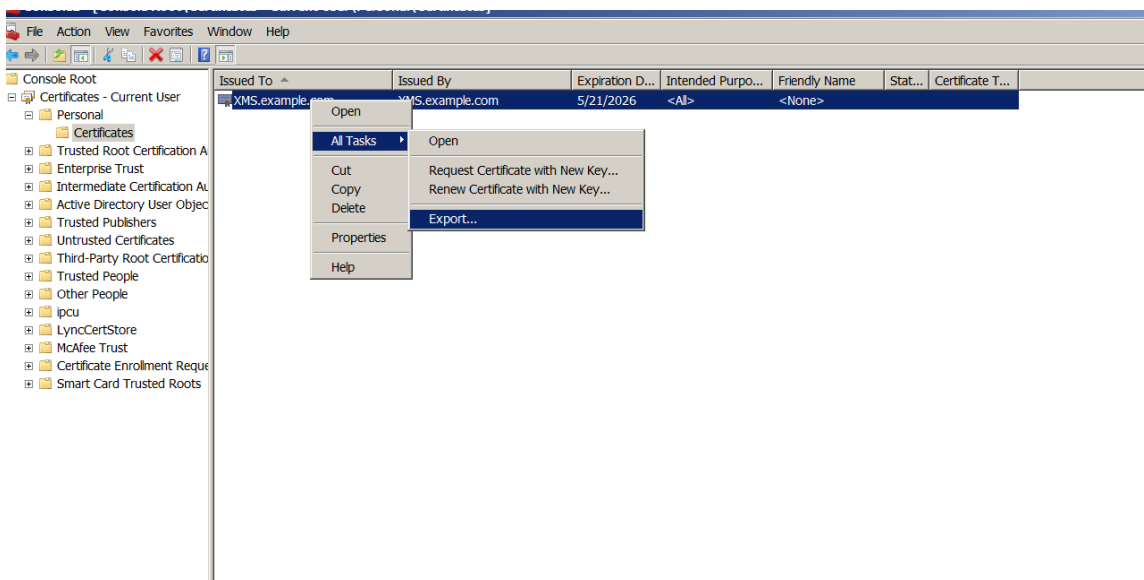
3. 다운로드 디렉터리에 있는 인증서를 찾아 선택합니다.



4. 모든 인증서를 다음 저장소에 저장을 선택하고 인증서 저장소로 개인을 선택합니다. 다음을 클릭합니다.



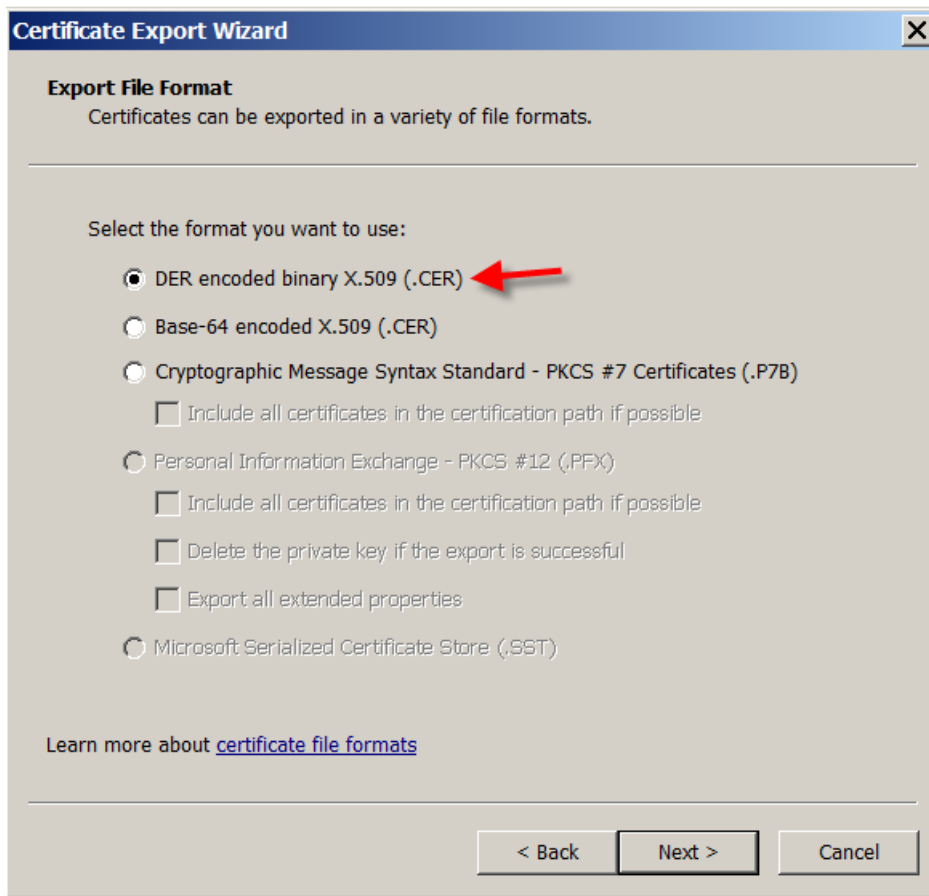
5. 선택 내용을 검토하고 마침을 클릭합니다. 확인을 클릭하여 확인 창을 닫습니다.
6. MMC 에서 인증서를 마우스 오른쪽 단추로 클릭하고 모든 작업 > 내보내기를 선택합니다.



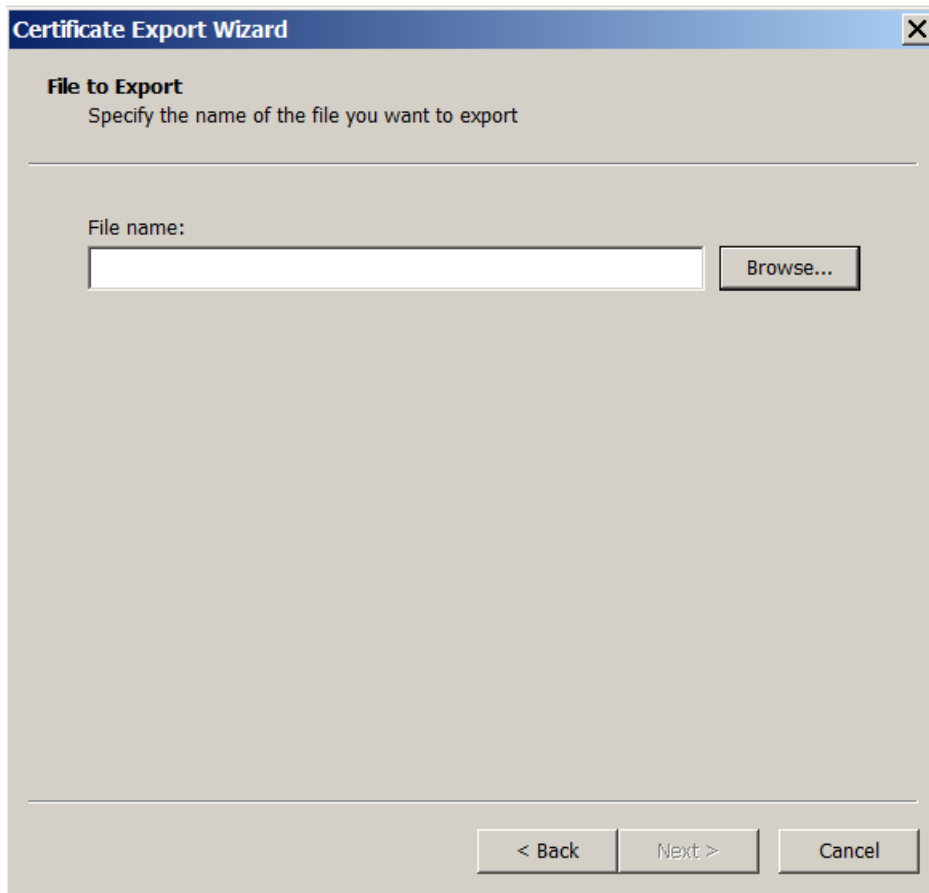
7. 인증서 내보내기 마법사가 나타나면 다음을 클릭합니다.



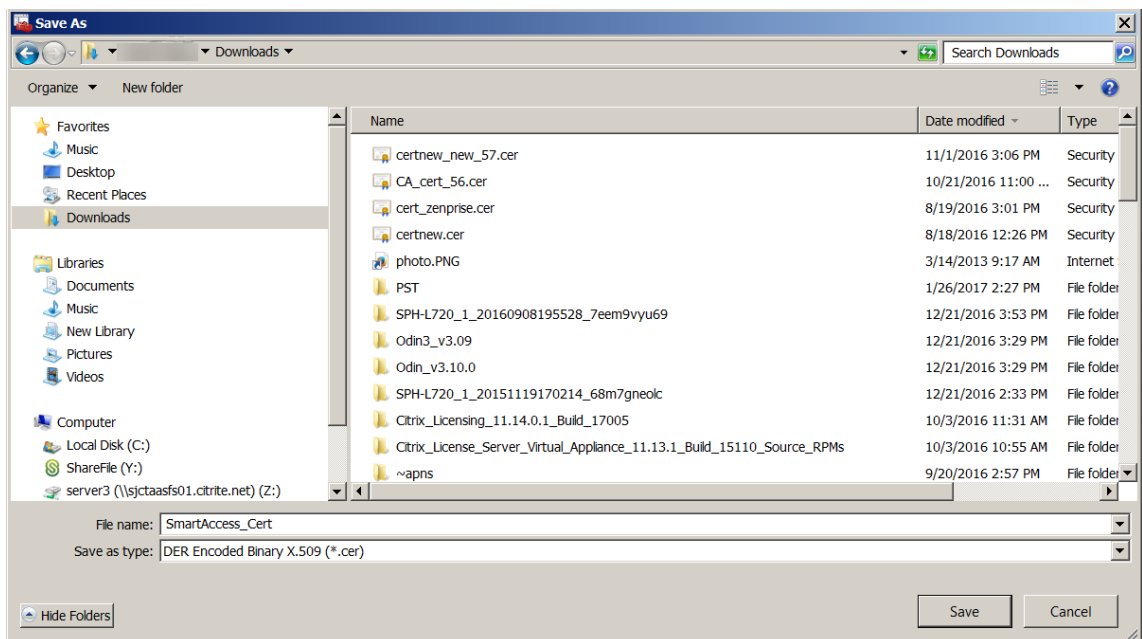
8. **DER** 로 인코딩된 바이너리 **X.509(.CER)** 형식을 선택합니다. 다음을 클릭합니다.



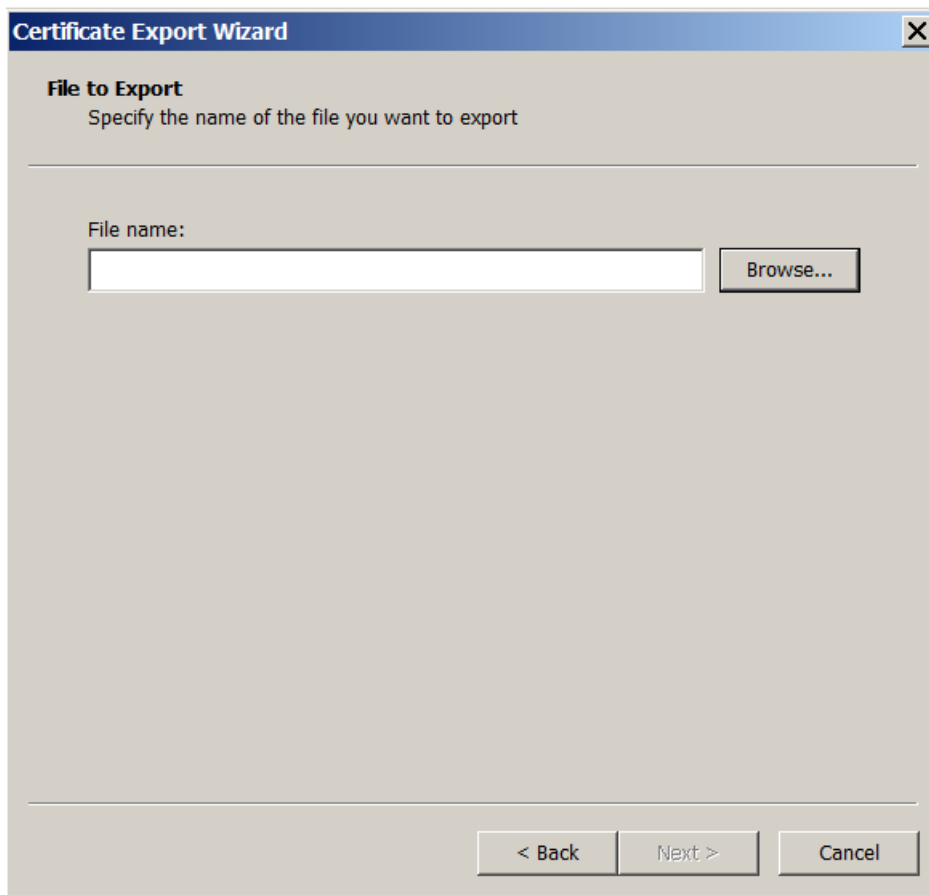
9. 인증서를 찾아봅니다. 인증서의 이름을 입력한 후 다음을 클릭합니다.



10. 인증서를 저장합니다.



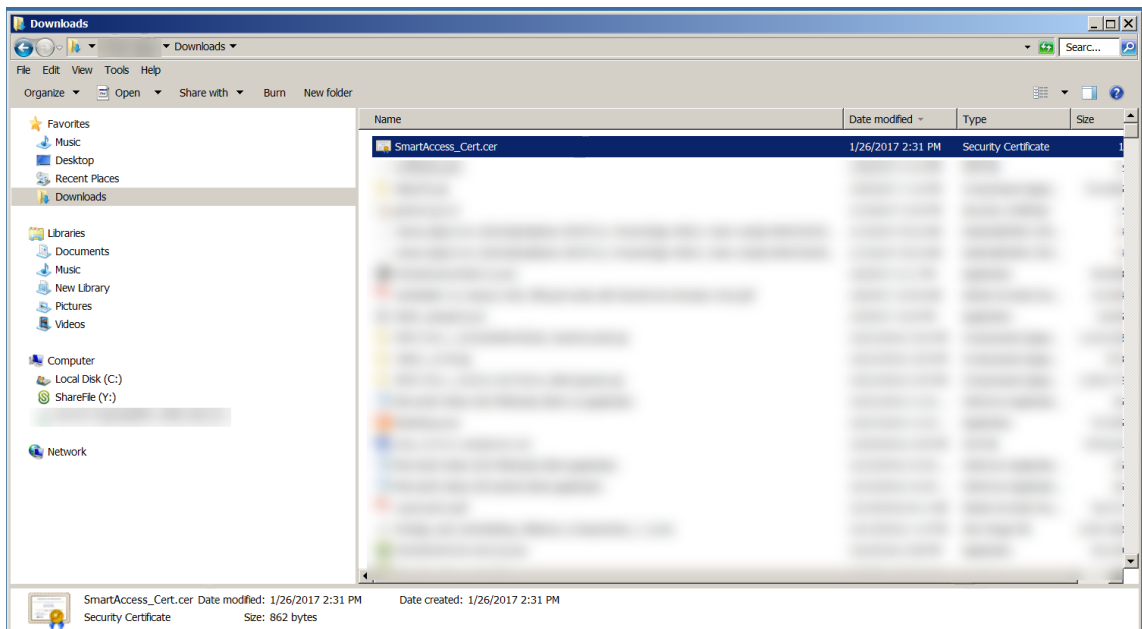
11. 인증서를 찾아 선택하고 다음을 클릭합니다.



12. 선택 내용을 검토하고 마침을 클릭합니다. 확인을 클릭하여 확인 창을 닫습니다.

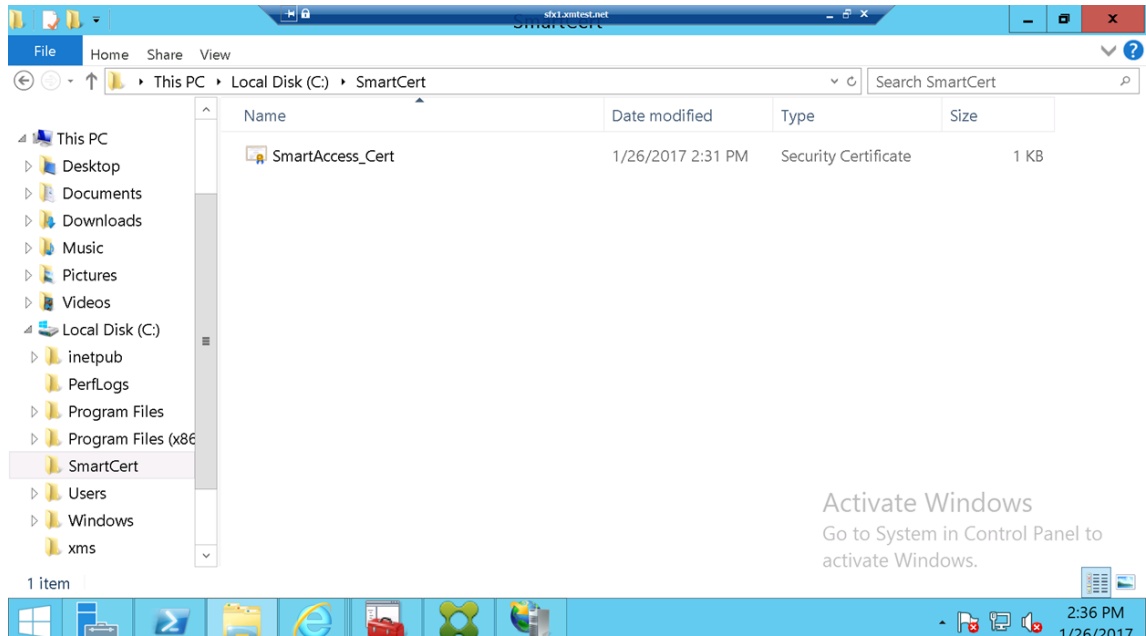


13. 다운로드 디렉터리에서 인증서를 찾습니다. 인증서는 CER 형식입니다.



인증서를 **StoreFront** 서버에 복사합니다

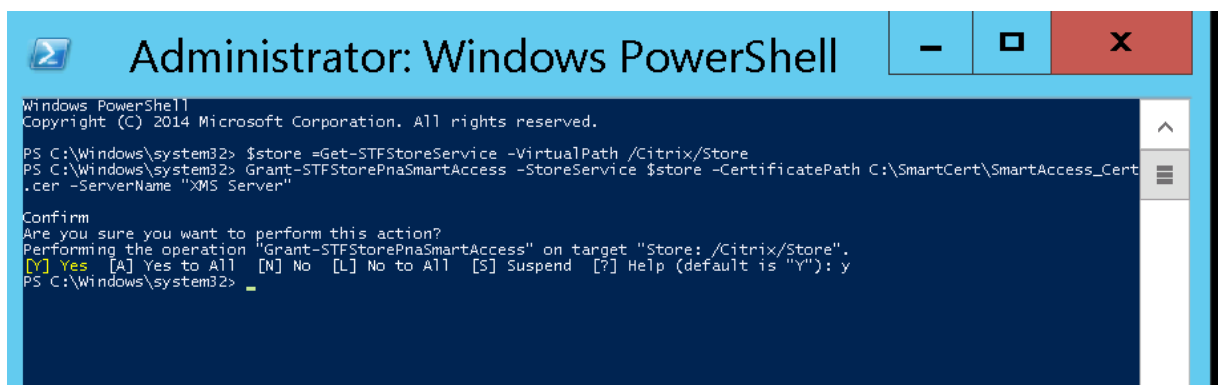
1. StoreFront 서버에서 **SmartCert** 라는 폴더를 만듭니다.
2. 인증서를 **SmartCert** 폴더에 복사합니다.



StoreFront 저장소에서 인증서 구성

StoreFront 서버에서 다음 PowerShell 명령을 실행하여 저장소에서 변환된 XenMobile Server 인증서를 구성합니다.

```
1 Grant-STFStorePnaSmartAccess - StoreService $store -
   CertificatePath "C:\xms\xms.cer" - ServerName "XMS server"
2 <!--NeedCopy-->
```



StoreFront 저장소에 기존 인증서가 있는 경우 다음 PowerShell 명령을 실행하여 인증서를 해지합니다.

```
1 Revoke-STFStorePnaSmartAccess - StoreService $store - All
2 <!--NeedCopy-->
```

```
PS C:\Windows\system32> $store = Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Revoke-STFStorePnaSmartAccess -StoreService $store -All

Confirm
Are you sure you want to perform this action?
Performing the operation "Revoke-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32>
```

또는 다음 PowerShell 명령 중 하나를 StoreFront 서버에서 실행하여 StoreFront 저장소의 기존 인증서를 해지할 수 있습니다.

- 이름으로 해지:

```
1 $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess -StoreService $store - ServerName "
  My XM Server"
4 <!--NeedCopy-->
```

- 지문으로 해지:

```
1 $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess -StoreService $store -
  CertificateThumbprint "ReplaceWithThumbprint"
4 <!--NeedCopy-->
```

- 서버 개체로 해지:

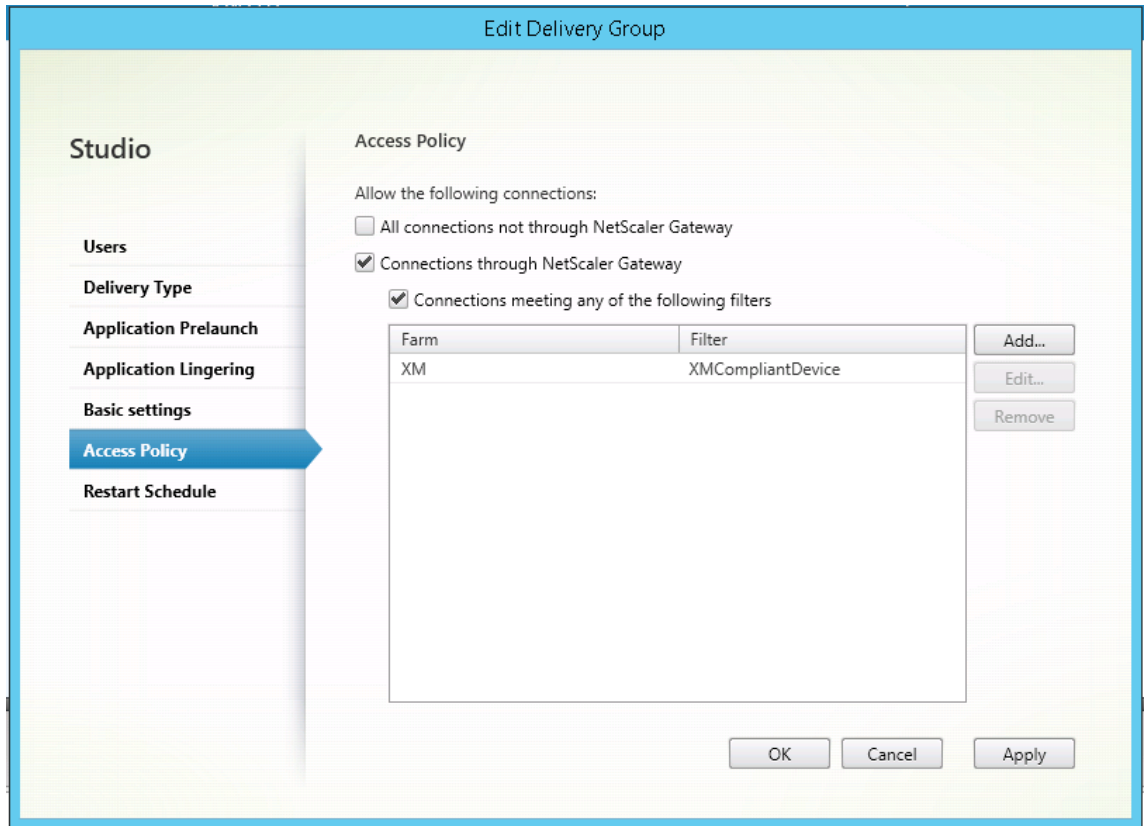
```
1 $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3 $access = Get-STFStorePnaSmartAccess -StoreService $store
4
5 Revoke-STFStorePnaSmartAccess -StoreService $store - SmartAccess
  $access.AccessConditionsTrusts[0]
6 <!--NeedCopy-->
```

Virtual Apps and Desktops 에 대한 SmartAccess 정책 구성

필요한 SmartAccess 정책을 HDX 앱을 전달하는 배달 그룹에 추가하려면:

1. Virtual Apps and Desktops 서버에서 Citrix Studio 를 엽니다.
2. Studio 탐색 창에서 **Delivery Groups**(배달 그룹) 를 선택합니다.
3. 액세스 권한을 제어하려는 하나 이상의 앱을 전달하는 그룹을 선택합니다. **Actions**(동작) 창에서 **Edit Delivery Group**(배달 그룹 편집) 을 선택합니다.
4. **Access Policy**(액세스 정책) 페이지에서 **Connections through NetScaler Gateway**(NetScaler Gateway 를 통한 연결) 및 **Connection meeting any of the following**(다음과 일치하는 연결) 을 선택합니다.

5. 추가를 클릭합니다.
6. **Farm(팜)** 이 **XM** 이고 **Filter(필터)** 가 **XMCompliantDevice** 인 액세스 정책을 추가합니다.



7. **Apply(적용)** 를 클릭하여 모든 변경 내용을 적용하고 창을 열린 채로 두거나, **OK(확인)** 를 클릭하여 변경 내용을 적용하고 창을 닫습니다.

XenMobile 에서 자동화된 동작 설정

HDX 앱에 대한 배달 그룹에 설정된 SmartAccess 정책은 장치가 규정을 위반하면 장치에 대한 액세스를 거부합니다. 장치를 규정 위반으로 표시하는 자동화된 동작을 사용합니다.

Devices									
Devices Show filter									
Add Import Export Refresh									
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Out of Compliance
<input type="checkbox"/>		MDM	MAM	XXXXXXXXXX	iOS	8.1	iPad	06/29/2016 10:37:56 am	212 days
<input type="checkbox"/>		MDM	MAM	XXXXXXXXXX	iOS	10.2	iPhone	01/27/2017 10:10:59 am	0 day
									True

Showing 1 - 2 of 2 items Items per page: 10

1. XenMobile 콘솔에서 구성 > 동작을 클릭합니다. 동작 페이지가 나타납니다.

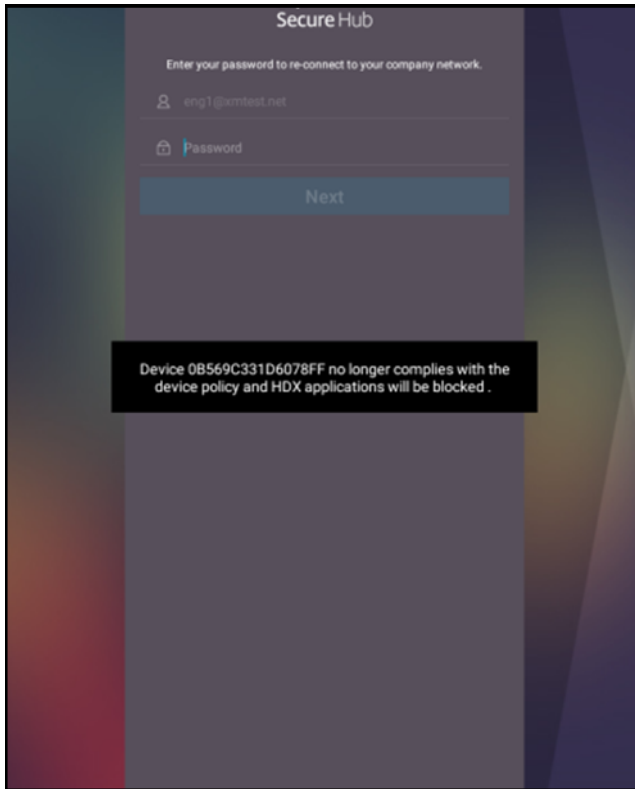
2. 추가를 클릭하여 동작을 추가합니다. 동작 정보 페이지가 나타납니다.
3. 동작 정보 페이지에서 동작의 이름 및 설명을 입력합니다.
4. 다음을 클릭합니다. 동작 세부 정보 페이지가 나타납니다. 다음 예에서는 장치에 사용자 속성 이름 **eng5** 또는 **eng6** 이 있는 경우 즉시 장치를 규정 위반으로 표시하는 트리거를 만듭니다.

5. 트리거 목록에서 장치 속성, 사용자 속성 또는 설치된 앱 이름을 선택합니다. SmartAccess 는 이벤트 트리거를 지원하지 않습니다.
6. 동작 목록에서 다음을 수행합니다.
 - 장치를 규정 위반으로 표시를 선택합니다.
 - **Is** 를 선택합니다.
 - **True** 를 선택합니다.
 - 트리거 조건이 충족되면 즉시 장치를 규정 위반으로 표시하도록 동작을 설정하려면 시간 프레임을 **0** 으로 설정합니다.
7. 이 동작을 적용할 XenMobile 배달 그룹을 하나 이상 선택합니다.
8. 동작 요약을 검토합니다.
9. 다음을 클릭한 후 저장을 클릭합니다.

장치가 규정 위반으로 표시된 경우 Secure Hub 저장소에 더 이상 HDX 앱이 나타나지 않습니다. 사용자는 더 이상 앱을 구독하지 않습니다. 장치에 알림이 전송되지 않으며 Secure Hub 저장소에 HDX 응용 프로그램이 이전에 사용 가능했다는 내용이 표시되지 않습니다.

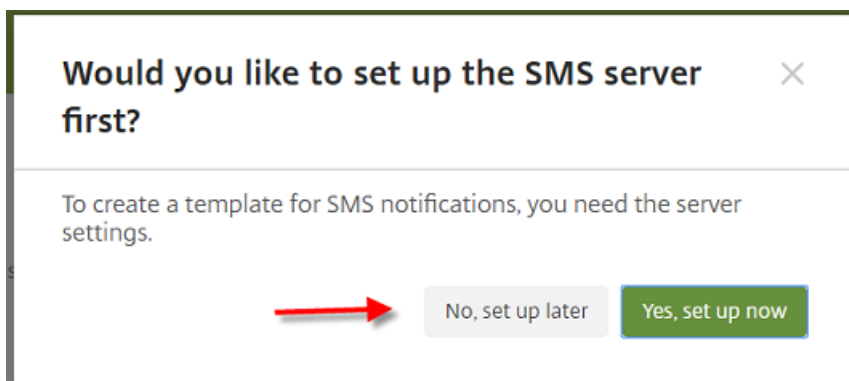
장치가 규정 위반으로 표시될 때 사용자에게 알려려면 알림을 만든 다음 해당 알림을 보내는 자동화된 동작을 만듭니다.

이 예에서는 다음과 같은 알림을 만들고 장치가 규정 위반으로 표시되는 경우 알림을 보냅니다. “Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked.(장치 일련 번호 또는 전화 번호가 더 이상 장치 정책을 준수하지 않으므로 HDX 응용 프로그램이 차단됩니다.)”



장치가 규정 위반으로 표시될 때 사용자에게 표시되는 알림 만들기

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 알림 템플릿을 클릭합니다. 알림 템플릿 페이지가 나타납니다.
3. 추가를 클릭하여 알림 템플릿 페이지에 추가합니다.
4. SMS 서버를 먼저 설정하라는 메시지가 나타나면 아니요, 나중에 설정합니다를 클릭합니다.



5. 다음 설정을 구성합니다.

- 이름: HDX Application Block
- 설명: Agent notification when device is out of compliance

- 유형: 임시 알림
- **Secure Hub:** 활성화됨
- 메시지: Device \${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

Name*	HDX Application Block
Description	
Type	Ad-Hoc Notification Manual sending supported
SMTP	Activate
Sender	
Recipient	
Subject	
Message	
Secure Hub	Activated Deactivate
Message*	Device S{firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked .

6. 저장을 클릭합니다.

장치가 규정 위반으로 표시되면 알림을 보내는 동작 만들기

1. XenMobile 콘솔에서 구성 > 동작을 클릭합니다. 동작 페이지가 나타납니다.

2. 추가를 클릭하여 동작을 추가합니다. 동작 정보 페이지가 나타납니다.

3. 동작 정보 페이지에서 동작의 이름 및 설명을 입력합니다.

- 이름: HDX 차단 알림
- 설명: 장치가 규정을 위반할 경우 HDX 차단 알림

4. 다음을 클릭합니다. 동작 세부 정보 페이지가 나타납니다.

5. 트리거 목록에서 다음을 수행합니다.

- 장치 속성을 선택합니다.
- 규정 위반을 선택합니다.
- **Is** 를 선택합니다.
- **True** 를 선택합니다.

6. 동작 목록에서 트리거 조건이 충족될 때 실행할 동작을 지정합니다.

- 알림 보내기를 선택합니다.
- 앞서 만든 **HDX Application Block** 알림을 선택합니다.
- **0** 을 선택합니다. 이 값을 0 으로 설정하면 트리거 조건이 충족되는 즉시 알림이 전송됩니다.

7. 이 동작을 적용할 XenMobile 배달 그룹을 하나 이상 선택합니다. 이 예제에서는 **AllUsers** 를 선택합니다.

8. 동작 요약을 검토합니다.

9. 다음을 클릭한 후 저장을 클릭합니다.

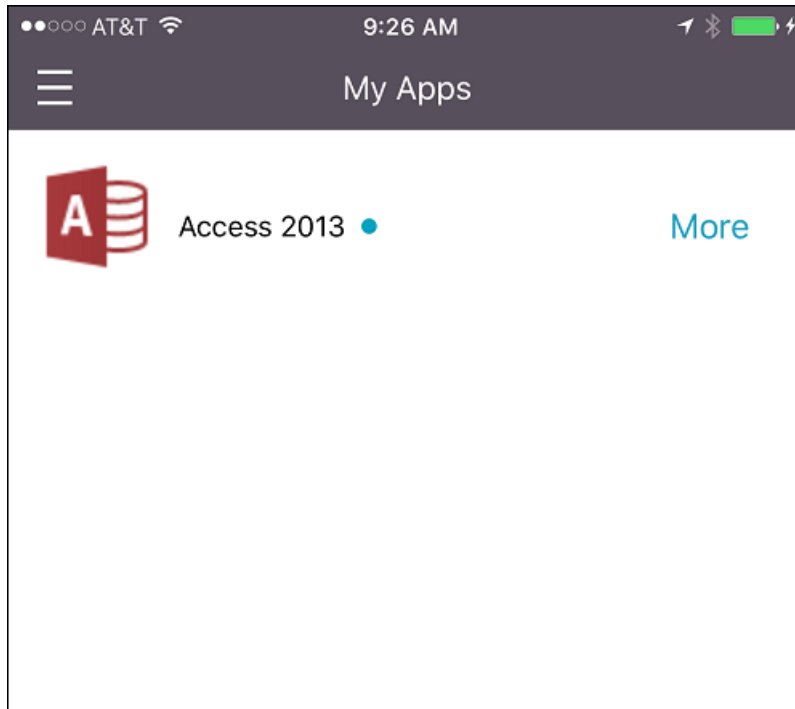
자동화된 동작을 설정하는 것에 대한 자세한 내용은 [자동화된 동작](#)을 참조하십시오.

사용자가 **HDX** 앱에 대한 액세스 권한을 복구하는 방법

장치가 다시 규정을 준수하게 되면 HDX 앱에 액세스할 수 있게 됩니다.

1. 장치에서 **Secure Hub** 저장소로 이동하여 저장소의 앱을 새로 고칩니다.
2. 앱으로 이동하고 앱에 대한 추가를 누릅니다.

앱이 추가되면 내 앱에 나타나며 새로 설치된 앱이기 때문에 옆에 파란색 점이 있습니다.



미디어 추가

March 19, 2021

XenMobile 에 미디어를 추가하여 사용자 장치에 미디어를 배포합니다. XenMobile 을 사용하여 Apple 볼륨 구매를 통해 취득한 Apple Book 을 배포할 수 있습니다.

XenMobile 에서 볼륨 구매 계정을 구성하면 구성 > 미디어에 구입한 서적 및 무료 서적이 나타납니다. 미디어 페이지에서 배달 그룹을 선택하고 배포 규칙을 지정하여 iOS 장치에 배포할 서적을 구성합니다.

사용자가 처음으로 서적을 수신하고 볼륨 구매 라이선스를 수락하면 배포된 서적이 장치에 설치됩니다. 서적은 Apple Book 앱에 표시됩니다. 관리자는 사용자에게서 서적 라이선스를 분리하거나 장치에서 서적을 제거할 수 없습니다. XenMobile 은 서적을 필수 미디어로 설치합니다. 사용자가 장치에서 설치된 서적을 삭제하는 경우 서적은 Apple Book 앱에 유지되며 바로 다운로드할 수 있습니다.







사전 요구 사항

- iOS 장치

- [Apple 볼륨 구매](#)에 설명된 대로 XenMobile 에서 Apple 볼륨 구매를 구성합니다.

서적 구성

볼륨 구매를 통해 취득한 Apple Book 은 구성 > 미디어 페이지에 표시됩니다.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
Media Show filter						
<input type="text" value="Search"/>						
<input type="checkbox"/>	Icon	Media Name	Type	Created On	Last Updated	Vpp Account
<input type="checkbox"/>		The Wonderful Wizard of Oz - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:41 PM	test
<input type="checkbox"/>		Cool Werewolf Jokes For Kids - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:28 PM	test
<input type="checkbox"/>		Science Fiction Stories - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:32 PM	test
<input type="checkbox"/>		Coming Out - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:45 AM	test
<input type="checkbox"/>		Short Stories - VPP	Apple iBooks	6/15/17 1:29 PM	6/15/17 1:29 PM	test
<input type="checkbox"/>		A Diamond in My Pocket - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:39 AM	test
Showing 1 - 6 of 6 items Items per page: <input type="text" value="10"/>						

배포할 Apple Book 구성

1. 구성 > 미디어에서 서적을 선택하고 편집을 클릭합니다. 서적 정보 페이지가 나타납니다.

iBook	Book Information
1 Book Information	<div> <div>Name *</div> <input type="text" value="Cool Werewolf Jokes For Kids - VPP"/> </div> <div> <div>Description</div> <input type="text" value="Cool Werewolf Jokes For Kids - VPP"/> </div>
2 Platform	
iPhone	
iPad	
3 Delivery Group Assignments (optional)	

이름 및 설명은 XenMobile 콘솔과 로그에만 표시됩니다.

2. **iPhone iBook** 설정 및 **iPad iBook** 설정 페이지에서: 필요한 경우 서적 이름과 설명을 변경할 수 있지만 Citrix 에서는 이러한 설정을 변경하지 않기를 권장합니다. 이미지는 정보를 위한 것이며 편집할 수 없습니다. 유료 **iBook** 은 Apple 볼륨 구매를 통해 구매한 서적을 나타냅니다.

iBook

1 Book Information

2 Platform

iPhone

iPad

3 Delivery Group Assignments (optional)

iPhone iBook Settings

Type a book title or keyword in the field and search for your desired iBook. Once you choose the iBook in the results, you can configure how the iBook appears in the store.

iBook Details

Name*

Cool Werewolf Jokes For Kids

Description*

Cool Werewolf Jokes For Kids - VPP

Image

Paid iBook

ON

Deployment Rules

Volume Purchase Program

배포 규칙을 지정하거나 볼륨 구매 정보를 볼 수도 있습니다.

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

iBook

1 Book Information

2 Platform

iPhone

iPad

3 Delivery Group Assignments (optional)

Paid iBook

ON

Deployment Rules

Volume purchase

Volume purchase License

Use Volume purchase company token

Volume purchase Account

test

Volume purchase ID Assignment

License Usage: 6 of 10

	License ID	Usage Status	Associated User
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	

Showing 1 - 6 of 6 items

3. 필요한 경우 서적을 배달 그룹에 할당하고 배포 일정을 설정합니다.

iBook

1 Book Information

2 Platform

iPhone

iPad

3 Delivery Group Assignments (optional)

Delivery Group Assignments (optional)

Assign this book to one or more delivery groups.

Choose delivery groups

Type to search

Search

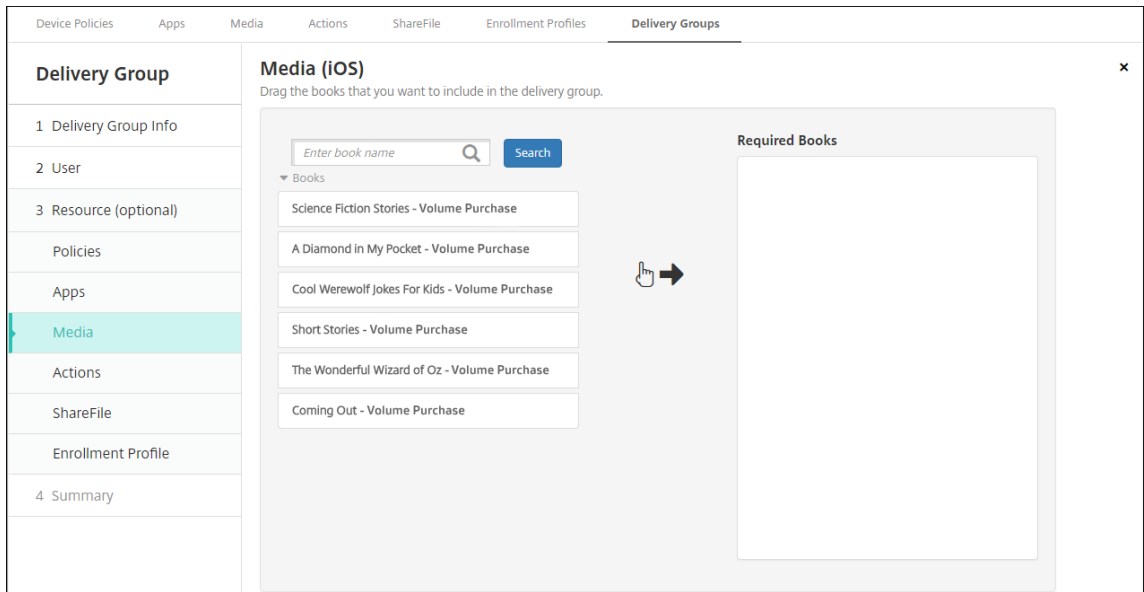
☐ AllUsers

☐ test

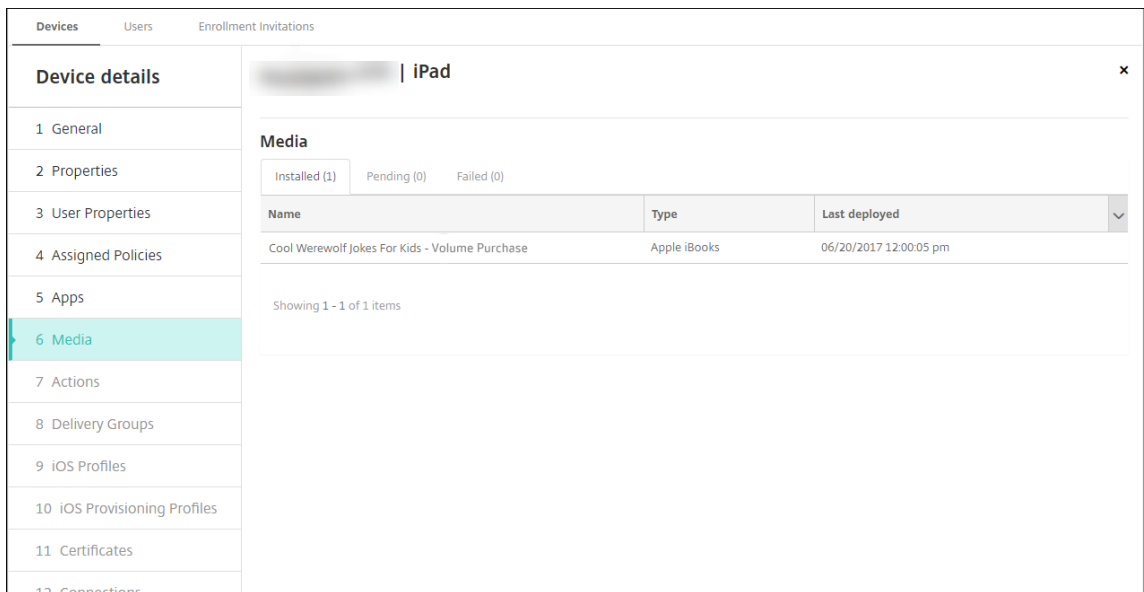
☐ as_grp_citrixw

Deployment Schedule ⓘ

또한 구성 > 배달 그룹의 미디어 탭에서 배달 그룹에 서적을 할당할 수도 있습니다. XenMobile 은 필수 서적 배포만 지원합니다.



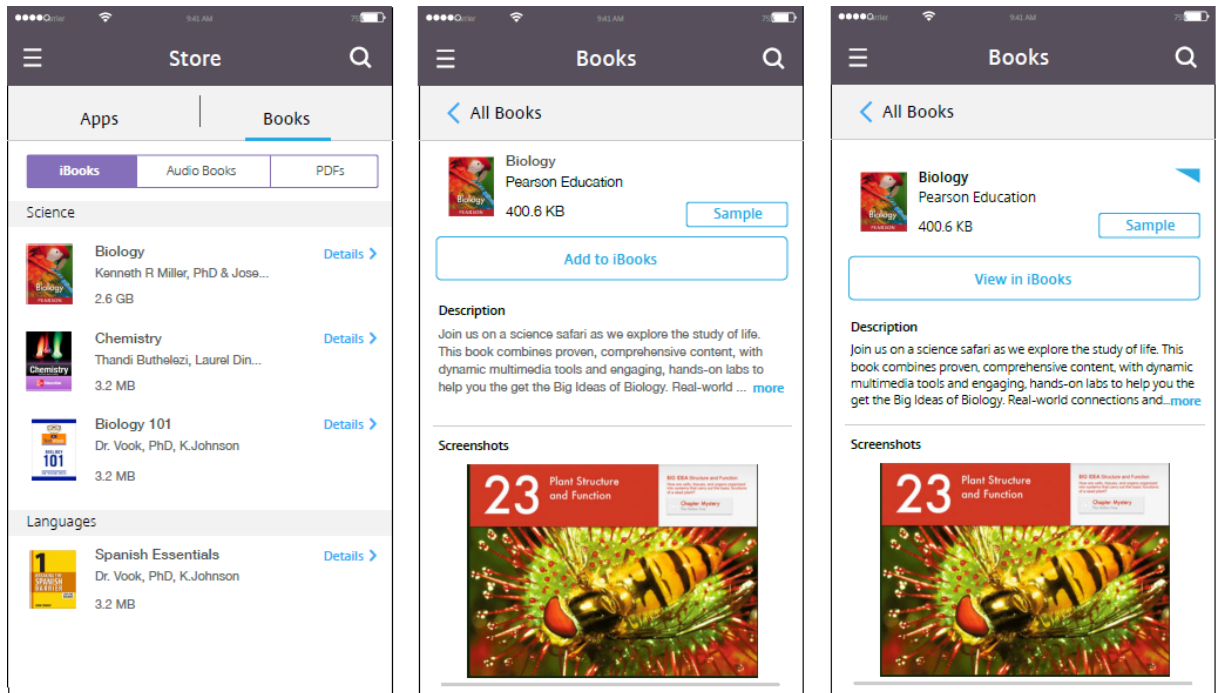
4. 배포 상태를 보려면 관리 > 장치의 미디어 탭을 사용합니다.



참고:

구성 > 미디어 페이지에서 서적을 선택하고 삭제를 클릭하면 XenMobile 이 목록에서 해당 서적을 제거합니다. 그러나 Apple 볼륨 구매에서 서적을 제거하지 않은 경우 XenMobile 이 다음에 Apple 볼륨 구매와 동기화되면 해당 서적이 목록에 다시 표시됩니다. 목록에서 서적을 제거해도 장치에서 서적이 삭제되지는 않습니다.

서적은 다음 예에 표시된 것과 같이 사용자 장치에 표시됩니다.



리소스 배포

March 15, 2024

장치 구성 및 관리에는 일반적으로 XenMobile 콘솔에서 리소스 (정책, 앱 및 미디어) 및 동작을 만들고 배달 그룹을 사용하여 패키징하는 단계가 포함됩니다. XenMobile 이 배달 그룹의 리소스 및 동작을 장치로 푸시하는 순서를 배포 순서라고 합니다. 이 문서에서 설명하는 내용:

- 배달 그룹 추가, 관리 및 배포
- 배달 그룹에서 리소스 및 작업의 배포 순서 변경
- XenMobile 은 사용자가 중복 또는 충돌하는 정책이 있는 여러 배달 그룹에 속한 경우에 배포 순서를 결정합니다.

배달 그룹은 정책, 앱, 미디어 및 동작 조합을 배포하는 대상 장치의 사용자 범주를 지정합니다. 일반적으로 회사, 국가, 부서, 사무실 주소, 직함과 같은 사용자의 특성에 따라 특정 배달 그룹에 사용자를 포함시킵니다. 배달 그룹을 통해 누가 어떤 리소스를 어떤 경우에 이용할 수 있는지를 보다 효과적으로 제어할 수 있습니다. 배달 그룹은 모든 사용자에게 배포하거나 좀더 구체적으로 정의된 그룹의 사용자에게 배포할 수 있습니다.

배달 그룹에 배포한다는 것은 지원되는 iOS 및 Windows 장치의 모든 사용자에게 푸시 알림을 보내는 것을 의미합니다. 이러한 사용자는 배달 그룹에 속해 있어야 XenMobile 에 다시 연결됩니다. 장치를 재평가하고 배달 그룹에 포함되는 정책, 앱, 미디어 및 동작을 배포할 수 있습니다.

Android 장치 사용자: 이미 연결된 경우 즉시 리소스를 받습니다. 그렇지 않은 경우에는 예약 정책에 기반하여 다음에 연결할 때 리소스를 받습니다.

XenMobile 을 설치하고 구성하면 기본 AllUsers 배달 그룹이 만들어집니다. 여기에는 모든 로컬 사용자와 Active Directory 사용자가 포함되어 있습니다. AllUsers 그룹은 삭제할 수 없지만 일부 사용자에게 리소스를 푸시하지 않으려는 경우 이 그룹을 사용하지 않도록 설정할 수 있습니다.

배포 순서

배포 순서는 XenMobile 이 장치에 리소스를 푸시하는 순서입니다. 배포 순서는 MDM(장치 관리)에 대해 구성된 등록 프로필이 있는 배달 그룹의 장치에만 적용됩니다.

배포 순서를 결정할 때 XenMobile 은 리소스에 배포 규칙 및 배포 일정과 같은 필터와 제어 조건을 적용합니다. 리소스에는 정책, 앱, 동작 및 배달 그룹이 포함됩니다. 배달 그룹을 추가하기 전에 배포 목표를 고려하여 이 섹션의 내용을 검토하십시오.

배포 순서와 관련된 주요 개념을 요약하면 다음과 같습니다.

- **배포 순서:** XenMobile 이 장치에 리소스 (정책, 앱 및 미디어) 및 동작을 푸시하는 순서입니다. 약관 및 소프트웨어 인벤토리와 같은 일부 정책의 배포 순서는 다른 리소스에 영향을 주지 않습니다. 작업이 배포되는 순서는 다른 리소스에 영향을 주지 않습니다. 따라서 XenMobile 에서 리소스를 배포할 때 해당 위치는 무시됩니다.
- **배포 규칙:** XenMobile 은 장치 속성에 지정된 배포 규칙을 사용하여 정책, 앱, 미디어, 동작 및 배달 그룹을 필터링합니다. 예를 들어, 도메인 이름이 특정 값과 일치하는 경우 배포 패키지를 푸시하도록 배포 규칙을 지정할 수 있습니다.
- **배포 일정:** XenMobile 은 정책, 앱, 미디어 및 동작에 지정된 배포 일정을 사용하여 해당 항목의 배포를 제어합니다. 배포가 특정 날짜 및 시간에 즉시 이루어지거나 배포 조건에 따라 이루어지도록 지정할 수 있습니다.

다음 표에는 다양한 개체 및 리소스 유형에 대한 필터 및 제어 기준이 나와 있습니다. 배포 규칙은 장치 속성에 기반합니다.

개체/리소스	장치 플랫폼	배포 규칙	배포 일정	사용자/그룹
장치 정책	예	예	예	-
앱	예	예	예	-
미디어	예	예	예	-
동작	-	예	예	-
배달 그룹	-	예	-	예

일반적인 환경에서는 단일 사용자에게 여러 배달 그룹이 할당되어 다음과 같은 결과가 나타날 가능성이 큼니다.

- 배달 그룹 내에서 중복된 개체가 존재합니다.
- 사용자에게 할당된 여러 배달 그룹에서 특정 정책이 서로 다르게 구성됩니다.

이러한 상황이 발생할 경우 XenMobile 은 특정 장치에 배달하거나 관련 작업을 수행해야 하는 모든 개체의 배포 순서를 계산합니다. 계산 단계는 장치 플랫폼에 독립적입니다.

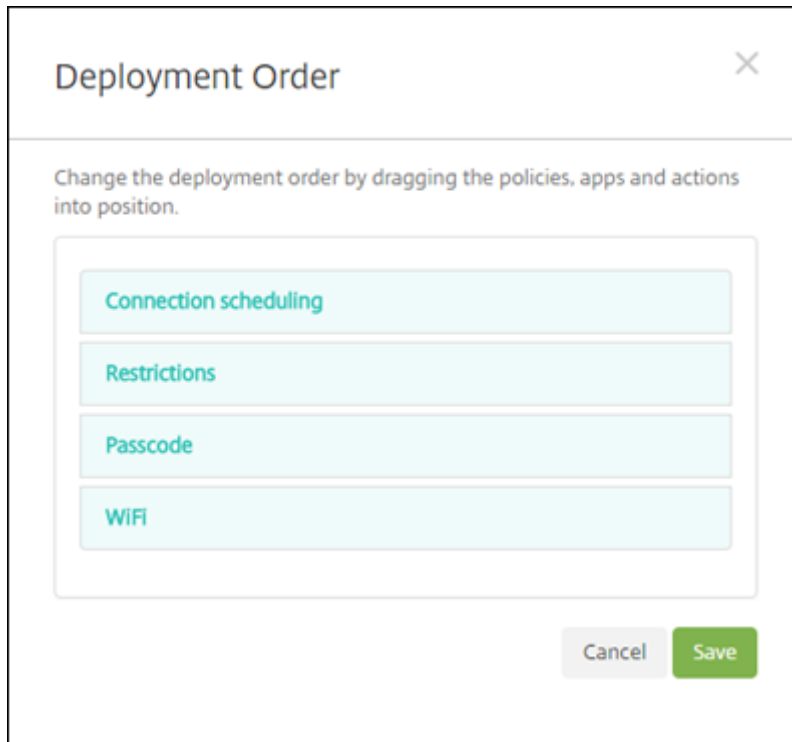
계산 단계

1. 사용자, 그룹 및 배포 규칙의 필터에 기반하여 특정 사용자의 모든 배달 그룹을 결정합니다.
2. 선택된 배달 그룹 내의 모든 리소스 (정책, 앱, 미디어 및 동작) 의 순서 지정된 목록을 만듭니다. 목록은 장치 플랫폼, 배포 규칙 및 배포 일정의 필터를 기반으로 합니다. 순서 지정 알고리즘은 다음과 같습니다.
 - a) 사용자 정의 배포 순서가 있는 배달 그룹의 리소스를 사용자 정의 배포 순서가 없는 배달 그룹의 리소스보다 먼저 배치합니다. 이렇게 배치하는 이유는 이러한 단계 다음에 설명되어 있습니다.
 - b) 배달 그룹 간에 순서가 동일한 경우에는 배달 그룹 이름에 따라 배달 그룹 리소스 순서를 지정합니다. 예를 들어, 배달 그룹 A 의 리소스를 배달 그룹 B 의 리소스보다 먼저 배치합니다.
 - c) 정렬할 때는 배달 그룹 리소스에 사용자 정의 배포 순서가 지정된 경우 해당 순서를 유지합니다. 그렇지 않은 경우 리소스 이름으로 배달 그룹 내 리소스를 정렬합니다.
 - d) 동일한 리소스가 두 번 이상 나타나는 경우 중복된 리소스를 제거합니다.

사용자 정의 순서가 있는 리소스는 사용자 정의 순서가 없는 리소스보다 먼저 배포됩니다. 하나의 리소스가 사용자에게 할당된 여러 배달 그룹에 존재할 수 있습니다. 위의 단계에 나온 것처럼 계산 알고리즘은 중복된 리소스를 제거하고 이 목록에 있는 첫 번째 리소스만 제공합니다. 이러한 방식으로 중복된 리소스를 제거함으로써 XenMobile 은 XenMobile 관리자가 정의한 순서를 적용합니다.

예를 들어, 다음과 같은 두 개의 배달 그룹이 있는 경우를 살펴보겠습니다.

- 배달 그룹, 계정 관리자 1: 리소스 순서가 지정되지 않습니다. 정책 **WiFi** 및 암호를 포함합니다.
- 배달 그룹, 계정 관리자 2: 리소스 순서가 지정됩니다. 정책 연결 예약, 제한, 암호, **WiFi** 를 포함합니다. 이 상태에서 암호 정책을 **WiFi** 정책보다 먼저 배포하려고 합니다.



계산 알고리즘이 이름으로만 배포 그룹 순서를 지정한 경우 XenMobile 은 배포 그룹 계정 관리자 1 부터 시작하여 **WiFi**, 암호, 연결 예약, 제한 순서로 배포를 수행합니다. 계정 관리자 2 배포 그룹의 암호 및 **WiFi** 두 가지는 중복되므로 무시됩니다.

하지만 계정 관리자 2 그룹에는 관리자가 지정한 배포 순서가 있습니다. 따라서 계산 알고리즘은 계정 관리자 2 배포 그룹의 리소스를 다른 배포 그룹의 리소스보다 높은 순서로 목록에 배치합니다. 따라서 XenMobile 은 연결 예약, 제한, 암호, **WiFi** 순서로 정책을 배포합니다. 계정 관리자 1 배포 그룹의 **WiFi** 및 암호 정책은 중복되므로 무시됩니다. 이처럼 계산 알고리즘은 XenMobile 관리자가 지정한 순서를 따릅니다.

배포 규칙

특정 조건이 있는 경우에만 리소스를 제공하도록 배포 규칙을 구성합니다. 기본 또는 고급 배포 규칙을 구성할 수 있습니다.

기본 편집기를 사용하여 배포 규칙을 추가할 때는 먼저 리소스를 배포할 시기를 선택합니다.

Deployment Rules

Base

Advanced

Deploy when

All

conditions are met.

New Rule

Deploy this resource rega...

only

shareable

Installed app name

is equal to

Secure Hub

Passcode compliant

True

Manage cellular roaming

domestic

- 모두: 사용자 또는 장치가 구성한 모든 조건을 충족하면 리소스를 전달합니다.
- 모두: 사용자 또는 장치가 구성한 조건 중 하나 이상을 충족하는 경우 리소스를 제공합니다.

새 규칙을 클릭하여 조건을 추가합니다. 규칙은 배포 중인 리소스와 리소스를 구성하는 플랫폼에 따라 다릅니다. 몇 가지 유형의 규칙이 있습니다. 다음 경우에 리소스를 배포하도록 선택할 수 있습니다.

- 선택한 속성이 존재하는 경우만 또는 선택한 속성이 존재하는 경우 제외
- 속성이 정확히 입력한 텍스트와 일치할 경우 속성에 입력한 텍스트가 포함되거나 속성이 입력한 텍스트와 일치하지 않습니다.
- 장치 또는 사용자가 선택한 속성을 준수하거나 선택한 속성을 준수하지 않는 경우
- 장치 또는 사용자 속성이 미리 정의된 목록에서 선택한 조건과 일치하는 경우

고급 편집기를 사용하여 보다 복잡한 배포 규칙을 만들 수 있습니다. 더 많은 규칙을 선택할 수 있으며 고급 규칙을 만들 때 서로 다른 부울 논리 연산자를 결합할 수 있습니다.

▼ Deployment Rules

Base Advanced

AND

- Passcode compliant True
- OR
- Installed app name contains Authenticator
- NOT
- Device ownership Unknown

AND OR NOT EDIT New Rule Delete

배달 그룹을 추가하려면

Citrix에서는 장치 정책과 등록 프로필을 만들기 전에 배달 그룹을 만들 것을 권장합니다.

1. 콘솔에서 구성 > 배달 그룹을 클릭합니다.
2. 배달 그룹 페이지에서 추가를 클릭합니다.
3. 배달 그룹 정보 페이지에서 배달 그룹의 이름과 설명을 입력하고 다음을 클릭합니다.

사용자가 등록 프로필이 다른 여러 배달 그룹에 속하는 경우 사용되는 등록 프로필은 배달 그룹의 이름에 따라 결정됩니다.

XenMobile은 사전순으로 표시된 배달 그룹 목록의 마지막에 나타나는 배달 그룹을 선택합니다. 자세한 내용은 [등록 프로필](#)을 참조하십시오.

4. 사용자 할당 페이지에서 배달 그룹 사용자 할당 관리 방식을 지정합니다.

중요:

사용자 그룹이 만들어진 후에는 사용자 할당 관리 설정을 변경할 수 없습니다.

- **도메인 선택:** 목록에서 사용자를 선택할 도메인을 선택합니다.
- **사용자 그룹 포함:** 다음 중 하나를 수행합니다.
 - 사용자 그룹 목록에서 추가하려는 그룹을 클릭합니다. 선택한 그룹이 선택된 사용자 그룹 목록에 나타납니다.
 - 검색을 클릭하여 선택된 도메인의 모든 사용자 그룹 목록을 봅니다.
 - 검색 상자에 전체 또는 일부 그룹 이름을 입력한 다음 검색을 클릭하여 사용자 그룹의 목록을 제한합니다.

선택된 사용자 그룹 목록에서 사용자 그룹을 제거하려면 다음 중 하나를 수행합니다.

- 선택된 사용자 그룹 목록에서 제거할 각 그룹 옆에 있는 **X**를 클릭합니다.
- 검색을 클릭하여 선택된 도메인의 모든 사용자 그룹 목록을 봅니다. 목록을 스크롤하면서 제거할 각 그룹의 확인란을 선택 취소합니다.
- 검색 상자에 전체 또는 일부 그룹 이름을 입력한 다음 검색을 클릭하여 사용자 그룹의 목록을 제한합니다. 목록을 스크롤하면서 제거할 각 그룹의 확인란을 선택 취소합니다.
- **또는/및:** 리소스를 배포하기 위해 사용자가 임의의 그룹에 있을 수 있는지 (또는), 아니면 모든 그룹에 있어야 하는지 (및)를 선택합니다.
- **익명 사용자에게 배포:** 배달 그룹의 인증되지 않은 사용자에게 배포할 것인지 여부를 선택합니다. 인증되지 않은 사용자는 인증하지 못했지만 XenMobile에 장치를 연결할 수 있도록 허용한 사용자입니다.

5. 배포 규칙을 구성합니다.

6. 다음을 클릭합니다. 배달 그룹 리소스 페이지가 나타납니다. 필요한 경우 배달 그룹에 대한 정책, 앱 또는 동작을 추가할 수도 있습니다. 이 단계를 건너뛰려면 배달 그룹 아래에서 요약을 클릭하여 배달 그룹 구성의 요약을 봅니다.

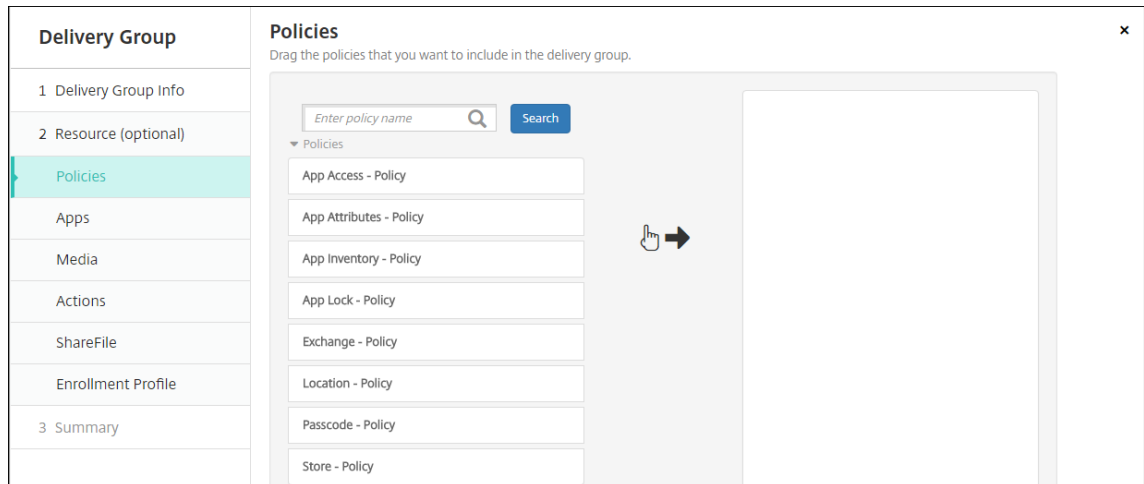
리소스를 건너뛰려면 리소스 (선택 사항) 아래에서 추가할 리소스를 클릭하고 해당 리소스에 대한 단계를 수행합니다.

정책을 추가하려면

1. 추가하려는 각 정책에 대해 다음을 수행합니다.

- 사용 가능한 정책 목록을 스크롤하면서 추가할 정책을 찾습니다.
- 또는 검색 상자에 전체 또는 일부 정책 이름을 입력한 다음 검색을 클릭하여 정책 목록을 제한합니다.
- 추가할 정책을 클릭하고 오른쪽의 상자로 끌어옵니다.

정책을 제거하려면 오른쪽 상자에서 정책 이름 옆에 있는 **X**를 클릭합니다.



2. 다음을 클릭합니다. 앱 페이지가 나타납니다.

앱을 추가하려면

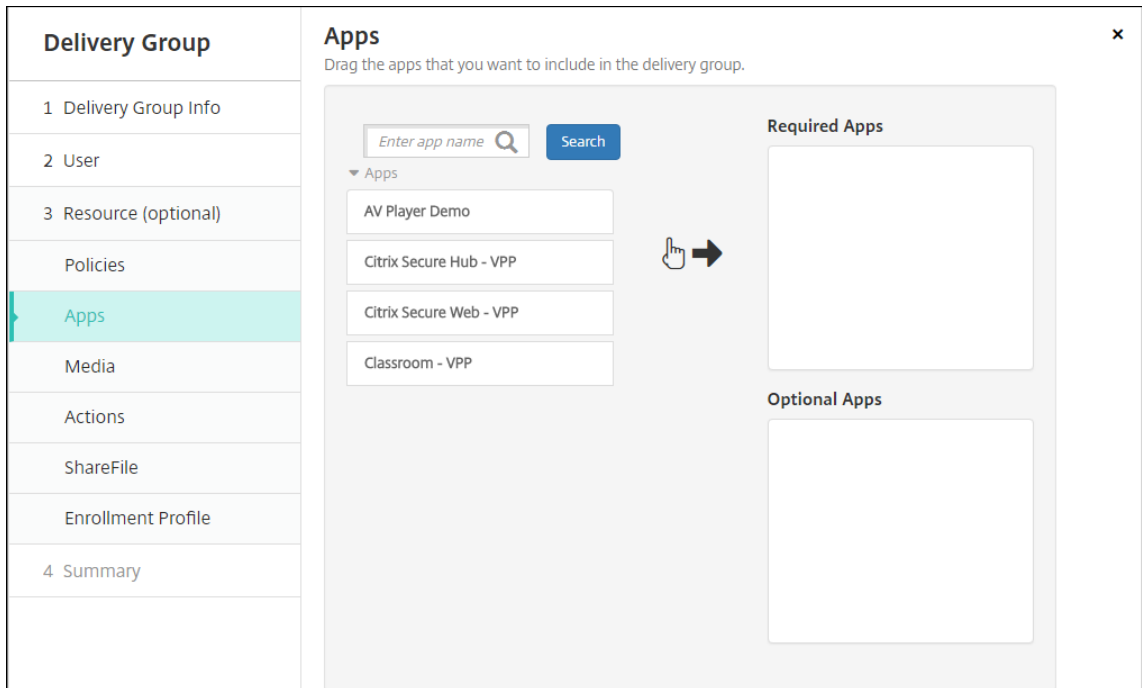
1. 추가하려는 각 앱에 대해 다음을 수행합니다.

- 사용 가능한 앱 목록을 스크롤하면서 추가할 앱을 찾습니다.
- 검색 상자에 전체 또는 일부 앱 이름을 입력한 다음 검색을 클릭하여 앱 목록을 제한합니다.
- 추가할 앱을 클릭하고 필수 앱 상자 또는 선택적 앱 상자로 끕니다.

필수로 표시된 앱의 경우 사용자는 다음과 같은 경우에 곧바로 업데이트를 받을 수 있습니다.

- 사용자가 새 앱을 업로드하고 필수 앱으로 표시합니다.
- 사용자가 기존 앱을 필수 앱으로 표시합니다.
- 사용자가 필수 앱을 삭제합니다.
- Secure Hub 업데이트가 제공됩니다.

기능을 사용하도록 설정하는 방법을 포함하여 필수 앱의 강제 배포에 대한 자세한 내용은 [필수 앱과 선택적 앱 정보](#)를 참조하십시오.



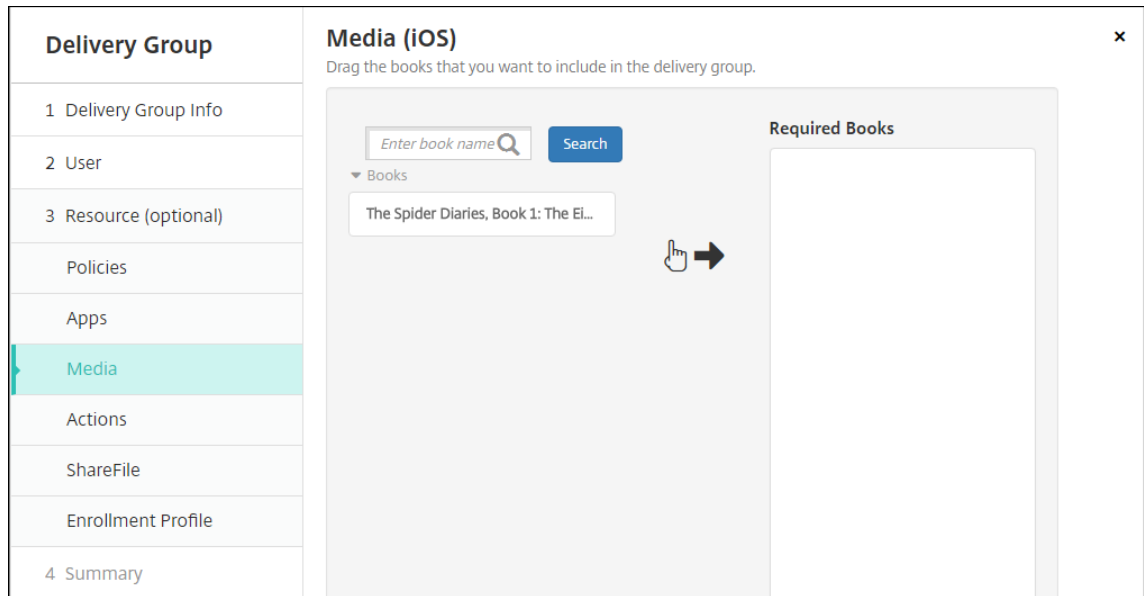
앱을 제거하려면 오른쪽 상자에서 앱 이름 옆에 있는 **X**를 클릭합니다.

2. 다음을 클릭합니다. 미디어 페이지가 나타납니다.

미디어를 추가하려면

1. 추가할 각 서적에 대해 다음을 수행합니다.

- 사용 가능한 서적 목록을 스크롤하면서 추가할 서적을 찾습니다.
- 검색 상자에 전체 또는 일부 서적 이름을 입력한 다음 검색을 클릭하여 서적 목록을 제한합니다.
- 추가할 서적을 클릭하고 필수 서적 상자로 끌어옵니다.



필수로 표시된 서적의 경우 사용자는 다음과 같은 경우에 곧바로 업데이트를 받습니다.

- 새 서적을 업로드하고 필수 앱으로 표시합니다.
- 기존 서적을 필수 서적으로 표시합니다.
- 사용자가 필수 서적을 삭제합니다.
- Secure Hub 업데이트가 제공됩니다.

서적을 제거하려면 오른쪽 상자에서 서적 이름 옆에 있는 **X**를 클릭합니다.

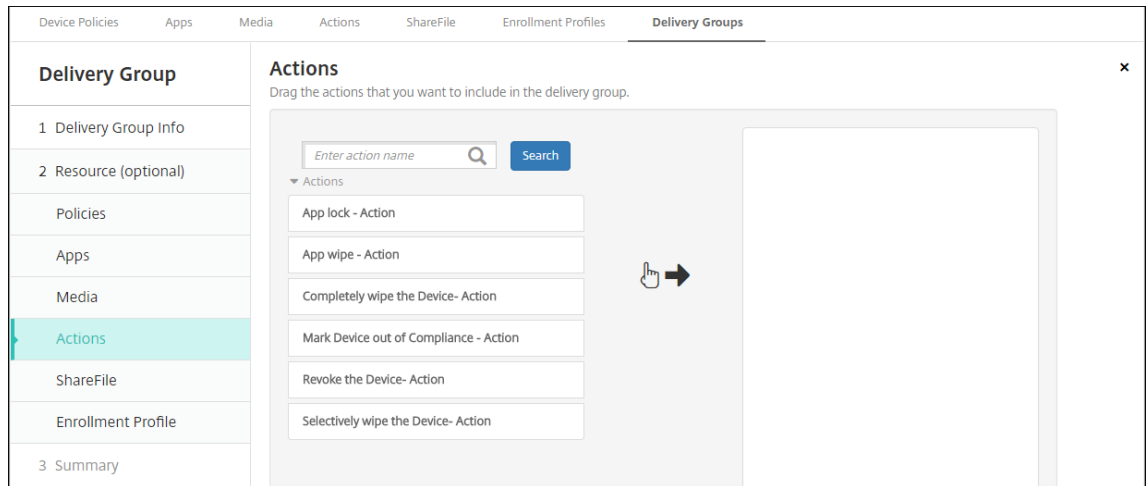
2. 다음을 클릭합니다. 동작 페이지가 나타납니다.

동작을 추가하려면

1. 추가할 각 동작에 대해 다음을 수행합니다.

- 사용 가능한 동작 목록을 스크롤하면서 추가할 동작을 찾습니다.
- 검색 상자에 전체 또는 일부 동작 이름을 입력한 다음 검색을 클릭하여 동작 목록을 제한합니다.
- 추가할 동작을 클릭하고 오른쪽 상자로 끌어옵니다.

동작을 제거하려면 오른쪽 상자에서 동작 이름 옆에 있는 **X**를 클릭합니다.

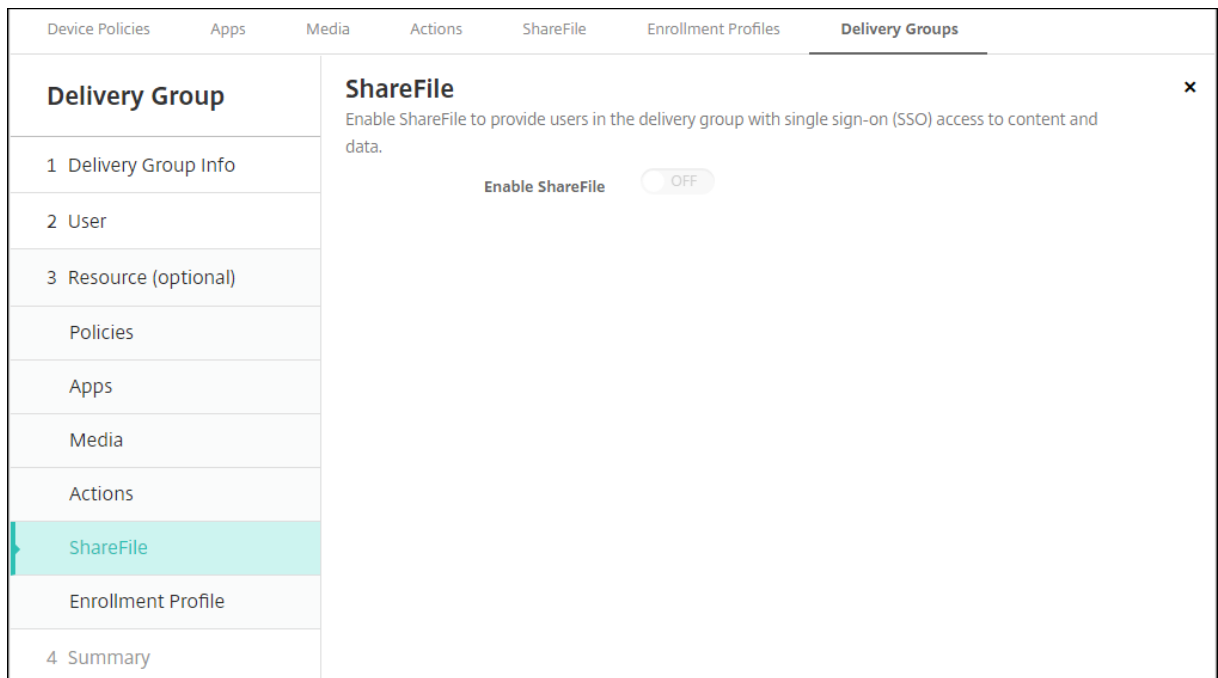


2. 다음을 클릭합니다. **ShareFile** 페이지가 나타납니다.

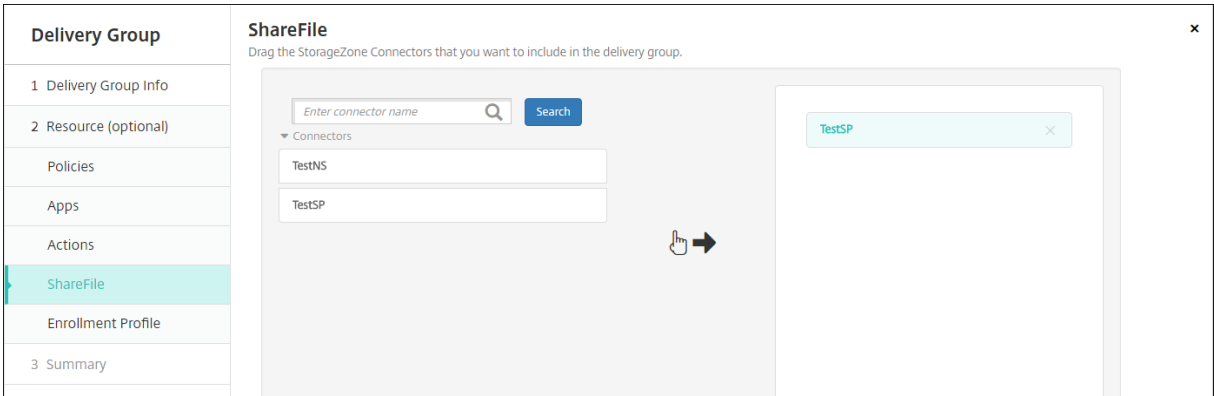
ShareFile 구성을 적용하려면

ShareFile 페이지는 XenMobile(구성 > **ShareFile**)에 Enterprise 계정을 사용하도록 구성했는지, 아니면 StorageZone 커넥터를 사용하도록 구성했는지에 따라 달라집니다.

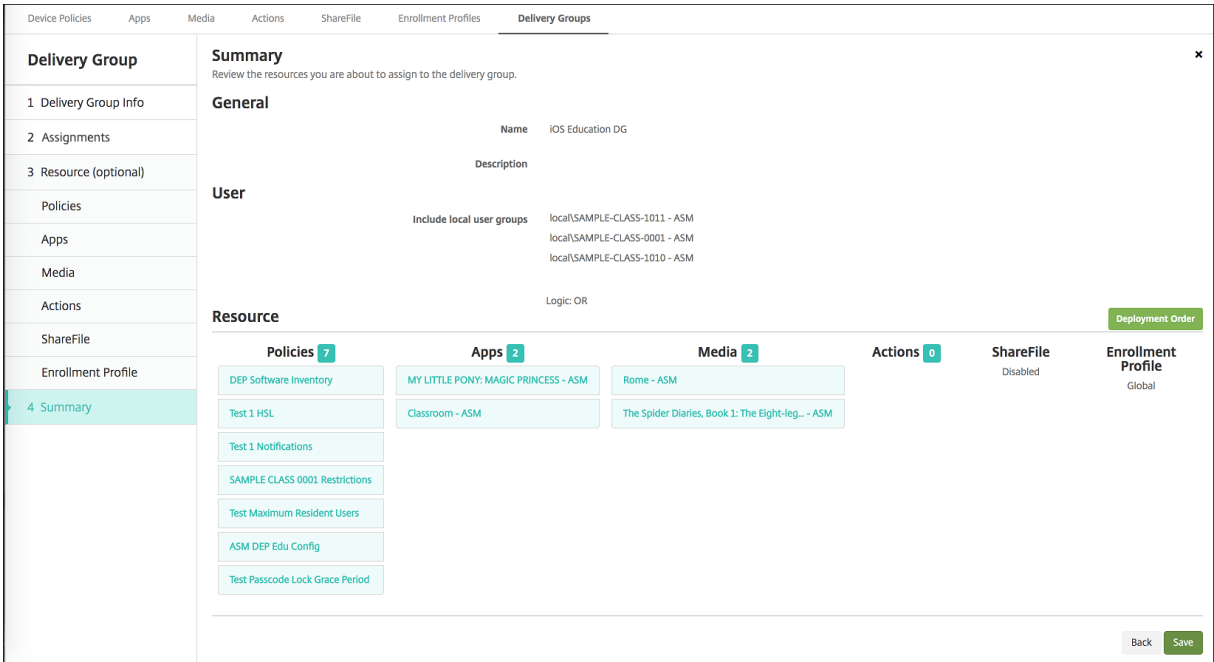
XenMobile에 Enterprise 계정을 사용하도록 구성한 경우 **ShareFile** 사용을 커짐으로 설정하여 배달 그룹에 ShareFile 콘텐츠 및 데이터에 대한 SSO(Single Sign-On) 액세스를 제공합니다.



XenMobile에 StorageZone 커넥터를 사용하도록 구성한 경우 배달 그룹에 포함할 StorageZone 커넥터를 선택합니다.



구성된 옵션을 검토하고 배포 순서를 변경하려면



요약 페이지에서 배달 그룹에 구성된 옵션을 검토하고 리소스의 배포 순서를 변경할 수 있습니다. 요약 페이지에 리소스가 범주별로 표시됩니다. 요약 페이지에는 배포 순서는 반영되지 않습니다.

1. 뒤로를 클릭하여 이전 페이지로 돌아가서 구성에 필요한 조정을 수행합니다.
2. 배포 순서를 클릭하여 배포 순서를 확인하거나 재정렬합니다. 배포 순서 대화 상자가 나타납니다.

Deployment Order

Change the deployment order by dragging the policies, apps and actions into position.

AV Player Demo

Citrix Secure Hub - VPP

Citrix Secure Web - VPP

Classroom - VPP

DEP Software Inventory

EDU

Wipe device

CancelSave

3. 리소스를 클릭하고 배포할 위치로 끌어 옵니다. 배포 순서를 변경한 후 XenMobile 은 목록의 위에서 아래로 리소스를 배포합니다.
4. 저장을 클릭하여 배포 순서를 저장합니다.
5. 저장을 클릭하여 배달 그룹을 저장합니다.

배달 그룹을 편집하려면

기존 배달 그룹의 이름은 변경할 수 없습니다. 다른 설정을 업데이트하려면: 구성 > 배달 그룹으로 이동하고 편집할 그룹을 선택한 후 편집을 클릭합니다.

AllUsers 배달 그룹을 사용하거나 사용하지 않도록 설정하려면

AllUsers 배달 그룹만 사용하거나 사용하지 않도록 설정할 수 있습니다.

배달 그룹 페이지에서 **AllUsers** 옆에 있는 확인란을 선택하고 AllUsers 가 포함된 줄을 클릭하여 AllUsers 배달 그룹을 선택합니다. 다음 중 하나를 실행합니다.

- AllUsers 배달 그룹을 사용하지 않도록 설정하려면 사용 안 함을 클릭합니다. 이 명령은 AllUsers 를 사용하도록 설정된 (기본값) 경우에만 사용할 수 있습니다. 배달 그룹 테이블의 사용 안 함 머리글 아래에 사용 안 함이 표시됩니다.
- AllUsers 배달 그룹을 사용하도록 설정하려면 사용을 클릭합니다. 이 명령은 AllUsers 를 사용하지 않도록 설정한 경우에만 사용할 수 있습니다. 배달 그룹 테이블의 사용 안 함 머리글 아래에 사용 안 함이 사라집니다.

배달 그룹에 배포하려면

배달 그룹에 배포한다는 것은 iOS 및 Windows 태블릿 장치의 모든 사용자에게 푸시 알림을 보내는 것을 의미합니다. 이러한 사용자는 배달 그룹에 속해 있어야 XenMobile 에 다시 연결됩니다. 이 방법을 통해 장치를 재평가하고 앱, 정책 및 작업을 배포할 수 있습니다.

다른 플랫폼 장치의 사용자: 해당 장치가 이미 XenMobile 에 연결된 경우 즉시 리소스를 받습니다. 그렇지 않은 경우에는 예약 정책에 기반하여 다음에 연결할 때 리소스를 받습니다. Android Enterprise 플랫폼의 사용자는 Firebase Cloud Messaging 알림 시스템에서 알림을 받은 다음 XenMobile Server 에 연결하여 리소스를 검색합니다.

Android 장치에 있는 XenMobile Store 의 업데이트 사용 가능 목록에 업데이트된 앱이 표시되게 하려면 먼저 앱 인벤토리 정책을 사용자 장치에 배포해야 합니다.

1. 배달 그룹 페이지에서 다음 중 하나를 수행합니다.

- 한 번에 둘 이상의 배달 그룹에 배포하려면 배포하려는 그룹 옆에 있는 확인란을 선택합니다.
- 하나의 배달 그룹에 배포하려면 해당 이름 옆의 확인란을 선택하거나 해당 이름이 포함된 줄을 클릭합니다.

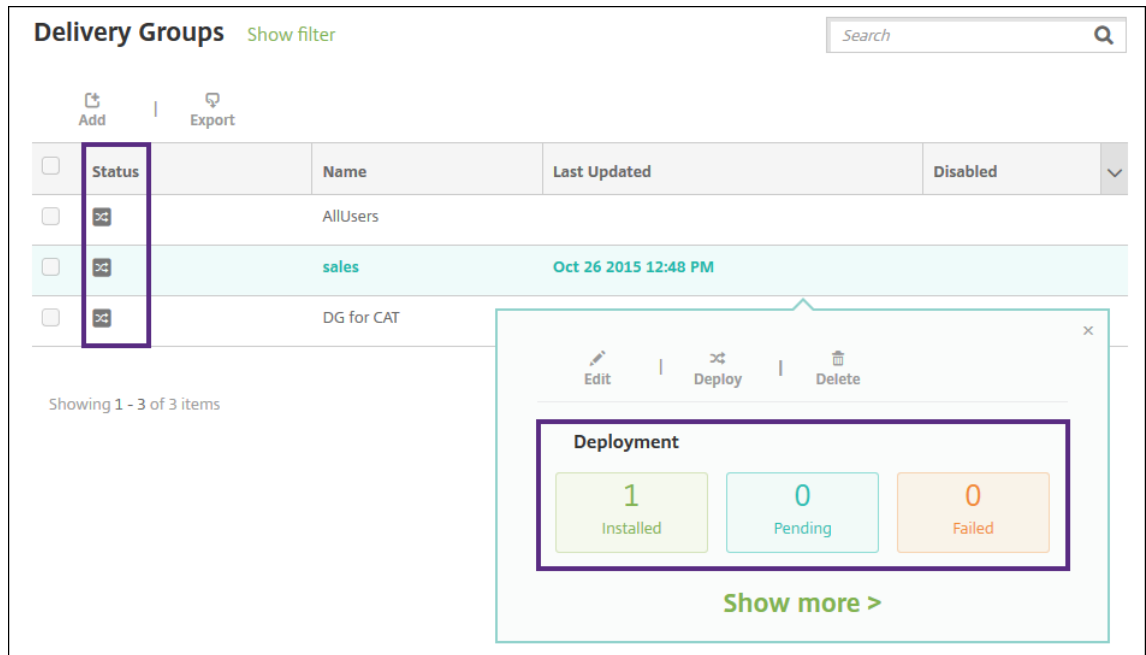
2. 배포를 클릭합니다.

배달 그룹을 선택한 방법에 따라 배달 그룹 위 또는 오른쪽에 배포 명령이 나타납니다.

앱, 정책 및 동작을 배포할 그룹이 나열되어 있는지 확인하고 배포를 클릭합니다. 장치 플랫폼과 예약 정책에 따라 선택한 그룹에 앱, 정책 및 동작이 배포됩니다.

배달 그룹 페이지에서 다음 방법 중 하나로 배포 상태를 확인할 수 있습니다.

- 배달 그룹의 상태 머리글 아래에 있는 배포 아이콘을 확인합니다. 배포가 실패한 경우 이 아이콘에 나타납니다.
- 배달 그룹이 포함된 줄을 클릭하여 설치됨, 보류 중 및 실패 배포를 나타내는 오버레이를 표시합니다.



배달 그룹을 삭제하려면

AllUsers 배달 그룹은 삭제할 수 없지만 일부 사용자에게 리소스를 푸시하지 않으려는 경우 이 그룹을 사용하지 않도록 설정할 수 있습니다.

1. 배달 그룹 페이지에서 다음 중 하나를 수행합니다.

- 한 번에 둘 이상의 배달 그룹을 삭제하려면 삭제하려는 그룹 옆에 있는 확인란을 선택합니다.
- 하나의 배달 그룹을 삭제하려면 해당 이름 옆의 확인란을 선택하거나 해당 이름이 포함된 줄을 클릭합니다.

2. 삭제를 클릭합니다. 삭제 대화 상자가 나타납니다.

단일 배달 그룹을 선택하는 방법에 따라 배달 그룹 위 또는 오른쪽에 삭제 명령이 나타납니다.

중요:

삭제는 실행 취소할 수 없습니다.

3. 삭제를 클릭합니다.

배달 그룹 테이블을 내보내려면

1. 배달 그룹 테이블 위에 있는 내보내기 단추를 클릭합니다. 배달 그룹 테이블에 있는 정보를 추출하여.csv 파일로 변환합니다.
2. 브라우저의 일반적인 단계에 따라.csv 파일을 열거나 저장합니다. 또한 작업을 취소할 수도 있습니다.

매크로

May 6, 2022

XenMobile 은 다음 항목의 텍스트 필드 내에 사용자 또는 장치 속성 데이터를 채우기 위한 방법으로 매크로를 제공합니다.

- 정책
- 알림
- 등록 템플릿
- 자동화된 동작
- 자격 증명 공급자 인증서 서명 요청

XenMobile 은 매크로를 해당 사용자 또는 시스템 값으로 바꿉니다. 예를 들어 사용자 수천 명에 대해 단일 Exchange 프로필을 보유한 각 사용자의 사서함 값을 미리 채울 수 있습니다.

매크로 구문

매크로는 다음과 같은 형식을 사용할 수 있습니다.

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]] }`

달러 기호 (\$) 뒤에 오는 모든 구문은 중괄호 ({}) 로 묶습니다.

- 정규화된 속성 이름은 사용자 속성, 장치 속성 또는 사용자 지정 속성을 참조합니다.
- 정규화된 속성 이름은 접두사와 접두사 뒤에 오는 실제 속성 이름으로 구성됩니다.
- 사용자 속성은 `${ user.[PROPERTYNAME] (prefix="user.") }` 형식을 사용합니다.
- 장치 속성은 `${ device.[PROPERTYNAME] (prefix="device.") }` 형식을 사용합니다.
- 속성 이름은 대/소문자를 구분합니다.
- 함수는 제한된 목록 또는 함수를 정의하는 타사 참조에 대한 링크일 수 있습니다. 알림 메시지를 위한 다음 매크로에는 함수 **firstnotnull** 이 포함됩니다.

`${ firstnotnull(device.TEL_NUMBER,device.serialNumber) }` 장치는 차단되었습니다...

- 사용자 지정 매크로 (사용자가 정의하는 속성) 의 접두사는 `${ custom }` 입니다. 접두사는 생략할 수 있습니다.

다음은 정책의 텍스트 필드에 사용자 이름 값을 채우는 널리 사용되는 매크로 `${ user.username }` 의 예제입니다. 이 매크로는 다수의 사용자가 사용하는 Exchange ActiveSync 프로필 및 기타 프로필을 구성할 때 유용합니다. 다음 예제에서는

Exchange 정책에서 매크로를 사용하는 방법을 보여줍니다. 사용자에 대한 매크로는 **`${ user.username }`**입니다. 전자 메일 주소에 대한 매크로는 **`${ user.mail }`**입니다.

다음 예제에서는 인증서 서명 요청에 매크로를 사용하는 방법을 보여줍니다. 주체 이름에 대한 매크로는 **`CN=$user.username`**입니다. 주체 대체 이름의 값에 대한 매크로는 **`$user.userprincipalname`**입니다.

다음 예제에서는 알림 템플릿에서 매크로를 사용하는 방법을 보여줍니다. 예제 템플릿은 HDX 응용 프로그램이 규정을 준수하지 않는 장치 때문에 차단되었을 때 사용자에게 보내는 메시지를 정의합니다. 메시지에 대한 매크로는 다음과 같습니다.

Device **`${ firstnotnull(device.TEL_NUMBER,device.serialNumber) }`** no longer complies with the device policy and HDX applications will be blocked.

Settings > Notification Templates > Add Notification Template

Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

Name*

HDX Application Block

Description

Type

Ad-Hoc Notification

Manual sending supported

Channels

Secure Hub

Activate

Message

Device
\${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

알림에 사용되는 매크로에 대한 더 많은 예제를 보려면 설정 > 알림 템플릿으로 이동하고 사전 정의된 템플릿을 선택한 다음 편집을 클릭하십시오.

다음 예제에서는 장치 이름 장치 정책의 매크로를 보여줍니다. 매크로, 매크로 조합 또는 매크로와 텍스트 조합을 입력하여 각 장치에 고유한 이름을 지정할 수 있습니다. 예를 들어 `${ device.serialnumber }`를 사용하여 장치 이름을 각 장치의 일련 번호로 설정합니다. 장치 이름에 사용자 이름을 포함하려면 `${ device.serialnumber } ${ user.username }`을 사용합니다. 장치 이름 장치 정책은 감독되는 iOS 및 macOS 장치에서 작동합니다.

Device Name Policy

1 Policy Info

2 Platforms

☒ iOS

☒ Mac OS X

3 Assignment

Device Name Policy

This policy lets you apply a name on a supervised device on iOS and Mac OS X devices. Available in iOS 8 and later.

Device name*

`${device.serialnumber}`

Deployment Rules

기본 알림 템플릿에 대한 매크로

기본 알림 템플릿에서 사용할 수 있는 매크로는 다음과 같습니다.

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`

- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`
- `${ enrollment.urls }`
- `${ enrollment.ios.url }`
- `${ enrollment.macos.url }`
- `${ enrollment.android.url }`
- `${ enrollment.ios.platform }`
- `${ enrollment.macos.platform }`
- `${ enrollment.android.platform }`
- `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${ firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${ outofcompliance.reason(smg_block)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`

참고:

XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는 용어가 포함됩니다. 향후 릴리스에서 이러한 용어를 “차단 목록” 및 “허용 목록” 으로 변경하는 중입니다.

- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

특정 정책에 대한 매크로

장치 이름 장치 정책 (iOS 및 macOS 용) 의 경우 장치 이름에 다음 매크로를 사용할 수 있습니다.

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`

- `${ enrollment.pin }`
- `${ user.dnsroot }`

웹 클립 장치 정책의 경우 **URL** 에 다음 매크로를 사용할 수 있습니다.

- `${ webeas-url }`

Samsung MDM 라이선스 키 장치 정책의 경우 **ELM** 라이선스 키에 다음 매크로를 사용할 수 있습니다.

- `${ elm.license.key }`

기본 제공 장치 속성을 가져오는 매크로

표시 이름	매크로
장치 ID	<code>\$device.id</code>
장치 GUID	<code>\$device.uniqueid</code>
장치 IMEI	<code>\$device.imei</code>
OS 제품군	<code>\$device.OSFamily</code>
일련 번호	<code>\$device.serialNumber</code>

모든 장치 속성에 대한 매크로

다음 목록에는 표시 이름, 웹 요소 및 매크로가 나와 있습니다.

계정이 일시 중단되었습니까?

- `GOOGLE_AW_DIRECTORY_SUSPENDED`
- `${device.GOOGLE_AW_DIRECTORY_SUSPENDED}`

활성화 잠금 바이패스 코드

- `ACTIVATION_LOCK_BYPASS_CODE`
- `${device.ACTIVATION_LOCK_BYPASS_CODE}`

활성화 잠금이 사용됨

- `ACTIVATION_LOCK_ENABLED`
- `${device.ACTIVATION_LOCK_ENABLED}`

활성 iTunes 계정

- `ACTIVE_ITUNES`

- `${device.ACTIVE_ITUNES}`

MSP 에 알려진 ActiveSync 장치

- `AS_DEVICE_KNOWN_BY_ZMSP`
- `${device.AS_DEVICE_KNOWN_BY_ZMSP}`

ActiveSync ID

- `EXCHANGE_ACTIVESYNC_ID`
- `${device.EXCHANGE_ACTIVESYNC_ID}`

관리자 사용 안 함

- `ADMIN_DISABLED`
- `${device.ADMIN_DISABLED}`

AIK 가 있습니까?

- `WINDOWS_HAS_AIK_PRESENT`
- `${device.WINDOWS_HAS_AIK_PRESENT}`

Amazon MDM API 사용 가능

- `AMAZON_MDM`
- `${device.AMAZON_MDM}`

Android Enterprise 장치 ID

- `GOOGLE_AW_DEVICE_ID`
- `${device.GOOGLE_AW_DEVICE_ID}`

Android Enterprise 에서 활성화된 장치?

- `GOOGLE_AW_ENABLED_DEVICE`
- `${device.GOOGLE_AW_ENABLED_DEVICE}`

Android Enterprise 설치 유형

- `GOOGLE_AW_INSTALL_TYPE`
- `${device.GOOGLE_AW_INSTALL_TYPE}`

스파이웨어 방지 프로그램 서명 상태

- `ANTI_SPYWARE_SIGNATURE_STATUS`
- `${device.ANTI_SPYWARE_SIGNATURE_STATUS}`

스파이웨어 방지 프로그램 상태

- ANTI_SPYWARE_STATUS
- \${device.ANTI_SPYWARE_STATUS}

바이러스 백신 서명 상태

- ANTI_VIRUS_SIGNATURE_STATUS
- \${device.ANTI_VIRUS_SIGNATURE_STATUS}

바이러스 백신 상태

- ANTI_VIRUS_STATUS
- \${device.ANTI_VIRUS_STATUS}

ASM DEP 활성화 잠금 바이패스 코드

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- \${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}

ASM DEP 에스스로 키

- DEP_ESCROW_KEY
- \${device.DEP_ESCROW_KEY}

자산 태그

- ASSET_TAG
- \${device.ASSET_TAG}

소프트웨어 업데이트 자동 확인

- AutoCheckEnabled
- \${device.AutoCheckEnabled}

백그라운드에서 소프트웨어 업데이트 자동 다운로드

- BackgroundDownloadEnabled
- \${device.BackgroundDownloadEnabled}

앱 업데이트 자동 설치

- AutomaticAppInstallationEnabled
- \${device.AutomaticAppInstallationEnabled}

OS 업데이트 자동 설치

- AutomaticOSInstallationEnabled
- \${device.AutomaticOSInstallationEnabled}

보안 업데이트 자동 설치

- AutomaticSecurityUpdatesEnabled
- \${device.AutomaticSecurityUpdatesEnabled}

자동 업데이트 상태

- AUTOUPDATE_STATUS
- \${device.AUTOUPDATE_STATUS}

사용 가능한 RAM

- MEMORY_AVAILABLE
- \${device.MEMORY_AVAILABLE}

사용 가능한 소프트웨어 업데이트

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- \${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}

사용 가능한 스토리지 공간

- FREEDISK
- \${device.FREEDISK}

백업 배터리

- BACKUP_BATTERY_PERCENT
- \${device.BACKUP_BATTERY_PERCENT}

기저대역 펌웨어 버전

- MODEM_FIRMWARE_VERSION
- \${device.MODEM_FIRMWARE_VERSION}

배터리 충전

- BATTERY_CHARGING_STATUS
- \${device.BATTERY_CHARGING_STATUS}

배터리 충전

- BATTERY_CHARGING
- \${device.BATTERY_CHARGING}

배터리 잔량

- BATTERY_ESTIMATED_CHARGE_REMAINING
- \${device.BATTERY_ESTIMATED_CHARGE_REMAINING}

배터리 런타임

- BATTERY_RUNTIME
- \${device.BATTERY_RUNTIME}

배터리 상태

- BATTERY_STATUS
- \${device.BATTERY_STATUS}

MS 에 알려진 BES 장치

- BES_DEVICE_KNOWN_BY_ZMSP
- \${device.BES_DEVICE_KNOWN_BY_ZMSP}

BES PIN

- BES_PIN
- \${device.BES_PIN}

BES 서버 에이전트 ID

- AGENT_ID
- \${device.AGENT_ID}

BES 서버 이름

- BES_SERVER
- \${device.BES_SERVER}

BES 서버 버전

- BES_VERSION
- \${device.BES_VERSION}

BIOS 정보

- BIOS_INFO
- \${device.BIOS_INFO}

BitLocker 상태

- WINDOWS_HAS_BIT_LOCKER_STATUS
- \${device.WINDOWS_HAS_BIT_LOCKER_STATUS}

Bluetooth MAC 주소

- BLUETOOTH_MAC
- \${device.BLUETOOTH_MAC}

부팅 디버깅이 사용됩니까?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- \${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}

부팅 관리자 수정 목록 버전

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- \${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}

이동 통신 사업자 코드

- CARRIER_CODE
- \${device.CARRIER_CODE}

이동 통신 사업자 설정 버전

- CARRIER_SETTINGS_VERSION
- \${device.CARRIER_SETTINGS_VERSION}

카탈로그 URL

- CatalogURL
- \${device.CatalogURL}

셀룰러 고도

- GPS_ALTITUDE_FROM_CELLULAR
- \${device.GPS_ALTITUDE_FROM_CELLULAR}

셀룰러 코스

- GPS_COURSE_FROM_CELLULAR
- \${device.GPS_COURSE_FROM_CELLULAR}

셀룰러 수평 정확도

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- \${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}

셀룰러 위도

- GPS_LATITUDE_FROM_CELLULAR
- \${device.GPS_LATITUDE_FROM_CELLULAR}

셀룰러 경도

- GPS_LONGITUDE_FROM_CELLULAR
- \${device.GPS_LONGITUDE_FROM_CELLULAR}

셀룰러 속도

- GPS_SPEED_FROM_CELLULAR
- \${device.GPS_SPEED_FROM_CELLULAR}

셀룰러 기술

- CELLULAR_TECHNOLOGY
- \${device.CELLULAR_TECHNOLOGY}

셀룰러 타임스탬프

- GPS_TIMESTAMP_FROM_CELLULAR
- \${device.GPS_TIMESTAMP_FROM_CELLULAR}

셀룰러 수직 정확도

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- \${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

다음 로그인 시 암호를 변경하시겠습니까?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- \${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

클라이언트 장치 ID

- CLIENT_DEVICE_ID
- \${device.CLIENT_DEVICE_ID}

클라우드 백업이 활성화됨

- CLOUD_BACKUP_ENABLED
- \${device.CLOUD_BACKUP_ENABLED}

코드 무결성이 사용됩니까?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- \${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}

코드 무결성 수정 목록 버전

- WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- \${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION}

색

- COLOR
- \${device.COLOR}

CPU 클럭 속도

- CPU_CLOCK_SPEED
- \${device.CPU_CLOCK_SPEED}

CPU 유형

- CPU_TYPE
- \${device.CPU_TYPE}

만든 시간

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- \${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}

중요 소프트웨어 업데이트

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- \${device.AVAILABLE_OS_UPDATE_IS_CRITICAL}

현재 이동 통신 사업자 네트워크

- 이동 통신 사업자
- \${device.CARRIER}

현재 모바일 국가 코드

- CURRENT_MCC
- \${device.CURRENT_MCC}

현재 모바일 네트워크 코드

- CURRENT_MNC
- \${device.CURRENT_MNC}

데이터 로밍 허용

- DATA_ROAMING_ENABLED
- \${device.DATA_ROAMING_ENABLED}

마지막 iCloud 백업 날짜

- LAST_CLOUD_BACKUP_DATE
- \${device.LAST_CLOUD_BACKUP_DATE}

기본 카탈로그

- IsDefaultCatalog
- \${device.IsDefaultCatalog}

DEP 계정 이름

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- \${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}

DEP 정책

- WINDOWS_HAS_DEP_POLICY
- \${device.WINDOWS_HAS_DEP_POLICY}

DEP 프로필이 할당됨

- PROFILE_ASSIGN_TIME
- \${device.PROFILE_ASSIGN_TIME}

DEP 프로필이 푸시됨

- PROFILE_PUSH_TIME
- \${device.PROFILE_PUSH_TIME}

DEP 프로필이 제거됨

- PROFILE_REMOVE_TIME
- \${device.PROFILE_REMOVE_TIME}

DEP 등록자

- DEVICE_ASSIGNED_BY
- \${device.DEVICE_ASSIGNED_BY}

DEP 등록 날짜

- DEVICE_ASSIGNED_DATE
- \${device.DEVICE_ASSIGNED_DATE}

설명

- DESCRIPTION
- \${device.DESCRPTION}

장치 식별자

- Activesyncid
- \${device.activesyncid}

장치 모델

- SYSTEM_OEM
- \${device.SYSTEM_OEM}

장치 이름

- DEVICE_NAME
- \${device.DEVICE_NAME}

장치 유형

- DEVICE_TYPE
- \${device.DEVICE_TYPE}

방해 금지가 활성화됨

- DO_NOT_DISTURB
- \${device.DO_NOT_DISTURB}

ELAM 드라이버가 로드되었습니까?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- \${device.WINDOWS_HAS_ELAM_DRIVER_LOADED}

암호화 규정 준수

- ENCRYPTION_COMPLIANCE
- \${device.ENCRYPTION_COMPLIANCE}

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- \${device.ENROLLMENT_KEY_GENERATION_DATE}

엔터프라이즈 ID

- ENTERPRISEID
- \${device.ENTERPRISEID}

외부 스토리지 1: 사용 가능한 공간

- EXTERNAL_STORAGE1_FREE_SPACE
- \${device.EXTERNAL_STORAGE1_FREE_SPACE}

외부 스토리지 1: 이름

- EXTERNAL_STORAGE1_NAME
- \${device.EXTERNAL_STORAGE1_NAME}

외부 스토리지 1: 총 공간

- EXTERNAL_STORAGE1_TOTAL_SPACE
- \${device.EXTERNAL_STORAGE1_TOTAL_SPACE}

외부 스토리지 2: 사용 가능한 공간

- EXTERNAL_STORAGE2_FREE_SPACE
- \${device.EXTERNAL_STORAGE2_FREE_SPACE}

외부 스토리지 2: 이름

- EXTERNAL_STORAGE2_NAME
- \${device.EXTERNAL_STORAGE2_NAME}

외부 스토리지 2: 총 공간

- EXTERNAL_STORAGE2_TOTAL_SPACE
- \${device.EXTERNAL_STORAGE2_TOTAL_SPACE}

외부 스토리지가 암호화됨

- EXTERNAL_ENCRYPTION
- \${device.EXTERNAL_ENCRYPTION}

FileVault 사용

- IS_FILEVAULT_ENABLED
- \${device.IS_FILEVAULT_ENABLED}

방화벽 상태

- DEVICE_FIREWALL_STATUS
- \${device.DEVICE_FIREWALL_STATUS}

방화벽 상태

- FIREWALL_STATUS
- \${device.FIREWALL_STATUS}

펌웨어 버전

- FIRMWARE_VERSION
- \${device.FIRMWARE_VERSION}

첫 번째 동기화

- ZMSP_FIRST_SYNC
- \${device.ZMSP_FIRST_SYNC}

Google Directory 별칭

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- \${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}

Google Directory 패밀리 이름

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- \${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}

Google Directory 이름

- GOOGLE_AW_DIRECTORY_NAME
- \${device.GOOGLE_AW_DIRECTORY_NAME}

Google Directory 기본 전자 메일

- GOOGLE_AW_DIRECTORY_PRIMARY
- \${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google Directory 사용자 ID

- GOOGLE_AW_DIRECTORY_USER_ID
- \${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS 고도

- GPS_ALTITUDE_FROM_GPS
- \${device.GPS_ALTITUDE_FROM_GPS}

GPS 코스

- GPS_COURSE_FROM_GPS
- \${device.GPS_COURSE_FROM_GPS}

GPS 수평 정확도

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- \${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS}

GPS 위도

- GPS_LATITUDE_FROM_GPS
- \${device.GPS_LATITUDE_FROM_GPS}

GPS 경도

- GPS_LONGITUDE_FROM_GPS
- \${device.GPS_LONGITUDE_FROM_GPS}

GPS 속도

- GPS_SPEED_FROM_GPS
- \${device.GPS_SPEED_FROM_GPS}

GPS 타임스탬프

- GPS_TIMESTAMP_FROM_GPS
- \${device.GPS_TIMESTAMP_FROM_GPS}

GPS 수직 정확도

- GPS_VERTICAL_ACCURACY_FROM_GPS
- \${device.GPS_VERTICAL_ACCURACY_FROM_GPS}

하드웨어 장치 ID

- HW_DEVICE_ID
- \${device.HW_DEVICE_ID}

하드웨어 암호화 기능

- HARDWARE_ENCRYPTION_CAPS
- \${device.HARDWARE_ENCRYPTION_CAPS}

HAS_CONTAINER

- HAS_CONTAINER
- \${device.HAS_CONTAINER}

현재 로그인되어 있는 iTunes 스토어 계정의 해시

- ITUNES_STORE_ACCOUNT_HASH
- \${device.ITUNES_STORE_ACCOUNT_HASH}

홈 이동 통신 사업자 네트워크

- SIM_CARRIER_NETWORK
- \${device.SIM_CARRIER_NETWORK}

홈 모바일 국가 코드

- SIM_MCC
- \${device.SIM_MCC}

홈 모바일 네트워크 코드

- SIM_MNC
- \${device.SIM_MNC}

ICCID

- ICCID
- \${device.ICCID}

ID

- AS_DEVICE_IDENTITY
- \${device.AS_DEVICE_IDENTITY}

IMEI/MEID 번호

- IMEI
- \${device.IMEI}

IMSI

- SIM_ID
- \${device.SIM_ID}

내부 스토리지가 암호화됨

- LOCAL_ENCRYPTION
- \${device.LOCAL_ENCRYPTION}

IP 위치

- IP_LOCATION
- \${device.IP_LOCATION}

IPv4 주소

- IP_ADDRESSV4
- \${device.IP_ADDRESSV4}

IPv6 주소

- IP_ADDRESSV6
- \${device.IP_ADDRESSV6}

실행 시간

- WINDOWS_HAS_ISSUED_AT
- \${device.WINDOWS_HAS_ISSUED_AT}

탈옥/루팅

- ROOT_ACCESS
- \${device.ROOT_ACCESS}

커널 디버깅이 사용됩니까?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- \${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}

키오스크 모드

- IS_KIOSK
- \${device.IS_KIOSK}

마지막으로 알려진 IP 주소

- LAST_IP_ADDR
- \${device.LAST_IP_ADDR}

마지막 정책 업데이트 시간

- LAST_POLICY_UPDATE_TIME
- \${device.LAST_POLICY_UPDATE_TIME}

마지막 검사 날짜

- PreviousScanDate
- \${device.PreviousScanDate}

마지막 검사 결과

- PreviousScanResult
- \${device.PreviousScanResult}

마지막으로 예약된 소프트웨어 업데이트

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- \${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}

마지막으로 예약된 소프트웨어 업데이트 실패 메시지

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- \${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}

마지막으로 예약된 소프트웨어 업데이트 상태

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- \${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}

마지막 동기화

- ZMSP_LAST_SYNC
- \${device.ZMSP_LAST_SYNC}

로케이터 서비스 사용

- DEVICE_LOCATOR
- \${device.DEVICE_LOCATOR}

MAC 주소

- MAC_ADDRESS
- \${device.MAC_ADDRESS}

MAC 주소 네트워크 연결

- MAC_NETWORK_CONNECTION
- \${device.MAC_NETWORK_CONNECTION}

MAC 주소 유형

- MAC_ADDRESS_TYPE
- \${device.MAC_ADDRESS_TYPE}

사서함 설정

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- \${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP}

기본 배터리

- MAIN_BATTERY_PERCENT
- \${device.MAIN_BATTERY_PERCENT}

MDM 분실 모드 활성화

- IS_MDM_LOST_MODE_ENABLED
- \${device.IS_MDM_LOST_MODE_ENABLED}

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- \${device.MDX_SHARED_ENCRYPTION_KEY}

MEID

- MEID
- \${device.MEID}

휴대폰 번호

- TEL_NUMBER
- \${device.TEL_NUMBER}

모델 ID

- MODEL_ID
- \${device.MODEL_ID}

모델 번호

- MODEL_NUMBER
- \${device.MODEL_NUMBER}

네트워크 어댑터 유형

- NETWORK_ADAPTER_TYPE
- \${device.NETWORK_ADAPTER_TYPE}

운영 체제 빌드

- SYSTEM_OS_BUILD
- \${device.SYSTEM_OS_BUILD}

운영 체제 버전

- OS_EDITION
- \${device.OS_EDITION}

운영 체제 언어 (로캘)

- SYSTEM_LANGUAGE
- \${device.SYSTEM_LANGUAGE}

운영 체제 버전

- SYSTEM_OS_VERSION
- \${device.SYSTEM_OS_VERSION}

조직 주소

- ORGANIZATION_ADDRESS
- \${device.ORGANIZATION_ADDRESS}

조직 전자 메일

- ORGANIZATION_EMAIL
- \${device.ORGANIZATION_EMAIL}

조직 매직

- ORGANIZATION_MAGIC
- \${device.ORGANIZATION_MAGIC}

조직 이름

- ORGANIZATION_NAME
- \${device.ORGANIZATION_NAME}

조직 전화 번호

- ORGANIZATION_PHONE
- \${device.ORGANIZATION_PHONE}

규정 위반

- OUT_OF_COMPLIANCE
- \${device.OUT_OF_COMPLIANCE}

소유자

- CORPORATE_OWNED
- \${device.CORPORATE_OWNED}

암호 규정 준수

- PASSCODE_IS_COMPLIANT
- \${device.PASSCODE_IS_COMPLIANT}

구성을 준수하는 암호

- PASSCODE_IS_COMPLIANT_WITH_CFG
- \${device.PASSCODE_IS_COMPLIANT_WITH_CFG}

현재 암호

- PASSCODE_PRESENT
- \${device.PASSCODE_PRESENT}

PCR0

- WINDOWS_HAS_PCR0
- \${device.WINDOWS_HAS_PCR0}

경계 위반

- GPS_PERIMETER_BREACH
- \${device.GPS_PERIMETER_BREACH}

정기적인 확인

- PerformPeriodicCheck
- \${device.PerformPeriodicCheck}

개인 핫스팟이 활성화됨

- PERSONAL_HOTSPOT_ENABLED
- \${device.PERSONAL_HOTSPOT_ENABLED}

지오펜스의 PIN 코드

- PIN_CODE_FOR_GEO_FENCE
- \${device.PIN_CODE_FOR_GEO_FENCE}

플랫폼

- SYSTEM_PLATFORM
- \${device.SYSTEM_PLATFORM}

플랫폼 API 수준

- API_LEVEL
- \${device.API_LEVEL}

정책 이름

- POLICY_NAME
- \${device.POLICY_NAME}

기본 전화 번호

- IDENTITY1_PHONENUMBER
- \${device.IDENTITY1_PHONENUMBER}

기본 SIM 이동 통신 사업자 운영자

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- \${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}

기본 SIM ICCID

- IDENTITY1_ICCID
- \${device.IDENTITY1_ICCID}

기본 SIM 카드 IMEI

- IDENTITY1_IMEI
- \${device.IDENTITY1_IMEI}

기본 SIM 카드 IMSI

- IDENTITY1_IMSI
- \${device.IDENTITY1_IMSI}

기본 SIM 카드 로밍

- IDENTITY1_ROAMING
- \${device.IDENTITY1_ROAMING}

기본 SIM 로밍 규정 준수

- IDENTITY1_ROAMING_COMPLIANCE
- \${device.IDENTITY1_ROAMING_COMPLIANCE}

제품 이름

- PRODUCT_NAME
- \${device.PRODUCT_NAME}

게시자 장치 ID

- PUBLISHER_DEVICE_ID
- \${device.PUBLISHER_DEVICE_ID}

재설정 횟수

- WINDOWS_HAS_RESET_COUNT
- \${device.WINDOWS_HAS_RESET_COUNT}

다시 시작 횟수

- WINDOWS_HAS_RESTART_COUNT
- \${device.WINDOWS_HAS_RESTART_COUNT}

안전 모드가 사용됩니까?

- WINDOWS_HAS_SAFE_MODE
- \${device.WINDOWS_HAS_SAFE_MODE}

Samsung KNOX API 사용 가능

- SAMSUNG_KNOX
- \${device.SAMSUNG_KNOX}

Samsung KNOX API 버전

- SAMSUNG_KNOX_VERSION
- \${device.SAMSUNG_KNOX_VERSION}

Samsung KNOX 증명

- SAMSUNG_KNOX_ATTESTED
- \${device.SAMSUNG_KNOX_ATTESTED}

Samsung KNOX 증명 업데이트 날짜

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- \${device.SAMSUNG_KNOX_ATT_UPDATED_TIME}

Samsung SAFE API 사용 가능

- SAMSUNG_MDM
- \${device.SAMSUNG_MDM}

Samsung SAFE API 버전

- SAMSUNG_MDM_VERSION
- \${device.SAMSUNG_MDM_VERSION}

SBCP 해시

- WINDOWS_HAS_SBCP_HASH
- \${device.WINDOWS_HAS_SBCP_HASH}

화면: 높이

- SCREEN_HEIGHT
- \${device.SCREEN_HEIGHT}

화면: 색상 수

- SCREEN_NB_COLORS
- \${device.SCREEN_NB_COLORS}

화면: 크기

- SCREEN_SIZE
- \${device.SCREEN_SIZE}

화면: 너비

- SCREEN_WIDTH
- \${device.SCREEN_WIDTH}

화면: X 축 해상도

- SCREEN_XDPI
- \${device.SCREEN_XDPI}

화면: Y 축 해상도

- SCREEN_YDPI
- \${device.SCREEN_YDPI}

보조 전화 번호

- IDENTITY2_PHONENUMBER
- \${device.IDENTITY2_PHONENUMBER}

보조 SIM 이동 통신 사업자 운영자

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- \${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}

보조 SIM ICCID

- IDENTITY2_ICCID
- \${device.IDENTITY2_ICCID}

보조 SIM 카드 IMEI

- IDENTITY2_IMEI
- \${device.IDENTITY2_IMEI}

보조 SIM 카드 IMSI

- IDENTITY2_IMSI
- \${device.IDENTITY2_IMSI}

보조 SIM 카드 로밍

- IDENTITY2_ROAMING
- \${device.IDENTITY2_ROAMING}

보조 SIM 로밍 규정 준수

- IDENTITY2_ROAMING_COMPLIANCE
- \${device.IDENTITY2_ROAMING_COMPLIANCE}

보안 부팅이 사용됩니까?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- \${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}

보안 부팅 상태

- SECURE_BOOT_STATE
- \${device.SECURE_BOOT_STATE}

SecureContainer 사용

- DLP_ACTIVE
- \${device.DLP_ACTIVE}

보안 패치 수준

- SYSTEM_SECURITY_PATCH_LEVEL
- \${device.SYSTEM_SECURITY_PATCH_LEVEL}

일련 번호

- SERIAL_NUMBER
- \${device.SERIAL_NUMBER}

SMS 지원

- IS_SMS_CAPABLE
- \${device.IS_SMS_CAPABLE}

감독됨

- SUPERVISED
- \${device.SUPERVISED}

일시 중단 이유

- GOOGLE_AW_DIRECTORY_SUSPENSION_REASON
- \${device.GOOGLE_AW_DIRECTORY_SUSPENSION_REASON}

무단 변경된 상태

- TAMPERED_STATUS
- \${device.TAMPERED_STATUS}

약관

- TERMS_AND_CONDITIONS
- \${device.TERMS_AND_CONDITIONS}

약관에 동의하십니까?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- \${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}

테스트 서명이 사용됩니까?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- \${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}

총 RAM

- MEMORY
- \${device.MEMORY}

총 스토리지 공간

- TOTAL_DISK_SPACE
- \${device.TOTAL_DISK_SPACE}

TPM 버전

- TPM_VERSION
- \${device.TPM_VERSION}

UDID

- UDID
- \${device.UDID}

사용자 계정 제어 상태

- UAC_STATUS
- \${device.UAC_STATUS}

사용자 에이전트

- USER_AGENT
- \${device.USER_AGENT}

사용자 정의 #1

- USER_DEFINED_1
- \${device.USER_DEFINED_1}

사용자 정의 #2

- USER_DEFINED_2
- \${device.USER_DEFINED_2}

사용자 정의 #3

- USER_DEFINED_3
- \${device.USER_DEFINED_3}

사용자 언어 (로캘)

- USER_LANGUAGE
- \${device.USER_LANGUAGE}

공급업체

- VENDOR
- \${device.VENDOR}

음성 지원

- IS_VOICE_CAPABLE
- \${device.IS_VOICE_CAPABLE}

음성 로밍 허용

- VOICE_ROAMING_ENABLED
- \${device.VOICE_ROAMING_ENABLED}

VSM 이 사용됩니까?

- WINDOWS_HAS_VSM_ENABLED
- \${device.WINDOWS_HAS_VSM_ENABLED}

WiFi MAC 주소

- WIFI_MAC
- \${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- \${device.WINDOWS_ENROLLMENT_KEY}

WinPE 가 사용됩니까?

- WINDOWS_HAS_WINPE
- \${device.WINDOWS_HAS_WINPE}

WNS 알람 상태

- PROPERTY_WNS_PUSH_STATUS
- \${device.PROPERTY_WNS_PUSH_STATUS}

WNS 알람 URL

- PROPERTY_WNS_PUSH_URL
- \${device.PROPERTY_WNS_PUSH_URL}

WNS 알람 URL 만료 날짜

- PROPERTY_WNS_PUSH_URL_EXPIRY
- \${device.PROPERTY_WNS_PUSH_URL_EXPIRY}

XenMobile 에이전트 ID

- ENROLLMENT_AGENT_ID
- \${device.ENROLLMENT_AGENT_ID}

XenMobile 에이전트 수정

- EW_REVISION
- \${device.EW_REVISION}

XenMobile 에이전트 버전

- EW_VERSION
- \${device.EW_VERSION}

Zebra API 사용 가능

- ZEBRA_MDM
- \${device.ZEBRA_MDM}

Zebra MXMF 버전

- ZEBRA_MDM_VERSION
- \${device.ZEBRA_MDM_VERSION}

Zebra 패치 버전

- ZEBRA_PATCH_VERSION
- \${device.ZEBRA_PATCH_VERSION}

기본 제공 사용자 속성을 가져오는 매크로

표시 이름	매크로
domainname(도메인 이름 또는 기본 도메인)	<code>\${ user.domainname }</code>
loginname(사용자 이름 + 도메인 이름)	<code>\${ user.loginname }</code>
username(도메인이 있는 경우 도메인을 제외한 로그인 이름)	<code>\${ user.username }</code>

모든 사용자 속성에 대한 매크로

표시 이름	웹 요소	매크로
Active Directory 실패한 로그인 시도 횟수	badpwdcount	<code>\${ user.badpwdcount }</code>
ActiveSync 사용자 전자 메일	asuseremail	<code>\${ user.asuseremail }</code>
ASM 데이터 원본	asmpersonsource	<code>\${ user.asmpersonsource }</code>
ASM DEP 계정 이름	asmdepaccount	<code>\${ user.asmdepaccount }</code>

표시 이름	웹 요소	매크로
ASM 관리되는 Apple ID	asmpersonmanagedappleid	<code>\${ user. asmpersonmanagedappleid }</code>
ASM 암호 유형	asmpersonpasscodetype	<code>\${ user. asmpersonpasscodetype }</code>
ASM 사용자 ID	asmpersonid	<code>\${ user.asmpersonid }</code>
ASM 사용자 상태	asmpersonstatus	<code>\${ user. asmpersonstatus }</code>
ASM 사용자 직위	asmpersontitle	<code>\${ user. asmpersontitle }</code>
ASM 사용자 고유 ID	asmpersonuniqueid	<code>\${ user. asmpersonuniqueid }</code>
ASM 소스 시스템 ID	asmpersonsourcesystemid	<code>\${ user. asmpersonsourcesystemid }</code>
ASM 학생의 학년	asmpersongrade	<code>\${ user. asmpersongrade }</code>
BES 사용자 전자 메일	besuseremail	<code>\${ user.besuseremail }</code>
회사	company	<code>\${ user.company }</code>
회사 이름	companyname	<code>\${ user.companyname }</code>
국가	c	<code>\${ user.c }</code>
부서	department	<code>\${ user.department }</code>
설명	description	<code>\${ user.description }</code>
사용하지 않는 사용자	disableduser	<code>\${ user.disableduser }</code>
표시 이름	displayname	<code>\${ user.displayname }</code>
고유 이름	distinguishedname	<code>\${ user. distinguishedname }</code>
도메인 이름	domainname	<code>\${ user.domainname }</code>
전자 메일	mail	<code>\${ user.mail }</code>

표시 이름	웹 요소	매크로
이름	givenname	<code>\${ user.givenname }</code>
집 주소	homestreetaddress	<code>\${ user.homestreetaddress }</code>
집 구/군/시	homecity	<code>\${ user.homecity }</code>
집 국가	homecountry	<code>\${ user.homecountry }</code>
집 팩스	homefax	<code>\${ user.homefax }</code>
집 전화	homephone	<code>\${ user.homephone }</code>
집 시/도/지역	homestate	<code>\${ user.homestate }</code>
집 우편 번호	homezip	<code>\${ user.homezip }</code>
IP 전화	ipphone	<code>\${ user.ipphone }</code>
중간 이니셜	middleinitial	<code>\${ user.middleinitial }</code>
중간 이름	middlename	<code>\${ user.middlename }</code>
모바일	mobile	<code>\${ user.mobile }</code>
이름	cn	<code>\${ user.cn }</code>
사무실 주소	physicaldeliveryofficename	<code>\${ user.physicaldeliveryofficename }</code>
사무실 구/군/시	l	<code>\${ user.l }</code>
사무실 팩스 번호	facsimiletelephonenumber	<code>\${ user.facsimiletelephonenumber }</code>
사무실 시/도	st	<code>\${ user.st }</code>
사무실 세부 주소	officestreetaddress	<code>\${ user.officestreetaddress }</code>
사무실 전화 번호	telephonenumber	<code>\${ user.telephonenumber }</code>
사무실 우편 번호	postalcode	<code>\${ user.postalcode }</code>
사서함	postofficebox	<code>\${ user.postofficebox }</code>
호출기	pager	<code>\${ user.pager }</code>

표시 이름	웹 요소	매크로
주 그룹 ID	primarygroupid	<code>\${ user. primarygroupid }</code>
SAM 계정	samaccountname	<code>\${ user. samaccountname }</code>
세부 주소	streetaddress	<code>\${ user.streetaddress }</code>
성	sn	<code>\${ user.sn }</code>
직위	title	<code>\${ user.title }</code>
사용자 로그인 이름	userprincipalname	<code>\${ user. userprincipalname }</code>

자동화된 동작

March 15, 2024

XenMobile 에서 이벤트, 사용자 또는 장치 속성 또는 사용자 장치의 앱 존재에 대한 반응을 프로그래밍하는 자동화된 동작을 만들 수 있습니다. 자동화된 동작을 만드는 경우 XenMobile 에 연결하는 사용자 장치에서 수행되는 동작은 동작에 정의된 트리거에 따라 결정됩니다. 이벤트가 트리거되면 더 심각한 동작이 수행되기 전에 문제를 수정하도록 사용자에게 알림을 보낼 수 있습니다.

자동으로 발생하도록 설정하는 효과의 범위는 다음과 같습니다.

- 장치를 전체적으로 또는 선택적으로 초기화
- 장치를 규정 위반으로 설정
- 장치 해지
- 더 심각한 조치가 취해지기 전에 문제를 수정하도록 사용자에게 알림 전송

MAM 전용 모드에 대해 앱 잠금 및 앱 초기화 동작을 구성할 수 있습니다.

참고:

사용자에게 알림을 보내려면 XenMobile 이 메시지를 보낼 수 있도록 먼저 SMTP 및 SMS 에 대한 XenMobile 설정에서 알림 서버를 구성해야 합니다. 자세한 내용은 [알림](#)을 참조하십시오. 또한 계속하기 전에 사용하려는 모든 알림 템플릿을 설정합니다. 자세한 내용은 [알림 템플릿 만들기 및 업데이트](#)를 참조하십시오.

예제 작업

다음은 자동화된 작업을 사용하는 몇 가지 예입니다.

예제 1

- 이전에 차단한 앱 (예: “Words with Friends”) 을 검색하려고 합니다. “Words with Friends” 앱을 감지한 후 사용자 장치가 규정을 준수하지 않도록 설정하는 트리거를 특정할 수 있습니다. 그런 다음 사용자에게 앱을 삭제해야 기기를 규정 준수 상태로 되돌릴 수 있다고 알립니다. 또한 사용자가 준수할 때까지 대기할 기간에 대한 시간 제한을 설정할 수 있습니다. 이 시간 제한이 지나면 정의된 동작 (예: 장치를 선택적으로 초기화) 이 수행됩니다.

예제 2

- 고객이 최신 펌웨어를 사용하고 있는지 확인하고 사용자가 장치를 업데이트해야 하는 경우 리소스에 대한 액세스를 차단하려고 합니다. 사용자 장치에 최신 버전이 없는 경우 사용자 장치를 규정 위반으로 설정하는 트리거를 지정할 수 있습니다. 자동화된 작업을 사용하여 리소스를 차단하고 고객에게 알릴 수 있습니다.

예제 3

- 사용자 장치가 규정 위반 상태가 되고 사용자가 장치를 수정합니다. 장치를 규정 준수 상태로 재설정하는 패키지를 배포하도록 정책을 구성할 수 있습니다.

예제 4

- 특정 기간 동안 비활성 상태인 사용자 장치를 규정 위반으로 표시하려고 합니다. 비활성 장치에 대해 다음과 같이 자동화된 작업을 생성할 수 있습니다.
 1. XenMobile 콘솔에서 설정 > 네트워크 액세스 제어로 이동한 다음 비활성 장치를 선택합니다. 비활성 장치 설정에 대한 자세한 내용은 [네트워크 액세스 제어](#)에서 확인하십시오.
 2. [작업 추가 및 관리](#)에 설명된 대로 단계에 따라 작업을 추가합니다. 유일한 차이점은 작업 세부 정보 페이지에서 다음과 같이 설정을 구성한다는 것입니다.
 - 트리거. 장치 속성, 규정 위반, **True** 를 선택합니다.
 - 작업. 알림 전송을 선택하고 설정에서 알림 템플릿을 사용하여 생성한 템플릿을 선택합니다. 그런 다음 동작을 수행하기 전의 지연 기간을 일, 시간 또는 분 단위로 설정합니다. 사용자가 동작을 트리거한 문제를 해결할 때까지 동작을 반복할 간격을 설정합니다.

팁:

비활성 장치를 대량으로 삭제하려면 [REST 서비스용 공용 API](#)를 사용합니다. 먼저 삭제할 비활성 장치의 장치 ID 를 수동으로 얻은 다음 삭제 API 를 실행하여 대량으로 삭제합니다.

작업 추가 및 관리

자동화된 작업을 추가, 편집 및 필터링하려면 다음을 수행합니다.

1. XenMobile 콘솔에서 구성 > 동작을 클릭합니다. 동작 페이지가 나타납니다.

2. 동작 페이지에서 다음 중 하나를 수행합니다.

- 추가를 클릭하여 동작을 추가합니다.
- 기존 동작을 선택하여 편집하거나 삭제합니다. 사용할 옵션을 클릭합니다.

3. 동작 정보 페이지가 나타납니다.

4. 동작 정보 페이지에서 다음 정보를 입력하거나 수정합니다.

- 이름: 동작을 고유하게 식별하는 이름을 입력합니다. 이것은 필수 필드입니다.
- 설명: 동작의 의미를 설명합니다.

5. 다음을 클릭합니다. 동작 세부 정보 페이지가 나타납니다.

다음 예제는 이벤트 트리거를 설정하는 방법을 보여 줍니다. 다른 트리거를 선택할 경우 여기에 표시된 것과 다른 옵션이 표시됩니다.

The screenshot displays the 'Action details' configuration page in the XenMobile Server interface. On the left, a sidebar lists 'Actions' with sub-items: '1 Action Info', '2 Details' (highlighted), '3 Assignment (optional)', and '4 Summary'. The main content area is titled 'Action details' and includes a sub-header 'Choose a trigger event and the associated action for that event.' Below this, there are two dropdown menus: 'Trigger*' and 'Action*', both currently showing 'Select a trigger' and 'Select an action' respectively. A 'Summary' section contains the text 'If CONDITION IS FULFILLED, then DO ACTION.' At the bottom, a list of links for 'Deployment Rules' is provided for various platforms: iOS, macOS, Android, Windows Mobile/CE, Windows Desktop/Tablet, and Windows Phone.

6. 동작 세부 정보 페이지에서 다음 정보를 입력하거나 수정합니다.

트리거 목록에서 이 동작에 대한 이벤트 트리거 유형을 클릭합니다. 각 트리거의 의미는 다음과 같습니다.

- 이벤트: 미리 정의된 이벤트에 반응합니다.
- 장치 속성: MDM 관리 장치에서 장치 특성을 확인하고 이에 반응합니다. 자세한 내용은 [장치 속성 이름 및 값](#)을 참조하십시오.
- 사용자 속성: 일반적으로 Active Directory의 사용자 특성에 반응합니다.
- 설치된 앱 이름: 설치되는 앱에 반응합니다. MAM 전용 모드에는 적용되지 않습니다. 장치에서 앱 인벤토리 정책을 사용하도록 설정해야 합니다. 앱 인벤토리 정책은 모든 플랫폼에서 기본적으로 사용하도록 설정됩니다. 자세한 내용은 [앱 인벤토리 장치 정책](#)을 참조하십시오.

7. 다음 목록에서 트리거에 대한 응답을 클릭합니다.

8. 동작 목록에서 트리거 조건이 충족될 때 수행할 동작을 클릭합니다. 알림 보내기를 제외하고 사용자가 트리거를 야기한 문제를 해결할 수 있는 시간을 선택합니다. 해당 시간 내에 문제가 해결되지 않으면 선택한 동작이 수행됩니다. 동작의 정의는 [보안 동작](#)을 참조하십시오.

알림 보내기를 선택하는 경우 다음 단계를 사용하여 알림 동작을 보냅니다.

9. 다음 목록에서 알림에 사용할 템플릿을 선택합니다. 해당 알림 유형에 대한 템플릿이 없는 경우를 제외하고 선택한 이벤트와 관련된 알림 템플릿이 나타납니다. 해당하는 템플릿이 없는 경우에는 “이 이벤트 유형에 대한 템플릿이 없습니다”라는 메시지와 함께 템플릿 구성 메시지가 표시됩니다. 설정에서 알림 템플릿을 사용하여 템플릿을 만듭니다.

사용자에게 알림을 보내려면 XenMobile 이 메시지를 보낼 수 있도록 먼저 SMTP 및 SMS 에 대한 설정에서 알림 서버를 구성해야 합니다. [알림](#)을 참조하십시오. 또한 계속하기 전에 사용하려는 모든 알림 템플릿을 설정합니다. 알림 템플릿 설정에 대한 자세한 내용은 [알림 템플릿 만들기 및 업데이트](#)를 참조하십시오.

템플릿을 선택한 후 알림 메시지 미리 보기를 클릭하여 알림을 미리 볼 수 있습니다.

10. 다음 필드에서 동작을 수행하기 전의 지연 시간을 일, 시간 또는 분 단위로 설정합니다. 사용자가 동작을 트리거한 문제를 해결할 때까지 동작을 반복할 간격을 설정합니다.

11. 요약에서 의도한 자동화 동작이 만들어졌는지 확인합니다.

Summary

If The installed app name is " APP ", then notify USING TEMPLATE after 1 hour(s).

12. 동작 세부 정보를 구성한 후 각 플랫폼에 대한 배포 규칙을 개별적으로 구성할 수 있습니다. 이렇게 하려면 선택한 각 플랫폼에 대한 13 단계를 완료합니다.

13. 배포 규칙을 구성합니다. 배포 규칙 구성에 대한 일반 정보는 [리소스 배포](#)를 참조하십시오.

이 예에서:

- 장치 소유권은 **BYOD** 여야 합니다.
- 장치 로컬 암호화는 **True** 여야 합니다.
- 장치는 암호 규정을 준수해야 합니다.
- 장치 MCC(모바일 국가 코드) 로 안도라만 지정될 수는 없습니다.

14. 동작에 대한 플랫폼 배포 규칙을 구성한 후 다음을 클릭합니다. 동작 할당 페이지가 나타나면 여기에서 배달 그룹에 동작을 할당합니다. 이 단계는 선택 사항입니다.

15. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.

16. 배포 일정을 확장하고 다음 설정을 구성합니다.

- 배포 옆에서 켜짐을 클릭하여 배포를 예약하거나 꺼짐을 클릭하여 배포를 차단합니다. 기본 옵션은 켜짐입니다. 꺼짐을 선택하는 경우 다른 옵션은 필요하지 않습니다.
- 배포 일정 옆에서 지금 또는 나중에를 클릭합니다. 기본 옵션은 켜짐입니다.
- 나중에를 클릭하는 경우 달력 아이콘을 클릭하고 배포 날짜와 시간을 선택합니다.
- 배포 조건 옆에서 모든 연결에서를 클릭하거나 이전 배포가 실패한 경우에만을 클릭합니다. 기본 옵션은 모든 연결에서입니다.
- 상시 연결에 대해 배포 옆에서 켜짐 또는 꺼짐을 클릭합니다. 기본 옵션은 꺼짐입니다.

설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우에만 이 옵션이 적용됩니다. iOS 장치에는 상시 연결 옵션을 사용할 수 없습니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 모든 플랫폼에 적용되지만 상시 연결에 대해 배포를 선택한 경우 iOS 에는 적용되지 않습니다.

17. 다음을 클릭합니다. 요약 페이지가 나타나고 여기서 동작 구성을 확인할 수 있습니다.

18. 저장을 클릭하여 동작을 저장합니다.

MAM 전용 모드에 대한 앱 잠금 및 앱 초기화 동작

XenMobile 콘솔에 나열된 모든 4 개 범주의 트리거 (이벤트, 장치 속성, 사용자 속성 및 설치된 앱 이름) 에 대한 응답으로 장치의 앱을 초기화하거나 잠글 수 있습니다.

자동 앱 초기화 또는 앱 잠금을 구성하려면

1. XenMobile 콘솔에서 구성 > 동작을 클릭합니다.
2. 동작 페이지에서 추가를 클릭합니다.
3. 동작 정보 페이지에서 동작 이름과 선택적 설명을 입력합니다.
4. 동작 세부 정보 페이지에서 원하는 트리거를 선택합니다.
5. 동작에서 동작을 선택합니다.

이 단계에서는 다음 조건을 유의하십시오.

트리거 유형이 이벤트이고 값이 **Active Directory** 에서 사용하지 않도록 설정된 사용자인 경우 앱 초기화 및 앱 잠금 동작이 표시되지 않습니다.

트리거 유형이 장치 속성이고 값이 **MDM** 분실 모드 활성화인 경우 다음 동작이 표시되지 않습니다.

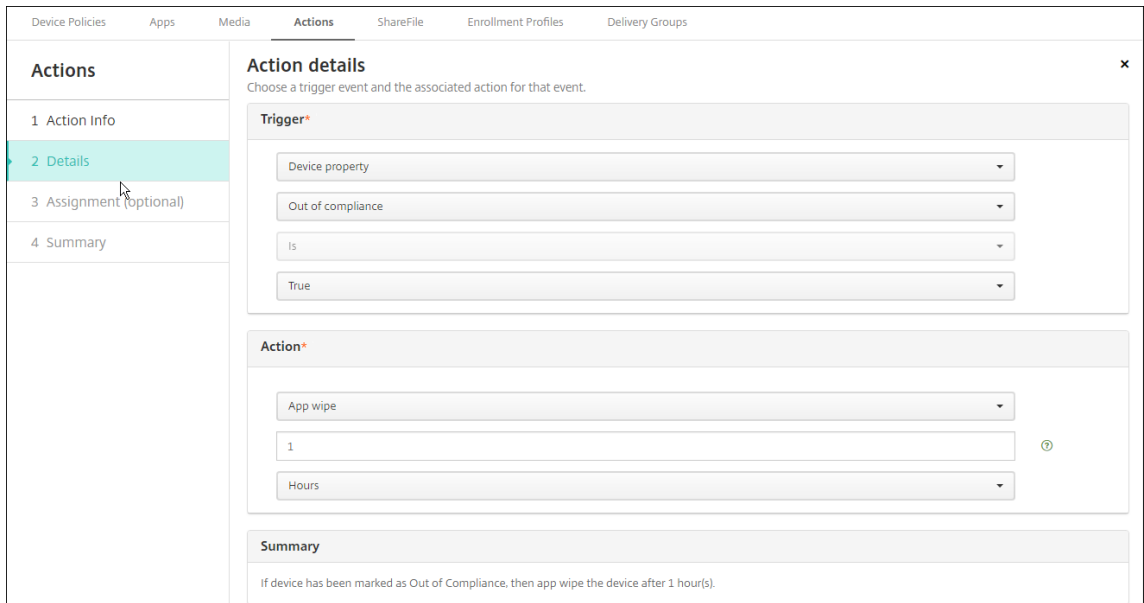
- 장치를 선택적으로 초기화
- 장치를 완전히 초기화
- 장치 해지

각 옵션에 대해 1 시간이 지연이 자동으로 설정되지만 지연 기간을 분, 시간 또는 일 단위로 선택할 수 있습니다. 지연의 목적은 동작이 발생하기 전에 사용자에게 문제를 수정할 시간을 주기 위한 것입니다. 앱 초기화 및 앱 잠금 동작에 대한 자세한 내용은 [보안 동작](#)을 참조하십시오.

참고:

트리거를 이벤트로 설정하는 경우 반복 간격은 자동으로 최소 1 시간으로 설정됩니다. 알림을 수신하려면 장치에서 정책 새로 고침을 수행하여 서버와 동기화해야 합니다. 일반적으로 장치는 사용자가 로그인하거나 Secure Hub 를 통해 수동으로 정책을 새로 고칠 때 서버와 동기화됩니다.

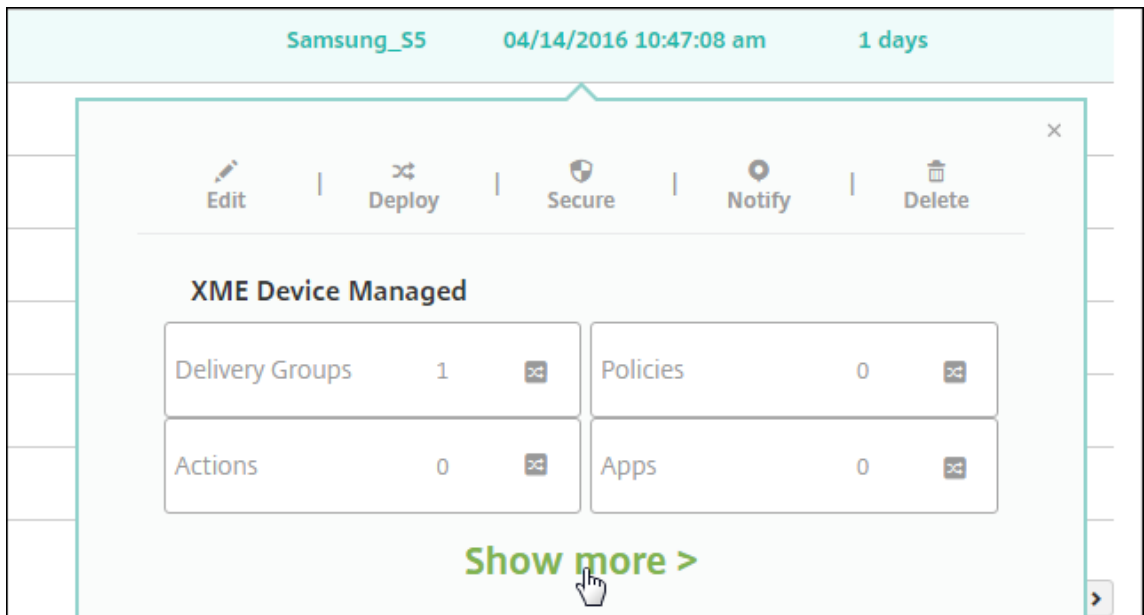
Active Directory 데이터베이스가 XenMobile 과 동기화될 수 있도록 동작이 수행되기 전에 약 1 시간의 추가 지연이 발생할 수 있습니다.



6. 배포 규칙을 구성하고 다음을 클릭합니다.
7. 배달 그룹 할당 및 배포 일정을 구성하고 다음을 클릭합니다.
8. 저장을 클릭합니다.

앱 잠금 또는 앱 초기화 상태를 확인하려면

1. 관리 > 장치로 이동하고 장치를 클릭한 후 자세히 표시를 클릭합니다.



2. 장치 앱 초기화 및 장치 앱 잠금으로 스크롤합니다.

Device details	
1 General	WiFi MAC Address: NONE Bluetooth MAC Address: NONE Device Ownership: <input type="radio"/> Corporate <input type="radio"/> BYOD
2 Properties	
3 User Properties	
4 Assigned Policies	
5 Apps	
6 Actions	
7 Delivery Groups	
8 Certificates	
9 Connections	
10 TouchDown	
	Security Strong ID: YEMXRMSG Full Wipe of Device: No device wipe. Selective Wipe of Device: No device selective wipe. Lock Device: No device lock. Device locate: No device locate. <div> Device App Wipe: No device App Wipe. Device App Lock: App Lock was requested at 04/15/2016 01:59:47 pm. </div>

장치가 초기화되면 PIN 코드를 입력하라는 메시지가 표시됩니다. 사용자가 코드를 잊은 경우 장치 세부 정보에서 코드를 조회할 수 있습니다.

모니터링 및 지원

March 15, 2024

XenMobile 대시보드 및 XenMobile 지원 페이지를 사용하여 XenMobile Server 를 모니터링하고 문제를 해결할 수 있습니다. XenMobile 지원 페이지를 사용하여 지원 관련 정보 및 도구에 액세스합니다.

온-프레미스 XenMobile Server 의 경우 XenMobile CLI 에서도 동작을 수행할 수 있습니다. 자세한 내용은 [CLI\(명령줄 인터페이스\) 옵션](#)을 참조하십시오.

XenMobile 콘솔에서 오른쪽 위 모서리의 렌치 아이콘을 클릭합니다.



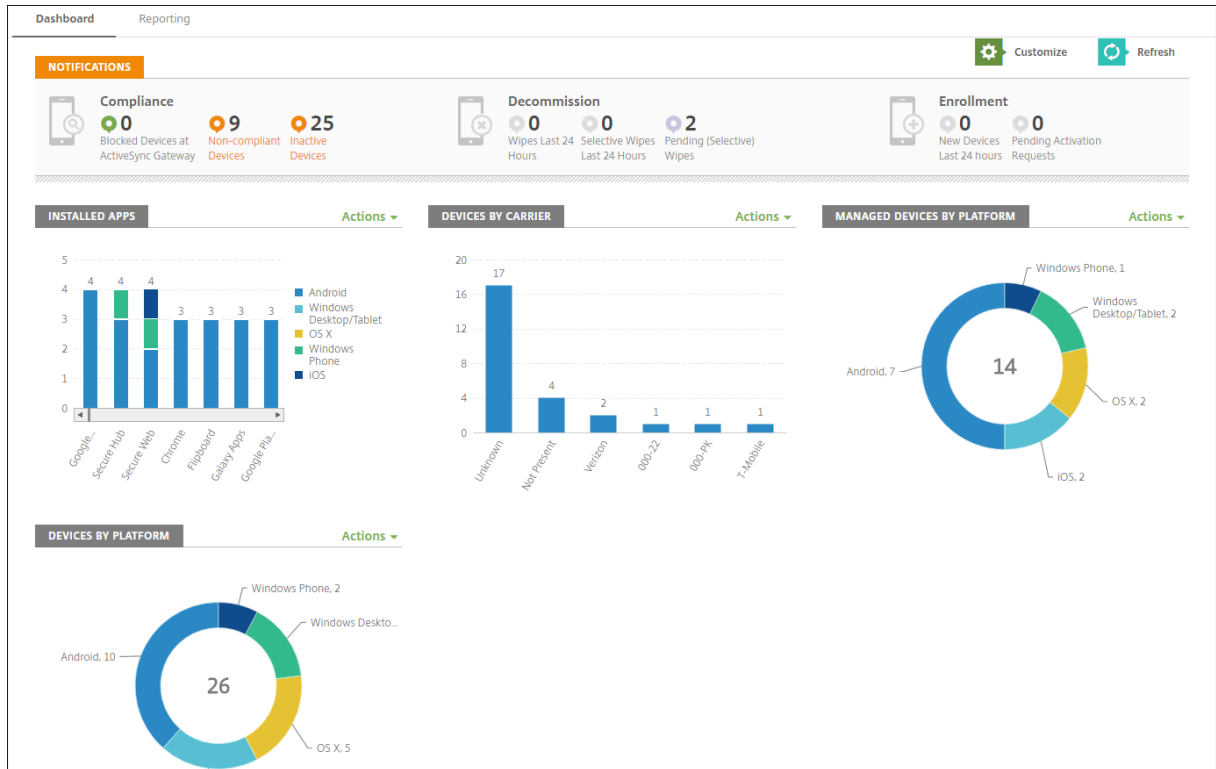
문제 해결 및 지원 페이지가 표시됩니다.

XenMobile 지원 페이지를 사용하여 다음을 수행합니다.

- 진단 액세스

- 지원 번들 만들기 (온-프레미스 설치에만 해당)
- Citrix 제품 설명서 및 Knowledge Center 에 대한 링크 액세스
- 로그 작업 액세스
- 고급 구성 옵션 사용
- 도구 및 유틸리티 집합 액세스

또한 XenMobile 콘솔 대시보드에 액세스하여 정보를 한 눈에 볼 수 있습니다. 이러한 정보를 사용하면 위젯을 통해 신속하게 문제점과 성공 여부를 확인할 수 있습니다.



대시보드는 일반적으로 XenMobile 콘솔에 로그인할 때 처음 나타나는 페이지입니다. 콘솔의 다른 곳에서 대시보드에 액세스하려면 분석을 클릭합니다. 페이지의 레이아웃을 편집하고 나타나는 위젯을 편집하려면 대시보드에서 사용자 지정을 클릭합니다.

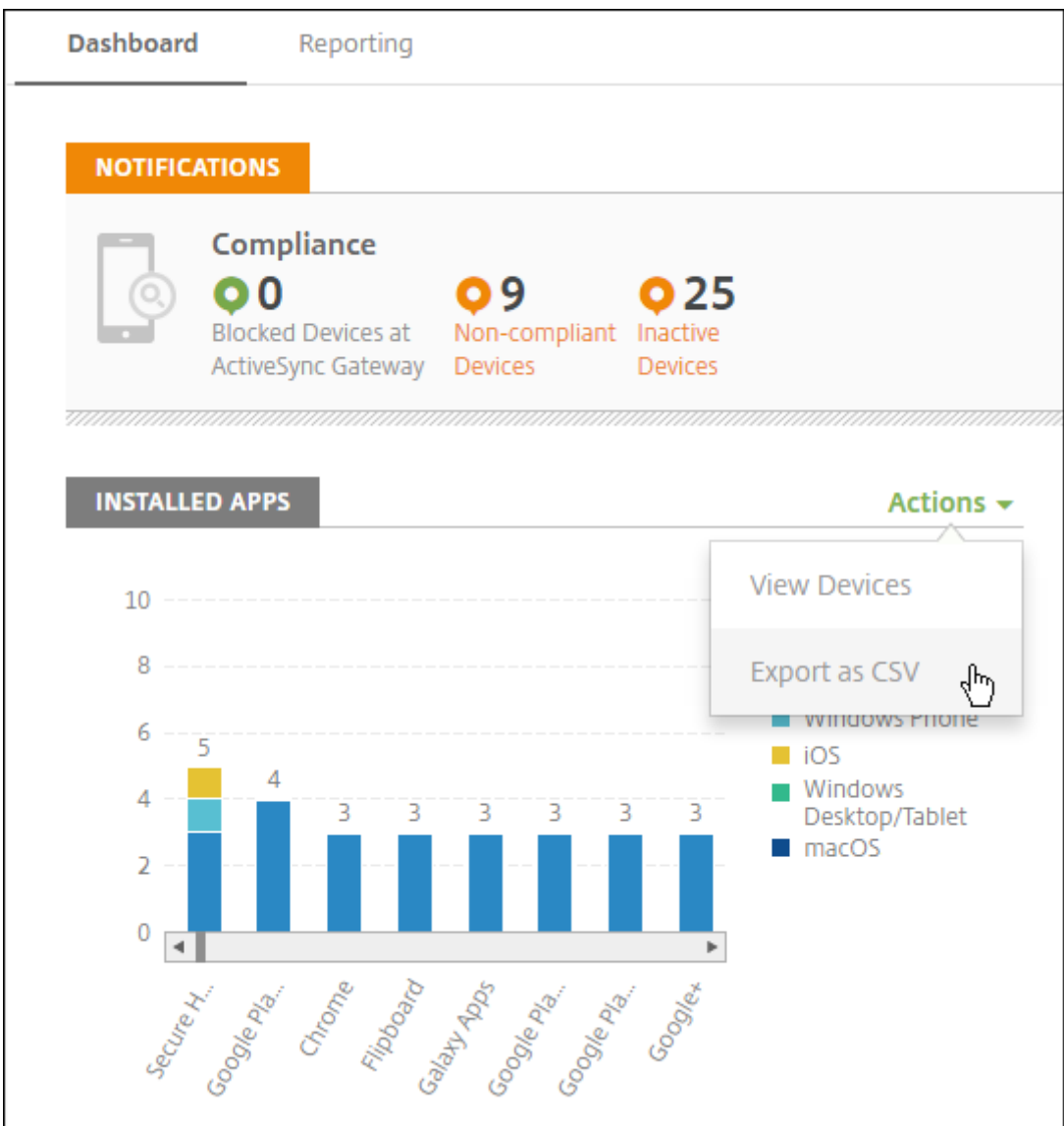
- **내 대시보드:** 최대 네 개의 대시보드를 저장할 수 있습니다. 이러한 대시보드를 개별적으로 편집하고 저장된 대시보드를 선택하여 각 대시보드를 볼 수 있습니다.
- **레이아웃 스타일:** 이 행에서는 대시보드에 표시되는 위젯 수와 위젯 배치 방법을 선택할 수 있습니다.
- **위젯 선택:** 대시보드에 표시할 정보를 선택할 수 있습니다.
 - **알림:** 왼쪽의 숫자 위에 있는 확인란을 선택하여 위젯 위에 알림 표시줄을 추가합니다. 이 표시줄에는 규격 장치, 비활성 장치 및 지난 24 시간 동안 초기화되거나 등록된 장치의 수가 표시됩니다.
 - **장치 (플랫폼 기준):** 플랫폼별로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다.
 - **장치 (이동 통신 사업자 기준):** 이동 통신 사업자별로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다. 각 표시줄을 클릭하여 플랫폼별 분석을 볼 수 있습니다.
 - **관리되는 장치 (플랫폼 기준):** 플랫폼별로 관리되는 장치의 수를 표시합니다.

- 관리되지 않는 장치 (플랫폼 기준): 플랫폼별로 관리되지 않는 장치의 수를 표시합니다. 이 차트에 나타나는 장치는 에이전트가 설치되어 있지만 권한이 해제되었거나 초기화되었을 수 있습니다.
- 장치 (ActiveSync Gateway 상태 기준): ActiveSync Gateway 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 차단됨, 허용됨 또는 알 수 없음 상태가 표시됩니다. 각 표시줄을 클릭하여 플랫폼별로 데이터를 분류할 수 있습니다.
- 장치 (소유권 기준): 소유권 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 회사 소유, 직원 소유 또는 알 수 없는 소유권 상태가 표시됩니다.
- 실패한 배달 그룹 배포: 패키지당 실패한 배포의 총 수를 표시합니다. 배포에 실패한 패키지만 나타납니다.
- 장치 (차단된 이유 기준): ActiveSync 에 의해 차단된 장치의 수를 표시합니다.
- 설치된 앱: 앱 정보의 그래프에 대한 앱 이름을 입력합니다.
- 볼륨 구매 앱 라이선스 사용 현황: Apple 볼륨 구매 앱에 대한 라이선스 사용 현황 통계를 표시합니다.

각 위젯에서 개별 부분을 클릭하여 자세한 정보를 드릴다운할 수 있습니다.



또한 동작 메뉴를 클릭하여 정보를.csv 파일로 내보낼 수도 있습니다.

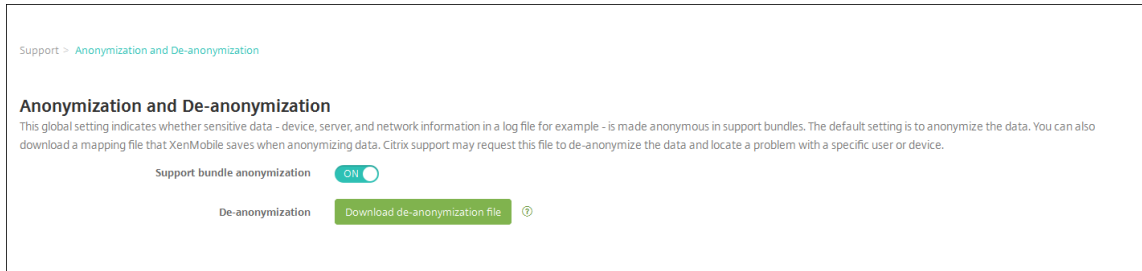


지원 번들의 데이터 익명화

August 24, 2018

XenMobile 에서 지원 번들을 만드는 경우 중요한 사용자, 서버 및 네트워크 데이터가 기본적으로 익명으로 만들어집니다. 익명화 및 익명화 취소 페이지에서 이 동작을 변경할 수 있습니다. 또한 데이터를 익명화할 때 XenMobile 이 저장하는 매핑 파일을 다운로드할 수도 있습니다. Citrix 지원에서 데이터의 익명화를 취소하고 특정 사용자 또는 장치의 문제를 찾기 위해 이 파일을 요청할 수 있습니다.

1. XenMobile 콘솔에서 오른쪽 위 모서리의 런치 아이콘을 클릭합니다. 지원 페이지가 나타납니다.
2. 지원 페이지에서 고급 아래에 있는 익명화 및 익명화 취소를 클릭합니다. 익명화 및 익명화 취소 페이지가 나타납니다.



3. 지원 번들 익명화에서 데이터를 익명화할지 여부를 선택합니다. 기본값은 켜짐입니다.
4. 익명화 취소 옆에서 익명화 취소 파일 다운로드를 클릭하여 문제 진단을 위해 특정 장치 또는 사용자 정보가 필요할 경우 Citrix 지원에 보낼 매핑 파일을 다운로드합니다.

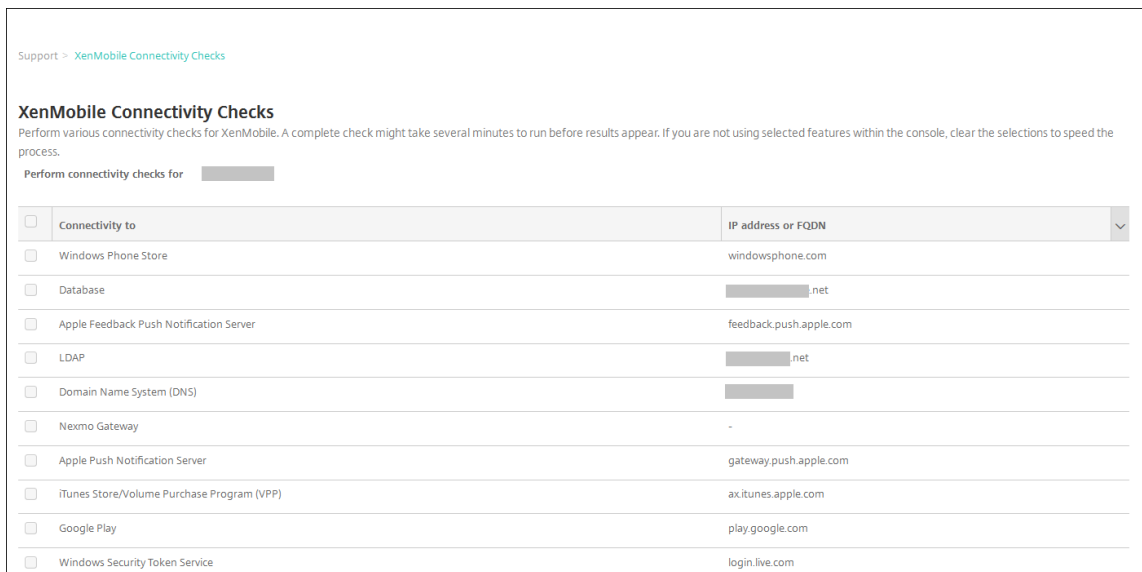
연결 확인

December 1, 2020

XenMobile 지원 페이지에서 Citrix Gateway 및 기타 서버/위치에 대한 XenMobile 연결을 확인할 수 있습니다.

XenMobile 연결 확인 수행

1. XenMobile 콘솔에서 오른쪽 위 모서리의 렌치 아이콘을 클릭합니다. 지원 페이지가 나타납니다.
2. 진단 아래에서 **XenMobile** 연결 확인을 클릭합니다. **XenMobile** 연결 확인 페이지가 나타납니다. XenMobile 환경에 클러스터된 노드가 포함되는 경우 모든 노드가 표시됩니다.



3. 연결 테스트에 포함할 서버를 선택한 후 연결 테스트를 클릭합니다. 테스트 결과 페이지가 나타납니다.

XenMobile Connectivity Checks
Perform various connectivity checks for XenMobile. A complete check might take several minutes to run before results appear. If you are not using selected features within the console, clear the selections to speed the process.
Perform connectivity checks for 10.

<input type="checkbox"/>	Connectivity to	IP address or FQDN	
<input type="checkbox"/>	Database	net	✓
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	✓

Showing 1 - 2 of 2 items

Clear ResultsTest Connectivity

- 테스트 결과 테이블에서 서버를 선택하여 해당 서버에 대한 자세한 결과를 확인합니다.

	IP address or FQDN
	.net

Successful Connection
Connectivity results for '10. .net'
net
Server is reachable.
Port 1433/TCP is open.
Server is a valid database server.

Citrix Gateway 연결 확인 수행


- 지원 페이지의 진단 아래에서 **Citrix Gateway** 연결 확인을 클릭합니다. **Citrix Gateway** 연결 확인 페이지가 나타납니다. Citrix Gateway 서버를 추가하지 않은 경우 테이블은 비어 있습니다.

Troubleshooting and Support > Citrix Gateway Connectivity Checks

Citrix Gateway Connectivity Checks

Perform various connectivity checks for Citrix Gateway. A complete check might take several minutes to run before results appear.

Test connectivity to the following Citrix Gateway server(s)

 Add

<input type="checkbox"/>	IP	User name
--------------------------	----	-----------

No results found.

Test Connectivity

2. 추가를 클릭합니다. **Citrix Gateway** 서버 추가 대화 상자가 나타납니다.

Add Citrix Gateway Server

Citrix Gateway Management IP *

User name *

Password *

Cancel

Add

3. **Citrix Gateway** 관리 IP 에서 테스트하려는 Citrix Gateway 가 실행되는 서버의 관리 IP 주소를 입력합니다.

참고:

이전에 이미 추가된 Citrix Gateway 서버에 대한 연결 확인을 수행하는 경우 해당 IP 주소가 제공됩니다.

4. 이 Citrix Gateway 의 관리자 자격 증명을 입력합니다.

참고:

이전에 이미 추가된 Citrix Gateway 서버에 대한 연결 확인을 수행하는 경우 해당 사용자 이름이 제공됩니다.

5. 추가를 클릭합니다. Citrix Gateway 가 **Citrix Gateway** 연결 확인 페이지의 테이블에 추가됩니다.
6. Citrix Gateway 서버를 선택한 후에 연결 테스트를 클릭합니다. 테스트 결과 테이블에 결과가 표시됩니다.
7. 테스트 결과 테이블에서 서버를 선택하여 해당 서버에 대한 자세한 결과를 확인합니다.

사용자 환경 개선 프로그램

January 5, 2022

Citrix CEIP(사용자 환경 개선 프로그램)는 XenMobile에서 익명의 구성 및 사용 현황 데이터를 수집하여 Citrix에 보냅니다. 이 데이터는 Citrix가 XenMobile의 품질, 안정성 및 성능을 개선하는 데 도움이 됩니다. CEIP 참여는 전적으로 자발적입니다. XenMobile을 처음 설치하거나 업데이트를 설치할 때 CEIP 참여를 선택할 수 있습니다. 참여하는 경우 일반적으로 주 단위로 데이터가 수집되며 성능 및 사용 현황 데이터는 매 시간 수집됩니다. 데이터는 디스크에 저장되고 HTTPS를 통해 안전하게 Citrix로 매주 전송됩니다. XenMobile 콘솔에서 CEIP 참여 여부를 변경할 수 있습니다. CEIP에 대한 자세한 내용은 [About the Citrix Customer Experience Improvement Program \(CEIP\)](#)(Citrix CEIP(사용자 환경 개선 프로그램) 정보)를 참조하십시오.

CEIP 참여 선택

XenMobile을 처음 설치하거나 업데이트를 수행하면 참여할지를 묻는 다음 대화 상자가 표시됩니다.


Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

[Learn more](#)



The diagram illustrates the data flow for the CEIP program. It shows three stylized human figures on the left, representing users. A blue arrow points from the users to the Citrix logo on the right. A green arrow points from the Citrix logo back to the users, forming a circular loop that signifies a continuous process of data collection and feedback.

Would you like to help make Citrix products better by joining the program?
(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)

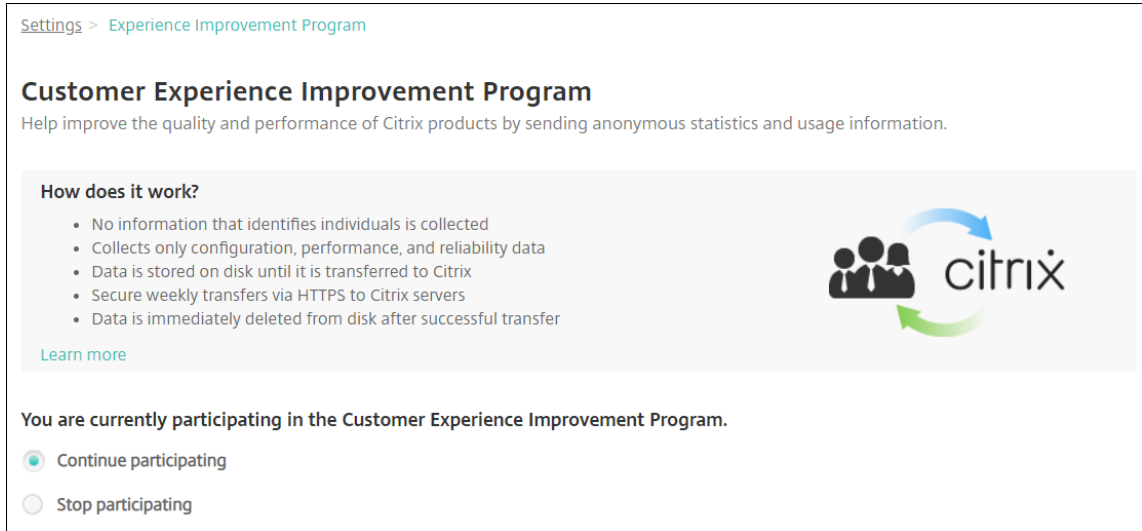
☒ **Yes, send anonymous usage and statistics information.**

☐ **No**

CancelSave

CEIP 참여 설정 변경

1. CEIP 참여 설정을 변경하려면 XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭하여 설정 페이지를 엽니다.
2. 서버에서 환경 개선 프로그램을 클릭합니다. 사용자 환경 개선 프로그램 페이지가 나타납니다. 표시되는 정확한 페이지는 현재 CEIP 참여 여부에 따라 다릅니다.



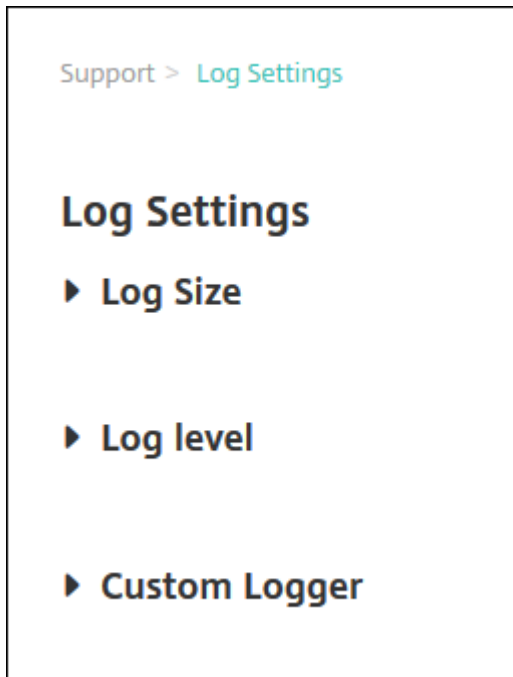
3. 현재 CEIP에 참여 중이고 참여를 중지하려는 경우 참여 중지를 클릭합니다.
4. 현재 CEIP에 참여하고 있지 않고 참여를 시작하려는 경우 참여 시작을 클릭합니다.
5. 저장을 클릭합니다.

로그

January 6, 2020

XenMobile에서 생성하는 로그 출력을 사용자 지정하도록 로그 설정을 구성할 수 있습니다. 클러스터된 XenMobile 서버가 있는 경우 XenMobile 콘솔에서 로그 설정을 구성하면 해당 설정이 클러스터의 다른 모든 서버와 공유됩니다.

1. XenMobile 콘솔에서 오른쪽 위 모서리의 렌치 아이콘을 클릭합니다. 지원 페이지가 나타납니다.
2. 로그 작업 아래에서 로그 설정을 클릭합니다. 로그 설정 페이지가 나타납니다.



로그 설정 페이지에서 다음과 같은 옵션에 액세스할 수 있습니다.

- 로그 크기. 이 옵션을 사용하여 로그 파일의 크기와 데이터베이스에 유지되는 최대 로그 백업 파일 수를 제어합니다. 로그 크기는 XenMobile 에서 지원하는 각 로그 (디버그 로그, 관리자 작업 로그 및 사용자 작업 로그) 에 적용됩니다.
- 로그 수준. 이 옵션을 사용하여 로그 수준을 변경하거나 설정을 유지할 수 있습니다.
- 사용자 지정 로거. 이 옵션을 사용하여 사용자 지정 로거를 만듭니다. 사용자 지정 로그에는 클래스 이름과 로그 수준이 필요합니다.

로그 크기 옵션을 구성하려면

1. 로그 설정 페이지에서 로그 크기를 확장합니다.

[Support](#) > [Log Settings](#)

Log Settings

▼ Log Size

Debug log file size (MB)	10
Maximum number of debug backup files	50
Admin activity log file size (MB)	10
Maximum number of admin activity backup files	300
User activity log file size (MB)	10
Maximum number of user activity backup files	600

2. 다음 설정을 구성합니다.

- 디버그 로그 파일 크기 **(MB)**: 목록에서 5MB 에서 20MB 사이의 크기를 클릭하여 디버그 파일의 최대 크기를 변경합니다. 기본 파일 크기는 **10MB** 입니다.
- 디버그 백업 파일의 최대 수: 목록에서 서버가 유지하는 디버그 파일의 최대 수를 클릭합니다. 기본적으로 XenMobile 은 서버에 50 개의 백업 파일을 유지합니다.
- 관리자 작업 로그 파일 크기 **(MB)**: 목록에서 5MB 에서 20MB 사이의 크기를 클릭하여 관리자 작업 로그 파일의 최대 크기를 변경합니다. 기본 파일 크기는 **10MB** 입니다.
- 관리자 작업 백업 파일의 최대 수: 목록에서 서버가 유지하는 관리자 작업 파일의 최대 수를 클릭합니다. 기본적으로 XenMobile 은 서버에 300 개의 백업 파일을 유지합니다.
- 사용자 작업 로그 파일 크기 **(MB)**: 목록에서 5MB 에서 20MB 사이의 크기를 클릭하여 사용자 작업 로그 파일의 최대 크기를 변경합니다. 기본 파일 크기는 **10MB** 입니다.
- 사용자 작업 백업 파일의 최대 수: 목록에서 서버가 유지하는 사용자 작업 파일의 최대 수를 클릭합니다. 기본적으로 XenMobile 은 서버에 300 개의 백업 파일을 유지합니다.

로그 수준 옵션을 구성하려면

로그 수준을 사용하여 XenMobile 이 로그에서 수집하는 정보의 유형을 지정할 수 있습니다. 모든 사례에 대해 동일한 수준을 설정하거나 개별 사례를 특정 수준으로 설정할 수 있습니다.



1. 로그 설정 페이지에서 로그 수준을 확장합니다. 모든 로그 클래스의 테이블이 나타납니다.

Support > Log Settings

Log Settings

▶ Log Size

▼ Log level

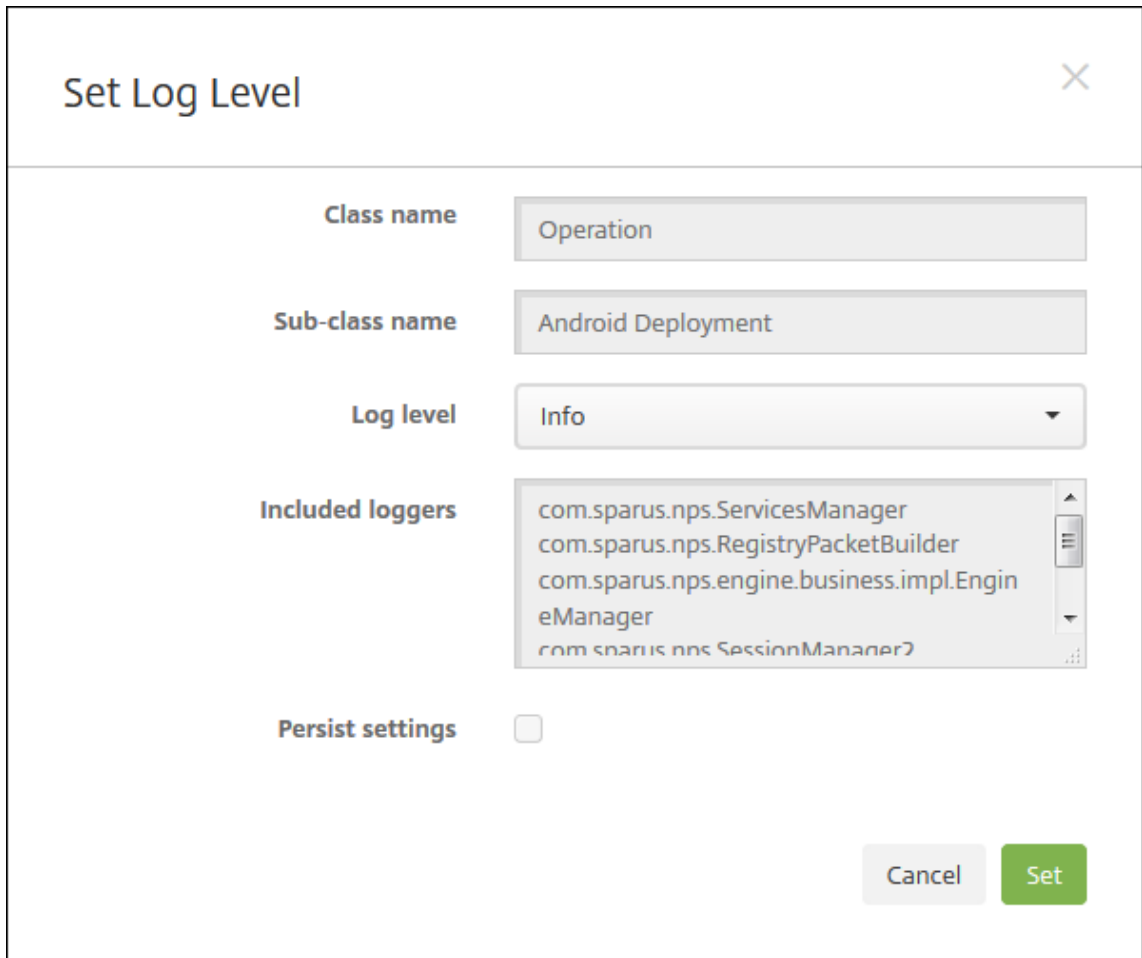
 Edit all |  Reset

<input type="checkbox"/>	Class	Sub-class	Log level	▼
<input type="checkbox"/>	Data Access	All	Info	
<input type="checkbox"/>	Data Access	XDM	Info	
<input type="checkbox"/>	Data Access	XAM	Info	
<input type="checkbox"/>	Data Access	Console	Info	
<input type="checkbox"/>	Data Access	OCA	Info	
<input type="checkbox"/>	IMI Services	All	Info	
<input type="checkbox"/>	IMI Services	Category Service	Info	
<input type="checkbox"/>	IMI Services	OPN Service	Info	

2. 다음 중 하나를 수행합니다.

- 원하는 클래스 옆에 있는 확인란을 클릭한 다음 수준 설정을 클릭하여 해당 클래스의 로그 수준을 변경합니다.
- 모두 편집을 클릭하여 로그 수준 변경 내용을 테이블의 모든 클래스에 적용합니다.

로그 수준을 설정하고 XenMobile 서버를 다시 부팅할 때 로그 수준 설정을 유지할지 여부를 선택할 수 있는 로그 수준 설정 대화 상자가 나타납니다.



The dialog box titled "Set Log Level" contains the following fields and controls:

- Class name:** A text input field containing "Operation".
- Sub-class name:** A text input field containing "Android Deployment".
- Log level:** A dropdown menu currently set to "Info".
- Included loggers:** A list box containing the following loggers:
 - com.sparus.nps.ServicesManager
 - com.sparus.nps.RegistryPacketBuilder
 - com.sparus.nps.engine.business.impl.EngineManager
 - com.sparus.nps.SessionManager2
- Persist settings:** An unchecked checkbox.
- Buttons:** "Cancel" and "Set" buttons at the bottom right.

- **클래스 이름:** 모든 클래스의 로그 수준을 변경할 때에는 이 필드에 '모두'가 표시되지만, 그렇지 않은 경우에는 개별 클래스 이름이 표시됩니다. 이 필드는 편집할 수 없습니다.
- **하위 클래스 이름:** 모든 클래스의 로그 수준을 변경할 때에는 이 필드에 '모두'가 표시되지만, 그렇지 않은 경우에는 개별 클래스의 하위 클래스 이름이 표시됩니다. 이 필드는 편집할 수 없습니다.
- **로그 수준:** 목록에서 로그 수준을 클릭합니다. 지원되는 로그 수준은 다음과 같습니다.
 - 심각
 - 오류
 - 경고
 - 정보
 - 디버그
 - 추적
 - 꺼짐
- **포함된 로거:** 모든 클래스의 로그 수준을 변경하는 경우에는 이 필드가 비어 있지만 개별 클래스의 경우에는 현재 구성된 로거가 표시됩니다. 이 필드는 편집할 수 없습니다.
- **설정 유지:** 서버를 다시 부팅할 때 로그 수준 설정을 유지하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 서버를 다시 부팅할 때 로그 수준 설정이 기본값으로 되돌아갑니다.

3. 설정을 클릭하여 변경 내용을 커밋합니다.

사용자 지정 로거를 추가하려면

1. 로그 설정 페이지에서 사용자 지정 로거를 확장합니다. 사용자 지정 로거 테이블이 나타납니다. 사용자 지정 로거를 추가하지 않은 경우에는 테이블이 비어 있습니다.

Support > Log Settings

Log Settings

- ▶ Log Size
- ▶ Log level
- ▼ Custom Logger

Add

Set Level

Delete

<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

Showing 1 - 2 of 2 items

2. 추가를 클릭합니다. 사용자 지정 로거 추가 대화 상자가 나타납니다.

Add custom logger

Class name

Custom

Log level

Fatal

Included loggers

Cancel

Add

3. 다음 설정을 구성합니다.

- 클래스 이름: 이 필드에는 사용자 지정이 표시됩니다. 이 필드는 편집할 수 없습니다.
- 로그 수준: 목록에서 로그 수준을 클릭합니다. 지원되는 로그 수준은 다음과 같습니다.
 - 심각
 - 오류
 - 경고
 - 정보
 - 디버그
 - 추적
 - 꺼짐
- 포함된 로거: 사용자 지정 로거에 포함시키려는 특정 로거를 입력하거나 모든 로거를 포함시키려면 필드를 비워 둡니다.

4. 추가를 클릭합니다. 사용자 지정 로거가 사용자 지정 로거 테이블에 추가됩니다.

Custom Logger				
<div> <div>Add</div> <div>→ Set Level</div> <div>Delete</div> </div>				
<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

사용자 지정 로거를 삭제하려면

1. 로그 설정 페이지에서 사용자 지정 로거를 확장합니다.
2. 삭제할 사용자 지정 로거를 선택합니다.
3. 삭제를 클릭합니다. 사용자 지정 로거를 삭제할지 묻는 대화 상자가 나타납니다. 확인을 클릭합니다.

중요:

이 작업은 실행 취소할 수 없습니다.

모바일 서비스 공급자

January 6, 2020

XenMobile 에서 모바일 서비스 공급자 인터페이스를 사용하여 BlackBerry 및 Exchange ActiveSync 장치를 쿼리하고 작업을 실행할 수 있습니다.

예를 들어 조직에 1,000 명의 사용자가 있고 각 사용자가 하나 이상의 장치를 사용할 수 있습니다. 모든 사용자에게 관리를 위해 XenMobile 에 장치를 등록해야 한다고 알린 후 XenMobile 콘솔에 사용자가 등록한 장치 수가 나타납니다. 이 설정을 구성하면 Exchange Server 에 연결한 장치 수를 확인할 수 있습니다. 이 방법으로 다음을 수행할 수 있습니다.

- 특정 사용자가 장치를 등록해야 하는지 여부를 확인할 수 있습니다.
- Exchange Server 에 연결하는 사용자 장치에 데이터 초기화와 같은 명령을 실행할 수 있습니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 모바일 서비스 공급자를 클릭합니다. 모바일 서비스 공급자 페이지가 나타납니다.

Mobile Service Provider

Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

Web service URL*

User name*

Password*

Automatically update BlackBerry and ActiveSync device connections

☐ OFF

Test Connection

Cancel

Save

3. 다음 설정을 구성합니다.

- 웹 서비스 **URL**: 웹 서비스의 URL 을 입력합니다 (예: <https://<XmmServer>/services/xdmservice>).
- 사용자 이름: domain\admin 형식으로 사용자 이름을 입력합니다.
- 암호: 암호를 입력합니다.
- **BlackBerry** 및 **ActiveSync** 장치 연결 자동 업데이트: 장치 연결을 자동으로 업데이트할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 연결 테스트를 클릭하여 연결을 확인합니다.

4. 저장을 클릭합니다.

보고서

March 15, 2024

XenMobile 은 앱 및 장치 배포를 분석하는 데 사용할 수 있는 미리 정의된 보고서를 제공합니다. 각 보고서는 표와 차트로 표시됩니다. 열을 기준으로 표를 정렬하고 필터링할 수 있습니다. 차트의 특정 요소를 선택하여 더 자세한 정보를 볼 수 있습니다.

- 앱 배포 총 시도 횟수: 사용자가 자신의 장치에 설치하려고 시도한 배포된 앱을 나열합니다.
- 플랫폼별 앱: 앱과 앱 버전을 장치 플랫폼 및 버전별로 나열합니다.
- 유형별 앱: 버전, 유형 및 범주별로 앱을 나열합니다.
- 장치 등록: 등록된 모든 장치를 나열합니다.
- 장치 및 앱: 관리되는 앱을 실행 중인 장치를 나열합니다.
- 비활성 장치: XenMobile Server 속성 device.inactivity.days.threshold 로 지정된 일 수 동안 활동이 없었던 장치의 목록입니다.
- 탈옥/루팅 장치: 탈옥 iOS 장치 및 루팅 Android 장치를 나열합니다.

- **약관:** 약관 계약에 동의 및 거부한 사용자를 나열합니다. 차트 일부를 선택하여 더 자세히 볼 수 있습니다.
- **상위 10 개 앱:** 배포에 실패한 앱을 10 개까지 나열합니다.
- **장치 및 사용자의 블랙리스트 앱:** 사용자의 장치에 있는 차단된 앱을 나열합니다.

참고:

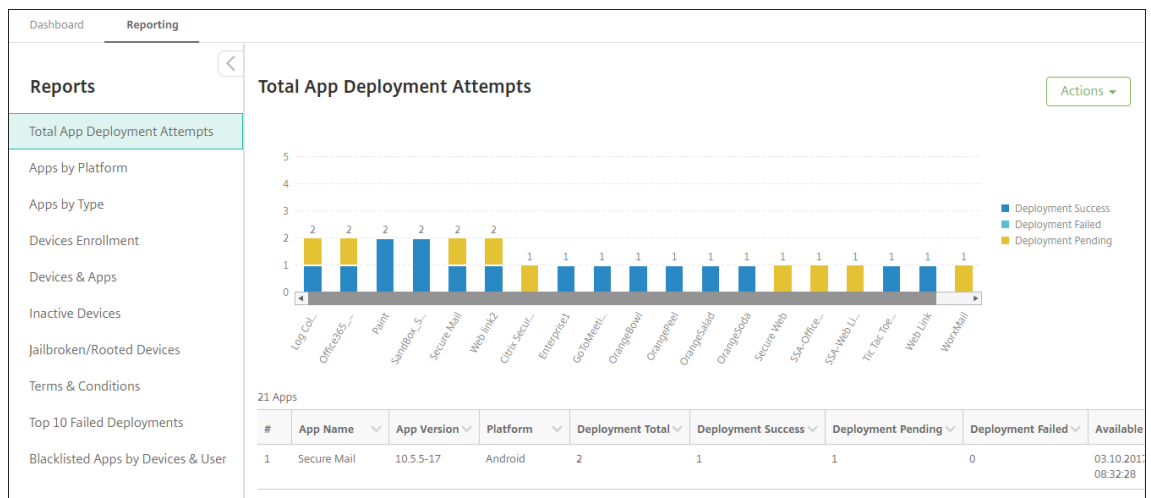
XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는 용어가 포함됩니다. 향후 릴리스에서 이러한 용어를 “차단 목록” 및 “허용 목록” 으로 변경하는 중입니다.

- **규정을 준수하지 않는 장치:** 장치의 탈옥 여부, OS 버전 실행 여부, 장치에 암호가 있는지 여부와 같은 규정 준수 기준을 충족하지 않는 장치를 나열합니다.

각 표의 데이터를.csv 형식으로 내보낼 수 있으며 Microsoft Excel 과 같은 프로그램을 사용하여 열 수 있습니다. 각 보고서의 차트를 PDF 형식으로 내보낼 수 있습니다.

보고서를 생성하려면

1. XenMobile 콘솔에서 분석 > 보고를 클릭합니다. 보고 페이지가 나타납니다.
2. 생성할 보고서를 클릭합니다.



보고서의 더 상세한 정보를 보려면

1. 자세히 볼 차트 부분을 클릭하면 상세 정보가 표시됩니다.



표 열을 정렬, 필터링 또는 검색하려면 열 머리글을 클릭합니다

Dashboard Reporting

Reports

- Total App Deployment Attempts
- Apps by Platform
- Apps by Type
- Devices Enrollment
- Devices & Apps
- Inactive Devices
- Jailbroken/Rooted Devices
- Terms & Conditions
- Top 10 Failed Deployments
- Blacklisted Apps by Devices & User

22 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Enterprise1	↑ Sort Ascending		1	1	0	0	03.10.2017 09:10:10
2	SandBox_S	↓ Sort Descending		1	1	0	0	03.10.2017 08:38:40
3	Fonts	Filter with secure X		1	0	1	0	03.10.2017 09:45:07
4	SandBox_S	<input type="checkbox"/> Secure Web		1	1	0	0	03.10.2017 08:38:40
5	GoToMeeti	Filter		1	1	0	0	03.10.2017 12:34:35
6	Secure Mail	10.5.5-17	Android	1	1	0	0	03.10.2017 08:32:28
7	GreedyPenguins		Windows Mobile	1	1	0	0	03.10.2017 13:01:50

보고서를 날짜로 필터링하려면

1. 열 머리글을 클릭하면 필터 설정이 표시됩니다.

Dashboard

Reporting

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:07	↑ Sort Ascending ↓ Sort Descending		03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:07	Filter Condition is on		03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:07	Value MM / DD / YYYY		03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S

2. 필터 조건에서 보고되는 날짜를 제한할 방법을 선택합니다.

Dashboard

Reporting

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:07	↑ Sort Ascending ↓ Sort Descending		03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:07	Filter Condition is on is on is on or before is on or after between		03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:07			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S

3. 날짜 선택기를 사용하여 날짜를 지정합니다.

Dashboard

Reporting

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:07	↑ Sort Ascending ↓ Sort Descending		03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:07	Filter Condition is on or before		03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:07	Value MM / DD / YYYY		03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	April 2017		03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27			09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:55:27			09.27.2016 04:48:39	Unknown		SUCCESS	Jota Text Editor

4. 날짜 필터가 있는 열이 다음 예제처럼 표시됩니다.

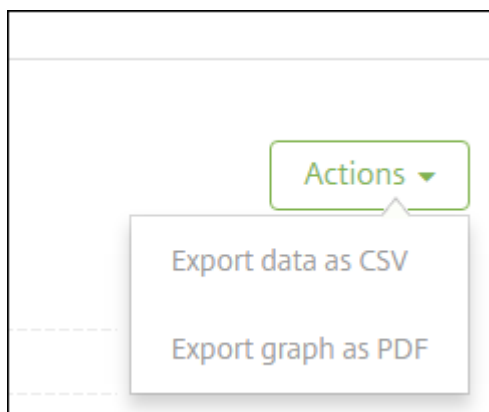
Dashboard		Reporting							
Reports									
Total App Deployment Attempts									
Apps by Platform									
Apps by Type									
Devices Enrollment									
Devices & Apps									
Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name	
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_5	
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito	

5. 필터를 제거하려면 열 머리글을 클릭한 다음 필터 제거를 클릭합니다.

Dashboard		Reporting							
Reports									
Total App Deployment Attempts									
Apps by Platform									
Apps by Type									
Devices Enrollment									
Devices & Apps									
Inactive Devices									
Jailbroken/Rooted Devices									
Terms & Conditions									
Top 10 Failed Deployments									
Blacklisted Apps by Devices & User									
Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name	
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_5	
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito	
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre	
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link	

차트 또는 표를 내보내려면

- 차트를 PDF 형식으로 내보내려면 동작, **PDF** 로 그래프 내보내기를 차례로 클릭합니다.
- 표 데이터를 CSV 형식으로 내보내려면 동작, **CSV** 로 데이터 내보내기를 차례로 클릭합니다.



중요:

SQL Server 를 사용하여 사용자 지정 보고서를 만들 수 있지만 이 방법은 권장하지 않습니다. Citrix 는 스키마를 게시하지 않으며 알림 없이 스키마를 변경할 수 있습니다. 이 방법의 보고를 사용하기로 결정한 경우 읽기 전용 계정을 사용

하여 SQL 쿼리를 실행해야 합니다. 여러 조인이 포함되어 실행에 시간이 다소 걸리는 쿼리는 그 시간 동안 XenMobile Server 성능에 영향을 미칠 수 있습니다.

SNMP 모니터링

March 15, 2024

XenMobile Server 에서 SNMP 모니터링을 사용하도록 설정하여 모니터링 시스템이 XenMobile 노드를 쿼리하고 노드의 정보를 가져오도록 허용할 수 있습니다. 쿼리에는 프로세서 로드, 로드 평균, 메모리 사용 현황 및 연결 같은 매개 변수가 사용됩니다. 인증 및 암호화 사양을 비롯하여 SNMP v3 에 대한 자세한 내용은 [RFC 3414](#)에 대한 공식 SNMP 설명서를 참조하십시오.

참고:

SNMP v3 모니터링은 XenMobile Server 10.8 이상에서 지원됩니다.

SCOM 과 같은 SNMP 모니터링을 지원하는 다양한 모니터링 응용 프로그램을 사용할 수 있습니다. SCOM 구성에 대한 자세한 내용은 이 [Citrix Support Knowledge Center 문서](#)를 참조하십시오.

사전 요구 사항

다음 TCP 포트를 구성합니다.

- 포트 **161(UDP)**: UDP 프로토콜을 사용하는 SNMP 트래픽에 사용됩니다. 원본은 SNMP 관리자이고 대상은 XenMobile 입니다.
- 포트 **162(UDP)**: XenMobile 의 SNMP 트랩 알림을 SNMP 관리자로 보내는 데 사용됩니다. 원본은 XenMobile 이고 대상은 SNMP 관리자입니다.

XenMobile 포트 구성에 대한 자세한 내용은 [포트 요구 사항](#)을 참조하십시오.

SNMP 를 포함하는 온-프레미스 XenMobile 배포의 아키텍처 다이어그램은 [온-프레미스 배포용 참조 아키텍처](#)를 참조하십시오.

SNMP 를 설정하는 일반적인 단계는 다음과 같습니다.

1. 사용자 추가: 사용자는 트랩을 수신하고 XenMobile Server 를 모니터링할 수 있는 권한을 상속합니다.
2. 트랩을 수신할 **SNMP** 관리자 추가: 트랩은 XenMobile 노드가 사용자 정의된 최대 임계값을 초과할 경우 XenMobile 에서 생성되는 알림입니다.
3. **XenMobile** 과 상호 작용하도록 **SNMP** 관리자 구성: XenMobile Server 는 특정 MIB(관리 정보 데이터베이스)를 사용하여 작업을 수행합니다. MIB 는 XenMobile 콘솔의 설정 > **SNMP** 구성 페이지에서 다운로드합니다. 그런 다음 MIB 가져오기 도구를 사용하여 SNMP 관리자로 MIB 를 가져옵니다.

참고:

모든 SNMP 관리자에는 자체 MIB 가져오기 도구가 있습니다.

4. 트랩 사용: XenMobile 콘솔에서 트랩을 사용하도록 설정하고 환경의 요구 사항에 따라 간격 및 임계값을 정의합니다.
5. 타사 **SNMP** 관리자에서 트랩 보기: 트랩을 보려면 SNMP 관리자를 확인합니다. 그러나 일부 관리자의 경우 관리자 외부에서도 알림을 사용하도록 설정을 구성할 수 있습니다. 예를 들어 전자 메일에 알림을 표시하도록 구성할 수 있습니다.

XenMobile 에서 생성할 수 있는 트랩은 다음과 같습니다.

트랩 이름: 프로세서 로드

- 모니터링 **OID(개체 ID):** .1.3.6.1.2.1.25.3.3.1.2
- 설명: 사용자 정의된 간격마다 시스템의 CPU 로드를 모니터링합니다. 로드가 사용자 지정 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: 1 분 동안의 로드 평균

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.10.1.5.1
- 설명: 사용자 정의된 간격마다 1 분 동안 평균 시스템 로드를 모니터링합니다. 로드 평균이 사용자 지정 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: 5 분 동안의 로드 평균

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.10.1.5.2
- 설명: 사용자 정의된 간격마다 5 분 동안 평균 시스템 로드를 모니터링합니다. 로드 평균이 사용자 지정 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: 15 분 동안의 로드 평균

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.10.1.5.3
- 설명: 사용자 정의된 모든 간격마다 15 분 동안 평균 시스템 로드를 모니터링합니다. 로드 평균이 사용자 지정 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: 사용 가능한 총 메모리

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.4.11
- 설명: 사용자 정의된 모든 간격마다 사용 가능한 메모리를 모니터링합니다. 사용 가능한 메모리가 사용자 지정 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다. 참고: 사용 가능한 총 메모리에는 RAM 과 스왑 메모리 (가상 메모리) 가 모두 포함됩니다. 총 스왑 메모리를 검색하려면 SNMP OID .1.3.6.1.4.1.2021.4.3 을 사용하여 쿼리할 수 있습니다. 사용 가능한 스왑 메모리를 검색하려면 SNMP OID .1.3.6.1.4.1.2021.4.4 를 사용하여 쿼리할 수 있습니다.

트랩 이름: 사용된 총 디스크 스토리지

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.9.1.9.1

- **설명:** 사용자 정의된 모든 간격마다 시스템 디스크 스토리지를 모니터링합니다. 디스크 스토리지가 사용자 지정 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Java 힙 메모리 사용 현황

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.2.4.0
- **설명:** 사용자 정의된 모든 간격마다 XenMobile 의 JVM(Java Virtual Machine) 힙 메모리 사용 현황을 모니터링합니다. 사용 현황이 사용자 지정 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Java Metaspace 사용 현황

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.2.5.0
- **설명:** 사용자 정의된 모든 간격마다 XenMobile 의 Java Metaspace 사용 현황을 모니터링합니다. 사용 현황이 임계값을 초과하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: LDAP 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **설명:** 사용자 정의된 모든 간격마다 LDAP 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: DNS 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **설명:** 사용자 정의된 모든 간격마다 DNS 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Google 스토어 서버 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **설명:** 사용자 정의된 모든 간격마다 Google 스토어 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Windows Tab 스토어 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- **설명:** 사용자 정의된 모든 간격마다 Tab 스토어 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Windows 보안 토큰 서버 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **설명:** 사용자 정의된 모든 간격마다 Windows 보안 토큰 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Windows 알림 서버 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- 설명: 사용자 정의된 모든 간격마다 Windows 알림 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: APNs(Apple 푸시 알림 서버) 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- 설명: 사용자 정의된 모든 간격마다 APNs 와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Apple 피드백 서버 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- 설명: 사용자 정의된 모든 간격마다 Apple 피드백 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Apple Store 서버 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- 설명: 사용자 정의된 모든 간격마다 Apple Store 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: XenMobile 데이터베이스 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- 설명: 사용자 정의된 모든 간격마다 XenMobile 데이터베이스와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Firebase Cloud Messaging 서버 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- 설명: 사용자 정의된 모든 간격마다 Firebase Cloud Messaging 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Citrix 라이선스 서버 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- 설명: 사용자 정의된 모든 간격마다 Citrix 라이선스 서버와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: Citrix Gateway 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- 설명: 사용자 정의된 모든 간격마다 Citrix Gateway 와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: XenMobile 노드 간 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- 설명: 사용자 정의된 모든 간격마다 XenMobile 클러스터 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

트랩 이름: XenMobile Tomcat 노드 서비스 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- 설명: 사용자 정의된 모든 간격마다 XenMobile Tomcat 노드 서비스와 XenMobile 노드 사이의 연결을 모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을 생성합니다.

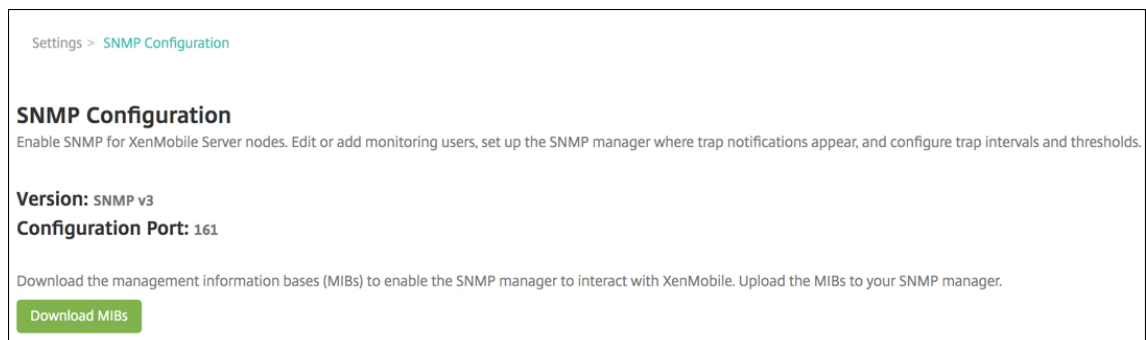
SNMP 임계값을 구성할 때 최상의 서버 성능을 유지하려면 다음 요인을 고려하십시오.

- 호출 빈도
- 수집할 트랩 데이터와 임계값 확인
- 노드 간 통신 메커니즘
- 연결 확인 빈도
- 확인 중 실패에 대한 시간 초과

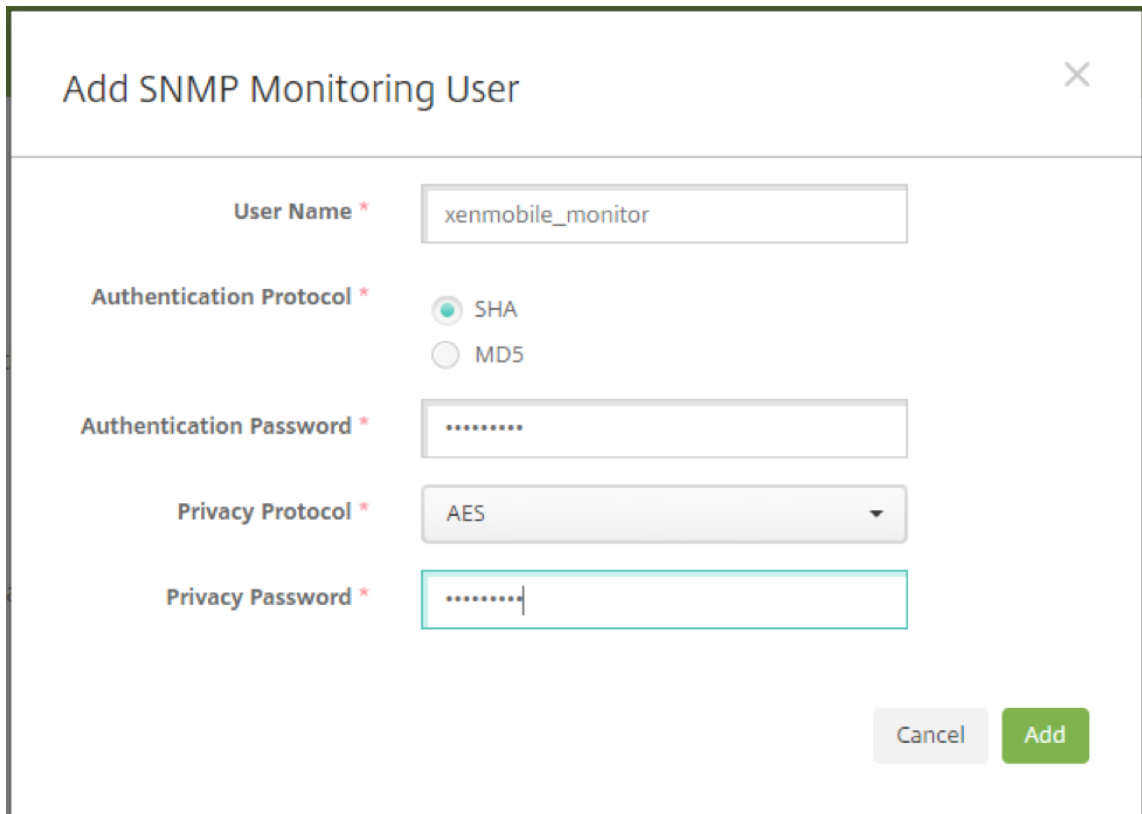
SNMP 사용자를 추가하려면

SNMP 사용자는 SNMP 관리자와 상호 작용하고 트랩을 수신합니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 모니터링에서 **SNMP** 구성을 클릭합니다. **SNMP** 구성 페이지가 나타납니다.



3. **SNMP** 모니터링 사용자에서 추가를 클릭합니다.
4. **SNMP** 모니터링 사용자 추가 대화 상자에서 다음 설정을 구성합니다.



The dialog box titled "Add SNMP Monitoring User" contains the following fields and options:

- User Name ***: A text input field containing "xenmobile_monitor".
- Authentication Protocol ***: Two radio button options: "SHA" (selected) and "MD5".
- Authentication Password ***: A password input field with masked characters ".....".
- Privacy Protocol ***: A dropdown menu currently showing "AES".
- Privacy Password ***: A password input field with masked characters ".....".

At the bottom right, there are two buttons: "Cancel" and "Add".

사용자 이름: SNMP 관리자에 로그인할 때 사용되는 사용자 이름입니다. 영숫자, 밑줄 및 하이픈을 사용할 수 있지만 공백과 다른 특수 문자는 사용자 이름에 사용할 수 없습니다.

참고:

“xmsmonitor”는 XenMobile의 내부 사용을 위해 예약된 이름이므로 사용자 이름으로 추가할 수 없습니다.

인증 프로토콜:

- **SHA**(권장)
- **MD5**

인증 암호: 8~18 자의 암호를 입력합니다. 영숫자와 특수 문자를 포함할 수 있습니다.

개인 정보 프로토콜:

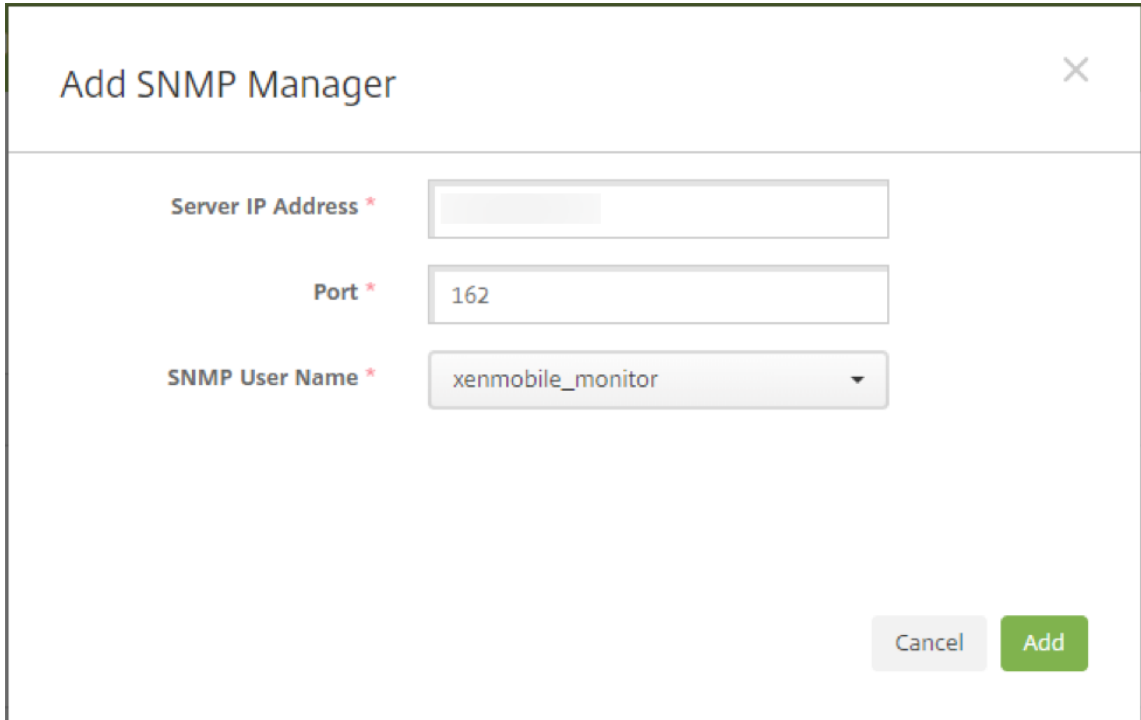
- **DES**
- **AES 128**(권장)

개인 정보 암호: 8~18 자의 암호를 입력합니다. 영숫자와 특수 문자를 포함할 수 있습니다.

SNMP 관리자를 추가하려면

1. **SNMP** 관리자에서 추가를 클릭합니다.

2. **SNMP** 관리자 추가 대화 상자에서 다음 설정을 구성합니다.



The image shows a dialog box titled "Add SNMP Manager" with a close button (X) in the top right corner. It contains three input fields: "Server IP Address *" (empty), "Port *" (containing "162"), and "SNMP User Name *" (a dropdown menu showing "xenmobile_monitor"). At the bottom right, there are two buttons: "Cancel" and "Add".

서버 IP 주소: SNMP 관리자의 IP 주소를 입력합니다.

포트: 필요한 경우 포트 번호를 변경합니다. 기본값은 162 입니다.

SNMP 사용자 이름: 관리자에 액세스할 수 있는 사용자 이름을 선택합니다.

SNMP 트랩을 사용하고 구성하려면

환경에 적합한 트랩 설정을 확인하려면 [확장성 및 성능](#)을 참조하십시오. 예를 들어 1 분 동안 XenMobile 로드 평균을 모니터링하려면 1 분 동안의 로드 평균을 사용하도록 설정하고 임계값을 입력합니다. XenMobile Server 의 1 분 동안의 로드 평균이 지정된 임계값을 초과하면 구성된 SNMP 관리자에서 트랩을 수신합니다.

- 개별 트랩을 사용하려면 다음 중 하나를 수행합니다.
 - 매개 변수 옆의 확인란을 선택하고 사용을 클릭합니다.
 - 목록의 모든 트랩을 사용하려면 맨 위의 확인란을 선택하고 사용을 클릭합니다.
- 트랩을 편집하려면 매개 변수를 선택하고 편집을 클릭합니다.
- SNMP** 트랩 세부 정보 편집 대화 상자에서 개별 트랩의 임계값을 편집할 수 있습니다.

×

Edit SNMP Trap Details

Monitors the average system load over a period of 1 minute for the user-defined interval. XenMobile generates the SNMP trap if the load average exceeds the custom threshold value.

Trap Name

Load Average for 1 Minute

Interval (in seconds) *

60

Threshold *

12

Status *

OFF

Cancel

Save

트랩 이름: 트랩의 이름입니다. 이 필드는 편집할 수 없습니다.

간격 (초): 60~86400(24 시간) 범위의 값을 사용할 수 있습니다.

임계값: 다음 트랩의 임계값만 변경할 수 있습니다.

- 프로세서 로드
- 1 분 동안의 로드 평균
- 5 분 동안의 로드 평균
- 15 분 동안의 로드 평균
- 사용 가능한 총 메모리
- 사용된 총 디스크 스토리지
- Java 힙 메모리 사용 현황
- Java Metaspace 사용 현황

상태: 트랩에 SNMP 모니터링을 사용하려면 켜짐을 선택합니다. 모니터링을 사용하지 않으려면 꺼짐을 선택합니다.

SNMP 를 사용한 XenMobile 모니터링에 대한 도움이 되는 정보를 보려면 이 [블로그 게시물](#)을 참조하십시오.

지원 번들

March 15, 2024

Citrix 에 문제를 보고하거나 문제를 해결하려면 지원 번들을 만듭니다. 그런 다음 지원 번들을 CIS(Citrix Insight Services)에 업로드합니다.

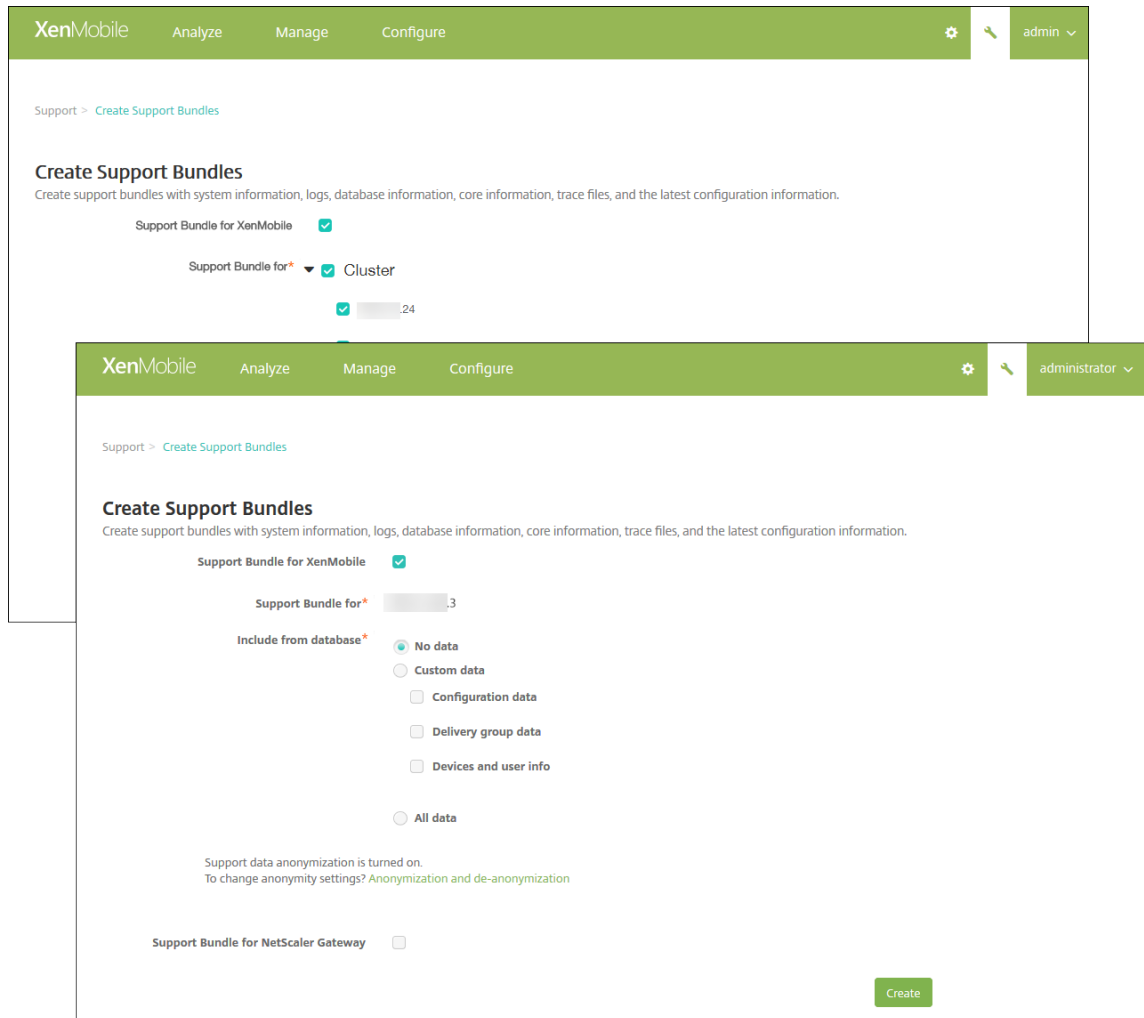
기본적으로 지원 번들에는 다음 파일에 대한 최대 100 개의 백업 아카이브가 포함됩니다. 이러한 파일의 기본 파일 크기는 10MB입니다.

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

지원 번들에 이러한 각 범주에 대한 100 개의 로그 아카이브 파일이 포함되는 경우 로그 파일이 롤오버됩니다. 로그 파일의 최대 수를 이보다 작게 구성하면 XenMobile 이 해당 노드의 추가 로그 파일을 즉시 삭제합니다. 로그 파일 수를 구성하려면 문제 해결 및 지원 > 로그 설정으로 이동합니다.

지원 번들을 만들려면:

1. XenMobile 콘솔에서 오른쪽 맨 위의 렌치 아이콘을 클릭합니다. 지원 페이지가 나타납니다.
2. 지원 페이지에서 지원 번들 만들기를 클릭합니다. 지원 번들 만들기 페이지가 나타납니다. XenMobile 환경에 클러스터된 노드가 포함되는 경우 모든 노드가 표시됩니다.

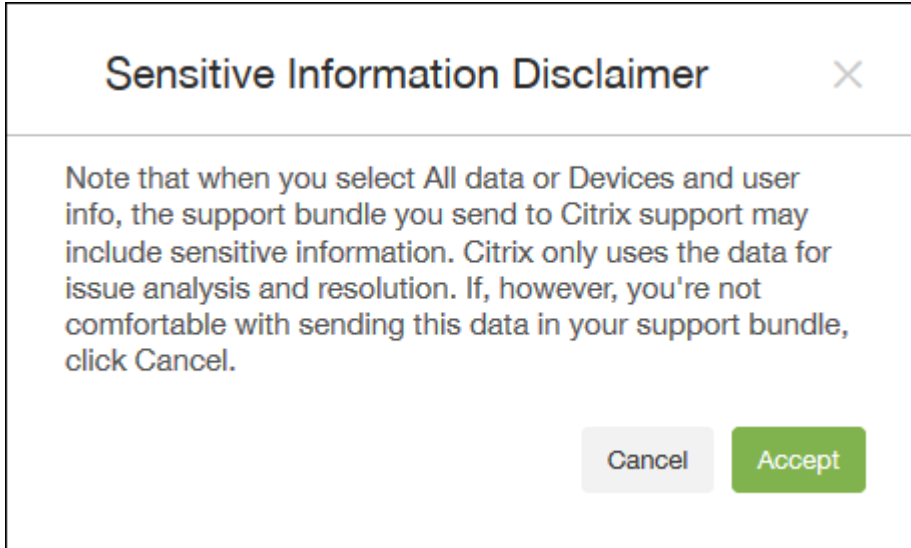


3. **XenMobile** 용 지원 번들 확인란이 선택되어 있는지 확인합니다.
4. XenMobile 환경에 클러스터된 노드가 포함되는 경우 다음을 위한 지원 번들에서 모든 노드를 선택하거나 데이터를 가져올 노드 조합을 선택할 수 있습니다.
5. 데이터베이스에서 포함에서 다음 중 하나를 수행합니다.
 - 데이터 없음을 클릭합니다.
 - 사용자 지정 데이터를 클릭합니다. 기본적으로 이 모든 옵션이 선택됩니다.
 - 구성 데이터: 인증서 구성 및 장치 관리자 정책이 포함됩니다.
 - 배달 그룹 데이터: 앱 유형 및 앱 배달 정책 세부 정보를 포함한 앱 배달 그룹 정보가 포함됩니다.
 - 장치 및 사용자 정보: 장치 정책, 앱, 동작 및 배달 그룹이 포함됩니다.
 - 모든 데이터를 클릭합니다.

참고:

장치 및 사용자 정보 또는 모든 데이터를 선택하고 처음으로 지원 번들을 만든 경우 중요한 정보에 대한 고지 사항 대화 상자가 나타납니다. 고지 사항을 읽고 동의 또는 취소를 클릭합니다. 취소를 클릭하면 지원 번들을 Citrix 에

업로드할 수 없습니다. 동의를 클릭하면 지원 번들을 Citrix 에 업로드할 수 있으며 다음에 장치 또는 사용자 데이터가 포함된 지원 번들을 만들 때 고지 사항이 표시되지 않습니다.



Sensitive Information Disclaimer ✕

Note that when you select All data or Devices and user info, the support bundle you send to Citrix support may include sensitive information. Citrix only uses the data for issue analysis and resolution. If, however, you're not comfortable with sending this data in your support bundle, click Cancel.

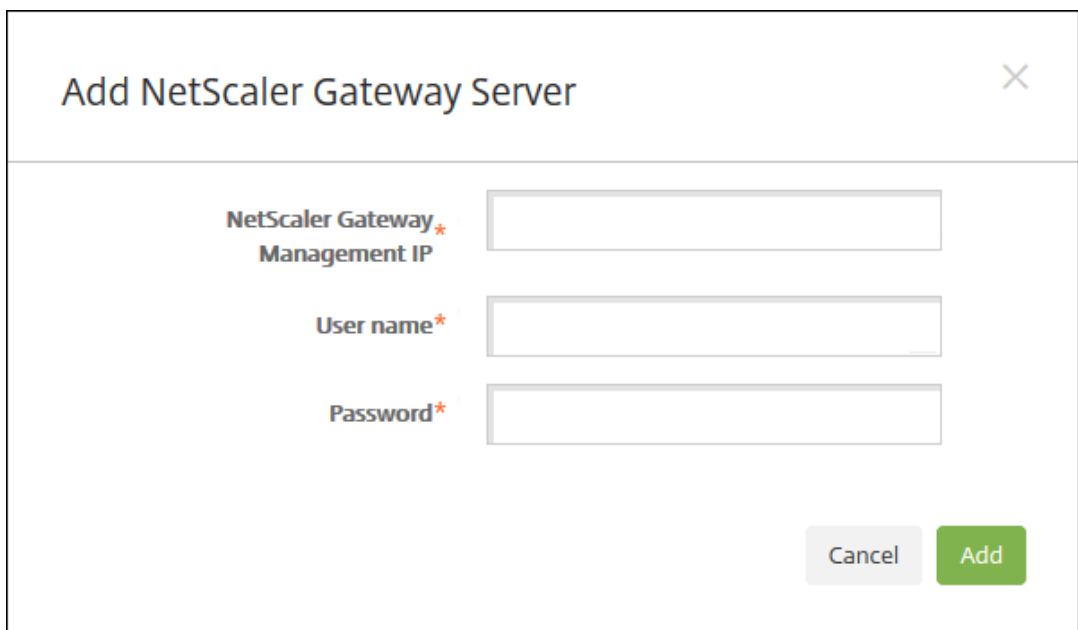
Cancel Accept

6. 지원 데이터 익명화가 켜져 있습니다 옵션은 기본 설정이 데이터를 익명화하는 것임을 나타냅니다. 데이터 익명화는 중요한 사용자, 서버 및 네트워크 데이터가 지원 번들에서 익명으로 표시되는 것을 의미합니다.

이 설정을 변경하려면 익명화 및 익명화 취소를 클릭합니다. 데이터 익명화에 대한 자세한 내용은 [지원 번들의 데이터 익명화](#)를 참조하십시오.

7. Citrix Gateway 의 지원 번들을 포함하려면: **Citrix Gateway** 용 지원 번들 확인란을 선택하고 다음을 수행합니다.

- a) 추가를 클릭합니다. **Citrix Gateway** 서버 추가 대화 상자가 나타납니다.



Add NetScaler Gateway Server ✕

NetScaler Gateway*
Management IP

User name*

Password*

Cancel Add

- b) **Citrix Gateway** 관리 IP 에 지원 번들 데이터를 가져올 Citrix Gateway 의 Citrix ADC 관리 IP 주소를 입력합니다.

참고:

이미 추가된 Citrix Gateway 서버에서 번들을 만드는 경우 IP 주소가 입력됩니다.

- c) 사용자 이름 및 암호에 Citrix Gateway 실행 서버에 액세스하는 데 필요한 사용자 자격 증명을 입력합니다.

참고:

이미 추가된 Citrix Gateway 서버에서 번들을 만드는 경우 사용자 이름이 입력됩니다.

8. 추가를 클릭합니다. 새 Citrix Gateway 지원 번들이 테이블에 추가됩니다.
9. Citrix Gateway 지원 번들을 추가하려면 7 단계를 반복합니다.
10. **Create(만들기)** 를 클릭합니다. 지원 번들이 만들어지고 두 개의 새 단추인 **CIS** 에 업로드 및 클라이언트에 다운로드가 나타납니다.

Citrix Insight Services 에 지원 번들 업로드

지원 번들을 만든 후 번들을 CIS(Citrix Insight Services) 에 업로드하거나 컴퓨터에 다운로드할 수 있습니다.

XenMobile 에서 CIS 로의 업로드에는 SSL 아웃바운드 연결이 사용됩니다. CIS 서버 IP 주소 (52.88.24.76, 52.88.118.220, 52.11.72.119) 에 대해 포트 443 을 엽니다. HTTPS 트래픽에 대한 프록시가 있는 경우 해당 프록시에서 CIS 서버 IP 주소에 연결할 수 있는지 확인하십시오.

다음 단계는 CIS 에 번들을 업로드하는 방법을 보여 줍니다. CIS 에 업로드하려면 My Citrix ID 와 암호가 필요합니다.

1. 지원 번들 만들기 페이지에서 **CIS** 에 업로드를 클릭합니다. **CIS(Citrix Insight Services)** 에 업로드 대화 상자가 나타납니다.
2. 사용자 이름에 My Citrix ID 를 입력합니다.
3. 암호에 My Citrix 암호를 입력합니다.
4. 이 번들을 기존 서비스 요청 번호에 연결하려는 경우 **SR#** 과 연결 확인란을 선택하고 표시되는 두 개의 새로운 필드에서 다음을 수행합니다.

- **SR** 번호에 이 번들을 연결할 8 자리 서비스 요청 번호를 입력합니다.
- **SR** 설명에 SR 의 설명을 입력합니다.

5. 업로드를 클릭합니다.

CIS 에 지원 번들을 업로드한 것이 처음이고 다른 제품을 통해 CIS 에 계정을 만들지 않아 데이터 수집 및 개인 정보 계약에 동의하지 않은 경우 다음 대화 상자가 나타납니다. 업로드를 시작하려면 계약에 동의해야 합니다. CIS 에 계정이 있고 이전에 계약에 동의한 경우 지원 번들이 즉시 업로드됩니다.



6. 계약을 읽고 동의 및 업로드를 클릭합니다. 지원 번들이 업로드됩니다.

컴퓨터에 지원 번들 다운로드

지원 번들을 만든 후 번들을 CIS 에 업로드하거나 컴퓨터에 다운로드할 수 있습니다. 직접 문제를 해결하려는 경우 지원 번들을 컴퓨터에 다운로드합니다.

지원 번들 만들기 페이지에서 클라이언트에 다운로드를 클릭합니다. 번들이 컴퓨터에 다운로드됩니다.

지원 번들에는 다양한 분석 값의 파일이 포함되어 있습니다. 파일 목록 및 분석 값은 다음 표를 참고하십시오.

파일 이름	유형	설명	값
DbDump.json	JSON 데이터베이스 덤프	사용자/장치/애플리케이션 정보	높음
Garbage.html	HTML 파일	Java 가비지 수집기	Low(낮음)
MemoryInfo.html	HTML 파일	메모리 사용 현황 - Java 관련 메모리 사용 현황	높음
MultiNodeClusterInfo.html	HTML 파일	클러스터 구성	높음
Patches.html	HTML 파일	패치 정보. xmspatches.txt 보다 개선됨	높음
pg_dump0.sql	PG 덤프	기본 포스트그레스 인스턴스 덤프	중간

파일 이름	유형	설명	값
rt_db/*	DB 복사본 (중복, pg_dump0.sql 의 이진 표 현임)		해당 없음
sas_config/c3p0.properties	속성 파일	C3P0 DB 구성 속성	중간
sas_config/catalina.policy	정책 파일	웹 서버 Catalina 정책 - 파 일이 변경되지 않음	Low(낮음)
sas_config/catalina.properties	속성 파일	웹 서버 Catalina 속성 - 파 일이 변경되지 않음	Low(낮음)
sas_config/ew- config.properties	속성 파일	XM 서버 구성에 대한 정보	높음
sas_config/ew-config- reloadable.properties	속성 파일	보안 모델 정보	높음
sas_config/hazelcast.xml	XML 파일	Hazelcast 로그 - 별로 도움 이 되지 않을 수 있음	Low(낮음)
sas_config/pki.xml	XML 파일	타사 PKI 서버를 사용 중인지 확인하는 데 사용할 수 있음	높음
sas_config/push_services.xml	XML 파일	푸시 서비스 - 파일이 변경되 지 않음	Low(낮음)
sas_config/server.xml	XML 파일	여기에 암호 정보 - 보안 관련	높음
sas_config/sftu_config/AppC.properties	속성 파일	AppC 속성 - 파일이 변경되 지 않음	Low(낮음)
sas_config/sftu_config/catalina.policy	정책 파일	Catalina 정책 - 파일이 변 경되지 않음	Low(낮음)
sas_config/sftu_config/catalina.properties	속성 파일	Catalina 속성 - 파일이 변 경되지 않음	Low(낮음)
sas_config/sftu_config/logging.properties	속성 파일	로깅 속성 - 파일이 변경되지 않음	Low(낮음)
sas_config/sftu_config/security.xml	XML 파일	여기에 암호 정보 - 보안 관련	높음
sas_config/sftu_config/security.xml	XML 파일	마이그레이션 정보	높음
sas_config/sftu_config/security.xml	XML 파일	최초 사용자 설정	높음
sas_config/sftu_config/tomcat-users.xml	XML 파일	TomCat 사용자 - 파일이 변 경되지 않음	Low(낮음)
sas_config/sftu_config/web.xml	XML 파일	웹 - 파일이 변경되지 않음	Low(낮음)
sas_config/sftu.properties	속성 파일	SFTU 구성 속성	높음
sas_config/variables.xml	XML 파일	변수 - 파일이 변경되지 않음	Low(낮음)

파일 이름	유형	설명	값
sas_config/web.xml	XML 파일	웹 서버 관련 정보	중간
sas_log/AdminAuditLogFile.log	Linux 로그 파일	모든 구성 변경 사항	높음
sas_log/create_sb_output.log	Linux 로그 파일	지원 생성 명령 출력	Low(낮음)
sas_log/DebugLogFile.log	Linux 로그 파일	모든 기능 로그	높음
sas_log/HibernateStats.log	Linux 로그 파일	최대 절전 모드 기록	Low(낮음)
sas_log/kafka-consumer.log	Linux 로그 파일	Kafka 로그	Low(낮음)
sas_log/kafka-server.log	Linux 로그 파일	Kafka 로그	Low(낮음)
sas_log/kafka-topics.log	Linux 로그 파일	Kafka 로그	Low(낮음)
sas_log/LPE.log	Linux 로그 파일	LPE 로그	Low(낮음)
sas_log/migration.log	Linux 로그 파일	마이그레이션 프로세스 출력	중간
sas_log/PlatformAuditLogFile.log	Linux 로그 파일	백엔드 감사 수준 정보	높음
sas_log/PlatformDebugLogFile.log	Linux 로그 파일	백엔드 서버 관련 로그	높음
sas_log/postgres.log	Linux 로그 파일	PostGres 로그	중간
sas_log/SFTU.log	Linux 로그 파일	SFTU 로그	중간
sas_log/tc1/catalina.log	Linux 로그 파일	Catalina 로그	Low(낮음)
sas_log/tc1/console	Linux 로그 파일	콘솔	Low(낮음)
sas_log/tc1/host-manager.log	Linux 로그 파일	호스트 관리자	Low(낮음)
sas_log/tc1/localhost.log	Linux 로그 파일	LocalHost	Low(낮음)
sas_log/updates.log	Linux 로그 파일	패치 프로세스 출력	중간
sas_log/UserAuditLogFile.log	Linux 로그 파일	사용자 작업	높음
sas_log/zookeeper.txt	텍스트 파일	Zookeeper 로그	Low(낮음)
snmp/snmpd_etc_netsnmp.conf	설정 파일	SNMP 구성 속성	Low(낮음)
snmp/snmpd_privileges.conf	설정 파일	SNMP 구성 속성	Low(낮음)
sys_info/arp_entries.txt	텍스트 파일	XMS 서버의 ARP 항목	중간
sys_info/chrony.txt	텍스트 파일	Chrony 로그	Low(낮음)
sys_info/diskspace_usage.txt	텍스트 파일	디스크 공간 사용 현황	높음

파일 이름	유형	설명	값
sys_info/firewall_rules.txt	텍스트 파일	XMS 에 정의된 방화벽 규칙	중간
sys_info/interface_config.txt	텍스트 파일	시스템 명령 출력	중간
sys_info/net_connections.txt	텍스트 파일	시스템 명령 출력	중간
sys_info/root_account_info.txt	텍스트 파일	시스템 명령 출력	중간
sys_info/routing_table.txt	텍스트 파일	높은 값	높음
sys_info/running_processes.txt	텍스트 파일	높은 값	높음
sys_info/top.txt	텍스트 파일	시스템 명령 출력	중간
ThreadDump.html	HTML 파일	더 이상 사용되지 않음	Low(낮음)
ThreadDumpV2.html	HTML 파일	스레드 스택 추적 등	중간
var_log/auth.log	Linux 로그 파일	OS 수준 로그	중간
var_log/boot.log	Linux 로그 파일	OS 수준 로그	중간
var_log/btmp	Linux 로그 파일	OS 수준 로그	중간
var_log/daemon.log	Linux 로그 파일	OS 수준 로그	중간
var_log/kern.log	Linux 로그 파일	OS 수준 로그	중간
var_log/lastlog	Linux 로그 파일	OS 수준 로그	중간
var_log/mail.log	Linux 로그 파일	OS 수준 로그	중간
var_log/sys.log	Linux 로그 파일	OS 수준 로그	중간
var_log/user.log	Linux 로그 파일	OS 수준 로그	중간
var_log/wtmp	Linux 로그 파일	OS 수준 로그	중간
version.txt	텍스트 파일	XM 서버 버전	중간
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	XML 파일	XMS 서버의 연결 확인 결과	중간
xmspatches.txt	텍스트 파일	패치 정보.	높음

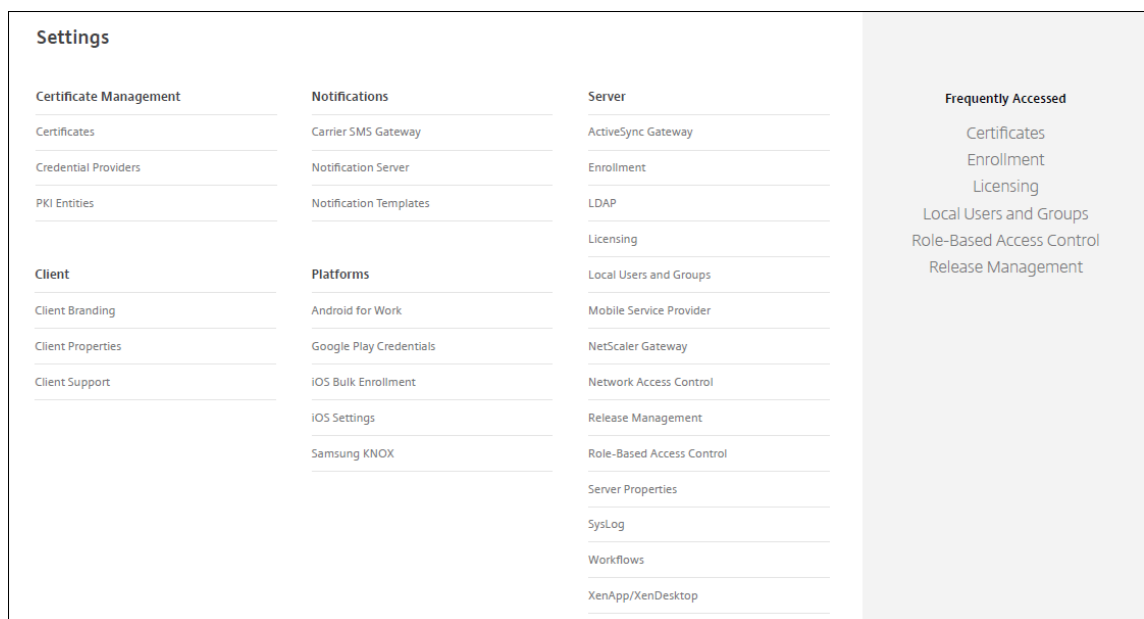
지원 옵션 및 원격 지원

March 15, 2024

사용자가 지원 담당자에게 연락할 수 있도록 전자 메일 주소를 제공할 수 있습니다. 사용자가 장치에서 지원을 요청하면 전자 메일 주소가 표시됩니다.

또한 사용자가 장치에서 지원 센터로 로그를 보내는 방법도 구성할 수 있습니다. 직접 또는 전자 메일을 사용하여 로그를 보내도록 구성할 수 있습니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.



2. 클라이언트에서 클라이언트 지원을 클릭합니다. 클라이언트 지원 페이지가 나타납니다.

3. 다음 설정을 구성합니다.

- 지원 전자 메일 (**IT** 지원 센터): IT 지원 센터 연락처의 전자 메일 주소를 입력합니다.
- 장치 로그를 **IT** 지원 센터에 보내기: 장치 로그를 직접 보낼지 아니면 전자 메일로 보낼지를 선택합니다. 기본값은 전자 메일로입니다.
 - 직접을 사용하면 ShareFile(현재 ShareFile)에 로그 저장에 대한 설정이 나타납니다. ShareFile에 로그 저장을 사용하는 경우 Citrix Files로 직접 로그가 전송됩니다. 그렇지 않은 경우 XenMobile로 전송된 다음 전자 메일을 통해 지원 센터로 전송됩니다. 또한 기본적으로 사용하도록 설정되는 직접 보내기가 실패하면 전자 메일 사용 옵션이 나타납니다. 클라이언트 전자 메일을 사용하여 서버 문제에 대한 로그를 전송하지 않으려면 이 옵션을 사용하지 않을 수 있습니다. 그러나 이 옵션을 사용하지 않고 서버 문제가 발생하면 로그가 전송되지 않습니다.
 - 전자 메일로 사용하면 로그를 전송할 때 클라이언트 전자 메일이 항상 사용됩니다.

4. 저장을 클릭합니다.

원격 지원

참고:

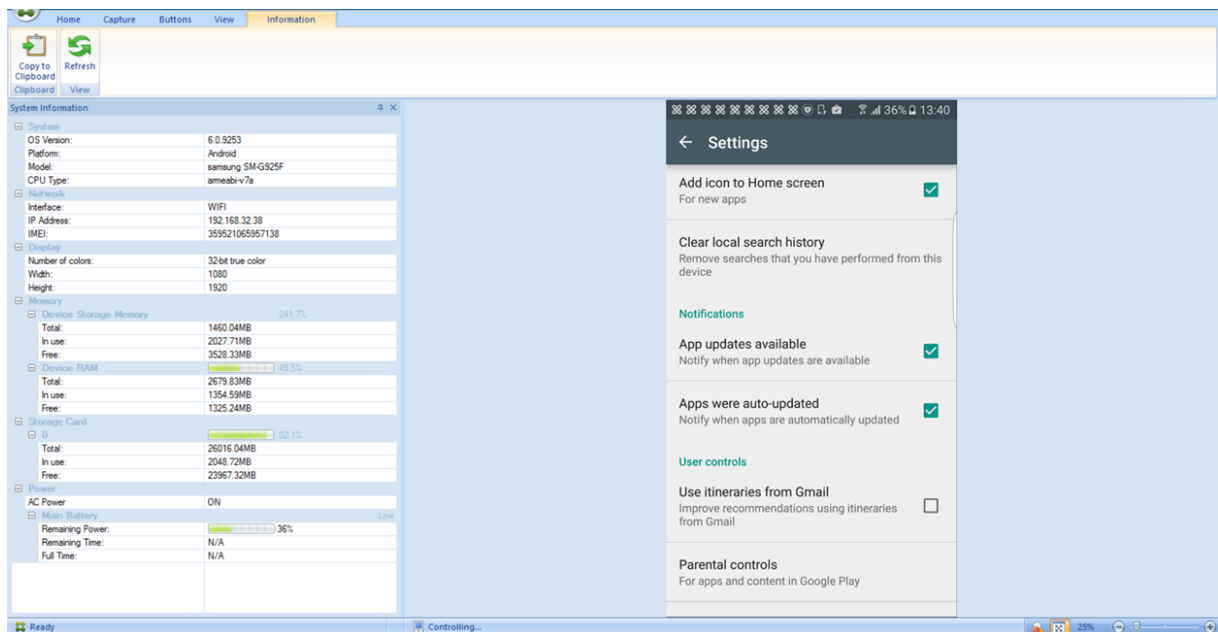
2019년 1월 1일부터 신규 고객에게는 더 이상 원격 지원이 제공되지 않습니다. 기존 고객은 제품을 계속 사용할 수 있지만 Citrix는 개선 사항이나 수정 사항을 제공하지 않습니다.

온-프레미스 XenMobile Server 배포의 경우: 원격 지원을 사용하면 지원 센터 담당자가 관리되는 Android 모바일 장치를 원격으로 제어할 수 있습니다. 스크린캐스트는 Samsung Knox 장치에서만 지원됩니다.

원격 지원은 클러스터링된 온-프레미스 XenMobile Server 배포에서 지원되지 않습니다.

원격 제어 세션 중에:

- 사용자의 모바일 장치에 원격 제어 세션이 활성 상태임을 나타내는 아이콘이 표시됩니다.
- 원격 지원 사용자는 원격 지원 응용 프로그램 창과 원격 제어 창에서 제어되는 장치의 렌더링을 볼 수 있습니다.



원격 지원을 사용하여 다음을 수행할 수 있습니다.

- 사용자 장치에 원격으로 로그인하고 화면을 제어합니다. 사용자는 원격 지원 담당자가 화면을 탐색하는 것을 지켜볼 수 있으며 이는 교육용으로도 유용합니다.
- 원격 장치를 실시간으로 탐색하고 복구합니다. 구성을 변경하고, 운영 체제 문제를 해결하고, 문제가 되는 앱 또는 프로세스를 사용하지 않도록 설정하거나 중지할 수 있습니다.
- 네트워크 액세스를 원격으로 사용하지 않도록 설정하고, 불법 프로세스를 중지하고, 앱 또는 맬웨어를 제거하여 위협이 다른 모바일 장치로 확산되기 전에 격리하고 억제합니다.
- 장치 벨소리를 원격으로 사용하도록 설정하고 전화를 걸어 사용자가 장치를 찾을 수 있도록 합니다. 사용자가 장치를 찾을 수 없는 경우 장치를 초기화하여 중요한 데이터가 손상되지 않도록 합니다.

또한 지원 담당자는 원격 지원을 사용하여 다음을 수행할 수 있습니다.

- 하나 이상의 XenMobile 인스턴스 내에서 연결된 모든 장치 목록을 표시합니다.
- 장치 모델, 운영 체제 수준, IMEI(International Mobile Station Equipment Identity), 일련 번호, 메모리 및 배터리 상태, 연결 등을 비롯한 시스템 정보를 표시합니다.
- XenMobile의 사용자 및 그룹을 표시합니다.
- 활성 프로세스를 표시 및 종료하고 모바일 장치를 다시 시작할 수 있는 장치 작업 관리자를 실행합니다.
- 모바일 장치와 중앙 파일 서버 간의 양방향 파일 전송을 포함하는 원격 파일 전송을 실행합니다.
- 소프트웨어 프로그램을 일괄 처리로 하나 이상의 모바일 장치에 다운로드하고 설치합니다.
- 장치에서 원격 레지스트리 키 설정을 구성합니다.
- 실시간 장치 화면 원격 제어를 사용하여 저 대역폭 셀룰러 네트워크에서 응답 시간을 최적화합니다.
- 대부분의 모바일 장치 브랜드 및 모델에 대한 장치 스킨을 표시합니다. 스킨 편집기를 표시하여 새 장치 모델을 추가하고 물리적 키를 매핑합니다.
- 비디오 AVI 파일을 만드는 장치에서 일련의 상호 작용을 캡처하는 기능을 통해 장치 화면 캡처, 녹화 및 재생을 사용하도록 설정합니다.
- 모바일 사용자와 지원 직원 간에 공유 화이트보드, VoIP 기반 음성 통신 및 채팅을 사용하여 라이브 모임을 수행합니다.

원격 지원 시스템 요구 사항

원격 지원 소프트웨어는 다음 요구 사항을 충족하는 Windows 기반 컴퓨터에 설치됩니다. 포트 요구 사항은 [포트 요구 사항](#)을 참조하십시오.

지원되는 플랫폼:

- Intel Xeon/Pentium 4 -1GHz 워크스테이션급 이상
- 512MB RAM 이상
- 최소 100MB 디스크 여유 공간

지원되는 운영 체제:

- Microsoft Windows 2003 Server Standard Edition 또는 Enterprise Edition SP1 이상
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 이상
- Microsoft Windows Vista SP1 이상
- Microsoft Windows 10 또는 Windows 11
- Microsoft Windows 8
- Microsoft Windows 7

명령줄에서 원격 지원을 설치하려면 다음 명령을 실행합니다.

```
1 *RemoteSupport*.exe /S
```

*RemoteSupport*는 설치 프로그램의 이름입니다. 예:

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

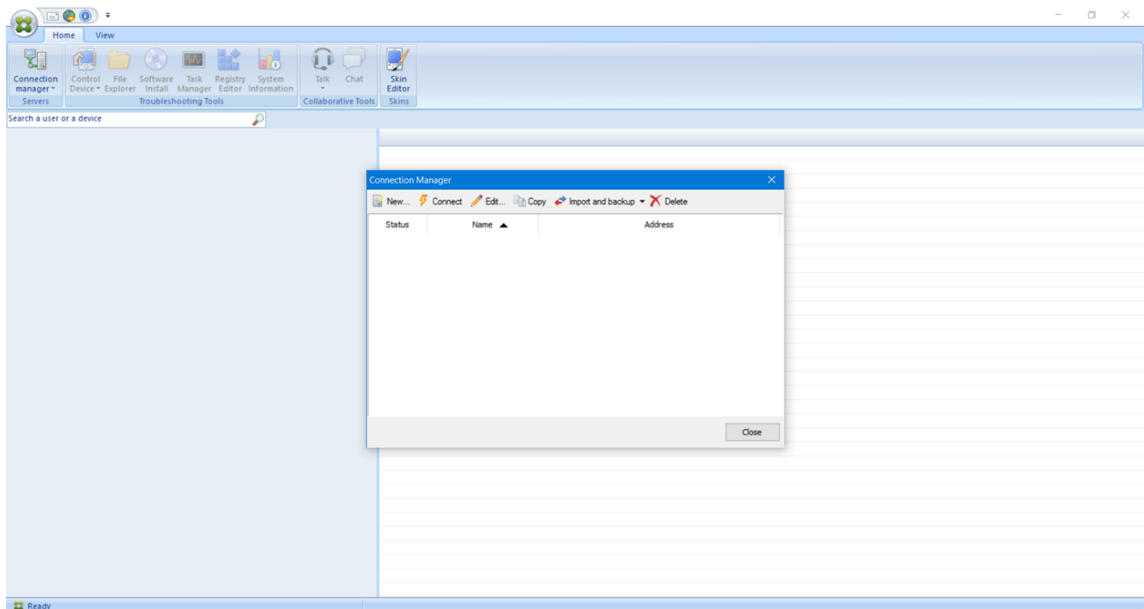
원격 지원 소프트웨어를 설치할 때 다음 변수를 사용할 수 있습니다.

- /S: 기본 매개 변수를 사용하여 자동으로 원격 지원 소프트웨어를 설치합니다.
- /D=dir: 사용자 지정 설치 디렉터리를 지정합니다.

원격 지원을 **XenMobile** 에 연결하려면

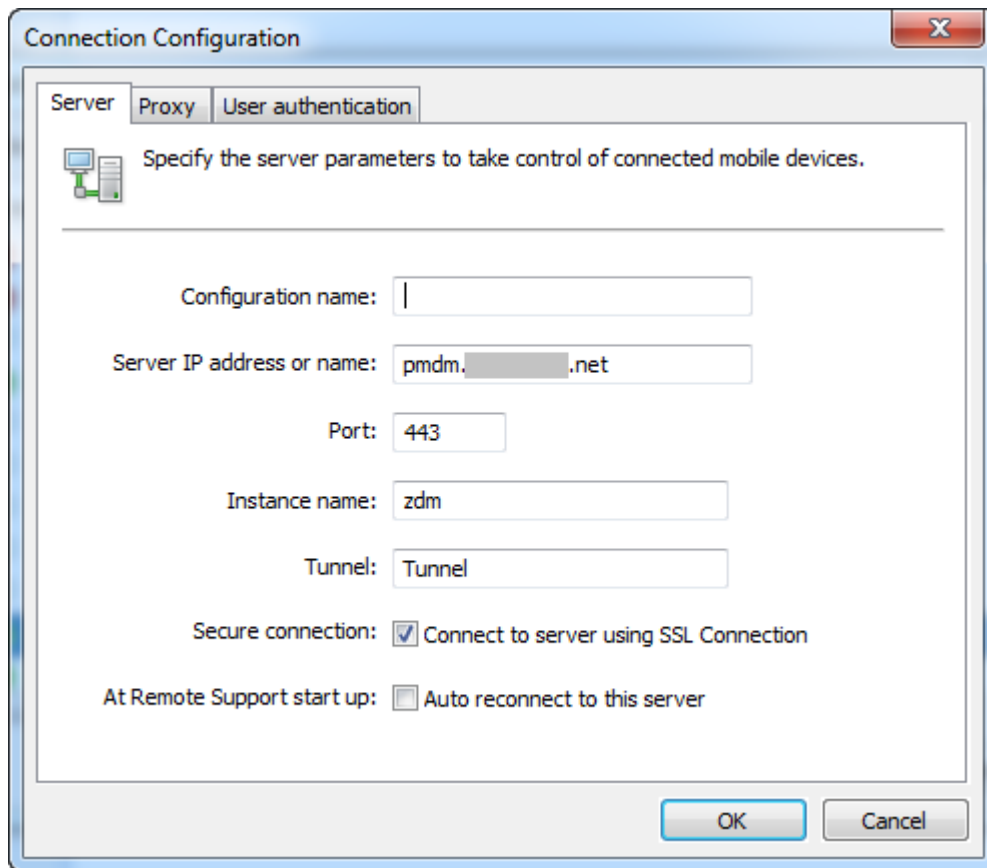
관리되는 장치에 대한 원격 지원 연결을 설정하려면 장치를 관리하는 하나 이상의 XenMobile Server 에 원격 지원의 연결을 추가해야 합니다. 이러한 연결은 Android 장치에 대한 장치 정책인 터널 MDM 정책에서 정의한 앱 터널을 통해 실행됩니다. 원격 지원을 XenMobile 에 연결하려면 먼저 앱 터널을 정의해야 합니다. 자세한 내용은 [앱 터널링 장치 정책](#)을 참조하십시오.

1. 원격 지원 소프트웨어를 시작하고 XenMobile 자격 증명을 사용하여 로그인합니다.
2. **Connection Manager**(연결 관리자)에서 **New**(새로 만들기)를 클릭합니다.

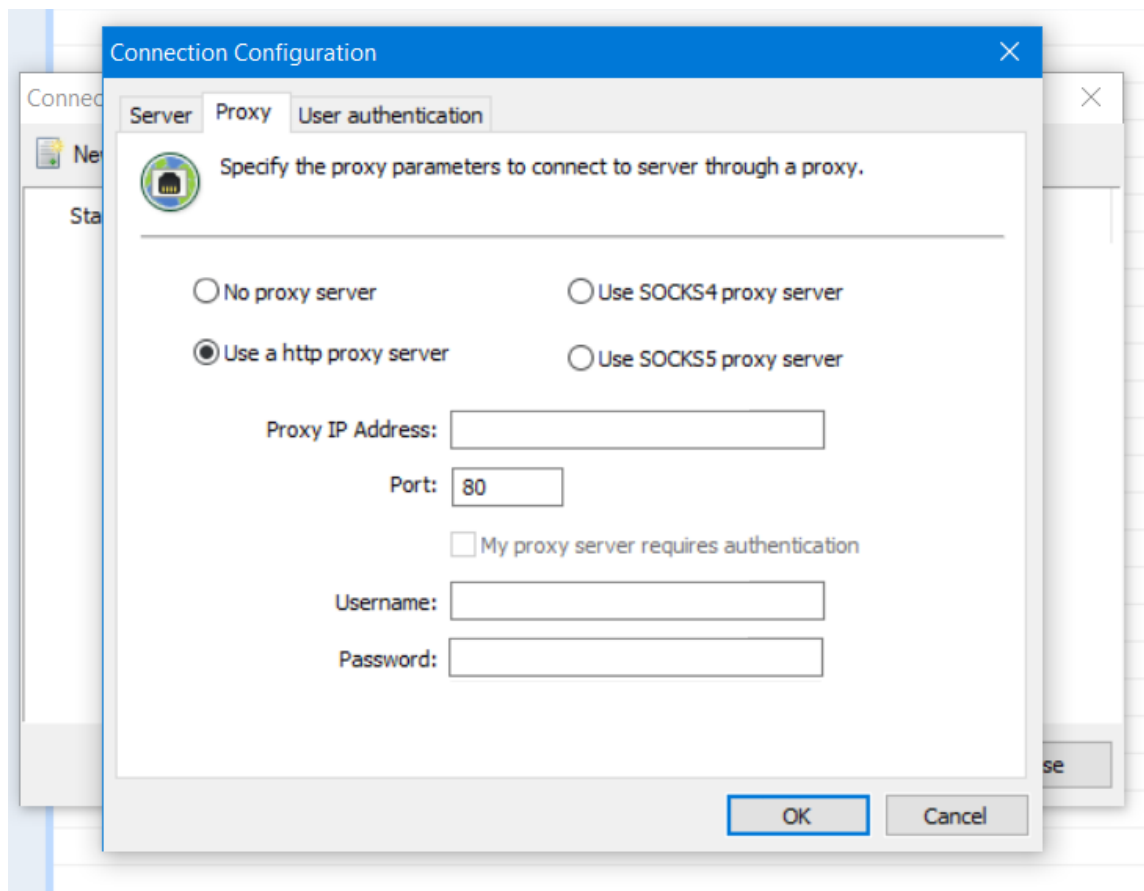


3. **Connection Configuration**(연결 구성) 대화 상자의 **Server**(서버) 탭에 다음 값을 입력합니다.
 - a) **Configuration name**(구성 이름)에 구성 항목의 이름을 입력합니다.
 - b) **Server IP address or name**(서버 IP 주소 또는 이름)에 XenMobile Server의 IP 주소 또는 DNS 이름을 입력합니다.
 - c) **Port**(포트)에 XenMobile Server 구성에서 정의한 TCP 포트 번호를 입력합니다.
 - d) XenMobile이 다중 테넌트 배포에 포함되는 경우 **Instance name**(인스턴스 이름)에 인스턴스 이름을 입력합니다.
 - e) **Tunnel**(터널)에 터널 정책의 이름을 입력합니다.
 - f) **Connect to server using SSL Connection**(SSL 연결을 사용하여 서버에 연결) 확인란을 선택합니다.

- g) 원격 지원 응용 프로그램을 시작할 때마다 구성된 XenMobile Server 에 연결하려면 **Auto reconnect to this server**(이 서버에 자동으로 다시 연결) 확인란을 선택합니다.



4. **Proxy**(프록시) 탭에서 **Use an http proxy server**(http 프록시 서버 사용) 를 선택하고 다음 정보를 입력합니다.
- Proxy IP Address**(프록시 IP 주소) 에 프록시 서버의 IP 주소를 입력합니다.
 - Port**(포트) 에 프록시에서 사용하는 TCP 포트 번호를 입력합니다.
 - 프록시 서버에 트래픽 허용을 위한 인증이 필요한 경우 **My proxy server requires authentication**(내 프록시 서버에 인증 필요) 확인란을 선택합니다.
 - Username**(사용자 이름) 에 프록시 서버에서 인증할 사용자 이름을 입력합니다.
 - Password**(암호) 에 프록시 서버에서 인증할 암호를 입력합니다.



5. **User Authentication(사용자 인증)** 탭에서 **Remember my login and password(로그인 및 암호 저장)** 확인란을 선택하고 자격 증명을 입력합니다.

6. 확인을 클릭합니다.

XenMobile 에 연결하려면 이전에 만든 연결을 두 번 클릭한 후 연결에 대해 구성한 사용자 이름과 암호를 입력합니다.

Samsung Knox 장치에 대해 원격 지원을 사용하려면

XenMobile 에서 **Samsung Knox** 장치에 대한 원격 액세스를 제공하는 원격 지원 정책을 만듭니다. 두 가지 유형의 지원을 구성할 수 있습니다.

- **기본:** 장치에 대한 진단 정보를 볼 수 있습니다. 예를 들어 시스템 정보, 실행 중인 프로세스, 작업 관리자 (메모리 및 CPU 사용량), 설치된 소프트웨어 폴더 내용 등을 볼 수 있습니다.
- **프리미엄:** 원격으로 장치 화면을 제어할 수 있습니다. 예를 들어 창 색상을 제어하고, 지원 센터와 사용자 간의 VoIP 세션을 설정하고, 지원 센터와 사용자 간의 채팅 세션을 설정할 수 있습니다.

프리미엄 지원을 사용하려면 XenMobile 콘솔에서 **Samsung MDM** 라이선스 키 장치 정책을 구성해야 합니다. 이 정책을 구성하는 경우 **Samsung KNOX** 플랫폼만 선택합니다. SAFE 플랫폼의 경우 **Samsung** 장치가 XenMobile

에 등록될 때 ELM 키가 자동으로 배포됩니다. 따라서 이 정책에는 Samsung SAFE 플랫폼을 선택하지 마십시오. 자세한 내용은 [Samsung MDM 라이선스 키](#)를 참조하십시오.

원격 지원 정책 구성에 대한 자세한 내용은 [원격 지원 장치 정책](#)을 참조하십시오.

원격 지원 세션을 사용하려면

원격 지원을 시작하면 원격 지원 응용 프로그램 창의 왼쪽에 XenMobile 콘솔에서 정의한 XenMobile 사용자 그룹이 표시됩니다. 기본적으로 현재 연결된 사용자를 포함하는 그룹만 표시됩니다. 사용자 항목 옆에서 각 사용자의 장치를 볼 수 있습니다.

1. 모든 사용자를 보려면 왼쪽 열에서 각 그룹을 확장합니다.
현재 XenMobile Server에 연결된 사용자는 녹색 아이콘으로 표시됩니다.
2. 현재 연결되지 않은 사용자를 포함한 모든 사용자를 표시하려면 **View(보기)**를 클릭하고 **Non-connected devices(연결되지 않은 장치)**를 선택합니다.
작은 녹색 아이콘이 없는 연결되지 않은 사용자가 표시됩니다.

XenMobile Server에 연결되었지만 사용자에게 할당되지 않은 장치는 익명 모드로 표시됩니다. 목록에 **Anonymous(익명)** 문자열이 표시됩니다. 이러한 장치는 로그인한 사용자의 장치와 같은 방법으로 제어할 수 있습니다.

장치를 제어하려면 장치 행을 클릭한 후 **Control Device(장치 제어)**를 클릭하여 장치를 선택합니다. Remote Control(원격 제어) 창에 장치 렌더링이 나타납니다. 제어되는 장치와 다음과 같은 방법으로 상호 작용할 수 있습니다.

- 주 창 또는 개별적인 부동 창에서 색상 제어를 포함하여 장치 화면을 제어합니다.
- 지원 센터와 사용자 간의 VoIP 세션을 설정합니다. VoIP 설정을 구성합니다.
- 사용자와의 채팅 세션을 설정합니다.
- 장치 작업 관리자에 액세스하여 메모리 사용량, CPU 사용량 및 실행 중인 앱과 같은 항목을 관리합니다.
- 모바일 장치의 로컬 디렉터리를 탐색합니다. 파일을 전송합니다.
- 장치 시스템 정보 및 설치된 모든 소프트웨어를 표시합니다.
- 모바일 장치와 XenMobile Server의 연결 상태를 업데이트합니다.

Syslog

March 15, 2024

시스템 로그 (syslog) 서버에 로그 파일을 보내도록 XenMobile Server(온-프레미스)를 구성할 수 있습니다. 서버 호스트 이름 또는 IP 주소가 필요합니다.

Syslog는 장비에서 실행되는 감사 모듈과 원격 시스템에서 실행될 수 있는 서버라는 두 가지 구성 요소가 있는 표준 로깅 프로토콜입니다. Syslog 프로토콜에서는 데이터 전송에 UDP(User Datagram Protocol)를 사용합니다. 관리자 이벤트 및 사용자 이벤트가 기록됩니다.

다음과 같은 유형의 정보를 수집하도록 서버를 구성할 수 있습니다.

- XenMobile 에서 수행한 동작의 레코드가 포함된 시스템 로그
- XenMobile 의 시스템 작업을 시간순으로 기록한 감사 로그

syslog 서버가 장비에서 수집하는 로그 정보는 메시지 형태로 로그 파일에 저장됩니다. 이러한 메시지에는 대개 다음과 같은 정보가 포함됩니다.

- 로그 메시지를 생성한 장비의 IP 주소
- 타임스탬프
- 메시지 유형
- 이벤트와 관련된 로그 수준 (중요, 오류, 알림, 경고, 정보, 디버그, 경보 또는 긴급)
- 메시지 정보

XenMobile 은 log4j syslog 어펜더를 사용하여 RFC5424 형식의 syslog 메시지를 전송합니다. syslog 메시지 데이터는 특정 형식이 없는 일반 텍스트입니다.

이 정보를 사용하여 경고 출처를 분석하고 필요한 경우 교정 조치를 취할 수 있습니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. **Syslog** 를 클릭합니다. **Syslog** 페이지가 나타납니다.
3. 다음 설정을 구성합니다.

- 서버: syslog 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름) 을 입력합니다.
- 포트: 포트 번호를 입력합니다. 기본적으로 포트는 514 로 설정됩니다.
- 로깅할 정보: 시스템 로그 및 감사를 선택하거나 선택 취소합니다.
 - 시스템 로그는 XenMobile 에서 수행한 동작을 포함합니다.
 - 감사 로그는 XenMobile 의 시스템 작업을 시간순으로 기록한 레코드를 포함합니다.
 - XenMobile 의 디버그 로그

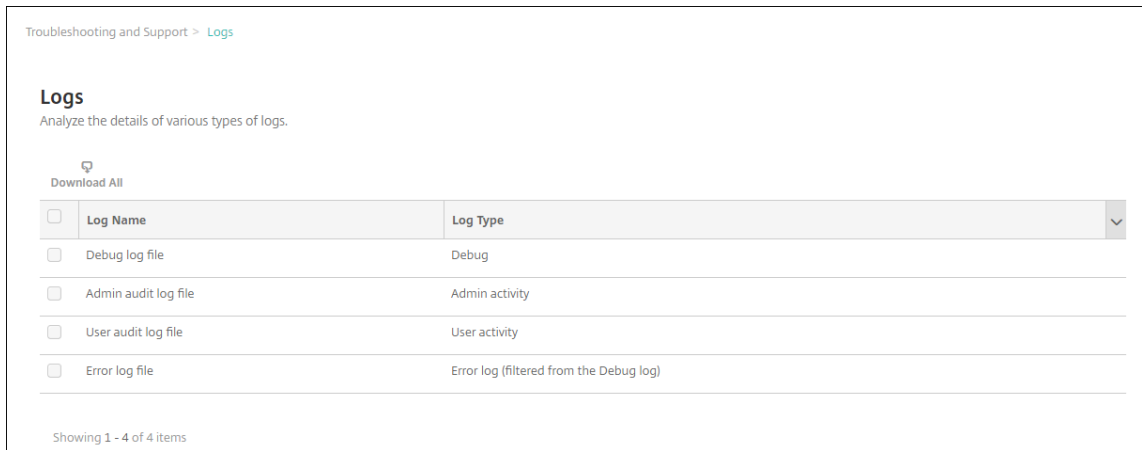
4. 저장을 클릭합니다.

XenMobile 에서 로그 파일 보기

March 15, 2024

XenMobile 을 사용한 관리에 도움이 되는 로그를 보고 조작하고 다운로드할 수 있습니다.

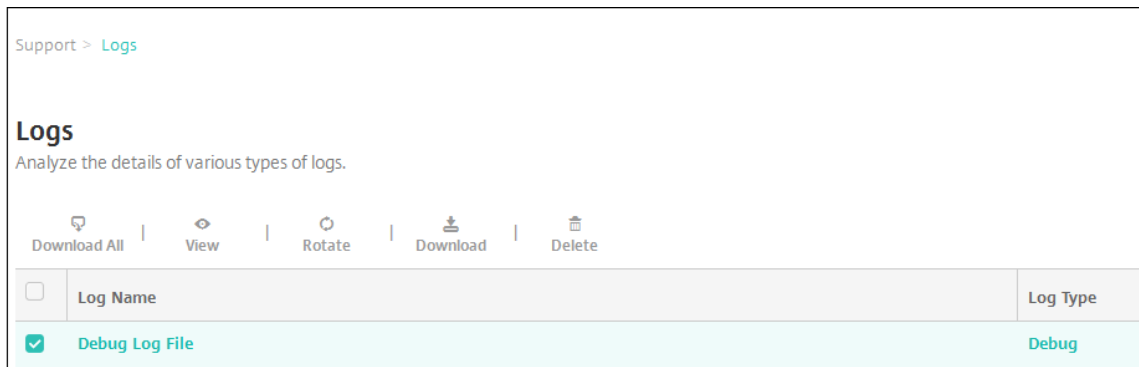
1. XenMobile 콘솔에서 오른쪽 위 모서리의 런치 아이콘을 클릭합니다. 지원 페이지가 나타납니다.
2. 로그 작업 아래에서 로그를 클릭합니다. 로그 페이지가 나타납니다. 개별 로그가 테이블에 표시됩니다.



3. 보려는 로그를 선택합니다.

- 디버그 로그 파일에는 오류 메시지, 서버 관련 동작 등 Citrix 지원에 대한 유용한 정보가 들어 있습니다.
- 관리자 감사 로그 파일에는 XenMobile 콘솔 작업에 대한 감사 정보가 포함되어 있습니다.
- 사용자 감사 로그 파일에는 구성된 사용자와 관련된 정보가 포함되어 있습니다.
- 오류 로그 파일에는 디버그 로그에서 필터링된 오류 메시지만 포함되어 있습니다.

4. 테이블 상단에 있는 모두 다운로드, 보기, 순환, 단일 로그 다운로드 또는 선택한 로그 삭제 동작을 수행합니다.



참고:

- 여러 개의 로그 파일을 선택하는 경우 모두 다운로드와 순환만 사용할 수 있습니다.
- XenMobile 서버를 클러스터링한 경우 연결된 서버에 대한 로그만 볼 수 있습니다. 다른 서버에 대한 로그를 보려면 다운로드 옵션 중 하나를 사용합니다.

5. 다음 중 하나를 수행합니다.

- 모두 다운로드: 시스템에 있는 모든 로그 (디버그, 관리자 감사, 사용자 감사, 서버 로그 등) 가 다운로드됩니다.
- 보기: 테이블 아래에 선택한 로그 내용이 표시됩니다.
- 순환: 현재 로그 파일이 보관되고 로그 항목을 캡처할 새 파일이 생성됩니다. 로그 파일을 보관하는 경우 대화 상자가 나타납니다. 계속하려면 순환을 클릭합니다.
- 다운로드: 콘솔은 선택한 단일 로그 파일 유형만 다운로드합니다. 또한 동일한 유형의 아카이브된 로그도 모두 다운로드합니다.

- **삭제:** 선택한 로그 파일을 영구적으로 제거합니다.

Logs

Analyze the details of various types of logs.

Download All

View

Rotate

Download

Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

2016-11-06T06:28:38.908-0800 |

INFO |

node.scheduled.executor-8 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:29:38.926-0800 |

INFO |

node.scheduled.executor-10 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:30:38.762-0800 |

INFO |

node.pooled.executor2 |

com.citrix.cg.task.handlers.NonPrvsnTask |

Begin method executeNonPrvsnTaskJob: Sun Nov 06 06:45:38 PST 2016

2016-11-06T06:30:38.766-0800 |

INFO |

node.pooled.executor2 |

com.citrix.cg.task.handlers.NonPrvsnTask |

The number of non provision tasks Picked 2.

2016-11-06T06:30:38.945-0800 |

INFO |

node.scheduled.executor-2 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:31:38.965-0800 |

INFO |

node.scheduled.executor-9 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:32:38.985-0800 |

INFO |

node.scheduled.executor-4 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:33:39.3-0800 |

INFO |

node.scheduled.executor-2 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:34:39.24-0800 |

INFO |

node.scheduled.executor-8 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:35:39.42-0800 |

INFO |

node.scheduled.executor-5 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

2016-11-06T06:36:39.593-0800 |

INFO |

node.scheduled.executor-1 |

com.citrix.feature.FeatureManagerFactory |

Enabling local feature management

REST API

March 15, 2024

참고:

이 문서에서는 XenMobile Server 용 REST API 에 대해 다룹니다. Endpoint Management 용 REST API 에 대해서는 [REST API](#)를 참조하십시오.

XenMobile REST API 를 사용하여 XenMobile 콘솔을 통해 표시되는 서비스를 호출할 수 있습니다. 모든 REST 클라이언트를 사용하여 REST 서비스를 호출할 수 있습니다. API 를 사용하면 XenMobile 콘솔에 로그인하지 않고 서비스를 호출할 수 있습니다.

현재 사용 가능한 전체 API 집합을 보려면 [REST 서비스에 대한 공용 API](#) PDF 를 다운로드하십시오.

REST API 액세스에 필요한 권한

REST API 에 액세스하려면 다음 권한 중 하나가 필요합니다.

- 공용 API 액세스 권한은 역할 기반 액세스 구성의 일부로 설정됩니다. 자세한 내용은 [RBAC 를 사용하여 역할 구성](#)을 참조하십시오.
- 슈퍼 사용자 권한

REST API 서비스를 호출하려면

REST 클라이언트 또는 cURL 명령을 사용하여 REST API 서비스를 호출할 수 있습니다. 다음 예제에서는 Chrome 용 Advanced REST 클라이언트를 사용합니다.

참고:

다음 예제에서 호스트 이름 및 포트 번호를 환경에 맞게 변경하십시오.

로그인

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

요청: { `"login": "administrator", "password": "password"` }

메서드 형식: POST

콘텐츠 형식: application/json

The screenshot displays the Advanced REST Client interface. At the top, the URL bar shows `https://localhost:4443/xenmobile/api/v1/publicapi/login`. Below the URL bar, the HTTP method is set to `POST`. The `Headers` tab is active, showing no headers. The `Payload` tab is also active, displaying a JSON body: `{ "login": "administrator", "password": "password" }`. The `Content-Type` header is set to `application/json`. The `Send` button is visible. Below the request configuration, the `Status` bar shows `200 OK` with a loading time of 265 ms. The `Request headers` section lists: `User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.101 Safari/537.36`, `Origin: chrome-extension://hgmloofddfnphfcgellkdtbfbjeloo`, `Content-Type: application/json`, `Accept: */*`, `Accept-Encoding: gzip, deflate`, `Accept-Language: en-US,en;q=0.8`, and `Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163`. The `Response headers` section lists: `Server: Apache-Coyote/1.1`, `Content-Type: text/plain`, `Content-Length: 53`, and `Date: Sun, 22 Mar 2015 22:43:48 GMT`. The `Response` tab is active, showing the JSON body: `{ "auth_token": "" }`. At the bottom, there are links for `Open output in new window`, `Copy to clipboard`, `Save as file`, and `Open in JSON tab`.

관련 정보

- [XenMobile REST API](#)

Exchange ActiveSync 용 Endpoint Management 커넥터

March 15, 2024

XenMobile Mail Manager 는 이제 Exchange ActiveSync 용 Endpoint Management 커넥터입니다. Citrix 통합 포트폴리오에 대한 자세한 내용은 [Citrix 제품 가이드](#)를 참조하십시오.

이 커넥터는 다음과 같이 XenMobile 의 기능을 확장합니다.

- EAS(Exchange Active Sync) 장치에 대한 동적 액세스 제어. EAS 장치는 Exchange 서비스에 대한 액세스가 자동으로 허용 또는 차단될 수 있습니다.
- XenMobile 이 Exchange 에서 제공하는 EAS 장치 파트너 관계 정보에 액세스하는 기능.
- EAS 상태를 기반으로 모바일 장치를 초기화하는 XenMobile 의 기능입니다.
- XenMobile 이 Blackberry 장치에 대한 정보에 액세스하고 초기화 및 ResetPassword 같은 제어 작업을 수행하는 기능.

EAS 상태를 기반으로 장치를 초기화하려면 ActiveSync 트리거로 자동화된 작업을 구성합니다. [자동화된 동작](#)을 참조하십시오.

Exchange ActiveSync 용 Endpoint Management 커넥터를 다운로드하려면:

1. <https://www.citrix.com/downloads>로 이동합니다.
2. **Citrix Endpoint Management(및 Citrix XenMobile Server) > XenMobile Server(온-프레미스) > 제품 소프트웨어 > XenMobile Server 10 > 서버 구성 요소**로 이동합니다.
3. **Exchange ActiveSync 용 Citrix Endpoint Management** 커넥터 타일에서 파일 다운로드를 클릭합니다.

중요:

2022 년 10 월부터 Exchange ActiveSync 용 Endpoint Management 및 Citrix Gateway 커넥터는 Microsoft 가 [여기](#)에서 발표한 인증 변경사항에 따라 더 이상 Exchange Online 을 지원하지 않습니다. Exchange 용 Endpoint Management 커넥터는 Microsoft Exchange Server(온-프레미스) 에서 계속 작동합니다.

새로운 항목

이후 섹션에는 이전의 XenMobile Mail Manager 인 Exchange ActiveSync 용 Endpoint Management 커넥터에 대한 새로운 기능이 나열됩니다.

버전 10.1.10 의 새로운 기능

다음 문제는 버전 10.1.10 에서 수정되었습니다.

- 네트워크 문제를 자주 경험하는 고객은 이전에 제공된 3 번의 시도에서 스냅샷을 완료하지 못할 수 있습니다. 이 릴리스에서는 관리자가 최대 시도 횟수 (1~10) 를 구성할 수 있습니다. 이 수정 사항이 적용됨에 따라 통신에서 스냅샷이 여러 번 중단되더라도 스냅샷 프로세스가 완전히 중단되지 않습니다. CXM-70837

- 이전 버전에서는 스냅샷 유형이 Exchange 구성 목록에 나타나지 않았습니다. 이제 스냅샷 유형이 나타납니다. [CXM-70846]
- PowerShell 을 통해 보고되는 PSRemotingTransport 예외는 Exchange 세션을 더 이상 실행할 수 없음을 나타냅니다. 상태는 기본적으로 구성 파일의 심각한 오류 목록에 추가됩니다. 따라서 PSRemotingTransportException 이 검색되면 이후 삭제를 위해 연결이 오류 상태인 것으로 표시됩니다. 다음번 통신에는 유효한 연결이 사용되거나 새 연결이 만들어집니다. [XMHELP-2184, CXM-70836]
- 구성 변경이 저장되면 새 구성을 로드하기 전에 이전에 구성된 내부 구성 요소 중 일부가 제대로 삭제되지 않을 수 있습니다. 이 문제로 인해 예측할 수 없는 동작이 발생할 수 있습니다. 이 동작은 특정 변경 사항에 따라 다르며 변경 사항이 이전 구성과 충돌하는지 여부에 따라 달라집니다. 이 릴리스에서는 새 구성을 로드하기 전에 모든 내부 구성 요소가 삭제됩니다. [XMHELP-2259, CXM-71388]

이전 버전의 새로운 기능

다음 섹션에는 Exchange ActiveSync 용 Endpoint Management 커넥터의 이전 버전에 포함된 기능과 수정된 문제가 나와 있습니다.

버전 **10.1.9** 의 새로운 기능

다음 문제는 버전 10.1.9 에서 수정되었습니다.

- 이제 구성 변경이 보다 일관된 방식으로 처리됩니다. 서비스가 구성 변경을 감지하면 각 내부 하위 시스템이 중지됩니다. 즉, 모든 활성 또는 예약 처리가 중단됩니다. 그런 다음 새 구성이 로드되고 하위 시스템이 다시 시작됩니다. 즉, 모든 예약 및 기타 내부 인프라가 새 설정으로 다시 설정됩니다. 이 문제는 버전 10.1.8 의 알려진 문제를 수정합니다. [CXM-47709, CXM-61330]
- 업그레이드 중에 기존 데이터베이스 구성이 새 구성 파일에 병합되지 않았습니다. 이제 데이터베이스 구성이 업그레이드 된 구성 파일에 병합됩니다. [CXM-49326]
- 스냅샷 관련 진단 파일에서 열 헤더가 누락되었습니다. 헤더가 복원되었습니다. [CXM-62680]
- 이전 버전에서 업그레이드하는 경우 사용 중인 구성 파일의 유사한 섹션이 구성 파일의 기본값 섹션을 덮어씁니다. 이 문제로 인해 업그레이드 후 기본값 섹션에 추가 또는 개선 사항이 로드되지 않습니다. 이 버전부터는 기본값 섹션에 항상 최신 구성이 반영됩니다. [CXM-62681]
- 관리자는 응용 프로그램을 실행할 때 더 이상 Shift 키를 눌러 특정 옵션에 액세스할 수 없습니다. 이러한 옵션은 이전에 Citrix 사용 권한으로 사용할 수 있었습니다. 이제 리디렉션 허용과 같은 일부 옵션을 완벽하게 사용할 수 있으며 감지 중지 및 개수 수정 같은 다른 옵션은 사용되지 않습니다. [CXM-62767]

The screenshot shows the 'Configuration' window for XenMobile. The settings are as follows:

- Type: On Premise
- Exchange Server: [Empty field]
- User: [Empty field]
- Password: [Empty field]
- Major snapshot: Every 4 Hours
- Minor snapshot: Every 5 Minutes
- Snapshot Type: Shallow
- Default Access: Unchanged
- Command Mode: Powershell
- Connection Expiration: Every 00 Hours 30 Minutes
- Enable Diagnostics: ☐
- Days to Keep Snapshot Data: 00
- View Entire Forest: ☐
- Authentication: Kerberos
- Allow Redirection: ☐

Buttons: Test Connectivity, Save, Cancel.

버전 **10.1.8** 의 새로운 기능

다음 문제는 버전 10.1.8 에서 수정되었습니다.

- Exchange 는 Exchange ActiveSync 서비스에 대한 Citrix Endpoint Management 커넥터를 제한하여 커넥터에서 너무 자주 명령이 실행되지 않도록 합니다. 이는 Office 365 에 대한 연결에서 일반적인 사항입니다. 제한이 적용 되면 다음 명령을 전송하기 전에 서비스를 지정된 기간 동안 일시 중지해야 합니다. 이제 구성 콘솔에 남은 일시 중지 시간이 표시됩니다. [CXM-48044]
- 구성 파일 (config.xml) 의 “Watchdog” 또는 “SpecialistsDefaults” 섹션을 수정하는 경우 업그레이드 후 구성 파일에 변경 사항이 반영되지 않습니다. 이 릴리스에서는 수정한 내용이 새 구성 파일에 올바르게 병합됩니다. [CXM-52523]
- Google Analytics 로 전송되는 분석에 특히 스냅샷과 관련하여 더 많은 세부 정보가 추가되었습니다. [CXM-56691]
- Exchange 테스트 연결 기능은 연결 초기화를 한 번만 시도합니다. Office 365 연결은 제한될 수 있기 때문에 제한 되는 경우 테스트 연결이 실패한 것으로 나타날 수 있었습니다. 이제 Exchange ActiveSync 용 Citrix Endpoint Management 커넥터가 연결 시작을 최대 세 번까지 시도합니다. [CXM-58180]
- Exchange 에서 정책을 시행하려면 Exchange ActiveSync 용 Citrix Endpoint Management 커넥터가 각 사서함의 모든 관련 장치를 허용 목록과 차단 목록에 포함하는 **Set-CASMailbox** 명령을 컴파일해야 합니다. 장치가 목록에 포함되지 않은 경우 Exchange 는 기본 액세스 상태로 폴백합니다. 이 기본 액세스 상태가 장치의 원하는 상태와 다른 경우 장치는 규정 준수 위반 상태가 됩니다. 따라서 Exchange 기본 액세스 상태가 허용됨 상태여야 하지만 차단됨인

경우 사용자는 전자 메일에 액세스하지 못할 수 있습니다. 또는 전자 메일에 대한 액세스가 차단되어야 하는 사용자에게 액세스 권한이 부여될 수 있습니다. 이제 Exchange ActiveSync 용 Citrix Endpoint Management 커넥터가 원하는 상태의 모든 장치를 각 **Set-CasMailbox** 명령에 포함합니다. [CXM-61251]

다음은 버전 10.1.8 에서 알려진 문제입니다.

스냅샷 또는 정책 평가 같은 장기 작업이 서비스에서 실행되는 동안 관리자가 구성 응용 프로그램에서 구성 데이터를 수정하는 변경을 수행하면 서비스가 규정 불가능한 상태로 전환될 수 있습니다. 이 경우 정책 변경이 처리되지 않거나 스냅샷이 시작되지 않는 등의 증상이 나타날 수 있습니다. 서비스를 작동 상태로 되돌리려면 서비스를 다시 시작해야 합니다. 서비스를 시작하기 전에 Windows 서비스 관리자를 사용하여 서비스 프로세스를 종료해야 할 수 있습니다. [CXM-61330]

버전 **10.1.7** 의 새로운 기능

- XenMobile Mail Manager 는 이제 Exchange ActiveSync 용 Endpoint Management 커넥터입니다.
- Exchange 구성 대화 상자에서 **Disable Pipelining**(파이프라인 처리 사용 안 함) 옵션이 더 이상 지원되지 않습니다. config.xml 파일에서 각 명령에 대한 여러 단계를 구성하여 동일한 기능을 구현할 수 있습니다. [CXM-54593]

다음 문제는 버전 10.1.7 에서 수정되었습니다.

- 스냅샷 기록 창에서 오류 메시지가 컨텍스트가 부족한 상태로 표시될 수 있습니다. 이제 오류 메시지에 발생 위치에 대한 컨텍스트가 접두사로 추가됩니다. [CXM-49157]
- XmmGoogleAnalytics.dll 에 이 릴리스에 해당하는 파일 버전이 없습니다. [CXM-52518]
- 진단을 개선하기 위해 최근에 사서함 허용/차단된 상태를 설정하는 데 사용되는 장치 ID 목록에 대한 문자열 형식을 변경했습니다. 하지만 너무 많은 장치를 지정하면 최대 문자열 크기가 초과되었습니다. 이제 내부 배열 데이터 구조를 사용합니다. 이 구조에는 크기 제한이 없으며 데이터의 형식을 진단 용도에 적합하게 지정합니다. [CXM-52610]
- Exchange 와 동기화되지 않은 장치 정책이 검색되는 경우 해당 명령에 관련 사서함에 속하지 않는 장치가 포함되어 있을 수 있습니다. 이제 Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange 에 대한 명령에 관련 사서함에 속한 장치만 나타나게 합니다. [CXM-54842]
- 일부 환경에서 Microsoft 어셈블리를 사용할 수 없습니다. 필요한 어셈블리가 이제 응용 프로그램과 함께 명시적으로 설치됩니다. [CXM-55439]
- 장치 또는 사서함의 고유 이름에서 특성 이름과 등호 사이 및/또는 등호와 값 사이에 공백이 있는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터가 장치와 사서함을 올바르게 일치시키지 못할 수 있습니다. 결과적으로 스냅샷 조정 중에 일부 장치 및/또는 사서함이 거부될 수 있습니다. [CXM-56088]

참고:

이후 섹션에서는 Exchange ActiveSync 용 Endpoint Management 커넥터가 이전 이름인 XenMobile Mail Manager 로 나타납니다. 이 이름은 버전 10.1.7 에서 변경되었습니다.

버전 **10.1.6.20** 의 업데이트

10.1.6 에 대한 업데이트에는 버전 10.1.6.20 의 다음과 같은 수정 사항이 포함되어 있습니다.

- Exchange 와 동기화되지 않은 장치 정책이 검색되는 경우 해당 명령에 관련 사서함에 속하지 않는 장치가 포함되어 있을 수 있습니다. 이제 XenMobile Mail Manager 는 Exchange 에 대한 명령에 관련 사서함에 속한 장치만 나타나게 합니다. [CXM-54842]

버전 10.1.6 의 새로운 기능

XenMobile Mail Manager 버전 10.1.6 에는 다음과 같은 수정된 문제와 개선 사항이 포함되어 있습니다.

- 경우에 따라 스냅샷 기록 창이 더 이상 업데이트되지 않는 상태로 전환됩니다. 더욱 안정적으로 업데이트되도록 창 새로 고침 메커니즘이 개선되었습니다. [CXM-47983]
- 파티셔닝된 스냅샷과 파티셔닝되지 않은 스냅샷에 두 가지 별도의 모드와 코드 경로가 사용되었습니다. 파티셔닝되지 않은 스냅샷은 단일 “*” 파티션을 사용하는 구성의 파티셔닝된 스냅샷과 동일하기 때문에 파티셔닝되지 않은 스냅샷 모드가 제거되었습니다. 이제 36 개의 파티션 (0-9, A-Z) 이 있는 파티셔닝된 스냅샷이 기본 스냅샷 모드입니다. [CXM-49093]
- 스냅샷 기록 창에서 오류 메시지가 상태 메시지로 덮어씌웁니다. 이제 XenMobile Mail Manager 에 두 개의 별도 필드가 표시되어 사용자가 상태와 오류를 동시에 볼 수 있습니다. [CXM-51942]
- Exchange Online(Office 365) 에 연결할 때 스냅샷 관련 쿼리로 인해 데이터 집합이 잘릴 수 있습니다. 이 문제는 XenMobile Mail Manager 가 다중 명령 파이프라인이 있는 스크립트를 실행하는 경우에 발생할 수 있습니다. 업스트림 명령이 다운스트림 명령에 충분히 빠르게 데이터를 전달할 수 없어 작업이 조기에 완료됩니다. 그 결과 불완전한 데이터가 발생합니다. 이제 XenMobile Mail Manager 가 파이프라인 자체를 모방하고 업스트림 명령이 완료될 때까지 기다린 후에 다운스트림 명령을 호출할 수 있습니다. 이 변경 사항에 따라 이제 모든 데이터가 처리되고 캡처됩니다. [CXM-52280]
- Exchange 에 대한 정책 업데이트 명령에서 해결할 수 없는 오류가 발생할 경우 동일한 명령이 오랫동안 반복적으로 작업 대기열에 반환됩니다. 이 경우 해당 명령이 Exchange 에 여러 번 전송되었습니다. 이 XenMobile Mail Manager 버전에서는 오류를 일으키는 명령이 작업 대기열에 불연속적으로만 반환됩니다. [CXM-52633]
- 특정 사서함에 대한 정책 업데이트에 모든 장치 허용 또는 차단이 포함된 경우 **Set-CASMailbox** 명령 실행이 실패합니다. 빈 목록이 **NULL** 이 아닌 빈 문자열로 변환되기 때문입니다. 이제 올바른 데이터가 전송됩니다. [CXM-53759]
- 새 장치를 처리할 때 Exchange 에서 얼마 동안 (대개 15 분) “DeviceDiscovery” 로 상태가 반환될 수 있습니다. XenMobile Mail Manager 가 이 상태를 특별히 처리하지 않았습니다. 이제 XenMobile Mail Manager 가 이 상태를 처리합니다. 사용자가 UI 의 모니터 탭에서 이 상태의 장치로 필터링할 수 있습니다. [CXM-53840]
- XenMobile Mail Manager 가 XenMobile Mail Manager 데이터베이스에 쓸 수 있는 권한을 확인하지 않았습니다. 따라서 권한이 제한된 경우 동작을 예측할 수 없었습니다. 이제 XenMobile Mail Manager 가 데이터베이스에서 필요한 권한을 캡처하고 확인합니다. XenMobile Mail Manager 는 권한이 감소된 것을 연결 테스트 시 (메시지가 표시됨) 또는 기본 구성 창 하단의 데이터베이스 표시기에 (마우스 포인터를 이동하면 메시지가 표시됨) 표시합니다. [CXM-54219]
- XenMobile Mail Manager 서비스를 중지하려고 할 때 현재 작업 부하에 따라 서비스가 즉시 중지되지 않을 수 있습니다. 따라서 서비스가 응답하지 않는 상태로 나타납니다. 진행 중인 작업이 중단되어 보다 정상적으로 종료될 수 있도록 기능이 개선되었습니다. [CXM-54282]

버전 10.1.5 의 새로운 기능

XenMobile Mail Manager 버전 10.1.5 에는 다음과 같은 수정된 문제가 포함되어 있습니다.

- Exchange 가 XenMobile Mail Manager 작업에 제한을 적용하는 경우 로그 이외에는 제한이 적용되었다는 점이 표시되지 않습니다. 이 릴리스에서는 사용자가 활성 스냅샷으로 마우스 포인터를 이동하면 “제한” 상태가 표시됩니다. 또한 XenMobile Mail Manager 에 제한이 적용되는 동안에는 Exchange 에서 제한이 해제될 때까지 주 스냅샷의 시작이 금지됩니다. [CXM-49617]
- 주 스냅샷 작업 중 XenMobile Mail Manager 에 Exchange 의 제한이 적용될 경우 다음 스냅샷을 실행하기까지 허용되는 경과 시간이 부족할 수 있습니다. 이 문제로 인해 제한이 연장되고 스냅샷이 실패합니다. 이제 XenMobile Mail Manager 가 Exchange 에서 지정한 최소 스냅샷 시도 대기 간격 동안 대기합니다. [CXM-49618]
- 진단이 사용되는 경우 명령 파일에서 **Set-CasMailbox** 명령의 각 속성 이름 앞에 하이픈이 누락된 것으로 나타납니다. 이 문제는 진단 파일의 형식에서만 발생하며 Exchange 에 대한 실제 명령에서는 발생하지 않습니다. 하이픈 누락으로 인해 사용자는 테스트 또는 유효성 검사를 위해 명령을 잘라내어 PowerShell 프롬프트에 바로 붙여 넣지는 못합니다. 하이픈이 추가되었습니다. [CXM-52520]
- 사서함 ID 가 “lastname, firstname” 형식인 경우 Exchange 가 쿼리에서 데이터를 반환할 때 쉼표 앞에 백슬래시를 추가합니다. XenMobile Mail Manager 가 추가 데이터 쿼리를 위해 ID 를 사용할 때 이 백슬래시를 제거해야 합니다. [CXM-52635]

알려진 제한 사항

참고:

다음 제한 사항은 버전 10.1.6 에서 해결되었습니다.

XenMobile Mail Manager 에는 알려진 제한 제한이 있으며, 이로 인해 Exchange 에 대한 명령이 실패할 수 있습니다. Exchange 에 정책 변경 사항을 적용하기 위해 XenMobile Mail Manager 는 **Set-CASMailbox** 명령을 실행합니다. 이 명령은 두 가지 장치 목록, 즉 허용 목록과 차단 목록을 사용할 수 있습니다. 이 명령은 사서함에 연결된 장치에 적용됩니다.

이러한 목록은 Microsoft API 에 의해 각각 256 자로 제한됩니다. 이러한 목록 중 하나가 제한을 초과할 경우 명령이 완전히 실패하여 사서함의 해당 장치에 대한 모든 정책이 설정되지 않습니다. XenMobile Mail Manager 로그에 다음과 같은 오류가 보고됩니다. 차단 목록에 대한 예입니다.

“Message:’ Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’ to the target. Exception setting ‘ActiveSyncBlockedDeviceIDs’ : “The length of the property is too long. The maximum length is 256 and the length of the value provided is ...”

장치 ID 길이는 달라질 수 있지만 일반적으로 동시에 10 개 이상의 허용 또는 차단 장치가 포함될 경우 제한이 초과될 수 있습니다. 특정 사서함에 많은 장치가 연결되는 경우는 드물지만 있을 수 있습니다. XenMobile Mail Manager 가 이러한 경우를 처리하도록 개선될 때까지 사용자와 사서함에 연결되는 장치 수를 10 개 이하로 제한하는 것이 좋습니다. [CXM-52633]

버전 10.1.4 의 새로운 기능

XenMobile Mail Manager 버전 10.1.4 에는 다음과 같은 수정된 문제가 포함되어 있습니다.

- PCI Council에서는 보안이 취약한 TLS 1.0의 사용을 중지하고 있습니다. XenMobile Mail Manager에는 TLS 1.1 및 1.2에 대한 지원이 추가되었습니다. [CXM-38573, CXM-32560]
- XenMobile Mail Manager에는 새로운 진단 파일이 포함됩니다. Exchange 사양에서 **Enable Diagnostics**(진단 사용)를 선택하면 새 스냅샷 기록 파일이 생성됩니다. 스냅샷을 시도할 때마다 스냅샷의 결과로 파일에 행이 추가됩니다. [CXM-49631]
- **Set-CASMailbox** 명령에 대한 명령 진단 파일에 허용되거나 차단된 장치 목록이 나타나지 않았습니다. 대신, 파일의 관련된 인수에 내부 클래스 이름이 표시되었습니다. 이제 XenMobile Mail Manager의 deviceID 목록이 심표로 구분된 목록으로 표시됩니다. [CXM-50693]
- 잘못된 사양으로 인해 Exchange에 대한 연결 시도가 실패할 경우 오류 메시지가 “All connections in use(모든 연결을 사용 중임)”라는 잘못된 메시지로 재정의되었습니다. 이제 보다 설명적인 메시지가 나타납니다. 예를 들어 “All connections are inoperable(모든 연결이 작동하지 않음)”, “Connection pool is empty(연결 풀이 비어 있음)”, “All connections are throttled(모든 연결이 제한됨)” 및 “No available connections(사용 가능한 연결 없음)” 같은 메시지가 나타납니다. [CXM-50783]
- 경우에 따라 허용/차단/초기화 명령이 XenMobile Mail Manager 내부 캐시의 대기열에 여러 번 배치됩니다. 이 문제로 인해 Exchange로 전송되는 명령이 지연됩니다. 이제 XenMobile Mail Manager가 각 명령에 대한 단일 인스턴스만 대기열에 배치합니다. [CXM-51524]

버전 10.1.3의 새로운 기능

- **Google Analytics** 지원: XenMobile Mail Manager가 어떻게 사용되는지를 확인하여 제품의 개선 영역에 집중할 수 있습니다.
- 진단 사용 설정: **Configuration**(구성) 대화 상자의 Configure console(콘솔 구성)에 **Enable Diagnostic**(진단 사용) 확인란이 나타납니다.

The screenshot shows the 'Configuration' window for an Exchange Server. The 'Type' is set to 'On Premise'. The 'Exchange Server' field is empty. The 'User' and 'Password' fields are also empty. The 'Major snapshot' is set to 'Every 4 Hours', 'Minor snapshot' to 'Every 5 Minutes', and 'Snapshot Type' to 'Shallow'. The 'Default Access' is 'Unchanged' and 'Command Mode' is 'Powershell'. The 'Connection Expiration' is set to 'Every 00 Hours 00 Minutes'. The 'Enable Diagnostics' and 'View Entire Forest' checkboxes are unchecked. The 'Authentication' is set to 'Kerberos'. There is a 'Test Connectivity' button and a large empty text area below it. At the bottom are 'Save' and 'Cancel' buttons.

버전 10.1.3 의 수정된 문제

- **Snapshot History**(스냅샷 기록) 창에서 스냅샷의 현재 상태를 보여 주는 도구 설명에 실제 상태가 반영되지 않습니다. [CXM-5570]
가끔, XenMobile Mail Manager 에서 명령 진단 파일이 작성되지 않습니다. 이 경우 명령 기록이 하나도 기록되지 않습니다. [CXM-49217]
- 연결 오류가 발생하는 경우 연결이 “errored” 로 표시되지 않습니다. 그 결과 후속 명령에서 연결 사용을 시도하고 다른 오류가 발생할 수 있습니다. [CXM-49495]
- Exchange Server 에서 제한이 발생하면 상태 확인 루틴에서 예외가 발생할 수 있습니다. 그 결과 오류가 발생하거나 만료된 연결을 삭제하지 못할 수 있습니다. 또한 XenMobile Mail Manager 에서 제한 시간이 만료되기 전까지 연결을 만들지 못할 수 있습니다. [CXM-49794]
- Exchange 의 최대 세션 수가 초과되면 XenMobile Mail Manager 가 정확한 메시지가 아닌 “Device Capture Failed(장치 캡처 실패)” 오류를 보고합니다. XenMobile Mail Manager 가 Exchange 통신에 정상적으로 사용하는 세션 두 개가 사용 중임을 나타내는 메시지가 보고되어야 합니다. [CXM-49994]

버전 10.1.2 의 새로운 기능

- **Exchange** 에 대한 연결 개선: XenMobile Mail Manager 는 PowerShell 세션을 사용하여 Exchange 와 통신합니다. PowerShell 세션을 Office 365 를 통해 처리하는 경우 잠시 후 세션이 불안정해지고 후속 명령이 성공적으로

실행되지 않을 수 있습니다. 이제 XenMobile Mail Manager 에서 연결의 만료 기간을 설정할 수 있습니다. 연결이 만료 시간에 도달하면 XenMobile Mail Manager 가 PowerShell 세션을 정상적으로 종료하고 세션을 만들 수 있습니다. 이렇게 하면 PowerShell 세션이 불안정해질 가능성이 줄고 스냅샷 실패 확률이 크게 감소합니다.

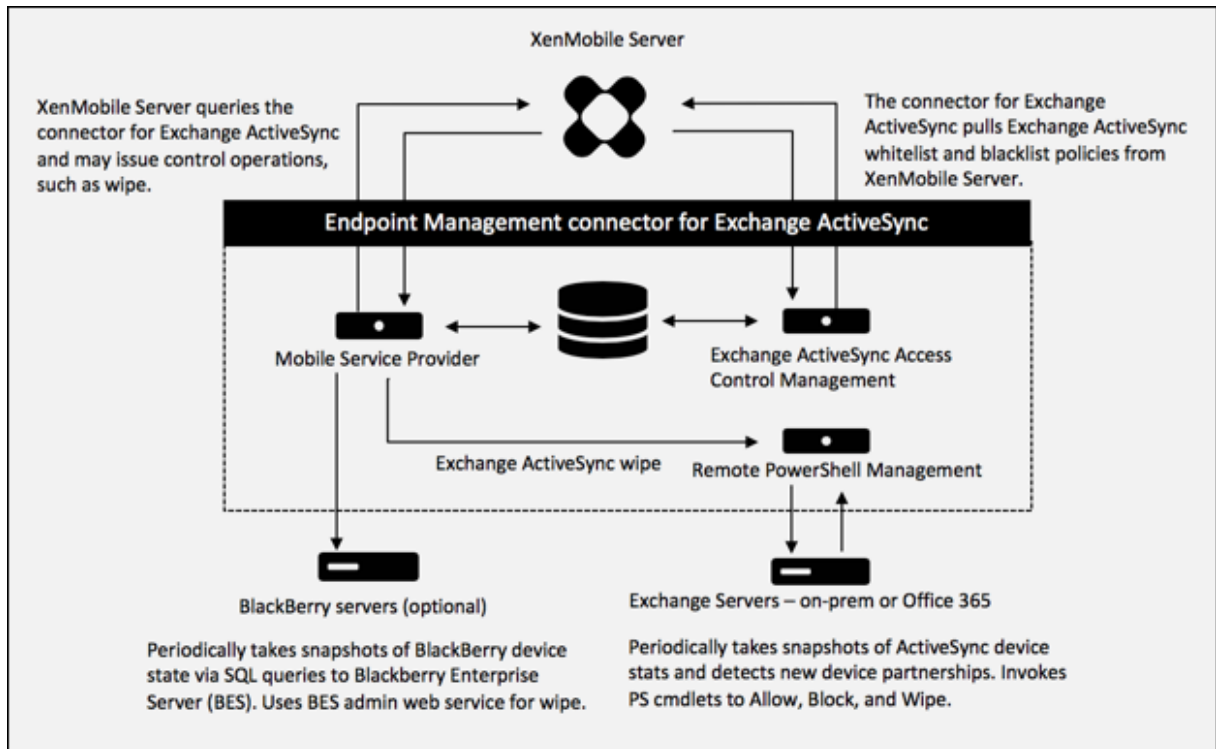
- 스냅샷 워크플로 개선: 주 스냅샷을 생성하는 데 시간이 오래 걸리고 프로세스가 복잡합니다. 이제 스냅샷 생성 중에 오류가 발생할 경우 XenMobile Mail Manager 가 여러 번의 시도 (최대 3 회) 를 통해 스냅샷을 완료합니다. 후속 시도는 처음부터 시작되지 않습니다. XenMobile Mail Manager 는 중단된 위치에서 시도를 계속합니다. 스냅샷을 진행하는 동안 일시적인 오류를 넘길 수 있으므로 일반적으로 스냅샷 성공률이 개선됩니다.
- 진단 개선: 스냅샷 중에 선택적으로 생성할 수 있는 새로운 세 가지 진단 파일을 사용하여 스냅샷 문제를 이제 보다 쉽게 해결할 수 있습니다. 이러한 파일은 PowerShell 명령 문제, 정보가 누락된 사서함 및 사서함에 연결할 수 없는 장치를 식별하는 데 도움이 됩니다. 관리자는 이러한 파일을 사용하여 Exchange 에서 수정할 수 없는 데이터를 식별할 수 있습니다.
- 메모리 사용 개선: 이제 XenMobile Mail Manager 가 보다 효율적으로 메모리를 사용합니다. 관리자는 XenMobile Mail Manager 를 자동으로 다시 시작하도록 예약하여 시스템에 정리된 슬레이트를 제공할 수 있습니다.
- **Microsoft .NET Framework 4.6** 사전 요구 사항: Microsoft .NET Framework 의 사전 요구 사항은 이제 버전 4.6 입니다.

수정된 문제

- 자격 증명 오류 표시: 이 오류는 종종 Office 365 세션 불안정으로 인해 발생했습니다. Exchange 에 대한 연결 개선으로 이 문제가 해결됩니다. (XMHELP-293, XMHELP-311, XMHELP-801)
- 정확하지 않은 사서함 및 장치 수: XenMobile Mail Manager 의 사서함-장치 연결 알고리즘이 개선되었습니다. 개선된 진단 기능을 사용하면 XenMobile Mail Manager 가 책임 영역 내에 없다고 간주하는 사서함 및 장치를 식별할 수 있습니다. (XMHELP-623)
- 허용/차단/초기화 명령이 인식되지 않음: 가끔 XenMobile Mail Manager 허용/차단/초기화 명령이 인식되지 않는 버그가 수정되었습니다. (XMHELP-489)
- 메모리 관리: 메모리 관리 및 완화가 개선되었습니다. (XMHELP-419)

아키텍처

다음 그림에서는 Exchange ActiveSync 용 Endpoint Management 커넥터의 주요 구성 요소를 보여 줍니다. 자세한 참조 아키텍처 다이어그램은 [아키텍처](#)를 참조하십시오.



세 가지 주요 구성 요소는 다음과 같습니다.

- **Exchange ActiveSync 액세스 제어 관리:** XenMobile 과 통신하여 XenMobile 에서 Exchange ActiveSync 정책을 검색하고 이 정책을 로컬로 정의된 정책과 병합하여 Exchange 에 대한 액세스가 허용 또는 거부되어야 하는 Exchange ActiveSync 장치를 결정합니다. 로컬 정책을 통해 Active Directory 그룹, 사용자, 장치 유형 또는 장치 사용자 에이전트 (일반적으로 모바일 플랫폼 버전) 별로 액세스 제어를 허용하도록 정책 규칙을 확장할 수 있습니다.
- **원격 PowerShell 관리:** 원격 PowerShell 명령을 예약하고 호출하여 Exchange ActiveSync Access Control Management 에서 작성된 정책을 시행합니다. 주기적으로 Exchange ActiveSync 데이터베이스의 스냅샷을 생성하여 변경되었거나 새로운 Exchange ActiveSync 장치를 감지합니다.
- **모바일 서비스 공급자:** XenMobile 이 Exchange ActiveSync 및/또는 Blackberry 장치를 쿼리하고 이러한 장치에 대한 초기화 같은 제어 작업을 실행할 수 있도록 웹 서비스 인터페이스를 제공합니다.

시스템 요구 사항 및 사전 요구 사항

다음은 Exchange ActiveSync 용 Endpoint Management 커넥터를 사용하는 데 필요한 최소 시스템 요구 사항입니다.

- Windows Server 2016, Windows Server 2012 R2 또는 Windows Server 2008 R2 서비스 팩 1. 영어 기반 서버여야 합니다. Windows Server 2008 R2 서비스 팩 1 에 대한 지원은 2020 년 1 월 14 일에 종료되며, Windows Server 2012 R2 에 대한 지원은 2023 년 10 월 10 일에 종료됩니다.
- Microsoft SQL Server 2016 서비스 팩 2 또는 SQL Server 2014 서비스 팩 3.
- Microsoft .NET Framework 4.6.

- BlackBerry Enterprise Service, 버전 5(선택 사항).

Microsoft Exchange Server 의 지원되는 최소 버전

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013(2023 년 4 월 11 일에 지원 종료)
- Exchange Server 2010 서비스 팩 3(2020 년 1 월 14 일에 지원 종료)

사전 요구 사항

- Windows Management Framework 가 설치되어 있어야 합니다.
 - PowerShell V5, V4, V3
- PowerShell 실행 정책이 Set-ExecutionPolicy RemoteSigned 를 통해 RemoteSigned 로 설정되어 있어야 합니다.
- Exchange ActiveSync 용 Endpoint Management 커넥터를 실행하는 컴퓨터와 원격 Exchange Server 사이에 TCP 포트 80 이 열려 있어야 합니다.
- 장치 전자 메일 클라이언트: 일부 전자 메일 클라이언트는 한 장치에 대해 동일한 ActiveSync ID 를 일관되게 반환하지 않습니다. Exchange ActiveSync 용 Endpoint Management 커넥터에서는 각 장치에 고유한 ActiveSync ID 를 사용하도록 요구하므로 각 장치에 대해 동일한 고유 ActiveSync ID 를 일관되게 생성하는 전자 메일 클라이언트만 지원됩니다. 다음과 같은 전자 메일 클라이언트는 Citrix 의 테스트에서 오류 없이 실행되는 것으로 확인되었습니다.
 - Samsung 기본 전자 메일 클라이언트
 - iOS 기본 전자 메일 클라이언트

- **Exchange:** Exchange 를 실행하는 온-프레미스 컴퓨터의 요구 사항은 다음과 같습니다.

Exchange 구성 UI 에 지정된 자격 증명으로 Exchange Server 에 연결할 수 있고 다음 Exchange 관련 PowerShell cmdlet 을 실행할 수 있는 전체 권한이 이 자격 증명에 있어야 합니다.

- **Exchange Server 2010 SP2** 의 경우:

- ★ Get-CASMailbox
- ★ Set-CASMailbox
- ★ Get-Mailbox
- ★ Get-ActiveSyncDevice
- ★ Get-ActiveSyncDeviceStatistics
- ★ Clear-ActiveSyncDevice
- ★ Get-ExchangeServer
- ★ Get-ManagementRole
- ★ Get-ManagementRoleAssignment

– **Exchange Server 2013** 및 **Exchange Server 2016** 의 경우:

- ★ Get-CASMailbox
 - ★ Set-CASMailbox
 - ★ Get-Mailbox
 - ★ Get-MobileDevice
 - ★ Get-MobileDeviceStatistics
 - ★ Clear-MobileDevice
 - ★ Get-ExchangeServer
 - ★ Get-ManagementRole
 - ★ Get-ManagementRoleAssignment
- Exchange ActiveSync 용 Endpoint Management 커넥터가 전체 포리스트를 보도록 구성된 경우 **Set-AdServerSettings -ViewEntireForest \$true** 를 실행할 수 있는 권한이 부여되어 있어야 합니다.
- 제공된 자격 증명에 원격 셸을 통해 Exchange Server 에 연결할 수 있는 권한이 있어야 합니다. 기본적으로 Exchange 를 설치한 사용자가 이 권한을 갖습니다.
- 원격 연결을 설정하고 원격 명령을 실행하려면 원격 컴퓨터 관리자인 사용자에게 해당하는 자격 증명이 있어야 합니다. Set-PSSessionConfiguration 을 사용하여 관리 요구 사항을 제거할 수 있지만 이 명령에 대한 설명은 이 문서에 나와 있지 않습니다. 자세한 내용은 Microsoft 문서 [세션 구성 정보](#)를 참조하십시오.
- HTTP 를 통해 원격 PowerShell 요청을 지원하도록 Exchange Server 를 구성해야 합니다. 일반적으로 Exchange Server 에서 다음 PowerShell 명령을 실행하는 관리자이면 됩니다. WinRM QuickConfig.
- Exchange 에는 많은 제한 정책이 있습니다. 정책 중 하나는 사용자당 허용되는 동시 PowerShell 연결 수를 제어합니다. Exchange 2010 의 경우 사용자당 허용되는 동시 연결 수의 기본값은 18 입니다. 연결 제한에 도달하면, Exchange ActiveSync 용 Endpoint Management 커넥터에서 Exchange Server 에 연결할 수 없습니다. PowerShell 을 통해 허용되는 최대 동시 연결 수를 변경하는 방법이 있지만 이 문서의 범위를 벗어나 있습니다. 관심 있는 경우 PowerShell 을 통한 원격 관리와 관련된 Exchange 제한 정책에 대해 알아보십시오.

Office 365 Exchange 에 대한 요구 사항

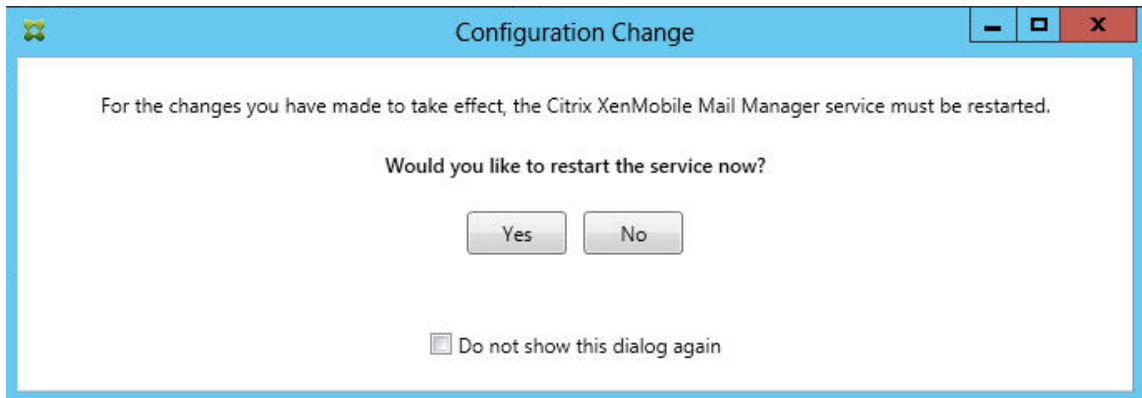
- 권한: Exchange 구성 UI 에 지정된 자격 증명으로 Office 365 에 연결할 수 있고 다음 Exchange 관련 PowerShell cmdlet 을 실행할 수 있는 전체 권한이 이 자격 증명에 있어야 합니다.
 - Get-CASMailbox
 - Set-CASMailbox
 - Get-Mailbox
 - Get-MobileDevice
 - Get-MobileDeviceStatistics
 - Clear-MobileDevice
 - Get-ExchangeServer
 - Get-ManagementRole
 - Get-ManagementRoleAssignment

- **권한:** 제공된 자격 증명에 원격 셀을 통해 Office 365 서버에 연결할 수 있는 권한이 있어야 합니다. 기본적으로 Office 365 온라인 관리자에게는 필수 권한이 있습니다.
- **제한 정책:** Exchange 에는 많은 제한 정책이 있습니다. 정책 중 하나는 사용자당 허용되는 동시 PowerShell 연결 수를 제어합니다. Office 365 의 경우 사용자당 허용되는 동시 연결 수의 기본값은 3 입니다. 연결 제한에 도달하면, Exchange ActiveSync 용 Endpoint Management 커넥터에서 Exchange Server 에 연결할 수 없습니다. PowerShell 을 통해 허용되는 최대 동시 연결 수를 변경하는 방법이 있지만 이 문서의 범위를 벗어나 있습니다. 관심 있는 경우 PowerShell 을 통한 원격 관리와 관련된 Exchange 제한 정책에 대해 알아보십시오.

설치 및 구성

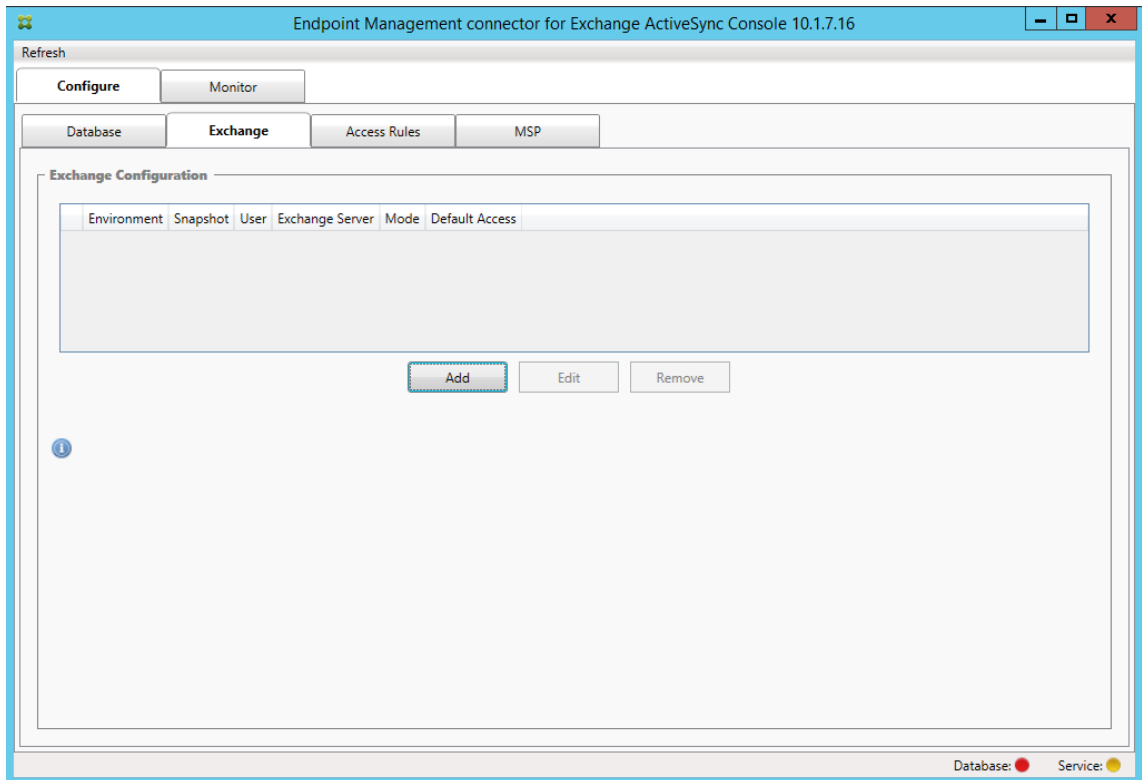
1. XmmSetup.msi 파일을 클릭한 후 설치 프로그램의 메시지에 따라 Exchange ActiveSync 용 Endpoint Management 커넥터를 설치합니다.
2. 설치 마법사의 마지막 화면에서 **Launch the Configure utility(구성 유틸리티 실행)** 를 선택한 상태로 둡니다. 또는 **Start(시작)** 메뉴에서 Exchange ActiveSync 용 Endpoint Management 커넥터를 엽니다.
3. 다음 데이터베이스 속성을 구성합니다.
 - **Configure(구성) > Database(데이터베이스)** 탭을 선택합니다.
 - SQL Server 의 이름을 입력합니다 (기본값은 localhost).
 - 데이터베이스를 기본값인 **CitrixXmm** 으로 유지합니다.
4. SQL 에 사용되는 다음 인증 모드 중 하나를 선택합니다.
 - **SQL:** 유효한 SQL 사용자의 사용자 이름과 암호를 입력합니다.
 - **Windows Integrated(Windows 통합):** 이 옵션을 선택하는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스의 로그인 자격 증명을 SQL Server 액세스 권한이 있는 Windows 계정으로 변경해야 합니다. 이렇게 하려면 제어판 > 관리 도구 > 서비스를 열고 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스 항목을 마우스 오른쪽 단추로 클릭한 후 로그인 탭을 클릭합니다.

BlackBerry 데이터베이스 연결에 Windows 통합을 선택하는 경우 여기서 지정하는 Windows 계정에 BlackBerry 데이터베이스 액세스 권한이 있어야 합니다.
5. **Test Connectivity(연결 테스트)** 를 클릭하여 SQL Server 에 연결되는지 확인한 후 **Save(저장)** 를 클릭합니다.
6. 서비스를 다시 시작하라는 메시지가 표시됩니다. **Yes(예)** 를 클릭합니다.



7. 하나 이상의 Exchange Server 를 구성합니다.

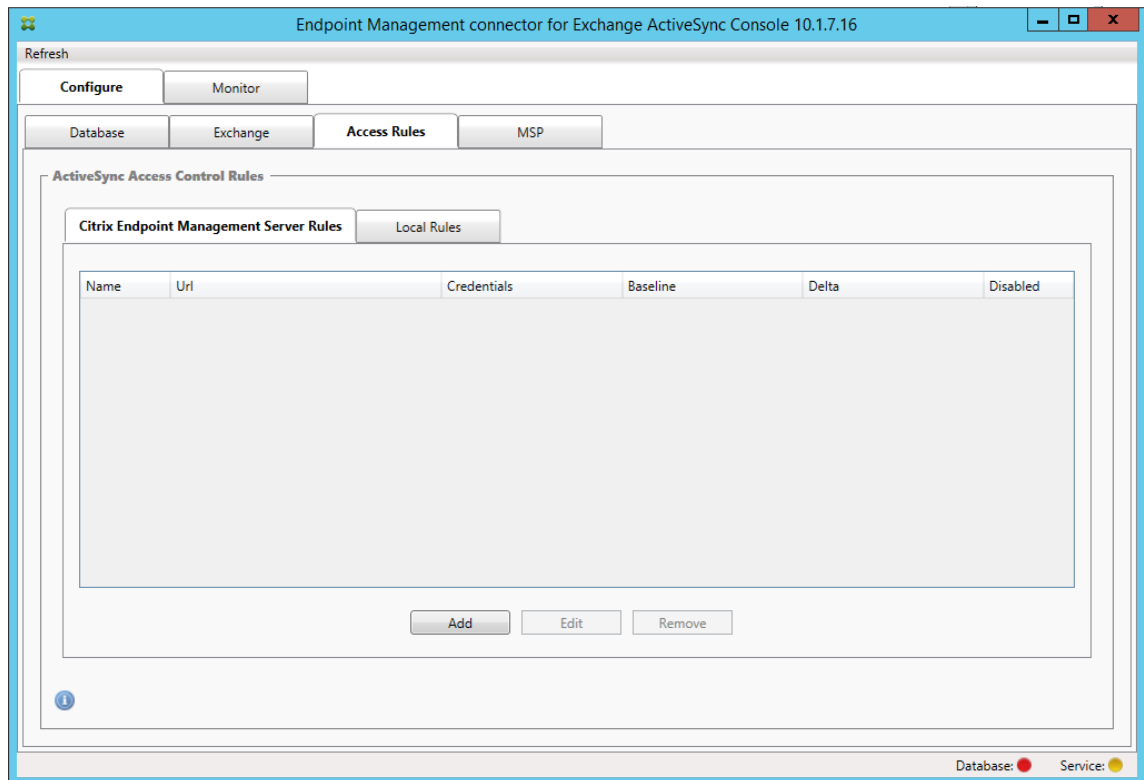
- 단일 Exchange 환경을 관리하는 경우 단일 서버만 지정합니다. 여러 Exchange 환경을 관리하는 경우 각 Exchange 환경에 하나의 Exchange Server 를 지정합니다.
- **Configure(구성) > Exchange** 탭을 클릭하고 **Add(추가)** 를 클릭합니다.



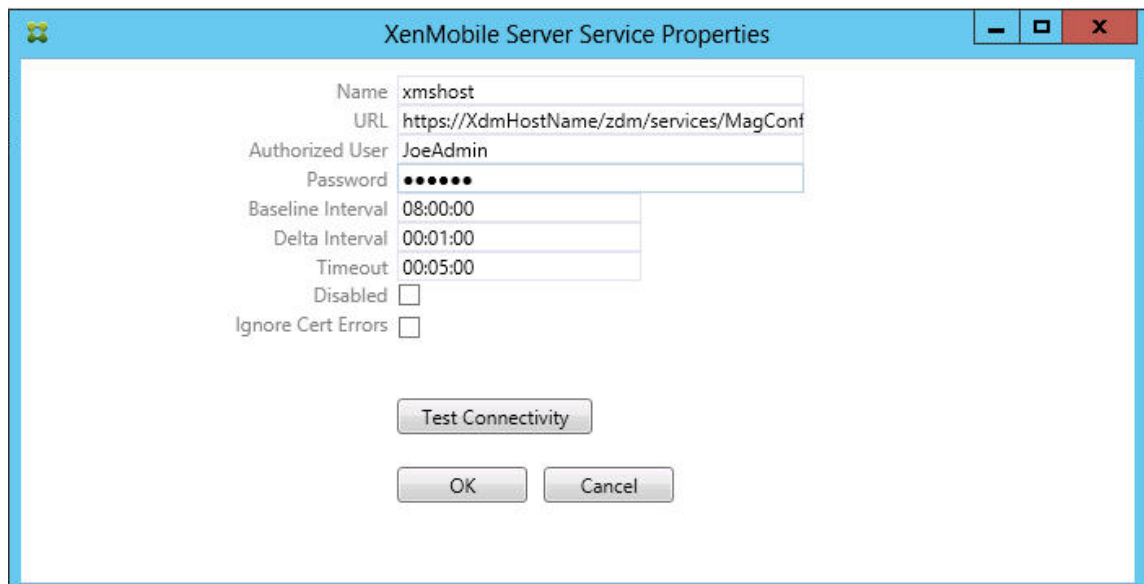
8. Exchange Server 환경 유형을 **On Premise**(온 프레미스) 또는 **Office 365** 중에서 선택합니다.

- **On Premise**(온-프레미스) 를 선택하는 경우 원격 PowerShell 명령에 사용할 Exchange Server 의 이름을 입력합니다.
- Requirements(요구 사항) 섹션에 명시된 대로 적절한 Exchange Server 권한이 있는 Windows ID 의 사용자 이름을 입력하고 사용자에게 대한 암호를 입력합니다.
- 주 스냅샷을 실행할 일정을 선택합니다. 주 스냅샷은 모든 Exchange ActiveSync 파트너 관계를 검색합니다.

- 부 스냅샷을 실행할 일정을 선택합니다. 부 스냅샷은 새로 생성된 Exchange ActiveSync 파트너 관계를 검색합니다.
 - 스냅샷 유형을 **Deep(전체)** 또는 **Shallow(단순)** 중에서 선택합니다. 단순 스냅샷은 일반적으로 훨씬 빠르며 Exchange ActiveSync 용 Endpoint Management 커넥터의 모든 Exchange ActiveSync 액세스 제어 기능을 수행하기에 충분합니다. 전체 스냅샷은 더 긴 시간이 소요될 수 있으며 ActiveSync 에 대해 모바일 서비스 공급자를 사용하는 경우에만 필요합니다. 이 옵션을 사용하면 XenMobile 에서 관리되지 않는 장치를 쿼리할 수 있습니다.
 - **Allow(허용)**, **Block(차단)** 또는 **Unchanged(변경되지 않음)** 중에서 기본 액세스 권한을 선택합니다. 이 설정은 명시적인 XenMobile 또는 로컬 규칙에 의해 식별되지 않은 모든 장치를 어떻게 처리할지를 제어합니다. **Allow(허용)** 를 선택하면 이러한 모든 장치에 대한 ActiveSync 액세스가 허용됩니다. **Block(차단)** 을 선택하면 액세스가 거부됩니다. **Unchanged(변경되지 않음)** 를 선택하면 변경이 수행되지 않습니다.
 - **PowerShell** 또는 **Simulation(시뮬레이션)** 중에서 ActiveSync 명령 모드를 선택합니다.
 - **PowerShell** 모드에서 Exchange ActiveSync 용 Endpoint Management 커넥터는 PowerShell 명령을 실행하여 원하는 액세스 제어를 수행합니다. 시뮬레이션 모드에서 Exchange ActiveSync 용 Endpoint Management 커넥터는 PowerShell 명령을 실행하지 않지만 의도한 명령 및 의도한 결과를 데이터베이스에 기록합니다. 시뮬레이션 모드에서 사용자는 **Monitor(모니터)** 탭을 사용하여 PowerShell 모드를 사용할 경우 일어나는 결과를 볼 수 있습니다.
 - **Connection Expiration(연결 만료)** 에서 연결 수명에 대한 시간 및 분을 설정합니다. 연결이 지정된 수명에 도달하면 만료된 연결로 표시되고 다시 사용되지 않습니다. 만료된 연결이 더 이상 사용되지 않으면 Exchange ActiveSync 용 Endpoint Management 커넥터가 연결을 정상적으로 종료합니다. 연결이 다시 필요할 경우, 사용 가능한 연결이 없으면 새로운 연결이 초기화됩니다. 지정되지 않은 경우 기본값인 30 분이 사용됩니다.
 - **View Entire Forest(전체 포리스트 보기)** 를 선택하여 Exchange 환경의 전체 Active Directory 포리스트를 보도록 Exchange ActiveSync 용 Endpoint Management 커넥터를 구성합니다.
 - **Kerberos** 또는 **Basic(기본)** 중에서 인증 프로토콜을 선택합니다. Exchange ActiveSync 용 Endpoint Management 커넥터는 온-프레미스 배포에서 기본 인증을 지원합니다. 따라서 Exchange ActiveSync 용 Endpoint Management 커넥터가 Exchange Server 가 상주하는 도메인의 구성원이 아닌 경우 Exchange ActiveSync 용 Endpoint Management 커넥터를 사용할 수 있습니다.
 - **Test Connectivity(연결 테스트)** 를 클릭하여 Exchange Server 에 연결되는지 확인한 후 **Save(저장)** 를 클릭합니다.
 - 서비스를 다시 시작하라는 메시지가 표시됩니다. **Yes(예)** 를 클릭합니다.
9. 액세스 규칙을 구성합니다. **Configure(구성) > Access Rules(액세스 규칙)** 탭을 선택하고 **XMS Rules(XMS 규칙)** 탭을 클릭한 다음 **Add(추가)** 를 클릭합니다.



10. **XenMobile server Service Properties(XenMobile 서버 서비스 속성)** 페이지에서 XenMobile Server 를 가리키도록 URL 문자열을 수정합니다. 예를 들어 인스턴스 이름이 **zdm** 인 경우 <https://<XdmHostName>/zdm/services/MagConfigService>를 입력합니다. 이 예에서는 **XdmHostName** 을 XenMobile Server 의 IP 또는 DNS 주소로 바꿉니다.



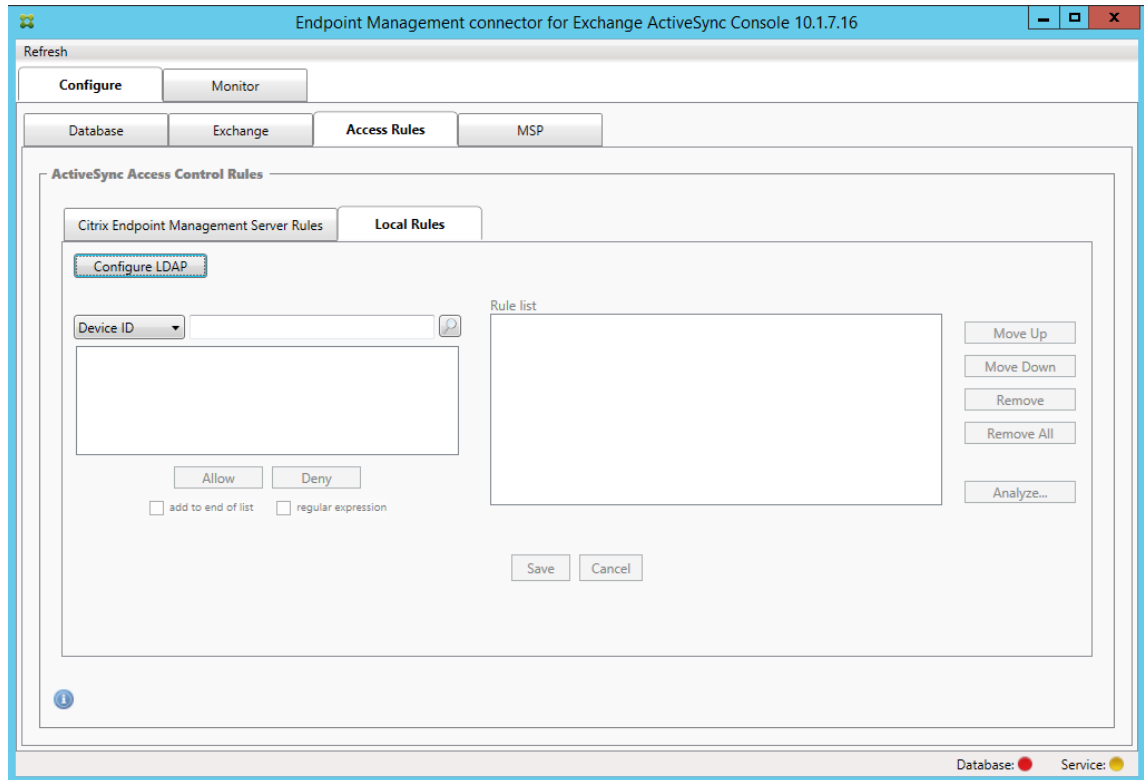
- 권한이 있는 서버 사용자를 입력합니다.
- 사용자의 암호를 입력합니다.
- **Baseline Interval**(기준 간격), **Delta Interval**(델타 간격) 및 **Timeout values**(시간 초과 값) 를 기본

값으로 유지합니다.

- **Test Connectivity**(연결 테스트) 를 클릭하여 서버 연결을 확인한 후 **OK**(확인) 를 클릭합니다.

Disabled(사용 안 함) 확인란이 선택된 경우 XenMobile 메일 서비스가 XenMobile 에서 정책을 수집하지 않습니다.

11. **Local Rules**(로컬 규칙) 탭을 클릭합니다.



- ActiveSync 장치 ID, 장치 유형, AD 그룹, 사용자 또는 장치 UserAgent 를 기준으로 로컬 규칙을 추가할 수 있습니다. 목록에서 해당하는 유형을 선택합니다.
- 텍스트 상자에 텍스트 또는 텍스트 부분을 입력합니다. 필요한 경우 쿼리 단추를 클릭하여 부분과 일치하는 엔터티를 봅니다.

Group(그룹) 유형이 아닌 다른 모든 유형은 스냅샷에서 검색된 장치에 기반합니다. 따라서 스냅샷을 시작하고 완료하지 않은 경우 엔터티가 제공되지 않습니다.

- 텍스트 값을 선택한 후 **Allow**(허용) 또는 **Deny**(거부) 를 클릭하여 오른쪽의 **Rule List**(규칙 목록) 창에 추가합니다. **Rule List**(규칙 목록) 창 오른쪽의 단추를 사용하여 규칙 순서를 변경하거나 제거할 수 있습니다. 규칙은 지정된 사용자 및 장치에 대해 규칙이 표시된 순서로 평가되고 순서가 높은 규칙 (최상위 규칙에 가까운 규칙) 에 대한 일치 항목이 검색되면 다음 규칙이 적용되지 않으므로 그 순서가 중요합니다. 예를 들어 모든 iPad 장치를 허용하는 규칙과 사용자 Matt 를 차단하는 후속 규칙이 있는 경우 iPad 규칙이 Matt 규칙보다 적용 우선 순위가 높으므로 Matt 의 iPad 가 허용됩니다.
- 규칙 목록 내의 규칙을 분석하여 잠재적 재정의, 충돌 또는 보조 구성을 찾으려면 **Analyze**(분석) 를 클릭하고 **Save**(저장) 를 클릭합니다.

12. Active Directory 그룹에서 작동하는 로컬 규칙을 구성하려는 경우 **Configure LDAP(LDAP 구성)** 를 클릭한 후 LDAP 연결 속성을 구성합니다.

The image shows the 'LDAP Configuration' dialog box. It contains the following fields and controls:

- Address:** LDAP://DC=test, DC=net
- Authentication:** None (dropdown menu)
- User:** JoeAdmin@test.net
- Password:** [Redacted with dots]
- Test Connectivity:** A button that has been clicked, resulting in a success message.
- Message:** Connection succeeded: 155 groups found
- Buttons:** OK and Cancel

13. 모바일 서비스 공급자를 구성합니다.

모바일 서비스 공급자는 선택 사항입니다. 이 설정은 모바일 서비스 공급자 인터페이스를 사용하여 관리되지 않는 장치를 쿼리하도록 XenMobile 을 구성한 경우에만 필요합니다.

- **Configure(구성) > MSP** 탭을 클릭합니다.

The image shows the 'Endpoint Management connector for Exchange ActiveSync Console 10.1.7.16' window. The 'MSP' tab is selected, showing the 'MSP Web Service Configuration' section. It includes the following fields and controls:

- Service Transport:** None (dropdown menu)
- Service Port:** 443
- Authorization:** Group (dropdown menu)
- Administrators:** [Redacted]
- Enable ActiveSync:** [Checked]
- Filter ActiveSync:** WorxMail.*
- Buttons:** Save and Cancel

Below the 'MSP Web Service Configuration' section is the 'Blackberry Configuration' section, which includes a table with columns for 'Blackberry SQL Server', 'Database Name', and 'BAS Server'. The table is currently empty. Below the table are 'Add', 'Edit', and 'Remove' buttons.

- 모바일 서비스 공급자 서비스에 대한 Service Transport(서비스 전송) 유형을 **HTTP** 또는 **HTTPS** 로 설정합니다.
- 모바일 서비스 공급자 서비스에 대한 서비스 포트 (일반적으로 80 또는 443) 를 설정합니다. 포트 443 을 사용하는 경우 IIS 에서 포트에 바인딩된 SSL 인증서가 필요합니다.
- **Authorization Group**(인증 그룹) 또는 **User**(사용자) 를 설정합니다. 이 설정은 XenMobile 에서 모바일 서비스 공급자 서비스에 연결할 수 있는 사용자 또는 사용자 집합을 설정합니다.
- ActiveSync 쿼리를 사용할지 여부를 설정합니다. XenMobile Server 에 대해 ActiveSync 쿼리를 사용하는 경우 하나 이상의 Exchange Server 에 대한 스냅샷 유형을 **Deep**(전체) 으로 설정해야 합니다. 이 경우 스냅샷 생성 시 성능이 크게 저하될 수 있습니다.
- 기본적으로 정규식 WorxMail.* 와 일치하는 ActiveSync 장치는 XenMobile 로 전송되지 않습니다. 이 동작을 변경하려면 **Filter ActiveSync**(ActiveSync 필터링) 필드를 필요에 따라 변경합니다.
비워 두면 모든 장치가 XenMobile 에 전달됩니다.
- 저장을 클릭합니다.

14. 필요한 경우 BES(BlackBerry Enterprise Server) 를 구성합니다. **Add**(추가) 를 클릭하고 BES SQL Server 의 서버 이름을 입력합니다.

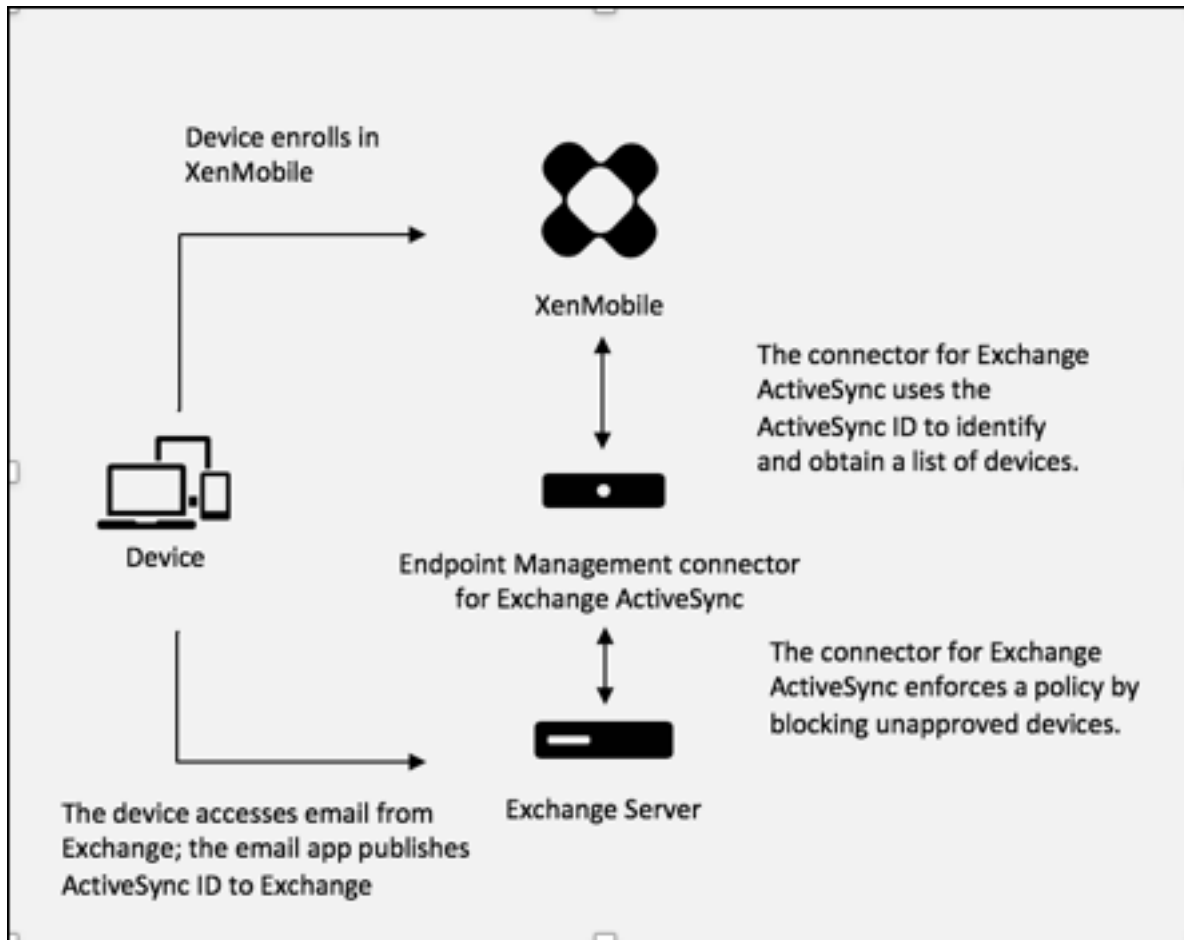
The screenshot shows the 'BES Properties' window. It is divided into two main sections. The top section, 'BES Sql Server', contains input fields for 'Server' (BesServer), 'Database' (BesMgmt), 'Authentication' (a dropdown menu showing 'Sql'), 'User name' (JoeAdmin), and 'Password' (masked with dots). Below these fields is a 'Test Connectivity' button and a 'Sync Schedule' dropdown menu set to 'Every 30 Minutes'. The bottom section, 'Blackberry Device Administration from XMS', has an 'Enabled' checkbox that is checked. Below it are fields for 'BAS Server' (BAServer), 'BAS Port' (443), 'Domain\User' (ServerName\JoeAdmin), and 'Password' (masked with dots). A 'Test Connectivity' button is also present. At the very bottom of the window are 'Save' and 'Cancel' buttons.

- BES 관리 데이터베이스의 데이터베이스 이름을 입력합니다.
- **Authentication(인증)** 모드를 선택합니다. Windows 통합 인증을 선택하는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스의 사용자 계정이 BES SQL Server 에 연결할 때 사용되는 계정입니다. Exchange ActiveSync 용 Endpoint Management 커넥터 데이터베이스 연결에 대해서도 Windows 통합 인증을 선택하는 경우 여기서 지정한 Windows 계정에 Exchange ActiveSync 용 Endpoint Management 커넥터 데이터베이스에 액세스할 수 있는 권한이 있어야 합니다.
- **SQL authentication(SQL 인증)** 을 선택하는 경우 사용자 이름과 암호를 입력합니다.
- **Sync Schedule(동기화 일정)** 을 설정합니다. BES SQL Server 에 연결할 때 사용되는 일정이며 모든 장치 업데이트를 확인합니다.
- **Test Connectivity(연결 테스트)** 를 클릭하여 SQL Server 연결을 확인합니다. Windows 통합을 선택하는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스 사용자가 아닌 현재 로그인한 사용자를 사용하여 테스트가 수행되므로 SQL 인증이 정확히 테스트되지 않습니다.
- XenMobile 에서 BlackBerry 장치의 원격 초기화 및 암호 재설정을 지원하려면 **Enabled(사용)** 확인란을 선택합니다.
- BES FQDN(정규화된 도메인 이름) 을 입력합니다.
- 관리 웹 서비스에 사용되는 BES 포트를 입력합니다.
- BES 서비스에 필요한 정규화된 사용자 및 암호를 입력합니다.
- **Test Connectivity(연결 테스트)** 를 클릭하여 BES 연결을 테스트합니다.
- 저장을 클릭합니다.

ActiveSync ID 를 사용하여 전자 메일 정책 적용

회사 전자 메일 정책에 따라 특정 장치가 회사 전자 메일을 사용하도록 승인되지 않을 수 있습니다. 이 정책을 준수하려면 직원이 그와 같은 장치에서 회사 전자 메일에 액세스할 수 없도록 해야 합니다. Exchange ActiveSync 용 Endpoint Management 커넥터 및 XenMobile 은 함께 작동하여 이러한 전자 메일 정책을 적용합니다. XenMobile 은 회사 전자 메일 액세스에 대한 정책을 설정하고 승인되지 않은 장치가 XenMobile 에 등록하면 Exchange ActiveSync 용 Endpoint Management 커넥터가 정책을 적용합니다.

장치의 전자 메일 클라이언트는 장치를 식별하는 데 사용되는 장치 ID(ActiveSync ID 라고도 함) 를 사용하여 자신을 Exchange Server(또는 Office 365) 에 알립니다. Secure Hub 는 유사한 식별자를 구하고 장치가 등록될 때 XenMobile 에 해당 식별자를 보냅니다. 두 장치 ID 를 비교하여 Exchange ActiveSync 용 Endpoint Management 커넥터는 특정 장치에 회사 전자 메일 액세스 권한이 있는지 여부를 결정할 수 있습니다. 다음 그림에서는 이 개념을 보여 줍니다.



XenMobile 이 장치가 게시하는 ID 와 다른 Exchange ActiveSync 용 Endpoint Management 커넥터 ID 를 Exchange 에 보내는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터가 장치로 수행할 작업을 Exchange 에 알릴 수 없습니다.

ActiveSync ID 일치는 대부분의 플랫폼에서 안정적으로 작동합니다. 하지만 일부 Android 구현 환경에서 장치의 ActiveSync ID 가 메일 클라이언트가 Exchange 에 알리는 ID 와 다르다는 것이 밝혀졌습니다. 이 문제를 완화하려면 다음을 수행할 수 있습니다.

- Samsung SAFE 플랫폼에서는 XenMobile 에서 장치 ActiveSync 구성을 무시합니다.

회사 전자 메일 액세스 정책이 올바르게 적용되도록 하려면 방어적 보안 입장을 채택하고 기본적으로 거부하는 정적 정책을 설정하여 전자 메일을 차단하도록 Exchange ActiveSync 용 Endpoint Management 커넥터를 구성할 수 있습니다. 즉, 직원이 Android 장치에서 전자 메일 클라이언트를 구성하는 경우와 ActiveSync ID 검색이 제대로 작동하지 않는 경우 해당 직원의 회사 전자 메일 액세스가 거부됩니다.

액세스 제어 규칙

Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange ActiveSync 장치에 대한 액세스 제어를 동적으로 구성하는 규칙 기반 접근 방식을 제공합니다. Exchange ActiveSync 용 Endpoint Management 커넥터 액세스

제어 규칙은 일치하는 식과 원하는 액세스 상태 (허용 또는 차단) 의 두 부분으로 구성됩니다. 지정된 Exchange ActiveSync 장치에 대해 규칙을 평가하여 규칙이 장치에 적용되는지 또는 장치와 일치하는지를 결정할 수 있습니다. 일치하는 식에는 여러 종류가 있습니다. 예를 들어 규칙은 지정된 장치 유형의 모든 장치 또는 특정 Exchange ActiveSync 장치 ID 또는 특정 사용자의 모든 장치와 일치할 수 있습니다.

규칙 목록의 규칙을 추가, 제거 및 재정렬하는 동안 언제든지 **Cancel(취소)** 단추를 클릭하면 처음 규칙 목록을 열었을 때의 상태로 목록이 되돌려집니다. **Save(저장)** 를 클릭하지 않고 구성 도구를 닫으면 이 창에서 수행한 변경 내용이 손실됩니다.

Exchange ActiveSync 용 Endpoint Management 커넥터에는 로컬 규칙, XenMobile Server 규칙 (XDM 규칙이라고도 함) 및 기본 액세스 규칙의 세 가지 규칙이 있습니다.

로컬 규칙: 로컬 규칙은 우선 순위가 가장 높습니다. 로컬 규칙에 일치하는 장치가 있을 경우 규칙 평가가 중지됩니다. XenMobile Server 규칙 또는 기본 액세스 규칙은 확인되지 않습니다. 로컬 규칙은 **Configure(구성) > Access Rules(액세스 규칙) > Local Rules(로컬 규칙)** 탭을 통해 Exchange ActiveSync 용 Endpoint Management 커넥터에 로컬로 구성됩니다. 지원 일치는 지정된 Active Directory 그룹 내의 사용자 구성원 자격에 기반합니다. 지원 일치는 다음 필드에 대한 정규식에 기반합니다.

- ActiveSync Device ID(ActiveSync 장치 ID)
- ActiveSync Device Type(ActiveSync 장치 유형)
- User Principal Name (UPN)(UPN(사용자 계정 이름))
- ActiveSync User Agent(ActiveSync 사용자 에이전트)(일반적으로 장치 플랫폼 또는 전자 메일 클라이언트)

주 스냅샷이 완료되고 장치를 찾은 경우 일반 또는 정규식 규칙을 추가할 수 있습니다. 주 스냅샷이 완료되지 않은 경우 정규식 규칙만 추가할 수 있습니다.

XenMobile 서버 규칙: XenMobile Server 규칙은 관리되는 장치에 대한 규칙을 제공하는 외부 XenMobile Server 에 대한 참조입니다. XenMobile Server 는 XenMobile 에 알려진 속성 (예: 장치가 탈옥 장치인지 여부 또는 장치에 금지된 앱이 포함되었는지 여부) 을 기반으로 장치를 허용 또는 차단된 장치로 식별하는 간략한 규칙으로 구성될 수 있습니다. XenMobile 은 이 간략한 규칙을 평가하고 허용 또는 차단된 ActiveSync 장치 ID 집합을 생성한 다음 Exchange ActiveSync 용 Endpoint Management 커넥터에 전달합니다.

기본 액세스 규칙: 기본 액세스 규칙은 잠재적으로 모든 장치와 일치할 수 있고 항상 마지막에 평가된다는 것이 특징입니다. 이 규칙은 지정된 장치가 로컬 또는 XenMobile Server 규칙과 일치하지 않을 경우 기본 액세스 규칙의 원하는 액세스 상태가 장치의 원하는 액세스 상태를 결정하는 광범위한 규칙입니다.

- **Default Access - Allow(기본 액세스 - 허용):** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치가 허용됩니다.
- **Default Access - Block(기본 액세스 - 차단):** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치가 차단됩니다.
- **Default Access - Unchanged(기본 액세스 - 변경되지 않음):** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치의 액세스 상태가 Exchange ActiveSync 용 Endpoint Management 커넥터에 의해 수정되지 않습니다. Exchange 에서 장치를 격리 모드로 설정한 경우 아무런 조치도 취하지 않습니다. 예를 들어 장치를 격리 모드에서 제거하는 유일한 방법은 로컬 또는 XDM 규칙으로 격리를 명시적으로 재정의하는 것입니다.

규칙 평가 정보

Exchange 가 Exchange ActiveSync 용 Endpoint Management 커넥터에 보고하는 각 장치에 대해 다음과 같이 높은 우선 순위에서 낮은 우선 순위로 규칙이 평가됩니다.

- 로컬 규칙
- XenMobile Server 규칙
- 기본 액세스 규칙

일치가 발견되면 평가가 중지됩니다. 예를 들어 로컬 규칙이 지정된 장치와 일치할 경우 XenMobile Server 규칙 또는 기본 액세스 규칙으로 장치가 평가되지 않습니다. 이는 지정된 규칙 유형 내에서도 마찬가지입니다. 예를 들어 로컬 규칙 목록에 지정된 장치와 일치하는 규칙이 둘 이상인 경우 첫 번째 일치가 발견되면 평가가 중지됩니다.

장치 속성이 변경되거나 장치가 추가 또는 제거되거나 규칙 자체가 변경될 경우 Exchange ActiveSync 용 Endpoint Management 커넥터가 현재 정의된 규칙 집합을 다시 평가합니다. 주 스냅샷은 구성 가능한 간격으로 장치 속성 변경 및 제거를 확인합니다. 부 스냅샷은 구성 가능한 간격으로 새 장치를 확인합니다.

Exchange ActiveSync 에도 액세스를 제어하는 규칙이 있습니다. Exchange ActiveSync 용 Endpoint Management 커넥터의 컨텍스트에서 이러한 규칙의 작동 방식을 이해하는 것이 중요합니다. Exchange 는 개별 면제, 장치 규칙 및 조직 설정의 세 가지 규칙 수준으로 구성될 수 있습니다. Exchange ActiveSync 용 Endpoint Management 커넥터는 개별 면제 목록에 영향을 주는 원격 PowerShell 요청을 프로그래밍 방식으로 실행하여 액세스 제어를 자동화합니다. 개별 면제 목록은 지정된 사서함에 연결된 허용 또는 차단된 Exchange ActiveSync 장치 ID 의 목록입니다. Exchange ActiveSync 용 Endpoint Management 커넥터를 배포하면 Exchange 내 면제 목록의 관리가 실질적으로 커넥터에 이전됩니다. 자세한 내용은 Microsoft 문서 [장치 액세스 제어](#)를 참조하십시오.

분석은 동일한 필드에 여러 규칙이 정의된 경우 특히 유용합니다. 규칙 간의 관계 문제를 해결할 수 있습니다. 규칙 필드의 관점에서 분석을 수행합니다. 예를 들어, ActiveSync 장치 ID, ActiveSync 장치 유형, 사용자 및 사용자 에이전트와 같이 일치하는 필드를 기준으로 규칙을 그룹화하여 분석합니다.

규칙 용어

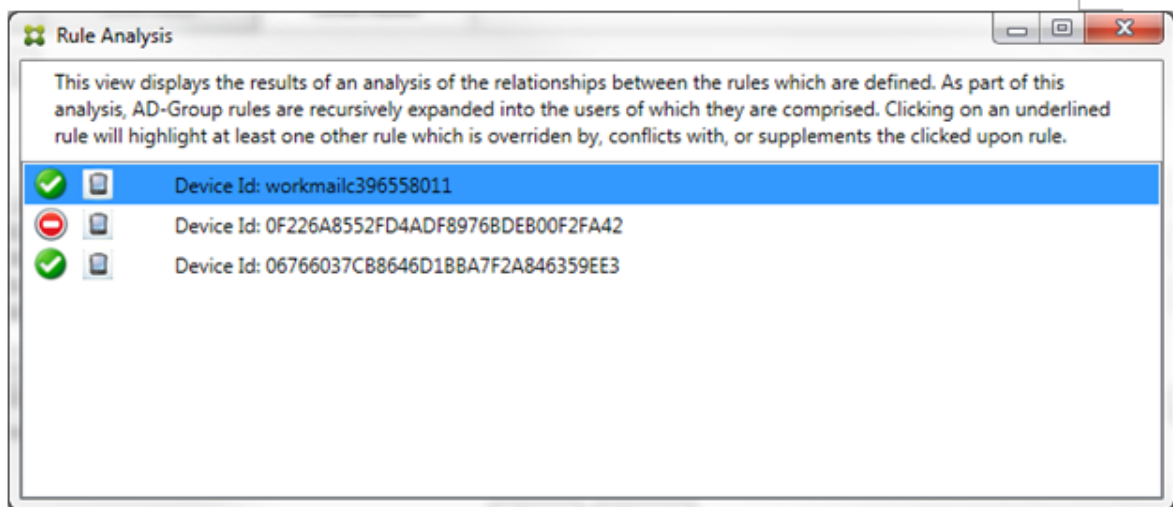
- **재정의 규칙:** 재정의는 둘 이상의 규칙이 동일한 장치에 적용될 수 있는 경우 발생합니다. 규칙은 목록의 우선 순위에 따라 평가되므로 적용될 수 있는 마지막의 규칙 인스턴스가 평가되지 않을 수 있습니다.
- **충돌 규칙:** 충돌은 둘 이상의 규칙이 동일한 장치에 적용될 수 있지만 액세스 (허용/차단) 가 일치하지 않는 경우 발생합니다. 충돌 규칙이 정규식 규칙이 아닌 경우 충돌은 항상 암시적으로 재정의를 의미합니다.
- **보완 규칙:** 보완은 둘 이상의 규칙이 정규식 규칙이어서 둘 이상의 정규식을 하나의 정규식 규칙으로 결합할 수 있는지, 또는 중복되는 기능이 아닌지를 확인해야 할 때 발생합니다. 보완 규칙은 액세스 (허용/차단) 에서도 충돌할 수 있습니다.
- **주 규칙:** 주 규칙은 대화 상자 안에서 클릭된 규칙입니다. 이 규칙은 실선 테두리로 표시됩니다. 또한 위 또는 아래를 가리키는 녹색 화살표가 하나 또는 두 개 포함됩니다. 화살표가 위를 가리키는 경우 주 규칙 앞에 보조 규칙이 있음을 나타냅니다. 화살표가 아래를 가리키는 경우 주 규칙 뒤에 보조 규칙이 있음을 나타냅니다. 한 번에 하나의 주 규칙만 활성화될 수 있습니다.
- **보조 규칙:** 보조 규칙은 재정의, 충돌 또는 추가 관계를 통해 주 규칙과 관련됩니다. 이 규칙은 파선 테두리로 표시됩니다. 각 주 규칙에 대해 여러 개의 보조 규칙이 있을 수 있습니다. 밑줄이 표시된 항목을 클릭하면 항상 주 규칙의 관점에서 보조

규칙인 규칙이 강조 표시됩니다. 예를 들어 보조 규칙은 주 규칙으로 재정의되고 주 규칙과 액세스에서 충돌하며 주 규칙을 보완합니다.

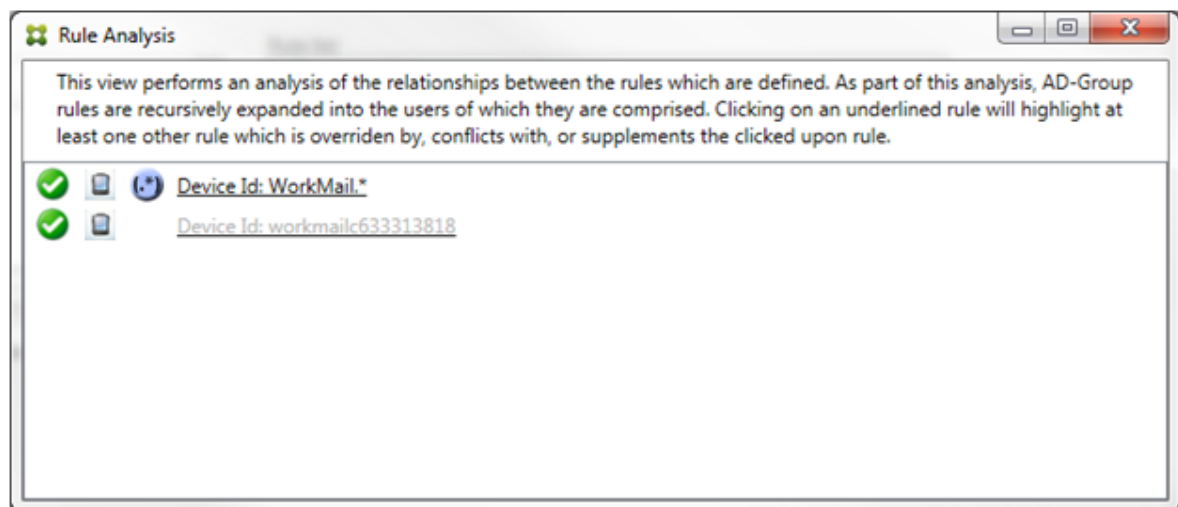
Rule Analysis(규칙 분석) 대화 상자에 규칙 유형이 표시되는 방법

충돌, 재정의 또는 보완이 없는 경우 Rule Analysis(규칙 분석) 대화 상자에 밑줄이 그어진 항목이 표시되지 않습니다. 항목을 클릭해도 아무런 영향이 없습니다. 예를 들어 선택된 항목이 일반적으로 모습으로 표시됩니다.

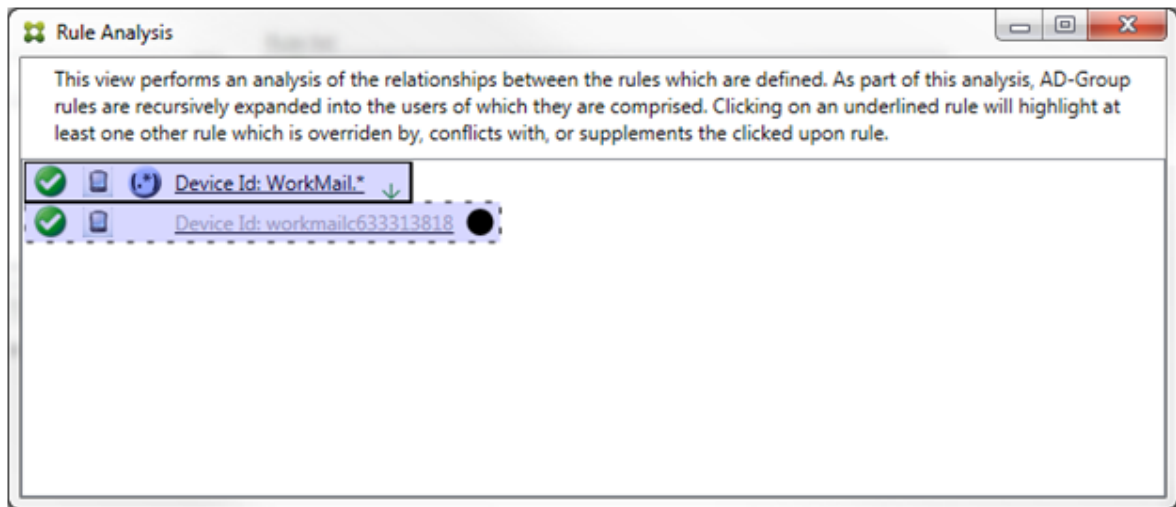
Rule Analysis(규칙 분석) 창에는 선택할 경우 충돌, 재정의, 중복 또는 보완 규칙만 표시되는 확인란이 있습니다.



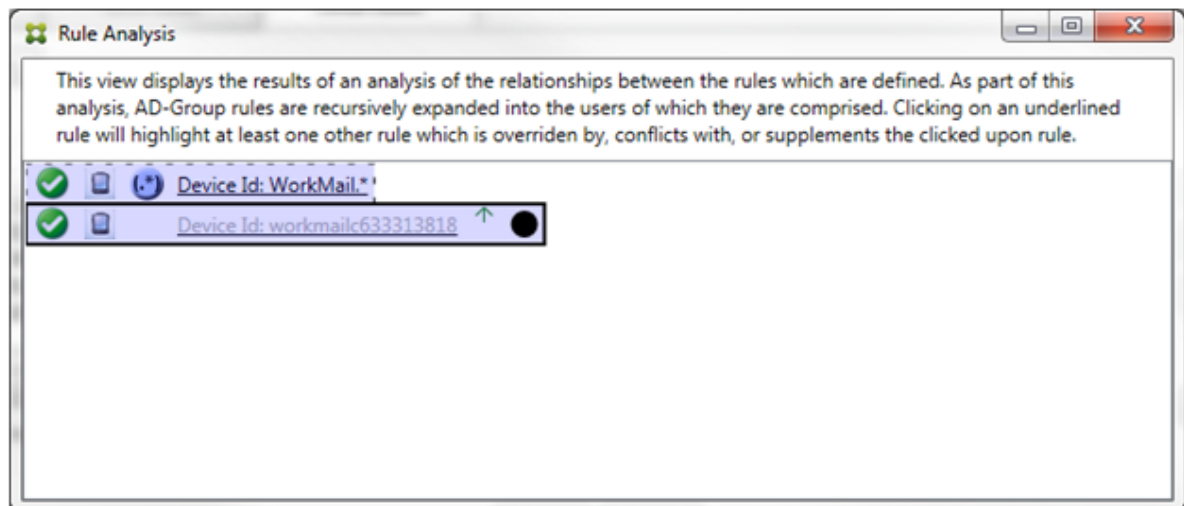
재정의가 발생하는 경우 2 개 이상의 규칙 (주 규칙과 보조 규칙) 에 밑줄이 표시됩니다. 우선 순위가 더 높은 규칙으로 재정의된 하나 이상의 보조 규칙은 연한 글꼴로 표시됩니다. 재정의된 규칙을 클릭하면 해당 규칙을 재정의한 규칙을 볼 수 있습니다. 규칙이 주 규칙이 되거나 보조 규칙이 되어 재정의된 규칙이 강조 표시되면 그 옆에 해당 규칙이 비활성 상태를 나타내는 검정색 원이 표시됩니다. 예를 들어 규칙을 클릭하기 전에 대화 상자는 다음과 같이 표시됩니다.



우선 순위가 가장 높은 규칙을 클릭하면 대화 상자가 다음과 같이 표시됩니다.

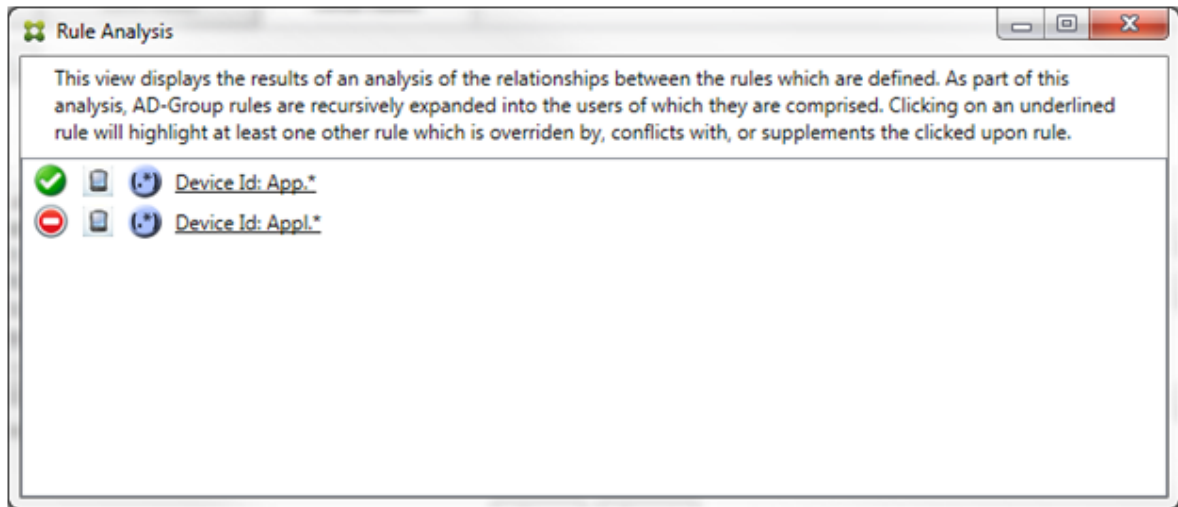


이 예에서 정규식 규칙 `WorkMail.*`는 주 규칙 (실선 테두리로 표시됨) 이고 일반 규칙 `workmailc633313818`은 보조 규칙 (파선 테두리로 표시됨) 입니다. 보조 규칙 옆의 검정색 점은 이 규칙보다 우선하는 더 높은 우선 순위의 정규식 규칙이 있어 해당 규칙이 비활성화 (따라서 평가되지 않음) 되었음을 나타내는 시각적 표시입니다. 재정의된 규칙을 클릭한 후 대화 상자는 다음과 같이 표시됩니다.

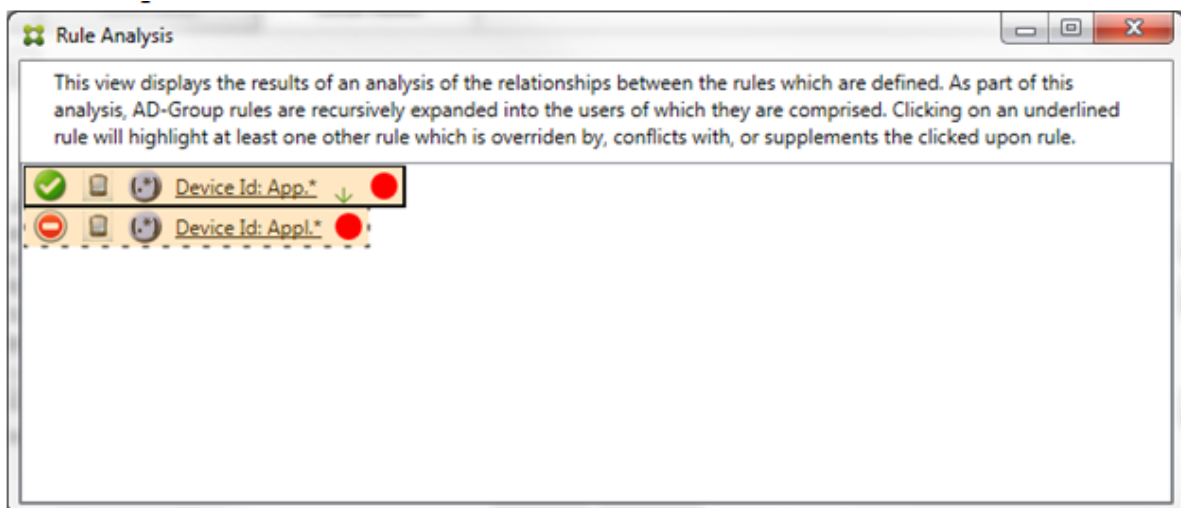


이전 예에서 정규식 규칙 `WorkMail.*`는 보조 규칙 (파선 테두리로 표시됨) 이고 일반 규칙 `workmailc633313818`은 주 규칙 (실선 테두리로 표시됨) 입니다. 이 단순 예제에서는 큰 차이가 없습니다. 더 복잡한 예제는 이 항목의 뒷부분에 나오는 복합식 예제를 참조하십시오. 여러 개의 규칙이 정의된 시나리오에서 재정의된 규칙을 클릭하면 해당 규칙을 재정의한 규칙을 빠르게 식별할 수 있습니다.

충돌이 발생하는 경우 2 개 이상의 규칙 (주 규칙과 보조 규칙) 에 밑줄이 표시됩니다. 충돌하는 규칙은 빨간색 점으로 표시됩니다. 서로 충돌하는 규칙은 둘 이상의 정규식이 정의된 경우에만 가능합니다. 다른 모든 충돌 시나리오에서는 충돌이 발생하지 않으며 재정의만 발생합니다. 단순 예제에서 규칙 중 하나를 클릭하기 전의 대화 상자는 다음과 같이 표시됩니다.

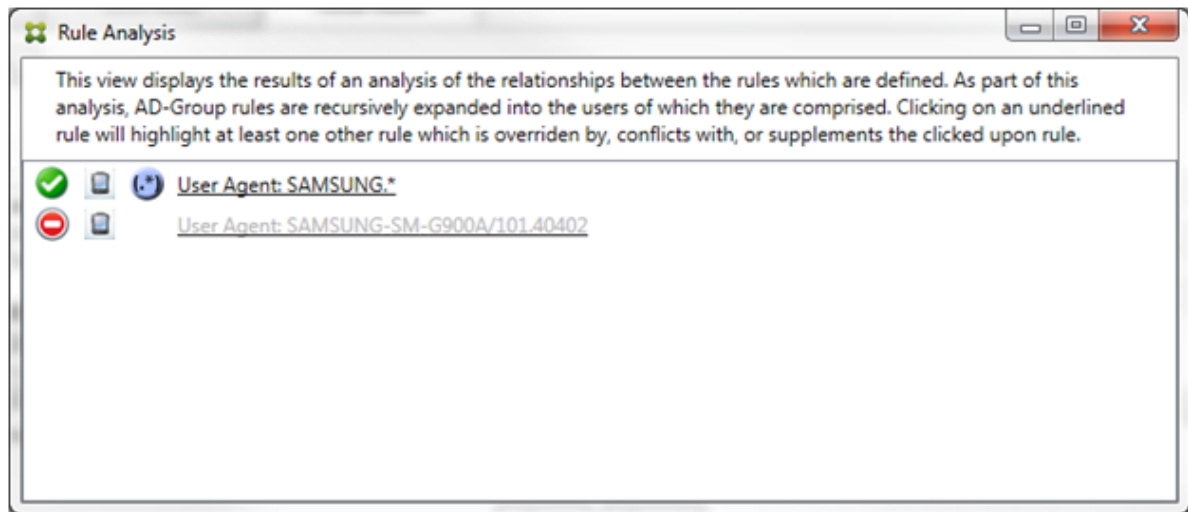


두 정규식 규칙을 검사하면 첫 번째 규칙은 장치 ID에 “App”이 포함된 모든 장치를 허용하고, 두 번째 규칙은 장치 ID에 “Appl”이 포함된 모든 장치를 거부하는 것을 알 수 있습니다. 또한 두 번째 규칙이 장치 ID에 “Appl”이 포함된 모든 장치를 거부하지만 허용 규칙의 우선 순위가 더 높기 때문에 두 번째 규칙의 조건과 일치하는 장치가 거부되지 않습니다. 첫 번째 규칙을 클릭한 후 대화 상자는 다음과 같이 표시됩니다.



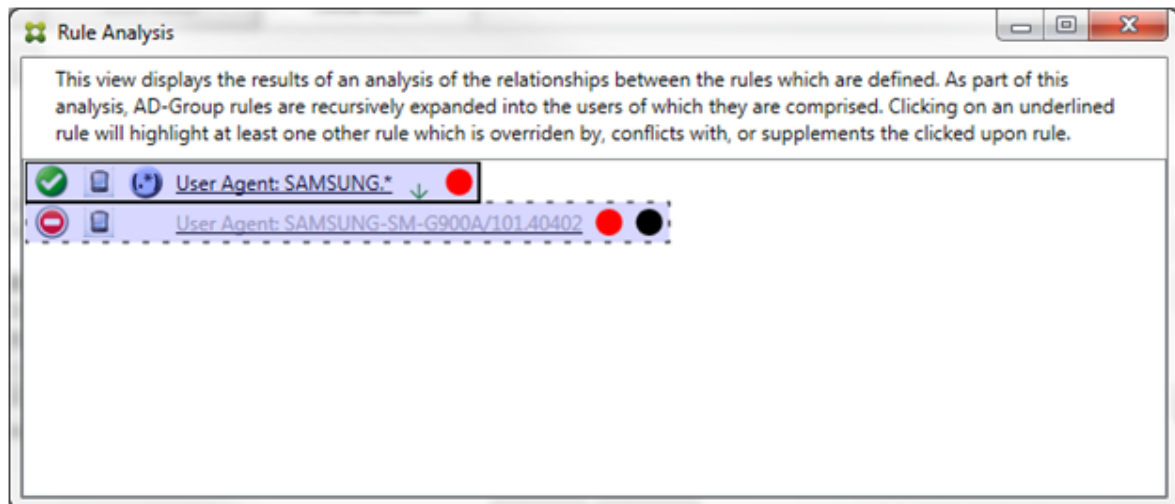
앞의 시나리오에서는 주 규칙 (정규식 규칙 `App.*`) 과 보조 규칙 (정규식 규칙 `Appl.*`) 이 모두 노란색으로 강조 표시됩니다. 이는 둘 이상의 정규식 규칙이 단일의 일치 가능한 필드에 적용되어 중복성 문제 또는 보다 심각한 문제가 발생할 수 있음을 알리는 시각적 경고입니다.

충돌과 재정의가 모두 발생하는 시나리오에서는 주 규칙 (정규식 규칙 `App.*`) 과 보조 규칙 (정규식 규칙 `Appl.*`) 이 노란색으로 강조 표시됩니다. 이는 둘 이상의 정규식 규칙이 단일의 일치 가능한 필드에 적용되어 중복성 문제 또는 보다 심각한 문제가 발생할 수 있음을 알리는 시각적 경고입니다.



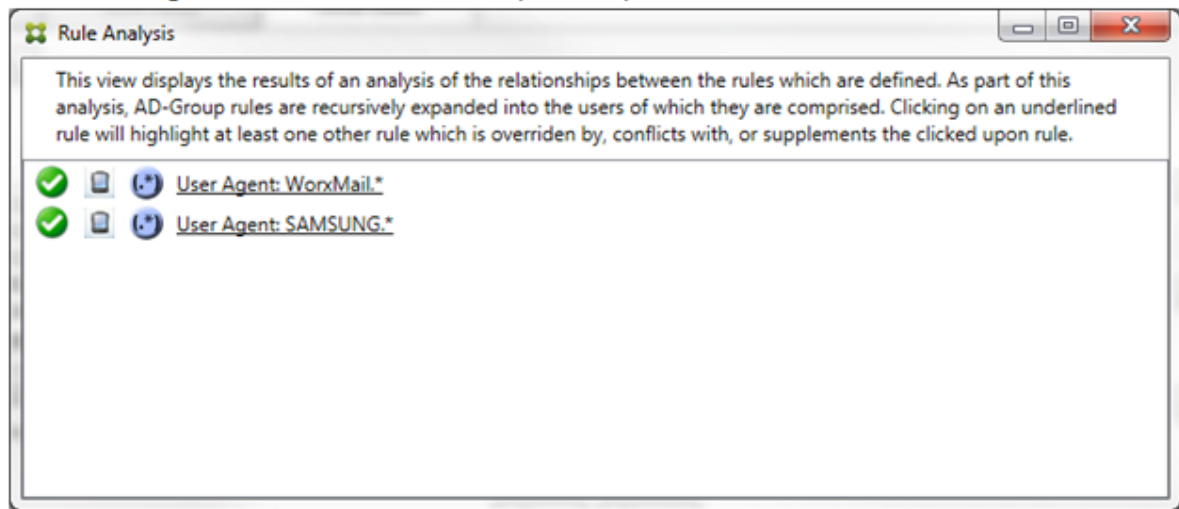
앞의 예제에서 첫 번째 규칙 (정규식 규칙 `SAMSUNG.*`) 은 다음 규칙 (일반 규칙 `SAMSUNG-SM-G900A/101.40402`) 을 재정의할 뿐 아니라 액세스 (주 규칙은 허용을 지정하고 보조 규칙은 차단을 지정함) 에서도 다르다는 것을 알 수 있습니다. 두 번째 규칙 (일반 규칙 `SAMSUNG-SM-G900A/101.40402`) 은 재정의되고 비활성화되었음을 나타내는 색이 연한 텍스트로 표시됩니다.

정규식 규칙을 클릭한 후 대화 상자는 다음과 같이 표시됩니다.

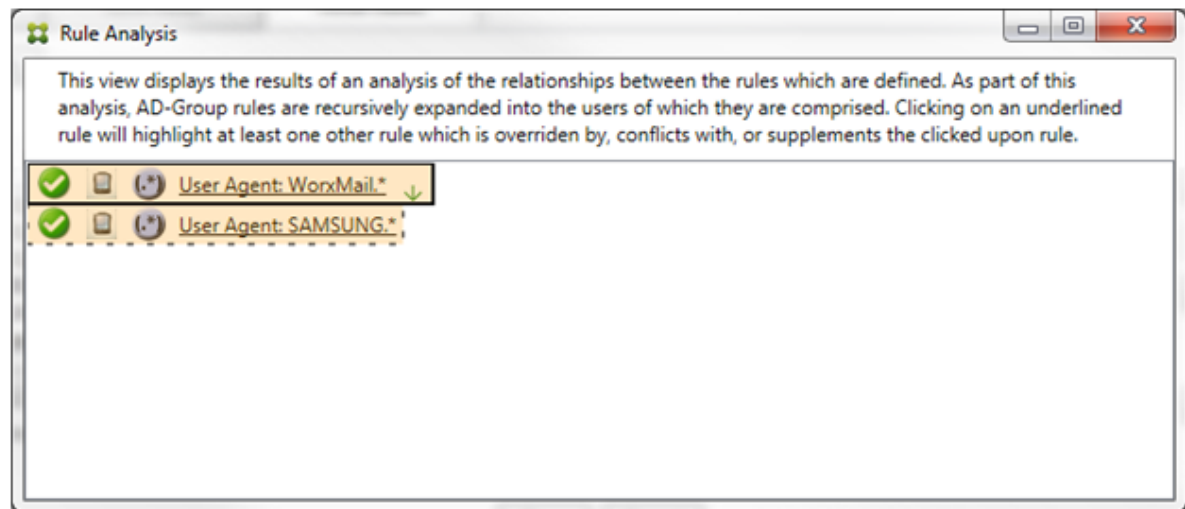


주 규칙 (정규식 규칙 `SAMSUNG.*`) 뒤에 액세스 상태가 하나 이상의 보조 규칙과 충돌함을 나타내는 빨간색 점이 표시됩니다. 보조 규칙 (일반 규칙 `SAMSUNG-SM-G900A/101.40402`) 뒤에 액세스 상태가 주 규칙과 충돌함을 나타내는 빨간색 점이 표시됩니다. 이 규칙 뒤에는 규칙이 재정의되었고 그로 인해 비활성화되었음을 나타내는 검정색 점도 표시됩니다.

2 개 이상의 규칙 (주 규칙과 보조 규칙) 에 밑줄이 표시됩니다. 다른 규칙을 보완하는 규칙에는 정규식 규칙만 포함됩니다. 다른 규칙을 보완하는 규칙은 노란색 오버레이로 표시됩니다. 단순 예제에서 규칙 중 하나를 클릭하기 전의 대화 상자는 다음과 같이 표시됩니다.



Exchange ActiveSync 용 Endpoint Management 커넥터의 ActiveSync 장치 ID 필드에 정규식 규칙인 두 규칙이 모두 적용된 것을 쉽게 알 수 있습니다. 첫 번째 규칙을 클릭한 후 대화 상자는 다음과 같이 표시됩니다.



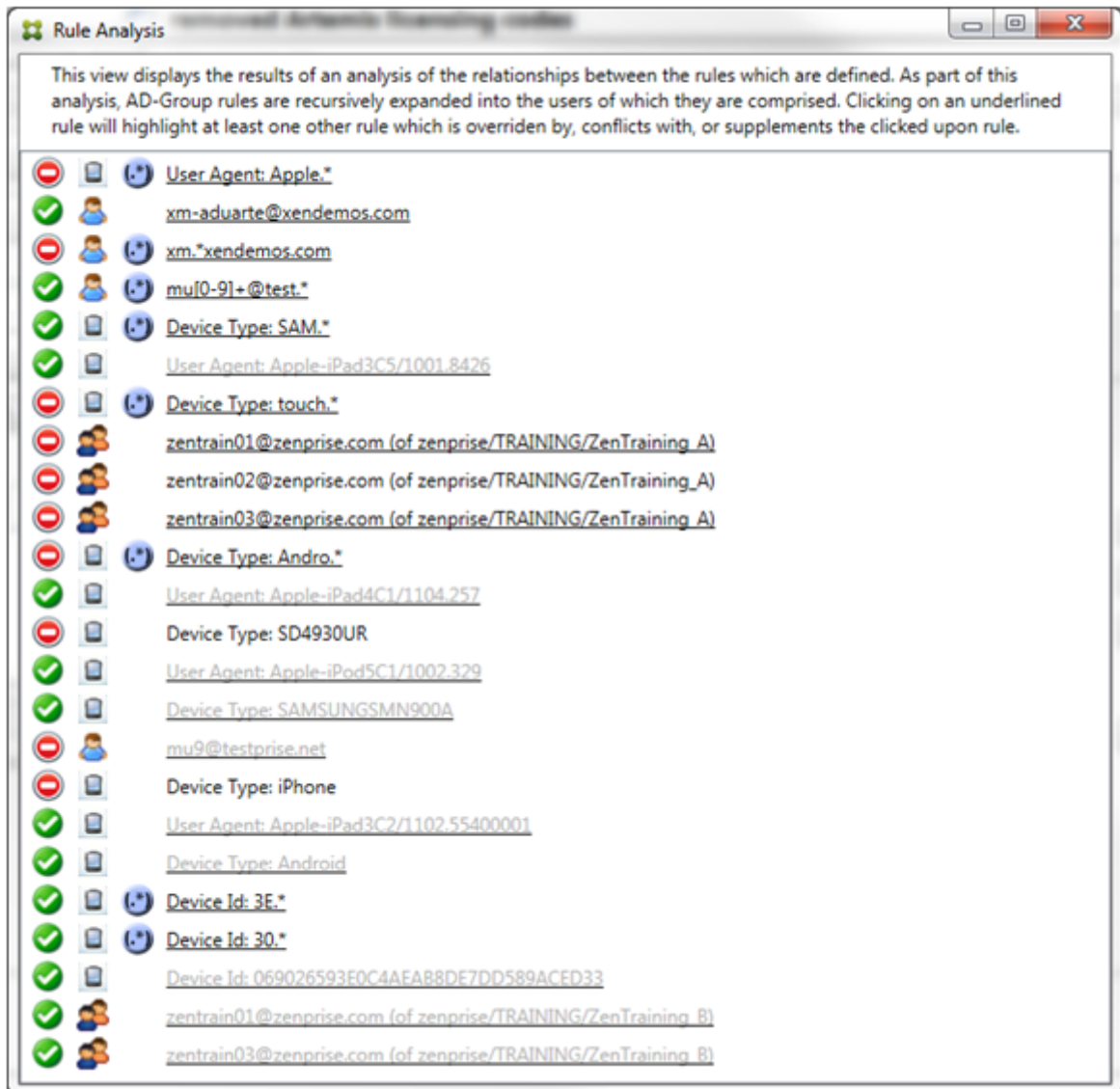
주 규칙 (정규식 규칙 **WorkMail.***) 이 하나 이상의 추가 보조 규칙 (정규식 규칙) 이 있음을 나타내는 노란색 오버레이로 강조 표시됩니다. 보조 규칙 (정규식 규칙 **SAMSUNG.***) 이 Exchange ActiveSync 용 Endpoint Management 커넥터의 동일한 필드 (ActiveSync 장치 ID 필드) 에 이 규칙과 주 규칙 (모두 정규식 규칙임) 이 적용되고 있음을 나타내는 노란색 오버레이로 강조 표시됩니다. 이 경우 필드는 ActiveSync 장치 ID 입니다. 정규식은 겹치거나 겹치지 않을 수 있습니다. 정규식이 적절하게 작성되었는지 여부는 직접 판단해야 합니다.

복합식의 예제

재정의, 충돌 또는 보완이 발생할 수 있는 상황은 많습니다. 따라서 가능한 모든 시나리오의 예를 제공하기란 불가능합니다. 다음 예제에서는 하지 말아야 할 사항을 설명하고 규칙 분석의 시각적 구조가 제공하는 모든 기능을 설명합니다. 다음 그림에는 항목의 대부분에 밑줄이 표시되어 있습니다. 문제의 규칙이 우선 순위가 더 높은 규칙으로 재정의되었음을 나타내는 연한 글꼴로 렌더링



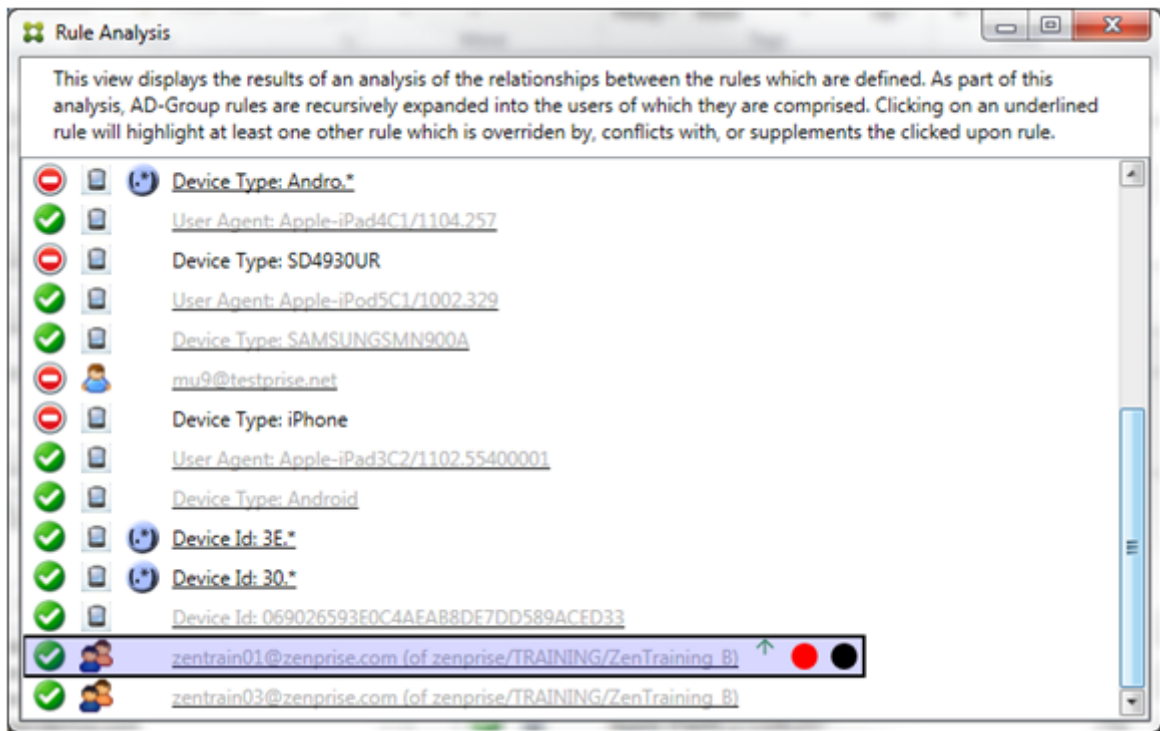
된 항목이 많습니다. 아이콘으로 표시되는 정규식 규칙의 수도 목록에 포함되어 있습니다.



재정의의 분석하는 방법

특정 규칙을 재정의한 규칙을 보려면 규칙을 클릭합니다.

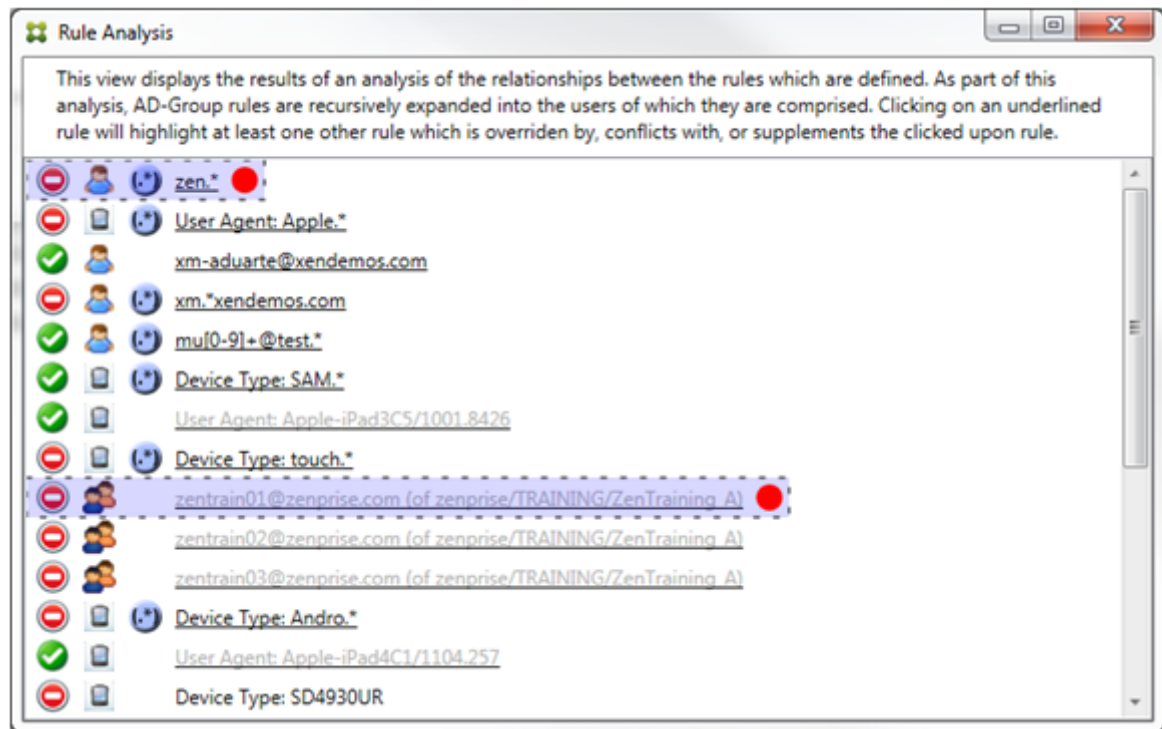
예제 1: 이 예제에서는 zentrain01@zenprise.com이 재정의된 이유를 검사합니다.



주 규칙 (AD 그룹 규칙 `zenprise/TRAINING/ZenTraining B`, 여기서 `zentrain01@zenprise.com`은 구성원임)의 특징은 다음과 같습니다.

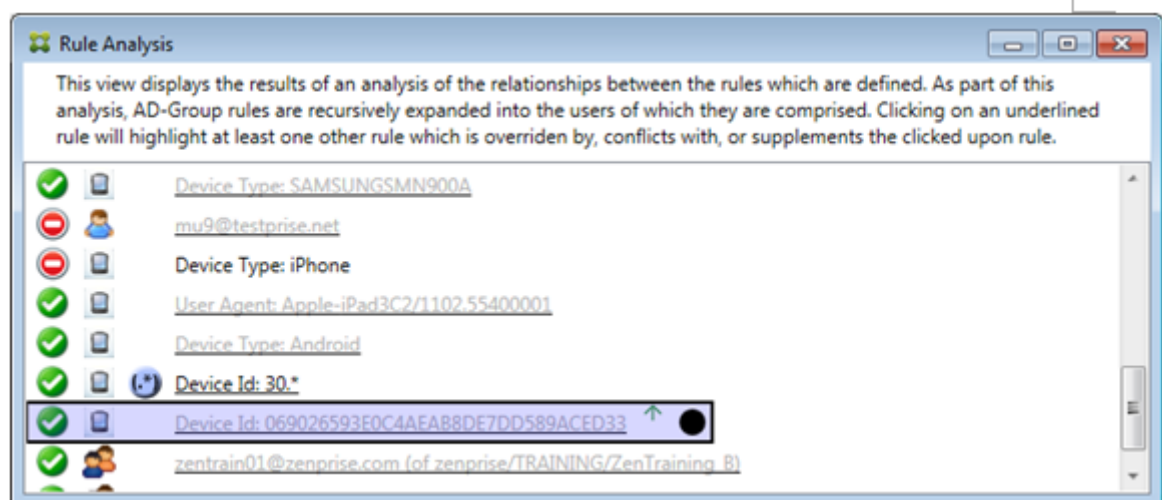
- 파란색으로 강조 표시되고 실선 테두리가 포함되어 있습니다.
- 위쪽을 가리키는 녹색 화살표가 있습니다 (위에 보조 규칙이 있음을 나타냄).
- 각각 하나 이상의 보조 규칙과 액세스 상태가 충돌하고, 주 규칙으로 재정의되어 비활성화되었음을 나타내는 빨간색 원과 검정색 원이 뒤에 있습니다.

위로 스크롤하면 다음이 표시됩니다.



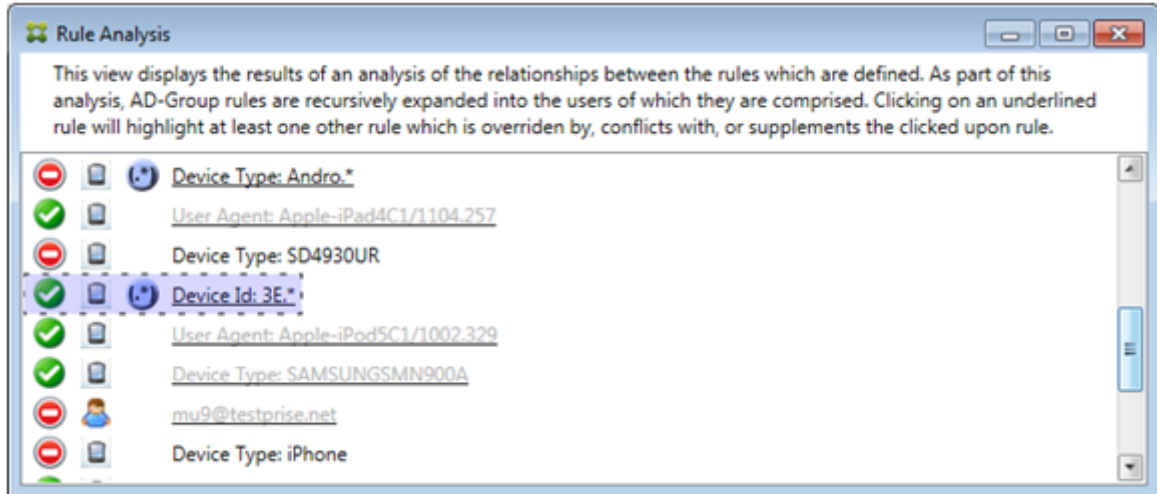
이 예에서는 정규식 규칙인 `zen.*`과 일반 규칙인 `zentrain01@zenprise.com(zenprise/TRAINING/ZenTraining A)`의 보조 규칙 2 개가 주 규칙을 재정의합니다. 두 번째 보조 규칙에서는 Active Directory 그룹 규칙 `ZenTraining A`에 사용자 `zentrain01@zenprise.com`이 포함되고 Active Directory 그룹 규칙 `ZenTraining B`에도 사용자 `zentrain01@zenprise.com`이 포함됩니다. 그러나 보조 규칙이 주 규칙보다 우선 순위가 높기 때문에 주 규칙이 재정의되었습니다. 주 규칙의 액세스는 허용이고 두 보조 규칙의 액세스는 차단이므로 액세스가 충돌함을 나타내는 빨간색 원이 뒤에 표시됩니다.

예제 2: 이 예제에서는 ActiveSync 장치 ID 가 `069026593E0C4AEAB8DE7DD589ACED33`인 장치가 재정의된 이유를 보여 줍니다.



주 규칙 (일반 장치 ID 규칙 `069026593E0C4AEAB8DE7DD589ACED33`)의 특징은 다음과 같습니다.

- 파란색으로 강조 표시되고 실선 테두리가 포함되어 있습니다.
- 위쪽을 가리키는 녹색 화살표가 있습니다 (위에 보조 규칙이 있음을 나타냄).
- 주 규칙이 보조 규칙으로 재정의되어 비활성화되었음을 나타내는 검정색 원이 뒤에 표시되어 있습니다.

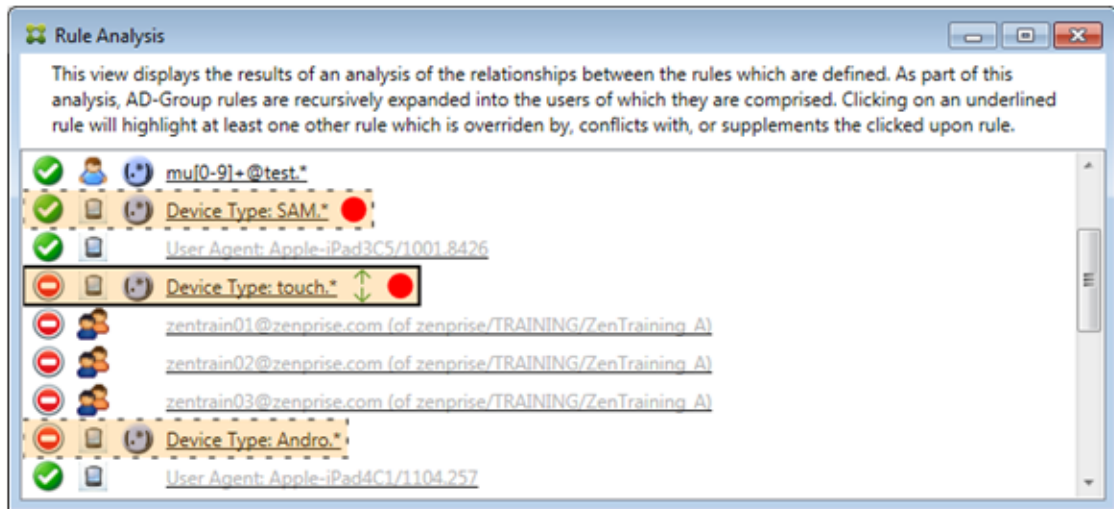


이 예에서는 단일의 보조 규칙이 주 규칙을 재정의합니다. 정규식 ActiveSync 장치 ID 규칙은 3E.*입니다. 정규식 3E.*가 069026593E0C4AEAB8DE7DD589ACED33과 일치하므로 주 규칙이 평가되지 않습니다.

보안 및 충돌을 분석하는 방법

이 예에서 기본 규칙은 정규식 ActiveSync 장치 유형 규칙인 touch.*입니다. 특징은 다음과 같습니다.

- 특정 규칙 필드 (이 예에서는 ActiveSync 장치 유형)에 둘 이상의 정규식 규칙이 작동함을 나타내는 경고로 노란색 오버레이가 실선 테두리와 함께 표시되어 있습니다.
- 각각 위쪽과 아래쪽을 가리키는 두 개의 화살표가 있습니다 (우선 순위가 높은 보조 규칙과 우선 순위가 낮은 보조 규칙이 1 개 이상 있음을 나타냄).
- 액세스 상태가 허용으로 설정되어 주 규칙의 액세스 상태인 차단과 충돌하는 보조 규칙이 1 개 이상임을 나타내는 빨간색 원이 옆에 표시되어 있습니다.
- 정규식 ActiveSync 장치 유형 규칙 SAM.* 및 정규식 ActiveSync 장치 유형 규칙 Andro.*의 보조 규칙 2 개가 있습니다.
- 두 보조 규칙은 보조 규칙임을 나타내는 파선 테두리로 표시되어 있습니다.
- 두 보조 규칙에는 ActiveSync 장치 유형 규칙 필드에도 적용됨을 나타내는 노란색 오버레이가 표시되어 있습니다.
- 이러한 시나리오에서는 정규식 규칙이 중복되지 않는지 확인해야 합니다.



규칙을 추가로 분석하는 방법

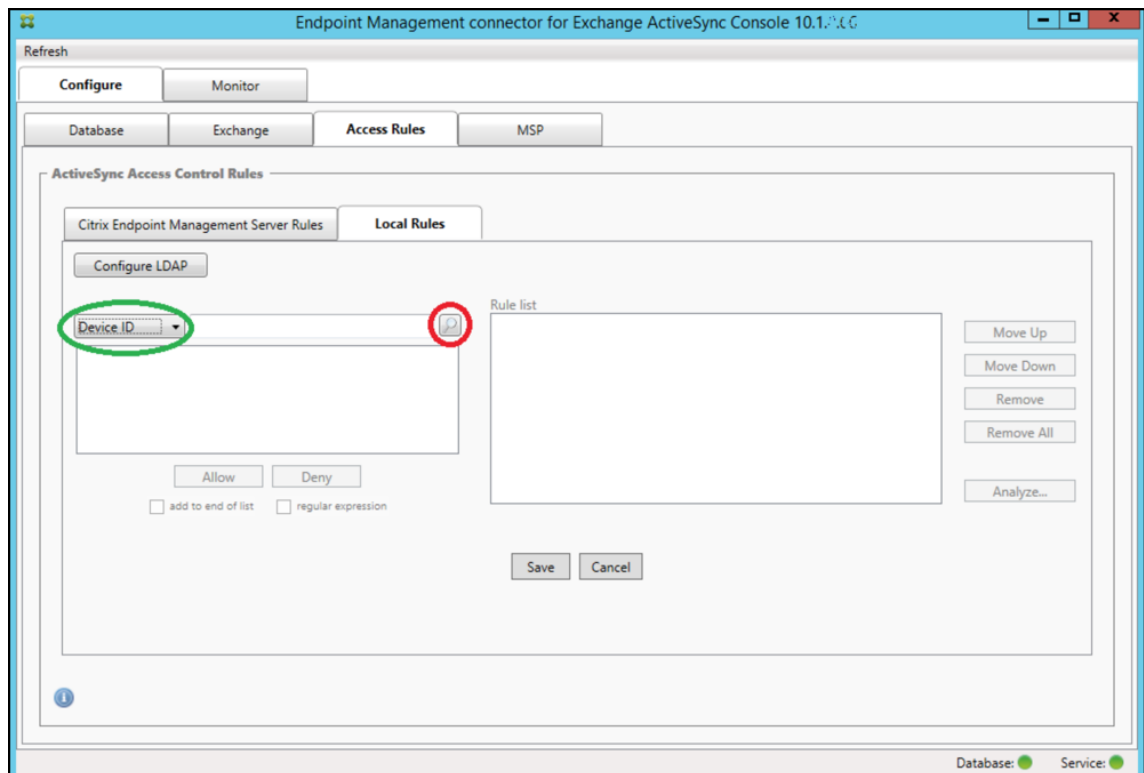
이 예제에서는 규칙 관계가 항상 주 규칙의 관점에서 파생된다는 점을 설명합니다. 앞의 예제에서는 정규식 규칙 클릭이 값이 `touch.*`인 장치 유형의 필드에 적용되는 방법을 보여줬습니다. 보조 규칙 `Andro.*`를 클릭하면 다른 보조 규칙 집합이 강조 표시됩니다.



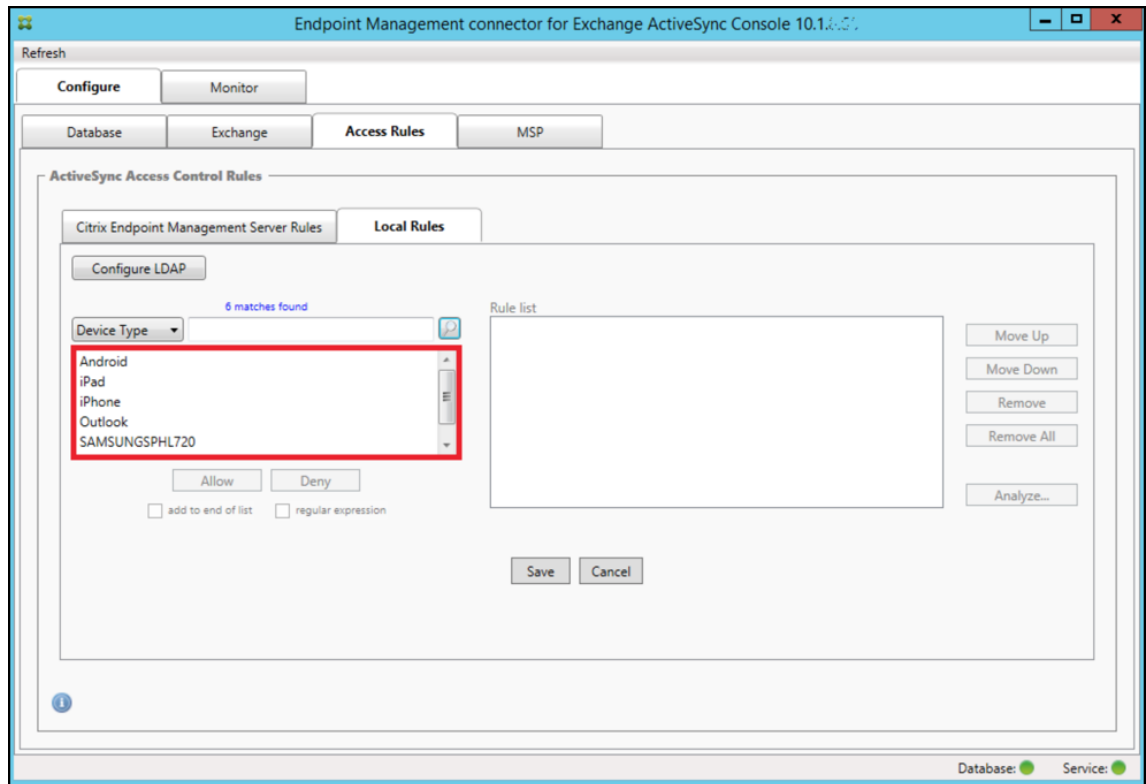
이 예제는 규칙 관계에 포함된 재정의된 규칙을 보여 줍니다. 이 규칙은 일반 ActiveSync 장치 유형 규칙인 **Android**이며 재정의 (연한 글꼴로 표시되고 검정색 원이 표시됨) 되었으며 주 규칙인 정규식 ActiveSync 장치 유형 규칙 **Andro.***와 액세스 상태가 충돌합니다. 이 규칙은 클릭하기 전에 보조 규칙이었습니다. 앞의 예에서 일반 ActiveSync 장치 유형 규칙 **Android**는 보조 규칙으로 표시되지 않았습니다. 주 규칙 (정규식 ActiveSync 장치 유형 규칙 **touch.***) 의 관점에서 주 규칙과 관련되지 않았기 때문입니다.

일반식 로컬 규칙을 구성하려면

1. **Access Rules**(액세스 규칙) 탭을 클릭합니다.



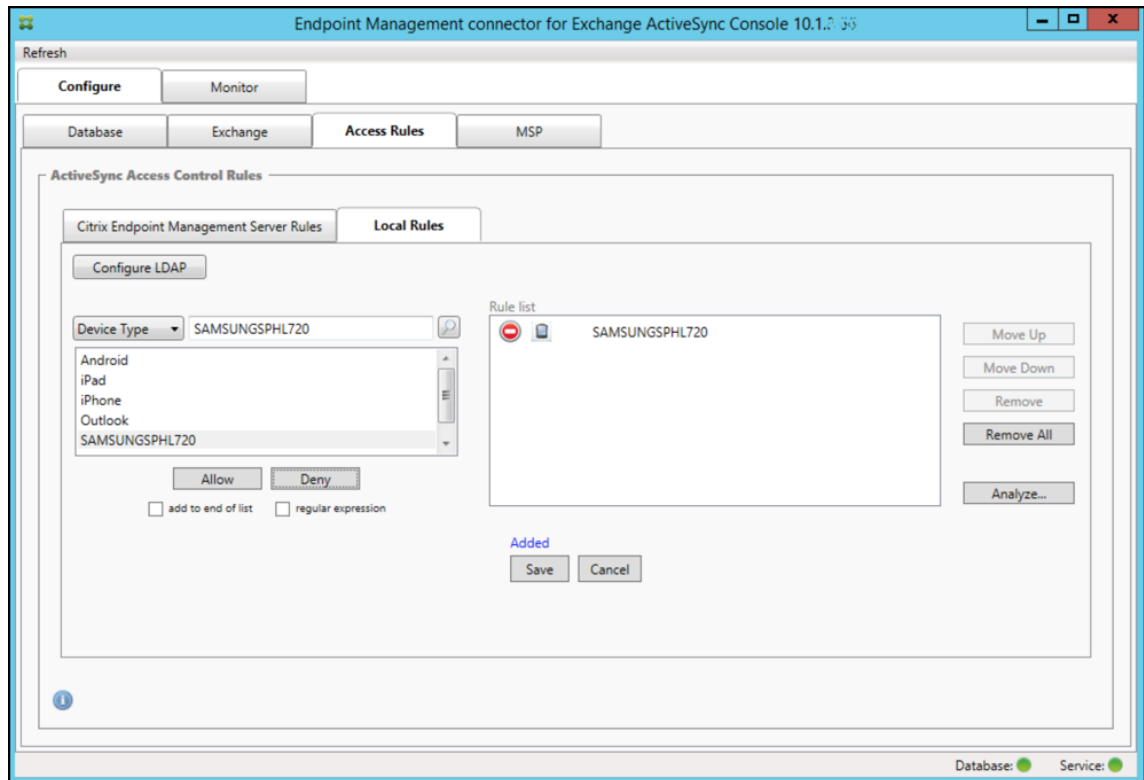
2. **Device ID**(장치 ID) 목록에서 로컬 규칙을 만들 필드를 선택합니다.
3. 돋보기 아이콘을 클릭하여 선택한 필드의 모든 고유한 일치 항목을 표시합니다. 이 예제에서는 **Device Type**(장치 유형) 필드가 선택되었고 목록 상자 아래에 선택 항목이 표시되어 있습니다.



4. 결과 목록 상자에서 항목 하나를 클릭하고 다음 옵션 중 하나를 클릭합니다.

- **Allow(허용)** 을 클릭하면 일치하는 모든 장치의 ActiveSync 트래픽을 허용하도록 Exchange 가 구성됩니다.
- **Deny(거부)** 을 클릭하면 일치하는 모든 장치의 ActiveSync 트래픽을 거부하도록 Exchange 가 구성됩니다.

이 예에서는 장치 유형이 SamsungSPhl720 인 모든 장치의 액세스가 거부됩니다.



정규식을 추가하려면

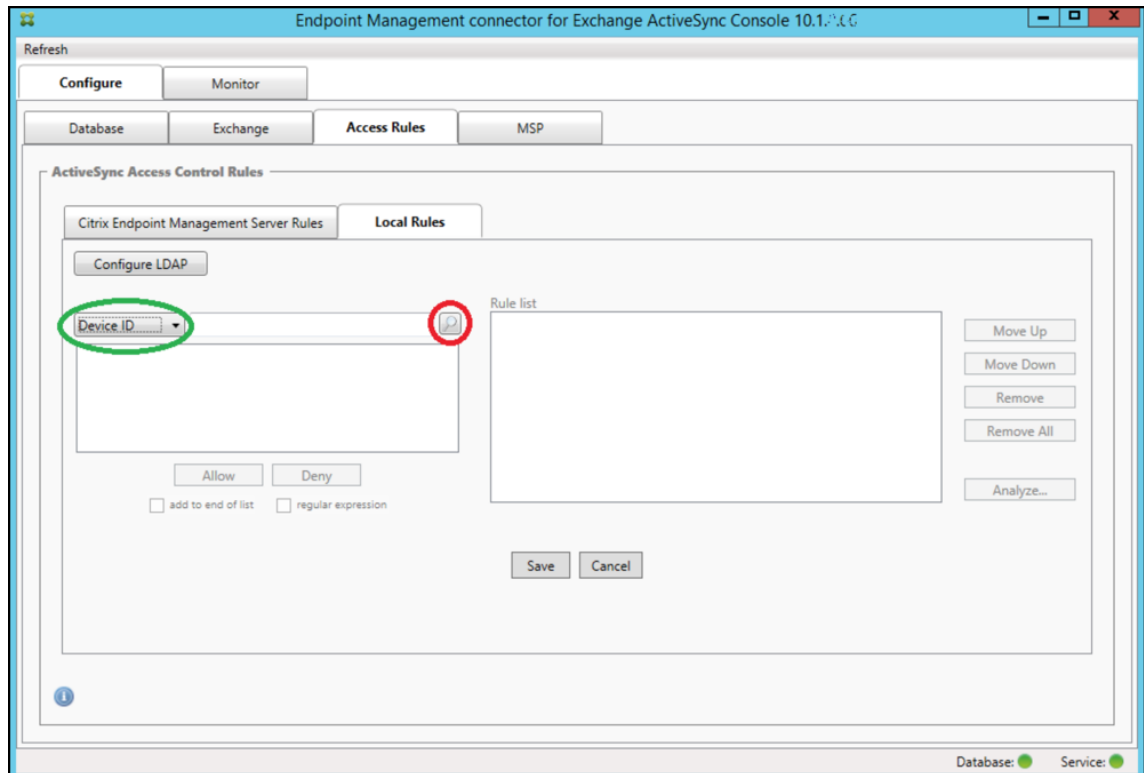


정규식 로컬 규칙은 옆에 표시되는 아이콘으로 구분할 수 있습니다.

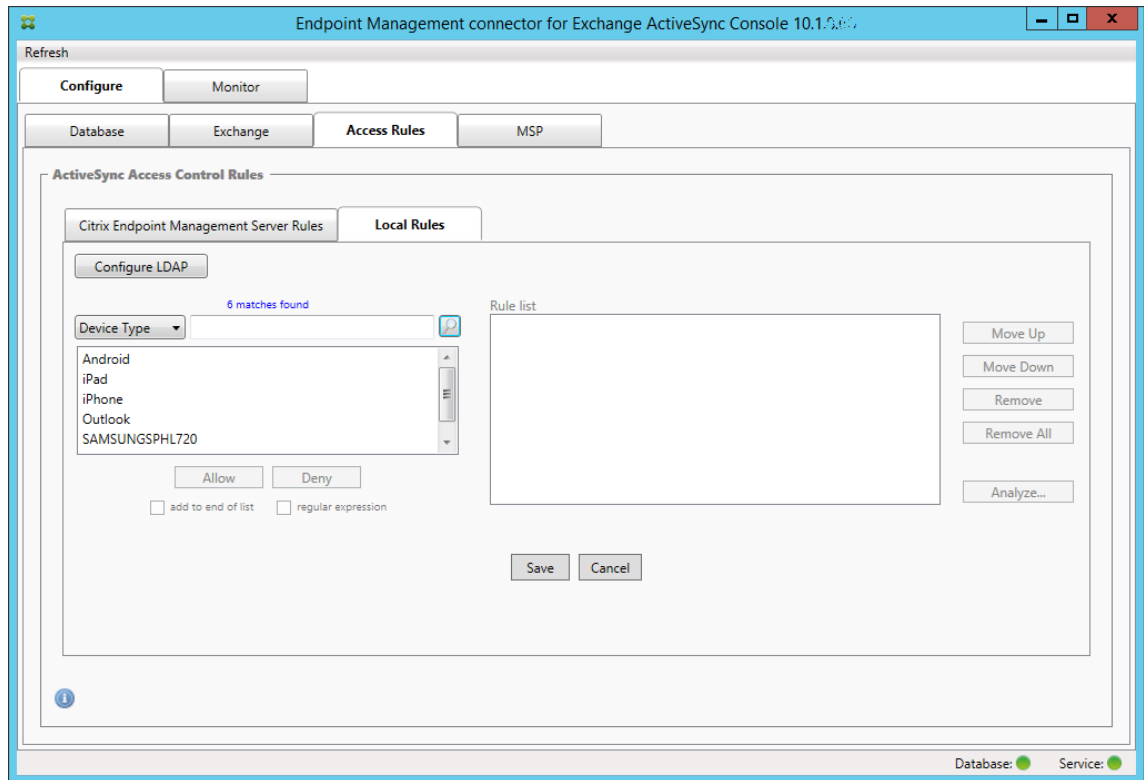
정규식 규칙을 추가하려면 지정된 필드에 대한 결과 목록의 기존 값을 사용하여 정규식 규칙을 작성하거나 (주 스냅샷이 완료되어야 함) 원하는 정규식을 입력하면 됩니다.

기존 필드 값에서 정규식을 작성하려면

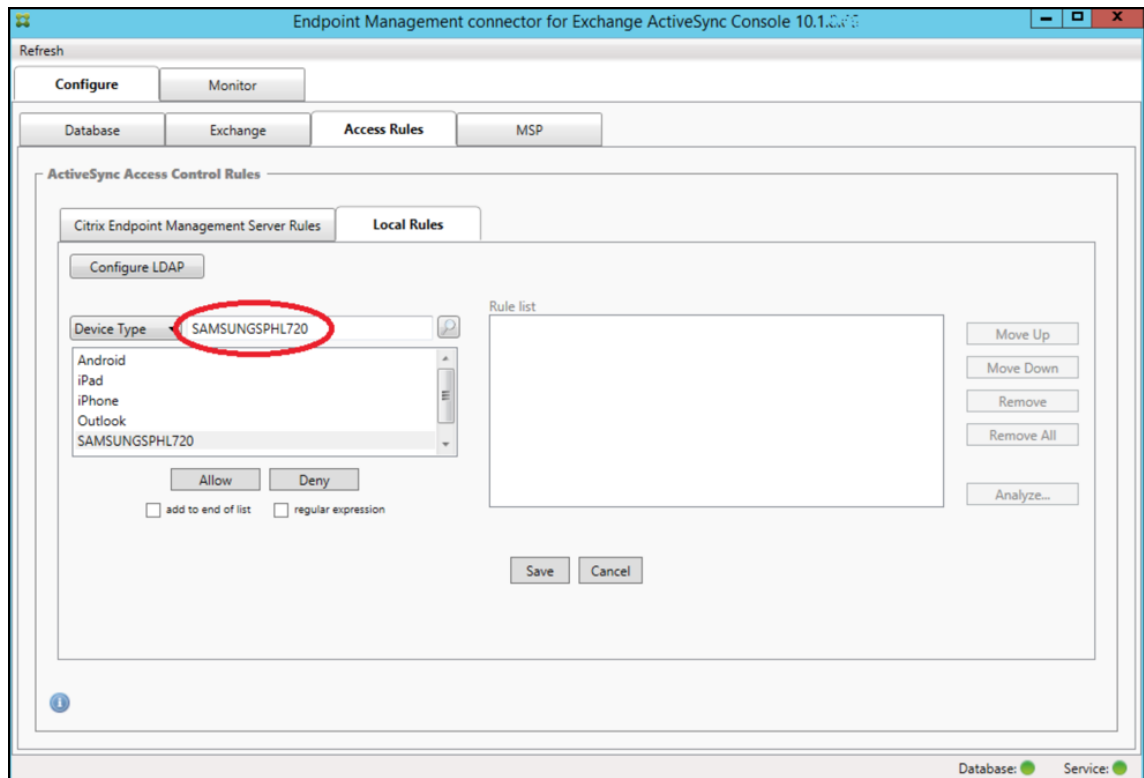
1. **Access Rules**(엑세스 규칙) 탭을 클릭합니다.



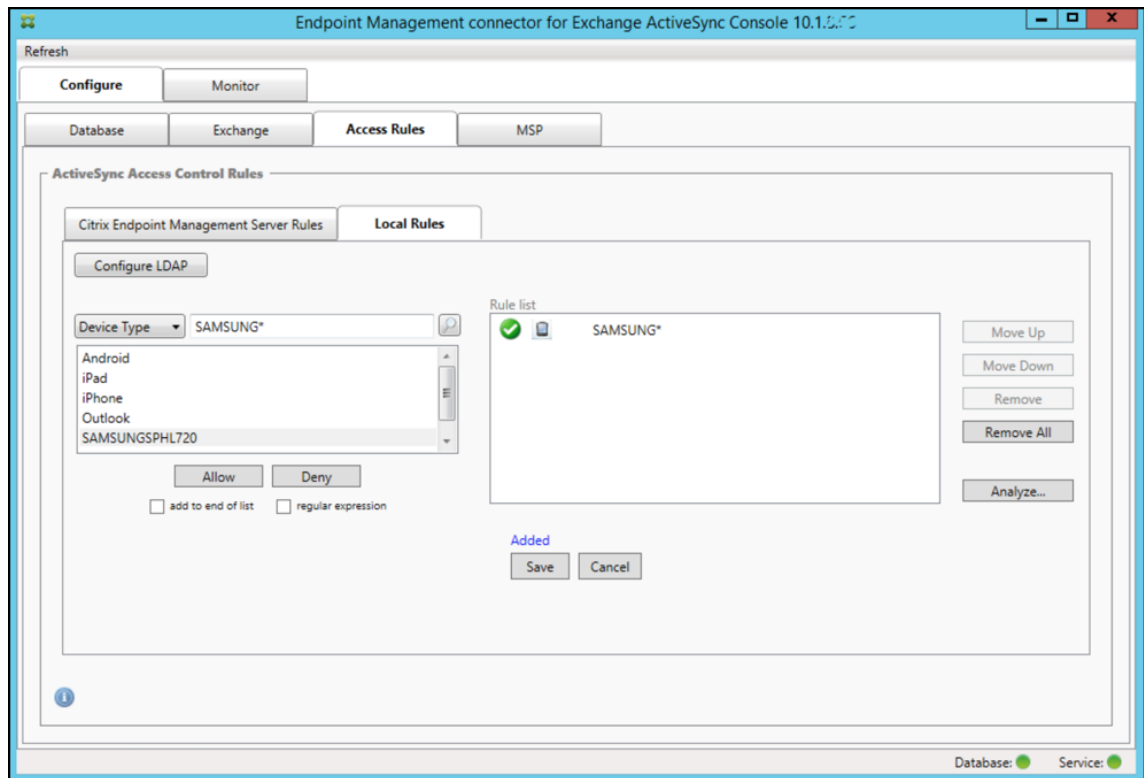
2. **Device ID(장치 ID)** 목록에서 정규식 로컬 규칙을 만들 필드를 선택합니다.
3. 돋보기 아이콘을 클릭하여 선택한 필드의 모든 고유한 일치 항목을 표시합니다. 이 예제에서는 **Device Type(장치 유형)** 필드가 선택되었고 목록 상자 아래에 선택 항목이 표시되어 있습니다.



4. 결과 목록에서 항목 중 하나를 클릭합니다. 이 예제에서는 **SAMSUNGSPHL720** 이 선택되었고 **Device Type**(장치 유형) 옆의 텍스트 상자에 표시되어 있습니다.

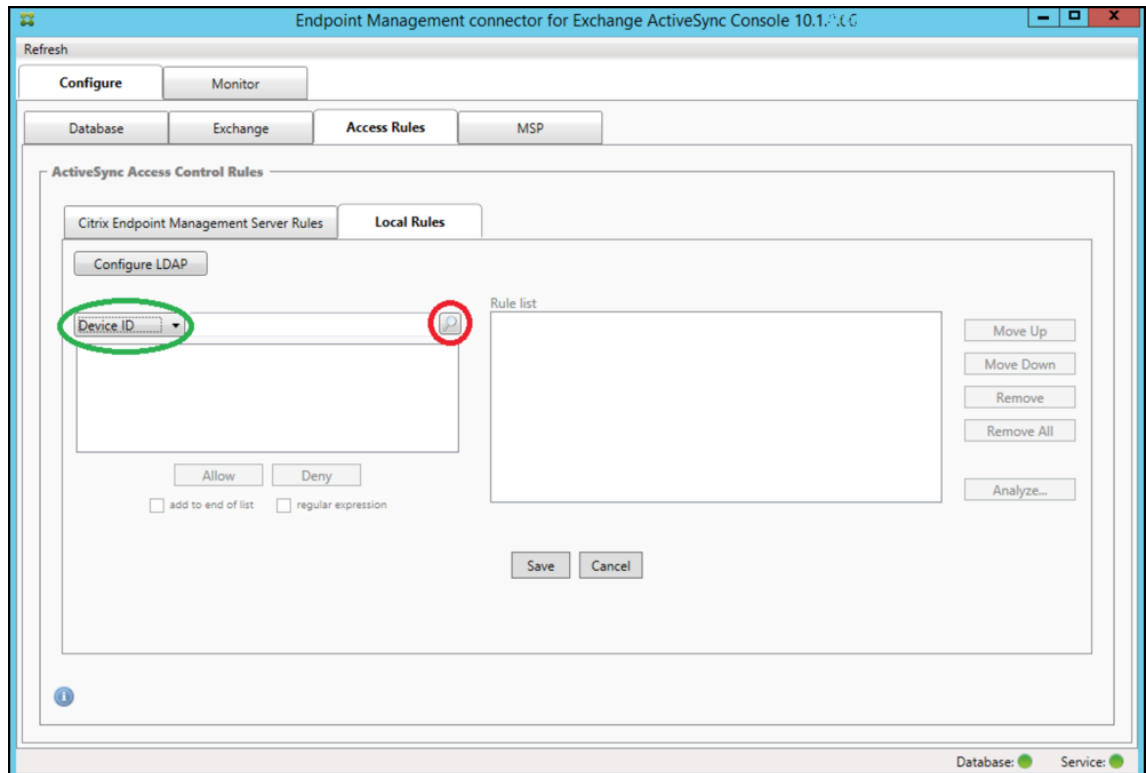


5. 장치 유형 값에 “Samsung” 이 포함되는 모든 장치 유형을 허용하려면 다음 단계에 따라 정규식 규칙을 추가합니다.
 - a) 선택한 항목 텍스트 상자 안쪽을 클릭합니다.
 - b) 텍스트를 **SAMSUNGSPHL720** 에서 다음으로 변경합니다. **SAMSUNG.***.
 - c) regular expression(정규식) 확인란이 선택되어 있는지 확인합니다.
 - d) **Allow**(허용) 를 클릭합니다.

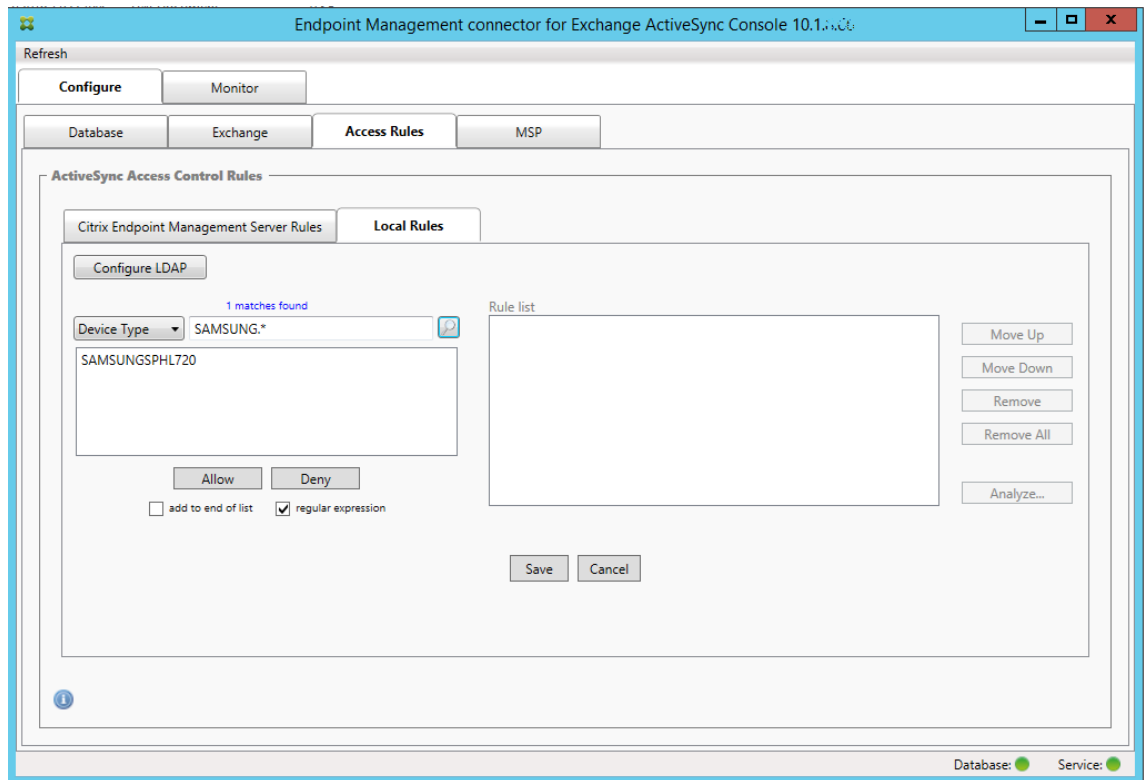


액세스 규칙을 작성하려면

1. **Local Rules**(로컬 규칙) 탭을 클릭합니다.
2. 정규식을 입력하려면 Device ID(장치 ID) 목록과 선택한 항목 텍스트 상자를 모두 사용해야 합니다.



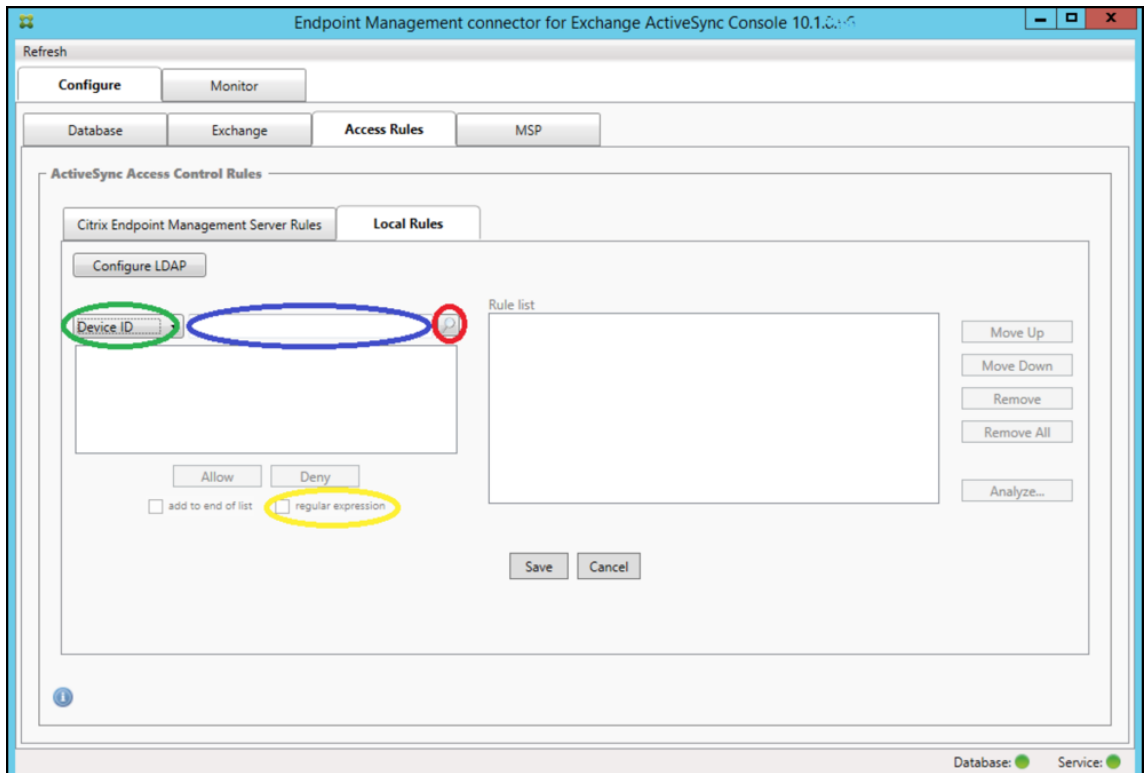
3. 일치 기준으로 사용할 필드를 선택합니다. 이 예제에서는 Device Type(장치 유형) 을 사용합니다.
4. 정규식을 입력합니다. 이 예에서는 다음을 사용합니다. `samsung.*`
5. regular expression(정규식) 확인란이 선택되었는지 확인한 후 **Allow**(허용) 또는 **Deny**(거부) 를 클릭합니다. 이 예에서는 **Allow**(허용) 를 선택합니다. 최종 결과는 다음과 같습니다.



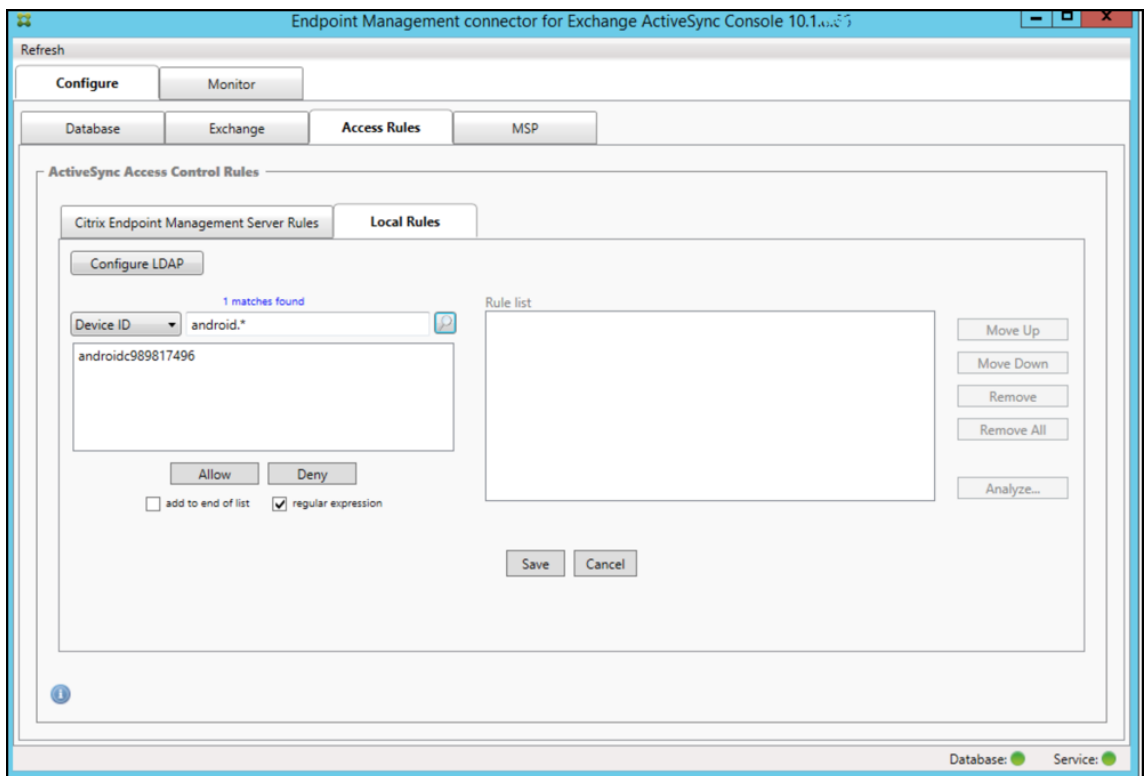
장치를 찾으려면

정규식 확인란을 선택하면 지정된 식과 일치하는 특정 장치에 대한 검색을 실행할 수 있습니다. 이 기능은 주 스냅샷을 성공적으로 완료한 경우에만 사용할 수 있습니다. 정규식 규칙을 사용할 계획이 없는 경우에도 이 기능을 사용할 수 있습니다. 예를 들어 ActiveSync 장치 ID에 “workmail” 텍스트가 포함된 모든 장치를 찾을 수 있습니다. 이렇게 하려면 다음 절차를 따르십시오.

1. **Access Rules(액세스 규칙)** 탭을 클릭합니다.
2. 장치 일치 필드 선택기가 Device ID(장치 ID)(기본값)로 설정되었는지 확인합니다.



3. 선택한 항목 텍스트 상자 (이전 그림에서 파란색으로 표시됨) 안쪽을 클릭한 후 **workmail.***를 입력합니다.
4. **regular expression**(정규식) 확인란이 선택되었는지 확인한 후 돋보기 아이콘을 클릭하여 다음 그림에 표시된 것과 같이 일치하는 항목을 표시합니다.

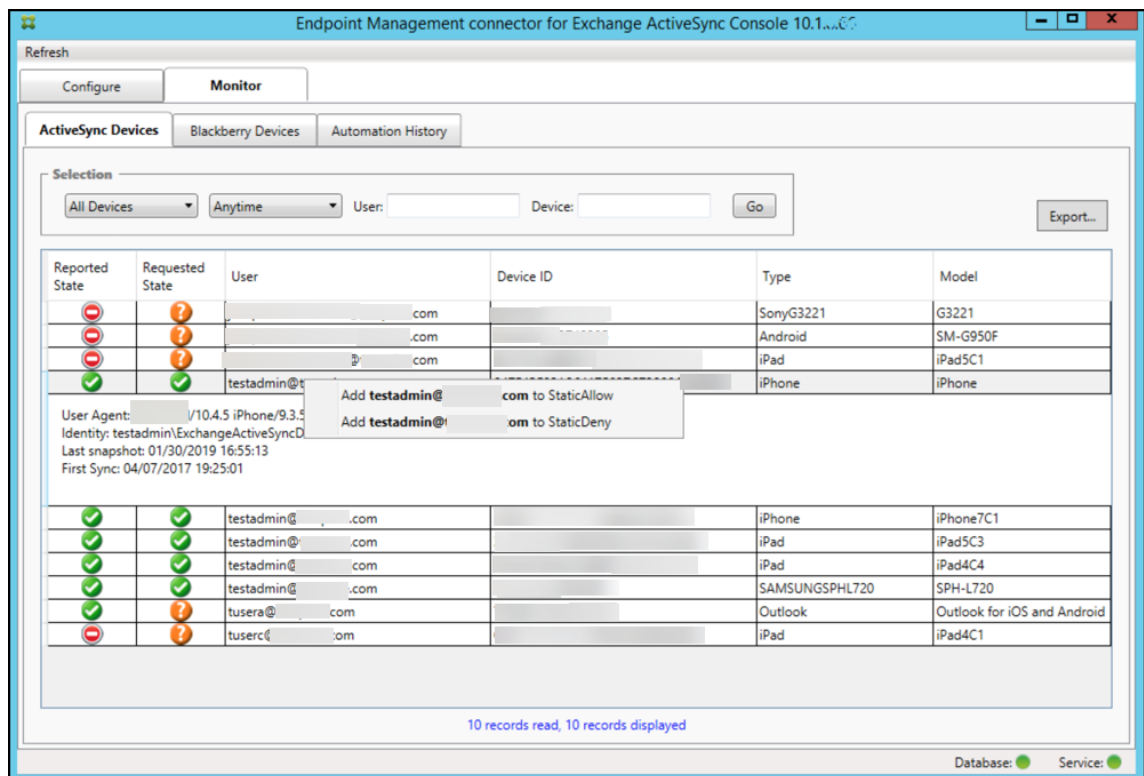


개별 사용자, 장치 또는 장치 유형을 정적 규칙에 추가하려면

ActiveSync Devices(ActiveSync 장치) 탭에서 사용자, 장치 ID 또는 장치 유형에 기반한 정책 규칙을 추가할 수 있습니다.

1. **ActiveSync Devices(ActiveSync 장치)** 탭을 클릭합니다.
2. 목록에서 사용자, 장치 또는 장치 유형을 마우스 오른쪽 단추로 클릭하고 선택 항목을 허용 또는 거부할지 여부를 선택합니다.

다음 이미지는 user1 을 선택한 경우의 Allow/Deny(허용/거부) 옵션을 보여 줍니다.



장치 모니터링

Exchange ActiveSync 용 Endpoint Management 커넥터의 **Monitor(모니터)** 탭을 사용하면 검색된 Exchange ActiveSync 및 BlackBerry 장치와 자동화된 PowerShell 명령의 실행 기록을 탐색할 수 있습니다. **Monitor(모니터)** 탭에는 다음과 같은 세 개의 탭이 있습니다.

- **ActiveSync Devices(ActiveSync 장치):**

- **Export(내보내기)** 단추를 클릭하여 표시된 ActiveSync 장치 파트너 관계를 내보낼 수 있습니다.
- **User(사용자), Device ID(장치 ID)** 또는 **Type(유형)** 열을 마우스 오른쪽 단추로 클릭하고 적절한 허용 또는 차단 규칙 유형을 선택하여 로컬 (정적) 규칙을 추가할 수 있습니다.
- 확장된 행을 축소하려면 Ctrl 키를 누른 채로 확장된 행을 클릭합니다.

- **Blackberry Devices(Blackberry 장치)**
- **Automation History(자동화 기록)**

Configure(구성) 탭에는 모든 스냅샷 기록이 표시됩니다. 스냅샷 기록은 스냅샷 생성 시점, 스냅샷 지속 기간, 검색된 장치 수 및 발생한 모든 오류를 보여 줍니다.

- **Exchange** 탭에서 원하는 Exchange Server 의 정보 아이콘을 클릭합니다.
- **MSP** 탭에서 원하는 BlackBerry Server 의 정보 아이콘을 클릭합니다.

문제 해결 및 진단

Exchange ActiveSync 용 Endpoint Management 커넥터는 오류 및 기타 작업 정보를 해당 로그 파일 (설치 폴더\log\XmmWindowsService.log) 에 기록합니다. 또한 Exchange ActiveSync 용 Endpoint Management 커넥터는 중요한 이벤트를 Windows 이벤트 로그에 기록합니다.

로깅 수준을 변경하려면

Exchange ActiveSync 용 Endpoint Management 커넥터에는 오류, 정보, 경고, 디버그 및 추적 로깅 수준이 포함됩니다.

참고:

뒤로 갈수록 더 많은 세부 정보 (더 많은 데이터) 가 생성됩니다. 예를 들어 오류 수준은 가장 작은 세부 정보를 제공하며 추적 수준은 가장 많은 세부 정보를 제공합니다.

로깅 수준을 변경하려면 다음을 수행합니다.

1. C:\Program Files\Citrix\Citrix Endpoint Management 커넥터에서 nlog.config 파일을 엽니다.
2. <rules> 섹션에서 *minilevel* 매개 변수를 원하는 로깅 수준으로 변경합니다. 예:

```
1      <rules>
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. 파일을 저장합니다.

변경 사항은 즉시 적용됩니다. Exchange ActiveSync 에 대한 커넥터를 다시 시작할 필요가 없습니다.

일반적인 오류

다음 목록에는 일반적인 오류가 포함되어 있습니다.

- Exchange ActiveSync 용 Endpoint Management 커넥터 서비스가 시작되지 않음

로그 파일 및 Windows 이벤트 로그에서 오류를 확인합니다. 일반적인 원인은 다음과 같습니다.

- Exchange ActiveSync 용 Endpoint Management 커넥터 서비스가 SQL Server 에 액세스할 수 없습니다. 원인은 다음 문제일 수 있습니다.
 - * SQL Server 서비스가 실행되고 있지 않습니다.
 - * 인증에 실패했습니다.

Windows 통합 인증이 구성된 경우 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스의 사용자 계정이 허용된 SQL 로그인이어야 합니다. Exchange ActiveSync 용 Endpoint Management 커넥터 서비스의 계정은 기본적으로 로컬 시스템으로 설정되지만 로컬 관리자 권한이 없는 다른 계정으로 변경될 수 있습니다. SQL 인증이 구성된 경우 SQL 에서 SQL 로그인이 적절히 구성되어야 합니다.

- MSP(모바일 서비스 공급자) 에 대해 구성된 포트를 사용할 수 없습니다. 시스템의 다른 프로세스에서 사용하지 않는 수신 포트를 선택해야 합니다.

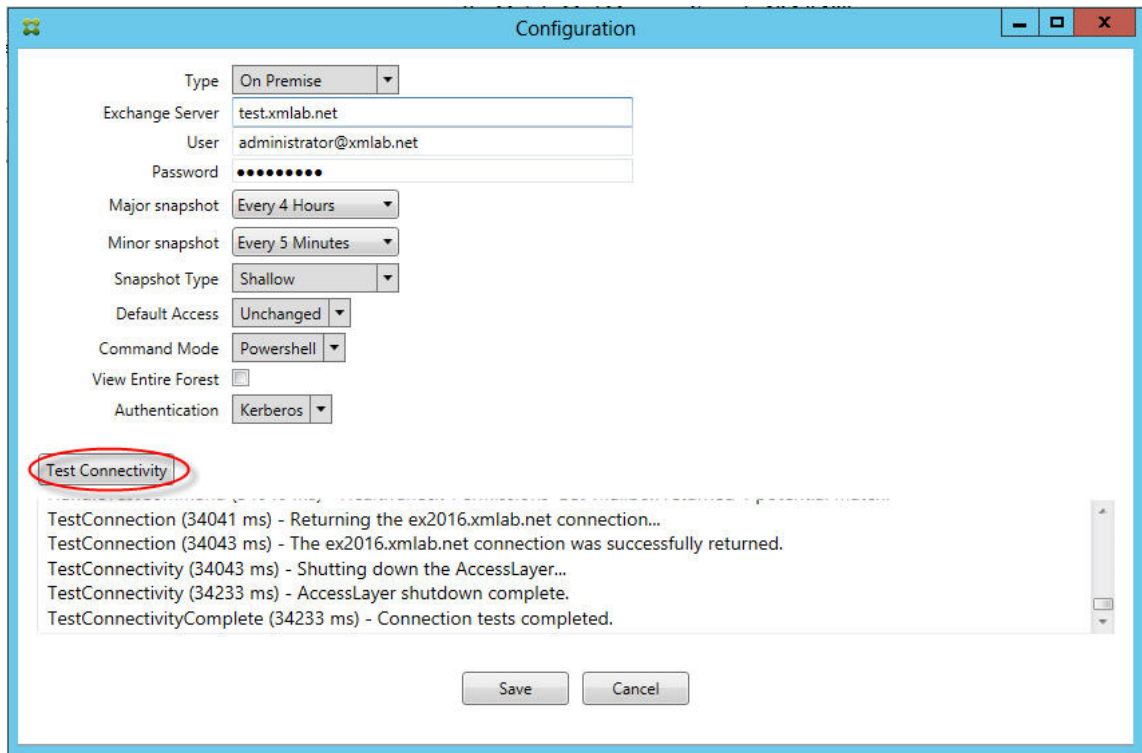
- XenMobile 에서 MSP 에 연결할 수 없음

Exchange ActiveSync 용 Endpoint Management 커넥터 콘솔의 **Configure(구성) > MSP** 탭에서 MSP 서비스 포트 및 전송이 올바르게 구성되었는지 확인합니다. 인증 그룹 또는 사용자가 올바르게 설정되었는지 확인합니다.

HTTPS 가 구성된 경우 유효한 SSL 서버 인증서가 설치되어야 합니다. IIS 가 설치된 경우 IIS Manager 를 사용하여 인증서를 설치할 수 있습니다. IIS 가 설치되지 않은 경우 [How to configure a port with an SSL certificate\(SSL 인증서로 포트를 구성하는 방법\)](#)에서 인증서 설치에 대한 자세한 내용을 확인하십시오.

Exchange ActiveSync 용 Endpoint Management 커넥터에는 MSP 서비스 연결을 테스트하는 유틸리티 프로그램이 있습니다. *InstallFolder\MspTestServiceClient.exe* 프로그램을 실행하고 URL 및 자격 증명을 XenMobile 에서 구성할 URL 및 자격 증명으로 설정한 후 연결 테스트를 클릭합니다. XenMobile Server 에서 실행하는 웹 서비스 요청이 시뮬레이션됩니다. HTTPS 가 구성된 경우 서버의 실제 호스트 이름을 지정해야 합니다 (SSL 인증서에 지정된 이름).

연결 테스트를 사용하는 경우 하나 이상의 ActiveSyncDevice 레코드가 있어야 합니다. 그렇지 않을 경우 테스트가 실패합니다.



문제 해결 도구

Support\PowerShell 폴더에 문제 해결을 위한 일련의 PowerShell 유틸리티가 있습니다.

문제 해결 도구는 사용자 사서함 및 장치를 심층 분석하여 오류 조건 및 잠재적 오류 영역을 감지하고 사용자에게 대한 RBAC 분석을 수행합니다. 모든 cmdlet의 원시 출력을 텍스트 파일에 저장할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터

March 15, 2024

XenMobile Citrix ADC Connector 는 이제 Exchange ActiveSync 용 Citrix Gateway 입니다. Citrix 통합 포트폴리오에 대한 자세한 내용은 [Citrix 제품 가이드](#)를 참조하십시오.

Exchange ActiveSync 용 커넥터는 Exchange ActiveSync 프로토콜의 역방향 프록시 역할을 하는 Citrix ADC 에 ActiveSync 클라이언트의 장치 수준 인증 서비스를 제공합니다. 인증은 XenMobile 내에서 정의된 정책의 조합과 Exchange ActiveSync 용 Citrix Gateway 커넥터에서 로컬로 정의된 규칙으로 제어됩니다.

자세한 내용은 [ActiveSync Gateway](#)를 참조하십시오.

자세한 참조 아키텍처 다이어그램은 [아키텍처](#)를 참조하십시오.

Exchange ActiveSync 용 Citrix Gateway 커넥터의 현재 릴리스는 버전 8.5.2 입니다.

중요:

2022 년 10 월부터 Exchange ActiveSync 용 Endpoint Management 및 Citrix Gateway 커넥터는 Microsoft 가 [여기](#)에서 발표한 인증 변경사항에 따라 더 이상 Exchange Online 을 지원하지 않습니다. Exchange 용 Endpoint Management 커넥터는 Microsoft Exchange Server(온-프레미스) 에서 계속 작동합니다.

새로운 항목

이후 섹션에는 이전의 XenMobile Citrix ADC Connector 인 Exchange ActiveSync 용 Citrix Gateway 커넥터의 현재 및 이전 버전에 대한 새로운 기능이 나열됩니다.

버전 **8.5.3** 의 새로운 기능

- 이 릴리스에는 ActiveSync 프로토콜 16.0 및 16.1 에 대한 지원이 추가되었습니다.
- Google Analytics 로 전송되는 분석에 특히 스냅샷과 관련하여 더 많은 세부 정보가 추가되었습니다. [CXM-52261]

버전 **8.5.2** 의 새로운 기능

- XenMobile Citrix ADC Connector 는 이제 Exchange ActiveSync 용 Citrix Gateway 입니다.

이 릴리스에서는 다음과 같은 문제가 수정되었습니다.

- 둘 이상의 기준이 정책 규칙을 정의하는 데 사용되고 이러한 기준 중 하나에 사용자 ID 가 포함된 경우 사용자에게 여러 별칭이 있으면 규칙을 적용 할 때 별칭이 확인되지 않는 문제가 발생할 수 있습니다. [CXM-55355]

참고:

다음의 새로운 기능 섹션에는 Exchange ActiveSync 용 Citrix Gateway 커넥터가 이전 이름인 XenMobile Citrix ADC Connector 로 나타납니다. 이 이름은 버전 8.5.2 에서 변경되었습니다.

버전 **8.5.1.11** 의 새로운 기능

- 시스템 요구 사항 변경: Citrix ADC Connector 의 현재 버전에는 Microsoft .NET Framework 4.5 가 필요합니다.
- **Google Analytics** 지원: XenMobile Citrix ADC Connector 가 어떻게 사용되는지를 확인하여 제품의 개선 영역에 집중할 수 있습니다.
- **TLS 1.1** 및 **1.2** 에 대한 지원: PCI Council에서는 보안이 취약한 TLS 1.0 의 사용을 중지하고 있습니다. XenMobile Citrix ADC Connector 에는 TLS 1.1 및 1.2 에 대한 지원이 추가되었습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 모니터링

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티는 Exchange Server 를 통과하면서 Secure Mobile Gateway 에 의해 허용 또는 차단된 모든 트래픽을 볼 수 있는 자세한 로깅을 제공합니다.

로그 탭을 사용하면 권한 부여를 위해 Citrix ADC 가 Exchange ActiveSync 용 커넥터로 전달한 ActiveSync 요청의 기록을 볼 수 있습니다.

또한 Exchange ActiveSync 용 Citrix Gateway 커넥터 웹 서비스가 실행 중인지 확인하려면 커넥터 서버의 브라우저에 URL <https://<host:port>/services/ActiveSync/Version>을 로드합니다. URL 이 제품 버전을 문자열로 반환하면 웹 서비스가 응답하는 상태입니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터로 ActiveSync 트래픽을 시뮬레이션하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용하여 정책과 관련된 ActiveSync 트래픽을 시뮬레이션할 수 있습니다. 커넥터 구성 유틸리티에서 **Simulator(시뮬레이터)** 탭을 선택합니다. 결과에는 구성된 규칙에 따라 정책이 적용되는 방식이 표시됩니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에 대한 필터 선택

Exchange ActiveSync 용 Citrix Gateway 커넥터 필터는 장치의 정책 위반 또는 속성 설정을 분석하여 작동합니다. 장치가 조건을 충족하면 장치가 장치 목록에 배치됩니다. 이 장치 목록은 허용 목록이나 차단 목록이 아닙니다. 정의된 조건을 충족하는 장치의 목록입니다. XenMobile 내에서 커넥터에 사용 가능한 필터는 다음과 같습니다. 각 필터에는 **Allow(허용)** 또는 **Deny(거부)** 의 두 옵션이 있습니다.

- **익명 장치:** XenMobile 에 등록되었지만 사용자의 ID 를 알 수 없는 장치를 허용 또는 거부합니다. 예를 들어 등록은 되었지만 사용자의 Active Directory 암호가 만료된 사용자 또는 알 수 없는 자격 증명으로 등록된 사용자일 수 있습니다.
- **Samsung KNOX 증명 실패:** Samsung 장치에는 보안과 진단을 위한 기능이 있습니다. 이 필터는 장치가 KNOX 에 대해 설정되었다는 확인을 제공합니다. 자세한 내용은 [Samsung Knox](#)를 참조하십시오.
- **금지된 앱:** 차단 목록 정책에 정의된 장치 목록 및 차단된 앱의 존재 여부를 기준으로 장치를 허용하거나 거부합니다.
- **암시적 허용/거부:** 다른 필터 규칙 조건을 충족하지 않는 모든 장치의 장치 목록을 만들고 해당 목록을 기반으로 허용 또는 거부합니다. 암시적 허용/거부 옵션을 사용하면 장치 탭에서 Exchange ActiveSync 용 Citrix Gateway 커넥터 상태가 사용되고 장치의 커넥터 상태가 표시됩니다. 또한 암시적 허용/거부 옵션은 선택되지 않은 다른 모든 커넥터 필터도 제어합니다. 예를 들어 차단된 앱은 커넥터에 의해 거부되지만 암시적 허용/거부 옵션이 허용으로 설정되었기 때문에 다른 모든 필터는 허용됩니다.
- **비활성 장치:** 지정된 시간 동안 XenMobile 과 통신하지 않은 장치의 장치 목록을 만듭니다. 이러한 장치는 비활성 상태로 간주됩니다. 필터는 그에 따라 장치를 허용 또는 거부합니다.
- **누락된 필수 앱:** 사용자가 등록하면 설치해야 하는 필수 앱 목록을 받게 됩니다. 누락된 필수 앱 필터는 예를 들어 사용자가 하나 이상의 앱을 삭제하여 하나 이상의 앱이 더 이상 없음을 나타냅니다.
- **비추천 앱:** 사용자가 등록하면 설치해야 하는 앱 목록을 받게 됩니다. 비추천 앱 필터는 해당 목록에 없는 앱이 장치에 있는지 확인합니다.

- 규정을 준수하지 않는 암호: 장치에 암호가 없는 모든 장치의 장치 목록을 만듭니다.
- 규정 위반 장치: 자체 내부 IT 규정 준수 조건을 충족하는 장치를 거부하거나 허용할 수 있습니다. 규정 준수는 규정 위반이라는 이름의 장치 속성 (**True** 또는 **False** 인 부울 플래그) 으로 정의되는 임의의 설정입니다. 이 속성은 수동으로 만들어 값을 설정하거나 장치가 특정 조건을 충족하거나 충족하지 않는 경우 자동화된 동작을 사용하여 장치에서 이 속성을 만들 수 있습니다.
 - 규정 위반 = **True**. 장치가 IT 부서에서 설정한 규정 표준 및 정책 정의를 충족하지 않는 경우 장치는 규정을 위반하는 것입니다.
 - 규정 위반 = **False**. 장치가 IT 부서에서 설정한 규정 표준 및 정책 정의를 충족하는 경우 장치는 규정을 준수하는 것입니다.
- 해지된 상태: 모든 해지된 장치의 장치 목록을 만들고 해지된 상태를 기반으로 하여 허용 또는 거부합니다.
- 루팅된 **Android**/탈옥 **iOS** 장치. 루팅된 것으로 플래그 지정된 모든 장치의 장치 목록을 만들고 루팅된 상태에 따라 허용 또는 거부합니다.
- 관리되지 않는 장치. XenMobile 데이터베이스에 있는 모든 장치의 장치 목록을 만듭니다. 모바일 응용 프로그램 게이트웨이는 차단 모드에서 배포해야 합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에 대한 연결을 구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터는 Secure Web 서비스를 통해 XenMobile 및 다른 원격 구성 공급자와 통신합니다.

1. 커넥터 구성 유틸리티에서 **Config Providers**(구성 공급자) 탭을 클릭하고 **Add**(추가) 를 클릭합니다.
2. **Config Providers**(구성 공급자) 대화 상자의 **Name**(이름) 에서 관리 권한이 있는 사용자 이름을 입력합니다. 이 이름은 XenMobile Server 와의 기본 HTTP 인증에 사용됩니다.
3. **Url** 에서 XenMobile GCS 의 웹 주소를 입력합니다 (일반적으로 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 형식). *MagConfigService* 이름은 대/소문자를 구분합니다.
4. **Password**(암호) 에서 XenMobile Server 와의 기본 HTTP 인증에 사용되는 암호를 입력합니다.
5. **Managing Host**(호스트 관리) 에서 커넥터 서버 이름을 입력합니다.
6. **Baseline Interval**(기준 간격) 에서 새로 고침 동적 규칙 집합을 Device Manager 에서 가져올 기간을 지정합니다.
7. **Delta interval**(델타 간격) 에서 동적 규칙의 업데이트를 가져올 기간을 지정합니다.
8. **Request Timeout**(요청 시간 초과) 에서 서버 요청 시간 초과 간격을 지정합니다.
9. **Config Provider**(구성 공급자) 에서 구성 공급자 서버 인스턴스가 정책 구성을 제공하는지 여부를 선택합니다.
10. **Events Enabled**(이벤트 사용) 에서는 장치가 차단되었을 때 커넥터가 XenMobile 에 알리도록 하려면 이 옵션을 선택합니다. XenMobile 자동화된 동작에서 커넥터 규칙을 사용하는 경우 이 옵션이 필요합니다.
11. **Save**(저장) 를 클릭한 다음 **Test Connectivity**(연결 테스트) 를 클릭하여 게이트웨이와 구성 공급자의 연결을 테스트합니다. 연결이 실패하면 로컬 방화벽 설정에서 연결이 허용되는지 확인하거나 관리자에게 문의하십시오.
12. 연결이 성공하면 **Disabled**(사용 안 함) 확인란을 선택 취소한 다음 **Save**(저장) 를 클릭합니다.

새 구성 공급자를 추가하면 Exchange ActiveSync 용 Citrix Gateway 커넥터는 공급자와 연결된 하나 이상의 정책을 자동으로 생성합니다. 이러한 정책은 NewPolicyTemplate 섹션의 `config\policyTemplates.xml`에 포함된 템플릿 정의로 정의됩니다. 이 섹션 내에 정의된 각 정책 요소에 대해 새 정책이 생성됩니다.

운영자는 정책 요소가 스키마 정의를 준수하며 표준 대체 문자열 (중괄호 안에 포함됨) 을 수정하지 않는 범위에서 정책 요소를 추가, 제거 또는 수정할 수 있습니다. 그런 다음 공급자에 대한 새 그룹을 추가하고 새 그룹이 포함되도록 정책을 업데이트합니다.

XenMobile 에서 정책을 가져오려면

1. Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티에서 **Config Providers**(구성 공급자) 탭을 클릭하고 **Add**(추가) 를 클릭합니다.
2. **Config Providers**(구성 공급자) 대화 상자의 **Name**(이름) 에서 XenMobile Server 와의 기본 HTTP 인증에 사용되며 관리 권한이 있는 사용자 이름을 입력합니다.
3. **Url** 에서 XenMobile GCS(Gateway Configuration Service) 의 웹 주소를 입력합니다 (일반적으로 <https://<xdmHost>/xdm/services/<MagConfigService>> 형식). MagConfigService 이름은 대/소문자를 구분합니다.
4. **Password**(암호) 에서 XenMobile Server 와의 기본 HTTP 인증에 사용되는 암호를 입력합니다.
5. **Test Connectivity**(연결 테스트) 를 클릭하여 게이트웨이와 구성 공급자의 연결을 테스트합니다. 연결이 실패하면 로컬 방화벽 설정에서 연결이 허용되는지 확인하거나 관리자에게 문의하십시오.
6. 연결이 성공하면 **Disabled**(사용 안 함) 확인란을 선택 취소한 다음 **Save**(저장) 를 클릭합니다.
7. **Managing Host**(호스트 관리) 에서 로컬 호스트 컴퓨터의 기본 DNS 이름을 그대로 둡니다. 이 설정은 다수의 Forefront TMG(Threat Management Gateway) 서버가 배열로 구성된 경우 XenMobile 와의 통신을 조정하는 데 사용됩니다.

설정을 저장한 후 GCS 를 엽니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 정책 모드 구성

Exchange ActiveSync 용 Citrix Gateway 커넥터는 다음 6 개 모드에서 실행될 수 있습니다.

- **Allow All**(모두 허용). 이 정책 모드는 커넥터를 통과하는 모든 트래픽에 대한 액세스를 허용합니다. 다른 필터링 규칙은 사용되지 않습니다.
- **Deny All**(모두 거부). 이 정책 모드는 커넥터를 통과하는 모든 트래픽에 대한 액세스를 거부합니다. 다른 필터링 규칙은 사용되지 않습니다.
- **Static Rules: Block Mode**(정적 규칙: 차단 모드). 이 정책 모드는 끝에 암시적 거부 또는 차단 문이 있는 정적 규칙을 실행합니다. 커넥터는 다른 필터 규칙을 통해 허용되지 않는 장치를 차단합니다.
- **Static Rules: Permit Mode**(정적 규칙: 허용 모드). 이 정책 모드는 끝에 암시적 허용 문이 있는 정적 규칙을 실행합니다. 다른 필터 규칙을 통해 차단 또는 거부되지 않는 장치는 커넥터를 통해 허용됩니다.
- **Static + ZDM Rules: Block Mode**(정적 + ZDM 규칙: 차단 모드). 이 정책 모드는 정적 규칙을 먼저 실행한 다음, 끝에 암시적 거부 또는 차단 문이 있는 XenMobile 의 동적 규칙을 실행합니다. 장치는 정의된 필터 및 Device Manager 규칙에 기반하여 허용 또는 거부됩니다. 정의된 필터 및 규칙에 일치하지 않는 모든 장치는 차단됩니다.

- **Static + ZDM Rules:** Permit Mode(정적 + ZDM 규칙: 허용 모드). 이 정책 모드는 정적 규칙을 먼저 실행한 다음, 끝에 암시적 허용 문이 있는 XenMobile의 동적 규칙을 실행합니다. 장치는 정의된 필터 및 XenMobile 규칙에 기반하여 허용 또는 거부됩니다. 정의된 필터 및 규칙에 일치하지 않는 모든 장치는 허용됩니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 프로세스는 XenMobile에서 수신된 iOS 및 Windows 기반 모바일 장치의 고유 ActiveSync ID를 기반으로 하여 동적 규칙에 대한 허용 또는 거부를 처리합니다. Android 장치의 동작은 제조사에 따라 다르며 일부는 고유 ActiveSync ID를 제공하지 않습니다. 이에 따라 XenMobile은 허용 또는 차단을 결정하기 위해 Android 장치의 사용자 ID 정보를 보냅니다. 그 결과 사용자에게 Android 장치가 하나인 경우에는 허용 및 차단이 정상적으로 작동합니다. 사용자에게 Android 장치가 여러 개인 경우에는 Android 장치를 구분할 수 없기 때문에 모든 장치가 허용됩니다. 알려진 장치의 경우 ActiveSyncID가 이러한 장치를 정적으로 차단하도록 게이트웨이를 구성할 수 있습니다. 또한 장치 유형 또는 사용자 에이전트에 따라 차단하도록 게이트웨이를 구성할 수도 있습니다.

정책 모드를 지정하려면 SMG Controller Configuration 유틸리티에서 다음을 수행합니다.

1. **Path Filters**(경로 필터) 탭을 클릭하고 **Add**(추가)를 클릭합니다.
2. **Path Properties**(경로 속성) 대화 상자의 **Policy**(정책) 목록에서 정책 모드를 선택한 다음 **Save**(저장)를 클릭합니다.

구성 유틸리티의 **Policies**(정책) 탭에서 규칙을 검토할 수 있습니다. 규칙은 Exchange ActiveSync용 Citrix Gateway 커넥터에서 하향식으로 처리됩니다. 허용 정책에는 녹색 확인 표시가 나타납니다. 거부 정책은 선이 그어진 빨간색 원으로 표시됩니다. 화면을 새로 고쳐 최근 업데이트된 규칙을 보려면 **Refresh**(새로 고침)를 클릭합니다. config.xml 파일에서 규칙 순서를 수정할 수도 있습니다.

규칙을 테스트하려면 **Simulator**(시뮬레이터) 탭을 클릭합니다. 필드에 값을 지정합니다. 로그에서 가져올 수도 있습니다. Allow(허용) 또는 Block(차단)을 지정하는 결과 메시지가 나타납니다.

정적 규칙을 구성하려면

ActiveSync 연결 HTTP 요청의 ISAPI 필터링이 읽는 값이 포함된 정적 규칙을 입력합니다. 정적 규칙을 사용하면 Exchange ActiveSync용 Citrix Gateway 커넥터가 다음 조건에 따라 트래픽을 허용하거나 차단할 수 있습니다.

- **User:** Exchange ActiveSync용 Citrix Gateway 커넥터는 장치 등록 도중 캡처된 권한 부여된 사용자 값 및 이름 구조를 사용합니다. 이러한 구조는 일반적으로 LDAP를 통해 Active Directory에 연결된 XenMobile이 실행되는 서버가 참조하는 도메인\사용자 이름으로 발견됩니다. 커넥터 구성 유틸리티 내의 **Log**(로그) 탭에 커넥터를 통해 전달되는 값이 표시됩니다. 값 구조를 구분해야 하거나 값 구조가 다른 경우 값이 전달됩니다.
- **Deviceid (ActiveSyncID):** 연결된 장치의 ActiveSyncID라고도 합니다. 이 값은 일반적으로 XenMobile 콘솔의 특정 장치 속성 페이지 내에서 볼 수 있습니다. 또한 이 값은 커넥터 구성 유틸리티의 로그 탭에서 숨겨질 수도 있습니다.
- **DeviceType:** 커넥터는 장치가 iPhone, iPad 또는 기타 장치 유형 중 무엇인지 판별하고 이 조건에 따라 허용 또는 차단할 수 있습니다. 다른 값과 마찬가지로 커넥터 구성 유틸리티는 ActiveSync 연결을 처리 중인 모든 연결된 장치 유형을 표시할 수 있습니다.
- **UserAgent:** 사용되는 ActiveSync 클라이언트에 대한 정보가 포함됩니다. 대개의 경우 지정된 값은 모바일 장치 플랫폼의 특정 운영 체제 빌드 및 버전에 해당합니다.

서버에서 실행되는 커넥터 구성 유틸리티는 항상 정적 규칙을 관리합니다.

1. SMG Controller 구성 유틸리티에서 **Static Rules**(정적 규칙) 탭을 클릭한 다음 **Add**(추가) 를 클릭합니다.
2. **Static Rule Properties**(정적 규칙 속성) 대화 상자에서 조건으로 사용할 값을 지정합니다. 예를 들어 사용자 이름 (예: AllowedUser) 을 입력한 다음 **Disabled**(사용 안 함) 확인란을 선택 취소하여 액세스를 허용할 사용자를 입력할 수 있습니다.
3. 저장을 클릭합니다.

이제 정적 규칙이 적용됩니다. 또한 정규식을 사용하여 값을 정의할 수 있지만 config.xml 파일에서 규칙 처리 모드를 사용하도록 설정해야 합니다.

동적 규칙을 구성하려면

XenMobile 의 장치 정책 및 속성은 동적 규칙을 정의하며 동적 Exchange ActiveSync 용 Citrix Gateway 커넥터 필터를 트리거할 수 있습니다. 이러한 필터는 정책 위반 또는 속성 설정의 존재 유무에 따라 트리거됩니다. 커넥터 필터는 장치의 정책 위반 또는 속성 설정을 분석하여 작동합니다. 장치가 조건을 충족하면 장치가 장치 목록에 배치됩니다. 이 장치 목록은 허용 목록이 나 차단 목록이 아닙니다. 정의된 조건을 충족하는 장치의 목록입니다. 다음 구성 옵션을 사용하면 장치 목록의 장치를 커넥터를 사용하여 허용하거나 거부할지 여부를 정의할 수 있습니다.

참고:

동적 규칙을 구성하려면 XenMobile 콘솔을 사용해야 합니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 **ActiveSync Gateway** 를 클릭합니다. ActiveSync Gateway 페이지가 나타납니다.
3. **Activate the following rules**(다음 규칙 활성화) 에서 활성화하려는 하나 이상의 규칙을 선택합니다.
4. Android 만의 **Android** 도메인 사용자를 **ActiveSync Gateway** 로 보내기에서 예를 클릭하여 XenMobile 이 Android 장치 정보를 Secure Mobile Gateway 로 보냅니다.

이 옵션을 사용하도록 설정하면 XenMobile 에 Android 장치 사용자에게 대한 ActiveSync 식별자가 없는 경우 XenMobile 이 Android 장치 정보를 Exchange ActiveSync 용 Citrix Gateway 커넥터로 보냅니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 XML 파일을 편집하여 사용자 지정 정책을 구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티 **Policies**(정책) 탭의 기본 구성에서 기본 정책을 볼 수 있습니다. 사용자 지정 정책을 만들려면 Exchange ActiveSync 용 Citrix Gateway 커넥터 XML 구성 파일 (config\config.xml) 을 편집할 수 있습니다.

1. 파일에서 **PolicyList** 섹션을 찾은 다음 새 정책 요소를 추가합니다.
2. 다른 정적 그룹이나 다른 GCP 를 지원하기 위한 그룹과 같은 새 그룹도 필요한 경우 **GroupList** 섹션에 새 그룹 요소를 추가합니다.
3. 필요한 경우 **GroupRef** 요소를 재정렬하여 기존 정책 내의 그룹 순서를 변경할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 XML 파일 구성

Exchange ActiveSync 용 Citrix Gateway 커넥터는 XML 구성 파일을 사용하여 커넥터 동작을 설명합니다. 이 파일은 다른 항목 중 그룹 파일과 HTTP 요청을 평가할 때 필터가 수행할 관련 동작을 지정합니다. 기본적으로 파일의 이름은 config.xml이며, \\Program Files\\Citrix\\XenMobile Citrix ADC Connector\\config 위치에서 찾을 수 있습니다.

GroupRef 노드

GroupRef 노드는 논리적 그룹 이름을 정의합니다. 기본값은 AllowGroup 및 DenyGroup 입니다.

참고:

GroupRefList 노드에 나타나는 GroupRef 노드의 순서는 중요한 의미를 갖습니다.

GroupRef 노드의 ID 값은 특정 사용자 계정 또는 장치를 찾는 데 사용되는 구성원의 논리적 컨테이너 또는 컬렉션을 식별합니다. 작업 특성은 컬렉션의 규칙에 일치하는 구성원을 어떤 방식으로 필터링하는지를 지정합니다. 예를 들어 AllowGroup 집합의 규칙과 일치하는 사용자 계정 또는 장치는 “통과” 됩니다. 통과란 Exchange CAS 에 대한 액세스가 허용되는 것을 의미합니다. DenyGroup 집합의 규칙과 일치하는 사용자 계정 또는 장치는 “거부” 됩니다. 거부란 Exchange CAS 에 대한 액세스가 허용되지 않는 것을 의미합니다.

특정 사용자 계정/장치 또는 조합이 두 그룹 모두의 규칙을 충족할 경우에는 우선권 규칙이 사용되어 요청의 결과가 도출됩니다. 우선권은 config.xml 파일에서 위에서 아래로 GroupRef 노드의 순서를 따릅니다. GroupRef 노드는 우선 순위에 따라 순위가 매겨집니다. 허용 그룹의 특정 조건에 대한 규칙은 거부 그룹의 동일 조건에 대한 규칙보다 항상 더 높은 우선 순위를 가집니다.

그룹 노드

config.xml 에서는 그룹 노드도 정의합니다. 이러한 노드는 논리적 컨테이너 AllowGroup 및 DenyGroup 을 외부 XML 파일에 연결합니다. 외부 파일에 저장된 항목이 필터 규칙의 기본을 구성합니다.

참고:

이 릴리스에서는 외부 XML 파일만 지원됩니다.

기본 설치 구성에서 두 개의 XML 파일인 allow.xml 및 deny.xml 을 구현합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성

속성 **Active Sync** 서비스 ID, 장치 유형, 사용자 에이전트 (장치 운영 체제), 인증된 사용자 및 **ActiveSync** 명령을 기반으로 ActiveSync 요청을 선택적으로 차단 또는 허용하도록 Exchange ActiveSync 용 Citrix Gateway 커넥터를 구성할 수 있습니다.

기본 구성은 정적 및 동적 그룹의 조합을 지원합니다. **SMG Controller Configuration** 유틸리티를 사용하여 정적 그룹을 유지합니다. 정적 그룹은 지정된 사용자 에이전트를 사용하는 모든 장치와 같이 알려진 장치 범주로 구성될 수 있습니다.

동적 그룹은 **Gateway Configuration Provider** 라고 하는 외부 소스에 의해 유지됩니다. Exchange ActiveSync 용 Citrix Gateway 커넥터는 주기적으로 그룹을 연결합니다. XenMobile 은 허용 및 차단된 장치 그룹과 사용자 그룹을 커넥터로 내보낼 수 있습니다.

동적 그룹은 **Gateway Configuration Provider** 라고 하는 외부 소스에 의해 유지되며 Exchange ActiveSync 용 Citrix Gateway 커넥터가 주기적으로 수집합니다. XenMobile 은 허용 및 차단된 장치 그룹과 사용자 그룹을 커넥터로 내보낼 수 있습니다.

정책은 각 그룹마다 연관된 작업 (허용 또는 차단) 과 그룹 구성원 목록이 있는 순서 지정된 그룹 목록입니다. 정책에 포함될 수 있는 그룹의 수에는 제한이 없습니다. 일치 항목이 발견될 때 그룹의 작업이 수행되며 이후 그룹은 평가되지 않기 때문에 정책 내의 그룹 순서는 중요합니다.

구성원은 요청의 속성을 일치시키는 방법을 정의합니다. 장치 ID 와 같은 단일 속성에 일치시키거나 장치 유형 및 사용자 에이전트와 같은 여러 속성에 일치시킬 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에 대한 보안 모델 선택

규모에 상관없이 모든 조직에게 있어 보안 모델의 확립은 성공적 모바일 장치 배포를 위해 매우 중요합니다. 사용자, 컴퓨터 또는 장치에 대한 액세스를 기본적으로 허용하는 보호 또는 격리된 네트워크 제어를 사용하는 경우가 많습니다. 하지만 이 방식이 항상 좋은 방법은 아닙니다. IT 보안을 관리하는 조직은 모두 모바일 장치의 보안에 대해 조금씩 다른 방법이나 맞춤형 방법을 사용할 수 있습니다.

모바일 장치 보안에는 동일한 논리가 적용됩니다. 모바일 장치의 수와 유형, 사용자당 모바일 장치의 수, 사용 가능한 운영 체제 플랫폼과 앱의 수가 매우 많기 때문에 허용 모델의 사용은 취약한 선택입니다. 대개의 조직에서는 제한 모델이 더 논리적인 선택입니다.

Citrix 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를 XenMobile 과 통합할 때 허용하는 구성 시나리오는 다음과 같습니다.

허용 모델 (허용 모드)

허용 보안 모델은 기본적으로 모든 것이 허용되거나 액세스 권한이 부여된다는 전제 하에 작동합니다. 규칙 및 필터링을 통해서만 무언가 차단되고 제한이 적용됩니다. 허용 보안 모델은 모바일 장치에 대한 보안 우려가 비교적 느슨한 조직에 적합합니다. 이 모델은 해당하는 경우 (정책 규칙이 실패한 경우) 액세스를 거부하는 제한적인 제어만 적용합니다.

제한 모델 (차단 모드)

제한 보안 모델은 기본적으로 어떤 것도 허용되지 않거나 액세스 권한이 부여되지 않는 전제 하에 작동합니다. 보안 검사점을 통과하는 모든 항목이 필터링 및 검사되며 액세스를 허용하는 규칙을 통과하지 못하면 액세스가 거부됩니다. 제한 보안 모델은 모바일

장치에 대한 보안 기준이 비교적 엄격한 조직에 적합합니다. 이 모드에서는 액세스 허용을 위한 모든 규칙을 통과한 경우 네트워크 서비스의 기능 및 사용에 대한 액세스를 허용합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 관리

Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용하여 액세스 제어 규칙을 작성할 수 있습니다. 액세스 제어 규칙은 관리되는 장치의 ActiveSync 연결 요청에 대한 액세스를 허용하거나 차단합니다. 액세스는 장치 상태, 앱 허용 또는 차단 목록 및 기타 규정 준수 조건에 따라 허용되거나 차단됩니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티를 사용하면 회사 전자 메일 정책을 적용하여 규정 표준을 위반하는 사용자를 차단할 수 있는 동적 및 정적 규칙을 만들 수 있습니다. 또한 전자 메일 첨부 파일 암호화를 설정하여, Exchange Server 를 통과하여 관리되는 장치로 전송되는 모든 첨부 파일을 암호화하고 권한 있는 사용자만 관리되는 장치에 이를 볼 수 있도록 할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터를 제거하려면

1. 관리자 계정으로 XncInstaller.exe 를 실행합니다.
2. 화면 지침에 따라 제거를 완료합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터를 설치, 업그레이드 또는 제거하려면

1. 관리자 계정으로 XncInstaller.exe 를 실행하여 커넥터를 설치하거나 기존 커넥터의 업그레이드 또는 제거를 허용합니다.
2. 화면 지침에 따라 설치, 업그레이드 또는 제거를 완료합니다.

커넥터를 설치한 후에는 XenMobile 구성 서비스 및 알림 서비스를 수동으로 다시 시작해야 합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 설치

Exchange ActiveSync 용 Citrix Gateway 커넥터를 자체 Windows Server 에 설치합니다.

커넥터가 서버에 가하는 CPU 부하는 관리되는 장치 수에 따라 다릅니다. 장치 수가 많은 경우 (50,000 개 초과) 클러스터링 환경이 아니라면 둘 이상의 코어를 프로비전해야 할 수 있습니다. 커넥터의 메모리 사용량은 추가 메모리가 필요할 정도로 높지 않습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 시스템 요구 사항

Exchange ActiveSync 용 Citrix Gateway 커넥터는 Citrix ADC 장비에 구성된 SSL 브리지를 통해 Citrix ADC 와 통신합니다. 이 SSL 브리지는 장비가 모든 보안 트래픽을 XenMobile 에 직접 연결할 수 있도록 해줍니다. 커넥터에는 다음의 최소 시스템 구성이 필요합니다.

구성 요소	요구 사항
컴퓨터 및 프로세서	733MHz Pentium III 733MHz 이상 프로세서. 2.0GHz Pentium III 이상 프로세서 (권장)
Citrix ADC	소프트웨어 버전 10 Citrix ADC 장비
메모리	1 GB
하드 디스크	150MB 의 사용 가능한 하드 디스크 공간이 있으며 NTFS 로 포맷된 로컬 파티션
운영 체제	Windows Server 2016, Windows Server 2012 R2 또는 Windows Server 2008 R2 서비스 팩 1. 영어 기반 서버여야 합니다. Windows Server 2008 R2 서비스 팩 1 에 대한 지원은 2020 년 1 월 14 일에 종료되며, Windows Server 2012 R2 에 대한 지원은 2023 년 10 월 10 일에 종료됩니다.
기타 장치	내부 네트워크와 통신하기 위해 호스트 운영 체제와 호환되는 네트워크 어댑터
Microsoft .NET Framework	버전 8.5.1.11 에는 Microsoft .NET Framework 4.5 가 필요합니다.
디스플레이	VGA 또는 고해상도 모니터

Exchange ActiveSync 용 Citrix Gateway 커넥터의 호스트 컴퓨터에는 다음의 최소 사용 가능한 하드 디스크 공간이 필요합니다.

- 응용 프로그램: 10MB~15MB(100MB 권장)
- 로깅: 1GB(20GB 권장)

Exchange ActiveSync 용 Citrix Gateway 커넥터의 플랫폼 지원에 대한 자세한 내용은 [지원되는 장치 운영 체제](#)를 참조하십시오.

장치 전자 메일 클라이언트

일부 전자 메일 클라이언트는 한 장치에 대해 동일한 ActiveSync ID 를 일관되게 반환하지 않습니다. Exchange ActiveSync 용 Citrix Gateway 커넥터에서는 각 장치에 고유한 ActiveSync ID 를 사용하도록 요구하므로 각 장치에 대해 동일한 고유 ActiveSync ID 를 일관되게 생성하는 전자 메일 클라이언트만 지원됩니다. 다음과 같은 전자 메일 클라이언트는 Citrix 의 테스트에서 오류 없이 실행되는 것으로 확인되었습니다.

- Samsung 기본 전자 메일 클라이언트
- iOS 기본 전자 메일 클라이언트

Exchange ActiveSync 용 Citrix Gateway 커넥터 배포

Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용하면 Citrix ADC 를 통해 XenMobile Server 와 XenMobile 관리되는 장치의 통신을 프록시 및 부하 분산할 수 있습니다. 커넥터는 주기적으로 XenMobile 과 통신하여 정책을 동기화합니다. 커넥터 및 XenMobile 은 함께 또는 독립적으로 클러스터링될 수 있으며 Citrix ADC 로 부하 분산될 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 요소

- **Exchange ActiveSync 용 Citrix Gateway 커넥터 서비스:** 이 서비스는 장치로부터의 ActiveSync 요청이 인증되었는지 확인하기 위해 Citrix ADC 가 호출할 수 있는 REST 웹 서비스 인터페이스를 제공합니다.
- **XenMobile 구성 서비스:** 이 서비스는 XenMobile 과 통신하여 XenMobile 정책 변경 내용을 커넥터와 동기화합니다.
- **XenMobile 알림 서비스:** 이 서비스는 권한이 없는 장치 액세스의 알림을 XenMobile 에 보냅니다. 이렇게 하면 XenMobile 이 장치가 차단된 이유를 사용자에게 알리는 등의 적절한 조치를 취할 수 있습니다.
- **Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티:** 관리자는 이 응용 프로그램을 사용하여 커넥터를 구성하고 모니터링할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에 대한 수신 주소를 설정하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터에서 Citrix ADC 의 ActiveSync 트래픽 승인 요청을 수신할 수 있도록 하려면 다음을 수행합니다. 커넥터가 Citrix ADC 웹 서비스 호출을 수신하는 포트를 지정합니다.

1. **Start(시작)** 메뉴에서 Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티를 선택합니다.
2. **Web Service(웹 서비스)** 탭을 클릭한 다음 커넥터 웹 서비스의 수신 주소를 입력합니다. **HTTP** 또는 **HTTPS** 또는 둘 다를 선택할 수 있습니다. 커넥터와 XenMobile 이 동일한 서버에 함께 설치된 경우에는 XenMobile 과 충돌하지 않는 포트 값을 선택하십시오.
3. 값이 구성되면 **Save(저장)** 를 클릭한 다음 **Start Service(서비스 시작)** 를 클릭하여 웹 서비스를 시작합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에서 장치 액세스 제어 정책을 구성하려면

관리되는 장치에 적용할 액세스 제어 정책을 구성하려면 다음을 수행하십시오.

1. Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티에서 **Path Filters(경로 필터)** 탭을 클릭합니다.
2. 첫 번째 행인 **Microsoft-Server-ActiveSync is for ActiveSync(Microsoft-Server-ActiveSync 가 ActiveSync 용)** 를 선택한 다음 **Edit(편집)** 를 클릭합니다.
3. **Policy(정책)** 목록에서 원하는 정책을 선택합니다. XenMobile 정책을 포함하는 정책의 경우 **Static + ZDM: Permit Mode(정적 + ZDM: 허용 모드)** 또는 **Static + ZDM: Block Mode(정적 + ZDM: 차단 모드)** 를 선택합니다. 이러한 정책은 로컬 또는 정적 규칙을 XenMobile 의 규칙과 결합합니다. Permit Mode(허용 모드) 는 규칙에 의해 명시적으로 식별되지 않는 모든 장치가 ActiveSync 에 액세스할 수 있도록 허용됨을 의미합니다. Block Mode(차단 모드) 는 이러한 장치가 차단됨을 의미합니다.

4. 정책을 설정한 후 **Save(저장)** 를 클릭합니다.

XenMobile 과의 통신을 구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터 및 Citrix ADC 와 함께 사용할 XenMobile Server(구성 공급자라고도 함) 의 이름과 속성을 지정합니다.

참고:

이 작업에서는 이미 XenMobile 을 설치 및 구성한 것으로 간주합니다.

1. Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티에서 **Config Providers(구성 공급자)** 탭을 클릭하고 **Add(추가)** 를 클릭합니다.
2. 이 배포에서 사용 중인 XenMobile Server 의 이름과 URL 을 입력합니다. 다중 테넌트 배포에서 여러 XenMobile Server 를 배포한 경우 이 이름은 각 서버 인스턴스에 대해 고유해야 합니다. 예를 들어 **Name(이름)** 에 **XMS** 를 입력할 수 있습니다.
3. **Url** 에서 XenMobile GCP(GlobalConfig Provider) 의 웹 주소를 입력합니다 (일반적으로 <https://<FQDN>/<instanceName>/services/<MagConfigService>> 형식). *MagConfigService* 이름은 대/소문자를 구분합니다.
4. **Password(암호)** 에서 XenMobile 웹 서버와의 기본 HTTP 인증에 사용될 암호를 입력합니다.
5. **Managing Host(관리 호스트)** 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를 설치한 서버 이름을 입력합니다.
6. **Baseline Interval(기준 간격)** 에서 새로 고침 동적 규칙 집합을 XenMobile 에서 가져올 기간을 지정합니다.
7. **Request Timeout(요청 시간 초과)** 에서 서버 요청 시간 초과 간격을 지정합니다.
8. **Config Provider(구성 공급자)** 에서 구성 공급자 서버 인스턴스가 정책 구성을 제공하는지 여부를 선택합니다.
9. **Events Enabled(이벤트 사용)** 에서는 장치가 차단되었을 때 Secure Mobile Gateway 가 XenMobile 에 알리도록 하려면 이 옵션을 선택합니다. Device Manager 자동화된 동작에서 Secure Mobile Gateway 규칙을 사용하는 경우 이 옵션이 필요합니다.
10. 서버를 구성한 후 **Test Connectivity(연결 테스트)** 를 클릭하여 XenMobile 연결을 테스트합니다.
11. 연결이 되면 **Save(저장)** 를 클릭합니다.

중복성 및 확장성을 위한 Exchange ActiveSync 용 Citrix Gateway 커넥터 배포

Exchange ActiveSync 용 Citrix Gateway 커넥터 및 XenMobile 배포를 확장하려면 모두 동일한 XenMobile 인스턴스를 가리키는 커넥터 인스턴스를 여러 Windows 서버에 설치한 다음 Citrix ADC 를 사용하여 서버의 부하를 분산할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성에는 두 가지 모드가 있습니다.

- 비공유 모드에서는 각 Exchange ActiveSync 용 Citrix Gateway 커넥터 인스턴스가 XenMobile Server 와 통신하며 결과 정책의 자체 사본을 유지합니다. 예를 들어 XenMobile Server 의 클러스터가 있는 경우 커넥터 인스턴스를 각 XenMobile Server 에서 실행할 수 있으며 커넥터는 로컬 XenMobile 인스턴스에서 정책을 가져옵니다.

- 공유 모드에서는 하나의 커넥터 노드가 주 노드로 지정되며 이 노드가 XenMobile 과 통신합니다. 결과 구성은 Windows 네트워크 공유 또는 Windows(또는 타사) 복제에 의해 다른 노드 간에 공유됩니다.

전체 커넥터 구성은 하나의 폴더 (몇 개의 XML 파일로 구성됨) 에 있습니다. 커넥터 프로세스는 이 폴더에 있는 모든 파일의 변경 내용을 감지하여 자동으로 구성을 다시 로드합니다. 공유 모드에서는 주 노드에 대한 장애 조치 (failover) 가 없습니다. 하지만 마지막으로 알려진 정상 구성이 커넥터 프로세스에 캐시되기 때문에 시스템은 주 서버 중지를 몇 분 동안 (예를 들어 다시 시작할 때까지) 허용합니다.

고급 개념

November 1, 2023

참고:

이 문서에서는 XenMobile Server 의 고급 개념에 대해 다룹니다. Citrix Endpoint Management 의 고급 정보에 대해서는 [고급 개념](#)을 참조하십시오.

XenMobile 고급 개념 문서는 XenMobile 의 제품 설명서에 대한 상세한 정보를 제공합니다. 전문 기술을 통해 배포 시간을 단축하는 것이 목표인 이 문서에는 콘텐츠를 작성한 기술 전문가의 설명이 인용될 수 있습니다.

전체 XenMobile 환경에 대한 의사 결정 사안, 권장 사항, 일반적인 질문 및 사용 사례는 이 섹션의 XenMobile 배포 안내서를 참조하십시오.

XenMobile 의 커뮤니티 지원 포럼은 [Citrix Discussions](#)를 참조하십시오.

온-프레미스 XenMobile 과 Active Directory 상호 작용

March 15, 2024

이 문서에서는 XenMobile Server 와 Active Directory 의 상호 작용에 대해 설명합니다. XenMobile Server 는 인라인과 백그라운드에서 Active Directory 와 상호 작용합니다. Active Directory 상호 작용과 관련된 인라인 및 백그라운드 작업에 대한 자세한 내용은 이후 섹션에 나와 있습니다.

참고:

이 문서는 상호 작용의 개요로, 상세한 내용은 다루지 않습니다. XenMobile 콘솔에서 Active Directory 및 LDAP 를 구성하는 것에 대한 자세한 내용은 [도메인 인증 또는 도메인 및 보안 토큰 인증](#)을 참조하십시오.

인라인 상호 작용

XenMobile Server 는 관리자가 구성한 LDAP 설정을 사용하여 Active Directory 와 통신합니다. 이 설정은 사용자 및 그룹에 대한 정보를 검색합니다. 다음 작업을 수행하면 XenMobile Server 와 Active Directory 가 상호 작용합니다.

1. **LDAP 구성.** Active Directory 를 구성하면 Active Directory 와의 상호 작용이 발생합니다. XenMobile Server 는 정보의 유효성을 검사하기 위해 Active Directory 를 통해 정보를 인증합니다. 서버는 제공된 인터넷 프로토콜, 포트 및 서비스 계정 자격 증명을 사용하여 인증을 수행합니다. 바인딩에 성공하면 연결이 올바르게 구성된 것입니다.

2. 그룹 기반 상호 작용.

- a) RBAC(역할 기반 액세스 제어) 및 배포 그룹 정의 생성 시 하나 이상의 그룹 검색. XenMobile Server 관리자가 XenMobile 콘솔에서 검색 텍스트 문자열을 입력하면 XenMobile Server 가 선택된 도메인에서 관리자가 입력한 하위 문자열을 포함하는 모든 그룹을 검색합니다. 그런 다음 검색에서 식별된 그룹의 objectGUID, sAMAccountName 및 고유 이름 특성을 검색합니다.

참고:

이 정보는 XenMobile Server 데이터베이스에 저장되지 않습니다.

- b) RBAC 및 배포 그룹 정의 추가 또는 업데이트. XenMobile Server 관리자가 이전 검색 결과에서 해당하는 Active Directory 그룹을 선택하고 배포 그룹 정의에 포함하면 XenMobile Server 가 Active Directory 에서 한 번에 하나씩 특정 그룹을 검색합니다. XenMobile Server 는 objectGUID 특성을 검색하고 구성원 자격을 포함하여 관리자가 선택한 특성을 검색합니다. 그룹 구성원 자격 정보는 검색된 그룹의 구성원 자격과 XenMobile Server 데이터베이스의 기존 사용자 또는 그룹의 구성원 자격을 확인하는 데 도움이 됩니다. 그룹 구성원 자격이 변경된 경우 영향받은 사용자 구성원에 대한 RBAC 및 배포 그룹이 파생되고 사용자에게 권한이 부여됩니다.

참고:

배포 그룹 정의가 변경된 경우 영향받은 사용자의 앱 또는 정책 권한 부여가 변경될 수 있습니다.

- c) **OTP(일회용 PIN)** 초대. XenMobile Server 관리자가 XenMobile Server 데이터베이스에 있는 Active Directory 그룹 목록에서 그룹을 선택하면 이 그룹의 모든 직접 및 간접 사용자가 Active Directory 에서 검색됩니다. 이전 단계에서 식별된 사용자에게 OTP 초대가 전송됩니다.

참고:

이전의 세 가지 상호 작용은 XenMobile Server 구성 변경에 따라 그룹 기반 상호 작용이 트리거되었음을 나타냅니다. 구성이 변경되지 않은 경우 Active Directory 와의 상호 작용이 발생하지 않습니다. 또한 그룹 측 변경 사항을 주기적으로 캡처하는 백그라운드 작업을 수행하지 않아도 됩니다.

3. 사용자 기반 상호 작용

- a) 사용자 증: 사용자 인증 워크플로에서는 Active Directory 와의 상호 작용이 두 번 발생합니다.

- 제공된 자격 증명을 사용하여 사용자를 인증합니다.
- objectGUID, Distinguished Name, sAMAccountName 및 그룹에 대한 직접 구성원 자격을 포함한 선별된 사용자 특성을 XenMobile Server 데이터베이스에 추가하거나 업데이트합니다. 그룹 구성원 자격이 변경된 경우 앱, 정책 및 액세스 권한 부여가 재평가됩니다.

사용자는 장치 또는 XenMobile Server 콘솔에서 인증을 수행할 수 있습니다. 두 시나리오에서 Active Directory 와의 상호 작용은 동일한 동작을 따릅니다.

- b) 앱 스토어 액세스 및 새로 고침: 스토어를 새로 고치면 직접 그룹 구성원 자격을 포함한 사용자 특성이 새로 고쳐집니다. 이 동작을 수행하면 사용자 권한 부여를 재평가할 수 있습니다.
- c) 장치 체인인 관리자는 XenMobile 콘솔에서 주기적 장치 체인인을 구성할 수 있습니다. 장치가 체크인될 때마다 직접 그룹 구성원 자격을 포함한 해당하는 사용자 특성이 새로 고쳐집니다. 이러한 체인인을 통해 사용자 권한 부여를 재평가할 수 있습니다.
- d) 그룹별 **OTP** 초대: XenMobile Server 관리자가 XenMobile Server 데이터베이스에 있는 Active Directory 그룹 목록에서 그룹을 선택하면 Active Directory 에서 직접 및 간접 (중첩) 사용자 구성원이 검색되고 XenMobile Server 데이터베이스에 저장됩니다. 이전 단계에서 식별된 사용자 구성원에게 OTP 초대가 전송됩니다.
- e) 사용자별 **OTP** 초대: 관리자가 XenMobile 콘솔 내에 검색 텍스트 문자열을 입력합니다. XenMobile Server 가 Active Directory 를 쿼리하여 입력 텍스트 문자열과 일치하는 사용자 레코드를 반환합니다. 관리자가 OTP 초대를 보낼 사용자를 선택합니다. XenMobile Server 는 Active Directory 에서 사용자 세부 정보를 검색하고 데이터베이스에 이 세부 정보를 업데이트한 후 사용자에게 초대를 전송합니다.

백그라운드 상호 작용

Active Directory 와의 인라인 통신에서는 XenMobile Server 구성이 변경되면 그룹 기반 상호 작용이 트리거됩니다. 구성이 변경되지 않은 경우 그룹에 대해 Active Directory 와의 상호 작용이 발생하지 않습니다.

이 그룹 기반 상호 작용에는 Active Directory 와 주기적으로 동기화하고 관심 그룹에 대한 변경 내용을 업데이트하는 백그라운드 작업이 필요합니다.

다음은 Active Directory 와 상호 작용하는 백그라운드 작업입니다.

1. 그룹 동기화 작업. 이 작업의 목적은 Active Directory 를 통해 관심 그룹의 고유 이름 또는 sAMAccountName 특성에 대한 변경 내용을 한 번에 하나씩 쿼리하는 것입니다. Active Directory 에 검색 쿼리를 수행하면 관심 그룹의 objectGUID 를 사용하여 고유 이름 및 sAMAccountName 특성의 현재 값이 확인되고 관심 그룹의 고유 이름 또는 sAMAccountName 값에 대한 변경 내용이 데이터베이스에 업데이트됩니다.

참고:

이 작업은 사용자-그룹 구성원 자격 정보를 업데이트하지 않습니다.

2. 중첩 그룹 동기화 작업. 이 작업은 관심 그룹의 중첩 계층에 대한 변경 내용을 업데이트합니다. XenMobile Server 에서는 관심 그룹의 직접 구성원과 간접 구성원에게 권한을 부여할 수 있습니다. 사용자의 직접 구성원 자격은 사용자 기반 인라인 상호 작용에서 업데이트됩니다. 백그라운드에서 실행되는 경우 이 작업은 간접 구성원 자격을 추적합니다. 간접 구성원 자격은 관심 그룹의 구성원인 그룹에 사용자가 포함되는 경우를 말합니다.

이 작업은 XenMobile Server 데이터베이스에서 Active Directory 그룹 목록을 수집합니다. 이러한 그룹은 배포 그룹 또는 RBAC 정의에 포함되어 있는 그룹입니다. XenMobile Server 는 이 목록에 있는 각 그룹의 구성원을 가져옵니다. 그룹의 구성원은 사용자 및 그룹을 나타내는 고유 이름의 목록으로 표시됩니다.

XenMobile Server 는 Active Directory 를 다시 쿼리하여 관심 그룹의 사용자 구성원만 가져옵니다. 두 목록의 차이점을 바탕으로 관심 그룹에만 포함되는 그룹 구성원을 확인한 후 구성원 그룹의 변경 내용을 데이터베이스에 업데이트 합니다. 계층의 모든 그룹에 대해 동일한 프로세스가 반복됩니다.

중첩 그룹이 변경된 경우 영향받은 사용자에게 권한 부여 변경 프로세스가 실행됩니다.

3. 사용하지 않는 사용자 확인. 이 작업은 XenMobile 관리자가 사용하지 않는 사용자를 확인하는 동작을 생성한 경우에만 실행됩니다. 이 작업은 그룹 동기화 작업의 범위 내에서 실행됩니다. Active Directory 를 쿼리하여 사용 안 함 상태의 관심 사용자를 한 번에 하나씩 확인합니다.

FAQ

백그라운드 작업은 기본적으로 얼마의 빈도로 실행됩니까?

- 현지 시간으로 02:00 부터 5 시간에 한 번씩 그룹 동기화 작업이 실행됩니다.
- 중첩 그룹 동기화 작업은 현지 시간으로 자정부터 하루에 한 번 실행됩니다.

그룹 동기화 작업이 필요한 이유는 무엇입니까?

- Active Directory 에 있는 사용자 레코드의 **memberOf** 특성에는 사용자가 직접 구성원인 그룹 목록이 나와 있습니다. 그룹의 OU 가 변경되면 **memberOf** 특성에 고유 이름의 최신 값이 반영됩니다. XenMobile Server 데이터베이스도 마지막으로 새로 고쳐진 값으로 업데이트됩니다. 그룹의 고유 이름이 일치하지 않으면 사용자가 배포 그룹에 액세스할 수 없게 됩니다. 또한 해당 배포 그룹에 연결된 앱 및 정책에도 액세스하지 못할 수 있습니다.
- 백그라운드 작업은 XenMobile Server 데이터베이스에 포함되는 그룹의 고유 이름 특성을 최신 상태로 유지하여 사용자가 부여받은 권한에 따라 액세스할 수 있도록 합니다.
- 동기화 작업은 Active Directory 내 그룹이 자주 변경되지 않을 것으로 가정하여 5 시간마다 실행되도록 예약됩니다.

그룹 동기화 작업을 끌 수 있습니까?

- 관심 그룹의 OU 가 변경되지 않은 것을 알고 있다면 이 작업을 꺼도 됩니다.

중첩된 그룹을 처리하는 백그라운드 작업이 필요한 이유는 무엇입니까?

- Active Directory 에서 그룹 중첩에 대한 변경은 일상적으로 발생하는 작업이 아닙니다. 관심 그룹의 중첩 계층이 변경되면 영향받는 사용자의 권한 부여가 변경됩니다. 그룹이 계층에 추가되면 구성원 사용자에게 해당하는 역할이 부여됩니다. 그룹을 중첩 계층 밖으로 이동하면 그룹의 구성원 사용자가 역할 기반 권한에 액세스하지 못할 수 있습니다.
- 중첩에 대한 변경 내용은 사용자를 새로 고칠 때 캡처되지 않습니다. 중첩 변경 내용은 주문형으로 캡처할 수 없으며 백그라운드 작업을 통해 캡처됩니다.
- 중첩 변경은 자주 발생하지 않는다는 전제에 따라 변경 내용을 확인하는 백그라운드 작업은 하루에 한 번 실행됩니다.

중첩된 그룹을 처리하는 작업을 끌 수 있습니까?

- 관심 그룹의 중첩이 변경되지 않은 것을 알고 있다면 이 작업을 꺼도 됩니다.

XenMobile 배포

March 15, 2024

XenMobile 배포를 계획할 때는 고려할 사항이 많습니다.

- 어떤 장치를 선택할지,
- 어떤 장치를 관리할지,
- 네트워크를 보호하면서 뛰어난 사용자 환경을 어떻게 조성할지,
- 어떤 하드웨어가 필요하고 문제는 어떻게 해결할 수 있는지.

이 섹션의 목표는 이와 같은 질문에 답을 할 수 있도록 지원하는 것입니다. 배포 관련 항목에 대한 사용 사례 및 권장 사항도 확인할 수 있습니다.

일부 환경 또는 사용 사례에는 지침 또는 권장 사항이 적용되지 않을 수 있습니다. XenMobile 을 실제로 배포하기 전에 테스트 환경을 설정하십시오.

이 섹션의 문서에서는 다음과 같은 분야를 다룹니다.

- 평가: 배포 계획 시 고려해야 할 일반적인 사용 사례 및 질문
- 설계 및 구성: 환경의 설계 및 구성에 대한 권장 사항
- 작동 및 모니터링: 실행 중인 환경이 원활하게 작동하는지 확인

평가

다른 배포와 마찬가지로 가장 먼저 요구 사항을 평가해야 합니다. XenMobile 을 통해 기본적으로 해결해야 하는 요구 사항은 무엇입니까? 환경의 모든 장치를 관리해야 합니까? 아니면 앱만 관리하면 됩니까? 둘 다 관리해야 합니까? XenMobile 환경에 필요한 보안 수준은 무엇입니까? 다음으로 배포 계획 시 고려해야 하는 일반적인 사용 사례 및 질문에 대해 살펴봅니다.

- [관리 모드](#)
- [장치 요구 사항](#)
- [보안 및 사용자 환경](#)
- [앱](#)
- [사용자 커뮤니티](#)
- [전자 메일 전략](#)
- [XenMobile 통합](#)
- [다중 사이트 요구 사항](#)

설계 및 구성

배포 요구 사항을 평가한 후에는 환경의 설계 및 구성을 결정할 수 있습니다. 계획해야 할 몇 가지 사항:

- 서버의 하드웨어 선택
- 앱 및 장치에 대한 정책 설정
- 등록된 사용자 가져오기

이 섹션에는 이러한 각 시나리오에 대한 사용 사례 및 권장 사항이 포함되어 있습니다.

- [Citrix ADC 및 Citrix Gateway 통합](#)
- [MDX 앱에 대한 SSO 및 프록시 고려 사항](#)
- [인증](#)
- [온-프레미스 배포용 참조 아키텍처](#)
- [서버 속성](#)
- [장치 및 앱 정책](#)
- [사용자 등록 옵션](#)
- [XenMobile 작업 조정](#)

작동 및 모니터링

XenMobile 을 시작하고 실행한 후에는 모니터링을 통해 원활하게 작동하는지 확인해야 합니다. 모니터링 섹션에서는 다음 내용을 다룹니다.

- XenMobile 및 해당 구성 요소가 생성하는 다양한 로그 및 메시지를 찾을 수 있는 위치
- 해당 로그를 읽는 방법

또한 이 섹션에는 고객 지원 피드백 시간을 줄일 수 있는 일반적인 문제 해결 단계가 포함되어 있습니다.

- [앱 프로비전 및 프로비전 해제](#)
- [대시보드 기반 작업](#)
- [역할 기반 액세스 제어 및 XenMobile 지원](#)
- [시스템 모니터링](#)
- [재해 복구](#)
- [Citrix 지원 프로세스](#)

관리 모드

March 15, 2024

각 XenMobile 인스턴스 (단일 서버 또는 노드 클러스터) 에 대해 장치, 앱 또는 둘 다를 관리할지 여부를 선택할 수 있습니다. XenMobile 에서는 장치 및 앱 관리 모드에 다음 용어를 사용합니다.

- MDM 모드 (모바일 기기 관리 모드)
- MAM 모드 (모바일 앱 관리 모드)
- MDM+MAM 모드 (엔터프라이즈 모드)

MDM 모드 (모바일 기기 관리 모드)

중요:

MDM 모드를 구성하고 나중에 ENT 모드로 변경하는 경우 동일한 인증 (Active Directory) 을 사용해야 합니다. XenMobile 은 사용자 등록 후의 인증 모드 변경을 지원하지 않습니다. 자세한 내용은 [업그레이드](#)를 참조하십시오.

MDM 을 사용하는 경우 모바일 장치를 구성하고 보호하고 지원할 수 있습니다. MDM 을 사용하면 장치와 장치의 데이터를 시스템 수준에서 보호할 수 있습니다. 정책, 동작 및 보안 기능을 구성할 수 있습니다. 예를 들어 장치의 분실, 도난 또는 규정 위반 시 장치를 선택적으로 초기화할 수 있습니다. MDM 모드에서는 앱 관리를 사용할 수 없지만 이 모드에서 공용 앱 스토어 및 엔터프라이즈 앱 같은 모바일 앱을 제공할 수 있습니다. 다음은 MDM 모드의 일반적인 사용 사례입니다.

- MDM 은 장치 수준 관리 정책 또는 제한 (예: 전체 초기화, 선택적 초기화 또는 지리적 위치 찾기) 이 필요한 회사 소유 장치를 위한 모드입니다.
- 고객이 실제 장치를 관리해야 하지만 MDX 정책 (예: 앱 컨테이너화, 앱 데이터 공유 제어 또는 Micro VPN) 은 필요하지 않은 경우.
- 사용자가 모바일 장치의 기본 전자 메일 클라이언트로 전자 메일을 전송하기만 하면 되고 이미 외부 액세스가 가능한 Exchange ActiveSync 또는 클라이언트 액세스 서버가 있는 경우. 이 사용 사례에서는 MDM 을 사용하여 전자 메일 전송을 구성할 수 있습니다.
- 기본 엔터프라이즈 앱 (비 MDX), 공용 앱 스토어 앱 또는 공용 스토어에서 제공되는 MDX 앱을 배포하는 경우. MDM 솔루션을 단독으로 사용하는 경우 장치의 앱 간에 전송되는 기밀 정보의 데이터 유출을 방지하지 못할 수 있습니다. 데이터 유출은 Office 365 앱의 복사 및 붙여넣기 또는 다른 이름으로 저장 작업에서 발생할 수 있습니다.

MAM 모드 (모바일 앱 관리)

MAM 은 앱 데이터를 보호하며 앱 데이터 공유를 제어할 수 있는 기능을 제공합니다. 또한 MAM 에서는 회사 데이터 및 리소스를 개인 데이터와 따로 관리할 수 있습니다. XenMobile 을 MAM 모드로 구성하면 MDX 사용 모바일 앱을 사용하여 앱별 컨테이너화 및 제어를 제공할 수 있습니다. MAM 모드를 MAM 전용 모드라고도 합니다. 이 용어는 이 모드를 레거시 MAM 모드와 구분합니다.

XenMobile 은 MDX 정책을 활용하여 네트워크 액세스 (예: Micro VPN), 앱 및 장치 상호 작용, 데이터 암호화 및 앱 액세스를 앱 수준에서 제어합니다.

MAM 은 주로 BYO(Bring-Your-Own) 장치에 적합합니다. 이 모드에서는 장치가 관리되지 않지만 회사 데이터가 보호되는 상태로 유지되기 때문입니다. MDX 에는 MDM 컨트롤이 필요하지 않은 MAM 전용 정책이 많이 있습니다.

또한 MAM 은 모바일 생산성 앱을 지원합니다. 이 지원에는 Citrix Secure Mail 로의 보안 전자 메일 전송, 보안이 적용된 모바일 생산성 앱 간의 데이터 공유 및 Citrix Files 의 보안 데이터 스토리지가 포함됩니다. 자세한 내용은 [모바일 생산성 앱](#)을 참조하십시오.

MAM 은 주로 다음과 같은 사례에 적합합니다.

- 앱 수준에서 관리되는 모바일 앱 (예: MDX 앱) 을 제공합니다.
- 장치를 시스템 수준에서 관리할 필요가 없습니다.

MDM+MAM(엔터프라이즈 모드)

MDM+MAM 은 엔터프라이즈 모드라고도 하는 하이브리드 모드로, XenMobile EMM(엔터프라이즈 모빌리티 관리) 솔루션에서 사용 가능한 모든 기능 집합을 사용하도록 설정합니다. XenMobile 을 MDM+MAM 모드로 구성하면 MDM 기능과 MAM 기능을 모두 사용할 수 있습니다.

XenMobile 에서는 사용자로 하여금 장치 관리의 등록 취소를 선택할 수 있도록 하거나 장치 관리의 등록을 의무화할지 여부를 지정할 수 있습니다. 이 유연성은 여러 사용 사례가 포함되는 환경에 유용합니다. 이러한 환경에서는 MAM 리소스에 액세스할 때 MDM 정책을 통한 장치 관리가 필요하거나 필요하지 않을 수 있습니다.

MDM+MAM 은 다음과 같은 사례에 적합합니다.

- MDM 과 MAM 이 모두 필요한 사용 사례가 한 가지 있습니다. MAM 리소스에 액세스할 때 MDM 이 필요합니다.
- 일부 사용 사례에 MDM 이 필요하고 다른 사용 사례에는 필요하지 않습니다.
- 일부 사용 사례에 MAM 이 필요하고 다른 사용 사례에는 필요하지 않습니다.

서버 모드 속성을 사용하여 XenMobile Server 의 관리 모드 를 지정합니다. XenMobile 콘솔에서 설정을 구성합니다. 모드는 MDM, MAM 또는 ENT(MDM+MAM) 일 수 있습니다.

사용할 수 있는 관리 모드 및 기타 기능은 다음 표에 표시된 것과 같이 라이선스가 있는 XenMobile 버전에 따라 결정됩니다.

XenMobile MDM Edition	XenMobile Advanced Edition
MDM 기능	MDM 기능
-	MAM 기능
-	MAM SDK
Secure Hub	Secure Hub
-	Secure Mail
-	Secure Web

관리 모드 및 등록 프로필

관리 모드와 등록 프로필은 함께 작동합니다. 등록 프로필을 사용하여 Android 및 iOS 기기의 장치 관리 및 앱 관리 등록 옵션을 구성합니다. Android 의 경우 MDM+MAM 서버 모드에 제공되는 등록 옵션은 MDM 모드의 옵션과 다릅니다. 자세한 내용은 [등록 프로필](#)을 참조하십시오.

장치 관리 및 MDM 등록

XenMobile Enterprise 환경에는 여러 사용 사례가 혼재할 수 있으며 일부 사용 사례에는 MAM 리소스에 액세스할 때 MDM 정책을 통한 장치 관리가 필요합니다. 모바일 생산성 앱을 사용자에게 배포하기 전에 사용 사례를 철저히 평가하고 MDM 등록

이 필요한지 여부를 결정해야 합니다. MDM 등록에 대한 요구 사항을 나중에 변경하려는 경우 사용자가 장치를 재등록해야 합니다.

참고:

사용자에게 MDM 등록을 요구할지 여부를 지정하려면 XenMobile 콘솔 (설정 > 서버 속성) 에서 XenMobile Server 속성 등록 필요를 사용합니다. 이 글로벌 서버 속성은 XenMobile 인스턴스의 모든 사용자 및 장치에 적용됩니다. 이 속성은 XenMobile Server 모드가 ENT 인 경우에만 적용됩니다.

다음은 XenMobile 엔터프라이즈 모드 배포에서 MDM 등록을 요구할 때의 장점과 단점 (완화 옵션 포함) 을 요약한 것입니다.

MDM 등록이 선택 사항인 경우

장점:

- 사용자가 장치를 MDM 관리에 등록하지 않고 MAM 리소스에 액세스할 수 있습니다. 이 옵션은 사용자 채택률을 높입니다.
- MAM 리소스에 대한 액세스를 보호하여 엔터프라이즈 데이터를 보호할 수 있습니다.
- MDX 정책 (예: 앱 암호) 을 사용하여 각 MDX 앱에 대한 앱 액세스를 제어할 수 있습니다.
- Citrix PIN 과 함께 Citrix ADC, XenMobile Server 및 응용 프로그램별 시간 초과를 구성하여 추가 계층의 보호를 제공할 수 있습니다.
- MDM 동작은 장치에 적용되지 않지만 일부 MDX 정책을 사용하여 MAM 액세스를 거부할 수 있습니다. 거부는 시스템 설정 (예: 탈옥 또는 루팅 장치) 에 따라 수행됩니다.
- 사용자가 첫 사용 시 장치를 MDM 에 등록할지 여부를 선택할 수 있습니다.

단점:

- MDM 에 등록되지 않은 장치에서 MAM 리소스를 사용할 수 있습니다.
- MDM 정책 및 동작을 MDM 등록 장치에서만 사용할 수 있습니다.

완화 옵션:

- 사용자가 규정 위반을 선택하는 경우 책임을 져야 한다는 회사 약관에 동의하도록 합니다. 관리자에게 관리되지 않는 장치를 모니터링하도록 합니다.
- 응용 프로그램 타이머를 사용하여 응용 프로그램 액세스 및 보안을 관리합니다. 시간 초과 값을 줄이면 보안이 개선되지만 사용자 경험에 영향을 미칠 수 있습니다.
- 필요한 경우 두 번째 XenMobile 환경에서 MDM 등록을 요구할 수 있습니다. 이 옵션을 고려할 때는 두 환경을 관리하는 것으로 인해 추가 오버헤드가 발생하고 리소스가 추가로 필요하다는 점을 염두에 두십시오.

MDM 등록이 필수인 경우

장점:

- MAM 리소스에 대한 액세스를 MDM 관리 장치로만 제한할 수 있습니다.
- 원하는 경우 MDM 정책 및 동작을 환경의 모든 장치에 적용할 수 있습니다.
- 사용자가 장치 등록을 취소할 수 없습니다.

단점:

- 모든 사용자가 필수적으로 MDM 에 등록해야 합니다.
- 회사에서 개인 장치를 관리하는 것을 반대하는 사용자의 채택이 감소할 수 있습니다.

완화 옵션:

- XenMobile 이 실제로 장치에서 관리하는 항목과 관리자가 액세스할 수 있는 정보를 사용자에게 알려줍니다.
- MDM 관리가 필요하지 않은 장치에 대해 MAM 서버 모드 (MAM 전용 모드) 의 두 번째 XenMobile 환경을 사용할 수 있습니다. 이 옵션을 고려할 때는 두 환경을 관리하는 것으로 인해 추가 오버헤드가 발생하고 리소스가 추가로 필요하다는 점을 염두에 두십시오.

MAM 모드와 레거시 **MAM** 모드 정보

XenMobile 10.3.5 에는 새로운 MAM 전용 서버 모드가 도입되었습니다. 이전 MAM 모드와 새 MAM 모드를 구분하기 위해 설명서에는 다음과 같은 용어가 사용됩니다. 새 모드는 MAM 전용 또는 MA 라고 하며 이전 MAM 모드는 레거시 MAM 모드라고 합니다.

MAM 전용 모드는 XenMobile 의 서버 모드 속성이 MAM 일 때 적용됩니다. 장치는 MAM 모드에서 등록됩니다.

레거시 MAM 기능은 XenMobile 의 서버 모드 속성이 ENT 이고 사용자가 장치 등록을 선택하지 않는 경우 적용됩니다. 이 경우 장치는 MAM 모드에서 등록됩니다. MDM 관리를 등록 취소하는 사용자에게는 계속해서 레거시 MAM 기능이 제공됩니다.

참고:

이전에는 서버 모드 속성을 MAM 으로 설정해도 ENT 로 설정할 때와 동일한 효과가 있었습니다. MDM 관리를 선택하지 않은 사용자에게 레거시 MAM 기능이 제공되었습니다.

다음 표에는 특정 라이선스 유형 및 원하는 장치 모드에 사용되는 서버 모드 설정이 요약되어 있습니다.

라이선스 버전	장치 등록에 사용할 모드	설정된 서버 모드 속성
Enterprise/Advanced/MDM	MDM 모드	MDM
Enterprise/Advanced	MAM 모드 (MAM 전용 모드)	MAM
Enterprise/Advanced	MDM+MAM 모드	ENT(레거시 MAM 모드에서 작동하는 장치 관리에 등록하지 않는 사용자)

MAM 전용 모드는 이전에 ENT 모드에서만 사용할 수 있었던 다음 기능을 지원합니다.

- **인증서 기반 인증:** MAM 전용 모드는 인증서 기반 인증을 지원합니다. 사용자는 Active Directory 암호가 만료된 경우에도 계속해서 앱에 액세스할 수 있습니다. MAM 장치에서 인증서 기반 인증을 사용하는 경우 Citrix Gateway 를 구성해야 합니다. 기본적으로 **XenMobile 설정 > Citrix Gateway** 에서 인증을 위한 사용자 인증서 제공은 꺼짐으로 설정되어 있습니다. 이는 사용자 이름과 암호 인증이 사용됨을 의미합니다. 이 설정을 켜짐으로 설정하면 인증서 인증이 사용됩니다.
- **자가 지원 포털:** 사용자가 직접 앱 잠금 및 앱 초기화를 수행할 수 있습니다. 이러한 동작은 장치의 모든 앱에 적용됩니다. 구성 > 동작에서 앱 잠금 및 앱 초기화 동작을 구성할 수 있습니다.
- **모든 등록 보안 모드:** 관리 > 등록 초대에서 구성된 높은 수준의 보안, 초대 URL 및 2 단계가 포함됩니다.
- **Android 및 iOS** 장치에 대한 장치 등록 제한: 사용자당 장치 수 서버 속성이 구성 > 등록 프로필로 이동했고 이제 모든 서버 모드에 적용됩니다.
- **MAM 전용 API:** MAM 전용 장치에서 REST 서비스를 호출할 수 있습니다. REST 클라이언트와 XenMobile REST API 를 사용하여 XenMobile 콘솔에 표시되는 서비스를 호출할 수 있습니다.
- MAM 전용 API 를 사용하여 다음을 수행할 수 있습니다.
 - 초대 URL 과 일회용 PIN 을 전송합니다.
 - 장치에서 앱 잠금 치 초기화를 실행합니다.

다음 표에는 레거시 MAM 기능과 MAM 전용 기능의 차이점이 요약되어 있습니다.

등록 시나리오 및 기타 기능	레거시 MAM(ENT 서버 모드)	MAM 전용 모드 (MAM 서버 모드)
인증서 인증	지원되지 않음.	지원됨. 인증서 인증을 사용하려면 Citrix Gateway 가 필요합니다.
배포 요구 사항	장치에서 직접 XenMobile Server 에 액세스하지 않아도 됩니다.	장치에서 직접 XenMobile Server 에 액세스하지 않아도 됩니다.
등록 옵션	Citrix Gateway FQDN 을 사용하거나 MDM FQDN 을 사용하는 경우 등록하지 않도록 선택합니다.	XenMobile Server FQDN 을 사용합니다.
등록 방법 *	사용자 이름 + 암호	사용자 이름 + 암호, 높은 수준의 보안, 초대 URL + PIN, 초대 URL + 암호, 2 단계, 사용자 이름 + PIN
앱 잠금 및 초기화	지원됨.	지원됨.
앱 잠금 및 초기화에 대한 자가 지원 포털 옵션	지원되지 않음.	지원됨.
앱 초기화 동작	앱이 장치에 유지되지만 사용할 수 없습니다. XenMobile 은 클라이언트의 계정만 삭제합니다.	앱이 장치에 유지되지만 사용할 수 없습니다. XenMobile 은 클라이언트의 계정만 삭제합니다.
MAM 전용 사용에 대한 자동화 동작.	이벤트, 장치 속성, 사용자 속성 동작이 지원됩니다. 설치된 앱 기반 자동화 동작은 지원되지 않습니다.	이벤트, 장치 속성, 사용자 속성 및 일부 앱 기반 동작 (예: 앱 초기화 및 앱 잠금)이 지원됩니다.

Active Directory 사용자가 삭제될 때 의 기본 제공 동작	앱 초기화가 지원됩니다.	앱 초기화가 지원됩니다.
등록 제한	지원됨. 등록 프로필을 통해 구성됩니다.	지원됨. 등록 프로필을 통해 구성됩니다.
소프트웨어 인벤토리	지원됨. XenMobile 이 장치에 설치된 앱을 나열합니다.	지원되지 않음.

* 알림 관련: 등록 초대를 보낼 때는 SMTP 방법만 지원됩니다.

중요:

MAM 전용 모드에서 이전에 등록한 사용자는 장치를 재등록해야 합니다. 사용자 등록에 필요한 XenMobile Server FQDN 을 사용자에게 알려줘야 합니다. MAM 전용 모드에서는 ENT 모드와 마찬가지로 XenMobile Server FQDN 을 사용하여 장치를 등록합니다. (레거시 MAM 모드에서는 Citrix Gateway FQDN 을 사용하여 장치를 등록합니다.)

장치 요구 사항

January 5, 2022

모든 배포에서 가장 중요한 고려 사항 중 하나는 돌아올 장치입니다. iOS, Android 및 Windows 플랫폼에서 옵션은 많습니다. XenMobile 이 지원하는 장치 목록은 [지원되는 장치 플랫폼](#)을 참조하십시오.

BYOD(Bring Your Own Device) 환경에서는 여러 유형의 지원되는 플랫폼이 사용될 수 있습니다. 그러나 등록할 수 있는 장치를 사용자에게 알릴 때에는 지원되는 장치 플랫폼 문서의 제한 사항을 고려하십시오. 환경에서 1~2 개의 장치만 허용한다 하더라도 XenMobile 은 iOS, Android 및 Windows 장치에서 조금씩 다르게 작동합니다. 각 플랫폼에서 사용할 수 있는 기능 집합이 다릅니다.

또한 모든 앱이 태블릿 폼 팩터와 휴대폰 폼 팩터 모두에서 사용할 수 있도록 설계되는 것은 아닙니다. 대대적인 변경을 수행하기 전에 앱을 테스트하여 돌아올하려는 장치 화면에 앱이 맞는지 확인하십시오.

다음과 같은 등록 요소도 고려할 수 있습니다. Apple 및 Google 은 엔터프라이즈 등록 프로그램을 제공합니다. [Apple 배포 프로그램](#)과 [Google Android Enterprise](#)를 통해 직원이 바로 사용할 수 있도록 미리 구성된 장치를 구입할 수 있습니다.

등록에 대한 자세한 내용은 [사용자 등록 옵션](#)을 참조하십시오.

보안 및 사용자 환경

March 15, 2024

보안은 모든 조직에서 중요하지만 보안과 사용자 환경 사이의 균형을 맞춰야 합니다. 예를 들어 매우 안전하지만 사용하기가 어려운 환경을 구축할 수 있는가 하면, 액세스 제어가 엄격하지 않은 사용자 친화적인 환경을 구축할 수도 있습니다. 보안 기능은 이 가상 안내서의 다른 섹션에서 자세히 다룹니다. 이 문서의 목적은 일반적인 보안 우려 사항과 XenMobile에서 제공되는 보안 옵션을 대략적으로 설명하는 것입니다.

다음은 각 사용 사례에서 주로 고려해야 할 사항입니다.

- 특정 앱, 전체 장치 또는 둘 다를 보호해야 합니까?
- 사용자 ID를 인증할 때 어떤 방법을 사용하고 있습니까? LDAP 인증, 인증서 기반 인증 또는 두 인증의 조합을 사용할 계획입니까?
- 사용자 세션 시간 초과를 어떻게 처리하려고 합니까? 백그라운드 서비스, Citrix ADC 및 오프라인 중 앱 액세스에 대한 시간 초과 값이 서로 다르다는 점에 유의하십시오.
- 사용자가 장치 수준 암호, 앱 수준 암호 또는 모두를 설정해야 합니까? 사용자가 시도할 수 있는 로그인 횟수는 몇 번입니까? MAM으로 구현되는 추가적인 앱별 인증 요구 사항이 사용자 환경에 미치는 영향을 염두에 두십시오.
- 사용자에게 적용하려는 다른 제한 사항은 무엇입니까? 사용자가 Siri와 같은 클라우드 서비스에 액세스하길 원합니까? 사용자는 제공된 각 앱을 사용하여 무엇을 할 수 있고 무엇을 할 수 없습니까? 사무실 공간 안에 있는 동안 셀룰러 데이터 요금이 소비되지 않도록 회사 Wi-Fi 정책을 배포해야 합니까?

앱 대 장치

일단 모바일 앱 관리 (MAM)를 사용하여 특정한 앱의 보안만 확보할지 여부를 먼저 고려해야 합니다. 아니면 모바일 장치 관리 (MDM)를 사용하여 전체 장치를 관리할 수도 있습니다. 일반적으로, 장치 수준 제어가 필요하지 않은 경우, 특히 조직에서 BYOD(Bring Your Own Device)를 지원하는 경우에는 모바일 앱만 관리하면 됩니다.

XenMobile을 통해 관리되지 않는 장치의 사용자는 앱 스토어를 통해 앱을 설치할 수 있습니다. 선택적 초기화 또는 전체 초기화 같은 장치 수준 제어 대신 앱 정책을 사용하여 앱 액세스를 제어할 수 있습니다. 설정한 값에 따라 정책은 장치에서 주기적으로 XenMobile에 연결하여 앱 실행이 허용되는지 여부를 확인해야 합니다.

MDM을 사용하면 하나의 장치에 모든 소프트웨어의 인벤토리를 가져오는 기능 등 전체 장치의 보안을 확보할 수 있습니다. 장치가 탈옥 또는 루팅되거나 장치에 안전하지 않은 소프트웨어가 설치되면 등록할 수 없게 만들 수 있습니다. 그러나 이 수준의 제어를 사용하면 사용자가 개인 장치에 이렇게 많은 권한을 허용하는 것을 주저하고 등록 비율이 감소할 수 있습니다.

인증

인증은 사용자 환경과 많은 관련이 있는 영역입니다. 이미 Active Directory를 실행 중인 조직에서는 Active Directory를 사용하여 시스템에 대한 사용자 액세스를 제공하는 것이 가장 간단한 방법입니다.

인증 사용자 환경에서 중요한 또 다른 요소는 시간 초과입니다. 보안 수준이 높은 환경에서는 사용자가 시스템에 액세스할 때마다 로그인해야 하지만 일부 조직에서는 이 옵션이 적합하지 않습니다. 예를 들어 전자 메일에 액세스할 때마다 자격 증명을 입력하도록 하면 사용자 환경에 크게 영향을 미칠 수 있습니다.

사용자 엔트로피

보안을 추가하려면 사용자 엔트로피라고 하는 기능을 사용할 수 있습니다. Citrix Secure Hub 와 일부 다른 앱은 암호, PIN 및 인증서 같은 공통 데이터를 공유하여 모든 기능이 올바르게 작동되도록 합니다. 이 정보는 Secure Hub 의 일반 저장소에 저장됩니다. **Encrypt Secrets(암호 암호화)** 옵션을 통해 사용자 엔트로피를 사용하면 XenMobile 이 UserEntropy 라는 이름의 새 저장소를 만듭니다. XenMobile 은 이 정보를 일반 저장소에서 새 저장소로 옮깁니다. Secure Hub 또는 다른 앱에서 데이터에 액세스하려면 사용자가 암호 또는 PIN 을 입력해야 합니다.

사용자 엔트로피를 사용하면 여러 위치에서 인증 계층이 추가됩니다. 그 결과, 사용자는 앱이 UserEntropy 저장소에서 인증서 등의 공유 데이터에 대한 액세스를 요구할 때마다 암호 또는 PIN 을 입력해야 합니다.

사용자 엔트로피에 대한 자세한 내용은 XenMobile 설명서에서 [About the MDX Toolkit\(MDX Toolkit 정보\)](#)를 참조하십시오. 사용자 엔트로피를 켜려면 [클라이언트 속성](#)에서 관련 설정을 찾을 수 있습니다.

정책

MDX 정책과 MDM 정책은 조직에 많은 유연성을 제공하지만 사용자를 제한할 수도 있습니다. 예를 들면 Siri 또는 iCloud 와 같이 민감한 데이터를 여러 위치로 전송할 가능성이 있는 클라우드 응용 프로그램에 대한 액세스를 차단하는 것이 좋습니다. 이러한 서비스에 대한 액세스를 차단하는 정책을 설정할 수 있지만 이러한 정책으로 인해 의도치 않은 결과가 발생할 수 있다는 점을 고려해야 합니다. iOS 키보드 마이크에도 클라우드 액세스가 사용되며 이 기능에 대한 액세스도 차단할 수 있습니다.

앱

EMM(엔터프라이즈 모빌리티 관리) 은 MDM(모바일 기기 관리) 과 MAM(모바일 응용 프로그램 관리) 으로 나뉩니다. MDM 은 모바일 장치의 보안 및 제어에 사용되고 MAM 은 응용 프로그램의 제공 및 관리를 용이하게 합니다. BYOD 채택이 증가하면 MAM 솔루션을 구현하여 응용 프로그램 제공, 소프트웨어 라이선스, 구성 및 응용 프로그램 수명 주기 관리를 지원할 수 있습니다.

XenMobile 을 사용하면 특정 MAM 정책 및 VPN 설정을 구성하여 데이터 유출 및 기타 보안 위협을 방지함으로써 이러한 앱을 추가로 보호할 수 있습니다. XenMobile 을 사용하면 조직에서는 다음 솔루션 중 하나를 유연하게 배포할 수 있습니다.

- MAM 전용 환경
- MDM 전용 환경
- 동일한 플랫폼에서 MDM 및 MAM 기능을 모두 제공하는 통합 XenMobile 엔터프라이즈 환경

모바일 장치에 앱을 제공하는 것에 더해 XenMobile 은 MDX 기술을 통해 앱을 컨테이너화할 수 있는 기능을 제공합니다. MDX 은 플랫폼에서 제공하는 장치 수준 암호화와는 다른 암호화를 통해 앱의 보안을 확보합니다. 앱을 삭제하거나 잠글 수 있으며 앱은 점진적인 정책 기반 제어의 대상이 됩니다. ISV(독립 소프트웨어 공급업체) 는 Mobile Apps SDK 를 사용하여 이러한 제어를 적용할 수 있습니다.

기업 환경에서 사용자는 다양한 모바일 앱을 사용하여 업무를 지원합니다. 공용 앱 스토어의 앱, 사내에서 개발한 앱 및 기본 앱이 여기에 포함될 수 있습니다. XenMobile 은 이러한 앱을 다음과 같이 범주화합니다.

공용 앱: Apple App Store 또는 Google Play 와 같은 공용 앱 스토어에서 무료 또는 유료로 제공되는 앱이 포함됩니다. 조직 외부의 공급업체는 주로 공용 앱 스토어를 통해 앱을 제공합니다. 이 옵션을 사용하는 경우 공급업체의 고객이 인터넷에서 직접 앱을 다운로드할 수 있습니다. 조직의 사용자는 사용자 요구 사항에 따라 수많은 공용 앱을 사용할 수 있습니다. 예를 들어 GoToMeeting, Salesforce 및 EpicCare 앱이 이러한 앱에 포함됩니다.

Citrix 는 공용 앱 스토어에서 직접 앱 이진을 다운로드한 다음 MDX Toolkit 을 사용하여 엔터프라이즈 배포용으로 래핑하는 것을 지원하지 않습니다. 타사 응용 프로그램에 MDX 를 사용하려면 앱 공급업체에 문의하여 앱 바이너리를 받아야 합니다. MDX Toolkit 으로 바이너리를 래핑하거나 바이너리와 MAM SDK 를 통합할 수 있습니다.

사내 앱: 많은 조직이 사내 개발자를 통해 특정 기능을 제공하는 앱을 만듭니다. 사내 개발자는 조직 내에서 이러한 앱을 독립적으로 개발하고 배포합니다. 경우에 따라 일부 조직에서는 ISV 가 제공하는 앱을 사용하기도 합니다. 이러한 앱을 기본 앱으로 배포하거나 XenMobile 같은 MAM 솔루션을 사용하여 앱을 컨테이너화할 수 있습니다. 예를 들어 의료 조직에서는 의사가 모바일 장치에서 환자 정보를 볼 수 있도록 하는 사내 앱을 만들 수 있습니다. 그런 다음 조직에서는 앱에 MAM SDK 를 사용하거나 MDM 를 래핑하여 환자 정보를 보호하고 백엔드 환자 데이터베이스 서버에 대한 VPN 액세스를 지원할 수 있습니다.

웹 및 SaaS 앱: 내부 네트워크에서 액세스되는 앱 (웹 앱) 또는 공용 네트워크를 통해 액세스되는 앱 (SaaS) 이 포함됩니다. XenMobile 에서는 앱 커넥터 목록을 사용하여 사용자 지정 웹 및 SaaS 앱을 만들 수도 있습니다. 이러한 앱 커넥터를 사용하면 기존 웹 앱에 대한 SSO(Single Sign-on) 를 쉽게 구현할 수 있습니다. 자세한 내용은 [앱 커넥터 유형](#)을 참조하십시오. 예를 들어 Google Apps 에 대한 SAML(Security Assertion Markup Language) 기반 SSO 에는 Google Apps SAML 을 사용할 수 있습니다.

모바일 생산성 앱: Citrix 에서 개발한 앱으로, XenMobile 라이선스에 포함됩니다. 자세한 내용은 [모바일 생산성 앱 정보](#)를 참조하십시오. 또한 Citrix 는 다른 ISV 에서 Worx App SDK 를 사용하여 개발하는 다른 [비즈니스용 앱](#)을 제공합니다.

HDX 앱: Windows 에서 호스트되는 앱으로, StoreFront 를 사용하여 게시합니다. Citrix Virtual Apps and Desktops 환경이 있는 경우 이러한 앱을 XenMobile 과 통합하여 등록된 사용자에게 앱을 제공할 수 있습니다.

XenMobile 을 사용하여 배포하고 관리하려는 모바일 앱의 유형에 따라 기본 구성과 아키텍처가 달라집니다. 예를 들어 권한 수준이 서로 다른 여러 사용자 그룹이 단일 앱을 사용하려는 경우 개별 배포 그룹을 만들어 앱의 두 가지 버전을 배포할 수 있습니다. 또한 사용자 장치에서 정책 불일치가 발생하지 않도록 사용자 그룹 구성원 자격이 상호 배타적인지 확인해야 합니다.

Apple 볼륨 구매를 사용하여 iOS 응용 프로그램 라이선스를 관리하는 것이 좋을 수도 있습니다. 이 옵션을 사용하려면 Apple 볼륨 구매에 등록하고 XenMobile 콘솔에서 XenMobile 볼륨 구매 설정을 구성해서 볼륨 구매 라이선스로 앱을 배포해야 합니다. 이와 같은 다양한 활용 사례에서는 XenMobile 환경을 구현하기 전에 MAM 전략을 평가하고 계획하는 것이 중요합니다. MAM 전략을 계획하려면 먼저 다음을 정의합니다.

앱 유형 - 지원하려는 서로 다른 유형의 앱을 나열하고 범주화합니다. 예를 들면, 공용, 기본, 모바일 생산성 앱, 웹, 사내, ISV, 앱 등이 있습니다. 또한 서로 다른 장치 플랫폼 (예: iOS 및 Android) 에 대한 앱을 범주화합니다. 이러한 범주화는 각 앱 유형에 필요한 XenMobile 설정을 조정하는 데 유용합니다. 예를 들어, 특정 앱은 래핑할 수 없거나 다른 앱과의 인터랙션을 위해 특수한 API 를 지원하는 Mobile Apps SDK 가 필요할 수 있습니다.

네트워크 요구 사항: 특정 네트워크 액세스 요구 사항 및 적절한 설정으로 앱을 구성합니다. 예를 들어, 특정 앱은 VPN 을 통해 내부 네트워크에 액세스해야 할 수 있습니다. 일부 앱은 DMZ 를 통해 인터넷 액세스를 라우팅해야 할 수 있습니다. 이러한 앱에서 필요한 네트워크에 연결할 수 있으려면 다양한 설정을 적절히 구성해야 합니다. 앱별 네트워크 요구 사항을 정의하면 아키텍처 의사 결정이 조기에 확정되므로 전체 구현 프로세스가 간소화됩니다.

보안 요구 사항: 개별 앱 또는 모든 앱에 적용할 보안 요구 사항을 정의하는 것은 중요합니다. 이러한 계획을 통해 XenMobile Server 설치 시 올바른 구성을 만들 수 있습니다. MDX 정책과 같은 설정은 개별 앱에 적용하더라도 세션 및 인증 설정은 모든 앱에 적용됩니다. 일부 앱에는 배포의 간소화를 위해 사전에 개괄적으로 살펴볼 수 있는 구체적인 암호화, 컨테이너화, 래핑, 암호화, 인증, 지오펜싱, 암호 또는 데이터 공유 요구 사항이 있을 수 있습니다.

배포 요구 사항: 정책 기반 배포를 사용하면 규정을 준수하는 사용자만 게시된 앱을 다운로드하도록 허용할 수 있습니다. 예를 들어, 특정 앱에서 다음 중 하나를 요구하길 원할 수 있습니다.

- 플랫폼 기반 장치 암호화 사용 설정됨
- 장치가 관리됨
- 장치가 최소 운영 체제 버전을 충족함
- 특정 앱이 기업 사용자에게만 제공됨

또한 특정 앱을 회사 사용자에게만 제공할 수도 있습니다. 이러한 요구 사항을 사전에 간략히 정의해야 적절한 배포 규칙 또는 동작을 구성할 수 있습니다.

라이선스 요구 사항: 앱 관련 라이선스 요구 사항을 기록합니다. 이러한 메모는 라이선스 사용 현황을 효과적으로 관리하고, XenMobile 에서 라이선스를 용이하게 하는 특정 기능을 구성할지 여부를 결정하는 데 도움이 됩니다. 예를 들어 무료 또는 유료 iOS 앱을 배포할 경우 Apple 에서는 사용자가 반드시 iTunes 계정에 로그인하도록 하여 해당 앱에 라이선스 요구 사항을 실행합니다. Apple 볼륨 구매에 등록하면 이러한 앱을 XenMobile 을 통해 배포하고 관리할 수 있습니다. 볼륨 구매를 사용하면 사용자가 iTunes 계정에 로그인하지 않고 앱을 다운로드할 수 있습니다. 또한 Samsung SAFE 및 Samsung Knox 같은 도구에는 기능을 배포하기 전에 완료해야 하는 특수한 라이선스 요구 사항이 있습니다.

허용 목록 및 차단 목록 요구 사항: 사용자가 일부 앱을 설치하거나 사용하지 못하도록 할 수 있습니다. 장치를 규정 위반으로 만드는 앱의 허용 목록을 만듭니다. 그런 다음 장치가 규정을 준수하지 않을 때 트리거할 정책을 설정합니다. 또한 사용은 허용되지만 어떤 이유로 차단 목록에 포함되는 앱이 존재할 수 있습니다. 이 경우 허용 목록에 앱을 추가하고, 앱을 사용할 수 있지만 필수는 아님을 나타낼 수 있습니다. 또한 새 장치에 미리 설치된 앱에는 운영 체제의 일부는 아니지만 자주 사용되는 앱이 포함될 수 있습니다. 이러한 앱은 차단 목록 전략과 충돌할 수 있습니다.

앱 사용 사례

한 의료 조직에서 XenMobile 을 배포하여 모바일 앱의 MAM 솔루션으로 사용하려고 합니다. 모바일 앱은 회사 및 BYOD 사용자에게 제공됩니다. IT 부서에서는 다음 앱을 제공하고 관리하기로 결정합니다.

- **모바일 생산성 앱:** Citrix 가 제공하는 iOS 및 Android 앱입니다.
- **Secure Mail:** 전자 메일, 일정 및 연락처 앱입니다.
- **Secure Web:** 인터넷 및 인트라넷 사이트에 대한 액세스를 제공하는 보안 웹 브라우저입니다.
- **Citrix Files:** 공유 데이터에 액세스하고 파일 공유, 동기화 및 편집을 수행하는 앱입니다.

공용 앱 스토어

- **Secure Hub:** XenMobile 과 통신하는 모든 모바일 장치에 사용되는 클라이언트입니다. IT 부서에서는 Secure Hub 클라이언트를 통해 보안 설정, 구성 및 모바일 앱을 모바일 장치에 푸시합니다. Android 및 iOS 장치는 Secure Hub 를 통해 XenMobile 에 등록됩니다.

- **Citrix Receiver:** 사용자가 모바일 장치에서 Citrix Virtual Apps and Desktops 로 호스트된 응용 프로그램을 열 때 사용하는 모바일 앱입니다.
- **GoToMeeting:** 사용자가 다른 컴퓨터 사용자, 고객, 클라이언트 또는 동료와 인터넷을 통해 실시간으로 만날 수 있도록 하는 온라인 모임, 데스크톱 공유 및 비디오 컨퍼런스 클라이언트입니다.
- **Salesforce1:** Salesforce1 을 사용하면 사용자가 모바일 장치에서 Salesforce 에 액세스하고 모든 Salesforce 사용자에게 대한 통합 환경에서 모든 Chatter, CRM, 사용자 지정 앱 및 비즈니스 프로세스를 확인할 수 있습니다.
- **RSA SecurID:** 2 단계 인증을 위한 소프트웨어 기반 토큰입니다.
- **EpicCare** 앱: 환자 차트, 환자 목록, 일정 및 메시징에 대한 액세스를 보호하고 이동 중에 액세스할 수 있도록 하는 의료 기관 종사자용 앱입니다.
 - **Haiku:** iPhone 및 Android 폰용 모바일 앱입니다.
 - **Canto:** iPad 용 모바일 앱입니다.
 - **Rover:** iPhone 및 iPad 용 모바일 앱입니다.

HDX: Citrix Virtual Apps and Desktops 를 통해 제공되는 앱입니다.

- **Epic Hyperspace:** 전자 의료 기록 관리를 위한 Epic 클라이언트 응용 프로그램입니다.

ISV

- **Vocera:** HIPAA 준수 VoIP(Voice-over IP) 및 메시징 모바일 앱으로, iPhone 및 Android 스마트폰을 통해 시간과 장소에 관계없이 Vocera 음성 기술의 이점을 활용할 수 있도록 합니다.

사내 앱

- **HCMail:** 암호화된 메시지를 작성하고, 내부 메일 서버의 주소록을 검색하고, 암호화된 메시지를 전자 메일 클라이언트를 사용하여 연락처로 보내는 데 유용한 앱입니다.

사내 웹 앱

- **PatientRounding:** 여러 부서에서 환자 건강 정보를 기록하는 데 사용되는 웹 응용 프로그램입니다.
- **Outlook Web Access:** 웹 브라우저를 통해 전자 메일에 액세스할 수 있습니다.
- **SharePoint:** 조직 전체의 파일 및 데이터 공유에 사용됩니다.

다음 표에는 MAM 구성에 필요한 기본 정보가 나와 있습니다.

앱 이름	앱 유형	MDX 래핑	iOS	Android
Secure Mail	XenMobile App	아니요 (버전 10.4.1 이상의 경우)	예	예

Secure Web	XenMobile App	아니요 (버전 10.4.1 이상의 경우)	예	예
Citrix Files	XenMobile App	아니요 (버전 10.4.1 이상의 경우)	예	예
Secure Hub	공용 앱	해당 없음	예	예
Citrix Receiver	공용 앱	해당 없음	예	예
GoToMeeting	공용 앱	해당 없음	예	예
Salesforce1	공용 앱	해당 없음	예	예
RSA SecurID	공용 앱	해당 없음	예	예
Epic Haiku	공용 앱	해당 없음	예	예
Epic Canto	공용 앱	해당 없음	예	아니요
Epic Rover	공용 앱	해당 없음	예	아니요
Epic Hyperspace	HDX 앱	해당 없음	예	예
Vocera	ISV 앱	예	예	예
HCMail	사내 앱	예	예	예
PatientRounding	웹 앱	해당 없음	예	예
Outlook Web Access	웹 앱	해당 없음	예	예
SharePoint	웹 앱	해당 없음	예	예

다음 표에는 XenMobile 에서 MAM 정책을 구성할 때 참조할 수 있는 특정 요구 사항이 나와 있습니다.

** 앱 이름 ** **VPN 필요 ** ** 상호 작용 ** ** 상호 작용 ** ** 플랫폼 기반 장치 암호화 **
(컨테이너 외부의 앱과 상호 작용) (컨테이너 외부의 앱에서 상호 작용)
————— — ————— ————— —————
Secure Mail 예 선택적으로 허용 허용 필요 없음
Secure Web 예 허용 허용 필요 없음
Citrix Files 예 허용 허용 필요 없음
Secure Hub 예 해당 없음 해당 없음 해당 없음
Citrix Receiver 예 해당 없음 해당 없음 해당 없음
GoToMeeting 아니요 해당 없음 해당 없음 해당 없음
Salesforce1 아니요 해당 없음 해당 없음 해당 없음
RSA SecurID 아니요 해당 없음 해당 없음 해당 없음
Epic Haiku 예 해당 없음 해당 없음 해당 없음

Epic Canto	예	해당 없음	해당 없음	해당 없음
Epic Rover	예	해당 없음	해당 없음	해당 없음
Epic Hyperspace	예	해당 없음	해당 없음	해당 없음
Vocera	예	차단됨	차단됨	필요 없음
HCMail	예	차단됨	차단됨	필수
PatientRounding	예	해당 없음	해당 없음	필수
Outlook Web Access	예	해당 없음	해당 없음	필요 없음
SharePoint	예	해당 없음	해당 없음	필요 없음

앱 이름	프록시 필터링	라이선싱	지오펜스	Mobile Apps SDK	최소 운영 체제 버전
Secure Mail	필수	해당 없음	선택적으로 필요	해당 없음	적용
Secure Web	필수	해당 없음	필요 없음	해당 없음	적용
Citrix Files	필수	해당 없음	필요 없음	해당 없음	적용
Secure Hub	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Citrix Receiver	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
GoToMeeting	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Salesforce1	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
RSA SecurID	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Haiku	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Canto	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Rover	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Hyperspace	필요 없음	해당 없음	필요 없음	해당 없음	적용되지 않음
Vocera	필수	해당 없음	필수	필수	적용
HCMail	필수	해당 없음	필수	필수	적용
PatientRounding	필수	해당 없음	필요 없음	해당 없음	적용되지 않음
Outlook Web Access	필수	해당 없음	필요 없음	해당 없음	적용되지 않음
SharePoint	필수	해당 없음	필요 없음	해당 없음	적용되지 않음

사용자 커뮤니티

모든 조직은 서로 다른 기능적 역할로 운영되는 다양한 사용자 커뮤니티로 구성됩니다. 이러한 사용자 커뮤니티는 사용자의 모바일 장치를 통해 제공되는 다양한 리소스를 사용하여 서로 다른 작업 및 사무 기능을 수행합니다. 사용자는 관리자가 제공한 모바일 장치를 사용하여 재택 근무를 하거나 원격 사무실에서 근무할 수 있습니다. 또는 개인 모바일 장치를 사용하여 특정 보안 규정 준수 규칙이 적용되는 도구에 액세스할 수 있습니다.

모바일 장치를 사용하는 사용자 커뮤니티가 많아지면 EMM(엔터프라이즈 모빌리티 관리) 을 통해 데이터 유출을 방지하고 보안 제한을 시행해야 합니다. 관리자는 효율적이고 정교한 모바일 기기 관리를 위해 사용자 커뮤니티를 범주화할 수 있습니다. 이렇게 하면 사용자를 리소스에 매핑하는 작업이 간소화되고 올바른 보안 정책을 해당하는 사용자에게 적용할 수 있습니다.

다음 예는 의료 조직의 사용자 커뮤니티를 EMM 용으로 분류하는 방법을 설명합니다.

사용자 커뮤니티 사용 사례

이 예의 의료 조직은 기술 리소스 및 액세스 권한을 다수의 사용자 (예: 네트워크 및 계열사 직원 및 자원 봉사자) 에게 제공합니다. 조직은 EMM 솔루션을 일반 사용자에게만 롤아웃하기로 선택했습니다.

이 조직의 사용자 역할 및 기능은 임상, 비임상 및 계약업체를 포함하는 하위 그룹으로 분류될 수 있습니다. 선택한 사용자 집합에는 회사 모바일 장치가 제공되고 다른 사용자 집합은 개인 장치에서 제한된 회사 리소스에 액세스할 수 있습니다. 적절한 수준의 보안 제한을 적용하고 데이터 유출을 방지하기 위해 조직은 회사 IT 부서를 통해 회사에서 제공하거나 BYOD 인 각 등록 장치를 관리하기로 결정했습니다. 또한 사용자는 단일 장치만 등록할 수 있습니다.

다음 섹션에는 각 하위 그룹의 역할 및 기능에 대한 개요가 나와 있습니다.

임상

- 간호사
- 의사 (진료의, 외과의 등)
- 전문가 (영양사, 마취의, 방사선사, 심장전문의, 종양전문의 등)
- 외부 의사 (직원이 아닌 의사 및 원격 사무실에서 근무하는 근로자)
- 가정 건강 서비스 (환자의 집을 방문하여 의사 서비스를 수행하는 사무실 및 모바일 근로자)
- 연구 전문가 (6 개 연구기관에서 약물 문제에 대한 답을 찾는 임상 연구를 수행하는 지식 근로자 및 고급 사용자)
- 교육 및 훈련 (교육 및 훈련 중인 간호사, 의사 및 전문가)

비임상

- 공유 서비스 (HR, 급여, 미지급금, 공급망 서비스 등 다양한 경영 지원 기능을 수행하는 사무실 근로자)
- 의사 서비스 (관리 서비스, 분석 및 비즈니스 인텔리전스, 비즈니스 시스템, 클라이언트 서비스, 재무, 관리되는 치료 관리, 환자 액세스 솔루션, 매출 주기 솔루션 등 다양한 건강 관리, 관리 서비스 및 비즈니스 프로세스 공급자 솔루션을 수행하는 사무실 근로자)
- 지원 서비스 (복리후생 관리, 임상 통합, 커뮤니케이션, 보상 및 실적 관리, 설비 및 부동산 서비스, HR 기술 시스템, 정보 서비스, 내부 감사 및 프로세스 개선 등 다양한 비임상 기능을 수행하는 사무실 근로자)

- 자선 프로그램 (자선 프로그램 지원과 관련된 다양한 기능을 수행하는 사무실 및 모바일 근로자)

계약업체

- 제조업체 및 공급업체 파트너 (내부에서 근무하거나 사이트 간 VPN 을 통해 원격으로 연결하여 다양한 비임상 지원 기능을 제공)

이 조직에서는 위의 정보를 바탕으로 다음과 같은 엔터티를 만들었습니다. XenMobile 의 배달 그룹에 대한 자세한 내용은 [리소스 배포](#)를 참조하십시오.

Active Directory OU(조직 구성 단위) 및 그룹 **OU = XenMobile 리소스인 경우:**

- OU = 임상, 그룹 =
 - XM 간호사
 - XM 의사
 - XM 전문가
 - XM 외부 의사
 - XM 가정 건강 서비스
 - XM 연구 전문가
 - XM 교육 및 훈련
- OU = 비임상, 그룹 =
 - XM 공유 서비스
 - XM 의사 서비스
 - XM 지원 서비스
 - XM 자선 프로그램

XenMobile 로컬 사용자 및 그룹 그룹 = 계약업체인 경우, 사용자 =

- 공급업체 1
- 공급업체 2
- 공급업체 3
- ...공급업체 10

XenMobile 배달 그룹

- 임상 간호사
- 임상 의사
- 임상 전문가
- 임상 외부 의사

- 임상 가정 건강 서비스
- 임상 연구 전문가
- 임상 교육 및 훈련
- 비임상 공유 서비스
- 비임상 의사 서비스
- 비임상 지원 서비스
- 비임상 자선 프로그램

배달 그룹과 사용자 그룹 매핑

Active Directory 그룹

XM 간호사

XM 의사

XM 전문가

XM 외부 의사

XM 가정 건강 서비스

XM 연구 전문가

XM 교육 및 훈련

XM 공유 서비스

XM 의사 서비스

XM 지원 서비스

XM 자선 프로그램

XenMobile 배달 그룹

임상 간호사

임상 의사

임상 전문가

임상 외부 의사

임상 가정 건강 서비스

임상 연구 전문가

임상 교육 및 훈련

비임상 공유 서비스

비임상 의사 서비스

비임상 지원 서비스

비임상 자선 프로그램

배달 그룹과 리소스 매핑 다음 표에는 이 사용 사례의 각 배달 그룹에 할당되는 리소스가 설명되어 있습니다. 첫 번째 표는 모바일 앱 할당을 보여줍니다. 두 번째 표는 공용 앱, HDX 앱 및 장치 관리 리소스를 보여줍니다.

XenMobile 배달 그룹

Citrix 모바일 앱

공용 모바일 앱

HDX 모바일 앱

임상 간호사

X

임상 의사

임상 전문가

임상 외부 의사	X		
임상 가정 건강 서비스	X		
임상 연구 전문가	X		
임상 교육 및 훈련		X	X
비임상 공유 서비스		X	X
비임상 의사 서비스		X	X
비임상 지원 서비스	X	X	X
비임상 자선 프로그램	X	X	X
계약업체	X	X	X

XenMobile 배달 그룹	공용 앱: RSA SecurID	공용 앱: EpicCare Haiku	HDX 앱: Epic Hy- perspace	암호 정책	장치 제한	자동화된 동 작	WiFi 정책
임상 간호사							X
임상 의사					X		
임상 전문가							
임상 외부 의 사							
임상 가정 건 강 서비스							
임상 연구 전 문가							
임상 교육 및 훈련		X	X				
비임상 공유 서비스		X	X				
비임상 의사 서비스		X	X				
비임상 지원 서비스		X	X				

참고 및 사전 요구 사항

- XenMobile 을 초기 구성하는 동안 모든 사용자라는 이름의 기본 배달 그룹이 만들어집니다. 이 배달 그룹을 사용하는 경우 모든 Active Directory 사용자가 XenMobile 에 등록할 수 있습니다.
 - XenMobile 은 요청이 있을 경우 LDAP 서버에 대한 동적 연결을 사용하여 Active Directory 사용자 및 그룹을 동기화합니다.
 - 사용자가 XenMobile 에서 매핑되지 않은 그룹에 포함되는 경우 해당 사용자는 등록할 수 없습니다. 마찬가지로 사용자가 여러 그룹의 구성원인 경우 XenMobile 은 해당 사용자를 XenMobile 에 매핑된 그룹의 구성원으로만 범주화합니다.
 - MDM 등록을 필수로 규정하려면 XenMobile 콘솔의 서버 속성에서 등록 필요 옵션을 True 로 설정해야 합니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.
 - SQL Server 데이터베이스의 dbo.userlistgrps 아래에서 항목을 삭제하여 XenMobile 배달 그룹에서 사용자 그룹을 삭제할 수 있습니다.
- 주의: 이 동작을 수행하기 전에 XenMobile 및 데이터베이스의 백업을 만드십시오.

XenMobile 의 장치 소유권 정보

사용자 장치의 소유자에 따라 사용자를 그룹화할 수 있습니다. 장치 소유권에는 회사 소유 장치와 BYOD(Bring Your Own Device) 라고 하는 사용자 소유 장치가 포함됩니다. XenMobile 콘솔의 설정 페이지에서 각 리소스 유형의 배포 규칙과 서버 속성을 통해 BYOD 장치의 네트워크 연결 방법을 제어할 수 있습니다. 배포 규칙에 대한 자세한 내용은 XenMobile 설명서에서 [배포 규칙 구성](#)을 참조하십시오. 서버 속성에 대한 자세한 내용은 [서버 속성](#)을 참조하십시오.

앱에 액세스하려는 모든 BYOD 사용자에게 회사의 장치 관리에 대한 동의를 요구할 수 있습니다. 또는 장치 관리를 요구하지 않고 회사 앱에 대한 액세스 권한을 제공할 수 있습니다.

서버 설정 **wsapi.mdm.required.flag** 를 **true** 로 설정하면 XenMobile 이 모든 BYOD 장치를 관리하며 등록을 거부하는 사용자는 앱 액세스가 거부됩니다. 엔터프라이즈 IT 팀이 보안을 강화하는 동시에 사용자에게 긍정적인 사용자 환경을 조성해야 한다면 XenMobile 에서 사용자 장치를 등록할 때 **wsapi.mdm.required.flag** 를 **true** 로 설정하는 방안을 고려하십시오.

wsapi.mdm.required.flag 를 기본 설정인 **false** 로 유지하면 사용자가 등록을 거부할 수 있지만 사용자는 장치에서 XenMobile Store 를 통해 앱에 액세스할 수 있습니다. 장치 관리 없이 엔터프라이즈 앱 관리 만으로 개인 정보 보호, 법적 또는 규제 제한을 준수할 수 있는 환경에서는 **wsapi.mdm.required.flag** 를 **false** 로 설정하는 것이 좋습니다.

XenMobile 을 통해 관리되지 않는 장치의 사용자는 XenMobile Store 를 통해 앱을 설치할 수 있습니다. 선택적 초기화 또는 전체 초기화 같은 장치 수준 제어 대신 앱 정책을 사용하여 앱 액세스를 제어할 수 있습니다. 설정한 값에 따라 정책은 장치에서 주기적으로 XenMobile Server 에 연결하여 앱 실행이 허용되는지 여부를 확인해야 합니다.

보안 요구 사항

XenMobile 환경을 배포할 때의 보안 고려 사항은 그 수가 급속도로 많아질 수 있습니다. 서로 맞물린 항목과 설정이 많습니다. 허용되는 수준의 보호를 시작하고 선택할 수 있도록 지원하기 위해 Citrix 에서는 다음 표에 간략히 설명된 바와 같이 높은 수준의 보안, 더 높은 수준의 보안 및 가장 높은 수준의 보안에 대한 권장 사항을 제공합니다.

배포 모드 선택에는 보안 우려 사항 이상의 요소가 개입됩니다. 또한 배포 모드를 선택하기 전에 사용 사례의 요구 사항을 검토하고 보안 고려 사항을 완화할 수 있는지 여부를 결정해야 합니다.

높음: 이러한 설정을 사용하면 최적의 사용자 환경을 제공하면서 대부분의 조직에 허용되는 기본적인 수준의 보안을 유지할 수 있습니다.

더 높음: 이러한 설정은 보안과 사용 편의성 간에 더 적절한 균형을 잡습니다.

가장 높음: 이러한 권장 사항을 따르면 사용 편의성 및 사용자 채택을 포기하고 높은 수준의 보안을 제공할 수 있습니다.

배포 모드 보안 고려 사항

다음 표에는 각 보안 수준에 대한 배포 모드가 명시되어 있습니다.

높은 수준의 보안	더 높은 수준의 보안	최고 수준의 보안
MAM 또는 MDM	MDM+MAM	MDM+MAM 및 FIPS

참고:

- 사용 사례에 따라 MDM 전용 또는 MAM 전용 배포로 보안 요구 사항을 충족하고 우수한 사용자 환경을 제공할 수 있습니다.
- 앱 컨테이너화, Micro VPN 또는 앱별 정책이 필요하지 않은 경우 MDM 만으로도 충분히 장치를 관리하고 보호할 수 있습니다.
- 앱 컨테이너화만으로도 모든 비즈니스 및 보안 요구 사항을 충족할 수 있는 BYOD 와 같은 사용 사례의 경우 Citrix 에서 는 MAM 전용 모드를 권장합니다.
- 보안 수준이 높은 환경 (및 회사에서 발행한 장치) 에서는 MDM+MAM 모드를 사용하여 제공되는 모든 보안 기능을 활용 하는 것이 좋습니다. MDM 등록을 실행해야 합니다.
- FIPS 옵션은 정부 기관처럼 가장 높은 보안 수준이 요구되는 환경을 위한 옵션입니다.

FIPS 모드를 사용하는 경우 SQL 트래픽을 암호화하도록 SQL Server 를 구성해야 합니다.

Citrix ADC 및 Citrix Gateway 보안 고려 사항

다음 표에는 각 보안 수준에 대한 Citrix ADC 및 Citrix Gateway 권장 사항이 명시되어 있습니다.

높은 수준의 보안	더 높은 수준의 보안	최고 수준의 보안
-----------	-------------	-----------

Citrix ADC 를 사용하는 것이 좋습니다. MAM 및 ENT 의 경우 Citrix Gateway 가 필요하며 MDM 의 경우 권장됩니다.	XenMobile 이 DMZ 에 있는 경우 SSL 브리지가 지원되는 XenMobile 용 표준 Citrix ADC 마법사 구성이 권장됩니다. XenMobile Server 가 내부 네트워크에 있는 경우 보안 표준을 충족해야 한다면 SSL 오프로드를 사용합니다.	SSL 오프로드 및 종단 간 암호화
---	---	---------------------

참고:

- MDM 의 경우 NAT 또는 기존 타사 프록시 및 부하 분산 장치를 통해 XenMobile Server 를 인터넷에 노출할 수 있습니다. 그러나 이 설정을 사용하면 SSL 트래픽이 XenMobile Server 에서 종료되어야 하며 이로 인해 보안 위험이 제기될 수 있습니다.
- 보안 수준이 높은 환경에서 기본 XenMobile 구성의 Citrix ADC 는 일반적으로 보안 요구 사항을 충족하거나 초과합니다.
- 보안 요구 사항이 가장 높은 MDM 환경에서는 Citrix ADC 에서 SSL 을 종료하여 경계에서 트래픽을 검사하고 종단 간 SSL 암호화를 유지할 수 있습니다.
- 필요한 경우 SSL/TLS 암호화를 정의할 수 있습니다.
- SSL FIPS Citrix ADC 하드웨어도 사용할 수 있습니다.
- 자세한 내용은 [Citrix Gateway](#) 및 [Citrix ADC 통합](#)을 참조하십시오.

등록 보안 고려 사항

다음 표에는 각 보안 수준에 대한 Citrix ADC 및 Citrix Gateway 권장 사항이 명시되어 있습니다.

높은 수준의 보안	더 높은 수준의 보안	최고 수준의 보안
Active Directory 그룹 구성원 자격만 사용됩니다. 모든 사용자 배달 그룹은 사용되지 않습니다.	초대 전용 등록 보안 모드를 사용합니다. Active Directory 그룹 구성원 자격만 사용됩니다. 모든 사용자 배달 그룹은 사용되지 않습니다.	장치 ID 에 연결된 등록 보안 모드를 사용합니다. Active Directory 그룹 구성원 자격만 사용됩니다. 모든 사용자 배달 그룹은 사용되지 않습니다.

참고:

- 일반적으로, 미리 정의된 Active Directory 그룹의 사용자로만 등록을 제한하는 것이 좋습니다. 이 설정에서는 기본 제공되는 모든 사용자 배달 그룹을 비활성화해야 합니다.

- 등록 초대를 사용하여 초대받은 사용자 등록을 제한할 수 있습니다. Windows 장치에서는 등록 초대 사용할 수 없습니다.
- OTP(일회용 PIN) 등록 초대 2 단계 인증 솔루션으로 사용하고 사용자가 등록할 수 있는 장치 수를 제어할 수 있습니다. Windows 장치에서는 OTP 초대 사용할 수 없습니다.

장치 암호 보안 고려 사항

다음 표에는 각 보안 수준에 대한 장치 암호 권장 사항이 명시되어 있습니다.

높은 수준의 보안	더 높은 수준의 보안	최고 수준의 보안
권장됩니다. 장치 수준 암호화에는 높은 수준의 보안이 필요합니다. MDM 을 사용하여 적용됩니다. MDX 정책, 정책 준수 장치 동작을 사용하여 MAM 전용에 대한 필수로 높은 보안을 설정할 수 있습니다.	MDM, MDX 정책 또는 둘 다를 사용하여 적용됩니다.	MDM 및 MDX 정책을 사용하여 적용됩니다. MDM 복잡한 암호 정책.

참고:

- Citrix 는 장치 암호의 사용을 권장합니다.
- 장치 암호는 MDM 정책을 통해 적용할 수 있습니다.
- MDX 정책을 사용하여 장치 암호를 관리되는 앱 사용을 위한 요구 사항 중 하나로 만들 수 있습니다. BYOD 사용 사례를 예로 들 수 있습니다.
- MDM 과 MDX 정책 옵션을 결합하여 MDM+MAM 환경의 보안을 강화하는 것이 좋습니다.
- 보안 요구 사항이 가장 높은 환경에서는 복잡한 암호 정책을 구성하고 MDM 을 통해 적용할 수 있습니다. 장치가 암호 정책을 준수하지 않는 경우 관리자에게 알리거나 선택적/전체 장치 초기화를 실행하는 자동화된 동작을 구성할 수 있습니다.

앱

March 15, 2024

EMM(엔터프라이즈 모빌리티 관리) 은 MDM(모바일 기기 관리) 과 MAM(모바일 응용 프로그램 관리) 으로 나뉩니다. MDM 은 모바일 장치의 보안 및 제어에 사용되고 MAM 은 응용 프로그램의 제공 및 관리를 용이하게 합니다. BYOD 채택을 지원하기 위해 보통 XenMobile 과 같은 MAM 솔루션을 구현하여 다음을 지원할 수 있습니다.

- 응용 프로그램 제공
- 소프트웨어 라이선싱

- 구성
- 응용 프로그램 수명 주기 관리

사용자가 MDM 관리도 선택하도록 요구 또는 허용할 수 있습니다.

XenMobile 을 사용하면 특정 MAM 정책 및 VPN 설정을 구성하여 데이터 유출 및 기타 보안 위협을 방지함으로써 이러한 앱을 추가로 보호할 수 있습니다. XenMobile 을 사용하면 조직에서는 솔루션을 다음으로 유연하게 배포할 수 있습니다.

- MAM 전용 환경
- MDM 전용 환경
- MDM 및 MAM 기능을 모두 제공하는 통합 XenMobile 엔터프라이즈 환경

모바일 장치에 앱을 제공하는 것에 더해 XenMobile 은 MDX 기술을 통해 앱을 컨테이너화할 수 있는 기능을 제공합니다. 앱은 점진적인 정책 기반 제어의 대상이 됩니다. ISV(독립 소프트웨어 공급업체) 는 Mobile Apps SDK 를 사용하여 이러한 제어를 적용할 수 있습니다.

기업 환경에서 사용자는 다양한 모바일 앱을 사용하여 업무를 지원합니다. 공용 앱 스토어의 앱, 사내에서 개발한 앱 또는 기본 앱이 여기에 포함될 수 있습니다. XenMobile 은 이러한 앱을 다음과 같이 범주화합니다.

- **공용 앱:** Apple App Store 또는 Google Play 와 같은 공용 앱 스토어에서 무료 또는 유료로 제공되는 앱이 포함됩니다. 조직 외부의 공급업체는 주로 공용 앱 스토어를 통해 앱을 제공합니다. 이 옵션을 사용하는 경우 공급업체의 고객이 인터넷에서 직접 앱을 다운로드할 수 있습니다. 조직의 사용자는 사용자 요구 사항에 따라 수많은 공용 앱을 사용할 수 있습니다. 예를 들어 GoToMeeting, Salesforce 및 EpicCare 앱이 이러한 앱에 포함됩니다.
 - **MAM SDK** 를 사용하는 경우: 앱 공급업체로부터 앱 바이너리를 확보합니다. 그런 다음 MAM SDK 를 앱에 통합합니다.
 - **MDX Toolkit** 을 사용하는 경우: Citrix 는 공용 앱 스토어에서 직접 앱 이진을 다운로드한 다음 MDX Toolkit 을 사용하여 엔터프라이즈 배포용으로 래핑하는 것을 지원하지 않습니다. 타사 응용 프로그램을 래핑하려면 앱 공급업체를 통해 앱 바이너리를 받아야 합니다. 이후에 MDX Toolkit 을 사용하여 바이너리를 래핑할 수 있습니다.
- **사내 앱:** 많은 조직이 사내 개발자를 통해 특정 기능을 제공하는 앱을 만듭니다. 사내 개발자는 조직 내에서 이러한 앱을 독립적으로 개발하고 배포합니다. 경우에 따라 일부 조직에서는 ISV 가 제공하는 앱을 사용하기도 합니다. 이러한 앱을 기본 앱으로 배포하거나 XenMobile 같은 MAM 솔루션을 사용하여 앱을 컨테이너화할 수 있습니다.

예를 들어 의료 조직에서는 의사가 모바일 장치에서 환자 정보를 볼 수 있도록 하는 사내 앱을 만들 수 있습니다. 그러면 조직에서는 다음 중 하나를 사용하여 환자 정보의 보안을 확보하고 환자 데이터베이스에 대한 VPN 액세스를 설정할 수 있습니다.

 - MAM SDK
 - MDX Toolkit
- **웹 및 SaaS 앱:** 내부 네트워크에서 액세스되는 앱 (웹 앱) 또는 공용 네트워크를 통해 액세스되는 앱 (SaaS) 이 포함됩니다. XenMobile 에서는 앱 커넥터 목록을 사용하여 사용자 지정 웹 및 SaaS 앱을 만들 수도 있습니다. 이러한 앱 커넥터를 사용하면 기존 웹 앱에 대한 SSO(Single Sign-on) 를 쉽게 구현할 수 있습니다. 자세한 내용은 [앱 커넥터 유형](#)을 참조하십시오. 예를 들어 Google Apps 에 대한 SAML(Security Assertion Markup Language) 기반 SSO 에는 Google Apps SAML 을 사용할 수 있습니다.

- **모바일 생산성 앱:** 모바일 생산성 앱은 Citrix 에서 개발한 앱으로, XenMobile 라이선스에 포함됩니다. 자세한 내용은 [모바일 생산성 앱 정보](#)를 참조하십시오. 또한 Citrix 는 다른 ISV 에서 Worx App SDK 를 사용하여 개발하는 다른 [비즈니스용 앱](#)을 제공합니다.
- **HDX 앱:** HDX 앱은 Windows 에서 호스트되는 앱으로, StoreFront 를 사용하여 게시합니다. Citrix Virtual Apps and Desktops 와 Citrix Workspace 를 사용한다면 HDX 앱이 등록된 사용자에게 제공됩니다.

XenMobile 을 사용하여 배포하고 관리하려는 모바일 앱의 유형에 따라 기본 구성이 달라질 수 있습니다. 예를 들어, 권한 수준이 다른 여러 사용자 그룹이 단일 앱을 사용할 수 있습니다. 이 경우 개별 배달 그룹을 만들어 동일한 앱의 두 가지 개별 버전을 배포할 수 있습니다. 또한 사용자 장치에서 정책 불일치가 발생하지 않도록 사용자 그룹 구성원 자격이 상호 배타적인지 확인해야 합니다.

Apple 볼륨 구매를 사용하여 iOS 응용 프로그램 라이선스를 관리할 수도 있습니다. 이 옵션을 사용하려면 볼륨 구매 프로그램에 등록하고 XenMobile 콘솔에서 볼륨 구매 설정을 구성해야 합니다. 이 구성을 사용하면 볼륨 구매 라이선스로 앱을 배포할 수 있습니다. 이와 같은 다양한 활용 사례에서는 XenMobile 환경을 구현하기 전에 MAM 전략을 평가하고 계획하는 것이 중요합니다. MAM 전략을 계획하려면 먼저 다음을 정의합니다.

- **앱 유형 -** 지원하려는 서로 다른 유형의 앱을 나열하고 공용, 기본, 웹, 사내, ISV 앱으로 앱을 범주화합니다. 또한 서로 다른 장치 플랫폼 (예: iOS 및 Android) 에 대한 앱을 범주화합니다. 이러한 범주화는 각 앱 유형에 필요한 여러 XenMobile 설정을 조정하는 데 유용합니다. 예를 들어 일부 앱의 경우 Mobile Apps SDK 로 다른 앱과의 상호 작용을 위한 특수 API 를 사용하도록 설정해야 할 수 있습니다.
- **네트워크 요구 사항:** 특정 네트워크 액세스 요구 사항이 있는 앱 설정을 구성합니다. 예를 들어, 특정 앱은 VPN 을 통해 내부 네트워크에 액세스해야 할 수 있습니다. 일부 앱은 DMZ 를 통해 인터넷 액세스를 라우팅해야 할 수 있습니다. 이러한 앱에서 필요한 네트워크에 연결할 수 있으려면 다양한 설정을 적절히 구성해야 합니다. 앱별 네트워크 요구 사항을 정의하면 아키텍처 의사 결정이 조기에 확정되므로 전체 구현 프로세스가 간소화됩니다.
- **보안 요구 사항:** 개별 앱 또는 모든 앱에 적용할 보안 요구 사항을 정의할 수 있습니다.
 - MDX 정책과 같은 설정은 개별 앱에 적용됩니다.
 - 세션 및 인증 설정은 모든 앱에 적용됩니다.
 - 일부 앱에는 구체적인 컨테이너화, MDX, 인증, 지오펜싱, 암호 또는 데이터 공유 요구 사항이 있을 수 있습니다.

사전에 이러한 요구 사항을 개략적으로 설명하면 배포를 간소화할 수 있습니다. Endpoint Management 의 보안에 대한 자세한 내용은 [보안 및 사용자 환경](#)을 참조하십시오.

- **배포 요구 사항:** 정책 기반 배포를 사용하면 규정을 준수하는 사용자만 게시된 앱을 다운로드하도록 허용할 수 있습니다. 예를 들어 특정 앱에서는 장치가 관리되거나 장치가 최소 운영 체제 버전을 충족해야 할 수 있습니다. 또한 특정 앱을 회사 사용자에게만 제공할 수도 있습니다. 이러한 요구 사항을 사전에 간략히 정의해야 적절한 배포 규칙 또는 동작을 구성할 수 있습니다.
- **라이선스 요구 사항:** 앱 관련 라이선스 요구 사항을 기록합니다. 이러한 메모는 라이선스 사용 현황을 효과적으로 관리하고, XenMobile 에서 라이선스를 용이하게 하는 특정 기능을 구성할지 여부를 결정하는 데 도움이 됩니다. 예를 들어 무료 또는 유료 iOS 앱을 배포할 경우 Apple 에서는 해당 앱에 라이선스 요구 사항을 실행합니다. 그 결과, 사용자는 반드시 Apple App Store 계정에 로그인해야 합니다.

그러나, Apple 볼륨 구매에 등록하면 이러한 앱을 XenMobile 로 배포하고 관리할 수 있습니다. 볼륨 구매를 사용하면 사용자가 Apple App Store 계정에 로그인하지 않고 앱을 다운로드할 수 있습니다.

또한 Samsung SAFE, Samsung Knox 같은 일부 플랫폼에는 기능을 배포하기 전에 완료해야 하는 특수한 라이선스 요구 사항이 있습니다.

- **허용 목록 및 차단 목록 요구 사항:** 사용자가 설치 또는 사용하지 않아야 할 앱을 식별할 수 있습니다. 차단 목록을 만들면 규정 위반 이벤트가 정의됩니다. 그런 다음 이러한 이벤트 발생 시 트리거할 정책을 설정할 수 있습니다. 또한 사용은 허용되지만 어떤 이유로 차단 목록에 포함되는 앱이 존재할 수 있습니다. 이 경우 허용 목록에 앱을 추가하고, 앱을 사용할 수 있지만 필수는 아님을 나타낼 수 있습니다. 또한 새 장치에 미리 설치된 앱에는 운영 체제의 일부는 아니지만 자주 사용되는 앱이 포함될 수 있습니다. 이러한 앱은 차단 목록 전략과 충돌할 수 있습니다.

사용 사례

한 의료 조직에서 XenMobile 을 배포하여 모바일 앱의 MAM 솔루션으로 사용하려고 합니다. 모바일 앱은 회사 및 BYOD 사용자에게 제공됩니다. IT 부서에서는 다음 앱을 제공하고 관리하기로 결정합니다.

모바일 생산성 앱: Citrix 가 제공하는 iOS 및 Android 앱입니다. 자세한 내용은 [모바일 생산성 앱](#)을 참조하십시오.

Citrix Secure Hub: XenMobile 과 통신하는 모든 모바일 장치에 사용되는 클라이언트입니다. Secure Hub 로 보안 설정, 구성 및 모바일 앱을 모바일 장치에 푸시합니다. Android 및 iOS 장치는 Secure Hub 를 통해 XenMobile 에 등록됩니다.

Citrix Receiver: 모바일 장치 사용자가 Citrix Virtual Apps 로 호스트된 응용 프로그램을 열 때 사용하는 모바일 앱입니다.

GoToMeeting: 사용자가 다른 컴퓨터 사용자, 고객, 클라이언트 또는 동료와 인터넷을 통해 실시간으로 만날 수 있도록 하는 온라인 모임, 데스크톱 공유 및 비디오 컨퍼런스 클라이언트입니다.

SalesForce1: Salesforce1 을 사용하면 사용자가 모바일 장치에서 Salesforce 에 액세스하고 모든 Salesforce 사용자에 대한 통합 환경에서 모든 Chatter, CRM, 사용자 지정 앱 및 비즈니스 프로세스를 확인할 수 있습니다.

RSA SecurID: 2 단계 인증을 위한 소프트웨어 기반 토큰입니다.

EpicCare 앱: 환자 차트, 환자 목록, 일정 및 메시징에 대한 액세스를 보호하고 이동 중에 액세스할 수 있도록 하는 의료 기관 종사자용 앱입니다.

Haiku: iPhone 및 Android 폰용 모바일 앱입니다.

Canto: iPad 용 모바일 앱입니다.

Rover: iPhone 및 iPad 용 모바일 앱입니다.

HDX: Citrix Virtual Apps 에서 HDX 앱을 제공합니다.

- **Epic Hyperspace:** 전자 의료 기록 관리를 위한 Epic 클라이언트 응용 프로그램입니다.

ISV:

- **Vocera:** HIPAA 준수 VoIP(Voice-over IP) 및 메시징 모바일 앱으로, iPhone 및 Android 스마트폰을 통해 시간과 장소에 관계없이 Vocera 음성 기술의 이점을 활용할 수 있도록 합니다.

사내 앱:

- **HCMail:** 암호화된 메시지를 작성하고, 내부 메일 서버의 주소록을 검색하고, 암호화된 메시지를 전자 메일 클라이언트를 사용하여 연락처로 보내는 데 유용한 앱입니다.

사내 웹 앱:

- **PatientRounding:** 여러 부서에서 환자 건강 정보를 기록하는 데 사용되는 웹 응용 프로그램입니다.
- **Outlook Web Access:** 웹 브라우저를 통해 전자 메일에 액세스할 수 있습니다.
- **SharePoint:** 조직 전체의 파일 및 데이터 공유에 사용됩니다.

다음 표에는 MAM 구성에 필요한 기본 정보가 나와 있습니다.

앱 이름	앱 유형	MAM SDK 통합 또는 MDX 래핑	iOS	Android
Secure Mail	XenMobile App	아니요 (버전 10.4.1 이상의 경우)	예	예
Secure Web	XenMobile App	아니요 (버전 10.4.1 이상의 경우)	예	예
Citrix Files	XenMobile App	아니요 (버전 10.4.1 이상의 경우)	예	예
Secure Hub	공용 앱	해당 없음	예	예
Citrix Receiver	공용 앱	해당 없음	예	예
GoToMeeting	공용 앱	해당 없음	예	예
SalesForce1	공용 앱	해당 없음	예	예
RSA SecurID	공용 앱	해당 없음	예	예
Epic Haiku	공용 앱	해당 없음	예	예
Epic Canto	공용 앱	해당 없음	예	아니요
Epic Rover	공용 앱	해당 없음	예	아니요
Epic Hyperspace	HDX 앱	해당 없음	예	예
Vocera	ISV 앱	예	예	예
HCMail	사내 앱	예	예	예
PatientRounding	웹 앱	해당 없음	예	예

Outlook Web Access	웹 앱	해당 없음	예	예
SharePoint	웹 앱	해당 없음	예	예

다음 표에는 XenMobile 에서 MAM 정책을 구성할 때 참조할 수 있는 특정 요구 사항이 나와 있습니다.

앱 이름	VPN 필요	상호 작용 (컨테이너 외부 앱과 의 상호 작 용)	상호 작용 (컨테이너 외부 앱에 서의 상호 작용)	프록시 필 터링	라이센싱	지오펀스	Mobile Apps SDK	최소 운영 체제 버전
Secure Mail	예	선택적으 로 허용	허용	필수	해당 없음	선택적으 로 필요	해당 없음	적용
Secure Web	예	허용	허용	필수	해당 없음	필요 없음	해당 없음	적용
Citrix Files	예	허용	허용	필수	해당 없음	필요 없음	해당 없음	적용
Secure Hub	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Citrix Receiver	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
GoToMeeting	아니요	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
SalesForce1	아니요	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
RSA SecurID	아니요	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Haiku	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Canto	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Rover	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음
Epic Hyper-space	예	해당 없음	해당 없음	필요 없음	해당 없음	필요 없음	해당 없음	적용되지 않음
Vocera	예	차단됨	차단됨	필수	해당 없음	필수	필수	적용

앱 이름	VPN 필요	상호 작용	상호 작용	프록시 필	라이센싱	지오편스	Mobile Apps SDK	최소 운영 체제 버전
		(컨테이너 외부 앱과 의 상호 작용)	(컨테이너 외부 앱에 서의 상호 작용)					
HCMail	예	차단됨	차단됨	필수	해당 없음	필수	필수	적용
PatientRound- ing	예	해당 없음	해당 없음	필수	해당 없음	필요 없음	해당 없음	적용되지 않음
Outlook Web Access	예	해당 없음	해당 없음	필수	해당 없음	필요 없음	해당 없음	적용되지 않음
SharePoint	예	해당 없음	해당 없음	필수	해당 없음	필요 없음	해당 없음	적용되지 않음

사용자 커뮤니티

March 15, 2024

모든 조직은 서로 다른 기능적 역할로 운영되는 다양한 사용자 커뮤니티로 구성됩니다. 이러한 사용자 커뮤니티는 사용자 모바일 장치를 통해 제공되는 다양한 리소스를 사용하여 서로 다른 작업 및 사무 기능을 수행합니다. 사용자는 관리자가 제공하는 모바일 장치를 사용하거나 개인 모바일 장치를 사용하여 자택 또는 원격 사무실에서 근무할 수 있으며 이러한 장치에서 특정 보안 규정 준 수 규칙이 적용되는 도구에 액세스할 수 있습니다.

모바일 장치를 사용하는 사용자 커뮤니티가 많아지면 EMM(엔터프라이즈 모빌리티 관리) 을 통해 데이터 유출을 방지하고 조직 의 보안 제한을 시행해야 합니다. 관리자는 효율적이고 정교한 모바일 기기 관리를 위해 사용자 커뮤니티를 범주화할 수 있습니다. 이렇게 하면 사용자를 리소스에 매핑하는 작업이 간소화되고 올바른 보안 정책을 해당하는 사용자에게 적용할 수 있습니다.

사용자 커뮤니티를 범주화하는 작업에는 다음과 같은 구성 요소가 사용됩니다.

- Active Directory OU(조직 구성 단위) 및 그룹
특정 Active Directory 보안 그룹에 추가된 사용자는 정책 및 리소스 (예: 앱) 를 받을 수 있습니다. Active Directory 보안 그룹에서 사용자를 제거하면 이전에 허용되었던 XenMobile 리소스에 대한 액세스 권한이 제거됩니다.
- XenMobile 로컬 사용자 및 그룹
Active Directory 에 계정이 없는 사용자는 로컬 XenMobile 사용자로 만들 수 있습니다. 관리자는 로컬 사용자를 Active Directory 사용자와 동일한 방식으로 배달 그룹에 추가하고 리소스를 프로비전할 수 있습니다.
- XenMobile 배달 그룹

권한 수준이 서로 다른 여러 사용자 그룹이 단일 앱을 사용하려는 경우 개별 배달 그룹을 만들어야 할 수 있습니다. 개별 배달 그룹을 사용하면 동일한 앱의 두 가지 개별 버전을 배포할 수 있습니다.

- 배달 그룹과 사용자 그룹 매핑

Active Directory 그룹에 대한 배달 그룹 매핑은 일대일 또는 일대다 방식일 수 있습니다. 기본 정책 및 앱을 일대다 배달 그룹 매핑에 할당합니다. 기능별 정책 및 앱을 일대일 배달 그룹 매핑에 할당합니다.

- 배달 그룹과 앱 리소스 매핑

특정 앱을 각 배달 그룹에 할당합니다.

- 배달 그룹과 MDM 리소스 매핑

앱 및 특정 장치 관리 리소스를 각 배달 그룹에 할당합니다. 예를 들어 앱 유형 (공용, HDX 및 기타), 앱 유형별 특정 앱 및 리소스 (예: 장치 정책 및 자동화된 동작) 를 혼합하여 배달 그룹을 구성합니다.

다음 예는 의료 조직의 사용자 커뮤니티를 EMM 용으로 분류하는 방법을 설명합니다.

사용 사례

이 예의 의료 조직은 기술 리소스 및 액세스 권한을 다수의 사용자 (예: 네트워크 및 계열사 직원 및 자원 봉사자) 에게 제공합니다. 조직은 EMM 솔루션을 일반 사용자에게만 돌아오하기로 선택했습니다.

이 조직의 사용자 역할 및 기능은 임상, 비임상 및 계약업체를 포함하는 하위 그룹으로 나눌 수 있습니다. 선택한 사용자 집합에는 회사 모바일 장치가 제공되고 다른 사용자 집합은 개인 장치 (BYOD) 에서 제한된 회사 리소스에 액세스할 수 있습니다. 적절한 수준의 보안 제한을 적용하고 데이터 유출을 방지하기 위해 조직은 회사 IT 부서를 통해 등록된 각 장치를 관리하기로 결정했습니다. 또한 사용자는 단일 장치만 등록할 수 있습니다.

다음 섹션에는 각 하위 그룹의 역할 및 기능에 대한 개요가 나와 있습니다.

임상

- 간호사
- 의사 (진료의, 외과의 등)
- 전문가 (영양사, 임상병리사, 마취의, 방사선사, 심장전문의, 종양전문의 등)
- 외부 의사 (직원이 아닌 의사 및 원격 사무실에서 근무하는 근로자)
- 가정 건강 서비스 (환자의 집을 방문하여 의사 서비스를 수행하는 사무실 및 모바일 근로자)
- 연구 전문가 (6 개 연구기관에서 약물 문제에 대한 답을 찾는 임상 연구를 수행하는 지식 근로자 및 고급 사용자)
- 교육 및 훈련 (교육 및 훈련 중인 간호사, 의사 및 전문가)

비임상

- 공유 서비스 (HR, 급여, 미지급금, 공급망 서비스 등 다양한 경영 지원 기능을 수행하는 사무실 근로자)

- 의사 서비스 (관리 서비스, 분석 및 비즈니스 인텔리전스, 비즈니스 시스템, 클라이언트 서비스, 재무, 관리되는 치료 관리, 환자 액세스 솔루션, 매출 주기 솔루션 등 다양한 건강 관리, 관리 서비스 및 비즈니스 프로세스 공급자 솔루션을 수행하는 사무실 근로자)
- 지원 서비스 (복리후생 관리, 임상 통합, 커뮤니케이션, 보상 및 실적 관리, 설비 및 부동산 서비스, HR 기술 시스템, 정보 서비스, 내부 감사 및 프로세스 개선 등 다양한 비임상 기능을 수행하는 사무실 근로자)
- 자선 프로그램 (자선 프로그램 지원과 관련된 다양한 기능을 수행하는 사무실 및 모바일 근로자)

계약업체

- 제조업체 및 공급업체 파트너 (내부에서 근무하거나 사이트 간 VPN 을 통해 원격으로 연결하여 다양한 비임상 지원 기능을 제공)

이 조직에서는 위의 정보를 바탕으로 다음과 같은 엔터티를 만들었습니다. XenMobile 의 배달 그룹에 대한 자세한 내용은 XenMobile 제품 설명서에서 [리소스 배포](#)를 참조하십시오.

Active Directory OU(조직 구성 단위) 및 그룹

OU = XenMobile 리소스인 경우

- OU = 임상, 그룹 =
 - XM 간호사
 - XM 의사
 - XM 전문가
 - XM 외부 의사
 - XM 가정 건강 서비스
 - XM 연구 전문가
 - XM 교육 및 훈련
- OU = 비임상, 그룹 =
 - XM 공유 서비스
 - XM 의사 서비스
 - XM 지원 서비스
 - XM 자선 프로그램

XenMobile 로컬 사용자 및 그룹

그룹 = 계약업체인 경우, 사용자 =

- 공급업체 1
- 공급업체 2

- 공급업체 3
- ...공급업체 10

XenMobile 배달 그룹

- 임상 간호사
- 임상 의사
- 임상 전문가
- 임상 외부 의사
- 임상 가정 건강 서비스
- 임상 연구 전문가
- 임상 교육 및 훈련
- 비임상 공유 서비스
- 비임상 의사 서비스
- 비임상 지원 서비스
- 비임상 자선 프로그램

배달 그룹과 사용자 그룹 매핑

Active Directory 그룹

XM 간호사
XM 의사
XM 전문가
XM 외부 의사
XM 가정 건강 서비스
XM 연구 전문가
XM 교육 및 훈련
XM 공유 서비스
XM 의사 서비스
XM 지원 서비스
XM 자선 프로그램

XenMobile 배달 그룹

임상 간호사
임상 의사
임상 전문가
임상 외부 의사
임상 가정 건강 서비스
임상 연구 전문가
임상 교육 및 훈련
비임상 공유 서비스
비임상 의사 서비스
비임상 지원 서비스
비임상 자선 프로그램

배달 그룹과 앱 리소스 매핑

	Secure Mail	Secure Web	ShareFile	Receiver	SalesForce	RSA SecurID	EpicCare Haiku	Epic Hyper-space
임상 간호사	X	X	X					
임상 의사								
임상 전문가								
임상 외부 의사	X		X					
임상 가정 건강 서비스	X		X					
임상 연구 전문가	X		X					
임상 교육 및 훈련							X	X
비임상 공유 서비스							X	X
비임상 의사 서비스							X	X
비임상 지원 서비스	X		X				X	X
비임상 자선 프로그램	X		X				X	X
램 계약업체	X		X	X	X		X	X

배달 그룹과 MDM 리소스 매핑

	MDM: 암호 정책	MDM: 장치 제한	MDM: 자동화된 동작	MDM: WiFi 정책
임상 간호사				X

임상 의사	X
임상 전문가	
임상 외부 의사	
임상 가정 건강 서비스	
임상 연구 전문가	
임상 교육 및 훈련	
비임상 공유 서비스	
비임상 의사 서비스	
비임상 지원 서비스	
비임상 자선 프로그램	
계약업체	X

참고 및 사전 요구 사항

- XenMobile 을 초기 구성하는 동안 모든 사용자라는 이름의 기본 배달 그룹이 만들어집니다. 이 배달 그룹을 사용하는 경우 모든 Active Directory 사용자가 XenMobile 에 등록할 수 있습니다.
- XenMobile 은 요청이 있을 경우 LDAP 서버에 대한 동적 연결을 사용하여 Active Directory 사용자 및 그룹을 동기화합니다.
- 사용자가 XenMobile 에서 매핑되지 않은 그룹에 포함되는 경우 해당 사용자는 등록할 수 없습니다. 마찬가지로 사용자가 여러 그룹의 구성원인 경우 XenMobile 은 해당 사용자를 XenMobile 에 매핑된 그룹의 구성원으로 범주화합니다.
- MDM 등록을 필수로 규정하려면 XenMobile 콘솔의 서버 속성에서 등록 필요 옵션을 **True** 로 설정합니다. 자세한 내용은 [서버 속성](#)을 참조하십시오.
- XenMobile 배달 그룹에서 사용자 그룹을 삭제하려면 SQL Server 데이터베이스의 dbo.userlistgrps 아래에서 항목을 삭제합니다.

주의:

이 동작을 수행하기 전에 XenMobile 및 데이터베이스의 백업을 만드십시오.

XenMobile 의 장치 소유권 정보

사용자 장치의 소유자에 따라 사용자를 그룹화할 수 있습니다. 장치 소유권에는 회사 소유 장치와 BYOD(Bring Your Own Device) 라고 하는 사용자 소유 장치가 포함됩니다. XenMobile 콘솔의 설정 페이지에서 배포 규칙과 XenMobile 서버 속성

을 사용하여 BYOD 장치의 네트워크 연결 방법을 제어할 수 있습니다. 배포 규칙에 대한 자세한 내용은 XenMobile 설명서에서 [리소스 배포](#)를 참조하십시오. 서버 속성에 대한 자세한 내용은 이 안내서에서 [서버 속성](#)을 참조하십시오.

앱에 액세스하려는 모든 BYOD 사용자에게 회사의 장치 관리에 대한 동의를 요구하도록 서버 속성을 설정할 수 있습니다. 또는 장치 관리를 요구하지 않고 회사 앱에 대한 액세스 권한을 제공할 수 있습니다.

서버 속성 **wsapi.mdm.required.flag**를 **true**로 설정하면 XenMobile이 모든 BYOD 장치를 관리하며 등록을 거부하는 사용자는 앱 액세스가 거부됩니다. 엔터프라이즈 IT 팀이 보안을 강화하는 동시에 사용자에게 개선된 등록 경험을 제공해야 한다면 **wsapi.mdm.required.flag**를 **true**로 설정하는 것이 좋습니다.

wsapi.mdm.required.flag를 기본 설정인 **false**로 유지하면 사용자가 등록을 거부할 수 있습니다. 그러나 사용자는 장치에서 XenMobile Store를 통해 앱에 액세스할 수 있습니다. 장치 관리 없이 엔터프라이즈 앱 관리 만으로 개인 정보 보호, 법적 또는 규제 제한을 준수할 수 있는 환경에서는 **wsapi.mdm.required.flag**를 **false**로 설정하는 것이 좋습니다.

XenMobile을 통해 관리되지 않는 장치의 사용자는 XenMobile Store를 통해 앱을 설치할 수 있습니다. 선택적 초기화 또는 전체 초기화 같은 장치 수준 제어 대신 앱 정책을 사용하여 앱 액세스를 제어할 수 있습니다. 일부 정책 설정을 사용하려면 장치에서 주기적으로 XenMobile 서버에 연결하여 앱 실행이 허용되는지 여부를 확인해야 합니다.

전자 메일 전략

January 22, 2021

조직에서 모빌리티 관리 이니셔티브를 시행하는 주된 이유는 모바일 장치에서 전자 메일에 안전하게 액세스할 수 있도록 하기 위해서입니다. XenMobile 설계의 주요 구성 요소 중 하나는 올바른 전자 메일 전략을 결정하는 것입니다. XenMobile은 보안, 사용자 환경 및 통합 요구 사항에 따라 다양한 사용 사례를 수용하는 다수의 옵션을 제공합니다. 이 문서에서는 클라이언트 선택부 터 메일 트래픽 흐름에 이르는 올바른 솔루션을 선택하기 위한 일반적인 설계 의사 결정 프로세스와 고려 사항에 대해 다룹니다.

전자 메일 클라이언트 선택

전체 전자 메일 전략을 설계할 때는 일반적으로 클라이언트를 가장 먼저 선택합니다. Citrix Secure Mail, 특정 모바일 플랫폼 운영 체제에 포함되는 기본 메일 또는 공용 앱 스토어를 통해 제공되는 타사 클라이언트를 포함하는 여러 클라이언트 중에서 선택할 수 있습니다. 요구 사항에 따라 단일 (표준) 클라이언트를 사용하여 사용자 커뮤니티를 지원하거나 클라이언트 조합을 사용해야 할 수 있습니다.

다음 표에는 사용 가능한 여러 클라이언트 옵션에 대한 몇 가지 간략한 설계 고려 사항이 나와 있습니다.

항목	Secure Mail	기본 (예: iOS Mail)	타사 메일
최소 XenMobile 버전	고급	MDM	MDM

구성	MDX 정책을 통해 구성된 Exchange 계정 프로필.	MDM 정책을 통해 구성된 Exchange 계정 프로필. Android 지원은 SAFE/KNOX 및 Android Enterprise 로 제한됩니다. 다른 모든 클라이언트는 타사 클라이언트로 간주됩니다.	일반적으로 사용자가 수동으로 구성해야 합니다.
보안	설계 시부터 보안이 적용되어 가장 높은 수준의 보안을 제공합니다. 데이터 암호화 수준이 추가된 MDX 정책을 사용합니다. Secure Mail 은 MDX 정책을 통해 완벽하게 관리되는 앱입니다. Citrix PIN 을 사용하여 인증 계층을 추가합니다.	공급업체/앱 기능 집합에 따릅니다. 더 높은 수준의 보안을 제공합니다. 장치 암호화 설정을 사용합니다 (MDX 정책을 통한 보안 없음). 앱 액세스에 대해 장치 수준 인증을 사용합니다.	공급업체/앱 기능 집합에 따릅니다. 높은 수준의 보안을 제공합니다.
통합	기본적으로 관리되는 앱 (MDX) 과의 상호 작용을 허용합니다. Citrix Secure Web 을 사용하여 웹 URL 을 엽니다. 파일 저장 및 첨부 시 Citrix Files 를 사용합니다. GoToMeeting 에 직접 참여하고 전화 접속합니다.	기본적으로 관리되지 않는 다른 앱 (비 MDX) 과의 상호 작용만 가능합니다.	기본적으로 관리되지 않는 다른 앱 (비 MDX) 과의 상호 작용만 가능합니다.
배포/라이선스	공용 앱 스토어에서 MDM 을 통해 직접 Secure Mail 을 푸시할 수 있습니다. XenMobile Advanced 및 Enterprise 라이선스에 포함됩니다.	플랫폼 운영 체제에 포함된 클라이언트 앱입니다. 추가 라이선스 요구 사항이 없습니다.	MDM 을 통해 엔터프라이즈 앱으로 푸시하거나 공용 앱 스토어에서 직접 푸시할 수 있습니다. 앱 공급업체에 따라 연결된 라이선스 모델/비용이 적용됩니다.
지원	클라이언트 및 EMM 솔루션을 단일 공급업체 (Citrix) 가 지원합니다. Secure Hub/앱 디버그 로깅 기능에 지원 연락처가 포함되어 있습니다. 하나의 클라이언트만 지원하면 됩니다.	공급업체 (Apple/Google) 가 정의한 지원을 사용할 수 있습니다. 장치 플랫폼에 따라 여러 클라이언트를 지원해야 할 수 있습니다.	공급업체가 정의한 지원을 사용할 수 있습니다. 모든 관리되는 장치 플랫폼에서 타사 클라이언트가 지원된다고 가정하면 하나의 클라이언트만 지원하면 됩니다.

메일 트래픽 흐름 및 필터링 고려 사항

이 섹션에서는 XenMobile의 컨텍스트에서 메일 (ActiveSync) 트래픽의 흐름과 관련된 세 가지 주요 시나리오 및 설계 고려 사항에 대해 설명합니다.

시나리오 1: 공개된 **Exchange**

일반적으로 Exchange ActiveSync 서비스를 인터넷에 공개하는 외부 클라이언트를 지원하는 환경입니다. 모바일 ActiveSync 클라이언트는 이 외부 대상 경로를 통해 역방향 프록시 (예: Citrix ADC) 또는 에지 서버를 사용하여 연결합니다. 이 옵션은 기본 또는 타사 메일 클라이언트를 사용하려는 경우 필요하며 이 시나리오에서 이러한 클라이언트가 주로 사용될 수 있도록 합니다. 일반적인 사례는 아니지만 이 시나리오에서 Secure Mail 클라이언트를 사용할 수도 있습니다. 이 경우 앱의 MDX 정책 및 관리를 통해 제공되는 보안 기능을 활용할 수 있습니다.

시나리오 2: **Citrix ADC**를 통해 터널링됨 (**Micro VPN** 및 **STA**)

Secure Mail 클라이언트를 사용하는 경우 Micro VPN 기능을 사용하려면 이 시나리오가 기본적으로 적용됩니다. 이 경우 Secure Mail 클라이언트는 Citrix Gateway를 통해 ActiveSync에 대한 보안 연결을 설정합니다. 기본적으로, Secure Mail은 내부 네트워크에서 ActiveSync에 직접 연결하는 클라이언트로 간주될 수 있습니다. Citrix 고객은 Secure Mail을 모바일 ActiveSync 클라이언트로 표준화하는 경우가 많습니다. 이러한 표준화는 첫 번째 시나리오에 설명된 것과 같이 공개된 Exchange Server에서 ActiveSync 서비스가 인터넷에 공개되는 것을 방지하기 위해 수행됩니다.

MAM SDK 사용 또는 MDX 래핑 앱에서만 마이크로 VPN 기능을 사용할 수 있습니다. MDX 래핑을 사용하는 경우 이 시나리오는 기본 클라이언트에 적용되지 않습니다. 타사 클라이언트를 MDX Toolkit으로 래핑할 수도 있지만 일반적인 사례는 아닙니다. 장치 수준 VPN 클라이언트를 사용하여 기본 또는 타사 클라이언트에 대한 터널링된 액세스를 허용하려는 솔루션은 과정이 복잡하고 실행 가능하지 않은 것으로 검증되었습니다.

시나리오 3: 클라우드에서 호스트되는 **Exchange** 서비스

클라우드에서 호스트되는 Exchange 서비스 (예: Microsoft Office 365)의 인기가 높아지고 있습니다. XenMobile의 컨텍스트에서 이 시나리오는 첫 번째 시나리오와 동일하게 다뤄질 수 있습니다. ActiveSync 서비스가 인터넷에 공개되기 때문입니다. 이 경우 클라우드 서비스 공급자 요구 사항에 따라 클라이언트를 선택해야 합니다. 일반적으로 대부분의 ActiveSync 클라이언트 (예: Secure Mail) 및 다른 기본 또는 타사 클라이언트를 선택할 수 있습니다.

XenMobile은 이 시나리오의 세 가지 영역에서 더 많은 가치를 제공합니다.

- Secure Mail의 MDX 정책 및 앱 관리를 사용하는 클라이언트
- 지원되는 기본 이메일 클라이언트에서 MDM 정책을 사용하여 클라이언트 구성
- Exchange ActiveSync용 Endpoint Management 커넥터를 사용한 ActiveSync 필터링 옵션

메일 트래픽 필터링 고려 사항

인터넷에 공개되는 대부분의 서비스와 마찬가지로, 경로를 보호하고 허가된 액세스에 대한 필터링을 제공해야 합니다. XenMobile 솔루션에는 기본 및 타사 클라이언트를 위한 ActiveSync 필터링 기능을 제공하도록 설계된 두 가지 구성 요소가 포함되어 있습니다. Exchange ActiveSync 용 Citrix Gateway 커넥터와 Exchange ActiveSync 용 Endpoint Management 커넥터입니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터

Exchange ActiveSync 용 Citrix Gateway 커넥터는 Citrix ADC 를 ActiveSync 트래픽의 프록시로 사용하여 경계에서 ActiveSync 필터링을 제공합니다. 필터링 구성 요소가 메일 트래픽 흐름의 경로에 배치되므로 메일이 환경에 들어오거나 환경에서 나갈 때 트래픽을 가로챍니다. Exchange ActiveSync 용 Citrix Gateway 커넥터는 Citrix ADC 와 XenMobile Server 의 중간자 역할을 합니다. 장치가 Citrix ADC 의 ActiveSync 가상 서버를 통해 Exchange 와 통신하면 Citrix ADC 가 Exchange ActiveSync 용 커넥터 서비스에 대한 HTTP 콜아웃을 수행합니다. 그러면 이 서비스가 XenMobile 을 통해 장치 상태를 확인합니다. 장치 상태에 따라 Exchange ActiveSync 용 커넥터는 연결 허용 또는 거부에 대한 회신을 Citrix ADC 로 보냅니다. 사용자, 에이전트 및 장치 유형 또는 ID 에 따라 액세스를 필터링하는 정적 규칙을 구성할 수도 있습니다.

이 설정을 사용하면 추가 보안 계층을 통해 Exchange ActiveSync 서비스를 인터넷에 공개하여 허가되지 않은 액세스를 방지할 수 있습니다. 설계 고려 사항은 다음과 같습니다.

- **Windows Server:** Exchange ActiveSync 용 커넥터 구성 요소를 사용하려면 Windows Server 가 필요합니다.
- **필터링 규칙 설정:** Exchange ActiveSync 용 커넥터는 사용자 정보가 아닌 장치 상태 및 정보를 바탕으로 필터링하도록 설계되었습니다. 사용자 ID 로 필터링하는 정적 규칙을 구성할 수는 있지만 예를 들어 Active Directory 그룹 구성원 자격으로 필터링하는 옵션은 없습니다. Active Directory 그룹 필터링에 대한 요구 사항이 있는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터를 대신 사용할 수 있습니다.
- **Citrix ADC 확장성:** Citrix ADC 를 통한 ActiveSync 트래픽 프록시에 대한 요구 사항이 있는 경우 Citrix ADC 인스턴스 크기를 올바르게 조정하여 모든 ActiveSync SSL 연결의 추가된 작업 부하를 지원하는 것이 중요합니다.
- **Citrix ADC 통합 캐싱:** Citrix ADC 의 Exchange ActiveSync 용 커넥터 구성은 통합 캐싱 기능을 사용하여 Exchange ActiveSync 용 커넥터의 응답을 캐싱합니다. 이 구성으로 인해 Citrix ADC 는 지정된 세션의 모든 ActiveSync 트랜잭션에 대한 요청을 Exchange ActiveSync 용 Citrix Gateway 커넥터에 전송하지 않아도 됩니다. 이 구성은 충분한 성능 및 확장성에 대해서도 중요한 역할을 합니다. 통합 캐싱은 Citrix ADC Platinum Edition 을 통해 사용하거나 Enterprise Edition 의 기능에 대한 라이선스를 개별적으로 취득할 수 있습니다.
- **사용자 지정 필터링 정책:** 사용자 지정 Citrix ADC 정책을 만들어 표준의 기본 모바일 클라이언트 외의 특정 ActiveSync 클라이언트를 제한해야 할 수 있습니다. 이 구성을 사용하려면 ActiveSync HTTP 요청 및 Citrix ADC 응답자 정책 만들기에 대한 지식이 있어야 합니다.
- **Secure Mail 클라이언트:** Secure Mail 에는 Micro VPN 기능이 있습니다. 이 기능을 사용하면 경계에서 필터링을 수행하지 않아도 됩니다. Secure Mail 클라이언트는 Citrix Gateway 를 통해 연결되는 경우 일반적으로 내부 (신뢰할 수 있는) ActiveSync 클라이언트로 여겨집니다. 기본 및 타사 (Exchange ActiveSync 용 커넥터 포함) 클라이언트와 Secure Mail 클라이언트를 모두 지원해야 합니다. Secure Mail 트래픽은 Exchange ActiveSync 용 커넥터에 사용된 Citrix ADC 가상 서버를 통하지 않는 것이 좋습니다. 이 트래픽이 DNS 를 통해 흐르도록 하고 Exchange ActiveSync 용 커넥터 정책이 Secure Mail 클라이언트에 영향을 미치지 않도록 할 수 있습니다.

XenMobile 배포의 Exchange ActiveSync 용 Citrix Gateway 커넥터 다이어그램은 [온-프레미스 배포용 참조 아키텍처](#)를 참조하십시오.

Exchange ActiveSync 용 Endpoint Management 커넥터

Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange 서비스 수준에서 ActiveSync 필터링을 제공하는 XenMobile 구성 요소입니다. 따라서 메일이 XenMobile 환경에 들어올 때가 아니라 Exchange 서비스에 도달할 때만 필터링이 한 번 수행됩니다. Mail Manager 은 PowerShell 을 사용하여 Exchange ActiveSync 에 장치 파트너 관계 정보를 쿼리하고 장치 격리 동작을 통해 액세스를 제어합니다. 이러한 동작은 Exchange ActiveSync 용 Endpoint Management 커넥터 규칙 기준에 따라 장치를 격리하거나 격리 해제합니다. Exchange ActiveSync 용 Citrix Gateway 커넥터와 마찬가지로 Exchange ActiveSync 용 Endpoint Management 커넥터는 XenMobile 을 통해 장치 상태를 확인하여 장치 규정 준수에 따라 액세스를 필터링합니다. 장치 유형 또는 ID, 에이전트 버전 및 Active Directory 그룹 구성원 자격에 따라 액세스를 필터링하는 정적 규칙을 구성할 수도 있습니다.

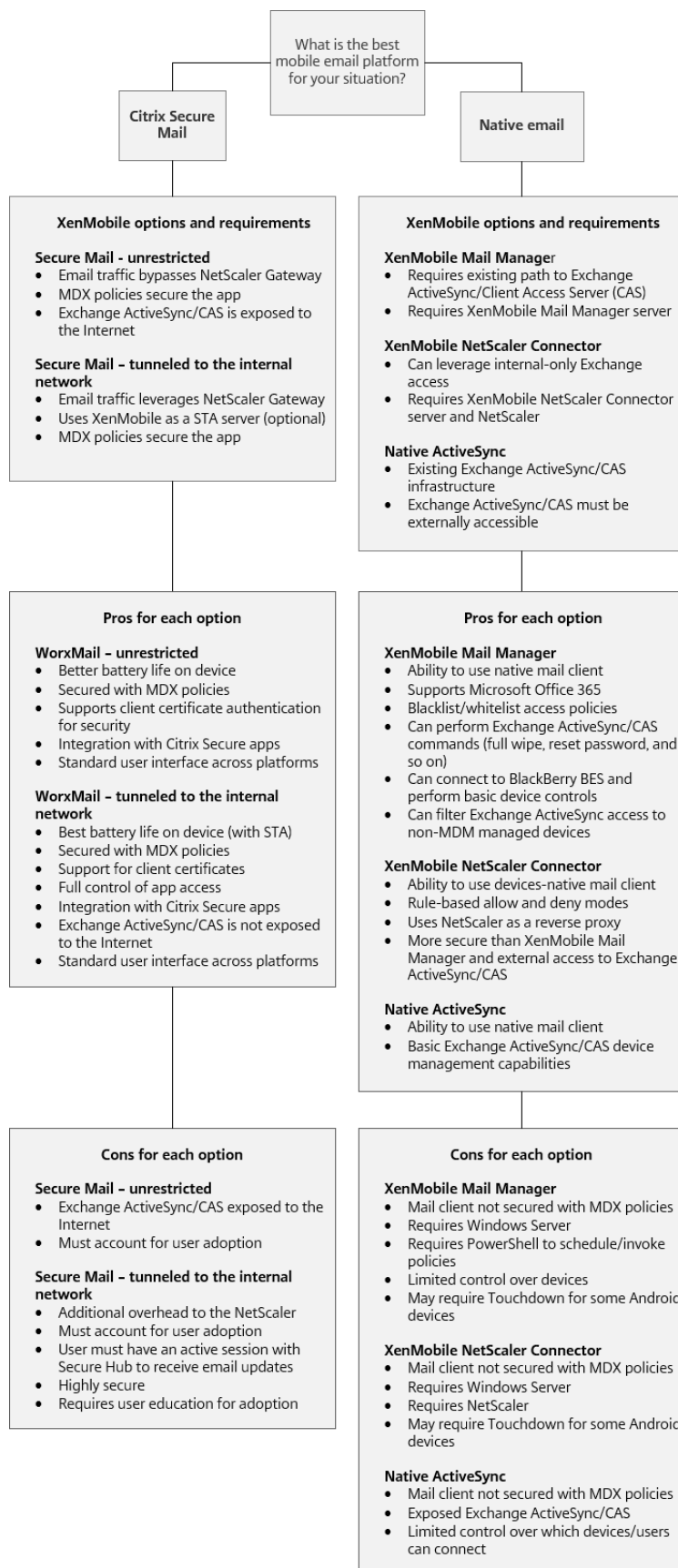
이 솔루션에는 Citrix ADC 의 사용이 필요하지 않습니다. 기존 ActiveSync 트래픽의 라우팅을 변경하지 않고 Exchange ActiveSync 용 Endpoint Management 커넥터를 배포할 수 있습니다. 설계 고려 사항은 다음과 같습니다.

- Windows Server: Exchange ActiveSync 용 Endpoint Management 커넥터 구성 요소를 사용하려면 Windows Server 를 배포해야 합니다.
- 필터링 규칙 설정: Exchange ActiveSync 용 Citrix Gateway 커넥터와 마찬가지로 Exchange ActiveSync 용 Endpoint Management 커넥터에는 장치 상태를 평가하는 필터링 규칙이 포함됩니다. 또한 Exchange ActiveSync 용 Endpoint Management 커넥터는 Active Directory 그룹 구성원 자격을 기준으로 필터링하는 정적 규칙을 지원합니다.
- Exchange 통합: Exchange ActiveSync 용 Endpoint Management 커넥터는 ActiveSync 역할을 호스팅하는 Exchange CAS(클라이언트 액세스 서버)에 직접 액세스하고 장치 격리 동작을 제어할 수 있어야 합니다. 이 요구 사항은 환경 아키텍처 및 보안 상태에 따라 문제가 될 수 있습니다. 따라서 이 기술 요구 사항을 사전에 평가하는 것이 중요합니다.
- 다른 ActiveSync 클라이언트: Exchange ActiveSync 용 Endpoint Management 커넥터는 ActiveSync 서비스 수준에서 필터링을 수행하므로 XenMobile 환경 외의 다른 ActiveSync 클라이언트를 고려해야 합니다. Exchange ActiveSync 용 Endpoint Management 커넥터 정적 규칙을 구성하면 다른 ActiveSync 클라이언트에 의도하지 않은 영향이 발생하는 것을 방지할 수 있습니다.
- 확장된 Exchange 기능: Exchange ActiveSync 와 Exchange ActiveSync 용 Endpoint Management 커넥터를 직접 통합하면 XenMobile 이 모바일 장치에서 Exchange ActiveSync 초기화를 수행할 수 있습니다. 또한 XenMobile 은 Exchange ActiveSync 용 Endpoint Management 커넥터를 통해 Blackberry 장치에 대한 정보에 액세스하고 다른 제어 작업을 수행할 수 있습니다.

XenMobile 배포의 Exchange ActiveSync 용 Endpoint Management 커넥터 다이어그램은 [온-프레미스 배포용 참조 아키텍처](#)를 참조하십시오.

전자 메일 플랫폼 의사 결정 트리

다음 그림은 XenMobile 배포에서 기본 전자 메일과 Secure Mail 솔루션을 사용할 때의 장점과 단점을 이해하는 데 도움이 됩니다. 연결된 XenMobile 옵션과 서버, 네트워크 및 데이터베이스 액세스 지원을 위한 요구 사항을 고려하여 솔루션을 선택할 수 있습니다. 장점 및 단점에는 보안, 정책 및 사용자 인터페이스 고려 사항에 대한 세부 정보가 포함됩니다.



XenMobile 통합

November 27, 2023

이 문서에서는 XenMobile 과 기존 네트워크 및 솔루션의 통합을 계획할 때 고려해야 할 사항에 대해 다룹니다. 예를 들어 Virtual Apps and Desktops 에 Citrix ADC 를 사용 중인 경우 다음을 고려해야 할 수 있습니다.

- 기존 Citrix ADC 인스턴스를 사용해야 합니까? 새로운 전용 인스턴스를 사용해야 합니까?
- StoreFront 를 사용하여 게시된 HDX 앱을 XenMobile 과 통합하려고 합니까?
- XenMobile 에서 Citrix Files 를 사용할 계획입니까?
- XenMobile 에 통합하려는 네트워크 액세스 제어 솔루션이 있습니까?
- 네트워크의 모든 아웃바운드 트래픽에 대한 웹 프록시를 배포합니까?

Citrix ADC 및 Citrix Gateway

XenMobile ENT 및 MAM 모드에는 Citrix Gateway 가 필요합니다. Citrix Gateway 는 모든 회사 리소스에 액세스할 수 있는 Micro VPN 경로를 제공하며 강력한 다중 단계 인증을 지원합니다. 다음의 경우 모든 XenMobile Server 장치 모드에 Citrix ADC 부하 분산이 필요합니다.

- 다수의 XenMobile Server 가 있는 경우
- XenMobile Server 가 DMZ 또는 내부 네트워크에 있는 경우 (트래픽이 장치에서 Citrix ADC 를 거쳐 XenMobile 로 흐르는 경우).

기존 Citrix ADC 인스턴스를 사용하거나 XenMobile 전용의 새 인스턴스를 설정할 수 있습니다. 다음 섹션에서는 기존 Citrix ADC 인스턴스 또는 새로운 전용 Citrix ADC 인스턴스를 사용할 때의 장점과 단점을 살펴봅니다.

XenMobile 용으로 만든 Citrix Gateway VIP 를 Citrix ADC MPX 와 공유

장점:

- 모든 Citrix 원격 연결 (Citrix Virtual Apps and Desktops, 전체 VPN 및 클라이언트 없는 VPN) 에 공통된 Citrix ADC 인스턴스를 사용합니다.
- 인증서 인증 및 DNS, LDAP 및 NTP 같은 서비스 액세스 시 기존 Citrix ADC 구성을 사용합니다.
- 단일 Citrix ADC 플랫폼 라이선스를 사용합니다.

단점:

- 동일한 Citrix ADC 에서 두 개의 다른 사용 사례를 처리하는 경우 확장을 계획하기가 더 어렵습니다.
- 가끔, Citrix Virtual Apps and Desktops 사용 사례에 대한 특정 Citrix ADC 버전이 필요할 수 있습니다. 이러한 버전에는 XenMobile 의 알려진 문제가 포함될 수 있습니다. 또는 XenMobile 에 Citrix ADC 버전의 알려진 문제가 포함될 수 있습니다.

- Citrix Gateway 가 있는 경우 XenMobile 에 대한 Citrix ADC 구성을 만들 때 XenMobile 용 Citrix ADC 마법사를 두 번 실행할 수 없습니다.
- Citrix Gateway 11.1 이상에서 Platinum 라이선스를 사용하는 경우를 제외하고 Citrix ADC 에 설치되고 VPN 연결에 필요한 사용자 액세스 라이선스가 풀링됩니다. 모든 Citrix ADC 가상 서버에서 이러한 라이선스를 사용할 수 있으므로 XenMobile 외의 다른 서비스에 의해 라이선스가 소비될 수 있습니다.

전용 **Citrix ADC VPX/MPX** 인스턴스

장점:

Citrix ADC 의 전용 인스턴스를 사용하는 것이 좋습니다.

- 확장을 계획하기가 쉽고 XenMobile 트래픽이 이미 리소스 제약이 있을 수 있는 Citrix ADC 인스턴스와 분리됩니다.
- XenMobile 과 Citrix Virtual Apps and Desktops 에서 서로 다른 Citrix ADC 소프트웨어 버전을 사용해야 하는 경우 문제가 방지됩니다. XenMobile 과 호환되는 최신 Citrix ADC 버전 및 빌드를 사용하는 것이 일반적으로 권장됩니다.
- XenMobile 용 기본 제공 Citrix ADC 마법사를 통해 XenMobile 에서 Citrix ADC 를 구성할 수 있습니다.
- 가상 서비스와 물리적 서비스가 분리됩니다.
- Citrix Gateway 11.1 이상에서 Platinum 라이선스를 사용하는 경우를 제외하고 XenMobile 에 필요한 사용자 라이선스가 Citrix ADC 의 XenMobile 서비스에만 제공됩니다.

단점:

- Citrix ADC 에서 XenMobile 구성을 지원하는 추가 서비스를 설정해야 합니다.
- 다른 Citrix ADC 플랫폼 라이선스가 필요합니다. 각 Citrix ADC 인스턴스에 Citrix Gateway 라이선스가 있어야 합니다.

Citrix ADC 및 Citrix Gateway 를 XenMobile 서버 모드와 통합할 때의 고려 사항에 대한 자세한 내용은 [Citrix ADC 와 Citrix Gateway 의 통합](#)을 참조하십시오.

StoreFront

Citrix Virtual Apps and Desktops 환경이 있는 경우 StoreFront 를 사용하여 HDX 응용 프로그램을 XenMobile 과 통합할 수 있습니다. HDX 앱을 XenMobile 과 통합하는 경우:

- XenMobile 에 등록된 사용자가 앱을 사용할 수 있습니다.
- XenMobile Store 에 다른 모바일 앱과 함께 앱이 표시됩니다.
- XenMobile 이 StoreFront 의 레거시 PNAgent(서비스) 사이트를 사용합니다.
- Citrix Receiver 가 장치에 설치된 경우 HDX 앱이 Citrix Receiver 사용을 시작합니다.

StoreFront 에는 StoreFront 인스턴스당 하나의 서비스 사이트를 사용해야 하는 제한이 있습니다. 여러 저장소가 있고 이러한 저장소를 다른 프로덕션 사용과 구분해야 하는 경우 XenMobile 에 사용할 새 StoreFront 인스턴스 및 서비스 사이트를 만드는 것이 좋습니다.

고려 사항은 다음과 같습니다.

- StoreFront에 대한 특정 인증 요구 사항이 있습니까? StoreFront 서비스 사이트에 로그인하려면 Active Directory 자격 증명이 필요합니다. 인증서 기반 인증만 사용하는 고객은 동일한 Citrix Gateway를 사용하는 XenMobile을 통해 응용 프로그램을 열거할 수 없습니다.
- 동일한 저장소를 사용합니까? 새 저장소를 만듭니까?
- 동일한 StoreFront 서버를 사용합니까? 새 StoreFront 서버를 사용합니까?

다음 섹션에서는 Receiver 및 모바일 생산성 앱에 대해 개별 StoreFront 또는 결합된 StoreFront를 사용할 때의 장점과 단점을 살펴봅니다.

기존 **StoreFront** 인스턴스를 **XenMobile** 서버와 통합

장점:

- 동일한 저장소: 동일한 Citrix ADC VIP를 HDX 액세스에 사용하는 것으로 가정할 경우 XenMobile용 StoreFront를 추가로 구성할 필요가 없습니다. 동일한 저장소를 사용하고 Receiver 액세스를 새 Citrix ADC VIP로 연결한다고 가정할 수 있습니다. 이 경우 적절한 Citrix Gateway 구성을 StoreFront에 추가해야 합니다.
- 동일한 StoreFront 서버: 기존 StoreFront 설치 및 구성을 사용합니다.

단점:

- 동일한 저장소: Virtual Apps and Desktops 작업 부하를 지원하기 위해 StoreFront를 재구성할 경우 XenMobile에도 부정적인 영향이 발생할 수 있습니다.
- 동일한 StoreFront 서버: 대규모 환경의 경우 XenMobile에서 앱을 열거하고 시작할 때 PNAgent를 사용하므로 추가 부하가 발생할 수 있습니다.

XenMobile 서버 통합에 새로운 전용 **StoreFront** 인스턴스 사용

장점:

- 새 저장소: XenMobile의 StoreFront 저장소에 대한 구성 변경이 기존 Virtual Apps and Desktops 작업 부하에 영향을 미치지 않습니다.
- 새 StoreFront 서버: 서버 구성 변경이 Virtual Apps and Desktops 워크플로에 영향을 미치지 않습니다. 또한 XenMobile에서 PNAgent를 사용하여 앱을 열거하고 시작할 때 발생하는 부하 외의 부하가 확장성에 영향을 미치지 않습니다.

단점:

- 새 저장소: StoreFront 저장소 구성.
- 새 StoreFront 서버: 새 StoreFront 설치 및 구성이 필요합니다.

자세한 내용은 XenMobile 설명서에서 [Citrix Secure Hub를 통한 Virtual Apps and Desktops](#)를 참조하십시오.

ShareFile 및 Citrix Files

사용자는 Citrix Files 를 사용하여 모든 장치의 모든 데이터에 액세스하고 동기화할 수 있습니다. Citrix Files 를 사용하면 조직 내부 및 외부 사용자와 안전하게 데이터를 공유할 수 있습니다. ShareFile 을 XenMobile Advanced Edition 또는 Enterprise Edition 과 통합하면 XenMobile 을 통해 Citrix Files 에 다음을 제공할 수 있습니다.

- XenMobile App 사용자의 SSO(Single Sign-on) 인증.
- Active Directory 기반 사용자 계정 프로비전.
- 포괄적인 액세스 제어 정책.

모바일 사용자는 모든 Enterprise 계정 기능 집합을 사용할 수 있습니다.

또는 StorageZone 커넥터만 통합하도록 XenMobile 을 구성할 수 있습니다. Citrix Files 는 StorageZone 커넥터를 통해 다음에 대한 액세스를 제공합니다.

- 문서 및 폴더
- 네트워크 파일 공유
- SharePoint 사이트: 사이트 모음 및 문서 라이브러리.

연결된 파일 공유에는 Citrix Virtual Apps and Desktops 환경에 사용된 것과 동일한 네트워크 홈 드라이브가 포함될 수 있습니다. XenMobile 콘솔을 사용하여 Citrix Files 또는 StorageZones 커넥터와의 통합을 구성할 수 있습니다. 자세한 내용은 [XenMobile](#) 에서 [Citrix Files 사용](#) 을 참조하십시오.

다음 섹션에서는 Citrix Files 에 대한 설계 의사 결정을 내릴 때 고려할 수 있는 질문을 살펴봅니다.

Citrix Files 또는 StorageZone 커넥터만 통합

질문:

- Citrix 에서 관리하는 StorageZones 에 데이터를 저장해야 합니까?
- 사용자에게 파일 공유 및 동기화 기능을 제공하려고 합니까?
- 사용자가 Citrix Files 웹 사이트의 파일에 액세스할 수 있어야 합니까? 또는 모바일 장치에서 Office 365 콘텐츠 및 개인용 클라우드 커넥터에 액세스해야 합니까?

설계 의사 결정:

- 위 질문 중 하나 이상에 대한 답이 “예” 인 경우 Citrix Files 와 통합합니다.
- StorageZone 커넥터만 통합하는 경우 SharePoint 사이트 및 네트워크 파일 공유 등의 기존 온-프레미스 스토리지 저장소에 대한 보안 모바일 액세스를 iOS 사용자에게 제공할 수 있습니다. 이 구성에서는 ShareFile 하위 도메인을 설정하거나, Citrix Files 에 사용자를 프로비전하거나, Citrix Files 데이터를 호스팅하지 않습니다. StorageZones 커넥터를 XenMobile 과 함께 사용하면 사용자 정보가 회사 네트워크 밖으로 유출되지 않도록 하는 보안 제한 사항을 준수할 수 있습니다.

StorageZones Controller 서버 위치

질문:

- 온-프레미스 스토리지 또는 기능 (예: StorageZone 커넥터) 이 필요합니까?
- Citrix Files 의 온-프레미스 기능을 사용하는 경우 StorageZones Controller 는 네트워크의 어디에 위치합니까?

설계 의사 결정:

- StorageZones Controller 서버의 위치 (Citrix Files 클라우드, 온-프레미스 단일 테넌트 스토리지 시스템 또는 지원되는 타사 클라우드 스토리지) 를 결정합니다.
- StorageZones Controller 를 사용하려면 인터넷 액세스를 통해 Citrix Files 제어부와 통신해야 합니다. 직접 액세스, NAT/PAT 구성 또는 프록시 구성 등 다양한 방법으로 연결할 수 있습니다.

StorageZone 커넥터

질문:

- CIFS 공유 경로는 무엇입니까?
- SharePoint URL 은 무엇입니까?

설계 의사 결정:

- 온-프레미스 StorageZones Controller 에서 이러한 위치에 액세스해야 하는지 여부를 결정합니다.
- StorageZone 커넥터에서 파일 저장소, CIFS 공유 및 SharePoint 같은 내부 리소스와 통신해야 하므로 StorageZones Controller 를 내부 네트워크의 DMZ 방화벽 뒤와 Citrix ADC 앞에 배치하는 것이 좋습니다.

SAML 과 **XenMobile Enterprise** 통합

질문:

- Citrix Files 에 Active Directory 인증이 필요합니까?
- XenMobile 용 Citrix Files 앱을 처음으로 사용할 때 SSO 가 필요합니까?
- 현재 환경에 표준 IdP 가 있습니까?
- SAML 을 사용해야 하는 도메인은 몇 개입니까?
- Active Directory 사용자에게 전자 메일 별칭이 여러 개입니까?
- Active Directory 도메인 마이그레이션이 진행 중이거나 곧 예약되어 있습니까?

설계 의사 결정:

XenMobile Enterprise 환경에서는 SAML 을 Citrix Files 의 인증 메커니즘으로 사용할 수 있습니다. 인증 옵션은 다음과 같습니다.

- XenMobile 서버를 SAML 의 IdP(ID 공급자) 로 사용합니다.

이 옵션을 사용하면 사용자 환경을 향상하고 Citrix Files 계정 생성을 자동화하는 동시에 모바일 앱 SSO 기능을 지원할 수 있습니다.

- XenMobile 서버에서 이 프로세스가 향상되며 Active Directory 동기화가 필요하지 않습니다.
- Citrix Files 사용자 관리 도구를 사용자 프로비전에 사용합니다.
- 지원되는 타사 공급업체를 SAML의 IdP로 사용합니다.

기존의 지원되는 IdP가 있고 모바일 앱 SSO 기능이 필요하지 않은 경우 이 옵션이 가장 적합할 수 있습니다. 이 옵션을 사용하려면 계정 프로비전에 Citrix Files 사용자 관리 도구를 사용해야 합니다.

타사 IdP 솔루션 (예: ADFS)을 사용하는 경우 Windows 클라이언트 측에서 SSO 기능을 사용할 수도 있습니다. Citrix Files SAML IdP를 선택하기 전에 사용 사례를 평가하십시오.

또한 두 사용 사례를 모두 충족하기 위해 [ADFS 및 XenMobile](#)을 이중 IdP로 구성할 수 있습니다.

모바일 앱

질문:

- 사용하려는 Citrix Files 모바일 앱은 무엇입니까 (공용, MDM, MDX)?

설계 의사 결정:

- Apple App Store 및 Google Play Store로부터 모바일 생산성 앱을 배포할 수 있습니다. 공용 앱 스토어 배포를 사용하는 경우 Citrix 다운로드 페이지에서 래핑된 앱을 받을 수 있습니다.
- 보안 수준이 낮고 컨테이너화가 필요하지 않은 경우 공용 Citrix Files 응용 프로그램은 적합하지 않을 수 있습니다. MDM 전용 환경에서는 XenMobile을 MDM 모드에서 사용하여 Citrix Files 앱의 MDM 버전을 제공할 수 있습니다.
- 자세한 내용은 [XenMobile용 Citrix Files](#)에서 앱을 참조하십시오.

보안, 정책 및 액세스 제어

질문:

- 데스크톱, 웹 및 모바일 사용자에게 적용해야 하는 제한은 무엇입니까?
- 사용자에게 적용하려는 표준 액세스 제어 설정은 무엇입니까?
- 사용하려는 파일 보존 정책은 무엇입니까?

설계 의사 결정:

- Citrix Files를 사용하여 직원 권한 및 장치 보안을 관리할 수 있습니다. 자세한 내용은 [Employee Permissions\(직원 권한\)](#)과 [Managing Devices and Apps\(장치 및 앱 관리\)](#)를 참조하십시오.
- 일부 Citrix Files 장치 보안 설정 및 MDX 정책은 동일한 기능을 제어합니다. 이러한 경우 XenMobile 정책이 우선하며 Citrix Files 장치 보안 설정이 그 다음으로 적용됩니다. 예: Citrix Files에서 외부 앱을 사용하지 않도록 설정하고 XenMobile에서 사용하도록 설정하면 외부 앱이 Citrix Files에서 사용되지 않습니다. XenMobile에서는 PIN/암호를 사용하지 않고 Citrix Files 앱에서 PIN/암호를 사용하도록 앱을 구성할 수 있습니다.

표준 **StorageZone** 와 제한된 **StorageZone** 비교

질문:

- 제한된 StorageZone 이 필요합니까?

설계 의사 결정:

- 표준 StorageZone 은 중요하지 않은 데이터에 사용되며 이를 통해 직원들은 직원 이외의 사람들과 데이터를 공유할 수 있습니다. 이 옵션은 도메인 외부의 데이터 공유와 관련된 워크플로를 지원합니다.
- 제한된 StorageZone 은 중요한 데이터를 보호합니다. 인증된 도메인 사용자만 해당 영역에 저장된 데이터에 액세스할 수 있습니다.

웹 프록시

HTTP(S)/SOCKS 프록시를 통해 XenMobile 트래픽을 라우팅하는 가장 일반적인 시나리오는 XenMobile 서버가 상주하는 서버넷에서 아웃바운드 인터넷 액세스를 통해 필요한 Apple, Google 또는 Microsoft IP 주소에 액세스할 수 없는 경우입니다. XenMobile 에서 모든 인터넷 트래픽을 프록시 서버로 라우팅하도록 프록시 서버 설정을 지정할 수 있습니다. 자세한 내용은 [프록시 서버 사용](#)을 참조하십시오.

다음 표에서는 XenMobile 에 사용되는 가장 일반적인 프록시의 장점 및 단점에 대해 설명합니다.

옵션	장점	단점
XenMobile 서버에서 HTTP(S)/SOCKS 프록시를 사용합니다.	정책이 XenMobile 서버 서버넷의 아웃바운드 인터넷 연결을 허용하지 않는 경우 HTTP(S) 또는 SOCKS 프록시를 구성하여 인터넷 연결을 제공할 수 있습니다.	프록시 서버가 실패하면 APNs(iOS) 또는 Firebase Cloud Messaging(Android) 연결이 끊깁니다. 그 결과 모든 iOS 및 Android 장치에 대한 장치 알림이 실패합니다.
Secure Web 에서 HTTP(S) 프록시를 사용합니다.	HTTP/HTTPS 트래픽을 모니터링하여 인터넷 활동이 조직의 표준을 준수하는지 확인할 수 있습니다.	이 구성에서는 모든 Secure Web 인터넷 트래픽을 회사 네트워크로 다시 터널링한 다음 인터넷으로 전송해야 합니다. 회사의 인터넷 연결이 브라우징을 제한하는 경우 이 구성이 인터넷 브라우징 성능에 영향을 미칠 수 있습니다.

분할 터널링에 대한 Citrix ADC 세션 프로필 구성은 트래픽에 다음과 같은 영향을 미칩니다.

Citrix ADC 분할 터널링이 꺼짐인 경우:

- MDX 네트워크 액세스 정책이 내부 네트워크로 터널링됨인 경우: 모든 트래픽에 Citrix Gateway 로 다시 터널링되는 Micro VPN 또는 cVPN(클라이언트 없는 VPN) 터널이 사용됩니다.

- 프록시 서버에 대한 Citrix ADC 트래픽 정책/프로필을 구성하고 Citrix Gateway VIP 에 정책을 바인딩합니다.

중요:

Secure Hub cVPN 트래픽을 프록시에서 제외하십시오.

- 자세한 내용은 [XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode\(Secure Browse 모드에서 프록시 서버를 통한 XenMobile Secure Hub 트래픽\)](#)를 참조하십시오.

Citrix ADC 분할 터널링이 켜짐인 경우:

- MDX 네트워크 액세스 정책이 내부 네트워크로 터널링됨으로 구성된 앱의 경우: 앱이 웹 리소스에 직접 액세스를 시도합니다. 웹 리소스가 공개적으로 제공되지 않는 경우 이러한 앱은 Citrix Gateway 로 폴백합니다.
- 프록시 서버에 대한 Citrix ADC 트래픽 정책 및 프로필을 구성합니다. 그런 다음 이러한 정책 및 프로필을 Citrix Gateway VIP 에 바인딩합니다.

중요:

Secure Hub cVPN 트래픽을 프록시에서 제외하십시오.

Split DNS(DNS 분할)(Client experience(클라이언트 환경) 아래) 에 대한 Citrix ADC 세션 프로필 구성은 분할 터널링과 유사하게 작동합니다.

Split DNS(DNS 분할) 를 사용하고 둘 다로 설정한 경우:

- 클라이언트가 FQDN 을 로컬로 확인한 다음 실패 시 Citrix ADC 로 폴백하여 DNS 를 확인합니다.

Split DNS(DNS 분할) 를 원격으로 설정한 경우:

- DNS 확인이 Citrix ADC 에서만 수행됩니다.

Split DNS(DNS 분할) 를 로컬로 설정한 경우:

- 클라이언트가 FQDN 을 로컬로 확인합니다. Citrix ADC 는 DNS 확인에 사용되지 않습니다.

액세스 제어

회사에서 네트워크 내부 및 외부의 모바일 장치를 관리할 수 있습니다. XenMobile 같은 엔터프라이즈 모빌리티 관리 솔루션은 모바일 장치의 위치에 관계없이 보안 및 제어를 제공할 수 있습니다. 그뿐만 아니라 NAC(네트워크 액세스 제어) 솔루션과 함께 사용할 경우 QoS 를 추가하고 네트워크 내부의 장치를 보다 세부적으로 제어할 수 있습니다. 이러한 결합을 사용할 경우 XenMobile 장치의 보안 평가를 NAC 솔루션을 통해 확장할 수 있습니다. 그런 다음 NAC 솔루션에서 XenMobile 보안 평가를 사용하여 인증 의사 결정을 지원하고 처리할 수 있습니다.

다음 솔루션 중 하나를 사용하여 NAC 정책을 적용할 수 있습니다.

- Citrix Gateway
- Cisco Identity Services Engine(ISE)

- ForeScout

Citrix 는 다른 NAC 솔루션에 대한 통합을 보장하지 않습니다.

NAC 솔루션과 XenMobile 의 통합은 다음과 같은 장점을 제공합니다.

- 엔터프라이즈 네트워크의 모든 끝점에 대한 보안, 규정 준수 및 제어가 개선됩니다.
- NAC 솔루션은 다음과 같은 기능을 제공합니다.
 - 회사 네트워크에 연결하는 장치를 즉시 감지합니다.
 - XenMobile 에 장치 특성을 쿼리합니다.
 - 해당 장치 정보를 사용하여 이러한 장치를 허용, 차단, 제한 또는 리디렉션할지 결정합니다. 이러한 결정은 회사에서 선택하는 보안 정책에 따라 다릅니다.
- IT 관리자는 NAC 솔루션을 사용하여 관리되지 않는 장치와 규정을 준수하지 않는 장치를 확인할 수 있습니다.

XenMobile 에서 지원되는 NAC 규정 준수 필터에 대한 설명 및 구성 개요는 [네트워크 액세스 제어](#)에서 확인하십시오.

다중 사이트 요구 사항

March 15, 2024

고가용성 및 재해 복구를 위한 여러 사이트를 포함하는 XenMobile 배포를 설계하고 구성할 수 있습니다. 이 문서에서는 XenMobile 배포에 사용되는 고가용성 및 재해 복구 모델의 개요를 제공합니다.

고가용성

- XenMobile 클러스터 노드의 경우 Citrix ADC 가 부하 분산을 처리합니다. 자세한 내용은 [클러스터링 구성](#)을 참조하십시오.
- XenMobile 서버 노드는 활성/활성 구성으로 작동합니다.
- 용량이 필요하면 추가 XenMobile 서버 노드가 고가용성 클러스터에 추가됩니다. 단일 노드는 최대 약 8,500 개의 사용자 장치를 처리할 수 있습니다 (자세한 내용은 [확장성 및 성능](#) 참조).
- 8,500 개 사용자 장치를 처리하는 서버 하나와 중복성을 위한 추가 서버 하나를 나타내는 “n+1” 로 XenMobile 서버를 구성하는 것이 좋습니다.
- 가능한 경우 모든 Citrix ADC 인스턴스에 대해 고가용성을 구성하여 두 번째 Citrix ADC 와 구성을 동기화하는 것이 좋습니다.
- 표준 Citrix ADC 고가용성 쌍은 활성/비활성 구성으로 작동합니다.

일반적인 고가용성 XenMobile 배포에는 다음이 포함됩니다.

- Citrix ADC 인스턴스 2 개 (VPX 또는 MPX). Citrix ADC SDX 플랫폼을 사용하는 경우에도 고가용성을 고려해야 합니다.
- 동일한 데이터베이스 설정으로 구성된 둘 이상의 XenMobile 서버.

재해 복구

활성 데이터 센터 1 개와 비활성 데이터 센터 1 개로 구성된 데이터 센터 2 개를 사용하여 XenMobile 의 재해 복구를 구성할 수 있습니다. 활성/활성 설정의 사용자 환경을 제공하기 위해 활성/활성 데이터 경로를 만들려면 Citrix ADC 와 GSLB(Global Server Load Balancing) 를 사용합니다.

재해 복구를 위한 XenMobile 배포에는 다음이 포함됩니다.

- 하나 이상의 Citrix ADC 인스턴스, XenMobile 서버 및 SQL Server 데이터베이스가 포함된 데이터 센터 2 개.
- 트래픽을 데이터 센터로 전달하는 GSLB 서버. 사이트에 대한 트래픽을 처리하는 XenMobile 등록 URL 과 Citrix Gateway URL 모두에 대해 GSLB 서버를 구성합니다.
- XenMobile 용 Citrix ADC 마법사를 사용하여 Citrix Gateway 를 구성하는 경우, 기본적으로 GSLB 가 XenMobile 등록 서버에 대한 트래픽과 Citrix Gateway 에 대한 트래픽을 MAM 부하 분산 서버로 이동하는 중에 확인하도록 설정되지 않습니다. 따라서 더 많은 단계가 필요합니다. 이러한 단계의 준비 및 구현에 대한 자세한 내용은 [재해 복구](#) 를 참조하십시오.
- Always On 가용성 그룹의 클러스터링된 SQL Server.
- XenMobile 서버와 SQL Server 간 대기 시간은 5 밀리초 미만이어야 합니다.

참고:

이 안내서에 설명된 재해 복구 방법은 액세스 계층에 대한 자동 재해 복구만 제공합니다. 장치에서 XenMobile 서버에 연결하려면 장애 조치 (failover) 사이트에서 모든 XenMobile 서버 노드와 SQL Server 데이터베이스를 수동으로 시작해야 합니다.

Citrix Gateway 및 Citrix ADC 통합

March 15, 2024

Citrix Gateway 를 XenMobile 과 통합하면 내부 네트워크로 원격 액세스하는 MAM 장치에 대한 인증 메커니즘을 사용할 수 있습니다. 이 통합을 사용하면 마이크로 VPN 을 통해 인터넷의 기업 서버에 모바일 생산성 앱을 연결할 수 있습니다. 모바일 장치의 앱에서 Citrix Gateway 로 마이크로 VPN 이 생성됩니다. Citrix Gateway 는 모든 회사 리소스에 액세스할 수 있는 Micro VPN 경로를 제공하며 강력한 다중 단계 인증을 지원합니다.

다음의 경우 모든 XenMobile Server 장치 모드에 Citrix ADC 부하 분산이 필요합니다.

- 다수의 XenMobile Server 가 있는 경우
- XenMobile Server 가 DMZ 또는 내부 네트워크에 있는 경우 (트래픽이 장치에서 Citrix ADC 를 거쳐 XenMobile 로 흐르는 경우)

XenMobile Server 모드에 대한 통합 요구 사항

Citrix Gateway 및 Citrix ADC 의 통합 요구 사항은 XenMobile Server 모드 (MAM, MDM 및 ENT) 에 따라 다릅니다.

MAM

XenMobile Server 를 MAM 모드에서 사용:

- **Citrix Gateway** 가 필요합니다. Citrix Gateway 는 모든 회사 리소스에 액세스할 수 있는 Micro VPN 경로를 제공하며 강력한 다중 단계 인증을 지원합니다.
- 부하 분산에는 **Citrix ADC** 가 권장됩니다.

XenMobile 앞에 부하 분산 장치를 배치하는 고가용성 구성으로 XenMobile 을 배포하는 것이 좋습니다. 자세한 내용은 [MAM 모드와 레거시 MAM 모드 정보](#)를 참조하십시오.

MDM

XenMobile Server 를 MDM 모드에서 사용:

- Citrix Gateway 가 필요하지 않습니다. MDM 배포의 경우 Citrix Gateway 는 모바일 장치 VPN 에 권장됩니다.
- 보안 및 부하 분산에는 Citrix ADC 가 권장됩니다.

보안 및 부하 분산을 위해 Citrix ADC 장비를 XenMobile Server 앞에 배포하는 것이 좋습니다. XenMobile 을 DMZ 에 배포하는 표준 배포의 경우 XenMobile 용 Citrix ADC 마법사와 함께 XenMobile Server 부하 분산을 SSL 브리지 모드에서 사용하는 것이 좋습니다. 다음과 같은 배포의 경우 SSL 오프로드도 고려할 수 있습니다.

- XenMobile Server 가 DMZ 가 아닌 내부 네트워크에 있는 배포
- 보안 팀에서 SSL 브리지 구성을 요구하는 배포

Citrix 에서는 NAT 또는 기존 타사 프록시 또는 MDM 용 부하 분산 장치를 통해 XenMobile Server 를 인터넷에 노출하는 것을 권장하지 않습니다. XenMobile Server(SSL 브리지) 에서 SSL 트래픽이 종료되더라도 이러한 구성은 잠재적인 보안 위험을 유발합니다.

보안 수준이 높은 환경에서 기본 XenMobile 구성의 Citrix ADC 는 보안 요구 사항을 충족하거나 초과합니다.

보안 요구 사항이 가장 높은 MDM 환경에서는 SSL 을 Citrix ADC 에서 종료하여 경계에서 트래픽을 검사하는 동시에 중단 간 SSL 암호화를 유지할 수 있습니다. 자세한 내용은 [보안 요구 사항](#)을 참조하십시오. Citrix ADC 는 SSL/TLS 암호화 및 SSL FIPS Citrix ADC 하드웨어를 정의하는 옵션을 제공합니다.

ENT(MAM+MDM)

XenMobile Server 를 ENT 모드에서 사용:

- Citrix Gateway 가 필요합니다. Citrix Gateway 는 모든 회사 리소스에 액세스할 수 있는 Micro VPN 경로를 제공하며 강력한 다중 단계 인증을 지원합니다.

XenMobile Server 모드가 ENT 이고 사용자가 MDM 등록을 선택하는 경우 장치는 레거시 MAM 모드에서 작동합니다. 레거시 MAM 모드에서는 Citrix Gateway FQDN 을 사용하여 장치를 등록합니다. 자세한 내용은 [MAM 모드와 레거시 MAM 모드 정보](#)를 참조하십시오.

- 부하 분산에는 Citrix ADC 가 권장됩니다. 자세한 내용은 이 문서에서 앞서 살펴본 “MDM” 아래의 Citrix ADC 요점을 참고하십시오.

중요:

초기 등록의 경우 사용자 장치의 트래픽은 SSL 오프로드 또는 SSL 브리지에 대한 부하 분산 가상 서버의 구성 여부와 관계 없이 XenMobile Server 에서 인증됩니다.

설계 의사 결정

다음 섹션에는 Citrix Gateway 와 XenMobile 의 통합을 계획할 때 고려해야 하는 다수의 설계 의사 결정이 요약되어 있습니다.

라이선스 및 버전

의사 결정 세부 정보:

- 사용하려는 Citrix ADC 버전은 무엇입니까?
- Citrix ADC 에 플랫폼 라이선스를 적용했습니까?
- MAM 기능이 필요한 경우 Citrix ADC Universal Access 라이선스를 적용했습니까?

설계 지침:

Citrix Gateway 에 올바른 라이선스를 적용하십시오. Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용하는 경우 통합 캐싱이 필요할 수 있습니다. 따라서, 적절한 Citrix ADC 버전이 있어야 합니다.

Citrix ADC 기능을 사용하기 위한 라이선스 요구 사항은 다음과 같습니다.

- XenMobile MDM 부하 분산을 사용하려면 Citrix ADC Standard 이상의 플랫폼 라이선스가 필요합니다.
- StorageZones Controller 를 통한 ShareFile 부하 분산에는 최소한 Citrix ADC 표준 플랫폼 라이선스가 필요합니다.
- XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드) 에는 MAM 에 필요한 Citrix Gateway Universal 라이선스가 포함되어 있습니다.
- Exchange 부하 분산을 사용하려면 Citrix ADC Platinum 플랫폼 라이선스 또는 Citrix ADC Enterprise 플랫폼 라이선스 (통합 캐싱 라이선스 포함) 가 필요합니다.

XenMobile 용 Citrix ADC 버전

의사 결정 세부 정보:

- XenMobile 환경에서 실행되는 Citrix ADC 버전은 무엇입니까?
- 별도의 인스턴스가 필요합니까?

설계 지침:

Citrix Gateway 가상 서버를 위한 전용 Citrix ADC 인스턴스를 사용하는 것이 좋습니다. XenMobile 환경에서 필요한 최소 버전의 Citrix ADC 와 빌드가 사용되고 있는지 확인하십시오. 일반적으로 XenMobile 과 호환되는 최신 Citrix ADC 버전 및 빌드를 사용하는 것이 가장 좋습니다. Citrix Gateway 업그레이드가 기존 환경에 영향을 미칠 수 있는 경우 XenMobile 을 위한 두 번째 전용 인스턴스를 만드는 것이 적절할 수 있습니다.

XenMobile 의 Citrix ADC 인스턴스를 VPN 연결을 사용하는 다른 앱과 공유하려는 경우 두 앱에서 사용하기에 충분한 VPN 라이선스가 있는지 확인하십시오. XenMobile 테스트 및 프로덕션 환경에서는 Citrix ADC 인스턴스를 공유할 수 없습니다.

인증서

의사 결정 세부 정보:

- XenMobile 환경을 등록하고 액세스할 때 더 높은 수준의 보안이 필요합니까?
- LDAP 를 사용할 수 없습니까?

설계 지침:

XenMobile 에 대한 기본 구성은 사용자 이름 및 암호 인증입니다. XenMobile 환경에 대한 등록 및 액세스 시 추가 보안 계층을 추가하려면 인증서 기반 인증을 사용하는 것이 좋습니다. 인증서를 LDAP 와 함께 2 단계 인증에 사용하여 RSA 서버 없이 더 높은 수준의 보안을 제공할 수 있습니다.

LDAP 를 허용하지 않고 스마트 카드 또는 유사한 방법을 사용하는 경우 인증서를 구성하면 XenMobile 에 스마트 카드를 나타낼 수 있습니다. 그런 다음 사용자는 XenMobile 에서 생성된 고유한 PIN 을 사용하여 등록합니다. 사용자가 액세스 권한을 획득하면 XenMobile 이 XenMobile 환경에 인증하는 데 사용될 인증서를 만들어 배포합니다.

XenMobile 은 타사 인증 기관에 대해서만 CRL(인증서 해지 목록) 을 지원합니다. Microsoft CA 가 구성된 경우 XenMobile 은 Citrix ADC 를 사용하여 인증서 해지를 관리합니다. 클라이언트 인증서 기반 인증을 구성하는 경우 Citrix ADC CRL(인증서 해지 목록) 설정인 **Enable CRL Auto Refresh**(CRL 자동 새로 고침 사용) 를 구성할지 여부를 고려합니다. 이 단계는 MAM 전용으로 등록된 장치 사용자가 장치의 기존 인증서를 사용하여 인증할 수 없도록 합니다. XenMobile 에서는 인증서가 해지된 경우 사용자가 사용자 인증서를 생성할 수 있으므로 새 인증서가 다시 발급됩니다. 이 설정을 사용하면 CRL 이 만료된 PKI 엔터티를 확인하는 경우 PKI 엔터티의 보안이 강화됩니다.

네트워킹 토폴로지

의사 결정 세부 정보:

- 필요한 Citrix ADC 토폴로지는 무엇입니까?

설계 지침:

XenMobile 에는 Citrix ADC 인스턴스를 사용하는 것이 좋습니다. 하지만 네트워크 내부에서 DMZ 로 나가는 트래픽을 원하지 않을 수도 있습니다. 이 경우에는 Citrix ADC 추가 인스턴스 설정을 고려해 보십시오. 내부 사용자를 위한 Citrix ADC 인스

턴스 하나, 외부 사용자를 위한 인스턴스 하나를 사용합니다. 사용자가 내부 네트워크와 외부 네트워크를 전환하는 경우 DNS 레코드 캐싱으로 인해 Secure Hub 에서 로그인 시도가 증가할 수 있습니다.

XenMobile 은 Citrix Gateway 이중 호를 지원하지 않습니다.

전용 또는 공유 **Citrix Gateway VIP**

의사 결정 세부 정보:

- 현재 Virtual Apps and Desktops 에 Citrix Gateway 를 사용하고 있습니까?
- XenMobile 에서 Virtual Apps and Desktops 와 동일한 Citrix Gateway 를 사용할 계획입니까?
- 두 트래픽 흐름에 대한 인증 요구 사항은 무엇입니까?

설계 지침:

Citrix 환경에 XenMobile 에 더해 Virtual Apps and Desktops 가 포함되는 경우 동일한 Citrix ADC 인스턴스와 Citrix Gateway 가상 서버를 동시에 사용할 수 있습니다. 버전 관리 충돌 및 환경 격리가 발생할 수 있으므로 각 XenMobile 환경에서 전용 Citrix ADC 인스턴스 및 Citrix Gateway 를 사용하는 것이 좋습니다. 그러나 전용 Citrix ADC 인스턴스를 사용할 수 없는 경우 Citrix에서는 전용 Citrix Gateway 가상 서버를 사용하여 Secure Hub 트래픽 흐름을 분리하기를 권장합니다. 가상 서버 대신 이러한 구성이 XenMobile 과 Virtual Apps and Desktops 사이에 공유됩니다.

LDAP 인증을 사용하는 경우 Receiver 및 Secure Hub 에서 동일한 Citrix Gateway 에 문제 없이 인증할 수 있습니다. 인증서 기반 인증을 사용하는 경우 XenMobile 은 인증서를 MDX 컨테이너에 푸시하고 Secure Hub 는 이 인증서를 사용하여 Citrix Gateway 에 인증합니다. Receiver 는 Secure Hub 와 분리되며 Secure Hub 와 동일한 인증서를 사용하여 동일한 Citrix Gateway 에 인증할 수 없습니다.

이 경우 두 개의 Citrix Gateway VIP 에 동일한 FQDN 을 사용하는 다음과 같은 문제 해결 방식을 고려해 볼 수 있습니다.

- IP 주소가 동일한 Citrix Gateway VIP 를 두 개 만듭니다. Secure Hub 에 사용할 VIP 에는 표준 443 포트를 사용하고 Virtual Apps and Desktops(Receiver 배포) 에 사용할 VIP 에는 포트 444 를 사용합니다.
- 그러면 하나의 FQDN 이 동일한 IP 주소로 확인됩니다.
- 이 해결 방법을 사용하는 경우 기본적으로 포트 443 이 아닌 포트 444 에 대해 ICA 파일을 반환하도록 StoreFront 를 구성할 수 있습니다. 이 해결 방법을 사용하는 경우 사용자가 포트 번호를 입력할 필요가 없습니다.

Citrix Gateway 시간 초과

의사 결정 세부 정보:

- XenMobile 트래픽에 대한 Citrix Gateway 시간 초과를 어떻게 구성할 것입니까?

설계 지침:

Citrix Gateway에는 Session time-out(세션 시간 초과) 및 Forced time-out(강제 시간 초과) 라는 설정이 포함됩니다. 자세한 내용은 [권장되는 구성](#)을 참조하십시오. 백그라운드 서비스, Citrix ADC 및 오프라인 중 응용 프로그램 액세스에 대한 시간 초과 값이 서로 다르다는 점에 유의하십시오.

MAM에 대한 **XenMobile** 부하 분산 장치 IP 주소

의사 결정 세부 정보:

- VIP에 내부 또는 외부 IP 주소를 사용합니까?

설계 지침:

공용 IP 주소를 Citrix Gateway VIP에 사용할 수 있는 환경에서 XenMobile 부하 분산 VIP 및 주소를 이 방식으로 할당하면 등록 실패가 발생할 수 있습니다.

이 시나리오에서 등록 실패를 방지하려면 부하 분산 VIP에 내부 IP가 사용되어야 합니다. 이 가상 IP 주소는 사실 IP 주소의 RFC 1918 표준을 준수해야 합니다. 비사설 IP 주소를 이 가상 서버에 사용하는 경우 Citrix ADC가 인증 프로세스 중에 XenMobile Server에 연결할 수 없습니다. 자세한 내용은 <https://support.citrix.com/article/CTX200430>에서 참조하십시오.

MDM 부하 분산 메커니즘

의사 결정 세부 정보:

- Citrix Gateway로 XenMobile Servers의 부하를 분산하려면 어떻게 해야 합니까?

설계 지침:

XenMobile이 DMZ에 있는 경우 SSL 브리지를 사용합니다. XenMobile이 내부 네트워크에 있는 경우 보안 표준을 충족해야 한다면 SSL 오프로드를 사용합니다.

- SSL 브리지 모드에서 Citrix ADC VIP를 사용하여 XenMobile Server 부하를 분산하는 경우 인터넷 트래픽이 XenMobile Server로 직접 흐르고 여기서 연결이 종료됩니다. SSL 브리지 모드는 설정 및 문제 해결이 가장 간단한 모드입니다.
- SSL 오프로드 모드에서 Citrix ADC VIP를 사용하여 XenMobile Server 부하를 분산하는 경우 인터넷 트래픽이 Citrix ADC로 직접 흐르고 여기서 연결이 종료됩니다. 그런 다음 Citrix ADC는 Citrix ADC에서 XenMobile Server로의 새 세션을 설정합니다. SSL 오프로드 모드는 설정 및 문제 해결이 좀 더 복잡합니다.

SSL 오프로드를 통한 **MDM** 부하 분산의 서비스 포트

의사 결정 세부 정보:

- 부하 분산에 SSL 오프로드 모드를 사용하려는 경우 백엔드 서비스에 사용할 포트는 무엇입니까?

설계 지침:

SSL 오프로드의 경우 다음과 같이 포트 80 또는 8443을 선택합니다.

- 포트 80을 사용하여 XenMobile Server에 다시 연결함으로써 완벽한 오프로드를 수행합니다.

- 종단 간 암호화, 즉 트래픽 재암호화는 지원되지 않습니다. 자세한 내용은 Citrix 지원 문서 [Supported Architectures Between NetScaler and XenMobile Server](#)(NetScaler 와 XenMobile Server 간에 지원되는 아키텍처)를 참조하십시오.

등록 FQDN

의사 결정 세부 정보:

- 등록 및 XenMobile 인스턴스/부하 분산 VIP 에 무엇을 FQDN 으로 사용할 계획입니까?

설계 지침:

클러스터의 첫 번째 XenMobile Server 를 처음으로 구성할 때는 XenMobile Server FQDN 을 제공해야 합니다. 이 FQDN 은 MDM VIP URL 및 내부 MAM LB VIP URL 과 일치해야 합니다. (내부 Citrix ADC 주소 레코드는 MAM LB VIP 를 확인합니다.) 자세한 내용은 이 문서의 나중에 나오는 “관리 모드별 등록 FQDN” 을 참조하십시오.

추가로, 다음과 동일한 인증서를 사용해야 합니다.

- XenMobile SSL 수신기 인증서
- 내부 MAM LB VIP 인증서
- MDM VIP 인증서 (MDM VIP 에 SSL 오프로드를 사용 중인 경우)

중요:

등록 FQDN 을 구성한 후에는 변경할 수 없습니다. 새 등록 FQDN 을 사용하려면 새 SQL Server 데이터베이스와 XenMobile Server 를 다시 구축해야 합니다.

Secure Web 트래픽

의사 결정 세부 정보:

- Secure Web 을 내부 웹 브라우징으로만 제한할 계획입니까?
- 내부 및 외부 웹 브라우징에 Secure Web 을 사용할 계획입니까?

설계 지침:

내부 웹 브라우징에만 Secure Web 을 사용할 계획이라면 Citrix Gateway 구성이 간편합니다. Secure Web 은 기본적으로 모든 내부 사이트에 도달해야 합니다. 방화벽과 프록시 서버를 구성해야 할 수 있습니다.

내부와 외부 브라우징에 모두 Secure Web 을 사용할 계획이라면 SNIP 에서 아웃바운드 인터넷 액세스가 가능해야 합니다. IT 에서는 일반적으로 등록된 장치 (MDX 컨테이너 사용) 를 기업 네트워크의 확장으로 봅니다. 따라서, IT 에서는 보통 Secure Web 연결이 Citrix ADC 로 돌아와서 프록시 서버를 거친 다음 인터넷으로 나가기를 원합니다. 기본적으로 Secure Web 에서 는 내부 네트워크로의 응용 프로그램별 VPN 터널이 모든 네트워크 액세스에 사용됩니다. Citrix ADC 는 분할 터널 설정을 사용합니다.

Secure Web 연결에 대한 설명은 [사용자 연결 구성](#)을 참조하십시오.

Secure Mail 에 대한 푸시 알림

의사 결정 세부 정보:

- 푸시 알림을 사용할 계획입니까?

iOS 용 설계 지침:

Citrix Gateway 구성에 Secure Ticket Authority(STA) 가 포함되고 분할 터널링이 사용 중지되어 있을 수 있습니다. 그러면 Citrix Gateway 는 Secure Mail 에서 iOS 용 Secure Mail 의 푸시 알림에 지정된 Citrix 수신기 서비스 URL 로의 트래픽을 허용해야 합니다.

Android 용 설계 지침:

FCM(Firebase Cloud Messaging) 을 사용하여 Android 장치의 XenMobile 연결 방법 및 시기를 제어합니다. FCM 을 구성하면 모든 보안 동작 또는 배포 명령이 실행될 때 사용자에게 XenMobile Server 에 다시 연결하라는 메시지를 표시하는 Secure Hub 푸시 알림이 트리거됩니다.

HDX STA

의사 결정 세부 정보:

- HDX 응용 프로그램 액세스를 통합할 계획이라면 사용할 STA 는 무엇입니까?

설계 지침:

HDX STA 는 StoreFront 의 STA 와 일치해야 하며 Virtual Apps and Desktops 팜에서 유효해야 합니다.

Citrix Files 및 ShareFile

의사 결정 세부 정보:

- 환경에서 Storage Zone Controller 를 사용할 계획입니까?
- 사용할 Citrix Files VIP URL 은 무엇입니까?

설계 지침:

환경에 Storage Zone Controller 를 포함할 예정이라면 다음을 올바르게 구성해야 합니다.

- Citrix Files 스위치 VIP(Citrix Files 제어부에서 StorageZone Controller 서버와 통신하는 데 사용됨)
- Citrix Files 부하 분산 VIP
- 모든 필수 정책 및 프로필

자세한 내용은 [StorageZones Controller 설명서](#)를 참조하십시오.

SAML IdP

의사 결정 세부 정보:

- Citrix Files 에 SAML 이 필요한 경우 XenMobile 을 SAML IdP 로 사용할 것입니까?

설계 지침:

권장되는 모범 사례는 Citrix Files 를 XenMobile Advanced Edition, XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드) 와 통합하는 것입니다. 이 방법은 SAML 기반 페더레이션을 구성하는 것보다 더 간단한 대안입니다. 이러한 XenMobile 버전으로 Citrix Files 을 사용할 경우 XenMobile 은 Citrix Files 에 다음을 제공합니다.

- 모바일 생산성 앱 사용자의 Single sign-on(SSO) 인증
- Active Directory 기반 사용자 계정 프로비전
- 포괄적인 액세스 제어 정책

XenMobile 콘솔을 사용하여 Citrix Files 구성을 수행하고 서비스 수준 및 라이선스 사용 현황을 모니터링할 수 있습니다.

Citrix Files 클라이언트에는 XenMobile 용 Citrix Files 클라이언트 (래핑된 Citrix Files) 와 Citrix Files Mobile 클라이언트 (래핑되지 않은 Citrix Files) 의 두 가지가 있습니다. 차이점을 알아보려면 [Citrix Files for XenMobile 클라이언트](#) 와 [Citrix Files 모바일 클라이언트의 차이점](#)을 참조하십시오.

SAML 을 사용하여 다음에 대한 SSO 액세스를 제공하도록 XenMobile 및 ShareFile 을 구성할 수 있습니다.

- Citrix Files 모바일 앱
- 웹사이트, Outlook 플러그인 또는 동기화 클라이언트와 같이 래핑되지 않은 Citrix Files 클라이언트

XenMobile 을 Citrix Files 의 SAML IdP 로 사용하려면 적절한 구성이 있는지 확인합니다. 자세한 내용은 [Citrix Files SSO 용 SAML](#)을 참조하십시오.

ShareConnect 직접 연결

의사 결정 세부 정보:

- ShareConnect 를 실행하는 컴퓨터 또는 모바일 장치에서 사용자가 호스트 컴퓨터에 액세스할 때 직접 연결을 사용해야 합니까?

설계 지침:

ShareConnect 를 사용할 경우 사용자는 iPad, Android 태블릿 및 Android 휴대폰을 통해 컴퓨터에 안전하게 연결하여 파일 및 응용 프로그램에 액세스할 수 있습니다. 직접 연결의 경우, XenMobile 은 Citrix Gateway 를 사용하여 로컬 네트워크 외부의 리소스에 대한 보안 액세스를 제공합니다. 구성에 대한 자세한 내용은 [ShareConnect](#)를 참조하십시오.

각 관리 모드의 등록 **FQDN**

관리 모드	등록 FQDN
엔터프라이즈 (MDM+MAM) 및 MDM 등록 필수	XenMobile Server FQDN
엔터프라이즈 (MDM+MAM) 및 MDM 등록 선택	XenMobile Server FQDN 또는 Citrix Gateway FQDN
MDM 전용	XenMobile Server FQDN
MAM 전용 (레거시)	Citrix Gateway FQDN
MAM 전용	XenMobile Server FQDN

배포 요약

올바른 구성을 위해 XenMobile 용 Citrix ADC 마법사를 사용하는 것이 좋습니다. 마법사는 한 번만 사용할 수 있습니다. 테스트, 개발 및 프로덕션 환경을 위한 다수의 XenMobile 인스턴스가 있는 경우 추가 환경에 대한 Citrix ADC 를 수동으로 구성해야 합니다. 작동 중인 환경에서는 XenMobile 에서 사용할 Citrix ADC 를 수동으로 구성하기 전에 설정을 기록해 두십시오.

마법사를 사용하는 경우 결정해야 하는 중요한 사항은 XenMobile Server 에 대한 통신에 HTTPS 를 사용할지, 아니면 HTTP 를 사용할지입니다. HTTPS 는 Citrix ADC 와 XenMobile 간의 트래픽을 암호화하는 보안 백엔드 통신을 제공합니다. 재암호화는 XenMobile Server 성능에 영향을 미칩니다. HTTP 는 XenMobile Server 성능을 개선합니다. Citrix ADC 와 XenMobile 사이의 트래픽은 암호화되지 않습니다. 다음 표에 XenMobile Server 용 Citrix ADC 의 HTTP 및 HTTPS 포트 요구 사항이 나와 있습니다.

HTTPS

일반적으로, Citrix ADC MDM 가상 서버 구성에는 SSL 브리지가 권장됩니다. MDM 가상 서버에서 사용되는 Citrix ADC SSL 오프로드의 경우 XenMobile 은 포트 80 만 백엔드 서비스로 지원합니다.

관리 모드	Citrix ADC 부하 분산 방법	SSL 재암호화	XenMobile 서버 포트
MDM	SSL 브리지	해당 없음	443, 8443
MAM	SSL 오프로드	사용	8443
Enterprise	MDM: SSL 브리지	해당 없음	443, 8443
Enterprise	MAM: SSL 오프로드	사용	8443

HTTP

관리 모드	Citrix ADC 부하 분산 방법	SSL 재암호화	XenMobile 서버 포트
MDM	SSL 오프로드	지원되지 않음	80
MAM	SSL 오프로드	사용	8443
Enterprise	MDM: SSL 오프로드	지원되지 않음	80
Enterprise	MAM: SSL 오프로드	사용	8443

XenMobile 배포의 Citrix Gateway 다이어그램은 [온-프레미스 배포용 참조 아키텍처](#)를 참조하십시오.

MDX 앱에 대한 SSO 및 프록시 고려 사항

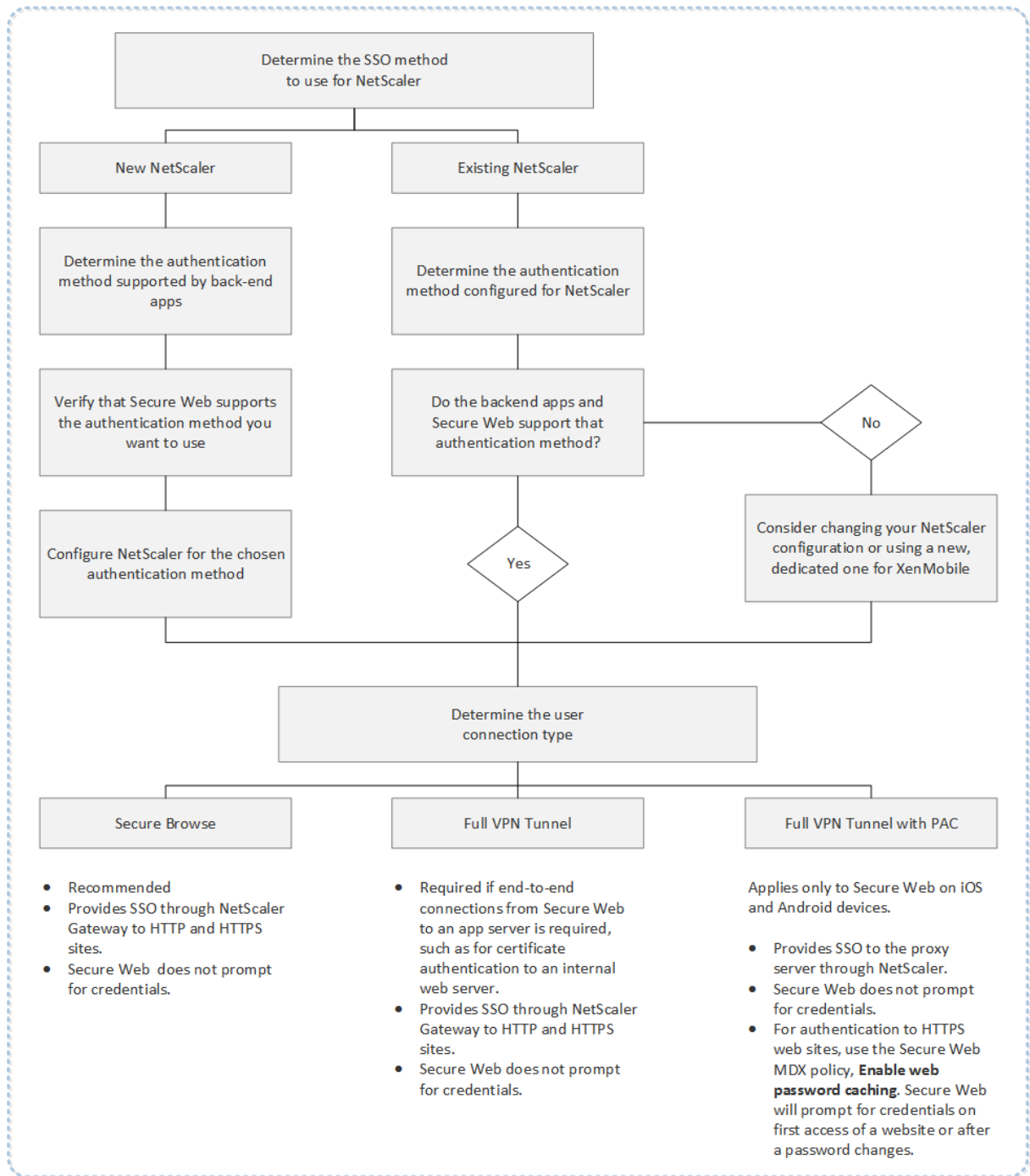
January 5, 2022

XenMobile 을 Citrix ADC 와 통합하면 모든 백엔드 HTTP/HTTPS 리소스에 대한 SSO(Single Sign-on) 를 사용자에게 제공할 수 있습니다. SSO 인증 요구 사항에 따라 다음 옵션 중 하나를 사용하도록 MDX 앱에 대한 사용자 연결을 구성할 수 있습니다.

- 클라이언트 없는 VPN 유형인 Secure Browse
- 전체 VPN 터널

환경에서 SSO 를 제공하기에 Citrix ADC 가 적합하지 않은 경우 정책 기반 로컬 암호 캐싱을 통해 MDX 앱을 구성할 수 있습니다. 이 문서에서는 Secure Web 을 중심으로 다양한 SSO 및 프록시 옵션에 대해 알아봅니다. 개념은 다른 MDX 앱에도 적용됩니다.

다음 순서도는 SSO 및 사용자 연결에 대한 의사 결정 흐름을 요약한 것입니다.



Citrix ADC 인증 방법

이 섹션에서는 Citrix ADC 가 지원하는 인증 방법에 대한 일반 정보를 제공합니다.

SAML 인증

SAML(Security Assertion Markup Language) 을 사용하도록 Citrix ADC 를 구성하는 경우 사용자는 SSO(Single Sign-on) 에 SAML 프로토콜을 지원하는 웹 앱에 연결할 수 있습니다. Citrix Gateway 는 SAML 웹 앱에 대해 IdP(ID 공급자) SSO(Single Sign-on) 를 지원합니다.

필요한 구성:

- Citrix ADC 트래픽 프로필에서 SAML SSO 를 구성합니다.
- 요청한 서비스에 대한 SAML IdP 를 구성합니다.

NTLM 인증

세션 프로필에서 웹 앱에 대한 SSO 를 사용하도록 설정하면 Citrix ADC 가 자동으로 NTLM 인증을 수행합니다.

필요한 구성:

- Citrix ADC 세션 또는 트래픽 프로필에서 SSO 를 사용하도록 설정합니다.

Kerberos 가장

XenMobile 은 Secure Web 에 대해서만 Kerberos 를 지원합니다. Kerberos SSO 를 사용하도록 Citrix ADC 를 구성하는 경우 사용자 암호가 Citrix ADC 에 제공되면 Citrix ADC 가 가장을 사용합니다. 가장은 Citrix ADC 가 Secure Web 같은 서비스에 액세스하는 데 필요한 티켓을 사용자 자격 증명을 사용하여 가져온다는 것을 의미합니다.

필요한 구성:

- 연결에서 Kerberos 영역을 식별할 수 있도록 Citrix ADC “Worx” 세션 정책을 구성합니다.
- Citrix ADC 에서 KCD(Kerberos 제한 위임) 계정을 구성합니다. 이 계정을 암호 없이 구성하고 XenMobile 게이트웨이의 트래픽 정책에 바인딩합니다.
- 이러한 구성 및 다른 구성에 대한 세부 정보는 Citrix 블로그 [WorxWeb and Kerberos Impersonation SSO\(WorxWeb 및 Kerberos 가장 SSO\)](#)를 참조하십시오.

Kerberos 제한 위임

XenMobile 은 Secure Web 에 대해서만 Kerberos 를 지원합니다. Kerberos SSO 를 사용하도록 Citrix ADC 를 구성하는 경우 사용자 암호가 Citrix ADC 에 제공되지 않으면 Citrix ADC 가 제한 위임을 사용합니다.

제한 위임을 사용하는 경우 Citrix ADC 는 사용자 및 서비스에 대한 티켓을 가져올 때 지정된 관리자 계정을 사용합니다.

필요한 구성:

- Citrix ADC 의 필요한 권한 및 KCD 계정을 사용하여 Active Directory 에서 KCD 계정을 구성합니다.
- Citrix ADC 트래픽 프로필에서 SSO 를 사용하도록 설정합니다.
- Kerberos 인증에 대한 백엔드 웹 사이트를 구성합니다.

양식 입력 인증

양식 기반 SSO(Single Sign-on) 를 사용하도록 Citrix ADC 를 구성하는 경우 사용자는 단 한 번의 로그인으로 네트워크의 모든 보호되는 앱에 액세스할 수 있습니다. 이 인증 방법은 Secure Browse 또는 전체 VPN 모드를 사용하는 앱에 적용됩니다.

필요한 구성:

- Citrix ADC 트래픽 프로필에서 양식 기반 SSO 를 구성합니다.

다이제스트 HTTP 인증

세션 프로필에서 웹 앱에 대한 SSO 를 사용하도록 설정하면 Citrix ADC 가 자동으로 다이제스트 HTTP 인증을 수행합니다. 이 인증 방법은 Secure Browse 또는 전체 VPN 모드를 사용하는 앱에 적용됩니다.

필요한 구성:

- Citrix ADC 세션 또는 트래픽 프로필에서 SSO 를 사용하도록 설정합니다.

기본 HTTP 인증

세션 프로필에서 웹 앱에 대한 SSO 를 사용하도록 설정하면 Citrix ADC 가 자동으로 기본 HTTP 인증을 수행합니다. 이 인증 방법은 Secure Browse 또는 전체 VPN 모드를 사용하는 앱에 적용됩니다.

필요한 구성:

- Citrix ADC 세션 또는 트래픽 프로필에서 SSO 를 사용하도록 설정합니다.

Secure Browse, 전체 VPN 터널 또는 PAC 포함 전체 VPN 터널

다음 섹션에서는 Secure Web 에 대한 사용자 연결 유형에 대해 설명합니다. 자세한 내용은 Citrix 설명서에서 Secure Web 문서 [사용자 연결 구성](#)을 참조하십시오.

전체 VPN 터널

내부 네트워크로 터널링되는 연결은 전체 VPN 터널을 사용할 수 있습니다. Secure Web 의 기본 설정 VPN 모드 정책을 사용하여 전체 VPN 터널을 구성할 수 있습니다. 클라이언트 인증서 또는 종단 간 SSL 을 사용하여 내부 네트워크의 리소스로 연결되는 경우 전체 VPN 터널을 사용하는 것이 좋습니다. 전체 VPN 터널은 모든 프로토콜을 TCP 를 통해 처리합니다. 전체 VPN 터널을 Windows, Mac, iOS 및 Android 장치에서 사용할 수 있습니다.

전체 VPN 터널 모드에서 Citrix ADC 는 HTTPS 세션 내부를 볼 수 없습니다.

Secure Browse

내부 네트워크에 터널링되는 연결은 Secure Browse 라고 하는 클라이언트 없는 VPN 의 변형을 사용할 수 있습니다. Secure Browse 는 Secure Web 의 기본 설정 **VPN** 모드 정책에 대해 지정된 기본 구성입니다. SSO(Single Sign-On) 가 필요한 연결에는 Secure Browse 를 사용하는 것이 좋습니다.

Secure Browse 모드에서 Citrix ADC 는 HTTPS 세션을 두 부분으로 분리합니다.

- 클라이언트에서 Citrix ADC 로
- Citrix ADC 에서 백엔드 리소스 서버로

Citrix ADC 는 이와 같은 분리를 통해 클라이언트와 서버 간의 모든 트랜잭션을 파악하고 SSO 를 제공합니다.

Secure Browse 모드에서 사용될 때 Secure Web 에 대해 프록시 서버를 구성할 수도 있습니다. 자세한 [XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode](#)(Secure Browse 모드에서 프록시 서버를 통한 XenMobile WorxWeb 트래픽) 블로그를 참조하십시오.

PAC 포함 전체 VPN 터널

iOS 및 Android 장치의 Secure Web 에 대해 전체 VPN 터널 배포와 함께 PAC(Proxy Automatic Configuration) 파일을 사용할 수 있습니다. XenMobile 은 Citrix ADC 에 의해 제공되는 프록시 인증을 지원합니다. PAC 파일에는 웹 브라우저에서 해당 URL 에 액세스하기 위해 프록시를 선택하는 방식을 정의하는 규칙이 포함됩니다. PAC 파일 규칙은 내부 및 외부 사이트에 대한 처리 방식을 지정할 수 있습니다. Secure Web 은 PAC 파일 규칙을 구문 분석하고 프록시 서버 정보를 Citrix Gateway 로 보냅니다. Citrix Gateway 는 PAC 파일 또는 프록시 서버를 인지하지 못합니다.

HTTPS 웹 사이트 인증의 경우 Secure Web MDX 정책인 웹 암호 캐싱 사용을 통해 Secure Web 을 인증하고 MDX 를 통해 프록시 서버에 SSO 를 제공할 수 있습니다.

Citrix ADC 분할 터널링

SSO 및 프록시 구성을 계획할 때는 Citrix ADC 분할 터널링을 사용할지 여부 또한 결정해야 합니다. Citrix ADC 분할 터널링은 필요한 경우에만 사용하는 것이 좋습니다. 이 섹션에서는 분할 터널링의 작동 방식을 간략히 설명합니다. Citrix ADC 는 라우팅 테이블에 따라 트래픽 경로를 결정합니다. Citrix ADC 분할 터널링이 켜져 있는 경우 Secure Hub 는 인터넷 트래픽에서 내부 (보호되는) 네트워크 트래픽을 구분합니다. Secure Hub 는 DNS 접미사 및 인트라넷 응용 프로그램을 사용하여 트래픽을 구분합니다. 그런 다음 Secure Hub 는 내부 네트워크 트래픽만 VPN 터널을 통해 터널링합니다. Citrix ADC 분할 터널링이 꺼져 있는 경우 모든 트래픽이 VPN 터널을 통과합니다.

- 보안상의 이유로 모든 트래픽을 모니터링해야 하는 경우 Citrix ADC 분할 터널링을 사용 중지하십시오. 그러면 모든 트래픽이 VPN 터널을 통과합니다.
- PAC 포함 전체 VPN 터널을 사용하는 경우 Citrix Gateway 분할 터널링을 사용하지 않아야 합니다. 분할 터널링이 켜져 있고 PAC 파일이 구성된 경우 PAC 파일 규칙이 Citrix ADC 분할 터널링 규칙보다 우선합니다. 트래픽 정책에 구성된 프록시 서버는 Citrix ADC 분할 터널링 규칙을 재정의하지 않습니다.

기본적으로 네트워크 액세스 정책은 **Secure Web**에 대해 내부 네트워크로 터널링됨으로 설정됩니다. 이 구성에서 MDX 앱은 Citrix ADC 분할 터널링 설정을 사용합니다. 일부 다른 모바일 생산성 앱의 경우 네트워크 액세스 정책의 기본값이 다릅니다.

Citrix Gateway에는 Micro VPN 역분할 터널링 모드도 있습니다. 이 구성에서는 Citrix ADC로 터널링되지 않는 IP 주소로 구성된 제외 목록을 사용할 수 있습니다. 이러한 주소는 장치의 인터넷 연결을 사용하여 전송됩니다. 역분할 터널링에 대한 자세한 내용은 Citrix Gateway 설명서를 참조하십시오.

XenMobile에는 역분할 터널링 제외 목록이 포함됩니다. 특정 웹 사이트를 Citrix Gateway를 통해 터널링하지 않으려는 경우 LAN을 대신 사용하여 연결하는 FQDN(정규화된 도메인 이름) 또는 DNS 접미사의 심표로 구분된 목록을 추가할 수 있습니다. 이 목록은 역분할 터널링이 구성된 Citrix Gateway의 Secure Browse 모드에서만 적용됩니다.

인증

March 15, 2024

XenMobile 배포에서 인증을 구성하는 방법을 결정할 때는 여러 요소를 고려해야 합니다. 이 섹션에서는 다음을 설명하여 인증에 영향을 미치는 다양한 요소를 쉽게 이해할 수 있도록 합니다.

- 인증과 관련된 기본 MDX 정책, XenMobile 클라이언트 속성 및 Citrix Gateway 설정.
- 이러한 정책, 클라이언트 속성 및 설정의 상호 작용 방식.
- 각 선택의 득실.

이 문서에는 보안 수준을 높이려는 경우 권장되는 구성에 대한 세 가지 예제도 포함되어 있습니다.

광범위하게 말해 보안이 강력하면 사용자가 더 자주 인증해야 하므로 사용자 환경이 덜 최적화됩니다. 이러한 요소의 균형을 맞추는 방식은 조직의 요구 사항 및 우선 순위에 따라 다릅니다. 권장되는 세 가지 구성을 검토하여 사용 가능한 인증 방법의 상호 작용과 XenMobile 환경의 배포를 최적화하는 방법을 파악하십시오.

인증 모드

온라인 인증: 사용자가 XenMobile 네트워크에 들어갈 수 있습니다. 인터넷 연결이 필요합니다.

오프라인 인증: 인증이 장치에서 수행됩니다. 사용자가 보안 저장소의 잠금을 해제하고, 다운로드된 메일, 캐싱된 웹 사이트 및 메모 같은 항목에 오프라인으로 액세스합니다.

인증 방법

1 단계 LDAP: XenMobile에서 LDAP(Lightweight Directory Access Protocol)와 호환되는 하나 이상의 디렉터리(예: Active Directory)에 대한 연결을 구성할 수 있습니다. 회사 환경에 대한 SSO(Single Sign-on)를 제공할 때 주로 사용되는 방법입니다. Active Directory 암호 캐싱을 통해 Citrix PIN을 사용하도록 선택하면 LDAP로 사용자 환경을 개선하는 동시에 등록, 암호 만료 및 계정 잠금 시 복잡한 암호를 사용하는 보안을 제공할 수 있습니다.

자세한 내용은 [도메인 또는 도메인 및 STA](#)를 참조하십시오.

클라이언트 인증서: XenMobile 을 업계 표준 인증 기관과 통합하여 인증서를 온라인 인증의 유일한 방법으로 사용할 수 있습니다. XenMobile 은 일회용 암호, 초대 URL 또는 LDAP 자격 증명이 필요한 사용자 등록 후 이 인증서를 제공합니다. 클라이언트 인증서를 기본적인 인증 방법으로 사용하는 경우 Citrix PIN 을 사용하여 클라이언트 인증서 전용 환경에서 장치의 인증서를 보호해야 합니다.

XenMobile 은 타사 인증 기관에 대해서만 CRL(인증서 해지 목록) 을 지원합니다. Microsoft CA 가 구성된 경우 XenMobile 은 Citrix ADC 를 사용하여 인증서 해지를 관리합니다. 클라이언트 인증서 기반 인증을 구성하는 경우 Citrix ADC CRL(인증서 해지 목록) 설정인 Enable CRL Auto Refresh(CRL 자동 새로 고침 사용) 를 구성할지 여부를 고려합니다. 이 단계는 MAM 전용 모드의 장치 사용자가 장치의 기존 인증서를 사용하여 인증할 수 없도록 합니다. XenMobile 에서는 인증서가 해지된 경우 사용자가 사용자 인증서를 생성할 수 있으므로 새 인증서가 다시 발급됩니다. 이 설정을 사용하면 CRL 이 만료된 PKI 엔터티를 확인하는 경우 PKI 엔터티의 보안이 강화됩니다.

인증서 기반 인증을 사용하여 사용자를 인증하거나 엔터프라이즈 CA(인증 기관) 를 사용하여 장치 인증서를 발급하려는 경우 필요한 배포를 보여주는 다이어그램은 [온-프레미스 배포용 참조 아키텍처](#)를 참조하십시오.

2 단계 LDAP + 클라이언트 인증서: XenMobile 환경에서 이 구성은 Citrix ADC 의 2 단계 인증을 통한 보안과 최상의 SSO 기능으로 보안과 사용자 환경을 최적화합니다. LDAP 와 클라이언트 인증서를 모두 사용하면 사용자가 알고 있는 것 (Active Directory 암호) 과 사용자가 가지고 있는 것 (장치의 클라이언트 인증서) 을 사용하여 보안을 제공할 수 있습니다. Secure Mail(및 다른 모바일 생산성 앱) 은 올바르게 구성된 Exchange 클라이언트 액세스 서버 환경에서 클라이언트 인증서 인증을 통해 처음 사용하는 사용자를 위한 원활한 환경을 자동으로 구성하고 제공할 수 있습니다. 사용 편의성을 최적화하기 위해 이 옵션을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다.

LDAP + 토큰: 이 구성에서는 전형적인 LDAP 자격 증명 구성에 더해 RADIUS 프로토콜을 사용하는 일회용 암호를 사용할 수 있습니다. 사용 편의성을 최적화하기 위해 이 옵션을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다.

인증과 관련된 중요 정책, 설정 및 클라이언트 속성

다음은 권장되는 세 가지 구성에서 중요한 역할을 하는 정책, 설정 및 클라이언트 속성입니다.

MDX 정책

앱 암호: 커짐인 경우, 앱을 시작하거나 비활성화된 후 다시 시작할 때 앱 잠금을 해제하려면 Citrix PIN 또는 암호가 필요합니다. 기본값은 커짐입니다.

모든 앱에 대해 비활성화 타이머를 구성하려면 XenMobile 콘솔에서 설정 탭의 클라이언트 속성에서 INACTIVITY_TIMER 값을 분으로 설정합니다. 기본값은 15 분입니다. 비활성화 타이머를 사용하지 않고 앱을 시작할 때만 PIN 또는 암호 입력 메시지가 표시되도록 하려면 값을 0 으로 설정합니다.

참고:

암호화 키 정책에 대해 보안 오프라인을 선택하는 경우 이 정책이 자동으로 사용됩니다.

온라인 세션 필요: 꺼짐인 경우, 사용자가 엔터프라이즈 네트워크에 연결되어 있고 세션이 활성 상태여야 장치의 앱에 액세스할 수 있습니다. 꺼짐인 경우 활성 세션이 없어도 장치의 앱에 액세스할 수 있습니다. 기본값은 꺼짐입니다.

최대 오프라인 기간 (시간): XenMobile 에서 앱 권한 부여 재확인 및 정책 새로 고침 없이 앱을 실행할 수 있는 최대 기간을 정의합니다. 최대 오프라인 기간을 설정하는 경우 iOS 용 Secure Hub 에 유효한 Citrix Gateway 토큰이 있으면 앱이 사용자 작업 중단 없이 XenMobile 에서 MDX 앱에 대한 새 정책을 검색합니다. Secure Hub 에 유효한 Citrix ADC 토큰이 없는 경우 앱 정책을 업데이트하려면 사용자가 Secure Hub 를 통해 인증해야 합니다. Citrix Gateway 세션이 비활성화되거나 세션 시간 초과 정책이 적용되는 경우 Citrix ADC 토큰이 무효화될 수 있습니다. 사용자가 Secure Hub 에 다시 로그인하면 앱을 계속 실행할 수 있습니다.

이 기간이 만료되기 30 분, 15 분 및 5 분 전에 사용자에게 로그인하라는 메시지가 표시되며 이 기간이 만료되면 사용자가 로그인할 때까지 앱은 잠긴 상태를 유지합니다. 기본값은 **72 시간 (3 일)** 입니다. 최소 기간은 1 시간입니다.

참고:

사용자가 이동이 잦고 해외 로밍을 사용해야 할 수 있는 시나리오의 경우 72 시간 (3 일) 의 기본값이 너무 짧을 수 있습니다.

백그라운드 서비스 티켓 만료: 백그라운드 네트워크 서비스 티켓이 유효한 기간입니다. Secure Mail 이 Citrix Gateway 를 통해 ActiveSync 를 실행하는 Exchange Server 에 연결하는 경우 XenMobile 에서 Secure Mail 이 내부 Exchange Server 에 연결하는 데 사용할 토큰을 발급합니다. 이 속성 설정에 따라 Secure Mail 이 인증 및 Exchange Server 에 대한 연결에 사용할 새 토큰을 요구하지 않고 토큰을 사용할 수 있는 기간이 결정됩니다. 시간 제한이 만료되면 사용자가 다시 로그인해야 새 토큰이 생성됩니다. 기본값은 **168 시간 (7 일)** 입니다. 이 시간 제한이 만료되면 메일 알림이 중단됩니다.

온라인 세션에 필요한 유예 기간 (분): 온라인 세션 필요 정책에 따라 앱을 더 이상 사용하지 못하게 될 때까지 온라인 세션의 유효성이 검사되지 않고도 사용자가 앱을 오프라인으로 사용할 수 있는 시간 (분) 을 결정합니다. 기본값은 0(유예 기간 없음) 입니다.

인증 정책에 대한 정보는 다음을 참조하십시오.

- MAM SDK 를 사용하는 경우: [MAM SDK 개요](#)
- MDX Toolkit 을 사용하는 경우: [iOS 용 MDX 정책](#) 및 [Android 용 MDX 정책](#)

XenMobile 클라이언트 속성

참고:

클라이언트 속성은 XenMobile 에 연결하는 모든 장치에 적용되는 글로벌 설정입니다.

Citrix PIN: 단순한 로그인 환경을 제공하려면 Citrix PIN 을 사용하도록 선택할 수 있습니다. PIN 을 사용하면 사용자가 Active Directory 사용자 이름 및 암호 같은 다른 자격 증명을 반복적으로 입력하지 않아도 됩니다. Citrix PIN 을 독립 실행형 오프라인 인증으로만 구성하거나 PIN 을 Active Directory 암호 캐싱과 결합하여 인증을 간소화함으로써 사용 편의성을 최적화할 수 있습니다. XenMobile 콘솔의 설정 > 클라이언트 > 클라이언트 속성에서 Citrix PIN 을 구성할 수 있습니다.

다음은 몇 가지 속성을 요약한 것입니다. 자세한 내용은 [클라이언트 속성](#) 을 참조하십시오.

ENABLE_PASSCODE_AUTH

표시 이름: Enable Citrix PIN Authentication(Citrix PIN 인증 사용)

이 키를 사용하여 Citrix PIN 기능을 활성화할 수 있습니다. Citrix PIN 또는 암호를 사용하는 경우 Active Directory 암호 대신 사용할 PIN 을 정의하라는 메시지가 나타납니다. **ENABLE_PASSWORD_CACHING** 을 사용하도록 설정했거나 XenMobile 에서 인증서 인증을 사용하는 경우 이 설정을 사용하도록 설정해야 합니다.

가능한 값: **true** 또는 **false**

기본값: **false**

ENABLE_PASSWORD_CACHING

표시 이름: Enable User Password Caching(사용자 암호 캐싱 사용)

이 키를 사용하면 사용자의 Active Directory 암호가 모바일 장치에 로컬로 캐싱됩니다. 이 키를 true 로 설정하면 Citrix PIN 또는 암호를 설정하라는 메시지가 사용자에게 표시됩니다. 이 키를 true 로 설정하는 경우 **ENABLE_PASSCODE_AUTH** 키를 **true** 로 설정해야 합니다.

가능한 값: **true** 또는 **false**

기본값: **false**

PASSCODE_STRENGTH

표시 이름: PIN Strength Requirement(PIN 강도 요구 사항)

이 키는 Citrix PIN 또는 암호의 강도를 정의합니다. 이 설정을 변경하면 사용자가 다음번에 인증을 수행할 때 새 Citrix PIN 또는 암호를 설정하라는 메시지가 나타납니다.

가능한 값: 약함, 중간, 강함

기본값: 중간

INACTIVITY_TIMER

표시 이름: Inactivity Timer(비활성 타이머)

이 키는 사용자가 장치를 비활성 상태로 둔 후에 Citrix PIN 또는 암호를 입력하라는 메시지 없이 앱에 액세스할 수 있는 시간 (분 단위) 을 정의합니다. MDX 앱에 대해 이 설정을 사용되도록 설정하려면 앱 암호 설정을 꺼짐으로 설정해야 합니다. 앱 암호 설정이 꺼짐으로 설정된 경우 사용자는 전체 인증을 수행하기 위해 Secure Hub 로 리디렉션됩니다. 이 설정을 변경하면 다음에 사용자에게 인증하라는 메시지가 표시될 때 값이 적용됩니다. 기본값은 15 분입니다.

ENABLE_TOUCH_ID_AUTH

표시 이름: Enable Touch ID Authentication(Touch ID 인증 사용)

오프라인 인증에서 지문 판독기 (iOS 만 해당) 를 사용할 수 있습니다. 온라인 인증에서는 기본 인증 방법을 사용해야 합니다.

ENCRYPT_SECRETS_USING_PASSCODE

표시 이름: Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)

이 키를 사용하면 민감한 데이터를 iOS 키 집합과 같은 플랫폼 기반 기본 저장소가 아닌 모바일 장치의 기밀 저장소에 저장할 수 있습니다. 이 구성 키는 주요 아티팩트의 강력한 암호화를 활성화하지만 사용자 엔트로피 (사용자만 알고 있는 사용자 생성 임의 PIN 코드) 도 증가합니다.

가능한 값: **true** 또는 **false**

기본값: **false**

Citrix ADC 설정

Session time-out(세션 시간 초과): 이 설정을 사용하면 Citrix ADC 에서 지정된 간격 동안 네트워크 활동이 감지되지 않을 경우 Citrix Gateway 가 세션 연결을 끊습니다. 이 설정은 Citrix Gateway 플러그인, Citrix Receiver, Secure Hub 또는 웹 브라우저를 통해 연결하는 사용자에게 적용됩니다. 기본값은 **1440** 분입니다. 이 값을 0 으로 설정하면 설정이 사용되지 않습니다.

Forced time-out(시간 초과 강제 적용): 이 설정을 사용하면 Citrix Gateway 가 시간 초과 간격이 지난 후 사용자의 활동 여부와 관계없이 세션 연결을 끊습니다. 시간 초과 간격이 경과하면 사용자는 어떠한 작업으로도 연결 종단을 방지할 수 없습니다. 이 설정은 Citrix Gateway 플러그인, Citrix Receiver, Secure Hub 또는 웹 브라우저를 통해 연결하는 사용자에게 적용됩니다. Secure Mail 에서 특수 Citrix ADC 모드인 STA 를 사용하는 경우 Secure Mail 세션에는 시간 초과 강제 적용 설정이 적용되지 않습니다. 기본값은 **1440** 분입니다. 이 값을 비워 두면 설정이 사용되지 않습니다.

Citrix Gateway 의 시간 초과 설정에 대한 자세한 내용은 Citrix ADC 설명서를 참조하십시오.

장치에서 자격 증명을 입력하여 XenMobile 을 통해 인증하라는 메시지를 사용자에게 표시하는 시나리오에 대한 자세한 내용은 [인증 프롬프트 시나리오](#)를 참조하십시오.

기본 구성 설정

이러한 설정은 다음에서 제공하는 기본값입니다.

- NetScaler for XenMobile 마법사
- MAM SDK 또는 MDX Toolkit
- XenMobile 콘솔

설정	설정을 찾는 위치	기본 설정
세션 시간 초과	Citrix Gateway	1440 분
Force time-out(강제 시간 초과)	Citrix Gateway	1440 분
최대 오프라인 기간	MDX 정책	72 시간
백그라운드 서비스 티켓 만료	MDX 정책	168 시간 (7 일)
온라인 세션 필요	MDX 정책	꺼짐

설정	설정을 찾는 위치	기본 설정
온라인 세션에 필요한 유예 기간	MDX 정책	0
앱 암호	MDX 정책	켜짐
Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)	XenMobile 클라이언트 속성	False
Enable Citrix PIN Authentication(Citrix PIN 인증 사용)	XenMobile 클라이언트 속성	False
PIN Strength Requirement(PIN 강도 요구 사항)	XenMobile 클라이언트 속성	중간
PIN Type(PIN 유형)	XenMobile 클라이언트 속성	숫자
Enable User Password Caching(사용자 암호 캐싱 사용)	XenMobile 클라이언트 속성	False
Inactivity Timer(비활성화 타이머)	XenMobile 클라이언트 속성	15
Enable Touch ID Authentication(Touch ID 인증 사용)	XenMobile 클라이언트 속성	False

권장되는 구성

이 섹션에서는 가장 낮은 수준의 보안과 최적의 사용자 환경부터 가장 높은 수준의 보안과 좀 더 불편한 사용자 환경에 이르는 세 가지 XenMobile 구성 예제를 제공합니다. 이러한 예제는 자체 구성을 적용할 위치를 결정할 때 유용한 참조로 사용될 수 있습니다. 이러한 설정을 수정하려면 다른 설정도 함께 변경해야 합니다. 예를 들어 최대 오프라인 기간은 세션 시간 초과보다 작아야 합니다.

최고 수준의 보안

이 구성은 가장 높은 수준의 보안을 제공하지만 사용 편의성이 크게 떨어지는 단점이 있습니다.

설정	설정을 찾는 위치	권장되는 설정	동작의 영향
----	-----------	---------	--------

세션 시간 초과	Citrix Gateway	1440	사용자는 온라인 인증이 요구되는 경우에만 24 시간마다 Secure Hub 자격 증명을 입력합니다.
Force time-out(강제 시간 초과)	Citrix Gateway	1440	온라인 인증이 24 시간마다 엄격히 요구됩니다. 활동이 있다고 해서 세션 수명이 연장되지는 않습니다.
최대 오프라인 기간	MDX 정책	23	매일 정책을 새로 고쳐야 합니다.
백그라운드 서비스 티켓 만료	MDX 정책	72 시간	STA에 대한 시간 제한으로, Citrix Gateway 세션 토큰 없이 세션 수명을 연장할 수 있습니다. Secure Mail의 경우 STA 시간 초과를 세션 시간 초과보다 길게 설정하면 사용자가 세션이 만료되기 전에 앱을 열지 않은 경우 사용자에게 메시지를 표시하지 않고 메일 알림이 중지되는 상황을 방지할 수 있습니다.
온라인 세션 필요	MDX 정책	꺼짐	유효한 네트워크 연결 및 Citrix Gateway 세션에서 앱을 사용할 수 있습니다.
온라인 세션에 필요한 유예 기간	MDX 정책	0	유예 기간이 없습니다 (온라인 세션 필요를 사용하는 경우).
앱 암호	MDX 정책	켜짐	응용 프로그램에 대한 암호가 필요합니다.
Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)	XenMobile 클라이언트 속성	true	사용자 엔트로피에서 파생된 키로 저장소를 보호합니다.
Enable Citrix PIN Authentication(Citrix PIN 인증 사용)	XenMobile 클라이언트 속성	true	Citrix PIN을 사용하여 사용자 인증 환경을 간소화합니다.
PIN Strength Requirement(PIN 강도 요구 사항)	XenMobile 클라이언트 속성	Strong(강함)	높은 수준의 암호 복잡성을 요구합니다.

PIN Type(PIN 유형)	XenMobile 클라이언트 속 성	영숫자	영숫자 시퀀스의 PIN 을 사용 합니다.
Enable Password Caching(암호 캐싱 사용)	XenMobile 클라이언트 속 성	False	Active Directory 암호는 캐싱되지 않으며 오프라인 인 증의 경우 Citrix PIN 이 사 용됩니다.
Inactivity Timer(비활성 화 타이머)	XenMobile 클라이언트 속 성	15	사용자가 이 기간에 MDX 앱 또는 Secure Hub 를 사용 하지 않으면 오프라인 인증에 대한 메시지가 표시됩니다.
Enable Touch ID Authentication(Touch ID 인증 사용)	XenMobile 클라이언트 속 성	False	iOS 에서 오프라인 인증에 대 해 Touch ID 를 사용하지 않 도록 설정합니다.

더 높은 수준의 보안

중도에 가까운 접근 방식인 이 구성은 7 일 대신 최대 3 일에 한 번씩 사용자 인증을 요구하고 보안을 강화합니다. 인증 횟수가 증
가하여 컨테이너가 더 자주 잠기므로 장치를 사용하지 않을 때의 데이터 보안이 강화됩니다.

설정	설정을 찾는 위치	권장되는 설정	동작의 영향
세션 시간 초과	Citrix Gateway	4320	사용자는 온라인 인증이 요구 되는 경우에만 3 일마다 Secure Hub 자격 증명을 입력합니다.
Force time-out(강제 시간 초과)	Citrix Gateway	값을 지정하지 않음	활동이 있는 경우 세션이 연장 됩니다.
최대 오프라인 기간	MDX 정책	71	정책을 3 일마다 새로 고쳐야 합니다. 시간 차이를 두면 세 션 시간 초과 전에 정책을 새 로 고칠 수 있습니다.

백그라운드 서비스 티켓 만료	MDX 정책	168 시간	STA 에 대한 시간 제한으로, Citrix Gateway 세션 토큰 없이 세션 수명을 연장할 수 있습니다. Secure Mail 의 경우 STA 시간 초과를 세션 시간 초과보다 길게 설정하면 사용자가 세션이 만료되기 전에 앱을 열지 않은 경우 사용자에게 메시지를 표시하지 않고 메일 알림이 중지되는 상황을 방지할 수 있습니다.
온라인 세션 필요	MDX 정책	꺼짐	유효한 네트워크 연결 및 Citrix Gateway 세션에서 앱을 사용할 수 있습니다.
온라인 세션에 필요한 유예 기간	MDX 정책	0	유예 기간이 없습니다 (온라인 세션 필요를 사용하는 경우).
앱 암호	MDX 정책	켜짐	응용 프로그램에 대한 암호가 필요합니다.
Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)	XenMobile 클라이언트 속성	False	사용자 엔트로피 없이 저장소를 암호화할 수 있습니다.
Enable Citrix PIN Authentication(Citrix PIN 인증 사용)	XenMobile 클라이언트 속성	true	Citrix PIN 을 사용하여 사용자 인증 환경을 간소화합니다.
PIN Strength Requirement(PIN 강도 요구 사항)	XenMobile 클라이언트 속성	중간	중간 수준의 암호 복잡성 규칙을 적용합니다.
PIN Type(PIN 유형)	XenMobile 클라이언트 속성	숫자	숫자 시퀀스의 PIN 을 사용합니다.
Enable Password Caching(암호 캐싱 사용)	XenMobile 클라이언트 속성	true	사용자 PIN 이 캐싱되고 Active Directory 암호를 보호하는 데 사용됩니다.
Inactivity Timer(비활성화 타이머)	XenMobile 클라이언트 속성	30	사용자가 이 기간에 MDX 앱 또는 Secure Hub 를 사용하지 않으면 오프라인 인증에 대한 메시지가 표시됩니다.

Enable Touch ID Authentication(Touch ID 인증 사용)	XenMobile 클라이언트 속성	true	iOS 에서 오프라인 인증에 대해 Touch ID 를 사용하도록 설정합니다.
--	--------------------	------	--

높은 수준의 보안

이 구성은 사용자에게 가장 편리한 환경과 기본 수준의 보안을 제공합니다.

설정	설정을 찾는 위치	권장되는 설정	동작의 영향
세션 시간 초과	Citrix Gateway	10080	사용자는 온라인 인증이 요구되는 경우에만 7 일마다 Secure Hub 자격 증명을 입력합니다.
Force time-out(강제 시간 초과)	Citrix Gateway	값을 지정하지 않음	활동이 있는 경우 세션이 연장됩니다.
최대 오프라인 기간	MDX 정책	167	정책을 매주 (7 일마다) 새로 고쳐야 합니다. 시간 차이를 두면 세션 시간 초과 전에 정책을 새로 고칠 수 있습니다.
백그라운드 서비스 티켓 만료	MDX 정책	240	STA 에 대한 시간 제한으로, Citrix Gateway 세션 토큰 없이 세션 수명을 연장할 수 있습니다. Secure Mail 의 경우 STA 시간 초과를 세션 시간 초과보다 길게 설정하면 사용자가 세션이 만료되기 전에 앱을 열지 않은 경우 사용자에게 메시지를 표시하지 않고 메일 알림이 중지되는 상황을 방지할 수 있습니다.
온라인 세션 필요	MDX 정책	꺼짐	유효한 네트워크 연결 및 Citrix Gateway 세션에서 앱을 사용할 수 있습니다.

온라인 세션에 필요한 유예 기간	MDX 정책	0	유예 기간이 없습니다 (온라인 세션 필요를 사용하는 경우).
앱 암호	MDX 정책	켜짐	응용 프로그램에 대한 암호가 필요합니다.
Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)	XenMobile 클라이언트 속성	False	사용자 엔트로피 없이 저장소를 암호화할 수 있습니다.
Enable Citrix PIN Authentication(Citrix PIN 인증 사용)	XenMobile 클라이언트 속성	true	Citrix PIN 을 사용하여 사용자 인증 환경을 간소화합니다.
PIN Strength Requirement(PIN 강도 요구 사항)	XenMobile 클라이언트 속성	Low(낮음)	암호 복잡성을 요구하지 않습니다.
PIN Type(PIN 유형)	XenMobile 클라이언트 속성	숫자	숫자 시퀀스의 PIN 을 사용합니다.
Enable Password Caching(암호 캐싱 사용)	XenMobile 클라이언트 속성	true	사용자 PIN 이 캐싱되고 Active Directory 암호를 보호하는 데 사용됩니다.
Inactivity Timer(비활성화 타이머)	XenMobile 클라이언트 속성	90	사용자가 이 기간에 MDX 앱 또는 Secure Hub 를 사용하지 않으면 오프라인 인증에 대한 메시지가 표시됩니다.
Enable Touch ID Authentication(Touch ID 인증 사용)	XenMobile 클라이언트 속성	true	iOS 에서 오프라인 인증에 대해 Touch ID 를 사용하도록 설정합니다.

상위 단계 인증 사용

일부 앱에는 향상된 인증 (예: 토큰 또는 적극적 세션 시간 초과 같은 보조 인증 요소) 이 필요할 수 있습니다. 이 인증 방법을 MDX 정책을 통해 제어할 수 있습니다. 또한 이 방법을 사용하려면 별개의 가상 서버를 사용하여 동일하거나 다른 Citrix ADC 장비에서 인증 방법을 제어해야 합니다.

설정	설정을 찾는 위치	권장되는 설정	동작의 영향
대체 Citrix Gateway	MDX 정책	보조 Citrix ADC 장비의 FQDN 및 포트가 필요합니다.	보조 Citrix ADC 장비 인증 및 세션 정책을 사용하여 향상된 인증을 제어할 수 있습니다.

사용자가 대체 Citrix Gateway 인스턴스에 로그인하는 앱을 열면 다른 모든 앱이 이 Citrix Gateway 인스턴스를 사용하여 내부 네트워크와 통신합니다. 세션은 향상된 보안을 사용하는 Citrix Gateway 인스턴스에서 세션이 시간 초과되는 경우에만 하위 수준의 보안을 사용하는 Citrix Gateway 인스턴스로 전환됩니다.

온라인 세션 필요 사용

Secure Web 같은 특정 응용 프로그램의 경우 사용자 세션이 인증되고 장치가 인터넷에 연결된 동안에만 사용자의 앱 실행을 허용해야 할 수 있습니다. 이 정책을 사용하면 이 옵션이 적용되고 유예 기간 동안 사용자가 작업을 마칠 수 있습니다.

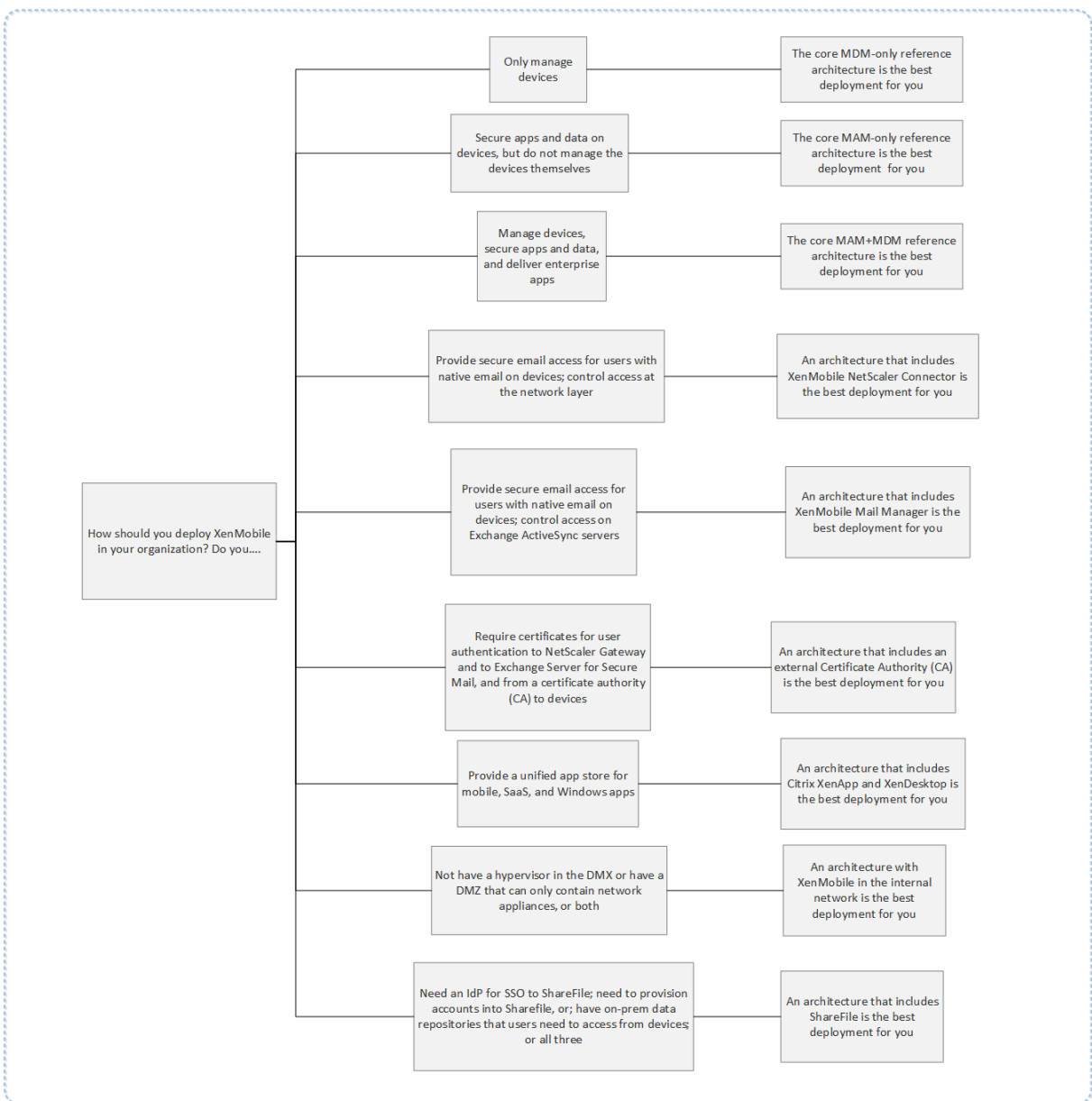
설정	설정을 찾는 위치	권장되는 설정	동작의 영향
온라인 세션 필요	MDX 정책	켜짐	장치가 온라인 상태이고 유효한 인증 토큰이 있는지 확인합니다.
온라인 세션에 필요한 유예 기간	MDX 정책	15	사용자의 앱 사용을 중지하기 전에 15 분의 유예 기간을 허용합니다.

온-프레미스 배포용 참조 아키텍처

March 15, 2024

이 문서의 그림은 XenMobile 의 온-프레미스 배포에 대한 참조 아키텍처를 설명합니다. 배포 시나리오에는 MDM 전용, MAM 전용 및 MDM+MAM 을 핵심 아키텍처로 배포하는 시나리오와 SNMP Manager, Exchange ActiveSync 용 Citrix Gateway 커넥터, Exchange ActiveSync 용 Endpoint Management 커넥터 및 Virtual Apps and Desktops 같은 구성 요소를 포함하는 배포 시나리오가 포함됩니다. 그림에는 XenMobile 에 필요한 최소 구성 요소가 나와 있습니다.

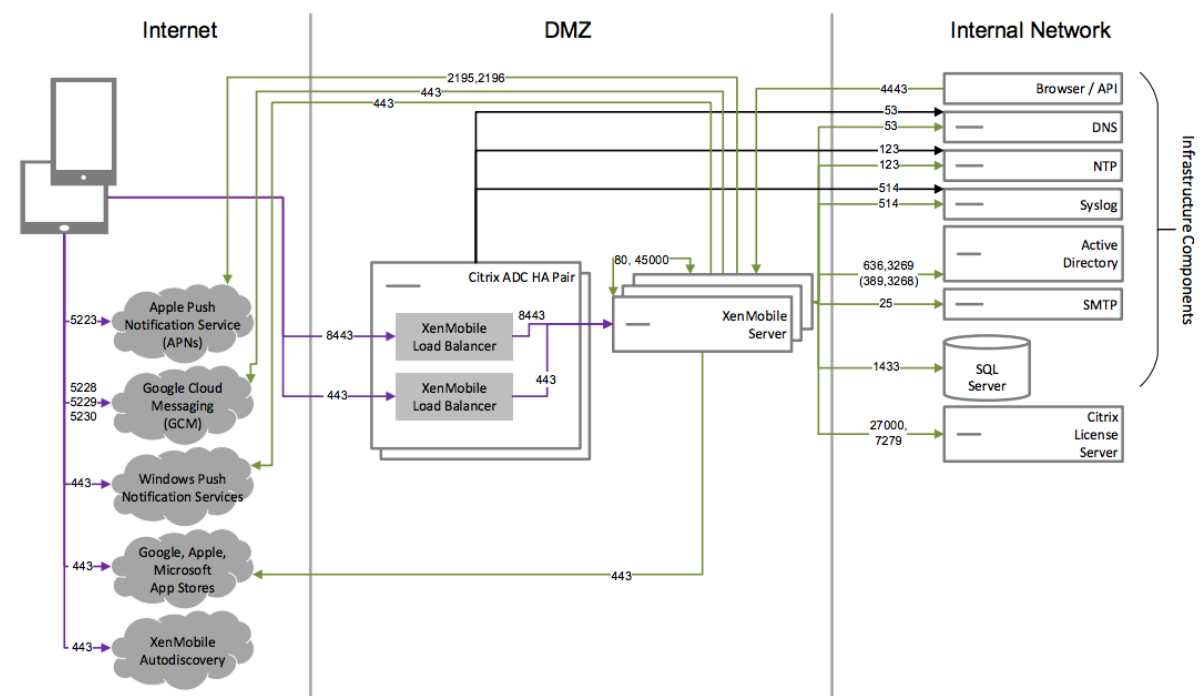
이 차트를 배포 의사 결정의 일반 지침으로 사용하십시오.



그림에서 커넥터 위의 숫자는 구성 요소 간 연결을 허용하기 위해 열어야 하는 포트를 나타냅니다. 전체 포트 목록은 XenMobile 설명서에서 [포트 요구 사항](#)을 참조하십시오.

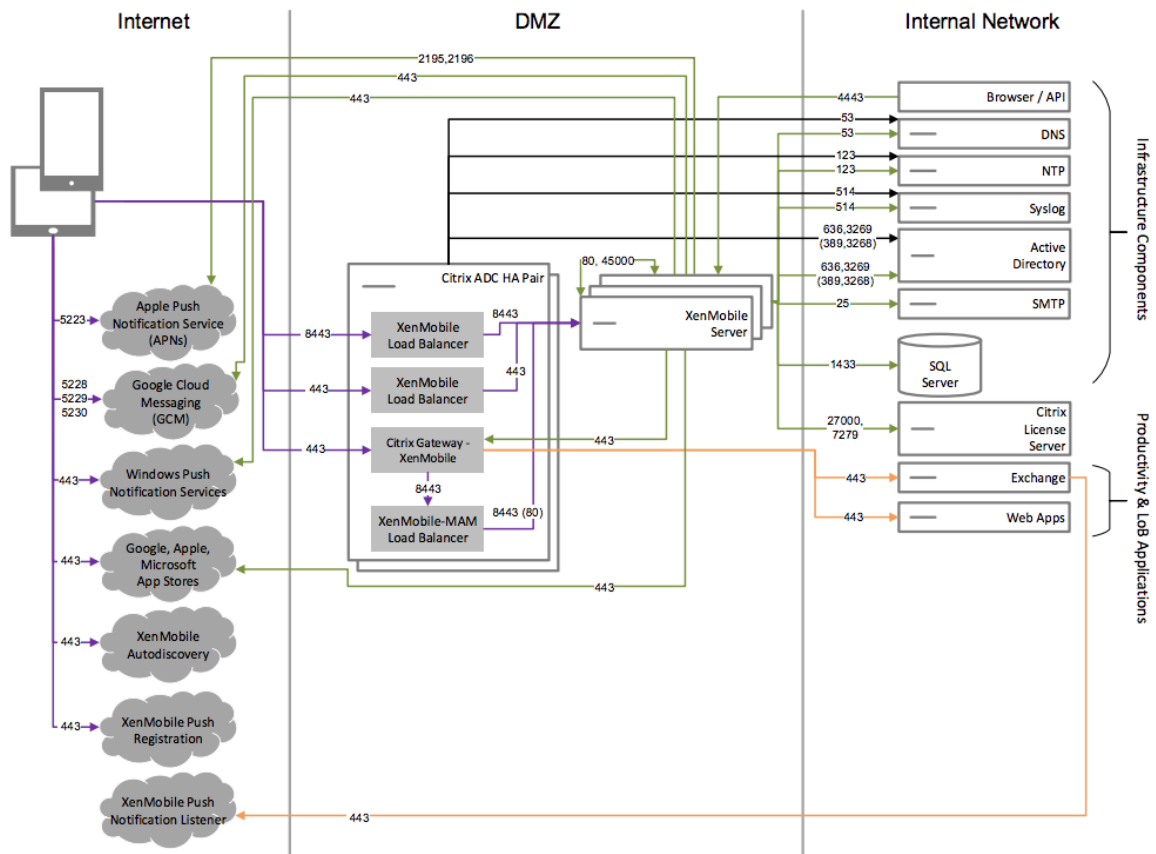
핵심 MDM 전용 참조 아키텍처

XenMobile의 MDM 기능만 사용하려는 경우 이 아키텍처를 배포합니다. 예를 들어 회사에서 발급한 장치를 MDM을 통해 관리하여 장치 정책 및 앱을 배포하고, 자산 인벤토리를 검색하고, 장치 초기화 같은 동작을 장치에 수행해야 하는 경우 이 아키텍처를 배포합니다.



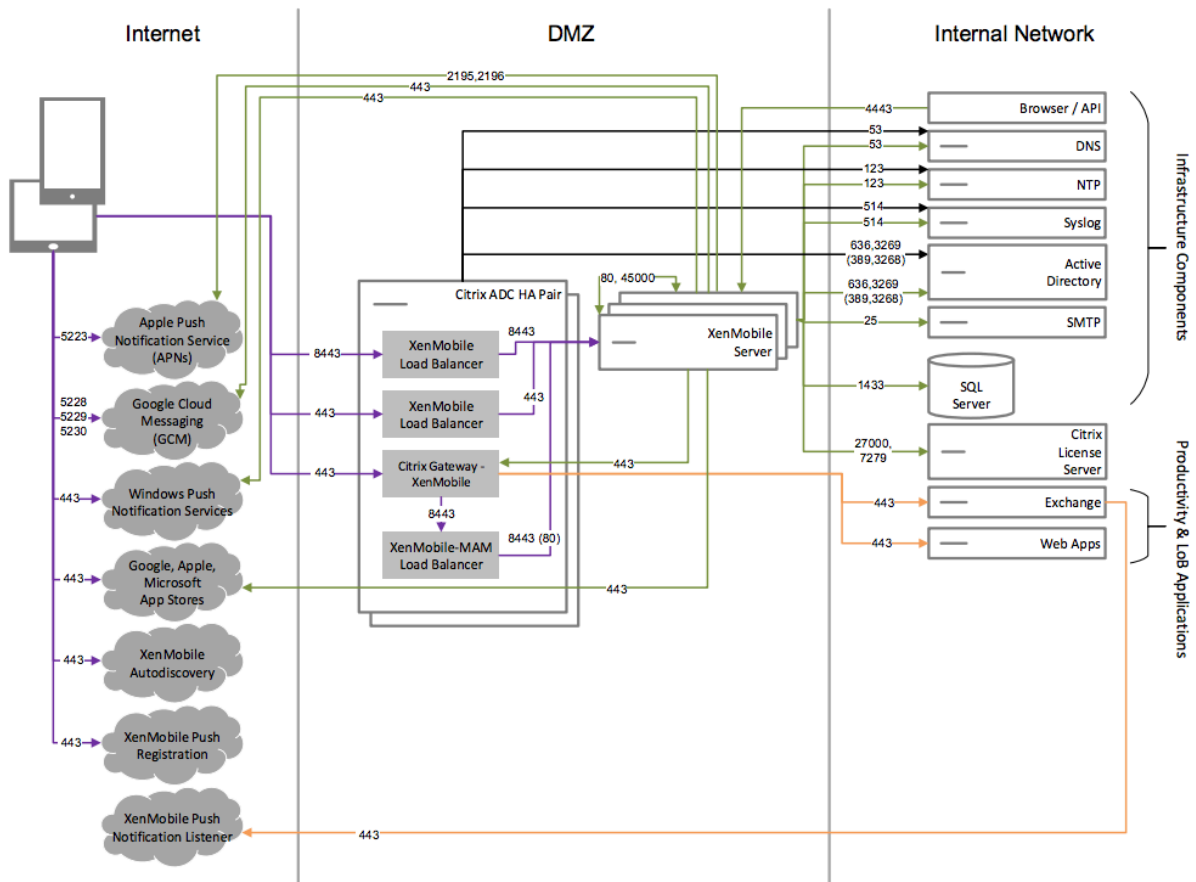
핵심 **MAM** 전용 참조 아키텍처

MDM 에 대한 장치 등록 없이 XenMobile 의 MAM 기능만 사용하려는 경우 이 아키텍처를 배포합니다. 예를 들어 BYO 모바일 장치의 앱 및 데이터를 보호하려는 경우와 엔터프라이즈 모바일 앱을 제공하고 앱 잠금 및 데이터 초기화 기능을 사용하려는 경우 이 아키텍처를 배포할 수 있습니다. 장치를 MDM 에 등록할 수 없습니다.



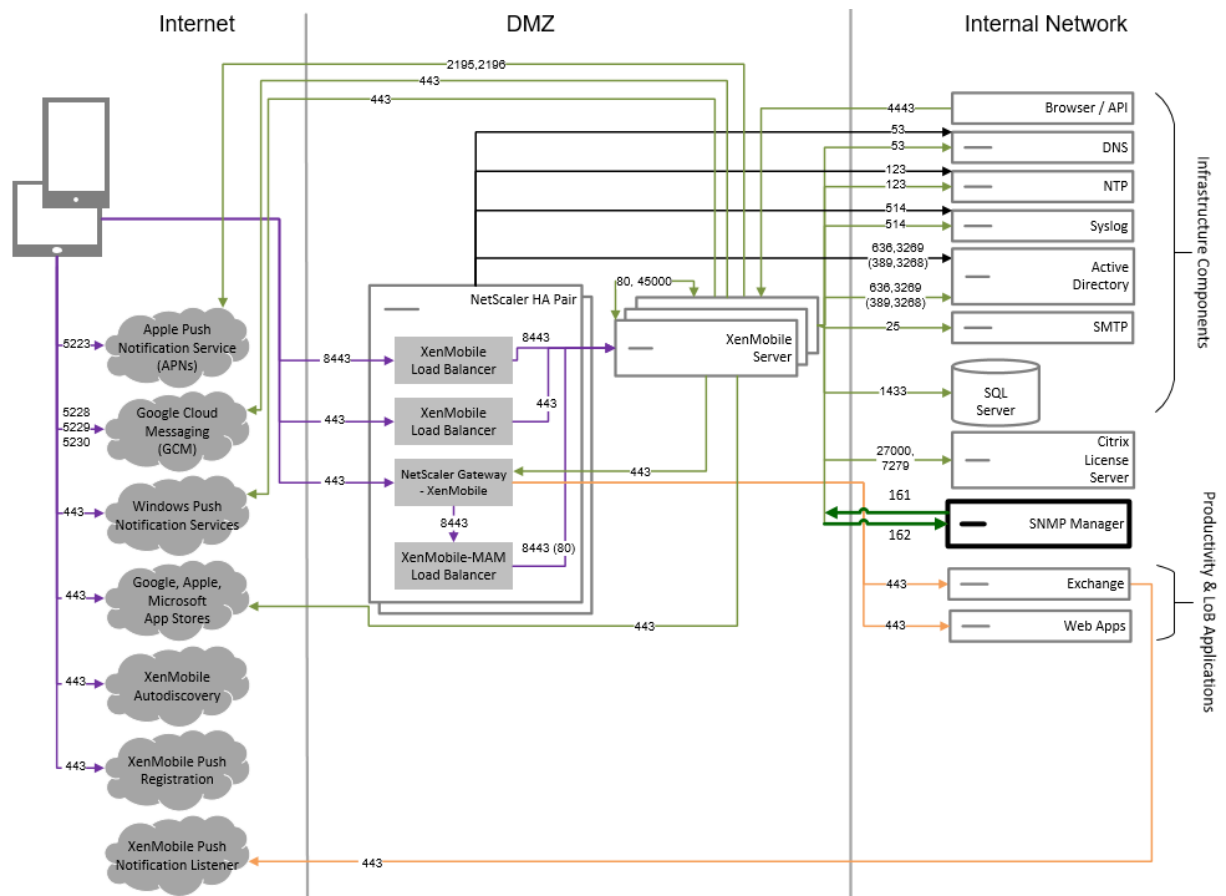
핵심 MAM+MDM 참조 아키텍처

XenMobile의 MDM+MAM 기능을 사용하려는 경우 이 아키텍처를 배포합니다. 예를 들어 회사가 발급한 장치를 MDM을 통해 관리하려는 경우, 장치 정책 및 앱을 배포하려는 경우, 자산 인벤토리를 검색하고 장치를 초기화하는 기능을 사용하려는 경우 이 아키텍처를 배포합니다. 또한 엔터프라이즈 모바일 앱을 제공하고 앱 잠금 및 장치의 데이터 초기화 기능을 사용하려는 경우에도 이 아키텍처를 배포할 수 있습니다.



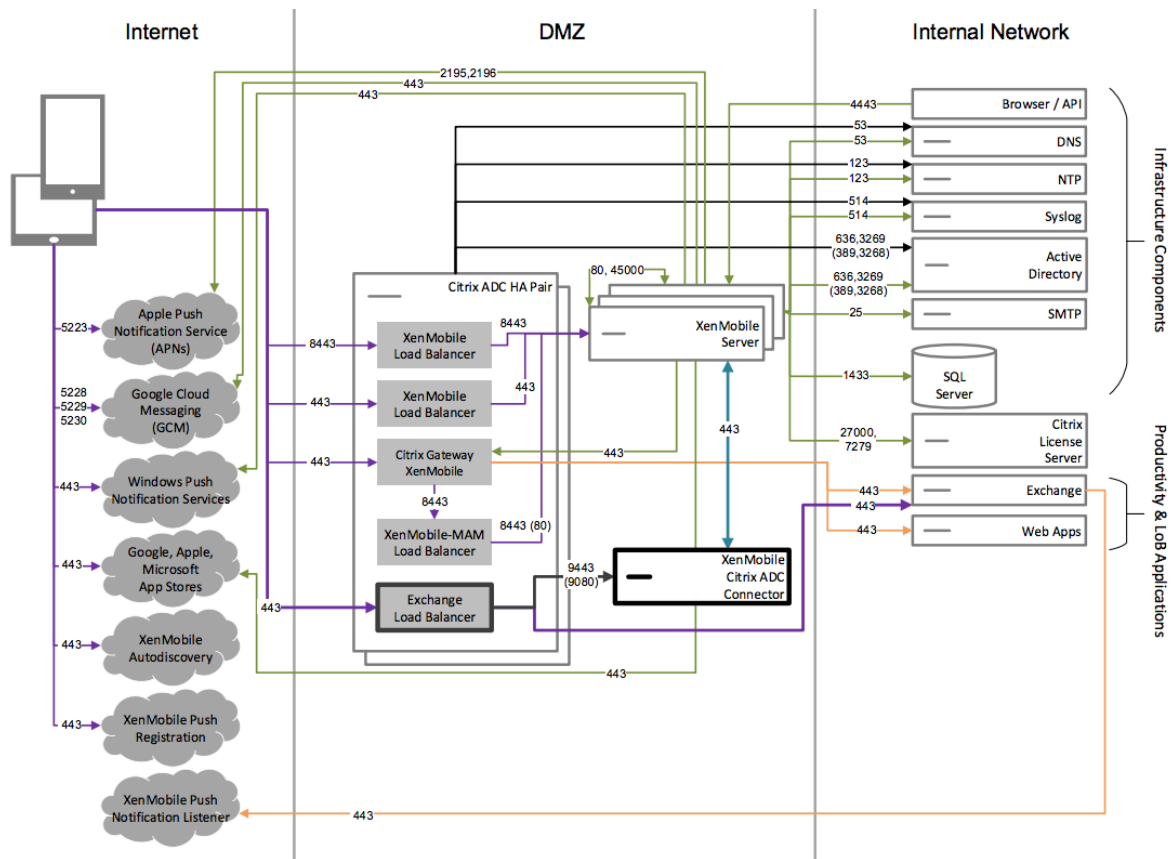
SNMP 를 사용하는 참조 아키텍처

XenMobile 과 함께 SNMP 모니터링을 사용하려는 경우 이 아키텍처를 배포합니다. 예를 들어 모니터링 시스템이 XenMobile 노드를 쿼리하고 노드의 정보를 가져오도록 허용하려는 경우 이 아키텍처를 배포할 수 있습니다. 자세한 내용은 [SNMP 모니터링](#)을 참조하십시오.



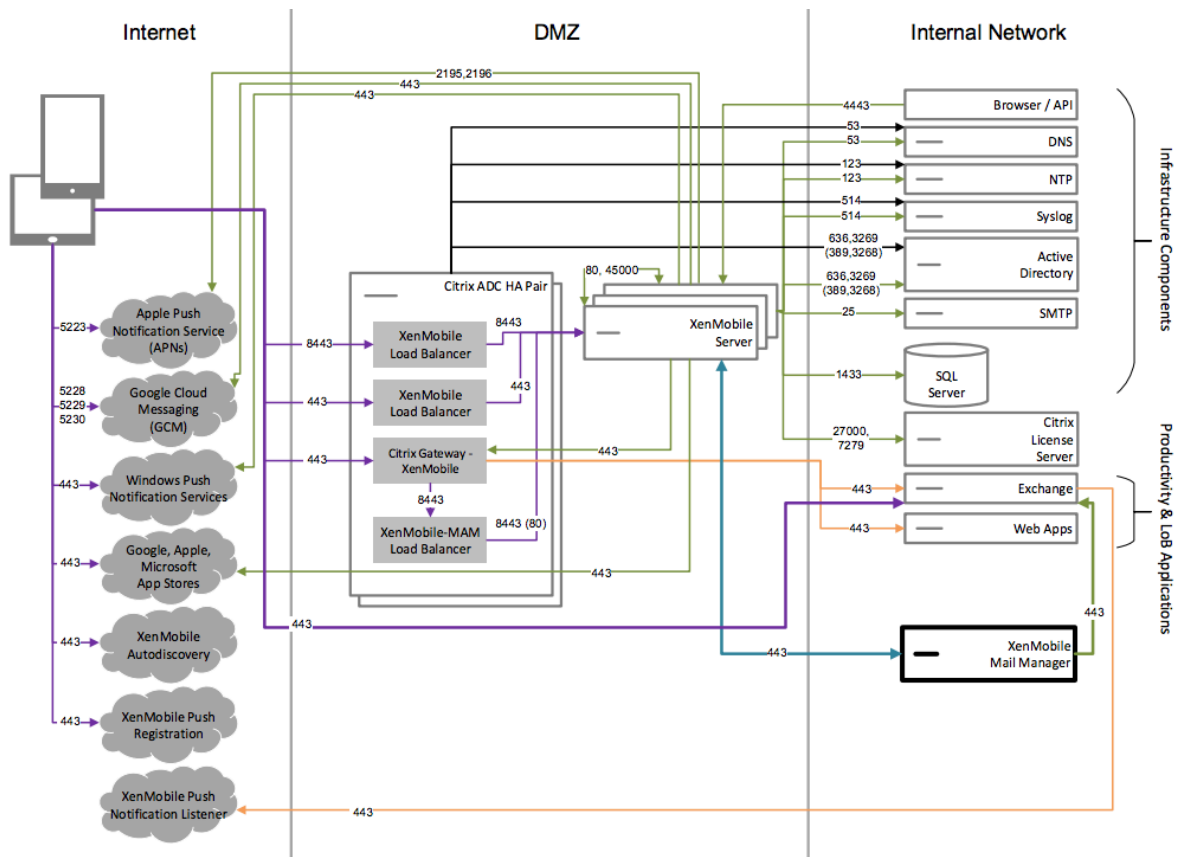
Exchange ActiveSync 용 Citrix Gateway 커넥터가 포함된 참조 아키텍처

XenMobile 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어 기본 모바일 전자 메일 앱을 사용하는 사용자에게 보안 전자 메일 액세스를 제공해야 하는 경우 이 아키텍처를 배포할 수 있습니다. 이러한 사용자는 계속해서 기본 앱을 통해 전자 메일에 액세스하거나 시간이 지남에 따라 Citrix Secure Mail 로 전환할 수 있습니다. 액세스 제어는 트래픽이 Exchange Active Sync 서버에 도달하기 전에 네트워크 계층에서 수행되어야 합니다. 다이어그램에는 Exchange ActiveSync 용 커넥터가 MDM 과 MAM 아키텍처에 배포된 것으로 표시되었지만 Exchange ActiveSync 용 커넥터를 동일한 방식으로 MDM 전용 아키텍처의 일부로 배포할 수도 있습니다.



Exchange ActiveSync 용 Endpoint Management 커넥터가 포함된 참조 아키텍처

XenMobile 에서 Exchange ActiveSync 용 Endpoint Management 커넥터를 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어 기본 모바일 전자 메일 앱을 사용하는 사용자에게 보안 전자 메일 액세스를 제공해야 하는 경우 이 아키텍처를 배포할 수 있습니다. 이러한 사용자는 계속해서 기본 앱을 통해 전자 메일에 액세스하거나 시간이 지남에 따라 Secure Mail 로 전환할 수 있습니다. 액세스 제어는 Exchange ActiveSync 서버에서 수행할 수 있습니다. 다이어그램에는 MDM 및 MAM 아키텍처에 배포된 Exchange ActiveSync 용 Endpoint Management 커넥터가 표시되어 있지만 동일한 방식으로 MDM 전용 아키텍처의 일부로 Exchange ActiveSync 용 Endpoint Management 커넥터를 배포할 수도 있습니다.

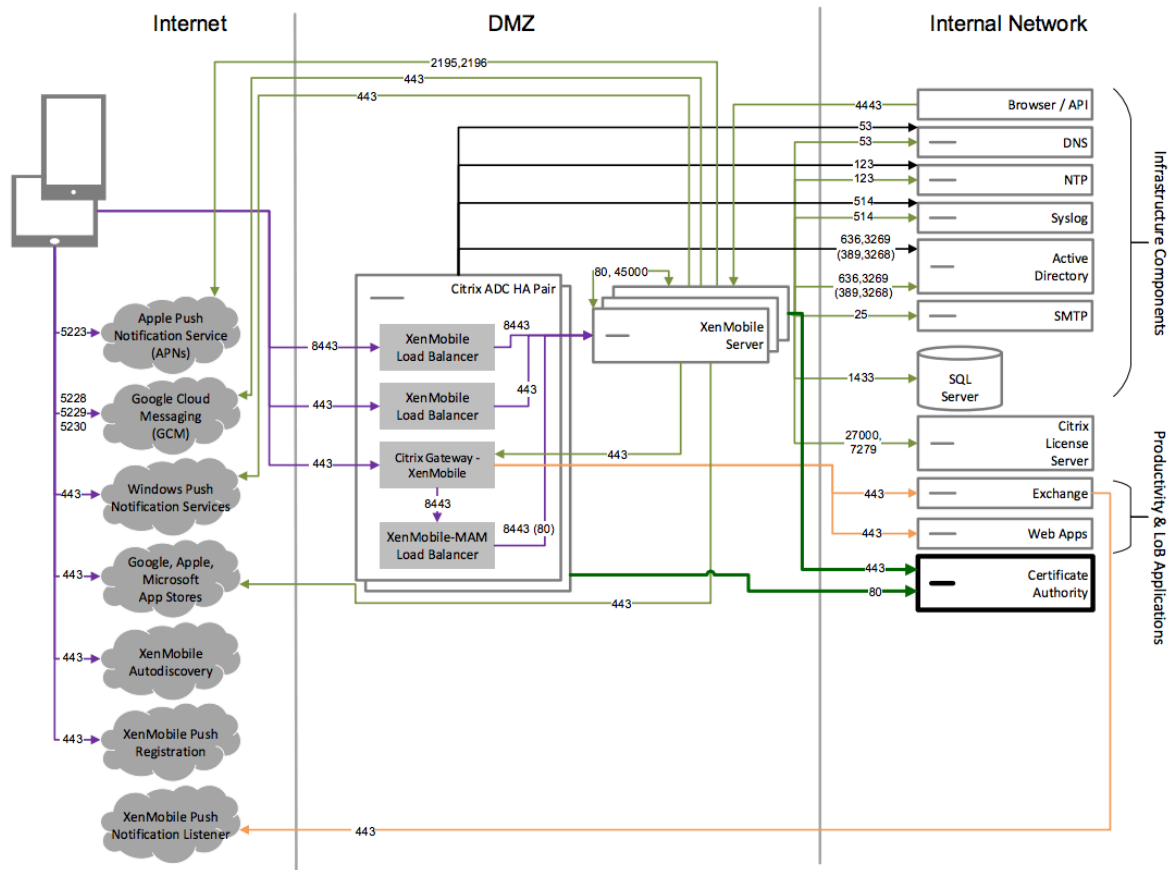


외부 인증 기관을 사용하는 참조 아키텍처

외부 인증 기관을 포함하는 배포는 다음 요구 사항을 하나 이상 충족해야 하는 경우 권장됩니다.

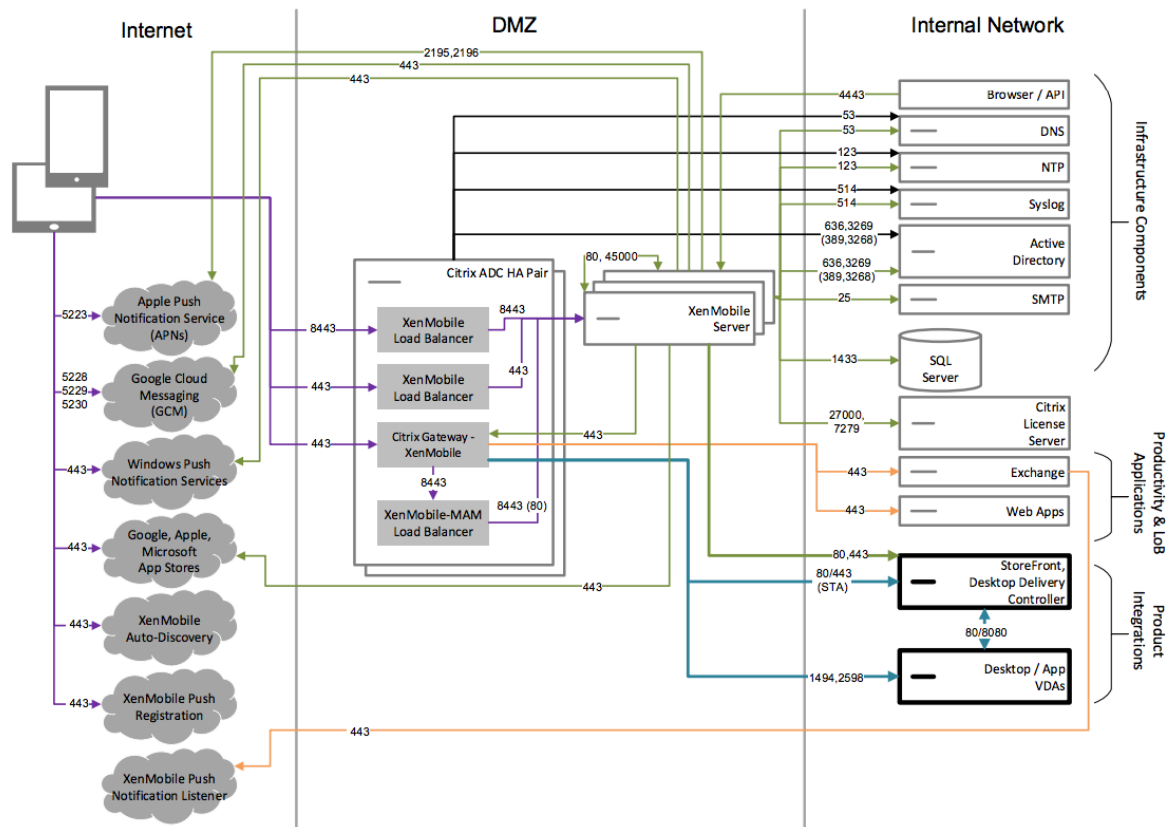
- Citrix Gateway 에 대한 사용자 인증 (인트라넷 액세스) 에 사용자 인증서를 사용해야 합니다.
- Secure Mail 사용자에게 사용자 인증서를 사용하여 Exchange Server 에 인증하도록 해야 합니다.
- 회사 인증 기관에서 발급한 인증서를 모바일 장치 (예: WiFi 액세스 시) 에 푸시해야 합니다.

다이어그램에는 MDM+MAM 아키텍처로 배포된 외부 인증 기관이 표시되어 있지만 외부 인증 기관을 동일한 방식으로 MDM 전용 또는 MAM 전용 아키텍처의 일부로 배포할 수도 있습니다.



Virtual Apps and Desktops 를 사용하는 참조 아키텍처

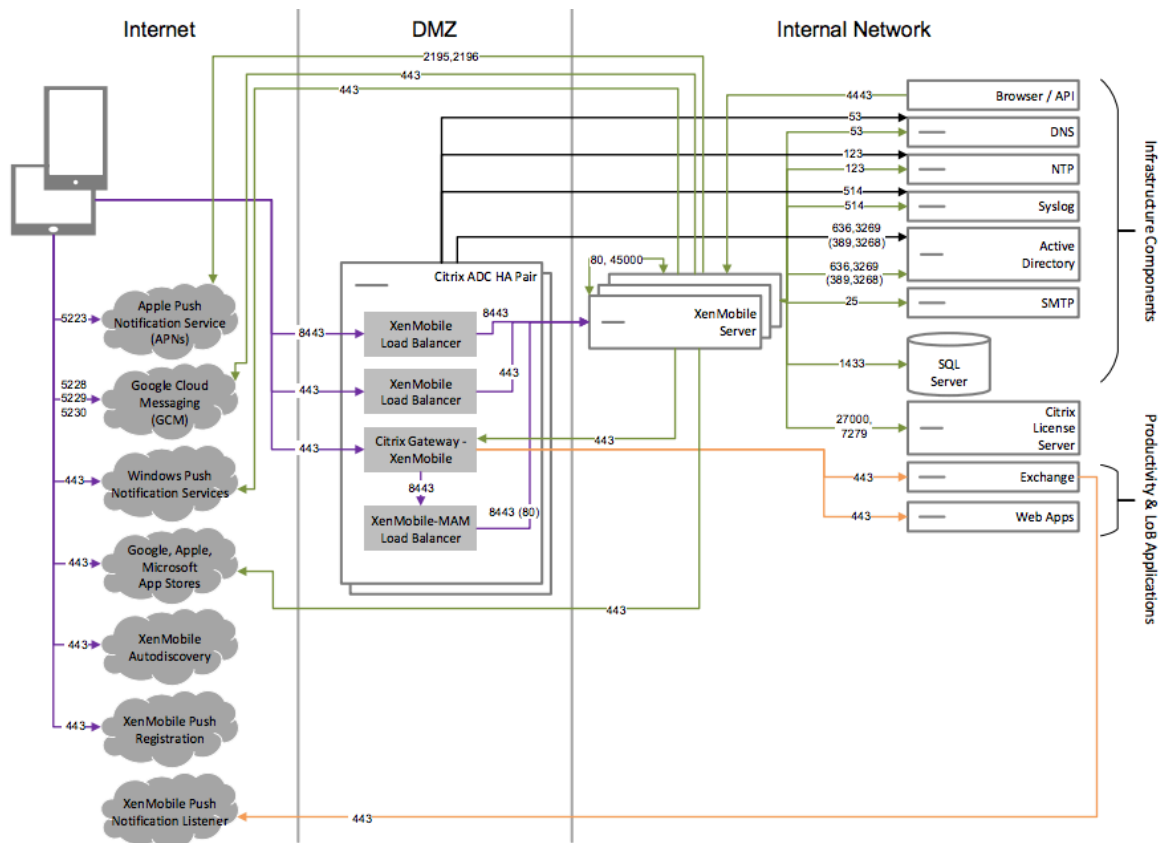
Virtual Apps and Desktops 를 XenMobile 과 통합하려는 경우 이 아키텍처를 배포합니다. 예를 들어 모바일 사용자에게 모든 유형의 응용 프로그램 (모바일, SaaS 및 Windows) 에 대한 통합 앱 스토어를 제공해야 하는 경우 이 아키텍처를 배포할 수 있습니다. 다이어그램에는 Virtula Desktops 가 MDM+MAM 아키텍처로 배포된 것으로 표시되었지만 이러한 데스크톱을 동일한 방식으로 MAM 전용 아키텍처의 일부로 배포할 수도 있습니다.



XenMobile 이 내부 네트워크에 있는 참조 아키텍처

다음 요구 사항 중 하나 이상을 충족해야 하는 경우 내부 네트워크의 XenMobile 을 사용하는 아키텍처를 배포할 수 있습니다.

- DMZ 에 하이퍼바이저가 없거나 배치할 수 없습니다.
- DMZ 에는 네트워크 장비만 포함되어야 합니다.
- 보안 요구 사항에 따라 SSL 오프로드를 사용해야 합니다.



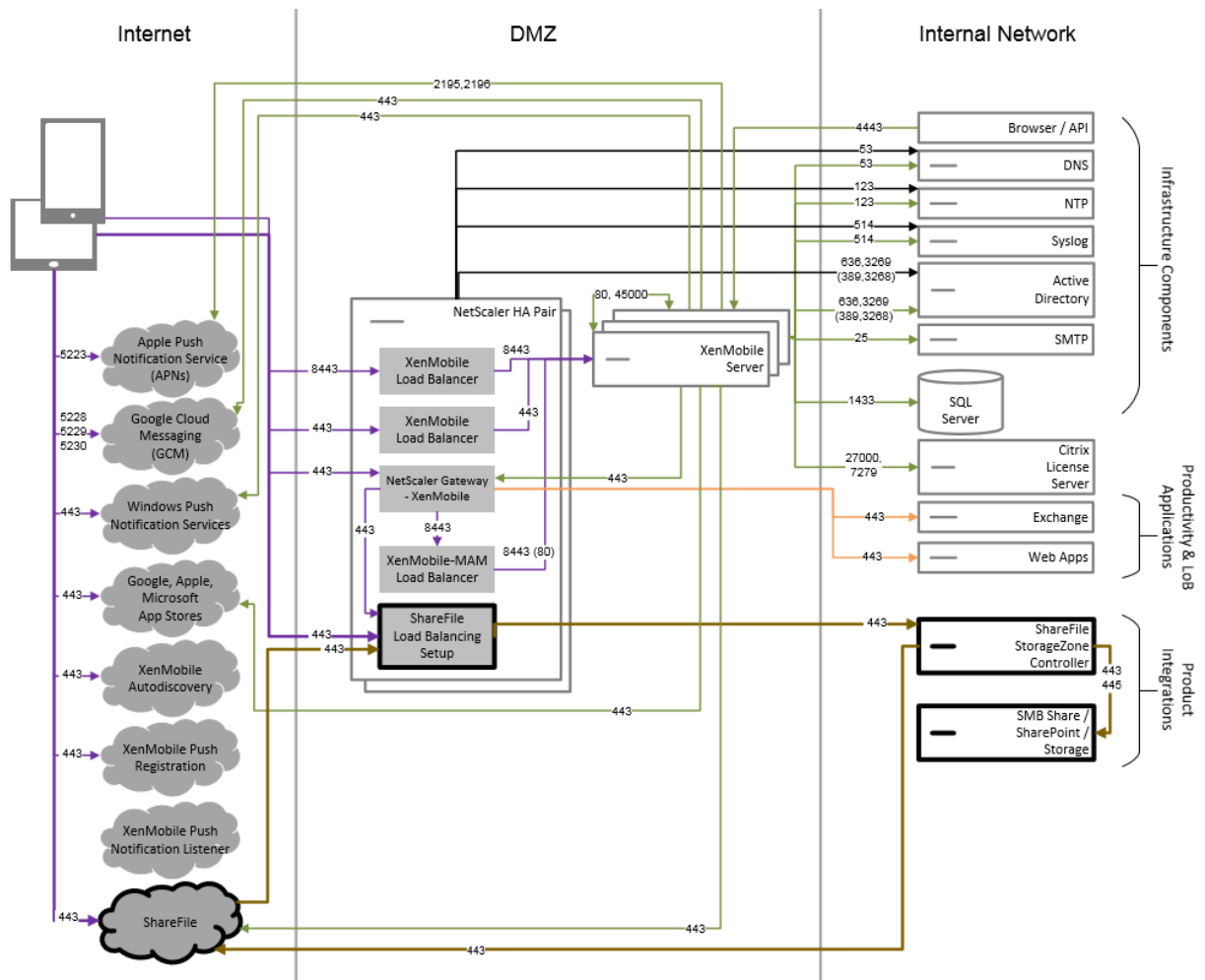
ShareFile 을 사용하는 참조 아키텍처

Citrix Files 또는 StorageZone 커넥터만 XenMobile 과 통합하려는 경우 이 아키텍처를 배포합니다. Citrix Files 를 통합 하면 다음 요구 사항 중 하나 이상을 충족할 수 있습니다.

- IdP 를 통해 ShareFile.com 에 대한 SSO(Single Sign-on) 를 사용자에게 제공해야 합니다.
- ShareFile.com 에 계정을 프로비전할 수 있어야 합니다.
- 모바일 장치에서 액세스해야 하는 온-프레미스 데이터 저장소가 있습니다.

StorageZone 커넥터만 통합하는 경우 SharePoint 사이트 및 네트워크 파일 공유 등의 기존 온-프레미스 스토리지 저장소에 대한 보안 모바일 액세스를 사용자에게 제공할 수 있습니다. 이 구성에서는 ShareFile 하위 도메인을 설정하거나, Citrix Files 에 사용자를 프로비전하거나, Citrix Files 데이터를 호스팅할 필요가 없습니다.

다이어그램에는 Citrix Files 가 MDM+MAM 아키텍처로 배포된 것으로 표시되었지만 Citrix Files 를 동일한 방식으로 MAM 전용 아키텍처의 일부로 배포할 수도 있습니다.



서버 속성

March 15, 2024

서버 속성은 전체 XenMobile 인스턴스의 작업, 사용자 및 장치에 적용되는 글로벌 속성입니다. 이 문서에서 다루는 서버 속성이 현재 환경에 해당하는지 여부를 평가하는 것이 좋습니다. 다른 서버 속성을 변경하기 전에 Citrix 에 문의하십시오.

일부 서버 속성을 변경하려면 각 XenMobile 서버 노드를 다시 시작해야 합니다. 다시 시작이 필요한 경우 XenMobile 이 알림을 제공합니다.

일부 서버 속성은 성능 및 안정성을 개선하는 데 도움이 됩니다. 자세한 내용은 [XenMobile 작업 조정](#)을 참조하십시오.

Android Enterprise 장치에 레거시 **Android** 앱 제공: `afw.allow.legacy.apps`가 **true**로 설정된 경우 Android Enterprise 장치는 레거시 Android 앱과 Android Enterprise 앱을 모두 수신합니다. **false**인 경우 Android Enterprise 장치는 Android Enterprise 앱만 수신합니다. 기본값은 **true**입니다.

파일 정책에 대한 파일 확장명 허용: 관리자가 Files 장치 정책을 사용해 업로드할 수 있는 심표로 구분된 파일 유형 목록으로 `file.extension.allowlist`를 구성합니다. 다음 파일 유형은 이 허용 목록에 추가해도 업로드할 수 없습니다.

- .cab
- .appx
- .ipa
- .apk
- .xap
- .mdx
- .exe

기본값은 `7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,miscr,pl,py,rb,sh,tcl,txt,htm,html,doc,docx,rtf,xap`입니다.

관리되는 **Google Play Store**의 모든 앱에 액세스 **true**인 경우 관리되는 Google Play Store에서 공용 Google Play Store의 모든 앱에 액세스할 수 있습니다. 이 속성을 **true**로 설정하면 모든 Android Enterprise 사용자에게 대한 공용 Google Play Store 앱이 허용됩니다. 이후 관리자는 **제한 장치 정책**을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다. **false**로 기본 설정되어 있습니다.

회사 소유 장치의 **Android Enterprise** 작업 프로필 등록: `afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled`가 **true**로 설정된 경우 Android 11 이상을 실행하는 장치는 회사 소유 장치 모드의 작업 프로필 (WPCOD)에서 등록할 수 있습니다. XenMobile Server 콘솔에는 이 등록 모드에 대한 변경 사항이 반영됩니다. **false**로 설정하면 WPCOD 설정을 사용할 수 없습니다. 기본값은 **true**입니다.

추가 **Android Enterprise** 제한 설정: `afw.restriction.policy.v2` 속성이 **true**로 설정된 경우 Android Enterprise 장치에 대해 다음과 같은 제한 설정을 사용할 수 있습니다.

- 앱 제거 허용
- Bluetooth 공유 허용

이러한 설정에 대한 자세한 내용은 **제한 장치 정책**을 참조하십시오.

COPE 장치의 **Android Enterprise** 제한: 제한 장치 정책에서 회사 소유 장치의 작업 프로필이 있는 완전 관리형 장치에 적용 설정을 사용하려면 `afw.restriction.cope`를 **true**로 설정합니다. 기본값은 **true**입니다. 이 설정에 대한 자세한 내용은 **제한 장치 정책**을 참조하십시오.

iOS App Store 링크에 호스트 이름 허용: `ios.app.store.allowed.hostnames` 속성은 공용 API를 사용하여 공용 앱 스토어 앱을 서버에 업로드할 때 허용되는 호스트 이름의 목록입니다. 서버를 통해 앱을 업로드하지 않고 공용 API를 사용하여 공용 앱 스토어 앱을 업로드할 계획이라면 이 속성을 구성하십시오. 기본값은 `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`입니다.

대체 **APN** 포트: 포트 443 대신 포트 2197을 사용하여 `api.push.apple.com`에서 APN 알림을 보내고 받을 수 있습니다. 포트는 HTTP/2 기반 APN 공급자 API를 사용합니다. 포트 2197을 사용하려면 **true** 속성을 `apns.http2.alternate.port.enabled`로 설정합니다. 서버 속성 `apns.http2.alternate.port.enabled`의 기본값은 **false**입니다.

로컬 사용자가 취약한 암호를 사용하지 못하도록 암호 유효성 검사 활성화: `enable.password.strength.validation`이 `true`로 설정되어 있으면 취약한 암호를 사용하는 로컬 사용자를 추가할 수 없습니다. `false`로 설정하면 약한 암호로 로컬 사용자를 만들 수 있습니다. 기본값은 `true`입니다.

루팅된 **Android** 및 탈옥 **iOS** 장치의 등록 차단: 이 속성이 `true`인 경우 XenMobile 은 루팅된 Android 장치와 탈옥 iOS 장치에 대한 등록을 차단합니다. 기본값은 `true`입니다. 권장되는 설정은 모든 보안 수준에 대해 `true`입니다.

등록 필요: `wsapi.mdm.required.flag` XenMobile Server 모드가 ENT 인 경우에만 적용되며 사용자의 MDM 등록을 필수로 규정할지 여부를 지정합니다. 이 속성은 XenMobile 인스턴스의 모든 사용자 및 장치에 적용됩니다. 등록이 필수이면 더 높은 수준의 보안이 제공됩니다. 그러나 이러한 결정은 MDM 을 요구할지 여부에 따라 달라집니다. 기본적으로 등록은 필수가 아닙니다.

이 속성이 `false`인 경우 사용자는 등록을 거부할 수 있으며 장치에서 XenMobile Store 를 통해 앱에 액세스할 수 있습니다. 이 속성이 `true`인 경우 등록을 거부하는 모든 사용자는 앱 액세스가 거부됩니다.

사용자 등록 후 이 속성을 변경하면 사용자가 재등록해야 합니다.

MDM 등록의 필수 여부에 대한 설명은 [장치 관리 및 MDM 등록](#)을 참조하십시오.

다중 모드 등록 지원: `enable.multimode.xms` 속성을 사용하면 Android 및 iOS 장치의 장치와 앱 모두를 관리하기 위해 등록 설정을 제어하는 하나의 XenMobile Server 에서 등록 프로필을 만들 수 있습니다. 또한, 새롭게 강화된 등록 프로필 기능은 Android 전용 장치 등록과 Android 및 iOS 장치의 MAM 전용 등록을 지원합니다. 이 속성이 `false`인 경우 등록 프로필 설정 시 이러한 등록 옵션을 사용할 수 없습니다. 기본값은 `true`입니다. 속성이 `true`일 때 등록된 장치는 속성을 `false`로 변경해도 계속 작동합니다.

자가 지원 포털 사용: `shp.console.enable`이 `false`인 경우 자가 지원 포털에 액세스할 수 없습니다. 포트 443 에서 자가 지원 포털로 이동하는 사용자에게는 404 오류가 표시됩니다. 포트 4443 에서 포털로 이동하는 사용자에게는 “액세스 거부” 메시지가 표시됩니다. `true`인 경우 포트 443 을 통해 자가 지원 포털에 액세스할 수 있습니다. `false`로 기본 설정되어 있습니다.

로컬 사용자 계정 잠금 한도: 제한 정책을 사용하여 Active Directory 사용자의 로그인 시도에 한도를 설정할 수 있습니다. `local.user.account.lockout.limit` 키를 사용하여 로컬 사용자 계정도 동일한 작업을 수행할 수 있습니다. 사용자가 지정된 횟수만큼 로그인을 시도한 후에는 일정 시간이 지나기 전까지 다시 시도할 수 없습니다. 로컬 사용자 계정 잠금 시간 속성으로 해당 시간을 구성합니다. 기본값은 6입니다.

로컬 사용자 계정 잠금 시간: `local.user.account.lockout.time` 속성을 사용하면 잠긴 로컬 사용자 계정으로 다시 로그인을 시도할 수 있기 전에 지나야 하는 시간 (분) 을 설정할 수 있습니다. 기본값은 30분입니다.

설정된 파일 업로드 최대 크기 제한: `max.file.size.upload.restriction`을 `true`로 설정하여 최대 업로드 파일 크기를 제한할 수 있습니다. 이 제한을 설정하면 `max.file.size.upload.allowed`로 최대 파일 크기를 구성할 수 있습니다. 이 속성의 기본값은 `true`입니다.

허용되는 파일 업로드 최대 크기: `max.file.size.upload.allowed`를 사용하여 업로드의 최대 파일 크기를 지정할 수 있습니다. 예시 값으로는 500 B, 1 KB, 1 MB, 1 MiB, 1 G 또는 1 GiB가 있습니다. 기본값은 5 MB입니다.

비활성 시간 제한 (분): XenMobile Server 의 공용 API 를 사용하여 XenMobile 콘솔 또는 타사 앱에 액세스한 비활성 사용

자가 XenMobile 에서 로그아웃되기까지의 시간 (분) 입니다. 시간 제한 값이 0이면 비활성 사용자가 로그인된 상태로 유지됩니다. API 에 액세스하는 타사 앱의 경우 일반적으로 로그인 유지가 필요합니다. 기본값은 5입니다.

iOS 장치 관리 등록 루트 **CA** 설치 필요: Apple 의 최신 등록 워크플로에서 사용자는 MDM 프로필을 수동으로 설치해야 합니다. Apple Business Manager 또는 Apple School Manager 에서 할당된 서버에 대한 MDM 등록에는 이 워크플로가 적용되지 않습니다. 그러나 MDM 수동 등록 중에 iOS 장치 사용자에게는 등록 중에 MDM 장치 인증서를 묻는 메시지만 표시됩니다.

수동 등록 중에 더 나은 사용자 환경을 제공할 수 있도록 `ios.mdm.enrollment.installRootCaIfRequired` 서버 속성을 **false**로 변경하는 것이 좋습니다. 기본값은 **true**입니다. 이 변경이 적용되면 MDM 등록 중에 사용자가 간편하게 프로필을 설치할 수 있는 Safari 창이 열립니다.

VPP 기준 간격: `vpp.baseline` 속성은 XenMobile 이 Apple 에서 볼륨 구매 라이선스를 다시 가져오는 최소 간격을 설정합니다. 라이선스 정보를 새로 고치면 볼륨 구매에서 가져온 앱을 수동으로 삭제하는 것과 같은 모든 변경 내용을 XenMobile 에 반영할 수 있습니다. 기본적으로 XenMobile 에서 볼륨 구매 라이선스 기준은 최소 1440분마다 새로 고쳐집니다.

설치된 볼륨 구매 라이선스가 많은 경우 (예: 50,000 개 초과) Citrix 에서는 라이선스 가져오기의 오버헤드가 줄도록 기준 간격을 늘릴 것을 권장합니다. Apple 에서 볼륨 구매 라이선스가 자주 변경될 것으로 예상되는 경우 Citrix 에서는 XenMobile 에 변경 내용이 업데이트되도록 값을 낮출 것을 권장합니다. 두 기준 사이의 최소 간격은 60 분입니다. cron 작업은 60 분마다 실행되므로 볼륨 구매 기준 간격이 60 분인 경우 기준 사이의 간격이 최대 119 분까지 지연될 수 있습니다.

XenMobile MDM 자가 지원 포털 콘솔의 최대 비활성 간격입니다 (분): 이 속성 이름에는 이전 XenMobile 버전이 반영됩니다. 이 속성은 XenMobile 콘솔의 최대 비활성 간격을 제어합니다. 이 간격은 XenMobile 콘솔에서 비활성 사용자가 로그아웃되기까지의 시간 (분) 입니다. 시간 제한이 0 인 경우 비활성 사용자가 로그인 상태로 유지됩니다. 기본값은 30입니다.

Nexmo SMS 게이트웨이에 대한 지원 중단: `deprecate.carrier.sms.gateway` 속성은 기본적으로 **True** 로 설정된 Nexmo SMS 게이트웨이에 대한 지원을 제거합니다. Nexmo SMS 는 자가 지원 포털에서도 더 이상 사용되지 않습니다.

MSP(Mobile Service Provider) 인터페이스에 대한 지원 중단: `deprecate.mobile.service.provider` 속성은 기본적으로 **True** 로 설정된 XenMobile Server 콘솔에서 MSP 인터페이스를 제거합니다.

Windows Information Protection 정책에 대한 지원 중단: Windows 발표에 따라 XenMobile Server 는 Windows Information Protection(WIP) 에 대한 지원을 중단했습니다. `windows.wip.deprecation` 서버 속성은 기본적으로 **True** 로 설정된 WIP 에 대한 지원을 제거합니다.

macOS 장치의 엔터프라이즈 앱 지원: `mac.app.push` 속성이 **True** 로 설정된 경우 macOS 를 실행하는 장치에 다운로드할 때 엔터프라이즈 앱이 자동으로 설치됩니다.

iOS 장치의 **eSIM** 지원: `ios.esim.support` 속성이 **True** 로 설정된 경우 XenMobile Server 는 iOS 장치에서 eSIM 정보를 가져와 사용자 인터페이스에 eSIM 관련 장치 속성을 표시합니다.

Android Enterprise 용 **802.1x** 설정에 대한 **Wi-Fi** 정책의 ‘도메인’ 필드 지원: `afw.network.domain.support` 속성을 **True** 로 설정하면 **Android Enterprise** 용 **802.1x** 설정에 도메인 필드가 추가됩니다.

장치 및 앱 정책

March 15, 2024

XenMobile 장치 및 앱 정책을 사용하면 다음과 같은 요소 간의 균형을 최적화할 수 있습니다.

- 엔터프라이즈 보안
- 회사 데이터 및 자산 보호
- 사용자 개인 정보 보호
- 사용자 환경의 생산성 및 품질 개선

이러한 요소 간의 최적화된 균형은 상황에 따라 다를 수 있습니다. 예를 들어 규제가 많은 조직 (예: 금융)의 경우 기본적으로 사용자 생산성이 고려되는 교육, 소매 등의 다른 업종보다 엄격한 보안 제어가 필요합니다.

사용자 ID, 장치, 위치 및 연결 유형에 따라 정책을 중앙에서 제어하고 구성하여 회사 콘텐츠의 악의적 사용을 제한할 수 있습니다. 장치의 분실 또는 도난이 발생하는 경우 비즈니스 응용 프로그램 및 데이터를 원격으로 사용하지 않도록 설정하거나, 잠그거나, 초기화할 수 있습니다. 전체적인 결과는 직원 만족도 및 생산성을 개선하는 동시에 보안 및 관리 제어를 보장하는 솔루션을 구현하는 것입니다.

이 문서에서는 보안과 관련된 다수의 장치 및 앱 정책을 중점적으로 다룹니다.

보안 위험을 해결하는 정책

XenMobile의 장치 및 앱 정책은 보안 위험을 나타낼 수 있는 다수의 상황을 해결합니다. 예를 들면 다음과 같습니다.

- 사용자가 신뢰할 수 없는 장치와 예측할 수 없는 위치에서 앱 및 데이터에 액세스를 시도하는 경우
- 사용자가 장치 간에 데이터를 이동하는 경우
- 권한이 없는 사용자가 데이터에 액세스를 시도하는 경우
- 회사에서 자신의 장치 (BYOD)를 사용한 사용자가 퇴사한 경우
- 사용자가 장치를 부적절한 장소에 두는 경우
- 사용자가 항상 안전하게 네트워크에 액세스해야 하는 경우.
- 사용자가 직접 장치를 관리하고, 관리자가 업무용 데이터와 개인용 데이터를 분리해야 하는 경우
- 유효 상태의 장치에서 사용자 자격 증명을 다시 확인해야 하는 경우
- 사용자가 중요한 콘텐츠를 복사하여 보호되지 않는 전자 메일 시스템에 붙여 넣는 경우
- 사용자가 중요한 데이터가 포함된 전자 메일 첨부 파일 또는 웹 링크를 개인 계정과 회사 계정이 모두 저장된 장치에서 수신하는 경우

이러한 상황은 다음과 같은 회사 데이터를 보호할 때 두 가지 영역과 관련하여 고려되어야 합니다.

- 유효 데이터
- 전송 중 데이터

XenMobile 이 유휴 데이터를 보호하는 방법

모바일 장치에 저장된 데이터를 유휴 데이터라고 합니다. XenMobile 은 iOS 및 Android 플랫폼에서 제공하는 장치 암호화를 사용합니다. XenMobile 은 Citrix MAM SDK 를 통해 제공되는 규정 준수 확인 등의 기능이 포함된 플랫폼 기반 암호화를 보완합니다.

XenMobile 의 MAM(모바일 응용 프로그램 관리) 기능을 사용하면 모바일 생산성 앱, MDX 사용 앱 및 연결된 데이터를 완벽하게 관리하고, 보호하고, 제어할 수 있습니다.

Mobile Apps SDK 를 사용하면 앱에서 Citrix MDX 앱 컨테이너 기술을 사용하여 XenMobile 을 배포할 수 있습니다. 컨테이너 기술은 회사 앱 및 데이터를 사용자 장치의 개인 앱 및 데이터와 분리합니다. 데이터를 분리하면 포괄적인 정책 기반 제어를 통해 사용자 지정 개발, 타사 또는 BYO 모바일 앱을 보호할 수 있습니다.

XenMobile 에는 앱 수준 암호화도 포함되어 있습니다. XenMobile 은 모든 MDX 사용 앱 안에 저장된 데이터를 개별적으로 암호화하며 장치 암호가 필요하지 않고 정책을 적용하기 위해 장치를 관리할 필요가 없습니다.

정책 및 Mobile Apps SDK 를 사용하면 다음을 수행할 수 있습니다.

- 비즈니스 앱 및 데이터와 개인용 앱 및 데이터를 안전한 모바일 컨테이너로 분리합니다.
- 암호화 및 기타 모바일 DLP(데이터 손실 방지) 기술을 사용하여 앱을 보호합니다.

MDX 정책은 다양한 운영 제어를 제공합니다. 모든 커뮤니케이션을 제어하면서 동시에 MAM SDK 사용 앱이나 MDX 래핑 앱 사이를 원활하게 통합할 수 있습니다. 이렇게 하면 MAM SDK 사용 또는 MDX 래핑 앱에서만 데이터에 액세스할 수 있도록 하는 등의 정책을 적용할 수 있습니다.

장치 및 앱 정책 제어 외에 유휴 데이터를 보호하는 가장 좋은 방법은 암호화입니다. XenMobile 은 MDX 사용 앱에 저장된 모든 데이터에 암호화 계층을 추가하여 공개 파일 암호화, 개인 파일 암호화 및 암호화 제외 같은 기능을 정책을 통해 제어할 수 있도록 합니다. Mobile Apps SDK 는 FIPS 140-2 호환 AES 256 비트 암호화와 함께 보호되는 Citrix Secret Vault 에 저장된 키를 사용합니다.

XenMobile 이 전송 중 데이터를 보호하는 방법

사용자의 모바일 장치와 회사의 내부 네트워크를 이동하는 데이터를 전송 중 데이터라고 합니다. MDX 앱 컨테이너 기술은 Citrix Gateway 를 통해 내부 네트워크에 대한 응용 프로그램별 VPN 액세스를 제공합니다.

직원이 모바일 장치에서 보안되는 기업 네트워크에 상주하는 다음 리소스에 액세스하려는 상황을 고려해 보십시오.

- 회사 전자 메일 서버
- 회사 인트라넷에서 호스팅되는 SSL 지원 웹 응용 프로그램
- 파일 서버 또는 Microsoft SharePoint 에 저장된 문서

MDX 를 사용하면 모바일 장치에서 응용 프로그램별 Micro VPN 을 통해 이 모든 엔터프라이즈 리소스에 액세스할 수 있습니다. 각 장치에는 전용 Micro VPN 터널이 생성됩니다.

Micro VPN 기능은 신뢰할 수 없는 모바일 장치의 보안을 침해할 수 있는 장치 전체 VPN 을 사용하지 않습니다. 따라서 내부 네트워크가 전체 회사 시스템을 감염시킬 수 있는 맬웨어 또는 공격에 노출되지 않습니다. 회사 모바일 앱과 개인용 모바일 앱이 한 장치에서 공존할 수 있습니다.

더 강력한 수준의 보안을 제공하려면 MDX 사용 앱을 앱 인증 및 Micro VPN 세션에 사용되는 대체 Citrix Gateway 정책으로 구성할 수 있습니다. 대체 Citrix Gateway 를 정책이 필요한 온라인 세션에서 사용하여 앱에서 특정 게이트웨이에 대한 재인증을 강제할 수 있습니다. 이러한 게이트웨이는 보통 다른 (높은 수준의 보장) 인증 요구 사항 및 트래픽 관리 정책을 가지게 됩니다.

마이크로 VPN 기능은 보안 기능 외에도 압축 알고리즘 등의 데이터 최적화 기법을 제공합니다. 압축 알고리즘으로 다음이 가능해집니다.

- 최소한의 데이터만 전송됩니다.
- 전송이 가장 빠른 시간 내에 완료됩니다. 속도는 사용자 환경을 개선하며, 이는 모바일 장치 채택의 핵심적인 성공 요인입니다.

다음과 같은 상황에서는 장치 정책을 주기적으로 재평가합니다.

- XenMobile 의 새 버전에 장치 운영 체제 업데이트 릴리스로 인한 새 정책 또는 업데이트된 정책이 포함되는 경우
- 다음과 같이 새 장치 유형을 추가하는 경우
많은 정책이 모든 장치에 공통적으로 적용되지만 각 장치에 해당 운영 체제와 관련된 일련의 정책이 있습니다. 따라서 iOS, Android 및 Windows 장치 간에는 물론 여러 제조업체의 Android 장치 사이에서도 차이가 있을 수 있습니다.
- XenMobile 작업을 엔터프라이즈 또는 산업 변경 (예: 새로운 회사 보안 정책 또는 규정 준수 규제) 과 동기화해야 하는 경우
- MAM SDK 의 새 버전에 새로운 정책 또는 업데이트된 정책이 포함되는 경우
- 앱을 추가하거나 업데이트하는 경우
- 새 앱 또는 새 요구 사항의 결과로 새로운 사용자 워크플로를 통합하려는 경우

앱 정책 및 사용 사례 시나리오

Secure Hub 를 통해 제공할 앱을 선택할 수 있지만 이러한 앱이 XenMobile 과 상호 작용하는 방식을 정의해야 할 수도 있습니다. 다음 경우에 앱 정책을 사용합니다.

- 특정 기간이 지난 후 사용자를 인증하려는 경우
- 사용자에게 정보에 대한 오프라인 액세스 권한을 제공하려는 경우

다음 섹션에는 몇 가지 정책 및 예시 사용 현황이 포함되어 있습니다.

- MAM SDK 로 iOS 및 Android 앱에 통합할 수 있는 타사 정책 목록은 [MAM SDK 개요](#)를 참고하시기 바랍니다.
- 각 플랫폼에 대한 모든 MDX 앱 정책의 목록은 [MDX 정책 요약](#)을 참조하십시오.

인증 정책

- 장치 암호

이 정책의 용도: 사용자가 장치 암호를 사용하는 장치에서만 MDX 앱에 액세스할 수 있도록 하려면 장치 암호 정책을 사용하도록 설정합니다. 이 기능은 장치 수준에서 iOS 암호화가 사용되도록 합니다.

사용자 예: 이 정책을 사용하면 사용자가 iOS 장치에서 암호를 설정해야 MDX 앱에 액세스할 수 있습니다.

- 앱 암호

이 정책의 용도: 사용자가 앱을 열고 데이터에 액세스하기 전에 관리되는 앱에 인증하라는 Secure Hub 메시지를 표시하려면 앱 암호 정책을 사용하도록 설정합니다. 사용자는 관리자가 XenMobile Server 설정의 클라이언트 속성에서 구성한 설정에 따라 Active Directory 암호, Citrix PIN 또는 iOS TouchID를 사용하여 인증할 수 있습니다. 클라이언트 속성에서 비활성 타이머를 설정하면 사용이 지속되는 동안 타이머가 다시 만료되기 전까지 Secure Hub가 관리되는 앱에 대한 사용자 인증 메시지를 표시하지 않습니다.

앱 암호는 장치 암호와 다릅니다. 장치 암호 정책이 장치에 푸시된 경우 Secure Hub는 암호 또는 PIN을 구성하라는 메시지를 표시합니다. 장치를 켜거나 비활성 타이머가 만료되는 경우 사용자는 구성된 암호 또는 PIN을 사용하여 장치 잠금을 해제해야 장치에 액세스할 수 있습니다. 자세한 내용은 배포 안내서의 [XenMobile의 인증](#)을 참조하십시오.

사용자 예: 장치에서 Citrix Secure Web 응용 프로그램을 열 때 비활성 기간이 만료된 경우 사용자가 웹 사이트를 탐색하려면 Citrix PIN을 입력해야 합니다.

- 온라인 세션 필요

이 정책의 용도: 응용 프로그램의 실행에 웹 앱 (웹 서비스) 액세스가 필요한 경우 이 정책을 사용하면 XenMobile이 앱을 사용하기 전에 엔터프라이즈 네트워크에 연결하거나 활성 세션이 있어야 한다는 내용의 메시지를 표시합니다.

사용자 예: 사용자가 온라인 세션 필요 정책을 사용하는 MDX 앱을 열려는 경우 셀룰러 또는 Wi-Fi 서비스를 사용하여 네트워크에 연결하기 전까지 앱을 사용할 수 없습니다.

- 최대 오프라인 기간

이 정책의 용도: 사용자가 오랜 시간 동안 앱을 오프라인으로 실행하는 경우 XenMobile에서 앱 권한 부여를 재확인하거나 정책을 새로 고치도록 하려면 이 정책을 추가 보안 옵션으로 사용합니다.

사용자 예: 최대 오프라인 기간을 사용하여 MDX 앱을 구성하면 사용자가 오프라인 타이머 기간이 만료되기 전까지 앱을 오프라인으로 열고 사용할 수 있습니다. 이 시점에서 메시지가 표시되면 사용자가 셀룰러 또는 Wi-Fi 서비스를 통해 네트워크에 다시 연결하고 재인증해야 합니다.

기타 액세스 정책

- 앱 업데이트 유예 기간 (시간)

이 정책의 용도: XenMobile Store에 최신 버전이 출시된 앱의 경우 사용자는 앱 업데이트 유예 기간 내에 앱을 업데이트해야 합니다. 기간이 만료되면 사용자가 앱을 업데이트해야 앱의 데이터에 액세스할 수 있습니다. 이 값을 설정할 때는 특히 해외 출장으로 인해 장시간 오프라인 상태로 유지될 수 있는 모바일 작업자의 요구 사항을 고려하십시오.

사용자 예: Secure Mail의 새 버전을 XenMobile Store에 로드한 다음 앱 업데이트 유예 기간을 6시간으로 설정합니다. 6시간이 만료되기 전에 Secure Mail 앱을 업데이트하라는 메시지가 모든 Secure Mail 사용자에게 표시됩니다. 6시간이 만료되면 Secure Hub가 사용자를 XenMobile Store로 라우팅합니다.

- **활성 폴링 기간 (분)**

이 정책의 용도: 활성 폴링 기간은 앱 잠금, 앱 초기화 등의 보안 동작을 수행하기 위해 XenMobile 이 앱을 확인하는 간격입니다.

사용자 예: 활성 폴링 기간 정책을 60 분으로 설정한 경우 앱 잠금 명령을 XenMobile 에서 장치로 전송하면 마지막 폴링 시간으로부터 60 분 내에 잠금이 수행됩니다.

규정을 준수하지 않는 장치 동작 정책

장치가 최소 규정 준수 요구 사항을 충족하지 못하는 경우 규정을 준수하지 않는 장치 동작 정책을 사용하여 수행할 작업을 선택할 수 있습니다. 자세한 내용은 [규정을 준수하지 않는 장치 동작](#)을 참조하십시오.

앱 상호 작용 정책

이 정책의 용도: MDX 앱에서 장치의 다른 앱으로 이동하는 문서 및 데이터의 흐름을 제어하려면 앱 상호 작용 정책을 사용합니다. 예를 들어 사용자는 컨테이너 외부의 개인용 앱으로 데이터를 이동하거나 컨테이너 외부의 데이터를 컨테이너화된 앱에 붙여 넣을 수 없습니다.

사용자 예: 앱 상호 작용 정책을 제한됨으로 설정하면 사용자가 Secure Mail 의 텍스트를 Secure Web 에 복사할 수 있지만 이 데이터를 컨테이너 외부의 개인용 Safari 또는 Chrome 브라우저에 복사할 수 없습니다. 또한 사용자는 Secure Mail 의 첨부 문서를 Citrix Files 또는 Quick Edit 에서 열 수 있지만 컨테이너 외부의 개인용 파일 보기 앱에서는 이 첨부 문서를 열 수 없습니다.

앱 제한 정책

이 정책의 용도: MDX 앱이 열려 있는 동안 사용자가 액세스할 수 있는 기능을 제어하려면 앱 제한 정책을 사용합니다. 이 정책을 사용하면 앱이 실행되는 동안 악의적인 활동을 수행할 수 없습니다. 앱 제한 정책은 iOS 와 Android 에서 조금 다릅니다. 예를 들어 iOS 에서는 MDX 앱이 실행되는 동안 iCloud 에 대한 액세스를 차단할 수 있습니다. Android 에서는 MDX 앱이 실행되는 동안 NFC 사용을 중지할 수 있습니다.

사용자 예: 앱 제한 정책을 사용하여 iOS 의 MDX 앱에서 받아쓰기를 차단하는 경우 사용자는 MDX 앱이 실행되는 동안 iOS 키보드에서 받아쓰기 기능을 사용할 수 없습니다. 따라서 사용자가 받아쓰 데이터가 보안되지 않은 타사 클라우드 받아쓰기 서비스로 전달되지 않습니다. 사용자가 컨테이너 외부의 개인용 앱을 열 때는 개인 커뮤니케이션용으로 받아쓰기 옵션을 사용할 수 있습니다.

앱 네트워크 액세스 정책

이 정책의 용도: 장치의 컨테이너에 있는 MDX 앱에서 회사 네트워크 안의 데이터에 액세스할 수 있도록 하려면 앱 네트워크 액세스 정책을 사용합니다. 네트워크 액세스 정책에서 내부 네트워크로 터널링된 옵션을 설정하면 MDX 앱에서 Citrix ADC 를 통한 백엔드 웹 서비스 또는 데이터 저장소로의 Micro VPN 이 자동화됩니다.

사용자 예: 사용자가 터널링을 사용하는 MDX 앱 (예: Secure Web) 을 열면 사용자가 VPN 을 시작하지 않아도 브라우저가 열리고 인트라넷 사이트가 시작됩니다. Secure Web 앱이 Micro VPN 기술을 사용하여 내부 사이트에 자동으로 액세스합니다.

앱 지오로케이션 및 지오펜스 정책

이 정책의 용도: 앱 지오로케이션 및 지오펜스를 제어하는 정책에는 중심점 경도, 중심점 위도 및 반경이 포함됩니다. 이러한 정책은 MDX 앱의 데이터에 대한 액세스를 특정 지리적 영역으로 제한합니다. 정책은 위도 및 경도 좌표의 반경을 사용하여 지리적 영역을 정의합니다. 사용자가 정의된 반경 밖에서 앱을 사용하려고 하면 앱이 잠긴 상태로 유지되고 사용자가 앱 데이터에 액세스할 수 없습니다.

사용자 예: 사용자는 사무실 위치에 있는 동안 합병 및 인수 데이터에 액세스할 수 있습니다. 사무실 위치 밖으로 이동하면 이 중요한 데이터에 액세스할 수 없게 됩니다.

Secure Mail 앱 정책

- 백그라운드 네트워크 서비스

이 정책의 용도: Secure Mail 의 백그라운드 네트워크 서비스는 실질적으로 SOCKS5 프록시인 STA(Secure Ticket Authority) 를 활용하여 Citrix Gateway 를 통해 연결합니다. STA 는 오래 유지되는 연결을 지원하며 Micro VPN 에 비해 개선된 배터리 수명을 제공합니다. 따라서 STA 는 지속적으로 연결되는 메일에 적합합니다. Secure Mail 을 사용하는 경우 이러한 설정을 구성하는 것이 좋습니다. XenMobile 용 Citrix ADC 마법사는 Secure Mail 에 대해 자동으로 STA 를 설정합니다.

사용자 예: STA 가 사용되지 않는 경우 Android 사용자가 Secure Mail 을 열면 VPN 을 열라는 메시지가 표시됩니다. VPN 은 장치에서 열린 상태로 유지됩니다. STA 가 사용되는 경우 Android 사용자가 Secure Mail 을 열면 Secure Mail 이 VPN 없이 원활하게 연결됩니다.

- 기본 동기화 간격

이 정책의 용도: 이 설정은 사용자가 Secure Mail 에 처음으로 액세스할 때 Secure Mail 과 동기화되는 전자 메일의 기본 일 수를 지정합니다. 참고로 2 주간의 전자 메일은 3 일보다 동기화가 오래 걸리며 사용자 설정 프로세스가 길어집니다.

사용자 예: 사용자가 Secure Mail 을 처음 설정할 때 기본 동기화 간격을 3 일로 설정하면 현재부터 지난 3 일까지 받은 전자 메일이 받은 편지함에 표시됩니다. 사용자가 3 일 전의 전자 메일을 보려는 경우 검색을 수행할 수 있습니다. 그러면 Secure Mail 이 서버에 저장된 이전 전자 메일을 표시합니다. Secure Mail 을 설치한 후 각 사용자는 요구 사항에 적합하게 이 설정을 변경할 수 있습니다.

장치 정책 및 사용 사례 동작

장치 정책은 MDM 정책이라고도 하며 XenMobile 이 장치에서 작동하는 방식을 결정합니다. 많은 정책이 모든 장치에 공통적으로 적용되지만 각 장치에 해당 운영 체제와 관련된 일련의 정책이 있습니다. 다음 목록에는 일부 장치 정책과 정책을 사용하는 방법이 포함되어 있습니다. 모든 장치 정책의 목록은 [장치 정책](#) 아래 문서를 참조하십시오.

- 앱 인벤토리 정책

이 정책의 용도: 사용자에게 의해 설치된 앱을 확인해야 하는 경우 장치에 앱 인벤토리 정책을 배포합니다. 앱 인벤토리 정책을 배포하지 않은 경우 사용자가 XenMobile Store 에서 설치한 앱만 표시되며 개인적으로 설치한 응용 프로그램은 표시되지 않습니다. 회사 장치에서 실행할 수 없는 특정 앱을 차단하려는 경우 이 정책을 사용해야 합니다.

사용자 예: MDM 으로 관리되는 장치의 사용자는 이 기능을 사용하지 않도록 설정할 수 없습니다. 사용자가 개인적으로 설치한 응용 프로그램이 XenMobile 관리자에게 표시됩니다.

- 앱 잠금 정책

이 정책의 용도: Android 용 앱 잠금 정책을 사용하면 앱을 차단하거나 허용할 수 있습니다. 예를 들어 앱을 허용하여 키오스크 장치를 구성할 수 있습니다. 일반적으로 앱 잠금 정책은 사용자가 설치할 수 있는 앱을 제한하므로 회사 소유 장치에만 배포됩니다. 재정의 암호를 설정하여 차단된 앱에 대한 사용자 액세스를 제공할 수 있습니다.

사용자 예: Angry Birds 앱을 차단하는 앱 잠금 정책을 배포한다고 가정할 경우 사용자는 Angry Birds 앱을 Google Play 에서 설치할 수 있지만 앱을 열면 관리자가 앱을 차단했다는 내용의 메시지가 표시됩니다.

- 연결 예약 정책

이 정책의 용도: Windows Mobile 장치에서 MDM 관리, 앱 푸시 및 정책 배포를 위해 XenMobile Server 에 다시 연결할 수 있도록 하려면 연결 예약 정책을 사용해야 합니다. Android, Android Enterprise 및 Chrome OS 장치의 경우 이 정책 대신 Google FCM(Firebase Cloud Messaging) 을 사용하여 XenMobile Server 에 대한 연결을 제어합니다. 예약 옵션은 다음과 같습니다.

- 항상: 연결을 영구적으로 활성 상태로 유지합니다. 보안을 최적화하려면 이 옵션을 사용하는 것이 좋습니다. 항상을 선택하는 경우 연결로 인해 배터리가 소진되지 않도록 연결 타이머 정책도 사용하십시오. 연결을 활성 상태로 유지하면 초기화 또는 잠금과 같은 보안 명령을 주문형으로 장치에 푸시할 수 있습니다. 또한 장치에 배포하는 각 정책에서 배포 일정 옵션 상시 연결에 대해 배포를 선택해야 합니다.
- 안 함: 수동으로 연결합니다. 안 함 옵션을 사용하면 보안 정책을 장치에 배포할 수 없어 사용자가 새 앱 또는 정책을 받을 수 없으므로 프로덕션 배포에 사용하지 않는 것이 좋습니다.
- 매: 지정된 간격으로 연결합니다. 이 옵션이 적용될 때 잠금 또는 초기화와 같은 보안 정책을 전송하면 다음번 장치 연결 시 XenMobile 에서 정책이 처리됩니다.
- 일정 정의: 사용하면 네트워크 연결이 끊긴 후 XenMobile 이 사용자 장치를 XenMobile Server 에 다시 연결하고 제어 패킷을 정의된 시간 내에 정기적으로 전송하여 연결을 모니터링합니다.

사용자 예: 등록된 장치에 암호 정책을 배포하려고 합니다. 예약 정책을 사용하면 장치가 정기적인 간격으로 서버에 다시 연결하여 새 정책을 수집합니다.

- 자격 증명 정책

이 정책의 용도: 주로 WiFi 정책과 함께 사용됩니다. 자격 증명 정책을 사용하면 인증서 인증이 필요한 내부 리소스에 대한 인증에 사용할 인증서를 배포할 수 있습니다.

사용자 예: 장치의 무선 네트워크를 구성하는 Wi-Fi 정책을 배포합니다. Wi-Fi 네트워크를 사용하려면 인증서로 인증해야 합니다. 자격 증명 정책은 인증서를 배포하고 배포된 인증서는 운영 체제 키 저장소에 저장됩니다. 그러면 사용자가 내부 리소스에 연결할 때 인증서를 선택할 수 있습니다.

- **Exchange 정책**

이 정책의 용도: XenMobile에서는 두 가지 옵션을 사용하여 Microsoft Exchange ActiveSync 전자 메일을 전송할 수 있습니다.

- **Secure Mail 앱:** 공용 앱 스토어 또는 XenMobile Store에서 배포하는 Secure Mail 앱을 사용하여 전자 메일을 전송합니다.
- **기본 전자 메일 앱:** 장치의 기본 전자 메일 클라이언트에서 ActiveSync 전자 메일을 사용하도록 설정하려면 Exchange 정책을 사용합니다. 기본 전자 메일에 대한 Exchange 정책을 사용하는 경우 Active Directory 특성에서 사용자 데이터를 채우는 매크로를 사용할 수 있습니다. 예를 들어 `${user.username}` 을 사용하여 사용자 이름을 채우고 `${user.domain}` 을 사용하여 사용자 도메인을 채울 수 있습니다.

사용자 예: Exchange 정책을 푸시할 때 Exchange Server 세부 정보를 장치에 전송합니다. 그러면 Secure Hub가 인증 메시지를 표시하고 전자 메일 동기화가 시작됩니다.

- **위치 정책**

이 정책의 용도: 위치 정책을 사용하면 장치가 Secure Hub에 대한 GPS를 사용하는 경우 지도에서 장치의 위치를 찾을 수 있습니다. 이 정책을 배포한 후 XenMobile Server에서 위치 명령을 보내면 장치가 위치 좌표를 사용하여 응답합니다.

사용자 예: 위치 정책이 배포되고 GPS가 장치에서 사용되는 경우 장치를 찾지 못하는 사용자는 XenMobile자가 지원 포털에 로그인하고 찾기 옵션을 선택하여 지도에서 장치의 위치를 확인할 수 있습니다. 사용자는 Secure Hub에서 위치 서비스를 사용할 수 있도록 선택해야 합니다. 사용자가 직접 장치를 등록하는 경우 관리자는 위치 서비스 사용을 적용할 수 없습니다. 이 정책을 사용할 때는 배터리 수명에 미치는 영향도 고려해야 합니다.

- **암호 정책**

이 정책의 용도: 암호 정책을 사용하면 관리되는 장치에 PIN 코드 또는 암호를 적용할 수 있습니다. 이 암호 정책을 사용하면 장치에 암호에 대한 복잡성 및 시간 초과를 설정할 수 있습니다.

사용자 예: 관리되는 장치에 암호 정책을 배포하면 Secure Hub가 암호 또는 PIN을 구성하라는 메시지를 표시합니다. 장치를 켜거나 비활성 타이머가 만료되는 경우 사용자는 구성된 암호 또는 PIN을 사용하여 장치 잠금을 해제해야 장치에 액세스할 수 있습니다.

- **프로필 제거 정책**

이 정책의 용도: 사용자 그룹에 정책을 배포하고 나중에 일부 사용자에게서 정책을 제거해야 하는 경우 프로필 제거 정책을 만들고 프로필 제거 정책을 지정된 사용자 이름에만 배포하는 배포 규칙을 사용하여 선택한 사용자에 대한 정책을 제거할 수 있습니다.

사용자 예: 프로필 제거 정책을 사용자 장치에 배포하는 경우 사용자는 변경 내용을 알지 못할 수 있습니다. 예를 들어 프로필 제거 정책이 장치 카메라를 사용할 수 없도록 하는 제한을 제거하는 경우 사용자는 카메라 사용이 허용된 것을 알지 못합니다. 사용자 경험에 영향을 미치는 변경이 발생하는 경우 해당 사항을 사용자에게 알려주는 것이 좋습니다.

- **제한 정책**

이 정책의 용도: 제한 정책은 관리되는 장치의 기능을 잠그고 제어할 수 있는 다수의 옵션을 제공합니다. 지원되는 장치에 대한 수백 가지 제한 옵션을 사용할 수 있으며 여기에는 장치의 카메라 또는 마이크 사용을 제한하는 옵션부터 앱 스토어 같은 타사 서비스에 대한 로밍 규칙 및 액세스를 적용하는 옵션이 포함됩니다.

사용자 예: iOS 장치에 제한을 배포하는 경우 사용자는 iCloud 또는 Apple App Store 에 액세스하지 못할 수 있습니다.

- **약관 정책**

이 정책의 용도: 관리자는 장치 관리와 관련된 법적 영향을 사용자에게 알려야 할 수 있습니다. 또한 회사 데이터를 장치에 푸시할 때의 보안 위험을 사용자가 숙지할 수 있도록 해야 합니다. 사용자가 등록하기 전에 관리자는 사용자 지정 약관 문서를 사용하여 규칙 및 고지 사항을 게시할 수 있습니다.

사용자 예: 사용자 등록 프로세스 중에 약관 정보가 표시됩니다. 사용자가 명시된 조건에 동의하지 않으면 등록 프로세스가 종료되고 사용자는 회사 데이터에 액세스할 수 없게 됩니다. 약관에 동의하거나 거부한 사용자를 보여주는 보고서를 생성하여 HR/법무/규정 준수 팀에 제공할 수 있습니다.

- **VPN 정책**

이 정책의 용도: 이전 VPN Gateway 기술을 사용하여 백엔드 시스템에 대한 액세스를 제공하려면 VPN 정책을 사용합니다. 이 정책은 Cisco AnyConnect, Juniper 및 Citrix VPN 을 포함하는 다수의 VPN 공급자를 지원합니다. VPN 게이트웨이가 이 옵션을 지원하는 경우 이 정책을 CA 에 연결하고 주문형 VPN 을 사용하도록 설정할 수도 있습니다.

사용자 예: VPN 정책을 사용하면 사용자가 내부 도메인에 액세스할 때 사용자 장치에서 VPN 연결이 열립니다.

- **웹 클립 정책**

이 정책의 용도: 웹 사이트를 직접 여는 아이콘을 장치에 푸시하려면 웹 클립 정책을 사용합니다. 웹 클립에는 웹 사이트 링크가 포함되며 사용자 지정 아이콘을 포함할 수 있습니다. 장치에서 웹 클립은 앱 아이콘처럼 표시됩니다.

사용자 예: 사용자는 웹 클립 아이콘을 클릭하여 액세스가 필요한 서비스를 제공하는 인터넷 사이트를 열 수 있습니다. 웹 링크를 사용하면 브라우저 앱을 열고 링크 주소를 입력하는 것보다 편리합니다.

- **WiFi 정책**

이 정책의 용도: Wi-Fi 정책을 사용하면 SSID, 인증 데이터 및 구성 데이터 같은 Wi-Fi 네트워크 세부 정보를 관리되는 장치에 배포할 수 있습니다.

사용자 예: Wi-Fi 정책을 배포하면 장치가 자동으로 Wi-Fi 네트워크에 연결되고 사용자를 인증합니다. 인증된 사용자는 네트워크에 액세스할 수 있습니다.

- **Windows Information Protection 정책**

이 정책의 용도: 엔터프라이즈 데이터의 잠재적 유출을 방지하려면 WIP(Windows Information Protection) 정책을 사용합니다. 설정한 적용 수준에서 Windows Information Protection 이 필요한 앱을 지정할 수 있습니다. 예를 들어 부적절한 데이터 공유를 차단하거나 부적절한 데이터 공유에 대해 경고를 표시하고 사용자의 정책 재정의 허용할 수 있습니다. 부적절한 데이터 공유를 로깅하고 허용하는 동안 WIP 를 자동으로 실행할 수 있습니다.

사용자 예: 부적절한 데이터 공유를 차단하는 WIP 정책을 구성하는 경우 사용자가 보호되는 파일을 보호되지 않는 위치로 복사하거나 저장하면 보호되는 콘텐츠가 포함된 작업을 이 위치에 배치할 수 없다는 내용의 메시지가 표시됩니다.

• XenMobile Store 정책

이 정책의 용도: XenMobile Store 는 관리자가 사용자에게 필요한 모든 회사 앱 및 데이터 리소스를 게시할 수 있는 통합 앱 스토어입니다. 관리자는 다음을 추가할 수 있습니다.

- 웹 앱, SaaS 앱, MAM SDK 사용 앱 또는 MDX 래핑 앱
- Citrix 모바일 생산성 앱
- .ipa 또는 .apk 파일과 같은 기본 모바일 앱
- Apple App Store 및 Google Play 앱
- 웹 링크
- Citrix StoreFront 로 게시된 Citrix Virtual Apps

사용자 예: XenMobile 에 장치를 등록한 후 사용자는 Citrix Secure Hub 앱을 통해 XenMobile Store 에 액세스합니다. 여기서 사용자는 제공되는 모든 회사 앱 및 서비스를 확인할 수 있습니다. 사용자는 XenMobile Store 에서 앱을 클릭하여 설치하고, 데이터에 액세스하고, 앱을 평가하고 후기를 작성하고, 앱 업데이트를 다운로드할 수 있습니다.

사용자 등록 옵션

September 29, 2021

다양한 방법으로 사용자 장치를 XenMobile 에 등록하도록 할 수 있습니다. 구체적인 사항을 고려하기 전에 MDM+MAM, MDM 또는 MAM 으로 등록하고자 하는 장치를 결정하십시오. 관리 모드에 대한 자세한 내용은 [관리 모드](#)를 참조하십시오.

개괄적으로 등록 옵션에는 네 가지가 있습니다.

- 등록 초대: 사용자에게 등록 초대 또는 초대 URL 을 전송합니다. Windows 장치에서는 등록 초대와 URL 을 사용할 수 없습니다.
- 자가 지원 포털: 사용자가 방문하여 Secure Hub 를 다운로드하고 장치를 등록하거나 등록 초대를 직접 전송할 수 있는 포털을 설정합니다.
- 수동 등록: 사용자에게 시스템을 등록할 수 있음을 알리는 전자 메일, 안내서 또는 기타 커뮤니케이션을 전송합니다. 그러면 사용자가 Secure Hub 를 다운로드하고 수동으로 장치를 등록합니다.
- 엔터프라이즈: 다른 장치 등록 옵션은 Apple 배포 프로그램 및 Google Android Enterprise 를 사용하는 것입니다. 이러한 프로그램을 통해 미리 구성되고 직원이 사용할 수 있도록 준비된 장치를 구입할 수 있습니다. 자세한 내용은 [Apple 지원](#)의 Apple 배포 프로그램 문서와 [Android Enterprise 웹사이트](#)의 Google Android Enterprise 문서를 참조하십시오.

등록 초대

iOS, macOS, Android Enterprise 및 레거시 Android 장치 사용자에게 전자 메일로 등록 초대를 보낼 수 있습니다. Windows 장치에서는 등록 초대와 URL 을 사용할 수 없습니다.

또한 iOS, macOS, Android 또는 Windows 장치 사용자에게 SMTP 또는 SMS 를 통해 설치 링크를 보낼 수 있습니다. 자세한 내용은 [장치 등록](#)을 참조하십시오.

등록 초대 방법을 사용하기로 할 경우 다음이 가능합니다.

- 초대 **URL**, 초대 **URL+PIN** 또는 초대 **URL+** 암호 등록 보안 모드를 선택합니다.
- 모드를 조합하여 사용할 수 있습니다.
- 설정 페이지에서 모드를 활성화하거나 비활성화할 수 있습니다.

각 등록 보안 모드에 대한 자세한 내용은 [등록 보안 모드 구성](#)을 참조하십시오.

초대는 많은 용도로 사용됩니다. 초대 의 가장 일반적인 용도는 사용자에게 시스템을 사용할 수 있고 등록할 수 있음을 알리는 것입니다. 초대 URL 은 고유합니다. 사용자가 초대 URL 을 사용하고 나면 더 이상 URL 을 사용할 수 없습니다. 이 속성을 사용하여 시스템에 등록하는 사용자 또는 장치를 제한할 수 있습니다.

등록 프로필을 구성하면 특정 사용자가 등록할 수 있는 장치 수를 Active Directory 그룹에 따라 제어할 수 있습니다. 예를 들어 재무 부서에 사용자당 하나의 장치만 허용할 수 있습니다.

특정 등록 옵션을 사용할 경우 추가 비용 및 문제가 발생할 수 있다는 점에 주의하십시오. 예를 들어 SMS 를 사용하여 초대장을 전송하려면 추가적인 인프라가 필요합니다. 이 옵션에 대한 자세한 내용은 [알림](#)을 참조하십시오.

또한 전자 메일로 초대장을 보내려면 사용자가 Secure Hub 외부에서 전자 메일에 액세스할 방법이 있는지 확인하십시오. MDM 등록의 경우 OTP(일회용 암호) 등록 보안 모드를 Active Directory 암호 대신 사용할 수 있습니다.

자가 지원 포털

사용자는 자가 지원 포털을 통해 등록 초대장을 요청할 수 있습니다. 자가 지원 포털 설정에 대한 자세한 내용은 [등록 보안 모드 구성](#)을 참조하십시오.

수동 등록

수동 등록에서는 사용자가 AutoDiscovery 를 사용하거나 서버 정보를 입력하여 XenMobile 에 연결합니다. AutoDiscovery 를 사용하는 경우 사용자는 전자 메일 주소 또는 Active Directory 자격 증명만 사용자 계정 이름 형식으로 입력하여 로그인합니다. AutoDiscovery 를 사용하지 않는 경우 사용자는 서버 주소와 Active Directory 자격 증명을 입력해야 합니다. AutoDiscovery 설정에 대한 자세한 내용은 [XenMobile AutoDiscovery Service](#)를 참조하십시오.

수동 등록은 여러 가지 방법으로 간편하게 완료할 수 있습니다. 가이드를 생성하고 가이드를 사용자에게 배포한 다음 직접 등록하도록 합니다. IT 부서를 통해 특정 시간 슬롯의 사용자 그룹을 수동으로 등록할 수 있습니다. 사용자가 자격 증명, 서버 정보 또는 둘 다를 입력해야 하는 유사한 방법을 사용할 수 있습니다.

사용자 등록

환경을 설정한 후에는 사용자를 환경에 등록하는 방법을 결정해야 합니다. 사용자 등록 보안 모드에 대한 구체적인 내용은 이 문서의 이전 섹션에 설명되어 있습니다. 이 섹션에서는 사용자에게 연락하는 방법을 설명합니다.

공개 등록과 선택적 초대

사용자를 온보딩할 때는 다음의 두 가지 기본적인 방법을 통해 등록을 허용할 수 있습니다.

- 공개 등록. 기본적으로 LDAP 자격 증명과 XenMobile 환경 정보가 있는 모든 사용자가 등록할 수 있습니다.
- 제한된 등록. 등록 초대를 받은 사용자만 허용하여 사용자 수를 제한할 수 있습니다. Active Directory 그룹을 기준으로 공개 등록을 제한할 수도 있습니다.

초대 방법을 사용하는 경우 사용자가 등록할 수 있는 장치 수를 제한할 수도 있습니다. 공개 등록은 대부분의 경우 허용되지만 몇 가지 고려해야 할 사항이 있습니다.

- MAM 등록의 경우 Active Directory 그룹 구성원 자격을 통해 간편하게 공개 등록을 제한할 수 있습니다.
- MDM 등록의 경우 Active Directory 그룹 구성원 자격에 따라 등록할 수 있는 장치의 수를 제한할 수 있습니다. 환경에서 회사 장치만 허용하려는 경우 이러한 제한은 보통 문제가 되지 않습니다. 그러나 BYOD 작업 공간에서 환경의 장치 수를 제한하려는 경우 이 방법을 고려하는 것이 좋습니다.

선택적 초대는 공개 등록보다 필요한 작업이 약간 더 많기 때문에 일반적으로 덜 자주 수행됩니다. 사용자가 환경에서 장치를 등록하려면 각 사용자에게 고유한 초대를 보내야 합니다. 등록 초대를 보내는 방법에 대한 자세한 내용은 [등록 초대 보내기](#)를 참조하십시오.

Active Directory 그룹을 사용하여 초대를 일괄적으로 생성할 수 있지만 이 접근 방식은 연속적으로 수행해야 합니다.

먼저 사용자에게 연락

공개 등록 또는 선택적 초대 중 선택하고 이러한 환경을 설정한 후에는 사용자에게 등록 옵션을 알려야 합니다.

선택적 초대 방법을 사용하는 경우 전자 메일 및 SMS 메시지가 프로세스에 포함됩니다. 공개 등록의 경우에도 XenMobile 콘솔을 통해 전자 메일을 보낼 수 있습니다. 자세한 내용은 [등록 초대 보내기](#)를 참조하십시오.

두 경우 모두 전자 메일을 사용하려면 SMTP 서버가 필요합니다. 문자 메시지의 경우 SMS 서버가 필요합니다. 이러한 서버의 경우 의사 결정을 내릴 때 추가 비용을 고려해야 할 수 있습니다. 방법을 선택하기 전에 새 사용자가 정보 (예: 전자 메일) 에 액세스하는 방법을 고려해야 합니다. 모든 사용자로 하여금 XenMobile 을 통해 전자 메일에 액세스하도록 하려는 경우 초대 전자 메일을 보내는 것이 문제가 될 수 있습니다.

공개 등록 환경에서는 XenMobile 이외의 다른 수단으로도 커뮤니케이션을 전송할 수 있습니다. 이 옵션의 경우 관련 정보를 모두 포함해야 합니다. 사용자에게 Secure Hub 앱을 받을 수 있는 위치와 등록에 사용하는 방법을 알려줍니다. 검색이 꺼져 있으면 사용자에게 XenMobile Server 주소도 제공합니다. AutoDiscovery 에 대한 자세한 내용은 [XenMobile AutoDiscovery Service](#)를 참조하십시오.

XenMobile 작업 조정

March 15, 2024

XenMobile 작업의 성능 및 안정성은 XenMobile 의 많은 설정과 관련되며 Citrix ADC 및 SQL Server 데이터베이스 구성에 따라 달라집니다. 이 문서에서는 XenMobile 의 조정 및 최적화와 관련하여 관리자가 가장 자주 구성하는 설정을 중점적으로 설명합니다. XenMobile 을 배포하기 전에 이 문서의 각 설정을 평가하는 것이 좋습니다.

중요:

다음 지침은 XenMobile 서버 CPU 및 RAM 이 장치 수에 적합하다고 가정합니다. 확장성에 대한 자세한 내용은 [확장성 및 성능](#)을 참조하십시오.

다음 서버 속성은 전체 XenMobile 인스턴스의 작업, 사용자 및 장치에 글로벌로 적용됩니다. 일부 서버 속성을 변경하려면 각 XenMobile 서버 노드를 다시 시작해야 합니다. 다시 시작이 필요한 경우 XenMobile 이 알림을 제공합니다.

다음 조정 지침은 클러스터된 환경과 클러스터되지 않은 환경에 모두 적용됩니다.

hibernate.c3p0.idle_test_period

XenMobile Server 속성인 사용자 지정 키는 연결 유효성이 자동으로 검사되기까지의 유효 시간 (초) 을 결정합니다. 다음과 같이 키를 구성합니다. 기본값은 **30** 입니다.

- 키: 사용자 지정 키
- 키: **hibernate.c3p0.idle_test_period**
- 값: **120**
- 표시 이름: **hibernate.c3p0.idle_test_period**
- 설명: **Hibernate** 유효 테스트 기간

hibernate.c3p0.max_size

이 사용자 지정 키는 XenMobile 에서 SQL Server 데이터베이스에 대해 열 수 있는 최대 연결 수를 결정합니다. XenMobile 은 이 사용자 지정 키에 지정한 값을 상한으로 사용합니다. 필요한 경우에만 연결이 열립니다. 데이터베이스 서버의 용량에 따라 설정을 결정합니다.

클러스터된 구성에서는 다음 수식을 참고하십시오. c3p0 연결에 노드 수를 곱한 값은 XenMobile 이 SQL Server 데이터베이스에 실제로 열 수 있는 최대 연결 수와 동일합니다.

클러스터된 구성 및 클러스터되지 않은 구성에서 SQL Server 규모를 작게 하여 이 값을 너무 높게 설정하면 최고 부하 중에 SQL 측에서 리소스 문제가 발생할 수 있습니다. 이 값을 너무 낮게 설정하면 사용 가능한 SQL 리소스를 활용하지 못할 수 있습니다.

다음과 같이 키를 구성합니다. 기본값은 **1000** 입니다.

- 키: **hibernate.c3p0.max_size**
- 값: **1000**
- 표시 이름: **hibernate.c3p0.max_size**
- 설명: SQL 에 대한 DB 연결

hibernate.c3p0.min_size

이 사용자 지정 키는 XenMobile 에서 SQL Server 데이터베이스에 대해 여는 최소 연결 수를 결정합니다. 다음과 같이 키를 구성합니다. 기본값은 **100** 입니다.

- 키: **hibernate.c3p0.min_size**
- 값: **100**
- 표시 이름: **hibernate.c3p0.min_size**
- 설명: SQL 에 대한 DB 연결

hibernate.c3p0.timeout

이 사용자 지정 키는 유휴 시간 초과를 결정합니다. 데이터베이스 클러스터 장애 조치 (failover) 를 사용하는 경우 이 사용자 지정 키를 추가하고, 유휴 시간 초과를 낮추도록 설정하는 것이 좋습니다. 기본값은 **120** 입니다.

- 키: 사용자 지정 키
- 키: **hibernate.c3p0.timeout**
- 값: **120**
- 표시 이름: **hibernate.c3p0.timeout**
- 설명: 데이터베이스 유휴 시간 초과

푸시 서비스 하트비트 간격

이 설정은 iOS 장치에서 중간에 APNs 알림이 전송되지 않았는지를 확인하는 빈도를 결정합니다. APNs 하트비트 빈도를 늘리면 데이터베이스 통신을 최적화할 수 있습니다. 값이 너무 크면 불필요한 부하가 추가될 수 있습니다. 이 설정은 iOS 에만 적용됩니다. 기본값은 **20** 시간입니다.

환경에 iOS 장치가 많은 경우 하트비트 간격으로 인해 필요 이상의 부하가 발생할 수 있습니다. 선택적 초기화, 잠금 및 전체 초기화 같은 보안 동작은 이 하트비트를 사용하지 않습니다. 이러한 동작이 실행될 때는 APNs 알림이 장치로 전송되기 때문입니다.

이 값은 Active Directory 그룹 구성원 자격이 변경된 후 정책을 업데이트하는 속도를 제어합니다. 그러므로 부하를 줄이려면 이 값을 12~20 시간 사이의 값으로 늘리는 것이 적절합니다.

iOS MDM APNS 연결 풀 크기

장치 수가 100 대 이상인 경우 APNs 연결 풀이 너무 작으면 APNs 작업 성능에 부정적인 영향을 미칠 수 있습니다. 앱 및 정책이 장치에 느리게 배포되고 장치 등록이 느려지는 등의 성능 문제가 발생할 수 있습니다. 기본값은 **1** 입니다. 약 400 개의 장치마다 이 값을 1 씩 늘리는 것이 좋습니다.

auth.ldap.connect.timeout

느린 LDAP 응답을 보완하려면 다음 사용자 지정 키의 서버 속성을 추가하는 것이 좋습니다.

- 키: 사용자 지정 키
- 키: **auth.ldap.connect.timeout**
- 값: **60000**
- 표시 이름: **auth.ldap.connect.timeout**
- 설명: **LDAP** 연결 시간 초과

auth.ldap.read.timeout

느린 LDAP 응답을 보완하려면 다음 사용자 지정 키의 서버 속성을 추가하는 것이 좋습니다.

- 키: 사용자 지정 키
- 키: **auth.ldap.read.timeout**
- 값: **60000**
- 표시 이름: **auth.ldap.read.timeout**
- 설명: **LDAP** 읽기 시간 제한

기타 서버 최적화

서버 속성	기본 설정	이 설정을 변경하는 이유
백그라운드 배포	1,440 분	백그라운드 정책 배포의 빈도 (분)입니다. Android 장치의 상시 연결에만 적용됩니다. 정책 배포 빈도를 늘리면 서버 부하가 감소합니다. 권장되는 설정은 1440 (24 시간)입니다.
백그라운드 하드웨어 인벤토리	1,440 분	백그라운드 하드웨어 인벤토리의 빈도 (분)입니다. Android 장치의 상시 연결에만 적용됩니다. 하드웨어 인벤토리 빈도를 늘리면 서버 부하가 감소합니다. 권장되는 설정은 1440 (24 시간)입니다.

삭제된 **Active Directory** 사용자를 15 분
확인하는 간격

MaxNumberOfWorker 3

Active Directory 의 표준 동기화 시
간은 **15** 분입니다. 값이 **0** 인 경우
XenMobile 이 삭제된 Active
Directory 사용자를 확인하지 않습니
다. 권장되는 설정은 **15** 분입니다.
많은 수의 볼륨 구매 라이선스를 가져올
때 사용되는 스레드 수입니다. 기본값은
3 입니다. 추가 최적화가 필요한 경우 스
레드 수를 늘릴 수 있습니다. 그러나 예
를 들어 6 과 같이 스레드 수가 커지면 볼
륨 구매를 가져올 때 CPU 사용량이 높
아집니다.

SQL DB 에서 교착 상태를 확인하고 기록 데이터를 삭제하는 방법

교착 상태가 발견되면 다음 쿼리를 실행하여 교착 상태를 확인하십시오. 그런 다음 데이터베이스 관리자 또는 Microsoft SQL
팀을 통해 정보를 확인할 수 있습니다.

SQL 쿼리

```
1 SELECT
2
3 db.name DB_Service,
4
5 tl.request_session_id,
6
7 wt.blocking_session_id,
8
9 OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,
10
11 tl.resource_type,
12
13 h1.TEXT AS RequestingText,
14
15 h2.TEXT AS BlockingTest,
16
17 tl.request_mode
18
19 FROM sys.dm_tran_locks AS tl
20
21 INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id
22
```

```

23 INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
    resource_address
24
25 INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
    resource_associated_entity_id
26
27 INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
    request_session_id
28
29 INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
    blocking_session_id
30
31 CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1
32
33 CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2
34
35 GO
36 <!--NeedCopy-->

```

데이터베이스 정리

중요:

테이블을 변경하기 전에 데이터베이스를 백업합니다.

1. 다음 쿼리를 실행하여 기록 데이터를 확인합니다.

```

1 select COUNT(*) as total_record from dbo.EWDEPLOY_HISTO;
2 select COUNT(*) as total_record from dbo.EWSESS;
3 select COUNT(*) as total_record from dbo.EWAUDIT;
4 <!--NeedCopy-->

```

2. 이전의 3 개 테이블에서 데이터를 삭제합니다.

참고:

기록 데이터가 테이블에 표시되지 않을 수 있습니다. 이 경우 실행을 건너뛰고 특정 테이블에 대한 쿼리를 잘라냅니다.

```

1 truncate TABLE dbo.EWDEPLOY_HISTO;
2 truncate TABLE dbo.EWSESS;
3 truncate TABLE dbo.EWAUDIT;
4 <!--NeedCopy-->

```

3. 교착 상태로 인해 차단되었던 SELECT 쿼리를 차단 해제합니다. 이 단계에서 추가 교착 상태가 처리됩니다.

```

1 ALTER DATABASE <database_name> SET          READ_COMMITTED_SNAPSHOT
    ON WITH ROLLBACK IMMEDIATE
2 <!--NeedCopy-->

```

4. 기본적으로 데이터베이스 정리는 세션 보존 및 감사 보존 데이터 유지를 위해 7 일로 설정되며 사용자가 많은 경우 값이 증가합니다. 정리 값을 1 일 또는 2 일로 변경합니다. 서버 속성에서 다음 변경을 수행합니다.

```

1 zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
2 zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
3 zdm.dbcleanup.auditRetentionTimeInDays=1 day
4 <!--NeedCopy-->

```

KEYSTORE 테이블에서 분리된 항목 정리

XenMobile 노드의 성능이 좋지 않으면 KEYSTORE 테이블이 너무 크지 않은지 확인합니다. XenMobile Server 은 등록 인증서를 ENROLLMENT_CERTIFICATE 및 KEYSTORE 테이블에 저장합니다. 장치를 삭제하거나 재등록하면 ENROLLMENT_CERTIFICATE 테이블의 인증서가 삭제됩니다. KEYSTORE 테이블의 항목은 그대로 유지되며, 이로 인해 성능 문제가 발생할 수 있습니다. KEYSTORE 테이블에서 분리된 항목을 정리하려면 다음 절차를 수행하십시오.

중요:

테이블을 변경하기 전에 데이터베이스를 백업합니다.

1. 다음 쿼리를 실행하여 기록 데이터를 확인합니다.

```

1 select COUNT(*) from KEYSTORE
2 <!--NeedCopy-->

```

2. 다음 쿼리를 사용하여 KEYSTORE 테이블에서 분리된 항목이 있는지 확인합니다.

```

1 WITH cte(KEYSTORE_ID)
2 AS (SELECT KEYSTORE_ID
3     FROM ENROLLMENT_CERTIFICATE
4     UNION
5     SELECT CA_KEYSTORE_ID
6     FROM LDAP_CONFIG
7     UNION
8     SELECT CLIENT_KEYSTORE_ID
9     FROM LDAP_CONFIG
10    UNION
11    SELECT KEYSTORE_ID
12    FROM SAML_SERVICE_PROVIDER
13    UNION
14    SELECT KEYSTORE_ID
15    FROM SERVER_CERTIFICATE)
16 SELECT keystore.id
17 FROM keystore
18     LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
19 WHERE KEYSTORE_ID IS NULL;
20 <!--NeedCopy-->

```

3. 다음 쿼리를 사용하여 분리된 항목을 지웁니다.

```

1 WITH cte(KEYSTORE_ID)
2 AS (SELECT KEYSTORE_ID
3     FROM ENROLLMENT_CERTIFICATE
4     UNION

```



```

5      SELECT CA_KEYSTORE_ID
6      FROM LDAP_CONFIG
7      UNION
8      SELECT CLIENT_KEYSTORE_ID
9      FROM LDAP_CONFIG
10     UNION
11     SELECT KEYSTORE_ID
12     FROM SAML_SERVICE_PROVIDER
13     UNION
14     SELECT KEYSTORE_ID
15     FROM SERVER_CERTIFICATE)
16 DELETE FROM keystore
17 WHERE id IN
18 (
19     SELECT keystore.id
20     FROM keystore
21     LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
22     WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
23 );
24 <!--NeedCopy-->

```

4. KEYSTORE 테이블에 인덱스를 추가하여 검색 효율성을 높입니다.

```

1 DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
2 ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
3 CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
4     ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
5     DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
6 <!--NeedCopy-->

```

앱 프로비전 및 프로비전 해제

September 14, 2022

응용 프로그램 프로비전은 주로 XenMobile 환경 내 모바일 앱의 준비, 구성, 제공 및 관리로 구성되는 모바일 앱 수명 주기를 중심으로 수행됩니다. 일부 경우에는 응용 프로그램 코드의 배포나 수정도 프로비전 프로세스에 포함될 수 있습니다. XenMobile에는 앱 프로비전에 사용할 수 있는 다양한 도구와 프로세스가 포함되어 있습니다.

앱 프로비전에 관한 이 문서를 읽기 전에 다음 문서를 읽어 보는 것이 좋습니다.

- [앱 - 사용자 커뮤니티](#)

조직에서 사용자에게 제공할 앱의 유형을 확정된 후에 앱의 수명 주기 관리 프로세스에 대한 개요를 작성할 수 있습니다.

앱 프로비전 프로세스를 정의할 때는 다음 요점을 고려하십시오.

- **앱 프로파일링:** 조직에서 처음에는 제한된 수의 앱을 사용하여 시작할 수 있습니다. 하지만 사용자 채택률이 증가하고 환경의 규모가 확장됨에 따라 관리하는 앱의 수가 빠른 속도로 증가할 수 있습니다. 앱 프로비전을 쉽게 관리하려면 처음부

터 구체적인 앱 프로필을 정의합니다. 앱 프로파일링은 앱을 비기술적인 관점의 논리적 그룹으로 범주화하는 데 도움이 됩니다. 예를 들어 다음과 같은 요소를 기준으로 앱 프로필을 생성할 수 있습니다.

- 버전: 추적에 사용할 앱 버전
- 인스턴스: 서로 다른 사용자 집합 (예: 서로 다른 액세스 수준) 에 배포되는 다수의 인스턴스
- 플랫폼: iOS, Android 또는 Windows
- 대상: 표준 사용자, 부서, 최고 수준 경영진
- 소유권: 앱을 소유하는 부서
- 유형: MDX, 공용, 웹 및 SaaS 또는 웹 링크
- 업그레이드 주기: 앱을 업그레이드하는 빈도
- 라이선스: 라이선스 요구 사항 및 소유권
- MAM SDK 또는 MDX 정책: MDX 기능을 모바일 앱에 적용합니다.
- 네트워크 액세스: 액세스 유형 (예: Secure Browse 또는 전체 VPN)

참고:

터널링됨 - 웹 SSO 는 MDX 설정에서 Secure Browse 의 이름입니다. 동작은 동일합니다.

예:

요소	Secure Mail	메일	사내	Epic Rover
버전	10.1	10.1	X.x	X.x
인스턴스	중요 발신인	의사	임상	임상
플랫폼	iOS	iOS	iOS	iOS
대상 사용자	VIP 사용자	의사	임상 사용자	임상 사용자
소유권	IT	IT	IT	IT
유형	MDX	MDX	기본	공개
업그레이드 주기	분기별	분기별	매년	해당 없음
라이선싱	해당 없음	해당 없음	해당 없음	볼륨 구매
MDX 정책	예	예	예	아니요
네트워크 액세스	VPN	VPN	VPN	공개

- **앱 버전 관리:** 앱 버전을 유지 관리하고 추적하는 작업은 프로비전 프로세스의 중요한 부분입니다. 버전 관리는 사용자에게 미치는 영향 없이 수행됩니다. 앱의 새 버전을 다운로드할 수 있을 때만 사용자에게 알림이 제공됩니다. 관리자의 관점에서 프로덕션 환경에 미치는 영향을 방지하려면 비 프로덕션 용량에서 각 앱 버전을 검토하고 테스트해야 합니다.

이러한 검토 및 테스트는 특정 업그레이드가 필요한지 여부를 평가할 때에도 중요합니다. 앱 업그레이드에는 보통 두 가지 유형이 있습니다. 그 중 하나는 특정 버그의 수정과 같은 부차적 업그레이드입니다. 다른 하나는 주요 릴리스로, 이를 통해

앱을 대대적으로 변경하고 개선합니다. 어떤 경우에도 앱 릴리스 정보를 꼼꼼하게 검토하여 업그레이드가 필요한지를 평가하십시오.

- **앱 개발:** 개발하는 모바일 응용 프로그램에서 MAM SDK 를 통합할 때 이러한 앱에 MDX 기능을 적용합니다. [MAM SDK 개요](#)를 참조하십시오.

MAM SDK 는 2023 년 7 월 사용 중단이 예정된 MDX Toolkit 을 대체합니다. 앱 래핑에 대한 자세한 내용은 [MDX Toolkit](#)을 참조하십시오. 래핑된 앱의 앱 프로비전 프로세스는 래핑되지 않은 표준 앱의 프로비전 프로세스와 다릅니다.

- **앱 보안:** 프로비전 프로세스의 일부로 개별 앱 또는 앱 프로필의 보안 요구 사항을 정의합니다. 앱을 배포하기 전에 구체적인 MDM 또는 MAM 정책에 보안 요구사항을 매핑할 수 있습니다. 이렇게 계획하면 앱 배포가 간소하고 빨라집니다. 예:
 - 특정 앱은 다르게 배포할 수 있습니다.
 - XenMobile 환경의 아키텍처를 변경하는 것이 좋을 수도 있습니다. 변경 사항은 앱에 필요한 보안 규정 준수 유형에 따라 다릅니다. 예를 들어 중요한 비즈니스 인텔리전스 앱을 사용할 수 있도록 장치를 암호화해야 하거나 중단 간 SSL 암호화 또는 지오펜스가 필요한 특정 앱을 사용해야 할 수 있습니다.
- **앱 제공:** XenMobile 에서는 앱을 MDM 앱 또는 MAM 앱으로 제공할 수 있습니다. MDM 앱은 XenMobile Store 에 표시됩니다. 이 스토어에서는 공개 또는 기본 앱을 사용자에게 편리하게 제공할 수 있습니다. 관리하는 유일한 MDM 앱 제어는 장치 수준 제한을 시행하기 위한 것입니다. 그러나 MAM 을 사용하여 앱을 제공하면 앱 제공 및 앱 자체를 완벽하게 제어할 수 있습니다. MAM 을 통해 앱을 제공하는 것이 보통 더 적절합니다.
- **응용 프로그램 유지 관리:**
 - 초기 감사 수행: 프로덕션 환경의 앱 버전과 마지막 업그레이드 주기를 추적합니다. 업그레이드가 필요한 특정 기능 또는 버그 수정을 기록하십시오.
 - 기준 설정: 각 앱의 안정적인 최신 릴리스 목록을 유지합니다. 업그레이드 후 예기치 않은 문제가 발생할 경우 이 앱 버전으로 롤백합니다. 또한, 롤백 계획을 개발합니다. 프로덕션 환경 이전에 테스트 환경에서 앱 업그레이드를 테스트합니다. 가능한 경우 업그레이드를 프로덕션 사용자 하위 집단에 먼저 배포한 다음 전체 사용자 기반으로 배포합니다.
 - 앱 최신 릴리스 정보를 확인하는 것은 중요하므로 Citrix 소프트웨어 업데이트 알림과 타사 소프트웨어 공급업체 알림을 구독합니다. EAR(Early Access Release) 빌드가 테스트를 위해 제공될 수도 있습니다.
 - 사용자 알림을 위한 전략 고안: 앱 업그레이드가 제공될 때 사용자에게 알림을 전송하는 전략을 정의합니다. 배포 전에 교육을 제공하여 사용자가 준비할 수 있도록 합니다. 앱 업데이트 전에 여러 번 알림을 전송할 수 있습니다. 앱에 따라 전자 메일 알림 또는 웹 사이트가 가장 좋은 알림 방법이 될 수 있습니다.

앱 수명 주기 관리는 앱의 초기 배포부터 사용 중지까지의 전체 수명 주기를 나타냅니다. 앱 수명 주기는 다음과 같은 세 단계로 이루어져 있습니다.

1. 사양 요구 사항: 비즈니스 사례 및 사용자 요구 사항에서 시작됩니다.
2. 개발: 앱이 비즈니스 요구 사항을 충족하는지 검증합니다.
3. 테스트: 테스트 사용자, 문제 및 버그를 식별합니다.
4. 배포: 앱을 프로덕션 사용자에게 배포합니다.
5. 유지 관리: 앱 버전을 업데이트합니다. 프로덕션 환경에서 앱을 업데이트하기 전에 테스트 환경에서 앱을 배포하십시오.

Secure Mail 을 사용한 응용 프로그램 수명 주기의 예

1. 사양 요구 사항: 보안 요구 사항에 따라, 컨테이너화되고 MDX 보안 정책을 지원하는 메일 앱이 필요합니다.
2. 개발: 앱이 비즈니스 요구 사항을 충족하는지 검증합니다. MDX 정책 제어를 앱에 적용할 수 있어야 합니다.
3. 테스트: Secure Mail 을 테스트 사용자 그룹에 할당하고 XenMobile Server 에서 해당하는 MDX 파일을 배포합니다. 테스트 사용자가 전자 메일을 성공적으로 보내고 받을 수 있으며 일정 및 연락처에 액세스할 수 있음을 검증합니다. 또한 테스트 사용자는 문제를 보고하고 버그를 식별합니다. 테스트 사용자의 피드백에 따라 Secure Mail 구성을 프로덕션 사용에 맞게 최적화합니다.
4. 배포: 테스트 단계가 완료되면 Secure Mail 을 프로덕션 사용자에게 할당하고 XenMobile 에서 해당하는 MDX 파일을 배포합니다.
5. 유지 관리: Secure Mail 의 새로운 업데이트가 제공됩니다. Citrix 다운로드에서 새 MDX 파일을 다운로드하고 XenMobile Server 의 기존 MDX 파일을 대체합니다. 사용자에게 업데이트를 수행하도록 알립니다. 참고: Citrix 는 테스트 환경에서 이 프로세스를 완료하고 테스트하기를 권장합니다. 그런 다음 앱을 XenMobile 프로덕션 환경에 업로드하고 사용자에게 배포합니다.

자세한 내용은 [iOS 모바일 앱 래핑](#) 및 [Android 모바일 앱 래핑](#)을 참조하십시오.

대시보드 기반 작업

January 5, 2022

XenMobile 콘솔 대시보드에 액세스하여 정보를 한 눈에 볼 수 있습니다. 이러한 정보를 사용하면 위젯을 통해 신속하게 문제점과 성공 여부를 확인할 수 있습니다.

대시보드는 일반적으로 XenMobile 콘솔에 처음 로그인할 때 나타나는 화면입니다. 콘솔의 다른 곳에서 대시보드에 액세스하려면 분석을 클릭합니다. 페이지의 레이아웃을 편집하고 나타나는 위젯을 편집하려면 대시보드에서 사용자 지정을 클릭합니다.

- 내 대시보드: 최대 네 개의 대시보드를 저장할 수 있습니다. 이러한 대시보드를 개별적으로 편집하고 저장된 대시보드를 선택하여 각 대시보드를 볼 수 있습니다.
- 레이아웃 스타일: 이 행에서는 대시보드에 표시되는 위젯 수와 위젯 배치 방법을 선택할 수 있습니다.
- 위젯 선택: 대시보드에 표시할 정보를 선택할 수 있습니다.
 - 알림: 왼쪽의 숫자 위에 있는 확인란을 선택하여 위젯 위에 알림 표시줄을 추가합니다. 이 표시줄에는 규격 장치, 비활성 장치 및 지난 24 시간 동안 초기화되거나 등록된 장치의 수가 표시됩니다.
 - 장치 (플랫폼 기준): 플랫폼별로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다.
 - 장치 (이동 통신 사업자 기준): 이동 통신 사업자로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다. 각 표시줄을 클릭하여 플랫폼별 분석을 볼 수 있습니다.
 - 관리되는 장치 (플랫폼 기준): 플랫폼별로 관리되는 장치의 수를 표시합니다.
 - 관리되지 않는 장치 (플랫폼 기준): 플랫폼별로 관리되지 않는 장치의 수를 표시합니다. 이 차트에 나타나는 장치는 에이전트가 설치되어 있지만 권한이 해지되었거나 초기화되었을 수 있습니다.

- 장치 (**ActiveSync Gateway** 상태 기준): ActiveSync Gateway 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 차단됨, 허용됨 또는 알 수 없음 상태가 표시됩니다. 각 표시줄을 클릭하여 플랫폼별로 데이터를 분류할 수 있습니다.
- 장치 (소유권 기준): 소유권 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 회사 소유, 직원 소유 또는 알 수 없는 소유권 상태가 표시됩니다.
- 실패한 배달 그룹 배포: 패키지당 실패한 배포의 총 수를 표시합니다. 배포에 실패한 패키지만 나타납니다.
- 장치 (차단된 이유 기준): ActiveSync 에 의해 차단된 장치의 수를 표시합니다.
- 설치된 앱: 이 위젯을 사용하면 앱 이름을 입력하여 그래프에 해당 앱에 대한 정보를 표시할 수 있습니다.
- 볼륨 구매 앱 라이선스 사용 현황: Apple 볼륨 구매 앱에 대한 라이선스 사용 현황 통계를 표시합니다.

사용 사례

대시보드 위젯을 사용하여 환경을 모니터링하는 다수의 방법에 대한 몇 가지 예제는 다음과 같습니다.

- 모바일 생산성 앱을 배포한 후 모바일 생산성 앱이 장치에 설치되지 않는다는 내용의 지원 티켓을 받았습니다. 규정 위반 장치 및 설치된 앱 위젯을 사용하여 모바일 생산성 앱이 설치되지 않은 장치를 확인합니다.
- 비활성 장치를 환경에서 제거하고 라이선스를 재확보하기 위해 비활성 장치를 모니터링하려고 합니다. 비활성 장치 위젯을 사용하여 이 통계를 추적합니다.
- 데이터가 올바르게 동기화되지 않는다는 내용의 지원 티켓을 받았습니다. 장치 (**ActiveSync Gateway** 상태 기준) 및 장치 (차단된 이유 기준) 위젯을 사용하여 문제가 ActiveSync 와 관련된 것인지 여부를 확인할 수 있습니다.

보고

환경 설정 및 사용자 등록이 완료된 후 보고서를 실행하여 배포에 관한 내용을 확인할 수 있습니다. XenMobile 은 환경에서 실행되는 장치를 파악하는 데 도움이 되는 다수의 보고서를 기본적으로 제공합니다. 자세한 내용은 [보고서](#)를 참조하십시오.

중요:

SQL Server 를 사용하여 사용자 지정 보고서를 만들 수 있지만 이 방법은 권장하지 않습니다. SQL Server 데이터베이스를 이 방법으로 사용하면 XenMobile 배포에 예기치 않은 결과가 발생할 수 있습니다. 이 방법의 보고를 사용하기로 결정한 경우 읽기 전용 계정을 사용하여 SQL 쿼리를 실행해야 합니다.

역할 기반 액세스 제어 및 XenMobile 지원

March 15, 2024

XenMobile 은 RBAC(역할 기반 액세스 제어) 를 사용하여 XenMobile 시스템 기능 (예: XenMobile 콘솔, 원격 지원 및 공용 API) 에 대한 사용자 및 그룹의 액세스를 제한합니다. 이 문서에서는 XenMobile 에 기본 제공되는 역할과 XenMobile 에서 RBAC 를 활용하는 지원 모델을 결정할 때의 고려 사항에 대해 설명합니다.

참고:

2019 년 1 월 1 일부터 신규 고객에게는 더 이상 원격 지원이 제공되지 않습니다. 기존 고객은 제품을 계속 사용할 수 있지만 Citrix 는 개선 사항이나 수정 사항을 제공하지 않습니다.

기본 제공 역할

다음과 같은 기본 제공 역할에 부여되는 액세스 권한을 변경하고 역할을 추가할 수 있습니다. 각 역할에 연결된 액세스 및 기능 권한과 역할의 기본 설정을 모두 보려면 XenMobile 설명서에서 [Role-Based Access Control Defaults\(역할 기반 액세스 제어 기본값\)](#)를 다운로드하십시오. 각 기능에 대한 정의는 XenMobile 설명서에서 [RBAC 를 사용하여 역할 구성](#)을 참조하십시오.

관리 역할

부여되는 기본 액세스 권한:

- 원격 지원을 제외한 전체 시스템 액세스 권한
- 기본적으로 관리자는 일부 지원 작업 (예: 연결 확인 및 지원 번들 만들기) 을 수행할 수 있습니다.

고려 사항:

- 일부 관리자 또는 전체 관리자가 원격 지원에 액세스해야 합니까? 그렇다면 관리 역할을 편집하거나 고나리 역할을 추가할 수 있습니다.
- 일부 관리자 또는 관리자 그룹에 대한 액세스를 추가로 제한하려면 관리 템플릿에 따라 역할을 추가하고 권한을 편집합니다.

지원

부여되는 기본 액세스 권한:

- 원격 지원에 대한 액세스 권한.

고려 사항:

- 온-프레미스 XenMobile Server 배포의 경우: 원격 지원을 사용하면 지원 센터 담당자가 관리되는 Android 모바일 장치를 원격으로 제어할 수 있습니다. 스크린캐스트는 Samsung Knox 장치에서만 지원됩니다.
- 원격 지원은 클러스터링된 온-프레미스 XenMobile Server 배포에서 지원되지 않습니다.

사용자

부여되는 기본 액세스 권한:

- XenMobile 콘솔에 대한 제한된 액세스 권한: 장치 기능 (예: 장치 초기화, 잠금/잠금 해제, 컨테이너 잠금/잠금 해제, 위치 확인 및 지리적 제한 설정, 장치 벨 울림, 컨테이너 암호 재설정), 등록 초대 추가, 제거 및 보내기.

고려 사항:

- 사용자 역할을 할당하면 사용자가 직접 지원 리소스를 찾을 수 있습니다.
- 공유 장치를 지원하려면 공유 장치 등록에 대한 사용자 역할을 만듭니다.

XenMobile 지원 모델에 대한 고려 사항

채택할 수 있는 지원 모델은 매우 방대하며, 수준 1 및 2 지원을 처리하는 타사와 수준 3 및 4 지원을 처리하는 직원이 포함될 수 있습니다. 지원 부하를 분산하는 방식에 관계없이 XenMobile 배포 및 사용자 기반에 관한 이 섹션의 고려 사항을 숙지하십시오.

사용자가 회사 소유의 장치를 사용합니까? **BYO** 장치를 사용합니까?

지원에 영향을 미치는 기본적인 질문은 XenMobile 환경의 사용자 장치를 누가 소유하는지에 대한 것입니다. 사용자가 회사 소유의 장치를 사용하는 경우 관리자는 장치를 잠그는 방법으로 하위 수준을 지원을 제공할 수 있습니다. 이 경우 관리자는 지원 센터를 통해 장치 문제에 대한 지원 및 장치 사용 방법에 대한 지원을 사용자에게 제공할 수 있습니다. 지원해야 하는 장치의 유형에 따라 지원 센터에 대한 RBAC 장치 프로비전 및 지원 역할을 어떻게 사용할지 고려하십시오.

사용자가 BYO 장치를 사용하는 경우 사용자는 장치 지원에 대한 자료를 직접 찾아야 할 수 있습니다. 이 경우 조직이 제공하는 지원은 XenMobile 관련 문제에 중점을 둔 관리 역할에 더 가깝습니다.

데스크톱의 지원 모델은 무엇입니까?

데스크톱의 지원 모델이 다른 회사 소유 장치에 적절한지 여부를 고려하십시오. 동일한 지원 조직을 사용할 수 있습니까? 어떤 추가 교육이 필요한가요?

XenMobile 자가 지원 포털에 대한 액세스 권한을 사용자에게 제공하시겠습니까?

설정 > 등록을 사용하여 등록 보안 모드에 자가 지원 포털을 사용 설정합니다. 자가 지원 포털에서 사용자는 장치를 등록하거나 등록 초대를 보내는 데 사용하는 등록 링크를 생성할 수 있습니다. [등록 보안 모드 구성](#)을 참조하십시오.

시스템 모니터링

March 15, 2024

앱 액세스 및 연결을 위한 작동 시간을 최적화하려면 XenMobile 환경에서 다음과 같은 핵심 구성 요소를 모니터링해야 합니다.

XenMobile Server

XenMobile 서버는 로그를 생성하여 로컬 스토리지에 저장합니다. 이 로그를 시스템 로그 (syslog) 서버로 내보낼 수 있습니다. 로그 설정을 구성하여 크기 제약 또는 로그 수준을 지정하거나 특정 이벤트를 필터링하는 사용자 지정 로거를 생성할 수 있습니다.

언제든지 XenMobile 콘솔에서 XenMobile 서버 로그를 확인할 수 있습니다. 또한 syslog 서버를 통해 로그의 정보를 프로덕션 Splunk 로깅 서버로 내보낼 수 있습니다.

다음 목록에는 XenMobile 에서 사용할 수 있는 서로 다른 로그 파일 유형이 설명되어 있습니다.

디버그 로그 파일: XenMobile 의 핵심 웹 서비스에 대한 디버그 수준 정보 (오류 메시지 및 서버 관련 동작 포함) 가 포함됩니다.

메시지 형식:

<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>

- 여기서 <id>는 고유 식별자 (예: sessionId) 입니다.
- 여기서 <log message>는 응용 프로그램이 제공하는 메시지입니다.

관리자 감사 로그 파일: XenMobile 콘솔 작업에 대한 감사 정보가 포함됩니다.

참고:

관리자 감사 로그와 사용자 감사 로그에는 동일한 형식이 사용됩니다.

메시지 형식:

필수적인 날짜 및 타임스탬프 값을 제외한 다른 모든 특성은 선택 사항입니다. 선택적 필드는 메시지에서 “”로 표시됩니다.

<date> <timestamp> "<username/id>"<sessionid>"<deviceid>"<clientip>"<action>"<status>"<application name>"<app user id>"<user agent>"<details>"

다음 표에는 사용 가능한 관리자 감사 로그 이벤트가 나열되어 있습니다.

이벤트용 관리자 감사 로그 메시지	상태
로그인	성공/실패
로그아웃	성공/실패
관리자 가져오기	성공/실패
관리자 업데이트	성공/실패
응용 프로그램 가져오기	성공/실패
응용 프로그램 추가	성공/실패
응용 프로그램 업데이트	성공/실패
응용 프로그램 삭제	성공/실패
응용 프로그램 바인딩	성공/실패
응용 프로그램 바인딩 해제	성공/실패

이벤트용 관리자 감사 로그 메시지	상태
응용 프로그램 사용 안 함	성공/실패
응용 프로그램 사용	성공/실패
범주 가져오기	성공/실패
범주 추가	성공/실패
범주 업데이트	성공/실패
그룹 삭제	성공/실패
인증서 추가	성공/실패
인증서 삭제	성공/실패
활성 인증서	성공/실패
CSR 인증서	성공/실패
인증서 내보내기	성공/실패
인증서 체인 삭제	성공/실패
인증서 체인 추가	성공/실패
커넥터 가져오기	성공/실패
커넥터 추가	성공/실패
커넥터 삭제	성공/실패
커넥터 업데이트	성공/실패
장치 가져오기	성공/실패
장치 잠금	성공/실패
장치 잠금 해제	성공/실패
장치 초기화	성공/실패
장치 초기화 취소	성공/실패
장치 삭제	성공/실패
역할 가져오기	성공/실패
역할 추가	성공/실패
역할 업데이트	성공/실패
역할 삭제	성공/실패
역할 바인딩	성공/실패
역할 바인딩 해제	성공/실패

이벤트용 관리자 감사 로그 메시지	상태
구성 설정 업데이트	성공/실패
워크플로 전자 메일 업데이트	성공/실패
워크플로 추가	성공/실패
워크플로 삭제	성공/실패
Active Directory 추가	성공/실패
Active Directory 업데이트	성공/실패
masteruserlist 추가	성공/실패
masteruserlist 업데이트	성공/실패
DNS 업데이트	성공/실패
네트워크 업데이트	성공/실패
로그 서버 업데이트	성공/실패
로그 서버의 로그 전송	성공/실패
syslog 업데이트	성공/실패
Receiver 업데이트 관련 업데이트	성공/실패
시간 서버 업데이트	성공/실패
신뢰 업데이트	성공/실패
서비스 레코드 추가	성공/실패
서비스 레코드 업데이트	성공/실패
Receiver 전자 메일 업데이트	성공/실패
패치 업로드	성공/실패
스냅샷 가져오기	성공/실패
앱 스토어 앱 세부 정보 가져오기	성공/실패
MDM 업데이트	성공/실패
MDM 삭제	성공/실패
HDX 추가	성공/실패
HDX 업데이트	성공/실패
HDX 삭제	성공/실패
브랜딩 추가	성공/실패
브랜딩 삭제	성공/실패

이벤트용 관리자 감사 로그 메시지	상태
SSL 오프로드 업데이트	성공/실패
계정 속성 추가	성공/실패
계정 속성 삭제	성공/실패
계정 속성 업데이트	성공/실패
알림 추가	성공/실패

사용자 감사 로그 파일: 등록된 장치의 사용자 활동과 관련된 정보가 포함됩니다.

참고:

사용자 감사 로그와 관리자 감사 로그에는 동일한 형식이 사용됩니다.

메시지 형식:

필수적인 날짜 및 타임스탬프 값을 제외한 다른 모든 특성은 선택 사항입니다. 선택적 필드는 메시지에서 “”로 표시됩니다. 예를 들면 다음과 같습니다.

```
<date> <timestamp> "<username/id>"<sessionid>"<deviceid>"<clientip>"<action>"<status>"<application name>"<app user id>"<user agent>"<details>"
```

다음 표에는 사용 가능한 사용자 감사 로그 이벤트가 나열되어 있습니다.

이벤트용 사용자 감사 로그 메시지	상태
로그인	성공/실패
세션 시간 초과	성공/실패
구독	성공/실패
등록 취소	성공/실패
사전 시작	성공/실패
AGEE SSO	성공/실패
Citrix Files 용 SAML 토큰	성공/실패
장치 등록	성공/실패
장치 확인	잠금/초기화
장치 업데이트	성공/실패
토큰 새로 고침	성공/실패

이벤트용 사용자 감사 로그 메시지

상태

암호 저장됨	성공/실패
암호 검색됨	성공/실패
사용자가 암호 변경을 시작함	성공/실패
모바일 클라이언트 다운로드	성공/실패
로그아웃	성공/실패
검색 서비스	성공/실패
끝점 서비스	성공/실패

MDM 기능

상태

REGHIVE	성공/실패
Cab 인벤토리	성공/실패
Cab	성공/실패
Cab 자동 설치	성공/실패
Cab 셀 설치	성공/실패
Cab 폴더 만들기	성공/실패
Cab 파일 가져오기	성공/실패
파일 폴더 만들기	성공/실패
파일 가져오기	성공/실패
파일 전송됨	성공/실패
스크립트 폴더 만들기	성공/실패
스크립트 가져오기	성공/실패
스크립트 전송됨	성공/실패
스크립트 셀 실행	성공/실패
스크립트 자동 실행	성공/실패
APK 인벤토리	성공/실패
APK	성공/실패
APK 셀 설치	성공/실패
APK 자동 설치	성공/실패

MDM 기능	상태
APK 폴더 만들기	성공/실패
APK 파일 가져오기	성공/실패
APK 앱	성공/실패
EXT 앱	성공/실패
목록 가져오기	성공/실패
목록 전송됨	성공/실패
장치 찾기	성공/실패
CFG	성공/실패
잠금 해제	성공/실패
SharePoint 초기화	성공/실패
SharePoint 구성	성공/실패
프로필 제거	성공/실패
응용 프로그램 제거	성공/실패
관리되지 않는 응용 프로그램 제거	성공/실패
관리되지 않는 프로필 제거	성공/실패
IPA 앱	성공/실패
EXT 앱	성공/실패
상환 코드 적용	성공/실패
설정 적용	성공/실패
장치 추적 사용	성공/실패
앱 관리 정책	성공/실패
SD 카드 초기화	성공/실패
암호화된 전자 메일 첨부 파일	성공/실패
브랜딩	성공/실패
보안 브라우저	성공/실패
컨테이너 브라우저	성공/실패
컨테이너 잠금 해제	성공/실패
컨테이너 암호 재설정	성공/실패

Citrix ADC 는 각 XenMobile 서버 클러스터 노드에 대한 HTTP 요청을 시뮬레이션하는 지능형 모니터링 프로브로 구성된 XenMobile 웹 서비스 상태도 모니터링합니다. 이 프로브는 서비스가 온라인 상태인지 확인한 후 수신된 응답에 따라 응답합니다. 노드가 예상대로 응답하지 않는 경우 Citrix ADC 는 서버를 중단 상태로 표시합니다. 또한 Citrix ADC 는 노드를 부하 분산 풀에서 제거하고, Citrix ADC 모니터링 솔루션을 통해 알림을 생성하는 데 사용할 이벤트를 기록합니다.

관리자는 표준 하이퍼바이저 모니터링 도구를 사용하여 XenMobile 가상 컴퓨터를 모니터링하고 CPU, 메모리, 스토리지 사용률 메트릭에 관한 알림을 제공할 수도 있습니다.

SQL Server 및 데이터베이스

SQL Server 및 데이터베이스 성능은 XenMobile Service 에 직접적인 영향을 미칩니다. XenMobile 인스턴스는 항상 데이터베이스에 액세스할 수 있어야 하며 SQL 인프라가 중단될 경우 오프라인으로 전환됩니다 (예: 응답하지 않음). XenMobile 콘솔은 SQL Server 에서 디스크 공간 문제가 발생한 후 잠시 동안 작동을 계속할 수 있습니다. 데이터베이스 가동 시간을 최대화하고 XenMobile 작업 부하를 처리하기에 충분한 수준의 성능을 유지하려면 SQL Server 의 상태를 사전에 모니터링해야 합니다. SQL Server 모니터링에 대한 자세한 내용은 [성능 모니터링 및 튜닝 개요](#)를 참조하십시오. 또한 XenMobile 환경이 확장에 따라 CPU, 메모리 및 스토리지에 대한 리소스 할당을 조정하여 서비스 수준 계약을 보장해야 합니다.

Citrix ADC

Citrix ADC 는 내부 스토리지에 메트릭을 기록하거나 외부 로깅 서버로 로그를 보낼 수 있는 기능을 제공합니다. Citrix ADC 로그를 프로덕션 Splunk 로깅 서버로 내보내도록 syslog 서버를 구성할 수 있습니다. Citrix ADC 에서는 다음과 같은 로깅 수준을 사용할 수 있습니다.

- 긴급
- 알림
- 중요
- 오류
- 경고
- 정보

로그 파일은 Citrix ADC 스토리지의 /var/log/ns.log 디렉터리에 newnslog 라는 이름으로도 저장됩니다. Citrix ADC 는 GZIP 알고리즘을 사용하여 파일을 롤오버하고 압축합니다. 로그 파일 이름은 newnslog.xx.gz 형식을 사용하며 여기서 xx 는 실행 번호를 나타냅니다.

Citrix ADC 는 모니터링 옵션으로 SNMP 트랩 및 알림도 지원합니다. SNMP 트랩 목록은 [SNMP 모니터링](#)을 참조하십시오.

재해 복구

March 15, 2024

재해 복구를 위해 활성/수동 장애 조치 (failover) 전략을 사용하여 여러 사이트가 포함된 XenMobile 배포를 설계하고 구성할 수 있습니다.

이 문서에서 설명하는 권장 재해 복구 전략은 다음으로 구성됩니다.

- 모든 엔터프라이즈 사용자에게 글로벌 서비스를 제공하는 첫 번째 지리적 위치의 데이터 센터에 있는 단일의 XenMobile 활성 사이트 (기본 사이트).
- 두 번째 지리적 위치의 데이터 센터에 있는 두 번째 XenMobile 사이트 (재해 복구 사이트). 이 재해 복구 사이트는 기본 사이트에서 사이트 전체 데이터 센터 장애가 발생하는 경우 활성-비활성 사이트 장애 조치 (failover) 를 제공합니다. 기본 사이트에는 장애 조치 (failover) 를 용이하게 하는 XenMobile, SQL 데이터베이스, Citrix ADC 인프라가 포함되며 기본 사이트에 대한 연결 실패 이벤트를 통해 사용자에게 XenMobile 에 대한 액세스를 제공합니다.

재해 복구 사이트의 XenMobile 서버는 정상 작동 중에 오프라인으로 유지되며 기본 사이트의 전체 사이트를 재해 복구 사이트로 장애 조치 (failover) 해야 하는 재해 복구 시나리오에서만 온라인으로 전환됩니다. 재해 복구 사이트의 SQL Server 는 재해 복구 사이트에서 XenMobile 서버를 시작하기 전에 활성 상태이고 연결을 제공할 준비가 되어 있어야 합니다.

이 재해 복구 전략은 중단 시 MDM 및 MAM 연결을 재해 복구 사이트로 라우팅하도록 DNS 를 변경함으로써 Citrix ADC 액세스 계층을 수동으로 장애 조치 (failover) 합니다.

참고:

이 아키텍처를 사용하려면 비동기식 데이터베이스 백업에 대한 프로세스와 SQL 인프라의 고가용성을 보장할 방법이 있어야 합니다.

재해 복구 장애 조치 (failover) 프로세스

1. 재해 복구 장애 조치 (failover) 프로세스를 테스트하려면 기본 사이트에서 XenMobile 서버를 종료하여 사이트 장애를 시뮬레이션합니다.
2. XenMobile 서버의 공용 DNS 레코드를 재해 복구 사이트의 외부 IP 주소를 가리키도록 변경합니다.
3. SQL Server 의 내부 DNS 레코드를 재해 복구 사이트의 SQL Server IP 주소를 가리키도록 변경합니다.
4. 재해 복구 사이트에서 XenMobile SQL 데이터베이스를 온라인으로 전환합니다. SQL Server 및 데이터베이스가 활성 상태이고 로컬 XenMobile 서버에서 사이트로의 연결을 제공할 준비가 되었는지 확인합니다.
5. 재해 복구 사이트에서 XenMobile 서버를 켭니다.

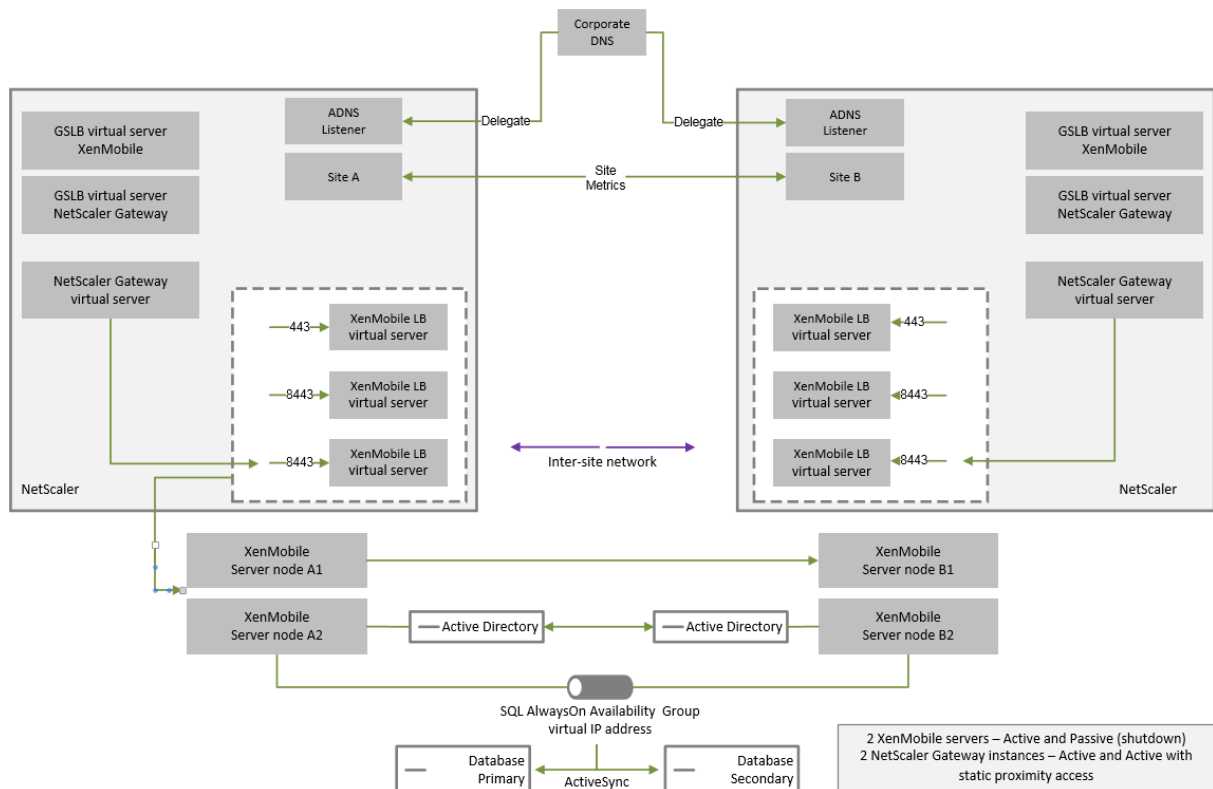
XenMobile 서버 업데이트 프로세스

패치 및 릴리스로 XenMobile 을 업데이트할 때는 다음 단계에 따라 기본 서버와 재해 복구 서버의 코드를 동일하게 유지하십시오.

1. 기본 사이트의 XenMobile 서버에 패치가 적용되었거나 업그레이드되었는지 확인합니다.
2. SQL Server 의 DNS 레코드가 기본 사이트의 활성 SQL Server 데이터베이스로 확인되는지 확인합니다.
3. 재해 복구 사이트의 XenMobile 서버를 온라인으로 전환합니다. 이 서버는 업그레이드 프로세스 중에만 WAN 의 기본 사이트 데이터베이스에 연결합니다.
4. 필요한 패치 및 업데이트를 모든 재해 복구 사이트의 XenMobile 서버에 적용합니다.
5. XenMobile Server 를 다시 시작하고 패치 또는 업그레이드가 성공했는지 확인합니다.

재해 복구 참조 아키텍처 다이어그램

다음 다이어그램은 XenMobile 의 재해 복구 배포에 대한 아키텍처 개요를 보여줍니다.



재해 복구용 GSLB

이 아키텍처의 주요 요소는 GSLB(Global Server Load Balancing) 를 사용하여 트래픽을 올바른 데이터 센터로 전달하는 것입니다.

기본적으로 XenMobile 용 Citrix ADC 마법사에서는 재해 복구에 GSLB 를 사용하지 않는 방식으로 Citrix Gateway 가 구성됩니다. 따라서 추가 조치를 취해야 합니다.

GSLB의 작동 방식

GSLB는 DNS 형태로 존재합니다. 참여 Citrix ADC 장비는 신뢰할 수 있는 DNS 서버 역할을 하며 DNS 레코드를 올바른 IP 주소 (일반적으로 트래픽을 수신할 수 있는 VIP)로 확인합니다. Citrix ADC 장비는 트래픽을 해당 시스템으로 전달하는 DNS 쿼리에 응답하기 전에 시스템 상태를 확인합니다.

레코드가 확인되면 트래픽을 확인하는 GSLB의 역할이 완료됩니다. 클라이언트는 대상 VIP(가상 IP) 주소와 직접 통신합니다. DNS 클라이언트 동작은 레코드의 만료 방식과 시기를 제어하는 데 있어서 중요한 역할을 합니다. 이는 주로 Citrix ADC 시스템의 경계 외부에서 수행됩니다. 따라서 GSLB에는 DNS 이름 확인과 동일한 제한이 적용됩니다. 클라이언트가 응답을 캐시하므로 이 방식의 부하 분산은 기존의 부하 분산과 달리 실시간으로 수행되지 않습니다.

Citrix ADC의 GSLB 구성 (사이트, 서비스 및 모니터 포함)은 올바른 DNS 이름 확인을 제공하는 데 사용됩니다.

서버 계시를 위한 실제 구성 (이 시나리오에서는 XenMobile용 Citrix ADC 마법사에서 생성되는 구성)은 GSLB의 영향을 받지 않습니다. GSLB는 Citrix ADC에 있는 개별 서비스입니다.

XenMobile에서 GSLB를 사용하는 경우의 도메인 위임 문제

XenMobile용 Citrix ADC 마법사는 XenMobile용 Citrix Gateway를 구성합니다. 이 마법사는 부하 분산 가상 서버 세 개와 Citrix Gateway 가상 서버 한 개를 생성합니다.

부하 분산 가상 서버 두 개는 포트 443 및 8443에서 MDM 트래픽을 처리합니다. Citrix Gateway는 포트 8443에서 MAM 트래픽을 수신한 후 세 번째 서버인 MAM 부하 분산 가상 서버에 전달합니다. MAM 부하 분산 가상 서버로 이동하는 모든 트래픽은 Citrix Gateway를 통과합니다.

MAM 부하 분산 가상 서버에는 XenMobile 서버와 동일한 SSL 인증서가 필요하며 장치 등록 시 사용된 FQDN과 동일한 FQDN이 사용됩니다. 또한 MAM 부하 분산 서버는 MDM 부하 분산 서버 중 하나와 동일한 포트 (8443)를 사용합니다. 트래픽을 확인하기 위해 XenMobile용 Citrix ADC 마법사는 Citrix Gateway에 로컬 DNS 레코드를 생성합니다. DNS 레코드는 장치 등록 시 사용된 FQDN과 일치합니다.

이 구성은 XenMobile 서버 URL이 GSLB 도메인 URL이 아닌 경우 적용됩니다. GSLB 도메인 URL이 재해 복구를 이유로 XenMobile 서버 URL로 사용된 경우 로컬 DNS 레코드로 인해 Citrix Gateway가 MDM 부하 분산 서버로의 트래픽을 확인할 수 없게 됩니다.

GSLB 재해 복구의 CNAME 방법

XenMobile용 Citrix ADC 마법사의 기본 구성으로 인해 발생하는 문제를 해결하려면 상위 도메인 ([company.com](#))에 XenMobile 서버 FQDN에 대한 CNAME 레코드를 생성하고 신뢰할 수 있는 Citrix ADC의 위임된 하위 영역 ([gslb.company.com](#))에 있는 레코드를 가리키면 됩니다. 이렇게 하면 트래픽을 확인하는 데 필요한 MAM 부하 분산 VIP 주소에 대한 정적 DNS A 레코드를 생성할 수 있습니다.

1. 외부 DNS에서 Citrix ADC GSLB의 GSLB 도메인 FQDN을 가리키는 XenMobile 서버 FQDN에 대한 CNAME을 생성합니다. 두 개의 GSLB 도메인이 필요합니다. 하나는 MDM 트래픽을 위한 것이고 다른 하나는 MAM(Citrix Gateway) 트래픽을 위한 것입니다.

예:

```
CNAME = xms.company.com IN CNAME xms.gslb.comany.com
```

2. 각 사이트의 Citrix Gateway 인스턴스에서 CNAME 레코드가 가리키는 FQDN 으로 GSLB 가상 서버를 생성합니다.

예:

```
bind gslb vserver xms-gslb -domainName xms.gslb.company.com
```

XenMobile 용 Citrix ADC 마법사를 사용하여 Citrix Gateway 를 배포하는 경우 MAM 부하 분산 서버를 구성할 때 XenMobile 서버 URL 을 사용하십시오. 그러면 XenMobile 서버 URL 에 대한 정적 DNS A 레코드가 생성됩니다.

3. XenMobile 서버 URL([xms.company.com](#)) 을 사용하여 Secure Hub 에 등록하는 클라이언트를 테스트합니다.

이 예에서는 다음 FQDN 을 사용합니다.

- [xms.company.com](#) - MDM 트래픽과 장치 등록에 사용되는 URL 이며 이 예에서는 XenMobile 용 Citrix ADC 마법사를 사용하여 구성되었습니다.
- [xms.gslb.company.com](#) - XenMobile 서버의 GSLB 도메인 FQDN 입니다.

Citrix 지원 프로세스

March 24, 2022

Citrix 기술 지원 서비스를 켜면 Citrix 제품 관련 문제에 대한 지원을 받을 수 있습니다. 이 그룹은 해결 방법 및 해결책을 제공하며 개발 팀과 협력하여 솔루션을 제공합니다.

Citrix Consulting Services 또는 Citrix Education Services 는 제품 교육과 관련된 지원과 함께 제품 사용, 구성, 설치 또는 환경 설계 및 아키텍처에 관한 조언을 제공합니다.

Citrix Consulting 은 POC, 경제적 영향 평가, 인프라 상태 확인, 설계 요구 사항 분석, 아키텍처 설계 확인, 통합 및 운영 프로세스 개발 등 Citrix 제품 관련 프로젝트를 지원합니다.

Citrix Education 은 Citrix 가상화, 클라우드 및 네트워킹 기술에 대한 업계 최고의 IT 교육 및 인증을 제공합니다.

지원 사례를 작성하기 전에 자가 지원 리소스 및 권장 사항을 완벽하게 검토하는 것이 좋습니다. 예를 들어 Citrix 기술 전문가가 작성한 문서와 공지에 액세스하거나, Citrix 솔루션 및 기술에 대한 제품 설명서를 보거나, Citrix 경영진, 제품 팀 및 기술 전문가의 직설을 읽어 볼 수 있는 다수의 위치가 있습니다. 각각 [Knowledge Center](#), [제품 설명서](#) 및 [블로그](#) 페이지를 참조하십시오.

추가적인 대화형 지원이 필요하다면 토론 포럼에 참여하여 다른 고객으로부터 질문에 대한 실시간 답변을 얻거나, 사용자 그룹 및 관심 그룹 내에서 아이디어, 의견, 기술 정보 및 모범 사례를 공유하거나, Citrix 지원의 소셜 네트워킹 사이트를 모니터링하는 Citrix 지원 엔지니어와 상호 작용할 수 있습니다. [지원 포럼](#) 및 [Citrix 커뮤니티](#) 페이지를 각각 참조하십시오.

교육 및 인증 과정에 액세스하여 기술을 강화할 수도 있습니다. [Citrix Education](#)을 참조하십시오.

Citrix Insight Services 는 단순한 온라인 문제 해결 플랫폼과 Citrix 환경을 위한 상태 검사기를 제공합니다. XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor 및 Citrix Gateway 에 사용할 수 있습니다. [Analysis Tool\(분석 도구\)](#)을 참조하십시오.

기술 지원을 받으려면 전화 또는 웹을 통해 지원 사례를 만들어야 합니다. 중요도가 낮거나 중간인 문제에 대해서는 웹을 사용하고, 중요도가 높은 문제에 대해서는 전화 옵션을 사용할 수 있습니다. XenMobile 문제에 대해 지원을 문의하려면 [Citrix 지원 서비스](#)를 참조하십시오.

Citrix 솔루션 제공에 대한 방대한 경험을 갖춘, 고도로 숙련된 단일의 담당자를 원한다면 Citrix 서비스의 Technical Relationship Manager 에게 문의할 수 있습니다. Citrix 서비스 제공 및 이점에 대한 자세한 내용은 [Citrix Worldwide Services](#)를 참조하십시오.

XenMobile 에서 그룹 등록 초대 보내기

March 15, 2024

XenMobile Server 에서 그룹 및 중첩 그룹에 등록 초대를 보낼 수 있습니다. Windows 장치에서는 등록 초대를 사용할 수 없습니다.

그룹 초대를 설정할 때 하나 이상의 장치 플랫폼을 지정할 수 있습니다. 또한 장치에 태그를 지정하여 회사 소유의 장치를 직원 소유의 장치와 구분하는 등의 작업을 수행할 수 있습니다. 그런 다음 사용자 장치에 대한 인증 유형을 설정합니다.

참고:

사용자 지정 알림 템플릿을 사용하려는 경우 등록 모드를 구성하기 전에 템플릿을 설정해야 합니다. 알림 템플릿에 대한 자세한 내용은 [알림 템플릿 만들기 및 업데이트](#)를 참조하십시오.

사용자 계정, 역할 및 등록 보안 모드와 초대의 기본 구성에 대한 자세한 내용은 [사용자 계정, 역할 및 등록](#)을 참조하십시오.

일반 단계

1. XenMobile 콘솔에서 관리 > 등록 초대로 이동합니다.
2. 화면 왼쪽 위의 추가를 클릭하고 초대 추가를 클릭합니다.
3. 받는 사람 메뉴에서 그룹을 클릭합니다.

이 단계에서 하나 이상의 플랫폼을 선택할 수 있습니다. 회사 내에 서로 다른 운영 체제 플랫폼 조합이 있는 경우 모든 플랫폼을 선택합니다. 확실히 사용되지 않는 플랫폼만 선택을 취소합니다.
4. 초대 프로세스 중에 장치 태그를 지정하도록 선택할 수 있습니다. 회사 또는 직원을 선택합니다.

태그를 지정하면 회사 소유의 장치와 직원 소유의 장치를 쉽게 구분할 수 있습니다.
5. 도메인 목록에서 그룹이 있는 도메인을 선택합니다.

6. 그룹 목록에서 초대할 보낼 Active Directory 그룹을 선택합니다.
7. 등록 모드를 사용하여 사용자에게 대해 선호하는 인증 보안 유형을 설정할 수 있습니다.

- 사용자 이름 + 암호
- 높은 수준의 보안
- 초대 URL
- 초대 URL + PIN
- 초대 URL + 암호
- 2 단계
- 사용자 이름 + PIN

참고:

등록 초대를 보내기 위해서는 초대 **URL**, 초대 **URL + PIN**, 초대 **URL + 암호** 등록 보안 모드만 사용할 수 있습니다. 사용자 이름 + 암호, 2 단계 또는 사용자 이름 + PIN 으로 등록하는 장치의 경우 사용자는 Secure Hub 에서 자격 증명을 수동으로 입력해야 합니다.

8. 에이전트 다운로드, 등록 **URL**, 등록 **PIN** 및 등록 확인 템플릿에 대해 이전에 만든 사용자 지정 알림 템플릿을 선택하거나 목록에 있는 기본값을 선택합니다.

사용자 지정 알림 템플릿을 사용하려는 경우 등록 모드를 구성하기 전에 템플릿을 설정해야 합니다. 알림 템플릿에 대한 자세한 내용은 [알림](#)을 참조하십시오.

이러한 알림 템플릿에는 XenMobile 내에서 구성한 SMTP 서버 설정을 사용합니다. 계속하기 전에 SMTP 정보를 먼저 설정합니다.

참고:

다음 이후에 만료 및 최대 시도 횟수 옵션은 선택한 등록 모드 옵션에 따라 변경됩니다. 이러한 옵션은 변경할 수 없습니다.

9. 초대 보내기에 대해 커짐을 선택한 다음 저장 및 보내기를 클릭하여 프로세스를 완료합니다.

중첩 그룹 지원

중첩 그룹을 사용하여 초대를 보낼 수 있습니다. 일반적으로 중첩 그룹은 유사한 권한을 가진 그룹이 서로 바인딩되어 있는 대규모 환경에서 사용됩니다.

설정 > **LDAP** 로 이동하고 중첩 그룹 지원 옵션을 사용하도록 설정합니다.

문제 해결 및 알려진 제한

문제: Active Directory 그룹에서 제거된 사용자에게도 초대가 전송됩니다.

해결 방법: Active Directory 환경의 규모에 따라 변경 내용이 모든 서버로 전파되는 데 최대 6 시간이 소요될 수 있습니다. 최근에 사용자 또는 중첩 그룹을 제거한 경우 XenMobile 에서 이러한 사용자가 그룹의 일부로 간주될 수 있습니다.

그러므로 그룹에 다른 그룹 초대를 보내기 전에 최대 6 시간을 기다리는 것이 가장 좋습니다.

온-프레미스 장치 상태 증명 서버 구성

March 15, 2024

Windows 10 및 Windows 11 모바일 장치에 대한 DHA(장치 상태 증명) 를 온-프레미스 Windows 서버를 통해 사용할 수 있습니다. DHA 온-프레미스를 사용하려면 먼저 DHA 서버를 구성해야 합니다.

DHA 서버를 구성한 후 온-프레미스 DHA 서비스를 사용하도록 설정하는 XenMobile Server 정책을 만듭니다. 이 정책 만들기기에 대한 자세한 내용은 [장치 상태 증명 장치 정책](#)을 참조하십시오.

DHA 서버의 사전 요구 사항

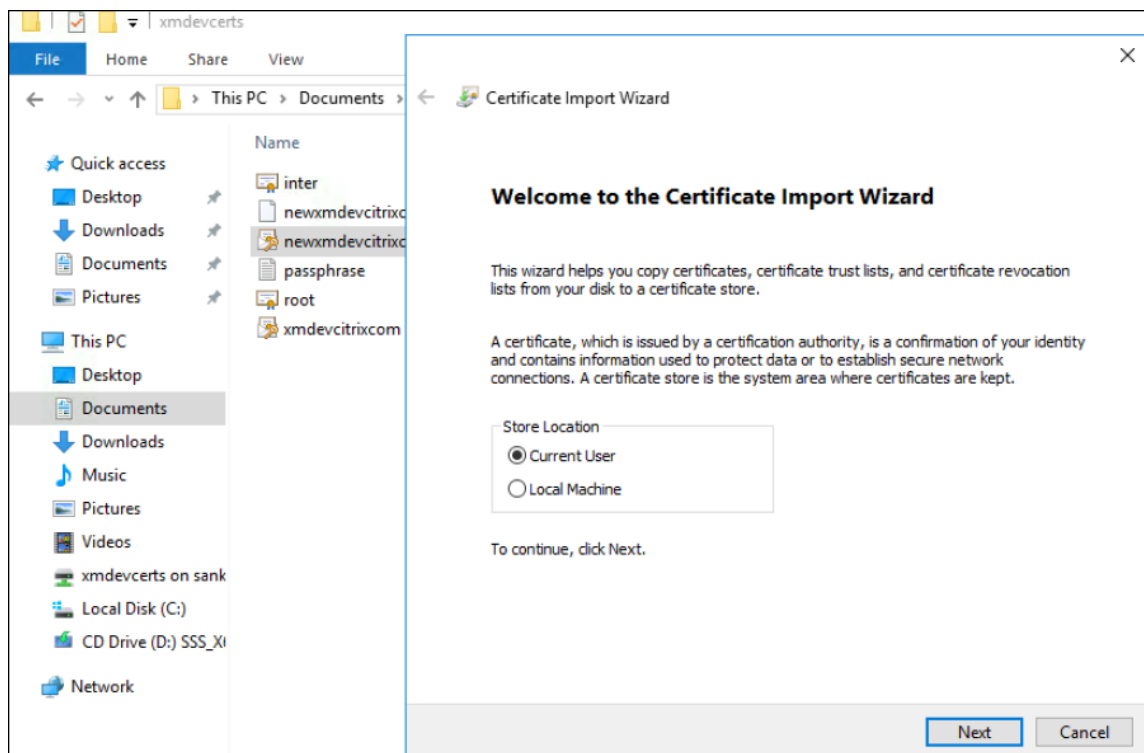
- 데스크톱 환경 설치 옵션을 사용하여 설치된 Windows Server Technical Preview 5 이상을 실행하는 서버.
- 하나 이상의 Windows 10 및 Windows 11 클라이언트 장치. 이러한 장치에는 최신 버전의 Windows 를 실행하는 TPM 1.2 또는 2.0 이 있어야 합니다.
- 인증서:
 - **DHA SSL** 인증서: 내보내기 가능한 개인 키를 사용하여 엔터프라이즈의 신뢰할 수 있는 루트에 체인으로 연결되는 x.509 SSL 인증서. 이 인증서는 다음과 같은 통신을 포함하여 전송 중인 DHA 데이터 통신을 보호합니다.
 - ★ 서버 간 통신 (DHA 서비스 및 MDM 서버)
 - ★ 서버-클라이언트 간 통신 (DHA 서비스 및 Windows 10 또는 Windows 11 장치)
 - **DHA 서명** 인증서: 내보내기 가능한 개인 키를 사용하여 엔터프라이즈의 신뢰할 수 있는 루트에 체인으로 연결되는 x.509 인증서. DHA 서비스는 이 인증서를 디지털 서명에 사용합니다.
 - **DHA 암호화** 인증서: 내보내기 가능한 개인 키를 사용하여 엔터프라이즈의 신뢰할 수 있는 루트에 체인으로 연결되는 x.509 인증서. DHA 서비스는 이 인증서를 암호화에도 사용합니다.
- 다음과 같은 인증서 유효성 검사 모드 중에서 하나를 선택합니다.
 - **EKCert:** EKCert 유효성 검사 모드는 인터넷에 연결되지 않은 조직의 장치에 최적화되었습니다. EKCert 유효성 검사 모드에서 실행되는 DHA 서비스에 연결하는 장치는 인터넷에 직접 연결할 수 없습니다.
 - **AIKCert:** AIKCert 유효성 검사 모드는 인터넷에 액세스할 수 있는 작동 환경에 최적화되었습니다. AIKCert 유효성 검사 모드에서 실행되는 DHA 서비스에 연결하는 장치는 인터넷에 직접 연결할 수 있고 Microsoft 에서 AIK 인증서를 가져올 수 있어야 합니다.

Windows 서버에 DHA 서버 역할 추가

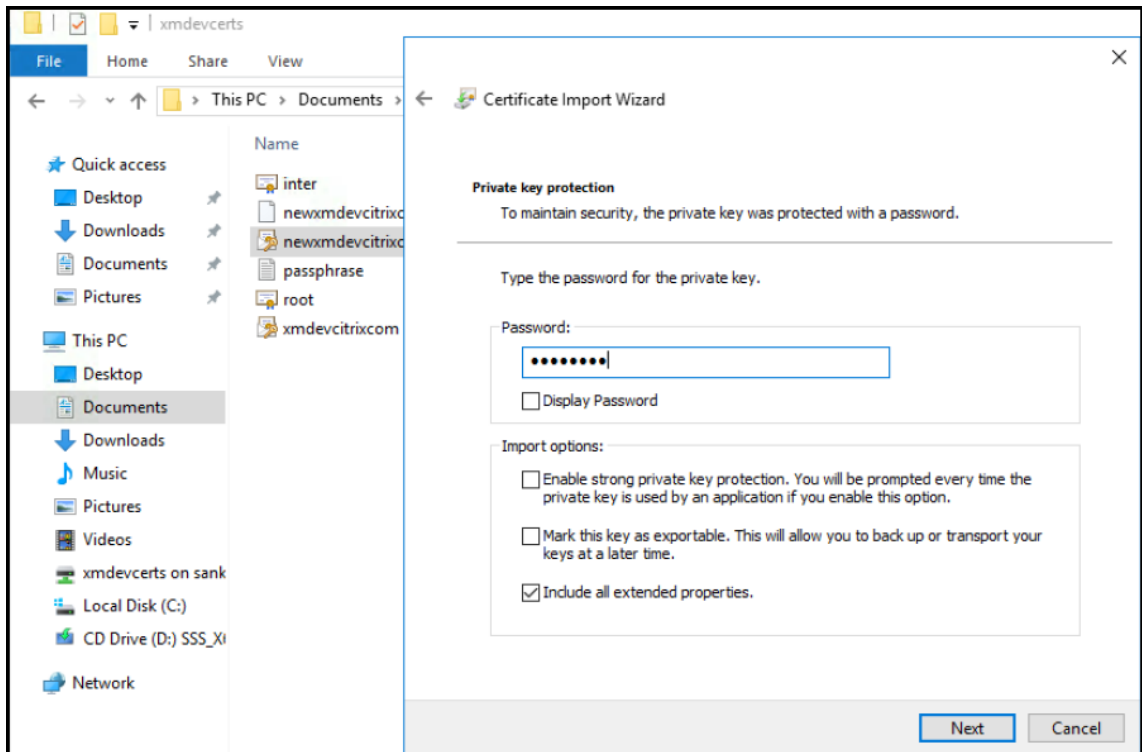
1. Windows 서버에서 서버 관리자가 이미 열려 있지 않은 경우 시작을 클릭하고 서버 관리자를 클릭합니다.
2. 역할 및 기능 추가를 클릭합니다.
3. 시작하기 전에 페이지에서 다음을 클릭합니다.
4. 설치 유형 선택 페이지에서 역할 기반 또는 기능 기반 설치를 클릭하고 다음을 클릭합니다.
5. 대상 서버 선택 페이지에서 서버 풀에서 서버 선택을 클릭하고 서버를 선택한 후 다음을 클릭합니다.
6. 서버 역할 선택 페이지에서 장치 상태 증명 확인란을 선택합니다.
7. 선택 사항: 기능 추가를 클릭하여 필요한 다른 역할 서비스 및 기능을 설치합니다.
8. 다음을 클릭합니다.
9. 기능 선택 페이지에서 다음을 클릭합니다.
10. 웹 서버 역할 (**IIS**) 페이지에서 다음을 클릭합니다.
11. 역할 서비스 선택 페이지에서 다음을 클릭합니다.
12. 장치 상태 증명 서비스 페이지에서 다음을 클릭합니다.
13. 설치 선택 확인 페이지에서 설치를 클릭합니다.
14. 설치가 완료되면 닫기를 클릭합니다.

서버의 인증서 저장소에 SSL 인증서 추가

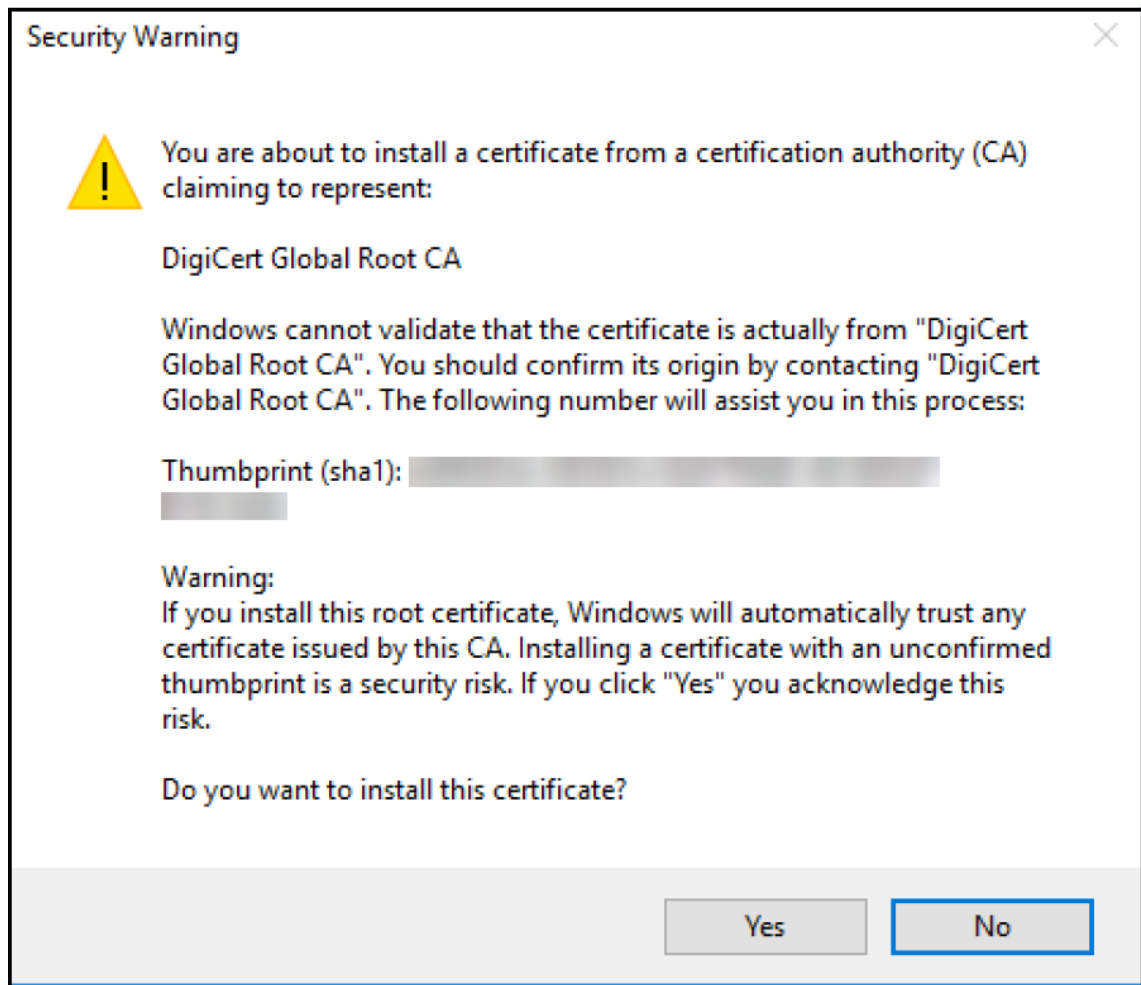
1. SSL 인증서 파일로 이동하고 파일을 선택합니다.
2. 현재 사용자를 저장소 위치로 선택하고 다음을 클릭합니다.



3. 개인 키에 대한 암호를 입력합니다.
4. 확장 속성 모두 포함 가져오기 옵션이 선택되었는지 확인합니다. 다음을 클릭합니다.

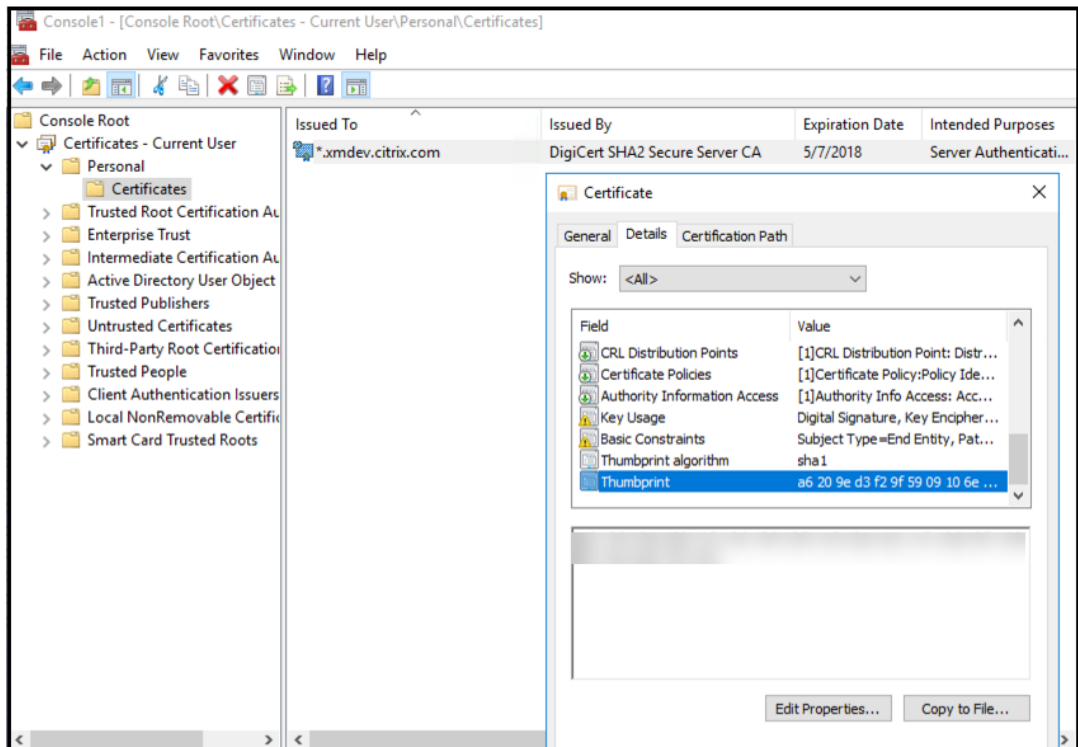


5. 이 창이 나타나면 예를 클릭합니다.

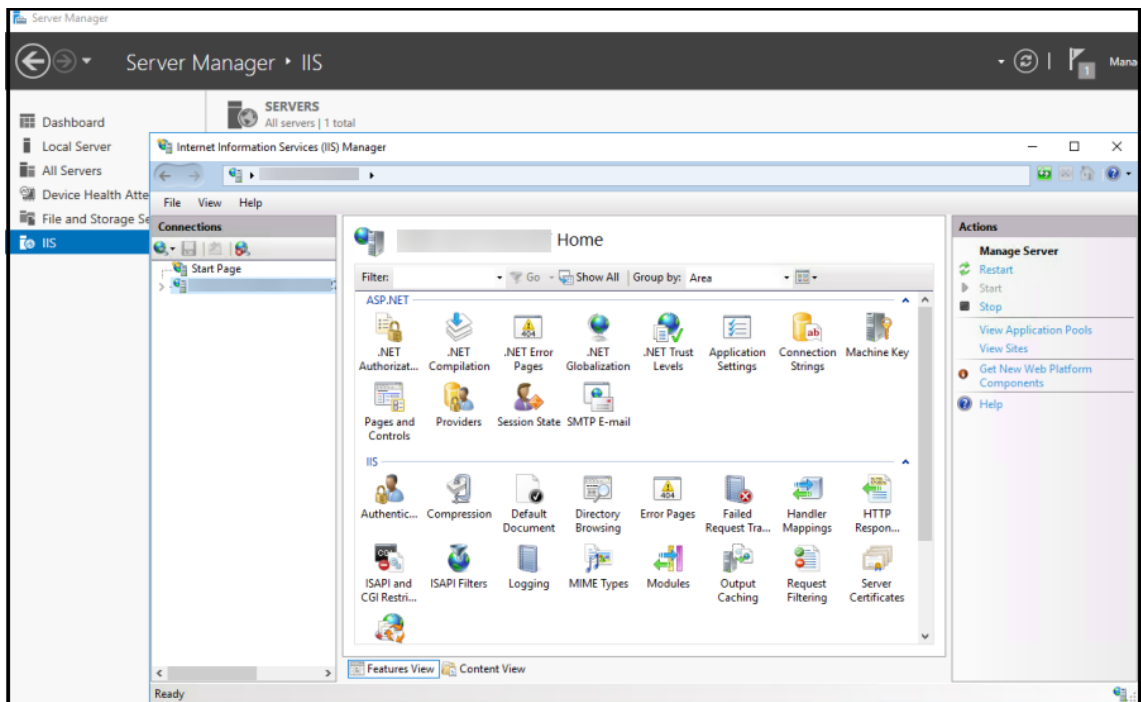


6. 인증서가 설치되었는지 확인합니다.

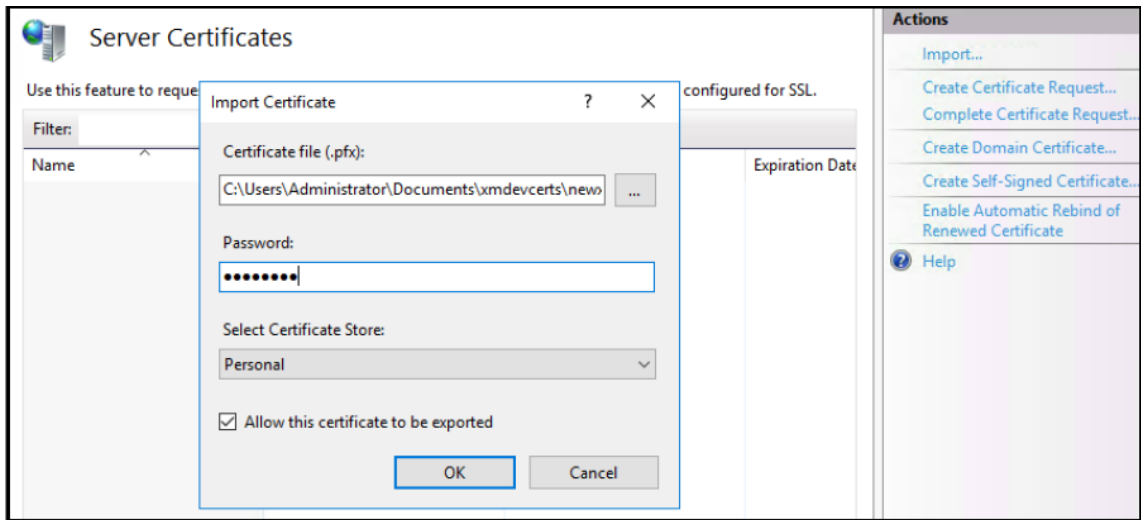
- a) 명령 프롬프트 창을 엽니다.
- b) **mmc** 를 입력하고 Enter 키를 누릅니다. 로컬 컴퓨터 저장소의 인증서를 보려면 관리자 역할이 있어야 합니다.
- c) 파일 메뉴에서 스냅인 추가/제거를 클릭합니다.
- d) 추가를 클릭합니다.
- e) 독립 실행형 스냅인 추가 대화 상자에서 인증서를 선택합니다.
- f) 추가를 클릭합니다.
- g) 인증서 스냅인 대화 상자에서 내 사용자 계정을 선택합니다. 서비스 계정 소유자로 로그인한 경우 서비스 계정을 선택합니다.
- h) 컴퓨터 선택 대화 상자에서 마침을 클릭합니다.



7. 서버 관리자 > IIS 로 이동하고 아이콘 목록에서 서버 인증서를 선택합니다.

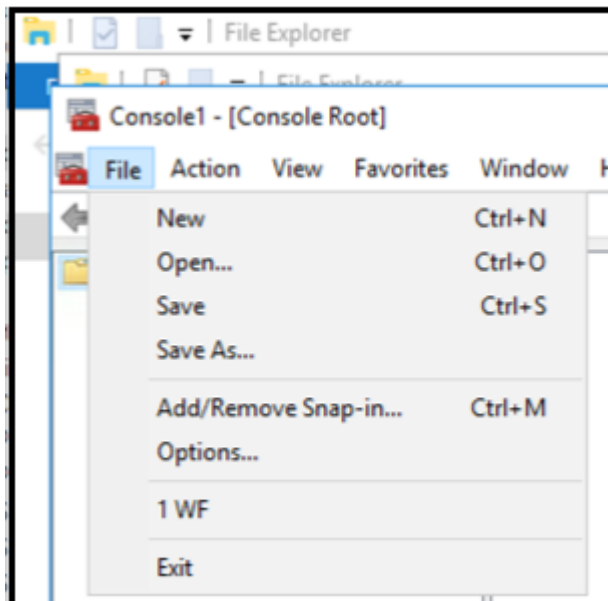


8. 작업 메뉴에서 가져오기...를 선택하여 SSL 인증서를 가져옵니다.

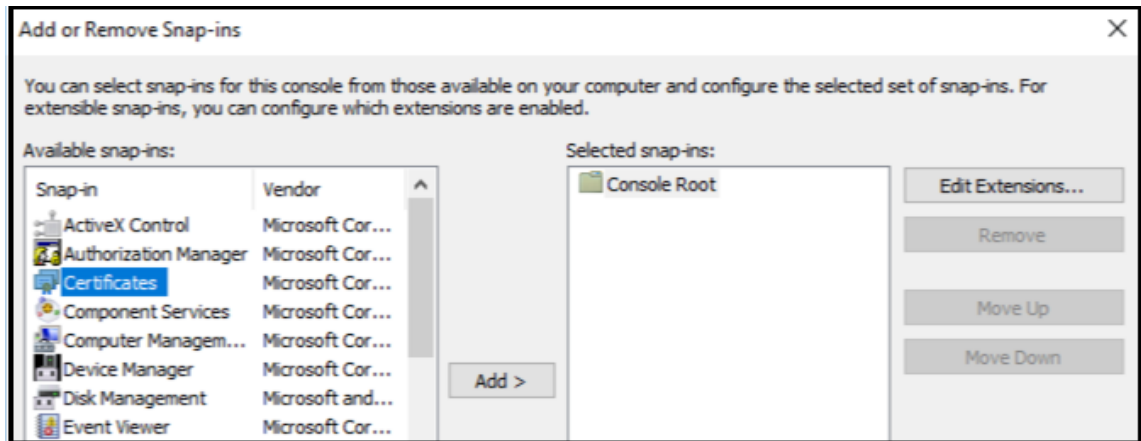


인증서 지문 검색 및 저장

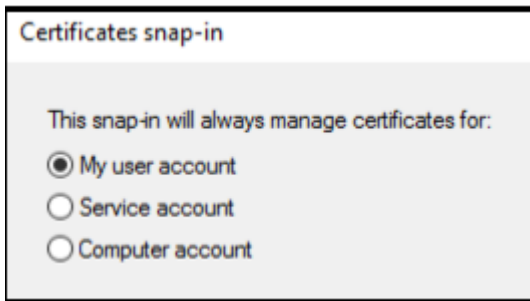
1. 파일 탐색기 검색 표시줄에 **mmc** 를 입력합니다.
2. 콘솔 루트 창에서 파일 > 스냅인 추가/제거...를 클릭합니다.



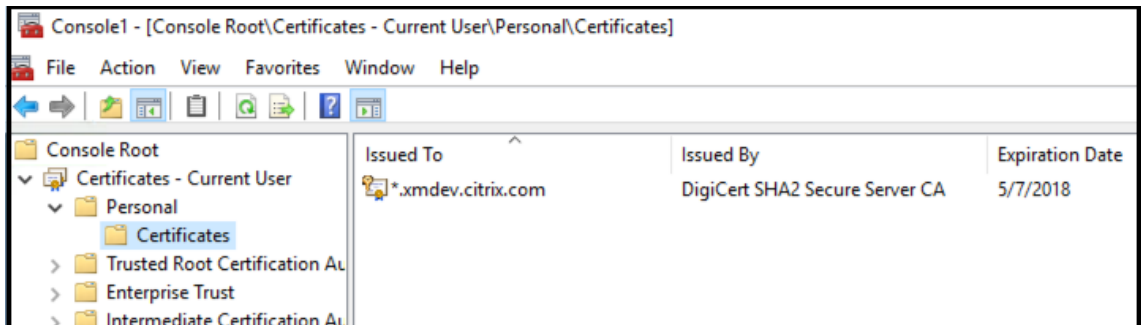
3. 사용 가능한 스냅인에서 인증서를 선택하고 선택한 스냅인에 추가합니다.



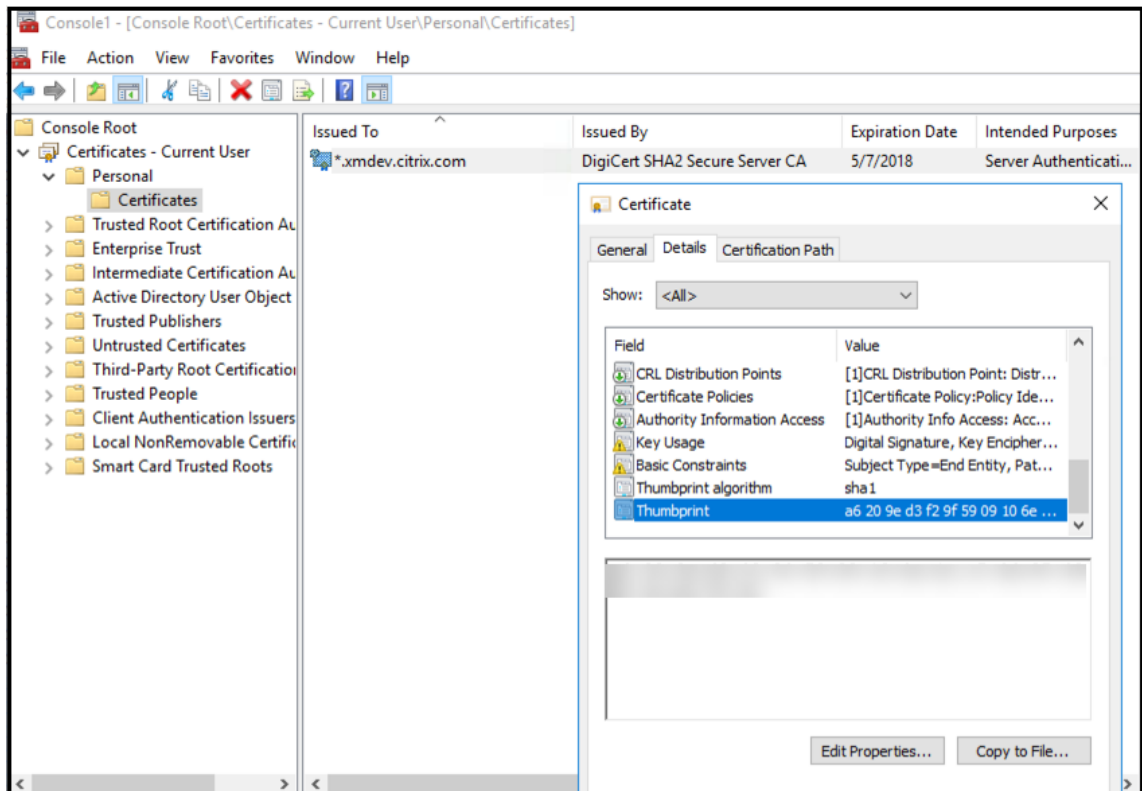
4. 내 사용자 계정을 선택합니다.



5. 인증서를 선택하고 확인을 클릭합니다.



6. 인증서를 두 번 클릭하고 세부 정보 탭을 선택합니다. 아래로 스크롤하여 인증서 지문을 표시합니다.



7. 지문을 파일에 복사합니다. PowerShell 명령에서 지문을 사용하는 경우 공백을 제거합니다.

서명 및 암호화 인증서 설치

Windows 서버에서 다음 PowerShell 명령을 실행하여 서명 및 암호화 인증서를 설치합니다.

표시된 것과 같이 ReplaceWithThumbprint 자리 표시자를 바꾸고 큰따옴표로 묶습니다.

```
1 $key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
2   $_.Thumbprint -like "ReplaceWithThumbprint" }
3
4
5 $keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
6
7 $keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
8   $keyname icacls $keypath /grant IIS_IUSRS`:R
9 <!--NeedCopy-->
```

TPM 루트 인증서 추출 및 신뢰할 수 있는 인증서 패키지 설치

Windows 서버에서 다음 명령을 실행합니다.

```
1 mkdir .\TrustedTpm
2
```

```
3 expand -F:* .\TrustedTpm.cab .\TrustedTpm
4
5 cd .\TrustedTpm
6
7 .\setup.cmd
8 <!--NeedCopy-->
```

DHA 서비스 구성

Windows 서버에서 다음 명령을 실행하여 DHA 서비스를 구성합니다.

ReplaceWithThumbprint 자리 표시자를 바꿉니다.

```
1 Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
   ReplaceWithThumbprint
2
3 -SigningCertificateThumbprint ReplaceWithThumbprint
4
5 -SslCertificateStoreName My -SslCertificateThumbprint
   ReplaceWithThumbprint
6
7 -SupportedAuthenticationSchema "AikCertificate"
8 <!--NeedCopy-->
```

Windows 서버에서 다음 명령을 실행하여 DHA 서비스에 대한 인증서 체인 정책을 설정합니다.

```
1 $policy = Get-DHASCertificateChainPolicy
2
3 $policy.RevocationMode = "NoCheck"
4
5 Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
6 <!--NeedCopy-->
```

다음 프롬프트에 다음과 같이 응답합니다.

```
1 Confirm
2
3 Are you sure you want to perform this action?
4
5 Performing the operation "Install-DeviceHealthAttestation" on
   target "WIN-N27D1FKCEBT".
6
7 [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?]
   Help (default is "Y"): A
8
9 Adding SSL binding to website 'Default Web Site'.
10
11 Add SSL binding?
12
13 [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
14
```

```

15 Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17 Add application pool?
18
19 [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
20
21 Adding web application 'DeviceHealthAttestation' to website '
    Default Web Site'.
22
23 Add web application?
24
25 [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
26
27 Adding firewall rule 'Device Health Attestation Service' to allow
    inbound connections on port(s) '443'.
28
29 Add firewall rule?
30
31 [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
32
33 Setting initial configuration for Device Health Attestation Service
    .
34
35 Set initial configuration?
36
37 [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
38
39 Registering User Access Logging.
40
41 Register User Access Logging?
42
43 [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
44 <!--NeedCopy-->

```

구성 확인

DHASActiveSigningCertificate 가 활성 상태인지 확인하려면 서버에서 다음 명령을 실행합니다.

```
Get-DHASActiveSigningCertificate
```

인증서가 활성 상태인 경우 인증서 유형 (서명) 과 지문이 표시됩니다.

DHASActiveSigningCertificate 가 활성 상태인지 확인하려면 서버에서 다음 명령을 실행합니다.

표시된 것과 같이 ReplaceWithThumbprint 자리 표시자를 바꾸고 큰따옴표로 묶습니다.

```

1 Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
   -Force
2
3 Get-DHASActiveEncryptionCertificate
4 <!--NeedCopy-->

```

인증서가 활성 상태인 경우 지문이 나타납니다.

최종 확인을 수행하려면 다음 URL 로 이동합니다.

<https://<dha.myserver.com>/DeviceHealthAttestation/ValidateHealthCertificate/v1>

DHA 서비스가 실행 중인 경우 “메서드를 사용할 수 없음” 이 나타납니다.



Secure Mail 푸시 알림을 통한 EWS 의 인증서 기반 인증 구성

March 15, 2024

작성자: Vijay Kumar Kunchakuri

Secure Mail 푸시 알림이 작동하려면 인증서 기반 인증을 사용하도록 Exchange Server 를 구성해야 합니다. Secure Hub 를 인증서 기반 인증을 사용하여 XenMobile 에 등록한 경우 이 요구 사항을 충족해야 합니다.

인증서 기반 인증을 사용하여 Exchange 메일 서버에 Active Sync 및 EWS(Exchange 웹 서비스) 가상 디렉터리를 구성해야 합니다.

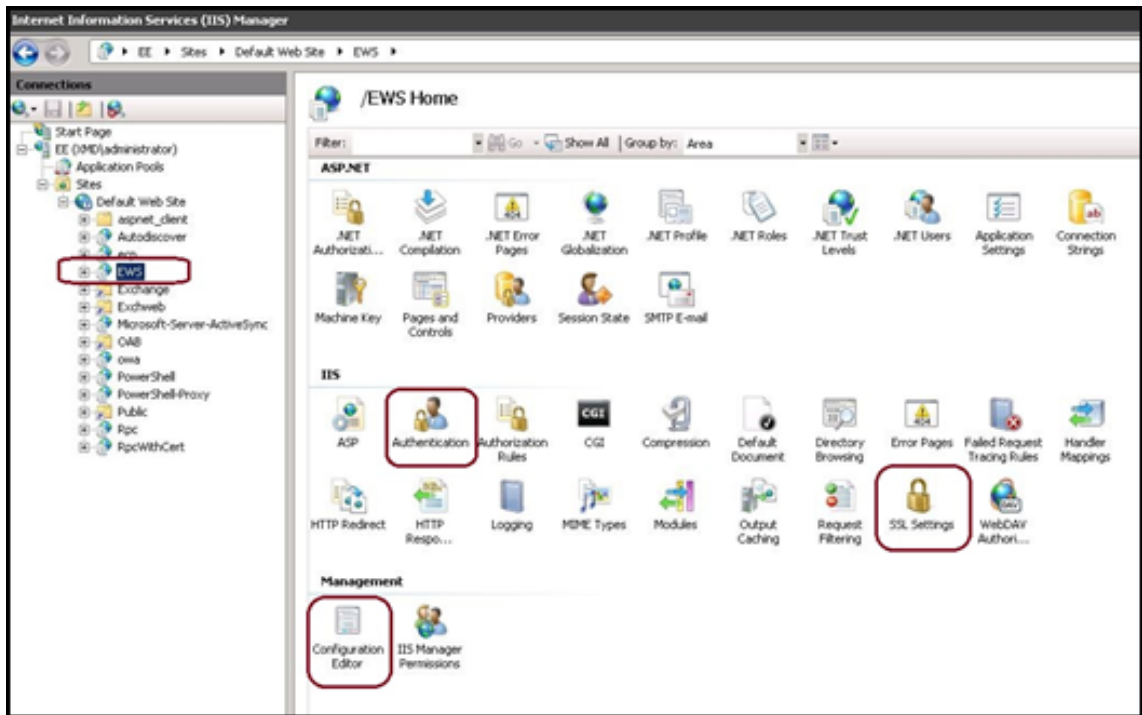
이러한 구성을 완료하지 않으면 Secure Mail 푸시 알림에 대한 구독이 실패하고 Secure Mail 에서 배지 업데이트가 수행되지 않습니다.

이 문서에서는 인증서 기반 인증을 구성하는 단계를 설명합니다. 구성은 Exchange Server 의 EWS 가상 디렉터리에 대한 것입니다.

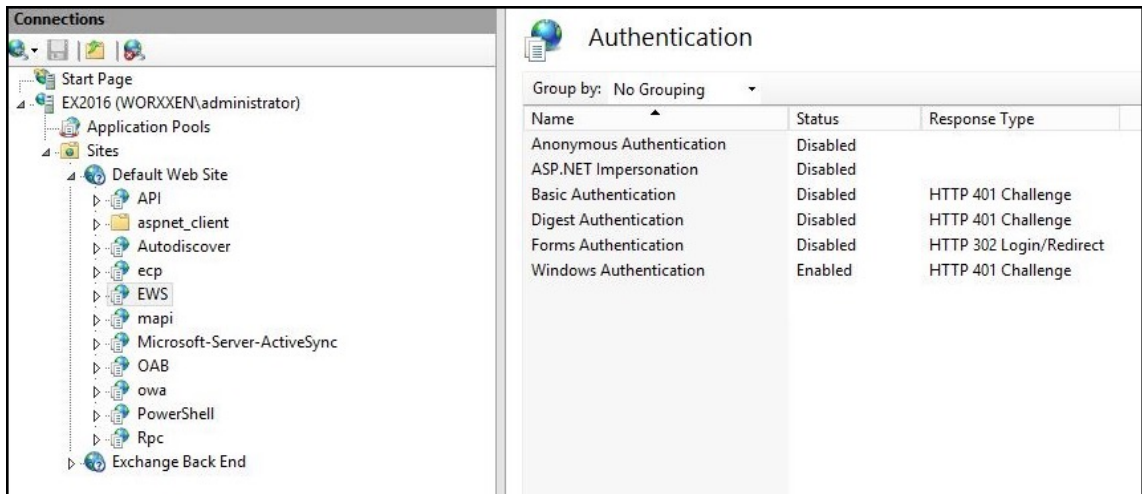
구성을 시작하려면 다음을 수행하십시오.

1. EWS 가상 디렉터리가 설치된 하나 이상의 서버에 로그인합니다.
2. IIS 관리자 콘솔을 엽니다.
3. 기본 웹 사이트에서 EWS 가상 디렉터리를 클릭합니다.

인증, SSL, 구성 편집기 스냅인은 IIS 관리자 콘솔의 오른쪽에 표시됩니다.

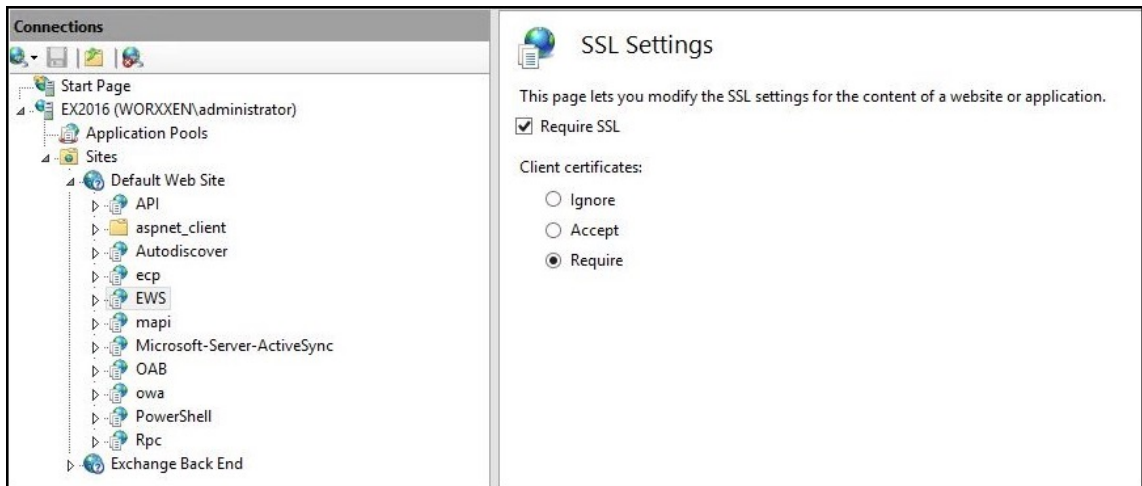


4. EWS에 대한 인증 설정이 다음 그림과 같이 구성되었는지 확인합니다.



5. EWS 가상 디렉터리에 대한 **SSL** 설정을 구성합니다.

- SSL** 필요 확인란을 선택합니다.
- 클라이언트 인증서에서 필요를 클릭합니다. 다른 EWS 메일 클라이언트가 사용자 이름과 암호를 자격 증명으로 사용하여 Exchange Server에 인증하고 연결하는 경우 이 옵션을 수락으로 설정할 수 있습니다.



6. 구성 편집기를 클릭합니다. 섹션 드롭다운 목록에서 다음 섹션으로 이동합니다.

- **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. **enabled** 값을 **True** 로 설정합니다.



8. 구성 편집기를 클릭합니다. 섹션 드롭다운 목록에서 다음 섹션으로 이동합니다.

- **system.webServer/serverRuntime**

9. **uploadReadAheadSize** 값을 **10485760**(10MB) 또는 **20971520**(20MB) 으로 설정하거나 조직에 필요한 값으로 설정합니다.

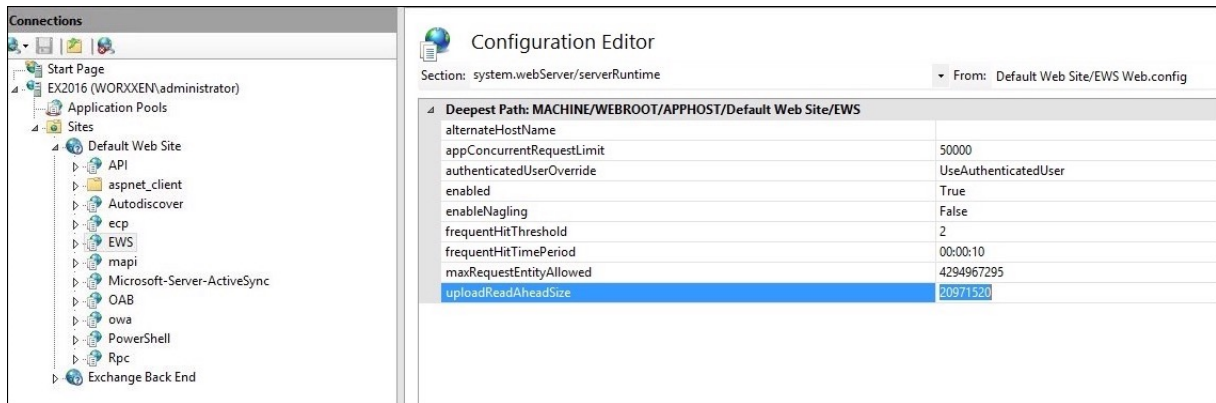
중요:

이 값을 올바르게 설정하지 않으면 인증서 기반 인증이 EWS 푸시 알림을 구독하는 동안 실패하고 오류 코드 413이 표시됩니다.

이 값을 **0** 으로 설정하지 마십시오.

자세한 내용은 다음 타사 리소스를 참조하십시오.

- [Microsoft IIS Server Runtime\(Microsoft IIS 서버 런타임\)](#)
- [Butsch Client Management Blog\(Butsch 클라이언트 관리 블로그\)](#)



iOS 푸시 알림과 관련된 Secure Mail 문제를 해결하는 방법에 대한 자세한 내용은 이 [Citrix Support Knowledge Center](#) 문서를 참조하십시오.

관련 정보

[iOS 용 Secure Mail 의 푸시 알림](#)

XenMobile MDM(모바일 기기 관리) 을 Cisco ISE(ID 서비스 엔진) 와 통합

March 15, 2024

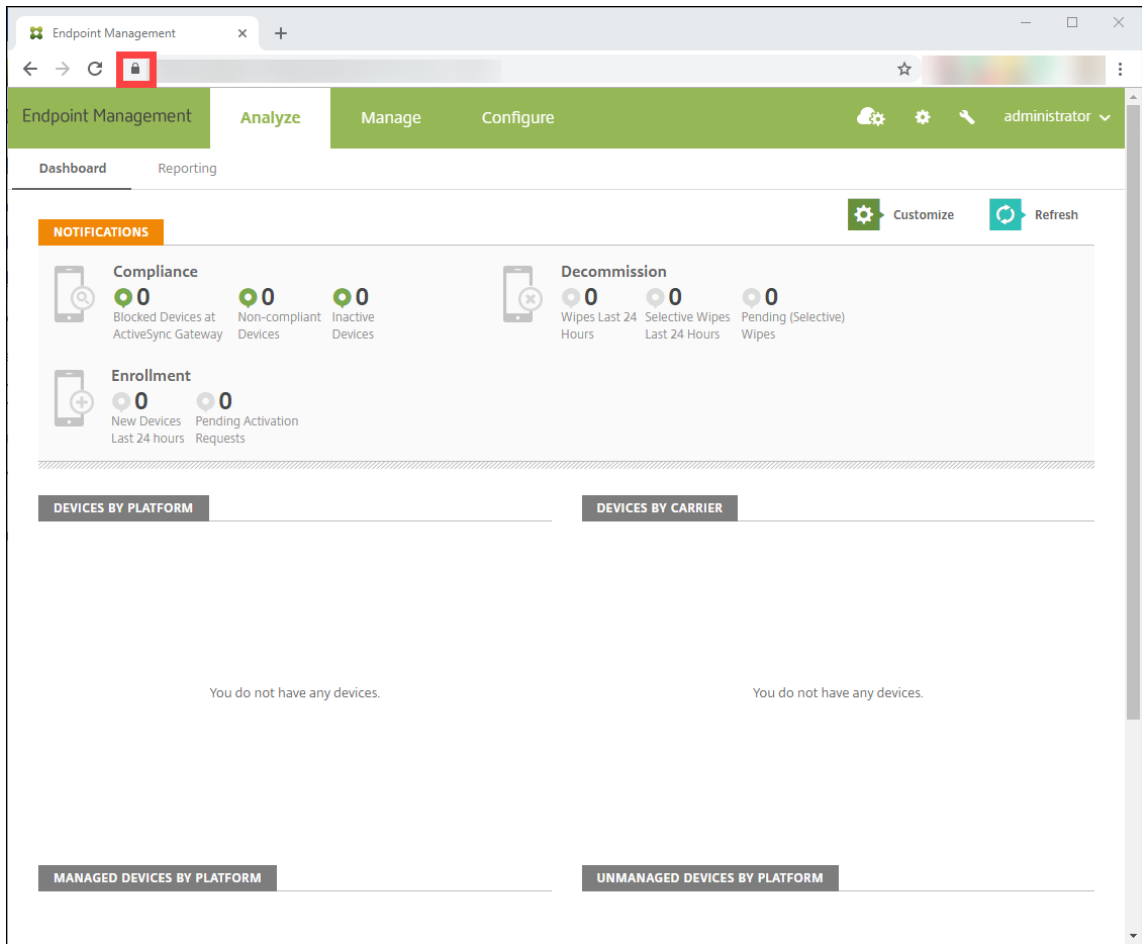
Cisco ISE 는 작업 공간에서 모바일 장치를 배포, 보안, 모니터링, 통합 및 관리하는 데 사용됩니다. 모바일 장치에 다운로드한 소프트웨어는 다음을 제어합니다.

- 응용 프로그램 및 패치 배포
- 엔드포인트의 데이터 및 구성

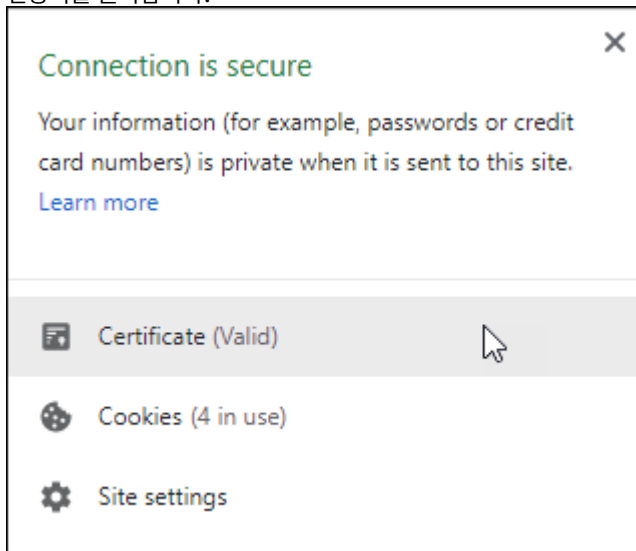
XenMobile 을 Cisco ISE 와 통합하면 Cisco ISE 콘솔에서 비호환 장치 및 관리되지 않는 장치를 관리할 수 있습니다. 또한 XenMobile 을 사용하면 회사 서비스에 대한 액세스를 선택적으로 허용, 거부 또는 격리할 수 있습니다.

XenMobile 과의 통합을 설정하려면 XenMobile Server 에서 관리자 RBAC 역할이 할당된 로컬 서비스 계정을 만듭니다. Cisco ISE 는 이 역할을 사용하여 XenMobile API 에 액세스할 수 있습니다. ISE 는 XenMobile 인증서를 신뢰해야 합니다. 이 인증서를 다운로드하려면 웹 브라우저를 열고 서버 URL 로 이동하여 로그인합니다.

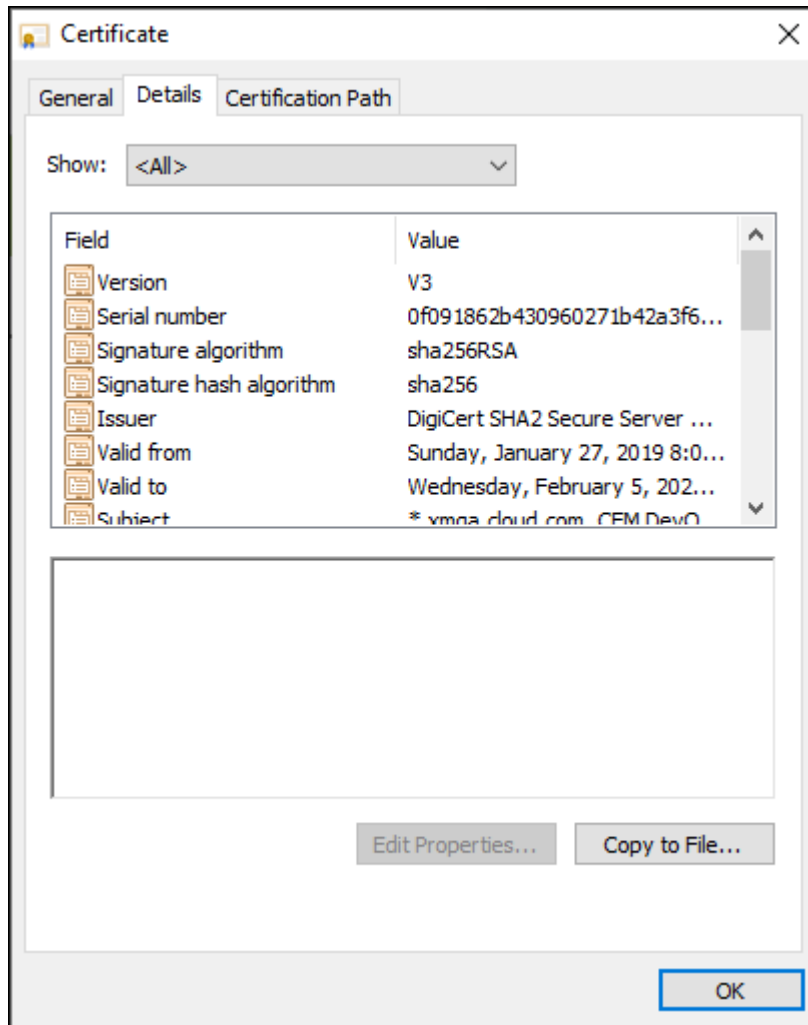
1. 로그인한 후 주소 표시줄의 URL 옆에 있는 잠금 표시를 클릭합니다.



2. 인증서를 클릭합니다.



3. 세부 정보 탭을 선택하고 파일로 복사를 클릭합니다.



4. 마법사에 따라 인증서를 로컬로 저장합니다.
5. Cisco ISE 콘솔에 로그인하고 이전에 다운로드한 XenMobile 인증서를 가져옵니다. 인증서를 Cisco ISE 의 신뢰할 수 있는 인증서 저장소로 가져옵니다. 이 가져오기는 Cisco ISE 가 XenMobile Server 와의 통신을 신뢰하는 데 필요합니다.
 - a) **Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > Trusted Certificates(신뢰할 수 있는 인증서)** 로 이동합니다. 가져오기를 클릭합니다.
 - b) 인증서 이름을 지정하고 **Trust for authentication within ISE(ISE 내의 인증 신뢰)** 및 **Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰)** 확인란을 선택합니다.
6. XenMobile 을 Cisco ISE 내부의 외부 MDM 으로 추가합니다.
 - a) **Administration(관리) > Network Resource(네트워크 리소스) > External MDM(외부 MDM)** 으로 이동합니다. **Add(추가)** 를 클릭하고 다음을 입력합니다.
 - **Server Host(서버 호스트):** XenMobile FQDN
 - **Port(포트):** 443

- **Instance name**(인스턴스 이름): XenMobile Server 의 인스턴스 이름입니다. 대부분의 배포에서 인스턴스 이름은 기본적으로 “zdm” 입니다.
- **User Name**(사용자 이름): 이 작업에 대해 만든 사용자 이름을 입력합니다. 사용자는 원래 관리자 RBAC 그룹의 로컬 관리자 계정이어야 합니다.
- **Password**(암호): 방금 추가한 사용자의 암호입니다.
- **Enable**(사용) 확인란을 선택합니다.

7. 테스트에 성공하면 **Submit**(제출) 을 클릭합니다.

Cisco ISE 에 대한 자세한 내용은 [Cisco 설명서](#)를 참조하십시오.

참고:

호스팅된 Endpoint Management 에서는 ISE 통합이 지원되지 않습니다.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).