롤링 패치 릴리스 정보

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

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

현재 릴리스 패치에 대한 릴리스 정보	게시일	지원 문서
10.16 롤링 패치 9	Sep 17, 2026	릴리스 정보
10.16 롤링 패치 8	Jan 27, 2026	릴리스 정보
10.16 롤링 패치 7	Nov 13, 2025	릴리스 정보
10.16 롤링 패치 6	Sep 26, 2025	릴리스 노트
10.16 롤링 패치 5	Apr 22, 2025	CTX692919
10.16 롤링 패치 4	Dec 18, 2024	CTX692370
10.16 롤링 패치 3	Aug 28, 2024	CTX691503
10.16 롤링 패치 2	Jul 02, 2024	CTX678043
10.16 롤링 패치 1	Jun 17, 2024	CTX677872

이전 릴리스 패치에 대한 릴리스 정보	게시일	지원 문서
10.15 롤링 패치 14	Jul 02, 2026	릴리스 정보
10.15 롤링 패치 13	Nov 20, 2025	릴리스 정보
10.15 롤링 패치 12	Oct 23, 2025	릴리스 정보
10.15 롤링 패치 11	May 13, 2025	CTX693257
10.15 롤링 패치 10	Jan 27, 2025	CTX692560

XENMOBILE® SERVER

이전 릴리스 패치에 대한 릴리스 정보	게시일	지원 문서
10.15 롤링 패치 9	Dec 04, 2024	CTX692268
10.15 롤링 패치 8	Jul 11, 2024	CTX691107
10.15 롤링 패치 7	Jun 06, 2024	CTX677079
10.15 롤링 패치 6	Mar 06, 2024	CTX625010
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
10.14 롤링 패치 13	Mar 08, 2024	CTX628921
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

이전 릴리스 패치에 대한 릴리스 정보	게시일	지원 문서
10.14 롤링 패치 1	Nov 19, 2021	CTX335342

XenMobile Server 10.16 Rolling Patch 9 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 Rolling Patch 9에 대한 개선 사항과 해결된 문제 및 알려진 문제를 설명합니다. XenMobile Server 10.16 Rolling Patch 9 소프트웨어 바이너리는 Sign-in to Download에서 다운로드할 수 있습니다.

새로운 기능

- **Launcher Configuration 장치 정책에서 시스템 정보 활성화 지원:**

  Android Enterprise 장치용 Launcher Configuration 장치 정책에 새로운 설정인 **시스템 정보 활성화**가 추가되었습니다. 이 설정을 통해 Citrix Launcher는 상태 표시줄에 시스템 정보를 표시할 수 있습니다. 기본값은 **해제**이며 Secure Hub 26.8 이상이 필요합니다. 자세한 내용은 Launcher Configuration Policy를 참조하십시오.

- **Launcher Configuration 장치 정책에서 앱 자동 실행 지원:**

  Android Enterprise 장치용 Launcher Configuration 장치 정책에 새로운 설정인 **앱 자동 실행**이 추가되었습니다. 이 설정을 통해 관리자는 Citrix Launcher가 시작될 때 **허용된 앱** 중 하나를 자동으로 시작하도록 선택할 수 있습니다. 기본값은 **없음(자동 실행 안 함)**이며 Citrix Launcher 26.8 이상이 필요합니다. 자세한 내용은 Launcher Configuration Policy를 참조하십시오.

  XenMobile Server에는 Launcher Configuration 정책으로 구성된 Android Enterprise 장치에 대해 앱 자동 실행을 구성할 수 있도록 하는 새로운 속성 `afw.launcher.auto_launch`이(가) 있습니다. 기본값은 **False**입니다. 자세한 내용은 Server properties를 참조하십시오.

- **장치 앱에 대한 앱 검색 옵션 지원:**

  XenMobile Server 콘솔의 **장치 > 장치 세부 정보 > 앱** 페이지에 새로운 **앱 검색** 옵션이 포함되었습니다.

- **앱 설정 장치 정책 지원:**

  구성(선언적) 아래에 새로운 장치 정책인 **앱 설정**이 추가되었습니다. 이 정책을 통해 Apple의 선언적 장치 관리를 사용하여 앱 허용 및 거부 목록을 구성할 수 있습니다. 이 정책은 감독되는 iOS 27 이상 장치만 지원합니다. 자세한 내용은 App Settings device policy를 참조하십시오.

XenMobile Server에는 앱 설정 장치 정책을 활성화하는 새로운 속성 `ios.mdm.ios27.ddm.support`이(가) 있습니다. 기본값은 **True**입니다. 자세한 내용은 Server properties를 참조하십시오.

- **iOS 및 macOS에 대한 배포 규칙에서 일련 번호 지원:**

  XenMobile Server는 이제 iOS 및 macOS에 대한 새로운 배포 규칙인 **일련 번호**를 지원합니다. 이 규칙은 **배포 규칙 > 고급**에서 추가합니다.

- **Android 17 지원:**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android 17을 실행하는 Android Enterprise 장치를 지원합니다. 보안 및 개인 정보 보호에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.

- **iOS 27 지원:**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 iOS 27과 호환됩니다.

- **Secure Hub APN 인증서 갱신:**

  XenMobile Server 10.16용 Secure Hub Apple Push Notification service(APNs) 인증서는 November 9, 2026에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 September 18, 2027까지 유효한 새 인증서로 자동 갱신합니다.

해결된 문제

- /api/v1/application/store/{id}/platform/iphone REST API를 통한 iOS 앱 업데이트가 오류 1493으로 실패합니다.
- 평가판 라이선스에서 라이선스 활성화 서비스(LAS) 라이선스로 마이그레이션한 후 라이선스 유형이 올바르게 설정되지 않고 등록 프로필에서 iOS 옵션이 누락됩니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

> **중요:**
>
> 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.16.0.48로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스 백업을 생성하십시오.

> 클러스터 모드로 구성된 시스템의 경우 다음 단계에 따라 각 노드를 차례로 업데이트하십시오.

1. Citrix® 웹 사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **Settings > Release Management**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **Update**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix downloads page에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음 **Settings > Release Management > Updates**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.16 Rolling Patch 9 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 Rolling Patch 9에 대한 개선 사항과 해결된 문제 및 알려진 문제를 설명합니다. XenMobile Server 10.16 Rolling Patch 9 소프트웨어 바이너리는 Sign-in to Download에서 다운로드할 수 있습니다.

새로운 기능

- **Launcher Configuration 장치 정책에서 시스템 정보 활성화 지원:**

  Android Enterprise 장치용 Launcher Configuration 장치 정책에 새로운 설정인 **시스템 정보 활성화**가 추가되었습니다. 이 설정을 통해 Citrix Launcher는 상태 표시줄에 시스템 정보를 표시할 수 있습니다. 기본값은 **해제**이며 Secure Hub 26.8 이상이 필요합니다. 자세한 내용은 Launcher Configuration Policy를 참조하십시오.

- **Launcher Configuration 장치 정책에서 앱 자동 실행 지원:**

  Android Enterprise 장치용 Launcher Configuration 장치 정책에 새로운 설정인 **앱 자동 실행**이 추가되었습니다. 이 설정을 통해 관리자는 Citrix Launcher가 시작될 때 **허용된 앱** 중 하나를 자동으로 시작하도록 선택할 수 있습니다. 기본값은 **없음(자동 실행 안 함)**이며 Citrix Launcher 26.8 이상이 필요합니다. 자세한 내용은 Launcher Configuration Policy를 참조하십시오.

XenMobile Server에는 Launcher Configuration 정책으로 구성된 Android Enterprise 장치에 대해 앱 자동 실행을 구성할 수 있도록 하는 새로운 속성 `afw.launcher.auto_launch`이(가) 있습니다. 기본값은 **False**입니다. 자세한 내용은 Server properties를 참조하십시오.

- **장치 앱에 대한 앱 검색 옵션 지원:**

  XenMobile Server 콘솔의 **장치 > 장치 세부 정보 > 앱** 페이지에 새로운 **앱 검색** 옵션이 포함되었습니다.

- **앱 설정 장치 정책 지원:**

  구성(선언적) 아래에 새로운 장치 정책인 **앱 설정**이 추가되었습니다. 이 정책을 통해 Apple의 선언적 장치 관리를 사용하여 앱 허용 및 거부 목록을 구성할 수 있습니다. 이 정책은 감독되는 iOS 27 이상 장치만 지원합니다. 자세한 내용은 App Settings device policy를 참조하십시오.

  XenMobile Server에는 앱 설정 장치 정책을 활성화하는 새로운 속성 `ios.mdm.ios27.ddm.support`이(가) 있습니다. 기본값은 **True**입니다. 자세한 내용은 Server properties를 참조하십시오.

- **iOS 및 macOS에 대한 배포 규칙에서 일련 번호 지원:**

  XenMobile Server는 이제 iOS 및 macOS에 대한 새로운 배포 규칙인 **일련 번호**를 지원합니다. 이 규칙은 **배포 규칙 > 고급**에서 추가합니다.

- **Android 17 지원:**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android 17을 실행하는 Android Enterprise 장치를 지원합니다. 보안 및 개인 정보 보호에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.

- **iOS 27 지원:**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 iOS 27과 호환됩니다.

- **Secure Hub APN 인증서 갱신:**

  XenMobile Server 10.16용 Secure Hub Apple Push Notification service(APNs) 인증서는 November 9, 2026에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 September 18, 2027까지 유효한 새 인증서로 자동 갱신합니다.

해결된 문제

- /api/v1/application/store/{id}/platform/iphone REST API를 통한 iOS 앱 업데이트가 오류 1493으로 실패합니다.
- 평가판 라이선스에서 라이선스 활성화 서비스(LAS) 라이선스로 마이그레이션한 후 라이선스 유형이 올바르게 설정되지 않고 등록 프로필에서 iOS 옵션이 누락됩니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

> **중요:**
>
> 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.16.0.48로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스 백업을 생성하십시오.
>
> 클러스터 모드로 구성된 시스템의 경우 다음 단계에 따라 각 노드를 차례로 업데이트하십시오.

1. Citrix® 웹 사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **Settings > Release Management**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **Update**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix downloads page에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음 **Settings > Release Management > Updates**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.16 롤링 패치 8 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 8의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 8 소프트웨어 바이너리는 다운로드에 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **선언적 장치 관리(DDM) 지원:**

XenMobile Server는 iOS 15 이상에서 Apple의 Declarative Device Management(DDM)를 지원합니다. 이 기능은 선언적 데이터 모델을 사용하여 성능과 확장성을 향상시키고, 직렬화된 명령 및 장치 폴링에 대한 의존도를 줄입니다. 자세한 내용은 선언적 관리 데이터 모델을 활용하여 장치 확장을 참조하십시오.

XenMobile Server에는 다음 두 가지 새로운 속성이 있습니다.

`ios.mdm.declarative.management`: iOS Declarative Device Management(DDM)를 활성화합니다.

`ios.mdm.software.update.settings`: 소프트웨어 업데이트 적용 장치 정책을 활성화합니다.

두 속성의 기본값은 **False**입니다. 자세한 내용은 서버 속성을 참조하십시오.

DDM 기능을 활성화하면 다음 선언적 장치 정책이 지원됩니다.

- Google 계정
- 암호
- 소프트웨어 업데이트 적용
- 소프트웨어 업데이트 설정
- 상태 구독
- 사용자 ID(/ko-kr/xenmobile/server/policies/declarative-device-management-policies/user-identity-device-policy.html)

- **iOS 장치에 대한 이동통신사 네트워크 관련 장치 정보 검색 지원:**

  XenMobile Server는 이제 iOS 장치의 각 SIM에 대한 추가 이동통신사 네트워크 관련 장치 정보 검색을 지원합니다. 이러한 세부 정보는 **장치 세부 정보 > 속성 > 슬롯 x SIM 정보**에서 볼 수 있습니다. 새로 지원되는 필드는 다음과 같습니다.

  - 슬롯 x — 이동통신사 설정 버전
  - 슬롯 x — 현재 이동통신사 네트워크
  - 슬롯 x — 현재 모바일 국가 코드 (이전에는 네트워크 정보 아래에 나열됨)
  - 슬롯 x — 현재 모바일 네트워크 코드 (이전에는 네트워크 정보 아래에 나열됨)
  - 슬롯 x — 데이터 우선 여부
  - 슬롯 x — 로밍 중 여부
  - 슬롯 x — 음성 우선 여부
  - 슬롯 x — 레이블 ID

- **Microsoft Exchange Online용 OAuth 인증 지원:**

  Microsoft는 Exchange Online이 March 2026에 클라이언트 제출(SMTP AUTH)을 통한 기본 인증 지원을 영구적으로 제거하고 April 30, 2026에는 100% 거부될 것이라고 발표했습니다. 자세한 내용은 클라이언트 제출(SMTP AUTH)에 대한 기본 인증을 중단하는 Exchange Online을 참조하십시오.

  XenMobile Server는 SMTP 서버에 대한 OAuth 인증을 지원합니다. **Microsoft Exchange Online OAuth 2.0**을 선택하고 필요한 **테넌트 ID**, **클라이언트 ID**, **클라이언트 암호**를 제공하여 이 기능을 활성화할 수 있습니다. Microsoft Exchange Online을 사용하는 경우 Citrix는 OAuth 인증으로 전환할 것을 권장합니다. 구성 세부 정보는 알림을 참조하십시오.

- **iOS 장치가 근접 설정을 수행하는 것을 방지하는 지원:**

  XenMobile Server에 전체 장치 초기화를 위한 새로운 옵션인 **다음 재부팅 시 근접 설정이 허용되지 않으며 설정 지원의 창이 건너뛰어집니다.**가 추가되었습니다. 이 옵션은 장치 설정 중에 iOS 장치가 근접 설정을 수행하는 것을 방지합니다. 이 기능은 iOS 11.3 이상에서 사용할 수 있습니다. 자세한 내용은 보안 작업을 참조하십시오.

- **iOS 26.x 앱 크기 검색을 지원하도록 앱 인벤토리 개선:**

  XenMobile Server는 iOS 26.x를 실행하는 장치에 대한 앱 크기 정보 검색을 지원합니다. 이 정보는 **장치 세부 정보 > 앱**에서 찾을 수 있습니다.

해결된 문제

- XenMobile Server 콘솔에서 장치, 앱 및 전달 그룹을 관리하는 등의 작업이 10.16 롤링 패치 5로 업그레이드한 후 현저히 느려지거나 때로는 실패합니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

> **중요:**
>
> 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.16.0.48로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스 백업을 생성하십시오.

> 클러스터 모드로 구성된 시스템의 경우 다음 단계에 따라 각 노드를 순서대로 업데이트하십시오.

1. Citrix® 웹사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.

2. 노드의 XenMobile Server 콘솔에서 **설정 > 릴리스 관리**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.

3. 릴리스 관리에서 **업데이트**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix 다운로드 페이지에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음 **설정 > 릴리스 관리 > 업데이트**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.16 롤링 패치 7 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 7의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 7 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Android Enterprise 장치에 대한 듀얼 SIM 및 eSIM 지원 강화:**

  XenMobile Server는 이제 iOS와의 기능 동등성을 보장하기 위해 Android Enterprise 장치에 대한 포괄적인 듀얼 SIM 지원을 제공합니다. 이 개선 사항을 통해 관리자는 두 개의 물리적 SIM 카드, SIM 카드 1개와 eSIM 1개, 또는 eSIM 2개로 구성된 설정을 포함하여 장치 속성에서 설치된 모든 SIM 카드 및 eSIM을 볼 수 있습니다. 이 업데이트는 듀얼 SIM Android Enterprise 장치의 채택 증가에 대응하고 고객에게 모바일 장치 연결 옵션에 대한 완벽한 가시성을 제공하며, 이전에 iOS 장치에 제공되었던 eSIM 기능과 일치합니다. 이 기능은 다음에서만 지원됩니다.

  - Secure Hub 버전 25.7.0 이상, 그리고
  - Android 13 이상

  XenMobile Server에는 새로운 속성 `ae.esim.support`이 있으며, 이 속성을 통해 XenMobile Server는 Android Enterprise 장치에서 eSIM 정보를 가져와 사용자 인터페이스에 eSIM 관련 장치 속성을 표시할 수 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 서버 속성을 참조하십시오.

- **라이선스 활성화 서비스:**

  XenMobile Server는 이제 라이선스 활성화 서비스(LAS) 라이선스 메커니즘을 지원합니다. LAS는 Citrix 제품군 전반에 걸쳐 기존 파일 기반 라이선싱에 대한 최신 대안을 제공하는 새로운 클라우드 기반 라

이선싱 솔루션입니다. 라이선스 활성화 서비스가 보유한 라이선스 및 권한을 사용하려면 Citrix License Server를 Citrix Cloud에 등록하십시오. 자세한 내용은 라이선스 활성화 서비스를 참조하십시오.

중요:

Citrix 플랫폼의 업계 표준 클라우드 기반 라이선싱 아키텍처로 전환하고 있습니다. 이러한 전환은 권한 및 활성화를 자동화하여 고객에게 다음과 같은 주요 이점을 제공합니다.

- **라이선스 파일 관리 불필요:** 라이선스 파일을 다운로드, 할당 또는 관리할 필요가 없어 관리 작업을 간소화합니다.
- **자동화된 권한 업데이트:** 계약 갱신 시 권한이 백그라운드에서 자동으로 업데이트되어 중단 없는 서비스를 보장합니다.
- **향상된 복원력:** 라이선스 서버가 더 이상 사용자 세션의 단일 실패 지점이 아니므로 환경의 안정성이 향상됩니다.

저희는 고객님께서 전환 시점까지의 시간을 활용하여 새로운 라이선스 모델을 April 15, 2026까지 채택하기 위한 전환을 계획하고 실행하시기를 권장하며, 모든 단계에서 고객님을 지원하기 위해 최선을 다하고 있습니다. 자세한 내용은 Citrix Modern Licensing Announcement를 참조하십시오.

- **Secure Hub APNs 인증서 갱신:**

  XenMobile Server 10.16용 Secure Hub Apple Push Notification service(APNs) 인증서는 January 4, 2026에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 November 9, 2026까지 유효한 새 인증서로 자동 갱신합니다.

- **iOS 18.x 버전의 새로운 iOS 제한 지원:**

  iOS 제한 정책에 Apple Intelligence(AI)에 대한 액세스를 차단하거나 일부 새로운 기능을 제한하기 위한 다음 새 설정이 추가되었습니다. 이 설정은 iOS 버전 18 이상에 적용됩니다. 기본값은 **켜짐**입니다. 자세한 내용은 제한 정책을 참조하십시오.

  - 외부 인텔리전스 통합 허용
  - 외부 인텔리전스 통합 로그인 허용
  - 메일 스마트 답장 허용
  - 메모 필사 허용
  - Safari 요약 허용

- 시각적 인텔리전스 요약 허용
- 메모 필사 요약 허용
- Apple Intelligence 보고서 허용
- 기본 통화 앱 수정 허용
- 기본 메시징 앱 수정 허용
- 외부 인텔리전스 작업 공간 ID 허용
- 기본 브라우저 수정
- FaceTime 원격 제어 허용

해결된 문제

- XenMobile 서버의 높은 CPU 및 메모리 사용률로 인해 장치 등록에 실패합니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

> **중요:**
>
> 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.16.0.48로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스 백업을 생성하십시오.

> 클러스터 모드로 구성된 시스템의 경우 다음 단계에 따라 각 노드를 차례로 업데이트하십시오.

1. Citrix® 웹 사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **설정 > 릴리스 관리**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **업데이트**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix 다운로드 페이지에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후, 관리자로 XenMobile Server 콘솔에 로그인한 다음, **설정 > 릴리스 관리 > 업데이트**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.16 롤링 패치 6 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 6의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 6 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Android 16 지원**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android 16을 실행하는 Android Enterprise 장치를 지원합니다. 보안 및 개인 정보 보호에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.

- **iOS 26 지원**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 iOS 26과 호환됩니다.

- **레거시 MDX 정책 업그레이드 알림 지원**

  XenMobile Server는 이제 레거시 정책을 사용하는 기존 Secure Mail 및 Secure Web MDX 앱이 버전 25.9.0으로 업데이트될 때 업그레이드 알림을 표시합니다.

- **인증서 기반 인증을 위한 새로운 강력한 인증서 매핑 지원**

  강력한 매핑 요구 사항을 충족하는 인증서 발급에 더 큰 유연성을 제공하기 위해 새로운 매핑 방법이 도입되었습니다. XenMobile Server는 이제 인증서의 주체 대체 이름(SAN)에 `URL=tag:microsoft.com`, `2022-09-14:sid:<user's SID>`를 추가합니다.

  - 기존 사용자를 위해 이 기능을 활성화하려면 고객 관리자가 클라이언트 속성 `MICROSOFT_CERTIFICATE_STRONG_MAPPING`을 추가해야 합니다. 자세한 내용은 클라이언트 속성을 참조하십시오.
  - 강력한 인증서 매핑은 **Windows Server 2019 이상**에서만 지원됩니다. 자세한 내용은 Microsoft 강력한 매핑을 참조하십시오.

- **iOS 17.x 버전에 대한 새로운 iOS 제한 지원**

  iOS 제한 정책에 iOS 버전 17.2 이상에 대한 다음 새 설정이 추가되었습니다. 기본값은 **켜짐**입니다. 자세한 내용은 제한 정책을 참조하십시오.

  - 실시간 음성 사서함 허용

- **구성 정책 텍스트 상자 관리**

  고객이 **Knox Service Plugin**과 **관리형 구성 정책**을 함께 사용하는 경우, **분리된 앱 정책**의 모든 텍스트 상자에 대한 최대 문자 길이가 8,192자로 증가합니다.

- **Apple 배포 프로그램 페이지에서 새로운 iOS 설정 지원 옵션 지원**

  Apple은 Apple Business Management 등록을 위해 몇 가지 새로운 iOS 설정 지원 옵션 화면을 추가했습니다. 다음 새 옵션은 **설정 > Apple 배포 프로그램 > iOS 설정 지원 옵션** 페이지에 추가되었습니다. XenMobile Server가 해당 화면을 건너뛰도록 구성할 수 있습니다. 자세한 내용은 iOS 설정 지원 옵션을 참조하십시오.

  - 동작 버튼
  - 잠금 모드
  - 지능
  - 카메라 버튼

- **Apple Business Manager와 동기화하여 장치 할당 관리**

  XenMobile® Server(XMS)는 이제 Apple Business Manager(ABM)와 동기화하여 정확한 장치 할당을 보장합니다. 이 업데이트는 올바르게 할당된 장치만 XMS에 표시되도록 하여 XMS에서 제거되고 다른 공급업체 관리 솔루션에 할당된 장치 기록을 방지합니다. 예를 들어, 장치가 다른 솔루션으로 이동되면 동기화 후 XMS에 더 이상 표시되지 않습니다.

  XMS에는 이제 `remove.unassigned.abm.devices`이라는 새 속성이 포함되어 있어 XMS가 이 서버에 더 이상 할당되지 않은 장치를 제거할 수 있습니다. 기본적으로 이 속성은 **False**로 설정되어 있습니다. 자세한 내용은 서버 속성을 참조하십시오.

해결된 문제

- 레거시 MDX 애플리케이션이 업로드되지 않았음에도 불구하고 레거시 MDX 경고가 XMS 콘솔에 계속 표시됩니다.
- 마우스 오른쪽 클릭 및 붙여넣기를 사용하여 암호를 입력하면 XenMobile 포털에서 로그인 버튼이 회색으로 비활성화됩니다.
- **새 보기 표시** 기능이 활성화된 경우, 장치 목록에 필터를 적용해도 장치 수가 올바르지 않게 표시됩니다.
- iOS 사용자는 Secure Mail/Secure Web 애플리케이션을 실행할 수 없으며, Secure Mail/Secure Web에서 Secure Hub로 리디렉션할 때 "열 수 없음" 오류가 발생합니다.
- DEP(Device Enrollment Program) 장치는 등록 프로필이 **MDM 전용**으로 구성되어 있어도 계속해서 **MDM+MAM** 등록을 수행합니다.

- iOS 장치에 설치되지 않은 애플리케이션에 대한 앱 잠금 정책이 있는 경우, 강제 재부팅 후에도 장치가 "안내된 접근 앱을 사용할 수 없습니다. 관리자에게 문의하십시오."라는 오류와 함께 잠기고 터치스크린이 응답하지 않습니다.
- XenMobile MDM 솔루션으로 Windows 클라이언트를 등록할 때 배달 그룹 배포가 실패합니다. 결과적으로 푸시된 정책을 적용하려면 수동 동기화 작업이 필요합니다. 해결 방법으로 단일 장치에 대한 수동 배포가 필요합니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

> **중요:**
>
> 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.16.0.48로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스를 백업하십시오.
>
> 클러스터 모드로 구성된 시스템의 경우, 다음 단계에 따라 각 노드를 하나씩 업데이트하십시오.

1. Citrix® 웹사이트에서 계정에 로그인하여 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **설정 > 릴리스 관리**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **업데이트**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix 다운로드 페이지에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음, **설정 > 릴리스 관리 > 업데이트**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.16 롤링 패치 5 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 5의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 5 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **관리형 구성 피드백 지원 (기술 미리 보기)**

  이 기능은 관리자가 관리형 구성 정책으로 구성된 Android 장치에서 앱 상태에 대한 피드백을 얻을 수 있도록 합니다. 자세한 내용은 관리형 구성 피드백 지원 (기술 미리 보기)을 참조하십시오.

  XenMobile Server에는 이제 관리자가 관리형 구성 정책으로 구성된 Android 장치에서 앱 상태에 대한 피드백을 얻을 수 있도록 하는 기능을 활성화하는 새로운 속성 `afw.app_managed_configurations.feedback`이 포함되어 있습니다. 기본적으로 이 속성은 **False**로 설정되어 있습니다. 자세한 내용은 서버 속성을 참조하십시오.

- **장치 페이지의 영구 필터 지원**

  새 장치 페이지에서 이제 모든 **필터링 가능** 옵션에 대해 필터가 지원됩니다. 이러한 필터는 로그인한 사용자의 세션 간에 저장되므로 관리자가 장치 페이지를 방문할 때마다 동일한 필터를 다시 적용할 필요가 없습니다. 해당 열이 선택 해제되면 필터가 자동으로 제거됩니다.

- **iPhone 및 iPad의 데이터 요금제 보존 지원**

  전체 장치 초기화를 수행할 때 '초기화 시 셀룰러 데이터 요금제 보존'이라는 새로운 옵션을 사용할 수 있습니다. 이 옵션을 사용하면 초기화 프로세스 중에 장치의 셀룰러 데이터 요금제(예: eSIM)를 보존할 수 있습니다. 이 기능은 iOS 버전 11 이상에서 사용할 수 있습니다. 자세한 내용은 보안 작업을 참조하십시오.

- **iOS용 새로운 iOS 18 설정 지원**

  iOS용 제한 정책에 Apple Intelligence(AI)에 대한 액세스를 차단하거나 일부 새로운 기능을 제한하기 위한 다음 새 설정이 추가되었습니다. 이 설정은 iOS 버전 18 이상에 적용됩니다. 기본값은 **켜짐**입니다. 자세한 내용은 제한 정책을 참조하십시오.

  - 통화 녹음
  - 숨길 앱
  - 잠글 앱
  - 메일 요약
  - RCS 메시징
  - 기본 브라우저 수정

- **macOS용 새로운 macOS 15 설정 지원**

  macOS용 제한 정책에 Apple Intelligence(AI)에 대한 액세스를 차단하거나 일부 새로운 기능을 제한하기 위한 다음 새 설정이 추가되었습니다. 이 설정은 macOS 버전 15 이상에 적용됩니다. 자세한 내용은 제한 정책을 참조하십시오.

  - 미디어 공유 수정 허용
  - 화면 캡처 경고 강제 우회
  - 메일 요약

해결된 문제

- '서버 속성' 권한이 없는 경우, 장치 페이지에서 '새 보기 표시(기술 미리 보기)'를 전환할 때 역할 기반 액세스 제어(RBAC) 관리자가 예기치 않게 로그아웃됩니다.
- 애플리케이션이 새 버전으로 업그레이드될 때 VPP(볼륨 구매 프로그램) 앱 아이콘이 업데이트되지 않습니다.
- MDM 인증서 갱신에 실패하면 이전 인증서가 XenMobile® Server에 의해 해지된 것으로 표시되어 Secure Hub(SH)가 서버에 다시 연결할 수 없게 됩니다. 결과적으로 SH는 아직 만료되지 않은 이전 인증서를 사용하여 서버와 통신할 수 없습니다.
- **새 보기 기술 미리 보기 표시** 기능이 활성화되면 역할 기반 액세스 제어(RBAC) 관리자가 예기치 않게 검색 입력 상자를 보게 됩니다.
- AE 장치에 대해 수많은 페이로드 인증서가 생성됩니다.
- **배포 일정**에서 **배포 조건**이 "이전 배포가 실패한 경우에만"으로 설정된 경우, 재등록 중에 일부 정책이 AE 장치에 배포되지 않습니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 정보는 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.16 롤링 패치 4 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 4의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 4 소프트웨어 바이너리는 다운로드에 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Secure Hub APNs 인증서 갱신**

  XenMobile Server 10.16용 Secure Hub Apple Push Notification service(APNs) 인증서는 February 9, 2025에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 January 4, 2026까지 유효한 새 인증서로 자동 갱신합니다.

- **macOS 15 지원**

  XenMobile® Server 및 Citrix Mobile 생산성 앱은 이제 macOS 15와 호환되지만, 현재 macOS 15의 모든 새로운 기능을 지원하지는 않습니다.

- **iOS 18 지원**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 iOS 18과 호환되지만, 현재 iOS 18의 모든 새로운 기능을 지원하지는 않습니다.

- **Android 15 지원**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android Enterprise 장치 업데이트를 Android 15로 지원합니다. 보안 및 개인 정보 보호 이점에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.

- **장치 분실 모드 API를 포함하도록 공용 REST API 문서 업데이트**

  공용 REST API 문서에 분실 모드 API를 추가했습니다.

- **API 호출을 URL 대신 POST 본문으로 수정**

  공용 REST API 문서에서 URL 대신 요청 본문에 데이터를 포함하도록 API 호출을 업데이트했습니다.

- **iOS용 Apple Intelligence 차단 또는 제한 지원**

  iOS용 제한 정책에 Apple Intelligence(AI)에 대한 액세스를 차단하거나 일부 새로운 기능을 제한하기 위한 다음 새 설정이 추가되었습니다. 이 설정은 iOS 버전 18 이상에 적용됩니다. 기본값은 **켜짐**입니다. 자세한 내용은 제한 정책을 참조하십시오.

  - 젠모지
  - 이미지 플레이그라운드
  - 이미지 완드
  - iPhone 미러링
  - 개인화된 필기 결과
  - 쓰기 도구

- **macOS용 Apple Intelligence 차단 또는 제한 지원**

  macOS용 제한 정책에 Apple Intelligence(AI)에 대한 액세스를 차단하거나 일부 새로운 기능을 제한하기 위한 다음 새 설정이 추가되었습니다. 이 설정은 macOS 버전 15 이상에 적용됩니다. 기본값은 **켜짐**입니다. 자세한 내용은 제한 정책을 참조하십시오.

  - 이미지 플레이그라운드

  - iPhone 미러링
  - 쓰기 도구

- **iOS 장치에 OS 업데이트 즉시 설치 지원**

  OS 업데이트 제어 장치 정책에서 iOS용 OS 업데이트 옵션에 **즉시 설치**라는 새 라디오 버튼이 추가되었습니다. 이 기능을 사용하면 이전에 다운로드한 OS 업데이트를 iOS 장치에 즉시 설치할 수 있습니다. 자세한 내용은 iOS용 OS 업데이트 제어 장치 정책을 참조하십시오.

- **시스템이 장치를 지울 때 eSIM 보존 지원**

  제한 정책에 새로운 설정인 **지우기 시 eSIM 보존**이 추가되었습니다. 이 설정은 여러 번의 암호 입력 실패로 인해 시스템이 장치를 지우거나 **설정** > **일반** > **재설정**에서 **모든 콘텐츠 및 설정 지우기** 옵션을 선택할 때 eSIM이 보존되도록 합니다. 이 기능은 iOS 버전 17.2 이상에서 사용할 수 있으며, 기본 설정은 **끔**으로 되어 있습니다. 자세한 내용은 제한 정책을 참조하십시오.

- **웹 배포 타사 앱 차단 지원**

  제한 정책에 iOS 장치에서 웹 배포 타사 앱을 차단하는 새로운 설정인 **웹 배포** 앱이 추가되었습니다. 이 설정은 iOS 버전 17.5 이상에 적용됩니다. 자세한 내용은 제한 정책을 참조하십시오.

- **복사 및 붙여넣기 기능 관리 지원**

  제한 정책에 새로운 설정인 **관리되는 붙여넣기 보드 필요**가 추가되어 복사 및 붙여넣기 기능이 **관리되지 않는 앱의 관리되는 앱 문서** 및 **관리되는 앱의 관리되지 않는 앱 문서**에 적용하는 것과 동일한 제한을 따르도록 합니다. 기본값은 **끔**입니다. 자세한 내용은 제한 정책을 참조하십시오.

- **삼성 강화된 인증 v3 지원**

  Samsung Enhanced Attestation v3는 Samsung Knox 장치에서 XMS 보안 기능을 향상시킵니다. 자세한 내용은 Samsung Knox Enhanced Attestation을 참조하십시오. XenMobile Server에는 이제 Samsung Knox 장치에서 XMS 보안 기능을 향상시킬 수 있는 기능을 활성화하는 새로운 속성 `afw.knox.attestation.v3`가 포함되어 있습니다. 기본적으로 이 속성은 **True**로 설정됩니다. 자세한 내용은 서버 속성을 참조하십시오.

해결된 문제

- SQL Server가 경고 메시지를 트리거할 때 발생하는 성능 문제로 인해 XenMobile Server가 새로운 Android Enterprise 장치를 성공적으로 등록할 수 없습니다.
- 고객이 FIPS 설정을 **true**로 활성화했음에도 불구하고 로그에는 계속 비활성화된 것으로 표시됩니다. 또한 고객이 CLI를 통해 데이터베이스 설정을 수정하려고 하면 XenMobile Server가 데이터베이스에 대한 연결을 설정하지 못하여 업데이트가 적용되지 않습니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.16 롤링 패치 3 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 3의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 3 소프트웨어 바이너리는 다운로드에 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **iPhone 및 iPad용 서비스 복귀 지원**

  서비스 복귀 기능을 사용하면 MDM 서버가 Wi-Fi 세부 정보와 기본 MDM 등록 프로필을 포함하는 지우기 명령을 사용자 장치로 보낼 수 있습니다. 그러면 장치는 모든 사용자 데이터를 자동으로 지우고, 지정된 Wi-Fi 네트워크에 연결하며, 제공된 등록 프로필을 사용하여 MDM 서버에 다시 등록합니다. 자세한 내용은 보안 작업을 참조하십시오.

  XenMobile Server에는 이제 iOS 17 이상을 실행하는 iPhone 및 iPad용 서비스 복귀 기능을 활성화하는 새로운 속성 `ios.mdm.return.to.service`이 포함되어 있습니다. 기본적으로 이 속성은 **True**로 설정되어 있습니다. 자세한 내용은 서버 속성을 참조하십시오.

- **자동 등록 시 설정을 완료하기 위한 최소 OS 버전 적용**

  iOS 17을 사용하면 MDM이 이제 자동 장치 등록을 통해 장치를 등록하는 데 필요한 최소 운영 체제 버전을 적용할 수 있습니다. 자세한 내용은 Apple 배포 프로그램을 통해 장치 배포를 참조하십시오.

  XenMobile Server에는 이제 iOS 17 이상에서 자동 등록 중 설정을 완료하기 위한 최소 OS 버전 요구 사항을 적용할 수 있는 새로운 속성 `ios.mdm.minimum_os_version.enrollment`이 포함되어 있습니다. 기본적으로 이 속성은 **True**로 설정되어 있습니다. 자세한 내용은 서버 속성을 참조하십시오.

- **개인 프로필에서 업무 프로필 이메일 앱에 액세스하고 사용하는 기능 지원**

  제한 장치 정책의 Android Enterprise 설정에 새로운 설정인 **업무 및 개인 프로필에서 이메일 앱 액세스**가 추가되었습니다. 이 설정을 통해 개인 프로필에서 업무 프로필 이메일 앱에 액세스하고 사용할 수 있습니다. 자세한 내용은 제한 장치 정책 - Android Enterprise 설정을 참조하십시오.

  XenMobile Server에는 이제 Android Enterprise 설정에서 개인 프로필에서 업무 프로필 이메일 앱에 액세스하고 사용할 수 있는 기능을 활성화하는 새로운 속성 `afw.mailapp.crossworkprofile`이 포함되어 있습니다. 기본적으로 이 속성은 **True**로 설정되어 있습니다. 자세한 내용은 서버 속성을 참조하십시오.

- **iOS 11.x, 12.x 및 13.x 버전에 대한 새로운 iOS 제한 지원**

  iOS용 제한 정책에 새로운 설정이 추가되었습니다.

  - 공유 iPad 임시 세션 허용

- eSIM 수정 허용
- 네트워크 드라이브 연결 허용
- USB 장치 연결 허용
- 나의 기기 찾기 허용
- 나의 친구 찾기 허용
- QuickPath 키보드 허용
- Wi-Fi 강제 켜기
- 자동 완성 전 인증 강제
- 개인용 핫스팟 설정 수정

자세한 내용은 제한 장치 정책 - iOS 설정을 참조하십시오.

- **Android Enterprise 관리형 구성 정책 개선 사항**

  관리형 구성 정책 아래 **애플리케이션 관리 정책** 페이지에 있는 모든 텍스트 상자의 최대 문자 길이가 4096자로 늘어났습니다.

해결된 문제

- 새 버전의 MAM SDK 지원 앱의 경우 Secure Hub 스토어에서 업데이트 옵션을 사용할 수 없습니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.16 롤링 패치 2 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 2의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 2 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

해결된 문제

- XenMobile Server 10.16 버전으로 업그레이드한 후 XenMobile Server가 Syslog 서버로 로그를 보내는 것을 중지했습니다.
- 프록시가 구성된 경우 HTTP v1 API를 사용하는 Firebase Cloud Messaging이 제대로 작동하지 않습니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 정보는 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.16 롤링 패치 1 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.16 롤링 패치 1의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.16 롤링 패치 1 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **iOS 17.4 이상용 타사 앱 차단 지원:** 제한 정책에 웹에서 대체 마켓플레이스 앱 설치를 방지하고 설치된 대체 마켓플레이스 앱이 앱을 설치하는 것을 방지하기 위한 새로운 설정인 **대체 앱 마켓플레이스**가 추가되었습니다. 자세한 내용은 제한 장치 정책을 참조하십시오.
- **레거시 MDX 모드로 게시된 MDX 앱이 있는 경우 XMS 콘솔에 경고 표시:** 레거시 MDX 모드로 게시된 MDX 앱이 있는 경우 XenMobile Server 콘솔에 경고가 표시됩니다. 자세한 내용은 서버 속성에서 **레거시 MDX 사용 중단 경고**를 참조하십시오.
- **새로운 HTTP v1 API를 사용하도록 마이그레이션된 Firebase Cloud Messaging 지원:** HTTP용 FCM 레거시 API는 Google에서 June 21, 2024에 더 이상 사용되지 않을 예정입니다. FCM이 새로운 API와 잘 작동하도록, 서비스 계정 키 JSON 파일을 업로드할 수 있도록 Firebase Cloud Messaging 페이지에 새로운 필드인 **서비스 계정 키 파일**이 추가되었습니다. 자세한 내용은 Firebase Cloud Messaging을 참조하십시오.

  XenMobile Server에는 새로운 HTTP v1 API와 함께 Firebase Cloud Messaging을 사용할 수 있도록 하는 새로운 속성 `afw.fcm.httpv1.migration`이 있습니다. 이 속성의 기본값은 **False**입니다. 자세한 내용은 서버 속성을 참조하십시오.

  XenMobile Server 10.16 롤링 패치 1 이상에서 FCM API V1을 활성화하려면 기술 자료 문서 CTX677031을 참조하십시오.

해결된 문제

- XenMobile Server 10.16 버전으로 업그레이드한 후 선택적 웹 링크가 계속해서 다시 설치됩니다.
- XenMobile Server를 10.16 버전으로 업그레이드한 후 **클라이언트 지원** 설정에서 **IT 헬프 데스크에 장치 로그 보내기**를 **직접**으로 선택하면 Secure Hub 로그를 IT 헬프 데스크로 보낼 수 없습니다.
- XenMobile® Server 콘솔 > **제한** > **Android Enterprise**에서 정책 설정 **모바일 네트워크 구성**에 대한 도구 설명이 독일어로 잘못 표시됩니다.

XenMobile Server 10.16.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 14 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 14의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 14 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Android 17 지원:**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android 17을 실행하는 Android Enterprise 장치를 지원합니다. 보안 및 개인 정보 보호에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.

- **Microsoft Exchange Online에 대한 OAuth 인증 지원:**

  Microsoft는 Exchange Online이 2026년 3월에 클라이언트 제출(SMTP AUTH)을 통한 기본 인증 지원을 영구적으로 제거하고 April 30, 2026에 100% 거부에 도달할 것이라고 발표했습니다. 자세한 내용은 클라이언트 제출(SMTP AUTH)에 대한 Exchange Online 기본 인증 사용 중단을 참조하십시오.

  XenMobile Server는 SMTP 서버에 대한 OAuth 인증을 지원합니다. **Microsoft Exchange Online OAuth 2.0**을 선택하고 필요한 **Tenant ID**, **Client ID**, **Client Secret**을 제공하여 이 기능을 활성화하십시오. Microsoft Exchange Online을 사용하는 경우 Citrix는 OAuth 인증으로 전환할 것을 권장합니다. 구성 세부 정보는 알림을 참조하십시오.

- **iOS 26.x 앱 크기 검색을 지원하도록 앱 인벤토리 개선:**

  XenMobile Server는 iOS 26.x를 실행하는 장치에 대한 앱 크기 정보 검색을 지원합니다. 이 정보는 **장치 세부 정보 > 앱**에서 찾을 수 있습니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

중요:

- 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.15.0.23으로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스 백업을 생성하십시오.
- 10.15 RP2 또는 10.15 RTM을 포함한 이전 릴리스에서 업그레이드하는 경우 클러스터된 XenMobile 배포 업그레이드의 단계를 따라 모든 클러스터 노드를 업그레이드하십시오.

클러스터 모드로 구성된 시스템의 경우, 각 노드를 하나씩 업데이트하려면 다음 단계를 따르십시오.

1. Citrix® 웹사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **설정 > 릴리스 관리**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **업데이트**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix 다운로드 페이지에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음 **설정 > 릴리스 관리 > 업데이트**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.15 롤링 패치 14 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 14의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 14 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Android 17 지원:**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android 17을 실행하는 Android Enterprise 장치를 지원합니다. 보안 및 개인 정보 보호에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.
- **Microsoft Exchange Online에 대한 OAuth 인증 지원:**

  Microsoft는 Exchange Online이 2026년 3월에 클라이언트 제출(SMTP AUTH)을 통한 기본 인증 지원을 영구적으로 제거하고 April 30, 2026에 100% 거부에 도달할 것이라고 발표했습니다. 자세한 내용은 클라이언트 제출(SMTP AUTH)에 대한 Exchange Online 기본 인증 사용 중단을 참조하십시오.

  XenMobile Server는 SMTP 서버에 대한 OAuth 인증을 지원합니다. **Microsoft Exchange Online OAuth 2.0**을 선택하고 필요한 **Tenant ID**, **Client ID**, **Client Secret**을 제공하여 이 기능을 활성화하십시오. Microsoft Exchange Online을 사용하는 경우 Citrix는 OAuth 인증으로 전환할 것을 권장합니다. 구성 세부 정보는 알림을 참조하십시오.

- **iOS 26.x 앱 크기 검색을 지원하도록 앱 인벤토리 개선:**

  XenMobile Server는 iOS 26.x를 실행하는 장치에 대한 앱 크기 정보 검색을 지원합니다. 이 정보는 **장치 세부 정보 > 앱**에서 찾을 수 있습니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

중요:

- 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.15.0.23으로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스 백업을 생성하십시오.
- 10.15 RP2 또는 10.15 RTM을 포함한 이전 릴리스에서 업그레이드하는 경우 클러스터된 XenMobile 배포 업그레이드의 단계를 따라 모든 클러스터 노드를 업그레이드하십시오.

클러스터 모드로 구성된 시스템의 경우, 각 노드를 하나씩 업데이트하려면 다음 단계를 따르십시오.

1. Citrix® 웹사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **설정 > 릴리스 관리**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **업데이트**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix 다운로드 페이지에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음 **설정 > 릴리스 관리 > 업데이트**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.15 롤링 패치 13 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 13의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 13 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **라이선스 활성화 서비스:**

  XenMobile Server는 이제 라이선스 활성화 서비스(LAS) 라이선스 메커니즘을 지원합니다. LAS는 Citrix 제품군 전체에서 기존 파일 기반 라이선싱에 대한 최신 대안을 제공하는 새로운 클라우드 기반 라이선싱 솔루션입니다. Citrix License Server를 Citrix Cloud에 등록하여 라이선스 활성화 서비스가 보유한 라이선스 및 권한을 사용하십시오. 자세한 내용은 라이선스 활성화 서비스를 참조하십시오.

  > **중요:**
  >
  > Citrix 플랫폼의 업계 표준 클라우드 기반 라이선싱 아키텍처로 전환하고 있습니다. 이 전환은 권한 및 활성화를 자동화하여 다음과 같은 주요 고객 이점을 제공합니다.
  >
  > - **라이선스 파일 관리 불필요:** 라이선스 파일을 다운로드, 할당 또는 관리할 필요가 없어 관리 작업이 간소화됩니다.
  > - **자동화된 권한 업데이트:** 계약 갱신 시 권한이 백그라운드에서 자동으로 업데이트되어 중단 없는 서비스를 보장합니다.
  > - **향상된 복원력:** License Server가 더 이상 사용자 세션의 단일 실패 지점이 아니므로 환경의 안정성이 향상됩니다. 저희는 여러분이 April 15, 2026까지 새로운 라이선싱 모델을 채택하기 위한 전환을 계획하고 실행하는 데 필요한 시간을 활용하시기를 권장하며, 모든 단계에서 지원을 아끼지 않을 것입니다. 자세한 내용은 Citrix Modern Licensing Announcement를 참조하십시오.
  >
  > *10.15 롤링 패치 13 이상 롤링 패치에서 라이선스 활성화 서비스가 활성화된 경우, 10.16.0.48로 직접 업그레이드하면 라이선스 활성화 서비스 구성이 재설정됩니다. 라이선스 활성화 서비스를 재구성할 수 있는 버전 10.16 롤링 패치 7 이상 버전의 10.16 롤링 패치를 계속 적용하십시오. 기존 장치는 영향을 받지 않습니다.*

해결된 문제

- XenMobile 서버의 높은 CPU 및 메모리 사용률로 인해 장치 등록에 실패합니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

중요:

- 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.15.0.23으로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 만들고 데이터베이스 백업을 생성하십시오.
- 10.15 RP2 또는 10.15 RTM을 포함한 이전 릴리스에서 업그레이드하는 경우, 모든 클러스터 노드를 업그레이드하려면 클러스터된 XenMobile 배포 업그레이드의 단계를 따르십시오.

클러스터 모드로 구성된 시스템의 경우 다음 단계에 따라 각 노드를 순서대로 업데이트하십시오.

1. Citrix® 웹사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **설정 > 릴리스 관리**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **업데이트**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix 다운로드 페이지에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포 확인

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음 **설정 > 릴리스 관리 > 업데이트**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.15 롤링 패치 12 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 12의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 12 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **인증서 기반 인증을 위한 새로운 강력한 인증서 매핑 지원**

강력한 매핑 요구 사항을 충족하는 인증서 발급에 더 큰 유연성을 제공하기 위해 새로운 매핑 방법이 도입되었습니다. XenMobile Server는 이제 인증서의 주체 대체 이름(SAN)에 `URL=tag:microsoft.com`, `2022-09-14:sid:<user's SID>`를 추가합니다.

  - 기존 사용자를 위해 이 기능을 활성화하려면 고객 관리자가 클라이언트 속성 `MICROSOFT_CERTIFICATE_STRONG_MAPPING`을 추가해야 합니다. 자세한 내용은 클라이언트 속성을 참조하십시오.
  - 강력한 인증서 매핑은 **Windows Server 2019 이상**에서만 지원됩니다. 자세한 내용은 Microsoft 강력한 매핑을 참조하십시오.

- **iOS 26 지원**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 iOS 26과 호환됩니다.

- **Android 16 지원**

  XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android 16을 실행하는 Android Enterprise 장치를 지원합니다. 보안 및 개인 정보 보호에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.

- **구성 정책 텍스트 상자 관리**

  고객이 **Knox Service Plugin**과 **관리형 구성 정책**을 함께 사용하는 경우, **분리된 앱 정책**의 모든 텍스트 상자에 대한 최대 문자 길이가 8,192자로 증가합니다.

- **Secure Hub APNs 인증서 갱신**

  XenMobile Server 10.15용 Secure Hub Apple Push Notification service(APNs) 인증서는 January 4, 2026에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 November 9, 2026까지 유효한 새 인증서로 자동 갱신합니다.

해결된 문제

- 마우스 오른쪽 클릭으로 암호를 붙여넣어 입력하면 XenMobile 포털의 로그인 버튼이 회색으로 비활성화됩니다.
- iOS 사용자가 Secure Mail/Secure Web에서 Secure Hub로 리디렉션할 때 Secure Mail/Secure Web 애플리케이션을 시작할 수 없으며 "열 수 없음" 오류가 발생합니다.
- 등록 프로필이 **MDM 전용**으로 구성된 경우에도 DEP(Device Enrollment Program) 장치는 계속해서 **MDM+MAM** 등록을 수행합니다.
- XenMobile MDM 솔루션으로 Windows 클라이언트를 등록할 때 배달 그룹 배포가 실패합니다. 결과적으로 푸시된 정책을 적용하려면 수동 동기화 작업이 필요합니다. 해결 방법으로 단일 장치에 수동 배포가 필요합니다.

- iOS 장치에 설치되지 않은 애플리케이션에 대한 앱 잠금 정책이 있는 경우, 강제 재부팅 후에도 장치가 "안내된 접근 앱을 사용할 수 없습니다. 관리자에게 문의하십시오." 오류와 함께 잠기고 터치스크린이 응답하지 않게 됩니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 업데이트 설치

중요:

- 이 업데이트를 설치하기 전에 XenMobile Server 버전 10.15.0.23으로 업그레이드했는지 확인하십시오. 또한 현재 설정의 스냅샷을 찍고 데이터베이스 백업을 생성하십시오.
- 10.15 RP2 또는 10.15 RTM을 포함한 이전 릴리스에서 업그레이드하는 경우, 클러스터된 XenMobile 배포 업그레이드의 단계를 따라 모든 클러스터 노드를 업그레이드하십시오.

클러스터 모드로 구성된 시스템의 경우, 다음 단계에 따라 각 노드를 차례로 업데이트하십시오.

1. Citrix® 웹사이트에서 계정에 로그인하고 XenMobile Server 업데이트(.bin) 파일을 적절한 위치에 다운로드합니다.
2. 노드의 XenMobile Server 콘솔에서 **설정 > 릴리스 관리**를 클릭합니다.

   릴리스 관리 페이지에는 현재 설치된 소프트웨어 버전과 업로드한 모든 업데이트, 패치 및 업그레이드 목록이 표시됩니다.
3. 릴리스 관리에서 **업데이트**를 클릭합니다. 업데이트 대화 상자가 나타납니다.
4. Citrix 다운로드 페이지에서 다운로드한 업데이트(.bin) 파일을 업로드하려면 **찾아보기**를 클릭합니다.
5. **업데이트**를 클릭한 다음, 메시지가 표시되면 명령줄을 사용하여 XenMobile Server 노드를 다시 시작합니다.

패치 배포를 확인하려면

이 패치를 설치한 후 관리자로 XenMobile Server 콘솔에 로그인한 다음 **설정 > 릴리스 관리 > 업데이트**로 이동합니다. 이 페이지에는 가장 최근에 설치된 패치에 대한 세부 정보가 표시됩니다.

XenMobile Server 10.15 롤링 패치 11 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 11의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 11 소프트웨어 바이너리는 다운로드에 로그인에서 다운로드할 수 있습니다.

해결된 문제

- 배포 일정에서 배포 조건이 "이전 배포가 실패한 경우에만"으로 설정된 경우 재등록 중에 일부 정책이 AE 장치에 배포되지 않습니다.
- AE 장치에 대해 수많은 페이로드 인증서가 생성됩니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 10 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 10의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 10 소프트웨어 바이너리는 다운로드 로그인에서 다운로드할 수 있습니다.

새로운 기능

Secure Hub APNs certificate renewal: XenMobile Server 10.15용 Secure Hub Apple Push Notification service(APNs) 인증서는 February 9, 2025에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 January 4, 2026까지 유효한 새 인증서로 자동 갱신합니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 9 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 9의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 9 소프트웨어 바이너리는 다운로드 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Android 15 지원**: XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android Enterprise 장치 업데이트를 Android 15까지 지원합니다. 보안 및 개인 정보 보호 이점에 대한 자세한 내용은 Android 개발자 설명서를 참조하십시오.
- **iOS 18 지원**: XenMobile® Server 및 Citrix Mobile 생산성 앱은 이제 iOS 18과 호환되지만, 현재 모든 새로운 iOS 18 기능을 지원하지는 않습니다.
- **macOS 15 지원**: XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 macOS 15와 호환되지만, 현재 모든 새로운 macOS 15 기능을 지원하지는 않습니다.
- **장치 분실 모드 API를 포함하도록 공용 REST API 문서 업데이트**: 공용 REST API 문서에 분실 모드 API를 추가했습니다.
- **API 호출을 URL 대신 POST 본문으로 수정**: 공용 REST API 문서에서 API 호출을 업데이트하여 URL 대신 요청 본문에 데이터를 포함하도록 했습니다.

- **구성 정책 텍스트 상자 관리**: 관리되는 구성 정책 아래의 **애플리케이션 관리 정책** 페이지에 있는 모든 텍스트 상자의 최대 문자 길이가 4,096자로 늘어났습니다.

해결된 문제

- 새 버전의 MAM SDK 지원 앱에 대해 Secure Hub 스토어에서 **업데이트** 옵션을 사용할 수 없습니다.
- SQL Server가 경고 메시지를 트리거할 때 발생하는 성능 문제로 인해 XenMobile Server가 새로운 Android Enterprise 장치를 성공적으로 등록할 수 없습니다.
- 고객이 FIPS 설정을 **true**로 활성화했음에도 불구하고 로그에는 계속 비활성화된 것으로 표시됩니다. 또한 고객이 CLI를 통해 데이터베이스 설정을 수정하려고 하면 XenMobile 서버가 데이터베이스에 대한 연결을 설정하지 못하여 업데이트가 적용되지 않습니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 정보는 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 8 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 8의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 8 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

해결된 문제

- 프록시가 구성된 경우 HTTP v1 API를 사용하는 Firebase Cloud Messaging이 제대로 작동하지 않습니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 정보는 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 7 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 7의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 7 소프트웨어 바이너리는 다운로드 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **iOS 17.4 이상용 타사 앱 차단 지원:** 제한 정책에 웹에서 대체 마켓플레이스 앱 설치를 방지하고 설치된 대체 마켓플레이스 앱이 앱을 설치하는 것을 방지하기 위한 새로운 설정인 **대체 앱 마켓플레이스**가 추가되었습니다. 자세한 내용은 제한 장치 정책을 참조하십시오.
- **레거시 MDX 모드로 게시된 MDX 앱이 있는 경우 XMS 콘솔에 경고 표시:** 레거시 MDX 모드로 게시된 MDX 앱이 있는 경우 XenMobile Server 콘솔에 경고가 표시됩니다. 자세한 내용은 서버 속성에서 **레거시 MDX 사용 중단 경고**를 참조하십시오.

- **새로운 HTTP v1 API를 사용하도록 마이그레이션된 Firebase Cloud Messaging 지원:** HTTP용 FCM 레거시 API는 June 21, 2024부터 Google에서 더 이상 사용되지 않습니다. FCM이 새 API와 잘 작동하도록, 서비스 계정 키 JSON 파일을 업로드할 수 있는 새 필드 **서비스 계정 키 파일**이 Firebase Cloud Messaging 페이지에 추가되었습니다. 자세한 내용은 Firebase Cloud Messaging을 참조하십시오.

  XenMobile Server에는 새로운 HTTP v1 API와 함께 Firebase Cloud Messaging을 사용할 수 있도록 하는 새로운 속성 `afw.fcm.httpv1.migration`이 있습니다. 이 속성의 기본값은 **False**입니다. 자세한 내용은 서버 속성를 참조하십시오.

  XenMobile Server 10.15 롤링 패치 7 이상에서 FCM API V1을 활성화하려면 기술 자료 문서 CTX677031을 참조하십시오.

해결된 문제

- Apple Business Manager(ABM) 공유 iPad의 경우, XenMobile® Server는 등록 전에 서버 데이터베이스에 없는 로그인 사용자를 "익명"으로 표시합니다.
- MacOS 및 iOS 플랫폼을 모두 지원하는 공용 VPP 앱이 XenMobile에 동기화될 때, iOS 플랫폼만 표시되고 MacOS 플랫폼은 누락됩니다.
- XenMobile Server의 일부 iOS 공용 앱은 Apple Store에서 찾을 수 없습니다.
- XenMobile Server 10.15 RP6으로 업그레이드한 후, DEP 설정 "구성 완료를 기다림"이 더 이상 적용되지 않아 정책 수신을 기다리지 않고 DEP 설정 지원 페이지가 빠르게 나타납니다.
- 업그레이드 후 XenMobile Server 콘솔에 로그인할 때 관리 탭에 오류 메시지 “**java.util.ConcurrentModificationException**”이 표시됩니다.
- XenMobile Server 10.15 RP6으로 업그레이드한 후, 선택적 웹 링크가 계속해서 다시 설치됩니다.
- XenMobile Server 콘솔 > **제한 사항** > **Android Enterprise**에서 정책 설정 **모바일 네트워크 구성**에 대한 도구 설명이 독일어로 잘못되었습니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 6 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 6의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 6 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Secure Hub APNs 인증서 갱신**

XenMobile Server 10.15용 Secure Hub Apple Push Notification Service(APNs) 인증서는 March 12, 2024에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 February 9, 2025에 만료되는 새 인증서로 자동으로 갱신합니다.

- **iOS용 웹 클립 정책 설정에 새 필드 프로필 범위 추가**

  iOS 장치의 경우 웹 클립 장치 정책의 **정책 설정** 아래에 **프로필 범위**라는 새 필드가 추가되었습니다. 이 기능을 사용하면 정책을 사용자에게 적용할지 시스템에 적용할지 선택할 수 있습니다. 자세한 내용은 웹 클립 장치 정책 - iOS 설정을 참조하십시오.

- **REST API를 사용하여 공용 스토어 앱에 대한 배포 규칙 업데이트**

  새 공용 스토어 앱 추가 및 **공용 스토어 앱 업데이트** REST API에 **규칙**이라는 새 필드가 추가되었습니다. 이 기능을 사용하면 공용 스토어 앱에 대한 배포 규칙을 업데이트할 수 있습니다. 자세한 내용은 공용 REST API 설명서를 참조하십시오.

- **앱 특성 장치 정책이 새로운 iOS 앱 특성 지원**

  이제 iOS 장치에 설치된 앱에 대해 다음 특성을 지정할 수 있습니다.

  - **제거 가능한 앱:** 관리되는 앱인 경우 사용자가 앱을 제거할 수 있는지 여부를 지정합니다.
  - **연결된 도메인 직접 다운로드 사용:** 앱이 도메인에서 직접 주장된 사이트 연결 확인을 수행할 수 있는지 여부를 지정합니다.
  - **연결된 도메인:** 앱에 추가할 연결된 도메인을 지정합니다.

  자세한 내용은 앱 특성 장치 정책을 참조하십시오.

- **새로운 Knox Platform for Enterprise Key 장치 정책 추가**

  Knox Platform for Enterprise Key라는 새로운 장치 정책이 추가되었습니다. 이 정책을 통해 필요한 Samsung Knox Platform for Enterprise(KPE) 라이선스 정보를 제공하고 KPE 라이선스를 사용하여 Samsung 장치의 보안을 강화할 수 있습니다. 자세한 내용은 Knox Platform for Enterprise Key 장치 정책을 참조하십시오.

- **공유 iPad용 Apple Business Manager 지원**

  XenMobile Server 10.15 RP6부터 공유 iPad는 XenMobile Server와 함께 Apple Business Manager(ABM)를 지원합니다. 이 기능을 통해 ABM 계정을 사용하여 공유 iPad에 로그인하고 사용할 수 있습니다. 자세한 내용은 공유 iPad 구성을 참조하십시오.

> **참고:**

> 현재 이 기능에는 로그인한 사용자가 XenMobile® Server 콘솔에 "익명"으로 표시될 수 있는 제한 사항이 있습니다. 결과적으로 "모든 사용자 삭제"와 같은 특정 보안 작업은 장치, 특히 공유 iPad로 사용되는 장치에서 수행되지 않을 수 있습니다. 이 문제를 해결하려면 XenMobile Server 콘솔에 DEP 사용자(관리형 Apple ID)를 수동으로 추가하는 것이 좋습니다. 특히 ABM의 공유 iPad를 사용하는 경우 더욱 그렇습니다. 영구적인 해결책은 향후 릴리스에 포함될 예정입니다.

- **공유 iPad용 모든 사용자 삭제라는 새로운 보안 작업 추가**

  XenMobile Server 10.15 RP6부터 XenMobile Server의 공유 iPad에 **모든 사용자 삭제**라는 새로운 보안 작업이 추가되었습니다. 이 기능을 통해 장치의 모든 사용자를 삭제할 수 있습니다. 자세한 내용은 공유 iPad용 보안 작업을 참조하십시오.

- **새로운 전송 그룹의 기반으로 사용할 전송 그룹 복제**

  이 기능을 사용하면 여러 정책, 앱 및 작업을 포함하는 복잡한 전송 그룹을 복사할 수 있습니다. 그런 다음 등록 프로필 또는 새로운 Active Directory 사용자 세트를 추가하는 등 복사본을 편집할 수 있습니다. 자세한 내용은 전송 그룹 복제를 참조하십시오.

- **iOS에서 선택적 앱의 자동 업데이트 지원**

  XenMobile Server 10.15 RP6부터 `apple.ios.optional_app_update`이라는 새 서버 속성이 추가되었습니다. 이 속성을 사용하면 iOS에서 선택적 앱을 자동 업데이트할 수 있습니다. `apple.ios.optional_app_update`의 기본값은 `False`으로 설정됩니다. 자세한 내용은 서버 속성를 참조하십시오.

  선택적 볼륨 구매 앱의 자동 업데이트에 대한 자세한 내용은 앱 업데이트 확인을 참조하십시오.

- **데이터베이스 업그레이드 메커니즘 최적화**

  데이터베이스 업그레이드 프로세스가 최적화되어 각 클러스터가 한 번만 업그레이드되도록 합니다. 이를 통해 HA 클러스터에서 롤링 패치 업데이트 중 다운타임을 최소화할 수 있습니다.

해결된 문제

- ABM 또는 ASM 구성을 사용하는 경우 iOS 공유 장치에 Webclip 장치 정책을 배포할 수 없습니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 5 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 5의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 5 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **Android Enterprise용 802.1x 설정에 새로운 필수 필드 “도메인” 추가**

  802.1x EAP 인증 유형에 대한 Android Enterprise 플랫폼 네트워크 정책 설정 페이지에 새로운 필드 **도메인**이 추가되었습니다. 자세한 내용은 Android Enterprise용 802.1x 설정을 참조하십시오.

  XenMobile Server에는 **Android Enterprise용 802.1x 설정**에 *도메인* 필드를 추가하는 새로운 속성 `afw.network.domain.support`이 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 서버 속성을 참조하십시오.

- **iOS용 OS 업데이트 제어 정책에 새로운 옵션 "OS 업데이트 버전" 추가**

  iOS 플랫폼용 **OS 업데이트 제어** 정책에서 **OS 업데이트 빈도** 필드 뒤에 새로운 옵션 **OS 업데이트 버전**이 추가되었습니다. 이 옵션을 사용하면 감독되는 iOS 장치를 업데이트하는 데 사용할 OS 버전을 지정할 수 있습니다. 자세한 내용은 iOS 설정을 참조하십시오.

- **iOS용 제한 정책 및 Exchange 정책에 새로운 설정 추가**

  - iOS용 Exchange 정책에 새로운 설정 **Mail Drop 허용**이 추가되었습니다. 자세한 내용은 Exchange 장치 정책 - iOS 설정을 참조하십시오.
  - iOS용 제한 정책에 다음 새로운 설정이 추가되었습니다.
    - 페어링되지 않은 장치에 의한 복구 부팅 허용
    - 신속 보안 응답 설치
    - 신속 보안 응답 제거
    - 메일 개인 정보 보호 허용
    - NFC
    - 앱 클립 허용
    - Apple 개인 맞춤형 광고 허용
    - 자동 잠금 해제

    자세한 내용은 제한 장치 정책 - iOS 설정을(를) 참조하십시오.

- **OS 업데이트**

  - **Android 14 지원:** XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android Enterprise 장치 업데이트를 Android 14까지 지원합니다. 보안 및 개인 정보 보호 이점에 대한 자세한 내용은 Android 설명서를 참조하십시오.
  - **iOS 17 지원:** XenMobile® Server 및 Citrix Mobile 생산성 앱은 이제 iOS 17과 호환되지만, 현재 iOS 17의 새로운 기능은 지원하지 않습니다.

- **macOS 14 지원:** XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 macOS 14와 호환되지만, 현재 macOS 14의 새로운 기능은 지원하지 않습니다.

해결된 문제

- XenMobile Server 10.15 RP3 또는 10.15 RP4로 업그레이드한 후, **Android Enterprise** > **관리형 Google Play 스토어 앱**의 **구성** > **앱** 페이지에서 **앱 구성** 버튼을 사용할 수 없습니다.
- XenMobile Server 10.15 RP3 또는 10.15 RP4로 업그레이드한 후, **Android Enterprise** 플랫폼용 Wi-Fi 정책을 구성하는 동안 **CA 인증서** 드롭다운 메뉴에서 어떤 값도 볼 수 없습니다. **인증서 선택** 옵션만 표시됩니다.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 4 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 4의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 4 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **장치 및 앱 보고서 액세스**

  이전에는 역할 기반 액세스 제어(RBAC)가 적용된 경우에도 **장치 및 앱** 보고서 페이지에 사용자 그룹과 관계없이 모든 사용자의 모든 장치 및 앱에 대한 정보가 표시되었습니다.

  XenMobile Server 10.15 롤링 패치 4 릴리스부터 **장치 및 앱** 보고서 페이지에는 RBAC 역할이 관리할 권한이 있는 **특정 사용자 그룹** 구성에 정의된 사용자 그룹에 특정한 장치 및 앱이 표시됩니다. RBAC를 사용하여 역할을 구성하는 방법에 대한 자세한 내용은 RBAC를 사용하여 역할 구성을 참조하십시오.

- **OS 업데이트 제어 장치 정책을 시스템 기본값으로 재설정 지원**

  XenMobile Server 10.15 롤링 패치 4 릴리스부터 Android Enterprise의 **OS 업데이트 제어** 페이지에 있는 **시스템 업데이트 정책** 드롭다운 목록에 새로운 값 **기본값**이 추가되었습니다. 이 기능을 사용하면 시스템 업데이트 정책을 시스템 기본값으로 재설정할 수 있습니다. 자세한 내용은 OS 업데이트 제어 장치 정책을 참조하십시오.

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

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

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

XenMobile Server 10.15 롤링 패치 4 릴리스부터 관련 설정을 활성화하여 iOS용 다음 동기화된 Exchange 서비스를 동기화할지 또는 재정의할지 선택할 수 있습니다.

- 캘린더
- 연락처
- 메일
- 참고
- 알림

자세한 내용은 Exchange 장치 정책을 참조하십시오.

- **iOS 장치에서 eSIM 지원**

  XenMobile Server에는 `ios.esim.support`이라는 새 속성이 있으며, 이 속성을 통해 XenMobile Server는 iOS 장치에서 eSIM 정보를 가져와 사용자 인터페이스에 eSIM 관련 장치 속성을 표시할 수 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 서버 속성을 참조하십시오.

XenMobile Server 10.15.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.15 롤링 패치 3 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 3의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 3 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **XenMobile Server에서 혼합 라이선스 유형 지원.** 이 기능을 통해 고객은 XenMobile Server 또는 Citrix Licensing Server를 사용하여 다양한 XenMobile 라이선스 유형 및 에디션을 활성화할 수 있습니다. 자세한 내용은 다른 라이선스를 활성화하려면을 참조하십시오.
- **macOS 장치에서 엔터프라이즈 앱 지원.** XenMobile Server에는 macOS를 실행하는 장치에서 엔터프라이즈 앱을 지원하는 새로운 속성 `mac.app.push`이 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 서버 속성을 참조하십시오.

해결된 문제

- **관리형 Google Play 계정**에서 앱을 다운로드할 수 없습니다.
- XenMobile® Server 콘솔에서 RSR(Rapid Security Response) 버전을 볼 수 없습니다.
- Android 장치에서 사용자가 레거시 MDX Toolkit에서 MAM SDK로 전환하면 Secure Mail 앱이 Secure Hub Store에서 제거됩니다.

- XenMobile Server 10.15 RP2로 업그레이드한 후, "**제한된 앱 사용**"을 사용하는 기존 iOS 제한 장치 정책이 iOS 장치에 배포되지 않습니다.

XenMobile Server 10.15 롤링 패치 2 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 2의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 2 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

XenMobile Analyzer 도구 사용 중단. 빈번하고 안정적인 릴리스 주기 덕분에 XenMobile Analyzer 도구는 더 이상 필요하지 않습니다. Citrix는 March 31, 2023부터 이 서비스를 중단했습니다. Citrix XenMobile 콘솔 또는 Citrix NetScaler Gateway 내에서 사용할 수 있는 연결 검사를 사용하는 것이 좋습니다. 자세한 내용은 연결 검사를 참조하십시오.

해결된 문제

- 알고리즘 APK 서명 체계 v2 이상을 사용하여 Android 플랫폼에서 엔터프라이즈 앱을 구성할 수 없습니다.
- NetScaler에서 nFactor 인증 정책을 사용하는 경우 Android 및 iOS 장치에서 MAM에 액세스할 수 없습니다.
- XenMobile Server 버전 10.14 이상에서 Citrix Gateway 인증 구성 스크립트를 내보내면 스크립트가 잘리고 작동하지 않습니다.
- XenMobile Server에서 설명에 **\b**가 포함된 동기화된 VPP 앱을 다시 편집할 수 없습니다.
- XenMobile Server 버전 10.15 이상에서 OCSP(Online Certificate Status Protocol)가 요청에 응답하지 않습니다.
- XenMobile® Server에서 Windows 11을 실행하는 장치를 등록할 수 없습니다.

XenMobile Server 10.15 롤링 패치 1 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.15 롤링 패치 1의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다. XenMobile Server 10.15 롤링 패치 1 소프트웨어 바이너리는 다운로드하려면 로그인에서 다운로드할 수 있습니다.

새로운 기능

- **네트워크 액세스 제어.** NAC(네트워크 액세스 제어) 솔루션을 사용하여 Android 및 Apple 장치에 대한 XenMobile 장치 보안 평가를 확장하십시오. NAC 솔루션은 XenMobile 보안 평가를 사용하여 인증 결정

을 용이하게 하고 처리합니다. NAC 어플라이언스를 구성한 후 XenMobile에서 구성한 장치 정책 및 NAC 필터가 적용됩니다. 자세한 내용은 네트워크 액세스 제어를 참조하십시오.

- **Secure Hub APNs 인증서 갱신.** XenMobile Server 10.15용 Secure Hub APNs(Apple Push Notification Service) 인증서는 April 8, 2023에 만료됩니다. 이 업데이트는 March 12, 2024에 만료될 Secure Hub APNs 인증서를 갱신합니다.

해결된 문제

- Android Enterprise 장치에서 관리형 구성 정책을 편집하거나 배포할 때 오류가 발생합니다.
- MAM 전용 모드에 등록된 iOS 장치에서는 Secure Hub 스토어에서 엔터프라이즈 또는 MDX 앱을 설치할 수 없습니다.
- 앱의 트랙 ID를 구성한 후 XenMobile® Server 콘솔에서 예상되는 앱 미리 보기 버전을 볼 수 없습니다. 대신 앱의 프로덕션 버전이 표시됩니다.
- XenMobile Server에서 프로비저닝 프로필 장치 정책이 보류 중인 상태일 때 Secure Hub 스토어에서 MDX 래핑된 앱을 설치할 수 없습니다.
- MDM 프로필 갱신 후 ABM 공유 iPad가 관리되지 않는 상태로 전환됩니다.

XenMobile Server 10.14 롤링 패치 13 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 13의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

Secure Hub APNs 인증서 갱신:

XenMobile Server 10.14용 Secure Hub Apple Push Notification Service (APNs) 인증서는 March 12, 2024에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 February 9, 2025에 만료되는 새 인증서로 자동으로 갱신합니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.14 롤링 패치 13 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 13의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

Secure Hub APNs 인증서 갱신:

XenMobile Server 10.14용 Secure Hub Apple Push Notification Service (APNs) 인증서는 March 12, 2024에 만료됩니다. 이 업데이트는 Secure Hub APNs 인증서를 February 9, 2025에 만료되는 새 인증서로 자동으로 갱신합니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.14 롤링 패치 12 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 12의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

해결된 문제

- **관리형 Google Play 계정**에서 앱을 다운로드할 수 없습니다.
- XenMobile Server 10.14 RP11로 업그레이드한 후 기존 iOS 제한 정책이 장치에 배포되지 않습니다.
- Secure Hub에 모바일 장치를 등록하면 Secure Hub 스토어 및 관리형 Google Play 스토어에 앱이 표시되지 않습니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 정보는 를 참조하십시오. (/ko-kr/xenmobile/server/release-notes.html).

XenMobile Server 10.14 롤링 패치 11 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 11의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

해결된 문제

- APK Signature Scheme v2 이상 알고리즘을 사용하여 Android 플랫폼에서 엔터프라이즈 앱을 구성할 수 없습니다.
- XenMobile Server에서 설명에 \b가 포함된 동기화된 VPP 앱을 다시 편집할 수 없습니다.
- XenMobile Server 버전 10.14 RP9 이상에서 온라인 인증서 상태 프로토콜(OCSP)이 요청에 응답하지 않습니다.
- XenMobile® Server에서 Windows 11을 실행하는 장치를 등록할 수 없습니다.
- XenMobile Server 콘솔에서 Rapid Security Response(RSR) 버전을 볼 수 없습니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 정보는 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.14 롤링 패치 10 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 10의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

- **Secure Hub APNs 인증서 갱신.** XenMobile Server 10.14용 Secure Hub Apple Push Notification Service(APNs) 인증서는 April 8, 2023에 만료됩니다. 이 업데이트는 March 12, 2024에 만료될 Secure Hub APNs 인증서를 갱신합니다.
- **XenMobile Analyzer Tool 사용 중단.** 잦고 안정적인 릴리스 주기 덕분에 XenMobile Analyzer Tool은 더 이상 필요하지 않습니다. Citrix는 March 31, 2023부터 이 서비스 제공을 중단하기로 결정했습니다. Citrix XenMobile 콘솔 또는 Citrix NetScaler Gateway에서 사용할 수 있는 연결 확인 기능을 사용하는 것이 좋습니다. 자세한 내용은 연결 확인을 참조하십시오.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

- MDM 프로필 갱신 후 ABM 공유 iPad가 관리되지 않는 상태로 전환됩니다.
- MAM 전용 모드로 등록된 iOS 장치에서는 Secure Hub 스토어에서 엔터프라이즈 또는 MDX 앱을 설치할 수 없습니다.
- NetScaler에서 nFactor 인증 정책을 사용하는 경우 Android 및 iOS 장치에서 MAM에 액세스할 수 없습니다.
- XenMobile Server 버전 10.14 이상에서 Citrix Gateway 인증 구성 스크립트를 내보낼 때 스크립트가 잘리고 작동하지 않습니다.

XenMobile Server 10.14 롤링 패치 9 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 9의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

네트워크 액세스 제어. NAC(네트워크 액세스 제어) 솔루션을 사용하여 Android 및 Apple 장치에 대한 XenMobile 장치 보안 평가를 확장합니다. NAC 솔루션은 XenMobile 보안 평가를 사용하여 인증 결정을 용이하게 하고 처리합니다. NAC 어플라이언스를 구성하면 XenMobile에서 구성한 장치 정책 및 NAC 필터가 적용됩니다. 자세한 내용은 네트워크 액세스 제어를 참조하십시오.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

- XenMobile Server 버전 10.14에서 라이선스 만료일이 알림 기간을 벗어났음에도 불구하고 라이선스 만료 알림을 받습니다.
- 일부 앱에서 설치된 버전이 최신 버전임에도 불구하고 Secure Hub 앱 스토어에 **업데이트 보류 중** 상태가 표시됩니다.
- XenMobile® Server에서 독일어 로케일로 제한 장치 정책을 생성하거나 편집할 수 없습니다.
- XenMobile Server 버전 10.14에서 비DEP iOS 장치의 경우 **소유자** 탭이 비어 있습니다.
- **주체 대체 이름 유형**이 *없음*이 아닌 경우 SCEP 장치 정책이 실패합니다.
- Android Enterprise 장치에서 관리형 구성 정책을 편집하거나 배포할 때 오류가 발생합니다.
- MAM 전용 모드로 등록된 iOS 장치에서는 Secure Hub 앱 스토어에서 엔터프라이즈 또는 MDX 앱을 설치할 수 없습니다.
- 앱의 트랙 ID를 구성한 후 XenMobile Server 콘솔에서 예상 미리 보기 버전의 앱을 볼 수 없습니다. 대신 앱의 프로덕션 버전이 표시됩니다.
- XenMobile Server에서 프로비저닝 프로필 장치 정책이 보류 중 상태일 때 Secure Hub 스토어에서 MDX 래핑 앱을 설치할 수 없습니다.

XenMobile Server 10.14 롤링 패치 8 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 8의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

Windows Information Protection 정책에 대한 지원 중단. Windows 공지에 따라 XenMobile Server는 Windows Information Protection(WIP)에 대한 지원을 중단했습니다. WIP 지원은 기본적으로 값이 **True**로 설정된 **windows.wip.deprecation**이라는 서버 속성을 추가하여 중단되었습니다. 자세한 내용은 서버 속성을 참조하십시오.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

- XenMobile® Server에서 독일어 로캘의 **관리되는 앱 자동 업데이트** 정책을 생성하거나 편집할 수 없습니다.

XenMobile Server 10.14 롤링 패치 7 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 7의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

- **OS 업데이트**
  - **iOS 16 지원.** XenMobile® Server 및 Citrix Mobile 생산성 앱은 iOS 16과 호환되지만, 현재 iOS 16의 새로운 기능은 지원하지 않습니다.
  - **Android 13 지원**. XenMobile Server는 이제 Android Enterprise 장치 업데이트를 Android 13으로 지원합니다. 보안 및 개인 정보 보호 이점에 대한 요약은 Android 설명서를 참조하십시오.
- **사용 중단된 기능.** 다음 기능에 대한 지원이 제거되었습니다:
  - RBAC 역할 - 공유 및 COSU 장치 등록자
  - Android - 소니 및 HTC
  - 고보안 등록 모드
  - 파생 자격 증명
  - SEAMS
  - 윈도우 폰 장치 ,
  - 일반, DigiCert 관리 및 Entrust 어댑터 PKI 엔터티.

  자세한 내용은 사용 중단을 참조하십시오.
- **모바일 서비스 공급자(MSP) 인터페이스 지원이 더 이상 사용되지 않습니다.** MSP 지원은 콘솔에서 MSP 인터페이스를 제거하는 `deprecate.mobile.service.provider`이라는 새 서버 속성을 추가하여 더 이상 사용되지 않도록 설정되었으며, 이 속성은 기본적으로 **True**로 설정됩니다. 자세한 내용은 서버 속성을 참조하십시오.
- **Windows 10 장치에 대한 *WiFi Sense 핫스팟에 자동 연결 허용* 제한 정책 지원이 제거되었습니다.** 자세한 내용은 Windows 데스크톱/태블릿 설정을 참조하십시오.
- **Nexmo SMS 게이트웨이 지원이 더 이상 사용되지 않습니다.** Nexmo SMS 지원은 기본적으로 **True**로 설정된 `deprecate.carrier.sms.gateway`이라는 서버 속성을 추가하여 더 이상 사용되지 않도록 설정되었습니다. Nexmo SMS는 셀프 도움말 포털에서도 더 이상 사용되지 않습니다. 자세한 내용은 알림을 참조하십시오.
- **Google의 API 사용 중단.** Google은 XenMobile Server에서 앱 카테고리 및 라이선스에 사용되는 여러 API를 더 이상 사용하지 않습니다. 다음 변경 사항이 적용됩니다.
  - 이제 승인하는 대신 추가할 앱을 선택합니다. 관리형 앱 스토어 앱을 참조하십시오.
  - 이제 앱을 카테고리 대신 컬렉션으로 구성합니다. 앱 구성을 참조하십시오.
  - 더 이상 사용자로부터 앱 라이선스를 분리할 수 없습니다. 앱 추가를 참조하십시오.

- **Android Enterprise 관리형 앱을 자동으로 업데이트하는 우선순위 구성.** Android Enterprise 관리형 앱이 낮은 우선순위로 자동으로 업데이트되는지 또는 높은 우선순위로 자동으로 업데이트되는지 지정합니다. 자동 업데이트를 연기할 수도 있습니다. 자세한 내용은 관리형 앱 장치 정책 자동 업데이트를 참조하십시오.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

- 일부 Android 실행 장치에서는 일부 공개 앱이 Google Play에서 제공되지 않을 때 Secure Hub에 액세스할 수 없습니다.
- 특정 macOS 장치에서는 SSL 인증서 갱신 후 설치된 프로필 및 인증서가 자동으로 제거됩니다.
- XenMobile Server 콘솔에서 이름에 **/** 기호가 있는 제한 장치 정책을 편집할 수 없습니다.
- 릴리스된 DEP 장치가 XenMobile Server 콘솔에 계속 표시됩니다.
- Secure Hub Store에 액세스할 수 없습니다. 다음 오류가 발생합니다. **로그온이 만료되었습니다. 계속하려면 다시 로그온하십시오.**

XenMobile Server 10.14 롤링 패치 6 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 6의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

새로운 제한 정책이 추가되었습니다. 제한 정책에 **작업 프로필에서 복사 및 붙여넣기 허용** 및 **개인 프로필에서 데이터 공유 허용**이 추가되었습니다. 개인 프로필에서 작업 프로필로 복사, 붙여넣기 및 가져오기를 제한하려면 이러한 정책을 **OFF**로 설정하십시오. 자세한 내용은 제한 장치 정책을 참조하십시오.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

- XenMobile® Server에서 일부 VPP 앱의 올바른 버전이 자동으로 업데이트되지 않습니다.
- XenMobile Server 버전 10.14에서 특정 Active Directory 사용자를 삭제할 수 없습니다.
- iOS 15를 실행하는 장치의 새 등록 시 연결 유형이 **AlwaysOn IKEv2 Dual Configuration**으로 설정된 경우 VPN 정책 배포가 실패합니다.

XenMobile Server 10.14 롤링 패치 5 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 5의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

- **Google 애널리틱스 사용**. XenMobile Server에서 Google 애널리틱스를 사용하려면 서버 속성 **xms.ga.enabled**의 값을 **True**로 설정합니다. 기본값은 **True**입니다.
- **Secure Hub APNs 인증서 갱신.** XenMobile Server 10.14용 Secure Hub Apple Push Notification Service(APNs) 인증서는 May 7, 2022에 만료됩니다. 이 업데이트는 April 8, 2023에 만료되는 Secure Hub APNs 인증서를 갱신합니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

- XenMobile® Server에서 장치 인증서 발급자 CA는 장치에서 CA 갱신 후 업데이트되지 않습니다.
- 일부 장치에는 SQL 데이터베이스에 두 개의 인증서 항목이 있어 오류가 발생합니다.
- XenMobile Server 버전 10.14에서는 프로비저닝 프로필 장치 정책을 편집할 수 없습니다.
- XenMobile Server에서 ShareFile Enterprise에서 Connectors로 변경할 때 GUI가 배달 그룹 아래에서 업데이트되지 않습니다.

XenMobile Server 10.14 롤링 패치 4 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 4의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

WSDL 서비스 활성화. XenMobile Server에서 WSDL 서비스를 활성화하려면 서버 속성 `wsdl.service.enabled`의 값을 **True**로 설정합니다. ActiveSync 게이트웨이 커넥터를 사용하는 경우 필요합니다. 기본값은 **False**입니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

- 일부 Android Enterprise 장치에서 배달 그룹 및 할당된 정책 또는 앱이 간헐적으로 적용되지 않습니다.
- XenMobile Server 버전 10.13에서는 스토리지 영역 커넥터만 사용하여 스토리지 영역 컨트롤러를 연결하고 구성할 수 없습니다.
- MDM 전용 모드에 등록된 iOS 장치에서 Secure Hub가 App Store에서 연 브라우저를 통해 앱을 추가할 수 없습니다. 다음 오류가 발생합니다: **로그인이 만료되었습니다. 계속하려면 다시 로그인하십시오.**
- XenMobile Server 버전 10.13 RP1 이상에서 SNMP 모니터링의 XenMobile 노드 간 연결 트랩이 작동하지 않습니다.

- XenMobile® Server에서 W-SU 시간대에 잘못된 시간이 표시됩니다.

XenMobile Server 10.14 롤링 패치 3 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 3의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

이 릴리스에는 버그 수정이 포함되어 있습니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

XenMobile Server 10.14 롤링 패치 2 릴리스용 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 2의 개선 사항, 해결된 문제 및 알려진 문제에 대해 설명합니다.

XenMobile Server 10.14.0의 이전 롤링 패치에 대한 자세한 내용은 롤링 패치 릴리스 정보를 참조하십시오.

해결된 문제

XenMobile® Server에서 피크 시간 동안 서버 노드에서 높은 CPU 사용률이 관찰됩니다.

XenMobile Server 10.14 롤링 패치 1 릴리스에 대한 릴리스 정보

이 릴리스 정보는 XenMobile Server 10.14 롤링 패치 1의 향상된 기능, 해결된 문제 및 알려진 문제에 대해 설명합니다.

새로운 기능

- **Windows 11 장치 지원.** 이제 XenMobile을 사용하여 Windows 11 장치를 관리할 수 있습니다. 자세한 내용은 운영 체제 지원 목록을 참조하십시오.
- **macOS용 연결 모드 및 네트워크 우선 순위 구성.** Wi-Fi 장치 정책에서 macOS 장치에 대한 **연결 모드** 설정을 활성화하여 사용자가 네트워크에 연결하는 방법을 선택합니다. 장치는 시스템 자격 증명 또는 로그인 창에 입력된 자격 증명을 사용하여 사용자를 인증할 수 있습니다. 여러 네트워크가 있는 경우 **우선 순위** 필드에 숫자를 입력하여 네트워크 연결의 우선 순위를 설정합니다. 장치는 가장 낮은 번호의 네트워크를 선택합니다. 자세한 내용은 Wi-Fi 장치 정책의 macOS 설정을 참조하십시오.
- Google에서 Android Enterprise 장치의 그룹 라이선스 지원을 중단함에 따라 XenMobile Server는 그룹 라이선스를 Google과 동기화할 수 없습니다. 자세한 내용은 이 문서를 참조하십시오.

알려진 문제

macOS 11 이하에서 macOS 12로 업그레이드된 등록된 장치 또는 macOS 12에 새로 등록된 장치는 장치의 **시스템 환경설정 > 프로필** 아래에 "확인되지 않음"으로 표시될 수 있습니다. 자세한 내용 및 해결 방법은 지원 문서를 참조하십시오.

해결된 문제

- iOS 15 또는 macOS 12 장치를 등록한 후 MDM 구성 프로필이 **확인되지 않음**으로 표시됩니다.
- XenMobile® Server 콘솔에서 앱 설정을 수정하여 모든 플랫폼을 지우고 저장하면 해당 앱이 **구성 > 앱**에 나열되지 않습니다.
- Android Enterprise 플랫폼에서 Citrix® 시작 관리자를 종료할 수 없습니다. 다음 오류가 발생합니다: **잘못된 암호**.
- XenMobile Server 버전 10.14에서는 **iOS 및 macOS 프로필 가져오기** 정책을 편집할 수 없습니다.

XenMobile Server 10.16의 새로운 기능

Citrix ADC에서 더 이상 사용되지 않는 Classic 정책에 대한 지속적인 지원

Citrix는 최근 Citrix ADC 12.0 빌드 56.20부터 일부 Classic 정책 기반 기능의 사용 중단을 발표했습니다. Citrix ADC 사용 중단 공지는 Citrix Gateway와 기존 XenMobile Server 통합에 영향을 미치지 않습니다. XenMobile Server는 Classic 정책을 계속 지원하며 별도의 조치가 필요하지 않습니다.

사용 중단 공지

단계적으로 중단되는 Citrix XenMobile 기능에 대한 사전 공지는 사용 중단을 참조하십시오.

엔드포인트를 iOS 14.5로 업그레이드하기 전에

어떤 엔드포인트든 iOS 14.5로 업그레이드하기 전에 Citrix는 앱 충돌을 완화하기 위해 다음 작업을 수행할 것을 권장합니다.

- Citrix Secure Mail 및 Secure Web을 21.2.X 이상으로 업그레이드합니다. MDX 또는 엔터프라이즈 앱 업그레이드를 참조하십시오.
- MDX Toolkit을 사용하는 경우 모든 타사 iOS 애플리케이션을 MDX Toolkit 21.3.X 이상으로 래핑합니다. 최신 버전은 MDX Toolkit 다운로드 페이지에서 확인하십시오.

온프레미스 Citrix ADC를 업그레이드하기 전에

온프레미스 Citrix ADC를 특정 버전으로 업그레이드하면 단일 Sign-On 오류가 발생할 수 있습니다. 브라우저에서 **회사 직원 Sign-in** 옵션을 사용하여 Citrix Files 또는 ShareFile 도메인 URL에 단일 Sign-On하면 오류가 발생합니다. 사용자가 Sign-in할 수 없습니다.

이 문제를 해결하려면: Citrix Gateway의 ADC CLI에서 다음 명령을 아직 실행하지 않았다면, 전역 SSO를 활성화하기 위해 실행하십시오.

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

자세한 내용은 다음을 참조하십시오.

- Citrix ADC 릴리스(기능 단계) 13.1 빌드 33.52
- 영향을 받는 SSO 구성

해결 방법을 완료하면 사용자는 브라우저에서 회사 직원 로그인 옵션을 사용하여 SSO로 Citrix Files 또는 ShareFile 도메인 URL에 인증할 수 있습니다.

XenMobile 10.16(온프레미스)으로 업그레이드하기 전

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 시스템 요구 사항 및 호환성 및 XenMobile 호환성을 참조하십시오.

1. 업그레이드할 XenMobile® Server를 실행하는 가상 머신의 RAM이 8GB 미만인 경우 RAM을 최소 8GB로 늘리는 것이 좋습니다.
2. XenMobile Server 10.16의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.17.2.0 Build 47000 이상으로 업데이트하십시오.

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

   > **참고:**
   >
   > XenMobile 10.16의 고객 성공 서비스 날짜(이전 Subscription Advantage 날짜)는 November 15, 2022입니다. Citrix 라이선스의 고객 성공 서비스 날짜는 이 날짜보다 늦어야 합니다.
   >
   > 라이선스 서버에서 라이선스 옆에 있는 날짜를 볼 수 있습니다. 최신 버전의 XenMobile을 이전 라이선스 서버 환경에 연결하면 연결 확인에 실패하고 라이선스 서버를 구성할 수 없습니다.
   >
   > 라이선스 날짜를 갱신하려면 Citrix Portal에서 최신 라이선스 파일을 다운로드하여 라이선스 서버에 업로드하십시오. 고객 성공 서비스를 참조하십시오.

   라이선스 활성화 서비스(LAS)는 Citrix 제품군 전체의 제품 활성화를 위한 차세대 기술입니다. 10.15 롤링 패치 13 이상 롤링 패치에서 라이선스 활성화 서비스가 활성화된 경우 10.16.0.48로 직접 업그레이드하면 라이선스 활성화 서비스 구성이 재설정됩니다. 라이선스 활성화 서비스를 재구성할 수 있는 버전 10.16 롤링 패치 7 이상 10.16 롤링 패치를 계속 적용하십시오. 기존 장치는 영향을 받지 않습니다.
3. 클러스터 환경의 경우: iOS 11 이상을 실행하는 장치에 대한 iOS 정책 및 앱 배포에는 다음 요구 사항이 있습니다.

- Citrix Gateway가 SSL 지속성을 위해 구성된 경우 모든 XenMobile Server 노드에서 포트 80을 열어야 합니다.

4. 권장 사항: XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 만드십시오. 또한 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하면 백업을 완료하여 복구할 수 있습니다.

업그레이드하려면

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

XenMobile 10.15.x 또는 10.14.x에서 XenMobile 10.16으로 직접 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 바이너리를 다운로드하십시오. Citrix 다운로드 페이지로 이동합니다. **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **Download File**을 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 **릴리스 관리** 페이지를 사용하십시오. 릴리스 관리 페이지를 사용하여 업그레이드하려면을 참조하십시오.

업그레이드 후

아웃바운드 연결과 관련된 기능이 작동을 멈추고 연결 구성을 변경하지 않은 경우, XenMobile Server 로그에서 다음과 같은 오류를 확인하십시오: "VPP 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다".

- 인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 확인을 비활성화해야 함을 의미합니다.
- 기본적으로 Microsoft PKI 서버를 제외한 아웃바운드 연결에서는 호스트 이름 확인이 활성화되어 있습니다.
- 호스트 이름 확인으로 인해 배포가 중단되는 경우, 서버 속성 `disable.hostname.verification`을 `true`(으)로 변경하십시오. 이 속성의 기본값은 `false`입니다.

플랫폼 업데이트

- **Android 14 지원:** XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 Android Enterprise 장치 업데이트를 Android 14로 지원합니다. 보안 및 개인 정보 보호 이점에 대한 자세한 내용은 Android 설명서를 참조하십시오.

- **iOS 17 지원:** XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 iOS 17과 호환되지만, 현재 iOS 17의 새로운 기능은 지원하지 않습니다.
- **macOS 14 지원:** XenMobile Server 및 Citrix Mobile 생산성 앱은 이제 macOS 14와 호환되지만, 현재 macOS 14의 새로운 기능은 지원하지 않습니다.

장치 및 앱 보고서 액세스

이전에는 **장치 및 앱** 보고서 페이지에 역할 기반 액세스 제어(RBAC)가 적용되었더라도 사용자 그룹과 관계없이 모든 사용자의 모든 장치 및 앱 정보가 표시되었습니다.

XenMobile Server 10.16 릴리스부터 **장치 및 앱** 보고서 페이지에는 RBAC 역할이 관리할 권한이 있는 **특정 사용자 그룹**에 정의된 사용자 그룹에 특정한 장치 및 앱이 표시됩니다. RBAC를 사용하여 역할을 구성하는 방법에 대한 자세한 내용은 RBAC를 사용하여 역할 구성을 참조하십시오.

Android Enterprise용 802.1x 설정에 새로운 필수 필드 “도메인” 추가

802.1x EAP 인증 유형에 대해 Android Enterprise 플랫폼 네트워크 정책 설정 페이지에 새로운 필드 **도메인**이 추가되었습니다. 자세한 내용은 Android Enterprise용 802.1x 설정을 참조하십시오.

iOS용 제한 장치 정책 및 Exchange 장치 정책에 새로운 설정 추가

- iOS용 Exchange 장치 정책에 새로운 설정 **메일 드롭 허용**이 추가되었습니다. 자세한 내용은 Exchange 장치 정책 - iOS 설정을 참조하십시오.
- iOS용 제한 장치 정책에 다음 새로운 설정이 추가되었습니다:
  - 페어링되지 않은 장치에 의한 복구 부팅 허용
  - 신속 보안 대응 설치
  - 신속 보안 대응 제거
  - 메일 개인 정보 보호 허용
  - NFC
  - 앱 클립 허용
  - Apple 개인 맞춤형 광고 허용
  - 자동 잠금 해제

자세한 내용은 제한 장치 정책 - iOS 설정을 참조하십시오.

iOS용 Exchange 장치 정책 설정에 새로운 OAuth 로그인 URL 및 OAuth 토큰 요청 URL 필드 추가

XenMobile Server 10.16 릴리스부터 **Exchange 정책** > **iOS** > **OAuth 사용** 라디오 버튼 아래에 **OAuth 로그인 URL** 및 **OAuth 토큰 요청 URL** 필드가 추가되었습니다. 자세한 내용은 Exchange 장치 정책을 참조하십시오.

새로운 Knox Platform for Enterprise Key 장치 정책 추가

Knox Platform for Enterprise Key라는 새 장치 정책이 추가되었습니다. 이 정책을 사용하면 필요한 Samsung Knox Platform for Enterprise(KPE) 라이선스 정보를 제공하고 KPE 라이선스를 사용하여 Samsung 장치의 보안을 강화할 수 있습니다. 자세한 내용은 Knox Platform for Enterprise Key 장치 정책을 참조하십시오.

새 딜리버리 그룹의 기반으로 사용할 딜리버리 그룹 복제

이 기능을 사용하면 여러 정책, 앱 및 작업을 포함하는 복잡한 딜리버리 그룹을 복사할 수 있습니다. 그런 다음 등록 프로필 또는 새로운 Active Directory 사용자 세트를 추가하는 등 복사본을 편집할 수 있습니다. 자세한 내용은 딜리버리 그룹 복제를 참조하십시오.

공유 iPad용 Apple Business Manager 지원

XenMobile Server 10.16 릴리스부터 공유 iPad는 XenMobile Server와 함께 Apple Business Manager(ABM)를 지원합니다. 이를 통해 ABM 계정을 사용하여 공유 iPad에 로그인하고 사용할 수 있습니다. 자세한 내용은 공유 iPad 구성을 참조하십시오.

공유 iPad용 '모든 사용자 삭제'라는 새 보안 작업 추가

XenMobile Server 10.16 릴리스부터 XenMobile Server의 공유 iPad에 **모든 사용자 삭제**라는 새 보안 작업이 추가되었습니다. 이를 통해 장치의 모든 사용자를 삭제할 수 있습니다. 자세한 내용은 공유 iPad용 보안 작업을 참조하십시오.

앱 속성 장치 정책, 새로운 iOS 앱 속성 지원

이제 iOS 장치에 설치된 앱에 대해 다음 속성을 지정할 수 있습니다.

- **제거 가능한 앱:** 관리되는 앱인 경우 사용자가 앱을 제거할 수 있는지 여부를 지정합니다.
- **연결된 도메인 직접 다운로드 활성화:** 앱이 도메인에서 직접 주장된 사이트 연결 확인을 수행할 수 있는지 여부를 지정합니다.

- **연결된 도메인:** 앱에 추가할 연결된 도메인을 지정합니다.

자세한 내용은 앱 속성 장치 정책을 참조하십시오.

iOS용 동기화된 Exchange 서비스 동기화 또는 재정의 지원

XenMobile Server 10.16 릴리스부터 관련 설정을 활성화하여 iOS용으로 동기화된 다음 Exchange 서비스를 동기화할지 또는 재정의할지 선택할 수 있습니다.

- 캘린더
- 연락처
- 메일
- 메모
- 미리 알림

자세한 내용은 Exchange 장치 정책을 참조하십시오.

OS 업데이트 제어 장치 정책을 시스템 기본값으로 재설정 지원

XenMobile Server 10.16 릴리스부터 Android Enterprise의 **OS 업데이트 제어** 아래에 있는 **시스템 업데이트 정책** 드롭다운 목록에 새로운 값 **기본값**이 추가되었습니다. 이 기능을 사용하면 시스템 업데이트 정책을 시스템 기본값으로 재설정할 수 있습니다. 자세한 내용은 OS 업데이트 제어 장치 정책을 참조하십시오.

iOS용 OS 업데이트 정책에 "OS 업데이트 버전" 새 옵션 추가

iOS 플랫폼의 **OS 업데이트 정책**에서 **OS 업데이트 빈도** 필드 다음에 새로운 옵션 **OS 업데이트 버전**이 추가되었습니다. 이 옵션을 사용하면 감독되는 iOS 장치를 업데이트하는 데 사용할 OS 버전을 지정할 수 있습니다. 자세한 내용은 iOS 설정을 참조하십시오.

네트워크 액세스 제어

NAC(네트워크 액세스 제어) 솔루션을 사용하여 Android 및 Apple 장치에 대한 XenMobile 장치 보안 평가를 확장합니다. NAC 솔루션은 XenMobile 보안 평가를 사용하여 인증 결정을 용이하게 하고 처리합니다. NAC 어플라이언스를 구성하면 XenMobile에서 구성한 장치 정책 및 NAC 필터가 적용됩니다. 자세한 내용은 네트워크 액세스 제어를 참조하십시오.

XenMobile Server에서 혼합 라이선스 유형 지원

이 기능을 사용하면 XenMobile Server 또는 Citrix Licensing Server를 사용하여 다양한 XenMobile 라이선스 유형 및 에디션을 활성화할 수 있습니다. 자세한 내용은 다른 라이선스 활성화를 참조하십시오.

iOS 장치에서 eSIM 지원

XenMobile Server에는 `ios.esim.support`이라는 새 속성이 있습니다. 이 속성을 사용하면 XenMobile Server가 iOS 장치에서 eSIM 정보를 가져와 사용자 인터페이스에 eSIM 관련 장치 속성을 표시할 수 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 서버 속성를 참조하십시오.

Android Enterprise 플랫폼용 VPN 장치 정책

이전에는 **XenMobile 옵션 장치 정책**에서 **Always-On VPN 사용** 옵션을 활성화하여 Android Enterprise에서 실행되는 장치에 VPN 서비스를 활성화할 수 있었습니다.

XenMobile Server 10.16부터는 **VPN 장치 정책**에서 **Always-On VPN 사용** 옵션을 활성화하여 Android Enterprise에서 실행되는 장치에 Always-On VPN 서비스를 활성화할 수 있습니다. 이전 릴리스에서 **XenMobile 옵션 장치 정책**의 **Always-On VPN 사용** 옵션을 이미 활성화한 경우, 새로 등록된 장치에 대해 **VPN 장치 정책**에서 동일한 옵션을 다시 활성화해야 합니다. 이미 등록된 장치에는 변경 사항이 필요하지 않습니다. 자세한 내용은 Android Enterprise 플랫폼용 VPN 장치 정책을 참조하십시오.

iOS용 Webclip 정책 설정에 새 필드 Profile scope 추가됨

iOS 장치의 Webclip 장치 정책에 있는 **정책 설정** 아래에 **프로필 범위**라는 새 필드가 추가되었습니다. 이를 통해 정책이 사용자에게 적용되는지 시스템에 적용되는지 선택할 수 있습니다. 자세한 내용은 Webclip 장치 정책 - iOS 설정을 참조하십시오.

Secure Hub APNs 인증서 갱신

이 업데이트는 XenMobile Server 10.16용 Secure Hub Apple Push Notification Service(APNs) 인증서를 February 9, 2025에 만료되는 새 인증서로 자동 갱신합니다.

REST API를 사용하여 공용 스토어 앱의 배포 규칙 업데이트

새 공용 스토어 앱 추가 및 **공용 스토어 앱 업데이트** REST API에 **규칙**이라는 새 필드가 추가되었습니다. 이를 통해 공용 스토어 앱의 배포 규칙을 업데이트할 수 있습니다. 자세한 내용은 공용 REST API 설명서를 참조하십시오.

iOS에서 선택적 앱 자동 업데이트 지원

XenMobile Server 10.16부터 `apple.ios.optional_app_update`이라는 새 서버 속성이 추가되었습니다. 이 속성을 사용하면 iOS에서 선택적 앱을 자동 업데이트할 수 있습니다.
`apple.ios.optional_app_update`의 기본값은 **False**로 설정됩니다. 자세한 내용은 서버 속성를 참조하십시오.

선택적 볼륨 구매 앱의 자동 업데이트에 대한 자세한 내용은 앱 업데이트 확인을 참조하십시오.

macOS 장치에서 엔터프라이즈 앱 지원

XenMobile Server에는 macOS를 실행하는 장치에서 엔터프라이즈 앱을 지원할 수 있도록 하는 새로운 속성 `mac.app.push`이(가) 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 서버 속성을(를) 참조하십시오.

총 앱 배포 시도 및 상위 100개 설치된 앱에 대한 장치 보고서 개선

XenMobile Server 콘솔의 분석 -> 보고서에서 총 앱 배포 시도에 **운영 체제 버전** 및 **장치 모델**이라는 두 개의 새 열이 추가되었으며, 각 플랫폼에 설치된 상위 100개 앱을 표시하는 새 장치 보고서인 **상위 100개 설치된 앱**이 추가되었습니다. 자세한 내용은 보고서를(을) 참조하십시오.

XenMobile Server에는 위에서 언급한 새로운 장치 보고서 개선 사항을 활성화하는 새로운 속성 `device.report.enhancement.enabled`이(가) 있습니다. 이 속성의 기본값은 **True**입니다. 자세한 내용은 서버 속성을(를) 참조하십시오.

장치 등록에서 정렬 및 필터링 현대화

XenMobile Server의 목록 보기는 현재 탐색하기 어렵고 사용자 친화적이지 않습니다. 필터링 및 정렬 옵션을 열 머리글로 이동하면 사용자가 이러한 기능을 결합하여 필요한 데이터를 훨씬 더 간단하고 직관적으로 찾을 수 있습니다.

사용 중단 및 제거

XenMobile Analyzer Tool 사용 중단: 빈번하고 안정적인 릴리스 주기에 따라 XenMobile Analyzer Tool은 더 이상 필요하지 않습니다. Citrix는 March 31, 2023부터 이 서비스를 중단했습니다. Citrix는 Citrix XenMobile 콘솔 또는 Citrix Gateway 내에서 사용할 수 있는 연결 확인 기능을 사용하는 것이 좋습니다. 자세한 내용은 연결 확인을 참조하십시오.

XenMobile Server 10.15의 새로운 기능

XenMobile Server 10.15 (PDF 다운로드)

Citrix ADC에서 더 이상 사용되지 않는 Classic 정책에 대한 지속적인 지원

Citrix는 최근 Citrix ADC 12.0 빌드 56.20부터 일부 Classic 정책 기반 기능의 사용 중단을 발표했습니다. Citrix ADC 사용 중단 알림은 Citrix Gateway와 기존 XenMobile Server 통합에 영향을 미치지 않습니다. XenMobile Server는 Classic 정책을 계속 지원하며 별도의 조치가 필요하지 않습니다.

사용 중단 공지

단계적으로 중단되는 Citrix XenMobile 기능에 대한 사전 공지는 사용 중단을 참조하십시오.

iOS 14.5로 엔드포인트를 업그레이드하기 전에

iOS 14.5로 엔드포인트를 업그레이드하기 전에 Citrix는 앱 충돌을 완화하기 위해 다음 작업을 수행할 것을 권장합니다.

- Citrix Secure Mail 및 Secure Web을 21.2.X 이상으로 업그레이드하십시오. MDX 또는 엔터프라이즈 앱 업그레이드를 참조하십시오.
- MDX Toolkit을 사용하는 경우 모든 타사 iOS 애플리케이션을 MDX Toolkit 21.3.X 이상으로 래핑하십시오. 최신 버전은 MDX Toolkit 다운로드 페이지에서 확인하십시오.

온프레미스 Citrix ADC를 업그레이드하기 전에

온프레미스 Citrix ADC를 특정 버전으로 업그레이드하면 단일 Sign-On 오류가 발생할 수 있습니다. 브라우저에서 **회사 직원 로그인** 옵션을 사용하여 Citrix Files 또는 ShareFile 도메인 URL에 단일 Sign-On하면 오류가 발생합니다. 사용자가 로그인할 수 없습니다.

이 문제를 해결하려면: Citrix Gateway의 ADC CLI에서 다음 명령을 아직 실행하지 않았다면, 전역 SSO를 활성화하기 위해 이 명령을 실행하십시오.

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

자세한 내용은 다음을 참조하십시오.

- Citrix ADC 릴리스(기능 단계) 13.1 빌드 33.52
- 영향을 받는 SSO 구성

해결 방법을 완료한 후 사용자는 브라우저에서 회사 직원 로그인 옵션을 사용하여 SSO로 Citrix Files 또는 ShareFile 도메인 URL에 인증할 수 있습니다.

XenMobile 10.15 (온프레미스)로 업그레이드하기 전에

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 시스템 요구 사항 및 호환성 및 XenMobile 호환성을 참조하십시오.

1. 업그레이드할 XenMobile® Server를 실행하는 가상 머신의 RAM이 8GB 미만인 경우 RAM을 최소 8GB로 늘리는 것이 좋습니다.
2. XenMobile Server 10.15의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.17 이상으로 업데이트하십시오.

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

   > **참고:**
   >
   > XenMobile 10.15의 Customer Success Services 날짜(이전 Subscription Advantage 날짜)는 November 15, 2022입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 늦어야 합니다.
   >
   > License Server에서 라이선스 옆에 있는 날짜를 확인할 수 있습니다. 최신 버전의 XenMobile을 이전 License Server 환경에 연결하면 연결 확인에 실패하고 License Server를 구성할 수 없습니다.
   >
   > 라이선스 날짜를 갱신하려면 Citrix Portal에서 최신 라이선스 파일을 다운로드하여 라이선스 서버에 업로드하십시오. Customer Success Services를 참조하십시오.
3. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 대한 iOS 정책 및 앱 배포에는 다음 요구 사항이 있습니다. Citrix Gateway가 SSL 지속성을 위해 구성된 경우 모든 XenMobile Server 노드에서 포트 80을 열어야 합니다.
4. 권장 사항: XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 만드십시오. 또한 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하면 백업을 통해 복구할 수 있습니다.

업그레이드하려면

이 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 XenMobile 10.15로 직접 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 바이너리를 다운로드하십시오. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **Download File**을 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 **릴리스 관리** 페이지를 사용하십시오. 릴리스 관리 페이지를 사용하여 업그레이드하려면을 참조하십시오.

업그레이드 후

아웃바운드 연결과 관련된 기능이 작동을 멈추고 연결 구성을 변경하지 않은 경우, XenMobile Server 로그에서 다음과 같은 오류를 확인하십시오. "VPP 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다".

- 인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 확인을 비활성화해야 함을 의미합니다.
- 기본적으로 Microsoft PKI 서버를 제외한 아웃바운드 연결에서는 호스트 이름 확인이 활성화되어 있습니다.
- 호스트 이름 확인으로 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 Mobile 생산성 앱은 iOS 16과 호환되지만, 현재 iOS 16의 새로운 기능은 지원하지 않습니다.

Android 13 지원. XenMobile Server는 Android Enterprise 장치의 Android 13 업데이트를 지원합니다. 보안 및 개인 정보 보호 이점에 대한 요약은 Android 설명서를 참조하십시오.

Windows 11 장치 지원. 이제 XenMobile을 사용하여 Windows 11 장치를 관리할 수 있습니다. 자세한 내용은 운영 체제 지원 목록을 참조하십시오.

macOS의 연결 모드 및 네트워크 우선순위 구성

Wi-Fi 장치 정책에서 macOS 장치의 **연결 모드** 설정을 활성화하여 사용자가 네트워크에 연결하는 방법을 선택합니다. 장치는 시스템 자격 증명 또는 로그인 창에 입력된 자격 증명을 사용하여 사용자를 인증할 수 있습니다. 여러 네트워크가 있는 경우 *우선순위* 필드에 숫자를 입력하여 네트워크 연결의 우선순위를 설정합니다. 장치는 가장 낮은 숫자의 네트워크를 선택합니다. 자세한 내용은 Wi-Fi 장치 정책의 macOS 설정을 참조하십시오.

Android Enterprise 관리 앱을 자동으로 업데이트하기 위한 우선순위 구성

Android Enterprise 관리 앱이 낮은 우선순위로 자동으로 업데이트될지 높은 우선순위로 자동으로 업데이트될지 지정합니다. 자동 업데이트를 연기할 수도 있습니다. 자세한 내용은 관리 앱 자동 업데이트 장치 정책을 참조하십시오.

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

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

XenMobile Server 버전 10.15부터 하드웨어 가상화 모드(HVM)가 지원됩니다. 새로운 XenMobile Server 설치의 경우 citrix.com에서 HVM xva 이미지를 다운로드하십시오. 기존 XenMobile Server 환경의 경우 PV에서 HVM 게스트로 마이그레이션하는 단계를 따르십시오. HVM 게스트 이미지는 XenMobile Server 버전 10.15 이상에서 citrix.com에서 사용할 수 있습니다.

전제 조건

- 클러스터를 사용하도록 설정하고 데이터베이스가 원격에 있는지 확인합니다.
- 백업으로 이전 PV 노드를 유지하거나 스냅샷을 저장합니다. PV 노드가 XenMobile Server 버전 10.14 또는 10.13에 있는 경우 데이터베이스도 백업하십시오.
- 마이그레이션 전에 새 HVM 노드로 전송되지 않는 이전 PV 노드에서 지원 번들을 다운로드하십시오.

마이그레이션 단계

1. XenMobile Server 10.15 HVM xva 이미지를 다운로드합니다.
2. 이전 PV 게스트 노드를 종료합니다.
3. Citrix Hypervisor에서 새 HVM 노드를 부팅합니다.
4. XenMobile Server 10.15 노드를 이전 노드와 동일한 데이터베이스 설정으로 구성하고, 기존 클러스터에서 서버의 PKI 키 저장소 암호를 함께 구성합니다.
5. 필요한 경우 Citrix Gateway 설정을 업데이트합니다.

> **참고:**
>
> 마이그레이션 중에 오류가 발생하면 동일한 버전의 데이터베이스로 이전 PV 노드를 부팅하십시오.

중요:

XenMobile PV 게스트에 대해 `/opt/xensource/bin/pv2hvm` 명령을 실행하지 마십시오. VM 부팅에 실패할 수 있습니다.

Google Analytics 사용 설정

XenMobile Server에서 Google Analytics를 사용하려면 서버 속성 *xms.ga.enabled*의 값을 **True**로 설정합니다. 기본값은 **True**입니다.

새 제한 정책 추가됨

업무 프로필에서 복사 및 붙여넣기 허용 및 *개인 프로필에서 데이터 공유 허용*이 제한 정책에 추가되었습니다. 개인 프로필에서 업무 프로필로 복사, 붙여넣기 및 가져오기를 제한하려면 이러한 정책을 **OFF**로 설정하십시오. 자세한 내용은 제한 장치 정책을 참조하십시오.

Secure Hub APNs 인증서 갱신

XenMobile Server용 Secure Hub Apple 푸시 알림 서비스(APNs) 인증서는 May 7, 2022에 만료되었습니다. 이 업데이트는 April 8, 2023에 만료될 Secure Hub APNs 인증서를 갱신합니다.

사용 중단 및 제거

- **Google의 API 사용 중단.** Google은 XenMobile Server에서 앱 카테고리 및 라이선스에 사용되는 여러 API를 사용 중단하고 있습니다. 다음 변경 사항이 적용됩니다.
  - 이제 승인하는 대신 추가할 앱을 선택합니다. 관리형 앱 스토어 앱을 참조하십시오.
  - 이제 카테고리 대신 컬렉션으로 앱을 구성합니다. 앱 구성을 참조하십시오.
  - 더 이상 사용자로부터 앱 라이선스를 분리할 수 없습니다. 앱 추가를 참조하십시오.
- **Windows 정보 보호 정책에 대한 지원 중단.** Windows 공지에 따라 XenMobile Server는 Windows 정보 보호(WIP)에 대한 지원을 중단했습니다. WIP 지원은 기본적으로 *True*로 설정된 *windows.wip.deprecation*이라는 서버 속성을 추가하여 중단되었습니다. 자세한 내용은 서버 속성을 참조하십시오.
- **모바일 서비스 공급자(MSP) 인터페이스에 대한 지원 중단.** MSP 지원은 콘솔에서 MSP 인터페이스를 제거하는 *deprecate.mobile.service.provider*라는 새 서버 속성을 추가하여 중단되었으며, 이 속성은 기본적으로 *True*로 설정됩니다. 자세한 내용은 서버 속성을 참조하십시오.
- **Nexmo SMS 게이트웨이 지원이 더 이상 사용되지 않습니다.** 기본적으로 *True*로 설정된 *deprecate.carrier.sms.gateway*라는 새 서버 속성을 추가하여 Nexmo SMS 지원이 더 이상 사용되지

않도록 설정되었습니다. Nexmo SMS는 셀프 도움말 포털에서도 더 이상 사용되지 않습니다. 자세한 내용은 알림을 참조하십시오.

- **Windows 10 장치에 대한 *WiFi Sense 핫스팟에 자동 연결 허용* 제한 정책 지원이 더 이상 사용되지 않습니다.** 자세한 내용은 Windows 데스크톱/태블릿 설정을 참조하십시오.
- **등록 초대 설정.** 장치 IMEI, 일련 번호 및 UDID를 사용하여 등록 초대를 생성하는 기능에 대한 지원이 더 이상 사용되지 않습니다. 등록 초대를 생성할 때 XenMobile Server 콘솔의 **관리 > 등록 초대**에서 사용 가능한 설정을 구성하십시오.
- **다음 기능에 대한 지원이 제거되었습니다.**
  - 안드로이드 - 아마존
  - 안드로이드 - 소니 및 에이치티씨
  - Zebra 장치의 사용자 지정 XML
  - 파생 자격 증명
  - 일반, DigiCert 관리 및 Entrust 어댑터 PKI 엔터티.
  - 높은 보안 등록 모드
  - RBAC 역할 - 공유 및 COSU 장치 등록자
  - 삼성 세이프 및 넉스
  - SEAMS
  - 윈도우 폰 장치

  자세한 내용은 더 이상 사용되지 않음을 참조하십시오.

XenMobile Server 10.14의 새로운 기능

XenMobile Server 10.14 (PDF 다운로드)

Citrix ADC에서 더 이상 사용되지 않는 Classic 정책에 대한 지속적인 지원

Citrix는 최근 Citrix ADC 12.0 빌드 56.20부터 일부 Classic 정책 기반 기능의 사용 중단을 발표했습니다. Citrix ADC 사용 중단 알림은 Citrix Gateway와 기존 XenMobile Server 통합에 영향을 미치지 않습니다. XenMobile Server는 Classic 정책을 계속 지원하며 별도의 조치가 필요하지 않습니다.

사용 중단 알림

단계적으로 중단되는 Citrix XenMobile 기능에 대한 사전 알림은 사용 중단을 참조하십시오.

엔드포인트를 iOS 14.5로 업그레이드하기 전에

엔드포인트를 iOS 14.5로 업그레이드하기 전에 앱 충돌을 완화하기 위해 다음 작업을 수행하는 것이 좋습니다.

- Citrix Secure Mail 및 Secure Web을 21.2.X 이상으로 업그레이드하십시오. MDX 또는 엔터프라이즈 앱 업그레이드를 참조하십시오.
- MDX Toolkit을 사용하는 경우 모든 타사 iOS 애플리케이션을 MDX Toolkit 21.3.X 이상으로 래핑하십시오. 최신 버전은 MDX Toolkit 다운로드 페이지에서 확인하십시오.

온프레미스 Citrix ADC를 업그레이드하기 전에

온프레미스 Citrix ADC를 특정 버전으로 업그레이드하면 단일 Sign-On 오류가 발생할 수 있습니다. 브라우저에서 **회사 직원 로그인** 옵션을 사용하여 Citrix Files 또는 ShareFile 도메인 URL에 단일 Sign-On하면 오류가 발생합니다. 사용자가 로그인할 수 없습니다.

이 문제를 해결하려면: Citrix Gateway의 ADC CLI에서 다음 명령을 아직 실행하지 않았다면 실행하여 전역 SSO를 활성화하십시오.

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

자세한 내용은 다음을 참조하십시오.

- Citrix ADC 릴리스(기능 단계) 13.0 빌드 67.39/67.43
- 영향받는 SSO 구성

해결 방법을 완료하면 사용자는 회사 직원 로그인 옵션을 사용하여 브라우저에서 SSO를 통해 Citrix Files 또는 ShareFile 도메인 URL에 인증할 수 있습니다.

XenMobile 10.14 (온프레미스)로 업그레이드하기 전에

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 시스템 요구 사항 및 호환성 및 XenMobile 호환성을 참조하십시오.

1. 업그레이드할 XenMobile® Server를 실행하는 가상 머신의 RAM이 8GB 미만인 경우, RAM을 최소 8GB로 늘리는 것이 좋습니다.
2. XenMobile Server 10.14의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.16 이상으로 업데이트하십시오.

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

> **참고:**
>
> XenMobile 10.14의 Customer Success Services 날짜(이전 Subscription Advantage 날짜)는 September 15, 2021입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 늦어야 합니다.
>
> License Server에서 라이선스 옆에 있는 날짜를 볼 수 있습니다. 최신 버전의 XenMobile을 이전 License Server 환경에 연결하면 연결 확인에 실패하고 License Server를 구성할 수 없습니다.
>
> 라이선스 날짜를 갱신하려면 Citrix Portal에서 최신 라이선스 파일을 다운로드하여 Licensing Server에 업로드하십시오. Customer Success Services를 참조하십시오.

3. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 대한 iOS 정책 및 앱 배포에는 다음 요구 사항이 있습니다. Citrix Gateway가 SSL 지속성을 위해 구성된 경우 모든 XenMobile Server 노드에서 포트 80을 열어야 합니다.
4. 권장 사항: XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 만드십시오. 또한 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하면 전체 백업을 통해 복구할 수 있습니다.

업그레이드하려면

이 릴리스부터 XenMobile은 VMware ESXi 7.0을 지원합니다. ESXi 7.0을 설치하거나 업그레이드하기 전에 10.14로 업그레이드해야 합니다.

XenMobile 10.13.x 또는 10.12.x에서 XenMobile 10.14로 직접 업그레이드할 수 있습니다. 업그레이드하려면 사용 가능한 최신 바이너리를 다운로드하십시오. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **파일 다운로드**를 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 **릴리스 관리** 페이지를 사용하십시오. 릴리스 관리 페이지를 사용하여 업그레이드하려면을 참조하십시오.

업그레이드 후

발신 연결과 관련된 기능이 작동을 멈추고 연결 구성을 변경하지 않은 경우, 다음과 같은 오류에 대해 **XenMobile Server 로그**를 확인하십시오. "VPP 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다.".

- 인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 확인을 비활성화해야 함을 의미합니다.
- 기본적으로 Microsoft PKI 서버를 제외한 발신 연결에서는 호스트 이름 확인이 활성화되어 있습니다.
- 호스트 이름 확인으로 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 Mobile 생산성 앱은 iOS 15와 호환되지만, 현재 새로운 iOS 15 기능을 지원하지 않습니다.
- **Android 12:** XenMobile Server는 Android 12를 지원합니다. Google 기기 관리 API의 사용 중단이 Android 10 이상을 실행하는 기기에 미치는 영향에 대한 자세한 내용은 기기 관리에서 Android Enterprise로 마이그레이션을 참조하십시오. 또한 이 Citrix 블로그도 참조하십시오.

장치 정책

- Google 설정과 더 밀접하게 일치하고 구성을 단순화하기 위해 모든 Android Enterprise 등록 모드에 두 가지 설정을 추가했습니다.

  - **Bluetooth 공유 허용:** 선택하지 않으면 사용자는 장치에서 발신 Bluetooth 공유를 설정할 수 없습니다.
  - **앱 제거 허용:** 사용자가 관리형 Google Play 스토어 내에서 앱을 제거할 수 있도록 허용합니다.

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

  이러한 변경 사항에 대한 자세한 내용은 (/ko-kr/xenmobile/server/policies/restrictions-policy.html#android-enterprise-settings) 및 (/ko-kr/xenmobile/server/policies/control-os-updates.html)를 참조하십시오.
- Android Enterprise의 제한 설정이 명확성을 위해 재구성되었습니다. 때때로 설정 이름에 약간의 변경이 있었습니다. 재구성에 대한 자세한 내용은 (/ko-kr/xenmobile/server/policies/restrictions-policy.html#android-enterprise-settings)을 참조하십시오.
- 이제 Android Enterprise 장치에서 관리되는 앱을 자동으로 업데이트할 수 있습니다. 자세한 내용은 (/ko-kr/xenmobile/server/policies/app-auto-update-policy.html)을 참조하십시오.
- 파일 장치 정책을 사용하여 업로드할 수 있는 파일 형식 목록을 구성할 수 있습니다. 다음 파일 형식은 허용 목록에 추가하더라도 업로드할 수 없습니다.

  - .캐브
  - .앱엑스
  - .ipa 파일

- .apk 파일
- .xap 파일
- .mdx 파일
- 실행 파일

자세한 내용은 (/ko-kr/xenmobile/server/advanced-concepts/xenmobile-deployment/server-properties.html)을 참조하십시오.

장치 등록

- 이제 iOS 및 Android 장치에 대해 다른 등록 프로필을 만들 수 있습니다. XenMobile Server는 다양한 등록 유형을 가진 여러 등록 프로필을 지원합니다. 자세한 내용은 (/ko-kr/xenmobile/server/users/enrollment-profiles.html)을 참조하십시오.
- 완전히 관리되는 Android 11 이상 장치는 기업 소유 장치 모드에서 업무 프로필에 등록됩니다. 새로운 모드는 장치의 개인 프로필과 업무 프로필을 더욱 분리합니다. 이 변경 사항은 조직에 관리되는 프로필에 대한 더 큰 제어 권한을 제공하고 사용자에게 개인 프로필에 대한 더 많은 개인 정보 보호를 제공합니다. 자세한 내용은 (/ko-kr/xenmobile/server/provision-devices/android-enterprise.html) 및 (/ko-kr/xenmobile/server/advanced-concepts/xenmobile-deployment/server-properties.html)를 참조하십시오.
- 이제 사용자가 iOS 또는 macOS 장치를 설정할 때 건너뛸 설정 화면을 더 많이 지정할 수 있습니다.
  - iOS
    - **복원 완료:** 사용자가 설정 중에 복원이 완료되는지 여부를 보지 못하도록 합니다. iOS 14.0 이상에서 사용 가능합니다.
    - **업데이트 완료:** 사용자가 설정 중에 소프트웨어 업데이트가 완료되는지 여부를 보지 못하도록 합니다. iOS 14.0 이상에서 사용 가능합니다.
  - macOS
    - **손쉬운 사용:** 사용자가 Voice Over를 자동으로 듣지 못하도록 합니다. 장치가 이더넷에 연결된 경우에만 사용할 수 있습니다. macOS 11 이상에서 사용 가능합니다.
    - **생체 인식:** 사용자가 Touch ID 및 Face ID를 설정하지 못하도록 합니다. macOS 10.12.4 이상에서 사용 가능합니다.
    - **True Tone:** 사용자가 디스플레이의 화이트 밸런스를 동적으로 조정하기 위해 4채널 센서를 설정하지 못하도록 합니다. macOS 10.13.6 이상에서 사용 가능합니다.

- **Apple Pay:** 사용자가 Apple Pay를 설정하지 못하도록 합니다. 이 설정이 해제되면 사용자는 Touch ID 및 Apple ID를 설정해야 합니다. **Apple ID** 및 **생체 인식** 설정이 해제되어 있는지 확인하십시오. macOS 10.12.4 이상에서 사용 가능합니다.
- **스크린 타임:** 사용자가 스크린 타임을 활성화하지 못하도록 합니다. macOS 10.15 이상에서 사용 가능합니다.

설정 옵션 구성에 대한 자세한 내용은 Apple 배포 프로그램을 통해 장치 배포를 참조하십시오.

업데이트 로그 파일 표시

문제 해결 메뉴의 **로그** 명령줄 인터페이스에 **업데이트 로그 파일 표시**라는 새로운 옵션이 제공됩니다. 이 옵션을 사용하면 업데이트 로그 콘텐츠 목록을 볼 수 있어 문제 해결 효율성이 향상됩니다. 명령줄 인터페이스 도구에 대한 자세한 내용은 명령줄 인터페이스 옵션을 참조하십시오.

오류 로그 파일

문제 해결 및 지원 > 로그에서 로그를 볼 때 이제 디버그 로그에서 필터링된 오류를 표시하는 로그를 볼 수 있습니다. 자세한 내용은 XenMobile에서 로그 파일 보기를 참조하십시오.

서버 속성

- `afw.allow.legacy.apps` 서버 속성을 구성하여 레거시 Android 앱을 Android Enterprise 앱으로 전달할지 여부를 결정할 수 있습니다. 자세한 내용은 서버 속성을 참조하십시오.
- XenMobile Server는 이제 포트 443 대신 포트 2197 사용을 지원합니다. `api.push.apple.com`에서 APN 알림을 주고받는 데 포트 2197을 사용합니다. 이 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 취약한 암호를 가진 사용자를 방지합니다. 속성 `enable.password.strength.validation`이 `true`로 설정된 경우, 취약한 암호를 가진 로컬 사용자를 생성할 수 없습니다.

VPN 가상 서버 목록 개선

VPN 서버 이름에 `_XM_XenMobileGetway`이 포함되어 있지 않으면 XenMobile Server는 목록에서 사용 가능한 첫 번째 VPN 가상 서버를 선택합니다.

시트릭스 런처 지원

XenMobile Server는 Android Enterprise 장치에서 Citrix Launcher를 지원합니다. 자세한 내용은 Launcher 구성 장치 정책을 참조하십시오.

XenMobile Server 색상 개편

XenMobile Server는 Citrix 브랜드 색상 업데이트를 준수합니다.

XenMobile Server 10.13의 새로운 기능

XenMobile Server 10.13 (PDF 다운로드)

Citrix ADC에서 더 이상 사용되지 않는 Classic 정책에 대한 지속적인 지원

Citrix는 최근 Citrix ADC 12.0 빌드 56.20부터 일부 Classic 정책 기반 기능의 사용 중단을 발표했습니다. Citrix ADC 사용 중단 알림은 Citrix Gateway와 기존 XenMobile Server 통합에 영향을 미치지 않습니다. XenMobile Server는 Classic 정책을 계속 지원하며 별도의 조치가 필요하지 않습니다.

사용 중단 알림

단계적으로 중단되는 Citrix XenMobile 기능에 대한 사전 알림은 사용 중단을 참조하십시오.

엔드포인트를 iOS 14.5로 업그레이드하기 전에

Citrix는 엔드포인트를 iOS 14.5로 업그레이드하기 전에 앱 충돌을 완화하기 위해 다음 작업을 수행할 것을 권장합니다.

- Citrix Secure Mail 및 Secure Web을 21.2.X 이상으로 업그레이드합니다. MDX 또는 엔터프라이즈 앱 업그레이드를 참조하십시오.
- MDX Toolkit을 사용하는 경우 모든 타사 iOS 애플리케이션을 MDX Toolkit 21.3.X 이상으로 래핑합니다. 최신 버전은 MDX Toolkit 다운로드 페이지에서 확인하십시오.

온프레미스 Citrix ADC를 업그레이드하기 전에

온프레미스 Citrix ADC를 특정 버전으로 업그레이드하면 단일 Sign-On 오류가 발생할 수 있습니다. 브라우저에서 **회사 직원 로그인** 옵션을 사용하여 Citrix Files 또는 ShareFile 도메인 URL에 단일 Sign-On하면 오류가 발생합니다. 사용자가 로그인할 수 없습니다.

이 문제를 해결하려면: Citrix Gateway의 ADC CLI에서 다음 명령을 아직 실행하지 않았다면, 전역 SSO를 활성화하기 위해 실행하십시오.

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

자세한 내용은 다음을 참조하십시오.

- Citrix ADC 릴리스(기능 단계) 13.0 빌드 67.39/67.43
- 영향을 받는 SSO 구성(/ko-kr/citrix-adc/current-release/aaa-tm/single-sign-on-types/enable-sso-for-auth-pol.html#impacted-sso-configurations)

해결 방법을 완료하면 사용자는 회사 직원 로그인 옵션을 사용하여 브라우저에서 SSO를 통해 Citrix Files 또는 ShareFile 도메인 URL에 인증할 수 있습니다.

XenMobile 10.13 (온프레미스)으로 업그레이드하기 전에

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 시스템 요구 사항 및 호환성 및 XenMobile 호환성을 참조하십시오.

1. 업그레이드할 XenMobile® Server를 실행하는 가상 머신의 RAM이 8GB 미만인 경우, RAM을 최소 8GB로 늘리는 것이 좋습니다.
2. XenMobile Server 10.13의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.16 이상으로 업데이트하십시오.

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

   > **참고:**
   >
   > XenMobile 10.13의 Customer Success Services 날짜(이전 Subscription Advantage 날짜)는 September 29, 2020입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 늦어야 합니다.
   >
   > 라이선스 서버에서 라이선스 옆에 있는 날짜를 볼 수 있습니다. XenMobile 최신 버전을 이전 라이선스 서버 환경에 연결하면 연결 확인이 실패하고 라이선스 서버를 구성할 수 없습니다.
   >
   > 라이선스 날짜를 갱신하려면 Citrix Portal에서 최신 라이선스 파일을 다운로드하여 라이선스 서버에 업로드하십시오. Customer Success Services를 참조하십시오.
3. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 대한 iOS 정책 및 앱 배포에는 다음 요구 사항이 있습니다. Citrix Gateway가 SSL 지속성을 위해 구성된 경우 모든 XenMobile Server 노드에서 포트 80을 열어야 합니다.
4. 권장 사항: XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 만드십시오. 또한 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하면 전체 백업을 통해 복구할 수 있습니다.

업그레이드하려면

이 릴리스부터 XenMobile은 VMware ESXi 7.0을 지원합니다. ESXi 7.0을 설치하거나 업그레이드하기 전에 10.13으로 업그레이드해야 합니다.

XenMobile 10.12.x 또는 10.11.x에서 XenMobile 10.13으로 직접 업그레이드할 수 있습니다. 업그레이드하려면 사용 가능한 최신 바이너리를 다운로드하십시오. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **Download File**을 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 **릴리스 관리** 페이지를 사용하십시오. 릴리스 관리 페이지를 사용하여 업그레이드하려면을 참조하십시오.

업그레이드 후

아웃바운드 연결과 관련된 기능이 작동을 멈추고 연결 구성을 변경하지 않은 경우, **XenMobile Server 로그**에서 다음과 같은 오류를 확인하십시오. "VPP 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다.".

- 인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 확인을 비활성화해야 함을 의미합니다.
- 기본적으로 Microsoft PKI 서버를 제외한 아웃바운드 연결에서는 호스트 이름 확인이 활성화되어 있습니다.
- 호스트 이름 확인으로 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 Mobile 생산성 앱은 iOS 14와 호환되지만, 현재 iOS 14의 새로운 기능은 지원하지 않습니다. MDX Toolkit 20.8.5 이상을 사용하거나 MAM SDK를 사용하여 앱을 준비하십시오.
- **Android 11:** XenMobile Server는 Android 11을 지원합니다. Google Device Administration API의 사용 중단이 Android 10 이상을 실행하는 장치에 미치는 영향에 대한 자세한 내용은 장치 관리에서 Android Enterprise로 마이그레이션을 참조하십시오. 이 Citrix 블로그도 참조하십시오.

단일 환경에서 여러 장치 및 앱 관리 모드 구성

이제 단일 XenMobile 사이트에서 여러 등록 구성을 지원하도록 구성할 수 있습니다. 등록 프로필의 역할이 장치 및 앱 관리를 위한 등록 설정을 포함하도록 확장되었습니다.

등록 프로필은 단일 XenMobile 콘솔 내에서 여러 사용 사례 및 장치 마이그레이션 경로를 지원합니다. 사용 사례는 다음과 같습니다.

- 모바일 장치 관리(MDM 전용)
- MDM+모바일 애플리케이션 관리(MAM)
- MAM 전용
- 기업 소유 등록
- BYOD 등록 (MDM 등록을 거부할 수 있는 기능)
- Android 장치 관리자 등록을 Android Enterprise 등록으로 마이그레이션 (완전 관리형, 업무 프로필, 전용 장치)

등록 프로필이 이제 더 이상 사용되지 않는 서버 속성 `xms.server.mode`을(를) 대체합니다. 이 변경 사항은 기존 전달 그룹 및 등록된 장치에 영향을 미치지 않습니다.

전용 장치를 등록할 필요가 없는 경우, 서버 속성 `enable.multimode.xms`을(를) `false`(으)로 설정하여 이 기능을 비활성화할 수 있습니다. 서버 속성을(를) 참조하십시오.

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

기존 서버 속성	새 관리 모드
ENT 모드 (iOS)	Citrix MAM을 사용한 Apple 장치 등록
ENT 모드 (Android)	Citrix MAM을 사용한 레거시 장치 관리자
기업 모드 (Android Enterprise)	Citrix MAM을 사용한 완전 관리형 (이전 COPE) 업무 프로필
MAM 모드 (iOS 및 Android)	시트릭스 모바일 애플리케이션 관리
MDM 모드 (iOS)	Apple 장치 등록
MDM 모드 (Android)	레거시 장치 관리자
모바일 장치 관리 모드 (안드로이드 엔터프라이즈)	완전 관리형의 회사 프로필

배달 그룹을 생성할 때 그룹에 등록 프로필을 연결할 수 있습니다. 등록 프로필을 연결하지 않으면 XenMobile이 전역 등록 프로필을 연결합니다.

등록 프로필은 다음 장치 관리 기능을 제공합니다.

- **Android 장치 관리자(DA) 모드에서 Android Enterprise로 더 쉽게 마이그레이션할 수 있습니다.** Android Enterprise 장치의 경우 설정에는 완전 관리형, 완전 관리형의 회사 프로필 또는 전용과 같은 장치 소유자 모드가 포함됩니다. Android Enterprise를 참조하십시오.

  Android용 등록 프로필 페이지(/en-us/xenmobile/server/media/enrollment-profile-android-mdm-mam-mode.png)

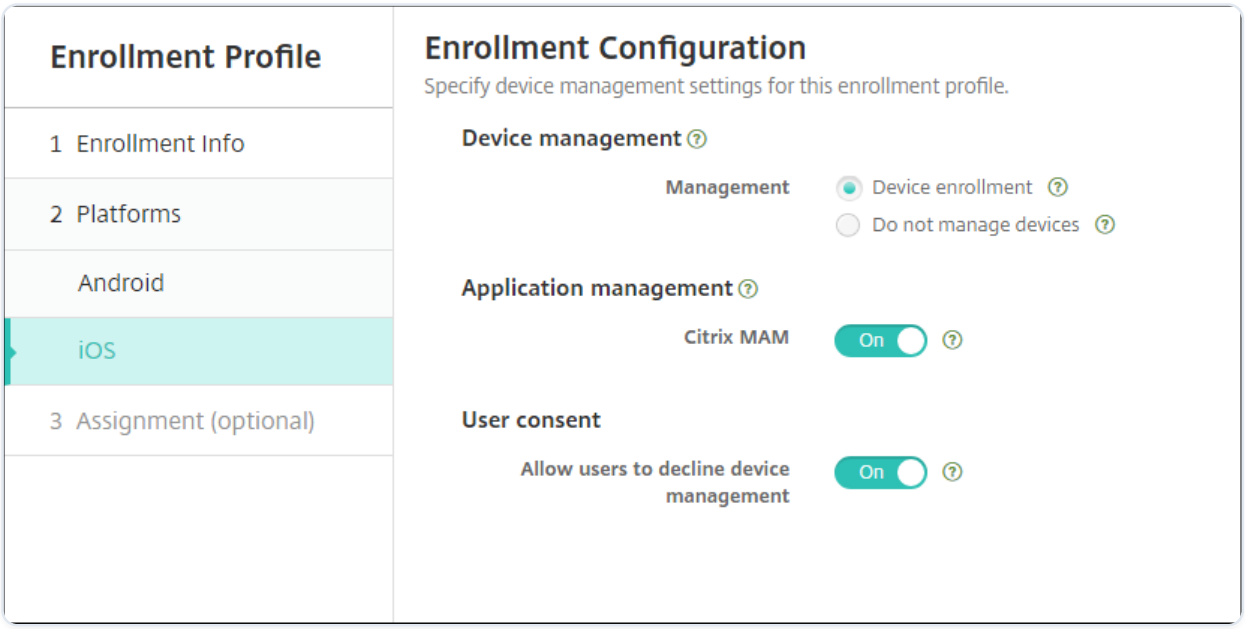
  이 업그레이드의 경우 서버 모드 및 **설정 > Android Enterprise**에 대한 현재 XenMobile 구성이 다음과 같이 새 등록 프로필 설정에 매핑됩니다.

현재 구성	관리 설정	기기 소유자 모드 설정	CITRIX MAM 설정
MDM. 관리형 Google Play (안드로이드 엔터프라이즈)	안드로이드 엔터프라이즈	완전 관리형의 회사 프로필	끔
MDM; G Suite (레거시 DA)	레거시 DA	해당 없음	끔
MAM	기기 관리 안 함	해당 없음	켬
MDM+MAM. 관리형 Google Play (안드로이드 엔터프라이즈)	안드로이드 엔터프라이즈*	완전 관리형 기기의 업무 프로필	켜짐
MDM+MAM; G Suite (레거시 DA)	레거시 DA*	해당 없음	켜짐

  * 등록이 필요한 경우, **사용자가 장치 관리를 거부하도록 허용**은 **꺼짐**입니다.

  업그레이드 후, 현재 등록 프로필은 해당 매핑을 반영합니다. 레거시 DA에서 전환하면서 새로운 사용 사례를 처리하기 위해 다른 등록 프로필을 생성할지 고려하십시오.

- **더 쉬워진 iOS 관리.** iOS 장치의 경우, 설정에는 장치를 관리형 또는 비관리형으로 등록할지 선택하는 옵션이 포함됩니다.



이번 업그레이드에서는 이전 구성이 다음과 같이 새로운 등록 프로필 설정에 매핑됩니다.

서버 모드	관리 설정	CITRIX MAM 설정
MDM	장치 등록	끔
MAM	장치 관리 안 함	켬
MDM+MAM	장치 등록	켬

등록이 필요한 경우, **사용자가 장치 관리를 거부하도록 허용**은 **끔**으로 설정됩니다.

향상된 등록 프로필에는 다음과 같은 제한 사항이 있습니다.

- 향상된 등록 프로필 기능은 일회용 PIN 또는 2단계 인증 등록 초대에는 사용할 수 없습니다.

등록 프로필을(를) 참조하십시오.

최신 HTTP/2 기반 APNs 공급자 API 지원

Apple Push Notification 서비스 레거시 이진 프로토콜에 대한 Apple 지원은 March 31, 2021부터 종료됩니다. Apple은 대신 HTTP/2 기반 APNs 공급자 API를 사용할 것을 권장합니다. XenMobile Server는 이제 HTTP/2 기반 API를 지원합니다. 자세한 내용은 `<https://developer.apple.com/>`의 뉴스 업데이트 "Apple Push Notification Service Update"를 참조하십시오. APNs 연결 확인에 대한 도움말은 연결 확인을(를) 참조하십시오.

다음 XenMobile Server 버전은 기본적으로 HTTP/2 기반 API 지원을 활성화합니다.

- 젠모바일 서버 10.13

- XenMobile Server 10.12 롤링 패치 5 이상

다음 XenMobile Server 버전을 사용하는 경우, 지원을 활성화하려면 서버 속성 **apple.apns.http2**를 추가해야 합니다.

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

더 이상 XenMobile Server 10.11을 지원하지 않으며, 최신 버전으로 업그레이드하는 것이 좋습니다.

여러 iOS 장치에서 장치 인증서 기반 IPsec VPN 사용

장치 인증서 기반 IPsec VPN이 필요한 각 iOS 장치에 대해 VPN 장치 정책 및 자격 증명 장치 정책을 구성하는 대신 프로세스를 자동화하십시오.

1. 연결 유형을 **Always on IKEv2**로 설정하여 iOS VPN 장치 정책을 구성합니다.
2. 장치 인증 방법으로 **장치 ID 기반 장치 인증서**를 선택합니다.
3. 사용할 **장치 ID 유형**을 선택합니다.
4. REST API를 사용하여 장치 인증서를 대량으로 가져옵니다.

VPN 장치 정책 구성에 대한 자세한 내용은 VPN 장치 정책을 참조하십시오. 인증서 대량 가져오기에 대한 자세한 내용은 REST API를 사용하여 인증서 대량 업로드를 참조하십시오.

Apple 볼륨 구매 앱 자동 업데이트

볼륨 구매 계정(**설정 > iOS 설정**)을 추가할 때 이제 모든 iOS 앱에 대해 자동 업데이트를 활성화할 수 있습니다. Apple Volume Purchase에서 **앱 자동 업데이트** 설정을 참조하십시오.

로컬 사용자 계정에 대한 암호 요구 사항

XenMobile 콘솔에서 로컬 사용자 계정을 추가하거나 편집할 때 최신 암호 요구 사항을 준수해야 합니다.

자세한 내용은 로컬 사용자 계정을 추가하려면을 참조하십시오.

- **암호 요구 사항:** XenMobile Server 콘솔에서 로컬 사용자 계정을 추가하거나 편집할 때 최신 암호 요구 사항을 따르십시오. 로컬 사용자 계정을 추가하려면을 참조하십시오.
- **로컬 사용자 계정 잠금:** 사용자가 연속으로 잘못된 로그인 시도 횟수 제한에 도달하면 로컬 사용자 계정이 30분 동안 잠깁니다. 시스템은 잠금 기간이 만료될 때까지 모든 추가 인증 시도를 거부합니다.
  XenMobile Server 콘솔에서 계정 잠금을 해제하려면 **관리 > 사용자**로 이동하여 사용자 계정을 선택한 다음 **로컬 사용자 잠금 해제**를 클릭합니다. 로컬 사용자 계정 잠금을 해제하려면을 참조하십시오.

장치 정책

Android Enterprise 장치에 대한 새로운 장치 정책 및 장치 정책 설정이 추가되었습니다.

Android Enterprise 장치에서 트레이 바 아이콘 숨기기

이제 Android Enterprise 장치에 대해 트레이 바 아이콘을 숨길지 표시할지 선택할 수 있습니다. XenMobile 옵션 장치 정책을 참조하십시오.

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

관리되는 키 저장소에 인증 기관을 설치하는 것 외에도 이제 다음 기능을 관리할 수 있습니다.

- **특정 관리 앱에서 사용하는 인증서 구성.** Android Enterprise용 자격 증명 장치 정책에 이제 **인증서를 사용할 앱** 설정이 포함됩니다. 이 정책에서 선택한 자격 증명 공급자가 발급한 사용자 인증서를 사용할 앱을 지정할 수 있습니다. 앱은 런타임 중에 인증서에 대한 액세스 권한을 자동으로 부여받습니다. 모든 앱에 인증서를 사용하려면 앱 목록을 비워 두십시오. 자격 증명 장치 정책을 참조하십시오.
- **관리되는 키 저장소에서 인증서를 자동으로 제거하거나 모든 비시스템 CA 인증서를 제거합니다.** 자격 증명 장치 정책을 참조하십시오.
- **사용자가 관리되는 키 저장소에 저장된 자격 증명을 수정하지 못하도록 합니다.** Android Enterprise용 제한 장치 정책에 이제 **사용자가 사용자 자격 증명을 구성하도록 허용** 설정이 포함됩니다. 기본적으로 이 설정은 **켜짐**입니다. 제한 장치 정책을 참조하십시오.

관리형 구성에서 인증서 별칭 사용 간소화

새 **자격 증명** 장치 정책의 **인증서 별칭** 설정을 **관리형 구성** 장치 정책과 함께 사용합니다. 이렇게 하면 사용자의 작업 없이 앱이 VPN에서 인증할 수 있습니다. 앱 로그에서 자격 증명 별칭을 찾는 대신 자격 증명 별칭을 만듭니다. **관리형 구성** 장치 정책의 **인증서 별칭** 필드에 입력하여 별칭을 만듭니다. 그런 다음 **자격 증명** 장치 정책의 **인증서 별칭** 설정에 동일한 인증서 별칭을 입력합니다. 관리형 구성 정책 및 자격 증명 장치 정책을 참조하십시오.

Android Enterprise 장치에서 "하나의 잠금 사용" 설정 제어

새 **암호** 장치 정책의 **통합 암호 사용** 설정을 통해 장치와 작업 프로필에 별도의 암호가 필요한지 여부를 제어할 수 있습니다. 이 설정이 있기 전에는 사용자가 장치의 **하나의 잠금 사용** 설정으로 이 동작을 제어했습니다. **통합 암호 사용**이 **켜짐**으로 설정된 경우 사용자는 장치와 작업 프로필에 동일한 암호를 사용할 수 있습니다. **통합 암호 사용**이 **꺼짐**으로 설정된 경우 사용자는 장치와 작업 프로필에 동일한 암호를 사용할 수 없습니다. 기본값은 **꺼짐**입니다. **통합 잠금 사용** 설정은 Android 9.0 이상을 실행하는 Android Enterprise 장치에서 사용할 수 있습니다. 암호 장치 정책을 참조하십시오.

규정을 준수하지 않는 Android Enterprise 장치에서 앱 및 바로 가기 표시

Android Enterprise용 암호 장치 정책에는 새로운 설정인 **암호가 규정을 준수하지 않는 동안 앱 및 바로 가기 표시**가 있습니다. 이 설정을 활성화하면 장치 암호가 더 이상 규정을 준수하지 않을 때 앱과 바로 가기가 계속 표시됩니다. Citrix는 암호가 규정을 준수하지 않을 때 장치를 규정 미준수로 표시하는 자동화된 작업을 생성할 것을 권장합니다. 암호 장치 정책을 참조하십시오.

Android Enterprise 작업 프로필 장치 또는 완전 관리형 장치에서 인쇄 기능 비활성화

제한 장치 정책에서 **인쇄 허용 안 함** 설정을 통해 사용자가 Android Enterprise 장치에서 액세스할 수 있는 모든 프린터로 인쇄할 수 있는지 여부를 지정할 수 있습니다. Android Enterprise 설정을 참조하십시오.

키오스크 정책에 패키지 이름을 추가하여 전용 장치에서 앱 허용

이제 Android Enterprise 플랫폼에서 허용하려는 패키지 이름을 입력할 수 있습니다. Android Enterprise 설정을 참조하십시오.

Android Enterprise 작업 프로필 및 완전 관리형 장치에 대한 키가드 기능 관리

Android 키가드는 장치 및 작업 챌린지 잠금 화면을 관리합니다. 키가드 관리 장치 정책을 사용하여 다음을 제어합니다.

- 작업 프로필 장치에서 키가드 관리. 사용자가 장치 키가드 및 작업 챌린지 키가드를 잠금 해제하기 전에 사용할 수 있는 기능을 지정할 수 있습니다. 예를 들어, 기본적으로 사용자는 지문 잠금 해제를 사용하고 잠금 화면에서 수정되지 않은 알림을 볼 수 있습니다. 또한 키가드 관리 정책을 사용하여 Android 9.0 이상을 실행하는 장치에 대한 모든 생체 인식 인증을 비활성화할 수 있습니다.
- 완전 관리형 및 전용 장치에서 키가드 관리. 사용자가 키가드 화면을 잠금 해제하기 전에 신뢰 에이전트 및 보안 카메라와 같은 사용 가능한 기능을 지정할 수 있습니다. 또는 모든 키가드 기능을 비활성화하도록 선택할 수 있습니다.

키가드 관리 장치 정책을 참조하십시오.

XenMobile 콘솔에서 Android Enterprise용 엔터프라이즈 앱 게시

Android Enterprise 개인 앱을 추가할 때 더 이상 Google Play 개발자 계정에 등록할 필요가 없습니다. XenMobile 콘솔은 APK 파일을 업로드하고 게시할 수 있도록 관리형 Google Play 스토어 UI를 엽니다. 자세한 내용은 엔터프라이즈 앱 추가를 참조하십시오.

XenMobile 콘솔에서 Android Enterprise용 웹 앱 게시

XenMobile용 Android Enterprise 웹 앱을 게시하기 위해 더 이상 관리형 Google Play 또는 Google 개발자 포털로 이동할 필요가 없습니다. **구성 > 앱 > 웹 링크**에서 **업로드**를 클릭하면 파일을 업로드하고 저장할 수

있는 관리형 Google Play 스토어 UI가 열립니다. 앱 승인 및 게시에는 약 10분이 소요될 수 있습니다. 자세한 내용은 웹 링크 추가를 참조하십시오.

XenMobile Server REST API를 사용하여 iOS 장치에 대량으로 인증서 업로드

인증서를 한 번에 하나씩 업로드하는 것이 비실용적인 경우 XenMobile Server REST API를 사용하여 iOS 장치에 인증서를 대량으로 업로드하십시오.

1. 연결 유형이 **Always on IKEv2**인 iOS VPN 장치 정책을 구성합니다.
2. 장치 인증 방법으로 **장치 ID 기반 장치 인증서**를 선택합니다.
3. 사용할 **장치 ID 유형**을 선택합니다.
4. REST API를 사용하여 장치 인증서를 대량으로 가져옵니다.

VPN 장치 정책 구성에 대한 자세한 내용은 VPN 장치 정책을 참조하십시오. 인증서 대량 가져오기에 대한 자세한 내용은 REST API를 사용하여 iOS 장치에 대량으로 인증서 업로드를 참조하십시오.

암호화 키 새로 고침

암호화 키 새로 고침 옵션이 XenMobile CLI의 고급 설정에 추가되었습니다. 이 옵션을 사용하여 한 번에 하나의 노드에서 암호화 키를 새로 고칠 수 있습니다. 시스템 옵션을 참조하십시오.

ESXi 7.0 지원

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

새 서버 속성

다음 서버 속성을 사용할 수 있습니다.

- **iOS App Store 링크에 호스트 이름 허용:** 콘솔 대신 공용 API를 사용하여 iOS용 공용 앱 스토어 앱을 추가하려면 원하는 경우 허용된 호스트 이름 목록을 구성합니다.
- **로컬 사용자 계정 잠금 제한:** 로컬 사용자의 계정이 잠기기 전까지 허용되는 로그인 시도 횟수를 구성합니다.
- **로컬 사용자 계정 잠금 시간:** 너무 많은 로그인 시도 실패 후 로컬 사용자가 잠기는 기간을 구성합니다.
- **파일 업로드 제한 최대 크기 사용:** 업로드된 파일의 최대 파일 크기 제한을 활성화합니다.
- **파일 업로드 허용 최대 크기:** 업로드된 파일의 최대 파일 크기를 설정합니다.

이러한 속성에 대한 자세한 내용은 서버 속성을 참조하십시오.

셀프 서비스 디스크 정리

문제 해결 메뉴에서 **디스크 사용량**이라는 새로운 명령줄 인터페이스 옵션을 사용할 수 있습니다. 이 옵션을 사용하면 코어 덤프 파일 및 지원 번들 파일 목록을 볼 수 있습니다. 목록을 본 후 명령줄을 통해 해당 파일을 모두 삭제하도록 선택할 수 있습니다. 명령줄 인터페이스 도구에 대한 자세한 내용은 명령줄 인터페이스 옵션을 참조하십시오.

XenMobile Server 10.12의 새로운 기능

XenMobile Server 10.12 (PDF 다운로드)

사용 중단 공지

단계적으로 중단되는 Citrix XenMobile 기능에 대한 사전 공지는 사용 중단을 참조하십시오.

예정된 변경 사항에 대비하여 Android 장치 준비

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

- Android 10용 장치 관리(DA) 등록:
  - **July 31, 2020:** Citrix®는 레거시 Android 장치 관리 모드에 대한 신규 등록을 중단합니다.
  - **November 1, 2020:** Google은 레거시 장치 관리 API를 중단합니다. 레거시 장치 관리 모드에서 실행되는 Android 10 장치는 더 이상 작동하지 않습니다.
- MDX 암호화:
  - **August 1, 2020:** Citrix는 Citrix 모바일 생산성 및 타사 MDX 앱에 대해 MDX 암호화에서 플랫폼 암호화로의 마이그레이션을 적용하기 시작합니다.
  - **September 1, 2020:** MDX 암호화가 수명 종료에 도달합니다.

레거시 DA에 등록된 장치의 경우

- MDX 암호화를 사용하지 않는 경우 별도의 조치가 필요하지 않습니다.
- MDX 암호화를 사용하는 경우, July 31, 2020 이전에 Android 장치를 Android Enterprise로 마이그레이션하십시오. Android 10을 실행하는 장치는 Android Enterprise를 사용하여 등록하거나 다시 등록해야 합니다. 이 요구 사항에는 MAM 전용 모드의 Android 장치가 포함됩니다. 장치 관리에서 Android Enterprise로 마이그레이션을 참조하십시오.

7월 31일부터 Android Enterprise에 이미 등록된 장치용

- Android Enterprise 플랫폼을 사용하여 앱을 게시한 경우 암호화는 이미 Android Enterprise를 통해 처리됩니다. 별도의 조치가 필요하지 않습니다.

- 레거시 Android 플랫폼을 사용하여 앱을 게시한 경우, July 31, 2020 이전에 Android Enterprise를 사용하여 앱을 다시 게시하십시오.

XenMobile 10.12 (온프레미스)로 업그레이드하기 전에

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 시스템 요구 사항 및 호환성 및 XenMobile 호환성을 참조하십시오.

1. XenMobile Server 10.12의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.16 이상으로 업데이트하십시오.

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

   > **참고:**
   >
   > 미리 보기에 자체 라이선스를 사용하려면, XenMobile 10.12의 Customer Success Services 날짜(이전 Subscription Advantage 날짜)가 January 20, 2020이라는 점을 알아두십시오. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 늦어야 합니다.
   >
   > License Server에서 라이선스 옆에 있는 날짜를 볼 수 있습니다. 최신 버전의 XenMobile®을 이전 License Server 환경에 연결하면 연결 확인이 실패하고 License Server를 구성할 수 없습니다.
   >
   > 라이선스 날짜를 갱신하려면 Citrix Portal에서 최신 라이선스 파일을 다운로드하여 Licensing Server에 업로드하십시오. 자세한 내용은 Customer Success Services를 참조하십시오.

2. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 대한 iOS 정책 및 앱 배포에는 다음 요구 사항이 있습니다. Citrix Gateway가 SSL 지속성을 위해 구성된 경우 모든 XenMobile Server 노드에서 포트 80을 열어야 합니다.
3. 업그레이드할 XenMobile Server를 실행하는 가상 머신의 RAM이 4GB 미만인 경우 RAM을 최소 4GB로 늘리십시오. 프로덕션 환경의 권장 최소 RAM은 8GB입니다.
4. 권장 사항: XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 만드십시오. 또한 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하는 경우 전체 백업을 통해 복구할 수 있습니다.

업그레이드하려면

XenMobile 10.11.x 또는 10.10.x에서 XenMobile 10.12로 직접 업그레이드할 수 있습니다. 업그레이드하려면 사용 가능한 최신 바이너리를 다운로드하십시오. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **Download File**을 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 **릴리스 관리** 페이지를 사용하십시오. 자세한 내용은 릴리스 관리 페이지를 사용하여 업그레이드하려면을 참조하십시오.

업그레이드 후

XenMobile 10.12 (온프레미스)로 업그레이드한 후:

아웃바운드 연결과 관련된 기능이 작동을 멈추고 연결 구성을 변경하지 않은 경우, 다음과 같은 오류에 대해 **XenMobile Server 로그**를 확인하십시오. "VPP 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다.".

인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 확인을 비활성화해야 함을 나타냅니다. 기본적으로 Microsoft PKI 서버를 제외한 아웃바운드 연결에서는 호스트 이름 확인이 활성화되어 있습니다. 호스트 이름 확인으로 인해 배포가 중단되는 경우 서버 속성 `disable.hostname.verification`을 `true`로 변경하십시오. 이 속성의 기본값은 `false`입니다.

iOS 13에 대한 추가 지원

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

- 등록 중에 몇 가지 새로운 iOS 설정 지원 옵션 화면이 나타납니다. Apple은 iOS 13에 새로운 iOS 설정 지원 옵션 화면을 추가했습니다. 새로운 옵션은 이 버전의 **설정 > Apple 장치 등록 프로그램(DEP)** 페이지에 포함되어 있습니다. XenMobile Server를 구성하여 해당 화면을 건너뛸 수 있습니다. 이 페이지는 iOS 13 장치 사용자에게 표시됩니다.
- 이전 iOS 버전에서 감독 또는 비감독 장치에서 사용할 수 있었던 일부 제한 장치 정책 설정은 iOS 13 이상 버전의 감독 장치에서만 사용할 수 있습니다. 현재 XenMobile Server 콘솔 도구 설명은 이러한 설정이 iOS 13 이상 버전의 감독 장치 전용이라는 것을 아직 나타내지 않습니다.
    - 하드웨어 제어 허용:
        - FaceTime
        - 앱 설치

    - 앱 허용:
        - 아이튠즈 스토어
        - 사파리
        - Safari > 자동 완성
    - 네트워크 - iCloud 작업 허용:
        - iCloud 문서 및 데이터
    - 감독 모드 전용 설정 - 허용:
        - Game Center > 친구 추가
        - Game Center > 멀티플레이어 게임
    - 미디어 콘텐츠 - 허용:
        - 선정적인 음악, 팟캐스트 및 iTunes U 자료

이러한 제한 사항은 다음과 같이 적용됩니다:

- iOS 12(이하) 기기가 이미 XenMobile Server에 등록되어 있고 iOS 13으로 업그레이드되는 경우, 앞서 언급된 제한 사항은 비감독 모드 및 감독 모드 기기에 적용됩니다.
- 비감독 모드 iOS 13 이상 기기가 XenMobile Server에 등록되는 경우, 앞서 언급된 제한 사항은 감독 모드 기기에만 적용됩니다.
- 감독 모드 iOS 13 이상 기기가 XenMobile Server에 등록되는 경우, 앞서 언급된 제한 사항은 감독 모드 기기에만 적용됩니다.

Apple 대량 구매 프로그램의 Apple Business Manager(ABM) 및 Apple School Manager(ASM)로의 마이그레이션

Apple Volume Purchase Program(VPP)을 사용하는 기업 및 기관은 Apple Business Manager 또는 Apple School Manager의 앱 및 도서로 December 1, 2019 이전에 마이그레이션해야 합니다.

XenMobile에서 VPP 계정을 마이그레이션하기 전에 이 Apple 지원 문서를 참조하십시오.

조직 또는 학교에서 볼륨 구매 프로그램(VPP)만 사용하는 경우 ABM/ASM에 등록한 다음 기존 VPP 구매자를 새 ABM/ASM 계정으로 초대할 수 있습니다. ASM의 경우 `<https://school.apple.com>`으로 이동하십시오. ABM의 경우 `<https://business.apple.com>`로 이동하십시오.

XenMobile에서 VPP 계정을 업데이트하려면:

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.

2. **iOS 설정**을 클릭합니다. **볼륨 구매 프로그램** 구성 페이지가 나타납니다.
3. ABM 또는 ASM 계정에 이전 VPP 계정과 동일한 앱 구성이 있는지 확인하십시오.
4. ABM 또는 ASM 포털에서 업데이트된 토큰을 다운로드합니다.
5. XenMobile 콘솔에서 다음을 수행하십시오.
    a. 해당 위치에 대한 업데이트된 토큰 정보로 기존 볼륨 구매 계정을 편집합니다.
    b. ABM 또는 ASM 자격 증명을 편집합니다. 접미사를 변경하지 마십시오.
    c. **저장**을 두 번 클릭합니다.

자세한 내용은 다음을 참조하십시오.

- Apple 배포 프로그램
- Apple 장치 대량 등록

Android Enterprise COPE 장치 지원

XenMobile Server는 이전에 COPE(기업 소유 개인 사용 가능) 장치로 알려졌던 작업 프로필이 있는 Android Enterprise 완전 관리형 장치를 지원합니다. 이러한 장치는 작업 프로필도 있는 Android Enterprise 완전 관리형 장치 유형입니다. 장치와 작업 프로필에 별도의 정책 설정을 적용할 수 있습니다. 이 릴리스의 경우:

- 자격 증명, 암호 및 제한과 같은 장치 정책을 사용하여 장치와 작업 프로필에 별도의 설정을 적용할 수 있습니다.
- 위치 장치 정책의 위치 모드 설정을 COPE 장치 자체에는 적용할 수 있지만 COPE 장치의 작업 프로필에는 적용할 수 없습니다. 위치 장치 정책의 다른 설정은 COPE 장치에 사용할 수 없습니다.
- 잠금 보안 작업을 장치 또는 작업 프로필에 개별적으로 적용할 수 있습니다.

장치 정책

작업 프로필이 있는 Android Enterprise 완전 관리형 장치(COPE 장치)의 경우 일부 장치 정책은 전체 장치와 작업 프로필에 별도의 설정을 적용할 수 있습니다. XenMobile Server 콘솔에서 일부 장치 정책을 사용하면 별도의 설정을 적용할 수 있습니다. 다른 장치 정책을 사용하여 전체 장치에만 또는 작업 프로필이 있는 완전 관리형 장치의 작업 프로필에만 설정을 적용할 수 있습니다.

보안 작업

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

- 잠금 보안 작업을 장치 또는 작업 프로필에 개별적으로 적용합니다.
- 장치에 대한 다른 모든 보안 작업.

등록 프로필은 Android 장치의 등록 옵션을 제어합니다

이제 등록 프로필은 XenMobile 배포에 Android Enterprise가 활성화된 경우 Android 장치가 등록되는 방식을 제어합니다. 등록 프로필은 Android 장치가 기본 Android Enterprise 모드(완전 관리형 또는 작업 프로필)로 등록될지 또는 레거시(장치 관리자) 모드로 등록될지 결정합니다.

기본적으로 전역 등록 프로필은 새 장치 및 공장 초기화된 Android Enterprise 장치를 완전 관리형 장치로 등록하고 BYOD Android Enterprise 장치를 작업 프로필 장치로 등록합니다. 자세한 내용은 Android Enterprise를 참조하십시오.

기본 등록으로 Android Enterprise를 위한 레거시 Android 장치 준비

Google은 장치 관리의 장치 관리자 모드를 더 이상 사용하지 않고 있으며 고객에게 모든 Android 장치를 장치 소유자 모드 또는 프로필 소유자 모드로 관리하도록 권장하고 있습니다. (Google Android Enterprise 개발자 가이드의 장치 관리자 사용 중단 참조) 이러한 변경 사항을 지원하기 위해 Android Enterprise는 이제 Android 장치의 기본 등록 옵션입니다.

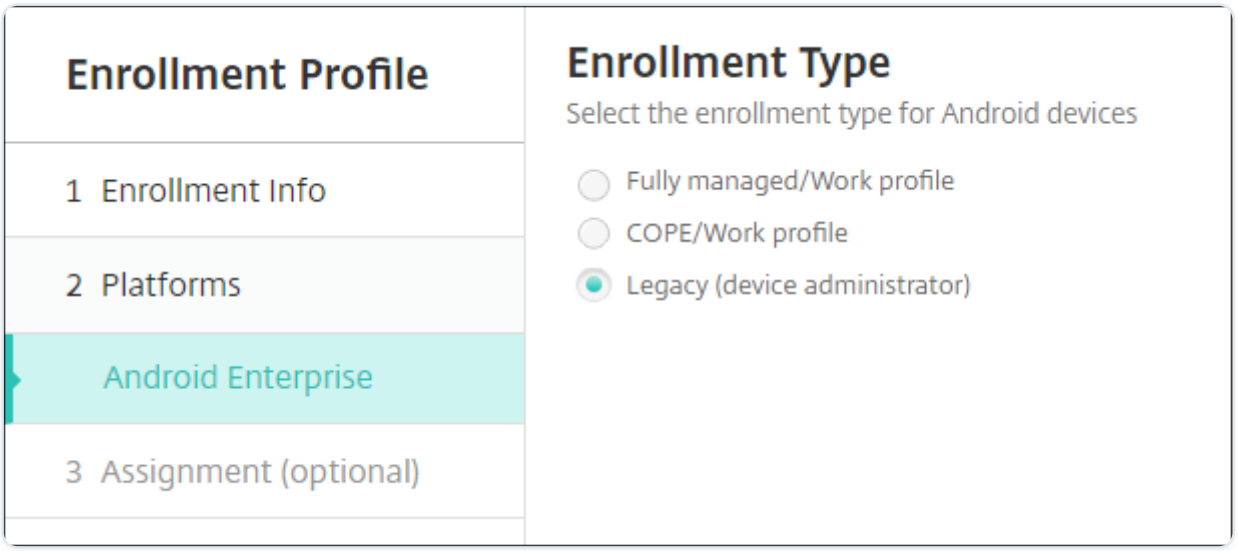
이 변경 사항은 XenMobile 배포에 Android Enterprise가 활성화된 경우 새로 등록되거나 재등록된 모든 Android 장치가 Android Enterprise 장치로 등록됨을 의미합니다.

이러한 변경 사항에 대비하여 XenMobile에서는 이제 Android 장치가 등록되는 방식을 제어하는 등록 프로필을 생성할 수 있습니다.

조직에서 디바이스 소유자 모드 또는 프로필 소유자 모드에서 레거시 Android 디바이스 관리를 시작할 준비가 되지 않았을 수 있습니다. 이 경우 디바이스 관리자 모드에서 계속 관리할 수 있습니다. 레거시 디바이스용 등록 프로필을 생성하고 등록된 모든 레거시 디바이스를 다시 등록합니다.

레거시 디바이스용 등록 프로필을 생성하려면:

1. XenMobile 콘솔에서 **구성 > 등록 프로필**로 이동합니다.
2. 등록 프로필을 추가하려면 **추가**를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다.
3. **다음**을 클릭하거나 **플랫폼**에서 **Android Enterprise**를 선택합니다. 등록 구성 페이지가 나타납니다.
4. **관리**를 **레거시(디바이스 관리)**로 설정합니다. **다음**을 클릭하거나 **할당(옵션)**을 선택합니다. 배달 그룹 할당 화면이 나타납니다.



5. 전용 디바이스를 등록하는 관리자가 있는 배달 그룹을 선택합니다. 그런 다음 **저장**을 클릭합니다.

디바이스 관리자 모드에서 레거시 디바이스를 계속 관리하려면 이 프로필을 사용하여 등록하거나 다시 등록합니다. 사용자가 Secure Hub를 다운로드하고 등록 서버 URL을 제공하도록 하여 작업 프로필 디바이스와 유사하게 디바이스 관리자 디바이스를 등록합니다.

Android Enterprise로의 전환에 대한 Endpoint Management 지원에 대한 자세한 내용은 블로그 Android Enterprise as default for Citrix Endpoint Management service를 참조하십시오.

Android Enterprise용 앱 관리 간소화

더 이상 XenMobile Server용 앱을 승인하거나 게시하기 위해 관리형 Google Play 또는 Google 개발자 포털로 이동할 필요가 없습니다. 결과적으로 앱 승인 및 게시에는 몇 시간이 아닌 약 10분이 소요됩니다.

XenMobile Server 콘솔에서 공용 앱 스토어용 Android Enterprise 앱 승인. 이제 XenMobile Server 콘솔을 벗어나지 않고도 관리형 Google Play 스토어 앱을 승인할 수 있습니다. 검색 필드에 앱 이름을 입력하면 관리형 Google Play 스토어 UI가 열리고 앱을 승인하고 저장하는 지침이 표시됩니다. 그러면 앱이 결과에 채워져 세부 정보를 구성할 수 있습니다. 공용 앱 스토어 앱 추가를 참조하십시오.

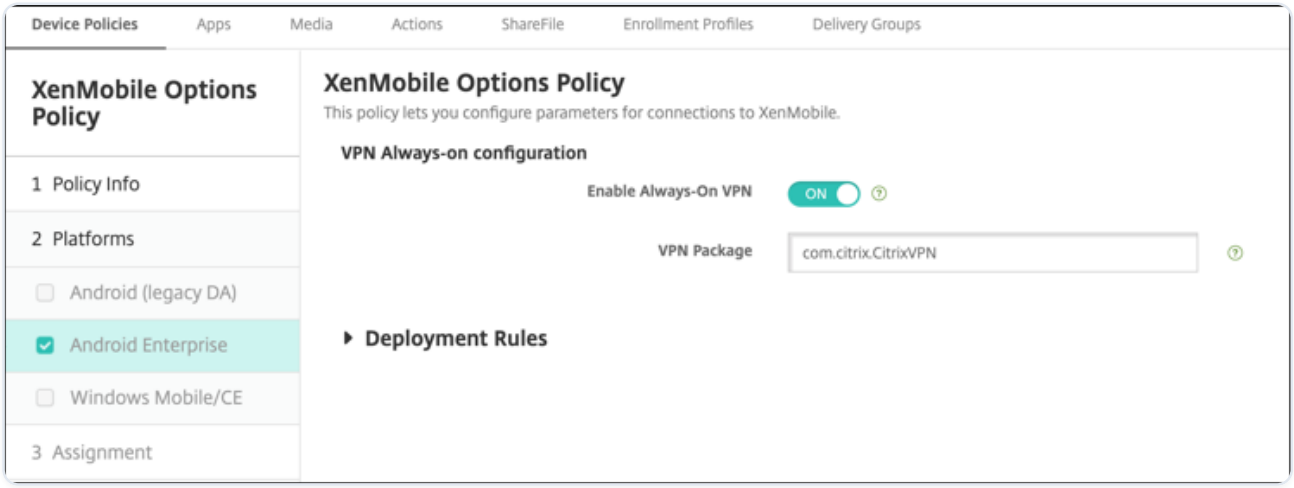
Android Enterprise용 MDX 앱 추가. 이제 XenMobile Server 콘솔에서 Android Enterprise를 MDX 앱 배포 플랫폼으로 지원합니다. MDX 앱 추가를 참조하십시오.

XenMobile Server 콘솔에서 Android Enterprise용 MDX 앱 승인. 이제 XenMobile Server 콘솔을 벗어나지 않고도 Android Enterprise용 관리형 Google Play 스토어 앱을 승인할 수 있습니다. MDX 파일을 업로드하면 관리형 Google Play 스토어 UI가 열리고 앱을 승인하고 저장하는 방법에 대한 지침이 표시됩니다. MDX 앱 추가를 참조하십시오.

Android Enterprise 환경에서 Always-On VPN 지원

이제 XenMobile Server 옵션 장치 정책을 통해 Android Enterprise용 Always-On VPN을 활성화할 수 있습니다.

Android Enterprise용 VPN 프로필을 구성할 때 **기본 VPN 프로필**에 VPN 프로필 이름을 입력합니다. 사용자가 특정 프로필을 탭하는 대신 Citrix SSO 앱의 사용자 인터페이스에서 연결 스위치를 탭하면 XenMobile이 이 프로필을 사용합니다. 이 필드를 비워두면 기본 프로필이 연결에 사용됩니다. 하나의 프로필만 구성된 경우 기본 프로필로 표시됩니다. Always-On VPN의 경우 이 필드는 Always-On VPN을 설정하는 데 사용될 VPN 프로필 이름으로 설정해야 합니다.



Android Enterprise 앱의 제품 트랙 구성

Android Enterprise용 공용 스토어 앱 또는 MDX 앱을 추가할 때 사용자 장치로 푸시할 제품 트랙을 구성합니다. 예를 들어, 테스트용으로 설계된 트랙이 있는 경우 해당 트랙을 선택하여 특정 전달 그룹에 할당할 수 있습니다. 릴리스 배포에 대한 자세한 내용은 Google Play 고객센터를 참조하십시오. 제품 트랙 구성에 대한 자세한 내용은 MDX 앱 추가 또는 공용 앱 스토어 앱 추가를 참조하십시오.

macOS 사용자에게 암호 재설정 강제 적용

macOS 장치가 암호 정책이 포함된 구성 프로필을 수신하면 사용자는 정책 설정을 충족하는 암호를 제공해야 합니다. 이제 사용자가 다음에 인증할 때 암호 재설정을 강제 적용할 수 있습니다. macOS(10.13 이상)용 암호 장치 정책에서 새로운 설정인 **암호 재설정 강제 적용**을 활성화합니다. 정책에 대한 자세한 내용은 암호 장치 정책을 참조하십시오.

XenMobile Server 10.11의 새로운 기능

XenMobile Server 10.11 (PDF 다운로드)

애플 볼륨 구매 프로그램의 Apple Business Manager (ABM) 및 Apple School Manager (ASM)로의 마이그레이션

Apple Volume Purchase Program(VPP)을 사용하는 회사 및 기관은 Apple Business Manager 또는 Apple School Manager의 앱 및 도서로 December 1, 2019 이전에 마이그레이션해야 합니다.

XenMobile에서 VPP 계정을 마이그레이션하기 전에 이 Apple 지원 문서를 참조하십시오.

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

XenMobile®에서 볼륨 구매(이전 VPP) 계정을 업데이트하려면 다음을 수행합니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **볼륨 구매**를 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. **저장**을 두 번 클릭합니다.

iOS 13에 대한 추가 지원

> **중요:**

> iOS 12 이상으로 장치 업그레이드를 준비하려면: iOS용 VPN 장치 정책의 Citrix VPN 연결 유형은 iOS 12 이상을 지원하지 않습니다. VPN 장치 정책을 삭제하고 Citrix SSO 연결 유형으로 VPN 장치 정책을 생성하십시오.

> VPN 장치 정책을 삭제한 후에도 이전에 배포된 장치에서는 Citrix VPN 연결이 계속 작동합니다. 새 VPN 장치 정책 구성은 사용자 등록 중에 XenMobile Server 10.11에서 적용됩니다.

> XenMobile Server는 iOS 13으로 업그레이드된 장치를 지원합니다. 업그레이드는 사용자에게 다음과 같은 영향을 미칩니다.

- 등록하는 동안 몇 가지 새로운 iOS 설정 지원 옵션 화면이 나타납니다. Apple은 iOS 13에 새로운 iOS 설정 지원 옵션 화면을 추가했습니다. 새 옵션은 이 버전의 **설정 > Apple 장치 등록 프로그램(DEP)** 페이지에 포함되어 있지 않습니다. 결과적으로 XenMobile Server를 구성하여 해당 화면을 건너뛸 수 없습니다. 해당 페이지는 iOS 13 장치의 사용자에게 표시됩니다.
- 이전 버전의 iOS에서 감독 또는 비감독 장치에서 사용할 수 있었던 일부 제한 장치 정책 설정은 iOS 13 이상에서는 감독 장치에서만 사용할 수 있습니다. 현재 XenMobile Server 콘솔 도구 설명은 이러한 설정이 iOS 13 이상에서 감독 장치 전용이라는 것을 아직 나타내지 않습니다.
    - 하드웨어 제어 허용:
        - FaceTime
        - 앱 설치
    - 앱 허용:
        - 아이튠즈 스토어
        - 사파리
        - Safari > 자동 완성
    - 네트워크 - iCloud 작업 허용:
        - iCloud 문서 및 데이터
    - 감독 전용 설정 - 허용:
        - Game Center > 친구 추가
        - Game Center > 멀티플레이어 게임
    - 미디어 콘텐츠 - 허용:
        - 노골적인 음악, 팟캐스트 및 iTunes U 자료

이러한 제한 사항은 다음과 같이 적용됩니다:

- iOS 12(또는 이전 버전) 장치가 이미 XenMobile Server에 등록되어 있고 iOS 13으로 업그레이드되는 경우, 앞서 언급된 제한 사항은 비감독 및 감독 장치에 적용됩니다.
- 비감독 iOS 13 이상 장치가 XenMobile Server에 등록되는 경우, 앞서 언급된 제한 사항은 감독 장치에만 적용됩니다.

- 감독 iOS 13 이상 장치가 XenMobile Server에 등록되는 경우, 앞서 언급된 제한 사항은 감독 장치에만 적용됩니다.

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

Apple은 TLS 서버 인증서에 대한 새로운 요구 사항을 발표했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는지 확인하십시오. Apple 발행물 `<https://support.apple.com/ko-kr/HT210176>`을 참조하십시오. 인증서 관리에 대한 도움말은 XenMobile에서 인증서 업로드를 참조하십시오.

GCM에서 FCM으로 업그레이드

April 10, 2018부터 Google은 Google Cloud Messaging (GCM)을 더 이상 사용하지 않도록 설정했습니다. Google은 May 29, 2019에 GCM 서버 및 클라이언트 API를 제거했습니다.

> **중요 요구 사항:**
>
> - XenMobile Server의 최신 버전으로 업그레이드하십시오.
> - Secure Hub의 최신 버전으로 업그레이드하십시오.

> Google은 FCM에서 사용할 수 있는 새로운 기능을 활용하기 위해 즉시 Firebase Cloud Messaging(FCM)으로 업그레이드할 것을 권장합니다. Google의 정보는 `<https://developers.google.com/cloud-messaging/faq>` 및 `<https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html>`를 참조하십시오.

Android 장치에 대한 푸시 알림 지원을 계속하려면: XenMobile Server와 함께 GCM을 사용하는 경우 FCM으로 마이그레이션하십시오. 그런 다음 Firebase Cloud Messaging Console에서 사용할 수 있는 새 FCM 키로 XenMobile Server를 업데이트하십시오.

다음 단계는 신뢰할 수 있는 인증서를 사용할 때의 등록 워크플로를 반영합니다.

업그레이드 단계:

1. Google의 정보에 따라 GCM에서 FCM으로 업그레이드하십시오.
2. Firebase Cloud Messaging Console에서 새 FCM 키를 복사하십시오. 다음 단계에서 필요합니다.
3. XenMobile Server 콘솔에서 **설정 > Firebase Cloud Messaging**으로 이동하여 설정을 구성하십시오.

장치는 XenMobile Server에 체크인하고 정책을 새로 고칠 때 다음 번에 FCM으로 전환됩니다. Secure Hub가 정책을 강제로 새로 고치도록 하려면: Secure Hub에서 **기본 설정 > 장치 정보**로 이동하여 **정책 새로 고침**을 탭하십시오. FCM 구성에 대한 자세한 내용은 Firebase Cloud Messaging을 참조하십시오.

XenMobile 10.11(온프레미스)으로 업그레이드하기 전에

일부 시스템 요구 사항이 변경되었습니다. 자세한 내용은 시스템 요구 사항 및 호환성 및 XenMobile 호환성을 참조하십시오.

1. XenMobile Server 10.11의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.15 이상으로 업데이트하십시오.

   XenMobile의 최신 버전에는 Citrix License Server 11.15(최소 버전)가 필요합니다.

   > **참고:**
   >
   > 미리 보기에 자체 라이선스를 사용하려면 XenMobile 10.11의 Customer Success Services 날짜(이전 Subscription Advantage 날짜)가 April 9, 2019임을 알아두십시오. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 늦어야 합니다.
   >
   > 라이선스 서버에서 라이선스 옆에 있는 날짜를 볼 수 있습니다. 최신 버전의 XenMobile을 이전 라이선스 서버 환경에 연결하면 연결 확인에 실패하고 라이선스 서버를 구성할 수 없습니다.
   >
   > 라이선스 날짜를 갱신하려면 Citrix Portal에서 최신 라이선스 파일을 다운로드하여 라이선스 서버에 업로드하십시오. 자세한 내용은 Customer Success Services를 참조하십시오.

2. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 대한 iOS 정책 및 앱 배포에는 다음 요구 사항이 있습니다. Citrix Gateway가 SSL 지속성을 위해 구성된 경우 모든 XenMobile Server 노드에서 포트 80을 열어야 합니다.
3. 업그레이드할 XenMobile Server를 실행하는 가상 머신의 RAM이 4GB 미만인 경우 RAM을 최소 4GB로 늘리십시오. 프로덕션 환경의 권장 최소 RAM은 8GB입니다.
4. 권장 사항: XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 만드십시오. 또한 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하면 전체 백업을 통해 복구할 수 있습니다.

업그레이드하려면

XenMobile 10.10.x 또는 10.9.x에서 XenMobile 10.11로 직접 업그레이드할 수 있습니다. 업그레이드하려면 사용 가능한 최신 바이너리를 다운로드하십시오. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **Download File**을 클릭합니다.

업그레이드를 업로드하려면 XenMobile 콘솔의 **Release Management** 페이지를 사용하십시오. 자세한 내용은 Release Management 페이지를 사용하여 업그레이드하려면을 참조하십시오.

업그레이드 후

XenMobile 10.11 (온프레미스)로 업그레이드한 후:

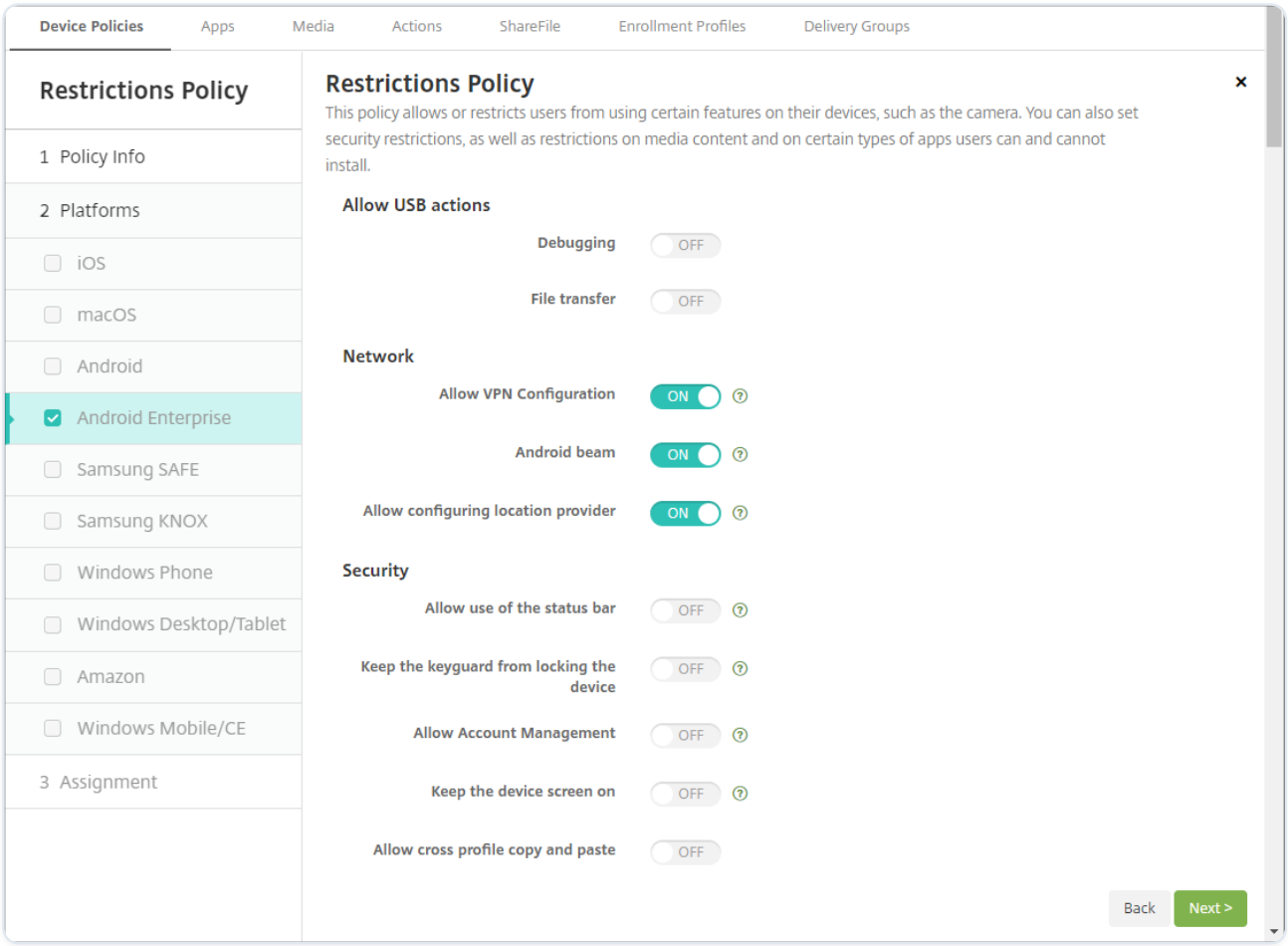
아웃바운드 연결과 관련된 기능이 작동을 멈추고 연결 구성을 변경하지 않은 경우, XenMobile Server 로그에서 다음과 같은 오류를 확인하십시오. “VPP 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다”.

인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 확인을 비활성화해야 함을 나타냅니다. 기본적으로 Microsoft PKI 서버를 제외한 아웃바운드 연결에서는 호스트 이름 확인이 활성화되어 있습니다. 호스트 이름 확인으로 인해 배포가 중단되는 경우 서버 속성 `disable.hostname.verification`을 `true`로 변경하십시오. 이 속성의 기본값은 `false`입니다.

Android Enterprise 장치용 새롭고 업데이트된 장치 정책 설정

Samsung Knox 및 Android Enterprise 정책 통합. Samsung Knox 3.0 이상 및 Android 8.0 이상을 실행하는 Android Enterprise 장치의 경우: Knox와 Android Enterprise는 통합된 장치 및 프로필 관리 솔루션으로 결합됩니다. 다음 장치 정책의 Android Enterprise 페이지에서 Knox 설정을 구성하십시오.

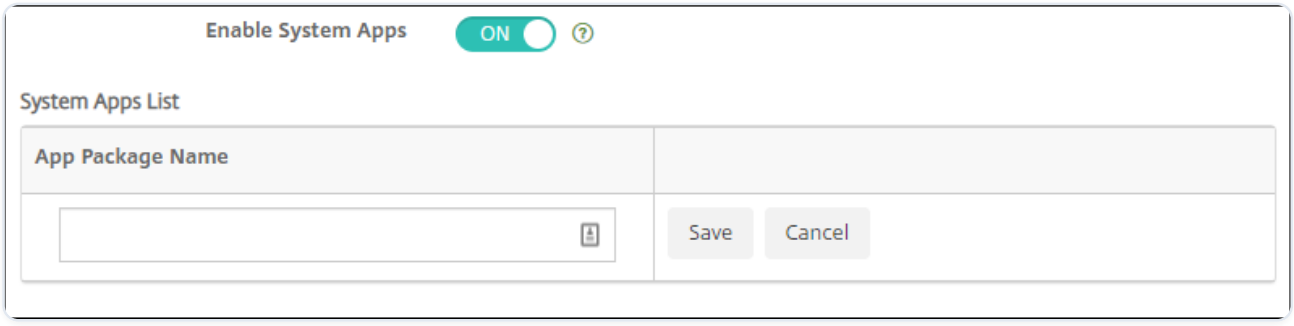
- OS 업데이트 장치 정책**.** Samsung Enterprise FOTA 업데이트 설정을 포함합니다.
- 암호 장치 정책**.**
- **Samsung MDM 라이선스 키 장치 정책.** Knox 라이선스 키를 구성합니다.
- 제한 장치 정책 설정**.**



Android Enterprise용 앱 인벤토리 장치 정책. 이제 관리되는 장치에서 Android Enterprise 앱의 인벤토리를 수집할 수 있습니다. 앱 인벤토리 장치 정책을 참조하십시오.

관리되는 Google Play 스토어의 모든 Google Play 앱에 액세스합니다. 관리되는 Google Play 스토어의 모든 앱에 액세스 서버 속성은 공개 Google Play 스토어의 모든 앱을 관리되는 Google Play 스토어에서 액세스할 수 있도록 합니다. 이 속성을 **true**로 설정하면 모든 Android Enterprise 사용자가 공개 Google Play 스토어 앱을 사용할 수 있습니다. 관리자는 제한 장치 정책을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다.

Android Enterprise 장치에서 시스템 앱 활성화. 사용자가 Android Enterprise 작업 프로필 모드 또는 완전 관리 모드에서 사전 설치된 시스템 앱을 실행할 수 있도록 하려면 제한 장치 정책을 구성하십시오. 이 구성은 카메라, 갤러리 등과 같은 기본 장치 앱에 대한 사용자 액세스를 허용합니다. 특정 앱에 대한 액세스를 제한하려면 Android Enterprise 앱 권한 장치 정책을 사용하여 앱 권한을 설정하십시오.



Android Enterprise 전용 장치 지원. XenMobile은 이제 이전에 COSU(corporate owned single use) 장치라고 불렸던 전용 장치 관리를 지원합니다.

전용 Android Enterprise 장치는 단일 사용 사례를 수행하도록 전용된 완전 관리형 장치입니다. 이러한 장치는 이 사용 사례에 필요한 작업을 수행하는 데 필요한 하나의 앱 또는 소수의 앱으로 제한됩니다. 또한 사용자가 다른 앱을 활성화하거나 장치에서 다른 작업을 수행하는 것을 방지합니다.

Android Enterprise 장치 프로비저닝에 대한 자세한 내용은 전용 Android Enterprise 장치 프로비저닝을 참조하십시오.

정책 이름 변경. Google 용어와 일치하도록 Android Enterprise 앱 제한 장치 정책이 이제 관리형 구성 장치 정책으로 변경되었습니다. 관리형 구성 장치 정책을 참조하십시오.

Android Enterprise용 암호 잠금 및 재설정

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

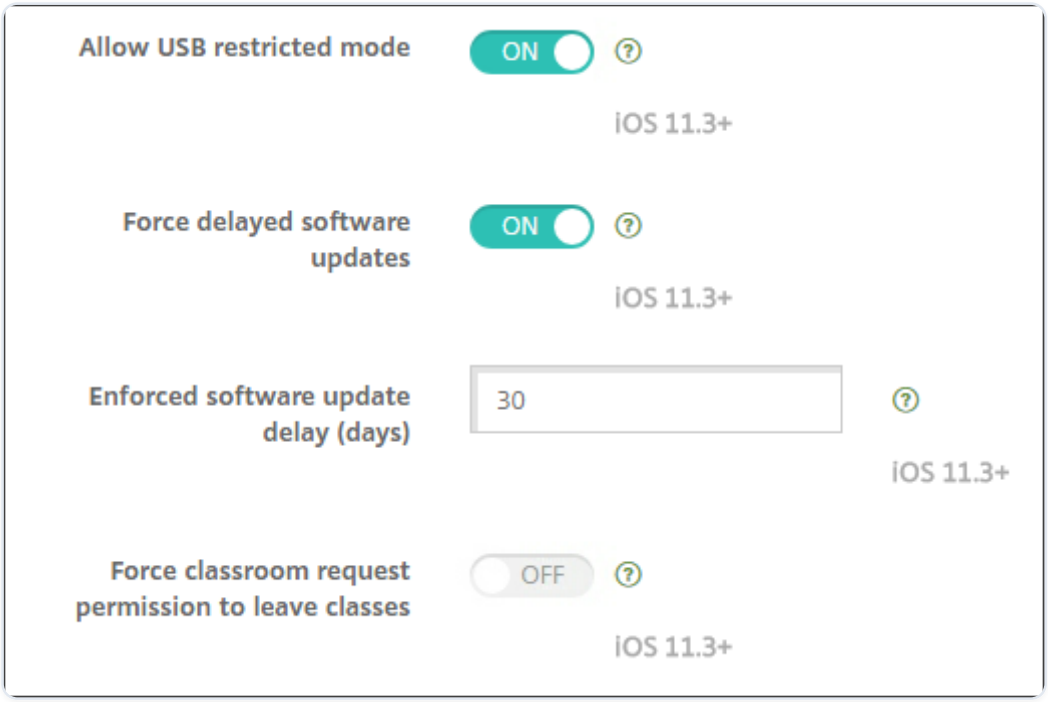
- 전송된 암호는 작업 프로필을 잠급니다. 장치는 잠기지 않습니다.
- 암호가 전송되지 않거나 전송된 암호가 암호 요구 사항을 충족하지 않는 경우:
  - 그리고 작업 프로필에 암호가 이미 설정되어 있지 않으면 장치가 잠깁니다.
  - 그리고 작업 프로필에 암호가 이미 설정되어 있습니다. 작업 프로필은 잠기지만 장치는 잠기지 않습니다.

잠금 및 암호 재설정 보안 작업에 대한 자세한 내용은 보안 작업을 참조하십시오.

iOS 또는 macOS용 새로운 제한 장치 정책 설정

- **관리되지 않는 앱이 관리되는 연락처를 읽음:** 선택 사항입니다. **관리되는 앱의 문서를 관리되지 않는 앱에서 사용**이 비활성화된 경우에만 사용할 수 있습니다. 이 정책을 활성화하면 관리되지 않는 앱이 관리되는 계정의 연락처에서 데이터를 읽을 수 있습니다. 기본값은 **끔**입니다. iOS 12부터 사용할 수 있습니다.
- **관리되는 앱이 관리되지 않는 연락처를 작성:** 선택 사항입니다. 활성화된 경우 관리되는 앱이 관리되지 않는 계정의 연락처에 연락처를 작성하도록 허용합니다. **관리되는 앱의 문서를 관리되지 않는 앱에서 사용**이 활성화된 경우 이 제한은 적용되지 않습니다. 기본값은 **끔**입니다. iOS 12부터 사용할 수 있습니다.
- **암호 자동 완성:** 선택 사항입니다. 비활성화된 경우 사용자는 암호 자동 완성 또는 자동 강력 암호 기능을 사용할 수 없습니다. 기본값은 **켬**입니다. iOS 12 및 macOS 10.14부터 사용할 수 있습니다.
- **암호 근접 요청:** 선택 사항입니다. 비활성화된 경우 사용자의 장치는 근처 장치에서 암호를 요청하지 않습니다. 기본값은 **켬**입니다. iOS 12 및 macOS 10.14부터 사용할 수 있습니다.

- **암호 공유:** 선택 사항입니다. 비활성화된 경우 사용자는 AirDrop 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 **켬**입니다. iOS 12 및 macOS 10.14부터 사용할 수 있습니다.
- **자동 날짜 및 시간 강제 적용:** 감독됨. 활성화된 경우 사용자는 **일반 > 날짜 및 시간 > 자동으로 설정** 옵션을 비활성화할 수 없습니다. 기본값은 **끔**입니다. iOS 12부터 사용할 수 있습니다.
- **USB 제한 모드 허용:** 감독되는 장치에서만 사용할 수 있습니다. 끔으로 설정하면 장치가 잠겨 있는 동안에도 항상 USB 액세서리에 연결할 수 있습니다. 기본값은 **켬**입니다. iOS 11.3부터 사용할 수 있습니다.
- **소프트웨어 업데이트 지연 강제 적용:** 감독되는 장치에서만 사용할 수 있습니다. **켬**으로 설정하면 사용자가 소프트웨어 업데이트를 볼 수 있는 시기가 지연됩니다. 이 제한이 적용되면 사용자는 소프트웨어 업데이트 릴리스 날짜로부터 지정된 일수가 지난 후에야 소프트웨어 업데이트를 볼 수 있습니다. 기본값은 **끔**입니다. iOS 11.3 및 macOS 10.13.4부터 사용할 수 있습니다.
- **강제 소프트웨어 업데이트 지연(일):** 감독되는 장치에서만 사용할 수 있습니다. 이 제한을 통해 관리자는 장치에서 소프트웨어 업데이트를 지연할 기간을 설정할 수 있습니다. 최대 90일이며 기본값은 **30**입니다. iOS 11.3 및 macOS 10.13.4부터 사용할 수 있습니다.
- **수업 나가기 권한 요청 강제:** 감독 모드 기기에서만 사용할 수 있습니다. **켜짐**으로 설정하면 Classroom에서 관리되지 않는 과정에 등록된 학생이 과정을 나가려고 할 때 교사에게 권한을 요청해야 합니다. 기본값은 **꺼짐**입니다. iOS 11.3부터 사용할 수 있습니다.



제한 장치 정책을 참조하십시오.

iOS 또는 macOS용 Exchange 장치 정책 업데이트

iOS 12부터 더 많은 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 재정의 가능: 켜짐**으로 설정하면 사용자가 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 **꺼짐**입니다.
- **S/MIME 서명 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자가 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 **꺼짐**입니다.

S/MIME 암호화의 경우:

- **암호화 ID 자격 증명:** 사용할 암호화 자격 증명을 선택합니다.
- **메시지별 S/MIME 스위치 사용: 켜짐**으로 설정하면 사용자가 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션이 표시됩니다. 기본값은 **꺼짐**입니다.
- **S/MIME 기본 암호화 사용자 재정의 가능: 켜짐**으로 설정하면 사용자가 장치 설정에서 S/MIME를 기본적으로 켤지 여부를 선택할 수 있습니다. 기본값은 **꺼짐**입니다.
- **S/MIME 암호화 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자가 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 **꺼짐**입니다.

iOS 12부터 Exchange OAuth 설정. 이제 Exchange와의 연결을 구성하여 인증에 OAuth를 사용할 수 있습니다.

macOS 10.14부터 Exchange OAuth 설정. 이제 Exchange와의 연결을 OAuth 인증에 사용하도록 구성할 수 있습니다. OAuth를 사용하여 인증하는 경우, AutoDiscovery를 사용하지 않는 설정에 대한 로그인 URL을 지정할 수 있습니다.

Exchange 장치 정책을(를) 참조하십시오.

iOS용 메일 장치 정책 업데이트

iOS 12부터 더 많은 S/MIME Exchange 서명 및 암호화 설정. 메일 장치 정책에는 S/MIME 서명 및 암호화를 구성하기 위한 더 많은 설정이 포함되어 있습니다.

S/MIME 서명의 경우:

- **S/MIME 서명 사용:** 이 계정이 S/MIME 서명을 지원하는지 여부를 선택합니다. 기본값은 **켜짐**입니다. **켜짐**으로 설정하면 다음 필드가 나타납니다.
  - **S/MIME 서명 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

- **S/MIME 서명 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

S/MIME 암호화의 경우:

- **S/MIME 암호화 사용:** 이 계정이 S/MIME 암호화를 지원하는지 여부를 선택합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정하면 다음 필드가 나타납니다.
  - **메시지별 S/MIME 전환 사용: 켜짐**으로 설정하면 사용자가 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션을 표시합니다. 기본값은 **꺼짐**입니다.
  - **S/MIME 기본 암호화 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME가 기본적으로 켜져 있는지 여부를 선택할 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
  - **S/MIME 암호화 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

메일 장치 정책을(를) 참조하십시오.

iOS용 앱 알림 장치 정책 업데이트

iOS 12부터 다음 앱 알림 설정이 제공됩니다.

- **CarPlay에 표시: 켬**으로 설정하면 알림이 Apple CarPlay에 표시됩니다. 기본값은 **켬**입니다.
- **긴급 알림 활성화: 켬**으로 설정하면 앱이 방해 금지 및 벨소리 설정을 무시하는 긴급 알림으로 알림을 표시할 수 있습니다. 기본값은 **끔**입니다.

앱 알림 장치 정책을 참조하십시오.

Apple Education과 함께 사용되는 공유 iPad 지원

Apple Education 기능과 XenMobile 통합은 이제 공유 iPad를 지원합니다. 교실의 여러 학생이 한 명 또는 여러 명의 강사가 가르치는 다양한 과목에 대해 iPad를 공유할 수 있습니다.

관리자 또는 강사가 공유 iPad를 등록한 다음 장치 정책, 앱 및 미디어를 장치에 배포합니다. 그 후 학생들은 관리형 Apple ID 자격 증명을 제공하여 공유 iPad에 로그인합니다. 이전에 학생들에게 교육 구성 정책을 배포한 경우, 더 이상 "다른 사용자"로 로그인하여 장치를 공유하지 않습니다.

공유 iPad의 필수 구성 요소:

- 모든 iPad Pro, iPad 5세대, iPad Air 2 이상, iPad mini 4 이상

- 최소 32GB 저장 공간
- 감독 모드

자세한 내용은 공유 iPad 구성을 참조하십시오.

역할 기반 액세스 제어(RBAC) 권한 변경

RBAC 권한인 로컬 사용자 추가/삭제가 이제 로컬 사용자 추가 및 로컬 사용자 삭제의 두 가지 권한으로 분할되었습니다.

자세한 내용은 RBAC를 사용하여 역할 구성을 참조하십시오.

타사 고지

XenMobile®의 이번 릴리스에는 다음 문서에 정의된 조건에 따라 라이선스가 부여된 타사 소프트웨어가 포함될 수 있습니다.

XenMobile 타사 고지

사용 중단

이 문서의 공지는 단계적으로 중단될 XenMobile Server 기능에 대한 사전 통지를 제공하기 위한 것입니다. 이 정보는 시기적절한 비즈니스 결정을 내릴 수 있도록 제공됩니다. Citrix는 고객의 사용 및 피드백을 모니터링하여 기능이 언제 철회될지 결정합니다. 공지는 후속 릴리스에서 변경될 수 있으며 모든 사용 중단된 기능 또는 기능을 포함하지 않을 수 있습니다. 제품 수명 주기 지원에 대한 자세한 내용은 제품 수명 주기 지원 정책 문서를 참조하십시오.

사용 중단 및 제거

다음 목록은 사용 중단되거나 제거된 XenMobile® Server 기능을 보여줍니다.

사용 중단됨 항목은 즉시 제거되지 않습니다. Citrix®는 향후 릴리스에서 제거될 때까지 사용 중단된 항목을 계속 지원합니다.

제거됨 항목은 XenMobile Server에서 제거되었거나 더 이상 지원되지 않습니다.

수명 종료(End of Life)에 도달한 모바일 생산성 앱에 대한 정보는 EOL 및 사용 중단된 앱을 참조하십시오.

항목	설명	사용 중단 발표	제거됨	대안
파일 기반 라이선싱	파일 기반 라이선싱은 April 15, 2026 이후 더 이	2025년 10월	2026년 4월	License Activation Service (LAS)는

항목	설명	사용 중단 발표	제거됨	대안
	상 작동하지 않습니다.			Citrix 제품군 전반의 제품 활성화를 위한 차세대 기술입니다. 파일 기반 라이선스를 사용하는 고객은 호환되는 릴리스로 업그레이드하고 April 15, 2026 이전에 이 기술 전환을 수행해야 합니다. LAS는 April 15, 2026 이후 Citrix 온프레미스 구성 요소를 활성화하고 라이선스를 부여하는 유일한 방법이 될 것입니다.
젠모바일 메일 관리자 (XMM)/젠모바일 넷스케일러 커넥터 (XNC)	XMM 및 XNC 지원 중단.	2025년 6월	2025년 9월	대안 없음.
하이퍼바이저	Citrix XenServer 8.2 및 이전 버전, VMware ESXi 6.x 및 이전 버전, Hyper-V 2016 지원 중단.	2025년 3월	2025년 5월	시스템을 다음 지원 버전 중 하나로 업데이트하십시오: Citrix Hypervisor 8.2 CU1 및 이후 버전, VMware (ESXi 7.0, ESXi 8.0), 또는 Hyper-V (Windows Server 2019 또는 Windows Server 2022).

항목	설명	사용 중단 발표	제거됨	대안
ShareFile 통합	ShareFile (현재 Progress)이(가) 지원을 중단하면 ShareFile 통합이 중단됩니다.	2025년 1월		대안 없음
Zebra용 사용자 지정 XML	Zebra 장치에서 사용자 지정 XML 지원 중단	2022년 1월	목표: 2022년 6월	Android Enterprise 관리 구성을 사용합니다.
Windows 정보 보호 (WIP)	Microsoft의 여기 발표에 따라 Windows 정보 보호 지원이 중단되었습니다.	2022년 8월	목표: 2022년 10월	대안 없음
젠모바일 분석기	XenMobile Analyzer 도구 지원 중단.	2022년 7월	목표: March 31, 2023	대안 없음
PKI ID: 일반, Symantec PKI, DigiCert 및 Entrust 어댑터	일반, DigiCert 관리 및 Entrust 어댑터 PKI 엔터티에 대한 지원이 더 이상 사용되지 않습니다.	2021년 6월	2022년 1월	대안 없음
등록 초대 설정	등록 초대를 생성하기 위해 장치 IMEI, 일련 번호 및 UDID를 사용하는 것에 대한 지원이 더 이상 사용되지 않습니다.	2022년 1월	2022년 5월	등록 초대를 생성할 때 XenMobile 콘솔의 **관리 > 등록 초대**에서 사용 가능한 설정을 구성합니다.
이동통신사 SMS 게이트웨이	Nexmo SMS 게이트웨이 알림에 대한 지원이 더 이상 사용되지 않습니다.	2022년 1월	2022년 4월	SMTP 서버 알림 사용

항목	설명	사용 중단 발표	제거됨	대안
모바일 서비스 공급자(MSP)	Blackberry 및 기타 Exchange ActiveSync 장치를 쿼리하고 작업을 발행하기 위한 MSP 인터페이스 지원 중단	2022년 1월	2022년 4월	대안 없음
Samsung 키오스크 모드	장치 관리자(DA) 모드 기반의 레거시 Samsung 키오스크 모드 지원 중단.	2022년 1월	2022년 3월	Android Enterprise(AE) 키오스크 모드 사용.
Windows 장치에 대한 Wi-Fi Sense 핫스팟 자동 연결 허용 제한	Windows 10 장치에 대한 Wi-Fi Sense 핫스팟 자동 연결 허용 제한 지원을 제거합니다. Windows 10은 더 이상 이 기능을 지원하지 않습니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.	2021년 10월	2022년 2월	대안 없음
삼성 SAFE/삼성 녹스 플랫폼	SAFE 및 Knox 플랫폼 지원이 중단되었습니다.	2022년 1월	2022년 6월	관리형 앱 구성 정책을 통해 Knox 서비스 플러그인을 사용하여 Android Enterprise로 Knox 정책을 설정합니다.
높은 보안 등록 모드	**높은 보안** 등록 보안 모드를 사용한 등록 초대 생성 지원이 중단되었습니다.	2021년 7월	2022년 2월	지원되는 등록 보안 모드 목록은 장치 등록을 참조하십시오.

항목	설명	사용 중단 발표	제거됨	대안
RBAC 역할 - 공유 장치 등록자 및 COSU 장치 등록자	공유 장치 등록자 및 COSU 장치 등록자 모두에 대한 사전 정의된 역할 기반 액세스 제어 설정 지원이 중단되었습니다.	2021년 7월	2021년 12월	iOS 장치는 지원되는 등록 방법을 통해 구성합니다. Android COSU(전용) 장치는 등록 프로필을 통해 구성합니다.
녹스 모바일 등록(기존 DA)	모든 Android 버전에서 레거시 장치 관리자 모드의 Knox Mobile Enrollment(KME) 지원이 중단되었습니다.	2021년 5월	2021년 6월	KME를 사용하여 Android Enterprise 모드로 등록합니다. Android 9, 10, 11은 Android Enterprise를 지원합니다.
Android 7.x 및 iOS 12.x용 Citrix 모빌리티 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.	2021년 4월	2021년 6월	각 주요 운영 체제 플랫폼의 현재 버전과 이전 버전을 최소한으로 사용하십시오. 이전 장치는 등록된 상태로 유지됩니다. 하지만 Citrix는 레거시 장치를 테스트하거나 지원하지 않습니다.
파생 자격 증명	파생 자격 증명 및 Citrix Derived Credentials Manager 앱에 대한 지원이 중단되었습니다.	2021년 3월	2021년 12월	iOS에서 지원되는 인증 유형 목록은 iOS를 참조하십시오.
인터넷 익스플로러 11	XenMobile Server 콘솔에서 Internet Explorer 사용 지	2021년 1월	2021년 1월	다음 웹 브라우저의 최신 버전을 사용하십시오: Google

항목	설명	사용 중단 발표	제거됨	대안
	원이 중단되었습니다.			Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Android용 RSA 소프트 토큰 지원	Android용 Secure Hub로 RSA 소프트 토큰을 직접 가져오는 기능에 대한 지원이 중단되었습니다.	2021년 1월	2021년 2월	Google Play에서 제공되는 RSA Secure ID 앱 내에서 RSA 소프트 토큰을 가져올 수 있습니다. 그런 다음 Citrix Gateway 인증에 토큰을 사용할 수 있습니다.
안드로이드 - 소니	Android Sony 장치 및 Sony 특정 정책에 대한 지원이 중단되었습니다.	2021년 1월	2022년 2월	안드로이드 엔터프라이즈 사용
안드로이드 - HTC	Android HTC 장치 및 HTC 특정 정책에 대한 지원이 더 이상 사용되지 않습니다.	2021년 1월	2022년 2월	안드로이드 엔터프라이즈 사용
안드로이드 - 아마존	Android Amazon 장치 및 Amazon 특정 정책에 대한 지원이 더 이상 사용되지 않습니다.	2021년 1월	2022년 2월	안드로이드 엔터프라이즈 사용
XenMobile 대시보드의 타사 구성 요소	XenMobile 대시보드의 일부로 사용되는 타사 구성 요소를 더 이상 사용하지 않을 예정입니다.	2020년 12월	2021년 1월	대시보드를 계속 사용하려면 XenMobile 10.12 이상으로 업그레이드하십시오.

항목	설명	사용 중단 발표	제거됨	대안
Android Enterprise 장치에서 레거시 장치 관리자 모드용으로 게시된 앱	더 이상 레거시 DA 플랫폼용으로 게시된 앱을 Android Enterprise에 등록된 장치에 제공하지 않습니다.	2020년 10월	2020년 11월	Android Enterprise 장치의 경우 Android Enterprise 플랫폼용 앱을 게시하십시오. DA 모드의 장치에 레거시 DA 앱을 계속 게시하려면 해당 앱에 대한 별도의 전달 그룹을 만드십시오.
APN 발신 포트	APNs 레거시 이진 프로토콜에 대한 Apple 지원은 March 31, 2021부터 종료됩니다. Apple은 대신 HTTP/2 기반 APNs 공급자 API를 사용할 것을 권장합니다. 이 변경의 일환으로, `*.push.apple.com`에 APNs 알림을 보내는 데 사용되는 포트 2195 및 2196에 대한 지원을 중단합니다.	2020년 10월	2021년 3월	대신 포트 443 또는 2197을 사용하십시오. 장치 관리를 위한 XenMobile 포트 열기를 참조하십시오.
Samsung SEAMS 컨테이너	Samsung SEAMS 컨테이너에 대한 지원이 중단되었습니다.	2020년 6월	2020년 8월	Android Enterprise용 Samsung Knox Service Plug-in(KSP) 앱을 사용하십시오. Knox 서비스 플

항목	설명	사용 중단 발표	제거됨	대안
				러그인 앱 추가를 참조하십시오.
자체 서명된 보안 소켓 계층(SSL) 인증서	모든 장치 플랫폼에 대한 자체 서명된 SSL 인증서 지원이 중단되었습니다.	2020년 5월		기존 자체 서명된 인증서를 잘 알려진 인증 기관(CA)의 신뢰할 수 있는 SSL 인증서로 교체하십시오.
인증서 기반 인증 서명 알고리즘(비 FIPS 및 약한 암호)	다음 서명 알고리즘에 대한 지원이 중단되었습니다. SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	2020년 5월	2021년 6월	XenMobile 콘솔에서 자격 증명 공급자에 대한 CSR을 생성할 때 (**설정 > 자격 증명 공급자 > 인증서 서명 요청**) 더 강력한 암호를 선택하십시오.
데이터베이스 서버	Microsoft SQL Server 2014 및 이전 버전에 대한 지원이 중단되었습니다.	2021년 10월	2022년 8월	시스템을 다음 지원 버전 중 하나로 업데이트하십시오. Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 또는 Microsoft SQL Server 2019 CTP 3.2. 시스템 요구 사항 및 호환

항목	설명	사용 중단 발표	제거됨	대안
				성에서 지원되는 서버 목록을 참조하십시오.
하이퍼바이저	Citrix XenServer 6.5.x 및 이전 버전, VMware ESXi 5.5 Update 3 및 이전 버전, Hyper-V 2012에 대한 지원이 중단되었습니다.	2020년 5월	2020년 8월	시스템을 다음 지원 버전 중 하나로 업데이트하십시오. Citrix Hypervisor 8.0 이상, Citrix XenServer 7.0 이상, VMware (ESXi 6.0, ESXi 6.5.0 Update 3, ESXi 6.7 Update 2 패치 10 또는 ESXi 7.0) 또는 Hyper-V (Windows Server 2016 또는 Windows Server 2019).
시트릭스 런처	레거시 Citrix Launcher 앱에 대한 지원이 중단되었습니다.	2020년 5월	2020년 8월 (앱 스토어에서 제거)	키오스크(전용 장치)로 프로비저닝된 장치와 Android Enterprise용 Citrix Launcher를 사용하십시오. 자세한 내용은 (/ko-kr/xenmobile/server/apps/citrix-launcher.html#citrix-launcher-replacement)을(를) 참조하십시오.

항목	설명	사용 중단 발표	제거됨	대안
Android 6.x 및 iOS 11.x용 Citrix 모빌리티 앱 및 Workspace 앱	Android 6.x 및 iOS 11.x 버전의 Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱에 대한 지원이 중단되었습니다.	2020년 4월	2020년 6월	각 주요 운영 체제 플랫폼의 현재 버전과 이전 버전을 최소한으로 사용하십시오.
MDX 툴킷 및 MDX 서비스	Mobile App Management (MAM) SDK를 대신하여 MDX Toolkit 및 MDX Service 지원이 중단되었습니다. 전환 기간 동안 MDX 래핑된 앱과 MAM SDK로 개발된 앱을 모두 사용할 수 있습니다.	2020년 3월	예정: 2023년 7월	엔터프라이즈 애플리케이션을 계속 관리하려면 MAM SDK를 사용하십시오.
MDX: 대체 게이트웨이 서버	iOS 및 Android 장치용 단계별 인증 지원이 중단되었습니다.	2020년 3월	2021년 9월	대안 없음
MDX: Micro VPN (전체 터널 모드)	iOS 및 Android 장치용 전체 가상 사설망(VPN) 터널 지원이 중단되었습니다.	2020년 3월	2021년 9월	MAM SDK 웹 SSO 모드를 사용하거나 Citrix SSO 연결 유형으로 앱별 VPN 정책을 생성하십시오.
MDX: PAC 파일 지원	iOS 및 Android 장치에 대한 전체 VPN 터널 배포를 통한 프록시 자동	2020년 3월	2021년 9월	내부 네트워크에 액세스하려면 Citrix Gateway를 사용하여 프록

항목	설명	사용 중단 발표	제거됨	대안
	구성(PAC) 파일 지원이 중단되었습니다.			시 서버를 통해 연결하십시오.
MDX 공유 장치 지원	MDX 앱에 대한 공유 장치 지원이 중단되었습니다.	2020년 3월	2021년 9월	Android Enterprise의 경우 MDM에 대한 공유 장치 지원을 사용하십시오. iOS의 경우 Apple School Manager 또는 GroundControl을 사용하십시오.
Android 10용 새 장치 관리자 등록	Android 10 장치에서 레거시 장치 관리자 모드로의 새로운 등록 또는 재등록 지원이 중단되었습니다. 이미 등록된 장치는 계속 작동합니다.	2020년 2월	2020년 9월	새로운 Android 10 이상 장치를 Android Enterprise에 등록하십시오.
Android 10 기기용 레거시 장치 관리자 모드	Google은 일부 장치 관리자 API를 더 이상 사용하지 않습니다. Citrix는 Android API 레벨 29를 대상으로 하는 Citrix Secure Hub™로 업그레이드한 후 장치 관리자 모드에 등록된 Android 10 기기를 지원하지 않습니다.	2020년 2월	2020년 11월	Android 10 기기를 Android Enterprise로 마이그레이션합니다.
MDX 암호화	MDX 암호화 및 XenMobile 콘솔	2019년 10월	2020년 9월	규정 준수 검사가 추가된 암호화 관

항목	설명	사용 중단 발표	제거됨	대안
	의 MDX 암호화 기능은 더 이상 사용되지 않습니다.			리 기능을 사용하여 iOS 또는 Android 플랫폼 암호화를 활성화합니다. 2020년 7월까지 MDX 암호화에서 마이그레이션할 계획을 세우고 테스트했는지 확인하십시오.
암호 장치 정책: Android Enterprise의 **제한 없음** 설정	Android 7 이상을 실행하는 Android Enterprise 기기는 문자 제한이 있는 암호만 지원합니다. 이전에 **필수 문자**를 **제한 없음**으로 설정한 경우, 이 업데이트는 해당 값을 **숫자만**으로 변경합니다.	2019년 2월	2019년 4월	이 변경 사항은 현재 사용자 로그인 환경에 영향을 미치지 않습니다.
원격 지원	클러스터형 온프레미스 XenMobile Server 배포용 원격 지원 클라이언트가 더 이상 사용되지 않습니다.	2019년 1월	2020년 8월	대안 없음
iOS용 Secure Hub 네트워크 확장	Secure Hub 20.3.0 릴리스부터 iOS 장치에 대한 네트워킹 기능을 사용자 지정할 수 있었던 네트워크 확장 프레임워	2018년 10월	2020년 3월	대안 없음

항목	설명	사용 중단 발표	제거됨	대안
	크가 더 이상 사용되지 않습니다.			
TLS 버전 1.0 및 1.1	XenMobile의 보안을 강화하기 위해 Citrix는 이제 TLS(전송 계층 보안) 1.0 및 1.1을 통한 모든 통신을 차단합니다. 보안 약화로 인해 PCI 위원회는 TLS 1.0 및 TLS 1.1을 더 이상 사용하지 않습니다.	2018년 6월	2019년 3월	TLS 1.2로 업그레이드하십시오.
윈도우즈 모바일/CE	Windows Mobile/CE 장치 지원이 중단되었습니다.	2018년 4월	2020년 9월	Windows 10 데스크톱 및 노트북을 사용하십시오.
안드로이드 터치다운	DigiCert에서 Android TouchDown 지원을 중단했습니다. Citrix는 Exchange 장치 정책에서 Android TouchDown 플랫폼 페이지를 제거할 예정입니다.	2018년 7월	2021	권장 사항: Citrix Secure Mail을 사용하십시오.
전체 VPN 터널 - Android	Android 전체 VPN 터널 지원이 중단되었습니다.	2020년 3월	2021년 9월	MAM SDK 웹 SSO 모드.
VPN 모드 전환 허용 - Android	Android VPN 모드 전환 허용 기능 지원이 중단되었습니다.	2020년 3월	2021년 9월	대안 없음

항목	설명	사용 중단 발표	제거됨	대안
인바운드 문서 교환 - Android	Android 인바운드 문서 교환 기능 지원이 중단되었습니다.	2020년 3월	2021년 9월	대안 없음

해결된 문제

XenMobile 10.16에는 다음과 같은 해결된 문제가 포함되어 있습니다.

- XenMobile Server 10.16 버전으로 업그레이드한 후, XenMobile Server가 Syslog 서버로 로그를 보내는 것을 중단했습니다.
- 프록시가 구성된 경우 HTTP v1 API를 사용하는 Firebase Cloud Messaging이 제대로 작동하지 않습니다.
- **MAM 전용** 모드로 등록된 iOS 장치에서 Secure Hub 스토어에서 엔터프라이즈 또는 MDX 앱을 설치할 수 없습니다.
- Android Enterprise 장치에서 **관리형 구성 정책**을 편집하거나 배포할 때 오류가 표시됩니다.
- 앱의 트랙 ID를 구성한 후 XenMobile® Server 콘솔에서 예상 미리 보기 버전의 앱을 볼 수 없습니다. 대신 앱의 프로덕션 버전이 표시됩니다.
- XenMobile Server에서 프로비저닝 프로필 장치 정책이 보류 중인 상태일 때 Secure Hub 스토어에서 MDX 래핑 앱을 설치할 수 없습니다.
- MDM 프로필 갱신 후 ABM 공유 iPad가 관리되지 않는 상태로 전환됩니다.
- APK 서명 스키마 v2 이상 알고리즘을 사용할 때 Android 플랫폼에서 엔터프라이즈 앱을 구성할 수 없습니다.
- device/filter API를 사용하여 장치를 내보낼 수 없습니다.
- NetScaler®에서 nFactor 인증 정책을 사용하여 MAM 및 MDM으로 Android 또는 iOS 장치를 등록하는 경우, 해당 장치는 MDM으로만 등록됩니다.
- XenMobile Server 버전 10.14 이상에서 Citrix Gateway 인증 구성 스크립트를 내보낼 때 스크립트가 잘리고 작동하지 않습니다.
- XenMobile Server에서 설명에 **\b**가 포함된 동기화된 VPP 앱을 다시 편집할 수 없습니다.
- XenMobile Server 버전 10.15 이상에서 OCSP(Online Certificate Status Protocol)가 요청에 응답하지 않습니다.
- XenMobile Server에서 Windows 11을 실행하는 장치를 등록할 수 없습니다.
- Android 장치에서 레거시 MDX Toolkit에서 MAM SDK로 전환하면 Secure Mail 앱이 Secure Hub Store에서 제거됩니다.
- XenMobile Server 콘솔에서 RSR(Rapid Security Response) 버전을 볼 수 없습니다.

- **관리형 Google Play 계정**에서 앱을 다운로드할 수 없습니다.
- XenMobile Server 10.16으로 업그레이드한 후, "제한된 앱 사용"을 사용하는 기존 iOS 제한 장치 정책이 iOS 장치에 배포되지 않습니다.
- ABM 또는 ASM 구성을 사용하는 경우 iOS 공유 장치에 Webclip 장치 정책을 배포할 수 없습니다.
- **Android Enterprise** > **관리형 Google Play 스토어 앱**에 대한 **구성** > **앱** 페이지에서 **앱 구성** 버튼을 볼 수 없습니다.
- **Android Enterprise** 플랫폼용 Wi-Fi 정책을 구성하는 동안 **CA 인증서** 드롭다운 메뉴에서 어떤 값도 볼 수 없습니다. **인증서 선택** 옵션만 표시됩니다.
- 버전 10.15.0 롤링 패치 릴리스의 해결된 문제는 다음을 참조하십시오.
  - XenMobile Server 10.15 롤링 패치 8 릴리스 정보
  - XenMobile Server 10.15 롤링 패치 7 릴리스 정보
  - XenMobile Server 10.15 롤링 패치 6 릴리스 정보
  - XenMobile Server 10.15 롤링 패치 5 릴리스 정보
  - XenMobile Server 10.15 롤링 패치 4 릴리스 정보
  - XenMobile Server 10.15 롤링 패치 3 릴리스 정보

관련 정보

XenMobile 지원 기술 자료 센터

알려진 문제

XenMobile 10.16에는 알려진 문제가 없습니다.

- 모바일 생산성 앱과 관련된 알려진 문제는 Secure Hub, Secure Mail, Secure Web을 참조하십시오.
- 최신 버전 10.15.0 롤링 패치의 알려진 문제는 XenMobile Server 10.15 Rolling Patch 7 릴리스 정보를 참조하십시오.

관련 정보

XenMobile 지원 기술 자료

아키텍처

조직의 장치 및 앱 관리 요구 사항에 따라 XenMobile® 아키텍처의 XenMobile® 구성 요소가 결정됩니다. XenMobile®의 구성 요소는 모듈식이며 서로 기반을 두고 있습니다. 예를 들어, 배포에는 Citrix Gateway가 포함됩니다.

- Citrix Gateway는 사용자에게 모바일 앱에 대한 원격 액세스를 제공하고 사용자 장치 유형을 추적합니다 .
- XenMobile은 이러한 앱과 장치를 관리하는 곳입니다.

XenMobile 구성 요소 배포: 다음 방법으로 사용자가 내부 네트워크의 리소스에 연결할 수 있도록 XenMobile을 배포할 수 있습니다.

- 내부 네트워크 연결. 사용자가 원격인 경우 Citrix Gateway를 통해 VPN 또는 마이크로 VPN 연결을 사용하여 연결할 수 있습니다. 이 연결은 내부 네트워크의 앱 및 데스크톱에 대한 액세스를 제공합니다.
- 장치 등록. 사용자는 XenMobile에 모바일 장치를 등록하여 네트워크 리소스에 연결하는 장치를 XenMobile 콘솔에서 관리할 수 있습니다.
- 웹, SaaS 및 모바일 앱. 사용자는 Secure Hub를 통해 XenMobile에서 웹, SaaS 및 모바일 앱에 액세스할 수 있습니다.
- Windows 기반 앱 및 가상 데스크톱. 사용자는 Citrix Receiver™ 또는 웹 브라우저를 사용하여 StoreFront 또는 Web Interface에서 Windows 기반 앱 및 가상 데스크톱에 액세스할 수 있습니다.

온프레미스 XenMobile Server에 대한 이러한 기능 중 하나를 달성하려면 Citrix는 다음 순서로 XenMobile 구성 요소를 배포할 것을 권장합니다.

- Citrix Gateway. Quick Configuration 마법사를 사용하여 XenMobile, StoreFront™ 또는 Web Interface와 통신할 수 있도록 Citrix Gateway에서 설정을 구성할 수 있습니다. Citrix Gateway에서 Quick Configuration 마법사를 사용하기 전에 다음 구성 요소 중 하나를 설치하여 통신을 설정해야 합니다: XenMobile, StoreFront 또는 Web Interface.
- XenMobile. XenMobile을 설치한 후 XenMobile 콘솔에서 사용자가 모바일 장치를 등록할 수 있도록 정책 및 설정을 구성할 수 있습니다. 모바일, 웹 및 SaaS 앱도 구성할 수 있습니다. 모바일 앱에는 Apple App Store 또는 Google Play의 앱이 포함될 수 있습니다. 사용자는 MDX Toolkit으로 래핑하여 콘솔에 업로드한 모바일 앱에도 연결할 수 있습니다.

- MAM SDK 또는 MDX Toolkit. MDX 래핑 기술은 2023년 7월에 수명 종료(EOL)될 예정입니다. 엔터프라이즈 애플리케이션을 계속 관리하려면 MAM SDK를 통합해야 합니다.

  모바일 애플리케이션 관리(MAM) SDK는 iOS 및 Android 플랫폼에서 다루지 않는 MDX 기능을 제공합니다. iOS 또는 Android 앱을 MDX 지원 및 보안할 수 있습니다. 이러한 앱은 내부 스토어 또는 공용 앱 스토어에서 사용할 수 있습니다. MDX App SDK를 참조하십시오.

- StoreFront (선택 사항). Receiver와의 연결을 통해 StoreFront에서 Windows 기반 앱 및 가상 데스크톱에 대한 액세스를 제공할 수 있습니다.
- Citrix Files(선택 사항). Citrix Files를 배포하는 경우, SAML(Security Assertion Markup Language) ID 공급자 역할을 하는 XenMobile을 통해 엔터프라이즈 디렉터리 통합을 활성화할 수 있습니다. ShareFile용 ID 공급자 구성에 대한 자세한 내용은 ShareFile 지원 사이트를 참조하십시오.

XenMobile은 XenMobile 콘솔을 통해 장치 관리 및 앱 관리를 제공합니다. 이 섹션에서는 XenMobile 배포를 위한 참조 아키텍처에 대해 설명합니다.

프로덕션 환경에서 Citrix는 확장성 및 서버 이중화를 위해 XenMobile 솔루션을 클러스터 구성으로 배포할 것을 권장합니다. 또한 Citrix ADC SSL 오프로드 기능을 사용하면 XenMobile Server의 부하를 더욱 줄이고 처리량을 늘릴 수 있습니다. Citrix ADC에서 두 개의 로드 밸런싱 가상 IP 주소를 구성하여 XenMobile용 클러스터링을 설정하는 방법에 대한 자세한 내용은 클러스터링을 참조하십시오.

재해 복구 배포를 위해 XenMobile을 구성하는 방법에 대한 자세한 내용은 배포 핸드북 재해 복구 문서를 참조하십시오. 이 문서에는 아키텍처 다이어그램이 포함되어 있습니다.

다음 섹션에서는 XenMobile 배포를 위한 다양한 참조 아키텍처에 대해 설명합니다. 참조 아키텍처 다이어그램은 XenMobile 배포 핸드북 문서인 온프레미스 배포를 위한 참조 아키텍처 및 아키텍처를 참조하십시오. 전체 포트 목록은 포트 요구 사항(온프레미스) 및 포트 요구 사항(클라우드)를 참조하십시오.

모바일 장치 관리(MDM) 모드

> **중요:**
>
> MDM 모드를 구성한 후 나중에 ENT 모드로 변경하는 경우, 동일한 (Active Directory) 인증을 사용해야 합니다. XenMobile은 사용자 등록 후 인증 모드 변경을 지원하지 않습니다. 자세한 내용은 XenMobile MDM Edition에서 Enterprise Edition으로 업그레이드를 참조하십시오.

XenMobile MDM Edition은 모바일 장치 관리를 제공합니다. 플랫폼 지원에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오. XenMobile의 MDM 기능만 사용하려는 경우 XenMobile을 MDM 모드로 배포합니다. 예를 들어, 다음을 수행하려는 경우입니다.

- 장치 정책 및 앱 배포.
- 자산 인벤토리 검색.
- 장치 초기화와 같은 장치 작업 수행.

권장 모델에서는 XenMobile Server가 DMZ에 배치되며, 선택적으로 Citrix ADC가 앞에 있어 XenMobile에 대한 추가 보호를 제공합니다.

모바일 앱 관리(MAM) 모드

MAM(MAM 전용 모드라고도 함)은 모바일 앱 관리를 제공합니다. 플랫폼 지원에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오. 장치를 MDM에 등록하지 않고 XenMobile의 MAM 기능만 사용하려는 경우 XenMobile을 MAM 모드로 배포합니다. 예를 들어, 다음을 수행하려는 경우입니다.

- BYO 모바일 장치에서 앱과 데이터를 보호합니다.
- 엔터프라이즈 모바일 앱을 제공합니다.
- 앱을 잠그고 데이터를 지웁니다.

장치를 MDM에 등록할 수 없습니다.

이 배포 모델에서는 XenMobile Server가 Citrix Gateway 앞에 배치되어 XenMobile에 대한 보호를 강화합니다.

MDM+MAM 모드

MDM 및 MAM 모드를 함께 사용하면 모바일 앱 및 데이터 관리와 모바일 장치 관리를 제공합니다. 플랫폼 지원에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오. XenMobile의 MDM+MAM 기능을 사용하려는 경우 XenMobile을 ENT(엔터프라이즈) 모드로 배포합니다. 예를 들어 다음을 수행하려는 경우:

- MDM을 사용하여 회사에서 발행한 장치 관리
- 장치 정책 및 앱 배포
- 자산 인벤토리 검색
- 장치 지우기
- 엔터프라이즈 모바일 앱 제공
- 앱을 잠그고 장치의 데이터를 지웁니다.

권장 배포 모델에서는 XenMobile Server가 Citrix Gateway 앞에 DMZ에 배치되어 XenMobile에 대한 보호를 강화합니다.

내부 네트워크의 XenMobile: 또 다른 배포 옵션은 온프레미스 XenMobile Server를 DMZ가 아닌 내부 네트워크에 배치하는 것입니다. 이 배포는 보안 정책에서 네트워크 어플라이언스만 DMZ에 배치할 수 있도록 요구하는 경우에 사용됩니다. 이 배포에서는 XenMobile Server가 DMZ에 있지 않습니다. 따라서 DMZ에서 SQL Server 및 PKI 서버에 대한 액세스를 허용하기 위해 내부 방화벽에서 포트를 열 필요가 없습니다.

시스템 요구 사항 및 호환성

참고:

이 문서에서는 XenMobile Server 10.16의 시스템 요구 사항 및 호환성에 대해 설명합니다. Endpoint Management의 시스템 요구 사항은 시스템 요구 사항을 참조하십시오.

추가 요구 사항 및 호환성 정보는 다음 문서를 참조하십시오.

- XenMobile 호환성
- 지원되는 장치 운영 체제
- 포트 요구 사항
- 확장성
- 라이선싱
- FIPS 140-2 규정 준수
- 언어 지원

XenMobile 10.16을 실행하려면 다음 최소 시스템 요구 사항이 필요합니다.

- 다음 중 하나:
  - Citrix Hypervisor 8.2 CU1 및 8.4. 자세한 내용은 XenServer를 참조하십시오. Citrix Hypervisor 버전 8.2 CU1 이상에서는 반가상화(PV) VM을 더 이상 지원하지 않습니다. XenServer를 업그레이드하기 전에 하드웨어 가상화 모드(HVM)로 마이그레이션하십시오. 자세한 내용은 Citrix Hypervisor 버전 8.2 CU1 이상에서 HVM 이미지 사용을 참조하십시오. XenServer 업그레이드에 대한 자세한 내용은 XenServer 업그레이드를 참조하십시오.
  - VMware (지원되는 버전: ESXi 6.0, ESXi 6.5.0 Update 3 또는 ESXi 6.7 Update 2 patch 10, ESXi 7.0 Update 3g, ESXi 8.0 Update 2); 자세한 내용은 ESXi 6.7 해결 방법 및 VMware를 참조하십시오.
  - Hyper-V (지원 버전: Windows Server 2016 및 Windows Server 2019); 자세한 내용은 Hyper-V를 참조하십시오.

- Exchange ActiveSync 10.1.10용 Endpoint Management 커넥터 또는 Exchange ActiveSync 8.5.3.19용 Citrix Gateway 커넥터
- 듀얼 코어 프로세서
- 가상 CPU 4개
- 프로덕션 환경용 RAM 8GB; 개념 증명 및 테스트 환경용 RAM 4GB
- 디스크 공간 50GB
- 시트릭스 라이선스 서버 11.16.

  XenMobile® Server를 업그레이드하기 전에 라이선스 서버를 업데이트하십시오.

ESXi 6.7 해결 방법

ESXi 6.7이 작동하려면 다음 해결 방법을 수행해야 합니다.

1. VMware에서 제공하는 OVF 도구를 사용하여 citrix.com에서 다운로드한 OVA 파일을 추출합니다. VMware 페이지에서 OVF 도구를 가져옵니다(https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491).
2. 추출된 세 파일 중 .vmdk 파일을 데이터 저장소에 업로드합니다.
3. 새 가상 머신을 생성합니다.
   a. 가상 머신의 이름을 지정하고 호환성 옵션으로 **ESX/ESXi 4.x 가상 머신**을 선택합니다.
   b. 게스트 OS 제품군으로 **Linux**를 선택합니다.
   c. 게스트 OS 버전의 경우 **Other 2.6.x Linux (64-bit)**를 선택합니다.
   d. 데이터 저장소의 경우 **Default**를 선택합니다.
   e. 사용자 지정 중에 기본 하드 디스크, USB 컨트롤러 및 CD/DVD 드라이브를 제거합니다.
   f. 네트워크에서 어댑터 유형으로 **VMXNET3**를 선택합니다.
   g. ESXi에서 디스크가 로컬인 경우 **SCSI Controller** 및 **LSI Logic Parallel**을 선택합니다. 공유 디스크를 사용하는 경우 **VMware Paravirtual**을 선택합니다.
   h. 다음을 클릭하여 VM 생성을 완료합니다.
4. 데이터 저장소로 이동하여 이전에 업로드한 .vmdk 파일을 복사합니다. XenMobile용으로 생성한 VM 디렉터리에 복사합니다.
5. ESXi 웹 인터페이스에서 VM을 선택하고 설정을 편집합니다.
6. **하드 디스크 추가**를 클릭합니다.
7. 이전에 복사한 .vmdk 파일을 선택하고 VM에 연결합니다.

8. **저장**을 클릭합니다.
9. VM의 전원을 웁니다.

Citrix Gateway 시스템 요구 사항

XenMobile 10.16과 함께 Citrix Gateway를 실행하려면 다음 최소 시스템 요구 사항이 필요합니다.

- Citrix Gateway (온프레미스). 지원되는 버전: 12.1 이상
- 또한 서비스 계정이 필요한 Active Directory와 통신할 수 있어야 합니다. 쿼리 및 읽기 액세스만 필요합니다.

XenMobile 10.16 데이터베이스 요구 사항

XenMobile에는 다음 데이터베이스 중 하나가 필요합니다.

- 마이크로소프트 SQL 서버

  XenMobile은 다음 지원 버전 중 하나를 실행하는 Microsoft SQL Server 데이터베이스를 지원합니다. Microsoft SQL Server 데이터베이스 및 하드웨어 요구 사항에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

  - 마이크로소프트 SQL 서버 2016 SP3
  - 마이크로소프트 SQL 서버 2017 CU 31
  - 마이크로소프트 SQL 서버 2019 CU 25
  - 마이크로소프트 SQL 서버 2022 CU 12

  Microsoft SQL Server 데이터베이스 요구 사항은 배포 규모에 따라 달라집니다. 배포 규모에 따른 Microsoft SQL Server 데이터베이스 요구 사항에 대한 자세한 내용은 확장성을 참조하십시오.

  XenMobile은 데이터베이스 고가용성을 위해 SQL 기본 가용성 그룹(Always On 가용성 그룹) 및 SQL 클러스터링을 지원합니다.

  Citrix는 Microsoft SQL을 원격으로 사용하는 것을 권장합니다.

  Microsoft SQL 업그레이드에 대한 자세한 내용은 Microsoft 문서 SQL Server 업그레이드를 참조하십시오.

- PostgreSQL (테스트 환경 전용). PostgreSQL은 XenMobile에 포함되어 있습니다. 테스트 환경에서 로컬 또는 원격으로 사용할 수 있습니다. 데이터베이스 마이그레이션은 지원되지 않습니다. 테스트 환경에서 생성된 데이터베이스를 프로덕션 환경으로 이동할 수 없습니다.

모든 XenMobile 에디션은 다음 제한 사항과 함께 Windows용 원격 PostgreSQL 9.5.1 및 9.5.11을 지원합니다: 프로덕션 환경에는 권장되지 않습니다. 최대 300개 장치 지원. 300개 이상의 장치에는 온프레미스 SQL Server를 사용하십시오. 클러스터링은 지원되지 않습니다.

SQL Server 서비스 계정 요구 사항

XenMobile과 함께 사용할 SQL Server의 서비스 계정에 `DBcreator` 역할 권한이 있는지 확인하십시오. XenMobile Server 설치 중에 지정하는 SQL Server 계정 암호를 기록해 두십시오. XenMobile Server 복구 중에 XenMobile 데이터베이스를 복제해야 하는 경우 해당 암호가 필요합니다.

투명한 데이터 암호화(TDE)를 사용하여 SQL Server 데이터베이스를 보호하십시오. 온프레미스 배포를 위한 참조 아키텍처에 표시된 참조 아키텍처와 같이 SQL Server 포트에 대한 외부 액세스를 허용하지 마십시오.

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

- Windows 서비스 계정 및 권한 구성
- 서버 수준 역할

버추얼 앱스 앤 데스크톱스 호환성

- 버추얼 앱스 앤 데스크톱스 7.15 LTSR CU3
- 가상 앱 및 데스크톱 7.1811
- 가상 앱 및 데스크톱 7 1906
- 가상 앱 및 데스크톱 7 1909
- 가상 앱 및 데스크톱 7 2006

StoreFront™ 호환성

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

기타 호환성

- 익스체인지 액티브싱크용 엔드포인트 관리 커넥터 10.1.10
  - 이전 버전은 테스트되지 않았습니다.
- 익스체인지 액티브싱크용 Citrix Gateway 커넥터 8.5.3.19
  - 이전 버전은 테스트되지 않았습니다.

XenMobile® 호환성

> **참고:**
>
> 이 문서에서는 XenMobile Server 호환성에 대해 설명합니다. Endpoint Management로 테스트된 구성 요소에 대한 자세한 내용은 Endpoint Management 호환성을 참조하십시오.

> 새로운 기능, 수정 사항 및 정책 업데이트를 사용하려면 Citrix®에서 다음의 최신 버전을 설치할 것을 권장합니다.

- Citrix는 MDX 기능을 앱에 적용하기 위해 Mobile Application Management (MAM) SDK를 엔터프라이즈 iOS 및 Android 앱과 통합할 것을 권장합니다.

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

이 문서에서는 통합할 수 있는 지원되는 XenMobile 구성 요소 버전을 요약합니다.

호환성 및 업그레이드 경로

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

모바일 생산성 앱의 최신 버전에는 Secure Hub의 최신 버전이 필요합니다. 앱의 이전 두 버전은 최신 Secure Hub와 호환됩니다. 자세한 내용은 Citrix 제품 매트릭스를 참조하십시오.

Citrix는 XenMobile 생산성 앱의 배포를 공개 앱 스토어를 통해서만 지원합니다.

XenMobile Server (온프레미스)

- Citrix는 XenMobile Server의 이전 두 버전에서 업그레이드를 지원합니다.

- XenMobile Server 최신 버전: XenMobile Server 10.16
- 다음에서 업그레이드:
  - XenMobile Server 10.15.x 버전
  - XenMobile Server 10.14.x 버전

모바일 생산성 앱

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

모바일 생산성 앱의 2주 단계별 릴리스 주기에 대한 자세한 내용은 릴리스 타임라인을 참조하십시오. 지원 세부 정보는 모바일 생산성 앱 지원을 참조하십시오.

MAM SDK

MAM SDK는 iOS 및 Android 플랫폼에서 다루지 않는 MDX 기능을 제공합니다. 이러한 앱은 내부 스토어 또는 공용 앱 스토어에서 사용할 수 있습니다. MDX App SDK를 참조하십시오.

MDX 툴킷

MDX 래핑 기술은 2023년 7월에 수명 종료(EOL)될 예정입니다. 엔터프라이즈 애플리케이션을 계속 관리하려면 MAM SDK를 통합해야 합니다.

Citrix는 MDX Toolkit의 최신 3개 릴리스(n.n.n)를 지원합니다. MDX Toolkit의 새로운 기능을 참조하십시오.

브라우저 지원

XenMobile Server 콘솔에는 다음 지원되는 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

> **참고:**

> 이 문서에서는 XenMobile Server에서 지원되는 장치 운영 체제에 대해 설명합니다. Endpoint Management에서 지원되는 운영 체제에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오.

> XenMobile®은 앱 및 장치 관리를 포함한 엔터프라이즈 모빌리티 관리를 위해 다음 플랫폼 및 운영 체제를 실행하는 장치를 지원합니다. 플랫폼 제한 및 보안 기능으로 인해 XenMobile은 모든 플랫폼에서 모든 기능을 지원하지는 않습니다.

> **참고:**

> XenMobile Server는 Windows x86 및 ARM 유형 장치에 대한 장치 관리를 지원합니다.

> 이 문서의 지원되는 장치 플랫폼 정보는 Exchange ActiveSync용 XenMobile 커넥터 및 Exchange ActiveSync용 Citrix Gateway 커넥터™에도 적용됩니다.

모바일 생산성 앱의 최신 버전 및 MDX 암호화에 지원되는 장치에 대한 자세한 내용은 모바일 생산성 앱 지원을 참조하십시오.

> **참고:**

> Citrix®는 최소한 각 주요 운영 체제 플랫폼의 현재 버전과 이전 버전을 지원합니다. Endpoint Management의 최신 버전의 모든 기능이 이전 플랫폼 릴리스에서 작동하는 것은 아닙니다.

> 사용 중단 공지에 대한 자세한 내용은 사용 중단을 참조하십시오.

운영 체제 지원 목록

Citrix XenMobile은 다음 운영 체제를 지원합니다.

- **안드로이드:** 10.x, 11.x, 12.x, 13.x, 14.x, 15.x, 16.x, 17.x

  Android 10 이상 버전에 대한 자세한 내용은 Android 고려 사항을 참조하십시오.

- **iOS:** 버전 13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  XenMobile 및 Citrix 모바일 앱은 iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x, iOS 18.x, iOS 26.x 및 iOS 27.x와 호환되지만, 현재 모든 새로운 iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x, iOS 18.x, iOS

26.x 및 iOS 27.x 기능을 지원하지 않습니다. iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x, iOS 18.x, iOS 26.x 및 iOS 27.x용 사내 엔터프라이즈 앱을 래핑하려면 MDX Toolkit 21.8.5 이상을 사용하거나 MAM SDK를 사용하여 앱을 준비하십시오.

- **iPadOS:** 버전 13.x, 14.x, 15.x, 16.x, 17.x, 18.x,26.x, 27.x

  XenMobile 및 Citrix 모바일 앱은 iPadOS 14.x, iPadOS 15.x, iPadOS 16.x, iPadOS 17.x, iPadOS 18.x, iPadOS 26.x 및 iPadOS 27.x와 호환되지만, 현재 모든 새로운 iPadOS 14.x, iPadOS 15.x, iPadOS 16.x, iPadOS 17.x, iPadOS 18.x, iPadOS 26.x 및 iPadOS 27.x 기능을 지원하지 않습니다.

- **macOS 버전:** 11.x, 12.x, 13.x, 14.x, 15.x

  XenMobile 및 Citrix 모바일 앱은 macOS 11, macOS 12, macOS 13, macOS 14 및 macOS 15와 호환되지만, 현재 macOS 11, macOS 12, macOS 13, macOS 14 및 macOS 15의 모든 새로운 기능을 지원하지 않습니다.

- **Windows 데스크톱 및 태블릿:** (MDM 전용). Windows 10 및 Windows 11

Android 고려 사항

> **중요:**
>
> 장치 관리 모드는 더 이상 지원되지 않습니다. 자세한 내용은 장치 관리에서 Android Enterprise로 마이그레이션을 참조하십시오.

- Citrix는 Android 장치를 레거시 장치 관리 모드에 등록하지 않도록 권장합니다. Google은 Android 10 이상을 실행하는 장치에 영향을 미치는 장치 관리 API를 더 이상 사용하지 않습니다. 레거시 장치 관리 모드에서 Android 장치를 등록하는 데 실패합니다. Citrix는 Android 11 장치를 장치 관리 모드에 등록하는 것을 지원하지 않습니다.
- Citrix는 Android 10 장치에 Android Enterprise를 사용할 것을 권장합니다. 자세한 내용은 장치 관리에서 Android Enterprise로 마이그레이션을 참조하십시오.
- Google API 변경 사항은 MAM 전용 모드에 등록된 장치에는 영향을 미치지 않습니다.

업그레이드하기 전에:

- 서버 인프라가 subjectAltName (SAN) 확장명에 일치하는 호스트 이름이 있는 보안 인증서를 준수하는지 확인하십시오.
- 호스트 이름을 확인하려면 서버는 일치하는 SAN이 있는 인증서를 제시해야 합니다. Citrix는 호스트 이름과 일치하는 SAN이 있는 경우에만 인증서를 신뢰합니다.

포트 요구 사항

장치와 앱이 XenMobile®과 통신할 수 있도록 방화벽에서 특정 포트를 열어야 합니다. 다음 표에는 열어야 하는 포트가 나열되어 있습니다.

앱 관리를 위한 Citrix Gateway 및 XenMobile용 개방형 포트

Citrix Secure Hub™, Citrix Receiver 및 Citrix Gateway 플러그인을 통해 Citrix Gateway에서 다음 구성 요소로 사용자 연결을 허용하려면 다음 포트를 엽니다.

- XenMobile
- StoreFront™
- 시트릭스 가상 앱 및 데스크톱™
- Exchange ActiveSync용 시트릭스 게이트웨이 커넥터™
- 인트라넷 웹사이트와 같은 기타 내부 네트워크 리소스

Citrix ADC에서 Launch Darkly로 트래픽을 활성화하려면 이 지원 기술 자료 문서에 언급된 IP 주소를 사용할 수 있습니다.

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

TCP 포트	설명	원본	대상
21 또는 22	지원 번들을 FTP 또는 SCP 서버로 보내는 데 사용됩니다.	XenMobile	FTP 또는 SCP 서버
53 (TCP 및 UDP)	DNS 연결에 사용됩니다.	시트릭스 게이트웨이, 젠모바일	DNS 서버
80	Citrix Gateway는 두 번째 방화벽을 통해 VPN 연결을 내부 네트워크 리소스로 전달합니다. 이 상황은 일반적으로 사용자가 Citrix Gateway 플러그인을 사용하여 로그온할 때 발생합니다.	시트릭스 게이트웨이	인트라넷 웹 사이트

TCP 포트	설명	원본	대상
80 또는 8080; 443	열거, 티켓팅 및 인증에 사용되는 XML 및 Secure Ticket Authority (STA) 포트입니다. Citrix는 포트 443을 사용하는 것을 권장합니다.	StoreFront 및 Web Interface XML 네트워크 트래픽; Citrix Gateway STA	가상 앱 또는 데스크톱
123 (TCP 및 UDP)	네트워크 시간 프로토콜(NTP) 서비스에 사용됩니다.	시트릭스 게이트웨이; 젠모바일	NTP 서버
389	안전하지 않은 LDAP 연결에 사용됩니다.	시트릭스 게이트웨이; 젠모바일	LDAP 인증 서버 또는 Microsoft Active Directory
443	Citrix Receiver™ 또는 Receiver for Web에서 StoreFront로, 가상 앱 및 데스크톱으로 연결하는 데 사용됩니다.	인터넷	시트릭스 게이트웨이
443	웹, 모바일 및 SaaS 앱 전송을 위해 XenMobile에 연결하는 데 사용됩니다.	인터넷	시트릭스 게이트웨이
443	XenMobile Server와의 일반적인 장치 통신에 사용됩니다.	XenMobile	XenMobile
443	모바일 장치에서 XenMobile로의 등록 연결에 사용됩니다.	인터넷	XenMobile
443	XenMobile에서 Exchange ActiveSync용 Citrix Gateway 커넥터로의 연결에 사용됩니다.	XenMobile	시트릭스 게이트웨이 Exchange ActiveSync용 커넥터

TCP 포트	설명	원본	대상
443	Exchange ActiveSync용 Citrix Gateway 커넥터에서 XenMobile으로의 연결에 사용됩니다.	Exchange ActiveSync용 시트릭스 게이트웨이 커넥터	XenMobile
443	인증서 인증이 없는 배포에서 콜백 URL에 사용됩니다.	XenMobile	시트릭스 게이트웨이
514	XenMobile과 syslog 서버 간의 연결에 사용됩니다.	XenMobile	Syslog 서버
636	보안 LDAP 연결에 사용됩니다.	시트릭스 게이트웨이; 젠모바일	LDAP 인증 서버 또는 Active Directory
1494	내부 네트워크의 Windows 기반 애플리케이션에 대한 ICA® 연결에 사용됩니다. Citrix는 이 포트를 열어 두는 것을 권장합니다.	시트릭스 게이트웨이	가상 앱 또는 데스크톱
1812	RADIUS 연결에 사용됩니다.	시트릭스 게이트웨이	RADIUS 인증 서버
2598	세션 안정성을 사용하여 내부 네트워크의 Windows 기반 애플리케이션에 대한 연결에 사용됩니다. Citrix는 이 포트를 열어 두는 것을 권장합니다.	시트릭스 게이트웨이	가상 앱 또는 데스크톱
3268	Microsoft 글로벌 카탈로그의 안전하지 않은 LDAP 연결에 사용됩니다.	시트릭스 게이트웨이; 젠모바일	LDAP 인증 서버 또는 Active Directory

TCP 포트	설명	원본	대상
3269	Microsoft Global Catalog 보안 LDAP 연결에 사용됩니다.	시트릭스 게이트웨이; 젠모바일	LDAP 인증 서버 또는 Active Directory
9080	Citrix ADC와 Exchange ActiveSync용 Citrix Gateway 커넥터 간의 HTTP 트래픽에 사용됩니다.	시트릭스 ADC	Exchange ActiveSync용 시트릭스 게이트웨이 커넥터
30001	HTTPS 서비스의 초기 스테이징을 위한 관리 API	내부 LAN	젠모바일 서버
9443	Citrix ADC와 Exchange ActiveSync용 Citrix Gateway 커넥터 간의 HTTPS 트래픽에 사용됩니다.	시트릭스 ADC	익스체인지 액티브싱크용 시트릭스 게이트웨이 커넥터
45000; 80	클러스터에 배포된 경우 두 XenMobile VM 간의 통신에 사용됩니다. 포트 80은 노드 간 통신 및 SSL 오프로드에 사용됩니다.	XenMobile	XenMobile
8443	등록, XenMobile Store 및 모바일 앱 관리(MAM)에 사용됩니다.	XenMobile; Citrix Gateway; 장치; 인터넷	XenMobile
4443	관리자가 브라우저를 통해 XenMobile 콘솔에 액세스하는 데 사용됩니다. 또한 한 노드에서 모든 XenMobile 클러스터 노드의 로그 및	액세스 지점(브라우저); XenMobile	XenMobile

TCP 포트	설명	원본	대상
	지원 번들을 다운로드하는 데 사용됩니다.		
27000	외부 Citrix License Server에 액세스하는 데 사용되는 기본 포트입니다.	XenMobile	Citrix 라이선스 서버
7279	Citrix 라이선스를 체크인 및 체크아웃하는 데 사용되는 기본 포트입니다.	XenMobile	Citrix 벤더 데몬
161	UDP 프로토콜을 사용하는 SNMP 트래픽에 사용됩니다.	SNMP 관리자	XenMobile
162	XenMobile에서 SNMP 관리자로 SNMP 트랩 경고를 보내는 데 사용됩니다. 소스는 XenMobile이고 대상은 SNMP 관리자입니다.	XenMobile	SNMP 관리자

장치 관리를 위해 XenMobile 포트 열기

XenMobile이 네트워크에서 통신할 수 있도록 다음 포트를 엽니다.

TCP 포트	설명	원본	대상
25	XenMobile 알림 서비스의 기본 SMTP 포트입니다. SMTP 서버가 다른 포트를 사용하는 경우 방화벽에서 해당 포트를 차단하지 않는지 확인하십시오.	XenMobile	SMTP 서버
80 및 443	Apple iTunes App Store 또는 Google	XenMobile	`ax.apps.apple.com` 및

TCP 포트	설명	원본	대상
	Play에 대한 Enterprise App Store 연결(80 사용 필수). Apple 볼륨 구매에 사용됩니다. iOS 또는 Android용 Secure Hub에서 앱 스토어의 앱을 게시하는 데 사용됩니다.		`*.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	XenMobile과 Nexmo SMS 알림 릴레이 간의 아웃바운드 연결에 사용됩니다.	XenMobile	Nexmo SMS 릴레이 서버
389	안전하지 않은 LDAP 연결에 사용됩니다.	XenMobile	LDAP 인증 서버 또는 Active Directory
443	Android용 등록 및 에이전트 설정에 사용됩니다.	인터넷	XenMobile
443	Android 및 Windows 장치와 MDM 원격 지원 클라이언트의 등록 및 에이전트 설정에 사용됩니다.	인터넷 LAN 및 Wi-Fi	XenMobile
1433	원격 데이터베이스 서버 연결에 기본적으로 사용됩니다(선택 사항).	XenMobile	SQL 서버
443 or 2197	`*.push.apple.com`에 APN 알림을 보내는 데 사용됩니다.	XenMobile	인터넷(공용 IP 주소 17.0.0.0/8을 사용하는 APN 호스트
5223	iOS 장치에서 `*.push.apple.com`	iOS 장치	인터넷(공용 IP 주소 17.0.0.0/8을 사용하는 APN 호스트)

TCP 포트	설명	원본	대상
	으로의 APN 아웃바운드 연결에 사용됩니다.		
8081	선택적 MDM 원격 지원 클라이언트의 앱 터널에 사용됩니다. 기본값은 8081입니다.	원격 지원 클라이언트	XenMobile
8443	iOS 장치 등록에 사용됩니다.	인터넷; LAN 및 Wi-Fi	XenMobile

AutoDiscovery 서비스 연결을 위한 포트 요구 사항

이 포트 구성은 Android용 Secure Hub에서 연결하는 Android 장치가 내부 네트워크 내에서 Citrix AutoDiscovery Service(ADS)에 액세스할 수 있도록 합니다. ADS를 통해 제공되는 보안 업데이트를 다운로드하려면 ADS에 액세스해야 합니다.

> **참고:**

> ADS 연결이 프록시 서버를 지원하지 않을 수 있습니다. 이 시나리오에서는 ADS 연결이 프록시 서버를 우회하도록 허용하십시오.

> 인증서 고정을 활성화하려면 다음 전제 조건을 수행하십시오.

- **XenMobile Server 및 Citrix ADC 인증서를 수집합니다.** 인증서는 PEM 형식이어야 하며 개인 키가 아닌 공개 인증서여야 합니다.
- **Citrix 지원팀에 문의하여 인증서 고정 활성화 요청을 제출합니다.** 이 과정에서 인증서를 요청받게 됩니다.

인증서 고정은 장치가 등록하기 전에 ADS에 연결해야 합니다. 이 요구 사항은 최신 보안 정보가 Secure Hub에서 사용 가능하도록 합니다. Secure Hub가 장치를 등록하려면 장치가 ADS에 도달해야 합니다. 따라서 내부 네트워크 내에서 ADS 액세스를 개방하는 것은 장치 등록을 활성화하는 데 중요합니다.

Android 또는 iOS용 Secure Hub에서 ADS에 대한 액세스를 허용하려면 다음 FQDN에 대해 포트 443을 여십시오.

FQDN	포트	IP 및 포트 사용
`discovery.cem.cloud.us`	443	Secure Hub - CloudFront를 통한 ADS 통신

지원되는 IP 주소에 대한 자세한 내용은 AWS의 클라우드 기반 스토리지 센터를 참조하십시오.

Android Enterprise 네트워크 요구 사항

Android Enterprise용 네트워크 환경을 설정할 때 고려해야 할 아웃바운드 연결에 대한 자세한 내용은 Google 지원 문서, Android Enterprise 네트워크 요구 사항을 참조하십시오.

XenMobile용 포트 요구 사항

Managed Google Play Enterprise를 생성하고 Managed Google Play iFrame에 액세스하려면 다음 대상 호스트에 네트워크에서 연결할 수 있어야 합니다. Google은 앱 검색 및 승인을 간소화하기 위해 EMM 개발자에게 Managed Play iFrame을 제공했습니다. Managed Play iFrame을 사용하려면 XenMobile 콘솔에 액세스하는 브라우저가 Google Play에 액세스할 수 있어야 합니다.

대상 호스트	포트	설명
`play.google.com`	TCP/443	Google Play 스토어, Play Enterprise 가입에 사용됩니다.
`*.googleapis.com`	TCP/443	Google Mobile Management, Google API, Google Play 스토어 API, FCM에 사용됩니다.
`accounts.youtube.com`, `accounts.google.com`	TCP/443	계정 인증에 사용됩니다.
`apis.google.com`	TCP/443	Google 웹 서비스에 사용됩니다.
`ogs.google.com`	TCP/443	iFrame UI 요소에 사용됩니다.
`notifications.google.com`	TCP/443	데스크톱 및 모바일 알림에 사용됩니다.
`fonts.googleapis.com`, `*.gstatic.com`, `*.googleusercontent.com`	TCP/443	Google Fonts 사용자 생성 콘텐츠에 사용됩니다. 예를 들어, 스토어의 앱 아이콘 등이 있습니다.

대상 호스트	포트	설명
`cri.pki.goog`, `ocsp.pki.goog`	TCP/443	인증서 유효성 검사에 사용됩니다.

확장성 및 성능

XenMobile® 인프라의 규모를 이해하는 것은 XenMobile을 배포하고 구성하는 방법에 중요한 역할을 합니다. 이 문서에는 확장성 테스트 데이터와 소규모에서 대규모 온프레미스 XenMobile 엔터프라이즈 배포를 위한 성능 및 확장성 인프라 요구 사항을 결정하는 방법에 대한 지침이 포함되어 있습니다.

여기서 확장성은 배포에 이미 등록된 장치가 동시에 배포에 다시 연결할 수 있는 능력에 따라 정의됩니다.

- *확장성*은 배포에 등록된 최대 장치 수로 정의됩니다.
- *로그인 속도*는 기존 장치가 배포에 다시 연결할 수 있는 최대 속도로 정의됩니다.

이 문서의 데이터는 10,000대에서 75,000대 규모의 배포에 대한 테스트에서 파생되었습니다. 테스트는 알려진 워크로드를 사용하는 모바일 장치로 구성되었습니다.

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

테스트는 Citrix Gateway 8200을 사용하여 수행되었습니다. 유사하거나 더 큰 용량의 Citrix ADC 어플라이언스는 유사하거나 더 큰 확장성 및 성능을 제공할 것으로 예상됩니다.

확장성 테스트 결과 요약은 다음과 같습니다.

최대 75,000대 장치 배포를 위한 확장성 테스트 결과 요약

로그인 속도 (기존 사용자의 재연결 속도) — 시간당 최대 9,375대 장치

사용된 구성:

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

장치 수 및 하드웨어 구성별 테스트 결과

장치 수	12,500	30,000	60,000	75,000
시간당 기존 장치 재연결 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 어플라이언스	메모리 = 8 GB RAM; vCPUs = 4	메모리 = 16 GB RAM; vCPUs = 6	메모리 = 24 GB RAM; vCPUs = 8	메모리 = 24 GB RAM; vCPUs = 8
액티브 디렉터리	메모리 = 4 GB RAM; vCPUs = 2	메모리 = 8 GB RAM; vCPU = 4	메모리 = 16 GB RAM; vCPU = 4	메모리 = 16 GB RAM; vCPU = 4
Microsoft SQL Server 외부 데이터베이스	메모리 = 8 GB RAM; vCPU = 4	메모리 = 16 GB RAM; vCPU = 8	메모리 = 24 GB RAM; vCPU = 16	메모리 = 24 GB RAM; vCPU = 16

확장성 프로필

액티브 디렉터리 구성	사용된 프로필
사용자	100,000
그룹	200,000
중첩 수준	5

XENMOBILE SERVER 구성	총계	사용자당
정책	20	20
앱	270	50
공개 앱	200	0

XENMOBILE SERVER 구성	총계	사용자당
MDX	50	30
웹 및 SaaS	20	20
작업	50	
전달 그룹	20	
전달 그룹당 Active Directory 그룹	10	
SQL		
데이터베이스 수	1	

장치 연결 및 앱 활동

이 확장성 테스트는 배포에 등록된 장치가 8시간 동안 다시 연결하는 능력에 대한 데이터를 수집했습니다.

이 테스트는 다시 연결하는 장치가 모든 권한이 부여된 보안 정책을 얻는 재연결 간격을 시뮬레이션하여 XenMobile Server 노드에 평소보다 높은 부하 조건을 가했습니다. 이후 재연결 시에는 변경되거나 새로운 정책만 iOS 장치로 푸시되어 XenMobile Server 노드의 부하가 줄어듭니다.

이 테스트에서는 iOS 장치 50%와 Android 장치 50%를 혼합하여 사용했습니다.

이 테스트는 다시 연결하는 Android 장치가 이전에 GCM 알림을 받았다고 가정합니다.

8시간 테스트 간격 동안 다음 앱 관련 활동이 발생했습니다.

- Secure Hub가 한 번 열려 권한이 부여된 앱을 열거했습니다.
- SAML 웹 앱 2개가 열렸습니다.
- MAM 앱 4개가 다운로드되었습니다.
- Secure Mail에서 사용할 STA 1개가 생성되었습니다.
- 마이크로 VPN을 통한 각 Secure Mail 재연결 이벤트에 대해 240개의 STA 티켓 유효성 검사가 수행되었습니다.

참조 아키텍처

이 확장성 테스트에 사용된 배포를 위한 참조 아키텍처는 온프레미스 배포를 위한 참조 아키텍처의 "핵심 MAM+MDM 참조 아키텍처"를 참조하십시오.

주의 사항 및 제한 사항

이 문서의 확장성 테스트 결과를 고려할 때 다음 사항에 유의하십시오.

- Windows 플랫폼은 테스트되지 않았습니다.
- 정책 푸시는 iOS 및 Android 장치에 대해 테스트되었습니다.
- 각 XenMobile Server 노드는 동시에 최대 12,000개의 장치를 지원합니다.

라이선스

XenMobile Server는 이제 License Activation Service (LAS) 라이선싱 메커니즘을 지원합니다. LAS는 Citrix 제품군 전반에 걸쳐 기존 파일 기반 라이선싱에 대한 최신 대안을 제공하는 새로운 클라우드 기반 라이선싱 솔루션입니다. License Activation Service가 보유한 라이선스 및 권한을 사용하려면 Citrix License Server를 Citrix Cloud에 등록하십시오. 자세한 내용은 License Activation Service를 참조하십시오.

중요:

- April 15, 2026까지 새로운 라이선싱 모델을 채택하십시오. 자세한 내용은 Citrix Modern Licensing Announcement를 참조하십시오.
- Citrix® 라이선스 반환 및 수정 절차는 November 4, 2020부로 변경되었습니다. 자세한 내용은 다음 문서를 참조하십시오.
  - 내 계정을 사용하여 라이선스를 반환하는 방법
  - 라이선스 파일을 재할당하는 방법

XenMobile®은 Citrix Licensing을 사용하여 라이선스를 관리합니다. XenMobile Server 및 Citrix Gateway에는 라이선스가 필요합니다.

Citrix Gateway 라이선싱에 대한 자세한 내용은 Citrix Gateway 설명서를 참조하십시오. Citrix Licensing에 대한 자세한 내용은 The Citrix Licensing System을 참조하십시오.

XenMobile Server를 구매하면 라이선스 활성화 지침이 포함된 주문 확인 이메일 메시지를 받게 됩니다. 신규 고객은 주문하기 전에 라이선스 프로그램에 등록해야 합니다. XenMobile 라이선싱 모델 및 프로그램에 대한 자세한 내용은 XenMobile licensing을 참조하십시오.

요구 사항

- XenMobile Server의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.16.x 이상으로 업데이트하십시오. 이전 라이선스 서버 버전은 XenMobile의 최신 버전을 지원하지 않습니다.
- XenMobile 라이선스를 다운로드하기 전에 Citrix Licensing을 설치해야 합니다. 라이선스 파일을 생성하려면 Citrix Licensing을 설치한 서버의 이름이 필요합니다. XenMobile을 설치하면 Citrix Licensing이 기본적으로 서버에 설치됩니다. 또는 기존 Citrix Licensing 배포를 사용하여 XenMobile 라이선스를 관리할 수 있습니다. Citrix Licensing 설치, 배포 및 관리에 대한 자세한 내용은 Licensing Your Product를 참조하십시오.
- XenMobile의 노드 또는 인스턴스를 클러스터링하려는 경우 원격 서버에서 Citrix Licensing을 사용해야 합니다.
- Citrix는 수신하는 모든 라이선스 파일의 로컬 복사본을 보관할 것을 권장합니다. 구성 파일의 백업 복사본을 저장하면 모든 라이선스 파일이 백업에 포함됩니다. 그러나 구성 파일을 먼저 백업하지 않고 XenMobile을 다시 설치하는 경우 원본 라이선스 파일이 필요합니다.

XenMobile 라이선싱 고려 사항

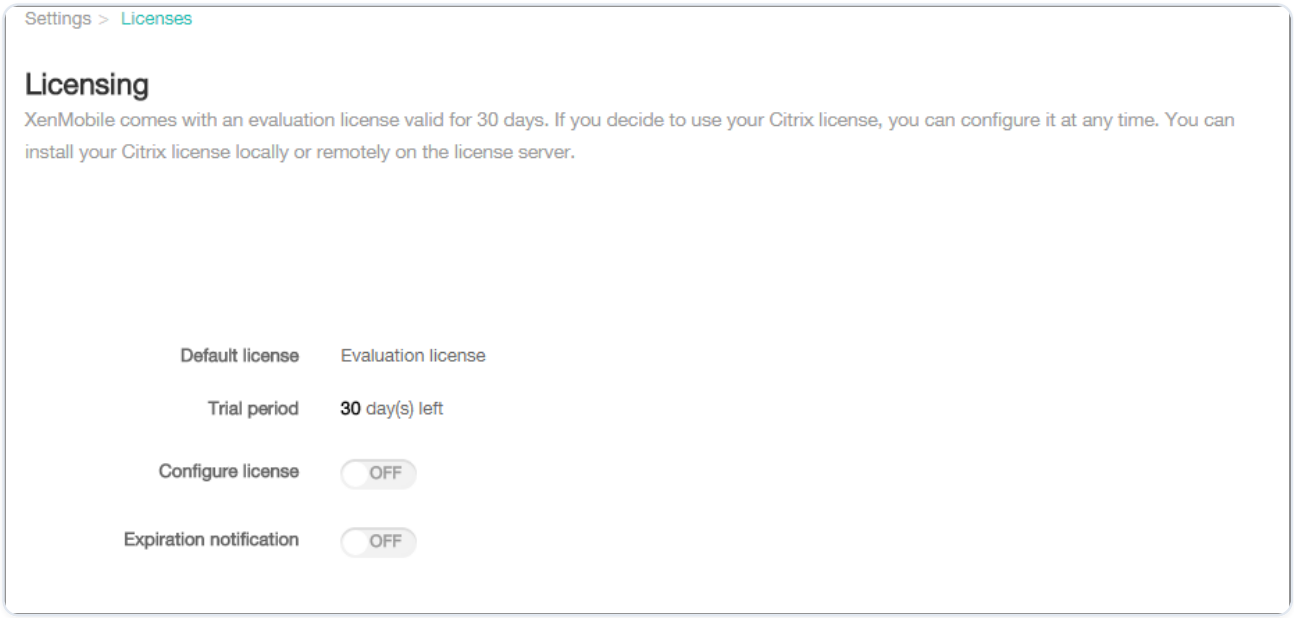
라이선스가 없는 경우, XenMobile은 30일의 유예 기간 동안 모든 기능을 갖춘 평가판 모드로 작동합니다. 이 평가판 모드는 XenMobile을 설치할 때 시작되는 30일 기간 동안 한 번만 사용할 수 있습니다. 유효한 XenMobile 라이선스 유무에 관계없이 XenMobile 웹 콘솔에 대한 액세스는 차단되지 않습니다. XenMobile 콘솔에서 평가판 기간이 며칠 남았는지 확인할 수 있습니다.

XenMobile은 여러 라이선스를 업로드할 수 있도록 허용하지만, 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 없으며, 등록된 장치에 배포된 앱 및 구성을 업데이트할 수 없습니다. XenMobile 라이선싱 모델 및 프로그램에 대한 자세한 내용은 XenMobile 라이선싱을 참조하십시오.

XenMobile 콘솔에서 라이선싱 페이지를 찾는 방법

XenMobile을 설치한 후 **라이선싱** 페이지가 처음 나타나면 라이선스는 기본 30일 평가판 모드로 설정되며 아직 구성되지 않은 상태입니다. 이 페이지에서 라이선스를 추가하고 구성할 수 있습니다.



1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **라이선싱**을 클릭합니다. **라이선싱** 페이지가 나타납니다.

로컬 라이선스 추가

새 라이선스를 추가하면 테이블에 나타납니다. 처음 추가된 라이선스는 자동으로 활성화됩니다. Enterprise 및 유형과 같이 동일한 범주의 라이선스를 여러 개 추가하는 경우, 이 라이선스들은 테이블의 한 행에 나타납니다. 이 경우 **총 라이선스 수** 및 **사용 중인 수**는 공통 라이선스의 총량을 반영합니다. **만료일**은 공통 라이선스 중 가장 늦은 만료일을 보여줍니다.

모든 로컬 라이선스는 XenMobile 콘솔을 통해 관리합니다.

1. Simple License Service, License Administration Console을 통해 또는 Citrix.com 계정에서 직접 라이선스 파일을 가져옵니다. 자세한 내용은 Citrix 라이선싱 설명서를 참조하십시오.
2. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
3. **라이선싱**을 클릭합니다. **라이선싱** 페이지가 나타납니다.
4. **Configure license**를 **On**으로 설정합니다. **License type** 목록, **Add** 버튼, **Licensing** 테이블이 나타납니다. **Licensing** 테이블에는 XenMobile과 함께 사용한 라이선스가 있습니다. Citrix 라이선스를 아직 추가하지 않은 경우 테이블은 비어 있습니다.

   라이선스 구성 화면 이미지(/en-us/xenmobile/server/media/configure-license.png)
5. **License type**이 **Local license**로 설정되어 있는지 확인한 다음 **Add**를 클릭합니다. **Add New License** 대화 상자가 나타납니다.

라이선스 구성 화면 이미지(/en-us/xenmobile/server/media/add-license.png)

6. **Add New License** 대화 상자에서 **Choose File**을 클릭한 다음 라이선스 파일 위치를 찾습니다.
7. **Upload**를 클릭합니다. 라이선스가 로컬로 업로드되어 테이블에 나타납니다.

   라이선스 구성 화면 이미지(/en-us/xenmobile/server/media/uploaded-local-license.png)
8. **Licensing** 페이지의 테이블에 라이선스가 나타나면 활성화합니다. 라이선스가 테이블에서 첫 번째인 경우 자동으로 활성화됩니다.

원격 라이선스를 추가하려면

원격 Citrix Licensing 서버를 사용하는 경우 Citrix Licensing 서버를 사용하여 *모든* 라이선스 활동을 관리합니다. 자세한 내용은 Licensing Your Product를 참조하십시오.

1. 라이선스 서버 인증서를 XenMobile Server로 가져옵니다 (**Settings > Certificates**).
2. 기본적으로 Microsoft PKI 서버를 제외한 아웃바운드 연결에서는 호스트 이름 확인이 활성화되어 있습니다. 호스트 이름 확인으로 인해 배포가 중단되는 경우 서버 속성 **disable.hostname.verification**을 **true**로 변경하십시오. 이 속성의 기본값은 **false**입니다.

   호스트 이름 확인에 실패하면 서버 로그에 다음과 같은 오류가 포함됩니다. “볼륨 구매 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다.”
3. **Licensing** 페이지에서 **Configure license**를 **On**으로 설정합니다. **License type** 목록, **Add** 버튼, **Licensing** 테이블이 나타납니다. **Licensing** 테이블에는 XenMobile과 함께 사용한 라이선스가 있습니다. Citrix 라이선스를 아직 추가하지 않은 경우 테이블은 비어 있습니다.
4. **License type**을 **Remote license**로 설정합니다. **License server** 및 **Port** 필드와 **Test Connection** 버튼이 **Add** 버튼을 대체합니다.

   Licensing 구성 화면 이미지(/en-us/xenmobile/server/media/add-remote-license.png)
5. 다음 설정을 구성합니다:

   - **라이선스 서버:** 원격 라이선스 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.
   - **포트:** 기본 포트를 사용하거나 라이선스 서버와 통신하는 데 사용되는 포트 번호를 입력합니다.
6. **연결 테스트**를 클릭합니다. 연결에 성공하면 XenMobile이 라이선스 서버에 연결되고 라이선스 테이블에 사용 가능한 라이선스가 채워집니다. 라이선스가 하나만 있는 경우 자동으로 활성화됩니다.

   연결 테스트를 클릭하면 XenMobile은 다음을 확인합니다:

   - XenMobile이 라이선스 서버와 통신할 수 있습니다.
   - 라이선스 서버의 라이선스가 유효합니다.

- 라이선스 서버가 XenMobile과 호환됩니다.

연결에 실패하면 표시된 오류 메시지를 검토하고 필요한 수정을 한 다음 **연결 테스트**를 클릭합니다.

XenMobile 연결 확인 화면 이미지(/en-us/xenmobile/server/media/connectivity-check-license-server.png)

다른 라이선스를 활성화하려면

여러 라이선스가 있는 경우 활성화할 라이선스를 선택할 수 있습니다.

1. **라이선싱** 페이지의 **라이선싱 테이블**에서 활성화할 라이선스를 선택합니다. 목록에서 아무 행이나 클릭하면 **활성화** 대화 상자가 나타납니다.

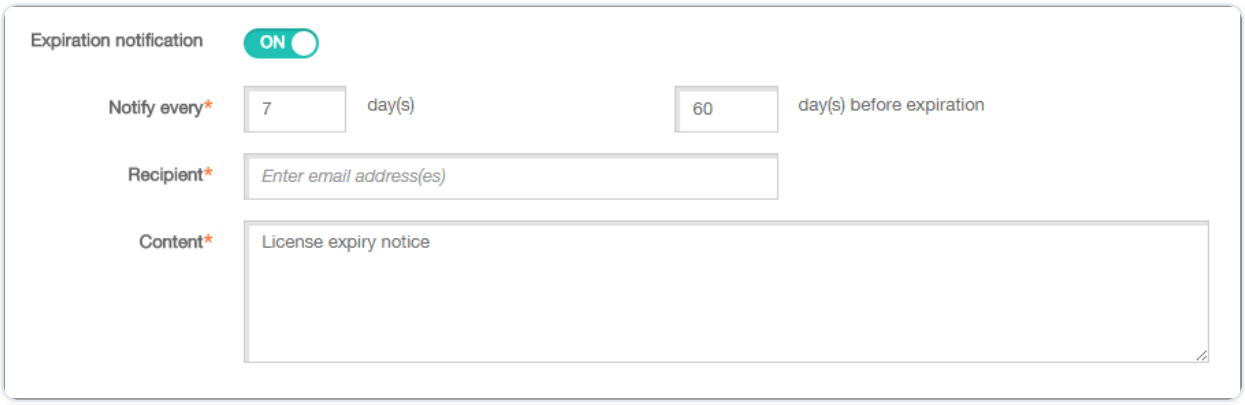
   Licensing 구성 화면 이미지(/en-us/xenmobile/server/media/activate-mixed-licenses.png)
2. **활성화**를 클릭합니다.
3. 라이선스 옆의 **활성** 행에 확인 표시가 나타나면 **저장**을 클릭합니다.

> **중요:**
>
> - **사용자**별 라이선스와 **장치**별 라이선스는 상호 배타적이므로 동시에 활성화할 수 없습니다.
> - ADV Edition 및 ENT Edition 라이선스만 혼합할 수 있습니다. MDM Edition 라이선스는 ADV Edition 또는 ENT Edition 라이선스와 혼합할 수 없습니다.
> - 동일한 에디션의 라이선스 파일이 동일한 상태를 갖는지 확인하십시오. 예를 들어, 하나의 ADV 에디션 파일이 활성화되면 나머지 ADV 파일은 자동으로 활성화됩니다.
> - XenMobile Server 10.15 Rolling Patch 3 이전 버전에서는 한 번에 하나의 라이선스만 활성화할 수 있습니다. 선택한 라이선스를 활성화하면 현재 활성화된 라이선스는 비활성화됩니다.

만료 알림을 자동화하려면

원격 또는 로컬 라이선스를 활성화한 후 XenMobile을 구성하여 라이선스 만료일이 다가올 때 사용자 또는 지정된 사람에게 알림을 보낼 수 있습니다.

1. **라이선싱** 페이지에서 **만료 알림**을 **켜기**로 설정합니다. 새 알림 관련 필드가 나타납니다.



2. 다음 설정을 구성합니다.

   - **알림 주기:** 입력:
   - 알림이 전송되는 빈도(예: **7**일마다).
   - 라이선스 만료 60일 전과 같이 알림 전송을 시작할 시점.
   - **수신자:** 본인의 이메일 주소 또는 라이선스 담당자의 이메일 주소를 입력합니다.
   - **내용:** 수신자가 알림에서 볼 만료 알림 메시지를 입력합니다.

3. **저장**을 클릭합니다. 설정에 따라 XenMobile은 **내용**에 입력한 텍스트가 포함된 이메일 메시지를 **수신자**에 입력한 수신자에게 보내기 시작합니다. 알림은 설정한 빈도로 전송됩니다.

라이선스 활성화 서비스

중요:

Citrix 플랫폼을 위한 업계 표준 클라우드 기반 라이선싱 아키텍처로 전환하고 있습니다. 이러한 전환은 권한 부여 및 활성화를 자동화하여 다음과 같은 주요 고객 이점을 제공합니다.

- **라이선스 파일 관리 불필요:** 라이선스 파일을 다운로드, 할당 또는 관리할 필요가 없어 관리 작업을 간소화합니다.
- **자동화된 권한 업데이트:** 계약 갱신 시 백그라운드에서 권한이 자동으로 업데이트되어 중단 없는 서비스를 보장합니다.
- **향상된 복원력:** 라이선스 서버가 더 이상 사용자 세션의 단일 실패 지점이 아니므로 환경의 안정성이 향상됩니다.

> 저희는 전환 시점까지의 시간을 활용하여 April 15, 2026까지 새로운 라이선싱 모델을 채택하기 위한 전환을 계획하고 실행하시기를 권장하며, 모든 단계에서 지원을 아끼지 않을 것입니다. 자세한 내용은 Citrix Modern Licensing Announcement를 참조하십시오.

> 라이선스 활성화 서비스(LAS)는 기존 Citrix 레거시 라이선싱을 대체하는 새로운 클라우드 기반 라이선싱 솔루션입니다. LAS는 활성화를 위한 새로운 모듈을 도입하여 라이선스 관리에 원활하고 현대적인 접근 방식을 보장합니다.

LAS는 Citrix 라이선싱 경험을 간소화합니다. 더 이상 라이선스 서버에 생성, 다운로드 또는 설치할 라이선스 액세스 코드나 파일이 없습니다. 라이선스 서버를 업그레이드하고 Citrix Cloud에 등록하기만 하면 됩니다. 호환되는 제품이 라이선스 서버를 가리키면 자동으로 활성화될 수 있습니다.

활성화 후 라이선스 서버는 라이선스 활성화 서비스와 정기적으로 통신하여 활성화를 최신 상태로 유지합니다. LAS는 클라우드 기술로 구축되어 성능을 향상하고 가동 중지 시간이 없도록 보장합니다. 어떤 이유로든 라이선스 서버 또는 LAS에 연결할 수 없는 경우 시스템은 라이선스 캐싱 모드로 전환되며, 이는 시스템이 라이선스 없이 작동하는 것을 방지하고 중단을 피하도록 설계되었습니다. 자세한 내용은 라이선스 캐싱 모드를 참조하십시오.

클라우드에 연결할 수 없는 라이선스 서버의 경우, LAS는 오프라인 활성화 옵션도 제공하여 다양한 네트워크 환경에 대한 유연성을 보장합니다. 이 서비스는 Citrix 제품 라이선스를 관리하는 데 원활하고 현대적인 접근 방식을 도입합니다.

LAS에 대한 자세한 내용은 라이선싱 문서 라이선스 활성화 서비스를 참조하십시오.

LAS 호환성

LAS와 호환되는 최소 XenMobile Server 버전은 다음과 같습니다.

- 10.16 롤링 패치 7
- 10.15 롤링 패치 13

> **참고:**

> April 15, 2026에 레거시 파일 기반 라이선싱은 더 이상 작동하지 않습니다. 레거시 파일 기반 라이선싱 메커니즘을 사용하는 배포는 최종 사용자에게 영향을 미칩니다.

사전 요구 사항

- 라이선스 서버를 버전 11.17.2 빌드 51000 이상으로 설치하거나 업데이트합니다.

- XenMobile Server 자격과 연결된 OrgID가 있는 Citrix Cloud 계정.
- 온라인 활성화를 위한 라이선스 서버 구성.

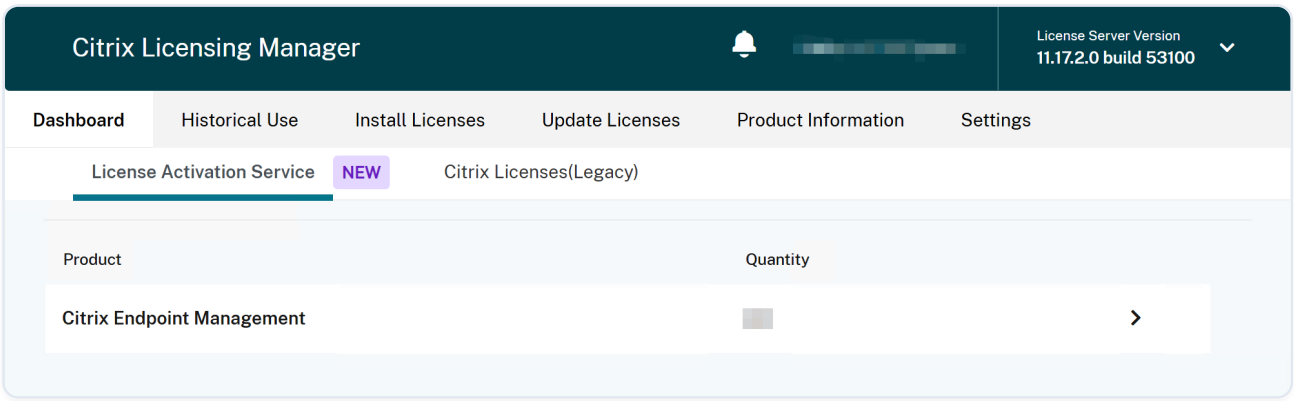
라이선스 활성화 서비스 구성

1단계: 라이선스 서버 설치 또는 업그레이드

라이선스 서버를 버전 11.17.2 빌드 51000 이상으로 설치하거나 업그레이드합니다. Windows용 Citrix 라이선스 서버는 Citrix 라이선싱 다운로드 페이지에서 다운로드할 수 있습니다.

2단계: LAS 구성

라이선스 활성화 서비스를 위한 라이선스 서버 구성 방법에 언급된 지침에 따라 LAS를 구성하고, 라이선스 서버 온보딩에 사용된 Citrix Cloud 고객 계정에 XenMobile Server 자격이 포함되어 있는지 확인하십시오.



3단계: XenMobile Server 업그레이드

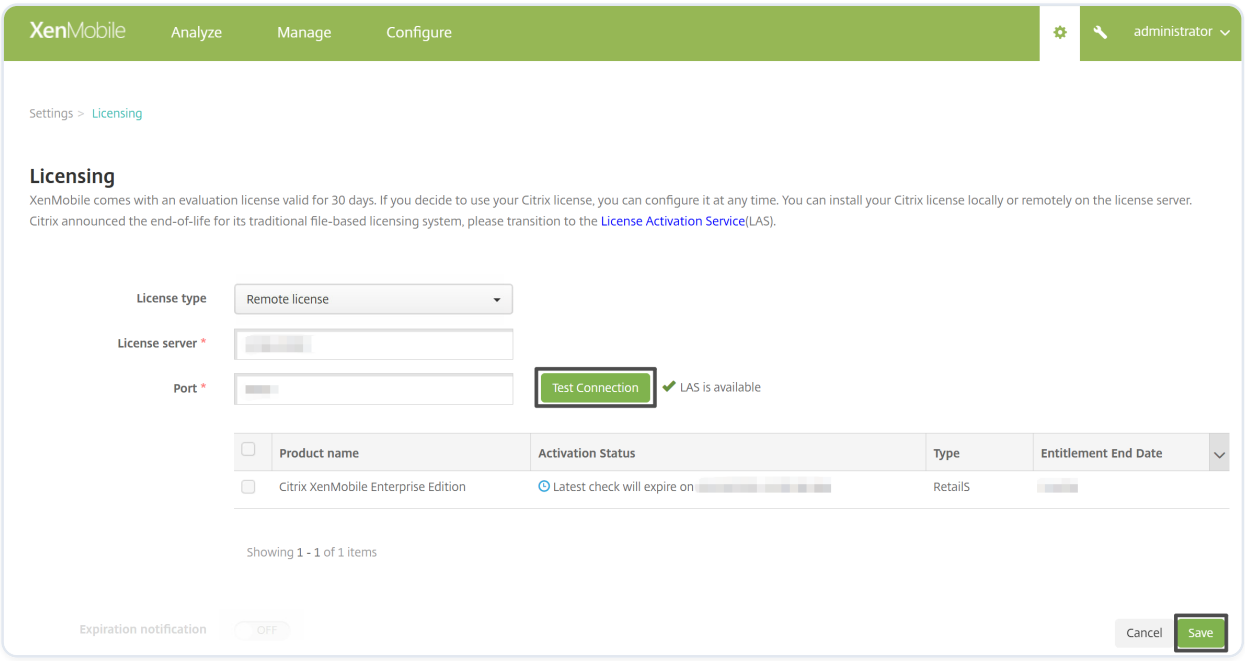
XenMobile Server를 LAS 호환 버전으로 업그레이드합니다. 최소 요구 XenMobile Server 버전은 다음과 같습니다.

- 10.16 롤링 패치 7
- 10.15 롤링 패치 13

4단계: LAS를 사용하도록 XenMobile Server 구성

1. XenMobile Server 콘솔에 로그인하고 **설정 > 라이선싱**으로 이동합니다.
2. **라이선스 유형**을 **원격 라이선스**로 설정합니다.
3. **라이선스 서버** 및 **포트** 구성:
    - **라이선스 서버:** 원격 라이선싱 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.
    - **포트:** 기본 포트(LAS의 경우 8083)를 수락하거나 LAS 라이선싱 서버와 통신하는 데 사용되는 사용자 지정 포트 번호를 입력합니다.

4. **연결 테스트**를 클릭합니다. 연결이 성공하면 LAS를 사용할 수 있으며 라이선싱 테이블에 사용 가능한 라이선스가 채워져 있음을 나타냅니다. 활성화 상태에 오류가 없는지 확인하십시오.



5. **저장**을 클릭합니다. 구성이 저장되고 XenMobile Server가 라이선스 활성화 서비스를 사용하도록 전환됩니다.

문제 해결

라이선스 서버 상태가 녹색이 아닌 경우 다음 단계에 따라 활성화 세부 정보를 확인하고 문제를 해결하십시오.

Citrix Cloud에서 XenMobile Server 활성화 세부 정보를 확인하려면 다음 단계를 수행하십시오.

1. **라이선싱** > **라이선스 배포** > **라이선스 서버**로 이동합니다.
2. XenMobile Server에서 사용되는 라이선스 서버를 찾아 **세부 정보 보기**를 클릭합니다.
3. 라이선스 서버 세부 정보 페이지에서 **Citrix Endpoint Management**를 확장하여 활성화 목록을 봅니다.

   각 활성화에 표시된 **ID**는 XenMobile Server 호스트 이름입니다.

   CEM 성공적인 연결 이미지(/en-us/xenmobile/server/media/cem-successful-connection.png)
4. 필요한 활성화에 대해 **세부 정보 보기**를 클릭합니다.

   세부 정보 페이지에는 다음 정보가 표시됩니다.

   - **XMS 호스트 이름:** XenMobile Server 호스트 이름.
   - **XMS IP:** XenMobile Server IP 주소.

- **호스트 이름:** XenMobile Server 호스트 이름.

LAS 세부 정보 보기 이미지(/en-us/xenmobile/server/media/xms-view-details.png)

FIPS 140-2 규정 준수

연방 정보 처리 표준(FIPS)은 미국 국립표준기술연구소(NIST)에서 발행합니다. FIPS는 보안 시스템에 사용되는 암호화 모듈에 대한 보안 요구 사항을 지정합니다. FIPS 140-2는 이 표준의 두 번째 버전입니다. NIST 검증 FIPS 140 모듈에 대한 자세한 내용은 NIST 컴퓨터 보안 리소스 센터를 참조하십시오.

중요:

- XenMobile® FIPS 모드는 초기 설치 중에만 활성화할 수 있습니다.
- XenMobile 모바일 장치 관리 전용, XenMobile 모바일 앱 관리 전용 및 XenMobile MDM+MAM은 HDX™ 앱을 사용하지 않는 경우 모두 FIPS를 준수합니다.

iOS의 모든 저장 데이터 및 전송 중 데이터 암호화 작업은 Citrix® 및 Apple에서 제공하는 FIPS 검증 암호화 모듈을 사용합니다. Android에서는 모든 저장 데이터 암호화 작업이 장치 제조업체에서 제공하는 플랫폼의 암호화 모듈에서 제공하는 FIPS 검증 암호화 모듈을 사용합니다. 장치 제조업체 모듈에 대한 자세한 내용은 Citrix 담당자에게 문의하십시오.

지원되는 Windows 장치의 모바일 장치 관리(MDM)를 위한 모든 저장 데이터 및 전송 중 데이터 암호화 작업은 FIPS 검증 암호화 모듈을 사용합니다.

XenMobile MDM의 모든 저장 데이터 및 전송 중 데이터 암호화 작업은 FIPS 검증 암호화 모듈을 사용합니다. MDM 흐름의 모든 저장 데이터 및 전송 중 데이터는 FIPS를 준수하는 암호화 모듈을 종단 간 사용합니다. 이 보안에는 모바일 장치에 대해 이전에 설명한 암호화 작업과 모바일 장치와 Citrix Gateway 간의 암호화 작업이 포함됩니다.

MDX Vault는 FIPS 검증 암호화 모듈을 사용하여 iOS 및 Android 장치 모두에서 MDX로 래핑된 앱과 관련 저장 데이터를 암호화합니다.

언어 지원

모바일 생산성 앱과 XenMobile 콘솔은 영어 이외의 언어로 사용하도록 조정되었습니다. 이 지원에는 앱이 사용자의 기본 언어로 현지화되지 않은 경우에도 비영어 문자 및 키보드 입력이 포함됩니다. 모든 Citrix 제품에

대한 국제화 지원에 대한 자세한 내용은 `<https://support.citrix.com/article/CTX119253>`을(를) 참조하십시오.

이 문서에는 XenMobile의 최신 릴리스에서 지원되는 언어가 나열되어 있습니다.

XenMobile 콘솔 및 셀프 서비스 포털

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

모바일 생산성 앱

X는 해당 앱이 특정 언어로 제공됨을 나타냅니다.

아이오에스 및 안드로이드

언어	시큐어 허브	시큐어 메일	시큐어 웹	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

언어	시큐어 허브	시큐어 메일	시큐어 웹	QUICKEDIT
덴마크어	X	X	X	X
스웨덴어	X	X	X	X
히브리어	X	X	X	iOS 전용
아랍어	X	X	X	X
러시아어	X	X	X	X
튀르키예어	X	X	Android 전용	-
폴란드어	X	X	X	-

윈도우

언어	시큐어 허브	시큐어 메일	시큐어 웹
프랑스어	X	X	X
독일어	X	X	X
스페인어	X	X	X
이탈리아어	X	X	X
덴마크어	X	X	X
스웨덴어	X	X	X

오른쪽에서 왼쪽으로 쓰는 언어 지원

다음 표는 각 앱에 대한 중동 언어 텍스트 지원을 요약한 것입니다. X는 해당 플랫폼에서 기능을 사용할 수 있음을 나타냅니다. Windows 장치에서는 오른쪽에서 왼쪽으로 쓰는 언어 지원을 사용할 수 없습니다.

앱	IOS	안드로이드
시큐어 허브	X	X
시큐어 메일	X	X

앱	IOS	안드로이드
시큐어 웹	X	X
QuickEdit	X	X

설치 및 구성

시작하기 전에

다음 사전 설치 점검 목록을 사용하여 온프레미스 XenMobile® 설치를 위한 필수 구성 요소 및 설정을 기록할 수 있습니다. 각 작업 또는 참고 사항에는 요구 사항이 적용되는 구성 요소 또는 기능을 나타내는 열이 포함되어 있습니다.

XenMobile 배포를 계획하는 데는 많은 고려 사항이 따릅니다. 전체 XenMobile 환경에 대한 권장 사항, 일반적인 질문 및 사용 사례는 XenMobile 배포 핸드북을 참조하십시오.

설치 단계는 이 문서의 뒷부분에 있는 XenMobile 설치 섹션을 참조하십시오.

사전 설치 점검 목록

기본 네트워크 연결

다음은 XenMobile 솔루션에 필요한 네트워크 설정입니다.

필수 구성 요소 또는 설정	구성 요소 또는 기능	설정 기록	
원격 사용자가 연결하는 정규화된 도메인 이름(FQDN)을 기록합니다.	젠모바일 및 시트릭스 게이트웨이		
공용 및 로컬 IP 주소를 기록합니다.			
네트워크 주소 변환(NAT)을 설정하기 위해 방화벽을 구성하려면 이러한 IP 주소가 필요합니다.	XenMobile 및 시트릭스 게이트웨이		

필수 구성 요소 또는 설정	구성 요소 또는 기능	설정 기록		
서브넷 마스크를 기록합니다.	XenMobile 및 시트릭스 게이트웨이			
DNS IP 주소를 기록합니다.	XenMobile 및 시트릭스 게이트웨이			
WINS 서버 IP 주소를 기록합니다(해당하는 경우).	시트릭스 게이트웨이			
Citrix Gateway 호스트 이름을 확인하고 기록합니다.	시트릭스 게이트웨이	이 항목은 FQDN이 아닙니다. FQDN은 가상 서버에 바인딩되고 사용자가 연결하는 서명된 서버 인증서에 포함되어 있습니다. Citrix Gateway의 설정 마법사를 사용하여 호스트 이름을 구성할 수 있습니다.	시트릭스 게이트웨이	
XenMobile의 IP 주소를 기록합니다. XenMobile 인스턴스를 하나 설치하는 경우 IP 주소 하나를 예약합니다. 클러스터를 구성하는 경우 필요한 모든 IP 주소를 기록합니다.	XenMobile			

필수 구성 요소 또는 설정	구성 요소 또는 기능	설정 기록	
Citrix Gateway에 구성된 공용 IP 주소 하나	시트릭스 게이트웨이		
Citrix Gateway용 외부 DNS 항목 1개	시트릭스 게이트웨이		
웹 프록시 서버 IP 주소, 포트, 프록시 호스트 목록, 관리자 사용자 이름 및 암호를 기록해 두십시오. 네트워크에 프록시 서버를 배포하는 경우(해당하는 경우) 이러한 설정은 선택 사항입니다.	시트릭스 게이트웨이	웹 프록시의 사용자 이름을 구성할 때 sAMAccountName 또는 UPN(User Principal Name)을 사용할 수 있습니다.	젠모바일 및 시트릭스 게이트웨이
기본 게이트웨이 IP 주소를 기록해 두십시오.	젠모바일 및 시트릭스 게이트웨이		
시스템 IP(NSIP) 주소 및 서브넷 마스크를 기록해 두십시오.	시트릭스 게이트웨이		
서브넷 IP(SNIP) 주소 및 서브넷 마스크를 기록해 두십시오.	시트릭스 게이트웨이		
인증서에서 Citrix Gateway 가상 서버 IP 주소 및 FQDN을 기록해 두십시오. 여러	시트릭스 게이트웨이		

필수 구성 요소 또는 설정	구성 요소 또는 기능	설정 기록	
가상 서버를 구성하려면 인증서에서 모든 가상 IP 주소 및 FQDN을 기록해 두십시오.			
사용자가 Citrix Gateway를 통해 액세스할 수 있는 내부 네트워크를 기록해 두십시오. 예: 10.10.0.0/24. 다음 경우에 사용자가 액세스해야 하는 모든 내부 네트워크 및 네트워크 세그먼트를 입력하십시오. 사용자가 Secure Hub 또는 Citrix Gateway Plug-in으로 연결하고 분할 터널링이 켜짐으로 설정된 경우.	시트릭스 게이트웨이		
XenMobile Server, Citrix Gateway, 외부 Microsoft SQL Server 및 DNS 서버 간의 네트워크 연결이 가능한지 확인하십시오.	젠모바일 및 시트릭스 게이트웨이		

라이선싱

XenMobile을 사용하려면 Citrix Gateway 및 XenMobile에 대한 라이선스 옵션을 구매해야 합니다. Citrix 라이선싱에 대한 자세한 내용은 Citrix 라이선싱 시스템을 참조하십시오.

필수 구성 요소	구성 요소	위치 기록
Citrix 웹사이트에서 Universal 라이선스를 얻으십시오. 자세한 내용은 Citrix Gateway 설명서의 라이선싱을 참조하십시오.	시트릭스 게이트웨이, 젠모바일 및 시트릭스 라이선스 서버	

인증서

XenMobile 및 Citrix Gateway는 다른 Citrix 제품 및 앱과 사용자 장치로부터의 연결을 활성화하기 위해 인증서가 필요합니다. 자세한 내용은 XenMobile 설명서의 인증서 및 인증 섹션을 참조하십시오.

필수 구성 요소	구성 요소	참고 사항
필요한 인증서를 획득하고 설치합니다.	젠모바일 및 시트릭스 게이트웨이	

포트

XenMobile 구성 요소와의 통신을 허용하도록 포트를 엽니다.

필수 구성 요소	구성 요소	참고
XenMobile용 포트 열기	젠모바일 및 시트릭스 게이트웨이	

데이터베이스

XenMobile에는 데이터베이스 연결 구성이 필요합니다. XenMobile 리포지토리에는 (/ko-kr/xenmobile/server/system-requirements.html)에 명시된 지원되는 버전 중 하나에서 실행되는 Microsoft SQL Server 데이터베이스가 필요합니다. Citrix는 Microsoft SQL을 원격으로 사용하는 것을 권장합니다. PostgreSQL은 XenMobile에 포함되어 있습니다. PostgreSQL은 테스트 환경에서 *만* 로컬 또는 원격으로 사용하십시오.

기본적으로 XenMobile은 jTDS 데이터베이스 드라이버를 사용합니다. XenMobile Server의 온프레미스 설치에 Microsoft JDBC 드라이버를 사용하려면 (/ko-kr/xenmobile/server/install-configure/sql-server-drivers.html)을 참조하십시오.

필수 구성 요소	구성 요소	참고
Microsoft SQL Server IP 주소 및 포트. XenMobile에서 사용할	XenMobile	

필수 구성 요소	구성 요소	참고
SQL Server의 서비스 계정에 DBcreator 역할 권한이 있는지 확인합니다.		

액티브 디렉터리 설정

필수 구성 요소	구성 요소	참고
기본 및 보조 서버의 Active Directory IP 주소와 포트를 기록합니다. 포트 636을 사용하는 경우 XenMobile에 CA의 루트 인증서를 설치하고 '보안 연결 사용' 옵션을 '예'로 변경합니다.	젠모바일 및 시트릭스 게이트웨이	
Active Directory 도메인 이름을 기록합니다.	젠모바일 및 시트릭스 게이트웨이	
사용자 ID, 암호 및 도메인 별칭이 필요한 Active Directory 서비스 계정을 기록합니다.		
Active Directory 서비스 계정은 XenMobile이 Active Directory를 쿼리하는 데 사용하는 계정입니다.	젠모바일 및 시트릭스 게이트웨이	
사용자가 위치한 디렉터리 수준인 사용자 기본 DN을 기록합니다. 예를 들어: `cn=users,dc=ace,dc=com`. Citrix Gateway 및 XenMobile은 사용자 기본 DN을 사용하여 Active Directory를 쿼리합니다.	젠모바일 및 시트릭스 게이트웨이	
그룹이 위치한 디렉터리 수준인 그룹 기본 DN을 기록해 둡니다. Citrix Gateway 및 XenMobile은 이 DN을 사용하여 Active Directory를 쿼리합니다.	젠모바일 및 시트릭스 게이트웨이	

XenMobile과 Citrix Gateway 간 연결

필수 구성 요소	구성 요소	설정을 기록해 둡니다.
XenMobile 호스트 이름을 기록해 둡니다.	XenMobile	
XenMobile의 FQDN 또는 IP 주소를 기록해 둡니다.	XenMobile	
사용자가 액세스할 수 있는 앱을 식별합니다.	시트릭스 게이트웨이	
콜백 URL을 기록해 둡니다.	XenMobile	

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

Citrix는 XenMobile과 Citrix Gateway 간, 그리고 XenMobile과 Secure Hub 간의 연결 설정을 구성하기 위해 Citrix ADC의 빠른 구성 마법사를 사용할 것을 권장합니다. Citrix Receiver™ 및 웹 브라우저에서 사용자 연결을 활성화하려면 두 번째 가상 서버를 생성합니다. 이러한 연결은 Virtual Apps and Desktops의 Windows 기반 애플리케이션 및 가상 데스크톱에 대한 것입니다. Citrix는 이러한 설정을 구성하기 위해 Citrix ADC의 빠른 구성 마법사를 사용할 것을 권장합니다.

필수 구성 요소	구성 요소	설정 기록
Citrix Gateway 호스트 이름과 외부 URL을 기록합니다. 외부 URL은 사용자가 연결하는 웹 주소입니다.	XenMobile	
Citrix Gateway 콜백 URL을 기록합니다.	XenMobile	
가상 서버의 IP 주소와 서브넷 마스크를 기록합니다.	시트릭스 게이트웨이	
Program Neighborhood Agent 또는 Virtual Apps and Desktops Site의 경로를 기록합니다.	시트릭스 게이트웨이 및 젠모바일	

필수 구성 요소	구성 요소	설정 기록
Secure Ticket Authority(STA)를 실행하는 Citrix Virtual Apps™ 및 Desktops 서버의 FQDN 또는 IP 주소를 기록합니다(ICA 연결에만 해당).	시트릭스 게이트웨이	
XenMobile의 공용 FQDN을 기록합니다.	시트릭스 게이트웨이	
Secure Hub의 공용 FQDN을 기록해 두십시오.	시트릭스 게이트웨이	

XenMobile 배포를 위한 순서도

이 순서도를 사용하여 XenMobile 배포의 주요 단계를 안내받을 수 있습니다. 각 단계에 대한 항목 링크는 그림 다음에 나옵니다.

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 환경 설정 구성

8: 포트 요구 사항

XenMobile 설치

XenMobile 가상 머신(VM)은 Citrix XenServer, VMware ESXi 또는 Microsoft Hyper-V에서 실행됩니다. XenCenter® 또는 vSphere 관리 콘솔을 사용하여 XenMobile을 설치할 수 있습니다.

> **참고:**

하이퍼바이저가 올바른 시간(NTP 서버 또는 수동 구성 사용)으로 구성되어 있는지 확인하십시오. XenMobile이 해당 시간을 사용하기 때문입니다. XenMobile 시간을 하이퍼바이저와 동기화할 때 시간대 문제가 발생하는 경우, XenMobile을 NTP 서버로 지정하여 문제를 피할 수 있습니다. 그렇게 하려면 (/ko-kr/xenmobile/server/install-configure/command-line-interface.html)에 설명된 대로 XenMobile CLI를 사용하십시오.

XenServer 또는 VMware ESXi 필수 구성 요소. XenServer 또는 VMware ESXi에 XenMobile을 설치하기 전에 다음을 수행해야 합니다. 자세한 내용은 XenServer 또는 VMware 설명서를 참조하십시오.

- 적절한 하드웨어 리소스가 있는 컴퓨터에 XenServer® 또는 VMware ESXi를 설치합니다.
- 별도의 컴퓨터에 XenCenter 또는 vSphere를 설치합니다. XenCenter 또는 vSphere를 호스팅하는 컴퓨터는 네트워크를 통해 XenServer 또는 VMware ESXi 호스트에 연결됩니다.

Hyper-V 필수 구성 요소. Hyper-V에 XenMobile을 설치하기 전에 다음을 수행해야 합니다. 자세한 내용은 Hyper-V 설명서를 참조하십시오.

- 적절한 시스템 리소스가 있는 컴퓨터에 Hyper-V가 활성화되고 역할이 활성화된 Windows Server 2016 또는 Windows Server 2019를 설치합니다. Hyper-V 역할을 설치하는 동안 Hyper-V가 가상 네트워크를 만드는 데 사용하는 서버의 NIC를 지정해야 합니다. 호스트를 위해 일부 NIC를 예약할 수 있습니다.
- Virtual Machines/<*build-specific UUID*>.xml 파일을 삭제합니다.
- Legacy/<*build-specific UUID*>.exp 파일을 Virtual Machines로 이동합니다.

FIPS 140-2 모드. FIPS 모드에서 XenMobile Server를 설치하려면 (/ko-kr/xenmobile/server/install-configure/fips.html)에 설명된 대로 필수 구성 요소 그룹을 완료하십시오.

XenMobile 제품 소프트웨어 다운로드

Citrix 웹사이트에서 제품 소프트웨어를 다운로드할 수 있습니다. 해당 사이트에 로그온한 다음 다운로드 링크를 사용하여 다운로드하려는 소프트웨어가 포함된 페이지로 이동하십시오.

XenMobile용 소프트웨어를 다운로드하려면

1. Citrix 웹사이트으로 이동합니다.
2. 검색 상자 옆에서 **로그온**을 클릭하고 계정에 로그온합니다.
3. **다운로드** 탭을 클릭합니다.

4. 다운로드 페이지의 **제품 선택** 목록에서 **Citrix Endpoint Management™(및 Citrix XenMobile Server)**를 클릭합니다. Citrix Endpoint Management(및 Citrix XenMobile Server) 페이지가 자동으로 나타납니다.

   제품 목록(/en-us/xenmobile/server/media/download1.png)

5. **XenMobile Server(온프레미스)**를 확장합니다.
6. **제품 소프트웨어**를 확장합니다.
7. **XenMobile Server 10**을 클릭합니다.
8. **다운로드로 이동** 메뉴를 클릭하고 XenMobile을 설치하는 데 사용할 적절한 가상 이미지를 선택합니다. 또는 페이지를 아래로 스크롤하여 설치하려는 이미지의 **파일 다운로드** 버튼을 찾습니다.
9. 화면의 지침에 따라 소프트웨어를 다운로드합니다.

Citrix Gateway용 소프트웨어를 다운로드하려면

이 절차를 사용하여 Citrix Gateway 가상 어플라이언스 또는 기존 Citrix Gateway 어플라이언스에 대한 소프트웨어 업그레이드를 다운로드할 수 있습니다.

1. Citrix 웹사이트로 이동합니다.
2. Citrix 웹사이트에 아직 로그인하지 않은 경우 검색 상자 옆에 있는 **로그온**을 클릭하고 계정에 로그인합니다.
3. **다운로드** 탭을 클릭합니다.
4. 다운로드 페이지의 제품 선택 목록에서 **Citrix Gateway**를 클릭합니다.
5. **이동**을 클릭합니다. Citrix Gateway 페이지가 나타납니다.
6. Citrix Gateway 페이지에서 실행 중인 Citrix Gateway 버전을 확장합니다.
7. **펌웨어**에서 다운로드하려는 어플라이언스 소프트웨어 버전을 클릭합니다.

   > **참고:**
   >
   > **가상 어플라이언스**를 클릭하여 Citrix ADC VPX를 다운로드할 수도 있습니다. 이 옵션을 선택하면 각 하이퍼바이저에 대한 가상 머신용 소프트웨어 목록이 표시됩니다.

8. 다운로드하려는 어플라이언스 소프트웨어 버전을 클릭합니다.
9. 다운로드하려는 버전의 어플라이언스 소프트웨어 페이지에서 해당 가상 어플라이언스에 대한 **다운로드**를 클릭합니다.
10. 화면의 지시에 따라 소프트웨어를 다운로드합니다.

XenMobile을 처음 사용하도록 구성

1. XenMobile의 IP 주소 및 서브넷 마스크, 기본 게이트웨이, DNS 서버 및 기타 설정을 구성하려면 XenCenter 또는 vSphere 명령줄 콘솔을 사용합니다.

   > **참고:**
   >
   > vSphere 웹 클라이언트를 사용하는 경우: **템플릿 사용자 지정** 페이지에서 OVF 템플릿을 배포하는 동안 네트워킹 속성을 구성하지 않는 것이 좋습니다. 고가용성 구성에서 이렇게 하면 두 번째 XenMobile 가상 머신을 복제한 다음 다시 시작할 때 발생하는 IP 주소 문제를 방지할 수 있습니다.

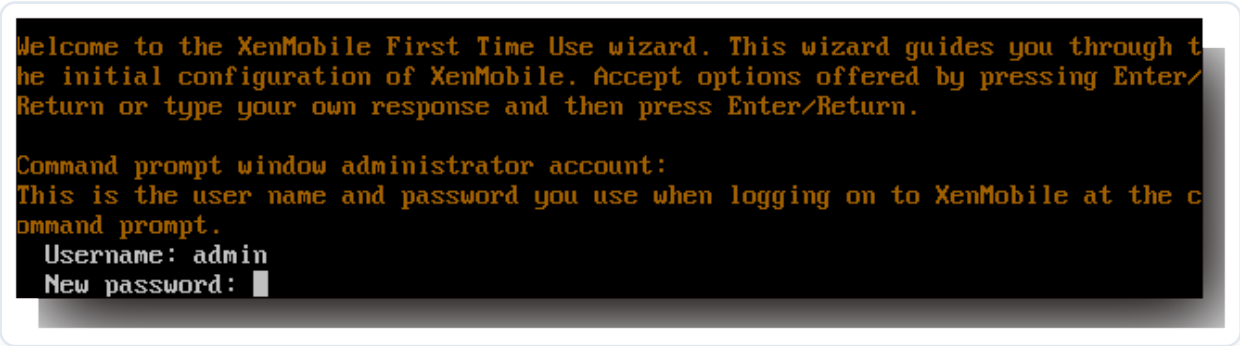
2. XenMobile 관리 콘솔은 XenMobile Server FQDN(정규화된 도메인 이름) 또는 노드의 IP 주소를 통해서만 액세스합니다.
3. 로그온한 다음 초기 로그온 화면의 단계를 따릅니다.

명령 프롬프트 창에서 XenMobile 구성

1. XenMobile 가상 머신을 Citrix XenServer, Microsoft Hyper-V 또는 VMware ESXi로 가져옵니다. 자세한 내용은 XenServer, Hyper-V 또는 VMware 설명서를 참조하십시오.
2. 하이퍼바이저에서 가져온 XenMobile 가상 머신을 선택하고 명령 프롬프트 보기를 시작합니다. 자세한 내용은 하이퍼바이저 설명서를 참조하십시오.
3. 하이퍼바이저 콘솔 페이지에서 관리자 사용자 이름과 암호를 입력하여 명령 프롬프트 창에 XenMobile용 관리자 계정을 만듭니다.

   명령 프롬프트 관리자 계정, PKI(공개 키 인프라) 서버 인증서 및 FIPS의 암호를 생성하거나 변경할 때 XenMobile은 XenMobile 외부에서 암호가 관리되는 Active Directory 사용자를 제외한 모든 사용자에게 다음 규칙을 적용합니다.

   - 암호는 8자 이상이어야 합니다.
   - 암호는 다음 복잡성 조건 중 최소 세 가지를 충족해야 합니다.
     - 대문자(A-Z)
     - 소문자(a-z)
     - 숫자(0-9)
     - 특수 문자(예: `! # $ %`)



새 암호를 입력할 때 별표와 같은 문자는 표시되지 않습니다.

4. 다음 네트워크 정보를 제공한 다음 **y**를 입력하여 설정을 커밋합니다.

   a. XenMobile Server의 IP 주소

   b. 넷마스크

   c. 기본 게이트웨이(DMZ의 기본 게이트웨이 IP 주소)

   d. 기본 DNS 서버(DNS 서버의 IP 주소)

   e. 보조 DNS 서버(선택 사항)



> **참고:**
>
> 이 이미지와 다음 이미지에 표시된 주소는 작동하지 않으며 예시로만 제공됩니다.

5. 임의의 암호화 암호를 생성하여 보안을 강화하려면 **y**를 입력하고, 직접 암호를 제공하려면 **n**을 입력합니다. Citrix에서는 임의의 암호를 생성하기 위해 **y**를 입력하는 것을 권장합니다.

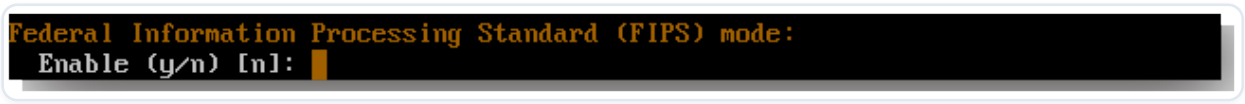
   암호는 중요한 데이터를 보호하는 데 사용되는 암호화 키를 보호하는 데 사용됩니다. 서버 파일 시스템에 저장된 암호의 해시는 데이터 암호화 및 암호 해독 중에 키를 검색하는 데 사용됩니다. 암호는 볼 수 없습니다.

> **참고:**

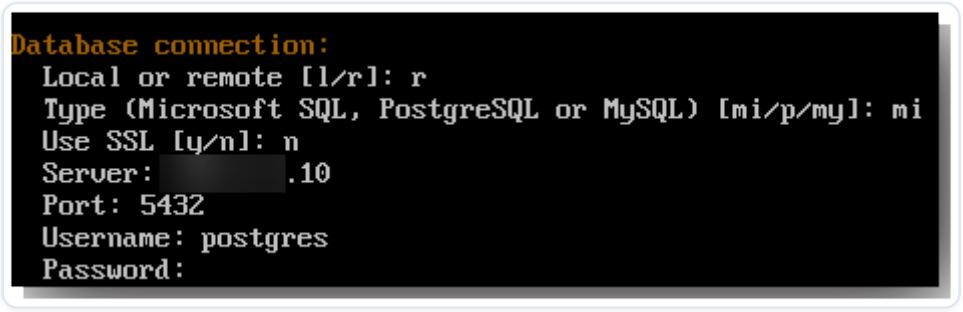
환경을 확장하고 더 많은 서버를 구성하려는 경우 직접 암호를 제공하십시오. 임의 암호를 선택하면 암호를 볼 수 없습니다.



6. 선택적으로 FIPS(Federal Information Processing Standard)를 활성화합니다. FIPS에 대한 자세한 내용은 FIPS를 참조하십시오. 또한 XenMobile에서 FIPS 구성에 설명된 대로 필수 구성 요소를 완료해야 합니다.



7. 데이터베이스 연결을 구성하려면 다음 정보를 제공하십시오.



- 데이터베이스는 로컬 또는 원격일 수 있습니다. 로컬의 경우 **l**을 입력하고 원격의 경우 **r**을 입력합니다.
- 데이터베이스 유형을 선택합니다. Microsoft SQL의 경우 **mi**를 입력하고 PostgreSQL의 경우 **p**를 입력합니다.

  중요:

  - Citrix는 Microsoft SQL을 원격으로 사용하는 것을 권장합니다. PostgreSQL은 XenMobile에 포함되어 있습니다. PostgreSQL은 테스트 환경에서 *만* 로컬 또는 원격으로 사용하십시오.
  - 데이터베이스 마이그레이션은 지원되지 않습니다. 테스트 환경에서 생성된 데이터베이스는 프로덕션 환경으로 이동할 수 없습니다.

- 선택적으로, 데이터베이스에 SSL 인증을 사용하려면 **y**를 입력합니다.

- XenMobile을 호스팅하는 서버의 FQDN(정규화된 도메인 이름)을 제공합니다. 이 단일 호스트 서버는 장치 관리 및 앱 관리 서비스를 모두 제공합니다.
- 기본 포트 번호와 다른 경우 데이터베이스 포트 번호를 입력합니다. Microsoft SQL의 기본 포트는 1433이고 PostgreSQL의 기본 포트는 5432입니다.
- 데이터베이스 관리자 사용자 이름을 입력합니다.
- 데이터베이스 관리자 암호를 입력합니다.
- 데이터베이스 이름을 입력합니다.
- 데이터베이스 설정을 커밋하려면 **Enter** 키를 누릅니다.

8. 선택적으로, XenMobile 노드 또는 인스턴스 클러스터링을 활성화하려면 **y**를 입력합니다.

> **중요:**
>
> XenMobile 클러스터를 활성화하는 경우, 시스템 구성이 완료된 후 클러스터 구성원 간의 실시간 통신을 활성화하려면 포트 80을 엽니다. 모든 클러스터 노드에서 해당 설정을 완료합니다.

9. XenMobile Server의 FQDN(정규화된 도메인 이름)을 입력합니다.

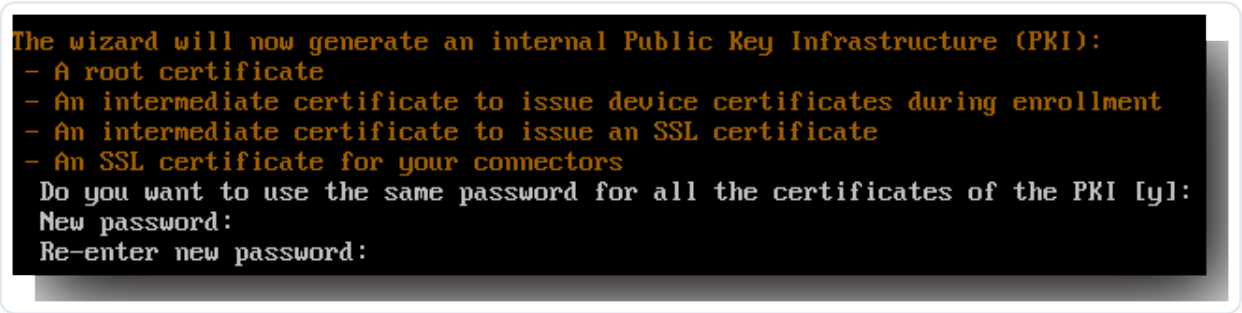


10. 설정을 적용하려면 **Enter** 키를 누릅니다.
11. 통신 포트를 식별합니다. 포트 및 해당 사용에 대한 자세한 내용은 포트 요구 사항을 참조하십시오.

> **참고:**
>
> **Enter** 키(Mac에서는 Return 키)를 눌러 기본 포트를 수락합니다.



12. XenMobile을 처음 설치하므로 이전 XenMobile 릴리스에서 업그레이드하는 것에 대한 다음 질문은 건너뜁니다.
13. 각 PKI(공개 키 인프라) 인증서에 동일한 암호를 사용하려면 **y**를 입력합니다. XenMobile PKI 기능에 대한 자세한 내용은 인증서 업로드를 참조하십시오.



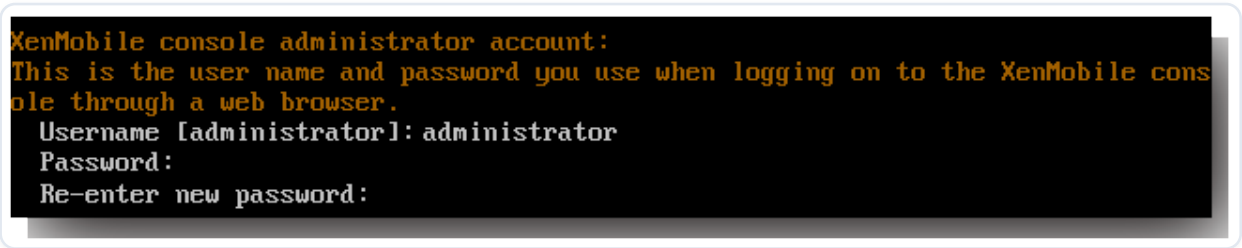
중요:

XenMobile의 노드 또는 인스턴스를 함께 클러스터링하려는 경우, 후속 노드에 동일한 암호를 제공하십시오.

14. 새 암호를 입력한 다음 새 암호를 다시 입력하여 확인합니다.

    새 암호를 입력할 때 별표와 같은 문자는 표시되지 않습니다.

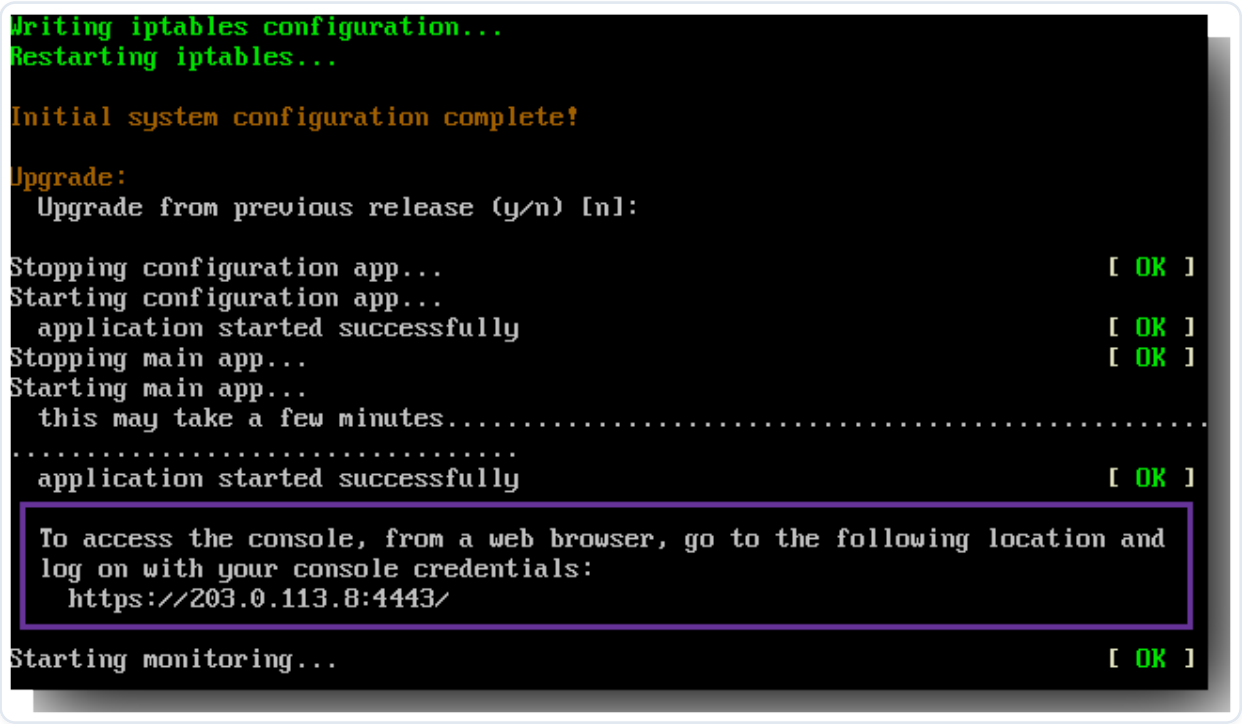
15. 설정을 적용하려면 **Enter** 키를 누릅니다.
16. 웹 브라우저를 사용하여 XenMobile 콘솔에 로그온할 관리자 계정을 만듭니다. 나중에 사용할 수 있도록 이 자격 증명을 기록해 두십시오.



참고:

새 암호를 입력할 때 별표와 같은 문자는 표시되지 않습니다.

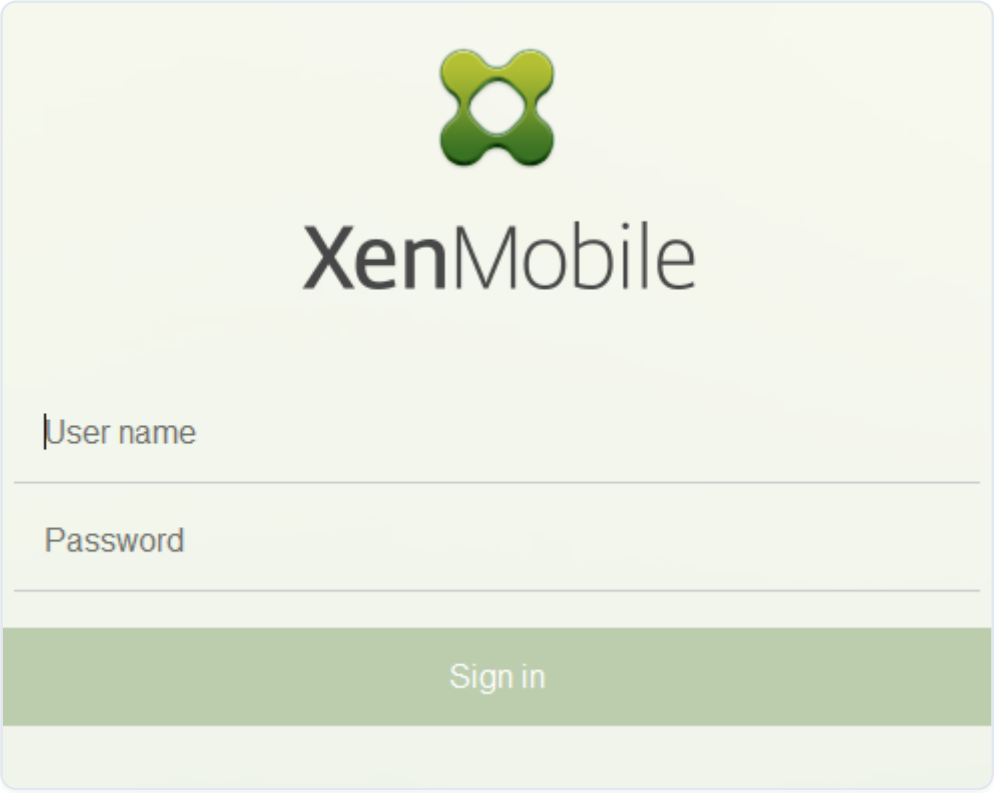
17. 설정을 적용하려면 **Enter** 키를 누릅니다. 초기 시스템 구성이 저장됩니다.
18. 업그레이드 여부를 묻는 메시지가 나타나면 새 설치이므로 **n**을 입력합니다.
19. 화면에 나타나는 전체 URL을 복사하고 웹 브라우저에서 이 초기 XenMobile 구성을 계속 진행합니다.



웹 브라우저에서 XenMobile 구성

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

1. 웹 브라우저에서 명령 프롬프트 창 구성이 완료될 때 제공된 위치로 이동합니다.
2. 명령 프롬프트 창에서 생성한 XenMobile 콘솔 관리자 계정 사용자 이름과 암호를 입력합니다.



3. 시작 페이지에서 **시작**을 클릭합니다. **라이선싱** 페이지가 나타납니다.
4. 라이선스를 구성합니다. 라이선스를 업로드하지 않으면 30일 동안 유효한 평가 라이선스를 사용합니다. 라이선스 추가 및 구성, 만료 알림 구성에 대한 자세한 내용은 라이선싱을 참조하십시오.

> **중요:**
>
> 클러스터 노드 또는 XenMobile 인스턴스를 추가하여 XenMobile 클러스터링을 사용하려는 경우 원격 서버에서 Citrix Licensing을 사용해야 합니다.

5. **인증서** 페이지에서 **가져오기**를 클릭합니다. 가져오기 대화 상자가 나타납니다.
6. APNs 및 SSL 수신기 인증서를 가져옵니다. iOS 장치 관리는 APNs 인증서를 필요로 합니다. 인증서 작업에 대한 자세한 내용은 인증서를 참조하십시오.

> **참고:**
>
> 이 단계에서는 서버를 다시 시작해야 합니다.

7. 환경에 적합한 경우 Citrix Gateway를 구성합니다. Citrix Gateway 구성에 대한 자세한 내용은 Citrix Gateway 및 XenMobile 및 XenMobile 환경 설정 구성을 참조하십시오.

> **참고:**
>
> - 내부 네트워크(또는 인트라넷)의 경계에 Citrix Gateway를 배포할 수 있습니다. 이 배포는 내부 네트워크에 있는 서버, 앱 및 기타 네트워크 리소스에 대한 안전한 단일 액세스 지점을 제공합니다. 이 배포에서는 모든 원격 사용자가 내부 네트워크의 리소스에 액세스하기 전에 Citrix Gateway에 연결해야 합니다.
> - Citrix Gateway는 선택적 설정이지만, 페이지에 데이터를 입력한 후에는 페이지를 떠나기 전에 필수 필드를 지우거나 완료해야 합니다.

8. Active Directory에서 사용자 및 그룹에 액세스하려면 LDAP 구성을 완료합니다. LDAP 연결 구성에 대한 자세한 내용은 LDAP 구성을 참조하십시오.
9. 사용자에게 메시지를 보낼 수 있도록 알림 서버를 구성합니다. 알림 서버 구성에 대한 자세한 내용은 알림을 참조하십시오.

사전 요구 사항. 인증서를 활성화하려면 XenMobile Server를 다시 시작하십시오.

XenMobile®로 FIPS 구성

XenMobile의 FIPS(Federal Information Processing Standards) 모드는 모든 암호화 작업에 FIPS 140-2 인증 라이브러리만 사용하여 미국 연방 정부 고객을 지원합니다. FIPS 모드로 XenMobile Server를 설치하면 XenMobile 클라이언트 및 서버의 모든 데이터가 FIPS 140-2를 완벽하게 준수합니다. 이 규정 준수는 저장 데이터 및 전송 중인 데이터에 적용됩니다.

FIPS 모드에서 XenMobile Server를 설치하기 전에 다음 필수 구성 요소를 완료하십시오.

- XenMobile 데이터베이스에 외부 SQL Server 2014를 사용합니다. SQL Server는 보안 SSL 통신을 위해 구성되어야 합니다. SQL Server에 대한 보안 SSL 통신 구성 지침은 데이터베이스 엔진에 대한 암호화된 연결 사용(SQL Server 구성 관리자)를 참조하십시오.
- 보안 SSL 통신을 위해서는 SQL Server에 잘 알려진 CA(인증 기관)의 신뢰할 수 있는 SSL 인증서를 설치해야 합니다. SQL Server 2014는 와일드카드 인증서를 허용할 수 없습니다. Citrix®는 SQL Server의 FQDN으로 SSL 인증서를 요청할 것을 권장합니다.

FIPS 모드 구성

FIPS 모드는 XenMobile Server의 초기 설정 중에만 활성화할 수 있습니다. 설치가 완료된 후에는 FIPS를 활성화할 수 없습니다. 따라서 FIPS 모드를 사용할 계획이라면 처음부터 FIPS 모드로 XenMobile Server를 설치해야 합니다. XenMobile 클러스터의 경우 모든 클러스터 노드에서 FIPS가 활성화되어야 합니다. 동일한 클러스터에서 FIPS 및 비FIPS XenMobile Server를 혼합하여 사용할 수 없습니다.

XenMobile 명령줄 인터페이스에는 프로덕션 용도가 아닌 **FIPS 모드 전환** 옵션이 있습니다. 이 옵션은 비프로덕션, 진단 용도로 사용되며 프로덕션 XenMobile Server에서는 지원되지 않습니다.

1. 초기 설정 중에 **FIPS 모드**를 활성화합니다.
2. SQL Server의 루트 CA 인증서를 업로드합니다.
3. SQL Server의 서버 이름과 포트, SQL Server 로그인 자격 증명, XenMobile용으로 생성할 데이터베이스 이름을 지정합니다.

> **참고:**
>
> SQL Server에 액세스하려면 SQL 로그인 또는 Active Directory 계정을 사용할 수 있지만, 사용하는 로그인은 DBcreator 역할을 가지고 있어야 합니다.

4. Active Directory 계정을 사용하려면 domain\\username 형식으로 자격 증명을 입력합니다.
5. 이러한 단계가 완료되면 XenMobile 초기 설정을 계속 진행합니다.

FIPS 모드 구성이 성공했는지 확인하려면 XenMobile 명령줄 인터페이스에 로그온하십시오. **In FIPS Compliant Mode** 문구가 로그온 배너에 나타납니다.

인증서 가져오기

다음 절차에서는 인증서를 가져와 XenMobile에서 FIPS를 구성하는 방법을 설명합니다.

SQL 필수 구성 요소

1. XenMobile에서 SQL 인스턴스로의 연결은 보안되어야 하며 SQL Server 2012 또는 SQL Server 2014 버전이어야 합니다. 연결을 보호하려면 Microsoft Management Console을 사용하여 SQL Server 인스턴스에 대한 SSL 암호화를 사용하도록 설정하는 방법을 참조하십시오.
2. 서비스가 제대로 다시 시작되지 않으면 다음을 확인하십시오. **Services.msc**를 엽니다.
    a. SQL Server 서비스에 사용되는 로그온 계정 정보를 복사합니다.
    b. SQL Server에서 MMC.exe를 엽니다.
    c. **파일** > **스냅인 추가/제거**로 이동한 다음 인증서 항목을 두 번 클릭하여 인증서 스냅인을 추가합니다. 마법사의 두 페이지에서 컴퓨터 계정과 로컬 컴퓨터를 선택합니다.
    d. **확인**을 클릭합니다.
    e. **인증서 (로컬 컴퓨터) > 개인 > 인증서**를 확장하고 가져온 SSL 인증서를 찾습니다.
    f. 가져온 인증서(SQL Server 구성 관리자에서 선택됨)를 마우스 오른쪽 버튼으로 클릭한 다음 **모든 작업 > 개인 키 관리**를 클릭합니다.
    g. **그룹 또는 사용자 이름** 아래에서 **추가**를 클릭합니다.
    h. 이전 단계에서 복사한 SQL 서비스 계정 이름을 입력합니다.
    i. **모든 권한 허용** 옵션을 지웁니다. 기본적으로 서비스 계정은 모든 권한 및 읽기 권한을 모두 가지고 있지만, 개인 키를 읽을 수만 있어야 합니다.
    j. **MMC**를 닫고 SQL 서비스를 시작합니다.
3. SQL 서비스가 올바르게 시작되었는지 확인합니다.

인터넷 정보 서비스(IIS) 필수 구성 요소

1. 루트 인증서(base 64)를 다운로드합니다.
2. 루트 인증서를 IIS 서버의 기본 사이트인 C:\\inetpub\\wwwroot에 복사합니다.
3. 기본 사이트의 **인증** 확인란을 선택합니다.

4. **익명**을 **사용**으로 설정합니다.
5. **실패한 요청 추적** 규칙 확인란을 선택합니다.
6. .cer이 차단되지 않았는지 확인합니다.
7. 로컬 서버에서 웹 브라우저를 통해 .cer 위치로 이동합니다. `https://localhost/certname.cer` 브라우저에 루트 인증서 텍스트가 나타납니다.
8. 웹 브라우저에 루트 인증서가 나타나지 않으면 다음과 같이 IIS 서버에서 ASP가 활성화되어 있는지 확인합니다.

    a. 서버 관리자를 엽니다.
    b. **관리 > 역할 및 기능 추가**에서 마법사로 이동합니다.
    c. 서버 역할에서 **웹 서버(IIS)**를 확장하고, **웹 서버**를 확장하고, **응용 프로그램 개발**을 확장한 다음, **ASP**를 선택합니다.
    d. 설치가 완료될 때까지 **다음**을 클릭합니다.

9. `https://localhost/cert.cer`(으)로 이동합니다.

    자세한 내용은 Web Server (IIS)을(를) 참조하십시오.

> **참고:**
>
> 이 절차에 CA의 IIS 인스턴스를 사용할 수 있습니다.

초기 FIPS 구성 중 루트 인증서 가져오기

명령줄 콘솔에서 XenMobile을 처음 구성하는 단계를 완료할 때 루트 인증서를 가져오려면 다음 설정을 완료해야 합니다. 설치 단계에 대한 자세한 내용은 Installing XenMobile을(를) 참조하십시오.

- FIPS 사용: 예
- 루트 인증서 업로드: 예
- 복사(c) 또는 가져오기(i): i
- 가져올 HTTP URL 입력: `https://<FQDN of IIS server>/cert.cer`
- 서버: *SQL Server의 FQDN*
- 포트: 1433
- 사용자 이름: 데이터베이스를 생성할 수 있는 서비스 계정 (`domain\username`).
- 암호: 서비스 계정의 암호.

- 데이터베이스 이름: 선택한 이름.

모바일 장치에서 FIPS 모드 활성화

기본적으로 모바일 장치에서는 FIPS 모드가 비활성화되어 있습니다. FIPS 모드를 활성화하려면 **설정 > 클라이언트 속성**으로 이동하여 **FIPS 모드 활성화** 속성을 편집하고 값을 **true**로 설정합니다. 자세한 내용은 클라이언트 속성을 참조하십시오.

클러스터링 구성

클러스터링을 구성하려면 Citrix ADC에서 다음 두 가지 로드 밸런싱 가상 IP 주소를 구성합니다.

- **모바일 장치 관리(MDM) 로드 밸런싱 가상 IP 주소:** 클러스터로 구성된 XenMobile® 노드와 통신하려면 MDM 로드 밸런싱 가상 IP 주소가 필요합니다. 이 로드 밸런싱은 SSL Bridge 모드에서 수행됩니다.
- **모바일 앱 관리(MAM) 로드 밸런싱 가상 IP 주소:** MAM 로드 밸런싱 가상 IP 주소는 Citrix Gateway가 클러스터로 구성된 XenMobile 노드와 통신하는 데 필요합니다. XenMobile에서는 기본적으로 Citrix Gateway의 모든 트래픽이 포트 8443의 로드 밸런싱 가상 IP 주소로 라우팅됩니다.

이 섹션의 절차에서는 XenMobile 가상 머신(VM)을 만들고 새 VM을 기존 VM에 연결하는 방법을 설명합니다. 이러한 단계는 클러스터 설정을 생성합니다.

전제 조건

- 필요한 XenMobile 노드를 완전히 구성했습니다.
- 모든 클러스터 노드와 XenMobile 데이터베이스에 NTP를 구성합니다. 클러스터링이 제대로 작동하려면 모든 서버의 시간이 동일해야 합니다.
- MDM 로드 밸런서용 공용 IP 주소 1개와 MAM용 사설 IP 주소 1개.
- 서버 인증서.
- Citrix Gateway 가상 IP 주소용 여유 IP 1개.
- 클러스터 설정 및 MDM 전용 또는 엔터프라이즈 모드(MDM+MAM)로 배포된 XenMobile의 경우: 모든 Citrix ADC MDM 로드 밸런서, 즉 포트 8443 및 443에 설정된 가상 서버에 **원본 IP 고정**을 사용하도록 Citrix ADC 로드 밸런서 구성을 수정합니다. 사용자 장치가 iOS 11로 업그레이드하기 전에 해당 구성을 완료하십시오. 자세한 내용은 다음 Citrix Knowledge Center 문서를 참조하십시오. `<https://support.citrix.com/article/CTX227406>`.
- iOS 11 장치에 XenMobile Store에서 앱을 설치하려면 XenMobile Server에서 포트 80을 활성화해야 합니다.

클러스터 구성의 XenMobile 10.x에 대한 참조 아키텍처 다이어그램은 아키텍처를 참조하십시오.

XenMobile 클러스터 노드 설치

필요한 노드 수에 따라 XenMobile VM을 생성합니다. 새 VM을 동일한 데이터베이스로 지정하고 동일한 PKI 인증서 암호를 제공합니다.

1. 새 VM의 명령줄 콘솔을 열고 관리자 계정의 새 암호를 입력합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-admin-password-cli.png)

2. 다음 그림과 같이 네트워크 구성 세부 정보를 제공합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-ip-address.png)

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

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-encryption-passphrase.png)

4. FIPS를 사용하려면 **y**를 입력합니다. 또는 **n**을 입력합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-fips-no.png)

5. 이전에 완전히 구성된 VM이 가리키던 동일한 데이터베이스를 가리키도록 데이터베이스를 구성합니다. 메시지가 표시됩니다: `Database already exists`.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-same-db-pointed.png)

6. 첫 번째 VM에 제공했던 인증서에 대해 동일한 암호를 입력합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-connect-existing-db3.png)

   암호를 입력하면 두 번째 노드의 초기 구성이 완료됩니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-initial-config-complete2.png)

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

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-node2-connected.png)

   > **참고:**
   >
   > 로그온 대화 상자는 첫 번째 VM의 로그온 대화 상자와 유사합니다. 이 일치는 두 VM이 동일한 데이터베이스 서버를 사용하고 있음을 확인할 수 있는 방법입니다.

8. XenMobile의 FQDN(정규화된 도메인 이름)을 사용하여 웹 브라우저에서 XenMobile 콘솔을 엽니다.
9. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 렌치 아이콘을 클릭합니다.

클러스터 정보 구성 화면(/en-us/xenmobile/server/media/select-support-wrench.png)

지원 페이지가 열립니다.

10. **고급** 아래에서 **클러스터 정보**를 클릭합니다.

    클러스터 정보 구성 화면(/en-us/xenmobile/server/media/support-page.png)

    클러스터 멤버, 장치 연결 정보, 작업 등 클러스터에 대한 모든 정보가 나타납니다. 새 노드는 이제 클러스터의 멤버입니다.

    클러스터 정보 구성 화면(/en-us/xenmobile/server/media/xmob-cluster-info-in-xm.png)

    동일한 단계를 따라 다른 노드를 추가할 수 있습니다. 클러스터에 처음 추가된 노드는 **OLDEST** 역할을 가집니다. 그 이후에 추가된 노드는 **NONE** 또는 **null** 역할을 표시합니다.

Citrix ADC에서 XenMobile 클러스터에 대한 로드 밸런싱 구성

필요한 노드를 XenMobile 클러스터의 멤버로 추가한 후, 클러스터에 액세스할 수 있도록 노드의 로드 밸런싱을 수행합니다. 로드 밸런싱은 Citrix ADC에서 사용할 수 있는 XenMobile 마법사를 실행하여 수행됩니다. 다음 단계에서는 마법사를 실행하여 XenMobile의 로드 밸런싱을 수행하는 방법을 설명합니다.

1. Citrix ADC에 로그인합니다.
2. 구성 탭에서 **XenMobile**을 클릭한 다음 **시작하기**를 클릭합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-ns-xm-wizard.png)

3. **Citrix Gateway를 통한 액세스** 확인란과 **XenMobile 서버 로드 밸런싱** 확인란을 선택한 다음 **계속**을 클릭합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-ns-xm-wizard-chck.png)

4. Citrix Gateway의 IP 주소를 입력한 다음 **계속**을 클릭합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-ng-vip.png)

5. 다음 중 하나를 수행하여 서버 인증서를 Citrix Gateway 가상 IP 주소에 바인딩한 다음 **계속**을 클릭합니다.

   - **기존 인증서 사용**에서 목록에서 서버 인증서를 선택합니다.
   - 새 서버 인증서를 업로드하려면 **인증서 설치** 탭을 클릭합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-ng-xm-wizard-ag-vip-cert-bind.png)

6. 인증 서버 세부 정보를 입력한 다음 **계속**을 클릭합니다.

클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-ng-vip-ad.png)

> **참고:**
>
> 서버 로그온 이름 특성이 XenMobile LDAP 구성에서 제공한 것과 동일한지 확인하십시오.

7. XenMobile 설정 아래에서 MAM에 대한 로드 밸런싱 FQDN을 입력한 다음 **계속**을 클릭합니다.

   클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mam-vip.png)

   > **참고:**
   >
   > MAM 로드 밸런싱 가상 IP 주소의 FQDN과 XenMobile의 FQDN이 동일한지 확인합니다.

8. SSL 브리지 모드(HTTPS)를 사용하려면 **XenMobile Server에 대한 HTTPS 통신**을 선택합니다. 그러나 SSL 오프로드를 사용하려면 이전 그림과 같이 **XenMobile Server에 대한 HTTP 통신**을 선택합니다. 이 문서에서는 SSL 브리지 모드(HTTPS)를 선택합니다.
9. MAM 로드 밸런싱 가상 IP 주소에 대한 서버 인증서를 바인딩한 다음 계속을 클릭합니다. 클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-ns-xm-wizard-mam-vip-certbind.png)
10. XenMobile 서버 아래에서 **서버 추가**를 클릭하여 XenMobile 노드를 추가합니다.

    클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mam-vip-addnodes.png)

11. XenMobile 노드의 IP 주소를 입력한 다음 추가를 클릭합니다.

    클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard.mam-vip-addnodes1.png)

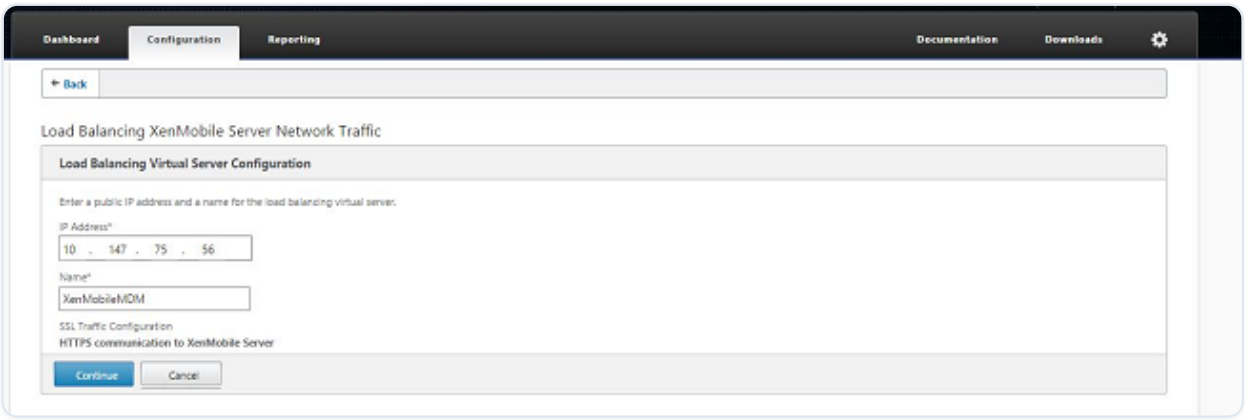
12. 10단계와 11단계를 반복하여 XenMobile 클러스터의 일부인 XenMobile 노드를 더 추가합니다. 추가한 모든 XenMobile 노드가 표시됩니다. 계속을 클릭합니다.

    클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mam-vip-addnodes2.png)

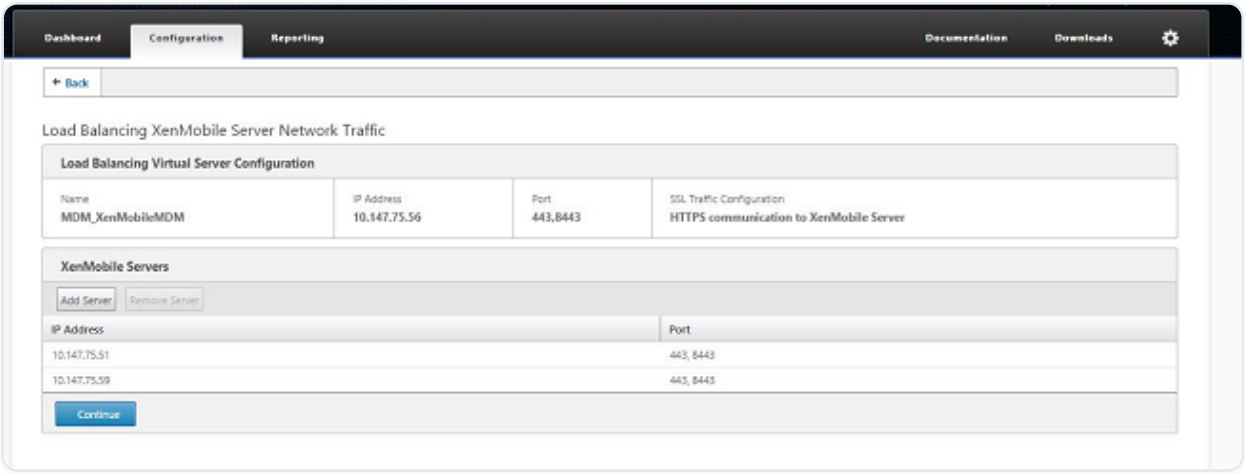
13. MDM 로드 밸런싱 구성을 계속하려면 **장치 관리자 서버 로드 밸런싱**을 클릭합니다.

    클러스터 노드 설정(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mdm-vip.png)

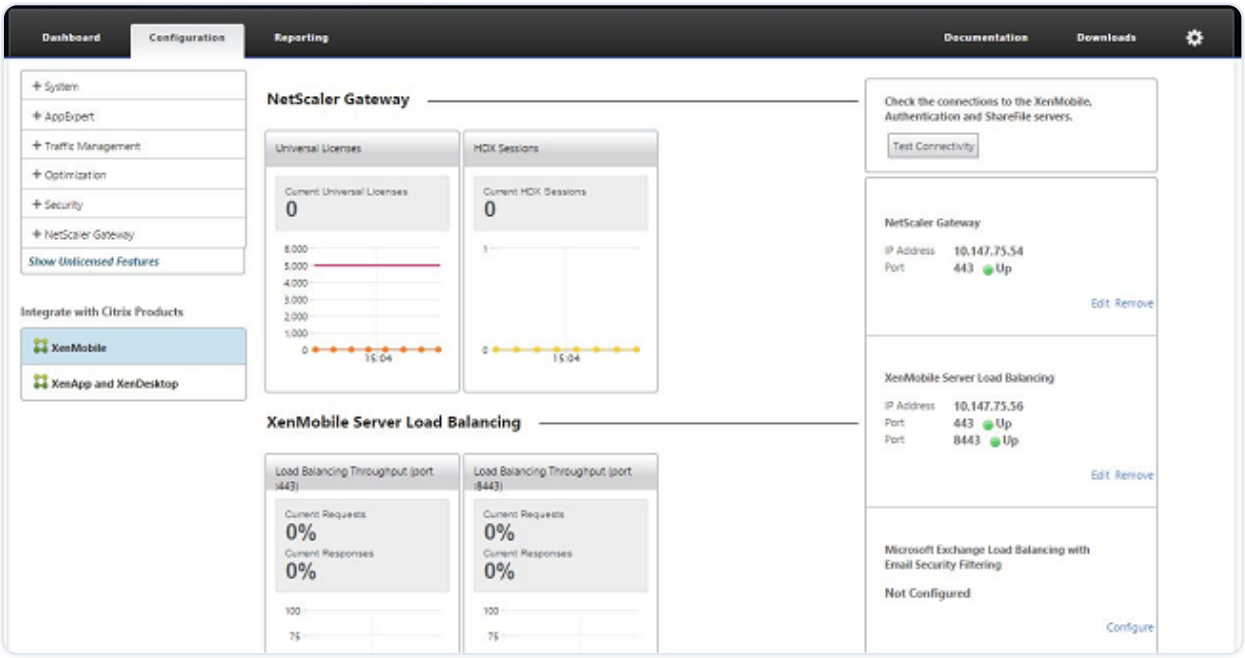
14. MDM 로드 밸런싱 IP 주소에 사용할 IP 주소를 입력한 다음 **계속**을 클릭합니다.



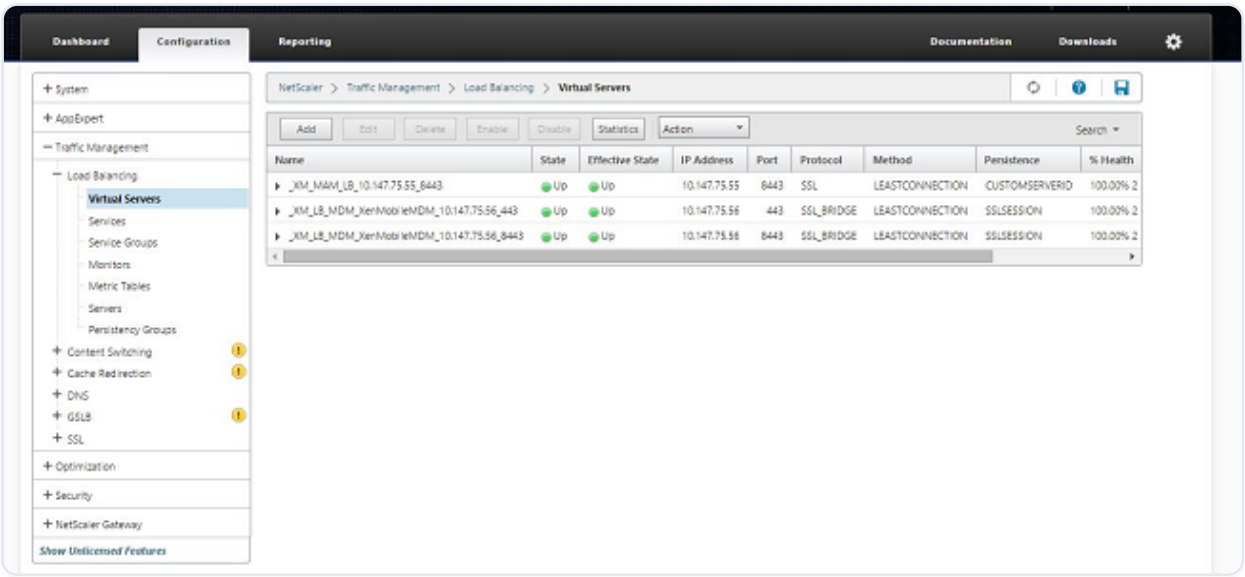
15. 목록에서 XenMobile 노드를 확인한 후, **계속**을 클릭한 다음 완료를 클릭하여 프로세스를 마칩니다.



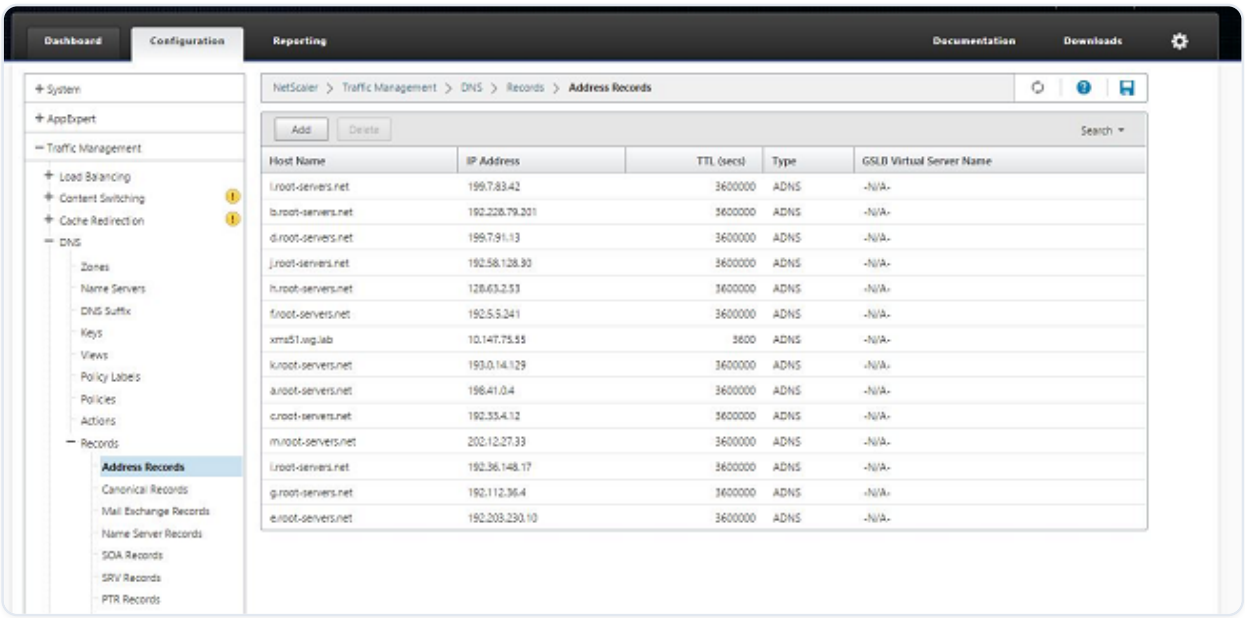
XenMobile 페이지에서 가상 IP 주소 상태를 확인할 수 있습니다.



16. 가상 IP 주소가 작동 중인지 확인하려면 구성 탭을 클릭한 다음 **트래픽 관리 > 로드 밸런싱 > 가상 서버**로 이동합니다.



또한 Citrix ADC의 DNS 항목이 MAM 로드 밸런싱 가상 IP 주소를 가리키는 것을 확인할 수 있습니다.



재해 복구 가이드

활성-수동 페일오버 전략을 사용하여 재해 복구를 위한 여러 사이트를 포함하는 XenMobile 배포를 설계하고 구성할 수 있습니다. 자세한 내용은 XenMobile 배포 핸드북의 재해 복구 문서를 참조하십시오.

프록시 서버 활성화

아웃바운드 인터넷 트래픽을 제어하기 위해 XenMobile®에서 프록시 서버를 설정하여 해당 트래픽을 전달할 수 있습니다. 프록시 서버는 명령줄 인터페이스(CLI)를 통해 설정합니다. 프록시 서버를 설정하려면 시스템을 다시 시작해야 합니다.

1. XenMobile CLI 주 메뉴에서 **2**를 입력하여 시스템 메뉴를 선택합니다.

2. 시스템 메뉴에서 **6**을 입력하여 프록시 서버 메뉴를 선택합니다.

   프록시 서버 설정 이미지(/en-us/xenmobile/server/media/proxy-server-setup-1.png)

3. 프록시 구성 메뉴에서 **1**을 입력하여 SOCKS를 선택합니다.

   이 설정을 저장하기 전에 HTTPS도 구성해야 합니다. 프록시는 SOCKS 및 HTTPS 설정을 동일한 구성으로 저장해야만 작동합니다.

   프록시 서버 설정 이미지(/en-us/xenmobile/server/media/proxy-server-setup-2.png)

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

   프록시 서버 설정 이미지(/en-us/xenmobile/server/media/proxy-server-setup-3.png)

5. **n**을 입력한 다음 **2**를 입력하여 HTTPS를 선택합니다.
6. 프록시 서버 IP 주소, 포트 번호 및 대상을 입력합니다.
7. 프록시 서버에서 인증을 위해 사용자 이름과 암호를 구성하려면 **y**를 입력한 다음 사용자 이름과 암호를 입력합니다.

   프록시 서버 설정 이미지(/en-us/xenmobile/server/media/proxy-server-setup-4.png)

8. 설정을 저장하려면 **y**를 입력합니다.

SQL Server 구성

온프레미스 XenMobile® Server에서 SQL Server로 연결하려면 다음 드라이버 중 하나를 사용할 수 있습니다:

- 기본 드라이버

- jTDS
- 마이크로소프트 자바 데이터베이스 연결 (JDBC) 드라이버

jTDS 드라이버는 다음 경우에 기본 드라이버입니다:

- 온프레미스 XenMobile Server를 설치합니다.
- jTDS 드라이버를 사용하도록 구성된 XenMobile Server에서 업그레이드합니다.

두 드라이버 모두 XenMobile은 SQL Server 인증 또는 Windows 인증을 지원합니다. 이러한 인증 및 드라이버 조합의 경우 SSL을 켜거나 끌 수 있습니다.

Microsoft JDBC 드라이버와 함께 Windows 인증을 사용하는 경우, 드라이버는 Kerberos를 사용하여 통합 인증을 수행합니다. XenMobile은 Kerberos에 연결하여 Kerberos Key Distribution Center (KDC) 세부 정보를 가져옵니다. 필요한 세부 정보를 사용할 수 없는 경우 XenMobile CLI는 Active Directory 서버의 IP 주소를 묻는 메시지를 표시합니다.

jTDS 드라이버에서 JDBC 드라이버로 전환하려면 모든 XenMobile Server 노드에 SSH로 연결하고 XenMobile CLI를 사용하여 구성하십시오. 단계는 현재 jTDS 드라이버 구성에 따라 다음과 같이 달라집니다.

Microsoft JDBC로 전환 (SQL Server 인증)

이 단계를 완료하려면 SQL Server 사용자 이름과 암호가 필요합니다.

1. 모든 XenMobile Server 노드에 SSH로 연결합니다.
2. XenMobile CLI 주 메뉴에서 **2**를 입력하여 **시스템 메뉴**를 선택합니다.
3. 고급 설정을 선택하려면 **12**를 입력합니다.
4. JDBC 드라이버 전환을 선택하려면 **7**을 입력한 다음, Microsoft의 경우 **m**을 입력합니다.

   JDBC 드라이버 선택 이미지(/en-us/xenmobile/server/media/cli-choose-jdbc-driver.png)
5. 메시지가 표시되면 SQL 인증을 선택하려면 **y**를 입력한 다음, SQL Server 사용자 이름과 암호를 입력합니다.
6. 각 XenMobile Server 노드에 대해 이 단계를 반복합니다.
7. 각 XenMobile Server 노드를 다시 시작합니다.

Microsoft JDBC로 전환 (SSL 꺼짐; Windows 인증)

이 단계를 완료하려면 Active Directory 사용자 이름과 암호, Kerberos KDC 영역, KDC 사용자 이름이 필요합니다.

1. 모든 XenMobile Server 노드에 SSH로 연결합니다.
2. XenMobile CLI 주 메뉴에서 **2**를 입력하여 **시스템 메뉴**를 선택합니다.
3. 고급 설정을 선택하려면 **12**를 입력합니다.
4. JDBC 드라이버 전환을 선택하려면 **7**을 입력한 다음, **m**을 입력합니다.
5. SQL Server 인증을 사용할지 묻는 메시지가 표시되면 **n**을 입력합니다.
6. 메시지가 표시되면 SQL 서버에 대해 구성된 Active Directory 사용자 이름과 암호를 입력합니다.
7. XenMobile이 Kerberos KDC 영역을 자동으로 검색하지 못하면 SQL 서버 FQDN을 포함한 KDC 세부 정보를 묻는 메시지가 표시됩니다.
8. SSL 사용 여부를 묻는 메시지가 나타나면 **n**을 입력합니다. XenMobile이 구성을 저장합니다. 오류로 인해 XenMobile이 구성을 저장할 수 없는 경우 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

Citrix Support에서 암호 변경을 지시하는 경우와 같이 XenMobile 데이터베이스 암호를 변경하려면 다음 지침을 따르십시오.

SQL 서버에서 Windows 인증을 사용하는 경우 Windows Active Directory에서 데이터베이스 암호를 변경합니다. 그런 다음 데이터베이스 서버에서 데이터베이스 관리자 계정을 새로 고쳐 암호 변경을 동기화합니다. 그런 다음 다음과 같이 XenMobile에서 암호를 변경할 수 있습니다.

중요:

- XenMobile에서 데이터베이스 암호를 변경하기 위한 예약된 유지 관리 기간을 계획하십시오. 암호 변경은 시스템 다운타임 중에 이루어져야 합니다.
- 암호를 변경할 때 모든 XenMobile 노드가 네트워크에 연결되어 있는지 확인하십시오. 암호를 변경한 후 XenMobile을 다시 시작하십시오.

  암호 변경 후 XenMobile을 다시 시작하지 않으면 XenMobile이 복구 모드로 전환됩니다. 이 경우 SQL 서버에서 이전 암호로 되돌리고 XenMobile을 다시 시작한 다음 암호를 다시 변경하십시오.

1. 모든 XenMobile Server 노드가 실행 중인지 확인합니다. 클러스터된 환경의 경우 모든 노드를 시작합니다.

2. 가상 서버를 비활성화하여 Citrix ADC 로드 밸런서에서 XenMobile로 들어오는 장치 트래픽을 차단합니다.
3. SQL 서버에서 데이터베이스 암호를 변경하려면: XenMobile CLI에 로그인하고 **Configuration > Database**로 이동한 다음 메시지가 표시되면 변경된 암호를 입력합니다.

```
Server []: <ipAddress>

Port [1433]: 1433

Username [sa]: <userName>

Password: <****>
```

4. 서버를 다시 시작하려면 **Y**를 선택합니다.
5. 클러스터의 다른 모든 노드에 대해 3단계와 4단계를 반복합니다.
6. Citrix ADC 로드 밸런서에서 가상 서버를 활성화하여 수신 장치 트래픽을 차단 해제합니다.

서버 속성

XenMobile®에는 서버 전체 작업에 적용되는 많은 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 **추가**를 클릭한 다음, **키**에서 **사용자 지정 키**를 선택합니다.

일반적으로 구성되는 속성에 대한 자세한 내용은 XenMobile 가상 핸드북의 서버 속성을 참조하십시오.

서버 속성 정의

항상 장치 추가

- **true**인 경우, XenMobile은 등록에 실패하더라도 장치를 XenMobile 콘솔에 추가하여 어떤 장치가 등록을 시도했는지 확인할 수 있도록 합니다. 기본값은 **false**입니다.

AG 클라이언트 인증서 발급 제한 간격

- 인증서 생성 간의 유예 기간입니다. 이 간격은 XenMobile이 짧은 시간 내에 장치에 대해 여러 인증서를 생성하는 것을 방지합니다. Citrix®는 이 값을 변경하지 않는 것이 좋습니다. 기본값은 **30**분입니다.

감사 로그 정리 실행 시간

- 감사 로그 정리를 시작할 시간으로, HH:MM AM/PM 형식입니다. 예시: 04:00 AM. 기본값은 **02:00 AM** 입니다.

감사 로그 정리 간격 (일 단위)

- XenMobile이 감사 로그를 보관하는 일수입니다. 기본값은 **1**입니다.

감사 로거

- **False**인 경우, 사용자 인터페이스(UI) 이벤트를 기록하지 않습니다. 기본값은 **False**입니다.

감사 로그 보존 (일 단위)

- XenMobile이 감사 로그를 보존하는 일수입니다. 기본값은 **7**입니다.

auth.ldap.connect.timeout 및 auth.ldap.read.timeout

- 느린 LDAP 응답을 보완하기 위해 Citrix는 다음 사용자 지정 키에 대한 서버 속성을 추가할 것을 권장합니다.
  - 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 초과**

인증서 갱신 (초 단위)

- XenMobile이 인증서 갱신을 시작하는 시점인 인증서 만료 전 시간(초)입니다. 예를 들어, 인증서가 12월 30일에 만료되고 이 속성이 30일로 설정된 경우: 장치가 12월 1일에서 12월 30일 사이에 연결되면 XenMobile은 인증서 갱신을 시도합니다. 기본값은 **2592000**초(30일)입니다.

연결 시간 초과

- XenMobile이 장치에 대한 TCP 연결을 닫은 후의 세션 비활성 시간 초과(분)입니다. 세션은 열린 상태로 유지됩니다. Android 장치 및 원격 지원에 적용됩니다. 기본값은 **5**분입니다.

Microsoft 인증 서버에 대한 연결 시간 초과

- XenMobile이 인증서 서버로부터 응답을 기다리는 시간(초)입니다. 인증서 서버가 느리거나 트래픽이 많으면 이 값을 60초 이상으로 늘리십시오. 120초 후에도 응답하지 않는 인증서 서버는 유지 관리가 필요합니다. 기본값은 **15000**밀리초(15초)입니다.

기본 배포 채널

- XenMobile이 장치에 리소스를 배포하는 방법을 결정합니다. 사용자 수준(**DEFAULT_TO_USER**) 또는 장치 수준에서 배포합니다. 기본값은 **DEFAULT_TO_DEVICE**입니다.

배포 로그 정리(일)

- XenMobile이 배포 로그를 보관하는 일수입니다. 기본값은 **7**입니다.

호스트 이름 확인 비활성화

- 기본적으로 Microsoft PKI 서버를 제외한 아웃바운드 연결에서는 호스트 이름 확인이 활성화됩니다. 호스트 이름 확인이 실패하면 서버 로그에 다음과 같은 오류가 포함됩니다. “볼륨 구매 서버에 연결할 수 없습니다: 호스트 이름 '192.0.2.0'이 피어에서 제공한 인증서 주체와 일치하지 않습니다”. 호스트 이름 확인으로 인해 배포에 문제가 발생하면 이 속성을 **true**로 변경하십시오. 기본값은 **false**입니다.

SSL 서버 확인 비활성화

- **True**인 경우, 다음 모든 조건이 충족될 때 SSL 서버 인증서 유효성 검사를 비활성화합니다.
    - XenMobile Server에서 인증서 기반 인증을 활성화했습니다.
    - Microsoft CA 서버가 인증서 발급자입니다.
    - 내부 CA가 인증서에 서명했지만, 해당 CA의 루트를 XenMobile Server가 신뢰하지 않습니다.

기본값은 **True**입니다.

콘솔 사용

- **true**인 경우, 사용자가 셀프 서비스 포털 콘솔에 액세스할 수 있도록 설정합니다. 기본값은 **true**입니다.

충돌 보고 사용

- **true**인 경우, Citrix는 iOS 및 Android용 Secure Hub 문제 해결에 도움이 되도록 충돌 보고서 및 진단 정보를 수집합니다. **false**인 경우, 데이터가 수집되지 않습니다. 기본값은 **true**입니다.

진단을 위한 Hibernate 통계 로깅 사용/사용 안 함

- **True**인 경우, 애플리케이션 성능 문제 해결을 돕기 위해 Hibernate 통계 로깅을 사용하도록 설정합니다. Hibernate는 XenMobile이 Microsoft SQL Server에 연결하는 데 사용되는 구성 요소입니다. 기본적으로 로깅은 애플리케이션 성능에 영향을 미치므로 비활성화되어 있습니다. 거대한 로그 파일이 생성되는 것을 방지하려면 짧은 기간 동안만 로깅을 활성화하십시오. XenMobile은 로그를 /opt/sas/logs/hibernate_stats.log에 기록합니다. 기본값은 **False**입니다.

macOS OTAE 사용

- **false**인 경우, macOS 장치에 대한 등록 링크 사용을 방지합니다. 즉, macOS 사용자는 등록 초대장을 통해서만 등록할 수 있습니다. 기본값은 **true**입니다.

알림 트리거 사용

- Secure Hub 클라이언트 알림을 사용하거나 사용하지 않도록 설정합니다. 값이 **true**이면 알림이 활성화됩니다. 기본값은 **true**입니다.

force.server.push.required.apps

- 다음과 같은 상황에서 Android 및 iOS 장치에 필수 앱을 강제로 배포하도록 설정합니다.
  - 새 앱을 업로드하고 필수로 표시하는 경우.
  - 기존 앱을 필수로 표시합니다.
  - 사용자가 필수 앱을 삭제합니다.
  - Secure Hub 업데이트를 사용할 수 있습니다.

필수 앱의 강제 배포는 기본적으로 **false**입니다. 강제 배포를 활성화하려면 사용자 지정 키를 생성하고 **값**을 **true**로 설정합니다. 강제 배포 중에는 엔터프라이즈 앱 및 공용 앱 스토어 앱을 포함한 MDX 지원 필수 앱이 즉시 업그레이드됩니다. 앱 업데이트 유예 기간에 대한 MDX 정책을 구성하고 사용자가 나중에 앱을 업그레이드하도록 선택하더라도 업그레이드가 발생합니다.

- 키: **사용자 지정 키**
- 키: **force.server.push.required.apps**
- 값: **false**
- 표시 이름: **force.server.push.required.apps**

- 설명: **필수 앱 강제 배포**

ActiveSync 허용 및 거부된 사용자 전체 가져오기

- XenMobile이 ActiveSync 허용 및 거부된 사용자 전체 목록(기준선)을 가져오는 간격(초)입니다. 기본값은 **28800**초입니다.

hibernate.c3p0.idle_test_period

- 이 XenMobile Server 속성(사용자 지정 키)은 연결이 자동으로 유효성 검사되기 전의 유휴 시간(초)을 결정합니다. 키는 다음과 같이 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 XenMobile이 SQL Server 데이터베이스에 열 수 있는 최대 연결 수를 결정합니다. XenMobile은 이 사용자 지정 키에 지정한 값을 상한으로 사용합니다. 연결은 필요한 경우에만 열립니다. 데이터베이스 서버의 용량에 따라 설정을 조정하십시오. 자세한 내용은 XenMobile 작업 튜닝을 참조하십시오. 키는 다음과 같이 구성합니다. 기본값은 **1000**입니다.
- 키: **hibernate.c3p0.max_size**
- 값: **1000**
- 표시 이름: **hibernate.c3p0.max_size**
- 설명: **SQL에 대한 DB 연결**

hibernate.c3p0.min_size

- 이 사용자 지정 키는 XenMobile이 SQL Server 데이터베이스에 여는 최소 연결 수를 결정합니다. 키는 다음과 같이 구성합니다. 기본값은 **100**입니다.
- 키: **hibernate.c3p0.min_size**
- 값: **100**
- 표시 이름: **hibernate.c3p0.min_size**
- 설명: **SQL에 대한 DB 연결**

hibernate.c3p0.timeout

- 이 사용자 지정 키는 유휴 시간 제한(초)을 결정합니다. 기본값은 **120**입니다.
- 키: **사용자 지정 키**
- 키: **hibernate.c3p0.timeout**
- 값: **120**
- 표시 이름: **hibernate.c3p0.timeout**
- 설명: **데이터베이스 유휴 시간 제한**

원격 분석 활성화 여부 식별

- 원격 분석(고객 환경 개선 프로그램 또는 CEIP)이 활성화되었는지 여부를 식별합니다. XenMobile을 설치하거나 업그레이드할 때 CEIP에 참여할 수 있습니다. XenMobile에서 15회 연속 업로드 실패가 발생하면 원격 분석이 비활성화됩니다. 기본값은 **false**입니다.

비활성 시간 제한(분)

- **WebServices 시간 제한 유형** 서버 속성이 **INACTIVITY_TIMEOUT**인 경우: 이 속성은 다음 작업을 수행한 비활성 관리자를 XenMobile이 로그아웃시키는 시간(분)을 정의합니다.
  - REST 서비스를 위한 XenMobile 공개 API를 사용하여 XenMobile 콘솔에 액세스했습니다.
  - REST 서비스를 위한 XenMobile 공개 API를 사용하여 타사 앱에 액세스했습니다. 시간 제한이 **0**이면 비활성 사용자가 계속 로그인되어 있음을 의미합니다.

기본값은 **5**입니다.

iOS 장치 관리 등록 자동 설치 활성화됨

- 이 속성이 true이면 장치 등록 중에 필요한 사용자 상호 작용의 양이 줄어듭니다. 사용자는 **루트 CA 설치**(필요한 경우) 및 **MDM 프로필 설치**를 클릭해야 합니다.

iOS 장치 관리 등록 첫 번째 단계 지연

- 사용자가 장치 등록 중에 자격 증명을 입력한 후, 이 값은 루트 CA를 요청하기 전에 대기할 시간을 지정합니다. Citrix는 네트워크 지연 또는 속도 문제에 대해서만 이 속성을 편집할 것을 권장합니다. 이 경우 값을 5000밀리초(5초) 이상으로 설정하지 마십시오. 기본값은 **1000**밀리초(1초)입니다.

iOS 장치 관리 등록 마지막 단계 지연

- 장치 등록 중에 이 속성 값은 MDM 프로필 설치와 장치에서 에이전트 시작 사이에 대기할 시간을 지정합니다. Citrix는 네트워크 지연 또는 속도 문제에 대해서만 이 속성을 편집할 것을 권장합니다. 이 경우 값을 5000밀리초(5초) 이상으로 설정하지 마십시오. 기본값은 **1000**밀리초(1초)입니다.

iOS 장치 관리 ID 전달 모드

- XenMobile이 MDM 인증서를 장치에 배포할 때 **SCEP**(보안상의 이유로 권장) 또는 **PKCS12** 중 어떤 방식을 사용할지 지정합니다. PKCS12 모드에서는 키 쌍이 서버에서 생성되며 협상이 수행되지 않습니다. 기본값은 **SCEP**입니다.

iOS 장치 관리 ID 키 크기

- MDM ID, iOS 프로필 서비스 및 XenMobile iOS 에이전트 ID에 대한 개인 키 크기를 정의합니다. 기본값은 **1024**입니다.

iOS 장치 관리 ID 갱신 일수

- 인증서 만료 전 몇 일부터 XenMobile이 인증서 갱신을 시작할지 지정합니다. 예를 들어, 인증서가 10일 후에 만료되고 이 속성이 **10**일인 경우, 장치가 만료 9일 전에 연결하면 XenMobile은 새 인증서를 발급합니다. 기본값은 **30**일입니다.

iOS MDM APNS 개인 키 암호

- 이 속성에는 XenMobile이 Apple 서버로 알림을 푸시하는 데 필요한 APN 암호가 있습니다.

장치 연결 해제 전 비활성 기간

- XenMobile이 장치를 연결 해제하기 전에 마지막 인증을 포함하여 장치가 비활성 상태로 유지될 수 있는 기간을 지정합니다. 기본값은 **7**일입니다.

MAM 전용 장치 최대값

- 이 사용자 지정 키는 각 사용자가 등록할 수 있는 MAM 전용 장치의 수를 제한합니다. 키는 다음과 같이 구성합니다. **값**이 **0**이면 무제한 장치 등록이 허용됩니다.
- 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 볼륨 구매 라이선스를 가져올 때 사용되는 스레드 수입니다. 기본값은 **3**입니다. 추가 최적화가 필요한 경우 스레드 수를 늘릴 수 있습니다. 그러나 6개와 같이 스레드 수가 많으면 볼륨 구매 가져오기로 인해 CPU 사용량이 높아집니다.

Citrix ADC 단일 사인온

- **False**인 경우 Citrix ADC에서 XenMobile로의 단일 Sign-On 중에 XenMobile 콜백 기능을 비활성화합니다. Citrix Gateway 구성에 콜백 URL이 포함된 경우 XenMobile은 콜백 기능을 사용하여 Citrix Gateway 세션 ID를 확인합니다. 기본값은 **False**입니다.

연속 실패한 업로드 수

- CEIP(고객 환경 개선 프로그램) 업로드 중 연속 실패 횟수를 표시합니다. 업로드에 실패하면 XenMobile은 값을 증가시킵니다. 15회 업로드 실패 후 XenMobile은 원격 분석이라고도 하는 CEIP를 비활성화합니다. 자세한 내용은 서버 속성 **원격 분석 사용 여부 식별**을 참조하십시오. 업로드가 성공하면 XenMobile은 값을 **0**으로 재설정합니다.

장치당 사용자 수

- 동일한 장치를 MDM에 등록할 수 있는 최대 사용자 수입니다. **0** 값은 무제한의 사용자가 동일한 장치를 등록할 수 있음을 의미합니다. 기본값은 **0**입니다.

허용 및 거부된 사용자의 증분 변경 가져오기

- XenMobile이 ActiveSync 장치의 델타를 가져오기 위해 PowerShell 명령을 실행할 때 도메인에서 응답을 기다리는 시간(초)입니다. 기본값은 **60**초입니다.

Microsoft 인증 서버 읽기 시간 초과

- XenMobile이 읽기를 수행할 때 인증서 서버에서 응답을 기다리는 시간(초)입니다. 인증서 서버가 느리거나 트래픽이 많으면 이 값을 60초 이상으로 늘릴 수 있습니다. 120초 후에도 응답하지 않는 인증서 서버는 유지 관리가 필요합니다. 기본값은 **15000**밀리초(15초)입니다.

REST 웹 서비스

- REST 웹 서비스를 활성화합니다. 기본값은 **true**입니다.

지정된 크기의 청크로 장치 정보 검색

- 이 값은 장치 내보내기 중 멀티스레딩에 내부적으로 사용됩니다. 값이 높으면 단일 스레드가 더 많은 장치를 구문 분석합니다. 값이 낮으면 더 많은 스레드가 장치를 가져옵니다. 값을 줄이면 내보내기 및 장치 목록 가져오기 성능이 향상될 수 있지만 사용 가능한 메모리가 줄어들 수 있습니다. 기본값은 **1000**입니다.

세션 로그 정리(일)

- XenMobile이 세션 로그를 보관하는 일수입니다. 기본값은 **7**입니다.

서버 모드

- XenMobile이 MAM, MDM 또는 ENT(엔터프라이즈) 모드(각각 앱 관리, 장치 관리 또는 앱 및 장치 관리)로 실행되는지 여부를 결정합니다. 다음 표에 설명된 대로 장치를 등록하려는 방식에 따라 서버 모드 속성을 설정합니다. 서버 모드는 라이선스 유형에 관계없이 기본적으로 **ENT**로 설정됩니다.

XenMobile MDM Edition 라이선스가 있는 경우, **서버 속성**에서 서버 모드를 어떻게 설정하든 관계없이 유효 서버 모드는 항상 MDM입니다. MDM Edition 라이선스가 있는 경우 서버 모드를 MAM 또는 ENT로 설정하여 앱 관리를 활성화할 수 없습니다.

라이선스 에디션	**장치를 이 모드로 등록하려는 경우**	**서버 모드 속성을 다음으로 설정**
엔터프라이즈 / 고급	MDM 모드	MDM
엔터프라이즈 / 고급	MDM+MAM 모드	ENT
MDM	MDM 모드	MDM

유효 서버 모드는 라이선스 유형과 서버 모드의 조합입니다. MDM 라이선스의 경우 유효 서버 모드는 서버 모드 설정과 관계없이 항상 MDM입니다. 엔터프라이즈 및 고급 라이선스의 경우 서버 모드가 **ENT** 또는 **MDM**이면 유효 서버 모드는 서버 모드와 일치합니다. 서버 모드가 **MAM**인 경우 유효 서버 모드는 ENT입니다.

XenMobile은 다음 각 활동에 대해 서버 모드를 서버 로그에 추가합니다. 라이선스가 활성화되거나, 라이선스가 삭제되거나, **서버 속성**에서 서버 모드를 변경하는 경우. 로그 파일 생성 및 보기에 대한 자세한 내용은 로그 및 XenMobile에서 로그 파일 보기 및 분석를 참조하십시오.

ShareFile 구성 유형

- Citrix Files 저장소 유형을 지정합니다. **ENTERPRISE**는 Citrix Files 엔터프라이즈 모드를 활성화합니다. **CONNECTORS**는 XenMobile 콘솔을 통해 생성하는 저장소 영역 커넥터에만 액세스를 제공합니다. 기본값은 **NONE**이며, 이 경우 **구성 > ShareFile** 화면의 초기 보기가 표시되어 Citrix Files Enterprise와 커넥터 중에서 선택할 수 있습니다. 기본값은 **NONE**입니다.

정적 시간 제한(분)

- **WebServices 시간 제한 유형** 서버 속성이 **STATIC_TIMEOUT**인 경우: 이 속성은 다음을 사용한 후 XenMobile이 관리자를 로그아웃시키는 시간(분)을 정의합니다.
  - XenMobile 콘솔에 액세스하기 위한 REST 서비스용 XenMobile 공개 API.
  - 타사 앱에 액세스하기 위한 REST 서비스용 XenMobile 공개 API.

기본값은 **60**입니다.

트리거 에이전트 메시지 억제

- Secure Hub 클라이언트 메시징을 활성화하거나 비활성화합니다. 값이 **false**이면 메시징이 활성화됩니다. 기본값은 **true**입니다.

트리거 에이전트 사운드 억제

- Secure Hub 클라이언트 사운드를 활성화하거나 비활성화합니다. 값이 **false**이면 사운드가 활성화됩니다. 기본값은 **true**입니다.

Android 장치용 인증되지 않은 앱 다운로드

- **True**인 경우, Android Enterprise를 실행하는 Android 장치에 자체 호스팅 앱을 다운로드할 수 있습니다. Google Play 스토어에서 다운로드 URL을 정적으로 제공하는 Android Enterprise 옵션이 활성화된 경우 XenMobile에 이 속성이 필요합니다. 이 경우 다운로드 URL에는 인증 토큰이 있는 일회성 티켓(**XAM One-Time Ticket server** 속성으로 정의됨)을 포함할 수 없습니다. 기본값은 **False**입니다.

Windows 장치용 인증되지 않은 앱 다운로드

- 일회성 티켓을 검증하지 않는 이전 Secure Hub 버전에만 사용됩니다. **False**인 경우, XenMobile에서 Windows 장치로 인증되지 않은 앱을 다운로드할 수 있습니다. 기본값은 **False**입니다.

ActiveSync ID를 사용하여 ActiveSync 장치 초기화 수행

- **true**인 경우, Exchange ActiveSync용 Endpoint Management 커넥터는 ActiveSync 식별자를 asWipeDevice 메서드의 인수로 사용합니다. 기본값은 **false**입니다.

Exchange에서만 사용자

- **true**인 경우, ActiveSync Exchange 사용자에 대한 사용자 인증을 비활성화합니다. 기본값은 **false**입니다.

VP 기준 간격

- XenMobile이 Apple에서 볼륨 구매 라이선스를 다시 가져오는 최소 간격입니다. 라이선스 정보를 새로 고치면 볼륨 구매에서 수동으로 가져온 앱을 삭제하는 경우와 같은 모든 변경 사항이 XenMobile에 반영됩니다. 기본적으로 XenMobile은 최소 **720**분마다 볼륨 구매 라이선스 기준을 새로 고칩니다.

많은 볼륨 구매 라이선스(예: 50,000개 이상)를 설치한 경우: Citrix는 라이선스 가져오기 빈도와 오버헤드를 줄이기 위해 기준 간격을 늘릴 것을 권장합니다.

Apple에서 볼륨 구매 라이선스 변경이 자주 발생할 것으로 예상되는 경우: Citrix는 변경 사항으로 XenMobile을 업데이트된 상태로 유지하기 위해 값을 낮출 것을 권장합니다. 두 기준선 사이의 최소 간격은 60분입니다. 또한 XenMobile은 마지막 가져오기 이후의 변경 사항을 캡처하기 위해 60분마다 델타 가져오기를 수행합니다. 따라서 볼륨 구매 기준 간격이 60분인 경우 기준선 사이의 간격은 최대 119분까지 지연될 수 있습니다.

웹 서비스 시간 초과 유형

- 공개 API에서 검색된 인증 토큰을 만료시키는 방법을 지정합니다. **STATIC_TIMEOUT**인 경우 XenMobile은 서버 속성 **정적 시간 초과(분)**에 지정된 값 이후에 인증 토큰이 만료된 것으로 간주합니다.

INACTIVITY_TIMEOUT인 경우 XenMobile은 서버 속성 **비활성 시간 초과(분)**에 지정된 값 동안 토큰이 비활성 상태인 후에 인증 토큰이 만료된 것으로 간주합니다. 기본값은 **STATIC_TIMEOUT**입니다.

Windows WNS 채널 - 갱신 전 일수

- ChannelURI의 갱신 빈도입니다. 기본값은 **10**일입니다.

Windows WNS 하트비트 간격

- XenMobile이 3분마다 5번 장치에 연결한 후 장치에 다시 연결하기 전에 대기하는 시간입니다. 기본값은 **6**시간입니다.

XAM 일회성 티켓

- 일회성 인증 토큰(OTT)이 앱 다운로드에 유효한 밀리초 수입니다. 이 속성과 **Android용 인증되지 않은 앱 다운로드** 및 **Windows용 인증되지 않은 앱 다운로드** 속성은 함께 작동합니다. 이러한 속성은 인증되지 않은 앱 다운로드를 허용할지 여부를 지정합니다. 기본값은 **3600000**입니다.

XenMobile MDM 셀프 서비스 포털 콘솔 최대 비활성 간격(분)

- XenMobile이 비활성 사용자를 XenMobile 셀프 서비스 포털에서 로그아웃시키는 시간(분)입니다. 시간 초과가 **0**이면 비활성 사용자가 로그인 상태를 유지합니다. 기본값은 **30**입니다.

서버 속성 추가, 편집 또는 삭제

XenMobile에서 서버에 속성을 적용할 수 있습니다. 변경한 후에는 변경 사항을 커밋하고 활성화하려면 모든 노드에서 XenMobile을 다시 시작해야 합니다.

> **참고:**

> XenMobile을 다시 시작하려면 하이퍼바이저를 통해 명령 프롬프트를 사용하십시오.

1. XenMobile 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **서버** 아래에서 **서버 속성**을 클릭합니다. **서버 속성** 페이지가 나타납니다. 이 페이지에서 서버 속성을 추가, 편집 또는 삭제할 수 있습니다.

   서버 속성(/en-us/xenmobile/server/media/settings-server-server-properties.png)

서버 속성을 추가하려면

1. **추가**를 클릭합니다. **새 서버 속성 추가** 페이지가 나타납니다.

   서버 속성(/en-us/xenmobile/server/media/settings-server-server-properties-add.png)
2. 다음 설정을 구성합니다.

   - 키: 목록에서 적절한 키를 선택합니다. 키는 대소문자를 구분합니다. 속성 값을 편집하거나 특별한 키를 요청하기 전에 Citrix 지원팀에 문의하십시오.
   - 값: 선택한 키에 따라 값을 입력합니다.
   - 표시 이름: **서버 속성** 테이블에 나타나는 새 속성 값의 이름을 입력합니다.
   - 설명: 선택 사항으로 새 서버 속성에 대한 설명을 입력합니다.
3. **저장**을 클릭합니다.

서버 속성을 편집하려면

1. **서버 속성** 테이블에서 편집할 서버 속성을 선택합니다.

   서버 속성 옆의 확인란을 선택하면 서버 속성 목록 위에 옵션 메뉴가 나타납니다. 목록의 다른 아무 곳이나 클릭하여 목록 오른쪽에 옵션 메뉴를 엽니다.
2. **편집**을 클릭합니다. **새 서버 속성 편집** 페이지가 나타납니다.

   서버 속성(/en-us/xenmobile/server/media/settings-server-server-properties-edit.png)
3. 다음 정보를 적절하게 변경합니다.

   - 키: 이 필드는 변경할 수 없습니다.
   - 값: 속성 값입니다.
   - 표시 이름: 속성 이름입니다.
   - 설명: 속성 설명입니다.
4. 변경 내용을 저장하려면 **저장**을 클릭하고, 속성을 변경하지 않으려면 **취소**를 클릭합니다.

서버 속성을 삭제하려면

1. **서버 속성** 테이블에서 삭제할 서버 속성을 선택합니다.

   각 속성 옆의 확인란을 선택하여 두 개 이상의 속성을 삭제할 수 있습니다.

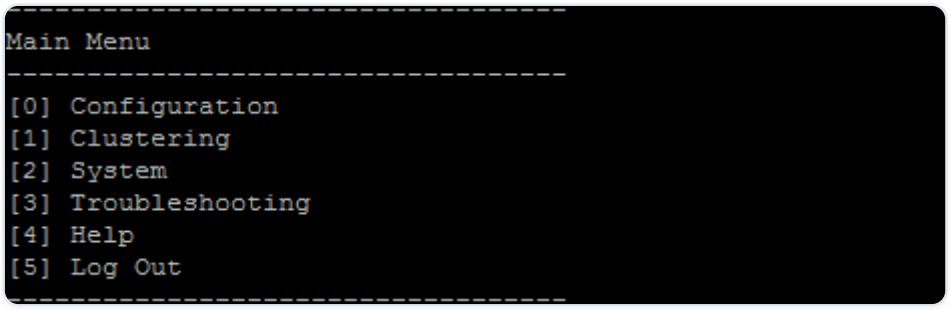
2. **삭제**를 클릭합니다. 확인 대화 상자가 나타납니다. **삭제**를 다시 클릭합니다.

명령줄 인터페이스 옵션

XenMobile® Server 온프레미스 설치의 경우 다음과 같이 CLI 옵션에 액세스할 수 있습니다.

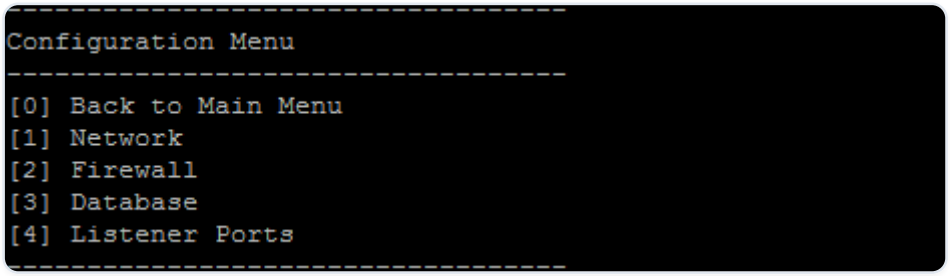
- **XenMobile을 설치한 하이퍼바이저에서:** 하이퍼바이저에서 가져온 XenMobile 가상 머신을 선택하고 명령 프롬프트 보기를 시작한 다음 XenMobile 관리자 계정에 로그온합니다. 자세한 내용은 하이퍼바이저 설명서를 참조하십시오.
- **방화벽에서 SSH가 활성화된 경우 SSH를 사용하여:** XenMobile 관리자 계정에 로그온합니다.

CLI를 사용하여 다양한 구성 및 문제 해결 작업을 수행할 수 있습니다. 다음 그림은 CLI의 최상위 메뉴를 보여줍니다.



구성 옵션

다음은 **구성 메뉴**의 샘플과 각 옵션에 표시되는 설정입니다.



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]:
```

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...
```

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]:
```

리스너 포트

명령줄 옵션(/en-us/xenmobile/server/media/cli-configuration-listener-ports.png)

클러스터링 옵션

다음은 **클러스터링 메뉴**의 샘플과 각 옵션에 표시되는 설정입니다.

명령줄 옵션(/en-us/xenmobile/server/media/cli-clustering-menu.png)

클러스터 상태 표시

명령줄 옵션(/en-us/xenmobile/server/media/cli-clustering-show-status.png)

클러스터 사용/사용 안 함

클러스터링을 사용하도록 설정하면 다음 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 설정하면 다음 메시지가 나타납니다:

`You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.`.

클러스터 멤버 화이트리스트

명령줄 옵션(/en-us/xenmobile/server/media/cli-clustering-member-white-list.png)

SSL 오프로드 사용 또는 사용 안 함

SSL 오프로드를 활성화하거나 비활성화하도록 선택하면 다음 메시지가 나타납니다.

`Enabling SSL offload opens port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.`.

Hazelcast 클러스터 표시

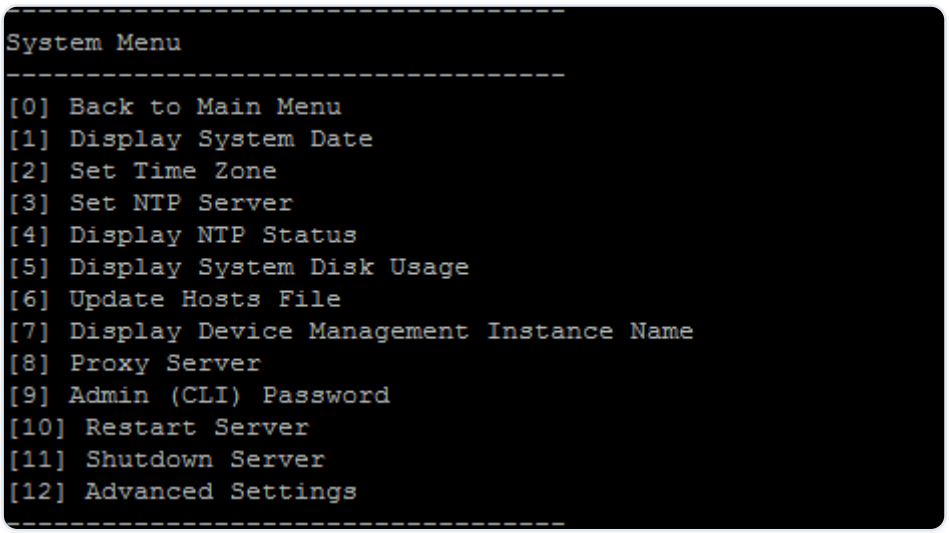
Hazelcast 클러스터를 표시하도록 선택하면 다음 옵션이 나타납니다.

Hazelcast 클러스터 멤버:

> **참고:**
>
> 구성된 노드가 클러스터의 일부가 아닌 경우 해당 노드를 다시 시작하십시오.

시스템 옵션

시스템 메뉴에서 시스템 수준 정보를 표시하거나 설정하고, 서버를 다시 시작하거나 종료하거나, **고급 설정**에 액세스할 수 있습니다.



NTP 서버 설정은 NTP 서버 정보를 지정할 수 있도록 합니다. XenMobile 시간을 하이퍼바이저와 동기화할 때 시간대 문제가 발생하는 경우, XenMobile을 NTP 서버로 지정하여 문제를 피할 수 있습니다. 이 옵션을 변경한 후 모든 클러스터 서버를 다시 시작하십시오.

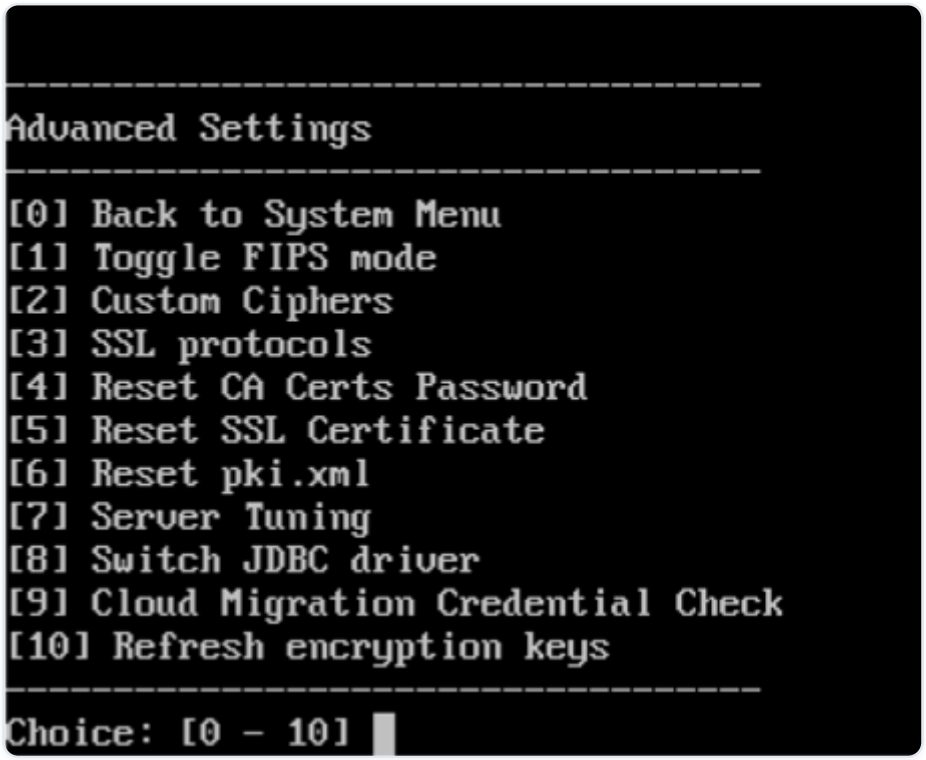
시스템 디스크 사용량 표시 메뉴 항목을 통해 디스크 공간을 확인할 수도 있습니다.

서버 노드 종료 정보

클러스터에서 단일 서버 노드를 종료하면, 다른 노드들은 일반적으로 확장성 및 성능에 설명된 요구 사항을 충족하는 경우 워크로드를 처리할 수 있습니다. 영향은 동시에 다운되는 노드 수, 총 사용자 수, 노드가 다운되는 기간에 따라 달라질 수 있습니다.

- 사용자는 Secure Hub 및 스토어에 계속 액세스할 수 있습니다.
- 사용 가능한 노드가 사용자 수를 처리할 수 있는 경우, 사용자는 배포된 관리 앱에 계속 액세스하고 실행할 수 있습니다. 연결 속도가 느려져 장치 체크인 속도가 느려질 수 있습니다.
- 모든 노드가 다운되지 않는 한 장치 정책은 계속 작동합니다. 리소스 및 장치 수에 따라 정책 배포가 더 느려질 수 있습니다.

고급 설정



SSL 프로토콜 옵션은 기본적으로 허용되는 모든 프로토콜로 설정됩니다. **활성화할 새 SSL 프로토콜** 프롬프트가 나타나면 활성화할 프로토콜을 입력합니다. XenMobile은 응답에 포함되지 않은 모든 프로토콜을 비활성화합니다. 예를 들어, TLSv1을 비활성화하려면 `TLSv1.2,TLSv1.1` 을 입력한 다음 **y**를 입력하여 XenMobile Server를 다시 시작합니다.

서버 튜닝 옵션에는 서버 연결 시간 초과, 최대 연결 수(포트별) 및 최대 스레드 수(포트별)가 포함됩니다.

JDBC 드라이버 전환 옵션은 **jTDS** 및 **Microsoft** JDBC입니다. 기본 드라이버는 jTDS입니다. Microsoft JDBC 드라이버로 전환하는 방법에 대한 자세한 내용은 SQL Server 드라이버를 참조하십시오.

문제 해결 옵션

다음은 **문제 해결 메뉴** 및 각 옵션에 대해 표시되는 설정의 예시입니다.

```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

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
-----------------------------------
```

로그

```
-----------------------------------
Logs Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Display debug log file
[2] Display update log file
```

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
-----------------------------------
```

디스크 사용량

```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

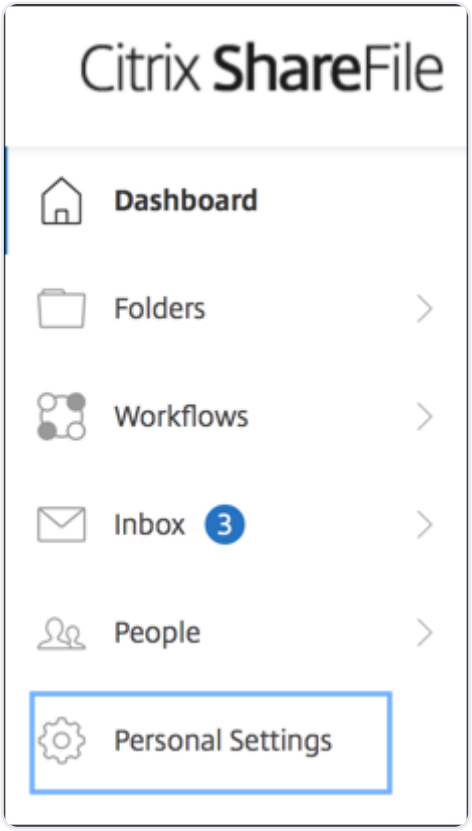
Citrix Files를 FTP 사이트로 사용하여 지원 번들을 업로드하려면

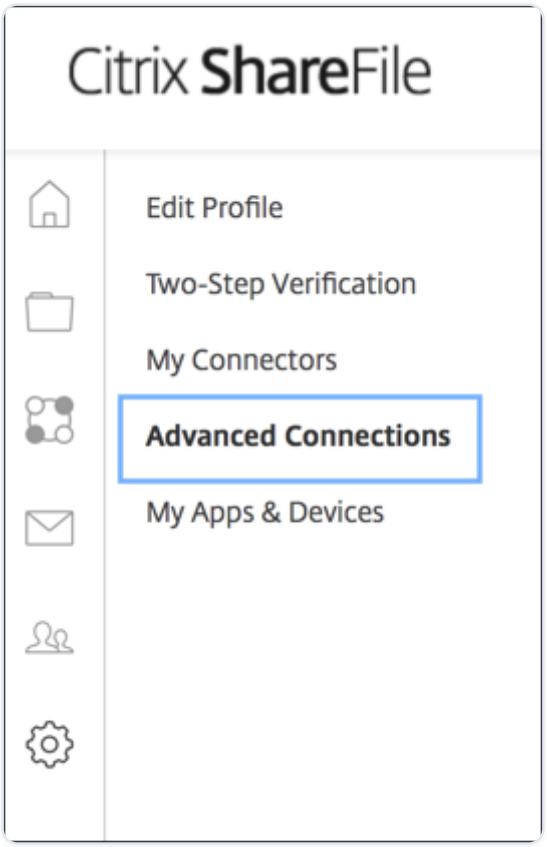
지원 번들 업로드를 시작하기 전에 Citrix Files에서 다음 필수 구성 요소를 구성하십시오.

1. FTP 로그온 세부 정보를 확인합니다.

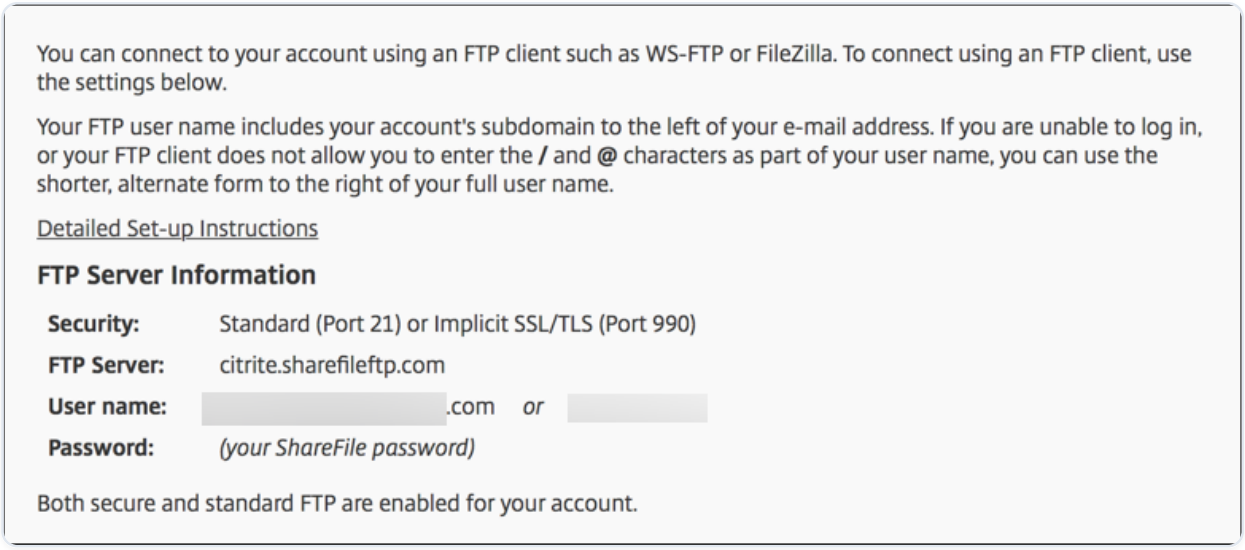
   a. 웹 브라우저에서 `<https://citrix.sharefile.com>`을(를) 엽니다.

   b. **개인 설정**을 클릭한 다음 **고급 연결**을 클릭합니다.





c. FTP 서버 정보에서 사용자 이름에 기본 하위 도메인/사용자 이름 세부 정보와 함께 영숫자 사용자 ID가 나타나는지 확인합니다.



참고:

- XenMobile에서 업로드하는 파일은 Linux CLI 기반 FTP 클라이언트입니다. 따라서 사용자 이름의 일부로 백슬래시(\) 및 앳 사인(@) 문자를 입력할 수 없습니다.

- 영숫자 사용자 ID가 보이지 않으면 ShareFile 관리자 또는 ShareFile 지원팀에 이 사용자 ID를 요청할 수 있습니다.

2. Citrix Files 서버가 FTPS와 함께 FTP 통신에 대해 활성화되어 있는지 확인하십시오. 이상적으로는 ShareFile 관리자가 사용자 계정을 FTP 통신에 사용할 수 있도록 허용합니다. 하지만 때로는 FTPS 통신만 허용되는 경우도 있습니다.

   관리자 권한이 있는 사용자는 **설정** > **관리자 설정** > **고급 기본 설정** > **ShareFile 도구 활성화**를 클릭하여 이 설정을 확인하고 활성화할 수 있습니다. **외부 앱** > **FTP 액세스**에서 **활성화** 확인란이 선택되어 있는지 확인하십시오.

   Citrix Files 활성화 확인란(/en-us/xenmobile/server/media/sharefile-externaltools-ftp.png)

3. FTP 클라이언트가 파일 업로드 디렉터리로 사용할 공유 폴더를 만드십시오. **홈**을 클릭하고 **폴더**를 클릭한 다음 **개인 폴더**를 클릭하십시오.
4. 맨 오른쪽에서 더하기 기호(+) 아이콘을 클릭하고 **폴더 만들기**를 클릭한 다음 폴더 이름을 입력하십시오.

   Citrix Files 공유 폴더 대화 상자(/en-us/xenmobile/server/media/sharefile-create-sharedfolder.png)

5. XenMobile Server CLI의 **주 메뉴**에서 **문제 해결 > 지원 번들**을 선택하십시오. 그런 다음 **지원 번들 메뉴**에서 **지원 번들 생성**을 선택하십시오.

   명령줄 옵션(/en-us/xenmobile/server/media/sharefile-ftp-cli-options.png)

   참고:

   지원 번들이 이미 있는 경우, 메시지가 표시되면 **y**를 입력하여 번들을 덮어쓰십시오.

6. 지원 번들을 FTP 서버에 업로드하십시오.

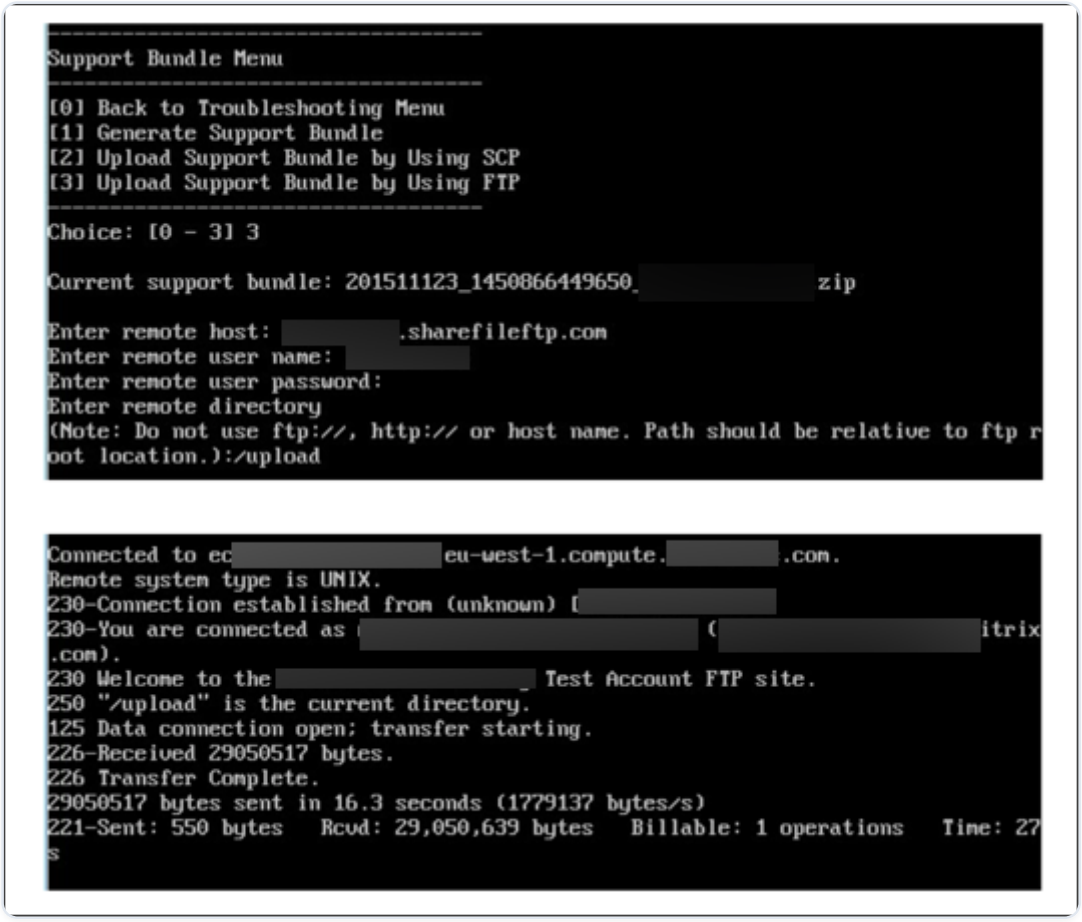
   a. **FTP를 사용하여 지원 번들 업로드**를 선택하십시오.

   b. **원격 호스트 입력:** 메시지가 표시되면 FTP 서버 이름을 입력하십시오. Citrix Files가 FTP 서버로 사용되는 경우, 회사 이름 뒤에 Citrix Files FTP 사이트 이름을 입력하십시오. 예를 들어, citrix.sharefileftp.com입니다.

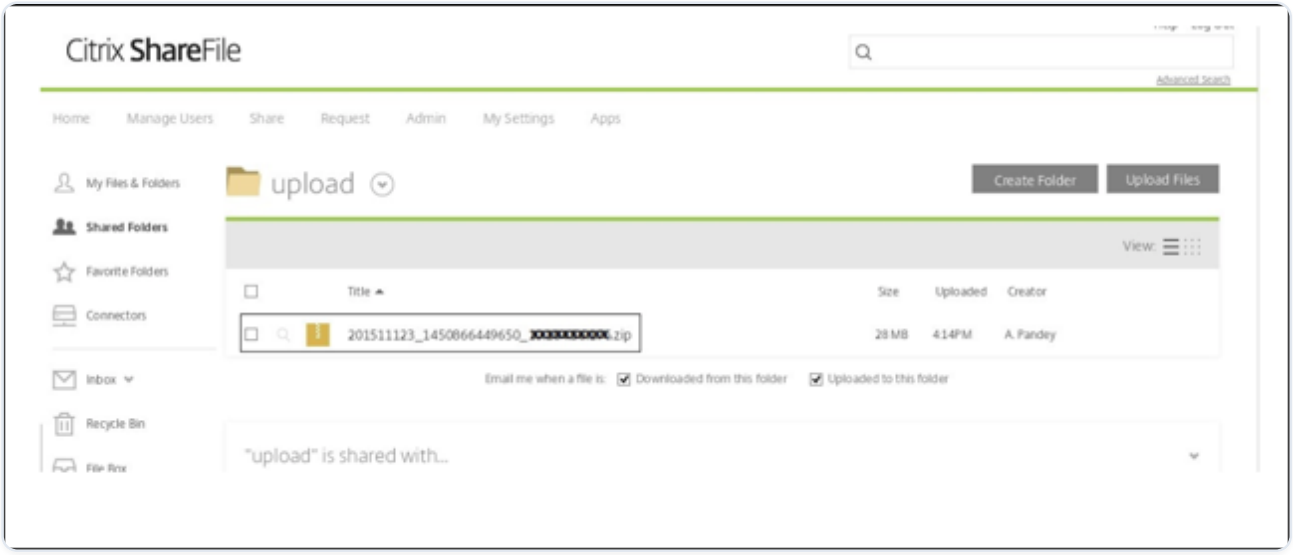
   c. **원격 사용자 이름 입력:** 메시지가 표시되면 영숫자 사용자 ID를 입력하십시오.

   d. **원격 사용자 암호 입력:** 프롬프트가 표시되면 암호를 입력합니다.

e. **원격 디렉터리 입력:** 프롬프트가 표시되면 Citrix Files에서 생성한 공유 폴더 이름을 입력한 다음 **Enter** 키를 누릅니다.



Citrix Files에서 생성한 공유 폴더에서 업로드된 지원 번들을 볼 수 있습니다.



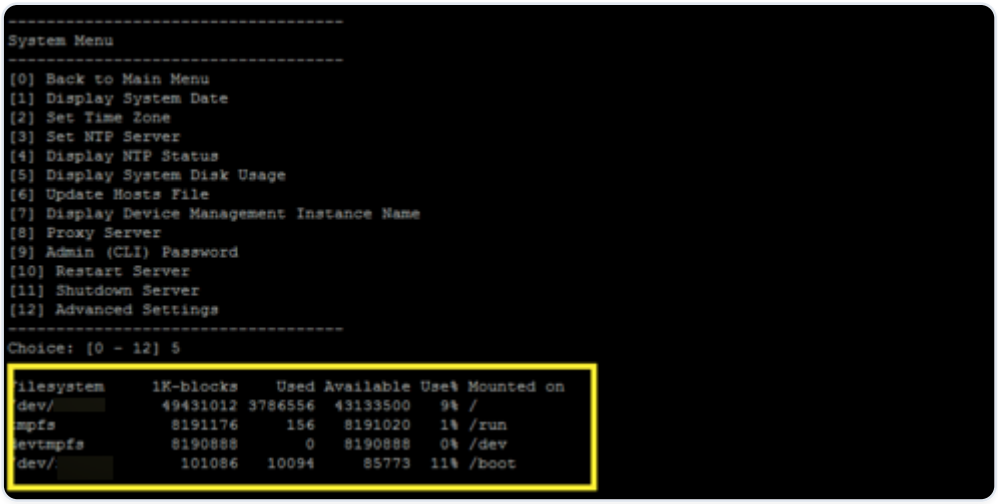
Citrix Files FTP에 대한 자세한 내용은 다음 Citrix 지원 기술 자료 문서를 참조하십시오.

디스크 공간 확인

CLI에서 시스템 디스크 공간을 다음과 같이 확인할 수 있습니다.

1. 기본 메뉴에서 **시스템** 메뉴를 선택합니다.
2. **시스템** 메뉴에서 **시스템 디스크 사용량 표시** 옵션을 선택합니다.

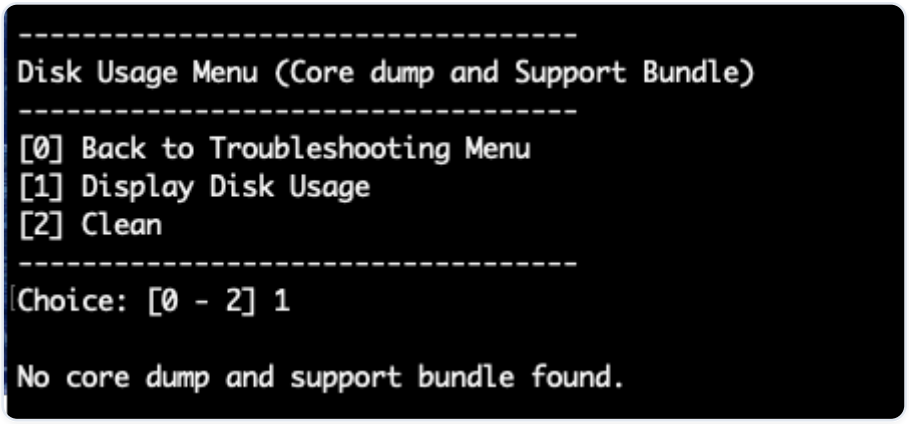
   파일 시스템 정보가 나타납니다.



셀프 서비스 디스크 정리 수행

CLI에서 디스크를 다음과 같이 정리할 수 있습니다.

1. **문제 해결** 메뉴에서 **디스크 사용량**을 선택합니다. **디스크 사용량** 목록에는 다음 옵션이 있습니다:



2. 코어 덤프 파일 및 지원 번들 파일 유형을 나열하려면 1을 입력합니다. 파일이 없으면 다음 메시지가 표시됩니다: **코어 덤프 및 지원 번들을 찾을 수 없습니다.**
3. 검색된 코어 덤프 파일 및 지원 번들 파일을 정리하려면 2를 입력합니다.

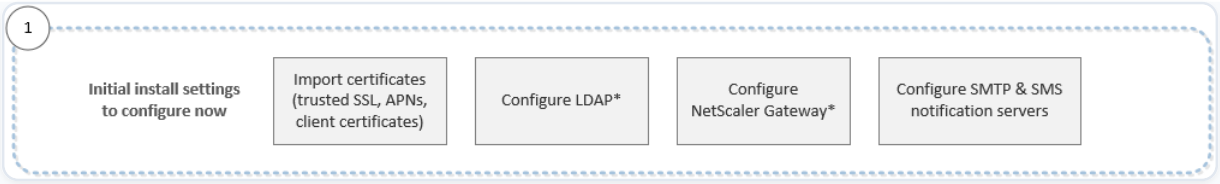
XenMobile® 콘솔 시작 워크플로

XenMobile 콘솔은 XenMobile의 통합 관리 도구입니다. 이 문서는 XenMobile을 설치했고 콘솔에서 작업할 준비가 되었다고 가정합니다. XenMobile을 아직 설치하지 않았다면 XenMobile 설치를 참조하십시오. XenMobile 콘솔의 브라우저 지원에 대한 자세한 내용은 XenMobile 호환성 문서를 참조하십시오.

초기 설정 워크플로

명령줄 콘솔에서 XenMobile을 먼저 구성하고 XenMobile 콘솔에서 다음으로 구성한 후 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 이러한 설치 설정을 완료하는 것을 고려하십시오. 시작하려면 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭하십시오.

> **참고:**
>
> 별표가 있는 항목은 선택 사항입니다.



각 설정에 대한 자세한 정보와 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

- 인증
- 시트릭스 게이트웨이 및 젠모바일
- 알림

Android, iOS 및 Windows 플랫폼을 지원하려면 다음 계정 관련 설정이 필요합니다.

안드로이드

- Google Play 자격 증명을 생성합니다. 자세한 내용은 Google Play 시작을 참조하십시오.
- Android Enterprise 관리자 계정을 생성합니다. 자세한 내용은 Android Enterprise를 참조하십시오.
- Google로 도메인 이름을 확인합니다. 자세한 내용은 Google Workspace용 도메인 확인을 참조하십시오.
- API를 활성화하고 Android Enterprise용 서비스 계정을 생성합니다. 자세한 내용은 Android Enterprise 도움말을 참조하십시오.

iOS

- Apple ID 및 개발자 계정을 생성합니다. 자세한 내용은 Apple 개발자 프로그램 웹사이트를 참조하십시오.
- Apple 푸시 알림 서비스(APNs) 인증서를 생성합니다. XenMobile Server 배포로 iOS 장치를 관리할 계획이라면 Apple APNs 인증서가 필요합니다. Secure Mail 배포에 푸시 알림을 사용하는 경우에도 Apple APNs 인증서가 필요합니다. Apple APNs 인증서 획득에 대한 자세한 내용은 Apple 푸시 인증서

포털을 참조하십시오. XenMobile 및 APNs에 대한 자세한 내용은 APNs 인증서 및 iOS용 Secure Mail 푸시 알림을 참조하십시오.

- 볼륨 구매 회사 토큰을 생성합니다. 자세한 내용은 Apple 볼륨 구매 프로그램을 참조하십시오.

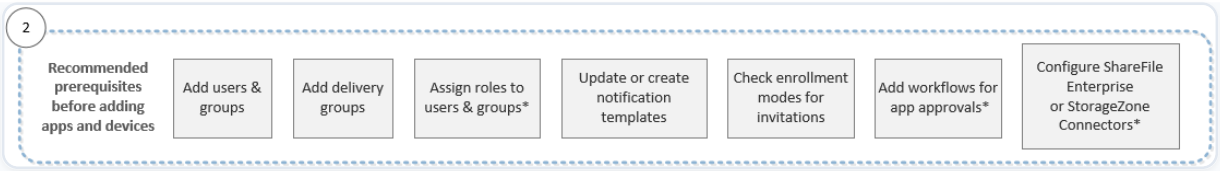
윈도우

- Microsoft Windows 스토어 개발자 계정을 생성합니다. 자세한 내용은 계정 유형, 위치 및 수수료를 참조하십시오.
- Microsoft Windows 스토어 게시자 ID를 가져옵니다. 자세한 내용은 계정 설정 및 프로필 정보 관리를 참조하십시오.
- Windows 장치 등록에 XenMobile AutoDiscovery를 사용할 계획이라면 공개 SSL 인증서가 있는지 확인하십시오. 자세한 내용은 XenMobile AutoDiscovery 서비스를 참조하십시오.

콘솔 필수 구성 요소 워크플로

이 워크플로는 앱 및 장치를 추가하기 전에 구성해야 할 필수 구성 요소를 보여줍니다.

> **참고:**
>
> 별표가 있는 항목은 선택 사항입니다.



각 설정에 대한 자세한 정보와 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

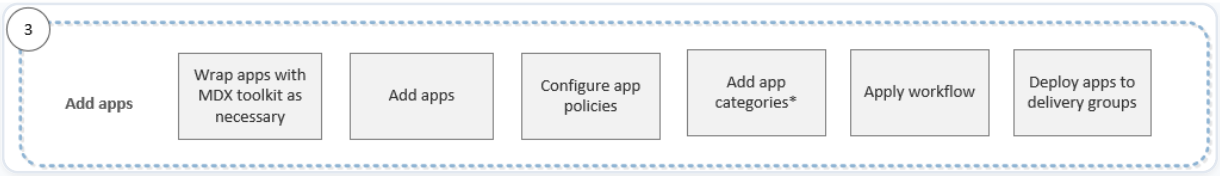
- 사용자 계정, 역할 및 등록
- 리소스 배포
- RBAC를 사용하여 역할 구성
- 알림
- 워크플로 적용
- XenMobile에서 ShareFile 사용

앱 추가 워크플로

이 워크플로는 XenMobile에 앱을 추가할 때 권장되는 순서를 보여줍니다.

참고:

별표가 있는 항목은 선택 사항입니다.



각 설정에 대한 자세한 정보와 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

- MDX Toolkit 정보
- 앱 추가
- 한눈에 보는 MDX 정책
- 워크플로 적용
- 리소스 배포

장치 추가 워크플로

이 워크플로는 XenMobile에 장치를 추가하고 등록할 때 권장되는 순서를 보여줍니다.

참고:

별표가 있는 항목은 선택 사항입니다.



각 설정에 대한 자세한 정보와 단계별 절차는 다음 Citrix 제품 설명서 문서 및 섹션을 참조하십시오.

- 장치
- 지원되는 장치 운영 체제
- 리소스 배포
- 모니터링 및 지원
- 자동화된 작업

사용자 장치 등록 워크플로

이 워크플로는 XenMobile에 사용자 장치를 등록할 때 따라야 할 권장 순서를 보여줍니다.

시작 워크플로 이미지(/en-us/xenmobile/server/media/console-workflow-5.png)

각 설정에 대한 자세한 내용과 단계별 절차는 다음 Citrix 제품 설명서 문서를 참조하십시오.

- 사용자 계정, 역할 및 등록
- 알림

지속적인 앱 및 장치 관리 워크플로

이 워크플로는 콘솔에서 수행할 수 있는 앱 및 장치 관리 활동을 보여줍니다.

> **참고:**

> 별표가 있는 항목은 선택 사항입니다.

> 시작 워크플로 이미지(/en-us/xenmobile/server/media/console-workflow-6.png)

콘솔의 오른쪽 상단 모서리에 있는 렌치 아이콘을 클릭하면 찾을 수 있는 지원 옵션에 대한 자세한 내용은 모니터링 및 지원을 참조하십시오.

인증서 및 인증

XenMobile® 작업 중 인증에는 여러 구성 요소가 사용됩니다.

- **XenMobile Server:** XenMobile Server는 등록 보안 및 등록 환경을 정의하는 곳입니다. 사용자 온보딩 옵션은 다음과 같습니다.
  - 모든 사용자에게 등록을 개방할지 또는 초대 전용으로 할지 여부.
  - 2단계 인증 또는 3단계 인증을 요구할지 여부. XenMobile의 클라이언트 속성을 통해 Citrix PIN 인증을 활성화하고 PIN의 복잡성 및 만료 시간을 구성할 수 있습니다.
- **Citrix ADC:** Citrix ADC는 마이크로 VPN SSL 세션에 대한 종료를 제공합니다. Citrix ADC는 또한 네트워크 전송 중 보안을 제공하며, 사용자가 앱에 액세스할 때마다 사용되는 인증 환경을 정의할 수 있도록 합니다.
- **Secure Hub:** Secure Hub와 XenMobile Server는 등록 작업에서 함께 작동합니다. Secure Hub는 Citrix ADC와 통신하는 장치의 엔터티입니다. 세션이 만료되면 Secure Hub는 Citrix ADC에서 인증 티켓을 가져와 MDX 앱에 전달합니다. Citrix는 중간자 공격을 방지하는 인증서 고정을 권장합니다. 자세한 내용은 Secure Hub 문서의 다음 섹션을 참조하십시오. 인증서 고정.

  Secure Hub는 또한 MDX 보안 컨테이너를 용이하게 합니다. Secure Hub는 정책을 푸시하고, 앱 시간이 초과되면 Citrix ADC와 세션을 생성하며, MDX 시간 초과 및 인증 환경을 정의합니다. Secure Hub는 또한 탈옥 감지, 지리적 위치 확인 및 적용하는 모든 정책을 담당합니다.
- **MDX 정책:** MDX 정책은 장치에 데이터 볼트를 생성합니다. MDX 정책은 마이크로 VPN 연결을 Citrix ADC로 다시 연결하고, 오프라인 모드 제한을 적용하며, 시간 초과와 같은 클라이언트 정책을 적용합니다.

단일 요소 및 2단계 인증 방법을 포함한 인증 구성에 대한 자세한 내용은 배포 핸드북 문서 인증을 참조하십시오.

XenMobile에서 인증서를 사용하여 보안 연결을 생성하고 사용자를 인증합니다. 이 문서의 나머지 부분에서는 인증서에 대해 설명합니다. 다른 구성 세부 정보는 다음 문서를 참조하십시오.

- 도메인 또는 도메인 및 보안 토큰 인증
- 클라이언트 인증서 또는 인증서 및 도메인 인증
- PKI 엔터티

- 자격 증명 공급자
- APNs 인증서
- Citrix Files를 사용한 단일 Sign-On용 SAML
- 마이크로소프트 애저 액티브 디렉터리 서버 설정
- Wi-Fi 서버에 인증하기 위해 장치에 인증서를 보내려면: Wi-Fi 장치 정책
- 인증에 사용되지 않는 고유 인증서(예: 내부 루트 CA(인증 기관) 인증서) 또는 특정 정책을 푸시하려면: 자격 증명 장치 정책

인증서

XenMobile은 설치 중에 서버로의 통신 흐름을 보호하기 위해 자체 서명된 SSL(Secure Sockets Layer) 인증서를 생성합니다. SSL 인증서를 잘 알려진 CA의 신뢰할 수 있는 SSL 인증서로 교체해야 합니다.

XenMobile은 자체 PKI(공개 키 인프라) 서비스를 사용하거나 클라이언트 인증서용 CA에서 인증서를 가져오기도 합니다. 모든 Citrix 제품은 와일드카드 및 SAN(주체 대체 이름) 인증서를 지원합니다. 대부분의 배포에서는 두 개의 와일드카드 또는 SAN 인증서만 필요합니다.

클라이언트 인증서 인증은 모바일 앱에 추가 보안 계층을 제공하고 사용자가 HDX™ 앱에 원활하게 액세스할 수 있도록 합니다. 클라이언트 인증서 인증이 구성되면 사용자는 XenMobile 지원 앱에 대한 SSO(단일 Sign-On) 액세스를 위해 Citrix PIN을 입력합니다. Citrix PIN은 사용자 인증 환경도 간소화합니다. Citrix PIN은 클라이언트 인증서를 보호하거나 Active Directory 자격 증명을 장치에 로컬로 저장하는 데 사용됩니다.

XenMobile으로 iOS 장치를 등록하고 관리하려면 Apple에서 APNs(Apple Push Notification Service) 인증서를 설정하고 생성합니다. 단계는 APNs 인증서를 참조하십시오.

다음 표는 각 XenMobile 구성 요소에 대한 인증서 형식 및 유형을 보여줍니다.

XENMOBILE 구성 요소	인증서 형식	필수 인증서 유형
시트릭스 게이트웨이	PEM (BASE64), PFX (PKCS #12)	SSL, 루트 (Citrix Gateway는 PFX를 PEM으로 자동 변환합니다.)
XenMobile 서버	.p12 (Windows 기반 컴퓨터에서는 .pfx)	SSL, SAML, APNs (XenMobile은 설치 프로세스 중에 전체 PKI를 생성합니다.) 중요: XenMobile Server는 .pem 확장자를 가진 인증서를 지원하지 않습니다. .pem 인증서를 사

XENMOBILE 구성 요소	인증서 형식	필수 인증서 유형
		용하려면 .pem 파일을 인증서와 키로 분할한 다음 각각을 XenMobile Server로 가져와야 합니다.
StoreFront™	PFX (PKCS #12)	SSL, 루트

XenMobile은 4096, 2048, 1024비트 길이의 SSL 수신기 인증서 및 클라이언트 인증서를 지원합니다. 1024비트 인증서는 쉽게 손상될 수 있습니다.

Citrix Gateway 및 XenMobile Server의 경우 Citrix는 Verisign, DigiCert 또는 Thawte와 같은 공용 CA에서 서버 인증서를 얻을 것을 권장합니다. Citrix Gateway 또는 XenMobile 구성 유틸리티에서 CSR(인증서 서명 요청)을 생성할 수 있습니다. CSR을 생성한 후 서명을 위해 CA에 제출합니다. CA가 서명된 인증서를 반환하면 Citrix Gateway 또는 XenMobile에 인증서를 설치할 수 있습니다.

> **중요: iOS, iPadOS 및 macOS에서 신뢰할 수 있는 인증서에 대한 요구 사항**

> Apple은 TLS 서버 인증서에 대한 새로운 요구 사항을 발표했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는지 확인하십시오. Apple 발행물 `<https://support.apple.com/ko-kr/HT210176>`을 참조하십시오.

> Apple은 TLS 서버 인증서의 최대 허용 수명을 단축하고 있습니다. 이 변경 사항은 2020년 9월 이후에 발급된 서버 인증서에만 영향을 미칩니다. Apple 발행물 `<https://support.apple.com/ko-kr/HT211025>`을 참조하십시오.

XenMobile에서 인증서 업로드

업로드하는 각 인증서는 내용 요약을 포함하여 인증서 테이블에 항목으로 표시됩니다. 인증서가 필요한 PKI 통합 구성 요소를 구성할 때 상황에 따라 달라지는 기준을 충족하는 서버 인증서를 선택합니다. 예를 들어, Microsoft 인증 기관(CA)과 통합하도록 XenMobile을 구성할 수 있습니다. Microsoft CA에 대한 연결은 클라이언트 인증서를 사용하여 인증되어야 합니다.

이 섹션에서는 인증서 업로드에 대한 일반적인 절차를 제공합니다. 클라이언트 인증서 생성, 업로드 및 구성에 대한 자세한 내용은 클라이언트 인증서 또는 인증서와 도메인 인증을 참조하십시오.

개인 키 요구 사항

XenMobile은 특정 인증서에 대한 개인 키를 소유할 수도 있고 소유하지 않을 수도 있습니다. 마찬가지로, XenMobile은 업로드된 인증서에 개인 키를 요구할 수도 있고 요구하지 않을 수도 있습니다.

인증서 업로드

인증서를 업로드하는 방법에는 두 가지가 있습니다.

- 인증서를 콘솔에 개별적으로 업로드합니다.
- REST API를 사용하여 iOS 장치에 인증서를 대량으로 업로드합니다.

콘솔에 인증서를 업로드할 때 두 가지 주요 옵션이 있습니다.

- 키 저장소를 가져오려면 클릭합니다. PKCS #12 형식을 업로드하는 경우가 아니라면, 설치하려는 키 저장소 리포지토리의 항목을 식별합니다.
- 인증서를 가져오려면 클릭합니다.

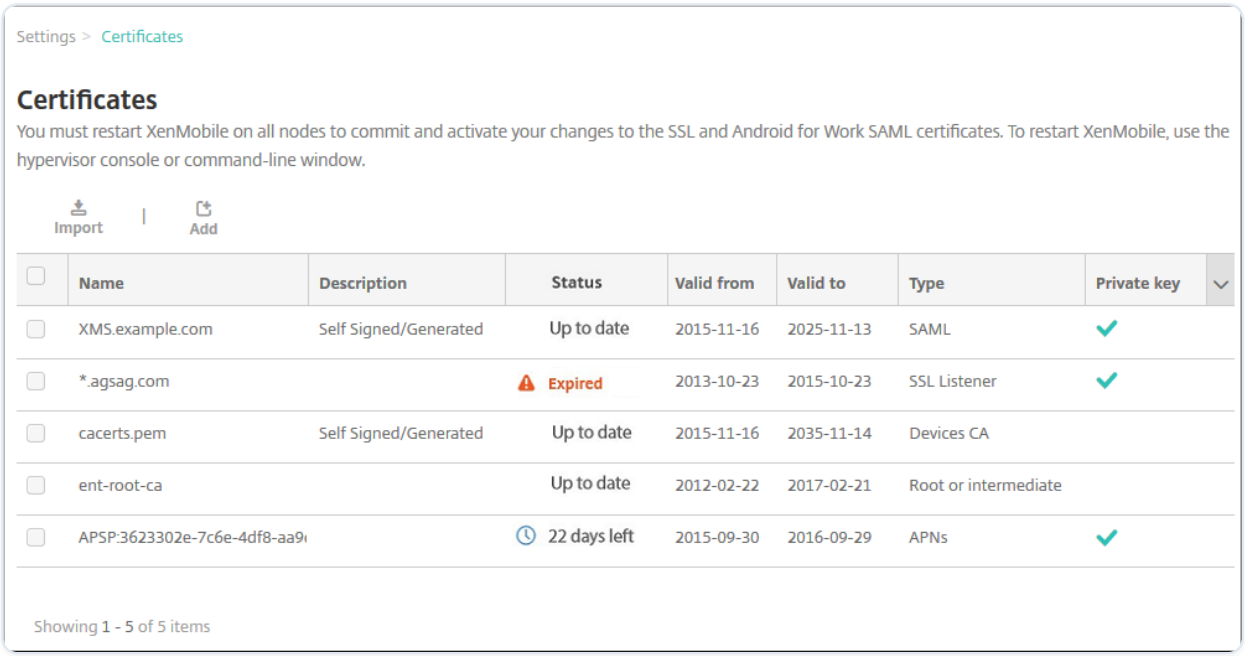
CA가 요청에 서명하는 데 사용하는 CA 인증서(개인 키 없음)를 업로드할 수 있습니다. 클라이언트 인증을 위해 SSL 클라이언트 인증서(개인 키 포함)를 업로드할 수도 있습니다.

Microsoft CA 엔터티를 구성할 때 CA 인증서를 지정합니다. CA 인증서인 모든 서버 인증서 목록에서 CA 인증서를 선택합니다. 마찬가지로, 클라이언트 인증을 구성할 때 XenMobile이 개인 키를 가지고 있는 모든 서버 인증서 목록에서 선택할 수 있습니다.

키 저장소를 가져오려면

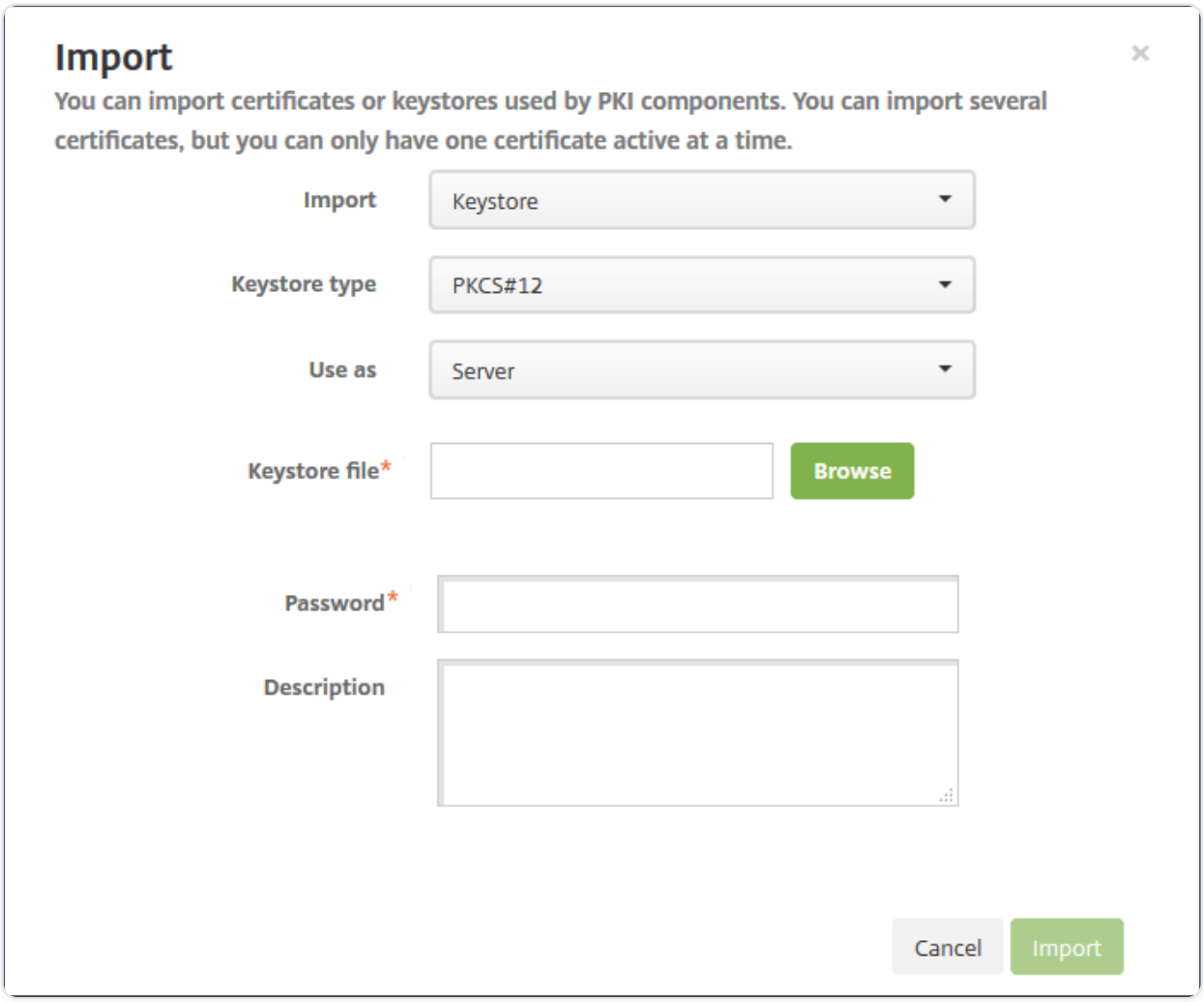
보안 인증서 리포지토리인 키 저장소는 설계상 여러 항목을 포함할 수 있습니다. 따라서 키 저장소에서 로드할 때 로드하려는 항목을 식별하는 항목 별칭을 지정하라는 메시지가 표시됩니다. 별칭을 지정하지 않으면 저장소의 첫 번째 항목이 로드됩니다. PKCS #12 파일은 일반적으로 하나의 항목만 포함하므로 키 저장소 유형으로 PKCS #12를 선택하면 별칭 필드가 나타나지 않습니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **인증서**를 클릭합니다. **인증서** 페이지가 나타납니다.



3. **가져오기**를 클릭합니다. **가져오기** 대화 상자가 나타납니다.
4. 다음 설정을 구성합니다:

   - **가져오기:** 목록에서 **키 저장소**를 클릭합니다. **가져오기** 대화 상자가 사용 가능한 키 저장소 옵션을 반영하도록 변경됩니다.



- **키 저장소 유형:** 목록에서 **PKCS #12**를 클릭합니다.
- **용도:** 목록에서 인증서를 사용할 방법을 클릭합니다. 사용 가능한 옵션은 다음과 같습니다:
  - **서버**. 서버 인증서는 XenMobile Server에서 기능적으로 사용되며 XenMobile 웹 콘솔에 업로드되는 인증서입니다. 여기에는 CA 인증서, RA 인증서 및 인프라의 다른 구성 요소와 클라이언트 인증을 위한 인증서가 포함됩니다. 또한 서버 인증서를 장치에 배포하려는 인증서의 저장소로 사용할 수 있습니다. 이 용도는 특히 장치에서 신뢰를 설정하는 데 사용되는 CA에 적용됩니다.
  - **SAML**. SAML(Security Assertion Markup Language) 인증을 통해 서버, 웹 사이트 및 앱에 SSO 액세스를 제공할 수 있습니다.
  - **APNs**. Apple의 APNs 인증서는 Apple 푸시 네트워크를 통해 모바일 장치 관리를 가능하게 합니다.
  - **SSL 수신기**. SSL(Secure Sockets Layer) 수신기는 SSL 암호화 활동을 XenMobile에 알립니다.
- **키 저장소 파일:** .p12 파일 형식(Windows 기반 컴퓨터에서는 .pfx)으로 가져올 키 저장소를 찾습니다.
- **암호:** 인증서에 할당된 암호를 입력합니다.

- **설명:** 선택적으로 키 저장소를 다른 키 저장소와 구별하는 데 도움이 되도록 설명을 입력합니다.

5. **가져오기**를 클릭합니다. 키 저장소가 인증서 테이블에 추가됩니다.

인증서 가져오기

파일 또는 키 저장소 항목에서 인증서를 가져올 때 XenMobile은 입력에서 인증서 체인을 구성하려고 시도합니다. XenMobile은 해당 체인의 모든 인증서를 가져와 각각에 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 발급자인 경우입니다.

가져온 인증서에 대한 선택적 설명을 추가할 수 있습니다. 설명은 체인의 첫 번째 인증서에만 첨부됩니다. 나머지 인증서의 설명은 나중에 업데이트할 수 있습니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭한 다음 **인증서**를 클릭합니다.
2. **인증서** 페이지에서 **가져오기**를 클릭합니다. **가져오기** 대화 상자가 나타납니다.
3. **가져오기** 대화 상자의 **가져오기**에서 아직 선택되지 않은 경우 **인증서**를 클릭합니다.
4. **가져오기** 대화 상자가 사용 가능한 인증서 옵션을 반영하도록 변경됩니다. **용도**에서 키 저장소를 어떻게 사용할지 선택합니다. 사용 가능한 옵션은 다음과 같습니다.

    - **서버**. 서버 인증서는 XenMobile 웹 콘솔에 업로드되는 XenMobile Server에서 기능적으로 사용되는 인증서입니다. 여기에는 CA 인증서, RA 인증서, 인프라의 다른 구성 요소와 클라이언트 인증을 위한 인증서가 포함됩니다. 또한 서버 인증서를 장치에 배포하려는 인증서의 저장소로 사용할 수 있습니다. 이 옵션은 특히 장치에서 신뢰를 설정하는 데 사용되는 CA에 적용됩니다.
    - **SAML**. SAML(Security Assertion Markup Language) 인증을 통해 서버, 웹 사이트 및 앱에 대한 SSO(Single Sign-On) 액세스를 제공할 수 있습니다.
    - **SSL 수신기**. SSL(Secure Sockets Layer) 수신기는 SSL 암호화 활동을 XenMobile에 알립니다.

5. 가져올 키 저장소(.p12 파일 형식, Windows 기반 컴퓨터에서는 .pfx)를 찾으려면 찾아봅니다.
6. 인증서에 대한 선택적 개인 키 파일을 찾으려면 찾아봅니다. 개인 키는 인증서와 함께 암호화 및 암호 해독에 사용됩니다.
7. 선택적으로 인증서에 대한 설명을 입력하여 다른 인증서와 구별하는 데 도움이 되도록 합니다.
8. **가져오기**를 클릭합니다. 인증서가 인증서 테이블에 추가됩니다.

REST API를 사용하여 iOS 기기에 대량으로 인증서 업로드

인증서를 하나씩 업로드하는 것이 비실용적이라면, REST API를 사용하여 iOS 기기에 대량으로 업로드할 수 있습니다. 이 방법은 .p12 형식의 인증서를 지원합니다. REST API에 대한 자세한 내용은 REST API를 참조하십시오.

1. 각 인증서 파일의 이름을 `device_identity_value.p12` 형식으로 변경합니다. `device_identity_value`는 각 장치의 IMEI, 일련 번호 또는 MEID가 될 수 있습니다.

   예를 들어, 식별 방법으로 일련 번호를 사용한다고 가정해 봅시다. 한 장치의 일련 번호가 `A12BC3D4EFGH`이라면, 해당 장치에 설치할 인증서 파일의 이름을 `A12BC3D4EFGH.p12`로 지정합니다.

2. .p12 인증서의 암호를 저장할 텍스트 파일을 만듭니다. 해당 파일에 각 장치의 장치 식별자와 암호를 새 줄에 입력합니다. `device_identity_value=password` 형식을 사용합니다. 다음을 참조하십시오.

   ```
   A12BC3D4EFGH.p12=password1!

   A12BC3D4EFIJ.p12=password2@

   A12BC3D4EFKL.p12=password3#
   ```

3. 생성한 모든 인증서와 텍스트 파일을 .zip 파일로 압축합니다.
4. REST API 클라이언트를 실행하고 XenMobile에 로그인한 다음 인증 토큰을 가져옵니다.
5. 메시지 본문에 다음 내용을 포함하여 인증서를 가져옵니다.

   ```
   {

       "alias": "",

       "useAs": "device",

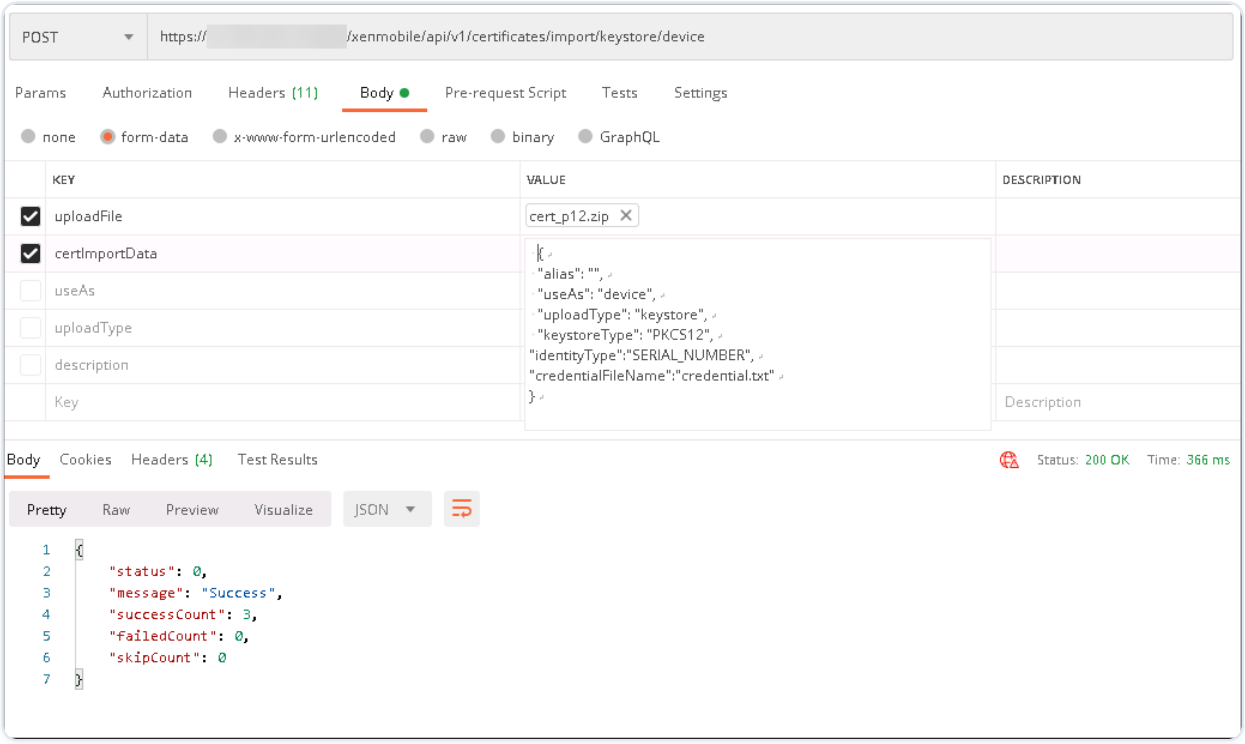
       "uploadType": "keystore",

       "keystoreType": "PKCS12",

       "identityType":"SERIAL_NUMBER",        # identity type can be
   "SERIAL_NUMBER","IMEI","MEID"

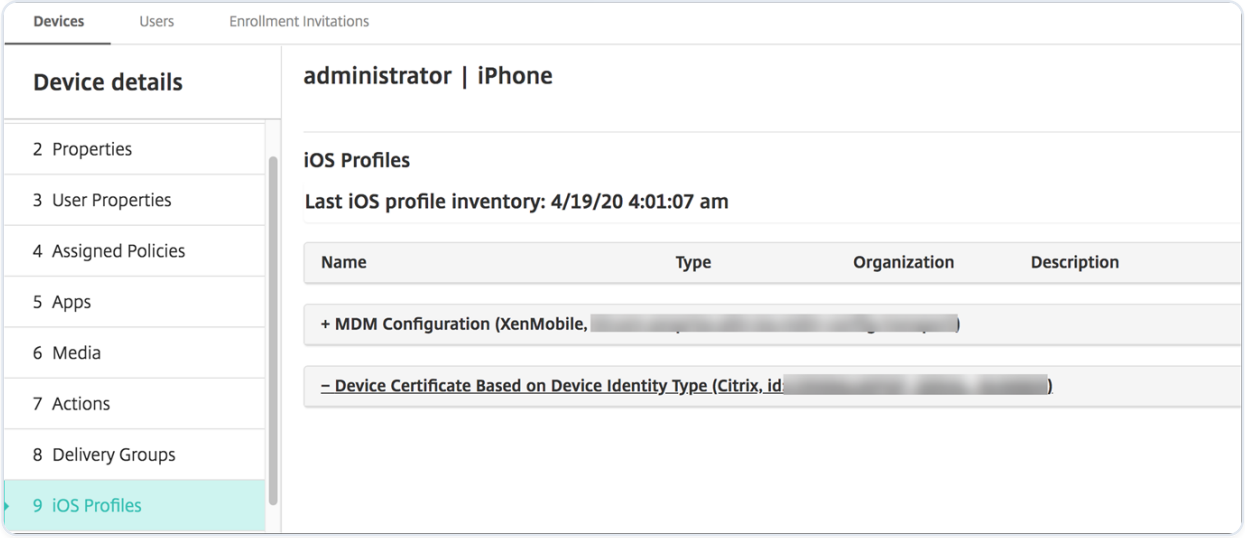
       "credentialFileName":"credential.txt"   # The credential file name
   in .zip
   ```

```
}
```



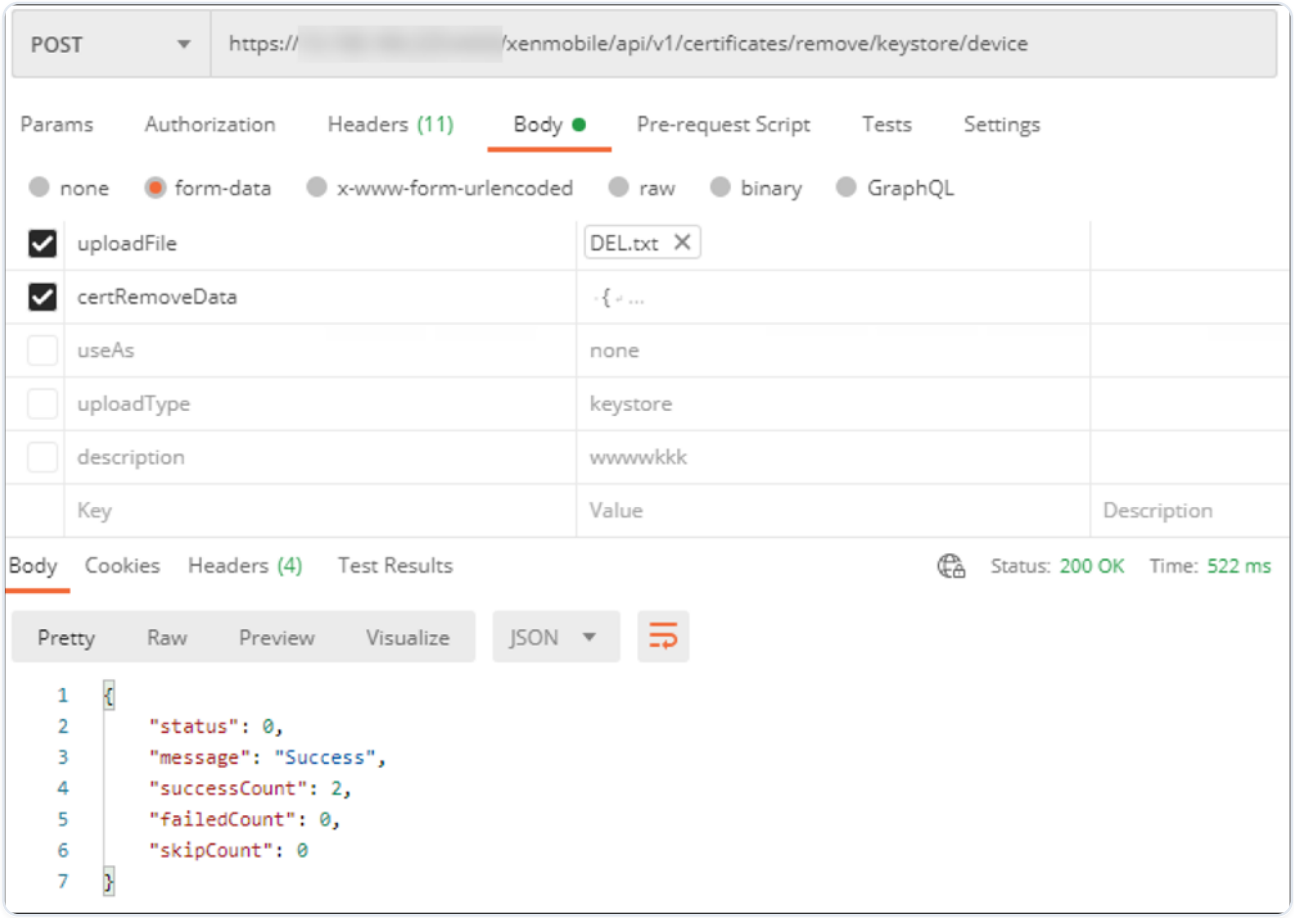
6. 자격 증명 유형이 **Always on IKEv2**이고 장치 인증 방법이 **Device Certificate Based on Device Identity**인 VPN 정책을 생성합니다. 인증서 파일 이름에 사용한 **장치 ID 유형**을 선택합니다. VPN 장치 정책을 참조하십시오.
7. iOS 장치를 등록하고 VPN 정책이 배포될 때까지 기다립니다. 장치에서 MDM 구성을 확인하여 인증서 설치를 확인합니다. XenMobile 콘솔에서 장치 세부 정보를 확인할 수도 있습니다.


12:08
Profile
MDM Configuration
MOBILE DEVICE MANAGEMENT
DEVICE IDENTITY CERTIFICATE
XenMobile MDM
Issued by: Devices Certificate Authority
Expires: April 17, 2022
CERTIFICATES (4)
Root Certificate Authority
Issued by: Root Certificate Authority
Expires: February 18, 2038
DigiCert SHA2 Secure Server CA
Issued by: DigiCert Global Root CA
Expires: March 8, 2023
DigiCert Global Root CA
Issued by: DigiCert Global Root CA
Expires: November 10, 2031
cem user02
Issued by:
Expires: February 25, 2021
SIGNING CERTIFICATE


Devices
Users
Enrollment Invitations
Device details
administrator | iPhone
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Media
7 Actions
8 Delivery Groups
9 iOS Profiles
iOS Profiles
Last iOS profile inventory: 4/19/20 4:01:07 am
Name
Type
Organization
Description
+ MDM Configuration (XenMobile,
– Device Certificate Based on Device Identity Type (Citrix, id

삭제할 각 인증서에 대해 `device_identity_value`이(가) 나열된 텍스트 파일을 생성하여 인증서를 대량으로 삭제할 수도 있습니다. REST API에서 삭제 API를 호출하고 다음 요청을 사용하며, `device_identity_value`를 적절한 식별자로 바꿉니다.

```
{
    "identityType"="device_identity_value"
}
```



인증서 업데이트

XenMobile은 한 번에 하나의 공개 키당 하나의 인증서만 시스템에 존재하도록 허용합니다. 이미 가져온 인증서와 동일한 키 쌍에 대한 인증서를 가져오려고 하면 기존 항목을 바꾸거나 항목을 삭제할 수 있습니다.

XenMobile 콘솔에서 인증서를 가장 효과적으로 업데이트하려면 다음을 수행하십시오. 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭하여 **설정** 페이지를 열고 **인증서**를 클릭합니다. **가져오기** 대화 상자에서 새 인증서를 가져옵니다.

서버 인증서를 업데이트하면 이전 인증서를 사용하던 구성 요소가 자동으로 새 인증서를 사용하도록 전환됩니다. 마찬가지로, 장치에 서버 인증서를 배포한 경우 다음 배포 시 인증서가 자동으로 업데이트됩니다.

인증서 갱신

XenMobile Server는 PKI를 위해 내부적으로 다음 인증 기관(CA)을 사용합니다: 루트 CA, 장치 CA, 서버 CA. 이러한 CA는 논리적 그룹으로 분류되어 그룹 이름이 제공됩니다. 새 XenMobile Server 인스턴스가 프로비저닝되면 세 개의 CA가 생성되고 "default"라는 그룹 이름이 부여됩니다.

XenMobile Server 콘솔 또는 공개 REST API를 사용하여 지원되는 iOS, macOS 및 Android 장치에 대한 CA를 갱신할 수 있습니다. 등록된 Windows 장치의 경우 사용자는 새 장치 CA를 받으려면 장치를 다시 등록해야 합니다.

다음 API는 XenMobile Server에서 내부 PKI CA를 갱신하거나 재생성하고 이러한 인증 기관에서 발급한 장치 인증서를 갱신하는 데 사용할 수 있습니다.

- 그룹 인증 기관(CA)을 생성합니다.
- 새 CA를 활성화하고 이전 CA를 비활성화합니다.
- 구성된 장치 목록에서 장치 인증서를 갱신합니다. 이미 등록된 장치는 중단 없이 계속 작동합니다. 장치 인증서는 장치가 서버에 다시 연결될 때 발급됩니다.
- 이전 CA를 여전히 사용하는 장치 목록을 반환합니다.
- 모든 장치에 새 CA가 설치된 후 이전 CA를 삭제합니다.

자세한 내용은 Public API for REST Services PDF의 다음 섹션을 참조하십시오.

- 섹션 3.16.58, 장치 인증서 갱신
- 섹션 3.23, 내부 PKI CA 그룹

장치 관리 콘솔에는 장치의 등록 인증서를 갱신하는 데 사용되는 보안 작업인 **인증서 갱신**이 포함되어 있습니다.

필수 구성 요소

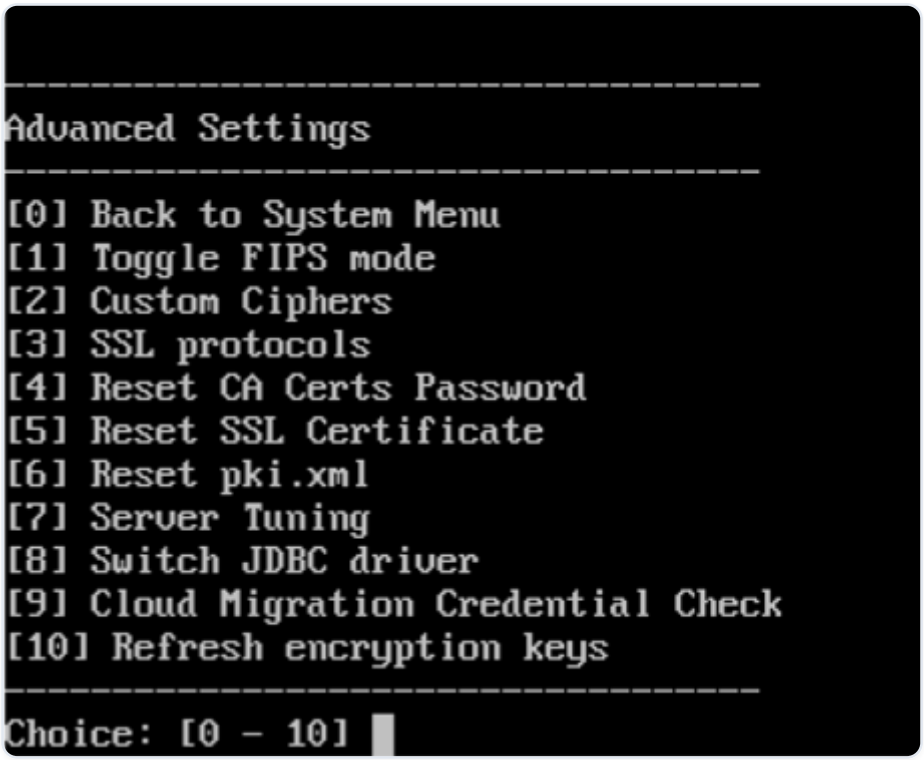
- 기본적으로 이 인증서 새로 고침 기능은 비활성화되어 있습니다. 인증서 새로 고침 기능을 활성화하려면 서버 속성 **refresh.internal.ca**의 값을 **True**로 설정하십시오.

> **중요:**

> Citrix ADC가 SSL 오프로드용으로 설정된 경우, 새 인증서를 생성할 때 로드 밸런서를 새 cacert.perm으로 업데이트해야 합니다. Citrix Gateway 설정에 대한 자세한 내용은 NetScaler VIP에 SSL 오프로드 모드를 사용하는 방법을 참조하십시오.

클러스터 노드의 서버 CA 인증서 암호를 재설정하는 CLI 옵션

하나의 XenMobile Server 노드에서 서버 CA 인증서를 생성한 후 XenMobile CLI를 사용하여 다른 클러스터 노드에서 인증서 암호를 재설정합니다. CLI 주 메뉴에서 **시스템 > 고급 설정 > CA 인증서 암호 재설정**을 선택합니다. 새 CA 인증서가 없을 때 암호를 재설정하면 XenMobile은 암호를 재설정하지 않습니다.



XenMobile 인증서 관리

XenMobile 배포에서 사용하는 인증서, 특히 만료 날짜 및 관련 암호를 목록으로 작성하는 것이 좋습니다. 이 섹션은 XenMobile에서 인증서 관리를 더 쉽게 하는 데 도움이 되도록 작성되었습니다.

환경에는 다음 인증서 중 일부 또는 전부가 포함될 수 있습니다.

- 젠모바일 서버
  - MDM FQDN용 SSL 인증서
  - SAML 인증서 (Citrix Files용)
  - 이전 인증서 및 기타 내부 리소스(StoreFront/프록시 등)용 루트 및 중간 CA 인증서

    - iOS 장치 관리용 APN 인증서
    - XenMobile Server Secure Hub 알림용 내부 APNs 인증서
    - PKI 연결용 PKI 사용자 인증서
- MDX 툴킷
    - Apple 개발자 인증서
    - Apple 프로비저닝 프로필 (애플리케이션별)
    - Apple APNs 인증서 (Citrix Secure Mail™과 함께 사용)
    - Android 키스토어 파일

  MAM SDK는 앱을 래핑하지 않으므로 인증서가 필요하지 않습니다.
- 시트릭스 ADC
    - MDM FQDN용 SSL 인증서
    - Gateway FQDN용 SSL 인증서
    - ShareFile SZC FQDN용 SSL 인증서
    - Exchange 부하 분산용 SSL 인증서 (오프로드 구성)
    - StoreFront 로드 밸런싱용 SSL 인증서
    - 이전 인증서에 대한 루트 및 중간 CA 인증서

XenMobile 인증서 만료 정책

인증서가 만료되도록 허용하면 인증서가 무효화됩니다. 더 이상 환경에서 보안 트랜잭션을 실행할 수 없으며 XenMobile 리소스에 액세스할 수 없습니다.

> **참고:**

> 인증 기관(CA)은 만료일 전에 SSL 인증서를 갱신하도록 요청합니다.

Citrix Secure Mail용 APNs 인증서

Apple Push Notification Service(APNs) 인증서는 매년 만료됩니다. 인증서가 만료되기 전에 APNs SSL 인증서를 생성하고 Citrix 포털에서 업데이트해야 합니다. 인증서가 만료되면 사용자는 Secure Mail 푸시 알림에서 불일치를 겪게 됩니다. 또한 앱에 대한 푸시 알림을 더 이상 보낼 수 없습니다.

iOS 장치 관리를 위한 APNs 인증서

XenMobile로 iOS 장치를 등록하고 관리하려면 Apple에서 APNs 인증서를 설정하고 생성하십시오. 인증서가 만료되면 사용자는 XenMobile에 등록할 수 없으며 iOS 장치를 관리할 수 없습니다. 자세한 내용은 APNs 인증서를 참조하십시오.

Apple Push Certificates Portal에 로그인하여 APNs 인증서 상태 및 만료일을 확인할 수 있습니다. 인증서를 생성한 동일한 사용자로 로그인해야 합니다.

또한 만료일 30일 및 10일 전에 Apple로부터 이메일 알림을 받게 됩니다. 알림에는 다음 정보가 포함됩니다.

```
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.



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.



Thank You,



Apple Push Notification Service
```

MDX Toolkit (iOS 배포 인증서)

물리적 iOS 장치에서 실행되는 앱(Apple App Store의 앱 제외)에는 다음과 같은 서명 요구 사항이 있습니다.

- 프로비저닝 프로필로 앱에 서명합니다.
- 해당 배포 인증서로 앱에 서명합니다.

유효한 iOS 배포 인증서가 있는지 확인하려면 다음을 수행하십시오.

1. Apple Enterprise Developer 포털에서 MDX Toolkit으로 래핑할 각 앱에 대한 명시적 앱 ID를 만듭니다. 허용되는 앱 ID의 예는 다음과 같습니다. `com.CompanyName.ProductName`.

2. Apple Enterprise Developer 포털에서 **프로비저닝 프로필 > 배포**로 이동하여 사내 프로비저닝 프로필을 만듭니다. 이전 단계에서 생성된 각 앱 ID에 대해 이 단계를 반복합니다.
3. 모든 프로비저닝 프로필을 다운로드합니다. 자세한 내용은 iOS 모바일 앱 래핑을 참조하십시오.

모든 XenMobile Server 인증서가 유효한지 확인하려면 다음을 수행하십시오.

1. XenMobile 콘솔에서 **설정 > 인증서**를 클릭합니다.
2. APN, SSL 수신기, 루트 및 중간 인증서를 포함한 모든 인증서가 유효한지 확인합니다.

Android 키 저장소

키 저장소는 Android 앱에 서명하는 데 사용되는 인증서를 포함하는 파일입니다. 키 유효 기간이 만료되면 사용자는 더 이상 앱의 새 버전으로 원활하게 업그레이드할 수 없습니다.

시트릭스 ADC

Citrix ADC에 대한 인증서 만료를 처리하는 방법에 대한 자세한 내용은 Citrix 지원 기술 자료에서 NetScaler에서 인증서 만료를 처리하는 방법을 참조하십시오.

만료된 Citrix ADC 인증서는 사용자가 Store에 등록하고 액세스하는 것을 방지합니다. 만료된 인증서는 또한 Secure Mail을 사용할 때 사용자가 Exchange Server에 연결하는 것을 방지합니다. 또한 사용자는 HDX 앱을 열거하고 열 수 없습니다(만료된 인증서에 따라 다름).

Expiry Monitor 및 Command Center는 Citrix ADC 인증서를 추적하는 데 도움이 될 수 있습니다. 센터는 인증서가 만료될 때 사용자에게 알립니다. 이러한 도구는 다음 Citrix ADC 인증서를 모니터링하는 데 도움이 됩니다.

- MDM FQDN용 SSL 인증서
- 게이트웨이 FQDN용 SSL 인증서
- ShareFile SZC FQDN용 SSL 인증서
- Exchange 부하 분산용 SSL 인증서 (오프로드 구성)
- StoreFront 부하 분산용 SSL 인증서
- 이전 인증서용 루트 및 중간 CA 인증서

시트릭스 게이트웨이 및 젠모바일®

XenMobile을 사용하여 Citrix Gateway를 구성할 때, 내부 네트워크에 대한 원격 장치 액세스를 위한 인증 메커니즘을 설정합니다. 이 기능은 모바일 장치의 앱이 인트라넷의 회사 서버에 액세스할 수 있도록 합니다. XenMobile은 장치의 앱에서 Citrix Gateway로 마이크로 VPN을 생성합니다.

XenMobile과 함께 사용하도록 Citrix Gateway를 구성하려면 XenMobile에서 스크립트를 내보내 Citrix Gateway에서 실행해야 합니다.

Citrix Gateway 구성 스크립트 사용을 위한 필수 구성 요소

Citrix ADC 요구 사항:

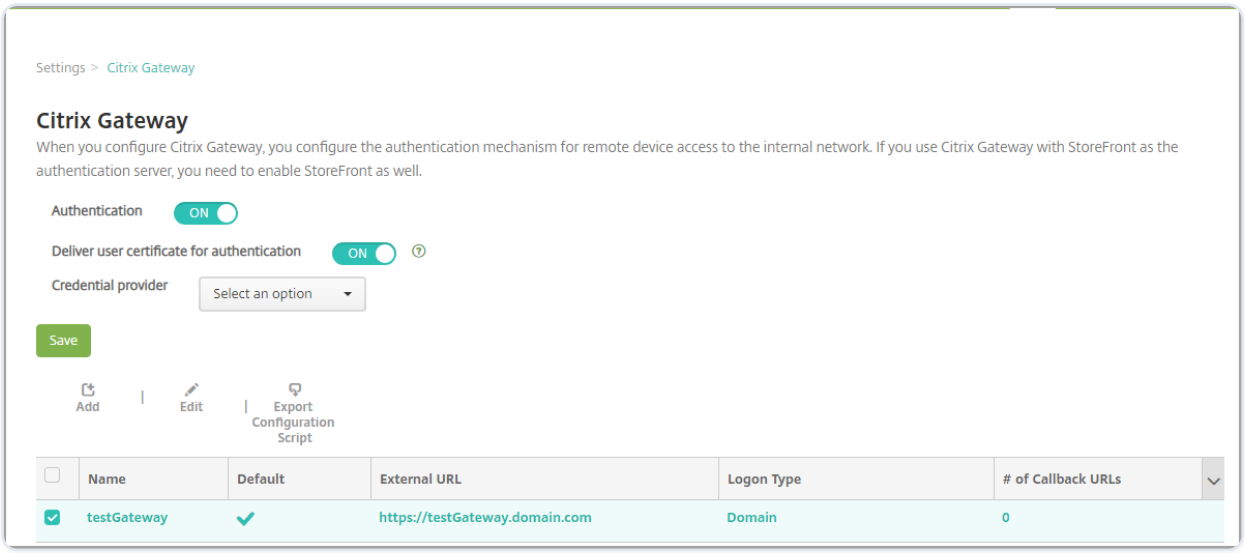
- Citrix ADC (최소 버전 11.0, 빌드 70.12).
- Citrix ADC IP 주소가 구성되어 있어야 하며, LDAP가 로드 밸런싱되지 않는 한 LDAP 서버에 연결되어 있어야 합니다.
- Citrix ADC 서브넷(SNIP) IP 주소가 구성되어 있어야 하며, 필요한 백엔드 서버에 연결되어 있어야 하고 , 포트 8443/TCP를 통해 공용 네트워크에 액세스할 수 있어야 합니다.
- DNS는 공용 도메인을 확인할 수 있어야 합니다.
- Citrix ADC는 Platform/Universal 또는 Trial 라이선스로 라이선스가 부여되어야 합니다. 자세한 내용은 `<https://support.citrix.com/article/CTX126049>`을 참조하십시오.
- Citrix Gateway SSL 인증서가 Citrix ADC에 업로드 및 설치되어 있어야 합니다. 자세한 내용은 `<https://support.citrix.com/article/CTX136023>`을 참조하십시오.

XenMobile 요구 사항:

- XenMobile Server (최소 버전 10.6).
- LDAP 서버가 구성되어 있어야 합니다.

내부 네트워크에 대한 원격 장치 액세스 인증 구성

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **서버** 아래에서 **Citrix Gateway**를 클릭합니다. **Citrix Gateway** 페이지가 나타납니다. 다음 예시에서는 Citrix Gateway 인스턴스가 존재합니다.



3. 다음 설정을 구성합니다.

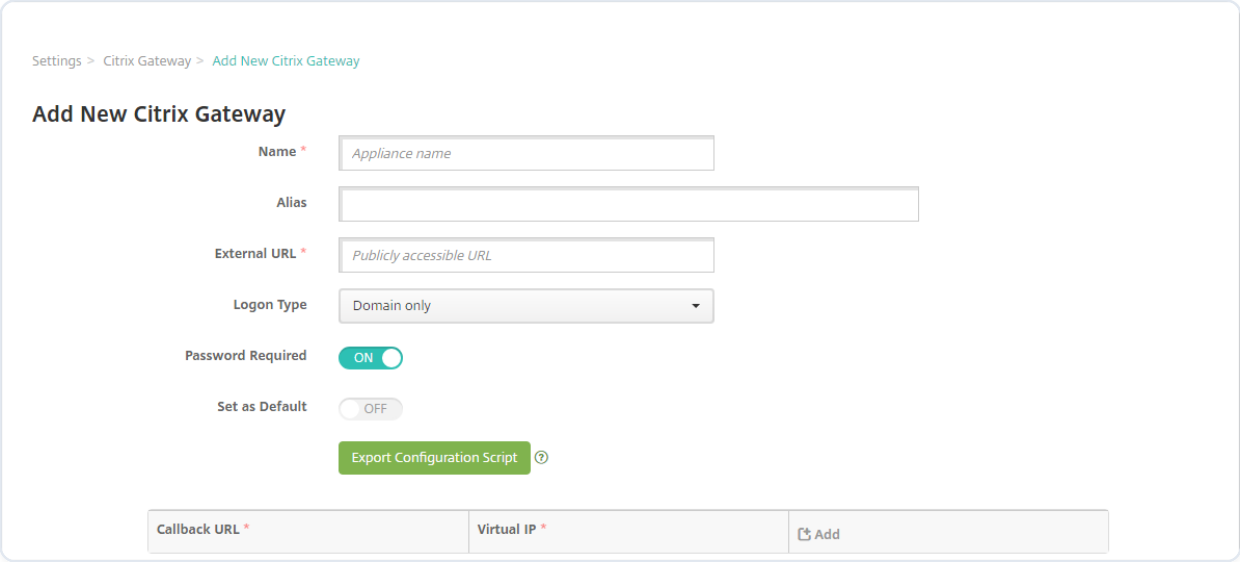
   - **인증:** 인증을 활성화할지 여부를 선택합니다. 기본값은 **ON**입니다.
   - **인증을 위한 사용자 인증서 전달:** XenMobile이 Secure Hub와 인증 인증서를 공유하여 Citrix Gateway가 클라이언트 인증서 인증을 처리하도록 할지 여부를 선택합니다. 기본값은 **OFF**입니다.
   - **자격 증명 공급자:** 목록에서 사용할 자격 증명 공급자를 클릭합니다. 자세한 내용은 자격 증명 공급자를 참조하십시오.

4. **저장**을 클릭합니다.

Citrix Gateway 인스턴스 추가

인증 설정을 저장한 후 XenMobile에 Citrix Gateway 인스턴스를 추가합니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 열립니다.
2. **서버** 아래에서 **Citrix Gateway**를 클릭합니다. **Citrix Gateway** 페이지가 나타납니다.
3. **추가**를 클릭합니다. **새 Citrix Gateway 추가** 페이지가 나타납니다.



4. 다음 설정을 구성합니다.

   - **이름:** Citrix Gateway 인스턴스의 이름을 입력합니다.
   - **별칭:** 선택적으로 Citrix Gateway의 별칭 이름을 포함합니다.
   - **외부 URL:** Citrix Gateway의 공개적으로 액세스 가능한 URL을 입력합니다. 예를 들어, `https://receiver.com`.
   - **로그온 유형:** 로그온 유형을 선택합니다. 유형에는 **도메인 전용**, **보안 토큰 전용**, **도메인 및 보안 토큰**, **인증서**, **인증서 및 도메인**, **인증서 및 보안 토큰**이 있습니다. **암호 필요** 필드의 기본 설정은 선택한 **로그온 유형**에 따라 변경됩니다. 기본값은 **도메인 전용**입니다.

   여러 도메인이 있는 경우 **인증서 및 도메인**을 사용합니다. XenMobile 및 Citrix Gateway를 사용하여 다중 도메인 인증을 구성하는 방법에 대한 자세한 내용은 다중 도메인 인증 구성을 참조하십시오.

   인증서 및 보안 토큰을 사용하는 경우 Secure Hub를 지원하려면 Citrix Gateway에 추가 구성이 필요합니다. 자세한 내용은 인증서 및 보안 토큰 인증을 위한 XenMobile 구성을 참조하십시오.

   자세한 내용은 배포 핸드북의 인증을 참조하십시오.

   - **암호 필요:** 암호 인증을 요구할지 여부를 선택합니다. 기본값은 선택한 **로그온 유형**에 따라 다릅니다.
   - **기본값으로 설정:** 이 Citrix Gateway를 기본값으로 사용할지 여부를 선택합니다. 기본값은 **OFF**입니다.
   - **구성 스크립트 내보내기:** 이 버튼을 클릭하여 XenMobile 설정으로 Citrix Gateway를 구성하기 위해 업로드할 구성 번들을 내보냅니다. 자세한 내용은 이 단계 다음에 나오는 "XenMobile Server와 함께 사용하도록 온프레미스 Citrix Gateway 구성"을 참조하십시오.
   - **콜백 URL** 및 **가상 IP:** 이 필드를 추가하기 전에 설정을 저장합니다. 자세한 내용은 이 문서의 콜백 URL 및 Citrix Gateway VPN 가상 IP 추가를 참조하십시오.

5. **저장**을 클릭합니다.

   새 Citrix Gateway가 추가되어 테이블에 나타납니다. 인스턴스를 편집하거나 삭제하려면 목록에서 이름을 클릭합니다.

XenMobile Server와 함께 사용하도록 Citrix Gateway 구성

XenMobile과 함께 사용하도록 온프레미스 Citrix Gateway를 구성하려면 이 문서에 자세히 설명된 다음 일반 단계를 수행합니다.

1. XenMobile Server에서 스크립트 및 관련 파일을 다운로드합니다. 최신 자세한 지침은 스크립트와 함께 제공된 readme 파일을 참조하십시오.
2. 환경이 필수 구성 요소를 충족하는지 확인합니다.
3. 환경에 맞게 스크립트를 업데이트합니다.
4. Citrix ADC에서 스크립트를 실행합니다.
5. 구성을 테스트합니다.

스크립트는 XenMobile에 필요한 다음 Citrix Gateway 설정을 구성합니다.

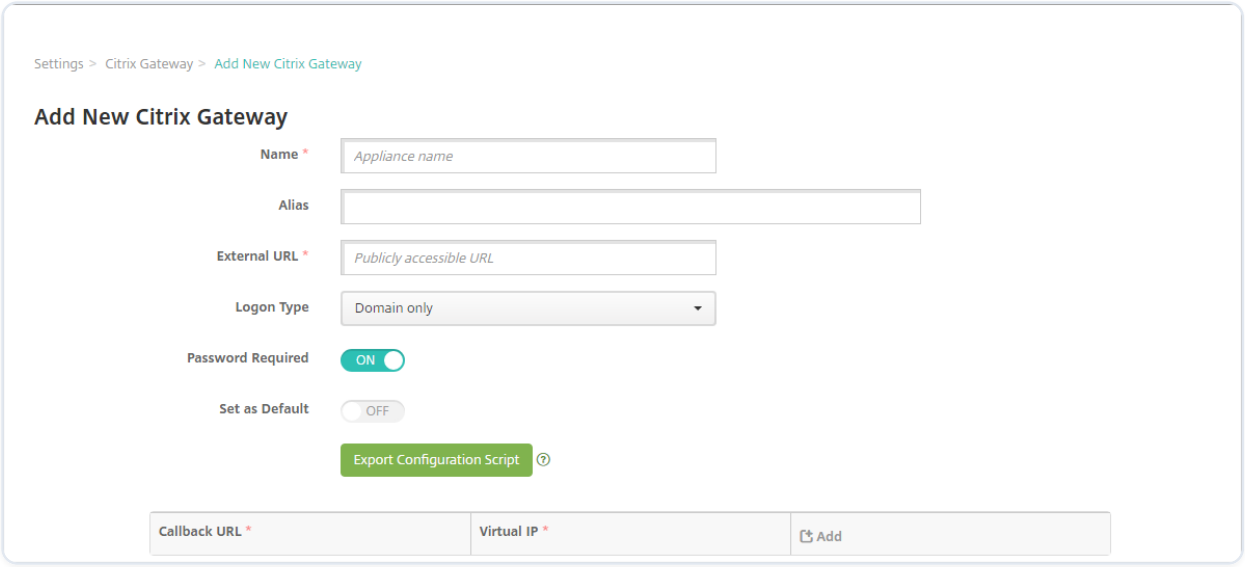
- MDM 및 MAM에 필요한 Citrix Gateway 가상 서버
- Citrix Gateway 가상 서버에 대한 세션 정책
- XenMobile Server 세부 정보
- Citrix Gateway 가상 서버에 대한 인증 정책 및 작업. 스크립트는 LDAP 구성 설정을 설명합니다.
- 프록시 서버에 대한 트래픽 작업 및 정책
- 클라이언트리스 액세스 프로필
- Citrix ADC의 정적 로컬 DNS 레코드
- 기타 바인딩: 서비스 정책, CA 인증서

스크립트는 다음 구성을 처리하지 않습니다.

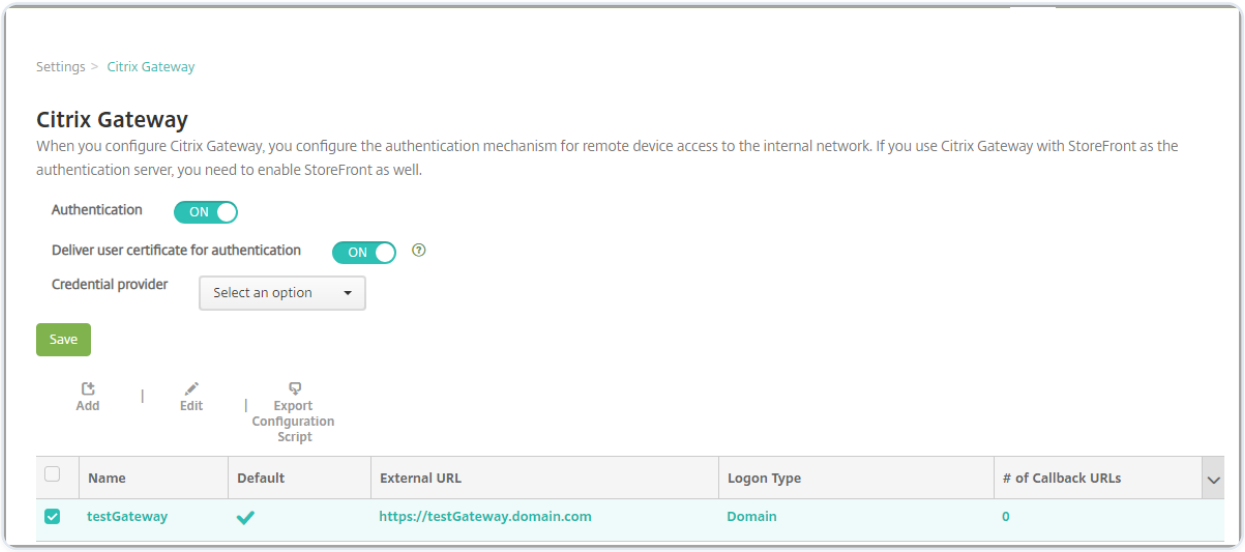
- Exchange 로드 밸런싱
- Citrix Files 로드 밸런싱
- ICA® 프록시 구성
- SSL 오프로드

스크립트 다운로드, 업데이트 및 실행

1. Citrix Gateway를 추가하는 경우 **새 Citrix Gateway 추가** 페이지에서 **구성 스크립트 내보내기**를 클릭합니다.



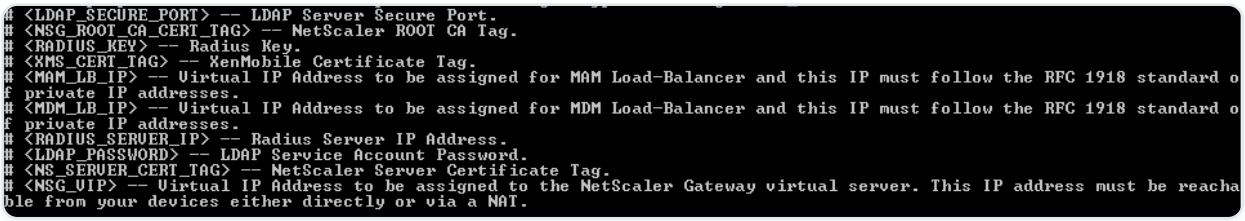
또는 Citrix Gateway 인스턴스를 추가하고 스크립트를 내보내기 전에 **저장**을 클릭한 경우: **설정 > Citrix Gateway**로 돌아가서 Citrix ADC를 선택하고 **구성 스크립트 내보내기**를 클릭한 다음 **다운로드**를 클릭합니다.



구성 스크립트 내보내기를 클릭하면 XenMobile에서 .tar.gz 스크립트 번들을 생성합니다. 스크립트 번들에는 다음이 포함됩니다.

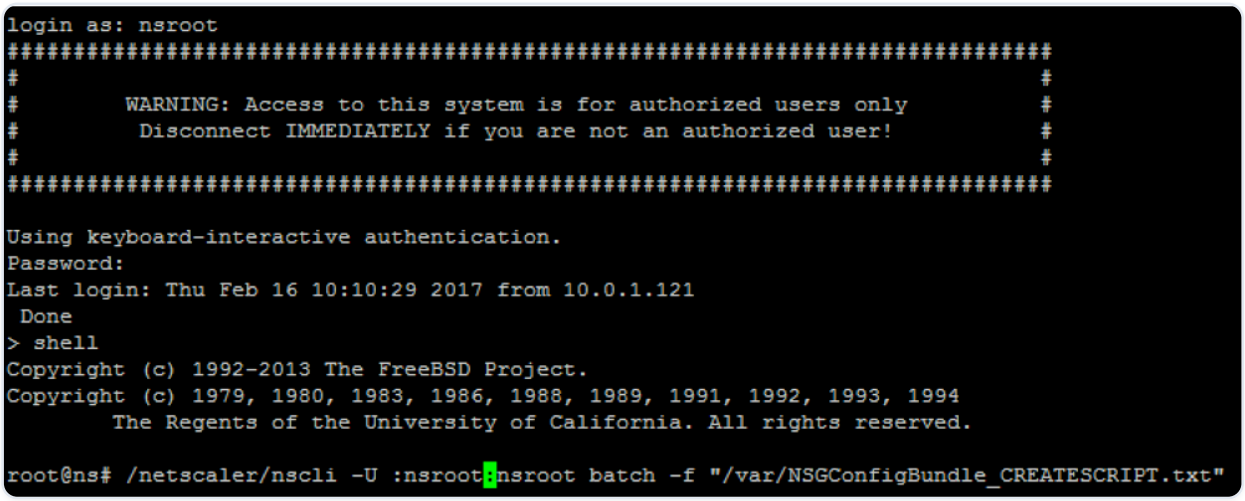
- 자세한 지침이 포함된 Readme 파일
- Citrix ADC에서 필요한 구성 요소를 구성하는 데 사용되는 Citrix ADC CLI 명령이 포함된 스크립트
- XenMobile Server의 공용 루트 CA 인증서 및 중간 CA 인증서(SSL 오프로드용인 이 인증서는 현재 릴리스에는 필요하지 않음)
- Citrix ADC 구성을 제거하는 데 사용되는 Citrix ADC CLI 명령이 포함된 스크립트

2. 스크립트(NSGConfigBundle_CREATESCRIPT.txt)를 편집하여 모든 자리 표시자를 환경의 세부 정보로 바꿉니다.

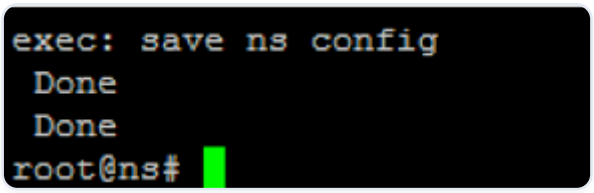


3. 스크립트 번들에 포함된 readme 파일에 설명된 대로 Citrix ADC bash 셸에서 편집된 스크립트를 실행합니다. 예시:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

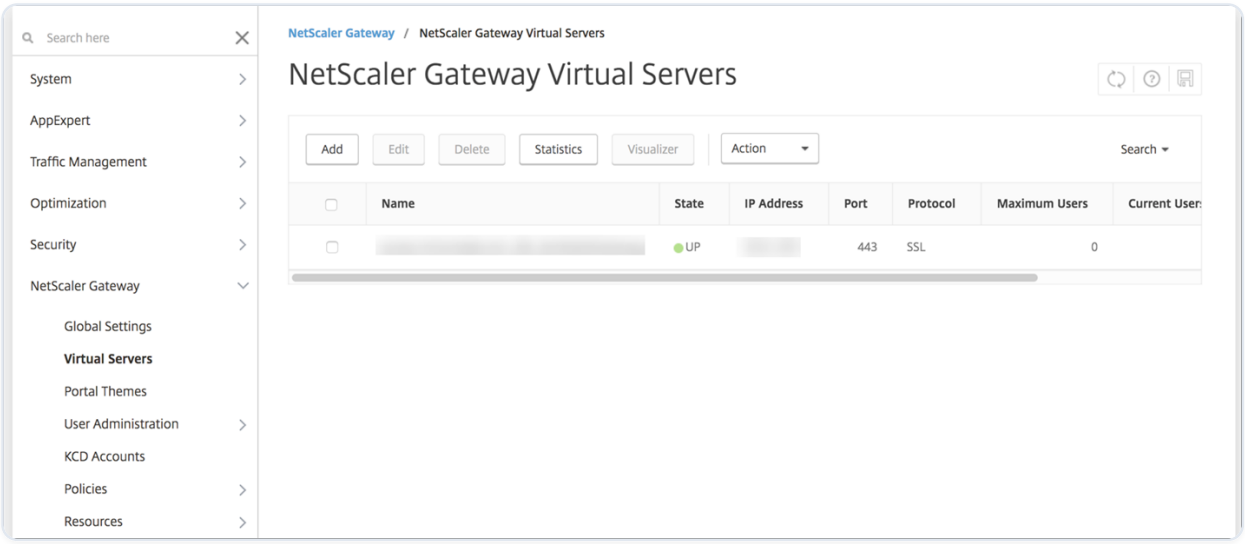


스크립트가 완료되면 다음 줄이 나타납니다.

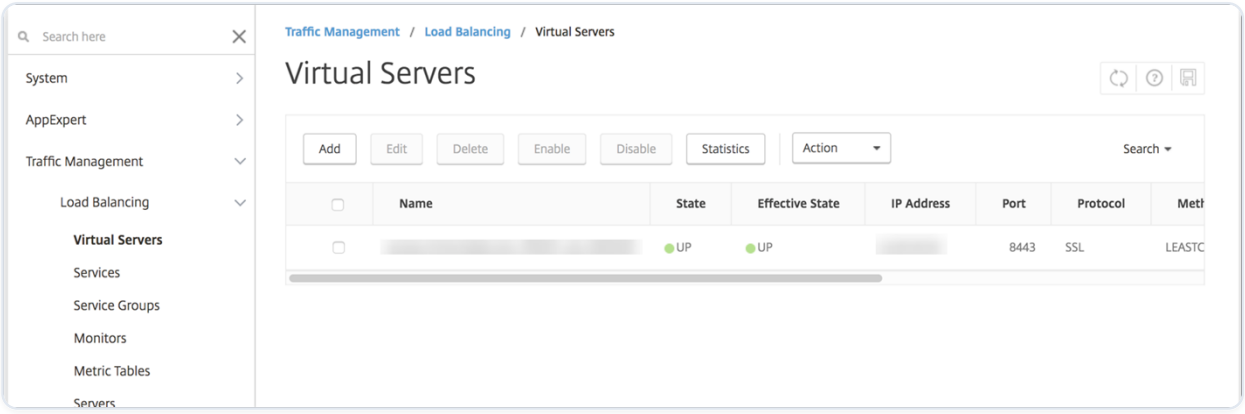


구성 테스트

1. Citrix Gateway 가상 서버의 상태가 **UP**으로 표시되는지 확인합니다.



2. 프록시 로드 밸런싱 가상 서버의 상태가 **UP**으로 표시되는지 확인합니다.



3. 웹 브라우저를 열고 Citrix Gateway URL에 연결한 다음 인증을 시도합니다. 인증에 실패하면 다음 메시지가 나타납니다: HTTP Status 404 - Not Found
4. 장치를 등록하고 MDM 및 MAM 등록을 모두 받는지 확인합니다.

콜백 URL 및 Citrix Gateway VPN 가상 IP 추가

Citrix Gateway 인스턴스를 추가한 후 콜백 URL을 추가하고 Citrix Gateway 가상 IP 주소를 지정할 수 있습니다. 이러한 설정은 선택 사항이지만, 특히 XenMobile Server가 DMZ에 있는 경우 추가 보안을 위해 구성할 수 있습니다.

1. **설정 > Citrix Gateway**에서 Citrix Gateway를 선택한 다음 **편집**을 클릭합니다.
2. 테이블에서 **추가**를 클릭합니다.
3. **콜백 URL**에 FQDN(정규화된 도메인 이름)을 입력합니다. 콜백 URL은 요청이 Citrix Gateway에서 시작되었는지 확인합니다.

   콜백 URL이 XenMobile Server에서 연결할 수 있는 IP 주소로 확인되는지 확인합니다. 콜백 URL은 외부 Citrix Gateway URL이거나 다른 URL일 수 있습니다.

4. Citrix Gateway **가상 IP** 주소를 입력한 다음 **저장**을 클릭합니다.

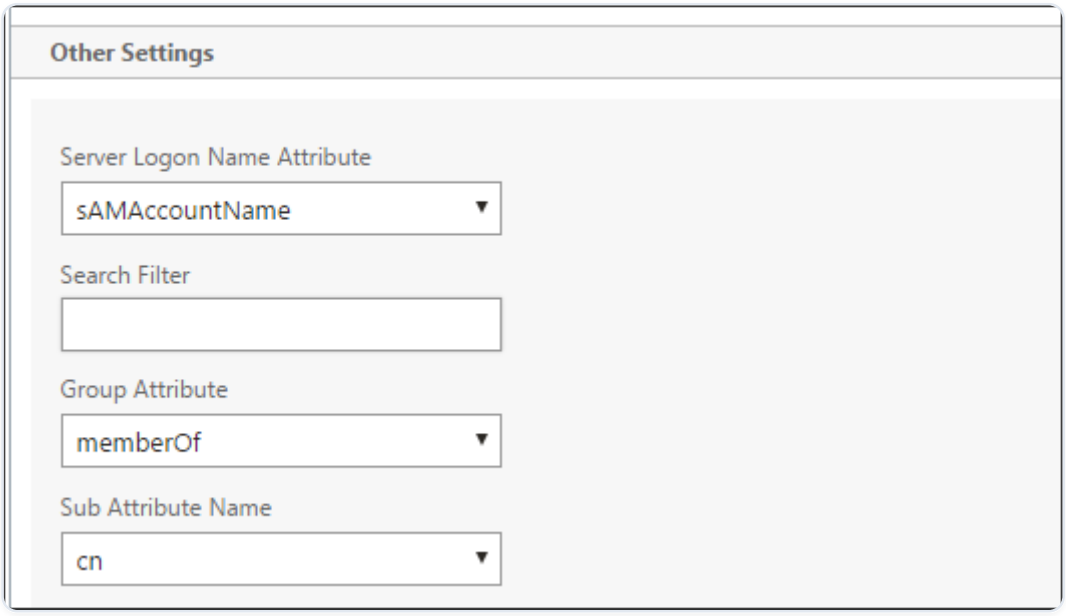
여러 도메인에 대한 인증 구성

테스트, 개발 및 프로덕션 환경과 같이 여러 XenMobile Server 인스턴스가 있는 경우 추가 환경에 대해 Citrix Gateway를 수동으로 구성합니다. (XenMobile 마법사용 Citrix ADC는 한 번만 사용할 수 있습니다.)

시트릭스 게이트웨이 구성

다중 도메인 환경에 대한 Citrix Gateway 인증 정책 및 세션 정책을 구성하려면 다음을 수행합니다.

1. Citrix Gateway 구성 유틸리티의 **구성** 탭에서 **Citrix Gateway > 정책 > 인증**을 확장합니다.
2. 탐색 창에서 **LDAP**를 클릭합니다.
3. 클릭하여 LDAP 프로필을 편집합니다. **서버 로그온 이름 특성**을 **userPrincipalName** 또는 검색에 사용할 특성으로 변경합니다. XenMobile 콘솔에서 LDAP 설정을 구성할 때 사용할 수 있도록 지정한 특성을 기록해 둡니다.

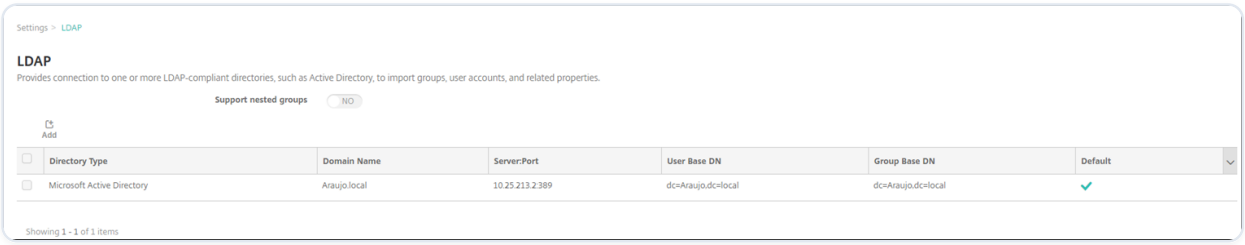


4. 각 LDAP 정책에 대해 이 단계를 반복합니다. 각 도메인에 대해 별도의 LDAP 정책이 필요합니다.
5. Citrix Gateway 가상 서버에 바인딩된 세션 정책에서 **세션 프로필 편집 > 게시된 응용 프로그램**으로 이동합니다. **단일 Sign-On 도메인**이 비어 있는지 확인합니다.

XenMobile Server 구성

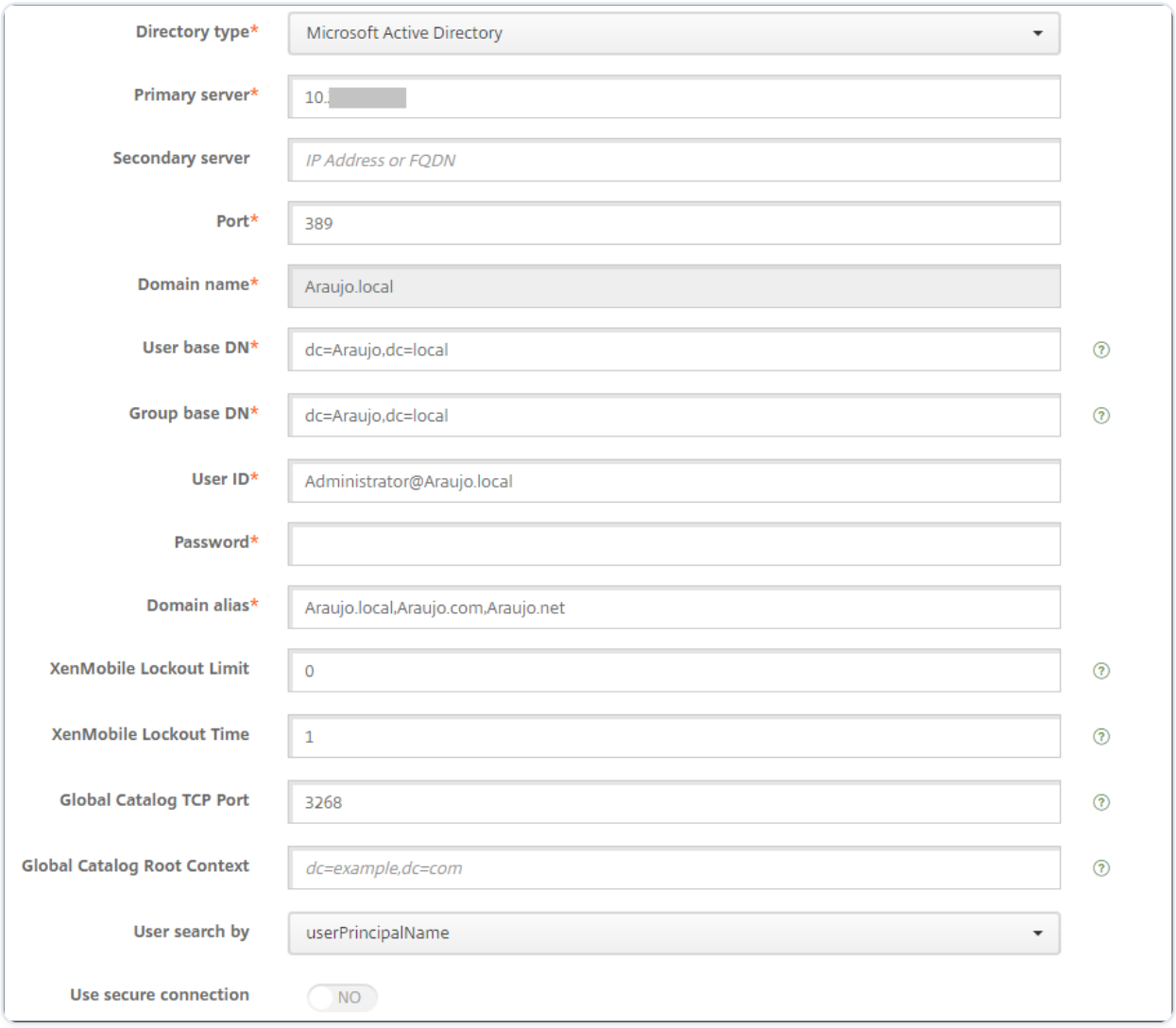
다중 도메인 XenMobile 환경에 대해 LDAP를 구성하려면 다음을 수행합니다.

1. XenMobile 콘솔에서 **설정 > LDAP**로 이동하여 디렉터리를 추가하거나 편집합니다.



2. 정보를 제공합니다.

   - **도메인 별칭**에서 사용자 인증에 사용할 각 도메인을 지정합니다. 도메인 사이에 쉼표로 구분하고 공백을 사용하지 마십시오. 예: `domain1.com,domain2.com,domain3.com`
   - **사용자 검색 기준** 필드가 Citrix Gateway LDAP 정책에 지정된 **서버 로그온 이름 특성**과 일치하는지 확인합니다.



특정 URL에 대한 인바운드 연결 요청 삭제

환경의 Citrix Gateway가 SSL 오프로드용으로 구성된 경우, 게이트웨이가 특정 URL에 대한 인바운드 연결 요청을 삭제하도록 하는 것이 좋습니다.

추가 보안을 선호하는 경우, Citrix Gateway에서 두 개의 MDM 로드 밸런서 가상 서버(포트 443용 하나, 포트 8443용 하나)를 구성합니다. 다음 정보를 설정 템플릿으로 사용하십시오.

> **중요:**
>
> 다음 업데이트는 SSL 오프로드용으로 구성된 Citrix Gateway에만 해당됩니다.

1. `XMS_DropURLs` 이름으로 패턴 세트를 생성합니다.

```
add policy patset XMS_DropURLs
```

2. 새 패턴 세트에 다음 URL을 추가합니다. 필요에 따라 이 목록을 사용자 지정하십시오.

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6

bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5

bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4

bind policy patset XMS_DropURLs /zdm/log.jsp -index 3

bind policy patset XMS_DropURLs /zdm/login.jsp -index 2

bind policy patset XMS_DropURLs /zdm/console -index 1
```

3. 연결 요청이 지정된 서브넷에서 시작되지 않는 한, 이러한 URL로 향하는 모든 트래픽을 차단하는 정책을 생성합니다.

```
add responder policy XMS_DROP_pol
“CLIENT.IP.SRC.IN_SUBNET(192.168.0.0/24).NOT &&

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"
```

4. 새 정책을 MDM 로드 밸런서 가상 서버(포트 443 및 8443) 모두에 바인딩합니다.

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST



bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST
```

5. 브라우저를 통한 MAM URL 액세스 차단

   브라우저를 통해 MAM URL에 직접 액세스하면 사용자에게 Active Directory 자격 증명을 입력하라는 메시지가 표시됩니다. 이는 사용자가 자격 증명을 확인하는 도구 역할을 하지만, 일부 사용자는 이를 보안 위반으로 간주할 수 있습니다. 다음 섹션에서는 NetScaler의 Responder Policy 기능을 사용하여 MAM URL(NetScaler® Gateway VIP)에 대한 브라우저 액세스를 제한하는 방법을 설명합니다.

   다음 Responder 정책 중 하나를 생성하고 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`을(를) 사용하여 NetScaler Gateway 가상 서버에 바인딩

참고:

`_XM_XenMobileGateway`은(는) NetScaler Gateway 가상 서버의 예시 이름입니다.

도메인 또는 도메인과 보안 토큰 인증

XenMobile®은 LDAP(Lightweight Directory Access Protocol)를 준수하는 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 통해 분산 디렉터리 정보 서비스에 액세스하고 유지 관리하기 위한 오픈 소스, 공급업체 중립적인 응용 프로그램 프로토콜입니다. 디렉터리 정보 서비스는 네트워크 전체에서 사용할 수 있는 사용자, 시스템, 네트워크, 서비스 및 응용 프로그램에 대한 정보를 공유하는 데 사용됩니다.

LDAP의 일반적인 용도는 여러 서비스에서 단일 암호(사용자당)를 공유하는 사용자에게 SSO(Single Sign-On)를 제공하는 것입니다. Single Sign-On을 사용하면 사용자가 회사 웹 사이트에 한 번 로그인하여 회사 인트라넷에 인증된 액세스를 할 수 있습니다.

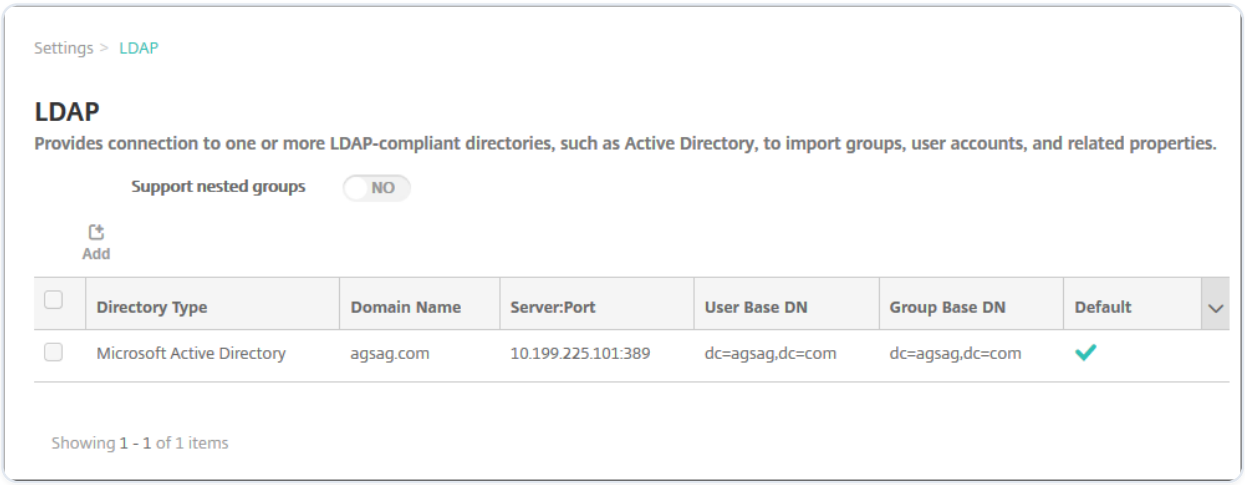
클라이언트는 DSA(Directory System Agent)로 알려진 LDAP 서버에 연결하여 LDAP 세션을 시작합니다. 그런 다음 클라이언트는 서버에 작업 요청을 보내고 서버는 적절한 인증으로 응답합니다.

중요:

XenMobile은 사용자가 XenMobile에 장치를 등록한 후 인증 모드를 도메인 인증에서 다른 인증 모드로 변경하는 것을 지원하지 않습니다.

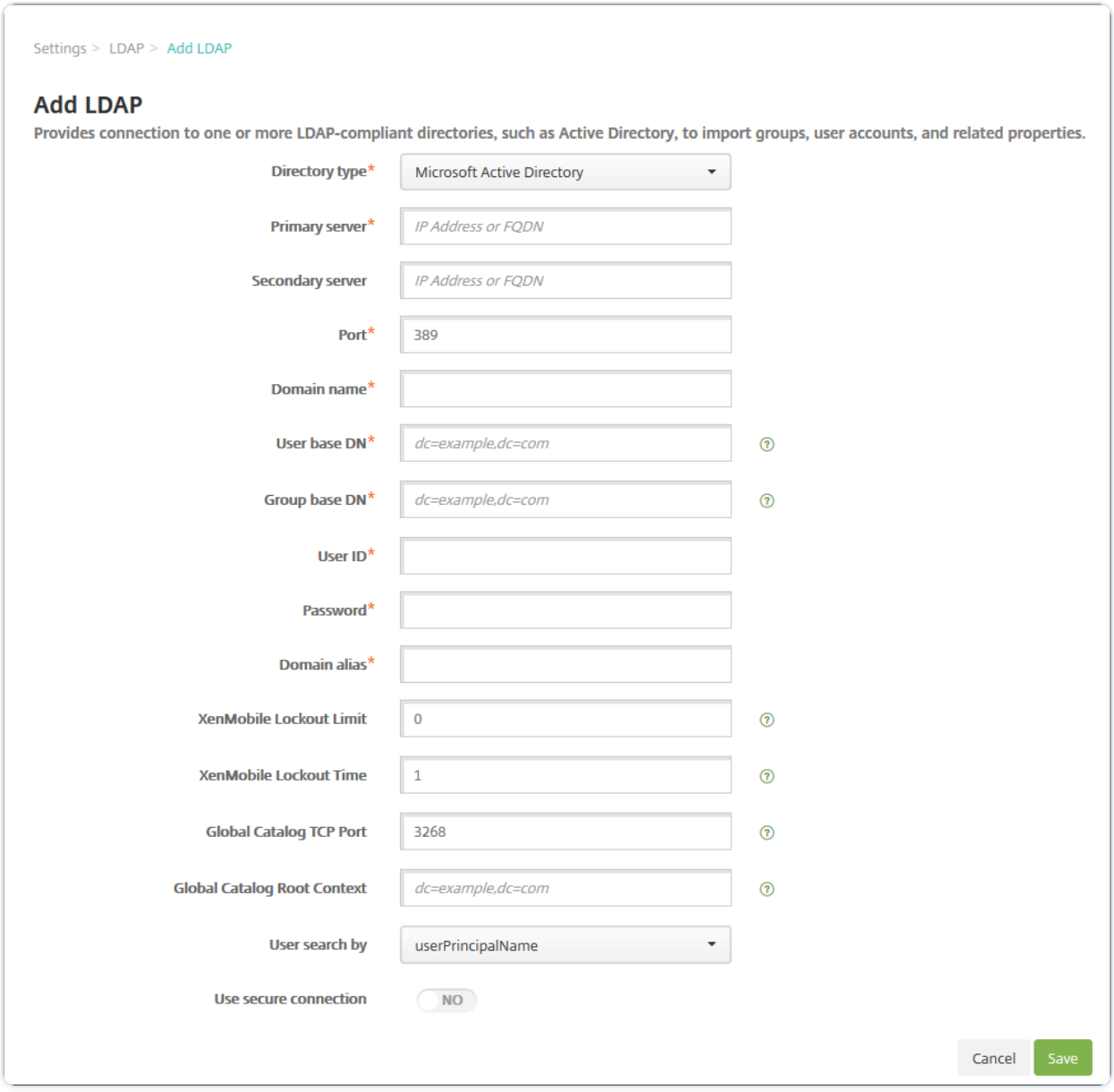
XenMobile에서 LDAP 연결을 추가하려면

1. XenMobile 콘솔에서 콘솔 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **서버**에서 **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 **추가**를 클릭합니다. **LDAP 추가** 페이지가 나타납니다.



2. 다음 설정을 구성합니다.

- **디렉터리 유형:** 목록에서 적절한 디렉터리 유형을 클릭합니다. 기본값은 **Microsoft Active Directory**입니다.
- **기본 서버:** LDAP에 사용되는 기본 서버를 입력합니다. IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력할 수 있습니다.
- **보조 서버:** 선택적으로 보조 서버가 구성된 경우 보조 서버의 IP 주소 또는 FQDN을 입력합니다. 이 서버는 기본 서버에 연결할 수 없을 때 사용되는 장애 조치 서버입니다.
- **포트:** LDAP 서버에서 사용하는 포트 번호를 입력합니다. 기본적으로 보안되지 않은 LDAP 연결의 경우 포트 번호는 **389**로 설정됩니다. 보안 LDAP 연결의 경우 포트 번호 **636**을 사용하고, Microsoft 보안되지 않은 LDAP 연결의 경우 **3268**을, Microsoft 보안 LDAP 연결의 경우 **3269**를 사용합니다.
- **도메인 이름:** 도메인 이름을 입력합니다.
- **사용자 기본 DN:** 고유 식별자를 통해 Active Directory에서 사용자의 위치를 입력합니다. 구문 예시는 `ou=users`, `dc=example` 또는 `dc=com`입니다.
- **그룹 기본 DN:** Active Directory에서 그룹의 위치를 입력합니다. 예를 들어, `cn=users, dc=domain, dc=net`에서 `cn=users`는 그룹의 컨테이너 이름을 나타내고 `dc`는 Active Directory의 도메인 구성 요소를 나타냅니다.
- **사용자 ID:** Active Directory 계정과 연결된 사용자 ID를 입력합니다.
- **암호:** 사용자와 연결된 암호를 입력합니다.
- **도메인 별칭:** 도메인 이름의 별칭을 입력합니다. 등록 후 **도메인 별칭** 설정을 변경하면 사용자는 다시 등록해야 합니다.
- **XenMobile 잠금 제한:** 실패한 로그온 시도 횟수에 대해 **0**에서 **999** 사이의 숫자를 입력합니다. 값이 **0**이면 XenMobile이 실패한 로그온 시도를 기반으로 사용자를 잠그지 않습니다.
- **XenMobile 잠금 시간:** 잠금 제한을 초과한 후 사용자가 기다려야 하는 시간(분)을 나타내는 **0**에서 **99999** 사이의 숫자를 입력합니다. 값이 **0**이면 잠금 후 사용자가 기다릴 필요가 없습니다.
- **글로벌 카탈로그 TCP 포트:** 글로벌 카탈로그 서버의 TCP 포트 번호를 입력합니다. 기본적으로 TCP 포트 번호는 **3268**로 설정되어 있으며, SSL 연결의 경우 포트 번호 **3269**를 사용합니다.
- **글로벌 카탈로그 루트 컨텍스트:** 선택적으로 Active Directory에서 글로벌 카탈로그 검색을 활성화하는 데 사용되는 글로벌 루트 컨텍스트 값을 입력합니다. 이 검색은 실제 도메인 이름을 지정할 필요 없이 모든 도메인에서 표준 LDAP 검색 외에 추가로 수행됩니다.
- **사용자 검색 기준:** 목록에서 **userPrincipalName** 또는 **sAMAccountName**을 클릭합니다. 기본값은 **userPrincipalName**입니다. 등록 후 **사용자 검색 기준** 설정을 변경하면 사용자는 다시 등록해야 합니다.
- **보안 연결 사용:** 보안 연결 사용 여부를 선택합니다. 기본값은 **아니요**입니다.

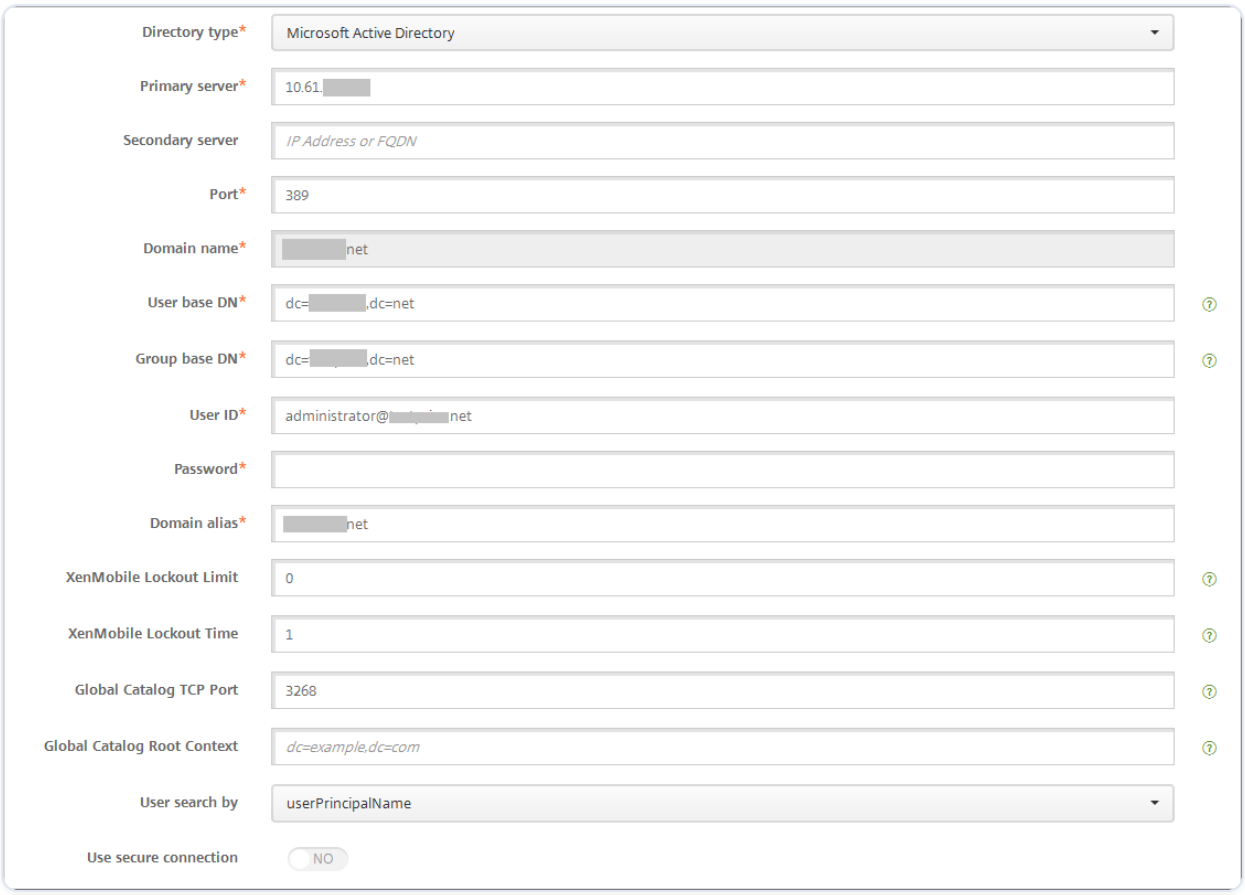
3. **저장**을 클릭합니다.

LDAP 호환 디렉터리를 편집하려면

1. **LDAP** 테이블에서 편집할 디렉터리를 선택합니다.

   디렉터리 옆의 확인란을 선택하면 LDAP 목록 위에 옵션 메뉴가 나타납니다. 목록의 다른 곳을 클릭하면 옵션 메뉴가 목록의 오른쪽에 나타납니다.

2. **편집**을 클릭합니다. **LDAP 편집** 페이지가 나타납니다.



3. 필요에 따라 다음 정보를 변경합니다.

   - **디렉터리 유형:** 목록에서 적절한 디렉터리 유형을 클릭합니다.
   - **기본 서버:** LDAP에 사용되는 기본 서버를 입력합니다. IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력할 수 있습니다.
   - **보조 서버:** 선택적으로 보조 서버의 IP 주소 또는 FQDN을 입력합니다(구성된 경우).
   - **포트:** LDAP 서버에서 사용하는 포트 번호를 입력합니다. 기본적으로 보안되지 않은 LDAP 연결의 경우 포트 번호는 **389**로 설정됩니다. 보안 LDAP 연결에는 포트 번호 **636**을 사용하고, Microsoft 보안되지 않은 LDAP 연결에는 **3268**을, Microsoft 보안 LDAP 연결에는 **3269**를 사용합니다.
   - **도메인 이름:** 이 필드는 변경할 수 없습니다.

- **사용자 기본 DN:** 고유 식별자를 통해 Active Directory에서 사용자의 위치를 입력합니다. 구문 예시는 `ou=users`, `dc=example` 또는 `dc=com`입니다.
- **그룹 기본 DN:** `cn=groupname`으로 지정된 그룹 기본 DN 그룹 이름을 입력합니다. 예를 들어, `cn=users`가 그룹 이름인 `cn=users, dc=servername, dc=net`입니다. `DN` 및 `servername`는 Active Directory를 실행하는 서버의 이름을 나타냅니다.
- **사용자 ID:** Active Directory 계정과 연결된 사용자 ID를 입력합니다.
- **암호:** 사용자와 연결된 암호를 입력합니다.
- **도메인 별칭:** 도메인 이름의 별칭을 입력합니다. 등록 후 **도메인 별칭** 설정을 변경하면 사용자는 다시 등록해야 합니다.
- **XenMobile 잠금 제한:** 실패한 로그온 시도 횟수에 대해 **0**에서 **999** 사이의 숫자를 입력합니다. 값이 **0**이면 XenMobile은 실패한 로그온 시도를 기반으로 사용자를 잠그지 않습니다.
- **XenMobile 잠금 시간:** 잠금 제한을 초과한 후 사용자가 기다려야 하는 시간(분)을 나타내는 **0**에서 **99999** 사이의 숫자를 입력합니다. 값이 **0**이면 사용자는 잠금 후 기다릴 필요가 없습니다.
- **글로벌 카탈로그 TCP 포트:** 글로벌 카탈로그 서버의 TCP 포트 번호를 입력합니다. 기본적으로 TCP 포트 번호는 **3268**로 설정되어 있으며, SSL 연결의 경우 포트 번호 **3269**를 사용합니다.
- **글로벌 카탈로그 루트 컨텍스트:** 선택적으로 Active Directory에서 글로벌 카탈로그 검색을 활성화하는 데 사용되는 글로벌 루트 컨텍스트 값을 입력합니다. 이 검색은 실제 도메인 이름을 지정할 필요 없이 모든 도메인에서 표준 LDAP 검색 외에 추가로 수행됩니다.
- **사용자 검색 기준:** 목록에서 **userPrincipalName** 또는 **sAMAccountName**을 클릭합니다. 등록 후 **사용자 검색 기준** 설정을 변경하면 사용자는 다시 등록해야 합니다.
- **보안 연결 사용:** 보안 연결을 사용할지 여부를 선택합니다.

4. 변경 내용을 저장하려면 **저장**을 클릭하고, 속성을 변경하지 않고 그대로 두려면 **취소**를 클릭합니다.

LDAP 호환 디렉터리를 삭제하려면

1. **LDAP** 테이블에서 삭제할 디렉터리를 선택합니다.

   각 속성 옆의 확인란을 선택하여 둘 이상의 속성을 삭제할 수 있습니다.

2. **삭제**를 클릭합니다. 확인 대화 상자가 나타납니다. **삭제**를 다시 클릭합니다.

여러 도메인에 대한 인증 구성

XenMobile Server에서 LDAP 구성에 여러 도메인 접미사를 사용하도록 구성하려면 Citrix Endpoint Management 설명서의 여러 도메인에 대한 인증 구성 절차를 참조하십시오. 이 단계는 XenMobile Server의 온프레미스 버전과 Endpoint Management 클라우드 릴리스에서 동일합니다.

도메인 및 보안 토큰 인증 구성

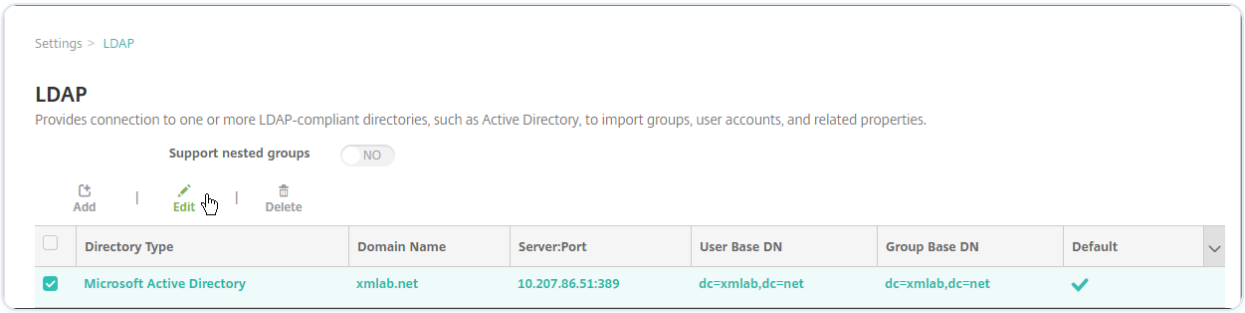
RADIUS 프로토콜을 사용하여 사용자가 LDAP 자격 증명과 일회용 암호로 인증하도록 XenMobile을 구성할 수 있습니다.

최적의 유용성을 위해 이 구성을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다. 이 구성을 사용하면 사용자가 LDAP 사용자 이름과 암호를 반복해서 입력할 필요가 없습니다. 사용자는 등록, 암호 만료 및 계정 잠금에 대해 사용자 이름과 암호를 입력합니다.

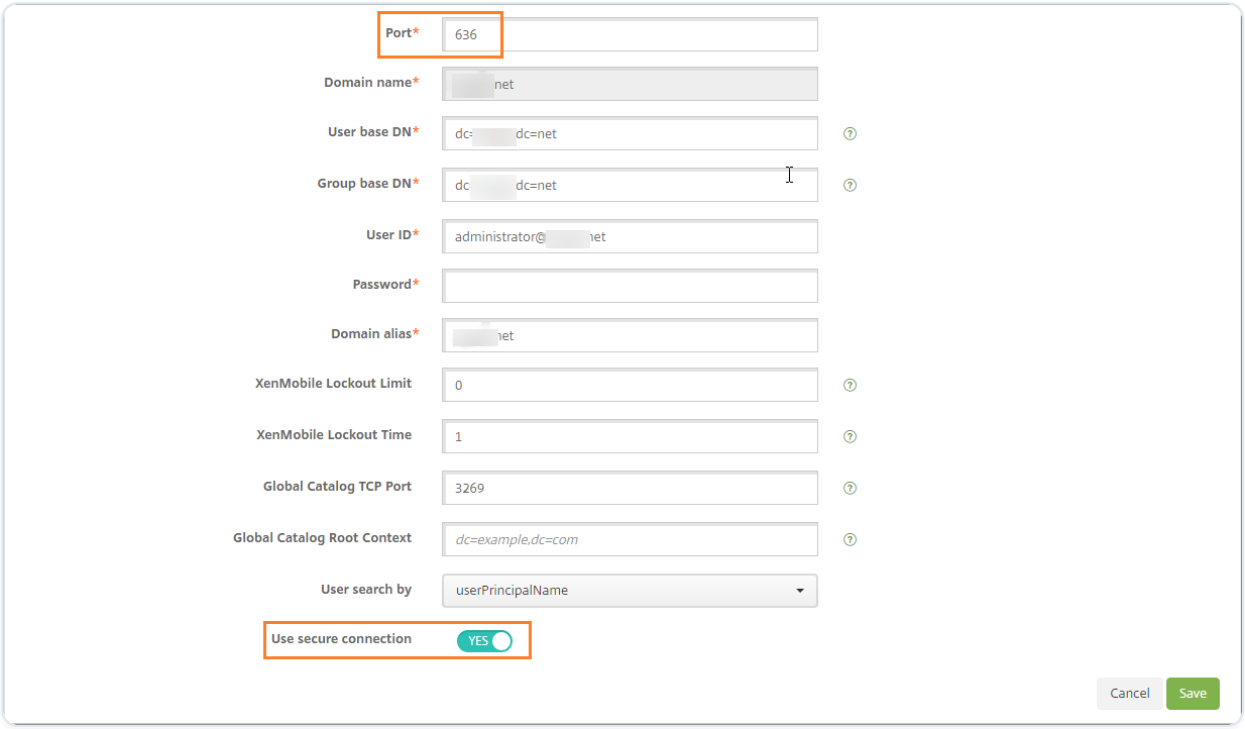
LDAP 설정 구성

인증을 위해 LDAP를 사용하려면 XenMobile에 인증 기관의 SSL 인증서를 설치해야 합니다. 자세한 내용은 XenMobile에서 인증서 업로드를 참조하십시오.

1. **설정**에서 **LDAP**를 클릭합니다.
2. **Microsoft Active Directory**를 선택한 다음 **편집**을 클릭합니다.



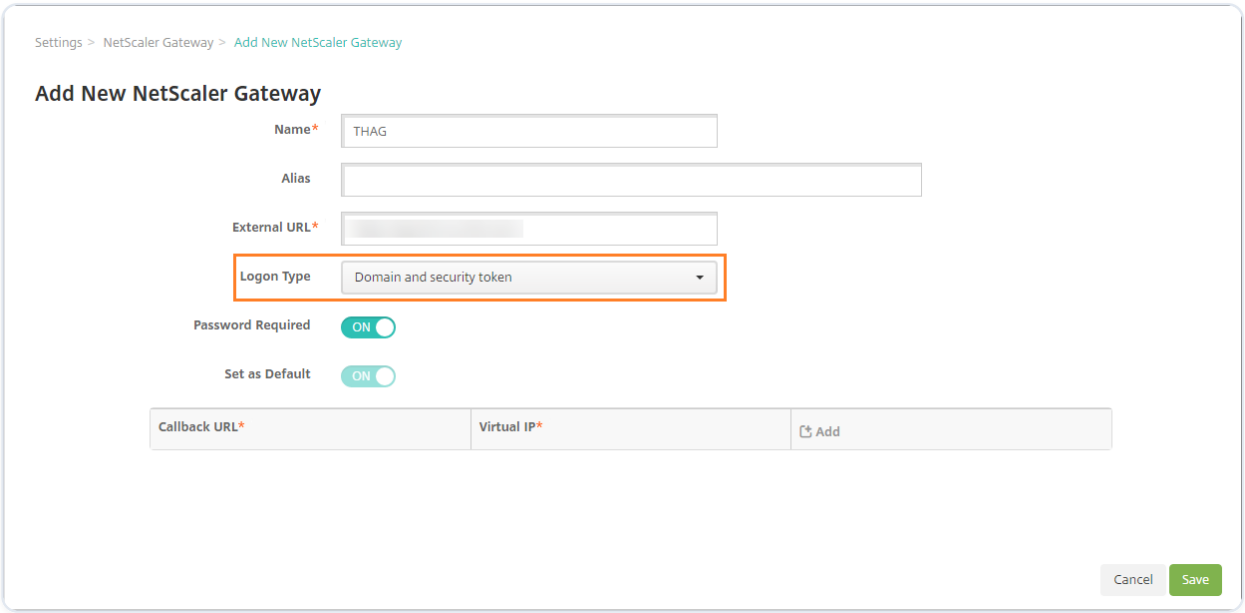
3. 포트가 보안 LDAP 연결용 **636** 또는 Microsoft 보안 LDAP 연결용 **3269**인지 확인합니다.
4. **보안 연결 사용**을 **예**로 변경합니다.



Citrix Gateway 설정 구성

다음 단계는 XenMobile에 Citrix Gateway 인스턴스를 이미 추가했다고 가정합니다. Citrix Gateway 인스턴스를 추가하려면 Citrix Gateway 인스턴스 추가를 참조하십시오.

1. **설정**에서 **Citrix Gateway**를 클릭합니다.
2. **Citrix Gateway**를 선택한 다음 **편집**을 클릭합니다.
3. **로그온 유형**에서 **도메인 및 보안 토큰**을 선택합니다.



Citrix PIN 및 사용자 암호 캐싱 사용

Citrix PIN 및 사용자 암호 캐싱을 사용하려면 **설정 > 클라이언트 속성**으로 이동하여 다음 확인란을 선택합니다. **Citrix PIN 인증 사용** 및 **사용자 암호 캐싱 사용**. 자세한 내용은 클라이언트 속성을 참조하십시오.

도메인 및 보안 토큰 인증을 위한 Citrix Gateway 구성

XenMobile과 함께 사용되는 가상 서버에 대한 Citrix Gateway 세션 프로필 및 정책을 구성합니다. 자세한 내용은 Citrix Gateway 설명서를 참조하십시오.

클라이언트 인증서 또는 인증서와 도메인 인증

XenMobile®의 기본 구성은 사용자 이름 및 암호 인증입니다. XenMobile 환경에 대한 등록 및 액세스에 보안 계층을 추가하려면 인증서 기반 인증 사용을 고려하십시오. XenMobile 환경에서 이 구성은 보안과 사용자 경험의 최상의 조합입니다. 인증서와 도메인 인증은 Citrix ADC에서 제공하는 2단계 인증과 결합된 최상의 SSO 가능성을 제공합니다.

최적의 유용성을 위해 인증서와 도메인 인증을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다. 결과적으로 사용자는 LDAP 사용자 이름과 암호를 반복해서 입력할 필요가 없습니다. 사용자는 등록, 암호 만료 및 계정 잠금에 대한 사용자 이름과 암호를 입력합니다.

중요:

XenMobile은 사용자가 XenMobile에 장치를 등록한 후 인증 모드를 도메인 인증에서 다른 인증 모드로 변경하는 것을 지원하지 않습니다.

LDAP를 허용하지 않고 스마트 카드 또는 유사한 방법을 사용하는 경우, 인증서를 구성하면 스마트 카드를 XenMobile에 나타낼 수 있습니다. 그러면 사용자는 XenMobile이 생성하는 고유한 PIN을 사용하여 등록합니다. 사용자가 액세스 권한을 얻으면 XenMobile은 XenMobile 환경에 인증하는 데 사용되는 인증서를 생성하고 배포합니다.

Citrix ADC 전용 인증 또는 인증서와 도메인 인증을 사용할 때 XenMobile에 필요한 구성을 수행하려면 Citrix ADC for XenMobile 마법사를 사용할 수 있습니다. Citrix ADC for XenMobile 마법사는 한 번만 실행할 수 있습니다.

보안 수준이 높은 환경에서는 공용 또는 안전하지 않은 네트워크에서 조직 외부의 LDAP 자격 증명 사용이 조직에 대한 주요 보안 위협으로 간주됩니다. 보안 수준이 높은 환경의 경우 클라이언트 인증서와 보안 토큰을 사용하는 2단계 인증이 옵션입니다. 자세한 내용은 인증서 및 보안 토큰 인증을 위한 XenMobile 구성을 참조하십시오.

클라이언트 인증서 인증은 XenMobile MAM 모드(MAM 전용) 및 ENT 모드(사용자가 MDM에 등록할 때)에서 사용할 수 있습니다. 클라이언트 인증서 인증은 사용자가 레거시 MAM 모드에 등록할 때 XenMobile ENT 모드에서는 사용할 수 없습니다. XenMobile ENT 및 MAM 모드에서 클라이언트 인증서 인증을 사용하려면 Microsoft 서버, XenMobile Server 및 Citrix Gateway를 구성해야 합니다. 이 문서에 설명된 일반적인 단계를 따르십시오.

Microsoft 서버에서:

1. Microsoft Management Console에 인증서 스냅인을 추가합니다.
2. 템플릿을 CA(인증 기관)에 추가합니다.
3. CA 서버에서 PFX 인증서를 생성합니다.

XenMobile Server에서:

1. 인증서를 XenMobile에 업로드합니다.
2. 인증서 기반 인증을 위한 PKI 엔터티를 생성합니다.

3. 자격 증명 공급자를 구성합니다.
4. 인증을 위해 사용자 인증서를 전달하도록 Citrix Gateway를 구성합니다.

Citrix Gateway 구성에 대한 자세한 내용은 Citrix ADC 설명서의 다음 문서를 참조하십시오.

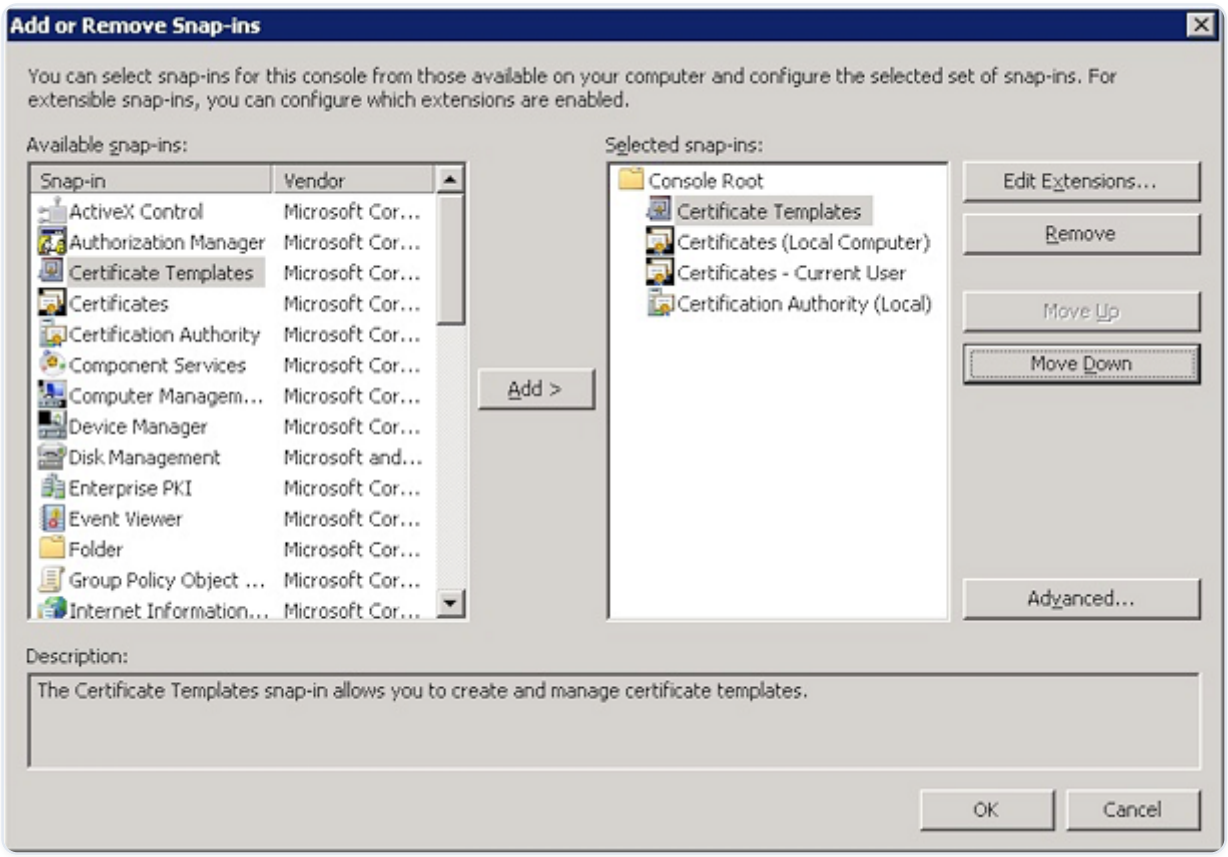
- 클라이언트 인증
- SSL 프로필 인프라
- 클라이언트 인증서 인증 정책 구성 및 바인딩

전제 조건

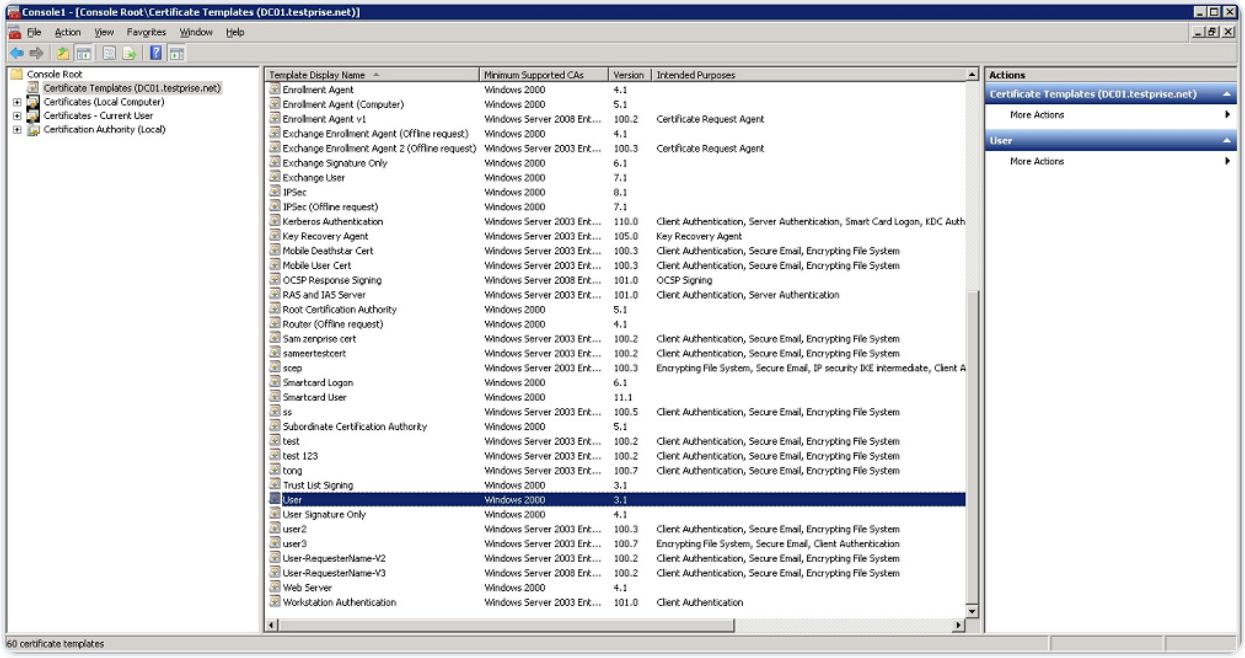
- Microsoft Certificate Services 엔터티 템플릿을 만들 때 특수 문자를 제외하여 등록된 장치에서 발생할 수 있는 인증 문제를 방지하십시오. 예를 들어, 템플릿 이름에 다음 문자를 사용하지 마십시오: `: ! $ () # % + * ~ ? | {} []`
- Exchange ActiveSync용 인증서 기반 인증을 구성하려면 이 Microsoft 블로그를 참조하십시오. Exchange ActiveSync용 인증 기관(CA) 서버 사이트에서 클라이언트 인증서를 요구하도록 구성하십시오.
- Exchange Server로의 ActiveSync 트래픽을 보호하기 위해 개인 서버 인증서를 사용하는 경우, 모바일 장치에 필요한 모든 루트/중간 인증서가 있는지 확인하십시오. 그렇지 않으면 Secure Mail에서 사서함 설정 중에 인증서 기반 인증이 실패합니다. Exchange IIS 콘솔에서 다음을 수행해야 합니다.
  - Exchange와 함께 XenMobile을 사용하기 위한 웹사이트를 추가하고 웹 서버 인증서를 바인딩합니다.
  - 포트 9443을 사용합니다.
  - 해당 웹사이트에 "Microsoft-Server-ActiveSync"용 애플리케이션 하나와 "EWS"용 애플리케이션 하나, 총 두 개의 애플리케이션을 추가해야 합니다. 두 애플리케이션 모두 **SSL 설정**에서 **SSL 필요**를 선택합니다.

Microsoft Management Console에 인증서 스냅인 추가

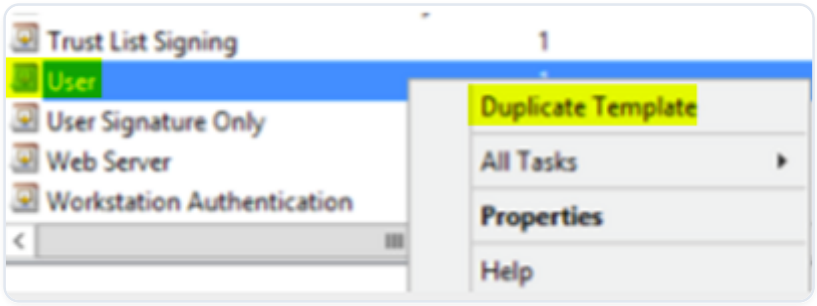
1. 콘솔을 열고 **스냅인 추가/제거**를 클릭합니다.
2. 다음 스냅인을 추가합니다.
   - 인증서 템플릿
   - 인증서 (로컬 컴퓨터)
   - 인증서 - 현재 사용자
   - 인증 기관 (로컬)



3. **인증서 템플릿**을 확장합니다.



4. **사용자** 템플릿을 선택하고 **템플릿 복제**를 선택합니다.



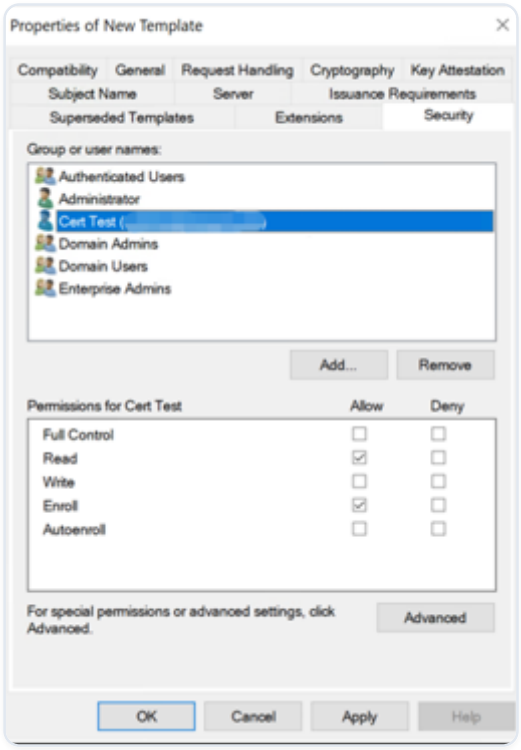
5. 템플릿 표시 이름을 제공합니다.

> **중요:**
>
> Active Directory에서 **인증서 게시** 옵션을 선택하는 것은 권장되지 않습니다. 이 옵션을 선택하면 Active Directory의 모든 사용자에 대한 클라이언트 인증서가 생성되어 Active Directory 데이터베이스가 복잡해질 수 있습니다.

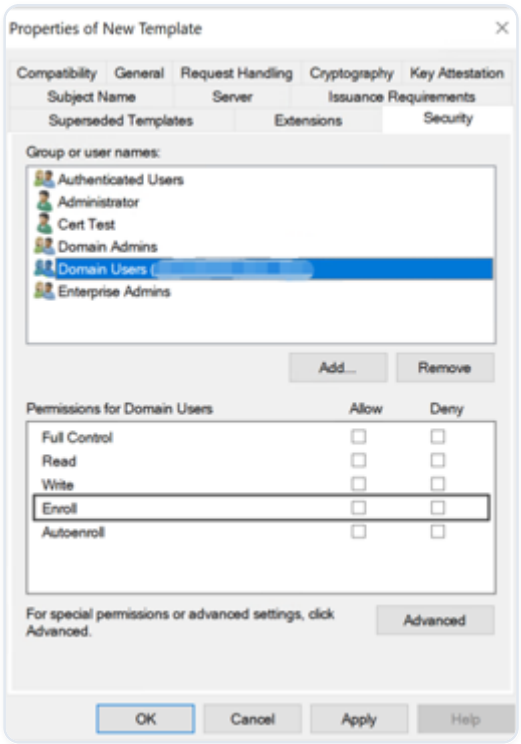
6. 템플릿 유형으로 **Windows 2003 Server**를 선택합니다. Windows 2012 R2 서버에서는 **호환성** 아래에서 **인증 기관**을 선택하고 수신자를 **Windows 2003**으로 설정합니다.
7. **보안** 아래에서 다음을 구성합니다:

   a. **추가**를 클릭한 다음 XenMobile Server가 인증서를 생성하는 데 사용하는 AD 사용자 계정을 선택합니다.

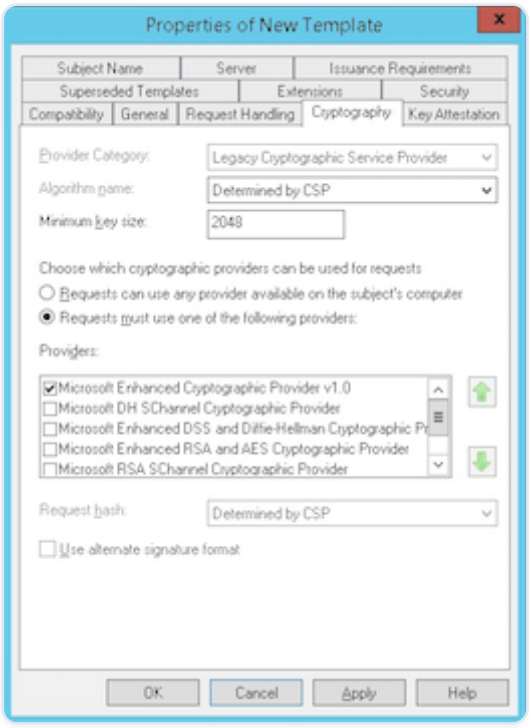
   > **중요:**
   >
   > 여기에 서비스 계정 사용자만 추가합니다. **등록** 권한은 이 AD 사용자 계정에만 추가합니다.
   >
   > 이 문서의 뒷부분에서 설명하는 것처럼 서비스 계정을 사용하여 사용자 .pfx 인증서를 생성합니다. 자세한 내용은 CA 서버에서 PFX 인증서 생성을 참조하십시오.



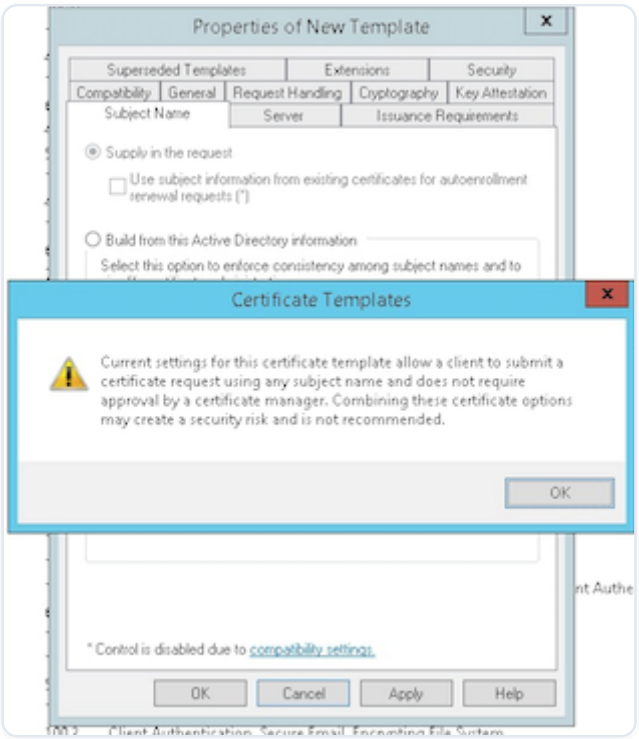
b. **도메인 사용자**에서 **등록** 권한을 취소합니다.



8. **암호화** 아래에서 키 크기를 제공했는지 확인합니다. 나중에 XenMobile을 구성할 때 키 크기를 입력합니다.

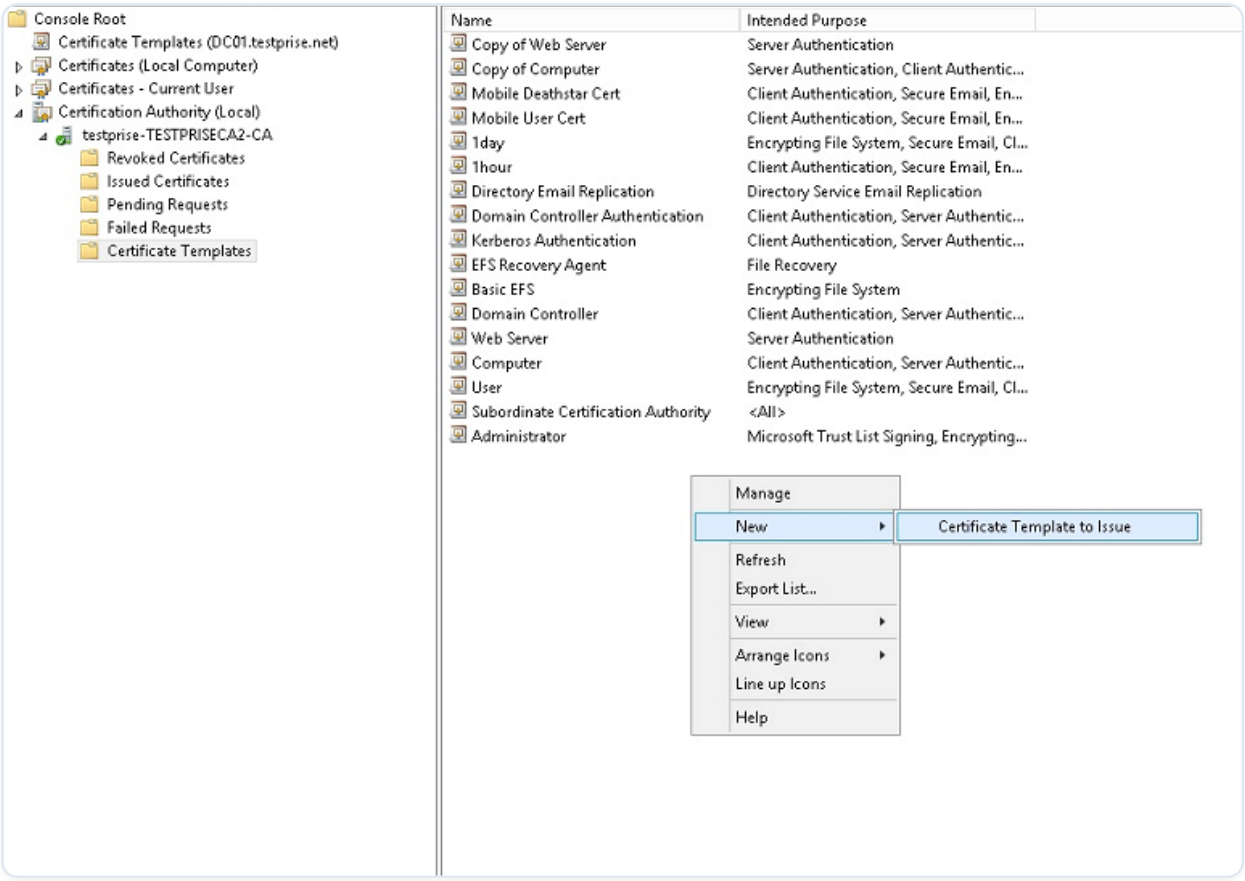


9. **주체 이름** 아래에서 **요청 시 제공**을 선택합니다. 변경 사항을 적용한 다음 저장합니다.

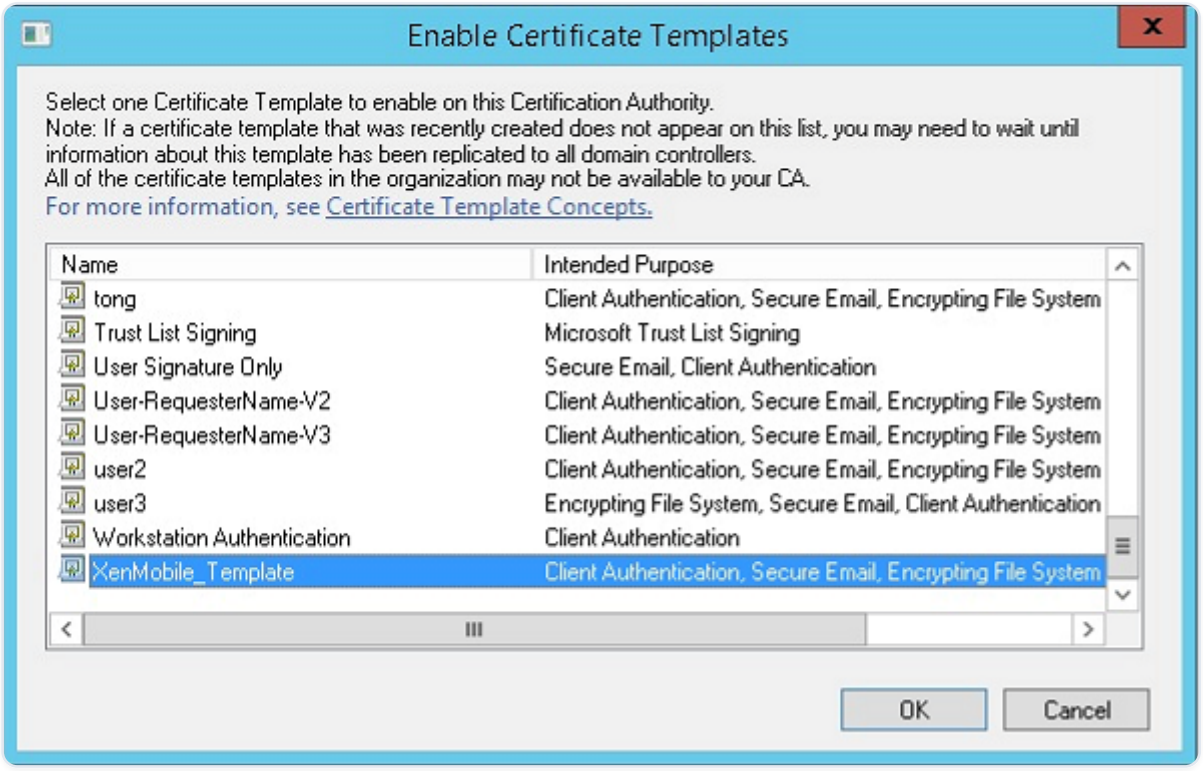


인증 기관에 템플릿 추가

1. **인증 기관**으로 이동하여 **인증서 템플릿**을 선택합니다.
2. 오른쪽 창에서 마우스 오른쪽 버튼을 클릭한 다음 **새로 만들기 > 발급할 인증서 템플릿**을 선택합니다.

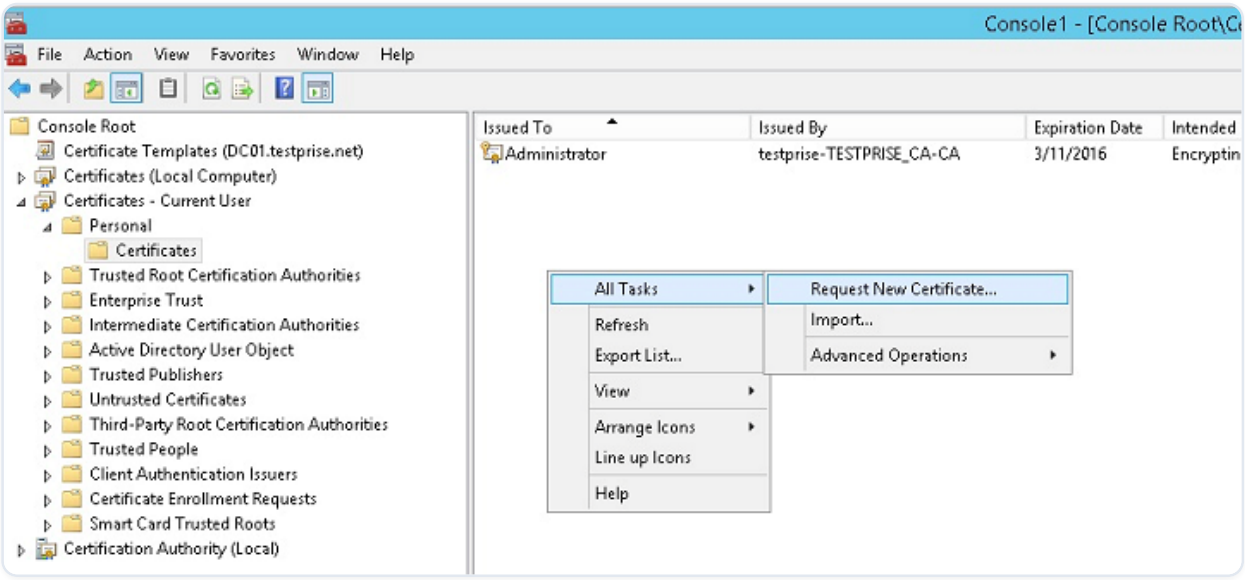


3. 이전 단계에서 생성한 템플릿을 선택한 다음 **확인**을 클릭하여 **인증 기관**에 추가합니다.

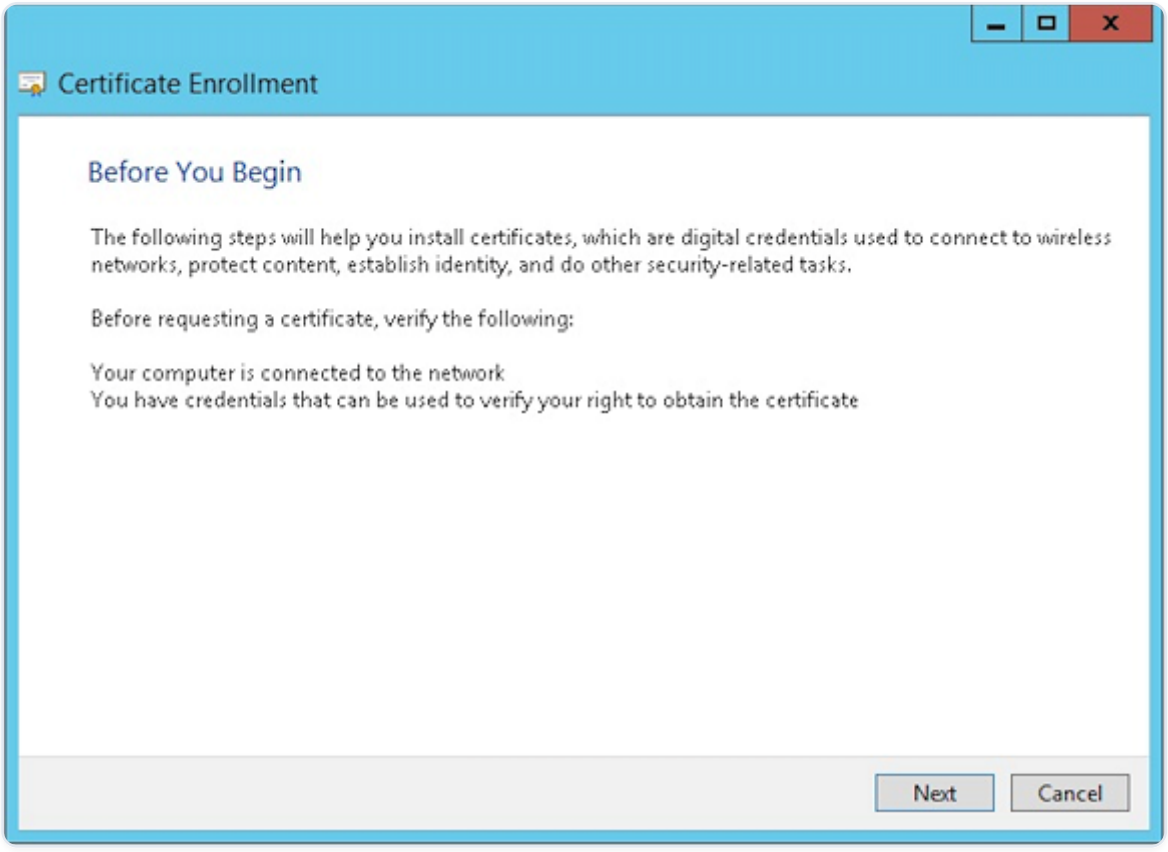


CA 서버에서 PFX 인증서 생성

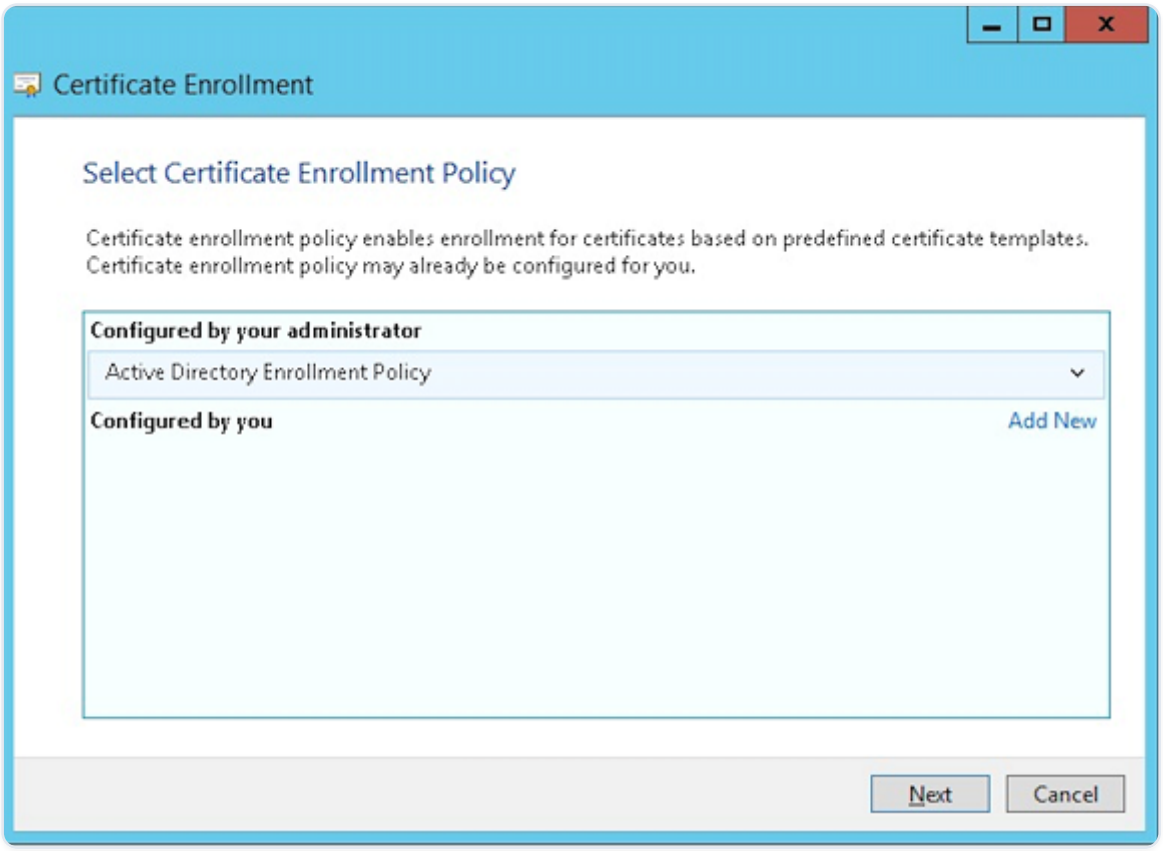
1. 로그인한 서비스 계정을 사용하여 사용자 .pfx 인증서를 생성합니다. 이 .pfx는 XenMobile에 업로드되며, XenMobile은 장치를 등록하는 사용자를 대신하여 사용자 인증서를 요청합니다.
2. **현재 사용자** 아래에서 **인증서**를 확장합니다.
3. 오른쪽 창에서 마우스 오른쪽 버튼을 클릭한 다음 **새 인증서 요청**을 클릭합니다.



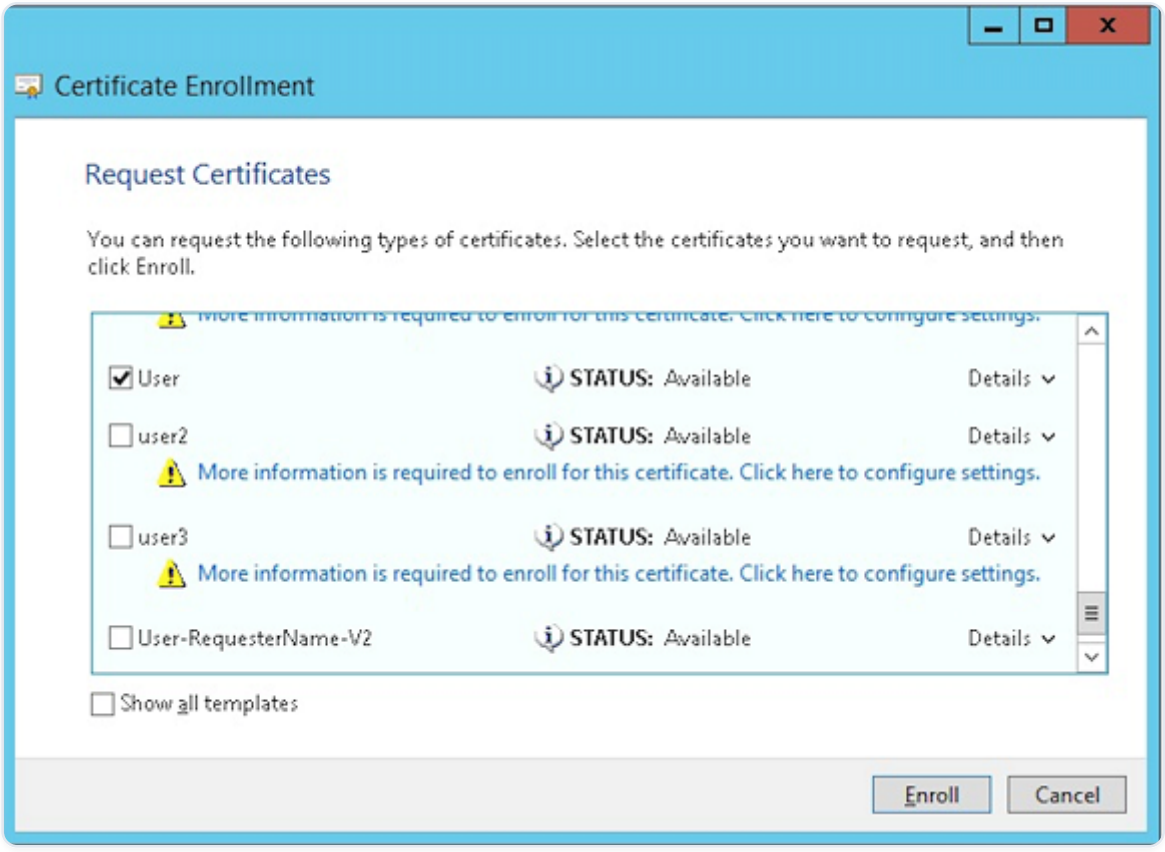
4. **인증서 등록** 화면이 나타납니다. **다음**을 클릭합니다.



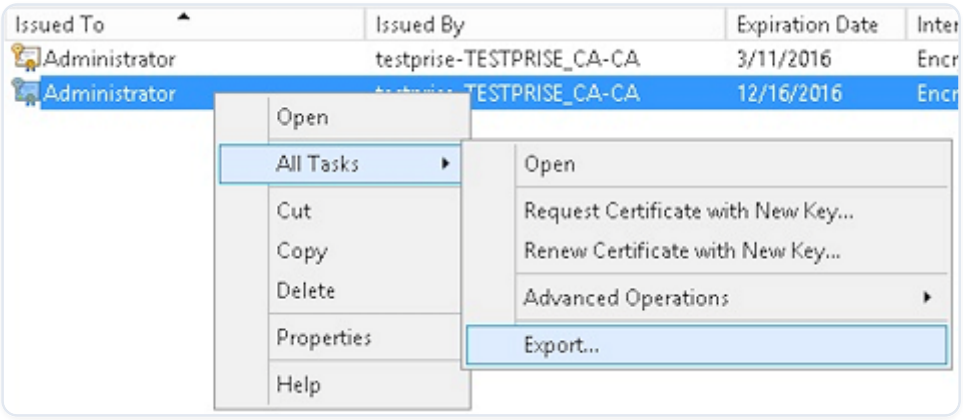
5. **Active Directory 등록 정책**을 선택한 다음 **다음**을 클릭합니다.



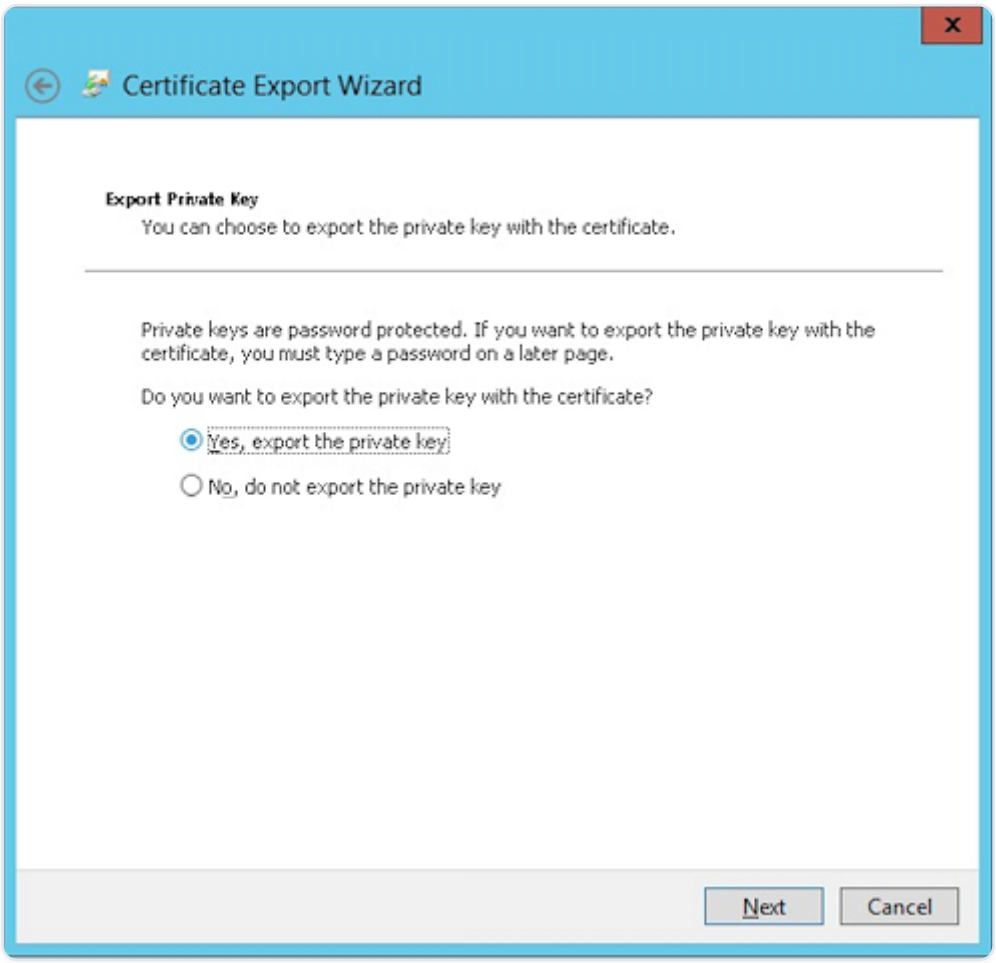
6. **사용자** 템플릿을 선택한 다음 **등록**을 클릭합니다.



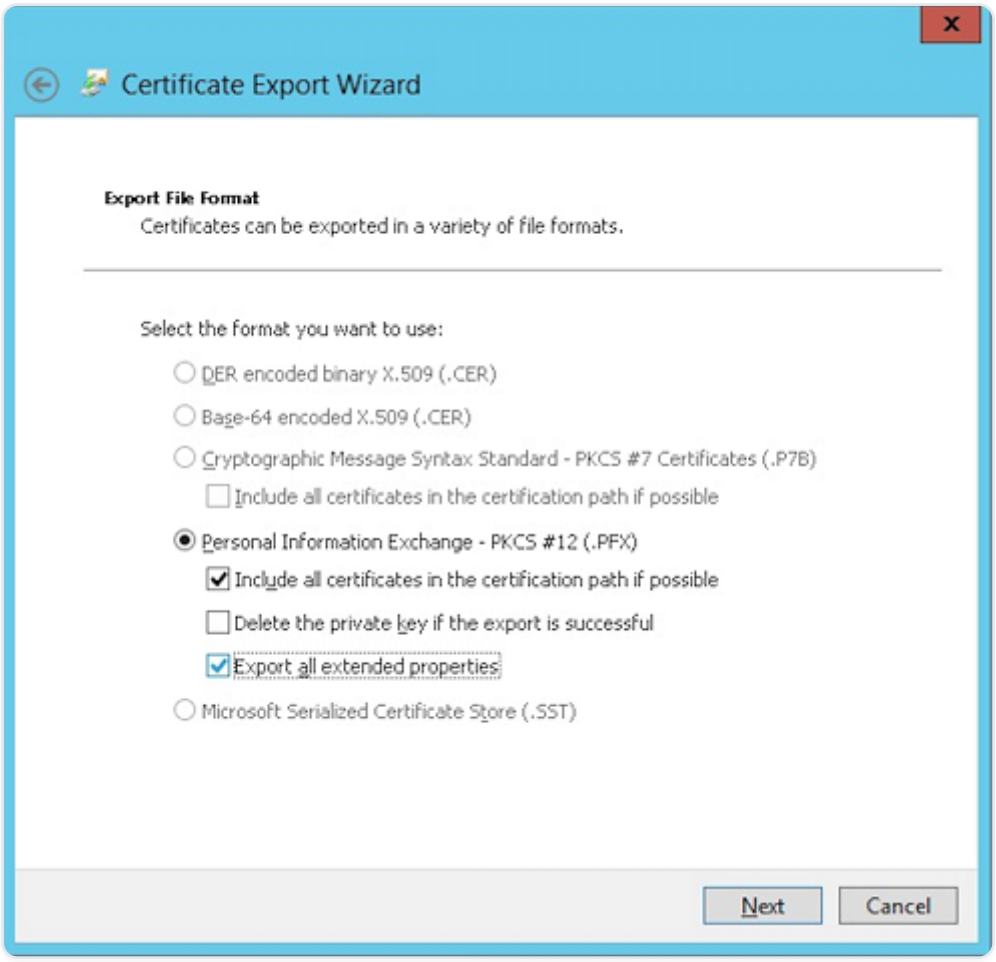
7. 이전 단계에서 생성한 .pfx 파일을 내보냅니다.



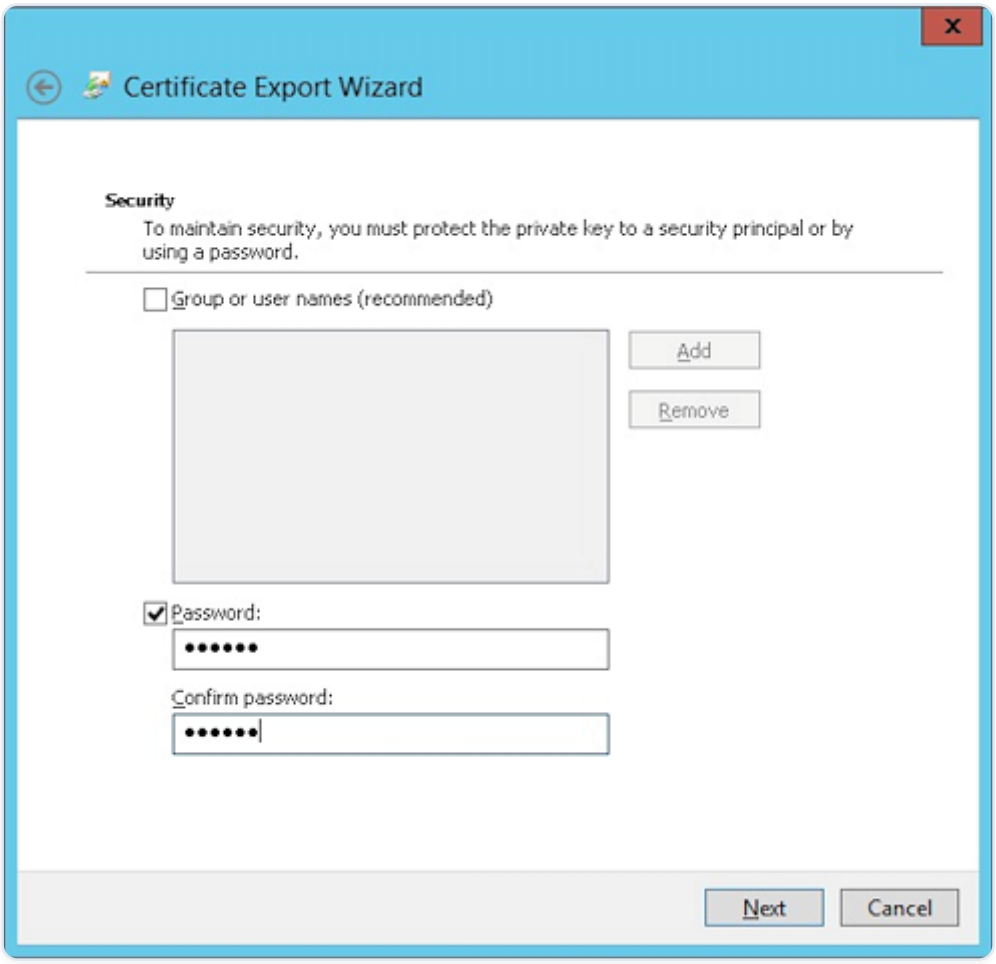
8. **예, 개인 키를 내보냅니다.**를 클릭합니다.



9. **가능하면 인증 경로에 있는 모든 인증서 포함**을(를) 선택하고 **모든 확장 속성 내보내기** 확인란을 선택합니다.



10. 이 인증서를 XenMobile에 업로드할 때 사용할 암호를 설정합니다.

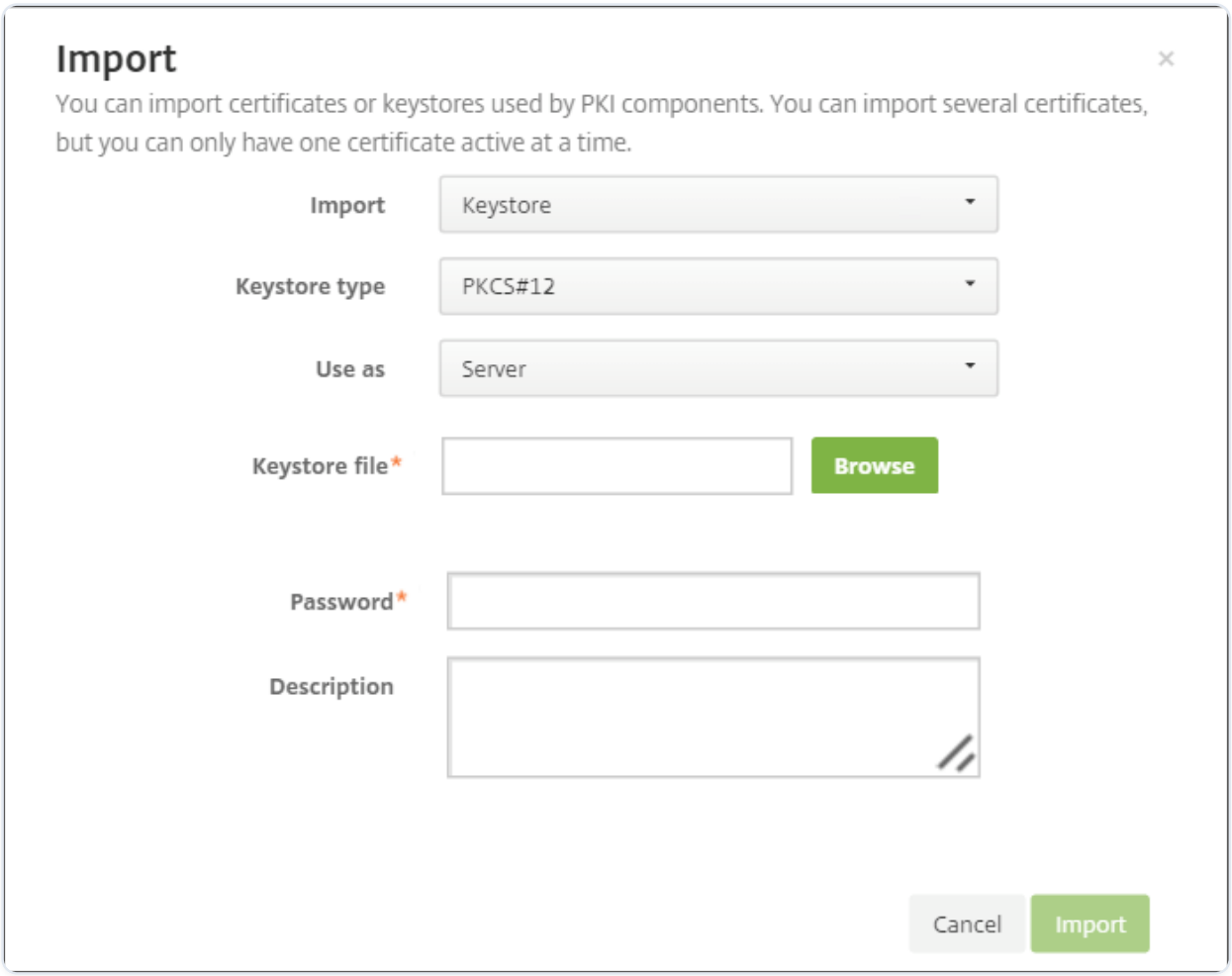


11. 인증서를 하드 드라이브에 저장합니다.

XenMobile에 인증서 업로드

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 화면이 나타납니다.
2. **인증서**를 클릭한 다음 **가져오기**를 클릭합니다.
3. 다음 매개변수를 입력합니다.

    - **가져오기:** 키 저장소
    - **키 저장소 유형:** PKCS #12
    - **용도:** 서버
    - **키 저장소 파일: 찾아보기**를 클릭하여 생성한 `.pfx` 인증서를 선택합니다.
    - **암호:** 이 인증서에 대해 생성한 암호를 입력합니다.



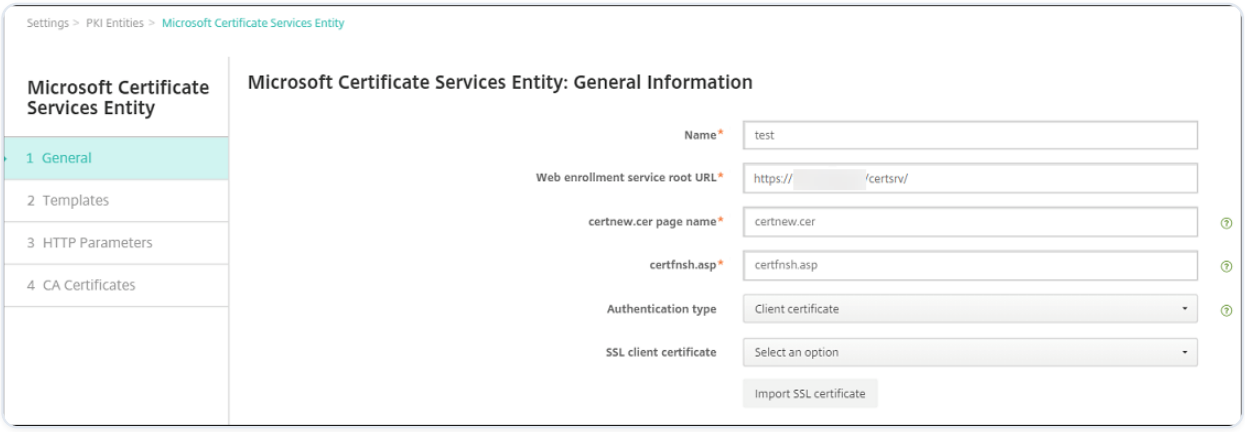
4. **가져오기**를 클릭합니다.
5. 인증서가 올바르게 설치되었는지 확인합니다. 올바르게 설치된 인증서는 사용자 인증서로 표시됩니다.

인증서 기반 인증을 위한 PKI 엔터티 생성

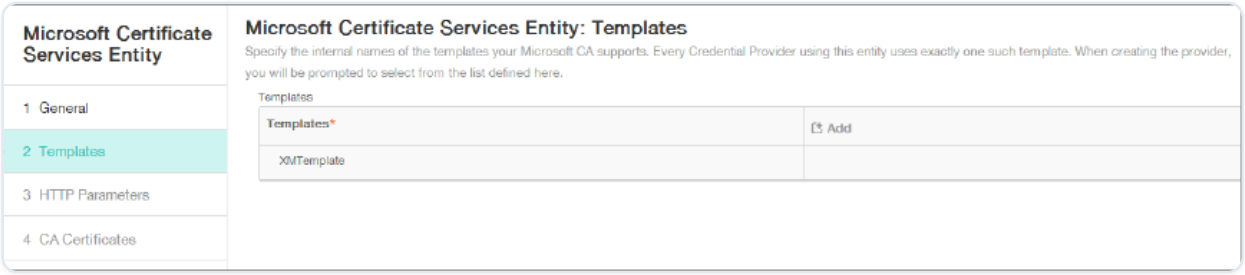
1. **설정**에서 **자세히 > 인증서 관리 > PKI 엔터티**로 이동합니다.
2. **추가**를 클릭한 다음 **Microsoft 인증서 서비스 엔터티**를 클릭합니다. **Microsoft 인증서 서비스 엔터티: 일반 정보** 화면이 나타납니다.
3. 다음 매개변수를 입력합니다.

   - **이름:** 아무 이름이나 입력합니다.
   - **웹 등록 서비스 루트 URL:** `https://RootCA-URL/certsrv/` (URL 경로에 마지막 슬래시(/)를 추가해야 합니다.)
   - **certnew.cer 페이지 이름:** certnew.cer (기본값)
   - **certfnsh.asp:** certfnsh.asp (기본값)
   - **인증 유형:** 클라이언트 인증서

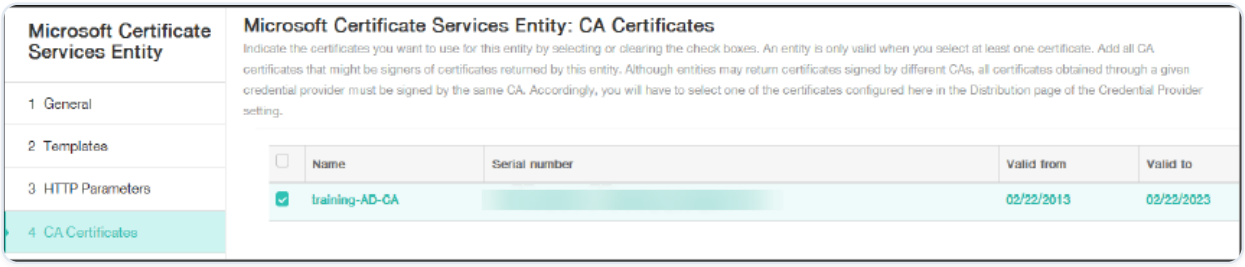
- **SSL 클라이언트 인증서:** XenMobile 클라이언트 인증서를 발급하는 데 사용할 사용자 인증서를 선택합니다.



4. **템플릿**에서 Microsoft 인증서를 구성할 때 생성한 템플릿을 추가합니다. 공백을 추가하지 마십시오.



5. HTTP 매개변수를 건너뛰고 **CA 인증서**를 클릭합니다.
6. 환경에 해당하는 루트 CA 이름을 선택합니다. 이 루트 CA는 XenMobile 클라이언트 인증서에서 가져온 체인의 일부입니다.



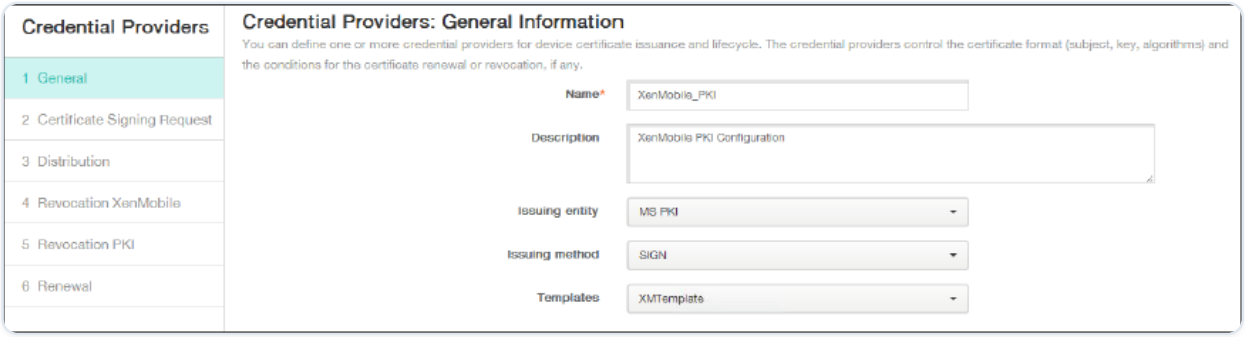
7. **저장**을 클릭합니다.

자격 증명 공급자 구성

1. **설정**에서 **자세히 > 인증서 관리 > 자격 증명 공급자**로 이동합니다.
2. **추가**를 클릭합니다.
3. **일반**에서 다음 매개변수를 입력합니다.

- **이름:** 아무 이름이나 입력합니다.
- **설명:** 아무 설명이나 입력합니다.

- **발급 엔터티:** 이전에 생성한 PKI 엔터티를 선택합니다.
- **발급 방법:** SIGN
- **템플릿:** PKI 엔터티에 추가된 템플릿을 선택합니다.

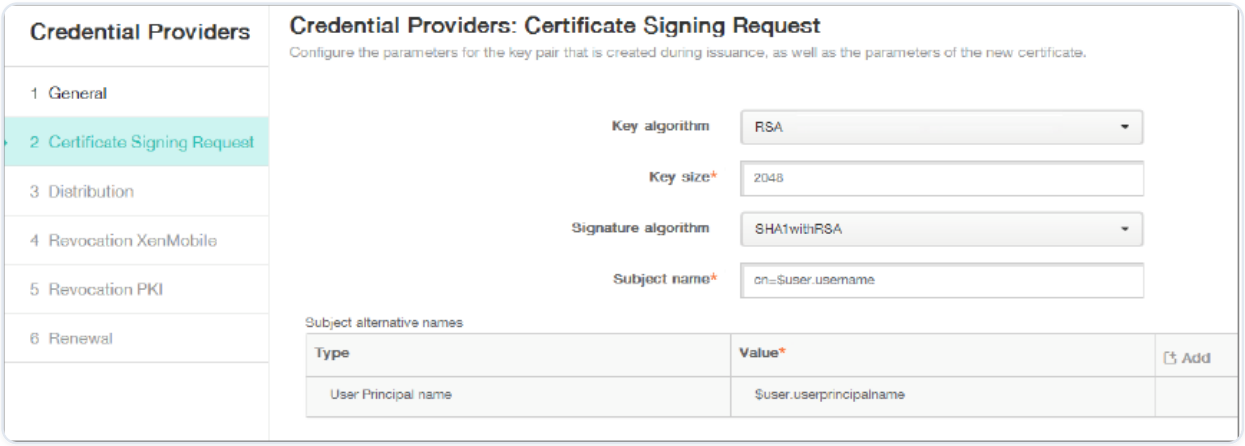


4. **인증서 서명 요청**을 클릭한 다음 다음 매개변수를 입력합니다.

   - **키 알고리즘:** RSA
   - **키 크기:** 2048
   - **서명 알고리즘:** SHA256withRSA
   - **주체 이름:** `cn=$user.username`

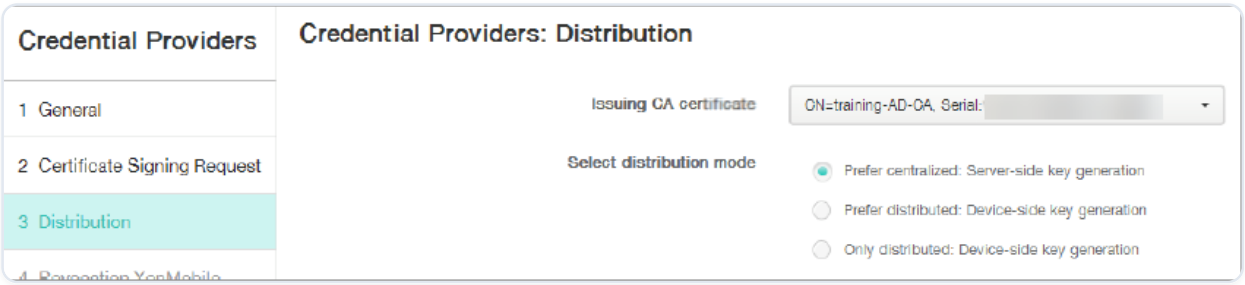
   주체 대체 이름의 경우 **추가**를 클릭한 다음 다음 매개변수를 입력합니다.

   - **유형:** 사용자 주체 이름
   - **값:** `$user.userprincipalname`

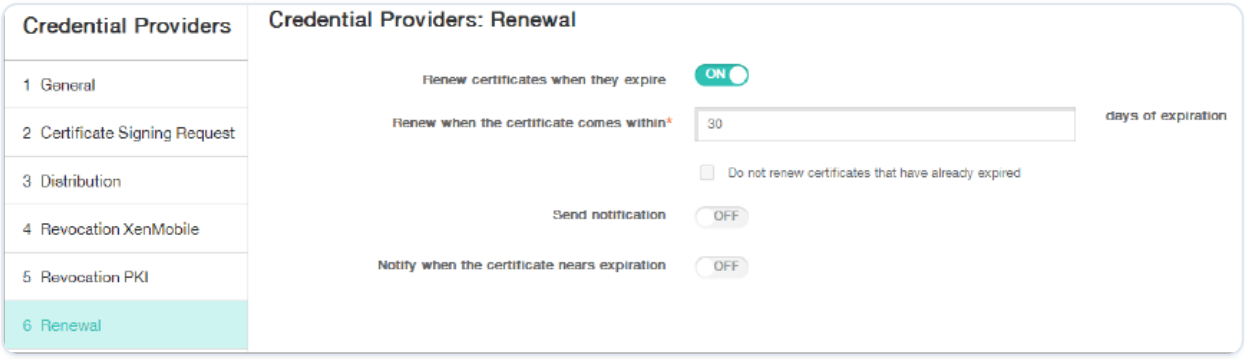


5. **배포**를 클릭하고 다음 매개변수를 입력합니다.

   - **발급 CA 인증서:** XenMobile 클라이언트 인증서에 서명한 발급 CA를 선택합니다.
   - **배포 모드 선택: 중앙 집중식 선호: 서버 측 키 생성**을 선택합니다.



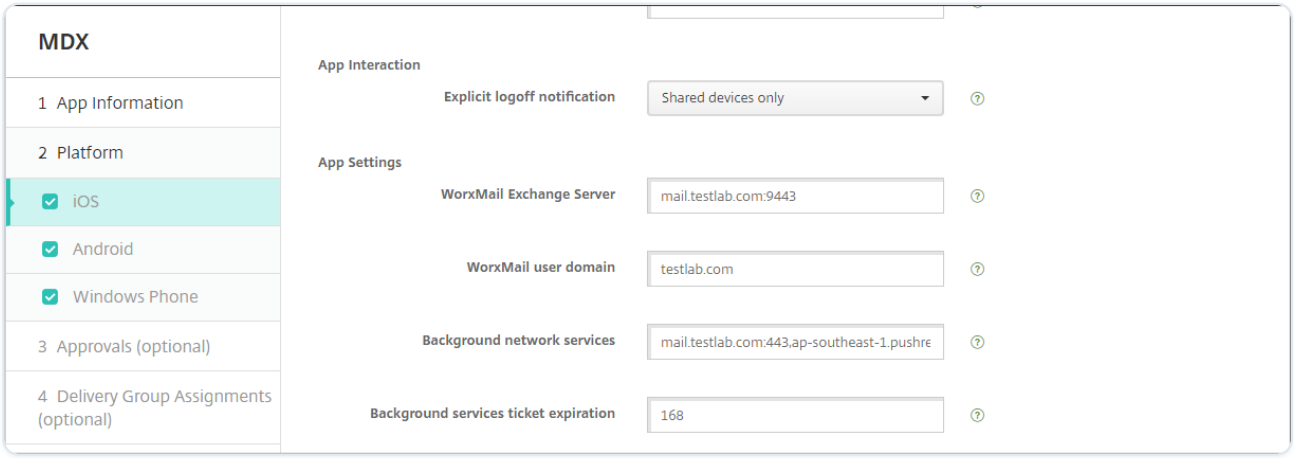
6. 다음 두 섹션인 **Revocation XenMobile** 및 **Revocation PKI**에 대해 필요에 따라 매개변수를 설정합니다. 이 예에서는 두 옵션 모두 건너뜁니다.
7. **갱신**을 클릭합니다.
8. **인증서 만료 시 갱신**에서 **켜기**를 선택합니다.
9. 다른 모든 설정은 기본값으로 두거나 필요에 따라 변경합니다.



10. **저장**을 클릭합니다.

인증서 기반 인증을 사용하도록 Secure Mail 구성

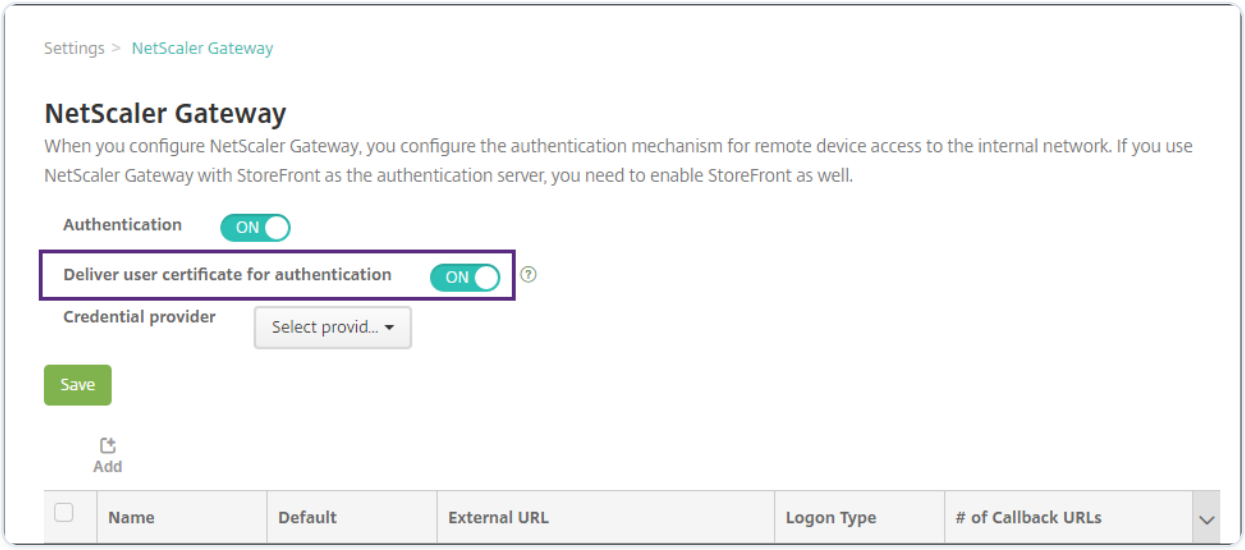
Secure Mail을 XenMobile에 추가할 때 **앱 설정**에서 Exchange 설정을 구성해야 합니다.



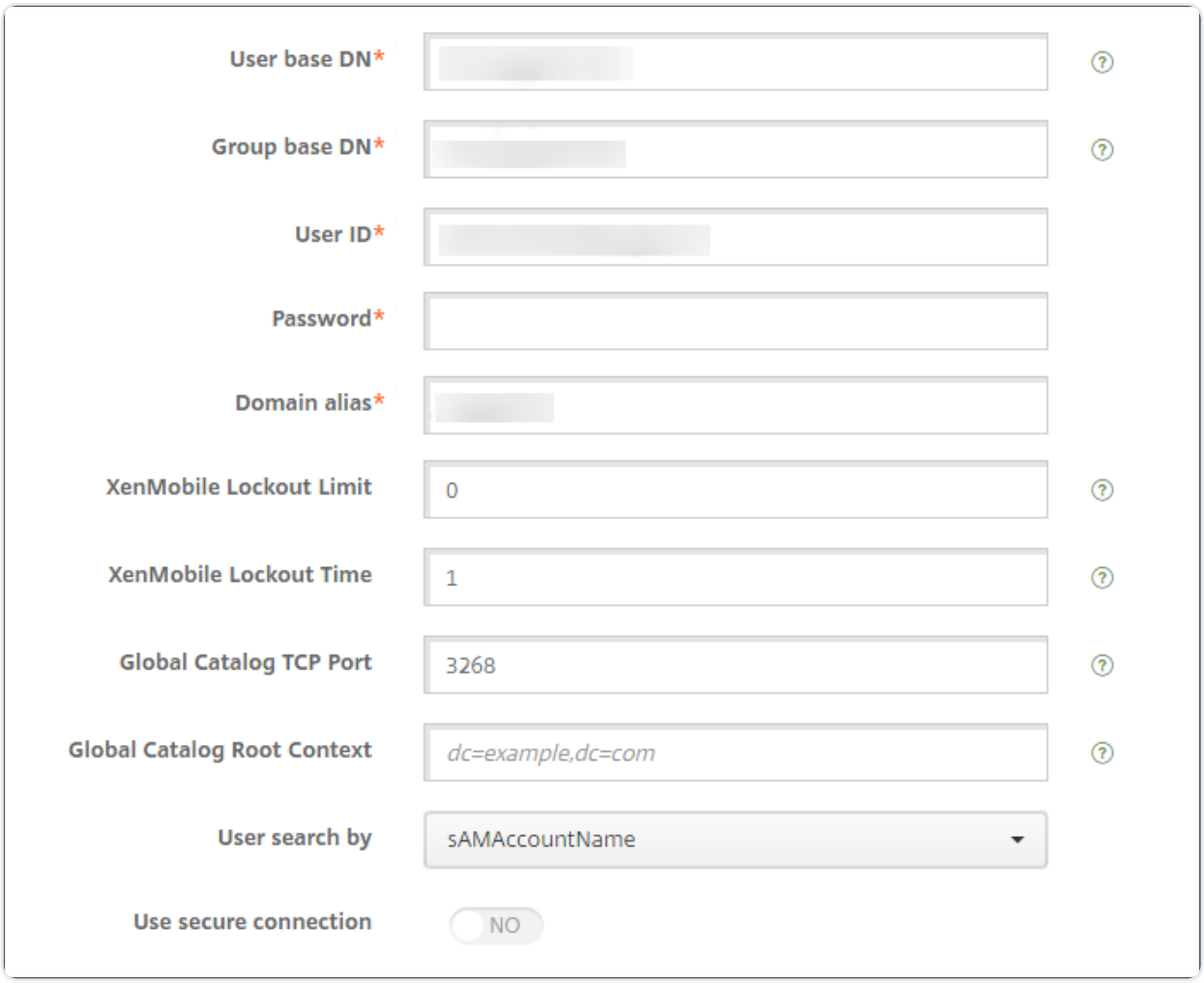
XenMobile에서 Citrix ADC 인증서 전송 구성

1. XenMobile 콘솔에 로그온하고 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 화면이 나타납니다.

2. **서버**에서 **Citrix Gateway**를 클릭합니다.
3. Citrix Gateway가 아직 추가되지 않은 경우 **추가**를 클릭하고 설정을 지정합니다.
   - **외부 URL:** `https://YourCitrixGatewayURL`
   - **로그온 유형:** 인증서 및 도메인
   - **암호 필요:** 끄기
   - **기본값으로 설정:** 켜기
4. **인증을 위한 사용자 인증서 전달**에서 **켜기**를 선택합니다.



5. **자격 증명 공급자**에서 공급자를 선택한 다음 **저장**을 클릭합니다.
6. 사용자 인증서의 sAMAccount 특성을 UPN(사용자 계정 이름) 대신 사용하려면 XenMobile에서 LDAP 커넥터를 다음과 같이 구성합니다. **설정 > LDAP**으로 이동하여 디렉터리를 선택하고 **편집**을 클릭한 다음 **사용자 검색 기준**에서 **sAMAccountName**을 선택합니다.



Citrix PIN 및 사용자 암호 캐싱 사용

Citrix PIN 및 사용자 암호 캐싱을 사용하려면 **설정 > 클라이언트 속성**으로 이동하여 **Citrix PIN 인증 사용** 및 **사용자 암호 캐싱 사용** 확인란을 선택합니다. 자세한 내용은 클라이언트 속성을 참조하십시오.

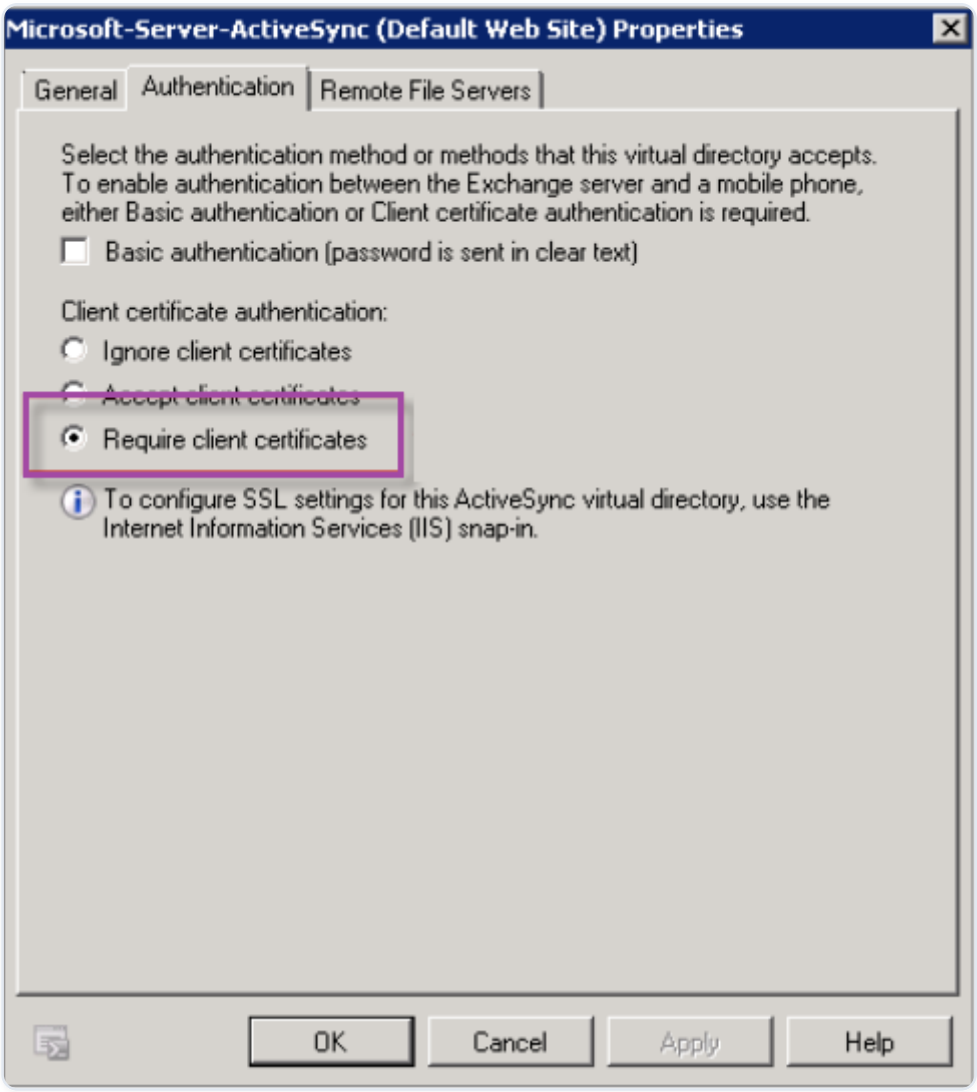
클라이언트 인증서 구성 문제 해결

이전 구성과 Citrix Gateway 구성이 성공적으로 완료되면 사용자 워크플로는 다음과 같습니다.

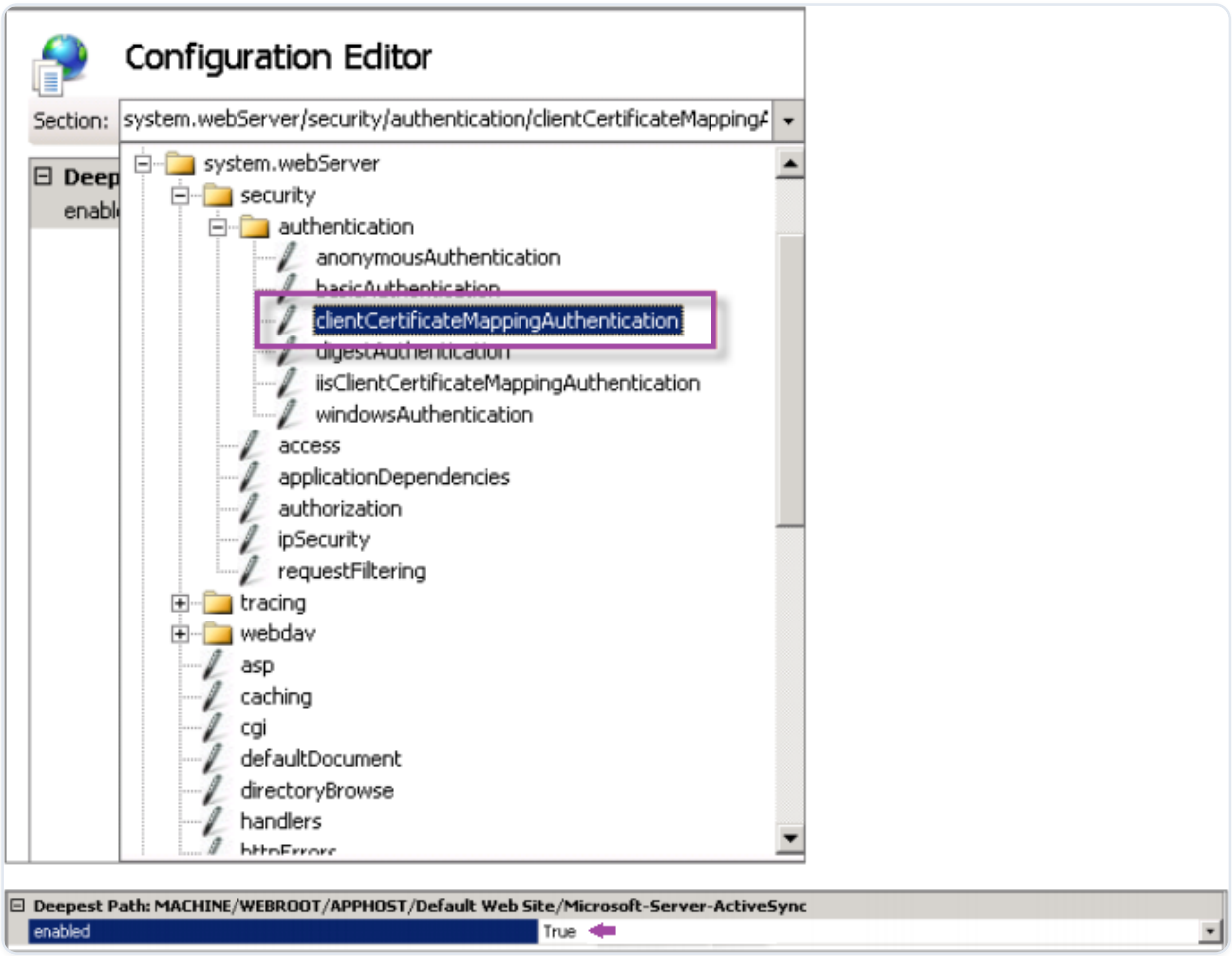
1. 사용자가 모바일 장치를 등록합니다.
2. XenMobile에서 사용자에게 Citrix PIN을 생성하라는 메시지를 표시합니다.
3. 그러면 사용자가 XenMobile Store로 리디렉션됩니다.
4. 사용자가 Secure Mail을 시작할 때 XenMobile은 사서함 구성을 위한 사용자 자격 증명을 요청하지 않습니다. 대신 Secure Mail은 Secure Hub에서 클라이언트 인증서를 요청하고 인증을 위해 Microsoft Exchange Server에 제출합니다. 사용자가 Secure Mail을 시작할 때 XenMobile에서 자격 증명을 요청하는 경우 구성을 확인하십시오.

사용자가 Secure Mail을 다운로드하여 설치할 수 있지만, 사서함 구성 중에 Secure Mail이 구성을 완료하지 못하는 경우:

1. Microsoft Exchange Server ActiveSync가 트래픽을 보호하기 위해 개인 SSL 서버 인증서를 사용하는 경우, 루트/중간 인증서가 모바일 장치에 설치되어 있는지 확인하십시오.
2. ActiveSync에 대해 선택된 인증 유형이 **클라이언트 인증서 필요**인지 확인하십시오.



3. Microsoft Exchange Server에서 **Microsoft-Server-ActiveSync** 사이트를 확인하여 클라이언트 인증서 매핑 인증이 활성화되어 있는지 확인하십시오. 기본적으로 클라이언트 인증서 매핑 인증은 비활성화되어 있습니다. 이 옵션은 **구성 편집기 > 보안 > 인증** 아래에 있습니다.



True를 선택한 후, 변경 사항을 적용하려면 반드시 **적용**을 클릭하십시오.

4. XenMobile 콘솔에서 Citrix Gateway 설정을 확인하십시오. **인증을 위한 사용자 인증서 전달**이 **켜짐**으로 설정되어 있고 **자격 증명 공급자**에 올바른 프로필이 선택되어 있는지 확인하십시오.

클라이언트 인증서가 모바일 장치로 전달되었는지 확인하는 방법

1. XenMobile 콘솔에서 **관리 > 장치**로 이동하여 장치를 선택하십시오.
2. **편집** 또는 **자세히 보기**를 클릭하십시오.
3. **전달 그룹** 섹션으로 이동하여 다음 항목을 검색하십시오.

   Citrix Gateway 자격 증명: 요청된 자격 증명, CertId=

클라이언트 인증서 협상이 활성화되어 있는지 확인하는 방법

1. IIS 웹사이트에 바인딩된 SSL 인증서 구성을 표시하려면 다음 `netsh` 명령을 실행하십시오.

   ```
   netsh http show sslcert
   ```

2. **클라이언트 인증서 협상(Negotiate Client Certificate)** 값이 **비활성화(Disabled)**인 경우, 다음 명령을 실행하여 활성화하십시오.

   ```
   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`

예시:

`netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable`

PKI 엔터티

XenMobile® 공개 키 인프라(PKI) 엔터티 구성은 실제 PKI 작업(발급, 해지 및 상태 정보)을 수행하는 구성 요소를 나타냅니다. 이러한 구성 요소는 XenMobile 내부에 있거나 외부에 있습니다. 내부 구성 요소는 재량적이라고 합니다. 외부 구성 요소는 회사 인프라의 일부입니다.

XenMobile은 다음 유형의 PKI 엔터티를 지원합니다.

- Microsoft 인증서 서비스
- 재량적 인증 기관(CA)

XenMobile은 다음 CA 서버를 지원합니다.

- 윈도우 서버 2019
- 윈도우 서버 2016

> **참고:**
>
> Windows Server 2012 R2, 2012 및 2008 R2는 수명 주기가 종료되어 더 이상 지원되지 않습니다. 자세한 내용은 Microsoft 제품 수명 주기 설명서를 참조하십시오.

일반적인 PKI 개념

유형에 관계없이 모든 PKI 엔터티에는 다음 기능 중 일부가 있습니다.

- **서명:** 인증서 서명 요청(CSR)을 기반으로 새 인증서를 발급합니다.
- **가져오기:** 기존 인증서 및 키 쌍을 복구합니다.
- **해지:** 클라이언트 인증서를 해지합니다.

CA 인증서 정보

PKI 엔터티를 구성할 때 해당 엔터티에서 발급(또는 복구)된 인증서의 서명자가 어떤 CA 인증서인지 XenMobile에 지정합니다. 해당 PKI 엔터티는 여러 다른 CA에서 서명한 인증서(가져오거나 새로 서명한)를 반환할 수 있습니다.

PKI 엔터티 구성의 일부로 각 CA의 인증서를 제공합니다. 이렇게 하려면 XenMobile에 인증서를 업로드한 다음 PKI 엔터티에서 참조합니다. 재량 CA의 경우 인증서는 암시적으로 서명 CA 인증서입니다. 외부 엔터티의 경우 인증서를 수동으로 지정해야 합니다.

> **중요:**
>
> Microsoft Certificate Services 엔터티 템플릿을 만들 때 등록된 장치에서 발생할 수 있는 인증 문제를 방지하려면 다음을 수행합니다. 템플릿 이름에 특수 문자를 사용하지 마십시오. 예를 들어, `! : $ ( ) # % + * ~ ? | { } [ ]`을(를) 사용하지 마십시오.

Microsoft 인증서 서비스

XenMobile은 웹 등록 인터페이스를 통해 Microsoft Certificate Services와 연동됩니다. XenMobile은 해당 인터페이스를 통한 새 인증서 발급만 지원합니다. Microsoft CA가 Citrix Gateway 사용자 인증서를 생성하는 경우 Citrix Gateway는 해당 인증서의 갱신 및 해지를 지원합니다.

XenMobile에서 Microsoft CA PKI 엔터티를 만들려면 Certificate Services 웹 인터페이스의 기본 URL을 지정해야 합니다. 원하는 경우 SSL 클라이언트 인증을 사용하여 XenMobile과 Certificate Services 웹 인터페이스 간의 연결을 보호할 수 있습니다.

Microsoft Certificate Services 엔터티 추가

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭한 다음 **PKI 엔터티**를 클릭합니다.
2. **PKI 엔터티** 페이지에서 **추가**를 클릭합니다.

   PKI 엔터티 유형 메뉴가 나타납니다.
3. **Microsoft Certificate Services 엔터티**를 클릭합니다.

Microsoft Certificate Services 엔터티: 일반 정보 페이지가 나타납니다.

4. **Microsoft Certificate Services 엔터티: 일반 정보** 페이지에서 다음 설정을 구성합니다.
   - **이름:** 새 엔터티의 이름을 입력합니다. 이 이름은 나중에 해당 엔터티를 참조하는 데 사용됩니다. 엔터티 이름은 고유해야 합니다.
   - **웹 등록 서비스 루트 URL:** Microsoft CA 웹 등록 서비스의 기본 URL을 입력합니다. 예를 들어, `https://192.0.2.13/certsrv/`입니다. URL은 일반 HTTP 또는 HTTP-over-SSL을 사용할 수 있습니다.
   - **certnew.cer 페이지 이름:** certnew.cer 페이지의 이름입니다. 특별한 이유로 이름을 변경하지 않았다면 기본 이름을 사용하십시오.
   - **certfnsh.asp:** certfnsh.asp 페이지의 이름입니다. 특별한 이유로 이름을 변경하지 않았다면 기본 이름을 사용하십시오.
   - **인증 유형:** 사용할 인증 방법을 선택합니다.
     - **없음**
     - **HTTP 기본:** 연결하는 데 필요한 사용자 이름과 암호를 입력합니다.
     - **클라이언트 인증서:** 올바른 SSL 클라이언트 인증서를 선택합니다.
5. **연결 테스트**를 클릭하여 서버에 액세스할 수 있는지 확인합니다. 액세스할 수 없는 경우, 연결 실패 메시지가 나타납니다. 구성 설정을 확인하십시오.
6. **다음**을 클릭합니다.

   Microsoft 인증서 서비스 엔터티: 템플릿 페이지가 나타납니다. 이 페이지에서 Microsoft CA가 지원하는 템플릿의 내부 이름을 지정합니다. 자격 증명 공급자를 생성할 때 여기에 정의된 목록에서 템플릿을 선택합니다. 이 엔터티를 사용하는 모든 자격 증명 공급자는 정확히 하나의 템플릿을 사용합니다.

   Microsoft 인증서 서비스 템플릿 요구 사항에 대해서는 사용 중인 Microsoft Server 버전의 Microsoft 설명서를 참조하십시오. XenMobile은 인증서에 명시된 인증서 형식 외에는 배포하는 인증서에 대한 요구 사항이 없습니다.
7. **Microsoft 인증서 서비스 엔터티: 템플릿** 페이지에서 **추가**를 클릭하고 템플릿 이름을 입력한 다음 **저장**을 클릭합니다. 추가하려는 각 템플릿에 대해 이 단계를 반복합니다.
8. **다음**을 클릭합니다.

   Microsoft 인증서 서비스 엔터티: HTTP 매개변수 페이지가 나타납니다. 이 페이지에서 XenMobile이 Microsoft 웹 등록 인터페이스에 대한 HTTP 요청에 추가할 사용자 지정 매개변수를 지정합니다. 사용자 지정 매개변수는 CA에서 실행되는 사용자 지정 스크립트에만 유용합니다.

9. **Microsoft Certificate Services Entity: HTTP parameters** 페이지에서 **추가**를 클릭하고 추가할 HTTP 매개변수의 이름과 값을 입력한 다음 **다음**을 클릭합니다.

   Microsoft Certificate Services Entity: CA Certificates 페이지가 나타납니다. 이 페이지에서 이 엔터티를 통해 시스템이 얻는 인증서의 서명자를 XenMobile에 알려야 합니다. CA 인증서가 갱신되면 XenMobile에서 업데이트하십시오. XenMobile은 변경 사항을 엔터티에 투명하게 적용합니다.

10. **Microsoft Certificate Services Entity: CA Certificates** 페이지에서 이 엔터티에 사용할 인증서를 선택합니다.
11. **저장**을 클릭합니다.

    엔터티가 PKI 엔터티 테이블에 나타납니다.

Citrix ADC 인증서 해지 목록(CRL)

XenMobile은 타사 인증 기관에 대해서만 인증서 해지 목록(CRL)을 지원합니다. Microsoft CA가 구성된 경우 XenMobile은 Citrix ADC를 사용하여 해지를 관리합니다.

클라이언트 인증서 기반 인증을 구성할 때 Citrix ADC 인증서 해지 목록(CRL) 설정인 **CRL 자동 새로 고침 사용**을 구성할지 여부를 고려하십시오. 이 단계는 MAM 전용 모드의 장치 사용자가 장치의 기존 인증서를 사용하여 인증할 수 없도록 합니다.

XenMobile은 사용자가 인증서가 해지된 후 사용자 인증서를 생성하는 것을 제한하지 않으므로 새 인증서를 다시 발급합니다. 이 설정은 CRL이 만료된 PKI 엔터티를 확인할 때 PKI 엔터티의 보안을 강화합니다.

재량적 CA

재량적 CA는 XenMobile에 CA 인증서와 관련 개인 키를 제공할 때 생성됩니다. XenMobile은 지정한 매개변수에 따라 인증서 발급, 해지 및 상태 정보를 내부적으로 처리합니다.

재량적 CA를 구성할 때 해당 CA에 대한 OCSP(Online Certificate Status Protocol) 지원을 활성화할 수 있습니다. OCSP 지원을 활성화하는 경우에만 CA는 CA가 발급하는 인증서에 `id-pe-authorityInfoAccess` 확장을 추가합니다. 이 확장은 다음 위치에 있는 XenMobile 내부 OCSP 응답자를 가리킵니다.

`https://<server>/<instance>/ocsp`

OCSP 서비스를 구성할 때 해당 재량적 엔터티에 대한 OCSP 서명 인증서를 지정합니다. CA 인증서 자체를 서명자로 사용할 수 있습니다. CA 개인 키의 불필요한 노출을 피하려면(권장): CA 인증서로 서명된 위임된 OCSP 서명 인증서를 생성하고 다음 확장 `id-kp-OCSPSigning extendedKeyUsage`을 포함합니다.

XenMobile OCSP 응답자 서비스는 기본 OCSP 응답과 요청에서 다음 해싱 알고리즘을 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.

재량적 CA 추가

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭한 다음 **자세히 > PKI 엔터티**를 클릭합니다.
2. **PKI 엔터티** 페이지에서 **추가**를 클릭합니다.

   PKI 엔터티 유형 메뉴가 나타납니다.
3. **재량적 CA**를 클릭합니다.

   재량적 CA: 일반 정보 페이지가 나타납니다.
4. **재량적 CA: 일반 정보** 페이지에서 다음을 수행합니다.

   - **이름:** 재량적 CA에 대한 설명적인 이름을 입력합니다.
   - **인증서 요청에 서명할 CA 인증서:** 재량적 CA가 인증서 요청에 서명하는 데 사용할 인증서를 클릭합니다.

     이 인증서 목록은 XenMobile의 **구성 > 설정 > 인증서**에서 업로드한 개인 키가 있는 CA 인증서에서 생성됩니다.
5. **다음**을 클릭합니다.

   재량적 CA: 매개변수 페이지가 표시됩니다.
6. **재량적 CA: 매개변수** 페이지에서 다음 작업을 수행합니다.

   - **일련 번호 생성기:** 재량적 CA는 발급하는 인증서에 대한 일련 번호를 생성합니다. 이 목록에서 **순차** 또는 **비순차**를 클릭하여 번호가 생성되는 방식을 결정합니다.
   - **다음 일련 번호:** 발급될 다음 번호를 결정할 값을 입력합니다.
   - **인증서 유효 기간:** 인증서가 유효한 일수를 입력합니다.
   - **키 사용:** 재량적 CA에서 발급한 인증서의 목적을 식별하려면 해당 키를 **켜기**로 설정합니다. 설정되면 CA는 해당 목적에 대한 인증서 발급으로 제한됩니다.

- **확장 키 사용:** 매개변수를 더 추가하려면 **추가**를 클릭하고 키 이름을 입력한 다음 **저장**을 클릭합니다.

7. **다음**을 클릭합니다.

   재량적 CA: 배포 페이지가 표시됩니다.

8. **재량적 CA: 배포** 페이지에서 배포 모드를 선택합니다.

   - **중앙 집중식: 서버 측 키 생성**. Citrix는 중앙 집중식 옵션을 권장합니다. 개인 키는 서버에서 생성 및 저장되며 사용자 장치로 배포됩니다.
   - **분산형: 장치 측 키 생성**. 개인 키는 사용자 장치에서 생성됩니다. 이 분산 모드는 SCEP를 사용하며 `keyUsage keyEncryption` 확장이 있는 RA 암호화 인증서와 `keyUsage digitalSignature` 확장이 있는 RA 서명 인증서가 필요합니다. 동일한 인증서를 암호화 및 서명에 모두 사용할 수 있습니다.

9. **다음**을 클릭합니다.

   재량 CA: 온라인 인증서 상태 프로토콜(OCSP) 페이지가 나타납니다.

   재량 CA: 온라인 인증서 상태 프로토콜(OCSP) 페이지에서 다음을 수행합니다.

   - 이 CA에서 서명한 인증서에 `AuthorityInfoAccess` (RFC2459) 확장을 추가하려면 **이 CA에 대한 OCSP 지원 사용**을 **켜기**로 설정합니다. 이 확장은 `https://<server>/<instance>/ocsp`에 있는 CA OCSP 응답자를 가리킵니다.
   - OCSP 지원을 사용하도록 설정한 경우 OCSP 서명 CA 인증서를 선택합니다. 이 인증서 목록은 XenMobile에 업로드한 CA 인증서에서 생성됩니다.

10. **저장**을 클릭합니다.

    재량 CA가 PKI 엔터티 테이블에 나타납니다.

자격 증명 공급자

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 일부이든 독립형이든(즉, 장치에 있는 그대로 푸시되든) 발생합니다.

장치 등록은 인증서 수명 주기를 제한합니다. 즉, XenMobile은 등록의 일부로 일부 인증서를 발급할 수 있지만, 등록 전에 인증서를 발급하지는 않습니다. 또한, 하나의 등록 컨텍스트 내에서 내부 PKI에서 발급된 인증서는 해당 등록이 해지될 때 해지됩니다. 관리 관계가 종료되면 유효한 인증서는 더 이상 남지 않습니다.

하나의 자격 증명 공급자 구성을 여러 곳에서 사용하여 하나의 구성이 동시에 여러 인증서를 관리할 수 있습니다. 이때 통일성은 배포 리소스와 배포에 있습니다. 예를 들어, 자격 증명 공급자 P가 구성 C의 일부로 장치 D에 배포되는 경우: P의 발급 설정은 D에 배포되는 인증서를 결정합니다. 마찬가지로, C가 업데이트될 때 D의 갱신 설정이 적용됩니다. 그리고 C가 삭제되거나 D가 해지될 때 D의 해지 설정도 적용됩니다.

이러한 규칙에 따라 XenMobile의 자격 증명 공급자 구성은 다음을 결정합니다.

- 인증서의 원본.
- 인증서를 얻는 방법: 새 인증서에 서명하거나 기존 인증서 및 키 쌍을 가져오기(복구)합니다.
- 발급 또는 복구 매개 변수. 예를 들어, 키 크기, 키 알고리즘 및 인증서 확장과 같은 CSR(인증서 서명 요청) 매개 변수.
- 인증서가 장치로 전달되는 방식.
- 해지 조건. 관리 관계가 단절되면 XenMobile의 모든 인증서가 해지되지만, 구성에서 더 이른 해지를 지정할 수 있습니다. 예를 들어, 구성은 연결된 장치 구성이 삭제될 때 인증서를 해지하도록 지정할 수 있습니다. 또한, 특정 조건에서는 XenMobile에서 연결된 인증서의 해지가 백엔드 PKI(공개 키 인프라)로 전송될 수 있습니다. 즉, XenMobile의 인증서 해지는 PKI에서 인증서 해지를 유발할 수 있습니다.
- 갱신 설정. 특정 자격 증명 공급자를 통해 얻은 인증서는 만료가 가까워지면 자동으로 갱신될 수 있습니다. 또는 해당 상황과 별개로, 만료가 다가올 때 알림이 발행될 수 있습니다.

구성 옵션의 가용성은 주로 자격 증명 공급자에 대해 선택하는 PKI 엔터티 유형 및 발급 방법에 따라 달라집니다.

인증서 발급 방법

서명을 통해 인증서를 얻을 수 있으며, 이를 서명 발급 방법이라고 합니다.

이 방법은 새 개인 키를 생성하고, CSR을 생성하며, 서명을 위해 CSR을 CA(인증 기관)에 제출하는 과정을 포함합니다. XenMobile은 MS 인증서 서비스 엔터티와 재량적 CA 엔터티 모두에 대해 서명 방법을 지원합니다.

자격 증명 공급자는 발급의 서명 방식을 사용합니다.

인증서 배포

XenMobile에서는 중앙 집중식과 분산식의 두 가지 인증서 배포 모드를 사용할 수 있습니다. 분산 모드는 SCEP(Simple Certificate Enrollment Protocol)를 사용하며 클라이언트가 프로토콜을 지원하는 경우(iOS만 해당)에만 사용할 수 있습니다. 분산 모드는 일부 상황에서 필수입니다.

자격 증명 공급자가 분산(SCEP 지원) 배포를 지원하려면 특별한 구성 단계인 RA(등록 기관) 인증서 설정이 필요합니다. RA 인증서는 SCEP 프로토콜을 사용하는 경우 XenMobile이 실제 인증 기관에 대한 대리인(등

록자) 역할을 하기 때문에 필요합니다. XenMobile은 클라이언트에게 그러한 권한이 있음을 증명해야 합니다. 이 권한은 이전에 언급된 인증서를 XenMobile에 업로드하여 설정됩니다.

두 가지 고유한 인증서 역할이 필요합니다(단일 인증서로 두 가지 요구 사항을 모두 충족할 수 있음): RA 서명 및 RA 암호화. 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 인증서를 XenMobile에 업로드한 다음 자격 증명 공급자에서 해당 인증서에 연결합니다.

자격 증명 공급자는 인증서 역할에 대해 구성된 인증서를 가지고 있는 경우에만 분산 배포를 지원하는 것으로 간주됩니다. 각 자격 증명 공급자를 중앙 집중식 모드를 선호하거나, 분산 모드를 선호하거나, 분산 모드를 요구하도록 구성할 수 있습니다. 실제 결과는 컨텍스트에 따라 달라집니다. 컨텍스트가 분산 모드를 지원하지 않지만 자격 증명 공급자가 이 모드를 요구하는 경우 배포가 실패합니다. 마찬가지로 컨텍스트가 분산 모드를 요구하지만 자격 증명 공급자가 분산 모드를 지원하지 않는 경우 배포가 실패합니다. 다른 모든 경우에는 선호하는 설정이 적용됩니다.

다음 표는 XenMobile 전체의 SCEP 배포를 보여줍니다.

컨텍스트	SCEP 지원	SCEP 필수
iOS 프로필 서비스	예	예
iOS 모바일 장치 관리 등록	예	아니요
iOS 구성 프로필	예	아니요
SHTP 등록	아니요	아니요
SHTP 구성	아니요	아니요
Windows 태블릿 등록	아니요	아니요
Windows 태블릿 구성	아니요. 단, Windows 10 및 Windows 11에서 지원되는 Wi-Fi 장치 정책은 예외입니다.	아니요

인증서 해지

해지에는 세 가지 유형이 있습니다.

- **내부 해지:** 내부 해지는 XenMobile에서 유지 관리하는 인증서 상태에 영향을 미칩니다. XenMobile은 제시된 인증서를 평가하거나 인증서에 대한 OCSP 상태 정보를 제공할 때 이 상태를 고려합니다. 자격 증명 공급자 구성은 다양한 조건에서 이 상태가 어떻게 영향을 받는지 결정합니다. 예를 들어, 자격 증명 공급자는 인증서가 장치에서 삭제될 때 인증서를 해지된 것으로 플래그 지정하도록 지정할 수 있습니다.
- **외부 전파 해지:** Revocation XenMobile이라고도 하는 이 유형의 해지는 외부 PKI에서 얻은 인증서에 적용됩니다. 자격 증명 공급자 구성에 정의된 조건에 따라 XenMobile이 내부적으로 인증서를 해지할 때 PKI에서 인증서가 해지됩니다.
- **외부 유도 해지:** Revocation PKI라고도 하는 이 유형의 해지는 외부 PKI에서 얻은 인증서에만 적용됩니다. XenMobile이 주어진 인증서 상태를 평가할 때마다 XenMobile은 해당 상태에 대해 PKI에 쿼리합니다. 인증서가 해지되면 XenMobile은 내부적으로 인증서를 해지합니다. 이 메커니즘은 OCSP 프로토콜을 사용합니다.

이 세 가지 유형은 배타적이지 않고 함께 적용됩니다. 외부 해지 또는 독립적인 발견은 내부 해지를 유발할 수 있습니다. 내부 해지는 잠재적으로 외부 해지에 영향을 미칩니다.

인증서 갱신

인증서 갱신은 기존 인증서 해지와 다른 인증서 발급의 조합입니다.

XenMobile은 발급 실패 시 서비스 중단을 방지하기 위해 이전 인증서를 해지하기 전에 먼저 새 인증서를 얻으려고 시도합니다. 분산(SCEP 지원) 전달의 경우, 해지는 인증서가 장치에 성공적으로 설치된 후에만 발생합니다. 그렇지 않으면 새 인증서가 장치로 전송되기 전에 해지가 발생합니다. 이 해지는 인증서 설치의 성공 또는 실패와는 무관합니다.

해지 구성에는 특정 기간(일)을 지정해야 합니다. 장치가 연결되면 서버는 인증서 `NotAfter` 날짜가 현재 날짜에서 지정된 기간을 뺀 날짜보다 늦은지 확인합니다. 인증서가 해당 조건을 충족하면 XenMobile은 인증서를 갱신하려고 시도합니다.

자격 증명 공급자 생성

자격 증명 공급자 구성은 주로 자격 증명 공급자에 대해 선택하는 발급 엔터티 및 발급 방법에 따라 달라집니다. 내부 엔터티 또는 외부 엔터티를 사용하는 자격 증명 공급자를 구분할 수 있습니다.

- XenMobile 내부에 있는 재량 엔터티는 내부 엔터티입니다. 재량 엔터티의 발급 방법은 항상 서명입니다. 서명이란 각 발급 작업에서 XenMobile이 엔터티에 대해 선택된 CA 인증서로 새 키 쌍에 서명한다는 의미입니다. 키 쌍이 장치에서 생성되는지 서버에서 생성되는지는 선택한 배포 방법에 따라 달라집니다.
- 회사 인프라의 일부인 외부 엔터티에는 Microsoft CA가 포함됩니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭한 다음 **설정 > 자격 증명 공급자**를 클릭합니다.

2. **자격 증명 공급자** 페이지에서 **추가**를 클릭합니다.

   자격 증명 공급자: 일반 정보 페이지가 나타납니다.

3. **자격 증명 공급자: 일반 정보** 페이지에서 다음을 수행합니다.

   - **이름:** 새 공급자 구성에 대한 고유한 이름을 입력합니다. 이 이름은 나중에 XenMobile 콘솔의 다른 부분에서 구성을 식별하는 데 사용됩니다.
   - **설명:** 자격 증명 공급자를 설명합니다. 이 필드는 선택 사항이지만 설명은 이 자격 증명 공급자에 대한 유용한 세부 정보를 제공할 수 있습니다.
   - **발급 엔터티:** 인증서 발급 엔터티를 클릭합니다.
   - **발급 방법:** 시스템이 구성된 엔터티에서 인증서를 얻는 방법으로 **서명** 또는 **가져오기**를 클릭합니다. 클라이언트 인증서 인증의 경우 **서명**을 사용합니다.
   - **템플릿** 목록을 사용할 수 있는 경우 자격 증명 공급자의 PKI 엔터티 아래에 추가한 템플릿을 선택합니다.

     이러한 템플릿은 **설정 > PKI 엔터티**에서 Microsoft 인증서 서비스 엔터티가 추가될 때 사용할 수 있게 됩니다.

4. **다음**을 클릭합니다.

   자격 증명 공급자: 인증서 서명 요청 페이지가 나타납s니다.

5. **Credential Providers: Certificate Signing Request** 페이지에서 인증서 구성에 따라 다음을 구성하십시오.

   - **키 알고리즘:** 새 키 쌍에 대한 키 알고리즘을 선택합니다. 사용 가능한 값은 **RSA**, **DSA**, **ECDSA**입니다.
   - **키 크기:** 키 쌍의 크기를 비트 단위로 입력합니다. 이 필드는 필수입니다.

     허용되는 값은 키 유형에 따라 다릅니다. 예를 들어, DSA 키의 최대 크기는 1024비트입니다. 기본 하드웨어 및 소프트웨어에 따라 달라지는 오탐을 방지하기 위해 XenMobile은 키 크기를 강제하지 않습니다. 프로덕션 환경에서 활성화하기 전에 항상 테스트 환경에서 자격 증명 공급자 구성을 테스트하십시오.
   - **서명 알고리즘:** 새 인증서에 대한 값을 클릭합니다. 값은 키 알고리즘에 따라 달라집니다.
   - **주체 이름:** 필수. 새 인증서 주체의 고유 이름(DN)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 **추가**를 클릭합니다. 대체 이름 유형을 선택한 다음 두 번째 열에 값을 입력합니다.

  클라이언트 인증서 인증의 경우 다음을 지정합니다.

  - **유형:** 사용자 계정 이름
  - **값:** `$user.userprincipalname`

    주체 이름과 마찬가지로, 값 필드에서 XenMobile 매크로를 사용할 수 있습니다.

6. **다음**을 클릭합니다.

   자격 증명 공급자: 배포 페이지가 나타납니다.

7. **자격 증명 공급자: 배포** 페이지에서 다음 작업을 수행합니다.

   - **발급 CA 인증서** 목록에서 제공된 CA 인증서를 클릭합니다. 자격 증명 공급자가 재량적 CA 엔터티를 사용하므로 자격 증명 공급자의 CA 인증서는 항상 엔터티 자체에 구성된 CA 인증서입니다. 외부 엔터티를 사용하는 구성과의 일관성을 위해 CA 인증서가 여기에 표시됩니다.
   - **배포 모드 선택**에서 다음 키 생성 및 배포 방법 중 하나를 클릭합니다.
     - **중앙 집중식 선호: 서버 측 키 생성:** Citrix는 이 중앙 집중식 옵션을 권장합니다. 이 옵션은 XenMobile에서 지원하는 모든 플랫폼을 지원하며 Citrix Gateway 인증을 사용할 때 필요합니다. 개인 키는 서버에서 생성 및 저장되어 사용자 장치로 배포됩니다.
     - **분산형 선호: 장치 측 키 생성:** 개인 키는 사용자 장치에서 생성 및 저장됩니다. 이 분산 모드는 SCEP를 사용하며 keyUsage keyEncryption이 있는 RA 암호화 인증서와 KeyUsage digitalSignature가 있는 RA 서명 인증서가 필요합니다. 동일한 인증서를 암호화 및 서명에 모두 사용할 수 있습니다.
     - **분산형만: 장치 측 키 생성:** 이 옵션은 분산형 선호: 장치 측 키 생성과 동일하게 작동합니다. 단, '선호'가 아닌 '만'이므로 장치 측 키 생성이 실패하거나 사용할 수 없는 경우 옵션을 사용할 수 없습니다.

   분산형 선호: 장치 측 키 생성 또는 **분산형만: 장치 측 키 생성**을 선택한 경우 RA 서명 인증서와 RA 암호화 인증서를 클릭합니다. 동일한 인증서를 둘 다에 사용할 수 있습니다. 이러한 인증서에 대한 새 필드가 나타납니다.

8. **다음**을 클릭합니다.

자격 증명 공급자: 해지 XenMobile 페이지가 나타납니다. 이 페이지에서 XenMobile이 이 공급자 구성을 통해 발급된 인증서를 내부적으로 해지된 것으로 플래그 지정하는 조건을 구성합니다.

9. **자격 증명 공급자: 해지 XenMobile** 페이지에서 다음 작업을 수행합니다.

   - **발급된 인증서 해지**에서 인증서를 해지할 시기를 나타내는 옵션 중 하나를 선택합니다.
   - 인증서가 해지될 때 XenMobile이 알림을 보내도록 지시하려면 **알림 보내기** 값을 **켜기**로 설정하고 알림 템플릿을 선택합니다.
   - XenMobile에서 인증서가 해지될 때 PKI에서 인증서를 해지하려면: **PKI에서 인증서 해지**를 **켜기**로 설정하고, **엔터티 목록**에서 템플릿을 클릭합니다. 엔터티 목록에는 해지 기능이 있는 모든 사용 가능한 엔터티가 표시됩니다. XenMobile에서 인증서가 해지되면 엔터티 목록에서 선택한 PKI로 해지 호출이 전송됩니다.

10. **다음**을 클릭합니다.

    자격 증명 공급자: 해지 PKI 페이지가 나타납니다. 이 페이지에서 인증서가 해지될 경우 PKI에서 수행할 작업을 식별합니다. 알림 메시지를 생성하는 옵션도 있습니다.

11. **자격 증명 공급자: 해지 PKI** 페이지에서 PKI에서 인증서를 해지하려면 다음을 수행합니다.

    - **외부 해지 확인 사용** 설정을 **켜기**로 변경합니다. 해지 PKI와 관련된 필드가 더 나타납니다.
    - **OCSP 응답자 CA 인증서** 목록에서 인증서 주체의 고유 이름(DN)을 클릭합니다.

      DN 필드 값에 XenMobile 매크로를 사용할 수 있습니다. 예: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`

    - **인증서 해지 시** 목록에서 인증서가 해지될 때 PKI 엔터티에서 수행할 다음 작업 중 하나를 클릭합니다.
      - 아무것도 하지 않습니다.
      - 인증서를 갱신합니다.
      - 장치를 해지하고 초기화합니다.
    - XenMobile이 인증서 해지 시 알림을 보내도록 지시하려면: **알림 보내기** 값을 **켜기**로 설정합니다.

      두 가지 알림 옵션 중에서 선택할 수 있습니다.
    - **알림 템플릿 선택**을 선택하면 미리 작성된 알림 메시지를 선택한 다음 사용자 지정할 수 있습니다. 이러한 템플릿은 알림 템플릿 목록에 있습니다.
    - **알림 세부 정보 입력**을 선택하면 자신만의 알림 메시지를 작성할 수 있습니다. 수신자의 이메일 주소와 메시지를 제공하는 것 외에도 알림이 전송되는 빈도를 설정할 수 있습니다.

12. **다음**을 클릭합니다.

자격 증명 공급자: 갱신 페이지가 나타납니다. 이 페이지에서 XenMobile이 다음을 수행하도록 구성할 수 있습니다.

- 인증서를 갱신합니다. 선택적으로 갱신 시 알림을 보낼 수 있으며, 선택적으로 이미 만료된 인증서를 작업에서 제외할 수 있습니다.
- 만료가 임박한 인증서에 대한 알림을 발행합니다(갱신 전 알림).

13. **자격 증명 공급자: 갱신** 페이지에서 인증서가 만료될 때 갱신하려면 다음을 수행합니다.

    인증서 만료 시 **인증서 갱신**을 **켜기**로 설정합니다. 추가 필드가 나타납니다.

    - **인증서가 다음 기간 내에 도달하면 갱신** 필드에 인증서를 갱신할 만료 전 일수를 입력합니다.
    - 선택적으로 **이미 만료된 인증서는 갱신하지 않음**을 선택합니다. 이 경우, "이미 만료됨"은 `NotAfter` 날짜가 과거임을 의미하며, 해지되었음을 의미하지 않습니다. XenMobile은 내부적으로 해지된 후에는 인증서를 갱신하지 않습니다.

    인증서가 갱신되었을 때 XenMobile이 알림을 보내도록 하려면: **알림 보내기**를 **켜기**로 설정합니다. 인증서 만료가 임박했을 때 XenMobile이 알림을 보내도록 하려면: **인증서 만료 임박 시 알림**을 **켜기**로 설정합니다. 두 가지 선택 사항 중 하나에 대해 다음 두 가지 알림 옵션 중에서 선택할 수 있습니다.

    - **알림 템플릿 선택:** 사용자 지정할 수 있는 미리 작성된 알림 메시지를 선택합니다. 이러한 템플릿은 알림 템플릿 목록에 있습니다.
    - **알림 세부 정보 입력:** 자신만의 알림 메시지를 작성합니다. 수신자의 이메일 주소, 메시지 및 알림 전송 빈도를 제공합니다.

    인증서가 다음 기간 내에 도달하면 알림 필드에 인증서 만료 전 며칠 이내에 알림을 보낼지 입력합니다.

14. **저장**을 클릭합니다.

    자격 증명 공급자가 자격 증명 공급자 테이블에 나타납니다.

APNs 인증서

중요:

Apple은 March 31, 2021부로 APNs 레거시 바이너리 프로토콜 지원을 종료합니다. Apple은 대신 HTTP/2 기반 APNs 공급자 API를 사용할 것을 권장합니다. 릴리스 10.13.0부터 XenMobile Server는 HTTP/2 기반 API를 지원합니다. 자세한 내용은 `<https://developer.apple.com/>`의 뉴스 업데이트 "Apple Push Notification Service Update"를 참조하십시오. APNs 연결 확인에 대한 도움말은 Connectivity checks를 참조하십시오.

> XenMobile®에서 iOS 및 macOS 장치를 등록하고 관리하려면, Apple에서 Apple Push Notification service (APNs) 인증서를 설정해야 합니다.

워크플로 요약:

- **1단계:** 다음 방법 중 하나를 통해 인증서 서명 요청 생성 (CSR):
  - macOS의 키체인 접근을 사용하여 CSR 생성 (Citrix® 권장)
  - Microsoft IIS를 사용하여 CSR 생성
  - OpenSSL을 사용하여 CSR 생성
- **2단계:** XenMobile Tools에서 CSR 서명
- **3단계:** 서명된 CSR을 Apple에 제출하여 APNs 인증서 획득
- **4단계:** 1단계에 사용된 동일한 컴퓨터를 사용하여 CSR을 완료하고 PKCS #12 파일 내보내기:
  - macOS의 키체인 접근을 사용하여 PKCS #12 파일 생성
  - Microsoft IIS를 사용하여 PKCS #12 파일 생성
  - OpenSSL을 사용하여 PKCS #12 파일 생성
- **5단계:** APNs 인증서를 XenMobile로 가져오기
- **6단계:** APNs 인증서 갱신

인증서 서명 요청 생성

macOS의 키체인 접근을 사용하여 CSR을 생성하는 것이 좋습니다. Microsoft IIS 또는 OpenSSL을 사용하여 CSR을 생성할 수도 있습니다.

> **중요:**
>
> - 인증서 생성에 사용된 Apple ID의 경우:
>   - Apple ID는 개인 ID가 아닌 회사 ID여야 합니다.
>   - 인증서 생성에 사용하는 Apple ID를 기록하십시오.
>   - 인증서를 갱신하려면 동일한 조직 이름과 Apple ID를 사용하십시오. 다른 Apple ID를 사용하여 인증서를 갱신하면 장치 재등록이 필요합니다.
> - 실수로 또는 의도적으로 인증서를 취소하면 장치를 관리할 수 없게 됩니다.

- iOS 개발자 엔터프라이즈 프로그램을 사용하여 모바일 장치 관리자 푸시 인증서를 생성한 경우: Apple 푸시 인증서 포털에서 마이그레이션된 인증서에 대한 모든 작업을 처리해야 합니다.

macOS의 키체인 접근을 사용하여 CSR 생성

1. macOS를 실행하는 컴퓨터에서 **응용 프로그램 > 유틸리티** 아래에서 키체인 접근 앱을 시작합니다.
2. **키체인 접근** 메뉴를 열고 **인증서 지원 > 인증 기관에서 인증서 요청**을 클릭합니다.
3. 인증서 지원이 다음 정보를 입력하라는 메시지를 표시합니다.
   - **이메일 주소:** 인증서 관리를 담당하는 개인 또는 역할 계정의 이메일 주소입니다.
   - **일반 이름:** 인증서 관리를 담당하는 개인 또는 역할 계정의 일반 이름입니다.
   - **CA 이메일 주소:** 인증 기관의 이메일 주소입니다.
4. **디스크에 저장** 및 **키 쌍 정보 지정** 옵션을 선택한 다음 **계속**을 클릭합니다.
5. CSR 파일의 이름을 입력하고 파일을 컴퓨터에 저장한 다음 **저장**을 클릭합니다.
6. 키 쌍 정보를 지정합니다. **키 크기** 2048비트와 **RSA 알고리즘**을 선택한 다음 **계속**을 클릭합니다. 이제 CSR 파일을 APNs 인증서 프로세스의 일부로 업로드할 준비가 되었습니다.
7. 인증서 도우미가 CSR 프로세스를 완료하면 **완료**를 클릭합니다.
8. 계속하려면 CSR 서명.

Microsoft IIS를 사용하여 CSR 생성

APNs 인증서 요청을 생성하는 첫 번째 단계는 CSR(인증서 서명 요청)을 만드는 것입니다. Windows의 경우 Microsoft IIS를 사용하여 CSR을 생성합니다.

1. Microsoft IIS를 엽니다.
2. IIS의 서버 인증서 아이콘을 두 번 클릭합니다.
3. **서버 인증서** 창에서 **인증서 요청 만들기**를 클릭합니다.
4. 적절한 DN(고유 이름) 정보를 입력한 다음 **다음**을 클릭합니다.
5. 암호화 서비스 공급자로 **Microsoft RSA SChannel Cryptographic Provider**를 선택하고 비트 길이는 **2048**을 선택한 다음 **다음**을 클릭합니다.
6. 파일 이름을 입력하고 CSR을 저장할 위치를 지정한 다음 **마침**을 클릭합니다.
7. 계속하려면 CSR 서명을(를) 참조하십시오.

OpenSSL을 사용하여 CSR 생성

macOS 장치 또는 Microsoft IIS를 사용하여 CSR을 생성할 수 없는 경우 OpenSSL을 사용하십시오. OpenSSL 웹 사이트에서 OpenSSL을 다운로드하여 설치할 수 있습니다.

1. OpenSSL을 설치한 컴퓨터에서 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 다음 메시지가 나타납니다. 요청된 정보를 입력합니다.

   ```
   You are about to be asked to enter information that will be
   incorporated into your certificate request.

   What you are about to enter is what is called a Distinguished Name or a
   DN.

   There are quite a few fields but you can leave some blank

   For some fields there will be a default value,

   If you enter '.', the field will be left blank.

   -----

   Country Name (2 letter code) [AU]:US

   State or Province Name (full name) [Some-State]:CA

   Locality Name (eg, city) []:RWC

   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

   Organizational Unit Name (eg, section) [:Marketing

   Common Name (eg, YOUR name) []:John Doe

   Email Address []:john.doe@customer.com
   ```

3. 다음 메시지에서 CSR 개인 키에 대한 암호를 입력합니다.

```
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

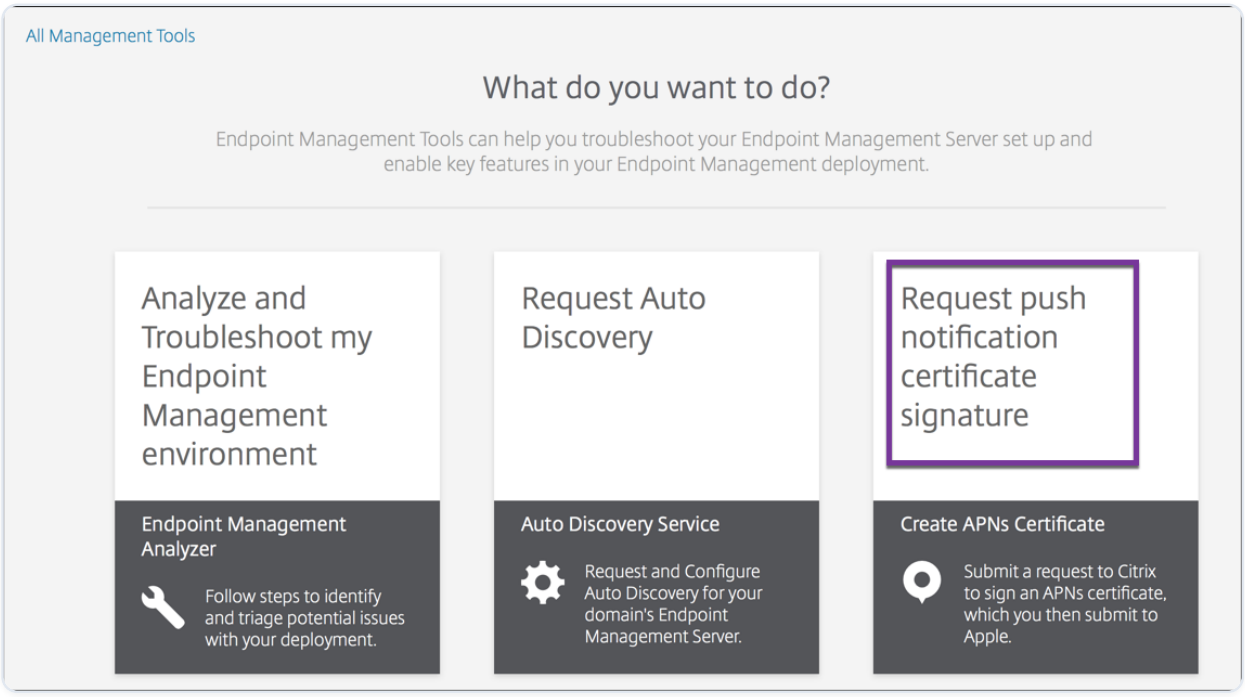
An optional company name []:
```

4. 계속하려면 다음 섹션에 설명된 대로 CSR에 서명합니다.

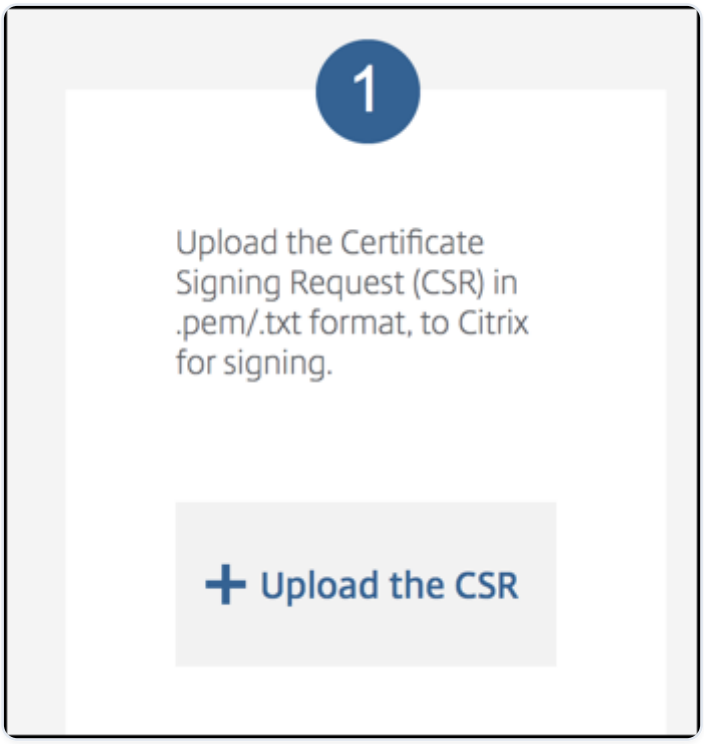
CSR 서명

XenMobile에서 인증서를 사용하려면 Citrix에 제출하여 서명해야 합니다. Citrix는 모바일 장치 관리 서명 인증서로 CSR에 서명하고 서명된 파일을 `.plist` 형식으로 반환합니다.

1. 브라우저에서 Endpoint Management Tools 웹 사이트로 이동한 다음 **푸시 알림 인증서 서명 요청**을 클릭합니다.



2. **새 인증서 만들기 페이지**에서 **CSR 업로드**를 클릭합니다.



3. 인증서를 찾아 선택합니다.

   인증서는 .pem/txt 형식이어야 합니다.

4. **Endpoint Management APNs CSR 서명** 페이지에서 **서명**을 클릭합니다. CSR이 서명되고 구성된 다운로드 폴더에 자동으로 저장됩니다.
5. 계속하려면 다음 섹션에 설명된 대로 서명된 CSR을 제출합니다.

서명된 CSR을 Apple에 제출하여 APNs 인증서 받기

Citrix로부터 서명된 CSR(인증서 서명 요청)을 받은 후, XenMobile로 가져오는 데 필요한 APNs 인증서를 받기 위해 해당 CSR을 Apple에 제출합니다.

> **참고:**
>
> 일부 사용자는 Apple Push Portal에 로그인하는 데 문제가 있다고 보고했습니다. 대안으로, Apple 개발자 포털에 로그인한 다음 다음 단계를 따르십시오.

1. 브라우저에서 Apple Push Certificates Portal로 이동합니다.
2. **인증서 생성**을 클릭합니다.
3. Apple에서 인증서를 처음 생성하는 경우: **이 약관을 읽고 동의합니다** 확인란을 선택한 다음 **수락**을 클릭합니다.

4. **파일 선택**을 클릭하고 컴퓨터에서 서명된 CSR을 찾아본 다음 **업로드**를 클릭합니다. 확인 메시지는 업로드가 성공했음을 나타냅니다.
5. **다운로드**를 클릭하여 .pem 인증서를 검색합니다.
6. 계속하려면 다음 섹션에 설명된 대로 CSR을 완료하고 PKCS #12 파일을 내보냅니다.

CSR을 완료하고 PKCS #12 파일 내보내기

Apple에서 APNs 인증서를 받은 후, 키체인 접근, Microsoft IIS 또는 OpenSSL로 돌아가 인증서를 PCKS #12 파일로 내보냅니다.

PKCS #12 파일에는 APNS 인증서 파일과 개인 키가 포함되어 있습니다. PFX 파일은 일반적으로 .pfx 또는 .p12 확장자를 가집니다. .pfx 및 .p12 파일은 상호 교환하여 사용할 수 있습니다.

> **중요:**
>
> Citrix는 로컬 시스템에서 개인 키와 공개 키를 저장하거나 내보낼 것을 권장합니다. APNs 인증서에 다시 액세스하려면 이 키가 필요합니다. 동일한 키가 없으면 인증서가 유효하지 않으며 전체 CSR 및 APNs 프로세스를 반복해야 합니다.

macOS의 키체인 접근을 사용하여 PKCS #12 파일 생성

> **중요:**
>
> 이 작업에는 CSR을 생성하는 데 사용했던 것과 동일한 macOS 장치를 사용하십시오.

1. 장치에서 Apple로부터 받은 프로덕션 ID(.pem) 인증서를 찾습니다.
2. 키체인 접근 애플리케이션을 시작하고 **로그인 > 나의 인증서** 탭으로 이동합니다. 프로덕션 ID 인증서를 열린 창으로 끌어다 놓습니다.
3. 인증서를 클릭하고 왼쪽 화살표를 확장하여 인증서에 연결된 개인 키가 포함되어 있는지 확인합니다.
4. 인증서를 PCKS #12(.pfx) 인증서로 내보내기 시작하려면 인증서와 개인 키를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 **2개 항목 내보내기**를 선택합니다.
5. XenMobile에서 사용할 인증서 파일에 고유한 이름을 지정합니다. 이름에 공백 문자를 포함하지 마십시오. 그런 다음, 저장된 인증서의 폴더 위치를 선택하고 .pfx 파일 형식을 선택한 후 **저장**을 클릭합니다.
6. 인증서 내보내기를 위한 암호를 입력합니다. Citrix는 고유하고 강력한 암호를 사용할 것을 권장합니다. 또한 나중에 사용하고 참조할 수 있도록 인증서와 암호를 안전하게 보관하십시오.

7. 키체인 접근 앱에서 로그인 암호 또는 선택한 키체인을 묻는 메시지가 표시됩니다. 암호를 입력한 다음 **확인**을 클릭합니다. 이제 저장된 인증서를 XenMobile Server에서 사용할 준비가 되었습니다.
8. 계속하려면 XenMobile로 APNs 인증서 가져오기를 참조하십시오.

Microsoft IIS를 사용하여 PKCS #12 파일 만들기

> **중요:**
>
> 이 작업에는 CSR을 생성하는 데 사용한 것과 동일한 IIS 서버를 사용하십시오.

1. Microsoft IIS를 엽니다.
2. **서버 인증서** 아이콘을 클릭합니다.
3. **서버 인증서** 창에서 **인증서 요청 완료**를 클릭합니다.
4. Apple에서 받은 Certificate.pem 파일을 찾아봅니다. 그런 다음, 식별하기 쉬운 이름 또는 인증서 이름을 입력하고 **확인**을 클릭합니다. 이름에 공백 문자를 포함하지 마십시오.
5. 4단계에서 식별한 인증서를 선택한 다음 **내보내기**를 클릭합니다.
6. .pfx 인증서의 위치와 파일 이름 및 암호를 지정한 다음 **확인**을 클릭합니다.

   XenMobile로 인증서를 가져오려면 암호가 필요합니다.
7. .pfx 인증서를 XenMobile을 설치할 서버에 복사합니다.
8. 계속하려면 XenMobile로 APNs 인증서 가져오기를 참조하십시오.

OpenSSL을 사용하여 PKCS #12 파일 만들기

CSR을 생성하는 데 OpenSSL을 사용하는 경우 OpenSSL을 사용하여 .pfx APNs 인증서를 생성할 수도 있습니다.

1. 명령 프롬프트 또는 셸에서 다음 명령을 실행합니다. `Customer.privatekey.pem`은 CSR의 개인 키입니다. `APNs_Certificate.pem`는 Apple에서 방금 받은 인증서입니다.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey
   Customer.privatekey.pem -out apns_identity.pfx
   ```
2. .pfx 인증서 파일의 암호를 입력합니다. 이 암호는 XenMobile에 인증서를 업로드할 때 다시 사용하므로 기억해야 합니다.
3. .pfx 인증서 파일의 위치를 기록해 둡니다. 그런 다음, 콘솔을 사용하여 파일을 업로드할 수 있도록 파일을 XenMobile Server로 복사합니다.

4. 계속하려면 다음 섹션에 설명된 대로 APNs 인증서를 XenMobile로 가져옵니다.

APNs 인증서를 XenMobile로 가져오기

새 APNs 인증서를 받은 후: APNs 인증서를 XenMobile로 가져와서 처음으로 인증서를 추가하거나 인증서를 교체합니다.

1. XenMobile 콘솔에서 **설정 > 인증서**로 이동합니다.
2. **가져오기 > 키 저장소**를 클릭합니다.
3. **사용 용도**에서 **APNs**를 선택합니다.
4. 컴퓨터에서 .pfx 또는 .p12 파일을 찾습니다.
5. 암호를 입력한 다음 **가져오기**를 클릭합니다.

XenMobile의 인증서에 대한 자세한 내용은 인증서 및 인증을 참조하십시오.

APNs 인증서 갱신

> **중요:**
>
> 갱신 프로세스에 다른 Apple ID를 사용하는 경우 사용자 장치를 다시 등록해야 합니다.

> APNs 인증서를 갱신하려면, 인증서 생성 단계를 수행한 다음, Apple Push Certificates Portal로 이동합니다. 해당 포털을 사용하여 새 인증서를 업로드합니다. 로그인하면 기존 인증서 또는 이전 Apple 개발자 계정에서 가져온 인증서가 나타납니다.

Certificates Portal에서 인증서를 갱신할 때 유일한 차이점은 **갱신**을 클릭한다는 것입니다. 사이트에 액세스하려면 Certificates Portal에 개발자 계정이 있어야 합니다. 인증서를 갱신하려면 동일한 조직 이름과 Apple ID를 사용하십시오.

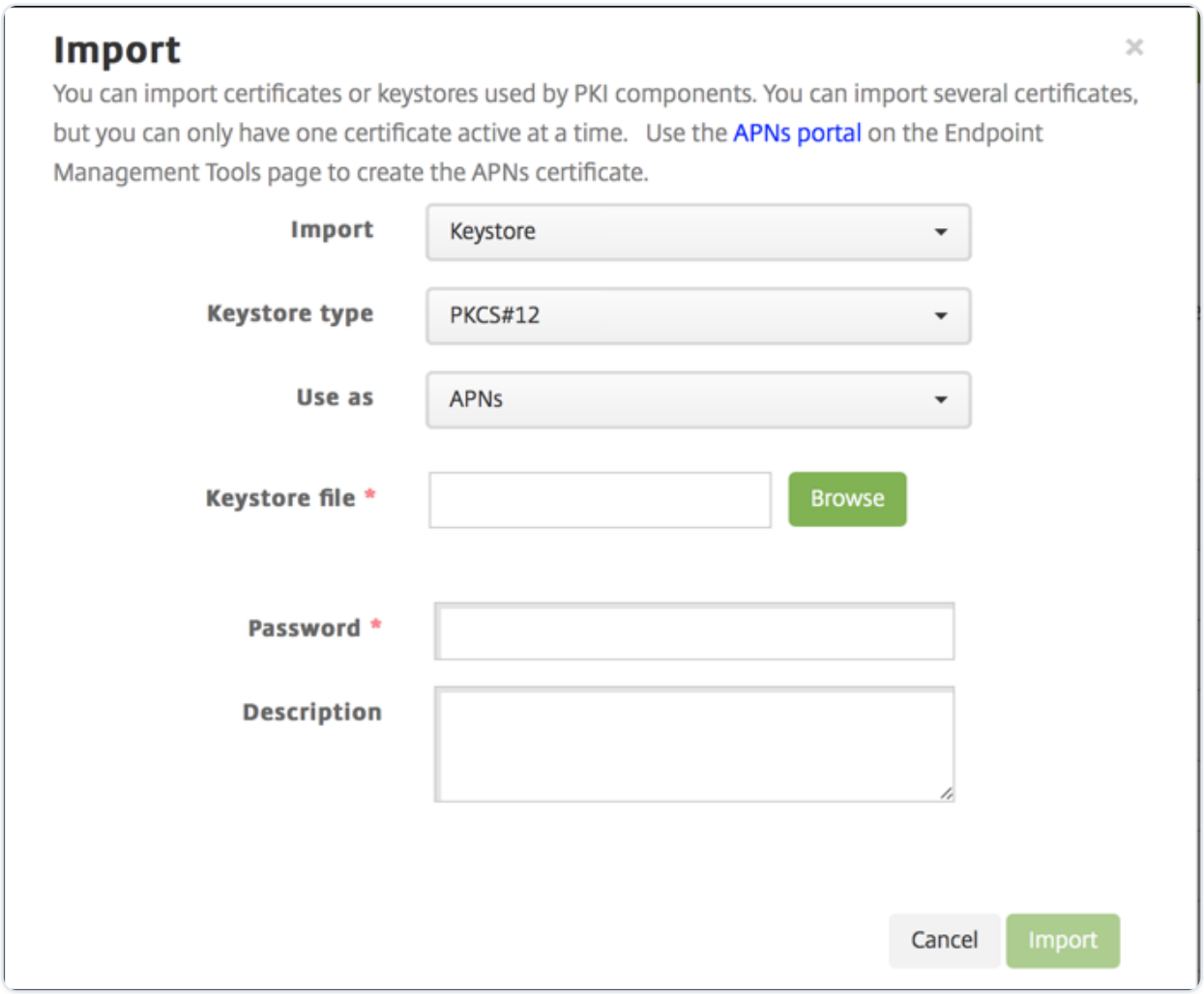
XenMobile 콘솔에서 APNs 인증서가 언제 만료되는지 확인하려면 **설정 > 인증서**로 이동하십시오. 인증서가 만료되더라도 해지하지 마십시오.

1. Microsoft IIS, 키체인 접근(macOS) 또는 OpenSSL을 사용하여 CSR을 생성합니다. CSR 생성에 대한 자세한 내용은 인증서 서명 요청 생성을 참조하십시오.
2. 브라우저에서 Endpoint Management Tools로 이동합니다. 그런 다음, **푸시 알림 인증서 서명 요청**을 클릭합니다.
3. **+ CSR 업로드**를 클릭합니다.

4. 대화 상자에서 CSR로 이동하여 **열기**를 클릭한 다음 **서명**을 클릭합니다.
5. `.plist` 파일을 받으면 저장합니다.
6. 3단계 제목에서 **Apple Push Certificates Portal**을 클릭하고 로그인합니다.
7. 갱신하려는 인증서를 선택한 다음 **갱신**을 클릭합니다.
8. `.plist` 파일을 업로드합니다. 출력으로 .pem 파일을 받게 됩니다. .pem 파일을 저장합니다.
9. 해당 .pem 파일을 사용하여 CSR을 완료합니다(1단계에서 CSR을 생성하는 데 사용한 방법에 따라).
10. 인증서를 .pfx 파일로 내보냅니다.

XenMobile 콘솔에서 .pfx 파일을 가져오고 다음과 같이 구성을 완료합니다.

1. **설정 > 인증서 > 가져오기**로 이동합니다.
2. **가져오기 메뉴**에서 **키 저장소**를 선택합니다.
3. **키 저장소 유형** 메뉴에서 **PKCS #12**를 선택합니다.
4. **용도**에서 **APNs**를 선택합니다.



5. **키 저장소 파일**에서 **찾아보기**를 클릭하고 파일로 이동합니다.

6. **암호**에 인증서 암호를 입력합니다.
7. 선택 사항인 **설명**을 입력합니다.
8. **가져오기**를 클릭합니다.

XenMobile은 사용자를 **인증서** 페이지로 다시 리디렉션합니다. **이름**, **상태**, **유효 시작일**, **유효 만료일** 필드가 업데이트됩니다.

Citrix Files와 단일 Sign-On을 위한 SAML

> **면책 조항:**

> ShareFile(현재 Progress)이 지원을 중단하면 이 기능은 더 이상 사용되지 않습니다.

> XenMobile® 및 ShareFile을 구성하여 SAML(Security Assertion Markup Language)을 사용하여 Citrix Files 모바일 앱에 대한 SSO(단일 Sign-On) 액세스를 제공할 수 있습니다. 이 기능에는 다음이 포함됩니다.

- MAM SDK가 활성화되었거나 MDX Toolkit을 사용하여 래핑된 Citrix Files 앱
- 웹사이트, Outlook 플러그인 또는 동기화 클라이언트와 같은 래핑되지 않은 Citrix Files 클라이언트
- **래핑된 Citrix Files 앱의 경우**. Citrix Files 모바일 앱을 통해 Citrix Files에 로그온하는 사용자는 사용자 인증 및 SAML 토큰 획득을 위해 Secure Hub로 리디렉션됩니다. 인증에 성공하면 Citrix Files 모바일 앱은 SAML 토큰을 ShareFile로 보냅니다. 초기 로그온 후 사용자는 SSO를 통해 Citrix Files 모바일 앱에 액세스할 수 있습니다. 또한 매번 로그온하지 않고도 ShareFile에서 Secure Mail 메일에 문서를 첨부할 수 있습니다.
- **래핑되지 않은 Citrix Files 클라이언트의 경우**. 웹 브라우저 또는 다른 Citrix Files 클라이언트를 사용하여 Citrix Files에 로그온하는 사용자는 XenMobile로 리디렉션됩니다. XenMobile은 사용자를 인증하고, 사용자는 SAML 토큰을 획득하여 ShareFile로 보냅니다. 초기 로그온 후 사용자는 매번 로그온하지 않고도 SSO를 통해 Citrix Files 클라이언트에 액세스할 수 있습니다.

XenMobile을 ShareFile에 대한 SAML IdP(ID 공급자)로 사용하려면 이 문서에 설명된 대로 XenMobile을 엔터프라이즈 계정과 함께 사용하도록 구성해야 합니다. 또는 XenMobile이 스토리지 영역 커넥터에서만 작동하도록 구성할 수 있습니다. 자세한 내용은 XenMobile과 함께 ShareFile 사용을 참조하십시오.

자세한 참조 아키텍처 다이어그램은 아키텍처를 참조하십시오.

전제 조건

XenMobile 및 Citrix Files 앱으로 SSO를 구성하기 전에 다음 전제 조건을 완료하십시오.

- MAM SDK 또는 호환되는 버전의 MDX Toolkit(Citrix Files 모바일 앱용).

  자세한 내용은 XenMobile 호환성을 참조하십시오.
- 호환되는 버전의 Citrix Files 모바일 앱 및 Secure Hub.
- ShareFile 관리자 계정.
- XenMobile과 ShareFile 간의 연결이 확인되었습니다.

ShareFile 액세스 구성

ShareFile용 SAML을 설정하기 전에 다음과 같이 ShareFile 액세스 정보를 제공하십시오.

1. XenMobile 웹 콘솔에서 **구성 > ShareFile**을 클릭합니다. **ShareFile** 구성 페이지가 나타납니다.

   ShareFile 구성 설정(/en-us/xenmobile/server/media/configure-content-collaboration-saml-for-non-mdx-apps.png)
2. 다음 설정을 구성합니다.

   - **도메인:** ShareFile 하위 도메인 이름을 입력합니다. 예: `example.sharefile.com`.
   - **전달 그룹에 할당:** ShareFile과 함께 SSO를 사용할 수 있도록 하려는 전달 그룹을 선택하거나 검색합니다.
   - **ShareFile 관리자 계정 로그온**
   - **사용자 이름:** ShareFile 관리자 사용자 이름을 입력합니다. 이 사용자는 관리자 권한이 있어야 합니다.
   - **암호:** ShareFile 관리자 암호를 입력합니다.
   - **사용자 계정 프로비저닝:** 이 설정을 비활성화된 상태로 둡니다. 사용자 프로비저닝에는 ShareFile 사용자 관리 도구를 사용합니다. 사용자 계정 및 배포 그룹 프로비저닝을 참조하십시오.
3. **연결 테스트**를 클릭하여 ShareFile 관리자 계정의 사용자 이름과 암호가 지정된 ShareFile 계정에 대해 인증되는지 확인합니다.
4. **저장**을 클릭합니다.

   - XenMobile은 ShareFile과 동기화하고 ShareFile 설정인 **ShareFile Issuer/Entity ID** 및 **Login URL**을 업데이트합니다.
   - **구성 > ShareFile** 페이지에 **앱 내부 이름**이 표시됩니다. 나중에 Citrix Files.com SSO 설정 수정에 설명된 단계를 완료하려면 이 이름이 필요합니다.

래핑된 Citrix Files MDX 앱용 SAML 설정

래핑된 Citrix Files MDX 앱으로 Single Sign-On을 구성하는 데 Citrix Gateway를 사용할 필요가 없습니다. 웹 사이트, Outlook 플러그인 또는 동기화 클라이언트와 같은 래핑되지 않은 Citrix Files 클라이언트에 대한 액세스를 구성하려면 다른 Citrix Files 클라이언트를 위한 Citrix Gateway 구성을 참조하십시오.

다음 단계는 iOS 및 Android 앱과 장치에 적용됩니다. 래핑된 Citrix Files MDX 앱용 SAML을 구성하려면 다음을 수행합니다.

1. MDX Toolkit을 사용하여 Citrix Files 모바일 앱을 래핑합니다. MDX Toolkit으로 앱을 래핑하는 방법에 대한 자세한 내용은 MDX Toolkit으로 앱 래핑을 참조하십시오.
2. XenMobile 콘솔에서 래핑된 Citrix Files 모바일 앱을 업로드합니다. MDX 앱 업로드에 대한 자세한 내용은 XenMobile에 MDX 앱 추가를 참조하십시오.
3. SAML 설정 확인: 이전에 구성한 관리자 사용자 이름과 암호를 사용하여 ShareFile에 로그온합니다.
4. ShareFile과 XenMobile이 동일한 시간대로 구성되었는지 확인합니다. XenMobile이 구성된 시간대에 대해 올바른 시간을 표시하는지 확인합니다. 그렇지 않으면 SSO가 실패할 수 있습니다.

Citrix Files 모바일 앱 유효성 검사

1. 사용자 장치에 Secure Hub를 설치하고 구성합니다.
2. XenMobile Store에서 Citrix Files 모바일 앱을 다운로드하여 설치합니다.
3. Citrix Files 모바일 앱을 시작합니다. Citrix Files가 사용자 이름이나 암호를 묻는 메시지 없이 시작됩니다.

Secure Mail로 유효성 검사

1. 사용자 장치에 아직 설치 및 구성되지 않은 경우 Secure Hub를 설치하고 구성합니다.
2. XenMobile Store에서 Secure Mail을 다운로드, 설치 및 설정합니다.
3. 새 이메일 양식을 열고 **Citrix Files에서 첨부**를 탭합니다. 사용자 이름이나 암호를 묻지 않고 이메일에 첨부할 수 있는 파일이 표시됩니다.

다른 Citrix Files 클라이언트를 위한 Citrix Gateway 구성

웹사이트, Outlook 플러그인 또는 동기화 클라이언트와 같은 래핑되지 않은 Citrix Files 클라이언트에 대한 액세스를 구성하려면 다음과 같이 XenMobile을 SAML ID 공급자로 사용하도록 Citrix Gateway를 구성합니다.

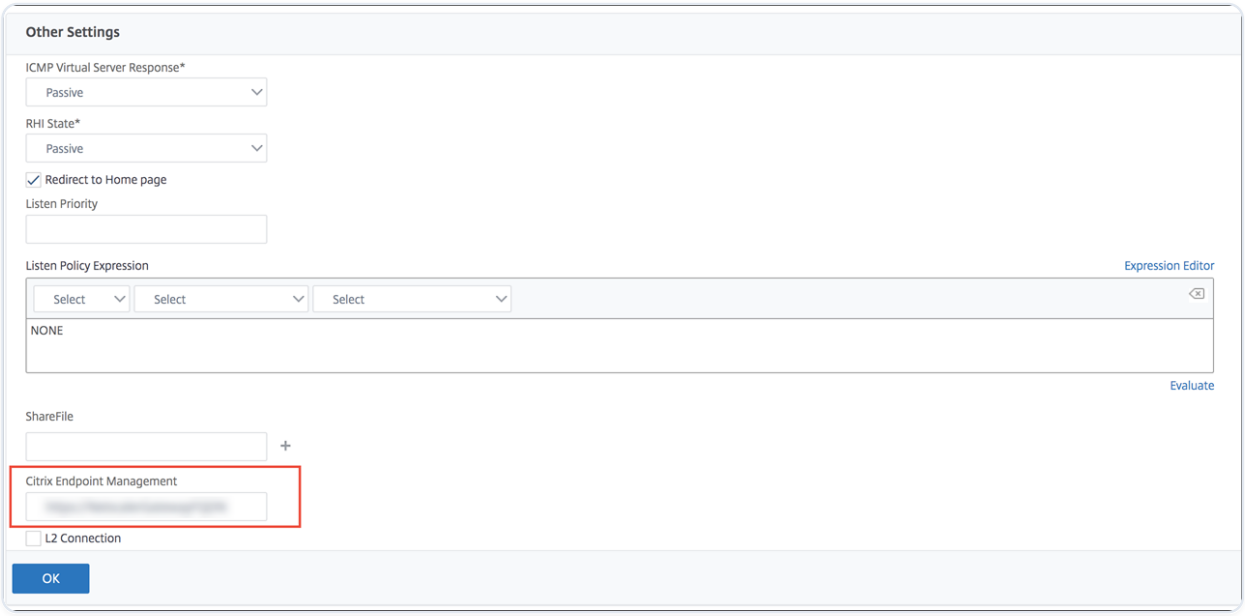
- 홈 페이지 리디렉션을 비활성화합니다.
- Citrix Files 세션 정책 및 프로필을 생성합니다.

- Citrix Gateway 가상 서버에서 정책을 구성합니다.

홈 페이지 리디렉션 비활성화

/cginfra 경로를 통해 들어오는 요청에 대한 기본 동작을 비활성화합니다. 이 작업을 통해 사용자는 구성된 홈 페이지 대신 원래 요청된 내부 URL을 볼 수 있습니다.

1. XenMobile 로그온에 사용되는 Citrix Gateway 가상 서버 설정을 편집합니다. Citrix ADC에서 **기타 설정**으로 이동한 다음 **홈 페이지로 리디렉션** 레이블이 지정된 확인란의 선택을 취소합니다.



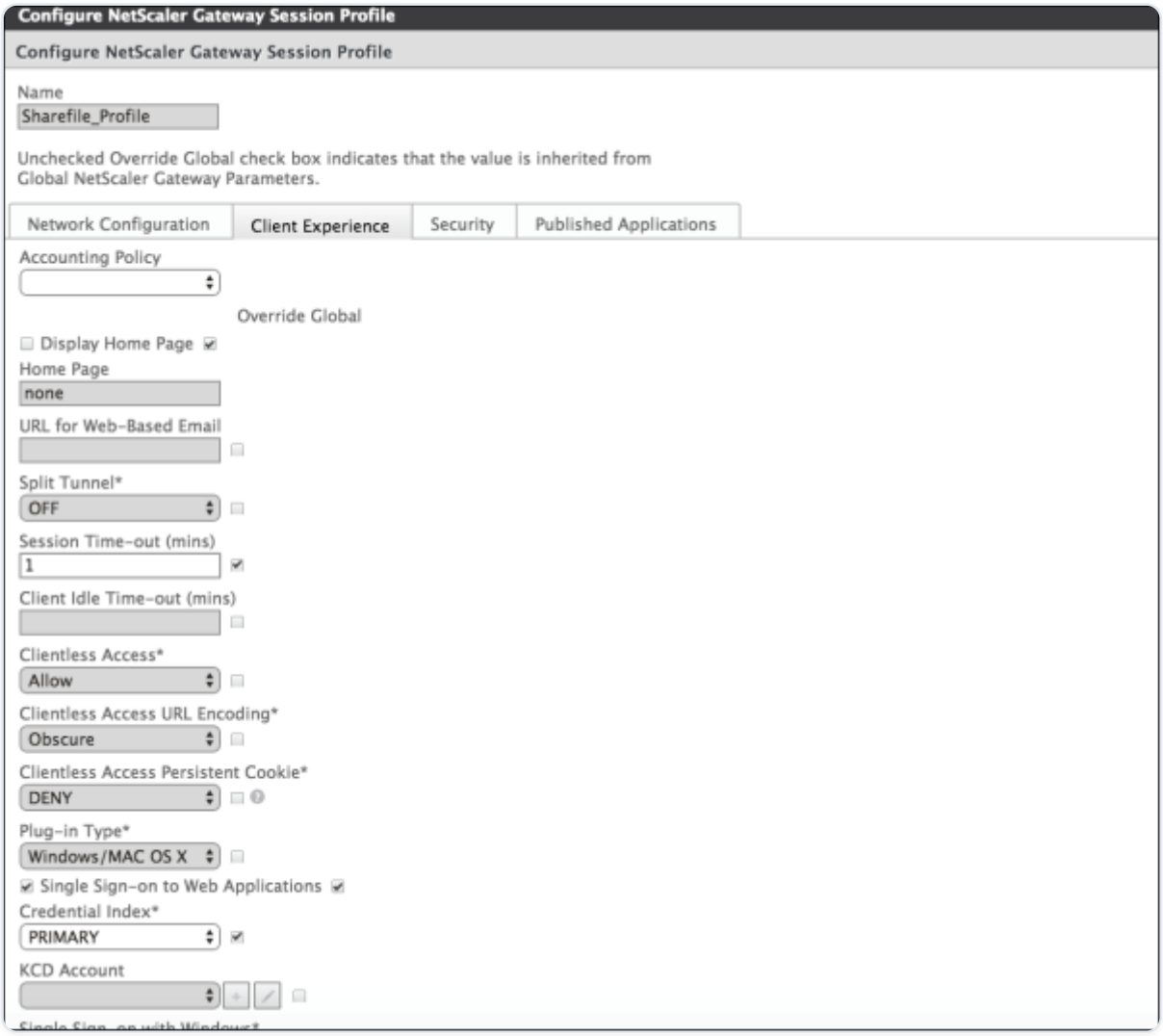
2. **ShareFile** (현재 ShareFile이라고 함) 아래에 XenMobile 내부 서버 이름과 포트 번호를 입력합니다.
3. **Citrix Endpoint Management™** 아래에 XenMobile URL을 입력합니다. 사용 중인 Citrix Gateway 버전은 이전 제품 이름인 **AppController**를 참조할 수 있습니다.

   이 구성은 /cginfra 경로를 통해 입력한 URL에 대한 요청을 승인합니다.

Citrix Files 세션 정책 및 요청 프로필 생성

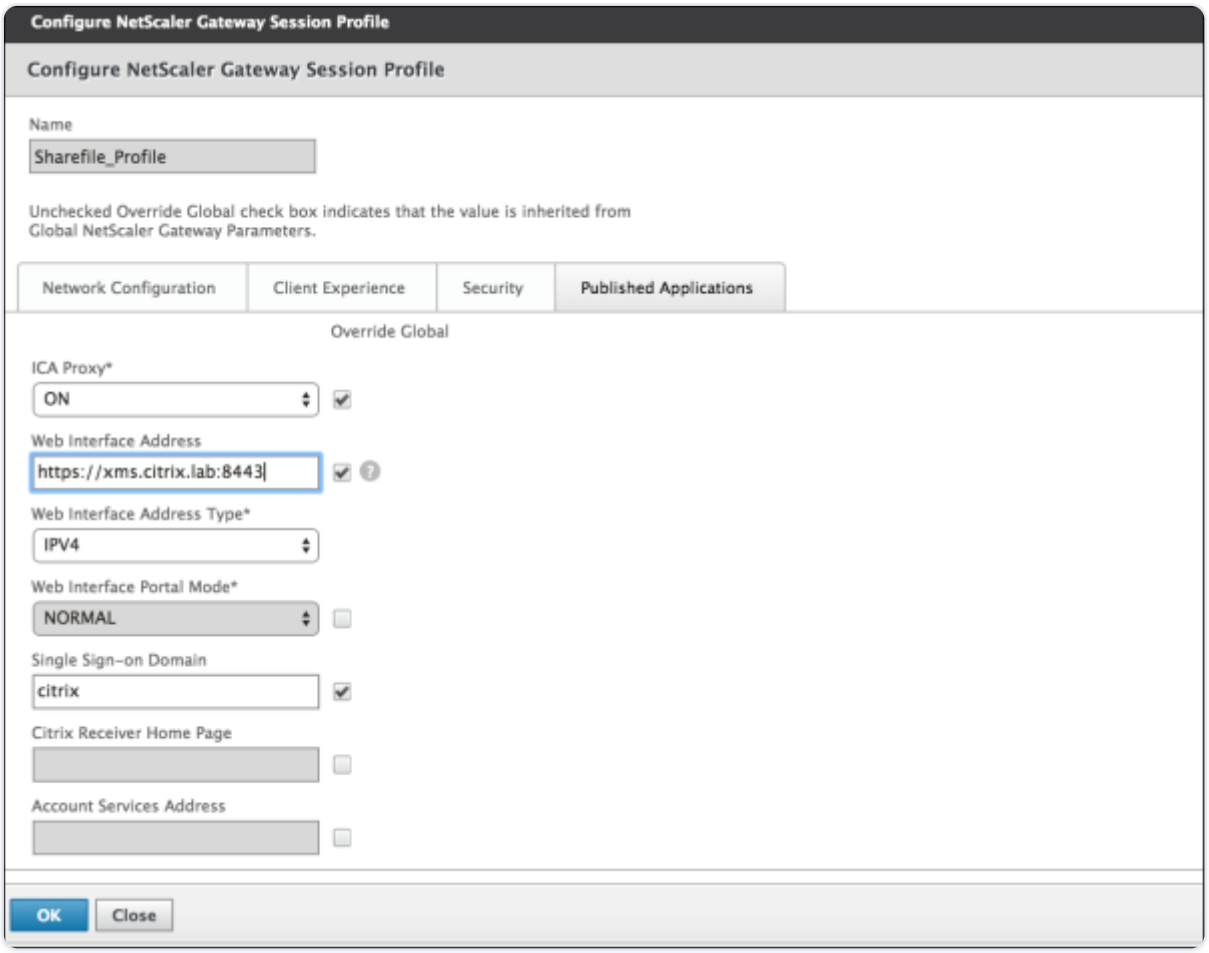
Citrix Files 세션 정책 및 요청 프로필을 생성하려면 다음 설정을 구성하십시오:

1. Citrix Gateway 구성 유틸리티의 왼쪽 탐색 창에서 **Citrix Gateway > Policies > Session**을 클릭합니다.
2. 세션 정책을 생성합니다. **Policies** 탭에서 **Add**를 클릭합니다.
3. **Name** 필드에 **ShareFile_Policy**를 입력합니다.
4. **+** 버튼을 클릭하여 작업을 생성합니다. **Create Session Profile** 페이지가 나타납니다.



다음 설정을 구성합니다:

- **이름: ShareFile_Profile**을 입력합니다.
- **Client Experience** 탭을 클릭한 다음 다음 설정을 구성합니다:
  - **홈 페이지: none**을 입력합니다.
  - **세션 시간 초과(분): 1**을 입력합니다.
  - **웹 애플리케이션에 대한 Single Sign-on:** 이 설정을 선택합니다.
  - **자격 증명 인덱스: PRIMARY**를 클릭합니다.
- **Published Applications** 탭을 클릭합니다.

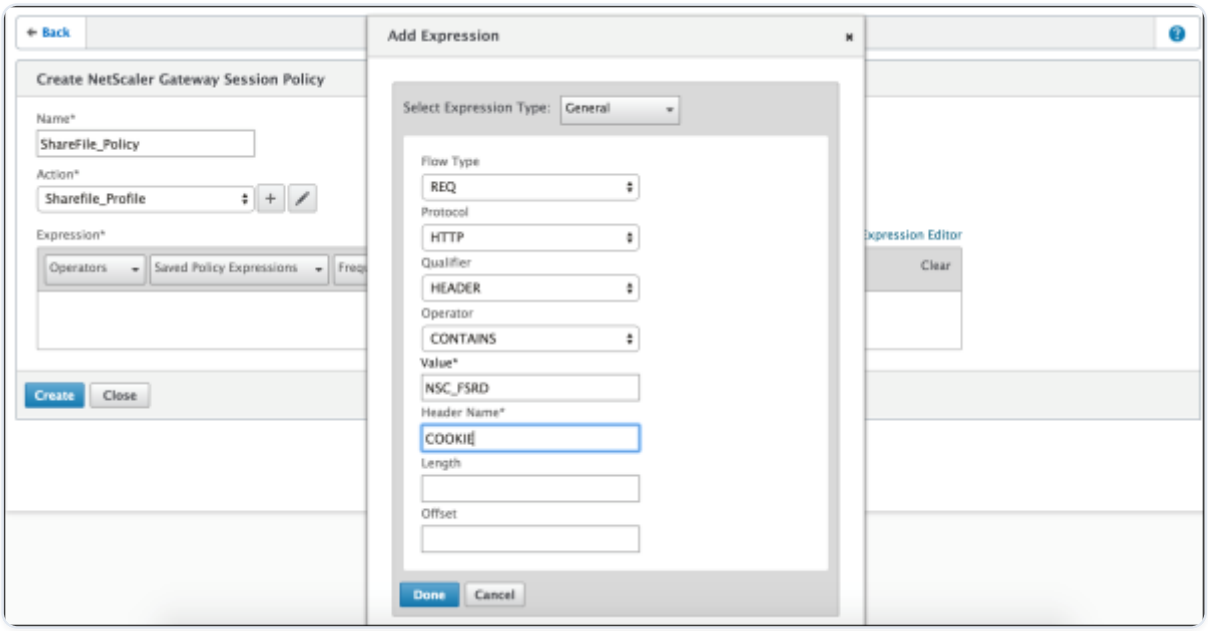


다음 설정을 구성하십시오:

- **ICA® Proxy: 켜기**를 클릭합니다.
- **웹 인터페이스 주소:** XenMobile Server URL을 입력합니다.
- **단일 Sign-on 도메인:** Active Directory 도메인 이름을 입력합니다.

  Citrix Gateway 세션 프로필을 구성할 때, **단일 Sign-on 도메인**의 도메인 접미사는 LDAP에 정의된 XenMobile 도메인 별칭과 일치해야 합니다.

5. 세션 프로필을 정의하려면 **생성**을 클릭합니다.
6. **표현식 편집기**를 클릭합니다.



다음 설정을 구성하십시오:

- **값: NSC_FSRD**를 입력합니다.
- **헤더 이름: COOKIE**를 입력합니다.

7. **생성**을 클릭한 다음 **닫기**를 클릭합니다.

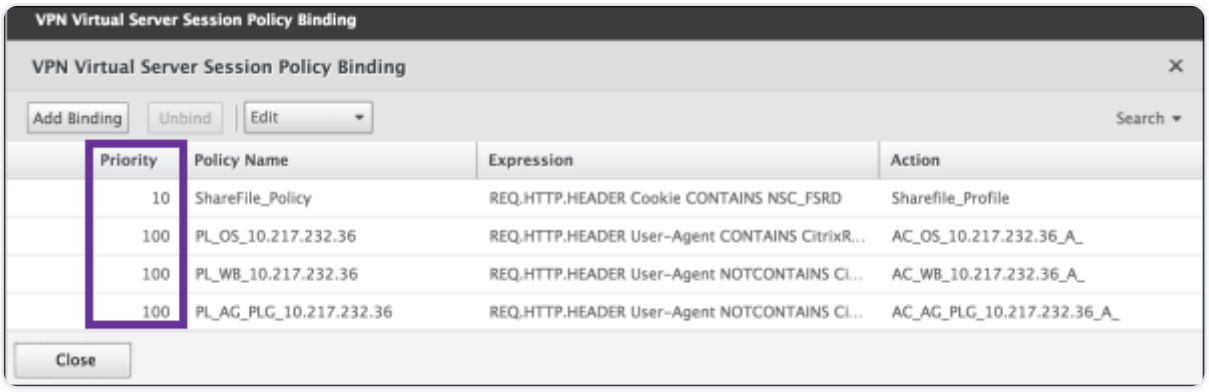


Citrix Gateway 가상 서버에서 정책 구성

Citrix Gateway 가상 서버에서 다음 설정을 구성합니다.

1. Citrix Gateway 구성 유틸리티의 왼쪽 탐색 창에서 **Citrix Gateway > 가상 서버**를 클릭합니다.
2. **세부 정보** 창에서 Citrix Gateway 가상 서버를 클릭합니다.
3. **편집**을 클릭합니다.
4. **구성된 정책 > 세션 정책**을 클릭한 다음 **바인딩 추가**를 클릭합니다.
5. **ShareFile_Policy**를 선택합니다.

6. 선택한 정책에 대해 자동으로 생성된 **우선 순위** 번호를 편집하여 나열된 다른 정책과 관련하여 가장 높은 우선 순위(가장 작은 숫자)를 갖도록 합니다. 예를 들어:



7. **완료**를 클릭한 다음 실행 중인 Citrix ADC 구성을 저장합니다.

Citrix Files.com SSO 설정 수정

MDX 및 비MDX Citrix Files 앱 모두에 대해 다음 변경 사항을 적용합니다.

> **중요:**

> 내부 애플리케이션 이름에 새 번호가 추가됩니다.

> - Citrix Files 앱을 편집하거나 다시 만들 때마다
> - XenMobile에서 ShareFile 설정을 변경할 때마다

> 결과적으로 Citrix Files 웹사이트의 로그인 URL도 업데이트된 앱 이름을 반영하도록 업데이트해야 합니다.

1. ShareFile 관리자로 ShareFile 계정(`https://<subdomain>.sharefile.com`)에 로그인합니다.
2. ShareFile 웹 인터페이스에서 **관리**를 클릭한 다음 **단일 Sign-on 구성**을 선택합니다.
3. **로그인 URL**을 다음과 같이 편집합니다.

   편집 전 **로그인 URL** 샘플은 다음과 같습니다: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1` .

   로그인 URL 샘플(/en-us/xenmobile/server/media/configure-sharefile-modify-sso-settings.png)

- XenMobile Server FQDN 앞에 Citrix Gateway 가상 서버 외부 FQDN과 **`/cginfra/https/`**을(를) 삽입한 다음 XenMobile FQDN 뒤에 **8443**을 추가합니다.

  편집된 URL 샘플은 다음과 같습니다: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

- 매개변수 `&app=ShareFile_SAML_SP`을(를) 내부 Citrix Files 애플리케이션 이름으로 변경합니다. 내부 이름은 기본적으로 `ShareFile_SAML`입니다. 그러나 구성을 변경할 때마다 내부 이름에 숫자가 추가됩니다(`ShareFile_SAML_2`, `ShareFile_SAML_3` 등). **구성 > ShareFile** 페이지에서 **앱 내부 이름**을 조회할 수 있습니다.

  편집된 URL 샘플은 다음과 같습니다: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- URL 끝에 `&nssso=true`을(를) 추가합니다.

  최종 URL 샘플은 다음과 같습니다: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. **선택적 설정**에서 **웹 인증 사용** 확인란을 선택합니다.

   선택적 설정 화면(/en-us/xenmobile/server/media/configure-sharefile-modify-optional-settings.png)

구성 유효성 검사

다음 단계를 수행하여 구성의 유효성을 검사합니다.

1. 브라우저를 `https://<subdomain>sharefile.com/saml/login`으로 이동합니다.

   Citrix Gateway 로그온 양식으로 리디렉션됩니다. 리디렉션되지 않으면 이전 구성 설정을 확인하십시오.

2. 구성한 Citrix Gateway 및 XenMobile 환경의 사용자 이름과 암호를 입력합니다.

   `<subdomain>.sharefile.com`에 있는 Citrix Files 폴더가 나타납니다. Citrix Files 폴더가 보이지 않으면 올바른 로그온 자격 증명을 입력했는지 확인하십시오.

IdP로서의 애저 액티브 디렉토리

Azure Active Directory(AAD)를 ID 공급자(IdP)로 구성하면 사용자가 Azure 자격 증명을 사용하여 XenMobile®에 등록할 수 있습니다.

iOS, Android, Windows 10 및 Windows 11 장치가 지원됩니다. iOS 및 Android 장치는 Secure Hub를 통해 등록됩니다. 이 인증 방법은 Citrix Secure Hub를 통해 MDM에 등록하는 사용자에게만 제공됩니다. MAM에 등록하는 장치는 AAD 자격 증명을 사용하여 인증할 수 없습니다. MDM+MAM과 함께 Secure Hub를 사용하려면 MAM 등록에 Citrix Gateway를 사용하도록 XenMobile을 구성하십시오. 자세한 내용은 Citrix Gateway 및 XenMobile을 참조하십시오.

설정 > 인증 > IDP에서 Azure를 IdP로 구성합니다. **IDP** 페이지는 이 XenMobile 버전에서 새로 추가되었습니다. 이전 XenMobile 버전에서는 **설정 > Microsoft Azure**에서 Azure를 구성했습니다.

요구 사항

- 버전 및 라이선스
  - iOS 또는 Android 장치를 등록하려면 Secure Hub 10.5.5가 필요합니다.
  - Windows 10 및 Windows 11 장치를 등록하려면 Microsoft Azure Premium 라이선스가 필요합니다.
- 디렉터리 서비스 및 인증
  - XenMobile Server는 인증서 기반 인증용으로 구성되어야 합니다.
  - 인증에 Citrix ADC를 사용하는 경우 Citrix ADC는 인증서 기반 인증용으로 구성되어야 합니다.
  - Secure Hub 인증은 Azure AD를 사용하며 Azure AD에 정의된 인증 모드를 따릅니다.
  - XenMobile Server는 LDAP를 사용하여 Windows Active Directory(AD)에 연결해야 합니다. 로컬 LDAP 서버를 Azure AD와 동기화하도록 구성하십시오.

인증 흐름

장치가 Secure Hub를 통해 등록되고 XenMobile이 Azure를 IdP로 사용하도록 구성된 경우:

1. 사용자는 Secure Hub에 표시된 Azure AD 로그인 화면에서 자신의 장치에 Azure Active Directory 사용자 이름과 암호를 입력합니다.
2. Azure AD는 사용자를 검증하고 ID 토큰을 보냅니다.
3. Secure Hub는 XenMobile Server와 ID 토큰을 공유합니다.
4. XenMobile은 ID 토큰과 ID 토큰에 있는 사용자 정보를 검증합니다. XenMobile은 세션 ID를 반환합니다.

Azure 계정 설정

Azure AD를 IdP로 사용하려면 먼저 Azure 계정에 로그인하여 다음 변경 사항을 적용하십시오.

1. 사용자 지정 도메인을 등록하고 도메인을 확인합니다. 자세한 내용은 Azure Active Directory에 사용자 지정 도메인 이름 추가를 참조하십시오.
2. 디렉터리 통합 도구를 사용하여 온프레미스 디렉터리를 Azure Active Directory로 확장합니다. 자세한 내용은 디렉터리 통합을 참조하십시오.

Azure AD를 사용하여 Windows 10 및 Windows 11 장치를 등록하려면 Azure 계정에 다음 변경 사항을 적용하십시오.

1. MDM을 Azure AD의 신뢰할 수 있는 당사자로 만듭니다. 이렇게 하려면 **Azure Active Directory > 애플리케이션**을 클릭한 다음 **추가**를 클릭합니다.
2. 갤러리에서 **애플리케이션 추가**를 선택합니다. **모바일 장치 관리**로 이동한 다음 **온프레미스 MDM 애플리케이션**을 선택합니다. 설정을 저장합니다.

   Citrix XenMobile 클라우드에 가입했더라도 온프레미스 애플리케이션을 선택합니다. Microsoft 용어에서 다중 테넌트가 아닌 모든 애플리케이션은 온프레미스 MDM 애플리케이션입니다.
3. 애플리케이션에서 XenMobile Server 검색, 사용 약관 엔드포인트 및 APP ID URI를 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. 2단계에서 생성한 온프레미스 MDM 애플리케이션을 선택합니다. 모든 사용자 또는 특정 사용자 그룹에 대해 MDM 관리를 사용하도록 설정하려면 **이러한 사용자의 장치 관리** 옵션을 활성화합니다.

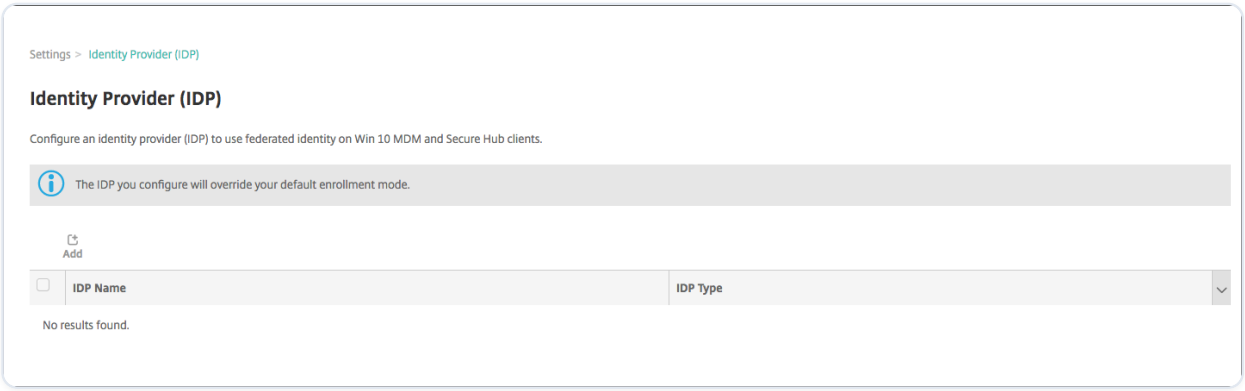
   Windows 10 및 Windows 11 장치에서 Azure AD를 사용하는 방법에 대한 자세한 내용은 Microsoft 문서 Azure Active Directory integration with MDM을 참조하십시오.

IdP로 Azure AD 구성

1. Azure 계정에서 필요한 정보를 찾거나 기록해 둡니다.

   - Azure 애플리케이션 설정 페이지의 테넌트 ID.
   - Azure AD를 사용하여 Windows 10 및 Windows 11 장치를 등록하려면 다음도 필요합니다.
     - **앱 ID URI:** XenMobile을 실행하는 서버의 URL입니다.
     - **클라이언트 ID:** Azure 구성 페이지에서 앱의 고유 식별자입니다.
     - **키:** Azure 애플리케이션 설정 페이지에서 가져옵니다.

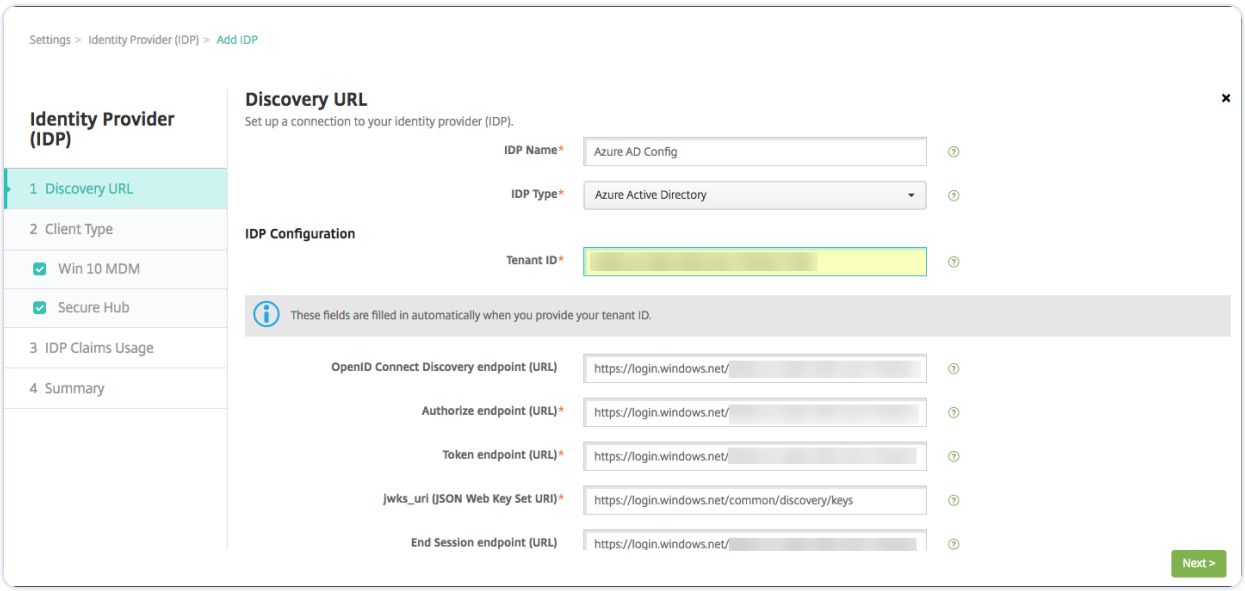
2. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
3. **인증** 아래에서 **ID 공급자(IDP)**를 클릭합니다. **ID 공급자** 페이지가 나타납니다.



4. **추가**를 클릭합니다. **IDP 구성** 페이지가 나타납니다.
5. IdP에 대한 다음 정보를 구성합니다.

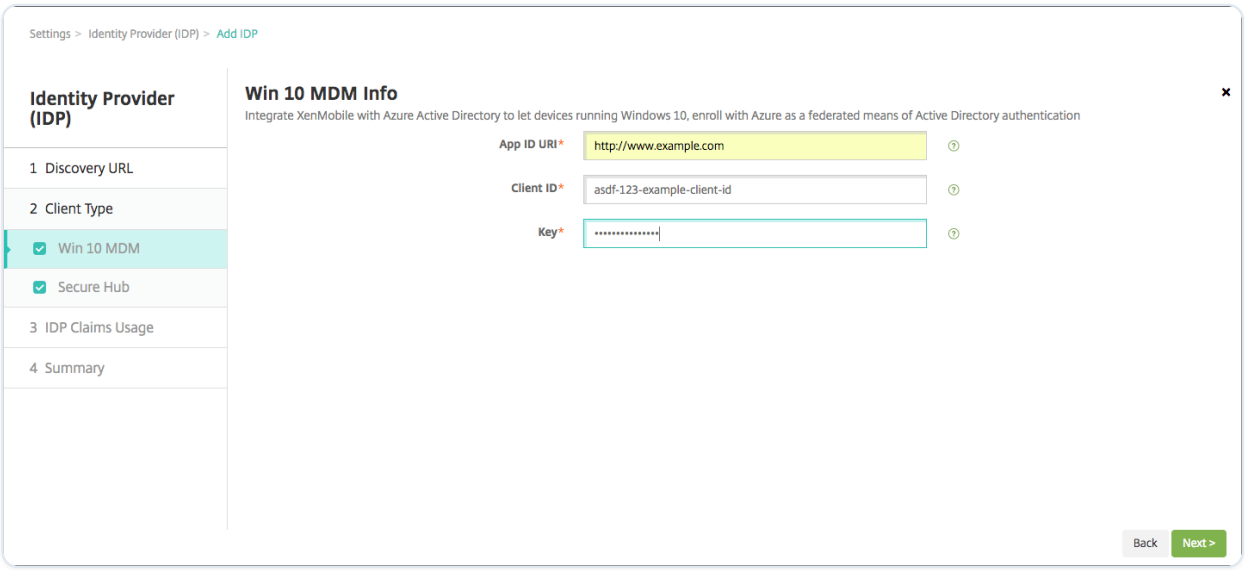
   - **IDP 이름:** 생성 중인 IdP 연결의 이름을 입력합니다.
   - **IDP 유형:** IdP 유형으로 Azure Active Directory를 선택합니다.
   - **테넌트 ID:** Azure 애플리케이션 설정 페이지에서 이 값을 복사합니다. 브라우저 주소 표시줄에서 숫자와 문자로 구성된 섹션을 복사합니다.

   예를 들어, `https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...`에서 테넌트 ID는 `abc123-abc123-abc123`입니다.



6. 나머지 필드는 자동으로 채워집니다. 필드가 채워지면 **다음**을 클릭합니다.
7. MDM 등록을 위해 Azure AD를 사용하여 Windows 10 및 Windows 11 장치를 등록하도록 XenMobile을 구성하려면 다음 설정을 구성합니다. 이 선택적 단계를 건너뛰려면 **Windows MDM**을 지웁니다.

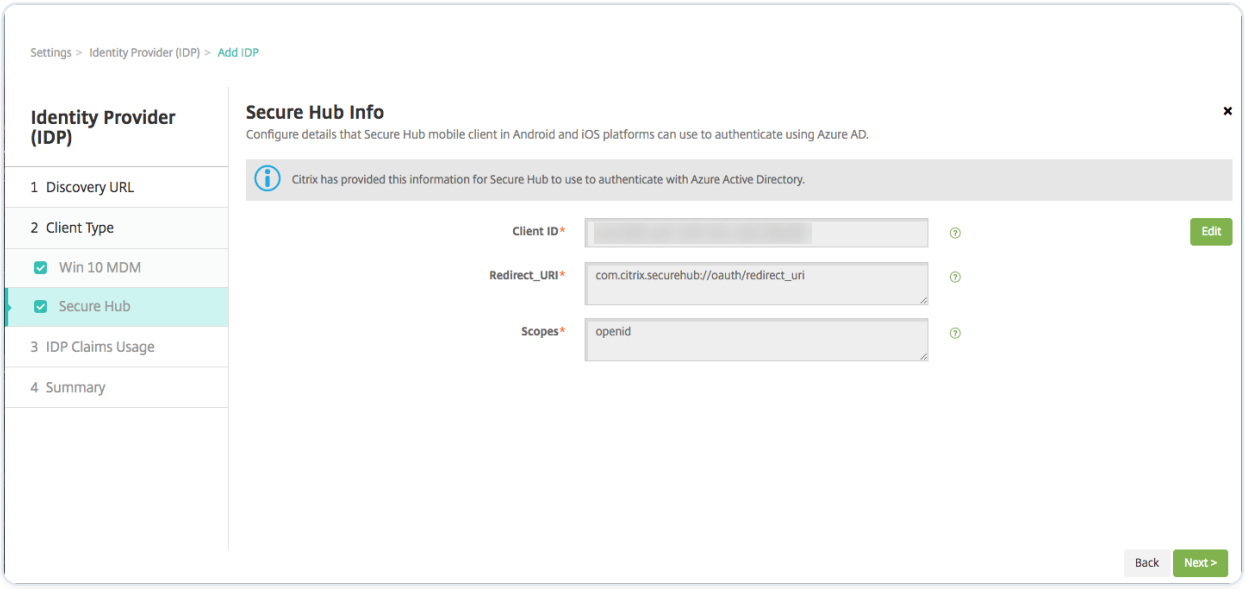
- **앱 ID URI:** Azure 설정을 구성할 때 입력한 XenMobile Server의 URL을 입력합니다.
- **클라이언트 ID:** Azure 구성 페이지에서 이 값을 복사하여 붙여넣습니다. 클라이언트 ID는 앱의 고유 식별자입니다.
- **키:** Azure 애플리케이션 설정 페이지에서 이 값을 복사합니다. 키 아래에서 목록에서 기간을 선택한 다음 설정을 저장합니다. 그런 다음 키를 복사하여 이 필드에 붙여넣을 수 있습니다. 앱이 Microsoft Azure AD에서 데이터를 읽거나 쓸 때 키가 필요합니다.



8. **다음**을 클릭합니다.

   Citrix는 Secure Hub를 Microsoft Azure에 등록하고 정보를 유지 관리합니다. 이 화면은 Secure Hub가 Azure Active Directory와 통신하는 데 사용하는 세부 정보를 보여줍니다. 이 페이지는 향후 이 정보 중 변경이 필요한 경우 사용됩니다. Citrix에서 지시하는 경우에만 이 페이지를 편집하십시오.

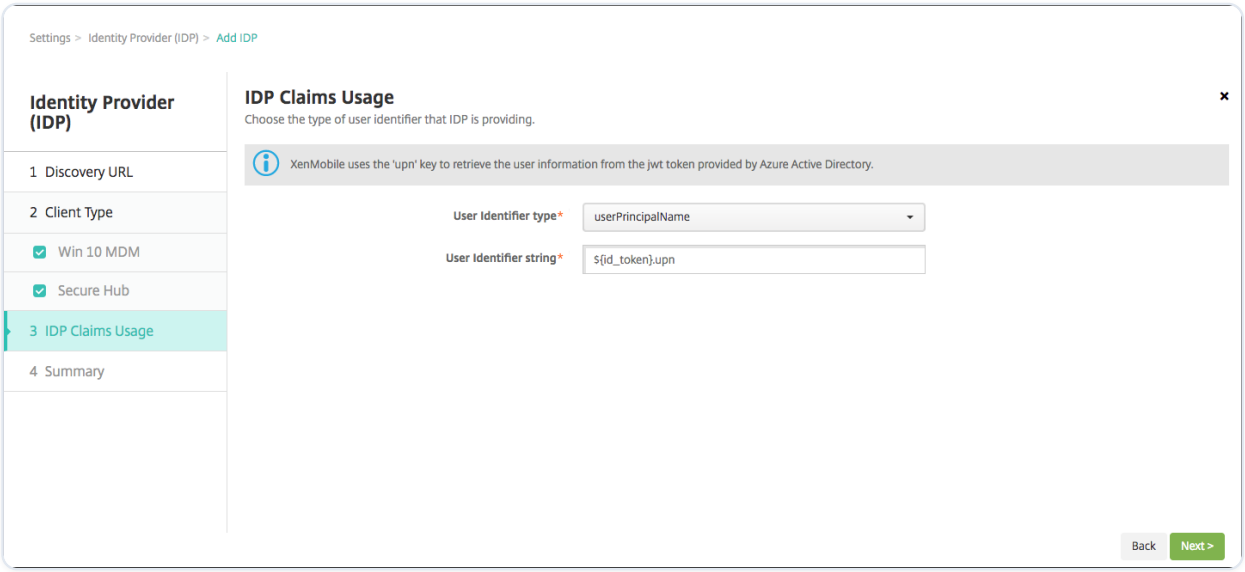
9. **다음**을 클릭합니다.



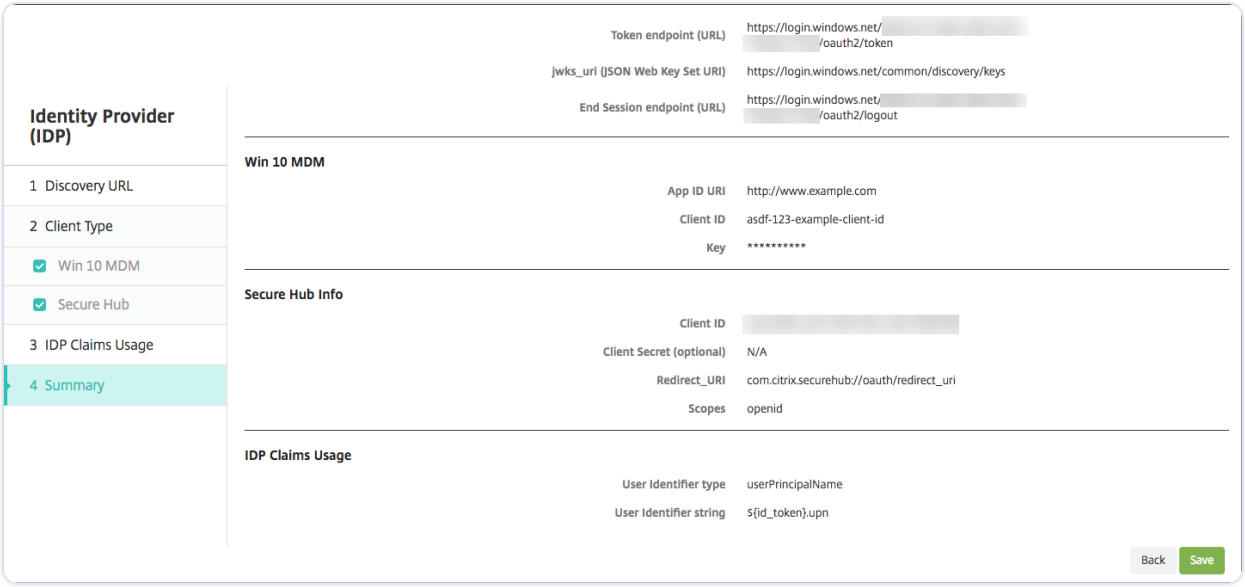
10. IdP가 제공하는 사용자 식별자 유형을 구성합니다:

- **사용자 식별자 유형:** 목록에서 **userPrincipalName**을 선택합니다.
- **사용자 식별자 문자열:** 이 필드는 자동으로 채워집니다.

11. **다음**을 클릭합니다.

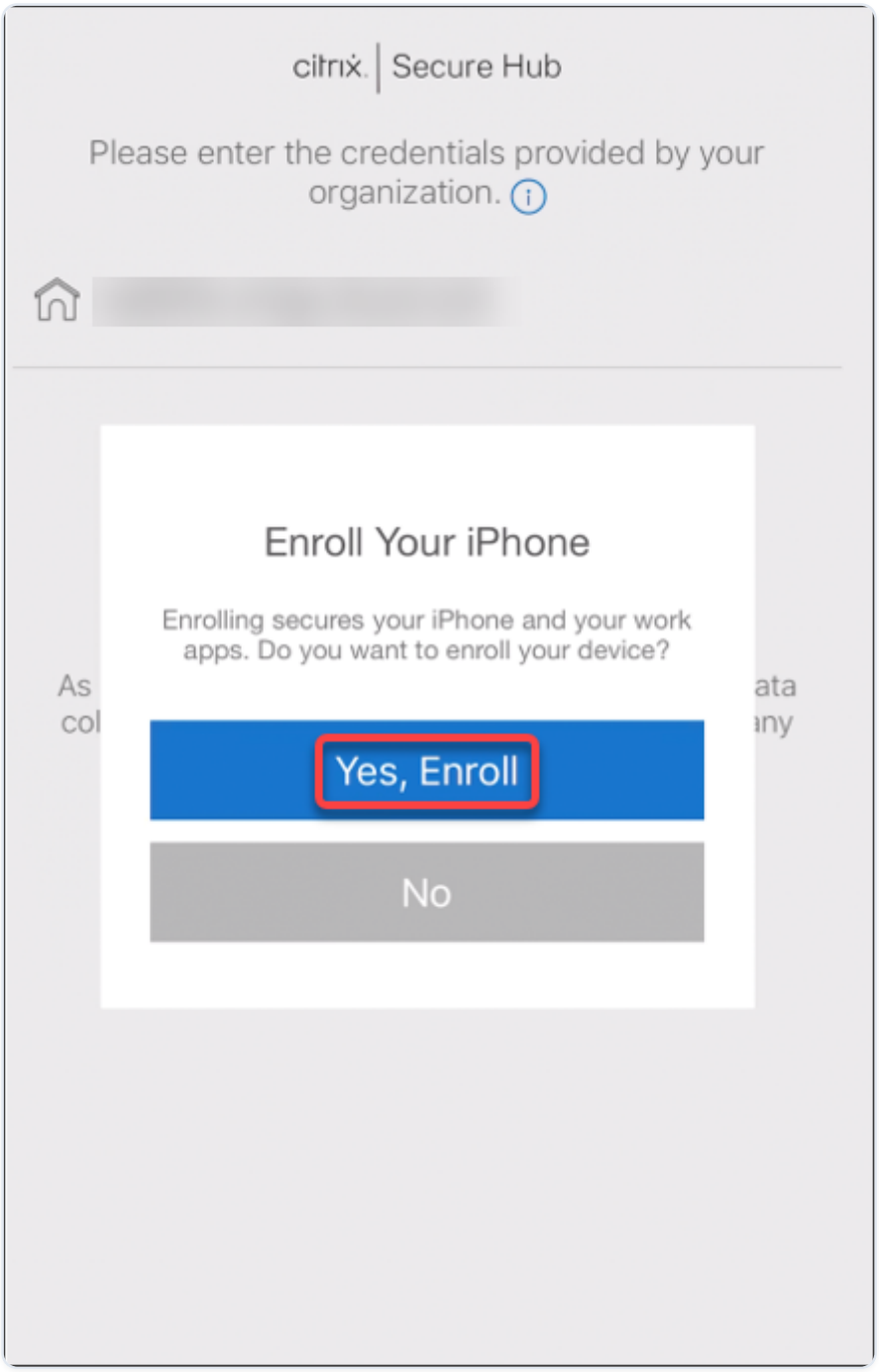


12. **요약** 페이지를 검토하고 **저장**을 클릭합니다.

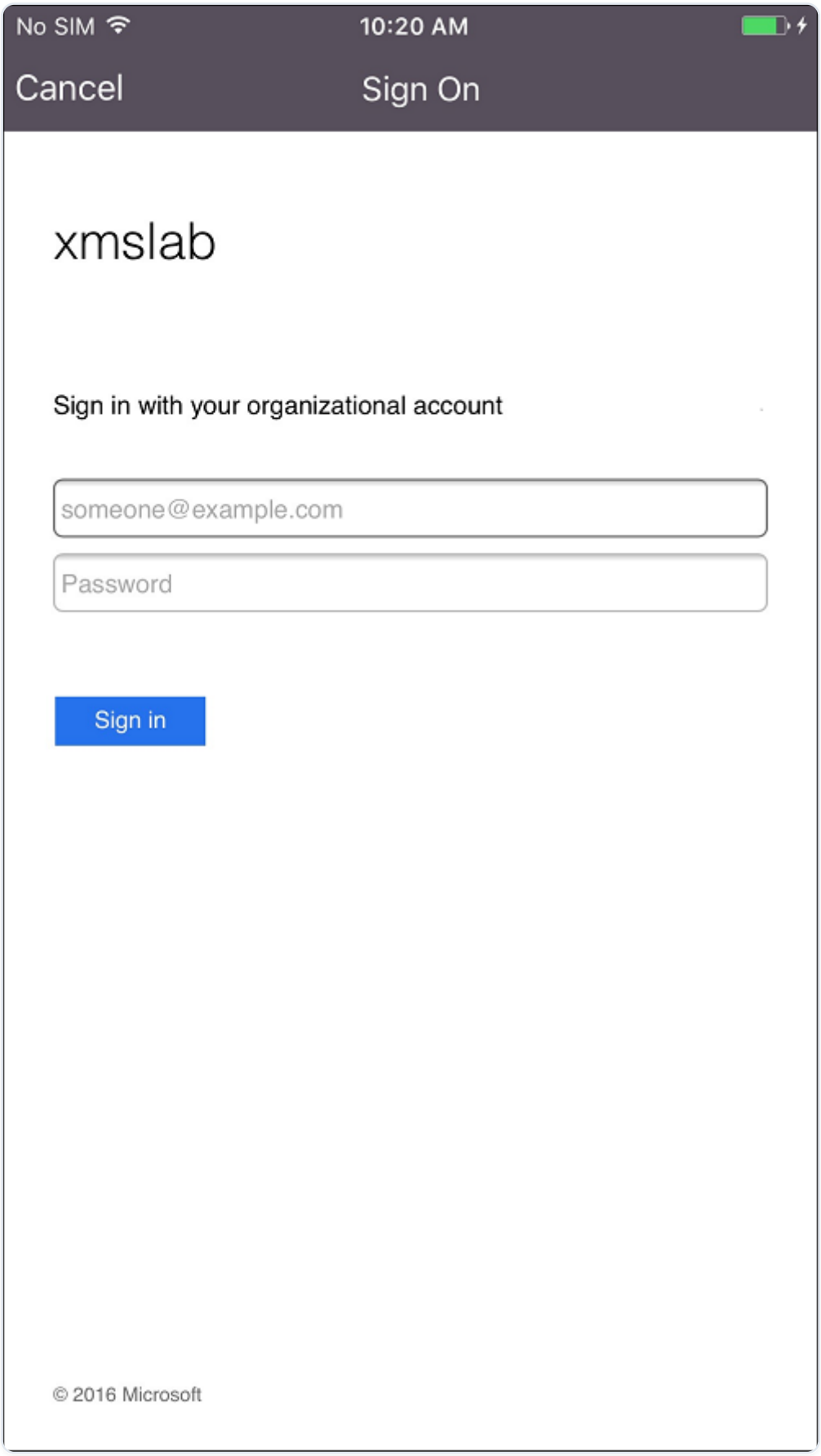


사용자 경험

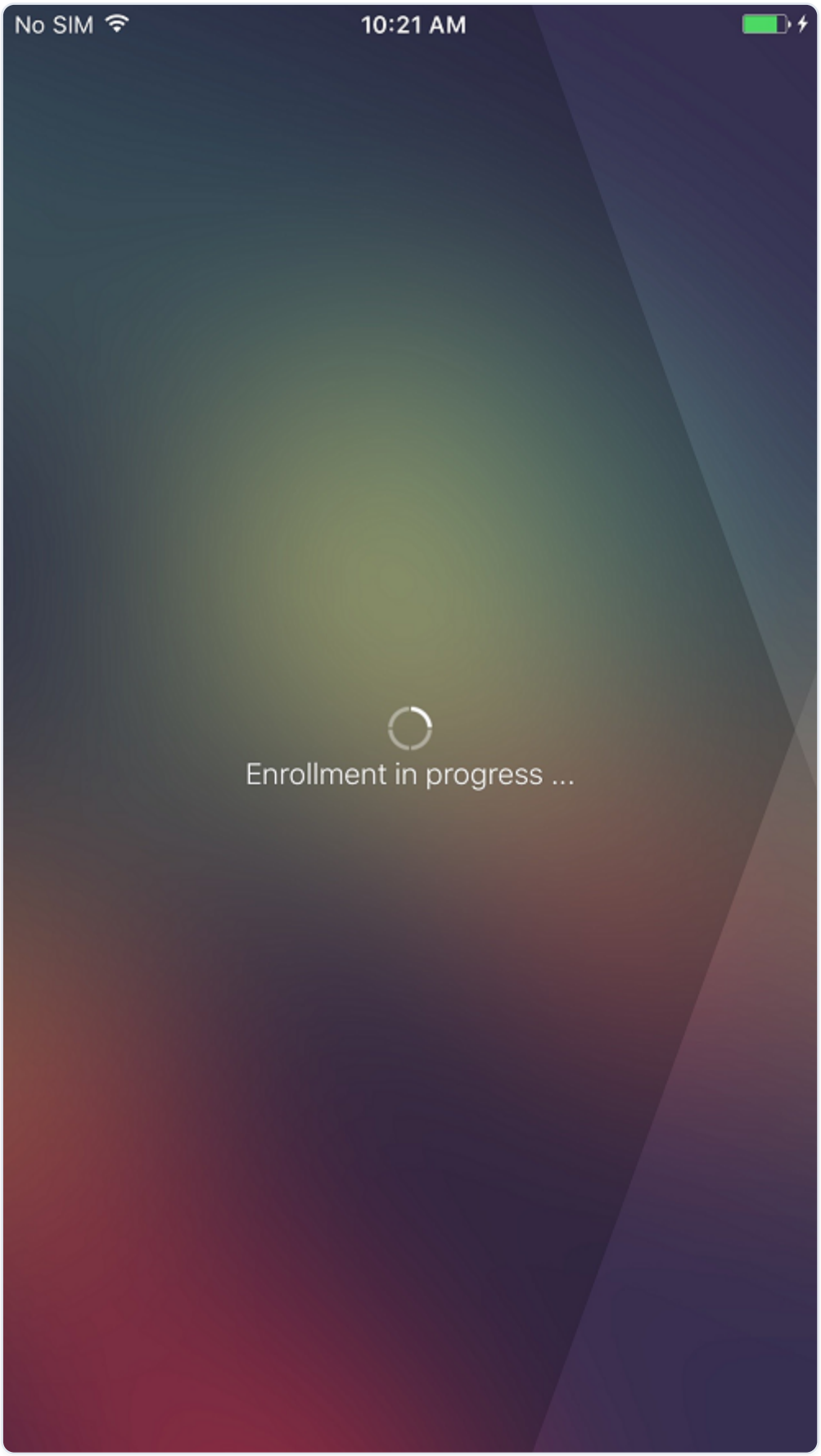
1. 사용자는 Secure Hub를 시작합니다. 그런 다음 XenMobile Server FQDN(정규화된 도메인 이름), UPN(사용자 계정 이름) 또는 이메일 주소를 입력합니다.

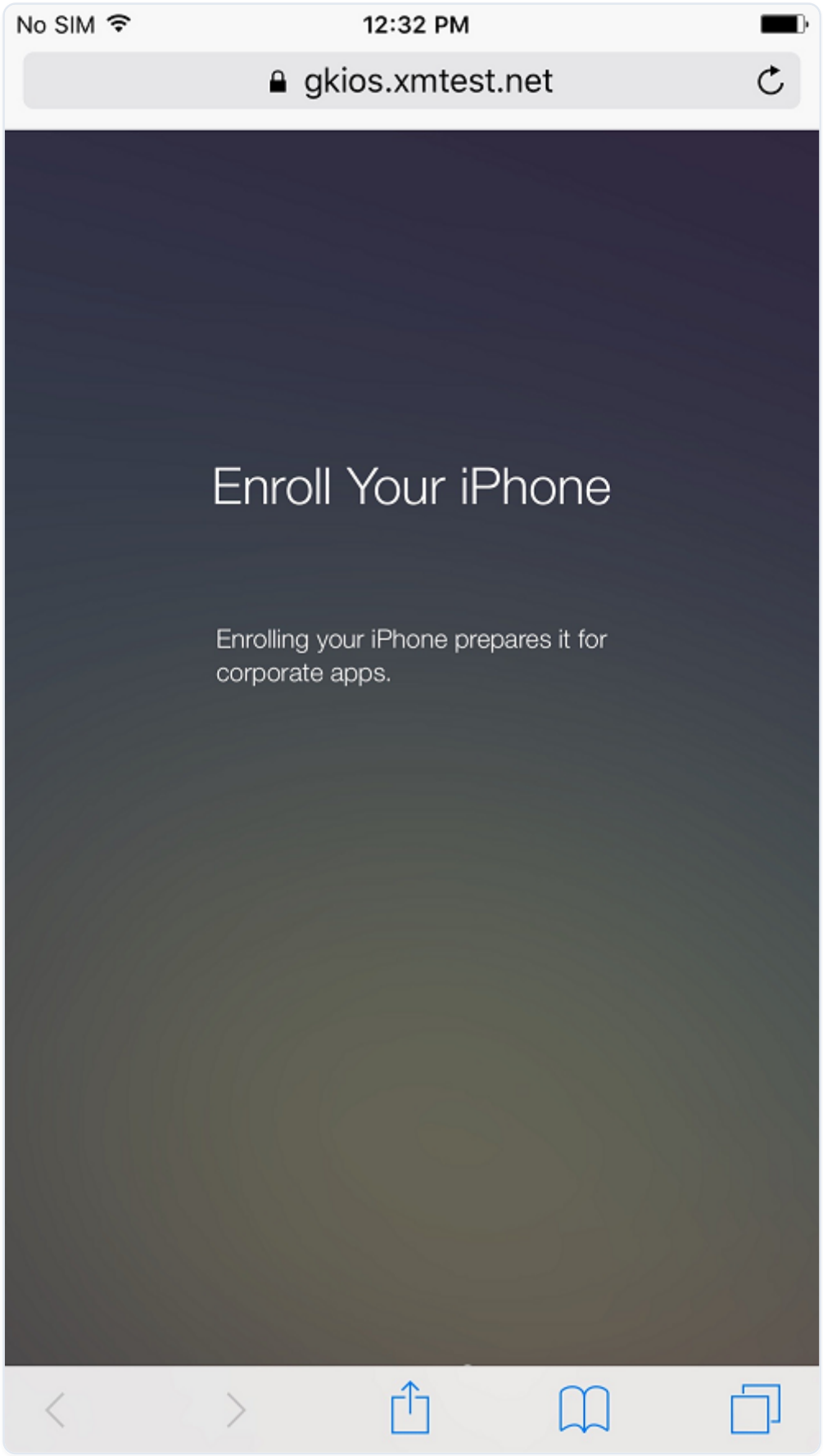


2. 사용자는 **예, 등록**을 클릭합니다.



3. 사용자는 Azure AD 자격 증명을 사용하여 로그인합니다.


No SIM
10:21 AM
Enrollment in progress ...



Secure Hub 화면 이미지(/en-us/xenmobile/server/media/secure-hub-ios-idp-enroll5.png)

4. 사용자는 Secure Hub를 통한 다른 등록과 동일한 방식으로 등록 단계를 완료합니다.

참고:

XenMobile은 등록 초대 시 Azure AD를 통한 인증을 지원하지 않습니다. 등록 URL이 포함된 등록 초대를 사용자에게 보내는 경우, 사용자는 Azure AD 대신 LDAP를 통해 인증합니다.

업그레이드

XenMobile 10.16으로 업그레이드하기 전에

1. XenMobile Server 10.16의 최신 버전으로 업데이트하기 전에 Citrix License Server를 11.17.2.0 Build 47000 이상으로 업데이트하십시오.

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

   XenMobile 10.16의 Customer Success Services 날짜(이전 Subscription Advantage 날짜)는 November 15, 2022입니다. Citrix 라이선스의 Customer Success Services 날짜는 이 날짜보다 늦어야 합니다. License Server에서 라이선스 옆에 있는 날짜를 확인할 수 있습니다. XenMobile 최신 버전을 이전 License Server 환경에 연결하면 연결 확인에 실패하고 License Server를 구성할 수 없습니다.

   라이선스 날짜를 갱신하려면 Citrix Portal에서 최신 라이선스 파일을 다운로드하여 Licensing Server에 업로드하십시오. 자세한 내용은 Customer Success Services를 참조하십시오.
2. 클러스터된 환경의 경우: iOS 11 이상을 실행하는 장치에 대한 iOS 정책 및 앱 배포에는 다음 요구 사항이 있습니다. Citrix Gateway가 SSL 지속성을 위해 구성된 경우, 모든 XenMobile® Server 노드에서 포트 80을 열어야 합니다.
3. 업그레이드할 XenMobile Server를 실행하는 가상 머신의 RAM이 8GB 미만인 경우, RAM을 최소 8GB로 늘리는 것이 좋습니다.
4. 권장 사항: XenMobile 업데이트를 설치하기 전에 VM의 기능을 사용하여 시스템 스냅샷을 만드십시오. 또한 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하면 전체 백업을 통해 복구할 수 있습니다.

업그레이드하려면

XenMobile 10.15.x 또는 10.14.x에서 XenMobile 10.16으로 직접 업그레이드할 수 있습니다. 업그레이드를 수행하려면 사용 가능한 최신 바이너리를 다운로드하십시오. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **Download File**을 클릭합니다. 업그레이드를 업로드하려면 XenMobile 콘솔의 **Release Management** 페이지를 사용하십시오.

Release Management 페이지를 사용하여 업그레이드하려면

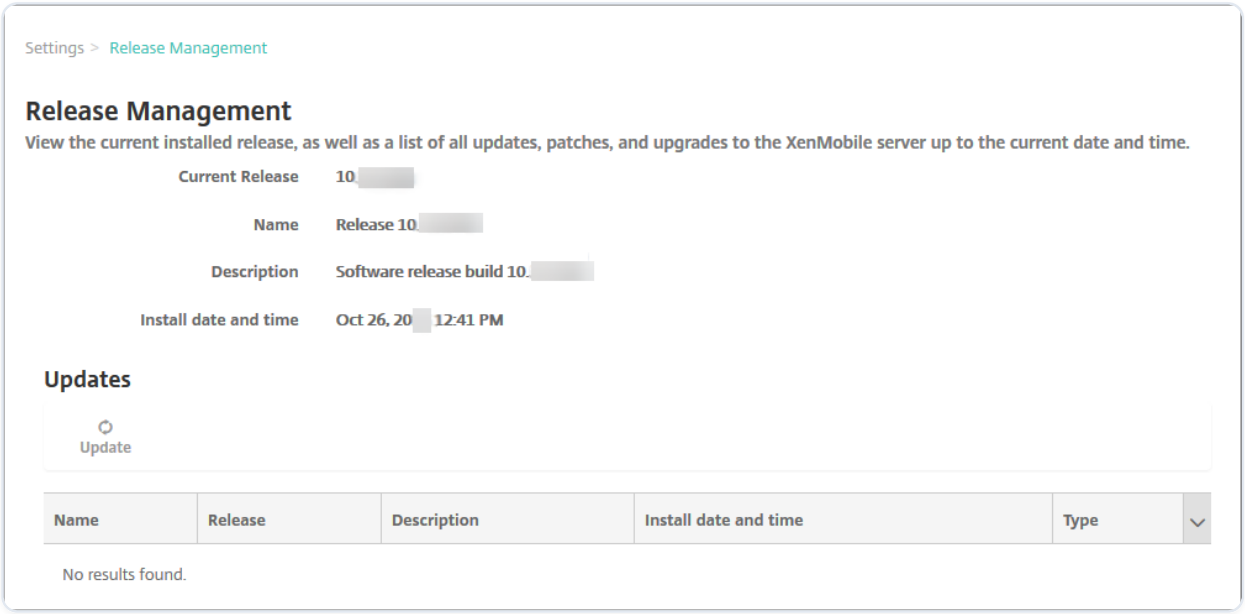
Release Management 페이지를 사용하여 XenMobile Server의 최신 버전으로 업그레이드하십시오.

전제 조건:

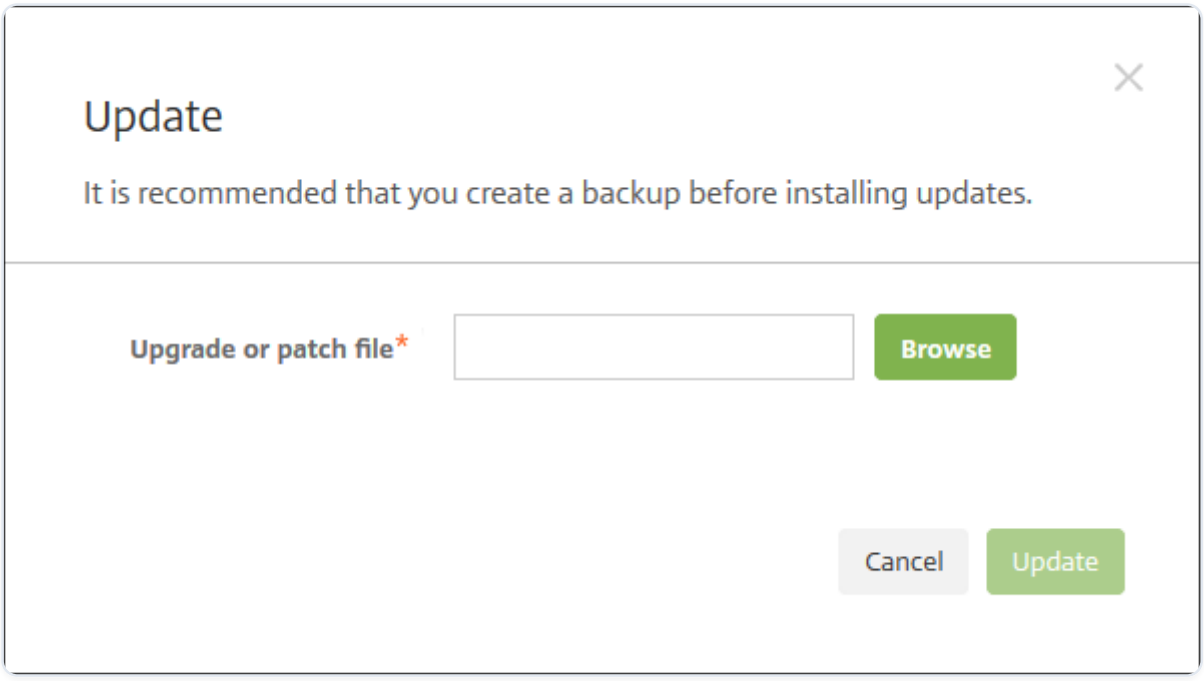
- 시스템 요구 사항을 검토하십시오.

클러스터형 배포를 사용하는 경우 이 문서의 끝에 있는 지침을 참조하십시오.

1. 사용 가능한 최신 바이너리를 다운로드합니다. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**으로 이동합니다. 하이퍼바이저용 XenMobile Server 소프트웨어 타일에서 **Download File**을 클릭합니다.
2. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **Settings** 페이지가 나타납니다.
3. **Release Management**를 클릭합니다. **Release Management** 페이지가 나타납니다.



4. **Updates**에서 **Update**를 클릭합니다. **Update** 대화 상자가 나타납니다.



5. **Browse**를 클릭하고 파일 위치로 이동하여 Citrix.com에서 다운로드한 XenMobile 업그레이드 파일을 선택합니다.
6. **Update**를 클릭한 다음 메시지가 표시되면 XenMobile을 다시 시작합니다.

   어떤 이유로든 업데이트를 성공적으로 완료할 수 없는 경우 문제 발생을 나타내는 오류 메시지가 나타납니다. 시스템은 업데이트 시도 이전 상태로 되돌려집니다.

업그레이드 후

업그레이드 후 XenMobile은 다시 시작해야 합니다. XenMobile CLI를 사용하여 XenMobile Server를 다시 시작하십시오. 시스템을 다시 시작한 후 브라우저 캐시를 지우는 것이 중요합니다.

아웃바운드 연결과 관련된 기능이 작동을 멈추고 연결 구성을 변경하지 않은 경우, **XenMobile Server 로그**에서 다음과 같은 오류를 확인하십시오: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer"

인증서 유효성 검사 오류는 XenMobile Server에서 호스트 이름 확인을 비활성화해야 함을 나타냅니다. 기본적으로 호스트 이름 확인은 Microsoft PKI 서버를 제외한 아웃바운드 연결에서 활성화됩니다. 호스트 이름 확인으로 인해 배포가 중단되는 경우 서버 속성 **disable.hostname.verification**을 **true**로 변경하십시오. 이 속성의 기본값은 **false**입니다.

Citrix는 XenMobile의 새 버전 또는 중요한 업데이트를 Citrix.com에 게시합니다. 동시에 각 고객의 등록된 담당자에게 알림이 전송됩니다.

클러스터링된 XenMobile 배포를 업그레이드하는 방법

> **중요:**
>
> XenMobile 업데이트를 설치하기 전에, 가상 머신(VM)의 기능을 사용하여 시스템 스냅샷을 생성하십시오. 또한, 시스템 구성 데이터베이스를 백업하십시오. 업그레이드 중에 문제가 발생하면, 완전한 백업을 통해 복구할 수 있습니다.

> 시스템이 클러스터 모드로 구성된 경우, XenMobile 10 릴리스에서 각 노드를 업데이트하려면 다음 단계를 따르십시오.

1. **설정 > 릴리스 관리**에서 모든 노드에 .bin 파일을 업로드합니다.
2. CLI의 **시스템 메뉴**에서 모든 노드를 종료합니다.
3. CLI의 **시스템 메뉴**에서 하나의 노드를 시작하고 서비스가 실행 중인지 확인합니다.
4. 다른 노드들을 차례로 시작합니다.

   XenMobile이 업데이트를 성공적으로 완료할 수 없는 경우, 문제를 나타내는 오류 메시지가 나타납니다. 그러면 XenMobile은 시스템을 업데이트 시도 이전 상태로 되돌립니다.

XenMobile MDM Edition에서 Enterprise Edition으로 업그레이드

iOS 및 Android 장치의 경우 XenMobile MDM Edition을 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 > 라이선싱**으로 이동하여 올바른 Enterprise Edition 라이선스 유형이 업로드되었는지 확인합니다.
2. **설정 > 서버 속성**으로 이동하여 **서버 모드** 속성을 **MDM**에서 **ENT**로 변경합니다.

3. **설정 > Citrix Gateway**로 이동하여 Citrix Gateway 세부 정보를 구성합니다. 인증 모드를 MDM Edition과 동일하게, 즉 도메인(Active Directory) 인증으로 설정합니다. XenMobile은 사용자 등록 후 인증 모드 변경을 지원하지 않습니다.
4. 선택 사항: **설정 > 클라이언트 속성**으로 이동하여 Citrix PIN 인증을 활성화합니다.

이 단계를 완료한 후, 사용자는 장치를 Enterprise 모드로 전환하기 위해 다음 단계를 수행해야 합니다.

iOS 사용자

1. Secure Hub 닫기: 장치 홈 버튼을 두 번(빠르게) 탭하고 Secure Hub 앱을 위로 밉니다.
2. Secure Hub를 엽니다.

Android 사용자

1. Secure Hub를 엽니다.
2. **기본 설정 > 장치 정보**로 이동합니다.
3. **정책 새로 고침**을 클릭합니다.

Citrix PIN 인증을 활성화한 경우, Secure Hub는 사용자에게 PIN 생성을 요청합니다. 사용자가 PIN을 생성하면 XenMobile은 장치를 Enterprise 모드로 구성합니다. XenMobile 콘솔의 **관리 > 장치** 페이지에는 해당 장치에 대해 MDM과 MAM이 모두 활성 상태로 표시됩니다.

사용자 계정, 역할 및 등록

XenMobile® 콘솔의 **관리** 탭과 **설정** 페이지에서 사용자 계정, 역할 및 등록을 구성합니다. 별도로 명시되지 않는 한, 다음 작업에 대한 단계는 이 문서에 제공됩니다.

- 사용자 계정 및 그룹:
  - **관리 > 사용자**에서 사용자 계정을 수동으로 추가하거나 .csv 프로비저닝 파일을 사용하여 계정을 가져오고 로컬 그룹을 관리합니다.
  - **설정 > 워크플로**에서 워크플로를 사용하여 사용자 계정 생성 및 제거를 관리합니다.
- 사용자 계정 및 그룹의 역할
  - **설정 > 역할 기반 액세스 제어**에서 사용자 및 그룹에 미리 정의된 역할 또는 권한 집합을 할당합니다. 이러한 권한은 사용자가 시스템 기능에 액세스할 수 있는 수준을 제어합니다. 자세한 내용은 RBAC를 사용하여 역할 구성을 참조하십시오.
  - **설정 > 알림 템플릿**에서 자동화된 작업, 등록 및 사용자에게 전송되는 표준 알림 메시지에 사용할 알림 템플릿을 생성하거나 업데이트합니다. Secure Hub, SMTP 또는 SMS의 세 가지 채널을 통해 메시지를 보내도록 알림 템플릿을 구성합니다. 자세한 내용은 알림 템플릿 생성 및 업데이트를 참조하십시오.
- 등록 보안 모드 및 초대
  - **설정 > 등록**에서 최대 7개의 등록 보안 모드를 구성하고 등록 초대를 보냅니다. 각 등록 보안 모드에는 고유한 보안 수준과 사용자가 장치를 등록하기 위해 수행해야 하는 단계가 있습니다.
  - 사용자 등록을 위해 XenMobile에서 AutoDiscovery 사용

로컬 사용자 계정 추가, 편집, 잠금 해제 또는 삭제

XenMobile에 로컬 사용자 계정을 수동으로 추가하거나 프로비저닝 파일을 사용하여 계정을 가져올 수 있습니다. 프로비저닝 파일에서 사용자 계정을 가져오는 단계는 사용자 계정 가져오기를 참조하십시오.

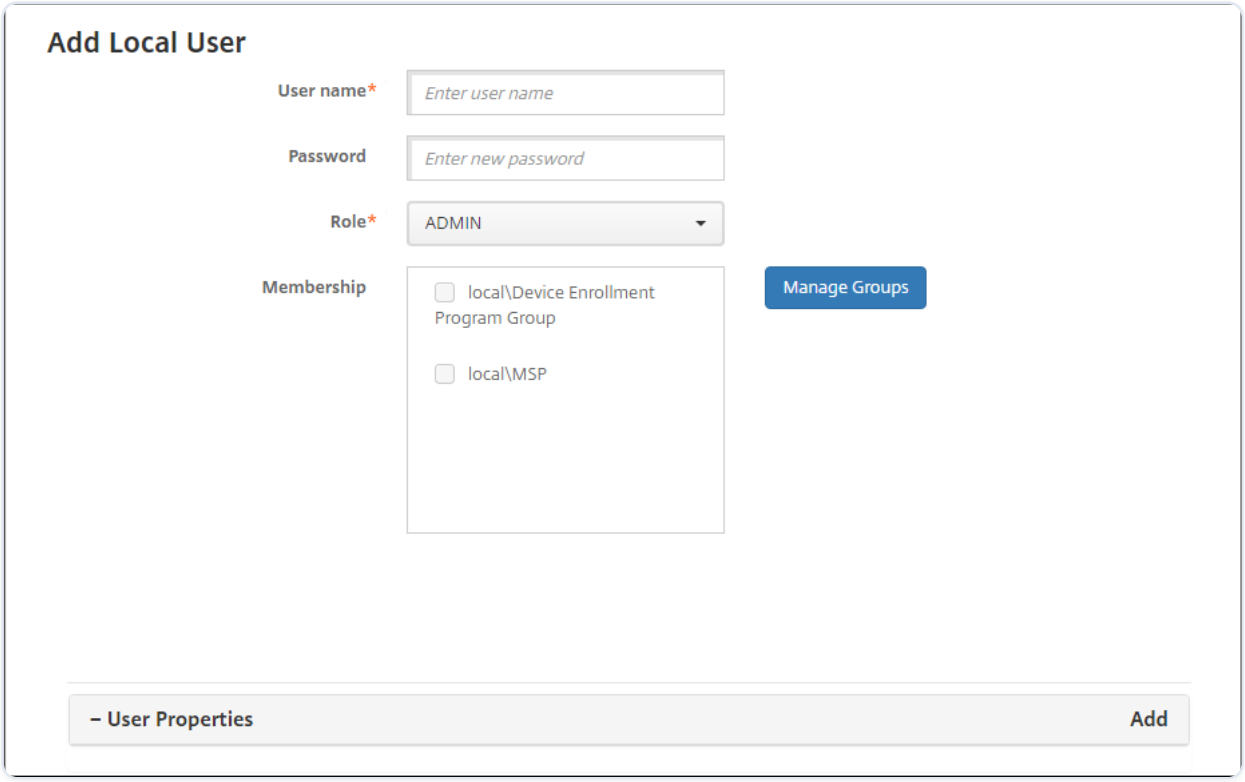
1. XenMobile 콘솔에서 **관리 > 사용자**를 클릭합니다. **사용자** 페이지가 나타납니다.

   (/en-us/xenmobile/server/media/manage-users-list.png)

2. **필터 표시**를 클릭하여 목록을 필터링합니다.

로컬 사용자 계정을 추가하려면

1. **사용자** 페이지에서 **로컬 사용자 추가**를 클릭합니다. **로컬 사용자 추가** 페이지가 나타납니다.



2. 다음 설정을 구성합니다.

- **사용자 이름:** 이름을 입력합니다(필수 필드). 이름에는 대소문자 외에 공백을 포함할 수 있습니다.
- **암호:** 선택 사항인 사용자 암호를 입력합니다. 암호는 14자 이상이어야 하며 다음 모든 조건을 충족해야 합니다.
  - 두 개 이상의 숫자를 포함해야 합니다.
  - 하나 이상의 대문자와 하나 이상의 소문자를 포함해야 합니다.
  - 하나 이상의 특수 문자를 포함해야 합니다.
  - 사전 단어 또는 제한된 단어(예: Citrix® 사용자 이름 또는 이메일 주소)를 포함하지 마십시오.
  - 세 개를 초과하는 연속 및 반복 문자 또는 키보드 패턴(예: 1111, 1234 또는 asdf)을 포함하지 마십시오.
- **역할:** 목록에서 사용자 역할을 클릭합니다. 역할에 대한 자세한 내용은 RBAC를 사용하여 역할 구성을 참조하십시오. 가능한 옵션은 다음과 같습니다.
  - ADMIN
  - DEVICE_PROVISIONING
  - 지원

    - 사용자

- **멤버십:** 목록에서 사용자를 추가할 그룹을 클릭합니다.
- **사용자 속성:** 선택적 사용자 속성을 추가합니다. 추가하려는 각 사용자 속성에 대해 **추가**를 클릭하고 다음을 수행합니다.

    - **사용자 속성:** 목록에서 속성을 클릭한 다음 속성 옆 필드에 사용자 속성 특성을 입력합니다.
    - 사용자 속성을 저장하려면 **완료**를 클릭하거나 **취소**를 클릭합니다.

  기존 사용자 속성을 삭제하려면 속성이 포함된 줄 위로 마우스를 가져간 다음 오른쪽에 있는 X를 클릭합니다. 속성이 즉시 삭제됩니다.

  기존 사용자 속성을 편집하려면 속성을 클릭하고 변경합니다. 변경 사항을 저장하려면 **완료**를 클릭하거나 변경하지 않고 목록을 유지하려면 **취소**를 클릭합니다.

3. **저장**을 클릭합니다.

로컬 사용자 계정을 편집하려면

1. **사용자** 페이지의 사용자 목록에서 사용자를 선택한 다음 **편집**을 클릭합니다. **로컬 사용자 편집** 페이지가 나타납니다.

   사용자 구성 페이지 이미지(/en-us/xenmobile/server/media/manage-users-edit-local.png)

2. 필요에 따라 다음 정보를 변경합니다.

    - **사용자 이름:** 사용자 이름을 변경할 수 없습니다.
    - **암호:** 사용자 암호를 변경하거나 추가합니다.
    - **역할:** 목록에서 사용자 역할을 클릭합니다.
    - **멤버십:** 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 해당 속성을 클릭하고 변경합니다. 변경된 목록을 저장하려면 **완료**를 클릭하고, 목록을 변경하지 않고 유지하려면 **취소**를 클릭합니다.
        - 추가하려는 각 사용자 속성에 대해 **추가**를 클릭하고 다음을 수행합니다.

            - **사용자 속성:** 목록에서 속성을 클릭한 다음 속성 옆 필드에 사용자 속성 특성을 입력합니다.
            - 사용자 속성을 저장하려면 **완료**를 클릭하고, 그렇지 않으면 **취소**를 클릭합니다.

        - 삭제하려는 기존 사용자 속성에 대해 해당 속성이 포함된 줄 위로 마우스를 가져간 다음 오른쪽에 있는 **X**를 클릭합니다. 속성이 즉시 삭제됩니다.

3. 변경 내용을 저장하려면 **저장**을 클릭하고, 사용자를 변경하지 않고 유지하려면 **취소**를 클릭합니다.

로컬 사용자 계정 잠금 해제

1. **사용자** 페이지의 사용자 계정 목록에서 사용자 계정을 클릭하여 선택합니다.
2. **로컬 사용자 잠금 해제**를 클릭합니다. 확인 대화 상자가 나타납니다.
3. 사용자 계정 잠금을 해제하려면 **잠금 해제**를 클릭하고, 사용자를 변경하지 않고 유지하려면 **취소**를 클릭합니다.

로컬 사용자 계정 삭제

1. **사용자** 페이지의 사용자 계정 목록에서 사용자 계정을 클릭하여 선택합니다.

각 사용자 계정 옆의 확인란을 선택하여 삭제할 사용자 계정을 두 개 이상 선택할 수 있습니다.

1. **삭제**를 클릭합니다. 확인 대화 상자가 나타납니다.
2. 사용자 계정을 삭제하려면 **삭제**를 클릭하거나 **취소**를 클릭합니다.

Active Directory 사용자 삭제

한 번에 하나 이상의 Active Directory 사용자를 삭제하려면 사용자를 선택하고 **삭제**를 클릭합니다.

삭제하는 사용자가 등록된 장치를 가지고 있고 해당 장치를 다시 등록하려면, 다시 등록하기 전에 장치를 삭제하십시오. 장치를 삭제하려면 **관리 > 장치**로 이동하여 장치를 선택한 다음 **삭제**를 클릭합니다.

사용자 계정 가져오기

수동으로 만들 수 있는 프로비저닝 파일이라는 .csv 파일에서 로컬 사용자 계정 및 속성을 가져올 수 있습니다. 프로비저닝 파일 형식에 대한 자세한 내용은 프로비저닝 파일 형식을 참조하십시오.

> **참고:**

- 로컬 사용자의 경우 가져오기 파일에서 사용자 이름과 함께 도메인 이름을 사용합니다. 예를 들어, username@domain을 지정합니다. 생성하거나 가져오는 로컬 사용자가 XenMobile의 관리되는 도메인에 속하는 경우, 해당 LDAP 자격 증명을 사용하여 등록할 수 없습니다.
- XenMobile 내부 사용자 디렉터리로 사용자 계정을 가져오는 경우, 가져오기 프로세스 속도를 높이려면 기본 도메인을 비활성화합니다. 도메인을 비활성화하면 등록에 영향을 미치므로 내부 사용자 가져오기가 완료된 후 기본 도메인을 다시 활성화해야 합니다.

- 로컬 사용자는 UPN(User Principal Name) 형식일 수 있습니다. 그러나 Citrix는 관리되는 도메인을 사용하지 않는 것이 좋습니다. 예를 들어, example.com이 관리되는 경우 user@example.com과 같은 UPN 형식으로 로컬 사용자를 만들지 마십시오.

프로비저닝 파일을 준비한 후 다음 단계에 따라 파일을 XenMobile로 가져옵니다.

1. XenMobile 콘솔에서 **관리 > 사용자**를 클릭합니다. **사용자** 페이지가 나타납니다.
2. **로컬 사용자 가져오기**를 클릭합니다. **프로비저닝 파일 가져오기** 대화 상자가 나타납니다.

   사용자 관리 이미지(/en-us/xenmobile/server/media/local-users-and-groups-import-provisioning-file.png)
3. 가져올 프로비저닝 파일 형식으로 **사용자** 또는 **속성** 중 하나를 선택합니다.
4. 사용할 프로비저닝 파일을 선택하려면 **찾아보기**를 클릭한 다음 파일 위치로 이동합니다.
5. **가져오기**를 클릭합니다.

프로비저닝 파일 형식

수동으로 프로비저닝 파일을 생성하여 XenMobile로 사용자 계정 및 속성을 가져올 수 있습니다. 유효한 형식은 다음과 같습니다.

- **사용자 프로비저닝 파일 필드:** `user;password;role;group1;group2`
- **사용자 속성 프로비저닝 파일 필드:**
  `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

참고:

- 프로비저닝 파일 내의 필드는 세미콜론(;)으로 구분합니다. 필드 일부에 세미콜론이 포함된 경우 백슬래시 문자(\\)로 이스케이프 처리합니다. 예를 들어, 프로비저닝 파일에서 속성 `propertyV;test;1;2`을 `propertyV\\;test\\;1\\;2`로 입력합니다.
- **역할**에 대한 유효한 값은 미리 정의된 USER, ADMIN, SUPPORT, DEVICE_PROVISIONING 역할과 사용자가 정의한 다른 모든 역할입니다.
- 그룹 계층을 만들려면 마침표(.) 문자를 구분 기호로 사용합니다. 그룹 이름에 마침표를 사용하지 마십시오.
- 속성 프로비저닝 파일의 속성 특성에는 소문자를 사용합니다. 데이터베이스는 대소문자를 구분합니다.

사용자 프로비저닝 콘텐츠 예시

항목 `user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` 은 다음을 의미합니다.

- **사용자:** `user01`
- **암호:** `pwd;01`
- **역할:** `USER`
- **그룹:**
  - `myGroup.users01`
  - `myGroup.users02`
  - `myGroup.users.users.users01`

다른 예로, `AUser0;1.password;USER;ActiveDirectory.test.net` 은(는) 다음을 의미합니다:

- **사용자:** `AUser0`
- **암호:** `1.password`
- **역할:** `USER`
- **그룹:** `ActiveDirectory.test.net`

사용자 속성 프로비저닝 콘텐츠 예시

항목 `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` 은(는) 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

XenMobile에서 장치 등록을 위한 보안 수준 및 알림 템플릿을 지정하도록 장치 등록 보안 모드를 구성합니다.

XenMobile은 각각 고유한 보안 수준과 사용자가 장치를 등록하기 위해 수행해야 하는 단계를 가진 7가지 등록 보안 모드를 제공합니다. XenMobile Server 콘솔의 **설정 > 등록** 페이지에서 등록 보안 모드를 구성합니다.

일부 모드는 셀프 서비스 포털에서 사용할 수 있습니다. 포털에서 사용자는 장치를 등록할 수 있는 등록 링크를 생성합니다. iOS, iPadOS, macOS, Android Enterprise 및 레거시 Android 사용자는 포털에서 등록 초대장을 자신에게 보낼 수 있습니다. Windows 장치에는 등록 초대장을 사용할 수 없습니다.

관리 > 등록 초대 페이지에서 등록 초대장을 보냅니다. 자세한 내용은 등록 초대 보내기를 참조하십시오.

> **참고:**
>
> 사용자 지정 알림 템플릿을 사용할 계획이라면 등록 보안 모드를 구성하기 전에 템플릿을 설정해야 합니다. 알림 템플릿에 대한 자세한 내용은 알림 템플릿 생성 또는 업데이트를 참조하십시오.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **등록**을 클릭합니다. 사용 가능한 모든 등록 보안 모드 테이블이 포함된 **등록** 페이지가 나타납니다. 기본적으로 모든 등록 보안 모드는 활성화되어 있습니다.
3. 목록에서 등록 보안 모드를 선택하여 편집합니다. 그런 다음 해당 모드를 기본값으로 설정하거나, 모드를 비활성화하거나, Self-Help Portal을 통해 사용자 액세스를 허용할 수 있습니다.

   > **참고:**
   >
   > 등록 보안 모드 옆의 확인란을 선택하면 등록 보안 모드 목록 위에 옵션 메뉴가 나타납니다. 목록의 다른 곳을 클릭하면 옵션 메뉴가 목록의 오른쪽에 나타납니다.

   > 등록 설정 이미지(/en-us/xenmobile/server/media/settings-enrollment.png)

   다음 등록 보안 모드 중에서 선택하십시오:

   - 사용자 이름 + 암호

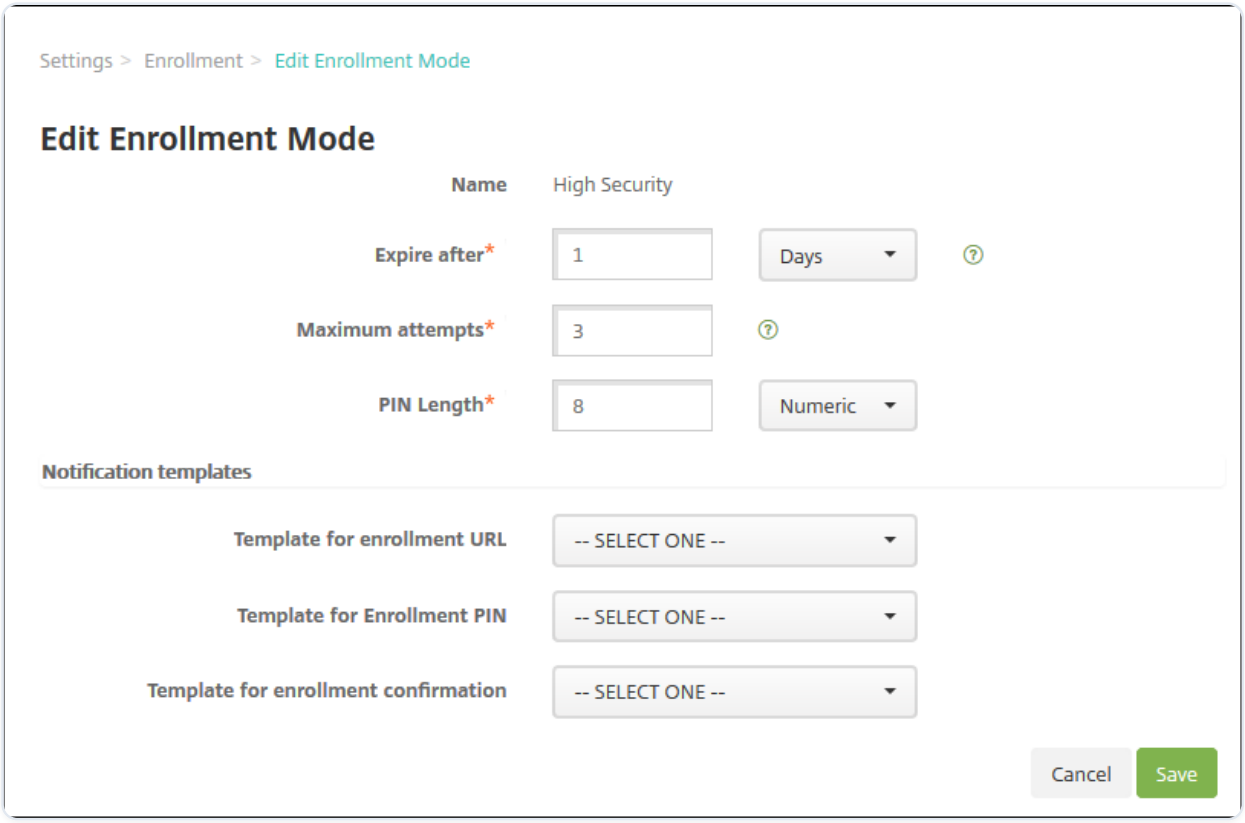
- 높은 보안
- 초대 URL
- 초대 URL + PIN
- 초대 URL + 암호
- 2단계 인증
- 사용자 이름 + PIN

등록 초대를 사용하여 초대받은 사용자에게만 등록을 제한할 수 있습니다. 등록 초대를 보내려면 **초대 URL**, **초대 URL + PIN** 또는 **초대 URL + 암호** 등록 보안 모드만 사용할 수 있습니다. **사용자 이름 + 암호**, **2단계 인증** 또는 **사용자 이름 + PIN**으로 등록하는 장치의 경우, 사용자는 Secure Hub에 자격 증명을 수동으로 입력해야 합니다.

일회용 PIN(OTP) 등록 초대를 2단계 인증 솔루션으로 사용할 수 있습니다. OTP 등록 초대는 사용자가 등록할 수 있는 장치 수를 제어합니다. OTP 초대는 Windows 장치에서는 사용할 수 없습니다.

등록 보안 모드를 편집하려면

1. **등록** 목록에서 등록 보안 모드를 선택한 다음 **편집**을 클릭합니다. **등록 모드 편집** 페이지가 나타납니다. 선택한 모드에 따라 표시되는 옵션이 결정됩니다.



2. 필요에 따라 다음 정보를 변경합니다.

- **만료 기간:** 사용자가 장치를 등록할 수 없게 되는 만료 기한을 입력합니다. 이 값은 사용자 및 그룹 등록 초대 구성 페이지에 나타납니다.

  초대가 만료되지 않도록 **0**을 입력합니다.
- **일:** 목록에서 **일** 또는 **시간**을 클릭하여 **만료 기간**에 입력한 만료 기한에 해당하도록 합니다.
- **최대 시도 횟수:** 사용자가 등록 프로세스에서 잠기기 전에 시도할 수 있는 등록 시도 횟수를 입력합니다. 이 값은 사용자 및 그룹 등록 초대 구성 페이지에 나타납니다.

  무제한 시도를 허용하려면 **0**을 입력합니다.
- **PIN 길이:** 생성된 PIN의 길이를 설정할 숫자를 입력합니다.
- **숫자:** 목록에서 PIN 유형으로 **숫자** 또는 **영숫자**를 클릭합니다.
- **알림 템플릿:**
  - **등록 URL용 템플릿:** 목록에서 등록 URL에 사용할 템플릿을 클릭합니다. 예를 들어, 등록 초대 템플릿은 사용자에게 이메일 또는 SMS를 보냅니다. 이 방법은 사용자가 XenMobile에 장치를 등록할 수 있도록 템플릿을 구성한 방식에 따라 달라집니다. 알림 템플릿에 대한 자세한 내용은 알림 템플릿 생성 또는 업데이트를 참조하십시오.
  - **등록 PIN용 템플릿:** 목록에서 등록 PIN에 사용할 템플릿을 클릭합니다.
  - **등록 확인용 템플릿:** 목록에서 사용자에게 등록이 성공적으로 완료되었음을 알리는 데 사용할 템플릿을 클릭합니다.

3. **저장**을 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. 등록 보안 모드가 기본값으로 설정되어 있지 않으면 각 장치 등록에 대해 등록 요청을 생성해야 합니다.

> **참고:**
>
> 기본값으로 사용할 수 있는 등록 보안 모드는 **사용자 이름 + 암호**, **2단계 인증** 또는 **사용자 이름 + PIN** 뿐입니다.

1. 기본 등록 보안 모드(예: **사용자 이름 + 암호**, **2단계 인증** 또는 **사용자 이름 + PIN**)를 선택합니다.

   모드를 기본값으로 사용하려면 먼저 해당 모드를 활성화해야 합니다.

2. **기본값**을 클릭합니다. 선택한 모드가 이제 기본값이 됩니다. 다른 등록 보안 모드가 기본값으로 설정되어 있었다면 해당 모드는 더 이상 기본값이 아닙니다.

등록 보안 모드를 비활성화하려면

등록 보안 모드를 비활성화하면 그룹 등록 초대 및 셀프 서비스 포털 모두에서 해당 모드를 사용할 수 없게 됩니다. 하나의 등록 보안 모드를 비활성화하고 다른 모드를 활성화하여 사용자가 장치를 등록하는 방법을 변경할 수 있습니다.

1. 등록 보안 모드를 선택합니다.

   기본 등록 보안 모드는 비활성화할 수 없습니다. 기본 등록 보안 모드를 비활성화하려면 먼저 기본 상태를 제거해야 합니다.

2. **비활성화**를 클릭합니다. 등록 보안 모드가 더 이상 활성화되지 않습니다.

셀프 서비스 포털에서 등록 보안 모드를 활성화하려면

셀프 서비스 포털에서 등록 보안 모드를 활성화하면 사용자가 XenMobile에 장치를 개별적으로 등록할 수 있습니다.

> **참고:**
>
> - 등록 보안 모드는 셀프 도움말 포털에서 사용할 수 있도록 활성화되고 알림 템플릿에 바인딩되어야 합니다.
> - 셀프 도움말 포털에서는 한 번에 하나의 등록 보안 모드만 활성화할 수 있습니다.

1. 등록 보안 모드를 선택합니다.
2. **셀프 도움말 포털**을 클릭합니다. 선택한 등록 보안 모드는 이제 셀프 도움말 포털에서 사용자에게 제공됩니다. 셀프 도움말 포털에서 이미 활성화된 모드는 더 이상 사용자에게 제공되지 않습니다.

그룹 추가 또는 제거

XenMobile 콘솔의 **사용자**, **로컬 사용자 추가** 또는 **로컬 사용자 편집** 페이지에서 **그룹 관리** 대화 상자를 통해 그룹을 관리합니다. 그룹 편집 명령은 없습니다.

그룹을 제거하는 경우, 그룹 제거가 사용자 계정에 영향을 미치지 않는다는 점을 명심하십시오. 그룹을 제거하면 해당 그룹과의 사용자 연결만 제거됩니다. 또한 사용자는 해당 그룹과 연결된 Delivery Group에서 제공

하는 앱 또는 프로필에 대한 액세스 권한을 잃게 됩니다. 그러나 다른 그룹 연결은 그대로 유지됩니다. 사용자가 다른 로컬 그룹과 연결되어 있지 않으면 최상위 수준에서 연결됩니다.

로컬 그룹을 추가하려면

1. 다음 중 하나를 수행합니다.

   - **사용자** 페이지에서 **로컬 그룹 관리**를 클릭합니다.

   사용자 그룹 관리 이미지(/en-us/xenmobile/server/media/local-users-and-groups-page-menu.png)

   - **로컬 사용자 추가** 페이지 또는 **로컬 사용자 편집** 페이지에서 **그룹 관리**를 클릭합니다.

   사용자 그룹 관리 이미지(/en-us/xenmobile/server/media/local-users-and-groups-manage-group.png)

   그룹 관리 대화 상자가 나타납니다.

   사용자 그룹 관리 이미지(/en-us/xenmobile/server/media/local-users-and-groups-manage-group-add.png)

2. 그룹 목록 아래에 새 그룹 이름을 입력한 다음 더하기 기호(**+**)를 클릭합니다. 사용자 그룹이 목록에 추가됩니다.
3. **닫기**를 클릭합니다.

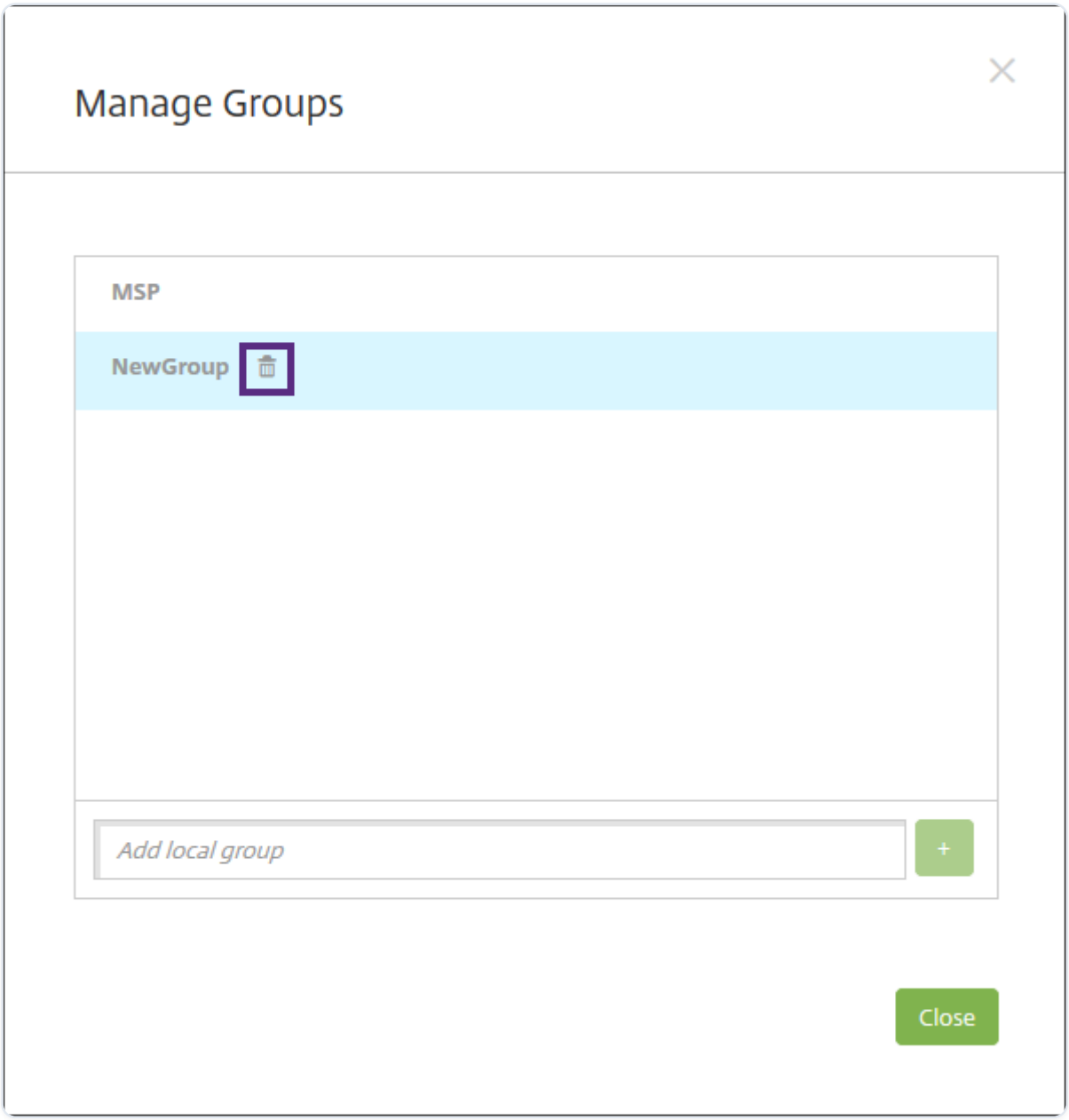
그룹을 제거하려면

그룹을 제거해도 사용자 계정에는 영향을 미치지 않습니다. 그룹을 제거하면 해당 그룹과의 사용자 연결만 제거됩니다. 사용자는 해당 그룹과 연결된 Delivery Group에서 제공하는 앱 또는 프로필에 대한 액세스 권한도 잃게 됩니다. 그러나 다른 그룹 연결은 그대로 유지됩니다. 사용자가 다른 로컬 그룹과 연결되어 있지 않은 경우 최상위 수준에서 연결됩니다.

1. 다음 중 하나를 수행합니다.

   - **사용자** 페이지에서 **로컬 그룹 관리**를 클릭합니다.
   - **로컬 사용자 추가** 페이지 또는 **로컬 사용자 편집** 페이지에서 **그룹 관리**를 클릭합니다.

   그룹 관리 대화 상자가 나타납니다.



2. **그룹 관리** 대화 상자에서 삭제할 그룹을 클릭합니다.
3. 그룹 이름 오른쪽에 있는 휴지통 아이콘을 클릭합니다. 확인 대화 상자가 나타납니다.
4. 작업을 확인하고 그룹을 제거하려면 **삭제**를 클릭합니다.

> **중요:**
>
> 이 작업은 실행 취소할 수 없습니다.

5. **그룹 관리** 대화 상자에서 **닫기**를 클릭합니다.

워크플로 생성 및 관리

워크플로를 사용하여 사용자 계정 생성 및 제거를 관리할 수 있습니다. 워크플로를 사용하기 전에 사용자 계정 요청을 승인할 권한이 있는 조직 내 개인을 식별해야 합니다. 그런 다음 워크플로 템플릿을 사용하여 사용자 계정 요청을 생성하고 승인할 수 있습니다.

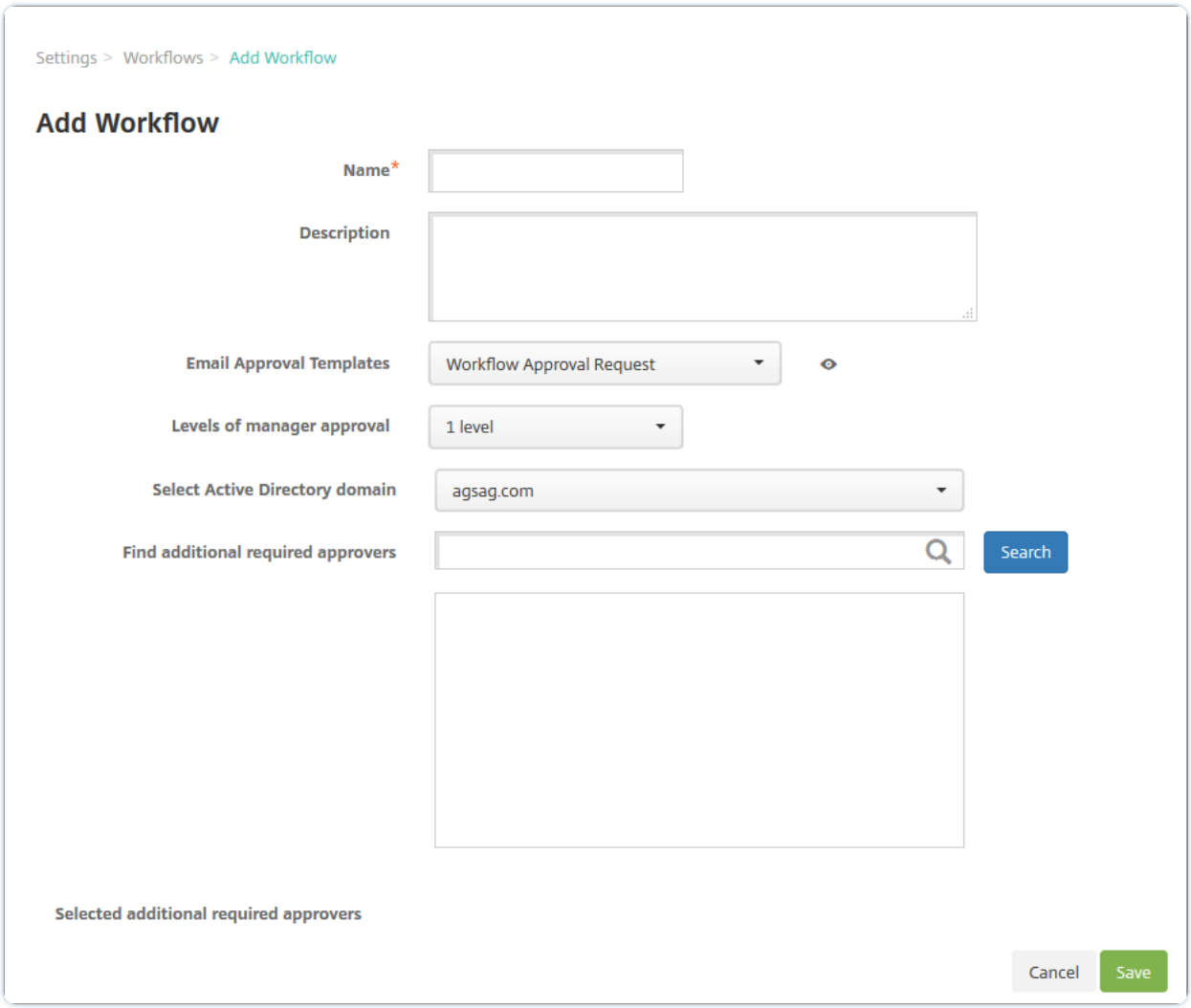
XenMobile을 처음 설정할 때 워크플로 이메일 설정을 구성합니다. 이 설정은 워크플로를 사용하기 전에 반드시 설정해야 합니다. 워크플로 이메일 설정은 언제든지 변경할 수 있습니다. 이 설정에는 이메일 서버, 포트, 이메일 주소, 그리고 사용자 계정 생성 요청에 승인이 필요한지 여부가 포함됩니다.

XenMobile에서 두 곳에서 워크플로를 구성할 수 있습니다.

- XenMobile 콘솔의 **워크플로** 페이지에서. **워크플로** 페이지에서 앱 구성에 사용할 여러 워크플로를 구성할 수 있습니다. 워크플로 페이지에서 워크플로를 구성할 때 앱을 구성할 때 해당 워크플로를 선택할 수 있습니다.
- 앱에서 애플리케이션 커넥터를 구성할 때 워크플로 이름을 제공한 다음 사용자 계정 요청을 승인할 수 있는 개인을 구성합니다. XenMobile에 앱 추가를 참조하십시오.

사용자 계정 관리자 승인을 위해 최대 3단계까지 할당할 수 있습니다. 다른 사람이 사용자 계정을 승인해야 하는 경우 이름 또는 이메일 주소를 사용하여 검색하고 선택할 수 있습니다. XenMobile이 해당 사용자를 찾으면 워크플로에 추가합니다. 워크플로의 모든 개인은 새 사용자 계정을 승인하거나 거부하는 이메일을 받습니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **워크플로**를 클릭합니다. **워크플로** 페이지가 나타납니다.
3. **추가**를 클릭합니다. **워크플로 추가** 페이지가 나타납니다.



4. 다음 설정을 구성합니다.

- **이름:** 워크플로의 고유한 이름을 입력합니다.
- **설명:** 선택적으로 워크플로에 대한 설명을 입력합니다.
- **이메일 승인 템플릿:** 목록에서 할당할 이메일 승인 템플릿을 선택합니다. 이메일 템플릿은 XenMobile 콘솔의 **설정** 아래 **알림 템플릿** 섹션에서 생성합니다. 이 필드 오른쪽에 있는 눈 아이콘을 클릭하면 구성 중인 템플릿의 미리보기를 볼 수 있습니다.
- **관리자 승인 수준:** 목록에서 이 워크플로에 필요한 관리자 승인 수준 수를 선택합니다. 기본값은 **1단계**입니다. 가능한 옵션은 다음과 같습니다.
  - 필요 없음
  - 1단계
  - 2단계
  - 3단계

- **Active Directory 도메인 선택:** 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
- **추가 필수 승인자 찾기:** 검색 필드에 이름을 입력한 다음 **검색**을 클릭합니다. 이름은 Active Directory에서 가져옵니다.
- 이름이 필드에 나타나면 이름 옆의 확인란을 선택합니다. 이름과 이메일 주소가 **선택된 추가 필수 승인자** 목록에 나타납니다.
    - 목록에서 이름을 제거하려면 다음 중 하나를 수행합니다.
        - **검색**을 클릭하여 선택한 도메인의 모든 사람 목록을 확인합니다.
        - 검색 상자에 전체 또는 부분 이름을 입력한 다음 **검색**을 클릭하여 검색 결과를 제한합니다.
        - **선택된 추가 필수 승인자** 목록의 사람들은 검색 결과 목록에서 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하여 제거하려는 각 이름 옆의 확인란을 지웁니다.

5. **저장**을 클릭합니다. 생성된 워크플로가 **워크플로** 페이지에 나타납니다.

워크플로를 생성한 후 워크플로 세부 정보를 보거나, 워크플로와 연결된 앱을 보거나, 워크플로를 삭제할 수 있습니다. 워크플로를 생성한 후에는 편집할 수 없습니다. 다른 승인 수준 또는 승인자가 있는 워크플로가 필요한 경우 다른 워크플로를 생성하십시오.

워크플로 세부 정보 보기 및 워크플로 삭제

1. **워크플로** 페이지의 기존 워크플로 목록에서 특정 워크플로를 선택합니다. 그러려면 테이블에서 행을 클릭하거나 워크플로 옆의 확인란을 선택합니다.
2. 워크플로를 삭제하려면 **삭제**를 클릭합니다. 확인 대화 상자가 나타납니다. 다시 **삭제**를 클릭합니다.

> **중요:**
>
> 이 작업을 실행 취소할 수 없습니다.

등록 프로필

등록 프로필은 다음을 지정합니다.

- Android 및 iOS 장치에 대한 장치 관리 등록 옵션. Android의 경우 MDM+MAM(ENT) 서버 모드에서 사용할 수 있는 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 오류 메시지를 통해 사용자에게 장치 등록 제한을 초과했음을 알립니다.

- 사용자가 장치 관리를 거부하도록 허용할지 여부.

등록 프로필을 사용하여 단일 XenMobile® Server 콘솔 내에서 여러 사용 사례와 장치 마이그레이션 경로를 결합할 수 있습니다. 일부 사용 사례는 다음과 같습니다.

- 모바일 장치 관리(MDM 전용)
- MDM+모바일 애플리케이션 관리(MAM)
- MAM 전용
- 회사 소유 등록
- BYOD 등록(MDM 등록을 거부할 수 있는 기능)
- Android 장치 관리자 등록을 Android Enterprise 등록(완전 관리형, 업무 프로필, 전용 장치)으로 마이그레이션

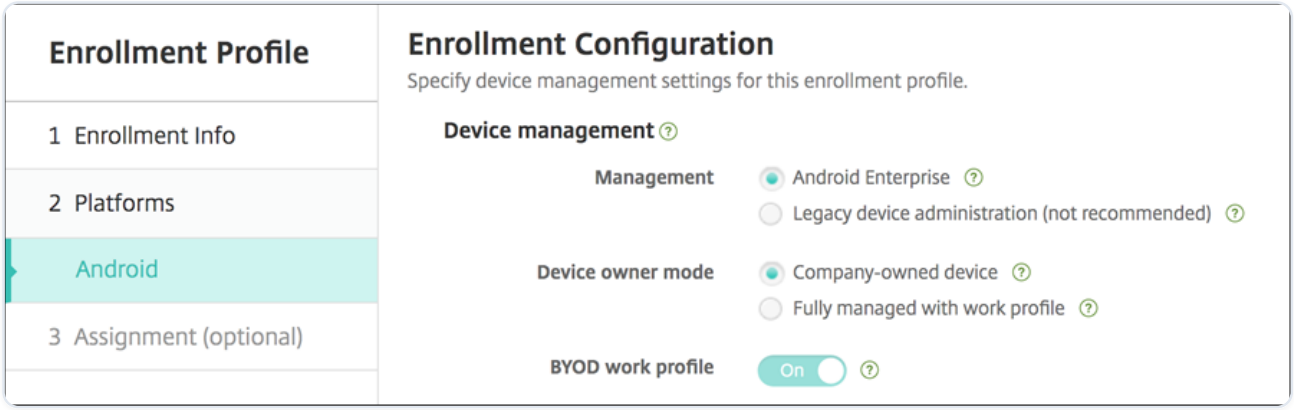
전송 그룹을 생성할 때 Global이라는 기본 등록 프로필을 사용하거나 다른 등록 프로필을 지정할 수 있습니다.

플랫폼별 등록 프로필 기능은 다음과 같습니다.

- **Android 장치의 경우:** 장치 소유자 모드를 지정합니다. 예를 들어, 완전 관리형, 업무 프로필이 있는 완전 관리형, BYOD 업무 프로필 등이 있습니다. **전용 장치** 옵션은 XenMobile에 대한 Enterprise 또는 Advanced 라이선스가 있는 경우에만 나타납니다. 새 장치는 기본적으로 Android Enterprise 및 앱 관리에 등록됩니다. **사용자 이름 + PIN**, **초대 URL**, **초대 URL + PIN**, **초대 URL + 암호** 등록 보안 모드는 Android Enterprise에서 사용할 수 없습니다.
- **iOS 장치의 경우:** 장치 등록 유형(장치 등록 또는 장치 관리 안 함)을 지정합니다. iOS 설정은 XenMobile에 대한 Enterprise 또는 Advanced 라이선스가 있는 경우에만 나타납니다. 새 장치는 기본적으로 Apple 장치 관리 및 앱 관리에 등록됩니다.

Android 장치에 대한 전용 장치 등록 또는 Android 또는 iOS 장치에 대한 MAM 전용 등록이 필요하지 않은 경우 서버 속성 `enable.multimode.xms`을(를) 비활성화할 수 있습니다. 그러나 이 속성을 활성화된 상태로 유지하면 모든 유형의 등록 프로필을 처리하기 위해 하나의 XenMobile Server만 있으면 됩니다. 서버 속성을(를) 참조하십시오.

`enable.multimode.xms`을(를) 비활성화하면 이 스크린샷의 설정만 사용할 수 있습니다.

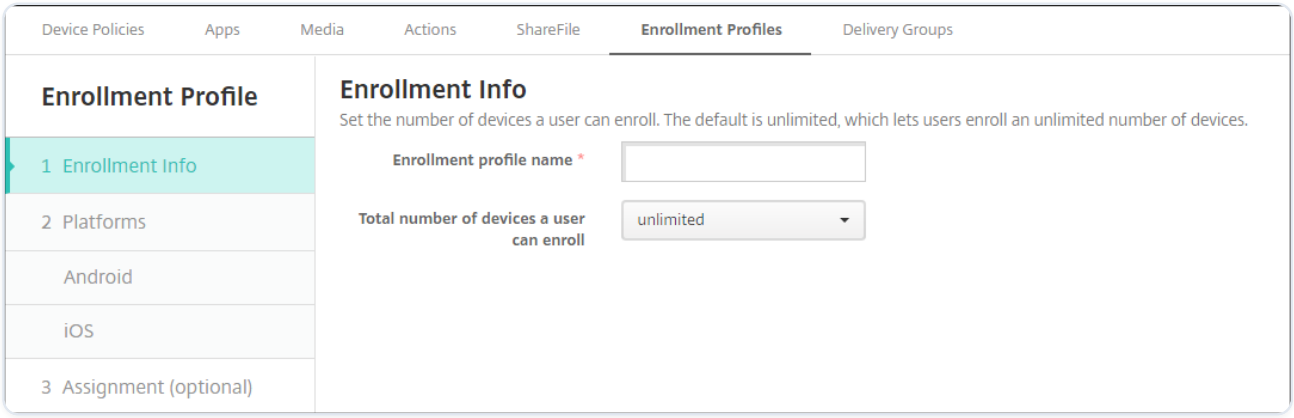


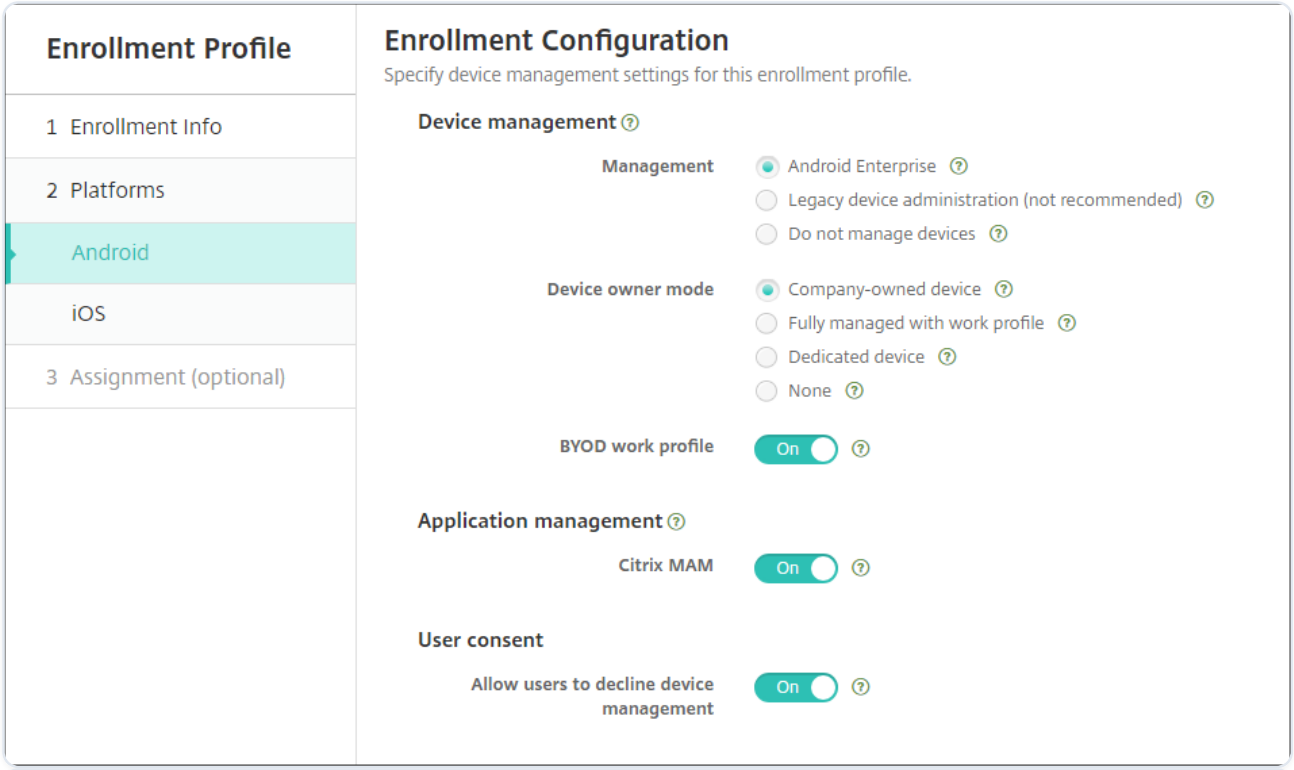
이러한 설정에 대한 자세한 내용은 Android Enterprise을(를) 참조하십시오.

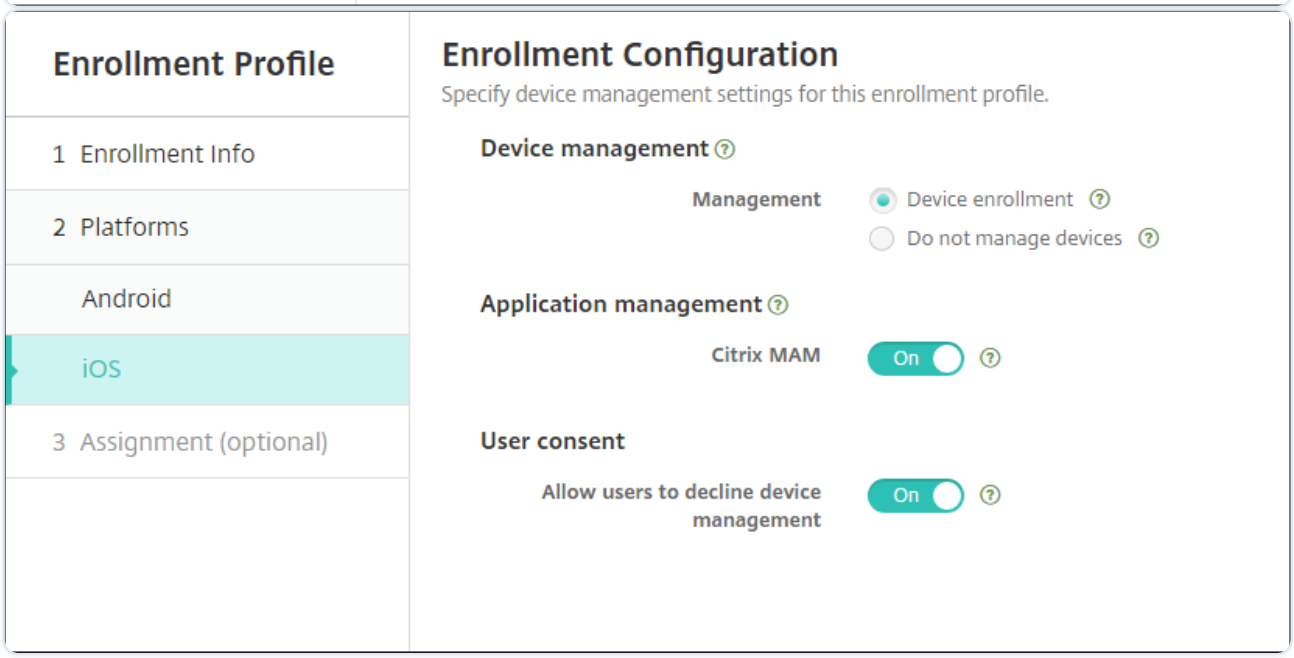
글로벌 등록 프로필

기본 등록 프로필 이름은 Global입니다. Global 프로필은 등록 프로필을 생성할 기회가 생길 때까지 테스트하는 데 유용합니다.

다음 스크린샷은 Global 등록 프로필의 기본 설정을 보여줍니다.







등록 프로필, 전송 그룹 및 등록

등록 프로필과 딜리버리 그룹은 다음과 같이 상호 작용합니다.

- 등록 프로필을 하나 이상의 딜리버리 그룹에 연결할 수 있습니다.
- 사용자가 서로 다른 등록 프로필을 가진 여러 딜리버리 그룹에 속해 있는 경우, 딜리버리 그룹의 이름이 사용되는 등록 프로필을 결정합니다. XenMobile Server는 딜리버리 그룹의 알파벳순 목록에서 마지막에 나타나는 딜리버리 그룹을 선택합니다. 예를 들어, 다음과 같은 상황을 가정해 보겠습니다.
  - "EP1" 및 "EP2"라는 두 개의 등록 프로필.

  - "DG1" 및 "DG2"라는 두 개의 딜리버리 그룹.
  - "DG1"은 "EP1"과 연결되어 있습니다.
  - "DG2"는 "EP2"와 연결되어 있습니다.

  등록하는 사용자가 "DG1" 및 "DG2" 딜리버리 그룹 모두에 속해 있는 경우, XenMobile Server는 "EP2" 등록 프로필을 사용하여 사용자의 등록 유형을 결정합니다.

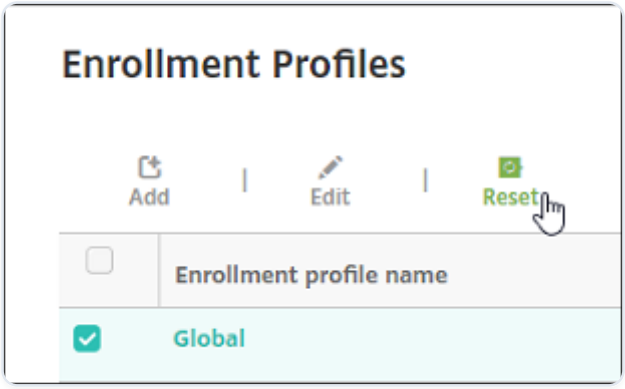
- 배포 순서는 MDM(장치 관리)용으로 구성된 등록 프로필이 있는 딜리버리 그룹의 장치에만 적용됩니다.
- 장치가 등록된 후 등록 프로필에 대한 일부 변경 사항은 재등록이 필요합니다.
  - MDM용으로 구성된 등록 프로필에 MAM을 추가하는 경우.
  - MDM에 등록된 장치를 MDM+MAM용으로 구성된 딜리버리 그룹으로 이동하는 경우. 이 변경 사항은 새로운 장치 등록에만 영향을 미칩니다. 기존 장치 등록에는 영향을 미치지 않습니다.
  - MAM용으로 구성된 등록 프로필에 MDM을 추가하는 경우.
- 다른 등록 프로필로 전환해도 기존 등록된 장치에는 영향을 미치지 않습니다. 그러나 변경 사항을 적용하려면 사용자가 해당 장치를 등록 해제한 다음 다시 등록해야 합니다.

등록 프로필을 생성하려면

1. XenMobile Server 콘솔에서 **구성 > 등록 프로필**로 이동합니다.
2. **등록 정보** 페이지에서 프로필에 대한 설명 이름을 입력합니다. 기본적으로 사용자는 무제한 장치를 등록할 수 있습니다. 사용자당 장치 수를 제한하려면 값을 선택합니다. 이 제한은 사용자가 등록하는 MAM 또는 MDM 관리 Android 및 iOS 장치의 합계에 적용됩니다.
3. 플랫폼 페이지를 완료합니다. 플랫폼별 등록 설정에 대한 자세한 내용은 다음을 참조하십시오.
   - 안드로이드 엔터프라이즈
   - iOS: 지원되는 등록 방법
4. **할당** 페이지에서 하나 이상의 전달 그룹을 등록 프로필에 연결합니다.

   사용자는 서로 다른 등록 프로필을 가진 여러 전달 그룹에 속할 수 있습니다. 이 경우 전달 그룹의 이름이 사용되는 등록 프로필을 결정합니다. XenMobile은 전달 그룹의 알파벳순 목록에서 마지막에 나타나는 전달 그룹을 선택합니다. 전달 그룹을 만들려면 **구성 > 전달 그룹**으로 이동합니다.

구성 > 등록 프로필 페이지에 등록 프로필 목록이 나타납니다. 전역 프로필을 편집하거나 원래 기본값으로 재설정하려면 전역 프로필 행을 선택하고 **재설정**을 클릭합니다. 전역 프로필은 삭제할 수 없습니다.



RBAC를 사용하여 역할 구성

각 사전 정의된 역할 기반 액세스 제어(RBAC) 역할에는 특정 액세스 및 기능 권한이 연결되어 있습니다. 이 문서에서는 각 권한이 수행하는 작업을 설명합니다. 각 기본 제공 역할에 대한 기본 권한의 전체 목록은 역할 기반 액세스 제어 기본값을 다운로드하십시오.

*권한을 적용*할 때, RBAC 역할이 관리할 수 있는 사용자 그룹을 정의하는 것입니다. 기본 관리자는 적용된 권한 설정을 변경할 수 없습니다. 기본적으로 적용된 권한은 모든 사용자 그룹에 적용됩니다.

*할당*을 수행할 때, RBAC 역할을 그룹에 할당하여 해당 사용자 그룹이 RBAC 관리자 권한을 소유하도록 합니다.

중요:

설정 권한에서 RBAC 권한은 관리자 사용자에게 자신의 권한을 할당하는 기능을 포함하여 모든 액세스 권한을 부여합니다. 이 액세스 권한은 Endpoint Management 시스템의 모든 것을 조작할 수 있는 권한을 부여하려는 사용자에게만 부여하십시오.

이 문서에는 다음 섹션이 있습니다.

- 관리자 역할
- 지원 역할
- 사용자 역할
- RBAC를 사용하여 역할 구성

관리자 역할

사전 정의된 관리자 역할을 가진 사용자는 XenMobile에서 다음 기능에 액세스하거나 액세스할 수 없습니다. 기본적으로 **승인된 액세스** (셀프 서비스 포털 제외), **콘솔 기능**, **권한 적용**이 활성화되어 있습니다.

승인된 액세스

관리 콘솔 액세스	관리자는 XenMobile 콘솔의 모든 기능에 액세스할 수 있습니다.
셀프 도움말 포털 액세스	관리자는 셀프 도움말 포털에 액세스할 수 없습니다 .
공유 장치 등록자	관리자는 공유 장치 등록자 액세스 권한이 없습니다 . 이 기능은 공유 장치를 등록해야 하는 사용자를 위한 것입니다.
원격 지원 액세스	관리자는 원격 지원 액세스 권한을 소유합니다.*
공용 API 액세스	관리자는 XenMobile 콘솔에서 사용할 수 있는 작업을 프로그래밍 방식으로 수행하기 위해 공용 API에 액세스할 수 있습니다. 이 작업에는 인증서, 앱, 장치, 전송 그룹 및 로컬 사용자 관리가 포함됩니다.
COSU 장치 등록자	등록 프로필을 사용하여 이 기능이 구성되지 않은 경우 관리자가 전용 Android Enterprise 장치(COSU 장치라고도 함)를 등록할 수 있는 방법을 제공합니다.

* 원격 지원을 통해 헬프데스크 담당자는 관리되는 Android 모바일 장치를 원격으로 제어할 수 있습니다. 화면 전송은 Samsung Knox 장치에서만 지원됩니다. 클러스터형 온프레미스 XenMobile Server 배포에서는 원격 지원을 사용할 수 없습니다. 원격 지원은 January 1, 2019부터 신규 고객에게 더 이상 제공되지 않습니다. 기존 고객은 제품을 계속 사용할 수 있지만 Citrix는 향상된 기능이나 수정 사항을 제공하지 않습니다.

콘솔 기능

관리자는 XenMobile 콘솔에 대한 무제한 액세스 권한을 가집니다.

대시보드	**대시보드**는 관리자가 XenMobile 콘솔에 로그인한 후 처음으로 보게 되는 페이지입니다. **대시보드**는 알림 및 장치에 대한 기본 정보를 표시합니다.	

보고	**분석 > 보고** 페이지는 앱 및 장치 배포를 분석할 수 있는 사전 정의된 보고서를 제공합니다.	
장치	**관리 > 장치** 페이지는 사용자 장치를 관리하는 곳입니다. 이 페이지에서 개별 장치를 추가하거나 장치 프로비저닝 파일을 가져와 한 번에 여러 장치를 추가할 수 있습니다.	
로컬 사용자 및 그룹	**관리 > 사용자** 페이지는 로컬 사용자 및 로컬 사용자 그룹을 추가, 편집 또는 삭제할 수 있는 곳입니다.	
등록	**관리 > 등록 초대** 페이지는 사용자가 XenMobile에 장치를 등록하도록 초대되는 방식을 관리하는 곳입니다.	
정책	**구성 > 장치 정책** 페이지는 VPN 및 Wi-Fi와 같은 장치 정책을 관리하는 곳입니다.	
앱	**구성 > 앱** 페이지는 사용자가 장치에 설치할 수 있는 다양한 앱을 관리하는 곳입니다.	
미디어	**구성 > 미디어** 페이지는 사용자가 장치에 설치할 수 있는 다양한 미디어를 관리하는 곳입니다.	
작업	**구성 > 작업** 페이지에서 트리거 이벤트에 대한 응답을 관리합니다.	
등록 프로필	**구성 > 등록 프로필** 페이지에서 사용자가 장치를 등록할 수 있도록 등록 프로필(모드)을 구성합니다.	

전달 그룹	**구성 > 전달 그룹** 페이지에서 전달 그룹 및 이와 관련된 리소스를 관리합니다.	
설정	**설정** 페이지에서 클라이언트 및 서버 속성, 인증서, 자격 증명 공급자와 같은 시스템 설정을 관리합니다. **중요:** 이러한 설정에는 RBAC 권한이 포함됩니다. RBAC 권한은 관리자에게 자신의 권한을 할당하는 기능을 포함하여 모든 권한을 부여합니다. 이 액세스 권한은 Endpoint Management 시스템의 모든 것을 조작할 수 있는 권한을 부여하려는 사용자에게만 부여하십시오.	
지원	**문제 해결 및 지원** 페이지에서 진단 실행 및 로그 생성과 같은 문제 해결 활동을 수행합니다.	

장치

관리자는 장치 제한 설정, 장치에 대한 알림 설정 및 전송, 장치에서 앱 관리 등을 통해 콘솔 전체에서 장치 기능에 액세스합니다.

장치 전체 초기화	장치에서 모든 데이터와 앱을 지웁니다. 장치에 메모리 카드가 있는 경우 메모리 카드도 포함됩니다.
제한 지우기	하나 이상의 장치 제한을 제거합니다.
장치 선택적 초기화	장치에서 모든 회사 데이터 및 앱을 지우고 개인 데이터 및 앱은 그대로 둡니다.
위치 보기	장치의 위치를 확인하고 지리적 제한을 설정합니다. 포함: 장치 찾기, 장치 위치 보기, 장치 추적, 시간 경과에 따른 장치 위치 추적.
장치 잠금	사용자가 장치를 사용할 수 없도록 장치를 원격으로 잠급니다.

장치 잠금 해제	사용자가 장치를 사용할 수 있도록 장치를 원격으로 잠금 해제합니다.
컨테이너 잠금	장치의 회사 컨테이너를 원격으로 잠급니다.
컨테이너 잠금 해제	장치의 회사 컨테이너를 원격으로 잠금 해제합니다.
컨테이너 암호 재설정	회사 컨테이너 암호를 재설정합니다.
ASM DEP/활성화 잠금 우회 활성화	활성화 잠금이 활성화된 경우 감독되는 iOS 장치에 우회 코드를 저장합니다. 장치를 지워야 하는 경우 이 코드를 사용하여 활성화 잠금을 자동으로 해제합니다.
장치 벨소리 울리기	Windows 장치에 5분 동안 최대 볼륨으로 원격 벨소리를 울립니다.
장치 재부팅	XenMobile 콘솔에서 Windows 장치를 다시 시작합니다.
장치에 배포	장치에 앱, 알림, 제한 등을 보냅니다.
장치 편집	장치의 설정을 변경합니다.
장치에 알림	장치에 알림을 보냅니다.
장치 추가/삭제	XenMobile에서 장치를 추가하거나 제거합니다.
장치 가져오기	파일에서 디바이스 그룹을 XenMobile로 가져옵니다.
디바이스 테이블 내보내기	디바이스 페이지에서 디바이스 정보를 수집하여 .csv 파일로 내보냅니다.
디바이스 해지	디바이스가 XenMobile에 연결하지 못하도록 금지합니다.
앱 잠금	디바이스의 모든 앱에 대한 액세스를 거부합니다. Android에서는 사용자가 XenMobile에 로그인할 수 없습니다. iOS에서는 사용자가 로그인할 수 있지만 앱에 액세스할 수 없습니다.

앱 초기화	Android에서는 이 작업이 사용자의 XenMobile 계정을 삭제합니다. iOS에서는 이 작업이 사용자가 XenMobile 기능에 액세스하는 데 필요한 암호화 키를 삭제합니다.
소프트웨어 인벤토리 보기	디바이스에 설치된 소프트웨어를 확인합니다.
AirPlay 미러링 요청	AirPlay 스트리밍 시작을 요청합니다.
AirPlay 미러링 중지	AirPlay 스트리밍을 중지합니다.
분실 모드 활성화	**관리 > 장치**에서 감독 대상 장치를 잠금 화면에서 차단하기 위해 분실 모드로 설정할 수 있습니다. 분실 모드는 장치를 분실하거나 도난당했을 때 장치를 찾을 수 있도록 합니다.
분실 모드 비활성화	**관리 > 장치**에서 분실 모드로 설정된 장치의 분실 모드를 비활성화할 수 있습니다.
장치 OS 업데이트	장치에 OS 업데이트 제어 장치 정책을 배포할 수 있습니다.
장치 종료	XenMobile 콘솔에서 iOS 장치를 종료합니다.
장치 재시작	XenMobile 콘솔에서 iOS 장치를 재시작합니다.

로컬 사용자 및 그룹

관리자는 XenMobile의 **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 가져오기
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 등록 초대장을 추가하거나 제거합니다.
사용자에게 알림	사용자 또는 사용자 그룹에 등록 초대장을 보냅니다.
등록 초대장 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 비활성화	기존 앱 정책을 비활성화합니다.
정책 내보내기	장치 정책 페이지에서 장치 정책 정보를 수집하여 .csv 파일로 내보냅니다.
정책 할당	하나 이상의 전달 그룹에 장치 정책을 할당합니다.

앱

관리자는 XenMobile의 **구성 > 앱** 페이지에서 앱을 관리합니다.

앱 스토어 또는 엔터프라이즈 앱 추가/삭제	공개 앱 스토어 앱 또는 엔터프라이즈 앱(MDX 사용 안 함)을 추가하거나 제거합니다.
앱 스토어 또는 엔터프라이즈 앱 편집	공개 앱 스토어 앱 또는 엔터프라이즈 앱(MDX 사용 안 함)을 변경합니다.
MDX, 웹 및 SaaS 앱 추가/삭제	MDX 사용 앱, 내부 네트워크의 앱(웹 앱) 또는 공개 네트워크의 앱(SaaS)을 XenMobile에 추가하거나 제거합니다.
MDX, 웹 및 SaaS 앱 편집	MDX 사용 앱, 내부 네트워크의 앱(웹 앱) 또는 공개 네트워크의 앱(SaaS)을 XenMobile에 변경합니다.
범주 추가/삭제	XenMobile Store에 앱이 표시될 수 있는 범주를 추가하거나 삭제합니다.
공개/엔터프라이즈 앱을 배달 그룹에 할당	배포를 위해 공개 앱 스토어 앱 또는 MDX 사용 앱을 배달 그룹에 할당합니다.
MDX/WebLink/SaaS 앱을 배달 그룹에 할당	MDX 사용 앱, 단일 Sign-On이 필요 없는 앱(WebLink) 또는 공개 네트워크의 앱(SaaS)을 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>`이(가) 설계상 LDAP 정보를 반환합니다.

미디어

공개 앱 스토어 또는 볼륨 구매 라이선스를 통해 얻은 미디어를 관리합니다.

앱 스토어 또는 엔터프라이즈 책 추가/삭제
공개/엔터프라이즈 책을 배달 그룹에 할당

앱 스토어 또는 엔터프라이즈 책 편집

작업

작업 추가/삭제	트리거(이벤트, 장치 또는 사용자 속성, 설치된 앱 이름) 및 관련 응답으로 정의된 작업을 추가하거나 제거합니다.
작업 편집	트리거(이벤트, 장치 또는 사용자 속성, 설치된 앱 이름) 및 관련 응답으로 정의된 작업을 변경합니다.
배달 그룹에 작업 할당	사용자 장치에 배포하기 위해 배달 그룹에 작업을 할당합니다.
작업 내보내기	작업 페이지에서 작업 정보를 수집하여 .csv 파일로 내보냅니다.

전달 그룹

관리자는 **구성 > 전달 그룹** 페이지에서 전달 그룹을 관리합니다.

전달 그룹 추가/삭제	지정된 사용자 및 선택적 정책, 앱, 작업을 추가하는 전달 그룹을 생성하거나 제거합니다.
전달 그룹 편집	기존 전달 그룹을 변경하여 사용자 및 선택적 정책, 앱, 작업을 수정합니다.
전달 그룹 배포	전달 그룹을 사용할 수 있도록 설정합니다.
전달 그룹 내보내기	전달 그룹 페이지에서 전달 그룹 정보를 수집하여 .csv 파일로 내보냅니다.

등록 프로필

등록 프로필을 관리합니다.

등록 프로필 추가/삭제
등록 프로필 편집

등록 프로필을 배달 그룹에 할당

설정

관리자는 **설정** 페이지에서 다양한 설정을 구성합니다.

RBAC	RBAC 할당, 역할 할당. **중요:** 이 권한은 관리자에게 자신의 권한을 할당하는 기능을 포함하여 모든 권한을 부여합니다. Endpoint Management 시스템의 모든 것을 조작할 수 있는 권한을 부여하려는 사용자에게만 이 액세스 권한을 부여하십시오.
LDAP	그룹, 사용자 계정 및 관련 속성을 가져오기 위해 Active Directory와 같은 하나 이상의 LDAP 호환 디렉터리를 관리합니다.
라이선스	온프레미스 XenMobile Server용. Citrix® 라이선스를 관리합니다.
등록	사용자 및 셀프 서비스 포털에 대한 등록 보안 모드를 활성화합니다.
릴리스 관리	현재 설치된 릴리스를 봅니다. 포함: 릴리스 관리 업데이트
인증서	APNS 인증서 편집, SSL 리스너 인증서
알림 템플릿	자동화된 작업, 등록 및 사용자에게 표준 알림 메시지 전달에 사용할 알림 템플릿을 생성합니다.
워크플로	앱 구성에 사용할 사용자 계정 생성, 승인 및 제거를 관리합니다.
자격 증명 공급자	장치 인증서를 발급할 권한이 있는 하나 이상의 자격 증명 공급자를 추가합니다. 자격 증명 공급자는 인증서 형식과 인증서 갱신 또는 해지 조건을 제어합니다.
PKI 엔터티	공개 키 인프라 엔터티(일반, Microsoft 인증서 서비스 또는 재량 CA)를 관리합니다.

PKI 연결 테스트	**설정 > PKI 엔터티** 페이지에서 **연결 테스트** 버튼을 사용하여 서버에 액세스할 수 있는지 확인합니다.
클라이언트 속성	암호 유형, 강도 또는 만료와 같은 사용자 장치의 다양한 속성을 관리합니다.
클라이언트 지원	사용자가 지원 서비스에 문의할 수 있는 방법(이메일, 전화 또는 지원 티켓 이메일)을 설정합니다.
클라이언트 브랜딩	XenMobile Store에 대한 사용자 지정 스토어 이름과 기본 스토어 보기를 만듭니다. XenMobile Store 또는 Secure Hub에 표시되는 사용자 지정 로고를 추가합니다.
통신사 SMS 게이트웨이	XenMobile이 통신사 SMS 게이트웨이를 통해 보내는 알림을 구성하도록 통신사 SMS 게이트웨이를 설정합니다.
알림 서버	사용자에게 이메일을 보내도록 SMTP 게이트웨이 서버를 설정합니다.
ActiveSync 게이트웨이	규칙 및 속성을 통해 사용자와 장치에 대한 사용자 액세스를 관리합니다.
Apple 배포 프로그램	XenMobile에 Apple 배포 프로그램 계정을 추가합니다.
Apple Configurator 장치 등록	XenMobile에서 Apple Configurator 설정을 구성합니다.
iOS/볼륨 구매 설정	Apple 볼륨 구매 계정을 추가합니다.
모바일 서비스 공급자	Mobile Service Provider 인터페이스를 사용하여 BlackBerry 및 기타 Exchange ActiveSync 장치를 쿼리하고 작업을 발행합니다.
시트릭스 게이트웨이	온프레미스 XenMobile Server용입니다. Citrix Gateway를 추가합니다. 인증을 활성화할지 여부와 인증을 위해 사용자 인증서를 푸시할지 여부를 선택합니다. 자격 증명 공급자를 선택합니다.

네트워크 액세스 제어	장치가 규정을 준수하지 않아 네트워크 액세스가 거부되는 조건을 설정합니다.
삼성 녹스	XenMobile이 Samsung Knox 증명 서버 REST API를 쿼리하도록 활성화하거나 비활성화합니다.
서버 속성	서버 속성을 추가하거나 수정합니다. 모든 노드에서 XenMobile을 다시 시작해야 합니다.
시스로그	온프레미스 XenMobile Server용입니다. 서버 호스트 이름 또는 IP 주소를 사용하여 로그 파일을 시스템 로그(syslog) 서버로 보냅니다.
XenApp 및 XenDesktop®	사용자가 Secure Hub를 통해 가상 앱 및 데스크톱을 추가할 수 있도록 허용합니다.
시트릭스 파일즈	Enterprise 계정과 함께 XenMobile을 사용하는 경우: ShareFile 계정 및 관리자 서비스 계정에 연결하여 사용자 계정을 관리하도록 설정을 구성합니다. 기존 Citrix Files 도메인 및 관리자 자격 증명이 필요합니다. 스토리지 영역 커넥터와 함께 XenMobile을 사용하는 경우: 스토리지 영역 커넥터에 정의된 네트워크 공유 및 SharePoint 위치를 가리키도록 XenMobile을 구성합니다.
경험 향상 프로그램	온프레미스 XenMobile Server용. 익명 통계 및 사용 정보를 Citrix에 전송할지 여부를 선택합니다.
마이크로소프트 애저	온프레미스 XenMobile Server용. XenMobile을 Microsoft Azure와 통합합니다.
안드로이드 엔터프라이즈	Android Enterprise 서버 설정을 구성합니다.
ID 공급자(IdP)	ID 공급자를 구성합니다.
XenMobile 도구	XenMobile 도구 페이지에 액세스합니다.
SNMP 구성	XenMobile Server 노드에 대해 SNMP를 활성화합니다. 모니터링 사용자를 편집하거나 추가하고, 트랩 알림이 표시되는 SNMP 관리자를 설정하고, 트랩 간격 및 임계값을 구성합니다.

지원

관리자는 다양한 지원 작업을 수행할 수 있습니다.

Citrix Gateway 연결 확인	IP 주소로 Citrix Gateway에 대한 다양한 연결 검사를 수행합니다. 사용자 이름과 암호가 필요합니다.
XenMobile 연결 검사	데이터베이스, DNS 또는 Google Plan과 같은 선택한 XenMobile 기능에 대한 연결 검사를 수행합니다.
지원 번들 생성	온프레미스 XenMobile Server용. 문제 해결을 위해 Citrix 지원팀에 보낼 파일을 생성합니다. 시스템 정보, 로그, 데이터베이스 정보, 코어 정보, 추적 파일, XenMobile 또는 Citrix Gateway의 최신 구성 정보가 포함됩니다.
Citrix 제품 설명서	공개 Citrix XenMobile 설명서 사이트에 액세스합니다.
Citrix 기술 자료 센터	기술 자료 문서를 검색하려면 Citrix 지원 사이트에 액세스합니다.
로그	디버그, 관리자 감사 및 사용자 감사를 위한 로그 파일 세부 정보에 액세스하고 분석합니다.
클러스터 정보	온프레미스 XenMobile Server용. 클러스터된 환경의 각 노드에 대한 정보에 액세스합니다.
가비지 컬렉션	온프레미스 XenMobile Server용. 더 이상 사용되지 않는 메모리 개체에 대한 정보에 액세스합니다.
Java 메모리 속성	온프레미스 XenMobile Server용. Java 메모리 사용량, 메모리 세부 정보 및 메모리 풀 세부 정보의 스냅샷에 액세스합니다.
매크로	프로필, 정책, 알림 또는 등록 템플릿의 텍스트 필드 내에 사용자 또는 장치 속성 데이터를 채웁니다. 단일 정책을 구성하고, 대규모 사용자 기반에 정책을 배포하고, 각 대상 사용자에게 사용자별 값이 표시되도록 합니다.
PKI 구성	PKI 구성 정보를 가져오고 내보냅니다.

APNS 서명 유틸리티	Apple 푸시 네트워크 서명(APNs) 인증서 요청을 제출하거나 iOS용 Secure Mail APNs 인증서를 업로드합니다.
Citrix Insight 서비스	다양한 문제에 대한 지원을 위해 Citrix Insight Services(CIS)에 로그를 업로드합니다.
익스체인지 액티브싱크 상태용 장치 시트릭스 게이트웨이 커넥터™	장치 ActiveSync ID를 기반으로 Exchange ActiveSync용 Citrix Gateway connector로 전송된 장치 상태를 XenMobile에 쿼리합니다.
익명화 및 익명화 해제	온프레미스 XenMobile Server용. XenMobile에서 지원 번들을 생성할 때 중요한 사용자, 서버 및 네트워크 데이터는 기본적으로 익명 처리됩니다. 이 동작은 **고급** 아래의 **지원 > 익명화 및 익명화 해제**에서 변경할 수 있습니다.
로그 설정	로그 수준을 사용자 지정하거나 사용자 지정 로거를 추가합니다.

그룹 액세스 제한

관리자 사용자는 모든 사용자 그룹에 권한을 적용할 수 있습니다.

지원 역할

지원 역할이 있는 사용자는 원격 지원에 액세스할 수 있습니다. 이들의 권한은 기본적으로 모든 사용자에게 적용되며 이 설정을 편집할 수 없습니다.

사용자 역할

사용자 역할이 있는 사용자는 XenMobile에 대해 다음과 같은 제한된 액세스 권한을 가집니다.

승인된 액세스

셀프 서비스 포털	사용자는 XenMobile의 셀프 서비스 포털에만 액세스할 수 있습니다.

콘솔 기능

사용자는 XenMobile 콘솔에 대해 다음과 같은 제한된 액세스 권한을 가집니다.

장치

장치 전체 초기화	장치에서 모든 데이터와 앱을 지웁니다. 장치에 메모리 카드가 있는 경우 메모리 카드도 포함됩니다.
선택적 초기화 장치	장치에서 모든 회사 데이터 및 앱을 지우고 개인 데이터 및 앱은 그대로 둡니다.
위치 보기	장치의 위치를 확인하고 지리적 제한을 설정합니다. 포함: 장치 찾기, 장치 위치 보기, 장치 추적, 시간 경과에 따른 장치 위치 추적
장치 잠금	장치를 원격으로 잠가 사용할 수 없도록 합니다.
장치 잠금 해제	장치를 원격으로 잠금 해제하여 사용할 수 있도록 합니다.
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/활성화 잠금 우회 사용	활성화 잠금이 활성화된 감독되는 iOS 장치에 우회 코드를 저장합니다. 장치를 지워야 하는 경우 이 코드를 사용하여 활성화 잠금을 자동으로 해제합니다.
장치 벨소리 울리기	Windows 장치에서 5분 동안 최대 볼륨으로 원격 벨소리를 울립니다.
장치 재부팅	Windows 장치를 다시 시작합니다.
소프트웨어 인벤토리 보기	장치에 설치된 소프트웨어를 확인합니다.

등록

등록 추가/삭제	사용자 또는 사용자 그룹에 등록 초대를 추가하거나 제거합니다.
사용자에게 알림	사용자 또는 사용자 그룹에 등록 초대를 보냅니다.

그룹 액세스 제한

네 가지 기본 역할 모두에 대해 이 권한은 기본적으로 설정되어 있으며 모든 사용자 그룹에 적용할 수 있습니다. 역할을 편집할 수 없습니다.

RBAC로 역할 구성

XenMobile의 역할 기반 액세스 제어(RBAC) 기능을 사용하면 미리 정의된 역할 또는 권한 집합을 사용자 및 그룹에 할당할 수 있습니다. 이러한 권한은 사용자가 시스템 기능에 액세스할 수 있는 수준을 제어합니다.

XenMobile은 시스템 기능에 대한 액세스를 논리적으로 분리하기 위해 네 가지 기본 사용자 역할을 구현합니다.

- **관리자:** 전체 시스템 액세스 권한을 부여합니다.
- **지원:** 원격 지원 액세스 권한을 부여합니다.
- **사용자:** 장치를 등록하고 셀프 도움말 포털에 액세스할 수 있는 사용자가 사용합니다.

기본 역할을 사용자 지정하여 사용자 역할을 만드는 템플릿으로 사용할 수도 있습니다. 기본 역할로 정의된 기능 외에 특정 시스템 기능에 액세스할 수 있는 역할 권한을 할당할 수 있습니다.

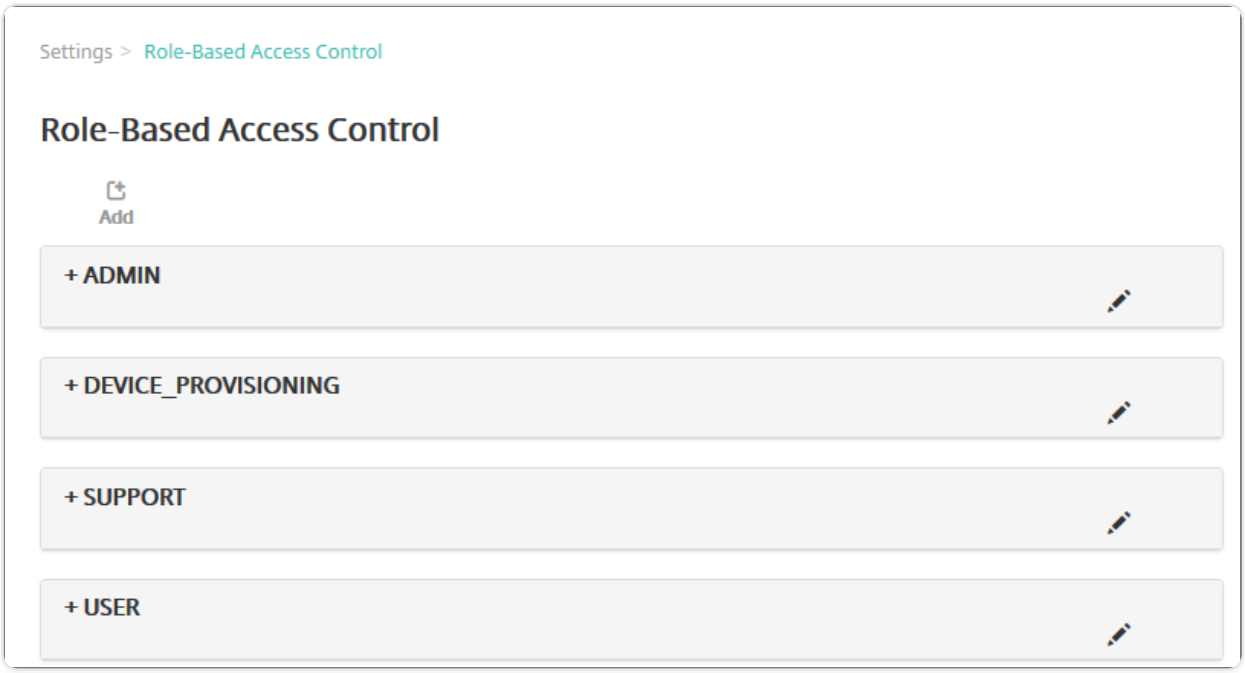
역할은 로컬 사용자(사용자 수준) 또는 Active Directory 그룹(해당 그룹의 모든 사용자가 동일한 권한을 가짐)에 할당할 수 있습니다. 사용자가 여러 Active Directory 그룹에 속하는 경우 모든 권한이 병합되어 해당 사용자의 권한을 정의합니다. 예를 들어, ADGroupA 사용자는 관리자 장치를 찾을 수 있고 ADGroupB 사용자는 직원 장치를 초기화할 수 있다고 가정해 보겠습니다. 이 경우 두 그룹에 모두 속하는 사용자는 관리자와 직원의 장치를 찾고 초기화할 수 있습니다.

> **참고:**
>
> 로컬 사용자에게는 하나의 역할만 할당될 수 있습니다.

> XenMobile의 RBAC 기능을 사용하여 다음을 수행할 수 있습니다.

- 역할 생성.
- 역할에 그룹 추가.
- 로컬 사용자를 역할에 연결.

1. XenMobile 콘솔에서 **설정 > 역할 기반 액세스 제어**로 이동합니다. **역할 기반 액세스 제어** 페이지가 나타나며, 여기에는 네 가지 기본 사용자 역할과 이전에 추가한 모든 역할이 표시됩니다.



역할 옆에 있는 더하기 기호(+)를 클릭하면 다음 그림과 같이 해당 역할에 대한 모든 권한이 표시되도록 역할이 확장됩니다.



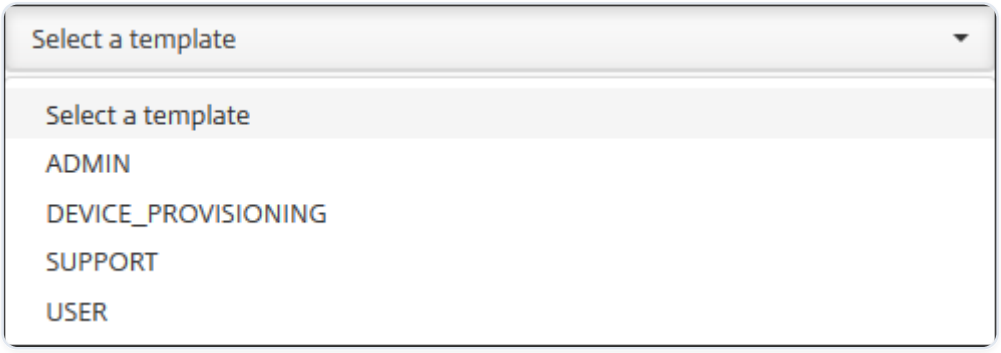
2. 새 사용자 역할을 추가하려면 **추가**를 클릭합니다. 역할을 편집하려면 기존 역할 오른쪽에 있는 펜 아이콘을 클릭합니다. 역할을 삭제하려면 역할 오른쪽에 있는 휴지통 아이콘을 클릭합니다. 기본 사용자 역할은 삭제할 수 없습니다.

   - **추가** 또는 펜 아이콘을 클릭하면 **역할 추가** 또는 **역할 편집** 페이지가 나타납니다.
   - 휴지통 아이콘을 클릭하면 확인 대화 상자가 나타납니다. 선택한 역할을 제거하려면 **삭제**를 클릭합니다.

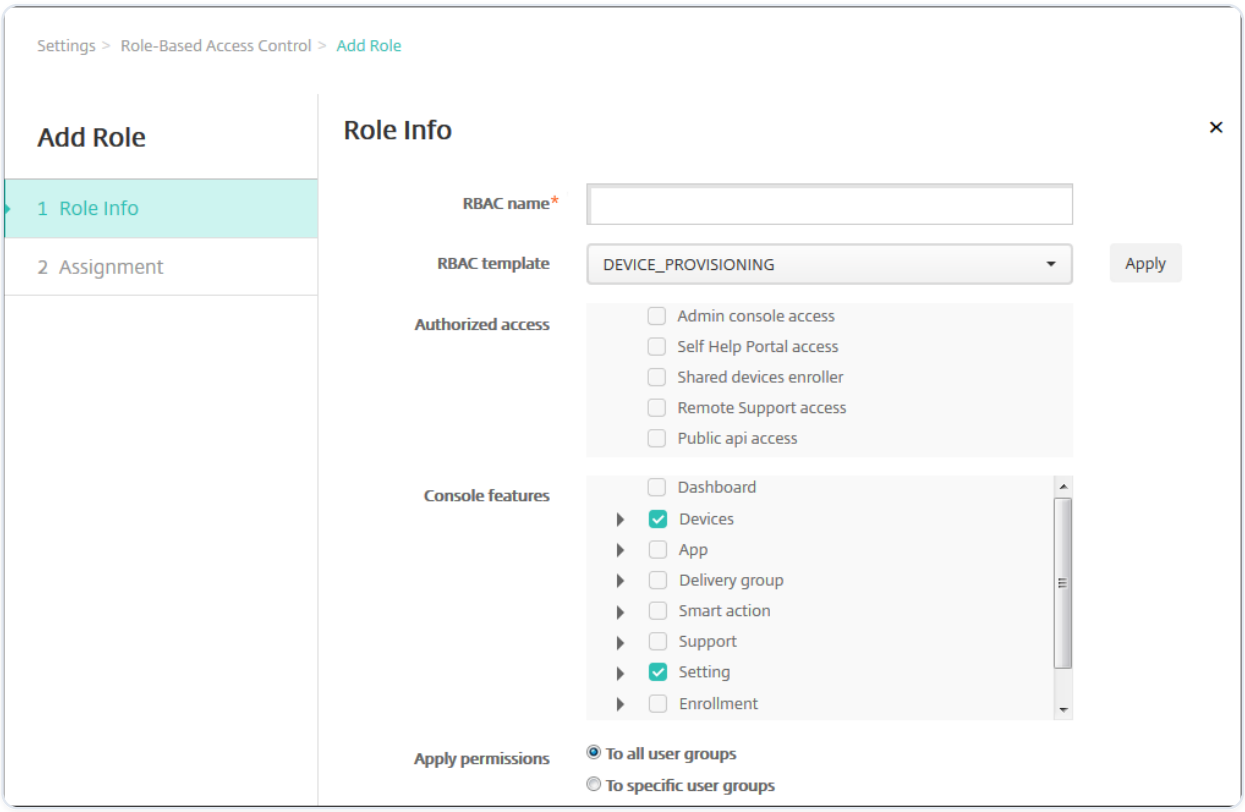
3. 사용자 역할을 생성하거나 편집하려면 다음 정보를 입력합니다.

   - **RBAC 이름:** 새 사용자 역할에 대한 설명이 포함된 이름을 입력합니다. 기존 역할의 이름은 변경할 수 없습니다.
   - **RBAC 템플릿:** 선택적으로 새 역할의 시작점으로 템플릿을 클릭합니다. 기존 역할을 편집하는 경우에는 템플릿을 선택할 수 없습니다.

RBAC 템플릿은 기본 사용자 역할입니다. 이 템플릿은 해당 역할과 연결된 사용자가 갖는 시스템 기능에 대한 액세스를 정의합니다. RBAC 템플릿을 선택한 후에는 **승인된 액세스** 및 **콘솔 기능** 필드에서 해당 역할과 연결된 모든 권한을 볼 수 있습니다. 템플릿 사용은 선택 사항입니다. **승인된 액세스** 및 **콘솔 기능** 필드에서 역할에 할당할 옵션을 직접 선택할 수 있습니다.

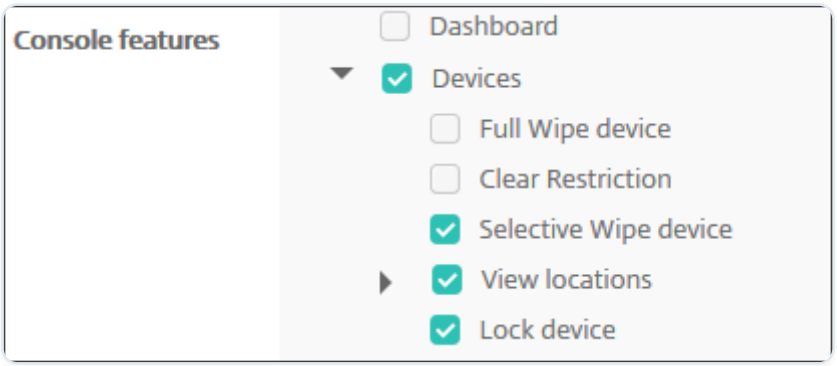


4. 선택한 **RBAC 템플릿** 필드 근처에 있는 **적용**을 클릭하여 **승인된 액세스** 및 **콘솔 기능**을 미리 정의된 액세스 및 기능 권한으로 채웁니다.



5. 역할을 사용자 지정하려면 **승인된 액세스** 및 **콘솔 기능**에서 확인란을 선택하거나 선택 취소합니다.

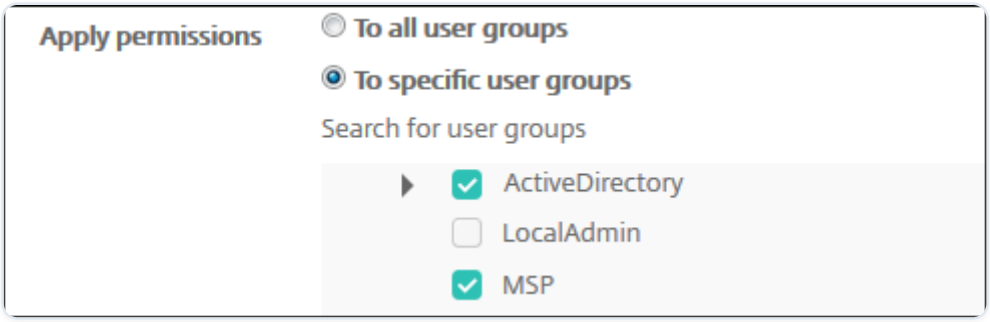
콘솔 기능 옆에 있는 삼각형을 클릭하면 해당 기능에 대한 특정 권한이 나타나며, 이를 선택하거나 선택 취소할 수 있습니다. 최상위 확인란을 클릭하면 해당 콘솔 영역에 대한 액세스가 금지됩니다. 최상위 아래의 개별 옵션을 선택하여 해당 옵션을 활성화합니다. 예를 들어, 다음 그림에서 **장치 전체 초기화** 및 **제한 지우기** 옵션은 해당 역할에 할당된 사용자에게는 나타나지 않습니다. 선택된 옵션은 나타납니다.



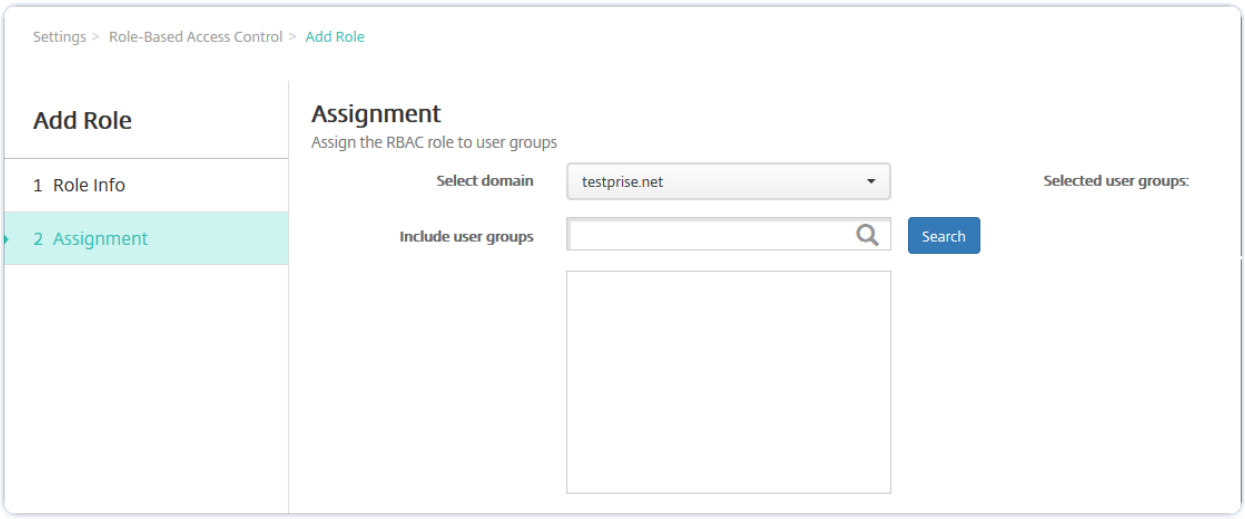
6. **권한 적용:** 관리자가 관리할 수 있는 그룹을 제한하려면 하나 이상의 사용자 그룹을 선택합니다. **특정 사용자 그룹에**를 클릭하면 그룹 목록이 나타나고, 이 목록에서 하나 이상의 그룹을 선택할 수 있습니다.

   예를 들어, RBAC 관리자가 ActiveDirectory 및 MSP 사용자 그룹에 대한 권한을 가지고 있는 경우:

   - 관리자는 ActiveDirectory 그룹, MSP 그룹 또는 두 그룹 모두에 속한 사용자에 대해서만 정보에 액세스할 수 있습니다.
   - 관리자는 다른 로컬 또는 AD 사용자를 볼 수 없습니다. 관리자는 해당 그룹 중 하나의 하위 그룹 구성원인 사용자를 볼 수 있습니다.
   - 관리자는 다음으로 초대장을 보낼 수 있습니다.
     - 권한 그룹 및 해당 하위 그룹
     - 권한 그룹 및 해당 하위 그룹의 구성원인 사용자

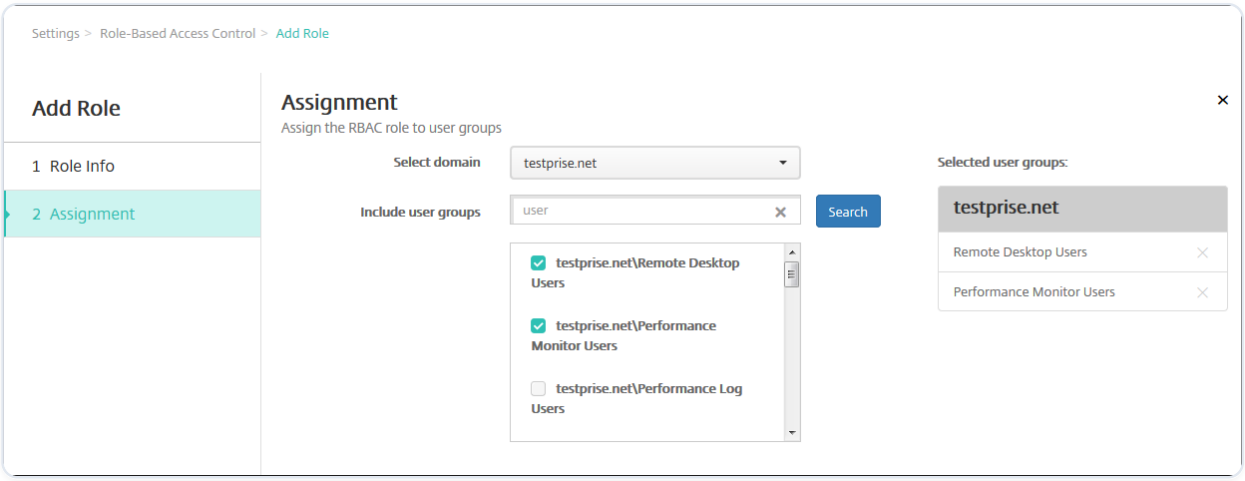


7. **다음**을 클릭합니다. **할당** 페이지가 나타납니다.



8. 역할을 사용자 그룹에 할당하려면 다음 정보를 입력합니다.

   - **도메인 선택:** 드롭다운 목록에서 도메인을 클릭합니다.
   - **사용자 그룹 포함:** 검색을 클릭하여 사용 가능한 모든 그룹 목록을 보거나, 전체 또는 부분 그룹 이름을 입력하여 해당 이름의 그룹으로만 목록을 제한합니다.
   - 나타나는 목록에서 역할을 할당할 사용자 그룹을 선택합니다. 사용자 그룹을 선택하면 해당 그룹이 **선택한 사용자 그룹** 목록에 나타납니다.



> **참고:**
>
> **선택된 사용자 그룹** 목록에서 사용자 그룹을 제거하려면 사용자 그룹 이름 옆의 X를 클릭합니다.

9. **저장**을 클릭합니다.

알림

XenMobile®에서 알림을 다음 용도로 사용할 수 있습니다.

- 여러 시스템 관련 기능에 대해 특정 사용자 그룹과 통신합니다. 또한 특정 사용자를 대상으로 이러한 알림을 보낼 수도 있습니다. 예를 들어, iOS 장치를 사용하는 모든 사용자, 규정 미준수 장치를 사용하는 사용자, 직원이 소유한 장치를 사용하는 사용자 등입니다.
- 사용자 및 장치를 등록합니다.
- 특정 조건이 충족될 때 사용자에게 자동으로 알립니다(자동화된 작업을 사용). 예를 들면 다음과 같습니다.
  - 사용자 장치가 규정 준수 문제로 인해 회사 도메인에서 차단될 예정인 경우.
  - 장치가 탈옥(jailbroken) 또는 루팅(rooted)된 경우

자동화된 작업에 대한 자세한 내용은 자동화된 작업을 참조하십시오.

XenMobile로 알림을 보내려면 게이트웨이와 알림 서버를 구성해야 합니다. XenMobile에서 알림 서버를 설정하여 SMTP(Simple Mail Transfer Protocol) 및 SMS(Short Message Service) 게이트웨이 서버를 구성하여 사용자에게 이메일 및 문자(SMS) 알림을 보낼 수 있습니다. 알림을 사용하여 SMTP 또는 SMS의 두 가지 채널을 통해 메시지를 보낼 수 있습니다.

- SMTP는 연결 지향적 텍스트 기반 프로토콜로, 메일 발신자가 명령 문자열을 발행하고 필요한 데이터를 제공함으로써 메일 수신자와 통신하며, 일반적으로 TCP(Transmission Control Protocol) 연결을 통해 이루어집니다. SMTP 세션은 SMTP 클라이언트(메시지를 보내는 사람)가 시작한 명령과 SMTP 서버의 해당 응답으로 구성됩니다.
- SMS는 전화, 웹 또는 모바일 통신 시스템의 문자 메시지 서비스 구성 요소입니다. SMS는 표준화된 통신 프로토콜을 사용하여 유선 또는 모바일 전화 장치가 짧은 문자 메시지를 교환할 수 있도록 합니다.

또한 XenMobile에서 캐리어 SMS 게이트웨이를 설정하여 캐리어의 SMS 게이트웨이를 통해 전송되는 알림을 구성할 수 있습니다. 캐리어는 SMS 게이트웨이를 사용하여 통신 네트워크로 또는 통신 네트워크에서 SMS 전송을 보내거나 받습니다. 이러한 텍스트 기반 메시지는 표준화된 통신 프로토콜을 사용하여 유선 또는 모바일 전화 장치가 짧은 문자 메시지를 교환할 수 있도록 합니다.

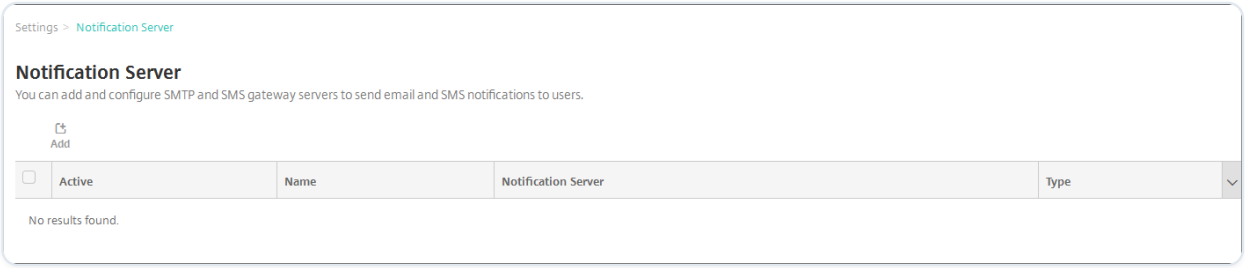
선행 조건

- SMS 게이트웨이를 구성하기 전에 시스템 관리자에게 문의하여 서버 정보를 확인하십시오. SMS 서버가 내부 회사 서버에서 호스팅되는지 또는 서버가 호스팅되는 이메일 서비스의 일부인지 아는 것이 중요합니다. 이 경우 서비스 공급자 웹 사이트에서 정보가 필요합니다.
- 사용자에게 메시지를 보내도록 SMTP 알림 서버를 구성합니다. 서버가 내부 서버에서 호스팅되는 경우 시스템 관리자에게 구성 정보를 문의하십시오. 서버가 호스팅되는 이메일 서비스인 경우 서비스 공급자 웹 사이트에서 적절한 구성 정보를 찾으십시오.
- 하나의 활성 SMTP 서버와 하나의 활성 SMS 서버를 동시에 사용할 수 있습니다. 두 통신 채널 모두 하나의 활성 구성을 허용합니다.

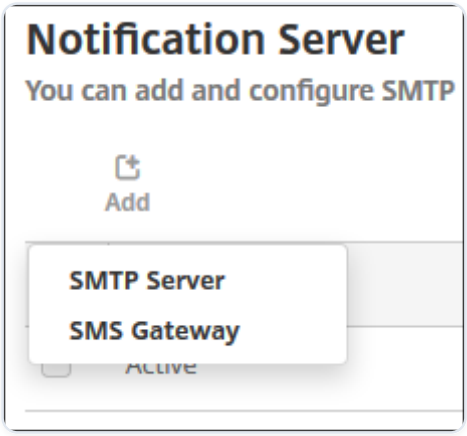
- 네트워크 DMZ에 있는 XenMobile에서 포트 25를 열어 내부 네트워크의 SMTP 서버로 다시 연결합니다. 이렇게 하면 XenMobile이 알림을 성공적으로 보낼 수 있습니다.

SMTP 서버 및 SMS 게이트웨이 구성

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **알림** 아래에서 **알림 서버**를 클릭합니다. **알림 서버** 페이지가 나타납니다.

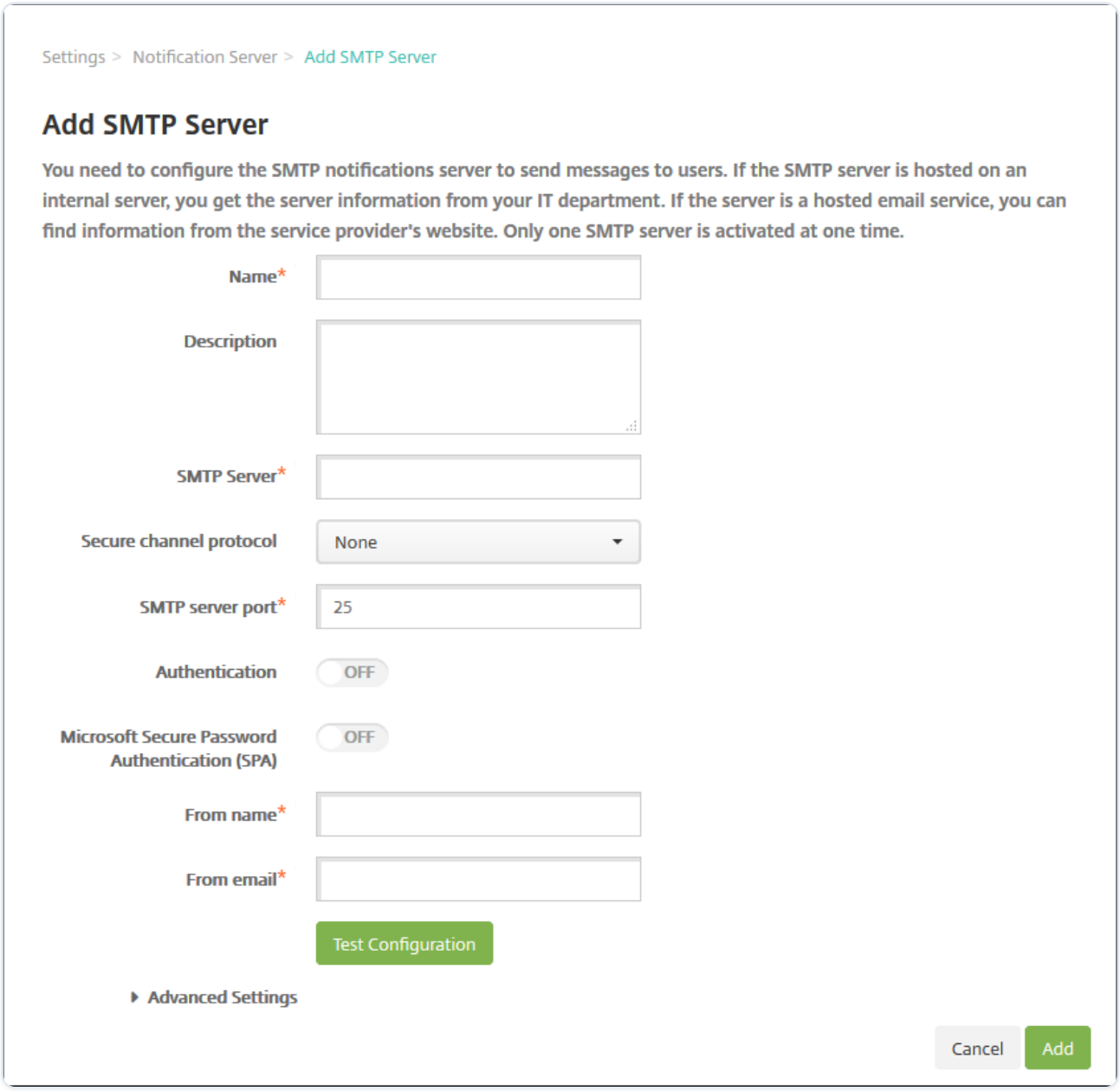


3. **추가**를 클릭합니다. SMTP 서버 또는 SMS 게이트웨이를 구성하는 옵션이 있는 메뉴가 나타납니다.



- SMTP 서버를 추가하려면 **SMTP 서버**를 클릭한 다음 이 설정을 구성하는 단계는 SMTP 서버를 추가하려면을 참조하십시오.
- SMS 게이트웨이를 추가하려면 **SMS 게이트웨이**를 클릭한 다음 이 설정을 구성하는 단계는 SMS 게이트웨이를 추가하려면을 참조하십시오.

SMTP 서버 추가



1. 다음 설정을 구성합니다.

   - **이름:** 이 SMTP 서버 계정과 연결된 이름을 입력합니다.
   - **설명:** 선택적으로 서버에 대한 설명을 입력합니다.
   - **SMTP 서버:** 서버의 호스트 이름을 입력합니다. 호스트 이름은 FQDN(정규화된 도메인 이름) 또는 IP 주소여야 합니다.
   - **보안 채널 프로토콜:** 서버에서 사용하는 보안 채널 프로토콜(서버가 보안 인증을 사용하도록 구성된 경우) 드롭다운 목록에서 **SSL**, **TLS** 또는 **없음**을 클릭합니다. 기본값은 **없음**입니다.
   - **SMTP 서버 포트:** SMTP 서버에서 사용하는 포트를 입력합니다. 기본적으로 포트는 25로 설정됩니다. SMTP 연결에서 SSL 보안 채널 프로토콜을 사용하는 경우 포트는 465로 설정됩니다.

- **인증: ON** 또는 **OFF**를 선택합니다. 기본값은 **OFF**입니다.
- **인증**을 사용하도록 설정하는 경우 다음 설정을 구성합니다.
  - **사용자 이름:** 인증에 사용할 사용자 이름을 입력합니다.
  - **암호:** 인증 사용자 암호를 입력합니다.

> **중요:**
>
> Microsoft Exchange Online에서 OAuth를 사용하려면 먼저 Microsoft Entra ID에 애플리케이션을 등록해야 합니다. 등록 후 **인증** 및 **Microsoft Exchange Online OAuth 2.0**을 사용하도록 설정합니다.

- **인증** 및 **Microsoft Exchange Online OAuth 2.0**을 사용하도록 설정하는 경우 다음 설정을 구성합니다.
  - **사용자 이름:** 인증에 사용할 사용자 이름을 입력합니다.
  - **테넌트 ID:** Microsoft Entra ID 디렉터리의 테넌트 ID를 입력합니다.
  - **클라이언트 ID:** 등록된 애플리케이션의 클라이언트(애플리케이션) ID를 입력합니다. Azure Portal > 등록된 애플리케이션 > **애플리케이션(클라이언트) ID**에서 찾을 수 있습니다.
  - **클라이언트 암호:** 등록된 애플리케이션의 클라이언트 암호를 입력합니다. Azure Portal > 등록된 애플리케이션 > **인증서 및 암호**에서 찾을 수 있습니다.
- **Microsoft SPA(Secure Password Authentication):** SMTP 서버에서 SPA를 사용하는 경우 **ON**을 클릭합니다. 기본값은 **OFF**입니다.
- **보낸 사람 이름:** 클라이언트가 이 서버로부터 알림 이메일을 받을 때 **보낸 사람** 상자에 표시될 이름을 입력합니다. 예: Corporate IT.
- **보낸 사람 이메일:** 이메일 수신자가 SMTP 서버에서 보낸 알림에 회신하는 경우 사용할 이메일 주소를 입력합니다.

2. 테스트 이메일 알림을 보내려면 **구성 테스트**를 클릭합니다.
3. **고급 설정**을 확장한 다음 다음 설정을 구성합니다.
   - **SMTP 재시도 횟수:** SMTP 서버에서 보낸 실패한 메시지를 재시도할 횟수를 입력합니다. 기본값은 5입니다.

- **SMTP 시간 제한:** SMTP 요청을 보낼 때 대기할 시간(초)을 입력합니다. 시간 초과로 인해 메시지 전송이 계속 실패하는 경우 이 값을 늘리십시오. 이 값을 줄일 때는 주의하십시오. 시간 초과 및 배달되지 않은 메시지 수가 증가할 수 있습니다. 기본값은 30초입니다.
- **최대 SMTP 수신자 수:** SMTP 서버에서 보낸 이메일 메시지당 최대 수신자 수를 입력합니다. 기본값은 100입니다.

4. **추가**를 클릭합니다.

SMS 게이트웨이 추가

알림 서버 SMS 추가(/en-us/xenmobile/server/media/settings-notifications-notification-server-add-sms.png)

> **참고:**
>
> XenMobile은 Nexmo SMS 메시징만 지원합니다. 아직 Nexmo 메시징을 사용할 계정이 없는 경우, 웹 사이트를 방문하여 계정을 만드십시오.

1. 다음 설정을 구성합니다.

   - **이름:** SMS 게이트웨이 구성의 이름을 입력합니다. 이 필드는 필수입니다.
   - **설명:** 선택적으로 구성에 대한 설명을 입력합니다.
   - **키:** 계정 활성화 시 시스템 관리자가 제공한 숫자 식별자를 입력합니다. 이 필드는 필수입니다.
   - **비밀:** 암호를 분실하거나 도난당했을 때 계정에 액세스하는 데 사용되는 시스템 관리자가 제공한 비밀을 입력합니다. 이 필드는 필수입니다.
   - **가상 전화번호:** 이 필드는 북미 전화번호(접두사 +1 포함)로 전송할 때 사용됩니다. Nexmo 가상 전화번호를 입력해야 하며, 이 필드에는 숫자만 사용해야 합니다. Nexmo 웹사이트에서 가상 전화번호를 구매할 수 있습니다.
   - **HTTPS:** Nexmo로 SMS 요청을 전송할 때 HTTPS를 사용할지 여부를 선택합니다. 기본값은 **OFF** 입니다.

   > **중요:**
   >
   > Citrix Support에서 **OFF**로 전환하라는 지침이 없는 한 HTTPS를 **ON**으로 설정해 두십시오.

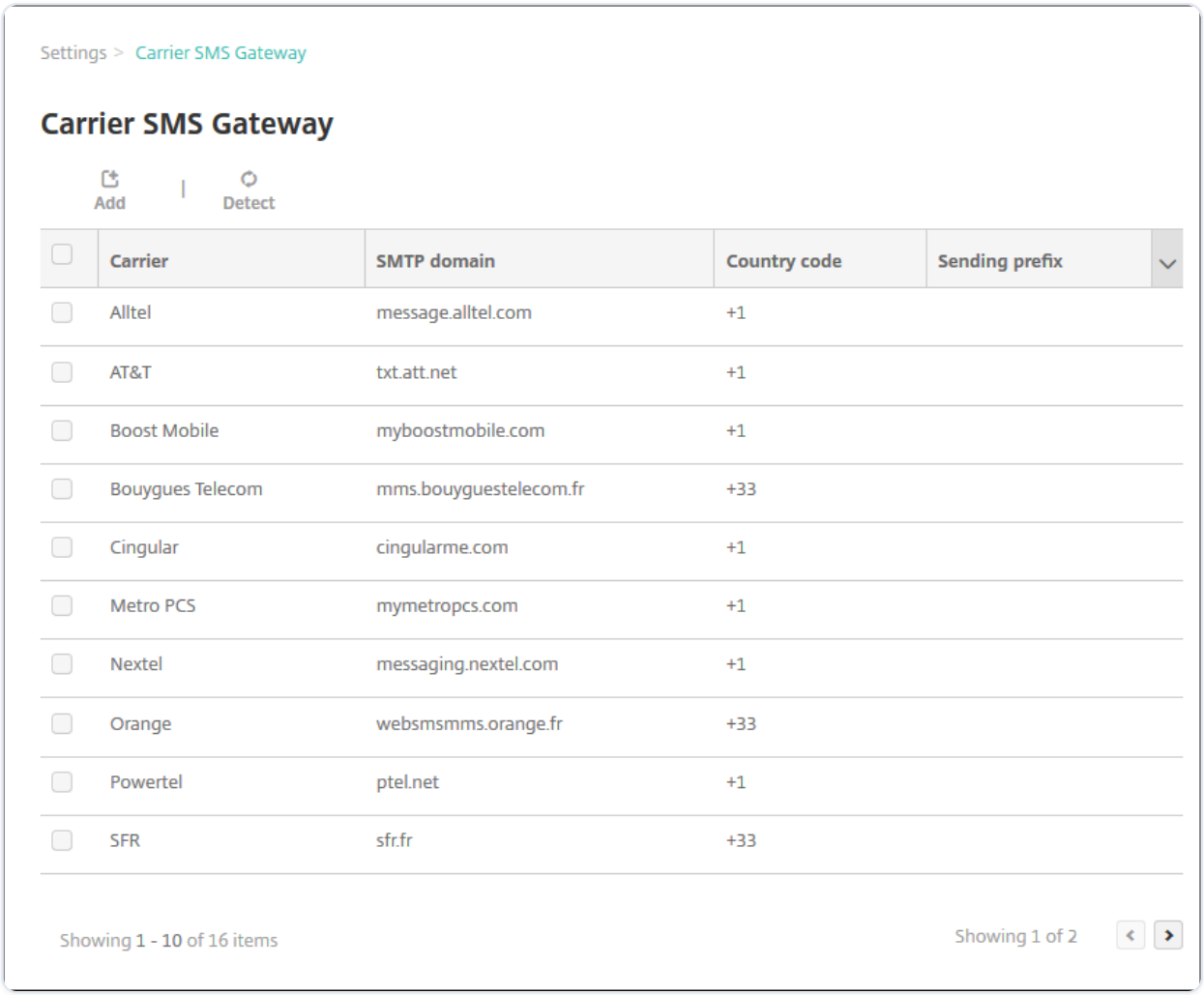
- **국가 코드:** 조직 내 수신자를 위한 기본 SMS 국가 코드 접두사를 드롭다운 목록에서 클릭합니다. 이 필드는 항상 + 기호로 시작합니다. 기본값은 **아프가니스탄 +93**입니다.

2. 현재 구성을 사용하여 테스트 메시지를 보내려면 **구성 테스트**를 클릭합니다. 인증 또는 가상 전화번호 오류와 같은 연결 오류가 감지되어 즉시 나타납니다. 메시지는 휴대폰 간에 전송되는 메시지와 동일한 시간 내에 수신됩니다.
3. **추가**를 클릭합니다.

통신사 SMS 게이트웨이 추가

XenMobile에서 통신사 SMS 게이트웨이를 설정하여 통신사의 SMS 게이트웨이를 통해 전송되는 알림을 구성할 수 있습니다. 통신사는 SMS(Short Message Service) 게이트웨이를 사용하여 통신 네트워크로 또는 통신 네트워크에서 SMS 전송을 보내거나 받습니다. 이러한 텍스트 기반 메시지는 표준화된 통신 프로토콜을 사용하여 유선 또는 휴대폰 장치가 짧은 텍스트 메시지를 교환할 수 있도록 합니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **알림** 아래에서 **통신사 SMS 게이트웨이**를 클릭합니다. **통신사 SMS 게이트웨이** 페이지가 열립니다.



3. 다음 중 하나를 수행합니다.

   - **감지**를 클릭하여 게이트웨이를 자동으로 검색합니다. 새로 감지된 통신사가 없거나 등록된 장치에서 감지된 새 통신사를 나열하는 대화 상자가 나타납니다.
   - **추가**를 클릭합니다. **통신사 SMS 게이트웨이 추가** 대화 상자가 나타납니다.

   알림 서버 SMS 게이트웨이 추가(/en-us/xenmobile/server/media/settings-notifications-carrier-sms-gateway-add.png)

   > **참고:**
   >
   > XenMobile은 Nexmo SMS 메시징만 지원합니다. Nexmo 메시징을 사용할 계정이 아직 없는 경우, 해당 웹사이트를 방문하여 계정을 만드십시오.

4. 다음 설정을 구성합니다.

   - **통신사:** 통신사 이름을 입력합니다.
   - **게이트웨이 SMTP 도메인:** SMTP 게이트웨이와 연결된 도메인을 입력합니다.
   - **국가 코드:** 드롭다운 목록에서 통신사의 국가 코드를 클릭합니다.
   - **이메일 전송 접두사:** 선택적으로 이메일 전송 접두사를 지정합니다.

5. 새 통신사를 추가하려면 **추가**를 클릭하거나, 새 통신사를 추가하지 않으려면 **취소**를 클릭합니다.

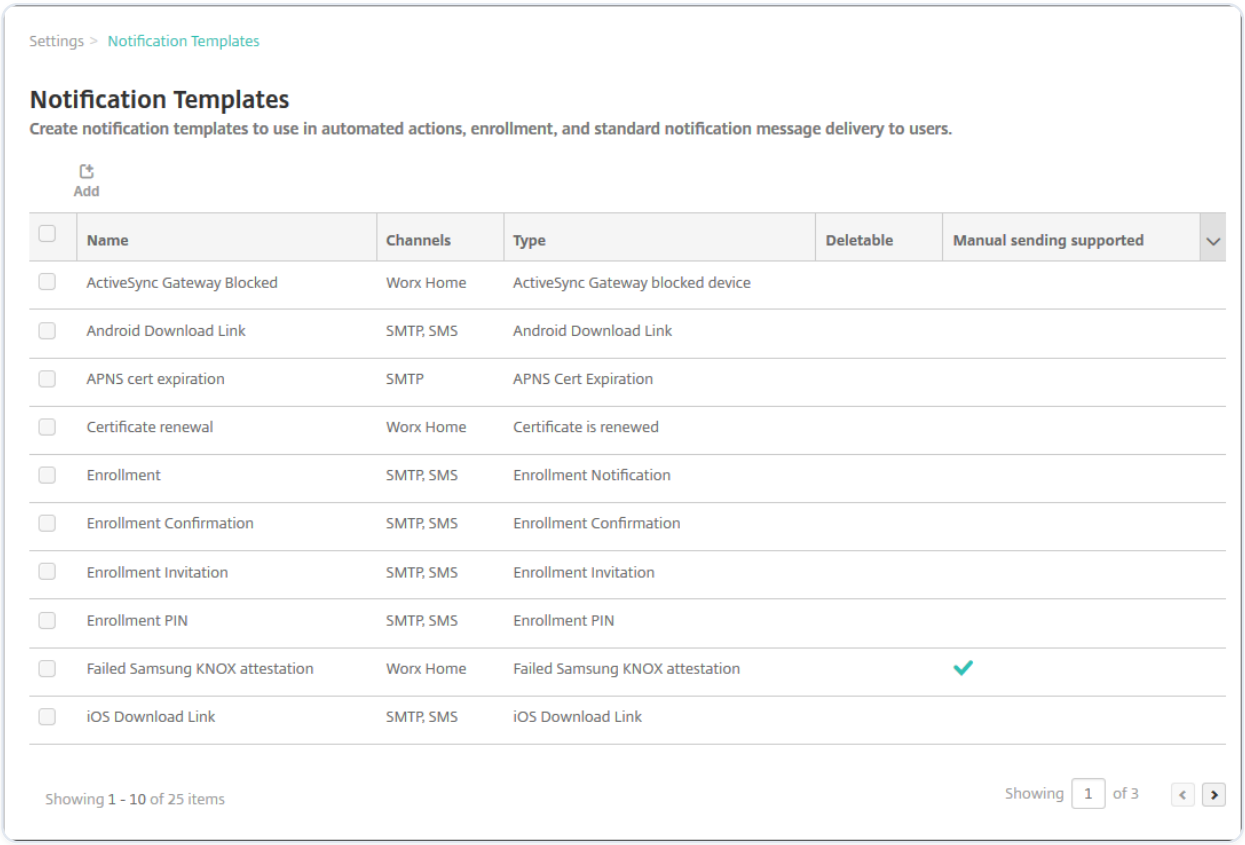
알림 템플릿 생성 및 업데이트

XenMobile에서 알림 템플릿을 생성하거나 업데이트하여 자동화된 작업, 등록 및 사용자에게 전송되는 표준 알림 메시지에 사용할 수 있습니다. 알림 템플릿은 Secure Hub, SMTP 또는 SMS의 세 가지 다른 채널을 통해 메시지를 보내도록 구성합니다.

XenMobile에는 시스템의 모든 장치에 대해 XenMobile이 자동으로 응답하는 고유한 유형의 이벤트를 반영하는 많은 사전 정의된 알림 템플릿이 포함되어 있습니다.

> **참고:**
>
> 사용자에게 알림을 보내기 위해 SMTP 또는 SMS 채널을 사용할 계획이라면, 채널을 활성화하기 전에 설정해야 합니다. XenMobile은 알림 템플릿을 추가할 때 채널이 아직 설정되지 않은 경우 채널 설정을 요청합니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **알림 템플릿**을 클릭합니다. **알림 템플릿** 페이지가 나타납니다.



알림 템플릿 추가

1. **추가**를 클릭합니다. SMS 게이트웨이 또는 SMTP 서버가 설정되지 않은 경우, SMS 및 SMTP 알림 사용에 대한 메시지가 나타납니다. 지금 SMTP 서버 또는 SMS 게이트웨이를 설정하거나 나중에 설정할 수 있습니다.

   지금 SMS 또는 SMTP 서버 설정을 선택하면 **설정** 페이지의 **알림 서버** 페이지로 리디렉션됩니다. 사용하려는 채널을 설정한 후 **알림 템플릿** 페이지로 돌아가 알림 템플릿을 계속 추가하거나 수정할 수 있습니다.

> **중요:**
>
> SMS 또는 SMTP 서버 설정을 나중에 설정하도록 선택하면 알림 템플릿을 추가하거나 편집할 때 해당 채널을 활성화할 수 없으며, 이는 해당 채널을 사용하여 사용자 알림을 보낼 수 없음을 의미합니다.

2. 다음 설정을 구성합니다.

   - **이름:** 템플릿에 대한 설명적인 이름을 입력합니다.
   - **설명:** 템플릿에 대한 설명을 입력합니다.
   - **유형:** 드롭다운 목록에서 알림 유형을 클릭합니다. 선택한 유형에 대해 지원되는 채널만 나타납니다. APNS 인증서 만료 템플릿은 미리 정의된 템플릿으로 하나만 허용됩니다. 즉, 이 유형의 새 템플릿을 추가할 수 없습니다.

   > **참고:**
   >
   > 일부 템플릿 유형의 경우, 유형 아래에 수동 전송 지원이라는 문구가 나타납니다. 이는 템플릿이 **대시보드** 및 **장치** 페이지의 **알림** 목록에서 사용 가능하며, 사용자에게 알림을 수동으로 보낼 수 있음을 의미합니다. 다음 매크로를 어떤 채널의 제목 또는 메시지 필드에서 사용하는 템플릿에서는 수동 전송을 사용할 수 없습니다.

   - ${outofcompliance.reason(allowlist_blocklist_apps_name)}
   - ${outofcompliance.reason(smg_block)}

3. **채널**에서 이 알림에 사용할 각 채널에 대한 정보를 구성합니다. 모든 채널을 선택할 수 있습니다. 선택하는 채널은 알림을 보내는 방법에 따라 달라집니다.

   - **Secure Hub**를 선택하는 경우 iOS 및 Android 장치만 알림을 받으며, 이 알림은 장치의 알림 트레이에 나타납니다.
   - **SMTP**를 선택하는 경우 대부분의 사용자는 이메일 주소로 등록했기 때문에 메시지를 받습니다.
   - **SMS**를 선택하는 경우 SIM 카드가 있는 장치를 사용하는 사용자만 알림을 받습니다.

   시큐어 허브:

   - **활성화:** 알림 채널을 활성화하려면 클릭합니다.
   - **메시지:** 사용자에게 보낼 메시지를 입력합니다. Secure Hub를 사용하는 경우 이 필드는 필수입니다. 메시지에서 매크로를 사용하는 방법에 대한 자세한 내용은 매크로를 참조하십시오.
   - **사운드 파일:** 알림을 받을 때 사용자가 듣는 알림 소리를 드롭다운 목록에서 클릭합니다.

   SMTP:

   - **활성화:** 알림 채널을 활성화하려면 클릭합니다.

     SMTP 서버를 설정한 후에만 SMTP 알림을 활성화할 수 있습니다.

- **보낸 사람:** 알림에 대한 선택적 보낸 사람(이름, 이메일 주소 또는 둘 다)을 입력합니다.
- **받는 사람:** 이 필드에는 알림이 올바른 SMTP 받는 사람 주소로 전송되도록 임시 알림을 제외한 모든 알림에 대한 미리 빌드된 매크로가 있습니다. Citrix는 템플릿에서 매크로를 수정하지 않는 것을 권장합니다. 주소를 세미콜론(;)으로 구분하여 추가하여 사용자 외에 받는 사람(예: 회사 관리자)을 추가할 수도 있습니다. 임시 알림을 보내려면 이 페이지에서 특정 받는 사람을 입력하거나 **관리 > 장치** 페이지에서 장치를 선택하여 거기에서 알림을 보낼 수 있습니다. 자세한 내용은 장치를 참조하십시오.
- **제목:** 알림에 대한 설명적인 제목을 입력합니다. 이 필드는 필수입니다.
- **메시지:** 사용자에게 보낼 메시지를 입력합니다. 메시지에서 매크로 사용에 대한 자세한 내용은 매크로를 참조하십시오.

SMS:

- **활성화:** 알림 채널을 활성화하려면 클릭합니다.

  SMTP 서버를 설정한 후에만 SMTP 알림을 활성화할 수 있습니다.
- **수신자:** 이 필드에는 알림이 올바른 SMS 수신자 주소로 전송되도록 Ad Hoc 알림을 제외한 모든 알림에 대한 미리 빌드된 매크로가 있습니다. Citrix는 템플릿의 매크로를 수정하지 않는 것이 좋습니다. Ad Hoc 알림을 보내려면 특정 수신자를 입력하거나 **관리 > 장치** 페이지에서 장치를 선택할 수 있습니다.
- **메시지:** 사용자에게 보낼 메시지를 입력합니다. 이 필드는 필수입니다. 메시지에서 매크로 사용에 대한 자세한 내용은 매크로를 참조하십시오.

4. **추가**를 클릭합니다. 모든 채널이 올바르게 구성되면 **알림 템플릿** 페이지에 SMTP, SMS, Secure Hub 순서로 표시됩니다. 올바르게 구성되지 않은 채널은 올바르게 구성된 채널 뒤에 나타납니다.

알림 템플릿 편집

1. 알림 템플릿을 선택합니다. 해당 템플릿에 대한 편집 페이지가 나타나며, 여기에서 **유형** 필드를 제외한 모든 항목을 변경하고 채널을 활성화 또는 비활성화할 수 있습니다.
2. **저장**을 클릭합니다.

알림 템플릿 삭제

추가한 알림 템플릿만 삭제할 수 있습니다. 미리 정의된 알림 템플릿은 삭제할 수 없습니다.

1. 기존 알림 템플릿을 선택합니다.
2. **삭제**를 클릭합니다. 확인 대화 상자가 나타납니다.
3. **삭제**를 클릭하여 알림 템플릿을 삭제하거나, **취소**를 클릭하여 알림 템플릿 삭제를 취소합니다.

장치

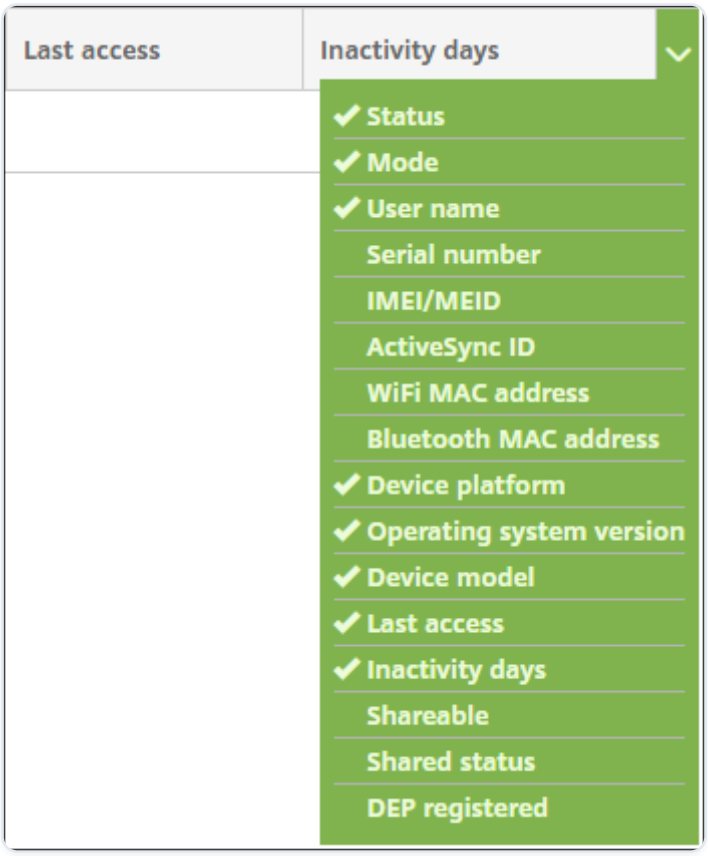
Citrix XenMobile®은 단일 관리 콘솔 내에서 광범위한 장치 유형을 프로비저닝, 관리, 보호 및 인벤토리할 수 있습니다.

XenMobile Server 데이터베이스는 모바일 장치 목록을 저장합니다. 고유한 일련 번호 또는 국제 모바일 가입자 식별 번호(IMEI)/모바일 장비 식별자(MEID)가 각 모바일 장치를 고유하게 정의합니다. XenMobile 콘솔에 장치를 채우려면 장치를 수동으로 추가하거나 파일에서 장치 목록을 가져올 수 있습니다. 장치 프로비저닝 파일 형식에 대한 자세한 내용은 이 문서의 뒷부분에 있는 장치 프로비저닝 파일 형식을 참조하십시오.

XenMobile 콘솔의 **장치** 페이지에는 각 장치와 다음 정보가 나열됩니다.

- **상태:** 아이콘은 장치가 탈옥되었는지, 관리되는지, Active Sync Gateway를 사용할 수 있는지, 배포 상태를 나타냅니다.
- **모드:** 장치 모드가 MDM, MAM 또는 둘 다인지 여부.
- 장치에 대한 기타 정보(예: **사용자 이름**, **장치 플랫폼**, **운영 체제 버전**, **장치 모델**, **마지막 액세스**, **비활성 일수**). 이 제목들은 기본적으로 표시됩니다.

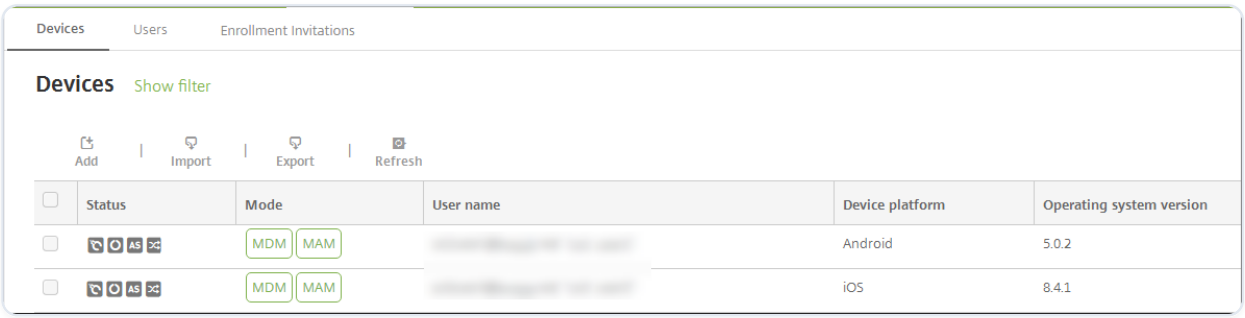
장치 테이블을 사용자 지정하려면 마지막 제목의 아래쪽 화살표를 클릭합니다. 그런 다음 테이블에서 보려는 추가 제목을 선택하거나 제거할 제목을 지웁니다.



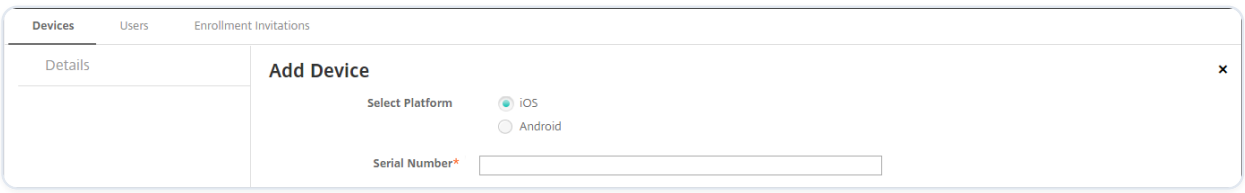
장치를 수동으로 추가하거나, 장치 프로비저닝 파일에서 장치를 가져오거나, 장치 세부 정보를 편집하거나, 보안 작업을 수행하거나, 장치에 알림을 보낼 수 있습니다. 또한 모든 장치 테이블 데이터를 .csv 파일로 내보내 사용자 지정 보고서를 만들 수 있습니다. 서버는 모든 장치 속성을 내보냅니다. 필터를 적용하면 XenMobile은 .csv 파일을 만들 때 해당 필터를 사용합니다.

장치 수동 추가

1. XenMobile 콘솔에서 **관리 > 장치**를 클릭합니다. **장치** 페이지가 나타납니다.



2. **추가**를 클릭합니다. **장치 추가** 페이지가 나타납니다.



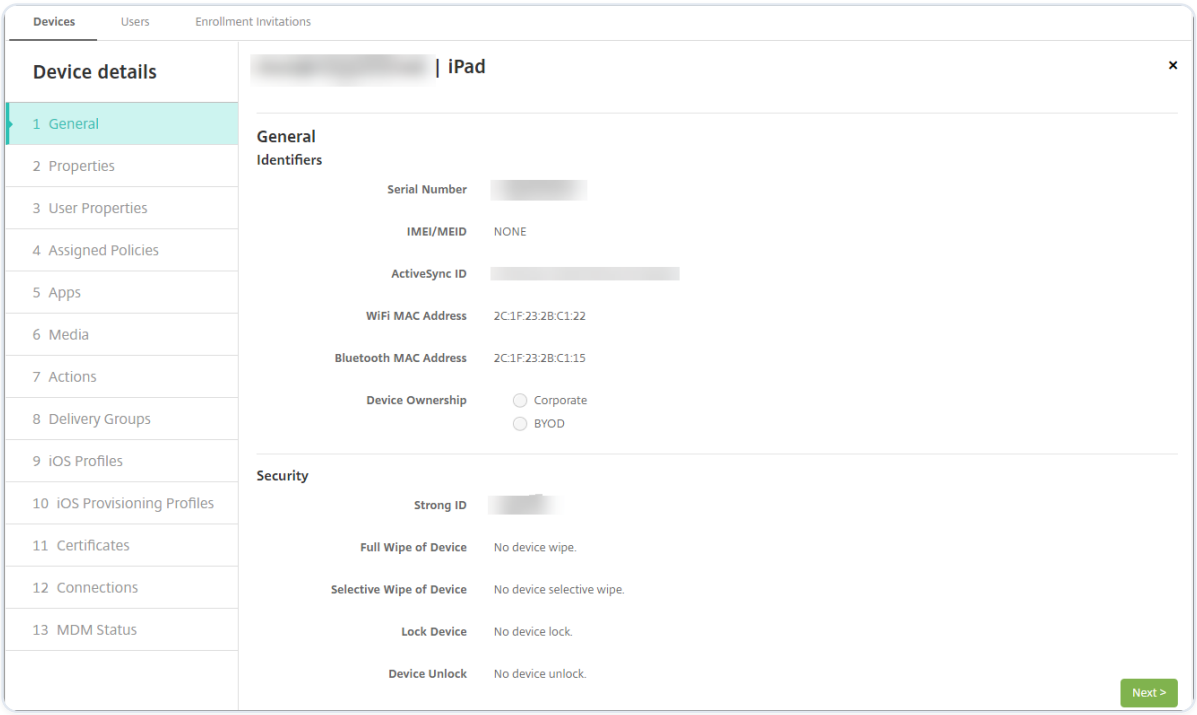
3. 다음 설정을 구성합니다:

- **플랫폼 선택: iOS** 또는 **Android**를 클릭합니다.
- **일련 번호:** 장치 일련 번호를 입력합니다.
- **IMEI/MEID:** 선택 사항으로, Android 장치에만 해당하며, 장치 IMEI/MEID 정보를 입력합니다.

4. **추가**를 클릭합니다. **장치** 테이블이 나타나고 장치가 목록 하단에 추가됩니다. 추가한 장치를 선택한 다음 나타나는 메뉴에서 **편집**을 클릭하여 장치 세부 정보를 확인합니다.

> **참고:**
>
> 장치 옆의 확인란을 선택하면 장치 목록 위에 옵션 메뉴가 나타납니다. 목록의 다른 곳을 클릭하면 옵션 메뉴가 목록의 오른쪽에 나타납니다.

- Enterprise (XME) 또는 MDM 모드로 구성된 XenMobile Server
- LDAP 구성됨
- 로컬 그룹 및 로컬 사용자를 사용하는 경우:
  - 하나 이상의 로컬 그룹.
  - 로컬 그룹에 할당된 로컬 사용자.
  - 전달 그룹은 로컬 그룹과 연결됩니다.
- Active Directory를 사용하는 경우:
  - 전달 그룹은 Active Directory 그룹과 연결됩니다.



5. **일반** 페이지에는 일련 번호, ActiveSync ID 및 플랫폼 유형에 대한 기타 정보와 같은 장치 **식별자**가 나열됩니다. **장치 소유권**의 경우 **회사 소유** 또는 **BYOD**를 선택합니다.

   일반 페이지에는 강력한 ID, 장치 잠금, 활성화 잠금 우회 및 플랫폼 유형에 대한 기타 정보와 같은 장치 **보안** 속성도 나열됩니다. **장치 전체 초기화** 필드에는 사용자 PIN 코드가 포함됩니다. 장치가 초기화된 후 사용자는 해당 코드를 입력해야 합니다. 사용자가 코드를 잊어버린 경우 여기에서 찾을 수 있습니다.

6. **속성** 페이지에는 XenMobile이 프로비저닝할 장치 속성이 나열됩니다. 이 목록은 장치를 추가하는 데 사용된 프로비저닝 파일에 포함된 모든 장치 속성을 보여줍니다. 속성을 추가하려면 **추가**를 클릭한 다음 목록에서 속성을 선택합니다. 각 속성에 대한 유효한 값은 PDF 장치 속성 이름 및 값을 참조하십시오.

   속성을 추가하면, 처음에는 추가한 카테고리 아래에 나타납니다. **다음**을 클릭한 다음 **속성** 페이지로 돌아오면, 해당 속성이 적절한 목록에 표시됩니다.

   속성을 삭제하려면 목록 위에 마우스를 올린 다음 오른쪽에 있는 **X**를 클릭합니다. XenMobile은 해당 항목을 즉시 삭제합니다.

7. 나머지 **장치 세부 정보** 섹션에는 장치에 대한 요약 정보가 포함되어 있습니다.

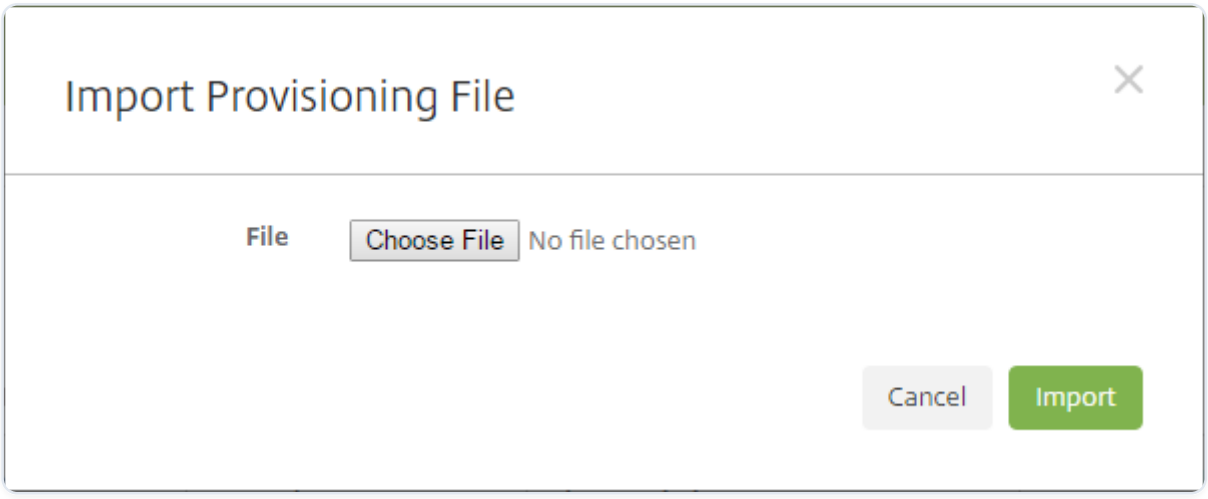
   - **사용자 속성:** RBAC 역할, 그룹 멤버십, 볼륨 구매 계정 및 사용자에 대한 속성을 표시합니다. 이 페이지에서 볼륨 구매 계정을 해지할 수 있습니다.
   - **할당된 정책:** 배포됨, 보류 중, 실패한 정책 수를 포함하여 할당된 정책 수를 표시합니다. 각 정책에 대한 정책 이름, 유형 및 마지막 배포 정보를 제공합니다.
   - **앱:** 마지막 인벤토리에 대해 설치됨, 보류 중, 실패한 앱 배포 수를 표시합니다. 앱 이름, 식별자, 유형 및 기타 정보를 제공합니다.

- **미디어:** 최신 인벤토리 기준으로 배포됨, 보류 중, 실패한 미디어 배포 수를 표시합니다.
- **작업:** 배포됨, 보류 중, 실패한 작업 수를 표시합니다. 작업 이름과 마지막 배포 시간을 제공합니다.
- **배포 그룹:** 성공, 보류 중, 실패한 배포 그룹의 수를 표시합니다. 각 배포에 대해 배포 그룹 이름과 배포 시간을 제공합니다. 배포 그룹을 선택하여 상태, 작업, 채널 또는 사용자를 포함한 자세한 정보를 볼 수 있습니다.
- **iOS 프로필:** 이름, 유형, 조직 및 설명을 포함하여 마지막 iOS 프로필 인벤토리를 표시합니다.
- **iOS 프로비저닝 프로필:** UUID, 만료일, 관리 여부 등 엔터프라이즈 배포 프로비저닝 프로필 정보를 표시합니다.
- **인증서:** 유효, 만료 또는 해지된 인증서에 대해 유형, 공급자, 발급자, 일련 번호 및 만료까지 남은 일수와 같은 정보를 표시합니다.
- **연결:** 첫 번째 연결 상태와 마지막 연결 상태를 표시합니다. 각 연결에 대해 사용자 이름, 마지막에서 두 번째 인증 시간 및 마지막 인증 시간을 제공합니다.
- **MDM 상태:** MDM 상태, 마지막 푸시 시간 및 마지막 장치 응답 시간과 같은 정보를 표시합니다.

프로비저닝 파일에서 장치 가져오기

이동통신사 또는 장치 제조업체에서 제공하는 파일을 가져오거나 자체 장치 프로비저닝 파일을 만들 수 있습니다. 자세한 내용은 이 문서의 뒷부분에 있는 장치 프로비저닝 파일 형식을 참조하십시오.

1. **관리 > 장치**로 이동한 다음 **가져오기**를 클릭합니다. **프로비저닝 파일 가져오기** 대화 상자가 나타납니다.

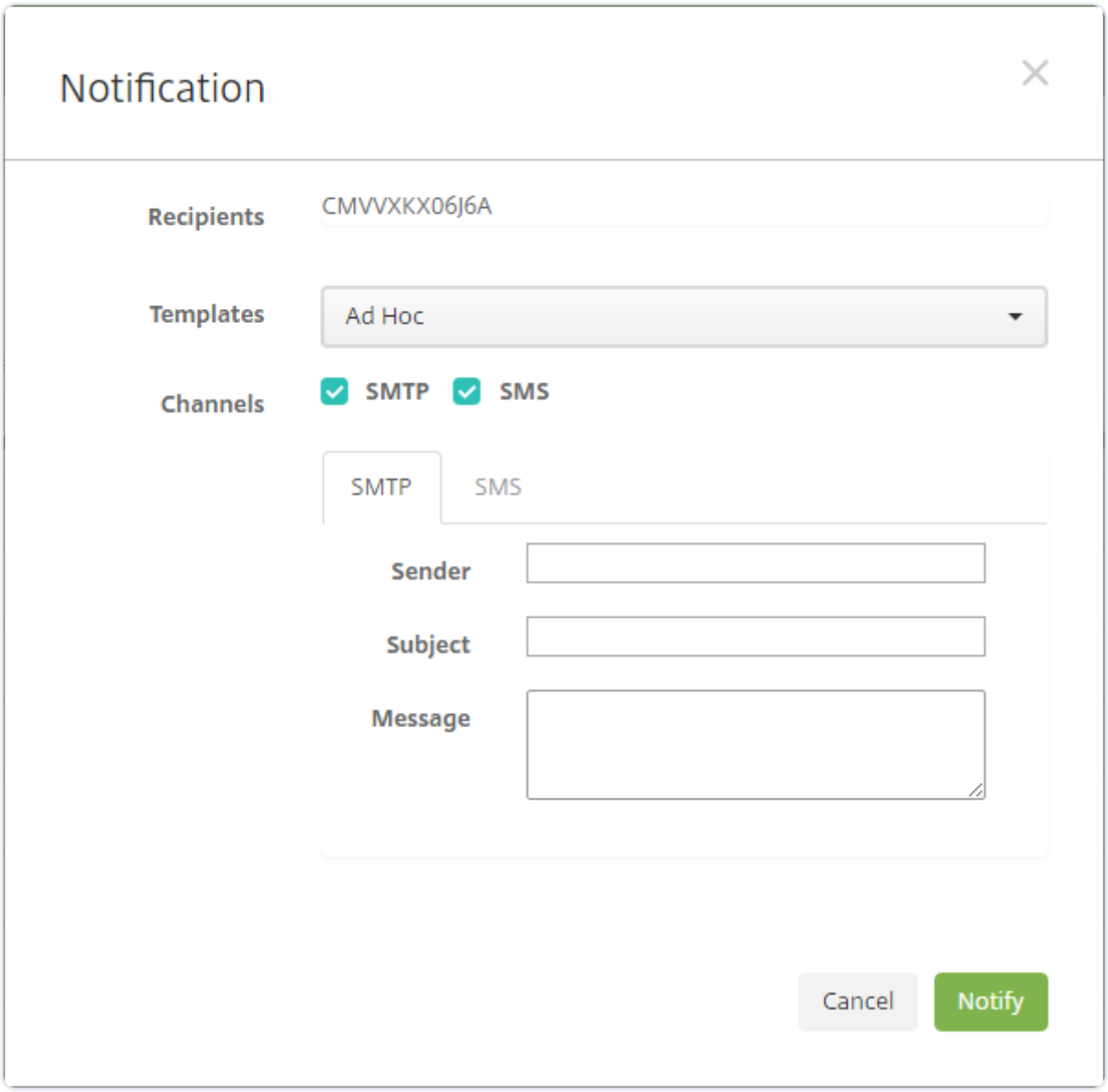


2. **파일 선택**을 클릭한 다음 가져올 파일로 이동합니다.
3. **가져오기**를 클릭합니다. **장치** 테이블에 가져온 파일이 나열됩니다.
4. 장치 정보를 편집하려면 해당 정보를 선택한 다음 **편집**을 클릭합니다. **장치 세부 정보** 페이지에 대한 자세한 내용은 장치 수동 추가를 참조하십시오.

장치에 알림 보내기

장치 페이지에서 장치에 알림을 보낼 수 있습니다. 알림에 대한 자세한 내용은 알림을 참조하십시오.

1. **관리 > 장치** 페이지에서 알림을 보낼 장치를 선택합니다.
2. **알림**을 클릭합니다. **알림** 대화 상자가 나타납니다. **수신자** 필드에는 알림을 받을 모든 장치가 나열됩니다
   .



3. 다음 설정을 구성합니다.

   - **템플릿:** 목록에서 보낼 알림 유형을 클릭합니다. **임시**를 제외한 각 템플릿에 대해 **제목** 및 **메시지** 필드에는 선택한 템플릿에 대해 구성된 텍스트가 표시됩니다.
   - **채널:** 메시지를 보내는 방법을 선택합니다. 기본값은 **SMTP** 및 **SMS**입니다. 각 채널의 메시지 형식을 보려면 탭을 클릭합니다.
   - **보낸 사람:** 선택적 보낸 사람을 입력합니다.

- **제목: 임시** 메시지의 제목을 입력합니다.
- **메시지: 임시** 메시지의 메시지를 입력합니다.

4. **알림**을 클릭합니다.

장치 테이블 내보내기

1. 내보내기 파일에 표시할 내용에 따라 **장치** 테이블을 필터링합니다.
2. **장치** 테이블 위에 있는 **내보내기** 단추를 클릭합니다. XenMobile은 필터링된 **장치** 테이블의 정보를 추출하여 .csv 파일로 변환합니다.
3. 메시지가 표시되면 .csv 파일을 열거나 저장합니다.

사용자 장치 수동으로 태그 지정

다음과 같은 방법으로 XenMobile에서 장치를 수동으로 태그 지정할 수 있습니다.

- 초대 기반 등록 프로세스 중.
- 셀프 서비스 포털 등록 프로세스 중.
- 장치 소유권을 장치 속성으로 추가하여

장치를 회사 소유 또는 직원 소유로 태그할 수 있습니다. 셀프 도움말 포털을 사용하여 장치를 자체 등록할 때 장치를 회사 소유 또는 직원 소유로 태그할 수 있습니다. 장치를 수동으로 태그할 수도 있으며, 방법은 다음과 같습니다.

1. XenMobile 콘솔의 **장치** 탭에서 장치에 속성을 추가합니다.
2. **소유자**라는 속성을 추가하고 **회사** 또는 **BYOD**(직원 소유) 중 하나를 선택합니다.

   소유자 속성 설정 이미지(/en-us/xenmobile/server/media/manage-devices-properties-owned-by.png)

장치 프로비저닝 파일 형식

많은 모바일 통신사 또는 장치 제조업체에서 승인된 모바일 장치 목록을 제공합니다. 이러한 목록을 사용하여 긴 모바일 장치 목록을 수동으로 입력할 필요가 없습니다. XenMobile은 지원되는 세 가지 장치 유형(Android, iOS, Windows) 모두에 공통적인 가져오기 파일 형식을 지원합니다.

수동으로 생성하여 XenMobile로 장치를 가져오는 데 사용하는 프로비저닝 파일은 다음 형식이어야 합니다.

SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

다음 사항을 유의하십시오.

- 각 속성의 유효한 값은 PDF 장치 속성 이름 및 값을 참조하십시오.
- UTF-8 문자 집합을 사용하십시오.
- 프로비저닝 파일 내의 필드를 구분하려면 세미콜론(;)을 사용하십시오. 필드의 일부에 세미콜론이 포함된 경우 백슬래시 문자(\)로 이스케이프 처리하십시오.

  예를 들어, 이 속성의 경우:

  `propertyV;test;1;2`

  다음과 같이 이스케이프 처리합니다.

  `propertyV\;test\;1\;2`
- iOS 장치의 경우 일련 번호가 iOS 장치 식별자이므로 일련 번호가 필요합니다.
- 다른 장치 플랫폼의 경우 일련 번호 또는 IMEI를 포함해야 합니다.
- **OperatingSystemFamily**에 유효한 값은 **WINDOWS**, **ANDROID**, 또는 **iOS**입니다.

장치 프로비저닝 파일의 예:

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;prop
ertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;prope
rtyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;`
```

파일의 각 줄은 장치를 설명합니다. 위 샘플의 첫 번째 항목은 다음을 의미합니다.

- 일련 번호: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- 운영 체제 제품군: `WINDOWS`
- 속성 이름: `propertyN`
- 속성 값: `propertyV\;test\;1\;2;prop 2`

ActiveSync 게이트웨이

ActiveSync는 Microsoft에서 개발한 모바일 데이터 동기화 프로토콜입니다. ActiveSync는 핸드헬드 장치 및 데스크톱(또는 랩톱) 컴퓨터와 데이터를 동기화합니다.

XenMobile에서 ActiveSync Gateway 규칙을 구성할 수 있습니다. 이러한 규칙에 따라 장치의 ActiveSync 데이터 액세스를 허용하거나 거부할 수 있습니다. 예를 들어, 필수 앱 누락 규칙을 활성화하면 XenMobile은 필수 앱에 대한 앱 액세스 정책을 확인하고 필수 앱이 누락된 경우 ActiveSync 데이터 액세스를 거부합니다. 각 규칙에 대해 **허용** 또는 **거부**를 선택할 수 있습니다. 기본 설정은 **허용**으로 설정됩니다.

앱 액세스 장치 정책에 대한 자세한 내용은 앱 액세스 장치 정책을 참조하십시오.

XenMobile은 다음 규칙을 지원합니다.

익명 장치: 장치가 익명 모드인지 확인합니다. 이 확인은 장치가 다시 연결을 시도할 때 XenMobile이 사용자를 다시 인증할 수 없는 경우에 사용할 수 있습니다.

Samsung KNOX 증명 실패: 장치가 Samsung KNOX 증명 서버 쿼리에 실패했는지 확인합니다.

금지된 앱: 앱 액세스 정책에 정의된 대로 장치에 금지된 앱이 있는지 확인합니다.

암시적 허용 및 거부: 이 작업은 ActiveSync Gateway의 기본값입니다. 게이트웨이는 다른 필터 규칙 조건을 충족하지 않는 모든 장치의 장치 목록을 생성하고 해당 목록을 기반으로 연결을 허용하거나 거부합니다. 일치하는 규칙이 없으면 기본값은 암시적 허용입니다.

비활성 장치: 서버 속성의 **장치 비활성 일수 임계값** 설정에 정의된 대로 장치가 비활성 상태인지 확인합니다.

필수 앱 누락: 앱 액세스 정책에 정의된 대로 장치에 필수 앱이 누락되었는지 확인합니다.

권장되지 않는 앱: 앱 액세스 정책에 정의된 대로 장치에 권장되지 않는 앱이 있는지 확인합니다.

비준수 암호: 사용자 암호가 규정을 준수하는지 확인합니다. iOS 및 Android 장치에서 XenMobile은 현재 장치에 있는 암호가 장치로 전송된 암호 정책을 준수하는지 여부를 확인할 수 있습니다. 예를 들어, iOS에서 XenMobile이 장치로 암호 정책을 보내면 사용자는 암호를 설정하는 데 60분이 주어집니다. 사용자가 암호를 설정하기 전에 암호가 규정을 준수하지 않을 수 있습니다.

규정 미준수 장치: 규정 미준수 장치 속성을 기반으로 장치가 규정을 준수하지 않는지 확인합니다. 이 속성은 일반적으로 자동화된 작업 또는 XenMobile API를 활용하는 타사에 의해 변경됩니다.

해지된 상태: 장치 인증서가 해지되었는지 확인합니다. 해지된 장치는 다시 승인될 때까지 재등록할 수 없습니다.

루팅된 Android 및 탈옥된 iOS 장치: Android 또는 iOS 장치가 탈옥되었는지 확인합니다.

관리되지 않는 장치: 장치가 XenMobile 제어 하에 관리되는 상태인지 확인합니다. 예를 들어, MAM에 등록된 장치 또는 등록되지 않은 장치는 관리되지 않습니다.

Android 도메인 사용자를 ActiveSync Gateway로 전송: XenMobile이 Android 장치 정보를 ActiveSync Gateway로 전송하도록 하려면 **예**를 클릭합니다.

ActiveSync Gateway 설정 구성

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **서버** 아래에서 **ActiveSync Gateway**를 클릭합니다. **ActiveSync Gateway** 페이지가 나타납니다.

ActiveSync Gateway 이미지(/en-us/xenmobile/server/media/settings-server-activesync-gateway.png)

1. **다음 규칙 활성화**에서 활성화할 규칙을 하나 이상 선택합니다.
2. **Android 전용**에서 **Android 도메인 사용자를 ActiveSync Gateway로 전송**에서 **예**를 클릭하여 XenMobile이 Android 장치 정보를 ActiveSync Gateway로 전송하도록 합니다.
3. **저장**을 클릭합니다.

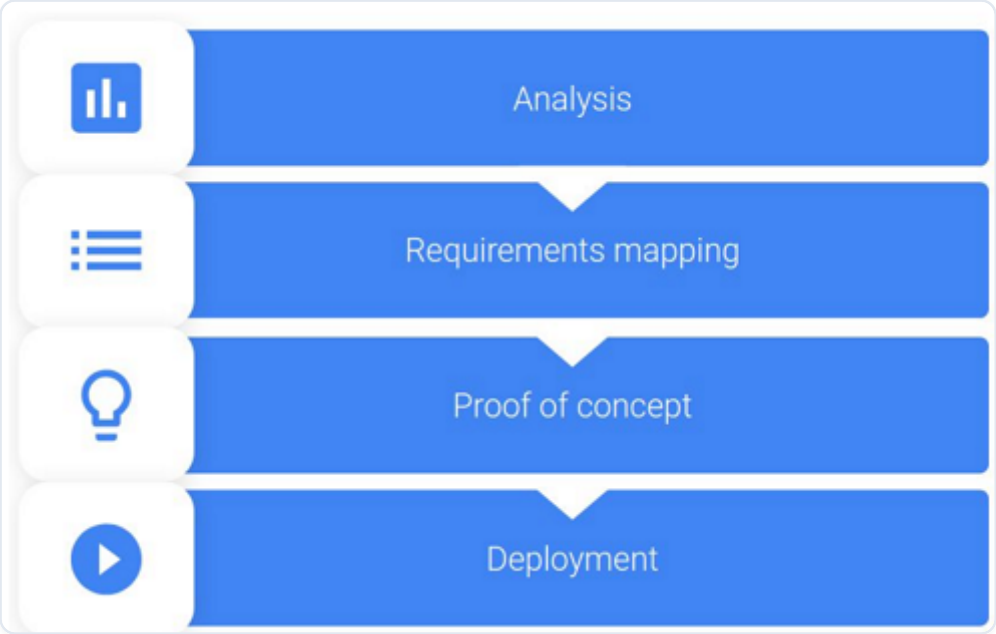
기기 관리에서 Android Enterprise로 마이그레이션

이 문서에서는 기존 Android 기기 관리에서 Android Enterprise로 마이그레이션하기 위한 고려 사항 및 권장 사항에 대해 설명합니다. Google은 Android 기기 관리 API를 더 이상 사용하지 않습니다. 이 API는 Android 기기에서 엔터프라이즈 앱을 지원했습니다. Android Enterprise는 Google 및 Citrix에서 권장하는 최신 관리 솔루션입니다.

XenMobile®은 Android 기기의 기본 등록 방법으로 Android Enterprise로 변경됩니다. Google이 API를 더 이상 사용하지 않게 되면 기기 관리 모드의 Android Q 기기에서는 등록이 실패합니다.

Android Enterprise는 완전 관리형 및 업무 프로필 기기 모드를 지원합니다. Google 발행물인 Android Enterprise Migration Bluebook은 기존 기기 관리와 Android Enterprise가 어떻게 다른지 자세히 설명합니다. Google의 마이그레이션 정보를 읽어보시는 것을 권장합니다.

이 발행물은 또한 기기 관리 마이그레이션의 네 가지 단계를 설명하고 다음 다이어그램을 포함합니다. 이 문서에는 마이그레이션 단계에 대한 XenMobile별 권장 사항이 포함되어 있습니다.



Android Enterprise Migration Bluebook의 다이어그램. Google의 허가를 받아 재게시되었습니다.

기기 관리 사용 중단이 미치는 영향

Google은 다음 기기 관리 API를 더 이상 사용하지 않습니다. Secure Hub를 Android Q API 수준을 대상으로 업그레이드한 후에는 이 API가 Android Q를 실행하는 기기에서 작동하지 않습니다.

- 카메라 비활성화: 기기 카메라에 대한 액세스를 제어합니다.
- 암호 만료: 구성 가능한 기간 후에 사용자가 암호를 변경하도록 강제합니다.
- 암호 제한: 제한적인 암호 요구 사항을 설정합니다.

더 이상 사용되지 않는 API는 Citrix MAM 전용 모드에 등록된 기기에는 영향을 미치지 않습니다.

권장 사항

다음 권장 사항은 이미 Android 레거시 기기 관리 모드에 등록된 기기, 등록되지 않은 기기 및 Citrix MAM 전용 모드에 등록된 기기에 대한 것입니다.

장치 등록 상태	권장 조치
기존 장치가 장치 관리 모드에 등록되어 있으며 Android Q로 업그레이드할 수 있습니다.	장치를 Android Q로 업그레이드하기 전에 장치 관리 모드에서 Android Enterprise로 마이그레이션하십시오.

장치 등록 상태	권장 조치
기존 장치가 장치 관리 모드에 등록되어 있습니다. 이 장치는 Android Q로 업그레이드할 수 없습니다.	장치는 장치 관리 모드를 유지할 수 있습니다. 그러나 장치 새로 고침 시 장치를 Android Enterprise로 이동할 계획을 세우십시오.
기존 장치가 장치 관리 모드에 등록되어 있으며 Android Q로 업그레이드되었습니다.	Google이 API를 더 이상 사용하지 않도록 설정하기 전에 장치 관리 모드에서 Android Enterprise로 마이그레이션하십시오. 이러한 장치에 대한 경고 메시지가 XenMobile 콘솔에 나타납니다.
Android Q와 함께 제공되고 장치 관리 모드에 등록된 새 장치.	Google이 API를 더 이상 사용하지 않도록 설정하기 전에 장치 관리 모드에서 Android Enterprise로 마이그레이션하십시오. 이러한 장치에 대한 경고 메시지가 XenMobile 콘솔에 나타납니다.
Android Q와 함께 제공되거나 Android Q로 업그레이드할 수 있는 새 장치. 장치가 등록되지 않았습니다.	모든 새 장치에 Android Enterprise를 사용하십시오.
Google이 API를 더 이상 사용하지 않도록 설정한 후 Android Q의 새 장치 또는 기존 장치가 장치 관리 모드에 등록됩니다.	더 이상 사용되지 않는 Google API의 영향을 피하려면 Google이 API를 더 이상 사용하지 않도록 설정하기 전에 Android Enterprise로 마이그레이션하는 것이 좋습니다. 해당 날짜 이후에는 이러한 장치의 등록이 실패합니다.
Citrix MAM 전용 모드에 등록된 새 장치 또는 기존 장치	조치할 필요가 없습니다. 더 이상 사용되지 않는 Google API는 MAM 전용 모드의 장치에 영향을 미치지 않습니다.

분석

마이그레이션의 분석 단계는 다음으로 구성됩니다.

- 기존 Android 설정 이해
- 기존 기능을 Android Enterprise 기능에 매핑할 수 있도록 기존 설정 문서화

권장 분석

1. XenMobile에서 Android Enterprise 평가: 완전 관리형, 업무 프로필이 있는 완전 관리형, 전용 장치, 업무 프로필(BYOD).
2. 현재 장치 관리 기능을 Android Enterprise와 비교하여 분석합니다.

3. 장치 관리 사용 사례를 문서화합니다.

장치 관리 사용 사례를 문서화하려면 다음을 수행합니다.

1. 스프레드시트를 만들고 XenMobile 콘솔에 있는 현재 정책 그룹을 나열합니다.
2. 기존 정책 그룹을 기반으로 별도의 사용 사례를 만듭니다.
3. 각 사용 사례에 대해 다음을 문서화합니다.
    - 이름
    - 사업주
    - 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 앱인지 비공개 앱인지 여부
    - 앱이 필수 앱인지 여부 (true/false)

요구 사항 매핑

완료된 분석을 기반으로 Android Enterprise 기능 요구 사항을 결정합니다.

권장 요구 사항 매핑

1. 관리 모드 및 등록 방법을 결정합니다.

- 업무 프로필 (BYOD): 재등록이 필요합니다. 공장 초기화는 필요하지 않습니다.
- 완전 관리형: 공장 초기화가 필요합니다. QR 코드, 근거리 무선 통신(NFC) 범프, 장치 정책 컨트롤러(DPC) 식별자, 제로 터치를 사용하여 장치를 등록합니다.

2. 앱 마이그레이션 전략을 만듭니다.
3. 사용 사례 요구 사항을 Android Enterprise 기능에 매핑합니다. 각 장치 요구 사항에 대해 해당 요구 사항과 가장 일치하는 기능 및 해당 Android 버전을 문서화합니다.
4. 기능 요구 사항(7.0, 8.0, 9.0)에 따라 최소 Android OS를 결정합니다.
5. ID 모델을 선택합니다.
   - 권장: 관리형 Google Play 계정
   - Google Cloud Identity 고객인 경우에만 Google G-Suite 계정을 사용하십시오.
6. 장치 전략을 만듭니다.
   - 조치 없음: 장치가 최소 OS 수준을 충족하는 경우
   - 업그레이드: 장치가 지원되는 OS를 지원하고 해당 OS로 업데이트할 수 있는 경우
   - 교체: 장치를 지원되는 OS 수준으로 업데이트할 수 없는 경우

권장 앱 마이그레이션 전략

요구 사항 매핑을 완료한 후, 앱을 Android 플랫폼에서 Android Enterprise 플랫폼으로 이동합니다. 앱 게시 방법에 대한 자세한 내용은 앱 추가를 참조하십시오.

- 공개 스토어 앱

  a. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 Google Play 설정을 지우고 플랫폼으로 **Android Enterprise**를 선택합니다.

  b. 전달 그룹을 선택합니다. 앱이 필수인 경우, 해당 앱을 전달 그룹의 **필수 앱** 목록으로 이동합니다.

  앱을 저장하면 Google Play 스토어에 나타납니다. 업무 프로필이 있는 경우, 앱은 업무 프로필의 Google Play 스토어에 나타납니다.

- 개인(기업) 앱

  개인 앱은 사내 또는 타사 개발자가 개발합니다. Google Play를 사용하여 개인 앱을 게시하는 것을 권장합니다.

  a. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 플랫폼으로 **Android Enterprise**를 선택합니다.

  b. APK 파일을 업로드한 다음 앱 설정을 구성합니다.

c. 필요한 전달 그룹에 앱을 게시합니다.

- MDX 앱

a. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 플랫폼으로 **Android Enterprise**를 선택합니다.

b. MDX 파일을 업로드합니다. 앱 승인 절차를 진행합니다.

c. MDX 정책을 선택합니다.

Enterprise MDX 앱의 경우 MDX SDK 모드 래핑 앱으로 변경하는 것이 좋습니다.

- 옵션 1: 조직에 비공개로 할당된 개발자 계정을 사용하여 Google Play에서 APK를 호스팅합니다. XenMobile에 MDX 파일을 게시합니다.
- 옵션 2: XenMobile에서 앱을 엔터프라이즈 앱으로 게시합니다. XenMobile에 APK를 게시하고 MDX 파일에 대한 플랫폼으로 **Android Enterprise**를 선택합니다.

Citrix 장치 정책 마이그레이션

Android 및 Android Enterprise 플랫폼 모두에서 사용할 수 있는 정책의 경우: 정책을 편집하고 플랫폼으로 **Android Enterprise**를 선택합니다.

Android Enterprise의 경우 등록 모드를 고려하십시오. 일부 정책 옵션은 업무 프로필 모드 또는 완전 관리 모드의 장치에서만 사용할 수 있습니다.

개념 증명

앱을 Android Enterprise로 마이그레이션한 후 마이그레이션 테스트를 설정하여 기능이 의도한 대로 작동하는지 확인할 수 있습니다.

권장 개념 증명 설정

1. 배포 인프라를 설정합니다.
   - Android Enterprise 테스트를 위한 Delivery Group을 생성합니다.
   - XenMobile에서 Android Enterprise를 구성합니다.
2. 사용자 앱을 설정합니다.
3. Android Enterprise 기능을 구성합니다.
4. Android Enterprise 전송 그룹에 정책을 할당합니다.
5. 기능을 테스트하고 확인합니다.
6. 각 사용 사례에 대한 장치 설정 연습을 완료합니다.
7. 사용자 설정 단계를 문서화합니다.

배포

이제 Android Enterprise 설정을 배포하고 사용자의 마이그레이션을 준비할 수 있습니다.

권장 배포 전략

Citrix에서 권장하는 배포 전략은 Android Enterprise용 모든 프로덕션 시스템을 테스트한 다음 나중에 장치 마이그레이션을 완료하는 것입니다.

- 이 시나리오에서는 사용자가 현재 구성으로 기존 장치를 계속 사용합니다. Android Enterprise 관리를 위해 새 장치를 설정합니다.
- 업그레이드 또는 교체가 필요한 경우에만 기존 장치를 마이그레이션합니다.
- 기존 장치를 일반적인 수명 주기 말에 Android Enterprise 관리로 마이그레이션합니다. 또는 분실 또는 파손으로 인해 교체가 필요한 경우 해당 장치를 마이그레이션합니다.

안드로이드 엔터프라이즈

Android Enterprise는 Android 장치를 위한 엔터프라이즈 관리 솔루션으로 Google에서 제공하는 도구 및 서비스 세트입니다. Android Enterprise를 사용하면 다음을 수행할 수 있습니다.

- XenMobile®을 사용하여 회사 소유 Android 장치와 개인 소유 장치(BYOD) Android 장치를 관리할 수 있습니다.
- 전체 장치 또는 장치 내의 별도 프로필을 관리할 수 있습니다. 별도 프로필은 비즈니스 계정, 앱 및 데이터를 개인 계정, 앱 및 데이터와 분리합니다.
- 재고 관리와 같이 단일 용도로 사용되는 장치도 관리할 수 있습니다. Google의 Android Enterprise 기능 개요는 Android Enterprise Management를 참조하십시오.

리소스:

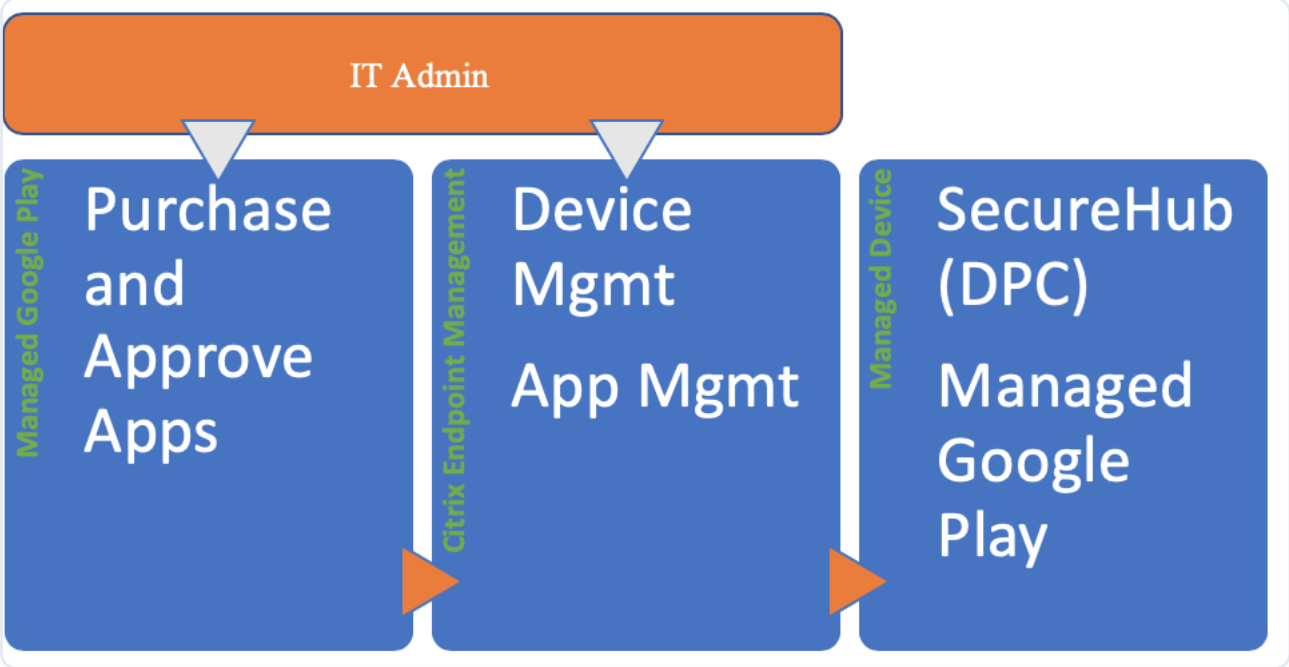
- Android Enterprise와 관련된 용어 및 정의 목록은 Google Android Enterprise 개발자 가이드의 Android Enterprise 용어를 참조하십시오. Google은 이러한 용어를 자주 업데이트합니다.
- XenMobile에서 지원되는 Android 운영 체제는 지원되는 장치 운영 체제를 참조하십시오.
- Android Enterprise용 네트워크 환경을 설정할 때 고려해야 할 아웃바운드 연결에 대한 자세한 내용은 Google 지원 문서인 Android Enterprise 네트워크 요구 사항을 참조하십시오.

XenMobile을 관리형 Google Play와 통합하여 Android Enterprise를 사용하면 엔터프라이즈를 생성하게 됩니다. Google은 엔터프라이즈를 조직과 엔터프라이즈 모바일 관리(EMM) 솔루션 간의 바인딩으로 정의합니다. 조직이 솔루션을 통해 관리하는 모든 사용자 및 장치는 해당 엔터프라이즈에 속합니다.

Android Enterprise용 엔터프라이즈는 EMM 솔루션, 장치 정책 컨트롤러(DPC) 앱, Google 엔터프라이즈 앱 플랫폼의 세 가지 구성 요소를 가집니다. XenMobile을 Android Enterprise와 통합하면 전체 솔루션은 다음 구성 요소를 갖게 됩니다.

- **XenMobile:** Citrix EMM입니다. XenMobile은 안전한 디지털 작업 공간을 위한 통합 XenMobile 솔루션입니다. XenMobile은 IT 관리자가 조직의 장치 및 앱을 관리할 수 있는 수단을 제공합니다.
- **Citrix Secure Hub™:** Citrix DPC 앱입니다. Secure Hub는 XenMobile의 시작점입니다. Secure Hub는 장치에 정책을 적용합니다.
- **관리형 Google Play:** XenMobile과 통합되는 Google 엔터프라이즈 앱 플랫폼입니다. Google Play EMM API는 앱 정책을 설정하고 앱을 배포합니다.

이 그림은 관리자가 이러한 구성 요소와 상호 작용하는 방식과 구성 요소가 서로 상호 작용하는 방식을 보여줍니다.



XenMobile에서 관리형 Google Play 사용

> **참고:**
>
> 관리형 Google Play 또는 Google Workspace를 사용하여 Citrix를 EMM 공급자로 등록할 수 있습니다. 이 문서에서는 관리형 Google Play와 함께 Android Enterprise를 사용하는 방법에 대해 설명합니다. 조직에서 Google Workspace를 사용하여 앱에 대한 액세스를 제공하는 경우 Android Enterprise와 함께 사용할 수 있습니다. Google Workspace(이전 G-Suite) 고객을 위한 레거시 Android Enterprise를 참조하십시오.

관리형 Google Play를 사용하는 경우 장치 및 최종 사용자를 위해 관리형 Google Play 계정을 프로비저닝합니다. 관리형 Google Play 계정은 관리형 Google Play에 대한 액세스를 제공하여 사용자가 사용 가능한 앱을 설치하고 사용할 수 있도록 합니다. 조직에서 타사 ID 서비스를 사용하는 경우 관리형 Google Play 계정을 기존 ID 계정과 연결할 수 있습니다.

이러한 유형의 엔터프라이즈는 도메인에 연결되어 있지 않으므로 단일 조직에 대해 둘 이상의 엔터프라이즈를 만들 수 있습니다. 예를 들어, 조직 내의 각 부서 또는 지역은 별도의 장치 및 앱 세트를 관리하기 위해 다른 엔터프라이즈로 등록할 수 있습니다.

XenMobile 관리자의 경우 관리형 Google Play는 Google Play의 사용자 경험 및 앱 스토어 기능을 엔터프라이즈용으로 설계된 관리 기능 세트와 결합합니다. 관리형 Google Play를 사용하여 장치의 Android Enterprise 작업 공간에 배포할 앱을 추가, 구매 및 승인합니다. Google Play를 사용하여 공개 앱, 비공개 앱 및 타사 앱을 배포할 수 있습니다.

관리형 장치 사용자의 경우 관리형 Google Play는 엔터프라이즈 앱 스토어입니다. 사용자는 앱을 찾아보고, 앱 세부 정보를 보고, 설치할 수 있습니다. Google Play의 공개 버전과 달리 사용자는 관리형 Google Play에서 사용자가 사용할 수 있도록 설정한 앱만 설치할 수 있습니다.

장치 배포 시나리오 및 작동 모드

장치 배포 시나리오는 배포하는 장치의 소유자와 관리 방법을 나타냅니다. 장치 프로필은 DPC가 장치에 대한 정책을 관리하고 적용하는 방법을 나타냅s니다.

업무 프로필은 업무 계정, 앱 및 데이터를 개인 계정, 앱 및 데이터와 분리합니다. 업무 프로필에 대한 자세한 내용은 Google Android Enterprise 도움말 항목인 업무 프로필이란?을 참조하십시오.

중요:

Android Enterprise 장치가 Android 11로 업데이트되면 Google은 "업무 프로필이 있는 완전 관리형"으로 관리되는 장치를 새로운 보안 강화 업무 프로필 환경으로 마이그레이션합니다. 자세한 내용은 Android Enterprise의 업무 프로필이 있는 완전 관리형에 대한 향후 변경 사항을 참조하십시오.

장치 관리	사용 사례	업무 프로필	개인 프로필	참고
회사 소유 기기 (완전 관리)	업무용으로만 사용하도록 지정된 회사 소유 기기	아니요	예. DPC는 기기 전체 연결 구성, 전역 설정 구성, 공장 초기화와 같은 기기 전체	새 기기 또는 공장 초기화된 기기에만 해당됩니다.

장치 관리	사용 사례	업무 프로필	개인 프로필	참고
			작업을 수행할 수 있습니다.	
업무 프로필로 완전 관리	업무 및 개인용으로 사용하도록 지정된 회사 소유 기기	예	예. 이러한 기기에서는 두 개의 DPC 복사본이 실행됩니다. 하나는 기기 소유자 모드에서 기기를 관리하고, 다른 하나는 프로필 소유자 모드에서 업무 프로필을 관리합니다. 기기와 업무 프로필에 별도의 정책을 적용할 수 있습니다.	이전에는 COPE(기업 소유 개인 사용 가능) 기기로 알려졌습니다.
전용 기기*	디지털 사이니지 또는 티켓 인쇄와 같은 단일 사용 사례를 위해 구성된 회사 소유 기기	아니요	예. 필요한 앱만 제공하고 사용자가 다른 앱을 추가하지 못하도록 합니다.	이전에는 기업 소유 단일 용도(COSU) 장치로 알려졌습니다.
BYOD 업무 프로필**	업무 프로필 모드(프로필 소유자 모드라고도 함)에 등록된 개인 장치	예	예. DPC는 전체 장치가 아닌 업무 프로필만 관리합니다.	이러한 장치는 새 장치이거나 공장 초기화된 장치일 필요가 없습니다.

* 사용자는 전용 장치를 공유할 수 있습니다. 사용자가 전용 장치에서 앱에 로그인하면 작업 상태는 장치가 아닌 앱에 있습니다.

** XenMobile은 BYOD 업무 프로필 모드에서 Zebra 장치를 지원하지 않습니다. XenMobile은 완전 관리형 장치 및 장치 레거시 모드(장치 관리자 모드라고도 함)에서 Zebra 장치를 지원합니다.

레거시 모드에서 장치 소유자 또는 프로필 소유자 모드로 마이그레이션하는 방법에 대한 자세한 내용은 장치 관리에서 Android Enterprise로 마이그레이션을 참조하십시오.

인증 방법

등록 프로필은 Android 장치가 MAM, MDM 또는 MDM+MAM에 등록되는지 여부를 결정하며, 사용자가 MDM에서 제외할 수 있는 옵션이 있습니다.

보안 수준 및 필수 등록 단계를 지정하는 방법에 대한 자세한 내용은 등록 보안 모드 구성을 참조하십시오.

XenMobile은 MDM+MAM에 등록된 Android 장치에 대해 다음 인증 방법을 지원합니다. 자세한 내용은 인증서 및 인증 아래의 문서를 참조하십시오.

- 도메인
- 도메인 및 보안 토큰
- 클라이언트 인증서
- 클라이언트 인증서 및 도메인
- ID 공급자:
  - 애저 액티브 디렉터리
  - Citrix ID 공급자

거의 사용되지 않는 다른 인증 방법은 클라이언트 인증서 및 보안 토큰입니다. 자세한 내용은 `<https://support.citrix.com/article/CTX215200>`을(를) 참조하십시오.

요구 사항

Android Enterprise를 사용하기 전에 다음이 필요합니다.

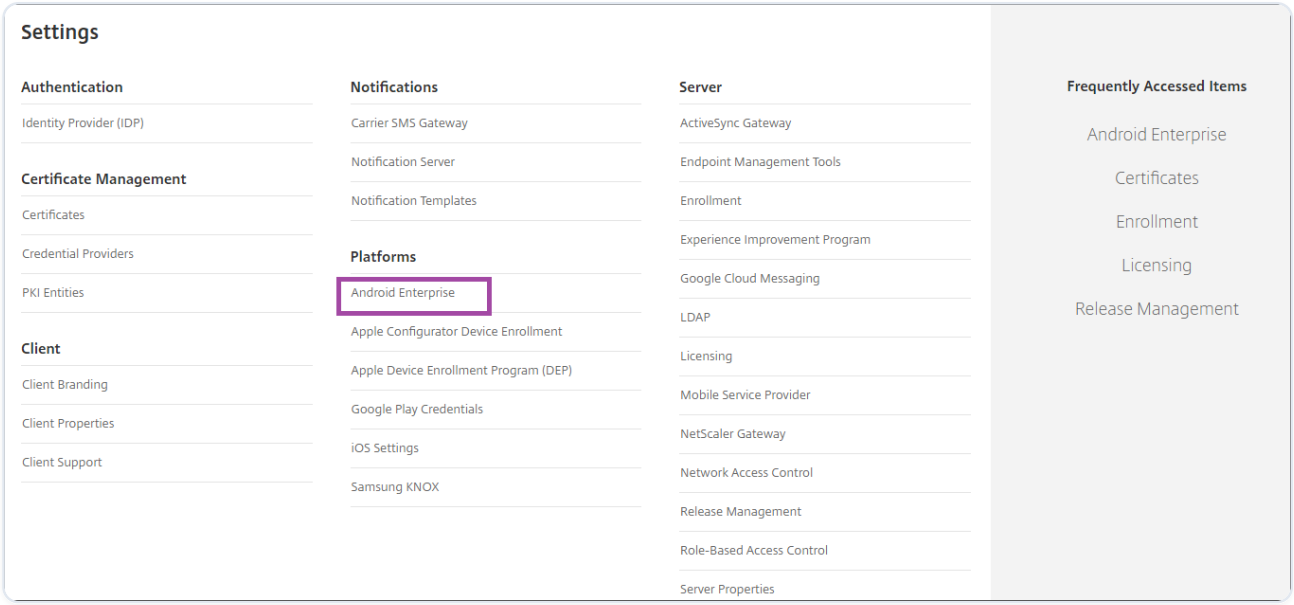
- 계정 및 자격 증명:
  - 관리형 Google Play로 Android Enterprise를 설정하려면 회사 Google 계정
  - 최신 MDX 파일을 다운로드하려면 Citrix 고객 계정
  - 개인 앱을 배포하려면(선택 사항) Google 개발자 계정
- XenMobile용으로 구성된 Firebase Cloud Messaging(FCM). 지침은 Firebase Cloud Messaging을(를) 참조하십시오.
- Samsung Knox Mobile Enrollment(선택 사항)의 경우 Knox 프리미엄 라이선스.

XenMobile을 Google Play에 연결

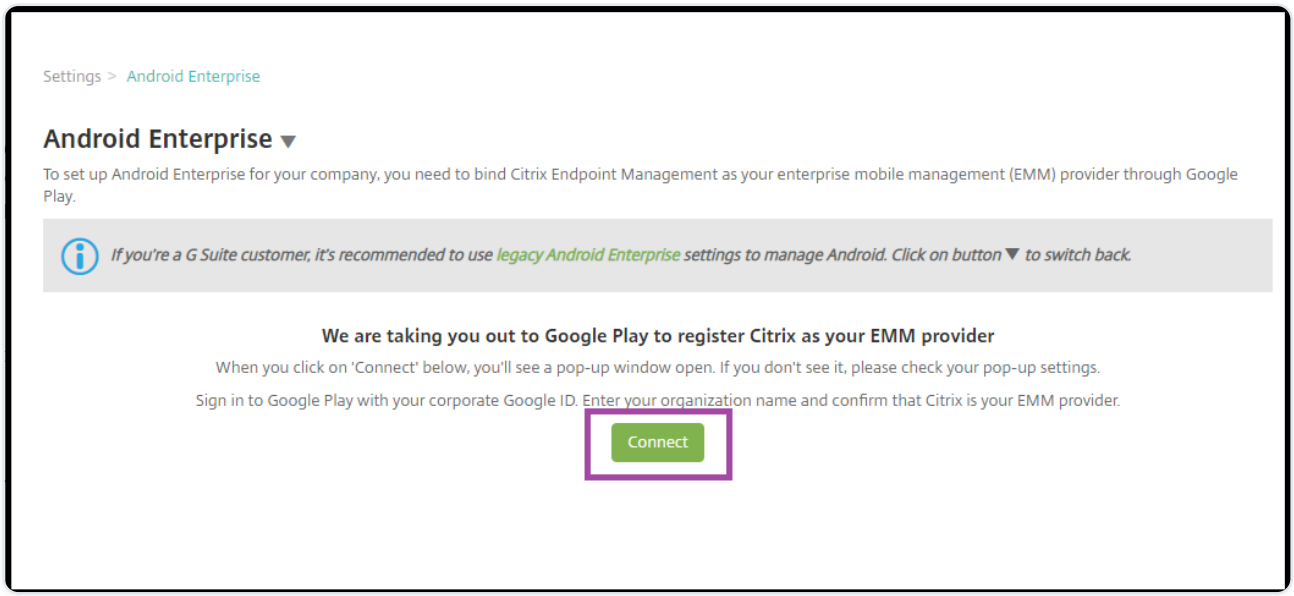
조직에 Android Enterprise를 설정하려면 관리형 Google Play를 통해 Citrix를 EMM 공급자로 등록하십시오. 이 설정은 관리형 Google Play를 XenMobile에 연결하고 XenMobile에 Android Enterprise용 엔터프라이즈를 생성합니다.

Google Play에 로그인하려면 회사 Google 계정이 필요합니다.

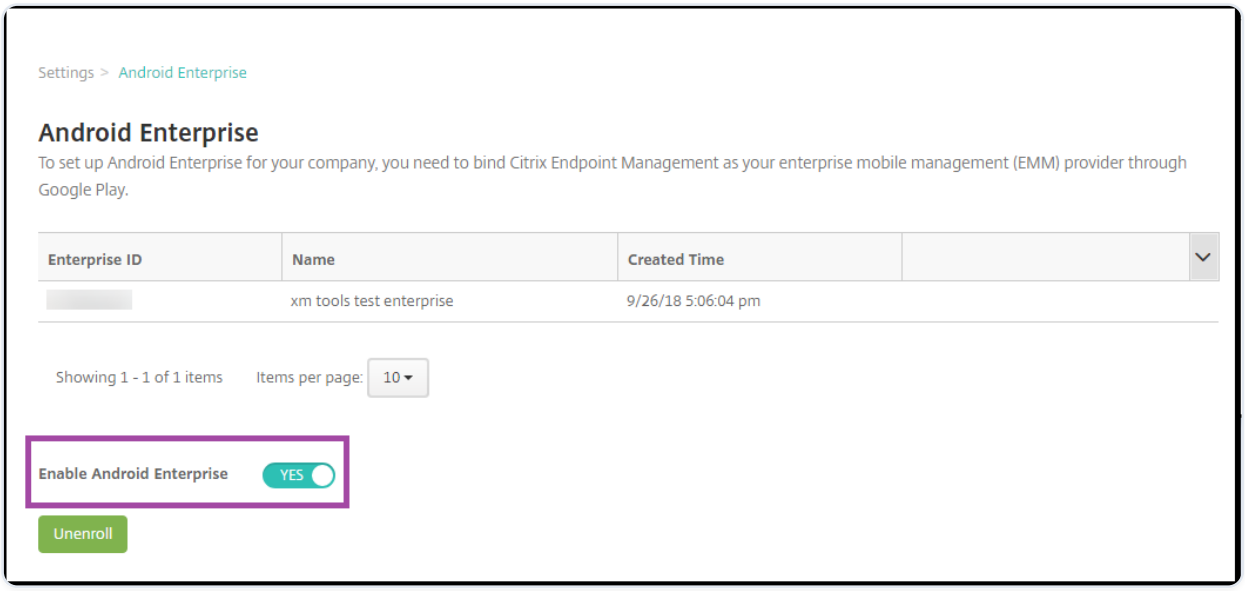
1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **설정 > Android Enterprise**로 이동합니다.



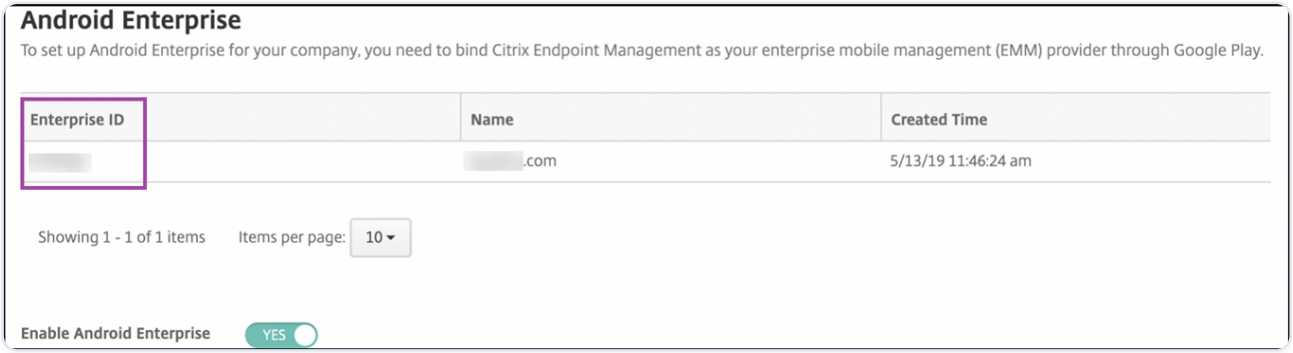
1. **연결**을 클릭합니다. Google Play가 열립니다.



1. 회사 Google 계정 자격 증명으로 Google Play에 로그인합니다. 조직 이름을 입력하고 Citrix가 EMM 공급자인지 확인합니다.
2. Android Enterprise용 엔터프라이즈 ID가 추가됩니다. Android Enterprise를 사용하도록 설정하려면 **Android Enterprise 사용**을 **예**로 밉니다.



엔터프라이즈 ID가 XenMobile 콘솔에 나타납니다.



환경이 Google에 연결되었으며 장치를 관리할 준비가 되었습니다. 이제 사용자에게 앱을 제공할 수 있습니다.

XenMobile은 사용자에게 Citrix 모바일 생산성 앱, MDX 앱, 공개 앱 스토어 앱, 웹 및 SaaS 앱, 엔터프라이즈 앱, 웹 링크를 제공하는 데 사용될 수 있습니다. 이러한 앱 유형 및 사용자에게 제공하는 방법에 대한 자세한 내용은 앱 추가를 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 액세스하는 데 사용하는 보안 챌린지 규칙을 구성합니다. 보안 챌린지 정책 구성을 참조하십시오.

게시하는 앱은 Android Enterprise 기업에 등록된 장치에서 사용할 수 있습니다.

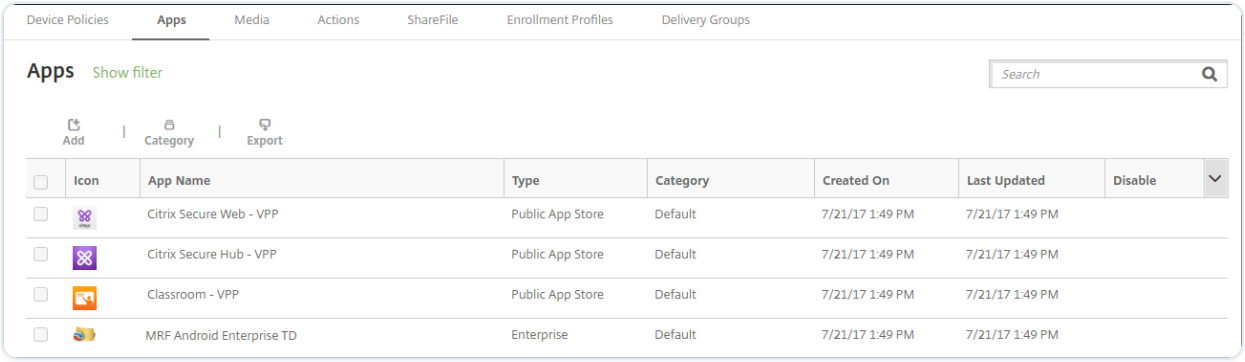
참고:

Android Enterprise 공개 앱 스토어 앱을 Android 사용자에게 배포하면 해당 사용자는 Android Enterprise에 자동으로 등록됩니다.

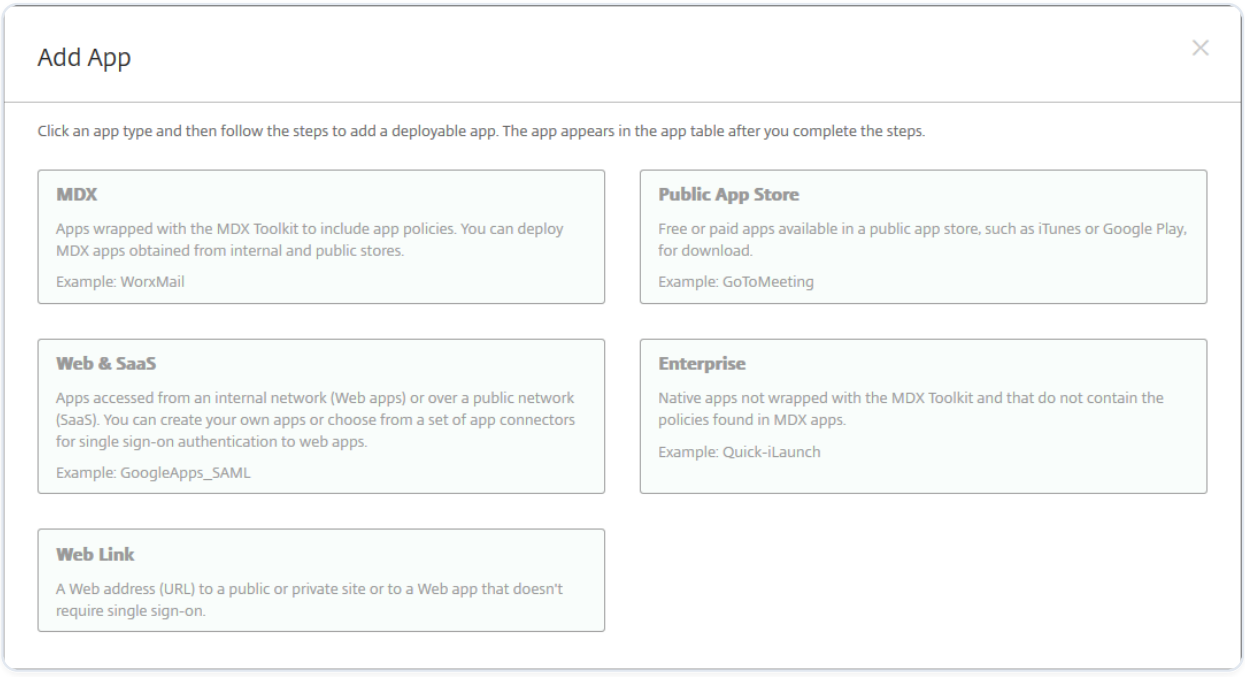
앱을 MDX 앱으로 구성

Android Enterprise용 MDX 앱으로 Citrix 생산성 앱을 구성하려면 다음을 수행합니다.

1. XenMobile 콘솔에서 **구성 > 앱**을 클릭합니다. **앱** 페이지가 나타납니다.



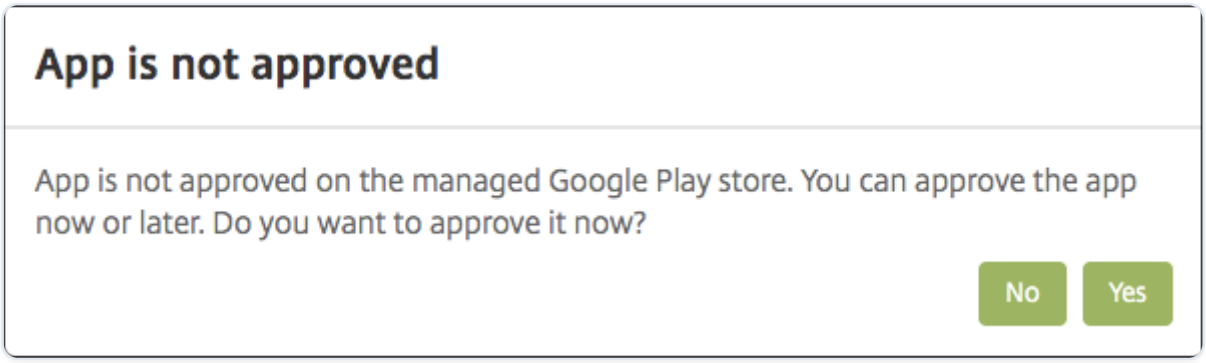
2. **추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.



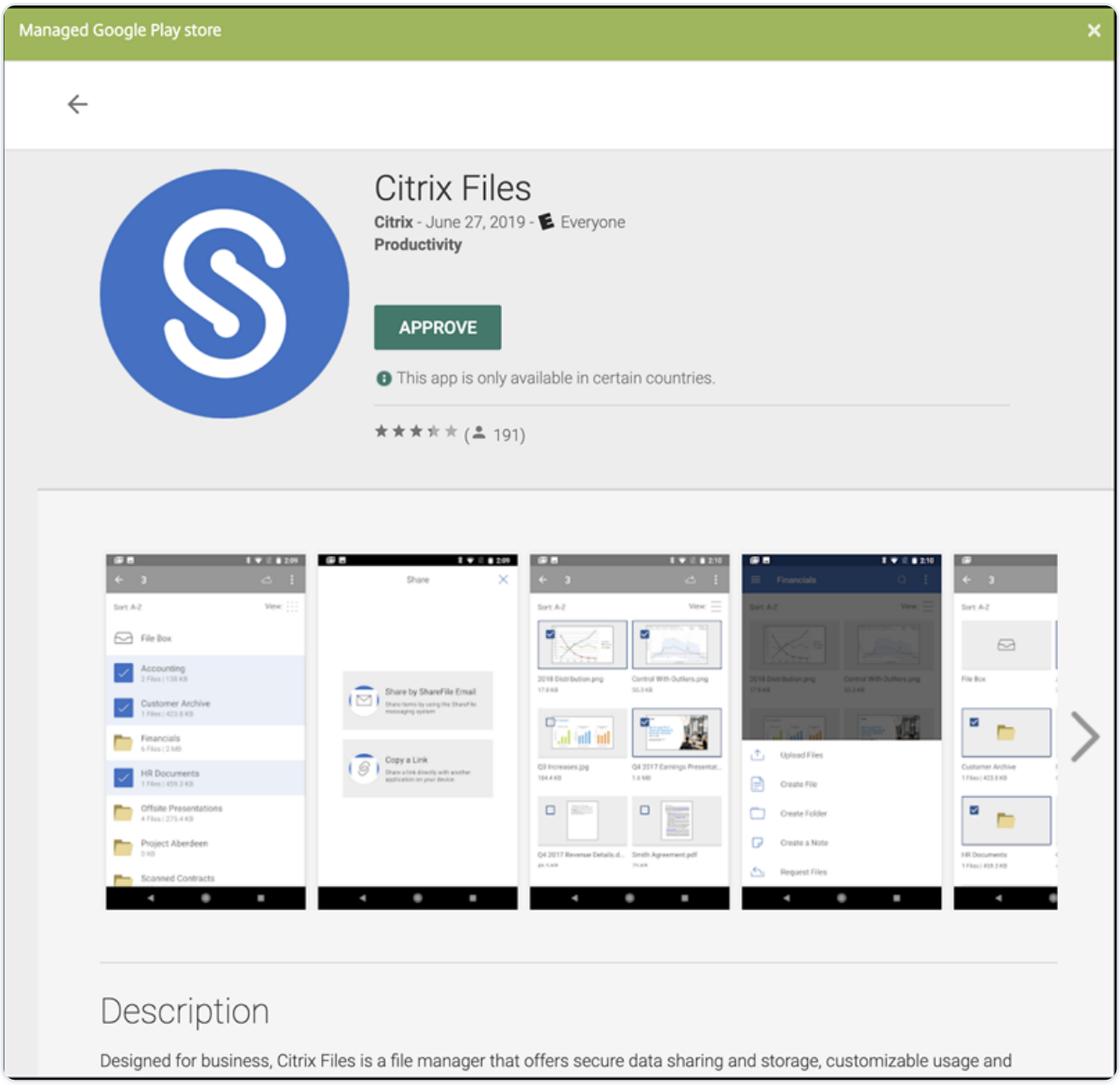
3. **MDX**를 클릭합니다. **앱 정보** 페이지가 나타납니다.
4. 페이지 왼쪽에서 플랫폼으로 **Android Enterprise**를 선택합니다.
5. **앱 정보** 페이지에서 다음 정보를 입력합니다.

- **이름:** 앱에 대한 설명이 포함된 이름을 입력합니다. 이 이름은 **앱** 테이블의 **앱 이름** 아래에 나타납니다.
- **설명:** 앱에 대한 선택적 설명을 입력합니다.
- **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

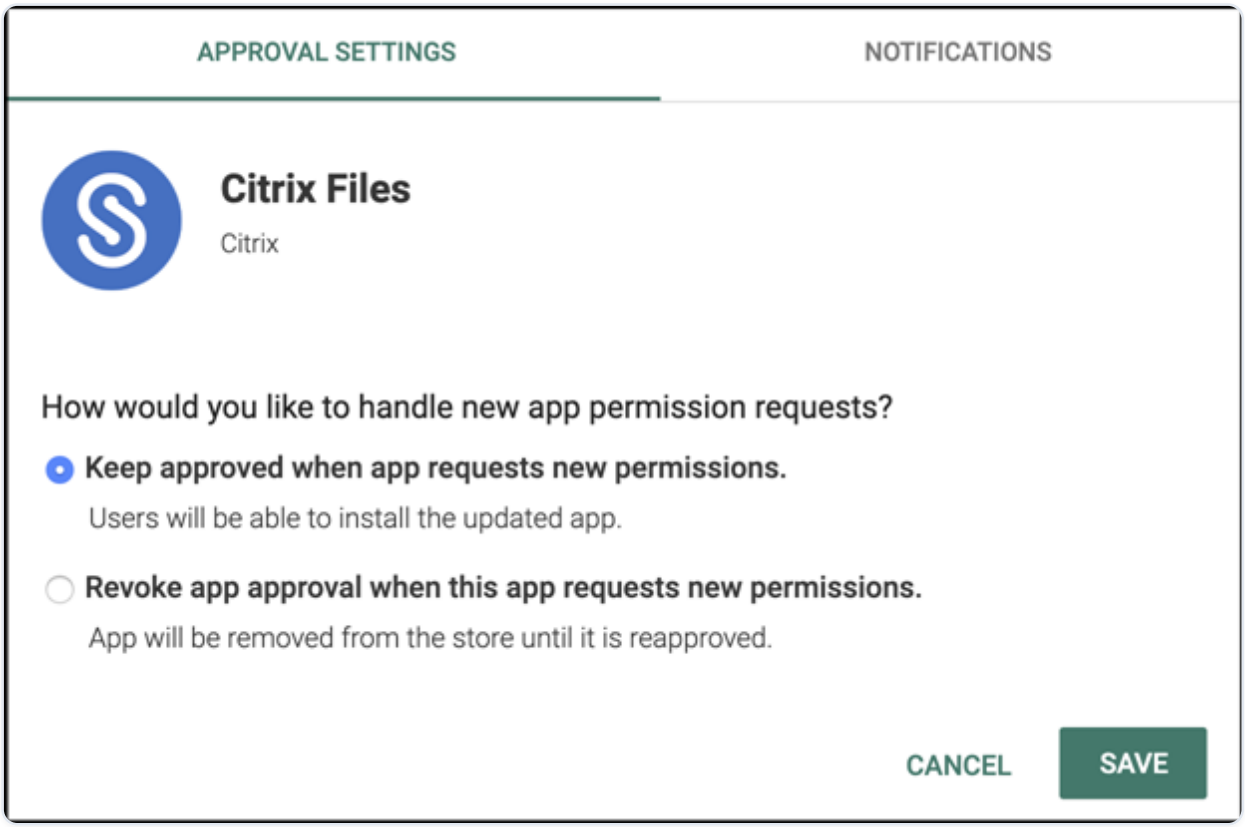
6. **다음**을 클릭합니다. **Android Enterprise MDX 앱** 페이지가 나타납s니다.
7. **업로드**를 클릭하고 앱의 .mdx 파일 위치로 이동합니다. 파일을 선택하고 **열기**를 클릭합니다.
8. 첨부된 애플리케이션에 관리형 Google Play 스토어의 승인이 필요한 경우 UI에서 알려줍니다. XenMobile 콘솔을 벗어나지 않고 애플리케이션을 승인하려면 **예**를 클릭합니다.



9. 관리형 Google Play 스토어 페이지가 열리면 **승인**을 클릭합니다.



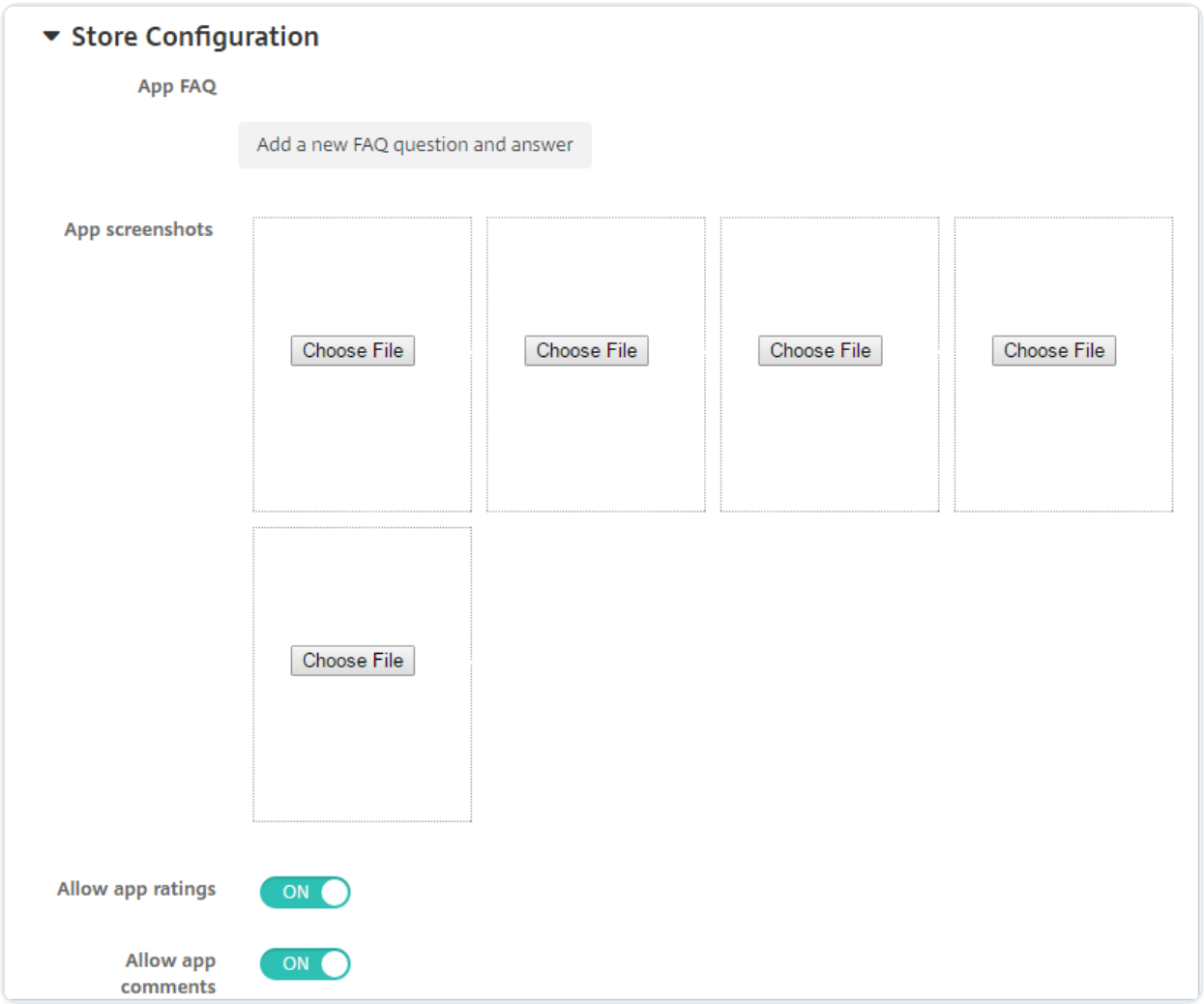
10. 다시 **승인**을 클릭합니다.
11. **앱이 새 권한을 요청할 때 승인 유지**를 선택합니다. **저장**을 클릭합니다.



12. 앱이 승인되고 저장되면 페이지에 더 많은 설정이 나타납니다. 다음 설정을 구성합니다.

    - **파일 이름:** 앱과 연결된 파일 이름을 입력합니다.
    - **앱 설명:** 앱에 대한 설명을 입력합니다.
    - **제품 트랙:** 사용자 장치로 푸시할 제품 트랙을 지정합니다. 테스트용으로 설계된 트랙이 있는 경우 해당 트랙을 선택하여 사용자에게 할당할 수 있습니다. 기본값은 Production입니다.
    - **앱 버전:** 선택적으로 앱 버전 번호를 입력합니다.
    - **패키지 ID:** Google Play 스토어에 있는 앱의 URL입니다.
    - **최소 OS 버전:** 선택적으로 장치에서 앱을 실행할 수 있는 가장 오래된 운영 체제 버전을 입력합니다.
    - **최대 OS 버전:** 선택적으로 장치에서 앱을 실행해야 하는 최신 운영 체제를 입력합니다.
    - **제외된 장치:** 선택적으로 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

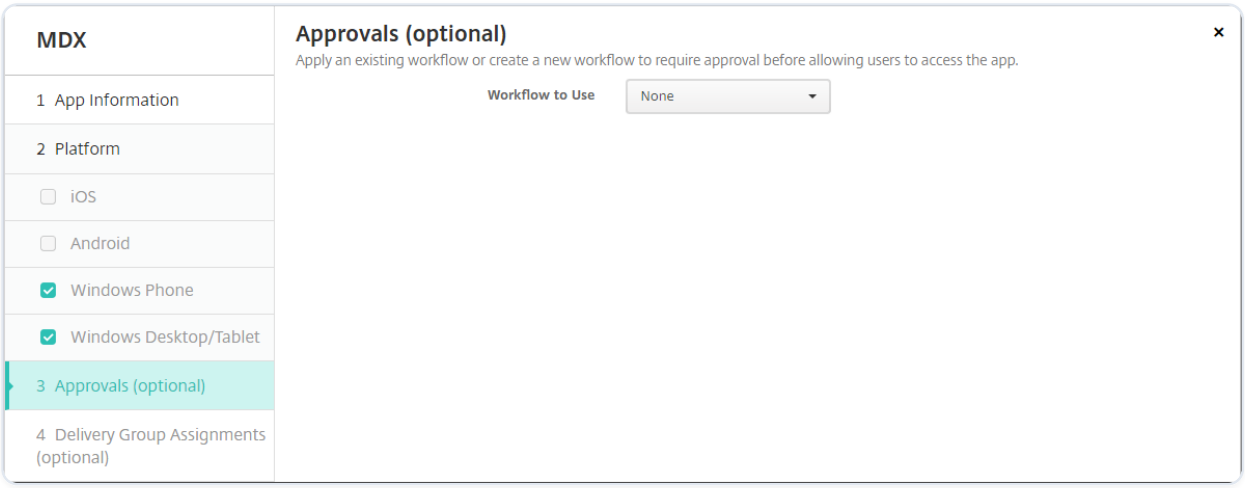
13. **MDX 정책**을 구성합니다. MDX 앱에 대한 앱 정책에 대한 자세한 내용은 MDX 정책 개요 및 MAM SDK 개요를 참조하십시오.
14. 배포 규칙을 구성합니다. 자세한 내용은 리소스 배포를 참조하십시오.
15. **스토어 구성**을 확장합니다. 이 설정은 관리형 Google Play에만 표시되는 Android Enterprise 앱에는 적용되지 않습니다.



선택적으로 앱에 대한 FAQ 또는 앱 스토어에 표시되는 화면 캡처를 추가할 수 있습니다. 또한 사용자가 앱을 평가하거나 댓글을 달 수 있는지 여부를 설정할 수도 있습니다.

- 다음 설정을 구성합니다.
  - **앱 FAQ:** 앱에 대한 FAQ 질문과 답변을 추가합니다.
  - **앱 스크린샷:** 앱 스토어에서 앱을 분류하는 데 도움이 되는 화면 캡처를 추가합니다. 업로드하는 그래픽은 PNG여야 합니다. GIF 또는 JPEG 이미지는 업로드할 수 없습니다.
  - **앱 평가 허용:** 사용자가 앱을 평가하도록 허용할지 여부를 선택합니다. 기본값은 **켜짐**입니다. **앱 댓글 허용:** 사용자가 선택한 앱에 대해 댓글을 달도록 허용할지 여부를 선택합니다. 기본값은 **켜짐**입니다.

16. **다음**을 클릭합니다. **승인** 페이지가 나타납니다.



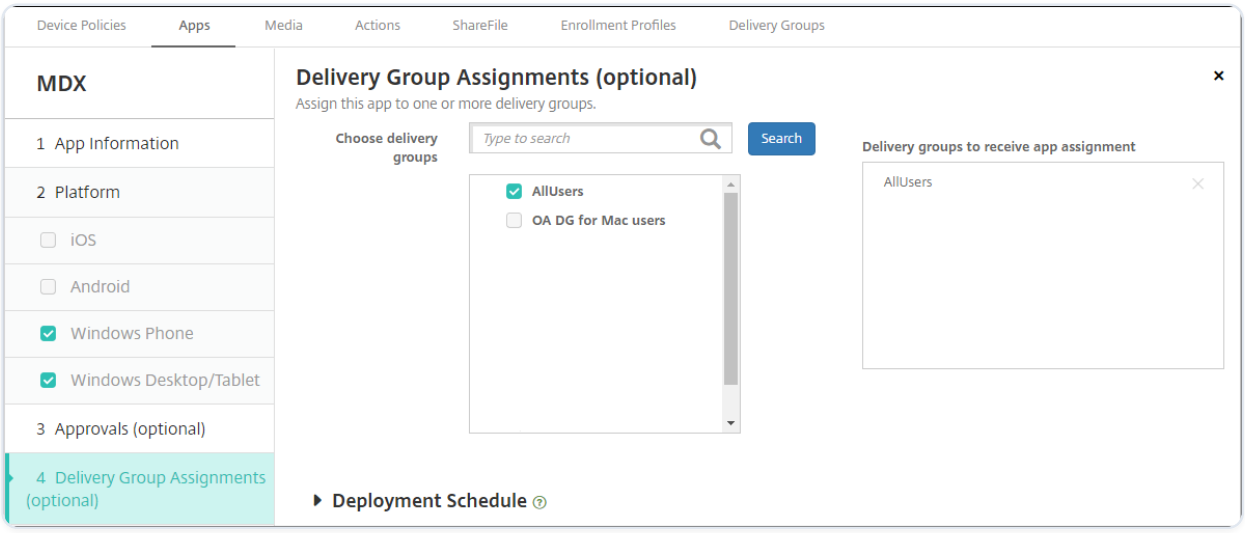
사용자 계정을 생성할 때 승인이 필요한 경우 워크플로를 사용합니다. 승인 워크플로를 설정하지 않으려면 15단계로 건너뛸 수 있습니다.

워크플로를 할당하거나 생성하려면 다음 설정을 구성합니다.

- **사용할 워크플로:** 목록에서 기존 워크플로를 클릭하거나 **새 워크플로 생성**을 클릭합니다. 기본값은 **없음**입니다.
- **새 워크플로 생성**을 선택하는 경우 다음 설정을 구성합니다. 자세한 내용은 워크플로 적용을 참조하십시오.
- **이름:** 워크플로의 고유한 이름을 입력합니다.
- **설명:** 선택적으로 워크플로에 대한 설명을 입력합니다.
- **이메일 승인 템플릿:** 목록에서 할당할 이메일 승인 템플릿을 선택합니다. 이 필드 오른쪽에 있는 눈 아이콘을 클릭하면 템플릿을 미리 볼 수 있는 대화 상자가 나타납니다.
- **관리자 승인 수준:** 목록에서 이 워크플로에 필요한 관리자 승인 수준 수를 선택합니다. 기본값은 1단계입니다. 가능한 옵션은 다음과 같습니다.
  - 필요 없음
  - 1단계
  - 2단계
  - 3단계
- **Active Directory 도메인 선택:** 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
- **추가 필수 승인자 찾기:** 검색 필드에 추가 필수 담당자의 이름을 입력한 다음 **검색**을 클릭합니다. 이름은 Active Directory에서 가져옵니다.
- 이름이 필드에 나타나면 이름 옆의 확인란을 선택합니다. 이름과 이메일 주소는 **선택된 추가 필수 승인자** 목록에 나타납니다.

- **선택된 추가 필수 승인자** 목록에서 담당자를 제거하려면 다음 중 하나를 수행합니다.
  - 선택한 도메인의 모든 담당자 목록을 보려면 **검색**을 클릭합니다.
  - 검색 상자에 전체 또는 부분 이름을 입력한 다음 **검색**을 클릭하여 검색 결과를 제한합니다.
  - **선택된 추가 필수 승인자** 목록의 담당자는 검색 결과 목록에서 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하여 제거하려는 각 이름 옆의 확인란을 지웁니다.

17. **다음**을 클릭합니다. **전달 그룹 할당** 페이지가 나타납니다.



18. **전달 그룹 선택** 옆에서 전달 그룹을 찾기 위해 입력하거나 목록에서 하나 이상의 그룹을 선택합니다. 선택한 그룹은 **앱 할당을 받을 전달 그룹** 목록에 나타납니다.
19. **배포 일정**을 확장한 다음 다음 설정을 구성합니다.

- **배포** 옆에서 배포를 예약하려면 **켜기**를 클릭하거나 배포를 방지하려면 **끄기**를 클릭합니다. 기본 옵션은 **켜기**로 설정되어 있습니다.
- 배포 일정 옆에서 **지금** 또는 **나중에**를 클릭합니다. 기본 옵션은 **지금**으로 설정되어 있습니다.
- **나중에**를 클릭하는 경우, 달력 아이콘을 클릭한 다음 배포 날짜와 시간을 선택합니다.
- **배포 조건** 옆에서 **모든 연결 시**를 클릭하거나 **이전 배포가 실패한 경우에만**을 클릭합니다. 기본 옵션은 **모든 연결 시**로 설정되어 있습니다.
- **항상 켜짐 연결에 배포** 옆에서 **OFF**가 선택되어 있는지 확인합니다. 기본 옵션은 **OFF**로 설정되어 있습니다. XenMobile 버전 10.18.19 이상을 사용하기 시작한 경우 Android Enterprise에서는 항상 켜짐 연결을 사용할 수 없습니다. 버전 10.18.19 이전에 XenMobile을 사용하기 시작한 고객에게는 연결을 권장하지 않습니다.

  이 옵션은 **설정 > 서버 속성**에서 예약 백그라운드 배포 키를 구성한 경우에 적용됩니다.

  구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. **항상 켜짐 연결에 배포**를 제외하고 변경하는 모든 내용은 모든 플랫폼에 적용됩니다.

20. **저장**을 클릭합니다.

각 모바일 생산성 앱에 대해 MDX 앱을 구성하려면 단계를 반복합니다.

보안 챌린지 정책 구성

XenMobile 암호 장치 정책은 사용자가 장치 또는 장치의 Android Enterprise 작업 프로필에 액세스하기 위한 보안 챌린지 규칙 집합을 구성합니다. 보안 챌린지는 암호 또는 생체 인식일 수 있습니다. 암호 정책에 대한 자세한 내용은 암호 장치 정책을 참조하십시오.

- Android Enterprise 배포에 BYOD 장치가 포함된 경우 작업 프로필에 대한 암호 정책을 구성합니다.
- 배포에 회사 소유의 완전 관리형 장치가 포함된 경우 장치 자체에 대한 암호 정책을 구성합니다.
- 배포에 두 가지 유형의 장치가 모두 포함된 경우 두 가지 유형의 암호 정책을 모두 구성합니다.

암호 정책을 구성하려면 다음을 수행합니다.

1. XenMobile 콘솔에서 **구성 > 장치 정책**으로 이동합니다.
2. **추가**를 클릭합니다.
3. **필터 표시**를 클릭하여 **정책 플랫폼** 창을 표시합니다. **정책 플랫폼** 창에서 **Android Enterprise**를 선택합니다.
4. 오른쪽 창에서 **암호**를 클릭합니다.

암호 보안 옵션(/en-us/xenmobile/server/media/password-security-policy.png)

1. **정책 이름**을 입력합니다. **다음**을 클릭합니다.

   암호 보안 이름(/en-us/xenmobile/server/media/password-security-name.png)
2. 암호 정책 설정을 구성합니다.
   - **장치 암호 필요**를 **켜기**로 설정하여 장치 자체의 보안 챌린지에 사용할 수 있는 설정을 확인합니다.
   - **작업 프로필 보안 챌린지**를 **켜기**로 설정하여 작업 프로필 보안 챌린지에 사용할 수 있는 설정을 확인합니다.
3. **다음**을 클릭합니다.
4. 하나 이상의 전달 그룹에 정책을 할당합니다.
5. **저장**을 클릭합니다.

등록 프로필 만들기

등록 프로필은 XenMobile 배포에 Android Enterprise가 활성화된 경우 Android 장치가 등록되는 방식을 제어합니다. Android Enterprise 장치를 등록하기 위한 등록 프로필을 만들 때 새 장치 및 공장 초기화 장치를 다음과 같이 등록하도록 등록 프로필을 구성할 수 있습니다.

- 완전히 관리되는 장치
- 전용 장치(COSU 장치)
- 업무 프로필이 있는 완전 관리형 장치(COPE 장치)

또한 이러한 각 Android Enterprise 등록 프로필을 구성하여 BYOD Android 장치를 업무 프로필 장치로 등록할 수 있습니다.

XenMobile 배포에 Android Enterprise가 활성화된 경우 새로 등록되거나 재등록된 모든 Android 장치는 Android Enterprise 장치로 등록됩니다. 기본적으로 전역 등록 프로필은 새 Android 장치 및 공장 초기화된 Android 장치를 완전 관리형 장치로 등록하고 BYOD Android 장치를 업무 프로필 장치로 등록합니다.

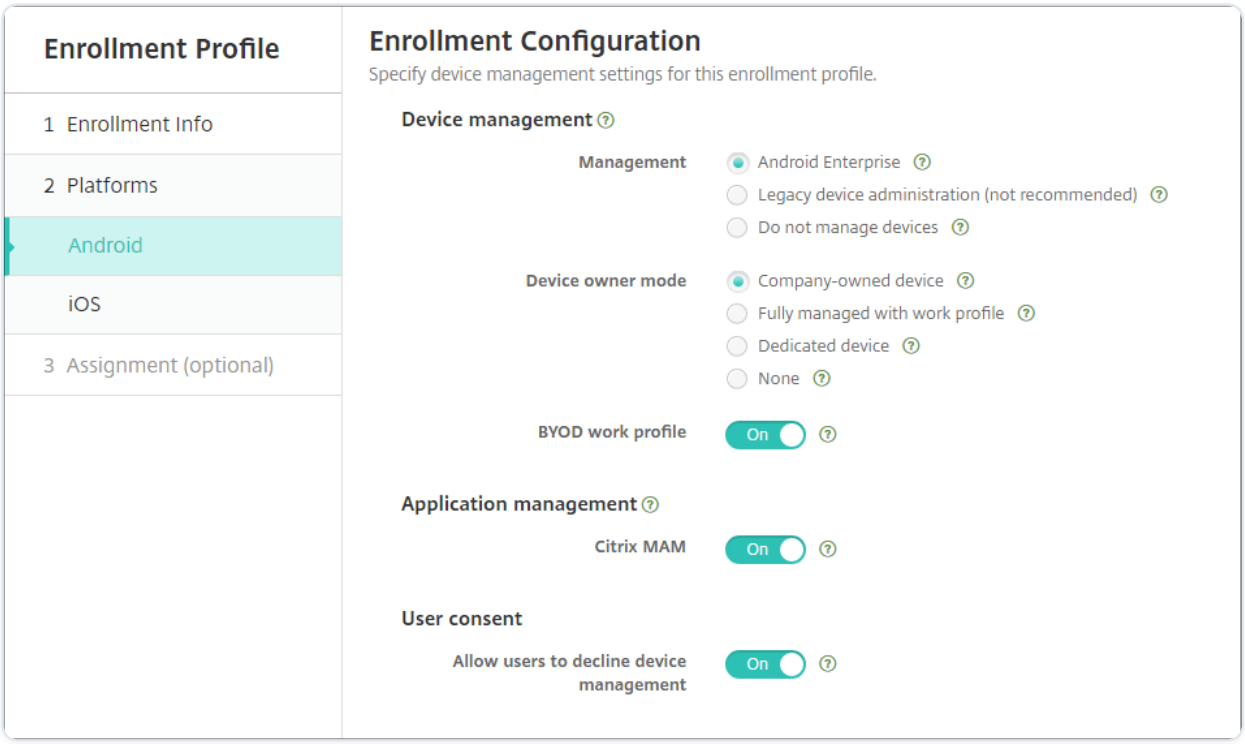
등록 프로필을 생성할 때 해당 프로필에 배달 그룹을 할당합니다. 사용자가 서로 다른 등록 프로필을 가진 여러 배달 그룹에 속해 있는 경우, 배달 그룹의 이름이 사용되는 등록 프로필을 결정합니다. XenMobile은 배달 그룹의 알파벳순 목록에서 마지막에 나타나는 배달 그룹을 선택합니다. 자세한 내용은 등록 프로필을 참조하십시오.

등록 프로필을 사용하여 MDM 전용, MDM+MAM, MAM 전용과 같은 여러 사용 사례를 결합할 수 있습니다. 서버 속성 `xms.server.mode`에 반영된 XenMobile Server 라이선스 유형에 따라 **구성 > 등록 프로필**에서 사용할 수 있는 설정이 결정됩니다.

완전 관리형 장치에 대한 등록 프로필 추가

전역 등록 프로필은 기본적으로 완전 관리형 장치를 등록하지만, 완전 관리형 장치를 등록하기 위해 더 많은 등록 프로필을 생성할 수 있습니다.

1. XenMobile 콘솔에서 **구성 > 등록 프로필**로 이동합니다.
2. 등록 프로필을 추가하려면 **추가**를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다.
3. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수를 설정합니다.
4. **플랫폼**에서 **Android**를 선택하거나 **다음**을 클릭합니다. 등록 구성 페이지가 나타납니다.
5. **관리**를 **Android Enterprise**로 설정합니다.
6. **장치 소유자 모드**를 **회사 소유 장치**로 설정합니다.



7. **BYOD 업무 프로필**을 사용하면 등록 프로필을 구성하여 BYOD 장치를 업무 프로필 장치로 등록할 수 있습니다. 새 장치 및 공장 초기화된 장치는 완전 관리형 장치로 등록됩니다.

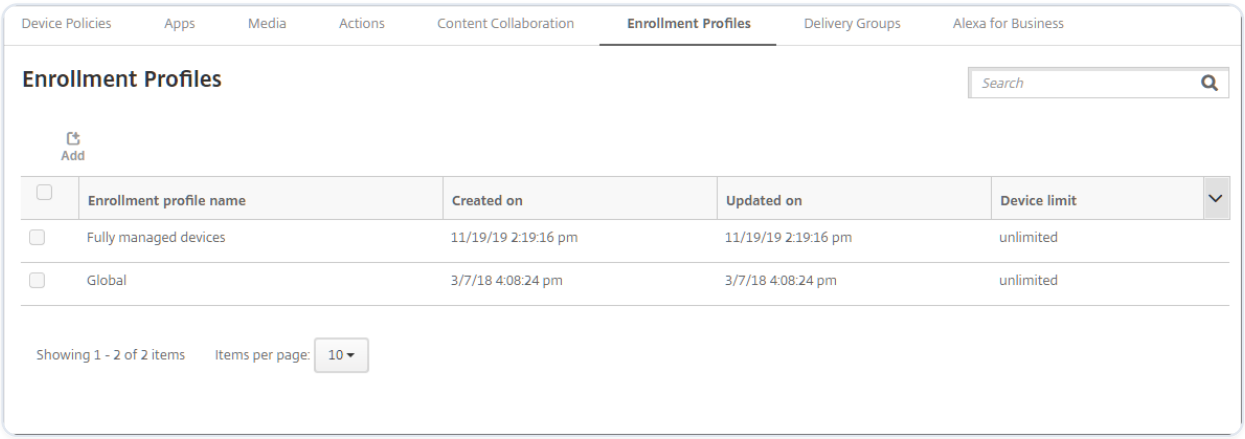
   - **BYOD 작업 프로필**을 **켜짐**으로 설정하여 BYOD 장치를 작업 프로필 장치로 등록할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
   - **BYOD 작업 프로필**을 **꺼짐**으로 설정하여 등록을 완전 관리형 장치로 제한합니다.

8. Citrix MAM에 장치를 등록할지 여부를 선택합니다.
9. **BYOD 작업 프로필**을 **켜짐**으로 설정한 경우 사용자 동의를 구성합니다. BYOD 작업 프로필 장치 사용자가 장치를 등록할 때 장치 관리를 거부할 수 있도록 허용하려면 **사용자가 장치 관리를 거부하도록 허용**을 **켜짐**으로 설정합니다.

   BYOD 작업 프로필이 **켜짐**으로 설정된 경우 **사용자가 장치 관리를 거부하도록 허용**의 기본값은 **켜짐**입니다. **BYOD 작업 프로필**이 **꺼짐**으로 설정된 경우 **사용자가 장치 관리를 거부하도록 허용**이 비활성화됩니다.

10. **할당(옵션)**을 선택합니다. 배달 그룹 할당 화면이 나타납니다.
11. 완전 관리형 장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 **저장**을 클릭합니다.

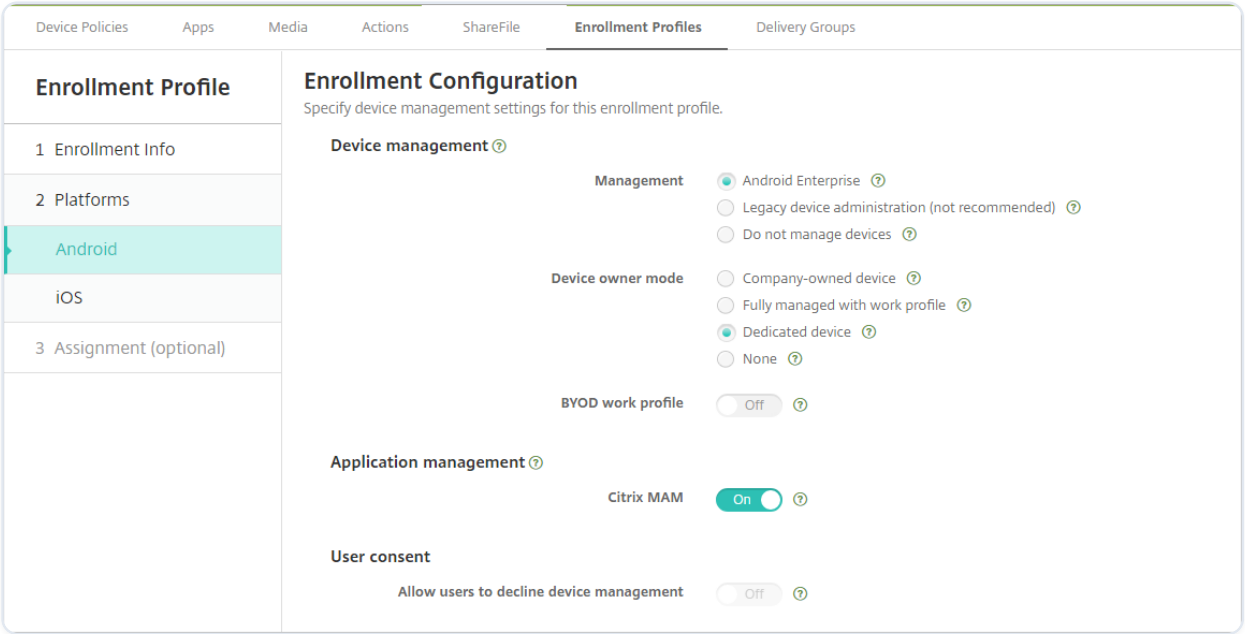
    추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.



전용 장치 등록 프로필 추가

XenMobile 배포에 전용 장치가 포함된 경우 단일 XenMobile 관리자 또는 소규모 관리자 그룹이 많은 전용 장치를 등록합니다. 이러한 관리자가 필요한 모든 장치를 등록할 수 있도록 하려면 사용자당 무제한 장치를 허용하는 등록 프로필을 생성합니다.

1. XenMobile 콘솔에서 **구성 > 등록 프로필**로 이동합니다.
2. 등록 프로필을 추가하려면 **추가**를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수가 무제한으로 설정되어 있는지 확인합니다.
3. **플랫폼** 아래에서 **Android**를 선택하거나 **다음**을 클릭합니다. 등록 구성 페이지가 나타납s니다.
4. **관리**를 **Android Enterprise**로 설정합니다.
5. **장치 소유자 모드**를 **전용 장치**로 설정합니다.



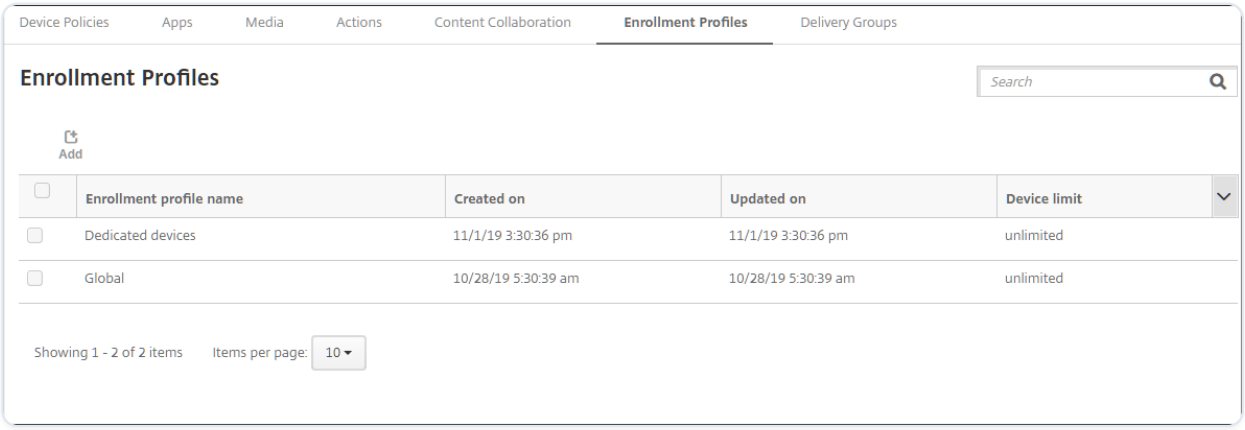
6. **BYOD 업무 프로필**을 사용하면 BYOD 장치를 업무 프로필 장치로 등록하도록 등록 프로필을 구성할 수 있습니다. 새 장치 및 공장 초기화된 장치는 전용 장치로 등록됩니다. BYOD 장치를 업무 프로필 장치로

등록하려면 **BYOD 업무 프로필**을 **켬**으로 설정합니다. 회사 소유 장치로 등록을 제한하려면 **BYOD 업무 프로필**을 **끔**으로 설정합니다. 기본값은 **켬**입니다.

7. Citrix MAM에 장치를 등록할지 여부를 선택합니다.
8. **BYOD 업무 프로필**을 **켬**으로 설정한 경우 사용자 동의를 구성합니다. BYOD 업무 프로필 장치 사용자가 장치를 등록할 때 장치 관리를 거부하도록 허용하려면 **사용자가 장치 관리를 거부하도록 허용**을 **켬**으로 설정합니다.

   BYOD 업무 프로필이 **켬**으로 설정된 경우 **사용자가 장치 관리를 거부하도록 허용**의 기본값은 **켬**입니다. **BYOD 업무 프로필**이 **끔**으로 설정된 경우 **사용자가 장치 관리를 거부하도록 허용**은 비활성화됩니다.
9. **할당(옵션)**을 선택합니다. 배달 그룹 할당 화면이 나타납니다.
10. 전용 장치를 등록하는 관리자가 있는 배달 그룹을 선택합니다. 그런 다음 **저장**을 클릭합니다.

    추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.



업무 프로필이 있는 완전 관리형 장치용 등록 프로필 추가

1. XenMobile 콘솔에서 **구성 > 등록 프로필**로 이동합니다.
2. 등록 프로필을 추가하려면 **추가**를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다.
3. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수를 설정합니다.
4. **플랫폼**에서 **Android**를 선택하거나 **다음**을 클릭합니다. 등록 구성 페이지가 나타납니다.
5. **관리**를 **Android Enterprise**로 설정합니다. **장치 소유자 모드**를 **업무 프로필로 완전 관리**로 설정합니다.

   등록 프로필 구성 화면(/en-us/xenmobile/server/media/android-enterprise-enrollment-profile-cope-multimode.png)
6. **BYOD 업무 프로필**을 사용하면 BYOD 장치를 업무 프로필 장치로 등록하도록 등록 프로필을 구성할 수 있습니다. 새로 등록되거나 공장 초기화된 장치는 업무 프로필이 있는 완전 관리형 장치로 등록됩니다.

BYOD 장치를 업무 프로필 장치로 등록하려면 **BYOD 업무 프로필**을 **켜기**로 설정합니다. 전용 장치로의 등록을 제한하려면 **BYOD 업무 프로필**을 **끄기**로 설정합니다. 기본값은 **끄기**입니다.

7. Citrix MAM에 장치를 등록할지 여부를 선택합니다.
8. **BYOD 업무 프로필**을 **켜기**로 설정한 경우 사용자 동의를 구성합니다. BYOD 업무 프로필 장치 사용자가 장치를 등록할 때 장치 관리를 거부하도록 허용하려면 **사용자가 장치 관리를 거부하도록 허용**을 **켜기**로 설정합니다.

   BYOD 업무 프로필이 **켜기**로 설정된 경우 **사용자가 장치 관리를 거부하도록 허용**의 기본값은 **켜기**입니다. **BYOD 업무 프로필**이 **끄기**로 설정된 경우 **사용자가 장치 관리를 거부하도록 허용**은 비활성화됩니다.
9. **할당(옵션)**을 선택합니다. 배달 그룹 할당 화면이 나타납니다.
10. 업무 프로필이 있는 완전 관리형 장치를 등록하는 관리자가 속한 배달 그룹을 선택합니다. 그런 다음 **저장**을 클릭합니다.

    추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.

    등록 프로필 페이지(/en-us/xenmobile/server/media/android-enterprise-enrollment-profile-cope-done.png)

레거시 장치용 등록 프로필 추가

Google은 장치 관리의 장치 관리자 모드를 더 이상 사용하지 않습니다. Google은 고객이 모든 Android 장치를 장치 소유자 모드 또는 프로필 소유자 모드로 관리하도록 권장합니다. (Google Android Enterprise 개발자 가이드에서 장치 관리자 사용 중단을 참조하십시오.)

이러한 변경 사항을 지원하기 위해:

- Citrix는 Android Enterprise를 Android 장치의 기본 등록 옵션으로 설정합니다.
- XenMobile 배포에 Android Enterprise가 활성화된 경우 새로 등록되거나 재등록된 모든 Android 장치는 Android Enterprise 장치로 등록됩니다.

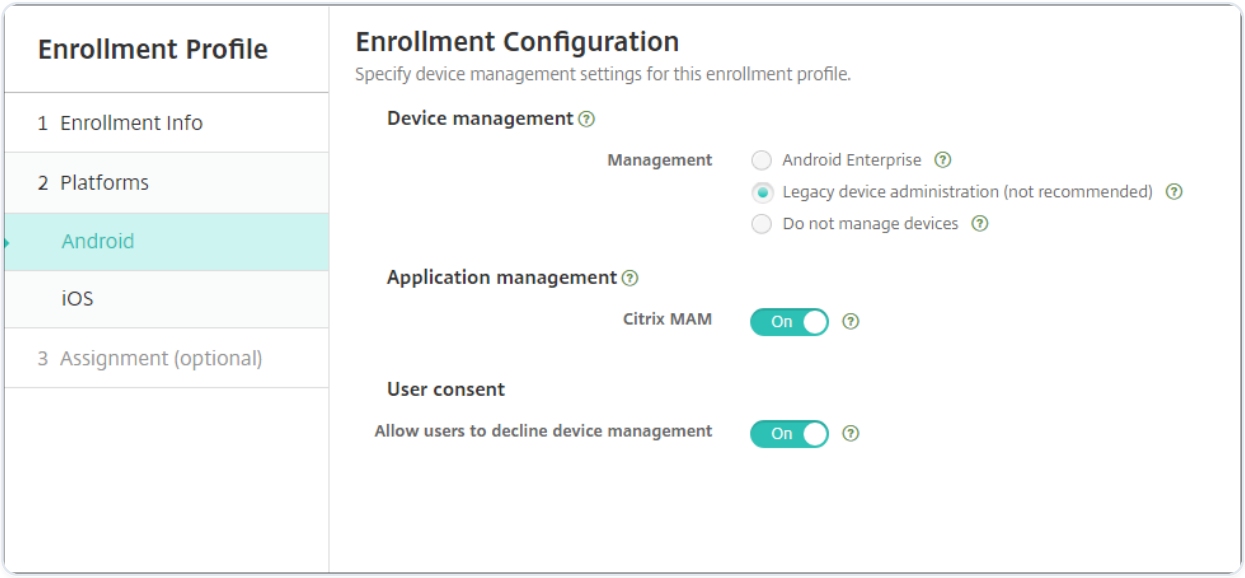
조직에서 Android Enterprise를 사용하여 레거시 Android 장치 관리를 시작할 준비가 되지 않았을 수 있습니다. 이 경우 장치 관리자 모드에서 계속 관리할 수 있습니다. 장치 관리자 모드에 이미 등록된 장치의 경우 XenMobile은 장치 관리자 모드에서 계속 관리합니다.

새 Android 장치 등록에서 장치 관리자 모드를 사용하도록 허용하려면 레거시 장치용 등록 프로필을 만듭니다.

레거시 장치용 등록 프로필을 만들려면 다음을 수행합니다.

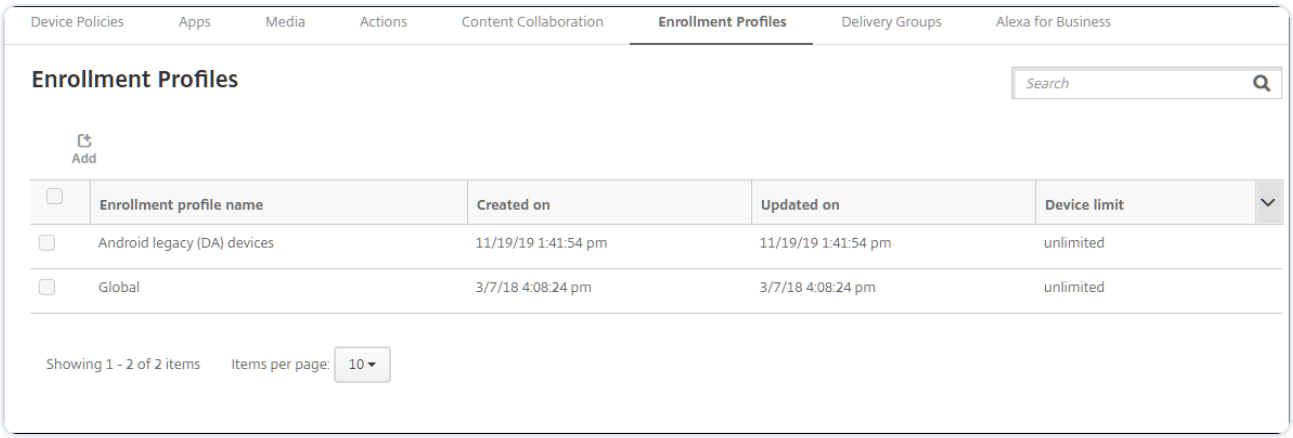
1. XenMobile 콘솔에서 **구성 > 등록 프로필**로 이동합니다.

2. 등록 프로필을 추가하려면 **추가**를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다.
3. 이 프로필을 가진 구성원이 등록할 수 있는 장치 수를 설정합니다.
4. **플랫폼**에서 **Android**를 선택하거나 **다음**을 클릭합니다. 등록 구성 페이지가 나타납니다.
5. **관리**를 **레거시 장치 관리(권장하지 않음)**로 설정합니다. **다음**을 클릭합니다.



6. Citrix MAM에 장치를 등록할지 여부를 선택합니다.
7. 사용자가 장치를 등록할 때 장치 관리를 거부하도록 허용하려면 **사용자가 장치 관리를 거부하도록 허용**을 **켜기**로 설정합니다. 기본값은 **켜기**입니다.
8. **할당(옵션)**을 선택합니다. 배달 그룹 할당 화면이 나타납니다.
9. 전용 장치를 등록하는 관리자가 있는 배달 그룹을 선택합니다. 그런 다음 **저장**을 클릭합니다.

추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.



레거시 장치를 장치 관리자 모드에서 계속 관리하려면 이 프로필을 사용하여 장치를 등록하거나 재등록하십시오. 사용자에게 Secure Hub를 다운로드하고 등록 서버 URL을 제공하도록 하여 작업 프로필 장치와 유사하게 장치 관리자 장치를 등록합니다.

Android Enterprise 작업 프로필 장치 프로비저닝

Android Enterprise 작업 프로필 장치는 프로필 소유자 모드로 등록됩니다. 이러한 장치는 새 장치이거나 공장 초기화된 장치일 필요가 없습니다. BYOD 장치는 작업 프로필 장치로 등록됩니다. 등록 환경은 XenMobile의 Android 등록과 유사합니다. 사용자는 Google Play에서 Secure Hub를 다운로드하여 장치를 등록합니다.

기본적으로 Android Enterprise에 작업 프로필 장치로 등록된 장치에서는 **USB 디버깅 및 알 수 없는 소스** 설정이 비활성화됩니다.

Android Enterprise에 장치를 작업 프로필 장치로 등록할 때는 항상 Google Play로 이동하십시오. 거기에서 Secure Hub가 사용자의 개인 프로필에 표시되도록 설정하십시오.

Android Enterprise 완전 관리형 장치 프로비저닝

이전 섹션에서 설정한 배포에 완전 관리형 장치를 등록할 수 있습니다. 완전 관리형 장치는 회사 소유 장치이며 장치 소유자 모드로 등록됩니다. 새 장치 또는 공장 초기화된 장치만 장치 소유자 모드로 등록할 수 있습니다.

다음 등록 방법 중 하나를 사용하여 장치를 장치 소유자 모드로 등록할 수 있습니다.

- **DPC 식별자 토큰:** 이 등록 방법을 사용하면 사용자가 장치를 설정할 때 `afw#xenmobile` 문자를 입력합니다. `afw#xenmobile`는 Citrix DPC 식별자 토큰입니다. 이 토큰은 장치가 XenMobile에 의해 관리됨을 식별하고 Google Play 스토어에서 Secure Hub를 다운로드합니다. Citrix DPC 식별자 토큰을 사용하여 장치 등록을 참조하십시오.
- **근거리 무선 통신(NFC) 범프:** NFC 범프 등록 방법은 근거리 무선 통신을 사용하여 두 장치 간에 데이터를 전송합니다. 새 장치 또는 공장 초기화된 장치에서는 Bluetooth, Wi-Fi 및 기타 통신 모드가 비활성화됩니다. NFC는 이 상태에서 장치가 사용할 수 있는 유일한 통신 프로토콜입니다. NFC 범프를 사용하여 장치 등록을 참조하십시오.
- **QR 코드:** QR 코드 등록은 태블릿과 같이 NFC를 지원하지 않는 분산된 장치 플릿을 등록하는 데 사용할 수 있습니다. QR 코드 등록 방법은 설정 마법사에서 QR 코드를 스캔하여 장치 프로필 모드를 설정하고 구성합니다. QR 코드를 사용하여 장치 등록을 참조하십시오.
- **제로 터치:** 제로 터치 등록을 사용하면 장치가 처음 전원을 켤 때 자동으로 등록되도록 구성할 수 있습니다. 제로 터치 등록은 Android 9.0 이상을 실행하는 일부 Android 장치에서 지원됩니다. 제로 터치 등록을 참조하십시오.
- **Google 계정:** 사용자는 프로비저닝 프로세스를 시작하기 위해 Google 계정 자격 증명을 입력합니다. 이 옵션은 Google Workspace를 사용하는 기업을 위한 것입니다.

Citrix DPC 식별자 토큰을 사용하여 장치 등록

사용자는 초기 설정을 위해 새 장치 또는 공장 초기화된 장치의 전원을 켠 후 Google 계정을 입력하라는 메시지가 표시되면 `afw#xenmobile`을(를) 입력합니다. 이 작업은 Secure Hub를 다운로드하고 설치합니다. 그런 다음 사용자는 Secure Hub 설정 프롬프트에 따라 등록을 완료합니다.

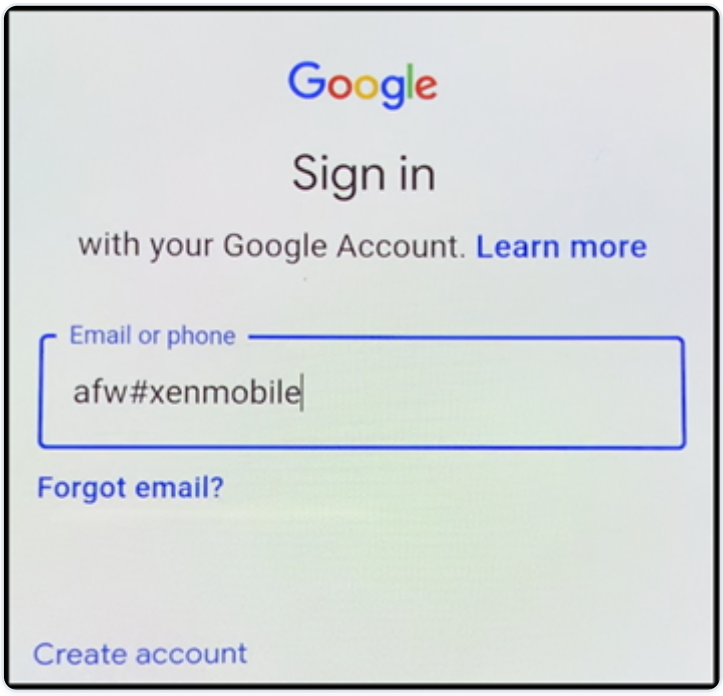
이 등록 방법은 Secure Hub의 최신 버전이 Google Play 스토어에서 다운로드되므로 대부분의 고객에게 권장됩니다. 다른 등록 방법과 달리 XenMobile Server에서 Secure Hub를 다운로드할 필요가 없습니다.

시스템 요구 사항

- Android OS를 실행하는 모든 Android 장치에서 지원됩니다.

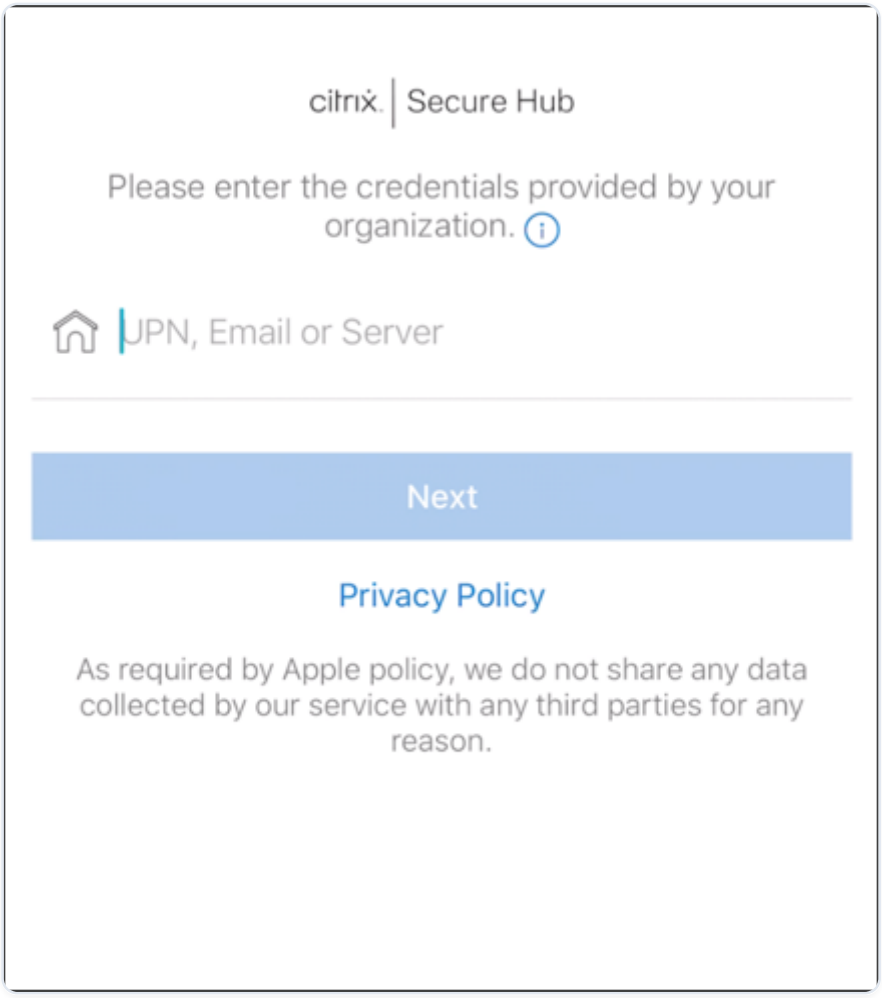
장치 등록

1. 새 장치 또는 공장 초기화된 장치를 웁니다.
2. 초기 장치 설정이 로드되고 Google 계정을 요청합니다. 장치 홈 화면이 로드되면 알림 표시줄에서 **설정 완료** 알림을 확인하십시오.
3. **이메일 또는 전화** 필드에 `afw#xenmobile`을(를) 입력합니다.



4. Secure Hub 설치를 요청하는 Android Enterprise 화면에서 **설치**를 탭합니다.
5. Secure Hub 설치 프로그램 화면에서 **설치**를 탭합니다.
6. 모든 앱 권한 요청에 대해 **허용**을 탭합니다.
7. Secure Hub를 설치하고 장치를 관리하도록 허용하려면 **동의 및 계속**을 탭합니다.

8. Secure Hub가 설치되었고 기본 등록 화면에 있습니다. 이 예시에서는 자동 검색(AutoDiscovery)이 설정되어 있지 않습니다. 설정되어 있다면 사용자는 사용자 이름/이메일을 입력하고 서버를 찾을 수 있습니다. 대신 환경에 대한 등록 URL을 입력하고 **다음**을 탭합니다.



9. XenMobile의 기본 구성은 사용자가 MAM 또는 MDM+MAM을 사용할지 선택할 수 있도록 합니다. 이와 같이 메시지가 표시되면 **예, 등록**을 탭하여 MDM+MAM을 선택합니다.
10. 사용자 이름과 암호를 입력한 다음 **다음**을 탭합니다.
11. 장치 암호를 구성하라는 메시지가 사용자에게 표시됩니다. **설정**을 탭하고 암호를 입력합니다.
12. 작업 프로필 잠금 해제 방법을 구성하라는 메시지가 사용자에게 표시됩니다. 이 예에서는 **암호**를 탭하고 **PIN**을 탭한 다음 PIN을 입력합니다.

    암호 옵션(/en-us/xenmobile/server/media/passcode-options.png)
13. 이제 장치가 Secure Hub **내 앱** 시작 화면에 있습니다. **스토어에서 앱 추가**를 탭합니다.
14. Secure Web을 추가하려면 **Secure Web**을 탭합니다.

    Secure Hub 스토어(/en-us/xenmobile/server/media/secure-hub-store.png)
15. **추가**를 탭합니다.

16. Secure Hub는 Secure Web을 설치하기 위해 사용자를 Google Play 스토어로 안내합니다. **설치**를 탭합니다.
17. Secure Web이 설치되면 **열기**를 탭합니다. 주소 표시줄에 내부 사이트의 URL을 입력하고 페이지가 로드되는지 확인합니다.
18. 장치에서 **설정 > 계정**으로 이동합니다. **관리 계정**을 수정할 수 없음을 확인합니다. 화면 공유 또는 원격 디버깅을 위한 개발자 옵션도 차단됩니다.

    계정 수정(/en-us/xenmobile/server/media/account-modification-not-allowed.png)

NFC 범프를 사용하여 장치 등록

NFC 범프를 사용하여 장치를 완전 관리형 장치로 등록하려면 두 개의 장치가 필요합니다. 하나는 공장 설정으로 재설정된 장치이고 다른 하나는 XenMobile Provisioning Tool을 실행하는 장치입니다.

시스템 요구 사항 및 전제 조건

- 지원되는 Android 장치.
- 새로 구입했거나 공장 초기화된 장치로, Android Enterprise용으로 완전 관리형 장치로 프로비저닝됩니다. 이 필수 구성 요소를 완료하는 단계는 이 문서의 뒷부분에서 찾을 수 있습니다.
- NFC 기능이 있고 구성된 프로비저닝 도구를 실행하는 다른 장치. 프로비저닝 도구는 Secure Hub 또는 Citrix 다운로드 페이지에서 사용할 수 있습니다.

각 장치에는 Secure Hub에서 관리하는 Android Enterprise 프로필이 하나만 있을 수 있습니다. 각 장치에는 하나의 프로필만 허용됩니다. 두 번째 DPC 앱을 추가하려고 하면 설치된 Secure Hub가 제거됩니다.

NFC 범프를 통해 전송되는 데이터

공장 초기화된 장치를 프로비저닝하려면 Android Enterprise를 초기화하기 위해 NFC 범프를 통해 다음 데이터를 전송해야 합니다.

- 장치 소유자 역할을 하는 DPC 앱의 패키지 이름(이 경우 Secure Hub).
- 장치가 DPC 앱을 다운로드할 수 있는 인트라넷/인터넷 위치.
- 다운로드가 성공했는지 확인하기 위한 DPC 앱의 SHA1 해시.
- 공장 초기화된 장치가 DPC 앱에 연결하고 다운로드할 수 있도록 하는 Wi-Fi 연결 세부 정보. 참고: Android는 현재 이 단계에서 802.1x Wi-Fi를 지원하지 않습니다.
- 장치의 시간대(선택 사항).
- 장치의 지리적 위치(선택 사항).

두 장치가 범프되면 프로비저닝 도구의 데이터가 공장 초기화된 장치로 전송됩니다. 이 데이터는 관리자 설정으로 Secure Hub를 다운로드하는 데 사용됩니다. 시간대 및 위치 값을 입력하지 않으면 Android가 새 장치에 값을 자동으로 구성합니다.

XenMobile 프로비저닝 도구 구성

NFC 범프를 수행하기 전에 프로비저닝 도구를 구성해야 합니다. 이 구성은 NFC 범프 중에 공장 초기화된 장치로 전송됩니다.

프로비저닝 도구 구성(/en-us/xenmobile/server/media/nfc-provisioning-secure-hub.png)

필수 필드에 데이터를 직접 입력하거나 텍스트 파일을 사용하여 채울 수 있습니다. 다음 절차의 단계에서는 텍스트 파일을 구성하는 방법과 각 필드에 대한 설명을 제공합니다. 앱은 입력한 정보를 저장하지 않으므로 나중에 사용할 정보를 보관하기 위해 텍스트 파일을 만드는 것이 좋습니다.

텍스트 파일을 사용하여 프로비저닝 도구를 구성하려면

파일 이름을 nfcprovisioning.txt로 지정하고 장치의 SD 카드에 있는 `/sdcard/` 폴더에 파일을 배치합니다. 그러면 앱이 텍스트 파일을 읽고 값을 채울 수 있습니다.

텍스트 파일에는 다음 데이터가 있어야 합니다.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

이 줄은 EMM 공급자 앱의 인트라넷/인터넷 위치입니다. 초기화된 장치가 NFC 범프 후 Wi-Fi에 연결되면 장치는 다운로드를 위해 이 위치에 액세스할 수 있어야 합니다. URL은 특별한 서식이 필요 없는 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 단계는 이 문서의 뒷부분에서 설명합니다.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

이 줄은 프로비저닝 도구가 실행 중인 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 639-1에 정의된 두 글자의 소문자 ISO 언어 코드(예: en)입니다. 국가 코드는 ISO 3166-1에 정의된 두 글자의 대문자 ISO 국가 코드(예: US)입니다. 예를 들어, 미국에서 사용되는 영어의 경우 en_US를 입력합니다. 코드를 입력하지 않으면 국가 및 언어가 자동으로 채워집니다.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

장치가 실행되는 시간대입니다. area/location 형식의 Olson 이름을 입력합니다. 예를 들어, 태평양 표준시의 경우 America/Los_Angeles를 입력합니다. 이름을 입력하지 않으면 시간대가 자동으로 채워집니다.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

이 값은 Secure Hub로 앱에 하드코딩되어 있으므로 이 데이터는 필요하지 않습니다. 완전성을 위해 여기에 언급된 것일 뿐입니다.

WPA2를 사용하여 보호되는 Wi-Fi가 있는 경우, 완성된 nfcprovisioning.txt 파일은 다음과 같을 수 있습니다.

`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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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`

보호되지 않은 Wi-Fi가 있는 경우, 완성된 nfcprovisioning.txt 파일은 다음과 같을 수 있습니다.

`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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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 Hub의 체크섬을 가져오려면

Secure Hub의 체크섬은 상수 값입니다: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`.
Secure Hub용 APK 파일을 다운로드하려면 다음 Google Play 스토어 링크를 사용하십시오: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

앱 체크섬을 가져오려면

전제 조건:

- Android SDK 빌드 도구의 **apksigner** 도구
- OpenSSL 명령줄

모든 앱의 체크섬을 가져오려면 다음 단계를 따르십시오:

1. Google Play 스토어에서 앱의 APK 파일을 다운로드합니다.
2. OpenSSL 명령줄에서 **apksigner** 도구로 이동하여 `android-sdk/build-tools/<version>/apksigner` 다음을 입력합니다:

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   ```

   명령은 유효한 체크섬을 반환합니다.
3. QR 코드를 생성하려면 `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` 필드에 체크섬을 입력합니다. 예시:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",


"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
```

```
      "serverURL": "https://supportablility.xm.cloud.com"

   }

}
```

사용된 라이브러리

프로비저닝 도구는 소스 코드에서 다음 라이브러리를 사용합니다:

- Apache license 2.0에 따라 Google에서 제공하는 v7 `appcompat` 라이브러리, 디자인 지원 라이브러리 및 v7 팔레트 라이브러리

  자세한 내용은 Support Library Features Guide를 참조하십시오.

- Apache license 2.0에 따라 Jake Wharton이 제공하는 Butter Knife

QR 코드를 사용하여 장치 등록

QR 코드를 사용하여 완전 관리형 장치를 등록하려면, JSON을 생성하고 해당 JSON을 QR 코드로 변환하여 QR 코드를 생성합니다. 장치 카메라는 QR 코드를 스캔하여 장치를 등록합니다.

시스템 요구 사항

- Android 9.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.

JSON에서 QR 코드 생성

다음 필드를 사용하여 JSON을 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: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-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 639-1에 정의된 두 글자의 소문자 ISO 언어 코드(예: en)입니다. 국가 코드는 ISO 3166-1에 정의된 두 글자의 대문자 ISO 국가 코드(예: US)입니다. 예를 들어, 미국에서 사용되는 영어의 경우 en_US를 입력합니다.

- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가 실행되는 시간대입니다.

  area/location 형식의 Olson 이름을(를) 입력합니다. 예를 들어, 태평양 표준시의 경우 America/Los_Angeles입니다. 입력하지 않으면 시간대가 자동으로 채워집니다.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Epoch 이후 밀리초 단위 시간입니다.

  유닉스 에포크(또는 유닉스 시간, POSIX 시간, 유닉스 타임스탬프)는 January 1, 1970(UTC/GMT 자정) 이후 경과된 초의 수입니다. 이 시간에는 윤초가 포함되지 않습니다(ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 프로필 생성 중 암호화를 건너뛰려면 **true**로 설정합니다. 프로필 생성 중 암호화를 강제하려면 **false**로 설정합니다.

일반적인 JSON은 다음과 같습니다.

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "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
}
```

https://jsonlint.com과 같은 JSON 유효성 검사 도구를 사용하여 생성된 JSON의 유효성을 검사합니다. https://www.qr-code-generator.com와 같은 온라인 QR 코드 생성기를 사용하여 해당 JSON 문자열을 QR 코드로 변환합니다.

이 QR 코드는 초기화된 기기에서 스캔되어 기기를 완전 관리형 기기로 등록합니다.

기기를 등록하려면

새 기기 또는 초기화된 기기의 전원을 켠 후:

1. 환영 화면에서 화면을 여섯 번 탭하여 QR 코드 등록 흐름을 시작합니다.
2. 메시지가 표시되면 Wi-Fi에 연결합니다. QR 코드(JSON으로 인코딩됨)에 있는 Secure Hub의 다운로드 위치는 이 Wi-Fi 네트워크를 통해 액세스할 수 있습니다.

   기기가 Wi-Fi에 성공적으로 연결되면 Google에서 QR 코드 리더를 다운로드하고 카메라를 실행합니다.
3. 코드를 스캔하려면 카메라를 QR 코드에 비춥니다.

   Android는 QR 코드의 다운로드 위치에서 Secure Hub를 다운로드하고, 서명 인증서 서명을 검증하고, Secure Hub를 설치한 다음 기기 소유자로 설정합니다.

자세한 내용은 Android EMM 개발자를 위한 Google 가이드 `<https://developers.google.com/android/work/prov-devices#qr_code_method>`를 참조하십시오.

제로 터치 등록

제로 터치 등록을 사용하면 기기가 처음 전원을 켰을 때 완전 관리형 기기로 자체 프로비저닝되도록 설정할 수 있습니다.

기기 리셀러는 Android 제로 터치 포털(기기에 구성을 적용할 수 있는 온라인 도구)에서 사용자 계정을 생성합니다. Android 제로 터치 포털을 사용하여 하나 이상의 제로 터치 등록 구성을 생성하고 해당 구성을 계정에 할당된 기기에 적용합니다. 사용자가 이 기기의 전원을 켜면 기기는 XenMobile에 자동으로 등록됩니다. 기기에 할당된 구성은 자동 등록 프로세스를 정의합니다.

시스템 요구 사항

- 제로 터치 등록은 Android 9.0부터 지원됩니다.

리셀러의 기기 및 계정 정보

- 제로 터치 등록에 적합한 장치는 엔터프라이즈 리셀러 또는 Google 파트너로부터 구매합니다. Android Enterprise 제로 터치 파트너 목록은 Android 웹사이트를 참조하십시오.
- 리셀러가 생성한 Android Enterprise 제로 터치 포털 계정.
- 리셀러가 제공한 Android Enterprise 제로 터치 포털 계정 로그인 정보.

제로 터치 구성 생성

제로 터치 구성을 생성할 때, 구성의 세부 정보를 지정하기 위해 사용자 지정 JSON을 포함합니다.

이 JSON을 사용하여 지정한 XenMobile Server에 장치를 등록하도록 구성합니다. 이 예에서 'URL' 대신 서버의 URL을 사용하십시오.

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

  {

        "serverURL":"URL",

   }

}
```

더 많은 매개변수가 포함된 선택적 JSON을 사용하여 구성을 추가로 사용자 지정할 수 있습니다. 이 예는 XenMobile Server와 이 구성을 사용하는 장치가 서버에 로그온하는 데 사용하는 사용자 이름 및 암호를 지정합니다.

```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

     {

         "serverURL":"URL",

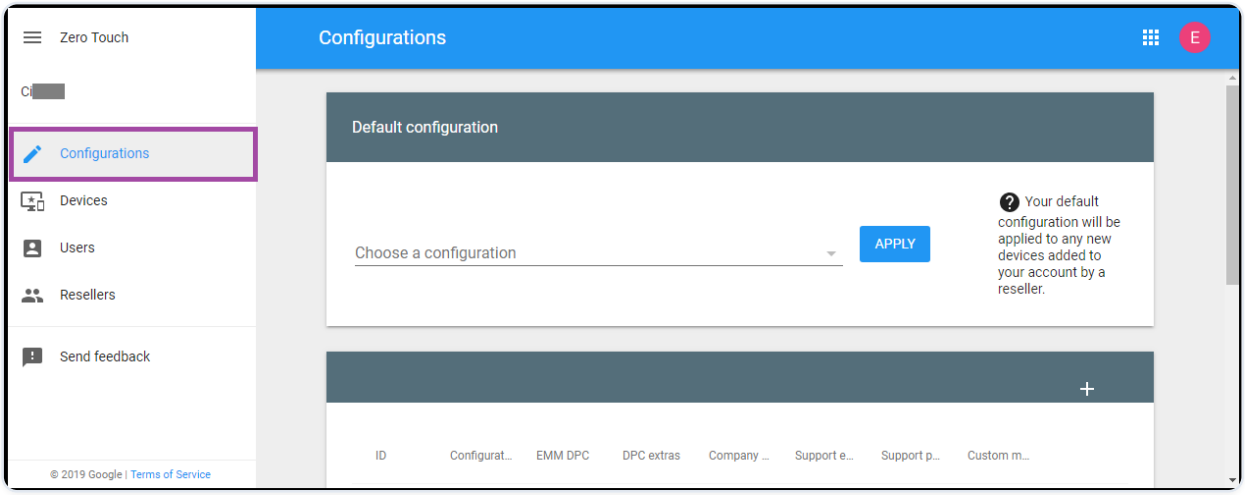
         "xm_username":"username",

         "xm_password":"password"

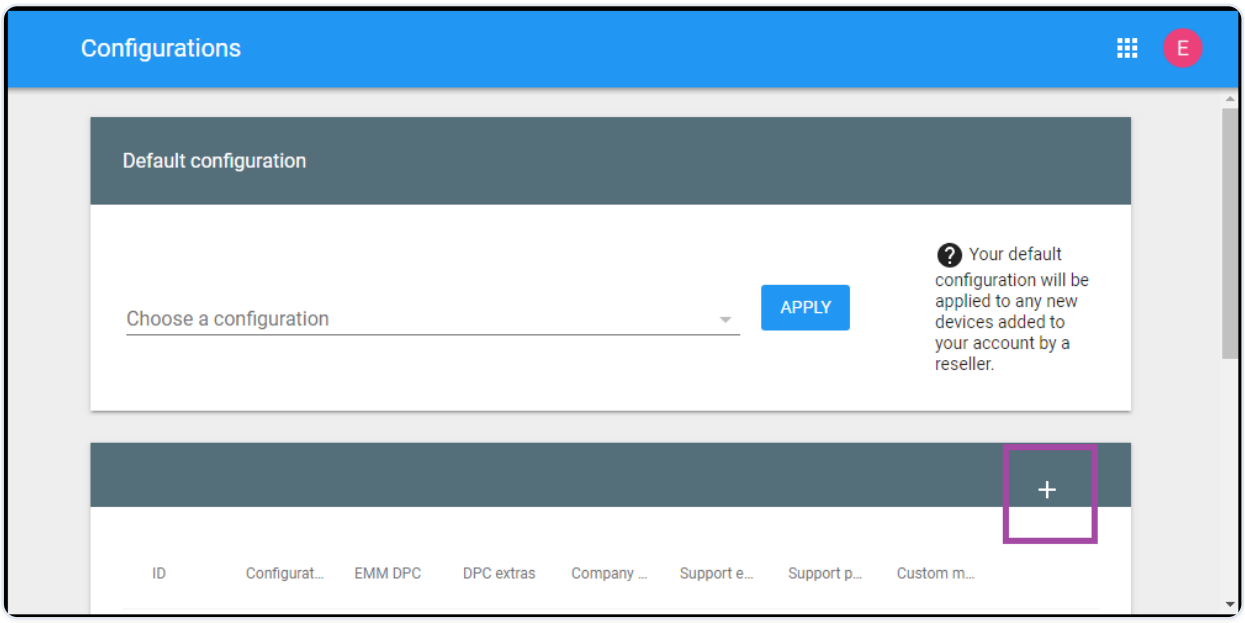
     }

       }
```

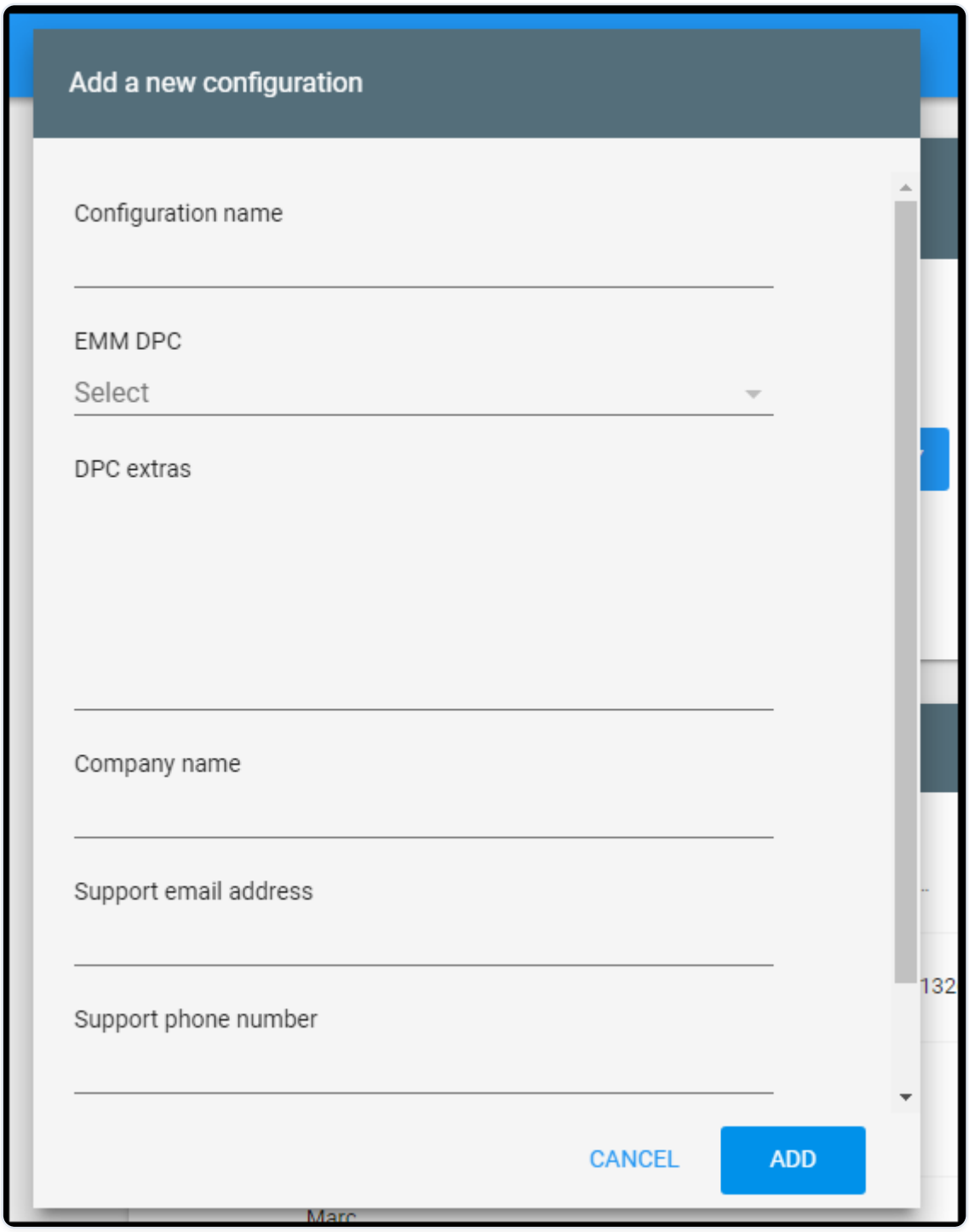
1. https://partner.android.com/zerotouch에서 Android 제로 터치 포털로 이동합니다. 제로 터치 장치 리셀러로부터 받은 계정 정보로 로그인합니다.
2. **Configuration**을 클릭합니다.



3. 구성 테이블 위에 있는 **+**를 클릭합니다.



4. 표시되는 구성 창에 구성 정보를 입력합니다.



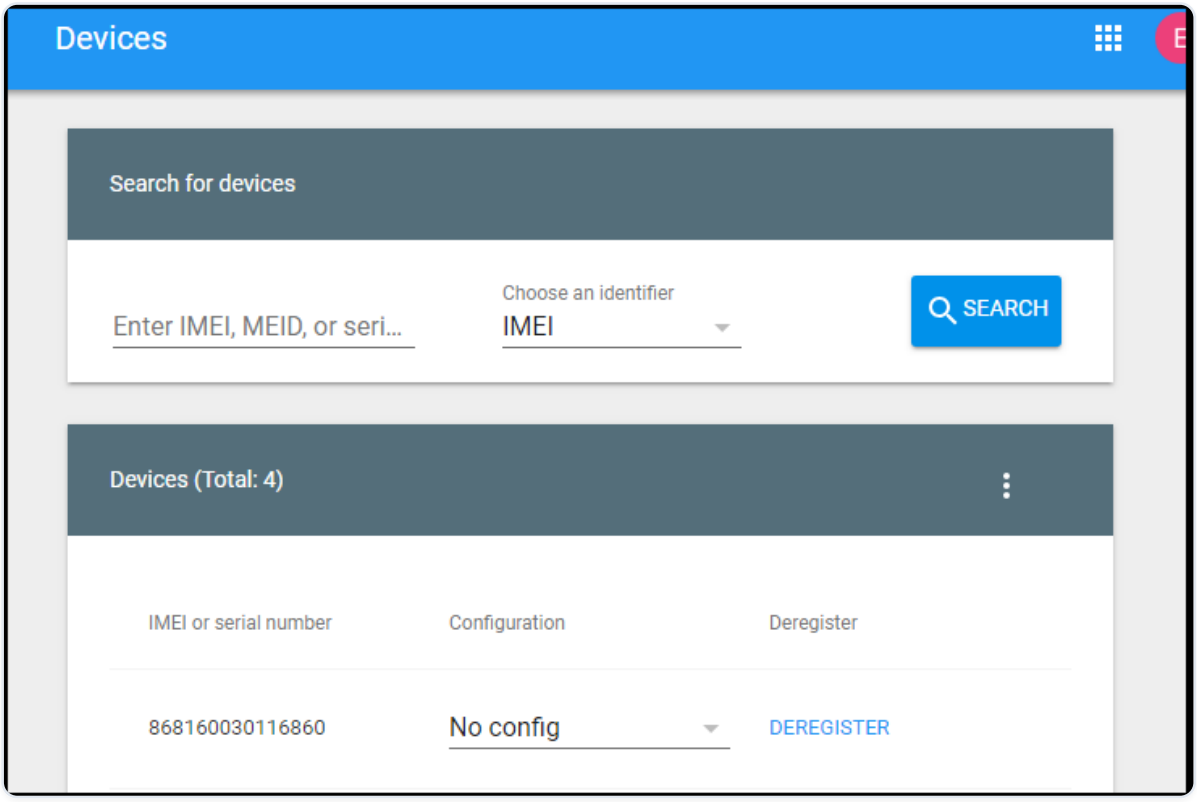
- **구성 이름:** 이 구성에 사용할 이름을 입력합니다.
- **EMM DPC: Citrix Secure Hub**를 선택합니다.
- **DPC 추가:** 사용자 지정 JSON 텍스트를 이 필드에 붙여넣습니다.
- **회사 이름:** 장치 프로비저닝 중에 Android Enterprise 제로 터치 장치에 표시할 이름을 입력합니다.
- **지원 이메일 주소:** 사용자가 도움을 요청할 수 있는 이메일 주소를 입력합니다. 이 주소는 장치 프로비저닝 전에 Android Enterprise 제로 터치 장치에 표시됩니다.

- **지원 전화번호:** 사용자가 도움을 요청할 수 있는 전화번호를 입력합니다. 이 전화번호는 장치 프로비저닝 전에 Android Enterprise 제로 터치 장치에 표시됩니다.
- **사용자 지정 메시지:** 선택적으로, 사용자가 연락하거나 장치에서 발생하는 상황에 대한 자세한 정보를 제공하는 데 도움이 되는 한두 문장을 추가합니다. 이 사용자 지정 메시지는 장치 프로비저닝 전에 Android Enterprise 제로 터치 장치에 표시됩니다.

5. **추가**를 클릭합니다.
6. 더 많은 구성을 만들려면 2단계부터 4단계까지 반복합니다.
7. 장치에 구성을 적용하려면:

   a. Android 제로 터치 포털에서 **장치**를 클릭합니다.

   b. 장치 목록에서 장치를 찾아 할당할 구성을 선택합니다.



   c. **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 등록을 참조하십시오. 이 Android Enterprise 도움말 항목에는 구성을 관리하고 장치에 적용하는 방법에 대한 자세한 정보가 있습니다.

전용 Android Enterprise 장치 프로비저닝

전용 Android Enterprise 장치는 단일 사용 사례를 충족하도록 전용된 완전 관리형 장치입니다. 전용 장치는 기업 소유 단일 사용(COSU) 장치라고도 합니다. 이러한 장치는 이 사용 사례에 필요한 작업을 수행하는 데 필요한 하나의 앱 또는 소수의 앱으로 제한됩니다. 또한 사용자가 다른 앱을 활성화하거나 장치에서 다른 작업을 수행하는 것을 방지합니다.

Android Enterprise 완전 관리형 장치 프로비저닝에 설명된 대로 다른 완전 관리형 장치에 사용되는 등록 방법 중 하나를 사용하여 전용 장치를 등록합니다. 전용 장치를 프로비저닝하려면 등록 전에 추가 설정이 필요합니다.

전용 장치를 프로비저닝하려면:

- 전용 장치를 XenMobile 배포에 등록하도록 허용하는 XenMobile 관리자를 위한 등록 프로필을 추가합니다. 등록 프로필 만들기를 참조하십시오.
- 전용 장치에서 액세스하려는 앱을 허용합니다.
- 선택적으로 허용된 앱이 잠금 작업 모드를 허용하도록 설정합니다. 앱이 잠금 작업 모드에 있으면 사용자가 앱을 열 때 앱이 장치 화면에 고정됩니다. 홈 버튼이 나타나지 않고 뒤로 버튼이 비활성화됩니다. 사용자는 로그아웃과 같이 앱에 프로그래밍된 작업을 사용하여 앱을 종료합니다.
- 추가한 등록 프로필에 각 장치를 등록합니다.

시스템 요구 사항

- 전용 장치 등록 지원은 Android 6.0부터 시작됩니다.

앱 허용 및 잠금 작업 모드 설정

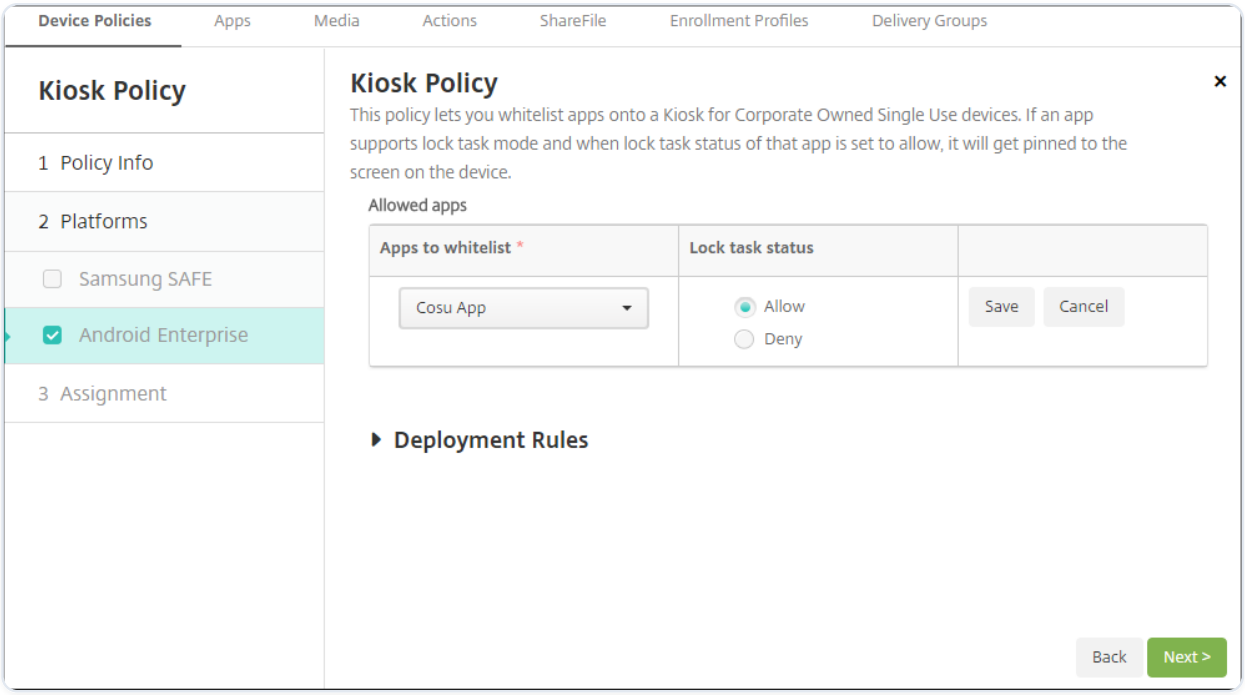
키오스크 장치 정책을 사용하면 앱을 허용하고 잠금 작업 모드를 설정할 수 있습니다. 기본적으로 Secure Hub 및 Google Play 서비스는 허용됩니다.

키오스크 정책을 추가하려면 다음을 수행합니다.

1. XenMobile 콘솔에서 **구성 > 장치 정책**을 클릭합니다. **장치 정책** 페이지가 나타납니다.
2. **추가**를 클릭합니다. **새 정책 추가** 대화 상자가 나타납니다.
3. **자세히**를 확장한 다음 보안 아래에서 **키오스크**를 클릭합니다. **키오스크 정책** 페이지가 나타납니다.
4. 플랫폼에서 **Android Enterprise**를 선택합니다. 다른 플랫폼은 지웁니다.
5. 정책 정보 창에서 **정책 이름**과 선택적 **설명**을 입력합니다.
6. **다음**을 클릭한 다음 **추가**를 클릭합니다.
7. 앱을 허용하고 해당 앱에 대한 잠금 작업 모드를 허용하거나 거부하려면 다음을 수행합니다.

목록에서 허용할 앱을 선택합니다.

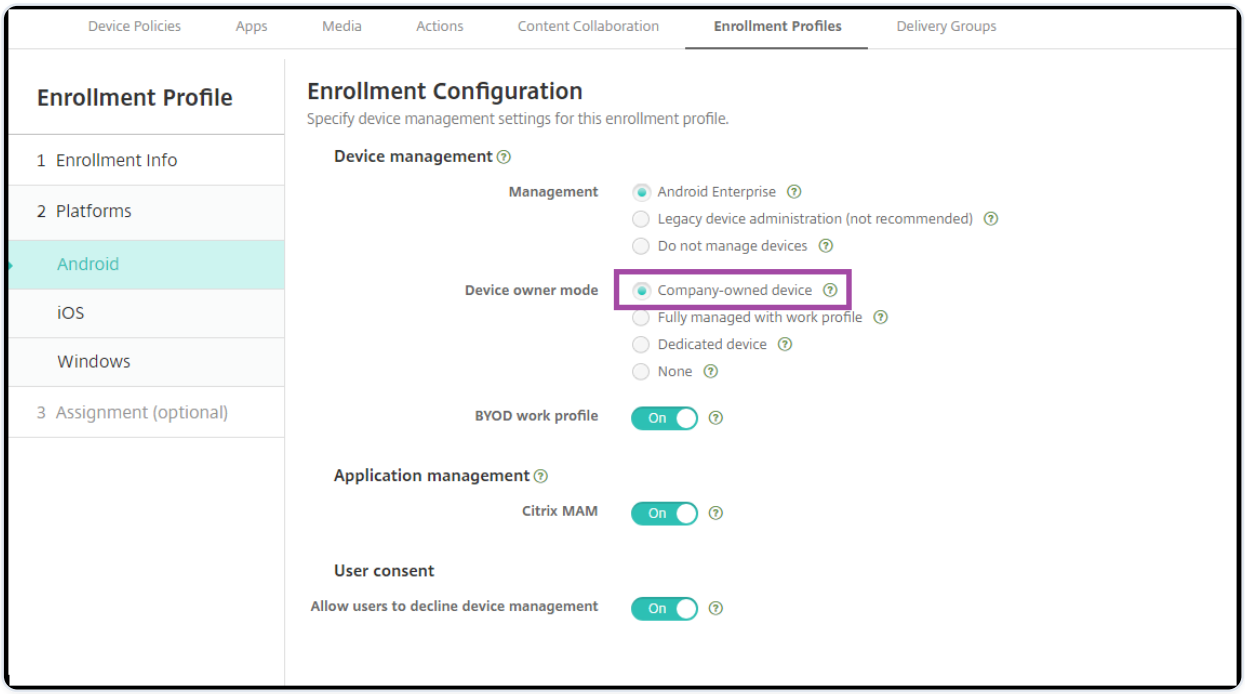
사용자가 앱을 시작할 때 앱이 장치 화면에 고정되도록 설정하려면 **허용**을 선택합니다. 앱이 고정되지 않도록 설정하려면 **거부**를 선택합니다. 기본값은 **허용**입니다.



8. **저장**을 클릭합니다.
9. 다른 앱을 허용하고 해당 앱에 대한 잠금 작업 모드를 허용하거나 거부하려면 **추가**를 클릭합니다.
10. 배포 규칙을 구성하고 배달 그룹을 선택합니다. 자세한 내용은 장치 정책을 참조하십시오.

장치를 등록하려면

1. **다음**을 클릭하거나 **플랫폼**에서 **Android**를 선택합니다. 등록 구성 페이지가 나타납니다.
2. **관리**를 **Android Enterprise**로 설정합니다.
3. **장치 소유자 모드**를 **회사 소유 장치**로 설정합니다.



4. **할당(옵션)**을 선택합니다. 배달 그룹 할당 화면이 나타납니다.
5. 전용 장치를 등록하는 관리자가 있는 배달 그룹을 선택합니다. 그런 다음 **저장**을 클릭합니다.

등록 프로필에서 **BYOD 업무 프로필**을 사용하도록 설정한 경우, 새 장치가 아니거나 공장 초기화되지 않은 장치는 업무 프로필 장치로 등록됩니다. Android Enterprise 업무 프로필 장치 프로비저닝을 참조하십시오.

업무 프로필이 있는 Android Enterprise 완전 관리형 기기 프로비저닝(COPE 기기)

이전에는 COPE 기기라고 불렸던 업무 프로필이 있는 완전 관리형 기기는 업무용 및 개인용으로 모두 사용되는 회사 소유 기기입니다. 조직에서 전체 기기를 관리합니다. 기기에는 하나의 정책 집합을 적용하고 업무 프로필에는 별도의 정책 집합을 적용할 수 있습니다.

XenMobile 콘솔에서 업무 프로필이 있는 완전 관리형 기기는 다음 용어로 표시됩니다.

- 기기 소유권은 "회사"입니다.
- 기기 Android Enterprise 설치 유형은 "개인적으로 활성화된 회사 소유자"입니다.

시스템 요구 사항

- 업무 프로필이 있는 완전 관리형 기기 등록 지원은 Android 9.0부터 Android 10.x까지입니다.

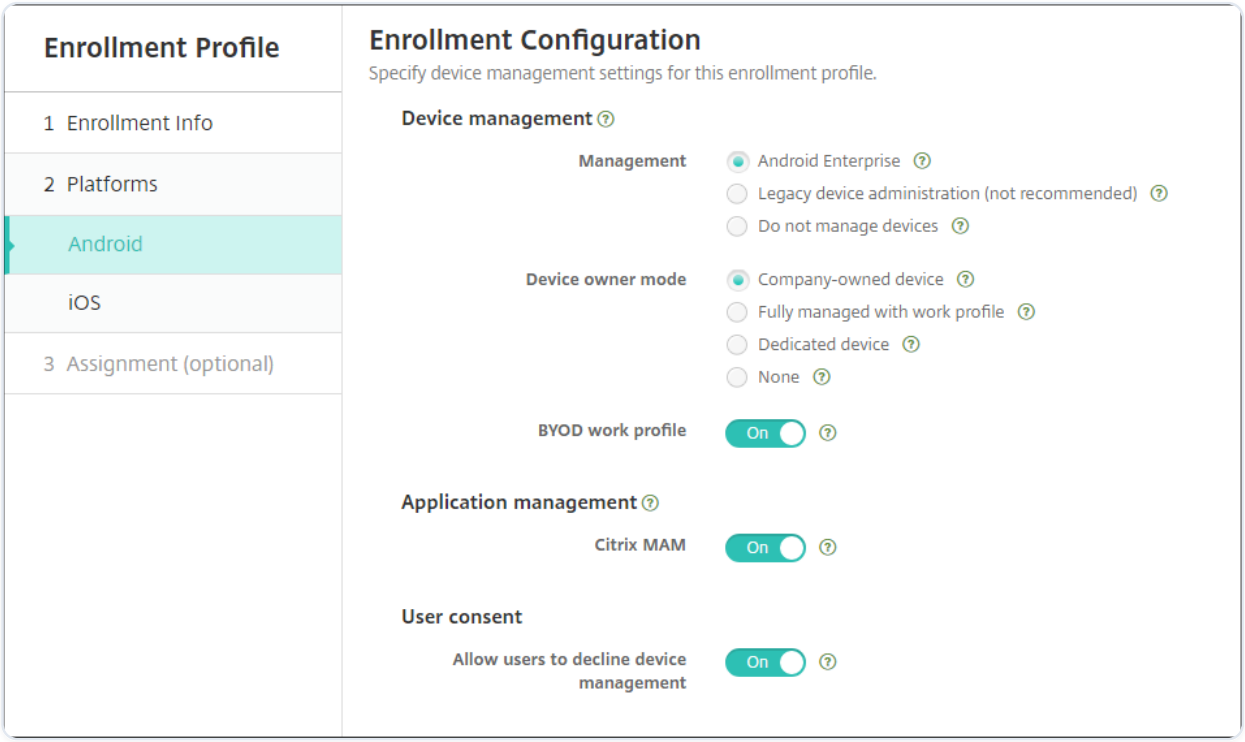
업무 프로필이 있는 완전 관리형 기기용 등록 프로필 추가

업무 프로필이 있는 완전 관리형 기기를 등록하기 위한 등록 프로필을 생성합니다. 이 등록 프로필에 할당된 전달 그룹의 관리자는 업무 프로필이 있는 완전 관리형 기기를 등록할 수 있습니다. 이러한 관리자가 필요한

모든 기기를 등록할 수 있도록 사용자당 무제한 기기를 허용하는 등록 프로필을 생성합니다. 이 프로필을 업무 프로필이 있는 완전 관리형 기기를 등록하는 관리자가 있는 전달 그룹에 할당합니다.

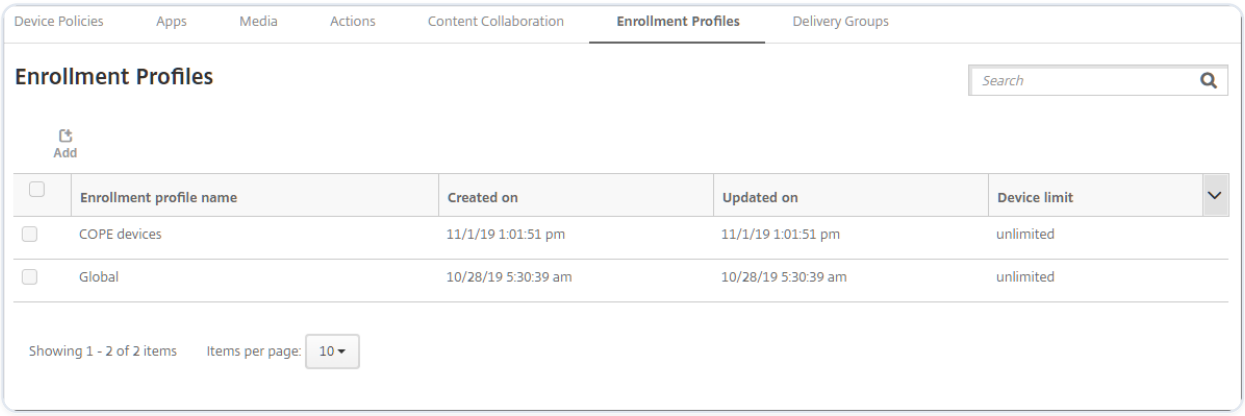
1. XenMobile 콘솔에서 **구성 > 등록 프로필**로 이동합니다.
2. 등록 프로필을 추가하려면 **추가**를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력합니다. 이 프로필을 가진 구성원이 등록할 수 있는 기기 수가 무제한으로 설정되어 있는지 확인합니다.
3. **다음**을 클릭하거나 **플랫폼**에서 **Android Enterprise**를 선택합니다. 등록 구성 페이지가 나타납니다.
4. **등록 유형**을 다음 중 하나로 설정합니다.

   - **완전 관리형/업무 프로필:** 새 기기 또는 공장 초기화된 기기는 완전 관리형으로 등록됩니다. BYOD 기기는 사용자가 관리하는 업무 프로필만으로 등록됩니다.
   - **COPE/업무 프로필:** 새 기기 또는 공장 초기화된 기기는 업무 프로필이 있는 완전 관리형으로 등록됩니다. BYOD 기기는 사용자가 관리하는 업무 프로필만으로 등록됩니다.



5. **할당(선택 사항)**을 선택하거나 **다음**을 클릭합니다. 배달 그룹 할당 화면이 나타납니다.
6. 전용 장치를 등록하는 관리자가 있는 배달 그룹을 선택합니다. 그런 다음 **저장**을 클릭합니다.

   추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.



사용자가 서로 다른 등록 프로필을 가진 여러 배달 그룹에 속하는 경우, 배달 그룹의 이름이 사용되는 등록 프로필을 결정합니다. XenMobile은 배달 그룹의 알파벳순 목록에서 마지막에 나타나는 배달 그룹을 선택합니다.

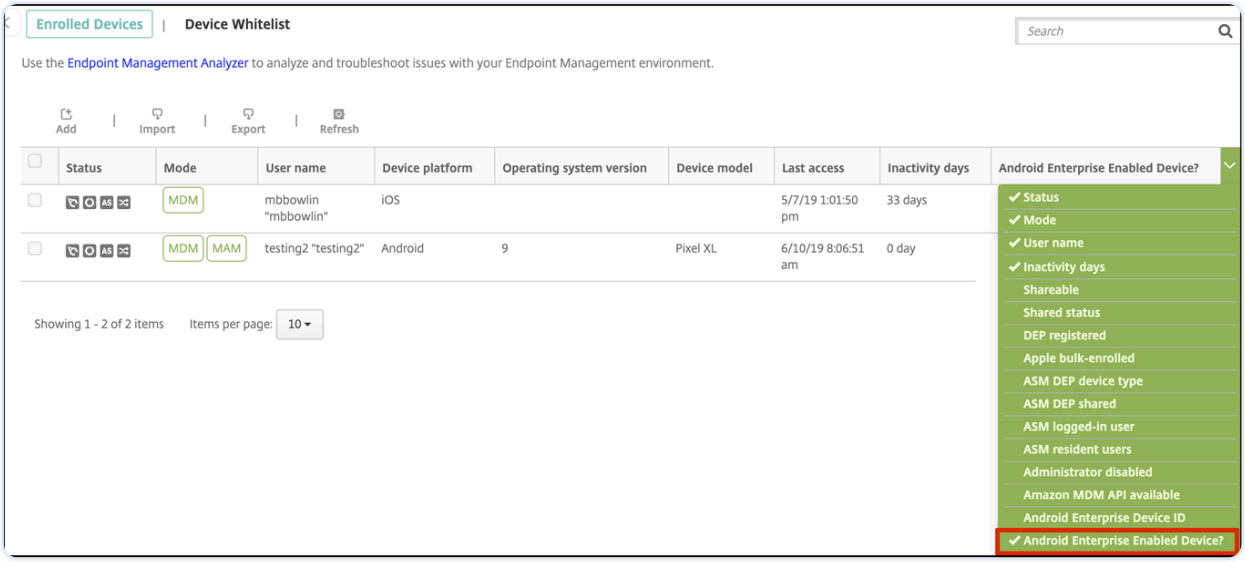
장치 등록

새 장치 및 공장 초기화된 장치는 DPC 식별자 토큰, 근거리 무선 통신(NFC) 범프 또는 QR 코드 방식을 사용하여 작업 프로필이 있는 완전 관리형 장치로 등록됩니다. Citrix DPC 식별자 토큰을 사용하여 장치 등록, NFC 범프를 사용하여 장치 등록 또는 QR 코드를 사용하여 장치 등록을 참조하십시오.

새 장치가 아니거나 공장 초기화되지 않은 장치는 Android Enterprise 작업 프로필 장치 프로비저닝에 설명된 대로 작업 프로필 장치로 등록됩니다.

XenMobile 콘솔에서 Android Enterprise 장치 보기

1. XenMobile 콘솔에서 **관리 > 장치**로 이동합니다.
2. 이 페이지의 테이블 오른쪽에 있는 메뉴를 클릭하여 **Android Enterprise 사용 장치?** 열을 추가합니다.



3. 사용 가능한 보안 작업을 보려면 완전 관리형 장치를 선택하고 **보안**을 클릭합니다. 장치가 완전 관리형인 경우 **전체 초기화** 작업은 사용할 수 있지만 **선택 초기화**는 사용할 수 없습니다. 이러한 차이는 장치가 관

리형 Google Play 스토어의 앱만 허용하기 때문입니다. 사용자가 공용 스토어에서 애플리케이션을 설치할 수 있는 옵션은 없습니다. 조직에서 장치의 모든 콘텐츠를 관리합니다.



Android Enterprise 장치 및 앱 정책 구성

장치 및 앱 수준에서 제어되는 정책에 대한 개요는 Android Enterprise용 지원되는 장치 정책 및 MDX 정책을(를) 참조하십시오.

정책에 대해 알아야 할 사항:

- **데이터 손실 방지:** XenMobile MAM 컨테이너 기술은 암호화 및 기타 모바일 데이터 손실 방지(DLP) 기술을 사용하여 앱을 보호합니다. Citrix MAM SDK 또는 MDX Toolkit을 사용하여 앱을 MDX 지원으로 설정하십시오.
- **장치 제한:** 수십 가지 장치 제한을 통해 다음과 같은 기능을 제어할 수 있습니다.
  - 장치 카메라 사용
  - 업무 및 개인 프로필 간 복사 및 붙여넣기 사용
- **앱별 VPN:** 관리형 구성 장치 정책을 사용하여 Android Enterprise용 VPN 프로필을 구성하십시오.
- **이메일 정책:** 관리형 구성 장치 정책을 사용하여 앱을 구성하는 것이 좋습니다.

이 표에는 Android Enterprise 장치에 사용할 수 있는 모든 장치 정책이 나열되어 있습니다.

> **중요:**

Android Enterprise에 등록하고 MDX 앱을 사용하는 장치의 경우: MDX 및 Android Enterprise를 통해 일부 설정을 제어할 수 있습니다. MDX에 대해 가장 제한이 적은 정책 설정을 사용하고 Android Enterprise를 통해 정책을 제어하십시오.

Android Enterprise 앱 권한	관리형 구성	앱 인벤토리
앱 제거	관리되는 앱 자동 업데이트(/ko-kr/xenmobile/server/policies/app-auto-update-policy.html)	OS 업데이트 제어(/ko-kr/xenmobile/server/policies/control-os-updates.html#android-enterprise-settings)
자격 증명(/ko-kr/xenmobile/server/policies/credentials-policy.html#android-enterprise-settings)	사용자 지정 XML(/ko-kr/xenmobile/server/policies/custom-xml-policy.html)	엑스체인지
파일(/ko-kr/xenmobile/server/policies/files-policy.html#android-enterprise-settings)	키가드 관리(/ko-kr/xenmobile/server/policies/android-enterprise-keyguard-management-policy.html)	키오스크(/ko-kr/xenmobile/server/policies/kiosk-policy.html#android-enterprise-settings)
위치(/ko-kr/xenmobile/server/policies/location-policy.html#android-enterprise-settings)	암호(/ko-kr/xenmobile/server/policies/passcode-policy.html#android-enterprise-settings)	제한(/ko-kr/xenmobile/server/policies/restrictions-policy.html#android-enterprise-settings)
Samsung MDM 라이선스 키(/ko-kr/xenmobile/server/policies/samsung-mdm-license-key-policy.html#samsung-safe-settings)	예약(/ko-kr/xenmobile/server/policies/connection-scheduling-policy.html)	와이파이
XenMobile 옵션(/ko-kr/xenmobile/server/policies/options-policy.html#android-enterprise-settings)		

업무 프로필이 있는 완전 관리형 기기(COPE 기기)용 기기 정책

업무 프로필이 있는 완전 관리형 기기(COPE 기기)의 경우, 일부 기기 정책을 사용하여 전체 기기와 업무 프로필에 별도의 설정을 적용할 수 있습니다. 다른 기기 정책을 사용하여 전체 기기에만 또는 업무 프로필이 있는 완전 관리형 기기의 업무 프로필에만 설정을 적용할 수 있습니다.

정책	적용 대상
Android Enterprise 앱 권한	업무 프로필
관리형 구성	업무 프로필
앱 인벤토리	업무 프로필
앱 제거	업무 프로필
관리형 앱 자동 업데이트	업무 프로필
OS 업데이트 제어	해당 없음
자격 증명	업무 프로필
사용자 지정 XML	해당 없음
익스체인지	해당 없음
파일	업무 프로필
키가드 관리	장치 및 업무 프로필
키오스크	해당 없음
위치	장치 (위치 모드만 해당)
암호	장치 및 업무 프로필
제한	장치 및 업무 프로필 (장치 및 업무 프로필에 대한 별도의 정책 생성)
Samsung MDM 라이선스 키	해당 없음
예약	업무 프로필
와이파이	장치

정책	적용 대상
XenMobile 옵션	업무 프로필

다음도 참조하십시오. Android Enterprise용 지원되는 장치 정책 및 MDX 정책 및 MAM SDK 개요.

보안 작업

Android Enterprise는 다음 보안 작업을 지원합니다. 각 보안 작업에 대한 설명은 보안 작업을(를) 참조하십시오.

보안 작업	업무 프로필	완전 관리형
인증서 갱신	예	예
전체 초기화	아니요	예
찾기	예	예
잠금	예	예
잠금 및 암호 재설정	아니요	예
알림(벨 울림)	예	예
취소	예	예
선택적 초기화	예	아니요

보안 작업 참고 사항

- 위치 장치 정책이 장치의 위치 모드를 **높은 정확도** 또는 **배터리 절약**으로 설정하지 않으면 위치 보안 작업이 실패합니다. 위치 장치 정책을 참조하십시오.
- Android 9.0 이전 버전의 Android를 실행하는 작업 프로필 장치에서:
  - 잠금 및 암호 재설정 작업은 지원되지 않습니다.
- Android 9.0 이상이 설치된 작업 프로필 장치에서:
  - 전송된 암호는 작업 프로필을 잠급니다. 장치 자체는 잠기지 않습니다.
  - 작업 프로필에 암호가 설정되지 않은 경우:
    - 암호가 전송되지 않거나 전송된 암호가 암호 요구 사항을 충족하지 않는 경우: 장치가 잠깁니다.

    - 작업 프로필에 암호가 설정된 경우:
        - 암호가 전송되지 않거나 전송된 암호가 암호 요구 사항을 충족하지 않는 경우: 작업 프로필은 잠기지만 장치 자체는 잠기지 않습니다.
- 작업 프로필이 있는 완전 관리형 장치(COPE 장치)에서:
    - 잠금 보안 작업을 장치 또는 작업 프로필에 개별적으로 적용할 수 있습니다.

Android Enterprise 엔터프라이즈 등록 취소

더 이상 Android Enterprise 엔터프라이즈를 사용하지 않으려면 해당 엔터프라이즈의 등록을 취소할 수 있습니다.

> **경고:**
>
> 엔터프라이즈 등록을 취소하면 해당 엔터프라이즈를 통해 이미 등록된 장치의 Android Enterprise 앱이 기본 상태로 재설정됩니다. Google은 더 이상 장치를 관리하지 않습니다. 새 Android Enterprise 엔터프라이즈에 등록하는 경우, 관리형 Google Play에서 새 조직에 대한 앱을 승인해야 합니다. 그런 다음 XenMobile 콘솔에서 앱을 업데이트할 수 있습니다.

Android Enterprise 엔터프라이즈 등록이 취소된 후:

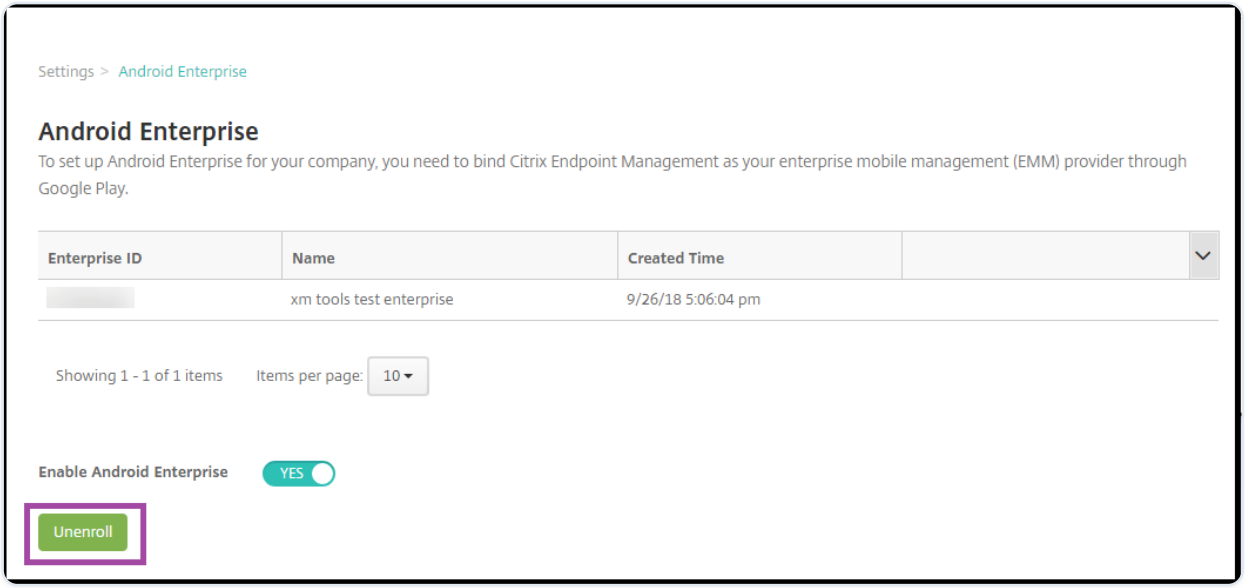
- 엔터프라이즈를 통해 등록된 장치 및 사용자는 Android Enterprise 앱이 기본 상태로 재설정됩니다. 이전에 적용된 관리형 구성 정책은 더 이상 작동에 영향을 미치지 않습니다.
- XenMobile은 엔터프라이즈를 통해 등록된 장치를 관리합니다. Google의 관점에서 보면 이러한 장치는 관리되지 않습니다. 새로운 Android Enterprise 앱을 추가할 수 없습니다. 관리형 구성 정책을 적용할 수 없습니다. 예약, 암호 및 제한과 같은 다른 정책은 이러한 장치에 적용할 수 있습니다.
- Android Enterprise에 장치를 등록하려고 하면 Android Enterprise 장치가 아닌 Android 장치로 등록됩니다.

XenMobile Server 콘솔 및 XenMobile Tools를 사용하여 Android Enterprise 엔터프라이즈 등록을 취소합니다.

이 작업을 수행하면 XenMobile Tools용 팝업 창이 열립니다. 시작하기 전에 XenMobile이 사용 중인 브라우저에서 팝업 창을 열 수 있는 권한이 있는지 확인하십시오. Google Chrome과 같은 일부 브라우저에서는 팝업 차단을 비활성화하고 XenMobile 사이트 주소를 팝업 차단 허용 목록에 추가해야 합니다.

Android Enterprise 엔터프라이즈 등록을 취소하려면:

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 설정 페이지에서 **Android Enterprise**를 클릭합니다.
3. **등록 취소**를 클릭합니다.



Android Enterprise 앱 배포

XenMobile®은 장치에 배포된 앱을 관리합니다. 다음 유형의 Android Enterprise 앱을 구성하고 배포할 수 있습니다.

- **관리형 앱 스토어 앱:** 이 앱에는 관리형 Google Play 스토어에서 사용할 수 있는 무료 앱이 포함됩니다. 예를 들어 GoToMeeting이 있습니다.
- **MDX:** MAM SDK로 준비되거나 MDX Toolkit으로 래핑된 앱입니다. 이 앱에는 MDX 정책이 포함됩니다. MDX 앱은 내부 소스 및 공용 스토어에서 가져옵니다. Citrix® 모바일 생산성 앱을 MDX 앱으로 배포합니다.
- **엔터프라이즈:** 개발하거나 다른 소스에서 얻은 개인 앱입니다. 관리형 Google Play 스토어를 통해 이러한 앱을 사용자에게 제공합니다. 관리형 Google Play 스토어는 Google 엔터프라이즈 앱 스토어입니다.
- **MDX 지원 개인 앱:** MAM SDK로 준비되거나 MDX Toolkit으로 래핑된 엔터프라이즈 앱입니다.

엔터프라이즈 앱과 MDX 지원 개인 앱을 두 가지 방법으로 추가할 수 있습니다.

- 이 문서의 Enterprise apps 및 MDX-enabled private apps 섹션에 설명된 대로 앱을 엔터프라이즈 앱으로 XenMobile 콘솔에 추가합니다.
- Google 개발자 계정을 사용하여 앱을 관리형 Google Play 스토어에 직접 게시합니다. 그런 다음 앱을 관리형 앱 스토어 앱으로 XenMobile 콘솔에 추가합니다. Managed app store apps를 참조하십시오.

Google 개발자 계정을 사용하여 앱을 게시한 다음 XenMobile 콘솔을 사용하는 것으로 전환하면 앱의 소유권이 달라집니다. 이 경우 두 위치에서 앱을 관리하십시오. Citrix는 한 가지 방법으로 앱을 추가하는 것을 권장합니다.

관리형 Google Play 스토어에서 자체 관리 앱을 제거해야 하는 경우 Google에 티켓을 여십시오. 개발자는 관리형 Google Play 스토어에서 앱을 비활성화할 수는 있지만 삭제할 수는 없습니다.

다음 섹션에서는 Android Enterprise 앱 구성에 대한 자세한 정보를 제공합니다. 앱 배포에 대한 자세한 내용은 Add Apps를 참조하십시오. 해당 문서에는 다음 내용이 포함됩니다.

- 웹 및 SaaS 앱 또는 웹 링크를 추가하기 위한 일반적인 워크플로
- 엔터프라이즈 및 공용 스토어 앱에 필요한 앱 워크플로
- Citrix Content Delivery Network (CDN) for Enterprise Apps에서 엔터프라이즈 앱을 제공하는 방법

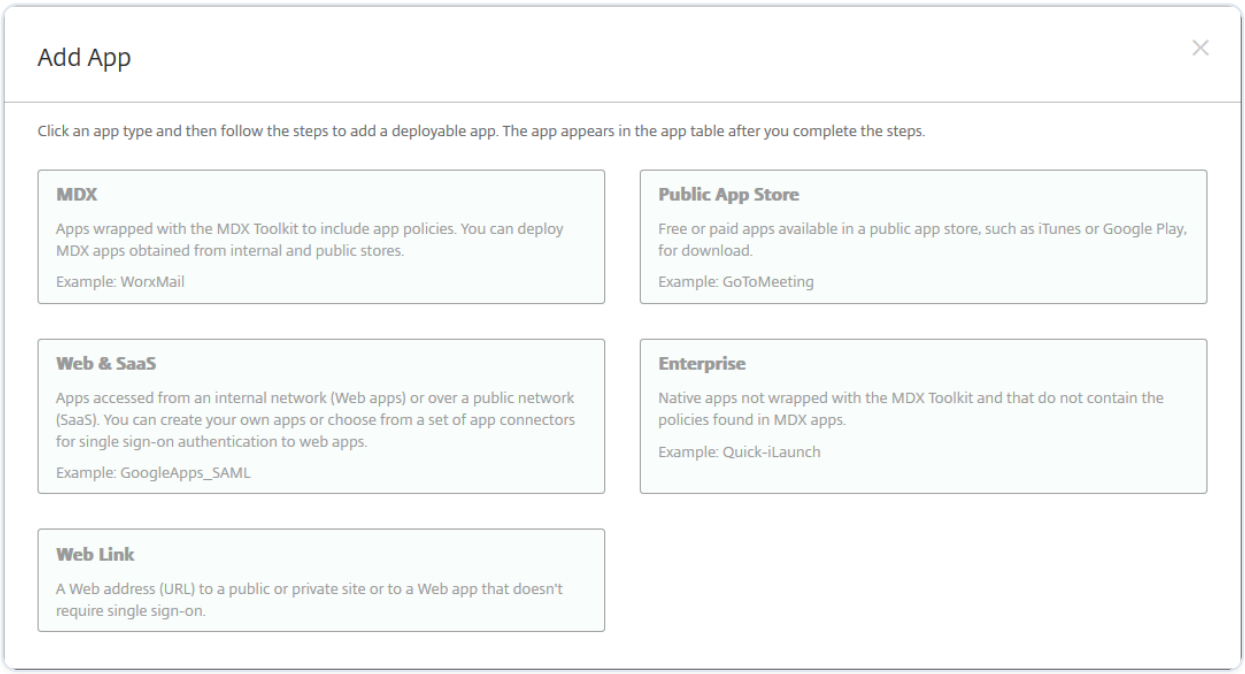
관리형 앱 스토어 앱

관리형 Google Play 스토어에서 사용할 수 있는 무료 앱을 XenMobile에 추가할 수 있습니다.

> **참고:**
>
> 관리형 Google Play에서 Google Play 스토어의 모든 앱에 액세스할 수 있도록 하려면 **Access all apps in the managed Google Play store** 서버 속성을 사용합니다. 서버 속성을 참조하십시오. 이 속성을 **true**로 설정하면 모든 Android Enterprise 사용자가 공개 Google Play 스토어 앱에 액세스할 수 있습니다. 그런 다음 제한 장치 정책을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다.

1단계: 앱 추가 및 구성

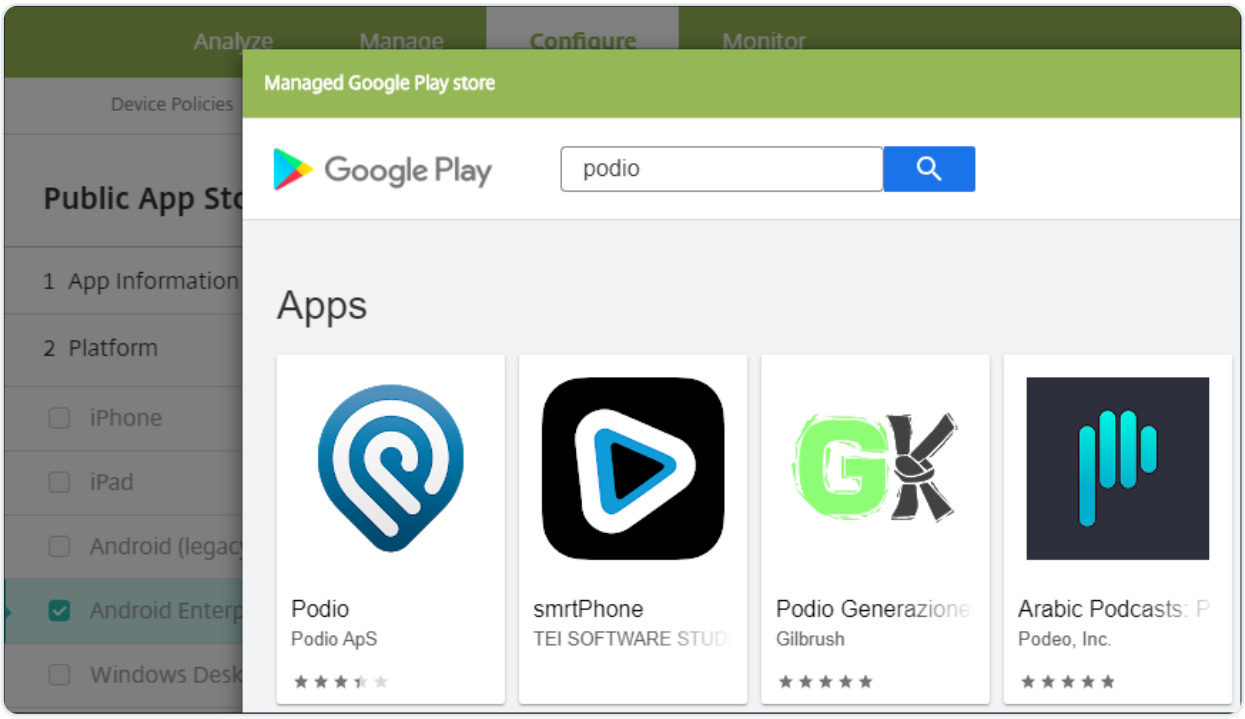
1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. **추가**를 클릭합니다.
2. **공개 앱 스토어**를 클릭합니다.



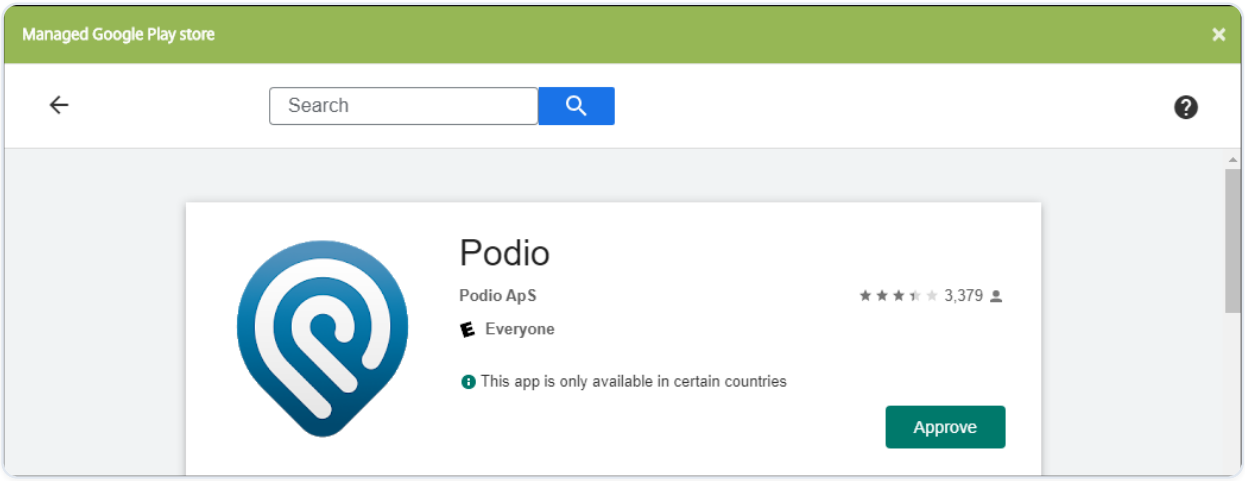
3. **앱 정보** 창에 다음 정보를 입력합니다.

   - **이름:** 앱에 대한 설명이 포함된 이름을 입력합니다. 이 이름은 **앱** 테이블의 **앱 이름** 아래에 나타납니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.
   - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

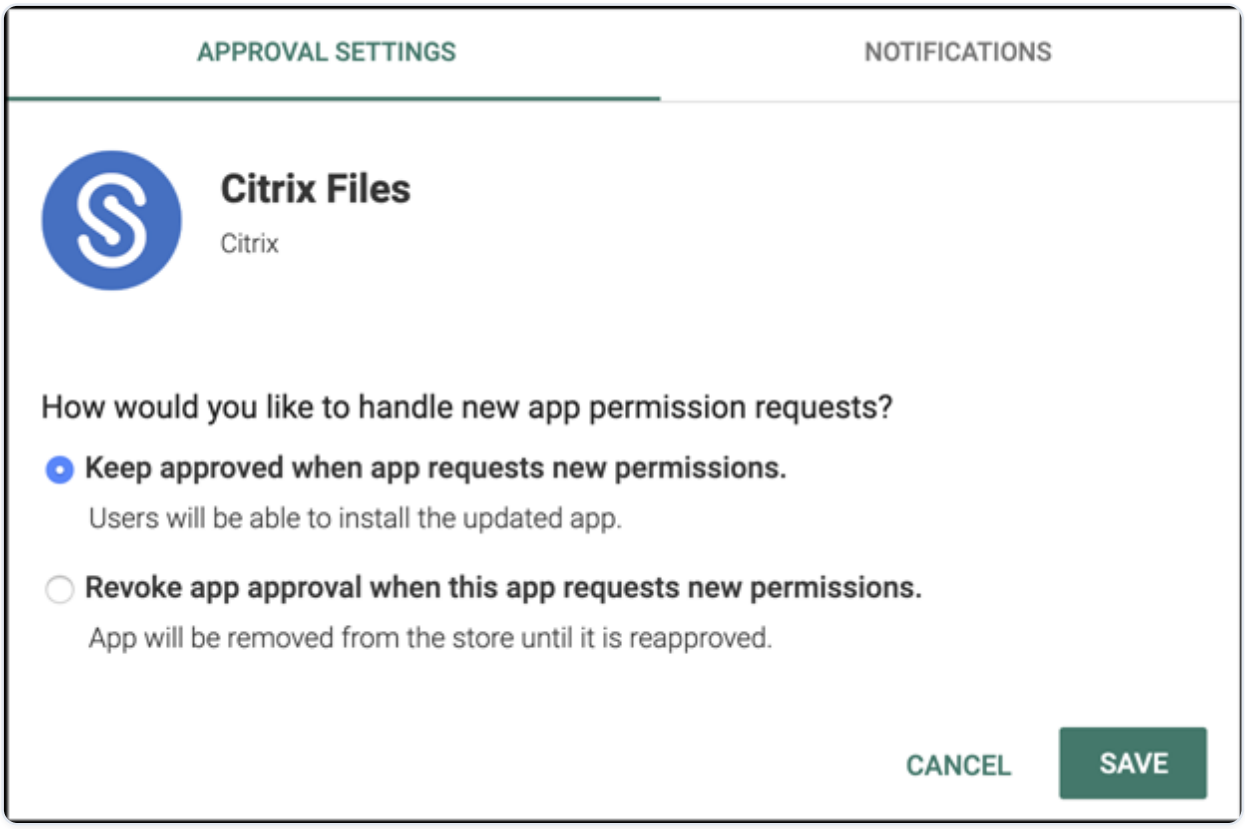
4. 플랫폼으로 **Android Enterprise**를 선택합니다.
5. 검색 상자에 앱 이름 또는 패키지 ID를 입력하고 **검색**을 클릭합니다. Google Play 스토어에서 패키지 ID를 찾을 수 있습니다. ID는 앱의 URL에 있습니다. 예를 들어, `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`에서 `com.Slack`이 패키지 ID입니다.



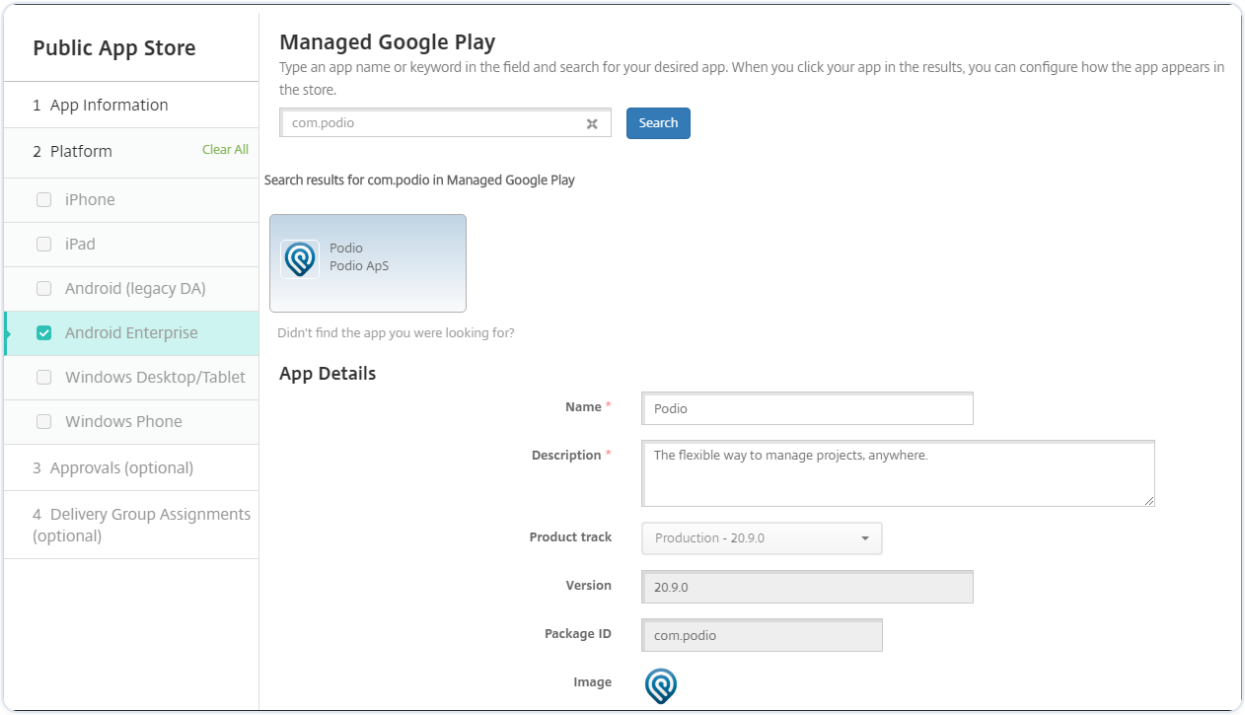
6. 검색 조건과 일치하는 앱이 나타납니다. 원하는 앱을 클릭한 다음 **승인**을 클릭합니다.



7. **승인**을 다시 클릭합니다.
8. **앱이 새 권한을 요청할 때 승인 유지**를 선택합니다. **저장**을 클릭합니다.



9. 앱 아이콘을 클릭하고 앱 **이름**과 **설명**을 구성합니다.

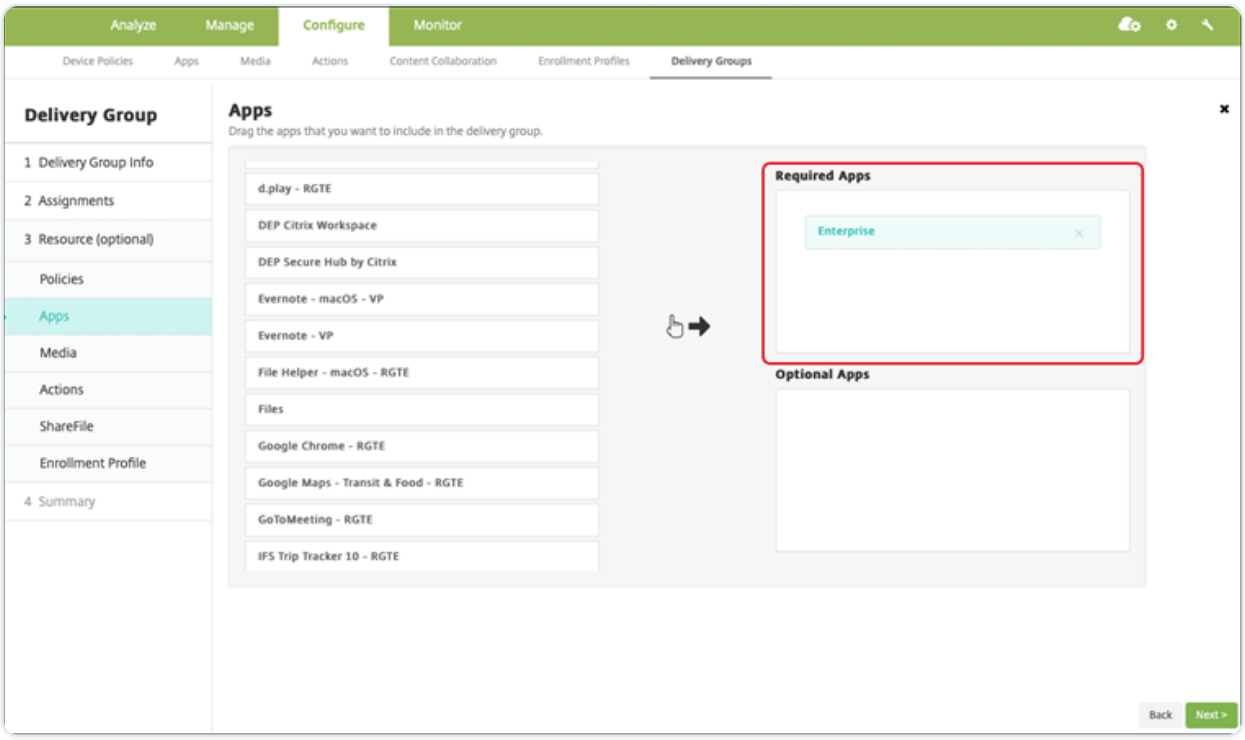


10. 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다. 자세한 내용은 리소스 배포를 참조하십시오.

2단계: 앱 배포 구성

1. **구성 > 배달 그룹**으로 이동하여 구성한 배달 그룹을 선택합니다. **편집**을 클릭합니다.

2. **앱** 섹션에서 원하는 앱을 **필수 앱** 상자로 끌어다 놓습니다.



3. **요약** 페이지에서 **저장**을 클릭합니다.
4. **배달 그룹** 페이지에서 배달 그룹을 선택하고 **배포**를 클릭합니다.

MDX 앱

XenMobile에 MDX 파일을 추가하고 앱 세부 정보 및 정책 설정을 구성합니다. Android Enterprise용 Citrix 모바일 생산성 앱을 구성하려면 MDX 앱으로 추가합니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

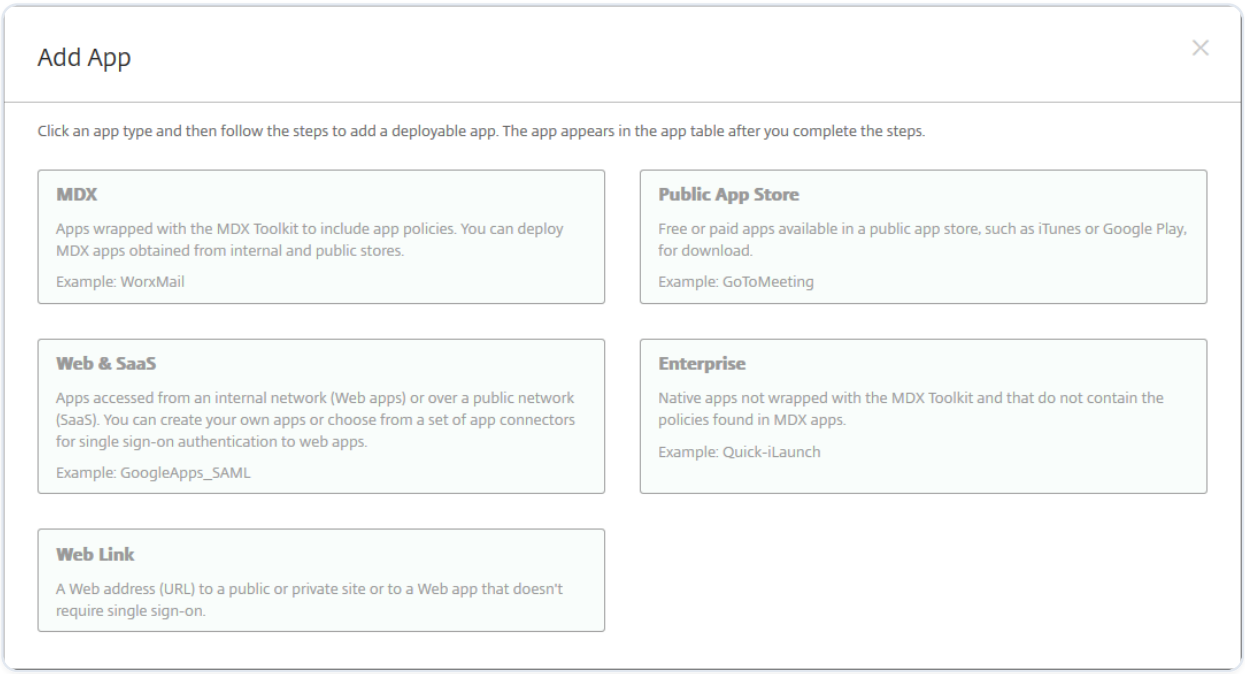
- MAM SDK 개요
- MDX 정책 한눈에 보기

1단계: 앱 추가 및 구성

1. Citrix 모바일 생산성 앱의 경우, 공용 스토어 MDX 파일을 다운로드합니다. `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**로 이동합니다.

   다른 유형의 MDX 앱의 경우, MDX 파일을 확보합니다.

2. XenMobile 콘솔에서 **구성 > 앱**을 클릭합니다. **추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.

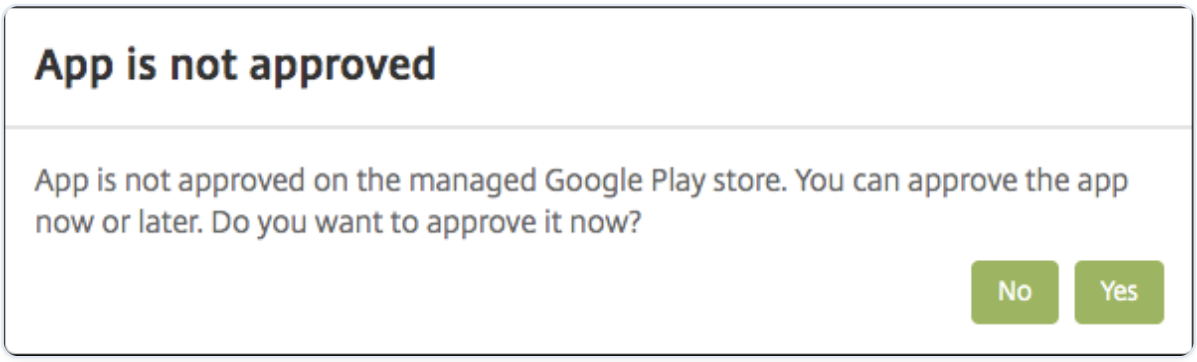


3. **MDX**를 클릭합니다. **MDX 앱 정보** 페이지가 나타납니다. **앱 정보** 창에 다음 정보를 입력합니다.

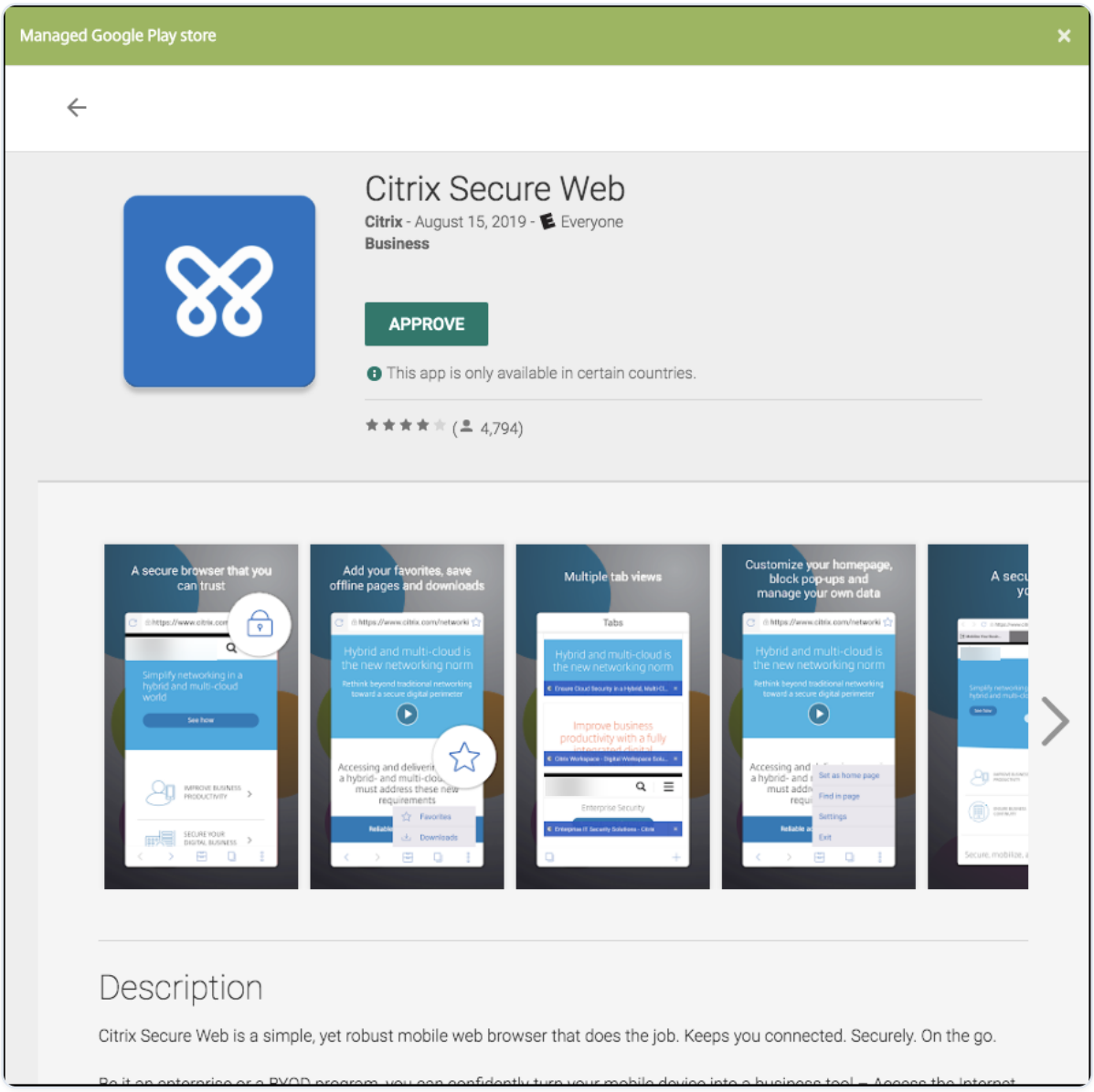
   - **이름:** 앱에 대한 설명적인 이름을 입력합니다. 이 이름은 **앱** 테이블의 **앱 이름** 아래에 나타납니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.
   - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

4. 플랫폼으로 **Android Enterprise**를 선택합니다.
5. **업로드**를 클릭하고 MDX 파일로 이동합니다. Android Enterprise는 MAM SDK 또는 MDX Toolkit으로 준비된 앱만 지원합니다.

   - 첨부된 애플리케이션이 관리형 Google Play 스토어의 승인을 필요로 하는 경우 UI에서 알려줍니다. XenMobile 콘솔을 벗어나지 않고 애플리케이션을 승인하려면 **예**를 클릭합니다.



   관리형 Google Play 스토어가 열리면 지침에 따라 앱을 승인하고 저장합니다.



앱을 성공적으로 추가하면 **앱 세부 정보** 페이지가 나타납니다.

6. 다음 설정을 구성합니다.

- **파일 이름:** 앱과 연결된 파일 이름을 입력합니다.
- **앱 설명:** 앱에 대한 설명을 입력합니다.
- **앱 버전:** 선택적으로 앱 버전 번호를 입력합니다.
- **패키지 ID:** 관리형 Google Play 스토어에서 얻은 앱의 패키지 ID를 입력합니다.
- **최소 OS 버전:** 선택적으로 장치가 앱을 실행하는 데 필요한 가장 오래된 운영 체제 버전을 입력합니다.
- **최대 OS 버전:** 선택적으로 장치가 앱을 실행하는 데 필요한 최신 운영 체제를 입력합니다.
- **제외된 장치:** 선택적으로 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

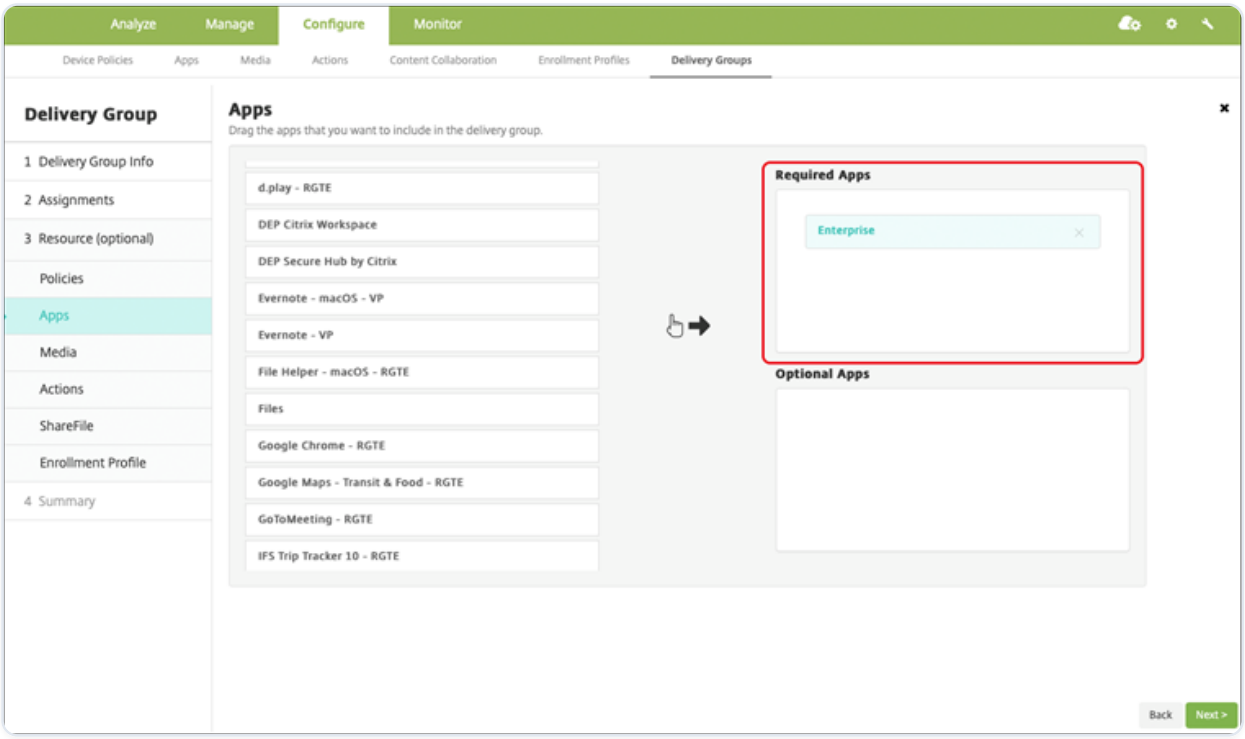
7. **MDX 정책**을 구성합니다. MDX 정책은 플랫폼에 따라 다르며 인증, 장치 보안 및 앱 제한을 포함한 정책 영역에 대한 옵션을 포함합니다. 콘솔에서 각 정책에는 정책을 설명하는 도구 설명이 있습니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

   - MAM SDK 개요
   - MDX 정책 한눈에 보기

8. 배포 규칙 및 스토어 구성을 구성합니다.
9. 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다. 자세한 내용은 리소스 배포를 참조하십시오.

2단계: 앱 배포 구성

1. **구성 > 배달 그룹**으로 이동하여 구성한 배달 그룹을 선택합니다. **편집**을 클릭합니다.
2. **앱** 섹션에서 원하는 앱을 **필수 앱** 상자로 끌어다 놓습니다.



3. **요약** 페이지에서 **저장**을 클릭합니다.
4. **배달 그룹** 페이지에서 배달 그룹을 선택하고 **배포**를 클릭합니다.

엔터프라이즈 앱

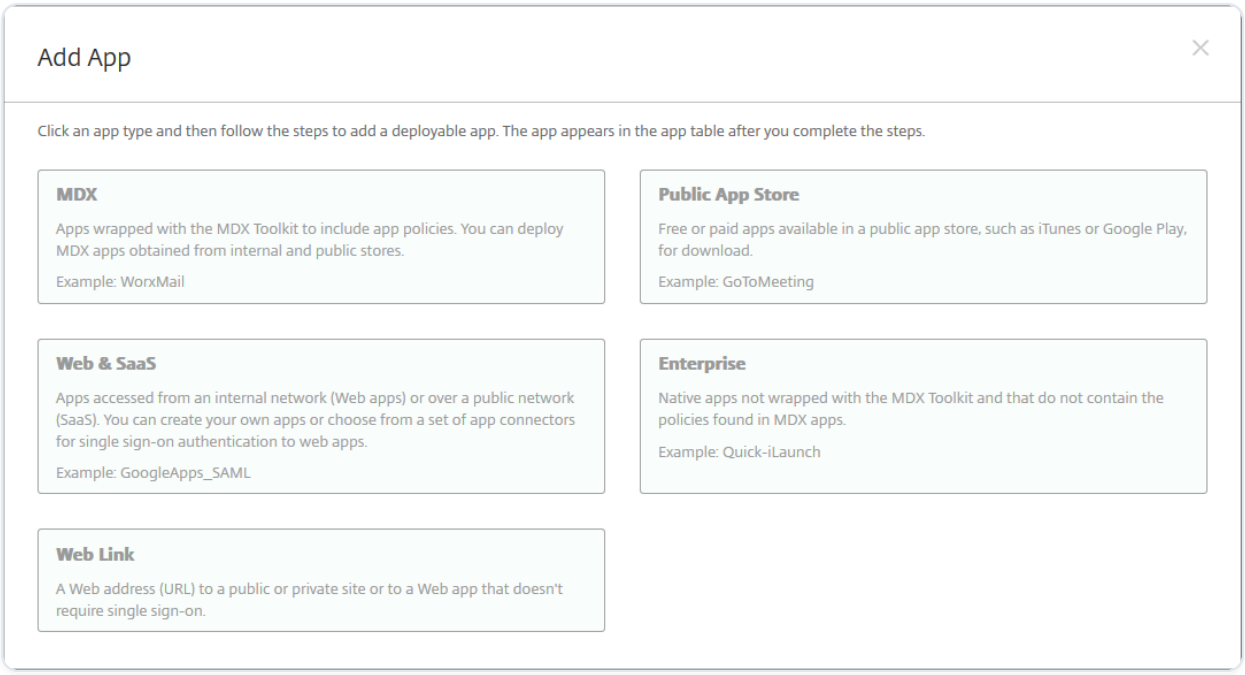
엔터프라이즈 앱은 MAM SDK 또는 MDX Toolkit으로 준비되지 않은 개인 앱을 나타냅니다. 이러한 앱은 직접 개발하거나 다른 소스에서 직접 가져옵니다. 엔터프라이즈 앱을 추가하려면 앱과 연결된 APK 파일이 필요합니다. Google의 개인 앱 모범 사례를 따르십시오.

1단계: 앱 추가 및 구성

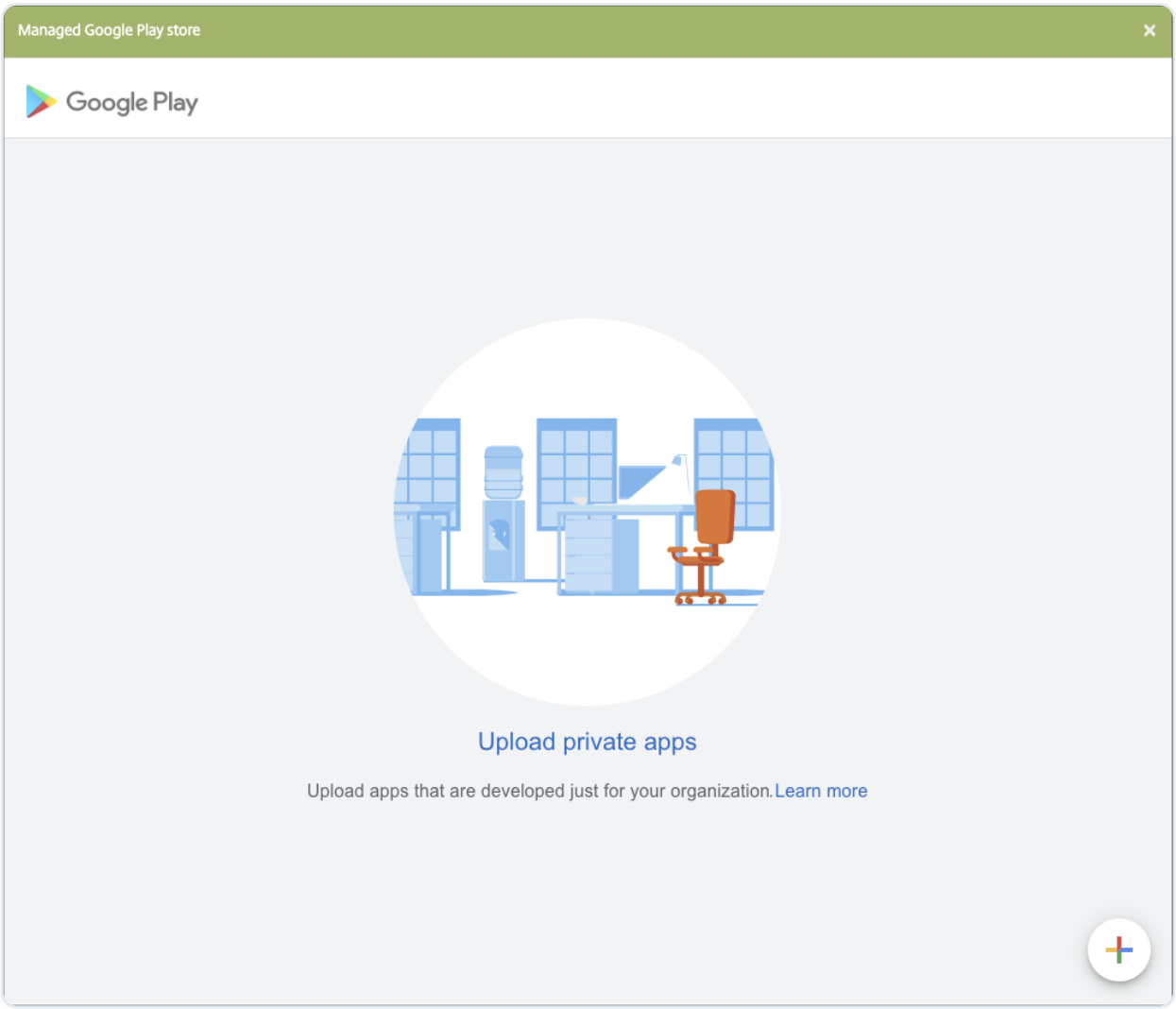
다음 두 가지 방법 중 하나로 앱을 추가합니다.

- 앱을 관리형 Google Play 스토어에 직접 게시하고 XenMobile 콘솔에 관리형 Play 스토어 앱으로 추가합니다. Google 문서에서 개인 앱 게시 방법을 따른 다음, 관리형 앱 스토어 앱 섹션의 단계를 따릅니다.
- 앱을 엔터프라이즈 앱으로 XenMobile 콘솔에 추가합니다. 다음 단계를 수행합니다.

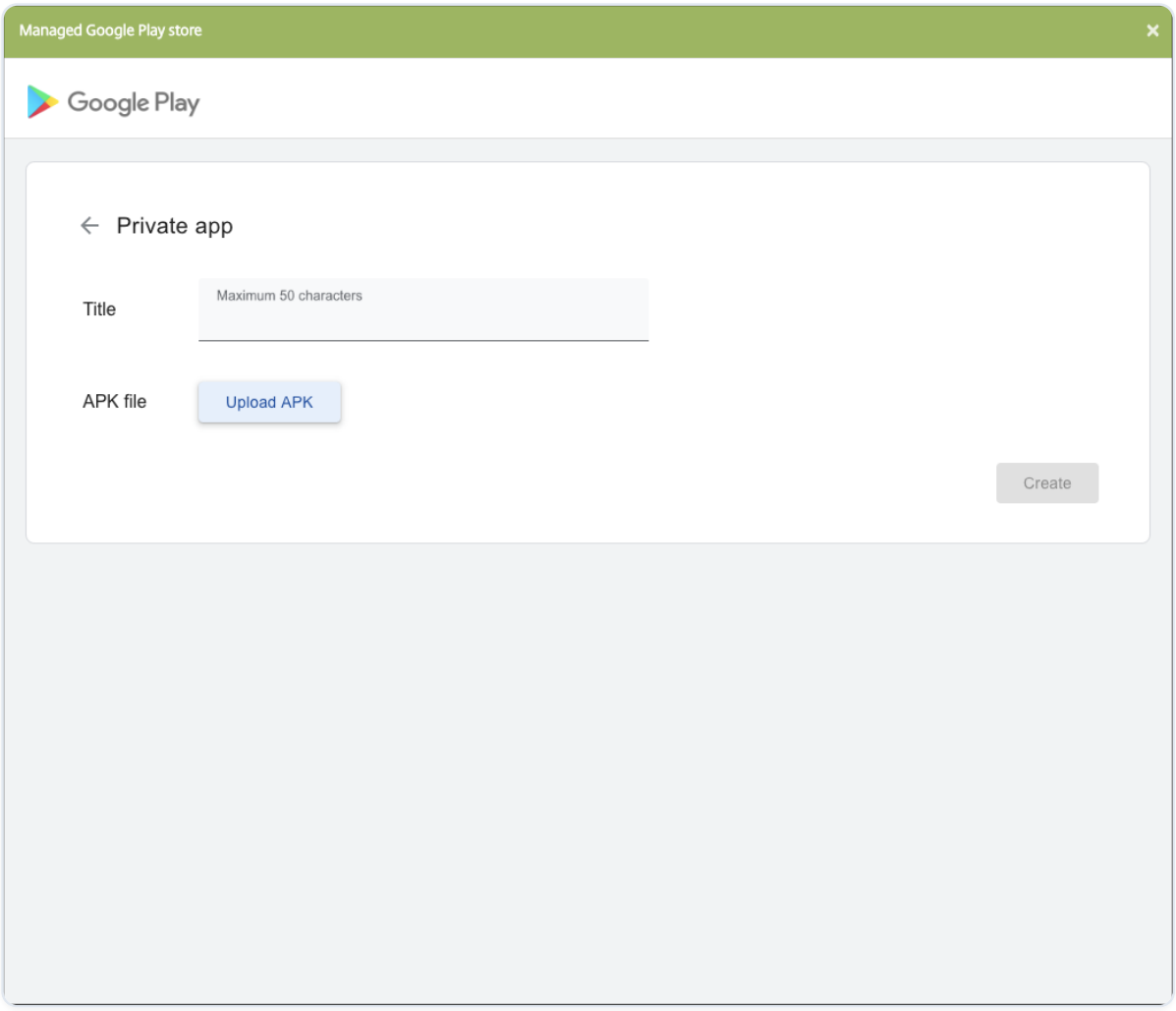
1. XenMobile 콘솔에서 **구성 > 앱**을 클릭합니다. **추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.



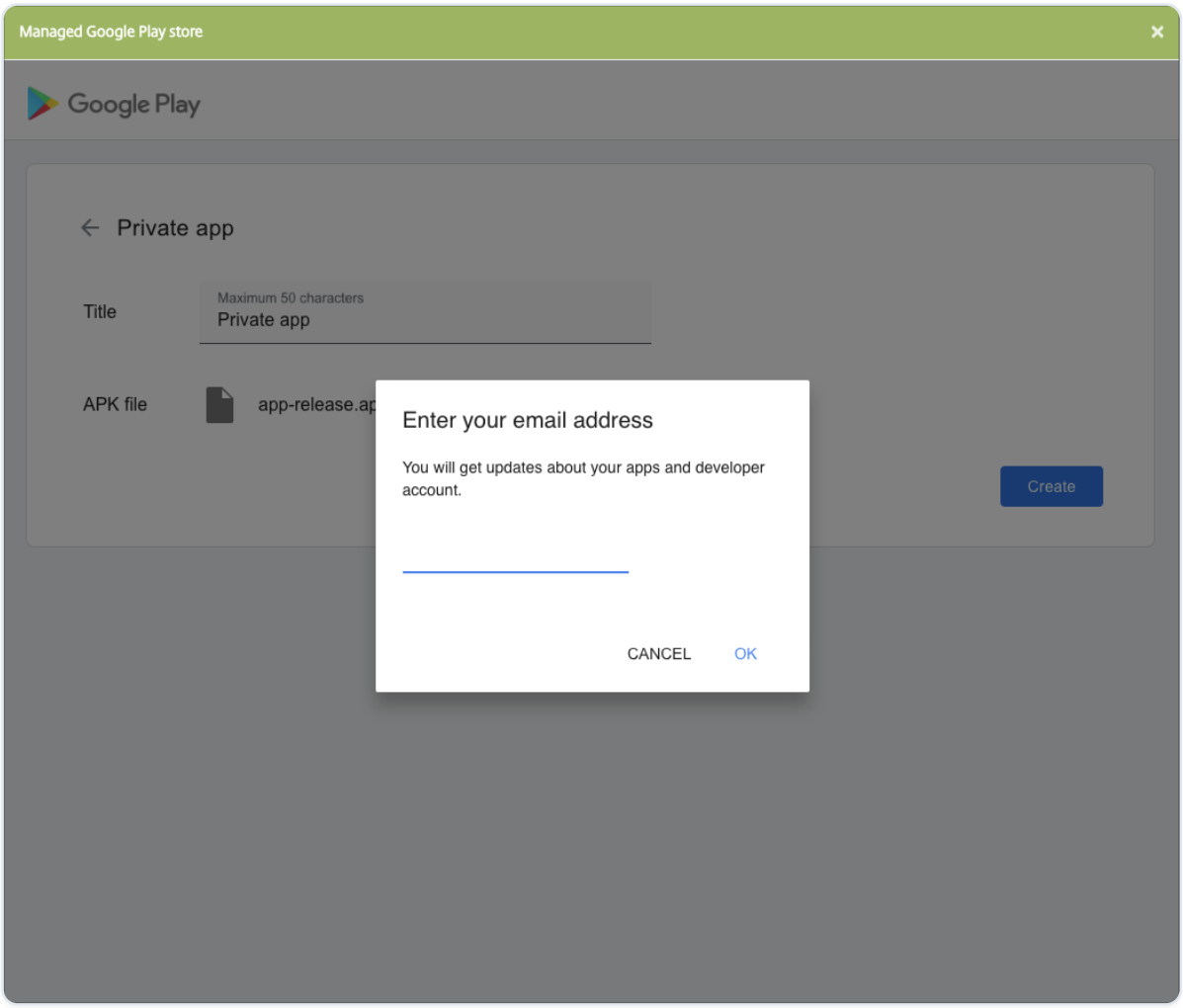
2. **Enterprise**를 클릭합니다. **앱 정보** 창에 다음 정보를 입력합니다.
   - **이름:** 앱에 대한 설명적인 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.
   - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.
3. 플랫폼으로 **Android Enterprise**를 선택합니다.
4. **업로드** 버튼을 클릭하면 관리형 Google Play 스토어가 열립니다. 비공개 앱을 게시하기 위해 개발자 계정을 등록할 필요는 없습니다. 계속하려면 오른쪽 하단 모서리에 있는 **더하기** 아이콘을 클릭합니다.



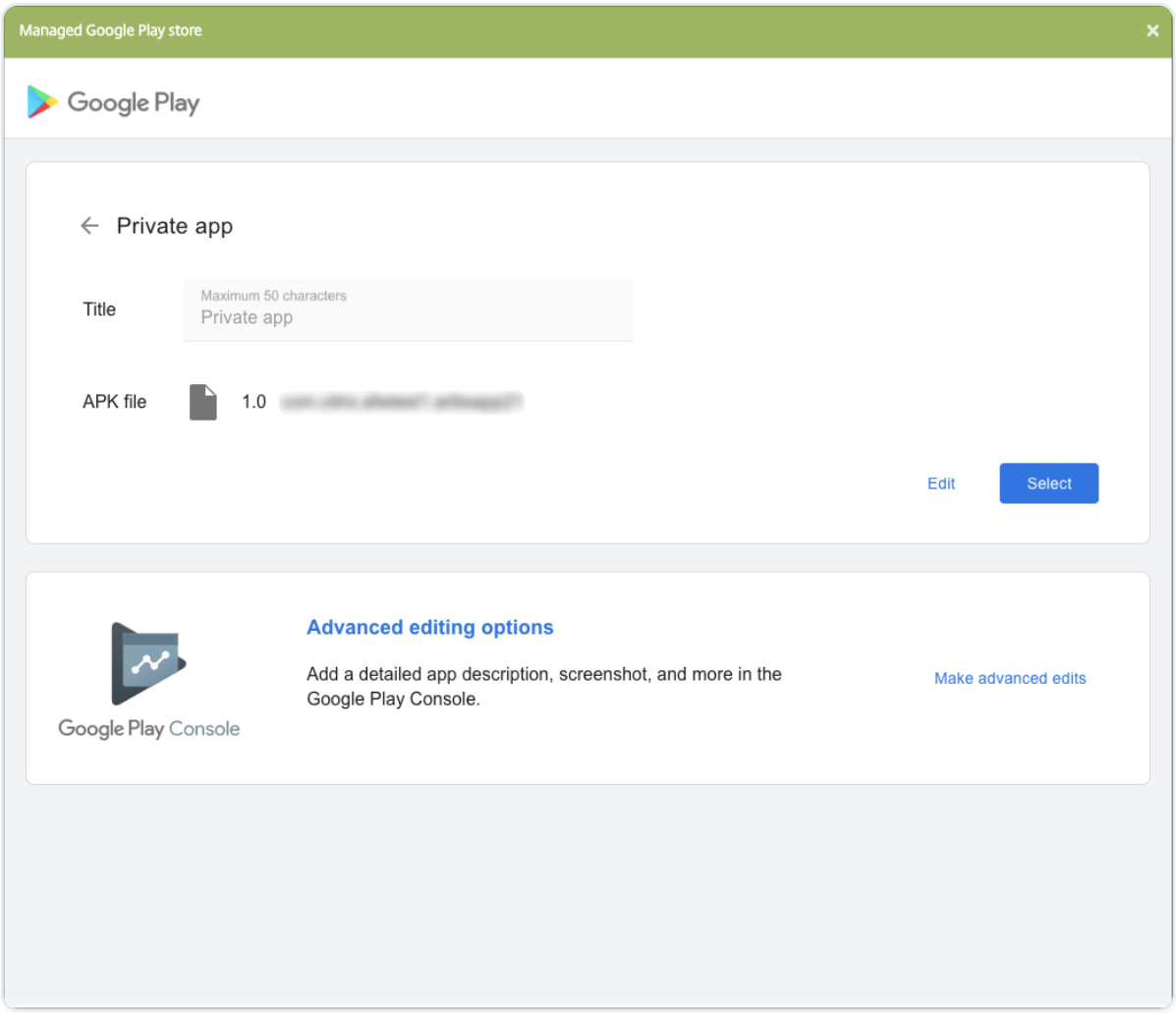
a. 앱 이름을 입력하고 .apk 파일을 업로드합니다. 완료되면 **만들기**를 클릭합니다. 비공개 앱이 게시되는 데 최대 10분이 걸릴 수 있습니다.



b. 앱 업데이트를 받으려면 이메일 주소를 입력합니다.



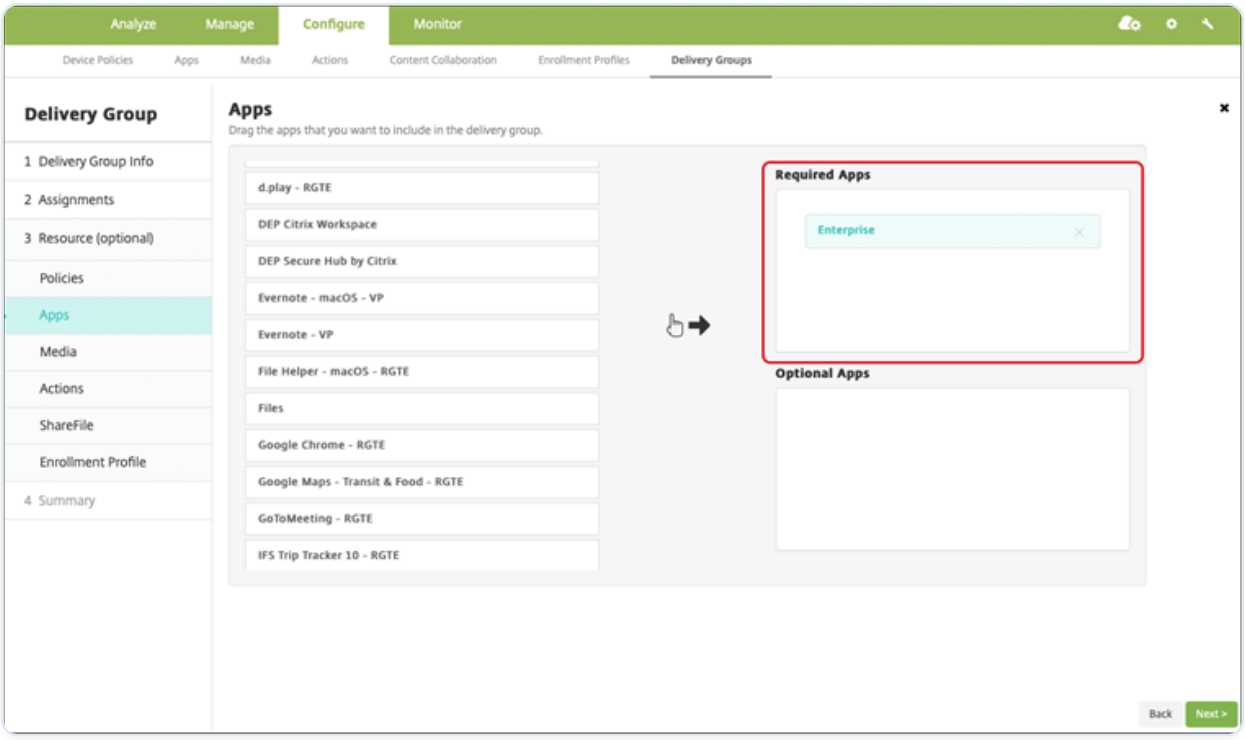
c. 애플리케이션이 게시되면 비공개 앱 아이콘을 클릭합니다. 앱 설명을 추가하거나 앱 아이콘을 변경하는 등의 작업을 수행하려면 **고급 편집**을 클릭합니다. 그렇지 않으면 **선택**을 클릭하여 앱 정보 페이지를 엽니다.



5. **다음**을 클릭합니다. 플랫폼에 대한 앱 정보 페이지가 나타납니다.
6. 다음과 같이 플랫폼 유형에 대한 설정을 구성합니다.
   - **파일 이름:** 선택적으로 앱의 새 이름을 입력합니다.
   - **앱 설명:** 선택적으로 앱의 새 설명을 입력합니다.
   - **앱 버전:** 이 필드는 변경할 수 없습니다.
   - **패키지 ID:** 앱의 고유 식별자입니다.
   - **최소 OS 버전:** 선택적으로 앱을 사용하기 위해 장치에서 실행할 수 있는 가장 오래된 운영 체제 버전을 입력합니다.
   - **최대 OS 버전:** 선택적으로 앱을 사용하기 위해 장치에서 실행해야 하는 최신 운영 체제를 입력합니다 .
   - **제외된 장치:** 선택적으로 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
7. 배포 규칙 및 스토어 구성을 구성합니다.
8. 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다. 자세한 내용은 리소스 배포를 참조하십시오.

2단계: 앱 배포 구성

1. **구성 > 배달 그룹**으로 이동하여 구성한 배달 그룹을 선택합니다. **편집**을 클릭합니다.
2. **앱** 섹션에서 원하는 앱을 **필수 앱** 상자로 끕니다.



3. **요약** 페이지에서 **저장**을 클릭합니다.
4. **배달 그룹** 페이지에서 배달 그룹을 선택하고 **배포**를 클릭합니다.

MDX 지원 개인 앱

Android Enterprise 앱을 MDX 지원 엔터프라이즈 앱으로 추가하려면 다음을 수행합니다.

1. 개인 Android Enterprise 앱을 생성하고 앱에 MDX를 활성화합니다.
2. XenMobile 콘솔에 앱을 추가합니다.
   - 관리형 Google Play 스토어에서 앱을 호스팅하고 게시합니다.
   - XenMobile 콘솔에 앱을 엔터프라이즈 앱으로 추가합니다.
3. MDX 파일을 XenMobile에 추가합니다.

Google Play 스토어를 통해 앱을 호스팅하고 게시하기로 결정한 경우 Google 인증서 서명에 동의하지 마십시오. 앱에 MDX를 활성화하는 데 사용된 것과 동일한 인증서로 앱에 서명합니다. 앱 게시에 대한 자세한 내용은 Google 문서의 앱 게시 및 앱 서명을 참조하십시오. MAM SDK는 앱을 래핑하지 않으므로 앱 개발에 사용된 인증서 외에 다른 인증서가 필요하지 않습니다.

Google Play Console을 통해 개인 앱을 게시하는 방법에 대한 자세한 내용은 Google 문서의 Play Console에서 개인 앱 게시를 참조하십시오.

XenMobile을 통해 앱을 게시하려면 다음 섹션을 참조하십시오.

개인 Android Enterprise 앱 준비

개인 Android Enterprise 앱을 생성할 때 Google의 개인 앱 모범 사례를 따르십시오.

개인 Android Enterprise 앱을 생성한 후 MAM SDK를 앱과 통합하거나 MDX Toolkit을 사용하여 앱을 래핑합니다. 그런 다음 결과 파일을 XenMobile에 추가합니다.

업데이트된 .apk 파일을 업로드하여 앱을 업데이트할 수 있습니다. 다음 단계에서는 MDX Toolkit을 사용한 앱 래핑에 대해 설명합니다.

1. 개인 Android Enterprise 앱을 생성하고 서명된 .apk 파일을 생성합니다.
2. 다음 샘플 파일에는 알려진 모든 정책이 포함되어 있으며, 그 중 일부는 사용자 환경에 적용되지 않을 수 있습니다. 사용할 수 없는 설정은 무시됩니다. 다음 매개변수를 사용하여 XML 파일을 생성합니다.

```
<?xml version="1.0" encoding="UTF-8"?>

<MobileAppPolicies>

    <PolicySchemaVersion>

        1.0

    </PolicySchemaVersion>

    <Policies>

        <DevicePasscode>false</DevicePasscode>

        <AppPasscode>false</AppPasscode>

        <MaxOfflinePeriod>72</MaxOfflinePeriod>

        <StepupAuthAddress/>

        <RequireUserEntropy>false</RequireUserEntropy>

        <BlockRootedDevices>true</BlockRootedDevices>
```

```
        <BlockDebuggerAccess>false</BlockDebuggerAccess>

        <RequireDeviceLock>false</RequireDeviceLock>

        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
NonCompliantDeviceBehavior>

        <WifiOnly>false</WifiOnly>

        <RequireInternalNetwork>false</RequireInternalNetwork>

        <InternalWifiNetworks/>

        <AllowedWifiNetworks/>

        <UpgradeGracePeriod>168</UpgradeGracePeriod>

        <WipeDataOnAppLock>false</WipeDataOnAppLock>

        <ActivePollPeriod>60</ActivePollPeriod>

        <PublicFileAccessLimitsList/>

        <CutAndCopy>Unrestricted</CutAndCopy>

        <Paste>Unrestricted</Paste>

        <DocumentExchange>Unrestricted</DocumentExchange>

        <OpenInExclusionList/>

        <InboundDocumentExchange>Unrestricted</InboundDocumentExchange>

        <InboundDocumentExchangeWhitelist/>

        <connectionSecurityLevel>TLS</connectionSecurityLevel>

        <DisableCamera>false</DisableCamera>

        <DisableGallery>false</DisableGallery>

        <DisableMicrophone>false</DisableMicrophone>
```

```
        <DisableLocation>false</DisableLocation>

        <DisableSms>false</DisableSms>

        <DisableScreenCapture>false</DisableScreenCapture>

        <DisableSensor>false</DisableSensor>

        <DisableNFC>false</DisableNFC>

        <BlockLogs>false</BlockLogs>

        <DisablePrinting>false</DisablePrinting>

        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
MvpnNetworkAccess>

        <MvpnSessionRequired>False</MvpnSessionRequired>

        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>

        <DisableLocalhostConnections>false</
DisableLocalhostConnections>

        <CertificateLabel/>

        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>

        <DefaultLoggerLevel>15</DefaultLoggerLevel>

        <MaxLogFiles>2</MaxLogFiles>

        <MaxLogFileSize>2</MaxLogFileSize>

        <RedirectSystemLogs>false</RedirectSystemLogs>

        <EncryptLogs>false</EncryptLogs>

        <GeofenceLongitude>0</GeofenceLongitude>

        <GeofenceLatitude>0</GeofenceLatitude>

        <GeofenceRadius>0</GeofenceRadius>
```

```
        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>

        <Authentication>OfflineAccessOnly</Authentication>

        <ReauthenticationPeriod>480</ReauthenticationPeriod>

        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>

    </Policies>

</MobileAppPolicies>
```

3. MDX Toolkit을 사용하여 앱을 래핑합니다. MDX Toolkit 사용에 대한 자세한 내용은 Android 모바일 앱 래핑을 참조하십시오.

   apptype 매개변수를 **Premium**으로 설정합니다. 다음 설명에 따라 이전 단계의 XML 파일을 사용합니다.

   앱의 스토어 URL을 알고 있다면 **storeURL** 매개변수를 해당 스토어 URL로 설정합니다. 앱을 게시한 후 사용자는 스토어 URL에서 앱을 다운로드합니다.

   다음은 SampleAEapp이라는 앱을 래핑하는 데 사용된 MDX Toolkit 명령의 예입니다.

```
```

 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en
-Duser.variant

 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap

 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk

 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx

 -MinPlatform 5.0

 -keystore /MyKeystore

 -storepass mystorepwd123

 -keyalias key0
```
```

```
 -keypass mykeypwd123

 -storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"

 -appType Premium

 -premiumMdxPolicies <Path to Premium policy XML>

```
```

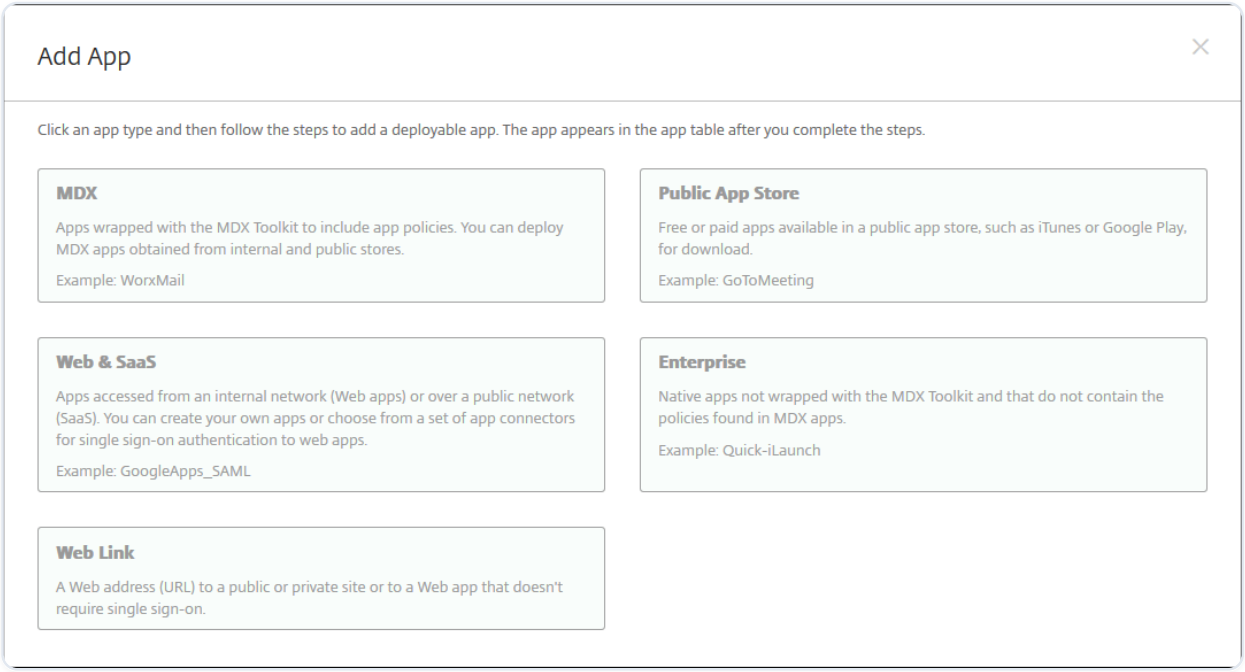
앱을 래핑하면 래핑된 .apk 파일과 .mdx 파일이 생성됩니다.

래핑된 .apk 파일 추가

다음 두 가지 방법 중 하나로 앱을 추가합니다.

- 앱을 관리형 Google Play 스토어에 직접 게시하고 XenMobile 콘솔에 관리형 Play 스토어 앱으로 추가합니다. 비공개 앱 게시 방법에 대한 Google 문서를 따른 다음, 관리형 앱 스토어 앱 섹션의 단계를 따릅니다.
- 앱을 XenMobile 콘솔에 엔터프라이즈 앱으로 추가합니다. 다음 단계를 수행합니다.

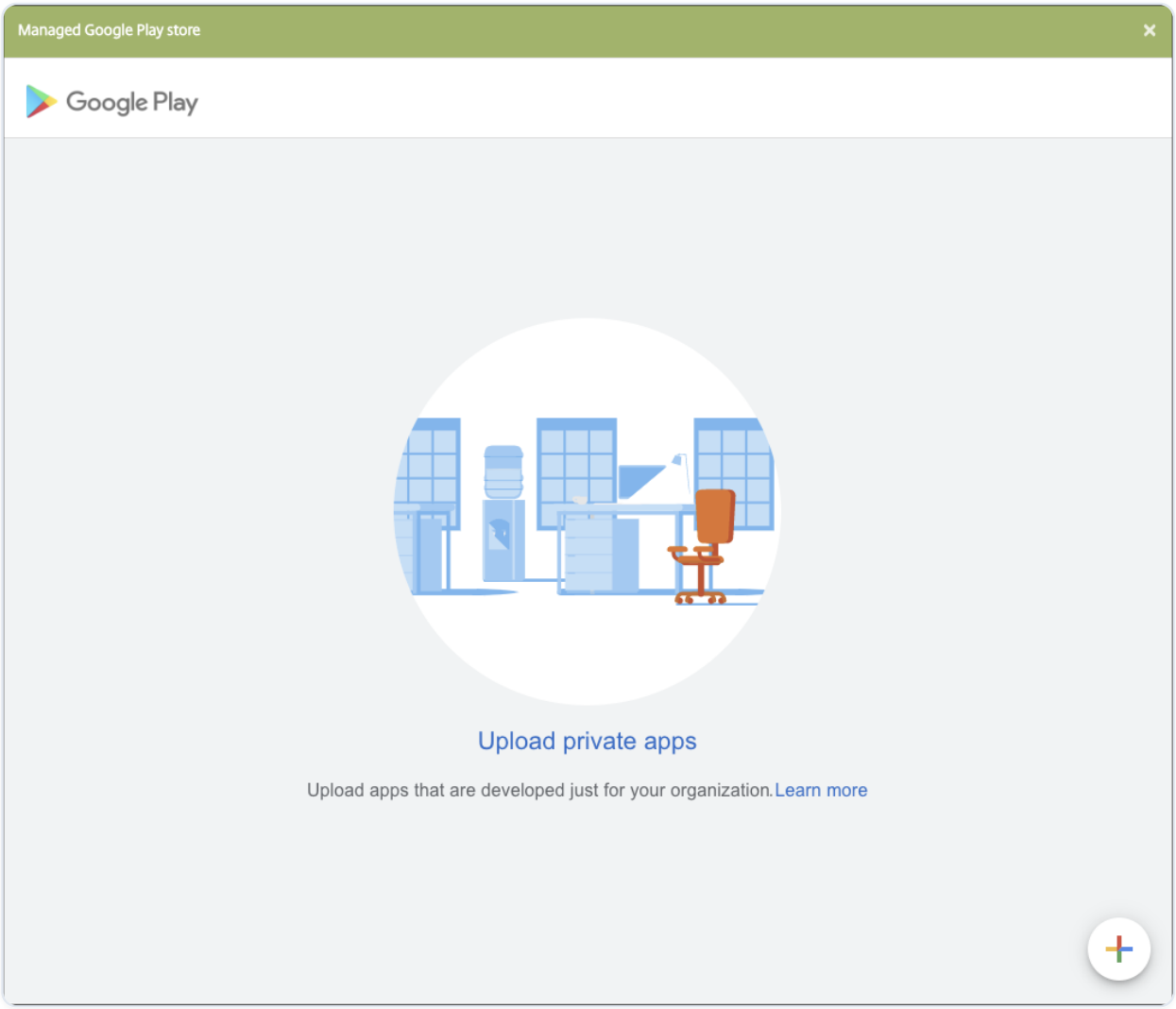
1. XenMobile 콘솔에서 **구성 > 앱**을 클릭합니다. **앱** 페이지가 열립니다.
2. **추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.



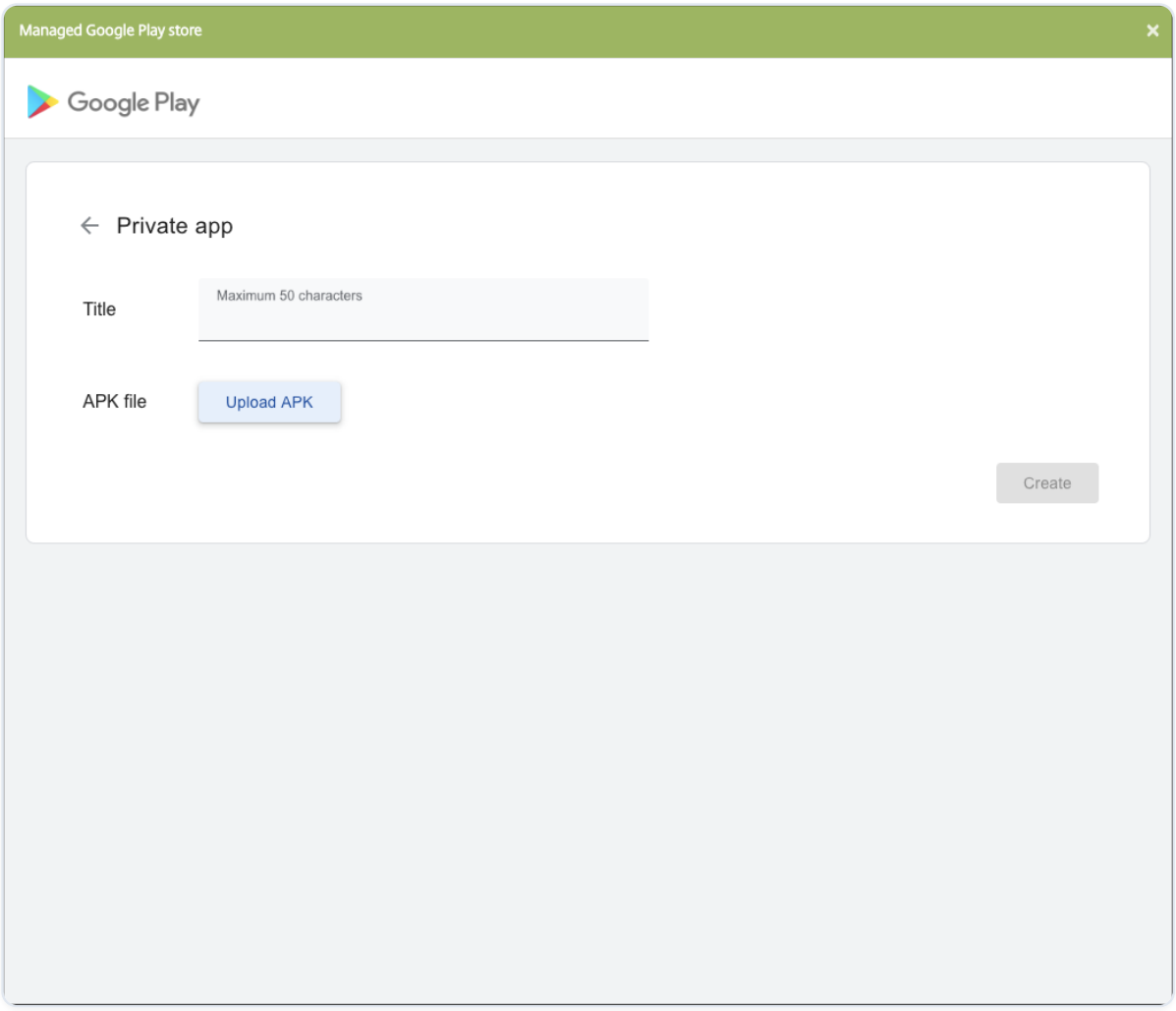
3. **엔터프라이즈**를 클릭합니다. **앱 정보** 창에 다음 정보를 입력합니다.
```

- **이름:** 앱에 대한 설명적인 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
- **설명:** 앱에 대한 선택적 설명을 입력합니다.
- **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

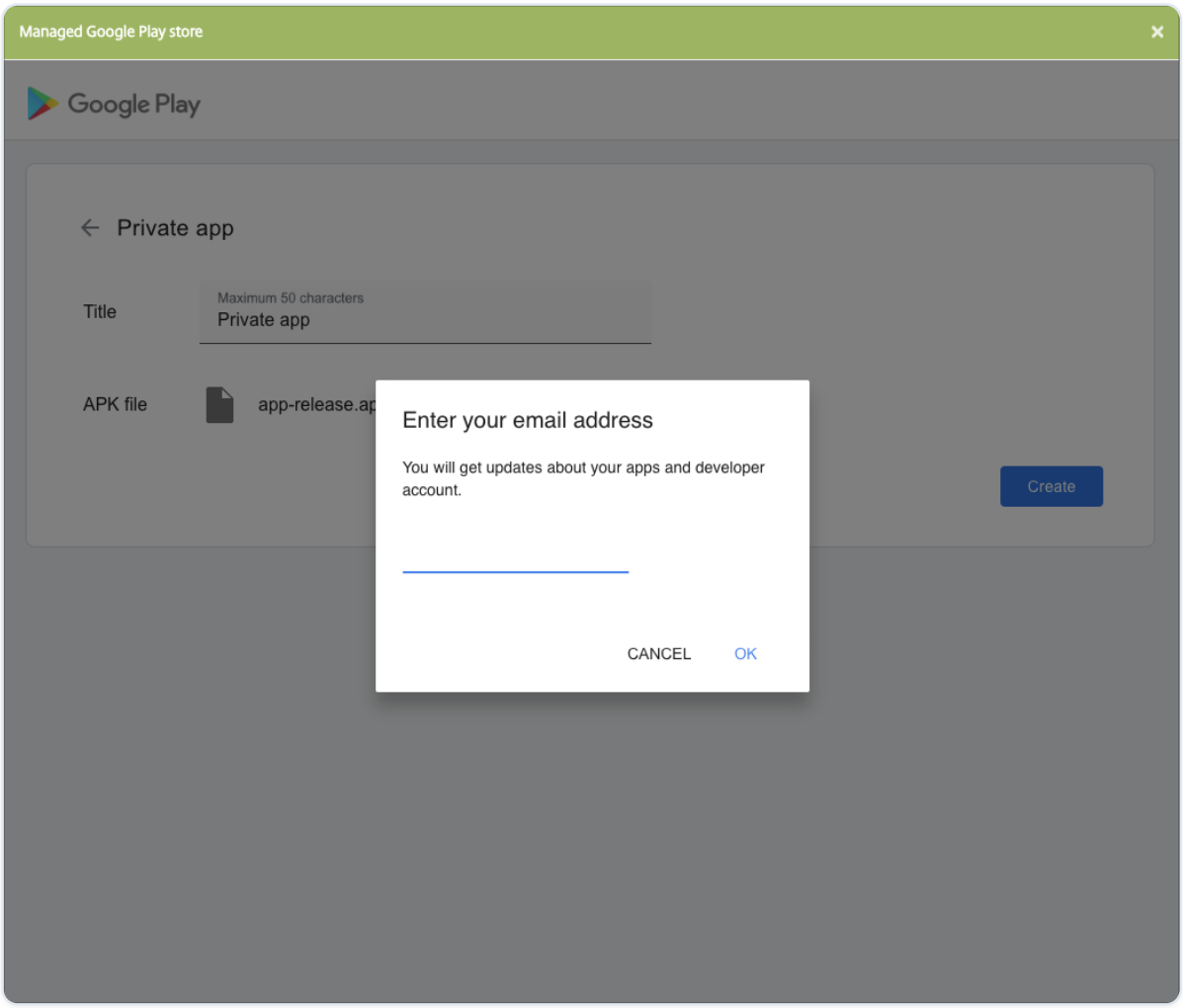
4. 플랫폼으로 **Android Enterprise**를 선택합니다.
5. **업로드** 버튼을 클릭하면 관리형 Google Play 스토어가 열립니다. 비공개 앱을 게시하기 위해 개발자 계정을 등록할 필요는 없습니다. 계속하려면 오른쪽 하단 모서리에 있는 **더하기** 아이콘을 클릭합니다.



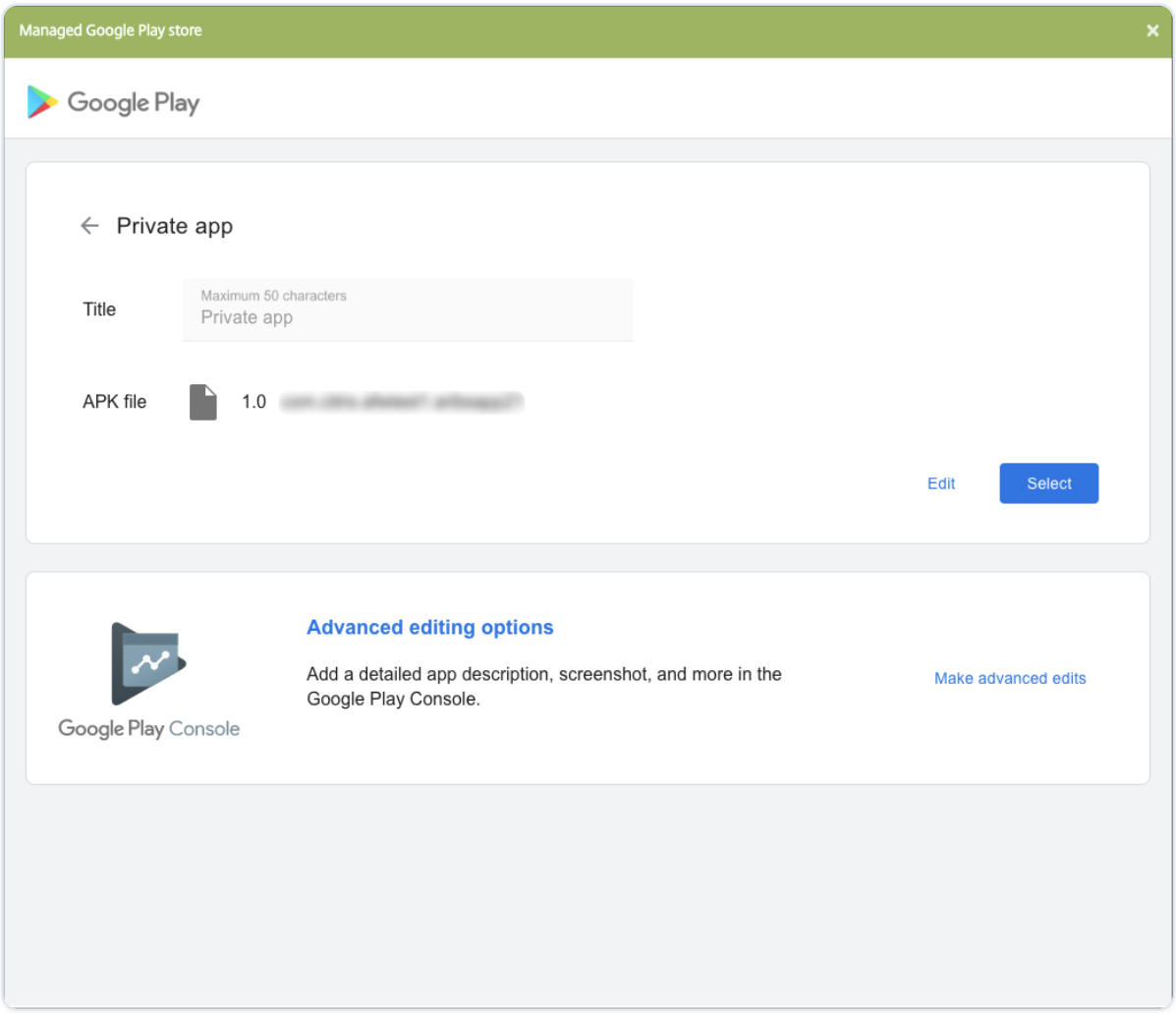
   a. 앱 이름을 입력하고 .apk 파일을 업로드합니다. 완료되면 **만들기**를 클릭합니다. 비공개 앱이 게시되는 데 최대 10분이 걸릴 수 있습니다.



b. 앱 업데이트를 받으려면 이메일 주소를 입력합니다.



c. 애플리케이션이 게시되면 비공개 앱 아이콘을 클릭하고 **선택**을 클릭하여 앱 정보 페이지를 엽니다.



6. **다음**을 클릭합니다. 플랫폼에 대한 앱 정보 페이지가 나타납니다.
7. 다음과 같이 플랫폼 유형에 대한 설정을 구성합니다.
   - **파일 이름:** 선택적으로 앱의 새 이름을 입력합니다.
   - **앱 설명:** 선택적으로 앱의 새 설명을 입력합니다.
   - **앱 버전:** 이 필드는 변경할 수 없습니다.
   - **패키지 ID:** 앱의 고유 식별자입니다.
   - **최소 OS 버전:** (선택 사항) 장치에서 앱을 실행하는 데 필요한 가장 오래된 운영 체제 버전을 입력합니다.
   - **최대 OS 버전:** (선택 사항) 장치에서 앱을 실행하는 데 필요한 최신 운영 체제 버전을 입력합니다.
   - **제외된 장치:** (선택 사항) 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
8. 배포 규칙 및 스토어 구성을 구성합니다.
9. **Android Enterprise 엔터프라이즈 앱** 페이지에서 **다음**을 클릭합니다. **승인** 페이지가 나타납니다.

워크플로를 사용하여 사용자가 앱에 액세스하기 전에 승인을 요구하려면 워크플로 적용을 참조하십시오. 승인 워크플로가 필요하지 않은 경우 13단계로 건너뛸 수 있습니다.

10. **다음**을 클릭합니다.
11. **전달 그룹 할당** 페이지가 나타납니다. 이 페이지에서는 아무 작업도 필요하지 않습니다. .mdx 파일을 추가할 때 이 앱에 대한 전달 그룹 및 배포 일정을 구성합니다. **저장**을 클릭합니다.

선택 사항: 스토어 URL 추가 또는 변경

앱을 래핑할 때 스토어 URL을 몰랐다면 지금 스토어 URL을 추가합니다.

1. 관리형 Google Play 스토어에서 앱을 봅니다. 앱을 선택하면 브라우저의 주소 표시줄에 스토어 URL이 나타납니다. URL 형식에서 앱의 패키지 이름을 복사합니다. 예를 들어: `https://play.google.com/store/apps/details?id=SampleAEappPackage`. 복사한 URL은 `https://play.google.com/work/`로 시작할 수 있습니다. `work`을 `store`로 변경해야 합니다.
2. MDX Toolkit을 사용하여 .mdx 파일에 스토어 URL을 추가합니다.

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \

setinfo \

-in ~/Desktop/SampleApps/Sample.mdx \

-out ~/Desktop/SampleApps/wrapped/Sample.mdx \

-storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"
```

.mdx 파일 추가

1. XenMobile 콘솔에서 **구성 > 앱**을 클릭합니다. **추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.

   앱 구성 화면(/en-us/xenmobile/server/media/configure-apps-add.png)

2. **MDX**를 클릭합니다. **MDX 앱 정보** 페이지가 나타납니다. **앱 정보** 창에 다음 정보를 입력합니다.

   - **이름:** 앱에 대한 설명적인 이름을 입력합니다. 이 이름은 **앱** 테이블의 **앱 이름** 아래에 나타납니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.
   - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

3. 플랫폼으로 **Android Enterprise**를 선택합니다.

4. **업로드**를 클릭하고 MDX 파일로 이동합니다. Android Enterprise는 MDX Toolkit으로 래핑된 앱만 지원합니다.

    - 연결된 애플리케이션이 관리형 Google Play 스토어의 승인을 필요로 하는 경우 UI에서 알려줍니다. XenMobile 콘솔을 벗어나지 않고 애플리케이션을 승인하려면 **예**를 클릭합니다.

      MDX 앱 추가(/en-us/xenmobile/server/media/mdx-app-not-approved.png)

      관리형 Google Play 스토어가 열리면 지침에 따라 앱을 승인하고 저장합니다.

      MDX 앱 승인(/en-us/xenmobile/server/media/mdx-approve-app.png)

      앱을 성공적으로 추가하면 **앱 세부 정보** 페이지가 나타납니다.

5. 다음 설정을 구성합니다.

    - **파일 이름:** 앱과 연결된 파일 이름을 입력합니다.
    - **앱 설명:** 앱에 대한 설명을 입력합니다.
    - **앱 버전:** 선택적으로 앱 버전 번호를 입력합니다.
    - **패키지 ID:** 관리형 Google Play 스토어에서 얻은 앱의 패키지 ID를 입력합니다.
    - **최소 OS 버전:** 선택적으로 장치가 앱을 실행하는 데 필요한 가장 오래된 운영 체제 버전을 입력합니다.
    - **최대 OS 버전:** 선택적으로 장치가 앱을 실행하는 데 필요한 최신 운영 체제를 입력합니다.
    - **제외된 장치:** 선택적으로 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.

6. **MDX 정책**을 구성합니다. MDX 정책은 플랫폼에 따라 다르며 인증, 장치 보안 및 앱 제한을 포함한 정책 영역에 대한 옵션을 포함합니다. 콘솔에서 각 정책에는 정책을 설명하는 도구 설명이 있습니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

    - MAM SDK 개요
    - MDX 타사 앱 정책 요약

7. 배포 규칙 및 스토어 구성을 구성합니다.

    항상 연결 배포는 **설정 > 서버 속성**에서 백그라운드 배포 키 예약을 구성한 경우에 적용됩니다.

    항상 연결 옵션:

    - 버전 10.18.19 이상으로 Endpoint Management 사용을 시작한 Android Enterprise 고객에게는 제공되지 않습니다.

- 버전 10.18.19 이전에 Endpoint Management 사용을 시작한 Android Enterprise 고객에게는 권장되지 않습니다.

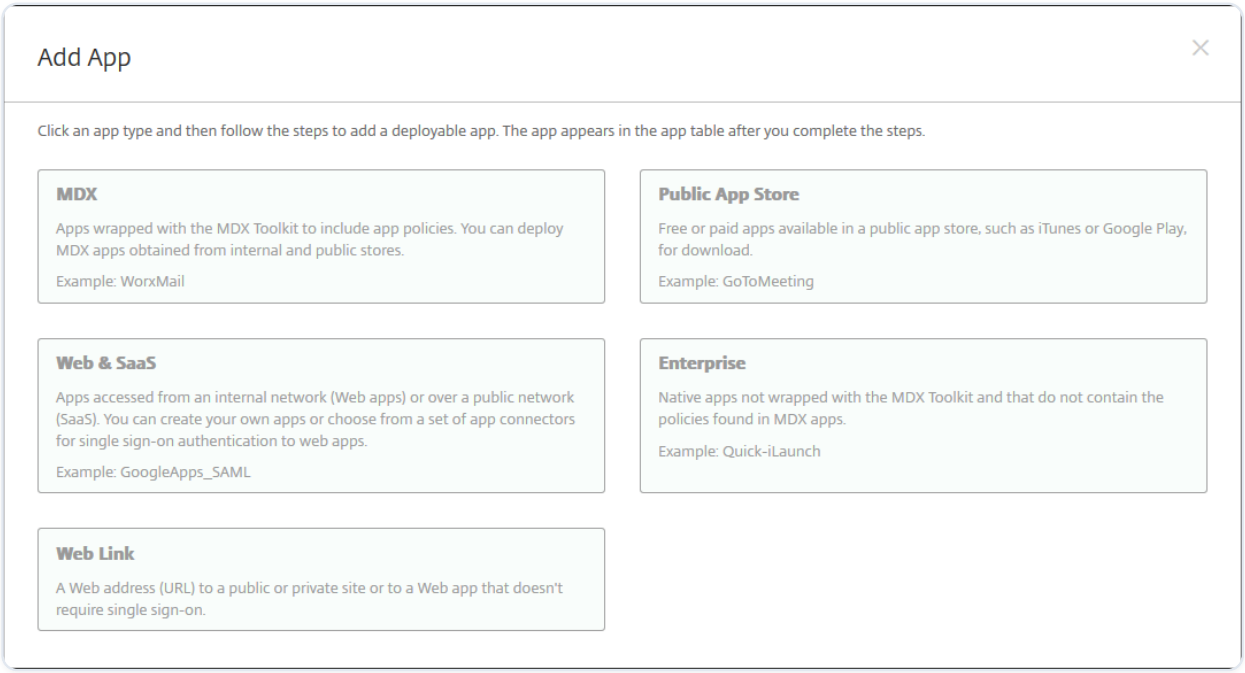
구성하는 배포 일정은 모든 플랫폼에서 동일합니다. **항상 연결 배포**를 제외하고 변경하는 모든 내용은 모든 플랫폼에 적용됩니다.

8. 앱에 딜리버리 그룹을 할당하고 **저장**을 클릭합니다. 자세한 내용은 리소스 배포를 참조하십시오.

앱 업데이트

Android Enterprise 앱을 업데이트하려면 업데이트된 .apk 파일을 래핑하고 업로드합니다.

1. MAM SDK 또는 MDX Toolkit을 사용하여 업데이트된 앱의 .apk 파일을 래핑합니다.
2. XenMobile 콘솔에서 **구성 > 앱**을 클릭합니다. **앱** 페이지가 열립니다.



3. **추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.
4. **Enterprise**를 클릭합니다. **앱 정보** 창에서 다음 정보를 입력합니다.

   - **이름:** 앱에 대한 설명적인 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.
   - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

5. 플랫폼으로 **Android Enterprise**를 선택합니다.
6. **다음**을 클릭합니다. **Android Enterprise Enterprise 앱** 페이지가 나타납니다.
7. **업로드**를 클릭합니다.

8. 관리형 Google Play 스토어 페이지에서 업데이트할 앱을 선택합니다.
9. 앱 정보 페이지에서 .apk 파일 이름 옆에 있는 **편집**을 클릭합니다.

   앱 편집(/en-us/xenmobile/server/media/publish-enterprise-app.png)
10. 새 .apk 파일로 이동하여 업로드합니다.
11. 관리형 Google Play 스토어 페이지에서 **저장**을 클릭합니다.

Google Workspace (이전 G Suite) 고객을 위한 레거시 Android Enterprise

Google Workspace (이전 G Suite) 고객은 레거시 Android Enterprise를 구성하려면 레거시 Android Enterprise 설정을 사용해야 합니다.

레거시 Android Enterprise 요구 사항:

- 공개적으로 액세스 가능한 도메인
- Google 관리자 계정
- 관리 프로필을 지원하고 Android 5.0+ Lollipop을 실행하는 장치
- Google Play가 설치된 Google 계정
- 장치에 설정된 작업 프로필

레거시 Android Enterprise 구성을 시작하려면 XenMobile® 설정의 **Android Enterprise** 페이지에서 **레거시 Android Enterprise**를 클릭합니다.

레거시 Android Enterprise 옵션 이미지(/en-us/xenmobile/server/media/android-for-work-legacy-1.png)

Android Enterprise 계정 생성

Android Enterprise 계정을 설정하기 전에 Google을 통해 도메인 이름을 확인해야 합니다.

Google을 통해 도메인 이름을 이미 확인했다면 이 단계를 건너뛸 수 있습니다: Android Enterprise 서비스 계정을 설정하고 Android Enterprise 인증서 다운로드.

1. `<https://gsuite.google.com/signup/basic/welcome>`으로 이동합니다.

   다음 페이지에 관리자 및 회사 정보를 입력하는 곳이 표시됩니다.

   계정 설정 페이지 이미지(/en-us/xenmobile/server/media/afw-account-setup-redirect.png)
2. 관리자 사용자 정보를 입력합니다.

   관리자 사용자 정보 이미지(/en-us/xenmobile/server/media/afw-enter-admin-user-info.png)

3. 관리자 계정 정보 외에 회사 정보를 입력합니다.

   회사 정보 화면 이미지(/en-us/xenmobile/server/media/afw-enter-company-info.png)

   프로세스의 첫 번째 단계가 완료되었으며 다음 페이지가 표시됩니다.

   확인 페이지 이미지.(/en-us/xenmobile/server/media/afw-dns-verification-1.png)

도메인 소유권 확인

다음 방법 중 하나로 Google이 도메인을 확인하도록 허용합니다.

- 도메인 호스트 웹사이트에 TXT 또는 CNAME 레코드를 추가합니다.
- 도메인의 웹 서버에 HTML 파일을 업로드합니다.
- 홈페이지에 `<meta>` 태그를 추가합니다. Google은 첫 번째 방법을 권장합니다. 이 문서에서는 도메인 소유권을 확인하는 단계를 다루지 않지만, 필요한 정보는 여기에서 찾을 수 있습니다: https://support.google.com/a/answer/6248925.

1. 도메인 확인을 시작하려면 **시작**을 클릭합니다.

   도메인 소유권 확인 페이지가 나타납니다. 페이지의 지침에 따라 도메인을 확인합니다.

2. **확인**을 클릭합니다.

   확인 버튼 이미지(/en-us/xenmobile/server/media/afw-verify-domain-ownership.png)

   확인 메시지 이미지(/en-us/xenmobile/server/media/afw-domain-verified.png)

3. Google에서 도메인 소유권을 확인합니다.

   도메인 소유권 확인 이미지(/en-us/xenmobile/server/media/afw-google-verification.png)

4. 확인이 성공적으로 완료되면 다음 페이지가 나타납니다. **계속**을 클릭합니다.

   성공 확인 페이지 이미지(/en-us/xenmobile/server/media/afw-dns-verification-9.png)

5. Google에서 Citrix®에 제공하고 Android Enterprise 설정을 구성할 때 사용하는 EMM 바인딩 토큰을 생성합니다. 토큰을 복사하여 저장합니다. 이 토큰은 나중에 설정 절차에서 필요합니다.

   바인딩 토큰 이미지(/en-us/xenmobile/server/media/afw-obtain-token.png)

6. **마침**을 클릭하여 Android Enterprise 설정을 완료합니다. 도메인이 성공적으로 확인되었음을 나타내는 페이지가 나타납니다.

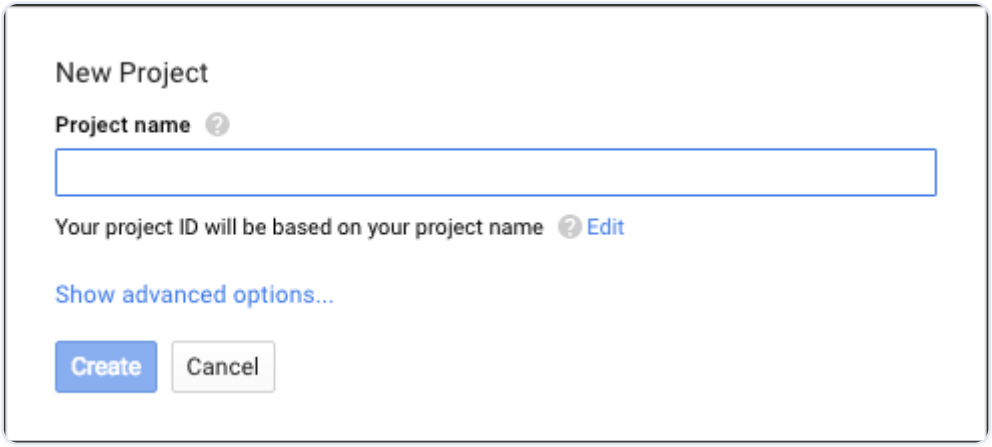
Android Enterprise 서비스 계정을 생성한 후 Google 관리 콘솔에 로그인하여 모빌리티 관리 설정을 관리할 수 있습니다.

Android Enterprise 서비스 계정 설정 및 Android Enterprise 인증서 다운로드

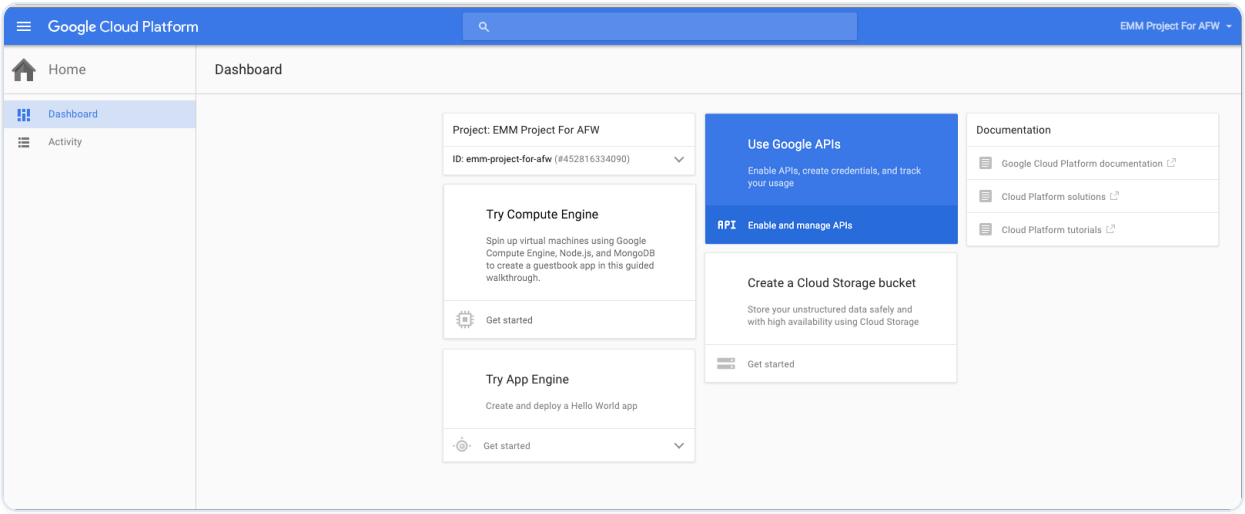
XenMobile이 Google Play 및 디렉터리 서비스에 연결할 수 있도록 하려면 개발자용 Google Project 포털을 사용하여 서비스 계정을 생성해야 합니다. 이 서비스 계정은 Android용 XenMobile과 Google 서비스 간의 서버-서버 통신에 사용됩니다. 사용 중인 인증 프로토콜에 대한 자세한 내용은 `<https://developers.google.com/identity/protocols/OAuth2ServiceAccount>`을 참조하십시오.

1. 웹 브라우저에서 `<https://console.cloud.google.com/project>`으로 이동하여 Google 관리자 자격 증명으로 로그인합니다.
2. **프로젝트** 목록에서 **프로젝트 만들기**를 클릭합니다.

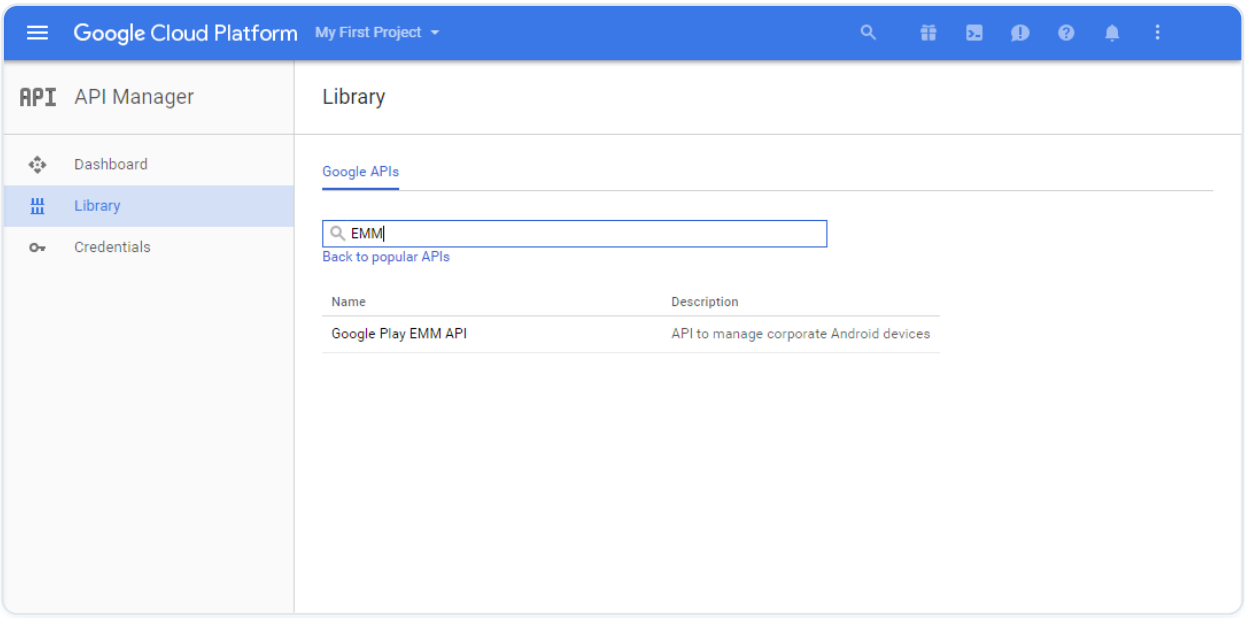
   프로젝트 만들기 옵션 이미지(/en-us/xenmobile/server/media/google-config-api-1.png)
3. **프로젝트 이름**에서 프로젝트 이름을 입력합니다.



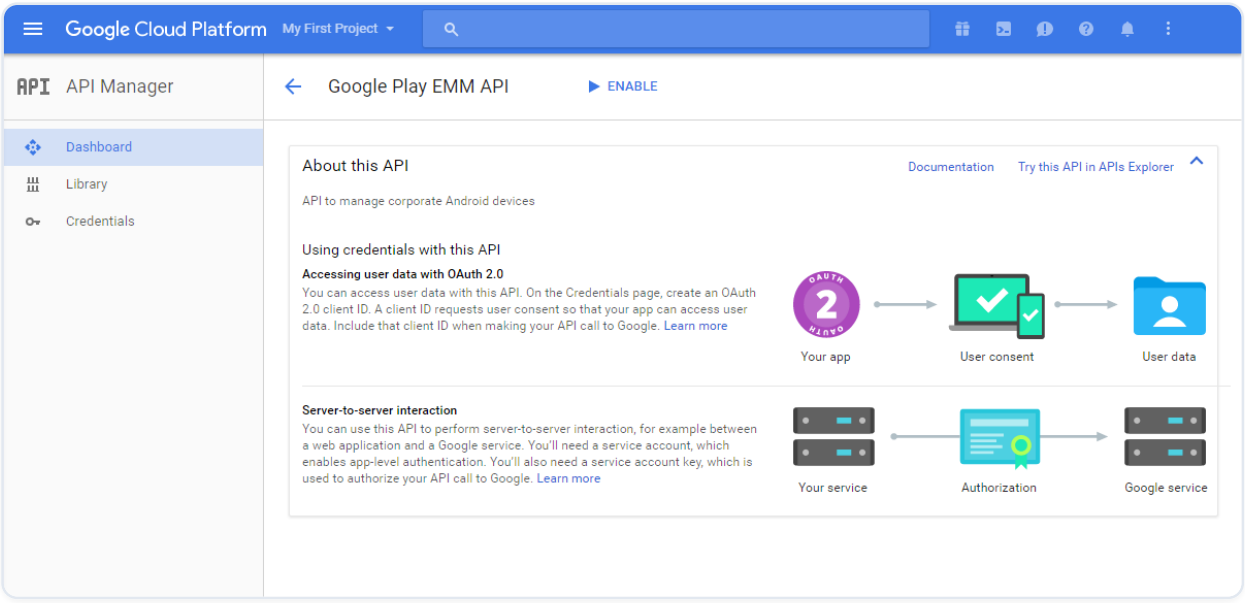
4. 대시보드에서 **Google API 사용**을 클릭합니다.



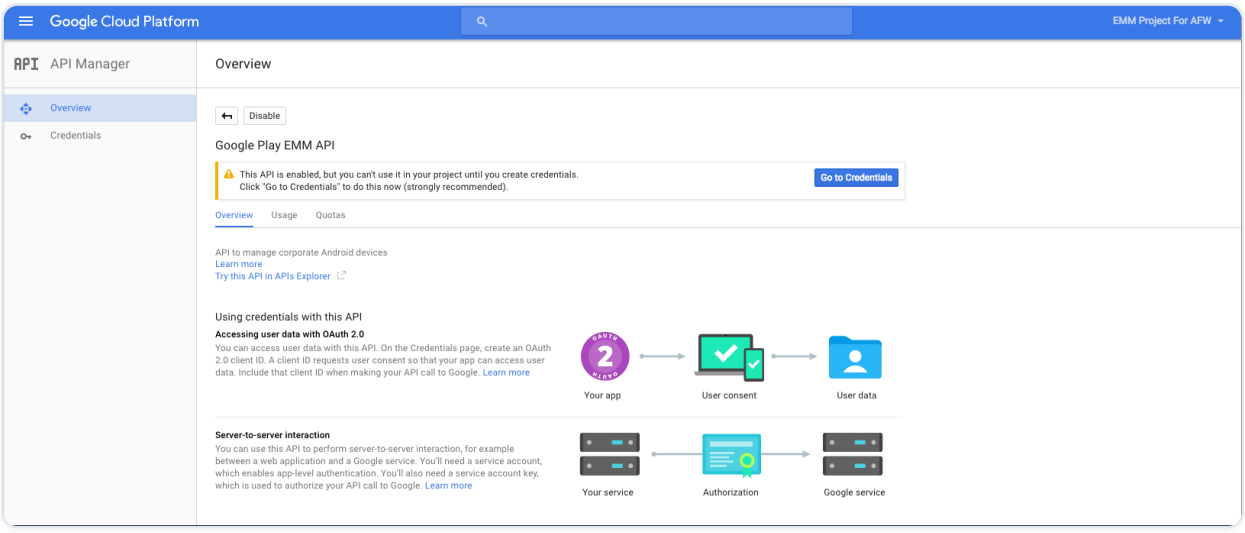
5. **라이브러리**를 클릭하고, **검색**에서 **EMM**을 입력한 다음 검색 결과를 클릭합니다.



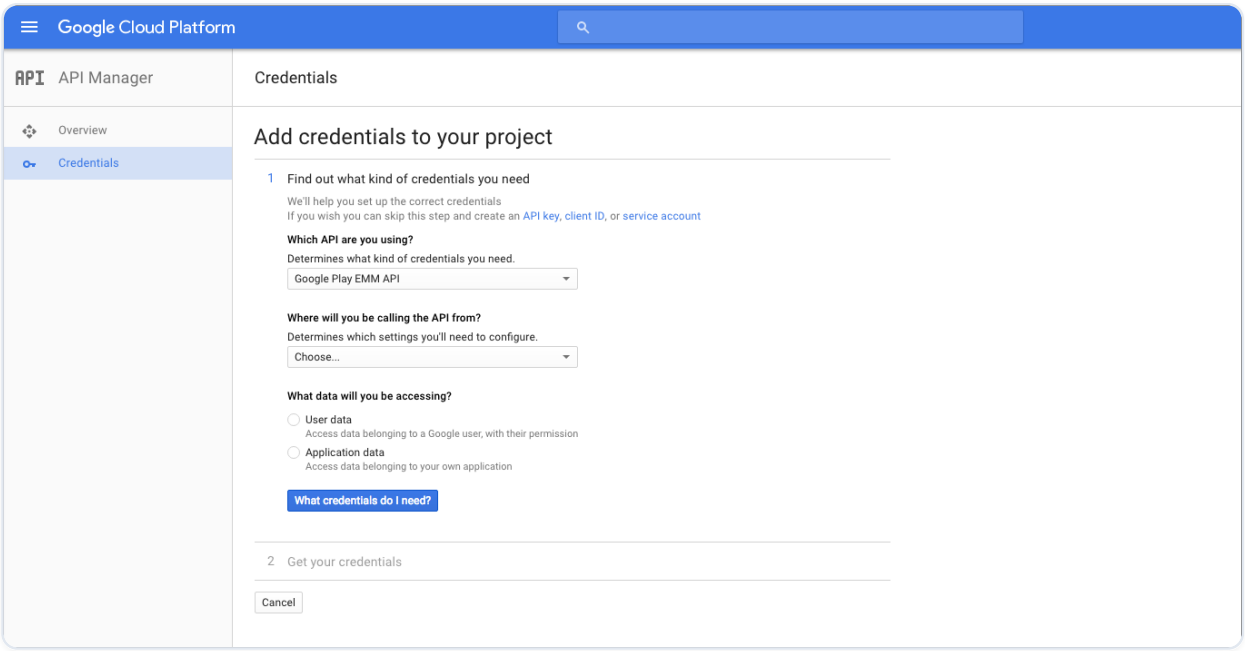
6. **개요** 페이지에서 **사용**을 클릭합니다.



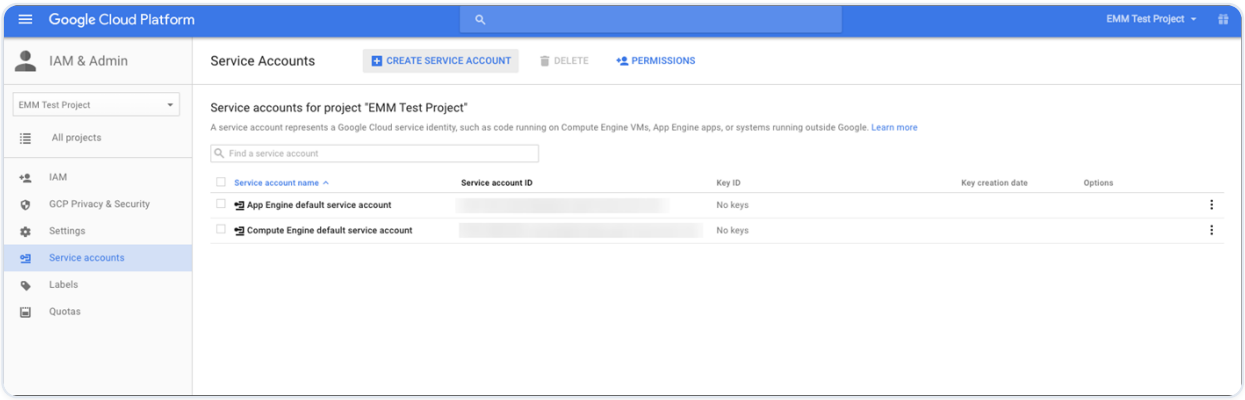
7. **Google Play EMM API** 옆에서 **자격 증명으로 이동**을 클릭합니다.



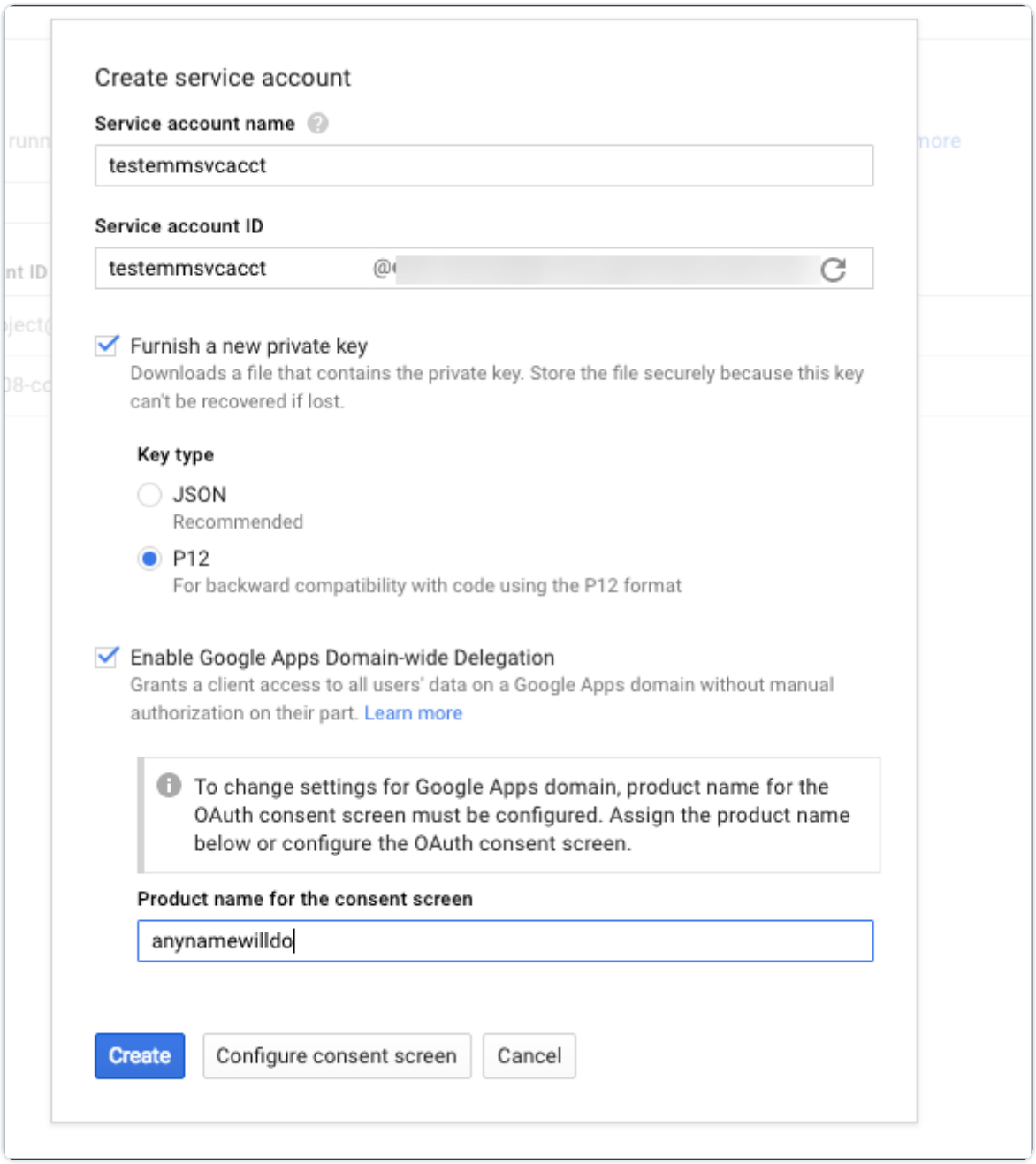
8. **프로젝트에 자격 증명 추가** 목록의 1단계에서 **서비스 계정**을 클릭합니다.



9. **서비스 계정** 페이지에서 **서비스 계정 만들기**를 클릭합니다.

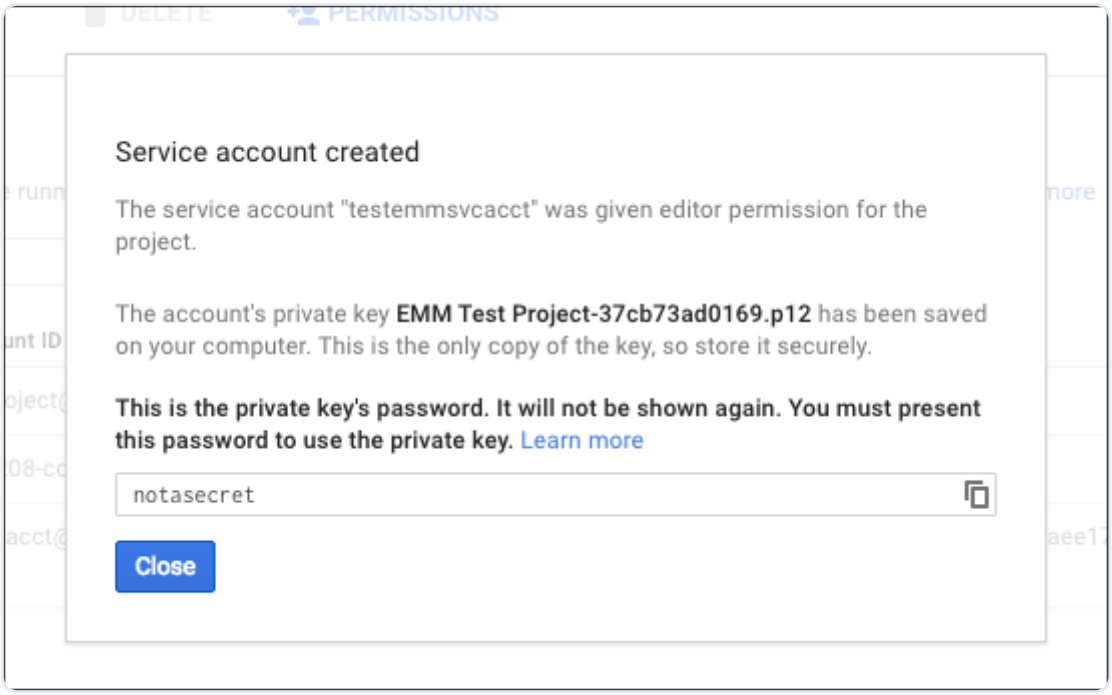


10. **서비스 계정 만들기**에서 계정 이름을 지정하고 **새 비공개 키 제공** 확인란을 선택합니다. **P12**를 클릭하고 **Google Apps 도메인 전체 위임 사용** 확인란을 선택한 다음 **만들기**를 클릭합니다.

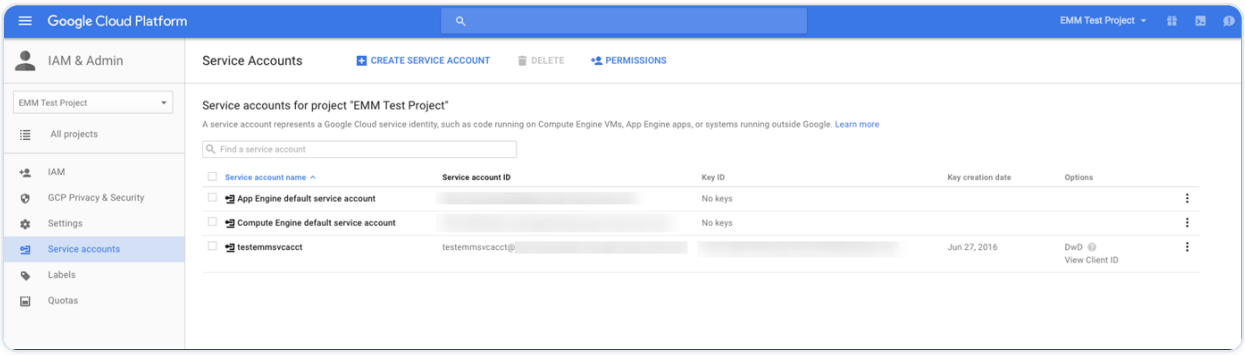


인증서(P12 파일)가 컴퓨터에 다운로드됩니다. 인증서를 안전한 위치에 저장해야 합니다.

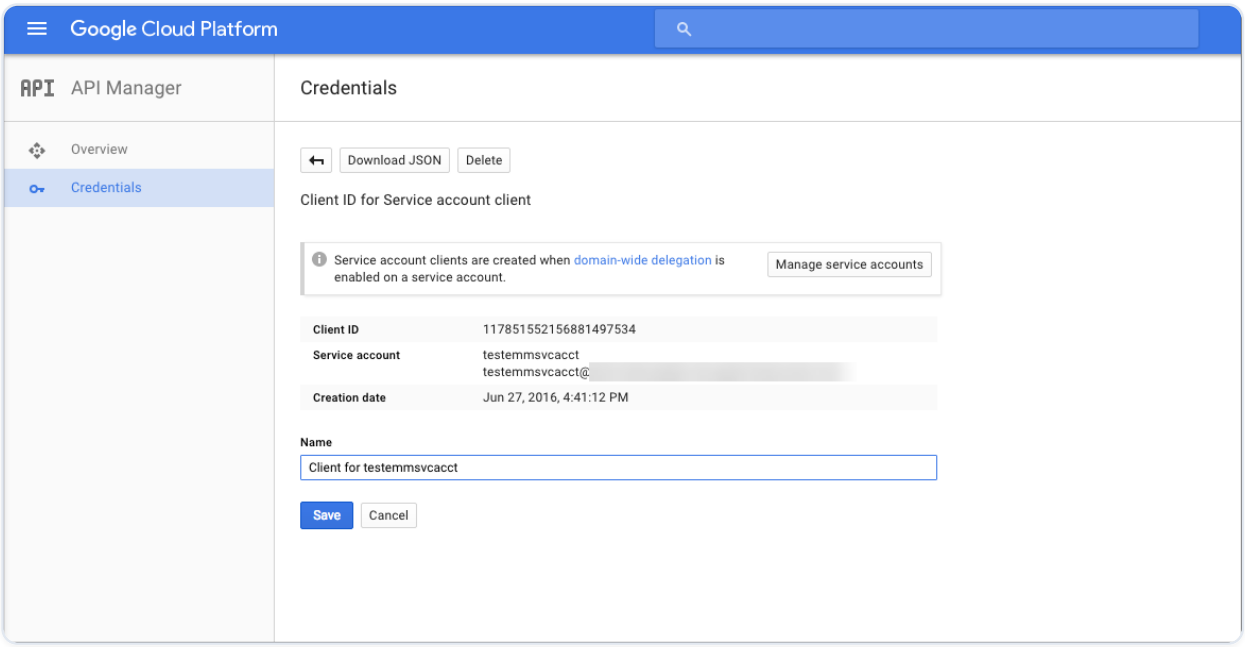
11. **서비스 계정 생성됨** 확인 페이지에서 **닫기**를 클릭합니다.



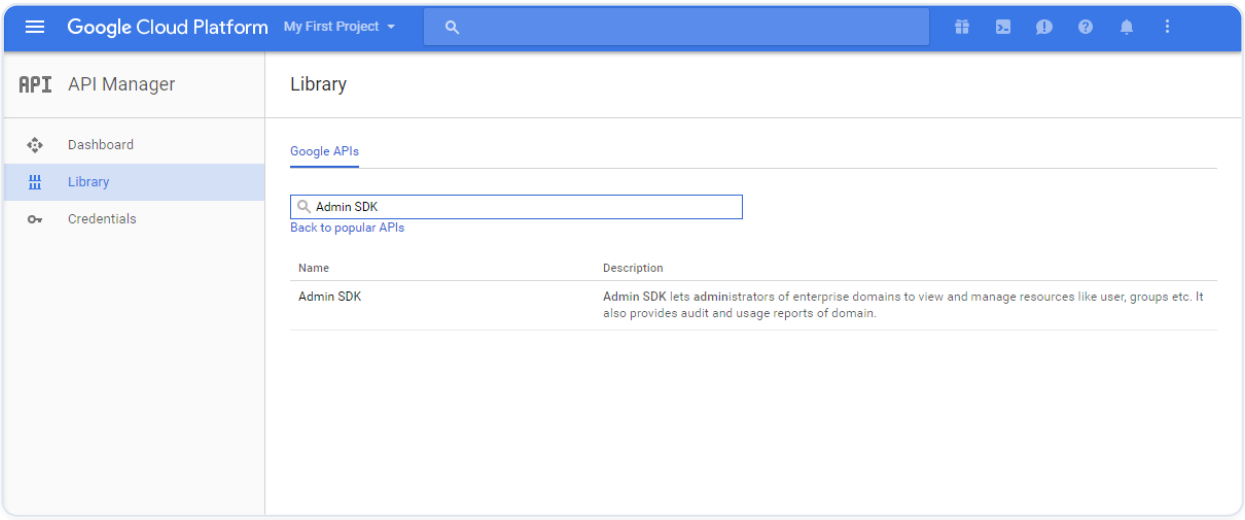
12. **권한**에서 **서비스 계정**을 클릭한 다음 서비스 계정의 **옵션** 아래에서 **클라이언트 ID 보기**를 클릭합니다.



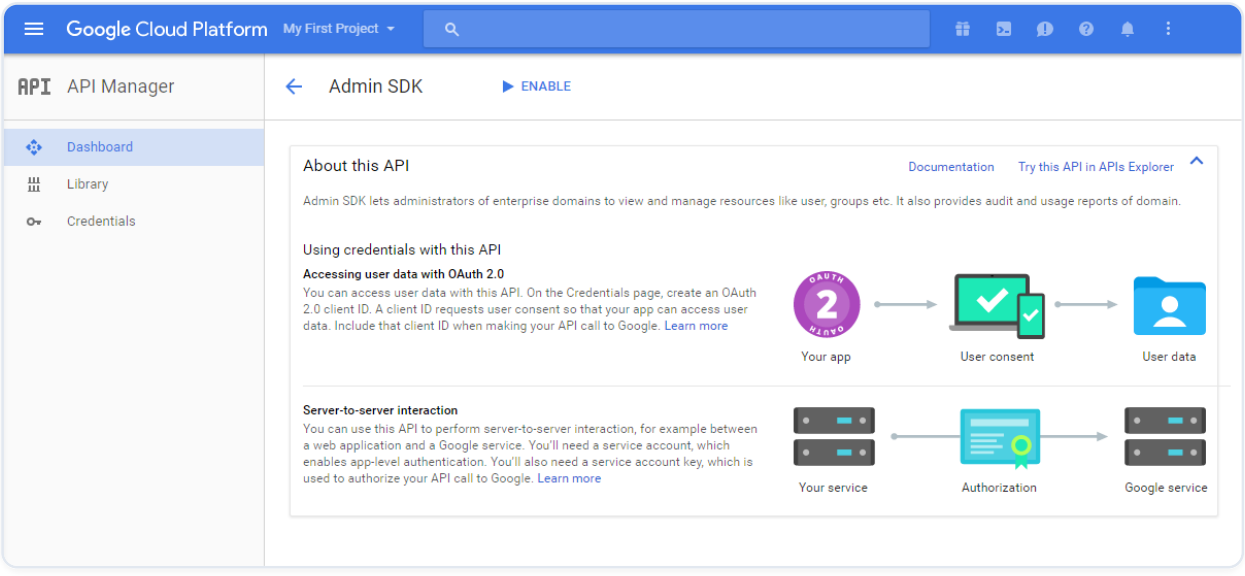
13. Google 관리 콘솔에서 계정 승인에 필요한 세부 정보가 표시됩니다. **클라이언트 ID**와 **서비스 계정 ID**를 나중에 정보를 검색할 수 있는 위치에 복사합니다. 이 정보와 도메인 이름을 Citrix 지원팀에 보내 승인을 받아야 합니다.



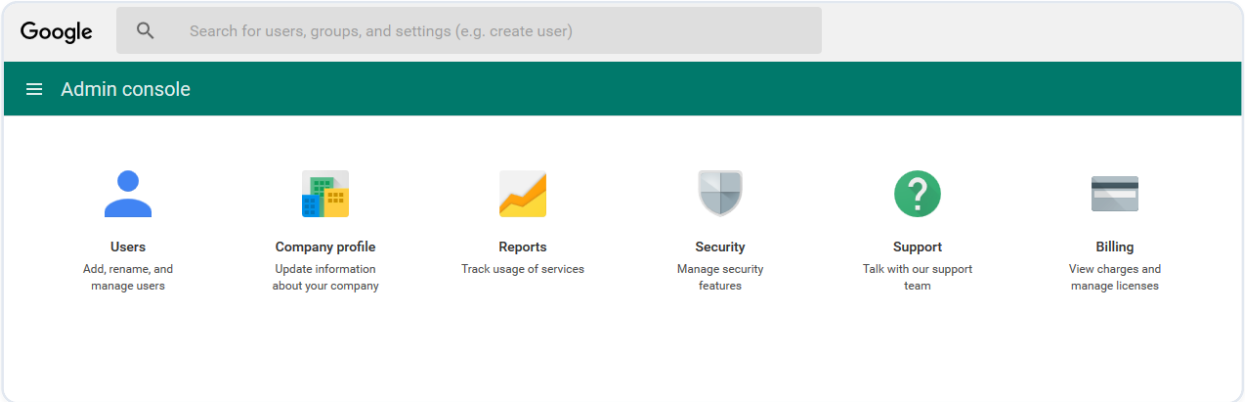
14. **라이브러리** 페이지에서 **Admin SDK**를 검색한 다음 검색 결과를 클릭합니다.



15. **개요** 페이지에서 **사용**을 클릭합니다.



16. 도메인의 Google 관리 콘솔을 열고 **보안**을 클릭합니다.



17. **설정** 페이지에서 **더 보기**를 클릭한 다음 **고급 설정**을 클릭합니다.

    고급 설정 이미지(/en-us/xenmobile/server/media/afw-admin-console-security-2.png)

    고급 설정 이미지(/en-us/xenmobile/server/media/afw-admin-console-security-3.png)

18. **API 클라이언트 액세스 관리**를 클릭합니다.

    API 클라이언트 액세스 관리 옵션 이미지(/en-us/xenmobile/server/media/afw-admin-console-security-4.png)

19. **클라이언트 이름**에 이전에 저장한 클라이언트 ID를 입력하고, **하나 이상의 API 범위**에 `https://www.googleapis.com/auth/admin.directory.user`을(를) 입력한 다음 **승인**을 클릭합니다.

    클라이언트 이름 옵션 이미지(/en-us/xenmobile/server/media/google-config-API-1l.png)

EMM에 바인딩

XenMobile을 사용하여 Android 장치를 관리하려면 Citrix 기술 지원팀에 문의하여 도메인 이름, 서비스 계정 및 바인딩 토큰을 제공해야 합니다. Citrix는 토큰을 엔터프라이즈 모빌리티 관리(EMM) 공급자로 XenMobile에 바인딩합니다. Citrix 기술 지원팀 연락처 정보는 Citrix 기술 지원을(를) 참조하십시오.

1. 바인딩을 확인하려면 Google 관리 포털에 로그인한 다음 **보안**을 클릭합니다.
2. **Android용 EMM 공급자 관리**를 클릭합니다.

   Google Android Enterprise 계정이 EMM 공급자로 Citrix에 바인딩된 것을 확인할 수 있습니다.

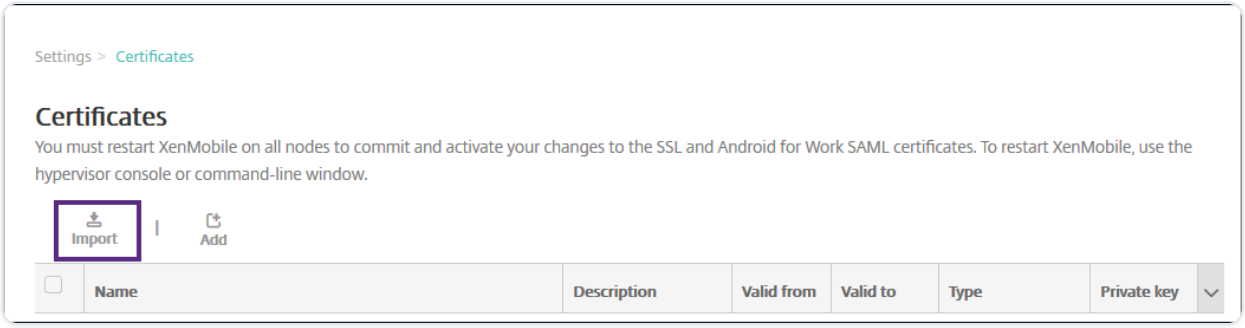
   토큰 바인딩을 확인한 후 XenMobile 콘솔을 사용하여 Android 장치를 관리할 수 있습니다. 14단계에서 생성한 P12 인증서를 가져옵니다. Android Enterprise 서버 설정을 설정하고, SAML 기반 Single Sign-On(SSO)을 활성화하고, 하나 이상의 Android Enterprise 장치 정책을 정의합니다.

   Android용 EMM 공급자 관리 옵션 이미지(/en-us/xenmobile/server/media/afw-verify-emm-binding.png)

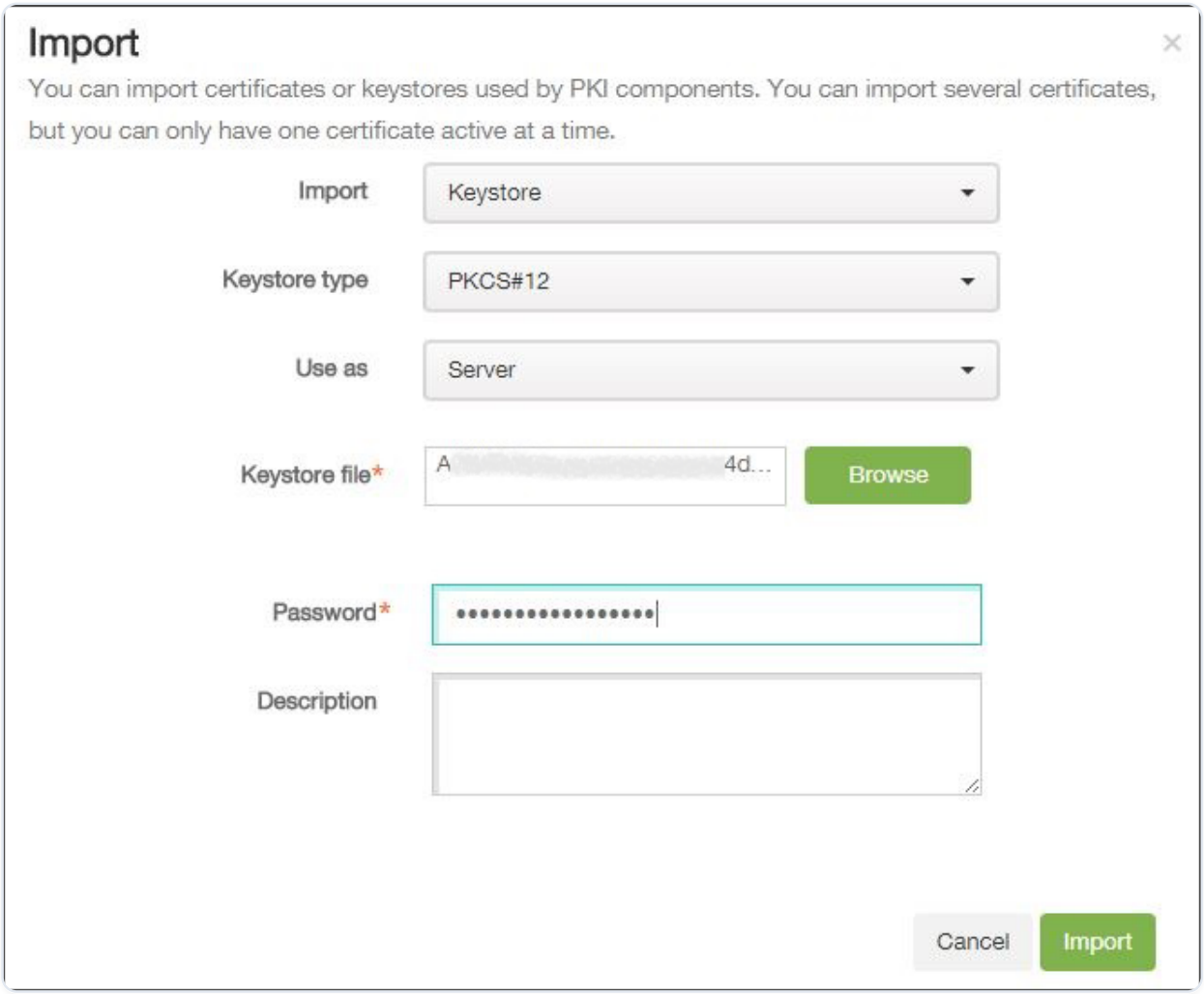
P12 인증서 가져오기

Android Enterprise P12 인증서를 가져오려면 다음 단계를 따르십시오.

1. XenMobile 콘솔에 로그인합니다.
2. 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭하여 **설정** 페이지를 연 다음 **인증서**를 클릭합니다. **인증서** 페이지가 나타납니다.



3. **가져오기**를 클릭합니다. **가져오기** 대화 상자가 나타납니다.



다음 설정을 구성합니다.

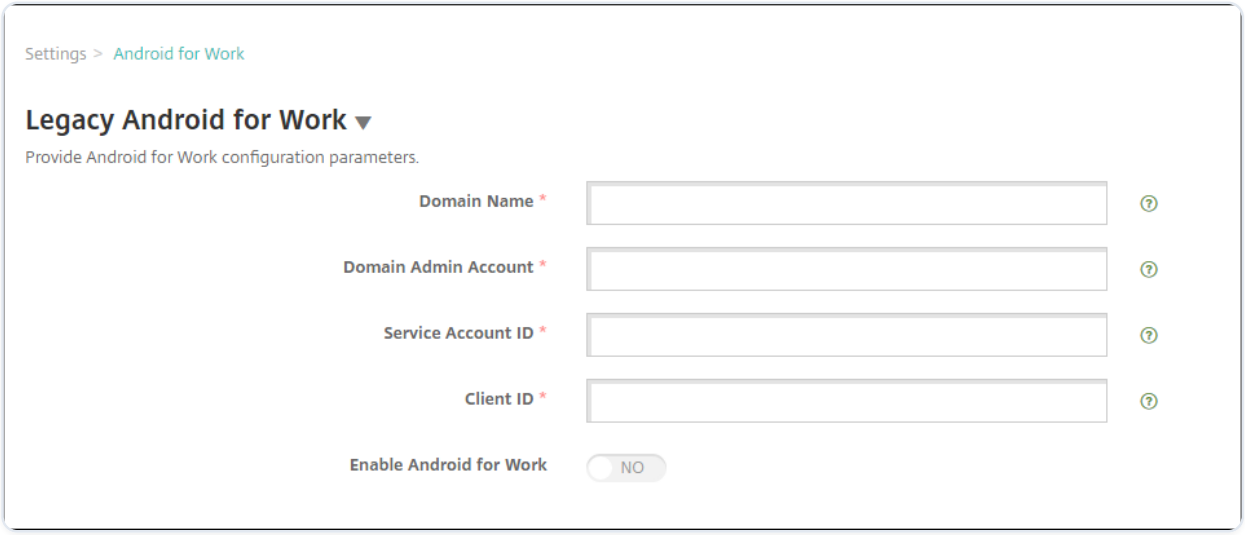
- **가져오기:** 목록에서 **키 저장소**를 클릭합니다.

- **키 저장소 유형:** 목록에서 **PKCS#12**를 클릭합니다.
- **용도:** 목록에서 **서버**를 클릭합니다.
- **키 저장소 파일: 찾아보기**를 클릭하고 P12 인증서로 이동합니다.
- **암호:** 키 저장소 암호를 입력합니다.
- **설명:** 선택적으로 인증서에 대한 설명을 입력합니다.

4. **가져오기**를 클릭합니다.

Android Enterprise 서버 설정

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **서버** 아래에서 **Android Enterprise**를 클릭합니다. **Android Enterprise** 페이지가 나타납니다.



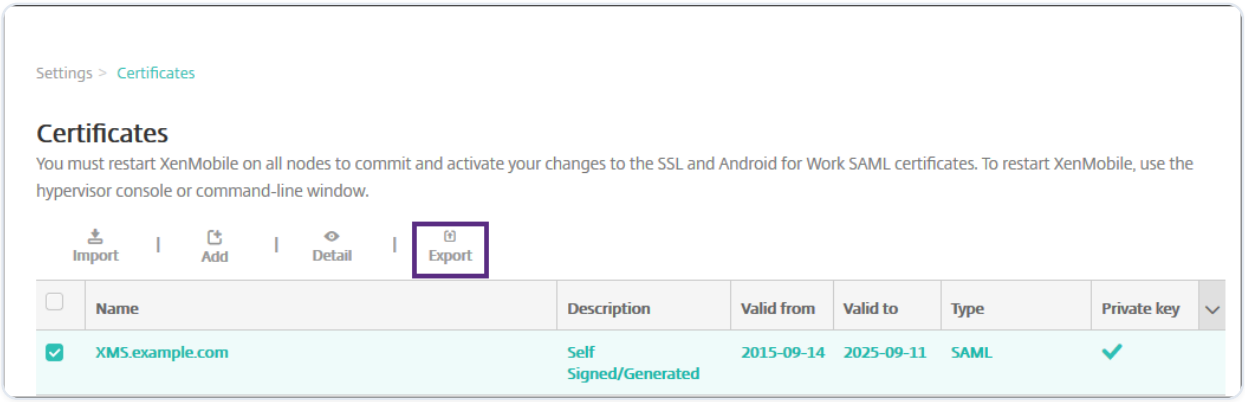
다음 설정을 구성한 다음 **저장**을 클릭합니다.

- **도메인 이름:** Android Enterprise 도메인 이름을 입력합니다. 예를 들어, domain.com입니다.
- **도메인 관리자 계정:** 도메인 관리자 사용자 이름을 입력합니다. 예를 들어, Google 개발자 포털에 사용된 이메일 계정입니다.
- **서비스 계정 ID:** 서비스 계정 ID를 입력합니다. 예를 들어, Google 서비스 계정에 연결된 이메일 (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`)입니다.
- **클라이언트 ID:** Google 서비스 계정의 숫자 클라이언트 ID를 입력합니다.
- **Android Enterprise 사용:** Android Enterprise를 사용하거나 사용하지 않도록 설정하려면 선택합니다.

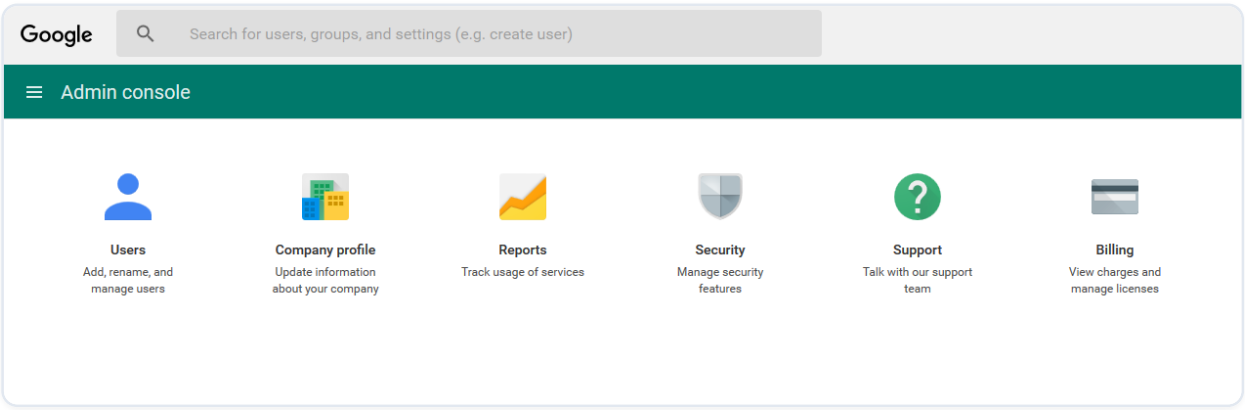
SAML 기반 Single Sign-On 사용

1. XenMobile 콘솔에 로그인합니다.

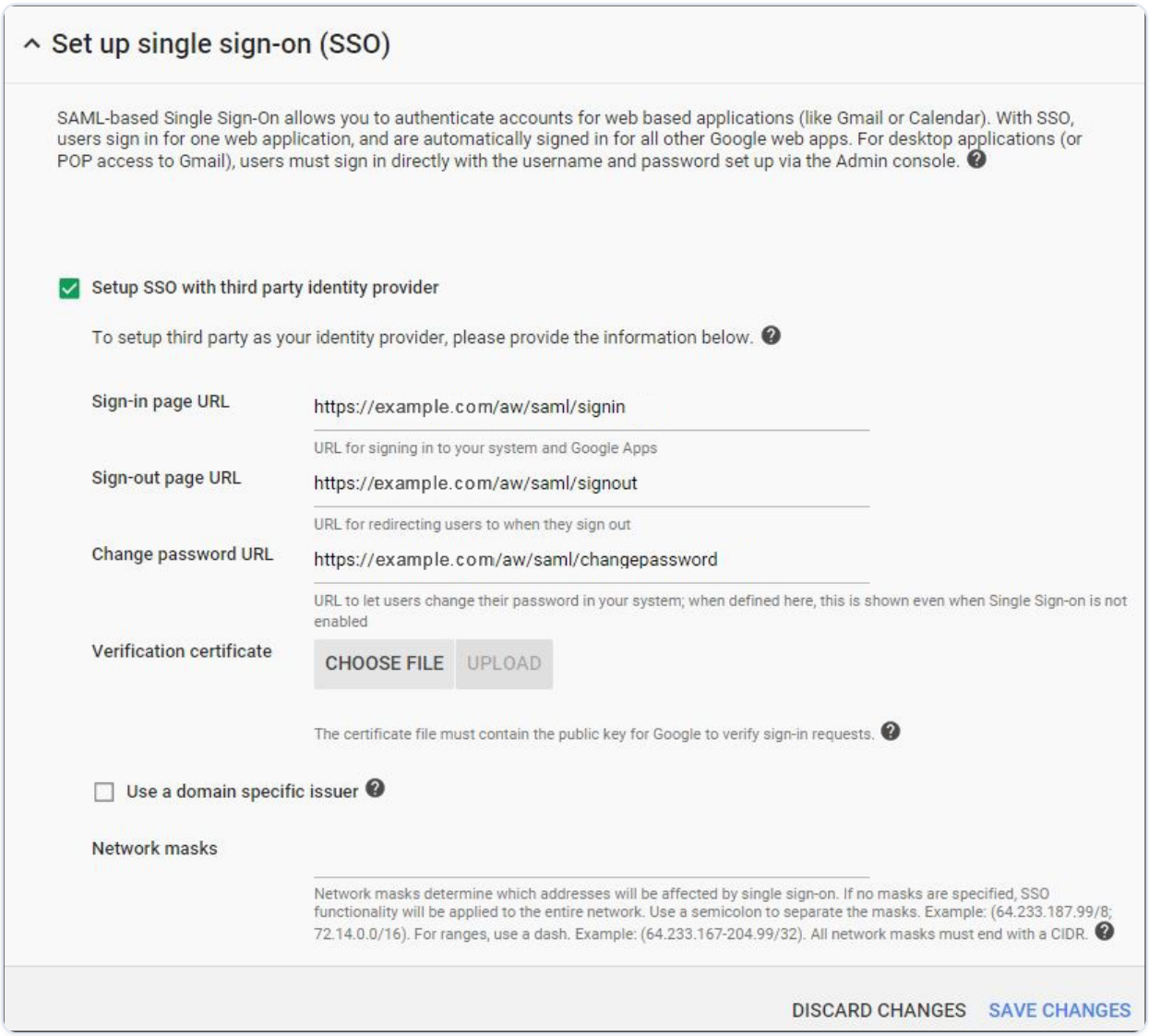
2. 콘솔의 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
3. **인증서**를 클릭합니다. **인증서** 페이지가 나타납니다.



4. 인증서 목록에서 SAML 인증서를 클릭합니다.
5. **내보내기**를 클릭하고 인증서를 컴퓨터에 저장합니다.
6. Android Enterprise 관리자 자격 증명을 사용하여 Google 관리 포털에 로그인합니다. 포털 액세스에 대한 자세한 내용은 Google 관리 포털을 참조하십시오.
7. **보안**을 클릭합니다.



8. **보안** 아래에서 **단일 Sign-On(SSO) 설정**을 클릭한 다음 다음 설정을 구성합니다.

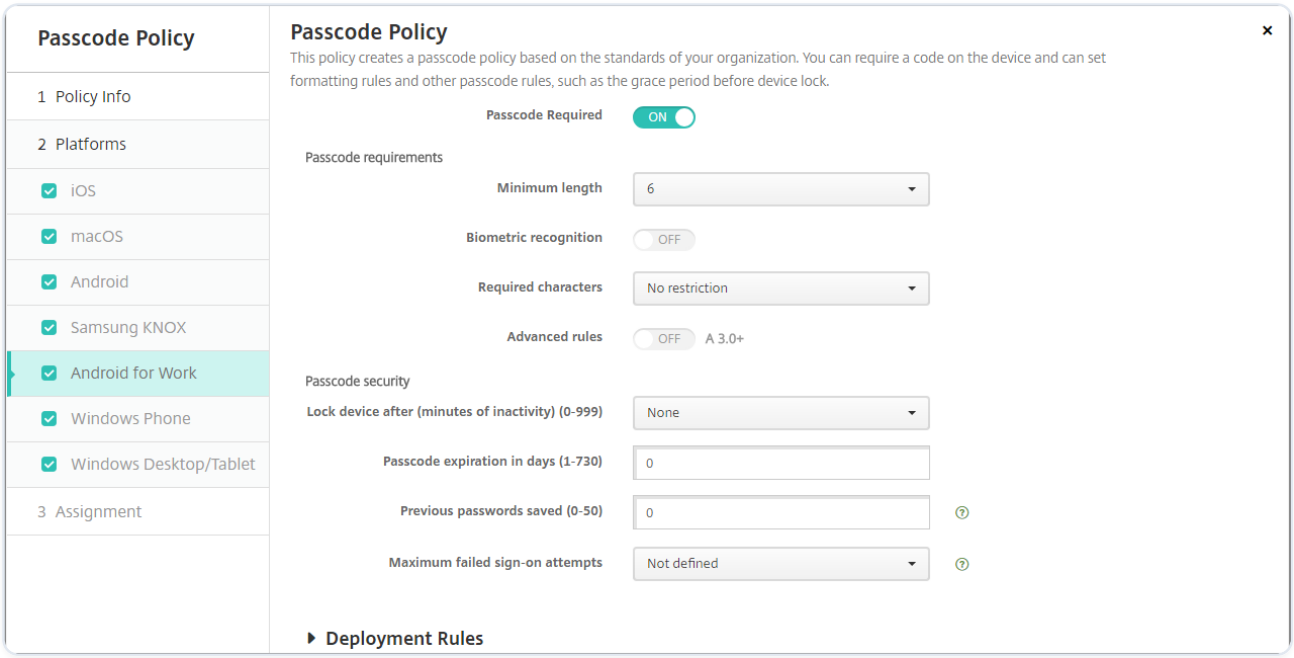


- **로그인 페이지 URL:** 사용자가 시스템 및 Google 앱에 로그인하는 데 사용하는 URL을 입력합니다. 예: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **로그아웃 페이지 URL:** 사용자가 로그아웃할 때 리디렉션되는 URL을 입력합니다. 예: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **암호 변경 URL:** 사용자가 시스템에서 암호를 변경할 수 있도록 하는 URL을 입력합니다. 예: `https://<Xenmobile-FQDN>/aw/saml/changepassword`. 이 필드가 정의된 경우 SSO를 사용할 수 없는 경우에도 사용자에게 이 메시지가 표시됩니다.
- **확인 인증서: 파일 선택**을 클릭한 다음 XenMobile에서 내보낸 SAML 인증서로 이동합니다.

9. **변경 사항 저장**을 클릭합니다.

Android Enterprise 장치 정책 설정

사용자가 처음 등록할 때 장치에 암호를 설정해야 하도록 암호 정책을 설정합니다.



모든 장치 정책을 설정하는 기본 단계는 다음과 같습니다.

1. XenMobile 콘솔에 로그인합니다.
2. **구성**을 클릭한 다음 **장치 정책**을 클릭합니다.
3. **추가**를 클릭한 다음 **새 정책 추가** 대화 상자에서 추가할 정책을 선택합니다. 이 예에서는 **암호**를 클릭합니다.
4. **정책 정보** 페이지를 작성합니다.
5. **Android Enterprise**를 클릭한 다음 정책 설정을 구성합니다.
6. 정책을 배달 그룹에 할당합니다.

Android Enterprise 계정 설정 구성

장치에서 Android 앱 및 정책 관리를 시작하기 전에 XenMobile에서 Android Enterprise 도메인 및 계정 정보를 설정해야 합니다. 먼저 Google에서 Android Enterprise 설정 작업을 완료하여 도메인 관리자를 설정하고 서비스 계정 ID 및 바인딩 토큰을 가져옵니다.

1. XenMobile 웹 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 표시됩니다.
2. **서버** 아래에서 **Android Enterprise**를 클릭합니다. **Android Enterprise** 구성 페이지가 나타납니다.

Android Enterprise 구성 페이지 이미지(/en-us/xenmobile/server/media/settings-server-legacy-android-for-work-1.png)

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 ID를 입력합니다.
- **클라이언트 ID::** Google 서비스 계정의 클라이언트 ID를 입력합니다.
- **Android Enterprise 사용:** Android Enterprise를 사용할지 여부를 선택합니다.

2. **저장**을 클릭합니다.

XenMobile용 Google Workspace 파트너 액세스 설정

Chrome의 일부 엔드포인트 관리 기능은 Google 파트너 API를 사용하여 XenMobile과 Google Workspace 도메인 간에 통신합니다. 예를 들어, XenMobile은 시크릿 모드 및 게스트 모드와 같은 Chrome 기능을 관리하는 장치 정책에 API가 필요합니다.

파트너 API를 사용하려면 XenMobile 콘솔에서 Google Workspace 도메인을 설정한 다음 Google Workspace 계정을 구성합니다.

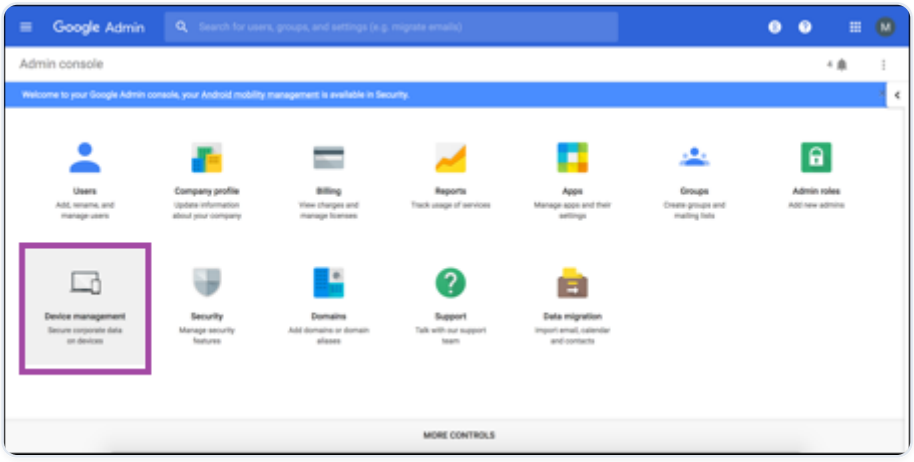
XenMobile에서 Google Workspace(이전 G Suite) 도메인 설정

XenMobile이 Google Workspace 도메인의 API와 통신할 수 있도록 하려면 **설정 > Google Chrome 구성**으로 이동하여 설정을 구성합니다.

- **G Suite 도메인:** XenMobile에 필요한 API를 호스팅하는 Google Workspace 도메인입니다.
- **G Suite 관리자 계정:** G Suite 도메인의 관리자 계정입니다.
- **G Suite 클라이언트 ID:** Citrix의 클라이언트 ID입니다. 이 값을 사용하여 Google Workspace 도메인의 파트너 액세스를 구성합니다.
- **G Suite 엔터프라이즈 ID:** Google 엔터프라이즈 계정에서 가져온 계정의 엔터프라이즈 ID입니다.

Google Workspace 도메인의 장치 및 사용자에 대한 파트너 액세스 사용

1. Google 관리 콘솔에 로그인합니다: `<https://admin.google.com>`
2. **기기 관리**를 클릭합니다.



3. **Chrome 관리**를 클릭합니다.

   Google 관리 콘솔 이미지(/en-us/xenmobile/server/media/google-admin-partner-access2.png)

4. **사용자 설정**을 클릭합니다.

   Google 관리 콘솔 이미지(/en-us/xenmobile/server/media/google-admin-partner-access3.png)

5. **Chrome 관리 - 파트너 액세스**를 검색합니다.

   Google 관리 콘솔 이미지(/en-us/xenmobile/server/media/google-admin-partner-access4.png)

6. **Chrome 관리 - 파트너 액세스 사용** 확인란을 선택합니다.
7. 파트너 액세스를 이해하고 사용하도록 설정하는 데 동의합니다. **저장**을 클릭합니다.
8. Chrome 관리 페이지에서 **기기 설정**을 클릭합니다.

   Google 관리 콘솔 이미지(/en-us/xenmobile/server/media/google-admin-partner-access5.png)

9. **Chrome 관리 - 파트너 액세스**를 검색합니다.

   Google 관리 콘솔 이미지(/en-us/xenmobile/server/media/google-admin-partner-access6.png)

10. **Chrome 관리 - 파트너 액세스 사용** 확인란을 선택합니다.
11. 파트너 액세스를 이해하고 사용하도록 설정하는 데 동의합니다. **저장**을 클릭합니다.
12. **보안** 페이지로 이동한 다음 **고급 설정**을 클릭합니다.

    Google 관리 콘솔 이미지(/en-us/xenmobile/server/media/google-admin-partner-access7.png)

13. **API 클라이언트 액세스 관리**를 클릭합니다.
14. XenMobile 콘솔에서 **설정 > Google Chrome 구성**으로 이동하여 Google Workspace 클라이언트 ID 값을 복사합니다. 그런 다음, **API 클라이언트 액세스 관리** 페이지로 돌아가서 복사한 값을 **클라이언트 이름** 필드에 붙여넣습니다.
15. **하나 이상의 API 범위**에서 URL을 추가합니다: `https://www.googleapis.com/auth/chromedevicemanagementapi`

    Google 관리 콘솔 이미지(/en-us/xenmobile/server/media/google-admin-partner-access8.png)

16. **승인**을 클릭합니다.

    "설정이 저장되었습니다." 메시지가 나타납니다.

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/restrictions-device-policy-ios113.png)

Android Enterprise 장치 등록

장치 등록 프로세스에서 사용자가 사용자 이름 또는 사용자 ID를 입력해야 하는 경우, 허용되는 형식은 XenMobile Server가 UPN(사용자 계정 이름) 또는 SAM 계정 이름으로 사용자를 검색하도록 구성된 방식에 따라 달라집니다.

XenMobile Server가 UPN으로 사용자를 검색하도록 구성된 경우, 사용자는 다음 형식으로 UPN을 입력해야 합니다:

- *사용자 이름@도메인*

XenMobile Server가 SAM으로 사용자를 검색하도록 구성된 경우, 사용자는 다음 형식 중 하나로 SAM을 입력해야 합니다:

- *사용자 이름@도메인*
- *domain\username*

XenMobile Server가 구성된 사용자 이름 유형을 확인하려면 다음을 수행합니다.

1. XenMobile Server 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **LDAP**를 클릭하여 LDAP 연결 구성을 확인합니다.
3. 페이지 하단에서 **사용자 검색 기준** 필드를 확인합니다.
    - **userPrincipalName**으로 설정된 경우 XenMobile Server는 UPN으로 설정됩니다.
    - **sAMAccountName**으로 설정된 경우 XenMobile Server는 SAM으로 설정됩니다.

Android Enterprise 엔터프라이즈 등록 취소

XenMobile Server 콘솔 및 XenMobile Tools를 사용하여 Android Enterprise 엔터프라이즈를 등록 취소할 수 있습니다.

이 작업을 수행하면 XenMobile Server가 XenMobile Tools용 팝업 창을 엽니다. 시작하기 전에 XenMobile Server가 사용 중인 브라우저에서 팝업 창을 열 수 있는 권한이 있는지 확인하십시오. Google Chrome과 같은 일부 브라우저는 팝업 차단을 비활성화하고 XenMobile 사이트 주소를 팝업 차단 허용 목록에 추가해야 합니다.

> **경고:**

> 엔터프라이즈가 등록 취소되면 해당 엔터프라이즈를 통해 이미 등록된 장치의 Android Enterprise 앱은 기본 상태로 재설정됩니다. 장치는 더 이상 Google에서 관리하지 않습니다. Android Enterprise 엔터프라이즈에 다시 등록해도 추가 구성 없이는 이전 기능을 복원하지 못할 수 있습니다.

> Android Enterprise 엔터프라이즈가 등록 취소된 후:

- 엔터프라이즈를 통해 등록된 장치 및 사용자는 Android Enterprise 앱이 기본 상태로 재설정됩니다. 이전에 적용된 Android Enterprise 앱 권한 및 Android Enterprise 앱 제한 정책은 더 이상 적용되지 않습니다.
- 엔터프라이즈를 통해 등록된 장치는 XenMobile에서 관리되지만 Google 관점에서는 관리되지 않습니다. 새로운 Android Enterprise 앱을 추가할 수 없습니다. Android Enterprise 앱 권한 또는 Android Enterprise 앱 제한 정책을 적용할 수 없습니다. 예약, 암호 및 제한과 같은 다른 정책은 이러한 장치에 계속 적용할 수 있습니다.
- Android Enterprise에 장치를 등록하려고 하면 Android Enterprise 장치가 아닌 Android 장치로 등록됩니다.

Android Enterprise 엔터프라이즈 등록을 취소하려면:

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 설정 페이지에서 **Android Enterprise**를 클릭합니다.
3. **엔터프라이즈 제거**를 클릭합니다.

   엔터프라이즈 제거 옵션 이미지(/en-us/xenmobile/server/media/settings-android-for-work-remove-enterprise.png)
4. 암호를 지정합니다. 등록 취소를 완료하려면 다음 단계에서 이 암호가 필요합니다. 그런 다음 **등록 취소**를 클릭합니다.

   등록 취소 옵션 이미지(/en-us/xenmobile/server/media/settings-android-for-work-unenroll.png)
5. XenMobile 도구 페이지가 열리면 이전 단계에서 생성한 암호를 입력합니다.

   암호 필드 이미지(/en-us/xenmobile/server/media/tools-unenroll-android-enterprise-step1.png)
6. **등록 취소**를 클릭합니다.

   등록 취소 옵션 이미지(/en-us/xenmobile/server/media/tools-unenroll-android-enterprise-step2.png)

Android Enterprise에서 완전 관리형 장치 프로비저닝

회사 소유 장치만 Android Enterprise의 완전 관리형 장치가 될 수 있습니다. 완전 관리형 장치에서는 업무 프로필뿐만 아니라 전체 장치가 회사 또는 조직에 의해 제어됩니다. 완전 관리형 장치는 업무 관리형 장치라고도 합니다.

XenMobile은 완전 관리형 장치에 대해 다음 등록 방법을 지원합니다.

- **afw#xenmobile:** 이 등록 방법을 사용하면 사용자가 장치를 설정할 때 "afw#xenmobile" 문자를 입력합니다. 이 토큰은 장치가 XenMobile에 의해 관리됨을 식별하고 Secure Hub를 다운로드합니다.
- **QR 코드:** QR 코드 프로비저닝은 태블릿과 같이 NFC를 지원하지 않는 분산된 장치 플릿을 프로비저닝하는 쉬운 방법입니다. QR 코드 등록 방법은 공장 설정으로 재설정된 플릿 장치에서 사용할 수 있습니다. QR 코드 등록 방법은 설정 마법사에서 QR 코드를 스캔하여 완전 관리형 장치를 설정하고 구성합니다.
- **근거리 무선 통신(NFC) 범프:** NFC 범프 등록 방법은 공장 설정으로 재설정된 플릿 장치에서 사용할 수 있습니다. NFC 범프는 근거리 무선 통신을 사용하여 두 장치 간에 데이터를 전송합니다. 공장 초기화된 장치에서는 Bluetooth, Wi-Fi 및 기타 통신 모드가 비활성화됩니다. NFC는 이 상태에서 장치가 사용할 수 있는 유일한 통신 프로토콜입니다.

afw#xenmobile

이 등록 방법은 새 장치 또는 공장 초기화된 장치의 전원을 켠 후 초기 설정에 사용됩니다. 사용자에게 Google 계정을 입력하라는 메시지가 표시되면 "afw#xenmobile"을 입력합니다. 이 작업은 Secure Hub를 다운로드하고 설치합니다. 그런 다음 사용자는 Secure Hub 설정 프롬프트에 따라 등록을 완료합니다.

이 등록 방법은 Secure Hub의 최신 버전이 Google Play 스토어에서 다운로드되므로 대부분의 고객에게 권장됩니다. 다른 등록 방법과 달리 XenMobile Server에서 Secure Hub를 다운로드할 수 있도록 제공할 필요가 없습니다.

전제 조건:

- Android 5.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.

QR 코드

QR 코드를 사용하여 장치 모드에 장치를 등록하려면 JSON을 생성하고 해당 JSON을 QR 코드로 변환하여 QR 코드를 생성합니다. 장치 카메라는 QR 코드를 스캔하여 장치를 등록합니다.

전제 조건:

- Android 7.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.

JSON에서 QR 코드 생성

다음 필드를 사용하여 JSON을 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: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

값: `https://path/to/securehub.apk`

참고:

Secure Hub이 엔터프라이즈 앱으로 Citrix XenMobile Server에 업로드된 경우, `https://<fqdn>:4443/*instanceName*/worxhome.apk`에서 다운로드할 수 있습니다. Secure Hub APK 경로는 장치가 프로비저닝 중에 연결하는 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 639-1에 정의된 두 글자의 소문자 ISO 언어 코드(예: en)입니다. 국가 코드는 ISO 3166-1에 정의된 두 글자의 대문자 ISO 국가 코드(예: US)입니다. 예를 들어, 미국에서 사용되는 영어의 경우 en_US를 입력합니다.

- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가 실행되는 시간대입니다.

  area/location 형식의 Olson 이름을 입력합니다. 예를 들어, 태평양 표준시의 경우 America/Los_Angeles를 입력합니다. 입력하지 않으면 시간대가 자동으로 채워집니다.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Epoch 이후 밀리초 단위 시간입니다.

  유닉스 에포크(또는 유닉스 시간, POSIX 시간 또는 유닉스 타임스탬프)는 January 1, 1970 (UTC/GMT 자정) 이후 경과된 초 수입니다. 이 시간에는 윤초가 포함되지 않습니다 (ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 프로필 생성 중 암호화를 건너뛰려면 **true**로 설정합니다. 프로필 생성 중 암호화를 강제하려면 **false**로 설정합니다.

일반적인 JSON은 다음과 같습니다.

```
{
  "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
}
```

https://jsonlint.com과 같은 JSON 유효성 검사 도구를 사용하여 생성된 JSON의 유효성을 검사합니다.

https://goqr.me와 같은 온라인 QR 코드 생성기를 사용하여 해당 JSON 문자열을 QR 코드로 변환합니다.

이 QR 코드는 초기화된 장치에서 스캔되어 장치를 업무용 관리 장치 모드로 등록합니다.

장치를 등록하려면

장치를 완전 관리형 장치로 등록하려면 장치가 초기화된 상태여야 합니다.

1. 환영 화면에서 화면을 6번 탭하여 QR 코드 등록 흐름을 시작합니다.
2. 메시지가 표시되면 Wi-Fi에 연결합니다. QR 코드(JSON으로 인코딩됨)의 Secure Hub 다운로드 위치는 이 Wi-Fi 네트워크를 통해 액세스할 수 있습니다.

   장치가 Wi-Fi에 성공적으로 연결되면 Google에서 QR 코드 리더를 다운로드하고 카메라를 실행합니다.
3. 카메라를 QR 코드에 대고 코드를 스캔합니다.

   Android는 QR 코드의 다운로드 위치에서 Secure Hub를 다운로드하고, 서명 인증서 서명을 확인하고, Secure Hub를 설치하고, 이를 장치 소유자로 설정합니다.

자세한 내용은 Android EMM 개발자를 위한 Google 가이드를 참조하십시오. `<https://developers.google.com/android/work/prov-devices#qr_code_method>`.

NFC 범프

NFC 범프를 사용하여 장치를 완전 관리형 장치로 등록하려면 두 대의 장치가 필요합니다. 한 대는 공장 설정으로 초기화된 장치이고 다른 한 대는 XenMobile Provisioning Tool을 실행하는 장치입니다.

전제 조건:

- Android 5.0, Android 5.1, Android 6.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.
- Android Enterprise에 대해 활성화된 XenMobile Server 버전 10.4.
- 완전히 관리되는 장치로 Android Enterprise에 프로비저닝된 새 장치 또는 공장 초기화된 장치. 이 필수 구성 요소를 완료하는 단계는 이 문서의 뒷부분에서 확인할 수 있습니다.
- 구성된 프로비저닝 도구를 실행하는 NFC 기능이 있는 다른 장치. 프로비저닝 도구는 Secure Hub 10.4 또는 Citrix 다운로드 페이지에서 사용할 수 있습니다.

각 장치에는 기업 모빌리티 관리(EMM) 앱으로 관리되는 Android Enterprise 프로필이 하나만 있을 수 있습니다. XenMobile에서 Secure Hub는 EMM 앱입니다. 각 장치에는 하나의 프로필만 허용됩니다. 두 번째 EMM 앱을 추가하려고 하면 첫 번째 EMM 앱이 제거됩니다.

NFC 범프를 통해 전송되는 데이터

공장 초기화된 장치를 프로비저닝하려면 Android Enterprise를 초기화하기 위해 NFC 범프를 통해 다음 데이터를 전송해야 합니다.

- 장치 소유자 역할을 하는 EMM 공급자 앱의 패키지 이름(이 경우 Secure Hub).
- 장치가 EMM 공급자 앱을 다운로드할 수 있는 인트라넷/인터넷 위치.
- 다운로드가 성공했는지 확인하기 위한 EMM 공급자 앱의 SHA1 해시.
- 공장 초기화된 장치가 EMM 공급자 앱에 연결하고 다운로드할 수 있도록 하는 Wi-Fi 연결 세부 정보. 참고: Android는 현재 이 단계에서 802.1x Wi-Fi를 지원하지 않습니다.
- 장치의 시간대(선택 사항).
- 장치의 지리적 위치(선택 사항).

두 장치가 범프되면 프로비저닝 도구의 데이터가 공장 초기화된 장치로 전송됩니다. 이 데이터는 관리자 설정으로 Secure Hub를 다운로드하는 데 사용됩니다. 시간대 및 위치 값을 입력하지 않으면 Android가 새 장치에서 값을 자동으로 구성합니다.

XENMOBILE 프로비저닝 도구 구성

NFC 범프를 수행하기 전에 프로비저닝 도구를 구성해야 합니다. 이 구성은 NFC 범프 중에 초기화된 장치로 전송됩니다.

프로비저닝 도구 구성 이미지(/en-us/xenmobile/server/media/nfc-provisioning-secure-hub.png)

필수 필드에 데이터를 직접 입력하거나 텍스트 파일을 통해 채울 수 있습니다. 다음 절차의 단계에서는 텍스트 파일을 구성하는 방법과 각 필드에 대한 설명을 제공합니다. 앱은 입력한 정보를 저장하지 않으므로 나중에 사용할 정보를 보관하기 위해 텍스트 파일을 만드는 것이 좋습니다.
텍스트 파일을 사용하여 프로비저닝 도구를 구성하려면
파일 이름을 nfcprovisioning.txt로 지정하고 장치의 SD 카드에 있는 /sdcard/ 폴더에 파일을 배치합니다. 그러면 앱이 텍스트 파일을 읽고 값을 채울 수 있습니다.

텍스트 파일에는 다음 데이터가 포함되어야 합니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>
```

이 줄은 EMM 공급자 앱의 인트라넷/인터넷 위치입니다. NFC 범프 후 초기화된 장치가 Wi-Fi에 연결되면 장치는 다운로드를 위해 이 위치에 액세스할 수 있어야 합니다. URL은 특별한 서식이 필요 없는 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 단계는 이 문서의 뒷부분에서 설명합니다.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

이 줄은 프로비저닝 도구가 실행 중인 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 비워두어야 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 639-1에 정의된 두 글자 소문자 ISO 언어 코드(예: en)입니다. 국가 코드는 ISO 3166-1에 정의된 두 글자 대문자 ISO 국가 코드(예: US)입니다. 예를 들어, 미국에서 사용되는 영어의 경우 en_US를 입력합니다. 코드를 입력하지 않으면 국가 및 언어가 자동으로 채워집니다.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

장치가 실행되는 시간대입니다. area/location 형식의 Olson 이름을 입력합니다. 예를 들어, 태평양 표준시의 경우 America/Los_Angeles를 입력합니다. 이름을 입력하지 않으면 시간대가 자동으로 채워집니다.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

이 값은 Secure Hub로 앱에 하드코딩되어 있으므로 이 데이터는 필요하지 않습니다. 여기서는 완전성을 위해 언급된 것입니다.

WPA2를 사용하여 보호되는 Wi-Fi가 있는 경우, 완성된 nfcprovisioning.txt 파일은 다음과 같을 수 있습니다.

`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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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`

보호되지 않은 Wi-Fi가 있는 경우, 완성된 nfcprovisioning.txt 파일은 다음과 같을 수 있습니다:

`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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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 가져오려면

모든 앱의 체크섬을 가져오려면 해당 앱을 엔터프라이즈 앱으로 추가합니다.

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동한 다음 **추가**를 클릭합니다.

   앱 추가 창이 나타납니다.
2. **엔터프라이즈**를 클릭합니다.

   앱 정보 페이지가 표시됩니다.

   앱 정보 페이지 이미지(/en-us/xenmobile/server/media/nfc-provisioning-add-app-enterprise.png)
3. 다음 구성을 선택한 다음 **다음**을 클릭합니다.

   Android Enterprise 엔터프라이즈 앱 페이지가 나타납니다.

   Android Enterprise 앱 이미지(/en-us/xenmobile/server/media/configure-apps-android-for-work-1.png)
4. .apk 경로를 제공한 다음 **다음**을 클릭하여 파일을 업로드합니다.

   업로드가 완료되면 업로드된 패키지의 세부 정보가 나타납니다.

   파일 업로드 페이지 이미지(/en-us/xenmobile/server/media/configure-apps-android-for-work-2.png)

5. **다음**을 클릭하여 JSON 파일을 다운로드하는 페이지를 엽니다. 이 파일은 Google Play에 업로드하는 데 사용됩니다. Secure Hub의 경우 Google Play에 업로드할 필요는 없지만, SHA1 값을 읽으려면 JSON 파일이 필요합니다.

   JSON 파일 다운로드 페이지 이미지(/en-us/xenmobile/server/media/nfc-provisioning-android-for-work-json.png)

   일반적인 JSON 파일은 다음과 같습니다.

   일반적인 JSON 파일 이미지(/en-us/xenmobile/server/media/nfc-provisioning-typical-json-file.png)

6. **file_sha1_base64 값**을 복사하여 프로비저닝 도구의 **해시** 필드에 사용합니다.

   > **참고:**
   >
   > 해시는 URL 안전해야 합니다.

   - 모든 **+** 기호를 **-**로 변환
   - 모든 **/** 기호를 **_**로 변환
   - 후행 **\\u003d**를 **=**로 바꿉니다.

   해시를 장치의 SD 카드에 있는 nfcprovisioning.txt 파일에 저장하는 경우 앱이 안전 변환을 수행합니다. 그러나 해시를 수동으로 입력하기로 선택한 경우 URL 안전성을 확인하는 것은 사용자 책임입니다.

사용된 라이브러리

프로비저닝 도구는 소스 코드에서 다음 라이브러리를 사용합니다:

- Google의 Apache license 2.0에 따른 v7 appcompat 라이브러리, Design support 라이브러리 및 v7 Palette 라이브러리

  자세한 내용은 Support Library Features Guide를 참조하십시오.

- Jake Wharton의 Apache 라이선스 2.0에 따라 Butter Knife

Android Enterprise에서 업무 프로필 장치 프로비저닝

Android Enterprise의 업무 프로필 장치에서는 장치에서 회사 영역과 개인 영역을 안전하게 분리합니다. 예를 들어, BYOD 장치는 업무 프로필 장치가 될 수 있습니다. 업무 프로필 장치의 등록 환경은 XenMobile의 Android 등록과 유사합니다. 사용자는 Google Play에서 Secure Hub를 다운로드하고 장치를 등록합니다.

기본적으로 Android Enterprise에 업무 프로필 장치로 등록된 장치에서는 USB 디버깅 및 알 수 없는 소스 설정이 비활성화됩니다.

팁:

Android Enterprise에 장치를 업무 프로필 장치로 등록할 때 항상 Google Play로 이동하십시오. 거기에서 Secure Hub가 사용자의 개인 프로필에 표시되도록 설정하십시오.

관리형 구성 피드백 지원 (기술 미리 보기)

참고:

기술 미리 보기의 기능은 비프로덕션 또는 제한된 프로덕션 환경에서 사용할 수 있으며, 고객에게 피드백을 공유할 기회를 제공합니다. Citrix®는 기술 미리 보기 기능에 대한 지원 사례를 접수하지 않지만, 개선을 위한 피드백은 환영합니다. **피드백 보내기**를 클릭하여 이 기능에 대한 피드백을 제공할 수 있습니다. Citrix는 피드백의 심각도, 중요성 및 중요도에 따라 조치할 수 있습니다.

관리형 구성 피드백 기능을 통해 관리자는 관리형 구성 정책으로 구성된 Android 장치에서 앱 상태에 대한 피드백을 얻을 수 있습니다. 이 피드백은 이러한 정책의 효율성과 상태를 모니터링하는 데 사용될 수 있습니다.

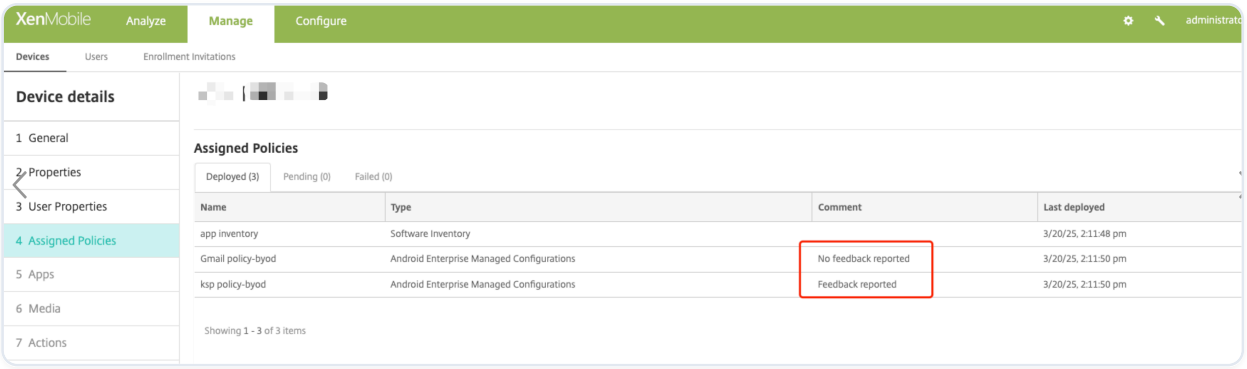
전제 조건

1. `App Support`: 애플리케이션은 관리형 구성 정책을 지원해야 합니다.
2. `Keyed App States`: 앱은 키 기반 앱 상태도 지원해야 합니다. 앱 피드백 작동 방식에 대한 자세한 내용은 EMM에 앱 피드백 보내기를 참조하십시오.

구성 피드백을 관리하고 활용하는 절차

1. 지정된 XenMobile Server에 대해 서버 속성 `afw.app_managed_configurations.feedback`을(를) 활성화합니다.
2. 관리형 구성 정책을 확인합니다.
   - Android 장치가 등록되었고 관리형 구성 정책이 성공적으로 적용되었는지 확인합니다.
   - **장치 세부 정보**로 이동하여 **할당된 정책**을 클릭합니다. 관리형 구성 정책과 관련된 주석이 표시됩니다.

- **피드백 보고됨**: 이 정책 관련 앱에 대한 피드백이 있음을 나타냅니다.
- **피드백 보고되지 않음**: 이 정책 관련 앱에 대해 보고된 피드백이 없음을 나타냅니다.



- **장치 세부 정보**로 이동하여 **앱**을 클릭합니다. 자세한 피드백은 모든 앱 데이터를 포함하는 **관리형 구성 피드백** 테이블 아래에 표시됩니다.

  구성 피드백 관리(/en-us/xenmobile/server/media/manage-config-feedback.png)

- 단일 관리형 구성 정책의 경우, 할당된 모든 장치에 대한 피드백 세부 정보를 확인할 수 있습니다.
  - **정보**: 오류 없이 피드백 데이터가 보고된 모든 장치.
  - **오류**: 오류가 포함된 피드백 데이터가 보고된 모든 장치.
  - **비어 있음**: 피드백 데이터가 보고되지 않은 모든 장치.

  피드백 세부 정보(/en-us/xenmobile/server/media/feedback-details.png)

- 피드백을 수동으로 받으려면 **관리**를 클릭하고 해당 장치를 찾기 위해 확인란을 선택합니다. 예를 들어, 해당 확인란을 선택하고 **앱 피드백**을 클릭할 수 있습니다.

  앱 피드백(/en-us/xenmobile/server/media/app-feedback.png)

- 선택한 장치에서 관리형 구성 피드백을 받으려면 **피드백 받기**를 클릭합니다.

  피드백 받기(/en-us/xenmobile/server/media/get-feedback.png)

- 관리형 구성 피드백 보고서에서 **분석**을 선택하고 **보고**를 클릭하여 전반적인 피드백을 받습니다. 모든 장치, 구성 정책 관리 및 관련 구성 실패에 대한 보고서를 볼 수 있습니다.

  구성 피드백 보고서 관리(/en-us/xenmobile/server/media/manage-config-feedback-report.png)

3. 피드백 일정을 조정하기 위해 두 가지 서버 속성이 도입되었습니다. 서버 속성을 사용하여 콘솔에서 값을 수정하고 피드백 데이터가 데이터베이스에 저장되는 시기를 제어합니다.

   a. Android Enterprise 관리형 구성 피드백 데이터베이스 업데이트를 위한 배치 크기:

   - 키: `android.managed.configuration.feedback.db.update.batch.size`

- DB에 저장할 보고서의 배치 크기를 정의할 수 있으며, DB에 저장된 데이터만 UI에 표시될 수 있습니다. 기본값은 100이고 최대값은 1000입니다.

b. Android Enterprise 관리형 구성 피드백 DB 업데이트 시간 간격:

- 키: `android.managed.configuration.feedback.db.update.time.interval`
- 배치 제한에 도달하지 않더라도 보고서가 데이터베이스에 저장되는 기간을 지정할 수 있습니다. 기본값은 6시간입니다.

문제 해결

기본적으로 피드백 보고서는 각 장치 체크인(Secure Hub가 서버에 연결될 때) 중에 검색됩니다. 그러나 앱 피드백 버튼을 사용하여 특정 장치에 대한 보고서를 수동으로 가져올 수 있습니다.

iOS

XenMobile Server에서 iOS 장치를 관리하려면 Apple에서 APNs(Apple Push Notification service) 인증서를 설정해야 합니다. 자세한 내용은 APNs 인증서를 참조하십시오.

등록 프로필은 사용자가 MDM에서 제외할 수 있는 옵션과 함께 iOS 장치가 MDM+MAM에 등록되는지 여부를 결정합니다. XenMobile Server는 MDM+MAM의 iOS 장치에 대해 다음 인증 유형을 지원합니다. 자세한 내용은 인증서 및 인증 아래의 문서를 참조하십시오.

- 도메인
- 도메인 및 보안 토큰
- 클라이언트 인증서
- 클라이언트 인증서 및 도메인

> **iOS 13에서 신뢰할 수 있는 인증서 요구 사항:**

> Apple은 TLS 서버 인증서에 대한 새로운 요구 사항을 발표했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는지 확인하십시오. Apple 발행물 `<https://support.apple.com/ko-kr/HT210176>`을 참조하십시오. 인증서 관리에 대한 도움말은 XenMobile Server에서 인증서 업로드를 참조하십시오.

> 지원되는 운영 체제에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오.

iOS 14 호환성

XenMobile® Server 및 Citrix® 모바일 앱은 iOS 14와 호환되지만, 현재 iOS 14의 새로운 기능을 지원하지는 않습니다.

감독되는 iOS 장치의 경우 소프트웨어 업그레이드를 최대 90일까지 지연할 수 있습니다. iOS용 제한 장치 정책에서 다음 설정을 사용하십시오.

- **소프트웨어 업데이트 지연 강제 적용**
- **강제 소프트웨어 업데이트 지연**

iOS 설정을 참조하십시오. 이러한 설정은 사용자 등록 모드 또는 감독되지 않은(전체 MDM) 모드의 장치에서는 사용할 수 없습니다.

열려 있어야 하는 Apple 호스트 이름

iOS, macOS 및 Apple App Store의 올바른 작동을 위해 일부 Apple 호스트 이름은 열려 있어야 합니다. 이러한 호스트 이름을 차단하면 iOS, iOS 앱, MDM 작동, 장치 및 앱 등록의 설치, 업데이트 및 올바른 작동에 영향을 미칠 수 있습니다. 자세한 내용은 `<https://support.apple.com/ko-kr/HT201999>`을 참조하십시오.

지원되는 등록 방법

등록 프로필에서 iOS 장치를 관리하는 방법을 지정합니다. 장치 등록 또는 MDM 등록 없음 중에서 선택할 수 있습니다.

iOS 장치에 대한 등록 설정을 구성하려면 **구성 > 등록 프로필 > iOS**로 이동합니다.

iOS용 등록 프로필 페이지(/en-us/xenmobile/server/media/enrollment-profile-ios.png)

다음 표에는 XenMobile Server가 iOS 장치에 대해 지원하는 등록 방법이 나열되어 있습니다.

방법	지원됨
Apple 배포 프로그램	예
Apple School Manager (애플 스쿨 매니저)	예
Apple Configurator (애플 컨피규레이터)	예
수동 등록	예
등록 초대	예

Apple은 비즈니스 및 교육 계정을 위한 장치 등록 프로그램을 제공합니다. 비즈니스 계정의 경우, XenMobile Server에서 장치 등록 및 관리를 위해 Apple 배포 프로그램에 등록합니다. 이 프로그램은 iOS 및 macOS 장치용입니다. Apple 배포 프로그램을 통한 장치 배포를 참조하십시오.

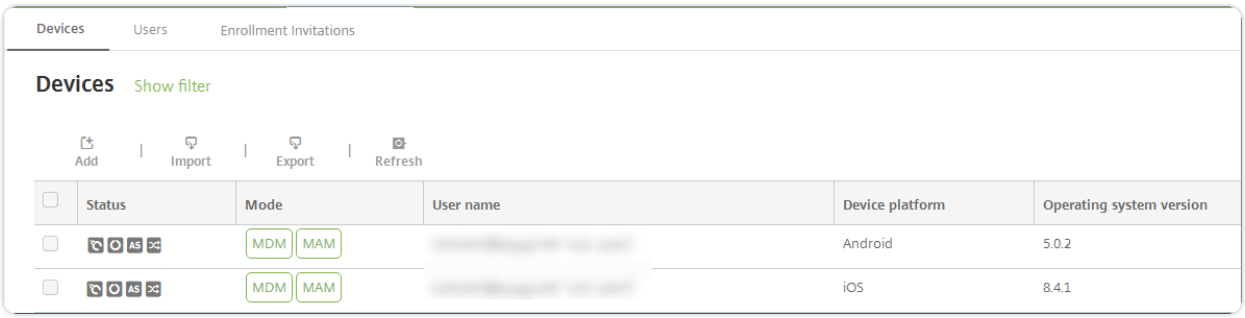
교육 계정의 경우, Apple School Manager 계정을 생성합니다. Apple School Manager는 배포 프로그램과 볼륨 구매를 통합합니다. Apple School Manager는 교육용 Apple 배포 프로그램의 한 유형입니다. Apple 교육 기능과 통합을 참조하십시오.

Apple 배포 프로그램을 사용하여 iOS 및 macOS 장치를 대량으로 등록할 수 있습니다. 해당 장치는 Apple, 참여 Apple 공인 리셀러 또는 통신사에서 직접 구매할 수 있습니다. iOS 장치를 Apple에서 직접 구매하는 경우에도 Apple Configurator를 사용하여 해당 장치를 등록할 수 있습니다. Apple 장치 대량 등록을 참조하십시오.

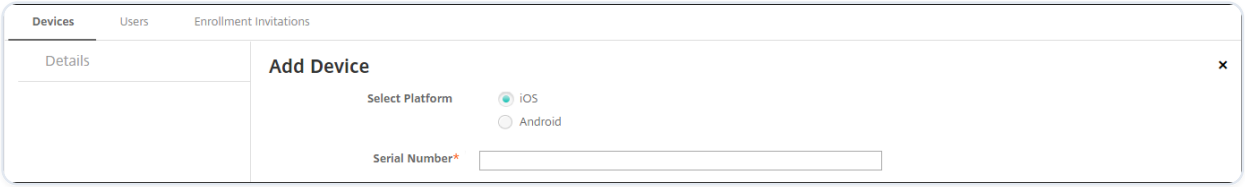
iOS 장치 수동 추가

테스트 목적으로 iOS 장치를 수동으로 추가하려면 다음 단계를 따르십시오.

1. XenMobile Server 콘솔에서 **관리 > 장치**를 클릭합니다. **장치** 페이지가 나타납니다.



2. **추가**를 클릭합니다. **장치 추가** 페이지가 나타납니다.



3. 다음 설정을 구성합니다.

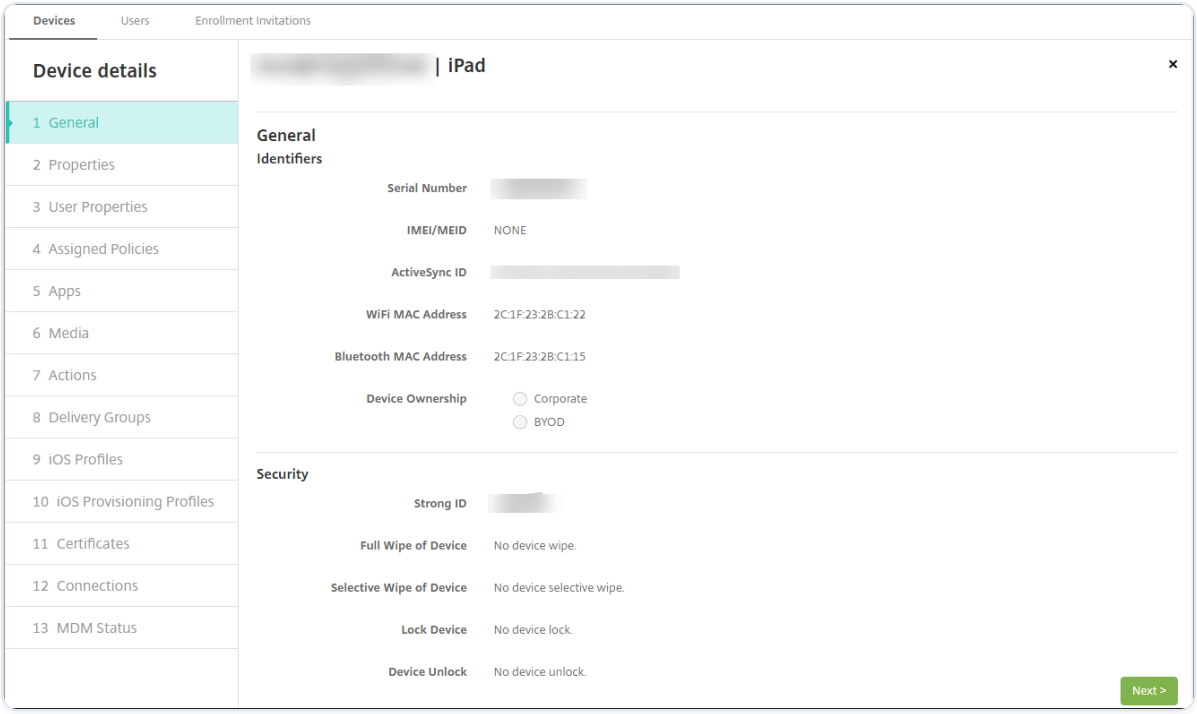
   - **플랫폼 선택: iOS**를 클릭합니다.
   - **일련 번호:** 장치 일련 번호를 입력합니다.

4. **추가**를 클릭합니다. **장치** 테이블이 나타나며 장치가 목록 하단에 추가됩니다. 장치 세부 정보를 보고 확인하려면 추가한 장치를 선택한 다음 나타나는 메뉴에서 **편집**을 클릭합니다.

> **참고:**

> 장치 옆의 확인란을 선택하면 장치 목록 위에 옵션 메뉴가 나타납니다. 목록의 다른 곳을 클릭하면 목록 오른쪽에 옵션 메뉴가 나타납니다.

- LDAP 구성됨
- 로컬 그룹 및 로컬 사용자를 사용하는 경우:
  - 하나 이상의 로컬 그룹.
  - 로컬 그룹에 할당된 로컬 사용자.
  - 전달 그룹은 로컬 그룹과 연결됩니다.
- Active Directory를 사용하는 경우:
  - 전달 그룹은 Active Directory 그룹과 연결됩니다.



5. **일반** 페이지에는 일련 번호 및 플랫폼 유형에 대한 기타 정보와 같은 장치 **식별자**가 나열됩니다. **장치 소유권**의 경우 **회사 소유** 또는 **BYOD**를 선택합니다.

   일반 페이지에는 강력한 ID, 장치 잠금, 활성화 잠금 우회 및 플랫폼 유형에 대한 기타 정보와 같은 장치 **보안** 속성도 나열됩니다. **장치 전체 초기화** 필드에는 사용자 PIN 코드가 포함됩니다. 사용자는 장치가 초기화된 후 해당 코드를 입력해야 합니다. 사용자가 코드를 잊어버린 경우 여기에서 찾을 수 있습니다.

6. **속성** 페이지에는 XenMobile Server가 프로비저닝할 장치 속성이 나열됩니다. 이 목록에는 장치를 추가하는 데 사용된 프로비저닝 파일에 포함된 모든 장치 속성이 표시됩니다. 속성을 추가하려면 **추가**를 클릭

한 다음 목록에서 속성을 선택합니다. 각 속성에 대한 유효한 값은 PDF 장치 속성 이름 및 값을 참조하십시오.

속성을 추가하면 처음에 추가한 범주 아래에 나타납니다. **다음**을 클릭한 다음 **속성** 페이지로 돌아가면 해당 속성이 적절한 목록에 나타납니다.

속성을 삭제하려면 목록 위로 마우스를 가져간 다음 오른쪽에 있는 **X**를 클릭합니다. XenMobile Server는 항목을 즉시 삭제합니다.

7. 나머지 **장치 세부 정보** 섹션에는 장치에 대한 요약 정보가 있습니다.

- **사용자 속성:** RBAC 역할, 그룹 멤버십, 볼륨 구매 계정 및 사용자에 대한 속성을 표시합니다. 이 페이지에서 볼륨 구매 계정을 해제할 수 있습니다.
- **할당된 정책:** 배포됨, 보류 중, 실패한 정책 수를 포함하여 할당된 정책 수를 표시합니다. 각 정책에 대한 정책 이름, 유형 및 마지막 배포 정보를 제공합니다.
- **앱:** 마지막 인벤토리에 대해 설치됨, 보류 중, 실패한 앱 배포 수를 표시합니다. 앱 이름, 식별자, 유형 및 기타 정보를 제공합니다. **HasUpdateAvailable**과 같은 iOS 및 macOS 인벤토리 키에 대한 설명은 모바일 장치 관리(MDM) 프로토콜을 참조하십시오.
- **미디어:** 마지막 인벤토리에 대해 배포됨, 보류 중, 실패한 미디어 배포 수를 표시합니다.
- **작업:** 배포됨, 보류 중, 실패한 작업 수를 표시합니다. 작업 이름과 마지막 배포 시간을 제공합니다.
- **전달 그룹:** 성공, 보류 중, 실패한 전달 그룹 수를 표시합니다. 각 배포에 대해 전달 그룹 이름과 배포 시간을 제공합니다. 전달 그룹을 선택하여 상태, 작업, 채널 또는 사용자를 포함한 자세한 정보를 볼 수 있습니다.
- **iOS 프로필:** 이름, 유형, 조직 및 설명을 포함하여 마지막 iOS 프로필 인벤토리를 표시합니다.
- **iOS 프로비저닝 프로필:** UUID, 만료 날짜 및 관리 상태와 같은 엔터프라이즈 배포 프로비저닝 프로필 정보를 표시합니다.
- **인증서:** 유효, 만료 또는 해지된 인증서에 대해 유형, 공급자, 발급자, 일련 번호 및 만료까지 남은 일수와 같은 정보를 표시합니다.
- **연결:** 첫 번째 연결 상태와 마지막 연결 상태를 표시합니다. 각 연결에 대해 사용자 이름, 마지막에서 두 번째 인증 시간 및 마지막 인증 시간을 제공합니다.
- **MDM 상태:** MDM 상태, 마지막 푸시 시간 및 마지막 장치 응답 시간과 같은 정보를 표시합니다.

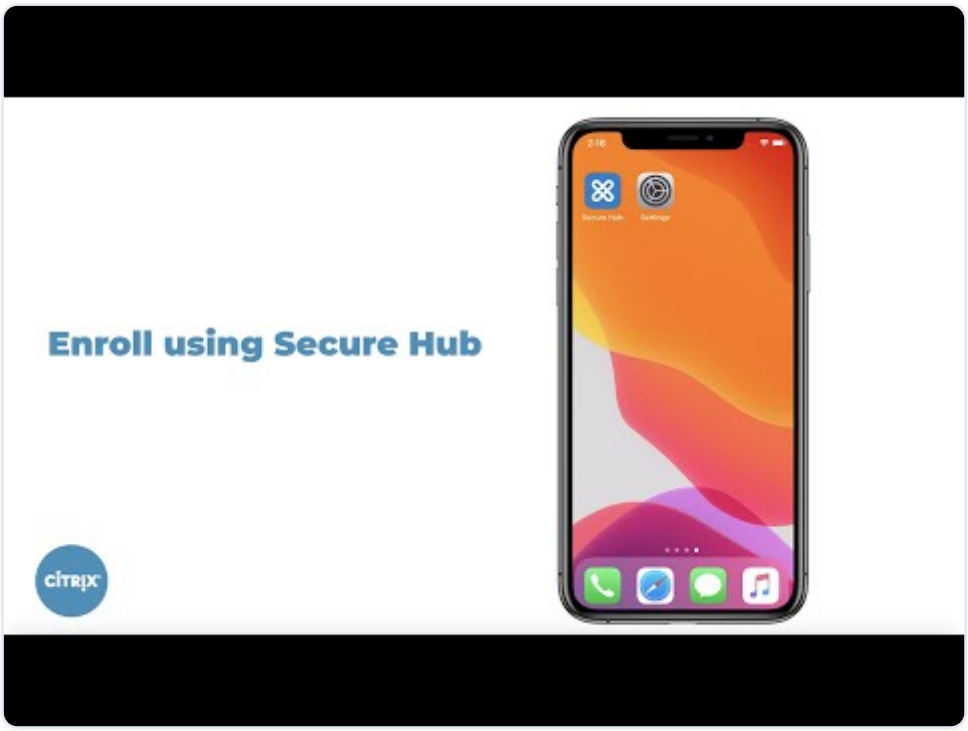
iOS 장치 정책 구성

이 정책을 사용하여 XenMobile Server가 iOS를 실행하는 장치와 상호 작용하는 방식을 구성합니다. 이 표에는 iOS 장치에 사용할 수 있는 모든 장치 정책이 나열되어 있습니다.

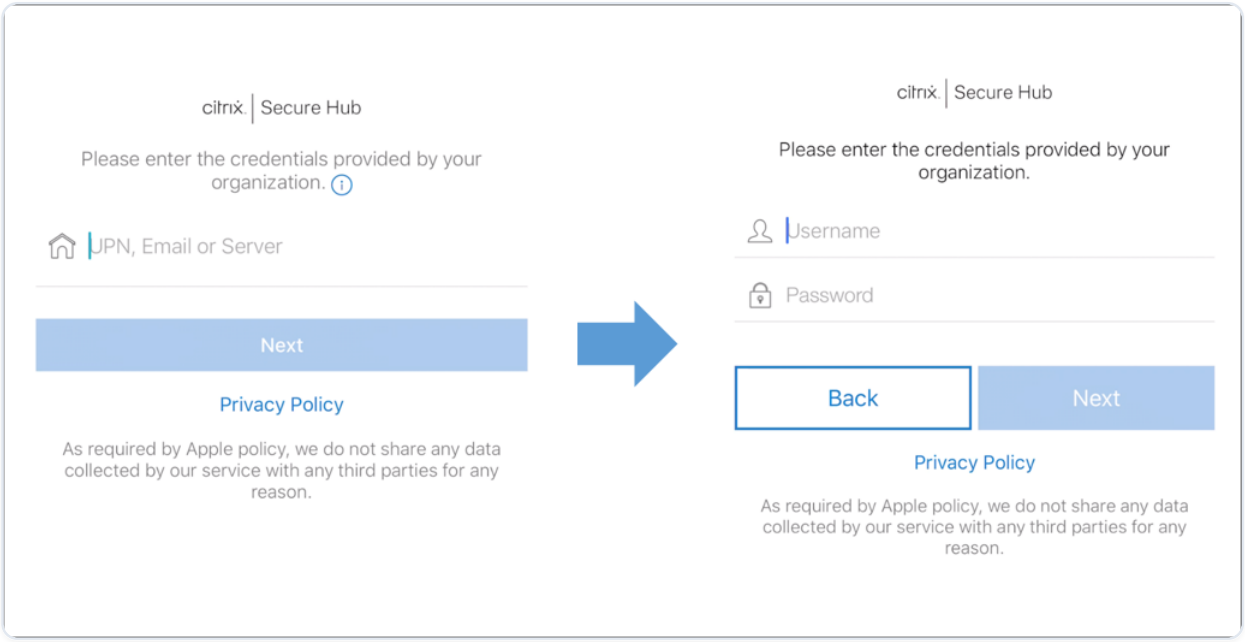
AirPlay 미러링	AirPrint	APN
앱 액세스	앱 속성	앱 구성
앱 인벤토리	앱 잠금	앱 네트워크 사용량
앱 제거	앱 알림	캘린더 (CalDAV)
셀룰러	연락처 (CardDAV)	OS 업데이트 제어
자격 증명	장치 이름	교육 구성
익스체인지	글꼴	홈 화면 레이아웃
iOS 및 macOS 프로필 가져오기	LDAP	위치
메일	관리되는 도메인	MDM 옵션
조직 정보	암호	개인용 핫스팟
프로필 제거	프로비저닝 프로필	프로비저닝 프로필 제거
프록시	제한 사항	로밍
SCEP	공유 iPad - 최대 상주 사용자	공유 iPad - 암호 잠금 유예 기간
SSO 계정	스토어	구독 캘린더
이용 약관	VPN	배경화면
웹 콘텐츠 필터	웹 클립	와이파이

iOS 장치 등록

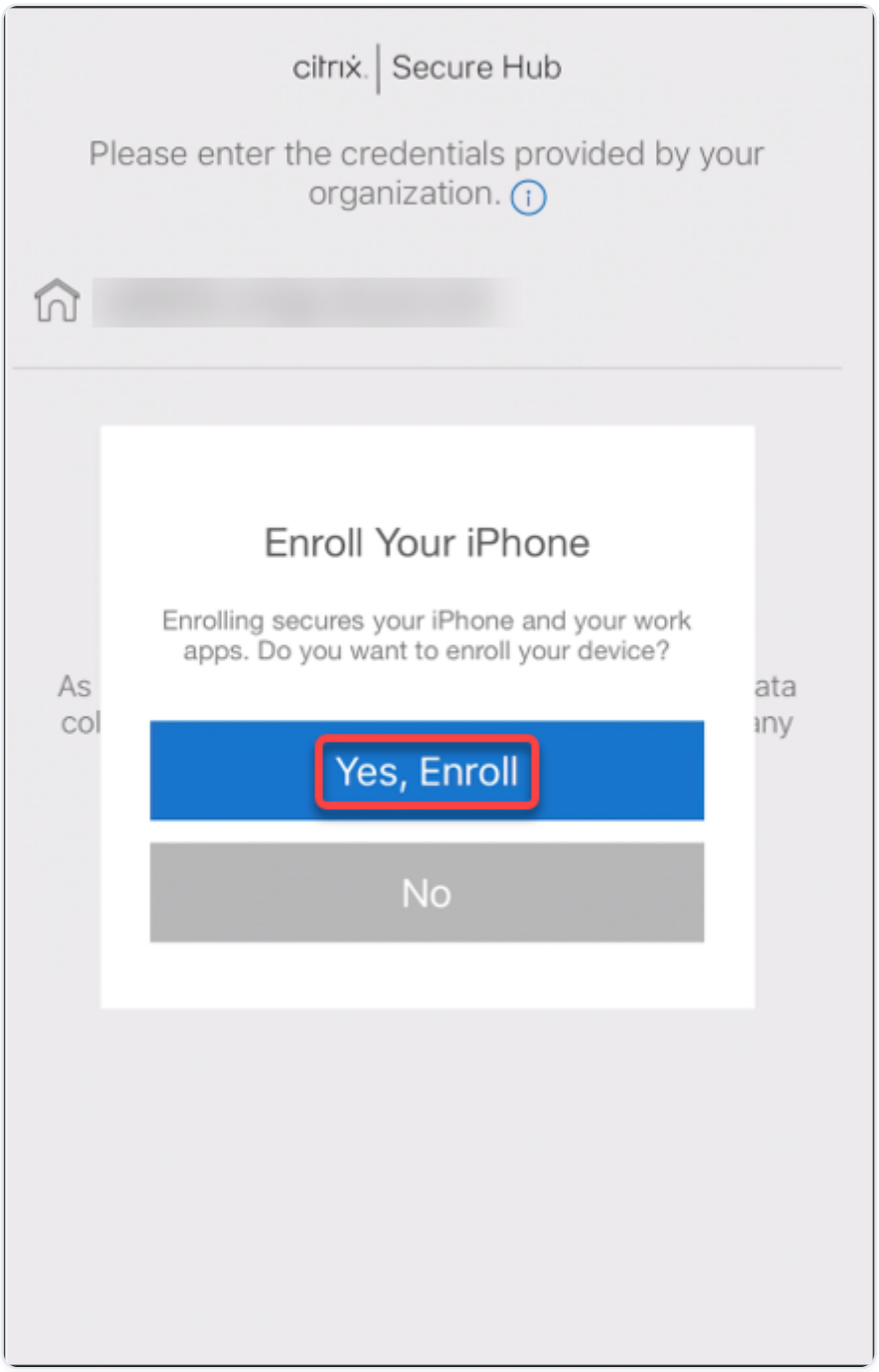
이 섹션에서는 사용자가 iOS 장치(12.2 이상)를 XenMobile Server에 등록하는 방법을 보여줍니다. iOS 등록에 대한 자세한 내용은 다음 비디오를 참조하십시오:



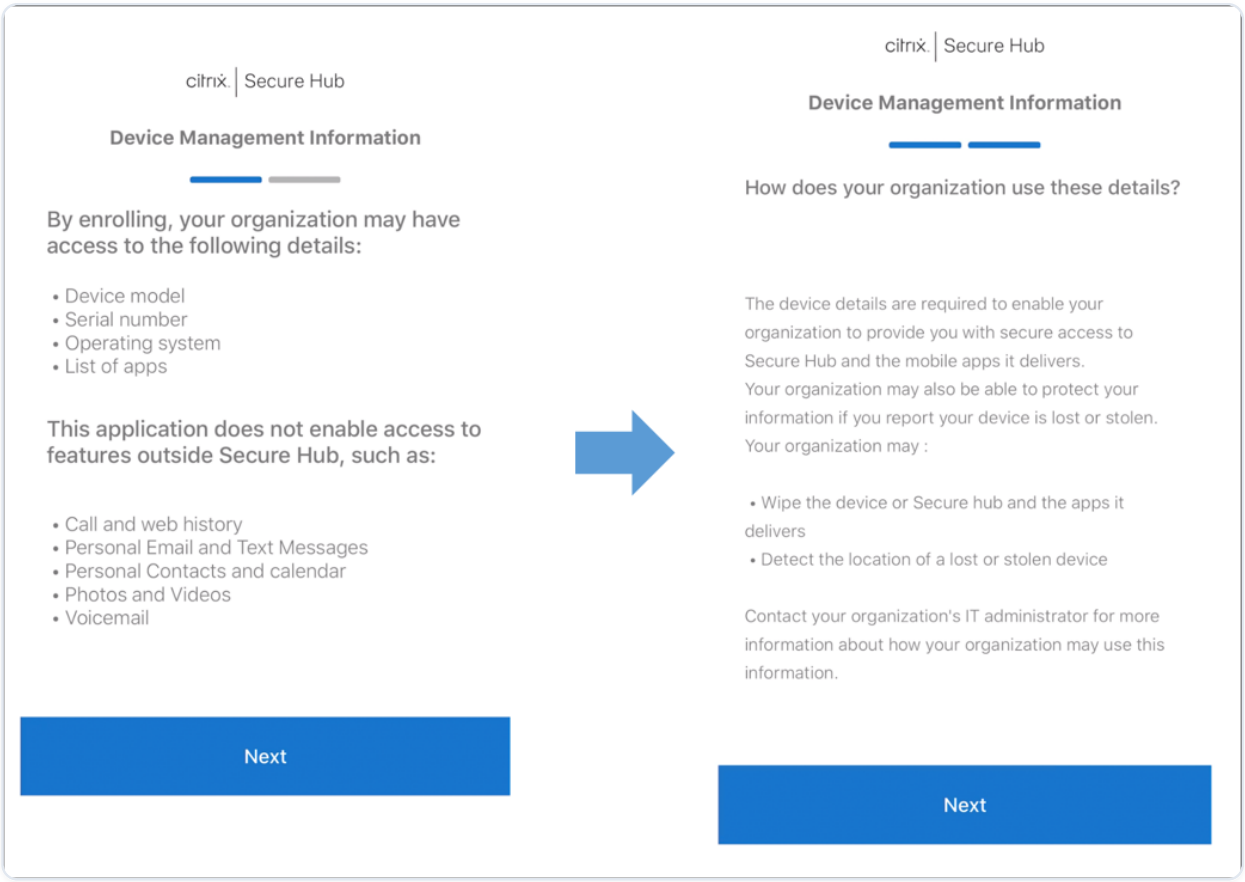
1. iOS 장치에서 Apple Store로 이동하여 Citrix Secure Hub™ 앱을 다운로드한 다음 앱을 탭합니다.
2. 앱 설치를 요청하면 **다음**을 탭한 다음 **설치**를 탭합니다.
3. Secure Hub가 설치되면 **열기**를 탭합니다.
4. XenMobile Server 서버 이름, UPN(사용자 계정 이름) 또는 이메일 주소와 같은 회사 자격 증명을 입력합니다. 그런 다음 **다음**을 클릭합니다.



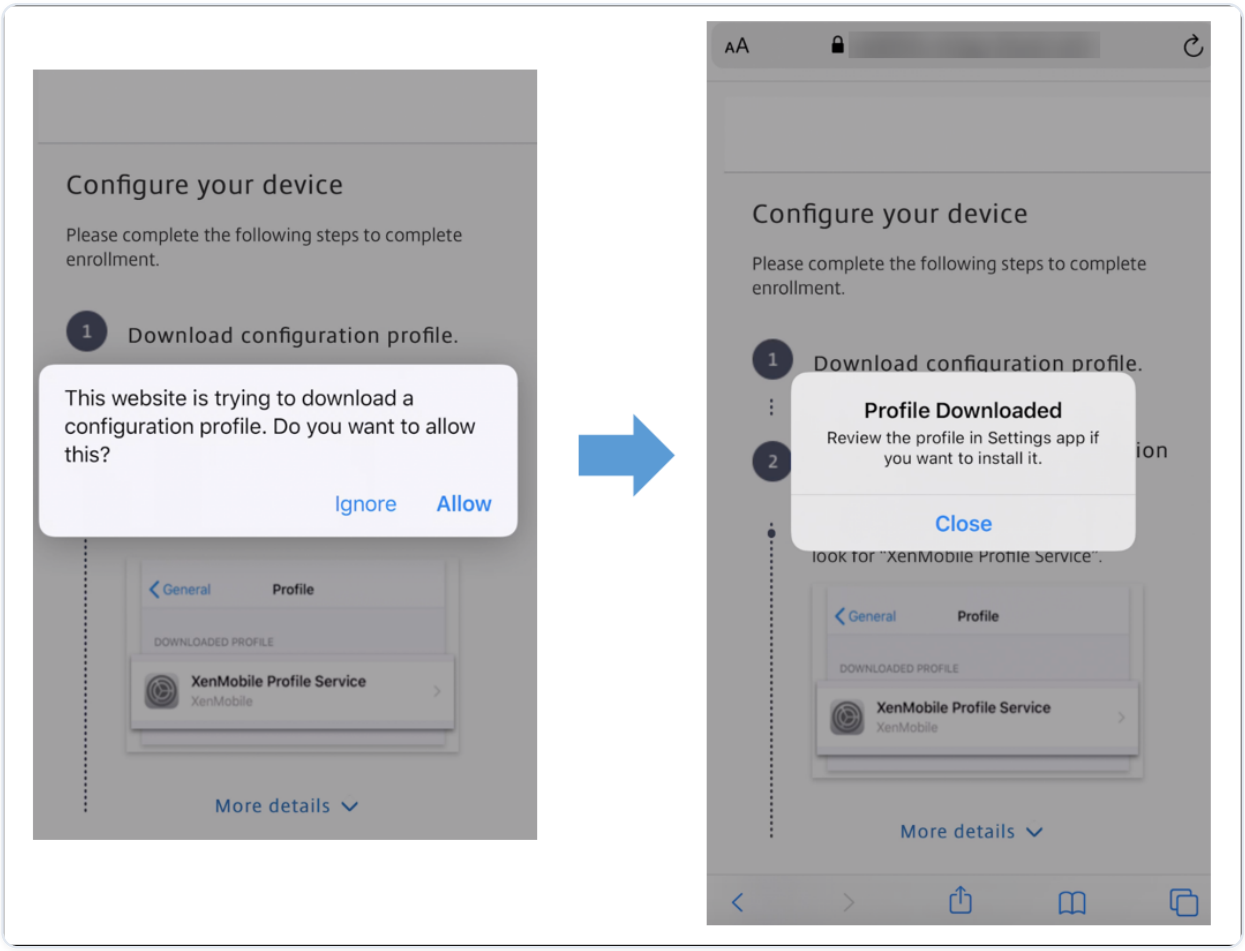
5. iOS 장치를 등록하려면 **예, 등록**을 탭합니다.



6. XenMobile Server가 수집하는 데이터 목록이 나타납니다. **다음**을 클릭합니다. 조직이 해당 데이터를 사용하는 방법에 대한 설명이 나타납니다. **다음**을 클릭합니다.



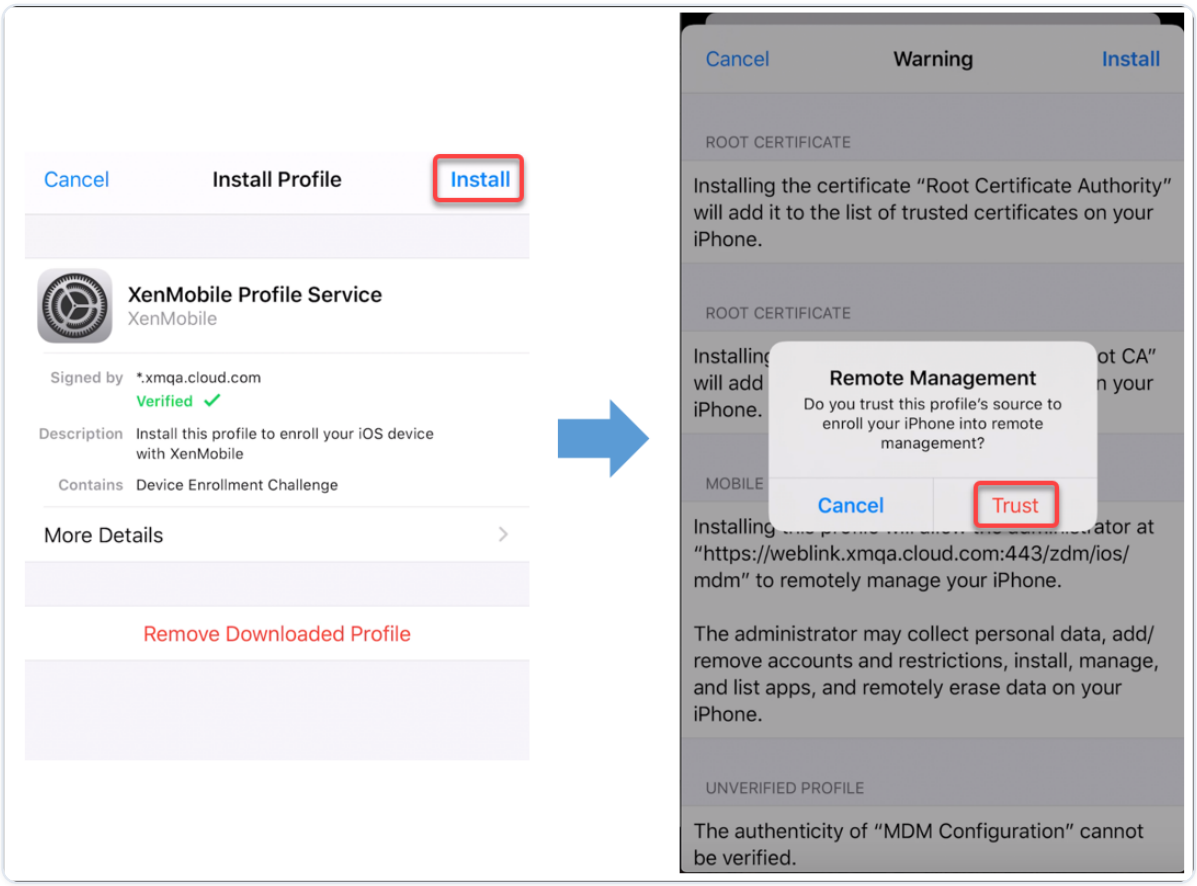
7. 자격 증명을 입력한 후 구성 프로필을 다운로드하라는 메시지가 표시되면 **허용**을 탭합니다. 구성 프로필을 다운로드한 후 **닫기**를 탭합니다.



8. 장치 설정에서 iOS 인증서를 설치하고 장치를 신뢰할 수 있는 목록에 추가합니다.

   - **설정 > 일반 > 프로필 > XenMobile 프로필 서비스**로 이동하여 **설치**를 탭하여 프로필을 추가합니다.

- 알림 창에서 **신뢰**를 탭하여 장치를 원격 관리로 등록합니다.



9. 등록이 성공하면 Secure Hub를 엽니다. MDM+MAM에 등록하는 경우: 자격 증명이 확인되면 메시지가 표시될 때 Citrix PIN을 생성하고 확인합니다.
10. 워크플로가 완료되면 장치가 등록됩니다. 그런 다음 앱 스토어에 액세스하여 iOS 장치에 설치할 수 있는 앱을 볼 수 있습니다.

보안 작업

iOS는 다음 보안 작업을 지원합니다. 각 보안 작업에 대한 설명은 보안 작업을 참조하십시오.

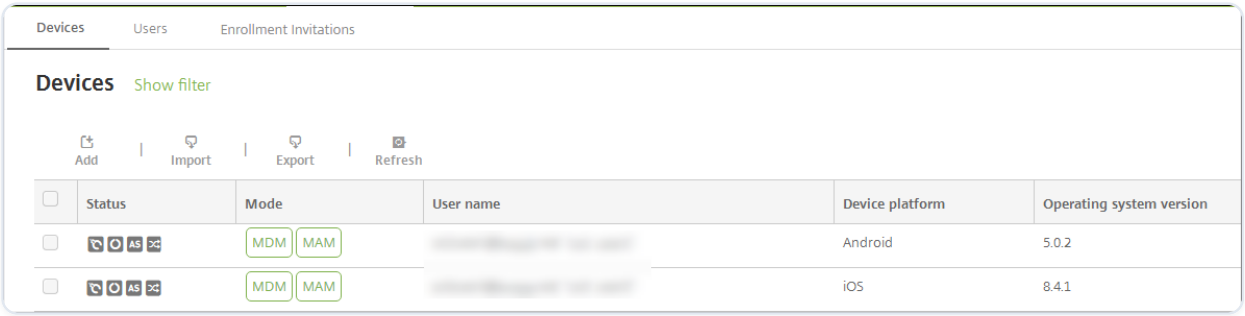
활성화 잠금 우회	앱 잠금	앱 초기화
ASM 활성화 잠금	인증서 갱신	제한 지우기
분실 모드 활성화/비활성화	추적 활성화/비활성화	전체 초기화
찾기	잠금	벨 울리기
AirPlay 미러링 요청/중지	다시 시작/종료	해지/승인
선택적 초기화	잠금 해제	

iOS 장치 잠금

분실된 iOS 장치를 잠글 수 있으며, 장치 잠금 화면에 메시지와 전화번호가 함께 표시됩니다.

잠긴 장치에 메시지와 전화번호를 표시하려면 XenMobile Server 콘솔에서 Passcode 정책을 **true**로 설정하십시오. 또는 사용자가 장치에서 수동으로 암호를 활성화할 수 있습니다.

1. **관리 > 장치**를 클릭합니다. **장치** 페이지가 나타납니다.



2. 잠그려는 iOS 장치를 선택합니다.

   장치 옆의 확인란을 선택하여 장치 목록 위에 옵션 메뉴를 표시합니다. 목록의 다른 곳을 클릭하여 목록 오른쪽에 옵션 메뉴를 표시합니다.

   옵션 메뉴(/en-us/xenmobile/server/media/manage-devices-with-commands-secure.png)

   옵션 메뉴(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-2.png)

3. 옵션 메뉴에서 **보안**을 클릭합니다. **보안 작업** 대화 상자가 나타납니다.

   보안 작업 대화 상자(/en-us/xenmobile/server/media/manage-devices-secure-lock.png)

4. **잠금**을 클릭합니다. **보안 작업** 확인 대화 상자가 표시됩니다.

   보안 작업 확인(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm.png)

5. 선택적으로 장치의 잠금 화면에 표시될 메시지와 전화번호를 입력합니다.

   iOS는 **메시지** 필드에 입력한 내용 뒤에 “Lost iPad”라는 단어를 추가합니다.

   메시지 필드를 비워두고 전화번호를 제공하면 Apple은 장치 잠금 화면에 “소유자에게 전화” 메시지를 표시합니다.

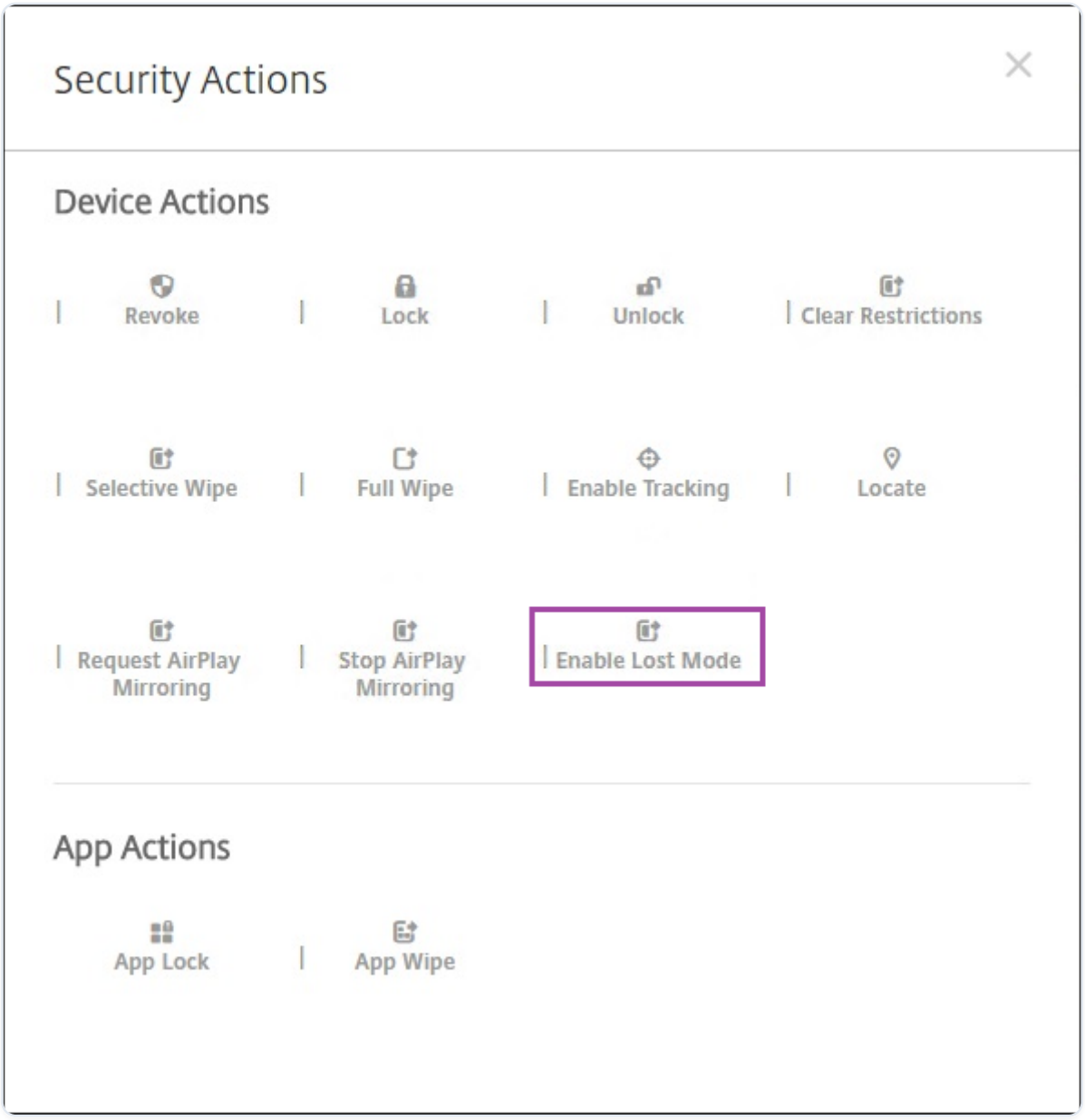
6. **장치 잠금**을 클릭합니다.

iOS 장치를 분실 모드로 전환

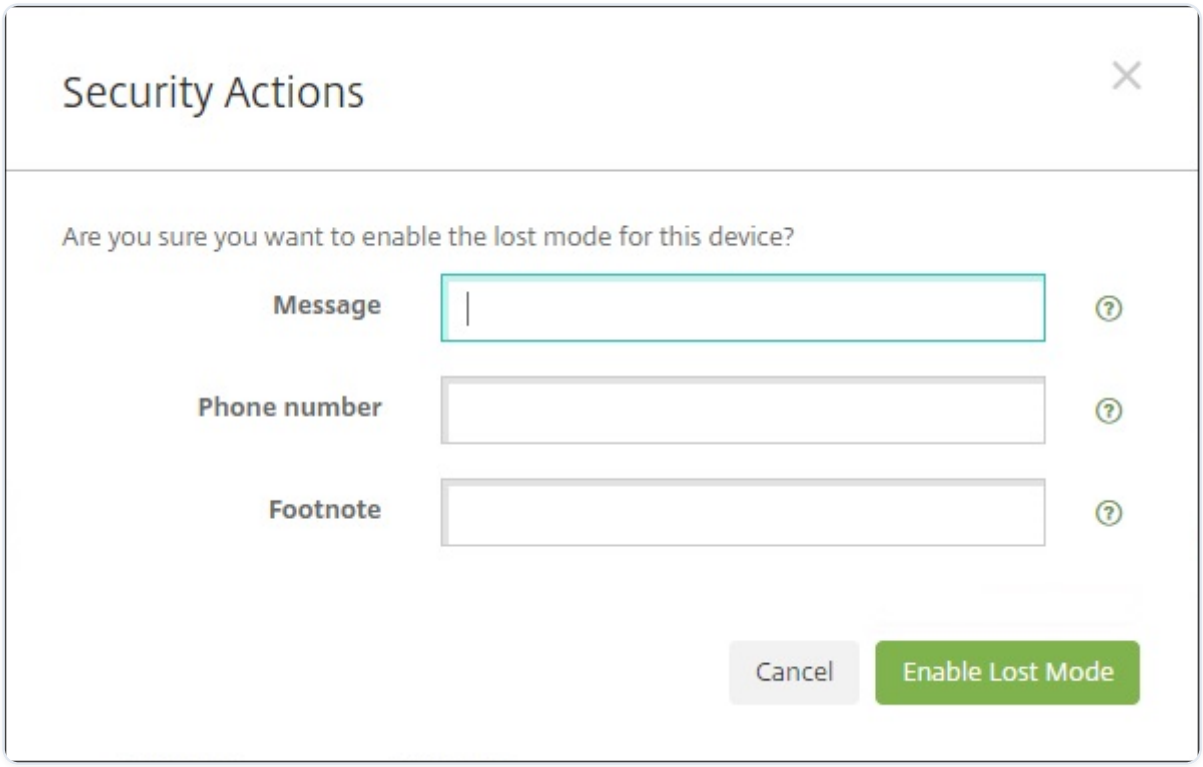
XenMobile Server 분실 모드 장치 속성은 iOS 장치를 분실 모드로 전환합니다. Apple 관리 분실 모드와 달리 XenMobile Server 분실 모드는 사용자가 장치 위치를 찾기 위해 다음 작업 중 하나를 수행할 필요가 없습니다. **나의 iPhone/iPad 찾기** 설정을 구성하거나 Citrix Secure Hub에 대한 위치 서비스를 활성화합니다.

XenMobile Server 분실 모드에서는 XenMobile Server만 장치를 잠금 해제할 수 있습니다. (대조적으로, XenMobile Server 장치 잠금 기능을 사용하는 경우 사용자는 제공된 PIN 코드를 사용하여 장치를 직접 잠금 해제할 수 있습니다.).

분실 모드를 활성화하거나 비활성화하려면: **관리 > 장치**로 이동하여 감독되는 iOS 장치를 선택한 다음 **보안**을 클릭합니다. 그런 다음 **분실 모드 활성화** 또는 **분실 모드 비활성화**를 클릭합니다.

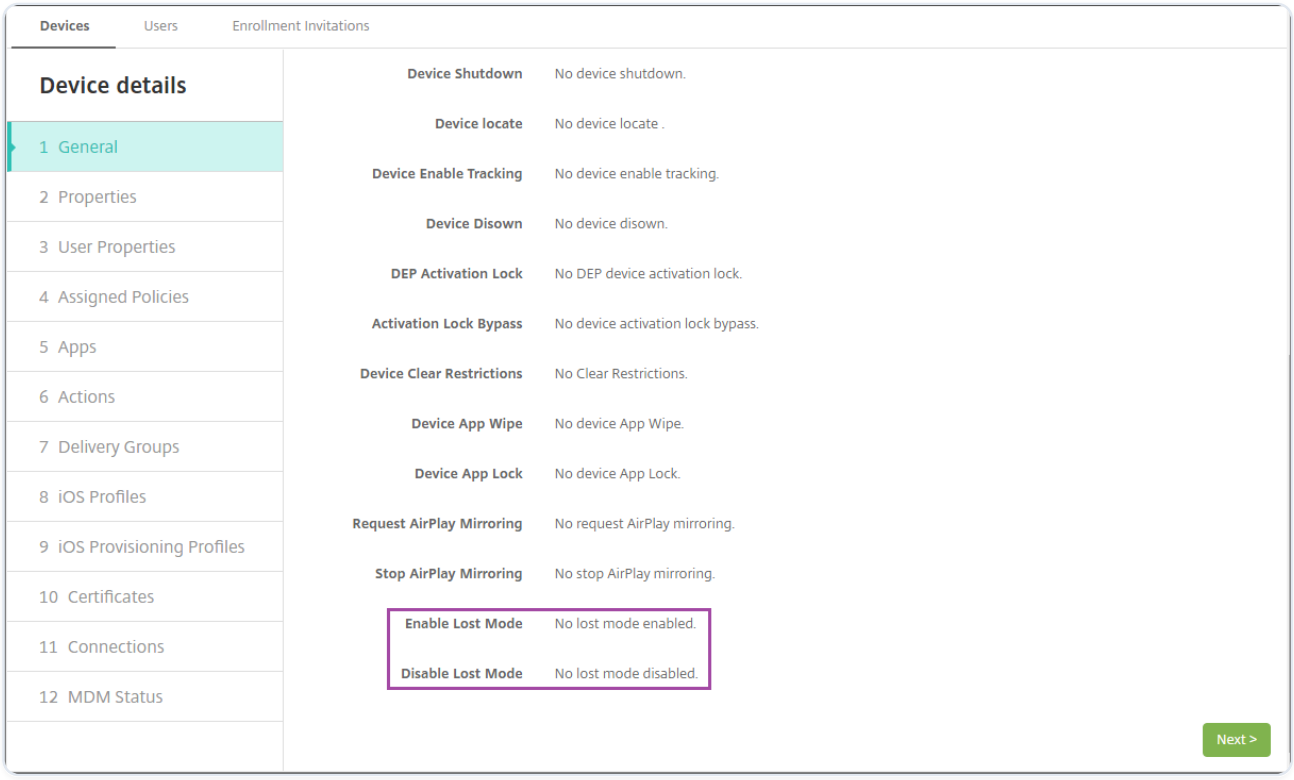


분실 모드 활성화를 클릭하면, 분실 모드일 때 장치에 표시될 정보를 입력합니다.

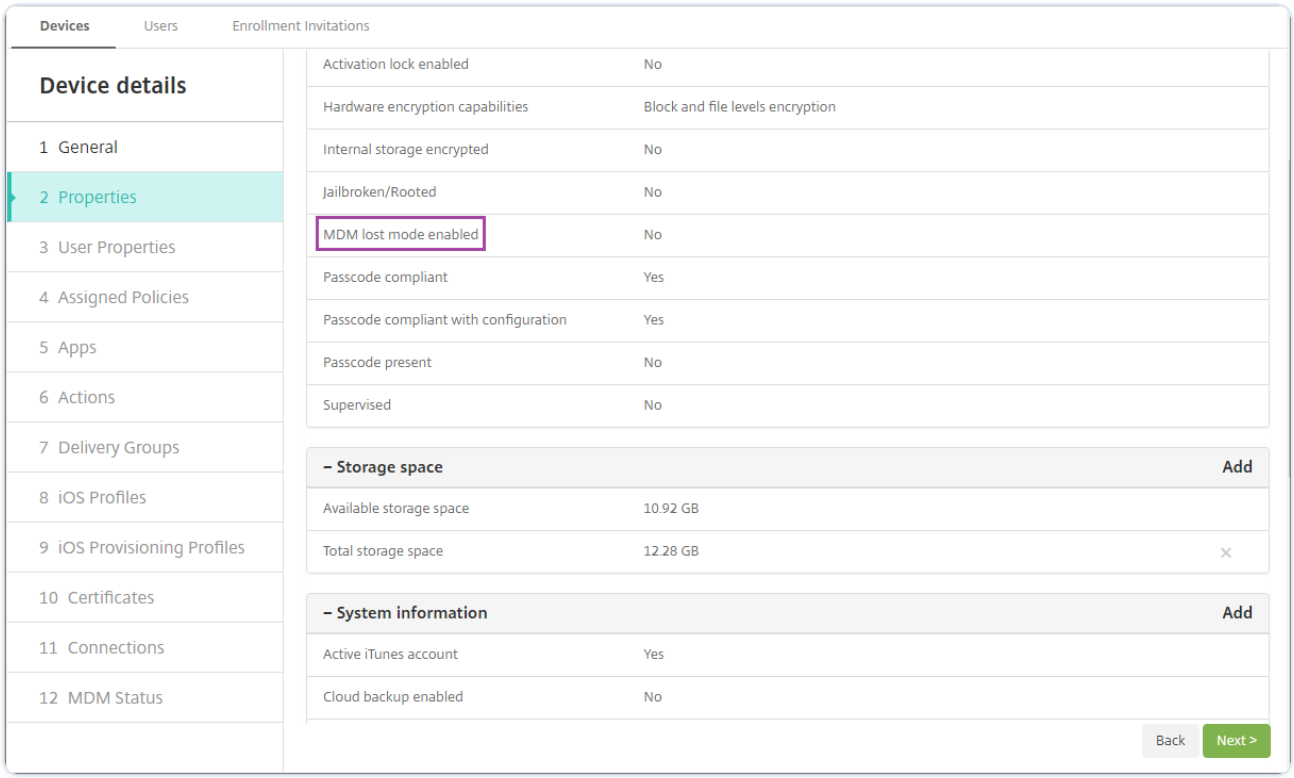


다음 방법 중 하나를 사용하여 분실 모드 상태를 확인합니다.

- **보안 작업** 창에서 버튼이 **분실 모드 비활성화**로 설정되어 있는지 확인합니다.
- **관리 > 장치**에서 **보안** 아래의 **일반** 탭에서 마지막 분실 모드 활성화 또는 분실 모드 비활성화 작업을 확인합니다.



- **관리 > 장치**에서 **속성** 탭에서 **MDM 분실 모드 활성화됨** 설정 값이 올바른지 확인합니다.



iOS 장치에서 XenMobile Server 분실 모드를 활성화하면 XenMobile Server 콘솔도 다음과 같이 변경됩니다.

- **구성 > 작업**에서 **작업** 목록에 다음 자동 작업이 포함되지 않습니다. **장치 해지**, **장치 선택적 초기화**, **장치 완전 초기화**.
- **관리 > 장치**에서 **보안 작업** 목록에 더 이상 **해지** 및 **선택적 초기화** 장치 작업이 포함되지 않습니다. 필요에 따라 보안 작업을 사용하여 **전체 초기화** 작업을 수행할 수 있습니다.

iOS는 **보안 작업** 화면의 **메시지**에 입력한 내용에 "Lost iPad"라는 단어를 추가합니다.

메시지를 비워두고 전화번호를 제공하면 Apple은 장치 잠금 화면에 "Call owner" 메시지를 표시합니다.

iOS 활성화 잠금 우회

활성화 잠금은 분실되거나 도난당한 감독 대상 기기의 재활성화를 방지하는 나의 iPhone/iPad 찾기 기능입니다. 활성화 잠금은 다음 작업을 수행하기 전에 사용자 Apple ID와 암호를 요구합니다. 나의 iPhone/iPad 찾기 끄기, 기기 지우기 또는 기기 재활성화. 조직이 소유한 기기의 경우, 예를 들어 기기를 재설정하거나 재할당하려면 활성화 잠금을 우회해야 합니다.

활성화 잠금을 활성화하려면 XenMobile Server MDM 옵션 기기 정책을 구성하고 배포합니다. 그러면 사용자의 Apple 자격 증명 없이 XenMobile Server 콘솔에서 기기를 관리할 수 있습니다. 활성화 잠금의 Apple 자격 증명 요구 사항을 우회하려면 XenMobile Server 콘솔에서 활성화 잠금 우회 보안 작업을 실행합니다.

예를 들어, 사용자가 분실한 휴대폰을 반환하거나 전체 초기화 전후에 기기를 설정하는 경우: 휴대폰에서 Apple App Store 계정 자격 증명을 요구하면 XenMobile Server 콘솔에서 활성화 잠금 우회 보안 작업을 실행하여 해당 단계를 우회할 수 있습니다.

활성화 잠금 우회를 위한 기기 요구 사항

- Apple Configurator 또는 Apple 배포 프로그램을 통해 감독됨
- iCloud 계정으로 구성됨
- 나의 iPhone/iPad 찾기 활성화됨
- XenMobile Server에 등록됨
- 활성화 잠금이 활성화된 MDM 옵션 기기 정책이 기기에 배포됨

기기를 전체 초기화하기 전에 활성화 잠금을 우회하려면 다음을 수행합니다.

1. **관리 > 기기**로 이동하여 기기를 선택하고 **보안**을 클릭한 다음 **활성화 잠금 우회**를 클릭합니다.
2. 기기를 초기화합니다. 기기 설정 중에 활성화 잠금 화면이 나타나지 않습니다.

기기를 전체 초기화한 후 활성화 잠금을 우회하려면 다음을 수행합니다.

1. 기기를 재설정하거나 초기화합니다. 기기 설정 중에 활성화 잠금 화면이 나타납니다.
2. **관리 > 기기**로 이동하여 기기를 선택하고 **보안**을 클릭한 다음 **활성화 잠금 우회**를 클릭합니다.
3. 장치에서 뒤로 버튼을 탭합니다. 홈 화면이 나타납니다.

다음 사항을 유의하십시오.

- 사용자에게 나의 iPhone/iPad 찾기를 끄지 않도록 권고하십시오. 장치에서 전체 초기화를 수행하지 마십시오. 두 경우 모두 사용자에게 iCloud 계정 암호를 입력하라는 메시지가 표시됩니다. 계정 유효성 검사 후, 모든 콘텐츠 및 설정을 지운 후에는 사용자에게 iPhone/iPad 활성화 화면이 표시되지 않습니다.
- 생성된 활성화 잠금 우회 코드가 있고 활성화 잠금이 활성화된 장치의 경우: 전체 초기화 후 iPhone/iPad 활성화 페이지를 우회할 수 없는 경우, XenMobile Server에서 장치를 삭제할 필요가 없습니다. 관리자 또는 사용자가 Apple 지원에 문의하여 장치를 직접 차단 해제할 수 있습니다.
- 하드웨어 인벤토리 중에 XenMobile Server는 장치에 활성화 잠금 우회 코드를 쿼리합니다. 우회 코드가 사용 가능한 경우, 장치는 이를 XenMobile Server로 보냅니다. 그런 다음 장치에서 우회 코드를 제거하려면 XenMobile Server 콘솔에서 활성화 잠금 우회 보안 작업을 보냅니다. 이 시점에서 XenMobile Server와 Apple은 장치 차단 해제에 필요한 우회 코드를 갖게 됩니다.
- 활성화 잠금 우회 보안 작업은 Apple 서비스의 가용성에 따라 달라집니다. 작업이 작동하지 않으면 다음과 같이 장치를 차단 해제할 수 있습니다. 장치에서 iCloud 계정 자격 증명을 수동으로 입력합니다. 또는 사용자 이름 필드를 비워두고 암호 필드에 우회 코드를 입력합니다. 우회 코드를 찾으려면 **관리 > 장치**로

이동하여 장치를 선택하고 **편집**을 클릭한 다음 **속성**을 클릭합니다. **활성화 잠금 우회 코드**는 **보안 정보** 아래에 있습니다.

macOS

XenMobile에서 macOS 장치를 관리하려면 Apple에서 Apple 푸시 알림 서비스(APNs) 인증서를 설정해야 합니다. 자세한 내용은 APNs 인증서를 참조하십시오.

XenMobile®은 macOS 장치를 MDM에 등록합니다. XenMobile은 MDM에서 macOS 장치에 대해 다음 등록 인증 유형을 지원합니다.

- 도메인
- 도메인 및 일회용 암호
- 초대 URL 및 일회용 암호

> **macOS 15에서 신뢰할 수 있는 인증서 요구 사항:**

> Apple은 TLS 서버 인증서에 대한 새로운 요구 사항을 발표했습니다. 모든 인증서가 새로운 Apple 요구 사항을 따르는지 확인하십시오. Apple 발행물 `<https://support.apple.com/ko-kr/HT210176>`을 참조하십시오. 인증서 관리에 대한 도움말은 XenMobile에서 인증서 업로드를 참조하십시오.

> macOS 장치 관리를 시작하기 위한 일반적인 워크플로는 다음과 같습니다.

1. macOS 장치 정책 구성.
2. macOS 장치 등록.
3. 장치 및 앱 보안 작업을 설정합니다. 보안 작업을 참조하십시오.

지원되는 운영 체제에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오.

열려 있어야 하는 Apple 호스트 이름

iOS, macOS 및 Apple App Store의 올바른 작동을 보장하려면 일부 Apple 호스트 이름이 열려 있어야 합니다. 해당 호스트 이름을 차단하면 다음의 설치, 업데이트 및 올바른 작동에 영향을 미칠 수 있습니다. iOS, iOS 앱, MDM 작동, 장치 및 앱 등록. 자세한 내용은 `<https://support.apple.com/ko-kr/HT201999>`을 참조하십시오.

지원되는 등록 방법

다음 표에는 XenMobile이 macOS 기기에 대해 지원하는 등록 방법이 나와 있습니다.

방법	지원됨
Apple 배포 프로그램	예
애플 스쿨 매니저	예
애플 컨피규레이터	아니요
수동 등록	예
등록 초대	예

Apple은 비즈니스 및 교육 계정을 위한 기기 등록 프로그램을 제공합니다. 비즈니스 계정의 경우, XenMobile에서 기기 등록 및 관리를 위해 Apple Deployment Program을 사용하려면 Apple Deployment Program에 등록해야 합니다. 이 프로그램은 iOS 및 macOS 기기용입니다. Apple Deployment Program을 통한 기기 배포를 참조하십시오.

교육 계정의 경우 Apple School Manager 계정을 생성합니다. Apple School Manager는 배포 프로그램과 대량 구매를 통합합니다. Apple School Manager는 교육용 Apple 배포 프로그램의 한 유형입니다. Apple 교육 기능과 통합을 참조하십시오.

Apple 배포 프로그램을 사용하여 iOS 및 macOS 장치를 대량으로 등록할 수 있습니다. 해당 장치는 Apple, 참여 Apple 공인 리셀러 또는 통신사에서 직접 구매할 수 있습니다.

macOS 장치 정책 구성

이러한 정책을 사용하여 XenMobile이 macOS를 실행하는 장치와 상호 작용하는 방식을 구성합니다. 이 표에는 macOS 장치에 사용할 수 있는 모든 장치 정책이 나열되어 있습니다.

AirPlay 미러링	앱 인벤토리	캘린더 (CalDAV)
연락처 (CardDAV)	OS 업데이트 제어	자격 증명
방화벽	글꼴	iOS 및 macOS 프로필 가져오기
LDAP	메일	암호

프로필 제거	제한	SCEP
VPN	웹 클립	와이파이

macOS 장치 등록

XenMobile은 macOS를 실행하는 장치를 등록하는 두 가지 방법을 제공합니다. 두 가지 방법 모두 macOS 사용자가 장치에서 직접 무선으로 등록할 수 있도록 합니다.

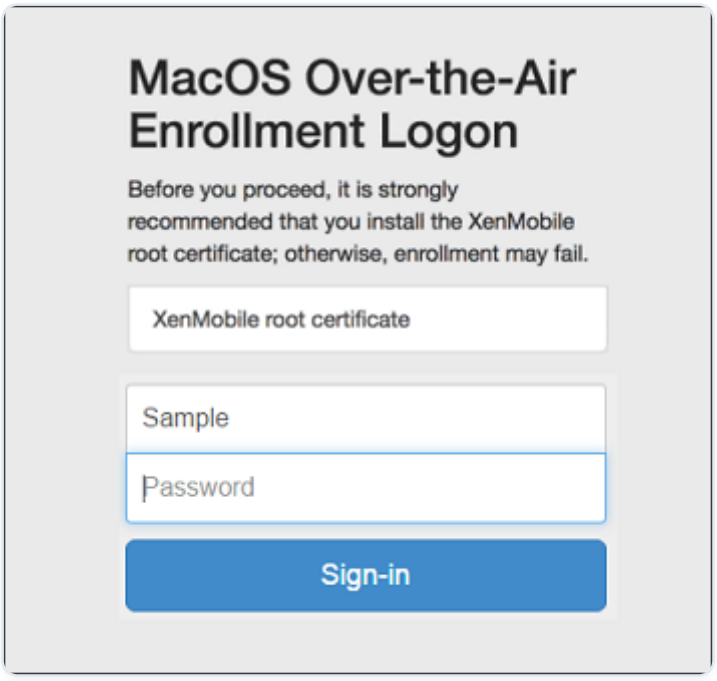
- **사용자에게 등록 초대 보내기:** 이 등록 방법을 사용하면 macOS 장치에 대해 다음 등록 보안 모드 중 하나를 설정할 수 있습니다.
  - 사용자 이름 + 암호
  - 사용자 이름 + PIN
  - 2단계 인증

  사용자가 등록 초대장의 지침을 따르면 사용자 이름이 채워진 로그인 화면이 나타납니다.
- **사용자에게 등록 링크 보내기:** macOS 장치용 이 등록 방법은 사용자에게 등록 링크를 보내며, 사용자는 이 링크를 Safari 또는 Chrome 브라우저에서 열 수 있습니다. 그런 다음 사용자는 사용자 이름과 암호를 제공하여 등록합니다.

  macOS 장치에 등록 링크를 사용하는 것을 방지하려면 서버 속성 **Enable macOS OTAE**를 **false**로 설정하십시오. 결과적으로 macOS 사용자는 등록 초대를 통해서만 등록할 수 있습니다.

macOS 사용자에게 등록 초대 보내기

1. macOS 사용자 등록을 위한 초대를 추가합니다. 등록 초대 만들기를 참조하십시오.
2. 사용자가 초대를 받고 링크를 클릭하면 Safari 브라우저에 다음 화면이 나타납니다. XenMobile이 사용자 이름을 채웁니다. 등록 보안 모드로 **2단계**를 선택한 경우 다른 필드가 나타납니다.



3. 사용자는 필요에 따라 인증서를 설치합니다. 사용자가 인증서 설치 프롬프트를 볼지 여부는 macOS에 대해 다음을 구성했는지에 따라 달라집니다: 공개적으로 신뢰할 수 있는 SSL 인증서 및 공개적으로 신뢰할 수 있는 디지털 서명 인증서. 인증서에 대한 자세한 내용은 인증서 및 인증을 참조하십시오.
4. 사용자는 요청된 자격 증명을 제공합니다.

   Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하는 것과 마찬가지로 XenMobile을 사용하여 macOS 장치를 관리할 수 있습니다.

macOS 사용자에게 설치 링크 보내기

1. 사용자가 Safari 또는 Chrome 브라우저에서 열 수 있는 등록 링크 `https://serverFQDN:8443/instanceName/macos/otae`를 보냅니다.

   - **serverFQDN**은 XenMobile을 실행하는 서버의 정규화된 도메인 이름(FQDN)입니다.
   - 포트 **8443**은 기본 보안 포트입니다. 다른 포트를 구성한 경우 8443 대신 해당 포트를 사용하십시오.
   - The **instanceName**은(는) 종종 `zdm`으로 표시되며, 서버 설치 중에 지정된 이름입니다.

   설치 링크 전송에 대한 자세한 내용은 등록 초대 보내기를 참조하십시오.
2. 사용자는 필요에 따라 인증서를 설치합니다. iOS 및 macOS용으로 공개적으로 신뢰할 수 있는 SSL 인증서와 디지털 서명 인증서를 구성한 경우, 사용자에게 인증서 설치 프롬프트가 표시됩니다. 인증서에 대한 자세한 내용은 인증서 및 인증을 참조하십시오.
3. 사용자가 Mac에 로그인합니다.

   Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하는 것과 마찬가지로 XenMobile을 사용하여 macOS 장치를 관리할 수 있습니다.

보안 작업

macOS는 다음 보안 작업을 지원합니다. 각 보안 작업에 대한 설명은 보안 작업을 참조하십시오.

취소	잠금	선택적 초기화
전체 초기화	인증서 갱신	

macOS 장치 잠금

분실된 macOS 장치를 원격으로 잠글 수 있습니다. XenMobile은 장치를 잠그고 PIN 코드를 생성하여 장치에 설정합니다. 장치에 액세스하려면 사용자가 PIN 코드를 입력해야 합니다. XenMobile 콘솔에서 잠금을 해제하려면 **잠금 취소**를 사용하십시오.

PIN 코드와 관련된 추가 설정을 구성하려면 암호 장치 정책을 사용할 수 있습니다. 자세한 내용은 macOS 설정을 참조하십시오.

1. **관리 > 장치**를 클릭합니다. **장치** 페이지가 나타납니다.

   장치 페이지(/en-us/xenmobile/server/media/manage-devices-macos.png)

2. 잠그려는 macOS 장치를 선택합니다.

   장치 옆의 확인란을 선택하여 장치 목록 위에 옵션 메뉴를 표시합니다. 나열된 항목의 다른 아무 곳이나 클릭하여 목록 오른쪽에 옵션 메뉴를 표시할 수도 있습니다.

   옵션 메뉴(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos.png)

   옵션 메뉴(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos-2.png)

3. 옵션 메뉴에서 **보안**을 클릭합니다. **보안 작업** 대화 상자가 나타납니다.

   보안 작업 대화 상자(/en-us/xenmobile/server/media/manage-devices-secure-lock-macos.png)

4. **잠금**을 클릭합니다. **보안 작업** 확인 대화 상자가 표시됩니다.

   보안 작업 확인(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm-macos.png)

5. **장치 잠금**을 클릭합니다.

> **중요:**

> XenMobile이 생성하는 코드 대신 암호를 지정할 수도 있습니다. 지정된 코드가 장치 또는 기존 작업 프로필의 코드 요구 사항을 충족하지 않으면 잠금 작업이 실패합니다.

Apple 기기 대량 등록

두 가지 방법으로 많은 수의 iOS, iPadOS 및 macOS 기기를 XenMobile®에 등록할 수 있습니다.

- Apple, 참여 Apple 공인 리셀러 또는 통신사로부터 직접 구매한 iOS, iPadOS 및 macOS 기기를 등록하려면 Apple 배포 프로그램을 사용하십시오. 이 지원에는 공유 iPad가 포함됩니다. XenMobile은 교육용 Apple Business Manager(ABM) 및 Apple School Manager(ASM)에 대한 Apple 배포 프로그램을 지원합니다. 이 문서에서는 여러 기기를 ABM 계정과 통합하는 방법을 설명합니다. ABM 등록 및 ABM 계정을 XenMobile과 연결하는 방법에 대한 자세한 내용은 Apple 배포 프로그램을 통해 기기 배포를 참조하십시오. Apple School Manager 계정에 대한 자세한 내용은 Apple 교육 기능과 통합을 참조하십시오.

  macOS 기기 등록의 경우 XenMobile은 기기가 macOS 10.10 이상을 실행해야 합니다.
- Apple에서 직접 구매했는지 여부와 관계없이 Apple Configurator 2를 사용하여 iOS 기기를 등록할 수도 있습니다.

ABM 사용 시:

- 기기를 만지거나 준비할 필요가 없습니다. 대신 ABM을 통해 기기 일련 번호 또는 구매 주문 번호를 제출하여 기기를 구성하고 등록합니다.
- XenMobile이 기기를 등록한 후에는 사용자에게 기기를 제공하여 즉시 사용할 수 있도록 할 수 있습니다. ABM으로 기기를 설정할 때 사용자가 기기를 처음 시작할 때 완료해야 할 수 있는 일부 설정 지원 단계를 제거할 수 있습니다.
- ABM 설정에 대한 자세한 내용은 Apple Business Manager에서 제공되는 설명서를 참조하십시오.

Apple Configurator 2 사용 시:

- macOS 10.7.2 이상 및 Apple Configurator 2 앱을 실행하는 Apple 컴퓨터에 iOS 기기를 연결합니다. Apple Configurator 2를 통해 iOS 기기를 준비하고 정책을 구성합니다.
- 필요한 정책으로 기기를 프로비저닝한 후 기기가 XenMobile에 처음 연결될 때 XenMobile에서 정책을 수신합니다. 그런 다음 기기 관리를 시작할 수 있습니다.
- Apple Configurator 2 사용에 대한 자세한 내용은 Apple Configurator 도움말을 참조하십시오.

전제 조건

XenMobile과 Apple 간의 연결에 필요한 포트를 엽니다. 자세한 내용은 포트 요구 사항을 참조하십시오.

Apple Business Manager 계정을 XenMobile과 통합

XenMobile에 ABM 계정이 설정되어 있지 않은 경우, Apple 배포 프로그램을 통해 장치 배포에서 다음 단계를 완료하십시오.

- Apple Business Manager에 등록합니다.
- Apple Business Manager 계정을 XenMobile에 연결합니다.
- 배포 프로그램이 활성화된 장치를 주문합니다.
- 배포 프로그램이 활성화된 장치를 관리합니다.

대량 등록을 위한 기본 서버 설정

대량의 iOS, iPadOS 및 macOS 장치를 MDM 서버에 할당하려면 XenMobile을 기본 서버로 설정할 수 있습니다.

1. 관리자 또는 장치 등록 관리자 계정을 사용하여 Apple Business Manager에 로그인합니다.
2. 사이드바에서 **설정 > 장치 관리 설정**을 클릭합니다.
3. 기존 MDM 서버를 선택합니다. **기본 장치 할당**에서 **변경**을 클릭합니다. 각 장치 유형에 대한 기본 XenMobile 서버를 선택합니다. **완료**를 클릭합니다.

ABM 계정에 대한 장치 정책 및 앱 배포 규칙 구성

구성 > 장치 정책 및 **구성 > 앱** 아래의 **배포 규칙** 섹션을 사용하여 ABM 계정을 다른 장치 정책 및 앱과 연결할 수 있습니다. 정책 또는 앱이 다음 중 하나를 수행하도록 지정할 수 있습니다.

- 특정 ABM 계정에만 배포합니다.
- 선택한 계정을 제외한 모든 ABM 계정에 배포합니다.

ABM 계정 목록에는 활성화 또는 비활성화 상태의 계정만 포함됩니다. ABM 계정이 비활성화된 경우 ABM 장치는 이 계정에 속하지 않습니다. 따라서 XenMobile은 앱이나 정책을 장치에 배포하지 않습니다.

다음 예에서 장치 정책은 ABM 계정 이름이 "ABM Account NR"인 장치에만 배포됩니다.

Apple 장치 프로그램 설정 화면(/en-us/xenmobile/server/media/apple-dep-deployment-rule-policy-example.png)

Apple 배포 프로그램 지원 장치 등록 시 사용자 경험

사용자가 Apple 배포 프로그램 지원 장치를 등록할 때의 경험은 다음과 같습니다.

1. 사용자가 Apple 배포 프로그램 지원 장치를 시작합니다.

2. XenMobile은 XenMobile 콘솔에서 구성한 Apple 배포 프로그램 구성을 Apple 배포 프로그램 지원 장치에 전달합니다.
3. 사용자가 장치에서 초기 설정을 구성합니다.
4. 장치가 XenMobile 장치 등록 프로세스를 자동으로 시작합니다.
5. 사용자가 장치에서 다른 초기 설정을 계속 구성합니다.
6. 홈 화면에서 사용자는 Citrix Secure Hub를 다운로드하기 위해 Apple App Store에 로그인하라는 메시지가 표시될 수 있습니다.

   > **참고:**
   >
   > 장치 기반 볼륨 구매 앱 할당을 사용하여 Secure Hub 앱을 배포하도록 XenMobile을 구성하는 경우 이 단계는 선택 사항입니다. 이 경우 Apple App Store 계정을 만들거나 기존 계정을 사용할 필요가 없습니다.

   > Apple 배포 프로그램 설정(/en-us/xenmobile/server/media/ios-dep-54.png)

7. 사용자가 Secure Hub를 열고 자격 증명을 입력합니다. 정책에 필요한 경우 사용자에게 Citrix PIN을 생성하고 확인하라는 메시지가 표시될 수 있습니다.

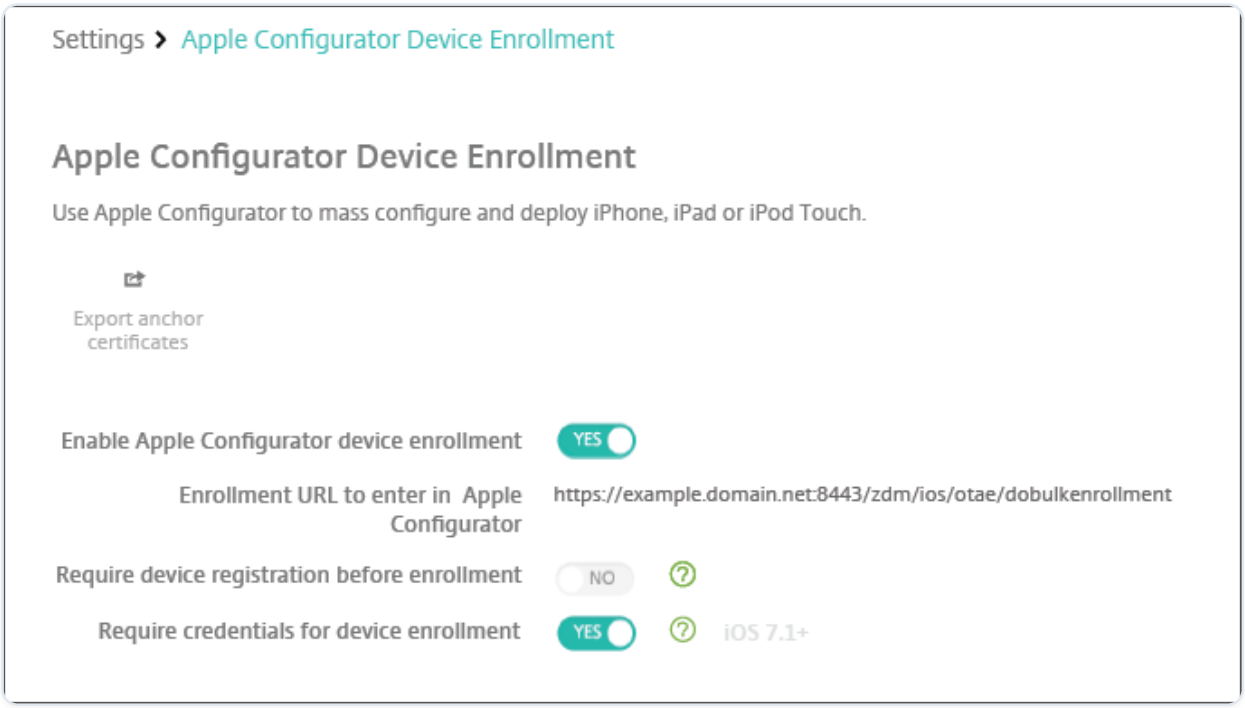
   XenMobile은 나머지 필수 앱을 장치에 배포합니다.

Apple Configurator 2 설정 구성

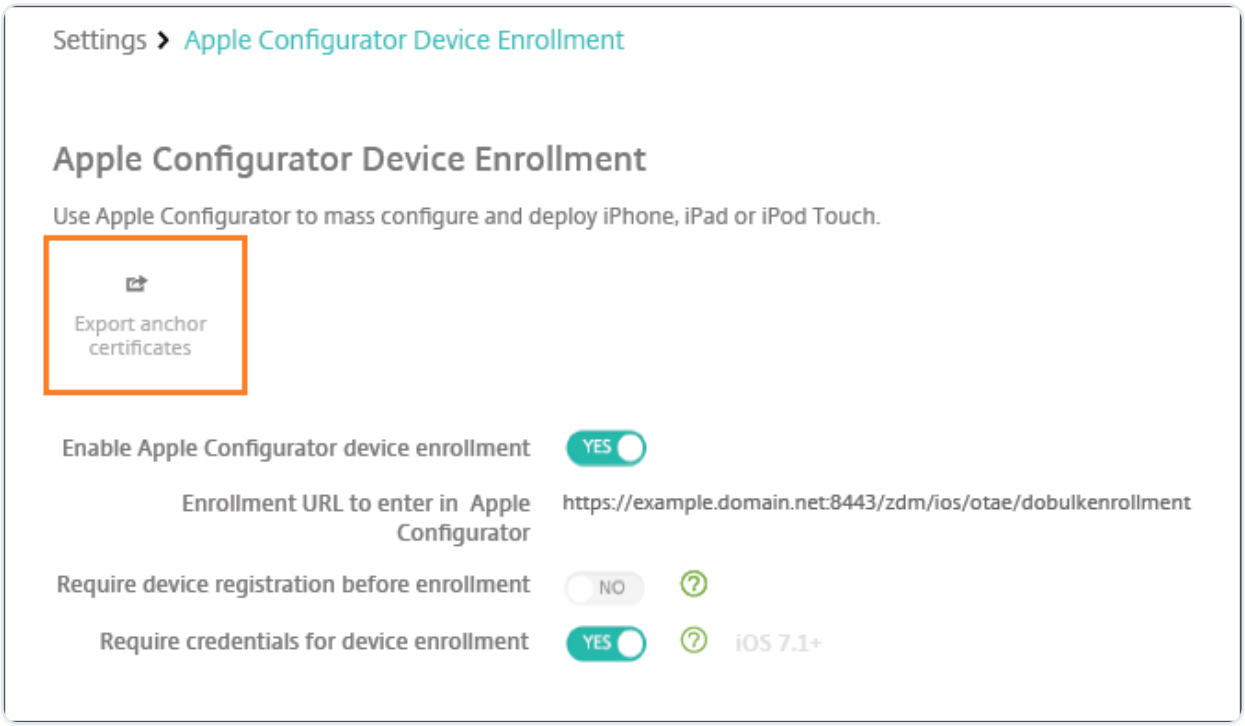
Apple Business Manager 대신 Apple Configurator 2를 사용하여 iPhone 및 iPad 장치를 대량으로 구성하고 배포할 수 있습니다.

1단계: XenMobile에서 설정 구성

1. XenMobile 콘솔에서 **설정 > Apple Configurator 장치 등록**으로 이동합니다.



2. **Apple Configurator 장치 등록 사용**을 **예**로 설정합니다.
3. **Apple Configurator에 입력할 등록 URL**은 읽기 전용 필드입니다. 이 설정은 Apple과 통신하는 XenMobile Server의 URL을 제공합니다. Apple Configurator 2에서 설정을 구성할 때 이 URL을 복사하여 붙여넣으십시오. 등록 URL은 `mdm.server.url.com`과 같은 XenMobile Server FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.
4. 알 수 없는 장치가 등록되는 것을 방지하려면 **등록 전 장치 등록 필요**를 **예**로 설정합니다. 참고: 이 설정이 **예**인 경우, 등록하기 전에 구성된 장치를 XenMobile의 **관리 > 장치**에 수동으로 또는 CSV 파일을 통해 추가해야 합니다.
5. iOS 장치 사용자가 등록할 때 자격 증명을 입력하도록 요구하려면 **장치 등록에 자격 증명 필요**를 **예**로 설정합니다. 기본값은 등록에 자격 증명을 요구하지 않는 것입니다.
6. 참고: XenMobile Server가 신뢰할 수 있는 SSL 인증서를 사용하는 경우 이 단계를 건너뛰십시오. **앵커 인증서 내보내기**를 클릭하고 certchain.pem 파일을 macOS 키체인(로그인 또는 시스템)에 저장합니다.



2단계: Apple Configurator 2에서 설정 구성

1. App Store에서 Apple Configurator 2를 설치합니다.
2. Dock Connector-USB 케이블을 사용하여 장치를 Apple Configurator 2를 실행하는 Mac에 연결합니다. 최대 30개의 연결된 장치를 동시에 구성할 수 있습니다. Dock Connector가 없는 경우 하나 이상의 전원 공급 USB 2.0 고속 허브를 사용하여 장치를 연결합니다.
3. Apple Configurator 2를 시작합니다. 구성자는 감독을 위해 준비할 수 있는 모든 장치를 표시합니다.
4. 장치를 감독용으로 준비하려면:
   - 구성을 정기적으로 다시 적용하여 장치 제어를 유지하려면 **장치 감독**을 선택합니다. **다음**을 클릭합니다.

     > **중요:**
     >
     > 장치를 감독 모드에 두면 선택한 iOS 버전이 장치에 설치되며, 이전에 저장된 사용자 데이터나 앱이 장치에서 완전히 지워집니다.

   - iOS에서 설치하려는 최신 iOS 버전에 대해 **최신**을 클릭합니다.
5. **MDM 서버 등록**에서 MDM 서버를 선택합니다. 새 서버를 추가하려면 **다음**을 클릭합니다.
6. **MDM 서버 정의**에서 서버 이름을 제공하고 XenMobile 콘솔에서 MDM 서버 URL을 붙여넣습니다.
7. **조직에 할당**에서 장치를 감독할 조직을 선택합니다.

Apple Configurator 2로 장치를 준비하는 방법에 대한 자세한 내용은 Apple Configurator 도움말 페이지 장치 준비를 참조하십시오.

8. 각 장치가 준비되면 장치를 켜서 iOS 설정 지원을 시작하고, 이는 장치를 처음 사용할 준비를 합니다.

Apple Configurator 2에서 Apple Business Manager로 장치 할당

Apple Configurator 2의 iPhone 및 iPad 장치를 Apple Business Manager 계정과 연결할 수 있습니다. 장치를 추가하면 **장치** 섹션에 나타납니다. 이러한 장치에는 더 이상 Apple Configurator 2를 통해 할당된 등록 설정이 포함되지 않습니다. 자세한 내용은 Apple Configurator 2에서 추가된 장치를 Apple Business Manager에 할당을 참조하십시오.

Apple 배포 프로그램을 사용할 때 인증서 갱신 또는 업데이트

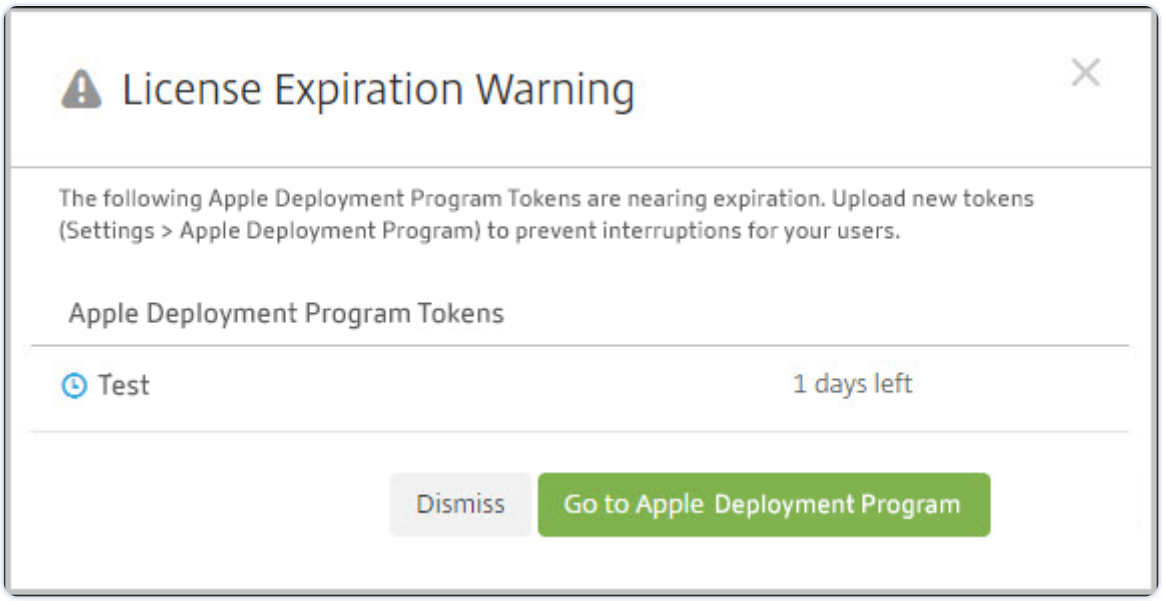
XenMobile SSL(Secure Sockets Layer) 인증서가 갱신되면 XenMobile 콘솔의 **설정 > 인증서**에서 새 인증서를 업로드합니다. **가져오기** 대화 상자의 **용도**에서 **SSL 수신기**를 클릭하여 인증서가 SSL에 사용되도록 합니다. 서버를 다시 시작하면 XenMobile이 새 SSL 인증서를 사용합니다. XenMobile의 인증서에 대한 자세한 내용은 XenMobile에서 인증서 업로드를 참조하십시오.

SSL 인증서를 갱신하거나 업데이트할 때 Apple Deployment Program과 XenMobile 간의 신뢰 관계를 다시 설정할 필요는 없습니다. 그러나 이 문서의 이전 단계를 따라 언제든지 **Apple Deployment Program** 설정을 다시 구성할 수 있습니다.

Apple Deployment Program에 대한 자세한 내용은 Apple 설명서를 참조하십시오.

Apple Deployment Program과 XenMobile 간의 연결 갱신

자동 장치 등록 서버 토큰이 만료되면 XenMobile에 라이선스 만료 경고가 표시됩니다.



Apple School Manager/Apple Business Manager에서 토큰을 교체합니다.

1단계: XenMobile Server에서 공개 키 다운로드

1. XenMobile 콘솔에서 **설정 > Apple Deployment Program**으로 이동하여 새 공개 키를 다운로드합니다.

2단계: Apple 계정에서 서버 토큰 파일 생성 및 다운로드

1. Apple Business Manager에 로그인하여 토큰을 다운로드합니다.
2. **설정**을 열고 토큰이 필요한 서버를 선택합니다. **편집**을 클릭합니다.
3. **MDM 서버 설정**에서 XenMobile에서 다운로드한 새 공개 키를 업로드하고 변경 사항을 저장합니다.
4. **토큰 다운로드**를 클릭하여 새 토큰을 다운로드합니다.

3단계: XenMobile에 서버 토큰 파일 업로드

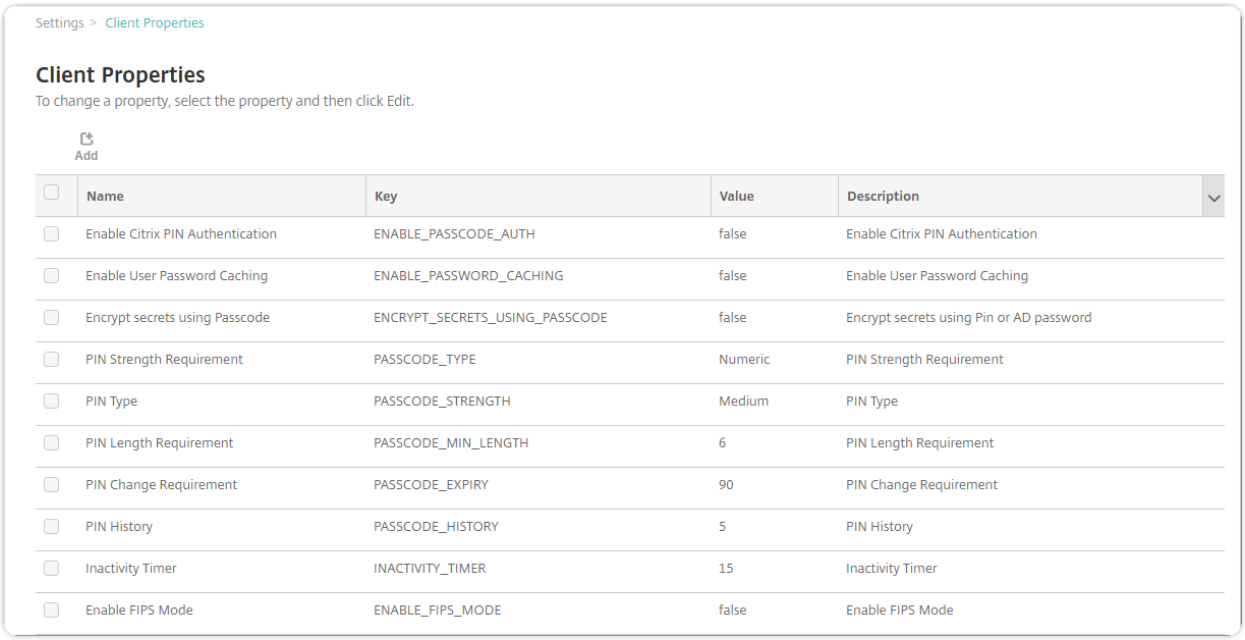
1. Citrix XenMobile에서 **설정 > Apple Deployment Program**으로 이동합니다.
2. 배포 프로그램 계정을 선택하고, **편집**을 클릭한 다음, 서버 토큰 파일을 업로드합니다.
3. **다음**을 클릭하고 변경 사항을 저장합니다.

클라이언트 속성

클라이언트 속성에는 사용자 장치의 Secure Hub에 직접 제공되는 정보가 있습니다. 이러한 속성을 사용하여 Citrix PIN과 같은 고급 설정을 구성할 수 있습니다. 클라이언트 속성은 Citrix 지원팀에서 얻을 수 있습니다.

클라이언트 속성은 Secure Hub의 모든 릴리스와 클라이언트 앱에 따라 변경될 수 있습니다. 더 일반적으로 구성된 클라이언트 속성에 대한 자세한 내용은 이 문서의 뒷부분에 있는 클라이언트 속성 참조를 참조하십시오.

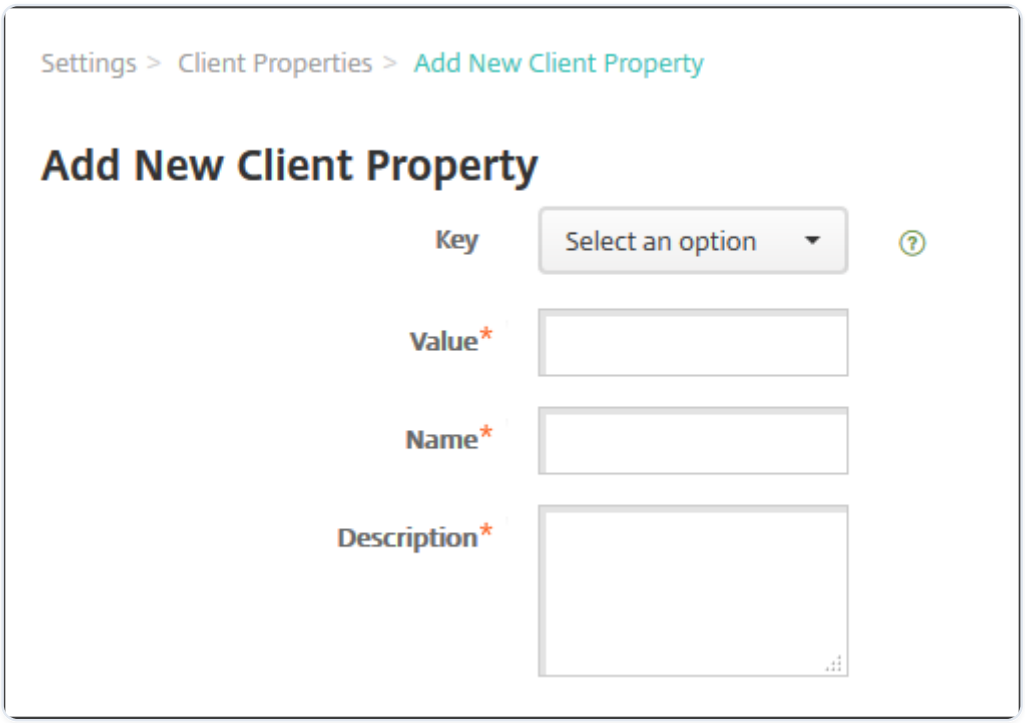
1. XenMobile® 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **클라이언트**에서 **클라이언트 속성**을 클릭합니다. **클라이언트 속성** 페이지가 나타납니다. 이 페이지에서 클라이언트 속성을 추가, 편집 및 삭제할 수 있습니다.



Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

클라이언트 속성을 추가하려면

1. **추가**를 클릭합니다. **새 클라이언트 속성 추가** 페이지가 나타납니다.



2. 다음 설정을 구성합니다.

   - **키:** 목록에서 추가할 속성 키를 클릭합니다. 중요: 설정을 업데이트하기 전에 Citrix 지원팀에 문의하십시오. 특별 키를 요청할 수 있습니다.
   - **값:** 선택한 속성의 값입니다.
   - **이름:** 속성의 이름입니다.
   - **설명:** 속성에 대한 설명입니다.

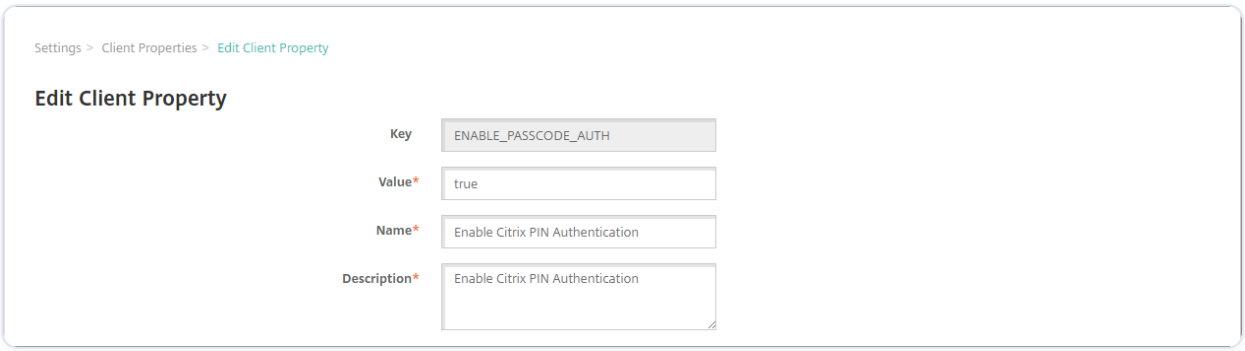
3. **저장**을 클릭합니다.

클라이언트 속성 편집

1. **클라이언트 속성** 테이블에서 편집할 클라이언트 속성을 선택합니다.

   클라이언트 속성 옆의 확인란을 선택하면 클라이언트 속성 목록 위에 옵션 메뉴가 나타납니다. 목록의 다른 곳을 클릭하면 목록 오른쪽에 옵션 메뉴가 나타납니다.

2. **편집**을 클릭합니다. **클라이언트 속성 편집** 페이지가 나타납니다.



3. 다음 정보를 필요에 따라 변경합니다.

   - **키:** 이 필드는 변경할 수 없습니다.
   - **값:** 속성 값입니다.
   - **이름:** 속성 이름입니다.
   - **설명:** 속성 설명입니다.

4. 변경 내용을 저장하려면 **저장**을 클릭하고, 속성을 변경하지 않으려면 **취소**를 클릭합니다.

클라이언트 속성 삭제

1. **클라이언트 속성** 테이블에서 삭제할 클라이언트 속성을 선택합니다.

   각 속성 옆의 확인란을 선택하여 여러 속성을 선택하여 삭제할 수 있습니다.

2. **삭제**를 클릭합니다. 확인 대화 상자가 나타납니다. **삭제**를 다시 클릭합니다.

클라이언트 속성 참조

XenMobile의 사전 정의된 클라이언트 속성 및 기본 설정은 다음과 같습니다.

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 표시 이름: MDX 컨테이너 자체 파괴 기간

- 자체 파괴는 지정된 비활성 일수 후에 Secure Hub 및 관리되는 앱에 대한 액세스를 방지합니다. 시간 제한이 지나면 앱을 더 이상 사용할 수 없습니다. 데이터 삭제에는 앱 캐시 및 사용자 데이터를 포함하여 설치된 각 앱의 앱 데이터 지우기가 포함됩니다.

  비활성 시간은 서버가 특정 기간 동안 사용자를 확인하기 위한 인증 요청을 받지 못하는 경우입니다. 예를 들어, 이 속성이 30일이고 사용자가 30일 이상 앱을 사용하지 않으면 정책이 적용됩니다.

  이 전역 보안 정책은 iOS 및 Android 플랫폼에 적용되며 기존 앱 잠금 및 삭제 정책을 개선한 것입니다.
- 이 전역 정책을 구성하려면 **설정 > 클라이언트 속성**으로 이동하여 사용자 지정 키 **CONTAINER_SELF_DESTRUCT_PERIOD**를 추가합니다.
- 값: 일수

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - 표시 이름: IT 헬프 데스크로 장치 로그 보내기
  - 이 속성은 IT 헬프 데스크로 로그를 보낼 수 있는 기능을 활성화하거나 비활성화합니다.
  - 가능한 값: **true** 또는 **false**
  - 기본값: **false**
- **DISABLE_LOGGING**
  - 표시 이름: 로깅 비활성화
  - 이 속성을 사용하여 사용자가 장치에서 로그를 수집하고 업로드하는 것을 방지할 수 있습니다. 이 속성은 Secure Hub 및 설치된 모든 MDX 앱에 대한 로깅을 비활성화합니다. 사용자는 지원 페이지에서 어떤 앱에 대해서도 로그를 보낼 수 없습니다. 메일 작성 대화 상자가 나타나더라도 로그는 첨부되지 않습니다. 로깅이 비활성화되었음을 나타내는 메시지가 표시됩니다. 이 설정은 또한 XenMobile 콘솔에서 Secure Hub 및 MDX 앱에 대한 로그 설정을 업데이트하는 것을 방지합니다.

    이 속성이 **true**로 설정되면 Secure Hub는 **Block application logs**를 **true**로 설정합니다. 결과적으로 새 정책이 적용되면 MDX 앱은 로깅을 중지합니다.
  - 가능한 값: **true** 또는 **false**
  - 기본값: **false** (로깅이 비활성화되지 않음)
- **ENABLE_CRASH_REPORTING**
  - 표시 이름: 충돌 보고 활성화
  - **true**인 경우 Citrix는 iOS 및 Android용 Secure Hub 문제 해결을 돕기 위해 충돌 보고서 및 진단 정보를 수집합니다. **false**인 경우 데이터가 수집되지 않습니다.

- 가능한 값: **true** 또는 **false**
- 기본값: **true**

- **ENABLE_CREDENTIAL_STORE**
  - 표시 이름: 자격 증명 저장소 활성화
  - 자격 증명 저장소를 활성화하면 Android 또는 iOS 사용자가 모바일 생산성 앱에 액세스할 때 암호를 한 번만 입력하면 됩니다. Citrix PIN을 활성화했는지 여부와 관계없이 자격 증명 저장소를 사용할 수 있습니다. Citrix PIN을 활성화하지 않으면 사용자는 Active Directory 암호를 입력합니다. XenMobile은 Secure Hub 및 공용 스토어 앱에 대해서만 자격 증명 저장소와 함께 Active Directory 암호 사용을 지원합니다. 자격 증명 저장소와 함께 Active Directory 암호를 사용하는 경우 XenMobile은 PKI 인증을 지원하지 않습니다.
  - Secure Mail의 자동 등록에는 이 속성을 **true**로 설정해야 합니다.
  - 이 사용자 지정 클라이언트 정책을 구성하려면 **Settings > Client Properties**로 이동하여 사용자 지정 키 **ENABLE_CREDENTIAL_STORE**를 추가하고 **Value**를 **true**로 설정합니다.

- **ENABLE_FIPS_MODE**
  - 표시 이름: FIPS 모드 사용
  - 이 속성은 모바일 장치에서 FIPS 모드를 활성화하거나 비활성화합니다. 값을 변경하면 Secure Hub가 다음 온라인 인증을 수행할 때 새 값을 장치로 전달합니다.
  - 가능한 값: **true** 또는 **false**
  - 기본값: **false**

- **ENABLE_PASSCODE_AUTH**
  - 표시 이름: Citrix PIN 인증 사용
  - 이 속성을 사용하면 Citrix PIN 기능을 켤 수 있습니다. Citrix PIN 또는 암호를 사용하면 사용자는 Active Directory 암호 대신 사용할 PIN을 정의하라는 메시지가 표시됩니다. 이 설정은 ENABLE_PASSWORD_CACHING이 활성화되거나 XenMobile이 인증서 인증을 사용할 때 자동으로 활성화됩니다.

    오프라인 인증의 경우 Citrix PIN은 로컬에서 유효성이 검사되며 사용자는 요청한 앱 또는 콘텐츠에 액세스할 수 있습니다. 온라인 인증의 경우 Citrix PIN 또는 암호는 Active Directory 암호 또는 인증서를 잠금 해제하며, 이는 XenMobile을 통한 인증을 위해 전송됩니다.

    ENABLE_PASSCODE_AUTH가 true이고 ENABLE_PASSWORD_CACHING이 false인 경우, Secure Hub가 암호를 저장하지 않으므로 온라인 인증은 항상 암호를 요청합니다.
  - 가능한 값: **true** 또는 **false**

- 기본값: **false**

- **ENABLE_PASSWORD_CACHING**
  - 표시 이름: 사용자 암호 캐싱 사용
  - 이 속성은 Active Directory 암호를 모바일 장치에 로컬로 캐시할 수 있도록 합니다. 이 속성을 **true**로 설정하면 **ENABLE_PASSCODE_AUTH** 속성도 **true**로 설정해야 합니다. 사용자 암호 캐싱이 활성화되면 XenMobile은 사용자에게 Citrix PIN 또는 암호를 설정하도록 요청합니다.
  - 가능한 값: **true** 또는 **false**
  - 기본값: **false**

- **ENABLE_TOUCH_ID_AUTH**
  - 표시 이름: Touch ID 인증 사용
  - Touch ID 인증을 지원하는 장치의 경우, 이 속성은 장치에서 Touch ID 인증을 활성화하거나 비활성화합니다. 요구 사항:

    사용자 장치에는 Citrix PIN 또는 LDAP가 활성화되어 있어야 합니다. LDAP 인증이 비활성화된 경우(예: 인증서 기반 인증만 사용되는 경우), 사용자는 Citrix PIN을 설정해야 합니다. 이 경우 클라이언트 속성 **ENABLE_PASSCODE_AUTH**가 **false**이더라도 XenMobile은 Citrix PIN을 요구합니다.

    ENABLE_PASSCODE_AUTH를 **false**로 설정하여 사용자가 앱을 시작할 때 Touch ID를 사용하라는 메시지에 응답해야 합니다.
  - 가능한 값: **true** 또는 **false**
  - 기본값: **false**

- **ENABLE_WORXHOME_CEIP**
  - 표시 이름: Worx Home CEIP 사용
  - 이 속성은 고객 경험 향상 프로그램(Customer Experience Improvement Program)을 웁니다. 이 기능은 익명의 구성 및 사용 데이터를 Citrix에 주기적으로 보냅니다. 이 데이터는 Citrix가 XenMobile의 품질, 안정성 및 성능을 개선하는 데 도움이 됩니다.
  - 값: **true** 또는 **false**
  - 기본값: **false**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 표시 이름: 암호로 비밀 암호화

  - 이 속성은 iOS 키체인과 같은 플랫폼 기반 기본 저장소 대신 비밀 저장소에 장치의 중요한 데이터를 저장합니다. 이 속성은 주요 아티팩트의 강력한 암호화를 가능하게 하고 사용자 엔트로피를 추가합니다. 사용자 엔트로피는 사용자만 아는 사용자 생성 무작위 PIN 코드입니다.

    Citrix는 사용자 장치에서 더 높은 보안을 제공하는 데 도움이 되도록 이 속성을 활성화할 것을 권장합니다. 결과적으로 사용자는 Citrix PIN에 대한 인증 프롬프트를 더 많이 경험하게 됩니다.
  - 가능한 값: **true** 또는 **false**
  - 기본값: **false**

- **INACTIVITY_TIMER**
  - 표시 이름: 비활성 타이머
  - 이 속성은 사용자가 장치를 비활성 상태로 유지한 후 Citrix PIN 또는 암호 프롬프트 없이 앱에 액세스할 수 있는 기간을 정의합니다. MDX 앱에 대해 이 설정을 사용하려면 앱 암호 설정을 켜짐으로 설정합니다. 앱 암호 설정이 꺼짐으로 설정된 경우 사용자는 전체 인증을 수행하기 위해 Secure Hub로 리디렉션됩니다. 이 설정을 변경하면 사용자가 인증하라는 메시지가 표시될 때 다음번에 값이 적용됩니다.

    iOS에서 비활성 타이머는 MDX 및 비MDX 앱의 Secure Hub 액세스도 제어합니다.
  - 가능한 값: 모든 양의 정수
  - 기본값: **15** (분)

- **ON_FAILURE_USE_EMAIL**
  - 표시 이름: 실패 시 이메일을 사용하여 장치 로그를 IT 헬프 데스크로 보냄
  - 이 속성은 이메일을 사용하여 장치 로그를 IT 부서로 보낼 수 있는 기능을 활성화하거나 비활성화합니다.
  - 가능한 값: **true** 또는 **false**
  - 기본값: **true**

- **PASSCODE_EXPIRY**
  - 표시 이름: PIN 변경 요구 사항
  - 이 속성은 Citrix PIN 또는 암호가 유효한 기간을 정의하며, 이 기간이 지나면 사용자는 Citrix PIN 또는 암호를 변경해야 합니다. 이 설정을 변경하면 현재 Citrix PIN 또는 암호가 만료될 때만 새 값이 설정됩니다.
  - 가능한 값: **1**에서 **99**까지 권장됩니다. PIN 재설정을 없애려면 값을 높은 숫자(예: 100,000,000,000)로 설정하십시오. 만료 기간을 원래 1일에서 99일 사이로 설정한 다음 해당 기간

동안 큰 숫자로 변경하는 경우: PIN은 초기 기간이 끝날 때 여전히 만료되지만, 그 이후에는 다시 만료되지 않습니다.

- 기본값: **90** (일)

- **PASSCODE_HISTORY**
  - 표시 이름: PIN 기록
  - 이 속성은 사용자가 Citrix PIN 또는 암호를 변경할 때 재사용할 수 없는 이전에 사용한 Citrix PIN 또는 암호의 수를 정의합니다. 이 설정을 변경하면 사용자가 다음에 Citrix PIN 또는 암호를 재설정할 때 새 값이 설정됩니다.
  - 가능한 값: **1**에서 **99**까지
  - 기본값: **5**
- **PASSCODE_MAX_ATTEMPTS**
  - 표시 이름: PIN 시도 횟수
  - 이 속성은 사용자가 전체 인증을 요청받기 전에 잘못된 Citrix PIN 또는 암호를 몇 번 시도할 수 있는지 정의합니다. 사용자가 전체 인증에 성공하면 Citrix PIN 또는 암호를 생성하라는 메시지가 표시됩니다.
  - 가능한 값: 모든 양의 정수
  - 기본값: **15**
- **PASSCODE_MIN_LENGTH**
  - 표시 이름: PIN 길이 요구 사항
  - 이 속성은 Citrix PIN의 최소 길이를 정의합니다.
  - 가능한 값: **4** ~ **10**
  - 기본값: **6**
- **PASSCODE_STRENGTH**
  - 표시 이름: PIN 강도 요구 사항
  - 이 속성은 Citrix PIN 또는 암호의 강도를 정의합니다. 이 설정을 변경하면 다음에 인증하라는 메시지가 표시될 때 사용자에게 Citrix PIN 또는 암호를 만들라는 메시지가 표시됩니다.
  - 가능한 값: **낮음**, **중간**, **높음**, 또는 **강함**
  - 기본값: **중간**
  - PASSCODE_TYPE 설정에 따른 각 강도 설정에 대한 암호 규칙은 다음과 같습니다.

숫자 암호 규칙:

암호 강도	숫자 암호 유형 규칙	허용됨	허용되지 않음
낮음	모든 숫자, 모든 순서 허용	444444, 123456, 654321	
중간 (기본 설정)	모든 숫자가 같거나 연속될 수 없습니다.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
높음	인접한 숫자는 같을 수 없습니다.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
강함	동일한 숫자를 두 번 이상 사용하지 마십시오. 세 개 이상의 연속된 숫자를 사용하지 마십시오. 세 개 이상의 역순 연속된 숫자를 사용하지 마십시오.	102983, 085085, 824673, 132312	132132, 131313, 902030

영숫자 암호에 대한 규칙:

암호 강도	영숫자 암호 유형 규칙	허용됨	허용되지 않음
낮음	최소한 하나의 숫자와 하나의 문자를 포함해야 합니다.	아아11비1, 에이비씨디1#, 에이비123~, 아아아아11, 아아11아아	에이에이에이아아아아, 아아아아아아, 에이비씨디이프
중간 (기본 설정)	낮은 암호 강도 규칙 외에도, 문자와 모든 숫자가 같을 수 없습니다. 문자는 연속될 수 없으며 숫자는 연속될 수 없습니다.	아아11비1, 아아아11비, 아아아1비2, 에이비씨145, 엑스와이즈135, 에스디프123, 에이비12씨3, 에이1비2씨3, 에이비씨디1#, 에이비123~	아아아아11, 아아11아아, 또는 아아아111; 에이비씨디12, 비씨디123, 123에이비씨, 엑스와이1234, 엑스와이즈345, 또는 씨비에이123
높음	대문자 하나 이상과 소문자 하나 이상을 포함합니다.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2

암호 강도	영숫자 암호 유형 규칙	허용됨	허용되지 않음
강력함	숫자 하나 이상, 특수 기호 하나 이상, 대문자 하나 이상, 소문자 하나 이상을 포함합니다.	에이비씨디1#, 에이비123~, 엑스와이12#3, 씨에이알12#, 에이에이비씨1#	에이비씨디12, 에이비씨디12, 디에프지12, 제이케이알티에이2

- **PASSCODE_TYPE**
  - 표시 이름: PIN 유형
  - 이 속성은 사용자가 숫자 Citrix PIN 또는 영숫자 암호를 정의할 수 있는지 여부를 정의합니다. **숫자**를 선택하면 사용자는 숫자만 사용할 수 있습니다(Citrix PIN). **영숫자**를 선택하면 사용자는 문자와 숫자의 조합을 사용할 수 있습니다(암호).

    이 설정을 변경하면 사용자는 다음에 인증하라는 메시지가 표시될 때 새 Citrix PIN 또는 암호를 설정해야 합니다.
  - 가능한 값: **숫자** 또는 **영숫자**
  - 기본값: **숫자**
- **REFRESHINTERVAL**
  - 표시 이름: REFRESHINTERVAL
  - 기본적으로 XenMobile은 고정된 인증서에 대해 3일마다 자동 검색 서버(ADS)에 핑을 보냅니다. 새로 고침 간격을 변경하려면 **설정 > 클라이언트 속성**으로 이동하여 사용자 지정 키 **REFRESHINTERVAL**을 추가하고 **값**을 시간(단위)으로 설정합니다.
  - 기본값: **72**시간 (3일)
- **SEND_LDAP_ATTRIBUTES**
  - Android, iOS 또는 macOS 장치의 MAM 전용 배포의 경우: 이메일 자격 증명으로 Secure Hub에 등록하는 사용자가 Secure Mail에 자동으로 등록되도록 XenMobile을 구성할 수 있습니다. 결과적으로 사용자는 Secure Mail에 등록하기 위해 추가 정보를 제공하거나 추가 단계를 수행할 필요가 없습니다.
  - 이 전역 클라이언트 정책을 구성하려면 **설정 > 클라이언트 속성**으로 이동하여 사용자 지정 키 **SEND_LDAP_ATTRIBUTES**를 추가하고 **값**을 다음과 같이 설정합니다.
  - 값: `userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}`
  - 속성 값은 MDM 정책과 유사하게 매크로로 지정됩니다.

- 이 속성에 대한 샘플 계정 서비스 응답은 다음과 같습니다.

  ```
  <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,em
  name="SEND_LDAP_ATTRIBUTES"/>
  ```

- 이 속성의 경우 XenMobile은 쉼표 문자를 문자열 종결자로 처리합니다. 따라서 속성 값에 쉼표가 포함된 경우 앞에 백슬래시를 붙입니다. 백슬래시는 클라이언트가 포함된 쉼표를 속성 값의 끝으로 해석하는 것을 방지합니다. 백슬래시 문자는 `"\\"`으로 나타냅니다.

- **HIDE_THREE_FINGER_TAP_MENU**
  - 이 속성이 설정되지 않았거나 **false**로 설정된 경우, 사용자는 장치에서 세 손가락 탭을 통해 숨겨진 기능 메뉴에 액세스할 수 있습니다. 숨겨진 기능 메뉴를 통해 사용자는 애플리케이션 데이터를 재설정할 수 있었습니다. 이 속성을 **true**로 설정하면 사용자가 숨겨진 기능 메뉴에 액세스할 수 없게 됩니다.
  - 이 전역 클라이언트 정책을 구성하려면 **설정 > 클라이언트 속성**으로 이동하여 사용자 지정 키 **HIDE_THREE_FINGER_TAP_MENU**를 추가하고 **값**을 설정합니다.

- **TUNNEL_EXCLUDE_DOMAINS**
  - 표시 이름: 터널 제외 도메인
  - 기본적으로 MDX는 XenMobile SDK 및 앱이 다양한 기능을 위해 사용하는 일부 서비스 엔드포인트를 마이크로 VPN 터널링에서 제외합니다. 예를 들어, 이러한 엔드포인트에는 Google Analytics, Citrix Cloud™ 서비스 및 Active Directory 서비스와 같이 엔터프라이즈 네트워크를 통한 라우팅이 필요 없는 서비스가 포함됩니다. 이 클라이언트 속성을 사용하여 제외된 도메인의 기본 목록을 재정의합니다.
  - 이 전역 클라이언트 정책을 구성하려면 **설정 > 클라이언트 속성**으로 이동하여 사용자 지정 키 **TUNNEL_EXCLUDE_DOMAINS**를 추가하고 **값**을 설정합니다.
  - 값: 기본 목록을 터널링에서 제외하려는 도메인으로 바꾸려면 쉼표로 구분된 도메인 접미사 목록을 입력합니다. 모든 도메인을 터널링에 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
    hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-
    staging.citrix.com,rttf-test.citrix.com,ssl.google-
    analytics.com,stream.launchdarkly.com
    ```

XenMobile Server의 사용자 지정 클라이언트 속성은 다음과 같습니다.

- **ENABLE_MAM_NFACTOR_SSO**

- 이 속성을 사용하면 NetScaler® Gateway에서 고급 인증 정책을 사용하는 동안 Secure Hub의 MAM 등록 또는 로그인 중에 MAM nFactor SSO를 활성화하거나 비활성화할 수 있습니다. 값이 **true**로 설정되면 Secure Hub의 MAM 등록 또는 로그인 중에 MAM nFactor SSO가 활성화됩니다.
- 이 속성을 구성하려면 **설정 > 클라이언트 속성**으로 이동하여 **추가**를 클릭합니다. **키** 드롭다운 메뉴에서 **사용자 지정 키**를 선택하고 다음 정보를 적절하게 업데이트합니다.
  - 키 - ENABLE_MAM_NFACTOR_SSO
  - 값 - true 또는 false
  - 이름 - ENABLE_MAM_NFACTOR_SSO
  - 설명 - 관련 설명 추가

- **MICROSOFT_CERTIFICATE_STRONG_MAPPING**
  - 이 속성은 Microsoft PKI(공개 키 인프라)와 함께 Secure Mail을 사용할 때 SID(보안 식별자)를 SAN(주체 대체 이름)에 추가하여 인증서 강력 매핑 기능을 지원하도록 기존 클라이언트 인증서를 갱신할지 여부를 제어합니다. 값이 **true**로 설정되면 기존 클라이언트 인증서가 SAN SID를 포함하도록 갱신됩니다.
  - 이 속성은 Microsoft PKI에만 적용됩니다.
  - 이 속성을 구성하려면 **설정 > 클라이언트 속성**으로 이동하여 **추가**를 클릭합니다. **키** 드롭다운 메뉴에서 **사용자 지정 키**를 선택하고 필요에 따라 다음 정보를 업데이트합니다.
    - 키 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
    - 값 - true 또는 false
    - 이름 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
    - 설명 - SAN SID를 포함하도록 클라이언트 인증서 갱신

Apple 배포 프로그램을 통해 장치 배포

Apple에는 비즈니스 및 교육 계정을 위한 장치 등록 프로그램이 있습니다. 비즈니스 계정의 경우, XenMobile에서 장치 등록 및 관리를 위해 Apple Business Manager(ABM) 또는 Apple School Manager(ASM)를 사용하려면 Apple 배포 프로그램에 등록합니다. 이 프로그램은 iOS, iPadOS 및 macOS 장치용입니다.

Apple 배포 프로그램은 개인용이 아닌 조직용입니다. Apple 배포 프로그램 계정을 생성하려면 상당한 수의 회사 세부 정보와 정보를 제공해야 합니다. 따라서 계정 요청 및 승인을 받는 데 시간이 걸릴 수 있습니다.

교육 계정의 경우 Apple School Manager 계정을 생성합니다. ASM은 Apple 배포 프로그램과 Apple 대량 구매를 통합합니다. Apple School Manager 계정을 생성하려면 Apple School 사이트로 이동하십시오.

Apple 배포 프로그램에 등록

Apple Business Manager에 등록하려면 business.apple.com으로 이동하십시오. **지금 등록**을 클릭하여 새 계정을 신청하십시오. `deployment@company.com`와 같이 조직의 이메일 주소를 사용하는 것이 가장 좋습니다. 등록 절차는 며칠이 걸릴 수 있습니다. 로그인 자격 증명을 받은 후 Apple Business Manager에서 제공하는 단계에 따라 계정을 생성하십시오.

> **참고:**
>
> 교육 계정의 경우 Apple 교육 기능과 통합을 참조하십시오.

Apple Business Manager 계정을 XenMobile에 연결

Apple Business Manager 계정을 XenMobile 배포에 연결하려면 XenMobile 콘솔 및 Apple Business Manager에 정보를 입력하십시오. 다음 단계를 따르십시오.

1단계: XenMobile Server에서 공개 키 다운로드

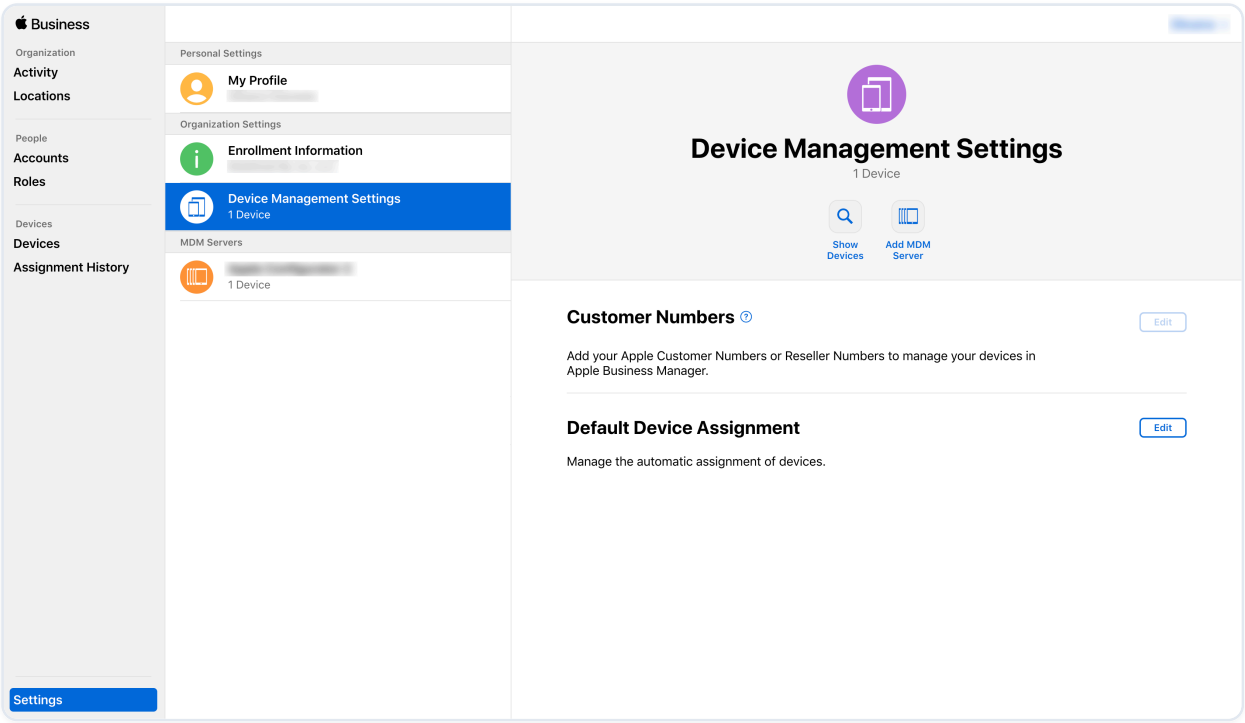
1. XenMobile 콘솔에서 **설정 > Apple 배포 프로그램**으로 이동합니다.



2. **공개 키 다운로드**에서 **다운로드**를 클릭합니다.

2단계: Apple 계정에서 서버 토큰 파일 생성 및 다운로드

1. 관리자 또는 기기 등록 관리자 계정을 사용하여 Apple Business Manager에 로그인합니다.
2. 사이드바 하단에서 **설정**을 클릭한 다음 **기기 관리 설정 > MDM 서버 추가**를 클릭합니다.



3. **MDM 서버 이름** 설정에 XenMobile Server의 이름을 입력합니다. 입력하는 서버 이름은 참조용입니다. 서버 URL 또는 이름이 아닙니다.
4. **공개 키 업로드**에서 **파일 선택**을 클릭합니다. XenMobile에서 다운로드한 공개 키를 업로드한 다음 변경 사항을 저장합니다.
5. **토큰 다운로드**를 클릭하여 서버 토큰 파일을 컴퓨터에 다운로드합니다.

   ABM 계정을 XenMobile에 추가할 때 서버 토큰 파일을 업로드해야 합니다. 토큰 파일을 가져온 후 XenMobile 콘솔에 ABM 토큰 정보가 나타납니다.
6. **기본 기기 할당**에서 **변경**을 클릭합니다. 기기를 할당할 방법을 선택한 다음 요청된 정보를 제공합니다. 자세한 내용은 ABM 사용자 가이드를 참조하십시오.

3단계: XenMobile에 ABM 계정 추가

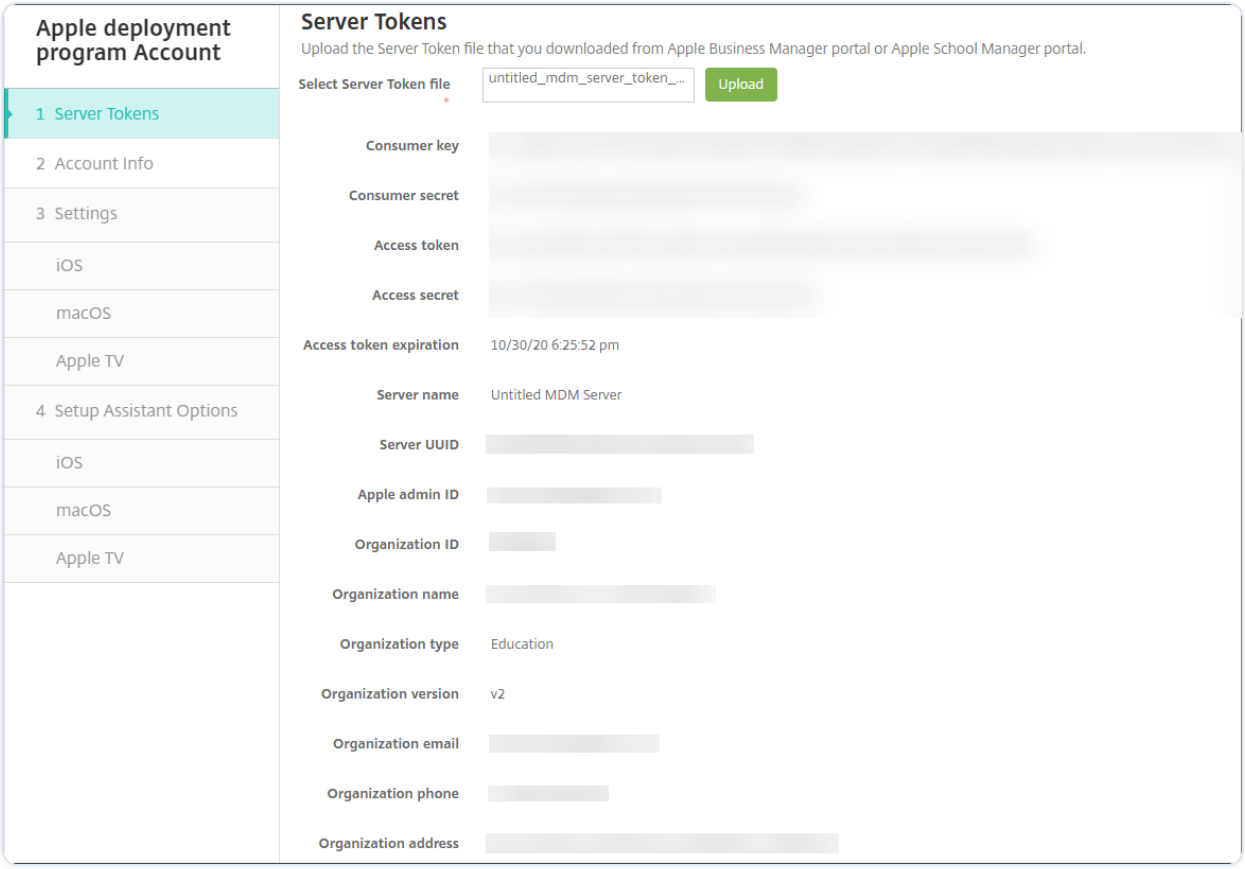
여러 ABM 계정을 XenMobile에 추가할 수 있습니다. 이 기능을 사용하면 국가, 부서 등에 따라 다른 등록 설정 및 설정 도우미 옵션을 사용할 수 있습니다. 그런 다음 ABM 계정을 다른 기기 정책과 연결합니다.

예를 들어, 다른 국가의 모든 ABM 계정을 동일한 XenMobile Server에 중앙 집중화하여 모든 ABM 기기를 가져오고 감독할 수 있습니다. 부서, 조직 계층 또는 기타 구조별로 등록 설정 및 설정 도우미 옵션을 사용자 지정하면 정책이 조직 전체에 적절한 기능을 제공하고 사용자는 적절한 지원을 받게 됩니다.

1. XenMobile 콘솔에서 **설정 > Apple Deployment Program**으로 이동한 다음 **Apple Deployment Program 계정 추가**에서 **추가**를 클릭합니다.

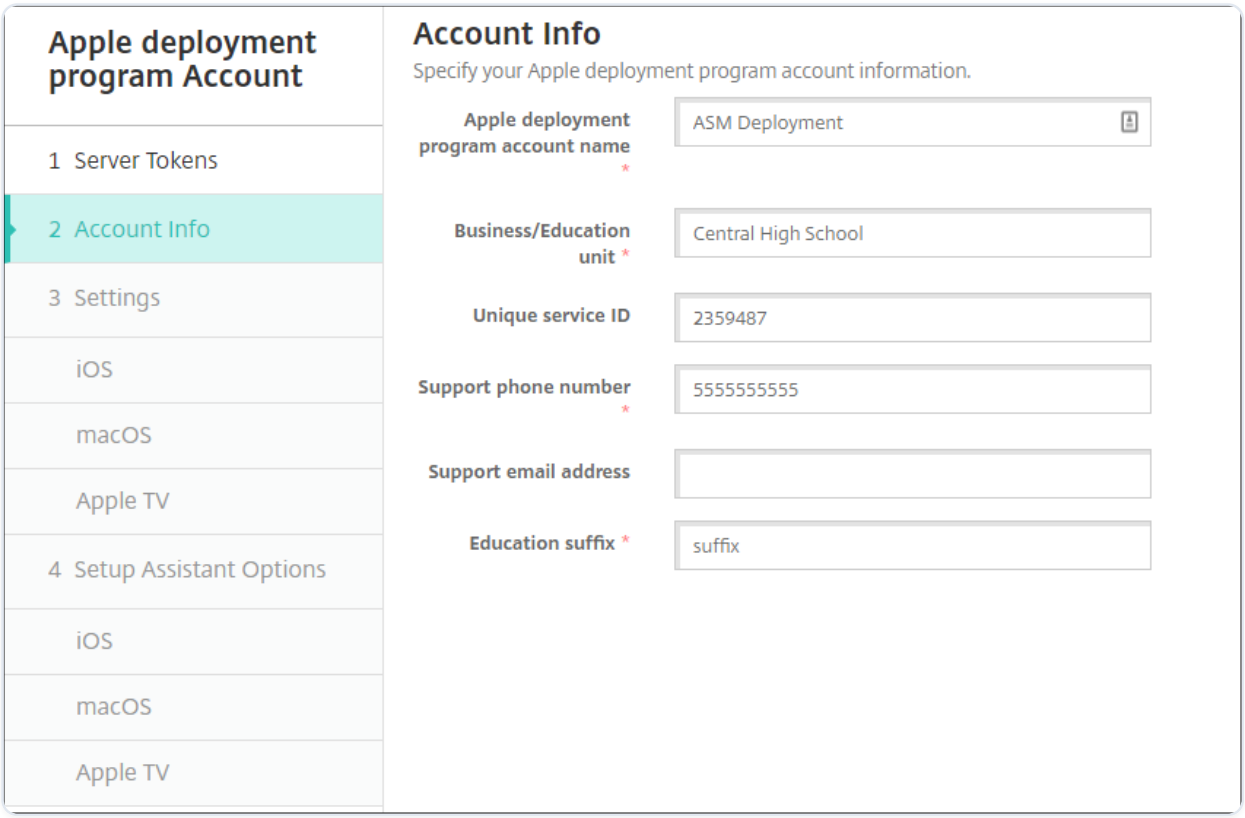


2. **서버 토큰** 페이지에서 서버 토큰 파일을 지정한 다음 **업로드**를 클릭합니다.



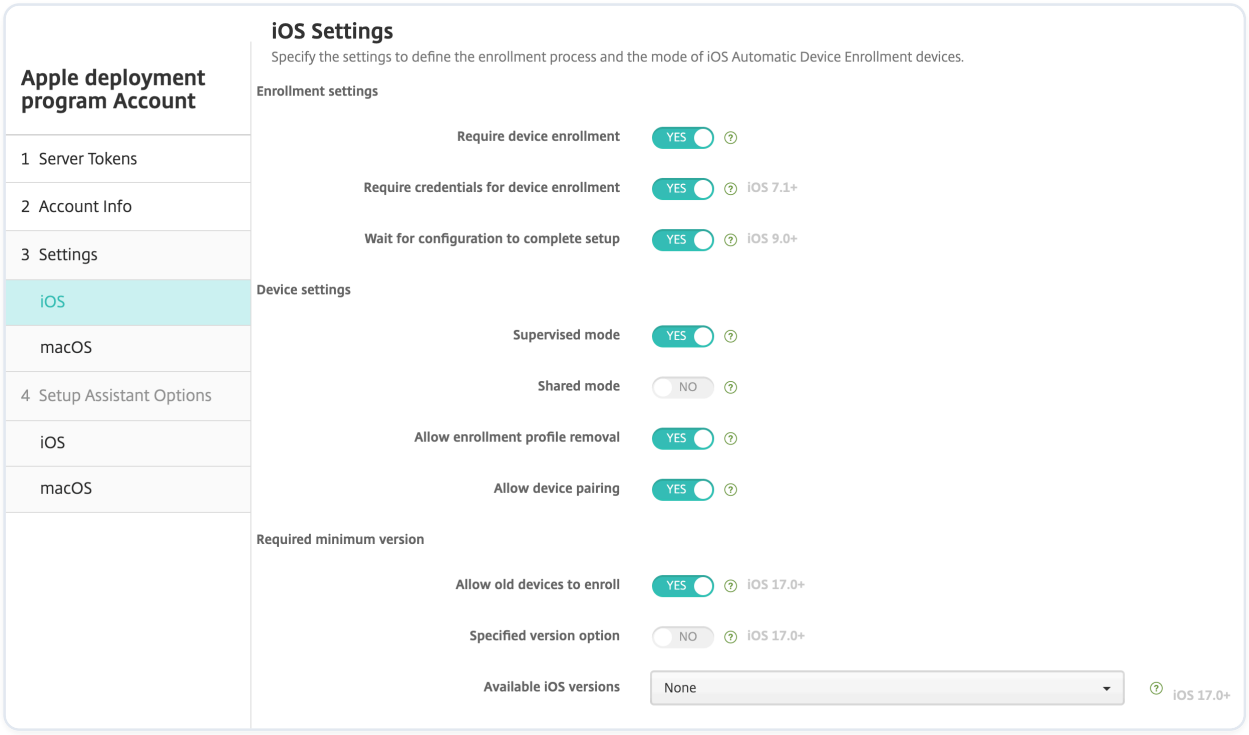
서버 토큰 정보가 나타납니다.

3. **계정 정보** 페이지에서 다음 설정을 지정합니다.



- **Apple Deployment Program 계정 이름:** 이 Apple Deployment Program 계정의 고유한 이름입니다. 국가 또는 조직 계층 구조와 같이 Apple Deployment Program 계정을 구성하는 방법을 반영하는 이름을 사용하십시오.
- **비즈니스/교육 단위:** 장치가 할당된 비즈니스 단위 또는 부서입니다. 이 필드는 필수입니다.
- **고유 서비스 ID:** 계정을 추가로 식별하는 데 도움이 되는 선택적 고유 ID입니다.
- **지원 전화 번호:** 사용자가 설정 중에 도움을 요청할 수 있는 지원 전화 번호입니다. 이 필드는 필수입니다.
- **지원 이메일 주소:** 최종 사용자가 사용할 수 있는 선택적 지원 이메일 주소입니다.
- **교육 접미사**: ASM 계정용입니다. 이 계정을 통해 등록된 장치에 할당된 접미사를 입력합니다.

4. **iOS 설정**에서 다음 설정을 지정합니다.



등록 설정

- **장치 등록 필요:** 사용자가 장치를 등록하도록 요구할지 여부입니다. 기본값은 **예**입니다.
- **장치 등록을 위한 자격 증명 필요:** ABM 설정 중에 사용자가 자격 증명을 입력하도록 요구할지 여부입니다. Citrix®는 모든 사용자가 장치 등록 중에 자격 증명을 입력하도록 요구하여 권한 있는 사용자만 장치를 등록할 수 있도록 하는 것을 권장합니다. 기본값은 **예**입니다.

  처음 설정하기 전에 ABM을 활성화하고 이 옵션을 선택하지 않으면 XenMobile이 ABM 구성 요소를 생성합니다. 이 생성에는 ABM 사용자, Secure Hub, 소프트웨어 인벤토리 및 ABM 배포 그룹과 같은 구성 요소가 포함됩니다. 이 옵션을 선택하면 XenMobile은 구성 요소를 생성하지 않습니다. 결과적으로 나중에 이 옵션을 해제하면 자격 증명을 입력하지 않은 사용자는 ABM 구성 요소가 없으므로 ABM에 등록할 수 없습니다. 이 경우 ABM 구성 요소를 추가하려면 ABM 계정을 비활성화한 다음 다시 활성화하십시오.
- **구성 완료 대기:** 모든 MDM 리소스가 장치에 배포될 때까지 사용자의 장치가 설정 지원 모드를 유지하도록 요구할지 여부입니다. 이 설정은 감독 모드의 장치에서 사용할 수 있습니다. 기본값은 **아니요**입니다.
- Apple 설명서에 따르면 장치가 설정 지원 모드에 있는 동안 다음 명령이 작동하지 않을 수 있습니다.
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring

- DeviceLock

장치 설정

- **감독 모드:** Apple Configurator를 사용하여 ABM 등록 장치를 관리하거나 **구성 완료 대기**가 활성화된 경우 **예**로 설정해야 합니다. 기본값은 **예**입니다. iOS 장치를 감독 모드에 두는 방법에 대한 자세한 내용은 Apple Configurator를 사용하여 iOS 장치를 감독 모드에 두는 방법을 참조하십시오.
- **등록 프로필 제거 허용:** 장치가 원격으로 제거할 수 있는 프로필을 사용하도록 허용할지 여부입니다. 기본값은 **아니요**입니다.
- **장치 페어링 허용:** ABM을 통해 등록된 장치의 경우 Apple Music 및 Apple Configurator를 통해 관리할 수 있는지 여부입니다. 기본값은 **아니요**입니다.

필수 최소 버전

- **이전 장치 등록 허용**: 활성화된 경우, 장치가 현재 필수 최소 버전으로 업그레이드할 수 없더라도 등록할 수 있습니다. 기본값은 켜짐입니다. 이 옵션은 iOS 17.0 이상에서만 사용할 수 있습니다.
- **지정된 버전 옵션**: 관리자가 지정된 버전을 수동으로 입력하도록 허용할지 여부입니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 17.0 이상에서만 사용할 수 있습니다.
- **사용 가능한 iOS 버전**: 목록에서 사용 가능한 iOS 버전을 선택할 수 있습니다. 장치에 현재 버전보다 낮은 iOS 버전이 있는 경우 장치에서 업데이트 프로세스를 시작합니다. 향후 버전이 만료되면 사용 가능한 버전 목록의 최소 버전이 사용됩니다. 기본값은 **없음**이며, **없음**으로 설정하면 적용되지 않습니다. 이 옵션은 iOS 17.0 이상에서만 사용할 수 있습니다.
- **지정된 버전**: 장치에 현재 버전보다 낮은 iOS 버전이 있는 경우 장치에서 업데이트 프로세스를 시작합니다. 향후 버전이 만료되면 사용 가능한 버전 목록의 최소 버전이 사용됩니다. 예기치 않은 오류를 방지하려면 올바른 버전 번호를 입력해야 합니다.

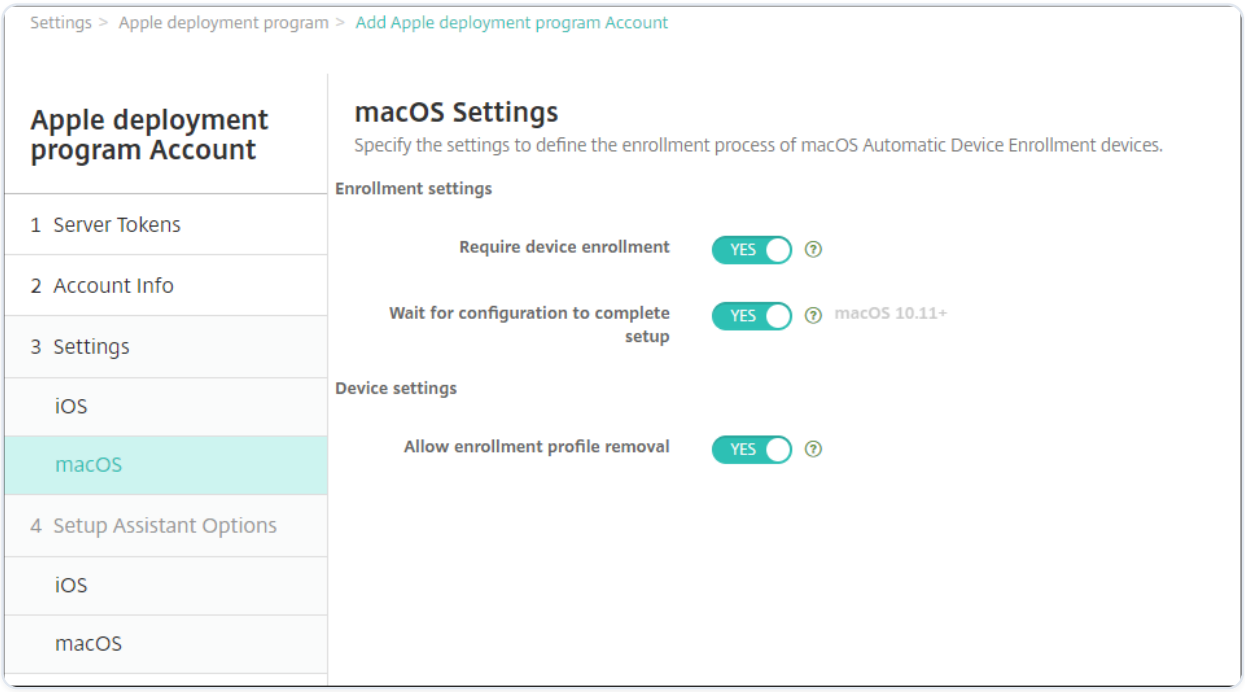
감독 ID

GroundControl 도구를 사용하는 경우 다음을 수행하도록 인증서를 추가할 수 있습니다.

- "이 호스트 신뢰" 프롬프트를 피하기 위해 페어링 제한을 재정의합니다.
- 사용자 상호 작용 없이 프로필 설치와 같은 작업을 수행하기 위해 USB를 통해 관리되는 장치 작업을 에스컬레이션합니다. 이렇게 하면 GroundControl이 체크아웃을 위해 단일 앱 모드 및 장치 잠금을 활성화할 수 있습니다.
- ABM 장치에 백업을 복원합니다.

GroundControl에 대한 자세한 내용은 GroundControl 웹사이트를 참조하십시오.

5. **macOS 설정**에서 다음 설정을 지정합니다.



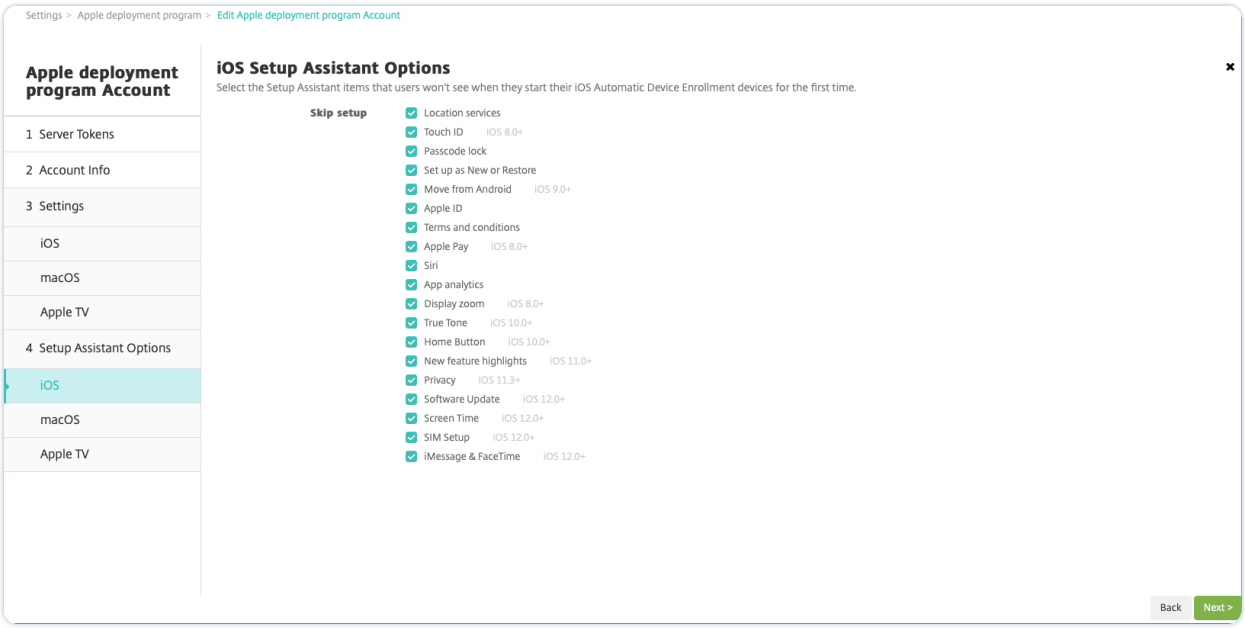
등록 설정

- **장치 등록 필요:** 사용자가 장치를 등록하도록 요구할지 여부. 기본값은 **예**입니다.
- **설정 완료를 위한 구성 대기: 예**인 경우 MDM 리소스 암호가 장치에 배포될 때까지 macOS 장치는 설정 지원을 계속하지 않습니다. 이 배포는 로컬 계정 생성 전에 발생합니다. 이 설정은 macOS 10.11 이상 장치에서 사용할 수 있습니다. 기본값은 **아니요**입니다.

장치 설정

- **등록 프로필 제거 허용:** 장치가 원격으로 제거할 수 있는 프로필을 사용하도록 허용할지 여부. 기본값은 **아니요**입니다.

6. **iOS 설정 지원 옵션**에서 사용자가 기기를 처음 시작할 때 iOS 설정 지원이 건너뛸 단계를 선택합니다. 화면을 건너뛰면 관련 기능은 기본 설정을 사용합니다. 해당 기능에 대한 액세스를 완전히 제한하지 않는 한, 사용자는 설정이 완료된 후 건너뛴 기능을 구성할 수 있습니다. 기능 액세스 제한에 대한 자세한 내용은 제한 장치 정책을 참조하십시오. 모든 항목의 기본값은 선택 해제되어 있습니다. 다음 설명은 설정을 선택할 때 발생하는 상황을 설명합니다.

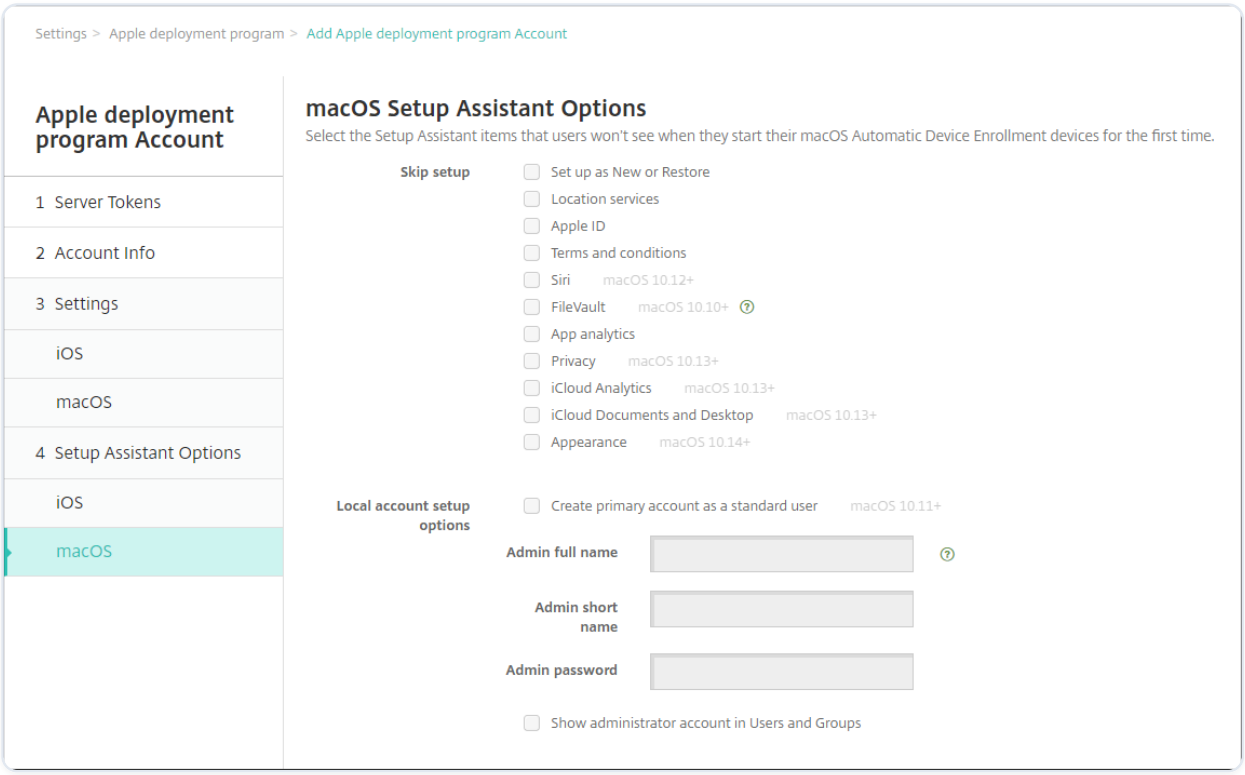


- **위치 서비스:** 사용자가 기기에서 위치 서비스를 설정하지 못하도록 합니다.
- **Touch ID:** 사용자가 iOS 기기에서 Touch ID 또는 Face ID를 설정하지 못하도록 합니다. iOS 15에서 더 이상 사용되지 않습니다.
- **암호 잠금:** 사용자가 기기에 암호를 설정하지 못하도록 합니다. 암호가 없으면 사용자는 Touch ID 또는 Apple Pay를 사용할 수 없습니다.
- **새 기기로 설정 또는 복원:** 사용자가 기기를 새 기기로 설정하거나 iCloud 또는 Apple App Store 백업에서 복원하지 못하도록 합니다.
- **Android에서 이동:** 사용자가 Android 기기에서 iOS 기기로 데이터를 전송하지 못하도록 합니다. 이 옵션은 **새 기기로 설정 또는 복원**이 선택된 경우(즉, 단계가 건너뛰어진 경우)에만 사용할 수 있습니다.
- **Apple ID:** 사용자가 기기에 관리형 Apple ID 계정을 설정하지 못하도록 합니다.
- **이용 약관:** 사용자가 기기 사용에 대한 이용 약관을 읽고 동의하지 못하도록 합니다.
- **Apple Pay:** 사용자가 Apple Pay를 설정하지 못하도록 합니다. 이 설정이 해제되면 사용자는 Touch ID 및 Apple ID를 설정해야 합니다. 해당 설정이 해제되어 있는지 확인하십시오.
- **Siri:** 사용자가 Siri를 구성하지 못하도록 합니다.
- **앱 분석:** 사용자가 충돌 데이터 및 사용 통계를 Apple과 공유할지 여부를 설정하지 못하도록 합니다.
- **디스플레이 확대/축소:** 사용자가 iOS 기기에서 디스플레이 해상도(표준 또는 확대/축소)를 설정하지 못하도록 합니다. iOS 17에서 더 이상 사용되지 않습니다.
- **True Tone:** 사용자가 4채널 센서를 설정하여 디스플레이의 화이트 밸런스를 동적으로 조정하지 못하도록 합니다.
- **홈 버튼:** 사용자가 홈 버튼 피드백 스타일을 설정하지 못하도록 합니다. iOS 15에서 더 이상 사용되지 않습니다.

- **새로운 기능 하이라이트:** 사용자가 Apple 소프트웨어의 새로운 기능에 대한 정보를 표시하는 화면을 보지 못하도록 합니다.
- **개인 정보 보호:** 사용자가 데이터 및 개인 정보 보호 창을 보지 못하도록 합니다. iOS 11.3 이상에서 적용됩니다.
- **소프트웨어 업데이트:** 사용자가 iOS를 최신 버전으로 업데이트하지 못하도록 합니다. iOS 12.0 이상에서 적용됩니다.
- **스크린 타임:** 사용자가 스크린 타임을 활성화하지 못하도록 합니다. iOS 12.0 이상에서 적용됩니다.
- **SIM 설정:** 사용자가 셀룰러 요금제를 설정하지 못하도록 합니다. iOS 12.0 이상에서 적용됩니다.
- **iMessage 및 FaceTime:** 사용자가 iMessage 및 FaceTime을 활성화하지 못하도록 합니다. iOS 12.0 이상에서 적용됩니다.
- **모양:** 사용자가 모양 모드를 선택하지 못하도록 합니다. iOS 13.0 이상에서 적용됩니다.
- **환영:** 사용자가 **시작하기** 화면을 보지 못하도록 합니다. iOS 13.0 이상에서 적용됩니다.
- **복원 완료:** 사용자가 설정 중에 복원이 완료되었는지 여부를 보지 못하도록 합니다. iOS 14.0 이상에서 적용됩니다.
- **업데이트 완료:** 사용자가 설정 중에 소프트웨어 업데이트가 완료되었는지 여부를 보지 못하도록 합니다. iOS 14.0 이상에서 적용됩니다.
- **동작 버튼:** 사용자가 동작 버튼 구성 창을 보지 못하도록 합니다. iOS 17.0 이상에서 적용됩니다.
- **잠금 모드:** Apple 계정이 설정된 경우 사용자가 잠금 모드 창을 보지 못하도록 합니다. iOS 17.1 이상에서 적용됩니다.
- **지능:** 사용자가 지능 창을 보지 못하도록 합니다. iOS 18.0 이상에서 적용됩니다.
- **카메라 버튼:** 사용자가 카메라 버튼 창을 보지 못하도록 합니다. iOS 18.0 이상에서 적용됩니다.

ABM 계정은 **설정 > Apple 배포 프로그램**에 나타납니다.

7. **macOS 설정 지원 옵션**에서 사용자가 장치를 처음 시작할 때 macOS 설정 지원이 건너뛸 단계를 선택합니다. 화면이 건너뛰어지면 관련 기능은 기본 설정을 사용합니다. 해당 기능에 대한 액세스를 완전히 제한하지 않는 한, 사용자는 설정이 완료된 후 건너뛴 기능을 구성할 수 있습니다. 기능 액세스 제한에 대한 자세한 내용은 제한 장치 정책을 참조하십시오. 모든 항목의 기본값은 지워집니다. 다음 설명은 설정이 선택될 때 발생하는 상황을 설명합니다.



- **새로 설정 또는 복원:** 사용자가 장치를 새로 설정하거나 Time Machine 백업에서 복원하거나 시스템 마이그레이션을 수행하는 것을 방지합니다.
- **위치 서비스:** 사용자가 장치에서 위치 서비스를 설정하는 것을 방지합니다. macOS 10.11 이상에 해당합니다.
- **Apple ID:** 사용자가 장치에 관리형 Apple ID 계정을 설정하는 것을 방지합니다.
- **이용 약관:** 사용자가 장치 사용에 대한 이용 약관을 읽고 동의하는 것을 방지합니다.
- **Siri:** 사용자가 Siri를 구성하는 것을 방지합니다. macOS 10.12 이상에 해당합니다.
- **FileVault:** FileVault를 사용하여 시동 디스크를 암호화합니다. XenMobile은 시스템에 단일 로컬 사용자 계정이 있고 해당 계정이 iCloud에 로그인되어 있는 경우에만 FileVault 설정을 적용합니다.

  macOS FileVault 디스크 암호화 기능을 사용하여 시스템 볼륨의 내용을 암호화하여 보호할 수 있습니다 (https://support.apple.com/ko-kr/HT204837). FileVault가 켜져 있지 않은 최신 휴대용 Mac에서 설정 지원을 실행하는 경우 이 기능을 켜라는 메시지가 표시될 수 있습니다. 이 메시지는 새 시스템과 OS X 10.10 또는 10.11로 업그레이드된 시스템 모두에 나타나지만, 시스템에 단일 로컬 관리자 계정이 있고 해당 계정이 iCloud에 로그인되어 있는 경우에만 나타납니다.
- **앱 분석:** 사용자가 충돌 데이터 및 사용 통계를 Apple과 공유할지 여부를 설정하는 것을 방지합니다.
- **개인 정보 보호:** 사용자가 데이터 및 개인 정보 보호 창을 보는 것을 방지합니다. macOS 10.13 이상에 해당합니다.
- **iCloud 분석:** 사용자가 진단 iCloud 데이터를 Apple에 보낼지 여부를 선택하는 것을 방지합니다. macOS 10.13 이상에 해당합니다.

- **iCloud 문서 및 데스크탑:** 사용자가 iCloud 데스크탑 및 문서를 설정하는 것을 방지합니다. macOS 10.13 이상에 해당합니다.
- **모양:** 사용자가 모양 모드를 선택하는 것을 방지합니다. macOS 10.14 이상에 해당합니다.
- **손쉬운 사용:** 사용자가 Voice Over를 자동으로 듣는 것을 방지합니다. 장치가 이더넷에 연결된 경우에만 사용할 수 있습니다. macOS 11 이상에 해당합니다.
- **생체 인식:** 사용자가 Touch ID 및 Face ID를 설정하지 못하도록 합니다. macOS 10.12.4 이상에서 사용 가능합니다.
- **True Tone:** 사용자가 디스플레이의 화이트 밸런스를 동적으로 조정하기 위해 4채널 센서를 설정하지 못하도록 합니다. macOS 10.13.6 이상에서 사용 가능합니다.
- **Apple Pay:** 사용자가 Apple Pay를 설정하지 못하도록 합니다. 이 설정을 지우면 사용자는 Touch ID 및 Apple ID를 설정해야 합니다. **Apple ID** 및 **생체 인식** 설정이 지워져 있는지 확인하십시오. macOS 10.12.4 이상에서 사용 가능합니다.
- **스크린 타임:** 사용자가 스크린 타임을 활성화하지 못하도록 합니다. macOS 10.15 이상에서 사용 가능합니다.
- **로컬 계정 설정 옵션:** 장치에 관리자 계정을 생성하기 위한 설정을 지정합니다. 사용자는 이 정보로 macOS 장치에 로그인합니다. XenMobile은 지정된 정보를 사용하여 계정을 생성합니다.
  - **기본 계정을 표준 사용자로 생성:** 이 사용자에게 장치에 대한 관리자 권한을 부여하는 대신, XenMobile은 표준 권한을 가진 사용자를 생성합니다. macOS는 관리자 계정을 필요로 하므로, XenMobile은 먼저 관리자 계정을 생성한 다음 새 표준 계정을 만들고 이를 기본 계정으로 설정합니다.
  - **관리자 전체 이름:** 시스템이 관리자 계정에 표시할 이름을 입력합니다.
  - **관리자 짧은 이름:** 장치가 홈 폴더 및 셸에 표시할 이름을 입력합니다.
  - **관리자 암호:** 관리자 계정에 대한 보안 암호를 입력합니다.
  - **사용자 및 그룹에 관리자 계정 표시:** 이 설정을 지우면 관리자 계정이 macOS 설정의 **사용자 및 그룹**에 표시되지 않습니다. 기본 계정을 표준 사용자로 생성하는 경우, 이 설정을 활성화하여 XenMobile이 먼저 생성하는 관리자 계정을 숨깁니다.

배포 프로그램 지원 장치 주문

배포 프로그램 지원 장치는 Apple 또는 배포 프로그램 지원 공인 리셀러나 통신사에서 직접 주문할 수 있습니다. Apple에서 주문하려면 Apple 배포 프로그램 포털에 Apple 고객 ID를 제공하십시오. 고객 ID를 통해 Apple은 구매한 장치를 Apple 배포 프로그램 계정과 연결할 수 있습니다.

리셀러 또는 통신사에서 주문하려면 Apple 리셀러 또는 통신사에 문의하여 Apple 배포 프로그램에 참여하는지 확인하십시오. 장치를 구매할 때 리셀러의 Apple 배포 프로그램 ID를 요청하십시오. Apple은 Apple 배포

프로그램 리셀러를 Apple 배포 프로그램 계정에 추가할 때 해당 정보를 요구합니다. 리셀러의 Apple 배포 프로그램 ID를 추가하면 배포 프로그램 고객 ID를 받게 됩니다. 배포 프로그램 고객 ID를 리셀러에게 제공하면 리셀러는 이 ID를 사용하여 장치 구매 정보를 Apple에 제출합니다. 자세한 내용은 이 Apple 장치 등록 사이트를 참조하십시오.

배포 프로그램 지원 장치 관리

주문이 배송된 후 iOS, iPadOS 및 macOS 장치를 XenMobile Server와 연결할 수 있습니다.

1. 관리자 또는 기기 등록 관리자 계정을 사용하여 Apple Business Manager에 로그인합니다.
2. 사이드바에서 **기기**를 클릭합니다. Apple에서 직접 구매한 기기는 자동으로 나타납니다. Apple Configurator 2의 기기를 Apple Business Manager에 할당하려면 Apple Business Manager 사용 설명서를 참조하십시오.
3. 목록에서 기기 또는 총 기기 수를 선택하고 **기기 관리 편집**을 클릭합니다. 두 가지 옵션이 있습니다.

    - MDM 서버에 기기를 할당하려면 **서버에 할당**에서 XenMobile Server의 이름을 선택합니다. **계속**을 클릭합니다.

      새 기기를 Apple Business Manager에 대량으로 할당하려면 배포를 위한 기본 XenMobile Server를 설정합니다. 자세한 내용은 대량 등록을 위한 기본 서버 설정을 참조하십시오.
    - XenMobile Server에서 기기 할당을 해제하려면 **할당 해제**를 선택합니다.

이제 Apple 배포 프로그램 기기가 선택한 XenMobile Server와 연결됩니다.

iOS, iPadOS 또는 macOS 기기를 서비스 수리를 위해 보내는 경우 Apple Business Manager에서 해당 기기를 제거해야 합니다. 수리된 기기를 다시 받으면 해당 기기를 XenMobile Server에 다시 할당해야 합니다. 기기를 교체하는 경우 주문 번호를 사용하여 새 기기를 XenMobile Server에 할당할 수 있습니다.

할당된 기기의 기록을 검토하려면 다음을 수행합니다.

1. 관리자 또는 기기 등록 관리자 계정을 사용하여 Apple Business Manager에 로그인합니다.
2. 사이드바에서 **할당 기록**을 클릭합니다. 그런 다음 할당을 선택하여 자세한 정보를 확인합니다.
3. **다운로드**를 클릭하여 할당된 모든 기기와 할당되지 않은 모든 기기의 일련 번호가 포함된 CSV 파일을 다운로드합니다.

기기가 판매되었거나 도난당했거나 수리할 수 없는 경우 Apple Business Manager에서 iOS, iPadOS 및 macOS 기기를 제거할 수 있습니다.

1. 관리자 또는 기기 등록 관리자 계정을 사용하여 Apple Business Manager에 로그인합니다.
2. 사이드바에서 **기기**를 클릭하고 기기를 검색합니다.

3. 장치를 선택하고 **장치 해제**를 클릭합니다. 대화 상자에서 변경 사항을 확인하여 프로그램에서 장치를 제거합니다. iOS 및 iPadOS 장치를 다시 추가하려면 Apple Configurator 2를 사용하십시오. Apple Configurator 2로는 macOS 장치를 다시 추가할 수 없습니다.

장치 등록

사용자 장치를 원격으로 안전하게 관리하려면 XenMobile에 사용자 장치를 등록해야 합니다. XenMobile 클라이언트 소프트웨어가 사용자 장치에 설치되고 사용자 ID가 인증됩니다. 그런 다음 XenMobile 및 사용자 프로필이 설치됩니다. 다음으로 XenMobile 콘솔에서 장치 관리 작업을 수행할 수 있습니다. 정책을 적용하고, 앱을 배포하고, 장치에 데이터를 푸시하고, 분실 또는 도난당한 장치를 잠그고, 초기화하고, 찾을 수 있습니다.

Azure Active Directory 등록은 iOS, Android, Windows 10 및 Windows 11 장치에서 지원됩니다. Azure를 ID 공급자(IdP)로 구성하는 방법에 대한 자세한 내용은 IdP로 Azure Active Directory와 XenMobile 통합을 참조하십시오.

> **참고:**

> iOS 장치 사용자를 등록하려면 먼저 APNs 인증서를 요청해야 합니다. 자세한 내용은 인증서 및 인증을 참조하십시오.

> 사용자 및 장치에 대한 구성 옵션을 업데이트하려면 **관리 > 등록 초대** 페이지로 이동하십시오. 자세한 내용은 이 문서의 등록 초대 보내기를 참조하십시오.

Android 장치

> **참고:**

> Android Enterprise 장치 등록에 대한 자세한 내용은 Android Enterprise를 참조하십시오.

1. Android 장치에서 Google Play 스토어로 이동하여 Citrix Secure Hub™ 앱을 다운로드한 다음 앱을 탭합니다.
2. 앱을 설치하라는 메시지가 표시되면 **다음**을 클릭한 다음 **설치**를 클릭합니다.
3. Secure Hub가 설치되면 **열기**를 탭합니다.

4. XenMobile Server 이름, 사용자 계정 이름(UPN) 또는 이메일 주소와 같은 회사 자격 증명을 입력합니다. 그런 다음 **다음**을 클릭합니다.
5. **장치 관리자 활성화** 화면에서 **활성화**를 탭합니다.
6. 회사 암호를 입력한 다음 **로그온**을 탭합니다.
7. XenMobile 구성 방식에 따라 Citrix PIN을 생성하라는 메시지가 표시될 수 있습니다. 이 PIN을 사용하여 Secure Hub 및 Secure Mail, Citrix Files와 같은 다른 XenMobile 지원 앱에 로그인할 수 있습니다. Citrix PIN을 두 번 입력합니다. **Citrix PIN 생성** 화면에서 PIN을 입력합니다.
8. PIN을 다시 입력합니다. Secure Hub가 열립니다. 그런 다음 XenMobile Store에 액세스하여 Android 장치에 설치할 수 있는 앱을 볼 수 있습니다.
9. 등록 후 XenMobile을 구성하여 앱을 장치로 자동으로 푸시하도록 설정한 경우, 사용자에게 앱 설치를 요청하는 메시지가 표시됩니다. 또한 XenMobile에서 구성한 정책이 장치에 배포됩니다. 앱을 설치하려면 **설치**를 탭합니다.

Android 장치 등록 취소 및 재등록 방법

사용자는 Secure Hub 내에서 등록을 취소할 수 있습니다. 다음 절차를 사용하여 등록을 취소하더라도 장치는 XenMobile 콘솔의 장치 인벤토리에 계속 표시됩니다. 그러나 장치에 대한 작업을 수행할 수는 없습니다. 장치를 추적할 수 없으며 장치 규정 준수를 모니터링할 수 없습니다.

1. Secure Hub 앱을 탭하여 엽니다.
2. 휴대폰 또는 태블릿 사용 여부에 따라 다음을 수행합니다.

   휴대폰에서:

   - 화면 왼쪽에서 스와이프하여 설정 창을 엽니다.
   - **기본 설정**을 탭하고 **계정**을 탭한 다음 **계정 삭제**를 탭합니다.

   태블릿에서:

   - 오른쪽 상단 모서리에 있는 이메일 주소 옆의 화살표를 탭합니다.
   - **기본 설정**을 탭하고 **계정**을 탭한 다음 **계정 삭제**를 탭합니다.
3. **재등록**을 탭합니다. 장치를 재등록할 것인지 확인하는 메시지가 나타납니다.
4. **확인**을 탭합니다.

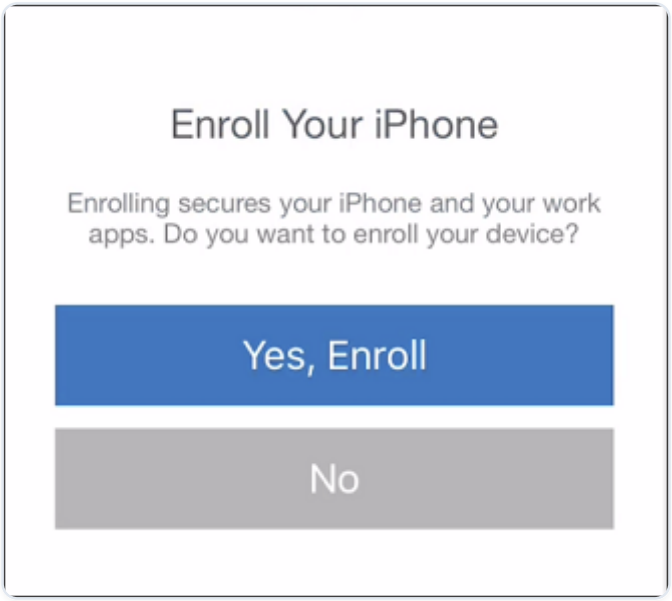
   기기가 등록 해제되었습니다.
5. 화면의 지침에 따라 기기를 다시 등록하십시오.

iOS 기기 등록

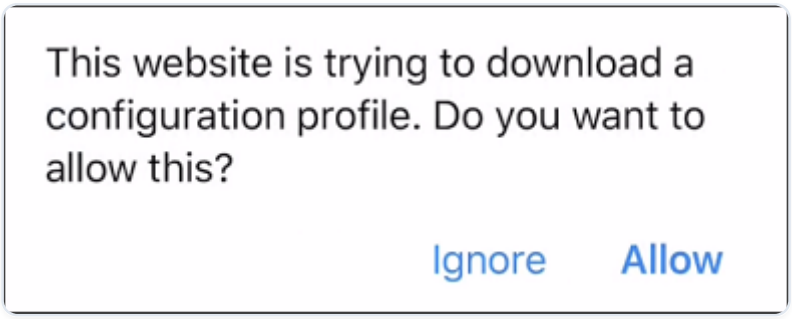
이 섹션에서는 사용자가 iOS 기기(12.2 이상)를 XenMobile Server에 등록하는 방법을 보여줍니다. iOS 등록에 대한 자세한 내용은 다음 비디오를 참조하십시오.



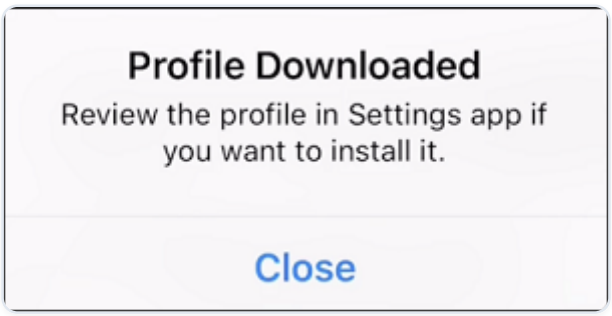
1. iOS 기기에서 Apple Store로 이동하여 Citrix Secure Hub 앱을 다운로드한 다음 앱을 탭합니다.
2. 앱 설치를 요청하면 **다음**을 탭한 다음 **설치**를 탭합니다.
3. Secure Hub가 설치되면 **열기**를 탭합니다.
4. XenMobile Server 이름, 사용자 계정 이름(UPN) 또는 이메일 주소와 같은 회사 자격 증명을 입력합니다. 그런 다음 **다음**을 클릭합니다.
5. iOS 기기를 등록하려면 **예, 등록**을 탭합니다.



6. 자격 증명을 입력한 후 메시지가 표시되면 구성 프로필을 다운로드하기 위해 **허용**을 탭합니다.



7. 구성 프로필을 다운로드한 후 **닫기**를 탭합니다.



8. 기기 설정에서 iOS 인증서를 설치하고 기기를 신뢰할 수 있는 목록에 추가합니다.

   - **설정 > 일반 > 프로필 > XenMobile 프로필 서비스**로 이동하여 **설치**를 탭하여 프로필을 추가합니다.

     프로필 추가(/en-us/xenmobile/server/media/simpler-enrollment-ios-4.png)

   - 알림 창에서 **신뢰**를 탭하여 기기를 원격 관리로 등록합니다.

     신뢰 설정(/en-us/xenmobile/server/media/simpler-enrollment-ios-5.png)

9. Secure Hub에 로그인합니다. MDM+MAM에 등록하는 경우: 자격 증명이 확인되면 메시지가 표시될 때 Citrix PIN을 생성하고 확인합니다.
10. 워크플로가 완료되면 기기가 등록됩니다. 그런 다음 앱 스토어에 액세스하여 iOS 기기에 설치할 수 있는 앱을 볼 수 있습니다.

iOS 기기

1. 기기에서 Apple iTunes App Store에서 Secure Hub 앱을 다운로드한 다음 기기에 앱을 설치합니다.
2. iOS 기기 홈 화면에서 Secure Hub 앱을 탭합니다.
3. Secure Hub 앱이 열리면 헬프 데스크에서 제공한 서버 주소를 입력합니다.

   XenMobile 구성 방식에 따라 표시되는 화면이 이 예시와 다를 수 있습니다.

4. 메시지가 표시되면 사용자 이름과 암호 또는 PIN을 입력합니다. **다음**을 클릭합니다.

5. 등록하라는 메시지가 표시되면 **예, 등록**을 클릭한 다음 메시지가 표시될 때 자격 증명을 입력합니다.
6. **설치**를 탭하여 Citrix Profile Services를 설치합니다.

   Citrix Profile Services 화면 이미지(/en-us/xenmobile/server/media/worxhome-enroll-5.png)
7. **신뢰**를 탭합니다.

   원격 관리 신뢰 화면 이미지(/en-us/xenmobile/server/media/worxhome-enroll-8.png)
8. **열기**를 탭한 다음 자격 증명을 입력합니다.

macOS 장치

XenMobile은 macOS를 실행하는 장치를 등록하는 두 가지 방법을 제공합니다. 두 가지 방법 모두 macOS 사용자가 장치에서 직접 무선으로 등록할 수 있도록 합니다.

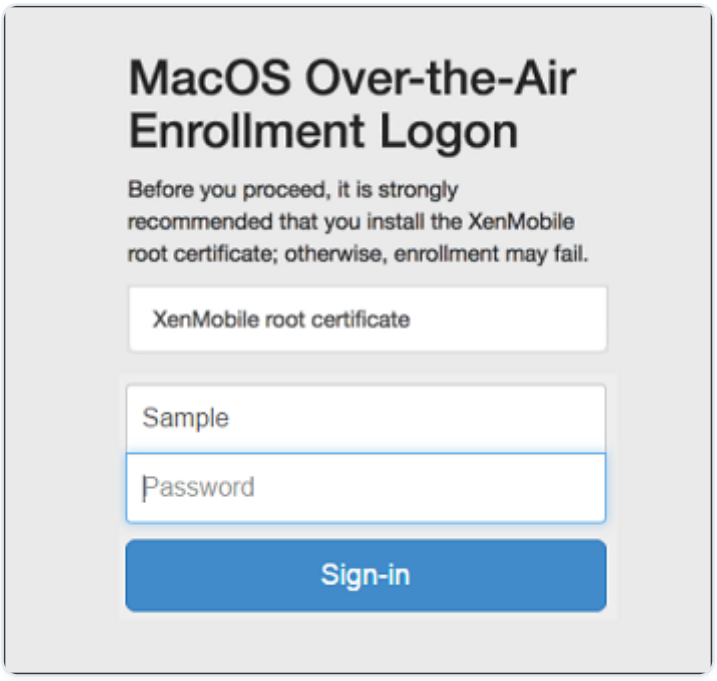
- **사용자에게 등록 초대 보내기:** 이 등록 방법을 사용하면 macOS 장치에 대해 다음 등록 보안 모드 중 하나를 설정할 수 있습니다.
  - 사용자 이름 + 암호
  - 사용자 이름 + PIN
  - 두 가지 요소

  사용자가 등록 초대의 지침을 따르면 사용자 이름이 채워진 로그인 화면이 나타납니다.
- **사용자에게 설치 링크 보내기:** macOS 장치에 대한 이 등록 방법은 사용자에게 등록 링크를 보내며, 사용자는 이 링크를 Safari 또는 Chrome 브라우저에서 열 수 있습니다. 그런 다음 사용자는 사용자 이름과 암호를 입력하여 등록합니다.

  macOS 장치에 대한 등록 링크 사용을 방지하려면 서버 속성 **Enable macOS OTAE**를 **false**로 설정합니다. 결과적으로 macOS 사용자는 등록 초대를 통해서만 등록할 수 있습니다.

사용자에게 등록 초대 보내기

1. 선택적으로 XenMobile 콘솔에서 macOS 장치 정책을 설정합니다. 장치 정책에 대한 자세한 내용은 장치 정책을 참조하십시오.
2. macOS 사용자 등록을 위한 초대장을 추가합니다. 자세한 내용은 이 문서의 등록 초대장 보내기를 참조하십시오.
3. 사용자가 초대장을 받고 링크를 클릭하면 Safari 브라우저에 다음 화면이 나타납니다. XenMobile이 사용자 이름을 채웁니다. 등록 보안 모드로 **두 가지 요소**를 선택한 경우 다른 필드가 나타납니다.



4. 사용자는 필요에 따라 인증서를 설치합니다. 사용자가 인증서 설치 프롬프트를 보는지 여부는 macOS에 대해 다음을 구성했는지에 따라 달라집니다. 공개적으로 신뢰할 수 있는 SSL 인증서 및 공개적으로 신뢰할 수 있는 디지털 서명 인증서. 인증서에 대한 자세한 내용은 인증서 및 인증을 참조하십시오.
5. 사용자는 요청된 자격 증명을 제공합니다.

   Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하는 것과 마찬가지로 XenMobile을 사용하여 Mac을 관리할 수 있습니다.

사용자에게 설치 링크 보내기

1. 필요에 따라 XenMobile 콘솔에서 macOS 장치 정책을 설정합니다. 장치 정책에 대한 자세한 내용은 장치 정책을 참조하십시오.
2. 사용자가 Safari 또는 Chrome 브라우저에서 열 수 있는 등록 링크 `https://serverFQDN:8443/instanceName/macos/otae`를 보냅니다.

   - **serverFQDN**은 XenMobile을 실행하는 서버의 정규화된 도메인 이름(FQDN)입니다.
   - 포트 **8443**은 기본 보안 포트입니다. 다른 포트를 구성한 경우 8443 대신 해당 포트를 사용하십시오.
   - 종종 zdm으로 표시되는 **instanceName**은 서버 설치 중에 지정된 이름입니다.

   설치 링크 전송에 대한 자세한 내용은 설치 링크를 보내려면을 참조하십시오.
3. 사용자는 필요에 따라 인증서를 설치합니다. iOS 및 macOS용으로 공개적으로 신뢰할 수 있는 SSL 인증서 및 디지털 서명 인증서를 구성한 경우 사용자는 인증서 설치 프롬프트를 보게 됩니다. 인증서에 대한 자세한 내용은 인증서 및 인증을 참조하십시오.
4. 사용자는 Mac에 로그인합니다.

Mac 장치 정책이 설치됩니다. 이제 모바일 장치를 관리하는 것과 마찬가지로 XenMobile을 사용하여 Mac을 관리할 수 있습니다.

Windows 장치

Windows 10 및 Windows 11 장치는 Active Directory 인증의 페더레이션 방식으로 Azure에 등록됩니다. 다음 방법 중 하나로 Windows 10 및 Windows 11 장치를 Microsoft Azure AD에 연결할 수 있습니다.

- 장치 전원을 처음 켤 때 기본 제공되는 Azure AD Join의 일부로 MDM에 등록합니다.
- 장치 구성 후 Windows 설정 페이지에서 Azure AD Join의 일부로 MDM에 등록합니다.

다음 Windows 운영 체제를 실행하는 장치를 XenMobile에 등록할 수 있습니다.

- 윈도우 10
- 윈도우 11

사용자는 장치를 통해 직접 등록할 수 있습니다.

> **참고:**

> Windows 10 RS2 Phone 및 Tablet의 경우 재등록 중에 사용자에게 서버 URL을 묻는 메시지가 표시되지 않습니다. 이 문제를 해결하려면 장치를 다시 시작하십시오. 또는 이메일 주소 화면에서 **서비스에 연결 중** 옆의 X를 탭하여 서버 URL 페이지로 이동하십시오. 이는 타사 문제입니다.

> 지원되는 Windows 장치 관리를 활성화하려면 사용자 등록을 위해 AutoDiscovery 및 Windows 검색 서비스를 구성해야 합니다.

Windows 장치 사용자가 Azure를 사용하여 등록하기 전에 XenMobile에서 Microsoft Azure 서버 설정을 구성해야 합니다. 자세한 내용은 Microsoft Azure Active Directory 서버 설정을 참조하십시오.

자동 검색으로 Windows 장치를 등록하려면

Windows 장치 관리를 활성화하려면 Citrix는 AutoDiscovery Service 및 Windows 검색 서비스를 구성할 것을 권장합니다. 자세한 내용은 XenMobile AutoDiscovery Service를 참조하십시오.

1. 장치에서 사용 가능한 모든 Windows 업데이트를 확인하고 설치합니다.
2. 참 메뉴에서 **설정**을 탭한 다음 **계정 > 회사 또는 학교 액세스 > 회사 또는 학교에 연결**을 탭합니다.
3. Windows 10 및 Windows 11의 경우: 회사 이메일 주소를 입력한 다음 **계속**을 탭합니다. Windows 8.1의 경우: **장치 관리 켜기**를 탭합니다. 로컬 사용자로 등록하려면 올바른 도메인 이름을 가진 존재하지 않는 이메일 주소를 입력합니다(예: `foo@mydomain.com`). 이렇게 하면 Windows의 기본 제공 장치 관리에

서 등록이 수행되는 알려진 Microsoft 제한 사항을 우회할 수 있습니다. **서비스에 연결** 대화 상자에서 로컬 사용자와 연결된 사용자 이름과 암호를 입력합니다. 장치가 자동으로 XenMobile Server를 찾아 등록 프로세스를 시작합니다.

4. 암호를 입력합니다. XenMobile의 사용자 그룹에 속한 계정과 연결된 암호를 사용합니다.
5. Windows 10 및 Windows 11의 경우: **사용 약관** 대화 상자에서 장치 관리에 동의함을 표시한 다음 **수락**을 탭합니다. Windows 8.1의 경우: **IT 관리자의 앱 및 서비스 허용** 대화 상자에서 장치 관리에 동의함을 표시한 다음 **켜기**를 탭합니다.

자동 검색 없이 Windows 장치 등록

AutoDiscovery 없이 Windows 장치를 등록할 수 있습니다. 그러나 Citrix는 AutoDiscovery를 구성할 것을 권장합니다. AutoDiscovery 없이 등록하면 원하는 URL에 연결하기 전에 포트 80으로 호출이 발생하므로 프로덕션 배포에 대한 모범 사례로 간주되지 않습니다. Citrix는 이 프로세스를 테스트 환경 및 개념 증명 배포에서만 사용할 것을 권장합니다.

1. 장치에서 사용 가능한 모든 Windows 업데이트를 확인하고 설치합니다.
2. Windows 10 및 Windows 11의 경우: 참 메뉴에서 **설정**을 탭한 다음 **계정 > 회사 또는 학교 액세스 > 회사 또는 학교에 연결**을 탭합니다. Windows 8.1의 경우: **PC 설정 > 네트워크 > 회사**를 탭합니다.
3. 회사 이메일 주소를 입력합니다.
4. Windows 10 및 Windows 11의 경우: AutoDiscovery가 구성되지 않은 경우 5단계에 설명된 대로 서버 세부 정보를 입력할 수 있는 옵션이 나타납니다. Windows 8.1의 경우: **서버 주소 자동 검색**이 **켜짐**으로 설정되어 있으면 탭하여 옵션을 **끔**으로 전환합니다.
5. Windows 10 및 Windows 11의 경우 **서버 주소 입력** 필드에 다음 주소를 입력합니다. `https://serverfqdn:8443/serverInstance/wpe`.

   인증되지 않은 SSL 연결에 8443 이외의 포트가 사용되는 경우 이 주소에서 8443 대신 해당 포트 번호를 사용합니다.

   Windows 8.1의 경우: 다음 형식으로 서버 주소를 입력합니다. `https://serverfqdn:8443/serverInstance/Discovery.svc`.

   인증되지 않은 SSL 연결에 8443 이외의 포트가 사용되는 경우 이 주소에서 8443 대신 해당 포트 번호를 사용합니다.
6. 암호를 입력합니다.
7. Windows 10 및 Windows 11의 경우: **사용 약관** 대화 상자에서 장치 관리에 동의함을 표시한 다음 **수락**을 탭합니다. Windows 8.1의 경우: **IT 관리자로부터 앱 및 서비스 허용** 대화 상자에서 장치 관리에 동의함을 표시한 다음 **켜기**를 탭합니다.

등록 초대 보내기

XenMobile 콘솔에서 iOS, macOS, Android Enterprise 및 레거시 Android 장치를 사용하는 사용자에게 등록 초대를 보낼 수 있습니다. iOS, Android Enterprise 또는 레거시 Android 장치를 사용하는 사용자에게 설치 링크를 보낼 수도 있습니다.

등록 초대는 다음과 같이 전송됩니다.

- 등록 초대가 단일 로컬 또는 Active Directory 사용자를 위한 경우: 사용자는 지정한 전화 번호 및 통신사 이름으로 SMS를 통해 초대를 받습니다.
- 등록 초대가 그룹을 위한 경우: 사용자는 SMS를 통해 초대를 받습니다. Active Directory 사용자가 Active Directory에 이메일 주소와 휴대폰 번호를 가지고 있는 경우 초대를 받습니다. 로컬 사용자는 사용자 속성에 지정된 이메일 및 전화 번호로 초대를 받습니다.

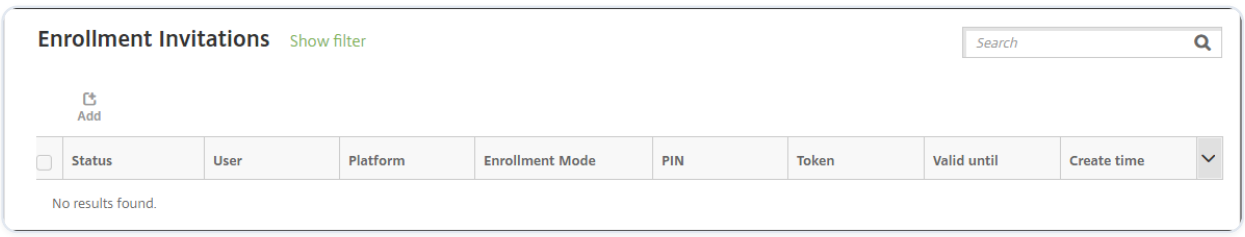
사용자가 등록하면 해당 장치가 **관리 > 장치**에 관리됨으로 표시됩니다. 초대 URL의 상태는 **사용됨**으로 표시됩니다.

전제 조건

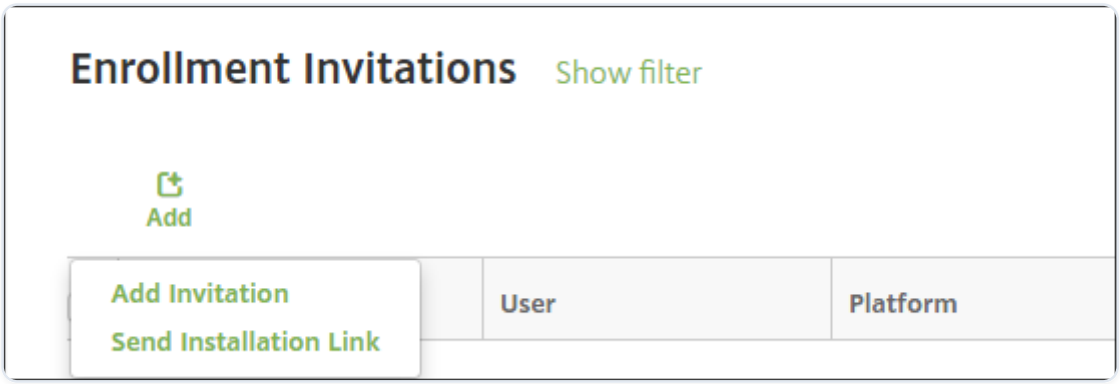
- Enterprise(XME) 또는 MDM 모드로 구성된 XenMobile Server
- LDAP 구성됨
- 로컬 그룹 및 로컬 사용자 사용 시:
  - 하나 이상의 로컬 그룹.
  - 로컬 그룹에 할당된 로컬 사용자.
  - 전달 그룹이 로컬 그룹과 연결되어 있습니다.
- Active Directory를 사용하는 경우:
  - 전송 그룹은 Active Directory 그룹과 연결됩니다.

등록 초대 만들기

1. XenMobile 콘솔에서 **관리 > 등록 초대**를 클릭합니다. **등록 초대** 페이지가 나타납니다.



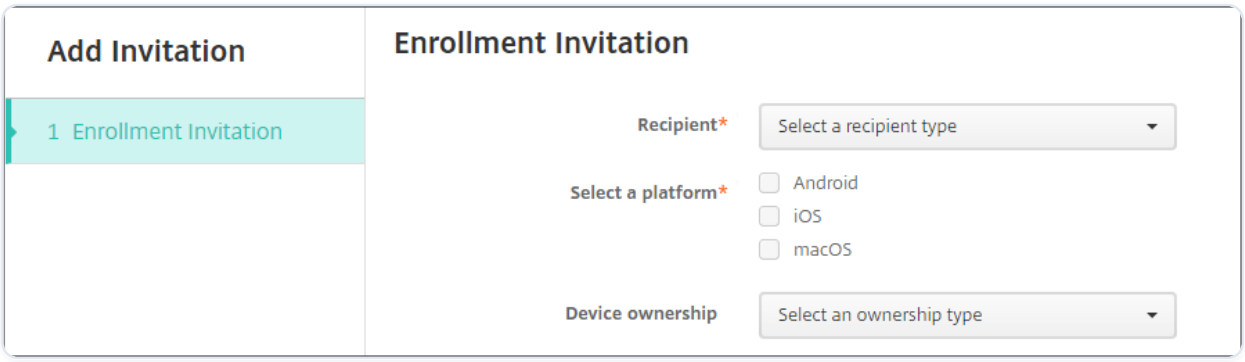
2. **추가**를 클릭합니다. 등록 옵션 메뉴가 나타납니다.



- 사용자 또는 그룹에 등록 초대를 보내려면 **초대 추가**를 클릭합니다.
- SMTP 또는 SMS를 통해 수신자 목록에 등록 설치 링크를 보내려면 **설치 링크 보내기**를 클릭합니다.

등록 초대 및 설치 링크 보내기는 다음 단계 다음에 설명되어 있습니다.

3. **초대 추가**를 클릭합니다. **등록 초대** 화면이 나타납니다.



4. 다음 설정을 구성합니다.

- **수신자: 그룹** 또는 **사용자**를 선택합니다.
- **플랫폼 선택: 수신자**가 **그룹**인 경우 모든 플랫폼이 선택됩니다. 플랫폼 선택을 변경할 수 있습니다. **수신자**가 **사용자**인 경우 플랫폼이 선택되지 않습니다. 플랫폼을 선택합니다.

  Android Enterprise 장치에 대한 등록 초대를 생성하려면 **Android > Android Enterprise**를 선택합니다.
- **장치 소유권: 회사** 또는 **직원**을 선택합니다.

다음 섹션에 설명된 대로 사용자 또는 그룹 설정이 나타납니다.

사용자에게 등록 초대 보내기

등록 초대 설정 이미지(/en-us/xenmobile/server/media/manage-enrollment-invitation-user.png)

1. 다음 **사용자** 설정을 구성합니다.

- **사용자 이름:** 사용자 이름을 입력합니다. 사용자는 XenMobile Server에 로컬 사용자 또는 Active Directory의 사용자로 존재해야 합니다. 사용자가 로컬인 경우 해당 사용자에게 알림을 보낼 수 있도

록 사용자의 이메일 속성이 설정되어 있는지 확인합니다. 사용자가 Active Directory에 있는 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 해당하는 값을 입력할 수 있는 필드가 나타납니다.
- **전화 번호:** 여러 플랫폼을 선택하거나 macOS만 선택한 경우에는 이 설정이 나타나지 않습니다. 선택적으로 사용자의 전화 번호를 입력합니다.
- **통신사:** 여러 플랫폼을 선택하거나 macOS만 선택한 경우에는 이 설정이 나타나지 않습니다. 사용자의 전화 번호와 연결할 통신사를 선택합니다.
- **등록 모드:** 사용자의 등록 보안 모드를 선택합니다. 기본값은 **사용자 이름 + 암호**입니다. 다음 옵션 중 일부는 모든 플랫폼에서 사용할 수 없습니다.
  - 사용자 이름 + 암호
  - 높은 보안
  - 초대 URL
  - 초대 URL + PIN
  - 초대 URL + 암호
  - 2단계 인증
  - 사용자 이름 + PIN

등록 초대를 보내려면 **초대 URL**, **초대 URL + PIN** 또는 **초대 URL + 암호** 등록 보안 모드만 사용할 수 있습니다. **사용자 이름 + 암호**, **2단계 인증** 또는 **사용자 이름 + PIN**으로 등록하는 장치의 경우 사용자가 Secure Hub에 자격 증명을 수동으로 입력해야 합니다.

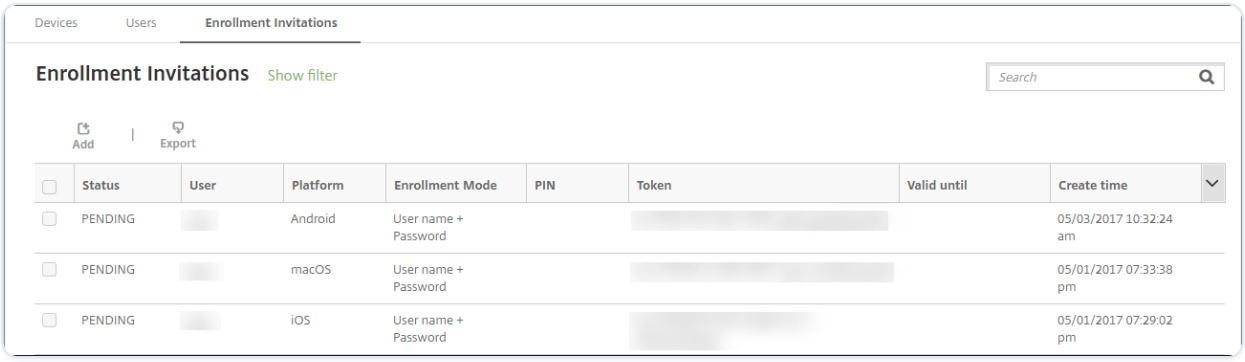
등록용 PIN은 일회용 PIN이라고도 합니다. 이러한 PIN은 사용자가 등록할 때만 유효합니다.

> **참고:**
>
> PIN을 포함하는 등록 보안 모드를 선택하면 **등록 PIN용 템플릿** 필드가 나타나고, 여기서 **등록 PIN**을 클릭합니다.

- **에이전트 다운로드용 템플릿: 다운로드 링크**라는 다운로드 링크 템플릿을 선택합니다. 이 템플릿은 지원되는 모든 플랫폼에 사용됩니다.
- **등록 URL용 템플릿: 등록 초대**를 선택합니다.
- **등록 확인용 템플릿: 등록 확인**을 선택합니다.

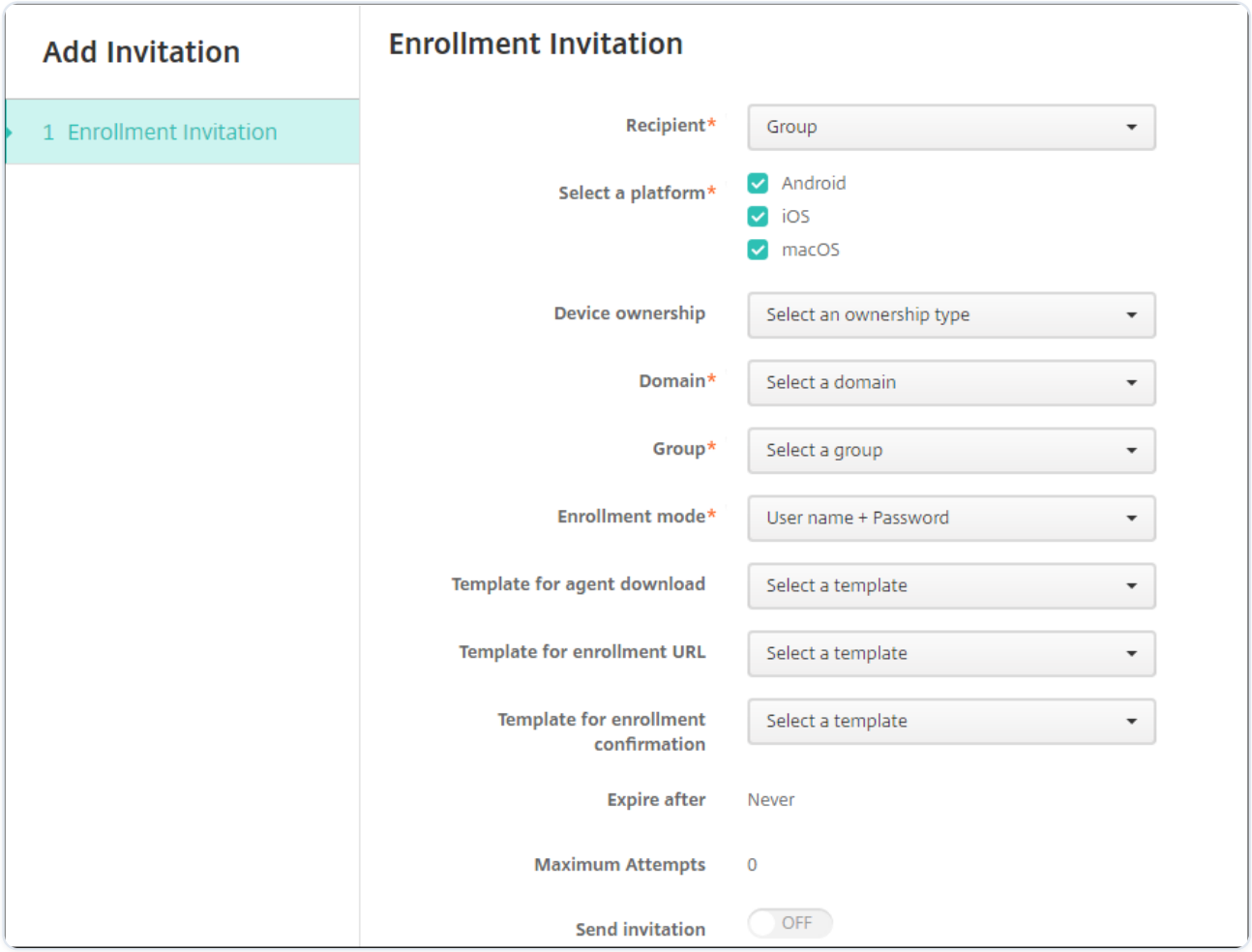
- **만료 기간:** 이 필드는 등록 모드를 구성할 때 설정되며 등록이 만료되는 시기를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 등록 보안 모드 구성을 참조하십시오.
- **최대 시도 횟수:** 이 필드는 **등록 모드**를 구성할 때 설정되며 등록 프로세스가 발생하는 최대 횟수를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 등록 보안 모드 구성을 참조하십시오.
- **초대 보내기:** 초대를 즉시 보내려면 **ON**을 선택합니다. 초대를 **등록 초대** 페이지의 테이블에 추가하지만 보내지 않으려면 **OFF**를 선택합니다.

2. **초대 보내기**를 활성화한 경우 **저장 및 보내기**를 클릭합니다. 그렇지 않은 경우 **저장**을 클릭합니다. 초대가 **등록 초대** 페이지의 테이블에 나타납니다.



그룹에 등록 초대장을 보내려면

다음 그림은 그룹에 대한 등록 초대장을 구성하는 설정을 보여줍니다.



1. 다음 설정을 구성합니다.

   - **도메인:** 초대장을 받을 그룹의 도메인을 선택합니다.
   - **그룹:** 초대장을 받을 그룹을 선택합니다.
   - **등록 모드:** 그룹의 사용자가 등록하는 방법을 선택합니다. 기본값은 **사용자 이름 + 암호**입니다. 다음 옵션 중 일부는 모든 플랫폼에서 사용할 수 없습니다.

     - 사용자 이름 + 암호
     - 높은 보안
     - 초대 URL
     - 초대 URL + PIN
     - 초대 URL + 암호
     - 두 가지 요소
     - 사용자 이름 + PIN

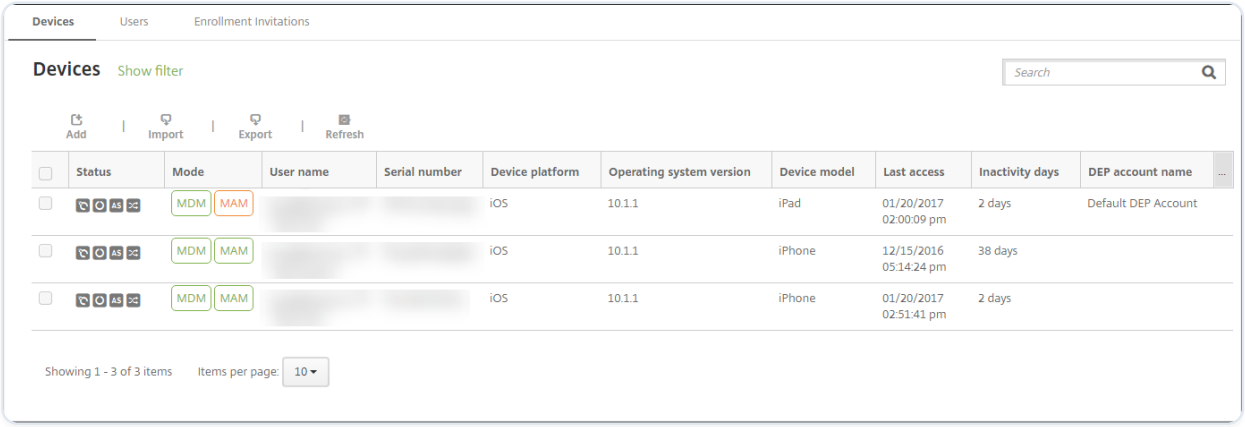
등록 초대장을 보내려면 **초대 URL**, **초대 URL + PIN** 또는 **초대 URL + 암호** 등록 보안 모드만 사용할 수 있습니다. **사용자 이름 + 암호**, **두 가지 요소** 또는 **사용자 이름 + PIN**으로 등록하는 장치의 경우 사용자는 Secure Hub에 자격 증명을 수동으로 입력해야 합니다.

선택한 각 플랫폼에 유효한 등록 보안 모드만 나타납니다.

> **참고:**
>
> PIN이 포함된 등록 보안 모드를 선택하면 **등록 PIN 템플릿** 필드가 나타나고, 여기서 **등록 PIN**을 클릭합니다.

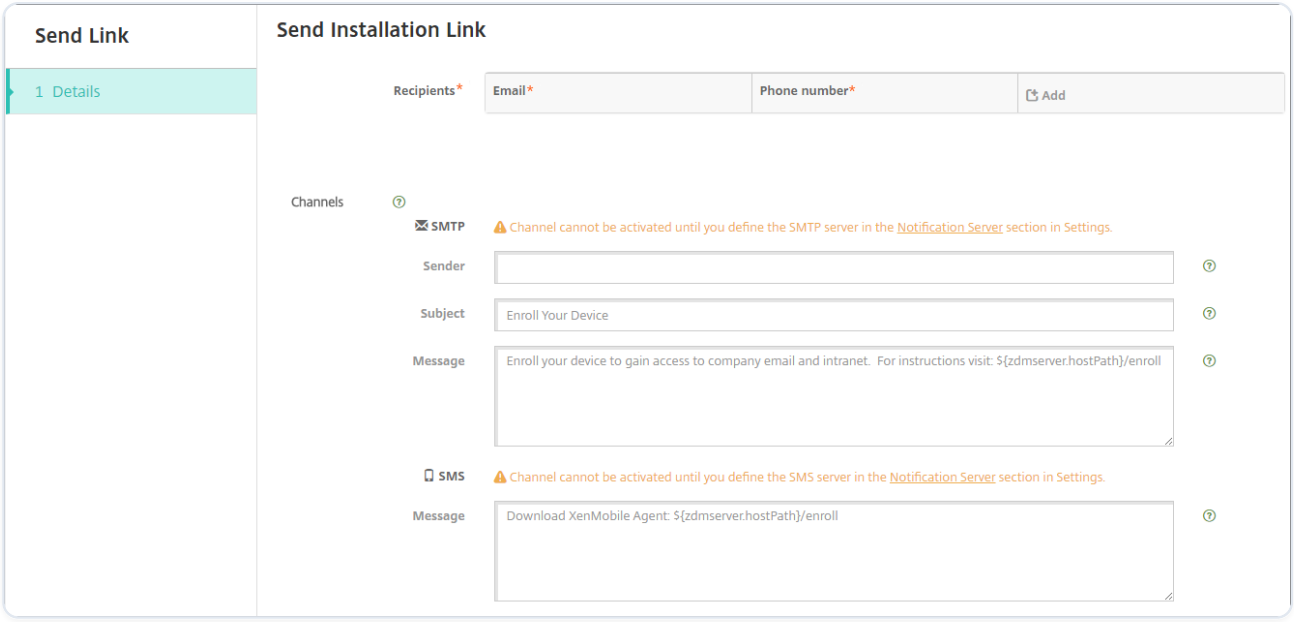
- **에이전트 다운로드 템플릿:** **다운로드 링크:**라는 다운로드 링크 템플릿을 선택합니다. 이 템플릿은 지원되는 모든 플랫폼에 사용됩니다.
- **등록 URL 템플릿: 등록 초대**를 선택합니다.
- **등록 확인 템플릿: 등록 확인**을 선택합니다.
- **만료 기간:** 이 필드는 등록 모드를 구성할 때 설정되며 등록이 만료되는 시기를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 등록 보안 모드 구성을 참조하십시오.
- **최대 시도 횟수:** 이 필드는 등록 모드를 구성할 때 설정되며 등록 프로세스가 발생하는 최대 횟수를 나타냅니다. 등록 보안 모드 구성에 대한 자세한 내용은 등록 보안 모드 구성을 참조하십시오.
- **초대 보내기:** 초대를 즉시 보내려면 **ON**을 선택합니다. 초대를 **등록 초대** 페이지의 테이블에 추가하지만 보내지 않으려면 **OFF**를 선택합니다.

2. **초대 보내기**를 활성화한 경우 **저장 및 보내기**를 클릭합니다. 그렇지 않으면 **저장**을 클릭합니다. 초대는 **등록 초대** 페이지의 테이블에 나타납니다.



설치 링크를 보내려면

등록 설치 링크를 보내려면 먼저 **설정** 페이지에서 알림 서버에 채널(SMTP 또는 SMS)을 구성해야 합니다. 자세한 내용은 알림을 참조하십시오.



1. 이 설정을 구성한 다음 **저장**을 클릭합니다.

   - **받는 사람:** 추가하려는 각 받는 사람에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
     - **이메일:** 받는 사람의 이메일 주소를 입력합니다. 이 필드는 필수입니다.
     - **전화번호:** 받는 사람의 전화번호를 입력합니다. 이 필드는 필수입니다.

   > **참고:**
   >
   > 기존 받는 사람을 삭제하려면 목록이 있는 줄 위로 마우스를 가져간 다음 오른쪽에 있는 휴지통 아이콘을 클릭합니다. 확인 대화 상자가 나타납니다. 목록을 삭제하려면 **삭제**를 클릭하고, 목록을 유지하려면 **취소**를 클릭합니다.

   > 기존 받는 사람을 편집하려면 목록이 있는 줄 위로 마우스를 가져간 다음 오른쪽에 있는 펜 아이콘을 클릭합니다. 목록을 업데이트한 다음 변경된 목록을 저장하려면 **저장**을 클릭하고, 목록을 변경하지 않으려면 **취소**를 클릭합니다.

   - **채널:** 등록 설치 링크를 보내는 데 사용할 채널을 선택합니다. **SMTP** 또는 **SMS**를 통해 알림을 보낼 수 있습니다. 이러한 채널은 **알림 서버**의 **설정** 페이지에서 서버 설정을 구성할 때까지 활성화할 수 없습니다. 자세한 내용은 알림을 참조하십시오.

- **SMTP:** 다음 선택적 설정을 구성합니다. 이 필드에 아무것도 입력하지 않으면 선택한 플랫폼에 대해 구성된 알림 템플릿에 지정된 기본값이 사용됩니다.
  - **보낸 사람:** 선택적 보낸 사람을 입력합니다.
  - **제목:** 메시지에 대한 선택적 제목을 입력합니다. 예를 들어, "장치 등록"과 같습니다.
  - **메시지:** 받는 사람에게 보낼 선택적 메시지를 입력합니다. 예를 들어, "조직 앱 및 이메일에 액세스하려면 장치를 등록하십시오."와 같습니다.
- **SMS:** 이 설정을 구성합니다. 이 필드에 아무것도 입력하지 않으면 선택한 플랫폼에 대해 구성된 알림 템플릿에 지정된 기본값이 사용됩니다.
  - **메시지:** 받는 사람에게 보낼 메시지를 입력합니다. 이 필드는 SMS 기반 알림에 필수입니다.

> **참고:** 북미에서는 160자를 초과하는 SMS 메시지가 여러 메시지로 전달됩니다.

2. **보내기**를 클릭합니다.

> **참고:**
>
> 환경에서 sAMAccountName을 사용하는 경우: 사용자가 초대를 받고 링크를 클릭한 후에는 인증을 완료하기 위해 사용자 이름을 편집해야 합니다. 사용자 이름은 `sAMAccountName@domainname.com` 형식으로 나타납니다. 사용자는 @domainname.com 부분을 제거해야 합니다.

플랫폼별 등록 보안 모드

다음 표는 사용자 장치를 등록하는 데 사용할 수 있는 보안 모드를 보여줍니다. 표에서 **예**는 특정 등록 및 관리 모드를 다양한 등록 프로필과 함께 지원하는 장치 플랫폼을 나타냅니다.

MDM 등록 보안 모드	CITRIX GATEWAY의 MAM 등록 보안 모드	관리 모드	다양한 등록 프로필 지원	ANDROID (레거시)	안드로이드 엔터프라이즈	IOS (사용자 등록 모드)	IOS	MACOS	윈도우즈
Citrix Cloud™를 통한 ID 공급자로서의 Azure AD 및 Okta	클라이언트 인증서	MDM+MAM 또는 MDM	예	예	예	예	예	아니요	아니요
사용자 이름 + 암호	LDAP, LDAP + 클라이언트 인증서, 클라이언트 인증서만	MDM+MAM, MDM 또는 MAM (MAM 전용 모드는 Citrix Gateway에서 클라이언트 인증서를 지원하	예	예	예	예	예	예	예

MDM 등록 보안 모드	CITRIX GATEWAY의 MAM 등록 보안 모드	관리 모드	다양한 등록 프로필 지원	ANDROID (레거시)	안드로이드 엔터프라이즈	IOS (사용자 등록 모드)	IOS	MACOS	윈도우즈
		지 않음)							
초대 URL	클라이언트 인증서	MDM+MAM 또는 MDM	예	예	예	아니요	예	아니요	아니요
초대 URL + PIN	클라이언트 인증서	MDM+MAM 또는 MDM	예	예	예	아니요	예	아니요	아니요
초대 URL + 암호	LDAP, LDAP + 클라이언트 인증서, 클라이언트 인증서만	MDM+MAM 또는 MDM	예	예	예	아니요	예	아니요	아니요
2단계 인증 (사용자 이름 +	LDAP, LDAP + 클라	MDM+MAM 또는 MDM	예	예	예	아니요	예	예	아니요

MDM 등록 보안 모드	CITRIX GATEWAY의 MAM 등록 보안 모드	관리 모드	다양한 등록 프로필 지원	ANDROID (레거시)	안드로이드 엔터프라이즈	IOS (사용자 등록 모드)	IOS	MACOS	윈도우즈
암호 + PIN)	이언트 인증서, 클라이언트 인증서만								
사용자 이름 + PIN	클라이언트 인증서	MDM+MAM 또는 MDM	예	예	예	아니요	예	예	아니요

다음은 iOS, Android 및 Android Enterprise 장치에서 등록 보안 모드가 작동하는 방식을 설명합니다.

- **사용자 이름 + 암호** (기본값)
  - 등록 URL이 포함된 단일 알림을 사용자에게 보냅니다. 사용자가 URL을 클릭하면 Secure Hub가 열립니다. 그러면 사용자는 XenMobile에 장치를 등록하기 위해 사용자 이름과 암호를 입력합니다.
- **초대 URL**
  - 등록 URL이 포함된 단일 알림을 사용자에게 보냅니다. 사용자가 URL을 클릭하면 Secure Hub가 열립니다. XenMobile Server 이름과 **예, 등록** 버튼이 나타납니다. 사용자는 XenMobile에 장치를 등록하기 위해 **예, 등록**을 탭합니다.
- **초대 URL + PIN**
  - 사용자에게 다음 이메일을 보냅니다:
    - 등록 URL이 포함된 이메일로, 사용자가 Secure Hub를 통해 XenMobile에 장치를 등록할 수 있습니다.

    - 장치를 등록할 때 사용자가 입력해야 하는 일회용 PIN과 사용자의 Active Directory(또는 로컬) 암호가 포함된 이메일.
  - 이 모드에서는 사용자가 알림의 등록 URL을 통해서만 등록합니다. 사용자가 알림 초대를 잃어버리면 등록할 수 없습니다. 하지만 다른 초대를 보낼 수 있습니다.

- **초대 URL + 암호**
  - 등록 URL이 포함된 단일 알림을 사용자에게 보냅니다. 사용자가 URL을 클릭하면 Secure Hub가 열립니다. XenMobile Server 이름과 함께 사용자가 암호를 입력할 수 있는 필드가 나타납니다.
- **2단계 인증**
  - 등록 URL과 일회용 PIN이 포함된 단일 알림을 사용자에게 보냅니다. 사용자가 URL을 클릭하면 Secure Hub가 열립니다. XenMobile Server 이름과 함께 사용자가 암호와 PIN 번호를 입력할 수 있는 두 개의 필드가 나타납s니다.
- **사용자 이름 + PIN**
  - 사용자에게 다음 이메일을 보냅니다:
    - 등록 URL이 포함된 이메일로, 사용자가 Secure Hub를 다운로드하고 설치할 수 있습니다. Secure Hub가 열리면 사용자는 XenMobile에 장치를 등록하기 위해 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
    - 장치를 등록할 때 사용자가 입력해야 하는 일회용 PIN과 사용자의 Active Directory(또는 로컬) 암호가 포함된 이메일.
  - 사용자가 알림 초대를 잃어버리면 등록할 수 없습니다. 하지만 다른 초대를 보낼 수 있습니다.

다음은 macOS 장치에서 등록 보안 모드가 작동하는 방식을 설명합니다:

- **사용자 이름 + 암호**
  - 사용자에게 등록 URL이 포함된 단일 알림을 보냅니다. 사용자가 URL을 클릭하면 Safari 브라우저가 열립니다. 로그인 페이지가 나타나고, 사용자에게 XenMobile에 장치를 등록하기 위한 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
- **2단계 인증**
  - 사용자에게 등록 URL과 일회용 PIN이 포함된 단일 알림을 보냅니다. 사용자가 URL을 클릭하면 Safari 브라우저가 열립니다. 로그인 페이지가 나타나고, 사용자에게 암호와 PIN 번호를 입력할 수 있는 두 개의 필드가 표시됩니다.
- **사용자 이름 + PIN**

- 사용자에게 다음 이메일을 보냅니다.
  - 등록 URL이 포함된 이메일. 사용자가 URL을 클릭하면 Safari 브라우저가 열립니다. 로그인 페이지가 나타나고, 사용자에게 XenMobile에 장치를 등록하기 위한 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
  - 장치를 등록할 때 사용자의 Active Directory(또는 로컬) 암호와 함께 입력해야 하는 일회용 PIN이 포함된 이메일.
- 사용자가 알림 초대를 분실하면 등록할 수 없습니다. 하지만 다른 초대를 보낼 수 있습니다.

Windows 장치에는 등록 초대를 보낼 수 없습니다. Windows 사용자는 장치를 통해 직접 등록합니다.

Firebase 클라우드 메시징

> **참고:**
>
> Firebase 클라우드 메시징(FCM)은 이전에 Google 클라우드 메시징(GCM)으로 알려져 있었습니다. 일부 XenMobile® 콘솔 레이블 및 메시지에서는 GCM 용어를 사용합니다.

> Citrix®는 Android 장치가 XenMobile에 연결하는 방법과 시기를 제어하기 위해 Firebase 클라우드 메시징(FCM)을 사용할 것을 권장합니다. FCM용으로 구성된 XenMobile은 FCM이 활성화된 Android 장치에 연결 알림을 보냅니다. 모든 보안 작업 또는 배포 명령은 푸시 알림을 트리거하여 사용자에게 XenMobile Server에 다시 연결하도록 요청합니다.

이 문서의 구성 단계를 완료하고 장치가 체크인하면, 장치는 XenMobile Server의 FCM 서비스에 등록됩니다. 이 연결을 통해 FCM을 사용하여 XenMobile 서비스에서 장치로 거의 실시간 통신이 가능합니다. FCM 등록은 새 장치 등록 및 이전에 등록된 장치 모두에 적용됩니다.

XenMobile이 장치에 대한 연결을 시작해야 할 때 FCM 서비스에 연결합니다. 그러면 FCM 서비스가 장치에 연결하도록 알립니다. 이러한 유형의 연결은 Apple이 푸시 알림 서비스에 사용하는 것과 유사합니다.

전제 조건

- 최신 Secure Hub 클라이언트
- Google 개발자 계정 자격 증명
- FCM 지원 Android 장치에 Google Play 서비스 설치

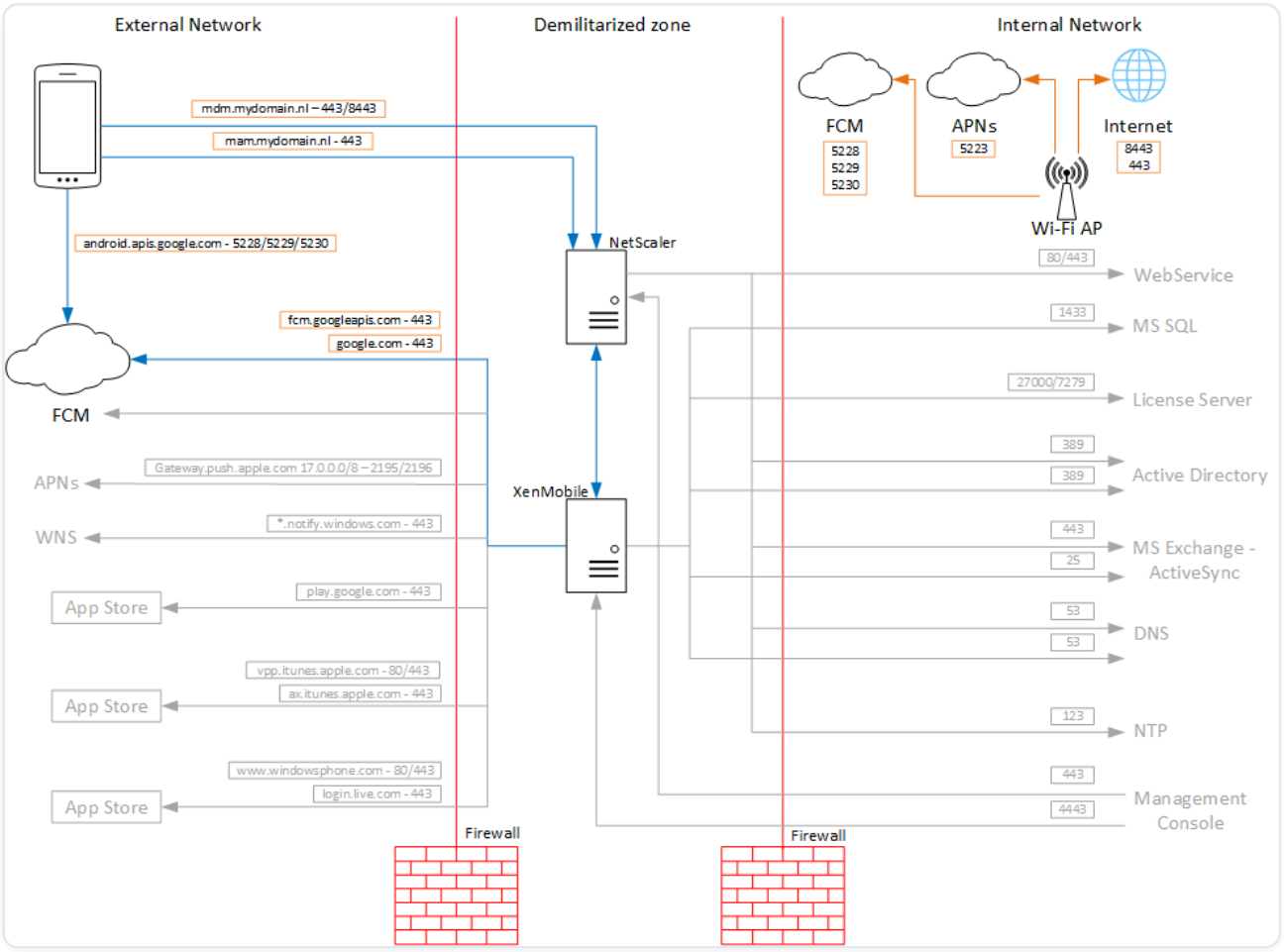
방화벽 포트

- XenMobile에서 `fcm.googleapis.com` 및 `Google.com`로 포트 443을 엽니다.
- 장치 Wi-Fi의 아웃바운드 인터넷 통신을 위해 포트 5228, 5229, 5230을 엽니다.
- 아웃바운드 연결을 허용하려면 FCM은 IP 제한 없이 포트 5228~5230을 허용할 것을 권장합니다. 그러나 IP 제한이 필요한 경우 FCM은 IPv4 및 IPv6 블록의 모든 IP 주소를 허용할 것을 권장합니다. 이러한 블록은 Google ASN of 15169에 나열되어 있습니다. 이 목록은 매월 업데이트하십시오. FCM 포트에 대한 자세한 내용은 Google 문서의 FCM 포트를 참조하십시오.

자세한 내용은 포트 요구 사항을 참조하십시오.

아키텍처

이 다이어그램은 외부 및 내부 네트워크에서 FCM의 통신 흐름을 보여줍니다.

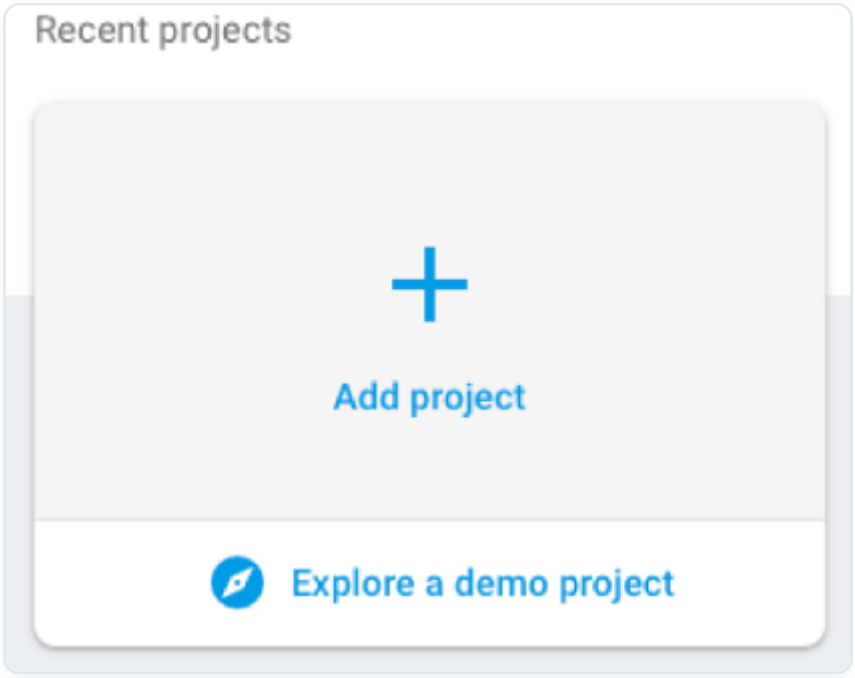


FCM용 Google 계정 구성

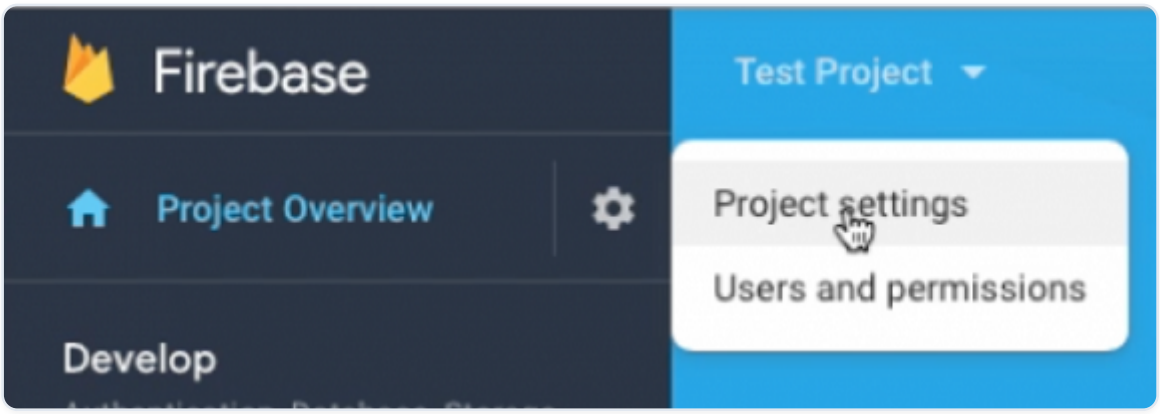
1. Google 개발자 계정 자격 증명을 사용하여 다음 URL에 로그인합니다.

   `<https://console.firebase.google.com/>`

2. **프로젝트 추가**를 클릭합니다.



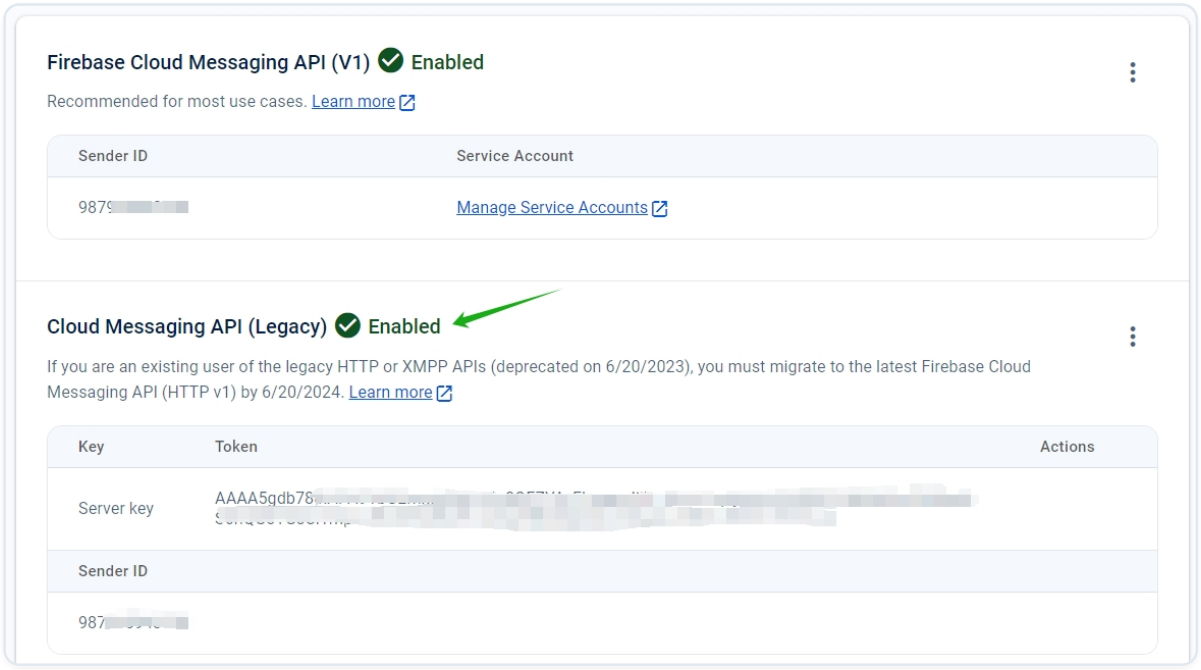
3. 프로젝트를 만든 후 **프로젝트 설정**을 클릭합니다.



> **참고:**
>
> Google은 현재 FCM 구현에 사용되는 HTTP용 FCM 레거시 API를 더 이상 사용하지 않을 예정입니다. 마이그레이션 기한은 June 21, 2024입니다. 레거시 FCM API에서 HTTP v1 API로 FCM을 마이그레이션해야 합니다. 자세한 내용은 레거시 FCM API에서 HTTP v1으로 마이그레이션을 참조하십시오.

4. **클라우드 메시징** 탭을 클릭합니다. Firebase 클라우드 메시징 API가 활성화되어 있는지 확인하고 **서비스 계정 관리**를 클릭합니다.

   a. 마이그레이션 전에 레거시 API를 사용할 수 있었으므로 클라우드 메시징 API(레거시)가 활성화되어 있는지 확인하십시오. **키** 및 **보낸 사람 ID** 필드에서 값을 복사합니다.



키가 나열되어 있지 않다면, **Actions** 아래의 줄임표를 클릭하여 키를 추가합니다.

작업(/en-us/xenmobile/server/media/fcm-copy-key-oauth-id.png)

b. 마이그레이션 후, Google에서 레거시 API가 더 이상 사용되지 않습니다. Firebase Cloud Messaging API(V1)를 활성화해야 합니다. 자세한 내용은 레거시 FCM API에서 HTTP v1으로 마이그레이션을 참조하십시오.

FCI 활성화(/en-us/xenmobile/server/media/enable-fcm.png)

프로젝트 설정 아래의 **서비스 계정**에서 서비스 계정 JSON 파일을 다운로드합니다. 서비스 계정에 대한 개인 키 파일을 생성하려면 자격 증명 수동 제공 섹션을 참조하십시오. **새 개인 키 생성**을 클릭하여 서비스 계정 키 JSON 파일을 다운로드합니다.

프로젝트 설정(/en-us/xenmobile/server/media/project-settings.png)

Android에서 FCM 클라이언트 앱을 설정하는 단계는 이 Google 개발자 클라우드 메시징 문서를 참조하십시오. `<https://firebase.google.com/docs/cloud-messaging/android/client>`.

FCM용 XenMobile 구성

XenMobile 콘솔에서 **설정 > Firebase Cloud Messaging**으로 이동합니다.

클라우드 메시징 API(레거시)용

1. Firebase Cloud Messaging 구성의 마지막 단계에서 얻은 Firebase Cloud Messaging **키**를 **API 키** 필드에 입력합니다.
2. 이전 절차에서 얻은 **보낸 사람 ID** 값을 입력합니다.

보낸 사람 ID 값 입력(/en-us/xenmobile/server/media/settings-google-cloud-messaging.png)

Firebase 클라우드 메시징 API (V1)용

> **참고:**
>
> - XenMobile Server 버전 10.15 롤링 패치 7 이상에서 FCM API V1을 활성화하려면 Knowledge Center 문서 CTX677031을 참조하십시오.
> - 새로운 FCM 사용자라면 1단계를 건너뛰고 2단계부터 진행하십시오.

1. 이미 FCM을 사용 중인 경우, 발신자 ID(Sender ID)가 현재 FCM 프로젝트로 자동 채워지고 **서비스 계정 키 파일(Service Account Key File)**을 업로드하는 새로운 옵션이 표시됩니다.

   기존 사용자를 위한 FCM(/en-us/xenmobile/server/media/fcm-in-use.png)
2. 새로운 FCM 사용자라면 **발신자 ID(Sender ID)**를 입력하고 이전 절차에서 얻은 **서비스 계정 키 파일(Service Account Key File)**을 업로드하십시오.

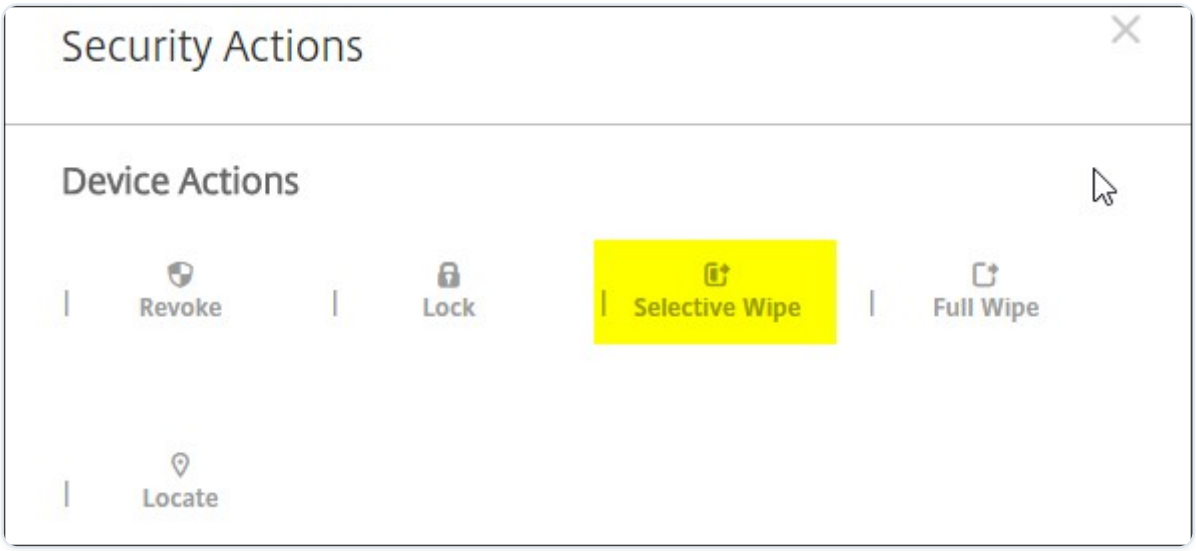
   새로운 FCM 사용자(/en-us/xenmobile/server/media/new-fcm-user.png)
3. 업로드된 파일이 구문 분석되고 해당 필드가 자동으로 생성됩니다.

   구문 분석된 서비스 계정(/en-us/xenmobile/server/media/parsed-service-account.png)
4. 정보를 확인하고 **저장**을 클릭하십시오.

구성 테스트

1. Android 장치를 등록하십시오.
2. 장치를 한동안 유휴 상태로 두어 XenMobile에서 연결이 끊어지도록 하십시오.
3. XenMobile 콘솔에 로그인하고 **관리**를 클릭한 다음 Android 장치를 선택하고 **보안**을 클릭하십시오.

   Android 장치 보안 옵션(/en-us/xenmobile/server/media/manage-devices-secure.png)
4. **장치 작업**에서 **선택적 초기화**를 클릭하십시오.



성공적으로 구성되면 장치에서 선택적 초기화가 발생합니다.

Apple Education 기능과 통합

Apple Education을 사용하는 환경에서 XenMobile®을 모바일 장치 관리(MDM) 솔루션으로 사용할 수 있습니다. XenMobile 지원에는 iPad용 Apple School Manager(ASM) 및 Classroom 앱이 포함됩니다. XenMobile Education 구성 장치 정책은 Apple Education과 함께 사용할 강사 및 학생 장치를 구성합니다.

사전 구성되고 감독되는 iPad를 강사와 학생에게 제공합니다. 이 구성에는 XenMobile의 ASM 등록, 새 암호로 구성된 관리형 Apple ID 계정, 필수 볼륨 구매 앱 및 iBooks가 포함됩니다.

다음은 Apple Education 기능에 대한 XenMobile 지원의 주요 내용입니다.

Apple 스쿨 매니저

ASM은 교육 기관에서 사용되는 iOS(iPadOS) 장치 및 macOS 랩톱을 설정, 배포 및 관리할 수 있는 서비스입니다. ASM에는 IT 관리자가 다음을 수행할 수 있는 웹 기반 포털이 포함되어 있습니다.

- Apple 배포 프로그램 장치를 다른 MDM 서버에 할당합니다.
- 앱 및 iBooks에 대한 볼륨 구매 라이선스를 구매합니다.
- **관리형 Apple ID**를 대량으로 생성합니다. 이러한 맞춤형 Apple ID는 iCloud Drive에 문서를 저장하고 Apple App Store 과정에 등록하는 것과 같은 Apple 서비스에 대한 액세스를 제공합니다.

여러 ASM 계정을 XenMobile에 추가할 수 있습니다. 예를 들어, 이 기능을 사용하면 교육 단위 또는 부서별로 다른 등록 설정 및 설정 지원 옵션을 사용할 수 있습니다. 그런 다음 ASM 계정을 다른 장치 정책과 연결합니다.

XenMobile 콘솔에 ASM 계정을 추가하면 XenMobile이 수업 및 명단 정보를 검색합니다. 장치 설정 중에 XenMobile은 다음을 수행합니다.

- 장치를 등록합니다.
- 장치 정책(교육 구성, 홈 화면 레이아웃 등)과 같이 배포를 위해 구성한 리소스를 설치합니다.
- 또한 볼륨 구매를 통해 구매한 앱과 iBooks를 모두 설치합니다.

그런 다음 사전 구성된 장치를 강사와 학생에게 제공합니다. 장치를 분실하거나 도난당한 경우 MDM 분실 모드 기능을 사용하여 장치를 잠그고 찾을 수 있습니다.

iPad용 교실 앱

iPad용 Classroom 앱을 사용하면 강사가 학생 장치에 연결하고 관리할 수 있습니다. 장치 화면을 보고, iPad에서 앱을 열고, 웹 링크를 공유하고 열 수 있습니다.

Classroom은 App Store에서 무료로 제공됩니다. 앱을 XenMobile 콘솔에 업로드합니다. 그런 다음 교육 구성 장치 정책을 사용하여 Classroom 앱을 구성하고 강사 장치에 배포합니다.

Apple 교육 기능에 대한 자세한 내용은 Apple 교육 사이트 및 동일한 사이트의 Apple 교육 배포 가이드를 참조하십시오.

전제 조건

- 시트릭스 게이트웨이
- MDM+MAM용으로 구성된 등록 프로필.
- Apple iPad 3세대(최소 버전) 또는 iPad Mini(iOS 9.3 최소 버전)

> **참고:**

> XenMobile은 ASM 사용자 계정을 LDAP 또는 Active Directory에 대해 유효성 검사하지 않습니다. 그러나 ASM 강사 또는 학생과 관련 없는 사용자 및 장치 관리를 위해 XenMobile을 LDAP 또는 Active Directory에 연결할 수 있습니다. 예를 들어, Active Directory를 사용하여 IT 관리자 및 관리자와 같은 다른 ASM 구성원에게 Secure Mail 및 Secure Web을 제공할 수 있습니다.

> ASM 강사 및 학생은 로컬 사용자이므로 장치에 Citrix Secure Hub™를 배포할 필요가 없습니다.

> Citrix Gateway 인증을 포함하는 MAM 등록은 로컬 사용자(Active Directory 사용자만 해당)를 지원하지 않습니다. 따라서 XenMobile은 필요한 볼륨 구매 앱과 iBooks만 강사 및 학생 장치에 배포합니다.

애플 스쿨 매니저 및 제노모바일 구성

Apple 또는 Apple 공인 리셀러 또는 통신사로부터 iPad를 구매한 후: 이 섹션의 워크플로에 따라 ASM 계정 및 장치를 설정합니다. 이 워크플로에는 ASM 포털 및 XenMobile 콘솔에서 수행하는 단계가 포함됩니다.

일대일 모델(학생당 iPad 1대) 또는 강사용 iPad(공유되지 않음)에 사용하는 모든 iPad에 대한 통합을 구성하려면 다음 지침을 따르십시오. 공유 iPad를 구성하려면 공유 iPad 구성을 참조하십시오.

1단계: Apple School Manager 계정 생성 및 설정 지원 완료

Apple 배포 프로그램에서 업그레이드할 계획이라면 Apple 지원 문서인 기관을 ASM으로 업그레이드를 참조하십시오. ASM 계정을 생성하려면 `<https://school.apple.com/>`로 이동하여 등록 지침을 따르십시오. ASM에 처음 로그인하면 설정 지원이 열립니다.

- ASM 필수 구성 요소, 설정 지원 및 관리 작업에 대한 자세한 내용은 Apple School Manager 사용 설명서를 참조하십시오.
- ASM을 설정할 때 Active Directory의 도메인 이름과 다른 도메인 이름을 사용하십시오. 예를 들어, ASM의 도메인 이름 앞에 `appleid`와 같은 접두사를 붙이십시오.
- ASM을 명단 데이터에 연결하면 ASM은 교사와 학생을 위한 관리형 Apple ID를 생성합니다. 명단 데이터에는 교사, 학생 및 수업이 포함됩니다. ASM에 명단 데이터를 추가하는 방법에 대한 자세한 내용은 이전에 언급된 ASM 사용 설명서를 참조하십시오.
- 이전에 언급된 ASM 사용 설명서에 설명된 대로 기관의 관리형 Apple ID 형식을 사용자 지정할 수 있습니다.

> **중요:**
>
> ASM 정보를 XenMobile로 가져온 후에는 관리형 Apple ID를 변경하지 마십시오.

- 리셀러 또는 통신사를 통해 장치를 구매한 경우 해당 장치를 ASM에 연결하십시오. 자세한 내용은 이전에 언급된 ASM 사용 설명서를 참조하십시오.

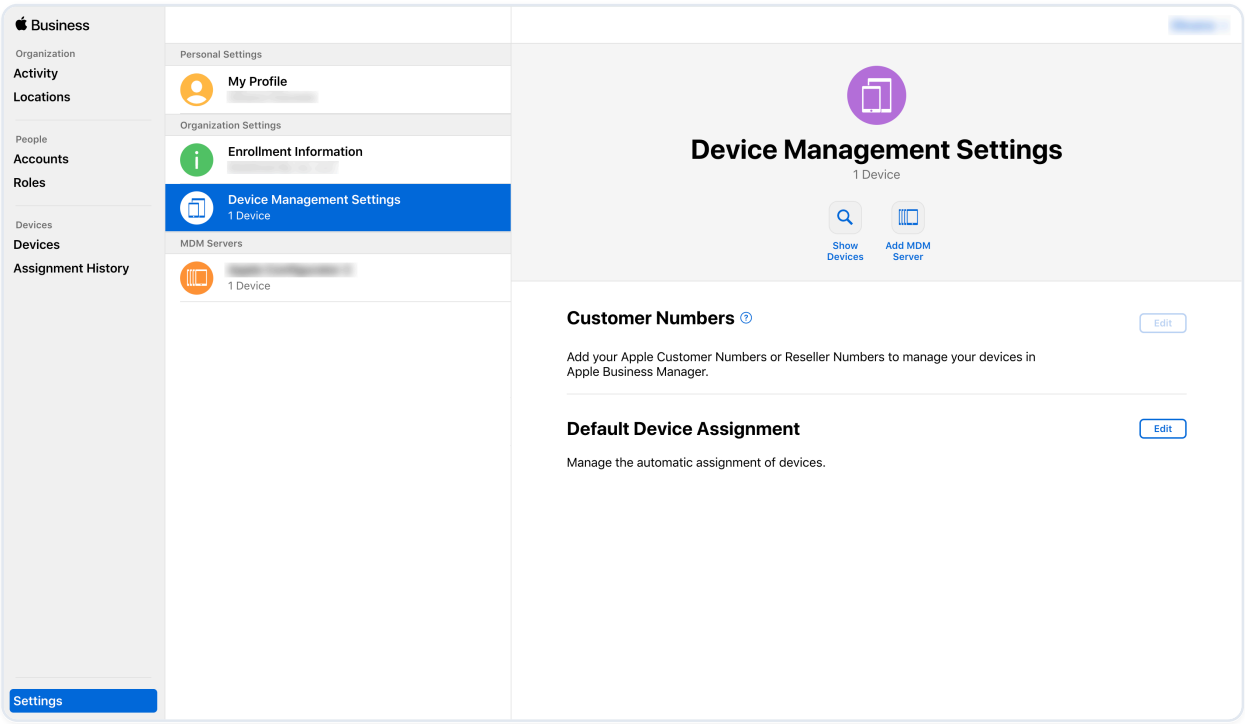
2단계: Apple School Manager의 MDM 서버로 XenMobile 구성 및 장치 할당 구성

ASM 포털에는 **MDM 서버** 탭이 포함되어 있습니다. 이 설정을 완료하려면 XenMobile의 공개 키 파일이 필요합니다.

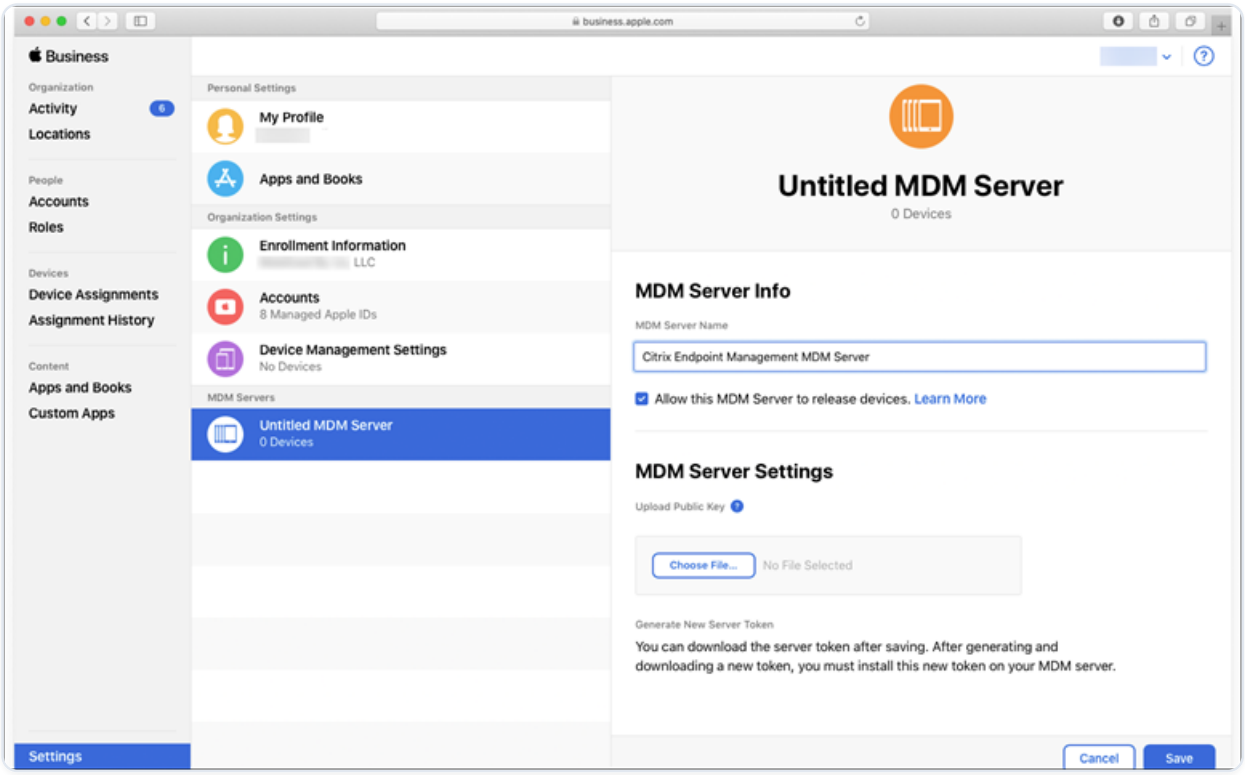
1. XenMobile의 공개 키를 로컬 컴퓨터에 다운로드합니다. XenMobile 콘솔에서 **설정 > Apple 배포 프로그램**으로 이동합니다.



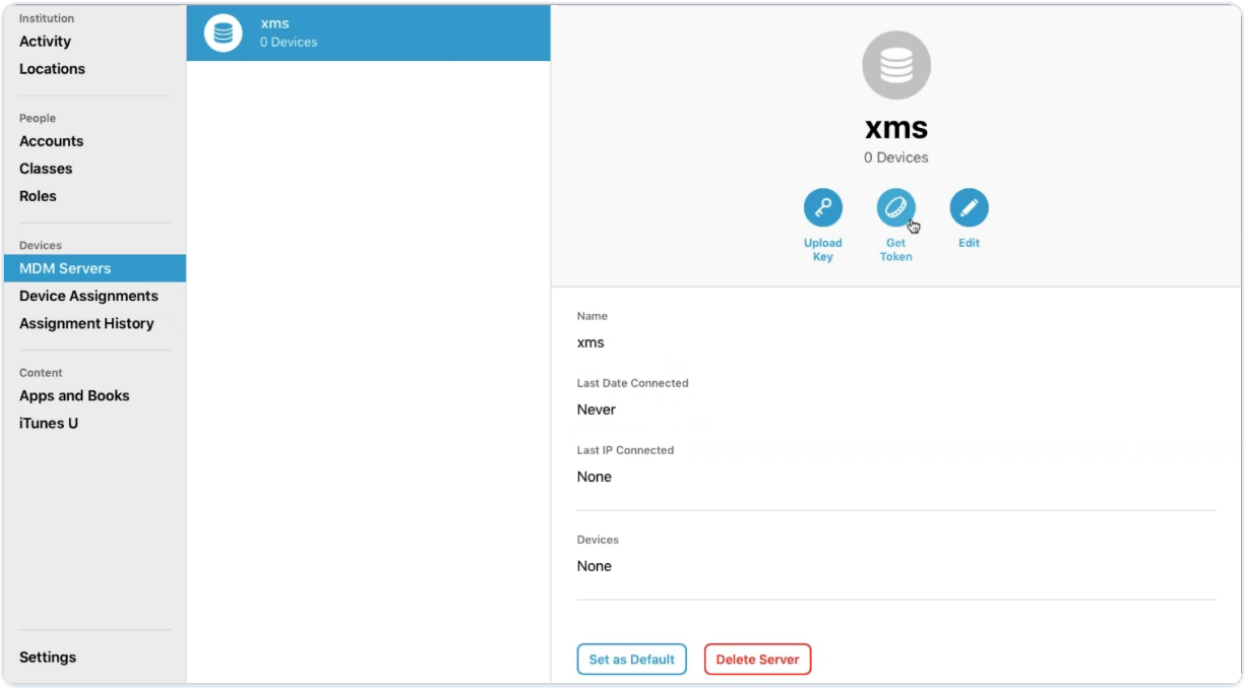
2. **공개 키 다운로드**에서 **다운로드**를 클릭한 다음 PEM 파일을 저장합니다.
3. **Apple School Manager** 포털에서 **설정**을 클릭한 다음 **장치 관리 설정**을 클릭합니다. **MDM 서버 추가**를 클릭합니다.



4. XenMobile의 이름을 입력합니다. 입력하는 서버 이름은 참조용이며 서버 URL 또는 이름이 아닙니다. **공개 키 업로드**에서 **파일 선택**을 클릭합니다.



5. XenMobile에서 다운로드한 공개 키를 업로드한 다음 **저장**을 클릭합니다.
6. 서버 토큰 생성: **토큰 다운로드**를 클릭하여 서버 토큰 파일을 컴퓨터에 다운로드합니다.



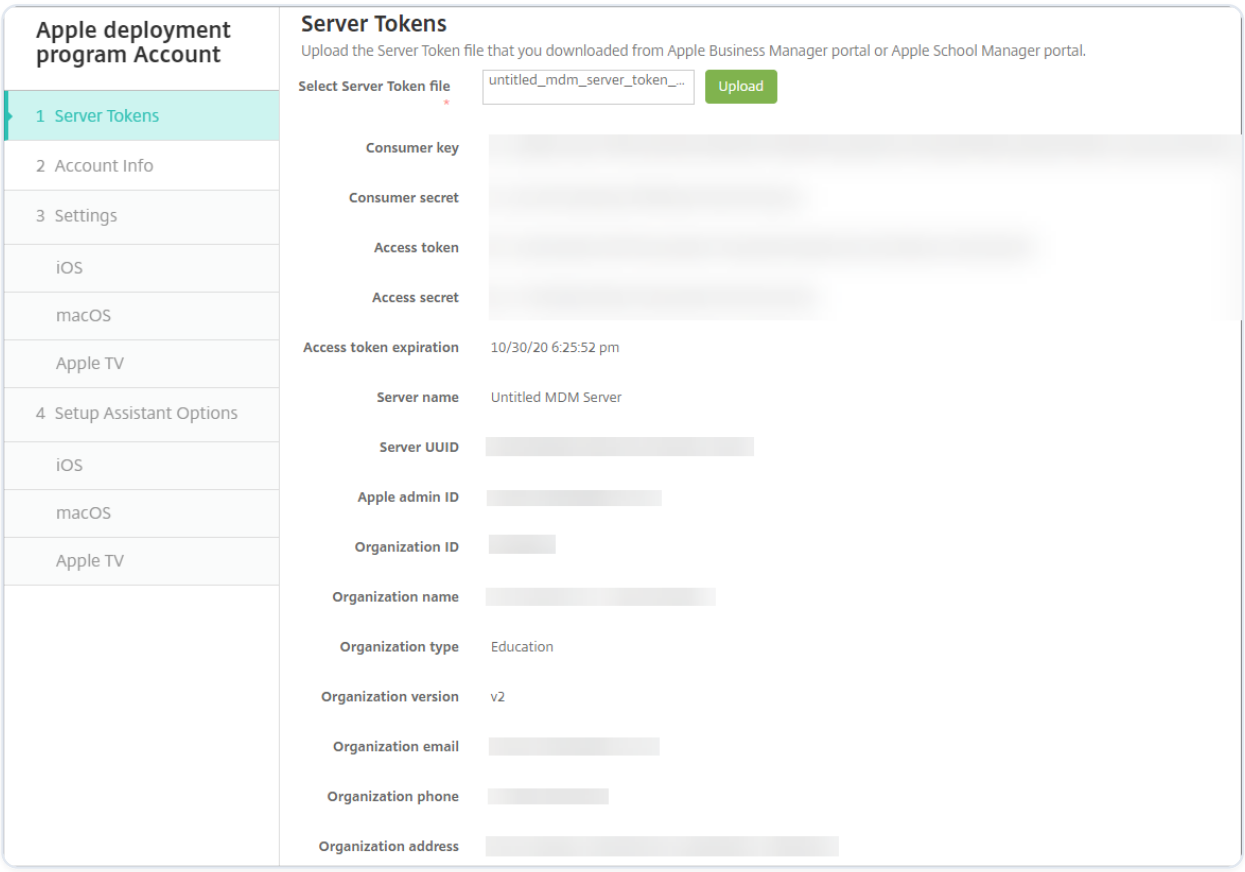
7. **기본 장치 할당**에서 **변경**을 클릭합니다. 장치를 할당할 방법을 선택한 다음 요청된 정보를 제공합니다. 자세한 내용은 ASM 사용자 가이드를 참조하십시오.

3단계: Apple School Manager 계정을 XenMobile에 추가

1. XenMobile 콘솔에서 **설정 > Apple 배포 프로그램**으로 이동한 다음 **Apple 배포 프로그램 계정 추가**에서 **추가**를 클릭합니다.



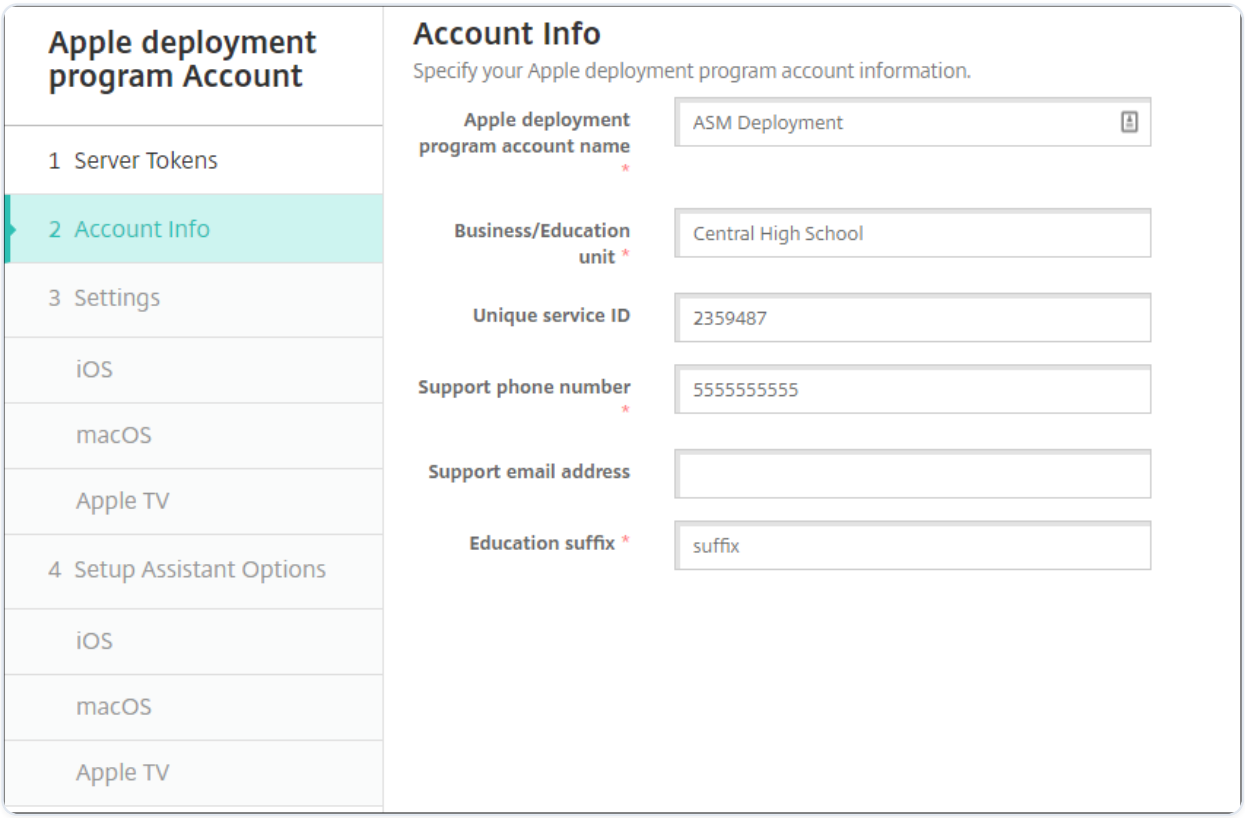
2. **서버 토큰** 페이지에서 **업로드**를 클릭하고 ASM 포털에서 다운로드한 서버 토큰(P7M 파일) 파일을 선택합니다. 토큰 정보가 나타납니다.



참고:

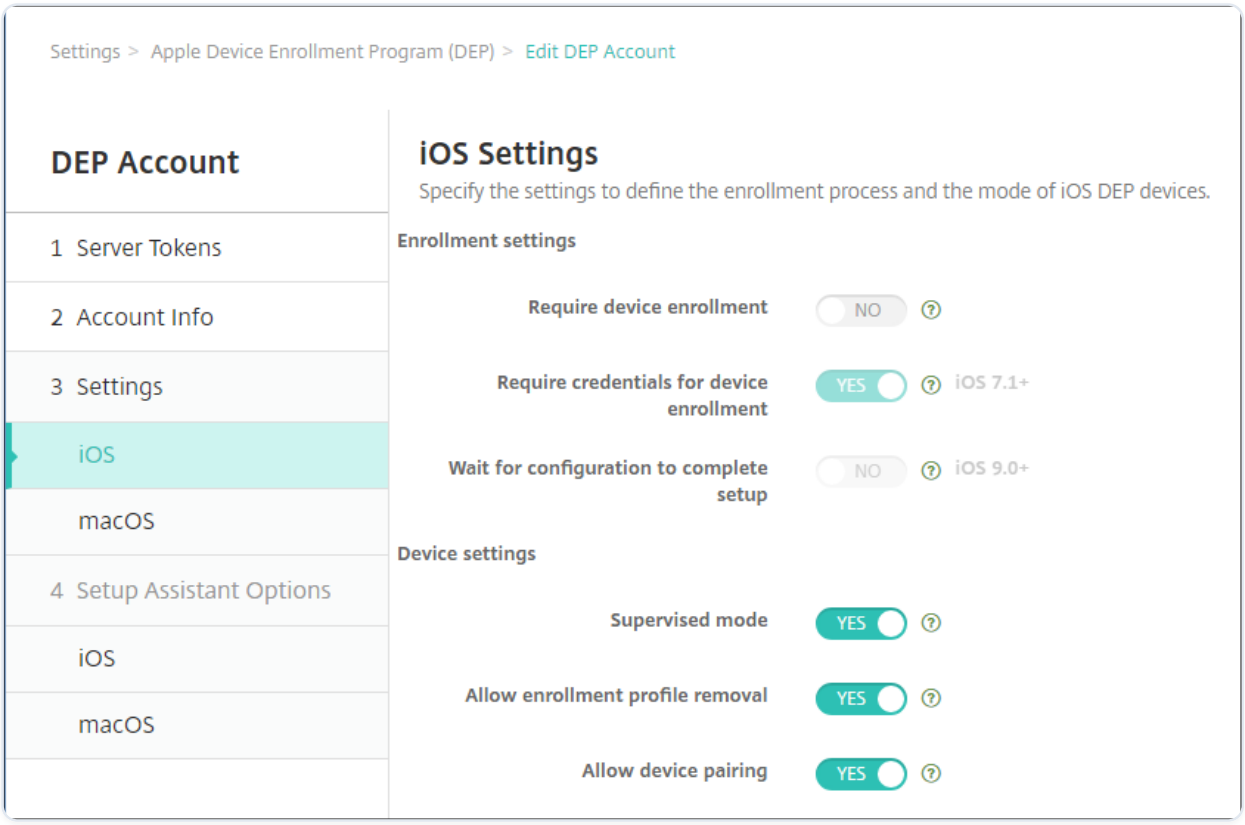
- **조직 ID**는 Apple 배포 프로그램의 고객 ID입니다.
- ASM 계정은 **조직 유형**이 **교육**이며 **조직 버전**은 **v2**입니다.

3. **계정 정보** 페이지에서 다음 설정을 지정합니다.



- **Apple 배포 프로그램 계정 이름:** 이 Apple 배포 프로그램 계정의 고유한 이름입니다. 국가 또는 조직 계층 구조와 같이 Apple 배포 프로그램 계정을 구성하는 방식을 반영하는 이름을 사용하십시오.
- **비즈니스/교육 단위:** 장치 할당을 위한 교육 단위 또는 부서입니다. 이 필드는 필수입니다.
- **고유 서비스 ID:** 계정을 추가로 식별하는 데 도움이 되는 선택적 고유 ID입니다.
- **지원 전화 번호:** 사용자가 설정 중에 도움을 요청할 수 있는 지원 전화 번호입니다. 이 필드는 필수입니다.
- **지원 이메일 주소:** 최종 사용자가 사용할 수 있는 선택적 지원 이메일 주소입니다.
- **교육 접미사:** 지정된 ASM 배포 프로그램 계정의 클래스를 표시합니다. (볼륨 구매 접미사는 지정된 볼륨 구매 계정의 앱 및 iBook을 표시합니다.) ASM 배포 프로그램 및 ASM 볼륨 구매 계정 모두에 동일한 접미사를 사용하는 것이 좋습니다.

4. **다음**을 클릭합니다. **iOS 설정**에서 다음 설정을 지정합니다.



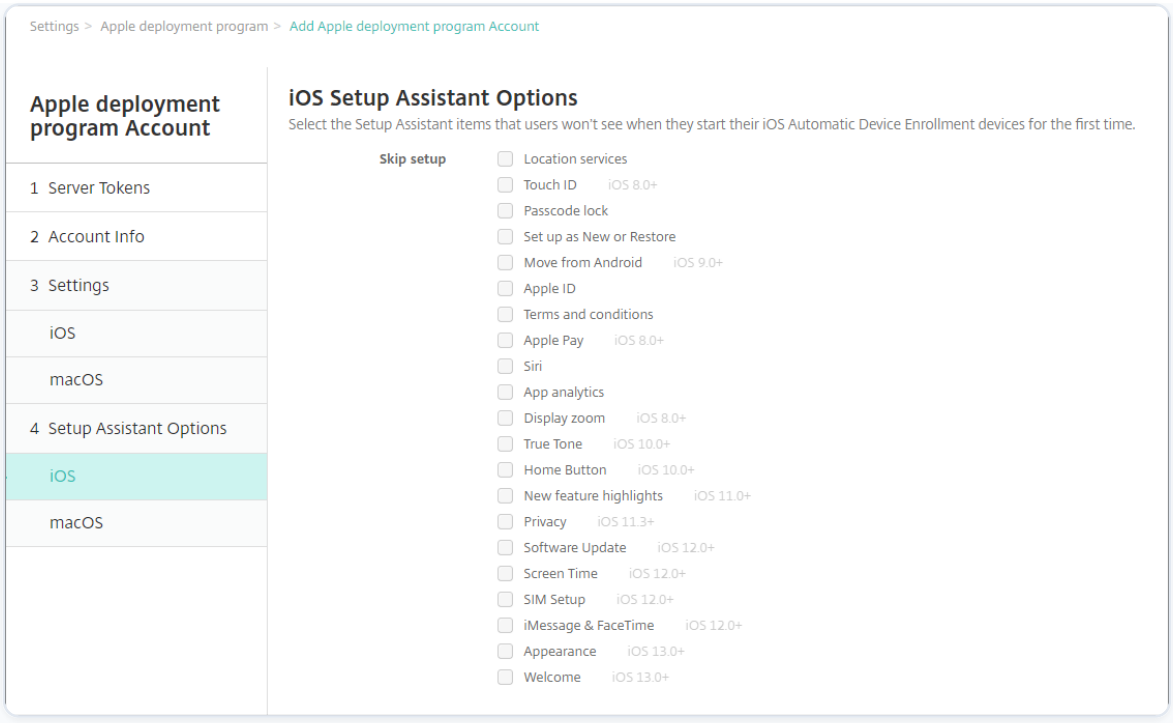
- **등록 설정**
  - **장치 등록 필요:** 사용자가 장치를 등록하도록 요구합니다. 이 설정을 **아니요**로 변경합니다.
  - **장치 등록을 위한 자격 증명 필요:** 사용자가 Apple 배포 프로그램 설정 중에 자격 증명을 입력하도록 요구합니다. XenMobile과 ASM 통합의 경우 이 설정은 기본적으로 **예**이며 변경할 수 없습니다. Apple 배포 프로그램은 장치 등록을 위해 자격 증명을 요구합니다.
  - **설정 완료를 위한 구성 대기:** 모든 MDM 리소스가 장치에 배포될 때까지 사용자 장치가 설정 지원 모드를 유지하도록 요구할지 여부입니다. XenMobile과 ASM 통합의 경우 이 설정은 기본적으로 **아니요**입니다. Apple 설명서에 따르면 장치가 설정 지원 모드에 있는 동안 다음 명령이 작동하지 않을 수 있습니다.
    - InviteToProgram
    - 애플리케이션 설치
    - 미디어 설치
    - 교환 코드 적용
- **장치 설정**
  - **감독 모드:** iOS 장치를 감독 모드에 배치합니다. 기본값인 **예**를 변경하지 마십시오. iOS 장치를 감독 모드에 배치하는 방법에 대한 자세한 내용은 Apple Configurator를 사용하여 iOS 장치를 감독 모드에 배치하는 방법을 참조하십시오.

- **공유 모드:** iPad에서 공유 모드를 활성화합니다. 최소 요구 사항을 충족하지 않는 장치는 공유할 수 없습니다.
- **등록 프로필 제거 허용:** ASM 통합의 경우 사용자가 장치에서 등록 프로필을 제거하도록 허용합니다. 이 설정을 **예**로 변경합니다.
- **장치 페어링 허용:** ASM 통합의 경우 Apple App Store 및 Apple Configurator를 통해 장치를 관리할 수 있도록 장치 페어링을 허용합니다. 이 설정을 **예**로 변경합니다.

5. **iOS 설정 지원 옵션**에서 사용자가 장치를 처음 시작할 때 건너뛸 iOS 설정 지원 단계를 선택합니다. 기본적으로 설정 지원에는 모든 단계가 포함됩니다. 설정 지원에서 단계를 제거하면 사용자 경험이 단순화된다는 점을 고려하십시오.

중요:

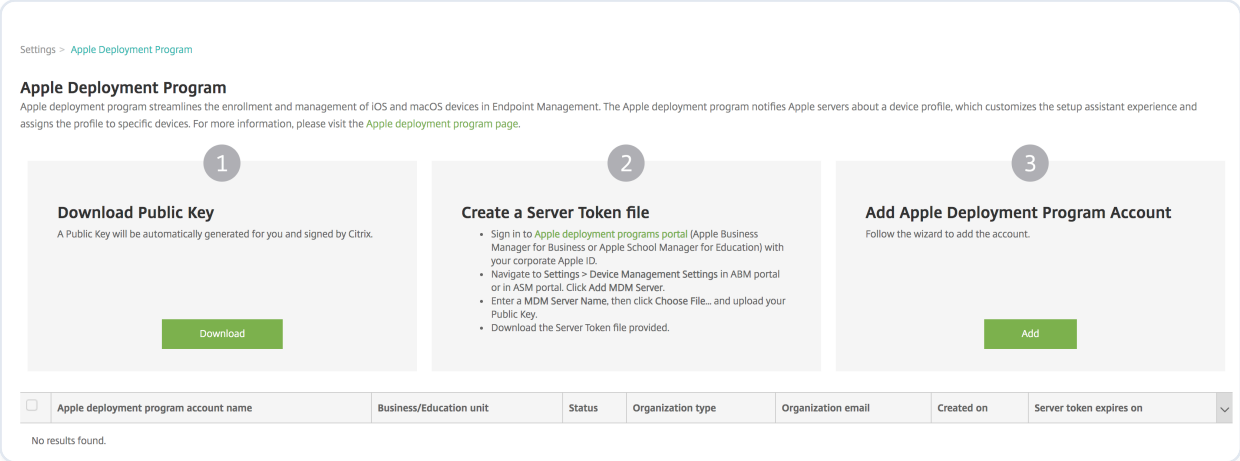
Citrix는 **Apple ID** 및 **이용 약관** 단계를 포함할 것을 강력히 권장합니다. 이러한 단계를 통해 강사와 학생은 새로운 관리형 Apple ID 암호를 제공하고 필수 이용 약관에 동의할 수 있습니다.



- **위치 서비스:** 장치에서 위치 서비스를 설정합니다.
- **Touch ID:** iOS 장치에서 Touch ID를 설정합니다.
- **암호 잠금:** 장치에 대한 암호를 생성합니다.
- **새로 설정 또는 복원:** 기기를 새로 설정하거나 iCloud 또는 Apple App Store 백업에서 설정합니다.

- **Android에서 이동:** Android 기기에서 iOS 기기로 데이터를 전송할 수 있도록 설정합니다. 이 옵션은 **새로 설정 또는 복원**이 선택된 경우에만 사용할 수 있습니다(즉, 이 단계는 건너뜁니다).
- **Apple ID:** 기기에 대한 Apple ID 계정을 설정합니다. Citrix는 이 단계를 포함하도록 확인란을 선택하는 것을 권장합니다.
- **이용 약관:** 사용자가 기기 사용에 대한 이용 약관에 동의하도록 요구합니다. Citrix는 이 단계를 포함하도록 확인란을 선택하는 것을 권장합니다.
- **Apple Pay:** iOS 기기에서 Apple Pay를 설정합니다.
- **Siri:** 기기에서 Siri를 사용하거나 사용하지 않도록 설정합니다.
- **앱 분석:** 충돌 데이터 및 사용 통계를 Apple과 공유할지 여부를 설정합니다.
- **디스플레이 확대/축소:** iOS 기기에서 디스플레이 해상도(표준 또는 확대/축소)를 설정합니다.
- **True Tone:** iOS 기기에서 True Tone 디스플레이를 설정합니다.
- **홈 버튼:** 홈 버튼 화면 감도를 설정합니다.
- **새로운 기능 하이라이트:** iOS 11.0 기기(최소 버전)에서 온보딩 정보 화면, 어디서든 Dock에 접근, 최근 앱 간 전환을 설정합니다.
- **개인 정보 보호:** Apple 배포 프로그램 기기 설정 중에 사용자가 데이터 및 개인 정보 보호 창을 보지 못하도록 합니다. iOS 11.3 이상에 해당합니다.
- **소프트웨어 업데이트:** Apple 배포 프로그램 기기 설정 중에 사용자가 필수 소프트웨어 업데이트 화면을 보지 못하도록 합니다. iOS 12.0 이상에 해당합니다.
- **스크린 타임:** Apple 배포 프로그램 기기 설정 중에 사용자가 스크린 타임 화면을 보지 못하도록 합니다. iOS 12.0 이상에 해당합니다.
- **SIM 설정:** Apple 배포 프로그램 기기 설정 중에 사용자가 셀룰러 요금제 추가 화면을 보지 못하도록 합니다. iOS 12.0 이상에 해당합니다.
- **iMessage & FaceTime:** Apple Deployment Program 장치 설정 중 사용자가 iMessage 및 FaceTime 화면을 보지 못하도록 합니다. iOS 12.0 이상에 해당합니다.

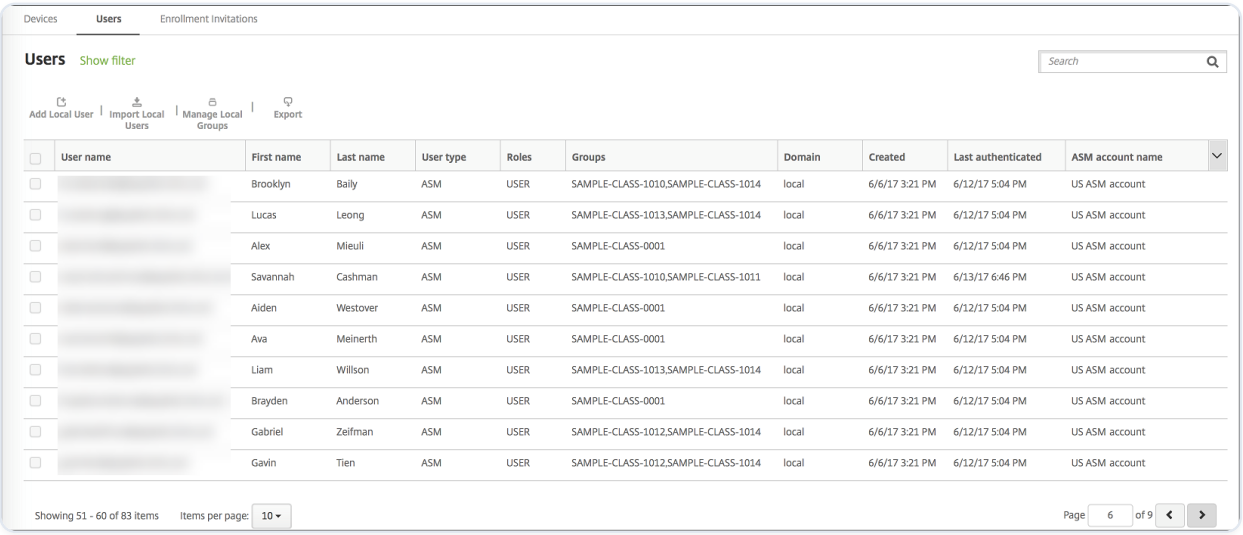
6. 해당 계정은 **설정 > Apple Deployment Program**에 나타납니다. XenMobile과 ASM 계정 간의 연결을 테스트하려면 해당 계정을 선택하고 **연결 테스트**를 클릭합니다.



상태 메시지가 나타납니다.



몇 분 후 ASM의 사용자 계정이 **관리 > 사용자** 페이지에 나타납니다. XenMobile은 각 사용자에 대해 가져온 Managed Apple ID를 기반으로 로컬 사용자 계정을 생성합니다. 다음 예에서 사용자 계정의 사용자 지정 Apple ID 도메인 이름 접두사는 `appleid`입니다.

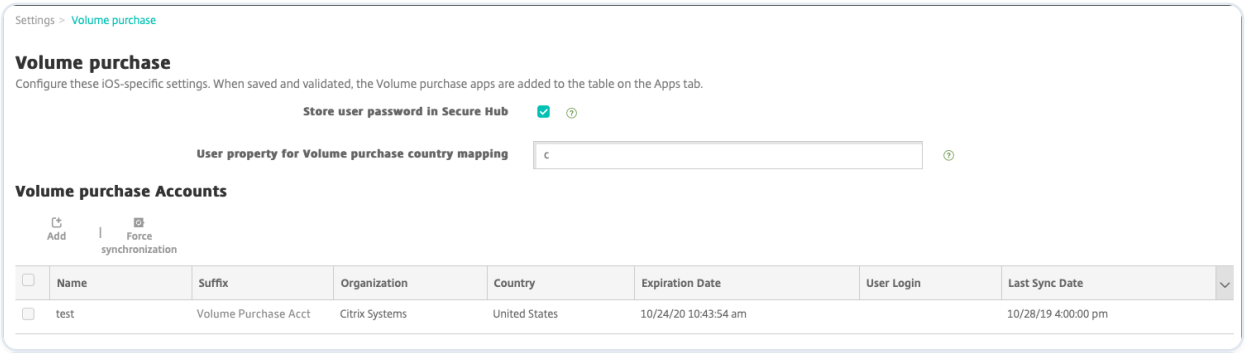


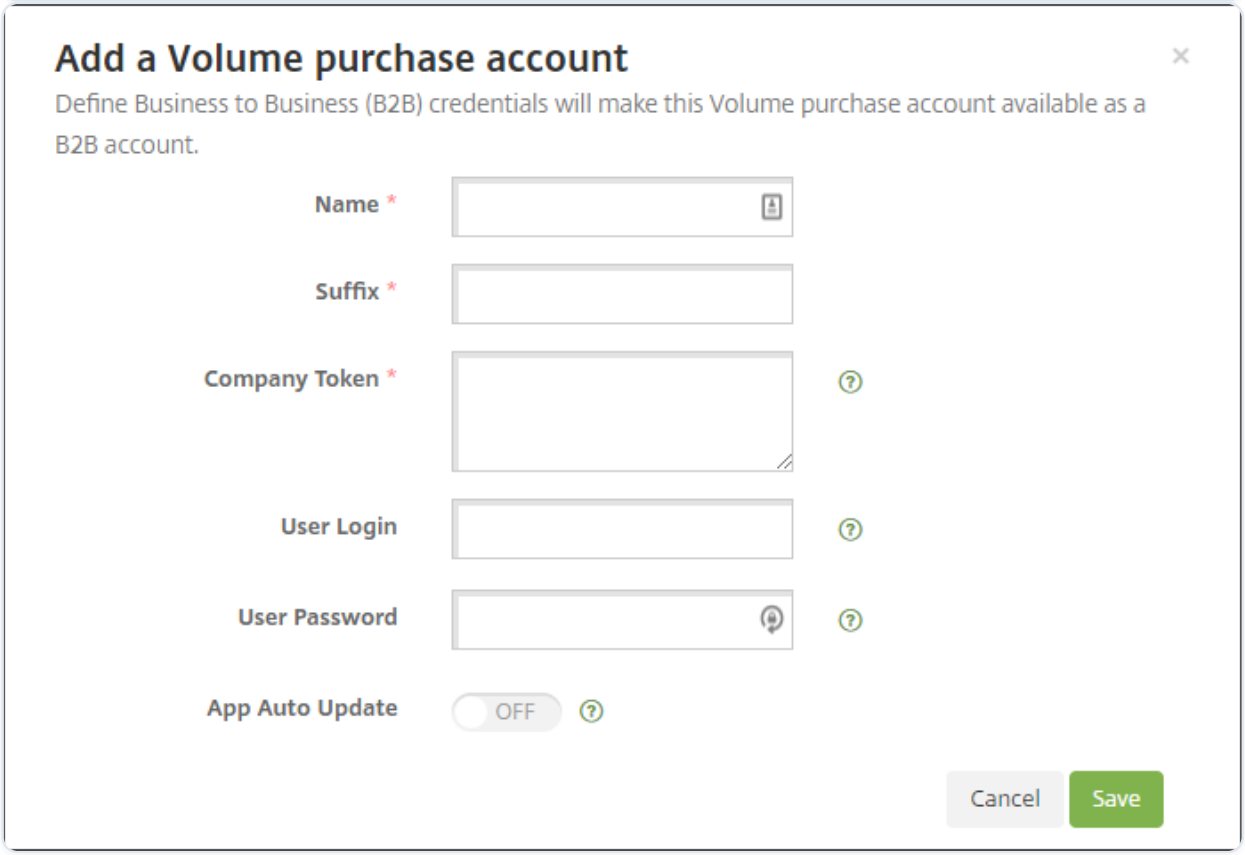
특정 ASM 계정의 모든 사용자를 찾으려면 사용자 검색 필드에 계정 이름을 입력합니다.

4단계: Apple School Manager용 교육 볼륨 구매 계정 구성

이 섹션에서는 앱 및 iBooks용 볼륨 구매 라이선스를 구매하는 데 사용하는 볼륨 구매 계정을 XenMobile에 지정합니다.

1. ASM용 교육 볼륨 구매 계정을 구성하려면 Apple 볼륨 구매의 지침을 따르십시오. 볼륨 구매 계정 추가 화면에서는 회사 토큰을 제공해야 합니다. 교육 볼륨 구매 계정에서 직접 토큰을 다운로드하여 **볼륨 구매 계정 추가** 화면에 붙여넣으십시오.





2. 볼륨 구매 라이선스가 XenMobile로 가져와질 때까지 몇 분 정도 기다리십시오.

5단계: Apple School Manager 사용자 암호 추가

ASM 계정을 추가하면 XenMobile은 ASM에서 클래스 및 사용자를 가져옵니다. XenMobile은 클래스를 로컬 그룹으로 처리하고 콘솔에서 "그룹"이라는 용어를 사용합니다. 클래스에 ASM에 그룹 이름이 있는 경우 XenMobile은 해당 그룹 이름을 클래스에 할당합니다. 그렇지 않으면 XenMobile은 그룹 이름에 소스 시스템 ID를 사용합니다. XenMobile은 ASM의 과정 이름이 고유하지 않으므로 과정 이름을 클래스 이름으로 사용하지 않습니다.

XenMobile은 관리형 Apple ID를 사용하여 사용자 유형이 **ASM**인 로컬 사용자를 생성합니다. ASM은 모든 외부 데이터 소스와 독립적으로 자격 증명을 생성하므로 사용자는 로컬입니다. 결과적으로 XenMobile은 디렉터리 서버를 사용하여 이러한 새 사용자를 인증하지 않습니다.

ASM은 임시 사용자 암호를 XenMobile로 보내지 않습니다. CSV 파일에서 가져오거나 수동으로 추가할 수 있습니다. 임시 사용자 암호를 가져오려면 다음을 수행합니다.

1. 관리형 Apple ID 임시 암호를 생성할 때 ASM에서 생성한 CSV 파일을 가져옵니다.
2. CSV 파일을 편집하여 임시 암호를 사용자가 XenMobile에 등록하기 위해 제공하는 새 암호로 바꿉니다. 이 목적을 위한 암호 유형에는 제약이 없습니다.

   CSV 파일의 항목 형식은 다음과 같습니다.
   `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!` !

   여기서:

   사용자: `user@appleid.citrix.com`

   이름: `Firstname`

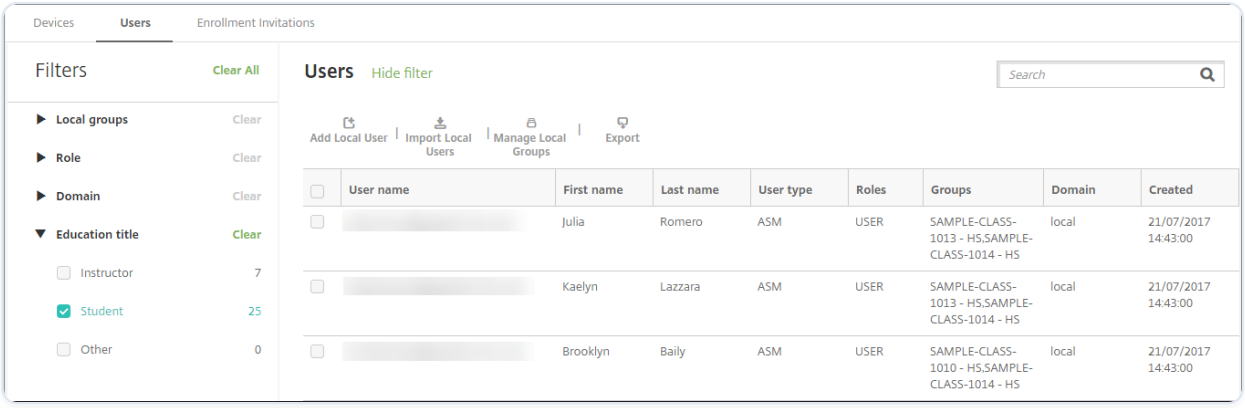
   중간 이름: `Middle`

   성: `Lastname`

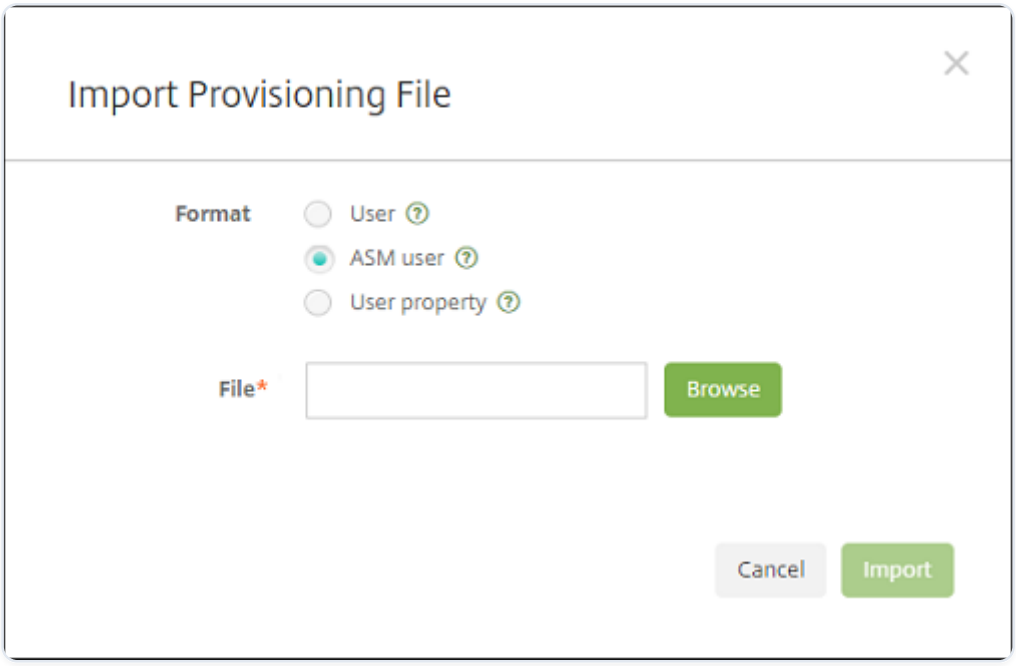
   암호: `Password123!` !
3. XenMobile 콘솔에서 **관리 > 사용자**를 클릭합니다. **사용자** 페이지가 나타납니다.

   다음 **관리 > 사용자** 화면 샘플은 ASM에서 가져온 사용자 목록을 보여줍니다. **사용자** 목록에서:

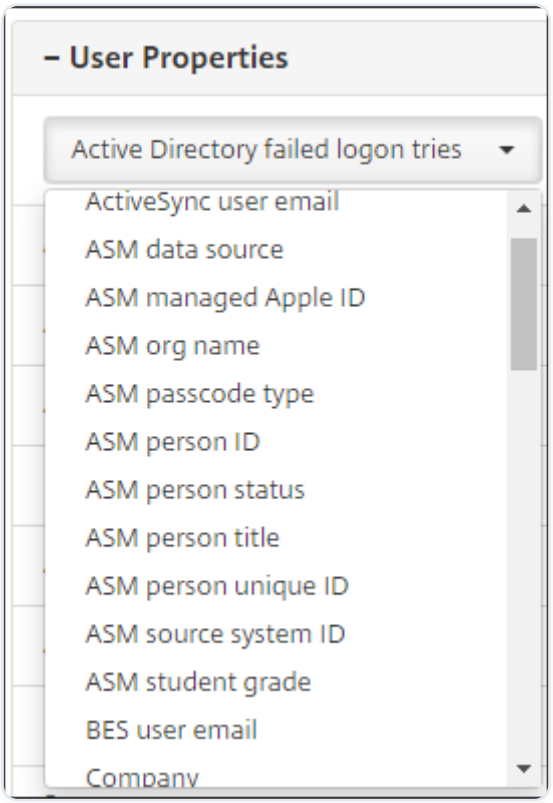
   - **사용자 이름**은 관리형 Apple ID를 보여줍니다.
   - 사용자 유형은 **ASM**이며, 이는 계정이 ASM에서 시작되었음을 나타냅니다.
   - **그룹**은 클래스를 보여줍니다.



4. **로컬 사용자 가져오기**를 클릭합니다. **프로비저닝 파일 가져오기** 대화 상자가 나타납니다.
5. 형식에서 **ASM 사용자**를 선택하고, 2단계에서 준비한 CSV 파일로 이동한 다음 **가져오기**를 클릭합니다
.



6. 로컬 사용자의 속성을 보려면 해당 사용자를 선택한 다음 **편집**을 클릭합니다.



이름 속성 외에도 다음 ASM 속성을 사용할 수 있습니다.

- **ASM 데이터 원본: CSV** 또는 **SFTP**와 같은 클래스의 데이터 원본입니다.

- **ASM 관리형 Apple ID:** 관리형 Apple ID에는 기관 이름과 `appleid`이(가) 포함될 수 있습니다. 예를 들어, ID는 `johnappleseed@appleid.myschool.edu`와(과) 유사할 수 있습니다. XenMobile은 인증을 위해 관리형 Apple ID를 필요로 합니다.
- **ASM 조직 이름:** XenMobile에서 계정에 부여한 이름입니다.
- **ASM 암호 유형:** 사용자의 암호 정책: **복잡함** (8자 이상의 숫자와 문자로 구성된 비학생 암호), **4자리** (숫자), 또는 **6자리** (숫자).
- **ASM 개인 고유 ID:** 사용자의 식별자입니다.
- **ASM 개인 상태:** 관리형 Apple ID가 **활성**인지 **비활성**인지 지정합니다. 이 상태는 사용자가 관리형 Apple ID 계정에 대한 새 암호를 제공한 후에 활성화됩니다.
- **ASM 사용자 직함:** 강사, 학생 또는 기타.
- **ASM 사용자 고유 ID:** 사용자의 고유 식별자입니다.
- **ASM 소스 시스템 ID:** 시스템 소스에 대한 식별자입니다.
- **ASM 학생 학년:** 학생 학년 정보(강사는 사용하지 않음).

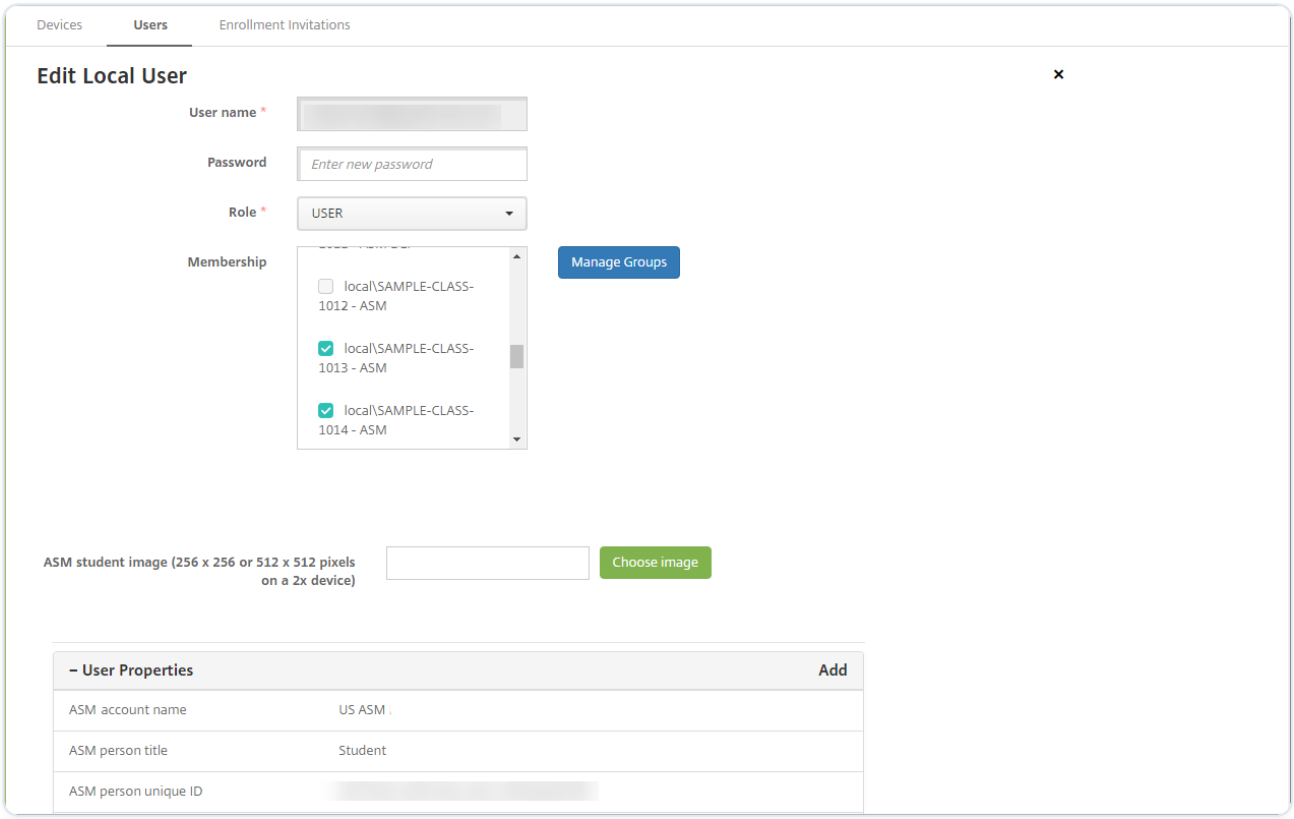
6단계: 선택적으로 학생 사진 추가

각 학생의 사진을 추가할 수 있습니다. 강사가 Apple Classroom 앱을 사용하는 경우 사진이 이 앱에 표시됩니다.

사진 권장 사항:

- 해상도: 256 x 256픽셀(2배 장치에서는 512 x 512픽셀)
- 형식: JPEG, PNG 또는 TIFF

사진을 추가하려면 **관리 > 사용자**로 이동하여 사용자를 선택하고 **편집**을 클릭한 다음 **이미지 선택**을 클릭합니다.



7단계: XenMobile에 리소스 및 전송 그룹 계획 및 추가

전송 그룹은 사용자 범주에 배포할 리소스를 지정합니다. 예를 들어, 강사와 학생을 위한 하나의 전송 그룹을 만들 수 있습니다. 또는 여러 전송 그룹을 만들어 다양한 강사 또는 학생에게 전송되는 앱, 미디어 및 정책을 사용자 지정할 수 있습니다. 수업당 하나 이상의 전송 그룹을 만들 수 있습니다. 관리자(교육 기관의 다른 직원)를 위한 하나 이상의 전송 그룹을 만들 수도 있습니다.

사용자 장치에 배포하는 리소스에는 장치 정책, 볼륨 구매 앱 및 iBooks가 포함됩니다.

- 장치 정책:

  강사가 Classroom 앱을 사용하는 경우, 교육 구성 장치 정책이 필요합니다. 강사 및 학생 iPad를 구성하고 제한하는 방법을 결정하려면 다른 장치 정책을 검토해야 합니다.

- 볼륨 구매 앱:

  XenMobile은 교육 사용자를 위한 필수 앱으로 볼륨 구매 앱을 배포하도록 요구합니다. XenMobile은 이러한 볼륨 구매 앱을 선택 사항으로 배포하는 것을 지원하지 않습니다.

  Apple Classroom 앱을 사용하는 경우, 강사 장치에만 배포하십시오.

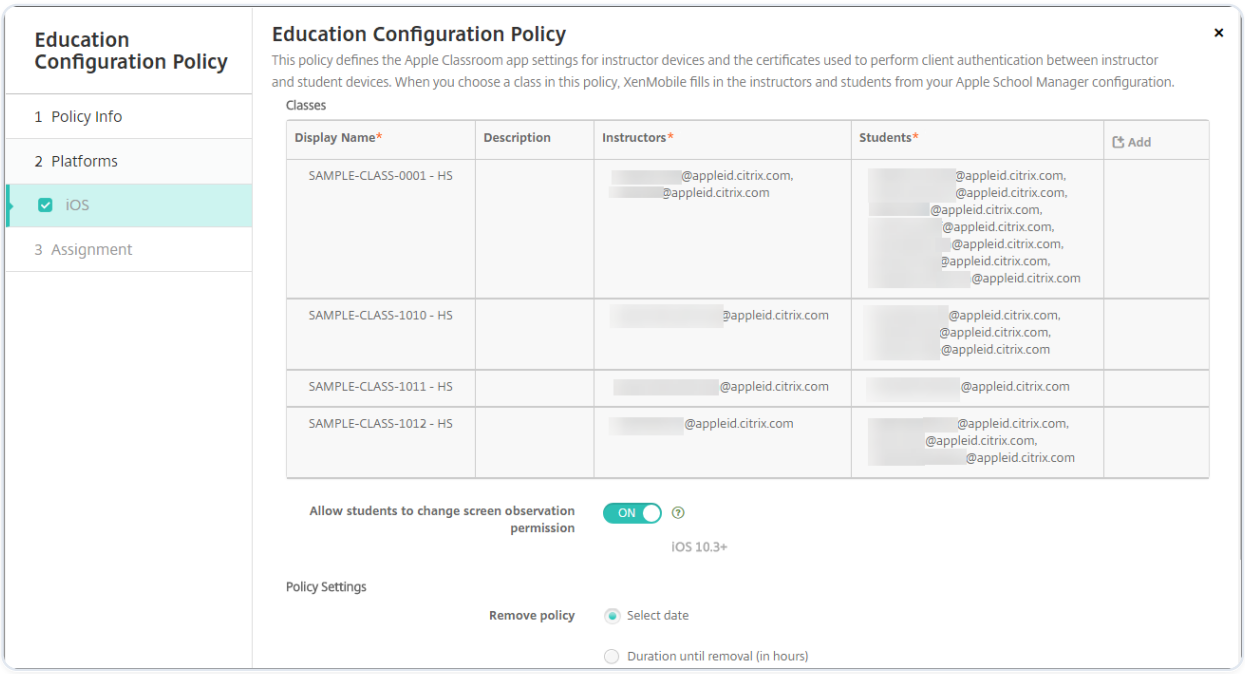
  강사 또는 학생에게 제공하려는 다른 앱을 배포하십시오. 이 솔루션은 Citrix Secure Hub 앱을 사용하지 않으므로 강사 또는 학생에게 배포할 필요가 없습니다.

- 볼륨 구매 iBooks:

XenMobile이 ASM 계정에 연결되면 구매한 iBooks가 XenMobile 콘솔의 **구성 > 미디어**에 나타납니다. 해당 페이지에 나열된 iBooks는 배달 그룹에 추가할 수 있습니다. XenMobile은 iBooks를 필수 미디어로만 추가하는 것을 지원합니다.

강사 및 학생을 위한 리소스와 배달 그룹을 계획한 후 XenMobile 콘솔에서 해당 항목을 생성할 수 있습니다.

1. 강사 또는 학생 장치에 배포하려는 장치 정책을 생성하십시오. 교육 구성 장치 정책에 대한 자세한 내용은 교육 구성 장치 정책을 참조하십시오.

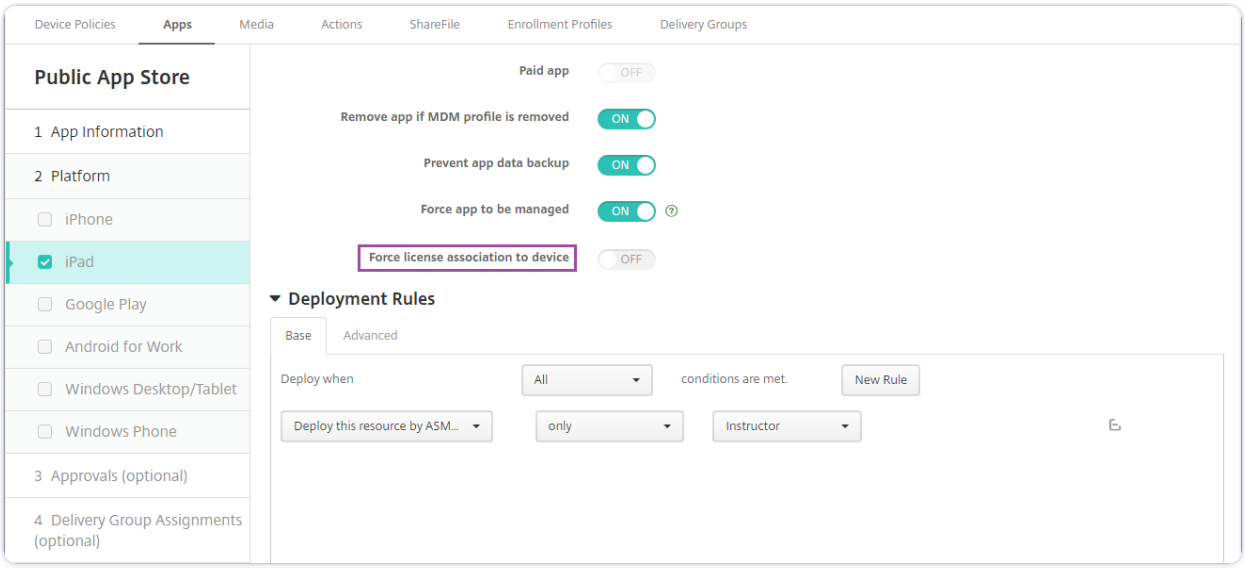


장치 정책에 대한 자세한 내용은 장치 정책 및 개별 정책 문서를 참조하십시오.

2. 앱 (**구성 > 앱**) 및 iBooks (**구성 > 미디어**) 구성:

   - 기본적으로 XenMobile은 사용자 수준에서 앱과 iBooks를 할당합니다. 첫 배포 시 강사와 학생은 ASM에 등록하라는 메시지를 받습니다. 초대를 수락한 후 사용자는 다음 배포(6시간 이내) 시 ASM 앱과 iBooks를 받습니다. Citrix는 새로운 ASM 사용자에게 앱과 iBooks 배포를 강제할 것을 권장합니다. 그렇게 하려면 배달 그룹을 선택하고 **배포**를 클릭하십시오.

     앱(iBooks 제외)을 장치 수준에서 할당하도록 선택할 수 있습니다. 그렇게 하려면 **장치에 라이선스 연결 강제** 설정을 **켜기**로 변경하십시오. 앱을 장치 수준에서 할당하면 사용자는 Apple 볼륨 구매에 참여하라는 초대를 받지 않습니다.

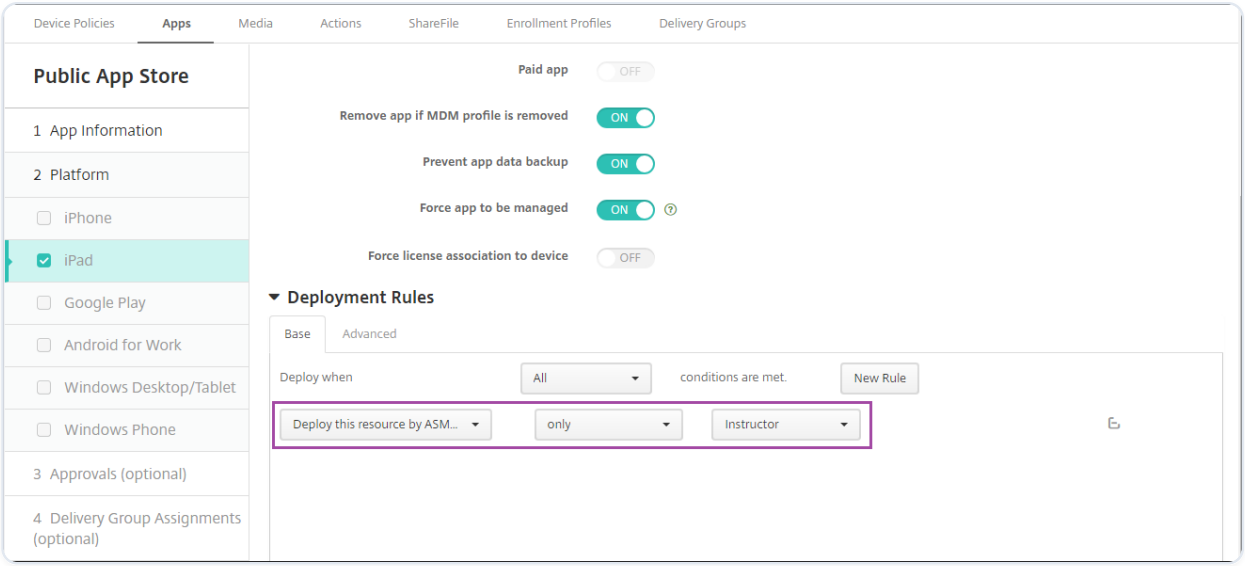


- 강사에게만 앱을 배포하려면 강사만 포함된 배달 그룹을 선택하거나 다음 배포 규칙을 사용하십시오.

```
Deploy this resource by ASM device type

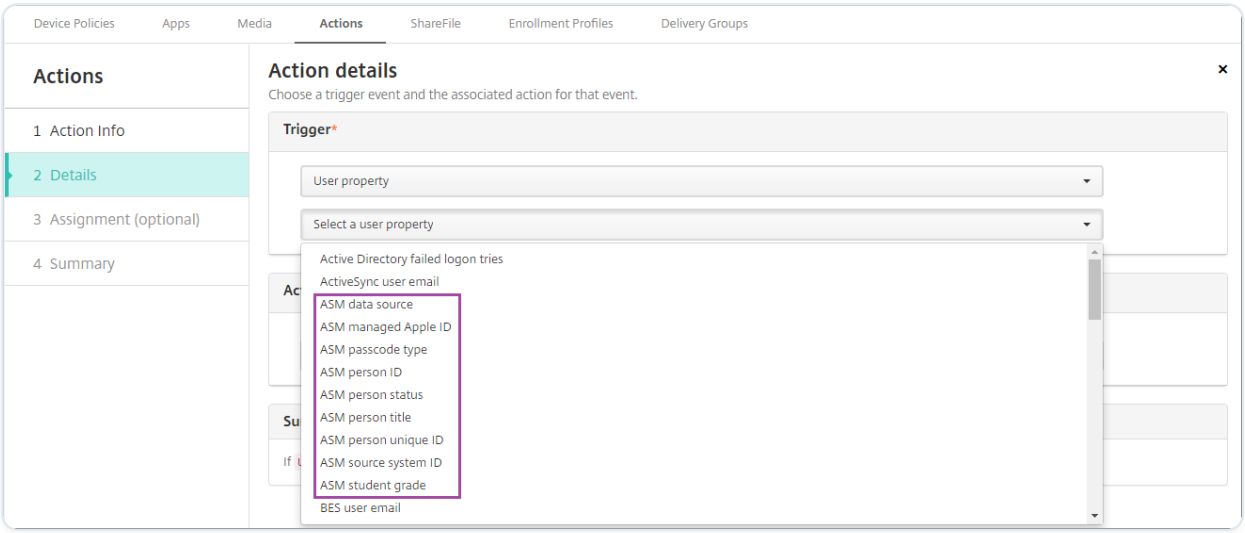
only

Instructor
```



- 볼륨 구매 앱 추가에 대한 도움말은 공개 앱 스토어 앱 추가를 참조하십시오.

3. 선택 사항입니다. ASM 사용자 속성을 기반으로 작업을 생성합니다. 예를 들어, 새 앱이 설치될 때 학생 장치에 알림을 보내는 작업을 생성할 수 있습니다. 또는 다음 예와 같이 사용자 속성이 트리거하는 작업을 생성할 수 있습니다.



작업을 생성하려면 **구성 > 작업**으로 이동하십시오. 작업 구성에 대한 자세한 내용은 자동화된 작업을 참조하십시오.

4. **구성 > 배달 그룹**에서 강사용 및 학생용 배달 그룹을 생성합니다. ASM에서 가져온 클래스를 선택합니다. 또한 강사 및 학생을 위한 배포 규칙을 생성합니다.

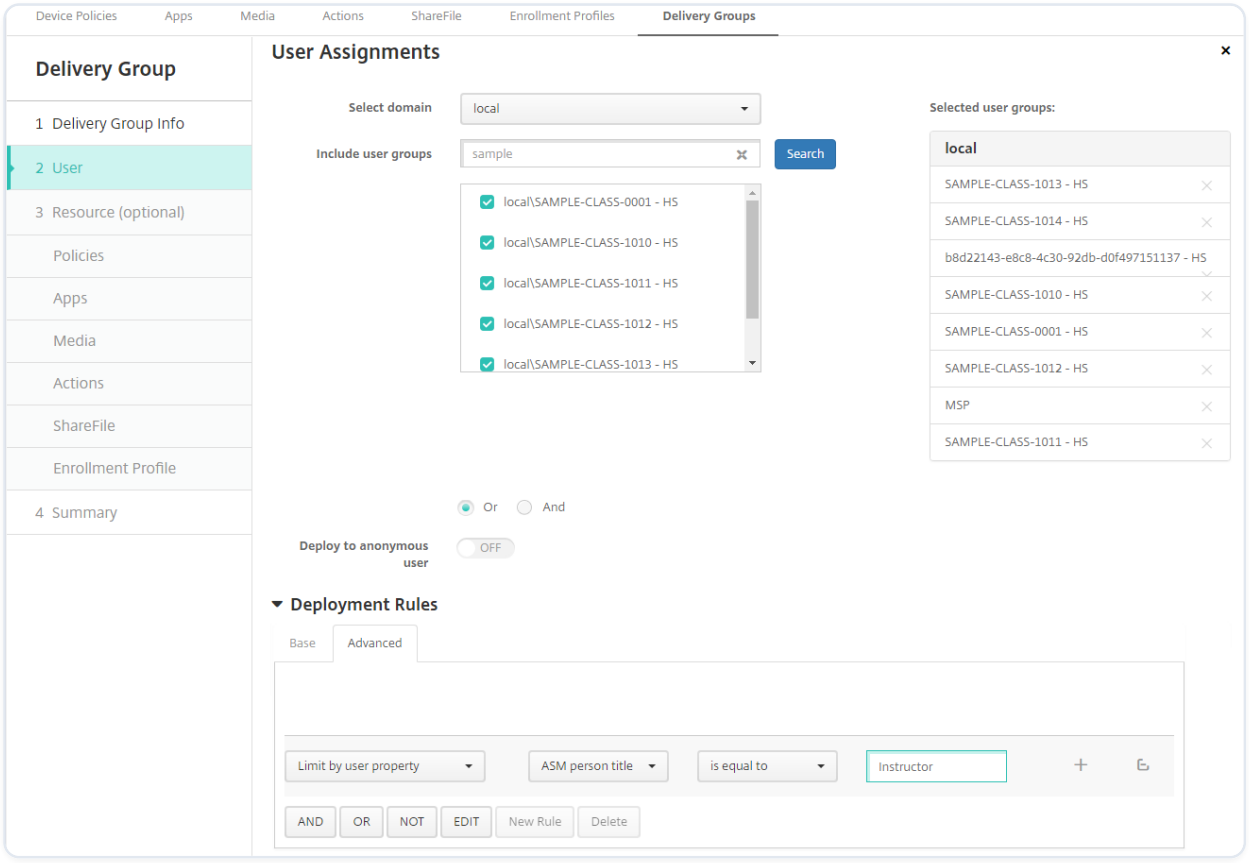
   예를 들어, 다음 사용자 할당은 강사용입니다. 배포 규칙은 다음과 같습니다.

   ```
   Limit by user property

   ASM person title

   is equal to

   Instructor
   ```



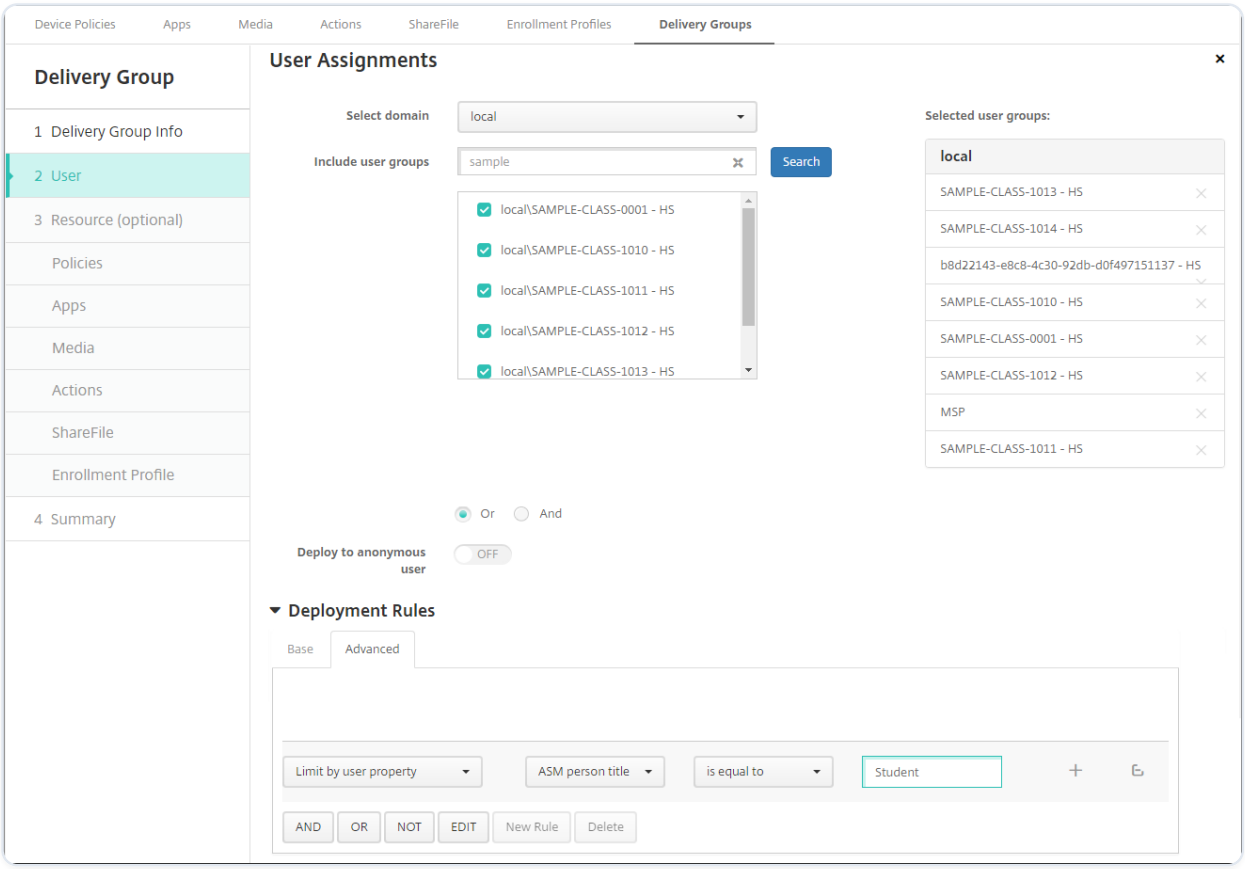
다음 사용자 할당은 학생용입니다. 배포 규칙은 다음과 같습니다.

```
Limit by user property

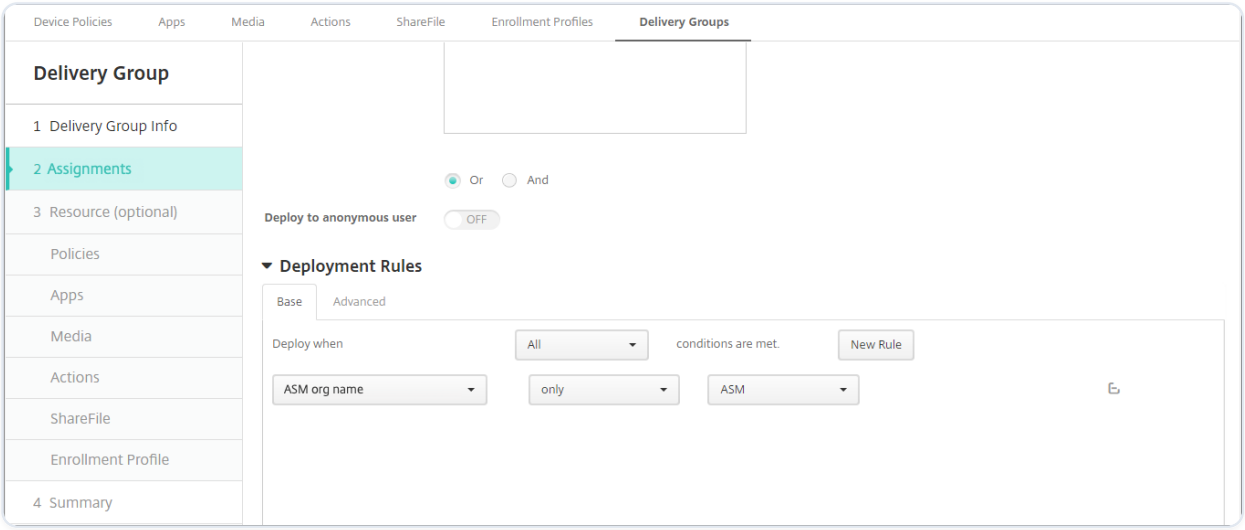
ASM person title

is equal to

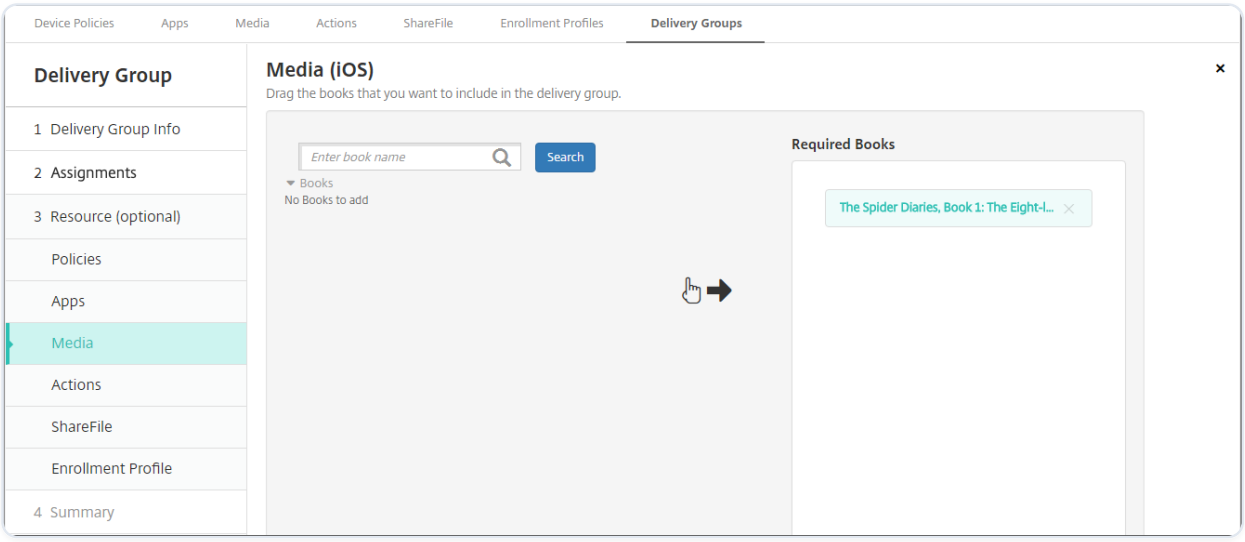
Student
```



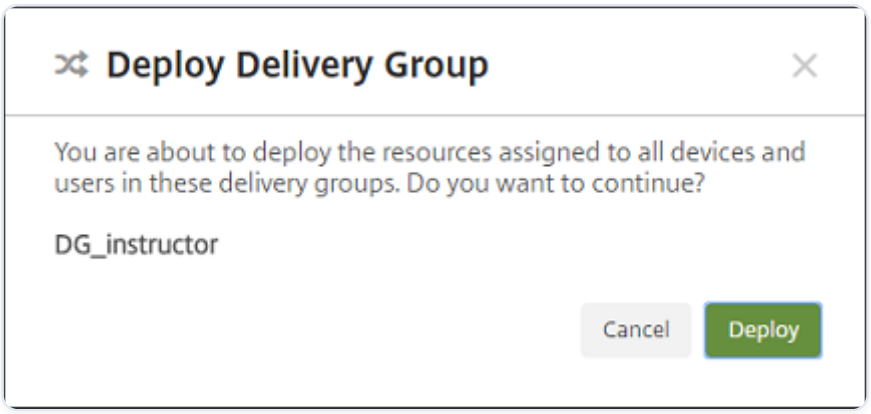
ASM 조직 이름을 기반으로 하는 배포 규칙을 사용하여 배달 그룹을 필터링할 수도 있습니다.



5. 리소스를 배달 그룹에 할당합니다. 다음 예는 배달 그룹에 포함된 iBook을 보여줍니다.



다음 예시는 배달 그룹을 선택하고 **배포**를 클릭할 때 나타나는 확인 대화 상자를 보여줍니다.



자세한 내용은 리소스 배포에서 "배달 그룹 편집" 및 "배달 그룹에 배포"를 참조하십시오.

8단계: 강사 및 학생 장치 등록 테스트

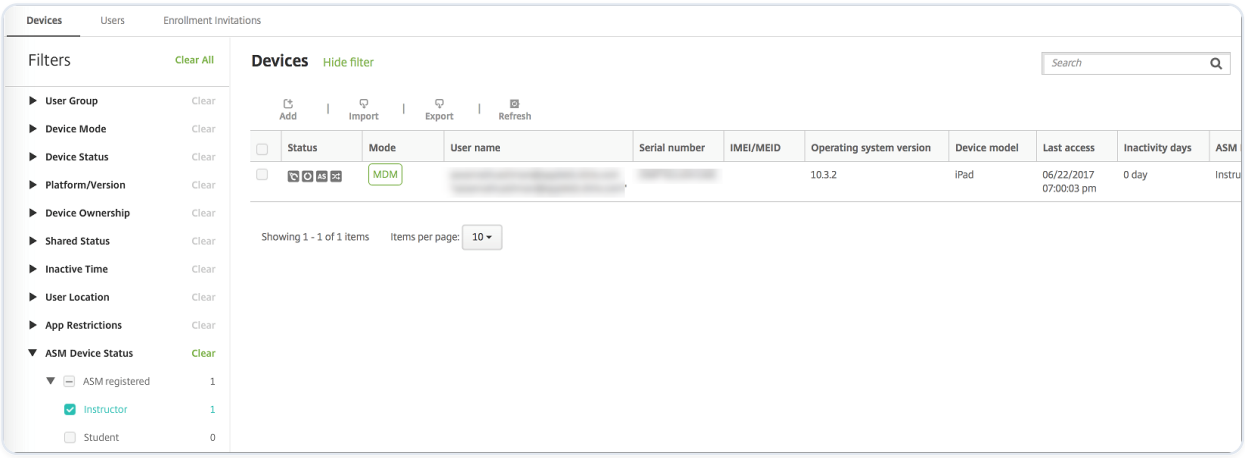
다음 방법 중 하나를 통해 장치를 등록할 수 있습니다.

- 학교 관리자는 XenMobile 콘솔에서 설정할 수 있는 사용자 암호를 사용하여 강사 및 학생 장치를 등록할 수 있습니다. 결과적으로 사용자에게 앱과 미디어가 이미 설정된 장치를 제공할 수 있습니다.
- 사용자가 장치를 받으면 제공된 사용자 암호를 사용하여 등록합니다. 등록이 완료되면 XenMobile은 장치 정책, 앱 및 미디어를 장치로 보냅니다.

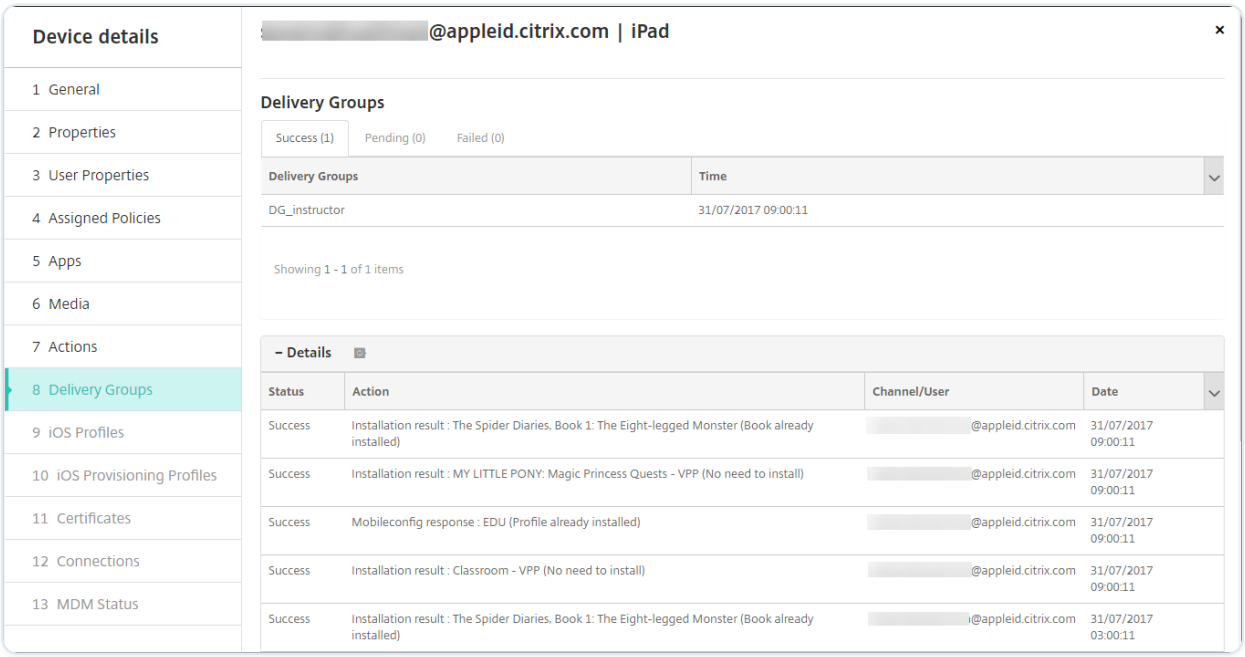
등록을 테스트하려면 ASM에 연결된 Apple 배포 프로그램 장치를 사용하십시오.

1. 장치가 ASM에 연결되어 있지 않으면 하드 리셋을 수행하여 장치 콘텐츠 및 설정을 지우십시오.
2. 강사로 ASM 장치를 등록합니다. 그런 다음 학생으로 ASM 장치를 등록합니다.
3. **관리 > 장치** 페이지에서 두 ASM 장치 모두 MDM에만 등록되었는지 확인합니다.

   장치 페이지를 ASM 장치 상태(예: **ASM 등록됨**, **ASM 공유됨**, **강사**, **학생**)별로 필터링할 수 있습니다.



4. 각 장치에 MDM 리소스가 올바르게 배포되었는지 확인하려면: 장치를 선택하고 **편집**을 클릭한 다음 다양한 페이지를 확인합니다.



9단계: 장치 배포

Apple은 강사와 학생에게 장치를 배포할 수 있도록 이벤트를 개최할 것을 권장합니다.

사전 등록된 장치를 배포하지 않는 경우, 다음 정보를 사용자에게 제공하십시오.

- 등록을 위한 XenMobile 암호
- 관리형 Apple ID를 위한 ASM 임시 암호.

최초 사용자 경험은 다음과 같습니다.

1. 사용자가 하드 리셋 후 장치를 처음 시작할 때, XenMobile은 등록 화면에서 장치를 등록하도록 안내합니다.
2. 사용자는 XenMobile에 인증하는 데 사용되는 관리형 Apple ID와 XenMobile 암호를 제공합니다.

3. Apple ID 설정 단계에서 장치는 사용자에게 관리형 Apple ID와 ASM 임시 암호를 제공하도록 안내합니다. 이 정보는 사용자를 Apple 서비스에 인증합니다.
4. 장치는 사용자에게 iCloud에서 데이터를 보호하는 데 사용되는 관리형 Apple ID의 암호를 생성하도록 안내합니다.
5. 설정 지원이 완료되면 XenMobile은 장치에 정책, 앱 및 미디어를 설치하기 시작합니다. 사용자 수준에서 할당된 앱 및 iBooks의 경우, 지원은 강사와 학생에게 볼륨 구매에 등록하도록 안내합니다. 초대를 수락한 후, 사용자는 다음 배포 시 (6시간 이내) 볼륨 구매 앱 및 iBooks를 받게 됩니다.

강사, 학생 및 수업 데이터 관리

강사, 학생 및 수업 데이터를 관리할 때 다음 사항에 유의하십시오.

- ASM 정보를 XenMobile로 가져온 후에는 관리형 Apple ID를 변경하지 마십시오. XenMobile은 또한 ASM 사용자 식별자를 사용하여 사용자를 식별합니다.
- 하나 이상의 교육 구성 장치 정책을 생성한 후 ASM에서 수업 데이터를 추가하거나 변경하는 경우: 정책을 편집한 다음 다시 배포하십시오.
- Education Configuration 장치 정책을 배포한 후 수업 강사가 변경되는 경우: 정책이 XenMobile 콘솔에서 업데이트되었는지 확인한 다음 정책을 다시 배포합니다.
- ASM 포털에서 사용자 속성을 업데이트하면 XenMobile도 콘솔에서 해당 속성을 업데이트합니다. 그러나 XenMobile은 다른 속성을 수신하는 것과 동일한 방식으로 ASM 개인 직함 속성(강사, 학생 또는 기타)을 수신하지 않습니다. 따라서 ASM에서 ASM 개인 직함을 변경하는 경우 XenMobile에 해당 변경 사항을 반영하려면 다음 단계를 완료하십시오.

데이터를 관리하려면:

1. ASM 포털에서 학생 등급을 업데이트하고 강사 등급을 지웁니다.
2. 학생 계정을 강사 계정으로 변경한 경우, 해당 사용자를 수업의 학생 목록에서 제거합니다. 그런 다음, 동일하거나 다른 수업의 강사 목록에 해당 사용자를 추가합니다.

   강사 계정을 학생 계정으로 변경한 경우, 해당 사용자를 수업에서 제거합니다. 그런 다음, 동일하거나 다른 수업의 학생 목록에 해당 사용자를 추가합니다. 업데이트는 다음 동기화(기본적으로 5분마다) 또는 가져오기(기본적으로 24시간마다) 중에 XenMobile 콘솔에 나타납니다.
3. 변경 사항을 적용하고 다시 배포하려면 Education Configuration 장치 정책을 편집합니다.

   - ASM 포털에서 사용자를 삭제하면 가져오기 후 XenMobile도 XenMobile 콘솔에서 해당 사용자를 삭제합니다.

     이 서버 속성 값인 **bulk.enrollment.fetchRosterInfoDelay** (기본값은 **1440**분)를 변경하여 두 기준선 사이의 간격을 줄일 수 있습니다.

- 리소스를 배포한 후: 학생이 수업에 참여하면 해당 학생만 포함하는 배달 그룹을 생성하고 학생에게 리소스를 배포합니다.
- 학생이나 강사가 임시 암호를 분실한 경우 ASM 관리자에게 문의하도록 합니다. 관리자는 임시 암호를 제공하거나 새 암호를 생성할 수 있습니다.

Apple School Manager Apple 배포 프로그램에 등록된 분실 또는 도난 장치 관리

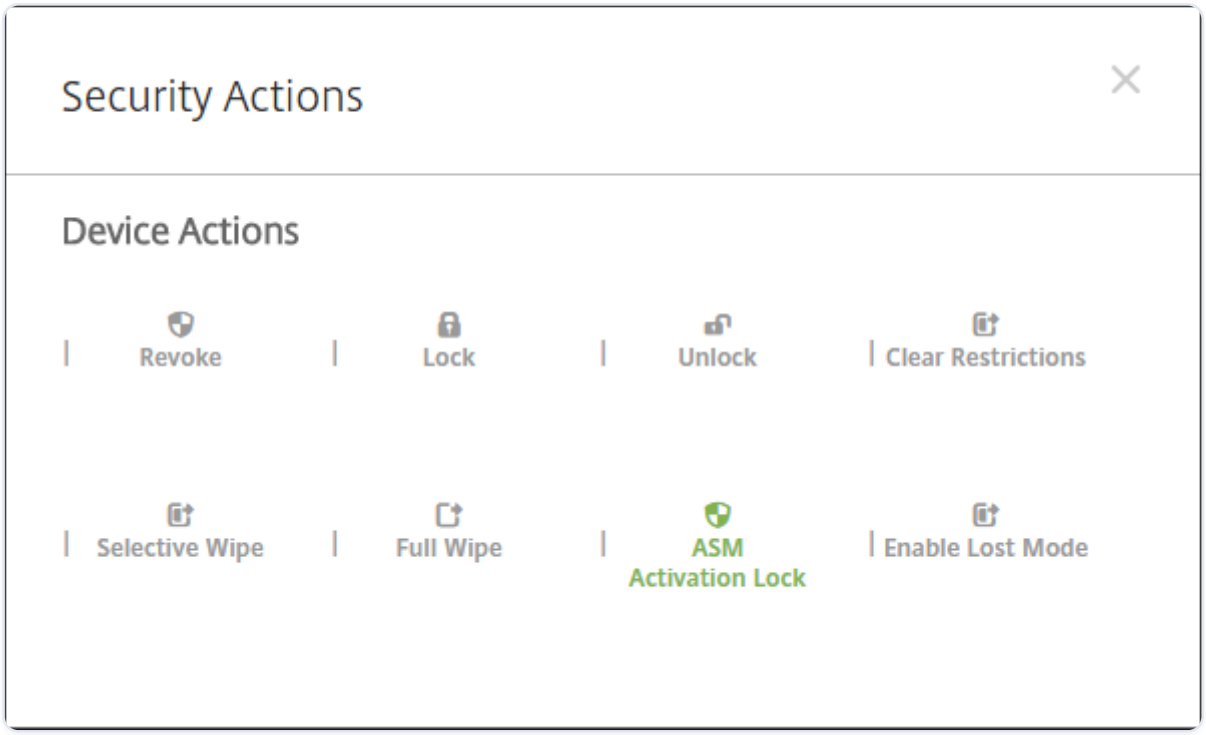
Apple 나의 iPhone/iPad 찾기 서비스에는 활성화 잠금 기능이 포함되어 있습니다. 활성화 잠금은 Apple 배포 프로그램에 등록된 분실 또는 도난 장치를 비인가 사용자가 사용하거나 재판매하는 것을 방지합니다.

XenMobile에는 ASM Apple 배포 프로그램에 등록된 장치에 잠금 코드를 보낼 수 있는 **ASM 활성화 잠금** 보안 작업이 포함되어 있습니다.

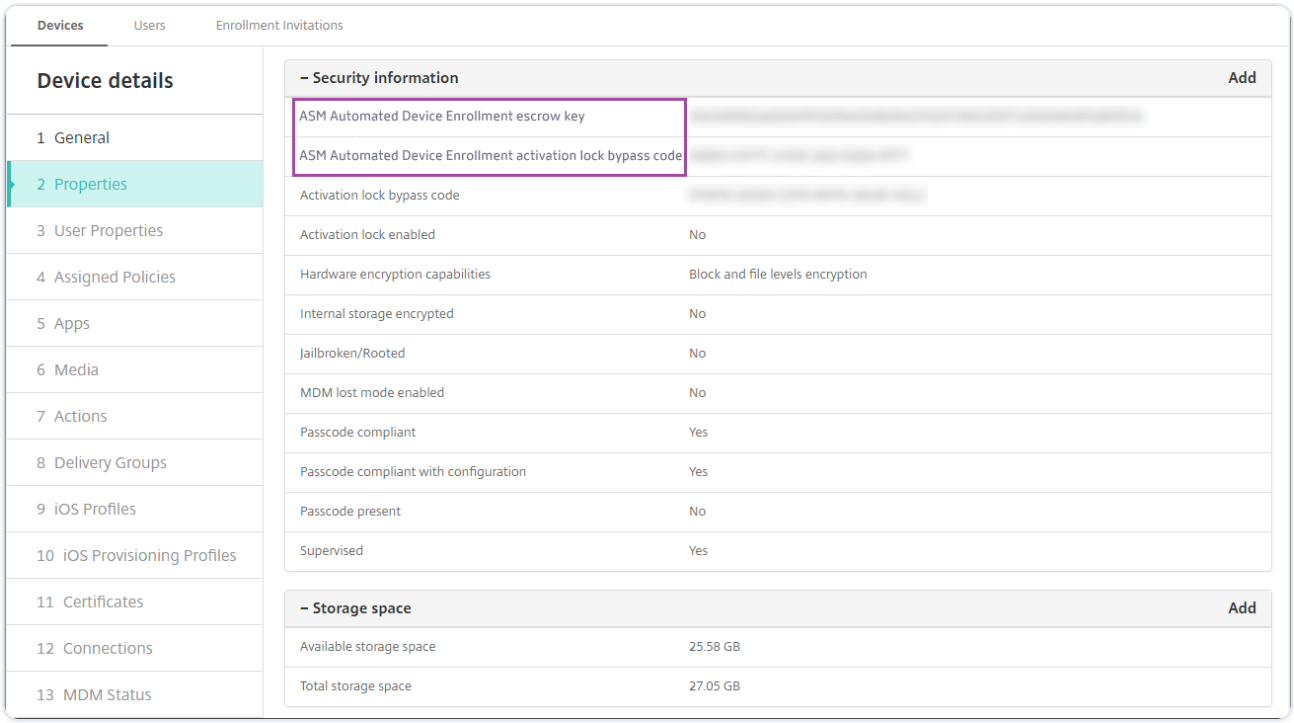
ASM 활성화 잠금 보안 작업을 사용하면 XenMobile이 사용자가 나의 iPhone/iPad 찾기 서비스를 활성화할 필요 없이 장치를 찾을 수 있습니다. ASM 장치가 하드 리셋되거나 완전히 초기화되면 사용자는 Managed Apple ID와 암호를 제공하여 장치를 잠금 해제합니다.

콘솔에서 잠금을 해제하려면 보안 작업 **활성화 잠금 우회**를 클릭합니다. 활성화 잠금 우회에 대한 자세한 내용은 iOS 활성화 잠금 우회를 참조하십시오. 사용자는 로그인 필드를 비워두고 **ASM 활성화 잠금 우회 코드**를 암호로 입력할 수도 있습니다. 이 정보는 **장치 세부 정보**의 **속성** 탭에서 확인할 수 있습니다.

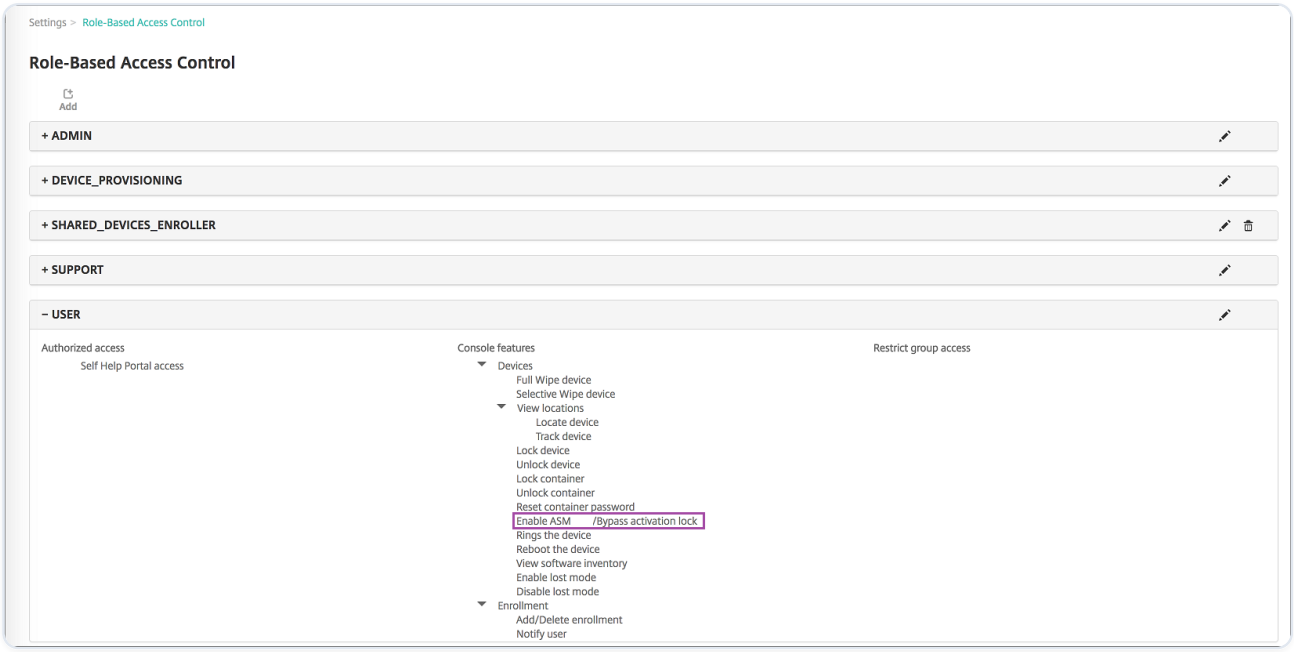
활성화 잠금을 설정하려면 **관리 > 장치**로 이동하여 장치를 선택하고 **보안**을 클릭한 다음 **ASM 활성화 잠금**을 클릭합니다.



ASM 에스크로 키 및 **ASM 활성화 잠금 우회 코드** 속성은 **장치 세부 정보**에 나타납니다.



ASM 활성화 잠금에 대한 RBAC 권한은 **장치 > ASM 우회 활성화 잠금 사용**입니다.



공유 iPad

공유 iPad 기능을 사용하면 여러 사용자가 iPad를 사용할 수 있습니다. 기기가 공유되더라도 사용자 경험은 개인화될 수 있습니다. 공유 iPad는 교육 또는 비즈니스용으로 사용할 수 있습니다. Apple School Manager (ASM)는 Apple Business Manager (ABM)가 지원하는 역할 외에도 교사 및 학생 역할을 지원합니다.

전제 조건

- 애플 스쿨 매니저 또는 애플 비즈니스 매니저

- 젠모바일® 서버
- 모든 iPad Pro, iPad 5세대, iPad Air 2 이상, iPad mini 4 이상
- 최소 32GB 저장 공간
- 감독됨

공유 iPad 구성

교실의 여러 학생이 한 명 또는 여러 명의 교사가 가르치는 다양한 과목을 위해 iPad를 공유할 수 있습니다.

관리자 또는 교사가 공유 iPad를 등록한 다음 기기에 장치 정책, 앱 및 미디어를 배포합니다. 그 후 학생들은 관리형 Apple ID 자격 증명을 제공하여 공유 iPad에 로그인합니다. 이전에 학생들에게 교육 구성 정책을 배포한 경우, 더 이상 공유 기기에 "다른 사용자"로 로그인하지 않습니다.

XenMobile은 공유 iPad에 대해 두 가지 통신 채널을 사용합니다. 장치 소유자(교사)를 위한 시스템 채널과 현재 상주 사용자(학생)를 위한 사용자 채널입니다. XenMobile은 이러한 채널을 사용하여 Apple에서 지원하는 리소스에 대해 적절한 MDM 명령을 보냅니다.

시스템 채널을 통해 배포되는 리소스는 다음과 같습니다.

- 장치 정책: 교육 구성, 최대 상주 사용자, 및 암호 잠금 유예 기간
- 장치 기반 볼륨 구매 앱

  Apple은 Shared iPad에서 Enterprise 앱 또는 사용자 기반 볼륨 구매 앱을 지원하지 않습니다. Shared iPad에 설치된 앱은 기기 전체에 적용되며 사용자별로 적용되지 않습니다.
- 사용자 기반 볼륨 구매 iBooks

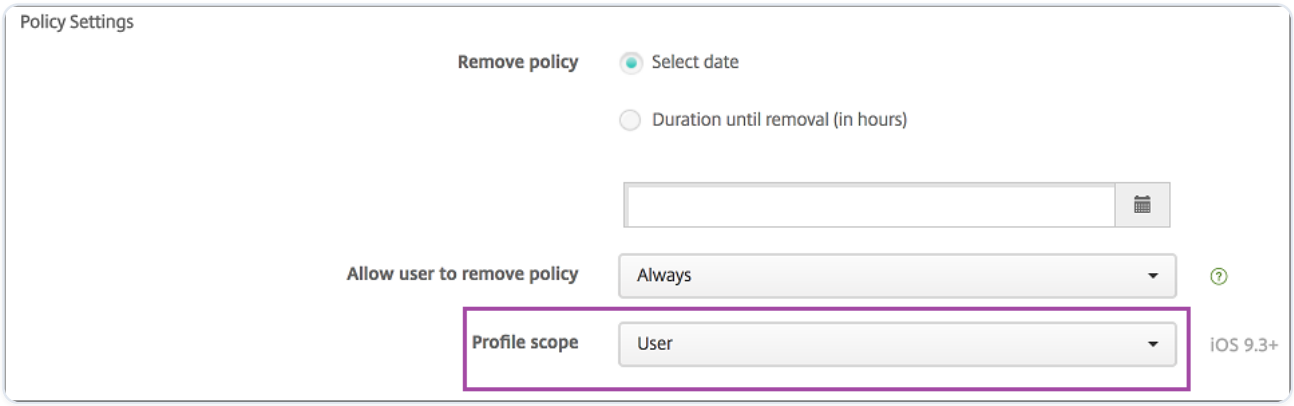
  Apple은 Shared iPad에서 사용자 기반 볼륨 구매 iBooks 할당을 지원합니다.

사용자 채널을 통해 배포되는 리소스는 다음과 같습니다:

- 기기 정책: 앱 알림, 홈 화면 레이아웃, 제한 사항 및 웹 클립

  XenMobile은 사용자 채널을 통한 이러한 기기 정책만 지원합니다.

기기 정책을 구성할 때 정책 설정 **프로필 범위**에서 배포 채널을 지정합니다.



사용자 채널을 통해 배포한 기기 정책을 제거하려면 프로필 제거 정책에 대해 **배포 범위**를 **사용자**로 선택해야 합니다.

일반적인 워크플로

일반적으로 사전 구성되고 감독되는 Shared iPad를 강사에게 제공합니다. 그러면 강사가 학생들에게 기기를 배포합니다. 사전 등록된 Shared iPad를 강사에게 배포하지 않는 경우: 강사가 기기를 등록할 수 있도록 XenMobile Server 암호를 제공해야 합니다.

Shared iPad를 구성하고 등록하는 일반적인 워크플로는 다음과 같습니다:

1. XenMobile Server 콘솔을 사용하여 **공유 모드**가 활성화된 ASM 또는 ABM 계정(**설정** > **Apple 배포 프로그램**)을 추가합니다. 자세한 내용은 Shared iPad용 ASM 또는 ABM 계정 관리를 참조하십시오.
2. 이 섹션에 설명된 대로 필요한 기기 정책, 앱 및 미디어를 XenMobile에 추가합니다. 해당 리소스를 배달 그룹에 할당합니다.
3. 강사가 Shared iPad를 하드 리셋하도록 합니다. 등록을 위한 원격 관리 화면이 나타납니다.
4. 강사들이 공유 iPad를 등록합니다.

   XenMobile은 구성된 리소스를 등록된 각 공유 iPad에 배포합니다. 자동 재시작 후 강사는 기기를 학생들과 공유할 수 있습니다. iPad에 로그인 페이지가 나타납니다.
5. 학생은 수업을 선택한 다음 관리형 Apple ID와 임시 ASM 또는 ABM 암호를 입력합니다.

   공유 iPad는 ASM 또는 ABM으로 인증하고 학생에게 ASM 또는 ABM 암호를 생성하도록 요청합니다. 다음 공유 iPad 로그인 시 학생은 새 암호를 입력해야 합니다.
6. iPad를 공유하는 다른 학생은 이전 단계를 반복하여 로그인할 수 있습니다.

공유 iPad용 Apple School Manager 또는 Apple Business Manager 계정 관리

Apple Education과 함께 XenMobile을 이미 사용하는 경우: 강사가 사용하는 기기와 같이 공유되지 않는 기기에 대해 XenMobile에 구성된 기존 ASM 또는 ABM 계정이 있습니다. 공유 기기와 비공유 기기 모두에 동일한 ASM 또는 ABM 및 동일한 XenMobile Server를 사용할 수 있습니다.

XenMobile은 다음 배포 시나리오를 지원합니다.

- 수업당 공유 iPad 그룹

  이 시나리오에서는 공유 iPad를 학생 수업에 할당합니다. iPad는 교실에 보관됩니다. 해당 수업에서 다른 과목을 가르치는 강사는 동일한 iPad 세트를 사용합니다.

- 강사당 공유 iPad 그룹

  이 시나리오에서는 공유 iPad를 강사에게 할당하며, 강사는 해당 iPad를 가르치는 다양한 수업에 사용합니다.

공유 iPad를 기기 그룹으로 구성

ASM 또는 ABM을 사용하면 여러 MDM 서버를 생성하여 기기를 그룹으로 구성할 수 있습니다. 공유 iPad를 MDM 서버에 할당할 때 수업 또는 강사별로 각 공유 iPad 그룹에 대한 기기 그룹을 생성합니다.

- 공유 iPad 그룹 1 > 기기 그룹 1 MDM 서버
- 공유 iPad 그룹 2 > 장치 그룹 2 MDM 서버
- 공유 iPad 그룹 N > 장치 그룹 N MDM 서버

각 장치 그룹에 대한 ASM 또는 ABM 계정 추가

XenMobile Server 콘솔에서 여러 ASM 또는 ABM 계정을 생성하면 공유 iPad 그룹(각 클래스 또는 강사용으로 하나씩)이 자동으로 가져와집니다.

- 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 iPad에 대한 특정 요구 사항은 다음과 같습니다.

- 다음 설정이 활성화된 각 장치 그룹에 대한 ASM 또는 ABM 계정 하나:
  - **장치 등록 필요**
  - **감독 모드**
  - **공유 모드**
- 주어진 교육 기관의 경우 모든 ASM 또는 ABM 계정에 동일한 **교육 접미사**를 사용해야 합니다.

계정을 추가하려면 **설정** > **Apple 배포 프로그램**으로 이동합니다.

Apple 배포 프로그램 설정 구성 화면(/en-us/xenmobile/server/media/settings-dep-account-ios-shared.png)

공유 iPad용 앱

공유 iPad는 장치 기반 볼륨 구매 앱 할당을 지원합니다. 공유 iPad에 앱을 배포하기 전에 XenMobile은 Apple 볼륨 구매 서버에 요청을 보내 장치에 볼륨 구매 라이선스를 할당합니다. 볼륨 구매 할당을 확인하려면 **구성** > **앱** > **iPad**로 이동하여 **볼륨 구매**를 확장합니다.

공유 iPad용 미디어

공유 iPad는 사용자 기반 볼륨 구매 iBooks 할당을 지원합니다. 공유 iPad에 iBooks를 배포하기 전에 XenMobile은 Apple 볼륨 구매 서버에 요청을 보내 학생들에게 볼륨 구매 라이선스를 할당합니다. 볼륨 구매 할당을 확인하려면 **구성** > **미디어** > **iPad**로 이동하여 **볼륨 구매**를 확장합니다.

미디어 구성 화면(/en-us/xenmobile/server/media/configure-media-shared-ipad.png)

공유 iPad용 배포 규칙

공유 iPad 배포의 경우, 배달 그룹 수준의 규칙은 사용자 속성과 관련되어 적용되지 않습니다. 각 장치 그룹에 대한 정책, 앱 및 미디어를 필터링하려면 계정 이름을 기반으로 리소스에 대한 배포 규칙을 추가합니다. 예를 들어:

- 장치 그룹 1 계정에 대해 다음 배포 규칙을 설정합니다.

```
Apple Deployment Program account name

Only

Device Group 1 account
```

- 장치 그룹 2 계정에 대해 다음 배포 규칙을 설정합니다.

```
Apple Deployment Program account name

Only
```

```
Device Group 2 account
```

- 장치 그룹 N 계정에 대해 다음 배포 규칙을 설정합니다.

```
Apple Deployment Program account name

Only

Device Group N account
```

장치 정책 구성 화면(/en-us/xenmobile/server/media/configure-policy-deployment-rule-instructor.png)

Apple Classroom 앱을 강사(공유되지 않은 iPad 사용)에게만 배포하려면 다음 배포 규칙을 사용하여 ASM 또는 ABM 공유 상태별로 리소스를 필터링합니다.

```
Deploy this resource regarding ASM or ABM shared mode

only

unshared
```

또는:

```
Deploy this resource regarding ASM or ABM shared mode

except

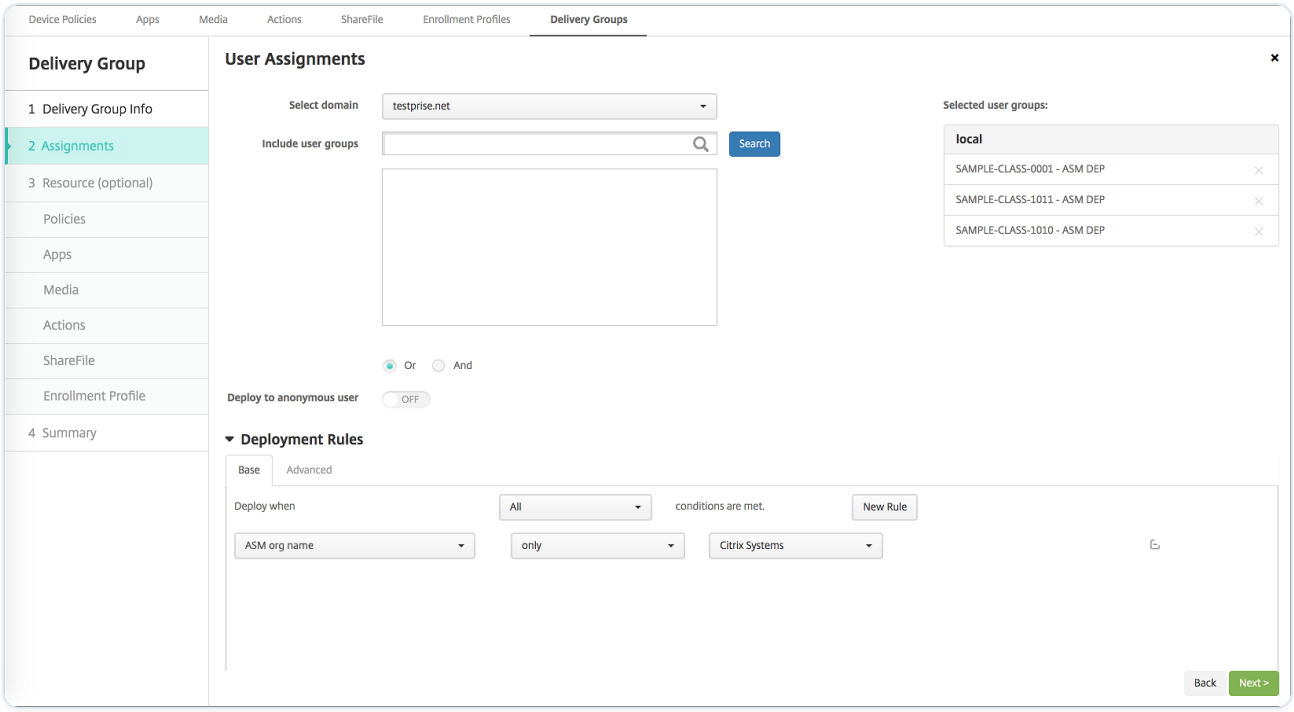
shareable
```

앱 구성 화면(/en-us/xenmobile/server/media/configure-apps-deployment-rule-shareable.png)

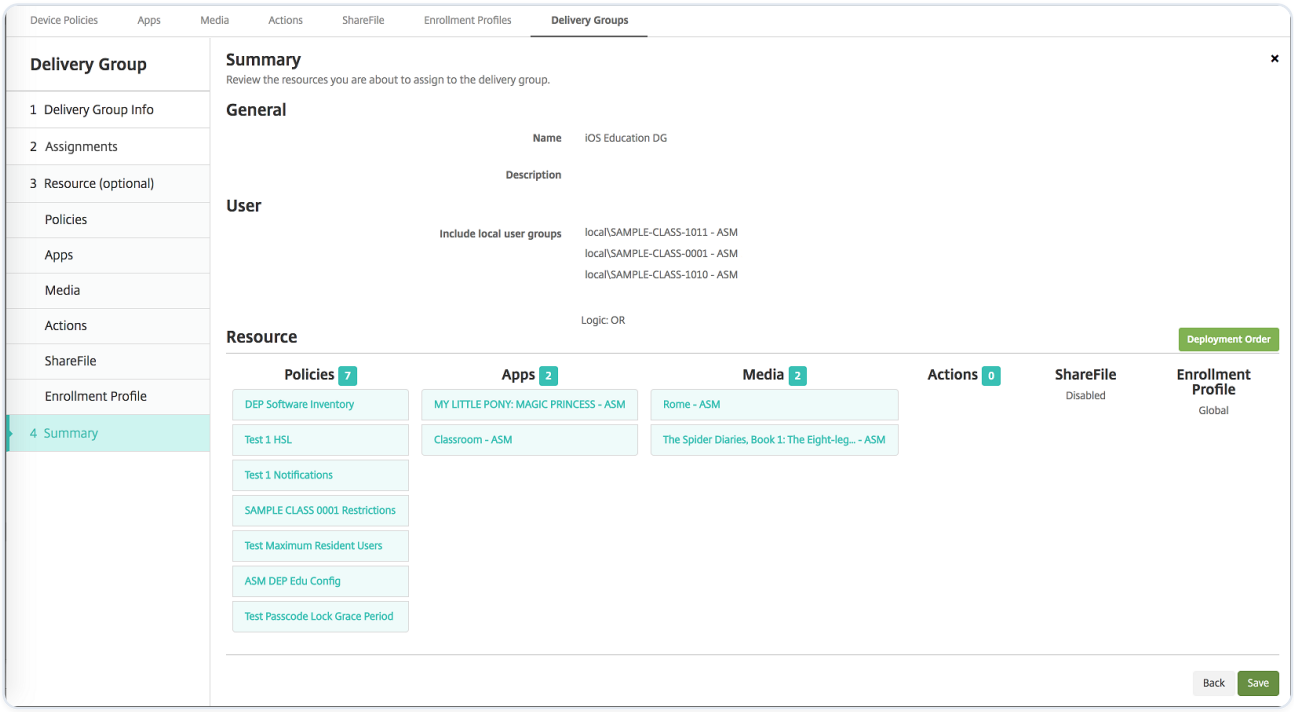
공유 iPad용 배달 그룹

각 강사용 장치 그룹의 경우:

- 하나의 배달 그룹을 구성합니다. 강사의 경우, 교육 구성 정책에서 정의하는 모든 수업을 할당합니다.



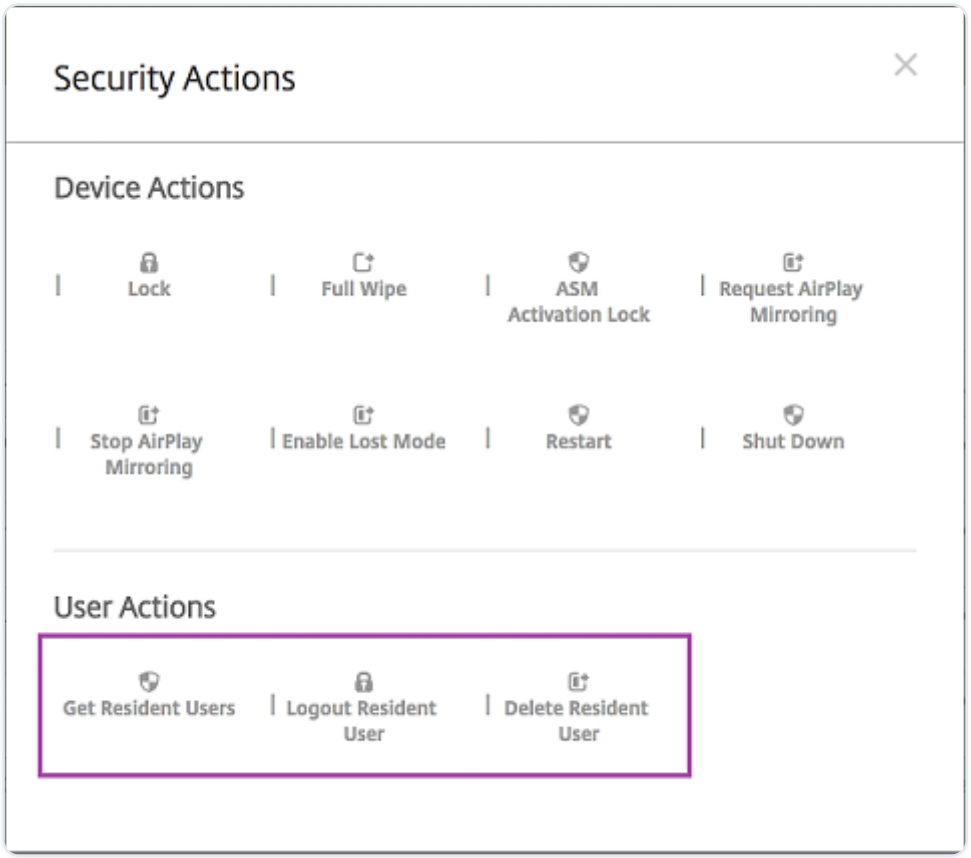
- 해당 배달 그룹에는 다음 MDM 리소스가 포함되어야 합니다:
  - 장치 정책:
    - 교육 구성
    - 앱 알림
    - 홈 화면 레이아웃
    - 제한 사항
    - 최대 상주 사용자
    - 암호 잠금 유예 기간
  - 필수 볼륨 구매 앱
  - 필수 볼륨 구매 iBooks



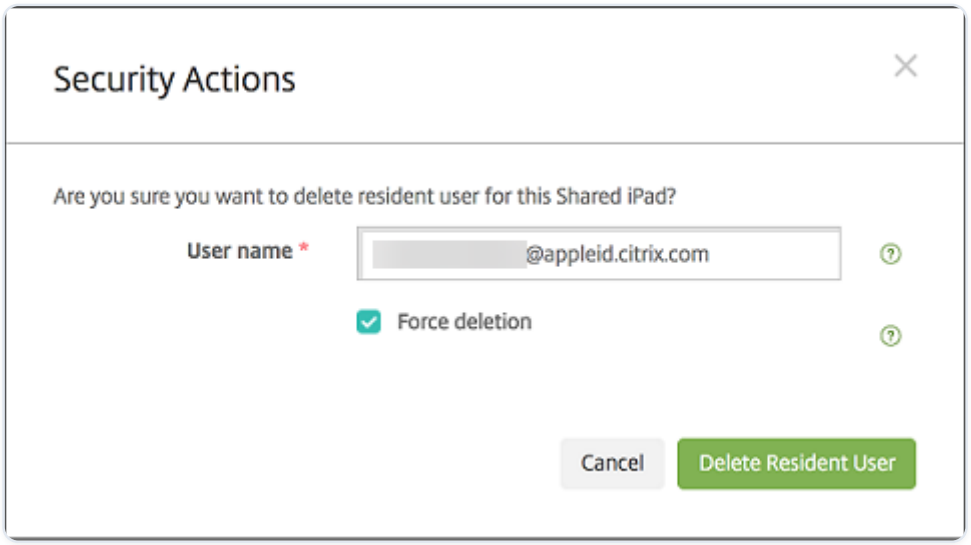
Shared iPad용 보안 작업

기존 보안 작업 외에도 공유 iPad에 대해 다음 보안 작업을 사용할 수 있습니다.

- **상주 사용자 가져오기:** 현재 장치에 활성 계정이 있는 사용자를 나열합니다. 이 작업은 장치와 XenMobile 콘솔 간의 동기화를 강제 실행합니다.
- **상주 사용자 로그아웃:** 현재 사용자의 로그아웃을 강제 실행합니다.
- **상주 사용자 삭제:** 특정 사용자의 현재 세션을 삭제합니다. 사용자는 다시 로그인할 수 있습니다.
- **모든 사용자 삭제:** 장치의 모든 사용자를 삭제합니다.



상주 사용자 삭제를 클릭한 후 사용자 이름을 지정할 수 있습니다.



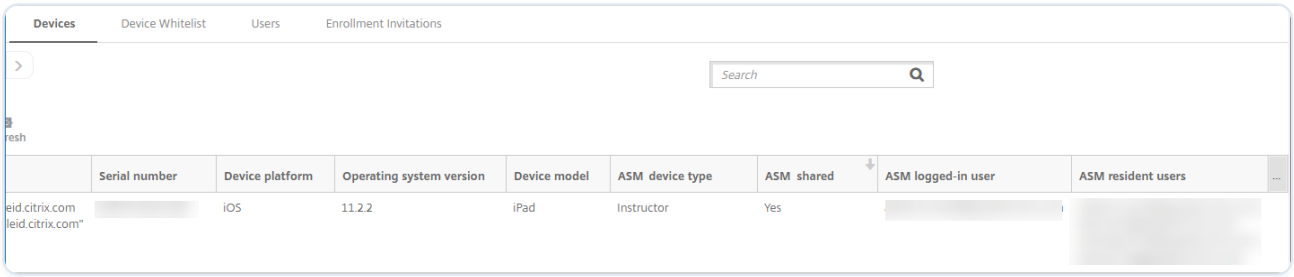
보안 작업 결과는 **관리** > **장치** > **일반** 및 **관리** > **장치** > **전달 그룹** 페이지에 나타납니다.

공유 iPad에 대한 정보 가져오기

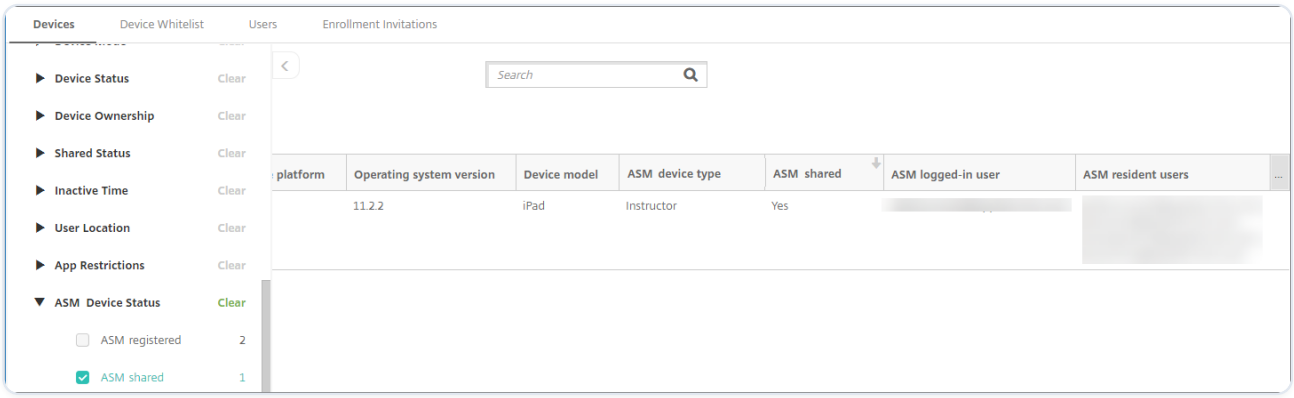
관리 > **장치** 페이지에서 공유 iPad에 대한 특정 정보를 찾으십시오.

- 다음 항목을 조회합니다.
  - 장치가 공유되는지 여부 (**ASM 또는 ABM 공유됨**)
  - 공유 장치에 로그인한 사용자 (**ASM 또는 ABM 로그인 사용자**)

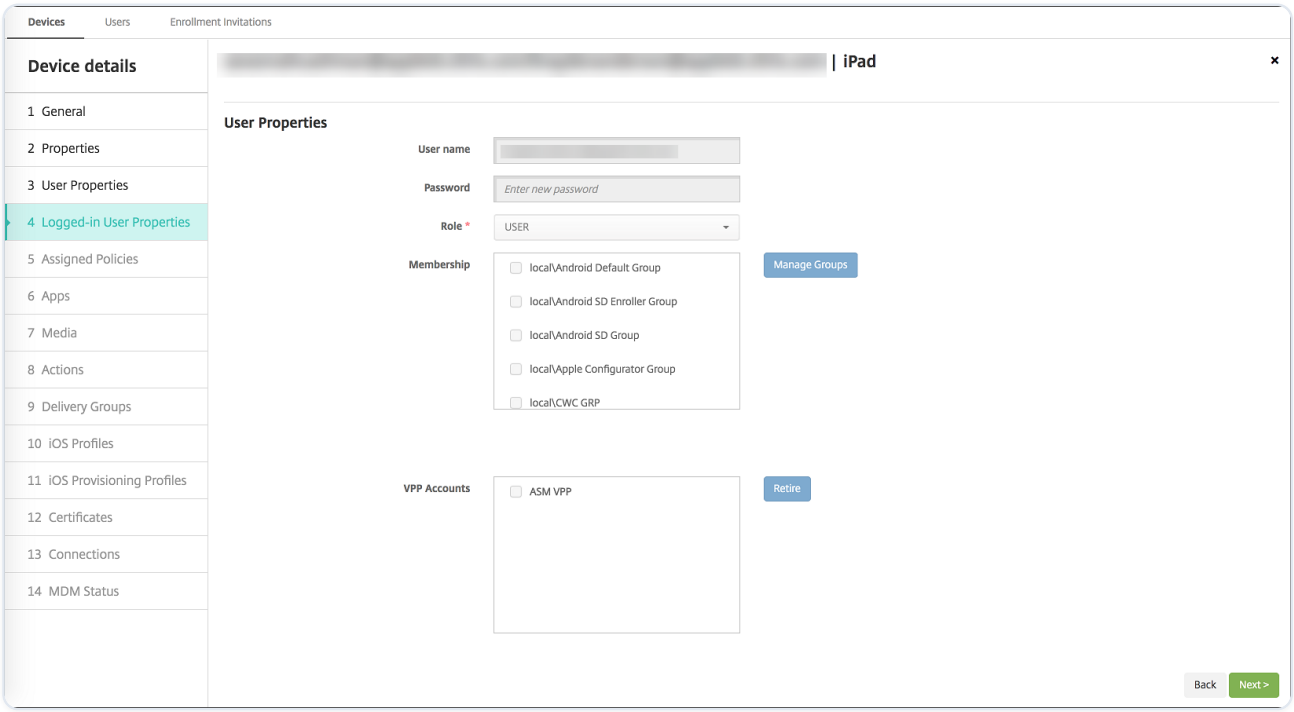
◦ 공유 장치에 할당된 모든 사용자 (**ASM 또는 ABM 상주 사용자**)

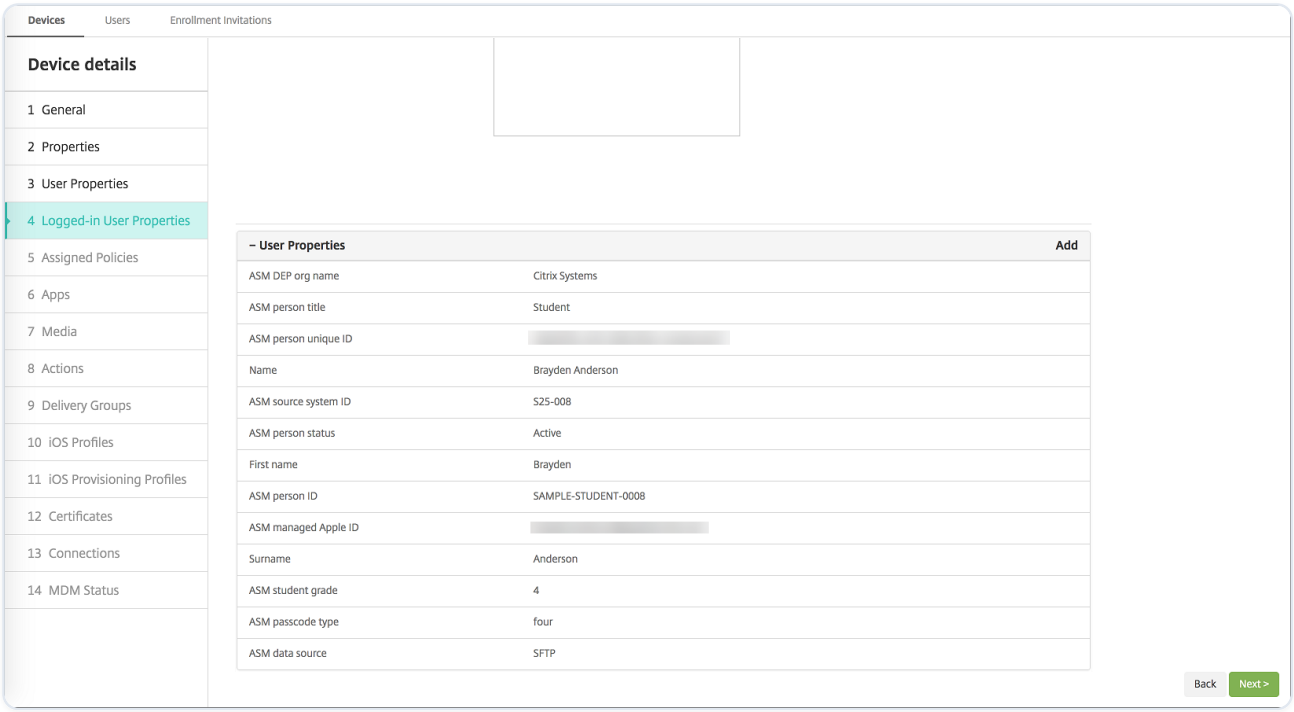


- 장치 목록을 **ASM 또는 ABM 장치 상태**로 필터링합니다.

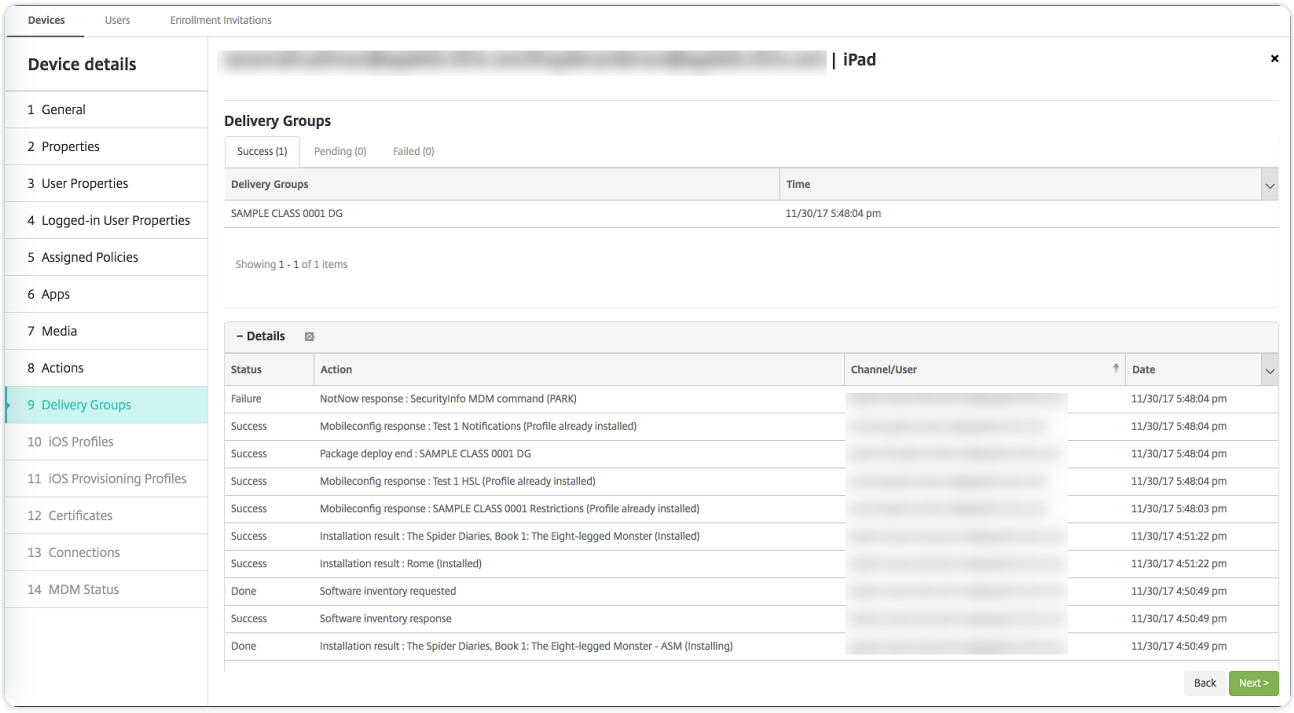


- **관리** > **장치** > **로그인한 사용자 속성** 페이지에서 공유 iPad에 로그인한 사용자에 대한 세부 정보를 봅니다.



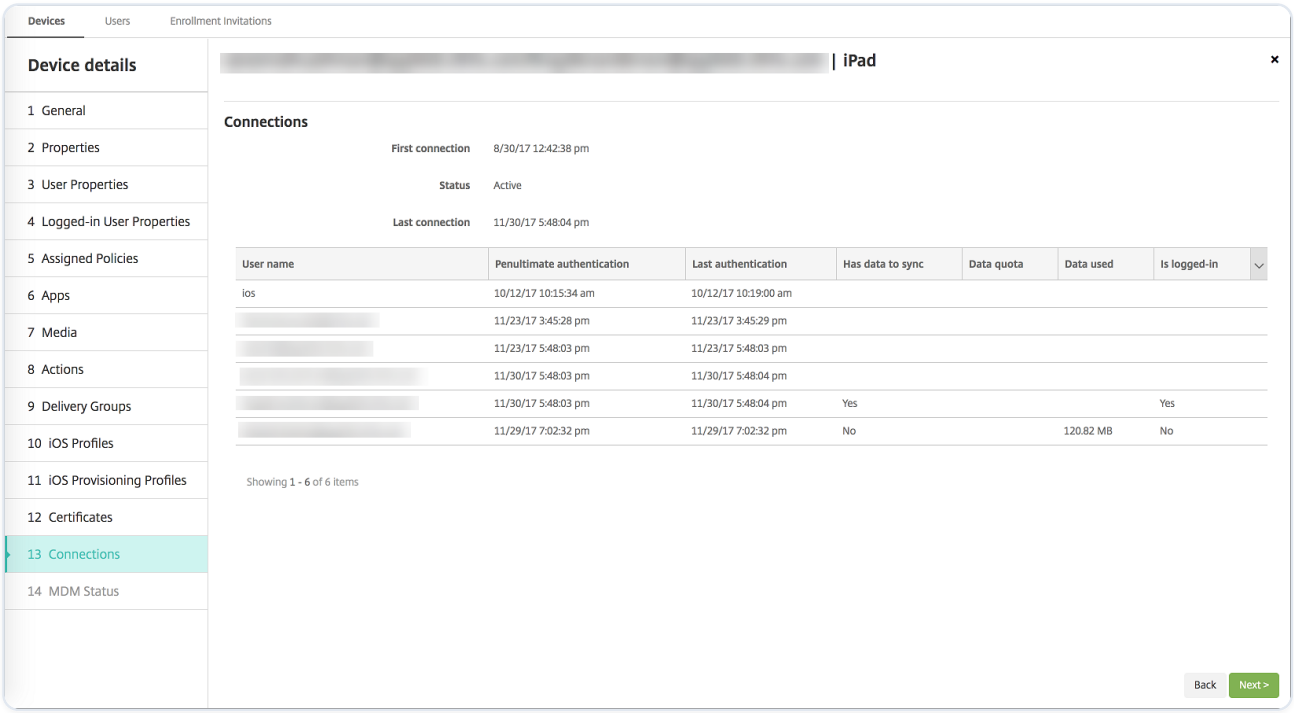


- **관리** > **장치** > **전달 그룹** 페이지에서 전달 그룹의 강사 및 사용자에게 리소스를 배포하는 데 사용되는 채널을 확인합니다. **채널/사용자** 열에는 유형(**시스템** 또는 **사용자**)과 수신자(강사 또는 학생)가 표시됩니다.

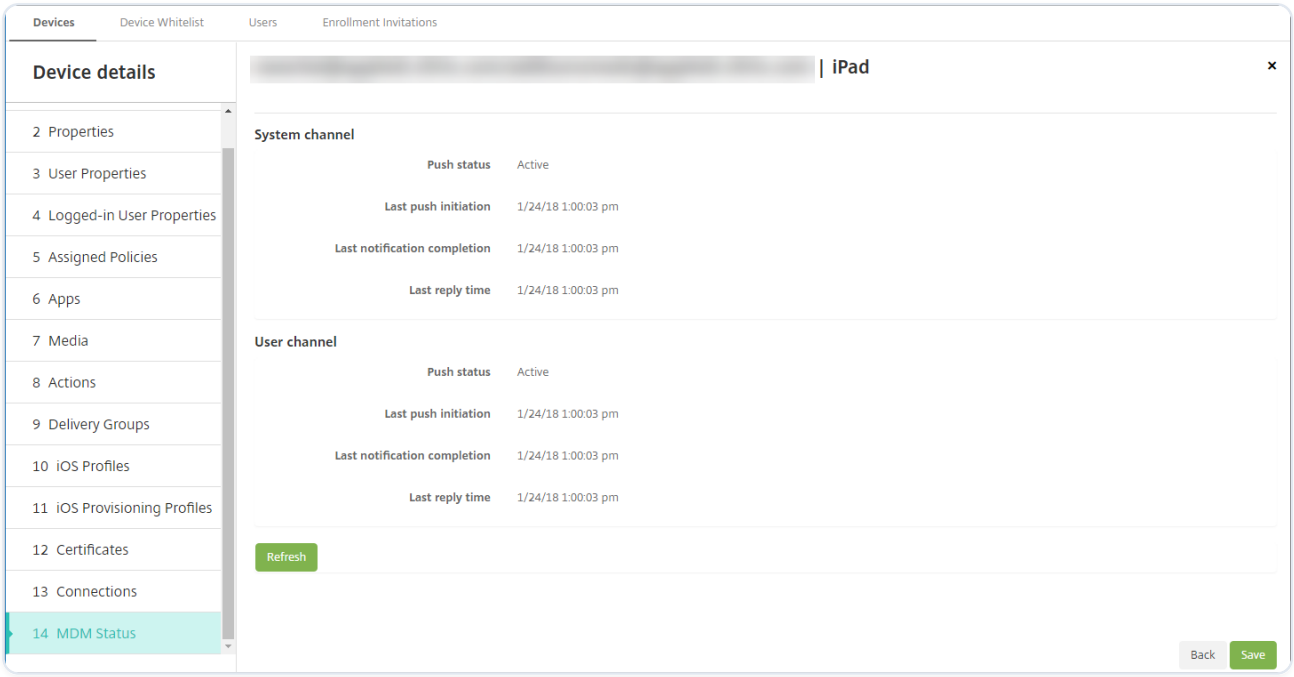


- 상주 사용자에 대한 정보 가져오기:
  - **동기화할 데이터가 있음:** 사용자가 클라우드에 동기화할 데이터가 있는지 여부.
  - **데이터 할당량:** 사용자에게 설정된 데이터 할당량(바이트). 사용자 할당량이 일시적으로 해제되었거나 사용자에게 적용되지 않는 경우 할당량이 표시되지 않을 수 있습니다.
  - **사용된 데이터:** 사용자가 사용한 데이터 양(바이트). 시스템이 정보를 수집하는 동안 오류가 발생하면 값이 표시되지 않을 수 있습니다.

- **로그인됨:** 사용자가 장치에 로그인되어 있는지 여부.



- 두 채널의 푸시 상태를 봅니다.



Apple 앱 배포

XenMobile은 장치에 배포된 앱을 관리합니다. 다음 유형의 iOS/iPadOS 및 macOS 앱을 구성하고 배포할 수 있습니다.

- **공개 앱 스토어(iOS/iPadOS만 해당):** 이러한 앱에는 Apple App Store 또는 Google Play와 같은 공개 앱 스토어에서 사용할 수 있는 무료 또는 유료 앱이 포함됩니다. 예를 들어 GoToMeeting이 있습니다.

- **엔터프라이즈(iOS/iPadOS/macOS):** MDX를 사용하도록 설정되지 않았으며 MDX 앱과 관련된 정책이 없는 기본 앱입니다.
- **MDX(iOS/iPadOS만 해당):** MAM SDK로 준비되었거나 MDX Toolkit으로 래핑된 앱입니다. 이러한 앱에는 MDX 정책이 포함됩니다. MDX 앱은 내부 소스 및 공개 스토어에서 가져옵니다.
- **볼륨 구매(iOS/iPadOS/macOS):** Apple 볼륨 구매 프로그램을 통해 라이선스가 관리되는 앱입니다.
- **iOS 사용자 지정 앱(iOS/iPadOS만 해당):** 사내 또는 타사에서 개발한 독점적인 B2B(기업 간) 앱입니다.

다양한 유형의 앱에 대한 자세한 내용은 앱 추가를 참조하십시오.

일부 배포에는 Apple Business Management(ABM) 또는 Apple School Management(ASM) 계정이 필요합니다. 자세한 내용은 다음 섹션을 참조하십시오.

각 앱 유형 및 배포 방법에 대해 Citrix는 일련의 구성 방식을 권장합니다. 다른 플랫폼용 앱 배포에 대한 자세한 내용은 앱 추가를 참조하십시오. 다음 섹션에서는 iOS 앱 구성에 대한 자세한 정보를 제공합니다.

앱 배포를 위한 일반적인 단계

시나리오	1단계: 계정 연결	2단계: 앱 추가 및 구성	3단계: 배달 그룹 구성 및 앱 배포
공개 앱 스토어 앱(#public-app-store-apps)(Citrix® 모빌리티 앱 포함)	해당 없음	**XenMobile®에서: 구성 > 앱**으로 이동하여 iPhone 또는 iPad용 **공개 앱 스토어** 앱을 추가합니다. 앱을 구성하고 배달 그룹에 할당합니다.	**XenMobile에서:** 배달 그룹을 사용하여 앱을 구성하고 배포합니다.
Apple 볼륨 구매로 제공되는 공개 앱 스토어 앱(#public-app-store-apps-delivered-with-apple-volume-purchase)(Citrix 모빌리티 앱 포함)	Apple 배포 프로그램에 등록합니다. **XenMobile에서: 설정 > 볼륨 구매**로 이동하여 볼륨 구매 계정을 추가합니다.	**ABM 또는 ASM에서:** 앱 및 도서에서 앱을 구매하고 추가합니다. **XenMobile에서: 구성 > 앱**으로 이동하여 앱을 구성하고 배달 그룹에 할당합니다.	**XenMobile에서:** 배달 그룹을 사용하여 앱을 구성하고 배포합니다.
엔터프라이즈 앱(#enterprise-apps)	해당 없음	**XenMobile에서: 구성 > 앱**으로 이동합니다. **추가**를 클릭한 다음 **엔터프라이즈**를 클릭합니다. IPA 파일을 업로드	**XenMobile에서:** 배달 그룹을 사용하여 앱을 구성하고 배포합니다.

시나리오	1단계: 계정 연결	2단계: 앱 추가 및 구성	3단계: 배달 그룹 구성 및 앱 배포
		합니다. 앱을 구성하고 배달 그룹에 할당합니다.	
MDX 앱(#mdx-apps)	해당 없음	**XenMobile에서: 구성 > 앱**으로 이동합니다. **추가**를 클릭한 다음 **MDX**를 클릭합니다. 플랫폼으로 **iPad/iPhone**을 선택했는지 확인합니다. MDX 파일을 업로드합니다. 앱을 구성하고 배달 그룹에 할당합니다.	**XenMobile에서:** 전송 그룹을 사용하여 앱을 구성하고 배포합니다.
Apple 볼륨 구매를 사용하여 배포된 MDX 앱	Apple 배포 프로그램에 등록합니다. **XenMobile에서: 설정 > 볼륨 구매**로 이동하여 볼륨 구매 계정을 추가합니다.	**ABM에서:** 앱 및 도서에서 MDX 앱을 구매하고 추가합니다. 앱을 ABM 계정에 연결합니다. **XenMobile에서: 구성 > 앱**으로 이동하여 앱을 구성하고 전송 그룹에 할당합니다.	**XenMobile에서:** 전송 그룹을 사용하여 앱을 구성하고 배포합니다.
사용자 지정 앱	Apple 배포 프로그램에 등록합니다. **XenMobile에서: 설정 > 볼륨 구매**로 이동하여 볼륨 구매 계정을 추가합니다.	**ABM에서:** 앱을 비공개 앱으로 App Store에 추가합니다. 앱을 ABM 계정에 연결합니다. **XenMobile에서: 구성 > 앱**으로 이동하여 앱을 구성하고 전송 그룹에 할당합니다.	**XenMobile에서:** 전송 그룹을 사용하여 앱을 구성하고 배포합니다.
MDX 지원 사용자 지정 앱	Apple 배포 프로그램에 등록합니다. **XenMobile에서: 설정 > 볼륨 구매**로 이동하여 볼륨 구매 계정을 추가합니다.	**ABM에서:** 앱을 비공개 앱으로 앱 스토어에 추가합니다. 앱을 ABM 계정에 연결합니다. **XenMobile에서: 구성 > 앱**으로 이동하여 MDX 파일을 업로드합	**XenMobile에서:** 전송 그룹을 사용하여 앱을 구성하고 배포합니다.

시나리오	1단계: 계정 연결	2단계: 앱 추가 및 구성	3단계: 배달 그룹 구성 및 앱 배포
		니다. 앱을 구성하고 전송 그룹에 할당합니다.	

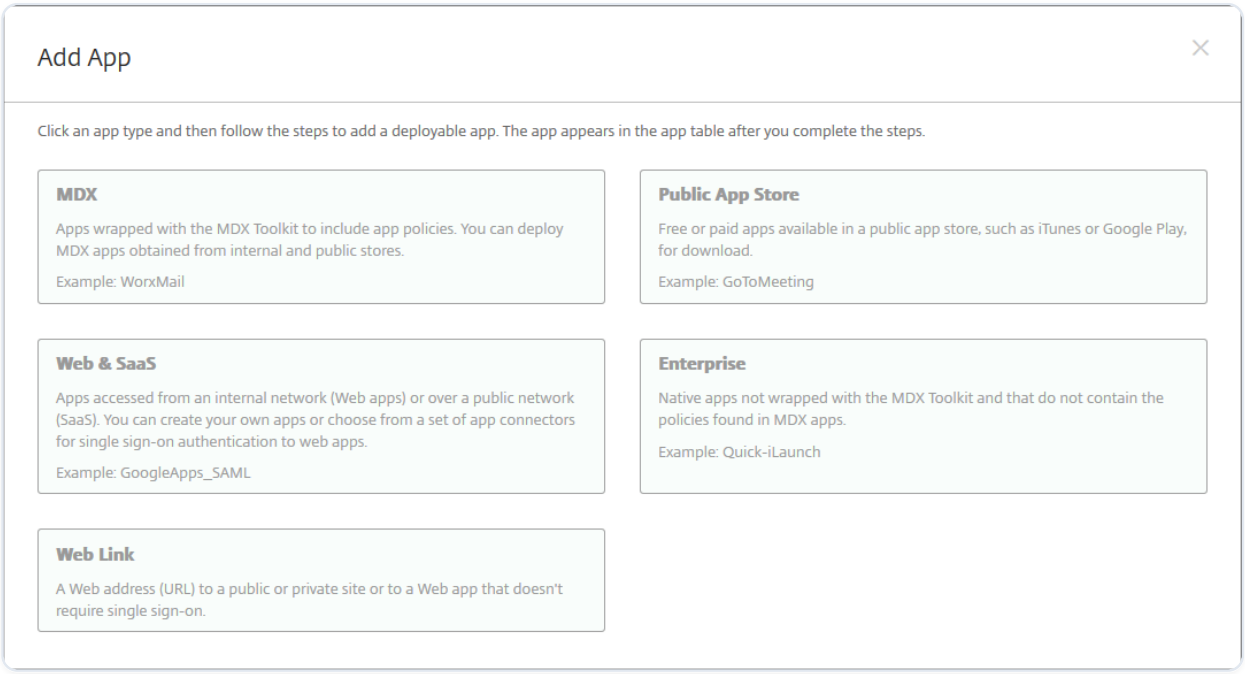
공개 앱 스토어 앱

App Store에서 사용할 수 있는 무료 및 유료 앱을 XenMobile에 추가할 수 있습니다.

기능 가용성	
장치 감독 필요	아니요
사용자 등록 모드에서 사용 가능	아니요
사용 가능	iOS/iPadOS

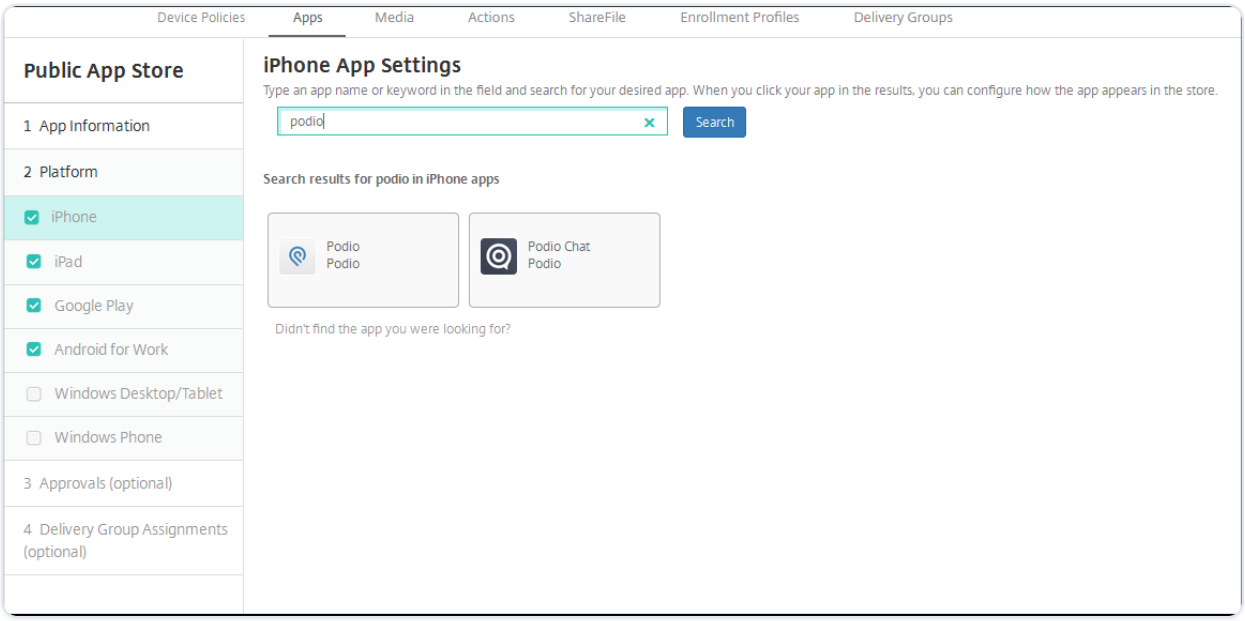
1단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. **추가**를 클릭합니다.
2. **공용 앱 스토어**를 클릭합니다.



3. 플랫폼으로 **iPhone** 또는 **iPad**를 선택합니다.

4. 검색 상자에 앱 이름을 입력하고 **검색**을 클릭합니다.

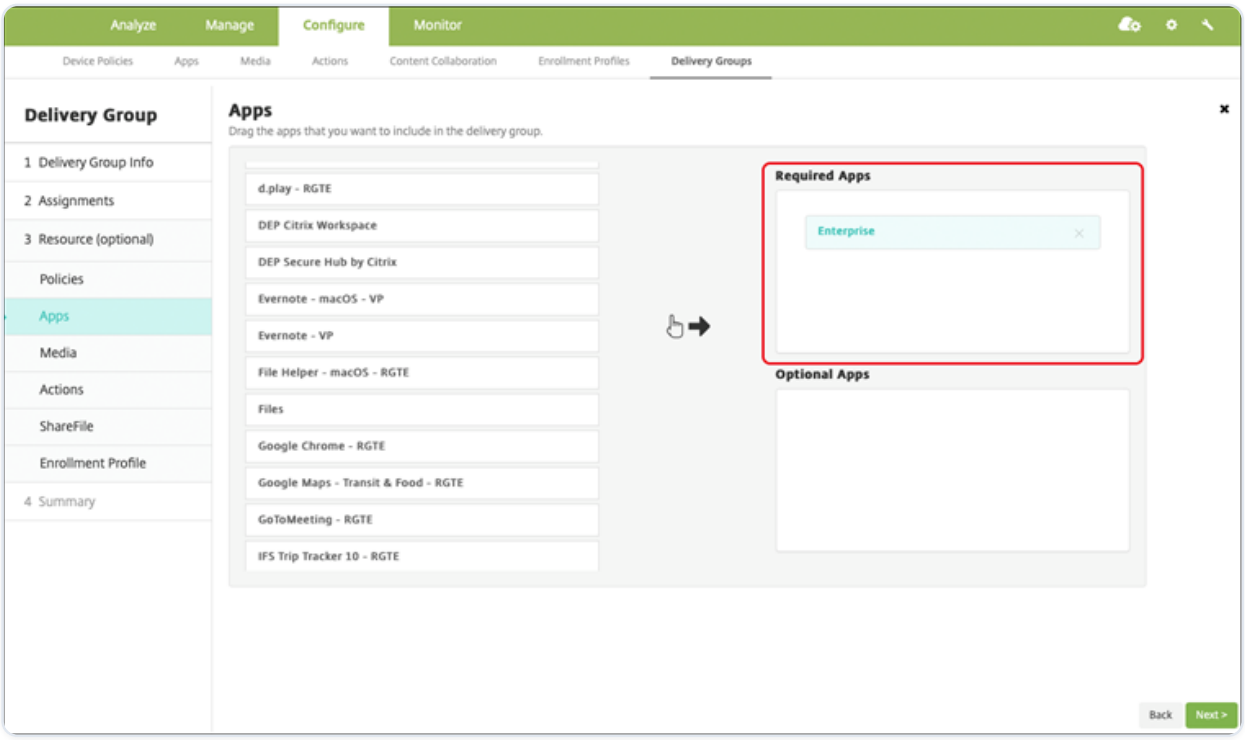


5. 검색 조건과 일치하는 앱이 나타납니다. 원하는 앱을 클릭합니다.
6. 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다.

2단계: 앱 배포 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다.
2. 구성하려는 앱을 선택하고 **편집**을 클릭합니다.
3. Citrix는 **앱 관리 강제 적용** 기능을 활성화할 것을 권장합니다.
4. 전달 그룹을 할당하고 **저장**을 클릭합니다.
5. **구성 > 전달 그룹 > 앱**으로 이동합니다.

6. 원하는 앱을 **필수**로 표시합니다.



7. **구성 > 전달 그룹**으로 다시 이동합니다.
8. 전달 그룹을 선택하고 **배포**를 클릭합니다.
9. 사용자는 앱 설치 요청을 받고, 수락하면 앱이 백그라운드에서 설치됩니다.



Apple 볼륨 구매로 제공되는 공개 앱 스토어 앱

Apple 볼륨 구매 프로그램을 통해 iOS/iPadOS 앱 라이선스를 관리할 수 있습니다. XenMobile에 볼륨 구매 앱을 추가하려면 다음 단계를 따르십시오.

기능 가용성	
장치 감독 필요	아니요
사용자 등록 모드에서 사용 가능	예
사용 가능	iOS/iPadOS/macOS

1단계: 계정 연결

1. Apple Business Manager(ABM) 또는 Apple School Manager(ASM)에 설정하고 등록합니다. 이러한 프로그램에 대한 자세한 내용은 Apple 설명서를 참조하십시오.
2. ABM/ASM 계정을 XenMobile과 연결합니다. 볼륨 구매 계정 연결에 대한 자세한 내용은 Apple 볼륨 구매를 참조하십시오.
3. 볼륨 구매 계정을 추가할 때 **앱 자동 업데이트**를 활성화합니다. 이 설정을 통해 Apple Store에 업데이트가 나타나면 사용자 장치의 앱이 자동으로 업데이트됩니다.

2단계: Apple에서 앱 및 라이선스 가져오기

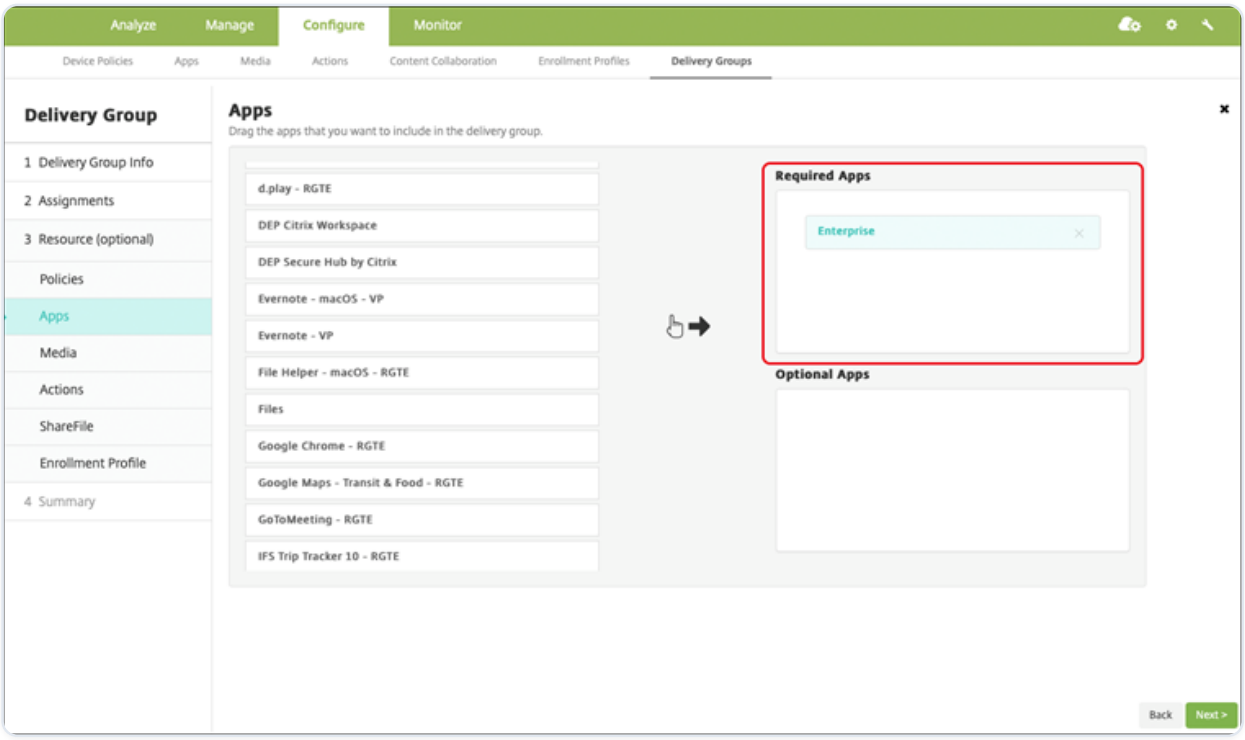
ABM/ASM 계정에 앱을 추가합니다. Apple App Store 또는 Apple Books(iOS/iPadOS만 해당)에서 구매 항목을 추가할 수 있습니다. 무료 앱이라도 모든 앱을 구매해야 한다는 점을 명심하십시오.

앱을 비즈니스에서 사용할 수 있도록 하는 방법에 대한 자세한 내용은 Apple 설명서를 참조하십시오.

3단계: 앱 배포 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다.
2. 구성하려는 볼륨 구매 앱을 선택하고 **편집**을 클릭합니다.
3. 플랫폼을 선택합니다: **iPhone**, **iPad** 또는 **macOS**.
4. Citrix는 **앱 관리 강제 적용** 기능(iOS/iPadOS만 해당)을 활성화할 것을 권장합니다.
5. 모든 전달 그룹을 할당하고 **저장**을 클릭합니다.
6. **구성 > 전달 그룹 > 앱**으로 이동합니다.

7. 원하는 앱을 **필수**로 표시합니다.



8. **구성 > 전달 그룹**으로 다시 이동합니다.
9. 전달 그룹을 선택하고 **배포**를 클릭합니다.
10. 사용자는 앱 설치 요청을 받으며, 수락하면 앱이 백그라운드에서 설치됩니다.



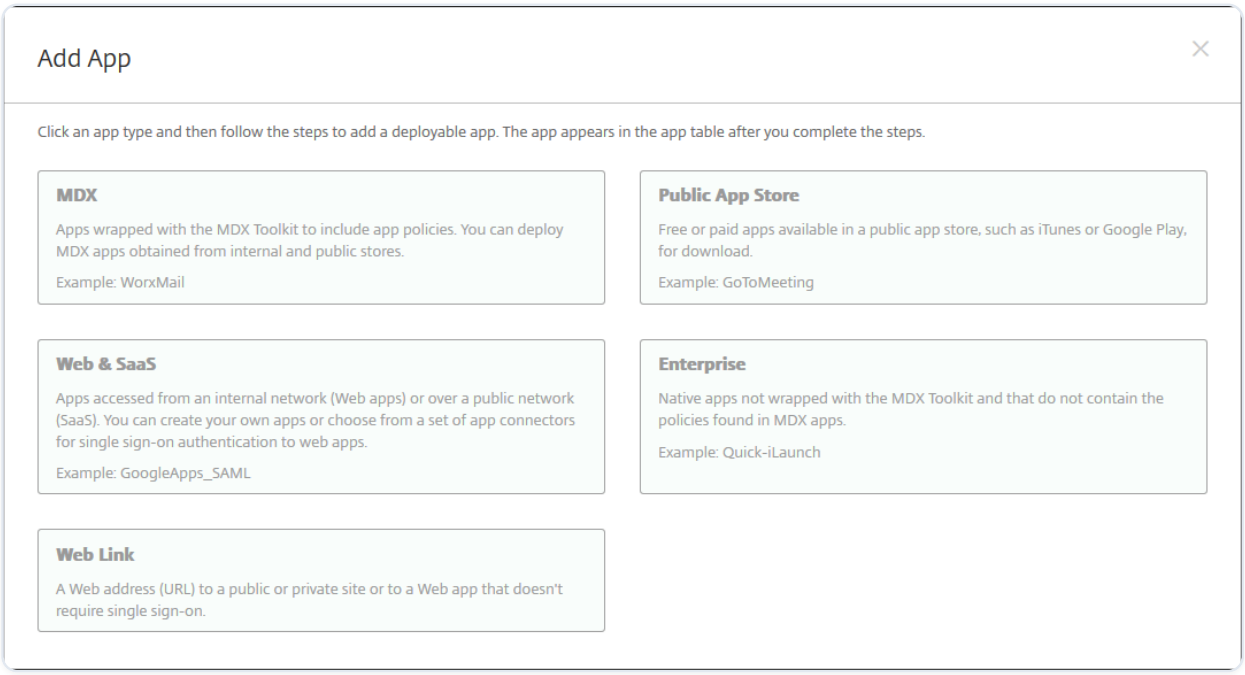
엔터프라이즈 앱

MDX 정책이 연결되지 않은 네이티브 앱도 추가할 수 있습니다. App Store에 없는 앱을 추가하려면 다음 단계를 따르십시오.

기능 가용성	
장치 감독 필요	아니요
사용자 등록 모드에서 사용 가능	예
OS	iOS/iPadOS/macOS

1단계: 앱 추가 및 구성

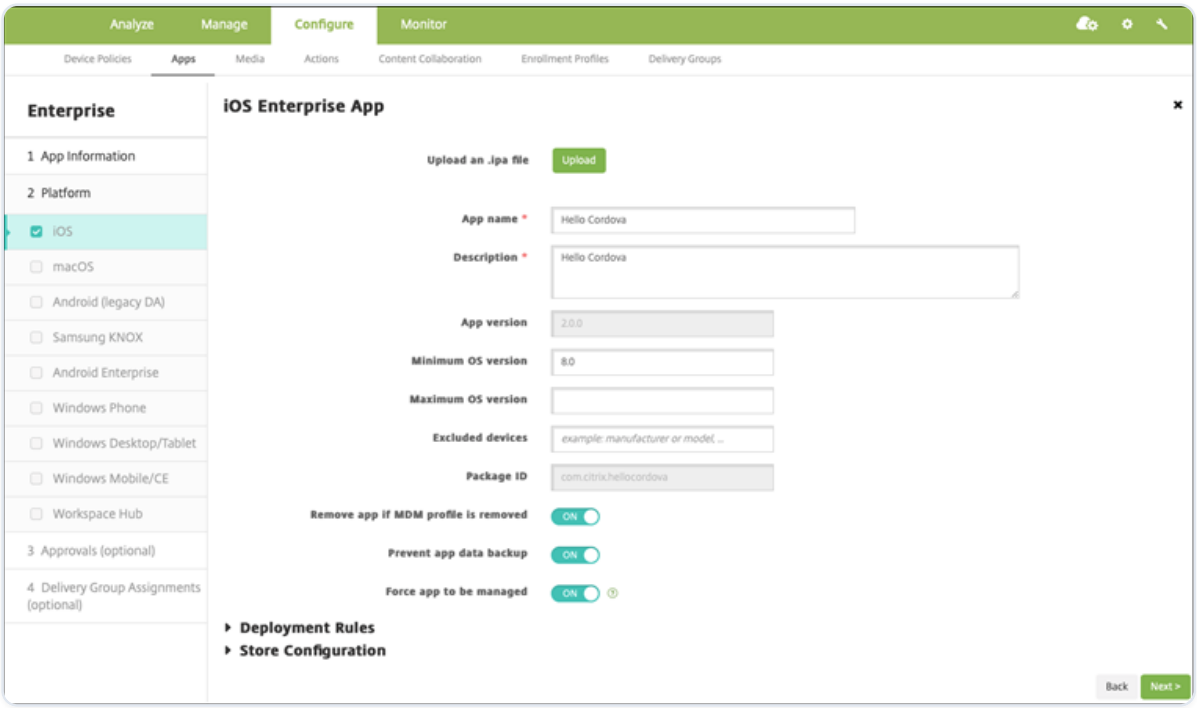
1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. **추가**를 클릭합니다.
2. **엔터프라이즈**를 클릭합니다.



3. **앱 정보** 페이지에서 다음을 구성합니다.
   - **이름:** 앱에 대한 설명이 포함된 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나타납니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.
   - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다.
4. **다음**을 클릭합니다. **앱 플랫폼** 페이지가 나타납니다.
5. 플랫폼을 선택합니다: **iPhone**, **iPad**, 또는 **macOS**.

6. IPA 파일(iOS/iPadOS) 또는 PKG 파일(macOS)을 업로드합니다.
7. **다음**을 클릭합니다. **앱 세부 정보** 페이지가 나타납니다.
8. 다음 설정을 구성합니다.

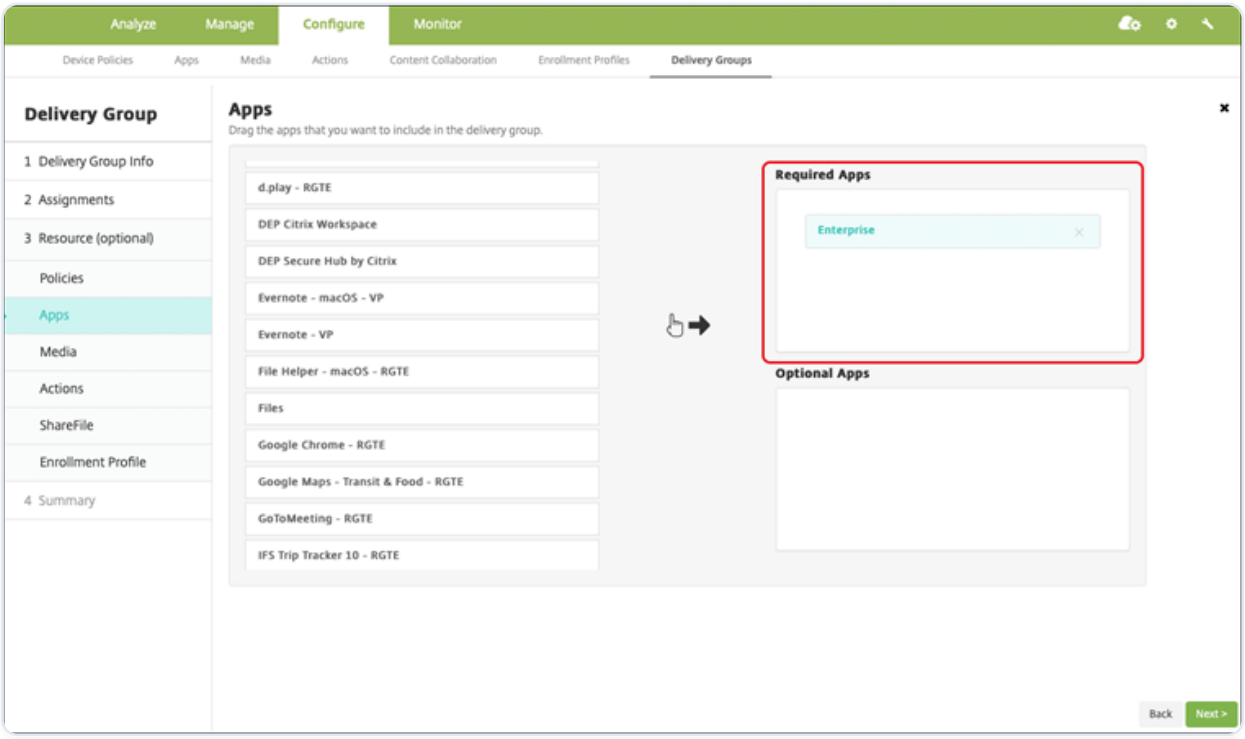
   - **파일 이름:** 선택적으로 앱의 새 이름을 입력합니다.
   - **앱 설명:** 선택적으로 앱의 새 설명을 입력합니다.
   - **앱 버전:** 이 필드는 변경할 수 없습니다.
   - **최소 OS 버전:** 선택적으로, 장치에서 앱을 실행하는 데 필요한 가장 오래된 운영 체제 버전을 입력합니다.
   - **최대 OS 버전:** 선택적으로, 장치에서 앱을 실행하는 데 필요한 가장 최신 운영 체제 버전을 입력합니다.
   - **제외된 장치:** 선택적으로, 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
   - **MDM 프로필 제거 시 앱 제거:** MDM 프로필이 제거될 때 장치에서 앱을 제거할지 여부를 선택합니다. 기본값은 켜짐입니다. (iOS/iPadOS만 해당)
   - **앱 데이터 백업 방지:** 앱이 데이터를 백업하지 못하도록 할지 여부를 선택합니다. 기본값은 켜짐입니다. (iOS/iPadOS만 해당)
   - **앱 관리 강제 적용:** 관리되지 않는 앱을 설치하는 경우, 감독되지 않는 장치의 사용자가 앱 관리를 허용하라는 메시지를 보게 하려면 **켜짐**을 선택합니다. 사용자가 메시지를 수락하면 앱이 관리됩니다. (iOS/iPadOS만 해당)



9. 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다.

2단계: 앱 배포 구성

1. XenMobile 콘솔에서 **구성 > 배달 그룹**으로 이동합니다. 구성할 배달 그룹을 선택하고 **앱** 페이지를 클릭합니다.
2. 원하는 앱을 **필수**로 표시합니다.



3. **구성 > 배달 그룹**으로 이동합니다.
4. 배달 그룹을 선택하고 **배포**를 클릭합니다.

5. 사용자는 앱 설치 요청을 받으며, 수락하면 앱이 백그라운드에서 설치됩니다.



MDX 앱

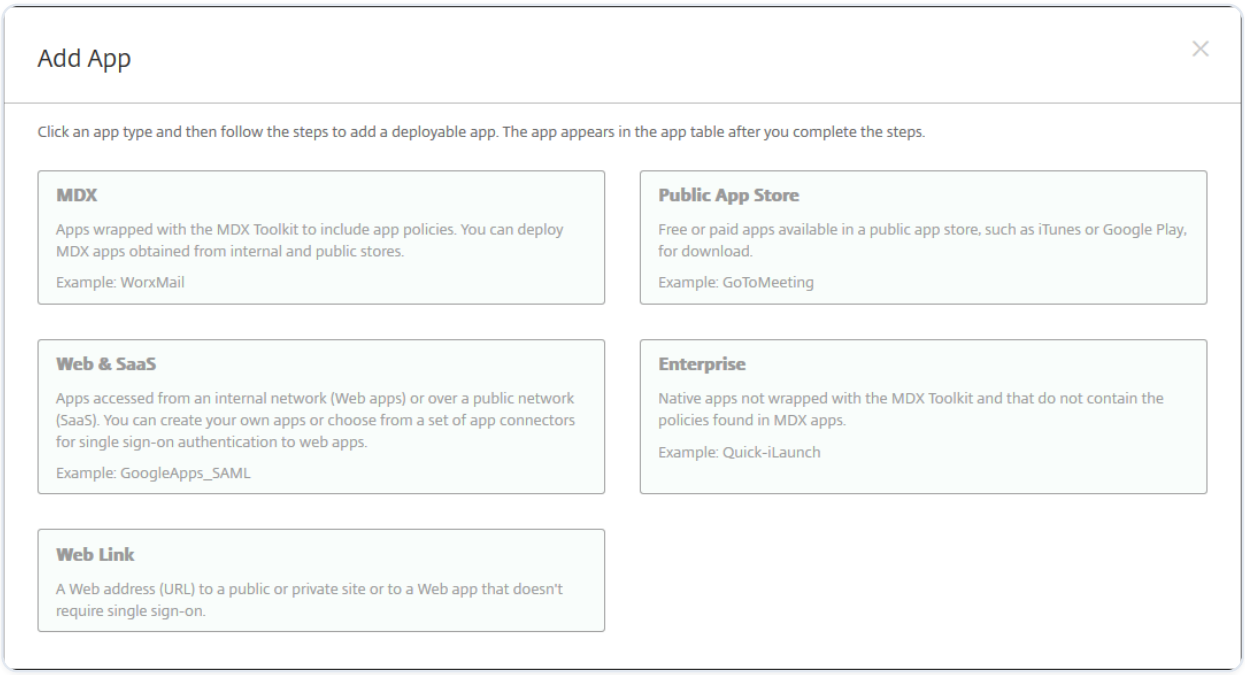
MDX 정책 및 보안 기능을 사용하려면 MAM SDK가 활성화되었거나 MDX로 래핑된 앱을 추가합니다. 볼륨 구매를 사용하거나 사용하지 않고 MDX 앱을 배포할 수 있습니다.

기능 가용성	
장치 감독 필요	아니요
사용자 등록 모드에서 사용 가능	예
사용 가능 플랫폼	iOS/iPadOS

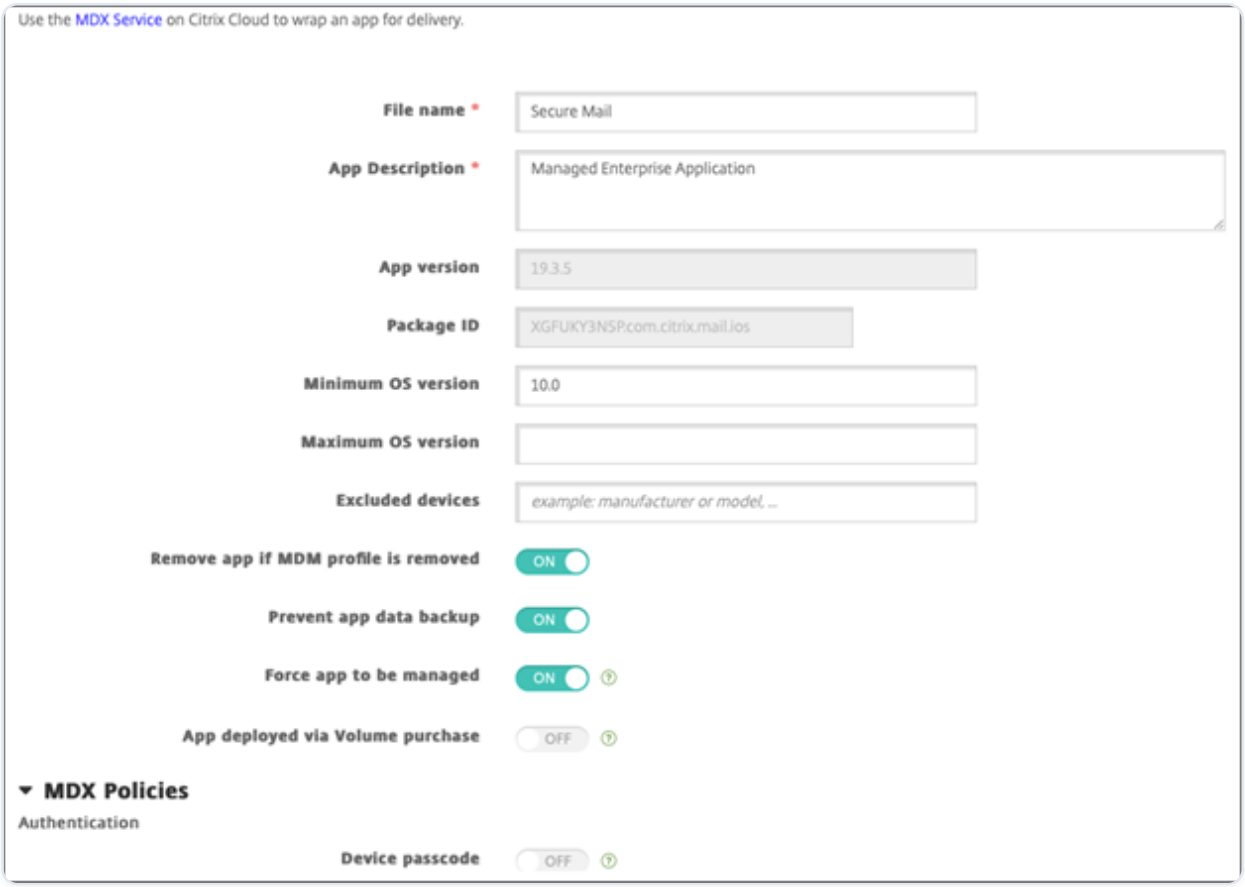
1단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. **추가**를 클릭합니다.

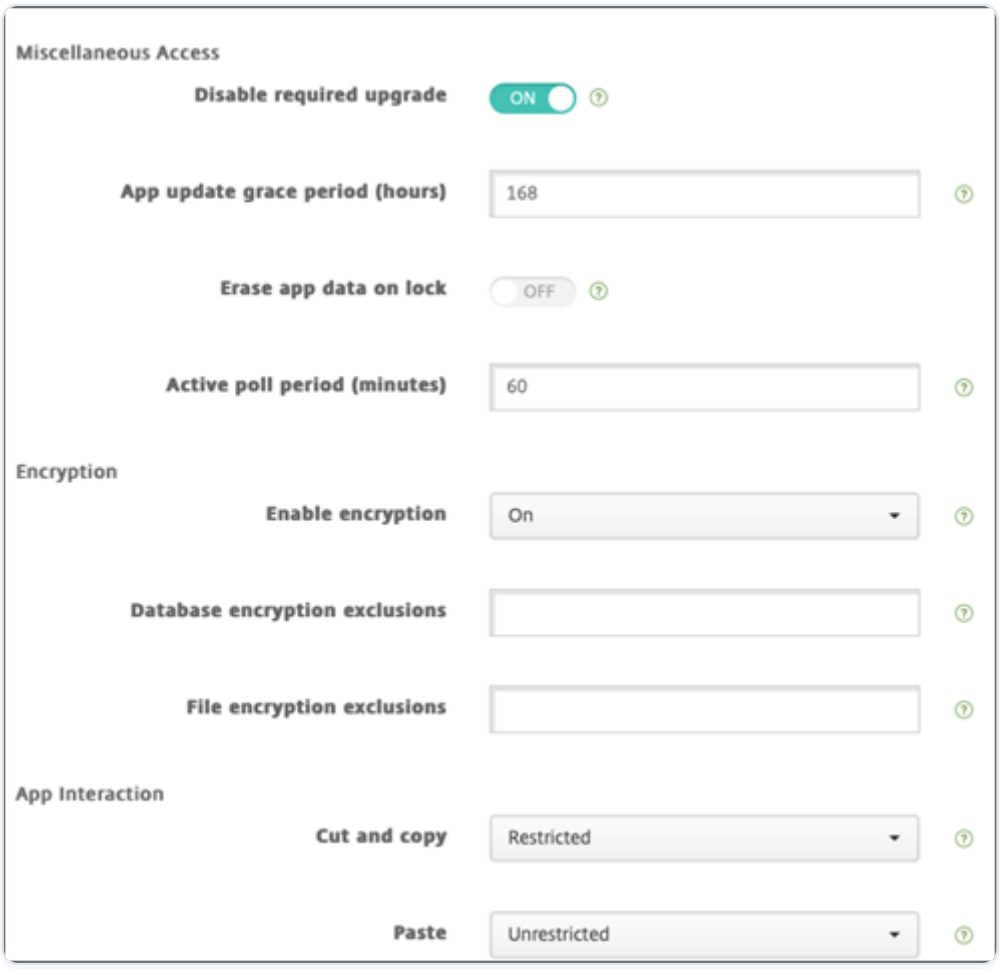
2. **MDX**를 클릭합니다.



3. 플랫폼으로 **iPhone** 또는 **iPad**를 선택합니다.
4. MDX 파일을 업로드합니다.
5. 앱 세부 정보를 구성합니다. **볼륨 구매를 통해 배포된 앱**을 **끄기**로 설정합니다. Citrix는 또한 **앱 관리 강제 적용** 기능을 활성화할 것을 권장합니다.



6. MDX 정책을 구성합니다. **필수 업그레이드 비활성화**를 **켜기**로 설정합니다.

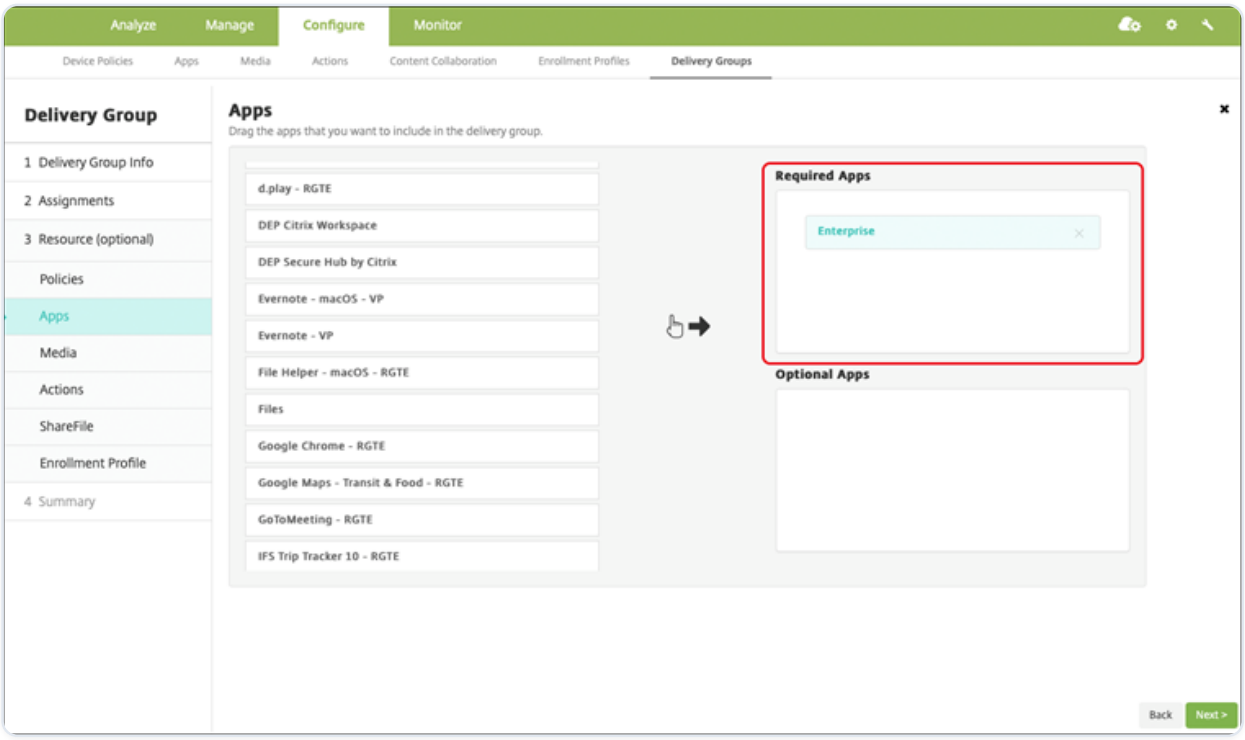


7. 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다.

2단계: 앱 배포 구성

1. XenMobile 콘솔에서 **구성 > 전달 그룹 > 앱**으로 이동합니다.

2. 원하는 앱을 **필수**로 표시합니다.



3. **구성 > 전달 그룹**으로 이동합니다.
4. 전달 그룹을 선택하고 **배포**를 클릭합니다.
5. 사용자는 앱 설치 요청을 받으며, 수락하면 앱이 백그라운드에서 설치됩니다.



Apple 볼륨 구매를 사용하여 배포된 MDX 앱

MDX 정책 및 보안 기능을 사용하려면 MAM SDK가 활성화되었거나 MDX로 래핑된 앱을 추가합니다. 볼륨 구매를 사용하여 앱을 배포하려면 앱이 앱 스토어에 있어야 합니다.

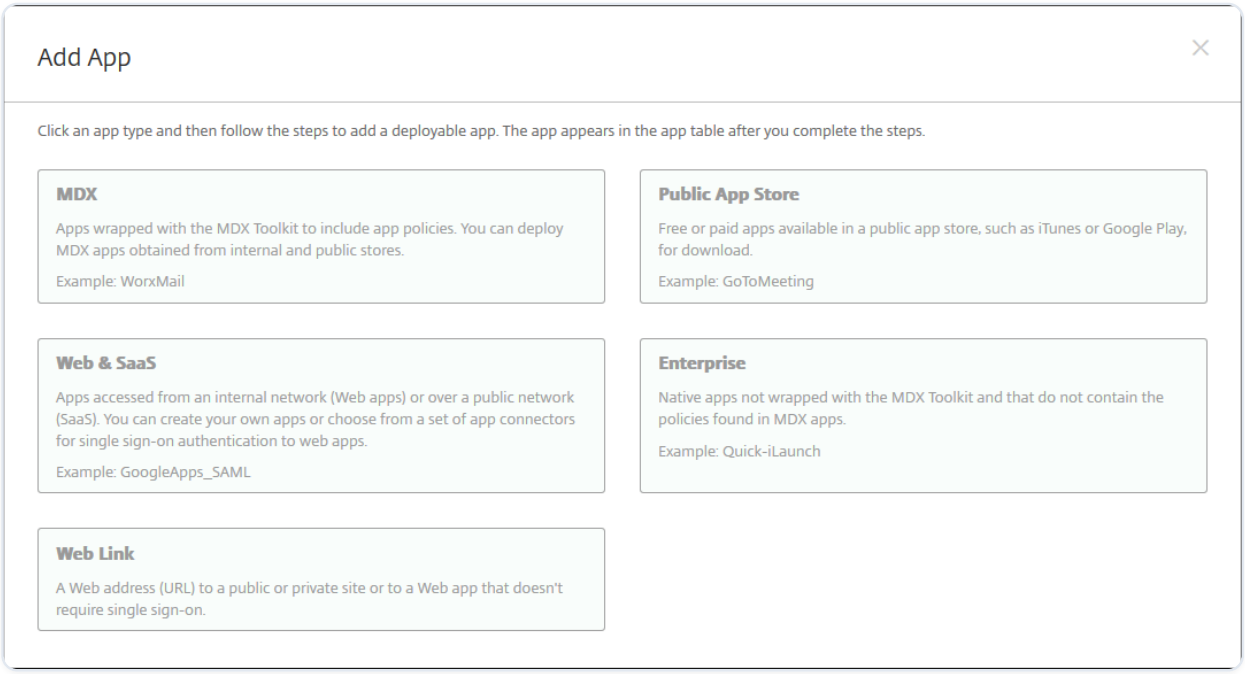
기능 가용성	
장치 감독 필요	아니요
사용자 등록 모드에서 사용 가능	예
사용 가능 플랫폼	iOS/iPadOS

1단계: 계정 연결

1. Apple Business Manager(ABM) 또는 Apple School Manager(ASM)를 설정하고 등록합니다. 이러한 프로그램에 대한 자세한 내용은 Apple 설명서를 참조하십시오.
2. ABM/ASM 계정을 XenMobile과 연결합니다. 볼륨 구매 계정 연결에 대한 자세한 내용은 Apple 볼륨 구매를 참조하십시오.
3. 볼륨 구매 계정을 추가할 때 **앱 자동 업데이트**를 활성화합니다. 이 설정은 Apple Store에 업데이트가 나타날 때 사용자 장치의 앱이 자동으로 업데이트되도록 합니다.

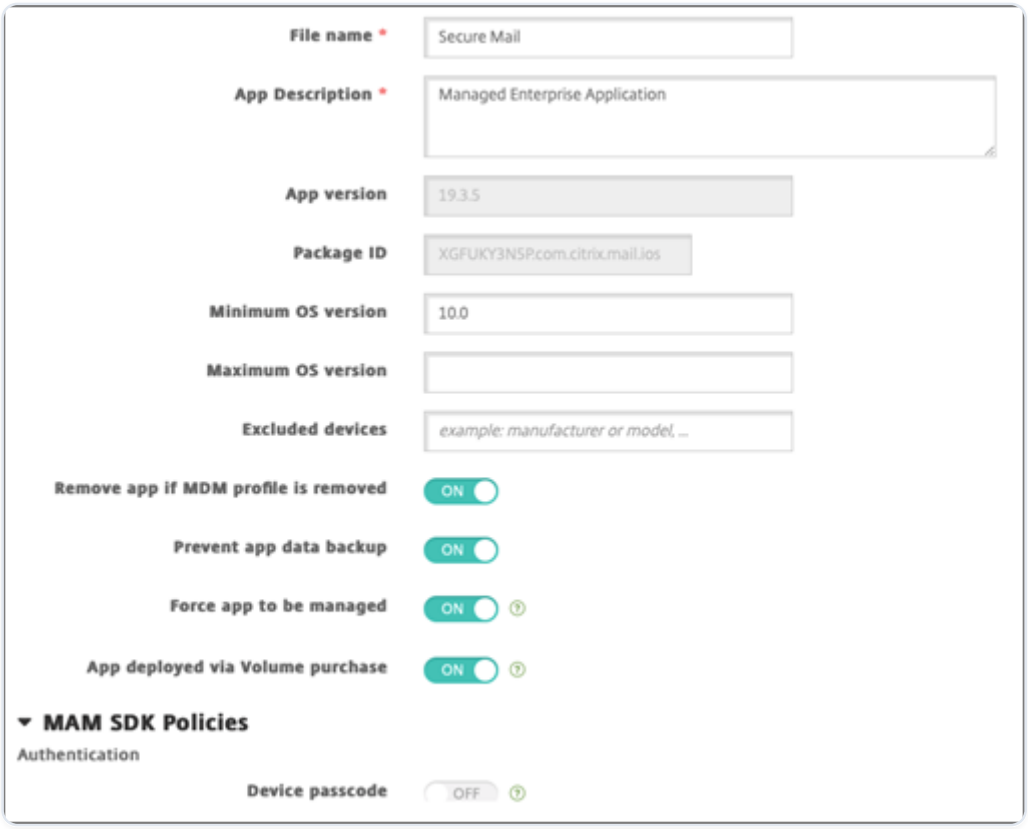
2단계: 앱 추가 및 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. **추가**를 클릭합니다.
2. **MDX**를 클릭합니다.

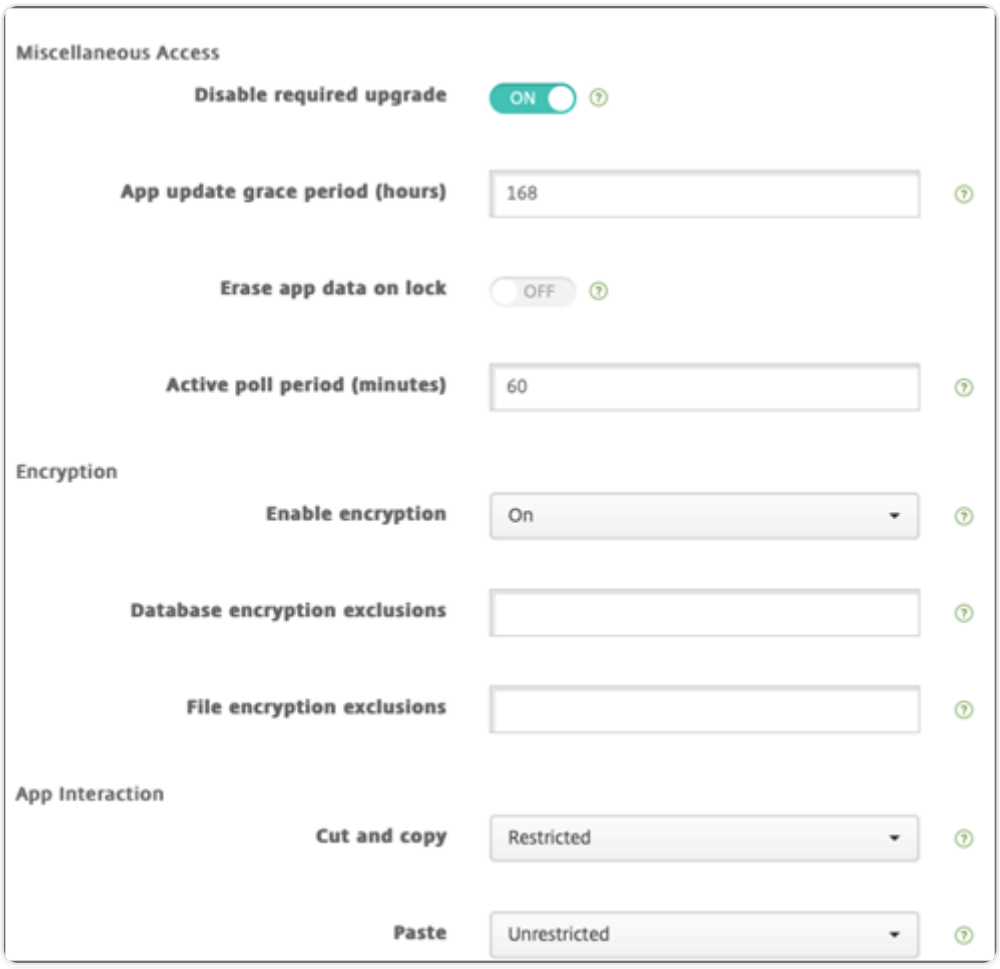


3. 플랫폼으로 **iPhone** 또는 **iPad**를 선택합니다.

4. MDX 파일을 업로드합니다.
5. 앱 세부 정보를 구성합니다. **볼륨 구매를 통해 배포된 앱**을 **켜기**로 설정합니다. Citrix는 또한 **앱 관리 강제 적용** 기능을 활성화할 것을 권장합니다.



6. MDX 정책을 구성합니다. **필수 업그레이드 비활성화**를 **켜기**로 설정합니다.



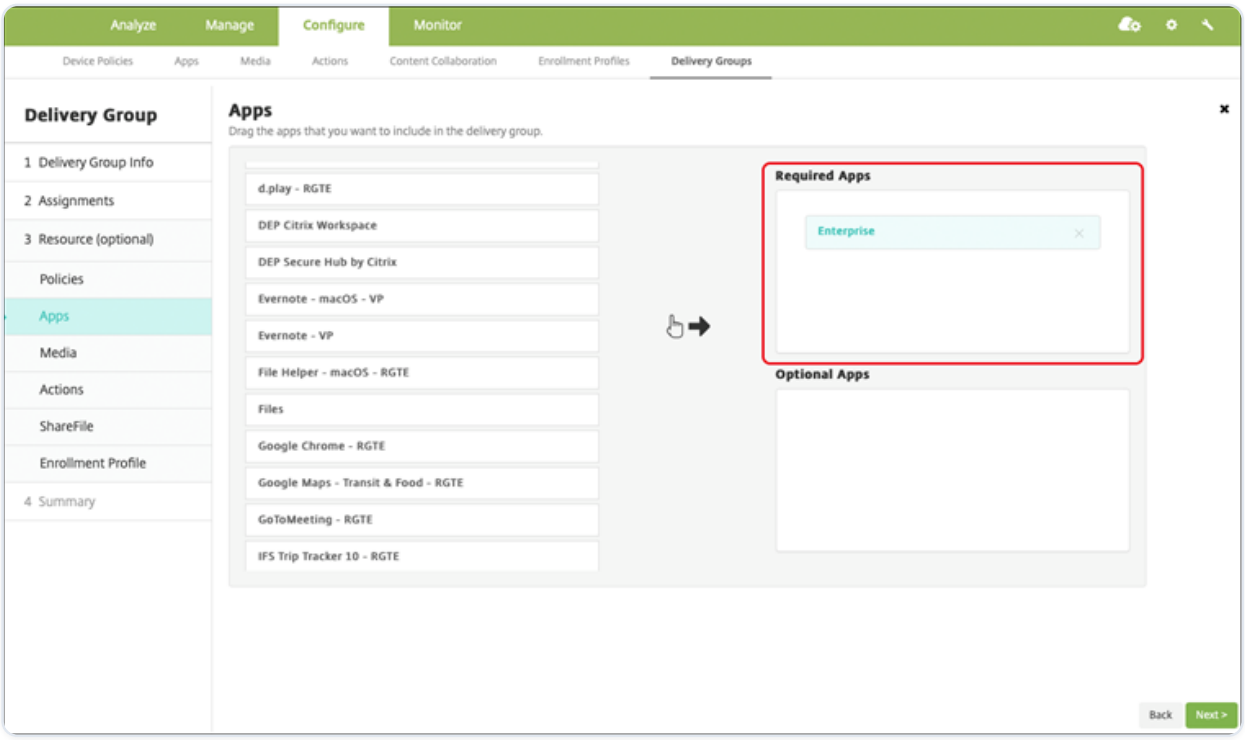
7. 각 플랫폼의 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다.

이 구성으로 인해 앱 목록에 이 앱에 대한 두 개의 항목이 나열됩니다. 구성할 앱을 선택할 때 **유형**이 **MDX**인 앱을 선택합니다.

3단계: 앱 배포 구성

1. XenMobile 콘솔에서 **구성 > 배달 그룹 > 앱**으로 이동합니다.

2. 원하는 볼륨 구매 앱을 **필수**로 표시합니다.



3. **구성 > 배달 그룹**으로 이동합니다.
4. 배달 그룹을 선택하고 **배포**를 클릭합니다.
5. 사용자가 앱 설치 요청을 받으면 수락 후 앱이 백그라운드에서 설치됩니다.



사용자 지정 앱

사용자 지정 앱은 독점적인 B2B(기업 간) 앱입니다. XenMobile 및 Apple 볼륨 구매를 사용하여 독점 앱을 비공개로 안전하게 배포할 수 있습니다. 특정 파트너, 클라이언트, 프랜차이즈 및 내부 직원에게 앱을 배포할 수 있습니다.

기능 가용성	
장치 감독 필요	아니요
사용자 등록 모드에서 사용 가능	예
사용 가능	iOS/iPadOS

사용자 지정 앱 요구 사항

- 애플 비즈니스 매니저 또는 애플 스쿨 매니저 계정
- Apple 볼륨 구매 계정(iOS 7 이상이 설치된 장치 필요)
- 다음 Apple 등록 모드 중 하나를 사용하여 XenMobile에 장치를 등록합니다.
  - 자동 장치 등록
  - 장치 등록
  - 사용자 등록

1단계: 계정 연결

볼륨 구매를 사용하여 사용자 지정 앱을 배포하려면 볼륨 구매 계정을 XenMobile에 연결합니다.

1. Apple Business Manager(ABM)를 설정하고 등록합니다. 이러한 프로그램에 대한 자세한 내용은 Apple 설명서를 참조하십시오.
2. ABM 계정을 XenMobile에 연결합니다. 볼륨 구매 계정 연결에 대한 자세한 내용은 Apple 볼륨 구매를 참조하십시오.
3. 볼륨 구매 계정을 추가할 때 **앱 자동 업데이트**를 활성화합니다. 이 설정을 통해 Apple Store에 업데이트가 나타나면 사용자 장치의 앱이 자동으로 업데이트됩니다.

2단계: ABM에서 앱 구성

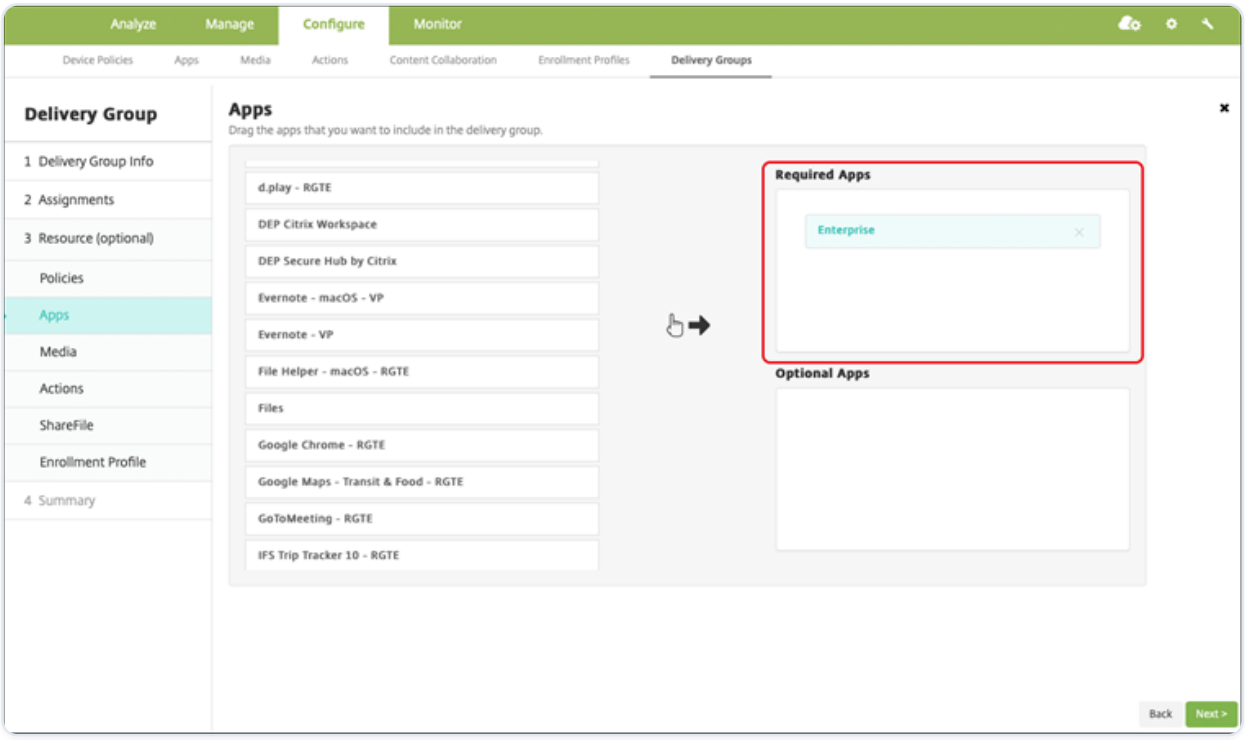
ABM 계정에 앱을 추가합니다. 사용자 지정 앱을 업로드 및 배포하거나 다른 조직에서 사용자 지정 앱 라이선스를 구매할 수 있습니다. ABM에서 사용자 지정 앱을 추가하고 활성화하는 방법에 대한 자세한 내용은 Apple 설명서를 참조하십시오.

3단계: XenMobile에서 앱 추가 및 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. 볼륨 구매 앱이 앱 목록에 나타납니다.
2. 구성할 앱을 선택합니다. **편집**을 클릭합니다.
3. 플랫폼을 선택합니다: **iPhone**, **iPad**, 또는 **macOS**.
4. 앱을 배포할 딜리버리 그룹을 선택합니다. **저장**을 클릭합니다.

4단계: 앱 배포 구성

1. XenMobile 콘솔에서 **구성 > 딜리버리 그룹 > 앱**으로 이동합니다.
2. 배포하려는 앱을 **필수**로 표시합니다.



3. **구성 > 딜리버리 그룹**으로 다시 이동합니다.
4. 배포하려는 딜리버리 그룹을 선택한 다음 **배포**를 클릭합니다.

5. 사용자는 앱 배포 요청을 받습니다. 사용자가 수락하면 앱이 백그라운드에서 설치됩니다.



MDX 지원 사용자 지정 앱

MDX 정책 및 보안 기능을 사용하려면 MAM SDK가 활성화되었거나 MDX로 래핑된 사용자 지정 앱을 추가합니다.

기능 가용성	
장치 감독 필요	아니요
사용자 등록 모드에서 사용 가능	예
사용 가능	iOS/iPadOS

1단계: 계정 연결

볼륨 구매를 사용하여 사용자 지정 앱을 배포하려면 볼륨 구매 계정을 XenMobile에 연결하십시오.

1. Apple Business Manager(ABM)를 설정하고 등록하십시오. 이러한 프로그램에 대한 자세한 내용은 Apple 설명서를 참조하십시오.
2. ABM 계정을 XenMobile에 연결하십시오. 볼륨 구매 계정 연결에 대한 자세한 내용은 Apple 볼륨 구매를 참조하십시오.

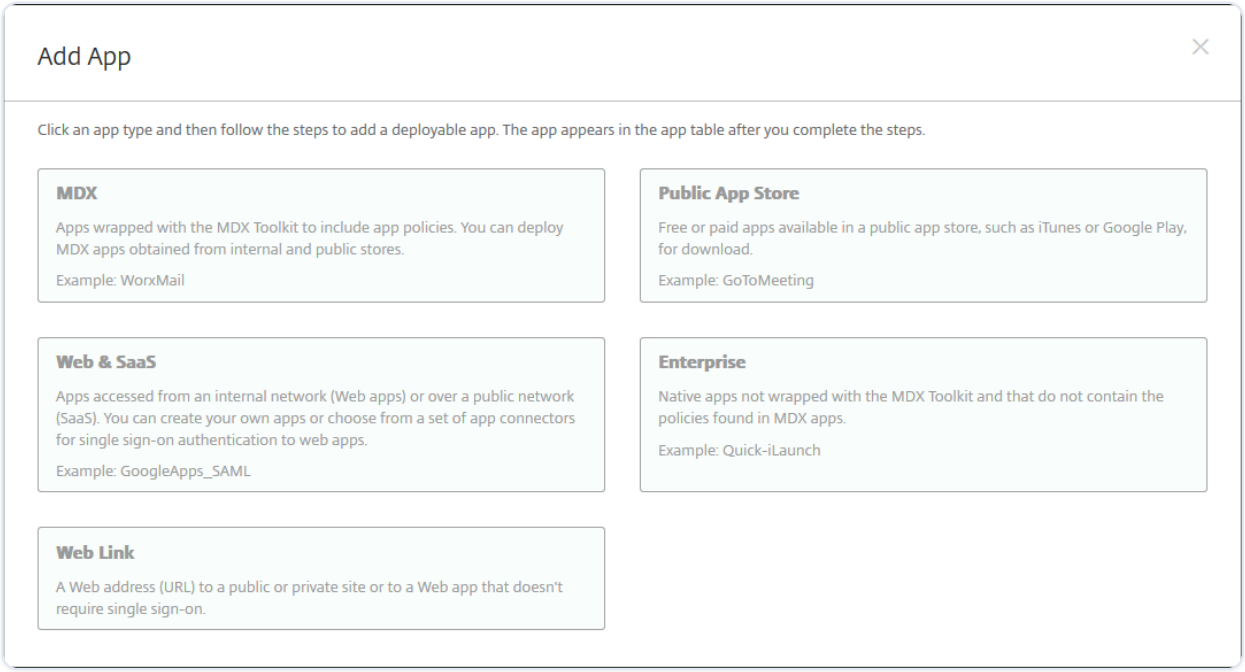
3. 볼륨 구매 계정을 추가할 때 **앱 자동 업데이트**를 활성화하십시오. 이 설정은 Apple Store에 업데이트가 나타날 때 사용자 장치의 앱이 자동으로 업데이트되도록 합니다.

2단계: ABM에서 앱 구성

ABM 계정에 앱을 추가하십시오. 자체 사용자 지정 앱을 업로드하고 배포하거나 다른 조직에서 사용자 지정 앱에 대한 라이선스를 구매할 수 있습니다. ABM에서 사용자 지정 앱을 추가하고 활성화하는 방법에 대한 자세한 내용은 Apple 설명서를 참조하십시오.

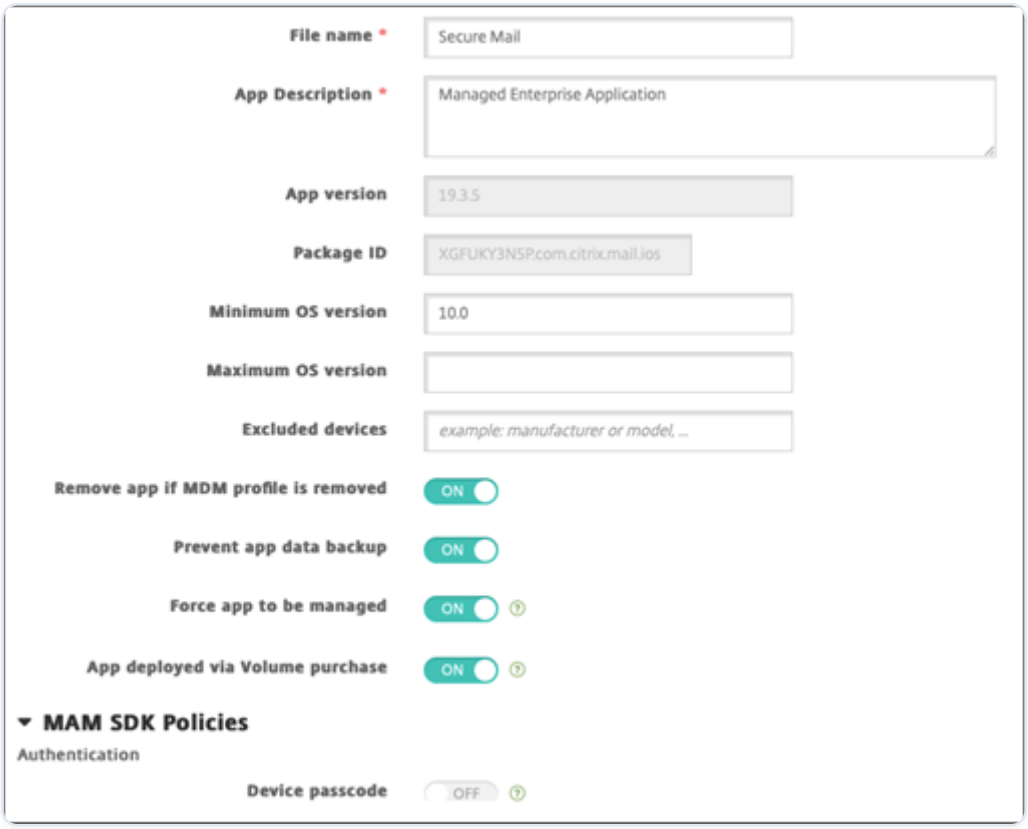
3단계: XenMobile에서 앱 추가 및 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. **추가**를 클릭합니다.
2. **MDX**를 클릭합니다.

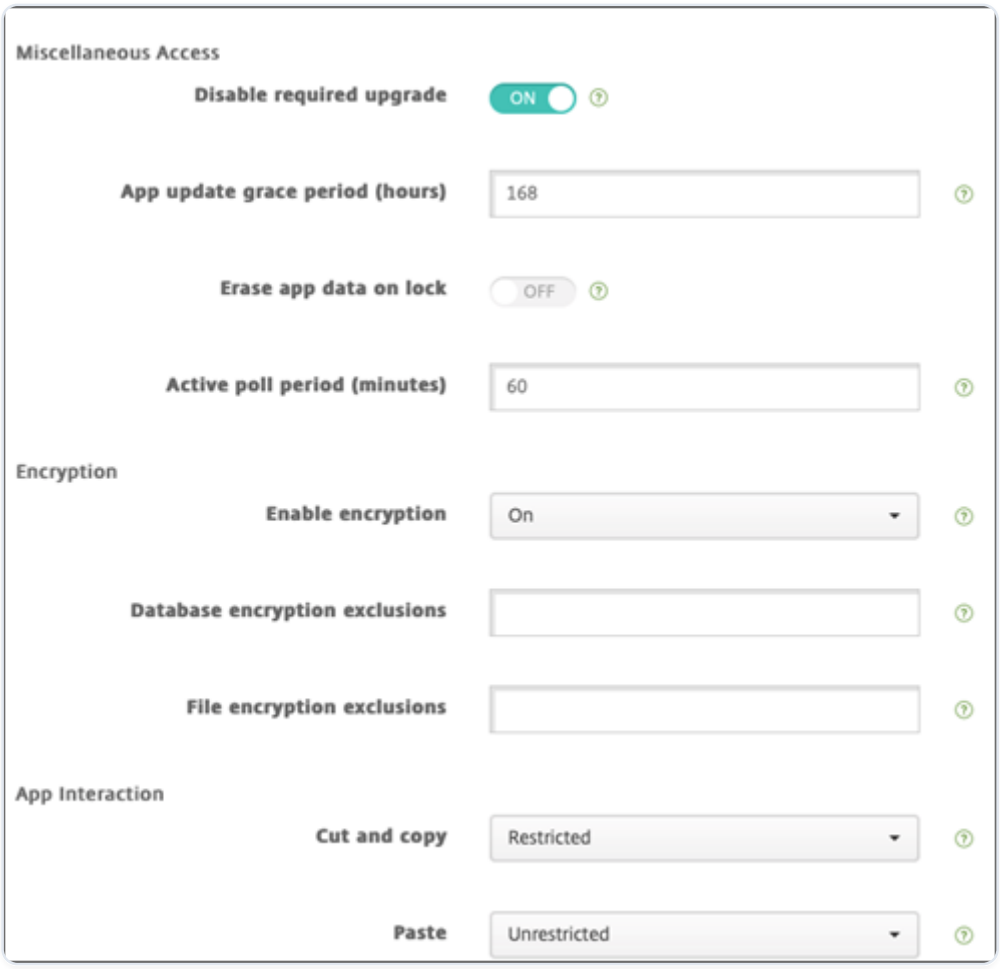


3. **iPhone** 또는 **iPad** 플랫폼을 선택합니다.
4. 추가하려는 앱의 MDX 파일을 업로드합니다.

5. 앱 세부 정보를 구성합니다. **볼륨 구매를 통해 배포된 앱**을 **켜기**로 설정합니다. Citrix는 또한 **앱 관리 강제 적용** 기능을 활성화할 것을 권장합니다.



6. MDX 정책을 구성합니다. **필수 업그레이드 비활성화**를 **켜기**로 설정합니다.



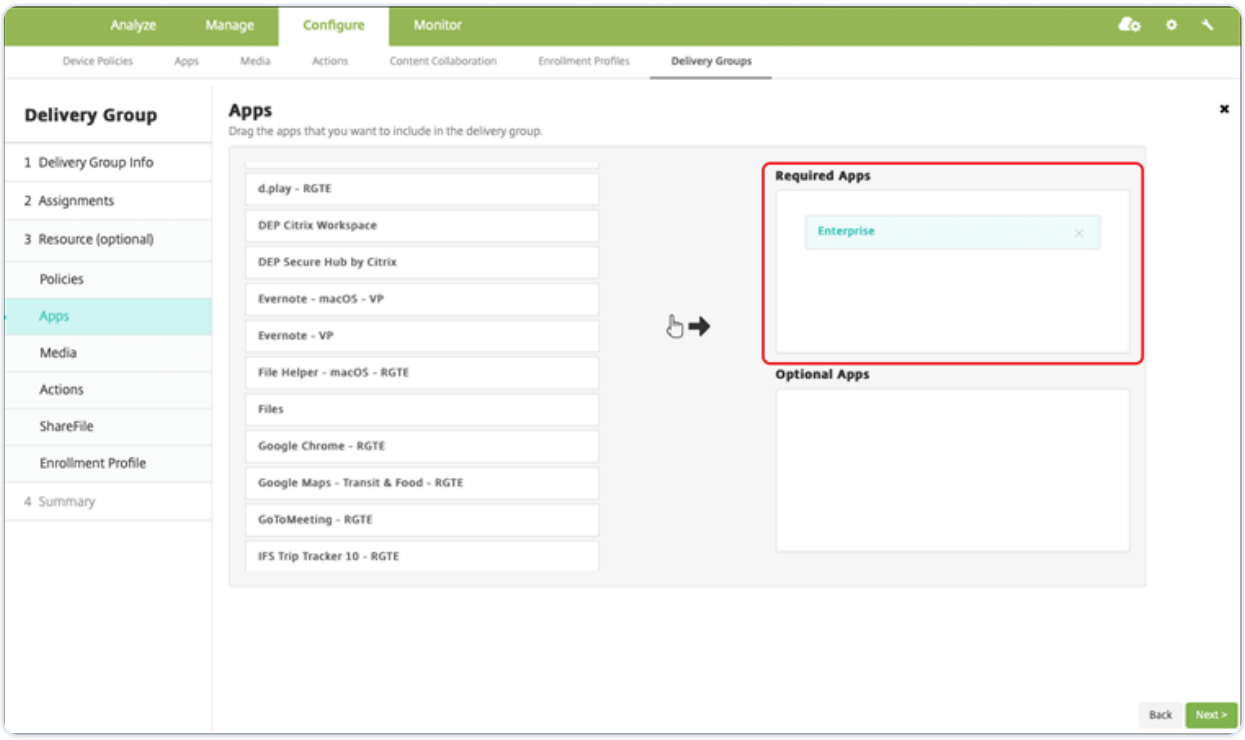
7. 앱에 배달 그룹을 할당하고 **저장**을 클릭합니다.

이 구성으로 인해 앱 목록에 이 앱에 대한 두 개의 항목이 표시됩니다. 앱을 구성하기 위해 선택할 때, **유형**이 **MDX**인 앱을 선택합니다.

4단계: 앱 배포 구성

1. XenMobile 콘솔에서 **구성 > 앱**으로 이동합니다. 볼륨 구매 앱이 앱 목록에 나타납니다.
2. 구성하려는 앱을 선택합니다. **편집**을 클릭합니다.
3. 각 플랫폼에서 앱을 배포할 배달 그룹을 선택합니다. **저장**을 클릭합니다.
4. **구성 > 배달 그룹 > 앱**으로 다시 이동합니다.

5. 배포하려는 앱을 **필수**로 표시합니다.



6. **구성 > 배달 그룹**으로 다시 이동합니다.
7. 배포하려는 배달 그룹을 선택하고 **배포**를 클릭합니다.
8. 사용자는 앱 배포 요청을 받습니다. 수락하면 앱이 백그라운드에서 설치됩니다.

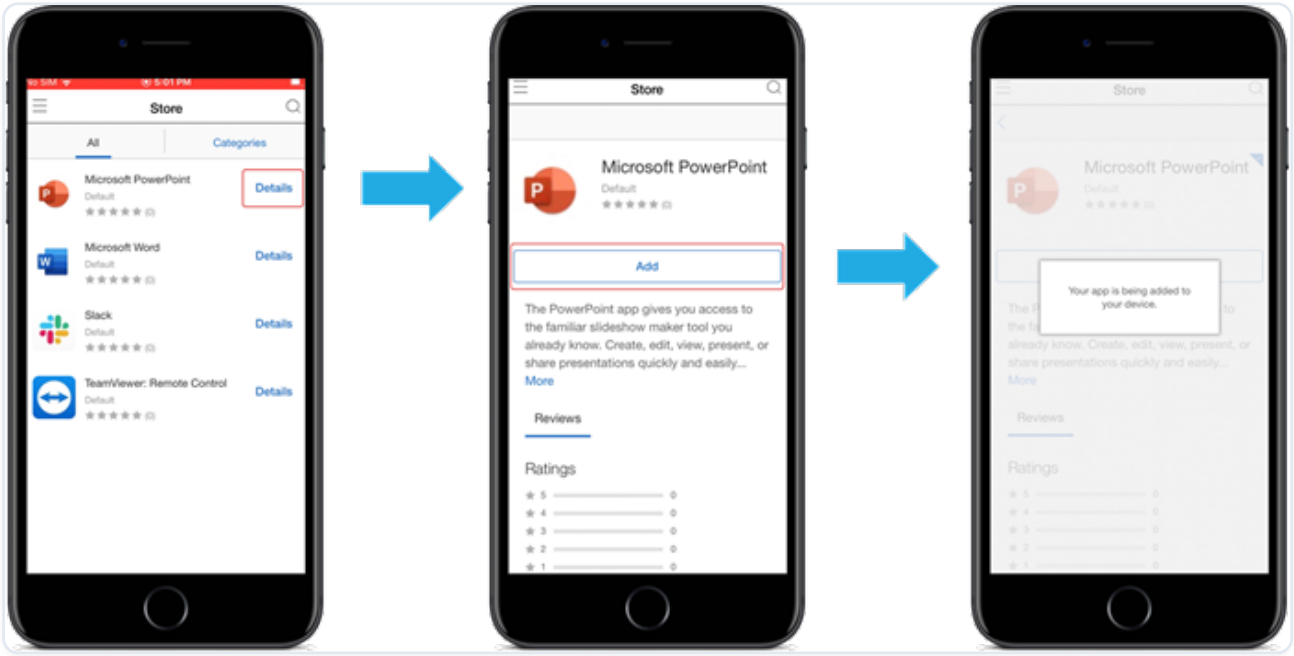


선택적 앱(iOS/iPadOS만 해당)

Citrix는 앱을 **필수**로 배포하는 것을 권장합니다. 필수 앱은 사용자 장치에 자동으로 설치되어 상호 작용을 최소화합니다. 이 기능을 활성화하면 앱이 자동으로 업데이트될 수도 있습니다.

선택적 앱을 사용하면 사용자가 설치할 앱을 선택할 수 있지만, 사용자는 Secure Hub를 통해 수동으로 설치를 시작해야 합니다.

선택적 앱을 설치하려면 사용자는 Secure Hub를 실행하고, **스토어**로 이동하여 원하는 앱의 **세부 정보**를 선택한 다음 **추가**를 클릭해야 합니다.



네트워크 액세스 제어

NAC(네트워크 액세스 제어) 솔루션을 사용하여 Android 및 Apple 장치에 대한 XenMobile® 장치 보안 평가를 확장할 수 있습니다. NAC 솔루션은 XenMobile 보안 평가를 사용하여 인증 결정을 용이하게 하고 처리합니다. NAC 어플라이언스를 구성한 후 XenMobile에서 구성한 장치 정책 및 NAC 필터가 적용됩니다.

NAC 솔루션과 함께 XenMobile을 사용하면 QoS 및 네트워크 내 장치에 대한 보다 세분화된 제어가 추가됩니다. NAC를 XenMobile과 통합할 때의 이점에 대한 요약은 (/ko-kr/xenmobile/server/advanced-concepts/xenmobile-deployment/integration.html#access-control)을(를) 참조하십시오.

Citrix®는 XenMobile과의 통합을 위해 다음 솔루션을 지원합니다.

- 시트릭스 게이트웨이
- 시스코 아이덴티티 서비스 엔진 (ISE)
- ForeScout

Citrix는 다른 NAC 솔루션과의 통합을 보장하지 않습니다.

네트워크에 NAC 어플라이언스가 있는 경우:

- XenMobile은 iOS, Android Enterprise 및 Android 장치에 대한 엔드포인트 보안 기능으로 NAC를 지원합니다.
- XenMobile에서 필터를 활성화하여 규칙 또는 속성을 기반으로 장치를 NAC에 대해 규정 준수 또는 비규정 준수로 설정할 수 있습니다. 예를 들면 다음과 같습니다.
    - XenMobile에서 관리되는 장치가 지정된 기준을 충족하지 않으면 XenMobile은 해당 장치를 비규정 준수로 표시합니다. NAC 어플라이언스는 네트워크에서 비규정 준수 장치를 차단합니다.
    - XenMobile에서 관리되는 장치에 비규정 준수 앱이 설치되어 있는 경우 NAC 필터가 VPN 연결을 차단할 수 있습니다. 결과적으로 비규정 준수 사용자 장치는 VPN을 통해 앱 또는 웹사이트에 액세스할 수 없습니다.
    - NAC에 Citrix Gateway를 사용하는 경우, Citrix Gateway 플러그인이 불필요한 네트워크 트래픽을 Citrix Gateway로 보내는 것을 방지하기 위해 분할 터널링을 활성화할 수 있습니다. 분할 터널링에 대한 자세한 내용은 (/ko-kr/citrix-gateway/13/vpn-user-config/configure-plugin-connections/ng-plugin-split-tunneling-tsk.html)을(를) 참조하십시오.

지원되는 NAC 규정 준수 필터

XenMobile Server는 다음 NAC 규정 준수 필터를 지원합니다.

익명 장치: 장치가 익명 모드인지 확인합니다. 이 검사는 장치가 다시 연결을 시도할 때 XenMobile이 사용자를 다시 인증할 수 없는 경우에 사용할 수 있습니다.

실패한 Samsung Knox 증명: 장치가 Samsung Knox 증명 서버에 대한 쿼리에 실패했는지 확인합니다.

금지된 앱: 앱 액세스 장치 정책에 정의된 대로 장치에 금지된 앱이 있는지 확인합니다. 해당 정책에 대한 자세한 내용은 앱 액세스 장치 정책을 참조하십시오.

비활성 장치: 서버 속성의 **장치 비활성 일수 임계값** 설정에 정의된 대로 장치가 비활성 상태인지 확인합니다. 자세한 내용은 서버 속성을 참조하십시오.

누락된 필수 앱: 앱 액세스 정책에 정의된 대로 장치에 누락된 필수 앱이 있는지 확인합니다.

권장되지 않는 앱: 앱 액세스 정책에 정의된 대로 장치에 권장되지 않는 앱이 있는지 확인합니다.

비준수 암호: 사용자 암호가 규정을 준수하는지 확인합니다. iOS 및 Android 장치에서 XenMobile은 현재 장치에 있는 암호가 장치로 전송된 암호 정책을 준수하는지 확인할 수 있습니다. 예를 들어, iOS에서

XenMobile이 장치로 암호 정책을 전송하면 사용자는 60분 이내에 암호를 설정해야 합니다. 사용자가 암호를 설정하기 전에는 암호가 비준수 상태일 수 있습니다.

규정 미준수 장치: 규정 미준수 장치 속성을 기반으로 장치가 규정을 준수하지 않는지 확인합니다. 일반적으로 자동화된 작업 또는 XenMobile API를 사용하는 타사에서 해당 장치 속성을 변경합니다.

해지된 상태: 장치 인증서가 해지되었는지 확인합니다. 해지된 장치는 다시 승인될 때까지 재등록할 수 없습니다.

루팅된 Android 및 탈옥된 iOS 장치: Android 또는 iOS 장치가 탈옥되었는지 확인합니다.

관리되지 않는 장치: 장치가 XenMobile 제어 하에 관리되는 상태인지 확인합니다. 예를 들어, MAM에 등록된 장치 또는 등록되지 않은 장치는 관리되지 않습니다.

> **참고:**
>
> 암시적 준수/비준수 필터는 XenMobile이 관리하는 장치에만 기본값을 설정합니다. 예를 들어, 차단된 앱이 설치되어 있거나 등록되지 않은 모든 장치는 비준수로 표시됩니다. NAC 어플라이언스는 해당 장치를 네트워크에서 차단합니다.

구성 개요

NAC 구성 요소를 나열된 순서대로 구성하는 것이 좋습니다.

1. NAC를 지원하도록 장치 정책 구성:

   iOS 장치의 경우: 을 참조하십시오(/ko-kr/xenmobile/server/policies/vpn-policy.html#configure-the-vpn-device-policy-to-support-nac).

   Android Enterprise 장치의 경우: 을 참조하십시오(/ko-kr/xenmobile/server/policies/managed-configurations-policy.html#create-an-android-enterprise-managed-configuration-for-citrix-sso).

   Android 장치의 경우: 을 참조하십시오(/ko-kr/xenmobile/server/policies/vpn-policy.html#configure-the-citrix-sso-protocol-for-android).
2. XenMobile에서 NAC 필터 사용.
3. NAC 솔루션 구성:

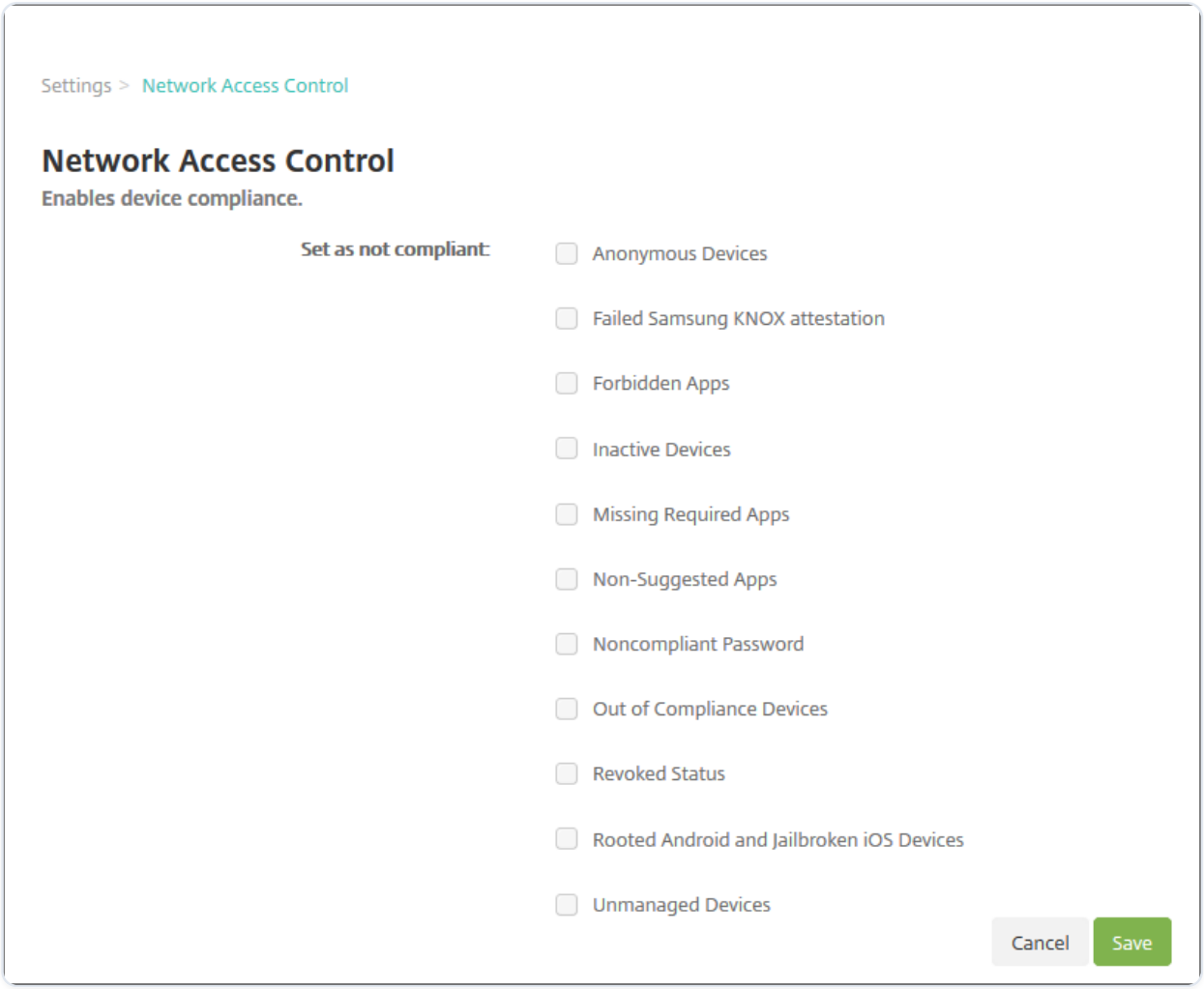
   - Citrix Gateway, 에 자세히 설명되어 있습니다(#update-citrix-gateway-policies-to-support-nac).

     장치에 Citrix SSO를 설치해야 합니다. 를 참조하십시오(/ko-kr/citrix-gateway/citrix-gateway-clients.html).

- Cisco ISE: Cisco 설명서를 참조하십시오.
- ForeScout: ForeScout 설명서를 참조하십시오.

XenMobile에서 NAC 필터 사용

1. XenMobile 콘솔에서 **설정 > 네트워크 액세스 제어**로 이동합니다.



2. 사용하려는 **비규격으로 설정** 필터의 확인란을 선택합니다.
3. **저장**을 클릭합니다.

NAC를 지원하도록 Citrix Gateway 정책 업데이트

VPN 가상 서버에서 고급(기존 방식 아님) 인증 및 VPN 세션 정책을 구성해야 합니다.

다음 단계는 다음 특성 중 하나를 가진 Citrix Gateway를 업데이트합니다.

- XenMobile Server 환경과 통합되어 있습니다.
- 또는 VPN용으로 설정되어 있고, XenMobile Server 환경의 일부가 아니며, XenMobile에 연결할 수 있습니다.

콘솔 창에서 가상 VPN 서버에 대해 다음을 수행합니다. 명령 및 예제의 IP 주소는 가상의 것입니다.

1. VPN 가상 서버에서 기존 정책을 사용하는 경우, 모든 기존 정책을 제거하고 바인딩을 해제합니다. 확인하려면 다음을 입력합니다.

   ```
   show vpn vserver <VPN_VServer>
   ```

   Classic이라는 단어가 포함된 결과를 제거합니다. 예: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   정책을 제거하려면 다음을 입력합니다.

   ```
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. 해당 고급 세션 정책을 생성하려면 다음을 입력합니다.

   ```
   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 vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
   ```

4. 다음을 입력하여 인증 가상 서버를 생성합니다.

   ```
   add authentication vserver <authentication vserver name> <service type> <ip address>
   ```

   예시: `add authentication vserver authvs SSL 0.0.0.0` 예시에서 `0.0.0.0`는 인증 가상 서버가 외부에 노출되지 않음을 의미합니다.

5. 다음을 입력하여 가상 서버에 SSL 인증서를 바인딩합니다.

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>
   ```

   예시: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. VPN 가상 서버에서 인증 가상 서버에 인증 프로필을 연결합니다. 먼저, 다음을 입력하여 인증 프로필을 생성합니다.

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication vserver name>
   ```

   예시:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. 다음을 입력하여 인증 프로필을 VPN 가상 서버에 연결합니다.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   예시:

   ```
   set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. 다음 내용을 입력하여 Citrix Gateway에서 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, 이 쿼리는 환경에 등록된 첫 번째 장치(`deviceid_1`)의 규정 준수 상태를 가져와 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 예와 유사합니다.

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. 이전 단계가 성공하면 XenMobile에 대한 웹 인증 작업을 생성합니다. 먼저 iOS VPN 플러그인에서 장치 ID를 추출하는 정책 표현식을 생성합니다. 다음을 입력합니다.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\', \'&\').VALUE(\"deviceidvalue\")"
   ```

10. 다음을 입력하여 XenMobile에 요청을 보냅니다. 이 예에서 XenMobile Server IP는 `10.207.87.82`이고 FQDN은 `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 -successRule "HTTP.RES.STATUS.EQ(\"200\") &&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"`

XenMobile NAC의 성공적인 출력은 `HTTP status 200 OK` 입니다. `X-Citrix-Device-State` 헤더는 `Compliant` 값을 가져야 합니다.

11. 다음을 입력하여 해당 작업을 연결할 인증 정책을 생성합니다.

    `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. 다음 내용을 입력하여 LDAP 정책을 연결할 정책 레이블을 추가합니다.

    `add authentication policylabel <policy_label_name>`

    예: `add authentication policylabel ldap_pol_label`

14. 다음 내용을 입력하여 LDAP 정책을 정책 레이블에 연결합니다.

    `bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT`

15. 규격 장치를 연결하여 NAC 테스트를 수행하고 LDAP 인증이 성공했는지 확인합니다. 다음 내용을 입력합니다.

    `bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END`

16. 인증 가상 서버와 연결할 UI를 추가합니다. 다음 명령을 입력하여 장치 ID를 검색합니다.

    `add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid`

17. 다음 내용을 입력하여 인증 가상 서버를 바인딩합니다.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100
-gotoPriorityExpression END
```

18. Secure Hub 연결을 활성화하기 위해 LDAP 고급 인증 정책을 생성합니다. 다음 내용을 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
```

삼성 녹스

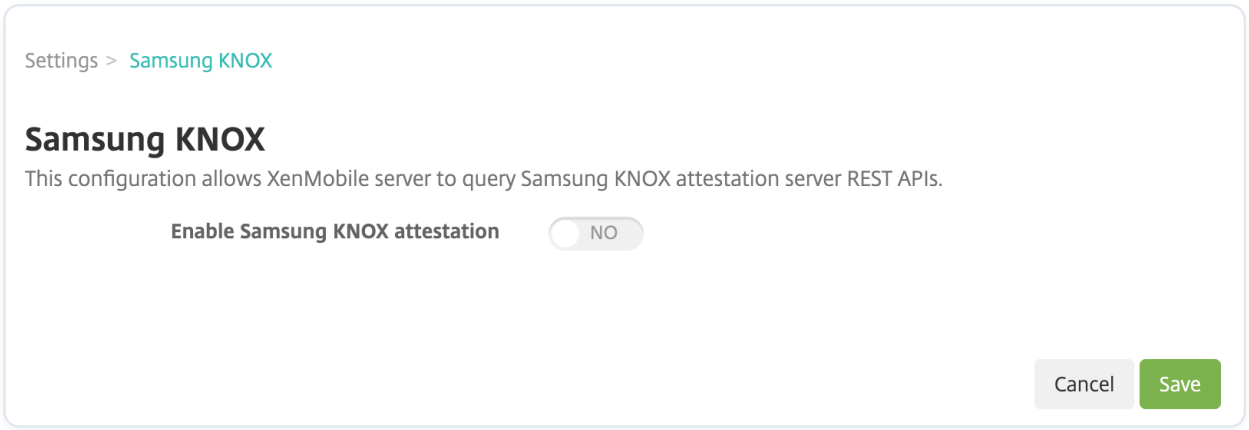
Samsung은 XenMobile® Server와 호환되는 여러 솔루션을 제공합니다.

- XenMobile은 호환되는 Samsung 장치에서 Samsung Knox 정책을 지원하고 확장합니다.
- Knox Service 플러그인(KSP)은 Knox Platform for Enterprise(KPE) 기능의 하위 집합을 지원하는 앱입니다. KPE에 대한 Samsung의 정보는 Knox Platform for Enterprise 구성 및 개요를 참조하십시오.

XenMobile이 Samsung Knox 증명 서버 REST API를 쿼리하도록 구성할 수 있습니다.

Samsung Knox는 운영 체제 및 애플리케이션에 여러 수준의 보호를 제공하는 하드웨어 보안 기능을 사용합니다. 이 보안의 한 수준은 증명을 통한 플랫폼에 있습니다. 증명 서버는 모바일 장치 코어 시스템 소프트웨어(예: 부트로더 및 커널)의 확인을 제공합니다. 확인은 신뢰할 수 있는 부팅 중에 수집된 데이터를 기반으로 런타임에 발생합니다.

1. XenMobile 웹 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **플랫폼**에서 **Samsung KNOX**를 클릭합니다. **Samsung KNOX** 페이지가 나타납니다.



3. **Samsung KNOX 증명 사용**에서 Samsung Knox 증명을 사용할지 여부를 선택합니다. 기본값은 **아니요**입니다.
4. **저장**을 클릭합니다.

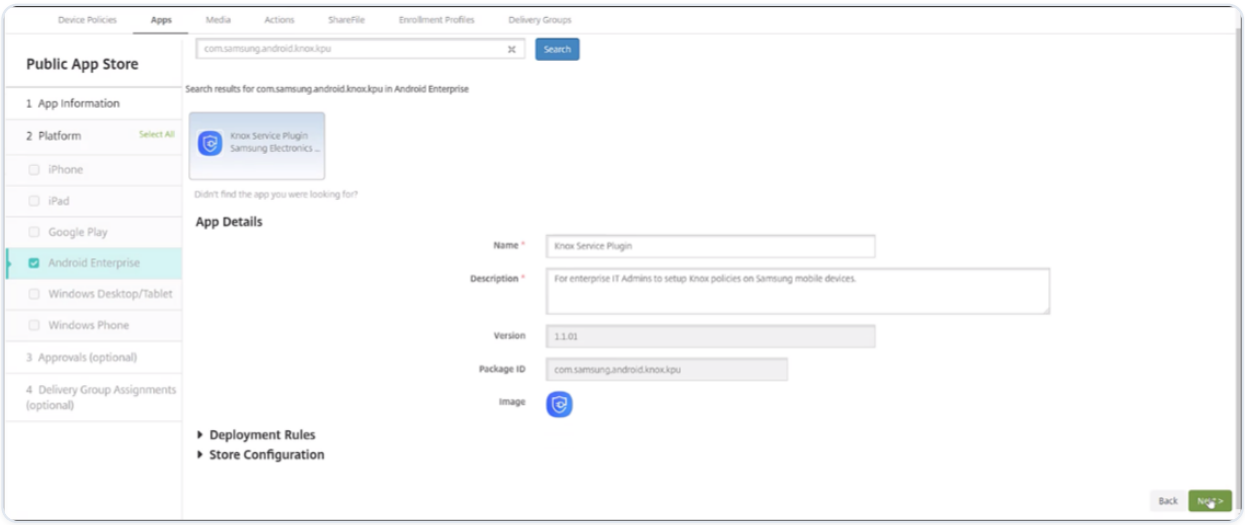
> **참고:**
>
> Samsung Knox Mobile Enrollment를 사용하여 각 장치를 수동으로 구성하지 않고도 여러 Samsung Knox 장치를 XenMobile(또는 모든 모바일 장치 관리자)에 등록할 수 있습니다. 자세한 내용은 Samsung Knox 대량 등록을 참조하십시오.

Knox 서비스 플러그인 앱 추가

Knox와 함께 Android Enterprise를 사용할 계획이라면 Knox 서비스 플러그인(KSP)을 XenMobile에 추가하십시오. KSP 앱은 AndroidOEMConfig를 사용하여 보안 정책, 유연한 VPN 구성 및 생체 인식 인증 제어와 같은 기능을 지원합니다. AndroidOEMConfig를 통해 OEM 및 EMM(엔드포인트 모빌리티 관리자)은 사용자 지정 OEM API를 지원할 수 있습니다. 이러한 API는 Android Enterprise를 통해 지원되지 않는 사용 사례를 다룹니다.

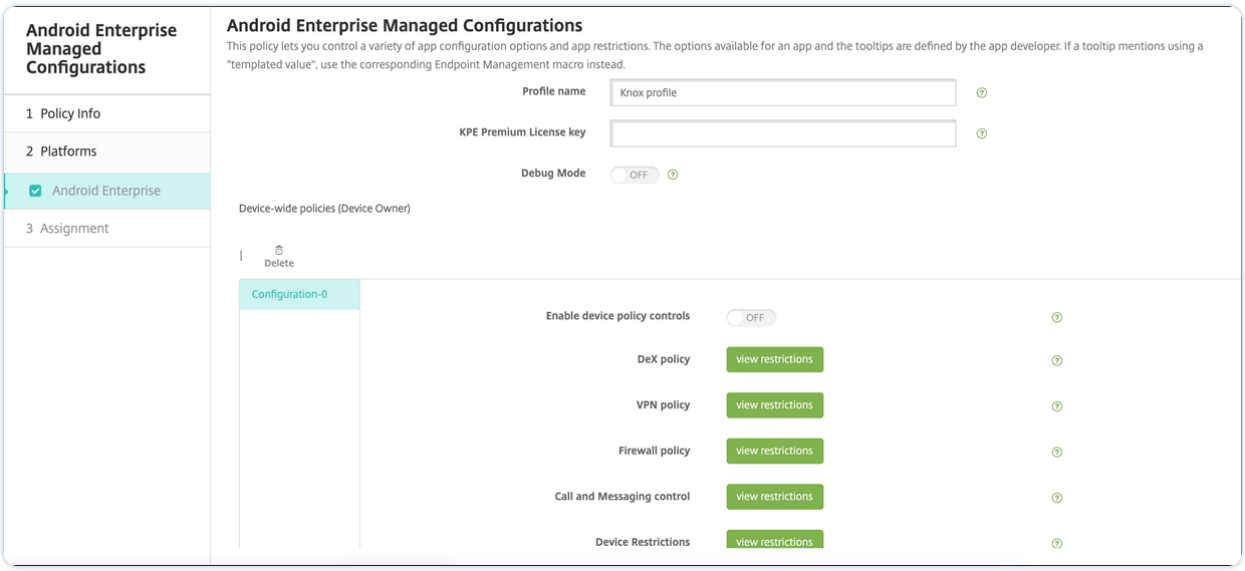
KSP에 대한 자세한 내용은 Knox Service Plugin Guide를 참조하십시오.

1. Google 계정에 로그인하고 `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`으로 이동합니다. Knox Service Plug-in 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 추가를 참조하십시오.

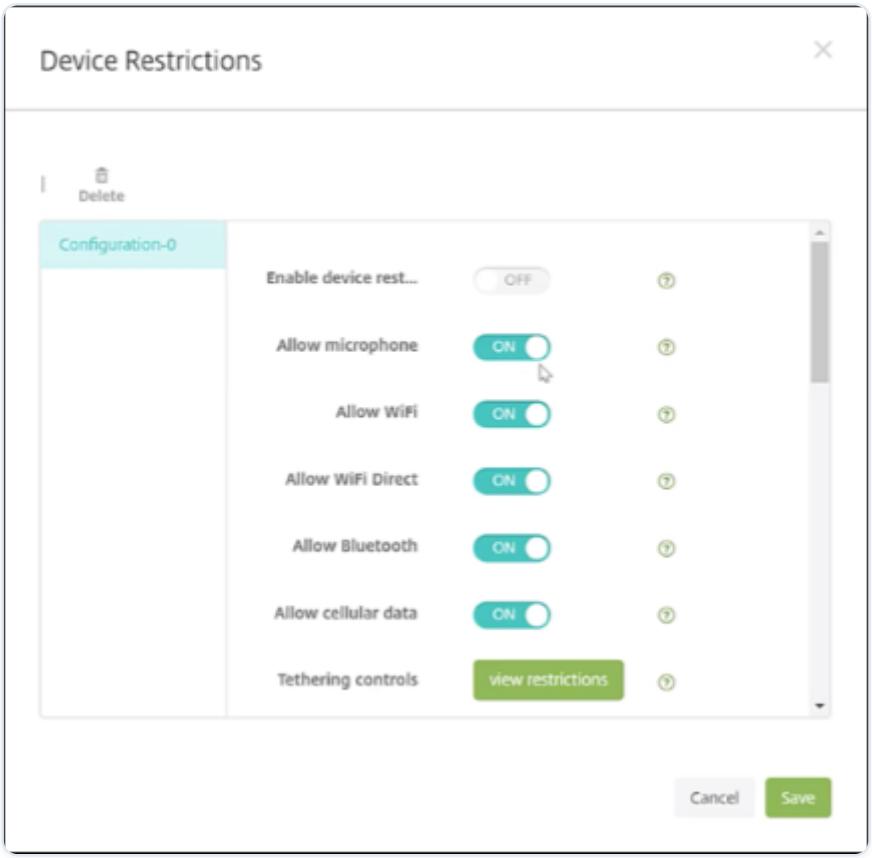


3. XenMobile 콘솔에서 **구성 > 장치 정책**으로 이동합니다. **추가**를 클릭합니다.
4. **관리되는 구성**을 클릭합니다. 나타나는 대화 상자에서 메뉴에서 **Knox Service Plugin**을 선택합니다. 관리되는 구성 정책에 대한 자세한 내용은 관리되는 구성 정책을 참조하십시오.

5. 정책 이름을 입력한 다음 플랫폼 페이지로 계속 진행합니다.



6. 플랫폼 페이지에서 Knox 프로필의 **프로필 이름**을 입력하고 Samsung에서 받은 **KPE 프리미엄 라이선스 키**를 입력합니다. 이 필드 아래에 나타나는 정책은 Knox 배포에서 가져온 것입니다. Knox 정책에 대한 자세한 내용은 이 섹션 앞부분에서 참조된 Knox Service Admin Plug-in Guide를 참조하십시오.



7. **다음**을 클릭하고 정책에 대한 배포 규칙을 구성합니다.
8. **저장**을 클릭합니다.

Samsung Knox 대량 등록

각 장치를 수동으로 구성하지 않고 여러 Samsung Knox 장치를 XenMobile®(또는 모든 모바일 장치 관리자)에 등록하려면 Knox Mobile Enrollment를 사용하십시오. 등록은 최초 사용 시 또는 공장 초기화 후에 이루어집니다. 관리자는 사용자 이름과 암호를 장치에 직접 전달할 수도 있으므로 사용자는 등록 시 정보를 입력할 필요가 없습니다.

> **참고:**
>
> Knox Mobile Enrollment 설정은 XenMobile Knox 컨테이너와 관련이 없습니다. Knox Mobile Enrollment에 대한 자세한 내용은 Knox Mobile Enrollment 관리 가이드를 참조하십시오.

Knox Mobile Enrollment를 위한 전제 조건

- XenMobile은 구성(라이선스 및 인증서 포함)되어 실행 중이어야 합니다.
- Secure Hub APK 파일. Knox Mobile Enrollment를 설정할 때 이 파일을 업로드합니다.
- KME 요구 사항 목록은 Knox Mobile Enrollment 소개를 참조하십시오.
- 장치 정책을 적용하는 데 필요한 Samsung Knox Platform for Enterprise (PKE) 라이선스. XenMobile 장치 정책인 Knox Platform for Enterprise에서 라이선스 키를 제공하십시오.

Secure Hub APK 파일을 다운로드하려면

Google Play 스토어에서 Android용 Citrix Secure Hub™ 파일을 다운로드하십시오.

방화벽 예외 구성

Knox Mobile Enrollment에 액세스하려면 다음 방화벽 예외를 구성하십시오. 이러한 방화벽 예외 중 일부는 모든 장치에 필요하며 일부는 장치의 지리적 지역에 따라 다릅니다.

장치 지역	URL	포트	대상
모두	`https://gslb.secb2b.com`	443	Knox Mobile Enrollment 시작을 위한 글로벌 로드 밸런서
모두	`https://gslb.secb2b.com`	80	일부 제한된 레거시 장치에서 Knox Mobile Enrollment 시작을 위한 글로벌 로드 밸런서

장치 지역	URL	포트	대상
모두	`umc-cdn.secb2b.com`	443	Samsung 에이전트 업데이트 서버
모두	`bulkenrollment.s3.amazonaws.com`	80	Knox Mobile Enrollment 고객 최종 사용자 라이선스 계약
모두	`eula.secb2b.com`	443	Knox Mobile Enrollment 고객 최종 사용자 라이선스 계약
모두	`us-be-api-mssl.samsungknox.com`	443	IMEI 확인을 위한 Samsung 서버
미국	`https://us-segd-api.secb2b.com`	443	미국 지역용 Samsung Enterprise Gateway
유럽	`https://eu-segd-api.secb2b.com`	443	유럽 지역용 Samsung Enterprise Gateway
중국	`https://china-segd-api.secb2b.com`	443	중국 지역용 Samsung Enterprise Gateway

참고:

Knox Mobile Enrollment 관리 가이드에서 방화벽 예외의 전체 목록을 찾을 수 있습니다.

Knox Mobile Enrollment 액세스 얻기

Samsung 설명서에 따라 KME 시작하기에서 Knox Mobile Enrollment에 액세스하십시오.

Knox 모바일 등록 환경 설정

Knox Mobile Enrollment에 액세스한 후 Knox 포털에 로그인합니다.

등록 프로세스는 다음 일반 단계를 따릅니다.

1. MDM 콘솔 정보 및 설정으로 MDM 프로필을 생성합니다.

   MDM 프로필은 장치가 MDM에 연결하는 방법을 알려줍니다.

2. 장치를 MDM 프로필에 추가합니다.

   장치 정보가 포함된 CSV 파일을 업로드하거나 Google Play에서 Knox 배포 앱을 설치하여 사용할 수 있습니다.

3. 장치 소유권이 확인되면 Samsung에서 알려줍니다.
4. 사용자에게 MDM 자격 증명을 제공합니다. Wi-Fi를 사용하여 인터넷에 연결하고 장치 등록 프롬프트를 수락하도록 지시합니다.

MDM 프로필을 생성하려면

프로필 구성에 대한 Samsung 설명서에 설명된 단계를 따르십시오.

다음 필드 또는 단계를 접할 때 설명된 대로 구성하십시오.

- **MDM 선택:** 메뉴에서 **Citrix®**를 선택합니다. 장치 소유자 프로필에만 해당됩니다.
- **MDM 에이전트 APK:** 장치 소유자 프로필에만 해당됩니다. Secure Hub APK 다운로드 URL을 입력하십시오: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

  APK 파일은 등록 중에 장치가 액세스할 수 있는 모든 서버에 있을 수 있습니다. 등록 중에 장치는 다음을 수행합니다.

  - APK 다운로드 URL에서 Secure Hub 다운로드
  - Secure Hub 설치
  - 그런 다음 다음에 설명된 사용자 지정 JSON 데이터로 Secure Hub를 엽니다.

  .apk 파일 이름의 대소문자는 입력하는 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 Hub는 등록을 위해 XenMobile Server 주소와 사용자 이름 및 암호가 필요합니다. Secure Hub가 사용자에게 이를 묻지 않도록 JSON으로 해당 데이터를 제공할 수 있습니다. Secure Hub는 필드가 JSON에서 누락된 경우에만 사용자에게 서버 주소, 사용자 이름 또는 암호를 묻습니다.

  사용자 지정 JSON 데이터의 형식은 다음과 같습니다.

`{"serverURL": "URL", "xm_username":"Username", "xm_password":"Password"}`

대량 등록에 일반적으로 사용되는 이 예시에서 Secure Hub는 등록 중에 사용자에게 서버 주소나 자격 증명을 묻지 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 일반적으로 사용되는 이 예시에서 Secure Hub는 사용자에게 자격 증명을 묻습니다.

`{"serverURL":"https://example.com/zdm"}`

Android Enterprise의 제로 터치 등록을 위한 사용자 지정 JSON을 입력할 수도 있습니다.

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

    {


"serverURL":"URL","xm_username":"username","xm_password":"password"

    }

}
```

장치가 등록을 시작하면 해당 장치는 제공된 URL에서 Secure Hub를 다운로드하고 Secure Hub를 설치한 다음 Secure Hub를 엽니다.

추가 구성

구성 방법에 대한 자세한 내용은 다음 Samsung 설명서 페이지를 참조하십시오.

- 장치 구성: 장치를 대량으로 추가합니다.
- Samsung Knox 배포 앱: Bluetooth, NFC 또는 Wi-Fi Direct 등록을 통해 장치를 등록합니다.
- Knox Mobile Enrollment: Samsung Knox에 대한 자세한 내용은 Samsung 설명서를 참조하십시오.

Knox API 버전 2.4 이전 버전을 실행하는 장치를 등록하려면

Knox API 버전 2.4 이전 버전을 사용하는 장치에서는 초기 장치 설정 중에 대량 등록이 시작되지 않습니다. 대신 사용자가 등록을 시작해야 합니다. 이를 위해 사용자는 Samsung 사이트로 이동하여 새 Mobile Enrollment 클라이언트를 다운로드하고 등록을 시작합니다.

다운로드된 등록 클라이언트는 Knox 2.4/2.4.1 장치용 Knox 대량 등록 포털에 구성된 것과 동일한 MDM 프로필 및 APK를 사용합니다.

사용자는 일반적으로 다음 단계를 따릅니다.

1. 장치를 켜고 Wi-Fi에 연결합니다. 모바일 등록이 시작되지 않거나 Wi-Fi를 사용할 수 없는 경우 다음을 수행합니다.
    a. Samsung Knox Mobile Enrollment(으)로 이동합니다.
    b. 모바일 데이터를 사용하여 장치를 등록하려면 **다음** 버튼을 탭합니다.
2. **Knox로 등록** 프롬프트가 나타나면 **계속**을 탭합니다.
3. EULA(사용 가능한 경우)를 읽습니다. **다음**을 탭합니다.
4. 메시지가 표시되면 IT 관리자가 제공한 **사용자 ID**와 **암호**를 입력합니다.

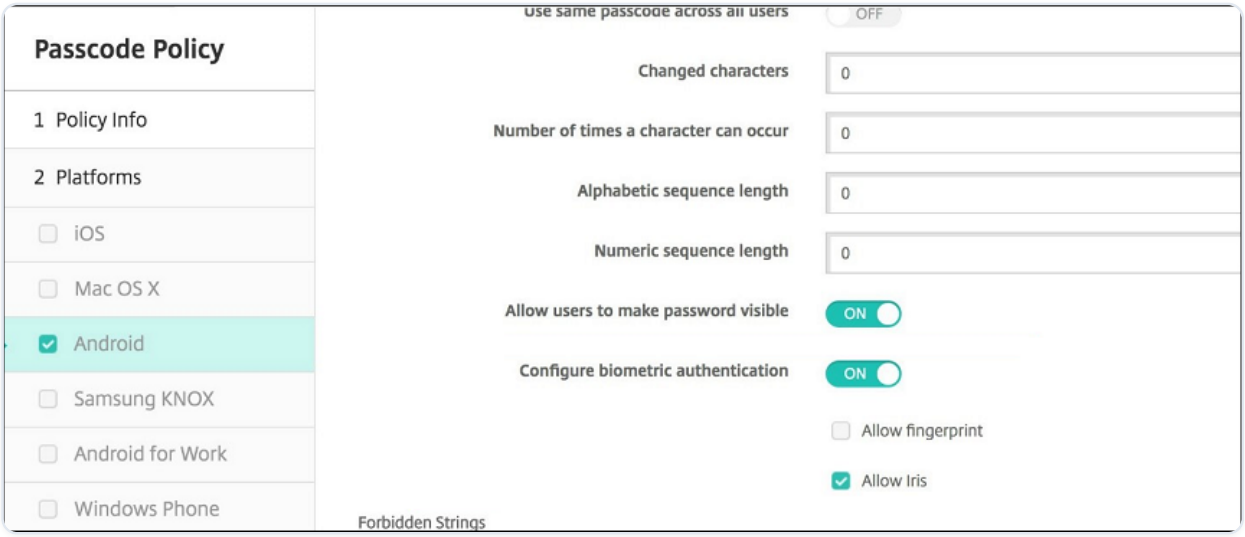
이 시점에서 사용자 자격 증명이 유효성 검사를 거치고 해당 장치가 조직의 엔터프라이즈 IT 환경에 등록됩니다.

Samsung 장치에 대한 생체 인식 인증 사용 및 사용 안 함

XenMobile은 생체 인식 인증이라고도 하는 지문 및 홍채 스캔 인증을 지원합니다. 사용자의 조치 없이 Samsung 장치에 대한 생체 인식 인증을 사용하거나 사용하지 않도록 설정할 수 있습니다. XenMobile에서 생체 인식 인증을 사용하지 않도록 설정하면 사용자 및 타사 앱에서 이 기능을 사용할 수 없습니다.

1. XenMobile 콘솔에서 **구성** > **장치 정책**을 클릭합니다. **장치 정책** 페이지가 나타납니다.
2. **추가**를 클릭합니다. **새 정책 추가** 페이지가 나타납니다.
3. **암호**를 클릭합니다. **암호 정책 정보** 페이지가 나타납니다.
4. **정책 정보** 창에서 다음 정보를 입력합니다.
    - **정책 이름:** 정책에 대한 설명적인 이름을 입력합니다.
    - **설명:** 선택적으로 정책에 대한 설명을 입력합니다.
5. **다음**을 클릭합니다. **플랫폼** 페이지가 나타납니다.
6. **플랫폼**에서 **Android** 또는 **Samsung Knox**를 선택합니다.

7. **생체 인식 인증 구성**을 **켜기**로 설정합니다.
8. **Android**를 선택한 경우, **Samsung SAFE**에서 **지문 허용**, **홍채 허용** 또는 둘 다를 선택합니다.



보안 작업

장치 및 앱 보안 작업은 **관리** > **장치** 페이지에서 수행합니다. 장치 작업에는 해지, 잠금, 잠금 해제 및 초기화가 포함됩니다. 앱 보안 작업에는 앱 잠금 및 앱 초기화가 포함됩니다.

- **활성화 잠금 우회:** 장치 활성화 전에 감독되는 iOS 장치에서 활성화 잠금을 제거합니다. 이 명령은 사용자의 개인 Apple ID 또는 암호를 요구하지 않습니다.
- **앱 잠금:** 장치의 모든 앱에 대한 액세스를 거부합니다. Android에서는 앱 잠금 후 사용자가 XenMobile에 로그인할 수 없습니다. iOS에서는 사용자가 로그인할 수 있지만 어떤 앱에도 액세스할 수 없습니다.
- **앱 초기화:** Secure Hub에서 사용자 계정을 제거하고 장치 등록을 취소합니다. **앱 초기화 해제** 작업을 수행하기 전까지는 사용자가 다시 등록할 수 없습니다.
- **ASM 배포 프로그램 활성화 잠금:** Apple School Manager DEP에 등록된 iOS 장치에 대한 활성화 잠금 우회 코드를 생성합니다.
- **제한 지우기:** 감독되는 iOS 장치에서 이 명령은 XenMobile이 사용자가 구성한 제한 암호 및 제한 설정을 지울 수 있도록 합니다.
- **분실 모드 활성화/비활성화:** 감독되는 iOS 장치를 분실 모드로 전환하고 장치에 표시할 메시지, 전화번호 및 각주를 보냅니다. 이 명령을 두 번째로 보내면 장치가 분실 모드에서 해제됩니다.
- **추적 활성화:** Android 또는 iOS 장치에서 이 명령은 XenMobile이 정의한 빈도로 특정 장치의 위치를 폴링할 수 있도록 합니다. 지도에서 장치 좌표 및 위치를 보려면 **관리 > 장치**로 이동하여 장치를 선택한 다음 **편집**을 클릭합니다. 장치 정보는 **보안** 아래의 **일반** 탭에 있습니다. **추적 활성화**를 사용하여 장치를 지속적으로 추적합니다. Secure Hub는 장치가 실행 중일 때 주기적으로 위치를 보고합니다.
- **전체 초기화:** 모든 메모리 카드를 포함하여 장치의 모든 데이터와 앱을 즉시 지웁니다.

- Android 장치의 경우 이 요청에는 메모리 카드 초기화 옵션도 포함될 수 있습니다.
- 작업 프로필이 있는 Android Enterprise 완전 관리형 장치(COPE 장치)의 경우 선택적 초기화로 작업 프로필을 제거한 후 전체 초기화를 수행할 수 있습니다.
- iOS 및 macOS 장치의 경우 장치가 잠겨 있어도 즉시 초기화가 발생합니다.
  - iOS 11 장치(최소 버전)의 경우: 전체 초기화를 확인할 때 장치의 셀룰러 데이터 요금제를 보존하도록 선택할 수 있습니다.
  - iOS 11.3 장치(최소 버전)의 경우: 전체 초기화를 확인할 때 iOS 장치가 근접 설정을 수행하지 못하도록 방지할 수 있습니다. 새 iOS 장치를 설정할 때 사용자는 일반적으로 이미 구성된 iOS 장치를 사용하여 자신의 장치를 설정할 수 있습니다. XenMobile Server에서 관리되고 초기화된 장치에서는 근접 설정을 차단할 수 있습니다.
  - iOS 17 기기(최소 버전)의 경우: 전체 초기화를 확인하면 기기가 모든 사용자 데이터를 자동으로 지우고, 지정된 Wi-Fi 네트워크에 연결하며, 제공된 등록 프로필을 사용하여 MDM 서버에 다시 등록됩니다.
- 기기 사용자가 메모리 카드 콘텐츠가 삭제되기 전에 기기를 끄면, 사용자는 여전히 기기 데이터에 접근할 수 있습니다.
- 초기화 요청이 기기로 전송되기 전까지는 요청을 취소할 수 있습니다.

- **찾기:** 기기를 찾고 **관리 > 기기** 페이지의 **기기 세부 정보 > 일반** 아래에 지도 포함 기기 위치를 보고합니다. 찾기는 일회성 작업입니다. **찾기**를 사용하여 작업을 수행할 당시의 현재 기기 위치를 표시합니다. 일정 기간 동안 기기를 계속 추적하려면 **추적 활성화**를 사용하십시오.
  - 이 작업을 Android(Android Enterprise 제외) 기기 또는 Android Enterprise(기업 소유 또는 BYOD) 기기에 적용할 때 다음 동작에 유의하십시오.
    - **찾기**는 등록 중에 사용자가 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 중에 권한을 부여하지 않으면 XenMobile은 **찾기** 명령을 보낼 때 위치 권한을 다시 요청합니다.
  - 이 기능을 iOS 또는 Android Enterprise 기기에 적용할 때 다음 제한 사항에 유의하십시오.
    - Android Enterprise 기기의 경우, 위치 기기 정책이 기기의 위치 모드를 **높은 정확도** 또는 **배터리 절약**으로 설정하지 않으면 이 요청이 실패합니다.
    - iOS 기기의 경우, 이 명령은 기기가 MDM 분실 모드에 있을 때만 성공합니다.
- **잠금:** 기기를 원격으로 잠급니다. 이 작업은 기기를 분실하고 도난당했는지 여부를 모를 때 유용합니다. 그러면 XenMobile이 PIN 코드를 생성하여 기기에 설정합니다. 기기에 접근하려면 사용자가 PIN 코드를 입력합니다. XenMobile 콘솔에서 잠금을 제거하려면 **잠금 취소**를 사용하십시오.

- **잠금 및 암호 재설정:** 기기를 원격으로 잠그고 암호를 재설정합니다.
  - Android 8.0 이전 버전의 Android를 실행하는 작업 프로필 모드의 Android Enterprise에 등록된 기기에서는 지원되지 않습니다.
  - Android 8.0 이상을 실행하는 작업 프로필 모드의 Android Enterprise에 등록된 기기에서:
    - 전송된 암호는 작업 프로필을 잠급니다. 기기는 잠기지 않습니다.
    - 암호가 전송되지 않거나 전송된 암호가 암호 요구 사항을 충족하지 않고 작업 프로필에 이미 설정된 암호가 없는 경우: 기기가 잠깁니다.
    - 암호가 전송되지 않거나 전송된 암호가 암호 요구 사항을 충족하지 않지만 작업 프로필에 이미 암호가 설정된 경우: 작업 프로필은 잠기지만 장치는 잠기지 않습니다.
- **알림(벨소리):** Android 장치에서 소리를 재생합니다.
- **재부팅:** Windows 10 및 Windows 11 장치를 다시 시작합니다. Windows 태블릿 및 PC의 경우 "시스템이 곧 재부팅됩니다"라는 메시지가 나타나고 5분 후에 재부팅이 발생합니다.
- **AirPlay 미러링 요청/중지:** 감독되는 iOS 장치에서 AirPlay 미러링을 시작하고 중지합니다.
- **다시 시작/종료:** 감독되는 iOS 장치를 즉시 다시 시작하거나 종료합니다.
- **취소:** 장치가 연결하는 것을 금지합니다.
- **취소/승인(iOS, macOS):** 선택적 초기화와 동일한 작업을 수행합니다. 취소 후 장치를 다시 승인하여 재등록할 수 있습니다.
- **벨소리:** 장치가 분실 모드인 경우, 벨소리는 감독되는 iOS 장치에서 소리를 재생합니다. 이 소리는 장치를 분실 모드에서 제거하거나 사용자가 소리를 비활성화할 때까지 재생됩니다.
- **선택적 초기화:** 장치에서 모든 회사 데이터 및 앱을 지우고 개인 데이터 및 앱은 그대로 둡니다. 선택적 초기화 후 사용자는 장치를 재등록할 수 있습니다.
  - Android 장치를 선택적으로 초기화해도 장치가 장치 관리자 및 회사 네트워크에서 연결 해제되지 않습니다. 장치가 장치 관리자에 액세스하는 것을 방지하려면 장치 인증서도 취소해야 합니다.
  - Android 장치를 선택적으로 초기화하면 장치도 취소됩니다. 장치를 다시 승인하거나 콘솔에서 삭제한 후에만 장치를 재등록할 수 있습니다.
  - 작업 프로필이 있는 Android Enterprise 완전 관리형 장치(COPE 장치)의 경우, 선택적 초기화로 작업 프로필을 제거한 후 전체 초기화를 수행할 수 있습니다. 또는 동일한 사용자 이름으로 장치를 재등록할 수 있습니다. 장치를 재등록하면 작업 프로필이 다시 생성됩니다.
  - Samsung Knox API가 활성화된 경우, 장치를 선택적으로 초기화하면 Samsung Knox 컨테이너도 제거됩니다.
  - iOS 및 macOS 장치의 경우 이 명령은 MDM을 통해 설치된 모든 프로필을 제거합니다.

    - Windows 장치에서 선택적 초기화를 수행하면 현재 로그인한 사용자의 프로필 폴더 내용도 제거됩니다. 선택적 초기화는 구성을 통해 사용자에게 제공하는 웹 클립을 제거하지 않습니다. 웹 클립을 제거하려면 사용자가 장치를 수동으로 등록 해제해야 합니다. 선택적으로 초기화된 장치는 재등록할 수 없습니다.

- **잠금 해제:** 장치가 잠겼을 때 전송된 암호를 지웁니다. 이 명령은 장치를 잠금 해제하지 않습니다.

관리 > 장치에서 **장치 세부 정보** 페이지에는 장치 보안 속성도 나열됩니다. 이러한 속성에는 강력한 ID, 장치 잠금, 활성화 잠금 우회 및 플랫폼 유형에 대한 기타 정보가 포함됩니다. **장치 전체 초기화** 필드에는 사용자 PIN 코드가 포함됩니다. 사용자는 장치가 초기화된 후 해당 코드를 입력해야 합니다. 사용자가 코드를 잊어버린 경우 여기에서 찾을 수 있습니다.

Android 장치에 대한 보안 작업

보안 작업	안드로이드 (ANDROID ENTERPRISE 장치 제외)	안드로이드 엔터프라이즈 (BYOD)	ANDROID ENTERPRISE (기업 소유)
앱 잠금	예	아니요	아니요
앱 초기화	예	아니요	아니요
전체 초기화	예	아니요	예
찾기	예: Android 6.0 이상을 실행하는 장치의 경우, 찾기 기능을 사용하려면 등록 중에 사용자가 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 중에 권한을 부여하지 않으면, XenMobile은 찾기 명령을 보낼 때 다시 위치 권한을 요청합니다.	예: Android 6.0 이상을 실행하는 장치의 경우, 찾기 기능을 사용하려면 등록 중에 사용자가 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 중에 권한을 부여하지 않으면, XenMobile은 찾기 명령을 보낼 때 다시 위치 권한을 요청합니다.	예: Android 6.0 이상을 실행하는 장치의 경우, 찾기 기능을 사용하려면 등록 중에 사용자가 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록 중에 권한을 부여하지 않으면, XenMobile은 찾기 명령을 보낼 때 다시 위치 권한을 요청합니다.
잠금	예	예	예
잠금 및 암호 재설정	예	아니요	예
알림 (벨 울림)	예	예	예

보안 작업	안드로이드 (ANDROID ENTERPRISE 장치 제외)	안드로이드 엔터프라이즈 (BYOD)	ANDROID ENTERPRISE (기업 소유)
취소	예	예	예
선택적 초기화	예	예	아니요

iOS 및 macOS 장치에 대한 보안 작업

보안 작업	IOS	MACOS
활성화 잠금 우회	예	아니요
앱 잠금	예	아니요
앱 초기화	예	아니요
ASM 배포 프로그램 활성화 잠금	예	아니요
제한 해제	예	아니요
분실 모드 활성화/비활성화	예	아니요
추적 활성화/비활성화	예	아니요
전체 초기화	예	예
찾기	예	아니요
잠금	예	예
벨 울리기	예	예
AirPlay 미러링 요청/중지	예	아니요
다시 시작/종료	예	아니요
취소/승인	예	예
선택적 초기화	예	예
잠금 해제	예	아니요

Windows 장치에 대한 보안 작업

보안 작업	WINDOWS 태블릿 10
찾기	예
잠금	예
잠금 및 암호 재설정	아니요
재부팅	예
취소	예
벨 울리기	아니요
선택적 초기화	예
초기화	예

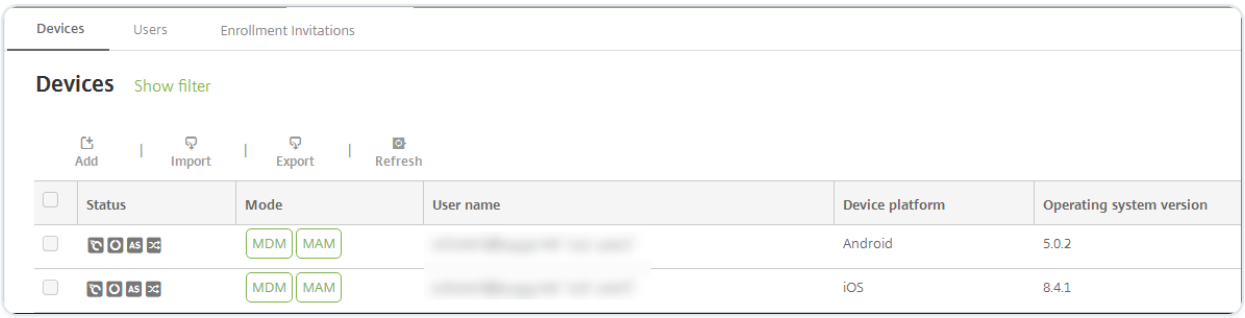
이 문서의 나머지 부분에서는 다양한 보안 작업을 수행하는 단계를 제공합니다. 일부 작업은 자동화할 수도 있습니다. 자세한 내용은 자동화된 작업을 참조하십시오.

iOS 장치 잠금

분실된 iOS 장치를 잠글 수 있으며, 장치 잠금 화면에 메시지와 전화번호가 함께 표시됩니다. 이 기능은 iOS 7 이상을 실행하는 장치에서 지원됩니다.

잠긴 장치에 메시지와 전화번호를 표시하려면 XenMobile 콘솔에서 암호 정책을 **true**로 설정하십시오. 또는 사용자가 장치에서 암호를 수동으로 활성화할 수 있습니다.

1. **관리 > 장치**를 클릭합니다. **장치** 페이지가 나타납니다.



2. 잠그려는 iOS 장치를 선택합니다.

   장치 옆의 확인란을 선택하면 장치 목록 위에 옵션 메뉴가 표시됩니다. 목록의 다른 곳을 클릭하면 옵션 메뉴가 목록의 오른쪽에 나타납니다.

옵션 메뉴 이미지(/en-us/xenmobile/server/media/manage-devices-with-commands-secure.png)

옵션 메뉴 이미지(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-2.png)

3. 옵션 메뉴에서 **보안**을 클릭합니다. **보안 작업** 대화 상자가 나타납니다.

   보안 작업 대화 상자 이미지(/en-us/xenmobile/server/media/manage-devices-secure-lock.png)

4. **잠금**을 클릭합니다. **보안 작업** 확인 대화 상자가 표시됩니다.

   보안 작업 확인 이미지(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm.png)

5. 선택적으로 장치의 잠금 화면에 표시될 메시지와 전화번호를 입력합니다.

   iOS 7 이상을 실행하는 iPad의 경우: iOS는 **메시지** 필드에 입력한 내용에 “분실된 iPad”라는 문구를 추가합니다.

   iOS 7 이상을 실행하는 iPhone의 경우: **메시지** 필드를 비워두고 전화번호를 제공하면 Apple은 장치 잠금 화면에 “소유자에게 전화” 메시지를 표시합니다.

6. **장치 잠금**을 클릭합니다.

XenMobile 콘솔에서 장치 제거

> **중요:**

> XenMobile 콘솔에서 장치를 제거하면 관리되는 앱과 데이터는 장치에 남아 있습니다. 장치에서 관리되는 앱과 데이터를 제거하려면 이 문서의 뒷부분에 있는 "장치 삭제"를 참조하십시오.

> XenMobile 콘솔에서 장치를 제거하려면 **관리 > 장치**로 이동하여 관리되는 장치를 선택한 다음 **삭제**를 클릭합니다.

삭제 옵션 이미지(/en-us/xenmobile/server/media/manage-devices-delete.png)

장치 선택적 초기화

1. **관리 > 장치**로 이동하여 관리되는 장치를 선택한 다음 **보안**을 클릭합니다.
2. **보안 작업**에서 **선택적 초기화**를 클릭합니다.
3. Android 장치에 한해 장치를 회사 네트워크에서 연결 해제합니다. 장치가 초기화된 후 **보안 작업**에서 **취소**를 클릭합니다.

초기화가 발생하기 전에 선택적 초기화 요청을 철회하려면 **보안 작업**에서 **선택적 초기화 취소**를 클릭합니다.

장치 삭제

이 절차는 장치에서 관리되는 앱과 데이터를 제거하고 XenMobile 콘솔의 장치 목록에서 장치를 삭제합니다. Endpoint Management Public REST API를 사용하여 장치를 대량으로 삭제할 수 있습니다.

1. **관리 > 장치**로 이동하여 관리되는 장치를 선택한 다음 **보안**을 클릭합니다.
2. **선택적 초기화**를 클릭합니다. 메시지가 표시되면 **선택적 초기화 수행**을 클릭합니다.
3. 초기화 명령이 성공했는지 확인하려면 **관리 > 장치**를 새로 고칩니다. **모드** 열에서 MDM 및 MAM의 황색은 초기화 명령이 성공했음을 나타냅니다.

   성공적인 초기화 명령 이미지(/en-us/xenmobile/server/media/manage-devices-check-wipe-status.png)
4. **관리 > 장치**에서 장치를 선택한 다음 **삭제**를 클릭합니다. 메시지가 표시되면 **삭제**를 다시 클릭합니다.

앱 잠금, 잠금 해제, 초기화 또는 초기화 해제

1. **관리 > 장치**로 이동하여 관리되는 장치를 선택한 다음 **보안**을 클릭합니다.
2. **보안 작업**에서 앱 작업을 클릭합니다.

   보안 작업 상자를 사용하여 Active Directory에서 계정이 비활성화되거나 삭제된 사용자의 장치 상태를 확인할 수도 있습니다. 앱 잠금 해제 또는 앱 초기화 해제 작업이 있으면 앱이 잠겨 있거나 초기화되었음을 나타냅니다.

앱 초기화 및 초기화 해제

1. **관리 > 장치**로 이동합니다. 장치를 선택합니다.
2. 앱 초기화
   - **보안 > 앱 초기화**를 클릭합니다. 다음 메시지가 포함된 대화 상자가 나타납니다. **이 장치를 앱 초기화하시겠습니까? 앱 초기화**를 클릭합니다.
3. 앱 초기화 해제
   - **보안 > 앱 초기화 해제**를 클릭합니다. 다음 메시지가 포함된 대화 상자가 나타납니다. **이 장치를 앱 초기화 해제하시겠습니까? 장치 앱 초기화 해제**를 클릭합니다.
4. 장치에서 Secure Hub를 열고 **스토어**를 클릭합니다.
5. Secure Hub를 시작합니다.

iOS 장치를 분실 모드로 전환

XenMobile 분실 모드 장치 속성은 iOS 장치를 분실 모드로 전환합니다. Apple 관리 분실 모드와 달리 XenMobile 분실 모드는 사용자가 장치를 찾을 수 있도록 다음 작업 중 하나를 수행할 필요가 없습니다. **나의 iPhone/iPad 찾기** 설정을 구성하거나 Citrix Secure Hub에 대한 위치 서비스를 활성화합니다.

XenMobile 분실 모드에서는 관리자만 장치를 잠금 해제할 수 있습니다. (대조적으로, XenMobile 장치 잠금 기능을 사용하는 경우 사용자는 제공된 PIN 코드를 사용하여 장치를 직접 잠금 해제할 수 있습니다.

분실 모드를 활성화하거나 비활성화하려면: **관리 > 장치**로 이동하여 감독되는 iOS 장치를 선택한 다음 **보안**을 클릭합니다. 그런 다음 **분실 모드 활성화** 또는 **분실 모드 비활성화**를 클릭합니다.

분실 모드 옵션 이미지(/en-us/xenmobile/server/media/manage-devices-enable-lost-mode-button.png)

분실 모드 활성화를 클릭하면 분실 모드일 때 장치에 표시될 정보를 입력합니다.

장치에 표시될 정보 이미지(/en-us/xenmobile/server/media/enable-lost-mode-dialog.png)

다음 방법 중 하나를 사용하여 분실 모드 상태를 확인합니다.

- **보안 작업** 창에서 버튼이 **분실 모드 비활성화**인지 확인합니다.
- **관리 > 장치**에서 **보안** 아래의 **일반** 탭에서 마지막 분실 모드 활성화 또는 분실 모드 비활성화 작업을 확인합니다.

일반 탭 이미지(/en-us/xenmobile/server/media/manage-devices-ios-lost-mode.png)

- **관리 > 장치**에서 **속성** 탭에서 **MDM 분실 모드 활성화됨** 설정 값이 올바른지 확인합니다.

MDM 분실 모드 활성화됨 설정 이미지(/en-us/xenmobile/server/media/manage-devices-details-properties.png)

iOS 장치에서 XenMobile 분실 모드를 활성화하면 XenMobile 콘솔도 다음과 같이 변경됩니다.

- **구성 > 작업**에서 **작업** 목록에는 다음 자동 작업이 포함되지 않습니다. **장치 해지**, **장치 선택적 초기화**, **장치 완전 초기화**.
- **관리 > 장치**에서 **보안 작업** 목록에는 더 이상 **해지** 및 **선택적 초기화** 장치 작업이 포함되지 않습니다. 필요에 따라 **전체 초기화** 작업을 수행하기 위해 보안 작업을 계속 사용할 수 있습니다.

iOS 7 이상을 실행하는 iPad의 경우: iOS는 **보안 작업** 화면의 **메시지**에 입력한 내용에 "Lost iPad"라는 단어를 추가합니다.

iOS 7 이상을 실행하는 iPhone의 경우: **메시지**를 비워두고 전화번호를 제공하면 Apple은 장치 잠금 화면에 "소유자에게 전화" 메시지를 표시합니다.

iOS 활성화 잠금 우회

활성화 잠금은 분실되거나 도난당한 감독 대상 장치의 재활성화를 방지하는 나의 iPhone/iPad 찾기 기능입니다. 활성화 잠금은 누군가가 나의 iPhone/iPad 찾기를 비활성화하거나, 장치를 지우거나, 장치를 재활성화하기 전에 사용자 Apple ID와 암호를 요구합니다. 조직이 소유한 장치의 경우, 예를 들어 장치를 재설정하거나 재할당하려면 활성화 잠금을 우회해야 합니다.

활성화 잠금을 활성화하려면 XenMobile MDM 옵션 장치 정책을 구성하고 배포합니다. 그러면 사용자의 Apple 자격 증명 없이 XenMobile 콘솔에서 장치를 관리할 수 있습니다. 활성화 잠금의 Apple 자격 증명 요구 사항을 우회하려면 XenMobile 콘솔에서 활성화 잠금 우회 보안 작업을 실행합니다.

예를 들어, 사용자가 분실한 휴대폰을 반환하거나 전체 초기화 전후에 장치를 설정하는 경우: 휴대폰에서 iTunes 계정 자격 증명을 요청하면 XenMobile 콘솔에서 활성화 잠금 우회 보안 작업을 실행하여 해당 단계를 우회할 수 있습니다.

활성화 잠금 우회를 위한 장치 요구 사항

- iOS 7.1 (최소 버전)
- Apple Configurator 또는 Apple DEP를 통해 감독됨
- iCloud 계정으로 구성됨
- 나의 iPhone/iPad 찾기 활성화됨
- XenMobile에 등록됨
- 활성화 잠금이 활성화된 MDM 옵션 장치 정책이 장치에 배포됨

장치를 전체 초기화하기 전에 활성화 잠금을 우회하려면 다음을 수행합니다.

1. **관리 > 장치**로 이동하여 장치를 선택하고 **보안**을 클릭한 다음 **활성화 잠금 우회**를 클릭합니다.
2. 장치를 초기화합니다. 장치 설정 중에 활성화 잠금 화면이 나타나지 않습니다.

장치를 전체 초기화한 후 활성화 잠금을 우회하려면 다음을 수행합니다.

1. 장치를 재설정하거나 초기화합니다. 장치 설정 중에 활성화 잠금 화면이 나타납니다.
2. **Manage > Devices**로 이동하여 장치를 선택하고 **Secure**를 클릭한 다음 **Activation Lock Bypass**를 클릭합니다.
3. 장치에서 뒤로 버튼을 탭합니다. 홈 화면이 나타납니다.

다음 사항에 유의하십시오.

- 사용자에게 나의 iPhone/iPad 찾기를 비활성화하지 않도록 권고하십시오. 장치에서 전체 초기화를 수행하지 마십시오. 두 경우 모두 사용자에게 iCloud 계정 암호를 입력하라는 메시지가 표시됩니다. 계정 유효성 검사 후 사용자는 모든 콘텐츠 및 설정을 지운 후에도 iPhone/iPad 활성화 화면을 볼 수 없습니다.
- 생성된 활성화 잠금 우회 코드가 있고 활성화 잠금이 활성화된 장치의 경우: 전체 초기화 후 iPhone/iPad 활성화 페이지를 우회할 수 없는 경우 XenMobile에서 장치를 삭제할 필요가 없습니다. 사용자 또는 관리자가 Apple 지원에 문의하여 장치를 직접 차단 해제할 수 있습니다.
- 하드웨어 인벤토리 중에 XenMobile은 장치에 활성화 잠금 우회 코드를 쿼리합니다. 우회 코드를 사용할 수 있는 경우 장치는 이를 XenMobile로 보냅니다. 그런 다음 장치에서 우회 코드를 제거하려면 XenMobile 콘솔에서 활성화 잠금 우회 보안 작업을 보냅니다. 이 시점에서 Apple은 장치 차단 해제에 필요한 우회 코드를 가지고 있습니다.
- 활성화 잠금 우회 보안 작업은 Apple 서비스의 가용성에 따라 달라집니다. 작업이 작동하지 않으면 다음과 같이 장치를 차단 해제할 수 있습니다. 장치에서 iCloud 계정 자격 증명을 수동으로 입력합니다. 또는 사용자 이름 필드를 비워두고 암호 필드에 우회 코드를 입력합니다. 우회 코드를 찾으려면 **Manage > Devices**로 이동하여 장치를 선택하고 **Edit**를 클릭한 다음 **Properties**를 클릭합니다. **Activation lock bypass code**는 **Security information** 아래에 있습니다.

XenMobile® AutoDiscovery 서비스

AutoDiscovery 서비스는 이메일 기반 URL 검색을 통해 사용자의 등록 프로세스를 간소화합니다. AutoDiscovery 서비스는 또한 Citrix Workspace™ 고객을 위한 등록 확인, 인증서 고정 및 기타 이점과 같은 기능을 제공합니다. Citrix Cloud™에서 호스팅되는 이 서비스는 많은 XenMobile 배포의 중요한 부분입니다.

AutoDiscovery 서비스를 통해 사용자는 다음을 수행할 수 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.com`.

보안 수준이 높은 환경에서는 AutoDiscovery 서비스를 사용하는 것이 좋습니다. AutoDiscovery 서비스는 공개 키 인증서 고정을 지원하여 중간자 공격을 방지합니다. 인증서 고정은 Citrix 클라이언트가 XenMobile과 통신할 때 엔터프라이즈에서 서명한 인증서가 사용되도록 합니다. XenMobile 사이트에 대한 인증서 고정을 구성하려면 Citrix 지원팀에 문의하십시오. 인증서 고정에 대한 자세한 내용은 인증서 고정을 참조하십시오.

AutoDiscovery 서비스에 액세스하려면 `<https://adsui.cloud.com>`(상업용) 또는 `<https://adsui.cem.cloud.us>`(정부용)로 이동하십시오.

사전 요구 사항

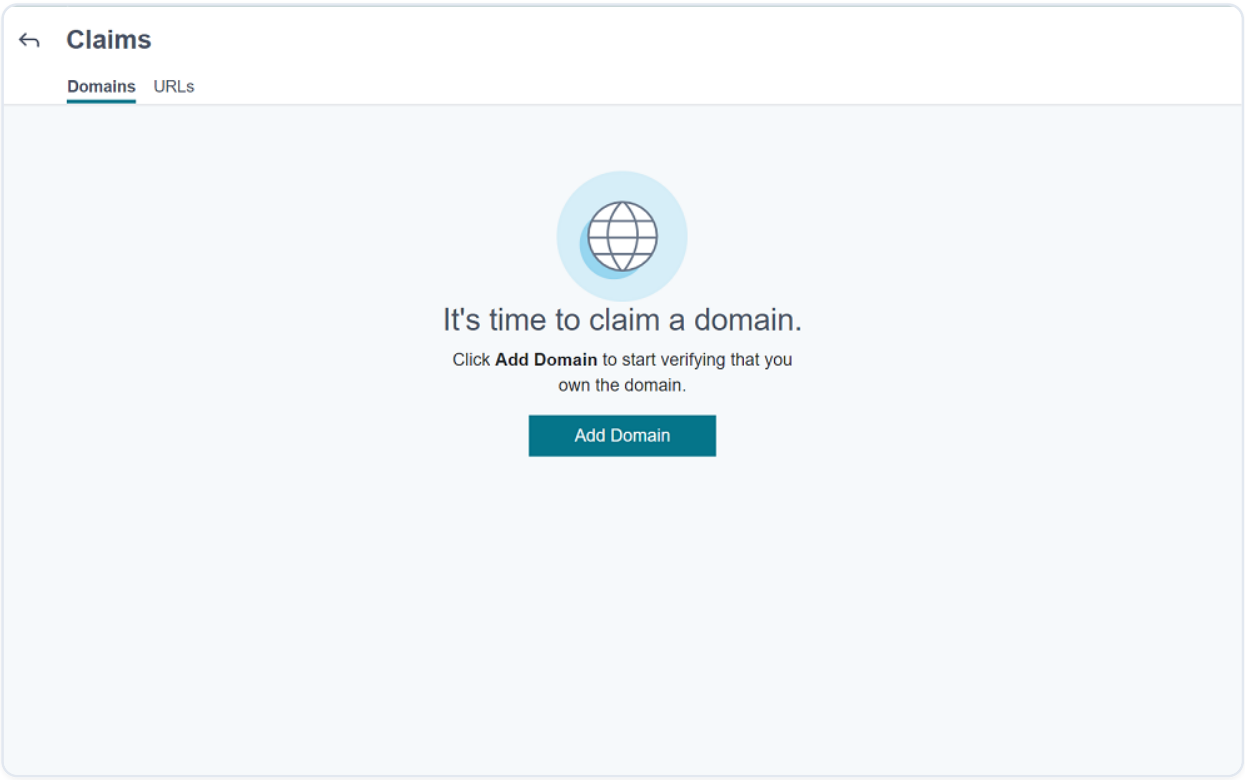
- Citrix Cloud의 새로운 AutoDiscovery 서비스에는 최신 버전의 Secure Hub가 필요합니다.
  - iOS의 경우 Secure Hub 버전 21.6.0 이상
  - Android의 경우 Secure Hub 버전 21.8.5 이상

  이전 버전의 Secure Hub에서 실행되는 장치는 서비스 중단을 경험할 수 있습니다.
- 새로운 AutoDiscovery 서비스에 액세스하려면 전체 액세스 권한이 있는 Citrix Cloud 관리자 계정이 있어야 합니다. AutoDiscovery 서비스는 사용자 지정 액세스 권한이 있는 관리자 계정을 지원하지 않습니다. 계정이 없는 경우 Citrix Cloud 가입을 참조하십시오.

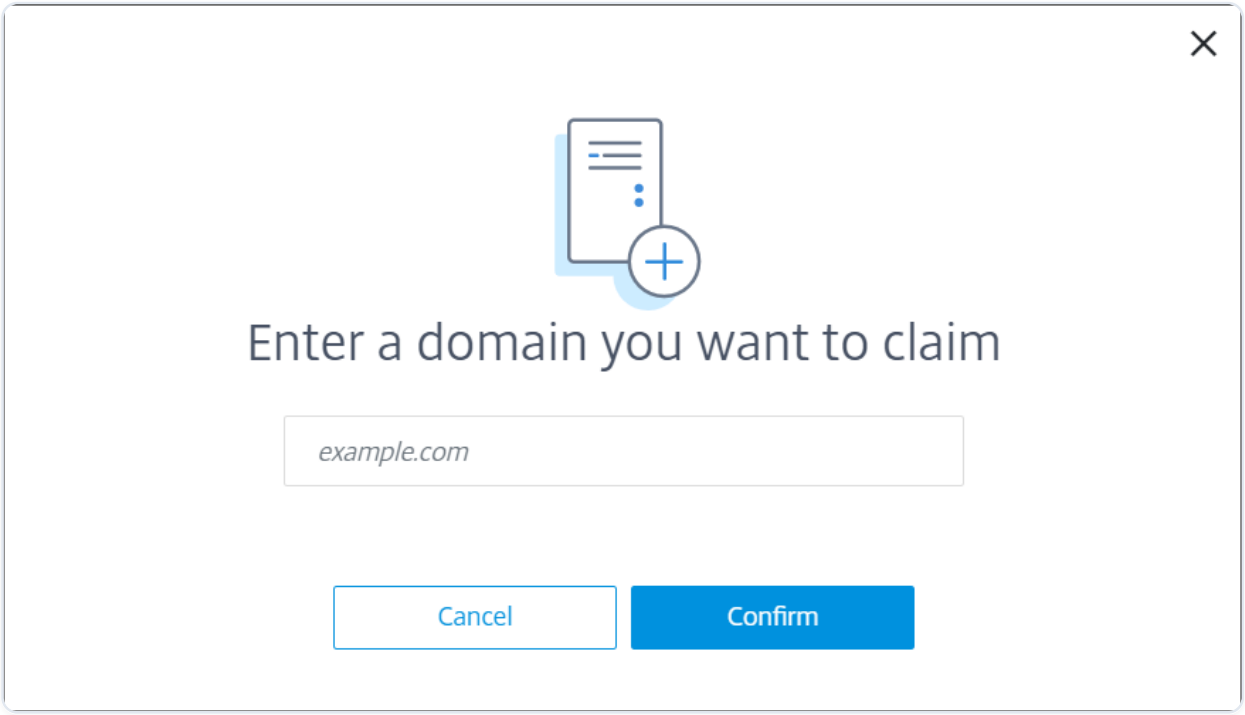
  Citrix는 모든 기존 AutoDiscovery 레코드를 서비스 중단 없이 Citrix Cloud로 마이그레이션했습니다. 마이그레이션된 레코드는 새 콘솔에 자동으로 나타나지 않습니다. 소유권을 증명하려면 새 AutoDiscovery 서비스에서 도메인을 다시 클레임해야 합니다. 자세한 내용은 CTX312339를 참조하십시오.
- Endpoint Management 배포용 AutoDiscovery 서비스를 사용하기 전에 도메인을 확인하고 클레임하십시오. 최대 10개의 도메인을 클레임할 수 있습니다. 클레임은 확인된 도메인을 AutoDiscovery 서비스와 연결합니다. 10개 이상의 도메인을 클레임하려면 SRE 티켓을 열거나 Citrix 기술 지원팀에 문의하십시오.
- MAM 트래픽을 데이터 센터로 전달하려면 Citrix Gateway FQDN 대신 MAM 포트 설정을 사용하십시오. Citrix Gateway의 포트와 함께 정규화된 도메인 이름을 입력하면 클라이언트 장치는 **MAM 포트** 설정의 구성을 사용합니다.
- 광고 차단기가 사이트 열기를 방해하는 경우 전체 웹 사이트에 대해 광고 차단기를 비활성화해야 합니다.

도메인 클레임

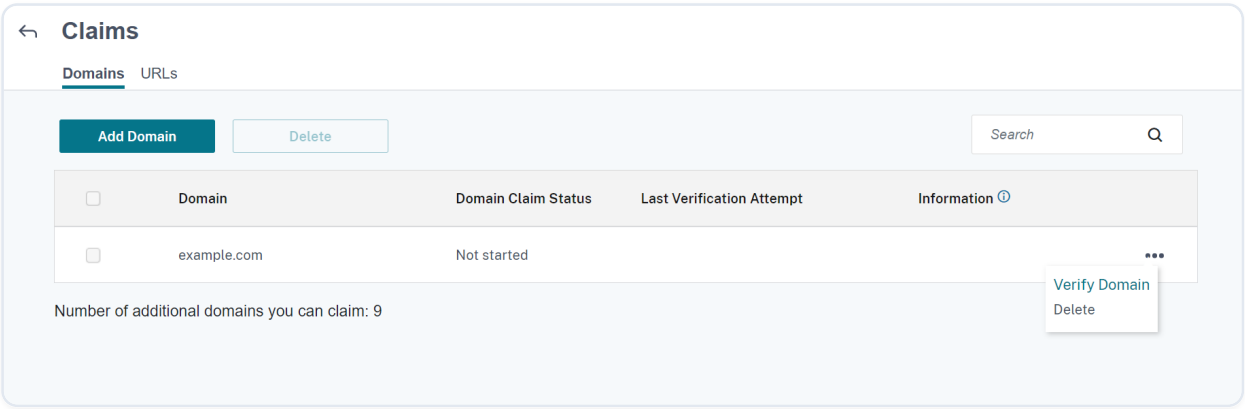
1. **클레임 > 도메인** 탭에서 **도메인 추가**를 클릭합니다.



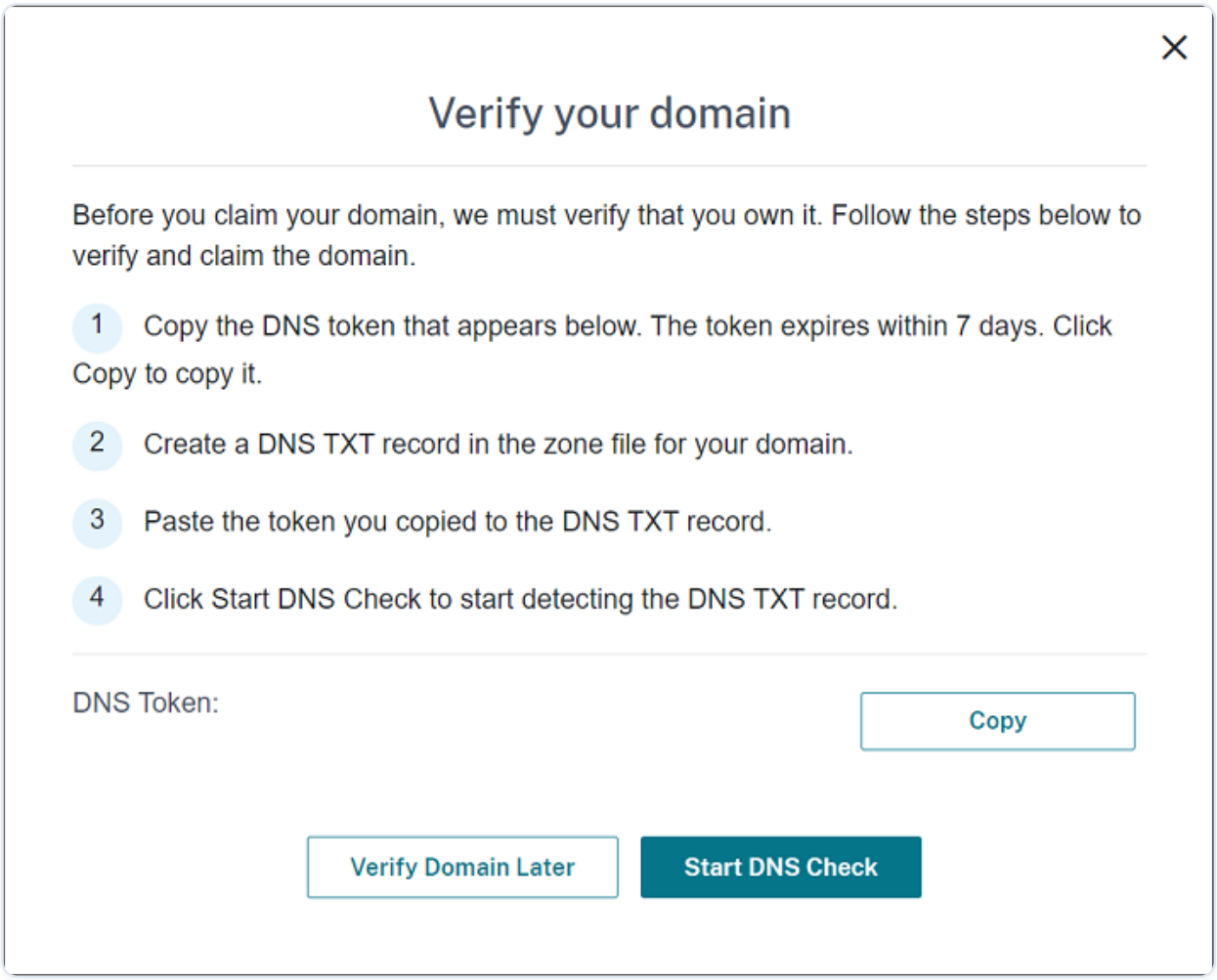
2. 나타나는 대화 상자에서 XenMobile 환경의 도메인 이름을 입력한 다음 **확인**을 클릭합니다. 도메인이 **클레임 > 도메인**에 나타납니다.



3. 추가한 도메인에서 줄임표 메뉴를 클릭하고 **도메인 확인**을 선택하여 확인 프로세스를 시작합니다. **도메인 확인** 페이지가 나타납니다.



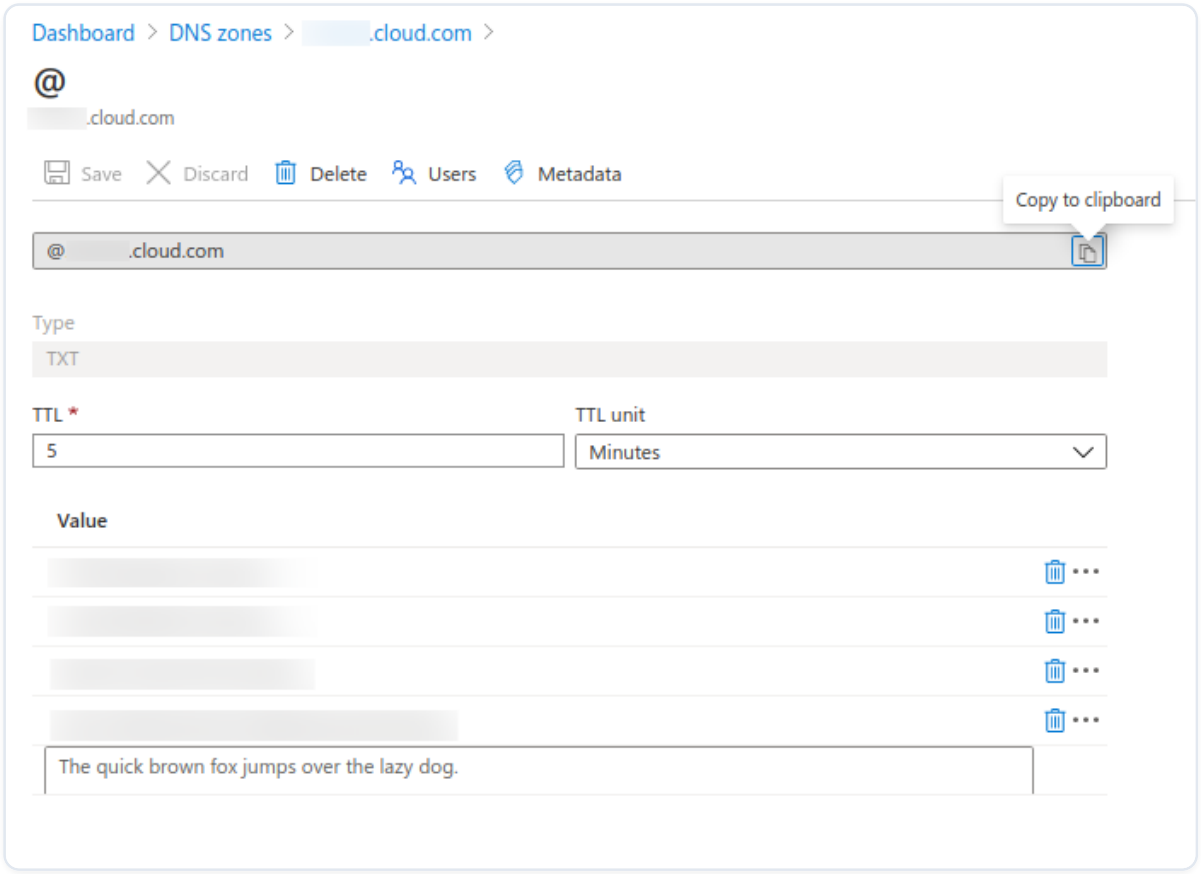
4. **도메인 확인** 페이지에서 지침에 따라 도메인 소유권을 확인합니다.



a. **복사**를 클릭하여 DNS 토큰을 클립보드에 복사합니다.

b. 도메인의 영역 파일에 DNS TXT 레코드를 생성합니다. 이렇게 하려면 도메인 호스팅 공급자 포털로 이동하여 복사한 DNS 토큰을 추가합니다.

   다음 스크린샷은 도메인 호스팅 공급자 포털을 보여줍니다. 사용자 포털은 다르게 보일 수 있습니다.



c. Citrix Cloud에서 **도메인 확인** 페이지에서 DNS TXT 레코드 검색을 시작하려면 **DNS 확인 시작**을 클릭합니다. 나중에 도메인을 확인하려면 **나중에 도메인 확인**을 클릭합니다.

확인 프로세스는 일반적으로 약 1시간이 소요됩니다. 하지만 응답이 반환되기까지 최대 이틀이 걸릴 수 있습니다. 상태 확인 중에 로그아웃했다가 다시 로그인해도 괜찮습니다.

구성이 완료되면 도메인 상태가 **보류 중**에서 **확인됨**으로 변경됩니다.

5. 도메인을 클레임한 후 AutoDiscovery 서비스에 대한 정보를 제공합니다. 추가한 도메인에서 줄임표 메뉴를 클릭한 다음 **Endpoint Management 정보 추가**를 클릭합니다. **AutoDiscovery 서비스 정보** 페이지가 나타납니다.
6. 다음 정보를 입력한 다음 **저장**을 클릭합니다.

- **Endpoint Management Server FQDN:** XenMobile Server의 정규화된 도메인 이름을 입력합니다. 예: `example.xm.cloud.com`. 이 설정은 MDM 및 MAM 제어 트래픽에 사용됩니다.
- **Citrix Gateway FQDN:** FQDN 또는 FQDN:포트 형식으로 Citrix Gateway의 정규화된 도메인 이름을 입력합니다. 예: `example.com`. 이 설정은 MAM 트래픽을 데이터 센터로 전달하는 데 사용됩니다. MDM 전용 배포의 경우 이 필드를 비워 둡니다.

> **참고:**

> Citrix는 MAM 트래픽을 제어하기 위해 **Citrix Gateway FQDN** 대신 **MAM 포트** 설정을 사용할 것을 권장합니다. Citrix Gateway의 포트와 함께 정규화된 도메인 이름을 입력하면 클라이언트 장치는 **MAM 포트** 설정의 구성을 사용합니다.

- **인스턴스 이름:** 이전에 구성한 XenMobile Server의 인스턴스 이름을 입력합니다. 인스턴스 이름을 모르는 경우 기본값인 **zdm**을 그대로 둡니다.
- **MDM 포트:** MDM 제어 트래픽 및 MDM 등록에 사용되는 포트를 입력합니다. 클라우드 기반 서비스의 경우 기본값은 443입니다.
- **MAM 포트:** MAM 제어 트래픽, MAM 등록, iOS 등록 및 앱 열거에 사용되는 포트를 입력합니다. 클라우드 기반 서비스의 경우 기본값은 8443입니다.

Windows 장치용 AutoDiscovery 요청

Windows 장치를 등록할 계획이라면 다음을 수행합니다.

1. Citrix Support에 문의하여 Windows AutoDiscovery를 활성화하기 위한 지원 요청을 생성하십시오.
2. `enterpriseenrollment.mycompany.com`에 대한 공개적으로 서명된 비와일드카드 SSL 인증서를 받으십시오. `mycompany.com` 부분은 사용자가 등록하는 데 사용하는 계정이 있는 도메인입니다. 이전 단계에서 생성된 지원 요청에 .pfx 형식의 SSL 인증서와 해당 암호를 첨부하십시오.

   Windows 장치를 등록하기 위해 둘 이상의 도메인을 사용하려면 다음 구조의 다중 도메인 인증서를 사용할 수도 있습니다.

   - 서비스하는 기본 도메인을 지정하는 CN이 있는 SubjectDN (예: enterpriseenrollment.mycompany1.com).
   - 나머지 도메인에 대한 적절한 SAN (예: enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com 등).
3. DNS에 CNAME(Canonical Name) 레코드를 생성하고 SSL 인증서 주소(enterpriseenrollment.mycompany.com)를 autodisc.xm.cloud.com에 매핑하십시오.

   Windows 장치 사용자가 UPN을 사용하여 등록하면 Citrix 등록 서버는 다음을 수행합니다.

   - XenMobile Server의 세부 정보를 제공합니다.
   - 장치에 XenMobile에서 유효한 인증서를 요청하도록 지시합니다.

이 시점에서 지원되는 모든 장치를 등록할 수 있습니다. 장치에 리소스를 제공할 준비를 하려면 다음 섹션으로 이동하십시오.

장치 정책

정책을 생성하여 XenMobile®이 장치와 상호 작용하는 방식을 구성할 수 있습니다. 많은 정책이 모든 장치에 공통적이지만, 각 장치에는 운영 체제에 특정한 정책 집합이 있습니다. 결과적으로 플랫폼 간, 심지어 Android 장치의 다른 제조업체 간에도 차이점을 발견할 수 있습니다.

각 장치 정책에 대한 요약 설명은 이 문서의 장치 정책 요약을 참조하십시오.

> **참고:**

> 환경이 GPO(그룹 정책 개체)로 구성된 경우:

> Windows 10 및 Windows 11 장치에 대한 XenMobile 장치 정책을 구성할 때 다음 규칙을 염두에 두십시오. 하나 이상의 등록된 장치에서 정책이 충돌하는 경우 GPO에 맞춰진 정책이 우선합니다.

> Android Enterprise 컨테이너가 지원하는 정책을 확인하려면 Android Enterprise를 참조하십시오.

필수 구성 요소

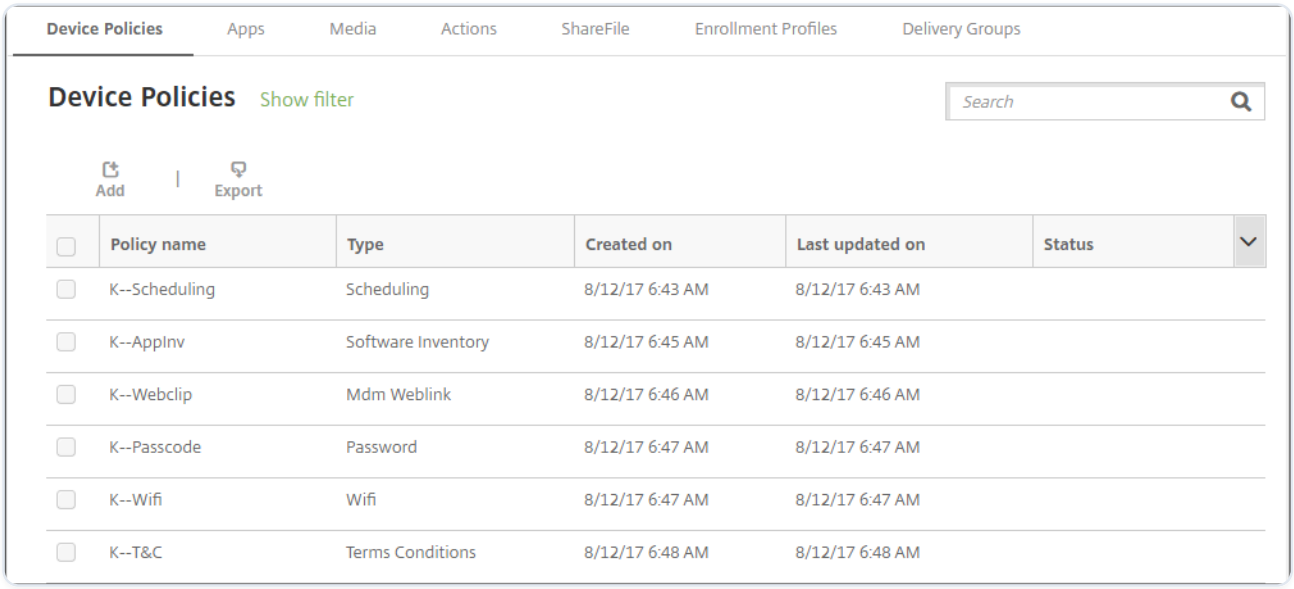
- 사용할 모든 배달 그룹을 생성합니다.
- 필요한 CA 인증서를 설치합니다.

장치 정책 추가

장치 정책을 생성하는 기본 단계는 다음과 같습니다.

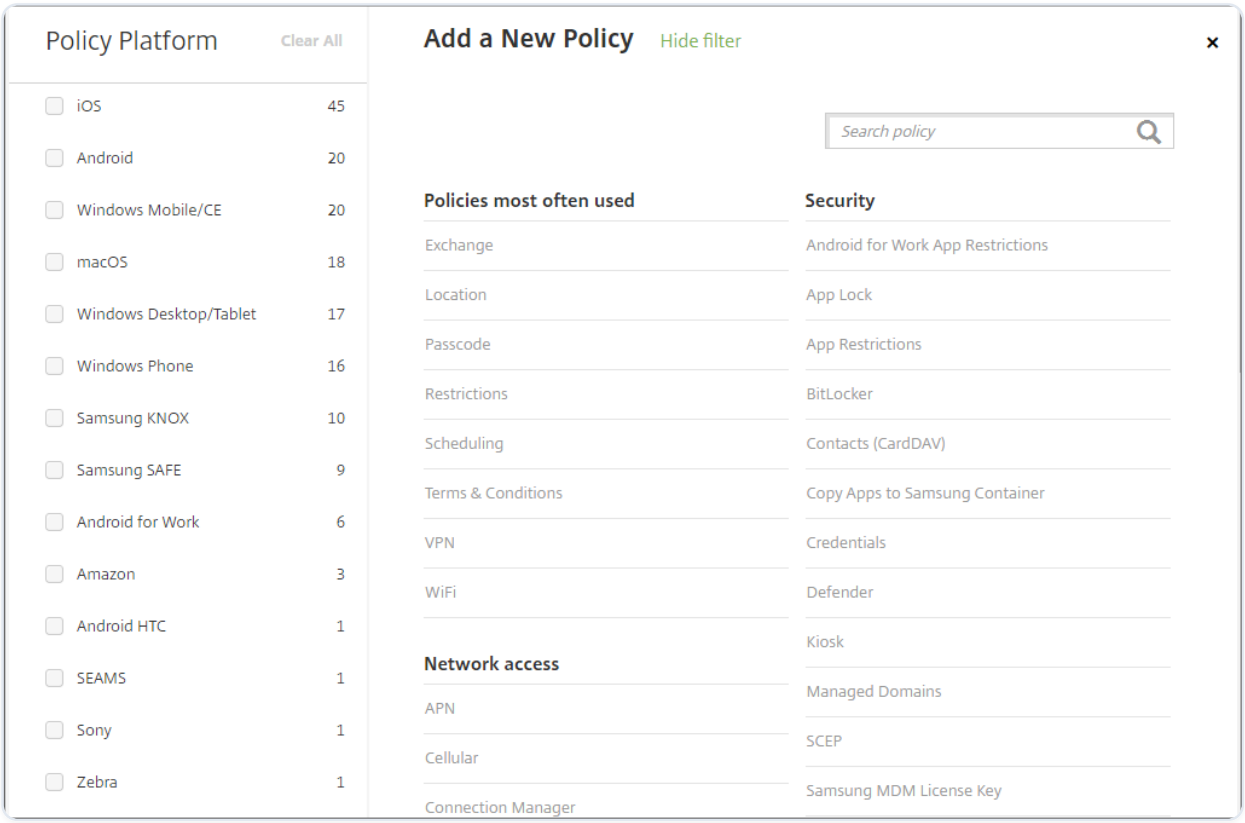
1. 정책의 이름을 지정하고 설명합니다.
2. 하나 이상의 플랫폼에 대한 정책을 구성합니다.
3. 배포 규칙을 생성합니다(선택 사항).
4. 정책을 배달 그룹에 할당합니다.
5. 배포 일정을 구성합니다(선택 사항).

장치 정책을 생성하고 관리하려면 **구성 > 장치 정책**으로 이동합니다.

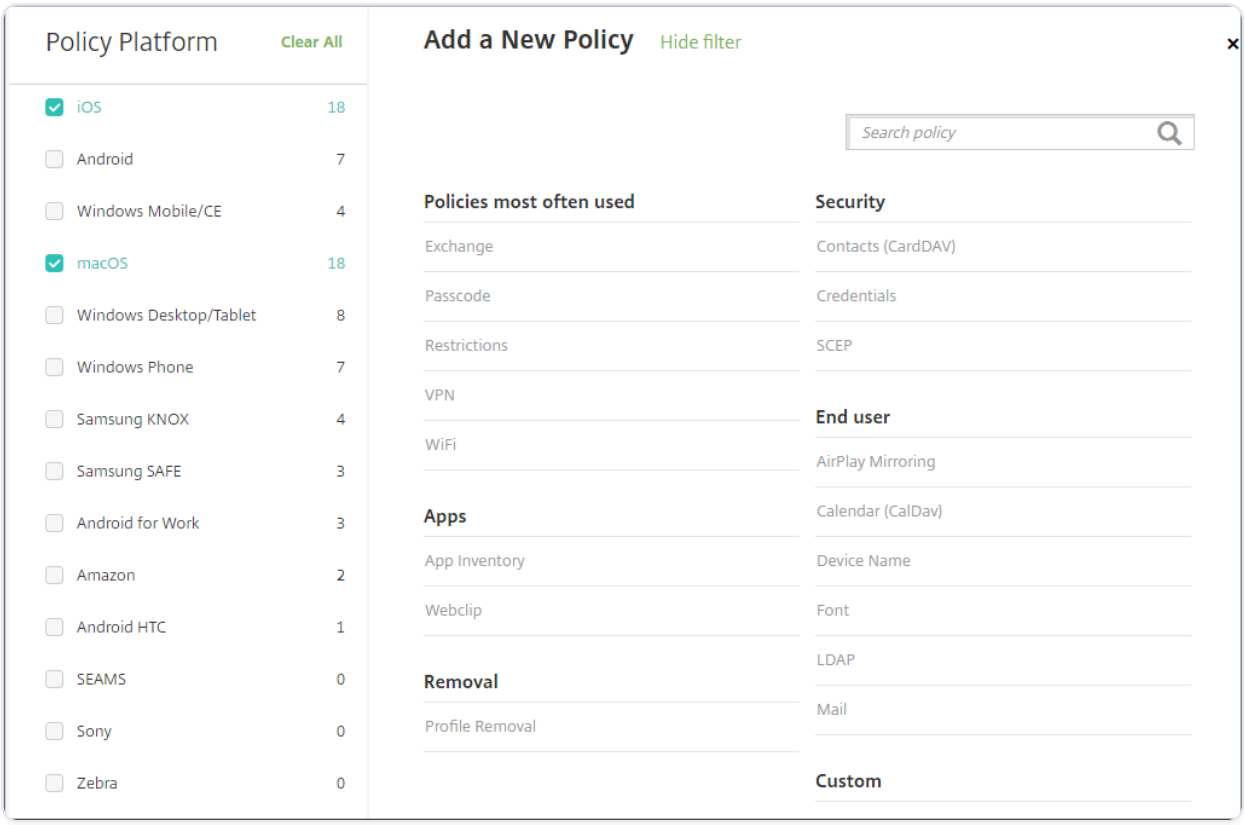


정책을 추가하려면 다음을 수행합니다.

1. **장치 정책** 페이지에서 **추가**를 클릭합니다. **새 정책 추가** 페이지가 나타납니다.



2. 하나 이상의 플랫폼을 클릭하여 선택한 플랫폼에 대한 장치 정책 목록을 봅니다. 정책 이름을 클릭하여 정책 추가를 계속합니다.



검색 상자에 정책 이름을 입력할 수도 있습니다. 입력하면 잠재적인 일치 항목이 나타납니다. 정책이 목록에 있으면 클릭합니다. 선택한 정책만 결과에 남습니다. 해당 정책의 **정책 정보** 페이지를 열려면 클릭합니다.

3. 정책에 포함할 플랫폼을 선택합니다. 선택한 플랫폼에 대한 구성 페이지는 5단계에 나타납니다.
4. **정책 정보** 페이지를 완료한 다음 **다음**을 클릭합니다. **정책 정보** 페이지는 정책 이름과 같은 정보를 수집하여 정책을 식별하고 추적하는 데 도움을 줍니다. 이 페이지는 모든 정책에 대해 유사합니다.
5. 플랫폼 페이지를 완료합니다. 플랫폼 페이지는 3단계에서 선택한 각 플랫폼에 대해 나타납니다. 이 페이지는 각 정책마다 다릅니다. 정책은 플랫폼마다 다를 수 있습니다. 모든 정책이 모든 플랫폼에 적용되는 것은 아닙니다.

   일부 페이지에는 항목 테이블이 포함되어 있습니다. 기존 항목을 삭제하려면 목록이 포함된 줄 위로 마우스를 가져간 다음 오른쪽에 있는 휴지통 아이콘을 클릭합니다. 확인 대화 상자에서 **삭제**를 클릭합니다.

   기존 항목을 편집하려면 목록이 포함된 줄 위로 마우스를 가져간 다음 오른쪽에 있는 펜 아이콘을 클릭합니다.

배포 규칙, 할당 및 일정을 구성하려면

배포 규칙 구성에 대한 자세한 내용은 리소스 배포를 참조하십시오.

1. 플랫폼 페이지에서 **배포 규칙**을 확장한 다음 다음 설정을 구성합니다. **기본** 탭이 기본적으로 나타납니다.

- 목록에서 정책을 배포할 시기를 결정하는 옵션을 클릭합니다. 모든 조건이 충족될 때 또는 모든 조건 중 하나라도 충족될 때 정책을 배포하도록 선택할 수 있습니다. 기본 옵션은 **모두**로 설정되어 있습니다.
- 조건을 정의하려면 **새 규칙**을 클릭합니다.
- 목록에서 **장치 소유권** 및 **BYOD**와 같은 조건을 클릭합니다.
- 조건을 더 추가하려면 **새 규칙**을 다시 클릭합니다. 원하는 만큼 조건을 추가할 수 있습니다.

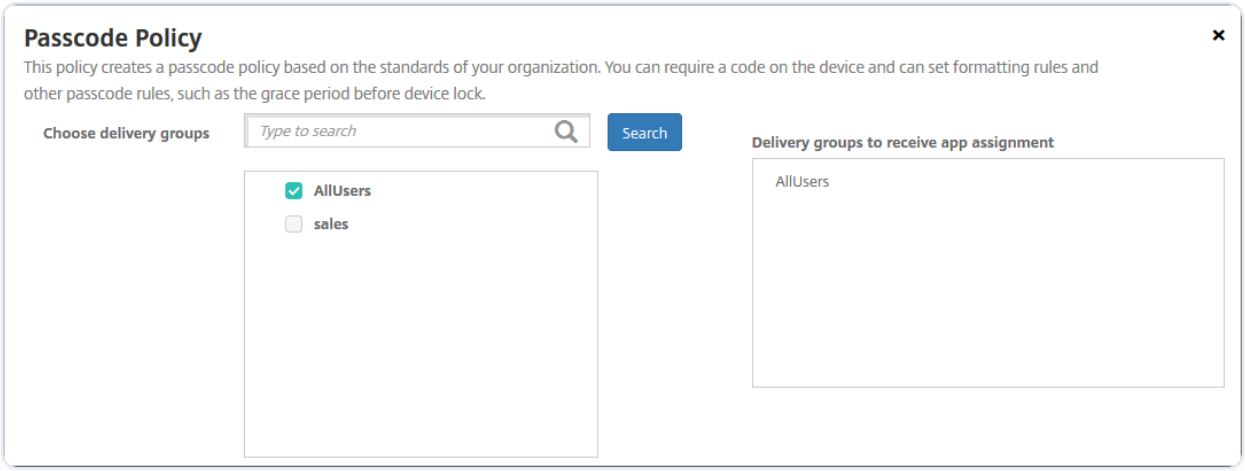
2. 규칙을 부울 옵션과 결합하려면 **고급** 탭을 클릭합니다. **기본** 탭에서 선택한 조건이 나타납니다.
3. 더 고급 부울 논리를 사용하여 규칙을 결합, 편집 또는 추가할 수 있습니다.

   - **AND**, **OR** 또는 **NOT**을 클릭합니다.
   - 목록에서 규칙에 추가할 조건을 선택합니다. 그런 다음 오른쪽에 있는 더하기 기호(**+**)를 클릭하여 조건을 규칙에 추가합니다.

     언제든지 조건을 클릭하여 선택한 다음 **편집**을 클릭하여 조건을 변경하거나 **삭제**를 클릭하여 조건을 제거할 수 있습니다.
   - 다른 조건을 추가하려면 **새 규칙**을 클릭합니다.

4. **다음**을 클릭하여 다음 플랫폼 페이지로 이동하거나, 모든 플랫폼 페이지가 완료되면 **할당** 페이지로 이동합니다.
5. **할당** 페이지에서 정책을 적용할 배달 그룹을 선택합니다. 배달 그룹을 클릭하면 해당 그룹이 **앱 할당을 받을 배달 그룹** 상자에 나타납니다.

   앱 할당을 받을 배달 그룹은 배달 그룹을 선택해야 나타납니다.

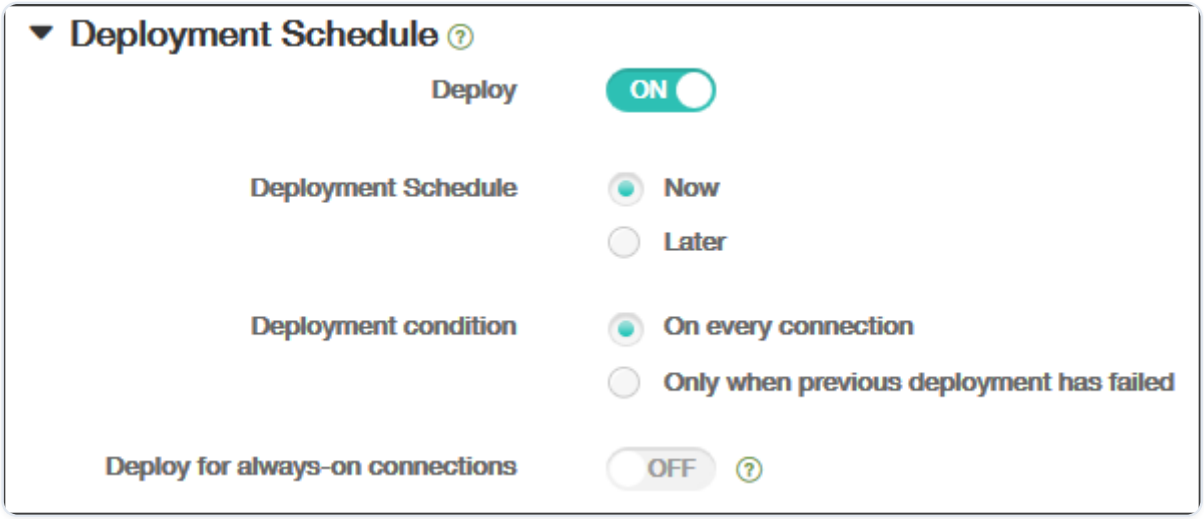


6. **할당** 페이지에서 **배포 일정**을 확장한 다음 다음 설정을 구성합니다.

   - **배포** 옆에서 **켜기**를 클릭하여 배포를 예약하거나 **끄기**를 클릭하여 배포를 방지합니다. 기본 옵션은 **켜기**로 설정되어 있습니다.

- **배포 일정** 옆에서 **지금** 또는 **나중에**를 클릭합니다. 기본 옵션은 **지금**으로 설정되어 있습니다.
- **나중에**를 클릭한 경우, 달력 아이콘을 클릭한 다음 배포 날짜와 시간을 선택합니다.
- **배포 조건** 옆에서 **모든 연결 시**를 클릭하거나 **이전 배포가 실패한 경우에만**을 클릭합니다. 기본 옵션은 **모든 연결 시**로 설정되어 있습니다.
- **항상 연결 배포** 옆에서 **켜기** 또는 **끄기**를 클릭합니다. 기본 옵션은 **끄기**로 설정되어 있습니다.

> **참고:**
>
> 이 옵션은 **설정 > 서버 속성**에서 백그라운드 배포 키 예약을 구성한 경우에 적용됩니다. 항상 연결 옵션은 iOS 장치에서는 사용할 수 없습니다.
>
> 구성하는 배포 일정은 모든 플랫폼에서 동일합니다. 변경 사항은 **항상 연결 배포**를 제외하고 모든 플랫폼에 적용되며, 이는 iOS에는 적용되지 않습니다.



7. **저장**을 클릭합니다.

   정책이 **장치 정책** 테이블에 나타납니다.

장치에서 장치 정책 제거

디바이스에서 디바이스 정책을 제거하는 단계는 플랫폼에 따라 다릅니다.

- 안드로이드

  Android 디바이스에서 디바이스 정책을 제거하려면 XenMobile 제거 디바이스 정책을 사용하십시오. 자세한 내용은 XenMobile 제거 디바이스 정책을 참조하십시오.

- iOS 및 macOS

  iOS 또는 macOS 디바이스에서 디바이스 정책을 제거하려면 프로필 제거 디바이스 정책을 사용하십시오. iOS 및 macOS 디바이스에서는 모든 정책이 MDM 프로필의 일부입니다. 따라서 제거하려는 정책에 대해서만 프로필 제거 디바이스 정책을 만들 수 있습니다. 나머지 정책과 프로필은 디바이스에 남아 있습니다. 자세한 내용은 프로필 제거 디바이스 정책을 참조하십시오.

- Windows 10 그리고 Windows 11

  Windows 데스크톱 또는 태블릿 디바이스에서 디바이스 정책을 직접 제거할 수 없습니다. 그러나 다음 방법 중 하나를 사용할 수 있습니다.

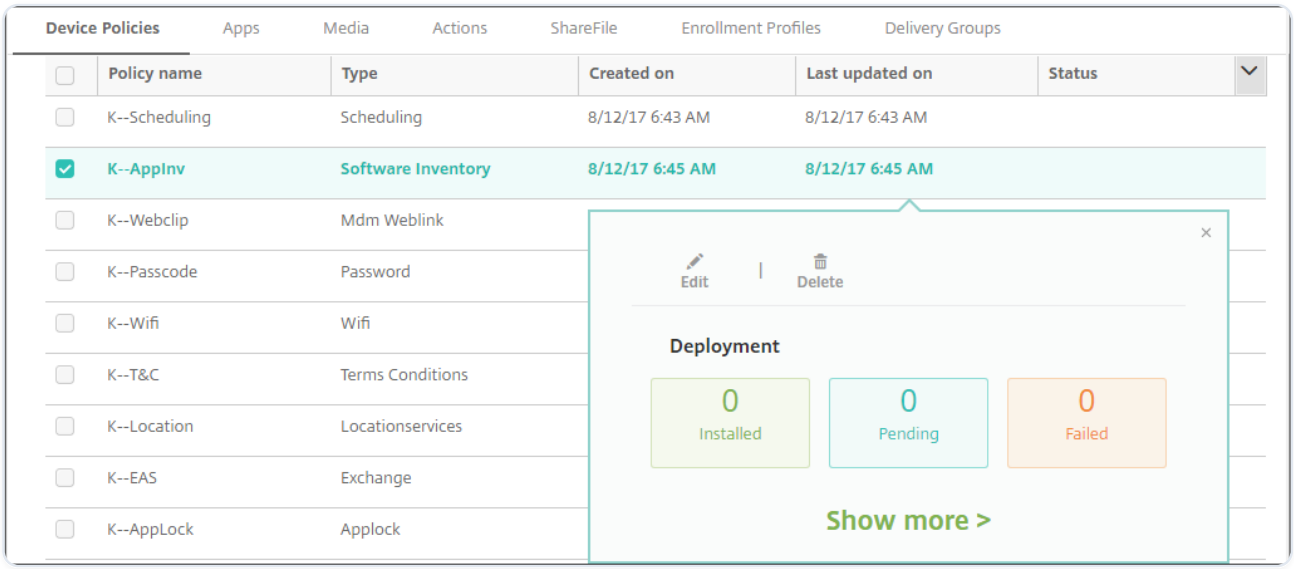
  - 디바이스 등록을 취소한 다음 새 정책 세트를 디바이스로 푸시합니다. 그러면 사용자가 계속하려면 다시 등록해야 합니다.
  - 특정 디바이스를 선택적으로 초기화하기 위해 보안 작업을 푸시합니다. 이 작업은 디바이스에서 모든 회사 앱과 데이터를 제거합니다. 그런 다음 해당 디바이스만 포함하는 전달 그룹에서 디바이스 정책을 제거하고 전달 그룹을 디바이스로 푸시합니다. 그러면 사용자가 계속하려면 다시 등록해야 합니다.

- 크롬 OS

  Chrome OS 디바이스에서 디바이스 정책을 제거하려면 해당 디바이스만 포함하는 전달 그룹에서 디바이스 정책을 제거할 수 있습니다. 그런 다음 전달 그룹을 디바이스로 푸시합니다.

디바이스 정책 편집

정책을 편집하려면 정책 옆의 확인란을 선택하여 정책 목록 위에 옵션 메뉴를 표시합니다. 또는 목록에서 정책을 클릭하여 목록 오른쪽에 옵션 메뉴를 표시합니다.



정책 세부 정보를 보려면 **자세히 보기**를 클릭합니다.

장치 정책의 모든 설정을 편집하려면 **편집**을 클릭합니다.

삭제를 클릭하면 확인 대화 상자가 나타납니다. 정책을 삭제하려면 **삭제**를 다시 클릭합니다.

정책 배포 상태 확인

구성 > 장치 정책 페이지에서 정책 행을 클릭하여 배포 상태를 확인합니다.

장치 정책 배포 상태 화면(/en-us/xenmobile/server/media/check-deployment-status.png)

정책 배포가 보류 중인 경우 사용자는 **기본 설정 > 장치 정보 > 정책 새로 고침**을 탭하여 Secure Hub에서 정책을 새로 고칠 수 있습니다.

추가된 장치 정책 목록 필터링

정책 유형, 플랫폼 및 연결된 전달 그룹별로 추가된 정책 목록을 필터링할 수 있습니다. **구성 > 장치 정책** 페이지에서 **필터 표시**를 클릭합니다. 목록에서 보려는 항목의 확인란을 선택합니다.

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/configure-device-policies-filtered.png)

필터를 저장하려면 **이 보기 저장**을 클릭합니다. 그러면 필터 이름이 **이 보기 저장** 버튼 아래의 버튼에 나타납니다.

장치 정책 요약

장치 정책 이름	장치 정책 설명
AirPlay 미러링	특정 AirPlay 장치(예: 다른 Mac 컴퓨터)를 iOS 장치에 추가합니다. 감독되는 장치에 대한 허용 목록에 장치를 추가하는 옵션도 있습니다. 이 옵션은 사용자를 허용 목록에 있는 AirPlay 장치로만 제한합니다.
AirPrint	iOS 장치의 AirPrint 프린터 목록에 AirPrint 프린터를 추가합니다. 이 정책을 사용하면 프린터와 장치가 서로 다른 서브넷에 있는 환경을 더 쉽게 지원할 수 있습니다.
Android Enterprise 앱 권한	작업 프로필 내 Android Enterprise 앱에 대한 요청이 Google에서 “위험한” 권한이라고 부르는 것을 처리하는 방법을 구성합니다.
Android Enterprise 앱 제한	Android 앱과 관련된 제한 사항을 업데이트합니다.

장치 정책 이름	장치 정책 설명
APN	특정 통신사의 GPRS(General Packet Radio Service)에 장치를 연결하는 데 사용되는 설정을 결정합니다. 이 설정은 대부분의 최신 휴대폰에 이미 정의되어 있습니다. 조직에서 모바일 장치에서 인터넷에 연결하기 위해 소비자 APN을 사용하지 않는 경우 이 정책을 사용하십시오.
앱 액세스	장치에서 필수, 선택 사항 또는 금지된 앱 목록을 정의합니다. 그런 다음 해당 앱 목록에 대한 장치 규정 준수에 반응하는 자동화된 작업을 생성할 수 있습니다.
앱 속성	iOS 장치에 대해 관리되는 앱 번들 ID 또는 앱별 VPN 식별자와 같은 속성을 지정합니다.
앱 구성	관리형 구성을 지원하는 앱의 다양한 설정 및 동작을 원격으로 구성합니다. 이를 위해 XML 구성 파일(속성 목록 또는 plist라고 함)을 iOS 장치에 배포합니다. 또는 Windows 10 휴대폰, Windows 10 또는 Windows 11을 실행하는 데스크톱 또는 태블릿 장치에 키/값 쌍을 배포합니다.
앱 인벤토리	관리되는 장치의 앱 인벤토리를 수집합니다. XenMobile은 이 인벤토리를 해당 장치에 배포된 앱 액세스 정책과 비교합니다. 이러한 방식으로 앱 액세스 허용 또는 차단 목록에 있는 앱을 감지하고 올바르게 조치할 수 있습니다.
앱 잠금	사용자가 iOS 또는 특정 Android 장치에서 실행할 수 있거나 실행할 수 없는 앱 목록을 정의합니다.
앱 네트워크 사용량	iOS 장치에서 관리되는 앱이 셀룰러 데이터 네트워크와 같은 네트워크를 사용하는 방법을 지정하는 네트워크 사용 규칙을 설정합니다. 이 규칙은 관리되는 앱에만 적용됩니다. 관리되는 앱은 XenMobile을 통해 사용자 장치에 배포하는 앱입니다.
앱 제거	사용자 장치에서 앱을 제거합니다.
앱 알림	iOS 사용자가 지정된 앱에서 알림을 받는 방법을 제어합니다.

장치 정책 이름	장치 정책 설명
관리되는 앱 자동 업데이트	Android Enterprise 장치에서 설치된 관리되는 앱이 업데이트되는 방식을 제어합니다.
BitLocker	Windows 10 및 Windows 11 장치의 BitLocker 인터페이스에서 사용할 수 있는 설정을 구성합니다.
캘린더 (CalDav)	iOS 또는 macOS 장치에 캘린더 (CalDAV) 계정을 추가합니다. CalDAV 계정을 통해 사용자는 CalDAV를 지원하는 모든 서버와 일정 데이터를 동기화할 수 있습니다.
셀룰러	셀룰러 네트워크 설정을 구성합니다.
연결 관리자	인터넷 및 사설 네트워크에 자동으로 연결하는 앱의 연결 설정을 지정합니다. 이 정책은 Windows Pocket PC에서만 사용할 수 있습니다.
연락처 (CardDAV)	iOS 또는 macOS 장치에 iOS 연락처(CardDAV) 계정을 추가합니다. CardDAV 계정을 통해 사용자는 CardDAV를 지원하는 모든 서버와 연락처 데이터를 동기화할 수 있습니다.
OS 업데이트 제어	지원되는 감독 대상 장치에 최신 OS 업데이트를 배포합니다.
자격 증명	XenMobile에서 PKI 구성과 통합 인증을 활성화합니다. 예를 들어, PKI 엔터티, 키 저장소, 자격 증명 공급자 또는 서버 인증서를 사용합니다.
사용자 지정 XML	장치 프로비저닝, 장치 기능 활성화, 장치 구성 및 오류 관리와 같은 기능을 사용자 지정합니다.
디펜더	Windows 10 및 Windows 11 데스크톱 및 태블릿용 Windows Defender 설정을 구성합니다.
장치 상태 증명	Windows 10 및 Windows 11 장치가 상태를 보고하도록 요구합니다. 이를 위해 특정 데이터와 런타임 정보를 분석을 위해 Health Attestation Service(HAS)로 보냅니다. HAS는 장치가 XenMobile로 보내는 Health Attestation Certificate를 생성하여 반환합니다. XenMobile이 Health Attestation Certificate를 받으면 해당 인증

장치 정책 이름	장치 정책 설명
	서의 내용에 따라 구성한 자동 작업을 배포할 수 있습니다.
장치 이름	장치를 식별할 수 있도록 iOS 및 macOS 장치에 이름을 설정합니다. 매크로, 텍스트 또는 이 둘의 조합을 사용하여 장치 이름을 정의할 수 있습니다.
교육 구성	Apple Education과 함께 사용할 강사 및 학생 장치를 구성합니다. 강사가 Classroom 앱을 사용하는 경우 교육 구성 장치 정책이 필요합니다.
익스체인지	장치의 기본 이메일 클라이언트에 ActiveSync 이메일을 활성화합니다.
파일	사용자에게 특정 기능을 수행하는 스크립트 파일을 XenMobile에 추가합니다. 또는 Android 장치 사용자가 자신의 장치에서 액세스할 수 있도록 하려는 문서 파일을 추가할 수 있습니다. 파일을 추가할 때 장치에 파일을 저장할 디렉터리를 지정할 수도 있습니다.
FileVault	이 정책을 통해 등록된 macOS 장치에서 FileVault 장치 암호화를 활성화할 수 있습니다. 또한 사용자가 로그인하는 동안 FileVault 설정을 건너뛸 수 있는 횟수를 제어할 수 있습니다. macOS 10.7 이상에서 사용할 수 있습니다.
글꼴	iOS 및 macOS 장치에 글꼴을 추가합니다. 글꼴은 TrueType(.TTF) 또는 OpenType(.OFT) 글꼴이어야 합니다. XenMobile은 글꼴 모음(.TTC 또는 .OTC)을 지원하지 않습니다.
홈 화면 레이아웃	iOS 9.3 이상 감독 장치의 iOS 홈 화면에 대한 앱 및 폴더 레이아웃을 지정합니다.
iOS 및 macOS 프로필 가져오기	iOS 및 macOS 장치용 장치 구성 XML 파일을 XenMobile로 가져옵니다. 이 파일에는 Apple Configurator를 사용하여 준비하는 장치 보안 정책 및 제한 사항이 포함되어 있습니다.
키가드 관리	사용자가 장치 키가드 및 작업 챌린지 키가드를 잠금 해제하기 전에 사용할 수 있는 기능을 제어합니다.

장치 정책 이름	장치 정책 설명
	또한 완전 관리형 및 전용 장치에 대한 장치 키가드 기능을 제어할 수 있습니다. 예를 들어, 지문 잠금 해제, 신뢰 에이전트 및 알림과 같은 잠금 화면 기능을 비활성화할 수 있습니다.
키오스크	Samsung SAFE 장치에서 앱 사용을 제한합니다. 사용 가능한 앱을 특정 앱으로 제한할 수 있습니다. 이 정책은 특정 유형 또는 클래스의 앱만 실행하도록 의도된 회사 장치에 유용합니다. 이 정책을 통해 키오스크 모드에서 장치 홈 화면 및 잠금 화면 배경 화면에 대한 사용자 지정 이미지를 선택할 수도 있습니다.
녹스 플랫폼 포 엔터프라이즈 키	필요한 Samsung Knox Platform for Enterprise (KPE) 라이선스 정보를 제공할 수 있습니다.
런처 구성	허용된 앱 및 런처 아이콘의 사용자 지정 로고 이미지와 같이 Android 장치에서 Citrix Launcher에 대한 설정을 지정합니다.
LDAP	LDAP 서버 호스트 이름과 같은 필요한 계정 정보를 포함하여 iOS 장치에 사용할 LDAP 서버에 대한 정보를 제공합니다. 이 정책은 또한 LDAP 서버를 쿼리할 때 사용할 LDAP 검색 정책 세트를 제공합니다.
위치	Secure Hub에 대해 장치에 GPS가 활성화되어 있다고 가정하고 지도에서 장치의 지리적 위치를 파악할 수 있습니다. 이 정책을 장치에 배포한 후 XenMobile Server에서 위치 찾기 명령을 보낼 수 있습니다. 그러면 장치가 위치 좌표로 응답합니다. XenMobile은 또한 지오펜싱 및 추적 정책을 지원합니다.
메일	iOS 또는 macOS 기기에서 이메일 계정을 구성합니다.
관리되는 도메인	이메일 및 Safari 브라우저에 적용되는 관리되는 도메인을 정의합니다. 관리되는 도메인은 Safari를 사용하여 도메인에서 다운로드한 문서를 어떤 앱이 열 수 있는지 제어하여 기업 데이터를 보호하는 데 도움이 됩니다. iOS 8 이상 감독 모드 기기의 경우, 사용

장치 정책 이름	장치 정책 설명
	자가 브라우저에서 문서, 첨부 파일 및 다운로드를 여는 방법을 제어하기 위해 URL 또는 하위 도메인을 지정할 수 있습니다.
MDM 옵션	감독 모드 iOS 7.0 이상 전화 기기에서 나의 iPhone 찾기 및 iPad 활성화 잠금을 관리합니다.
조직 정보	XenMobile이 iOS 기기에 배포하는 경고 메시지에 대한 조직 정보를 지정합니다.
암호	관리되는 기기에 PIN 코드 또는 암호를 적용합니다. 기기에서 암호의 복잡성과 시간 제한을 설정할 수 있습니다.
개인용 핫스팟	사용자가 Wi-Fi 네트워크 범위 내에 없을 때 인터넷에 연결할 수 있도록 허용합니다. 사용자는 개인용 핫스팟 기능을 사용하여 iOS 기기의 셀룰러 데이터 연결을 통해 연결합니다.
프로필 제거	iOS 또는 macOS 기기에서 앱 프로필을 제거합니다.
프로비저닝 프로필	기기로 보낼 엔터프라이즈 배포 프로비저닝 프로필을 지정합니다. iOS 엔터프라이즈 앱을 개발하고 코드 서명할 때 일반적으로 프로비저닝 프로필을 포함합니다. Apple은 앱이 iOS 기기에서 실행되려면 이 프로필을 요구합니다. 프로비저닝 프로필이 없거나 만료된 경우, 사용자가 앱을 열기 위해 탭하면 앱이 충돌합니다.
프로비저닝 프로필 제거	iOS 프로비저닝 프로필을 제거합니다.
프록시	iOS를 실행하는 장치에 대한 전역 HTTP 프록시 설정을 지정합니다. 장치당 하나의 전역 HTTP 프록시 정책만 배포할 수 있습니다.
제한	관리되는 장치에서 기능 및 기능을 잠그고 제어할 수 있는 수백 가지 옵션을 제공합니다. 제한 옵션의 예: 카메라 또는 마이크 비활성화, 로밍 규칙 적용, 앱 스토어와 같은 타사 서비스에 대한 액세스 적용.

장치 정책 이름	장치 정책 설명
로밍	iOS 장치에서 음성 및 데이터 로밍을 허용할지 여부를 구성합니다. 음성 로밍이 비활성화되면 데이터 로밍도 자동으로 비활성화됩니다.
스케줄링	MDM 관리, 앱 푸시 및 정책 배포를 위해 Android 장치가 XenMobile Server에 다시 연결하는 데 필요합니다. 이 정책을 장치에 보내지 않고 Google FCM을 활성화하지 않으면 장치가 서버에 다시 연결할 수 없습니다.
SCEP	iOS 및 macOS 장치가 외부 SCEP 서버에서 인증서를 검색하도록 구성합니다. XenMobile에 연결된 PKI에서 SCEP를 사용하여 장치에 인증서를 전달할 수도 있습니다. 이를 위해 분산 모드에서 PKI 엔터티 및 PKI 공급자를 생성합니다.
SSO 계정	사용자가 XenMobile 및 내부 회사 리소스에 한 번만 로그인하여 액세스할 수 있도록 단일 Sign-On(SSO) 계정을 생성합니다. 사용자는 장치에 어떤 자격 증명도 저장할 필요가 없습니다. XenMobile은 App Store의 앱을 포함하여 앱 전체에서 SSO 계정에 대한 엔터프라이즈 사용자 자격 증명을 사용합니다. 이 정책은 Kerberos 인증과 호환됩니다. iOS에서 사용할 수 있습니다.
구독 캘린더	iOS 장치의 캘린더 목록에 구독한 캘린더를 추가합니다. 사용자 장치의 구독 캘린더 목록에 추가하기 전에 캘린더를 구독해야 합니다.
이용 약관	사용자가 회사 네트워크 연결을 관리하는 회사별 정책에 동의하도록 요구합니다. 사용자가 XenMobile에 장치를 등록할 때, 장치를 등록하려면 이용 약관에 동의해야 합니다. 이용 약관을 거부하면 등록 프로세스가 취소됩니다.
터널	원격 지원에만 사용됩니다. 원격 지원을 통해 헬프데스크 담당자는 관리되는 Windows CE 및 Android 모바일 장치를 원격으로 제어할 수 있습니다. 클러스터링된 온프레미스 XenMobile Server 배포에서는 원격 지원을 사용할 수 없습니다. Remote Support는 January 1, 2019부터 신규 고객에게 더

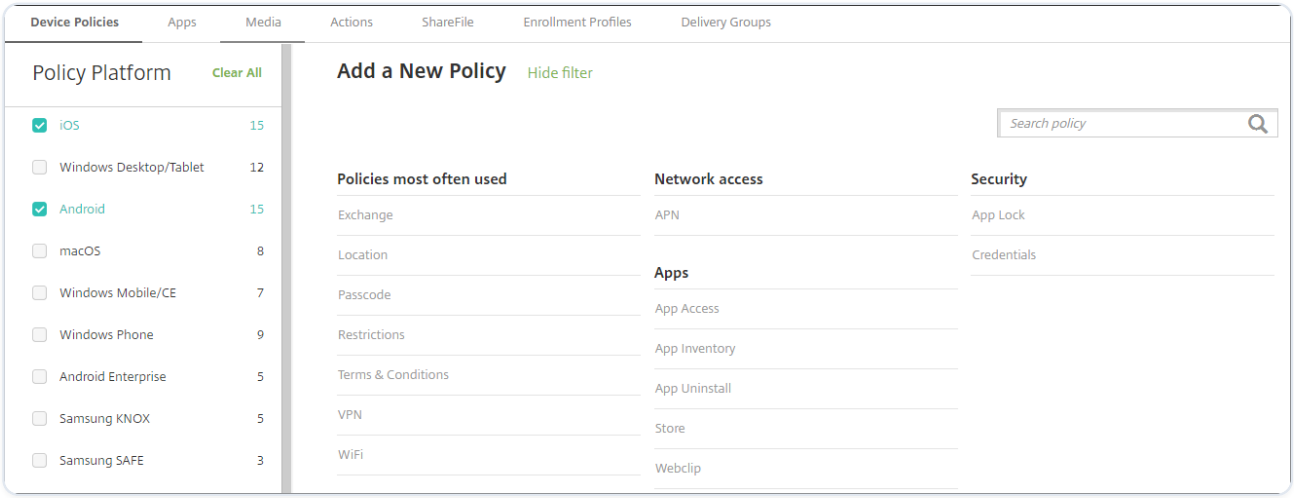
장치 정책 이름	장치 정책 설명
	이상 제공되지 않습니다. 기존 고객은 계속 제품을 사용할 수 있지만, Citrix는 개선 사항이나 수정 사항을 제공하지 않습니다.
VPN	레거시 VPN 게이트웨이 기술을 사용하는 백엔드 시스템에 대한 액세스를 제공합니다. 이 정책은 장치에 배포할 수 있는 VPN 게이트웨이 연결 세부 정보를 제공합니다. XenMobile은 Cisco AnyConnect, Juniper 및 Citrix VPN을 포함한 여러 VPN 공급자를 지원합니다. VPN 게이트웨이가 이 옵션을 지원하는 경우 이 정책을 CA에 연결하고 온디맨드 VPN을 활성화할 수 있습니다.
배경 화면	iOS 장치의 잠금 화면, 홈 화면 또는 둘 다에 배경 화면을 설정하기 위해 .png 또는 .jpg 파일을 추가합니다. iPad와 iPhone에서 다른 배경 화면을 사용하려면 다른 배경 화면 정책을 만들고 해당 사용자에게 배포합니다.
웹 콘텐츠 필터	iOS 장치에서 웹 콘텐츠를 필터링합니다. XenMobile은 Apple 자동 필터 기능과 허용 및 차단 목록에 추가하는 사이트를 사용합니다. iOS 감독 장치에서만 사용할 수 있습니다.
웹 클립	웹 사이트에 대한 바로 가기 또는 웹 클립을 배치하여 사용자 장치의 앱과 함께 표시되도록 합니다. iOS, macOS 및 Android 장치의 웹 클립을 나타내는 사용자 지정 아이콘을 지정할 수 있습니다. Windows 태블릿은 레이블과 URL만 필요합니다.
와이파이	관리자가 Wi-Fi 라우터 세부 정보를 관리되는 장치에 배포할 수 있도록 합니다. 라우터 세부 정보에는 SSID, 인증 데이터 및 구성 데이터가 포함됩니다.
Windows 정보 보호	정책에 설정한 적용 수준에서 Windows 정보 보호가 필요한 앱을 지정합니다. 이 정책은 Windows 10 및 Windows 11 감독 대상 장치용입니다.
XenMobile 스토어	XenMobile Store 웹 클립이 사용자 장치의 홈 화면에 표시되는지 여부를 지정합니다.

장치 정책 이름	장치 정책 설명
XenMobile 옵션	Android 장치에서 XenMobile에 연결할 때 Secure Hub 동작을 구성합니다.
XenMobile 제거	Android 및 Windows Mobile/CE 장치에서 XenMobile을 제거합니다. 배포되면 이 정책은 배포 그룹의 모든 장치에서 XenMobile을 제거합니다.

플랫폼별 장치 정책

플랫폼별로 사용 가능한 정책을 보려면 다음을 수행합니다.

1. XenMobile® 콘솔에서 **구성 > 장치 정책**으로 이동합니다.
2. **추가**를 클릭합니다.
3. 각 장치 플랫폼이 **정책 플랫폼** 창의 목록에 나타납니다. 해당 창이 열려 있지 않으면 **필터 표시**를 클릭합니다.
4. 플랫폼에 사용 가능한 모든 정책 목록을 보려면 해당 플랫폼을 선택합니다. 여러 플랫폼에 사용 가능한 정책 목록을 보려면 해당 플랫폼 각각을 선택합니다. 정책은 선택한 각 플랫폼에 적용되는 경우에만 목록에 나타납s니다.



최신 버전의 XenMobile은 다음 플랫폼에 대한 장치 정책을 지원합니다.

- 아마존
- 안드로이드
- 안드로이드 엔터프라이즈
- 안드로이드 지브라
- iOS

- macOS
- 삼성 SAFE
- 삼성 녹스
- 윈도우 10 및 윈도우 11 데스크톱/태블릿

XenMobile 최신 버전에서 지원되는 장치에 대한 자세한 내용은 지원되는 장치 플랫폼을 참조하십시오.

> **참고:**
>
> 환경이 그룹 정책 개체(GPO)로 구성된 경우:
>
> Windows 10 및 Windows 11용 XenMobile 장치 정책을 구성할 때 다음 규칙을 염두에 두십시오. 하나 이상의 등록된 장치에서 정책이 충돌하는 경우 GPO에 맞춰진 정책이 우선합니다.

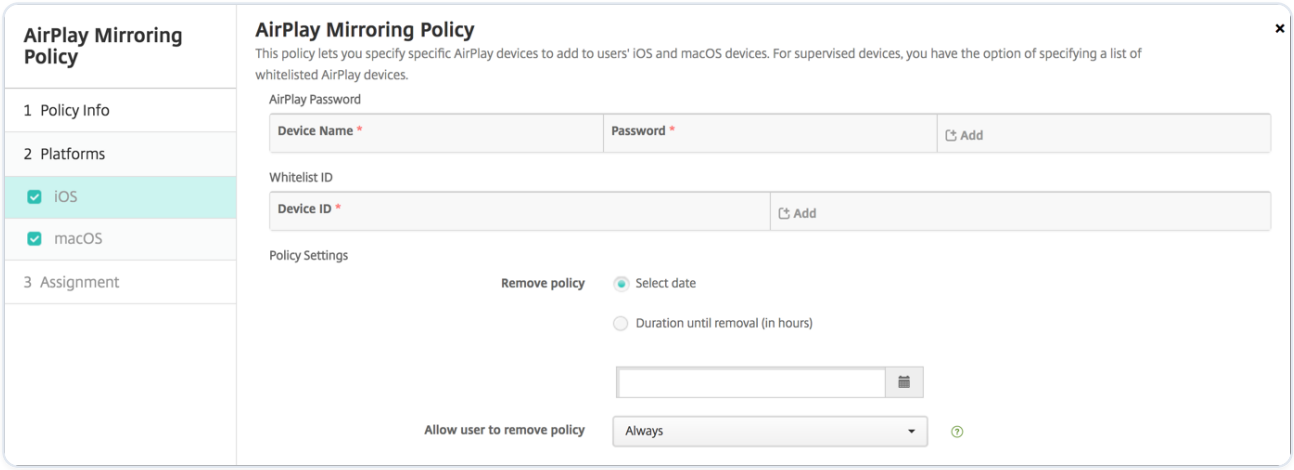
AirPlay 미러링 장치 정책

Apple AirPlay 기능을 사용하면 사용자가 장치 디스플레이에 표시되는 내용을 다른 Mac 컴퓨터에 정확히 미러링할 수 있습니다.

XenMobile에서 장치 정책을 추가하여 특정 AirPlay 장치(예: 다른 Mac 컴퓨터)를 iOS 장치에 추가할 수 있습니다. 또한 감독 대상 장치에 대한 허용 목록에 장치를 추가하는 옵션도 있으며, 이는 사용자를 허용 목록에 있는 AirPlay 장치로만 제한합니다. 장치를 감독 모드로 전환하는 방법에 대한 자세한 내용은 Apple Configurator를 사용하여 iOS 장치를 감독 모드로 전환하는 방법을 참조하십시오.

> **참고:**
>
> 계속하기 전에 추가하려는 모든 장치의 장치 ID와 암호를 준비해야 합니다.
>
> 이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

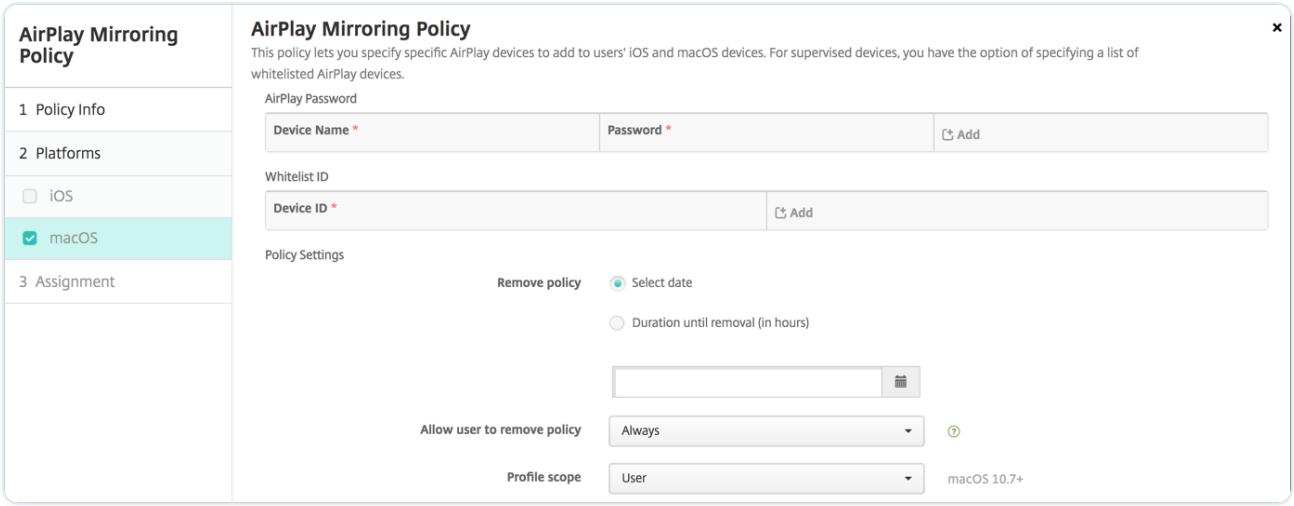


- **AirPlay 암호:** 추가하려는 각 장치에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **장치 ID:** 하드웨어 주소(MAC 주소)를 xx:xx:xx:xx:xx:xx 형식으로 입력합니다. 이 필드는 대소문자를 구분하지 않습니다.
  - **암호:** 장치에 대한 선택적 암호를 입력합니다.
  - 장치를 추가하려면 **추가**를 클릭하고, 장치 추가를 취소하려면 **취소**를 클릭합니다.
- **화이트리스트 ID:** 이 목록은 감독되지 않은 장치에는 무시됩니다. 이 목록의 장치 ID는 사용자 장치에서 사용할 수 있는 유일한 AirPlay 장치입니다. 목록에 추가하려는 각 AirPlay 장치에 대해 **추가**를 클릭한 다음 다음을 수행합니다.

> **참고:**
>
> XenMobile® Server 콘솔에는 "블랙리스트" 및 "화이트리스트"라는 용어가 포함되어 있습니다. 다음 릴리스에서는 이러한 용어를 "차단 목록" 및 "허용 목록"으로 변경할 예정입니다.

  - **장치 ID:** xx:xx:xx:xx:xx:xx 형식으로 장치 ID를 입력합니다. 이 필드는 대소문자를 구분하지 않습니다.
  - **추가**를 클릭하여 장치를 추가하거나 **취소**를 클릭하여 장치 추가를 취소합니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.

macOS 설정



- **AirPlay 암호:** 추가하려는 각 장치에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **장치 ID:** xx:xx:xx:xx:xx:xx 형식으로 하드웨어 주소(MAC 주소)를 입력합니다. 이 필드는 대소문자를 구분하지 않습니다.
  - **암호:** 장치에 대한 선택적 암호를 입력합니다.
  - **추가**를 클릭하여 장치를 추가하거나 **취소**를 클릭하여 장치 추가를 취소합니다.
- **화이트리스트 ID:** 이 목록은 감독되지 않은 장치에는 무시됩니다. 이 목록의 장치 ID는 사용자 장치에서 사용할 수 있는 유일한 AirPlay 장치입니다. 목록에 추가하려는 각 AirPlay 장치에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **장치 ID:** xx:xx:xx:xx:xx:xx 형식으로 장치 ID를 입력합니다. 이 필드는 대소문자를 구분하지 않습니다.
  - **추가**를 클릭하여 장치를 추가하거나 **취소**를 클릭하여 장치 추가를 취소합니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책이 제거될 때까지의 시간을 숫자로 입력합니다.
  - **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다. **암호 필요**를 선택한 경우, **제거 암호** 필드에 암호를 입력합니다.
  - **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 또는 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

AirPrint 장치 정책

XenMobile®에서 장치 정책을 추가하여 iOS 장치의 AirPrint 프린터 목록에 AirPrint 프린터를 추가할 수 있습니다. 이 정책을 사용하면 프린터와 장치가 서로 다른 서브넷에 있는 환경을 더 쉽게 지원할 수 있습니다.

이 정책은 iOS 7.0 이상에 적용됩니다.

> **참고:**
>
> 각 프린터의 IP 주소와 리소스 경로를 확인하십시오.
>
> 이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **AirPrint 대상:** 추가하려는 각 AirPrint 대상에 대해 **추가**를 클릭한 다음 다음을 수행하십시오.
  - **IP 주소:** AirPrint 프린터 IP 주소를 입력합니다.
  - **리소스 경로:** 프린터와 연결된 리소스 경로를 입력합니다. 이 값은 _ipps.tcp Bonjour 레코드의 매개변수에 해당합니다. 예를 들어, printers/Canon_MG5300_series 또는 printers/Xerox_Phaser_7600입니다.
  - 프린터를 추가하려면 **저장**을 클릭하고, 프린터 추가를 취소하려면 **취소**를 클릭합니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

Android Enterprise 앱 권한

작업 프로필 내 Android Enterprise 앱에 대한 요청이 Google이 “위험한” 권한이라고 부르는 것을 처리하는 방식을 구성할 수 있습니다. 사용자가 앱의 권한 요청을 허용할지 거부할지 여부를 제어합니다. 이 기능은 Android 7.0 이상을 실행하는 장치에 적용됩니다.

Google은 위험한 권한을 앱이 사용자의 개인 정보와 관련된 데이터 또는 리소스에 액세스하거나 사용자의 저장된 데이터 또는 다른 앱의 작동에 잠재적으로 영향을 미칠 수 있도록 하는 권한으로 정의합니다. 예를 들어, 사용자의 연락처를 읽을 수 있는 기능은 위험한 권한입니다.

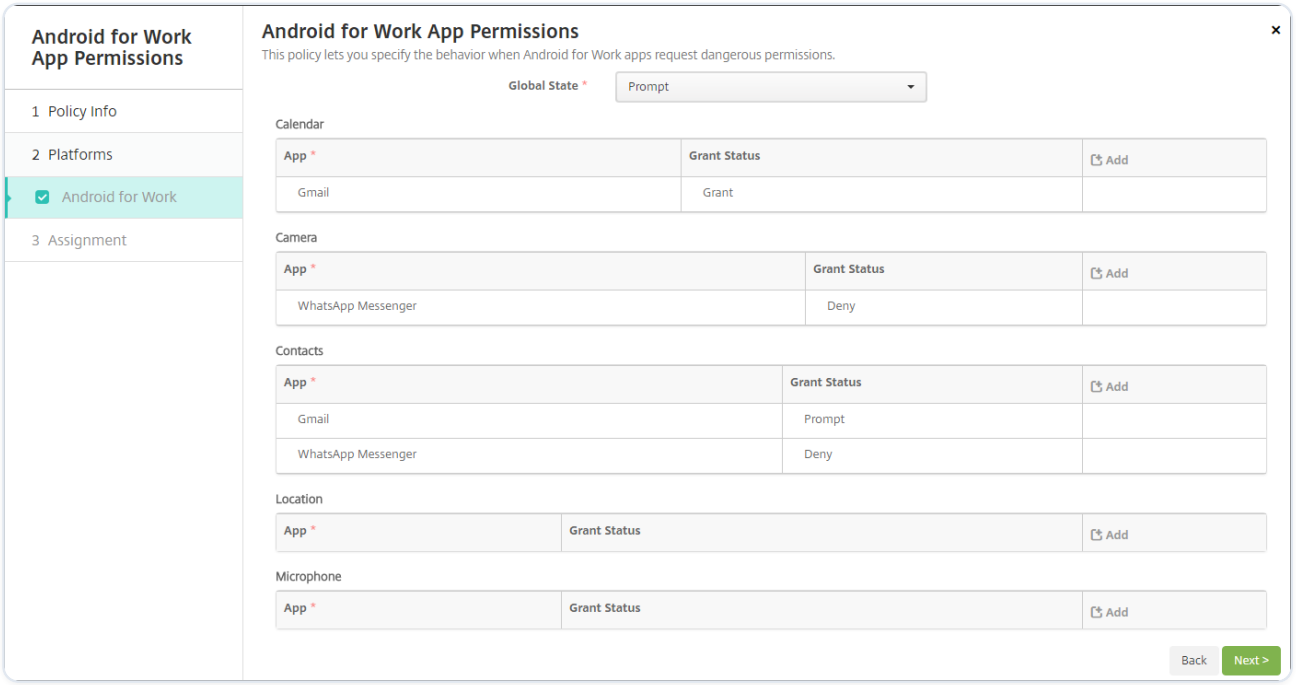
작업 프로필 내 Android Enterprise 앱에 대한 모든 위험한 권한 요청의 동작을 제어하는 전역 상태를 구성할 수 있습니다. 또한 Google이 정의한 대로 각 앱에 대한 개별 권한 그룹의 위험한 권한 요청 동작을 제어할 수 있습니다. 이러한 개별 설정은 전역 상태를 재정의합니다.

Google이 권한 그룹을 정의하는 방법에 대한 자세한 내용은 이 Android 개발자 가이드의 “권한 그룹”을 참조하십시오.

기본적으로 사용자는 위험한 권한 요청을 허용하거나 거부하도록 요청받습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

안드로이드 엔터프라이즈 설정



- **전역 상태:** 모든 위험한 권한 요청의 동작을 제어합니다. 목록에서 **프롬프트**, **허용** 또는 **거부**를 클릭합니다.
    - **프롬프트:** 사용자는 위험한 권한 요청을 허용하거나 거부하도록 요청받습니다.
    - **허용:** 모든 위험한 권한 요청이 허용됩니다. 사용자에게는 프롬프트가 표시되지 않습니다.
    - **거부:** 모든 위험한 권한 요청이 거부됩니다. 사용자에게는 프롬프트가 표시되지 않습니다.

  기본값은 **프롬프트**입니다.

- 각 앱의 각 권한 그룹에 대한 개별 동작을 설정합니다. 권한 그룹의 동작을 구성하려면: **추가**를 클릭합니다. **앱**에서 목록에서 앱을 선택합니다. Android Enterprise 시스템 앱을 구성하는 경우 **새로 추가**를 클릭하고 제한 장치 정책에서 활성화한 애플리케이션 패키지 이름을 입력합니다. 권한 상태에서 **프롬프트**, **허용** 또는 **거부**를 선택합니다. 이 권한 상태는 전역 상태를 재정의합니다.

  - **프롬프트:** 사용자는 이 앱에 대한 이 권한 그룹의 위험한 권한 요청을 허용하거나 거부하라는 메시지를 받습니다.
  - **허용:** 이 앱에 대한 이 권한 그룹의 위험한 권한 요청이 허용됩니다. 사용자에게 메시지가 표시되지 않습니다.

    > **참고:**
    >
    > **프로필 소유자** 모드에 등록된 장치의 경우, 장치가 Android 12 이상에서 실행 중인 경우 카메라, 위치, 마이크 및 센서에 대해 **허용** 권한이 적용되지 않습니다.

  - **거부:** 이 앱에 대한 이 권한 그룹의 위험한 권한 요청이 거부됩니다. 사용자에게 메시지가 표시되지 않습니다.

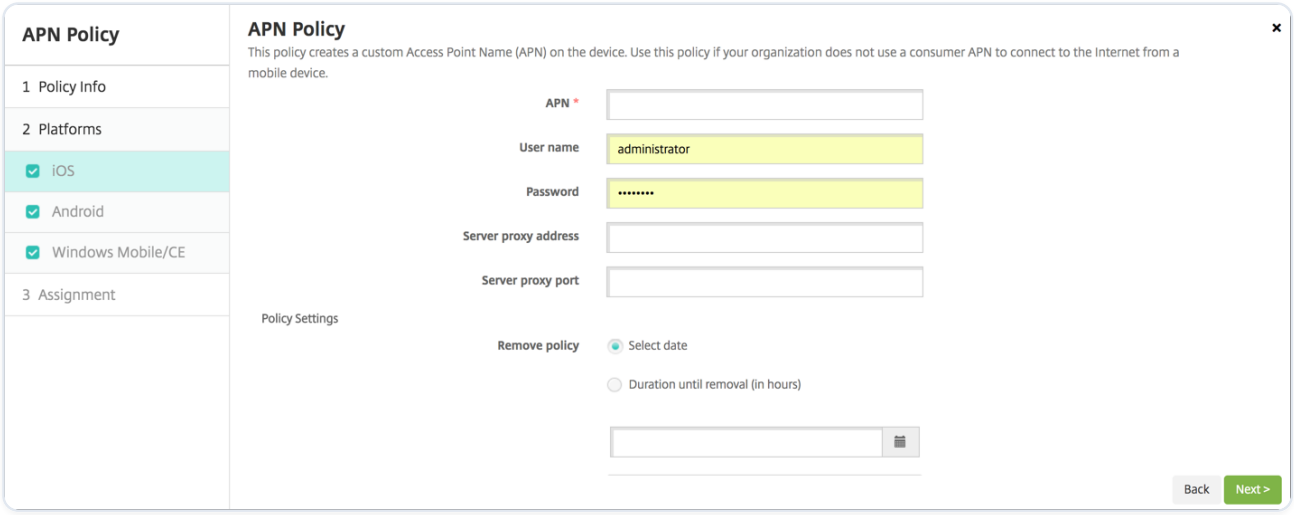
  기본값은 **프롬프트**입니다.
- 앱 및 허용 상태 옆에 있는 **저장**을 클릭합니다.
- 권한 그룹에 앱을 더 추가하려면 **추가**를 다시 클릭하고 이 단계를 반복합니다.
- 원하는 모든 권한 그룹에 대한 허용 상태 설정을 마쳤으면 **다음**을 클릭합니다.

APN 장치 정책

iOS 및 Android 장치에 대한 사용자 지정 APN(액세스 포인트 이름) 장치 정책을 추가할 수 있습니다. 이 정책은 조직에서 모바일 장치에서 인터넷에 연결하기 위해 소비자 APN을 사용하지 않는 경우에 사용합니다. APN 정책은 장치를 특정 전화 통신사의 GPRS(General Packet Radio Service)에 연결하는 데 사용되는 설정을 결정합니다. 이 설정은 대부분의 최신 전화기에서 이미 정의되어 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



- **APN:** 액세스 포인트의 이름을 입력합니다. 이 APN 이름은 허용되는 iOS APN과 일치해야 하며, 그렇지 않으면 정책이 실패합니다.
- **사용자 이름:** 이 문자열은 이 APN의 사용자 이름을 지정합니다. 사용자 이름이 없으면 장치에서 프로필 설치 중에 문자열을 묻는 메시지를 표시합니다.
- **암호:** 이 APN의 사용자 암호입니다. 난독화를 위해 암호는 인코딩됩니다. 페이로드에 없으면 장치에서 프로필 설치 중에 암호를 묻는 메시지를 표시합니다.
- **서버 프록시 주소:** APN 프록시의 IP 주소 또는 URL입니다.
- **서버 프록시 포트:** APN 프록시의 포트 번호입니다. 서버 프록시 주소를 입력한 경우 이 서버 프록시 포트 번호가 필요합니다.
- **정책 설정**에서 **정책 제거** 옆에 있는 **날짜 선택** 또는 **제거까지의 기간(시간)**을 클릭합니다.
    - **날짜 선택**을 클릭한 경우 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **사용자가 정책을 제거하도록 허용** 목록에서 **항상**, **암호 필요** 또는 **안 함**을 클릭합니다.
    - **암호 필요**를 클릭한 경우 **제거 암호** 옆에 필요한 암호를 입력합니다.
- **정책 설정**
    - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
        - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
        - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

Android 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/devicepolicy-apn-android.png)

- **APN:** 액세스 포인트의 이름을 입력합니다. 이 APN 이름은 허용되는 Android APN과 일치해야 하며, 그렇지 않으면 정책이 실패합니다.
- **사용자 이름:** 이 문자열은 이 APN의 사용자 이름을 지정합니다. 사용자 이름이 없으면 장치는 프로필 설치 중에 문자열을 요청합니다.
- **암호:** 이 APN 사용자의 암호입니다. 난독화를 위해 암호는 인코딩됩니다. 페이로드에 없으면 장치는 프로필 설치 중에 암호를 요청합니다.
- **서버:** 스마트폰 이전에 존재했던 이 설정은 일반적으로 비어 있습니다. 표준 웹사이트에 액세스하지 못할 수 있는 휴대폰을 위한 무선 애플리케이션 프로토콜(WAP) 게이트웨이 서버를 참조합니다.
- **APN 유형:** 이 설정은 액세스 포인트에 대한 통신사의 의도된 사용과 일치해야 합니다. APN 서비스 지정자의 쉼표로 구분된 문자열이며 무선 통신사의 게시된 정의와 일치해야 합니다. 예시는 다음과 같습니다.
  - *: 모든 트래픽은 이 액세스 포인트를 통해 전달됩니다.
  - mms: 멀티미디어 트래픽은 이 액세스 포인트를 통해 전달됩니다.
  - default: 멀티미디어를 포함한 모든 트래픽은 이 액세스 포인트를 통해 전달됩니다.
  - supl: Secure User Plane Location은 보조 GPS와 관련이 있습니다.
  - dun: 전화 접속 네트워킹은 오래되었으며 거의 사용되지 않습니다.
  - hipri" 고우선순위 네트워킹.
  - fota: 무선 펌웨어(Firmware over the air)는 펌웨어 업데이트를 수신하는 데 사용됩니다.
- **인증 유형:** 드롭다운 목록에서 사용할 인증 유형을 클릭합니다. 기본값은 없음입니다.
- **서버 프록시 주소:** 통신사 APN HTTP 프록시의 IP 주소 또는 URL입니다.
- **서버 프록시 포트:** APN 프록시의 포트 번호입니다. 서버 프록시 주소를 입력한 경우 이 서버 프록시 포트 번호가 필요합니다.
- **MMSC:** 통신사에서 제공하는 MMS 게이트웨이 서버 주소입니다.
- **멀티미디어 메시징 서버(MMS) 프록시 주소:** MMS 트래픽을 위한 멀티미디어 메시징 서비스 서버입니다. MMS는 사진이나 비디오와 같은 멀티미디어 콘텐츠가 포함된 더 큰 메시지를 보내기 위해 SMS를 대체했습니다. 이러한 서버에는 특정 프로토콜(예: MM1, ... MM11)이 필요합니다.
- **MMS 포트:** MMS 프록시에 사용되는 포트입니다.

앱 액세스 장치 정책

XenMobile®의 앱 액세스 장치 정책을 통해 다음을 정의할 수 있습니다.

- 장치에 설치해야 하는 앱 목록.
- 장치에 설치할 수 있는 앱 목록.
- 장치에 설치하면 안 되는 앱 목록.

그런 다음 앱 목록에 대한 장치 규정 준수에 반응하는 자동화된 작업을 생성할 수 있습니다. iOS 및 Android 장치용 앱 액세스 정책을 생성할 수 있습니다.

한 번에 한 가지 유형의 액세스 정책만 구성할 수 있습니다. 필수 앱, 권장 앱 또는 허용되지 않는 앱 목록 중 하나에 대한 정책을 추가할 수 있지만, 동일한 앱 액세스 정책 내에서 혼합할 수는 없습니다. 각 목록 유형에 대한 정책을 생성하는 경우, 각 정책의 이름을 신중하게 지정하는 것이 좋습니다. 각 정책의 이름을 신중하게 지정하면 XenMobile에서 어떤 정책이 어떤 앱 목록에 적용되는지 알 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

플랫폼 설정

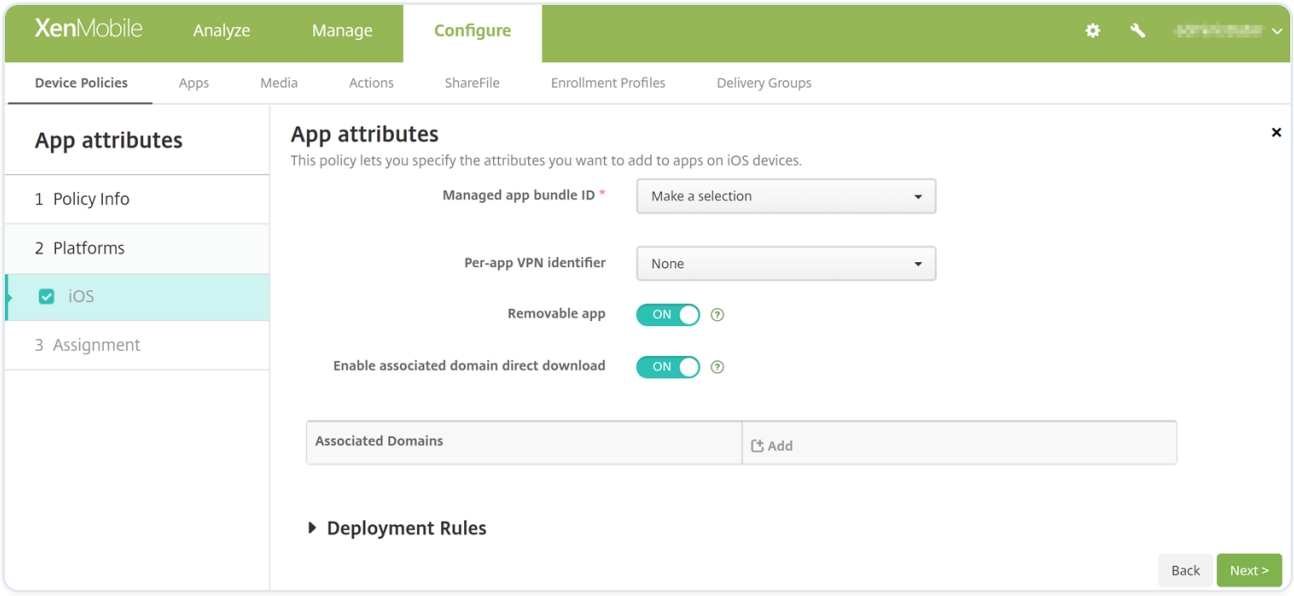
- **액세스 정책: 필수**, **권장** 또는 **금지**를 클릭합니다. 기본값은 **필수**입니다.
- 목록에 하나 이상의 앱을 추가하려면 **추가**를 클릭한 다음 다음을 수행합니다.
  - **앱 이름:** 앱 이름을 입력합니다.
  - **앱 식별자:** 선택적 앱 식별자를 입력합니다.
  - **저장** 또는 **취소**를 클릭합니다.
  - 추가하려는 각 앱에 대해 이 단계를 반복합니다.

앱 특성 장치 정책

앱 특성 장치 정책을 사용하면 iOS 장치에 대해 관리되는 앱 번들 ID 또는 앱별 VPN 식별자와 같은 특성을 지정할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



- **관리되는 앱 번들 ID:** 다음 방법으로 앱을 지정합니다.
  - 앱 번들 ID를 선택합니다. 옵션은 관리되는 장치의 앱 인벤토리를 수집하는 **앱 인벤토리** 장치 정책을 활성화한 후에만 사용할 수 있습니다.
  - **새로 추가**를 선택한 다음 앱 번들 ID를 입력합니다. 앱 번들 ID를 찾으려면 App Store에서 앱의 번들 ID 찾기를 참조하십시오.
- **앱별 VPN 식별자:** (선택 사항) 이 앱에 대한 앱별 VPN을 선택합니다. 옵션에는 **장치 정책** > **VPN 정책** 페이지에서 구성한 앱별 VPN 연결이 포함됩니다. 자세한 내용은 앱별 VPN 구성을 참조하십시오.
- **제거 가능한 앱:** (선택 사항) 관리되는 앱인 경우 사용자가 앱을 제거할 수 있는지 여부를 지정합니다. 사용자가 앱을 제거하지 못하도록 하려면 이 옵션을 **끔**으로 설정합니다. 기본값은 **켬**으로 설정되어 있습니다. iOS 14 이상에서 사용할 수 있습니다.
- **연결된 도메인 직접 다운로드 활성화:** (선택 사항) 앱이 Apple 서버 대신 도메인에서 직접 클레임된 사이트 연결 확인을 수행할 수 있는지 여부를 지정합니다. 인터넷에 액세스할 수 없는 도메인에 대해서만 이 옵션을 **켬**으로 설정합니다. 기본값은 **켬**으로 설정되어 있습니다. iOS 14 이상에서 사용할 수 있습니다.
- **연결된 도메인:** (선택 사항) 이 앱에 대한 연결된 도메인을 추가하려면 **추가**를 클릭한 다음 정규화된 도메인 이름(FQDN)을 입력합니다. iOS 13 이상에서 사용할 수 있습니다.

App Store에서 앱의 번들 ID 찾기

1. App Store에서 앱을 찾아 URL 끝에 있는 숫자를 복사합니다. 예를 들어, 363501921은 Citrix Workspace app의 앱 ID입니다.
2. `https://itunes.apple.com/lookup?id=`으로 이동하여 해당 URL 뒤에 숫자를 붙여넣습니다. TXT 파일이 컴퓨터에 자동으로 다운로드됩니다.

3. TXT 파일에서 `bundleId`을(를) 검색하여 앱의 번들 ID를 가져옵니다. 예를 들어, Citrix Workspace 앱의 번들 ID는 `com.citrix.ReceiveriPad`입니다.

앱 구성 장치 정책

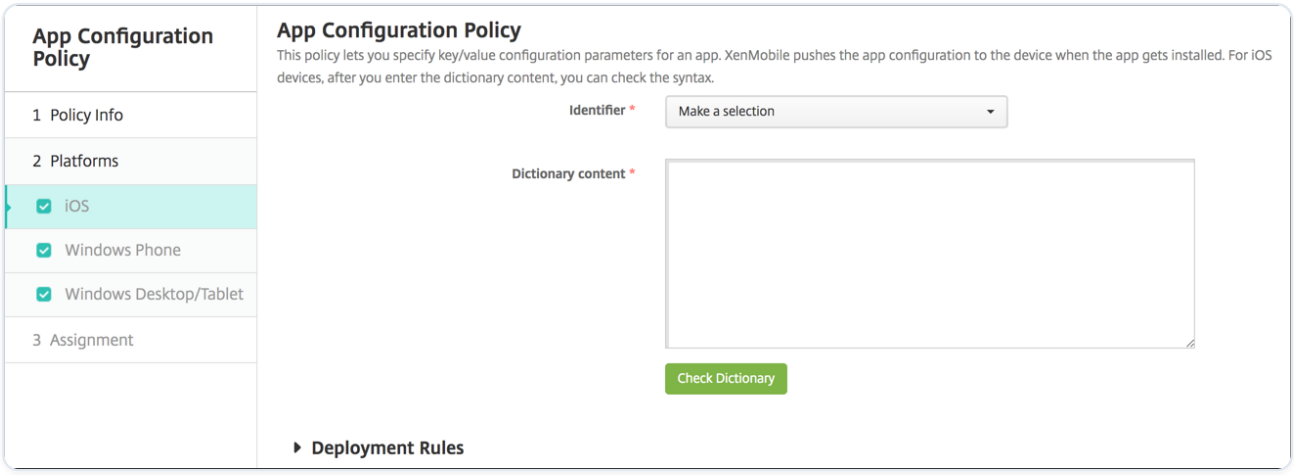
다음 항목을 배포하여 관리형 구성을 지원하는 앱을 원격으로 구성할 수 있습니다.

- iOS 장치에 XML 구성 파일(속성 목록 또는 plist라고 함)
- 또는 Windows 10 또는 Windows 11을 실행하는 Windows 10 휴대폰 또는 태블릿 또는 데스크톱 장치용 키/값 쌍.

이 구성은 앱의 다양한 설정과 동작을 지정합니다. XenMobile®은 사용자가 앱을 설치할 때 구성을 장치로 푸시합니다. 구성할 수 있는 실제 설정 및 동작은 앱에 따라 다르며 이 문서의 범위를 벗어납니다.

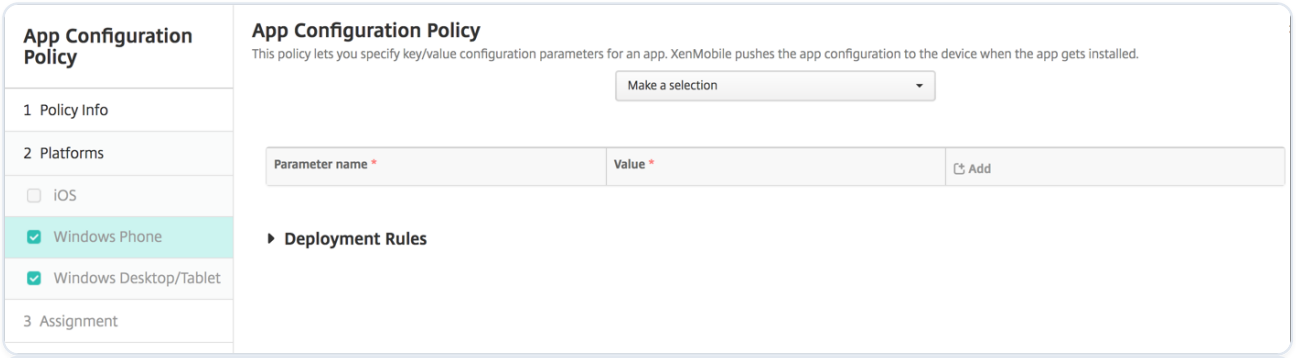
이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

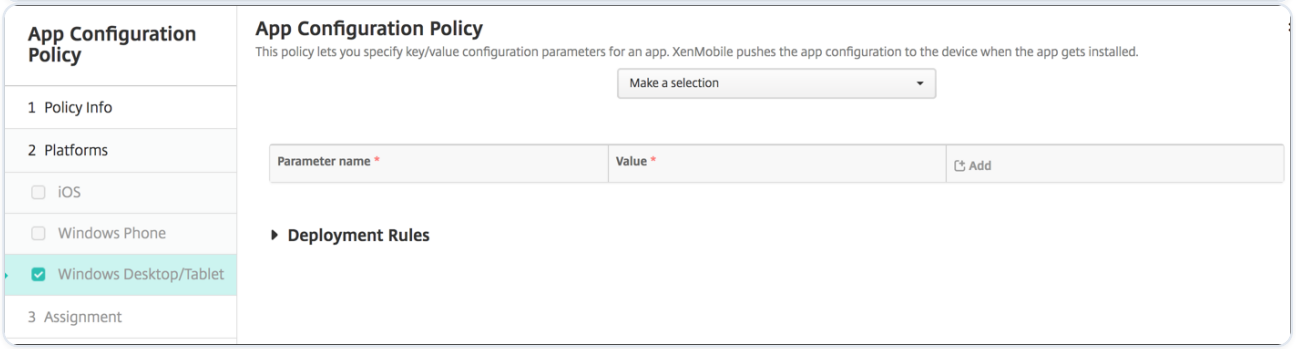
iOS 설정



- **식별자:** 구성하려는 앱을 드롭다운 목록에서 클릭하거나 **새로 추가**를 클릭하여 목록에 앱을 추가합니다.
  - **새로 추가**를 클릭하면 나타나는 필드에 앱 식별자를 입력합니다.
- **사전 콘텐츠:** XML 속성 목록(plist) 구성 정보를 입력하거나 복사하여 붙여넣습니다.
- **사전 확인**을 클릭합니다. XenMobile이 XML을 확인합니다. 오류가 없으면 콘텐츠 상자 아래에 **유효한 XML**이 표시됩니다. 콘텐츠 상자 아래에 구문 오류가 나타나면 계속하기 전에 오류를 수정해야 합니다.

Windows 데스크톱/태블릿 설정





- **선택** 목록에서 구성하려는 앱을 클릭하거나, 목록에 앱을 추가하려면 **새로 추가**를 클릭합니다.
  - **새로 추가**를 클릭하면 표시되는 필드에 패키지 제품군 이름을 입력합니다.
- 추가하려는 각 구성 매개변수에 대해 **추가**를 클릭한 다음 다음 작업을 수행합니다.
  - **매개변수 이름:** Windows 장치에 대한 응용 프로그램 설정의 키 이름을 입력합니다. Windows 앱 설정에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.
  - **값:** 지정된 매개변수에 대한 값을 입력합니다.
  - 매개변수를 추가하려면 **추가**를 클릭하거나, 매개변수 추가를 취소하려면 **취소**를 클릭합니다.

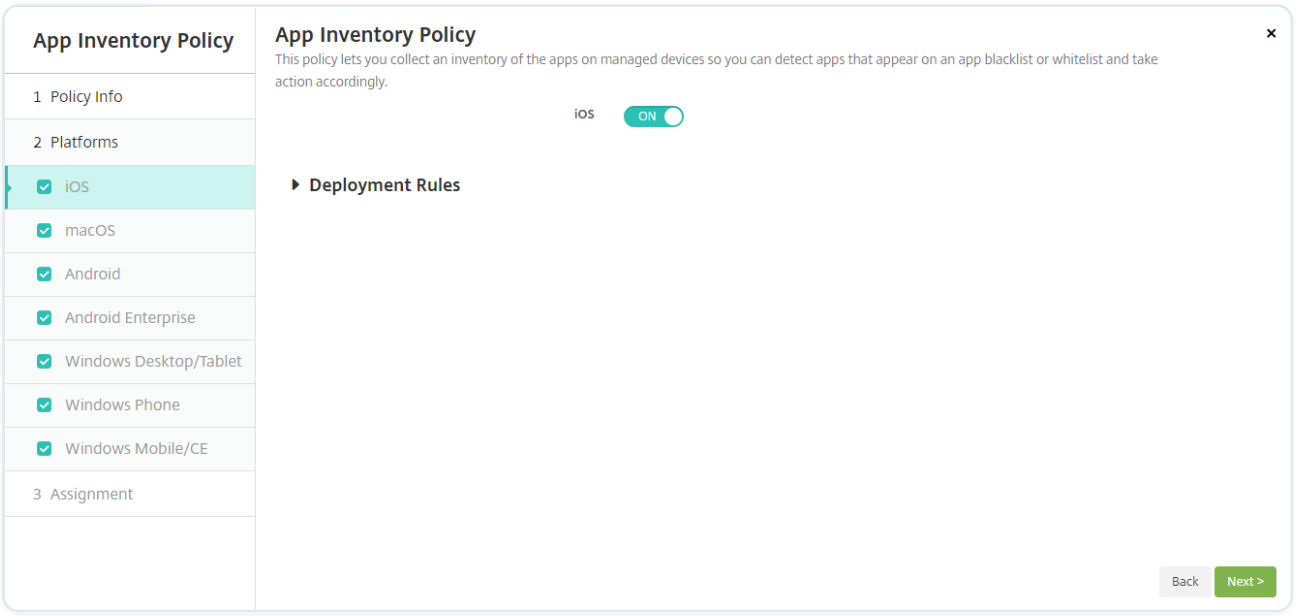
앱 인벤토리 장치 정책

앱 인벤토리 정책을 사용하면 관리되는 장치에 있는 앱의 인벤토리를 수집할 수 있습니다. 그러면 XenMobile®이 해당 인벤토리를 해당 장치에 배포된 모든 앱 액세스 정책과 비교할 수 있습니다. 이러한 방식으로 앱 허용 또는 차단 목록에 나타나는 앱을 감지하고 올바르게 조치할 수 있습니다.

iOS, macOS, Android, Android Enterprise 또는 Windows 데스크톱/태블릿 장치용 앱 액세스 정책을 만들 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

플랫폼 설정



- 선택하는 각 플랫폼에 대해 기본 설정을 그대로 두거나 설정을 **끄기**로 변경합니다. 기본값은 **켜기**입니다.

앱 잠금 장치 정책

앱 잠금 장치 정책은 장치에서 실행이 허용되는 앱 목록 또는 장치에서 실행이 차단되는 앱 목록을 정의합니다. 이 정책은 iOS 및 Android 장치 모두에 대해 구성할 수 있지만, 정책이 작동하는 정확한 방식은 각 플랫폼마다 다릅니다. 예를 들어, iOS 장치에서는 여러 앱을 차단할 수 없습니다.

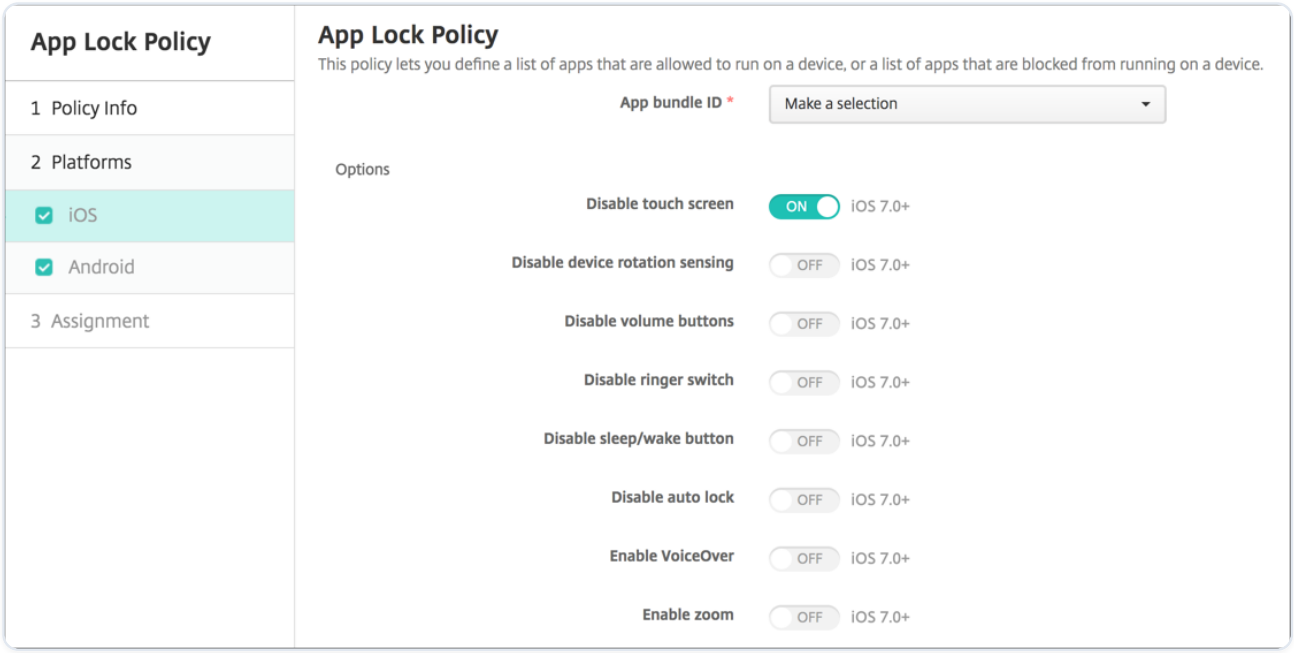
마찬가지로, iOS 장치의 경우 정책당 하나의 iOS 앱만 선택할 수 있습니다. 이는 사용자가 단일 앱을 실행하기 위해 장치를 사용할 수 있음을 의미합니다. 앱 잠금 정책이 적용될 때 특별히 허용하는 옵션을 제외하고는 장치에서 다른 활동을 할 수 없습니다.

또한 앱 잠금 정책을 푸시하려면 iOS 장치가 감독 모드여야 합니다.

장치 정책은 대부분의 Android L 및 M 장치에서 작동하지만, Google이 필요한 API를 더 이상 사용하지 않도록 설정했기 때문에 Android N 이상 장치에서는 앱 잠금이 작동하지 않습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



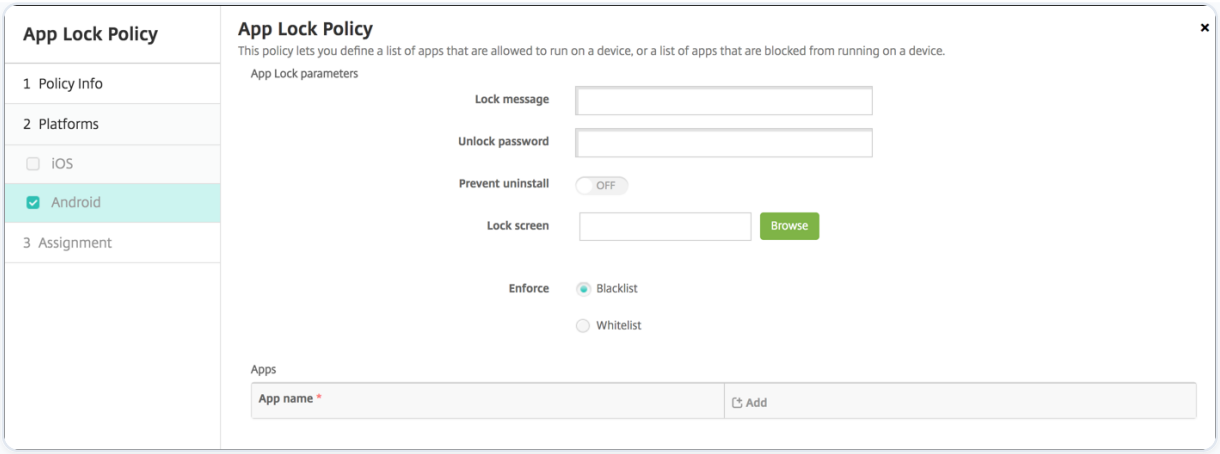
- **앱 번들 ID:** 이 정책이 적용될 드롭다운 목록에서 앱을 클릭하거나 **새로 추가**를 클릭하여 목록에 앱을 추가합니다. **새로 추가**를 선택한 경우 나타나는 필드에 앱 이름을 입력합니다.
- **옵션:** 다음 각 옵션은 iOS 7.0 이상에만 적용됩니다. 각 옵션의 기본값은 **끄기**이며, 터치 스크린 비활성화만 기본값이 **켜기**입니다.
  - 터치 스크린 비활성화
  - 장치 회전 감지 비활성화
  - 볼륨 버튼 비활성화
  - 벨소리 스위치 비활성화

    벨소리 스위치 비활성화가 **켜기**인 경우, 벨소리 동작은 스위치가 처음 비활성화되었을 때의 위치에 따라 달라집니다.
  - 잠자기/깨우기 버튼 비활성화
  - 자동 잠금 비활성화
  - VoiceOver 비활성화
  - 확대/축소 활성화
  - 색상 반전 활성화
  - AssistiveTouch 활성화
  - 선택 항목 말하기 활성화
  - 모노 오디오 활성화

- **사용자 활성화 옵션:** 다음 각 옵션은 iOS 7.0 이상에만 적용됩니다. 각 옵션의 기본값은 **끔**입니다.
  - VoiceOver 조정 허용
  - 확대/축소 조정 허용
  - 색상 반전 조정 허용
  - AssistiveTouch 조정 허용
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

Android 설정

> **참고:**
>
> 앱 잠금 장치 정책을 사용하여 Android 설정 앱을 차단할 수 없습니다.



- **앱 잠금 매개변수**
  - **잠금 메시지:** 잠긴 앱을 열려고 할 때 사용자에게 표시될 메시지를 입력합니다.
  - **잠금 해제 암호:** 앱 잠금을 해제할 암호를 입력합니다.
  - **제거 방지:** 사용자가 앱을 제거하도록 허용할지 여부를 선택합니다. 기본값은 **해제**입니다.

- **잠금 화면:** 찾아보기를 클릭하고 파일 위치로 이동하여 장치 잠금 화면에 표시될 이미지를 선택합니다.
- **강제 적용:** 장치에서 실행이 허용되지 않는 앱 목록을 만들려면 **블랙리스트**를 클릭하거나, 장치에서 실행이 허용되는 앱 목록을 만들려면 **화이트리스트**를 클릭합니다.

> **참고:**
>
> XenMobile® Server 콘솔에는 "블랙리스트" 및 "화이트리스트"라는 용어가 포함되어 있습니다. 다음 버전에서는 이러한 용어를 "차단 목록" 및 "허용 목록"으로 변경할 예정입니다.

- **앱: 추가**를 클릭한 다음 다음을 수행합니다.
  - **앱 이름:** 드롭다운 목록에서 앱 이름을 클릭하여 허용 또는 차단 목록에 추가하거나, **새로 추가**를 클릭하여 사용 가능한 앱 목록에 앱을 추가합니다.
  - **새로 추가**를 선택한 경우, 나타나는 필드에 앱 이름을 입력합니다.
  - **저장** 또는 **취소**를 클릭합니다.
  - 허용 또는 차단 목록에 추가하려는 각 앱에 대해 이 단계를 반복합니다.

앱 네트워크 사용 장치 정책

관리되는 앱이 iOS 장치에서 셀룰러 데이터 네트워크와 같은 네트워크를 사용하는 방법을 지정하는 네트워크 사용 규칙을 설정할 수 있습니다. 이 규칙은 관리되는 앱에만 적용됩니다. 관리되는 앱은 XenMobile을 통해 사용자 장치에 배포하는 앱입니다. 여기에는 사용자가 XenMobile을 통해 배포하지 않고 장치에 직접 다운로드한 앱이나 장치가 XenMobile에 등록될 때 이미 장치에 설치되어 있던 앱은 포함되지 않습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **로밍 셀룰러 데이터 허용:** 지정된 앱이 로밍 중에 셀룰러 데이터 연결을 사용할 수 있는지 여부를 선택합니다. 기본값은 **끔**입니다.
- **셀룰러 데이터 허용:** 지정된 앱이 셀룰러 데이터 연결을 사용할 수 있는지 여부를 선택합니다. 기본값은 **끔**입니다.
- **앱 식별자 일치:** 목록에 추가할 각 앱에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **앱 식별자:** 앱 식별자를 입력합니다.

- **저장**을 클릭하여 앱을 목록에 저장하거나 **취소**를 클릭하여 앱을 목록에 저장하지 않습니다.

앱 알림 장치 정책

앱 알림 정책을 사용하면 iOS 사용자가 지정된 앱에서 알림을 받는 방법을 제어할 수 있습니다. 이 정책은 iOS 9.3 이상을 실행하는 장치에서 지원됩니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/app-notifications-policy-ios.png)

- **앱 번들 식별자:** 이 정책을 적용할 앱을 지정합니다.
- **알림 허용:** 알림을 허용하려면 **켜기**를 선택합니다.
- **알림 센터에 표시:** 사용자 장치의 알림 센터에 알림을 표시하려면 **켜기**를 선택합니다.
- **앱 아이콘 배지:** 알림과 함께 배지 앱 아이콘을 표시하려면 **켜기**를 선택합니다.
- **사운드:** 알림에 사운드를 포함하려면 **켜기**를 선택합니다.
- **잠금 화면에 표시:** 사용자 장치의 잠금 화면에 알림을 표시하려면 **켜기**를 선택합니다.
- **CarPlay에 표시: 켜기**로 설정하면 Apple CarPlay에 알림이 표시됩니다. iOS 12 이상에서 사용할 수 있습니다. 기본값은 **켜기**입니다.
- **긴급 알림 활성화: 켜기**로 설정하면 앱이 방해 금지 및 벨소리 설정을 무시하는 긴급 알림으로 알림을 표시할 수 있습니다. iOS 12 이상에서 사용할 수 있습니다. 기본값은 **끄기**입니다.
- **잠금 해제된 알림 스타일:** 목록에서 **없음**, **배너** 또는 **알림**을 선택하여 잠금 해제된 알림의 모양을 구성합니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.
  - **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 또는 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **시스템**입니다. 이 옵션은 iOS 9.3 이상에서만 사용할 수 있습니다.

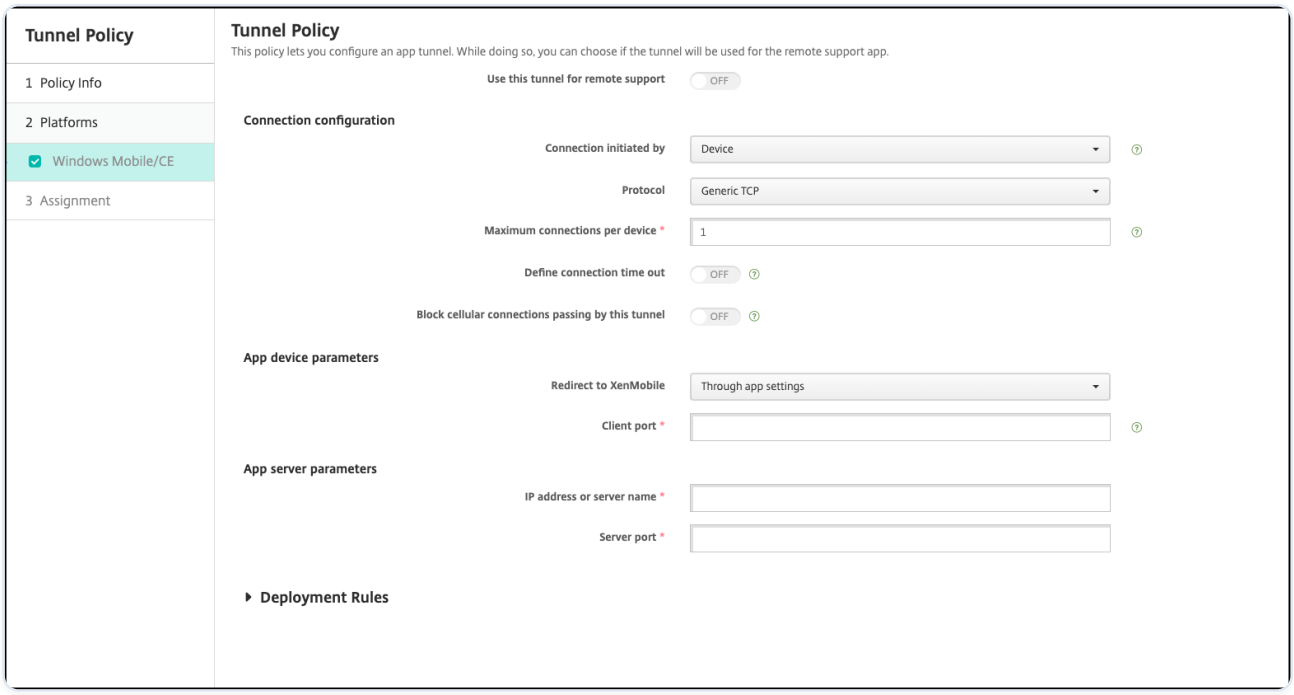
터널 장치 정책

애플리케이션 터널(앱 터널)은 모바일 앱의 서비스 연속성과 데이터 전송 안정성을 높이도록 설계되었습니다. 앱 터널은 모든 모바일 장치 앱의 클라이언트 구성 요소와 앱 서버 구성 요소 간의 프록시 매개변수를 정의합니다. Android 장치에 대한 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 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

Android 설정



- **연결 시작:** 연결을 시작하는 소스를 지정하려면 **장치** 또는 **서버**를 클릭합니다.
- **장치당 최대 연결 수:** 앱이 설정할 수 있는 동시 TCP 연결 수를 지정하려면 숫자를 입력합니다. 이 필드는 장치에서 시작된 연결에만 적용됩니다.
- **연결 시간 초과 정의:** 터널이 닫히기 전에 앱이 유휴 상태로 있을 수 있는 시간 길이를 설정할지 여부를 선택합니다.
    - **연결 시간 초과: 연결 시간 초과 정의**를 **켜기**로 설정한 경우, 터널이 닫히기 전에 앱이 유휴 상태로 있을 수 있는 시간(초)을 입력합니다.
- **이 터널을 통과하는 셀룰러 연결 차단:** 로밍 중에 이 터널을 차단할지 여부를 선택합니다. Wi-Fi 및 USB 연결은 차단되지 않습니다.
- **XenMobile로 리디렉션: 앱 설정 통해**를 선택합니다.

- **클라이언트 포트:** 클라이언트 포트 번호를 입력합니다. 일반적으로 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.

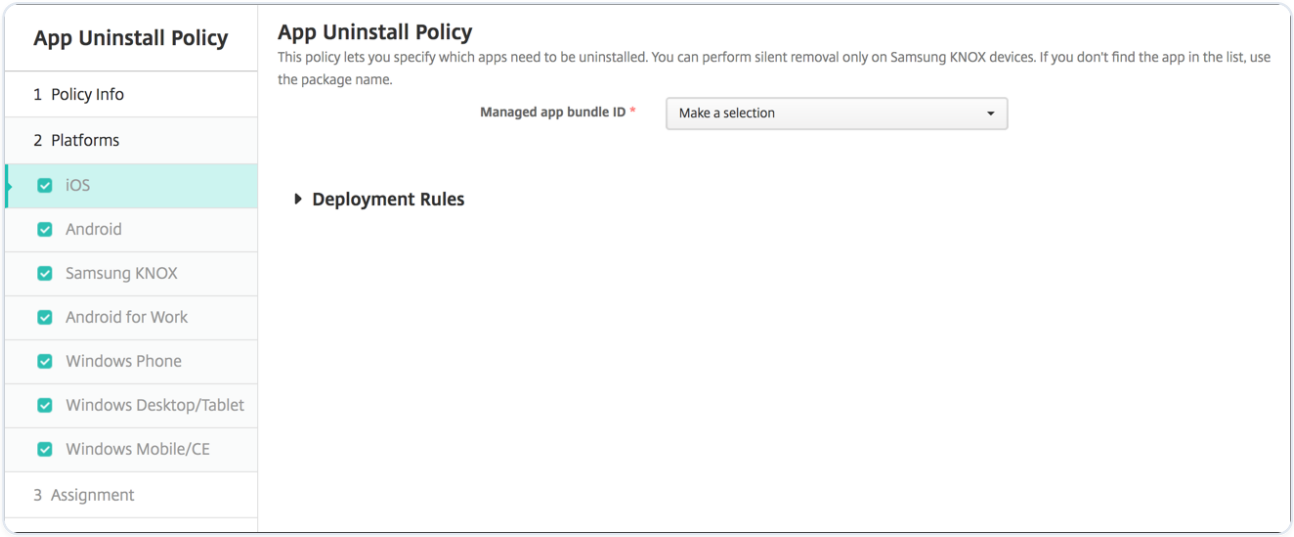
앱 제거 장치 정책

iOS, Android, Samsung Knox, Android Enterprise 및 Windows Desktop/Tablet 플랫폼용 앱 제거 정책을 만들 수 있습니다. 앱 제거 정책을 사용하면 여러 가지 이유로 사용자 장치에서 앱을 제거할 수 있습니다. 특정 앱을 더 이상 지원하지 않으려거나, 회사가 기존 앱을 다른 공급업체의 유사한 앱으로 교체하려 할 수 있습니다.

이 정책이 사용자 장치에 배포되면 앱이 제거됩니다. Samsung Knox 장치를 제외하고, 사용자는 앱 제거 프롬프트를 받습니다. Samsung Knox 장치 사용자는 앱 제거 프롬프트를 받지 않습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



- **관리되는 앱 번들 ID:** 드롭다운 목록에서 기존 앱을 클릭하거나 **새로 추가**를 클릭합니다. 이 플랫폼에 구성된 앱이 없으면 목록이 비어 있으므로 앱을 추가해야 합니다.
    - **추가**를 클릭하면 앱 이름을 입력할 수 있는 필드가 나타납니다.

기타 모든 플랫폼 설정

- **제거할 앱:** 추가하려는 각 앱에 대해 **추가**를 클릭한 다음 다음을 수행합니다.

- **앱 이름:** 드롭다운 목록에서 기존 앱을 클릭하거나 **새로 추가**를 클릭하여 새 앱 이름을 입력합니다. 이 플랫폼에 구성된 앱이 없으면 목록이 비어 있으므로 새 앱을 추가해야 합니다.
- **추가**를 클릭하여 앱을 추가하거나 **취소**를 클릭하여 앱 추가를 취소합니다.

해당 공용 앱 스토어 앱 설치 후 엔터프라이즈 앱 자동 제거

공용 앱 스토어 버전이 설치될 때 Citrix® 앱의 엔터프라이즈 버전을 제거하도록 XenMobile®을 구성할 수 있습니다. 이 기능은 공용 앱 스토어 버전이 설치된 후 사용자 장치에 두 개의 동일한 앱 아이콘이 있는 것을 방지합니다.

앱 제거 장치 정책에 대한 배포 조건은 새 버전이 설치될 때 XenMobile이 사용자 장치에서 이전 앱을 제거하도록 트리거합니다. 이 기능은 엔터프라이즈 모드(XME)에서 XenMobile Server에 연결된 관리형 iOS 장치에서만 사용할 수 있습니다.

설치된 앱 이름 조건을 사용하여 배포 규칙을 구성하려면:

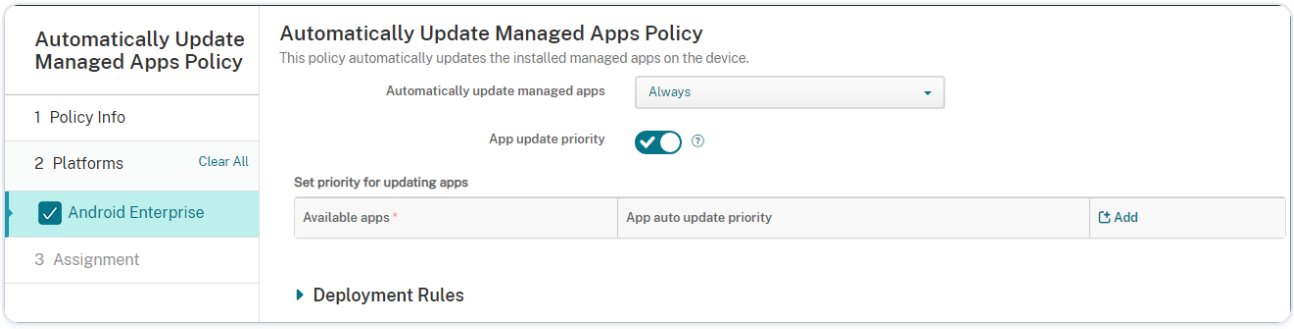
- 엔터프라이즈 앱에 대한 **관리되는 앱 번들 ID**를 지정합니다.
- 규칙 추가: **새 규칙**을 클릭한 다음, 샘플에 표시된 대로 **설치된 앱 이름** 및 **같음**을 선택합니다. 공개 앱 스토어 앱의 앱 번들 ID를 입력합니다.

예를 들어, 지정된 전달 그룹의 장치에 공개 앱 스토어 앱(com.citrix.mail.ios)이 설치되면 XenMobile은 엔터프라이즈 버전(com.citrix.mail)을 제거합니다.

관리되는 앱 자동 업데이트 장치 정책

이 정책은 Android Enterprise 장치에서 설치된 관리되는 앱이 업데이트되는 방식을 제어합니다. 사용자가 장치에서 앱의 자동 업데이트를 허용하는 기능을 제한할 수 있습니다. 사용자가 장치에서 앱의 자동 업데이트를 제어하도록 허용하면 관리되는 Google Play 스토어에서 자동 앱 업데이트 정책을 설정합니다.

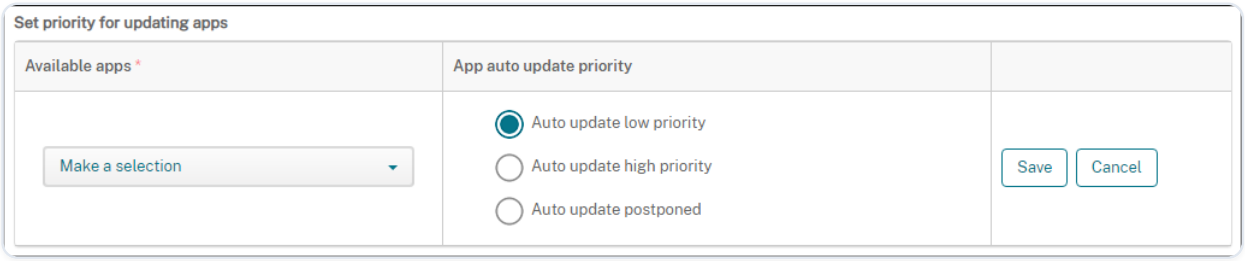
이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.



- **관리되는 앱 자동 업데이트**

- **항상:** 자동 앱 업데이트를 사용하도록 설정합니다. **항상**이 기본값입니다.
- **사용자가 정책을 구성하도록 허용:** 사용자가 관리되는 Google Play 스토어에서 장치에 대한 자동 앱 업데이트 정책을 구성하도록 허용합니다.
- **안 함:** 자동 앱 업데이트를 사용하지 않도록 설정합니다.
- **장치가 Wi-Fi에 연결된 경우에만:** 장치가 Wi-Fi에 연결된 경우에만 자동 앱 업데이트를 허용합니다.

- **앱 업데이트 우선순위: 켜짐**으로 설정하면 각 관리되는 앱에 대한 업데이트 우선순위 수준을 구성할 수 있습니다.
- **앱 업데이트 우선순위 설정: 추가**를 클릭하여 앱에 대한 업데이트 우선순위를 구성합니다.



- **사용 가능한 앱:** 메뉴에서 앱을 선택하여 업데이트 우선순위를 구성합니다.
- **앱 자동 업데이트 우선순위:** 다음 중에서 업데이트 우선순위를 선택합니다.
  - **자동 업데이트 낮은 우선순위:** 장치가 충전 중이고, 활발하게 사용되지 않으며, 무제한 네트워크에 연결되어 있을 때 앱이 업데이트됩니다.
  - **자동 업데이트 우선순위 높음:** 제약 없이 가능한 한 빨리 앱을 업데이트합니다.
  - **자동 업데이트 연기:** 새 버전이 출시된 후 최대 90일 동안 앱이 자동으로 업데이트되지 않습니다. 90일 후에는 앱이 낮은 우선순위로 자동으로 업데이트됩니다. 앱이 업데이트된 후에는 90일 동안 앱이 자동으로 업데이트되지 않습니다. 사용자는 언제든지 앱을 수동으로 업데이트할 수 있습니다.

- 완료되면 **저장**을 클릭합니다. 연필 아이콘을 클릭하여 구성을 편집할 수 있습니다. 휴지통을 클릭하여 구성을 삭제합니다.

BitLocker 장치 정책

Windows 10 및 Windows 11에는 BitLocker라는 디스크 암호화 기능이 포함되어 있어 분실 또는 도난당한 Windows 장치에 대한 무단 액세스로부터 추가 파일 및 시스템 보호를 제공합니다. 더 강력한 보호를 위해 BitLocker를 Trusted Platform Module(TPM) 칩 버전 1.2 이상과 함께 사용할 수 있습니다. TPM 칩은 암호화 작업을 처리하고 암호화 키를 생성, 저장 및 사용을 제한합니다.

Windows 10 빌드 1703부터 MDM 정책으로 BitLocker를 제어할 수 있습니다. XenMobile®의 BitLocker 장치 정책을 사용하여 Windows 10 및 Windows 11 장치의 BitLocker 마법사에서 사용할 수 있는 설정을 구성합니다. 예를 들어, BitLocker가 활성화된 장치에서 BitLocker는 사용자에게 시작 시 드라이브 잠금 해제 방

법, 복구 키 백업 방법, 고정 드라이브 잠금 해제 방법을 묻는 메시지를 표시할 수 있습니다. BitLocker 장치 정책 설정은 다음을 수행할지 여부도 구성합니다.

- TPM 칩이 없는 장치에서 BitLocker를 활성화합니다.
- BitLocker 인터페이스에 복구 옵션을 표시합니다.
- BitLocker가 활성화되지 않은 경우 고정 또는 이동식 드라이브에 대한 쓰기 액세스를 거부합니다.

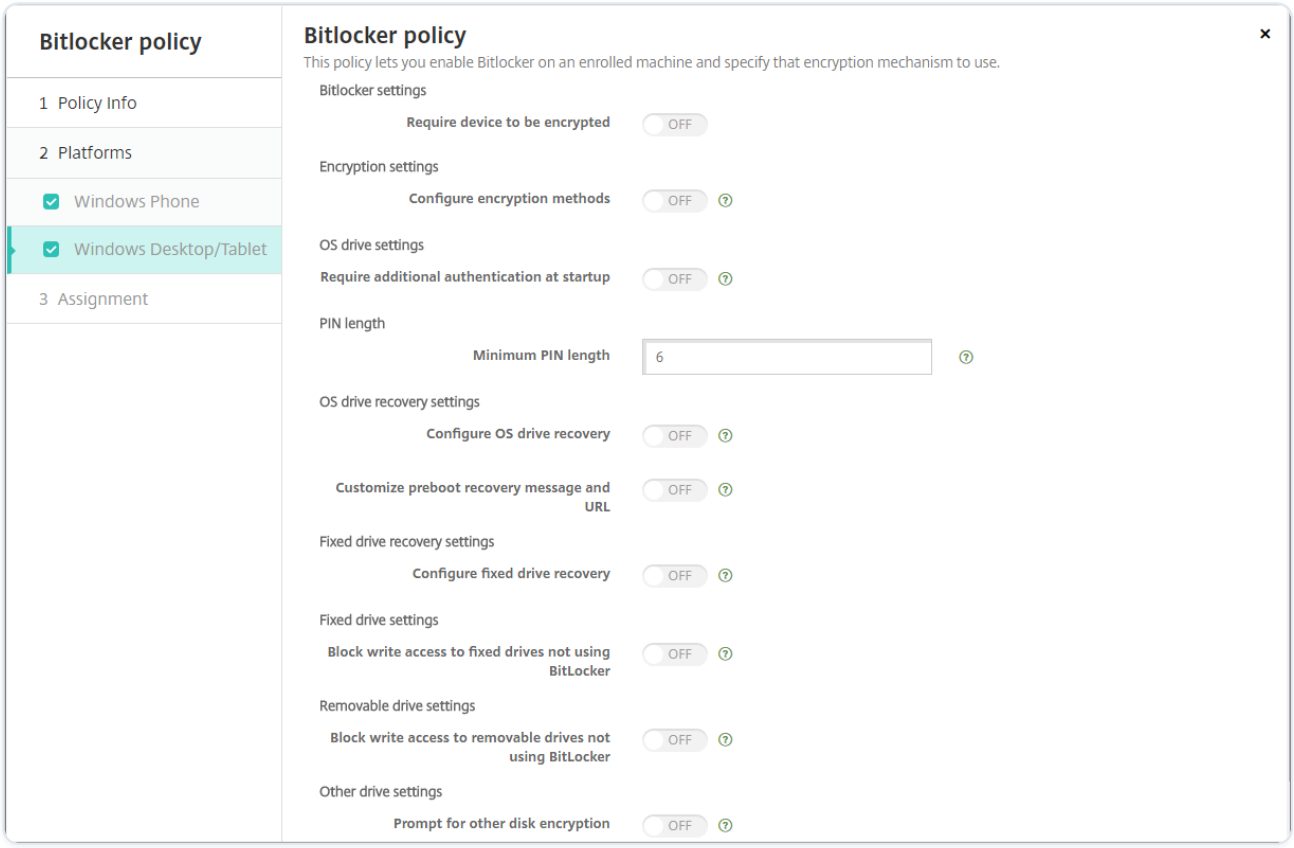
> **참고:**
>
> 장치에서 BitLocker 암호화가 시작된 후에는 업데이트된 BitLocker 장치 정책을 배포하여 나중에 장치의 BitLocker 설정을 변경할 수 없습니다.

> 이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

요구 사항

- BitLocker 장치 정책에는 Windows 10 또는 Windows 11 Enterprise 에디션이 필요합니다.
- BitLocker 장치 정책을 배포하기 전에 BitLocker 사용을 위한 환경을 준비하십시오. BitLocker 시스템 요구 사항 및 설정 등 Microsoft의 자세한 정보는 BitLocker 및 해당 노드 아래의 문서를 참조하십시오.

Windows 데스크톱 및 태블릿 설정



- **장치 암호화 필수:** Windows 데스크톱 또는 태블릿에서 사용자에게 BitLocker 암호화를 활성화하도록 요청할지 여부를 결정합니다. **켜짐**으로 설정하면 등록 완료 후 장치에 엔터프라이즈에서 장치 암호화를 요구한다는 메시지가 표시됩니다. **꺼짐**으로 설정하면 사용자에게 메시지가 표시되지 않고 BitLocker는 정책 설정을 사용합니다. 기본값은 **꺼짐**입니다.
- **암호화 방법 구성:** 특정 드라이브 유형에 사용할 암호화 방법을 결정합니다. **해제**인 경우 BitLocker 마법사가 사용자에게 드라이브 유형에 사용할 암호화 방법을 묻는 메시지를 표시합니다. 모든 드라이브의 암호화 방법은 기본적으로 XTS-AES 128비트입니다. 이동식 드라이브의 암호화 방법은 기본적으로 AES-CBC 128비트입니다. **설정**인 경우 BitLocker는 정책에 지정된 암호화 방법을 사용합니다. **설정**인 경우 다음 추가 설정이 나타납니다. **운영 체제 드라이브**, **고정 드라이브**, **이동식 드라이브**. 각 드라이브 유형에 대한 기본 암호화 방법을 선택합니다. 기본값은 **해제**입니다.
- **시작 시 추가 인증 필요:** 장치 시작 시 필요한 추가 인증을 지정합니다. 또한 TPM 칩이 없는 장치에서 BitLocker를 허용할지 여부를 지정합니다. **해제**인 경우 TPM이 없는 장치는 BitLocker 암호화를 사용할 수 없습니다. TPM에 대한 자세한 내용은 Microsoft 문서, 신뢰할 수 있는 플랫폼 모듈 기술 개요를 참조하십시오. **설정**인 경우 다음 추가 설정이 나타납니다. 기본값은 **해제**입니다.
    - **TPM 칩이 없는 장치에서 BitLocker 차단:** TPM 칩이 없는 장치에서 BitLocker는 사용자에게 잠금 해제 암호 또는 시작 키를 만들도록 요구합니다. 시작 키는 USB 드라이브에 저장되며, 사용자는 시작하기 전에 이 드라이브를 장치에 연결해야 합니다. 잠금 해제 암호는 최소 8자입니다. 기본값은 **해제**입니다.

  - **TPM 시작:** TPM이 있는 장치에는 TPM 전용, TPM + PIN, TPM + 키, TPM + PIN + 키의 네 가지 잠금 해제 모드가 있습니다. TPM 시작은 암호화 키가 TPM 칩에 저장되는 TPM 전용 모드에 해당합니다. 이 모드에서는 사용자가 추가 잠금 해제 데이터를 제공할 필요가 없습니다. 사용자 장치는 다시 시작하는 동안 TPM 칩의 암호화 키를 사용하여 자동으로 잠금 해제됩니다. 기본값은 **TPM 허용**입니다.
  - **TPM 시작 PIN:** 이 설정은 TPM + PIN 잠금 해제 모드입니다. PIN은 최대 20자리까지 가능합니다. **최소 PIN 길이** 설정을 사용하여 최소 PIN 길이를 지정합니다. 사용자는 BitLocker 설정 중에 PIN을 구성하고 장치 시작 중에 PIN을 제공합니다.
  - **TPM 시작 키:** 이 설정은 TPM + 키 잠금 해제 모드입니다. 시작 키는 USB 또는 기타 이동식 드라이브에 저장되며, 사용자는 시작하기 전에 이 드라이브를 장치에 연결해야 합니다.
  - **TPM 시작 키 및 PIN:** 이 설정은 TPM + PIN + 키 잠금 해제 모드입니다.

    잠금 해제에 성공하면 운영 체제가 로드되기 시작합니다. 잠금 해제에 실패하면 장치가 복구 모드로 들어갑니다.

- **최소 PIN 길이:** TPM 시작 PIN의 최소 길이입니다. 기본값은 **6**입니다.
- **OS 드라이브 복구 구성:** 잠금 해제 단계가 실패하면 BitLocker는 사용자에게 구성된 복구 키를 묻는 메시지를 표시합니다. 이 설정은 사용자가 잠금 해제 암호 또는 USB 시작 키가 없는 경우 사용할 수 있는 운영 체제 드라이브 복구 옵션을 구성합니다. 기본값은 **해제**입니다.

  - **인증서 기반 데이터 복구 에이전트 허용:** 인증서 기반 데이터 복구 에이전트를 허용할지 여부를 지정합니다. 그룹 정책 관리 콘솔(GPMC) 또는 로컬 그룹 정책 편집기에 있는 공개 키 정책에서 데이터 복구 에이전트를 추가합니다. 데이터 복구 에이전트에 대한 자세한 내용은 Microsoft 문서, BitLocker 그룹 정책 설정을 참조하십시오. 기본값은 **해제**입니다.
  - **OS 드라이브 복구를 위한 48비트 복구 암호 생성:** 사용자가 복구 암호를 사용하도록 허용할지 또는 요구할지 지정합니다. BitLocker는 암호를 생성하여 파일 또는 Microsoft 클라우드 계정에 저장합니다. 기본값은 **48자리 암호 허용**입니다.
  - **256비트 복구 키 생성:** 사용자가 복구 키를 사용하도록 허용할지 또는 요구할지 지정합니다. 복구 키는 USB 드라이브에 저장되는 BEK 파일입니다. 기본값은 **256비트 복구 키 허용**입니다.
  - **OS 드라이브 복구 옵션 숨기기:** BitLocker 인터페이스에서 복구 옵션을 표시할지 또는 숨길지 지정합니다. **설정**인 경우 BitLocker 인터페이스에 복구 옵션이 나타나지 않습니다. 이 경우 장치를 Active Directory에 등록하고, 복구 옵션을 Active Directory에 저장하고, **AD DS에 복구 정보 저장** 설정을 **설정**으로 지정합니다. 기본값은 **해제**입니다.
  - **AD DS에 복구 정보 저장:** 복구 옵션을 Active Directory Domain Services에 저장할지 여부를 지정합니다. 기본값은 **해제**입니다.

  - **AD DS에 저장된 복구 정보 구성:** BitLocker 복구 암호 또는 복구 암호와 키 패키지를 Active Directory 도메인 서비스에 저장할지 여부를 지정합니다. 키 패키지를 저장하면 물리적으로 손상된 드라이브에서 데이터를 복구할 수 있습니다. 기본값은 **복구 암호 백업**입니다.
  - **AD DS에 복구 정보 저장 후 BitLocker 사용:** 장치가 도메인에 연결되어 있고 BitLocker 복구 정보의 Active Directory 백업이 성공하지 않는 한 사용자가 BitLocker를 사용하도록 설정하는 것을 방지할지 여부를 지정합니다. **켜짐**으로 설정하면 BitLocker를 시작하기 전에 장치가 도메인에 가입되어 있어야 합니다. 기본값은 **꺼짐**입니다.

- **부팅 전 복구 메시지 및 URL 사용자 지정:** BitLocker가 복구 화면에 사용자 지정 메시지 및 URL을 표시할지 여부를 지정합니다. **켜짐**으로 설정하면 다음 추가 설정이 나타납니다: **기본 복구 메시지 및 URL 사용**, **빈 복구 메시지 및 URL 사용**, **사용자 지정 복구 메시지 사용**, **사용자 지정 복구 URL 사용**. **꺼짐**으로 설정하면 기본 복구 메시지 및 URL이 표시됩니다. 기본값은 **꺼짐**입니다.
- **고정 드라이브 복구 구성:** BitLocker로 암호화된 고정 드라이브에 대한 사용자 복구 옵션을 구성합니다. BitLocker는 고정 드라이브 암호화에 대한 메시지를 사용자에게 표시하지 않습니다. 시작 시 드라이브를 잠금 해제하려면 사용자가 암호 또는 스마트 카드를 제공합니다. 이 정책에 없는 시작 잠금 해제 설정은 사용자가 고정 드라이브에서 BitLocker 암호화를 사용하도록 설정할 때 BitLocker 인터페이스에 나타납니다. 관련 설정에 대한 자세한 내용은 이 목록의 앞부분에 있는 **OS 드라이브 복구 구성**을 참조하십시오. 기본값은 **꺼짐**입니다.
- **BitLocker를 사용하지 않는 고정 드라이브에 대한 쓰기 액세스 차단: 켜짐**으로 설정하면 사용자는 BitLocker로 암호화된 고정 드라이브에만 쓸 수 있습니다. 기본값은 **꺼짐**입니다.
- **BitLocker를 사용하지 않는 이동식 드라이브에 대한 쓰기 액세스 차단: 켜짐**으로 설정하면 사용자는 BitLocker로 암호화된 이동식 드라이브에만 쓸 수 있습니다. 이 설정을 조직에서 다른 조직의 이동식 드라이브에 대한 쓰기 액세스를 허용하는지 여부에 따라 구성하십시오. 기본값은 **꺼짐**입니다.
- **다른 디스크 암호화에 대한 프롬프트:** 장치에서 다른 디스크 암호화에 대한 경고 프롬프트를 비활성화할 수 있습니다. 기본값은 **꺼짐**입니다.

캘린더(CalDAV) 장치 정책

XenMobile®에서 장치 정책을 추가하여 사용자의 iOS 또는 macOS 장치에 캘린더(CalDAV) 계정을 추가할 수 있습니다. 이를 통해 CalDAV를 지원하는 모든 서버와 일정 데이터를 동기화할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이 필드는 필수입니다.
- **호스트 이름:** CalDAV 서버의 주소를 입력합니다. 이 필드는 필수입니다.

- **포트:** CalDAV 서버에 연결할 포트를 입력합니다. 이 필드는 필수입니다. 기본값은 **8443**입니다.
- **주요 URL:** 사용자의 캘린더에 대한 기본 URL을 입력합니다.
- **사용자 이름:** 사용자의 로그온 이름을 입력합니다. 이 필드는 필수입니다.
- **암호:** 선택 사항인 사용자 암호를 입력합니다.
- **SSL 사용:** CalDAV 서버에 대한 보안 소켓 계층 연결을 사용할지 여부를 선택합니다. 기본값은 **켜기**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 캘린더를 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이 필드는 필수입니다.
- **호스트 이름:** CalDAV 서버의 주소를 입력합니다. 이 필드는 필수입니다.
- **포트:** CalDAV 서버에 연결할 포트를 입력합니다. 이 필드는 필수입니다. 기본값은 **8443**입니다.
- **주요 URL:** 사용자의 캘린더에 대한 기본 URL을 입력합니다.
- **사용자 이름:** 사용자의 로그온 이름을 입력합니다. 이 필드는 필수입니다.
- **암호:** 선택 사항인 사용자 암호를 입력합니다.
- **SSL 사용:** CalDAV 서버에 대한 보안 소켓 계층 연결을 사용할지 여부를 선택합니다. 기본값은 **켜기**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.
  - **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다. **암호 필요**를 선택한 경우 **제거 암호** 필드에 암호를 입력합니다.

- **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 또는 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

셀룰러 장치 정책

이 정책을 사용하면 iOS 장치에서 셀룰러 네트워크 설정을 구성할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **APN 연결**
  - **이름:** 이 구성의 이름입니다.
  - **인증 유형:** 드롭다운 목록에서 Challenge Handshake Authentication Protocol (**CHAP**) 또는 Password Authentication Protocol (**PAP**)을 클릭합니다. 기본값은 **PAP**입니다.
  - **사용자 이름** 및 **암호:** 인증에 사용할 사용자 이름과 암호입니다.
- **APN**
  - **이름:** APN(액세스 포인트 이름) 구성의 이름입니다.
  - **인증 유형:** 드롭다운 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 제거 일정을 예약할 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

연결 예약 장치 정책

> **중요:**

> Citrix는 Android, Android Enterprise 및 Chrome OS 장치에서 XenMobile Server로의 연결을 제어하기 위해 Firebase Cloud Messaging(FCM)을 사용할 것을 권장합니다. FCM 사용에 대한 자세한 내용은 Firebase Cloud Messaging을 참조하십시오.

> FCM을 사용하지 않기로 선택한 경우, 사용자 장치가 XenMobile® Server에 연결하는 방법과 시기를 제어하기 위해 연결 예약 정책을 생성할 수 있습니다.

사용자가 장치를 수동으로 연결하도록 지정하거나, 장치가 정의된 시간 내에 연결하도록 지정할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

플랫폼 설정

- **장치 연결 요구 사항:** 이 일정에 대해 설정하려는 옵션을 클릭합니다.
  - **항상:** 연결을 영구적으로 유지합니다. 사용자 장치의 XenMobile은 네트워크 연결이 끊어진 후 XenMobile Server에 다시 연결을 시도하고, 제어 패킷을 정기적으로 전송하여 연결을 모니터링합니다. Citrix®는 최적화된 보안을 위해 이 옵션을 권장합니다. **항상**을 선택할 때, 장치 **터널 정책**에도 **연결 시간 초과 정의** 설정을 사용하여 연결로 인해 배터리가 소모되지 않도록 해야 합니다. 연결을 유지함으로써, 필요에 따라 장치에 초기화 또는 잠금과 같은 보안 명령을 푸시할 수 있습니다. 또한 장치에 배포된 각 정책에서 **배포 일정** 옵션 **항상 켜진 연결에 배포**를 선택해야 합니다.
  - **절대 안 함:** 수동으로 연결합니다. 사용자는 장치의 XenMobile에서 연결을 시작해야 합니다. Citrix는 이 옵션을 프로덕션 배포에 권장하지 않습니다. 이 옵션은 장치에 보안 정책을 배포하는 것을 방해하여 사용자가 새로운 앱이나 정책을 전혀 받지 못하게 하기 때문입니다.
  - **매번:** 지정된 간격으로 연결합니다. 이 옵션이 적용되고 잠금 또는 초기화와 같은 보안 정책을 보내면, XenMobile은 장치가 다음에 연결할 때 장치에서 작업을 처리합니다. 이 옵션을 선택하면 **N분마다 연결** 필드가 나타나며, 장치가 다시 연결해야 하는 분 수를 입력해야 합니다. 기본값은 **20**입니다.
  - **일정 정의:** 활성화되면, 사용자 장치의 XenMobile은 네트워크 연결이 끊어진 후 XenMobile Server에 다시 연결을 시도하고, 정의한 시간 프레임 내에서 제어 패킷을 정기적으로 전송하여 연결을 모니터링합니다. 연결 시간 프레임을 정의하는 방법은 다음 섹션인 연결 시간 프레임 정의를 참조하십시오.
    - **이 시간 동안 영구 연결 유지:** 사용자 장치는 정의된 시간 프레임 동안 연결되어 있어야 합니다.
    - **각 범위 내에서 연결 필요:** 사용자 장치는 정의된 시간 프레임 중 하나에서 최소 한 번 연결되어야 합니다.

- **UTC 대신 로컬 장치 시간 사용:** 정의된 시간 프레임을 협정 세계시(UTC) 대신 로컬 장치 시간과 동기화합니다.

연결 시간 프레임 정의

다음 옵션을 활성화하면 원하는 시간 프레임을 정의할 수 있는 타임라인이 나타납니다. 특정 시간 동안 영구 연결을 요구하거나 특정 시간 프레임 내에서 연결을 요구하도록 두 옵션 중 하나 또는 둘 다 활성화할 수 있습니다. 타임라인의 각 칸은 30분입니다. 따라서 매주 평일 오전 8시부터 오전 9시 사이에 연결을 원한다면, 매주 평일 오전 8시에서 오전 9시 사이의 타임라인에 있는 두 칸을 클릭합니다.

예를 들어, 다음 그림의 두 타임라인은 매주 평일 오전 8시부터 오전 9시 사이에 영구 연결, 토요일 오전 12시부터 일요일 오전 1시 사이에 영구 연결, 그리고 매주 평일 오전 5시부터 오전 8시 사이 또는 오전 10시부터 오후 11시 사이에 최소 한 번의 연결을 요구합니다.

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policy-scheduling-define-schedule.png)

연락처 (CardDAV) 장치 정책

XenMobile®에서 장치 정책을 추가하여 사용자의 iOS 또는 macOS 장치에 iOS 연락처(CardDAV) 계정을 추가할 수 있습니다. 이를 통해 사용자는 CardDAV를 지원하는 모든 서버와 연락처 데이터를 동기화할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이 필드는 필수입니다.
- **호스트 이름:** CardDAV 서버의 주소를 입력합니다. 이 필드는 필수입니다.
- **포트:** CardDAV 서버에 연결할 포트를 입력합니다. 이 필드는 필수입니다. 기본값은 **8443**입니다.
- **주요 URL:** 사용자의 캘린더에 대한 기본 URL을 입력합니다.
- **사용자 이름:** 사용자의 로그온 이름을 입력합니다. 이 필드는 필수입니다.
- **암호:** 선택 사항인 사용자 암호를 입력합니다.
- **SSL 사용:** CardDAV 서버에 Secure Socket Layer 연결을 사용할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
- **정책 설정**

- **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
  - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
  - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- **계정 설명:** 계정 설명을 입력합니다. 이 필드는 필수입니다.
- **호스트 이름:** CardDAV 서버 주소를 입력합니다. 이 필드는 필수입니다.
- **포트:** CardDAV 서버에 연결할 포트를 입력합니다. 이 필드는 필수입니다. 기본값은 **8443**입니다.
- **주요 URL:** 사용자 캘린더의 기본 URL을 입력합니다.
- **사용자 이름:** 사용자의 로그온 이름을 입력합니다. 이 필드는 필수입니다.
- **암호:** 선택 사항인 사용자 암호를 입력합니다.
- **SSL 사용:** CardDAV 서버에 보안 소켓 계층 연결을 사용할지 여부를 선택합니다. 기본값은 **켜기**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책이 제거될 때까지의 시간을 숫자로 입력합니다.
  - **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다. **암호 필요**를 선택한 경우 **제거 암호** 필드에 암호를 입력합니다.
  - **프로필 범위:** 이 정책을 **사용자**에게 적용할지 또는 전체 **시스템**에 적용할지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

OS 업데이트 제어 장치 정책

OS 업데이트 제어 장치 정책을 통해 다음을 배포할 수 있습니다:

- 감독되는 iOS 장치에 최신 OS 업데이트를 배포합니다.

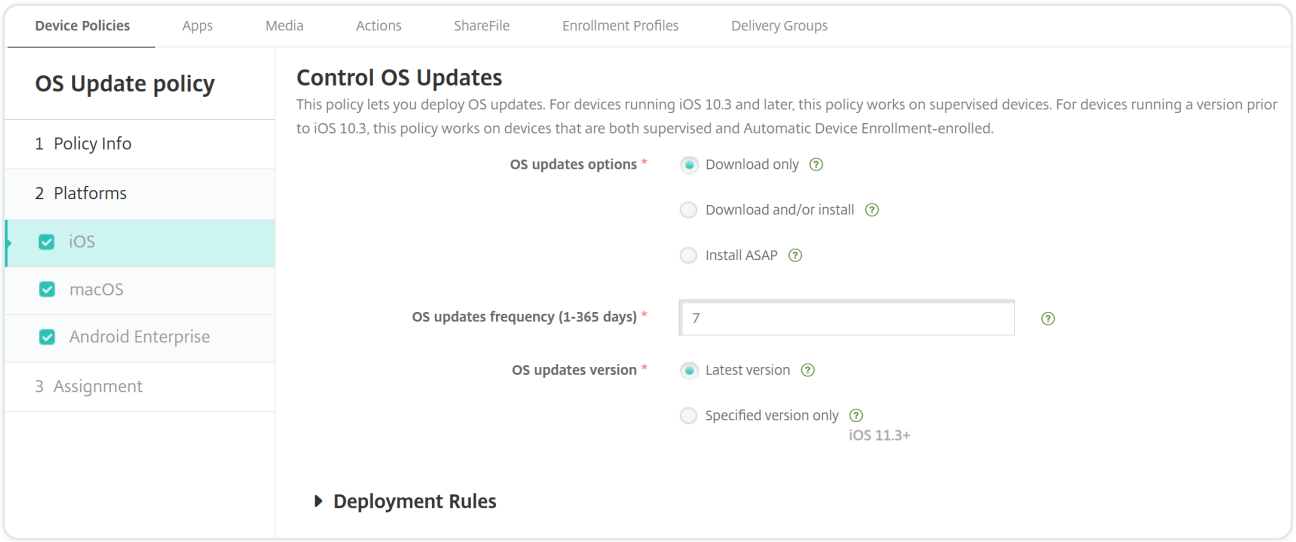
  OS 업데이트 장치 정책은 Apple 배포 프로그램에 등록된 감독되는 장치에서만 작동합니다.
- macOS 10.11.5 이상을 실행하는 DEP 등록 macOS 장치에 최신 OS 및 앱 업데이트를 배포합니다.

- Android Enterprise Work Managed 장치에 최신 OS 업데이트를 배포합니다.

  Android Enterprise Work Managed 장치의 경우, XenMobile®은 OS 업데이트 제어 정책을 Secure Hub로 전송하고, Secure Hub는 해당 정책을 장치에 적용합니다. **관리** > **장치** 페이지에는 XenMobile Server가 정책을 전송한 시점과 장치가 정책을 수신한 시점이 표시됩니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



- **OS 업데이트 옵션:**
  - **다운로드만:** OS 업데이트 빈도에 따라 최신 OS 업데이트를 감독되는 장치에 다운로드하지만 설치하지는 않습니다.
  - **다운로드 및/또는 설치:** OS 업데이트 빈도에 따라 최신 OS 업데이트를 감독되는 장치에 다운로드합니다. 장치에서 업데이트 설치를 요청합니다. 장치 잠금을 해제하면 프롬프트가 표시됩니다.
  - **즉시 설치:** 이전에 다운로드한 OS 업데이트를 즉시 설치할 수 있습니다.
- **OS 업데이트 빈도:** XenMobile이 장치 OS를 확인하고 업데이트하는 빈도를 결정합니다. 기본값은 **7**일입니다.
- **OS 업데이트 버전:** 감독되는 iOS 장치를 업데이트하는 데 사용할 OS 버전을 지정합니다. 기본값은 **최신 버전**입니다.
  - **최신 버전:** 최신 OS 버전으로 업데이트하려면 선택합니다.
  - **특정 버전만:** 특정 OS 버전으로 업데이트하려면 선택한 다음 버전 번호를 입력합니다. 이 옵션은 iOS 11.3 이상에 적용됩니다.

macOS 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/control-os-update-macos-platform.png)

- **OS 업데이트 옵션:** 두 옵션 모두 **OS 업데이트 빈도**에 따라 최신 macOS 업데이트를 다운로드합니다. 업데이트를 설치하거나 App Store를 통해 사용자에게 업데이트가 있음을 알릴 수 있습니다.
- **OS 업데이트 빈도:** XenMobile이 장치 OS를 확인하고 업데이트하는 빈도를 결정합니다. 기본값은 **7**일입니다.

iOS 및 macOS 업데이트 작업 상태 가져오기

iOS 및 macOS의 경우 XenMobile은 제어 OS 업데이트 정책을 장치에 배포하지 않습니다. 대신 XenMobile은 정책을 사용하여 다음 MDM 명령을 장치에 보냅니다.

- OS 업데이트 검사 예약: 장치가 OS 업데이트에 대한 백그라운드 검사를 수행하도록 요청합니다. (iOS의 경우 선택 사항)
- 사용 가능한 OS 업데이트: 장치에 사용 가능한 OS 업데이트 목록을 쿼리합니다.
- OS 업데이트 예약: 장치가 macOS 업데이트, 앱 업데이트 또는 둘 다 수행하도록 요청합니다. 따라서 장치 OS는 OS 및 앱 업데이트를 다운로드하거나 설치해야 하는 시기를 결정합니다.

관리 > 장치 > 장치 세부 정보 (일반) 페이지에는 예약된 및 사용 가능한 OS 업데이트 검사, 예약된 macOS 및 앱 업데이트 상태가 표시됩니다.

장치 세부 정보 화면 이미지(/en-us/xenmobile/server/media/control-os-update-general.png)

업데이트 작업 상태에 대한 자세한 내용은 **관리 > 장치 > 장치 세부 정보 (전송 그룹)** 페이지로 이동하십시오.

장치 세부 정보 화면 이미지(/en-us/xenmobile/server/media/control-os-update-delivery-group.png)

사용 가능한 OS 업데이트 및 마지막 설치 시도와 같은 세부 정보를 보려면 **관리 > 장치 > 장치 세부 정보(속성)** 페이지로 이동합니다.

장치 세부 정보 화면 이미지(/en-us/xenmobile/server/media/control-os-update-system-properties.png)

장치 세부 정보 화면 이미지(/en-us/xenmobile/server/media/control-os-update-custom-properties.png)

Android Enterprise에 대한 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policies-control-os-updates-android-enterprise.png)

- **시스템 업데이트 정책:** 시스템 업데이트가 발생하는 시기를 결정합니다. **Control Enterprise FOTA** 설정을 사용하도록 설정하면 이 설정의 구성과 관계없이 업데이트가 자동으로 발생합니다.

- **자동:** 업데이트가 사용 가능할 때 설치합니다.
- **창 방식: 시작 시간** 및 **종료 시간**에 지정된 일일 유지 관리 기간 내에 업데이트를 자동으로 설치합니다.
  - **시작 시간:** 장치 현지 시간으로 자정부터의 분 단위(**0** - **1440**)로 측정되는 유지 관리 기간의 시작입니다. 기본값은 **0**입니다.
  - **종료 시간:** 장치 현지 시간으로 자정부터의 분 단위(**0** - **1440**)로 측정되는 유지 관리 기간의 끝입니다. 기본값은 **120**입니다.
- **연기:** 사용자가 업데이트를 최대 30일까지 연기할 수 있도록 허용합니다.
- **기본값:** 업데이트 정책을 시스템 기본값으로 설정합니다.

- **무선 업그레이드 허용:** 비활성화된 경우 사용자 장치는 무선으로 소프트웨어 업데이트를 받을 수 없습니다. 기본값은 **켜짐**입니다.

자격 증명 장치 정책

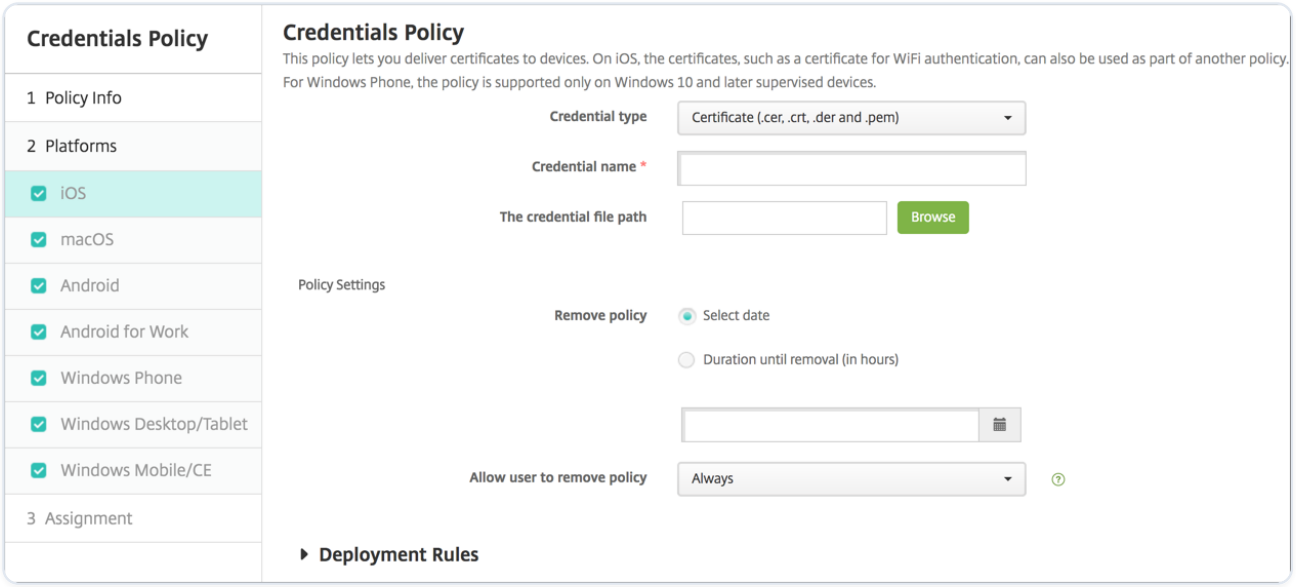
자격 증명 장치 정책은 XenMobile에 구성된 PKI를 가리킵니다. 예를 들어, PKI 구성에는 PKI 엔터티, 키 저장소, 자격 증명 공급자 또는 서버 인증서가 포함될 수 있습니다. 자격 증명에 대한 자세한 내용은 인증서 및 인증을 참조하십시오.

지원되는 각 플랫폼에는 다른 값 집합이 필요하며, 이 문서에 설명되어 있습니다.

> **참고:**
>
> 이 정책을 생성하기 전에 각 플랫폼에 사용할 자격 증명 정보와 모든 인증서 및 암호가 필요합니다.

> 이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

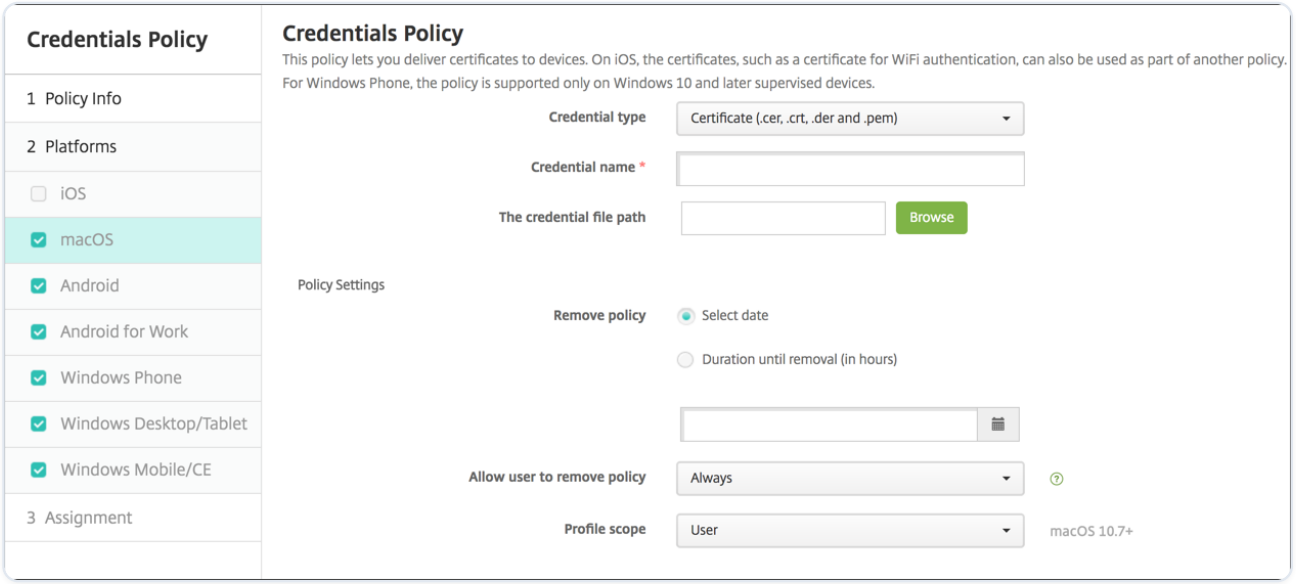


다음 설정을 구성합니다.

- **자격 증명 유형:** 이 정책과 함께 사용할 드롭다운 목록에서 자격 증명 유형을 클릭한 다음 선택한 자격 증명에 대한 다음 정보를 입력합니다.
  - **인증서**
    - **자격 증명 이름:** 자격 증명에 대한 고유한 이름을 입력합니다.
    - **자격 증명 파일 경로:** 찾아보기를 클릭하여 자격 증명 파일을 선택하고 파일 위치로 이동합니다.
  - **키 저장소**
    - **자격 증명 이름:** 자격 증명에 대한 고유한 이름을 입력합니다.
    - **자격 증명 파일 경로:** 찾아보기를 클릭하여 자격 증명 파일을 선택하고 파일 위치로 이동합니다.
    - **암호:** 자격 증명에 대한 키 저장소 암호를 입력합니다.
  - **서버 인증서**
    - **서버 인증서:** 드롭다운 목록에서 사용할 인증서를 클릭합니다.
  - **자격 증명 공급자**
    - **자격 증명 공급자:** 드롭다운 목록에서 자격 증명 공급자의 이름을 클릭합니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.

- **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
- **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

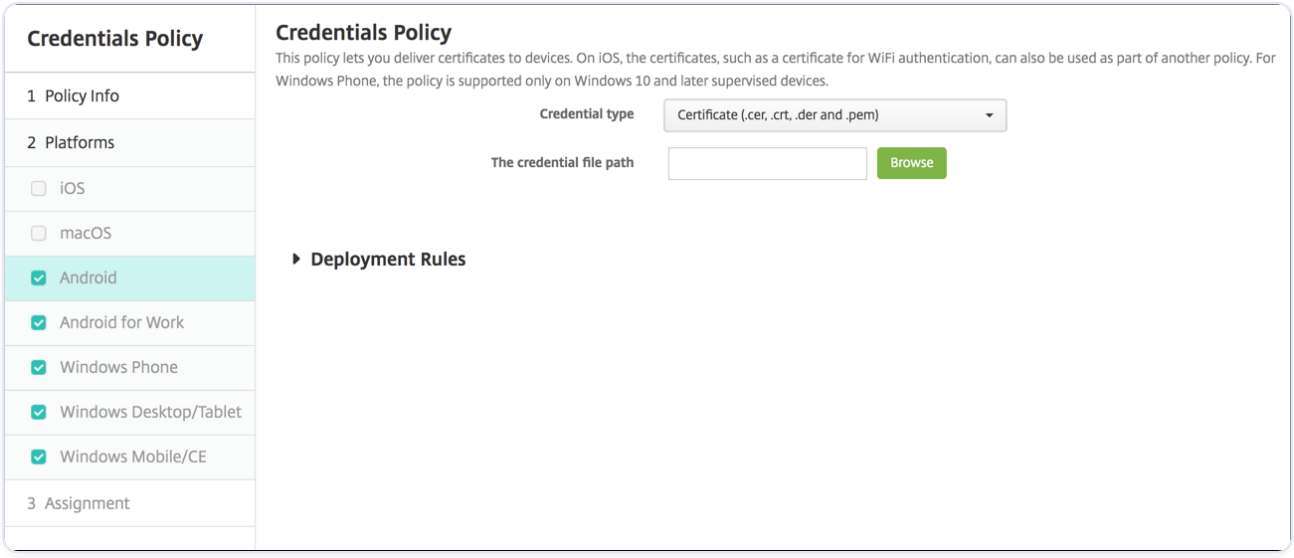


다음 설정을 구성합니다.

- **자격 증명 유형:** 이 정책과 함께 사용할 자격 증명 유형을 드롭다운 목록에서 클릭한 다음 선택한 자격 증명에 대한 다음 정보를 입력합니다.
  - **인증서**
    - **자격 증명 이름:** 자격 증명에 대한 고유한 이름을 입력합니다.
    - **자격 증명 파일 경로: 찾아보기**를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
  - **키 저장소**
    - **자격 증명 이름:** 자격 증명에 대한 고유한 이름을 입력합니다.
    - **자격 증명 파일 경로: 찾아보기**를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
    - **암호:** 자격 증명에 대한 키 저장소 암호를 입력합니다.
  - **서버 인증서**
    - **서버 인증서:** 드롭다운 목록에서 사용할 인증서를 클릭합니다.
  - **자격 증명 공급자**
    - **자격 증명 공급자:** 드롭다운 목록에서 자격 증명 공급자의 이름을 클릭합니다.

- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.
  - **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다. **암호 필요**를 선택하는 경우 **제거 암호** 필드에 암호를 입력합니다.
  - **프로필 범위:** 이 정책을 **사용자**에게 적용할지 아니면 전체 **시스템**에 적용할지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Android 설정



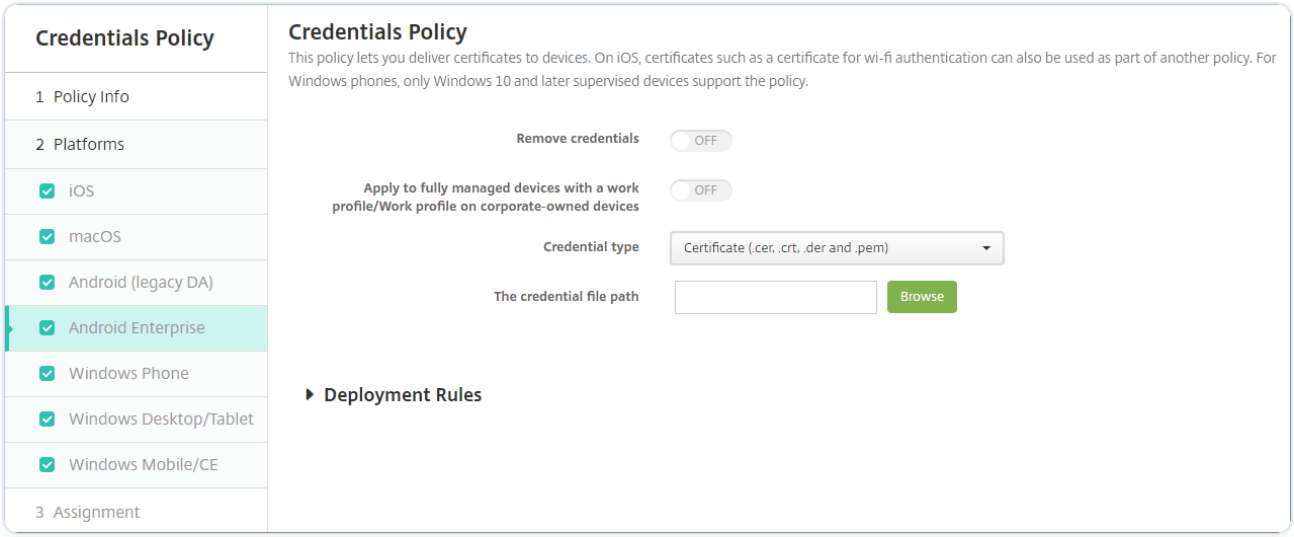
다음 설정을 구성합니다.

- **자격 증명 유형:** 이 정책과 함께 사용할 자격 증명 유형을 드롭다운 목록에서 클릭한 다음 선택한 자격 증명에 대한 다음 정보를 입력합니다.
  - **인증서**
    - **자격 증명 이름:** 자격 증명에 대한 고유한 이름을 입력합니다.
    - **자격 증명 파일 경로:** 찾아보기를 클릭하여 자격 증명 파일을 선택한 다음 파일 위치로 이동합니다.
  - **키 저장소**
    - **자격 증명 이름:** 자격 증명에 대한 고유한 이름을 입력합니다.

- **자격 증명 파일 경로: 찾아보기**를 클릭하여 자격 증명 파일을 선택한 다음 파일 위치로 이동합니다.
- **암호:** 자격 증명에 대한 키 저장소 암호를 입력합니다.

- **서버 인증서**
  - **서버 인증서:** 사용할 인증서를 드롭다운 목록에서 클릭합니다.
- **자격 증명 공급자**
  - **자격 증명 공급자:** 드롭다운 목록에서 자격 증명 공급자의 이름을 클릭합니다.

안드로이드 엔터프라이즈 설정



XenMobile®이 자격 증명 설정을 적용하는 방법을 결정하려면 다음 설정을 구성합니다.

- **자격 증명 제거:** 다음 설정을 구성하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
  - **사용자 자격 증명 제거:** 관리되는 키 저장소에서 인증서를 제거합니다. 기본값은 **꺼짐**입니다.
  - **신뢰할 수 있는 루트 인증서 제거:** 모든 비시스템 CA 인증서를 제거합니다. 기본값은 **꺼짐**입니다.
- **작업 프로필이 있는 완전 관리형 장치/회사 소유 장치의 작업 프로필에 적용:** 작업 프로필이 있는 완전 관리형 장치에 대한 자격 증명 정책 설정을 구성할 수 있습니다. 이 설정이 **켜짐**이면 구성하는 자격 증명 설정이 작업 프로필에만 적용됩니다. 이 설정이 **꺼짐**이면 구성하는 자격 증명 설정이 장치에만 적용됩니다. 기본값은 **꺼짐**입니다.

자격 증명 설정을 구성합니다.

- **자격 증명 유형:** 이 정책과 함께 사용할 자격 증명 유형을 드롭다운 목록에서 클릭한 다음 선택한 자격 증명에 대한 다음 정보를 입력합니다.
  - **인증서**

    - **자격 증명 파일 경로: 찾아보기**를 클릭하여 자격 증명 파일을 선택한 다음 파일 위치로 이동합니다.

  - **키 저장소**

    - **자격 증명 파일 경로: 찾아보기**를 클릭하여 자격 증명 파일을 선택한 다음 파일 위치로 이동합니다.
    - **인증서 별칭:** 인증서 별칭을 사용하면 앱이 인증서에 더 쉽게 액세스할 수 있습니다. 관리되는 구성 장치 정책에서 인증서 별칭을 구성합니다. 그런 다음 자격 증명 장치 정책의 **인증서 별칭** 필드에 별칭을 입력합니다. 앱은 사용자의 작업 없이 인증서를 검색하고 VPN을 인증합니다.
    - **암호:** 자격 증명에 대한 키 저장소 암호를 입력합니다.

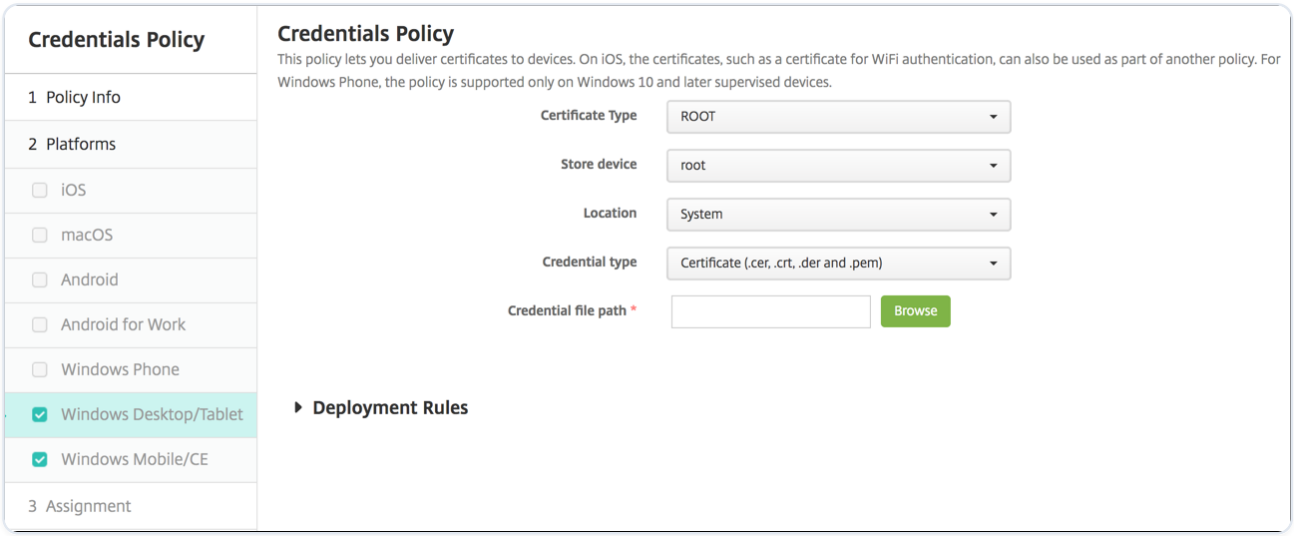
  - **서버 인증서**

    - **서버 인증서:** 사용할 인증서를 드롭다운 목록에서 클릭합니다.

  - **자격 증명 공급자**

    - **인증서 별칭:** 인증서 별칭을 사용하면 앱이 인증서에 더 쉽게 액세스할 수 있습니다. 관리되는 구성 장치 정책에서 인증서 별칭을 구성합니다. 그런 다음 자격 증명 장치 정책의 **인증서 별칭** 필드에 별칭을 입력합니다. 앱은 사용자의 작업 없이 인증서를 검색하고 VPN을 인증합니다.
    - **자격 증명 공급자:** 드롭다운 목록에서 자격 증명 공급자의 이름을 클릭합니다.
    - **인증서를 사용할 앱:** 이 공급자의 자격 증명에 자동 액세스할 앱을 지정하려면 **추가**를 클릭하고 앱을 선택한 다음 **저장**을 클릭합니다.

Windows 데스크톱/태블릿 설정



- **인증서 유형:** 드롭다운 목록에서 **ROOT** 또는 **CLIENT**를 클릭합니다.
- **ROOT**를 클릭하면 다음 설정을 구성합니다.

  - **장치 저장:** 자격 증명에 대한 인증서 저장소 위치에 대해 드롭다운 목록에서 **root**, **My** 또는 **CA**를 클릭합니다. **My**는 사용자 인증서 저장소에 인증서를 저장합니다.
  - **위치:** Windows 10 및 Windows 11 태블릿의 경우 **시스템**이 유일한 위치입니다.
  - **자격 증명 유형:** Windows 10 및 Windows 11 태블릿의 경우 **인증서**가 유일한 자격 증명 유형입니다.
  - **자격 증명 파일 경로: 찾아보기**를 클릭하여 파일 위치로 이동한 다음 인증서 파일을 선택합니다.

- **CLIENT**를 클릭하는 경우, 다음 설정을 구성하십시오:
- **위치:** Windows 10 및 Windows 11 태블릿의 경우, **System**이 유일한 위치입니다.
- **자격 증명 유형:** Windows 10 및 Windows 11 태블릿의 경우, **Keystore**가 유일한 자격 증명 유형입니다.
- **자격 증명 이름:** 자격 증명의 이름을 입력합니다. 이 필드는 필수입니다.
- **자격 증명 파일 경로: 찾아보기**를 클릭하여 인증서 파일을 선택하고 파일 위치로 이동합니다.
- **암호:** 자격 증명과 연결된 암호를 입력합니다. 이 필드는 필수입니다.

사용자 지정 XML 장치 정책

XenMobile®에서 사용자 지정 XML 정책을 생성하여 지원되는 Windows 장치에서 다음 기능을 사용자 지정할 수 있습니다.

- 프로비저닝(장치 구성, 기능 활성화 또는 비활성화 포함)
- 장치 구성(사용자가 설정 및 장치 매개변수를 변경하도록 허용하는 기능 포함)
- 소프트웨어 업그레이드(앱 및 시스템 소프트웨어를 포함하여 장치에 로드할 새 소프트웨어 또는 버그 수정 제공 포함)
- 장애 관리(장치로부터 오류 및 상태 보고서 수신 포함)

> **참고:**

> XML 콘텐츠를 생성할 때 \% 문자를 주의해서 사용하십시오. \% 문자는 XML 특수 문자를 이스케이프하는 데만 사용되는 XML 예약 문자입니다. 이름에 \%를 사용하려면 \%25로 인코딩하십시오.

> Windows 장치의 경우: Windows에서 OMA DM(Open Mobile Alliance Device Management) API를 사용하여 사용자 지정 XML 구성을 생성합니다. OMA DM API를 사용하여 사용자 지정 XML을 생

성하는 것은 이 항목의 범위를 벗어납니다. OMA DM API 사용에 대한 자세한 내용은 Microsoft 개발자 네트워크 사이트의 OMA Device Management를 참조하십시오.

참고:

Windows 10 RS2 Phone의 경우: Internet Explorer를 비활성화하는 사용자 지정 XML 정책 또는 제한 정책이 휴대폰에 배포된 후에도 브라우저는 계속 활성화된 상태로 유지됩니다. 이 문제를 해결하려면 휴대폰을 다시 시작하십시오. 이 문제는 타사 문제입니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

Windows 데스크톱/태블릿 설정

- **XML 콘텐츠:** 정책에 추가할 사용자 지정 XML 코드를 입력하거나 잘라내어 붙여넣습니다.

  다음을 클릭하면 XenMobile이 XML 콘텐츠 구문을 확인합니다. 구문 오류는 콘텐츠 상자 아래에 나타납니다. 계속하기 전에 오류를 수정하십시오.

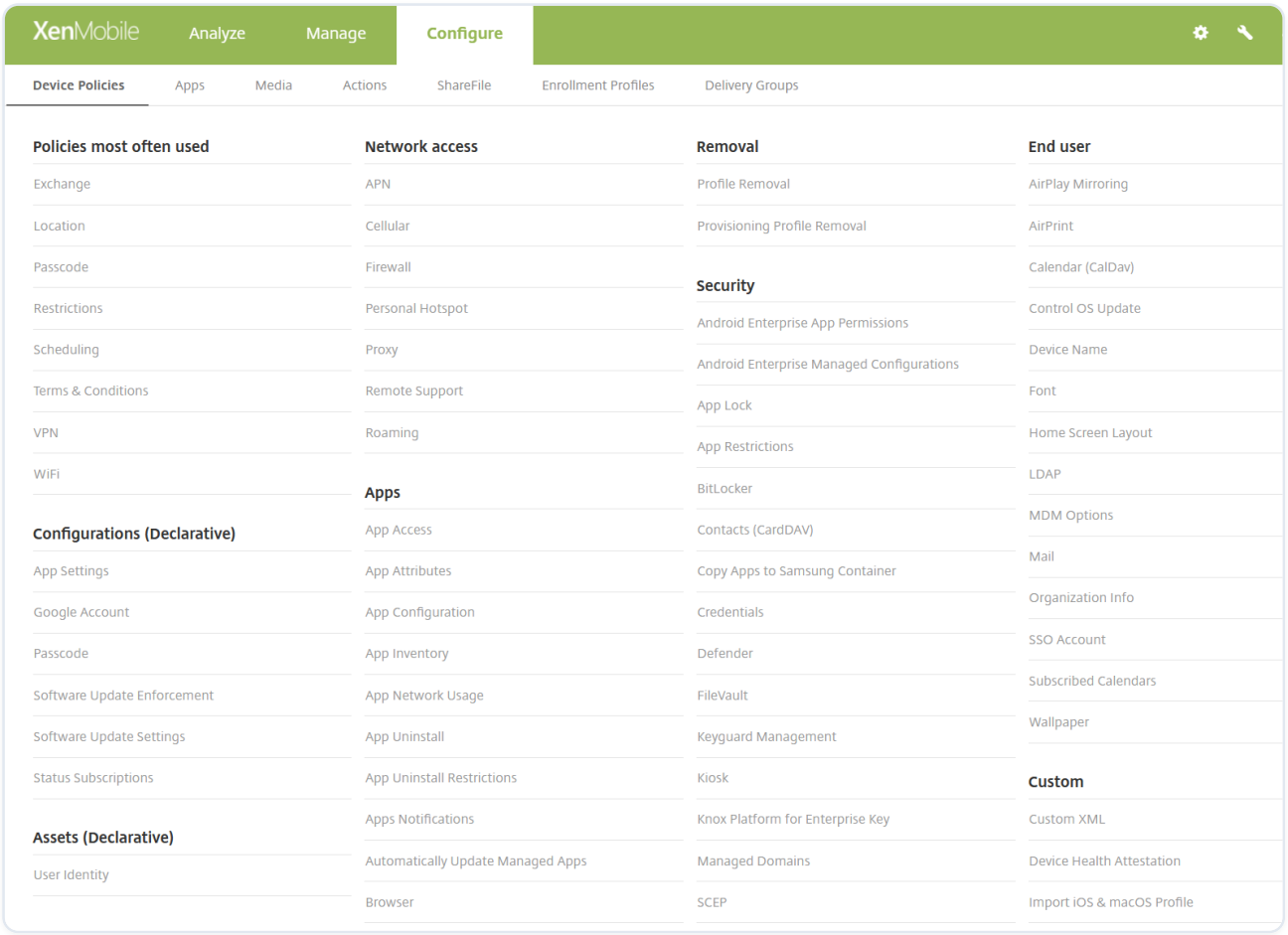
  구문 오류가 없으면 **사용자 지정 XML 정책** 할당 페이지가 표시됩니다.

선언적 장치 관리 정책

Apple은 iOS 15에서 선언적 데이터 모델 패러다임을 사용하여 선언적 장치 관리(DDM)를 발표했습니다. 이 패러다임을 통해 서버는 명령 직렬화 및 MDM을 통한 장치 폴링과 일반적으로 관련된 일반적인 성능 및 확장성 문제를 피할 수 있습니다. 자세한 내용은 장치 확장을 위한 선언적 관리 데이터 모델 활용을 참조하십시오.

DDM 기능을 활성화하면 다음 선언적 장치 정책이 지원됩니다.

- 앱 설정
- Google 계정
- 암호
- 소프트웨어 업데이트 적용
- 소프트웨어 업데이트 설정
- 상태 구독
- 사용자 ID



앱 설정 장치 정책

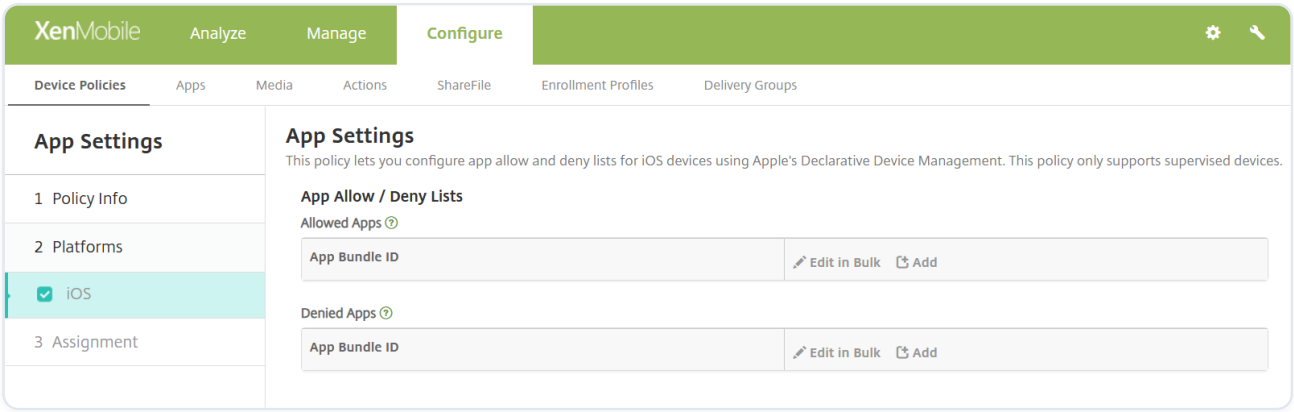
앱 설정 장치 정책을 사용하면 Apple의 선언적 장치 관리를 사용하여 앱 허용 및 거부 목록을 구성할 수 있습니다. 이 정책은 더 이상 사용되지 않는 `allowListedAppBundleIDs` 및 `blockedAppBundleIDs` 제한 키를 대체합니다. 이 정책은 감독되는 장치만 지원합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

- XenMobile Server 10.16 롤링 패치 9 이상.
- 서버 속성 `ios.mdm.ios27.ddm.support`이 **True**로 설정되어 있습니다.
- iOS 27 이상 및 iPadOS 27 이상에서 사용할 수 있습니다. 감독되는 장치만 지원합니다.

iOS 설정



- **앱 허용/거부 목록:**
  - **허용된 앱:** 이 목록에 있는 번들 ID를 가진 앱만 장치에 표시되거나 실행됩니다. 모든 웹 클립을 허용하려면 `com.apple.webapp` 값을 포함하십시오. 이는 App Store 앱, 마켓플레이스 앱 및 로컬에 설치된 앱(Configurator, Xcode 등 사용)에 적용됩니다.
    - **앱 번들 ID:** 앱 번들 ID를 추가하려면 **추가**를 클릭하고 앱 번들 ID를 입력한 다음 **저장**을 클릭합니다. 추가하려는 각 앱 번들 ID에 대해 이 과정을 반복합니다. **대량 편집**을 클릭하여 앱 번들 ID를 한 줄에 하나씩 또는 쉼표로 구분하여 입력하거나 붙여넣은 다음 **저장**을 클릭할 수도 있습니다.
  - **거부된 앱:** 이 목록에 있는 번들 ID를 가진 앱은 장치에 표시되거나 실행되지 않습니다. 모든 웹 클립을 제한하려면 `com.apple.webapp` 값을 포함하십시오. 이는 App Store 앱, 마켓플레이스 앱 및 로컬에 설치된 앱(Configurator, Xcode 등 사용)에 적용됩니다.

참고:

- 시스템 앱을 거부하면 다른 기능이 비활성화될 수 있습니다. 예를 들어, App Store 앱을 거부하면 사용자가 사용자 기반 VPP(볼륨 구매 프로그램)의 약관에 동의하지 못할 수 있습니다.
- 앱 허용 목록 또는 앱 거부 목록 중 하나를 구성하는 것을 권장하며, 둘 다 구성하지 마십시오.

Google 계정 장치 정책

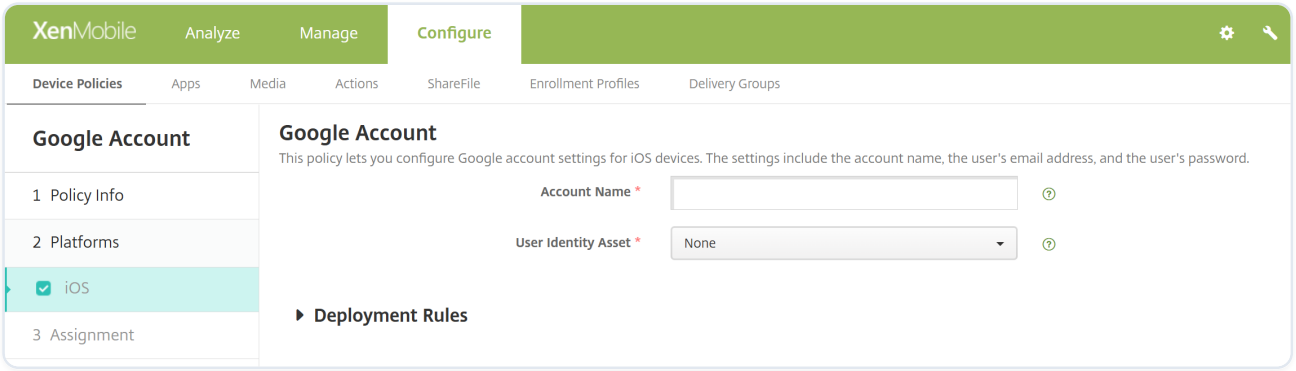
Google 계정 장치 정책을 사용하면 iOS 장치에 대한 Google 계정 설정을 구성할 수 있습니다. 이 설정에는 계정 이름과 이메일 주소 및 사용자의 전체 이름을 구성하는 사용자 ID 자산이 포함됩니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

- XenMobile Server 10.16 롤링 패치 8 이상.
- 서버 속성 `ios.mdm.declarative.management`이 **True**로 설정됩니다.
- 사용자 ID 정책이 구성됩니다. 사용자 ID 장치 정책을 참조하십시오.

iOS 설정



- **계정 이름:** Google 계정의 이름을 입력합니다.
- **사용자 ID 자산:** 목록에서 사용자의 이메일 주소와 전체 이름이 포함된 사용자 ID 정책에 의해 생성된 사용자 ID 자산을 선택합니다. 기본값은 **없음**입니다.

암호 장치 정책

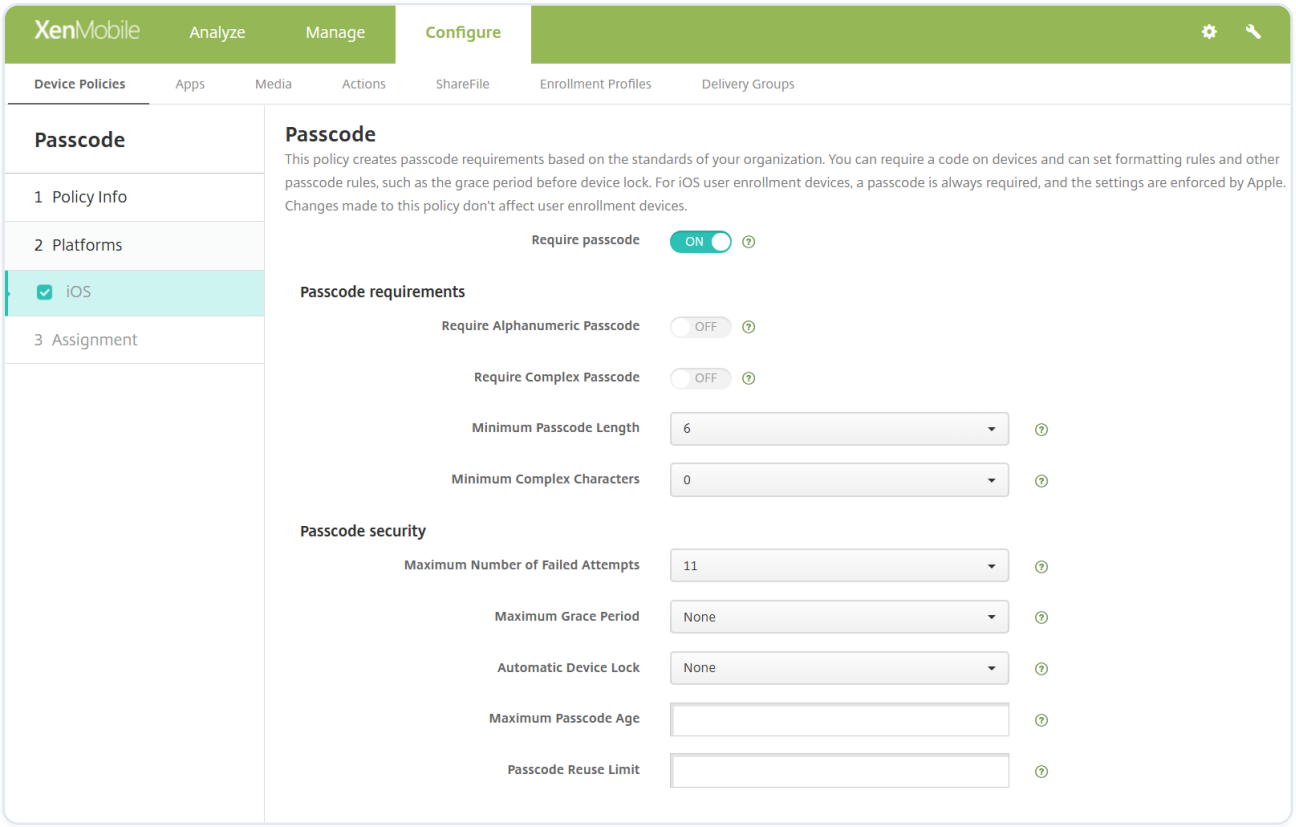
암호 장치 정책은 조직의 표준에 따라 암호 요구 사항을 생성합니다. 장치에 암호를 요구하고 서식 규칙 및 장치 잠금 전 유예 기간과 같은 기타 암호 규칙을 설정할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

- XenMobile Server 10.16 롤링 패치 8 이상.
- 서버 속성 `ios.mdm.declarative.management`이 **True**로 설정되어 있습니다.

iOS 설정



- **암호 요구:** 암호를 요구하고 iOS 암호 장치 정책에 대한 구성 옵션을 표시하려면 이 옵션을 선택합니다. **켜짐**으로 설정하면 사용자는 암호 길이 또는 품질에 대한 요구 사항 없이 암호를 설정해야 하며, 암호 요구 사항 및 암호 보안 설정을 구성할 수 있도록 페이지가 확장됩니다. 기본값은 **켜짐**입니다.
- **암호 요구 사항**
  - **영숫자 암호 요구:** 암호에 하나 이상의 알파벳 문자와 하나 이상의 숫자가 포함되어야 하는지 여부를 선택합니다. 기본값은 **꺼짐**입니다.
  - **복잡한 암호 요구:** 복잡한 암호를 요구할지 여부를 선택합니다. 복잡한 암호는 반복되는 문자나 증가 또는 감소하는 문자(예: 123 또는 CBA)를 포함하지 않으며, 하나 이상의 비숫자 및 비알파벳 문자를 포함해야 합니다. 기본값은 **꺼짐**입니다.
  - **최소 암호 길이:** 암호에 포함될 수 있는 최소 문자 수를 선택합니다. 기본값은 **6**입니다.
  - **최소 복잡한 문자 수:** 암호에 포함될 최소 복잡한 문자 수를 선택합니다. 복잡한 문자는 숫자나 문자가 아닌 문자(예: &, %, $, #)입니다. 기본값은 **0**입니다.
- **암호 보안**
  - **최대 실패 시도 횟수:** iOS가 장치를 지우기 전에 시스템이 사용자에게 허용하는 실패한 암호 시도 횟수를 선택합니다. 이 설정을 변경하지 않으면 6번의 실패 시도 후 장치는 사용자가 암호를 다시 입력하기 전에 시간 지연을 적용합니다. 시간 지연은 실패 시도 횟수가 늘어날수록 증가합니다. 마지막 실패 시도 후 시스템은 iOS 장치에서 모든 데이터와 설정을 안전하게 지웁니다. 암호 시간 지연은 6번째 시

도 후에 시작되므로, 이 값이 6 이하이면 시스템은 시간 지연 없이 사용자가 제한을 초과하는 즉시 지우기 또는 잠금을 트리거합니다. 기본값은 **11**입니다.

- **최대 유예 기간:** 사용자가 암호 없이 장치를 잠금 해제할 수 있는 최대 기간을 선택합니다. 유예 기간이 없도록 **즉시**를 선택하면 장치는 즉시 암호를 요구합니다. 기본값은 **없음**이며, 이는 사용자가 어떤 기간이든 선택할 수 있음을 의미합니다.
- **자동 장치 잠금:** 시스템이 장치를 자동으로 잠그기 전에 장치가 유휴 상태일 수 있는 최대 기간을 선택합니다. 장치가 이 제한에 도달하면 장치가 잠기고 사용자는 잠금 해제를 위해 암호를 입력해야 합니다. 기본값은 **없음**이며, 이는 사용자가 어떤 기간이든 선택할 수 있음을 의미합니다.
- **최대 암호 사용 기간:** 암호가 변경되지 않은 상태로 유지될 수 있는 최대 일수를 선택합니다. 이 일수가 지나면 시스템은 장치를 잠금 해제하기 전에 사용자에게 암호를 변경하도록 강제합니다. 유효한 값은 0–730입니다. **0** 값은 즉시 암호 변경을 강제합니다. 기본값은 비어 있으며, 이는 암호 사용 기간 제한이 없음을 의미합니다.
- **암호 재사용 제한:** 새 암호를 확인할 때 시스템이 확인하는 이전 암호 항목의 수를 선택합니다. 지정된 암호 기록 범위 내에서 이전에 사용된 암호와 일치하는 경우 장치는 새 암호를 거부합니다. 유효한 값은 1–50입니다. 기본값은 비어 있으며, 이는 시스템이 기록 확인을 수행하지 않음을 의미합니다.

> **참고:**
>
> 동일한 설정이 MDM 프로필 및 선언적 구성으로 장치에 전송되는 경우, 해당 설정이 여러 프로필에 의해 전달된 것과 동일한 규칙이 적용됩니다. 예를 들어, 암호 정책이 프로필(암호 정책을 통해) 및 구성(선언적 암호 정책을 통해)으로 구성된 경우, 정책이 병합되고 가장 엄격한 설정이 적용됩니다.

소프트웨어 업데이트 적용 장치 정책

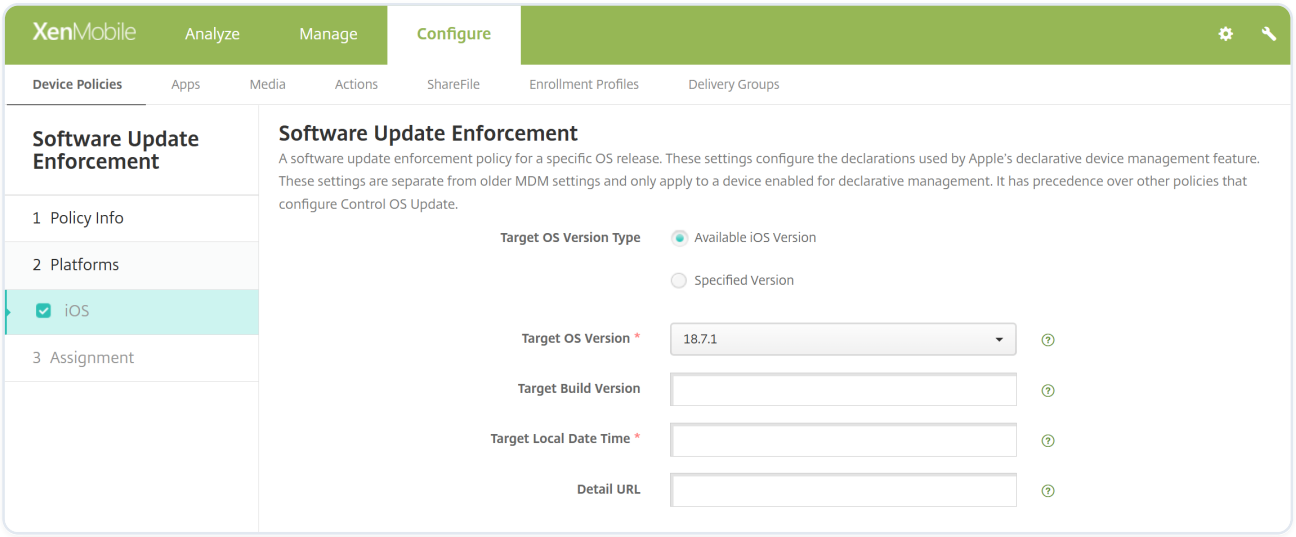
특정 OS 릴리스에 대한 소프트웨어 업데이트 적용 장치 정책을 통해 IT 관리자는 iOS 장치 업데이트를 관리하여 어떤 업데이트를 적용할지 제어하고 모든 업데이트 완료 기한을 설정할 수 있습니다. 이러한 설정은 Apple의 선언적 장치 관리 기능에서 사용하는 선언을 구성합니다. 이 설정은 이전 MDM 설정과 별개이며 선언적 관리가 활성화된 장치에만 적용됩니다. 동일한 설정에 대해 OS 업데이트 제어 정책보다 우선합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 다음을 참조하십시오. 장치 정책.

사전 요구 사항

- XenMobile Server 10.16 롤링 패치 8 이상.
- 서버 속성 `ios.mdm.declarative.management`이 **True**로 설정되어 있습니다.
- **iOS 17.0** 이상 및 **iPadOS 17.0** 이상에서 사용 가능합니다.

iOS 설정



- **대상 OS 버전 유형:** 대상 OS 버전을 구성하는 방법을 지정합니다. 기본값은 **사용 가능한 iOS 버전**입니다.
  - **사용 가능한 iOS 버전: 켜짐**으로 설정하면 **대상 OS 버전**에 사용 가능한 대상 OS 버전이 나열됩니다.
  - **지정된 버전: 켜짐**으로 설정하면 제안된 형식으로 OS 버전을 수동으로 입력합니다.
- **대상 OS 버전: (필수)** 적절한 시간까지 장치를 업데이트할 대상 OS 버전을 선택하거나 입력합니다. 이는 OS 버전 번호(예: 17.7)입니다. 보조 버전 식별자(예: 17.7.2)를 포함할 수도 있습니다.
- **대상 빌드 버전:** 적절한 시간까지 장치를 업데이트할 대상 빌드 버전(예: 20A242)을 입력합니다. 시스템은 시드 기간 동안 테스트를 위해 빌드 버전을 사용합니다. 빌드 버전에는 보조 버전 식별자(예: 20A242a)가 포함될 수 있습니다. 빌드 버전이 TargetOSVersion 키에 지정된 대상 OS 버전과 일치하지 않으면 대상 OS 버전이 우선합니다.
- **대상 현지 날짜 시간: (필수)** 소프트웨어 업데이트를 강제로 설치할 시점을 지정하는 현지 날짜 시간 값을 입력합니다. RFC3339에서 파생되었지만 시간대 오프셋을 포함하지 않는 yyyy-mm-ddThh:mm:ss 형식을 사용합니다. 사용자가 이 시간 전에 소프트웨어 업데이트를 트리거하지 않으면 장치가 강제로 설치합니다.
- **상세 URL:** 조직에서 제공하는 적용된 업데이트에 대한 세부 정보를 표시하는 웹 페이지의 URL을 입력합니다.

> **참고:**
>
> 소프트웨어 업데이트 적용 정책과 OS 업데이트 제어 정책은 모두 장치의 OS 업데이트를 관리할 수 있습니다. 그러나 소프트웨어 업데이트 적용 정책이 OS 업데이트 제어 정책보다 우선합니다. 두 정책이

> 동일한 설정으로 배포되면 OS 업데이트 제어 정책의 구성은 무시되고 적용되지 않습니다. 자세한 내용은 선언적 장치 관리로 전환을 참조하십시오.

> 또한 소프트웨어 업데이트 적용 정책과 OS 업데이트 제어 정책 간에는 몇 가지 차이점이 있습니다.

정책 유형	소프트웨어 업데이트 적용	OS 업데이트 제어
장치 유형	감독 또는 비감독 장치	감독 장치
업데이트 기한 적용	✓	✗
도움말 URL 입력	✓	✗
빌드 버전 번호 지정	✓	✗
최신 업데이트 자동 배포	✗	✓
최소 지원 버전	iOS 17.0	iOS 10.3 (감독됨)

소프트웨어 업데이트 설정 장치 정책

소프트웨어 업데이트 설정 장치 정책은 OS 업데이트를 연기하고 시스템 설정에서 사용자가 소프트웨어 업데이트와 수동으로 상호 작용하는 방식을 제어하는 데 사용할 수 있습니다. 이 정책은 감독 대상 장치만 지원합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

- XenMobile Server 10.16 롤링 패치 8 이상.
- 서버 속성 `ios.mdm.declarative.management` 및 `ios.mdm.software.update.settings`가 **True**로 설정되어 있습니다.
- **iOS 18.0** 이상 및 **iPadOS 18.0** 이상에서 사용 가능하며, 감독 대상 장치만 지원합니다.

iOS 설정

소프트웨어 업데이트 설정 장치 정책](/en-us/xenmobile/server/media/software-update-setting-ios-settings1.png)

- **자동 작업**

  - **다운로드:** 사용자가 사용 가능한 업데이트의 자동 다운로드를 제어할 수 있는지 여부를 지정합니다. 기본값은 **허용됨**입니다.
    - **허용됨** - 사용자가 자동 다운로드를 활성화하거나 비활성화할 수 있습니다.
    - **항상 켜짐** - 자동 다운로드가 항상 활성화됩니다.
    - **항상 꺼짐** - 자동 다운로드가 항상 비활성화됩니다.
  - **OS 업데이트 설치:** 사용자가 사용 가능한 업데이트의 자동 설치를 제어할 수 있는지 여부를 지정합니다. 기본값은 **허용됨**입니다.
    - **허용됨** - 사용자가 자동 설치를 활성화하거나 비활성화할 수 있습니다.
    - **항상 켜짐** - 자동 설치가 항상 활성화됩니다.
    - **항상 꺼짐** - 자동 설치가 항상 비활성화됩니다.

- **연기**
  - **결합된 기간(일):** 장치에서 주요 또는 부 OS 소프트웨어 업데이트를 연기할 일수를 지정합니다. 설정하면 소프트웨어 업데이트 릴리스 후 지정된 지연 후에만 소프트웨어 업데이트가 나타납니다. iOS 18 이상에서 사용할 수 있습니다. 유효 값은 0~90입니다. 기본값은 **0**이며, 이는 지연이 없음을 의미합니다.
- **권장 주기**
  - **권장 주기:** 장치가 사용자에게 소프트웨어 업데이트를 표시하는 방법을 지정합니다. 두 개 이상의 업데이트를 사용할 수 있는 경우 장치는 다음과 같이 작동합니다. 기본값은 **모두**입니다.
    - **모두** - 모든 소프트웨어 업데이트 버전을 표시합니다.
    - **가장 오래된 버전** - 가장 오래된(낮은 번호의) 소프트웨어 업데이트 버전만 표시합니다.
    - **최신 버전** - 가장 최신(가장 높은 번호의) 소프트웨어 업데이트 버전만 표시합니다.
- **알림**
  - **알림: 켜짐**으로 설정하면 장치가 모든 소프트웨어 업데이트 적용 알림을 표시합니다. **꺼짐**으로 설정하면 장치는 적용 마감 시간 1시간 전에 트리거된 알림과 다시 시작 카운트다운 알림만 표시합니다. 기본값은 **켜짐**입니다.
- **신속 보안 대응**
  - **활성화: 꺼짐**으로 설정하면 사용자 설치를 위한 신속 보안 대응이 제공되지 않습니다. 시스템은 `com.apple.configuration.softwareupdate.enforcement.specific` 구성을 통해 신속

보안 대응을 계속 설치할 수 있습니다. **켜짐**으로 설정하면 시스템이 사용자에게 신속 보안 대응을 제공합니다. 기본값은 **켜짐**입니다.

- **롤백 활성화: 꺼짐**으로 설정하면 시스템이 사용자에게 신속 보안 대응 롤백을 제공하지 않습니다. **켜짐**으로 설정하면 시스템이 사용자에게 신속 보안 대응 롤백을 제공합니다. 기본값은 **켜짐**입니다.

상태 구독 장치 정책

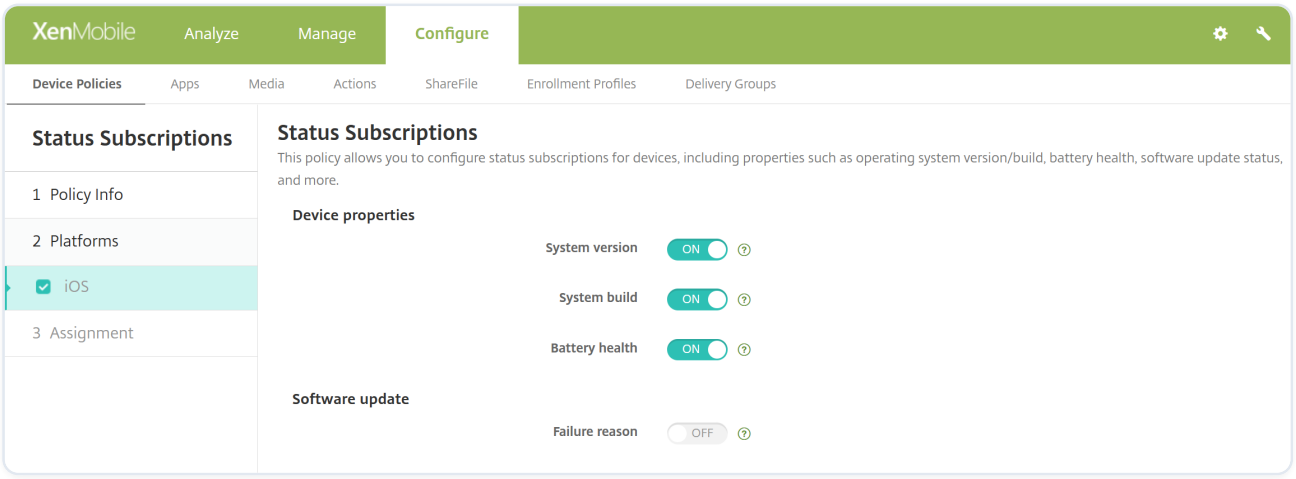
상태 구독 장치 정책을 사용하면 운영 체제 버전/빌드, 배터리 상태, 소프트웨어 업데이트 상태 등과 같은 속성을 포함하여 장치에 대한 상태 구독을 구성할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

- XenMobile Server 10.16 롤링 패치 8 이상.
- 서버 속성 `ios.mdm.declarative.management`이 **True**로 설정되어 있습니다.

iOS 설정



- **장치 속성**
  - **시스템 버전: 켜짐**으로 설정하면 장치가 운영 체제 버전(예: 18.0)을 보고하며, 이는 장치 속성의 시스템 정보 섹션에 표시됩니다. 버전 업그레이드가 발생할 때 장치가 자동으로 보고하므로 유용합니다. 기본값은 **켜짐**입니다. iOS 15 이상에서 사용할 수 있습니다.
  - **시스템 빌드: 켜짐**으로 설정하면 장치가 운영 체제 빌드 버전(예: 18F132)을 보고하며, 이는 장치 속성의 시스템 정보 섹션에 표시됩니다. 버전 업그레이드가 발생할 때 장치가 자동으로 보고하므로 유용합니다. 기본값은 **켜짐**입니다. iOS 15 이상에서 사용할 수 있습니다.

- **배터리 상태: 켜짐**으로 설정하면 장치 속성에 새로운 설정인 **배터리 상태**가 추가됩니다. 이 설정을 통해 관리자는 **관리 > 장치 > 속성 > 배터리 > 배터리 상태**로 이동하여 등록된 iOS 장치의 배터리 상태를 확인할 수 있습니다. 기본값은 **켜짐**입니다. iOS 17 이상에서 사용할 수 있습니다.

- **소프트웨어 업데이트**

  - **실패 이유: 켜짐**으로 설정하면 장치가 실패한 OS 업데이트의 이유를 보고하며, 이는 장치 속성의 소프트웨어 업데이트 정보 섹션에 표시됩니다. 기본값은 **꺼짐**입니다. iOS 17 이상에서 사용할 수 있습니다.

사용자 ID 장치 정책

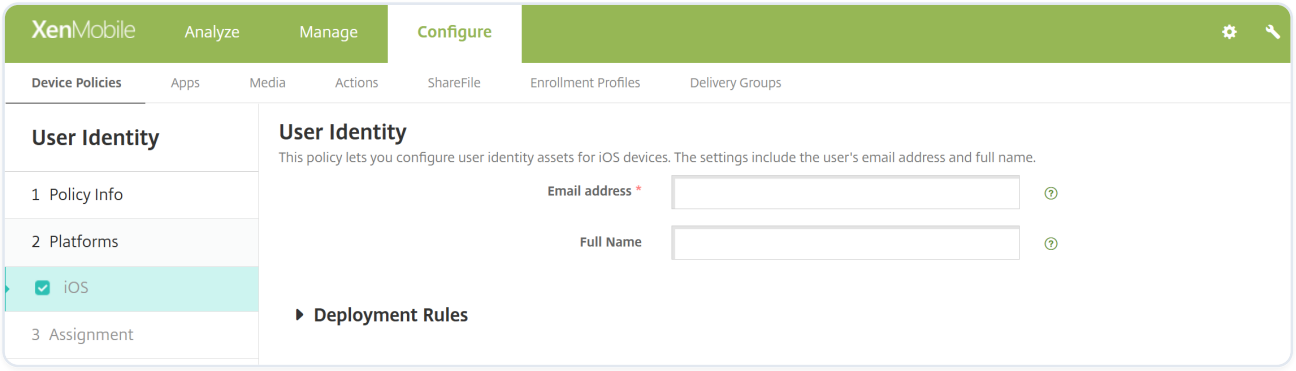
사용자 ID 장치 정책을 사용하면 iOS 장치에 대한 사용자 ID 자산을 구성할 수 있습니다. 설정에는 사용자의 이메일 주소와 전체 이름이 포함됩니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

- XenMobile Server 10.16 롤링 패치 8 이상.
- 서버 속성 `ios.mdm.declarative.management`이(가) **True**로 설정되어 있습니다.

iOS 설정



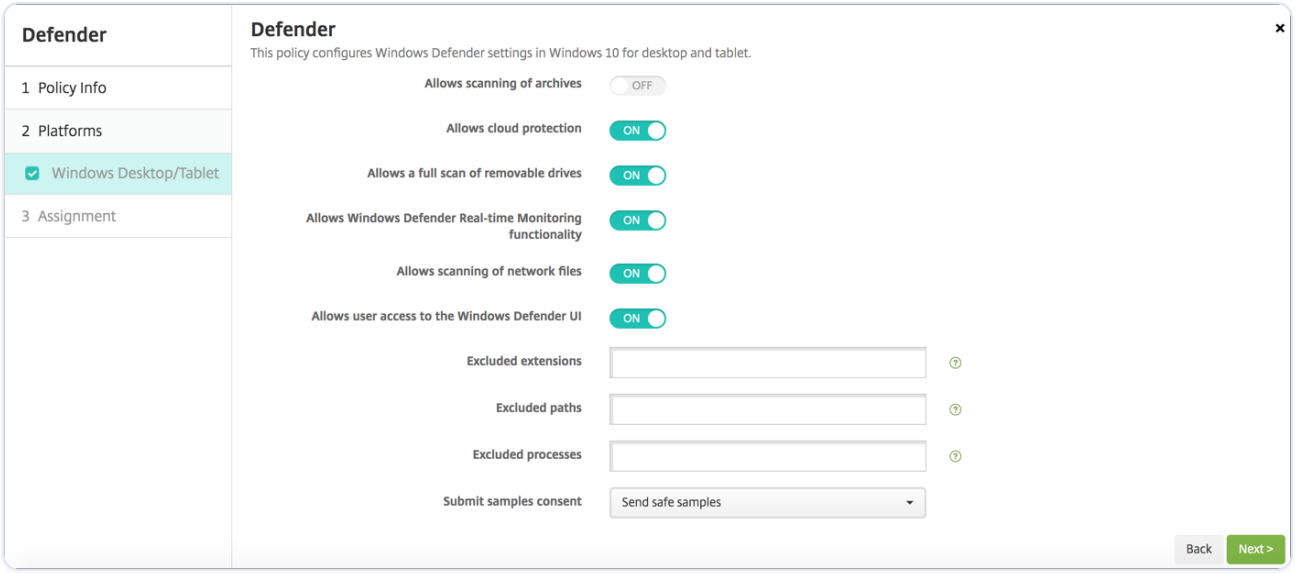
- **이메일 주소:** 사용자의 이메일 주소를 입력합니다. 이 필드는 필수입니다.
- **전체 이름:** 사용자의 전체 이름을 입력합니다.

Defender 장치 정책

Windows Defender는 Windows 10 및 Windows 11에 포함된 맬웨어 방지 기능입니다. XenMobile® 장치 정책인 Defender를 사용하여 데스크톱 및 태블릿용 Windows 10 및 Windows 11의 Microsoft Defender 정책을 구성할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

Windows 데스크톱 및 태블릿 설정



- **보관 파일 검색 허용:** Defender가 보관된 파일을 검색하도록 허용하거나 허용하지 않습니다. 기본값은 **끔**입니다.
- **클라우드 보호 허용:** Defender가 맬웨어 활동에 대한 정보를 Microsoft에 보내도록 허용하거나 허용하지 않습니다. 기본값은 **켬**입니다.
- **이동식 드라이브 전체 검색 허용:** Defender가 USB 스틱과 같은 이동식 드라이브를 검색하도록 허용하거나 허용하지 않습니다. 기본값은 **켬**입니다.
- **Windows Defender 실시간 모니터링 기능 허용:** 기본값은 **켬**입니다.
- **네트워크 파일 검색 허용:** Defender가 네트워크 파일을 검색하도록 허용하거나 허용하지 않습니다. 기본값은 **켬**입니다.
- **사용자의 Windows Defender UI 액세스 허용:** 사용자가 Windows Defender 사용자 인터페이스에 액세스할 수 있는지 여부를 지정합니다. 이 설정은 사용자 장치가 다음에 시작될 때 적용됩니다. 이 설정이 **끔**으로 되어 있으면 사용자는 Windows Defender 알림을 받지 않습니다. 기본값은 **켬**입니다.
- **제외된 확장명:** 실시간 또는 예약된 검색에서 제외할 확장명입니다. 확장명을 구분하려면 **\|** 문자를 사용합니다. 예: "lib\|obj".
- **제외된 경로:** 실시간 또는 예약된 검색에서 제외할 경로입니다. 경로를 구분하려면 **\|** 문자를 사용합니다. 예: "C:\\Example\|C:\\Example1".
- **제외된 프로세스:** 실시간 또는 예약된 검색에서 제외할 프로세스입니다. 프로세스를 구분하려면 **\|** 문자를 사용합니다. 예: "C:\\Example.exe\|C:\\Example1.exe".

- **샘플 제출 동의:** 추가 분석이 필요하여 악성 여부를 판단해야 할 수 있는 파일을 Microsoft에 보낼지 여부를 제어합니다. 옵션: **항상 확인**, **안전한 샘플 보내기**, **절대 보내지 않음**, **모든 샘플 보내기**. 기본값은 **안전한 샘플 보내기**입니다.

장치 상태 증명 장치 정책

XenMobile®에서 Windows 10 및 Windows 11 장치가 분석을 위해 특정 데이터 및 런타임 정보를 Health Attestation Service (HAS)로 전송하도록 하여 장치의 상태를 보고하도록 요구할 수 있습니다. HAS는 장치가 XenMobile로 전송하는 Health Attestation Certificate를 생성하여 반환합니다. XenMobile은 Health Attestation Certificate를 수신하면, 해당 Health Attestation Certificate의 내용에 따라 이전에 설정한 자동 작업을 배포할 수 있습니다.

HAS에 의해 확인되는 데이터는 다음과 같습니다.

- AIK 존재 여부
- BitLocker 상태
- 부팅 디버깅 사용 가능
- 부팅 관리자 개정 목록 버전
- 코드 무결성 사용 가능
- 코드 무결성 개정 목록 버전
- Apple 배포 프로그램 정책
- ELAM 드라이버 로드됨
- 발급 시점
- 커널 디버깅 사용 가능
- PCR
- 재설정 횟수
- 재시작 횟수
- 안전 모드 사용
- SBCP 해시
- 보안 부팅 사용
- 테스트 서명 사용
- VSM 사용
- WinPE 사용

자세한 내용은 Microsoft Device HealthAttestation CSP 페이지를 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

Microsoft Cloud를 사용하여 DHA 구성

장치 상태 증명 정책을 추가하고 선택한 각 플랫폼에 대해 이 설정을 구성합니다.

- **장치 상태 증명 사용:** 장치 상태 증명을 요구할지 여부를 선택합니다. 기본값은 **해제**입니다.

온프레미스 Windows DHA 서버를 사용하여 DHA 구성

온프레미스 DHA를 사용하려면 먼저 DHA 서버를 구성해야 합니다. 그런 다음 온프레미스 DHA 서비스를 사용하도록 XenMobile Server 정책을 생성합니다.

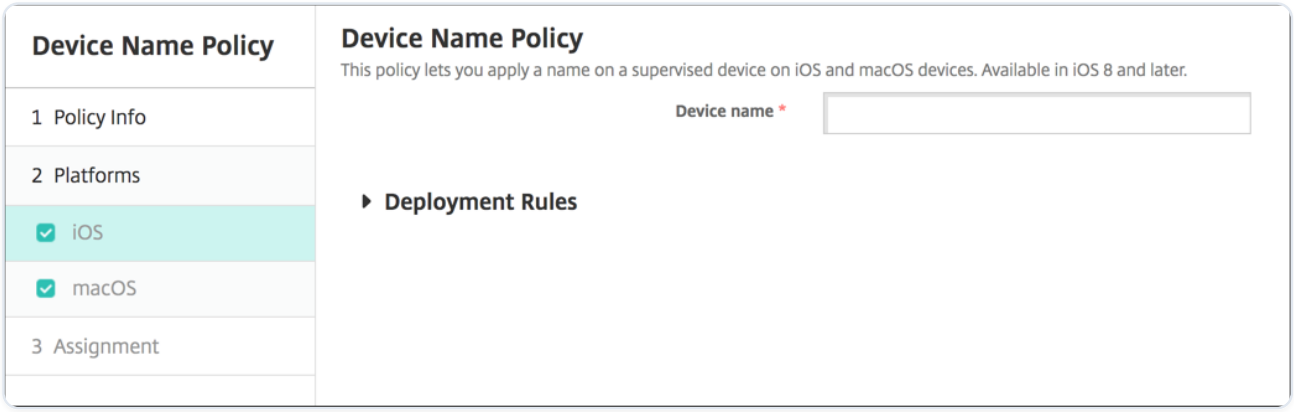
1. DHA 서버를 구성하려면 Windows Server 2016 Technical Preview 5 이상을 실행하는 컴퓨터에 DHA 서버 역할을 설치합니다. 지침은 온프레미스 장치 상태 증명 서버 구성을 참조하십시오.
2. 장치 상태 증명 정책을 추가하고 다음 설정을 구성합니다.
    - **장치 상태 증명 사용: 켜기**로 설정합니다.
    - **온프레미스 상태 증명 서비스 구성: 켜기**로 설정합니다.
    - **온프레미스 DHA 서비스 FQDN:** 설정한 DHA 서버의 정규화된 도메인 이름을 입력합니다.
    - **온프레미스 DHA API 버전:** DHA 서버에 설치된 DHA 서비스 버전을 선택합니다.

장치 이름 장치 정책

감독되는 iOS 및 macOS 장치에 이름을 설정하여 장치를 쉽게 식별할 수 있습니다. 매크로, 텍스트 또는 이 둘의 조합을 사용하여 장치 이름을 정의할 수 있습니다. 예를 들어, 장치 이름을 장치의 일련 번호로 설정하려면 ${device.serialnumber}를 사용해야 합니다. 장치 이름을 사용자 이름과 도메인의 조합으로 설정하려면 ${user.username}@example.com을 사용해야 합니다. 매크로에 대한 자세한 내용은 XenMobile의 매크로를 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 및 macOS 설정



- **장치 이름:** 각 장치에 고유한 이름을 지정하려면 매크로, 매크로 조합 또는 매크로와 텍스트 조합을 입력합니다. 예를 들어, 각 장치의 일련 번호로 장치 이름을 설정하려면 ${device.serialnumber}를 사용하거나, 장치 이름에 사용자 이름을 포함하려면 ${device.serialnumber} ${ user.username }을 사용합니다.

교육 구성 장치 정책

교육 구성 장치 정책은 다음을 정의합니다.

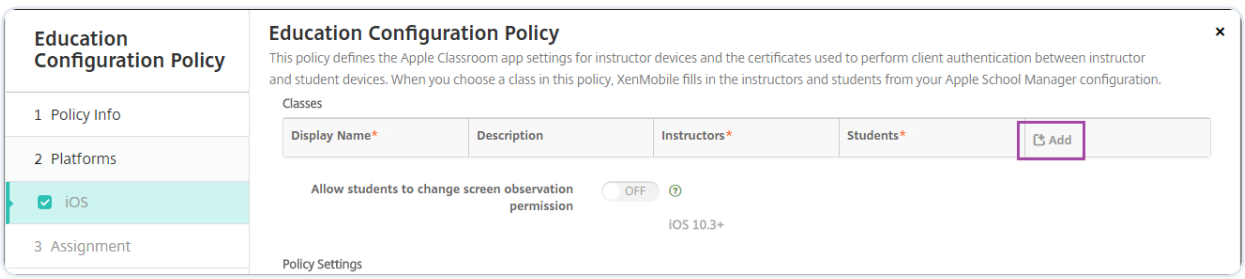
- 강사 장치용 Apple Classroom 앱 설정.
- 강사 장치와 학생 장치 간의 클라이언트 인증에 사용되는 인증서.

이 정책에서 수업을 선택하면 XenMobile® 콘솔이 Apple School Manager 구성에서 강사와 학생을 채웁니다. 이 정책의 Apple Classroom 앱 설정이 모든 수업에 대해 동일한 경우 하나의 정책을 생성합니다.

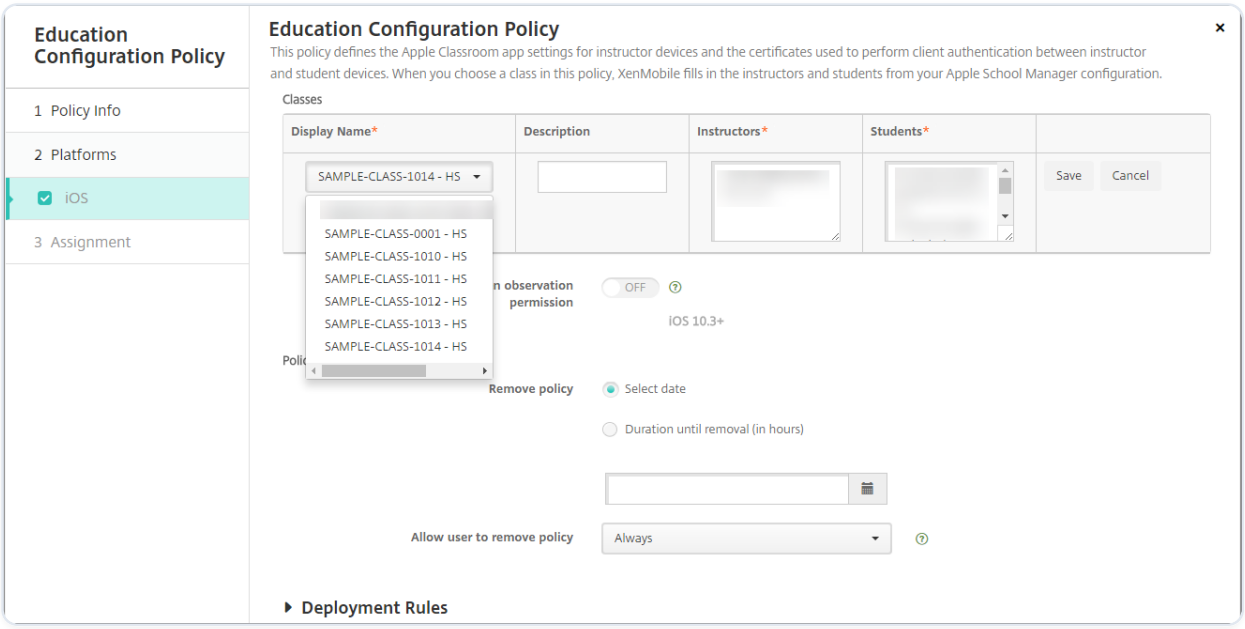
이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

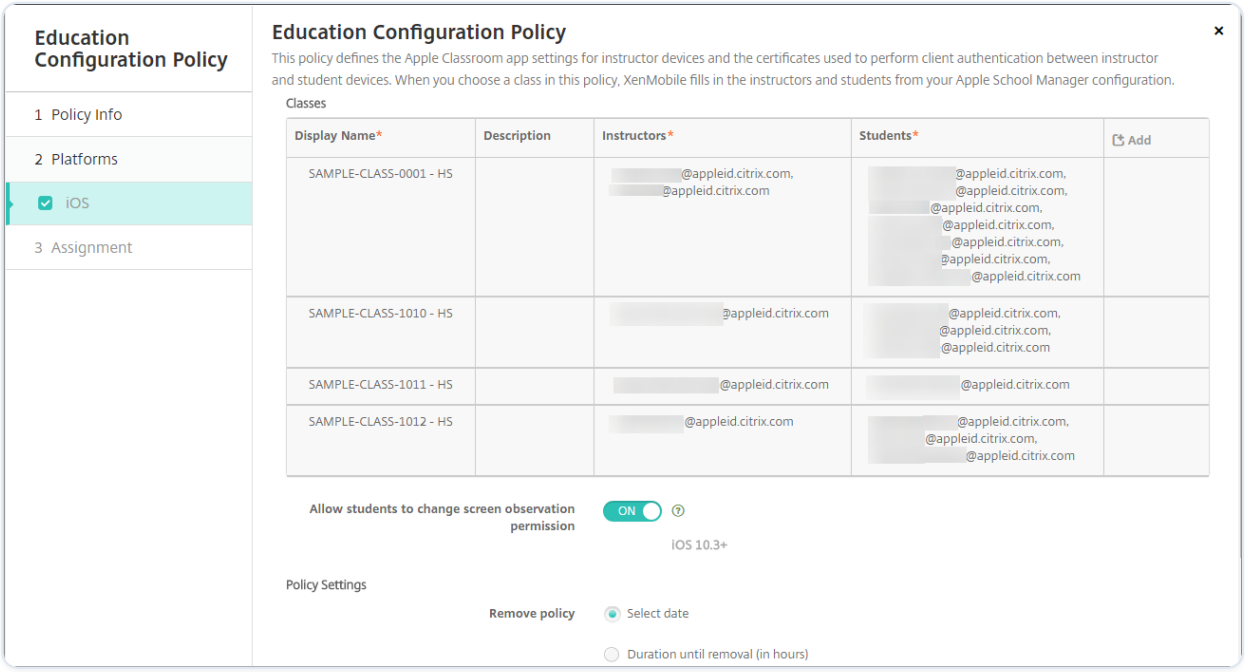
- **수업:** 수업을 추가하려면 **추가**를 클릭합니다.



그런 다음 **표시 이름** 목록을 클릭합니다. 연결된 Apple School Manager 계정에서 가져온 수업 목록이 나타납니다.



표시 이름에서 수업을 선택하면 XenMobile이 강사와 학생을 채웁니다. 계속해서 수업을 추가합니다.

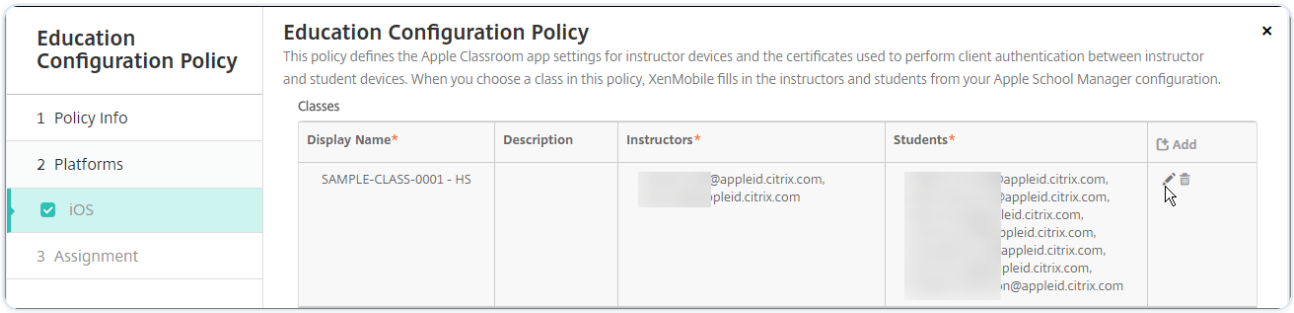


- **학생이 화면 관찰 권한을 변경하도록 허용: 켜짐**으로 설정하면 관리되는 수업에 등록된 학생은 교사가 자신의 장치 화면을 관찰하도록 허용할지 여부를 선택할 수 있습니다. 기본값은 **꺼짐**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.

정책에서 클래스 정보를 편집하려면

클래스에 설명을 추가할 수 있습니다(Classroom 앱의 "표시 이름"). 강사와 학생을 추가하거나 제거할 수도 있습니다. XenMobile은 이러한 변경 사항을 Apple School Manager 계정에 저장하지 않습니다. 자세한 내용은 Apple 교육 기능 통합에서 "강사, 학생 및 클래스 데이터 관리"를 참조하십시오.

편집하려는 클래스의 **추가** 열 위로 마우스를 가져간 다음 연필 아이콘을 클릭합니다.



정책에서 클래스를 삭제하려면 삭제하려는 클래스의 **추가** 열 위로 마우스를 가져간 다음 휴지통 아이콘을 클릭합니다.

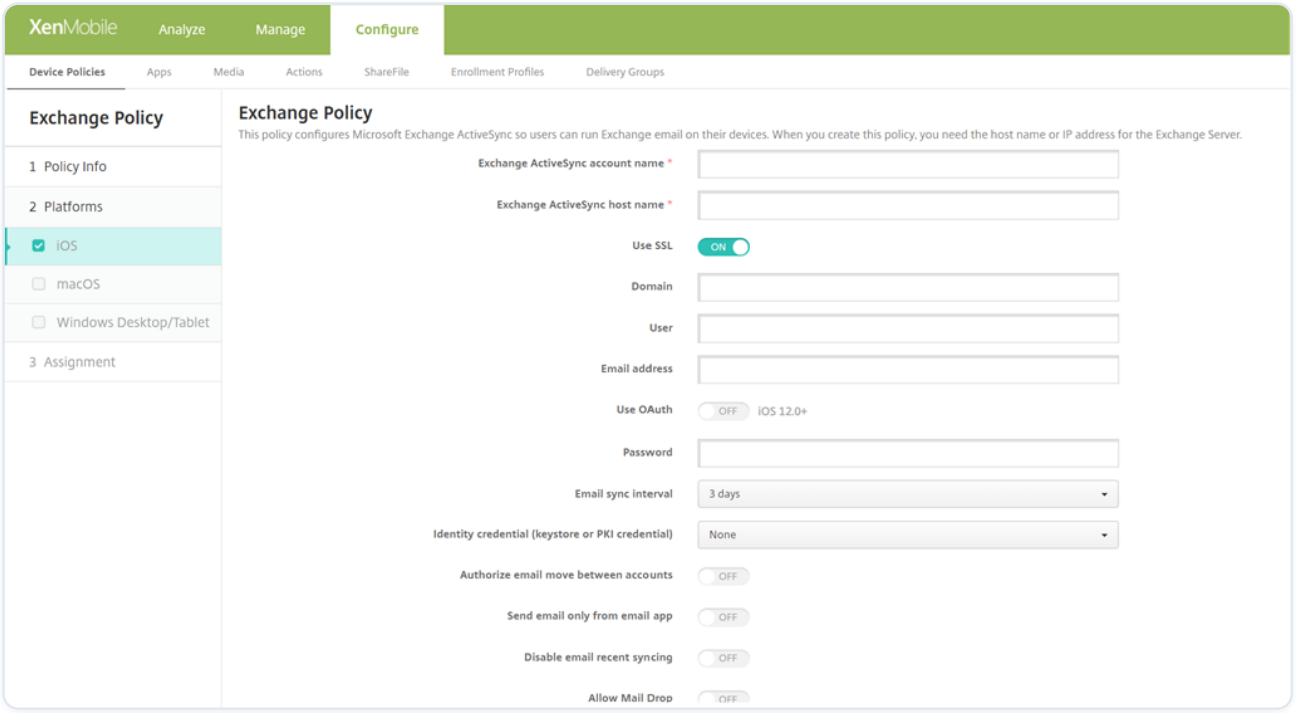
Exchange 장치 정책

Exchange ActiveSync 장치 정책을 사용하여 사용자 장치에서 이메일 클라이언트를 구성하여 Exchange에 호스팅된 회사 이메일에 액세스할 수 있도록 할 수 있습니다. iOS, macOS, Android Enterprise, Samsung SAFE, Samsung Knox 및 Windows Tablet용 정책을 생성할 수 있습니다. 각 플랫폼에는 다음 섹션에 자세히 설명된 대로 다른 값 집합이 필요합니다.

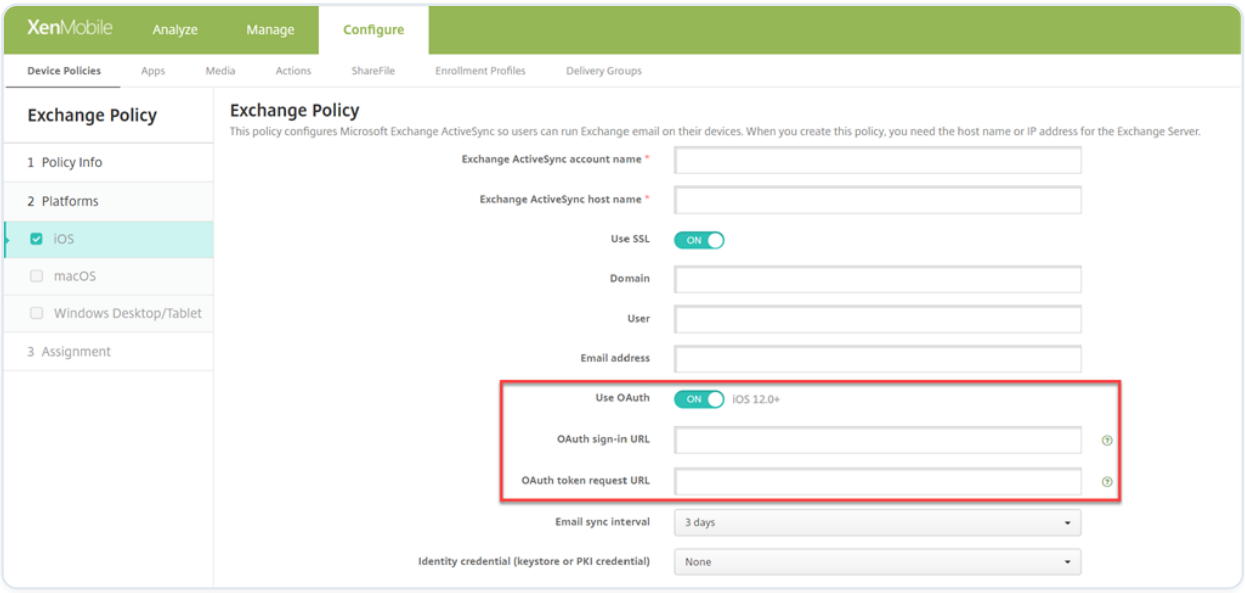
이 정책을 생성하려면 Exchange Server의 호스트 이름 또는 IP 주소가 필요합니다. ActiveSync 설정에 대한 자세한 내용은 Microsoft 문서 ActiveSync CSP를 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

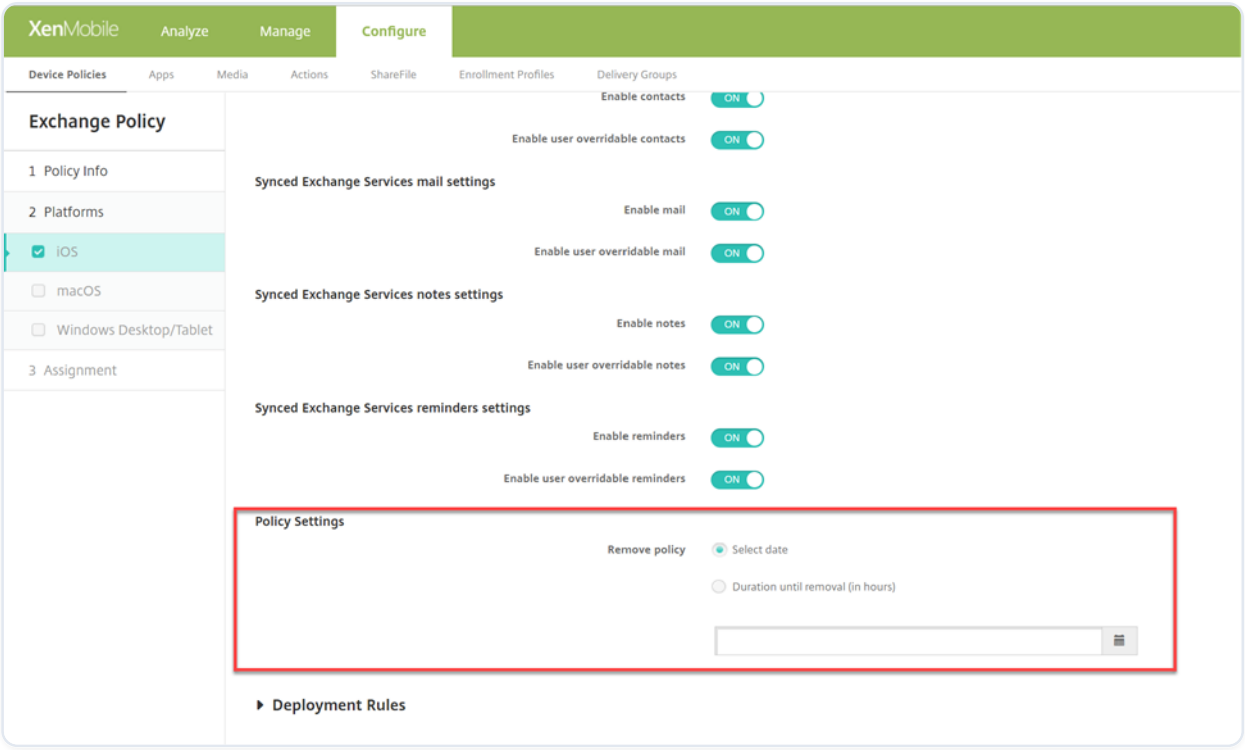


- **Exchange ActiveSync 계정 이름:** 사용자 장치에 표시되는 이메일 계정 설명을 입력합니다.
- **Exchange ActiveSync 호스트 이름:** 이메일 서버 주소를 입력합니다.
- **SSL 사용:** 사용자 장치와 Exchange Server 간의 연결을 보호할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
- **도메인:** Exchange Server가 있는 도메인을 입력합니다. 이 필드에서 시스템 매크로 $user.domainname을 사용하여 사용자 도메인 이름을 자동으로 조회할 수 있습니다.
- **사용자:** Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 시스템 매크로 $user.username을 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- **이메일 주소:** 전체 이메일 주소를 지정합니다. 이 필드에서 시스템 매크로 $user.mail을 사용하여 사용자 이메일 계정을 자동으로 조회할 수 있습니다.
- **OAuth 사용: 켜짐**으로 설정하면 연결은 인증을 위해 OAuth를 사용합니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
    - **OAuth 로그인 URL**: AutoDiscovery Service가 사용되지 않을 때 OAuth를 사용하여 인증하기 위해 웹뷰에 로드할 URL을 지정합니다. 이 필드는 **OAuth 사용**이 **켜짐**으로 설정된 경우에만 나타납니다.
    - **OAuth 토큰 요청 URL**: 계정이 OAuth 토큰 요청에 사용할 수 있는 URL을 지정합니다. 이 필드는 **OAuth 사용**이 **켜짐**으로 설정된 경우에만 나타납니다.

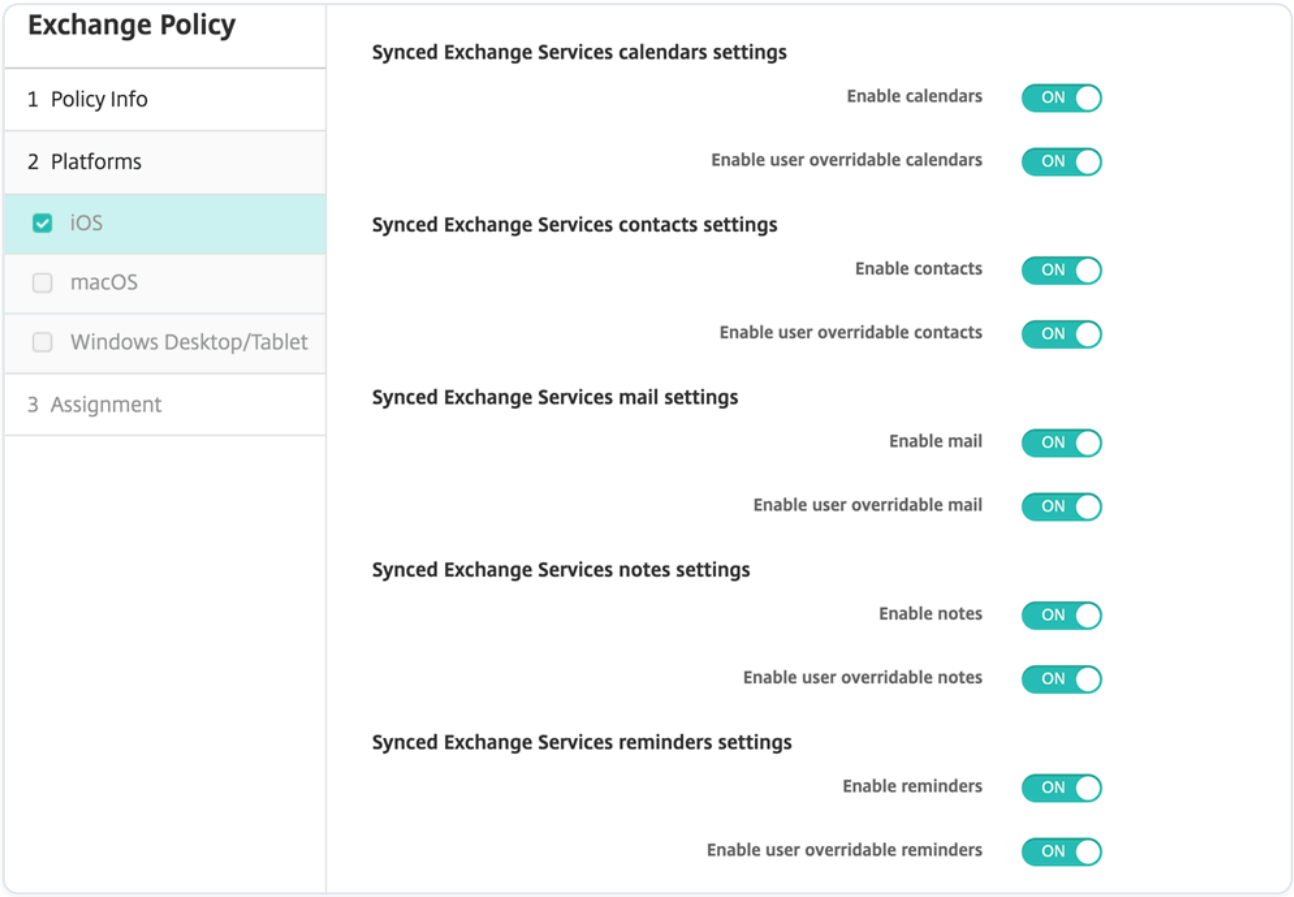


- **암호:** Exchange 사용자 계정에 대한 선택적 암호를 입력합니다. 이 설정은 **OAuth 사용**이 **켜짐**으로 설정된 경우에는 나타나지 않습니다.
- **이메일 동기화 간격:** 목록에서 Exchange Server와 이메일을 동기화하는 빈도를 선택합니다. 기본값은 **3일**입니다.
- **ID 자격 증명(키 저장소 또는 PKI):** XenMobile용 ID 공급자를 구성한 경우 드롭다운 목록에서 선택적 ID 자격 증명을 클릭합니다. 이 필드는 Exchange에서 클라이언트 인증서 인증을 요구하는 경우에만 필요합니다. 기본값은 **없음**입니다.
- **계정 간 이메일 이동 허용:** 사용자가 이 계정에서 다른 계정으로 이메일을 이동하고 다른 계정에서 전달 및 회신할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **이메일 앱에서만 이메일 보내기:** 사용자가 이메일을 보낼 때 iOS 메일 앱으로 제한할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **최근 이메일 동기화 비활성화:** 사용자가 최근 주소를 동기화하지 못하도록 할지 여부를 선택합니다. 기본값은 **끔**입니다. 이 옵션은 iOS 6.0 이상에만 적용됩니다.
- **Mail Drop 허용:** 계정에서 Mail Drop을 사용할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **S/MIME 서명 사용:** 이 계정에서 S/MIME 서명을 지원할지 여부를 선택합니다. 기본값은 **켜짐**입니다. **켜짐**으로 설정하면 다음 필드가 나타납니다.
  - **서명 ID 자격 증명:** 사용할 서명 자격 증명을 선택합니다.
  - **S/MIME 서명 사용자 재정의 가능: 켜짐**으로 설정하면 사용자가 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 **끔**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
  - **S/MIME 서명 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자가 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 **끔**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

- **S/MIME 암호화 사용:** 이 계정에서 S/MIME 암호화를 지원할지 여부를 선택합니다. 기본값은 **끔**입니다. **켜짐**으로 설정하면 다음 필드가 나타납니다.
  - **암호화 ID 자격 증명:** 사용할 암호화 자격 증명을 선택합니다.
  - **메시지별 S/MIME 스위치 사용: 켜짐**으로 설정하면 사용자가 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션을 표시합니다. 기본값은 **끔**입니다.
  - **S/MIME 기본 암호화 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME를 기본적으로 켤지 여부를 선택할 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
  - **S/MIME 암호화 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
- **정책 설정**
  - **정책 제거:** 정책 제거를 예약할 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간(단위: 시간)을 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.



동기화된 Exchange 서비스



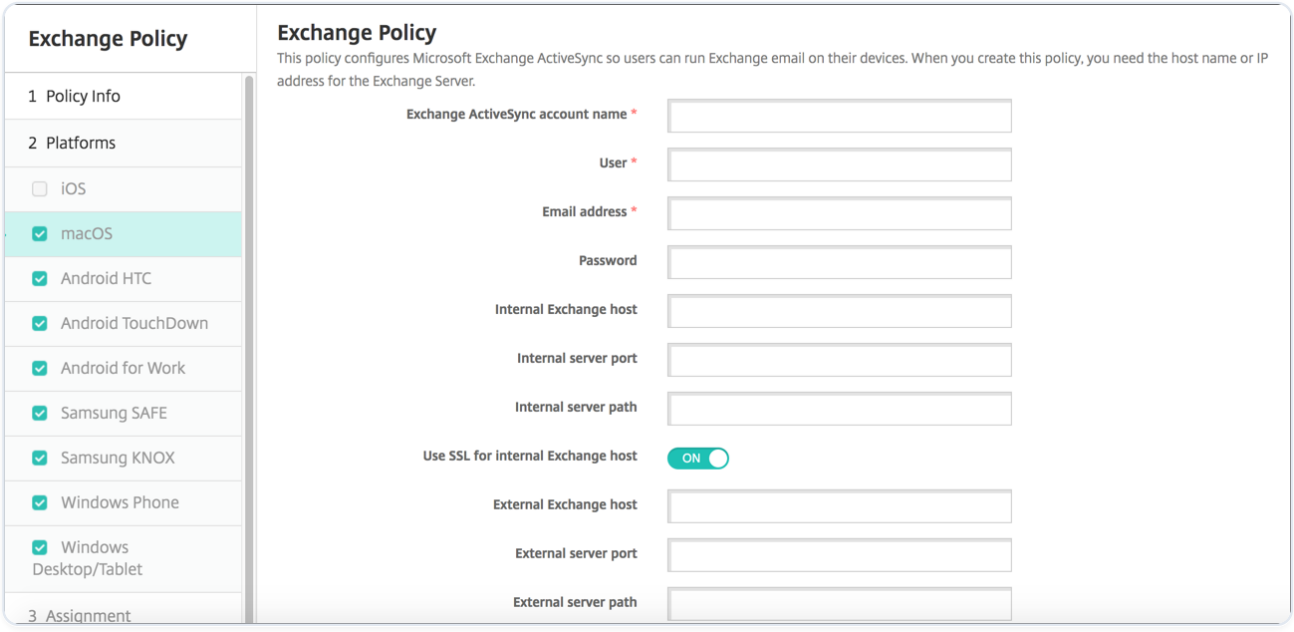
- **동기화된 Exchange 서비스 캘린더 설정**
  - **캘린더 사용**: 계정에 대한 *캘린더* 서비스를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본값은 **켜짐**입니다. **꺼짐**으로 설정하면 계정에 대한 *캘린더* 서비스가 비활성화됩니다. *캘린더* 서비스는 **사용자 재정의 가능 캘린더 사용** 버튼이 **켜짐**으로 설정된 경우에만 설정에서 다시 활성화할 수 있습니다.
  - **사용자 재정의 가능 캘린더 사용**: 설정에서 계정에 대한 *캘린더* 서비스 상태를 변경할 수 있습니다. 기본값은 **켜짐**입니다. **꺼짐**으로 설정하면 *캘린더* 서비스 상태를 변경할 수 없습니다.
- **동기화된 Exchange 서비스 연락처 설정**
  - **연락처 사용**: 계정에 대한 *연락처* 서비스를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본값은 **켜짐**입니다. **꺼짐**으로 설정하면 계정에 대한 *연락처* 서비스가 비활성화됩니다. *연락처* 서비스는 **사용자 재정의 가능 연락처 사용** 버튼이 **켜짐**으로 설정된 경우에만 설정에서 다시 활성화할 수 있습니다.
  - **사용자 재정의 가능 연락처 사용**: 설정에서 계정에 대한 *연락처* 서비스 상태를 변경할 수 있습니다. 기본값은 **켜짐**입니다. **꺼짐**으로 설정하면 *캘린더* 서비스 상태를 변경할 수 없습니다.
- **동기화된 Exchange 서비스 메일 설정**

  - **메일 사용**: 계정에 대한 *메일* 서비스를 활성화하거나 비활성화할 수 있습니다. 기본값은 **ON**입니다. **OFF**로 설정하면 계정에 대한 *메일* 서비스가 비활성화됩니다. *메일* 서비스는 **사용자 재정의 가능 메일 사용** 버튼이 **ON**으로 설정된 경우에만 설정에서 다시 활성화할 수 있습니다.
  - **사용자 재정의 가능 메일 사용**: 설정에서 계정에 대한 *메일* 서비스의 상태를 변경할 수 있습니다. 기본값은 **ON**입니다. **OFF**로 설정하면 *메일* 서비스의 상태를 변경할 수 없습니다.

- **동기화된 Exchange 서비스 노트 설정**
  - **노트 사용**: 계정에 대한 *노트* 서비스를 활성화하거나 비활성화할 수 있습니다. 기본값은 **ON**입니다. **OFF**로 설정하면 계정에 대한 *노트* 서비스가 비활성화됩니다. *노트* 서비스는 **사용자 재정의 가능 노트 사용** 버튼이 **ON**으로 설정된 경우에만 설정에서 다시 활성화할 수 있습니다.
  - **사용자 재정의 가능 노트 사용**: 설정에서 계정에 대한 *노트* 서비스의 상태를 변경할 수 있습니다. 기본값은 **ON**입니다. **OFF**로 설정하면 *노트* 서비스의 상태를 변경할 수 없습니다.

- **동기화된 Exchange 서비스 미리 알림 설정**
  - **미리 알림 사용**: 계정에 대한 *미리 알림* 서비스를 활성화하거나 비활성화할 수 있습니다. 기본값은 **ON**입니다. **OFF**로 설정하면 계정에 대한 *미리 알림* 서비스가 비활성화됩니다. *미리 알림* 서비스는 **사용자 재정의 가능 미리 알림 사용** 버튼이 **ON**으로 설정된 경우에만 설정에서 다시 활성화할 수 있습니다.
  - **사용자 재정의 가능 미리 알림 사용**: 설정에서 계정에 대한 *미리 알림* 서비스의 상태를 변경할 수 있습니다. 기본값은 **ON**입니다. **OFF**로 설정하면 *미리 알림* 서비스의 상태를 변경할 수 없습니다.

macOS 설정



- **Exchange ActiveSync 계정 이름:** 사용자 장치에 표시되는 이메일 계정 설명을 입력합니다.

- **사용자:** Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 시스템 매크로 $user.username을 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- **이메일 주소:** 전체 이메일 주소를 지정합니다. 이 필드에서 시스템 매크로 $user.mail을 사용하여 사용자 이메일 계정을 자동으로 조회할 수 있습니다.
- **OAuth 사용: On**으로 설정하면 연결에서 인증을 위해 OAuth를 사용합니다. 기본값은 **Off**입니다. 이 옵션은 macOS 10.14 이상에 적용됩니다.
- **OAuth 로그인 URL:** AutoDiscovery 서비스가 사용되지 않을 때 OAuth를 사용하여 인증하기 위해 웹 뷰에 로드할 URL을 지정합니다. 이 필드는 **OAuth 사용**이 **켜짐**으로 설정된 경우에 나타납니다.
- **암호:** Exchange 사용자 계정에 대한 선택적 암호를 입력합니다. 이 설정은 **OAuth 사용**이 **켜짐**으로 설정된 경우에는 나타나지 않습니다.
- **내부 Exchange 호스트:** 내부 및 외부 Exchange 호스트 이름이 서로 다르게 지정되도록 하려면 선택적 내부 Exchange 호스트 이름을 입력합니다.
- **내부 서버 포트:** 내부 및 외부 Exchange 서버 포트가 서로 다르게 지정되도록 하려면 선택적 내부 Exchange 서버 포트 번호를 입력합니다.
- **내부 서버 경로:** 내부 및 외부 Exchange 서버 경로가 서로 다르게 지정되도록 하려면 선택적 내부 Exchange 서버 경로를 입력합니다.
- **내부 Exchange 호스트에 SSL 사용:** 사용자 장치와 내부 Exchange 호스트 간의 연결을 보호할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
- **외부 Exchange 호스트:** 내부 및 외부 Exchange 호스트 이름이 서로 다르게 지정되도록 하려면 선택적 외부 Exchange 호스트 이름을 입력합니다.
- **외부 서버 포트:** 내부 및 외부 Exchange 서버 포트가 서로 다르게 지정되도록 하려면 선택적 외부 Exchange 서버 포트 번호를 입력합니다.
- **외부 서버 경로:** 내부 및 외부 Exchange 서버 경로가 서로 다르게 지정되도록 하려면 선택적 외부 Exchange 서버 경로를 입력합니다.
- **외부 Exchange 호스트에 SSL 사용:** 사용자 장치와 내부 Exchange 호스트 간의 연결을 보호할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
- **Mail Drop 허용:** 사용자가 기존 네트워크에 연결하지 않고 두 Mac 간에 무선으로 파일을 공유할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **꺼짐**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거를 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.

    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.
- **정책 제거 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요**, 또는 **안 함**을 선택합니다. **암호 필요**를 선택한 경우, **제거 암호** 필드에 암호를 입력합니다.
- **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 아니면 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Windows 데스크톱/태블릿 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policy-exchange-windowsdesktop.png)

> **참고:**
>
> 이 정책으로는 사용자 암호를 설정할 수 없습니다. 정책을 푸시한 후 사용자가 자신의 장치에서 해당 매개변수를 설정해야 합니다.

- **계정 이름 또는 표시 이름:** Exchange ActiveSync 계정 이름을 입력합니다.
- **서버 이름 또는 IP 주소:** Exchange Server 호스트 이름 또는 IP 주소를 입력합니다.
- **도메인:** Exchange Server가 있는 도메인을 입력합니다. 이 필드에서 시스템 매크로 $user.domainname을 사용하여 사용자 도메인 이름을 자동으로 조회할 수 있습니다.
- **사용자 ID 또는 사용자 이름:** Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 시스템 매크로 $user.username을 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- **이메일 주소:** 전체 이메일 주소를 지정합니다. 이 필드에서 시스템 매크로 $user.mail을 사용하여 사용자 이메일 계정을 자동으로 조회할 수 있습니다.
- **SSL 연결 사용:** 사용자 장치와 Exchange Server 간의 연결을 보호할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **동기화할 지난 일수:** 목록에서 장치의 모든 콘텐츠를 Exchange Server와 동기화할 지난 일수를 클릭합니다. 기본값은 **모든 콘텐츠**입니다.
- **빈도:** 목록에서 Exchange Server에서 장치로 전송되는 데이터를 동기화할 때 사용할 일정을 클릭합니다. 기본값은 **도착 시**입니다.
- **로깅 수준:** 드롭다운 목록에서 **사용 안 함**, **기본**, 또는 **고급**을 클릭하여 Exchange 활동 로깅 시 세부 정보 수준을 지정합니다. **기본값은 사용 안 함**입니다.

파일 장치 정책

사용자가 Android 및 Android Enterprise 장치에서 액세스할 수 있도록 파일을 추가하고 배포할 수 있습니다. 장치에 파일을 저장할 디렉터리를 지정합니다. 예를 들어, 사용자가 회사 문서 또는 .pdf 파일을 받도록 하려면 파일을 장치에 배포하고 사용자에게 파일 위치를 알려줍니다.

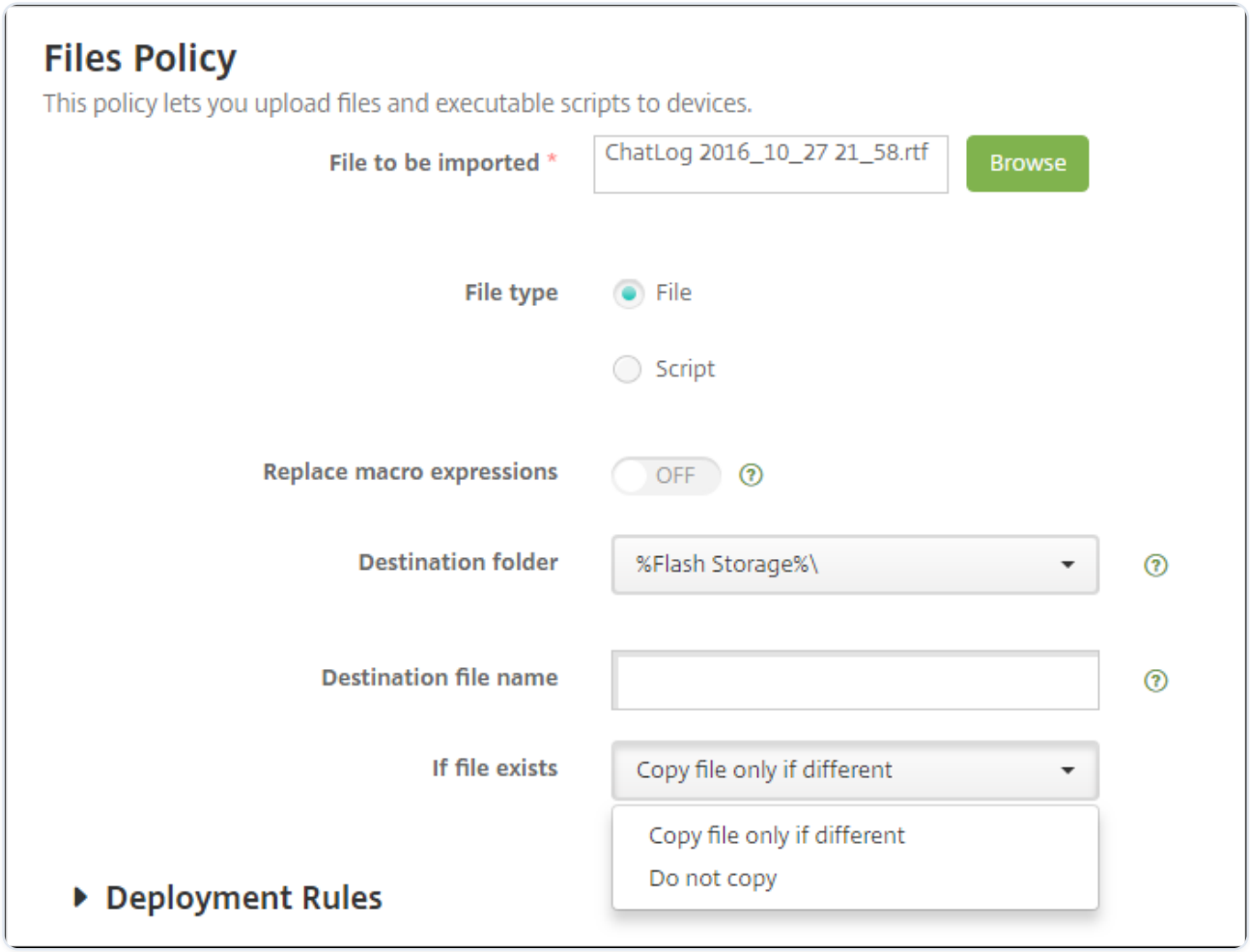
Android 장치는 스크립트를 기본적으로 실행하는 것을 지원하지 않습니다. 사용자는 스크립트를 실행하려면 타사 소프트웨어가 필요합니다.

이 정책으로 다음 파일 형식을 추가할 수 있습니다.

- 텍스트 기반 파일(.xml, .html, .py 등)
- 문서, 사진, 스프레드시트 또는 프레젠테이션과 같은 기타 파일

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

안드로이드 엔터프라이즈 설정



- **가져올 파일:** 가져올 파일을 선택하려면 **찾아보기**를 클릭하고 파일 위치로 이동합니다.

- **파일 형식: 파일**을 선택합니다.
- **대상 폴더:** 목록에서 업로드된 파일을 저장할 위치를 선택하거나 **새로 추가**를 클릭하여 목록에 없는 파일 위치를 선택합니다. %XenMobile Folder%\ 또는 %Flash Storage%\ 매크로를 모든 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 **다른 경우에만 파일 복사**입니다.

Android 설정

- **가져올 파일: 찾아보기**를 클릭하고 파일 위치로 이동하여 가져올 파일을 선택합니다.
- **파일 유형: 파일**을 선택합니다.
- **대상 폴더:** 목록에서 업로드된 파일을 저장할 위치를 선택하거나 **새로 추가**를 클릭하여 목록에 없는 파일 위치를 선택합니다. 또한, %XenMobile Folder%\\ 또는 %Flash Storage%\\ 매크로를 경로 식별자의 시작 부분으로 사용할 수 있습니다.
- **대상 파일 이름:** 선택 사항으로, 장치에 배포하기 전에 파일 이름을 변경해야 하는 경우 다른 이름을 입력합니다.
- **다른 경우에만 파일 복사:** 목록에서 기존 파일과 다른 경우 파일을 복사할지 여부를 선택합니다. 기본값은 다른 경우에만 파일을 복사하는 것입니다.

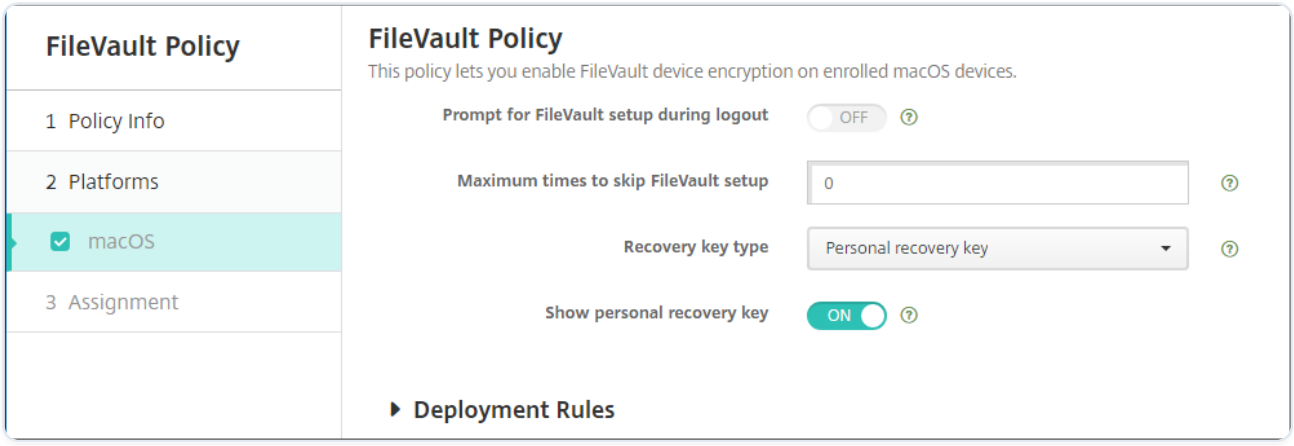
FileVault 장치 정책

macOS FileVault 디스크 암호화 기능은 시스템 볼륨의 내용을 암호화하여 보호합니다. macOS 장치에서 FileVault가 활성화되면 사용자는 장치가 시작될 때마다 계정 암호로 로그인합니다. 사용자가 암호를 잊어버린 경우 복구 키를 사용하여 디스크 잠금을 해제하고 암호를 재설정할 수 있습니다.

XenMobile 장치 정책인 FileVault는 FileVault 사용자 설정 화면을 활성화하고 복구 키와 같은 설정을 구성합니다. FileVault에 대한 자세한 내용은 Apple 지원 사이트 `<https://support.apple.com>`를 참조하십시오.

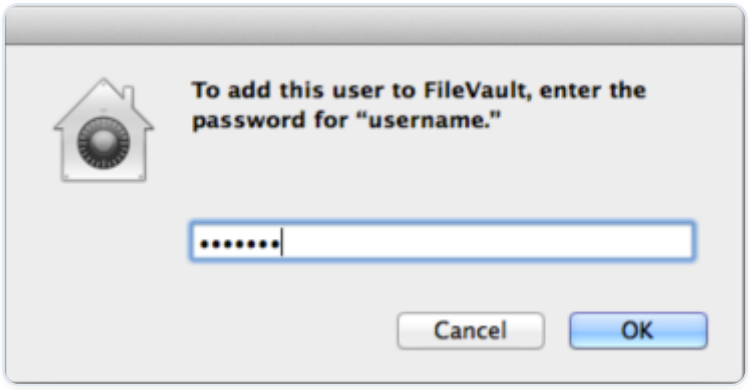
FileVault 정책을 추가하려면 **구성 > 장치 정책**으로 이동합니다.

macOS 설정

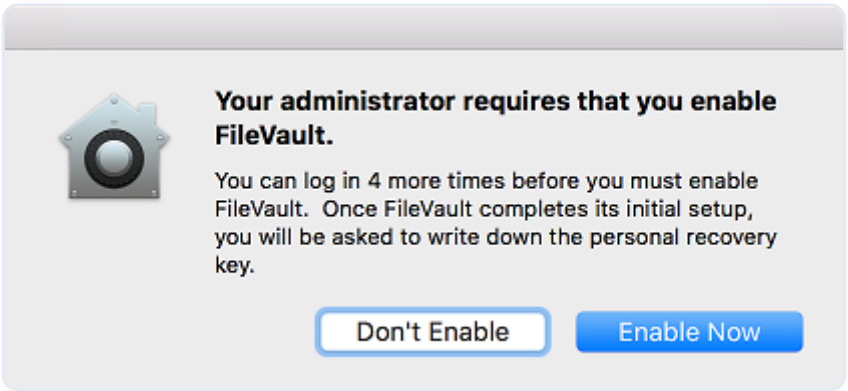


- **로그아웃 시 FileVault 설정 프롬프트 표시: 켜짐**으로 설정하면 **FileVault 설정을 건너뛸 최대 횟수** 옵션에 지정된 대로 다음 N회 로그아웃 시 사용자에게 FileVault를 활성화하도록 프롬프트가 표시됩니다. **꺼짐**으로 설정하면 FileVault 암호 프롬프트가 나타나지 않습니다.

이 설정을 켠 상태로 FileVault 정책을 배포하면 사용자가 장치에서 로그오프할 때 다음 화면이 나타납니다. 이 화면은 사용자에게 로그오프하기 전에 FileVault를 활성화할 수 있는 옵션을 제공합니다.



FileVault 설정을 건너뛸 최대 횟수 값이 0이 아닌 경우: 이 설정을 끈 상태로 FileVault 정책을 배포한 후 사용자가 로그인하면 다음 화면이 나타납니다.



FileVault 설정을 건너뛸 최대 횟수 값이 0이거나 사용자가 최대 횟수만큼 설정을 건너뛴 경우 다음 화면이 나타납니다.



글꼴 장치 정책

XenMobile®에서 iOS 및 macOS 장치에 더 많은 글꼴을 추가하기 위한 장치 정책을 추가할 수 있습니다. 글꼴은 TrueType (`.ttf`) 또는 OpenType (`.oft`) 글꼴이어야 합니다. 글꼴 모음 (`.ttc` 또는 `.otc`) 은 지원되지 않습니다.

iOS의 경우 이 정책은 iOS 7.0 이상에만 적용됩니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **사용자에게 표시되는 이름:** 사용자가 글꼴 목록에서 볼 이름을 입력합니다.
- **글꼴 파일: 찾아보기**를 클릭한 다음 파일 위치로 이동하여 사용자의 장치에 추가할 글꼴 파일을 선택합니다.
- **정책 설정**
    - **정책 제거:** 정책 제거를 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
        - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.

    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- **사용자에게 표시되는 이름:** 사용자가 글꼴 목록에서 볼 이름을 입력합니다.
- **글꼴 파일: 찾아보기**를 클릭한 다음 파일 위치로 이동하여 사용자의 장치에 추가할 글꼴 파일을 선택합니다.
- **정책 설정**
    - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
        - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
        - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.
    - **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다. **암호 필요**를 선택한 경우, **제거 암호** 필드에 암호를 입력합니다.
    - **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 또는 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

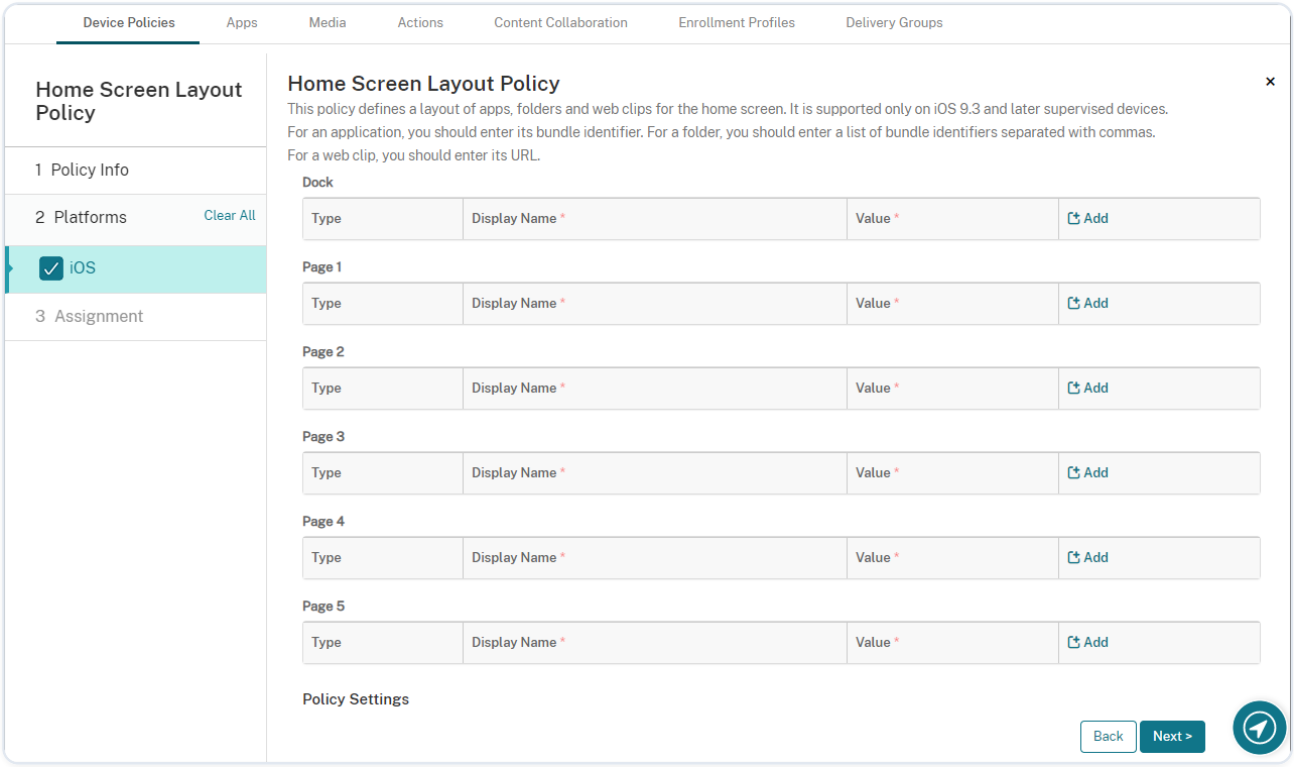
홈 화면 레이아웃 장치 정책

iOS 홈 화면의 앱 및 폴더 레이아웃을 지정할 수 있습니다. **홈 화면 레이아웃** 장치 정책은 iOS 9.3 이상 감독 모드 장치용입니다.

> **중요:**
>
> 여러 홈 화면 레이아웃 정책을 장치에 배포하면 장치에서 iOS 오류가 발생합니다. 이 제한은 이 XenMobile® 정책을 통해 홈 화면을 정의하든 Apple Configurator를 통해 정의하든 적용됩니다.

> 이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

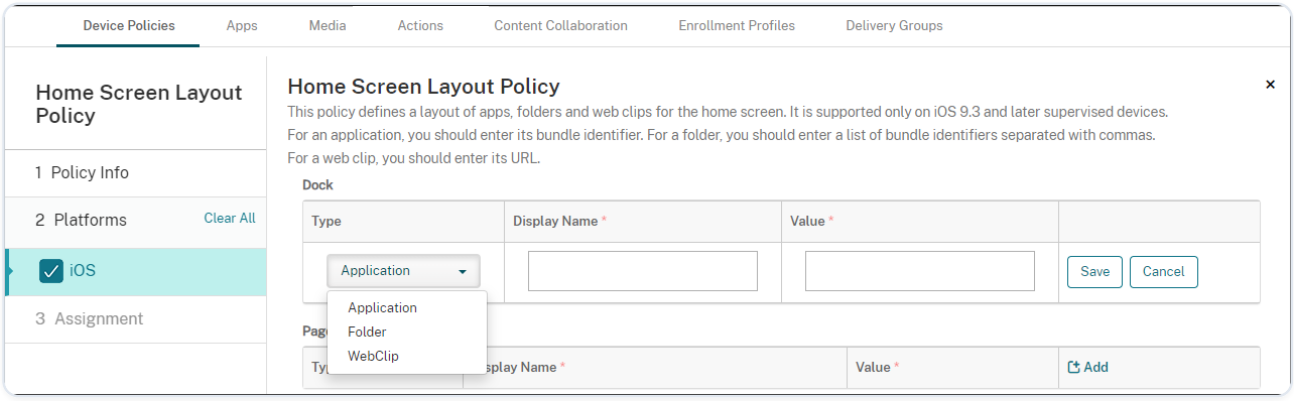
iOS 설정



- 구성하려는 각 화면 영역(예: **Dock** 또는 **Page 1**)에 대해 **추가**를 클릭합니다.
- **유형: 애플리케이션**, **폴더** 또는 **웹 클립** 중 하나를 선택합니다.

  제한 장치 정책의 **제한된 앱 사용 > 일부 앱만 허용** 설정은 웹 클립이 홈 화면에 제대로 표시되지 않도록 할 수 있습니다. 웹 클립이 제대로 표시되도록 하려면 다음 중 하나를 수행하십시오.

  - **제한된 앱 사용**을 **모든 앱 허용** 또는 **일부 앱 허용 안 함**으로 설정합니다.
  - **제한된 앱 사용**이 **일부 앱만 허용**으로 설정된 경우, 웹 클립을 허용하려면 번들 ID `com.apple.webapp`를 가진 앱을 추가합니다.



- **표시 이름:** 앱 또는 폴더의 홈 화면에 표시될 이름입니다.
- **값:** 앱의 경우 번들 식별자를 입력합니다. 폴더의 경우 쉼표로 구분된 번들 식별자 목록을 입력합니다. 웹 클립의 경우 번들 ID `com.apple.webClip.managed`를 입력하고 웹 클립 정책에서 웹 클립의 URL을

구성합니다. 동일한 URL을 가진 웹 클립 값이 두 개 이상 존재하는 경우, iOS 11.3 이상 장치에서는 동작이 정의되지 않습니다.

- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.
  - **프로필 범위:** 이 정책을 **사용자**에게 적용할지 아니면 전체 **시스템**에 적용할지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 iOS 9.3 이상에서만 사용할 수 있습니다.

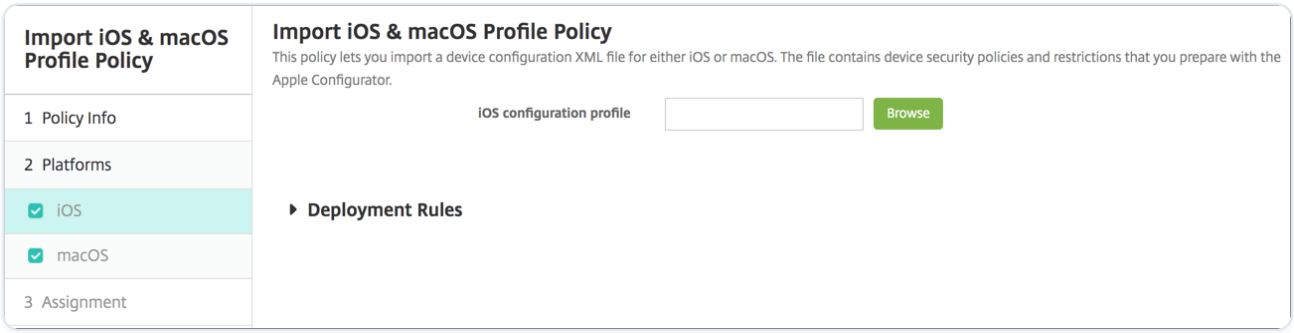
iOS 및 macOS 프로필 장치 정책 가져오기

iOS 및 macOS 장치용 장치 구성 XML 파일을 XenMobile로 가져올 수 있습니다. 이 파일에는 Apple Configurator로 준비한 장치 보안 정책 및 제한 사항이 포함되어 있습니다.

이 문서의 뒷부분에 설명된 대로 Apple Configurator를 사용하여 iOS 장치를 감독 모드에 둘 수 있습니다. 구성 파일을 만드는 데 Apple Configurator를 사용하는 방법에 대한 자세한 내용은 Apple Configurator 지원을 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 및 macOS 설정



- **iOS 구성 프로필** 또는 **macOS 구성 프로필:** 가져올 구성 파일을 선택하려면 **찾아보기**를 클릭하고 파일 위치로 이동합니다.

Apple Configurator를 사용하여 iOS 장치를 감독 모드에 두기

Apple Configurator를 사용하려면 macOS 10.7.2 이상을 실행하는 Apple 컴퓨터가 필요합니다.

중요:

장치를 감독 모드에 두면 선택한 iOS 버전이 장치에 설치되고, 이전에 저장된 모든 사용자 데이터 또는 앱이 장치에서 완전히 지워집니다.

1. iTunes에서 Apple Configurator를 설치합니다.
2. iOS 장치를 Apple 컴퓨터에 연결합니다.
3. Apple Configurator를 시작합니다. Configurator는 감독을 위해 준비할 장치가 있음을 보여줍니다.
4. 감독을 위해 장치를 준비하려면:
    a. **감독** 제어를 **켜기**로 전환합니다. Citrix®는 구성을 정기적으로 다시 적용하여 장치를 지속적으로 제어할 의향이 있는 경우 이 설정을 선택할 것을 권장합니다.
    b. 선택적으로 장치 이름을 제공합니다.
    c. iOS에서 설치하려는 최신 iOS 버전에 대해 **최신**을 클릭합니다.
5. 장치를 감독할 준비가 되면 **준비**를 클릭합니다.

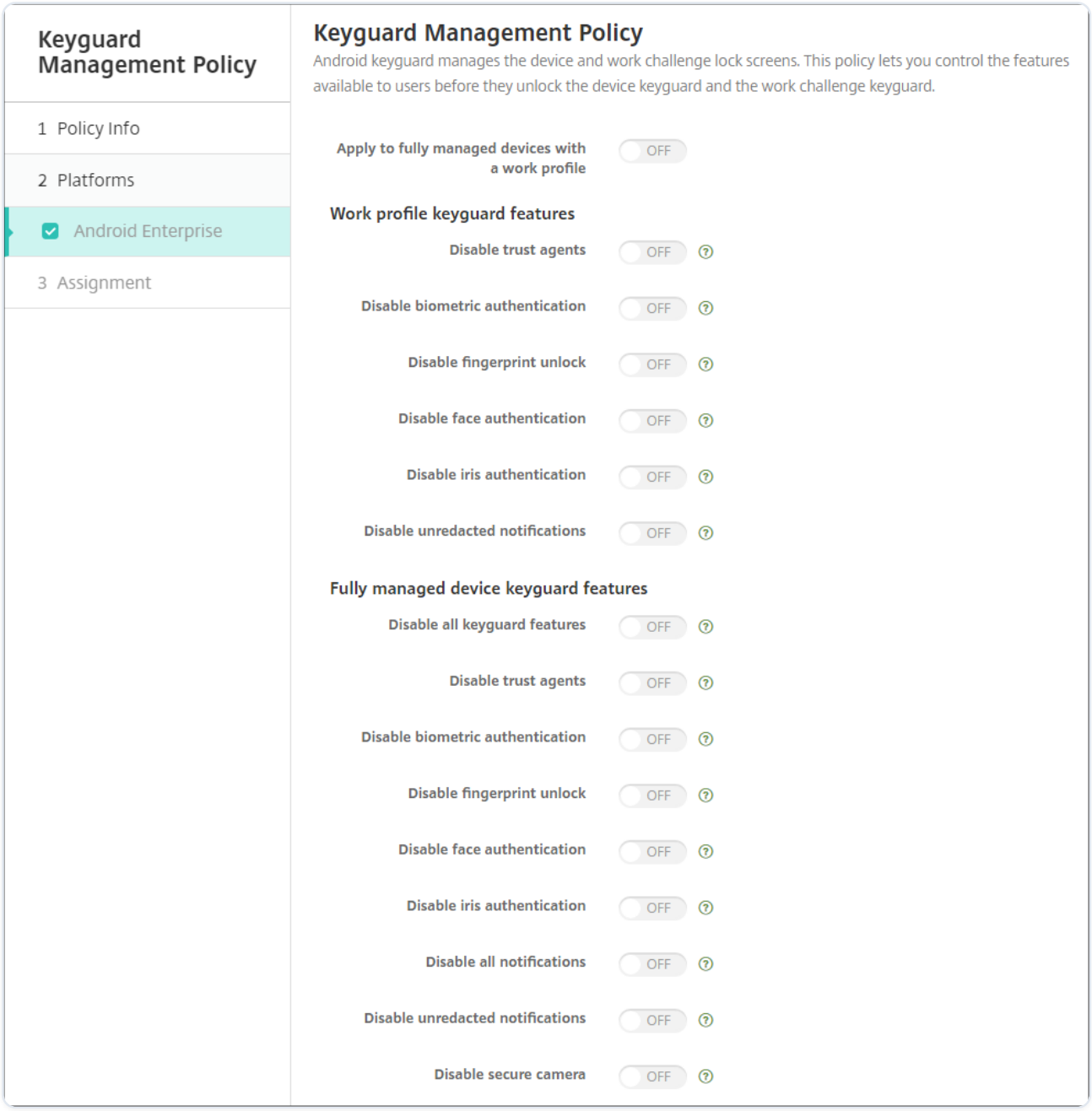
키가드 관리 장치 정책

Android 키가드는 장치 및 작업 챌린지 잠금 화면을 관리합니다. 이 정책을 통해 Android Enterprise 작업 프로필 키가드 및 고급 장치 키가드에 대한 기능을 관리할 수 있습니다. 다음을 제어할 수 있습니다.

- 작업 프로필 장치에서 키가드 관리. 사용자가 장치 키가드 및 작업 챌린지 키가드를 잠금 해제하기 전에 사용할 수 있는 기능을 지정할 수 있습니다. 예를 들어, 기본적으로 사용자는 지문 잠금 해제를 사용하고 잠금 화면에서 수정되지 않은 알림을 볼 수 있습니다.
- 완전 관리형 및 전용 장치에서 키가드 관리. 키가드 화면을 잠금 해제하기 전에 신뢰 에이전트 및 보안 카메라와 같은 사용 가능한 기능을 지정할 수 있습니다. 또는 모든 키가드 기능을 비활성화하도록 선택할 수 있습니다.
- 작업 프로필이 있는 완전 관리형 장치에서 키가드 관리. 하나의 키가드 관리 정책을 사용하여 장치와 작업 프로필에 별도의 설정을 적용할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

안드로이드 엔터프라이즈 설정



- **작업 프로필이 있는 완전 관리형 장치에 적용:** 작업 프로필이 있는 완전 관리형 장치에 대한 키가드 관리 장치 정책 설정을 구성할 수 있습니다.

  이 설정이 **켜짐**으로 설정된 경우, 작업 프로필이 있는 완전 관리형 장치에서 장치와 작업 프로필에 별도의 설정을 적용할 수 있습니다.

  이 설정이 **꺼짐**으로 설정된 경우, 작업 프로필 장치 또는 완전 관리형 장치에 설정을 적용할 수 있습니다. 작업 프로필에 대해 구성하는 설정은 작업 프로필 장치에만 적용됩니다. 완전 관리형 장치에 대해 구성하는 설정은 완전 관리형 장치에만 적용됩니다.

  기본값은 **꺼짐**입니다.

- **작업 프로필 키가드 기능:** 사용자가 작업 프로필 키가드(잠금 화면)를 잠금 해제하기 전에 다음 기능을 사용할 수 있는지 여부를 제어합니다.
  - **신뢰 에이전트 비활성화: 꺼짐**으로 설정된 경우, 작업 프로필에 챌린지가 설정되어 있을 때 신뢰 에이전트가 보안 키가드 화면에서 작동할 수 있습니다. 작업 프로필의 모든 신뢰 에이전트를 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
  - **생체 인증 비활성화: 꺼짐**으로 설정된 경우, 작업 프로필에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 생체 인증을 사용할 수 있습니다. 작업 프로필에서 생체 인증을 비활성화하려면 **켜짐**으로 설정합니다. 이 설정은 지문 잠금 해제, 얼굴 인증 및 홍채 인증을 비활성화합니다. 기본값은 **꺼짐**입니다. Android 9.0 이상에서 적용됩니다.
  - **지문 잠금 해제 비활성화: 켜짐**으로 설정된 경우, 작업 프로필에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 지문 잠금 해제를 사용할 수 없습니다. 작업 프로필에서 지문 잠금 해제를 사용하려면 **꺼짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
  - **얼굴 인증 비활성화: 꺼짐**으로 설정된 경우, 작업 프로필에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 얼굴 인증을 사용할 수 있습니다. 작업 프로필에서 얼굴 인증을 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다. Android 9.0 이상에서 사용 가능합니다.
  - **홍채 인증 비활성화: 꺼짐**으로 설정된 경우, 작업 프로필에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 홍채 인증을 사용할 수 있습니다. 작업 프로필에서 홍채 인증을 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다. Android 9.0 이상에서 사용 가능합니다.
  - **수정되지 않은 알림 비활성화: 꺼짐**으로 설정된 경우, 보안 키가드 화면에 수정된 알림과 수정되지 않은 알림이 모두 표시됩니다. 수정되지 않은 알림을 비활성화하고 수정된 알림만 표시하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
- **완전 관리형 장치 키가드 기능:** 사용자가 장치 키가드(잠금 화면)를 잠금 해제하기 전에 다음 기능을 사용할 수 있는지 여부를 제어합니다. 이 기능은 완전 관리형 또는 전용 장치에 적용됩니다.
  - **모든 키가드 기능 비활성화: 꺼짐**으로 설정된 경우, 현재 및 향후 모든 키가드 사용자 지정이 보안 키가드 화면에서 사용 가능합니다. 모든 키가드 사용자 지정을 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
  - **신뢰 에이전트 비활성화: 꺼짐**으로 설정된 경우, 신뢰 에이전트가 보안 키가드 화면에서 작동할 수 있습니다. 신뢰 에이전트를 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
  - **생체 인식 인증 비활성화: 꺼짐**으로 설정된 경우, 장치에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 생체 인식 인증을 사용할 수 있습니다. 장치에서 생체 인식 인증을 비활성화하려면 **켜짐**으로 설정합니다. 이렇게 하면 지문 잠금 해제, 얼굴 인증 및 홍채 인증이 비활성화됩니다. 기본값은 **꺼짐**입니다. Android 9.0 이상에서 사용 가능합니다.

- **지문 잠금 해제 비활성화: 꺼짐**으로 설정된 경우, 장치에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 지문 잠금 해제를 사용할 수 있습니다. 장치에서 지문 잠금 해제를 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
- **얼굴 인증 비활성화: 꺼짐**으로 설정된 경우, 장치에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 얼굴 인증을 사용할 수 있습니다. 장치에서 얼굴 인증을 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다. Android 9.0 이상에서 사용 가능합니다.
- **홍채 인증 비활성화: 꺼짐**으로 설정된 경우, 장치에 챌린지가 설정되어 있을 때 보안 키가드 화면에서 홍채 인증을 사용할 수 있습니다. 장치에서 홍채 인증을 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다. Android 9.0 이상에서 사용 가능합니다.
- **모든 알림 비활성화: 꺼짐**으로 설정된 경우, 보안 키가드 화면에 모든 알림이 표시됩니다. 모든 알림을 표시하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
- **수정되지 않은 알림 비활성화: 꺼짐**으로 설정된 경우, 보안 키가드 화면에 수정된 알림과 수정되지 않은 알림이 모두 표시됩니다. 수정되지 않은 알림을 비활성화하고 수정된 알림만 표시하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.
- **보안 카메라 비활성화: 꺼짐**으로 설정된 경우, 보안 키가드 화면에서 보안 카메라를 사용할 수 있습니다. 보안 카메라를 비활성화하려면 **켜짐**으로 설정합니다. 기본값은 **꺼짐**입니다.

키오스크 장치 정책

키오스크 정책을 사용하면 실행할 수 있는 앱을 제한하여 장치를 키오스크 모드로 제한할 수 있습니다. XenMobile®은 장치의 어떤 부분이 키오스크 모드에서 잠기는지 제어하지 않습니다. 정책을 배포한 후 장치에서 **키오스크 모드** 설정을 관리합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

키오스크 장치 정책을 추가하려면

키오스크 모드에 지정하는 모든 앱은 사용자 장치에 이미 설치되어 있어야 합니다.

일부 옵션은 Samsung MDM(모바일 장치 관리) API 4.0 이상에만 적용됩니다.

Android Enterprise 관련 설정

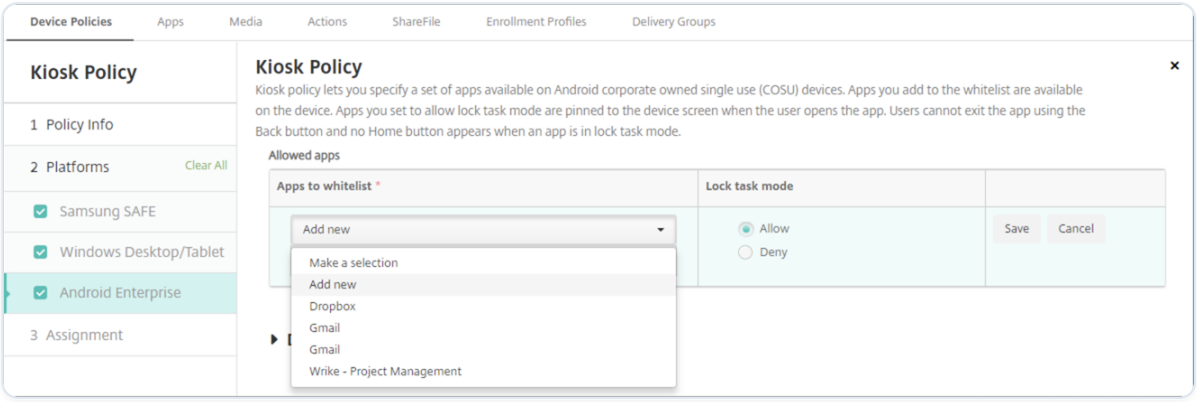
전용 Android Enterprise 장치(COSU(기업 소유 단일 사용) 장치라고도 함)에 대해 앱을 허용하고 잠금 작업 모드를 설정할 수 있습니다. 기본적으로 Secure Hub 및 Google Play 서비스는 허용 목록에 있습니다.

앱을 허용하려면 **추가**를 클릭합니다. 여러 앱을 허용할 수 있습니다. 자세한 내용은 Android Enterprise를 참조하십시오.

참고:

XenMobile Server 콘솔에는 "블랙리스트" 및 "화이트리스트"라는 용어가 포함되어 있습니다. 다음 릴리스에서는 이러한 용어를 "차단 목록" 및 "허용 목록"으로 변경할 예정입니다.

- **화이트리스트에 추가할 앱:** 화이트리스트에 추가할 앱의 패키지 이름을 입력하거나 목록에서 앱을 선택합니다.
  - **새로 추가**를 클릭하여 목록에 표시되도록 승인된 앱의 패키지 이름을 입력합니다.
  - 목록에서 기존 앱을 선택합니다. 이 목록에는 XenMobile Server에 업로드된 앱이 표시됩니다. 기본적으로 Secure Hub 및 Google Play 서비스는 화이트리스트에 추가됩니다.



- **잠금 작업 모드:** 사용자가 앱을 시작할 때 앱이 장치 화면에 고정되도록 설정하려면 **허용**을 선택합니다. 앱이 고정되지 않도록 설정하려면 **거부**를 선택합니다. 기본적으로 Secure Hub 및 Google Play 서비스는 허용됩니다. 기본값은 **허용**입니다.

앱이 잠금 작업 모드에 있을 때, 사용자가 앱을 열면 앱이 기기 화면에 고정됩니다. 홈 버튼이 나타나지 않으며 **뒤로** 버튼은 비활성화됩니다. 사용자는 로그아웃과 같이 앱에 프로그래밍된 작업을 사용하여 앱을 종료합니다.

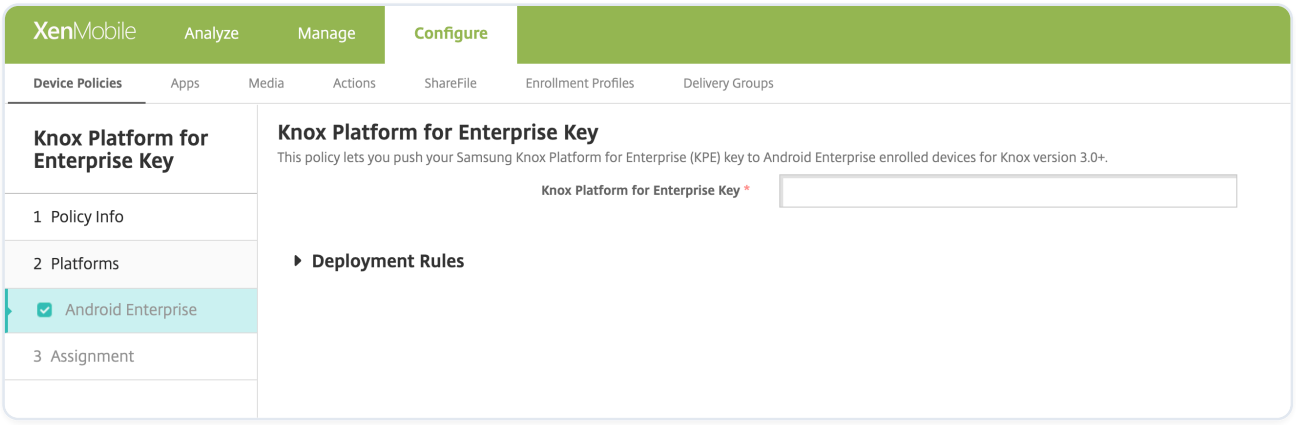
Knox Platform for Enterprise 키 장치 정책

이 정책을 통해 필요한 Samsung Knox Platform for Enterprise(KPE) 라이선스 정보를 제공할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성** > **장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

안드로이드 엔터프라이즈 설정

이 정책을 통해 Samsung Knox 버전 3.0 이상용 Android Enterprise 플랫폼에 등록된 장치에 Samsung Knox Platform for Enterprise(KPE) 라이선스 키를 푸시할 수 있습니다.



Knox Platform for Enterprise 키: Android Enterprise 장치에 푸시할 Samsung Knox Platform for Enterprise(KPE) 키를 입력합니다. Samsung Knox Platform for Enterprise(KPE) 키에서 KPE 라이선스 키를 신청하십시오.

런처 구성 장치 정책

Citrix Launcher를 사용하면 XenMobile에서 배포한 Android 장치의 사용자 환경을 사용자 지정할 수 있습니다. Citrix Launcher 및 런처 구성 장치 정책은 Android Enterprise와 호환되지 않습니다.

런처 구성 정책을 추가하여 다음 Citrix Launcher 기능을 제어할 수 있습니다.

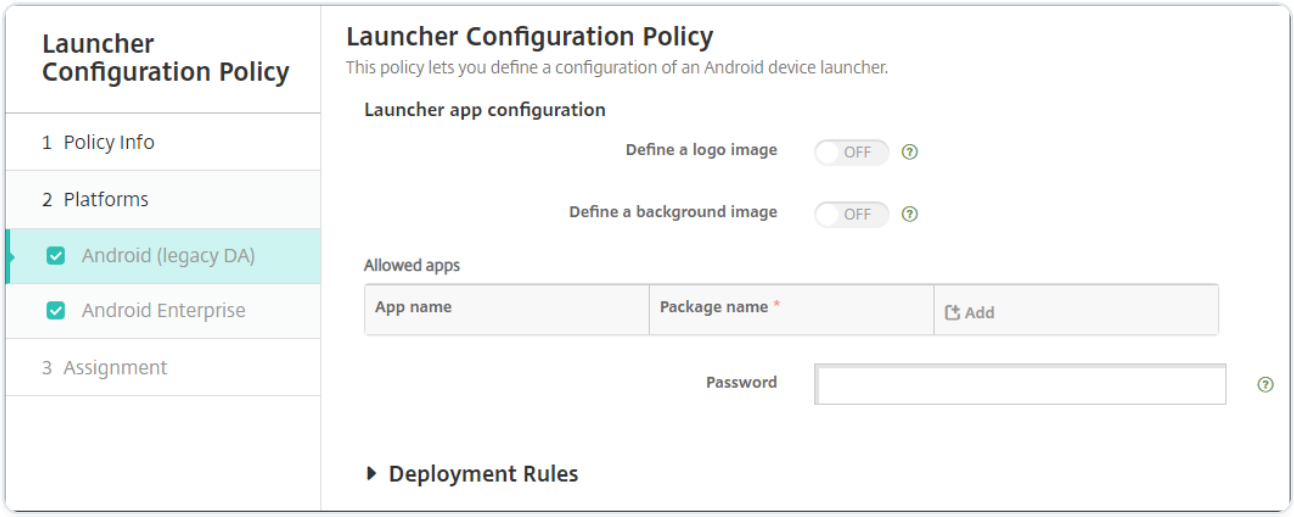
- 사용자가 지정한 앱에만 액세스할 수 있도록 Android 장치를 관리합니다.
- 선택적으로 Citrix Launcher 아이콘에 대한 사용자 지정 로고 이미지와 Citrix Launcher에 대한 사용자 지정 배경 이미지를 지정합니다.
- 사용자가 런처를 종료하기 위해 입력해야 하는 암호를 지정합니다.

Citrix Launcher를 통해 이러한 장치 수준 제한을 적용할 수 있지만, 런처는 Wi-Fi 설정, Bluetooth 설정 및 장치 암호 설정과 같은 장치 설정에 대한 기본 제공 액세스를 통해 사용자에게 필요한 운영 유연성을 제공합니다. Citrix Launcher는 장치 플랫폼이 이미 제공하는 보안 위에 추가 보안 계층으로 의도된 것이 아닙니다.

Citrix Launcher를 배포하면 XenMobile이 이를 설치하여 기본 Android 런처를 대체합니다.

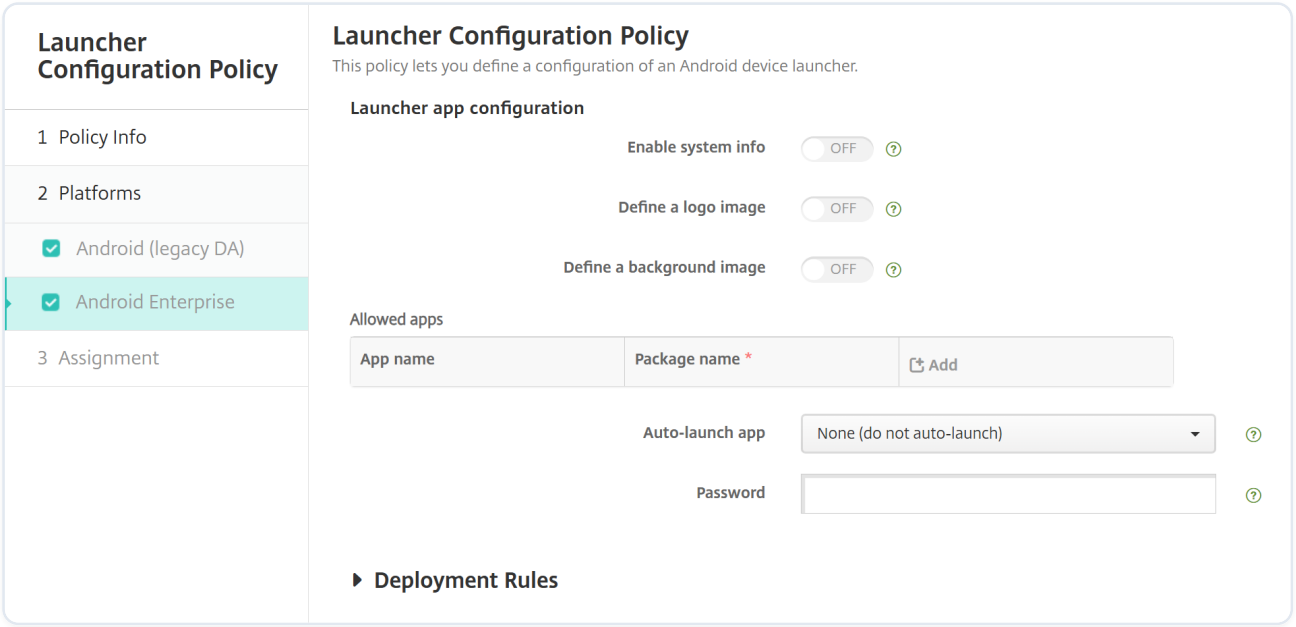
이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

Android 설정



- **로고 이미지 정의:** Citrix Launcher 아이콘에 사용자 지정 로고 이미지를 사용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **로고 이미지: 로고 이미지 정의**를 사용하도록 설정한 경우 **찾아보기**를 클릭하고 파일 위치로 이동하여 이미지 파일을 선택합니다. 지원되는 파일 형식은 PNG, JPG, JPEG 및 GIF입니다.
- **배경 이미지 정의:** Citrix Launcher 배경에 사용자 지정 이미지를 사용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **배경 이미지: 배경 이미지 정의**를 사용하도록 설정한 경우 **찾아보기**를 클릭하고 파일 위치로 이동하여 이미지 파일을 선택합니다. 지원되는 파일 형식은 PNG, JPG, JPEG 및 GIF입니다.
- **허용된 앱:** Citrix Launcher에서 허용하려는 각 앱에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **추가할 새 앱:** 추가할 앱의 전체 이름을 입력합니다. 예를 들어, Android 캘린더 앱의 경우 com.android.calendar입니다.
  - 앱을 추가하려면 **저장**을 클릭하고, 앱 추가를 취소하려면 **취소**를 클릭합니다.
- **암호:** 사용자가 Citrix Launcher를 종료하기 위해 입력해야 하는 암호입니다.

안드로이드 엔터프라이즈 설정



- **시스템 정보 사용:** Citrix Launcher 상태 표시줄에 시스템 정보를 표시할지 여부를 선택합니다. 기본값은 **끔**입니다. Secure Hub 26.8 이상이 필요합니다.
- **로고 이미지 정의:** Citrix Launcher 아이콘에 사용자 지정 로고 이미지를 사용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **로고 이미지: 로고 이미지 정의**를 사용하도록 설정하면 **찾아보기**를 클릭하여 이미지 파일을 선택하고 파일 위치로 이동합니다. 지원되는 파일 형식은 PNG, JPG, JPEG, GIF입니다.
- **배경 이미지 정의:** Citrix Launcher 배경에 사용자 지정 이미지를 사용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **배경 이미지: 배경 이미지 정의**를 사용하도록 설정하면 **찾아보기**를 클릭하여 이미지 파일을 선택하고 파일 위치로 이동합니다. 지원되는 파일 형식은 PNG, JPG, JPEG, GIF입니다.
- **허용된 앱:** Citrix Launcher에서 허용하려는 각 앱에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **추가할 새 앱:** 추가할 앱의 전체 이름을 입력합니다. 예를 들어, Android 캘린더 앱의 경우 com.android.calendar입니다.
  - 앱을 추가하려면 **저장**을 클릭하고, 앱 추가를 취소하려면 **취소**를 클릭합니다.
- **앱 자동 실행:** Citrix Launcher가 시작될 때 자동으로 시작할 **허용된 앱** 중 하나를 선택합니다. 기본값은 **없음** (자동 실행 안 함)입니다. Citrix Launcher 26.8 이상이 필요합니다.
- **암호:** 사용자가 Citrix Launcher를 종료하기 위해 입력해야 하는 암호입니다.

LDAP 장치 정책

XenMobile®에서 iOS 장치용 LDAP 정책을 생성하여 필요한 계정 정보를 포함한 사용할 LDAP 서버에 대한 정보를 제공합니다. 이 정책은 또한 LDAP 서버를 쿼리할 때 사용할 LDAP 검색 정책 세트를 제공합니다.

이 정책을 구성하기 전에 LDAP 호스트 이름이 필요합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **계정 설명:** 선택 사항인 계정 설명을 입력합니다.
- **계정 사용자 이름:** 선택 사항인 사용자 이름을 입력합니다.
- **계정 암호:** 선택 사항인 암호를 입력합니다. 이 필드는 암호화된 프로필에서만 사용하십시오.
- **LDAP 호스트 이름:** LDAP 서버 호스트 이름을 입력합니다. 이 필드는 필수입니다.
- **SSL 사용:** LDAP 서버에 대한 보안 소켓 계층 연결을 사용할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
- **검색 설정:** LDAP 서버를 쿼리할 때 사용할 검색 설정을 추가합니다. 원하는 만큼 검색 설정을 입력할 수 있지만, 계정을 유용하게 사용하려면 최소한 하나의 검색 설정을 추가해야 합니다. **추가**를 클릭한 다음 다음을 수행합니다.
    - **설명:** 검색 설정에 대한 설명을 입력합니다. 이 필드는 필수입니다.
    - **범위:** LDAP 트리에서 얼마나 깊이 검색할지 정의하려면 **기본**, **한 수준** 또는 **하위 트리**를 선택합니다. 기본값은 **기본**입니다.
        - **기본**은 검색 기본에서 가리키는 노드를 검색합니다.
        - **한 수준**은 기본 노드와 그 아래 한 수준을 검색합니다.
        - **하위 트리**는 깊이에 관계없이 기본 노드와 모든 하위 노드를 검색합니다.
    - **검색 기준:** 검색을 시작할 노드의 경로를 입력합니다. 예를 들어, ou=people 또는 0=example corp. 이 필드는 필수입니다.
    - 검색 설정을 추가하려면 **저장**을 클릭하고, 검색 설정 추가를 취소하려면 **취소**를 클릭합니다.
    - 추가하려는 각 검색 설정에 대해 이 단계를 반복합니다.
- **정책 설정**
    - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.

    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정

- **계정 설명:** 선택 사항인 계정 설명을 입력합니다.
- **계정 사용자 이름:** 선택 사항인 사용자 이름을 입력합니다.
- **계정 암호:** 선택 사항인 암호를 입력합니다. 이 필드는 암호화된 프로필에서만 사용합니다.
- **LDAP 호스트 이름:** LDAP 서버 호스트 이름을 입력합니다. 이 필드는 필수입니다.
- **SSL 사용:** LDAP 서버에 대한 보안 소켓 계층 연결을 사용할지 여부를 선택합니다. 기본값은 **켜기**입니다.
- **검색 설정:** LDAP 서버를 쿼리할 때 사용할 검색 설정을 추가합니다. 원하는 만큼 검색 설정을 입력할 수 있지만, 계정을 유용하게 사용하려면 최소한 하나의 검색 설정을 추가해야 합니다. **추가**를 클릭한 다음 다음을 수행합니다.
    - **설명:** 검색 설정에 대한 설명을 입력합니다. 이 필드는 필수입니다.
    - **범위:** LDAP 트리에서 검색할 깊이를 정의하려면 **기본(Base)**, **한 수준(One level)** 또는 **하위 트리(Subtree)**를 선택합니다. 기본값은 **기본(Base)**입니다.
        - **기본(Base)**은 검색 기준(Search base)이 가리키는 노드를 검색합니다.
        - **한 수준(One level)**은 기본(Base) 노드와 그 아래 한 수준을 검색합니다.
        - **하위 트리(Subtree)**는 깊이에 관계없이 기본(Base) 노드와 모든 하위 노드를 검색합니다.
    - **검색 기준:** 검색을 시작할 노드의 경로를 입력합니다. 예를 들어, ou=people 또는 0=example corp. 이 필드는 필수입니다.
    - 검색 설정을 추가하려면 **저장**을 클릭하고, 검색 설정 추가를 취소하려면 **취소**를 클릭합니다.
    - 추가하려는 각 검색 설정에 대해 이 단계를 반복합니다.
- **정책 설정**
    - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
        - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
        - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.

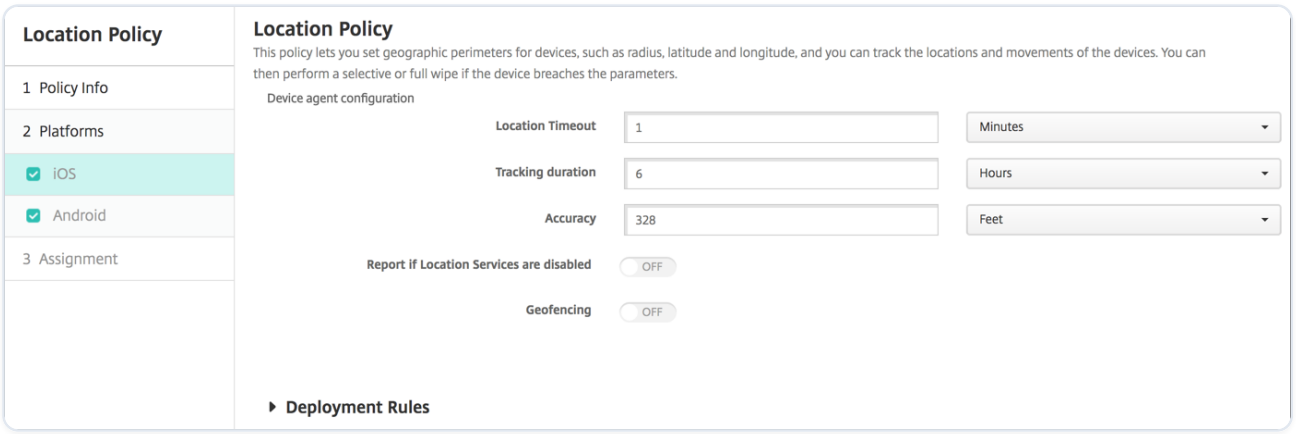
- **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다. **암호 필요**를 선택한 경우, **제거 암호** 필드에 암호를 입력합니다.
- **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 아니면 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

위치 장치 정책

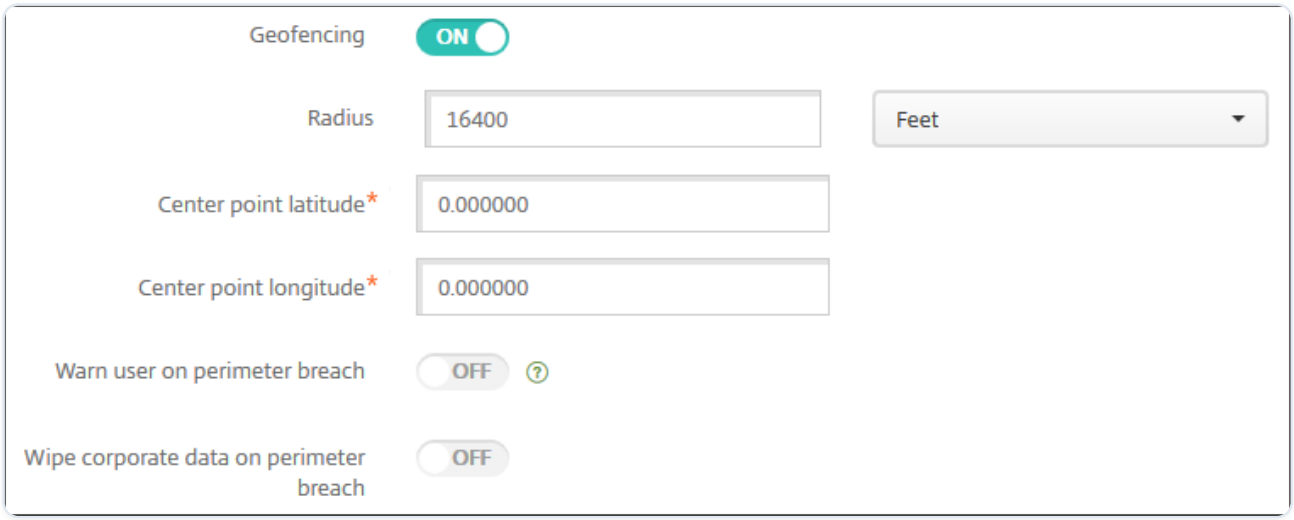
XenMobile에서 지리적 경계를 적용하기 위해 위치 장치 정책을 생성합니다. 사용자가 정의된 경계(일명 *지오펜스*)를 위반하면 XenMobile은 특정 작업을 수행할 수 있습니다. 예를 들어, 사용자가 정의된 경계를 위반할 때 경고 메시지를 발행하도록 정책을 구성할 수 있습니다. 또한 사용자가 경계를 위반할 때 즉시 또는 지연 후 사용자 기업 데이터를 삭제하도록 정책을 구성할 수 있습니다. 장치 추적 및 위치 파악 활성화와 같은 보안 작업에 대한 자세한 내용은 보안 작업을 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



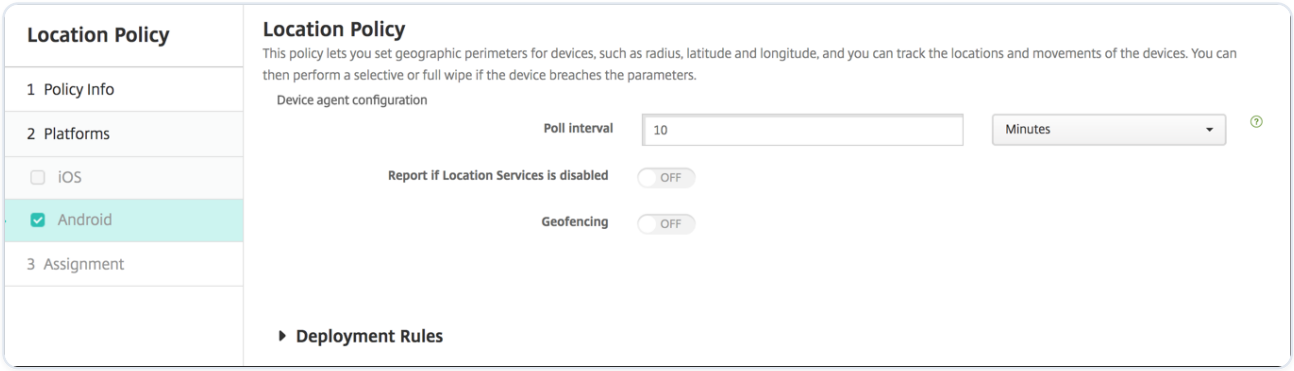
- **위치 시간 초과:** 숫자를 입력한 다음 목록에서 **초** 또는 **분**을 클릭하여 XenMobile®이 장치 위치를 확인하려는 빈도를 설정합니다. 유효 값은 60–900초 또는 1–15분입니다. 기본값은 1분입니다.
- **추적 기간:** 숫자를 입력한 다음 목록에서 **시간** 또는 **분**을 클릭하여 XenMobile이 장치를 추적하는 기간을 설정합니다. 유효 값은 1–6시간 또는 10–360분입니다. 기본값은 6시간입니다.
- **정확도:** 숫자를 입력한 다음 목록에서 **미터**, **피트** 또는 **야드**를 클릭하여 XenMobile이 장치를 추적하는 장치와의 근접도를 설정합니다. 유효 값은 10–5000야드 또는 미터, 또는 30–15000피트입니다. 기본값은 328피트입니다.
- **위치 서비스 비활성화 시 보고:** GPS가 비활성화될 때 장치가 XenMobile에 보고서를 보낼지 여부를 선택합니다. 기본값은 **끔**입니다.
- **지오펜싱**



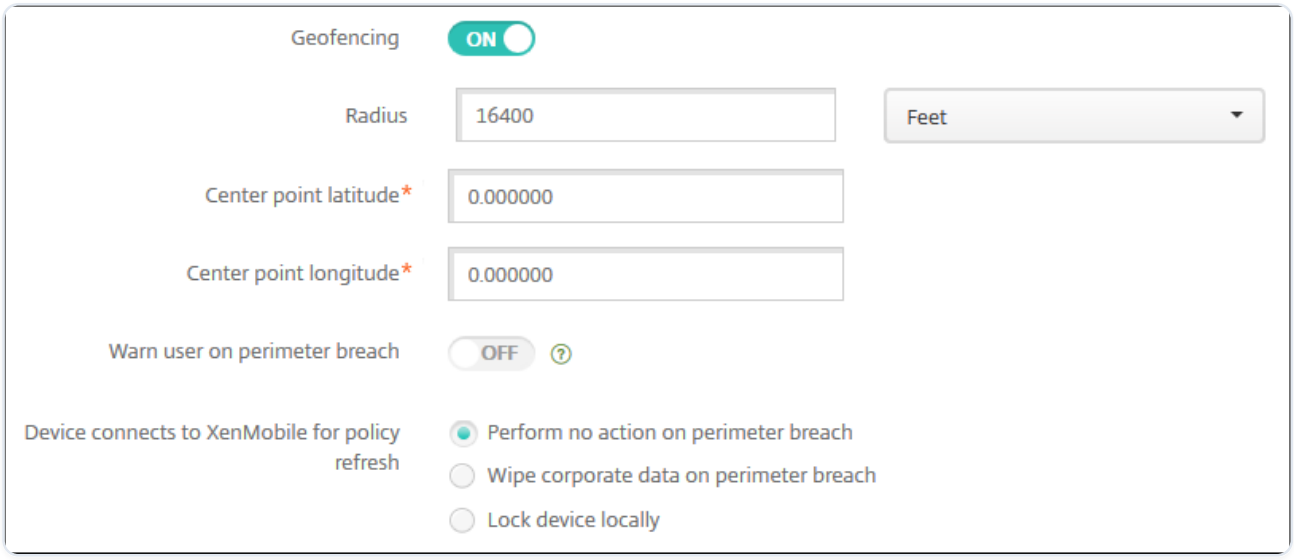
지오펜싱을 활성화하면 다음 설정을 구성합니다.

- **반경:** 숫자를 입력한 다음 목록에서 반경을 측정하는 데 사용할 단위를 클릭합니다. 기본값은 16,400피트입니다. 반경의 유효 값은 다음과 같습니다.
  - 164–164000피트
  - 50–50000미터
  - 54–54680 야드
  - 1–31 마일
- **중심점 위도:** 지오펜스 중심점의 위도를 정의하려면 37.787454와 같은 위도를 입력합니다.
- **중심점 경도:** 지오펜스 중심점의 경도를 정의하려면 122.402952와 같은 경도를 입력합니다.
- **경계 위반 시 사용자에게 경고:** 사용자가 정의된 경계를 위반할 때 경고 메시지를 발행할지 여부를 선택합니다. 기본값은 **해제**입니다. 경고 메시지를 표시하는 데 XenMobile에 대한 연결은 필요하지 않습니다.
- **경계 위반 시 회사 데이터 지우기:** 사용자가 경계를 위반할 때 사용자 장치를 지울지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 활성화하면 **로컬 지우기 지연 필드**가 나타납니다.
  - 숫자를 입력한 다음 목록에서 **초** 또는 **분**을 클릭하여 사용자 장치에서 회사 데이터를 지우기 전에 지연할 시간을 설정합니다. 이 설정은 XenMobile이 장치를 선택적으로 지우기 전에 사용자가 허용된 위치로 돌아갈 기회를 제공합니다. 기본값은 0초입니다.

Android 설정



- **폴링 간격:** 숫자를 입력한 다음 목록에서 **분**, **시간** 또는 **일**을 클릭하여 XenMobile이 장치 위치를 수정하려는 빈도를 설정합니다. 유효한 값은 1–1440분, 1–24시간 또는 임의의 일수입니다. 기본값은 10분입니다. 이 값을 10분 미만으로 설정하면 장치의 배터리 수명에 부정적인 영향을 미칠 수 있습니다.
- **위치 서비스 비활성화 시 보고:** GPS가 비활성화되었을 때 장치가 XenMobile에 보고서를 보낼지 여부를 선택합니다. 기본값은 **해제**입니다.
- **지오펜싱**



지오펜싱을 활성화하면 다음 설정을 구성합니다.

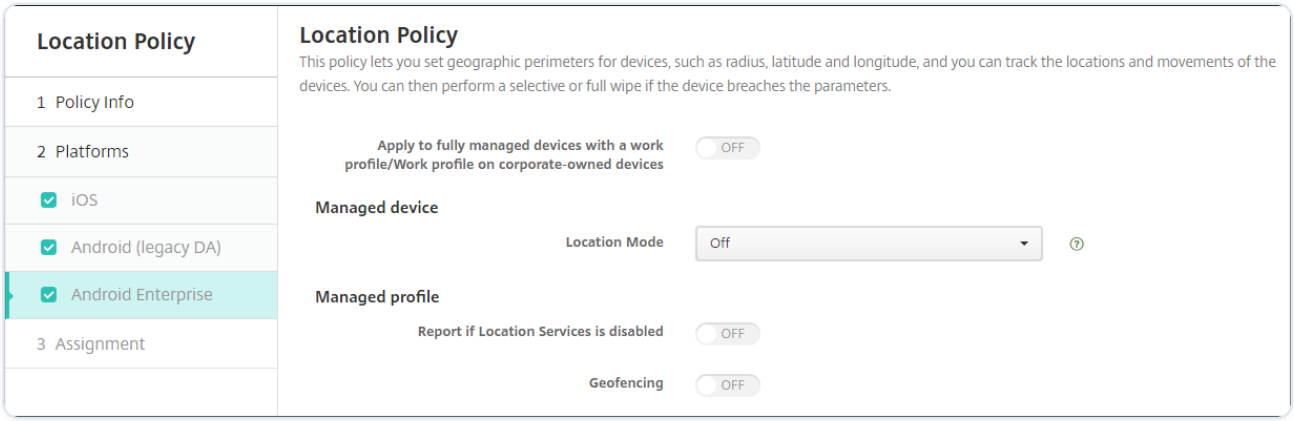
- **반경:** 숫자를 입력한 다음 목록에서 반경을 측정하는 데 사용할 단위를 클릭합니다. 기본값은 16,400피트입니다. 반경의 유효한 값은 다음과 같습니다.
  - 164–164000피트
  - 1–50킬로미터
  - 50–50000미터
  - 54–54680야드
  - 1–31마일

- **중심점 위도:** 37.787454와 같은 위도를 입력하여 지오펜스 중심점의 위도를 정의합니다.
- **중심점 경도:** 122.402952와 같은 경도를 입력하여 지오펜스 중심점의 경도를 정의합니다.
- **경계 위반 시 사용자에게 경고:** 사용자가 정의된 경계를 위반할 때 경고 메시지를 발행할지 여부를 선택합니다. 기본값은 **해제**입니다. 경고 메시지를 표시하는 데 XenMobile에 대한 연결이 필요하지 않습니다.
- **정책 새로 고침을 위해 장치가 XenMobile에 연결:** 사용자가 경계를 위반할 때 다음 옵션 중 하나를 선택합니다.
    - **경계 위반 시 아무 작업도 수행 안 함:** 아무것도 하지 않습니다. 이 설정이 기본값입니다.
    - **경계 위반 시 회사 데이터 지우기:** 지정된 시간 후에 회사 데이터를 지웁니다. 이 옵션을 사용하도록 설정하면 **로컬 지우기 지연** 필드가 나타납니다.
        - 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 사용자 장치에서 회사 데이터를 지우기 전에 지연할 시간을 설정합니다. 이 설정을 통해 사용자는 XenMobile이 장치를 선택적으로 지우기 전에 허용된 위치로 돌아갈 기회를 얻습니다. 기본값은 0초입니다.
    - **잠금 지연:** 지정된 시간 후에 사용자 장치를 잠급니다. 이 옵션을 사용하도록 설정하면 **잠금 지연 필드**가 나타납니다.
        - 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 사용자 장치를 잠그기 전에 지연할 시간을 설정합니다. 이 설정을 통해 사용자는 XenMobile이 장치를 잠그기 전에 허용된 위치로 돌아갈 기회를 얻습니다. 기본값은 0초입니다.

안드로이드 엔터프라이즈 설정

Android 위치 추적이 작동하려면 다음 요구 사항이 충족되었는지 확인하십시오.

- Android 8.5 이상
- Android Enterprise용 제한 장치 정책에서 **위치 공유 허용** 설정이 활성화됨
- 연결 스케줄링(Firebase Cloud Messaging 권장)



업무 프로필이 있는 완전 관리형 장치에 적용

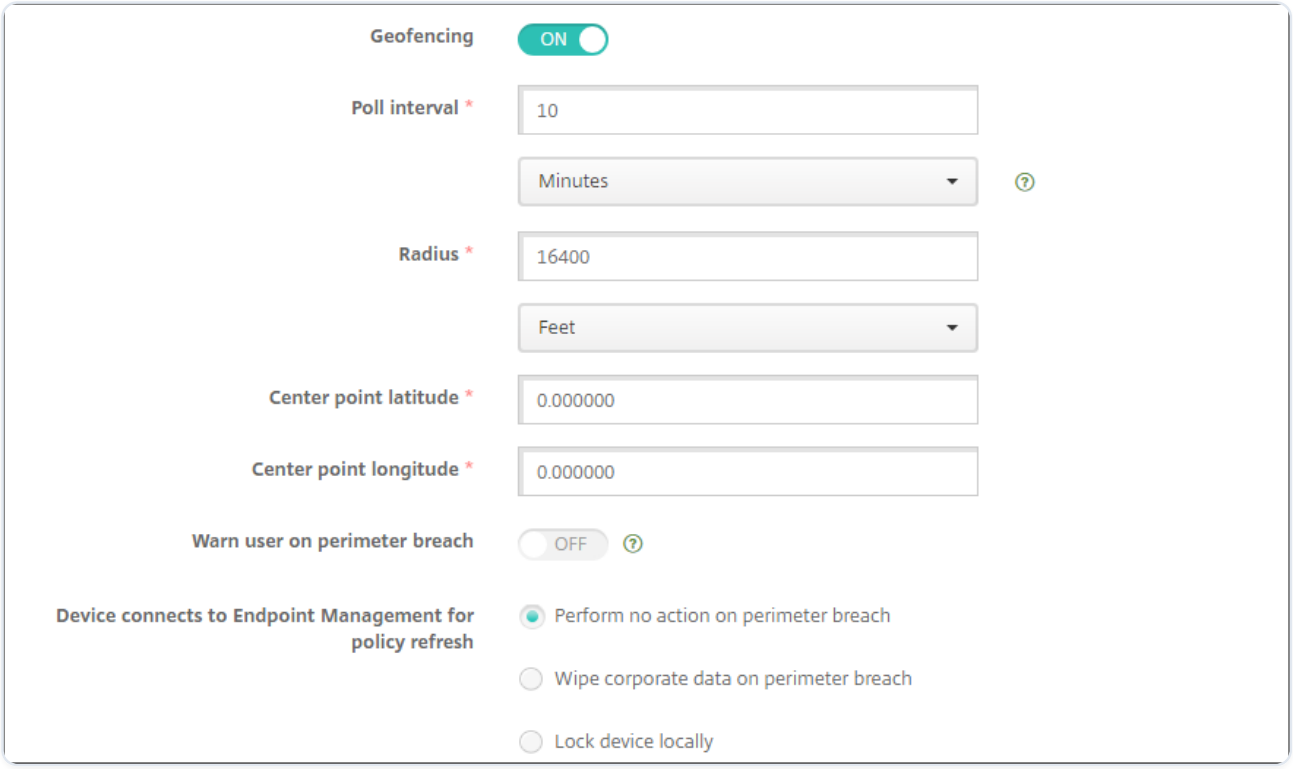
업무 프로필이 있는 완전 관리형 장치의 경우 위치 모드 설정만 사용할 수 있습니다.

- **업무 프로필이 있는 완전 관리형 장치/회사 소유 장치의 업무 프로필에 적용:** 업무 프로필이 있는 완전 관리형 장치의 위치 모드를 구성할 수 있습니다. 이 설정이 켜져 있으면 업무 프로필에 대한 위치 모드 설정을 구성합니다.
    - **위치 서비스 비활성화 시 보고:** 사용자가 GPS를 끄면 장치가 XenMobile Server에 보고서를 보낼지 여부를 선택합니다. 기본값은 **끔**입니다.
    - **지오펜싱:** 이 문서의 관리형 장치 아래에 있는 설정을 참조하십시오.

업무 프로필이 있는 완전 관리형 장치/회사 소유 장치의 업무 프로필에 적용이 꺼져 있으면 다음 섹션에 표시된 대로 설정이 관리형 장치 및 업무 프로필에 적용됩니다. 기본값은 **끔**입니다.

관리형 장치

- **위치 모드:** 활성화할 위치 감지 정도를 지정합니다. 위치 모드가 고정밀 또는 배터리 절약으로 설정된 경우에만 **찾기** 보안 작업을 사용할 수 있습니다. 기본값은 고정밀입니다.
    - **고정밀:** GPS, 네트워크 및 기타 센서를 포함한 모든 위치 감지 방법을 활성화합니다.
    - **센서 전용:** GPS 및 기타 센서만 활성화합니다.
    - **배터리 절약:** 네트워크 위치 공급자만 활성화합니다.
    - **끄기:** 위치 감지를 비활성화합니다.
- **지오펜싱:**



지오펜싱을 활성화하면 다음 설정을 구성합니다.

- **폴링 간격:** 숫자를 입력한 다음 **분**, **시간** 또는 **일**을 클릭하여 XenMobile Server가 장치의 위치를 수정하려는 빈도를 설정합니다. 유효한 값은 1~1440분, 1~24시간 또는 임의의 일 수입니다. 기본값은 **10분**입니다. 이 값을 10분 미만으로 설정하면 장치의 배터리 수명에 부정적인 영향을 미칠 수 있습니다.
- **반경:** 숫자를 입력한 다음 반경을 측정하는 데 사용할 단위를 클릭합니다. 기본값은 **16400피트(5000미터)**입니다. 반경의 유효한 값은 다음과 같습니다.
  - 164–164000피트
  - 1–50킬로미터
  - 50–50000미터
  - 54–54680야드
  - 1–31마일
- **중심점 위도:** 37.787454와 같은 위도를 입력하여 지오펜스 중심점의 위도를 정의합니다. 값을 조회하려면 **관리 > 장치**로 이동하여 장치를 선택하고 **보안**을 클릭한 다음 **찾기**를 클릭합니다. 장치를 찾은 후 XenMobile Server는 **보안** 아래의 장치 **세부 정보 > 일반** 페이지에 장치 위치를 보고합니다.
- **중심점 경도:** 122.402952와 같은 경도를 입력하여 지오펜스 중심점의 경도를 정의합니다.
- **경계 위반 시 사용자에게 경고:** 사용자가 정의된 경계를 위반할 때 경고 메시지를 발행할지 여부를 선택합니다. 기본값은 **끄기**입니다. 경고 메시지를 표시하는 데 XenMobile Server에 대한 연결이 필요하지 않습니다.

- **정책 새로 고침을 위해 장치가 XenMobile Server에 연결:** 사용자가 경계를 위반할 경우 다음 옵션 중 하나를 선택합니다.
  - **경계 위반 시 아무 작업도 수행하지 않음:** 아무 작업도 수행하지 않습니다. 이 설정이 기본값입니다.
  - **경계 위반 시 회사 데이터 지우기:** 지정된 시간 후에 회사 데이터를 지웁니다. 이 옵션을 활성화하면 **로컬 지우기 지연** 필드가 나타납니다.
    - 숫자를 입력한 다음 **초** 또는 **분**을 클릭하여 사용자 장치에서 회사 데이터를 지우기 전에 지연할 시간을 설정합니다. 이 지연 시간은 XenMobile Server가 장치를 선택적으로 지우기 전에 사용자가 허용된 위치로 돌아갈 기회를 제공합니다. 기본값은 **0초**입니다.
  - **장치 로컬 잠금:** 지정된 시간 후에 사용자 장치를 잠급니다. 이 옵션을 활성화하면 **잠금 지연** 필드가 나타납니다.
    - 숫자를 입력한 다음 **초** 또는 **분**을 클릭하여 사용자 장치를 잠그기 전에 지연할 시간을 설정합니다. 이 지연 시간은 XenMobile Server가 장치를 잠그기 전에 사용자가 허용된 위치로 돌아갈 기회를 제공합니다. 기본값은 **0초**입니다.

관리형 프로필

- **위치 서비스가 비활성화된 경우 보고:** 사용자가 GPS를 끄면 장치가 XenMobile Server에 보고서를 보낼지 여부를 선택합니다. 기본값은 **해제**입니다.
- **지오펜싱:** 이 문서의 관리형 장치 아래에 있는 설정을 참조하십시오.

메일 장치 정책

XenMobile®에서 메일 장치 정책을 추가하여 iOS 또는 macOS 장치에 이메일 계정을 구성할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 및 macOS 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policy-mail-ios.png)

- **계정 설명:** Mail 및 설정 앱에 표시되는 계정 설명을 입력합니다. 이 필드는 필수입니다.
- **계정 유형:** 사용자 계정에 사용할 프로토콜을 선택하려면 **IMAP** 또는 **POP**을 선택합니다. 기본값은 **IMAP**입니다. **POP**을 선택하면 다음 **경로** 접두사 옵션이 사라집니다.
- **경로 접두사: INBOX** 또는 IMAP 메일 계정 경로 접두사를 입력합니다. 이 필드는 필수입니다.
- **사용자 표시 이름:** 메시지 및 기타 용도로 사용할 전체 사용자 이름을 입력합니다. 이 필드는 필수입니다.

- **이메일 주소:** 계정의 전체 이메일 주소를 입력합니다. 이 필드는 필수입니다.
- **수신 이메일 설정**
  - **이메일 서버 호스트 이름:** 수신 메일 서버 호스트 이름 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
  - **이메일 서버 포트:** 수신 메일 서버 포트 번호를 입력합니다. 기본값은 **143**입니다. 이 필드는 필수입니다.
  - **사용자 이름:** 이메일 계정의 사용자 이름을 입력합니다. 이 이름은 일반적으로 @ 문자 앞까지의 이메일 주소와 동일합니다. 이 필드는 필수입니다.
  - **인증 유형:** 사용할 인증 유형을 선택합니다. 기본값은 **암호**입니다. **없음**을 선택하면 다음 **암호** 필드가 사라집니다.
  - **비밀번호:** 수신 메일 서버에 대한 선택적 비밀번호를 입력합니다.
  - **SSL 사용:** 수신 메일 서버가 Secure Socket Layer 인증을 사용하는지 여부를 선택합니다. 기본값은 **해제**입니다.
- **보내는 이메일 설정**
  - **이메일 서버 호스트 이름:** 보내는 메일 서버 호스트 이름 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
  - **이메일 서버 포트:** 보내는 메일 서버 포트 번호를 입력합니다. 포트 번호를 입력하지 않으면 지정된 프로토콜의 기본 포트가 사용됩니다.
  - **사용자 이름:** 이메일 계정의 사용자 이름을 입력합니다. 이 이름은 일반적으로 @ 문자 앞까지의 이메일 주소와 동일합니다. 이 필드는 필수입니다.
  - **인증 유형:** 사용할 인증 유형을 선택합니다. 기본값은 **비밀번호**입니다.
  - **비밀번호:** 보내는 메일 서버에 대한 선택적 비밀번호를 입력합니다.
  - **보내는 비밀번호를 받는 비밀번호와 동일하게:** 수신 및 발신 비밀번호가 동일한지 여부를 선택합니다. 기본값은 **해제**이며, 이는 비밀번호가 다르다는 것을 의미합니다.
  - **SSL 사용:** 보내는 메일 서버가 Secure Socket Layer 인증을 사용하는지 여부를 선택합니다. 기본값은 **해제**입니다.
- **정책**
  - **계정 간 이메일 이동 허용:** 사용자가 이 계정에서 다른 계정으로 이메일을 이동하고, 다른 계정에서 전달 및 회신할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **해제**입니다.
  - **메일 앱에서만 이메일 보내기:** 사용자가 이메일을 보낼 때 iOS 메일 앱으로 제한할지 여부를 선택합니다.

- **메일 최근 항목 동기화 비활성화:** 사용자가 최근 주소를 동기화하지 못하도록 할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션은 iOS 6.0 이상에만 적용됩니다.
- **Mail Drop 허용:** iOS 9.2 이상을 실행하는 기기에서 Apple Mail Drop 사용을 허용할지 여부를 선택합니다. 기본값은 **해제**입니다.
- **S/MIME 서명 활성화:** 이 계정이 S/MIME 서명을 지원하는지 선택합니다. 기본값은 **켜짐**입니다. **켜짐**으로 설정하면 다음 필드가 나타납니다.
  - **서명 ID 자격 증명:** 사용할 서명 자격 증명을 선택합니다.
  - **S/MIME 서명 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME 서명을 켜거나 끌 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
  - **S/MIME 서명 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 사용할 서명 자격 증명을 선택할 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
- **S/MIME 암호화 활성화:** 이 계정이 S/MIME 암호화를 지원하는지 선택합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정하면 다음 필드가 나타납니다.
  - **암호화 ID 자격 증명:** 사용할 암호화 자격 증명을 선택합니다.
  - **메시지별 S/MIME 스위치 활성화: 켜짐**으로 설정하면 사용자가 작성하는 각 메시지에 대해 S/MIME 암호화를 켜거나 끌 수 있는 옵션을 표시합니다. 기본값은 **꺼짐**입니다.
  - **S/MIME 기본 암호화 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME가 기본적으로 켜져 있는지 여부를 선택할 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
  - **S/MIME 암호화 인증서 UUID 사용자 재정의 가능: 켜짐**으로 설정하면 사용자는 장치 설정에서 S/MIME 암호화 ID 및 암호화를 켜거나 끌 수 있습니다. 기본값은 **꺼짐**입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.

- **정책 설정**
  - **정책 제거:** 나중에 정책을 제거하려면 이 설정을 구성하여 **날짜 선택** 또는 **제거까지의 기간(시간)**에 정책을 제거할 수 있습니다.
  - **사용자가 정책을 제거하도록 허용:** 사용자가 메일 정책을 **항상** 제거하거나, **암호 필요** 시에만 제거하거나, **절대 제거하지 않도록** 허용합니다.
  - **프로필 범위:** macOS에만 해당하며, 정책이 **사용자** 수준으로 적용될지 또는 전체 **시스템**에 걸쳐 적용될지 선택합니다.

관리형 구성 정책

관리형 구성 장치 정책은 다양한 앱 구성 옵션 및 앱 제한을 제어합니다. 앱 개발자가 앱에 사용할 수 있는 옵션과 도구 설명을 정의합니다. 도구 설명에 "템플릿화된 값" 사용이 언급된 경우, 해당 XenMobile 매크로를 대신 사용하십시오. 자세한 내용은 원격 구성 개요(Android 개발자 사이트) 및 매크로를 참조하십시오.

앱 구성 설정에는 다음과 같은 항목이 포함될 수 있습니다.

- 앱 이메일 설정
- 웹 브라우저의 URL 허용 또는 차단
- 셀룰러 연결 또는 Wi-Fi 연결을 통해서만 앱 콘텐츠 동기화를 제어하는 옵션

앱에 표시되는 설정에 대한 자세한 내용은 앱 개발자에게 문의하십시오.

필수 구성 요소

- Google에서 Android Enterprise 설정 작업을 완료하고 Android Enterprise를 관리형 Google Play에 연결합니다. 자세한 내용은 Android Enterprise를 참조하십시오.
- Android Enterprise 앱을 XenMobile에 추가합니다. 자세한 내용은 XenMobile에 앱 추가를 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

앱별 VPN 요구 사항

AE용 앱별 VPN을 생성하려면 관리형 구성 정책을 구성하는 것 외에 추가 단계를 수행해야 합니다. 또한 다음 필수 구성 요소가 충족되었는지 확인해야 합니다.

- 온프레미스 Citrix Gateway
- 다음 애플리케이션이 장치에 설치되어 있습니다.
  - 시트릭스 SSO
  - 시트릭스 시큐어 허브™

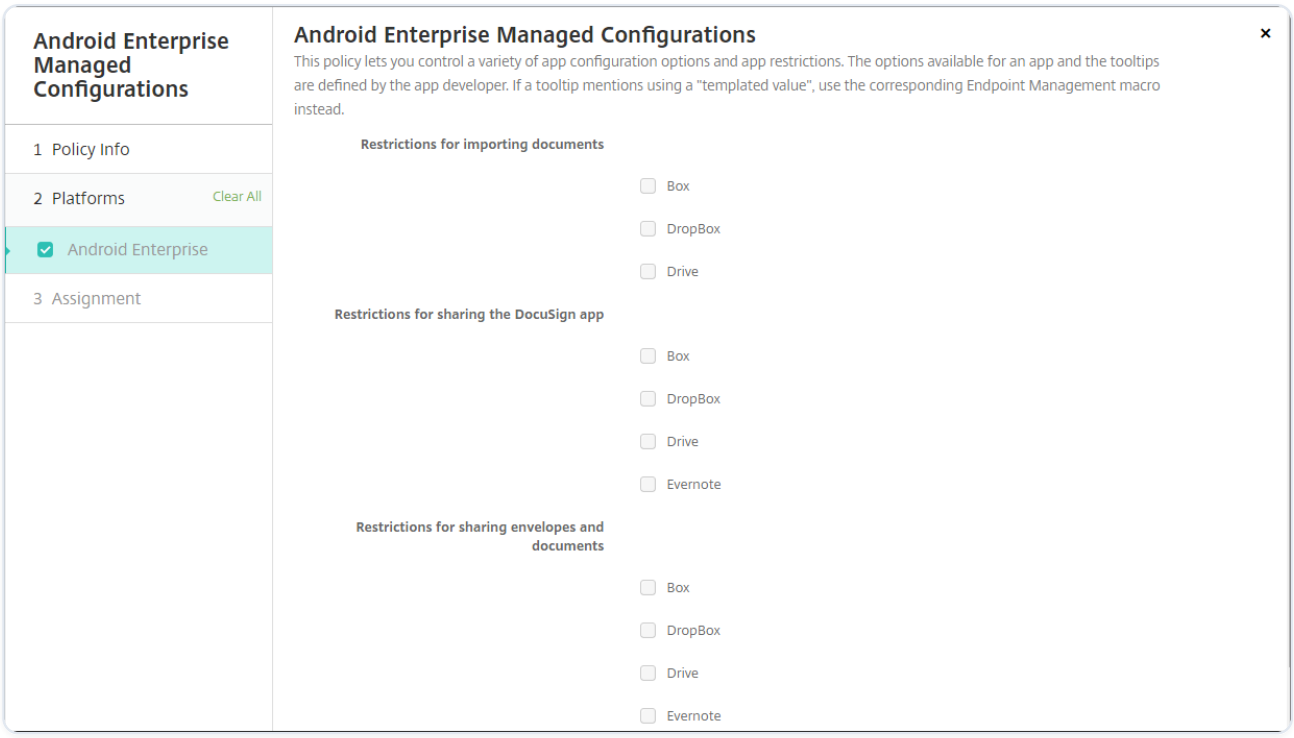
AE 장치용 앱별 VPN을 구성하는 일반적인 워크플로는 다음과 같습니다.

1. 이 문서에 설명된 대로 VPN 프로필을 구성합니다.
2. 앱별 VPN의 트래픽을 수락하도록 Citrix ADC를 구성합니다. 자세한 내용은 Citrix Gateway의 전체 VPN 설정을 참조하십시오.

안드로이드 엔터프라이즈 설정

관리형 구성 장치 정책을 추가하도록 선택하면 앱을 선택하라는 메시지가 나타납니다. XenMobile®에 추가된 Android Enterprise 앱이 없으면 계속할 수 없습니다.

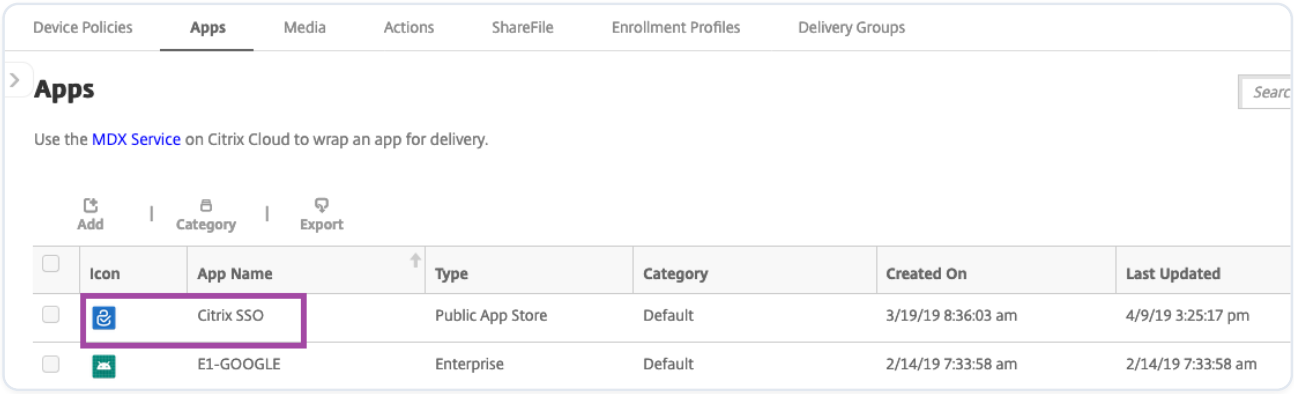
앱을 선택한 후 정책 설정을 구성합니다. 설정은 각 앱에 따라 다릅니다.



Android Enterprise용 VPN 프로필 구성

관리형 구성 장치 정책과 함께 Citrix SSO 앱을 사용하여 Android Enterprise 장치에서 VPN 프로필을 사용할 수 있도록 합니다.

Google Play 스토어 앱으로 Citrix SSO를 XenMobile 콘솔에 추가하는 것부터 시작합니다. 공개 앱 스토어 앱 추가를 참조하십시오.



Citrix SSO용 Android Enterprise 관리형 구성 생성

VPN 프로필을 생성하도록 Citrix SSO용 관리형 구성 장치 정책을 구성합니다. Citrix SSO 앱이 설치되어 있고 정책이 배포된 장치는 생성한 VPN 프로필에 액세스할 수 있습니다.

Citrix Gateway FQDN과 포트가 필요합니다.

1. XenMobile 콘솔에서 **구성 > 장치 정책**을 클릭합니다. **추가**를 클릭합니다.
2. **Android Enterprise**를 선택합니다. **관리되는 구성**을 클릭합니다.

   Android Enterprise 정책 선택 이미지 (/en-us/xenmobile/server/media/select-ae-managed-configuration-policy.png)
3. **응용 프로그램 ID 선택** 창이 나타나면 목록에서 **Citrix SSO**를 선택하고 **확인**을 클릭합니다.

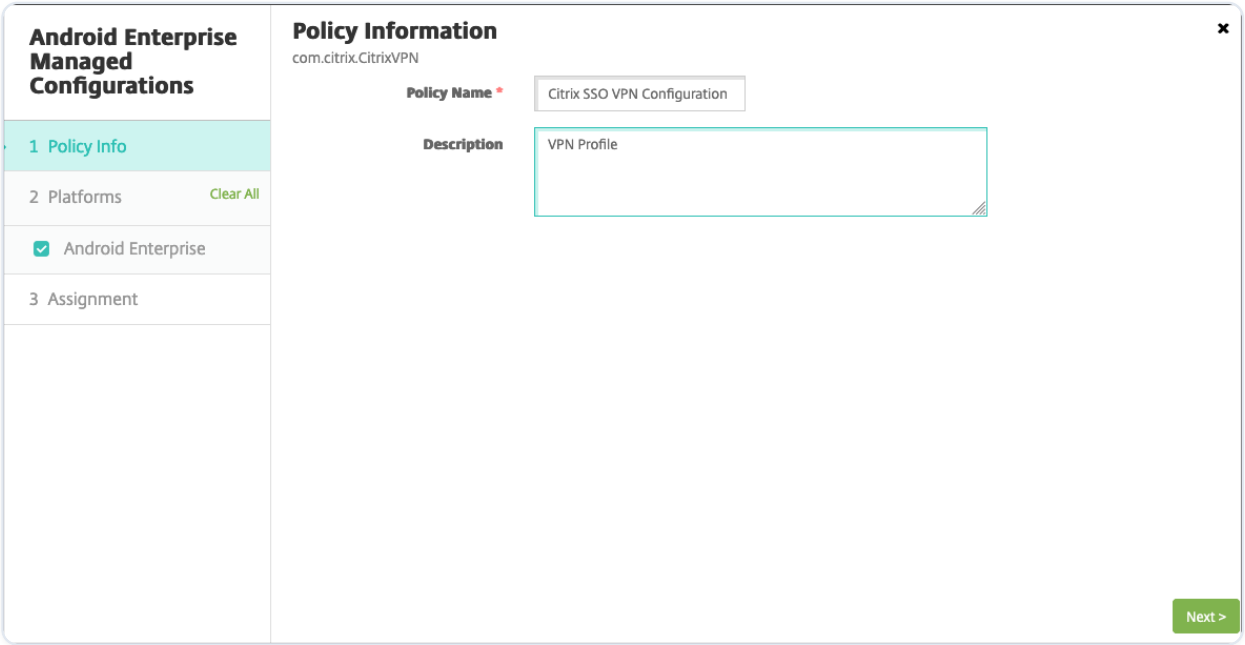
   응용 프로그램 ID 선택 창 이미지 (/en-us/xenmobile/server/media/citrix-sso-select-app-id.png)
4. Citrix SSO VPN 구성의 이름과 설명을 입력합니다. **다음**을 클릭합니다.

   Android Enterprise 관리되는 구성 마법사 이미지 (/en-us/xenmobile/server/media/citrix-sso-ae-managed-config-1.png)
5. VPN 프로필 매개변수를 구성합니다.

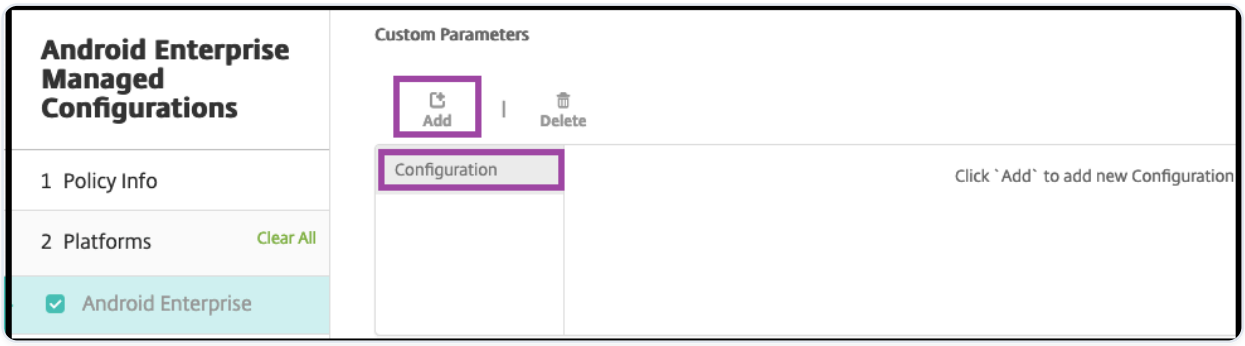
   - **VPN 프로필 이름.** VPN 프로필의 이름을 입력합니다. 두 개 이상의 VPN 프로필을 만드는 경우 각 프로필에 고유한 이름을 사용합니다. 이름을 제공하지 않으면 **서버 주소** 필드에 입력한 주소가 VPN 프로필 이름으로 사용됩니다.
   - **서버 주소(*).** Citrix Gateway FQDN을 입력합니다. Citrix Gateway 포트가 443이 아닌 경우 포트도 입력합니다. URL 형식을 사용합니다. 예를 들어, `https://gateway.mycompany.com:8443`.
   - **사용자 이름(선택 사항).** 최종 사용자가 Citrix Gateway에 인증하는 데 사용하는 사용자 이름을 제공합니다. 이 필드에 XenMobile 매크로 {user.username}을 사용할 수 있습니다. (매크로 참조). 사용자 이름을 제공하지 않으면 사용자가 Citrix Gateway에 연결할 때 사용자 이름을 제공하라는 메시지가 표시됩니다.
   - **암호(선택 사항).** 최종 사용자가 Citrix Gateway에 인증하는 데 사용하는 암호를 제공합니다. 암호를 제공하지 않으면 사용자가 Citrix Gateway에 연결할 때 암호를 제공하라는 메시지가 표시됩니다.
   - **인증서 별칭(선택 사항).** 인증서 별칭을 입력합니다. 인증서 별칭을 사용하면 앱이 인증서에 더 쉽게 액세스할 수 있습니다. 자격 증명 장치 정책과 동일한 인증서 별칭을 사용하면 앱이 인증서를 검색하고 사용자 작업 없이 VPN을 인증합니다.
   - **앱별 VPN 유형(선택 사항).** 이 VPN을 사용하는 앱을 제한하기 위해 앱별 VPN을 사용하는 경우 이 설정을 구성할 수 있습니다. **허용**을 선택하면 **PerAppVPN 앱 목록**에 나열된 앱 패키지 이름의 네트

워크 트래픽이 VPN을 통해 라우팅됩니다. 다른 모든 앱의 네트워크 트래픽은 VPN 외부로 라우팅됩니다. **허용 안 함**을 선택하면 **PerAppVPN 앱 목록**에 나열된 앱 패키지 이름의 네트워크 트래픽이 VPN 외부로 라우팅됩니다. 다른 모든 앱의 네트워크 트래픽은 VPN을 통해 라우팅됩니다. 기본값은 **허용**입니다.

- **PerAppVPN 앱 목록.** VPN에서 트래픽이 허용되거나 차단되는 앱 목록입니다. 이는 **Per-App VPN 유형** 값에 따라 달라집니다. 앱 패키지 이름을 쉼표나 세미콜론으로 구분하여 나열합니다. 앱 패키지 이름은 대소문자를 구분하며 Google Play 스토어에 표시된 것과 정확히 일치해야 합니다. 이 목록은 선택 사항입니다. 장치 전체 VPN을 프로비저닝하려면 이 목록을 비워 두십시오.
- **기본 VPN 프로필.** 사용자가 특정 프로필을 탭하는 대신 Citrix SSO 앱의 사용자 인터페이스에서 연결 스위치를 탭할 때 사용할 VPN 프로필 이름을 입력합니다. 이 필드를 비워두면 기본 프로필이 연결에 사용됩니다. 프로필이 하나만 구성된 경우 기본 프로필로 표시됩니다. 상시 연결 VPN의 경우 이 필드는 상시 연결 VPN을 설정하는 데 사용할 VPN 프로필 이름으로 설정해야 합니다.
- **사용자 프로필 비활성화.** 이 설정이 켜져 있으면 사용자는 장치에서 자체 VPN을 만들 수 없습니다. 이 설정이 꺼져 있으면 사용자는 장치에서 자체 VPN을 만들 수 있습니다. 기본값은 꺼짐입니다.
- **신뢰할 수 없는 서버 차단.** Citrix Gateway에 자체 서명된 인증서를 사용하거나 Citrix Gateway 인증서를 발급하는 CA의 루트 인증서가 시스템 CA 목록에 없는 경우 이 설정은 꺼집니다. 이 설정이 켜져 있으면 Android 운영 체제가 Citrix Gateway 인증서를 검증합니다. 검증에 실패하면 연결이 허용되지 않습니다. 기본값은 켜짐입니다.



6. 선택적으로 사용자 지정 매개변수를 생성합니다. 사용자 지정 매개변수 **XenMobileDeviceId** 및 **UserAgent**가 지원됩니다. 현재 VPN 구성을 선택하고 **추가**를 클릭합니다.



a. 사용자 지정 매개변수 생성:

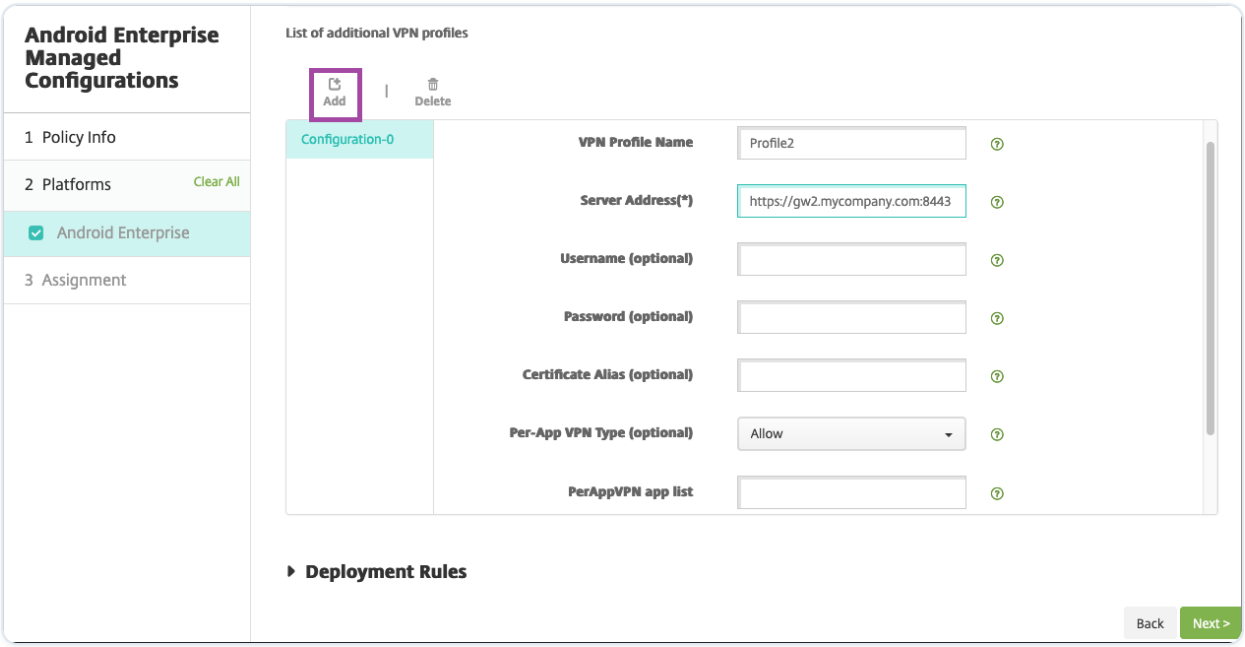
- **매개변수 이름. XenMobileDeviceId**를 입력합니다. 이 필드는 XenMobile에 장치 등록을 기반으로 네트워크 액세스 확인에 사용할 장치 ID입니다. XenMobile이 장치를 등록하고 관리하는 경우 VPN 연결이 허용됩니다. 그렇지 않으면 VPN 설정 시 인증이 거부됩니다.
- **매개변수 값.** XenMobile이 장치의 등록 및 관리 상태를 확인하려면 XenMobileDeviceID 값을 `DeviceID_${device.id}`으로 설정합니다.



a. 다른 사용자 지정 매개변수를 생성하려면 **추가**를 다시 클릭합니다. 이 사용자 지정 매개변수를 생성합니다.

- **매개변수 이름. UserAgent**를 입력합니다. 이 텍스트는 Citrix Gateway에서 추가 확인을 수행하기 위해 User-Agent HTTP 헤더에 추가됩니다. 이 텍스트의 값은 Citrix SSO 앱이 Citrix Gateway와 통신하는 동안 User-Agent HTTP 헤더에 추가됩니다.
- **매개변수 값.** User-Agent HTTP 헤더에 추가할 텍스트를 입력합니다. 이 텍스트는 HTTP User-Agent 사양을 준수해야 합니다.

7. 선택적으로 더 많은 VPN 프로필 구성을 생성합니다. 구성 목록 아래의 **추가**를 클릭합니다. 새 구성이 목록에 나타납니다. 새 구성을 선택하고 5단계와 선택적으로 6단계를 반복합니다.



8. 원하는 모든 VPN 프로필을 생성했으면 **다음**을 클릭합니다.
9. Citrix SSO에 대한 이 관리 구성의 배포 규칙을 구성합니다.
10. **저장**을 클릭합니다.

Citrix SSO에 대한 이 관리 구성이 이제 구성된 장치 정책 목록에 나타납니다.

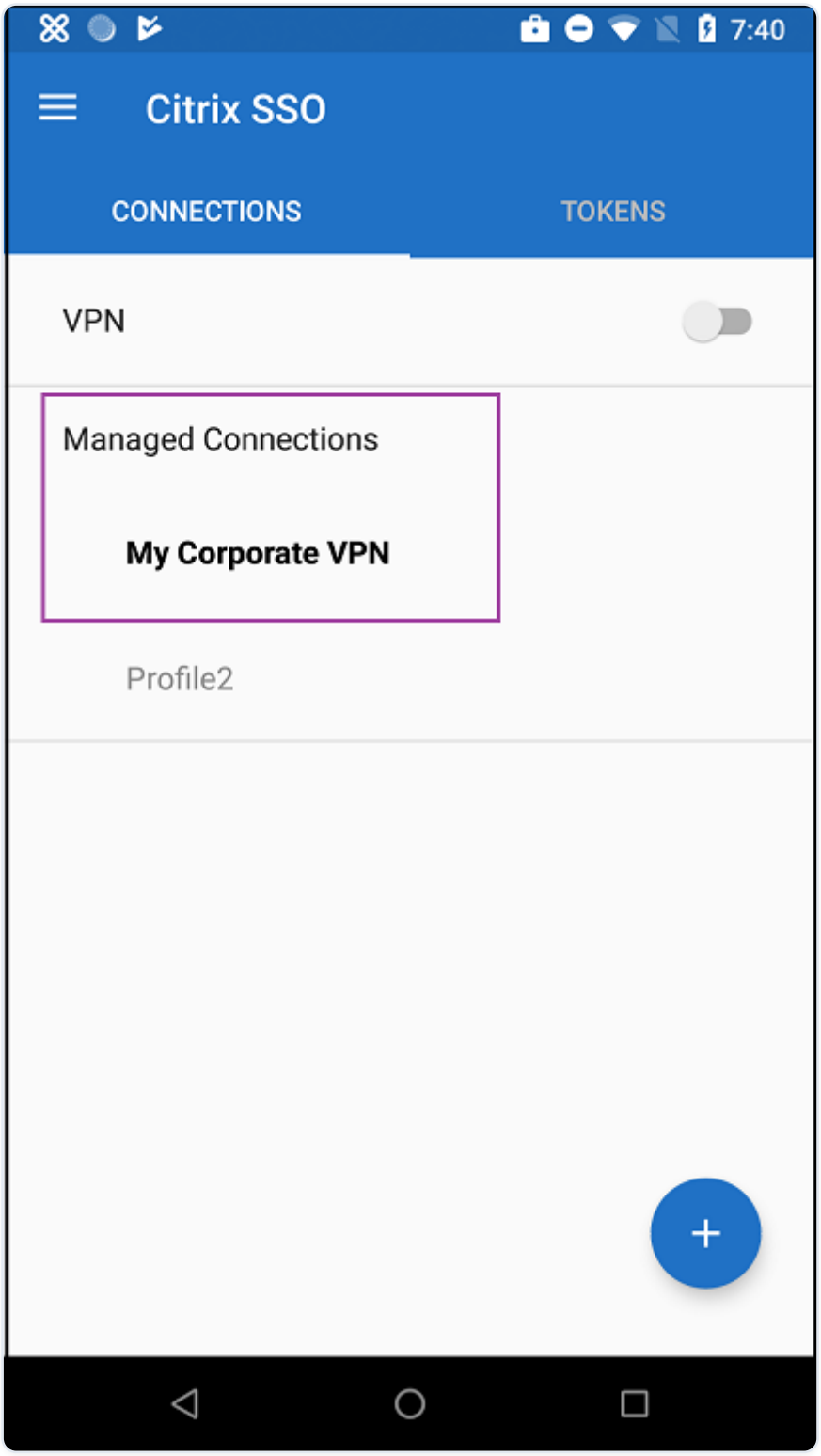
구성한 VPN 프로필에 대해 항상 켜짐을 활성화하려면 XenMobile 옵션 장치 정책을 설정합니다.

> **참고:** Android Enterprise의 항상 켜짐 VPN에는 Citrix Secure Hub 19.5.5 이상이 필요합니다.

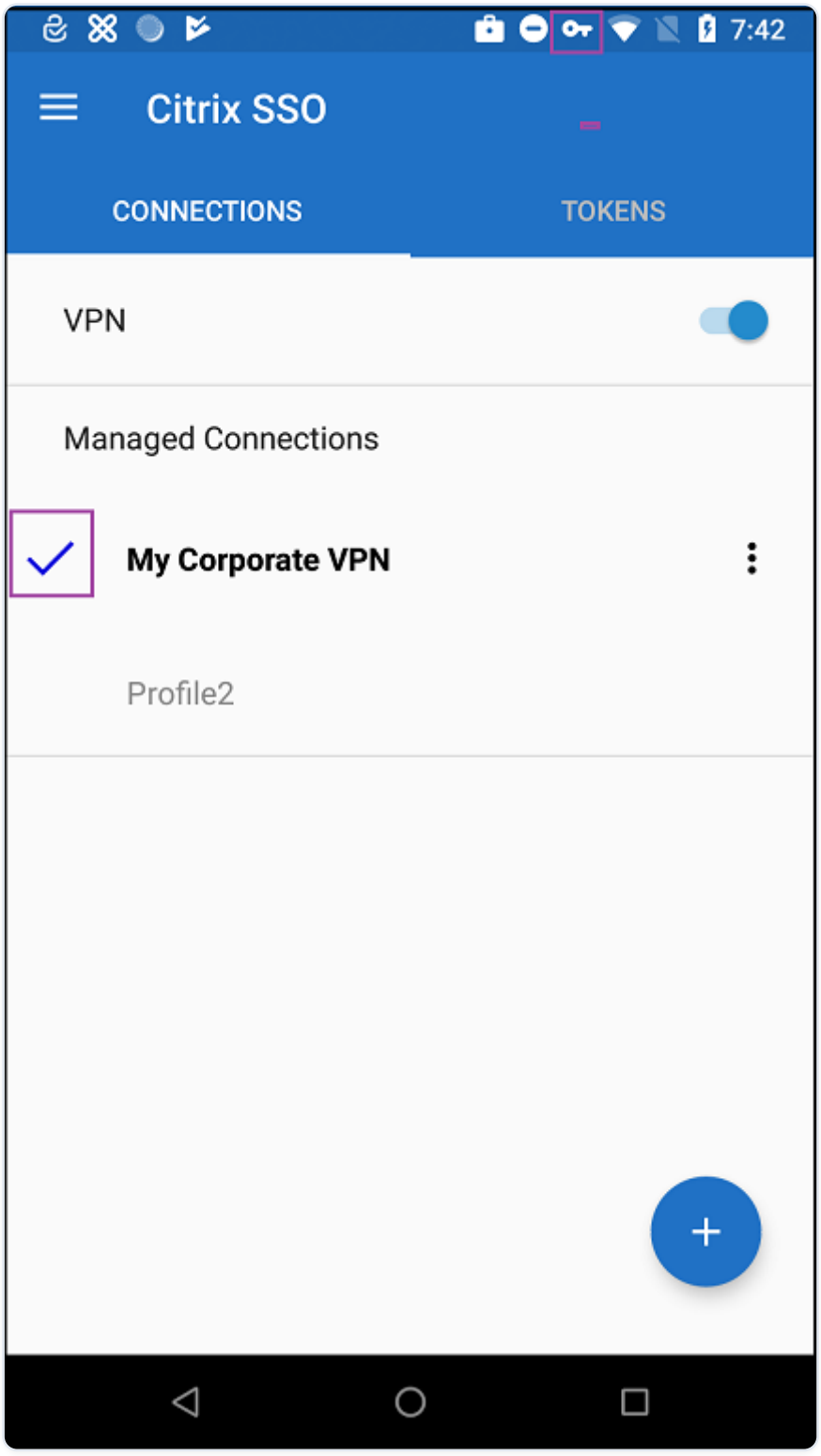
장치에서 VPN 프로필 액세스

생성한 VPN 프로필에 액세스하려면 Android Enterprise 사용자는 Google Play 스토어에서 Citrix SSO를 설치합니다.

구성한 VPN 프로필은 앱의 **관리되는 연결** 영역에 나타납니다. 사용자는 해당 VPN 프로필을 사용하여 연결하기 위해 VPN 프로필을 탭합니다.



사용자가 인증하고 연결하면 VPN 프로필 옆에 확인 표시가 나타납니다. 키 아이콘은 VPN이 연결되었음을 나타냅니다.



Zebra OEMConfig를 사용하여 Zebra Android 장치 관리

Zebra Technologies OEMConfig 관리 도구를 사용하여 Zebra Android 장치를 관리합니다. Zebra OEMConfig 앱에 대한 자세한 내용은 Zebra Technologies 웹사이트를 참조하십시오.

XenMobile은 Zebra OEMConfig 버전 9.2 이상을 지원합니다. 장치에 Zebra OEMConfig를 설치하기 위한 시스템 요구 사항에 대한 자세한 내용은 Zebra Technologies 웹 사이트의 OEMConfig 설정을 참조하십시오.

먼저 Zebra OEMConfig 앱을 Google Play 스토어 앱으로 XenMobile 콘솔에 추가합니다. 공개 앱 스토어 앱 추가를 참조하십시오.

Zebra OEMConfig 앱용 Android Enterprise 관리형 구성 생성

Zebra OEMConfig 앱에 대한 관리형 구성 장치 정책을 구성합니다. 이 정책은 Zebra OEMConfig 앱이 설치되고 정책이 배포된 Zebra 장치에 적용됩니다.

1. XenMobile 콘솔에서 **구성 > 장치 정책**을 클릭합니다. **추가**를 클릭합니다.
2. **Android Enterprise**를 선택합니다. **관리형 구성**을 클릭합니다.



3. **애플리케이션 ID 선택** 창이 나타나면 목록에서 **ZebraOEMConfig powered by MX**를 선택하고 **확인**을 클릭합니다.
4. Zebra OEMConfig 구성의 이름과 설명을 입력합니다. **다음**을 클릭합니다.
5. Zebra OEMConfig 구성의 이름을 입력합니다.
6. 사용 가능한 매개 변수를 구성합니다. 예를 들면 다음과 같습니다.
   - 장치 전면의 카메라를 비활성화하려면 **카메라 구성**을 선택하고 **전면 카메라 사용**을 **끔**으로 설정합니다.
   - 장치 시간 형식을 변경하려면 **시계 구성**을 선택하고 **시간 형식**을 12시간 형식의 경우 **12**로, 24시간 형식의 경우 **24**로 설정합니다.

사용 가능한 모든 구성 목록 및 설명은 Zebra Technologies 웹 사이트의 Zebra 관리형 구성을 참조하십시오.

1. 선택적으로 Zebra OEMConfig 구성을 더 만듭니다. 구성 목록 아래에서 **추가**를 클릭합니다. 새 구성이 목록에 나타납니다. 새 구성을 선택하고 매개 변수를 구성합니다.
2. 원하는 모든 Zebra OEMConfig 구성을 생성했으면 **다음**을 클릭합니다.
3. Zebra OEMConfig용 관리 구성에 대한 배포 규칙을 구성합니다.
4. **저장**을 클릭합니다.

관리되는 도메인 장치 정책

이메일 및 Safari 브라우저에 적용되는 관리되는 도메인을 정의할 수 있습니다. 관리되는 도메인은 Safari를 사용하여 도메인에서 다운로드한 문서를 열 수 있는 앱을 제어하여 회사 데이터를 보호하는 데 도움이 됩니다 .

iOS 8 이상 감독 모드 장치의 경우, 사용자가 브라우저에서 문서, 첨부 파일 및 다운로드를 여는 방법을 제어하기 위해 URL 또는 하위 도메인을 지정합니다. iOS 9.3 이상 감독 모드 장치의 경우, 사용자가 Safari에 암호를 저장할 수 있는 URL을 지정할 수 있습니다.

iOS 장치를 감독 모드로 설정하는 단계는 Apple Configurator를 사용하여 iOS 장치를 감독 모드로 전환하는 방법을 참조하십시오.

사용자가 관리되는 이메일 도메인 목록에 없는 도메인의 수신자에게 이메일을 보내면, 해당 메시지는 사용자의 장치에 플래그가 지정되어 회사 도메인 외부의 사람에게 메시지를 보내고 있음을 경고합니다.

문서, 첨부 파일 또는 다운로드와 같은 항목의 경우: 사용자가 관리되는 웹 도메인 목록에 있는 웹 도메인에서 Safari를 사용하여 항목을 열면, 적절한 회사 앱이 해당 항목을 엽니다. 항목이 관리되는 웹 도메인 목록에 있는 웹 도메인에서 온 것이 아니면, 사용자는 회사 앱으로 해당 항목을 열 수 없습니다. 개인용, 관리되지 않는 앱을 사용해야 합니다.

감독 모드 장치의 경우, Safari 암호 자동 완성 도메인을 지정하지 않더라도: 장치가 임시 다중 사용자(ephemeral multi-user)로 구성된 경우 사용자는 암호를 저장할 수 없습니다. 그러나 장치가 임시 다중 사용자(ephemeral multi-user)로 구성되지 않은 경우 사용자는 모든 암호를 저장할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

도메인을 지정하려면:

형식	설명
`example.com`	`example.com` 아래의 모든 경로는 관리되는 것으로 처리되지만, `site.example.com/`는 관리되지 않습니다.
`foo.example.com`	`foo.example.com` 아래의 모든 경로는 관리되지만, `example.com/` 또는 `bar.example.com/`는 관리되지 않습니다.

형식	설명
`*.example.com`	`foo.example.com` 또는 `bar.example.com` 아래의 모든 경로는 관리되지만, `example.com/` 는 관리되지 않습니다.
`example.com/sub`	`example.com/sub` 및 그 아래의 모든 경로는 관리되지만, `example.com/` 는 관리되지 않습니다.
`foo.example.com/sub`	`foo.example.com/sub` 아래의 모든 경로는 관리되지만, `example.com` , `example.com/sub` , `foo.example.com/` 또는 `bar.example.com/sub` 는 관리되지 않습니다.
`*.example.com/sub`	`foo.example.com/sub` 또는 `bar.example.com/sub` 아래의 모든 경로는 관리되지만, `example.com` 또는 `foo.example.com/` 는 관리되지 않습니다.

규칙:

- 도메인을 비교할 때 URL의 선행 "www." 및 후행 슬래시는 무시됩니다.
- 항목에 포트 번호가 있는 경우, 해당 포트 번호를 지정하는 주소만 관리되는 것으로 간주됩니다. 그렇지 않으면 표준 포트만 관리되는 것으로 간주됩니다(http의 경우 포트 80, https의 경우 포트 443). 예를 들어, 패턴 `*.example.com:8080` 은 `https://site.example.com:8080/page.html` 와 일치하지만 `https://site.example.com/page.html` 와는 일치하지 않으며, 패턴 `*.example.com` 는 `https://site.example.com/page.html` 및 `https://site.example.com/page.html` 와 일치하지만 `https://site.example.com:8080/page.html` 와는 일치하지 않습니다.
- 관리되는 Safari 웹 도메인 정의는 누적됩니다. 모든 관리되는 Safari 웹 도메인 페이로드에 의해 정의된 패턴은 URL 요청과 일치하는 데 사용됩니다.

설정:

- **관리되는 도메인**
  - **표시되지 않은 이메일 도메인:** 목록에 포함할 각 이메일 도메인에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
    - **관리되는 이메일 도메인:** 이메일 도메인을 입력합니다.
    - 이메일 도메인을 저장하려면 **저장**을 클릭하거나 이메일 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

- **관리되는 Safari 웹 도메인:** 목록에 포함할 각 웹 도메인에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **관리되는 웹 도메인:** 웹 도메인을 입력합니다.
  - 웹 도메인을 저장하려면 **저장**을 클릭하거나 웹 도메인을 저장하지 않으려면 **취소**를 클릭합니다.
- **Safari 암호 자동 완성 도메인:** 목록에 포함할 각 자동 완성 도메인에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **Safari 암호 자동 완성 도메인:** 자동 완성 도메인을 입력합니다.
  - 자동 완성 도메인을 저장하려면 **저장**을 클릭하거나 자동 완성 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

- **정책 설정**
  - **정책 제거:** 정책 제거를 예약할 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간(단위: 시간)을 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

최대 상주 사용자 장치 정책

최대 상주 사용자 장치 정책은 iOS(iPadOS)를 실행하는 공유 장치용입니다. 공유 iPad에 대한 자세한 내용은 Apple 교육 기능과 통합을 참조하십시오.

이 정책은 설정 지원 중 iPad가 "구성 대기 중" 단계에 있을 때 배포되어야 합니다. Apple은 공유 iPad가 등록된 후에는 이 정책을 배포하는 것을 허용하지 않습니다.

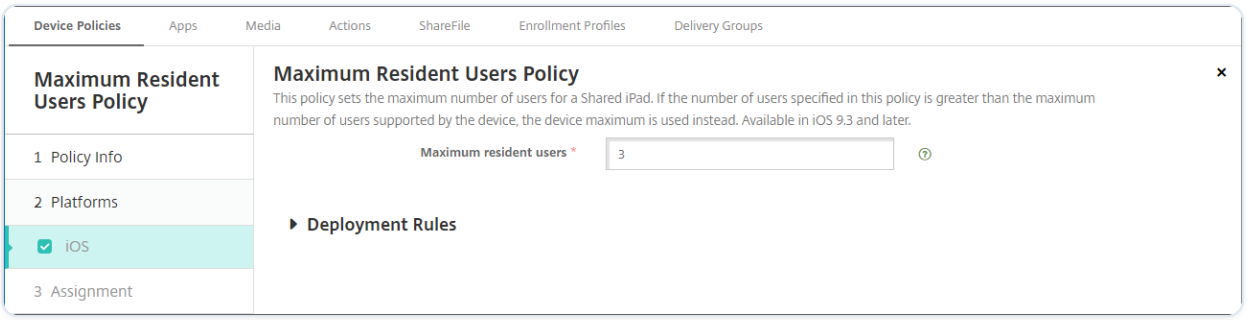
이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **최대 상주 사용자 수:** 공유 iPad의 최대 사용자 수입니다. 이 정책에 지정된 사용자 수가 장치에서 지원하는 최대 사용자 수보다 많은 경우: Citrix Endpoint Management는 대신 장치 최대값을 사용합니다. 기본값은 **5**명입니다.

  Apple은 최대 상주 사용자 값을 가능한 한 낮게 유지할 것을 권장합니다. 낮은 값은 각 사용자를 위한 iPad 저장 공간의 양을 최대화합니다. 또한 낮은 값은 iCloud와의 통신을 최소화하고 더 빠른 로그인 환경

을 제공합니다. Apple이 iPad에서 공유 저장 공간을 처리하는 방법에 대한 자세한 내용은 `<https://developer.apple.com/education/shared-ipad/>`을 참조하십시오.



MDM 옵션 장치 정책

XenMobile에서 장치 정책을 생성하여 감독되는 iOS 7.0 이상 전화 장치에서 나의 iPhone/iPad 찾기 활성화 잠금을 관리할 수 있습니다. iOS 장치를 감독 모드로 설정하는 단계는 Apple Configurator를 사용하여 iOS 장치를 감독 모드로 전환하는 방법을 참조하십시오.

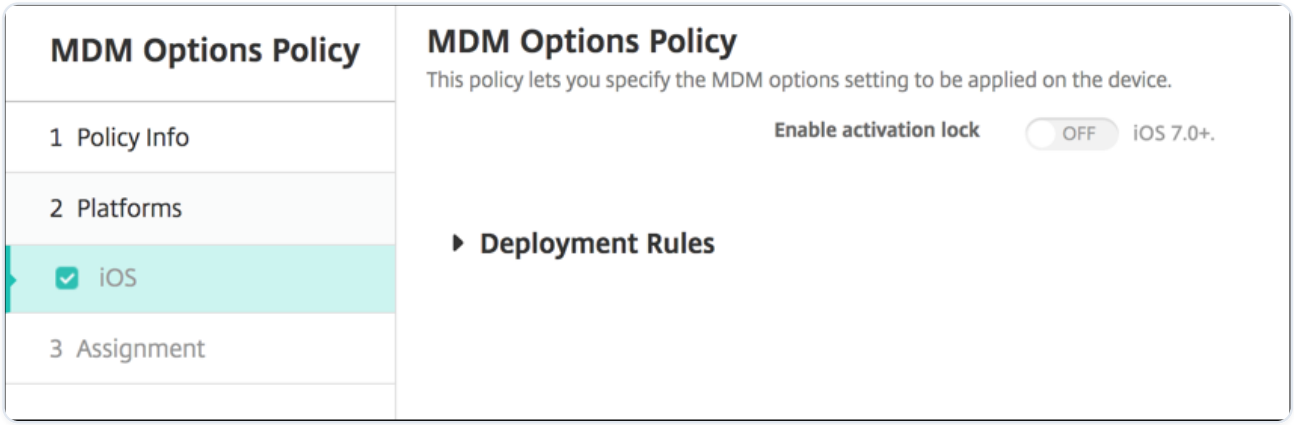
활성화 잠금은 분실되거나 도난당한 감독 장치의 재활성화를 방지하는 나의 iPhone/iPad 찾기 기능입니다. 활성화 잠금은 누군가 나의 iPhone/iPad 찾기를 끄거나, 장치를 지우거나, 장치를 재활성화하기 전에 사용자 Apple ID와 암호를 요구합니다. 조직이 소유한 장치의 경우, 예를 들어 장치를 재설정하거나 재할당하려면 활성화 잠금을 우회해야 합니다.

활성화 잠금을 활성화하려면 XenMobile® MDM 옵션 장치 정책을 구성하고 배포합니다. 그러면 사용자의 Apple 자격 증명 없이 XenMobile 콘솔에서 장치를 관리할 수 있습니다. 활성화 잠금의 Apple 자격 증명 요구 사항을 우회하려면 XenMobile 콘솔에서 활성화 잠금 우회 보안 작업을 실행하십시오.

예를 들어, 사용자가 분실한 전화를 반환하거나 전체 초기화 전후에 장치를 설정하는 경우: 전화에서 iTunes 계정 자격 증명을 요청할 때 XenMobile 콘솔에서 활성화 잠금 우회 보안 작업을 실행하여 해당 단계를 우회할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



- **활성화 잠금 활성화:** 이 정책을 배포할 장치에서 활성화 잠금을 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다.

MDM 옵션 장치 정책을 배포하여 활성화 잠금을 활성화한 후: **관리 > 장치** 페이지에서 해당 장치를 선택하고 **보안**을 클릭하면 보안 작업 **활성화 잠금 우회**가 나타납니다. 활성화 잠금 우회를 통해 장치 사용자의 Apple ID와 암호를 알지 못해도 장치 활성화 전에 감독되는 장치에서 활성화 잠금을 제거할 수 있습니다. 전체 초기화 전후에 장치로 활성화 잠금 우회를 보낼 수 있습니다. 자세한 내용은 보안 작업 문서의 iOS 활성화 잠금 우회를 참조하십시오.

조직 정보 장치 정책

XenMobile®에서 장치 정책을 추가하여 XenMobile에서 iOS 장치로 푸시되는 경고 메시지에 대한 조직 정보를 지정할 수 있습니다. 이 정책은 iOS 7 이상 장치에서 사용할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

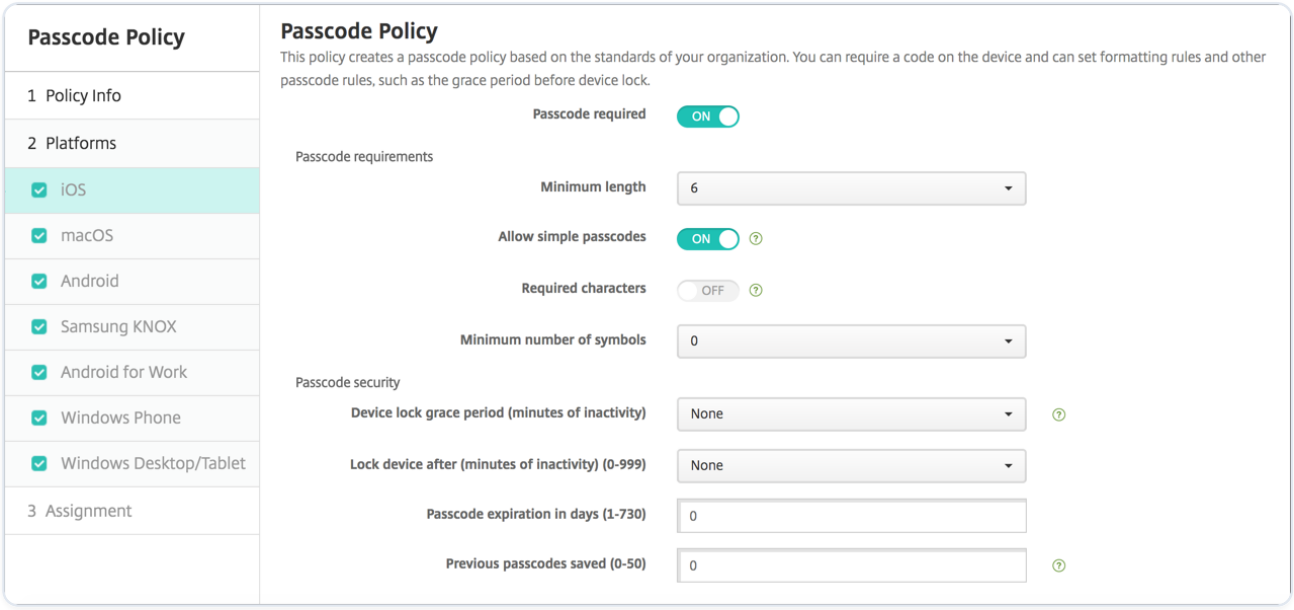
- **이름:** XenMobile을 실행하는 조직의 이름을 입력합니다.
- **주소:** 조직의 주소를 입력합니다.
- **전화:** 조직의 지원 전화번호를 입력합니다.
- **이메일:** 지원 이메일 주소를 입력합니다.
- **매직:** 조직에서 관리하는 서비스를 설명하는 단어 또는 문구를 입력합니다.

암호 장치 정책

조직의 표준에 따라 XenMobile에서 암호 정책을 만듭니다. 사용자의 장치에 암호를 요구하고 다양한 형식 및 암호 규칙을 설정할 수 있습니다. iOS, macOS, Android, Samsung Knox, Android Enterprise 및 Windows 데스크톱/태블릿용 정책을 만들 수 있습니다. 각 플랫폼에는 이 문서에 설명된 대로 다른 값 집합이 필요합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



- **암호 필요:** 암호를 요구하고 iOS 암호 장치 정책에 대한 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안 및 정책 설정에 대한 설정을 구성할 수 있습니다.
- **암호 요구 사항**
  - **최소 길이:** 드롭다운 목록에서 최소 암호 길이를 클릭합니다. 기본값은 **6**입니다.
  - **간단한 암호 허용:** 간단한 암호를 허용할지 여부를 선택합니다. 간단한 암호는 반복되거나 순차적인 문자 집합입니다. 기본값은 **켜짐**입니다.
  - **필수 문자:** 암호에 하나 이상의 문자가 포함되어야 하는지 여부를 선택합니다. 기본값은 **꺼짐**입니다.
  - **최소 기호 수:** 목록에서 암호에 포함되어야 하는 기호 수를 클릭합니다. 기본값은 **0**입니다.
- **암호 보안**
  - **장치 잠금 유예 기간(비활성 시간(분)):** 목록에서 사용자가 잠긴 장치의 잠금을 해제하기 위해 암호를 입력해야 하는 시간 길이를 클릭합니다. 기본값은 **없음**입니다.

- **다음 시간(비활성 시간(분)) 후 장치 잠금:** 목록에서 장치가 잠기기 전에 비활성 상태일 수 있는 시간 길이를 클릭합니다. 기본값은 없음입니다.
- **암호 만료일(1-730일):** 암호가 만료되는 일수를 입력합니다. 유효한 값은 1-730입니다. 기본값은 **0**이며, 이는 암호가 만료되지 않음을 의미합니다.
- **저장된 이전 암호(0-50):** 저장할 사용된 암호의 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0-50입니다. 기본값은 **0**이며, 이는 사용자가 암호를 재사용할 수 있음을 의미합니다.
- **최대 로그인 실패 시도 횟수:** 목록에서 사용자가 로그인에 성공하지 못하여 장치가 완전히 초기화되기 전까지 허용되는 실패 횟수를 클릭합니다. 기본값은 **정의되지 않음**입니다.

macOS 설정

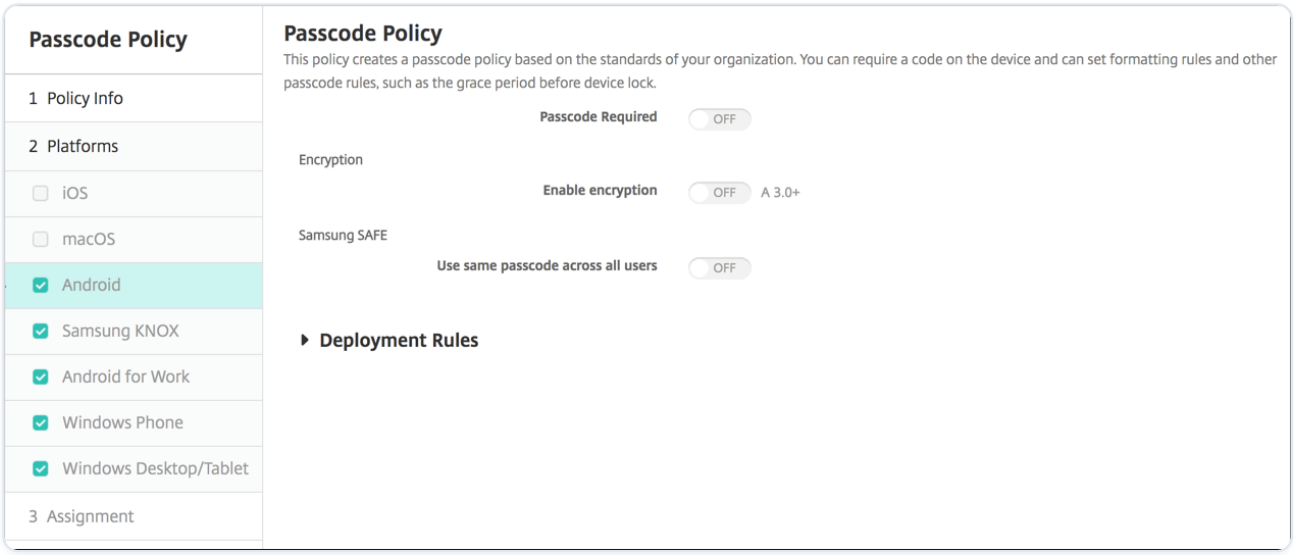
장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policy-passcode-macos.png)

- **암호 필요:** 암호를 요구하고 iOS 암호 장치 정책에 대한 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안 및 정책 설정에 대한 설정을 구성할 수 있습니다.
- **암호 필요**를 사용하도록 설정하지 않은 경우, **로그인 실패 시도 후 지연 시간(분)** 옆에 사용자가 암호를 다시 입력할 수 있도록 허용하기 전에 지연할 시간(분)을 입력합니다.
- **암호 필요**를 사용하도록 설정한 경우 다음 설정을 구성합니다.
- **암호 요구 사항**
  - **최소 길이:** 목록에서 최소 암호 길이를 클릭합니다. 기본값은 **6**입니다.
  - **간단한 암호 허용:** 간단한 암호를 허용할지 여부를 선택합니다. 간단한 암호는 반복되거나 순차적인 문자 집합입니다. 기본값은 **켜짐**입니다.
  - **필수 문자:** 암호에 최소 하나의 문자가 포함되어야 하는지 여부를 선택합니다. 기본값은 **꺼짐**입니다.
  - **최소 기호 수:** 목록에서 암호에 포함되어야 하는 기호 수를 클릭합니다. 기본값은 **0**입니다.
- **암호 보안**
  - **장치 잠금 유예 기간(비활성 시간(분)):** 목록에서 사용자가 잠긴 장치의 잠금을 해제하기 위해 암호를 입력해야 하는 시간 길이를 클릭합니다. 기본값은 **없음**입니다.
  - **다음 시간 후 장치 잠금(비활성 시간(분)):** 목록에서 장치가 잠기기 전까지 비활성 상태일 수 있는 시간 길이를 클릭합니다. 기본값은 **없음**입니다.
  - **암호 만료일(1-730):** 암호가 만료되는 일수를 입력합니다. 유효한 값은 1-730입니다. 기본값은 **0**이며, 이는 암호가 만료되지 않음을 의미합니다.

- **저장된 이전 암호(0-50):** 저장할 사용된 암호의 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0-50입니다. 기본값은 **0**이며, 이는 사용자가 암호를 재사용할 수 있음을 의미합니다.
- **최대 로그인 실패 시도 횟수:** 목록에서 사용자가 로그인에 성공하지 못하고 장치가 잠기기 전까지 시도할 수 있는 횟수를 클릭합니다. 기본값은 **정의되지 않음**입니다.
- **로그인 실패 시도 후 지연 시간(분):** 사용자가 암호를 다시 입력하기 전에 지연할 시간(분)을 입력합니다.
- **암호 재설정 강제 적용:** 사용자가 다음에 인증할 때 암호를 재설정해야 합니다.

- **정책 설정**
  - **프로필 범위:** 이 정책을 **사용자**에게 적용할지 또는 전체 **시스템**에 적용할지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Android 설정



> **참고:**
>
> Android의 기본 설정은 **해제**입니다.

- **암호 필요:** 암호를 요구하고 Android 암호 장치 정책에 대한 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안, 암호화 및 Samsung SAFE에 대한 설정을 구성할 수 있습니다.
- **암호 요구 사항**
  - **최소 길이:** 드롭다운 목록에서 최소 암호 길이를 선택합니다. 기본값은 6입니다.

- **생체 인식:** 생체 인식을 활성화할지 여부를 선택합니다. 이 옵션을 활성화하면 필수 문자 필드가 숨겨집니다. 기본값은 **해제**입니다.
- **필수 문자:** 드롭다운 목록에서 **제한 없음**, **숫자 및 문자 모두**, **숫자만**, 또는 **문자만**을 선택하여 암호 구성 방법을 설정합니다. 기본값은 제한 없음입니다.
- **고급 규칙:** 고급 암호 규칙을 적용할지 여부를 선택합니다. 이 옵션은 Android 3.0 이상에서 사용할 수 있습니다. 기본값은 **해제**입니다.
- **고급 규칙**을 활성화하면 다음 각 목록에서 암호에 포함되어야 하는 각 문자 유형의 최소 개수를 클릭합니다.
  - **기호:** 최소 기호 개수.
  - **문자:** 최소 문자 개수.
  - **소문자:** 최소 소문자 개수.
  - **대문자:** 최소 대문자 개수.
  - **숫자 또는 기호:** 최소 숫자 또는 기호 개수.
  - **숫자:** 최소 숫자 개수.

- **암호 보안**
  - **비활성 상태 (분) 후 장치 잠금:** 목록에서 장치가 잠기기 전까지 비활성 상태로 있을 수 있는 시간을 클릭합니다. 기본값은 **없음**입니다.
  - **암호 만료일 (1-730):** 암호가 만료되는 일수를 입력합니다. 유효한 값은 1-730입니다. 기본값은 **0**이며, 이는 암호가 만료되지 않음을 의미합니다.
  - **저장된 이전 암호 (0-50):** 저장할 사용된 암호의 개수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0-50입니다. 기본값은 **0**이며, 이는 사용자가 암호를 재사용할 수 있음을 의미합니다.
  - **최대 로그인 실패 시도 횟수:** 목록에서 사용자가 성공적으로 로그인하지 못하여 장치가 초기화되기 전까지의 시도 횟수를 클릭합니다. 기본값은 **정의되지 않음**입니다.

- **암호화**
  - **암호화 사용:** 암호화를 사용할지 여부를 선택합니다. 이 옵션은 Android 3.0 이상에서 사용할 수 있습니다. 이 옵션은 **암호 필요** 설정과 관계없이 사용할 수 있습니다.

    장치를 암호화하려면 사용자는 배터리를 충전한 상태에서 시작해야 하며, 암호화에 걸리는 한 시간 이상 동안 장치를 연결된 상태로 유지해야 합니다. 암호화 프로세스를 중단하면 장치의 데이터 일부 또는 전부를 잃을 수 있습니다. 장치가 암호화된 후에는 공장 초기화를 수행하여 장치의 모든 데이터를 지우는 경우를 제외하고는 프로세스를 되돌릴 수 없습니다.

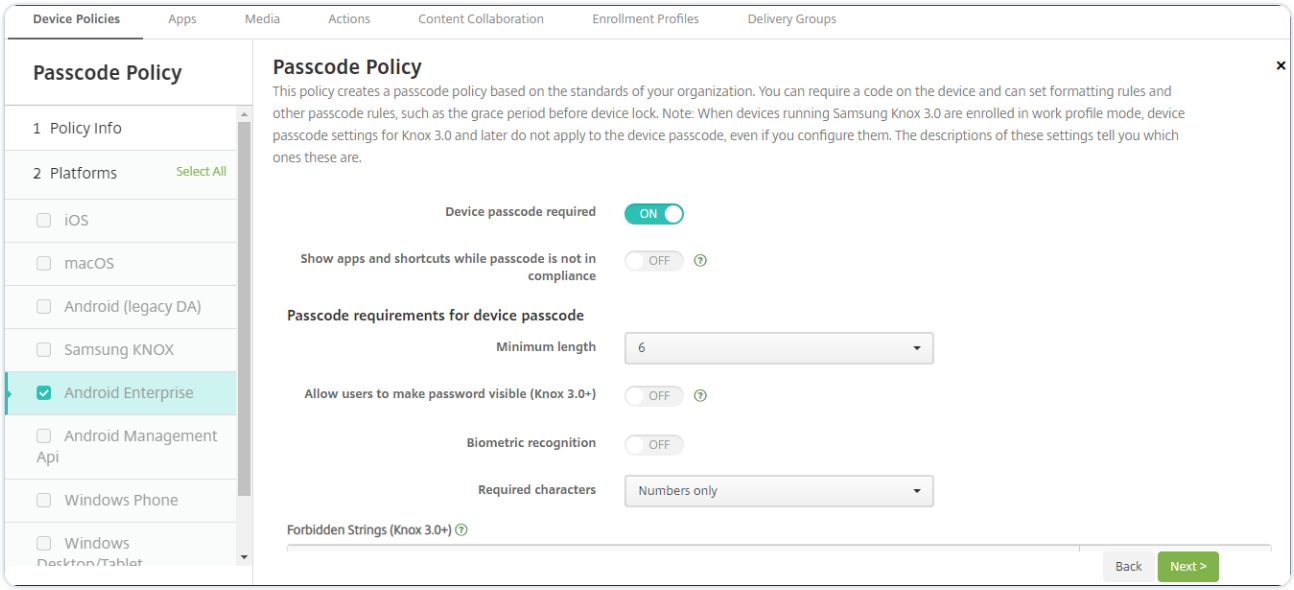
- **삼성 세이프**

> **참고:**
>
> Samsung SAFE 장치에서 얼굴 또는 홍채 인식을 비활성화하기 위한 해결 방법: Samsung SAFE에 대한 제한 장치 정책을 생성합니다. 제한 정책에서 **응용 프로그램 비활성화**를 켜고 `com.samsung.android.bio.face.service` 또는 `com.samsung.android.server.iris`를 테이블에 추가합니다. 그런 다음 제한 정책을 배포합니다.

  - **모든 사용자에게 동일한 암호 사용:** 모든 사용자에게 동일한 암호를 사용할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 설정은 Samsung SAFE 장치에만 적용되며 **암호 필요** 설정과 관계없이 사용할 수 있습니다.
  - **모든 사용자에게 동일한 암호 사용**을 활성화하면 **암호** 필드에 모든 사용자가 사용할 암호를 입력합니다.
  - **암호 필요**를 활성화하면 다음 Samsung SAFE 설정을 구성합니다.
    - **변경해야 하는 문자 수:** 사용자가 이전 암호에서 변경해야 하는 문자 수를 입력합니다. 기본값은 **0**입니다.
    - **문자가 나타날 수 있는 횟수:** 암호에 문자가 나타날 수 있는 최대 횟수를 입력합니다. 기본값은 **0**입니다.
    - **알파벳 순서 길이:** 암호에서 알파벳 순서의 최대 길이를 입력합니다. 기본값은 **0**입니다.
    - **숫자 순서 길이:** 암호에서 숫자 순서의 최대 길이를 입력합니다. 기본값은 **0**입니다.
    - **사용자가 암호를 표시하도록 허용:** 사용자가 암호를 표시할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
    - **생체 인증 구성**. 생체 인증을 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. **켜짐**으로 설정하면 다음 옵션을 설정할 수 있습니다.
      - **지문 허용**. 사용자가 지문을 사용하여 인증하도록 허용하려면 선택합니다.
      - **홍채 허용**. 사용자가 홍채를 사용하여 인증하도록 허용하려면 선택합니다.
    - **금지된 문자열:** 사용자가 "password", "pwd", "welcome", "123456", "111111"과 같이 추측하기 쉬운 안전하지 않은 문자열을 사용하지 못하도록 금지된 문자열을 만듭니다. 거부하려는 각 문자열에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
      - **금지된 문자열:** 사용자가 사용하지 않을 수 있는 문자열을 입력합니다.

- 문자열을 추가하려면 **저장**을 클릭하고, 문자열 추가를 취소하려면 **취소**를 클릭합니다.

안드로이드 엔터프라이즈 설정



Android Enterprise 장치의 경우 장치에 대한 암호 또는 Android Enterprise 업무 프로필에 대한 보안 챌린지 또는 둘 다를 요구할 수 있습니다.

Android 9.0 이상 및 Samsung Knox 3.0 이상을 실행하는 장치의 경우 **Android Enterprise** 페이지에서 Samsung Knox 설정을 구성합니다. 이전 버전의 Android 또는 Samsung Knox를 실행하는 장치의 경우 **Samsung Knox** 페이지를 사용합니다.

> **참고:**
>
> Samsung Knox 3.0을 실행하는 장치가 업무 프로필 장치로 등록된 경우, Knox 3.0 이상에 대한 장치 암호 설정은 구성하더라도 장치 암호에 적용되지 않습니다.

- **장치 암호 필요:** 장치에 암호를 요구합니다. 이 설정이 **켜짐**인 경우, **장치 암호 요구 사항** 및 **장치 암호 보안** 아래의 설정을 구성합니다. 기본값은 **꺼짐**입니다.
- **암호가 규정을 준수하지 않을 때 앱 및 바로 가기 표시:** 이 설정이 **켜짐**인 경우, 암호가 규정을 준수하지 않더라도 장치의 앱 및 바로 가기가 숨겨지지 않습니다. 이 설정이 **꺼짐**인 경우, 암호가 규정을 준수하지 않을 때 앱 및 바로 가기가 숨겨집니다. 이 설정을 활성화하는 경우, Citrix®는 암호가 규정을 준수하지 않을 때 장치를 규정 미준수로 표시하는 자동화된 작업을 생성할 것을 권장합니다. 기본값은 **꺼짐**입니다.
- **장치 암호 요구 사항:**
  - **최소 길이:** 최소 암호 길이를 지정합니다. 기본값은 6입니다.

- **사용자가 암호를 표시하도록 허용:** 유효한 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치에 해당합니다. 완전 관리형 장치에만 해당합니다. 이 설정은 업무 프로필 장치로 등록된 장치에는 적용되지 않습니다. 사용자가 암호를 표시하도록 허용합니다. 기본값은 **꺼짐**입니다.
- **생체 인식:** 생체 인식을 활성화합니다. 이 설정이 **켜짐**이면 **필수 문자** 필드가 숨겨집니다. 기본값은 **꺼짐**입니다.
- **필수 문자:** 암호에 필요한 문자 유형을 지정합니다. 목록에서 **제한 없음**, **숫자 및 문자 모두**, **숫자만** 또는 **문자만**을 선택합니다. Android 7.0을 실행하는 장치에만 **제한 없음**을 사용하십시오. Android 7.1 이상에서는 **제한 없음** 설정이 적용되지 않습니다. 기본값은 **숫자 및 문자 모두**입니다.
- **금지된 문자열:** 유효한 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치용입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로필 장치로 등록된 장치에는 적용되지 않습니다. 사용자가 암호로 사용할 수 없는 문자열을 지정합니다. "password", "pwd", "welcome", "123456", "111111"과 같이 추측하기 쉬운 안전하지 않은 문자열을 사용자가 사용하지 못하도록 금지된 문자열을 만듭니다. 거부하려는 각 문자열에 대해: **추가**를 클릭합니다. 사용자가 사용하지 않으려는 문자열을 입력합니다. 문자열을 추가하려면 **저장**을 클릭하고, 문자열 추가를 취소하려면 **취소**를 클릭합니다.
- **고급 규칙:** 암호에 포함될 수 있는 문자 유형에 대한 고급 규칙을 적용합니다. 이 설정이 **켜짐**이면 **최소 개수** 및 **최대 개수** 아래의 설정을 구성합니다. 이 설정은 Android 5.0 이전 Android 장치에서는 사용할 수 없습니다. 기본값은 **꺼짐**입니다.
- **최소 개수:**
  - **기호:** 최소 기호 개수를 지정합니다. 기본값은 **0**입니다.
  - **문자:** 최소 문자 개수를 지정합니다. 기본값은 **0**입니다.
  - **소문자:** 최소 소문자 개수를 지정합니다. 기본값은 **0**입니다.
  - **대문자:** 최소 대문자 개수를 지정합니다. 기본값은 **0**입니다.
  - **숫자 또는 기호:** 최소 숫자 또는 기호 개수를 지정합니다. 기본값은 **0**입니다.
  - **숫자:** 최소 숫자 개수를 지정합니다. 기본값은 **0**입니다.
  - **변경 문자:** 유효한 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치용입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로필 장치로 등록된 장치에는 적용되지 않습니다. 사용자가 이전 암호에서 변경해야 하는 문자 수를 지정합니다. 기본값은 **0**입니다.
- **최대 개수:** 유효한 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치용입니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로필 장치로 등록된 장치에는 적용되지 않습니다.
  - **문자 발생 횟수:** 암호에서 문자가 발생할 수 있는 최대 횟수를 지정합니다. 기본값은 **0**이며, 이는 최대 제한이 없음을 의미합니다.

  - **알파벳 순서 길이:** 암호에서 알파벳 순서의 최대 길이를 지정합니다. 기본값은 **0**이며, 이는 최대 제한이 없음을 의미합니다.
  - **숫자 시퀀스 길이:** 암호의 숫자 시퀀스 최대 길이를 지정합니다. 기본값은 **0**이며, 이는 최대 제한이 없음을 의미합니다.

- **장치 암호에 대한 암호 보안:**
  - **장치 초기화 (로그온 시도 실패 후):** 사용자가 로그온에 실패할 수 있는 횟수를 지정하며, 이 횟수를 초과하면 장치가 완전히 초기화됩니다. 기본값은 **정의되지 않음**입니다.
  - **장치 잠금 (비활성 시간(분) 후) (0-999):** 장치가 잠기기 전에 비활성 상태로 있을 수 있는 시간(분)을 지정합니다. 기본값은 **없음**입니다.
  - **암호 만료일 (일) (1-730):** 암호가 만료되는 일수를 지정합니다. 유효한 값은 1~730입니다. 기본값은 **0**이며, 이는 암호가 만료되지 않음을 의미합니다.
  - **저장된 이전 암호 (0-50):** 저장할 사용된 암호의 수를 지정합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0~50입니다. 기본값은 **0**이며, 이는 사용자가 암호를 재사용할 수 있음을 의미합니다.
  - **장치 잠금 (로그온 시도 실패 후)** 유효한 Knox 라이선스 키가 구성된 Samsung Knox 3.0 이상을 실행하는 장치에 적용됩니다. 완전 관리형 장치에만 해당됩니다. 이 설정은 작업 프로필 장치로 등록된 장치에는 적용되지 않습니다. 사용자가 로그온에 실패할 수 있는 횟수를 지정하며, 이 횟수를 초과하면 장치가 잠깁니다. 기본값은 **정의되지 않음**입니다.

- **작업 프로필 보안 챌린지:** Android Enterprise 작업 프로필에서 실행되는 앱에 액세스하려면 사용자가 보안 챌린지를 완료하도록 요구합니다. Android 7.0 이상을 실행하는 장치에 적용됩니다. 이 설정이 **켜짐**으로 되어 있으면, **작업 프로필 보안 챌린지 암호 요구 사항** 및 **작업 프로필 보안 챌린지 암호 보안** 아래의 설정을 구성합니다. 기본값은 **꺼짐**입니다.
- **작업 프로필 보안 챌린지 암호 요구 사항:**
  - **최소 길이:** 최소 암호 길이를 지정합니다. 기본값은 6입니다.
  - **사용자가 암호를 표시하도록 허용:** 유효한 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치에 적용됩니다. 사용자가 암호를 표시할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **생체 인식:** 생체 인식을 활성화합니다. 이 설정이 **켜짐**으로 되어 있으면, **필수 문자** 필드는 숨겨집니다. 기본값은 **꺼짐**입니다.
  - **필수 문자:** 암호에 필요한 문자 유형을 지정합니다. 목록에서 **제한 없음**, **숫자와 문자 모두**, **숫자만**, 또는 **문자만**을 선택합니다. **제한 없음**은 Android 7.0을 실행하는 장치에만 사용하십시오. Android 7.1 이상에서는 **제한 없음** 설정이 적용되지 않습니다. 기본값은 **숫자와 문자 모두**입니다.
  - **금지된 문자열:** 유효한 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치에 적용됩니다. 사용자가 암호로 사용할 수 없는 문자열을 지정합니다. "password", "pwd", "welcome", "123456",

"111111"과 같이 추측하기 쉬운 안전하지 않은 문자열을 사용자가 사용하지 못하도록 금지된 문자열을 만듭니다. 거부하려는 각 문자열에 대해: **추가**를 클릭합니다. 사용자가 사용하지 않기를 원하는 문자열을 입력합니다. 문자열을 추가하려면 **저장**을 클릭하고, 문자열 추가를 취소하려면 **취소**를 클릭합니다.

- **고급 규칙:** 암호에 포함될 수 있는 문자 유형에 대한 고급 규칙을 적용합니다. 이 설정이 **켜짐**으로 되어 있으면, **최소 개수** 및 **최대 개수** 아래의 설정을 구성합니다. 이 설정은 Android 5.0 이전 버전의 Android 장치에서는 사용할 수 없습니다. 기본값은 **꺼짐**입니다.
- **최소 개수:**
  - **기호:** 최소 기호 개수를 지정합니다. 기본값은 **0**입니다.
  - **문자:** 최소 문자 개수를 지정합니다. 기본값은 **0**입니다.
  - **소문자:** 최소 소문자 개수를 지정합니다. 기본값은 **0**입니다.
  - **대문자:** 최소 대문자 개수를 지정합니다. 기본값은 **0**입니다.
  - **숫자 또는 기호:** 최소 숫자 또는 기호 개수를 지정합니다. 기본값은 **0**입니다.
  - **숫자:** 최소 숫자 개수를 지정합니다. 기본값은 **0**입니다.
  - **변경된 문자:** Knox 3.0 이상을 실행하고 유효한 Knox 라이선스 키가 구성된 장치에 해당합니다. 사용자가 이전 암호에서 변경해야 하는 문자 수를 지정합니다. 기본값은 **0**입니다.
- **최대 개수:** Knox 3.0 이상을 실행하고 유효한 Knox 라이선스 키가 구성된 장치에 해당합니다.
  - **문자가 나타날 수 있는 횟수:** 암호에서 문자가 나타날 수 있는 최대 횟수를 지정합니다. 기본값은 **0**이며, 이는 최대 제한이 없음을 의미합니다.
  - **알파벳 순서 길이:** 암호에서 알파벳 순서의 최대 길이를 지정합니다. 기본값은 **0**이며, 이는 최대 제한이 없음을 의미합니다.
  - **숫자 순서 길이:** 암호에서 숫자 순서의 최대 길이를 지정합니다. 기본값은 **0**이며, 이는 최대 제한이 없음을 의미합니다.
- **통합 암호 사용: 켜짐**으로 설정하면 사용자는 장치 및 업무 프로필에 하나의 암호를 사용합니다. **꺼짐**으로 설정하면:
  - 사용자는 장치 및 업무 프로필에 다른 암호를 사용해야 합니다.
  - 사용자가 장치 및 업무 프로필에 하나의 암호를 사용하려는 경우 설정하는 장치의 **하나의 잠금 사용** 설정이 비활성화됩니다. 사용자는 이 설정을 활성화할 수 없습니다.
  - 작업 프로필 보안 챌린지에 대한 암호 요구 사항이 장치 암호보다 더 복잡한 경우: **하나의 잠금 사용** 설정이 활성화된 사용자는 작업 프로필 암호를 변경하라는 메시지가 표시됩니다.

기본값은 **해제**입니다. Android 9.0부터 사용할 수 있습니다.

- **작업 프로필 보안 챌린지를 위한 암호 보안**
  - **컨테이너 지우기 (로그온 시도 실패 후):** 사용자가 로그온에 실패할 수 있는 횟수를 지정하며, 이 횟수를 초과하면 작업 프로필과 해당 데이터가 장치에서 지워집니다. 지우기가 발생한 후 사용자는 작업 프로필을 다시 초기화해야 합니다. 기본값은 **정의되지 않음**입니다.
  - **컨테이너 잠금 (비활성 시간(분) 후):** 작업 프로필이 잠기기 전에 장치가 비활성 상태일 수 있는 시간(분)을 지정합니다. 기본값은 **없음**입니다.
  - **암호 만료일 (1-730일):** 암호가 만료되는 일수를 지정합니다. 유효 값은 1-730입니다. 기본값은 **0**이며, 이는 암호가 만료되지 않음을 의미합니다.
  - **저장된 이전 암호 (0-50개):** 저장할 사용된 암호의 수를 지정합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효 값은 0-50입니다. 기본값은 **0**이며, 이는 사용자가 암호를 재사용할 수 있음을 의미합니다.
  - **컨테이너 잠금 (로그온 시도 실패 후):** 유효한 Knox 라이선스 키가 구성된 Knox 3.0 이상을 실행하는 장치에 해당합니다. 사용자가 로그온에 실패할 수 있는 횟수를 지정하며, 이 횟수를 초과하면 장치가 잠깁니다. 기본값은 **정의되지 않음**입니다.

Windows 데스크톱/태블릿 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policy-passcode-windowsdesktop.png)

- **간편 로그온 허용 안 함:** 사용자가 그림 암호 또는 생체 인식 로그온으로 장치에 액세스할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **해제**입니다.
- **최소 암호 길이:** 드롭다운 목록에서 최소 암호 길이를 선택합니다. 기본값은 **6**입니다.
- **지우기 전 최대 암호 시도 횟수:** 목록에서 사용자가 로그온에 성공하지 못할 수 있는 횟수를 클릭합니다. 이 횟수를 초과하면 장치에서 회사 데이터가 지워집니다. 기본값은 **4**입니다.
- **암호 만료일 (0-730일):** 암호가 만료되는 일수를 입력합니다. 유효 값은 0-730입니다. 기본값은 **0**이며, 이는 암호가 만료되지 않음을 의미합니다.
- **암호 기록: (1-24):** 저장할 사용된 암호의 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효 값은 1-24입니다. 이 필드에는 1에서 24 사이의 숫자를 입력해야 합니다. 기본값은 **0**입니다.
- **장치 잠금 전 최대 비활성 시간(1-999분):** 장치가 잠기기 전에 비활성 상태일 수 있는 시간(분)을 입력합니다. 유효한 값은 1-999입니다. 이 필드에 1에서 999 사이의 숫자를 입력해야 합니다. 기본값은 **0**입니다.

개인용 핫스팟 장치 정책

사용자가 Wi-Fi 네트워크 범위 내에 없을 때 iOS 장치의 개인용 핫스팟 기능을 통해 셀룰러 데이터 연결을 사용하여 인터넷에 연결하도록 허용할 수 있습니다. iOS 7.0 이상에서 사용 가능합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

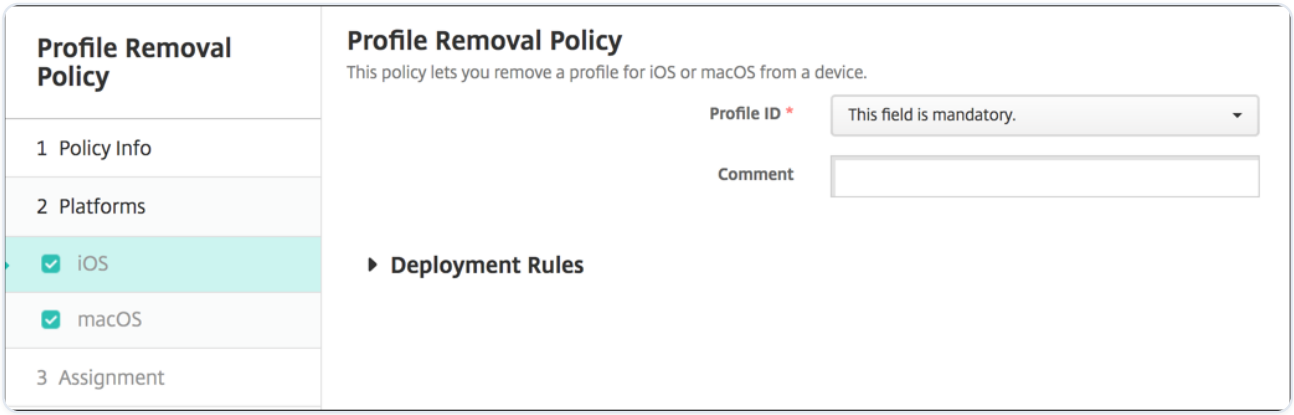
개인용 핫스팟 비활성화: 사용자 장치에서 개인용 핫스팟 기능을 비활성화할지 여부를 선택합니다. 기본값은 **끔**이며, 이는 사용자 장치에서 개인용 핫스팟을 끕니다. 이 정책은 기능을 비활성화하지 않습니다. 사용자는 여전히 장치에서 개인용 핫스팟을 사용할 수 있습니다. 그러나 정책이 배포되면 개인용 핫스팟은 기본적으로 켜져 있지 않도록 꺼집니다.

프로필 제거 장치 정책

XenMobile에서 앱 프로필 제거 장치 정책을 생성할 수 있습니다. 이 정책은 배포되면 사용자의 iOS 또는 macOS 장치에서 앱 프로필을 제거합니다.

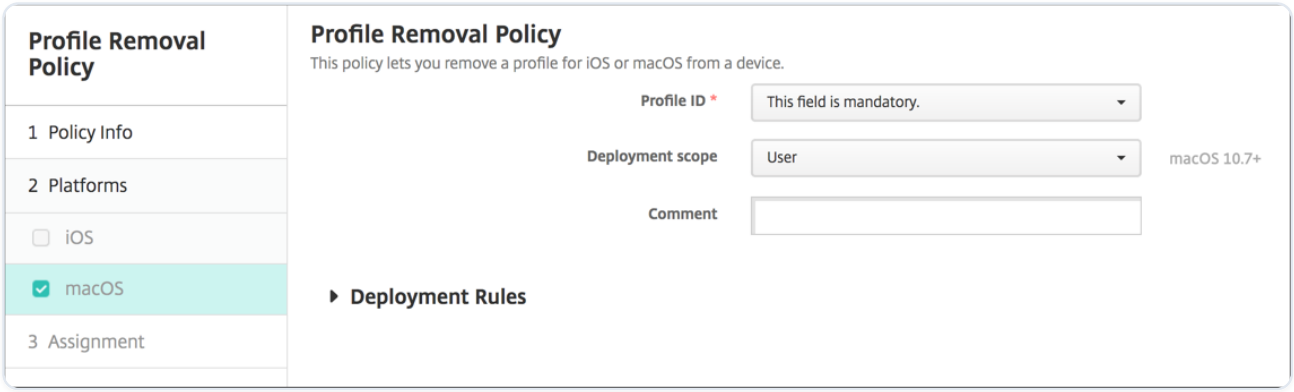
이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



- **프로필 ID:** 드롭다운 목록에서 앱 프로필 ID를 선택합니다. 이 필드는 필수입니다.
- **설명:** 선택 사항인 설명을 입력합니다.

macOS 설정



- **프로필 ID:** 드롭다운 목록에서 앱 프로필 ID를 선택합니다. 이 필드는 필수입니다.
- **배포 범위:** 드롭다운 목록에서 **사용자** 또는 **시스템**을 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.
- **설명:** 선택 사항인 설명을 입력합니다.

프로비저닝 프로필 장치 정책

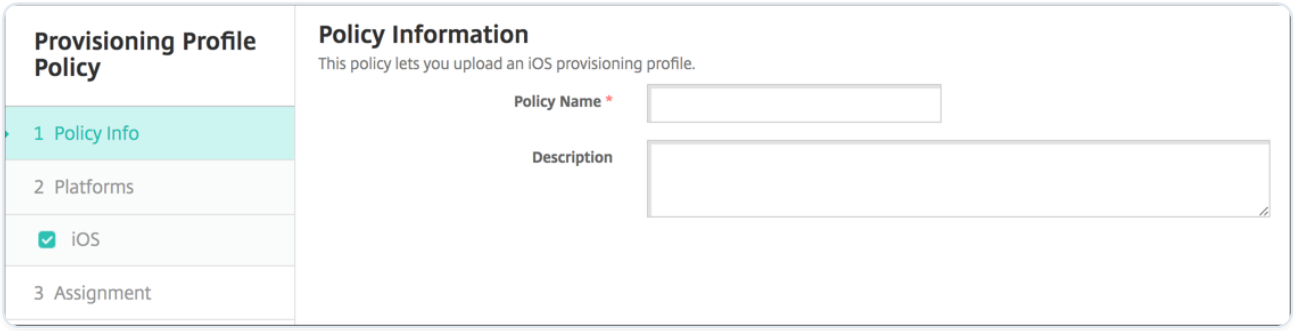
iOS 엔터프라이즈 앱을 개발하고 코드 서명할 때, 일반적으로 Apple이 iOS 장치에서 앱을 실행하는 데 필요한 엔터프라이즈 배포 프로비저닝 프로필을 포함합니다. 프로비저닝 프로필이 없거나 만료된 경우, 사용자가 앱을 열기 위해 탭하면 앱이 충돌합니다.

프로비저닝 프로필의 주요 문제는 Apple 개발자 포털에서 생성된 후 1년이 지나면 만료된다는 것입니다. 따라서 사용자가 등록한 모든 iOS 장치의 모든 프로비저닝 프로필에 대한 만료 날짜를 추적해야 합니다. 만료 날짜를 추적하는 것은 실제 만료 날짜를 추적하는 것뿐만 아니라 어떤 사용자가 어떤 버전의 앱을 사용하고 있는지도 파악하는 것을 포함합니다. 두 가지 해결책은 사용자에게 프로비저닝 프로필을 이메일로 보내거나 다운로드 및 설치를 위해 웹 포털에 게시하는 것입니다. 이러한 해결책은 작동하지만, 사용자가 이메일의 지침에 반응하거나 웹 포털로 이동하여 올바른 프로필을 다운로드한 다음 설치해야 하므로 오류가 발생하기 쉽습니다.

이 프로세스를 사용자에게 투명하게 만들기 위해 XenMobile®에서는 장치 정책을 사용하여 프로비저닝 프로필을 설치하고 제거할 수 있습니다. 누락되거나 만료된 프로필은 필요에 따라 제거되고 최신 프로필은 사용자 장치에 설치되므로, 앱을 탭하면 단순히 사용을 위해 열립니다.

프로비저닝 프로필 정책을 생성하기 전에 프로비저닝 프로필 파일을 생성해야 합니다. 자세한 내용은 Apple 개발자 사이트에서 개발 프로비저닝 프로필을 생성하는 방법에 대한 Apple 문서를 참조하십시오.

iOS 설정



- **iOS 프로비저닝 프로필: 찾아보기**를 클릭한 다음 파일 위치로 이동하여 가져올 프로비저닝 프로필 파일을 선택합니다.

프로비저닝 프로필 제거 장치 정책

장치 정책을 사용하여 iOS 프로비저닝 프로필을 제거할 수 있습니다. 프로비저닝 프로필에 대한 자세한 내용은 프로비저닝 프로필 장치 정책을 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **iOS 프로비저닝 프로필:** 제거하려는 드롭다운 목록에서 프로비저닝 프로필을 클릭합니다.
- **설명:** 선택적으로 설명을 추가합니다.

프록시 장치 정책

XenMobile에서 장치 정책을 추가하여 iOS 6.0 이상을 실행하는 장치에 대한 전역 HTTP 프록시 설정을 지정할 수 있습니다. 장치당 하나의 전역 HTTP 프록시 정책만 배포할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

이 정책을 배포하기 전에 전역 HTTP 프록시를 설정하려는 모든 iOS 장치를 감독 모드로 설정해야 합니다. 자세한 내용은 Apple Configurator를 사용하여 iOS 장치를 감독 모드로 전환하는 방법 또는 Apple 배포 프로그램을 통해 장치 배포를 참조하십시오.

장치에 프록시 정책을 보내기 전에 장치를 등록하도록 배포 규칙을 설정합니다.

iOS 설정

- **프록시 구성:** 사용자 장치에서 프록시를 구성하는 방법에 대해 **수동** 또는 **자동**을 클릭합니다.
  - **수동**을 클릭하면 다음 설정을 구성합니다.
    - **프록시 서버의 호스트 이름 또는 IP 주소:** 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
    - **프록시 서버의 포트:** 프록시 서버 포트 번호를 입력합니다. 이 필드는 필수입니다.
    - **사용자 이름:** 프록시 서버에 인증하기 위한 선택적 사용자 이름을 입력합니다.
    - **암호:** 프록시 서버에 인증하기 위한 선택적 암호를 입력합니다.
  - **자동**을 클릭하면 다음 설정을 구성합니다.
    - **프록시 PAC URL:** 프록시 구성을 정의하는 PAC 파일의 URL을 입력합니다.
    - **PAC에 연결할 수 없는 경우 직접 연결 허용:** PAC 파일에 연결할 수 없는 경우 사용자가 대상으로 직접 연결하도록 허용할지 여부를 선택합니다. 기본값은 **켜짐**입니다. 이 옵션은 iOS 7.0 이상에서만 사용할 수 있습니다.
- **캡티브 네트워크 액세스를 위해 프록시 우회 허용:** 캡티브 네트워크에 액세스하기 위해 프록시를 우회하도록 허용할지 여부를 선택합니다. 기본값은 **꺼짐**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

제한 장치 정책

제한 장치 정책을 사용하면 카메라와 같은 사용자 장치의 특정 기능 또는 기능을 허용하거나 제한할 수 있습니다. 또한 미디어 콘텐츠 제한 및 사용자가 설치할 수 있는 앱 유형에 대한 제한 외에도 보안 제한을 설정할 수 있습니다. 대부분의 제한 설정은 기본적으로 **켜짐** 또는 *허용*으로 설정됩니다. 주요 예외는 iOS 보안 - 강제 기능과 모든 Windows 태블릿 기능으로, 기본적으로 **꺼짐** 또는 *제한*으로 설정됩니다.

Windows 10 RS2 Phone의 경우: Internet Explorer를 비활성화하는 사용자 지정 XML 정책 또는 제한 정책이 휴대폰에 배포된 후에도 브라우저는 계속 활성화되어 있습니다. 이 문제를 해결하려면 휴대폰을 다시 시작하십시오. 이 문제는 타사 문제입니다.

팁:

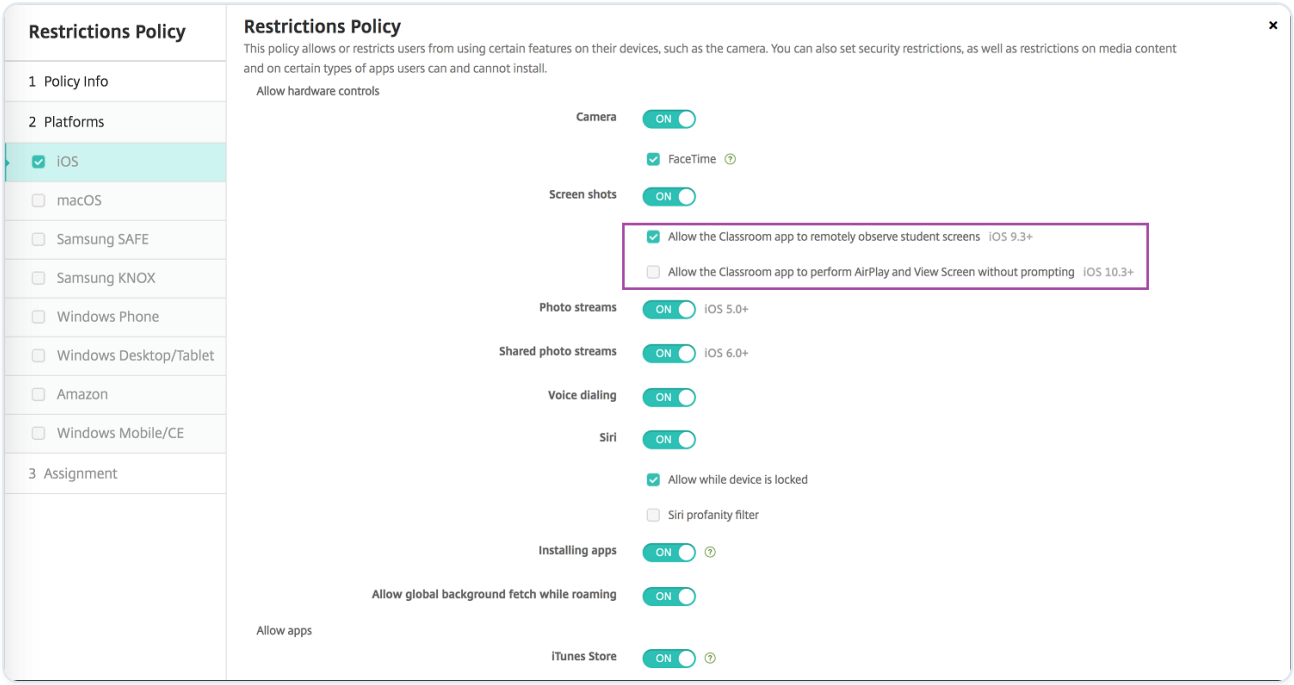
켜짐을 선택한 모든 옵션은 사용자가 해당 작업을 수행하거나 기능을 사용할 수 있음을 의미합니다. 예를 들어:

카메라. **켜짐**으로 설정하면 사용자는 장치에서 카메라를 사용할 수 있습니다. **꺼짐**으로 설정하면 사용자는 장치에서 카메라를 사용할 수 없습니다.

스크린샷. **켜짐**으로 설정하면 사용자는 장치에서 스크린샷을 찍을 수 있습니다. **꺼짐**으로 설정하면 사용자는 장치에서 스크린샷을 찍을 수 없습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정



일부 iOS 제한 정책 설정은 여기에 명시된 바와 같이 그리고 XenMobile® 콘솔 제한 정책 페이지에 명시된 바와 같이 특정 iOS 버전에만 적용됩니다.

iOS 제한 정책 설정은 장치가 사용자 등록 모드, 비감독(전체 MDM) 모드 또는 감독 모드로 등록될 때 적용될 수 있습니다. 다음 표는 iOS 13 이상에 대한 각 제한 정책 설정에 사용할 수 있는 등록 모드를 보여줍니다.

표에 명시된 바와 같이, 이전에 비감독 및 감독 모드에서 사용할 수 있었던 일부 설정은 iOS 13부터 감독 모드에서만 사용할 수 있습니다. 다음 규칙이 적용됩니다.

- 감독되는 iOS 13 이상 장치가 XenMobile에 등록되면 설정이 장치에 적용됩니다.
- 감독되지 않는 iOS 13 이상 장치가 XenMobile에 등록되면 설정이 장치에 적용되지 않습니다.
- iOS 12(이하) 기기가 XenMobile에 이미 등록되어 있고 iOS 13으로 업그레이드하는 경우 변경 사항이 없습니다. 설정은 업그레이드 전과 동일하게 기기에 적용됩니다.

iOS 기기를 감독 모드로 설정하는 방법에 대한 자세한 내용은 Apple Configurator를 사용하여 iOS 기기를 감독 모드로 전환하는 방법을(를) 참조하십시오.

설정	사용자 등록	비감독	감독
하드웨어 제어 허용			
카메라	아니요	예	예
FaceTime	아니요	아니요 (iOS 13에서 새로 추가됨)	예
FaceTime 원격 제어 허용	아니요	아니요	예
스크린샷	예	아니요	예
Classroom 앱이 학생 화면을 원격으로 관찰하도록 허용	아니요	아니요	예
Classroom 앱이 메시지 표시 없이 AirPlay 및 화면 보기를 수행하도록 허용	아니요	아니요	예
사진 스트림	아니요	예	예
공유 사진 스트림	아니요	예	예
공유 iPad 임시 세션 허용	아니요	예	예
음성 다이얼링	아니요	예	예
시리	예	예	예

설정	사용자 등록	비감독	감독
기기가 잠겨 있는 동안 허용	예	예	예
Siri 비속어 필터	아니요	아니요	예
앱 설치	아니요	아니요 (iOS 13에서 새로 추가됨)	예
대체 앱 마켓플레이스	아니요	아니요	예
웹 배포 앱	아니요	아니요	예
로밍 중 전역 백그라운드 가져오기 허용	아니요	예	예
앱 허용			
iTunes 스토어	아니요	아니요 (iOS 13에서 새로 추가됨)	예
앱 내 구입	아니요	예	예
구입 시 iTunes 암호 필요	아니요	예	예
사파리	아니요	아니요 (iOS 13부터 새로 추가됨)	예
자동 완성	아니요	아니요 (iOS 13부터 새로 추가됨)	예
사기 경고 강제	예	예	예
JavaScript 사용	아니요	예	예
팝업 차단	아니요	예	예
쿠키 허용	아니요	예	예
네트워크 - iCloud 작업 허용			

설정	사용자 등록	비감독	감독
iCloud 문서 및 데이터	아니요	아니요 (iOS 13부터 새로 추가됨)	예
iCloud 백업	아니요	예	예
iCloud 사진 키체인	아니요	예	예
iCloud 사진 보관함	아니요	예	예
보안 - 강제			
암호화된 백업	예	예	예
광고 추적 제한	아니요	예	예
첫 AirPlay 페어링 시 암호	예	예	예
손목 감지 사용을 위한 페어링된 Apple Watch	예	예	예
AirDrop을 사용하여 관리되는 문서 공유	예	예	예
보안 - 허용			
신뢰할 수 없는 SSL 인증서 허용	아니요	예	예
인증서 신뢰 설정 자동 업데이트	아니요	예	예
관리되는 붙여넣기판 필요	예	예	예
관리되지 않는 앱의 관리되는 앱 문서	예	예	예
관리되지 않는 앱이 관리되는 연락처를 읽음	아니요	아니요	예

설정	사용자 등록	비감독	감독
관리되는 앱이 관리되지 않는 연락처를 씀	아니요	아니요	예
관리되는 앱의 관리되지 않는 앱 문서	예	예	예
Apple에 진단 제출	예	예	예
Touch ID로 장치 잠금 해제	아니요	예	예
자동 잠금 해제	아니요	예	예
잠금 상태일 때 Passbook 알림	아니요	예	예
핸드오프	아니요	예	예
관리되는 앱에 대한 iCloud 동기화	예	예	예
엔터프라이즈 도서 백업	예	예	예
엔터프라이즈 도서에 대한 메모 및 하이라이트 동기화	예	예	예
Spotlight의 인터넷 결과	아니요	예	예
엔터프라이즈 앱 신뢰	아니요	예	예
Apple 개인 맞춤형 광고 허용	아니요	예	예
감독 전용 설정 - 허용			
eSIM 수정 허용	아니요	아니요	예
지울 때 eSIM 유지	아니요	아니요	예

설정	사용자 등록	비감독	감독
모든 콘텐츠 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
키보드 단축키	아니요	아니요	예
페어링된 Apple Watch	아니요	아니요	예
암호 수정	아니요	아니요	예
장치 이름 수정	아니요	아니요	예
배경화면 수정	아니요	아니요	예
앱 자동 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 13에서 새로 추가됨)	예
친구 추가	아니요	아니요	예

설정	사용자 등록	비감독	감독
멀티플레이어 게임	아니요	아니요 (iOS 13에서 새로 추가됨)	예
계정 설정 수정	아니요	아니요	예
앱 셀룰러 데이터 설정 수정	아니요	아니요	예
네트워크 드라이브 연결 허용	아니요	아니요	예
USB 장치 연결 허용	아니요	아니요	예
나의 기기 찾기 허용	아니요	아니요	예
나의 친구 찾기 허용	아니요	아니요	예
나의 친구 찾기 설정 수정	아니요	아니요	예
비-Configurator 호스트와 페어링	아니요	아니요	예
예측 키보드	아니요	아니요	예
키보드 자동 수정	아니요	아니요	예
키보드 맞춤법 검사	아니요	아니요	예
QuickPath 키보드 허용	아니요	아니요	예
정의 조회	아니요	아니요	예
단일 앱 번들 ID	아니요	아니요	예
뉴스	아니요	아니요	예
Apple Music 서비스	아니요	아니요	예
iTunes 라디오	아니요	아니요	예

설정	사용자 등록	비감독	감독
알림 수정	아니요	아니요	예
제한된 앱 사용	아니요	아니요	예
진단 제출 수정	아니요	아니요	예
Bluetooth 수정	아니요	아니요	예
받아쓰기 허용	아니요	아니요	예
Wi-Fi 강제 켜기	아니요	아니요	예
Wi-Fi 정책에 의해 설치된 Wi-Fi 네트워크만 연결	아니요	아니요	예
Classroom 앱이 메시지 표시 없이 AirPlay 및 화면 보기를 수행하도록 허용	아니요	아니요	예
Classroom 앱이 메시지 표시 없이 앱에 잠그고 장치를 잠그도록 허용	아니요	아니요	예
메시지 표시 없이 Classroom 앱 클래스에 자동으로 참여	아니요	아니요	예
AirPrint 허용	아니요	아니요	예
Keychain에 AirPrint 자격 증명 저장 허용	아니요	아니요	예
iBeacon을 사용하여 AirPrint 프린터 검색 허용	아니요	아니요	예
신뢰할 수 있는 인증서가 있는 대상으로만 AirPrint 허용	아니요	아니요	예

설정	사용자 등록	비감독	감독
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 지연 강제 적용	아니요	아니요	예
강제 소프트웨어 업데이트 지연	아니요	아니요	예
수업 종료 요청 권한 강제 적용	아니요	아니요	예
자동 완성 전 인증 강제	아니요	아니요	예
자동 날짜 및 시간 강제	아니요	아니요	예
암호 자동 완성	아니요	아니요	예
암호 근접 요청	아니요	아니요	예
암호 공유	아니요	아니요	예
개인용 핫스팟 설정 수정	아니요	아니요	예
페어링되지 않은 장치로 복구 부팅 허용	아니요	아니요	예
신속 보안 대응 설치	아니요	아니요	예
신속 보안 대응 제거	아니요	아니요	예
메일 개인 정보 보호 허용	아니요	아니요	예

설정	사용자 등록	비감독	감독
NFC	아니요	아니요	예
앱 클립 허용	아니요	아니요	예
젠모지	아니요	아니요	예
이미지 플레이그라운드	아니요	아니요	예
이미지 완드	아니요	아니요	예
iPhone 미러링	아니요	아니요	예
개인화된 필기 결과	아니요	아니요	예
쓰기 도구	아니요	아니요	예
통화 녹음	아니요	아니요	예
숨길 앱	아니요	아니요	예
잠글 앱	아니요	아니요	예
메일 요약	아니요	아니요	예
RCS 메시징	아니요	아니요	예
외부 인텔리전스 통합 허용	아니요	아니요	예
외부 인텔리전스 통합에 로그인 허용	아니요	아니요	예
메일 스마트 답장 허용	아니요	아니요	예
메모 필사 허용	아니요	아니요	예
Safari 요약 허용	아니요	아니요	예
시각 지능 요약 허용	아니요	아니요	예
메모 필사 요약 허용	아니요	아니요	예

설정	사용자 등록	비감독	감독
Apple Intelligence 보고서 허용	아니요	아니요	예
기본 통화 앱 수정 허용	아니요	아니요	예
기본 메시징 앱 수정 허용	아니요	아니요	예
외부 인텔리전스 작업 공간 ID 허용	아니요	아니요	예
기본 브라우저 수정	아니요	아니요	예
실시간 음성 사서함 허용	아니요	아니요	예
보안 - 잠금 화면에 표시			
제어 센터	예	예	예
알림	예	예	예
오늘 보기	예	예	예
미디어 콘텐츠 - 허용			
선정적인 음악, 팟캐스트 및 iTunes U 자료	아니요	아니요 (iOS 13에서 새로 추가됨)	예
iBooks의 노골적인 성적 콘텐츠	아니요	예	예
등급 지역	아니요	예	예
영화	아니요	예	예
TV 프로그램	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 장치에 해당합니다.
  - **FaceTime 원격 제어 허용:** 원격 FaceTime 세션이 장치 제어를 요청할 수 있도록 허용합니다. 감독되는 iOS 장치에 해당합니다. iOS 18.4 이상에서 사용할 수 있습니다.
- **스크린샷:** 사용자가 장치에서 스크린샷을 찍을 수 있도록 허용합니다.
  - **Classroom 앱이 학생 화면을 원격으로 관찰하도록 허용:** 이 제한을 선택하지 않으면 강사는 Classroom 앱을 사용하여 학생 화면을 원격으로 관찰할 수 없습니다. 기본 설정은 선택되어 있으며, 강사는 Classroom 앱을 사용하여 학생 화면을 관찰할 수 있습니다. **Classroom 앱이 메시지 없이 AirPlay 및 화면 보기를 수행하도록 허용** 설정은 학생이 강사에게 권한을 부여하라는 메시지를 받을지 여부를 결정합니다. 감독되는 iOS 장치에 해당합니다.
  - **Classroom 앱이 메시지 없이 AirPlay 및 화면 보기를 수행하도록 허용:** 이 제한을 선택하면 강사는 권한을 요청하는 메시지 없이 학생 장치에서 AirPlay 및 화면 보기를 수행할 수 있습니다. 기본 설정은 선택 해제되어 있습니다. 감독되는 iOS 장치에 해당합니다.
- **사진 스트림:** 사용자가 MyPhotoStream을 사용하여 iCloud를 통해 모든 iOS 장치에 사진을 공유할 수 있도록 허용합니다.
- **공유 사진 스트림:** 사용자가 iCloud 사진 공유를 사용하여 동료, 친구 및 가족과 사진을 공유할 수 있도록 허용합니다.
- **공유 iPad 임시 세션 허용:** 설정이 **끔**일 때 공유 iPad의 임시 세션에 대한 액세스를 방지합니다. 기본값은 **켬**입니다.
- **음성 통화:** 사용자 장치에서 음성 통화를 활성화합니다.
- **Siri:** 사용자가 Siri를 사용할 수 있도록 허용합니다.
  - **장치 잠금 중 허용:** 사용자가 장치가 잠겨 있는 동안 Siri를 사용할 수 있도록 허용합니다.
  - **Siri 비속어 필터:** Siri 비속어 필터를 활성화합니다. 기본값은 이 기능을 제한하는 것이며, 이는 비속어 필터링이 수행되지 않음을 의미합니다.

    Siri 및 보안에 대한 자세한 내용은 Siri 및 받아쓰기 정책을 참조하십시오.
- **앱 설치:** 사용자가 앱을 설치할 수 있도록 허용합니다. 감독되는 iOS 장치에 해당합니다.
- **대체 앱 마켓플레이스:** 웹에서 대체 마켓플레이스 앱을 설치하는 것을 방지하고, 설치된 대체 마켓플레이스 앱이 다른 앱을 설치하는 것을 방지합니다. 이 기능은 iOS 17.4 이상 버전에서 사용할 수 있습니다. 기본값은 **켜짐**입니다. 감독되는 iOS 장치에 해당합니다.

- **웹 배포 앱:** 고객 관리자가 iOS 장치에서 웹으로 배포된 타사 앱을 차단할 수 있도록 합니다. 이 기능은 iOS 17.5 이상 버전에 적용됩니다. 자세한 내용은 제한 사항을 참조하십시오.
- **로밍 중 전역 백그라운드 가져오기 허용:** 장치가 로밍 중일 때 메일 계정을 iCloud에 자동으로 동기화하도록 허용합니다. **끔**으로 설정하면 iOS 전화가 로밍 중일 때 전역 백그라운드 가져오기 활동을 비활성화합니다. 기본값은 **켜짐**입니다.

- **앱 허용**
  - **iTunes Store:** 사용자가 iTunes Store에 액세스할 수 있도록 허용합니다. 감독되는 iOS 장치에 해당합니다.
  - **앱 내 구매:** 사용자가 앱 내 구매를 할 수 있도록 허용합니다.
    - **구매 시 iTunes 암호 요구:** 앱 내 구매 시 암호를 요구합니다. 기본값은 이 기능을 제한하는 것이며, 이는 앱 내 구매에 암호가 필요하지 않음을 의미합니다.
  - **Safari:** 사용자가 Safari에 액세스할 수 있도록 허용합니다. 감독되는 iOS 장치에 해당합니다.
    - **자동 완성:** 사용자가 Safari에서 사용자 이름 및 암호에 대한 자동 완성을 설정할 수 있도록 허용합니다.
    - **사기 경고 강제:** 이 설정이 활성화되고 사용자가 의심스러운 피싱 웹사이트를 방문할 경우, Safari가 사용자에게 경고합니다. 기본적으로 이 기능은 제한되어 경고가 발행되지 않습니다.
    - **JavaScript 활성화:** Safari에서 JavaScript 실행을 허용합니다.
    - **팝업 차단:** 웹사이트를 볼 때 팝업을 차단합니다. 기본적으로 이 기능은 제한되어 팝업이 차단되지 않습니다.
  - **쿠키 허용:** 쿠키를 허용할 정도를 설정합니다. 목록에서 쿠키를 허용하거나 제한하는 옵션을 선택합니다. 기본 옵션은 **항상**으로, 모든 웹사이트가 Safari에 쿠키를 저장하도록 허용합니다. 다른 옵션으로는 **현재 웹사이트만**, **안 함**, **방문한 사이트에서만**이 있습니다.

- **네트워크 - iCloud 작업 허용**
  - **iCloud 문서 및 데이터:** 사용자가 문서 및 데이터를 iCloud에 동기화하도록 허용합니다. 감독되는 iOS 장치용.
  - **iCloud 백업:** 사용자가 장치를 iCloud에 백업하도록 허용합니다.
  - **iCloud 키체인:** 사용자가 암호, Wi-Fi 네트워크, 신용 카드 및 기타 정보를 iCloud 키체인에 저장하도록 허용합니다.
  - **클라우드 사진 보관함:** 사용자가 iCloud 사진 보관함에 액세스하도록 허용합니다.

- **보안 - 강제**

기본적으로 다음 기능은 제한되며, 이는 보안 기능이 활성화되지 않음을 의미합니다.

- **암호화된 백업:** iCloud로 백업 시 암호화를 강제합니다.
- **제한된 광고 추적:** 타겟 광고 추적을 차단합니다.
- **첫 AirPlay 페어링 시 암호:** AirPlay 지원 장치가 AirPlay를 사용하기 전에 일회성 화면 코드로 확인되도록 요구합니다.
- **페어링된 Apple Watch의 손목 감지 사용:** 페어링된 Apple Watch가 **손목 감지**를 사용하도록 요구합니다.
- **AirDrop을 사용하여 관리되는 문서 공유:** 이 옵션을 **켜기**로 설정하면 AirDrop이 관리되지 않는 드롭 대상으로 표시됩니다.

- **보안 - 허용**
  - **신뢰할 수 없는 SSL 인증서 수락:** 사용자가 웹사이트의 신뢰할 수 없는 SSL 인증서를 수락하도록 허용합니다.
  - **인증서 신뢰 설정 자동 업데이트:** 신뢰할 수 있는 인증서가 자동으로 업데이트되도록 허용합니다.
  - **관리되는 페이스트보드 필요:** 켜짐으로 설정하면 복사 및 붙여넣기 기능이 **관리되는 앱의 문서를 관리되지 않는 앱으로** 및 **관리되지 않는 앱의 문서를 관리되는 앱으로**에 적용하는 것과 동일한 제한을 따르도록 허용합니다. 기본값은 **끄기**입니다. 예를 들어, 다음을 구성합니다.
    - **관리되는 페이스트보드 필요**: 켜짐
    - **관리되는 앱의 문서를 관리되지 않는 앱으로**: 끄기
    - **관리되지 않는 앱의 문서를 관리되는 앱으로**: 켜짐

    > **참고:**
    >
    > iOS 장치에 정책을 배포한 후, 사용자는 관리되는 앱에서 관리되지 않는 앱으로 데이터를 복사하여 붙여넣을 수 없지만, 관리되지 않는 앱에서 관리되는 앱으로 데이터를 복사하여 붙여넣을 수 있습니다.

  - **관리되는 앱의 문서를 관리되지 않는 앱으로:** 사용자가 관리되는 (회사) 앱에서 관리되지 않는 (개인) 앱으로 데이터를 이동하도록 허용합니다.
  - **관리되지 않는 앱의 문서를 관리되는 앱으로:** 사용자가 관리되지 않는 (개인) 앱에서 관리되는 (회사) 앱으로 데이터를 이동하도록 허용합니다.
  - **Apple에 진단 제출:** 사용자의 장치에 대한 익명 진단 데이터가 Apple로 전송되도록 허용합니다.

- **Touch ID로 장치 잠금 해제:** 사용자가 지문을 사용하여 장치를 잠금 해제하도록 허용합니다.
- **자동 잠금 해제: 끄기**로 설정하면 사용자는 Apple Watch를 사용하여 페어링된 iPhone을 잠금 해제할 수 없습니다. 기본값은 **켜기**입니다. iOS 14.5 이상에서 사용할 수 있습니다.
- **잠금 상태일 때 Passbook 알림:** 잠금 화면에 Passbook 알림이 표시되도록 허용합니다.
- **Handoff:** 사용자가 한 iOS 장치에서 근처의 다른 iOS 장치로 활동을 전송할 수 있도록 허용합니다.
- **관리되는 앱의 iCloud 동기화:** 사용자가 관리되는 앱을 iCloud에 동기화할 수 있도록 허용합니다.
- **엔터프라이즈 도서 백업:** 엔터프라이즈 도서를 iCloud에 백업할 수 있도록 허용합니다.
- **엔터프라이즈 도서의 메모 및 하이라이트 동기화:** 사용자가 엔터프라이즈 도서에 추가한 메모 및 하이라이트를 iCloud에 동기화할 수 있도록 허용합니다.
- **엔터프라이즈 앱 신뢰:** 엔터프라이즈 애플리케이션을 신뢰할 수 있도록 허용합니다. 엔터프라이즈 앱은 조직을 위해 맞춤 제작된 모든 앱을 의미합니다. 이러한 앱은 내부적으로 제작되거나 외부 공급업체에서 개발 및 구매할 수 있습니다. 자세한 내용은 iOS에 사용자 지정 엔터프라이즈 앱 설치를 참조하십시오.
- **Spotlight의 인터넷 결과:** Spotlight가 장치 외에 인터넷에서 검색 결과를 표시하도록 허용합니다.
- **관리되지 않는 앱이 관리되는 연락처 읽기:** 선택 사항입니다. **관리되는 앱의 문서를 관리되지 않는 앱에서**가 비활성화된 경우에만 사용할 수 있습니다. 이 정책이 활성화되면 관리되지 않는 앱이 관리되는 계정의 연락처에서 데이터를 읽을 수 있습니다. 기본값은 **끔**입니다. iOS 12부터 사용할 수 있습니다.
- **관리되는 앱이 관리되지 않는 연락처 쓰기:** 선택 사항입니다. 활성화된 경우 관리되는 앱이 관리되지 않는 계정의 연락처에 연락처를 쓸 수 있도록 허용합니다. **관리되는 앱의 문서를 관리되지 않는 앱에서**가 활성화된 경우 이 제한은 적용되지 않습니다. 기본값은 **끔**입니다. iOS 12부터 사용할 수 있습니다.
- **Apple 개인 맞춤형 광고 허용: 끔**으로 설정하면 Apple 광고 플랫폼에서 사용자의 데이터를 사용하여 개인 맞춤형 광고를 제공하지 않습니다. 기본값은 **켬**입니다. iOS 14.0 이상에서 사용할 수 있습니다.

- **감독 전용 설정 - 허용**

  이 설정은 감독되는 장치에만 적용됩니다. iOS 장치를 감독 모드로 설정하는 단계는 Apple Configurator를 사용하여 iOS 장치를 감독 모드로 전환하는 방법을 참조하십시오.

  - **eSIM 수정 허용:** 사용자가 장치에서 eSIM 설정을 변경할 수 있도록 허용합니다.
  - **지울 때 eSIM 유지: 켬**으로 설정하면 암호 시도 실패 횟수 초과 또는 **설정** > **일반** > **재설정**의 모든 콘텐츠 및 설정 지우기 옵션으로 인해 장치를 지울 때 시스템이 eSIM을 유지합니다. 기본값은 **끔**입니다.

> **참고:**

> **나의 찾기**가 기기 지우기를 시작하면 시스템은 eSIM을 보존하지 않습니다.

- **모든 콘텐츠 및 설정 지우기:** 사용자가 기기에서 모든 콘텐츠 및 설정을 지울 수 있도록 허용합니다.
- **제한 구성:** 사용자가 기기에서 자녀 보호 기능을 구성할 수 있도록 허용합니다.
- **팟캐스트:** 사용자가 팟캐스트를 다운로드하고 동기화할 수 있도록 허용합니다.
- **구성 프로필 설치:** 사용자가 배포한 구성 프로필 외의 다른 구성 프로필을 설치할 수 있도록 허용합니다.
- **지문 수정:** 사용자가 Touch ID 지문을 변경하거나 삭제할 수 있도록 허용합니다.
- **기기에서 앱 설치:** 사용자가 앱을 설치할 수 있도록 허용합니다. 이 설정을 비활성화하면 최종 사용자가 새 앱을 설치할 수 없게 됩니다. App Store가 비활성화되고 해당 아이콘이 홈 화면에서 제거됩니다.
- **키보드 단축키:** 사용자가 자주 사용하는 단어나 문구에 대한 사용자 지정 키보드 단축키를 만들 수 있도록 허용합니다.
- **페어링된 Apple Watch:** 사용자가 감독되는 기기에 Apple Watch를 페어링할 수 있도록 허용합니다.
- **암호 수정:** 사용자가 감독되는 기기에서 암호를 변경할 수 있도록 허용합니다.
- **기기 이름 수정:** 사용자가 기기 이름을 변경할 수 있도록 허용합니다.
- **배경화면 수정:** 사용자가 기기의 배경화면을 변경할 수 있도록 허용합니다.
- **앱 자동 다운로드:** 앱을 다운로드할 수 있도록 허용합니다.
- **AirDrop:** 사용자가 근처 iOS 기기와 사진, 비디오, 웹사이트, 위치 등을 공유할 수 있도록 허용합니다.
- **iMessage:** 사용자가 iMessage를 사용하여 Wi-Fi를 통해 문자를 보낼 수 있도록 허용합니다.
- **Siri 사용자 생성 콘텐츠:** Siri가 웹에서 사용자 생성 콘텐츠를 쿼리하도록 허용합니다. 전통적인 언론인이 아닌 소비자가 사용자 생성 콘텐츠를 만듭니다. 예를 들어, Twitter 또는 Facebook에서 찾은 콘텐츠는 사용자 생성 콘텐츠입니다.
- **iBooks:** 사용자가 iBooks 앱을 사용하도록 허용합니다.
- **앱 제거:** 사용자가 장치에서 앱을 제거하도록 허용합니다.
- **Game Center:** 사용자가 장치에서 Game Center를 통해 온라인 게임을 플레이하도록 허용합니다.
  - **친구 추가:** 사용자가 친구에게 게임을 플레이하도록 알림을 보내도록 허용합니다.
  - **멀티플레이어 게임:** 사용자가 장치에서 멀티플레이어 게임 플레이를 시작하도록 허용합니다.
- **계정 설정 수정:** 사용자가 장치 계정 설정을 수정하도록 허용합니다.

- **앱 셀룰러 데이터 설정 수정:** 사용자가 앱이 셀룰러 데이터를 사용하는 방식을 수정하도록 허용합니다.
- **네트워크 드라이브 연결 허용:** 설정이 **끔**으로 되어 있으면 파일 앱에서 네트워크 드라이브에 연결하는 것을 방지합니다. 기본값은 **켬**입니다.
- **USB 장치 연결 허용:** 설정이 **끔**으로 되어 있으면 파일 앱에서 연결된 USB 장치에 연결하는 것을 방지합니다. 기본값은 **켬**입니다.
- **나의 장치 찾기 허용:** 설정이 **끔**으로 되어 있으면 나의 찾기 앱에서 **나의 장치 찾기** 옵션을 비활성화합니다. 기본값은 **켬**입니다.
- **나의 친구 찾기 허용:** 설정이 **끔**으로 되어 있으면 나의 찾기 앱에서 **나의 친구 찾기** 옵션을 비활성화합니다. 기본값은 **켬**입니다.
- **나의 친구 찾기 설정 수정:** 사용자가 나의 친구 찾기 설정을 변경하도록 허용합니다.
- **비 Configurator 호스트와 페어링:** 관리자가 사용자 장치가 페어링할 수 있는 장치를 제어하도록 허용합니다. 이 설정을 비활성화하면 Apple Configurator를 실행하는 감독 호스트를 제외하고 페어링이 방지됩니다. 감독 호스트 인증서가 구성되지 않은 경우 모든 페어링이 비활성화됩니다.
- **예측 키보드:** 사용자 장치가 입력할 때 단어를 제안하는 예측 키보드를 사용하도록 허용합니다. 사용자가 제안된 단어에 액세스하지 못하도록 하려는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- **키보드 자동 수정:** 사용자 장치에서 키보드 자동 수정을 사용하도록 허용합니다. 사용자가 자동 수정에 액세스하지 못하도록 하려는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화합니다.
- **키보드 맞춤법 검사:** 사용자 장치에서 입력하는 동안 맞춤법 검사를 사용하도록 허용합니다. 사용자가 맞춤법 검사기에 액세스하지 못하도록 하려는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화합니다.
- **QuickPath 키보드 허용:** 설정이 **끔**으로 되어 있으면 QuickPath 키보드를 비활성화합니다. 기본값은 **켬**입니다.
- **정의 조회:** 사용자 장치에서 입력하는 동안 정의 조회를 사용하도록 허용합니다. 사용자가 입력하는 동안 정의를 조회하지 못하도록 하려는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화합니다.
- **단일 앱 번들 ID:** 장치에 대한 제어권을 유지하고 다른 앱 또는 기능과의 상호 작용을 방지할 수 있는 앱 목록을 만듭니다. 앱을 추가하려면 **추가**를 클릭하고 **앱 이름**을 입력한 다음 **저장**을 클릭합니다. 추가하려는 각 앱에 대해 이 프로세스를 반복합니다.
- **뉴스:** 사용자가 뉴스 앱을 사용하도록 허용합니다.
- **Apple Music 서비스:** 사용자가 Apple Music 서비스를 사용하도록 허용합니다. Apple Music 서비스를 허용하지 않으면 음악 앱이 클래식 모드로 실행됩니다.

- **iTunes 라디오:** 사용자가 iTunes 라디오를 사용하도록 허용합니다.
- **알림 수정:** 사용자가 알림 설정을 수정하도록 허용합니다.
- **제한된 앱 사용:** 제공하는 번들 ID를 기반으로 사용자가 모든 앱을 사용하거나 앱을 사용하거나 사용하지 않도록 허용합니다. 감독되는 장치에만 적용됩니다. **일부 앱만 허용**을 선택하는 경우, 웹 클립을 허용하려면 번들 ID `com.apple.webapp`을(를) 사용하여 앱을 추가합니다.

  > **참고:**
  >
  > iOS 11부터 Apple은 앱 제한에 사용할 수 있는 정책을 변경했습니다. Apple은 더 이상 적절한 iOS 응용 프로그램 번들을 제한하여 설정 앱 및 전화 앱에 대한 액세스를 제거할 수 있도록 허용하지 않습니다.
  >
  > 일부 앱을 차단하도록 제한 장치 정책을 구성한 다음 정책을 배포한 후: 나중에 해당 앱 중 일부 또는 전부를 허용하려는 경우, 제한 장치 정책을 변경하고 배포해도 제한 사항이 변경되지 않습니다. 이 경우 iOS는 iOS 프로필에 변경 사항을 적용하지 않습니다. 계속하려면 프로필 제거 정책을 사용하여 iOS 프로필을 제거한 다음 업데이트된 제한 장치 정책을 배포합니다.

  이 설정을 **일부 앱만 허용**으로 변경하는 경우: 이 정책을 배포하기 전에 Apple 배포 프로그램을 사용하여 등록된 장치 사용자에게 설정 지원에서 Apple 계정에 로그인하도록 조언하십시오. 그렇지 않으면 사용자는 Apple 계정에 로그인하고 허용된 앱에 액세스하기 위해 장치에서 2단계 인증을 비활성화해야 할 수도 있습니다.
- **진단 제출 수정:** 사용자가 **설정 > 진단 및 사용량** 창에서 진단 제출 및 앱 분석 설정을 수정하도록 허용합니다.
- **Bluetooth 수정:** 사용자가 Bluetooth 설정을 수정할 수 있도록 허용합니다.
- **받아쓰기 허용:** 감독 모드에서만 가능합니다. 이 제한이 **끔**으로 설정된 경우, 음성-텍스트 변환을 포함한 받아쓰기 입력이 허용되지 않습니다. 기본 설정은 **켬**입니다.
- **Wi-Fi 강제 켜기:** 설정 또는 제어 센터에서 Wi-Fi를 켜거나 끄는 것을 방지합니다. 비행기 모드를 활성화해도 이 제한에는 영향을 미치지 않으며, 연결할 Wi-Fi 네트워크를 선택하는 것을 방해하지 않습니다. 기본값은 **끔**입니다.
- **Wi-Fi 정책으로 설치된 Wi-Fi 네트워크에만 연결:** 선택 사항입니다. 감독 모드에서만 가능합니다. 이 제한이 **켬**으로 설정된 경우, 장치는 구성 프로필을 통해 설정된 Wi-Fi 네트워크에만 연결할 수 있습니다. 기본 설정은 **끔**입니다.
- **Classroom 앱이 메시지 없이 AirPlay 및 화면 보기를 수행하도록 허용:** 이 제한이 선택된 경우, 강사는 허가 메시지 없이 학생 장치에서 AirPlay 및 화면 보기를 수행할 수 있습니다. 기본 설정은 선택 해제되어 있습니다. 감독 모드 iOS 장치용입니다.

- **Classroom 앱이 메시지 없이 앱에 고정하고 장치를 잠그도록 허용:** 이 제한이 **켬**으로 설정된 경우, Classroom 앱은 사용자에게 메시지를 표시하지 않고 사용자 장치를 앱에 자동으로 고정하고 장치를 잠급니다. 기본 설정은 **끔**입니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
- **Classroom 앱 수업에 메시지 없이 자동 참여:** 이 제한이 **켬**으로 설정된 경우, Classroom 앱은 사용자에게 메시지를 표시하지 않고 사용자를 수업에 자동으로 참여시킵니다. 기본 설정은 **끔**입니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
- **AirPrint 허용:** 이 제한이 **끔**으로 설정된 경우, 사용자는 AirPrint로 인쇄할 수 없습니다. 기본 설정은 **켬**입니다. 이 제한이 **켬**일 때, 이러한 추가 제한이 나타납니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
  - **AirPrint 자격 증명을 키체인에 저장 허용:** 이 제한이 선택 해제된 경우, AirPrint 사용자 이름과 암호는 키체인에 저장되지 않습니다. 기본 설정은 선택되어 있습니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
  - **iBeacon을 사용하여 AirPrint 프린터 검색 허용:** 이 제한이 선택 해제된 경우, iBeacon을 통한 AirPrint 프린터 검색이 비활성화됩니다. 이는 가짜 AirPrint Bluetooth 비콘이 네트워크 트래픽을 피싱하는 것을 방지합니다. 기본 설정은 선택되어 있습니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
  - **신뢰할 수 있는 인증서가 있는 대상으로만 AirPrint 허용:** 이 제한이 선택된 경우, 사용자는 신뢰할 수 있는 인증서가 있는 대상으로만 AirPrint를 사용하여 인쇄할 수 있습니다. 기본 설정은 선택 해제되어 있습니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
- **VPN 구성 추가:** 이 제한이 **끔**으로 설정된 경우, 사용자는 VPN 구성을 생성할 수 없습니다. 기본 설정은 **켬**입니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
- **셀룰러 요금제 설정 수정:** 이 제한이 **끔**으로 설정된 경우, 사용자는 셀룰러 요금제 설정을 수정할 수 없습니다. 기본 설정은 **켬**입니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
- **시스템 앱 제거:** 이 제한이 **끔**으로 설정된 경우, 사용자는 장치에서 시스템 앱을 제거할 수 없습니다. 기본 설정은 **켬**입니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
- **새로운 근처 장치 설정:** 이 제한이 끔으로 설정된 경우, 사용자는 새로운 근처 장치를 설정할 수 없습니다. 기본 설정은 켬입니다. iOS 11(최소 버전)을 실행하는 감독 모드 장치용입니다.
- **USB 제한 모드 허용:** **끔**으로 설정하면 장치가 잠겨 있는 동안에도 항상 USB 액세서리에 연결할 수 있습니다. 기본값은 **켬**입니다. 감독되는 iOS 11.3 이상 장치에서만 사용할 수 있습니다.
- **소프트웨어 업데이트 지연 강제 적용:** **켬**으로 설정하면 사용자가 소프트웨어 업데이트를 볼 수 있는 시기가 지연됩니다. 이 제한이 적용되면 사용자는 소프트웨어 업데이트 릴리스 날짜로부터 지정된 일수가 지난 후에야 소프트웨어 업데이트를 볼 수 있습니다. 기본값은 **끔**입니다. 감독되는 iOS 11.3 이상 장치에서만 사용할 수 있습니다.

- **강제 소프트웨어 업데이트 지연(일):** 장치에서 소프트웨어 업데이트를 지연할 일수를 지정할 수 있습니다. 최대 지연은 **90**일입니다. 기본값은 **30**일입니다. 감독되는 iOS 11.3 이상 장치에서만 사용할 수 있습니다.
- **수업 나가기 권한 요청 강제 적용:** **켬**으로 설정하면 Classroom으로 관리되지 않는 과정에 등록된 학생은 과정을 나가려고 할 때 교사에게 허락을 요청해야 합니다. 기본값은 **끔**입니다. 감독되는 iOS 11.3 이상 장치에서만 사용할 수 있습니다.
- **자동 완성 전 인증 강제 적용:** **켬**으로 설정하면 사용자는 Safari 및 앱에서 시스템이 암호 또는 신용 카드 정보를 자동 완성하기 전에 인증해야 합니다. Face ID 또는 Touch ID가 있는 장치에서만 지원됩니다. 기본값은 **끔**입니다.
- **자동 날짜 및 시간 강제 적용:** 감독되는 장치에서 날짜와 시간을 자동으로 설정할 수 있습니다. **켬**으로 설정하면 장치 사용자는 **일반 > 날짜 및 시간**에서 **자동으로 설정**을 끌 수 없습니다. 장치의 시간대는 장치가 위치를 확인할 수 있을 때만 업데이트됩니다. 즉, 장치에 셀룰러 연결이 있거나 위치 서비스가 활성화된 Wi-Fi 연결이 있을 때입니다. 기본값은 **끔**입니다. 감독되는 iOS 12 이상 장치에서만 사용할 수 있습니다.
- **암호 자동 완성:** 선택 사항입니다. 비활성화된 경우 사용자는 암호 자동 완성 또는 자동 강력 암호 기능을 사용할 수 없습니다. 기본값은 **켬**입니다. iOS 12부터 사용할 수 있습니다.
- **암호 근접 요청:** 선택 사항입니다. 비활성화된 경우 사용자의 장치는 근처 장치에서 암호를 요청하지 않습니다. 기본값은 **켬**입니다. iOS 12부터 사용할 수 있습니다.
- **암호 공유:** 선택 사항입니다. 비활성화된 경우 사용자는 AirDrop 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 **켬**입니다. iOS 12부터 사용할 수 있습니다.
- **개인용 핫스팟 설정 수정:** **끔**으로 설정하면 개인용 핫스팟 설정 수정이 비활성화됩니다. 기본값은 **켬**입니다.
- **페어링되지 않은 장치에 의한 복구 부팅 허용:** **켬**으로 설정하면 페어링되지 않은 장치에 의해 장치가 복구 모드로 부팅될 수 있습니다. 기본값은 **끔**입니다. iOS 14.5 이상에서 사용할 수 있습니다.
- **신속 보안 대응 설치:** **끔**으로 설정하면 신속 보안 대응 설치가 금지됩니다. 기본값은 **켬**입니다.
- **신속 보안 대응 제거:** **끔**으로 설정하면 신속 보안 대응 제거가 금지됩니다. 기본값은 **켬**입니다.
- **메일 개인 정보 보호 허용:** **끔**으로 설정하면 장치에서 메일 개인 정보 보호가 비활성화됩니다. 기본값은 **켬**입니다. iOS 15.2 이상에서 사용할 수 있습니다.
- **NFC:** **끔**으로 설정하면 NFC가 비활성화됩니다. 기본값은 **켬**입니다. iOS 14.2 이상에서 사용할 수 있습니다.
- **앱 클립 허용**: **끔**으로 설정하면 사용자가 앱 클립을 추가할 수 없으며 기기에 있는 기존 앱 클립이 모두 제거됩니다. 기본값은 **켬**입니다. iOS 14.0 이상에서 사용할 수 있습니다.
- **Genmoji:** **끔**으로 설정하면 새로운 Genmoji 생성이 금지됩니다. iOS 18 이상에서 사용할 수 있습니다.

- **이미지 플레이그라운드: 끔**으로 설정하면 이미지 생성 사용이 금지됩니다. iOS 18 이상에서 사용할 수 있습니다.
- **이미지 완드: 끔**으로 설정하면 이미지 완드 사용이 금지됩니다. iOS 18 이상에서 사용할 수 있습니다.
- **iPhone 미러링: 끔**으로 설정하면 iPhone 미러링 사용이 금지됩니다. iOS에서 사용 시, iPhone이 Mac으로 미러링되는 것을 방지합니다. iOS 18 이상에서 사용할 수 있습니다.
- **개인 맞춤형 필기 결과: 끔**으로 설정하면 시스템이 사용자의 필체로 텍스트를 생성하는 것을 방지합니다. iOS 18 이상에서 사용할 수 있습니다.
- **쓰기 도구: 끔**으로 설정하면 Apple Intelligence 쓰기 도구가 비활성화됩니다. iOS 18 이상에서 사용할 수 있습니다.
- **통화 녹음: 끔**으로 설정하면 통화 녹음이 비활성화됩니다. 감독 대상 기기가 필요합니다. iOS 18.1 이상에서 사용할 수 있습니다.
- **숨길 앱: 끔**으로 설정하면 사용자가 앱을 숨기는 기능이 금지됩니다. iOS에서 사용 시, 사용자가 앱을 숨기는 것을 방지하지만, 홈 화면에서 제거하면서도 앱 보관함에 앱을 남겨둘 수 있도록 허용합니다. 감독 대상 기기가 필요합니다. iOS 18 이상에서 사용할 수 있습니다.
- **잠글 앱: 끔**으로 설정하면 사용자가 앱을 잠그는 기능이 금지됩니다. iOS에서 사용 시, 사용자가 앱을 잠그는 것을 방지하며, 결과적으로 앱 숨기기도 방지합니다. 감독 대상 기기가 필요합니다. iOS 18 이상에서 사용할 수 있습니다.
- **메일 요약: 끔**으로 설정하면 이메일 메시지의 요약을 수동으로 생성하는 기능이 금지됩니다. iOS에서 사용 시, 자동 요약 생성에는 영향을 미치지 않습니다. 감독 대상 기기가 필요합니다. iOS 18.1 이상에서 사용할 수 있습니다.
- **RCS 메시징: 끔**으로 설정하면 RCS 메시징 사용이 방지됩니다. 감독 대상 기기가 필요합니다. iOS 18.1 이상에서 사용할 수 있습니다.
- **외부 인텔리전스 통합 허용: 끔**으로 설정하면 Siri와 함께 외부 클라우드 기반 인텔리전스 서비스 사용이 비활성화됩니다. 기본값은 **켬**입니다. iOS 18.2 이상에서 사용할 수 있습니다.
- **외부 인텔리전스 통합 로그인 허용: 끔**으로 설정하면 외부 인텔리전스 공급자가 익명 모드로 전환됩니다. 사용자가 이미 외부 인텔리전스 공급자에 로그인되어 있는 경우, 이 제한을 적용하면 다음 요청 시 로그아웃됩니다. 기본값은 **켬**입니다. iOS 18.2 이상에서 사용할 수 있습니다.
- **메일 스마트 답장 허용: 끔**으로 설정하면 메일의 스마트 답장이 비활성화됩니다. 기본값은 **켬**입니다. iOS 18.2 이상에서 사용할 수 있습니다.
- **메모 필사 허용: 끔**으로 설정하면 메모에서 필사를 비활성화합니다. 기본값은 **켬**입니다. iOS 18.2 이상에서 사용할 수 있습니다.
- **Safari 요약 허용: 끔**으로 설정하면 시스템이 Safari에서 콘텐츠를 요약하는 기능을 비활성화합니다. 기본값은 **켬**입니다. iOS 18.4 이상에서 사용할 수 있습니다.

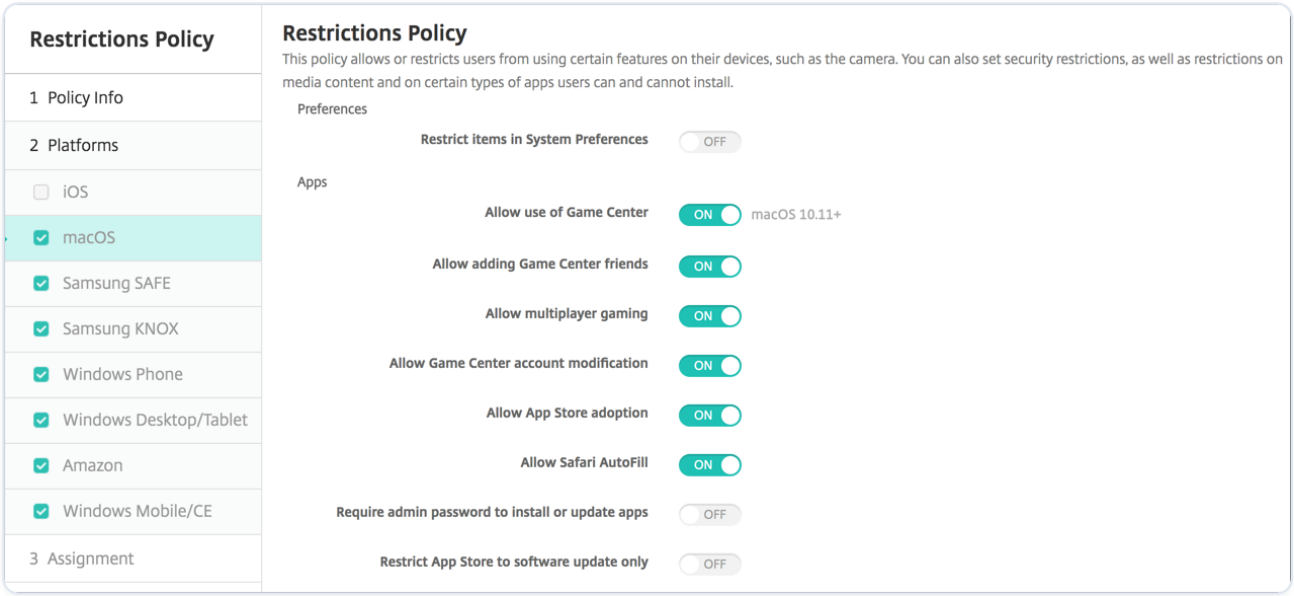
- **시각 지능 요약 허용:** **끔**으로 설정하면 시스템이 시각 지능 요약을 비활성화합니다. 기본값은 **켬**입니다. iOS 18.3 이상에서 사용할 수 있습니다.
- **메모 필사 요약 허용:** **끔**으로 설정하면 메모에서 필사 요약을 비활성화합니다. 기본값은 **켬**입니다. iOS 18.3 이상에서 사용할 수 있습니다.
- **Apple Intelligence 보고서 허용:** **끔**으로 설정하면 시스템이 Apple Intelligence 보고서를 비활성화합니다. 기본값은 **켬**입니다. iOS 18.4 이상에서 사용할 수 있습니다.
- **기본 통화 앱 수정 허용:** **끔**으로 설정하면 기본 통화 앱 기본 설정 수정을 비활성화합니다. 이 설정이 적용되어도 기본 통화 앱 기본 설정을 지정하는 MDM 설정 명령은 계속 작동합니다. 기본값은 **켬**입니다. iOS 18.4 이상에서 사용할 수 있습니다.
- **기본 메시징 앱 수정 허용:** **끔**으로 설정하면 기본 메시징 앱 기본 설정 수정을 비활성화합니다. 이 설정이 적용되어도 기본 메시징 앱 기본 설정을 지정하는 MDM 설정 명령은 계속 작동합니다. 기본값은 **켬**입니다. iOS 18.4 이상에서 사용할 수 있습니다.
- **외부 인텔리전스 작업 공간 ID 허용:** 문자열 배열이지만 현재 단일 요소로 제한됩니다. 이 설정이 있으면 Apple Intelligence는 지정된 외부 통합 작업 공간 ID만 사용하도록 허용하며, 요청하려면 로그인이 필요합니다. 사용자는 로그인 지원 통합에 로그인해야 합니다. 여러 페이로드는 교차 작업을 사용하여 결합됩니다. 이는 여러 페이로드에 충돌하는 값이 지정된 경우 허용되는 작업 공간 ID 집합이 빈 집합이 될 수 있음을 의미합니다. iOS 18.3 이상에서 사용할 수 있습니다.
  - **외부 인텔리전스 작업 공간 ID:** 외부 인텔리전스 작업 공간 ID를 추가하려면 **추가**를 클릭하고 **외부 인텔리전스 작업 공간 ID**를 입력한 다음 **저장**을 클릭합니다. 추가하려는 각 작업 공간 ID에 대해 이 과정을 반복합니다.
- **기본 브라우저 수정:** **끔**으로 설정하면 기본 브라우저 기본 설정 수정을 금지합니다. iOS에서 사용되는 경우에도 MDM 설정 명령을 통해 기본 브라우저 기본 설정을 지정할 수 있습니다. 감독 대상 기기가 필요합니다. iOS 18.2 이상에서 사용할 수 있습니다.
- **실시간 음성 사서함 허용:** **끔**으로 설정하면 시스템이 기기에서 실시간 음성 사서함을 비활성화합니다. 기본값은 **켬**입니다. iOS 17.2 이상에서 사용할 수 있습니다.

- **보안 - 잠금 화면에 표시**
  - **제어 센터:** 잠금 화면에서 제어 센터에 대한 접근을 허용합니다. 제어 센터를 통해 사용자는 비행기 모드, Wi-Fi, Bluetooth, 방해금지 모드 및 화면 회전 잠금 설정을 쉽게 수정할 수 있습니다.
  - **알림:** 잠금 화면에서 알림을 허용합니다.
  - **오늘 보기:** 잠금 화면에서 날씨 및 당일 캘린더 항목과 같은 정보를 집계하는 오늘 보기를 허용합니다.
- **미디어 콘텐츠 - 허용**

- **노골적인 음악, 팟캐스트 및 iTunes U 자료:** 사용자의 장치에서 노골적인 자료를 허용합니다.
- **iBooks의 노골적인 성적 콘텐츠:** iBooks에서 노골적인 자료를 다운로드할 수 있도록 허용합니다.
- **등급 지역:** 자녀 보호 등급을 가져올 지역을 설정합니다. 목록에서 국가를 클릭하여 등급 지역을 설정합니다. 기본값은 **미국**입니다.
- **영화:** 사용자의 장치에서 영화를 허용할지 여부를 설정합니다. 영화가 허용되는 경우, 선택적으로 영화 등급 수준을 설정합니다. 목록에서 옵션을 클릭하여 장치에서 영화를 허용하거나 제한합니다. 기본값은 모든 영화 허용입니다.
- **TV 프로그램:** 사용자의 장치에서 TV 프로그램을 허용할지 여부를 설정합니다. TV 프로그램이 허용되는 경우, 선택적으로 TV 프로그램 등급 수준을 설정합니다. 목록에서 옵션을 클릭하여 장치에서 TV 프로그램을 허용하거나 제한합니다. 기본값은 모든 TV 프로그램 허용입니다.
- **앱:** 사용자의 장치에서 앱을 허용할지 여부를 설정합니다. 앱이 허용되는 경우, 선택적으로 앱 등급 수준을 설정합니다. 목록에서 옵션을 클릭하여 장치에서 앱을 허용하거나 제한합니다. 기본값은 모든 앱 허용입니다.

- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.
  - **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 또는 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 iOS 9.3 이상에서만 사용할 수 있습니다.

macOS 설정



- **기본 설정**
  - **시스템 환경설정 항목 제한:** 사용자의 시스템 환경설정 접근을 허용하거나 제한합니다. 기본값은 **끔**이며, 이는 사용자에게 시스템 환경설정에 대한 전체 액세스를 허용합니다. 활성화된 경우 다음 설정을 구성합니다.
    - **시스템 환경설정 창:** 선택한 설정이 활성화될지 비활성화될지 선택합니다. 기본값은 모든 설정을 활성화하는 것이며, 이는 기본적으로 **켬**입니다.
      - 사용자 및 그룹
      - 일반
      - 손쉬운 사용
      - 앱 스토어
      - 소프트웨어 업데이트
      - 블루투스
      - CD 및 DVD
      - 날짜 및 시간
      - 데스크탑 및 화면 보호기
      - 디스플레이
      - 독
      - 에너지 절약
      - 확장 프로그램

    - FibreChannel
    - iCloud
    - 잉크
    - 인터넷 계정
    - 키보드
    - 언어 및 텍스트
    - 미션 컨트롤
    - 마우스
    - 네트워크
    - 알림
    - 자녀 보호
    - 프린터 및 스캐너
    - 프로파일
    - 보안 및 개인 정보 보호
    - 공유
    - 사운드
    - 발음 및 음성
    - 스포트라이트
    - 시동 디스크
    - 타임 머신
    - 트랙패드
    - 엑스샌

- **앱**
    - **Game Center 사용 허용:** 사용자가 Game Center를 통해 온라인 게임을 플레이할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
    - **Game Center 친구 추가 허용:** 사용자가 친구에게 게임 플레이 알림을 보낼 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
    - **멀티플레이어 게임 허용:** 사용자가 멀티플레이어 게임을 시작할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.

- **Game Center 계정 수정 허용:** 사용자가 Game Center 계정 설정을 수정할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **App Store 채택 허용:** App Store가 OS X에 미리 존재하는 앱을 채택하도록 허용하거나 제한합니다. 기본값은 **켜짐**입니다.
- **Safari 자동 완성 허용:** Safari가 저장된 암호, 주소 및 기타 기본 정보로 웹사이트의 필드를 자동으로 채우도록 허용합니다. 기본값은 **켜짐**입니다.
- **앱 설치 또는 업데이트 시 관리자 암호 요구:** 앱을 설치하거나 업데이트하려면 관리자 암호가 필요합니다. 기본값은 **꺼짐**이며, 이는 관리자 암호가 필요하지 않음을 의미합니다.
- **App Store를 소프트웨어 업데이트 전용으로 제한:** App Store를 업데이트 전용으로 제한하여 업데이트를 제외한 App Store의 모든 탭을 비활성화합니다. 기본값은 **끄기**이며, App Store에 대한 전체 액세스를 허용합니다.
- **실행이 허용되는 앱 제한:** 사용자가 사용할 수 있는 앱을 제한하거나 허용합니다. 기본값은 OFF이며, 모든 앱을 사용할 수 있도록 허용합니다. 활성화된 경우 다음 설정을 구성합니다.
  - **허용된 앱: 추가**를 클릭하고 실행이 허용된 앱의 이름과 번들 ID를 입력한 다음 **저장**을 클릭합니다. 실행이 허용된 각 앱에 대해 이 단계를 반복합니다.
  - **허용되지 않는 폴더: 추가**를 클릭하고 사용자 액세스를 제한하려는 폴더의 파일 경로(예: /Applications/Utilities)를 입력한 다음 **저장**을 클릭합니다. 사용자가 액세스하지 않기를 원하는 모든 폴더에 대해 이 단계를 반복합니다.
  - **허용된 폴더: 추가**를 클릭하고 사용자 액세스를 허용하려는 폴더의 파일 경로를 입력한 다음 **저장**을 클릭합니다. 사용자가 액세스하기를 원하는 모든 폴더에 대해 이 단계를 반복합니다.

- **위젯**
  - **다음 대시보드 위젯만 실행 허용:** 세계 시계 또는 계산기와 같은 대시보드 위젯 중 사용자가 실행할 수 있는 위젯을 허용하거나 제한합니다. 기본값은 **끄기**이며, 사용자가 모든 위젯을 실행할 수 있도록 허용합니다. 활성화된 경우 다음 설정을 구성합니다.
    - **허용된 위젯: 추가**를 클릭하고 실행이 허용된 위젯의 이름과 ID를 입력한 다음 **저장**을 클릭합니다. 대시보드에서 실행하려는 각 위젯에 대해 이 단계를 반복합니다.
- **미디어**
  - **AirDrop 허용:** 사용자가 근처 iOS 장치와 사진, 비디오, 웹사이트, 위치 등을 공유할 수 있도록 허용합니다.
- **공유**
  - **새 공유 서비스 자동 활성화:** 공유 서비스를 자동으로 활성화할지 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.
- **Aperture에 추가:** Aperture에 추가할 공유 기능을 허용할지 여부를 선택합니다.
- **Sina Weibo:** 공유 Sina Weibo 마이크로블로깅 계정을 허용할지 여부를 선택합니다.
- **Twitter:** 공유 Twitter 계정을 허용할지 여부를 선택합니다.
- **메시지:** 메시지에 대한 공유 액세스를 허용할지 여부를 선택합니다.
- **iPhoto에 추가:** iPhoto에 추가할 공유 기능을 허용할지 여부를 선택합니다.
- **읽기 목록에 추가:** 읽기 목록에 추가할 공유 기능을 허용할지 여부를 선택합니다.
- **AirDrop:** 공유 AirDrop 계정을 허용할지 여부를 선택합니다.

- **기능**
  - **데스크톱 사진 잠금:** 사용자가 데스크톱 사진을 변경할 수 있는지 여부를 선택합니다. 기본값은 **끔**이며, 이는 사용자가 데스크톱 사진을 변경할 수 있음을 의미합니다.
  - **카메라 사용 허용:** 사용자가 Mac에서 카메라를 사용할 수 있는지 여부를 선택합니다. 기본값은 **끔**이며, 이는 사용자가 카메라를 사용할 수 없음을 의미합니다.
  - **Apple Music 허용:** 사용자가 Apple Music 서비스를 사용할 수 있도록 허용합니다(macOS 10.12 이상). Apple Music 서비스를 허용하지 않으면 음악 앱이 클래식 모드로 실행됩니다. 감독되는 장치에만 적용됩니다. 기본값은 **켬**입니다.
  - **Spotlight 제안 허용:** 사용자가 Spotlight 제안을 사용하여 Mac을 검색하고 인터넷, iTunes 및 App Store에서 Spotlight 제안을 제공할 수 있는지 여부를 선택합니다. 기본값은 **끔**이며, 이는 사용자가 Spotlight 제안을 사용할 수 없도록 합니다.
  - **찾아보기 허용:** 사용자가 상황에 맞는 메뉴 또는 Spotlight 검색 메뉴를 사용하여 단어의 정의를 찾아볼 수 있는지 여부를 선택합니다. 기본값은 OFF이며, 이는 사용자가 Mac에서 찾아보기를 사용할 수 없도록 합니다.
  - **로컬 계정에 iCloud 암호 사용 허용:** 사용자가 Apple ID 및 iCloud 암호를 사용하여 Mac에 로그인할 수 있는지 여부를 선택합니다. 이 정책을 활성화하면 사용자는 Mac의 *모든* 로그인 화면에 대해 하나의 ID와 암호만 사용하게 됩니다. 기본값은 **켬**이며, 이는 사용자가 Apple ID 및 iCloud 암호를 사용하여 Mac에 액세스할 수 있도록 합니다.
  - **iCloud 문서 및 데이터 허용:** 사용자가 Mac에서 iCloud에 저장된 문서 및 데이터에 액세스할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **끔**이며, 이는 사용자가 Mac에서 iCloud 문서 및 데이터를 사용할 수 없도록 합니다.

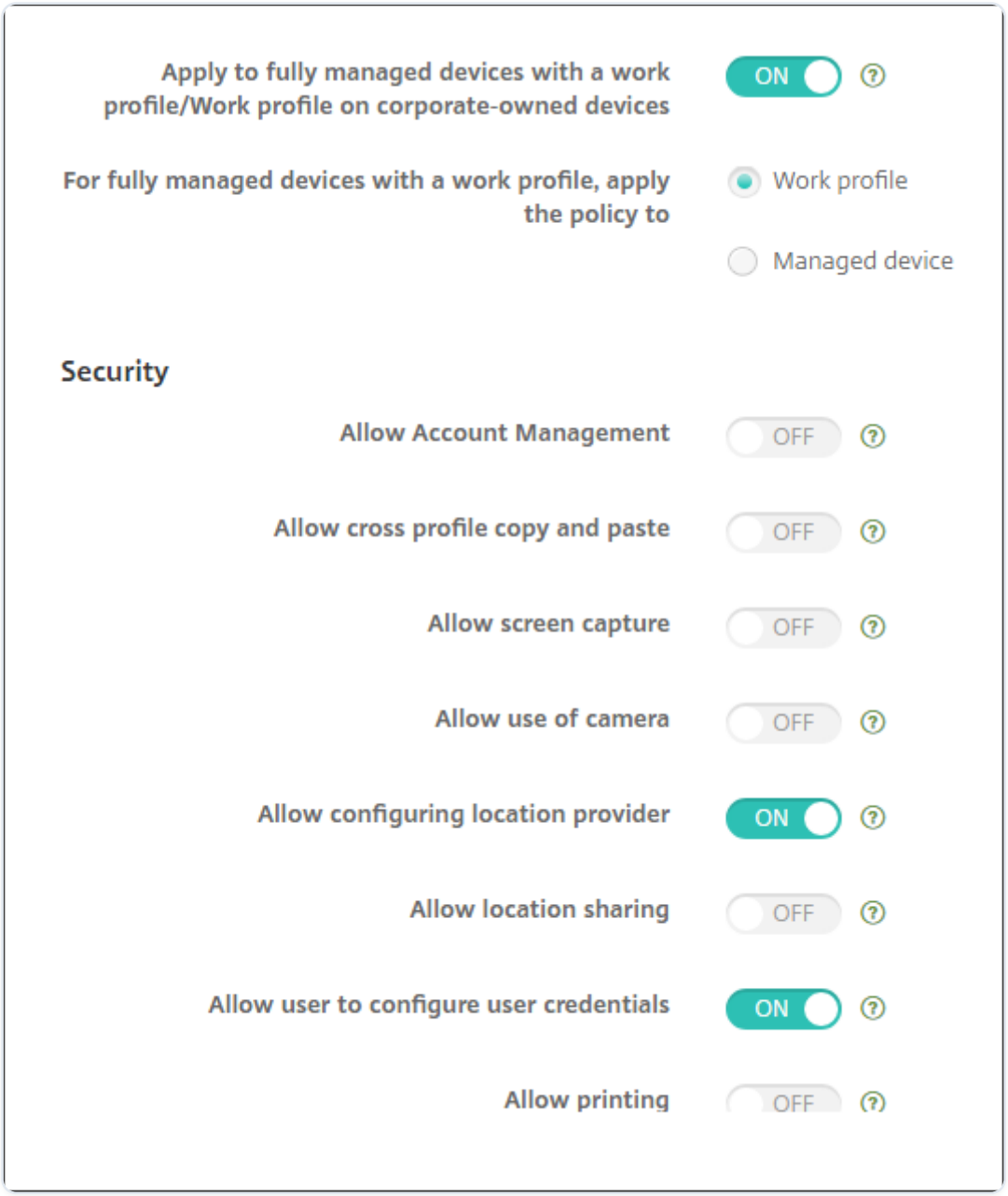
    - **iCloud 데스크탑 및 문서 허용:** (macOS 10.12.4 이상) 기본값은 선택됨입니다.
- **iCloud 키체인 동기화 허용:** iCloud 키체인 동기화를 허용합니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **iCloud Mail 허용:** 사용자가 iCloud Mail을 사용하도록 허용합니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **iCloud 연락처 허용:** 사용자가 iCloud 연락처를 사용하도록 허용합니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **iCloud 캘린더 허용:** 사용자가 iCloud 캘린더를 사용하도록 허용합니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **iCloud 미리 알림 허용:** 사용자가 iCloud 미리 알림을 사용하도록 허용합니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **iCloud 책갈피 허용:** 사용자가 iCloud 책갈피와 동기화하도록 허용합니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **iCloud 메모 허용:** 사용자가 Cloud Notes를 사용하도록 허용합니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **iCloud 사진 허용:** 이 설정을 **끔**으로 변경하면 iCloud 사진 보관함에서 완전히 다운로드되지 않은 모든 사진이 로컬 장치 저장소에서 제거됩니다 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **자동 잠금 해제 허용:** 이 옵션 및 Apple Watch에 대한 자세한 내용은 https://www.imore.com/auto-unlock을 참조하십시오 (macOS 10.12 이상). 기본값은 **켜짐**입니다.
- **Touch ID로 Mac 잠금 해제 허용:** (macOS 10.12.4 이상). 기본값은 **켜짐**입니다.
- **소프트웨어 업데이트 지연 강제 적용: 켜짐**으로 설정하면 이 설정은 사용자가 소프트웨어 업데이트를 볼 수 있는 시기를 지연시킵니다. 사용자는 소프트웨어 업데이트 릴리스 날짜로부터 지정된 일수가 지난 후에야 소프트웨어 업데이트를 볼 수 있습니다. 기본값은 **끔**입니다. macOS 10.13.4 이상을 실행하는 감독 대상 장치에서만 사용할 수 있습니다.
- **강제 소프트웨어 업데이트 지연(일):** 장치에서 소프트웨어 업데이트를 지연할 일수를 지정합니다. 최대 90일입니다. 기본값은 **30**입니다. macOS 10.13.4 이상을 실행하는 감독 대상 장치에서만 사용할 수 있습니다.
- **암호 자동 완성:** 선택 사항입니다. 비활성화된 경우 사용자는 암호 자동 완성 또는 자동 강력 암호 기능을 사용할 수 없습니다. 기본값은 **켜짐**입니다. macOS 10.14부터 사용할 수 있습니다.
- **암호 근접 요청:** 선택 사항입니다. 비활성화된 경우 사용자의 장치는 근처 장치에서 암호를 요청하지 않습니다. 기본값은 **켜짐**입니다. macOS 10.14부터 사용할 수 있습니다.
- **암호 공유:** 선택 사항입니다. 비활성화된 경우, 사용자는 AirDrop 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 **켜짐**입니다. macOS 10.14부터 사용할 수 있습니다.

- **이미지 플레이그라운드: 꺼짐**으로 설정하면 이미지 생성을 금지합니다. 기본값은 **켜짐**입니다. macOS 15 이상을 실행하는 감독 대상 기기에서만 사용할 수 있습니다.
- **iPhone 미러링: 꺼짐**으로 설정하면 iPhone 미러링 사용을 금지합니다. macOS에서 사용할 경우, Mac이 iPhone을 미러링하는 것을 방지합니다. 기본값은 **켜짐**입니다. macOS 15 이상을 실행하는 감독 대상 기기에서만 사용할 수 있습니다.
- **쓰기 도구: 꺼짐**으로 설정하면 Apple Intelligence 쓰기 도구를 비활성화합니다. 기본값은 **켜짐**입니다. macOS 15 이상을 실행하는 감독 대상 기기에서만 사용할 수 있습니다.
- **미디어 공유 수정 허용: 꺼짐**으로 설정하면 미디어 공유 설정 수정을 방지합니다. 기본값은 **켜짐**입니다. macOS 15.1 이상에서 사용할 수 있습니다.
- **화면 캡처 경고 강제 우회: 켜짐**으로 설정하면 화면 캡처 경고 표시를 우회합니다. 기본값은 **꺼짐**입니다. macOS 15.1 이상에서 사용할 수 있습니다.
- **메일 요약: 꺼짐**으로 설정하면 이메일 메시지를 수동으로 요약하는 기능을 비활성화합니다. 이는 자동 요약 생성에는 영향을 미치지 않습니다. 기본값은 **켜짐**입니다. macOS 15.1 이상에서 사용할 수 있습니다.

Android 설정

- **카메라:** 사용자가 기기에서 카메라를 사용할 수 있도록 허용합니다. **꺼짐**으로 설정하면 카메라가 비활성화됩니다. 기본값은 **켜짐**입니다.

안드로이드 엔터프라이즈 설정



새 Android 기기 또는 공장 초기화된 Android 기기가 작업 프로필 모드로 등록될 때, Android 9.0-10.x를 실행하는 기기는 작업 프로필이 있는 완전 관리형 기기로 등록됩니다. Android 11 이상을 실행하는 기기는 회사 소유 기기의 작업 프로필로 등록됩니다. 제한 정책은 기기의 작업 프로필 또는 관리형 기기에 적용될 수 있습니다.

회사 소유 기기 모드의 작업 프로필에 등록된 기기에서는 다음 제한 사항이 작업 프로필에만 적용됩니다:

- 백업 서비스 허용
- 시스템 앱 활성화
- 키가드가 장치를 잠그지 못하게 합니다.
- 상태 표시줄 사용 허용

- 장치 화면 켜짐 유지
- 사용자의 애플리케이션 설정 제어 허용
- 사용자가 사용자 자격 증명을 구성하도록 허용
- VPN 구성 허용
- USB 대용량 저장소 허용
- 공장 초기화 허용
- 앱 제거 허용
- 업무 및 개인 프로필에서 이메일 앱 액세스
- Google Play가 아닌 앱 허용
- 교차 프로필 복사 및 붙여넣기 허용
- 앱 확인 사용
- 계정 관리 허용
- 인쇄 허용
- NFC 허용
- 사용자 추가 허용

기본적으로, 기기가 작업 프로필 모드에서 Android Enterprise에 등록될 때 **USB 디버깅 및 알 수 없는 소스** 설정은 비활성화됩니다.

Android 9.0-10.x 및 Samsung Knox 3.0 이상을 실행하는 기기의 경우, **Android Enterprise** 페이지에서 Samsung Knox 및 Samsung SAFE 설정을 구성합니다. 이전 버전의 Android 또는 Samsung Knox를 실행하는 기기의 경우, **Samsung Knox** 및 **Samsung SAFE** 페이지를 사용합니다.

Samsung 제한 사항은 회사 소유 기기 모드의 작업 프로필에 등록된 기기에는 적용되지 않습니다. Knox Service Plugin (KSP)을 사용하여 이러한 기기에 Samsung 제한 사항을 적용하십시오. 자세한 내용은 Samsung 설명서를 참조하십시오.

최신 Samsung Knox 관리 기능을 사용하려면 Samsung Knox 3.4 이상을 사용하는 것이 좋습니다.

- **작업 프로필이 있는 완전 관리형 기기/회사 소유 기기의 작업 프로필에 적용:** 작업 프로필이 있는 완전 관리형 기기에 대한 제한 정책 설정을 구성할 수 있습니다. 이 설정이 **켜짐**인 경우 다음 설정 중 하나를 선택합니다.
  - **작업 프로필:** 구성하는 제한 설정은 기기의 작업 프로필에만 적용됩니다.
  - **기기 관리:** 구성하는 제한 설정은 기기에만 적용됩니다.

이 설정이 **꺼짐**인 경우, 구성하는 자격 증명 설정은 작업 프로필에 명시적으로 적용되는 설정을 제외하고 기기에 적용됩니다. 기본값은 **꺼짐**입니다.

작업 프로필이 있는 완전 관리형 기기/회사 소유 기기의 작업 프로필에 적용이 꺼져 있는 경우, 다음 설정을 구성합니다.

- **보안**
  - **계정 관리 허용:** 작업 프로필 및 관리되는 기기에 계정을 추가할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **교차 프로필 복사 및 붙여넣기 허용: 켜짐**인 경우, 사용자는 Android Enterprise 프로필의 앱과 개인 영역의 앱 간에 복사 및 붙여넣기를 할 수 있습니다. 기본값은 **꺼짐**입니다.
  - **화면 캡처 허용:** 사용자가 기기 화면을 녹화하거나 화면 캡처를 할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **카메라 사용 허용:** 사용자가 장치 카메라로 사진을 찍고 비디오를 만들 수 있도록 허용합니다. 기본값은 **끄기**입니다.
  - **VPN 구성 허용:** 사용자가 VPN 구성을 만들 수 있도록 허용합니다. Android 6 이상을 실행하는 업무 프로필 장치 및 완전 관리형 장치에 해당합니다. 기본값은 **켜기**입니다.
  - **백업 서비스 허용:** 사용자가 장치에서 애플리케이션 및 시스템 데이터를 백업할 수 있도록 허용합니다. 기본값은 **켜기**입니다.
  - **NFC 허용:** 사용자가 근거리 무선 통신(NFC)을 사용하여 장치에서 다른 장치로 웹 페이지, 사진, 비디오 또는 기타 콘텐츠를 보낼 수 있도록 허용합니다. MDM 4.0 이상에 해당합니다. 기본값은 **켜기**입니다.
  - **위치 공급자 구성 허용:** 사용자가 장치에서 GPS를 켤 수 있도록 허용합니다. Android API 28 이상에 해당합니다. 기본값은 **켜기**입니다.
  - **위치 공유 허용:** 관리형 프로필의 경우 장치 소유자가 이 설정을 재정의할 수 있습니다. 기본값은 **끄기**입니다.

    > **팁:**
    >
    > XenMobile에서 위치 장치 정책을 생성하여 지리적 경계를 적용할 수 있습니다. 위치 장치 정책을 참조하십시오.

  - **사용자 자격 증명 구성 허용:** 사용자가 관리형 키 저장소에서 자격 증명을 구성할 수 있는지 여부를 지정합니다. 기본값은 **켜기**입니다.

- **인쇄 허용: 켜기**로 설정하면 사용자가 사용자 장치에서 액세스할 수 있는 모든 프린터로 인쇄할 수 있습니다. 기본값은 **끄기**입니다. 사용 가능: Android 9 이상.
- **USB 디버깅 허용:** 기본값은 **끄기**입니다.

- **앱**
  - **시스템 앱 사용:** 사용자가 사전 설치된 장치 앱을 실행할 수 있도록 허용합니다. 기본값은 **끄기**입니다. 특정 앱을 사용하려면 **시스템 앱 목록** 테이블에서 **추가**를 클릭합니다.
    - **시스템 앱 목록:** 장치에서 사용하도록 설정할 시스템 앱 목록입니다. **시스템 앱 사용**을 **켜기**로 설정하고 앱 패키지 이름을 추가합니다. 시스템 앱의 패키지 이름을 찾으려면 Android Debug Bridge(`adb`)를 사용하여 Android 패키지 관리자(`pm`) 명령을 호출할 수 있습니다. 예를 들어, `adb shell "pm list packages -f name"`와 같이 사용하며, 여기서 "name"은 패키지 이름의 일부입니다. 자세한 내용은 `<https://developer.android.com/studio/command-line/adb>`를 참조하십시오. Android Enterprise 장치의 경우 Android Enterprise 앱 권한 정책을 사용하여 앱 권한을 제한할 수 있습니다.
  - **애플리케이션 비활성화:** 지정된 앱 목록이 장치에서 실행되지 않도록 차단합니다. 기본값은 **끄기**입니다. 설치된 앱을 비활성화하려면 설정을 **켜기**로 변경한 다음 **애플리케이션 목록** 테이블에서 **추가**를 클릭합니다.
    - **애플리케이션 목록:** 차단하려는 앱 목록입니다. **애플리케이션 비활성화**를 **켜짐**으로 설정하고 앱을 추가합니다. 앱 패키지 이름을 입력합니다. 앱 목록을 변경하고 배포하면 이전 앱 목록이 덮어쓰여집니다. 예를 들어, com.example1과 com.example2를 비활성화한 다음 나중에 목록을 com.example1과 com.example3으로 변경하면 XenMobile은 com.example.2를 활성화합니다.
  - **앱 확인 사용:** OS가 앱을 스캔하여 악성 동작을 감지하도록 합니다. 기본값은 **켜짐**입니다.
  - **Google 앱 사용:** 사용자가 Google Mobile Services에서 기기로 앱을 다운로드할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
  - **Google Play 외 앱 허용:** Google Play 외 스토어에서 앱을 설치할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **사용자의 애플리케이션 설정 제어 허용:** 사용자가 앱을 제거하고, 앱을 비활성화하고, 캐시 및 데이터를 지우고, 모든 앱을 강제 종료하고, 기본값을 지울 수 있도록 허용합니다. 사용자는 설정 앱에서 이러한 작업을 수행합니다. 기본값은 **꺼짐**입니다.
  - **앱 제거 허용:** 사용자가 관리형 Google Play 스토어 내에서 앱을 제거할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. 이 설정을 표시하려면 서버 속성 `afw.restriction.policy.v2`을(를) 활성화하십시오. 서버 속성에 대한 자세한 내용은 서버 속성을(를) 참조하십시오.

- **업무 및 개인 프로필에서 이메일 앱 액세스**: 설정이 **켜짐**일 때 사용자가 개인 프로필에서 업무 프로필 이메일 앱에 액세스하고 사용할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.

- **BYOD 업무 프로필**
  - **홈 화면에 업무 프로필 앱 위젯 허용:** 이 설정이 **켜짐**이면 사용자는 기기 홈 화면에 업무 프로필 앱 위젯을 배치할 수 있습니다. 이 설정이 **꺼짐**이면 사용자는 기기 홈 화면에 업무 프로필 앱 위젯을 배치할 수 없습니다. 기본값은 **꺼짐**입니다.
    - **위젯이 허용된 앱:** 홈 화면에 허용하려는 앱 목록입니다. **홈 화면에 업무 프로필 앱 위젯 허용**을 **켜짐**으로 설정하고 앱을 추가합니다. **추가**를 클릭하고 목록에서 홈 화면에 위젯을 허용하려는 앱을 선택합니다. **저장**을 클릭합니다. 더 많은 앱 위젯을 허용하려면 이 과정을 반복합니다.
  - **기기 연락처에 업무 프로필 연락처 허용:** 수신 전화의 경우 관리형 Android Enterprise 프로필의 연락처를 상위 프로필에 표시합니다(Android 7.0 이상). 기본값은 **꺼짐**입니다.

- **완전히 관리되는 기기만 해당**
  - **사용자 추가 허용:** 사용자가 기기에 새 사용자를 추가할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
  - **데이터 로밍 허용:** 사용자가 로밍 중에 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐이며, 이는 사용자 기기에서 로밍을 비활성화합니다. 기본값은 **꺼짐**입니다.
  - **SMS 허용:** 사용자가 SMS 메시지를 보내고 받을 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **상태 표시줄 사용 허용: 켜짐**으로 설정하면 관리되는 장치 및 전용 장치(COSU 장치라고도 함)에서 상태 표시줄을 활성화합니다. 이 설정은 전체 화면 모드에서 벗어날 수 있게 하는 알림, 빠른 설정 및 기타 화면 오버레이를 비활성화합니다. 사용자는 시스템 설정으로 이동하여 알림을 볼 수 있습니다. Android 6.0 이상에서 사용할 수 있습니다. 기본값은 **꺼짐**입니다.
  - **Bluetooth 허용:** 사용자가 Bluetooth를 사용할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
    - **Bluetooth 공유 허용:** 선택하지 않으면 사용자는 장치에서 Bluetooth를 통한 외부 공유를 설정할 수 없습니다. 기본값은 선택됨입니다. 이 설정을 표시하려면 서버 속성 `afw.restriction.policy.v2`을 활성화하십시오. 서버 속성에 대한 자세한 내용은 서버 속성을 참조하십시오.
  - **날짜 및 시간 구성 허용:** 사용자가 장치에서 날짜와 시간을 변경할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
  - **초기화 허용:** 사용자가 장치를 초기화할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
  - **장치 화면 켜짐 유지:** 이 설정을 **켜짐**으로 설정하면 장치가 연결되어 있을 때 장치 화면이 계속 켜져 있습니다. 기본값은 **꺼짐**입니다.

- **USB 대용량 저장소 허용:** 사용자 장치와 컴퓨터 간에 USB 연결을 통해 대용량 데이터 파일을 전송할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **마이크 허용:** 사용자가 장치에서 마이크를 사용할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **테더링 허용:** 사용자가 휴대용 핫스팟을 구성하고 데이터를 테더링할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
- **키가드가 장치를 잠그지 않도록 유지: 켜짐**으로 설정하면 관리되는 장치 및 전용 장치(COSU 장치라고도 함)의 잠금 화면에서 키가드를 비활성화합니다. 기본값은 **꺼짐**입니다.
- **Wi-Fi 변경 허용: 켜짐**으로 설정하면 사용자는 Wi-Fi를 켜거나 끄고 Wi-Fi 네트워크에 연결할 수 있습니다. 기본값은 **켜짐**입니다.
- **파일 전송 허용:** USB를 통한 파일 전송을 허용합니다. 기본값은 **꺼짐**입니다.

- **삼성**
  - **TIMA 키 저장소 활성화:** TIMA 키 저장소는 대칭 키에 대해 TrustZone 기반의 보안 키 저장소를 제공합니다. RSA 키 쌍 및 인증서는 저장을 위해 기본 키 저장소 공급자로 라우팅됩니다. 기본값은 **꺼짐**입니다.
  - **공유 목록 허용:** 사용자가 공유 목록의 앱 간에 콘텐츠를 공유할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
  - **감사 로그 사용:** 장치 포렌식 분석을 위한 이벤트 감사 로그 생성을 활성화합니다. 기본값은 **해제**입니다.

- **Samsung: 완전 관리형 장치만 해당**
  - **ODE 신뢰 부팅 확인 사용:** 부트로더에서 시스템 이미지까지 신뢰 체인을 설정하기 위해 ODE 신뢰 부팅 확인을 사용합니다. 기본값은 **설정**입니다.
  - **긴급 통화만 허용:** 사용자가 장치에서 긴급 통화 전용 모드를 활성화하도록 허용합니다. 기본값은 **해제**입니다.
  - **펌웨어 복구 허용:** 사용자가 장치에서 펌웨어를 복구하도록 허용합니다. 기본값은 **설정**입니다.
  - **빠른 암호화 허용:** 사용된 메모리 공간만 암호화하도록 허용합니다. 이 암호화는 모든 데이터를 암호화하는 전체 디스크 암호화와 대조됩니다. 해당 데이터에는 설정, 애플리케이션 데이터, 다운로드된 파일 및 애플리케이션, 미디어 및 기타 파일이 포함됩니다. 기본값은 **설정**입니다.
  - **공통 평가 기준 모드 사용:** 장치를 공통 평가 기준 모드로 전환합니다. 공통 평가 기준 구성은 엄격한 보안 프로세스를 적용합니다. 기본값은 **설정**입니다.
  - **재부팅 배너 사용:** 사용자의 장치가 다시 시작될 때 DoD 승인 시스템 사용 알림 메시지 또는 배너를 표시합니다. 기본값은 **해제**입니다.

- **설정 변경 허용:** 사용자가 완전 관리형 장치에서 설정을 변경하도록 허용합니다. 기본값은 **설정**입니다.
- **백그라운드 데이터 사용 사용:** 완전 관리형 장치에서 앱이 백그라운드에서 데이터를 동기화하도록 허용합니다. 기본값은 **설정**입니다.
- **클립보드 허용:** 사용자가 장치에서 클립보드로 데이터를 복사하도록 허용합니다.
  - **클립보드 공유 허용:** 사용자가 장치와 컴퓨터 간에 클립보드 콘텐츠를 공유하도록 허용합니다(MDM 4.0 이상).
- **홈 키 허용:** 사용자가 완전 관리형 장치에서 **홈** 키를 사용하도록 허용합니다. 기본값은 **설정**입니다.
- **모의 위치 허용:** 사용자가 GPS 위치를 위조하도록 허용합니다. 완전 관리형 장치에 해당합니다. 기본값은 **해제**입니다.
- **NFC:** 사용자가 완전 관리형 장치에서 NFC를 사용하도록 허용합니다(MDM 3.0 이상). 기본값은 **설정**입니다.
- **전원 끄기 허용:** 사용자가 완전히 관리되는 장치의 전원을 끌 수 있도록 허용합니다(MDM 3.0 이상). 기본값은 **켜짐**입니다.
- **Wi-Fi Direct 허용:** 사용자가 Wi-Fi 연결을 통해 다른 장치에 직접 연결할 수 있도록 허용합니다. 기본값은 **켜짐**입니다. **켜짐**으로 설정된 경우, **Wi-Fi 변경 허용** 설정을 활성화해야 합니다.
- **SD 카드 허용:** 사용자가 장치에서 SD 카드를 사용할 수 있도록 허용합니다(사용 가능한 경우). 기본값은 **켜짐**입니다.
- **USB 호스트 저장소 허용:** USB 장치가 사용자의 장치에 연결될 때 사용자의 장치가 USB 호스트 역할을 하도록 허용합니다. 그러면 사용자의 장치가 USB 장치에 전원을 공급합니다. 기본값은 **켜짐**입니다.
- **음성 다이얼러 허용:** 사용자가 장치에서 음성 다이얼러를 사용할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜짐**입니다.
- **S 빔 허용:** 사용자가 NFC 및 Wi-Fi Direct를 사용하여 다른 사람과 콘텐츠를 공유할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜짐**입니다.
- **S 보이스 허용:** 사용자가 장치에서 지능형 개인 비서 및 지식 탐색기를 사용할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜짐**입니다.
- **USB 테더링 허용:** 사용자가 USB 연결을 사용하여 모바일 데이터 연결을 다른 장치와 공유할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **테더링 허용** 설정도 **켜짐**으로 설정되어야 합니다.
- **Bluetooth 테더링 허용:** 사용자가 Bluetooth 연결을 사용하여 모바일 데이터 연결을 다른 장치와 공유할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **테더링 허용** 설정도 **켜짐**으로 설정되어야 합니다.

    - **Bluetooth 공유 허용:** 선택 취소된 경우, 사용자는 장치에서 Bluetooth를 통한 외부 공유를 설정할 수 없습니다. 기본값은 선택됨입니다. 이 설정을 표시하려면 서버 속성 `afw.restriction.policy.v2`을(를) 활성화하십시오. 서버 속성에 대한 자세한 내용은 서버 속성을(를) 참조하십시오.

- **Wi-Fi 테더링 허용:** 사용자가 Wi-Fi 연결을 사용하여 모바일 데이터 연결을 다른 장치와 공유할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **테더링 허용** 설정도 **켜짐**으로 설정되어야 합니다.
- **수신 MMS 허용:** 사용자가 MMS 메시지를 수신할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **SMS 허용** 설정을 켜야 합니다.
- **발신 MMS 허용:** 사용자가 MMS 메시지를 보낼 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **SMS 허용** 설정을 켜야 합니다.
- **수신 SMS 허용:** 사용자가 SMS 메시지를 수신할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **SMS 허용** 설정을 켜야 합니다.
- **발신 SMS 허용:** 사용자가 SMS 메시지를 보낼 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **SMS 허용** 설정을 켜야 합니다.
- **모바일 네트워크 구성:** 사용자가 셀룰러 데이터 연결을 사용할 수 있도록 허용합니다. 기본값은 **끄기**입니다.
- **일별 제한(MB):** 사용자가 매일 사용할 수 있는 모바일 데이터의 MB 수를 입력합니다. 기본값은 0이며, 이 경우 이 기능이 비활성화됩니다(MDM 4.0 이상).
- **주별 제한(MB):** 사용자가 매주 사용할 수 있는 모바일 데이터의 MB 수를 입력합니다. 기본값은 0이며, 이 경우 이 기능이 비활성화됩니다(MDM 4.0 이상).
- **월별 제한(MB):** 사용자가 매월 사용할 수 있는 모바일 데이터의 MB 수를 입력합니다. 기본값은 0이며, 이 경우 이 기능이 비활성화됩니다(MDM 4.0 이상).
- **보안 VPN 연결만 허용:** 사용자가 보안 연결만 사용할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜기**입니다.
- **오디오 녹음 허용:** 사용자가 장치로 오디오를 녹음할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜기**입니다. **켜기**로 설정된 경우 **마이크 허용** 설정을 켜야 합니다.
- **비디오 녹화 허용:** 사용자가 장치로 비디오를 녹화할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **끄기**입니다. **켜기**로 설정된 경우 **카메라 사용 허용** 설정을 켜야 합니다.
- **로밍 시 푸시 메시지 허용:** 사용자가 푸시를 위해 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 **끄기**입니다. **켜기**로 설정된 경우 **데이터 로밍 허용** 설정을 활성화해야 합니다.
- **로밍 시 자동 동기화 허용:** 사용자가 동기화를 위해 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 **끄기**입니다. **켜기**로 설정된 경우 **데이터 로밍 허용** 설정을 활성화해야 합니다.

  - **로밍 시 음성 통화 허용:** 사용자가 음성 통화를 위해 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 **끄기**입니다. **켜기**로 설정된 경우 **데이터 로밍 허용** 설정을 활성화해야 합니다.

- **Samsung: Knox 컨테이너/완전 관리형 장치**
  - **해지 확인 활성화:** 해지된 인증서 확인을 활성화합니다. 기본값은 **끄기**입니다.
- **Samsung: Knox 컨테이너만**
  - **앱을 컨테이너로 이동:** 사용자가 Knox 컨테이너와 장치의 개인 영역 간에 앱을 이동할 수 있도록 허용합니다. 기본값은 **켜기**입니다.
  - **다단계 인증 적용:** 사용자는 장치를 열기 위해 지문과 암호 또는 PIN과 같은 다른 인증 방법 중 하나를 사용해야 합니다. 기본값은 **켜기**입니다.
  - **컨테이너 인증 적용:** 장치 잠금 해제에 사용된 방법과 다른 인증 방법을 사용하여 KNOX 컨테이너를 엽니다. 기본값은 **켜짐**입니다.
  - **보안 키패드 사용:** Knox 컨테이너 내에서 사용자가 보안 키보드를 사용하도록 강제합니다. 기본값은 **켜짐**입니다.
- **삼성: DeX**
  - **Samsung DeX 사용:** 지원되는 Knox 지원 장치가 Samsung DeX 모드에서 실행되도록 합니다. Samsung Knox 3.1(최소 버전)이 필요합니다. 기본값은 **켜짐**입니다. Samsung DeX 장치 요구 사항 및 Samsung DeX 설정에 대한 자세한 내용은 Samsung 개발자 설명서를 참조하십시오.
    - **DeX 모드에서만 이더넷 허용:** Samsung DeX 모드에서 이더넷 사용을 허용합니다. DeX 모드에서는 셀룰러 데이터, Wi-Fi 및 테더링(Wi-Fi, Bluetooth 및 USB)이 제한됩니다. 기본값은 선택 해제됨입니다.
    - **DeX 로고 이미지 업로드:** Samsung DeX의 아이콘으로 사용할 .png 이미지를 지정하려면 이 설정을 선택합니다.
    - **DeX 화면 시간 초과(초):** DeX 화면이 꺼지기까지의 유휴 시간을 초 단위로 지정합니다. 시간 초과를 비활성화하려면 **0**을 입력합니다. 기본값은 **1200**초(20분)입니다.
    - **Samsung DeX에 앱 바로 가기 추가:** 앱의 바로 가기를 DeX에 추가할 앱 패키지 이름을 지정합니다. 앱 패키지 이름을 찾으려면 Google Play로 이동하여 앱을 선택합니다. URL에 패키지 이름이 포함되어 있습니다: `https://play.google.com/store/apps/details?id=<package.name>`.
    - **Samsung DeX에서 앱 바로 가기 제거:** DeX에서 바로 가기를 제거할 앱 패키지 이름을 지정합니다. 앱 패키지 이름을 찾으려면 Google Play로 이동합니다.

- **Samsung DeX에서 비활성화할 앱 패키지:** Samsung DeX 모드에서 차단하려는 앱 패키지를 쉼표로 구분하여 지정합니다. 예: `"com.android.chrome", "com.google.android.gm"`.

작업 프로필이 있는 완전 관리형 장치에 적용이 켜져 있고 **작업 프로필이 있는 완전 관리형 장치의 경우 정책을 다음 위치에 적용**이 **작업 프로필**로 설정된 경우 다음 설정을 구성합니다.

- **보안**
  - **계정 관리 허용:** 작업 프로필 및 관리되는 장치에 계정을 추가할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **프로필 간 복사 및 붙여넣기 허용: 켜짐**으로 설정하면 사용자는 Android Enterprise 프로필의 앱과 개인 영역의 앱 간에 복사 및 붙여넣기를 할 수 있습니다. 기본값은 **꺼짐**입니다.
  - **화면 캡처 허용:** 사용자가 장치 화면을 녹화하거나 화면 캡처를 할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **카메라 사용 허용:** 사용자가 장치 카메라로 사진을 찍고 비디오를 만들 수 있도록 허용합니다. 기본값은 **끄기**입니다.
  - **위치 공급자 구성 허용:** 사용자가 장치에서 GPS를 켤 수 있도록 허용합니다. Android API 28 이상에서 지원됩니다. 기본값은 **켜기**입니다.
  - **위치 공유 허용:** 관리되는 프로필의 경우 장치 소유자가 이 설정을 재정의할 수 있습니다. 기본값은 **끄기**입니다.

    > **팁:**
    >
    > XenMobile에서 위치 장치 정책을 생성하여 지리적 경계를 적용할 수 있습니다. 위치 장치 정책을 참조하십시오.

  - **사용자가 사용자 자격 증명을 구성하도록 허용:** 사용자가 관리되는 키 저장소에서 자격 증명을 구성할 수 있는지 여부를 지정합니다. 기본값은 **켜기**입니다.
  - **인쇄 허용: 켜기**로 설정하면 사용자가 사용자 장치에서 액세스할 수 있는 모든 프린터로 인쇄할 수 있습니다. 기본값은 **끄기**입니다. 지원 버전: Android 9 이상.
- **앱**
  - **시스템 앱 사용:** 사용자가 사전 설치된 장치 앱을 실행할 수 있도록 허용합니다. 기본값은 **끄기**입니다. 특정 앱을 사용하려면 **시스템 앱 목록** 테이블에서 **추가**를 클릭합니다.

- **시스템 앱 목록:** 장치에서 사용하려는 시스템 앱 목록입니다. **시스템 앱 사용**을 **켜기**로 설정하고 앱 패키지 이름을 추가합니다. 시스템 앱의 패키지 이름을 찾으려면 Android Debug Bridge (`adb`)를 사용하여 Android 패키지 관리자 (`pm`) 명령을 호출할 수 있습니다. 예를 들어, `adb shell "pm list packages -f name"`와 같이 "name"이 패키지 이름의 일부인 경우입니다. 자세한 내용은 `<https://developer.android.com/studio/command-line/adb>`를 참조하십시오. Android Enterprise 장치의 경우 Android Enterprise 앱 권한 정책을 사용하여 앱 권한을 제한할 수 있습니다.

- **응용 프로그램 비활성화:** 지정된 앱 목록이 장치에서 실행되지 않도록 차단합니다. 기본값은 **끄기**입니다. 설치된 앱을 비활성화하려면 설정을 **켜기**로 변경한 다음 **응용 프로그램 목록** 테이블에서 **추가**를 클릭합니다.

  - **응용 프로그램 목록:** 차단하려는 앱 목록입니다. **응용 프로그램 비활성화**를 **켜기**로 설정하고 앱을 추가합니다. 앱 패키지 이름을 입력합니다. 앱 목록을 변경하고 배포하면 이전 앱 목록이 덮어쓰여집니다. 예를 들어, com.example1 및 com.example2를 비활성화한 다음 나중에 목록을 com.example1 및 com.example3으로 변경하면 XenMobile은 com.example.2를 활성화합니다.

- **앱 확인 사용:** OS가 앱을 스캔하여 악성 동작을 감지할 수 있도록 합니다. 기본값은 **켜기**입니다.
- **Google 앱 사용:** 사용자가 Google Mobile Services에서 장치로 앱을 다운로드할 수 있도록 허용합니다. 기본값은 **켜기**입니다.
- **비 Google Play 앱 허용:** Google Play 외의 스토어에서 앱을 설치할 수 있도록 허용합니다. 기본값은 **끄기**입니다.
- **사용자에게 애플리케이션 설정 제어 허용:** 사용자가 앱을 제거하고, 앱을 비활성화하고, 캐시 및 데이터를 지우고, 모든 앱을 강제 중지하고, 기본값을 지울 수 있도록 허용합니다. 사용자는 설정 앱에서 이러한 작업을 수행합니다. 기본값은 **끔**입니다.
- **앱 제거 허용:** 사용자가 Managed Google Play 스토어 내에서 앱을 제거할 수 있도록 허용합니다. 기본값은 **끔**입니다. 이 설정을 표시하려면 서버 속성 `afw.restriction.policy.v2`을(를) 활성화하십시오. 서버 속성에 대한 자세한 내용은 서버 속성을(를) 참조하십시오.
- **업무 및 개인 프로필에서 이메일 앱 액세스:** 설정이 **켬**일 때 사용자가 개인 프로필에서 업무 프로필 이메일 앱에 액세스하고 사용할 수 있도록 허용합니다. 기본값은 **끔**입니다.

- **BYOD 업무 프로필**

  - **홈 화면에 업무 프로필 앱 위젯 허용:** 이 설정이 **켬**이면 사용자는 장치 홈 화면에 업무 프로필 앱 위젯을 배치할 수 있습니다. 이 설정이 **끔**이면 사용자는 장치 홈 화면에 업무 프로필 앱 위젯을 배치할 수 없습니다. 기본값은 **끔**입니다.

    - **허용된 위젯이 있는 앱:** 홈 화면에 허용할 앱 목록입니다. **홈 화면에 업무 프로필 앱 위젯 허용**을 **켬**으로 설정하고 앱을 추가합니다. **추가**를 클릭하고 목록에서 홈 화면에 위젯을 허용할 앱을 선택합니다. **저장**을 클릭합니다. 더 많은 앱 위젯을 허용하려면 이 과정을 반복합니다.
  - **장치 연락처에 업무 프로필 연락처 허용:** 수신 전화의 경우 관리되는 Android Enterprise 프로필의 연락처를 상위 프로필에 표시합니다(Android 7.0 이상). 기본값은 **끔**입니다.

- **삼성**
  - **TIMA 키 저장소 활성화:** 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 **끔**입니다.
  - **공유 목록 허용:** 사용자가 공유 목록의 앱 간에 콘텐츠를 공유할 수 있도록 허용합니다. 기본값은 **켬**입니다.
  - **감사 로그 활성화:** 장치 포렌식 분석을 위한 이벤트 감사 로그 생성을 활성화합니다. 기본값은 **끔**입니다.
- **Samsung: Knox 컨테이너/완전 관리형 장치**
  - **해지 확인 활성화:** 해지된 인증서 확인을 활성화합니다. 기본값은 **끔**입니다.
- **Samsung: Knox 컨테이너만**
  - **앱을 컨테이너로 이동:** 사용자가 Knox 컨테이너와 장치의 개인 영역 간에 앱을 이동할 수 있도록 허용합니다. 기본값은 **켬**입니다.
  - **다단계 인증 적용:** 사용자는 장치를 열려면 지문과 암호 또는 PIN과 같은 다른 인증 방법 중 하나를 사용해야 합니다. 기본값은 **켜짐**입니다.
  - **컨테이너에 대한 인증 적용:** 장치 잠금 해제에 사용된 방법과 다른 인증 방법을 사용하여 KNOX 컨테이너를 엽니다. 기본값은 **켜짐**입니다.
  - **보안 키패드 사용:** 사용자가 Knox 컨테이너 내에서 보안 키보드를 사용하도록 강제합니다. 기본값은 **켜짐**입니다.

작업 프로필이 있는 완전 관리형 장치에 적용이 켜져 있고 **작업 프로필이 있는 완전 관리형 장치의 경우 정책을 다음 위치에 적용**이 **관리형 장치**로 설정된 경우 다음 설정을 구성합니다.

- **보안**
  - **계정 관리 허용:** 작업 프로필 및 관리형 장치에 계정을 추가할 수 있습니다. 기본값은 **꺼짐**입니다.
  - **교차 프로필 복사 및 붙여넣기 허용: 켜짐**으로 설정하면 사용자는 Android Enterprise 프로필의 앱과 개인 영역의 앱 간에 복사 및 붙여넣기를 할 수 있습니다. 기본값은 **꺼짐**입니다.

- **화면 캡처 허용:** 사용자가 장치 화면을 녹화하거나 화면 캡처를 할 수 있습니다. 기본값은 **꺼짐**입니다.
- **카메라 사용 허용:** 사용자가 장치 카메라로 사진을 찍고 비디오를 만들 수 있습니다. 기본값은 **꺼짐**입니다.
- **VPN 구성 허용:** 사용자가 VPN 구성을 생성할 수 있습니다. Android 6 이상을 실행하는 작업 프로필 장치 및 완전 관리형 장치에 해당합니다. 기본값은 **켜짐**입니다.
- **백업 서비스 허용:** 사용자가 장치의 애플리케이션 및 시스템 데이터를 백업할 수 있습니다. 기본값은 **켜짐**입니다.
- **NFC 허용:** 사용자가 근거리 무선 통신(NFC)을 사용하여 웹 페이지, 사진, 비디오 또는 기타 콘텐츠를 자신의 장치에서 다른 장치로 보낼 수 있습니다. MDM 4.0 이상에 해당합니다. 기본값은 **켜짐**입니다.
- **위치 공급자 구성 허용:** 사용자가 장치에서 GPS를 켤 수 있습니다. Android API 28 이상에 해당합니다. 기본값은 **켜짐**입니다.
- **위치 공유 허용:** 관리형 프로필의 경우 장치 소유자가 이 설정을 재정의할 수 있습니다. 기본값은 **꺼짐**입니다.

  > **팁:**
  >
  > XenMobile에서 지리적 경계를 적용하기 위해 위치 장치 정책을 생성할 수 있습니다. 위치 장치 정책을 참조하십시오.

- **사용자가 사용자 자격 증명을 구성하도록 허용:** 관리되는 키 저장소에서 사용자가 자격 증명을 구성할 수 있는지 여부를 지정합니다. 기본값은 **켜짐**입니다.
- **인쇄 허용: 켜짐**으로 설정하면 사용자는 사용자 장치에서 액세스할 수 있는 모든 프린터로 인쇄할 수 있습니다. 기본값은 **꺼짐**입니다. 사용 가능: Android 9 이상.
- **USB 디버깅 허용:** 기본값은 **꺼짐**입니다.

- **앱**
  - **시스템 앱 사용:** 사용자가 사전 설치된 장치 앱을 실행할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. 특정 앱을 사용하려면 **시스템 앱 목록** 테이블에서 **추가**를 클릭합니다.
    - **시스템 앱 목록:** 장치에서 사용하려는 시스템 앱 목록입니다. **시스템 앱 사용**을 **켜짐**으로 설정하고 앱 패키지 이름을 추가합니다. 시스템 앱의 패키지 이름을 찾으려면 Android Debug Bridge (`adb`)를 사용하여 Android 패키지 관리자 (`pm`) 명령을 호출할 수 있습니다. 예를 들어, `adb shell "pm list packages -f name"`와 같이 "name"이 패키지 이름의 일부입니다.

자세한 내용은 `<https://developer.android.com/studio/command-line/adb>`를 참조하십시오. Android Enterprise 장치의 경우 Android Enterprise 앱 권한 정책을 사용하여 앱 권한을 제한할 수 있습니다.

- **응용 프로그램 비활성화:** 지정된 앱 목록이 장치에서 실행되지 않도록 차단합니다. 기본값은 **꺼짐**입니다. 설치된 앱을 비활성화하려면 설정을 **켜짐**으로 변경한 다음 **응용 프로그램 목록** 테이블에서 **추가**를 클릭합니다.
  - **응용 프로그램 목록:** 차단하려는 앱 목록입니다. **응용 프로그램 비활성화**를 **켜짐**으로 설정하고 앱을 추가합니다. 앱 패키지 이름을 입력합니다. 앱 목록을 변경하고 배포하면 이전 앱 목록이 덮어쓰여집니다. 예를 들어, com.example1과 com.example2를 비활성화한 다음 나중에 목록을 com.example1과 com.example3으로 변경하면 XenMobile은 com.example.2를 활성화합니다.
- **앱 확인 사용:** OS가 앱을 스캔하여 악성 동작을 감지할 수 있도록 합니다. 기본값은 **켜짐**입니다.
- **Google 앱 사용:** 사용자가 Google Mobile Services에서 장치로 앱을 다운로드할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **Google Play 외 앱 허용:** Google Play 외 스토어에서 앱을 설치할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
- **사용자의 응용 프로그램 설정 제어 허용:** 사용자가 앱을 제거하고, 앱을 비활성화하고, 캐시 및 데이터를 지우고, 모든 앱을 강제 중지하고, 기본값을 지울 수 있도록 허용합니다. 사용자는 설정 앱에서 이러한 작업을 수행합니다. 기본값은 **꺼짐**입니다.
- **앱 제거 허용:** 사용자가 Managed Google Play 스토어 내에서 앱을 제거할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. 이 설정을 표시하려면 서버 속성 `afw.restriction.policy.v2`을 활성화하십시오. 서버 속성에 대한 자세한 내용은 서버 속성를 참조하십시오.

- **완전히 관리되는 장치만 해당**
  - **사용자 추가 허용:** 사용자가 장치에 새 사용자를 추가할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
  - **데이터 로밍 허용:** 사용자가 로밍 중에 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 꺼짐이며, 이는 사용자 장치에서 로밍을 비활성화합니다. 기본값은 **꺼짐**입니다.
  - **SMS 허용:** 사용자가 SMS 메시지를 주고받을 수 있도록 허용합니다. 기본값은 **꺼짐**입니다.
  - **상태 표시줄 사용 허용: 켜짐**으로 설정하면 이 설정은 관리되는 장치 및 전용 장치(COSU 장치라고도 함)에서 상태 표시줄을 활성화합니다. 이 설정은 전체 화면 모드에서 벗어날 수 있는 알림, 빠른 설정 및 기타 화면 오버레이를 비활성화합니다. 사용자는 시스템 설정으로 이동하여 알림을 볼 수 있습니다. Android 6.0 이상용입니다. 기본값은 **꺼짐**입니다.
  - **Bluetooth 허용:** 사용자가 Bluetooth를 사용할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.

  - **Bluetooth 공유 허용:** 선택 취소하면 사용자는 장치에서 Bluetooth 공유를 설정할 수 없습니다. 기본값은 선택됨입니다. 이 설정을 표시하려면 서버 속성 `afw.restriction.policy.v2`을(를) 활성화하십시오. 서버 속성에 대한 자세한 내용은 서버 속성을(를) 참조하십시오.

- **날짜 및 시간 구성 허용:** 사용자가 장치에서 날짜와 시간을 변경할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **공장 초기화 허용:** 사용자가 장치를 공장 초기화할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **장치 화면 켜짐 유지:** 이 설정이 **켜짐**으로 설정되면 장치가 연결되어 있을 때 장치 화면이 계속 켜져 있습니다. 기본값은 **꺼짐**입니다.
- **USB 대용량 저장소 허용:** 사용자의 장치와 컴퓨터 간에 USB 연결을 통해 대용량 데이터 파일을 전송할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **마이크 허용:** 사용자가 장치에서 마이크를 사용할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **테더링 허용:** 사용자가 휴대용 핫스팟을 구성하고 데이터를 테더링할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. 이 설정이 켜져 있으면 다음 설정이 Samsung 장치에서 사용할 수 있습니다.
- **키가드가 장치를 잠그지 못하게 함: 켜짐**으로 설정하면 이 설정은 관리되는 장치 및 전용 장치(COSU 장치라고도 함)의 잠금 화면에서 키가드를 비활성화합니다. 기본값은 **꺼짐**입니다.
- **Wi-Fi 변경 허용: 켜짐**으로 설정하면 사용자는 Wi-Fi를 켜거나 끄고 Wi-Fi 네트워크에 연결할 수 있습니다. 기본값은 **켜짐**입니다.
- **파일 전송 허용:** USB를 통한 파일 전송을 허용합니다. 기본값은 **꺼짐**입니다.

- **삼성**
  - **TIMA 키 저장소 활성화:** TIMA 키 저장소는 대칭 키에 대해 TrustZone 기반의 보안 키 저장을 제공합니다. RSA 키 쌍 및 인증서는 저장을 위해 기본 키 저장소 공급자로 라우팅됩니다. 기본값은 **해제**입니다.
  - **공유 목록 허용:** 사용자가 공유 목록에서 앱 간에 콘텐츠를 공유할 수 있도록 허용합니다. 기본값은 **설정**입니다.
  - **감사 로그 활성화:** 장치의 포렌식 분석을 위한 이벤트 감사 로그 생성을 활성화합니다. 기본값은 **해제**입니다.

- **Samsung: 완전 관리형 장치만 해당**
  - **ODE 신뢰 부팅 확인 활성화:** ODE 신뢰 부팅 확인을 사용하여 부트로더에서 시스템 이미지까지 신뢰 체인을 설정합니다. 기본값은 **설정**입니다.
  - **긴급 통화만 허용:** 사용자가 장치에서 긴급 통화 전용 모드를 활성화할 수 있도록 허용합니다. 기본값은 **해제**입니다.
  - **펌웨어 복구 허용:** 사용자가 장치에서 펌웨어를 복구할 수 있도록 허용합니다. 기본값은 **설정**입니다.

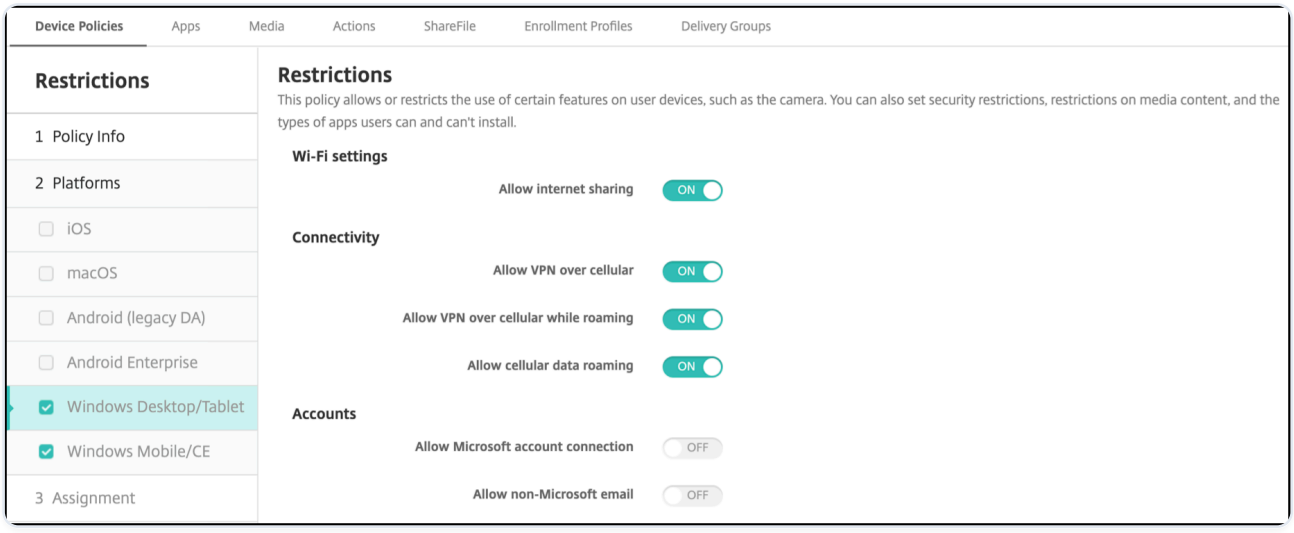
- **빠른 암호화 허용:** 사용된 메모리 공간만 암호화할 수 있도록 허용합니다. 이 암호화는 모든 데이터를 암호화하는 전체 디스크 암호화와 대조됩니다. 해당 데이터에는 설정, 애플리케이션 데이터, 다운로드된 파일 및 애플리케이션, 미디어 및 기타 파일이 포함됩니다. 기본값은 **설정**입니다.
- **공통 평가 기준 모드 활성화:** 장치를 공통 평가 기준 모드로 전환합니다. 공통 평가 기준 구성은 엄격한 보안 프로세스를 적용합니다. 기본값은 **설정**입니다.
- **재부팅 배너 활성화:** 사용자의 장치가 다시 시작될 때 DoD 승인 시스템 사용 알림 메시지 또는 배너를 표시합니다. 기본값은 **해제**입니다.
- **설정 변경 허용:** 사용자가 완전 관리형 장치에서 설정을 변경할 수 있도록 허용합니다. 기본값은 **설정**입니다.
- **백그라운드 데이터 사용 활성화:** 앱이 백그라운드에서 데이터를 동기화할 수 있도록 허용합니다. 완전 관리형 장치에 해당합니다. 기본값은 **설정**입니다.
- **클립보드 허용:** 사용자가 장치에서 클립보드로 데이터를 복사할 수 있도록 허용합니다. 기본값은 **설정**입니다.
  - **클립보드 공유 허용:** 사용자가 장치와 컴퓨터 간에 클립보드 콘텐츠를 공유할 수 있도록 허용합니다(MDM 4.0 이상).
- **홈 키 허용:** 사용자가 완전 관리형 기기에서 **홈** 키를 사용할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
- **모의 위치 허용:** 사용자가 GPS 위치를 위조할 수 있도록 허용합니다. 완전 관리형 기기용입니다. 기본값은 **꺼짐**입니다.
- **NFC:** 사용자가 완전 관리형 기기에서 NFC를 사용할 수 있도록 허용합니다(MDM 3.0 이상). 기본값은 **켜짐**입니다.
- **전원 끄기 허용:** 사용자가 완전 관리형 기기의 전원을 끌 수 있도록 허용합니다(MDM 3.0 이상). 기본값은 **켜짐**입니다.
- **Wi-Fi Direct 허용:** 사용자가 Wi-Fi 연결을 통해 다른 기기에 직접 연결할 수 있도록 허용합니다. 기본값은 **켜짐**입니다. **켜짐**으로 설정된 경우, **Wi-Fi 변경 허용** 설정을 활성화해야 합니다.
- **SD 카드 허용:** 사용자가 기기에서 SD 카드를 사용할 수 있도록 허용합니다(사용 가능한 경우). 기본값은 **켜짐**입니다.
- **USB 호스트 저장소 허용:** USB 기기가 사용자의 기기에 연결될 때 사용자의 기기가 USB 호스트 역할을 하도록 허용합니다. 그러면 사용자의 기기가 USB 기기에 전원을 공급합니다. 기본값은 **켜짐**입니다.
- **음성 다이얼러 허용:** 사용자가 기기에서 음성 다이얼러를 사용할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜짐**입니다.

- **S 빔 허용:** 사용자가 NFC 및 Wi-Fi Direct를 사용하여 다른 사람과 콘텐츠를 공유할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜짐**입니다.
- **S 보이스 허용:** 사용자가 기기에서 지능형 개인 비서 및 지식 내비게이터를 사용할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켜짐**입니다.
- **USB 테더링 허용:** 사용자가 USB 연결을 사용하여 다른 기기와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **테더링 허용** 설정도 **켜짐**으로 설정해야 합니다.
- **Bluetooth 테더링 허용:** 사용자가 Bluetooth 연결을 사용하여 다른 기기와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **테더링 허용** 설정도 **켜짐**으로 설정해야 합니다.
- **Wi-Fi 테더링 허용:** 사용자가 Wi-Fi 연결을 사용하여 다른 기기와 모바일 데이터 연결을 공유할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **테더링 허용** 설정도 **켜짐**으로 설정해야 합니다.
- **수신 MMS 허용:** 사용자가 MMS 메시지를 수신할 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **SMS 허용** 설정을 켜야 합니다.
- **발신 MMS 허용:** 사용자가 MMS 메시지를 보낼 수 있도록 허용합니다. 기본값은 **꺼짐**입니다. **켜짐**으로 설정된 경우, **SMS 허용** 설정을 켜야 합니다.
- **수신 SMS 허용:** 사용자가 SMS 메시지를 수신할 수 있도록 허용합니다. 기본값은 **끔**입니다. **켬**인 경우 **SMS 허용** 설정을 켜야 합니다.
- **발신 SMS 허용:** 사용자가 SMS 메시지를 보낼 수 있도록 허용합니다. 기본값은 **끔**입니다. **켬**인 경우 **SMS 허용** 설정을 켜야 합니다.
- **모바일 네트워크 구성:** 사용자가 셀룰러 데이터 연결을 사용할 수 있도록 허용합니다. 기본값은 **끔**입니다.
- **일별 제한(MB):** 사용자가 매일 사용할 수 있는 모바일 데이터의 MB 수를 입력합니다. 기본값은 0이며, 이 경우 이 기능이 비활성화됩니다(MDM 4.0 이상).
- **주별 제한(MB):** 사용자가 매주 사용할 수 있는 모바일 데이터의 MB 수를 입력합니다. 기본값은 0이며, 이 경우 이 기능이 비활성화됩니다(MDM 4.0 이상).
- **월별 제한(MB):** 사용자가 매월 사용할 수 있는 모바일 데이터의 MB 수를 입력합니다. 기본값은 0이며, 이 경우 이 기능이 비활성화됩니다(MDM 4.0 이상).
- **보안 VPN 연결만 허용:** 사용자가 보안 연결만 사용할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켬**입니다.
- **오디오 녹음 허용:** 사용자가 장치로 오디오를 녹음할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **켬**입니다. **켬**인 경우 **마이크 허용** 설정을 켜야 합니다.

- **비디오 녹화 허용:** 사용자가 장치로 비디오를 녹화할 수 있도록 허용합니다(MDM 4.0 이상). 기본값은 **끔**입니다. **켬**인 경우 **카메라 사용 허용** 설정을 켜야 합니다.
- **로밍 시 푸시 메시지 허용:** 사용자가 푸시를 위해 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 **끔**입니다. **켬**인 경우 **데이터 로밍 허용** 설정을 활성화해야 합니다.
- **로밍 시 자동 동기화 허용:** 사용자가 동기화를 위해 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 **끔**입니다. **켬**인 경우 **데이터 로밍 허용** 설정을 활성화해야 합니다.
- **로밍 시 음성 통화 허용:** 사용자가 음성 통화를 위해 셀룰러 데이터를 사용할 수 있도록 허용합니다. 기본값은 **끔**입니다. **켬**인 경우 **데이터 로밍 허용** 설정을 활성화해야 합니다.

- **Samsung: Knox 컨테이너/완전 관리형 장치**
  - **해지 확인 사용:** 해지된 인증서 확인을 활성화합니다. 기본값은 **끔**입니다.
- **Samsung: Knox 컨테이너만**
  - **앱을 컨테이너로 이동:** 사용자가 장치의 Knox 컨테이너와 개인 영역 간에 앱을 이동할 수 있도록 허용합니다. 기본값은 **켜짐**입니다.
  - **다단계 인증 적용:** 사용자는 장치를 열기 위해 지문과 암호 또는 PIN과 같은 다른 인증 방법 중 하나를 사용해야 합니다. 기본값은 **켜짐**입니다.
  - **컨테이너에 대한 인증 적용:** 장치 잠금 해제에 사용된 방법과 다른 인증 방법을 사용하여 KNOX 컨테이너를 엽니다. 기본값은 **켜짐**입니다.
  - **보안 키패드 사용:** 사용자가 Knox 컨테이너 내에서 보안 키보드를 사용하도록 강제합니다. 기본값은 **켜짐**입니다.

Windows 데스크톱/태블릿 설정



- **Wi-Fi 설정**

- **인터넷 공유 허용:** 장치를 Wi-Fi 핫스팟으로 전환하여 다른 장치와 인터넷 연결을 공유할 수 있도록 허용합니다.

- **연결**
  - **셀룰러를 통한 VPN 허용:** 장치가 VPN을 통해 셀룰러 네트워크에 연결할 수 있도록 허용합니다.
  - **로밍 중 셀룰러를 통한 VPN 허용:** 장치가 셀룰러 네트워크에서 로밍할 때 VPN을 통해 연결할 수 있도록 허용합니다.
  - **셀룰러 데이터 로밍 허용:** 사용자가 로밍 중에 셀룰러 데이터를 사용할 수 있도록 허용합니다.
- **계정**
  - **Microsoft 계정 연결 허용:** 장치가 이메일과 관련 없는 연결 인증 및 서비스에 Microsoft 계정을 사용할 수 있도록 허용합니다.
  - **비 Microsoft 이메일 허용:** 사용자가 비 Microsoft 이메일 계정을 추가할 수 있도록 허용합니다.
- **시스템**
  - **저장소 카드 허용:** 장치에서 저장소 카드를 사용하도록 허용합니다.
  - **원격 분석:** 드롭다운 목록에서 옵션을 선택하여 장치에서 원격 분석 정보를 보내는 것을 허용하거나 제한합니다. 기본값은 **허용됨**입니다. 다른 옵션은 **허용 안 함** 및 **보조 데이터 요청 제외, 허용됨**입니다.
  - **위치 서비스 허용:** 위치 서비스를 허용합니다.
  - **내부 빌드 미리 보기 허용:** 사용자가 Microsoft 내부 빌드를 미리 볼 수 있도록 허용합니다.
- **카메라:**
  - **카메라 사용 허용:** 사용자가 장치 카메라를 사용하도록 허용합니다.
- **블루투스:**
  - **검색 모드 허용:** Bluetooth 장치가 로컬 장치를 찾을 수 있도록 허용합니다.
  - **로컬 장치 이름:** 로컬 장치의 이름입니다.
- **경험:**
  - **Cortana 허용:** 사용자가 지능형 개인 비서이자 지식 탐색기인 Cortana에 액세스할 수 있도록 허용합니다.
  - **장치 검색 허용:** 장치의 네트워크 검색을 허용합니다.
  - **수동 MDM 등록 취소 허용:** 사용자가 XenMobile MDM에서 장치를 수동으로 등록 취소할 수 있도록 허용합니다.

  - **장치 설정 동기화 허용:** 사용자가 로밍 시 Windows 10 및 Windows 11 장치 간에 설정을 동기화할 수 있도록 허용합니다.

- **잠금 화면 위:**

  - **알림 허용:** 잠금 화면에서 알림을 허용합니다.

- **앱**

  - **앱 스토어 자동 업데이트 허용:** 앱 스토어의 앱이 자동으로 업데이트되도록 허용합니다.

- **개인 정보 보호:**

  - **입력 개인 설정 허용:** 사용자가 입력하는 내용에 따라 펜 및 터치 키보드와 같은 예측 입력을 개선하기 위해 입력 개인 설정 서비스가 실행되도록 허용합니다.

- **설정:**

  - **자동 실행 허용:** 사용자가 자동 실행 설정을 변경할 수 있도록 허용합니다.
  - **데이터 센스 허용:** 사용자가 데이터 센스 설정을 변경할 수 있도록 허용합니다.
  - **날짜 및 시간 허용:** 사용자가 날짜 및 시간 설정을 변경할 수 있도록 허용합니다.
  - **언어 허용:** 사용자가 언어 설정을 변경할 수 있도록 허용합니다.
  - **전원 및 절전 허용:** 사용자가 전원 및 절전 설정을 변경할 수 있도록 허용합니다.
  - **지역 허용:** 사용자가 지역 설정을 변경할 수 있도록 허용합니다.
  - **로그인 옵션 허용:** 사용자가 로그인 설정을 변경할 수 있도록 허용합니다.
  - **작업 공간 허용:** 사용자가 작업 공간 설정을 변경할 수 있도록 허용합니다.
  - **계정 허용:** 사용자가 계정 설정을 변경할 수 있도록 허용합니다.

로밍 장치 정책

XenMobile에서 장치 정책을 추가하여 사용자 iOS 장치에서 음성 및 데이터 로밍을 허용할지 여부를 구성할 수 있습니다. 음성 로밍이 비활성화되면 데이터 로밍도 자동으로 비활성화됩니다. iOS의 경우 이 정책은 iOS 5.0 이상 장치에서만 사용할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

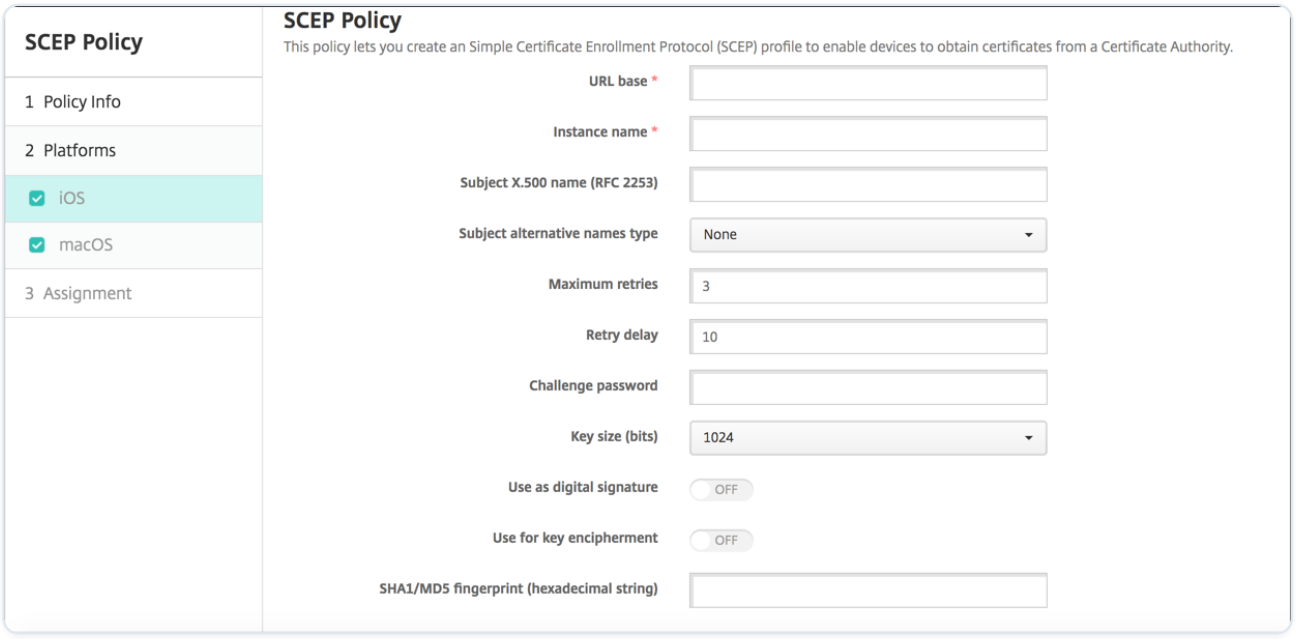
- **음성 로밍 비활성화:** 음성 로밍을 비활성화할지 여부를 선택합니다. 이 옵션을 사용하도록 설정하면 데이터 로밍이 자동으로 비활성화됩니다. 기본값은 **끔**이며, 이는 음성 로밍을 허용합니다.
- **데이터 로밍 비활성화:** 데이터 로밍을 비활성화할지 여부를 선택합니다. 이 옵션은 음성 로밍이 활성화된 경우에만 사용할 수 있습니다. 기본값은 **끔**이며, 이는 데이터 로밍을 허용합니다.

SCEP 장치 정책

이 정책을 사용하면 iOS 및 macOS 장치가 외부 SCEP 서버에서 SCEP(Simple Certificate Enrollment Protocol)를 사용하여 인증서를 검색하도록 구성할 수 있습니다. XenMobile에 연결된 PKI에서 SCEP를 사용하여 장치에 인증서를 전달하려면 분산 모드에서 PKI 엔터티 및 PKI 공급자를 생성해야 합니다. 자세한 내용은 PKI 엔터티를 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

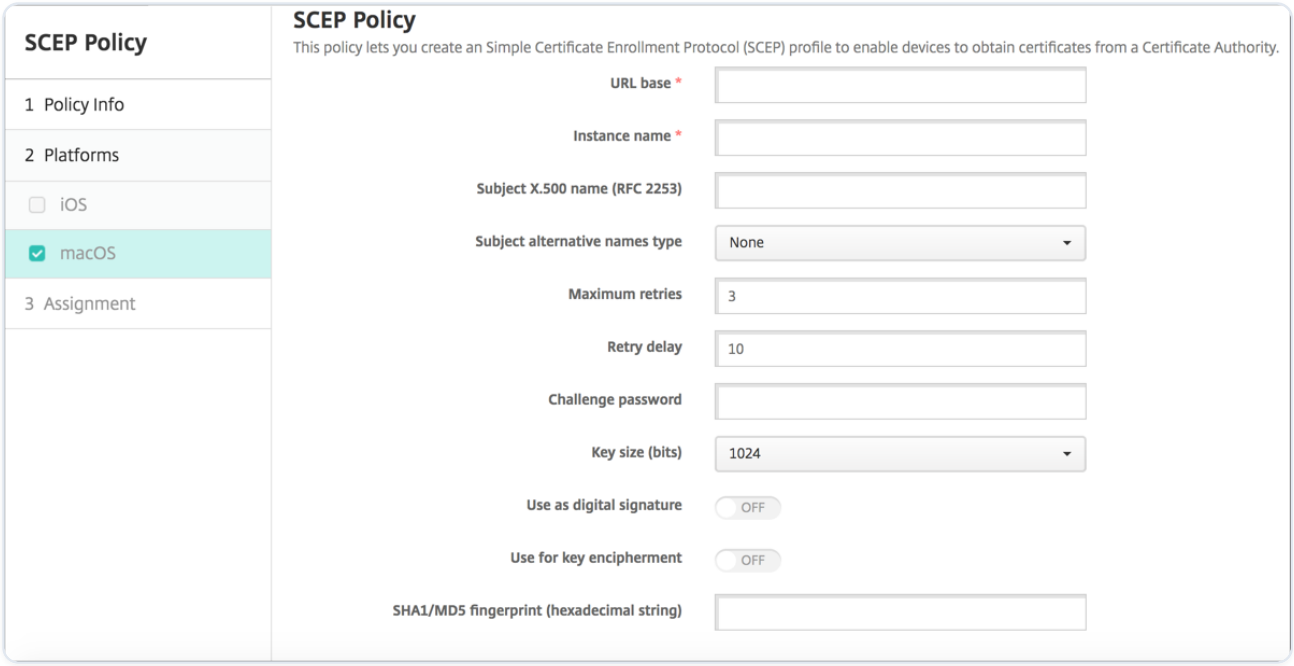
iOS 설정



- **URL 기본:** SCEP 요청이 HTTP 또는 HTTPS를 통해 전송되는 위치를 정의하려면 SCEP 서버의 주소를 입력합니다. 개인 키는 CSR(인증서 서명 요청)과 함께 전송되지 않으므로 암호화되지 않은 요청을 보내도 안전할 수 있습니다. 그러나 일회용 암호를 재사용할 수 있는 경우 HTTPS를 사용하여 암호를 보호해야 합니다. 이 단계는 필수입니다.
- **인스턴스 이름:** SCEP 서버가 인식하는 문자열을 입력합니다. 예를 들어, example.org와 같은 도메인 이름일 수 있습니다. CA에 여러 CA 인증서가 있는 경우 이 필드를 사용하여 필요한 도메인을 구분할 수 있습니다. 이 단계는 필수입니다.

- **주체 X.500 이름(RFC 2253):** OID(개체 식별자) 및 값의 배열로 표현된 X.500 이름의 표현을 입력합니다. 예를 들어, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar는 \[\[\["C", "US"\] \], \[\["O", "Apple Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \]로 변환될 수 있습니다. OID는 국가(C), 지역(L), 주(ST), 조직(O), 조직 구성 단위(OU) 및 일반 이름(CN)에 대한 바로 가기가 있는 점으로 구분된 숫자로 표현할 수 있습니다.
- **주체 대체 이름 유형:** 드롭다운 목록에서 대체 이름 유형을 클릭합니다. SCEP 정책은 CA가 인증서를 발급하는 데 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 보낼 때 장치가 재시도할 수 있는 횟수를 입력합니다. 기본값은 **3**입니다.
- **재시도 지연:** 후속 재시도 사이에 대기할 시간(초)을 입력합니다. 첫 번째 재시도는 지연 없이 시도됩니다. 기본값은 **10**입니다.
- **챌린지 암호:** 사전 공유 암호를 입력합니다.
- **키 크기(비트):** 비트 단위의 키 크기로 **2048** 이상을 선택합니다.
- **디지털 서명으로 사용:** 인증서를 디지털 서명으로 사용할지 여부를 지정합니다. 누군가 인증서를 사용하여 디지털 서명을 확인하는 경우(예: 인증서가 CA에서 발급되었는지 확인) SCEP 서버는 공개 키를 사용하여 해시를 해독하기 전에 인증서가 이러한 방식으로 사용될 수 있는지 확인합니다.
- **키 암호화에 사용:** 인증서를 키 암호화에 사용할지 여부를 지정합니다. 서버가 클라이언트가 제공한 인증서의 공개 키를 사용하여 데이터 조각이 개인 키로 암호화되었는지 확인하는 경우, 서버는 먼저 인증서가 키 암호화에 사용될 수 있는지 확인합니다. 그렇지 않으면 작업이 실패합니다.
- **SHA1/MD5 지문(16진수 문자열):** CA가 HTTP를 사용하는 경우, 이 필드를 사용하여 CA 인증서의 지문을 제공합니다. 이 지문은 장치가 등록 중에 CA 응답의 진위 여부를 확인하는 데 사용됩니다. SHA1 또는 MD5 지문을 입력하거나, 서명을 가져올 인증서를 선택할 수 있습니다.
- **정책 설정**
    - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
        - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
        - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정



- **URL 기본:** SCEP 요청이 HTTP 또는 HTTPS를 통해 전송되는 위치를 정의하기 위해 SCEP 서버의 주소를 입력합니다. 개인 키는 CSR(인증서 서명 요청)과 함께 전송되지 않으므로 암호화되지 않은 요청을 보내도 안전할 수 있습니다. 그러나 일회용 암호를 재사용할 수 있는 경우 암호를 보호하기 위해 HTTPS를 사용해야 합니다. 이 단계는 필수입니다.
- **인스턴스 이름:** SCEP 서버가 인식하는 문자열을 입력합니다. 예를 들어, example.org와 같은 도메인 이름일 수 있습니다. CA에 여러 CA 인증서가 있는 경우 이 필드를 사용하여 필요한 도메인을 구분할 수 있습니다. 이 단계는 필수입니다.
- **주체 X.500 이름 (RFC 2253):** OID(개체 식별자) 및 값의 배열로 표현된 X.500 이름의 표현을 입력합니다. 예를 들어, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar는 \[\[\["C", "US"\] \], \[\["O", "Apple Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \]로 변환됩니다. OID는 국가(C), 지역(L), 주(ST), 조직(O), 조직 단위(OU), 일반 이름(CN)에 대한 단축키가 있는 점으로 구분된 숫자로 표현할 수 있습니다.
- **주체 대체 이름 유형:** 드롭다운 목록에서 대체 이름 유형을 클릭합니다. SCEP 정책은 CA가 인증서를 발급하는 데 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 보낼 때 장치가 재시도할 수 있는 횟수를 입력합니다. 기본값은 **3**입니다.
- **재시도 지연:** 후속 재시도 사이에 대기할 시간(초)을 입력합니다. 첫 번째 재시도는 지연 없이 시도됩니다. 기본값은 **10**입니다.
- **챌린지 암호:** 사전 공유 암호를 입력합니다.
- **키 크기(비트):** 키 크기를 비트 단위로 **2048** 이상으로 선택합니다.

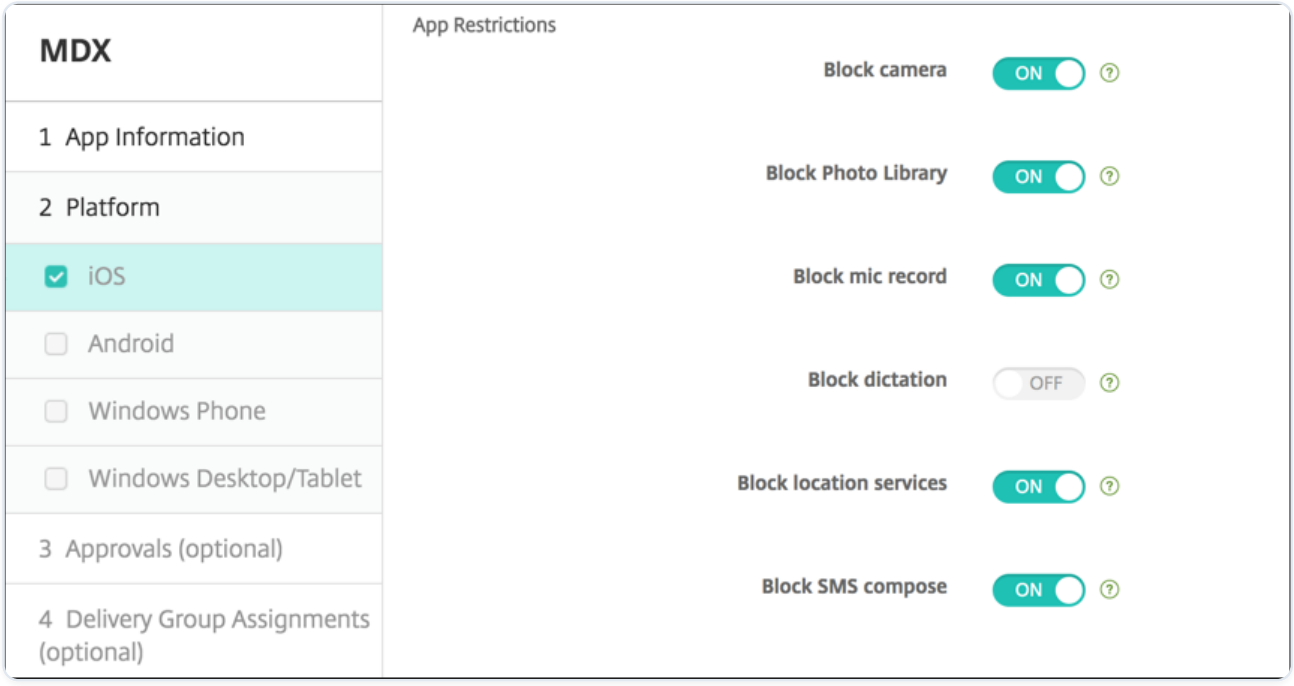
- **디지털 서명으로 사용:** 인증서를 디지털 서명으로 사용할지 여부를 지정합니다. 누군가 디지털 서명을 확인하기 위해 인증서를 사용하는 경우(예: 인증서가 CA에서 발급되었는지 확인), SCEP 서버는 공개 키를 사용하여 해시를 해독하기 전에 해당 인증서가 이러한 방식으로 사용될 수 있는지 확인합니다.
- **키 암호화에 사용:** 인증서를 키 암호화에 사용할지 여부를 지정합니다. 서버가 클라이언트가 제공한 인증서의 공개 키를 사용하여 데이터 조각이 개인 키를 사용하여 암호화되었는지 확인하는 경우, 서버는 먼저 인증서가 키 암호화에 사용될 수 있는지 확인합니다. 그렇지 않으면 작업이 실패합니다.
- **SHA1/MD5 지문(16진수 문자열):** CA가 HTTP를 사용하는 경우, 이 필드를 사용하여 CA 인증서의 지문을 제공합니다. 이 지문은 장치가 등록 중에 CA 응답의 신뢰성을 확인하는 데 사용됩니다. SHA1 또는 MD5 지문을 입력하거나, 서명을 가져올 인증서를 선택할 수 있습니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다.
  - **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요**, 또는 **안 함**을 선택합니다. **암호 필요**를 선택한 경우, **제거 암호** 필드에 암호를 입력합니다.
  - **프로필 범위:** 이 정책이 **사용자**에게 적용되는지 아니면 전체 **시스템**에 적용되는지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Siri 및 받아쓰기 정책

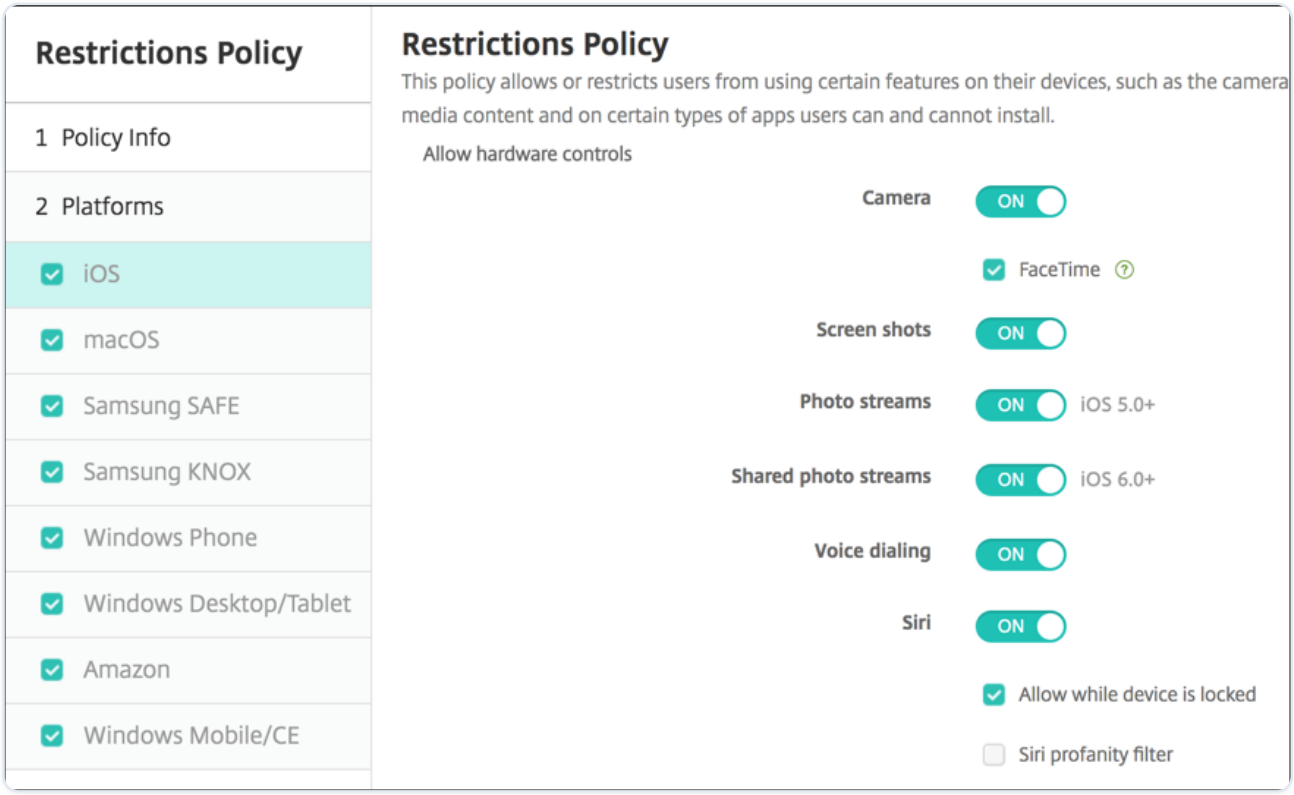
사용자가 관리되는 iOS 기기에서 Siri에게 질문하거나 텍스트를 받아쓰기할 때, Apple은 Siri 개선을 위해 음성 데이터를 수집합니다. 이 음성 데이터는 Apple의 클라우드 기반 서비스를 통해 전달되므로, 보안 XenMobile® 컨테이너 외부에 존재합니다. 그러나 받아쓰기 결과로 생성된 텍스트는 컨테이너 내부에 유지됩니다.

XenMobile은 보안 요구 사항에 따라 Siri 및 받아쓰기 서비스를 차단할 수 있도록 합니다.

MAM 배포에서 각 앱의 **받아쓰기 차단** 정책은 기본적으로 **켜짐**으로 설정되어 있으며, 이는 장치의 마이크를 비활성화합니다. 받아쓰기를 허용하려면 **꺼짐**으로 설정하십시오. 이 정책은 XenMobile 콘솔의 **구성 > 앱**에서 찾을 수 있습니다. 앱을 선택하고 **편집**을 클릭한 다음 **iOS**를 클릭하십시오.



MDM 배포에서는 **구성 > 장치 정책**에서 Siri 정책을 사용하여 Siri를 비활성화할 수도 있습니다. Siri 사용은 기본적으로 허용됩니다.



Siri 및 받아쓰기 허용 여부를 결정할 때 염두에 두어야 할 몇 가지 사항:

- Apple이 공개한 정보에 따르면, Apple은 Siri 및 받아쓰기 음성 클립 데이터를 최대 2년 동안 보관합니다. 이 데이터에는 사용자를 나타내는 임의의 숫자가 할당되며, 음성 파일은 이 임의의 숫자와 연결됩니다. 자세한 내용은 Wired 기사 Apple은 Siri가 데이터를 얼마나 오래 보관하는지 공개합니다를 참조하십시오.

- 모든 iOS 장치에서 **설정 > 일반 > 키보드**로 이동하여 **받아쓰기 활성화** 아래의 링크를 탭하면 Apple 개인 정보 보호 정책을 검토할 수 있습니다.

SSO 계정 장치 정책

XenMobile®에서 단일 Sign-On(SSO) 계정을 생성하여 사용자가 다양한 앱에서 XenMobile 및 내부 회사 리소스에 한 번만 Sign-On할 수 있도록 합니다. 사용자는 장치에 자격 증명을 저장할 필요가 없습니다. SSO 계정 엔터프라이즈 사용자 자격 증명은 App Store의 앱을 포함하여 여러 앱에서 사용됩니다. 이 정책은 Kerberos 인증 백엔드와 함께 작동하도록 설계되었습니다.

이 정책은 iOS 7.0 이상에만 적용됩니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **계정 이름:** 사용자 장치에 표시되는 Kerberos SSO 계정 이름을 입력합니다. 이 필드는 필수입니다.
- **Kerberos 주체 이름:** Kerberos 주체 이름을 입력합니다. 이 필드는 필수입니다.
- **ID 자격 증명(키 저장소 또는 PKI 자격 증명):** 사용자 상호 작용 없이 Kerberos 자격 증명을 갱신하는 데 사용할 수 있는 드롭다운 목록에서 선택적 ID 자격 증명을 클릭합니다.
- **Kerberos 영역:** 이 정책에 대한 Kerberos 영역을 입력합니다. 이 설정 값은 일반적으로 모두 대문자로 된 도메인 이름입니다(예: EXAMPLE.COM). 이 필드는 필수입니다.
- **허용된 URL:** SSO를 요구하려는 각 URL에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **허용된 URL:** 사용자가 iOS 장치에서 URL을 방문할 때 SSO를 요구하려는 URL을 입력합니다.

    예를 들어, 사용자가 사이트를 탐색하려고 시도하고 웹 사이트가 Kerberos 챌린지를 시작할 때: 해당 사이트가 URL 목록에 없으면 iOS 장치는 이전 Kerberos 로그온에서 Kerberos가 장치에 캐시했을 수 있는 Kerberos 토큰을 제공하여 SSO를 시도하지 않습니다. 일치는 URL의 호스트 부분에서 정확해야 합니다. 예를 들어, `https://shopping.apple.com`은 유효하지만 `https://*.apple.com`는 유효하지 않습니다.

    또한 호스트 일치를 기반으로 Kerberos가 활성화되지 않은 경우에도 URL은 표준 HTTP 호출로 대체됩니다. 이는 URL이 Kerberos를 사용하여 SSO용으로만 구성된 경우 표준 암호 챌린지 또는 HTTP 오류를 포함하여 거의 모든 것을 의미할 수 있습니다.
  - URL을 추가하려면 **추가**를 클릭하거나 URL 추가를 취소하려면 **취소**를 클릭합니다.
- **앱 식별자:** 이 로그인을 사용할 수 있는 각 앱에 대해 **추가**를 클릭한 다음 다음을 수행합니다.

- **앱 식별자:** 이 로그인을 사용할 수 있는 앱의 앱 식별자를 입력합니다. 앱 식별자를 추가하지 않으면 이 로그인은 **모든** 앱 식별자와 일치합니다.
- **추가**를 클릭하여 앱 식별자를 추가하거나 **취소**를 클릭하여 앱 식별자 추가를 취소합니다.

- **정책 설정**
  - **정책 제거:** 정책 제거를 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간(단위: 시간)을 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

스토어 장치 정책

XenMobile®에서 정책을 생성하여 iOS, Android 또는 Windows 태블릿 장치의 홈 화면에 XenMobile Store 웹 클립을 표시할지 여부를 지정할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

플랫폼 설정

구성하는 각 플랫폼에 대해 사용자 장치에 XenMobile Store 웹 클립이 표시될지 여부를 선택합니다. 기본값은 **켜짐**입니다.

구독 캘린더 장치 정책

XenMobile에서 장치 정책을 추가하여 iOS 장치의 캘린더 목록에 구독 캘린더를 추가할 수 있습니다. 구독할 수 있는 공개 캘린더 목록은 www.apple.com/downloads/macosx/calendars에서 확인할 수 있습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

전제 조건

사용자 장치의 구독 캘린더 목록에 캘린더를 추가하려면 먼저 캘린더를 구독해야 합니다.

iOS 설정

- **설명:** 캘린더에 대한 설명을 입력합니다. 이 필드는 필수입니다.

- **URL:** 캘린더 URL을 입력합니다. `webcal://` URL 또는 iCalendar 파일(.ics)에 대한 `https://` 링크를 입력할 수 있습니다. 이 필드는 필수입니다.
- **사용자 이름:** 사용자의 로그온 이름을 입력합니다. 이 필드는 필수입니다.
- **암호:** 선택 사항인 사용자 암호를 입력합니다.
- **SSL 사용:** 캘린더에 대한 보안 소켓 계층 연결을 사용할지 여부를 선택합니다. 기본값은 **해제**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 캘린더를 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

이용 약관 디바이스 정책

사용자가 회사 네트워크 연결을 관리하는 특정 정책에 동의하도록 하려면 XenMobile®에서 이용 약관 디바이스 정책을 생성합니다. 사용자가 XenMobile에 디바이스를 등록할 때 이용 약관이 제시되며, 디바이스를 등록하려면 이를 수락해야 합니다. 이용 약관을 거부하면 등록 프로세스가 취소됩니다.

회사가 해외 사용자를 보유하고 있으며 해당 사용자가 모국어로 이용 약관에 동의하도록 하려면 다양한 언어로 된 이용 약관에 대한 여러 정책을 생성할 수 있습니다. 배포하려는 각 플랫폼 및 언어 조합에 대한 파일을 제공해야 합니다. Android 및 iOS 디바이스의 경우 PDF 파일을 제공해야 합니다. Windows 디바이스의 경우 텍스트(.txt) 파일과 함께 이미지 파일을 제공해야 합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

iOS 및 Android 설정

- **가져올 파일: 찾아보기**를 클릭한 다음 파일 위치로 이동하여 가져올 이용 약관 파일을 선택합니다.
- **기본 이용 약관:** 이 파일이 서로 다른 이용 약관을 가진 여러 그룹의 구성원인 사용자를 위한 기본 문서인지 여부를 선택합니다. 기본값은 **해제**입니다.

Windows 태블릿 설정

- **가져올 파일: 찾아보기**를 클릭한 다음 파일 위치로 이동하여 가져올 이용 약관 파일을 선택합니다.
- **이미지: 찾아보기**를 클릭한 다음 파일 위치로 이동하여 가져올 이미지 파일을 선택합니다.

- **기본 이용 약관:** 이 파일이 서로 다른 이용 약관을 가진 여러 그룹의 구성원인 사용자를 위한 기본 문서인지 여부를 선택합니다. 기본값은 **해제**입니다.

VPN 장치 정책

VPN 장치 정책은 사용자 장치가 기업 리소스에 안전하게 연결할 수 있도록 가상 사설망(VPN) 설정을 구성합니다. 다음 플랫폼에 대해 VPN 장치 정책을 구성할 수 있습니다. 각 플랫폼에는 이 문서에 자세히 설명된 대로 다른 값 세트가 필요합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

앱별 VPN 요구 사항

VPN 정책을 통해 다음 플랫폼에 대한 앱별 VPN 기능을 구성합니다.

- iOS
- macOS
- Android (레거시 DA)
- 삼성 세이프
- 삼성 녹스

Android Enterprise 장치용 VPN을 구성하려면 Citrix SSO 앱에 대한 관리형 구성 장치 정책을 생성하십시오. Android Enterprise용 VPN 프로필 구성을 참조하십시오.

앱별 VPN 옵션은 특정 연결 유형에 사용할 수 있습니다. 다음 표는 앱별 VPN 옵션을 사용할 수 있는 시기를 나타냅니다.

플랫폼	연결 유형	비고
iOS	시스코 레거시 애니커넥트, 주니퍼 SSL, F5 SSL, 소닉월 모바일 커넥트, 아리바 VIA, 시트릭스 SSO 또는 사용자 지정 SSL.	
macOS	시스코 애니커넥트, 주니퍼 SSL, F5 SSL, 소닉월 모바일 커넥트, 아리바 VIA 또는 사용자 지정 SSL.	
Android (레거시 DA)	시트릭스 SSO	

플랫폼	연결 유형	비고
삼성 SAFE	IPSEC, SSL	VPN 유형이 **일반**으로 설정됨
삼성 녹스	IPSEC, SSL	VPN 유형이 **일반**으로 설정됨

Citrix SSO 앱을 사용하여 iOS 및 Android(레거시 DA) 장치용 앱별 VPN을 생성하려면 VPN 정책 구성 외에 추가 단계를 수행해야 합니다. 또한 다음 필수 구성 요소가 충족되었는지 확인해야 합니다.

- 온프레미스 Citrix Gateway
- 다음 애플리케이션이 장치에 설치되어 있어야 합니다:
  - 시트릭스 SSO
  - 시트릭스 시큐어 허브™

Citrix SSO 앱을 사용하여 iOS 및 Android 장치용 앱별 VPN을 구성하는 일반적인 워크플로는 다음과 같습니다.

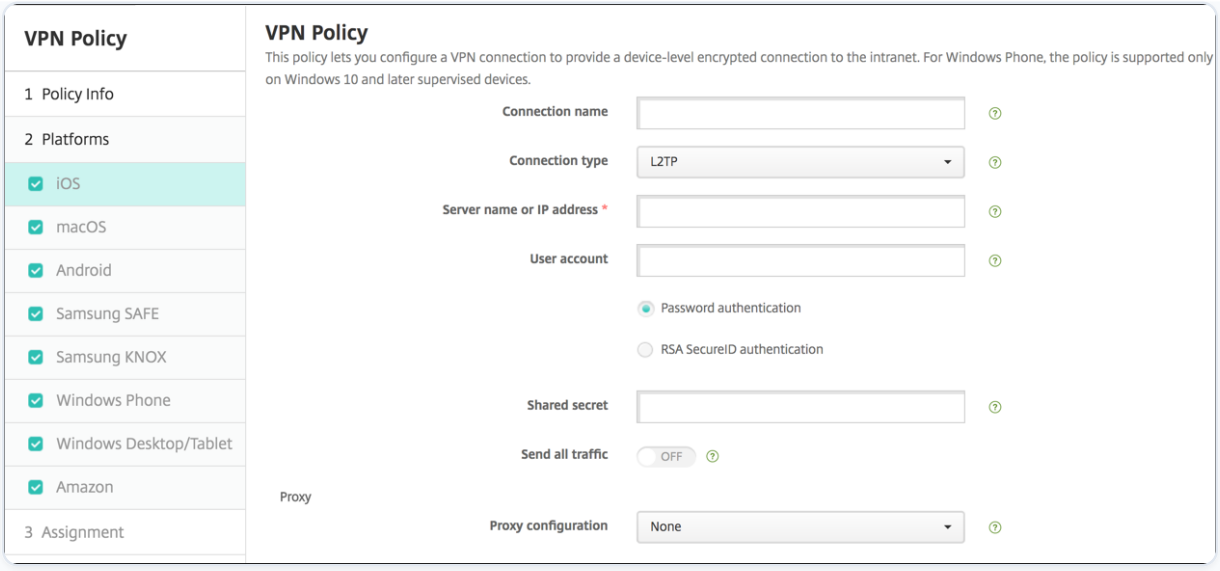
1. 이 문서에 설명된 대로 VPN 장치 정책을 구성합니다.
   - *iOS*의 경우 iOS용 Citrix SSO 프로토콜 구성을 참조하십시오. VPN 장치 정책을 통해 iOS용 Citrix SSO 프로토콜을 구성한 후에는 앱을 앱별 VPN 정책과 연결하기 위해 앱 속성 정책도 생성해야 합니다. 자세한 내용은 앱별 VPN 구성을 참조하십시오.
     - **연결 인증 유형** 필드에서 **인증서**를 선택하는 경우 먼저 Endpoint Management에 대한 인증서 기반 인증을 구성해야 합니다. 클라이언트 인증서 또는 인증서 및 도메인 인증을 참조하십시오.
   - *Android (레거시 DA)*의 경우 Android용 Citrix SSO 프로토콜 구성을 참조하십시오.
     - **연결 인증 유형** 필드에서 **인증서** 또는 **암호 및 인증서**를 선택하는 경우 먼저 Endpoint Management에 대한 인증서 기반 인증을 구성해야 합니다. 클라이언트 인증서 또는 인증서 및 도메인 인증을 참조하십시오.
2. 앱별 VPN에서 트래픽을 수락하도록 Citrix ADC를 구성합니다. 자세한 내용은 Citrix Gateway에서 전체 VPN 설정을 참조하십시오.

iOS 설정

> **iOS 12로 장치 업그레이드를 준비하려면:**

iOS용 VPN 장치 정책의 Citrix VPN 연결 유형은 iOS 12를 지원하지 않습니다. 다음 단계에 따라 기존 VPN 장치 정책을 삭제하고 Citrix SSO 연결 유형으로 VPN 장치 정책을 생성하십시오.

1. iOS용 VPN 장치 정책을 삭제합니다.
2. iOS용 VPN 장치 정책을 추가합니다. 중요 설정:
   - **연결 유형** = **Citrix SSO**
   - **앱별 VPN 사용** = **켜기**
   - **공급자 유형** = **패킷 터널**
3. iOS용 앱 속성 장치 정책을 추가합니다. **앱별 VPN 식별자**의 경우 **iOS_VPN**을 선택합니다.



- **연결 이름:** 연결 이름을 입력합니다.
- **연결 유형:** 목록에서 이 연결에 사용할 프로토콜을 선택합니다. 기본값은 **L2TP**입니다.
  - **L2TP:** 사전 공유 키 인증을 사용하는 계층 2 터널링 프로토콜입니다.
  - **PPTP:** 지점 간 터널링입니다.
  - **IPSec:** 회사 VPN 연결입니다.
  - **Cisco Legacy AnyConnect:** 이 연결 유형은 사용자 장치에 Cisco Legacy AnyConnect VPN 클라이언트가 설치되어 있어야 합니다. Cisco는 현재 사용되지 않는 VPN 프레임워크를 기반으로 하는 Cisco Legacy AnyConnect 클라이언트를 단계적으로 폐지하고 있습니다. 자세한 내용은 지원 문서 `<https://support.citrix.com/article/CTX227708>`를 참조하십시오.

    현재 Cisco AnyConnect 클라이언트를 사용하려면 **연결 유형**으로 **사용자 지정 SSL**을 사용하십시오. 필요한 설정은 이 섹션의 “사용자 지정 SSL 프로토콜 구성”을 참조하십시오.

- **Juniper SSL:** Juniper Networks SSL VPN 클라이언트입니다.
- **F5 SSL:** F5 Networks SSL VPN 클라이언트입니다.
- **SonicWALL Mobile Connect:** iOS용 Dell 통합 VPN 클라이언트입니다.
- **Ariba VIA:** Ariba Networks 가상 인터넷 액세스 클라이언트입니다.
- **IKEv2 (iOS 전용):** iOS 전용 Internet Key Exchange 버전 2입니다.
- **AlwaysOn IKEv2:** IKEv2를 사용하는 Always-on 액세스입니다.
- **AlwaysOn IKEv2 이중 구성:** IKEv2 이중 구성을 사용하는 Always-on 액세스입니다.
- **Citrix SSO:** iOS 12 이상용 Citrix SSO 클라이언트입니다.
- **사용자 지정 SSL:** 사용자 지정 보안 소켓 계층입니다. 이 연결 유형은 번들 ID가 **com.cisco.anyconnect**인 Cisco AnyConnect 클라이언트에 필요합니다. **연결 이름**을 **Cisco AnyConnect**로 지정합니다. VPN 정책을 배포하고 iOS 장치에 대한 네트워크 액세스 제어(NAC) 필터를 활성화할 수도 있습니다. 이 필터는 규정을 준수하지 않는 앱이 설치된 장치의 VPN 연결을 차단합니다. 이 구성에는 다음 iOS 섹션에 설명된 대로 iOS VPN 정책에 대한 특정 설정이 필요합니다. NAC 필터를 활성화하는 데 필요한 다른 설정에 대한 자세한 내용은 네트워크 액세스 제어를 참조하십시오.

다음 섹션에서는 이전 연결 유형 각각에 대한 구성 옵션을 나열합니다.

iOS용 L2TP 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **암호 인증** 또는 **RSA SecurID 인증**을 선택합니다.
- **공유 암호:** IPsec 공유 암호 키를 입력합니다.
- **모든 트래픽 보내기:** VPN을 통해 모든 트래픽을 보낼지 여부를 선택합니다. 기본값은 **해제**입니다.

iOS용 PPTP 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **암호 인증** 또는 **RSA SecurID 인증** 중 하나를 선택합니다.
- **암호화 수준:** 목록에서 암호화 수준을 선택합니다. 기본값은 **없음**입니다.
  - **없음:** 암호화를 사용하지 않습니다.
  - **자동:** 서버에서 지원하는 가장 강력한 암호화 수준을 사용합니다.
  - **최대 (128비트):** 항상 128비트 암호화를 사용합니다.

- **모든 트래픽 보내기:** VPN을 통해 모든 트래픽을 보낼지 여부를 선택합니다. 기본값은 **해제**입니다.

iOS용 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 **인증서** 중 하나를 선택합니다. 기본값은 **공유 암호**입니다.
- **공유 암호**를 사용하도록 설정하는 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 클라이언트에 자신을 인증한 다음 클라이언트가 서버에 자신을 인증합니다. 기본값은 **해제**입니다.
  - **암호 확인:** 사용자가 네트워크에 연결할 때 암호를 확인할지 여부를 선택합니다. 기본값은 **해제**입니다.
- **인증서**를 활성화하는 경우 다음 설정을 구성합니다.
  - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
  - **연결 시 PIN 입력 요청:** 사용자가 네트워크에 연결할 때 PIN을 입력하도록 요구할지 여부를 선택합니다. 기본값은 **해제**입니다.
  - **주문형 VPN 활성화:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. **주문형 VPN 활성화**가 **설정**된 경우 설정 구성에 대한 자세한 내용은 iOS용 주문형 VPN 활성화 설정 구성을 참조하십시오.
- **앱별 VPN 활성화:** 앱별 VPN을 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다.
- **주문형 일치 앱 활성화:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다. 기본값은 **해제**입니다.
- **Safari 도메인: 추가**를 클릭하여 Safari 도메인 이름을 추가합니다.

iOS용 Cisco 레거시 AnyConnect 프로토콜 구성

Cisco 레거시 AnyConnect 클라이언트에서 새 Cisco AnyConnect 클라이언트로 전환하려면 사용자 지정 SSL 프로토콜을 사용하십시오.

- **공급자 번들 식별자:** 레거시 AnyConnect 클라이언트의 번들 ID는 com.cisco.anyconnect.gui입니다.
- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.

- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **그룹:** 선택 사항인 그룹 이름을 입력합니다.
- **연결 인증 유형:** 목록에서 이 연결의 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 활성화하는 경우 **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 활성화하는 경우 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
        - **연결 시 PIN 프롬프트:** 사용자가 네트워크에 연결할 때 PIN을 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **해제**입니다.
        - **요청 시 VPN 활성화:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 활성화**가 **설정**된 경우 설정 구성에 대한 자세한 내용은 iOS용 요청 시 VPN 활성화 설정 구성을 참조하십시오.
- **앱별 VPN 활성화:** 앱별 VPN을 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 활성화하는 경우 다음 설정을 구성합니다.
    - **요청 시 앱 일치 활성화:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **공급자 유형:** 앱별 VPN이 **앱 프록시** 또는 **패킷 터널**로 제공되는지 여부를 선택합니다. 기본값은 **앱 프록시**입니다.
    - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
        - **도메인:** 추가할 도메인을 입력합니다.
        - **저장**을 클릭하여 도메인을 저장하거나 **취소**를 클릭하여 도메인을 저장하지 않습니다.

iOS용 Juniper SSL 프로토콜 구성

- **공급자 번들 식별자:** 앱별 VPN 프로필에 동일한 유형의 여러 VPN 공급자가 있는 앱의 번들 식별자가 있는 경우 여기에 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:** 선택 사항인 역할 이름을 입력합니다.

- **연결에 대한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 사용하도록 설정한 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 사용하도록 설정한 경우 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
        - **연결 시 PIN 확인:** 사용자가 네트워크에 연결할 때 PIN을 확인하도록 할지 여부를 선택합니다. 기본값은 **해제**입니다.
        - **요청 시 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결을 트리거할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 사용**이 **설정**된 경우 설정 구성에 대한 자세한 내용은 iOS용 요청 시 VPN 사용 설정 구성을 참조하십시오.
- **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 사용하도록 설정한 경우 다음 설정을 구성합니다.
    - **요청 시 일치 앱 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **공급자 유형:** 앱별 VPN이 **앱 프록시** 또는 **패킷 터널**로 제공되는지 여부를 선택합니다. 기본값은 **앱 프록시**입니다.
    - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
        - **도메인:** 추가할 도메인을 입력합니다.
        - **저장**을 클릭하여 도메인을 저장하거나 **취소**를 클릭하여 도메인을 저장하지 않습니다.

iOS용 F5 SSL 프로토콜 구성

- **공급자 번들 식별자:** 앱별 VPN 프로필에 동일한 유형의 여러 VPN 공급자가 있는 앱의 번들 식별자가 있는 경우, 여기에 사용할 공급자를 지정합니다.
- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **연결을 위한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 사용하도록 설정한 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 사용하도록 설정한 경우, 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.

    - **연결 시 PIN 프롬프트 표시:** 사용자가 네트워크에 연결할 때 PIN을 입력하라는 메시지를 표시할지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **요청 시 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 사용**이 **설정**된 경우 설정 구성에 대한 자세한 내용은 iOS용 요청 시 VPN 설정 구성을 참조하십시오.

- **앱별 VPN 사용:** 앱별 VPN을 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 활성화하는 경우 다음 설정을 구성합니다.
    - **요청 시 앱 일치 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다.
    - **공급자 유형:** 앱별 VPN이 **앱 프록시** 또는 **패킷 터널**로 제공될지 여부를 선택합니다. 기본값은 **앱 프록시**입니다.
    - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
        - **도메인:** 추가할 도메인을 입력합니다.
        - 도메인을 저장하려면 **저장**을 클릭하고, 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

iOS용 SonicWALL 프로토콜 구성

- **공급자 번들 식별자:** 앱별 VPN 프로필에 동일한 유형의 VPN 공급자가 여러 개 있는 앱의 번들 식별자가 있는 경우, 여기에 사용할 공급자를 지정합니다.
- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **로그온 그룹 또는 도메인:** 선택 사항인 로그온 그룹 또는 도메인을 입력합니다.
- **연결을 위한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 활성화하는 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 활성화하는 경우, 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
        - **연결 시 PIN 요청:** 사용자가 네트워크에 연결할 때 PIN을 요청할지 여부를 선택합니다. 기본값은 **해제**입니다.
        - **요청 시 VPN 활성화:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 활성화**가 **켜짐**일 때 설정을 구성하는 방법에 대한 자세한 내용은 iOS용 요청 시 VPN 활성화 설정 구성을 참조하십시오.

- **앱별 VPN 활성화:** 앱별 VPN을 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 켜짐으로 설정하는 경우 다음 설정을 구성합니다.
  - **요청 시 일치 앱 활성화:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거되도록 할지 여부를 선택합니다.
  - **공급자 유형:** 앱별 VPN이 **앱 프록시** 또는 **패킷 터널**로 제공되는지 여부를 선택합니다. 기본값은 **앱 프록시**입니다.
  - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
    - **도메인:** 추가할 도메인을 입력합니다.
    - 도메인을 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.

iOS용 Ariba VIA 프로토콜 구성

- **공급자 번들 식별자:** 앱별 VPN 프로필에 동일한 유형의 여러 VPN 공급자가 있는 앱의 번들 식별자가 있는 경우, 여기에 사용할 공급자를 지정합니다.
- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **연결에 대한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
  - **암호**를 활성화하는 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
  - **인증서**를 활성화하는 경우, 다음 설정을 구성합니다.
    - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
    - **연결 시 PIN 확인:** 사용자가 네트워크에 연결할 때 PIN을 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **요청 시 VPN 활성화:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 활성화**가 **켜짐**일 때 설정을 구성하는 방법에 대한 자세한 내용은 iOS용 요청 시 VPN 활성화 설정 구성을 참조하십시오.
- **앱별 VPN 활성화:** 앱별 VPN을 활성화할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 활성화하는 경우, 다음 설정을 구성합니다.
  - **요청 시 일치 앱 활성화:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다.

- **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
  - **도메인:** 추가할 도메인을 입력합니다.
  - 도메인을 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.

iOS용 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 네트워크 모두에 대해 이러한 모든 설정을 구성합니다.

- **사용자가 자동 연결을 비활성화하도록 허용:** AlwaysOn 프로토콜의 경우. 사용자가 장치에서 네트워크에 대한 자동 연결을 해제할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **서버의 호스트 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **로컬 식별자:** IKEv2 클라이언트의 FQDN 또는 IP 주소입니다. 이 필드는 필수입니다.
- **원격 식별자:** VPN 서버의 FQDN 또는 IP 주소입니다. 이 필드는 필수입니다.
- **장치 인증:** 이 연결에 대한 인증 유형으로 **공유 암호**, **인증서** 또는 **장치 식별자 기반 장치 인증서**를 선택합니다. 기본값은 **공유 암호**입니다.
  - **공유 암호**를 선택한 경우, 선택적 공유 암호 키를 입력합니다.
  - **인증서**를 선택한 경우, 사용할 **ID 자격 증명**을 선택합니다. 기본값은 **없음**입니다.
  - **장치 식별자 기반 장치 인증서**를 선택한 경우, 사용할 **장치 ID 유형**을 선택합니다. 기본값은 **IMEI**입니다. 이 옵션을 사용하려면 REST API를 사용하여 인증서를 대량으로 가져옵니다. REST API를 사용하여 iOS 장치에 인증서 대량 업로드를 참조하십시오. **Always On IKEv2**를 선택한 경우에만 사용할 수 있습니다.
- **확장 인증 사용:** 확장 인증 프로토콜(EAP)을 활성화할지 여부를 선택합니다. **켬**을 선택한 경우, **사용자 계정** 및 **인증 암호**를 입력합니다.
- **Dead Peer Detection 간격:** 피어 장치가 계속 연결 가능한지 확인하기 위해 피어 장치에 연락하는 빈도를 선택합니다. 기본값은 **없음**입니다. 옵션은 다음과 같습니다.
  - **없음:** Dead Peer Detection을 비활성화합니다.
  - **낮음:** 30분마다 피어에 연락합니다.
  - **중간:** 피어에 10분마다 연결합니다.
  - **높음:** 피어에 1분마다 연결합니다.
- **모빌리티 및 멀티호밍 비활성화:** 이 기능을 비활성화할지 여부를 선택합니다.

- **IPv4/IPv6 내부 서브넷 속성 사용:** 이 기능을 활성화할지 여부를 선택합니다.
- **리디렉션 비활성화:** 리디렉션을 비활성화할지 여부를 선택합니다.
- **장치가 절전 모드일 때 NAT Keepalive 활성화:** AlwaysOn 프로토콜용입니다. Keepalive 패킷은 IKEv2 연결에 대한 NAT 매핑을 유지합니다. 장치가 활성 상태일 때 칩은 이러한 패킷을 정기적으로 보냅니다. 이 설정이 켜져 있으면 장치가 절전 모드일 때도 칩은 Keepalive 패킷을 보냅니다. 기본 간격은 Wi-Fi를 통해 20초, 셀룰러를 통해 110초입니다. NAT Keepalive 간격 매개변수를 사용하여 간격을 변경할 수 있습니다.
- **NAT Keepalive 간격(초):** 기본값은 20초입니다.
- **완전 순방향 비밀성 활성화:** 이 기능을 활성화할지 여부를 선택합니다.
- **DNS 서버 IP 주소:** 선택 사항입니다. DNS 서버 IP 주소 문자열 목록입니다. 이러한 IP 주소에는 IPv4 및 IPv6 주소가 혼합될 수 있습니다. 주소를 입력하려면 **추가**를 클릭합니다.
- **도메인 이름:** 선택 사항입니다. 터널의 기본 도메인입니다.
- **검색 도메인:** 선택 사항입니다. 단일 레이블 호스트 이름을 완전히 한정하는 데 사용되는 도메인 문자열 목록입니다.
- **보조 일치 도메인을 확인자 목록에 추가:** 선택 사항입니다. 보조 일치 도메인 목록을 확인자의 검색 도메인 목록에 추가할지 여부를 결정합니다. 기본값은 **켜짐**입니다.
- **보조 일치 도메인:** 선택 사항입니다. DNS 서버 주소의 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 속하지 않는 호스트는 시스템의 기본 확인자를 사용하여 확인됩니다.

이 매개변수에 빈 문자열이 있으면 해당 문자열이 기본 도메인이 됩니다. 이것이 분할 터널 구성이 기본 DNS 서버보다 먼저 모든 DNS 쿼리를 VPN DNS 서버로 보낼 수 있는 방법입니다. VPN 터널이 네트워크의 기본 경로인 경우 나열된 DNS 서버가 기본 확인자가 됩니다. 이 경우 보조 일치 도메인 목록은 무시됩니다.

- **IKE SA 매개변수** 및 **자식 SA 매개변수**. 각 보안 연결(SA) 매개변수 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(재키 간격)을 나타내는 10에서 1440 사이의 정수를 입력합니다. 기본값은 **1440**분입니다.
- **서비스 예외:** AlwaysOn 프로토콜의 경우. 서비스 예외는 AlwaysOn VPN에서 제외되는 시스템 서비스입니다. 다음 서비스 예외 설정을 구성합니다.

- **음성 메일:** 목록에서 음성 메일 예외를 처리하는 방법을 선택합니다. 기본값은 **터널을 통한 트래픽 허용**입니다.
- **AirPrint:** 목록에서 AirPrint 예외를 처리하는 방법을 선택합니다. 기본값은 **터널을 통한 트래픽 허용**입니다.
- **VPN 터널 외부의 캡티브 웹 시트에서 트래픽 허용:** 사용자가 VPN 터널 외부의 공용 핫스팟에 연결할 수 있도록 허용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **VPN 터널 외부의 모든 캡티브 네트워킹 앱에서 트래픽 허용:** VPN 터널 외부의 모든 핫스팟 네트워킹 앱을 허용할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **캡티브 네트워킹 앱 번들 식별자:** 사용자가 액세스할 수 있는 각 핫스팟 네트워킹 앱 번들 식별자에 대해 **추가**를 클릭하고 핫스팟 네트워킹 앱 **번들 식별자**를 입력합니다. 앱 번들 식별자를 저장하려면 **저장**을 클릭합니다.

- **앱별 VPN**. IKEv2 연결 유형에 대한 다음 설정을 구성합니다.
  - **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **끔**입니다.
  - **주문형 일치 앱 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다. 기본값은 **끔**입니다.
  - **Safari 도메인:** Safari 도메인 이름을 추가하려면 **추가**를 클릭합니다.
- **프록시 구성:** VPN 연결이 프록시 서버를 통해 라우팅되는 방법을 선택합니다. 기본값은 **없음**입니다.

iOS용 Citrix SSO 프로토콜 구성

Citrix SSO 클라이언트는 `<https://apps.apple.com/us/app/citrix-sso/id1333396910>`의 Apple Store에서 사용할 수 있습니다.

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **연결을 위한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
  - **암호**를 사용하도록 설정한 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
  - **인증서**를 사용하도록 설정한 경우 다음 설정을 구성합니다.
    - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
    - **연결 시 PIN 프롬프트:** 사용자가 네트워크에 연결할 때 PIN을 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **OFF**입니다.

    - **요청 시 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **OFF**입니다. **요청 시 VPN 사용**이 **켜짐**으로 설정된 경우 설정 구성에 대한 자세한 내용은 iOS용 요청 시 VPN 사용 설정 구성을 참조하십시오.

- **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **끔**입니다. 이 옵션을 켜짐으로 설정하면 다음 설정을 구성합니다.

    - **요청 시 앱 일치 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다.
    - **공급자 유형:** 앱별 VPN이 **앱 프록시** 또는 **패킷 터널**로 제공되는지 여부를 선택합니다. 기본값은 **앱 프록시**입니다.
    - **공급자 유형: 패킷 터널**로 설정합니다.
    - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.

        - **도메인:** 추가할 도메인을 입력합니다.
        - 도메인을 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.

- **사용자 지정 XML:** 추가할 각 사용자 지정 XML 매개변수에 대해 **추가**를 클릭하고 키/값 쌍을 지정합니다. 사용 가능한 매개변수는 다음과 같습니다.

    - **disableL3:** 시스템 수준 VPN을 비활성화합니다. 앱별 VPN만 허용합니다. **값**은 필요하지 않습니다.
    - **useragent:** 이 장치 정책을 VPN 플러그인 클라이언트를 대상으로 하는 모든 Citrix Gateway 정책과 연결합니다. 플러그인에서 시작된 요청의 경우 이 키의 **값**이 VPN 플러그인에 자동으로 추가됩니다.

iOS용 사용자 지정 SSL 프로토콜 구성

Cisco Legacy AnyConnect 클라이언트에서 Cisco AnyConnect 클라이언트로 전환하려면 다음을 수행합니다.

1. 사용자 지정 SSL 프로토콜로 VPN 장치 정책을 구성합니다. 정책을 iOS 장치에 배포합니다.
2. `<https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>`에서 Cisco AnyConnect 클라이언트를 업로드하고, XenMobile에 앱을 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 식별자**에 지정된 앱에 동일한 유형(앱 프록시 또는 패킷 터널)의 VPN 공급자가 여러 개 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.
- **연결 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 사용하도록 설정하는 경우, **인증 암호** 필드에 선택적 인증 암호를 입력합니다.
    - **인증서**를 사용하도록 설정하는 경우, 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
        - **연결 시 PIN 프롬프트:** 사용자가 네트워크에 연결할 때 PIN을 입력하라는 메시지를 표시할지 여부를 선택합니다. 기본값은 **해제**입니다.
        - **VPN 요청 시 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. **VPN 요청 시 사용**이 **설정**된 경우 설정 구성에 대한 자세한 내용은 iOS용 VPN 요청 시 사용 설정 구성을 참조하십시오.
- **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 설정으로 지정하는 경우 다음 설정을 구성합니다.
    - **요청 시 앱 일치 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다.
    - **공급자 유형:** 공급자 유형은 공급자가 VPN 서비스인지 프록시 서비스인지를 나타냅니다. VPN 서비스의 경우 **패킷 터널**을 선택합니다. 프록시 서비스의 경우 **앱 프록시**를 선택합니다. Cisco AnyConnect 클라이언트의 경우 **패킷 터널**을 선택합니다.
    - **Safari 도메인:** 포함할 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
        - **도메인:** 추가할 도메인을 입력합니다.
        - 도메인을 저장하려면 **저장**을 클릭하거나 도메인을 저장하지 않으려면 **취소**를 클릭합니다.
- **사용자 지정 XML:** 추가할 각 사용자 지정 XML 매개 변수에 대해 **추가**를 클릭하고 다음을 수행합니다.
    - **매개 변수 이름:** 추가할 매개 변수의 이름을 입력합니다.
    - **값: 매개 변수 이름**과 연결된 값을 입력합니다.

- 매개변수를 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.

NAC를 지원하도록 VPN 장치 정책 구성

1. NAC 필터를 구성하려면 **연결 유형**을 **사용자 지정 SSL**로 설정해야 합니다.
2. **연결 이름**을 **VPN**으로 지정합니다.
3. **사용자 지정 SSL 식별자**에 **com.citrix.NetScalerGateway.ios.app**을 입력합니다.
4. **공급자 번들 식별자**에 **com.citrix.NetScalerGateway.ios.app.vpnplugin**을 입력합니다.

3단계와 4단계의 값은 NAC 필터링에 필요한 Citrix SSO 설치에서 가져옵니다. 인증 암호는 구성하지 않습니다. NAC 기능 사용에 대한 자세한 내용은 네트워크 액세스 제어를 참조하십시오.

iOS용 VPN 온디맨드 옵션 활성화 구성

- **온디맨드 도메인:** 사용자가 연결할 때 수행할 각 도메인 및 관련 작업에 대해 **추가**를 클릭하고 다음을 수행합니다.
- **도메인:** 추가할 도메인을 입력합니다.
- **작업:** 목록에서 가능한 작업 중 하나를 선택합니다.
  - **항상 설정:** 도메인이 항상 VPN 연결을 트리거합니다.
  - **절대 설정 안 함:** 도메인이 VPN 연결을 절대 트리거하지 않습니다.
  - **필요한 경우 설정:** 도메인 이름 확인에 실패하면 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버가 도메인을 확인할 수 없거나, 다른 서버로 리디렉션되거나, 시간 초과될 때 발생합니다.
  - 도메인을 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.
- **온디맨드 규칙**
  - **작업:** 목록에서 수행할 작업을 선택합니다. 기본값은 **EvaluateConnection**입니다. 가능한 작업은 다음과 같습니다.
    - **허용:** 트리거될 때 온디맨드 VPN 연결을 허용합니다.
    - **연결:** 무조건 VPN 연결을 시작합니다.
    - **연결 끊기:** VPN 연결을 제거하고 규칙이 일치하는 동안에는 온디맨드로 다시 연결하지 않습니다.
    - **EvaluateConnection:** 각 연결에 대해 ActionParameters 배열을 평가합니다.
    - **무시:** 기존 VPN 연결을 유지하지만, 규칙이 일치하는 동안에는 온디맨드로 다시 연결하지 않습니다.

- **DNSDomainMatch:** 추가하려는 장치의 검색 도메인 목록과 일치할 수 있는 각 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
  - **DNS 도메인:** 도메인 이름을 입력합니다. 여러 도메인을 일치시키기 위해 와일드카드 "*" 접두사를 사용할 수 있습니다. 예를 들어, *.example.com은 mydomain.example.com, yourdomain.example.com 및 herdomain.example.com과 일치합니다.
  - **저장**을 클릭하여 도메인을 저장하거나 **취소**를 클릭하여 도메인을 저장하지 않습니다.
- **DNSServerAddressMatch:** 추가하려는 네트워크의 지정된 DNS 서버 중 하나와 일치할 수 있는 각 IP 주소에 대해 **추가**를 클릭하고 다음을 수행합니다.
  - **DNS 서버 주소:** 추가하려는 DNS 서버 주소를 입력합니다. DNS 서버를 일치시키기 위해 와일드카드 "*" 접미사를 사용할 수 있습니다. 예를 들어, 17.*는 클래스 A 서브넷의 모든 DNS 서버와 일치합니다.
  - **저장**을 클릭하여 DNS 서버 주소를 저장하거나 **취소**를 클릭하여 DNS 서버 주소를 저장하지 않습니다.
- **InterfaceTypeMatch:** 목록에서 사용 중인 기본 네트워크 인터페이스 하드웨어 유형을 선택합니다. 기본값은 **지정되지 않음**입니다. 가능한 값은 다음과 같습니다.
  - **지정되지 않음:** 모든 네트워크 인터페이스 하드웨어와 일치합니다. 이 옵션이 기본값입니다.
  - **이더넷:** 이더넷 네트워크 인터페이스 하드웨어만 일치시킵니다.
  - **Wi-Fi:** Wi-Fi 네트워크 인터페이스 하드웨어만 일치시킵니다.
  - **셀룰러:** 셀룰러 네트워크 인터페이스 하드웨어만 일치시킵니다.
- **SSID 일치:** 추가하려는 현재 네트워크와 일치시킬 각 SSID에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **SSID:** 추가할 SSID를 입력합니다. 네트워크가 Wi-Fi 네트워크가 아니거나 SSID가 나타나지 않으면 일치가 실패합니다. 모든 SSID와 일치시키려면 이 목록을 비워 둡니다.
  - SSID를 저장하려면 **저장**을 클릭하거나 SSID를 저장하지 않으려면 **취소**를 클릭합니다.
- **URL 문자열 프로브:** 가져올 URL을 입력합니다. 이 URL이 리디렉션 없이 성공적으로 가져와지면 이 규칙이 일치합니다.
- **ActionParameters : 도메인:** 추가하려는 EvaluateConnection이 확인하는 각 도메인에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **도메인:** 추가할 도메인을 입력합니다.
  - 도메인을 저장하려면 **저장**을 클릭하거나 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

- **ActionParameters : 도메인 작업:** 목록에서 지정된 **ActionParameters : 도메인**에 대한 **VPN 동작**을 선택합니다. 기본값은 **필요한 경우 연결**입니다. 가능한 작업은 다음과 같습니다:
  - **필요한 경우 연결:** 도메인 이름 확인에 실패하면 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버가 도메인을 확인할 수 없거나, 다른 서버로 리디렉션되거나, 시간 초과될 때 발생합니다.
  - **연결 안 함:** 도메인은 VPN 연결을 절대 트리거하지 않습니다.
- **작업 매개변수: 필수 DNS 서버:** 지정된 도메인을 확인하는 데 사용될 각 DNS 서버 IP 주소에 대해 **추가**를 클릭한 다음 다음을 수행합니다:
  - **DNS 서버: ActionParameters** : **도메인 작업** = **필요한 경우 연결**일 때만 유효합니다. 추가할 DNS 서버를 입력합니다. 이 서버는 장치의 현재 네트워크 구성의 일부일 필요는 없습니다. DNS 서버에 연결할 수 없으면 응답으로 VPN 연결이 설정됩니다. 이 DNS 서버는 내부 DNS 서버이거나 신뢰할 수 있는 외부 DNS 서버여야 합니다.
  - DNS 서버를 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.
- **ActionParameters : RequiredURLStringProbe:** 선택적으로 GET 요청을 사용하여 프로브할 HTTP 또는 HTTPS(권장) URL을 입력합니다. URL의 호스트 이름을 확인할 수 없거나, 서버에 연결할 수 없거나, 서버가 응답하지 않으면 VPN 연결이 설정됩니다. **ActionParameters** : **DomainAction** = **ConnectIfNeeded**일 때만 유효합니다.
- **OnDemandRules : XML content:** XML 구성 온디맨드 규칙을 입력하거나 복사하여 붙여넣습니다.
  - XML 코드를 유효성 검사하려면 **사전 확인**을 클릭합니다. XML이 유효하면 **XML content** 텍스트 상자 아래 녹색 텍스트로 Valid XML이 표시됩니다. 유효하지 않으면 오류를 설명하는 오류 메시지가 주황색 텍스트로 표시됩니다.

- **프록시**
  - **프록시 구성:** 목록에서 VPN 연결이 프록시 서버를 통해 라우팅되는 방식을 선택합니다. 기본값은 **없음**입니다.
    - **수동**을 활성화하는 경우 다음 설정을 구성합니다.
      - **프록시 서버의 호스트 이름 또는 IP 주소:** 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
      - **프록시 서버의 포트:** 프록시 서버 포트 번호를 입력합니다. 이 필드는 필수입니다.
      - **사용자 이름:** 선택적 프록시 서버 사용자 이름을 입력합니다.
      - **암호:** 선택적 프록시 서버 암호를 입력합니다.

- **자동**을 구성하는 경우 다음 설정을 구성합니다.
  - **프록시 서버 URL:** 프록시 서버의 URL을 입력합니다. 이 필드는 필수입니다.

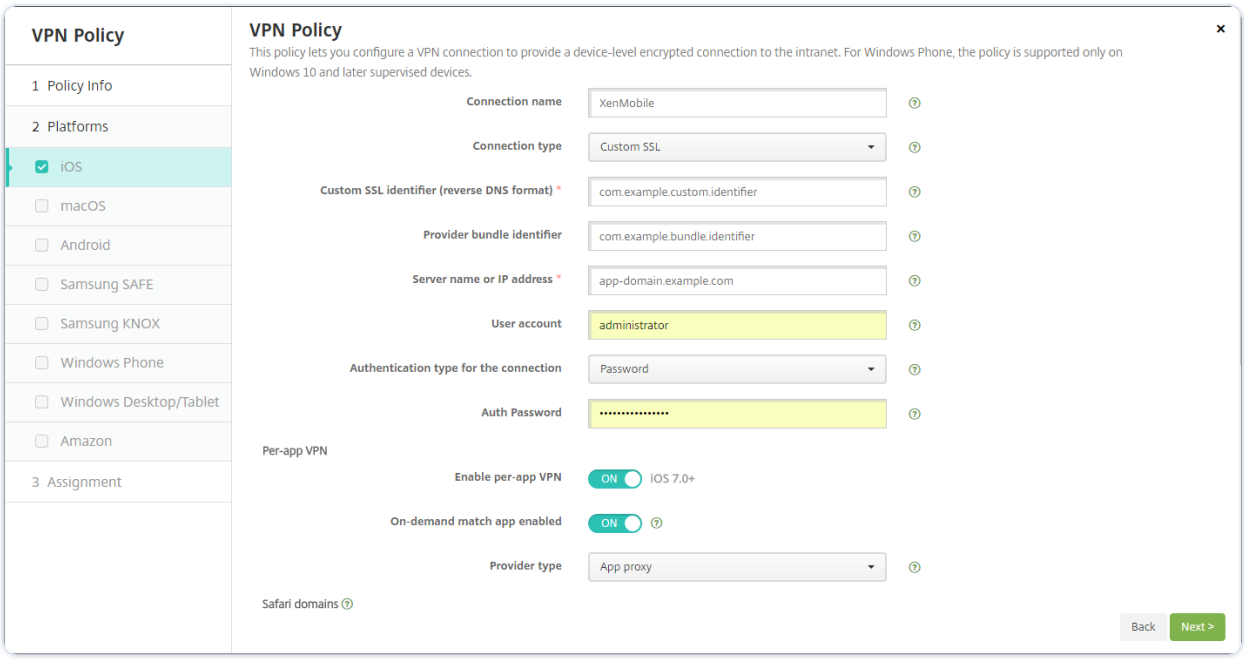
- **정책 설정**
  - **정책 설정**에서 **정책 제거** 옆에 있는 **날짜 선택** 또는 **제거까지의 기간(시간)**을 선택합니다.
  - **날짜 선택**을 선택한 경우, 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
  - **사용자가 정책을 제거하도록 허용** 목록에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다.
  - **암호 필요**를 선택한 경우, **제거 암호** 옆에 필요한 암호를 입력합니다.

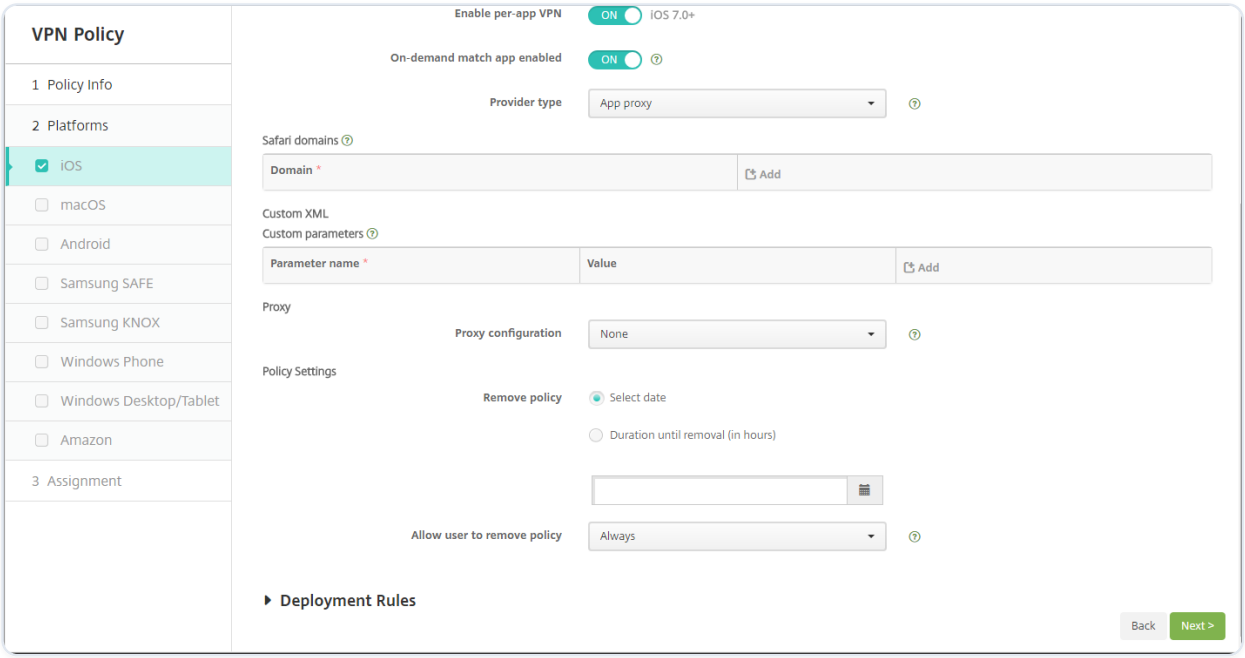
앱별 VPN 구성

iOS용 앱별 VPN 옵션은 Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO 및 Custom SSL과 같은 연결 유형에 사용할 수 있습니다.

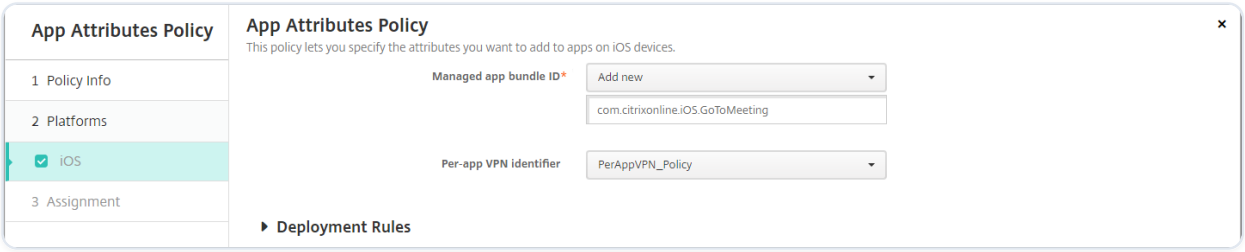
앱별 VPN을 구성하려면 다음을 수행합니다.

1. **구성 > 장치 정책**에서 VPN 정책을 생성합니다. 예시:



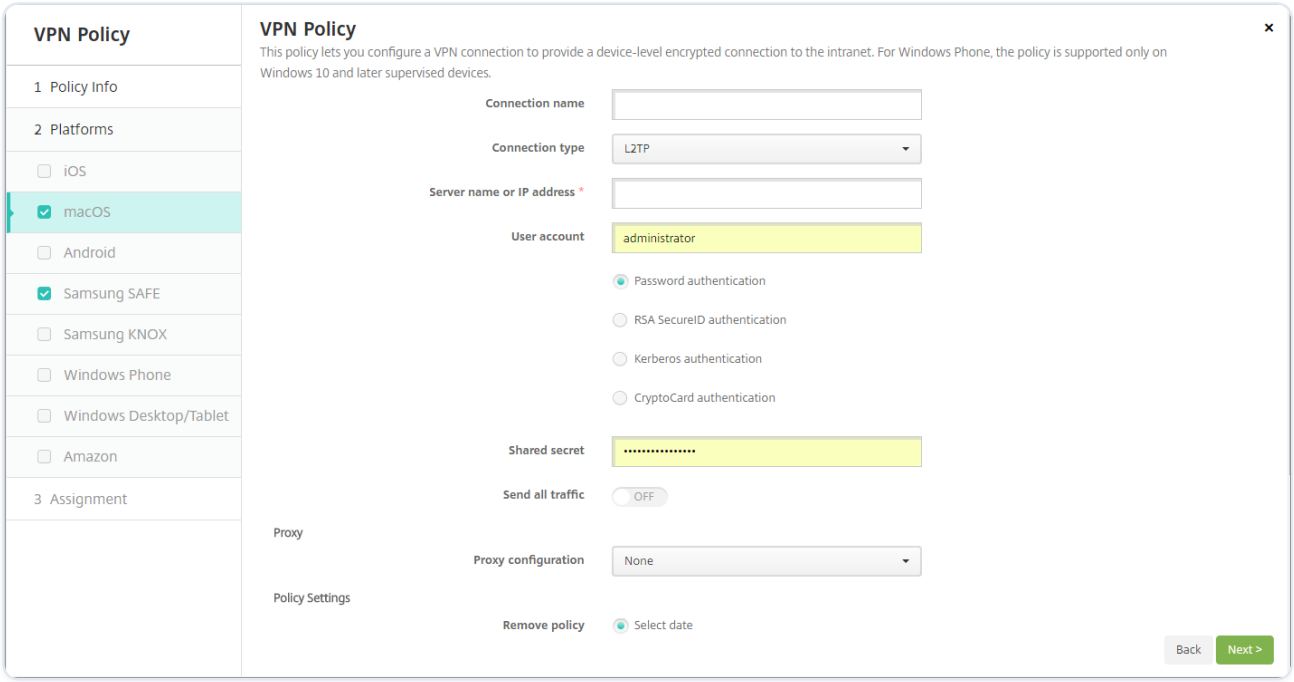


2. **구성 > 장치 정책**에서 앱을 앱별 VPN 정책과 연결하기 위한 앱 특성 정책을 생성합니다. **앱별 VPN 식별자**의 경우 1단계에서 생성한 VPN 정책의 이름을 선택합니다. **관리되는 앱 번들 ID**의 경우 앱 목록에서 선택하거나 앱 번들 ID를 입력합니다. (iOS 앱 인벤토리 정책을 배포하는 경우 앱 목록에 앱이 있습니다.)



- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정



- **연결 이름:** 연결 이름을 입력합니다.
- **연결 유형:** 목록에서 이 연결에 사용할 프로토콜을 선택합니다. 기본값은 L2TP입니다.
  - **L2TP:** 사전 공유 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:** iOS용 Dell 통합 VPN 클라이언트입니다.
  - **Ariba VIA:** Ariba Networks 가상 인터넷 액세스 클라이언트입니다.
  - **Citrix VPN:** Citrix VPN 클라이언트입니다.
  - **사용자 지정 SSL:** 사용자 지정 보안 소켓 계층입니다.

다음 섹션에서는 이전 연결 유형 각각에 대한 구성 옵션을 나열합니다.

macOS용 L2TP 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.

- **암호 인증**, **RSA SecurID 인증**, **Kerberos 인증** 또는 **CryptoCard 인증**을 선택합니다. 기본값은 **암호 인증**입니다.
- **공유 암호:** IPsec 공유 암호 키를 입력합니다.
- **모든 트래픽 보내기:** VPN을 통해 모든 트래픽을 보낼지 여부를 선택합니다. 기본값은 **끔**입니다.

macOS용 PPTP 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **암호 인증**, **RSA SecurID 인증**, **Kerberos 인증** 또는 **CryptoCard 인증**을 선택합니다. 기본값은 **암호 인증**입니다.
- **암호화 수준:** 원하는 암호화 수준을 선택합니다. 기본값은 **없음**입니다.
  - **없음:** 암호화를 사용하지 않습니다.
  - **자동:** 서버에서 지원하는 가장 강력한 암호화 수준을 사용합니다.
  - **최대** (128비트): 항상 128비트 암호화를 사용합니다.
- **모든 트래픽 보내기:** VPN을 통해 모든 트래픽을 보낼지 여부를 선택합니다. 기본값은 **끔**입니다.

macOS용 IPsec 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **연결에 대한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **공유 암호** 또는 **인증서**를 선택합니다. 기본값은 **공유 암호**입니다.
  - **공유 암호** 인증을 사용하도록 설정하는 경우 다음 설정을 구성합니다.
    - **그룹 이름:** 선택 사항인 그룹 이름을 입력합니다.
    - **공유 암호:** 선택 사항인 공유 암호 키를 입력합니다.
    - **하이브리드 인증 사용:** 하이브리드 인증을 사용할지 여부를 선택합니다. 하이브리드 인증을 사용하면 서버가 먼저 클라이언트에 자신을 인증한 다음 클라이언트가 서버에 자신을 인증합니다. 기본값은 **끔**입니다.
    - **암호 프롬프트:** 사용자가 네트워크에 연결할 때 암호를 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **끔**입니다.
  - **인증서** 인증을 사용하도록 설정하는 경우 다음 설정을 구성합니다.
    - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.

- **연결 시 PIN 프롬프트:** 사용자가 네트워크에 연결할 때 PIN을 입력하도록 요구할지 여부를 선택합니다. 기본값은 **끔**입니다.
- **요청 시 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용하도록 설정할지 여부를 선택합니다. 기본값은 **끔**입니다. **요청 시 VPN 사용**이 **켜짐**일 때 설정을 구성하는 방법에 대한 자세한 내용은 요청 시 VPN 사용 옵션 구성을 참조하십시오.

macOS용 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.
- **연결 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
  - **암호**를 사용하도록 설정한 경우, **인증 암호** 필드에 선택적 인증 암호를 입력합니다.
  - **인증서**를 사용하도록 설정한 경우, 다음 설정을 구성합니다.
    - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
    - **연결 시 PIN 확인:** 사용자가 네트워크에 연결할 때 PIN을 확인하도록 할지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **VPN 요청 시 사용:** 사용자가 네트워크에 연결할 때 VPN 연결을 트리거하도록 할지 여부를 선택합니다. 기본값은 **해제**입니다. **VPN 요청 시 사용**이 **설정**인 경우 설정 구성에 대한 자세한 내용은 (#configure-enable-vpn-on-demand-options)을 참조하십시오.
  - **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 사용하도록 설정한 경우 다음 설정을 구성합니다.
    - **요청 시 앱 일치 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거되도록 할지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
      - **도메인:** 추가할 도메인을 입력합니다.
      - 도메인을 저장하려면 **저장**을 클릭하고, 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

macOS용 Juniper SSL 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.

- **영역:** 선택 사항인 영역 이름을 입력합니다.
- **역할:** 선택 사항인 역할 이름을 입력합니다.
- **연결에 대한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 사용하도록 설정하는 경우 **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 사용하도록 설정하는 경우 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
        - **연결 시 PIN 확인:** 사용자가 네트워크에 연결할 때 PIN을 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **해제**입니다.
        - **요청 시 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 사용**이 **설정**인 경우 설정 구성에 대한 자세한 내용은 요청 시 VPN 사용 설정 구성을 참조하십시오.
- **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 사용하도록 설정하는 경우 다음 설정을 구성합니다.
    - **요청 시 일치 앱 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
        - **도메인:** 추가할 도메인을 입력합니다.
        - 도메인을 저장하려면 **저장**을 클릭하고, 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

macOS용 F5 SSL 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **연결을 위한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 사용하도록 설정하면 **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 사용하도록 설정하면 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.

    - **연결 시 PIN 프롬프트:** 사용자가 네트워크에 연결할 때 PIN을 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **요청 시 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 사용**이 **설정**된 경우 설정 구성에 대한 자세한 내용은 요청 시 VPN 사용 설정 구성을 참조하십시오.

- **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 사용하도록 설정하면 다음 설정을 구성합니다.
    - **요청 시 일치 앱 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다. 기본값은 **해제**입니다.
    - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
        - **도메인:** 추가할 도메인을 입력합니다.
        - 도메인을 저장하려면 **저장**을 클릭하고, 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

macOS용 SonicWALL Mobile Connect 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **로그온 그룹 또는 도메인:** 선택 사항인 로그온 그룹 또는 도메인을 입력합니다.
- **연결에 대한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 사용하도록 설정한 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 사용하도록 설정한 경우, 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
        - **연결 시 PIN 확인:** 사용자가 네트워크에 연결할 때 PIN을 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **해제**입니다.
        - **요청 시 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. **요청 시 VPN 사용**이 **설정**된 경우 설정 구성에 대한 자세한 내용은 요청 시 VPN 사용 설정 구성을 참조하십시오.

- **앱별 VPN 사용:** 앱별 VPN을 사용하도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션을 사용하도록 설정한 경우, 다음 설정을 구성합니다.

- **요청 시 앱 일치 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거되도록 설정할지 여부를 선택합니다. 기본값은 **해제**입니다.
- **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
  - **도메인:** 추가할 도메인을 입력합니다.
  - 도메인을 저장하려면 **저장**을 클릭하거나 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

macOS용 Ariba VIA 프로토콜 구성

- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
- **연결을 위한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
  - **암호**를 활성화하는 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
  - **인증서**를 활성화하는 경우, 다음 설정을 구성합니다.
    - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
    - **연결 시 PIN 프롬프트:** 사용자가 네트워크에 연결할 때 PIN을 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 **끔**입니다.
    - **VPN 요청 시 활성화:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **끔**입니다. **VPN 요청 시 활성화**가 **켜짐**일 때 설정을 구성하는 방법에 대한 자세한 내용은 VPN 요청 시 활성화 설정 구성을 참조하십시오.
- **앱별 VPN 활성화:** 앱별 VPN을 활성화할지 여부를 선택합니다. 기본값은 **끔**입니다. 이 옵션을 활성화하는 경우, 다음 설정을 구성합니다.
  - **요청 시 앱 일치 활성화:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다. 기본값은 **끔**입니다.
  - **Safari 도메인:** 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
    - **도메인:** 추가할 도메인을 입력합니다.
    - **저장**을 클릭하여 도메인을 저장하거나 **취소**를 클릭하여 도메인을 저장하지 않습니다.

macOS용 사용자 지정 SSL 프로토콜 구성

- **사용자 지정 SSL 식별자(역방향 DNS 형식):** 역방향 DNS 형식으로 SSL 식별자를 입력합니다. 이 필드는 필수입니다.
- **서버 이름 또는 IP 주소:** VPN 서버의 서버 이름 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
- **사용자 계정:** 선택 사항인 사용자 계정을 입력합니다.
    - **연결을 위한 인증 유형:** 목록에서 이 연결에 대한 인증 유형으로 **암호** 또는 **인증서**를 선택합니다. 기본값은 **암호**입니다.
    - **암호**를 활성화하는 경우, **인증 암호** 필드에 선택 사항인 인증 암호를 입력합니다.
    - **인증서**를 활성화하는 경우, 다음 설정을 구성합니다.
        - **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
        - **연결 시 PIN 프롬프트:** 사용자가 네트워크에 연결할 때 PIN을 입력하라는 메시지를 표시할지 여부를 선택합니다. 기본값은 **OFF**입니다.
        - **요청 시 VPN 활성화:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 활성화할지 여부를 선택합니다. 기본값은 **OFF**입니다. **요청 시 VPN 활성화**가 **켜짐**일 때 설정 구성에 대한 자세한 내용은 요청 시 VPN 활성화 설정 구성을 참조하십시오.
    - **앱별 VPN:** 앱별 VPN을 활성화할지 여부를 선택합니다. 기본값은 **끔**입니다. 이 옵션을 활성화하는 경우 다음 설정을 구성합니다.
        - **요청 시 일치 앱 활성화:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결이 자동으로 트리거될지 여부를 선택합니다.
        - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
            - **도메인:** 추가할 도메인을 입력합니다.
            - **저장**을 클릭하여 도메인을 저장하거나 **취소**를 클릭하여 도메인을 저장하지 않습니다.
- **사용자 지정 XML:** 추가하려는 각 사용자 지정 XML 매개변수에 대해 **추가**를 클릭하고 다음을 수행합니다.
    - **매개변수 이름:** 추가할 매개변수의 이름을 입력합니다.
    - **값: 매개변수 이름**과 연결된 값을 입력합니다.
    - 도메인을 저장하려면 **저장**을 클릭하거나 도메인을 저장하지 않으려면 **취소**를 클릭합니다.

VPN 온디맨드 옵션 활성화 구성

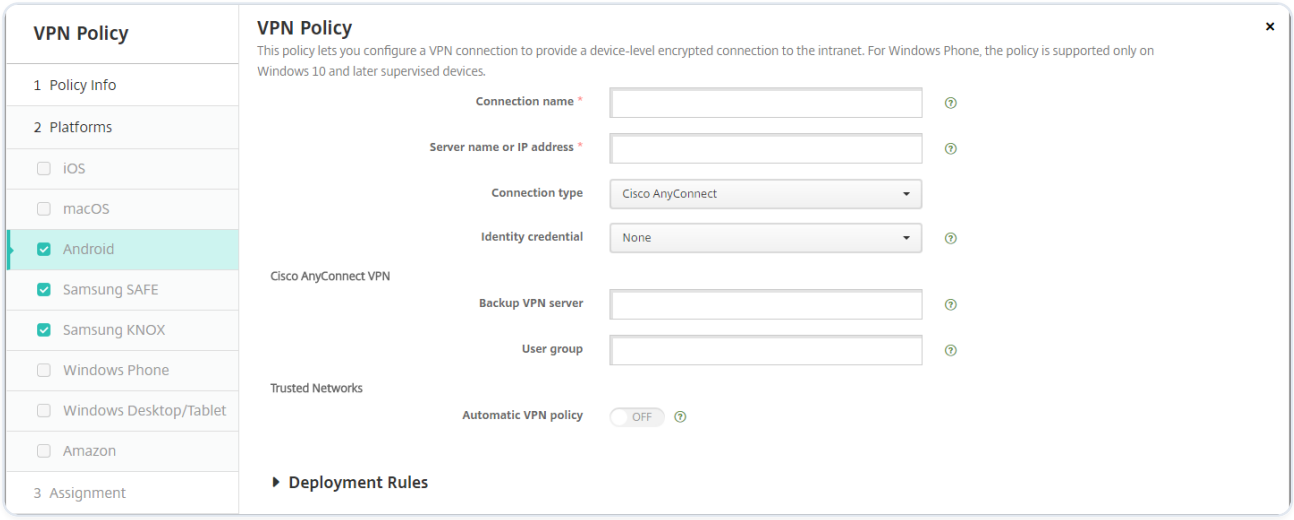
- **온디맨드 도메인:** 추가하려는 각 도메인 및 사용자가 해당 도메인에 연결할 때 수행할 관련 작업에 대해 **추가**를 클릭하고 다음을 수행합니다.
    - **도메인:** 추가할 도메인을 입력합니다.
    - **작업:** 목록에서 가능한 작업 중 하나를 선택합니다.
        - **항상 설정:** 도메인이 항상 VPN 연결을 트리거합니다.
        - **설정 안 함:** 도메인이 VPN 연결을 트리거하지 않습니다.
        - **필요한 경우 설정:** 도메인 이름 확인에 실패하면 도메인이 VPN 연결 시도를 트리거합니다. DNS 서버가 도메인을 확인할 수 없거나, 다른 서버로 리디렉션되거나, 시간 초과될 때 실패가 발생합니다.
    - 도메인을 저장하려면 **저장**을 클릭하거나 도메인을 저장하지 않으려면 **취소**를 클릭합니다.
- **온디맨드 규칙**
    - **작업:** 목록에서 수행할 작업을 선택합니다. 기본값은 **EvaluateConnection**입니다. 가능한 작업은 다음과 같습니다.
        - **허용:** 트리거될 때 VPN 온디맨드가 연결되도록 허용합니다.
        - **연결:** 무조건 VPN 연결을 시작합니다.
        - **연결 해제:** VPN 연결을 제거하고 규칙이 일치하는 한 온디맨드로 다시 연결하지 않습니다.
        - **EvaluateConnection:** 각 연결에 대해 **ActionParameters** 배열을 평가합니다.
        - **무시:** 기존 VPN 연결을 유지하지만, 규칙이 일치하는 한 요청 시 다시 연결하지 않습니다.
    - **DNS 도메인 일치:** 추가하려는, 사용자 장치의 검색 도메인 목록과 일치시킬 수 있는 각 도메인에 대해 **추가**를 클릭하고 다음을 수행합니다.
        - **DNS 도메인:** 도메인 이름을 입력합니다. 여러 도메인과 일치시키기 위해 와일드카드 "*" 접두사를 사용할 수 있습니다. 예를 들어, *.example.com은 mydomain.example.com, yourdomain.example.com 및 herdomain.example.com과 일치합니다.
        - 도메인을 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.
    - **DNS 서버 주소 일치:** 추가하려는, 네트워크의 지정된 DNS 서버 중 하나와 일치시킬 수 있는 각 IP 주소에 대해 **추가**를 클릭하고 다음을 수행합니다.

    - **DNS 서버 주소:** 추가하려는 DNS 서버 주소를 입력합니다. DNS 서버와 일치시키기 위해 와일드카드 "*" 접미사를 사용할 수 있습니다. 예를 들어, 17.*는 클래스 A 서브넷의 모든 DNS 서버와 일치합니다.
    - DNS 서버 주소를 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.
- **인터페이스 유형 일치:** 목록에서 사용 중인 기본 네트워크 인터페이스 하드웨어 유형을 클릭합니다. 기본값은 **지정되지 않음**입니다. 가능한 값은 다음과 같습니다.
    - **지정되지 않음:** 모든 네트워크 인터페이스 하드웨어와 일치합니다. 이 옵션이 기본값입니다.
    - **이더넷:** 이더넷 네트워크 인터페이스 하드웨어만 일치합니다.
    - **Wi-Fi:** Wi-Fi 네트워크 인터페이스 하드웨어만 일치합니다.
    - **셀룰러:** 셀룰러 네트워크 인터페이스 하드웨어만 일치합니다.
- **SSID 일치:** 추가하려는, 현재 네트워크와 일치시킬 각 SSID에 대해 **추가**를 클릭하고 다음을 수행합니다.
    - **SSID:** 추가할 SSID를 입력합니다. 네트워크가 Wi-Fi 네트워크가 아니거나 SSID가 나타나지 않으면 일치가 실패합니다. 모든 SSID와 일치시키려면 이 목록을 비워 둡니다.
    - SSID를 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.
- **URLStringProbe:** 가져올 URL을 입력합니다. 이 URL이 리디렉션 없이 성공적으로 가져와지면 이 규칙이 일치합니다.
- **ActionParameters : Domains:** EvaluateConnection이 확인하는 각 도메인에 대해 추가하려면 **추가**를 클릭하고 다음을 수행합니다.
    - **Domain:** 추가할 도메인을 입력합니다.
    - **저장**을 클릭하여 도메인을 저장하거나 **취소**를 클릭하여 도메인을 저장하지 않습니다.
- **ActionParameters : DomainAction:** 목록에서 지정된 **ActionParameters : Domains** 도메인에 대한 **VPN 동작**을 선택합니다. 기본값은 **ConnectIfNeeded**입니다. 가능한 동작은 다음과 같습니다.
    - **ConnectIfNeeded:** 도메인 이름 확인에 실패하면 도메인이 VPN 연결 시도를 트리거합니다. DNS 서버가 도메인을 확인할 수 없거나, 다른 서버로 리디렉션되거나, 시간 초과될 때 실패가 발생합니다.
    - **NeverConnect:** 도메인이 VPN 연결을 절대 트리거하지 않습니다.
- **Action Parameters: RequiredDNSServers:** 지정된 도메인을 확인하는 데 사용될 각 DNS 서버 IP 주소에 대해 **추가**를 클릭하고 다음을 수행합니다.

    - **DNS Server: ActionParameters** : **DomainAction** = **ConnectIfNeeded**일 때만 유효합니다. 추가할 DNS 서버를 입력합니다. 이 서버는 장치의 현재 네트워크 구성의 일부일 필요는 없습니다. DNS 서버에 연결할 수 없는 경우 VPN 연결이 설정됩니다. 이 DNS 서버는 내부 DNS 서버이거나 신뢰할 수 있는 외부 DNS 서버여야 합니다.
    - **저장**을 클릭하여 DNS 서버를 저장하거나 **취소**를 클릭하여 DNS 서버를 저장하지 않습니다.
  - **ActionParameters : RequiredURLStringProbe:** 선택적으로 HTTP 또는 HTTPS(권장) URL을 GET 요청을 사용하여 프로브하도록 입력합니다. URL의 호스트 이름을 확인할 수 없거나, 서버에 연결할 수 없거나, 서버가 응답하지 않으면 VPN 연결이 설정됩니다. **ActionParameters** : **DomainAction** = **ConnectIfNeeded**일 때만 유효합니다.
  - **OnDemandRules : XML content:** XML 온디맨드 규칙을 입력하거나 복사하여 붙여넣습니다.
    - **사전 확인**을 클릭하여 XML 코드를 유효성 검사합니다. XML이 유효하면 **XML content** 텍스트 상자 아래에 녹색 텍스트로 유효한 XML이 표시됩니다. 유효하지 않으면 오류를 설명하는 주황색 텍스트로 오류 메시지가 표시됩니다.

- **프록시**
  - **프록시 구성:** 목록에서 VPN 연결이 프록시 서버를 통해 라우팅되는 방식을 선택합니다. 기본값은 **없음**입니다.
    - **수동**을 사용하도록 설정하는 경우 다음 설정을 구성합니다.
      - **프록시 서버의 호스트 이름 또는 IP 주소:** 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
      - **프록시 서버의 포트:** 프록시 서버 포트 번호를 입력합니다. 이 필드는 필수입니다.
      - **사용자 이름:** 선택 사항인 프록시 서버 사용자 이름을 입력합니다.
      - **암호:** 선택 사항인 프록시 서버 암호를 입력합니다.
    - **자동**을 구성하는 경우 다음 설정을 구성합니다.
      - **프록시 서버 URL:** 프록시 서버의 URL을 입력합니다. 이 필드는 필수입니다.

Android 설정



Android용 Cisco AnyConnect VPN 프로토콜 구성

- **연결 이름:** Cisco AnyConnect VPN 연결의 이름을 입력합니다. 이 필드는 필수입니다.
- **서버 이름 또는 IP 주소:** VPN 서버의 이름 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
- **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 활성화 또는 비활성화하여 VPN이 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크에 어떻게 반응하는지 설정합니다. 활성화된 경우 다음 설정을 구성합니다.
    - **신뢰할 수 있는 네트워크 정책:** 목록에서 원하는 정책을 선택합니다. 기본값은 **연결 끊기**입니다. 가능한 옵션은 다음과 같습니다.
      - **연결 끊기:** 클라이언트가 신뢰할 수 있는 네트워크에서 VPN 연결을 종료합니다. 이 설정이 기본값입니다.
      - **연결:** 클라이언트가 신뢰할 수 있는 네트워크에서 VPN 연결을 시작합니다.
      - **아무것도 하지 않음:** 클라이언트가 아무런 조치도 취하지 않습니다.
      - **일시 중지:** 사용자가 신뢰할 수 없는 네트워크 외부에서 VPN 세션을 설정한 다음 신뢰할 수 있는 네트워크로 구성된 네트워크에 진입하면 VPN 세션이 일시 중단됩니다. 사용자가 신뢰할 수 있는 네트워크를 다시 떠나면 세션이 재개됩니다. 이 설정은 신뢰할 수 있는 네트워크를 떠난 후 새 VPN 세션을 설정할 필요를 없애줍니다.
    - **신뢰할 수 없는 네트워크 정책:** 목록에서 원하는 정책을 선택합니다. 기본값은 **연결**입니다. 가능한 옵션은 다음과 같습니다.

    - **연결:** 클라이언트가 신뢰할 수 없는 네트워크에서 VPN 연결을 시작합니다.
    - **아무것도 하지 않음:** 클라이언트가 신뢰할 수 없는 네트워크에서 VPN 연결을 시작합니다. 이 옵션은 상시 연결 VPN을 비활성화합니다.

- **신뢰할 수 있는 도메인:** 클라이언트가 신뢰할 수 있는 네트워크에 있을 때 네트워크 인터페이스가 가진 각 도메인 접미사에 대해 **추가**를 클릭하여 다음을 수행합니다.
    - **도메인:** 추가할 도메인을 입력합니다.
    - 도메인을 저장하려면 **저장**을 클릭하고, 도메인을 저장하지 않으려면 **취소**를 클릭합니다.
- **신뢰할 수 있는 서버:** 클라이언트가 신뢰할 수 있는 네트워크에 있을 때 네트워크 인터페이스가 가진 각 서버 주소에 대해 **추가**를 클릭하여 다음을 수행합니다.
    - **서버:** 추가할 서버를 입력합니다.
    - 서버를 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.

Android용 Citrix SSO 프로토콜 구성

- **연결 이름:** VPN 연결의 이름을 입력합니다. 이 필드는 필수입니다.
- **서버 이름 또는 IP 주소:** Citrix Gateway의 FQDN 또는 IP 주소를 입력합니다.
- **연결에 대한 인증 유형:** 인증 유형을 선택하고 해당 유형에 나타나는 필드를 모두 작성합니다.
    - **사용자 이름** 및 **암호: 암호** 또는 **암호 및 인증서**의 **인증 유형**에 대한 VPN 자격 증명을 입력합니다. 선택 사항입니다. VPN 자격 증명을 제공하지 않으면 Citrix VPN 앱에서 사용자 이름과 암호를 묻는 메시지가 표시됩니다.
    - **ID 자격 증명: 인증서** 또는 **암호 및 인증서**의 **인증 유형**에 나타납니다. 목록에서 ID 자격 증명을 선택합니다.
- **앱별 VPN 사용:** 앱별 VPN을 사용할지 여부를 선택합니다. 앱별 VPN을 사용하지 않으면 모든 트래픽이 Citrix VPN 터널을 통해 이동합니다. 앱별 VPN을 사용하도록 설정하면 다음 설정을 지정합니다. 기본값은 **해제**입니다.
    - **화이트리스트** 또는 **블랙리스트: 화이트리스트**인 경우 허용된 모든 앱은 이 VPN을 통해 터널링됩니다. **블랙리스트**인 경우 차단 목록에 있는 앱을 제외한 모든 앱은 이 VPN을 통해 터널링됩니다.

> **참고:**
>
> XenMobile® Server 콘솔에는 "블랙리스트" 및 "화이트리스트"라는 용어가 포함되어 있습니다. 다음 릴리스에서는 이러한 용어를 "차단 목록" 및 "허용 목록"으로 변경할 예정입니다.

- **응용 프로그램 목록:** 허용되거나 차단된 앱을 지정합니다. **추가**를 클릭한 다음 쉼표로 구분된 앱 패키지 이름 목록을 입력합니다.

- **사용자 지정 XML: 추가**를 클릭한 다음 사용자 지정 매개 변수를 입력합니다. XenMobile은 Citrix VPN에 대해 다음 매개 변수를 지원합니다.

  - **DisableUserProfiles:** 선택 사항입니다. 이 매개 변수를 사용하도록 설정하려면 **값**에 **예**를 입력합니다. 사용하도록 설정하면 XenMobile은 사용자가 추가한 VPN 연결을 표시하지 않으며 사용자는 연결을 추가할 수 없습니다. 이 설정은 전역 제한이며 모든 VPN 프로필에 적용됩니다.
  - **userAgent:** 문자열 값입니다. 각 HTTP 요청에 보낼 사용자 지정 User Agent 문자열을 지정할 수 있습니다. 지정된 사용자 에이전트 문자열은 기존 Citrix VPN 사용자 에이전트에 추가됩니다.

NAC를 지원하도록 VPN 구성

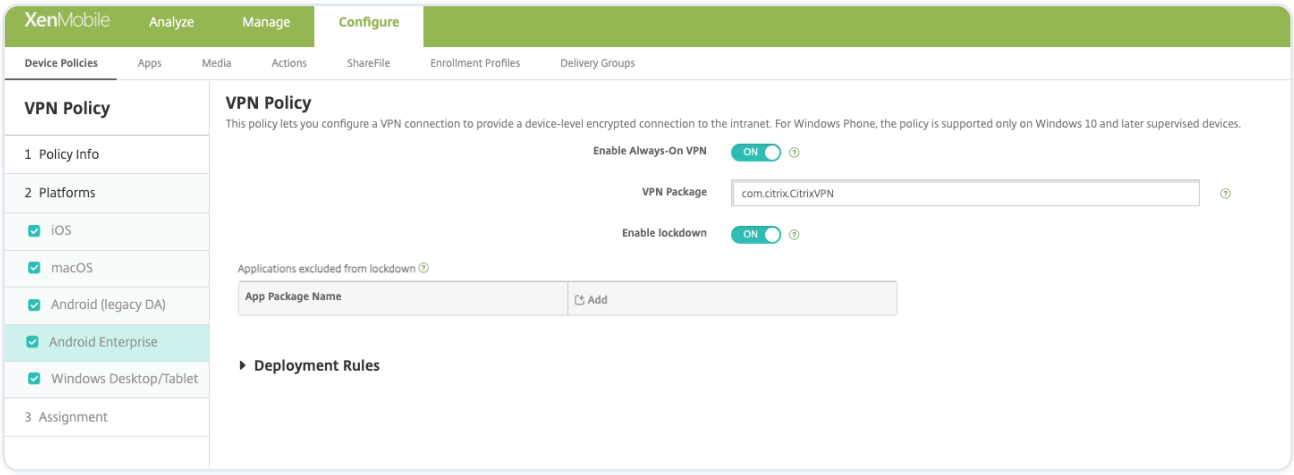
1. NAC 필터를 구성하려면 **연결 유형**을 **사용자 지정 SSL**로 사용합니다.
2. **연결 이름**을 **VPN**으로 지정합니다.
3. **사용자 지정 XML**의 경우 **추가**를 클릭하고 다음을 수행합니다.

   - **매개변수 이름: XenMobileDeviceId**를 입력합니다. 이 필드는 XenMobile에 디바이스 등록을 기반으로 NAC 확인에 사용할 디바이스 ID입니다. XenMobile이 디바이스를 등록하고 관리하는 경우 VPN 연결이 허용됩니다. 그렇지 않으면 VPN 설정 시 인증이 거부됩니다.
   - **값:** 매개변수 **XenMobileDeviceId**의 값인 **DeviceID_${device.id}**를 입력합니다.
   - 매개변수를 저장하려면 **저장**을 클릭합니다.

Android Enterprise용 VPN 구성

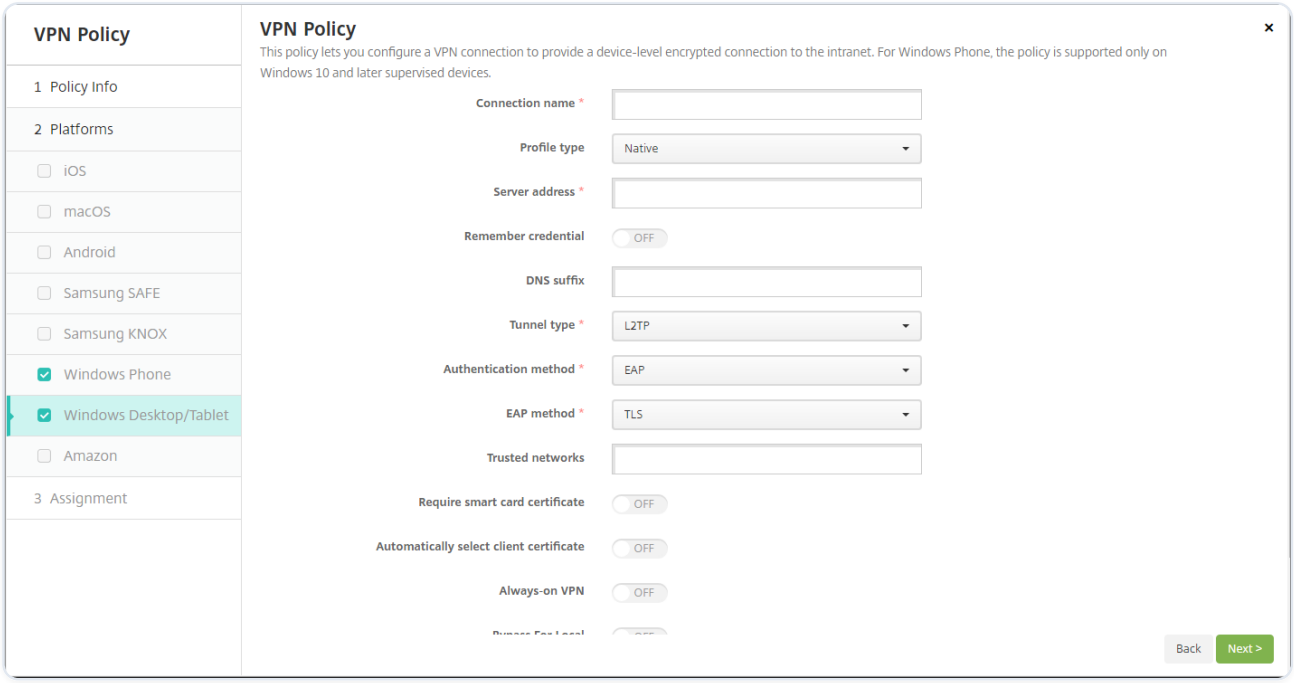
Android Enterprise 디바이스용 VPN을 구성하려면 Citrix SSO 앱에 대한 관리형 구성 디바이스 정책을 생성합니다. Android Enterprise용 VPN 프로필 구성을 참조하십시오.

안드로이드 엔터프라이즈 설정



- **Always-On VPN 사용:** VPN을 항상 켤지 여부를 선택합니다. 기본값은 **끔**입니다. 사용하도록 설정하면 사용자가 수동으로 연결을 끊을 때까지 VPN 연결이 유지됩니다.
- **VPN 패키지:** 디바이스에서 사용하는 VPN 앱의 패키지 이름을 입력합니다.
- **잠금 사용:** 비활성화된 경우 VPN 연결이 없으면 어떤 앱도 네트워크에 액세스할 수 없습니다. 활성화된 경우 다음 설정에서 구성한 앱은 VPN 연결이 없어도 네트워크에 액세스할 수 있습니다. Android 10 이상 디바이스에서 사용할 수 있습니다.
- **잠금에서 제외된 애플리케이션: 추가**를 클릭하여 잠금 설정을 우회하려는 앱의 패키지 이름을 입력합니다.

Windows 데스크톱/태블릿 설정



- **연결 이름:** 연결 이름을 입력합니다. 이 필드는 필수입니다.
- **프로필 유형:** 목록에서 **기본** 또는 **플러그인**을 선택합니다. 기본값은 **기본**입니다.
- **기본 프로필 유형 구성:** 이 설정은 사용자의 Windows 장치에 내장된 VPN에 적용됩니다.
  - **서버 주소:** VPN 서버의 FQDN 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
  - **자격 증명 기억:** 자격 증명을 캐시할지 여부를 선택합니다. 기본값은 **해제**입니다. 활성화되면 가능한 경우 항상 자격 증명이 캐시됩니다.
  - **DNS 접미사:** DNS 접미사를 입력합니다.
  - **터널 유형:** 목록에서 사용할 VPN 터널 유형을 선택합니다. 기본값은 **L2TP**입니다. 가능한 옵션은 다음과 같습니다.
    - **L2TP:** 사전 공유 키 인증을 사용하는 계층 2 터널링 프로토콜.

    - **PPTP:** 지점 간 터널링.
    - **IKEv2:** 인터넷 키 교환 버전 2.
  - **인증 방법:** 목록에서 사용할 인증 방법을 선택합니다. 기본값은 **EAP**입니다. 가능한 옵션은 다음과 같습니다.
    - **EAP:** 확장 인증 프로토콜.
    - **MSChapV2:** 상호 인증을 위해 Microsoft의 챌린지-핸드셰이크 인증을 사용합니다. 이 옵션은 터널 유형으로 **IKEv2**를 선택할 때는 사용할 수 없습니다.
  - **EAP 메서드:** 목록에서 사용할 EAP 메서드를 선택합니다. 기본값은 **TLS**입니다. MSChapV2 인증이 활성화된 경우에는 이 필드를 사용할 수 없습니다. 가능한 옵션은 다음과 같습니다.
    - **TLS:** 전송 계층 보안(Transport Layer Security)
    - **PEAP:** 보호된 확장 가능 인증 프로토콜(Protected Extensible Authentication Protocol)
  - **신뢰할 수 있는 네트워크:** 액세스에 VPN 연결이 필요하지 않은 네트워크 목록을 쉼표로 구분하여 입력합니다. 예를 들어, 사용자가 회사 무선 네트워크에 연결되어 있을 때 보호된 리소스에 직접 액세스할 수 있습니다.
  - **스마트 카드 인증서 필요:** 스마트 카드 인증서가 필요한지 여부를 선택합니다. 기본값은 **해제**입니다.
  - **클라이언트 인증서 자동 선택:** 인증에 사용할 클라이언트 인증서를 자동으로 선택할지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션은 **스마트 카드 인증서 필요**를 활성화하면 사용할 수 없습니다.
  - **항상 VPN 켜기:** VPN을 항상 켤지 여부를 선택합니다. 기본값은 **해제**입니다. 활성화하면 사용자가 수동으로 연결을 끊을 때까지 VPN 연결이 유지됩니다.
  - **로컬 우회:** 로컬 리소스가 프록시 서버를 우회하도록 허용할 주소와 포트 번호를 입력합니다.
- **플러그인 프로필 유형 구성:** 이 설정은 Windows 스토어에서 가져와 사용자 장치에 설치된 VPN 플러그인에 적용됩니다.
  - **서버 주소:** VPN 서버의 FQDN 또는 IP 주소를 입력합니다. 이 필드는 필수입니다.
  - **자격 증명 기억:** 자격 증명을 캐시할지 여부를 선택합니다. 기본값은 **해제**입니다. 활성화하면 가능한 경우 자격 증명이 캐시됩니다.
  - **DNS 접미사:** DNS 접미사를 입력합니다.
  - **클라이언트 앱 ID:** VPN 플러그인의 패키지 제품군 이름을 입력합니다.
  - **플러그인 프로필 XML: 찾아보기**를 클릭하여 파일 위치로 이동한 다음 사용할 사용자 지정 VPN 플러그인 프로필을 선택합니다. 형식 및 세부 정보는 플러그인 공급업체에 문의하십시오.

- **신뢰할 수 있는 네트워크:** 액세스에 VPN 연결이 필요하지 않은 네트워크 목록을 쉼표로 구분하여 입력합니다. 예를 들어, 사용자가 회사 무선 네트워크에 연결되어 있을 때 보호된 리소스에 직접 액세스할 수 있습니다.
- **항상 켜짐 VPN:** VPN을 항상 켤지 여부를 선택합니다. 기본값은 **끔**입니다. 활성화되면 사용자가 수동으로 연결을 끊을 때까지 VPN 연결이 유지됩니다.
- **로컬 우회:** 로컬 리소스가 프록시 서버를 우회하도록 허용하려면 주소와 포트 번호를 입력합니다.

배경화면 기기 정책

.png 또는 .jpg 파일을 추가하여 iOS 기기의 잠금 화면, 홈 화면 또는 둘 다에 배경화면을 설정할 수 있습니다. 감독되는 기기에만 iOS 7.1.2 이상에서 사용할 수 있습니다. iPad와 iPhone에 다른 배경화면을 사용하려면 다른 배경화면 정책을 생성하고 해당 사용자에게 배포해야 합니다.

다음 표에는 Apple이 권장하는 iOS 기기용 이미지 크기가 나와 있습니다.

iPhone

기기	픽셀 단위 이미지 크기
아이폰 12 프로 맥스	2778 x 1284
iPhone 12 및 iPhone 12 Pro	2532 x 1170
아이폰 12 미니	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
아이폰 XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
아이폰 SE 2세대	1334 x 750
아이폰 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750

기기	픽셀 단위 이미지 크기
아이폰 8 플러스	1334 x 750
iPhone 8	1334 x 750

iPad

장치	픽셀 단위 이미지 크기
iPad Pro (1세대, 2세대 및 3세대 12.9인치)	2732 x 2048
iPad Pro 10.5인치	2224 x 1668
iPad Pro (9.7인치)	1536 x 2048
iPad Air 2	2048 x 1536

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을(를) 참조하십시오.

iOS 설정

- **적용 대상:** 목록에서 배경 화면이 표시될 위치를 설정하려면 **잠금 화면**, **홈(아이콘 목록) 화면** 또는 **잠금 및 홈 화면**을 선택합니다.
- **배경 화면 파일: 찾아보기**를 클릭하고 파일 위치로 이동하여 배경 화면 파일을 선택합니다.

웹 콘텐츠 필터 장치 정책

XenMobile에서 장치 정책을 추가하여 Apple의 자동 필터 기능을 사용하여 허용 및 차단 목록에 추가하는 특정 사이트로 iOS 장치의 웹 콘텐츠를 필터링할 수 있습니다. 이 정책은 감독 모드의 iOS 7.0 이상 장치에서만 사용할 수 있습니다. iOS 장치를 감독 모드로 전환하는 방법에 대한 자세한 내용은 Apple Configurator를 사용하여 iOS 장치를 감독 모드로 전환하는 방법을 참조하십시오.

> **참고:**
>
> - Android 장치는 웹 콘텐츠 필터링을 지원하지 않습니다.

- iOS 버전 16.5 이상부터 웹 콘텐츠 필터 장치 정책은 허용 목록에서 `https://localhost`을 인식하지 않습니다. 이 문제로 인해 일부 앱이 응답하지 않게 됩니다. 또한 `http://localhost:`, `http://localhost:*` 등과 같은 URL의 파생 항목을 허용 목록에 추가해도 문제가 해결되지 않습니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **필터 유형:** 드롭다운 목록에서 **내장** 또는 **플러그인**을 클릭한 다음 선택한 옵션에 따라 다음 절차를 따르십시오. 기본값은 **내장**입니다.

내장 필터 유형

- **웹 콘텐츠 필터**
  - **자동 필터 사용:** 부적절한 콘텐츠에 대해 웹 사이트를 분석하기 위해 Apple 자동 필터 기능을 사용할지 여부. 기본값은 **끔**입니다.
  - **허용된 URL: 자동 필터 사용**이 **끔**으로 설정된 경우 이 목록은 무시됩니다. **자동 필터 사용**이 **켬**으로 설정된 경우 자동 필터가 액세스를 허용하는지 여부와 관계없이 이 목록의 항목은 항상 액세스할 수 있습니다. 허용 목록에 추가하려는 각 URL에 대해 **추가**를 클릭하고 다음을 수행하십시오.
    - 허용된 웹 사이트의 URL을 입력하십시오. 웹 주소 앞에 `http://` 또는 `https://`를 추가해야 합니다.
    - 웹 사이트를 허용 목록에 저장하려면 **저장**을 클릭하고 저장하지 않으려면 **취소**를 클릭하십시오.
  - **차단된 URL:** 이 목록의 항목은 항상 차단됩니다. 차단 목록에 추가하려는 각 URL에 대해 **추가**를 클릭하고 다음을 수행하십시오.
    - 차단할 웹사이트의 URL을 입력합니다. 웹 주소 앞에 `http://` 또는 `https://`를 추가해야 합니다.
    - **저장**을 클릭하여 웹사이트를 차단 목록에 저장하거나, **취소**를 클릭하여 저장하지 않습니다.

> **참고:**
>
> XenMobile® Server 콘솔에는 "blacklist" 및 "whitelist"라는 용어가 포함되어 있습니다. 다음 릴리스에서는 이러한 용어를 "block list" 및 "allow list"로 변경할 예정입니다.

- **북마크 화이트리스트**
  - **북마크 화이트리스트:** 사용자가 액세스할 수 있는 사이트를 지정합니다. 웹사이트 액세스를 활성화하려면 해당 URL을 추가합니다.
    - **URL:** 사용자가 액세스할 수 있는 각 웹사이트의 URL입니다. 예를 들어, Secure Hub 스토어에 대한 액세스를 활성화하려면 XenMobile Server URL을 **URL** 목록에 추가합니다. 웹 주소 앞에 `http://` 또는 `https://`를 추가해야 합니다. 이 필드는 필수입니다.
    - **북마크 폴더:** 선택 사항인 북마크 폴더 이름을 입력합니다. 이 필드를 비워두면 북마크가 기본 북마크 디렉터리에 추가됩니다.
    - **제목:** 웹사이트에 대한 설명적인 제목을 입력합니다. 예를 들어, URL `https://google.com`에 대해 "Google"을 입력합니다.
    - **저장**을 클릭하여 웹사이트를 허용 목록에 저장하거나, **취소**를 클릭하여 저장하지 않습니다.

플러그인 필터 유형

- **필터 이름:** 필터의 고유한 이름을 입력합니다.
- **식별자:** 필터링 서비스를 제공하는 플러그인의 번들 ID를 입력합니다.
- **서비스 주소:** 선택 사항인 서버 주소를 입력합니다. 유효한 형식은 IP 주소, 호스트 이름 또는 URL입니다.
- **사용자 이름:** 서비스에 대한 선택 사항인 사용자 이름을 입력합니다.
- **암호:** 서비스에 대한 선택적 암호를 입력합니다.
- **인증서:** 드롭다운 목록에서 사용자를 서비스에 인증하는 데 사용해야 하는 선택적 ID 인증서를 클릭합니다. 기본값은 **없음**입니다.
- **WebKit 트래픽 필터링:** WebKit 트래픽을 필터링할지 여부를 선택합니다.
- **소켓 트래픽 필터링:** 소켓 트래픽을 필터링할지 여부를 선택합니다.
- **사용자 지정 데이터:** 웹 필터에 추가할 각 사용자 지정 키에 대해 **추가**를 클릭한 다음 다음을 수행합니다.
  - **키:** 사용자 지정 키를 입력합니다.
  - **값:** 사용자 지정 키의 값을 입력합니다.
  - 사용자 지정 키를 저장하려면 **저장**을 클릭하고, 저장하지 않으려면 **취소**를 클릭합니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.

- **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
- **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간(숫자)을 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

웹 클립 장치 정책

사용자 장치의 앱과 함께 표시되도록 웹 사이트에 대한 바로 가기 또는 웹 클립을 배치할 수 있습니다. iOS, iPadOS, macOS 및 Android 장치용 웹 클립을 나타내는 사용자 지정 아이콘을 지정할 수 있습니다. Windows 태블릿은 레이블과 URL만 필요합니다. iOS 및 iPadOS 장치의 경우, 생성한 웹 클립을 구성하려면 홈 화면 레이아웃 장치 정책을 구성하십시오. iOS에서 앱 접근을 제한하는 경우, 웹 클립을 허용하도록 제한 장치 정책을 구성해야 합니다. 이러한 정책 구성에 대한 자세한 내용은 홈 화면 레이아웃 장치 정책 및 제한 장치 정책을 참조하십시오.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

iOS 설정

- **레이블:** 웹 클립과 함께 표시될 레이블을 입력합니다.
- **URL:** 웹 클립과 연결된 URL을 입력합니다. URL은 `https://server`과 같이 프로토콜로 시작해야 합니다.
- **제거 가능:** 사용자가 웹 클립을 제거할 수 있는지 여부를 선택합니다. 기본값은 **해제**입니다. 이 옵션은 공유 iPad에서는 지원되지 않습니다.
- **업데이트할 아이콘: 찾아보기**를 클릭하여 파일 위치로 이동한 다음 웹 클립에 사용할 아이콘을 선택합니다.
- **사전 구성된 아이콘:** 아이콘에 효과(둥근 모서리, 그림자, 반사 광택)가 적용되는지 여부를 선택합니다. 기본값은 **해제**이며, 이 경우 효과가 추가됩니다.
- **전체 화면:** 연결된 웹 페이지가 전체 화면 모드로 열리는지 여부를 선택합니다. 기본값은 **해제**입니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간(단위: 시간)을 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

- **프로필 범위:** 정책이 사용자에게 적용되는지 또는 전체 시스템에 적용되는지 선택합니다. 기본값은 **시스템**입니다. iOS 9.3 이상에서만 사용할 수 있습니다.

macOS 설정

- **레이블:** 웹 클립과 함께 표시될 레이블을 입력합니다.
- **URL:** 웹 클립과 연결된 URL을 입력합니다. URL은 `https://server`과 같은 프로토콜로 시작해야 합니다.
- **업데이트할 아이콘:** 찾아보기를 클릭하고 파일 위치로 이동하여 웹 클립에 사용할 아이콘을 선택합니다.

Android 설정

- **규칙:** 이 정책이 웹 클립을 추가할지 제거할지 선택합니다. 기본값은 **추가**입니다.
- **레이블:** 웹 클립과 함께 표시될 레이블을 입력합니다.
- **URL:** 웹 클립과 연결된 URL을 입력합니다.
- **아이콘 정의:** 아이콘 파일을 사용할지 여부를 선택합니다. 기본값은 **해제**입니다.
- **아이콘 파일: 아이콘 정의**가 **설정**인 경우, **찾아보기**를 클릭하고 파일 위치로 이동하여 사용할 아이콘 파일을 선택합니다.
- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지 남은 시간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지 남은 시간(시간):** 정책이 제거될 때까지의 시간을 시간 단위로 입력합니다.
  - **사용자가 정책을 제거하도록 허용:** 사용자가 장치에서 정책을 제거할 수 있는 시기를 선택할 수 있습니다. 메뉴에서 **항상**, **암호 필요** 또는 **안 함**을 선택합니다. **암호 필요**를 선택하는 경우, **제거 암호** 필드에 암호를 입력합니다.
  - **프로필 범위:** 이 정책이 **사용자**에게 적용될지 아니면 전체 **시스템**에 적용될지 선택합니다. 기본값은 **사용자**입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Windows 데스크톱/태블릿 설정

- **이름:** 웹 클립과 함께 표시될 레이블을 입력합니다.
- **URL:** 웹 클립과 연결된 URL을 입력합니다.

Wi-Fi 장치 정책

XenMobile®에서 **구성 > 장치 정책** 페이지를 사용하여 새 Wi-Fi 장치 정책을 생성하거나 기존 정책을 편집합니다. Wi-Fi 정책을 사용하면 다음 항목을 정의하여 사용자가 장치를 Wi-Fi 네트워크에 연결하는 방법을 관리할 수 있습니다.

- 네트워크 이름 및 유형
- 인증 및 보안 정책
- 프록시 서버 사용
- 기타 Wi-Fi 관련 세부 정보

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동하십시오. 자세한 내용은 장치 정책을 참조하십시오.

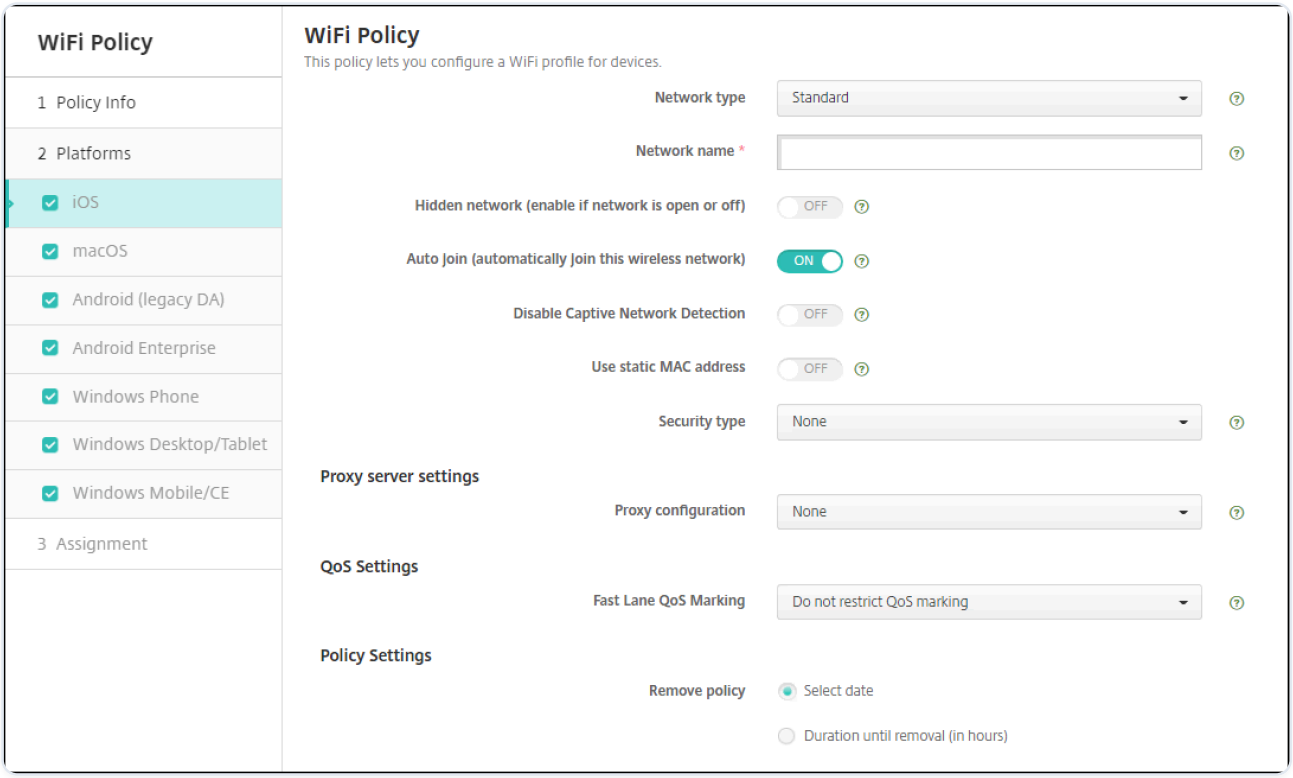
전제 조건

정책을 생성하기 전에 다음 단계를 완료해야 합니다.

- 사용할 모든 딜리버리 그룹을 생성합니다.
- 네트워크 이름과 유형을 알고 있어야 합니다.
- 사용할 인증 또는 보안 유형을 알고 있어야 합니다.
- 필요할 수 있는 프록시 서버 정보를 알고 있어야 합니다.
- 필요한 CA 인증서를 설치합니다.
- 필요한 공유 키를 가지고 있어야 합니다.
- 인증서 기반 인증을 위한 PKI 엔터티를 생성합니다.
- 자격 증명 공급자를 구성합니다.

자세한 내용은 인증 및 해당 하위 문서를 참조하십시오.

iOS 설정



- **네트워크 유형:** 목록에서 사용할 네트워크 유형을 설정하려면 **Standard**, **Legacy Hotspot** 또는 **Hotspot 2.0**을 선택합니다.
- **네트워크 이름:** 장치에서 사용 가능한 네트워크 목록에 표시되는 SSID를 입력합니다. **Hotspot 2.0**에는 적용되지 않습니다.
- **숨겨진 네트워크(네트워크가 열려 있거나 꺼져 있는 경우 활성화):** 네트워크를 숨길지 여부를 선택합니다.
- **자동 연결(이 무선 네트워크에 자동으로 연결):** 네트워크에 자동으로 연결할지 여부를 선택합니다. iOS 장치가 이미 다른 네트워크에 연결되어 있는 경우 이 네트워크에 연결되지 않습니다. 장치가 자동으로 연결되기 전에 사용자가 이전 네트워크에서 연결을 끊어야 합니다. 기본값은 **켜짐**입니다.
- **고정 MAC 주소 사용:** MAC 주소는 장치가 네트워크 내에서 전송하는 고유 식별자입니다. 개인 정보 보호를 강화하기 위해 iOS 및 iPadOS 장치는 네트워크에 연결할 때마다 다른 MAC 주소를 사용할 수 있습니다. **켜짐**으로 설정하면 장치는 이 네트워크에 연결할 때 항상 동일한 MAC 주소를 사용합니다. **꺼짐**으로 설정하면 장치는 이 네트워크에 연결할 때마다 다른 MAC 주소를 사용합니다. 기본값은 **꺼짐**입니다.
- **보안 유형:** 목록에서 사용할 보안 유형을 선택합니다. **Hotspot 2.0**에는 적용되지 않습니다.
  - 없음 - 추가 구성이 필요하지 않습니다.
  - WEP
  - WPA/WPA2 개인
  - 모든 (개인)

- WEP 엔터프라이즈
- WPA/WPA2 Enterprise: WPA-2 Enterprise를 사용하려면 SCEP(Simple Certificate Enrollment Protocol)를 구성해야 합니다. 그러면 XenMobile이 Wi-Fi 서버에 인증하기 위해 장치로 인증서를 보낼 수 있습니다. SCEP를 구성하려면 **설정 > 자격 증명 공급자**의 배포 페이지로 이동합니다. 자세한 내용은 자격 증명 공급자를 참조하십시오.
- 모두(엔터프라이즈)

다음 섹션에서는 이전 연결 유형 각각에 대해 구성하는 옵션을 나열합니다.

iOS용 WPA, WPA Personal, 모두(Personal) 설정

암호: 선택적 암호를 입력합니다. 이 필드를 비워두면 사용자가 로그인할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.

iOS용 WEP 엔터프라이즈, WPA 엔터프라이즈, WPA2 엔터프라이즈, 모두 (엔터프라이즈) 설정

이러한 설정 중 하나를 선택하면 해당 설정이 **프록시 서버 설정** 다음에 나열됩니다.

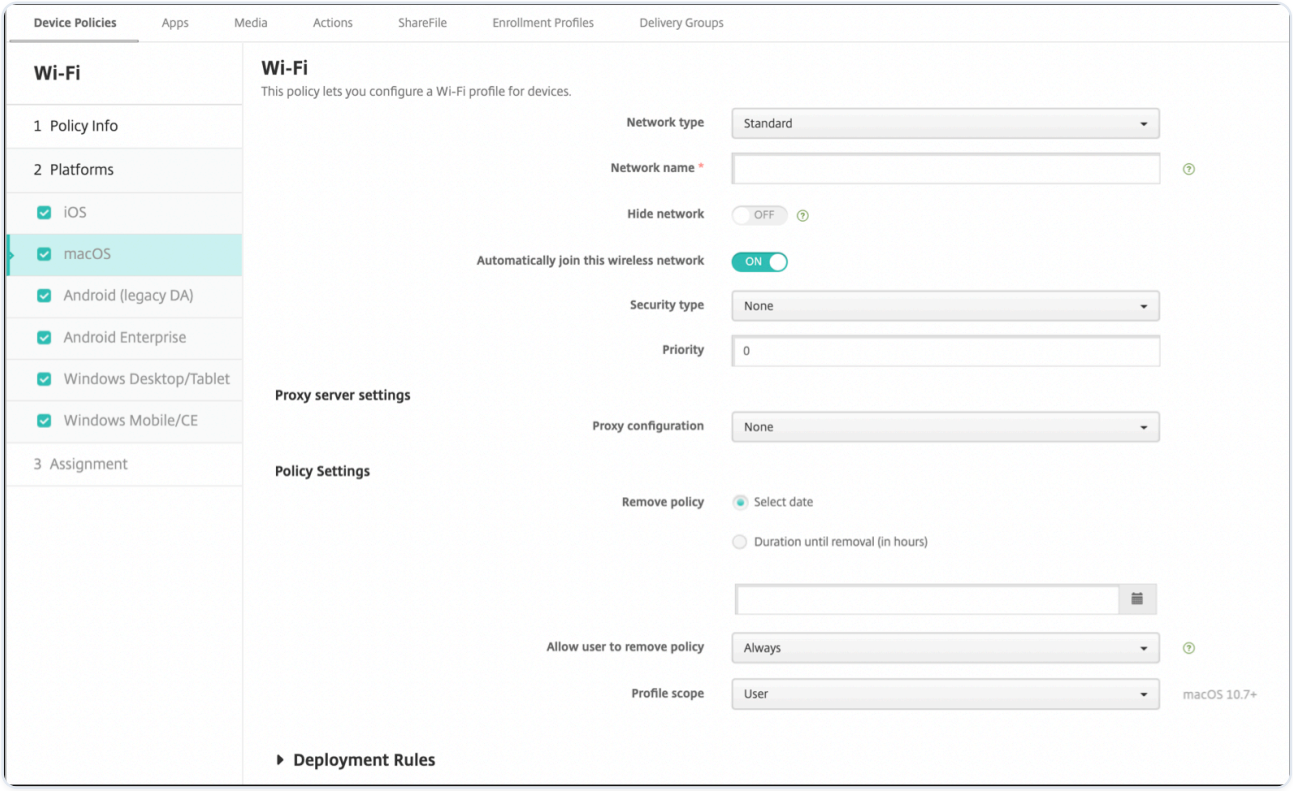
- **프로토콜, 허용되는 EAP 유형:** 지원하려는 EAP 유형을 사용하도록 설정한 다음 관련 설정을 구성합니다. 사용 가능한 각 EAP 유형의 기본값은 **해제**입니다.
- **내부 인증(TTLS):** *TTLS를 사용하도록 설정한 경우에만 필요합니다.* 목록에서 사용할 내부 인증 방법을 선택합니다. 옵션은 **PAP**, **CHAP**, **MSCHAP**, 또는 **MSCHAPv2**입니다. 기본값은 **MSCHAPv2**입니다.
- **프로토콜, EAP-FAST:** 보호된 액세스 자격 증명(PAC)을 사용할지 여부를 선택합니다.
  - **PAC 사용**을 선택하는 경우, 프로비저닝 PAC를 사용할지 여부를 선택합니다.
    - **프로비저닝 PAC**를 선택하는 경우, 최종 사용자 클라이언트와 XenMobile 간에 익명 TLS 핸드셰이크를 허용할지 여부를 선택합니다.
      - **익명으로 PAC 프로비저닝**
- **인증:**
  - **사용자 이름:** 사용자 이름을 입력합니다.
  - **연결별 암호:** 사용자가 로그온할 때마다 암호를 요구할지 여부를 선택합니다.
  - **암호:** 선택적 암호를 입력합니다. 이 필드를 비워두면 사용자가 로그온할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.
  - **ID 자격 증명(키 저장소 또는 PKI 자격 증명):** 목록에서 ID 자격 증명 유형을 선택합니다. 기본값은 **없음**입니다.

- **외부 ID: PEAP**, **TTLS**, *또는* **EAP-FAST**를 활성화한 경우에만 *필요합니다*. 외부에 표시되는 사용자 이름을 입력합니다. 사용자 이름이 표시되지 않도록 "anonymous"와 같은 일반적인 용어를 입력하여 보안을 강화할 수 있습니다.
- **TLS 인증서 요구:** TLS 인증서를 요구할지 여부를 선택합니다.

- **신뢰**
  - **신뢰할 수 있는 인증서:** 신뢰할 수 있는 인증서를 추가하려면 **추가**를 클릭하고 추가하려는 각 인증서에 대해 다음을 수행합니다.
    - **응용 프로그램:** 목록에서 추가하려는 응용 프로그램을 선택합니다.
    - 인증서를 저장하려면 **저장**을 클릭하거나 **취소**를 클릭합니다.
  - **신뢰할 수 있는 서버 인증서 이름:** 신뢰할 수 있는 서버 인증서 일반 이름을 추가하려면 **추가**를 클릭하고 추가하려는 각 이름에 대해 다음을 수행합니다.
    - **인증서:** 서버 인증서 이름을 입력합니다. wpa.*.example.com과 같이 와일드카드를 사용하여 이름을 지정할 수 있습니다.
    - 인증서 이름을 저장하려면 **저장**을 클릭하거나 **취소**를 클릭합니다.
- **신뢰 예외 허용:** 인증서가 신뢰할 수 없는 경우 사용자 장치에 인증서 신뢰 대화 상자가 나타날지 여부를 선택합니다. 기본값은 **켜짐**입니다.
- **프록시 서버 설정**
  - **프록시 구성:** 목록에서 **없음**, **수동** 또는 **자동**을 선택하여 VPN 연결이 프록시 서버를 통해 라우팅되는 방식을 설정한 다음 추가 옵션을 구성합니다. 기본값은 추가 구성이 필요 없는 **없음**입니다.
  - **수동**을 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 서버에 인증하기 위한 선택적 사용자 이름을 입력합니다.
    - **암호:** 프록시 서버에 인증하기 위한 선택적 암호를 입력합니다.
  - **자동**을 선택하는 경우 다음 설정을 구성합니다.
    - **서버 URL:** 프록시 구성을 정의하는 PAC 파일의 URL을 입력합니다.
    - **PAC에 연결할 수 없는 경우 직접 연결 허용:** PAC 파일에 연결할 수 없는 경우 사용자가 대상에 직접 연결하도록 허용할지 여부를 선택합니다. 기본값은 **켜짐**입니다. 이 옵션은 iOS 7.0 이상에서만 사용할 수 있습니다.

- **정책 설정**
  - **정책 제거:** 정책 제거 일정을 예약하는 방법을 선택합니다. 사용 가능한 옵션은 **날짜 선택** 및 **제거까지의 기간(시간)**입니다.
    - **날짜 선택:** 달력을 클릭하여 제거할 특정 날짜를 선택합니다.
    - **제거까지의 기간(시간):** 정책 제거가 발생할 때까지의 시간을 숫자로 입력합니다. iOS 6.0 이상에서만 사용할 수 있습니다.

macOS 설정



- **네트워크 유형:** 목록에서 사용할 네트워크 유형을 설정하려면 **Standard**, **Legacy Hotspot** 또는 **Hotspot 2.0**을 선택합니다.
- **네트워크 이름:** 장치에 사용 가능한 네트워크 목록에 표시되는 SSID를 입력합니다. **Hotspot 2.0**에는 적용되지 않습니다.
- **네트워크 숨기기:** 네트워크를 숨길지 여부를 선택합니다.
- **이 무선 네트워크에 자동으로 연결:** 네트워크에 자동으로 연결할지 여부를 선택합니다. 장치가 이미 다른 네트워크에 연결되어 있으면 이 네트워크에 연결되지 않습니다. 장치가 자동으로 연결되기 전에 사용자가 이전 네트워크에서 연결을 끊어야 합니다. 기본값은 **켜기**입니다.
- **보안 유형:** 목록에서 사용할 보안 유형을 선택합니다. **Hotspot 2.0**에는 적용되지 않습니다.
  - 없음 - 추가 구성이 필요하지 않습니다.

- WEP
- WPA/WPA2 개인
- 모두 (개인)
- WEP 엔터프라이즈
- WPA/WPA2 엔터프라이즈
- 모두 (엔터프라이즈)

- **우선 순위:** 여러 네트워크가 있는 경우 **우선 순위** 필드에 숫자를 입력하여 네트워크 연결의 우선 순위를 설정합니다. 장치는 가장 낮은 숫자의 네트워크를 선택합니다.

다음 섹션에서는 이전 연결 유형 각각에 대해 구성하는 옵션을 나열합니다.

macOS용 WPA, WPA 개인, WPA 2 개인, 모두 (개인) 설정

- **암호:** 선택적 암호를 입력합니다. 이 필드를 비워두면 사용자가 로그인할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, 모든 (엔터프라이즈) macOS 설정

이러한 설정 중 하나를 선택하면 해당 설정이 **프록시 서버 설정** 다음에 나열됩니다.

- **프로토콜, 허용되는 EAP 유형:** 지원하려는 EAP 유형을 활성화한 다음 관련 설정을 구성합니다. 사용 가능한 각 EAP 유형의 기본값은 **해제**입니다.
- **내부 인증 (TTLS):** *TTLS를 활성화하는 경우에만 필요합니다.* 목록에서 사용할 내부 인증 방법을 선택합니다. 옵션은 **PAP**, **CHAP**, **MSCHAP**, 또는 **MSCHAPv2**입니다. 기본값은 **MSCHAPv2**입니다.
- **프로토콜, EAP-FAST:** 보호된 액세스 자격 증명(PAC)을 사용할지 여부를 선택합니다.
  - **PAC 사용**을 선택하는 경우 프로비저닝 PAC를 사용할지 여부를 선택합니다.
    - **프로비저닝 PAC**를 선택하는 경우 최종 사용자 클라이언트와 XenMobile 간에 익명 TLS 핸드셰이크를 허용할지 여부를 선택합니다.
      - **익명으로 PAC 프로비저닝**
- **인증:**
  - **사용자 이름:** 사용자 이름을 입력합니다.
  - **연결별 암호:** 사용자가 로그인할 때마다 암호를 요구할지 여부를 선택합니다.
  - **암호:** 선택적 암호를 입력합니다. 이 필드를 비워두면 사용자가 로그인할 때 암호를 입력하라는 메시지가 표시될 수 있습니다.

- **ID 자격 증명 (키 저장소 또는 PKI 자격 증명):** 목록에서 ID 자격 증명 유형을 선택합니다. 기본값은 **없음**입니다.
- **외부 ID:** *다음 중 하나를 활성화할 때만 필요합니다:* **PEAP**, **TTLS**, *또는* **EAP-FAST**. 외부에 표시되는 사용자 이름을 입력합니다. 사용자 이름이 표시되지 않도록 'anonymous'와 같은 일반적인 용어를 입력하여 보안을 강화할 수 있습니다.
- **TLS 인증서 필요:** TLS 인증서가 필요한지 여부를 선택합니다.

- **신뢰**
  - **신뢰할 수 있는 인증서:** 신뢰할 수 있는 인증서를 추가하려면 **추가**를 클릭하고 추가하려는 각 인증서에 대해 다음을 수행합니다.
    - **애플리케이션:** 목록에서 추가하려는 애플리케이션을 선택합니다.
    - **저장**을 클릭하여 인증서를 저장하거나 **취소**를 클릭합니다.
  - **신뢰할 수 있는 서버 인증서 이름:** 신뢰할 수 있는 서버 인증서 일반 이름을 추가하려면 **추가**를 클릭하고 추가하려는 각 이름에 대해 다음을 수행합니다.
    - **인증서:** 추가하려는 서버 인증서의 이름을 입력합니다. wpa.*.example.com과 같이 와일드카드를 사용하여 이름을 지정할 수 있습니다.
    - **저장**을 클릭하여 인증서 이름을 저장하거나 **취소**를 클릭합니다.
- **신뢰 예외 허용:** 인증서가 신뢰할 수 없는 경우 사용자 장치에 인증서 신뢰 대화 상자가 나타날지 여부를 선택합니다. 기본값은 **켜짐**입니다.
- **로그인 창 구성으로 사용:** 로그인 창에 입력된 동일한 자격 증명을 사용하여 사용자를 인증할지 여부를 선택합니다.
- **프록시 서버 설정**
  - **프록시 구성:** 목록에서 **없음**, **수동** 또는 **자동**을 선택하여 VPN 연결이 프록시 서버를 통해 라우팅되는 방식을 설정한 다음 추가 옵션을 구성합니다. 기본값은 **없음**이며, 추가 구성이 필요하지 않습니다.
  - **수동**을 선택한 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 서버에 인증하기 위한 선택적 사용자 이름을 입력합니다.
    - **암호:** 프록시 서버에 인증하기 위한 선택적 암호를 입력합니다.
  - **자동**을 선택하는 경우 다음 설정을 구성합니다.

- **서버 URL:** 프록시 구성을 정의하는 PAC 파일의 URL을 입력합니다.
- **PAC에 연결할 수 없는 경우 직접 연결 허용:** PAC 파일에 연결할 수 없는 경우 사용자가 대상에 직접 연결하도록 허용할지 여부를 선택합니다. 기본값은 **켜기**입니다. 이 옵션은 iOS 7.0 이상에서만 사용할 수 있습니다.

Android 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policy-wifi-android.png)

- **네트워크 이름:** 사용자 장치의 사용 가능한 네트워크 목록에 있는 SSID를 입력합니다.
- **인증:** 목록에서 Wi-Fi 연결에 사용할 보안 유형을 선택합니다.
  - 열기
  - 공유
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

다음 섹션에서는 이전 연결 유형 각각에 대해 구성하는 옵션을 나열합니다.

Android용 Open, Shared 설정

- **암호화:** 목록에서 **비활성화됨** 또는 **WEP**를 선택합니다. 기본값은 **WEP**입니다.
- **암호:** 선택 사항인 암호를 입력합니다.

Android용 WPA, WPA-PSK, WPA2, WPA2-PSK 설정

- **암호화:** 목록에서 **TKIP** 또는 **AES**를 선택합니다. 기본값은 **TKIP**입니다.
- **암호:** 선택 사항인 암호를 입력합니다.

Android용 802.1x 설정

- **EAP 유형:** 목록에서 **PEAP**, **TLS** 또는 **TTLS**를 선택합니다. 기본값은 **PEAP**입니다.
- **암호:** 선택 사항인 암호를 입력합니다.
- **인증 2단계:** 목록에서 **없음**, **PAP**, **MSCHAP**, **MSCHAPPv2** 또는 **GTC**를 선택합니다. 기본값은 **PAP**입니다.
- **ID:** 선택 사항인 사용자 이름과 도메인을 입력합니다.

- **익명:** 선택 사항인 외부에서 보이는 사용자 이름을 입력합니다. 사용자 이름이 보이지 않도록 "anonymous"와 같은 일반적인 용어를 입력하여 보안을 강화할 수 있습니다.
- **CA 인증서:** 목록에서 사용할 인증서를 선택합니다.
- **신원 자격 증명:** 목록에서 사용할 신원 자격 증명을 선택합니다. 기본값은 **없음**입니다.
- **숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우 활성화):** 네트워크를 숨길지 여부를 선택합니다.

안드로이드 엔터프라이즈 설정

Wi-Fi 정책 Android Enterprise 이미지(/en-us/xenmobile/server/media/device-policy-wifi-android-enterprise.png)

- **네트워크 이름:** 사용자 장치에서 사용 가능한 네트워크 목록에 있는 SSID를 입력합니다.
- **인증:** 목록에서 Wi-Fi 연결에 사용할 보안 유형을 선택합니다.
  - 개방
  - 공유
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

다음 섹션에서는 이전 연결 유형 각각에 대해 구성하는 옵션을 나열합니다.

Android Enterprise용 개방, 공유 설정

- **암호화:** 목록에서 **Disabled** 또는 **WEP**를 선택합니다. 기본값은 **WEP**입니다.
- **암호:** 선택적 암호를 입력합니다.

Android Enterprise용 WPA, WPA-PSK, WPA2, WPA2-PSK 설정

- **암호화:** 목록에서 TKIP 또는 AES를 선택합니다. 기본값은 TKIP입니다.
- **암호:** 선택적 암호를 입력합니다.

Android Enterprise용 802.1x 설정

- **EAP 유형:** 목록에서 **PEAP**, **TLS** 또는 **TTLS**를 선택합니다. 기본값은 **PEAP**입니다.
- **암호:** 선택적 암호를 입력합니다.

- **인증 2단계:** 목록에서 **None**, **PAP**, **MSCHAP**, **MSCHAPPv2** 또는 **GTC**를 선택합니다. 기본값은 **PAP**입니다.
- **ID:** 선택적 사용자 이름과 도메인을 입력합니다.
- **익명:** 선택적이며 외부에서 볼 수 있는 사용자 이름을 입력합니다. 사용자 이름이 보이지 않도록 “anonymous”와 같은 일반적인 용어를 입력하여 보안을 강화할 수 있습니다.
- **CA 인증서:** 목록에서 사용할 인증서를 선택합니다.
- **도메인:** 필수 도메인 이름을 입력합니다. 자세한 내용은 도메인을 참조하십시오.

> **참고:**
>
> Android 13 이상을 실행하는 장치에서 Wi-Fi 정책을 구성할 때 **CA certificate** 및 **Domain** 필드는 필수로 업데이트해야 합니다. 업데이트되지 않으면 구성이 실패합니다.

- **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 **없음**입니다.
- **숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우 활성화):** 네트워크를 숨길지 여부를 선택합니다.

Windows 10 및 Windows 11 설정

장치 정책 구성 화면 이미지(/en-us/xenmobile/server/media/device-policy-wifi-windesktop.png)

- **인증:** 드롭다운 목록에서 Wi-Fi 연결에 사용할 보안 유형을 클릭합니다.
  - 개방형
  - WPA 개인
  - WPA-2 개인
  - WPA 엔터프라이즈
  - WPA-2 엔터프라이즈: WPA-2 엔터프라이즈를 사용하려면 SCEP를 구성해야 합니다. SCEP 구성은 XenMobile이 Wi-Fi 서버에 인증하기 위해 장치에 인증서를 보낼 수 있도록 합니다. SCEP를 구성하려면 **설정 > 자격 증명 공급자**의 **배포** 페이지로 이동합니다. 자세한 내용은 자격 증명 공급자를 참조하십시오.

다음 섹션에서는 이전 연결 유형 각각에 대해 구성하는 옵션을 나열합니다.

Windows 10 및 Windows 11용 개방형 설정

- **숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우 활성화):** 네트워크를 숨길지 여부를 선택합니다.
- **자동 연결:** 네트워크에 자동으로 연결할지 여부를 선택합니다.

Windows 10 및 Windows 11용 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 경우 활성화):** 네트워크가 숨겨져 있는지 여부를 선택합니다.
- **자동으로 연결:** 네트워크에 자동으로 연결할지 여부를 선택합니다.

Windows 10 및 Windows 11용 WPA-2 Enterprise 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:** 네트워크가 숨겨져 있는지 여부를 선택합니다.
- **자동으로 연결:** 네트워크에 자동으로 연결할지 여부를 선택합니다.
- **SCEP를 통해 인증서 푸시:** Simple Certificate Enrollment Protocol (SCEP)을 사용하여 사용자 장치에 인증서를 푸시할지 여부를 선택합니다.
- **SCEP용 자격 증명 공급자:** 목록에서 SCEP 자격 증명 공급자를 선택합니다. 기본값은 **없음**입니다.

Windows 정보 보호 장치 정책

이전에는 엔터프라이즈 데이터 보호(EDP)로 알려졌던 Windows Information Protection(WIP)은 엔터프라이즈 데이터의 잠재적 유출을 방지하는 Windows 기술입니다. 데이터 유출은 엔터프라이즈 데이터를 엔터프라이즈 보호되지 않은 앱과 공유하거나, 앱 간에 공유하거나, 조직 네트워크 외부로 공유할 때 발생할 수 있습니다. 자세한 내용은 Windows Information Protection(WIP)을 사용하여 엔터프라이즈 데이터 보호를 참조하십시오.

XenMobile®에서 장치 정책을 생성하여 설정한 적용 수준에서 Windows Information Protection이 필요한 앱을 지정할 수 있습니다. Windows Information Protection 정책은 Windows 10 또는 Windows 11을 실행하는 감독되는 태블릿 및 데스크톱용입니다.

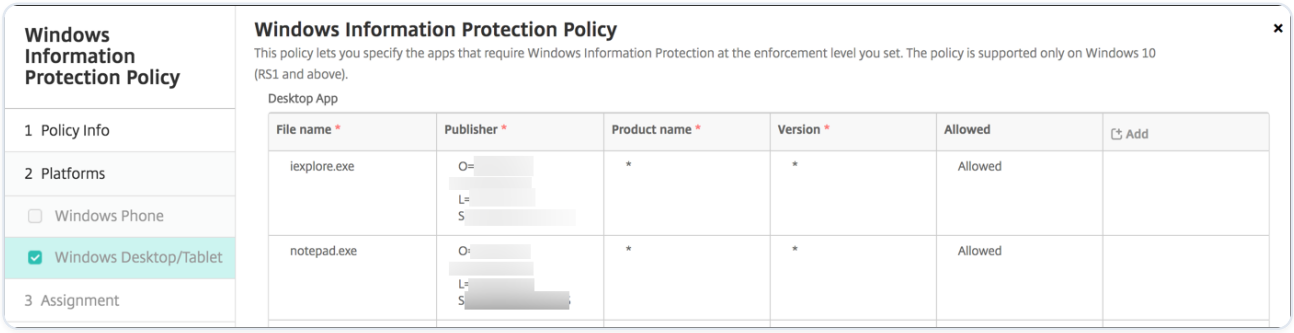
XenMobile에는 몇 가지 일반적인 앱이 포함되어 있으며 다른 앱을 추가할 수 있습니다. 정책에 대해 사용자 환경에 영향을 미치는 적용 수준을 지정합니다. 예를 들어 다음을 수행할 수 있습니다.

- 부적절한 데이터 공유를 차단합니다.
- 부적절한 데이터 공유에 대해 경고하고 사용자가 정책을 재정의하도록 허용합니다.
- 부적절한 데이터 공유를 로깅하고 허용하면서 WIP를 자동으로 실행합니다.

Windows Information Protection에서 앱을 제외하려면 Microsoft AppLocker XML 파일에 앱을 정의한 다음 해당 파일을 XenMobile로 가져옵니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

Windows 10 및 Windows 11 설정



- **데스크톱 앱** (Windows 10 또는 Windows 11 데스크톱), **스토어 앱** (Windows 10 또는 Windows 11 태블릿): XenMobile에는 이전 샘플에 표시된 대로 몇 가지 일반적인 앱이 포함되어 있습니다. 필요에 따라 해당 앱을 편집하거나 제거할 수 있습니다.

  다른 앱을 추가하려면: **데스크톱 앱** 또는 **스토어 앱** 테이블에서 **추가**를 클릭하고 앱 정보를 제공합니다.

  허용된 앱은 엔터프라이즈 데이터를 읽고, 생성하고, 업데이트할 수 있습니다. **거부된** 앱은 엔터프라이즈 데이터에 액세스할 수 없습니다. **제외된** 앱은 엔터프라이즈 데이터를 읽을 수 있지만 데이터를 생성하거나 수정할 수는 없습니다.

  - **AppLocker XML:** Microsoft는 WIP와 호환성 문제가 있는 것으로 알려진 Microsoft 앱 목록을 제공합니다. 해당 앱을 WIP에서 제외하려면 **찾아보기**를 클릭하여 목록을 업로드합니다. XenMobile은 업로드된 AppLocker XML과 구성된 데스크톱 및 스토어 앱을 장치로 전송되는 정책에 결합합니다. 자세한 내용은 Windows Information Protection 권장 차단 목록을 참조하십시오.
  - **적용 수준:** Windows 정보 보호가 데이터 공유를 보호하고 관리하는 방법을 지정하는 옵션을 선택합니다. 기본값은 **해제**입니다.
    - **0-해제:** WIP가 해제되어 데이터를 보호하거나 감사하지 않습니다.
    - **1-자동:** WIP가 자동으로 실행되어 부적절한 데이터 공유를 기록하지만 아무것도 차단하지 않습니다. 보고 CSP를 통해 로그에 액세스할 수 있습니다.

    - **2-재정의:** WIP는 잠재적으로 안전하지 않은 데이터 공유에 대해 사용자에게 경고합니다. 사용자는 경고를 재정의하고 데이터를 공유할 수 있습니다. 이 모드는 사용자 재정의를 포함한 작업을 감사 로그에 기록합니다.
    - **3-차단:** WIP는 사용자가 잠재적으로 안전하지 않은 데이터 공유를 완료하지 못하도록 방지합니다.

- **보호된 도메인 이름:** 엔터프라이즈가 사용자 ID에 사용하는 도메인입니다. 관리되는 ID 도메인 목록은 기본 도메인과 함께 관리 엔터프라이즈의 ID를 구성합니다. 목록의 첫 번째 도메인은 Windows UI에서 사용되는 기본 회사 ID입니다. 목록 항목을 구분하려면 "|"를 사용합니다. 예: `domain1.com | domain2.com`
- **데이터 복구 인증서: 찾아보기**를 클릭한 다음 암호화된 파일의 데이터 복구에 사용할 복구 인증서를 선택합니다. 이 인증서는 EFS(파일 암호화 시스템)의 데이터 복구 에이전트(DRA) 인증서와 동일하며, 그룹 정책 대신 MDM을 통해 제공됩니다. 복구 인증서를 사용할 수 없는 경우 생성합니다. 자세한 내용은 이 섹션의 "데이터 복구 인증서 만들기"를 참조하십시오.
- **네트워크 도메인 이름:** 엔터프라이즈의 경계를 구성하는 도메인 목록입니다. WIP는 이 목록에 있는 FQDN(정규화된 도메인 이름)으로의 모든 트래픽을 보호합니다. 이 설정은 **IP 범위** 설정과 함께 네트워크 엔드포인트가 개인 네트워크에서 엔터프라이즈인지 개인인지 감지합니다. 목록 항목을 구분하려면 쉼표를 사용합니다. 예: corp.example.com,region.example.com
- **IP 범위:** 엔터프라이즈 네트워크의 컴퓨터를 정의하는 엔터프라이즈 IPv4 및 IPv6 범위 목록입니다. WIP는 이러한 위치를 엔터프라이즈 데이터 공유를 위한 안전한 대상으로 간주합니다. 목록 항목을 구분하려면 쉼표를 사용합니다. 예:

  `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **IP 범위 목록이 신뢰할 수 있음:** Windows에서 IP 범위의 자동 감지를 방지하려면 이 설정을 **켜기**로 변경합니다. 기본값은 **끄기**입니다.
- **프록시 서버:** 엔터프라이즈가 회사 리소스에 사용할 수 있는 프록시 서버 목록입니다. 네트워크에서 프록시를 사용하는 경우 이 설정이 필요합니다. 프록시 서버가 없으면 클라이언트가 프록시 뒤에 있을 때 엔터프라이즈 리소스를 사용할 수 없을 수 있습니다. 예를 들어, 호텔 및 레스토랑의 특정 Wi-Fi 핫스팟에서 리소스를 사용할 수 없을 수 있습니다. 목록 항목을 구분하려면 쉼표를 사용합니다. 예:

  `proxy.example.com:80;157.54.11.118:443`
- **내부 프록시 서버:** 장치가 클라우드 리소스에 도달하기 위해 통과하는 프록시 서버 목록입니다. 이 서버 유형을 사용하면 연결하는 클라우드 리소스가 엔터프라이즈 리소스임을 나타냅니다. WIP로 보호되지 않는 트래픽에 사용되는 **프록시 서버** 설정의 서버는 이 목록에 포함하지 마십시오. 목록 항목을 구분하려면 쉼표를 사용합니다. 예:

  `example.internalproxy1.com;10.147.80.50`

- **클라우드 리소스:** WIP로 보호되는 클라우드 리소스 목록입니다. 각 클라우드 리소스에 대해, 해당 클라우드 리소스의 트래픽을 라우팅하도록 **프록시 서버** 목록에서 프록시 서버를 선택적으로 지정할 수 있습니다. **프록시 서버**를 통해 라우팅되는 모든 트래픽은 엔터프라이즈 트래픽으로 처리됩니다. 목록 항목은 쉼표로 구분합니다. 예를 들어:

  `domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.domain2.com`

- **등록 취소 시 WIP 인증서 해지:** 사용자 장치가 Windows Information Protection에서 등록 취소될 때 로컬 암호화 키를 해지할지 여부를 지정합니다. 암호화 키가 해지되면 사용자는 암호화된 회사 데이터에 액세스할 수 없습니다. **끔**으로 설정하면 키가 해지되지 않으며 사용자는 등록 취소 후에도 보호된 파일에 계속 액세스할 수 있습니다. 기본값은 **켬**입니다.
- **오버레이 아이콘 표시:** 탐색기의 회사 파일 및 시작 메뉴의 엔터프라이즈 전용 앱 타일에 Windows Information Protection 아이콘 오버레이를 포함할지 여부를 지정합니다. 기본값은 **끔**입니다.

데이터 복구 인증서 만들기

데이터 복구 인증서는 **Windows Information Protection** 정책을 활성화하는 데 필요합니다.

1. XenMobile 콘솔이 실행 중인 컴퓨터에서 명령 프롬프트를 열고 인증서를 만들려는 폴더(Windows\\System32 제외)로 이동합니다.
2. 다음 명령을 실행합니다:

   `cipher /r:ESFDRA`

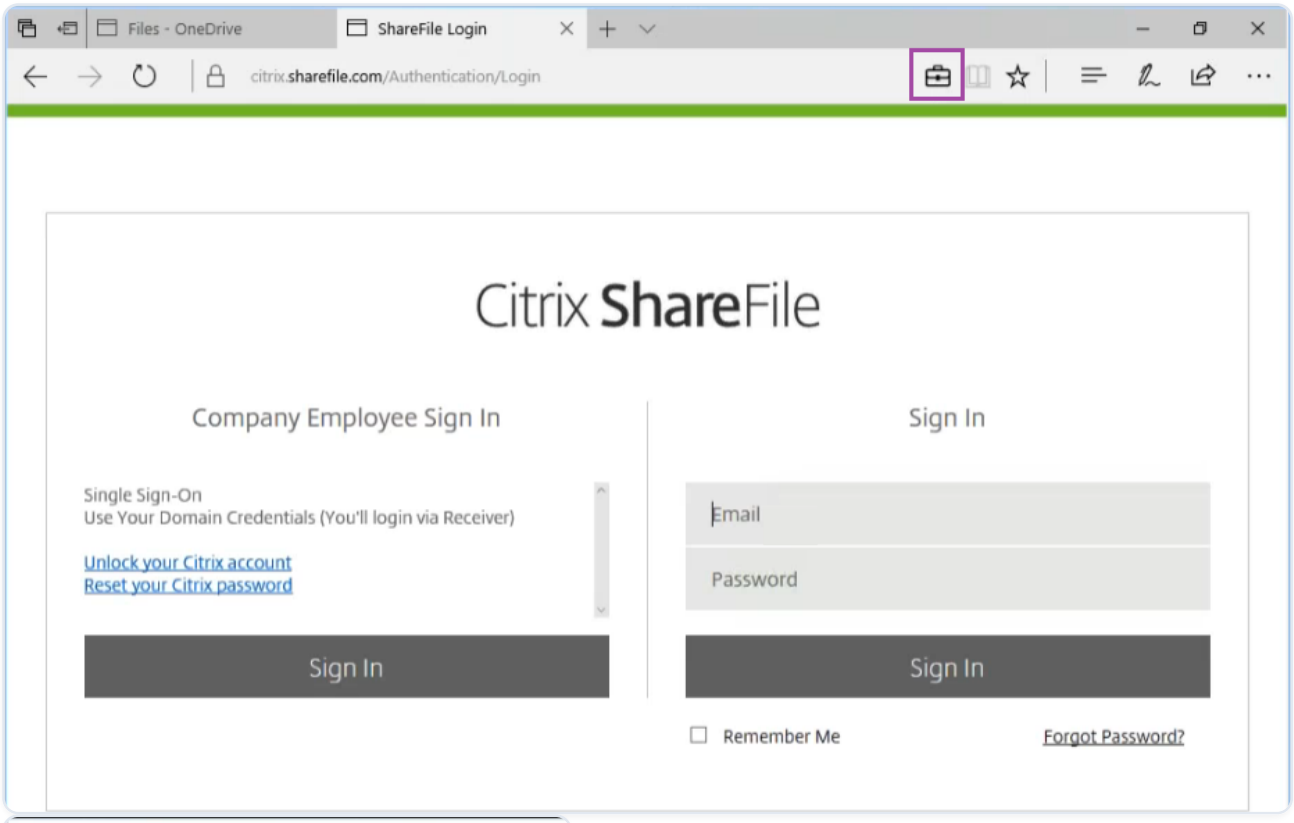
3. 메시지가 표시되면 개인 키 파일을 보호할 암호를 입력합니다.

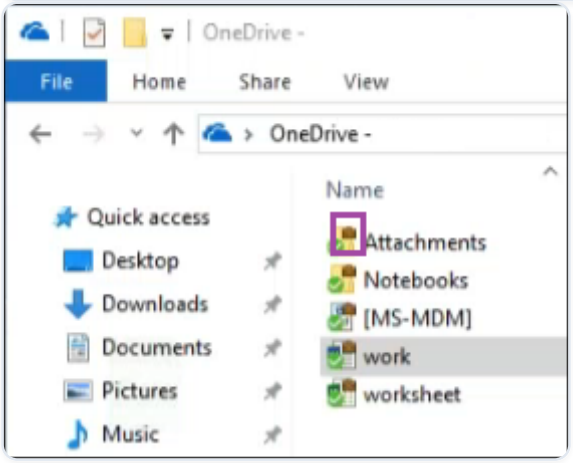
   cipher 명령은 .cer 및 .pfx 파일을 생성합니다.

4. XenMobile 콘솔에서 **설정 > 인증서**로 이동하여 Windows 10 및 Windows 11 태블릿에 적용되는 .cer 파일을 가져옵니다.

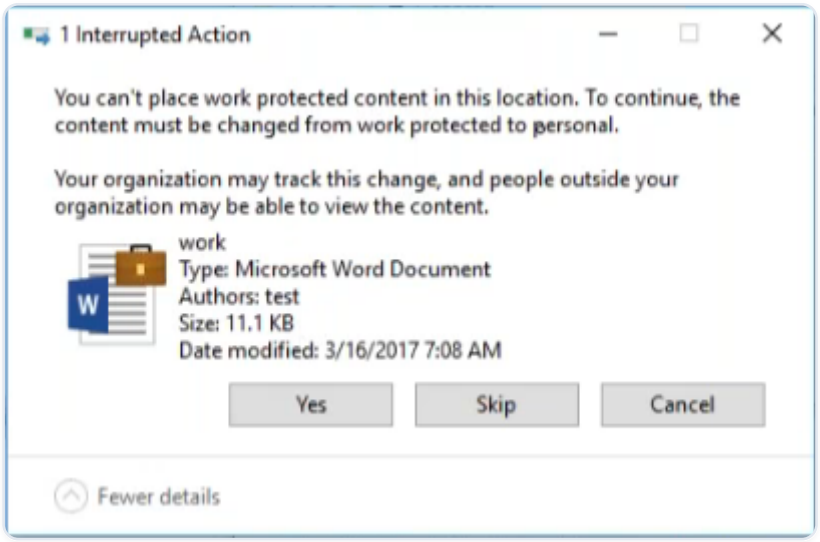
사용자 경험

Windows Information Protection이 적용되면 앱과 파일에 아이콘이 포함됩니다:





사용자가 보호된 파일을 보호되지 않은 위치로 복사하거나 저장하면 구성된 적용 수준에 따라 다음 알림이 나타납니다.

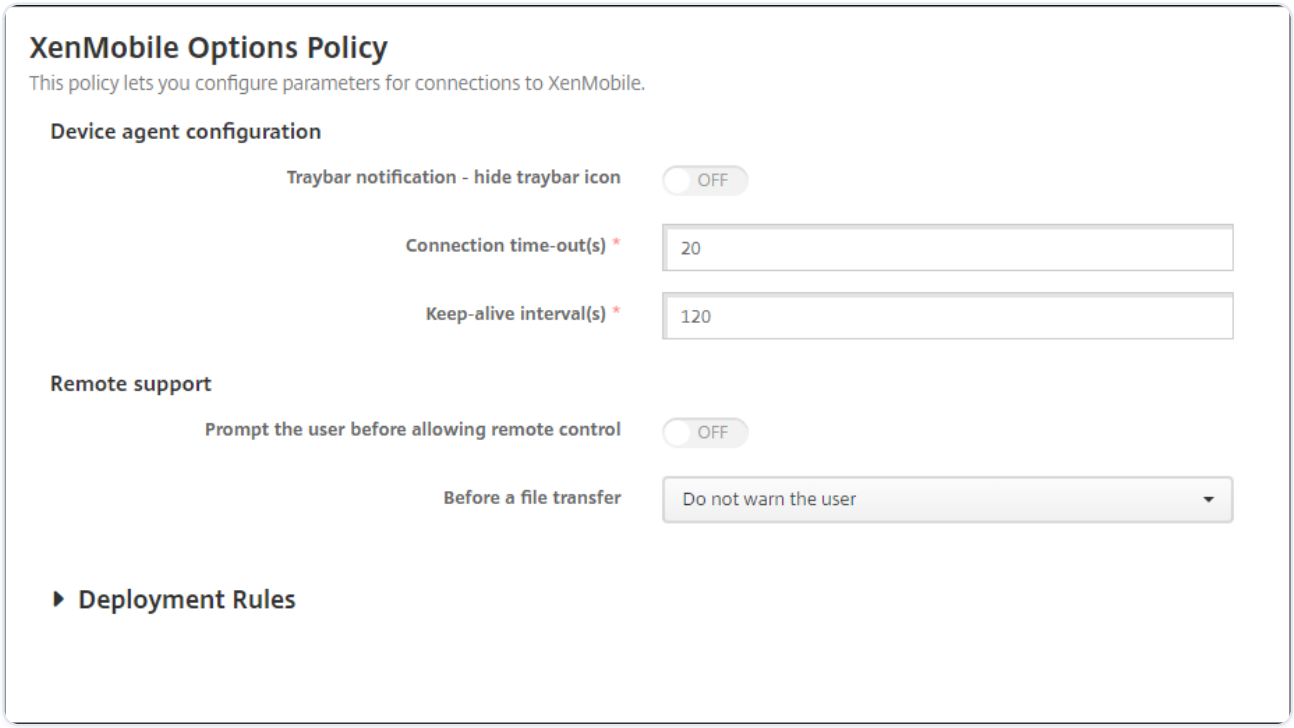


XenMobile® 옵션 장치 정책

Android 장치에서 XenMobile에 연결할 때 Secure Hub 동작을 구성하려면 XenMobile 옵션 정책을 추가합니다.

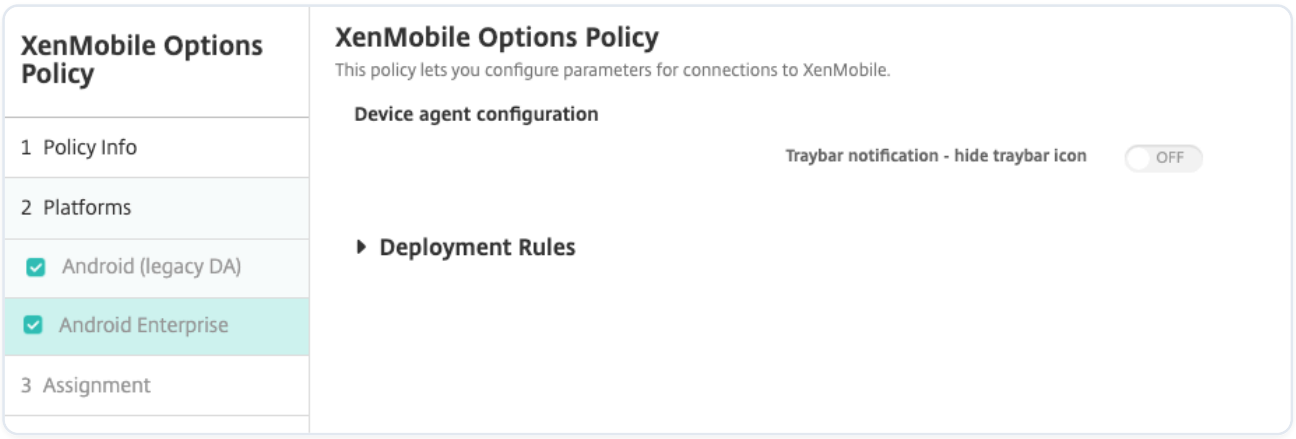
이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

Android 설정



- **트레이바 알림 - 트레이바 아이콘 숨기기:** 트레이바 아이콘을 숨길지 표시할지 선택합니다. 기본값은 **끄기**입니다.
- **연결: 시간 초과(초):** 연결이 시간 초과되기 전에 연결이 유휴 상태로 있을 수 있는 시간(초)을 입력합니다. 기본값은 20초입니다.
- **유지 간격(초):** 연결을 열어둘 시간(초)을 입력합니다. 기본값은 120초입니다.

안드로이드 엔터프라이즈 설정



Android 버전 7부터 지원됩니다.

트레이바 알림 - 트레이바 아이콘 숨기기: 트레이바 아이콘을 숨길지 표시할지 선택합니다. 기본값은 **끄기**입니다.

> **참고:**
>
> Android Enterprise에서 실행되는 장치에 대해 VPN 서비스를 활성화하려면 **VPN 장치 정책**에서 **항상 켜져 있는 VPN 활성화** 옵션을 활성화할 수 있습니다. 이전 릴리스에서 **XenMobile 옵션 장치 정책**에서 **항상 켜져 있는 VPN 활성화** 옵션을 이미 활성화한 경우, **VPN 장치 정책**에서 동일한 옵션을 다시 활성화해야 합니다. VPN 장치 정책에 대한 자세한 내용은 VPN 장치 정책 - Android Enterprise 설정을 참조하십시오.

XenMobile® 장치 제거 정책

XenMobile에서 Android 장치에서 XenMobile을 제거하는 장치 정책을 추가할 수 있습니다. 이 정책이 배포되면 배포 그룹의 모든 장치에서 XenMobile을 제거합니다.

이 정책을 추가하거나 구성하려면 **구성 > 장치 정책**으로 이동합니다. 자세한 내용은 장치 정책을 참조하십시오.

Android 설정 구성

- **장치에서 XenMobile 제거:** 이 정책을 배포하는 모든 장치에서 XenMobile을 제거할지 여부를 선택합니다. 기본값은 **해제**입니다.

앱 추가

XenMobile®에 앱을 추가하면 모바일 애플리케이션 관리(MAM) 기능을 사용할 수 있습니다. XenMobile은 애플리케이션 배포, 소프트웨어 라이선싱, 구성 및 애플리케이션 수명 주기 관리를 지원합니다.

MDX 지원 앱은 대부분의 앱 유형을 사용자 장치에 배포할 준비를 하는 데 중요한 부분입니다. MDX에 대한 소개는 MDX Toolkit 정보 및 MAM SDK 개요를 참조하십시오.

- Citrix는 MAM SDK를 사용하여 앱에 MDX를 지원하도록 권장합니다. 또는 MDX Toolkit이 더 이상 사용되지 않을 때까지 앱을 MDX 래핑할 수 있습니다. 사용 중단을 참조하십시오.
- MDX Toolkit을 사용하여 Citrix® 모바일 생산성 앱을 래핑할 수 없습니다. Citrix 다운로드에서 모바일 생산성 앱 MDX 파일을 가져오십시오.

XenMobile 콘솔에 앱을 추가할 때 다음을 수행합니다.

- 앱 설정 구성
- 선택적으로 Secure Hub에서 앱을 구성하기 위해 범주로 정렬
- 선택적으로 사용자가 앱에 액세스하기 전에 승인을 요구하는 워크플로 정의
- 사용자에게 앱 배포

이 문서에서는 앱 추가를 위한 일반적인 워크플로를 다룹니다. 플랫폼별 내용은 다음 문서를 참조하십시오.

- Android Enterprise 앱 배포
- Apple 앱 배포

앱 유형 및 기능

다음 표는 XenMobile로 배포할 수 있는 앱 유형을 요약한 것입니다.

앱 유형	출처	참고	참조
MDX	사용자를 위해 개발하는 iOS 및 Android 앱. Citrix 모바일 생산성 앱.	MAM SDK를 사용하여 iOS 또는 Android 앱을 개발하거나 MDX Toolkit으로 래핑합니다. 모바일 생산성 앱의 경우 Citrix 다운로드에	MDX 앱 추가

앱 유형	출처	참고	참조
		서 공개 스토어 MDX 파일을 다운로드합니다. 그런 다음 XenMobile에 앱을 추가합니다.	
공개 앱 스토어	Google Play 또는 Apple App Store와 같은 공개 앱 스토어의 무료 또는 유료 앱.	앱을 업로드하고, 앱을 MDX 지원 가능하게 설정한 다음, XenMobile에 앱을 추가합니다.	공개 앱 스토어 앱 추가
웹 및 SaaS	내부 네트워크(웹 앱) 또는 공용 네트워크(SaaS).	Citrix Workspace™는 MDM에 등록된 iOS 및 Android 장치에서 기본 SaaS 앱에 대한 모바일 단일 Sign-On을 제공합니다. 또는 SAML(Security Assertion Markup Language) 애플리케이션 커넥터를 사용합니다.	웹 또는 SaaS 앱 추가(#add-a-web-or-saas-app)
엔터프라이즈	MDX가 사용 설정되지 않은 Win 32 앱을 포함한 개인 앱. MDX가 사용 설정된 개인 Android Enterprise 앱. 엔터프라이즈 앱은 콘텐츠 전송 네트워크 위치 또는 XenMobile 서버에 상주합니다.	XenMobile에 앱을 추가합니다.	엔터프라이즈 앱 추가(#add-an-enterprise-app)
웹 링크	단일 Sign-On이 필요 없는 인터넷 웹 주소, 인트라넷 웹 주소 또는 웹 앱.	XenMobile에서 웹 링크를 구성합니다.	웹 링크 추가(#add-a-web-link)

앱 배포를 계획할 때 다음 기능을 고려하십시오.

- 자동 설치 정보(#about-silent-installations)

- 필수 및 선택적 앱 정보(#about-required-and-optional-apps)
- 앱 범주 정보(#about-app-categories)
- Microsoft 365 앱 사용(#enable-microsoft-365-apps)
- 워크플로 적용(#apply-workflows)
- 앱 스토어 및 Citrix Secure Hub™ 브랜딩

자동 설치 정보

Citrix는 iOS, Android Enterprise 및 Samsung 앱의 자동 설치 및 업그레이드를 지원합니다. 자동 설치는 사용자에게 장치에 배포하는 앱을 설치하라는 메시지가 표시되지 않음을 의미합니다. 앱은 백그라운드에서 자동으로 설치됩니다.

자동 설치를 구현하기 위한 전제 조건:

- iOS의 경우 관리되는 iOS 장치를 감독 모드로 설정합니다. 자세한 내용은 iOS 및 macOS 프로필 장치 정책 가져오기를 참조하십시오.
- Android Enterprise의 경우 앱은 장치의 Android 작업 프로필에 설치됩니다. 자세한 내용은 Android Enterprise를 참조하십시오.
- Samsung 장치의 경우 장치에서 Samsung Knox를 활성화합니다.

  이렇게 하려면 Samsung MDM 라이선스 키 장치 정책을 설정하여 Samsung ELM 및 Knox 라이선스 키를 생성합니다. 자세한 내용은 Samsung MDM 라이선스 키 장치 정책을 참조하십시오.

필수 앱 및 선택적 앱 정보

전달 그룹에 앱을 추가할 때 앱이 선택 사항인지 필수 사항인지 선택합니다. Citrix는 앱을 **필수**로 배포하는 것을 권장합니다.

- 필수 앱은 사용자 장치에 자동으로 설치되어 상호 작용을 최소화합니다. 이 기능을 활성화하면 앱이 자동으로 업데이트될 수도 있습니다.
- 선택적 앱을 사용하면 사용자가 설치할 앱을 선택할 수 있지만, 사용자는 Secure Hub를 통해 수동으로 설치를 시작해야 합니다.

필수로 표시된 앱의 경우 사용자는 다음과 같은 상황에서 업데이트를 즉시 받을 수 있습니다.

- 새 앱을 업로드하고 필수로 표시합니다.
- 기존 앱을 필수로 표시합니다.
- 사용자가 필수 앱을 삭제합니다.

- Secure Hub 업데이트를 사용할 수 있습니다.

필수 앱 강제 배포 요구 사항

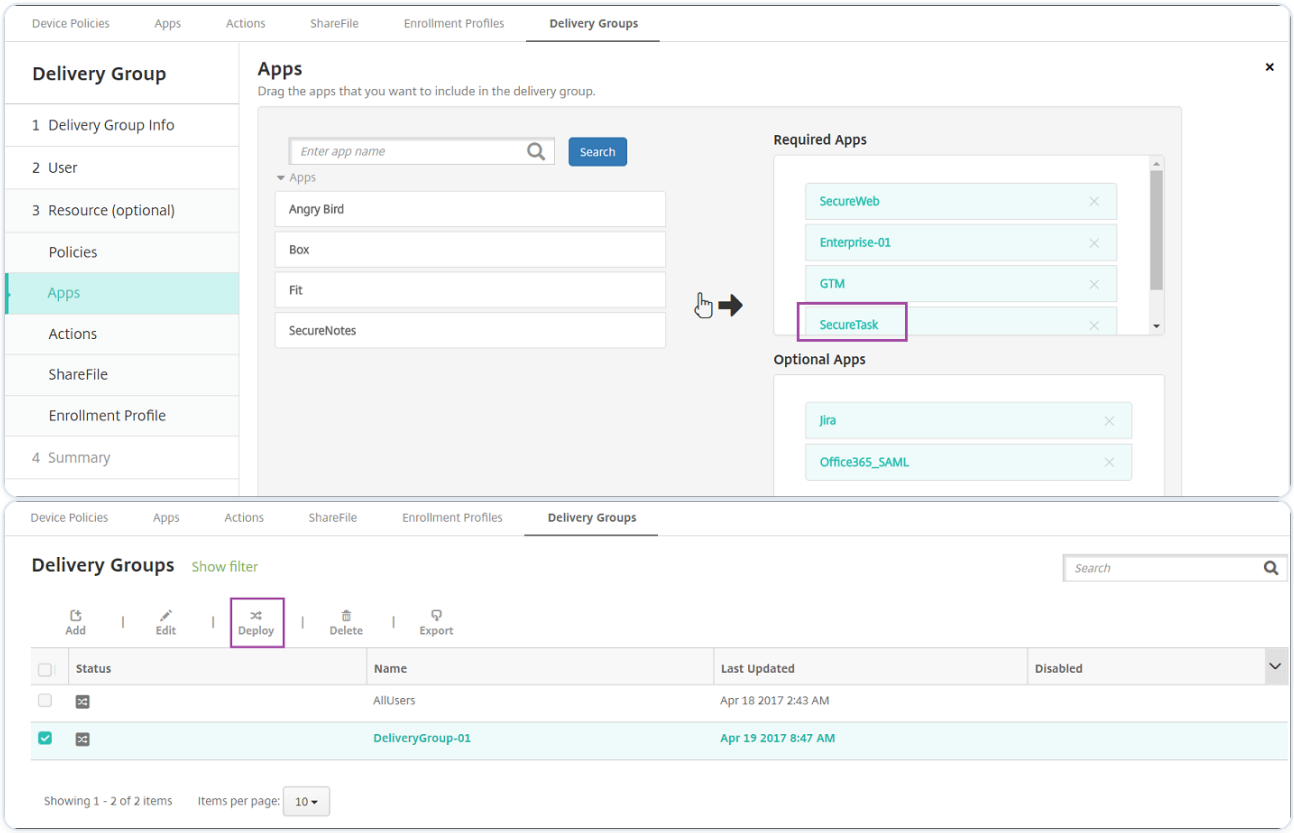
- XenMobile Server 10.6 (최소 버전)
- iOS용 Secure Hub 10.5.15 및 Android용 10.5.20 (최소 버전)
- MAM SDK 또는 MDX Toolkit 10.6 (최소 버전)
- 사용자 지정 서버 속성, force.server.push.required.apps

  필수 앱의 강제 배포는 기본적으로 비활성화되어 있습니다. 이 기능을 활성화하려면 사용자 지정 키 서버 속성을 생성하십시오. **키**와 **표시 이름**을 **force.server.push.required.apps**로 설정하고 **값**을 **true**로 설정하십시오.

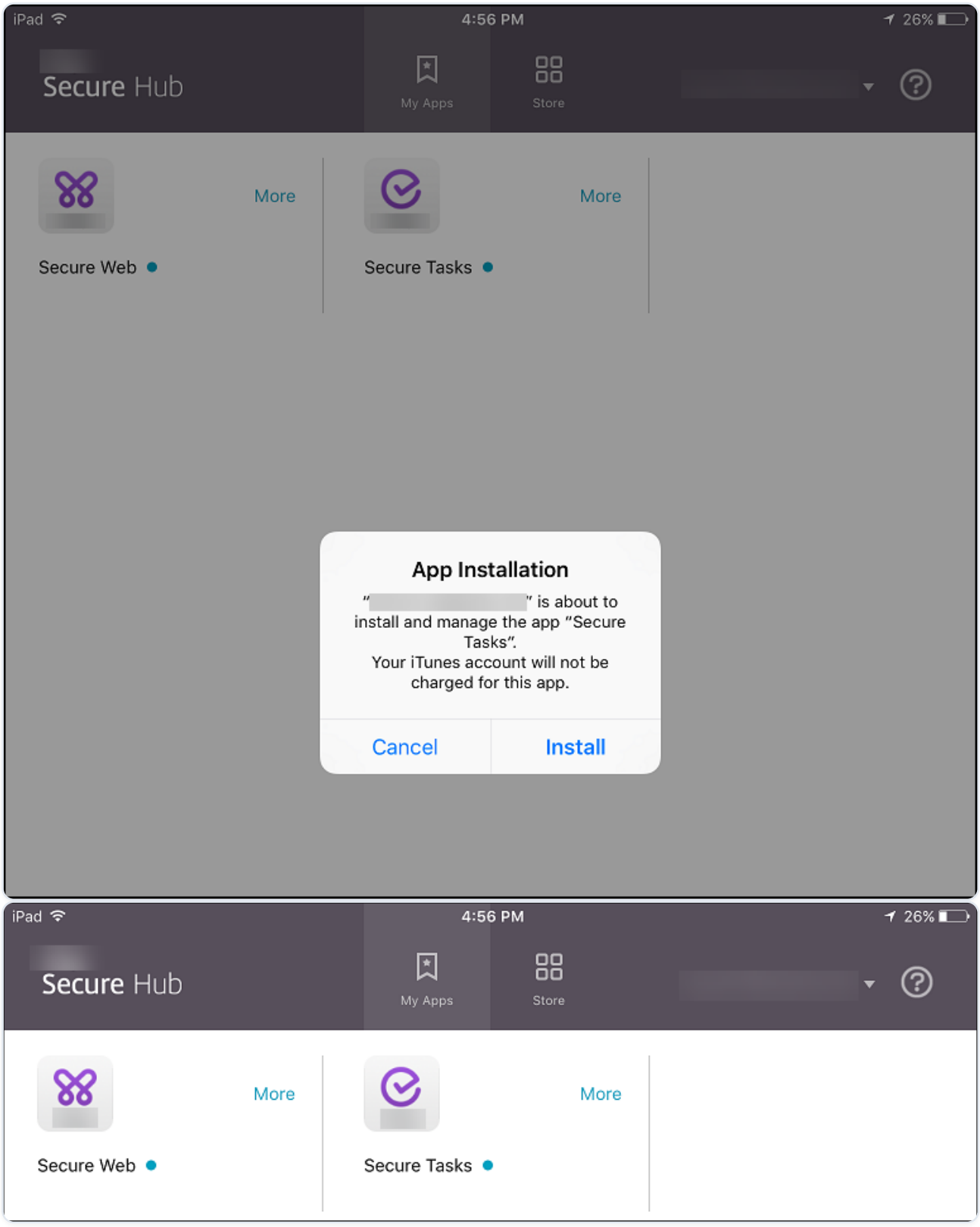
- XenMobile Server 및 Secure Hub를 업그레이드한 후: 등록된 장치를 사용하는 사용자는 필수 앱 배포 업데이트를 받으려면 Secure Hub에서 한 번 로그오프한 다음 다시 로그인해야 합니다.

예시

다음 예시는 Citrix Secure Tasks라는 앱을 배달 그룹에 추가한 다음 배달 그룹을 배포하는 순서를 보여줍니다.



샘플 앱인 Citrix Secure Tasks가 사용자 장치에 배포되면 Secure Hub는 사용자에게 앱 설치를 요청합니다.


iPad
4:56 PM
26%
Secure Hub
My Apps
Store
More
Secure Web
More
Secure Tasks
App Installation
" is about to install and manage the app "Secure Tasks".
Your iTunes account will not be charged for this app.
Cancel
Install
iPad
4:56 PM
26%
Secure Hub
My Apps
Store
More
Secure Web
More
Secure Tasks

중요:

> 엔터프라이즈 앱 및 공개 앱 스토어 앱을 포함한 MDX 지원 필수 앱은 즉시 업그레이드됩니다. 앱 업데이트 유예 기간에 대한 MDX 정책을 구성하고 사용자가 나중에 앱을 업그레이드하도록 선택하더라도 업그레이드가 수행됩니다.

엔터프라이즈 및 공개 스토어 앱용 iOS 필수 앱 워크플로

1. 초기 등록 중에 XenMobile 앱을 배포합니다. 필수 앱이 장치에 설치됩니다.
2. XenMobile 콘솔에서 앱을 업데이트합니다.
3. XenMobile 콘솔을 사용하여 필수 앱을 배포합니다.
4. 홈 화면의 앱이 업데이트됩니다. 그리고 공개 스토어 앱의 경우 업그레이드가 자동으로 시작됩니다. 사용자에게 업데이트하라는 메시지가 표시되지 않습니다.
5. 사용자가 홈 화면에서 앱을 엽니다. 앱 업데이트 유예 기간을 설정하고 사용자가 나중에 앱을 업그레이드하도록 탭하더라도 앱은 즉시 업그레이드됩니다.

엔터프라이즈 앱용 Android 필수 앱 워크플로

1. 초기 등록 중에 XenMobile 앱을 배포합니다. 필수 앱이 장치에 설치됩니다.
2. XenMobile 콘솔을 사용하여 필수 앱을 배포합니다.
3. 앱이 업그레이드됩니다. (Nexus 장치는 업데이트 설치를 요청하지만, Samsung 장치는 자동 설치를 수행합니다.)
4. 사용자가 홈 화면에서 앱을 엽니다. 앱 업데이트 유예 기간을 설정하고 사용자가 나중에 앱을 업그레이드하도록 탭하더라도 앱은 즉시 업그레이드됩니다. (Samsung 장치는 자동 설치를 수행합니다.)

공개 스토어 앱용 Android 필수 앱 워크플로

1. 초기 등록 중에 XenMobile 앱을 배포합니다. 필수 앱이 장치에 설치됩니다.
2. XenMobile 콘솔에서 앱을 업데이트합니다.
3. XenMobile 콘솔을 사용하여 필수 앱을 배포합니다. 또는 장치에서 Secure Hub Store를 엽니다. 업데이트 아이콘이 스토어에 나타납니다.
4. 앱 업그레이드가 자동으로 시작됩니다. (Nexus 장치는 사용자에게 업데이트 설치를 요청합니다.)
5. 홈 화면에서 앱을 엽니다. 앱이 업그레이드됩니다. 사용자에게 유예 기간이 요청되지 않습니다. (Samsung 장치는 자동 설치를 수행합니다.)

앱이 필수로 구성된 경우 앱 제거

필수로 구성된 앱을 사용자가 제거하도록 허용할 수 있습니다. **구성 > 배달 그룹**으로 이동하여 앱을 **필수 앱**에서 **선택적 앱**으로 이동합니다.

권장: 특정 사용자가 앱을 제거할 수 있도록 앱을 일시적으로 선택 사항으로 변경하려면 특별 배달 그룹을 사용하십시오. 그런 다음 기존 필수 앱을 선택 사항으로 변경하고 해당 배달 그룹에 앱을 배포한 다음 해당 장치에서 앱을 제거할 수 있습니다. 그 후 해당 배달 그룹에 대한 향후 등록에 앱이 필요하도록 하려면 앱을 다시 필수로 설정할 수 있습니다.

앱 구성 (Android Enterprise)

사용자가 Secure Hub에 로그인하면 XenMobile Server에서 설정한 앱, 웹 링크 및 스토어 목록을 받게 됩니다. Android Enterprise에서는 이러한 앱을 컬렉션으로 구성하여 사용자가 특정 앱, 스토어 또는 웹 링크에만 액세스하도록 할 수 있습니다. 예를 들어, 재무 컬렉션을 생성한 다음 재무와 관련된 앱만 해당 컬렉션에 추가할 수 있습니다. 또는 영업 앱을 할당할 영업 컬렉션을 구성할 수 있습니다.

1. XenMobile Server 콘솔에서 **구성 > 앱 > 앱 구성**을 클릭합니다. **관리형 Google Play 스토어** 창이 나타납니다.

   앱 구성(/en-us/xenmobile/server/media/configure-apps-organize.png)
2. 컬렉션을 **생성**하고 해당 컬렉션에 추가할 앱을 선택합니다.
3. 컬렉션 추가를 마쳤으면 **저장**을 클릭합니다.

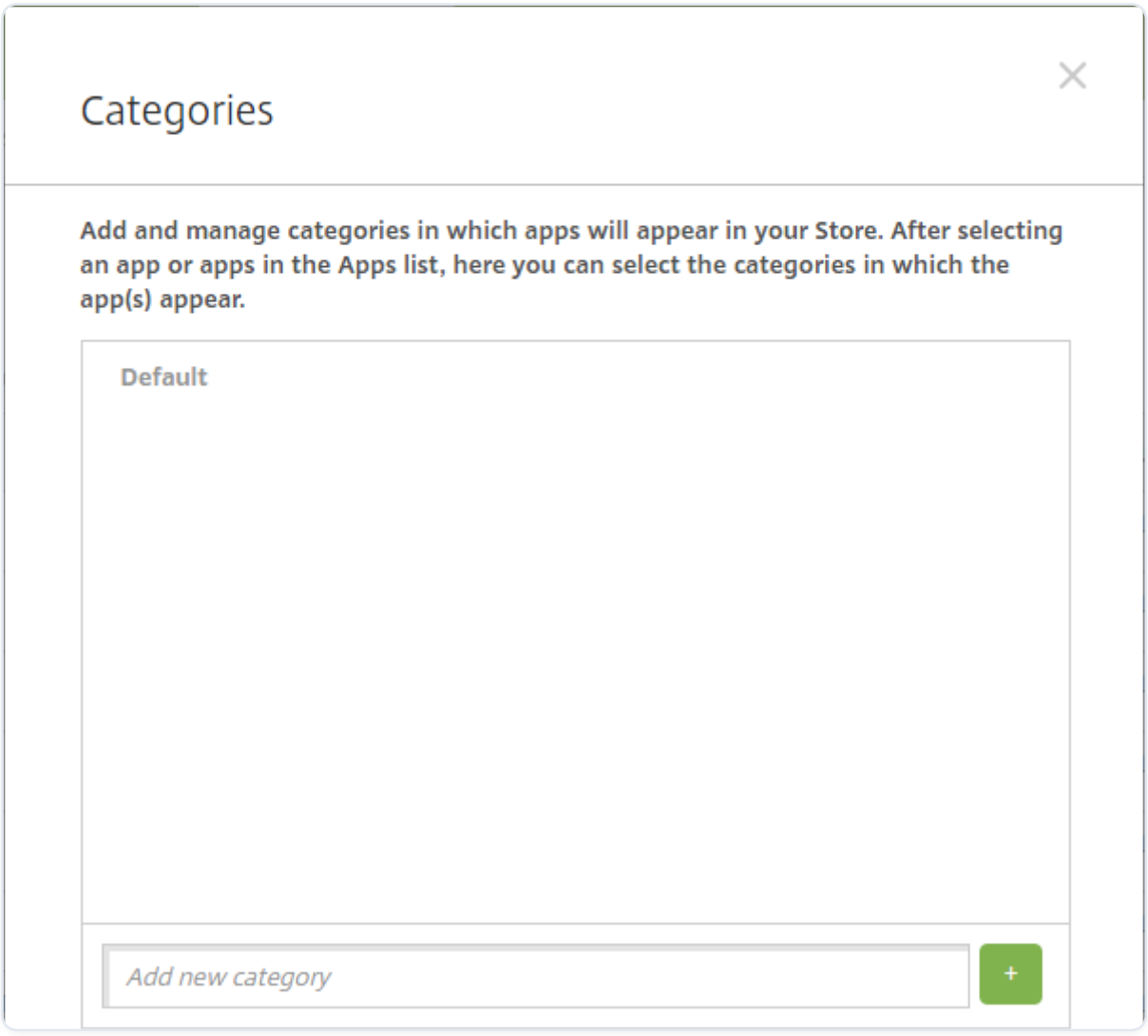
> **참고:**
>
> IT 관리자는 관리형 Google Play 창의 컬렉션에 앱을 추가하기 전에 앱을 승인해야 합니다. IT 관리자는 `<https://play.google.com/work>`으로 이동하여 앱을 승인할 수 있습니다. 향후 릴리스에서는 컬렉션에 앱을 추가하기 전에 앱을 승인할 필요가 없습니다.

앱 카테고리에 대하여

사용자가 Secure Hub에 로그인하면 XenMobile에서 설정한 앱, 웹 링크 및 스토어 목록을 받게 됩니다. 앱 카테고리를 사용하여 사용자가 특정 앱, 스토어 또는 웹 링크에만 액세스하도록 허용할 수 있습니다. 예를 들어, 재무 카테고리를 생성한 다음 재무와 관련된 앱만 해당 카테고리에 추가할 수 있습니다. 또는 영업 앱을 할당할 영업 카테고리를 구성할 수 있습니다.

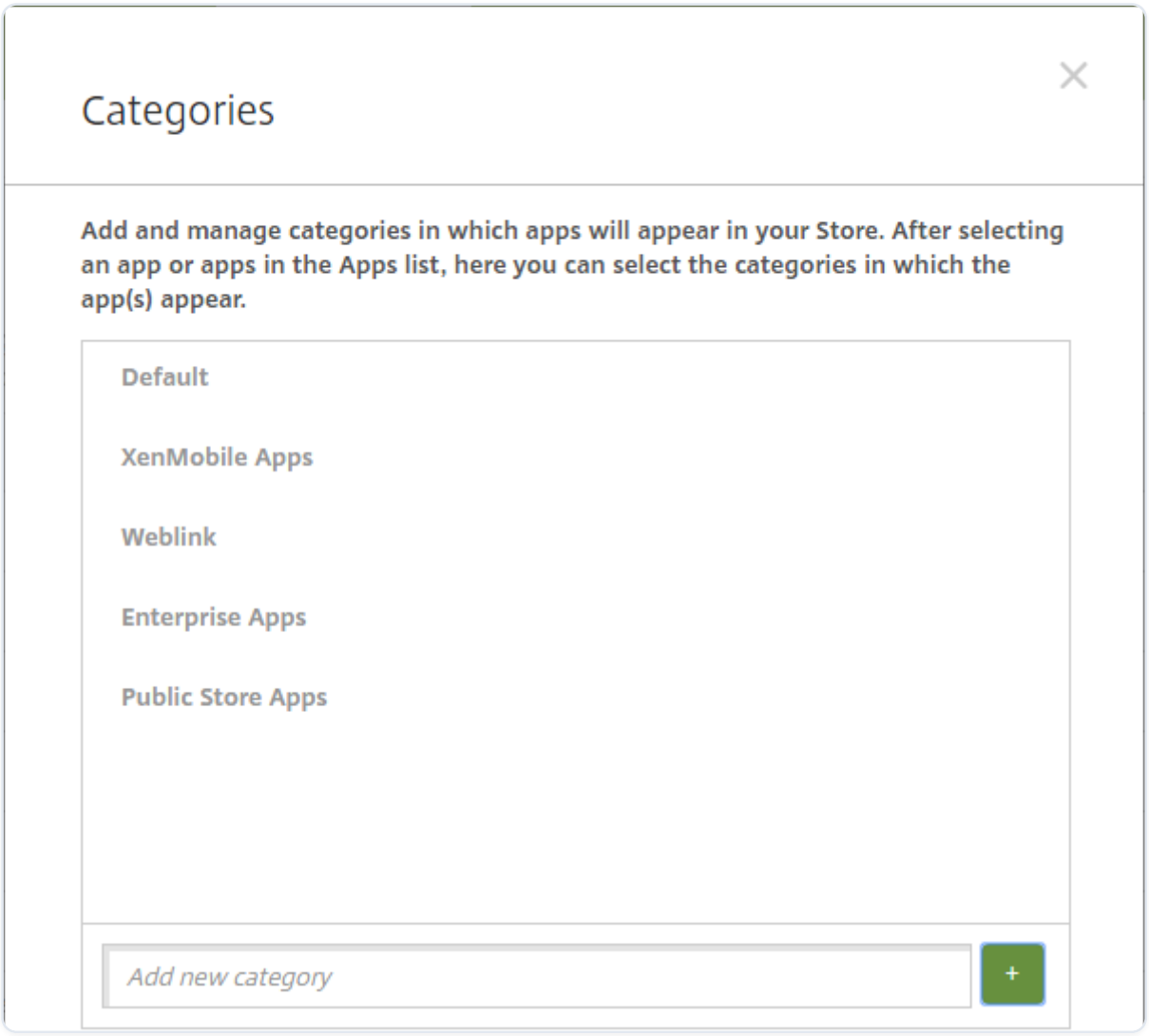
앱, 웹 링크 또는 스토어를 추가하거나 편집할 때 구성된 카테고리 중 하나 이상에 앱을 추가할 수 있습니다.

1. XenMobile 콘솔에서 **구성 > 앱 > 카테고리**를 클릭합니다. **카테고리** 대화 상자가 나타납니다.



2. 추가하려는 각 카테고리에 대해 다음을 수행합니다.

- 대화 상자 하단의 **새 카테고리 추가** 필드에 추가하려는 카테고리 이름을 입력합니다. 예를 들어, 엔터프라이즈 앱용 카테고리를 생성하기 위해 Enterprise Apps를 입력할 수 있습니다.
- 더하기 기호(+)를 클릭하여 카테고리를 추가합니다. 새로 생성된 카테고리가 추가되고 **카테고리** 대화 상자에 나타납니다.



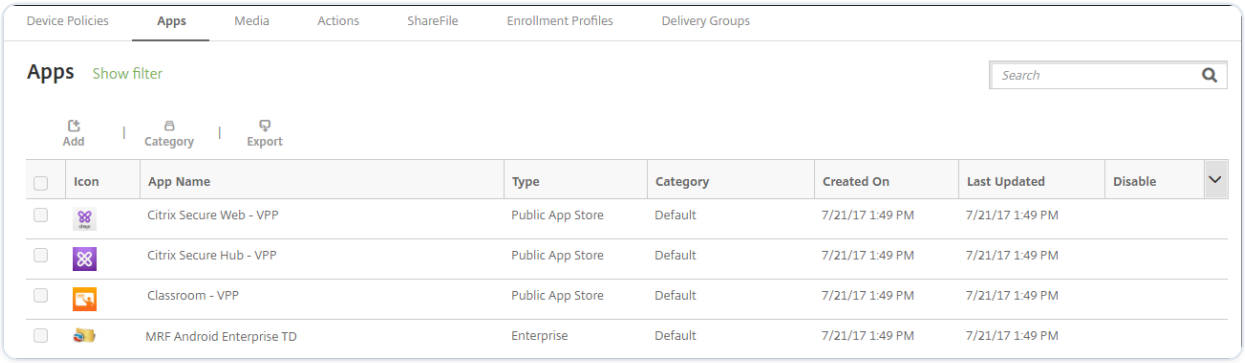
3. 카테고리 추가를 마쳤으면 **카테고리** 대화 상자를 닫습니다.
4. **앱** 페이지에서 기존 앱을 새 카테고리에 배치할 수 있습니다.
    - 카테고리화하려는 앱을 선택합니다.
    - **편집**을 클릭합니다. **앱 정보** 페이지가 나타납니다.
    - **앱 카테고리** 목록에서 해당 카테고리 확인란을 선택하여 새 카테고리를 적용합니다. 앱에 적용하지 않으려는 기존 카테고리의 확인란은 선택을 취소합니다.
    - **Delivery Groups Assignments** 탭을 클릭하거나 다음 각 페이지에서 **다음**을 클릭하여 나머지 앱 설정 페이지를 진행합니다.
    - **Delivery Groups Assignments** 페이지에서 **저장**을 클릭하여 새 범주를 적용합니다. 새 범주는 앱에 적용되며 **앱** 테이블에 나타납니다.

MDX 앱 추가

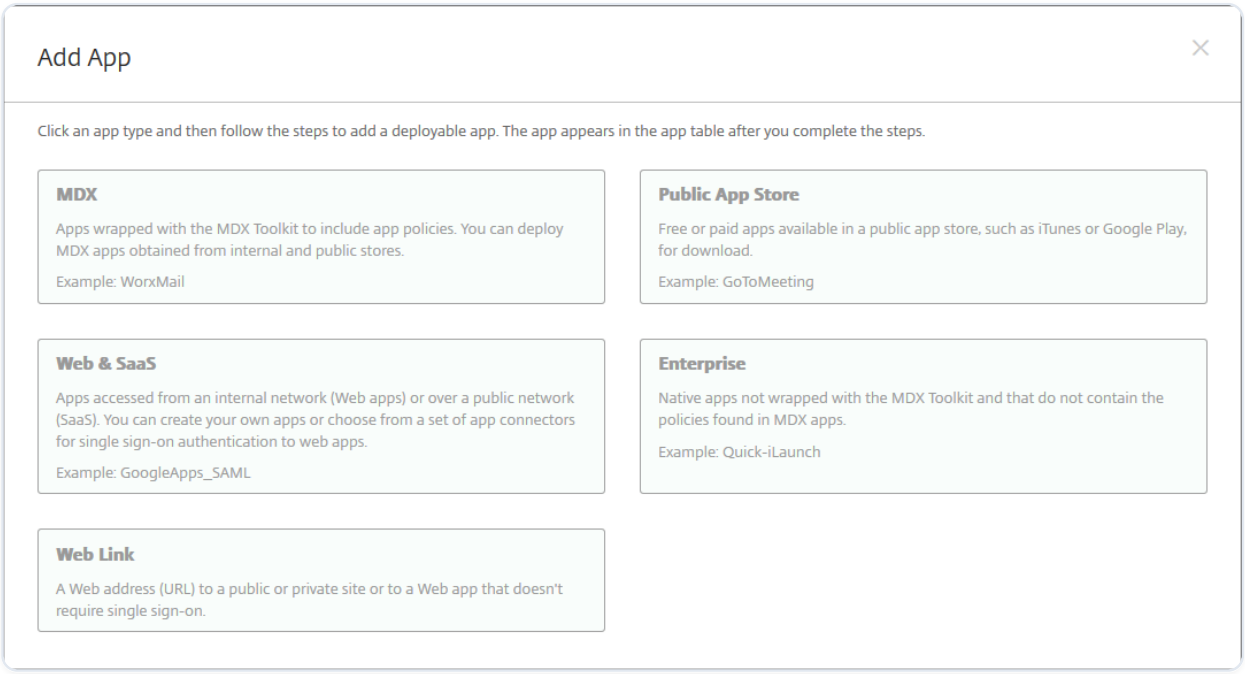
iOS 또는 Android 앱용 MDX 파일을 받으면 XenMobile에 앱을 업로드할 수 있습니다. 앱을 업로드한 후 앱 세부 정보 및 정책 설정을 구성할 수 있습니다. 각 장치 플랫폼 유형에 사용할 수 있는 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

- MAM SDK 개요
- MDX 정책 한눈에 보기

1. XenMobile 콘솔에서 **구성 > 앱**을 클릭합니다. **앱** 페이지가 나타납니다.



2. **추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.



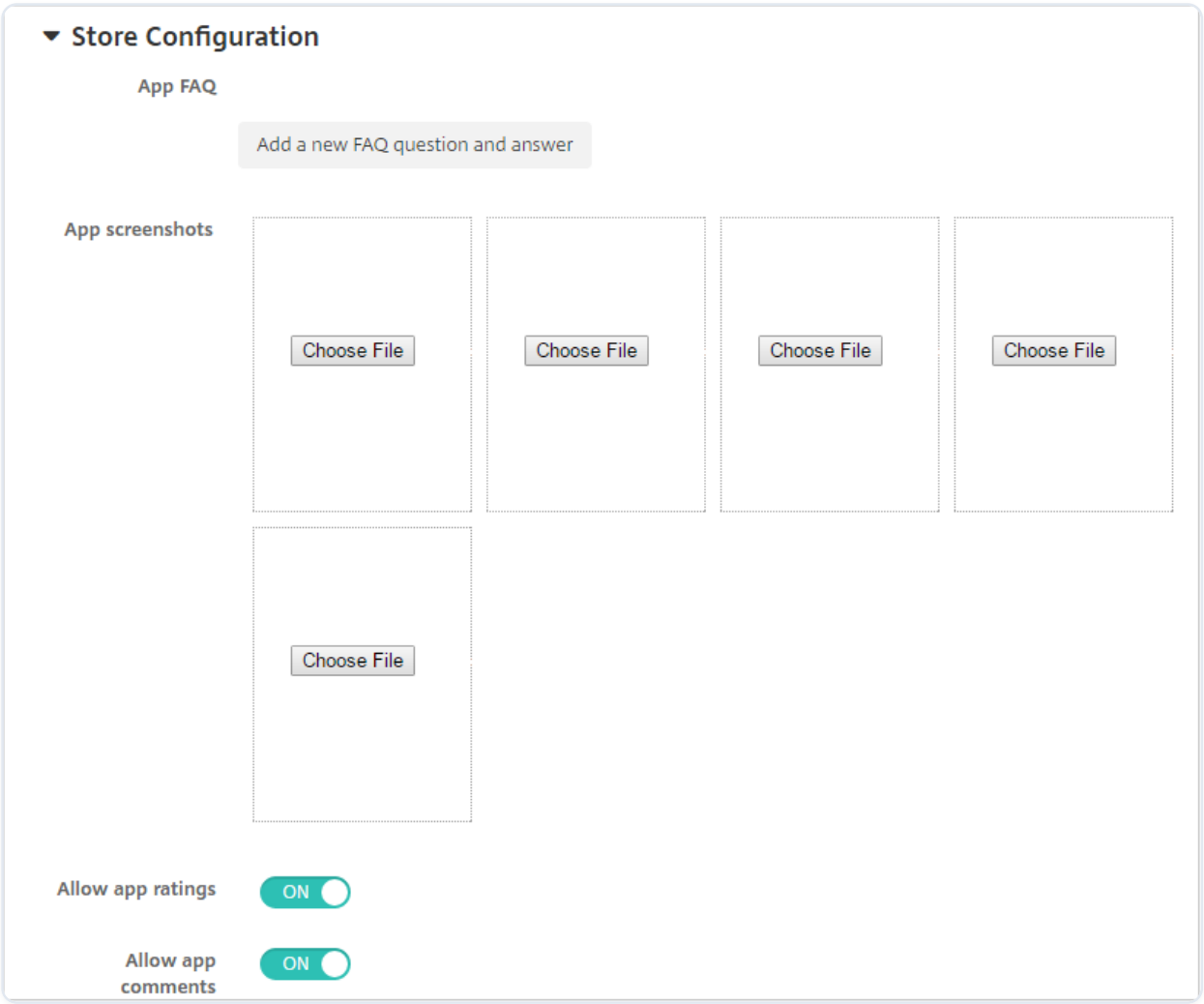
3. **MDX**를 클릭합니다. **MDX 앱 정보** 페이지가 나타납니다.
4. **앱 정보** 창에서 다음 정보를 입력합니다.
   - **이름:** 앱에 대한 설명적인 이름을 입력합니다. 이 이름은 **앱** 테이블의 **앱 이름** 아래에 나타납니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.

- **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

5. **다음**을 클릭합니다. **앱 플랫폼** 페이지가 나타납니다.
6. **플랫폼**에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼만 구성하는 경우 다른 플랫폼은 선택을 취소합니다.
7. 업로드할 MDX 파일을 선택하려면 **업로드**를 클릭하고 파일 위치로 이동합니다.
8. **앱 세부 정보** 페이지에서 다음 설정을 구성합니다.

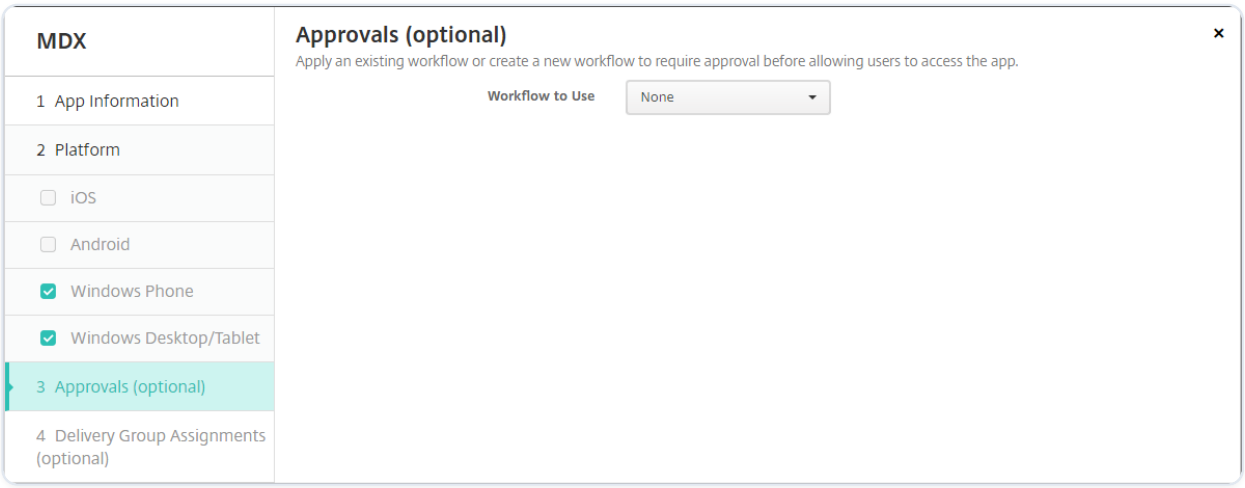
   - **파일 이름:** 앱과 연결된 파일 이름을 입력합니다.
   - **앱 설명:** 앱에 대한 설명을 입력합니다.
   - **앱 버전:** 선택적으로 앱 버전 번호를 입력합니다.
   - **패키지 ID:** 관리형 Google Play 스토어에서 가져온 앱의 패키지 ID를 입력합니다.
   - **최소 OS 버전:** 선택적으로 장치에서 앱을 실행하는 데 필요한 가장 오래된 운영 체제 버전을 입력합니다.
   - **최대 OS 버전:** 선택적으로 장치에서 앱을 실행하는 데 필요한 최신 운영 체제를 입력합니다.
   - **제외된 장치:** 선택적으로 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
   - **MDM 프로필 제거 시 앱 제거:** MDM 프로필이 제거될 때 iOS 장치에서 앱을 제거할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
   - **앱 데이터 백업 방지:** 사용자가 iOS 장치에서 앱 데이터를 백업하지 못하도록 할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
   - **제품 트랙:** iOS 장치로 푸시할 제품 트랙을 지정합니다. 테스트용으로 설계된 트랙이 있는 경우 해당 트랙을 선택하여 사용자에게 할당할 수 있습니다. 기본값은 **프로덕션**입니다.
   - **앱 관리 강제 적용:** 관리되지 않는 상태로 설치되는 앱의 경우, 감독되지 않는 iOS 장치에서 앱을 관리하도록 사용자에게 메시지를 표시할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
   - **볼륨 구매를 통해 배포된 앱:** Apple 볼륨 구매를 사용하여 앱을 배포할지 여부를 선택합니다. **켜짐**으로 설정하고 앱의 MDX 버전을 배포하며 볼륨 구매를 사용하여 앱을 배포하는 경우, Secure Hub에는 볼륨 구매 인스턴스만 표시됩니다. 기본값은 **꺼짐**입니다.

9. **MDX 정책**을 구성합니다. MDX 정책은 플랫폼에 따라 다르며 인증, 장치 보안 및 앱 제한과 같은 정책 영역에 대한 옵션을 포함합니다. 콘솔에서 각 정책에는 정책을 설명하는 도구 설명이 있습니다.
10. 배포 규칙을 구성합니다. 자세한 내용은 배포 규칙을 참조하십시오.
11. **스토어 구성**을 확장합니다.



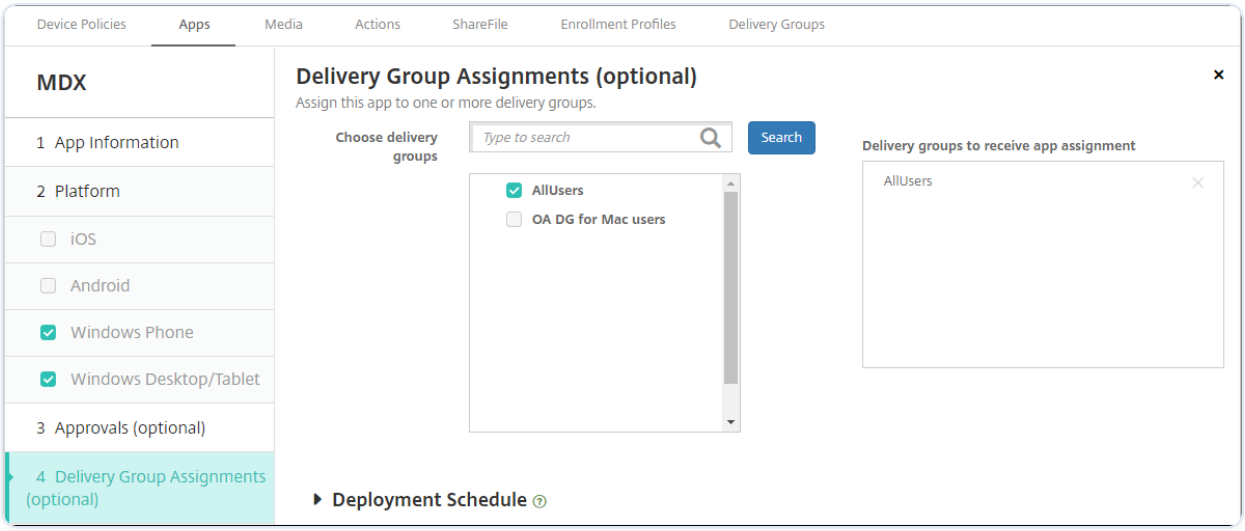
- **앱 FAQ:** 앱에 대한 FAQ를 만들려면 **새 FAQ 질문 및 답변 추가**를 클릭합니다.
- **휴대폰/태블릿용 스크린샷 추가:** 앱 스토어에 표시될 화면 캡처를 추가합니다.
- **앱 평가 허용:** 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- **앱 댓글 허용:** 사용자가 앱 스토어에서 앱에 댓글을 남기도록 허용합니다.

12. **다음**을 클릭합니다. **승인** 페이지가 나타납니다.



워크플로를 사용하여 사용자가 앱에 액세스하기 전에 승인을 요구하려면 워크플로 적용을 참조하십시오. 승인 워크플로를 설정하지 않으려면 다음 단계로 진행하십시오.

13. **다음**을 클릭합니다. **전달 그룹 할당** 페이지가 나타납니다.



14. **전달 그룹 선택** 옆에 전달 그룹을 찾기 위해 입력하거나 목록에서 하나 이상의 그룹을 선택합니다. 선택한 그룹은 **앱 할당을 받을 전달 그룹** 목록에 나타납니다.
15. **배포 일정**을 확장한 다음 다음 설정을 구성합니다.

    - **배포:** 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
    - **배포 일정:** 앱을 **지금** 배포할지 **나중에** 배포할지 선택합니다. **나중에**를 선택하는 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 **지금**입니다.
    - **배포 조건:** 장치가 연결될 때마다 앱을 배포하려면 **모든 연결 시**를 선택합니다. 이전에 장치가 앱을 수신하지 못한 경우 앱을 배포하려면 **이전 배포가 실패한 경우에만**을 선택합니다. 기본값은 **모든 연결 시**입니다.

    항상 연결 배포 옵션은 **설정 > 서버 속성**에서 예약 백그라운드 배포 키를 구성한 경우에 적용됩니다.

    구성하는 배포 일정은 모든 플랫폼에서 동일합니다. **항상 연결 배포**를 제외하고 변경하는 모든 내용은 모든 플랫폼에 적용됩니다.
16. **저장**을 클릭합니다.

공개 앱 스토어 앱 추가

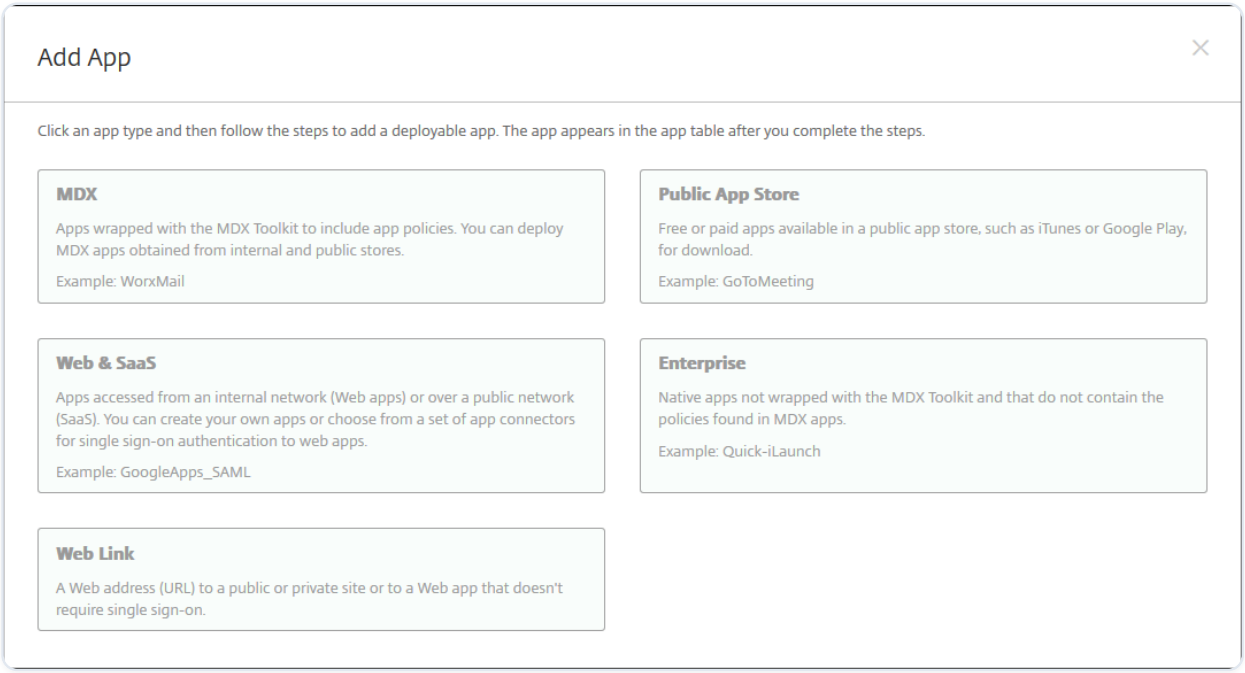
Apple App Store 또는 Google Play와 같은 공개 앱 스토어에서 사용할 수 있는 무료 또는 유료 앱을 XenMobile에 추가할 수 있습니다.

Apple App Store에서 앱 이름 및 설명을 검색하도록 설정을 구성할 수 있습니다. 스토어에서 앱 정보를 검색하면 XenMobile이 기존 이름과 설명을 덮어씁니다. Google Play 스토어 앱 정보를 수동으로 구성합니다.

Android Enterprise용 유료 공개 앱 스토어 앱을 추가할 때 대량 구매 라이선스 상태를 검토할 수 있습니다. 이 상태는 사용 가능한 총 라이선스 수, 현재 사용 중인 수, 라이선스를 사용하는 각 사용자의 이메일 주소입니다. Android Enterprise용 대량 구매 계획은 조직을 위해 앱 및 기타 데이터를 대량으로 찾고, 구매하고, 배포하는 프로세스를 간소화합니다.

앱 정보를 구성하고 앱을 배포할 플랫폼을 선택합니다.

1. XenMobile 콘솔에서 **구성 > 앱 > 추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.



2. **공개 앱 스토어**를 클릭합니다. **앱 정보** 페이지가 나타납니다.
3. **앱 정보** 창에서 다음 정보를 입력합니다.
   - **이름:** 앱에 대한 설명이 포함된 이름을 입력합니다. 이 이름은 **앱** 테이블의 **앱 이름** 아래에 나타납니다.
   - **설명:** 앱에 대한 선택적 설명을 입력합니다.
   - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.
4. **다음**을 클릭합니다. **앱 플랫폼** 페이지가 나타납니다.
5. **플랫폼**에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼에 대해서만 구성하는 경우 다른 플랫폼은 선택 취소합니다.

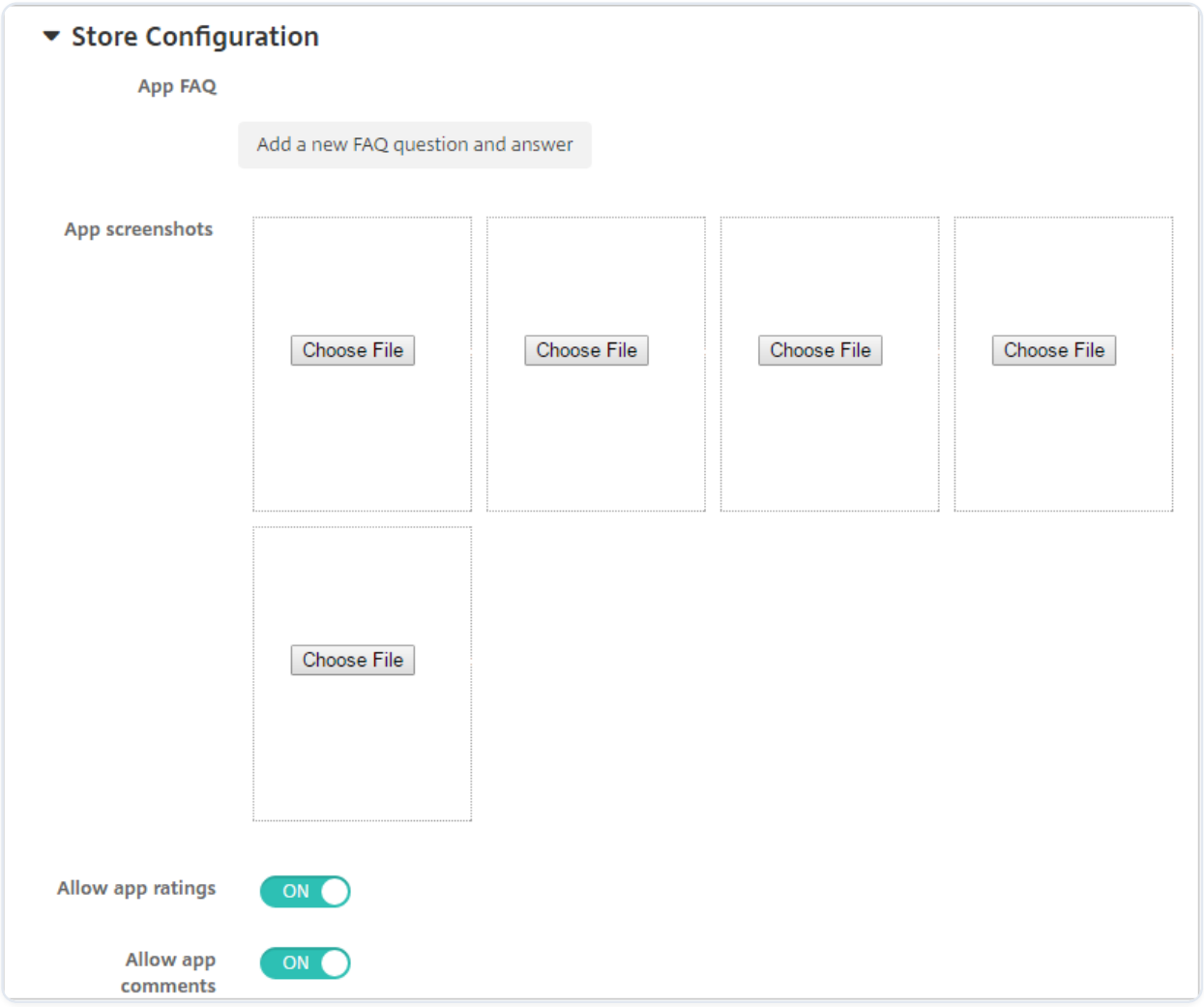
다음으로 각 플랫폼에 대한 앱 설정을 구성합니다. 다음을 참조하십시오.

- Google Play 앱에 대한 앱 설정 구성
- 관리형 앱 스토어 앱

- iOS 앱에 대한 앱 설정 구성

플랫폼에 대한 설정 구성을 완료하면 플랫폼 배포 규칙 및 앱 스토어 구성을 설정합니다.

1. 배포 규칙을 구성합니다. 자세한 내용은 배포 규칙을 참조하십시오.
2. **스토어 구성**을 확장합니다.



- **앱 FAQ: 새 FAQ 질문 및 답변 추가**를 클릭하여 앱에 대한 FAQ를 만듭니다.
- **폰/태블릿용 스크린샷 추가:** 앱 스토어에 표시될 스크린샷을 추가합니다.
- **앱 평가 허용:** 사용자가 앱 스토어에서 앱을 평가할 수 있도록 허용합니다.
- **앱 댓글 허용:** 사용자가 앱 스토어에서 앱에 댓글을 남길 수 있도록 허용합니다.

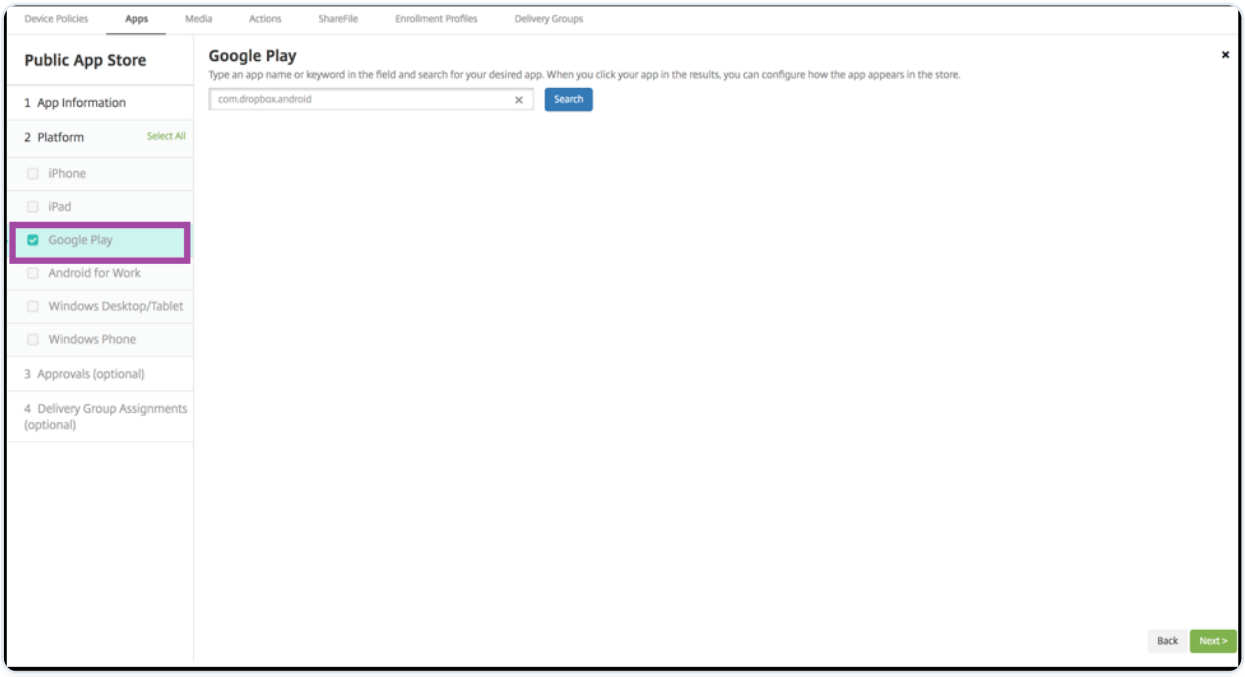
Google Play 앱의 앱 설정 구성

> **참고:**

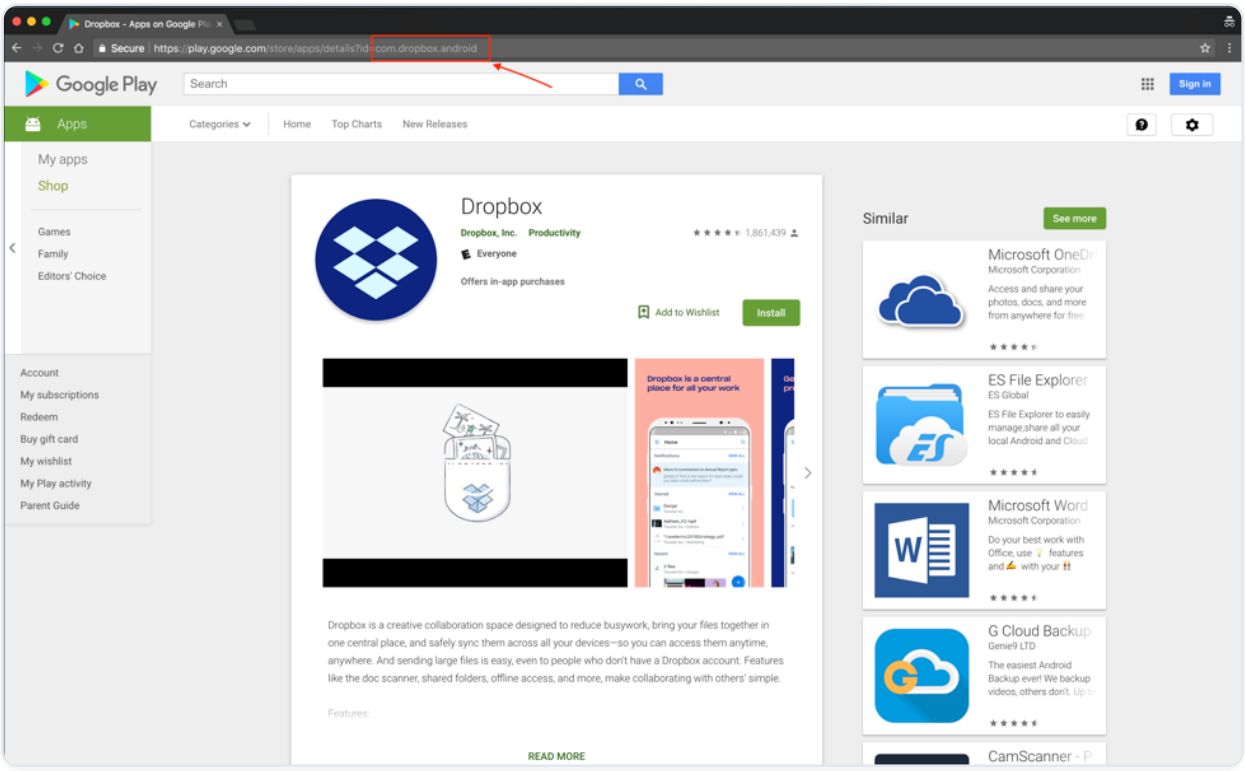
관리형 Google Play에서 Google Play 스토어의 모든 앱에 액세스할 수 있도록 하려면 XenMobile Server 속성 **관리형 Google Play 스토어의 모든 앱에 액세스**를 사용하십시오. 서버 속성을 참조하십시오. 이 속성을 **true**로 설정하면 모든 Android Enterprise 사용자가 공개 Google Play 스토어 앱에 액세스할 수 있습니다. 그런 다음 제한 장치 정책을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다.

Google Play 스토어 앱 설정을 구성하는 것은 다른 플랫폼의 앱과 다른 단계를 필요로 합니다. Google Play 스토어 앱 정보를 수동으로 구성해야 합니다.

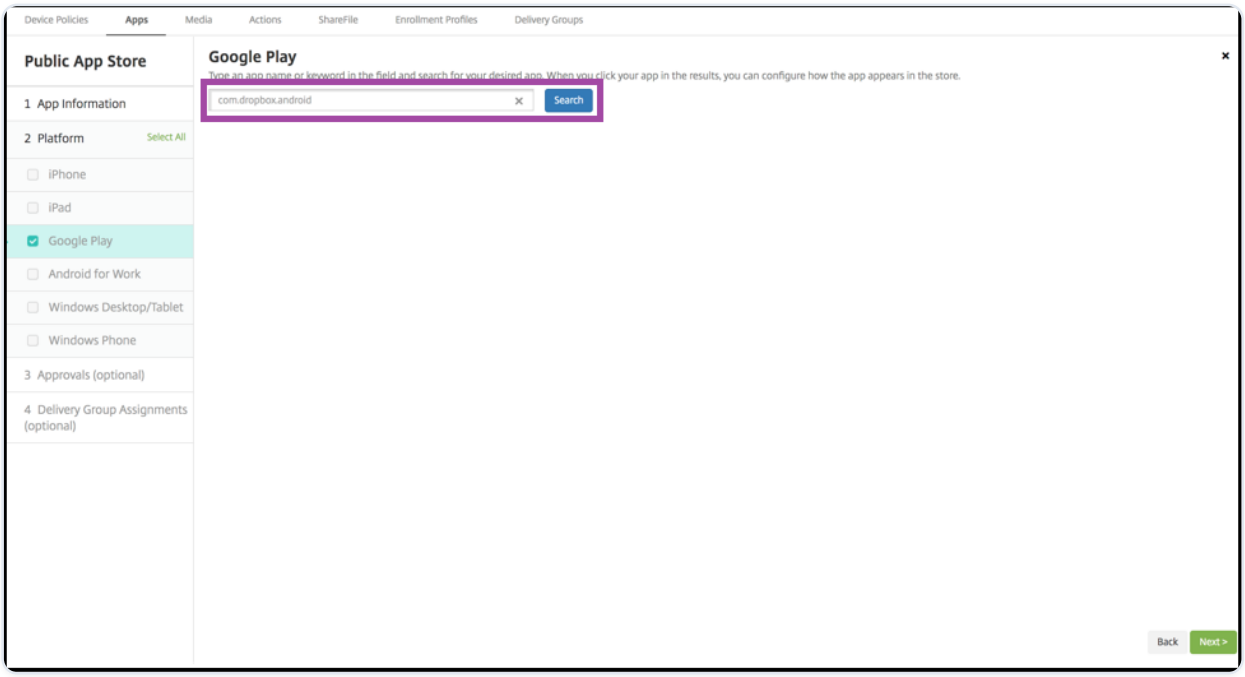
1. **플랫폼** 아래에서 **Google Play**가 선택되어 있는지 확인합니다.



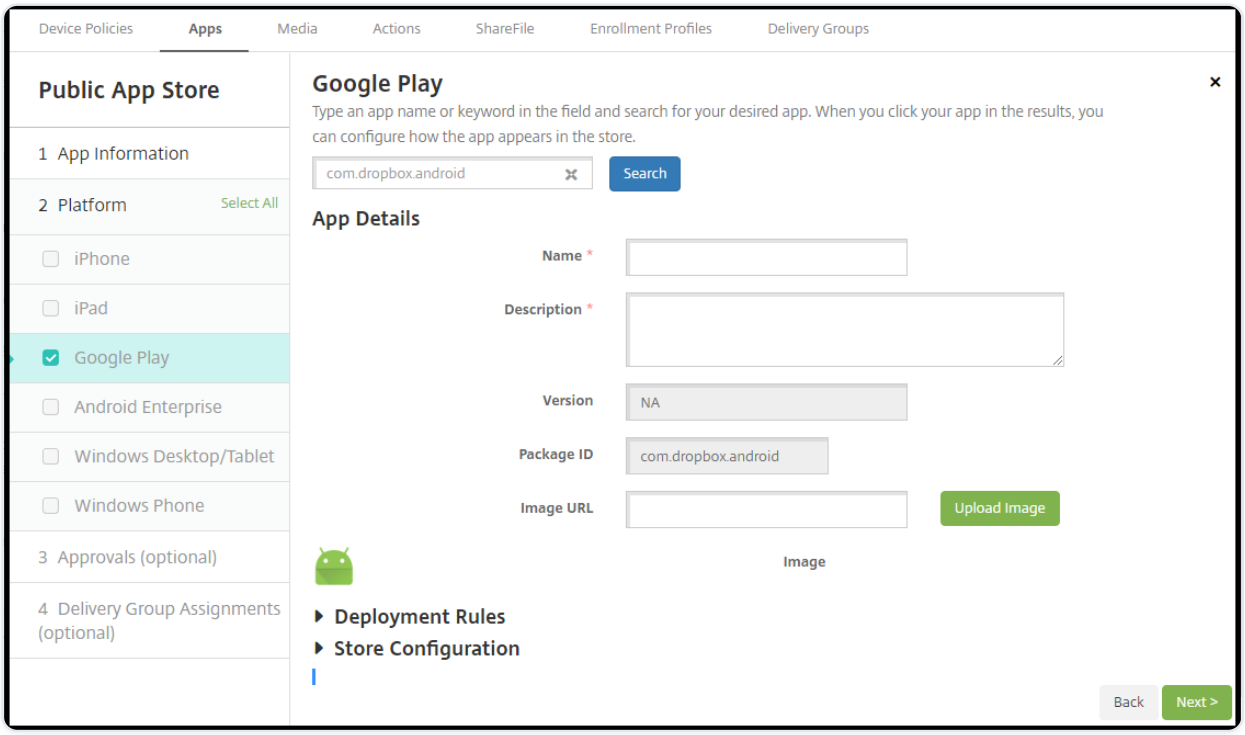
2. Google Play 스토어로 이동합니다. Google Play 스토어에서 패키지 ID를 복사합니다. ID는 앱의 URL에서 찾을 수 있습니다.



3. XenMobile Server 콘솔에서 공개 스토어 앱을 추가할 때 검색 창에 패키지 ID를 붙여넣습니다. **검색**을 클릭합니다.



4. 패키지 ID가 유효하면 앱 세부 정보를 입력할 수 있는 UI가 나타납니다.



5. 스토어에 앱과 함께 표시될 이미지의 URL을 구성할 수 있습니다. Google Play 스토어의 이미지를 사용하려면 다음을 수행합니다.

   a. Google Play 스토어로 이동합니다. 앱 이미지를 마우스 오른쪽 버튼으로 클릭하고 이미지 주소를 복사합니다.

   b. 이미지 주소를 **Image URL** 필드에 붙여넣습니다.

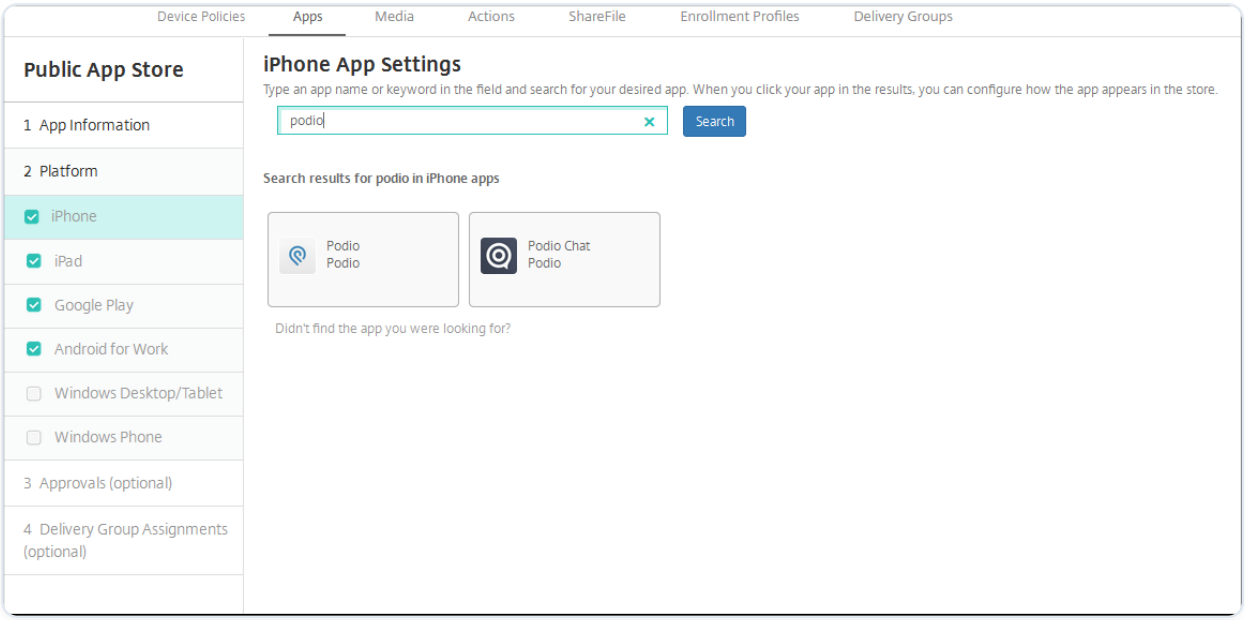
   c. **Upload image**를 클릭합니다. 이미지가 **Image** 옆에 나타납니다.

이미지를 구성하지 않으면 일반 Android 이미지가 앱과 함께 표시됩니다.

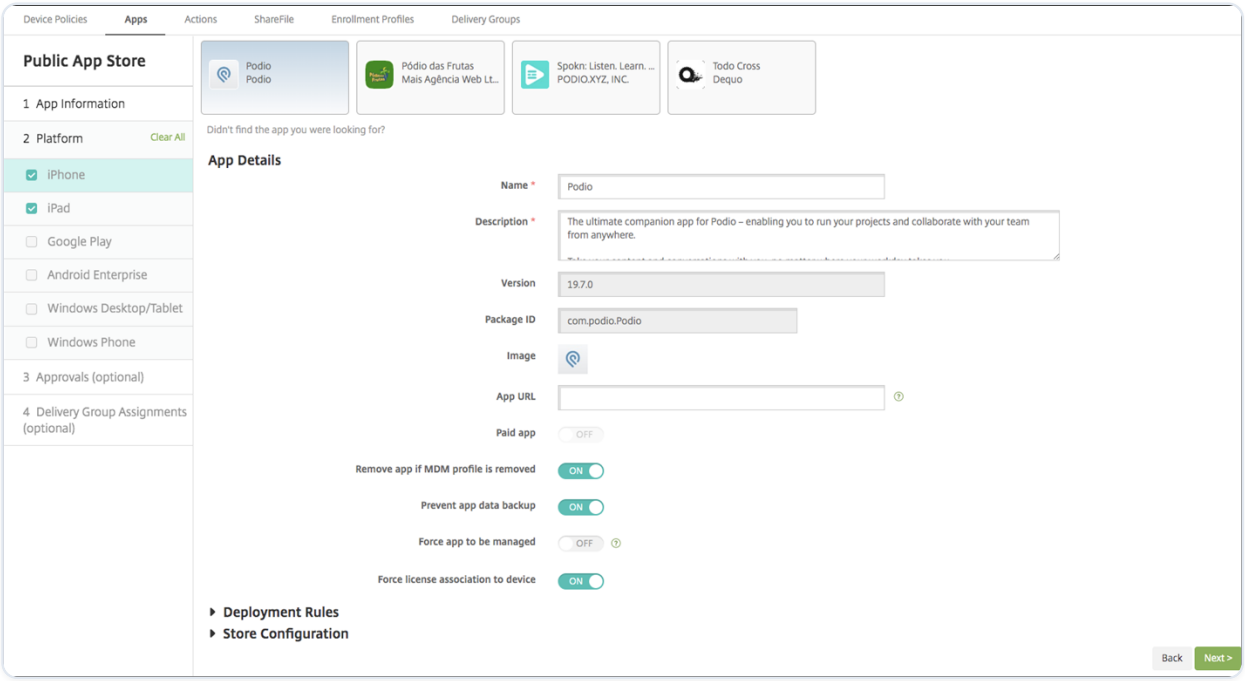
iOS 앱에 대한 앱 설정 구성

1. 검색 상자에 앱 이름을 입력하고 **Search**를 클릭합니다. 검색 조건과 일치하는 앱이 나타납니다.

   다음 그림은 iPhone 앱에서 **podio**를 검색한 결과입니다.



2. 추가하려는 앱을 클릭합니다.
3. **App Details** 필드는 선택한 앱과 관련된 정보(이름, 설명, 버전 번호 및 관련 이미지 포함)로 미리 채워집니다.

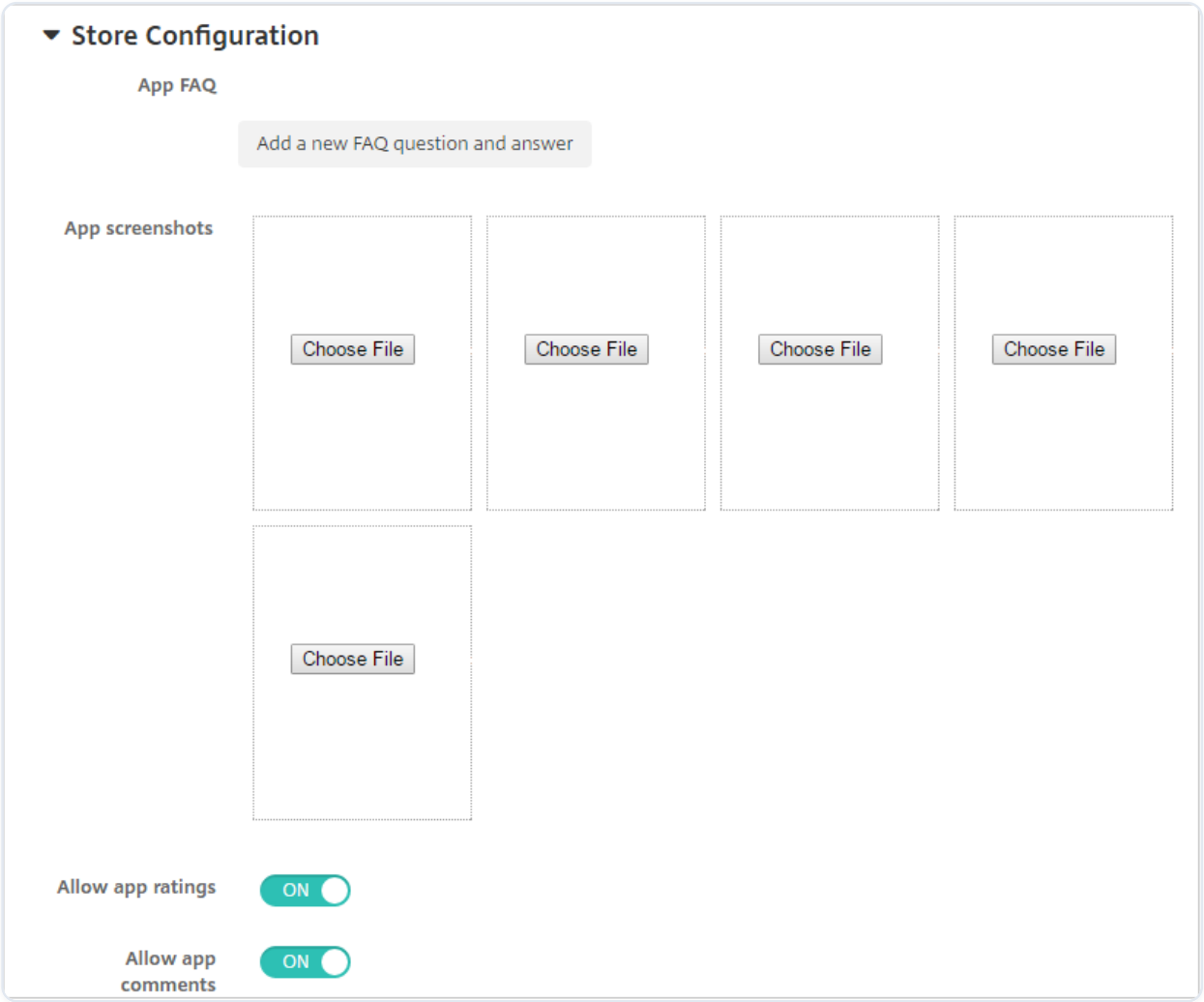


4. 설정을 구성합니다.

- 필요한 경우 앱의 이름과 설명을 변경합니다.
- **Paid app:** 이 필드는 미리 구성되어 있으며 변경할 수 없습니다.
- **MDM 프로필이 제거되면 앱 제거:** MDM 프로필이 제거될 경우 앱을 제거할지 여부를 선택합니다. 기본값은 **ON**입니다.

- **앱 데이터 백업 방지:** 앱이 데이터를 백업하지 못하도록 할지 여부를 선택합니다. 기본값은 **ON**입니다.
- **제품 트랙:** 사용자 장치로 푸시할 제품 트랙을 지정합니다. 테스트용으로 설계된 트랙이 있는 경우, 해당 트랙을 선택하여 사용자에게 할당할 수 있습니다. 기본값은 **Production**입니다.
- **앱 강제 관리:** 앱이 관리되지 않는 상태로 설치될 때, 감독되지 않는 장치에서 앱을 관리하도록 허용할지 사용자에게 메시지를 표시할지 여부를 선택합니다. 기본값은 **OFF**입니다. iOS 9.0 이상에서 사용할 수 있습니다.
- **라이선스를 장치에 강제 연결:** 장치 연결이 활성화된 상태로 개발된 앱을 사용자 대신 장치에 연결할지 여부를 선택합니다. iOS 9 이상에서 사용할 수 있습니다. 선택한 앱이 장치 할당을 지원하지 않는 경우 이 필드는 변경할 수 없습니다.

5. 배포 규칙을 구성합니다. 자세한 내용은 배포 규칙을 참조하십시오.
6. **스토어 구성**을 확장합니다.



- **앱 FAQ:** 앱에 대한 FAQ를 만들려면 **새 FAQ 질문 및 답변 추가**를 클릭합니다.
- **휴대폰/태블릿용 스크린샷 추가:** 앱 스토어에 표시될 화면 캡처를 추가합니다.

- **앱 평가 허용:** 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- **앱 댓글 허용:** 사용자가 앱 스토어에서 앱에 댓글을 남기도록 허용합니다.

7. iPhone 또는 iPad의 경우 **볼륨 구매**를 확장합니다.

   a. XenMobile이 앱에 볼륨 구매 라이선스를 적용하도록 하려면: **볼륨 구매 라이선스** 목록에서 **볼륨 구매 라이선스 업로드**를 클릭합니다.

   b. 나타나는 대화 상자에서 라이선스를 가져옵니다.

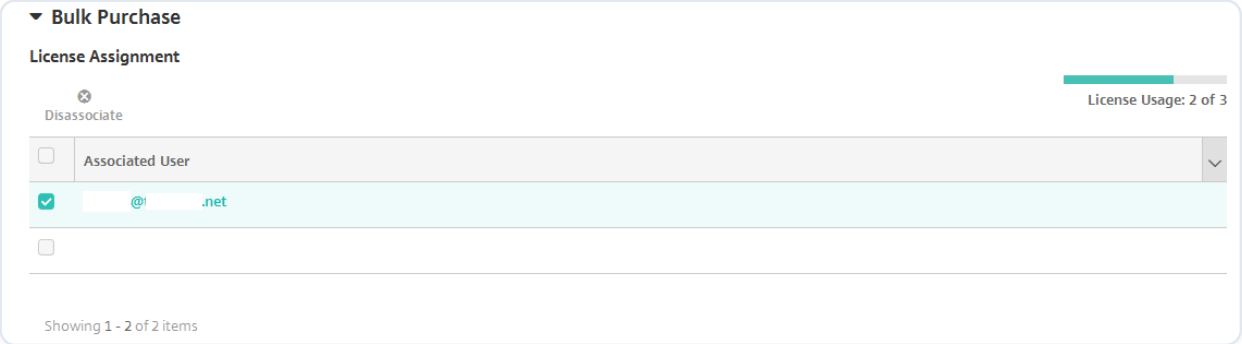
      라이선스 할당 테이블은 사용 가능한 총 라이선스 중에서 앱에 사용 중인 라이선스 수를 보여줍니다.

      개별 사용자에 대한 볼륨 구매 라이선스를 연결 해제할 수 있습니다. 이렇게 하면 라이선스 할당이 종료되고 라이선스가 해제됩니다.

8. Android Enterprise의 경우 **대량 구매** 섹션을 확장합니다.

   라이선스 할당 테이블은 사용 가능한 총 라이선스 중에서 앱에 사용 중인 라이선스 수를 보여줍니다.

   사용자를 선택한 다음 **연결 해제**를 클릭하여 해당 사용자의 라이선스 할당을 종료하고 다른 사용자를 위한 라이선스를 해제할 수 있습니다. 그러나 사용자가 특정 앱을 포함하는 배달 그룹의 일부가 아닌 경우에만 라이선스를 연결 해제할 수 있습니다.



9. **볼륨 구매** 또는 **대량 구매** 설정을 완료한 후 **다음**을 클릭합니다. **승인** 페이지가 나타납니다.

   사용자가 앱에 액세스하기 전에 승인을 요구하는 워크플로를 사용하려면 워크플로 적용을 참조하십시오. 승인 워크플로가 필요하지 않은 경우 다음 단계로 진행하십시오.

10. **다음**을 클릭합니다. **배달 그룹 할당** 페이지가 나타납니다.
11. **배달 그룹 선택** 옆에 입력하여 배달 그룹을 찾거나 목록에서 그룹을 선택합니다. 선택한 그룹은 **앱 할당을 받을 배달 그룹** 목록에 나타납니다.
12. **배포 일정**을 확장한 다음 다음 설정을 구성합니다.

    - **배포:** 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 **켜기**입니다.

- **배포 일정:** 앱을 **지금** 또는 **나중에** 배포할지 여부를 선택합니다. **나중에**를 선택하는 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 **지금**입니다.
- **배포 조건:** 장치가 연결될 때마다 앱을 배포하려면 **모든 연결 시**를 선택합니다. 장치가 이전에 앱을 받지 못한 경우 앱을 배포하려면 **이전 배포가 실패한 경우에만**을 선택합니다. 기본값은 **모든 연결 시**입니다.

항상 연결 배포는 **설정 > 서버 속성**에서 예약 백그라운드 배포 키를 구성한 경우에 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에서 동일합니다. **항상 연결 배포**를 제외하고 변경하는 모든 내용은 모든 플랫폼에 적용됩니다.

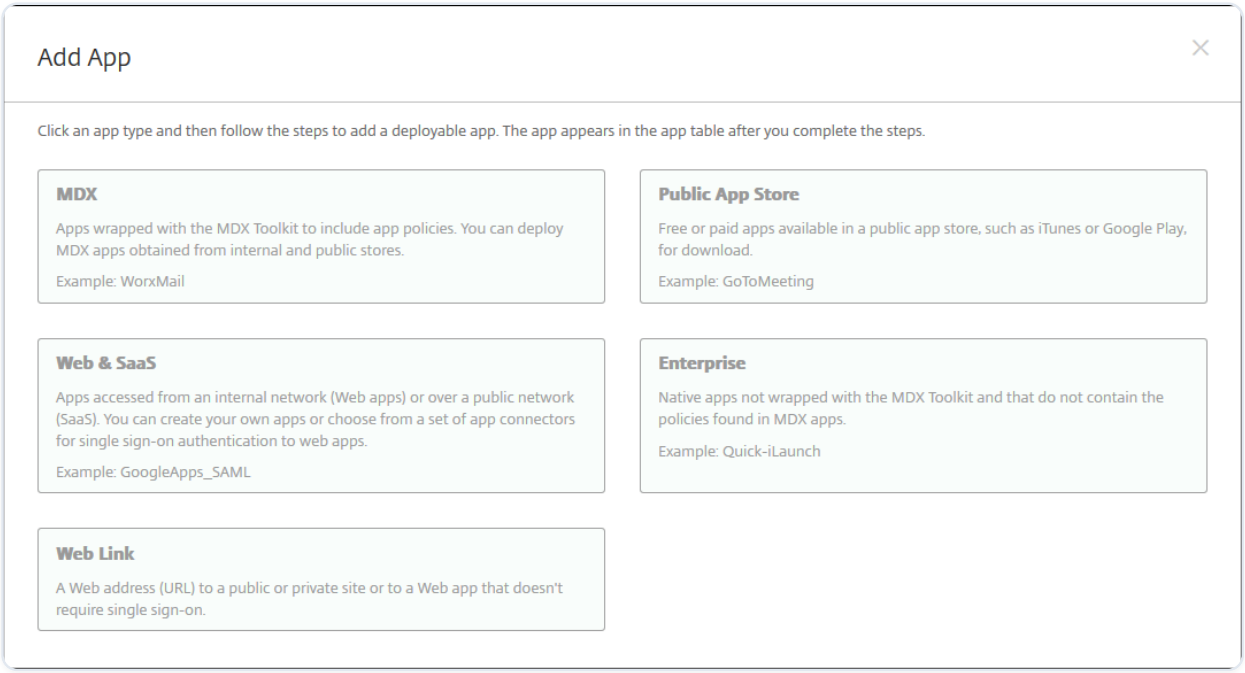
13. **저장**을 클릭합니다.

웹 또는 SaaS 앱 추가

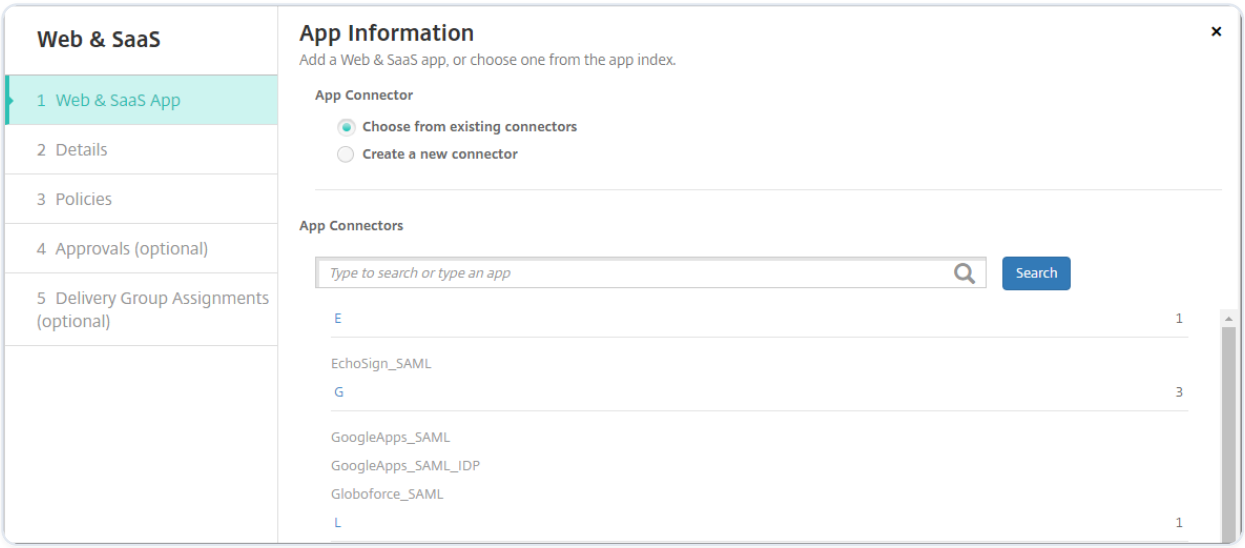
XenMobile 콘솔을 사용하여 모바일, 엔터프라이즈, 웹 및 SaaS 앱에 대한 사용자에게 SSO(Single Sign-On) 권한을 부여할 수 있습니다. 애플리케이션 커넥터 템플릿을 사용하여 앱에 SSO를 사용하도록 설정할 수 있습니다. XenMobile에서 사용할 수 있는 커넥터 유형 목록은 애플리케이션 커넥터 유형을 참조하십시오. 웹 또는 SaaS 앱을 추가할 때 XenMobile에서 사용자 고유의 커넥터를 빌드할 수도 있습니다.

앱이 SSO에만 사용 가능한 경우: 설정을 저장하면 XenMobile 콘솔의 **앱** 탭에 앱이 나타납니다.

1. XenMobile 콘솔에서 **구성 > 앱 > 추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.



2. **웹 및 SaaS**를 클릭합니다. **앱 정보** 페이지가 나타납니다.



3. 기존 또는 새 앱 커넥터를 다음과 같이 구성합니다.

기존 앱 커넥터를 구성하려면

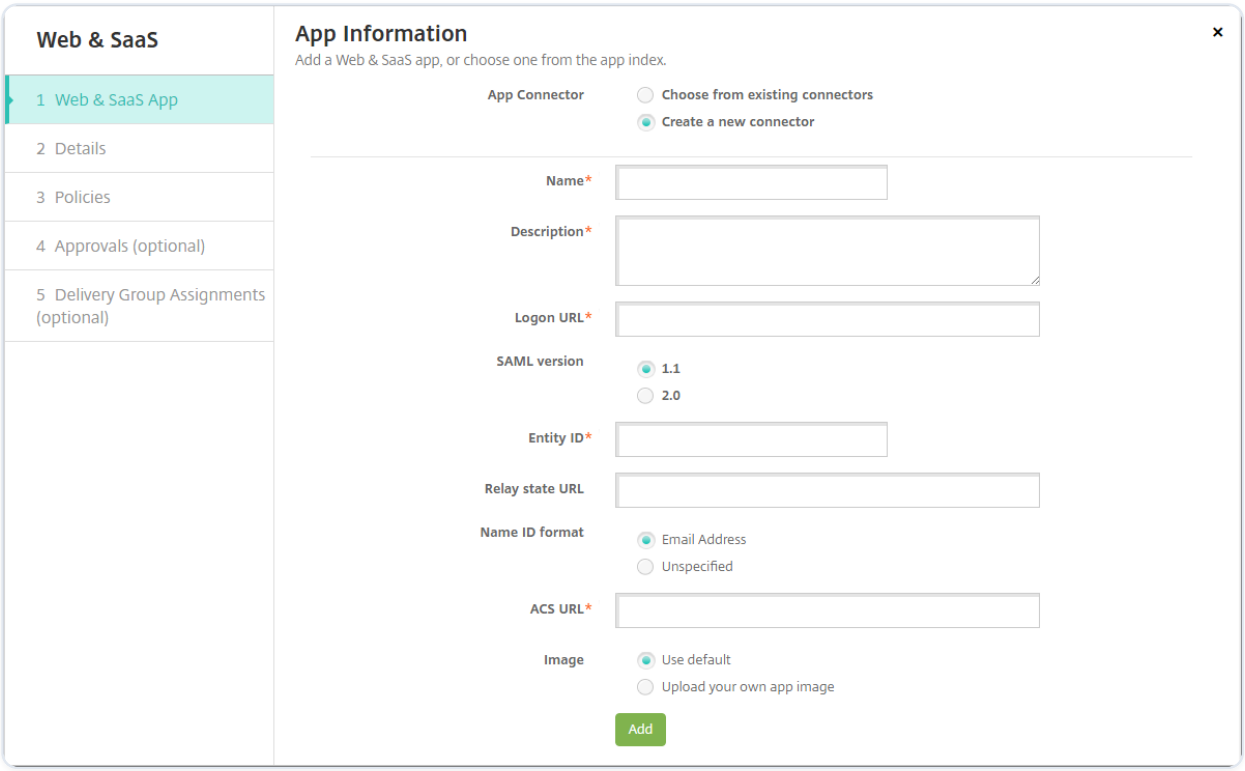
1. **앱 정보** 페이지에서 이전에 표시된 대로 **기존 커넥터에서 선택**이 이미 선택되어 있습니다. **앱 커넥터** 목록에서 사용할 커넥터를 클릭합니다. 앱 커넥터 정보가 나타납니다.
2. 다음 설정을 구성합니다.

   - **앱 이름:** 미리 채워진 이름을 수락하거나 새 이름을 입력합니다.
   - **앱 설명:** 미리 채워진 설명을 수락하거나 직접 입력합니다.
   - **URL:** 미리 채워진 URL을 수락하거나 앱의 웹 주소를 입력합니다. 선택한 커넥터에 따라 이 필드에는 다음 페이지로 이동하기 전에 교체해야 하는 자리 표시자가 포함될 수 있습니다.
   - **도메인 이름:** 해당하는 경우 앱의 도메인 이름을 입력합니다. 이 필드는 필수입니다.
   - **앱이 내부 네트워크에서 호스팅됨:** 앱이 내부 네트워크의 서버에서 실행 중인지 여부를 선택합니다. 사용자가 원격 위치에서 내부 앱에 연결하는 경우 Citrix Gateway를 통해 연결해야 합니다. 이 옵션을 **ON**으로 설정하면 앱에 VPN 키워드가 추가되고 사용자가 Citrix Gateway를 통해 연결할 수 있습니다. 기본값은 **OFF**입니다.
   - **앱 범주:** 목록에서 앱에 적용할 선택적 범주를 클릭합니다.
   - **사용자 계정 프로비저닝:** 애플리케이션에 대한 사용자 계정을 생성할지 여부를 선택합니다. Globoforce_SAML 커넥터를 사용하는 경우 원활한 SSO 통합을 위해 이 옵션을 활성화해야 합니다.
   - **사용자 계정 프로비저닝**을 활성화하는 경우 다음 설정을 구성합니다.
     - **서비스 계정**
       - **사용자 이름:** 앱 관리자의 이름을 입력합니다. 이 필드는 필수입니다.

        - **암호:** 앱 관리자 암호를 입력합니다. 이 필드는 필수입니다.
    - **사용자 계정**
        - **사용자 권한이 종료될 때:** 목록에서 사용자가 더 이상 앱에 액세스할 수 없을 때 수행할 작업을 클릭합니다. 기본값은 **계정 비활성화**입니다.
    - **사용자 이름 규칙**
        - 추가하려는 각 사용자 이름 규칙에 대해 다음을 수행합니다.
            - **사용자 속성:** 목록에서 규칙에 추가할 사용자 속성을 클릭합니다.
            - **길이(문자):** 목록에서 사용자 이름 규칙에 사용할 사용자 속성의 문자 수를 클릭합니다. 기본값은 **모두**입니다.
            - **규칙:** 추가하는 각 사용자 속성은 사용자 이름 규칙에 자동으로 추가됩니다.
- **비밀번호 요구 사항**
    - **길이:** 최소 사용자 비밀번호 길이를 입력합니다. 기본값은 **8**입니다.
- **비밀번호 만료**
    - **유효 기간(일):** 비밀번호가 유효한 일수를 입력합니다. 유효한 값은 **0–90**입니다. 기본값은 90입니다.
    - **만료 후 비밀번호 자동 재설정:** 비밀번호가 만료될 때 자동으로 재설정할지 여부를 선택합니다. 기본값은 **OFF**입니다. 이 필드를 활성화하지 않으면 사용자는 비밀번호가 만료된 후 앱을 열 수 없습니다.

새 앱 커넥터 구성

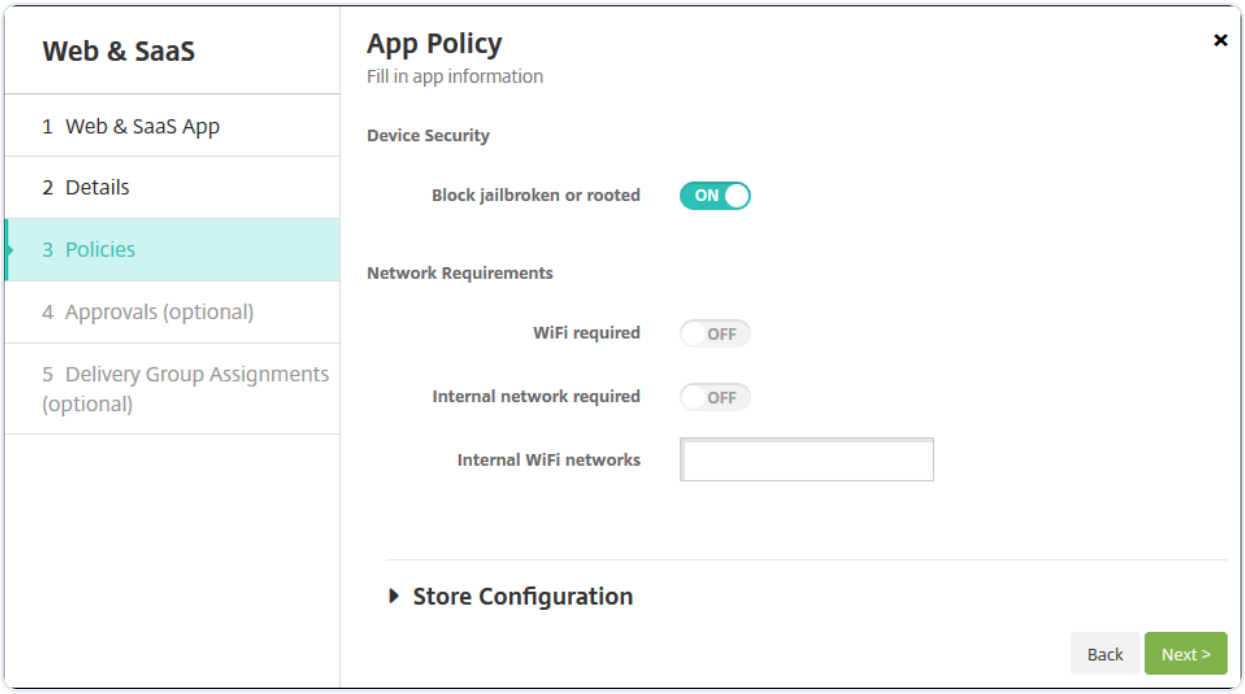
1. **앱 정보** 페이지에서 **새 커넥터 만들기**를 선택합니다. 앱 커넥터 필드가 나타납니다.



2. 다음 설정을 구성합니다:

- **이름:** 커넥터의 이름을 입력합니다. 이 필드는 필수입니다.
- **설명:** 커넥터에 대한 설명을 입력합니다. 이 필드는 필수입니다.
- **로그온 URL:** 사용자가 사이트에 로그온하는 URL을 입력하거나 복사하여 붙여넣습니다. 예를 들어, 추가하려는 앱에 로그온 페이지가 있는 경우 웹 브라우저를 열고 앱의 로그온 페이지로 이동합니다. 예를 들어, `https://www.example.com/logon`일 수 있습니다. 이 필드는 필수입니다.
- **SAML 버전: 1.1** 또는 **2.0**을 선택합니다. 기본값은 **1.1**입니다.
- **엔터티 ID:** SAML 앱의 ID를 입력합니다.
- **릴레이 상태 URL:** SAML 애플리케이션의 웹 주소를 입력합니다. 릴레이 상태 URL은 앱의 응답 URL입니다.
- **이름 ID 형식: 이메일 주소** 또는 **지정되지 않음**을 선택합니다. 기본값은 **이메일 주소**입니다.
- **ACS URL:** ID 공급자 또는 서비스 공급자의 Assertion Consumer Service URL을 입력합니다. ACS URL은 사용자에게 SSO 기능을 제공합니다.
- **이미지:** 기본 Citrix 이미지를 사용할지 또는 사용자 고유의 앱 이미지를 업로드할지 선택합니다. 기본값은 기본값 사용입니다.
  - 사용자 고유의 이미지를 업로드하려면 **찾아보기**를 클릭하고 파일 위치로 이동합니다. 파일은 .PNG 파일이어야 합니다. JPEG 또는 GIF 파일은 업로드할 수 없습니다. 사용자 지정 그래픽을 추가하면 나중에 변경할 수 없습니다.

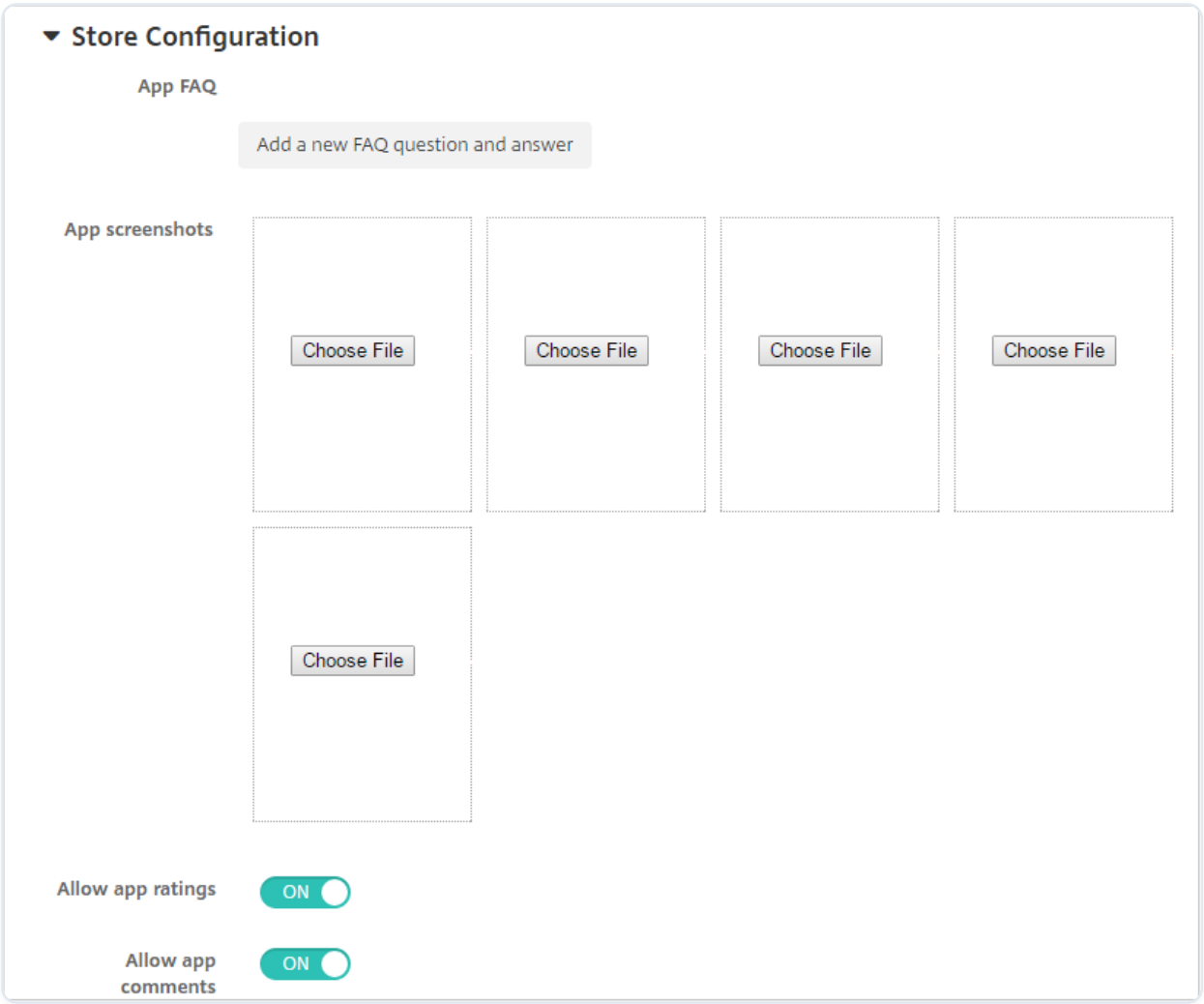
3. 완료되면 **추가**를 클릭합니다. **세부 정보** 페이지가 나타납니다.
4. **다음**을 클릭합니다. **앱 정책** 페이지가 나타납니다.



5. 다음 설정을 구성합니다.

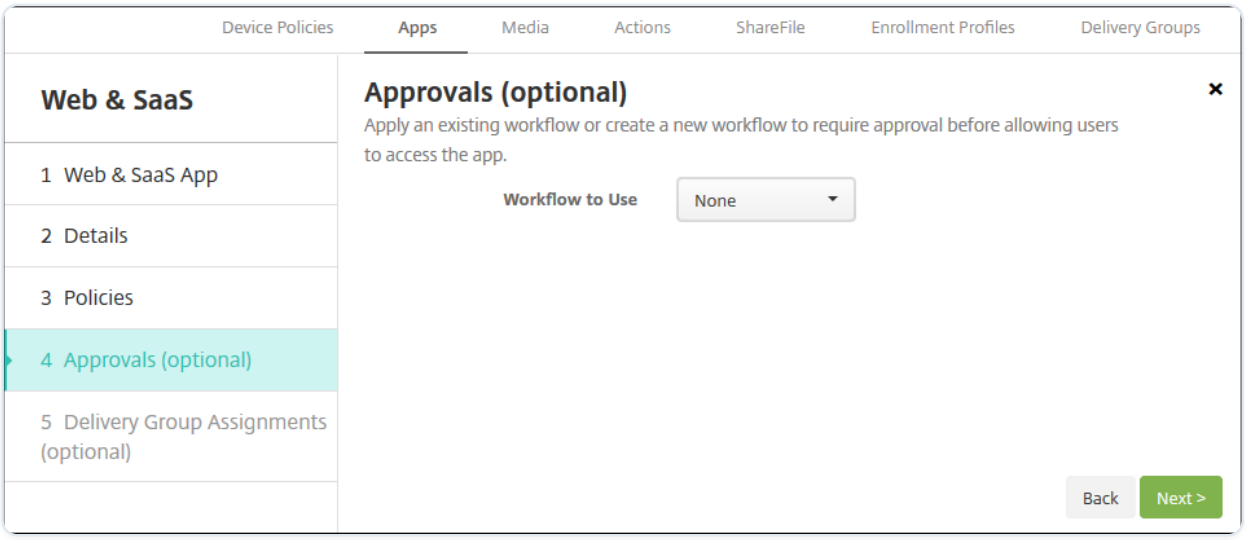
   - **장치 보안**
   - **탈옥 또는 루팅 차단:** 탈옥 또는 루팅된 장치가 앱에 액세스하는 것을 차단할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
   - **네트워크 요구 사항**
   - **WiFi 필요:** 앱을 실행하는 데 Wi-Fi 연결이 필요한지 여부를 선택합니다. 기본값은 **꺼짐**입니다.
   - **내부 네트워크 필요:** 앱을 실행하는 데 내부 네트워크가 필요한지 여부를 선택합니다. 기본값은 **꺼짐**입니다.
   - **내부 WiFi 네트워크: WiFi 필요**를 사용하도록 설정한 경우 사용할 내부 Wi-Fi 네트워크를 입력합니다.

6. 배포 규칙을 구성합니다. 자세한 내용은 배포 규칙을(를) 참조하십시오.
7. **스토어 구성**을 확장합니다.



- **앱 FAQ: 새 FAQ 질문 및 답변 추가**를 클릭하여 앱에 대한 FAQ를 생성합니다.
- **휴대폰/태블릿용 스크린샷 추가:** 앱 스토어에 표시될 화면 캡처를 추가합니다.
- **앱 평가 허용:** 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- **앱 댓글 허용:** 사용자가 앱 스토어에서 앱에 댓글을 남기도록 허용합니다.

8. **다음**을 클릭합니다. **승인** 페이지가 나타납니다.



사용자가 앱에 액세스하기 전에 승인을 요구하는 워크플로를 사용하려면 워크플로 적용을(를) 참조하십시오.

9. **다음**을 클릭합니다. **전달 그룹 할당** 페이지가 나타납니다.
10. **전달 그룹 선택** 옆에서 전달 그룹을 찾거나 하나 이상의 그룹을 선택하려면 입력합니다. 선택한 그룹은 **앱 할당을 받을 전달 그룹** 목록에 나타납니다.
11. **배포 일정**을 확장한 다음 다음 설정을 구성합니다.

    - **배포:** 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
    - **배포 일정:** 앱을 **지금** 배포할지 **나중에** 배포할지 선택합니다. **나중에**를 선택하는 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 **지금**입니다.
    - **배포 조건:** 장치가 연결될 때마다 앱을 배포하려면 **연결할 때마다**를 선택합니다. 이전에 장치가 앱을 수신하지 못한 경우 앱을 배포하려면 **이전 배포가 실패한 경우에만**을 선택합니다. 기본값은 **연결할 때마다**입니다.

    항상 켜짐 연결에 배포는 **설정 > 서버 속성**에서 예약 백그라운드 배포 키를 구성한 경우에 적용됩니다.

    구성하는 배포 일정은 모든 플랫폼에서 동일합니다. **항상 켜짐 연결에 배포**를 제외하고 변경하는 모든 사항은 모든 플랫폼에 적용됩니다.
12. **저장**을 클릭합니다.

엔터프라이즈 앱 추가

XenMobile의 엔터프라이즈 앱은 MAM SDK 또는 MDX Toolkit으로 준비되지 않은 기본 앱을 나타냅니다. 이러한 앱에는 MDX 앱과 관련된 정책이 포함되어 있지 않습니다. XenMobile 콘솔의 **앱** 탭에서 엔터프라이즈 앱을 업로드할 수 있습니다. 엔터프라이즈 앱은 다음 플랫폼(및 해당 파일 형식)을 지원합니다.

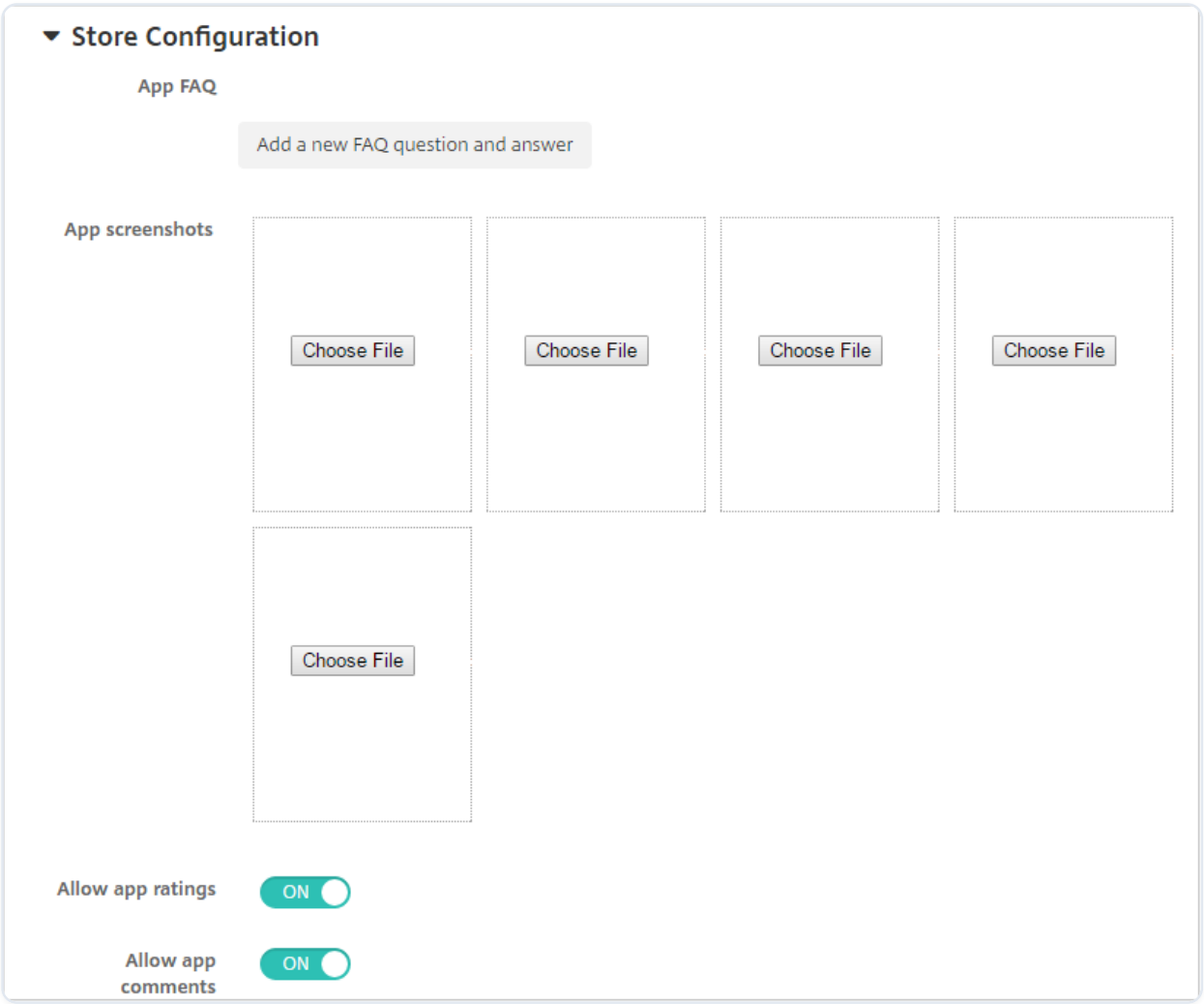
- iOS(.ipa 파일)
- Android(.apk 파일)
- 삼성 녹스 (.apk 파일)
- 안드로이드 엔터프라이즈 (.apk 파일)
- 참조: MDX 지원 개인 앱

Google Play 스토어에서 다운로드한 앱을 엔터프라이즈 앱으로 추가하는 것은 지원되지 않습니다. 대신 Google Play 스토어의 앱을 공용 앱 스토어 앱으로 추가하십시오. 공용 앱 스토어 앱 추가를 참조하십시오.

1. XenMobile 콘솔에서 **구성 > 앱 > 추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.

   (/en-us/xenmobile/server/media/configure-apps-add.png)

2. **엔터프라이즈**를 클릭합니다. **앱 정보** 페이지가 나타납니다.
3. **앱 정보** 창에서 다음 정보를 입력합니다.
    - **이름:** 앱에 대한 설명이 포함된 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다.
    - **설명:** 앱에 대한 선택적 설명을 입력합니다.
    - **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.
4. **다음**을 클릭합니다. **앱 플랫폼** 페이지가 나타납니다.
5. **플랫폼**에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼에 대해서만 구성하는 경우 다른 플랫폼은 선택을 취소합니다.
6. 선택한 각 플랫폼에 대해 **업로드**를 클릭하고 파일 위치로 이동하여 업로드할 파일을 선택합니다.
7. **다음**을 클릭합니다. 플랫폼에 대한 앱 정보 페이지가 나타납니다.
8. 다음과 같이 플랫폼 유형에 대한 설정을 구성합니다.
    - **파일 이름:** 선택적으로 앱의 새 이름을 입력합니다.
    - **앱 설명:** 선택적으로 앱의 새 설명을 입력합니다.
    - **앱 버전:** 이 필드는 변경할 수 없습니다.
    - **최소 OS 버전:** 선택적으로 장치에서 앱을 실행하는 데 필요한 가장 오래된 운영 체제 버전을 입력합니다.
    - **최대 OS 버전:** 선택적으로 장치에서 앱을 실행하는 데 필요한 최신 운영 체제를 입력합니다.
    - **제외된 장치:** 선택적으로 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
    - **패키지 ID:** 앱의 고유 식별자입니다.
    - **MDM 프로필 제거 시 앱 제거:** MDM 프로필이 제거될 때 장치에서 앱을 제거할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
    - **앱 데이터 백업 방지:** 앱이 데이터를 백업하지 못하도록 할지 여부를 선택합니다. 기본값은 **켜짐**입니다.
    - **앱 관리 강제 적용:** 관리되지 않는 앱을 설치하는 경우, 감독되지 않는 장치의 사용자에게 앱 관리를 허용하라는 메시지를 표시하려면 **켜짐**을 선택합니다. 사용자가 메시지를 수락하면 앱이 관리됩니다.
9. 배포 규칙을 구성합니다. 자세한 내용은 배포 규칙을 참조하십시오.
10. **스토어 구성**을 확장합니다.



- **앱 FAQ: 새 FAQ 질문 및 답변 추가**를 클릭하여 앱에 대한 FAQ를 만듭니다.
- **휴대폰/태블릿용 스크린샷 추가:** 앱 스토어에 표시되는 화면 캡처를 추가합니다.
- **앱 평가 허용:** 사용자가 앱 스토어에서 앱을 평가할 수 있도록 허용합니다.
- **앱 댓글 허용:** 사용자가 앱 스토어에서 앱에 대한 댓글을 남길 수 있도록 허용합니다.

11. **다음**을 클릭합니다. **승인** 페이지가 나타납니다.

    사용자가 앱에 액세스하기 전에 승인을 요구하는 워크플로를 사용하려면 워크플로 적용을 참조하십시오. 승인 워크플로가 필요하지 않은 경우 다음 단계로 진행합니다.

12. **다음**을 클릭합니다. **전달 그룹 할당** 페이지가 나타납니다.
13. **전달 그룹 선택** 옆에 전달 그룹을 찾기 위해 입력하거나 목록에서 그룹을 선택합니다. 선택한 그룹은 **앱 할당을 받을 전달 그룹** 목록에 나타납니다.
14. **배포 일정**을 확장한 다음 다음 설정을 구성합니다.

    - **배포:** 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 **켜짐**입니다.

- **배포 일정:** 앱을 **지금** 배포할지 **나중에** 배포할지 선택합니다. **나중에**를 선택하는 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 **지금**입니다.
- **배포 조건:** 장치가 연결될 때마다 앱을 배포하려면 **모든 연결 시**를 선택합니다. 이전에 장치가 앱을 수신하지 못했을 때 앱을 배포하려면 **이전 배포가 실패한 경우에만**을 선택합니다. 기본값은 **모든 연결 시**입니다.

항상 연결 배포는 **설정 > 서버 속성**에서 예약 백그라운드 배포 키를 구성한 경우에 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. **항상 연결 배포**를 제외하고 변경하는 모든 내용은 모든 플랫폼에 적용됩니다.

15. **저장**을 클릭합니다.

웹 링크 추가

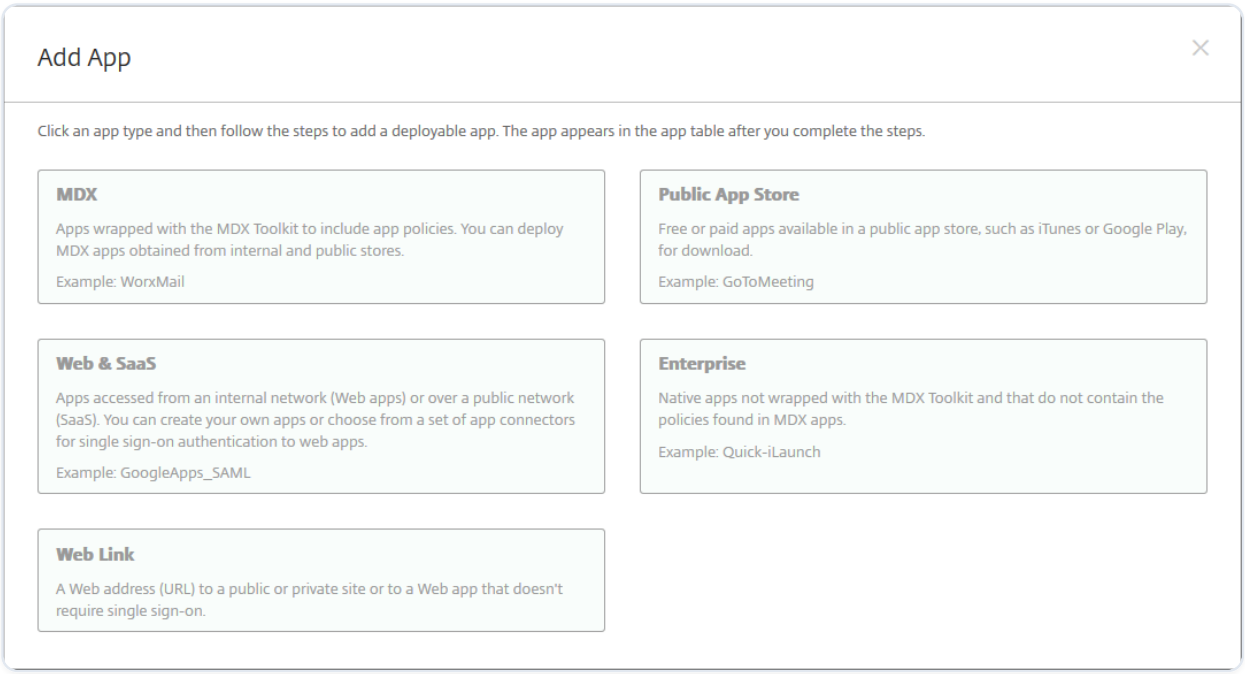
웹 링크는 인터넷 또는 인트라넷 사이트의 웹 주소입니다. 웹 링크는 SSO를 필요로 하지 않는 웹 응용 프로그램을 가리킬 수도 있습니다. 웹 링크 구성을 완료하면 링크가 앱 스토어에 아이콘으로 나타납니다. 사용자가 Secure Hub로 로그인하면 사용 가능한 앱 및 데스크톱 목록과 함께 링크가 나타납니다.

XenMobile 콘솔의 **앱** 탭에서 웹 링크를 구성할 수 있습니다. 웹 링크 구성을 완료하면 **앱** 테이블의 목록에 링크 아이콘으로 링크가 나타납니다. 사용자가 Secure Hub로 로그인하면 사용 가능한 앱 및 데스크톱 목록과 함께 링크가 나타납s니다.

링크를 추가하려면 다음 정보를 제공합니다.

- 링크 이름
- 링크 설명
- 웹 주소(URL)
- 범주
- 역할
- .png 형식의 이미지 (선택 사항)

1. XenMobile 콘솔에서 **구성 > 앱 > 추가**를 클릭합니다. **앱 추가** 대화 상자가 나타납니다.

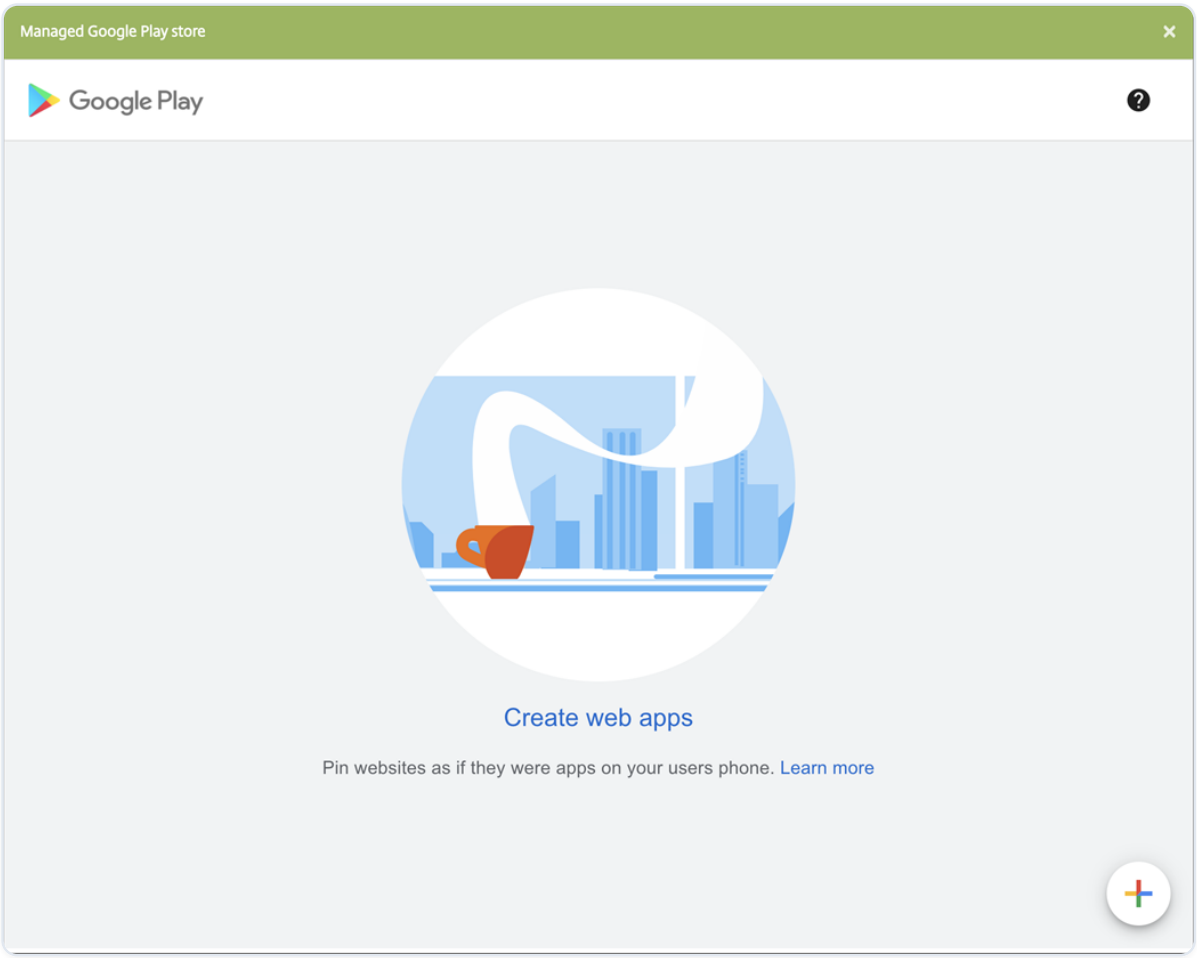


2. **웹 링크**를 클릭합니다. **앱 정보** 페이지가 나타납니다.
3. **앱 정보** 창에 다음 정보를 입력합니다.

   이름: 앱에 대한 설명적인 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나열됩니다. **설명:** 앱에 대한 선택적 설명을 입력합니다. **앱 범주:** 선택적으로 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 정보를 참조하십시오.

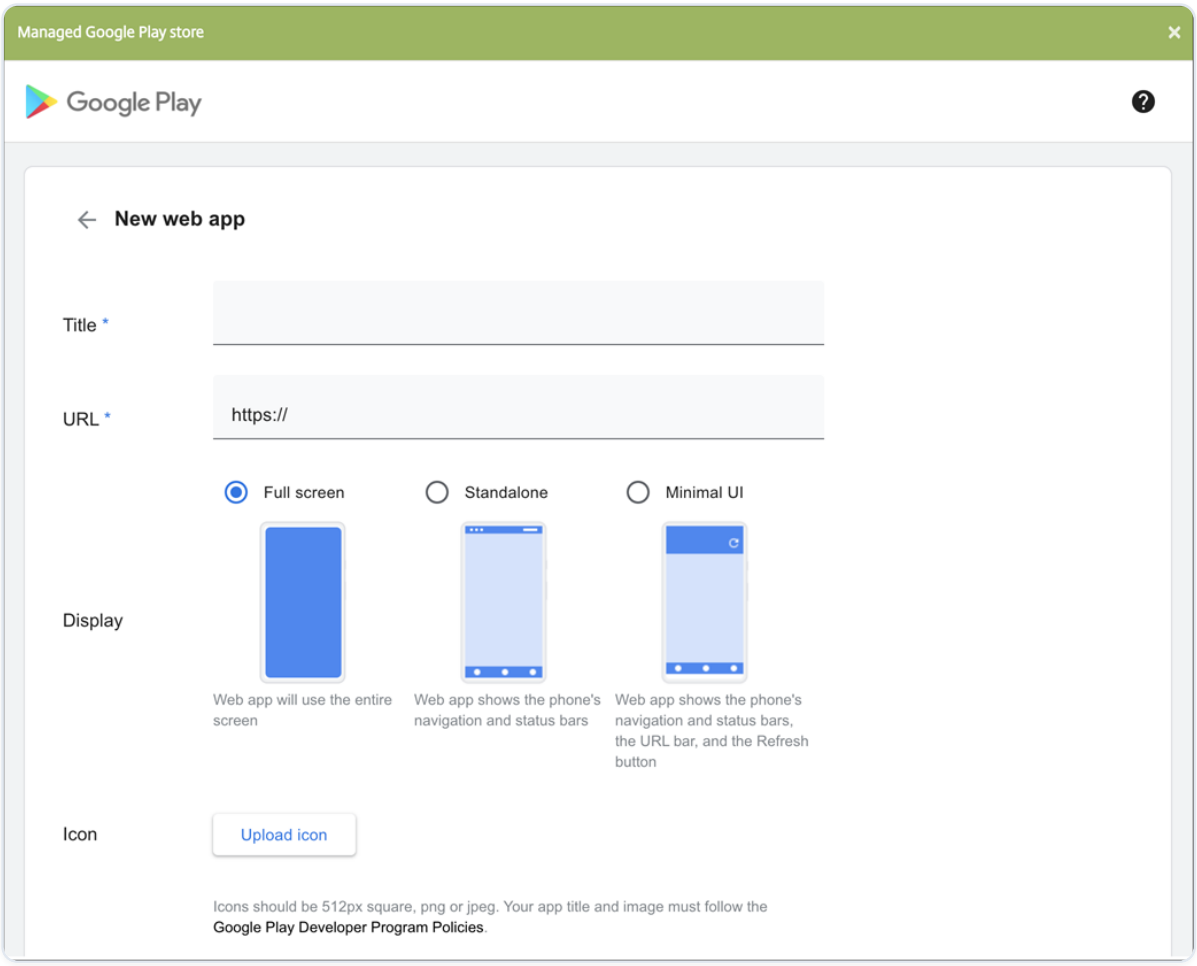
4. **다음**을 클릭합니다. **앱 플랫폼** 페이지가 나타납니다.
5. **플랫폼**에서 iOS 및 Android(레거시 DA)용 웹 앱을 추가하려면 **기타 플랫폼**을 선택하거나 **Android Enterprise**를 선택합니다. 추가하지 않으려는 확인란의 선택을 취소합니다.

   - **기타 플랫폼**을 선택한 경우 다음 단계로 진행하여 설정을 구성합니다.
   - **Android Enterprise**를 선택한 경우 **업로드** 버튼을 클릭하여 관리형 Google Play 스토어를 엽니다. 웹 앱을 게시하기 위해 개발자 계정을 등록할 필요는 없습니다. 계속하려면 오른쪽 하단 모서리에 있는 **더하기** 아이콘을 클릭합니다.



다음 설정을 구성합니다.

- **제목:** 웹 앱의 이름을 입력합니다.
- **URL:** 앱의 웹 주소를 입력합니다.
- **표시:** 사용자 장치에 웹 앱을 표시하는 방법을 선택합니다. 사용 가능한 옵션은 **전체 화면**, **독립 실행형** 및 **최소 UI**입니다.
- **아이콘:** 웹 앱을 나타내는 이미지를 업로드합니다.



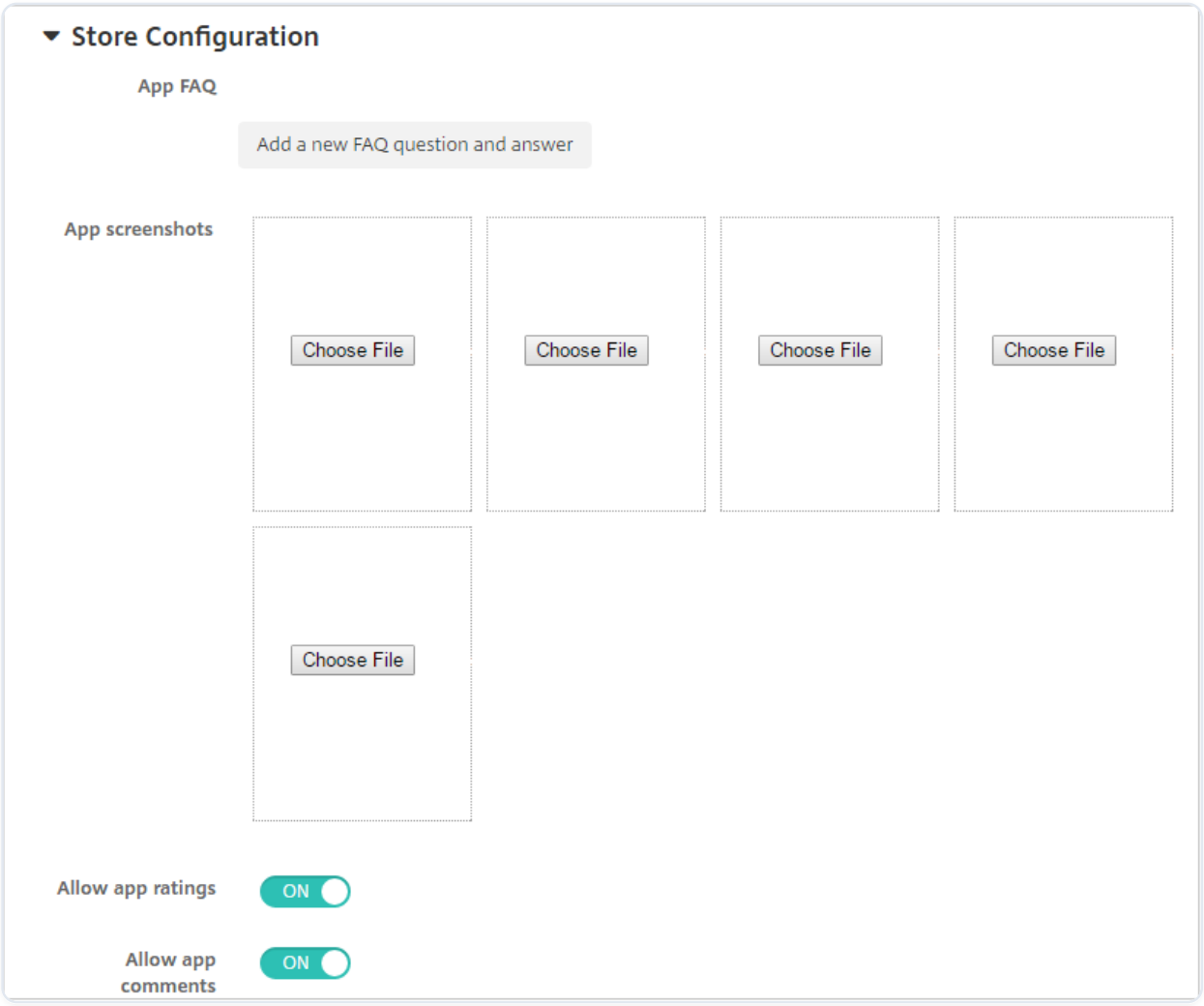
완료되면 **생성**을 클릭합니다. 웹 앱이 게시되는 데 최대 10분이 걸릴 수 있습니다.

6. Android Enterprise 이외의 플랫폼의 경우 다음 설정을 구성합니다.

   - **앱 이름:** 미리 채워진 이름을 수락하거나 새 이름을 입력합니다.
   - **앱 설명:** 미리 채워진 설명을 수락하거나 직접 입력합니다.
   - **URL:** 미리 채워진 URL을 수락하거나 앱의 웹 주소를 입력합니다. 선택한 커넥터에 따라 이 필드에는 다음 페이지로 이동하기 전에 바꿔야 하는 자리 표시자가 포함될 수 있습니다.
   - **앱이 내부 네트워크에서 호스팅됨:** 앱이 내부 네트워크의 서버에서 실행되는지 여부를 선택합니다. 사용자가 원격 위치에서 내부 앱에 연결하는 경우 Citrix Gateway를 통해 연결해야 합니다. 이 옵션을 **ON**으로 설정하면 앱에 VPN 키워드가 추가되고 사용자가 Citrix Gateway를 통해 연결할 수 있습니다. 기본값은 **OFF**입니다.
   - **앱 범주:** 목록에서 앱에 적용할 선택적 범주를 클릭합니다.
   - **이미지:** 기본 Citrix 이미지를 사용할지 또는 사용자 고유의 앱 이미지를 업로드할지 선택합니다. 기본값은 기본값 사용입니다.

     - 자신만의 이미지를 업로드하려면 **찾아보기**를 클릭하고 파일 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 규칙을 참조하십시오.
8. **스토어 구성**을 확장합니다.



- **앱 FAQ: 새 FAQ 질문 및 답변 추가**를 클릭하여 앱에 대한 FAQ를 만듭니다.
- **휴대폰/태블릿용 스크린샷 추가:** 앱 스토어에 표시되는 화면 캡처를 추가합니다.
- **앱 등급 허용:** 사용자가 앱 스토어에서 앱을 평가하도록 허용합니다.
- **앱 댓글 허용:** 사용자가 앱 스토어에서 앱에 댓글을 남기도록 허용합니다.

9. **다음**을 클릭합니다. **전달 그룹 할당** 페이지가 나타납니다.
10. **전달 그룹 선택** 옆에서 전달 그룹을 찾거나 목록에서 하나 이상의 그룹을 선택하려면 입력합니다. 선택한 그룹은 **앱 할당을 받을 전달 그룹** 목록에 나타납니다.
11. **배포 일정**을 확장한 다음 다음 설정을 구성합니다.

- **배포:** 앱을 장치에 배포할지 여부를 선택합니다. 기본값은 **켜기**입니다.
- **배포 일정:** 앱을 **지금** 배포할지 **나중에** 배포할지 선택합니다. **나중에**를 선택하는 경우 앱을 배포할 날짜와 시간을 구성합니다. 기본값은 **지금**입니다.

- **배포 조건:** 장치가 연결될 때마다 앱을 배포하려면 **모든 연결 시**를 선택합니다. 장치가 이전에 앱을 받지 못한 경우 앱을 배포하려면 **이전 배포가 실패한 경우에만**을 선택합니다. 기본값은 **모든 연결 시**입니다.

항상 켜져 있는 연결에 배포는 **설정 > 서버 속성**에서 예약 백그라운드 배포 키를 구성한 경우 적용됩니다.

구성하는 배포 일정은 모든 플랫폼에서 동일합니다. **항상 켜져 있는 연결에 배포**를 제외하고 변경한 모든 내용은 모든 플랫폼에 적용됩니다.

12. **저장**을 클릭합니다.

Microsoft 365 앱 사용

MDX 컨테이너를 열어 Secure Mail, Secure Web 및 Citrix Files가 문서와 데이터를 Microsoft Office 365 앱으로 전송하도록 허용할 수 있습니다. 자세한 내용은 Office 365 앱과의 보안 상호 작용 허용을 참조하십시오.

워크플로 적용

워크플로를 할당하거나 생성하려면 다음 설정을 구성합니다.

- **사용할 워크플로:** 목록에서 기존 워크플로를 클릭하거나 **새 워크플로 생성**을 클릭합니다. 기본값은 **없음**입니다.

  새 워크플로 생성을 선택한 경우 다음 설정을 구성합니다.

  - **이름:** 워크플로의 고유한 이름을 입력합니다.
  - **설명:** 선택적으로 워크플로에 대한 설명을 입력합니다.
  - **이메일 승인 템플릿:** 목록에서 할당할 이메일 승인 템플릿을 선택합니다. 이 필드 오른쪽에 있는 눈 아이콘을 클릭하면 템플릿을 미리 볼 수 있는 대화 상자가 나타납니다.
  - **관리자 승인 수준:** 목록에서 이 워크플로에 필요한 관리자 승인 수준 수를 선택합니다. 기본값은 1단계입니다. 가능한 옵션은 다음과 같습니다.
    - 필요 없음
    - 1단계
    - 2단계
    - 3단계
  - **Active Directory 도메인 선택:** 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.

- **추가 필수 승인자 찾기:** 검색 필드에 추가 필수 승인자의 이름을 입력한 다음 **검색**을 클릭합니다. 이름은 Active Directory에서 가져옵니다.
- 필드에 이름이 나타나면 이름 옆의 확인란을 선택합니다. 이름과 이메일 주소는 **선택된 추가 필수 승인자** 목록에 나타납니다.

  선택된 추가 필수 승인자 목록에서 사람을 제거하려면 다음 중 하나를 수행합니다.

  - **검색**을 클릭하여 선택한 도메인의 모든 사람 목록을 확인합니다.
  - 검색 상자에 전체 이름 또는 부분 이름을 입력한 다음 **검색**을 클릭하여 검색 결과를 제한합니다.
  - **선택된 추가 필수 승인자** 목록에 있는 사람의 이름 옆에는 검색 결과 목록에 확인 표시가 있습니다. 목록을 스크롤하여 제거하려는 각 이름 옆의 확인란을 선택 취소합니다.

앱 스토어 및 Citrix Secure Hub 브랜딩

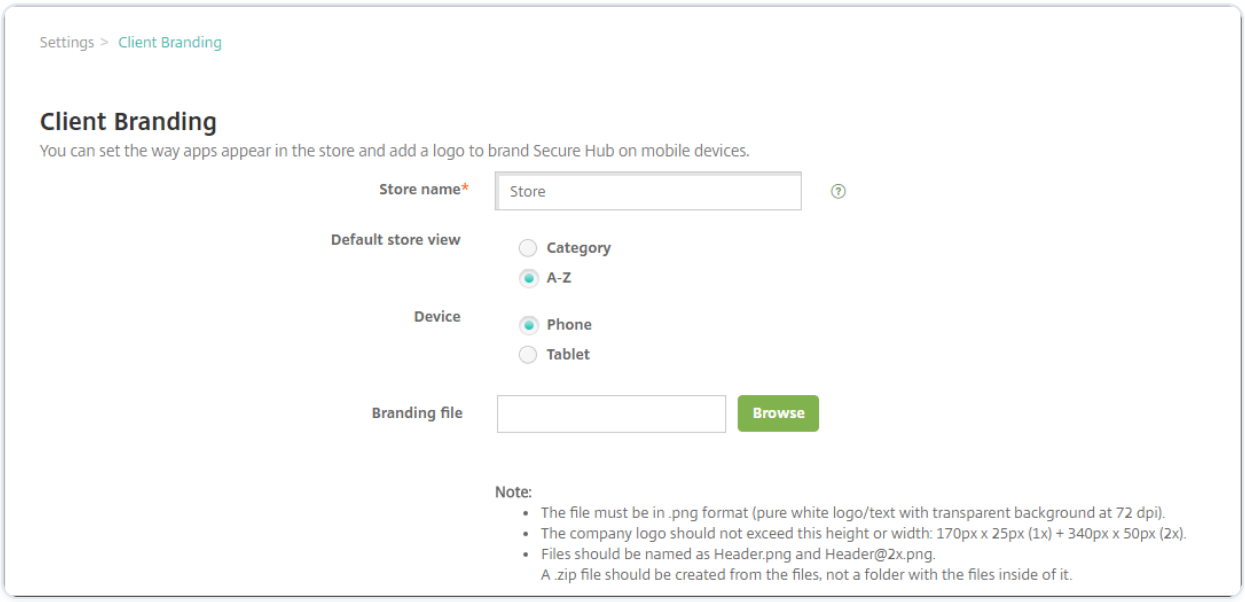
스토어에 앱이 표시되는 방식을 설정하고 로고를 추가하여 Secure Hub 및 앱 스토어의 브랜드를 지정할 수 있습니다. 이러한 브랜딩 기능은 iOS 및 Android 장치에서 사용할 수 있습니다.

시작하기 전에 사용자 지정 이미지를 준비하고 액세스할 수 있는지 확인하십시오.

사용자 지정 이미지는 다음 요구 사항을 충족해야 합니다.

- 파일은 .png 형식이어야 합니다.
- 72dpi의 투명한 배경에 순백색 로고 또는 텍스트를 사용합니다.
- 회사 로고는 다음 높이 또는 너비를 초과해서는 안 됩니다: 170px x 25px(1x) 및 340px x 50px(2x).
- 파일 이름을 Header.png 및 `Header@2x.png`으로 지정합니다.
- 파일이 들어 있는 폴더가 아닌 파일에서 .zip 파일을 만듭니다.

1. XenMobile Server 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **클라이언트** 아래에서 **클라이언트 브랜딩**을 클릭합니다. **클라이언트 브랜딩** 페이지가 나타납니다.



다음 설정을 구성합니다:

- **스토어 이름:** 스토어 이름은 사용자 계정 정보에 나타납니다. 이름을 변경하면 스토어 서비스에 액세스하는 데 사용되는 URL도 변경됩니다. 일반적으로 기본 이름을 변경할 필요는 없습니다.

  > **중요:**
  >
  > 스토어 이름은 영숫자 문자만 포함할 수 있습니다.

- **기본 스토어 보기: 범주** 또는 **A-Z**를 선택합니다. 기본값은 **A-Z**입니다.
- **장치 옵션: 전화** 또는 **태블릿**을 선택합니다. 기본값은 **전화**입니다.
- **브랜딩 파일: 찾아보기**를 클릭하여 파일 위치로 이동한 다음 브랜딩에 사용할 이미지 또는 이미지의 .zip 파일을 선택합니다.

3. **저장**을 클릭합니다.

앱 커넥터 유형

다음 표에는 웹 또는 SaaS 앱을 추가할 때 XenMobile®에서 사용할 수 있는 커넥터 및 커넥터 유형이 나열되어 있습니다. 웹 또는 SaaS 앱을 추가할 때 XenMobile에 새 커넥터를 추가할 수도 있습니다.

이 표는 커넥터가 사용자 계정 관리를 지원하는지 여부를 나타내며, 이를 통해 자동으로 또는 워크플로를 사용하여 새 계정을 생성할 수 있습니다.

커넥터 이름	SSO SAML	사용자 계정 관리 지원
EchoSign_SAML	예	예
Globoforce_SAML		**참고:** 이 커넥터를 사용할 때는 원활한 SSO 통합을 위해 프로비저닝을 위한 사용자 관리를 활성화해야 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

XenMobile에서 MDX 또는 엔터프라이즈 앱을 업그레이드하려면 XenMobile 콘솔에서 앱을 비활성화한 다음 새 버전의 앱을 업로드합니다. Citrix Secure Mail과 같은 공용 앱 스토어 앱은 비활성화할 필요가 없습니다.

1. XenMobile® 콘솔에서 **구성 > 앱**을 클릭합니다. **앱** 페이지가 나타납니다.
2. 관리되는 장치(모바일 장치 관리를 위해 XenMobile에 등록된 장치)의 경우 3단계로 건너뜁니다. 관리되지 않는 장치(엔터프라이즈 앱 관리 목적으로만 XenMobile에 등록된 장치)의 경우 다음을 수행합니다.

    a. **앱** 테이블에서 앱 옆의 확인란을 선택하거나 업데이트하려는 앱이 있는 줄을 클릭합니다.

b. 나타나는 메뉴에서 **비활성화**를 클릭합니다.

앱 메뉴(/en-us/xenmobile/server/media/configure-apps-disable-app.png)

c. 확인 대화 상자에서 **비활성화**를 클릭합니다. 앱의 **비활성화** 열에 *비활성화됨*이 나타납니다.

비활성화된 앱(/en-us/xenmobile/server/media/configure-apps-disable-app-disabled.png)

> **참고:**
>
> 앱이 비활성화된 동안에는 사용자가 로그오프한 후 앱에 다시 연결할 수 없습니다. 앱 비활성화는 선택 사항이지만, 앱 기능 관련 문제를 방지하기 위해 앱을 비활성화하는 것이 좋습니다. 예를 들어, 새 버전을 업로드하는 동시에 사용자가 앱 다운로드를 요청하면 문제가 발생할 수 있습니다.

3. **앱** 테이블에서 앱 옆의 확인란을 클릭하거나 업데이트하려는 앱이 있는 줄을 클릭합니다.
4. 나타나는 메뉴에서 **편집**을 클릭합니다. 앱에 대해 원래 선택했던 플랫폼이 선택된 상태로 **앱 정보** 페이지가 나타납니다.
5. 다음 설정을 구성합니다.
   - **이름:** 선택적으로 앱 이름을 변경합니다.
   - **설명:** 선택적으로 앱 설명을 변경합니다.
   - **앱 범주:** 선택적으로 앱 범주를 변경합니다.
6. **다음**을 클릭합니다. 첫 번째 선택한 플랫폼 페이지가 나타납니다. 선택한 각 플랫폼에 대해 다음을 수행합니다.
   a. **업로드**를 클릭하여 파일 위치로 이동한 다음 업로드할 대체 파일을 선택합니다. 앱이 XenMobile에 업로드됩니다.

   Android Enterprise용 앱을 업로드하는 경우 관리형 Google Play 창이 나타납니다. 여기에 새 버전의 앱을 업로드합니다. 자세한 내용은 Android Enterprise 앱 배포를 참조하십시오.

   b. 선택적으로 플랫폼에 대한 앱 세부 정보 및 정책 설정을 변경합니다.
   c. 선택적으로 배포 규칙 및 XenMobile Store 구성을 구성합니다. 자세한 내용은 앱 추가에서 MDX 앱 추가를 참조하십시오.
7. **저장**을 클릭합니다. **앱** 페이지가 나타납니다.
8. 2단계에서 앱을 비활성화한 경우 다음을 수행합니다.

a. **앱** 테이블에서 업데이트한 앱을 클릭하여 선택한 다음 나타나는 메뉴에서 **활성화**를 클릭합니다.

b. 나타나는 확인 대화 상자에서 **활성화**를 클릭합니다. 이제 사용자는 앱에 액세스하고 앱을 업그레이드하라는 알림을 받을 수 있습니다.

시트릭스 런처

시트릭스 런처 대체

Citrix는 2020년 8월에 앱 스토어에서 Citrix Launcher를 제거했습니다. Citrix Launcher를 대체하려면 이미 사용 가능한 기능을 사용할 수 있습니다.

디바이스를 키오스크(전용 디바이스)로 프로비저닝하려면 다음을 수행합니다.

1. XenMobile 관리자가 전용 디바이스를 XenMobile 배포에 등록할 수 있도록 하는 RBAC 역할을 추가합니다. 전용 Android Enterprise 디바이스 프로비저닝을 참조하십시오.
2. **등록 유형**이 **완전 관리형/회사 프로필**인 등록 프로필을 생성합니다. 등록 프로필을 생성하려면을 참조하십시오.
3. **작업 잠금 모드** 설정을 활성화하여 디바이스 화면에 앱을 고정하도록 구성하는 키오스크 디바이스 정책을 생성합니다. Android Enterprise 설정을 참조하십시오.

시트릭스 런처 정보

Citrix Launcher를 사용하면 XenMobile에서 배포한 Android 디바이스의 사용자 환경을 사용자 지정할 수 있습니다. Citrix Launcher의 Secure Hub 관리에 지원되는 최소 Android 버전은 Android 4.0.3입니다. Citrix Launcher 및 Launcher 구성 디바이스 정책은 Android Enterprise와 호환되지 않습니다.

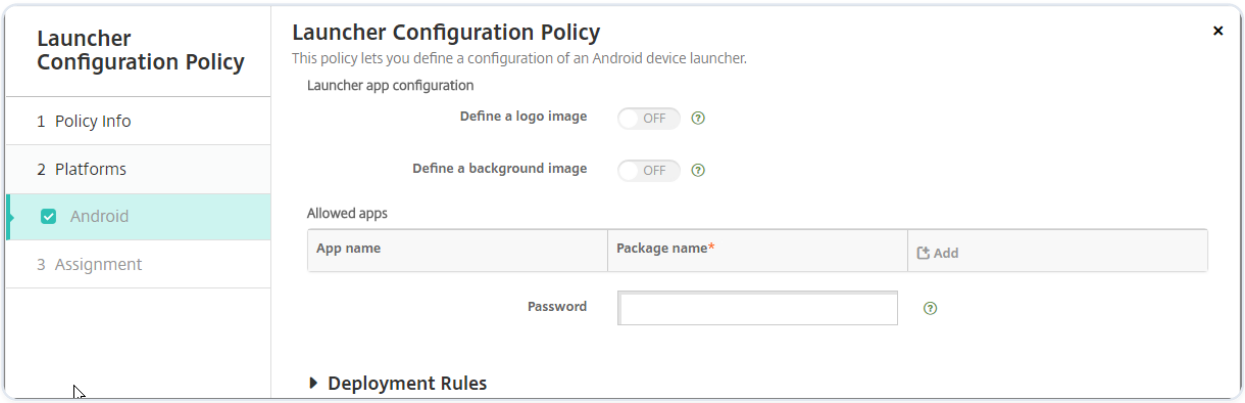
Launcher 구성 정책을 추가하여 다음 Citrix Launcher 기능을 제어할 수 있습니다.

- 사용자가 지정한 앱에만 액세스할 수 있도록 Android 디바이스를 관리합니다.
- 선택적으로 Citrix Launcher 아이콘에 대한 사용자 지정 로고 이미지와 Citrix Launcher에 대한 사용자 지정 배경 이미지를 지정합니다.
- 사용자가 런처를 종료하기 위해 입력해야 하는 암호를 지정합니다.

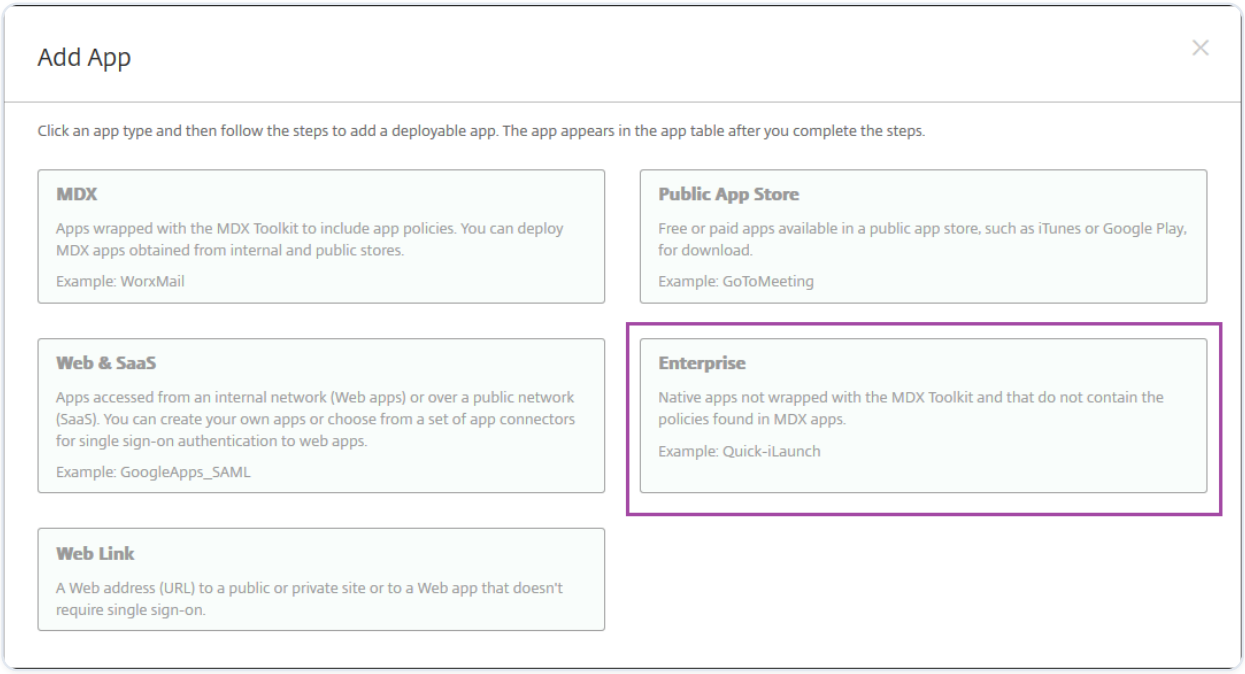
Citrix Launcher를 통해 이러한 디바이스 수준 제한을 적용할 수 있지만, 런처는 사용자에게 Wi-Fi 설정, Bluetooth 설정 및 디바이스 암호 설정과 같은 디바이스 설정에 대한 기본 제공 액세스 권한을 부여합니다. Citrix Launcher는 디바이스 플랫폼이 이미 제공하는 보안 위에 추가 보안 계층으로 의도된 것이 아닙니다.

Android 디바이스에 Citrix Launcher를 제공하려면 다음 일반 단계를 따르십시오.

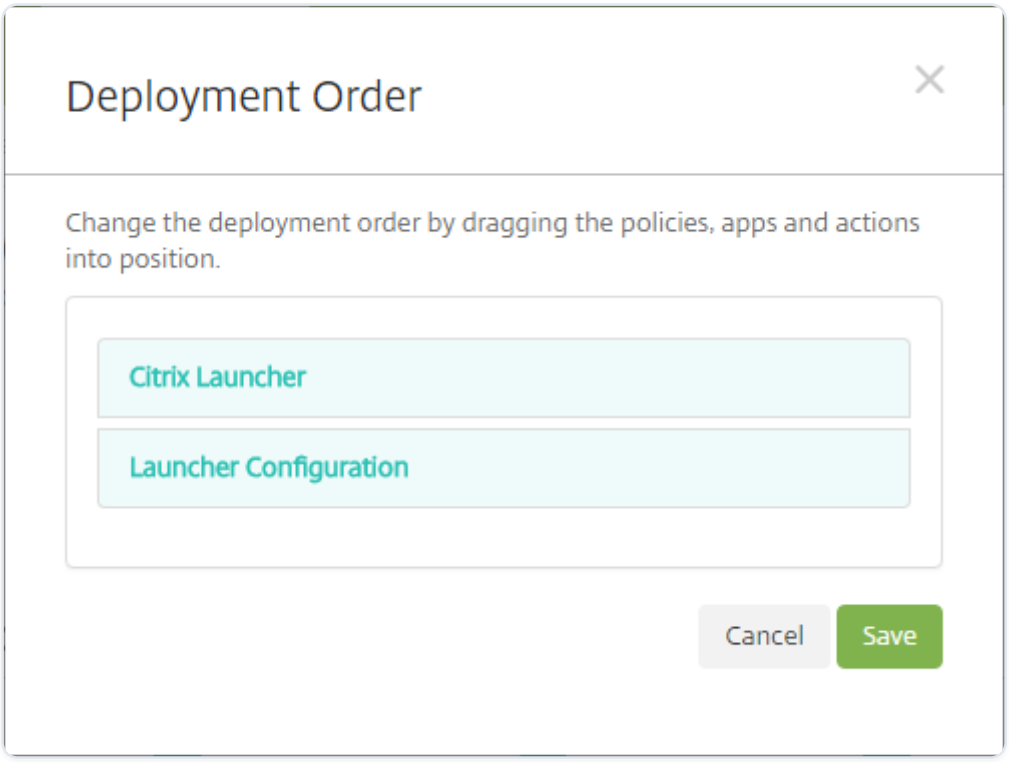
1. Citrix Launcher 앱을 다운로드하려면: `<https://www.citrix.com/downloads>`으로 이동합니다. **Citrix Launcher**를 검색합니다. 파일 이름은 CitrixLauncher.apk입니다. 이 파일은 XenMobile에 업로드할 준비가 되어 있으며 래핑이 필요하지 않습니다.
2. 장치 정책인 **Launcher Configuration Policy**를 추가합니다. **구성 > 장치 정책**으로 이동하여 **추가**를 클릭한 다음 **새 정책 추가** 대화 상자에서 **Launcher**를 입력하기 시작합니다. 자세한 내용은 Launcher Configuration Policy를 참조하십시오.



3. Citrix Launcher 앱을 엔터프라이즈 앱으로 XenMobile에 추가합니다. **구성 > 앱**에서 **추가**를 클릭한 다음 **엔터프라이즈**를 클릭합니다. 자세한 내용은 엔터프라이즈 앱 추가를 참조하십시오.



4. **구성 > 배달 그룹**에서 다음 구성으로 Citrix Launcher용 배달 그룹을 생성합니다.
   - **정책** 페이지에서 **Launcher Configuration Policy**를 추가합니다.
   - **앱** 페이지에서 **Citrix Launcher**를 **필수 앱**으로 끌어다 놓습니다.
   - **요약** 페이지에서 **배포 순서**를 클릭하고 **Citrix Launcher** 앱이 **Launcher Configuration** 정책보다 먼저 오도록 합니다.



자세한 내용은 리소스 배포를 참조하십시오.

Apple 볼륨 구매

Apple iOS 볼륨 구매를 사용하여 iOS 앱 라이선스를 관리할 수 있습니다. 볼륨 구매 솔루션은 조직을 위한 앱 및 기타 데이터를 대량으로 찾고, 구매하고, 배포하는 프로세스를 간소화합니다.

볼륨 구매를 통해 XenMobile®을 사용하여 공용 앱 스토어 앱을 배포할 수 있습니다.

- 볼륨 구매는 MAM 등록에 지원되지 않습니다. 볼륨 구매 장치는 MDM 또는 MDM+MAM에 등록해야 합니다.
- 볼륨 구매는 Citrix® 모바일 생산성 앱에 지원되지 않습니다.
- 볼륨 구매를 통해 XenMobile 공용 스토어 앱을 배포할 수 있지만, 배포가 최적화되지 않습니다. 이러한 제한 사항을 해결하려면 XenMobile 및 Secure Hub 스토어에 대한 개선 사항이 필요합니다.
- 볼륨 구매를 통해 XenMobile 공용 스토어 앱을 배포할 때 알려진 문제 목록은 Citrix Knowledge Center의 CTX222633을 참조하십시오.

볼륨 구매를 통해 해당 앱을 장치에 직접 배포할 수 있습니다. 또는 교환 코드를 사용하여 사용자에게 콘텐츠를 할당할 수 있습니다. XenMobile에서 iOS 볼륨 구매에 특정한 설정을 구성합니다.

XenMobile은 라이선스에 모든 변경 사항이 반영되도록 Apple에서 볼륨 구매 라이선스를 주기적으로 다시 가져옵니다. 이러한 변경 사항에는 가져온 앱을 볼륨 구매에서 수동으로 삭제하는 경우가 포함됩니다. 기본적으

로 XenMobile은 볼륨 구매 라이선스 기준선을 최소 1440분(24시간)마다 새로 고칩니다. 서버 속성 `VPP.baseline`을 통해 볼륨 구매 기준선 간격을 변경할 수 있습니다. 서버 속성을 참조하십시오.

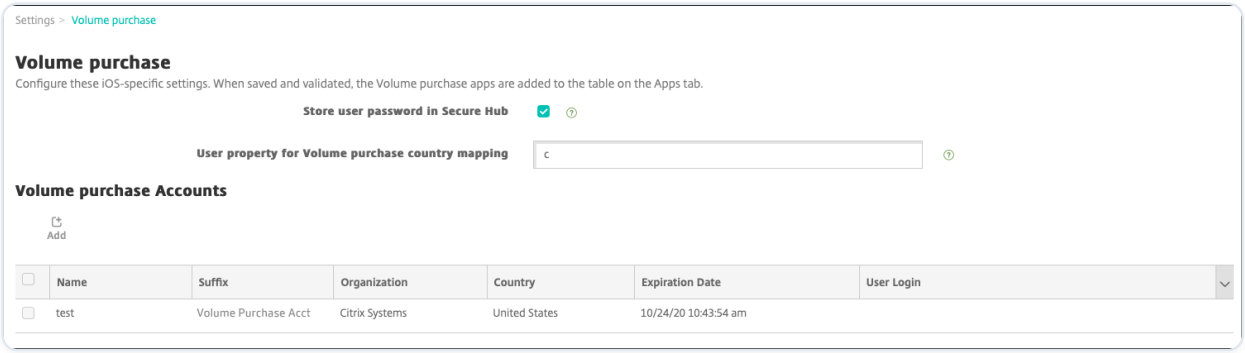
앱 자동 업데이트 설정도 `VPP.baseline` 서버 속성에 의존하며, 앱은 해당 속성에 설정된 동일한 일정에 따라 업데이트됩니다.

이 문서에서는 XenMobile을 사용하여 앱을 배포할 수 있도록 관리형 라이선스와 함께 볼륨 구매를 사용하는 데 중점을 둡니다. 현재 교환 코드를 사용하고 있으며 관리형 배포로 변경하려면 Apple 지원 문서 볼륨 구매를 통해 교환 코드에서 관리형 배포로 마이그레이션을 참조하십시오.

iOS 볼륨 구매에 대한 자세한 내용은 `<https://volume.itunes.apple.com/us/store>`을 참조하십시오. 볼륨 구매에 등록하려면 `<https://deploy.apple.com/qforms/open/register/index/avs>`로 이동하십시오. iTunes에서 볼륨 구매 스토어에 액세스하려면 `<https://volume.itunes.apple.com/?l=en>`로 이동하십시오.

XenMobile에서 이러한 iOS 볼륨 구매 설정을 저장하면 구매한 앱이 XenMobile 콘솔의 **구성 > 앱** 페이지에 나타납니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **볼륨 구매**를 클릭합니다. **볼륨 구매** 구성 페이지가 나타납니다.



3. 다음 설정을 구성합니다:

   - **Secure Hub에 사용자 암호 저장:** XenMobile 인증을 위해 Secure Hub에 사용자 이름과 암호를 저장할지 여부를 선택합니다. 기본적으로 이 보안 방법을 사용하여 정보를 저장합니다.
   - **볼륨 구매 국가 매핑을 위한 사용자 속성:** 사용자가 국가별 앱 스토어에서 앱을 다운로드할 수 있도록 코드를 입력합니다.

   XenMobile은 이 매핑을 사용하여 볼륨 구매의 속성 풀을 선택합니다. 예를 들어, 사용자 속성이 미국인 경우 볼륨 구매 코드가 영국용이면 해당 사용자는 앱을 다운로드할 수 없습니다. 국가 매핑 코드에 대한 자세한 내용은 볼륨 구매 계획 관리자에게 문의하십시오.

4. 추가하려는 각 볼륨 구매 계정에 대해 **추가**를 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 > 앱**으로 이동하여 플랫폼 페이지로 이동한 다음 **볼륨 구매**를 확장합니다.

   - **이름:** 볼륨 구매 계정 이름을 입력합니다.
   - **접미사:** 볼륨 구매 계정을 통해 얻은 앱 이름과 함께 표시될 접미사를 입력합니다. 예를 들어, **VP**를 입력하면 Secure Mail 앱이 앱 목록에 **Secure Mail - VP**로 표시됩니다.
   - **회사 토큰:** Apple에서 얻은 볼륨 구매 서비스 토큰을 복사하여 붙여넣습니다. 토큰을 얻으려면: Apple 볼륨 구매 포털의 **계정 요약** 페이지에서 **다운로드** 버튼을 클릭하여 볼륨 구매 파일을 생성하고 다운로드합니다. 이 파일에는 서비스 토큰과 국가 코드, 만료일과 같은 기타 정보가 포함되어 있습니다. 파일을 안전한 위치에 저장하십시오.
   - **사용자 로그인:** 사용자 지정 B2B 앱을 가져오는 데 사용되는 선택적 승인된 볼륨 구매 계정 관리자 이름을 입력합니다.
   - **사용자 암호:** 볼륨 구매 계정 관리자 암호를 입력합니다.
   - **앱 자동 업데이트: 켜짐**인 경우, Apple Store에 업데이트가 있으면 볼륨 구매 앱이 자동으로 업데이트됩니다. 기본값은 **꺼짐**입니다.

6. **저장**을 클릭하여 대화 상자를 닫습니다.
7. **저장**을 클릭하여 볼륨 구매 구성을 저장합니다.

   XenMobile이 **구성 > 앱** 페이지의 목록에 앱을 추가한다는 메시지가 나타납니다. 해당 페이지에서 볼륨 구매 계정의 앱 이름에 이전 구성에서 제공한 접미사가 포함되어 있음을 확인하십시오.

이제 볼륨 구매 앱 설정을 구성한 다음 볼륨 구매 앱에 대한 배달 그룹 및 장치 정책 설정을 조정할 수 있습니다. 이러한 구성을 완료하면 사용자가 장치를 등록할 수 있습니다. 다음 참고 사항은 해당 프로세스에 대한 고려 사항을 제공합니다.

- 볼륨 구매 앱 설정을 구성할 때 (**구성 > 앱**), **장치에 라이선스 연결 강제 적용**을 사용하도록 설정합니다.

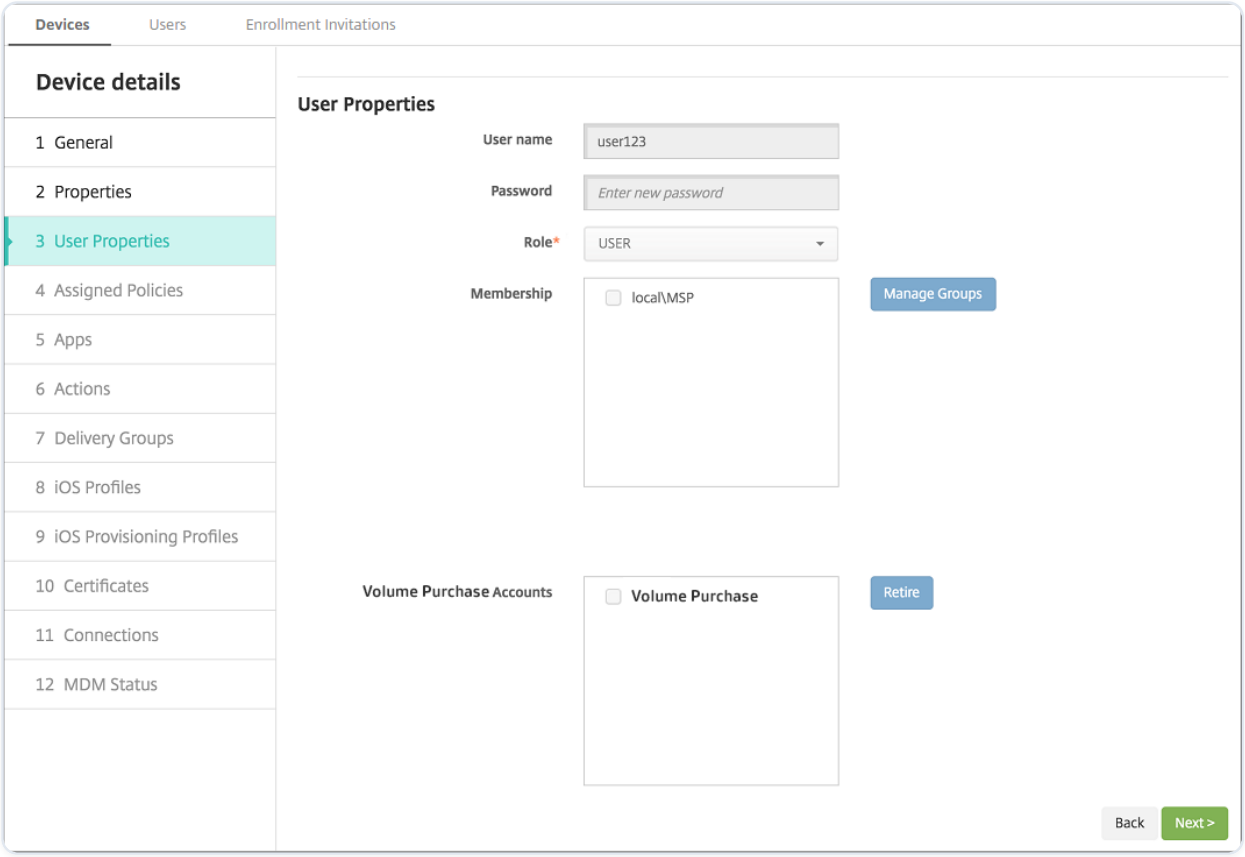
  감독되는 장치에서 Apple 볼륨 구매 및 배포 프로그램을 사용하는 이점은 XenMobile을 사용하여 앱을 사용자 수준이 아닌 장치 수준에서 할당할 수 있다는 것입니다. 결과적으로 Apple ID 장치를 사용할 필요

가 없습니다. 또한 사용자는 Apple 볼륨 구매에 참여하라는 초대를 받지 않습니다. 사용자는 iTunes 계정에 로그인하지 않고도 앱을 다운로드할 수 있습니다.

해당 앱의 볼륨 구매 정보를 보려면 **볼륨 구매**를 확장합니다. **볼륨 구매 라이선스 키** 테이블에서 라이선스가 장치와 연결되어 있음을 확인하십시오. 사용자가 토큰을 제거한 다음 다시 가져오면 Apple 개인 정보 보호 제한 때문에 일련 번호 대신 **숨김**이라는 단어가 나타납니다.

라이선스를 연결 해제하려면 라이선스 행을 클릭한 다음 **연결 해제**를 클릭합니다.

볼륨 구매 라이선스를 사용자와 연결하는 경우 XenMobile은 사용자를 볼륨 구매 계정에 통합합니다. 또한 사용자의 iTunes ID를 볼륨 구매 계정과 연결합니다. 사용자의 iTunes ID는 회사나 XenMobile Server에 절대 표시되지 않습니다. Apple은 사용자 개인 정보를 보호하기 위해 투명하게 연결을 생성합니다. Apple 볼륨 구매에서 사용자를 은퇴시켜 사용자 계정에서 모든 라이선스를 연결 해제할 수 있습니다. 사용자를 은퇴시키려면 **관리 > 장치**로 이동합니다.



- 앱을 배달 그룹에 할당할 때 기본적으로 XenMobile은 해당 앱을 선택적 앱으로 식별합니다. XenMobile이 장치에 앱을 배포하도록 하려면 **구성** > **배달 그룹**으로 이동합니다. **앱** 페이지에서 앱을 **필수 앱** 목록으로 이동합니다.

- 앱에 대한 업데이트를 사용할 수 있는 경우, 볼륨 구매는 해당 앱으로 업데이트를 푸시하고 장치에서 앱을 자동으로 업데이트합니다. 자세한 내용은 앱 업데이트 확인을 참조하십시오.

  Apple 볼륨 구매가 만료되면 XenMobile에 라이선스 만료 경고가 표시됩니다.

앱 업데이트 확인

볼륨 구매 계정을 추가할 때 **앱 자동 업데이트** 설정을 켜면 XenMobile Server는 볼륨 구매 앱(필수 앱) 및 Citrix Secure Hub 스토어에서 구독한 선택적 앱의 새 버전을 주기적으로 확인하고 업데이트합니다. XenMobile Server가 필수 앱의 새 버전을 받으면 수동으로 업데이트하라는 메시지를 표시하지 않고 자동으로 설치를 위해 장치로 새 버전을 푸시합니다. 그러나 선택적 앱을 자동 업데이트하려면 속성 `apple.ios.optional_app_update`을 **True**로 설정해야 합니다. 그렇지 않으면 선택적 앱을 수동으로 업데이트해야 합니다. 자세한 내용은 서버 속성을 참조하십시오.

앱의 새 버전을 수동으로 확인하고 업데이트하려면 다음 단계를 수행하십시오.

1. **구성** > **앱**을 클릭합니다.

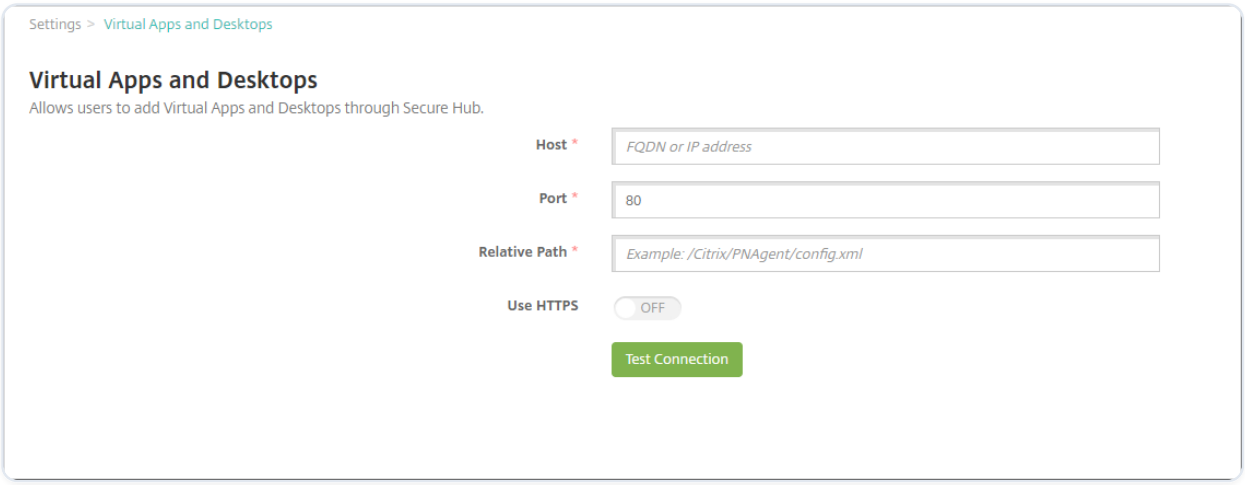
   앱 페이지가 나타납니다.
2. 앱을 선택하고 **편집**을 클릭합니다.
3. **플랫폼** 페이지로 이동한 다음 **버전** 옆에 있는 **업데이트 확인** 버튼을 클릭합니다.
4. **업데이트** 대화 상자에서 새 버전이 있는 경우 업데이트를 적용합니다.

Citrix Secure Hub™를 통한 가상 앱 및 데스크톱

XenMobile은 Virtual Apps and Desktops에서 앱을 수집하여 XenMobile Store에서 모바일 장치 사용자에게 제공할 수 있습니다. 사용자는 XenMobile Store 내에서 직접 앱을 구독하고 Secure Hub에서 앱을 실행합니다. 앱을 실행하려면 사용자 장치에 Citrix Receiver™가 설치되어 있어야 하지만, 구성할 필요는 없습니다.

이 설정을 구성하려면 Web Interface 사이트 또는 StoreFront에 대한 정규화된 도메인 이름(FQDN) 또는 IP 주소와 포트 번호가 필요합니다.

1. XenMobile® 웹 콘솔에서 오른쪽 상단 모서리에 있는 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 사이트 또는 StoreFront의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력합니다.
   - **포트:** Web Interface 사이트 또는 StoreFront의 포트 번호를 입력합니다. 기본값은 80입니다.
   - **상대 경로:** 경로를 입력합니다. 예: /Citrix/PNAgent/config.xml
   - **HTTPS 사용:** Web Interface 사이트 또는 StoreFront와 클라이언트 장치 간에 보안 인증을 활성화할지 여부를 선택합니다. 기본값은 **OFF**입니다.

4. **연결 테스트**를 클릭하여 XenMobile이 지정된 Virtual Apps and Desktops 서버에 연결할 수 있는지 확인합니다.
5. **저장**을 클릭합니다.

ShareFile을 XenMobile®과 함께 사용

> **면책 조항:**

> ShareFile(현재 Progress)이 지원을 중단하면 이 기능은 더 이상 사용되지 않습니다.

> XenMobile은 ShareFile과 통합하기 위한 두 가지 옵션인 Citrix Files 및 스토리지 영역 커넥터를 제공합니다. Citrix Files 또는 스토리지 영역 커넥터와의 통합에는 XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management™(클라우드)가 필요합니다.

시트릭스 파일

XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드)를 사용하는 경우 XenMobile을 구성하여 Citrix Files 계정에 대한 액세스를 제공할 수 있습니다. 해당 구성은 다음과 같습니다.

- 파일 공유, 파일 동기화 및 스토리지 영역 커넥터와 같은 전체 엔터프라이즈 기능 세트에 모바일 사용자가 액세스할 수 있도록 합니다.
- XenMobile 앱 사용자의 단일 Sign-On 인증 및 포괄적인 액세스 제어 정책을 Citrix Files에 제공할 수 있습니다.
- XenMobile 콘솔을 통해 Citrix Files 구성, 서비스 수준 모니터링 및 라이선스 사용량 모니터링을 제공합니다.

Citrix Files용 XenMobile 구성에 대한 자세한 내용은 Citrix Files를 사용한 단일 Sign-On용 SAML을 참조하십시오.

스토리지 영역 커넥터

XenMobile 콘솔을 통해 생성하는 스토리지 영역 커넥터에만 XenMobile이 액세스를 제공하도록 구성할 수 있습니다. 해당 구성은 다음과 같습니다.

- SharePoint 사이트 및 네트워크 파일 공유와 같은 기존 온프레미스 스토리지 리포지토리에 대한 보안 모바일 액세스를 제공합니다.
- ShareFile 하위 도메인을 설정하거나 Citrix Files 데이터를 호스팅할 필요가 없습니다.
- iOS 및 Android용 Citrix Files 모바일 생산성 앱을 통해 데이터에 대한 모바일 액세스를 제공합니다. Microsoft Office 문서를 편집할 수 있습니다. 또한 모바일 장치에서 Adobe PDF 파일을 미리 보고 주석을 달 수 있습니다.
- 회사 네트워크 외부로 사용자 정보가 유출되는 것을 방지하는 보안 제한 사항을 준수합니다.
- XenMobile 콘솔을 통해 스토리지 영역 커넥터의 간편한 설정을 제공합니다. 나중에 XenMobile과 함께 Citrix Files의 모든 기능을 사용하기로 결정하는 경우, XenMobile 콘솔에서 구성을 변경할 수 있습니다.
- XenMobile Advanced Edition (온프레미스) 또는 Citrix Endpoint Management (클라우드)가 필요합니다.

스토리지 영역 커넥터만 사용하는 XenMobile 통합의 경우:

- ShareFile은 Citrix Gateway에 대한 단일 Sign-On 구성을 사용하여 스토리지 영역 컨트롤러로 인증합니다.
- Citrix Files 제어 평면이 사용되지 않으므로 XenMobile은 SAML을 통해 인증하지 않습니다.

다음 다이어그램은 스토리지 영역 커넥터와 함께 XenMobile을 사용하는 경우의 상위 수준 아키텍처를 보여줍니다.

스토리지 영역 컨트롤러(/en-us/xenmobile/server/media/storagezone-controller-with-xenmobile-architecture.png)

요구 사항

- 최소 구성 요소 버전:
  - XenMobile Server 10.5 (온프레미스)
  - iOS용 ShareFile (MDX) 5.3
  - Android용 쉐어파일 (MDX) 5.3
  - 스토리지 영역 컨트롤러 5.0

    이 문서에서는 스토리지 영역 컨트롤러 5.0을 구성하는 방법에 대한 지침을 제공합니다.
- 스토리지 영역 컨트롤러를 실행할 서버가 시스템 요구 사항을 충족하는지 확인합니다. 요구 사항은 시스템 요구 사항을 참조하십시오.

Citrix Files 데이터용 스토리지 영역 및 제한된 스토리지 영역에 대한 요구 사항은 스토리지 영역 커넥터만 사용하는 XenMobile 통합에는 적용되지 않습니다.

XenMobile은 Documentum 커넥터를 지원하지 않습니다.

- PowerShell 스크립트를 실행하려면 다음을 수행합니다.
  - PowerShell의 32비트(x86) 버전에서 스크립트를 실행합니다.

설치 작업

스토리지 영역 컨트롤러를 설치하고 설정하려면 제시된 순서대로 다음 작업을 완료하십시오. 이 단계는 스토리지 영역 커넥터만 사용하는 XenMobile 통합에만 해당됩니다. 이 문서 중 일부는 스토리지 영역 컨트롤러 설명서에 있습니다.

1. 스토리지 영역 컨트롤러용 Citrix ADC 구성

   Citrix ADC를 스토리지 영역 컨트롤러의 DMZ 프록시로 사용할 수 있습니다.
2. SSL 인증서 설치

   표준 영역을 호스팅하는 스토리지 영역 컨트롤러에는 SSL 인증서가 필요합니다. 제한된 영역을 호스팅하고 내부 주소를 사용하는 스토리지 영역 컨트롤러에는 SSL 인증서가 필요하지 않습니다.
3. 서버 준비

스토리지 영역 커넥터에는 IIS 및 ASP.NET 설정이 필요합니다.

4. 스토리지 영역 컨트롤러 설치
5. 스토리지 영역 커넥터 전용으로 스토리지 영역 컨트롤러 준비
6. 스토리지 영역에 대한 프록시 서버 지정(/ko-kr/storagezones-controller/5-0/install/specify-proxy.html)

   스토리지 영역 컨트롤러 콘솔을 사용하면 스토리지 영역 컨트롤러에 대한 프록시 서버를 지정할 수 있습니다. 다른 방법을 사용하여 프록시 서버를 지정할 수도 있습니다.
7. 위임을 위해 도메인 컨트롤러가 스토리지 영역 컨트롤러를 신뢰하도록 구성(/ko-kr/storagezones-controller/5-0/install/configure-domain-controller.html)

   네트워크 공유 또는 SharePoint 사이트에서 NTLM 또는 Kerberos 인증을 지원하도록 도메인 컨트롤러를 구성합니다.
8. 보조 스토리지 영역 컨트롤러를 스토리지 영역에 연결(#join-a-secondary-storage-zones-controller-to-a-storage-zone)

   고가용성을 위해 스토리지 영역을 구성하려면 최소 두 개의 스토리지 영역 컨트롤러를 연결합니다.

스토리지 영역 컨트롤러 설치

1. 스토리지 영역 컨트롤러 소프트웨어 다운로드 및 설치:

   a. `<https://www.citrix.com/downloads>`으로 이동합니다. **ShareFile**을 검색한 다음 최신 스토리지 영역 컨트롤러 설치 관리자를 다운로드합니다.

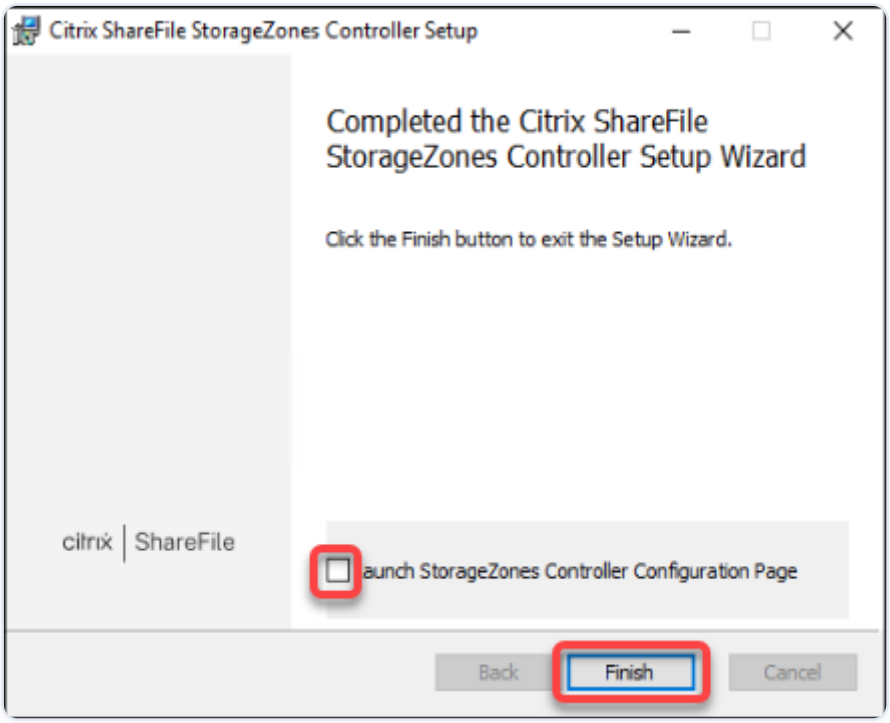
   b. 스토리지 영역 컨트롤러를 설치하면 서버의 기본 웹 사이트가 컨트롤러의 설치 경로로 변경됩니다. 기본 웹 사이트에서 **익명 인증**을 사용하도록 설정합니다.

2. 스토리지 영역 컨트롤러를 설치하려는 서버에서 StorageCenter.msi를 실행합니다.

   스토리지 영역 컨트롤러 설치 마법사가 시작됩니다.

3. 프롬프트에 응답합니다:

   - **대상 폴더** 페이지에서 IIS(Internet Information Services)가 기본 위치에 설치된 경우 기본값을 그대로 둡니다. 그렇지 않은 경우 IIS 설치 위치를 찾습니다.
   - 설치가 완료되면 **스토리지 영역 컨트롤러 구성 페이지 시작** 확인란을 선택 취소한 다음 **마침**을 클릭합니다.



4. 메시지가 표시되면 스토리지 영역 컨트롤러를 다시 시작합니다.
5. 설치가 성공했는지 테스트하려면 `https://localhost/` (으)로 이동합니다. 설치가 성공하면 Citrix Files 로고가 나타납니다.

   Citrix Files 로고가 나타나지 않으면 브라우저 캐시를 지우고 다시 시도하십시오.

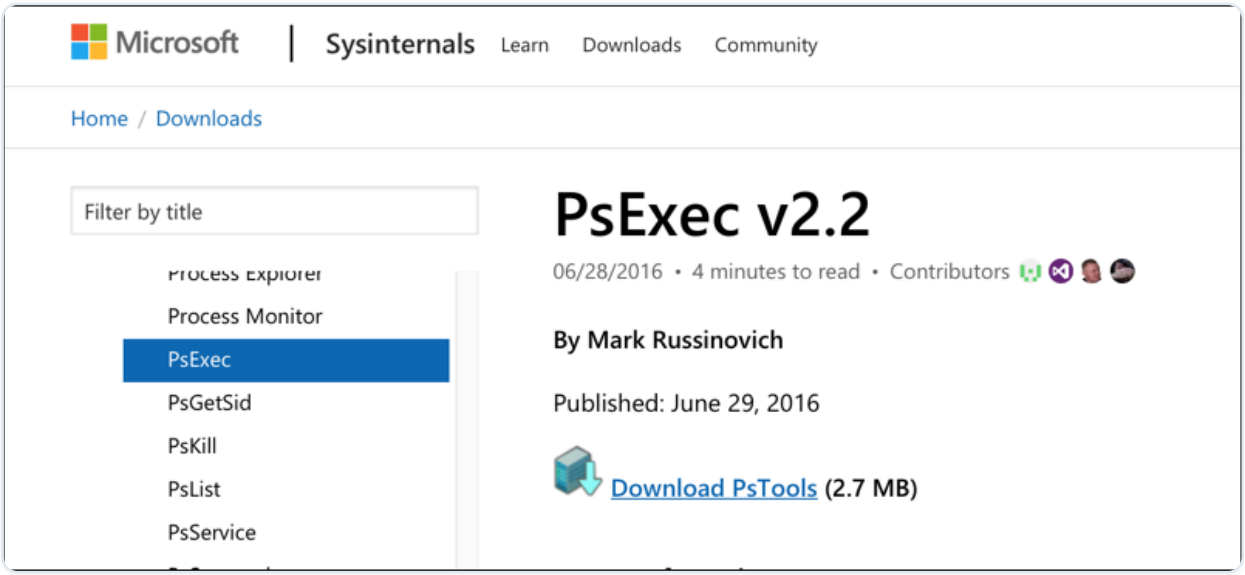
> **중요:**
>
> 스토리지 영역 컨트롤러를 복제할 계획이라면 스토리지 영역 컨트롤러 구성을 계속하기 전에 디스크 이미지를 캡처하십시오.

스토리지 영역 커넥터 전용으로 스토리지 영역 컨트롤러 준비

스토리지 영역 커넥터만 통합하는 경우 스토리지 영역 컨트롤러 관리 콘솔을 사용하지 않습니다. 해당 인터페이스에는 이 솔루션에 필요하지 않은 Citrix Files 관리자 계정이 필요합니다. 결과적으로 Citrix Files 제어 평면 없이 사용할 수 있도록 스토리지 영역 컨트롤러를 준비하는 PowerShell 스크립트를 실행합니다. 이 스크립트는 다음을 수행합니다.

- 현재 스토리지 영역 컨트롤러를 기본 스토리지 영역 컨트롤러로 등록합니다. 나중에 보조 스토리지 영역 컨트롤러를 기본 컨트롤러에 연결할 수 있습니다.
- 영역을 생성하고 암호를 설정합니다.

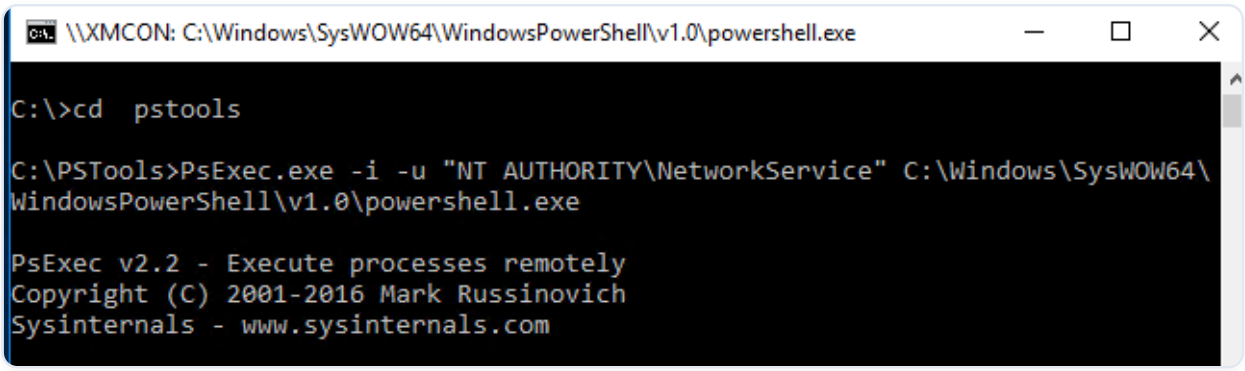
1. 스토리지 영역 컨트롤러 서버에서 PsExec 도구를 다운로드합니다. Microsoft Windows Sysinternals(으)로 이동한 다음 **PsTools 다운로드**를 클릭합니다. 도구를 C 드라이브의 루트에 압축 해제합니다.



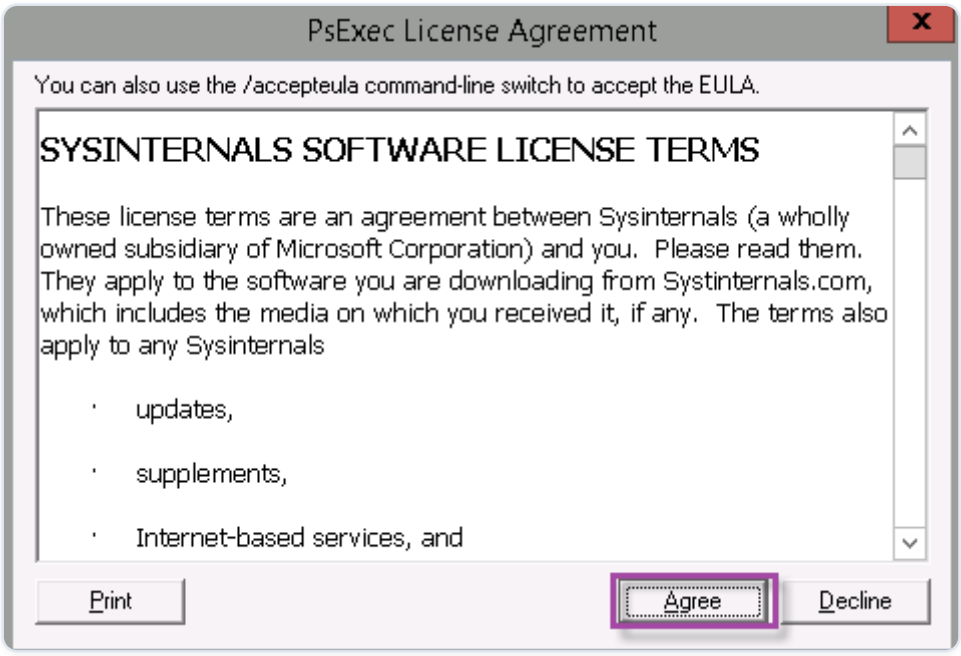
2. PsExec 도구 실행: 관리자 사용자로 명령 프롬프트를 연 다음 다음을 입력합니다.

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. 메시지가 표시되면 **동의**를 클릭하여 Sysinternals 도구를 실행합니다.



PowerShell 창이 열립니다.

4. PowerShell 창에서 다음을 입력합니다.

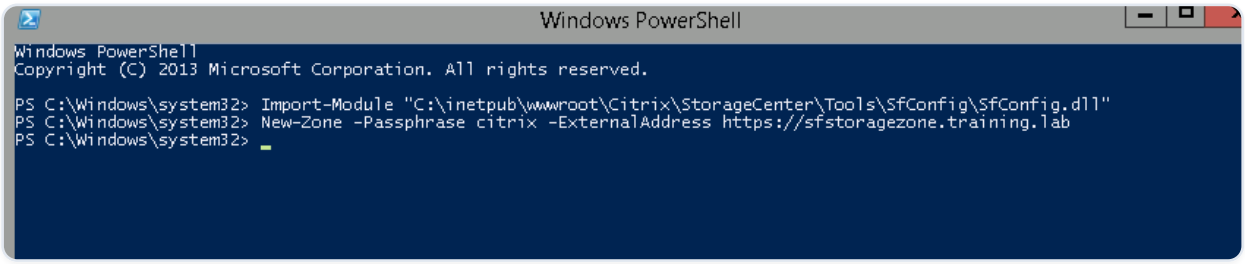
```
Import-Module "C:
\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

여기서:

암호: 사이트에 할당하려는 암호입니다. 컨트롤러에서 암호를 복구할 수 없으므로 기록해 두십시오. 암호를 잃어버리면 스토리지 영역 컨트롤러를 다시 설치할 수 없습니다. 서버에 오류가 발생하면 더 많은 스토리지 영역 컨트롤러를 스토리지 영역에 연결하거나 스토리지 영역을 복구하십시오.

ExternalAddress: 스토리지 영역 컨트롤러 서버의 외부 정규화된 도메인 이름입니다.



기본 스토리지 영역 컨트롤러가 이제 준비되었습니다.

스토리지 영역 커넥터를 생성하기 위해 XenMobile에 로그인하기 전에: 해당하는 경우 다음 구성을 완료하십시오.

스토리지 영역에 대한 프록시 서버 지정

위임을 위해 도메인 컨트롤러가 스토리지 영역 컨트롤러를 신뢰하도록 구성

보조 스토리지 영역 컨트롤러를 스토리지 영역에 연결

스토리지 영역 커넥터를 생성하려면 XenMobile에서 스토리지 영역 컨트롤러 연결 정의를 참조하십시오.

보조 스토리지 영역 컨트롤러를 스토리지 영역에 연결

고가용성을 위해 스토리지 영역을 구성하려면 최소 두 개의 스토리지 영역 컨트롤러를 연결하십시오. 보조 스토리지 영역 컨트롤러를 영역에 연결하려면 두 번째 서버에 스토리지 영역 컨트롤러를 설치하십시오. 그런 다음 해당 컨트롤러를 기본 컨트롤러의 영역에 연결하십시오.

1. 기본 서버에 연결하려는 스토리지 영역 컨트롤러 서버에서 PowerShell 창을 엽니다.
2. PowerShell 창에 다음을 입력합니다.

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

   예시:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

XenMobile에서 스토리지 영역 컨트롤러 연결 정의

스토리지 영역 커넥터를 추가하기 전에 스토리지 영역 커넥터에 대해 활성화된 각 스토리지 영역 컨트롤러의 연결 정보를 구성합니다. 이 섹션에 설명된 대로 또는 커넥터를 추가할 때 스토리지 영역 컨트롤러를 정의할 수 있습니다.

구성 > ShareFile 페이지를 처음 방문하면 이 페이지에 엔터프라이즈 계정에 XenMobile을 사용하는 것과 스토리지 영역 커넥터를 사용하는 것의 차이점이 요약되어 있습니다.

ShareFile 구성(/en-us/xenmobile/server/media/configure-sharefile-first-time-use.png)

이 문서의 구성 단계를 계속하려면 **커넥터 구성**을 클릭합니다.

ShareFile 구성(/en-us/xenmobile/server/media/configure-sharefile-storagezone-connectors-no-list.png)

1. **구성 > ShareFile**에서 **스토리지 영역 관리**를 클릭합니다.

   ShareFile 구성(/en-us/xenmobile/server/media/configure-sharefile-storagezone-connectors-empty.png)
2. **스토리지 영역 관리**에서 연결 정보를 추가합니다.

ShareFile 구성(/en-us/xenmobile/server/media/configure-sharefile-manage-storagezones-add-new.png)

- **이름:** XenMobile에서 StorageZone을 식별하는 데 사용되는 StorageZone에 대한 설명 이름입니다. 이름에 공백이나 특수 문자를 포함하지 마십시오.
- **FQDN 및 포트:** XenMobile Server에서 연결할 수 있는 스토리지 영역 컨트롤러의 정규화된 도메인 이름 및 포트 번호입니다.
- **보안 연결:** 스토리지 영역 컨트롤러에 대한 연결에 SSL을 사용하는 경우 기본 설정인 ON을 사용합니다. 연결에 SSL을 사용하지 않는 경우 이 설정을 OFF로 변경합니다.
- **관리자 사용자 이름** 및 **관리자 암호:** 관리자 서비스 계정 사용자 이름(도메인\\관리자 형식) 및 암호입니다. 또는 스토리지 영역 컨트롤러에 대한 읽기 및 쓰기 권한이 있는 사용자 계정입니다.

3. **저장**을 클릭합니다.
4. 연결을 테스트하려면 XenMobile Server가 포트 443에서 스토리지 영역 컨트롤러의 정규화된 도메인 이름에 연결할 수 있는지 확인합니다.
5. 다른 스토리지 영역 컨트롤러 연결을 정의하려면 **스토리지 영역 관리**에서 **추가** 버튼을 클릭합니다.

   스토리지 영역 컨트롤러 연결 정보를 편집하거나 삭제하려면 **스토리지 영역 관리**에서 연결 이름을 선택합니다. 그런 다음 **편집** 또는 **삭제**를 클릭합니다.

XenMobile에서 스토리지 영역 커넥터 추가

1. **구성 > ShareFile**로 이동한 다음 **추가**를 클릭합니다.

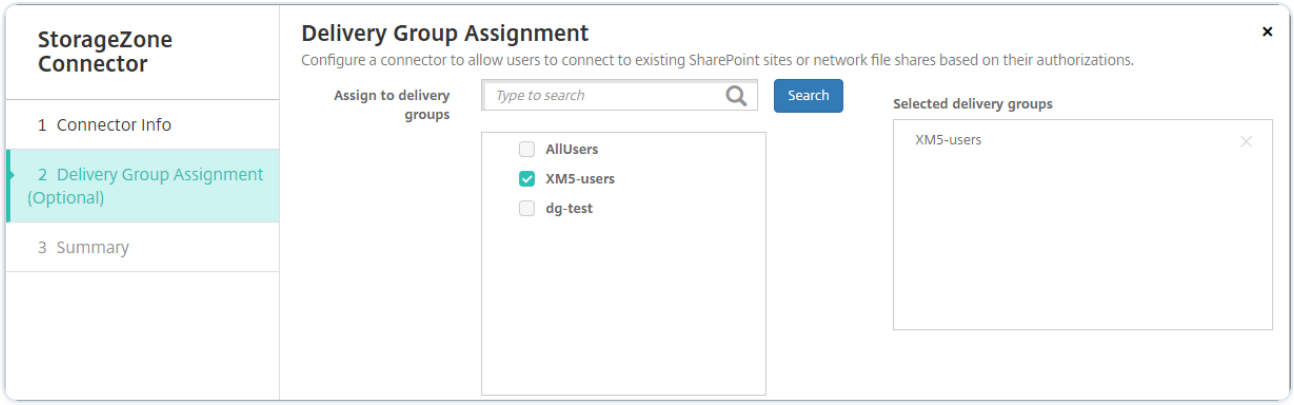
   ShareFile 구성(/en-us/xenmobile/server/media/configure-sharefile-storagezone-connectors-no-list.png)
2. **커넥터 정보** 페이지에서 다음 설정을 구성합니다.

   ShareFile 구성(/en-us/xenmobile/server/media/configure-sharefile-add-storagezone-connector.png)

   - **커넥터 이름:** XenMobile에서 스토리지 영역 커넥터를 식별하는 이름입니다.
   - **설명:** 이 커넥터에 대한 선택적 메모입니다.
   - **유형: SharePoint** 또는 **네트워크**를 선택합니다.
   - **StorageZone:** 커넥터와 연결된 스토리지 영역을 선택합니다. 스토리지 영역이 목록에 없으면 **StorageZones 관리**를 클릭하여 스토리지 영역 컨트롤러를 정의합니다.
   - **위치:** SharePoint의 경우 SharePoint 루트 수준 사이트, 사이트 모음 또는 문서 라이브러리의 URL을 `https://sharepoint.company.com` 형식으로 지정합니다. 네트워크 공유의 경우

UNC(Uniform Naming Convention) 경로의 정규화된 도메인 이름을 \\\\server\\share 형식으로 지정합니다.

3. **전송 그룹 할당** 페이지에서 선택적으로 커넥터를 전송 그룹에 할당합니다. 또는 **구성 > 전송 그룹**을 사용하여 커넥터를 전송 그룹에 연결할 수 있습니다.



1. **요약** 페이지에서 구성한 옵션을 검토할 수 있습니다. 구성을 조정하려면 **뒤로**를 클릭합니다.
2. **저장**을 클릭하여 커넥터를 저장합니다.
3. 커넥터 테스트:

   a. Citrix Files 클라이언트를 래핑할 때 다음을 수행합니다.

      - 네트워크 액세스 정책을 **내부 네트워크로 터널링됨**으로 설정합니다.

      이 작동 모드에서 XenMobile MDX 프레임워크는 Citrix Files 클라이언트의 모든 네트워크 트래픽을 가로챕니다. 트래픽은 앱별 마이크로 VPN을 사용하여 Citrix Gateway를 통해 리디렉션됩니다.

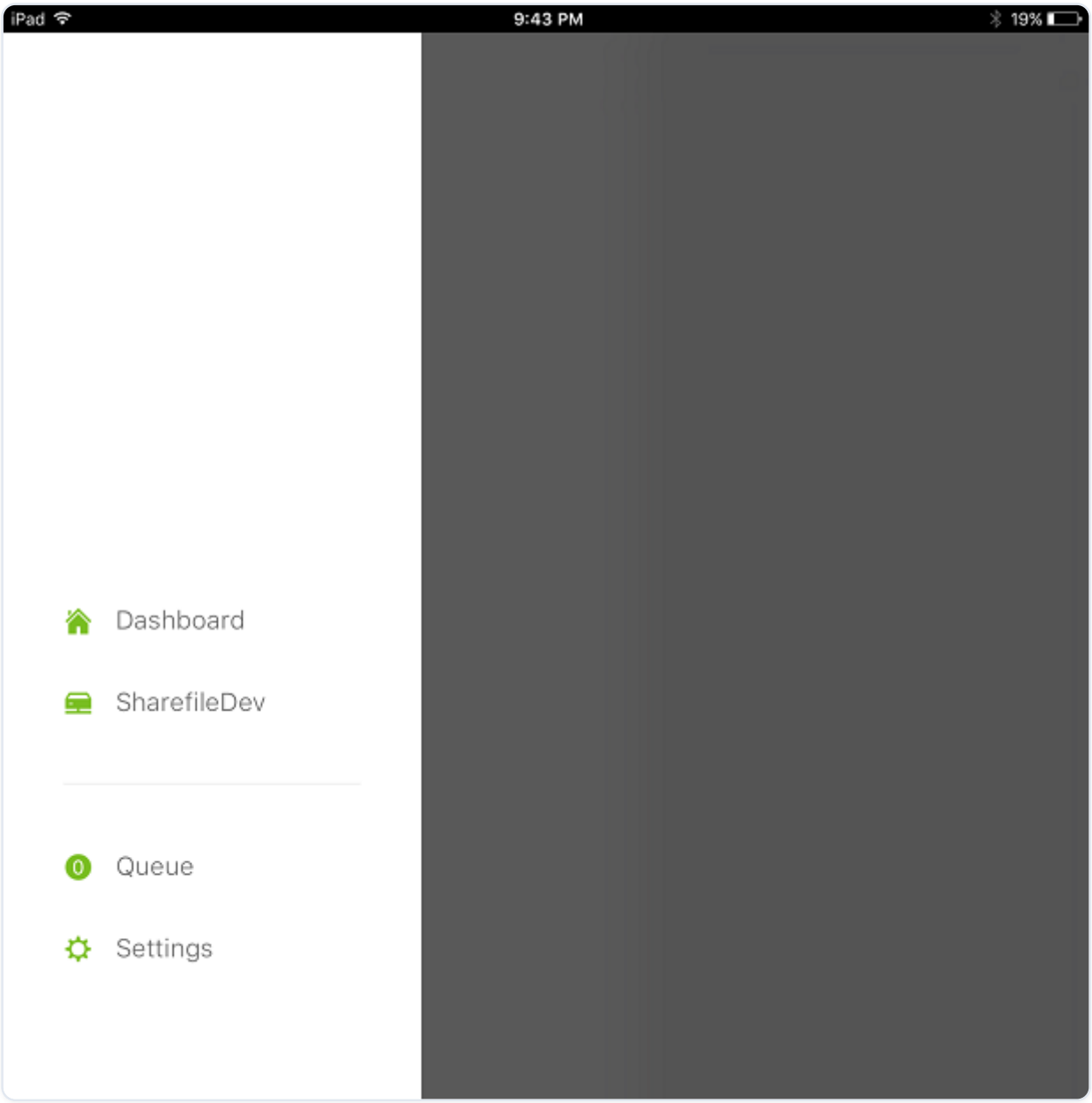
      - 기본 VPN 모드 정책을 **터널링됨 - 웹 SSO**로 설정합니다.

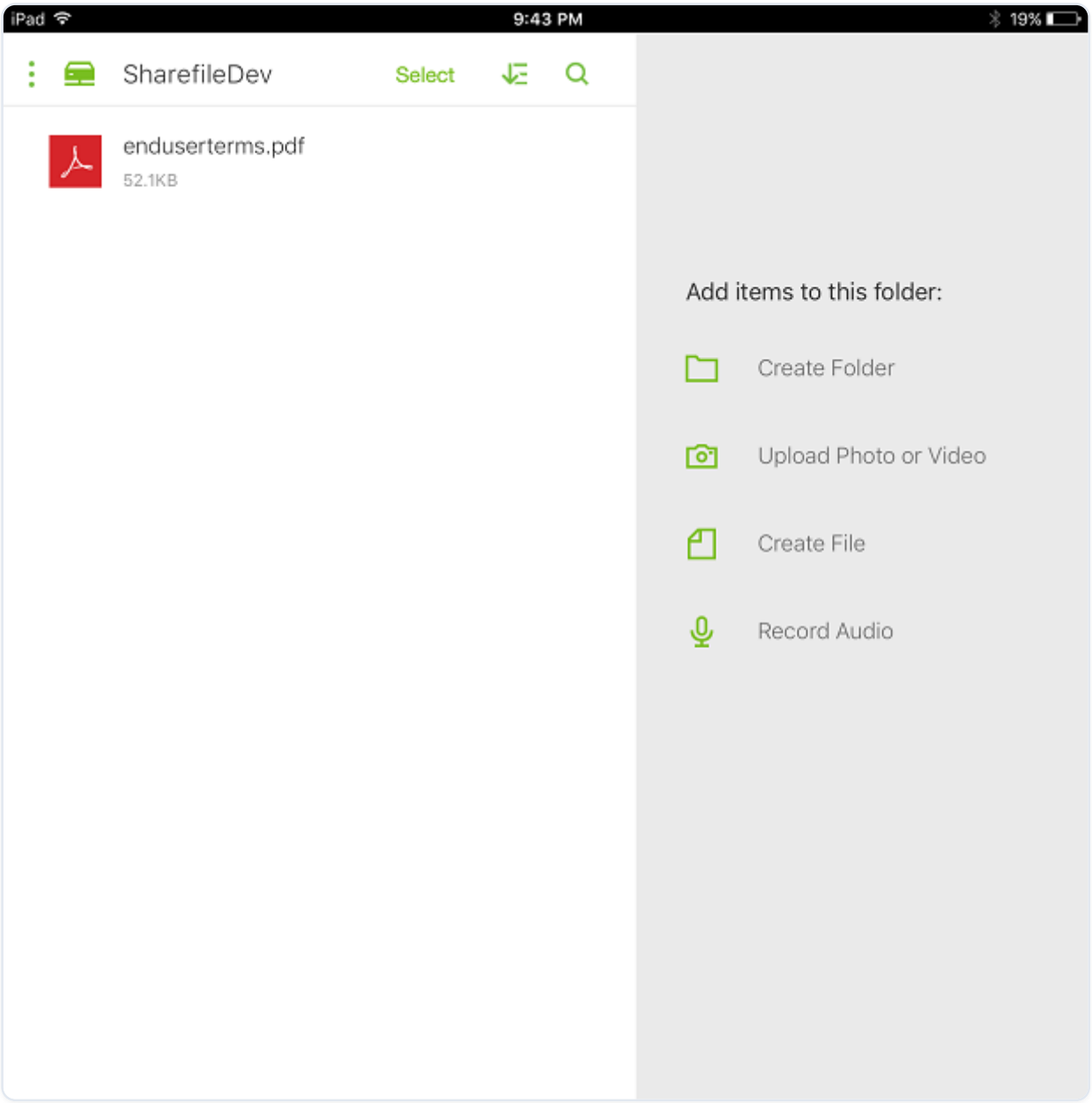
      이 터널링 모드에서 MDX 프레임워크는 MDX 앱의 SSL/HTTP 트래픽을 종료합니다. 그런 다음 MDX는 사용자를 대신하여 내부 연결에 대한 새 연결을 시작합니다. 이 정책 설정은 MDX 프레임워크가 웹 서버에서 발행한 인증 문제를 감지하고 응답할 수 있도록 합니다.

   b. Citrix Files 클라이언트를 XenMobile에 추가합니다. 자세한 내용은 Endpoint Management 클라이언트용 Citrix Files 통합 및 제공을 참조하십시오.

   c. 지원되는 장치에서 Citrix Files 및 커넥터에 대한 단일 Sign-On을 확인합니다.

다음 샘플에서 SharefileDev는 커넥터의 이름입니다.

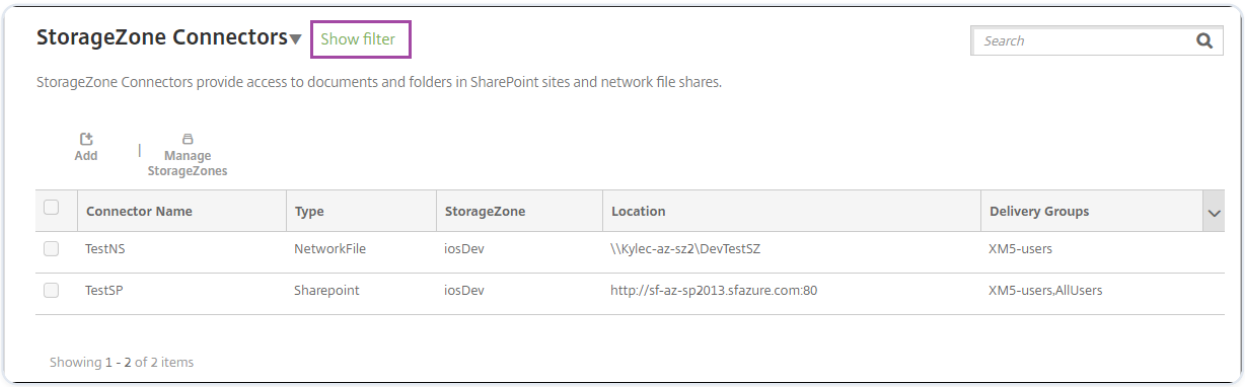

iPad
9:43 PM
19%
Dashboard
SharefileDev
0
Queue
Settings



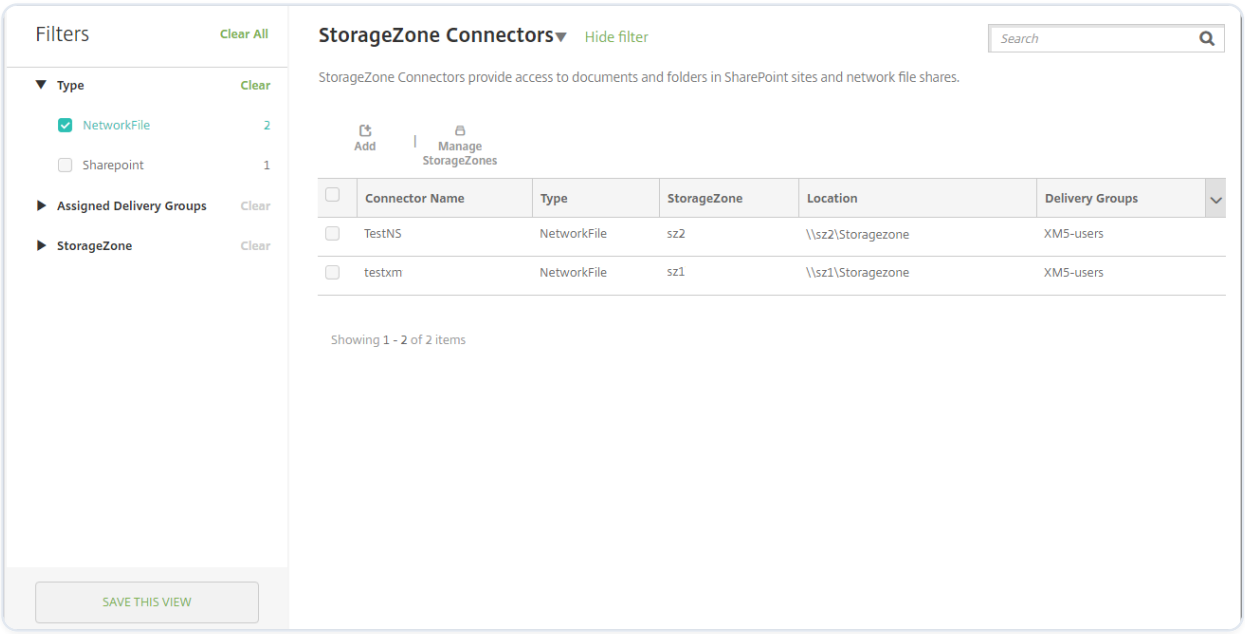
스토리지 영역 커넥터 목록 필터링

커넥터 유형, 할당된 전송 그룹 및 스토리지 영역별로 스토리지 영역 커넥터 목록을 필터링할 수 있습니다.

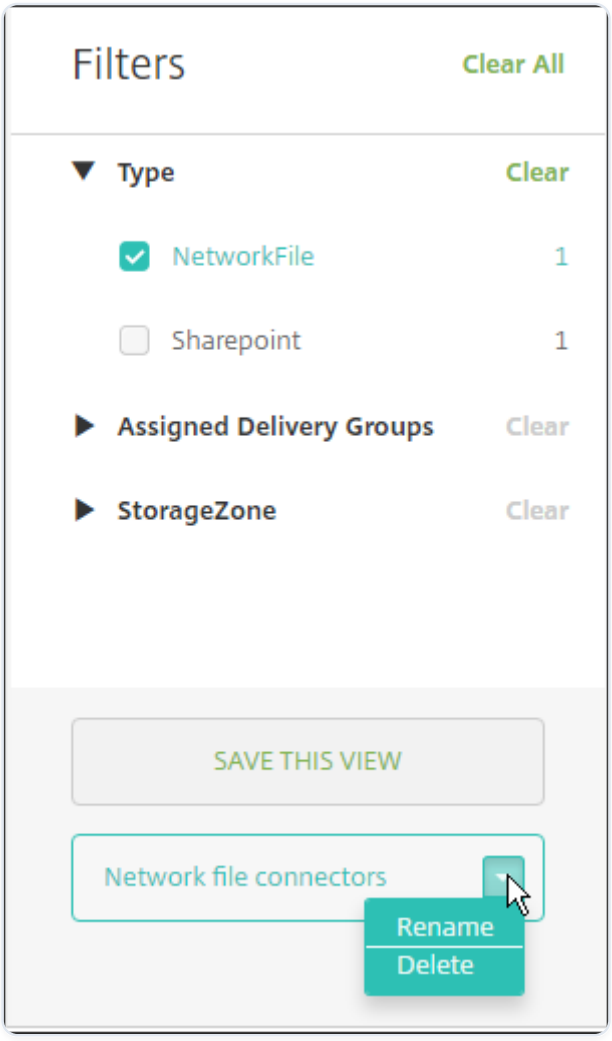
1. **구성 > ShareFile**로 이동한 다음 **필터 표시**를 클릭합니다.



2. 필터 제목을 확장하여 선택합니다. 필터를 저장하려면 **이 보기 저장**을 클릭하고 필터 이름을 입력한 다음 **저장**을 클릭합니다.



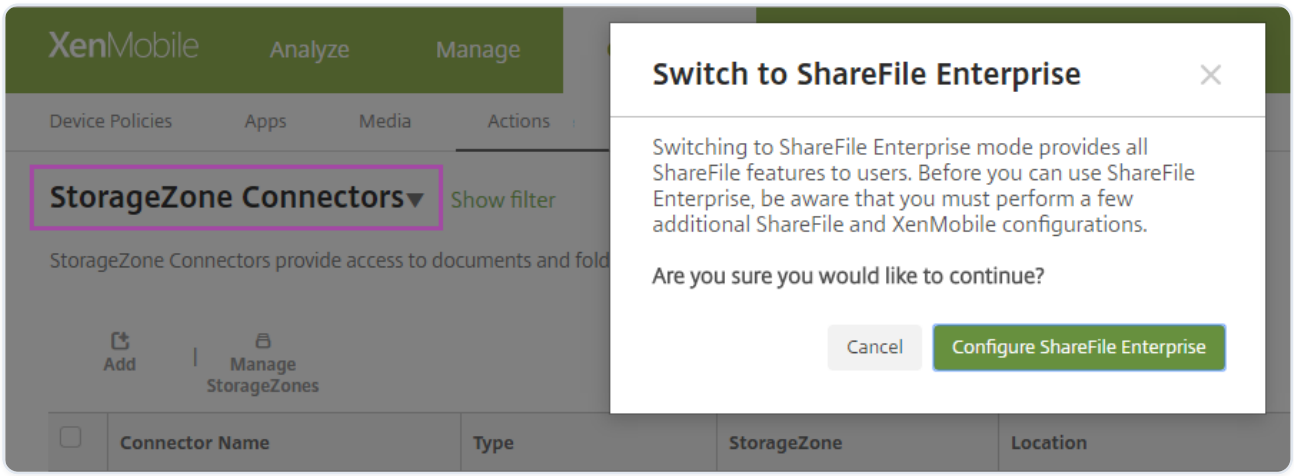
3. 필터 이름을 바꾸거나 삭제하려면 필터 이름 옆의 화살표 아이콘을 클릭합니다.



Citrix Files로 전환

스토리지 영역 커넥터를 XenMobile과 통합한 후 나중에 전체 Enterprise 기능 세트로 전환할 수 있습니다. Citrix Files 기능 세트를 사용하려면 XenMobile Advanced Edition(온프레미스) 또는 Citrix Endpoint Management(클라우드)가 필요합니다. XenMobile은 기존 스토리지 영역 커넥터 통합 설정을 유지합니다.

구성 > ShareFile로 이동하여 **스토리지 영역 커넥터** 드롭다운 메뉴를 클릭한 다음 **ShareFile Enterprise 구성**을 클릭합니다.



Citrix Files 구성에 대한 자세한 내용은 Citrix Files를 사용한 단일 Sign-On용 SAML을(를) 참조하십시오.

HDX™ 앱용 SmartAccess

이 기능은 장치 속성, 장치의 사용자 속성 또는 장치에 설치된 애플리케이션을 기반으로 HDX 앱에 대한 액세스를 제어할 수 있도록 합니다. 이 기능을 사용하려면 자동화된 작업을 설정하여 장치를 규정 미준수로 표시하고 해당 장치의 액세스를 거부합니다. 이 기능과 함께 사용되는 HDX 앱은 규정 미준수 장치에 대한 액세스를 거부하는 SmartAccess 정책을 사용하여 Virtual Apps and Desktops에서 구성됩니다. XenMobile은 서명되고 암호화된 태그를 사용하여 장치 상태를 StoreFront™에 전달합니다. 그러면 StoreFront는 앱의 액세스 제어 정책에 따라 액세스를 허용하거나 거부합니다.

이 기능을 사용하려면 배포에 다음이 필요합니다.

- 가상 앱 및 데스크톱 7.6
- StoreFront 3.7 또는 3.8
- StoreFront 서버에서 HDX 앱을 집계하도록 구성된 XenMobile® Server
- 태그 서명 및 암호화에 사용될 SAML 인증서로 구성된 XenMobile Server. 개인 키가 없는 동일한 인증서가 StoreFront 서버에 업로드됩니다.

이 기능을 사용하려면 다음을 수행합니다.

- XenMobile Server 인증서를 StoreFront 스토어에 구성

- 필요한 SmartAccess 정책으로 하나 이상의 Virtual Apps and Desktops 전달 그룹 구성
- XenMobile에서 자동화된 작업 설정

XenMobile Server 인증서를 내보내고 구성한 다음 StoreFront 스토어에 업로드

SmartAccess는 서명되고 암호화된 태그를 사용하여 XenMobile 및 StoreFront 서버 간에 통신합니다. 이 통신을 활성화하려면 XenMobile Server 인증서를 StoreFront 스토어에 추가합니다.

도메인 및 인증서 기반 인증이 활성화된 XenMobile과 StoreFront 통합에 대한 자세한 내용은 지원 기술 자료를 참조하십시오.

XenMobile Server에서 SAML 인증서 내보내기

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다. **인증서**를 클릭합니다.
2. XenMobile Server용 SAML 인증서를 찾습니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/locate-saml-certificate.png)
3. **개인 키 내보내기**가 **해제**로 설정되어 있는지 확인합니다. **내보내기**를 클릭하여 인증서를 다운로드 디렉터리로 내보냅니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/export-saml-certificate.png)
4. 다운로드 디렉터리에서 인증서를 찾습니다. 인증서는 PEM 형식입니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/locate-downloaded-certificate.png)

인증서를 PEM에서 CER로 변환

1. Microsoft Management Console (MMC)을 열고 **인증서 > 모든 작업 > 가져오기**를 마우스 오른쪽 버튼으로 클릭합니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/mmc-import-certificate.png)
2. 인증서 가져오기 마법사가 나타나면 **다음**을 클릭합니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/mmc-import-certificate-wizard.png)
3. 다운로드 디렉터리에서 인증서를 찾습니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/mmc-browse-certificate.png)
4. **모든 인증서를 다음 저장소에 저장**을 선택하고 인증서 저장소로 **개인**을 선택합니다. **다음**을 클릭합니다.

SmartAccess 구성(/en-us/xenmobile/server/media/mmc-import-certificate-store.png)

5. 선택 사항을 검토하고 **마침**을 클릭합니다. 확인 창을 닫으려면 **확인**을 클릭합니다.
6. MMC에서 인증서를 마우스 오른쪽 버튼으로 클릭한 다음 **모든 작업 > 내보내기**를 선택합니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/mmc-export-certificate.png)
7. 인증서 내보내기 마법사가 나타나면 **다음**을 클릭합니다.

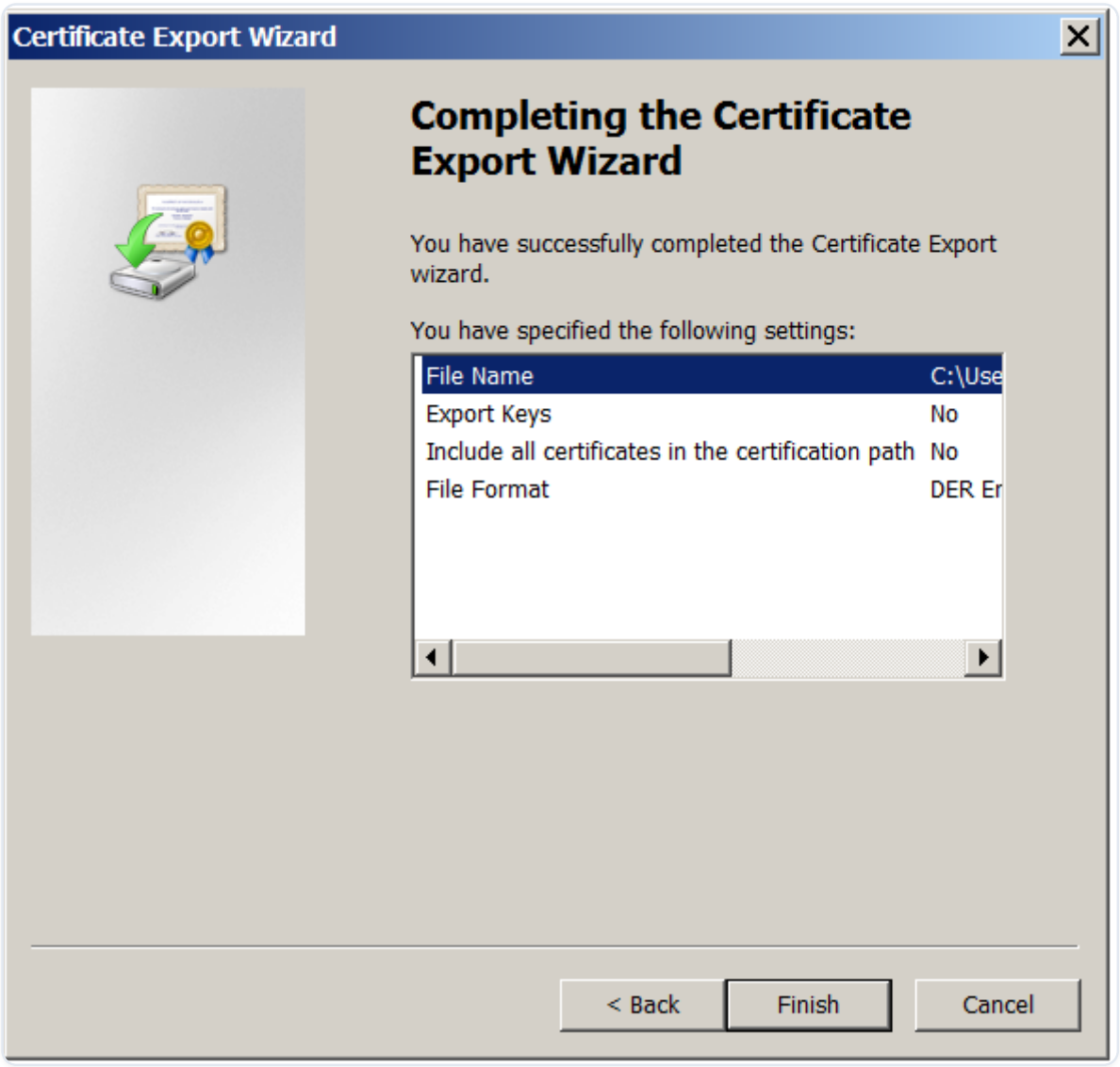
   SmartAccess 구성(/en-us/xenmobile/server/media/mmc-export-certificate-wizard.png)
8. **DER 인코딩 이진 X.509(.CER)** 형식을 선택합니다. **다음**을 클릭합니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/mmc-convert-certificate.png)
9. 인증서를 찾아봅니다. 인증서 이름을 입력한 다음 **다음**을 클릭합니다.

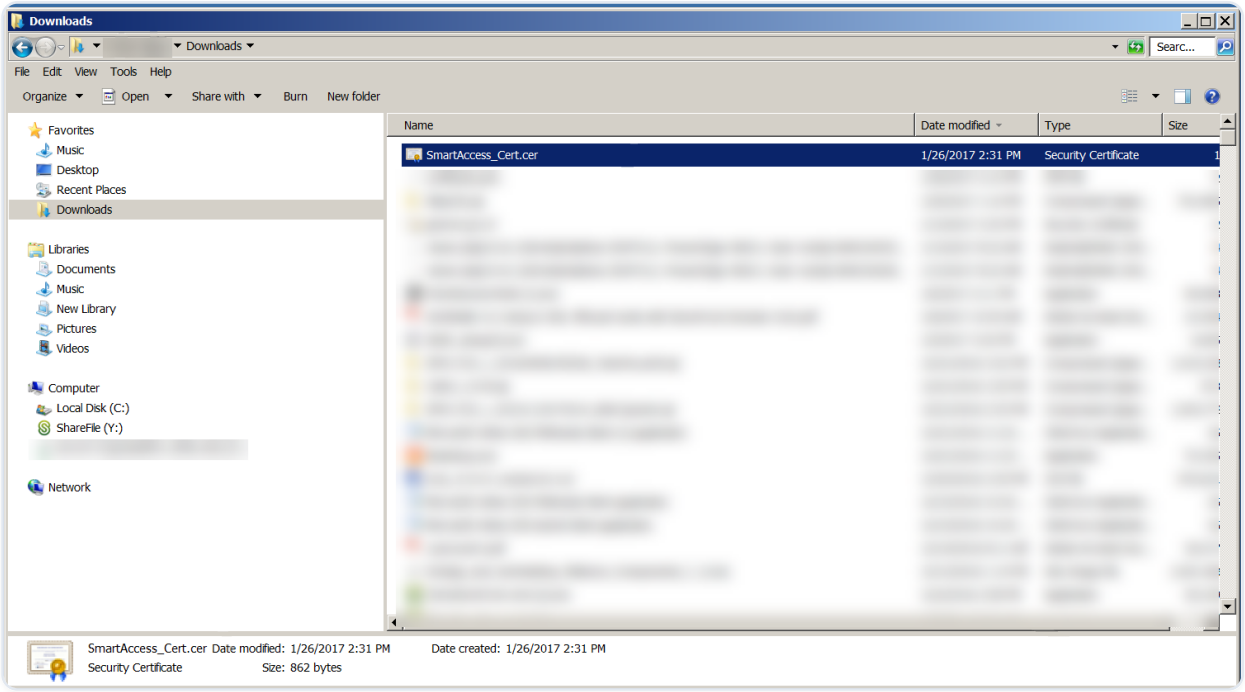
   SmartAccess 구성(/en-us/xenmobile/server/media/mmc-export-certificate-browse.png)
10. 인증서를 저장합니다.

    SmartAccess 구성(/en-us/xenmobile/server/media/mmc-export-certificate-save.png)
11. 인증서를 찾아보고 **다음**을 클릭합니다.

    SmartAccess 구성(/en-us/xenmobile/server/media/mmc-export-certificate-browse.png)
12. 선택 사항을 검토하고 **마침**을 클릭합니다. 확인 창을 닫으려면 **확인**을 클릭합니다.

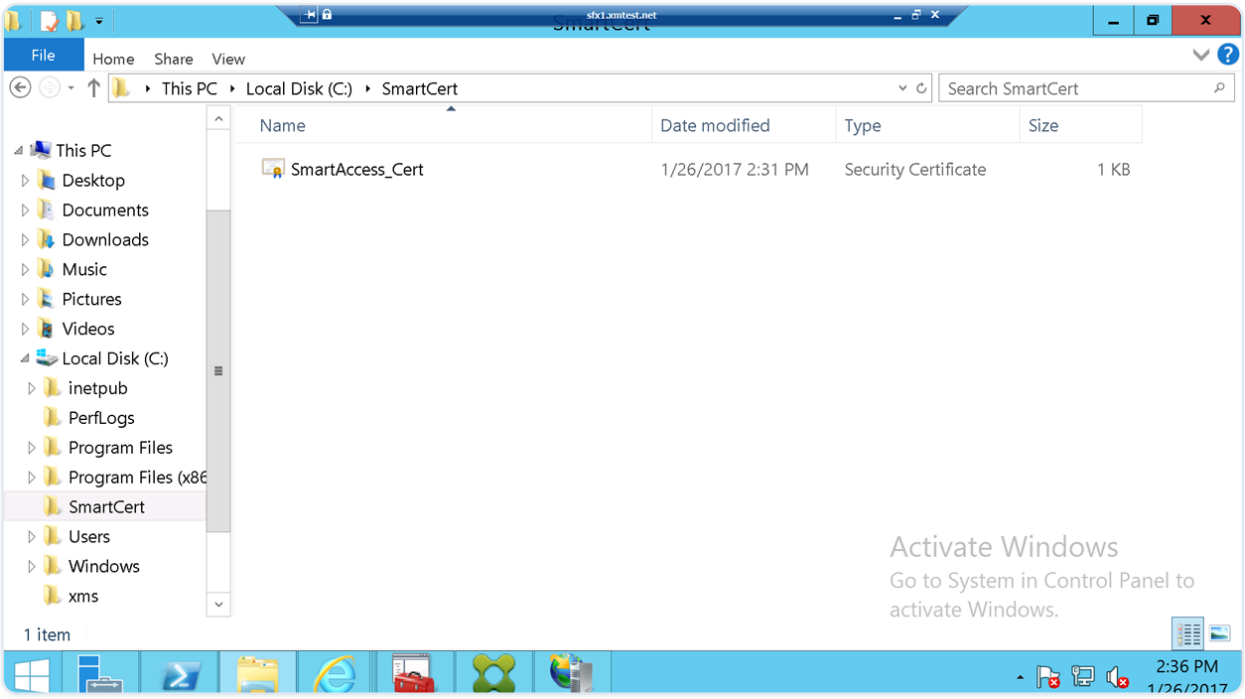


13. 다운로드 디렉터리에서 인증서를 찾습니다. 인증서는 CER 형식입니다.



인증서를 StoreFront 서버로 복사

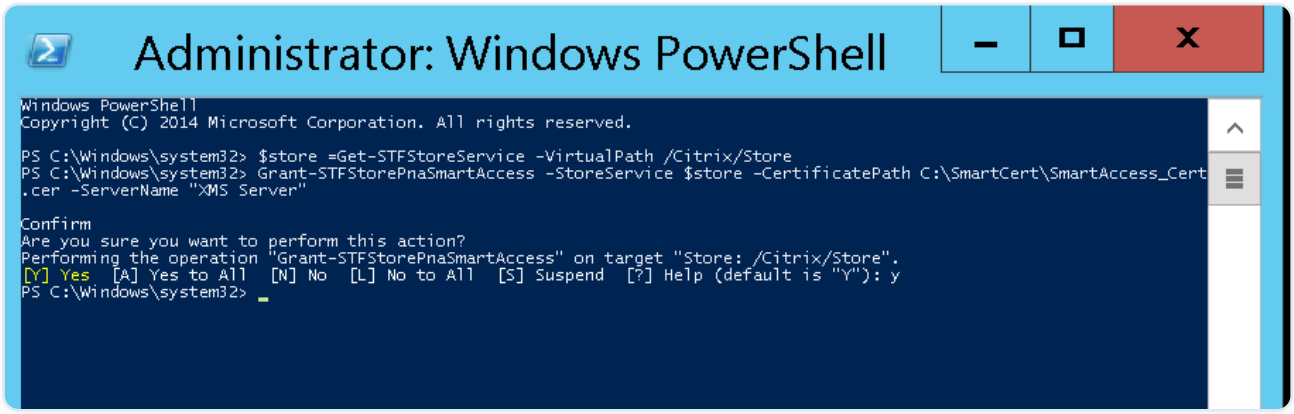
1. StoreFront 서버에서 **SmartCert**라는 폴더를 만듭니다.
2. 인증서를 **SmartCert** 폴더에 복사합니다.



StoreFront 스토어에서 인증서 구성

StoreFront 서버에서 이 PowerShell 명령을 실행하여 변환된 XenMobile Server 인증서를 스토어에 구성합니다.

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath  “C:\xms\xms.cer” –ServerName “XMS server”
```



StoreFront 스토어에 기존 인증서가 있는 경우 이 PowerShell 명령을 실행하여 해지합니다.

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```



또는 StoreFront 서버에서 다음 PowerShell 명령 중 하나를 실행하여 StoreFront 스토어의 기존 인증서를 해지할 수 있습니다.

- 이름으로 해지:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server"
```

- 지문으로 해지:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –CertificateThumbprint “ReplaceWithThumbprint”
```

- 서버 개체별 해지:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    $access = Get-STFStorePnaSmartAccess –StoreService $store



    Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess $access.AccessConditionsTrusts[0]
```

Virtual Apps and Desktops용 SmartAccess 정책 구성

HDX 앱을 제공하는 딜리버리 그룹에 필요한 SmartAccess 정책을 추가하려면 다음을 수행합니다.

1. Virtual Apps and Desktops 서버에서 Citrix Studio를 엽니다.
2. Studio 탐색 창에서 **딜리버리 그룹**을 선택합니다.
3. 액세스를 제어하려는 앱을 제공하는 그룹을 선택합니다. 그런 다음 **작업** 창에서 **딜리버리 그룹 편집**을 선택합니다.
4. **액세스 정책** 페이지에서 **NetScaler® Gateway를 통한 연결** 및 **다음 중 하나를 충족하는 연결**을 선택합니다.
5. **추가**를 클릭합니다.
6. **팜**이 **XM**이고 **필터**가 **XMCompliantDevice**인 액세스 정책을 추가합니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/delivery-group-app-desktop-access-policy.png)
7. 변경 사항을 적용하고 창을 열어 두려면 **적용**을 클릭하고, 변경 사항을 적용하고 창을 닫으려면 **확인**을 클릭합니다.

XenMobile에서 자동화된 작업 설정

HDX 앱의 딜리버리 그룹에 설정한 SmartAccess 정책은 장치가 규정을 준수하지 않을 경우 장치에 대한 액세스를 거부합니다. 자동화된 작업을 사용하여 장치를 규정 미준수로 표시합니다.

SmartAccess 구성(/en-us/xenmobile/server/media/actions-out-of-compliance.png)

1. XenMobile 콘솔에서 **구성 > 작업**을 클릭합니다. **작업** 페이지가 나타납니다.
2. **추가**를 클릭하여 작업을 추가합니다. **작업 정보** 페이지가 나타납니다.
3. **작업 정보** 페이지에서 작업의 이름과 설명을 입력합니다.
4. **다음**을 클릭합니다. **작업 세부 정보** 페이지가 나타납니다. 다음 예에서는 사용자 속성 이름이 **eng5** 또는 **eng6**인 경우 장치를 즉시 규정 미준수로 표시하는 트리거가 생성됩니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/configure-actions-trigger-example.png)
5. **트리거** 목록에서 **장치 속성**, **사용자 속성** 또는 **설치된 앱 이름**을 선택합니다. SmartAccess는 이벤트 트리거를 지원하지 않습니다.
6. **작업** 목록에서:
   - **장치를 규정 미준수로 표시**를 선택합니다.
   - **다음과 같음**을 선택합니다.
   - **True**를 선택합니다.
   - 트리거 조건이 충족될 때 장치를 즉시 규정 미준수로 표시하도록 작업을 설정하려면 시간 프레임을 **0**으로 설정합니다.

7. 이 작업을 적용할 XenMobile 전달 그룹을 선택합니다.
8. 작업 요약을 검토합니다.
9. **다음**을 클릭한 다음 **저장**을 클릭합니다.

장치가 규정 미준수로 표시되면 HDX 앱이 Secure Hub 스토어에 더 이상 나타나지 않습니다. 사용자는 더 이상 앱을 구독하지 않습니다. 장치로 알림이 전송되지 않으며 Secure Hub 스토어의 어떤 항목도 HDX 앱이 이전에 사용 가능했음을 나타내지 않습니다.

장치가 규정 미준수로 표시될 때 사용자에게 알림을 보내려면 알림을 생성한 다음 해당 알림을 보내는 자동화된 작업을 생성합니다.

이 예시는 장치가 규정 미준수로 표시될 때 다음 알림을 생성하고 보냅니다: "장치 일련 번호 또는 전화 번호가 더 이상 장치 정책을 준수하지 않으며 HDX 애플리케이션이 차단되었습니다."

SmartAccess 구성(/en-us/xenmobile/server/media/secure-hub-notification-out-of-compliance.png)

장치가 규정 미준수로 표시될 때 사용자에게 표시되는 알림 생성

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **알림 템플릿**을 클릭합니다. **알림 템플릿** 페이지가 나타납니다.
3. **알림 템플릿** 페이지에서 **추가**를 클릭합니다.
4. SMS 서버를 먼저 설정하라는 메시지가 표시되면 **아니요, 나중에 설정**을 클릭합니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/notification-template-set-up-sms-server-later.png)
5. 다음 설정을 구성합니다:

   - **이름:** HDX 애플리케이션 차단
   - **설명:** 장치가 규정 미준수 상태일 때 에이전트 알림
   - **유형:** 임시 알림
   - **Secure Hub:** 활성화됨
   - **메시지:** 장치 ${firstnotnull(device.TEL_NUMBER,device.serialNumber)}가 더 이상 장치 정책을 준수하지 않으며 HDX 애플리케이션이 차단되었습니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/notification-template-settings.png)
6. **저장**을 클릭합니다.

장치가 규정 미준수로 표시될 때 알림을 보내는 작업 생성

1. XenMobile 콘솔에서 **구성 > 작업**을 클릭합니다. **작업** 페이지가 나타납니다.
2. 작업을 추가하려면 **추가**를 클릭합니다. **작업 정보** 페이지가 나타납니다.
3. **작업 정보** 페이지에서 작업의 이름과 설명을 입력합니다.
   - **이름:** HDX 차단 알림
   - **설명:** 장치가 규정 미준수 상태이므로 HDX 차단 알림
4. **다음**을 클릭합니다. **작업 세부 정보** 페이지가 나타납니다.
5. **트리거** 목록에서:
   - **장치 속성**을 선택합니다.
   - **규정 미준수**를 선택합니다.
   - **입니다**를 선택합니다.
   - **참**을 선택합니다.

   SmartAccess 구성(/en-us/xenmobile/server/media/configure-actions-details-example.png)
6. **작업** 목록에서 트리거가 충족될 때 발생하는 작업을 지정합니다.
   - **알림 보내기**를 선택합니다.
   - **HDX 애플리케이션 차단, 생성한 알림**을 선택합니다.
   - **0**을 선택합니다. 이 값을 0으로 설정하면 트리거 조건이 충족될 때 알림이 전송됩니다.
7. 이 작업을 적용할 XenMobile 배달 그룹을 선택합니다. 이 예에서는 **AllUsers**를 선택합니다.
8. 작업 요약을 검토합니다.
9. **다음**을 클릭한 다음 **저장**을 클릭합니다.

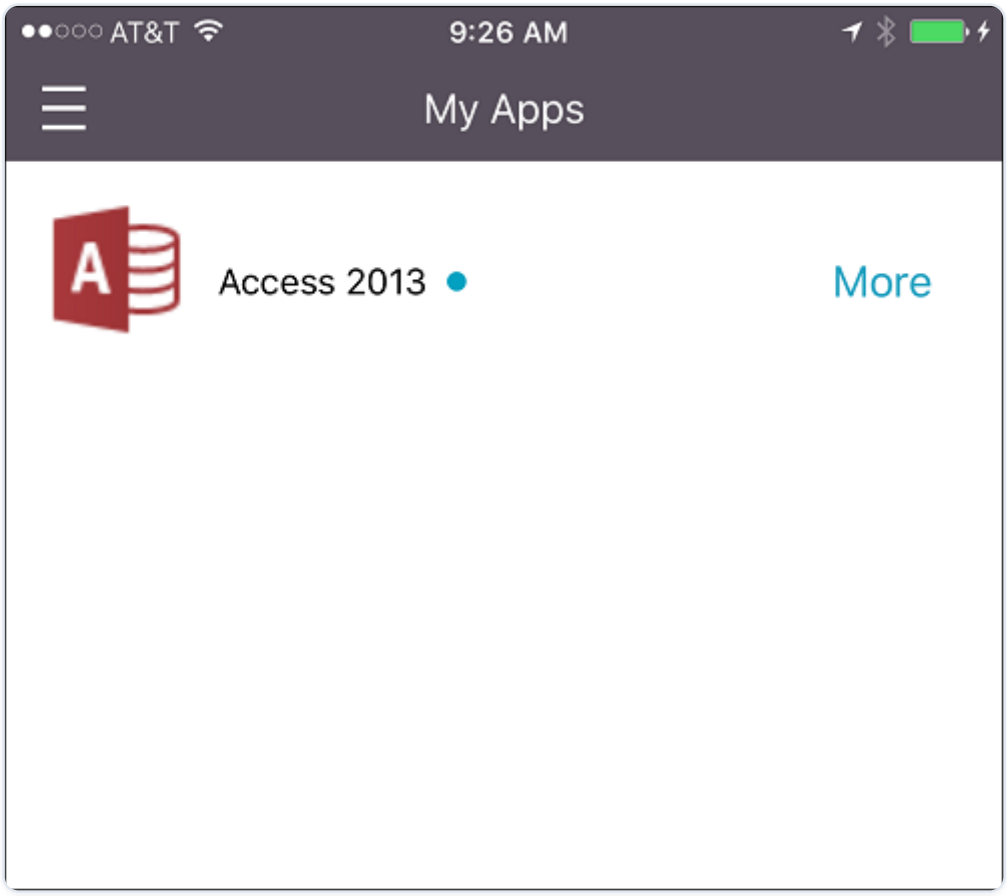
자동화된 작업 설정에 대한 자세한 내용은 자동화된 작업을 참조하십시오.

사용자가 HDX 앱에 다시 액세스하는 방법

장치가 규정 준수 상태로 돌아오면 사용자는 HDX 앱에 다시 액세스할 수 있습니다.

1. 장치에서 Secure Hub 스토어로 이동하여 스토어의 앱을 새로 고칩니다.
2. 앱으로 이동하여 앱에 **추가**를 탭합니다.

앱이 추가되면 새로 설치된 앱이므로 내 앱에 파란색 점과 함께 표시됩니다.


AT&T
9:26 AM
My Apps
Access 2013
More

미디어 추가

사용자 장치에 미디어를 배포할 수 있도록 XenMobile®에 미디어를 추가합니다. XenMobile을 사용하여 Apple 볼륨 구매를 통해 얻은 Apple Books를 배포할 수 있습니다.

XenMobile에서 볼륨 구매 계정을 구성한 후 구매한 책과 무료 책이 **구성 > 미디어**에 나타납니다. **미디어** 페이지에서 전달 그룹을 선택하고 배포 규칙을 지정하여 iOS 장치에 배포할 책을 구성합니다.

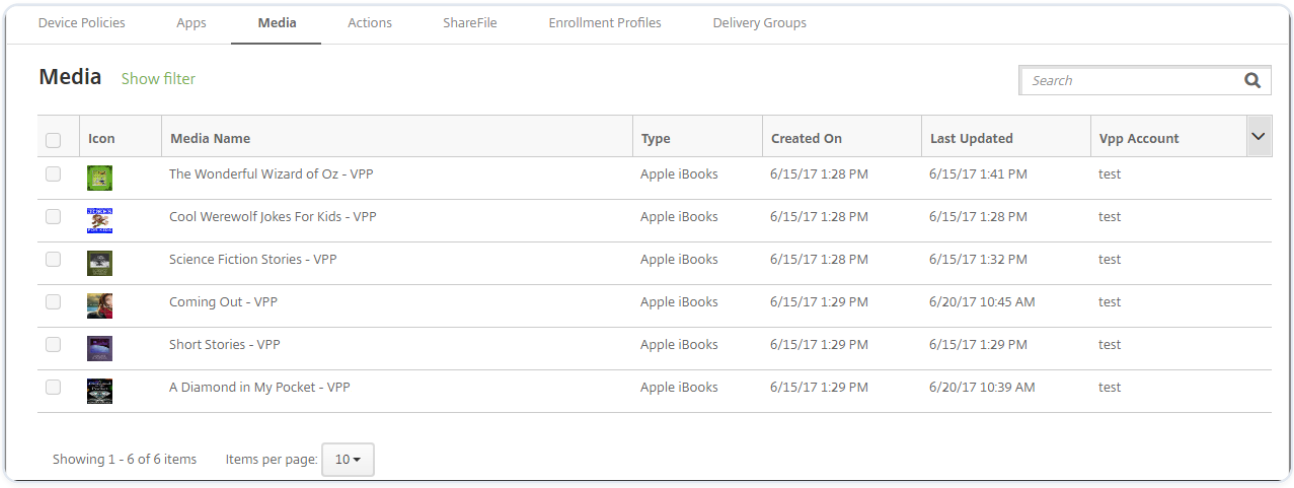
사용자가 책을 처음 받고 볼륨 구매 라이선스를 수락하면 배포된 책이 장치에 설치됩니다. 책은 Apple Book 앱에 나타납니다. 책 라이선스를 사용자로부터 분리하거나 장치에서 책을 제거할 수 없습니다. XenMobile은 책을 필수 미디어로 설치합니다. 사용자가 설치된 책을 장치에서 삭제하더라도 책은 Apple Book 앱에 남아 다운로드할 준비가 됩니다.

전제 조건

- iOS 장치
- (/ko-kr/xenmobile/server/apps/apple-volume-purchase.html)에 설명된 대로 XenMobile에서 Apple 볼륨 구매를 구성합니다.

책 구성

볼륨 구매를 통해 얻은 Apple Books는 **구성 > 미디어** 페이지에 나타납니다.



배포할 Apple Book을 구성하려면

1. **구성 > 미디어**에서 책을 선택하고 **편집**을 클릭합니다. **책 정보** 페이지가 나타납니다.



   이름과 **설명**은 XenMobile 콘솔 및 로그에만 나타납니다.

2. **iPhone iBook 설정** 및 **iPad iBook 설정** 페이지에서 책 이름과 설명을 선택적으로 변경할 수 있지만, Citrix®는 이러한 설정을 변경하지 않는 것을 권장합니다. 이미지는 정보용이며 편집할 수 없습니다. **유료 iBook**은 Apple 볼륨 구매를 통해 책이 구매되었음을 나타냅s니다.

   도서 구성(/en-us/xenmobile/server/media/configure-media-ibooks-vp-iphone.png)

   배포 규칙을 지정하거나 볼륨 구매 정보를 볼 수도 있습니다.

   도서 구성(/en-us/xenmobile/server/media/configure-media-ibooks-vp-settings.png)

3. 선택적으로, 도서를 배달 그룹에 할당하고 배포 일정을 설정합니다.

   도서 구성(/en-us/xenmobile/server/media/configure-media-ibooks-vp-delivery-groups.png)

   구성 > 배달 그룹의 **미디어** 탭에서 도서를 배달 그룹에 할당할 수도 있습니다. XenMobile은 필수 도서 배포만 지원합니다.

   도서 구성(/en-us/xenmobile/server/media/configure-delivery-groups-media-ibooks-vp.png)

4. **관리 > 장치**의 **미디어** 탭을 사용하여 배포 상태를 확인합니다.

   도서 구성(/en-us/xenmobile/server/media/manage-devices-media-ibook-vp.png)

> **참고:**
>
> **구성 > 미디어** 페이지에서 도서를 선택하고 **삭제**를 클릭하면 XenMobile이 목록에서 해당 도서를 제거합니다. 그러나 XenMobile이 다음에 Apple 볼륨 구매와 동기화할 때, Apple 볼륨 구매에서 제거되지 않은 한 해당 도서가 목록에 다시 나타납니다. 목록에서 도서를 삭제해도 장치에서 도서가 제거되지는 않습니다.

도서는 다음 예와 같이 사용자 장치에 표시됩니다.

도서 구성(/en-us/xenmobile/server/media/store-ibooks-samples.png)

리소스 배포

장치 구성 및 관리는 일반적으로 XenMobile® 콘솔에서 리소스(정책, 앱 및 미디어)와 작업을 생성한 다음 배달 그룹을 사용하여 패키징하는 것을 포함합니다. XenMobile이 배달 그룹의 리소스와 작업을 장치로 푸시하는 순서를 배포 순서라고 합니다. 이 문서에서는 다음 방법을 설명합니다.

- 배달 그룹을 추가, 관리 및 배포하는 방법
- 배달 그룹에서 리소스 및 작업의 배포 순서를 변경하는 방법
- 사용자가 중복되거나 충돌하는 정책이 있는 여러 배달 그룹에 속해 있을 때 XenMobile이 배포 순서를 결정하는 방법.

배달 그룹은 정책, 앱, 미디어 및 작업의 조합을 배포할 장치를 가진 사용자 범주를 지정합니다. 배달 그룹에 포함되는 것은 일반적으로 회사, 국가, 부서, 사무실 주소 및 직책과 같은 사용자 특성을 기반으로 합니다. 배달 그룹을 통해 누가 어떤 리소스를 언제 받는지에 대해 더 큰 제어 권한을 가질 수 있습니다. 배달 그룹을 모든 사람에게 배포하거나 더 좁게 정의된 사용자 그룹에 배포할 수 있습니다.

배달 그룹에 배포하는 것은 지원되는 iOS 및 Windows 장치를 가진 모든 사용자에게 푸시 알림을 보내는 것을 의미합니다. 해당 사용자는 XenMobile에 다시 연결하려면 배달 그룹에 속해야 합니다. 장치를 재평가하고 배달 그룹의 일부인 정책, 앱, 미디어 및 작업을 배포할 수 있습니다.

Android 장치 사용자의 경우: 이미 연결되어 있다면 즉시 리소스를 받습니다. 그렇지 않으면 예약 정책에 따라 다음에 연결할 때 리소스를 받습니다.

기본 AllUsers 배달 그룹은 XenMobile을 설치하고 구성할 때 생성됩니다. 이 그룹에는 모든 로컬 사용자 및 Active Directory 사용자가 포함됩니다. AllUsers 그룹을 삭제할 수는 없지만, 모든 사용자에게 리소스를 푸시하고 싶지 않을 때는 그룹을 비활성화할 수 있습니다.

배포 순서 지정

배포 순서는 XenMobile이 장치에 리소스를 푸시하는 순서입니다. 배포 순서는 장치 관리(MDM)용으로 구성된 등록 프로필이 있는 배달 그룹의 장치에만 적용됩니다.

배포 순서를 결정할 때 XenMobile은 배포 규칙 및 배포 일정과 같은 필터 및 제어 기준을 리소스에 적용합니다. 리소스에는 정책, 앱, 작업 및 배달 그룹이 포함됩니다. 배달 그룹을 추가하기 전에 이 섹션의 정보가 배포 목표와 어떻게 관련되는지 고려하십시오.

배포 순서와 관련된 주요 개념 요약은 다음과 같습니다.

- **배포 순서:** XenMobile이 리소스(정책, 앱 및 미디어)와 작업을 장치로 푸시하는 순서입니다. 이용 약관 및 소프트웨어 인벤토리와 같은 일부 정책의 배포 순서는 다른 리소스에 영향을 미치지 않습니다. 작업이 배포되는 순서는 다른 리소스에 영향을 미치지 않습니다. 따라서 XenMobile이 리소스를 배포할 때 해당 위치는 무시됩니다.
- **배포 규칙:** XenMobile은 장치 속성에 대해 지정한 배포 규칙을 사용하여 정책, 앱, 미디어, 작업 및 배달 그룹을 필터링합니다. 예를 들어, 배포 규칙은 도메인 이름이 특정 값과 일치할 때 배포 패키지를 푸시하도록 지정할 수 있습니다.
- **배포 일정:** XenMobile은 정책, 앱, 미디어 및 작업에 대해 지정하는 배포 일정을 사용하여 해당 항목의 배포를 제어합니다. 배포가 즉시, 특정 날짜 및 시간에 또는 배포 조건에 따라 발생하도록 지정할 수 있습니다.

다음 표는 다양한 개체 및 리소스 유형에 대한 필터 및 제어 기준을 보여줍니다. 배포 규칙은 장치 속성을 기반으로 합니다.

개체/리소스	장치 플랫폼	배포 규칙	배포 일정	사용자/그룹
장치 정책	Y	Y	Y	-
앱	Y	Y	예	-
미디어	예	예	예	-
작업	-	예	예	-
전달 그룹	-	예	-	Y

일반적인 환경에서는 여러 배달 그룹이 단일 사용자에게 할당될 가능성이 높으며, 다음과 같은 결과가 발생할 수 있습니다.

- 배달 그룹 내에 중복 개체가 존재합니다.
- 특정 정책이 사용자에게 할당된 둘 이상의 배달 그룹에서 다르게 구성됩니다.

이러한 상황 중 하나가 발생하면 XenMobile은 장치에 전달하거나 조치해야 하는 모든 개체에 대한 배포 순서를 계산합니다. 계산 단계는 장치 플랫폼과 무관합니다.

계산 단계

1. 사용자, 그룹 및 배포 규칙 필터를 기반으로 특정 사용자에 대한 모든 배달 그룹을 결정합니다.
2. 선택한 배달 그룹 내의 모든 리소스(정책, 앱, 미디어 및 작업)에 대한 정렬된 목록을 만듭니다. 이 목록은 장치 플랫폼, 배포 규칙 및 배포 일정 필터를 기반으로 합니다. 정렬 알고리즘은 다음과 같습니다.

a. 사용자 정의 배포 순서가 있는 배달 그룹의 리소스를 사용자 정의 배포 순서가 없는 배달 그룹의 리소스보다 앞에 배치합니다. 이 배치에 대한 근거는 다음 단계에서 설명합니다.

b. 배달 그룹 간의 동점 처리기로, 배달 그룹 이름별로 배달 그룹의 리소스를 정렬합니다. 예를 들어, 배달 그룹 A의 리소스를 배달 그룹 B의 리소스보다 앞에 배치합니다.

c. 정렬하는 동안 배달 그룹의 리소스에 대해 사용자 정의 배포 순서가 지정된 경우 해당 순서를 유지합니다. 그렇지 않으면 해당 배달 그룹 내의 리소스를 리소스 이름별로 정렬합니다.

d. 동일한 리소스가 두 번 이상 나타나면 중복 리소스를 제거합니다.

사용자 정의 순서가 연결된 리소스는 사용자 정의 순서가 없는 리소스보다 먼저 배포됩니다. 리소스는 사용자에게 할당된 여러 배달 그룹에 존재할 수 있습니다. 위 단계에서 언급했듯이 계산 알고리즘은 중복 리소스를 제거하고 이 목록에서 첫 번째 리소스만 전달합니다. 이러한 방식으로 중복 리소스를 제거함으로써 XenMobile은 XenMobile 관리자가 정의한 순서를 적용합니다.

예를 들어, 다음과 같은 두 개의 배달 그룹이 있다고 가정해 보겠습니다.

- 전달 그룹, 계정 관리자 1: 리소스에 대한 **지정되지 않은** 순서. **WiFi** 및 **암호** 정책을 포함합니다.
- 전달 그룹, 계정 관리자 2: 리소스에 대한 **지정된** 순서. **연결 스케줄링**, **제한**, **암호** 및 **WiFi** 정책을 포함합니다. 이 경우 **암호** 정책을 **WiFi** 정책보다 먼저 전달하려고 합니다.

전달 그룹 구성 화면(/en-us/xenmobile/server/media/configure-delivery-group-specify-order.png)

계산 알고리즘이 배포 그룹을 이름으로만 정렬했다면, XenMobile은 전달 그룹 계정 관리자 1부터 시작하여 **WiFi**, **암호**, **연결 스케줄링**, **제한** 순서로 배포를 수행할 것입니다. XenMobile은 계정 관리자 2 전달 그룹에서 중복되는 **암호** 및 **WiFi**를 무시할 것입니다.

그러나 계정 관리자 2 그룹에는 관리자가 지정한 배포 순서가 있습니다. 따라서 계산 알고리즘은 계정 관리자 2 전달 그룹의 리소스를 다른 전달 그룹의 리소스보다 목록에서 더 높은 순위에 배치합니다. 결과적으로 XenMobile은 **연결 스케줄링**, **제한**, **암호**, **WiFi** 순서로 정책을 배포합니다. XenMobile은 계정 관리자 1 전달 그룹의 **WiFi** 및 **암호** 정책이 중복되기 때문에 무시합니다. 따라서 해당 알고리즘은 XenMobile 관리자가 지정한 순서를 따릅니다.

배포 규칙

특정 조건이 존재할 때만 리소스를 전달하도록 배포 규칙을 구성합니다. 기본 또는 고급 배포 규칙을 구성할 수 있습니다.

기본 편집기를 사용하여 배포 규칙을 추가할 때, 먼저 리소스를 배포할 시기를 선택합니다.

배포 규칙 기본 구성(/en-us/xenmobile/server//media/deployment-rules.png)

- **모두:** 사용자 또는 장치가 구성한 모든 조건을 충족할 때 리소스를 전달합니다.

- **임의:** 사용자 또는 장치가 구성한 조건 중 하나 이상을 충족할 때 리소스를 전달합니다.

새 규칙을 클릭하여 조건을 추가합니다. 규칙은 배포되는 리소스와 리소스를 구성하는 플랫폼에 따라 다릅니다. 여러 유형의 규칙이 있습니다. 다음과 같이 리소스를 배포하도록 선택할 수 있습니다.

- 선택한 속성이 존재할 때만 또는 선택한 속성이 존재할 때를 제외하고.
- 속성이 입력한 텍스트와 정확히 일치할 때, 속성에 입력한 텍스트가 포함될 때, 또는 속성이 입력한 텍스트와 일치하지 않을 때.
- 장치 또는 사용자가 선택한 속성을 준수할 때 또는 선택한 속성을 준수하지 않을 때.
- 장치 또는 사용자 속성이 미리 정의된 목록에서 선택한 조건과 일치하는 경우.

고급 편집기를 사용하여 더 복잡한 배포 규칙을 만듭니다. 선택할 수 있는 규칙이 더 많으며 고급 규칙을 만들 때 다양한 부울 논리 연산자를 결합할 수 있습니다.

배포 규칙 고급 구성(/en-us/xenmobile/server//media/deployment-rules-advanced.png)

전달 그룹을 추가하려면

Citrix®는 장치 정책 및 등록 프로필을 만들기 전에 전달 그룹을 만들 것을 권장합니다.

1. 콘솔에서 **구성 > 전달 그룹**을 클릭합니다.
2. **전달 그룹** 페이지에서 **추가**를 클릭합니다.
3. **전달 그룹 정보** 페이지에서 전달 그룹의 이름과 설명을 입력한 다음 **다음**을 클릭합니다.

   사용자가 서로 다른 등록 프로필을 가진 여러 전달 그룹에 속하는 경우, 전달 그룹의 이름이 사용되는 등록 프로필을 결정합니다. XenMobile은 전달 그룹의 알파벳순 목록에서 마지막에 나타나는 전달 그룹을 선택합니다. 자세한 내용은 등록 프로필을 참조하십시오.
4. **사용자 할당** 페이지에서 전달 그룹 사용자 할당을 관리하는 방법을 지정합니다.

   전달 그룹 구성 화면(/en-us/xenmobile/server/media/configure-delivery-groups-assignments.png)

   > **중요:**
   >
   > 사용자 그룹이 생성된 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 그룹은 **선택한 사용자 그룹** 목록에 나타납니다.
- **검색**을 클릭하여 선택한 도메인의 모든 사용자 그룹 목록을 확인합니다.
- 검색 상자에 전체 또는 부분 그룹 이름을 입력한 다음 **검색**을 클릭하여 사용자 그룹 목록을 제한합니다.

선택한 사용자 그룹 목록에서 사용자 그룹을 제거하려면 다음 중 하나를 수행합니다.

- **선택한 사용자 그룹** 목록에서 제거하려는 각 그룹 옆에 있는 **X**를 클릭합니다.
- **검색**을 클릭하여 선택한 도메인의 모든 사용자 그룹 목록을 확인합니다. 목록을 스크롤하여 제거하려는 각 그룹의 확인란을 선택 취소합니다.
- 검색 상자에 전체 또는 부분 그룹 이름을 입력한 다음 **검색**을 클릭하여 사용자 그룹 목록을 제한합니다. 목록을 스크롤하여 제거하려는 각 그룹의 확인란을 선택 취소합니다.

- **또는/그리고:** 리소스가 사용자에게 배포되도록 하려면 사용자가 모든 그룹에 속할 수 있는지(또는) 또는 모든 그룹에 속해야 하는지(그리고)를 선택합니다.
- **익명 사용자에게 배포:** 배달 그룹의 인증되지 않은 사용자에게 배포할지 여부를 선택합니다. 인증되지 않은 사용자는 인증할 수 없었지만 장치가 XenMobile에 연결하도록 허용한 사용자입니다.

5. 배포 규칙을 구성합니다.
6. **다음**을 클릭합니다. **배달 그룹 리소스** 페이지가 나타납니다. 여기에서 배달 그룹에 대한 정책, 앱 또는 작업을 선택적으로 추가할 수 있습니다. 이 단계를 건너뛰려면 **배달 그룹** 아래에서 **요약**을 클릭하여 배달 그룹 구성 요약을 확인합니다.

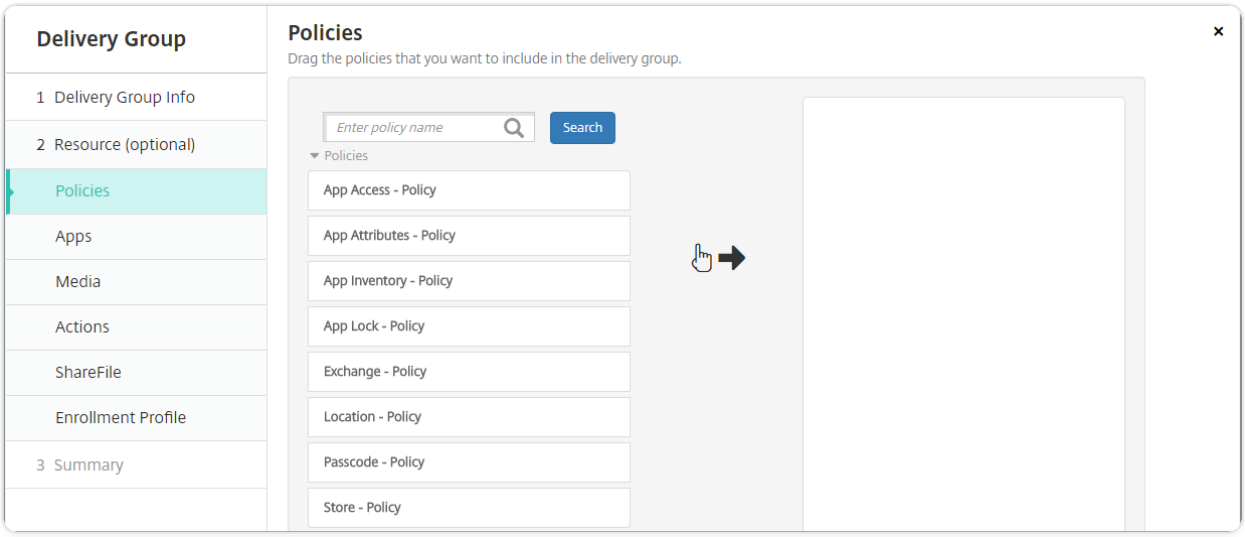
   리소스를 건너뛰려면 **리소스(선택 사항)** 아래에서 추가하려는 리소스를 클릭하고 해당 리소스에 대한 단계를 따릅니다.

정책을 추가하려면

1. 추가하려는 각 정책에 대해 다음을 수행합니다.

   - 사용 가능한 정책 목록을 스크롤하여 추가하려는 정책을 찾습니다.
   - 또는 정책 목록을 제한하려면 검색 상자에 전체 또는 부분 정책 이름을 입력한 다음 **검색**을 클릭합니다.
   - 추가하려는 정책을 클릭하여 오른쪽 상자로 끌어다 놓습니다.

   정책을 제거하려면 오른쪽 상자에서 정책 이름 옆에 있는 **X**를 클릭합니다.



2. **다음**을 클릭합니다. **앱** 페이지가 나타납니다.

앱을 추가하려면

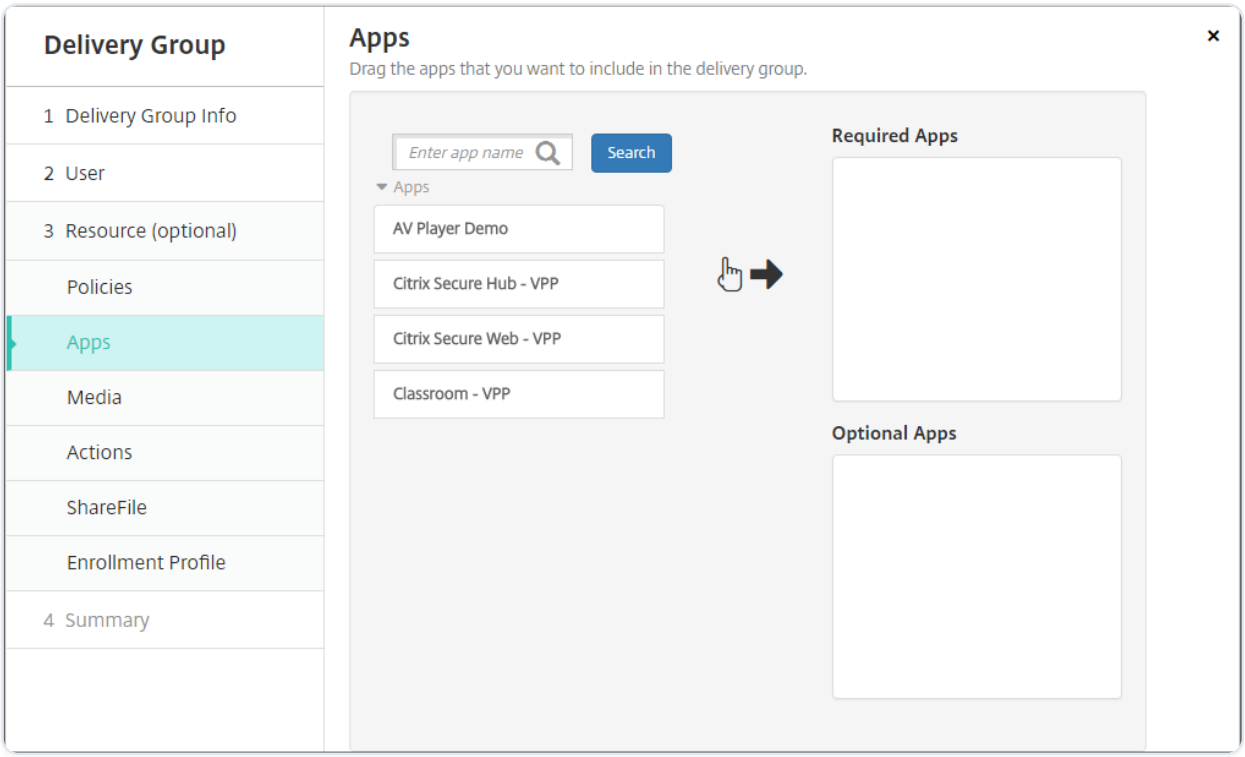
1. 추가하려는 각 앱에 대해 다음을 수행합니다.

   - 사용 가능한 앱 목록을 스크롤하여 추가하려는 앱을 찾습니다.
   - 또는 앱 목록을 제한하려면 검색 상자에 전체 또는 부분 앱 이름을 입력한 다음 **검색**을 클릭합니다.
   - 추가하려는 앱을 클릭하여 **필수 앱** 상자 또는 **선택적 앱** 상자로 끌어다 놓습니다.

   필수로 표시된 앱의 경우 사용자는 다음과 같은 상황에서 업데이트를 즉시 받을 수 있습니다.

   - 새 앱을 업로드하고 필수로 표시합니다.
   - 기존 앱을 필수로 표시합니다.
   - 사용자가 필수 앱을 삭제할 때.
   - Secure Hub 업데이트를 사용할 수 있습니다.

   필수 앱의 강제 배포 및 기능 활성화 방법에 대한 자세한 내용은 필수 및 선택적 앱 정보를 참조하십시오.



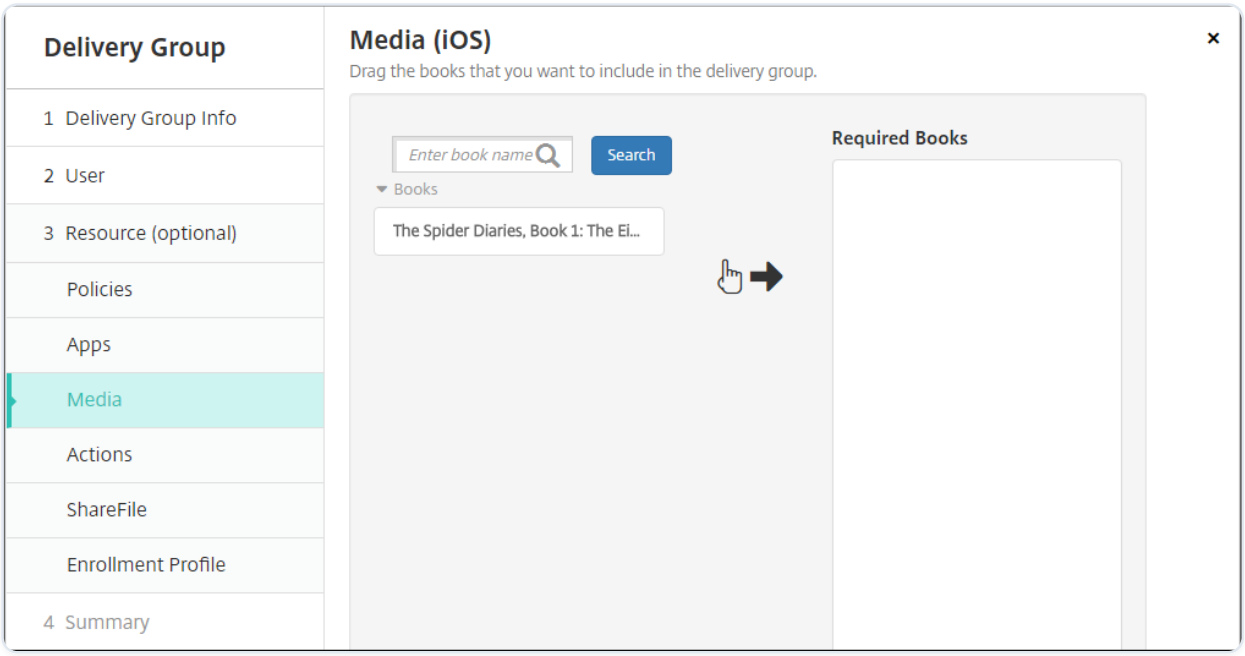
앱을 제거하려면 오른쪽 상자에서 앱 이름 옆에 있는 **X**를 클릭합니다.

2. **다음**을 클릭합니다. **미디어** 페이지가 나타납니다.

미디어 추가

1. 추가하려는 각 책에 대해 다음 작업을 수행합니다.

   - 사용 가능한 책 목록을 스크롤하여 추가하려는 책을 찾습니다.
   - 또는 책 목록을 제한하려면 검색 상자에 전체 또는 부분 책 이름을 입력한 다음 **검색**을 클릭합니다.
   - 추가하려는 책을 클릭하고 **필수 책** 상자로 끌어다 놓습니다.



필수로 표시된 책의 경우 사용자는 다음과 같은 상황에서 즉시 업데이트를 받습니다.

- 새 책을 업로드하고 필수로 표시합니다.
- 기존 책을 필수로 표시합니다.
- 사용자가 필수 책을 삭제하는 경우.
- Secure Hub 업데이트를 사용할 수 있습니다.

책을 제거하려면 오른쪽 상자의 책 이름 옆에 있는 **X**를 클릭합니다.

2. **다음**을 클릭합니다. **작업** 페이지가 나타납니다.

작업 추가

1. 추가하려는 각 작업에 대해 다음을 수행합니다.

   - 사용 가능한 작업 목록을 스크롤하여 추가하려는 작업을 찾습니다.
   - 또는 작업 목록을 제한하려면 검색 상자에 전체 또는 부분 작업 이름을 입력한 다음 **검색**을 클릭합니다.
   - 추가하려는 작업을 클릭하여 오른쪽 상자로 끕니다.

   작업을 제거하려면 오른쪽 상자의 작업 이름 옆에 있는 **X**를 클릭합니다.

   전달 그룹 구성 화면(/en-us/xenmobile/server/media/configure-delivery-groups-actions.png)

2. **다음**을 클릭합니다. **ShareFile** 페이지가 나타납니다.

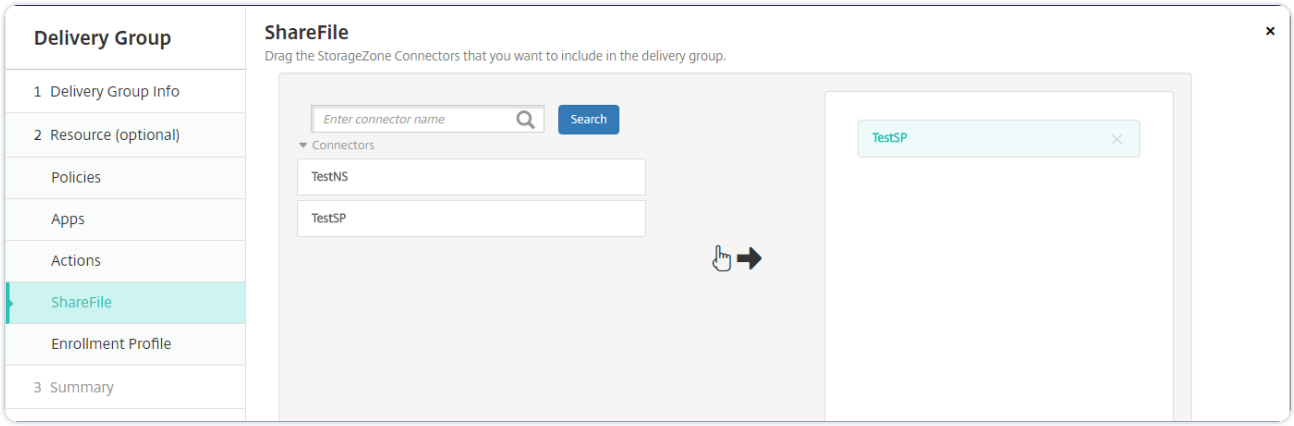
ShareFile 구성 적용

ShareFile 페이지는 XenMobile(**구성 > ShareFile**)을 엔터프라이즈 계정용으로 구성했는지 또는 스토리지 영역 커넥터용으로 구성했는지에 따라 다릅니다.

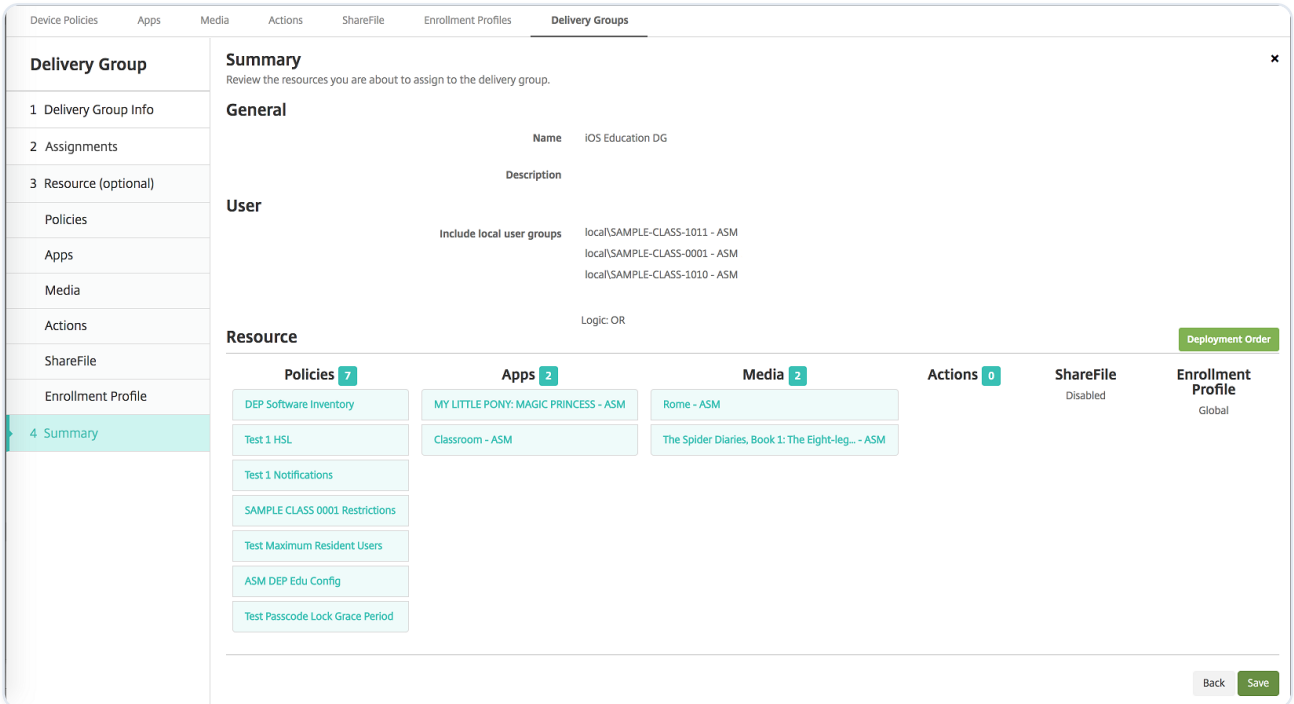
XenMobile과 함께 사용할 엔터프라이즈 계정을 구성한 경우: 전달 그룹에 ShareFile 콘텐츠 및 데이터에 대한 단일 Sign-On 액세스를 제공하려면 **ShareFile 사용**을 **켜기**로 설정합니다.

전달 그룹 구성 화면(/en-us/xenmobile/server/media/configure-delivery-groups-sharefile.png)

XenMobile과 함께 사용할 스토리지 영역 커넥터를 구성한 경우 전달 그룹에 포함할 스토리지 영역 커넥터를 선택합니다.

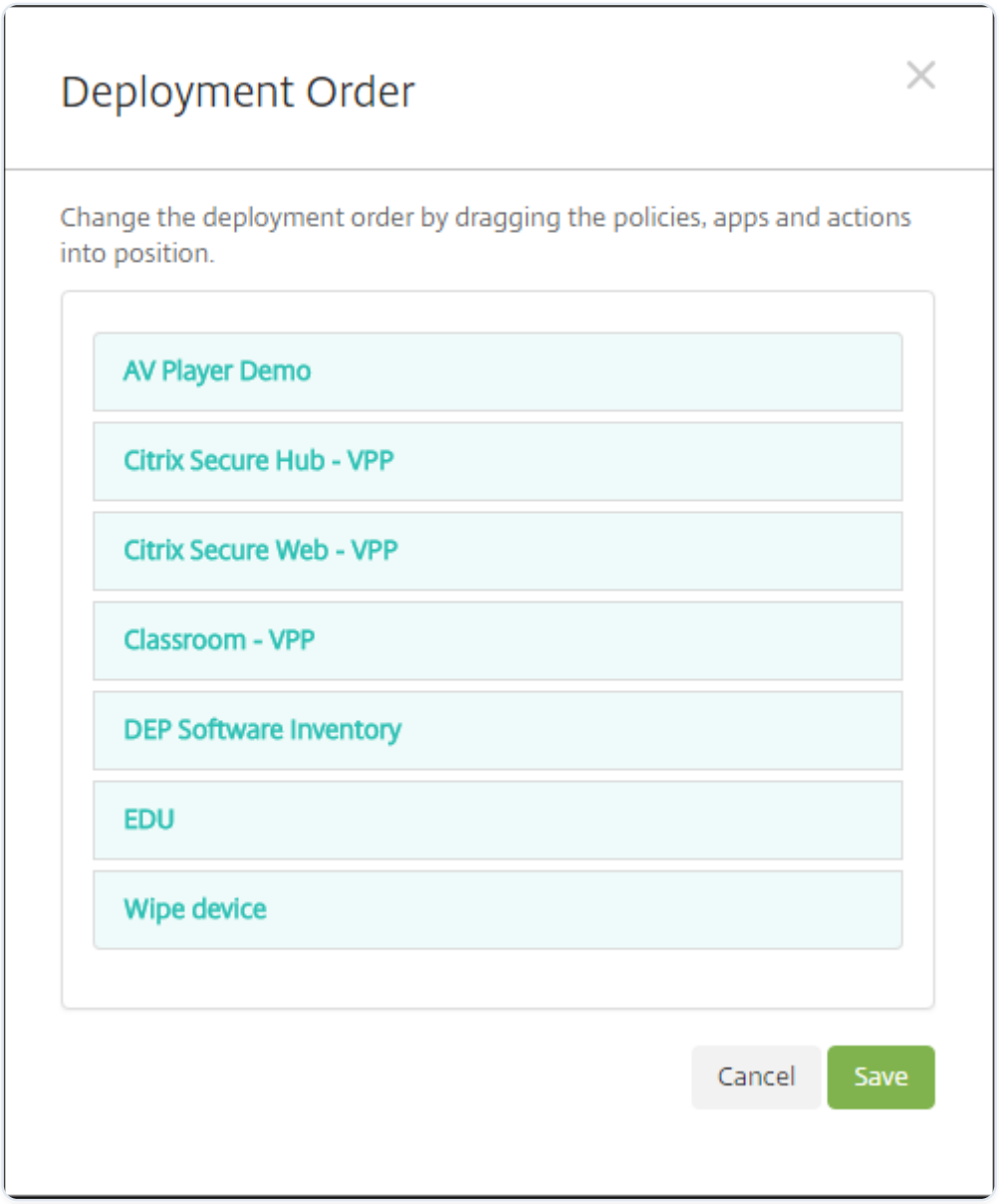


구성된 옵션 검토 및 배포 순서 변경



요약 페이지에서 전송 그룹에 대해 구성한 옵션을 검토하고 리소스의 배포 순서를 변경할 수 있습니다. 요약 페이지에는 범주별로 리소스가 표시됩니다. 요약 페이지는 배포 순서를 반영하지 않습니다.

1. 구성 변경이 필요한 경우 **뒤로**를 클릭하여 이전 페이지로 돌아갑니다.
2. 배포 순서를 보거나 다시 정렬하려면 **배포 순서**를 클릭합니다. **배포 순서** 대화 상자가 나타납니다.



3. 리소스를 클릭하여 배포하려는 위치로 끕니다. 배포 순서를 변경하면 XenMobile은 목록의 위에서 아래로 리소스를 배포합니다.
4. 배포 순서를 저장하려면 **저장**을 클릭합니다.
5. 전송 그룹을 저장하려면 **저장**을 클릭합니다.

전송 그룹 편집

기존 전송 그룹의 이름은 변경할 수 없습니다. 다른 설정을 업데이트하려면 **구성 > 전송 그룹**으로 이동하여 편집할 그룹을 선택한 다음 **편집**을 클릭합니다.

AllUsers 전송 그룹 활성화 및 비활성화

AllUsers는 활성화하거나 비활성화할 수 있는 유일한 전송 그룹입니다.

전송 그룹 페이지에서 **AllUsers** 옆의 확인란을 선택하거나 AllUsers가 포함된 줄을 클릭하여 AllUsers 전송 그룹을 선택합니다. 그런 다음 다음 중 하나를 수행합니다.

- **비활성화**를 클릭하여 AllUsers 배달 그룹을 비활성화합니다. 이 명령은 AllUsers가 활성화된 경우에만 사용할 수 있습니다(기본값). 배달 그룹 테이블의 **비활성화됨** 제목 아래에 **비활성화됨**이 나타납니다.
- **활성화**를 클릭하여 AllUsers 배달 그룹을 활성화합니다. 이 명령은 AllUsers가 비활성화된 경우에만 사용할 수 있습니다. 배달 그룹 테이블의 **비활성화됨** 제목 아래에서 **비활성화됨**이 사라집니다.

배달 그룹에 배포하려면

배달 그룹에 배포한다는 것은 iOS 및 Windows 태블릿 장치를 사용하는 모든 사용자에게 푸시 알림을 보내는 것을 의미합니다. 해당 사용자는 XenMobile에 다시 연결하려면 배달 그룹에 속해야 합니다. 이러한 방식으로 장치를 재평가하고 앱, 정책 및 작업을 배포할 수 있습니다.

다른 플랫폼 장치를 사용하는 사용자의 경우: 해당 장치가 이미 XenMobile에 연결되어 있는 경우, 즉시 리소스를 받습니다. 그렇지 않으면, 예약 정책에 따라 다음에 연결할 때 리소스를 받습니다. Android Enterprise 플랫폼의 사용자는 Firebase Cloud Messaging 알림 시스템에서 알림을 받은 다음 XenMobile Server에 연결하여 리소스를 검색합니다.

Android 장치의 XenMobile Store에서 업데이트된 앱이 '업데이트 가능' 목록에 표시되도록 하려면: 먼저 사용자 장치에 앱 인벤토리 정책을 배포합니다.

1. **배달 그룹** 페이지에서 다음 중 하나를 수행합니다.
   - 한 번에 둘 이상의 배달 그룹에 배포하려면, 배포하려는 그룹 옆의 확인란을 선택합니다.
   - 단일 배달 그룹에 배포하려면, 해당 이름 옆의 확인란을 선택하거나 해당 이름이 포함된 줄을 클릭합니다.
2. **배포**를 클릭합니다.

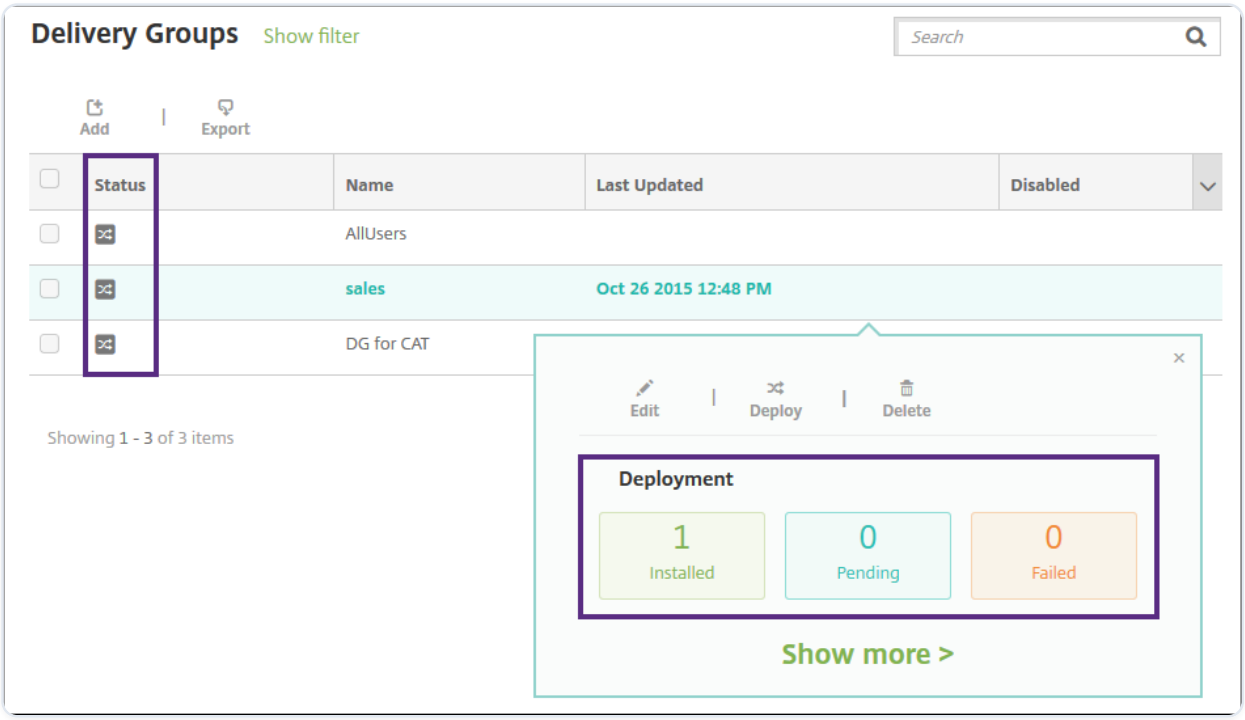
   단일 배달 그룹을 선택하는 방법에 따라, **배포** 명령이 배달 그룹 위 또는 오른쪽에 나타납니다.

   앱, 정책 및 작업을 배포하려는 그룹이 나열되어 있는지 확인한 다음 **배포**를 클릭합니다. 앱, 정책 및 작업은 장치 플랫폼 및 예약 정책에 따라 선택된 그룹에 배포됩니다.

   배달 그룹 페이지에서 다음 방법 중 하나로 배포 상태를 확인할 수 있습니다.

   - 배달 그룹의 **상태** 제목 아래에 있는 배포 아이콘을 확인하여 배포 실패 여부를 나타냅니다.

- 배달 그룹이 포함된 줄을 클릭하여 **설치됨**, **보류 중**, **실패** 배포를 나타내는 오버레이를 표시합니다.



전송 그룹을 복제하려면

기존 전송 그룹과 유사한 전송 그룹을 만들려면 전송 그룹을 복제합니다. 복제본을 새 전송 그룹의 시작점으로 사용합니다. 그런 다음 등록 프로필 또는 새로운 AD 사용자 세트 추가와 같이 복제본을 변경합니다.

1. XenMobile Server 콘솔에서 **구성**을 클릭한 다음 **전송 그룹** 탭을 선택합니다.
2. 전송 그룹 목록에서 새 그룹의 기반으로 사용할 그룹을 선택합니다.
3. **복제**를 선택합니다.
4. **전송 그룹 복제** 대화 상자에서 새 그룹의 이름과 설명(선택 사항)을 입력합니다.
5. **복제**를 선택합니다.

전송 그룹을 삭제하려면

AllUsers 전송 그룹은 삭제할 수 없지만, 모든 사용자에게 리소스를 푸시하지 않으려면 그룹을 비활성화할 수 있습니다.

1. **전송 그룹** 페이지에서 다음 중 하나를 수행합니다.
   - 한 번에 둘 이상의 전송 그룹을 삭제하려면 삭제할 그룹 옆의 확인란을 선택합니다.
   - 단일 전송 그룹을 삭제하려면 해당 이름 옆의 확인란을 선택하거나 이름이 포함된 줄을 클릭합니다.
2. **삭제**를 클릭합니다. **삭제** 대화 상자가 나타납니다.

단일 전송 그룹을 선택하는 방법에 따라 **삭제** 명령이 전송 그룹 위 또는 오른쪽에 나타납니다.

> **중요:**
>
> 삭제는 되돌릴 수 없습니다.

3. **삭제**를 클릭합니다.

딜리버리 그룹 테이블을 내보내려면

1. **딜리버리 그룹** 테이블 위에 있는 **내보내기** 버튼을 클릭합니다. XenMobile은 **딜리버리 그룹** 테이블의 정보를 추출하여 .csv 파일로 변환합니다.
2. 브라우저의 일반적인 단계에 따라 .csv 파일을 열거나 저장합니다. 작업을 취소할 수도 있습니다.

매크로

XenMobile®은 다음 항목의 텍스트 필드 내에서 사용자 또는 장치 속성 데이터를 채우는 방법으로 매크로를 제공합니다.

- 정책
- 알림
- 등록 템플릿
- 자동화된 작업
- 자격 증명 공급자 인증서 서명 요청

XenMobile은 매크로를 해당 사용자 또는 시스템 값으로 대체합니다. 예를 들어, 수천 명의 사용자에 걸쳐 단일 Exchange 프로필에서 사용자의 사서함 값을 미리 채울 수 있습니다.

매크로 구문

매크로는 다음 형식을 취할 수 있습니다.

- `${type.PROPERTYNAME}`
- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]}`

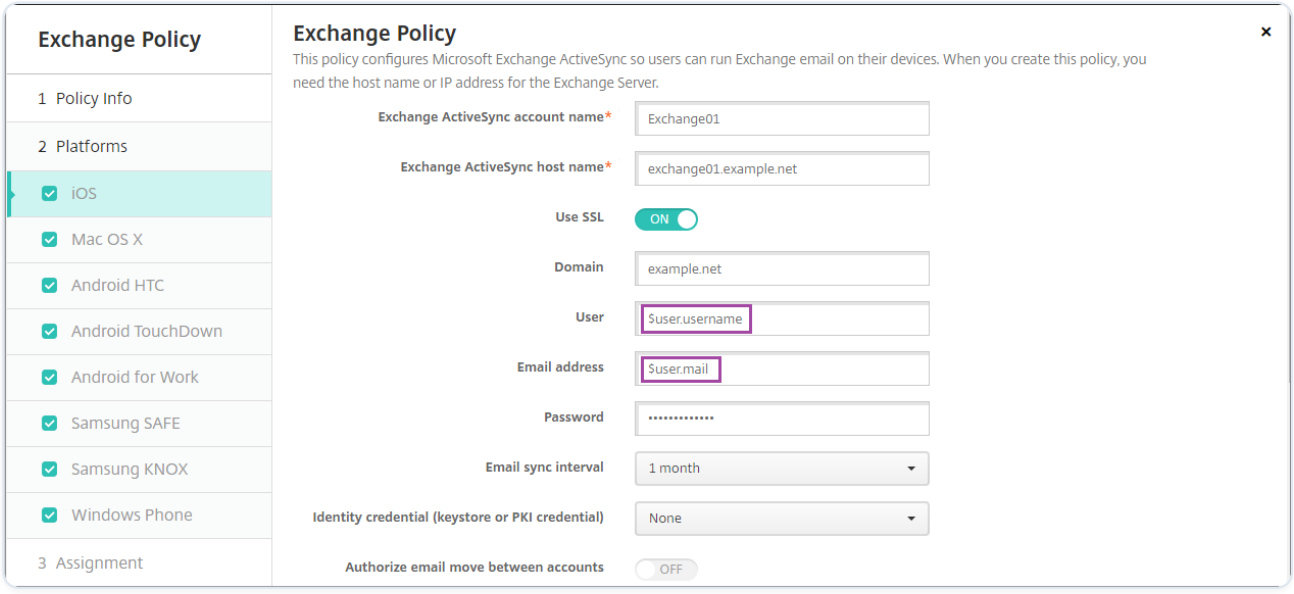
달러 기호($) 뒤에 오는 모든 구문은 중괄호({ })로 묶습니다.

- 정규화된 속성 이름은 사용자 속성, 장치 속성 또는 사용자 지정 속성을 참조합니다.

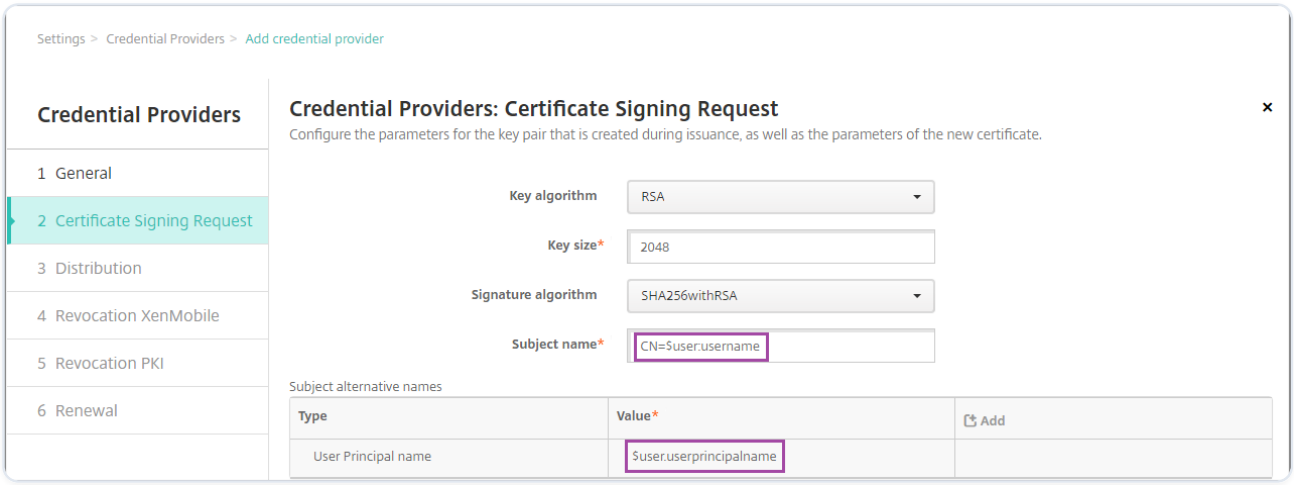
- 정규화된 속성 이름은 접두사 다음에 실제 속성 이름으로 구성됩니다.
- 사용자 속성은 `${user.[PROPERTYNAME] (prefix="user.")}` 형식입니다.
- 장치 속성은 `${device.[PROPERTYNAME] (prefix="device.")}` 형식입니다.
- 속성 이름은 대소문자를 구분합니다.
- 함수는 제한된 목록이거나 함수를 정의하는 타사 참조에 대한 링크일 수 있습니다. 알림 메시지에 대한 다음 매크로에는 **firstnotnull** 함수가 포함됩니다.

  장치 `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`이(가) 차단되었습니다...
- 사용자 지정 매크로(정의하는 속성)의 경우 접두사는 `${custom}`입니다. 접두사를 생략할 수 있습니다.

다음은 정책의 텍스트 필드에 사용자 이름 값을 채우는 데 일반적으로 사용되는 매크로 `${user.username}`의 예입니다. 이 매크로는 Exchange ActiveSync 프로필 및 여러 사용자가 사용하는 기타 프로필을 구성하는 데 유용합니다. 다음 예는 Exchange 정책에서 매크로를 사용하는 방법을 보여줍니다. **사용자**에 대한 매크로는 **`${user.username}`**입니다. **이메일 주소**에 대한 매크로는 **`${user.mail}`**입니다.

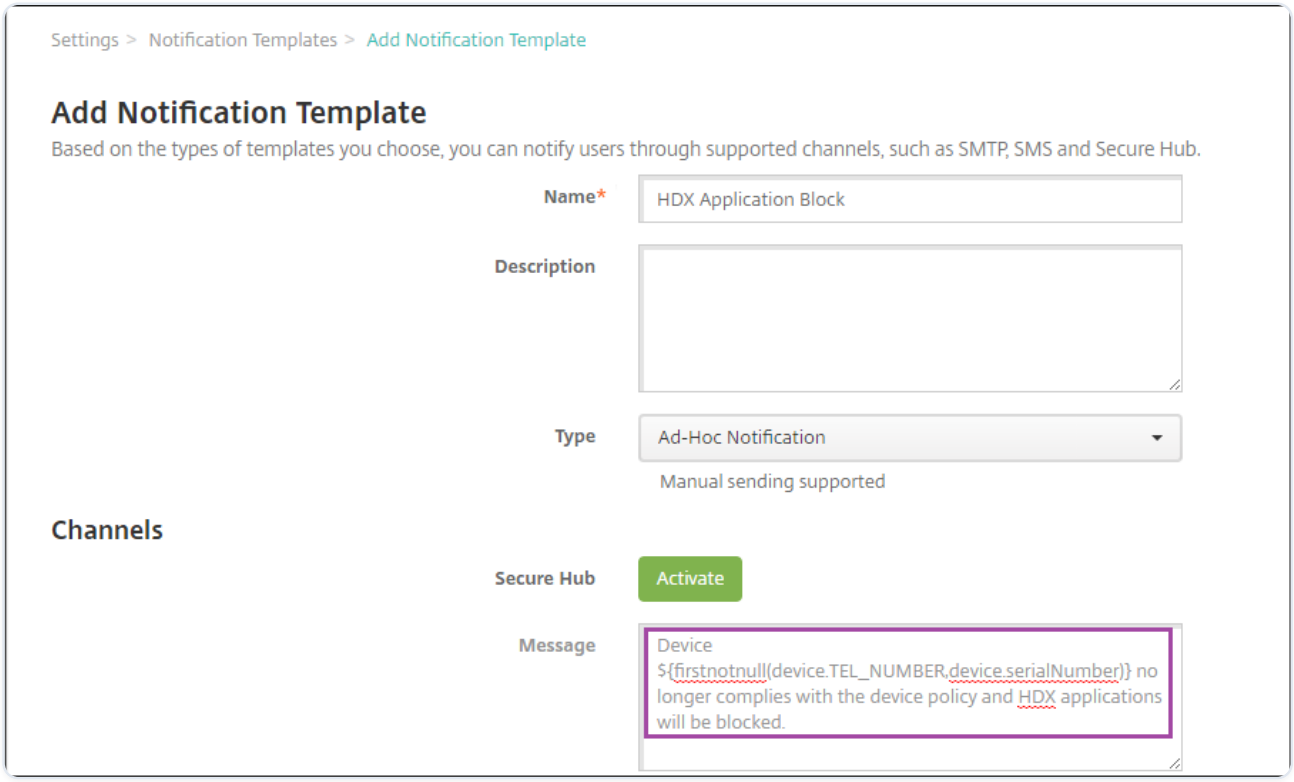


다음 예는 인증서 서명 요청에 매크로를 사용하는 방법을 보여줍니다. **주체 이름**에 대한 매크로는 **`CN=$user.username`**입니다. **주체 대체 이름**의 **값**에 대한 매크로는 **`$user.userprincipalname`**입니다.



다음 예는 알림 템플릿에서 매크로를 사용하는 방법을 보여줍니다. 예제 템플릿은 비준수 장치로 인해 HDX™ 애플리케이션이 차단될 때 사용자에게 전송되는 메시지를 정의합니다. **메시지**에 대한 매크로는 다음과 같습니다.

장치 `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`은(는) 더 이상 장치 정책을 따르지 않으며 HDX 애플리케이션이 차단됩니다.



알림에 사용되는 매크로의 더 많은 예시를 보려면 **설정 > 알림 템플릿**으로 이동하여 미리 정의된 템플릿을 선택한 다음 **편집**을 클릭합니다.

다음 예는 장치 이름 장치 정책의 매크로를 보여줍니다. 각 장치에 고유한 이름을 지정하기 위해 매크로, 매크로 조합 또는 매크로와 텍스트 조합을 입력할 수 있습니다. 예를 들어, 각 장치의 일련 번호로 장치 이름을 설정하려면 `${device.serialnumber}`을(를) 사용합니다. 장치 이름에 사용자 이름을 포함하려면 `$`

`{device.serialnumber} ${ user.username }`을(를) 사용합니다. 장치 이름 장치 정책은 감독되는 iOS 및 macOS 장치에서 작동합니다.

장치 정책 구성 화면의 매크로 이미지(/en-us/xenmobile/server/media/macro-example-device-name-policy.png)

기본 알림 템플릿용 매크로

기본 알림 템플릿에서 다음 매크로를 사용할 수 있습니다.

- `${account.SUPPORT_EMAIL}`
- `${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 포함되어 있습니다. 다가오는 릴리스에서는 이러한 용어를 "차단 목록" 및 "허용 목록"으로 변경할 예정입니다.

- `${vpp.account}`
- `${vpp.appname}`
- `${vpp.url}`
- `${zdmserver.hostPath}/enroll`

특정 정책에 대한 매크로

장치 이름 장치 정책(iOS 및 macOS용)의 경우 다음 매크로를 **장치 이름**에 사용할 수 있습니다.

- `${device.serialnumber}`
- `${user.username}@example.com`
- `${device.serialnumber}`
- `${device.serialnumber}`
- `${user.username}`
- `${enrollment.pin}`
- `${user.dnsroot}`

Webclip 장치 정책의 경우, **URL**에 이 매크로를 사용할 수 있습니다.

- `${webeas-url}`

Samsung MDM 라이선스 키 장치 정책의 경우, **ELM 라이선스 키**에 이 매크로를 사용할 수 있습니다.

- `${elm.license.key}`

내장 장치 속성을 얻기 위한 매크로

표시 이름	매크로
장치 ID	`$device.id`
장치 GUID	`$device.uniqueid`
장치 IMEI	`$device.imei`
OS 제품군	`$device.OSFamily`
일련 번호	`$device.serialNumber`

모든 장치 속성에 대한 매크로

다음 목록은 표시 이름, 웹 요소 및 매크로를 제공합니다.

계정 일시 중단됨?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED}

활성화 잠금 우회 코드

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE}

활성화 잠금 사용

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED}

활성 iTunes 계정

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

MSP에서 알려진 ActiveSync 장치

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP}

ActiveSync ID

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID}

관리자 비활성화됨

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED}

AIK 존재 여부?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT}

Amazon MDM API 사용 가능

- AMAZON_MDM
- ${device.AMAZON_MDM}

안드로이드 엔터프라이즈 장치 아이디

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID}

Android Enterprise 사용 장치?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE}

Android Enterprise 설치 유형

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE}

안티스파이웨어 시그니처 상태

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS}

안티스파이웨어 상태

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS}

안티바이러스 시그니처 상태

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS}

안티바이러스 상태

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS}

ASM DEP 활성화 잠금 우회 코드

- DEP_ACTIVATION_LOCK_BYPASS_CODE

- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}

ASM DEP 에스크로 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 저장 공간

- FREEDISK
- ${device.FREEDISK}

백업 배터리

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT}

베이스밴드 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}

MS에서 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}

블루투스 MAC 주소

- BLUETOOTH_MAC

- ${device.BLUETOOTH_MAC}

부팅 디버깅 사용?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}

부팅 관리자 개정 목록 버전

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}

이동통신사 코드

- CARRIER_CODE
- ${device.CARRIER_CODE}

이동통신사 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 암호 변경?

- 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 백업 사용

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED}

코드 무결성 사용?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}

코드 무결성 개정 목록 버전

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION}

색상

- COLOR
- ${device.COLOR}

CPU 클럭 속도

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED}

CPU 유형

- CPU_TYPE
- ${device.CPU_TYPE}

생성 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 통신사 네트워크

- CARRIER
- ${device.CARRIER}

현재 모바일 국가 코드

- CURRENT_MCC

- ${device.CURRENT_MCC}

현재 모바일 네트워크 코드

- CURRENT_MNC
- ${device.CURRENT_MNC}

데이터 로밍 허용됨

- 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 프로필 할당됨

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME}

DEP 프로필 푸시됨

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME}

DEP 프로필 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.DESCRIPTION}

장치 식별자

- 액티브싱크아이디
- ${device.activesyncid}

장치 모델

- SYSTEM_OEM
- ${device.SYSTEM_OEM}

장치 이름

- DEVICE_NAME
- ${device.DEVICE_NAME}

장치 유형

- DEVICE_TYPE
- ${device.DEVICE_TYPE}

방해 금지 모드 활성화됨

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB}

ELAM 드라이버 로드됨?

- 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 저장소 1: 사용 가능한 공간

- EXTERNAL_STORAGE1_FREE_SPACE
- ${device.EXTERNAL_STORAGE1_FREE_SPACE}

외부 저장소 1: 이름

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME}

외부 저장소 1: 총 공간

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE}

외부 저장소 2: 사용 가능한 공간

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE}

외부 저장소 2: 이름

- EXTERNAL_STORAGE2_NAME

- ${device.EXTERNAL_STORAGE2_NAME}

외부 저장소 2: 총 공간

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE}

외부 저장소 암호화됨

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION}

FileVault 활성화됨

- 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 동기화

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC}

Google 디렉터리 별칭

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}

Google 디렉터리 성

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}

Google 디렉터리 이름

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

Google 디렉터리 기본 이메일

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google 디렉터리 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 로그인된 iTunes Store 계정의 해시

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH}

홈 통신사 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}

식별

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY}

IMEI/MEID 번호

- IMEI
- ${device.IMEI}

IMSI

- SIM_ID
- ${device.SIM_ID}

내부 저장소 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}

발급일

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT}

탈옥/루팅됨

- ROOT_ACCESS
- ${device.ROOT_ACCESS}

커널 디버깅 사용?

- 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}

마지막 예약된 소프트웨어 업데이트

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}

마지막 예약된 소프트웨어 업데이트 실패 메시지

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}

마지막 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}

메인 배터리

- MAIN_BATTERY_PERCENT
- ${device.MAIN_BATTERY_PERCENT}

MDM 분실 모드 활성화됨

- 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 이메일

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL}

조직 매직

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC}

조직 이름

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME}

조직 전화번호

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE}

규정 미준수

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE}

소유자

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED}

암호 준수

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT}

구성 준수 암호

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG}

암호 존재

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT}

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0}

경계 위반

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH}

정기 점검

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck}

개인용 핫스팟 활성화됨

- PERSONAL_HOTSPOT_ENABLED

- ${device.PERSONAL_HOTSPOT_ENABLED}

지오펜스용 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 전화번호

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER}

기본 SIM 통신사

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}

기본 SIM ICCID

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID}

기본 SIM IMEI

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI}

기본 SIM IMSI

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI}

기본 SIM 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}

재시작 횟수

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT}

안전 모드 활성화됨?

- 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: X축 해상도

- SCREEN_XDPI
- ${device.SCREEN_XDPI}

화면: Y축 해상도

- SCREEN_YDPI
- ${device.SCREEN_YDPI}

보조 전화번호

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER}

보조 SIM 통신사

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}

보조 SIM ICCID

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID}

보조 SIM IMEI

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI}

보조 SIM IMSI

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI}

보조 SIM 로밍

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING}

보조 SIM 로밍 규정 준수

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE}

보안 부팅 사용 가능?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}

보안 부팅 상태

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE}

SecureContainer 사용 가능

- 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 사용 가능

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE}

감독됨

- SUPERVISED
- ${device.SUPERVISED}

정지 사유

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON}

변조 상태

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS}

이용 약관

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS}

이용 약관 동의 여부?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}

테스트 서명 활성화됨?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}

총 RAM

- MEMORY
- ${device.MEMORY}

총 저장 공간

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE}

TPM 버전

- TPM_VERSION
- ${device.TPM_VERSION}

UDID

- UDID

- ${device.UDID}

사용자 계정 컨트롤 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 통화 가능

- IS_VOICE_CAPABLE
- ${device.IS_VOICE_CAPABLE}

음성 로밍 허용됨

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED}

VSM 활성화됨?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED}

Wi-Fi MAC 주소

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY}

WinPE 사용 가능 여부?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE}

WNS 알림 상태

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS}

WNS 알림 URL

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL}

WNS 알림 URL 만료일

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY}

XenMobile 에이전트 ID

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID}

XenMobile 에이전트 개정

- 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}

내장 사용자 속성을 얻기 위한 매크로

표시 이름	매크로
domainname (도메인 이름; 기본 도메인)	`${user.domainname}`
loginname (사용자 이름 + 도메인 이름)	`${user.loginname}`
username (로그인 이름에서 도메인 제외, 있는 경우)	`${user.username}`

모든 사용자 속성에 대한 매크로

표시 이름	웹 요소	매크로
Active Directory 실패한 로그온 시도	잘못된 비밀번호 횟수	`${user.badpwdcount}`

표시 이름	웹 요소	매크로
ActiveSync 사용자 이메일	사용자 이메일	`${user.asuseremail}`
ASM 데이터 소스	사용자 소스	`${user.aspersonsource}`
ASM DEP 계정 이름	DEP 계정	`${user.asmdepaccount}`
ASM 관리형 Apple ID	사용자 관리형 Apple ID	`${user.aspersonmanagedappleid}`
ASM 암호 유형	사용자 암호 유형	`${user.aspersonpasscodetype}`
ASM 사용자 ID	아스엠퍼슨아이디	`${user.aspersonid}`
ASM 사용자 상태	아스엠퍼슨스테이터스	`${user.aspersonstatus}`
ASM 사용자 직함	아스엠퍼슨타이틀	`${user.aspersontitle}`
ASM 사용자 고유 ID	아스엠퍼슨유니크아이디	`${user.aspersonuniqueid}`
ASM 소스 시스템 ID	아스엠퍼슨소스시스템아이디	`${user.aspersonsourcesystemid}`
ASM 학생 등급	에이에스엠퍼슨그레이드	`${user.aspersongrade}`
BES 사용자 이메일	비이에스유저이메일	`${user.besuseremail}`
회사	회사	`${user.company}`
회사 이름	회사 이름	`${user.companyname}`
국가	c	`${user.c}`
부서	부서	`${user.department}`
설명	설명	`${user.description}`

표시 이름	웹 요소	매크로
비활성화된 사용자	비활성화된 사용자	`${user.disableduser}`
표시 이름	표시 이름	`${user.displayname}`
고유 이름	고유 이름	`${user.distinguishedname}`
도메인 이름	도메인 이름	`${user.domainname}`
이메일	메일	`${user.mail}`
이름	이름	`${user.givenname}`
집 주소	집 주소	`${user.homestreetaddress}`
거주 도시	거주 도시	`${user.homecity}`
거주 국가	거주 국가	`${user.homecountry}`
자택 팩스	자택 팩스	`${user.homefax}`
자택 전화	자택 전화	`${user.homephone}`
자택 주/지역	거주 주	`${user.homestate}`
자택 우편번호	자택 우편번호	`${user.homezip}`
IP 전화	IP 전화	`${user.ipphone}`
중간 이니셜	중간 이니셜	`${user.middleinitial}`
중간 이름	중간 이름	`${user.middlename}`
모바일	모바일	`${user.mobile}`
이름	cn	`${user.cn}`
사무실 주소	물리적 배송 사무실 이름	`${user.physicaldeliveryofficename}`

표시 이름	웹 요소	매크로
사무실 도시	l	`${user.l}`
사무실 팩스 번호	팩스 전화번호	`${user.facsimiletelephonenumber}`
사무실 주/도	st	`${user.st}`
사무실 도로명 주소	사무실 주소	`${user.officestreetaddress}`
사무실 전화번호	전화번호	`${user.telephonenumber}`
사무실 우편번호	우편번호	`${user.postalcode}`
사서함	사서함	`${user.postofficebox}`
호출기	호출기	`${user.pager}`
기본 그룹 ID	기본 그룹 ID	`${user.primarygroupid}`
SAM 계정	SAM 계정 이름	`${user.samaccountname}`
거리 주소	거리 주소	`${user.streetaddress}`
성	sn	`${user.sn}`
직함	직함	`${user.title}`
사용자 로그온 이름	사용자 계정 이름	`${user.userprincipalname}`

자동화된 작업

XenMobile®에서 자동화된 작업을 생성하여 이벤트, 사용자 또는 장치 속성, 또는 사용자 장치에 앱이 존재하는 것에 대한 반응을 프로그래밍할 수 있습니다. 자동화된 작업을 생성할 때, 해당 작업에 대해 정의된 트리거는 사용자 장치가 XenMobile에 연결될 때 어떤 일이 발생하는지 결정합니다. 이벤트가 트리거되면, 더 심각한 조치가 취해지기 전에 사용자에게 문제를 해결하도록 알림을 보낼 수 있습니다.

자동으로 발생하도록 설정하는 효과는 다음과 같습니다.

- 장치를 완전히 또는 선택적으로 초기화합니다.
- 장치를 규정 미준수 상태로 설정합니다.
- 장치를 해지합니다.
- 더 심각한 조치가 취해지기 전에 사용자에게 문제를 해결하도록 알림을 보냅니다.

MAM 전용 모드에 대해 앱 잠금 및 앱 초기화 작업을 구성할 수 있습니다.

> **참고:**
>
> 사용자에게 알림을 보내려면 XenMobile이 메시지를 보낼 수 있도록 XenMobile 설정에서 SMTP 및 SMS에 대한 알림 서버를 구성해야 합니다. 자세한 내용은 알림을 참조하십시오. 또한, 진행하기 전에 사용할 알림 템플릿을 설정하십시오. 자세한 내용은 알림 템플릿 생성 및 업데이트를 참조하십시오.

작업 예시

자동화된 작업을 사용하는 몇 가지 예시는 다음과 같습니다.

예시 1

- 이전에 차단한 앱(예: “Words with Friends”)을 감지하려고 합니다. “Words with Friends” 앱을 감지한 후 사용자 장치를 규정 미준수 상태로 설정하는 트리거를 지정할 수 있습니다. 그러면 해당 작업은 사용자에게 장치를 규정 준수 상태로 되돌리려면 앱을 제거해야 한다고 알립니다. 또한, 사용자가 규정을 준수할 때까지 기다릴 시간 제한을 설정할 수도 있습니다. 해당 시간 제한이 지나면 장치를 선택적으로 초기화하는 것과 같은 정의된 작업이 발생합니다.

예시 2

- 고객이 최신 펌웨어를 사용하고 있는지 확인하고, 사용자가 장치를 업데이트해야 하는 경우 리소스에 대한 액세스를 차단하려고 합니다. 사용자 장치가 최신 버전을 가지고 있지 않을 때 사용자 장치를 규정 미준수 상태로 설정하는 트리거를 지정할 수 있습니다. 자동화된 작업을 사용하여 리소스를 차단하고 고객에게 알릴 수 있습니다.

예시 3

- 사용자 장치가 규정 미준수 상태가 되었다가 사용자가 장치를 수정합니다. 장치를 규정 준수 상태로 재설정하는 패키지를 배포하도록 정책을 구성할 수 있습니다.

예시 4

- 특정 기간 동안 비활성 상태였던 사용자 장치를 규정 미준수로 표시하려고 합니다. 비활성 장치에 대해 다음과 같이 자동화된 작업을 생성할 수 있습니다.

  a. XenMobile 콘솔에서 **설정 > 네트워크 액세스 제어**로 이동한 다음 **비활성 장치**를 선택합니다. **비활성 장치** 설정에 대한 자세한 내용은 네트워크 액세스 제어를 참조하십시오.

  b. 작업 추가 및 관리에 설명된 대로 작업을 추가하는 단계를 따릅니다. 유일한 차이점은 **작업 세부 정보** 페이지에서 다음과 같이 설정을 구성한다는 것입니다.

  - **트리거**. **장치 속성**, **규정 미준수**, **True**를 선택합니다.
  - **작업**. **알림 보내기**를 선택하고 **설정**의 **알림 템플릿**을 사용하여 생성한 템플릿을 선택합니다. 그런 다음 작업을 수행하기 전 지연 시간을 일, 시간 또는 분 단위로 설정합니다. 사용자가 트리거 문제를 해결할 때까지 작업이 반복되는 간격을 설정합니다.

> **팁:**
>
> 비활성 장치를 대량으로 삭제하려면 REST 서비스용 공용 API를 사용하십시오. 먼저 삭제하려는 비활성 장치의 장치 ID를 수동으로 가져온 다음 삭제 API를 실행하여 대량으로 삭제합니다.

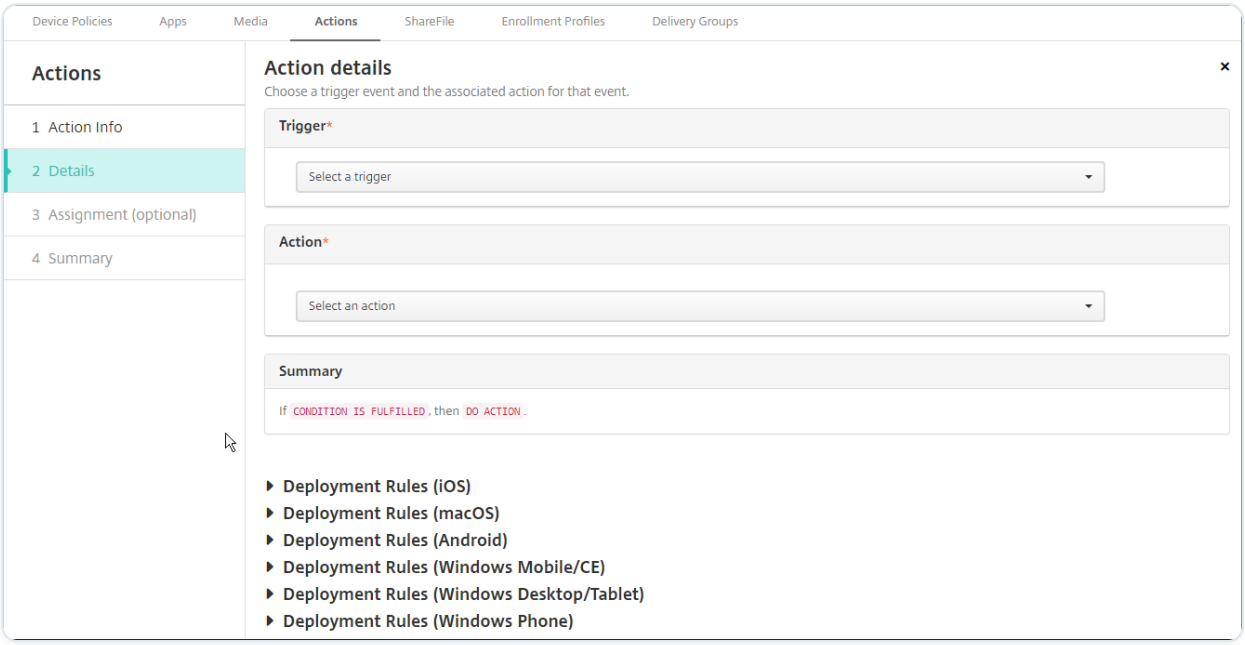
작업 추가 및 관리

자동화된 작업을 추가, 편집 및 필터링하려면 다음을 수행합니다.

1. XenMobile 콘솔에서 **구성 > 작업**을 클릭합니다. **작업** 페이지가 나타납니다.
2. **작업** 페이지에서 다음 중 하나를 수행합니다.
   - 작업을 추가하려면 **추가**를 클릭합니다.
   - 편집하거나 삭제할 기존 작업을 선택합니다. 사용하려는 옵션을 클릭합니다.

3. **작업 정보** 페이지가 나타납니다.
4. **작업 정보** 페이지에서 다음 정보를 입력하거나 수정합니다.
   - **이름:** 작업을 식별할 이름을 입력합니다. 이 필드는 필수입니다.
   - **설명:** 작업이 수행하도록 의도된 내용을 설명합니다.
5. **다음**을 클릭합니다. **작업 세부 정보** 페이지가 나타납니다.

   다음 예는 **이벤트** 트리거를 설정하는 방법을 보여줍니다. 다른 트리거를 선택하면 결과 옵션이 여기에 표시된 옵션과 다릅니다.



6. **작업 세부 정보** 페이지에서 다음 정보를 입력하거나 수정합니다.

   트리거 목록에서 이 작업에 대한 이벤트 트리거 유형을 클릭합니다. 각 트리거의 의미는 다음과 같습니다.

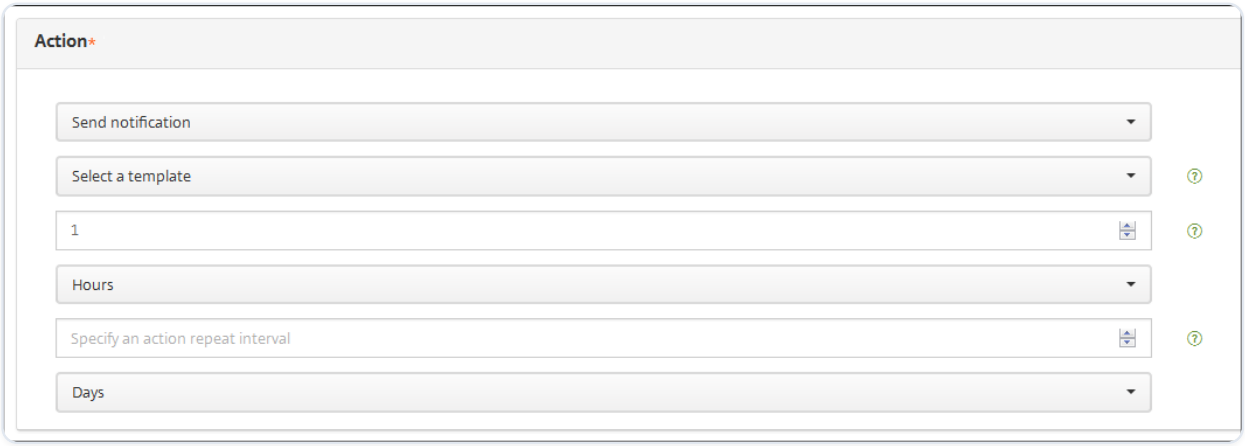
   - **이벤트:** 미리 정의된 이벤트에 반응합니다.
   - **장치 속성:** MDM 관리 장치에서 장치 속성을 확인한 다음 이에 반응합니다. 자세한 내용은 장치 속성 이름 및 값을 참조하십시오.
   - **사용자 속성:** 일반적으로 Active Directory의 사용자 속성에 반응합니다.
   - **설치된 앱 이름:** 앱이 설치되는 것에 반응합니다. MAM 전용 모드에는 적용되지 않습니다. 장치에서 앱 인벤토리 정책을 활성화해야 합니다. 앱 인벤토리 정책은 기본적으로 모든 플랫폼에서 활성화됩니다. 자세한 내용은 앱 인벤토리 장치 정책을 참조하십시오.
7. 다음 목록에서 트리거에 대한 응답을 클릭합니다.

8. **작업** 목록에서 트리거 조건이 충족될 때 수행할 작업을 클릭합니다. **알림 보내기**를 제외하고, 사용자가 트리거를 유발한 문제를 해결할 수 있는 기간을 선택합니다. 해당 기간 내에 문제가 해결되지 않으면 선택한 작업이 수행됩니다. 작업에 대한 정의는 보안 작업을 참조하십시오.

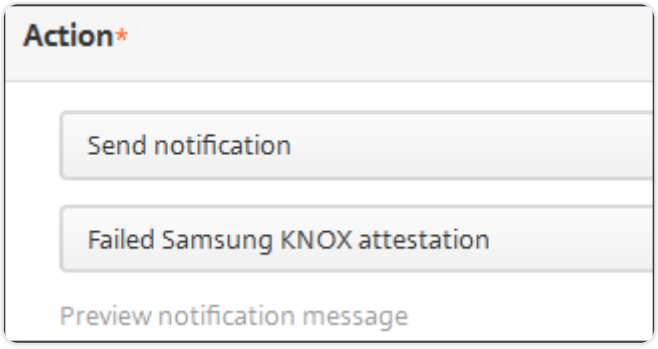
   알림 보내기를 선택하는 경우 다음 단계에 따라 알림 작업을 보냅니다.

9. 다음 목록에서 알림에 사용할 템플릿을 선택합니다. 선택한 이벤트와 관련된 알림 템플릿이 나타나지만, 해당 알림 유형에 대한 템플릿이 아직 없는 경우에는 다음 메시지와 함께 템플릿을 구성하라는 메시지가 표시됩니다. 이 이벤트 유형에 대한 템플릿이 없습니다. **설정**에서 **알림 템플릿**을 사용하여 템플릿을 만드십시오.

   사용자에게 알림을 보내려면 XenMobile이 메시지를 보낼 수 있도록 SMTP 및 SMS 설정에서 알림 서버를 구성해야 합니다. 알림을 참조하십시오. 또한 진행하기 전에 사용할 알림 템플릿을 설정하십시오. 알림 템플릿 설정에 대한 자세한 내용은 알림 템플릿 생성 및 업데이트를 참조하십시오.



   템플릿을 선택한 후 **알림 메시지 미리 보기**를 클릭하여 알림을 미리 볼 수 있습니다.



10. 다음 필드에서 작업을 수행하기 전 지연 시간을 일, 시간 또는 분 단위로 설정합니다. 사용자가 트리거 문제를 해결할 때까지 작업이 반복되는 간격을 설정합니다.



11. **요약**에서 의도한 대로 자동화된 작업을 생성했는지 확인합니다.



12. 작업 세부 정보를 구성한 후 각 플랫폼에 대한 배포 규칙을 개별적으로 구성할 수 있습니다. 이렇게 하려면 선택한 각 플랫폼에 대해 13단계를 완료하십시오.
13. 배포 규칙을 구성합니다. 배포 규칙 구성에 대한 일반적인 정보는 리소스 배포를 참조하십시오.

    이 예시의 경우:

    - 장치 소유권은 **BYOD**여야 합니다.
    - 장치 로컬 암호화는 **True**여야 합니다.
    - 장치는 암호 정책을 준수해야 합니다.
    - 장치 모바일 국가 코드는 안도라만 될 수 없습니다.

14. 작업에 대한 플랫폼 배포 규칙 구성을 마치면 **다음**을 클릭합니다. **작업 할당** 페이지가 나타나며, 여기서 하나 이상의 배달 그룹에 작업을 할당합니다. 이 단계는 선택 사항입니다.
15. **배달 그룹 선택** 옆에서 배달 그룹을 찾거나 목록에서 그룹을 선택하려면 입력합니다. 선택한 그룹은 **앱 할당을 받을 배달 그룹** 목록에 나타납니다.
16. 배포 일정을 확장한 다음 다음 설정을 구성합니다.

    - **배포** 옆에서 배포를 예약하려면 **켜기**를 클릭하거나 배포를 방지하려면 **끄기**를 클릭합니다. 기본 옵션은 **켜기**로 설정되어 있습니다. **끄기**를 선택하면 다른 옵션은 필요하지 않습니다.
    - **배포 일정** 옆에서 **지금** 또는 **나중에**를 클릭합니다. 기본 옵션은 **지금**으로 설정되어 있습니다.
    - **나중에**를 클릭하면 달력 아이콘을 클릭한 다음 배포 날짜와 시간을 선택합니다.
    - **배포 조건** 옆에서 **모든 연결 시**를 클릭하거나 **이전 배포가 실패한 경우에만**을 클릭합니다. 기본 옵션은 **모든 연결 시**로 설정되어 있습니다.
    - **항상 켜짐 연결에 배포** 옆에서 **켜기** 또는 **끄기**를 클릭합니다. 기본 옵션은 **끄기**로 설정되어 있습니다.

      이 옵션은 **설정 > 서버 속성**에서 예약 백그라운드 배포 키를 구성한 경우에 적용됩니다. 항상 켜짐 옵션은 iOS 장치에서는 사용할 수 없습니다.

    구성하는 배포 일정은 모든 플랫폼에서 동일합니다. 수정하는 모든 변경 사항은 모든 플랫폼에 적용됩니다. 단, iOS에는 적용되지 않는 **항상 켜짐 연결에 배포**는 예외입니다.

17. **다음**을 클릭합니다. **요약** 페이지가 나타나며, 여기서 작업 구성을 확인할 수 있습니다.
18. **저장**을 클릭하여 작업을 저장합니다.

MAM 전용 모드용 앱 잠금 및 앱 초기화 작업

XenMobile 콘솔에 나열된 다음 네 가지 범주의 트리거(이벤트, 장치 속성, 사용자 속성 및 설치된 앱 이름)에 대한 응답으로 장치에서 앱을 초기화하거나 잠글 수 있습니다.

자동 앱 초기화 또는 앱 잠금을 구성하려면

1. XenMobile 콘솔에서 **구성 > 작업**을 클릭합니다.
2. **작업** 페이지에서 **추가**를 클릭합니다.
3. **작업 정보** 페이지에서 작업 이름을 입력하고 선택적 설명을 입력합니다.
4. **작업 세부 정보** 페이지에서 원하는 트리거를 선택합니다.
5. **작업**에서 작업을 선택합니다.

   이 단계에서는 다음 조건을 염두에 두십시오.

   트리거 유형이 **이벤트**로 설정되어 있고 값이 **Active Directory 비활성화된 사용자**가 아닌 경우 **앱 초기화** 및 **앱 잠금** 작업이 나타나지 않습니다.

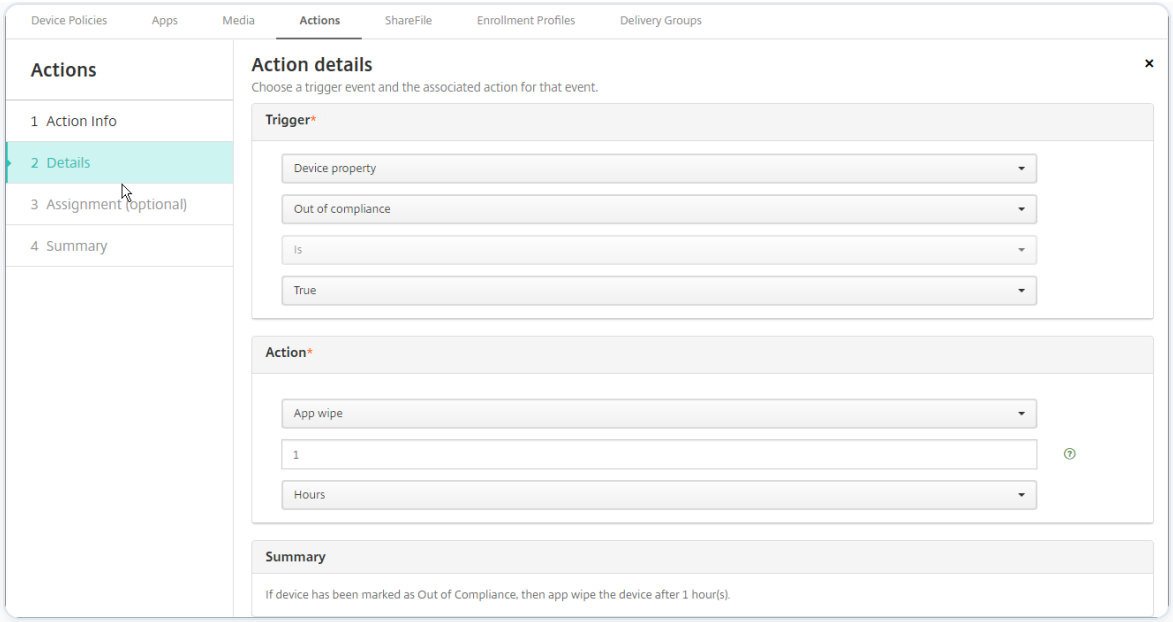
   트리거 유형이 **장치 속성**으로 설정되어 있고 값이 **MDM 분실 모드 사용**인 경우 다음 작업이 나타나지 않습니다.

   - 장치를 선택적으로 초기화
   - 장치를 완전히 초기화
   - 장치 해지

   각 옵션에 대해 1시간 지연이 자동으로 설정되지만, 지연 기간을 분, 시간 또는 일 단위로 선택할 수 있습니다. 지연의 목적은 작업이 발생하기 전에 사용자가 문제를 해결할 시간을 주기 위함입니다. 앱 초기화 및 앱 잠금 작업에 대한 자세한 내용은 보안 작업을 참조하십시오.

> **참고:**
>
> 트리거를 **event**로 설정하면 반복 간격이 자동으로 최소 1시간으로 설정됩니다. 알림이 수신되려면 장치가 서버와 동기화하기 위해 정책을 새로 고쳐야 합니다. 일반적으로 장치는 사용자가 로그인하거나 Secure Hub를 통해 정책을 수동으로 새로 고칠 때 서버와 동기화됩니다.

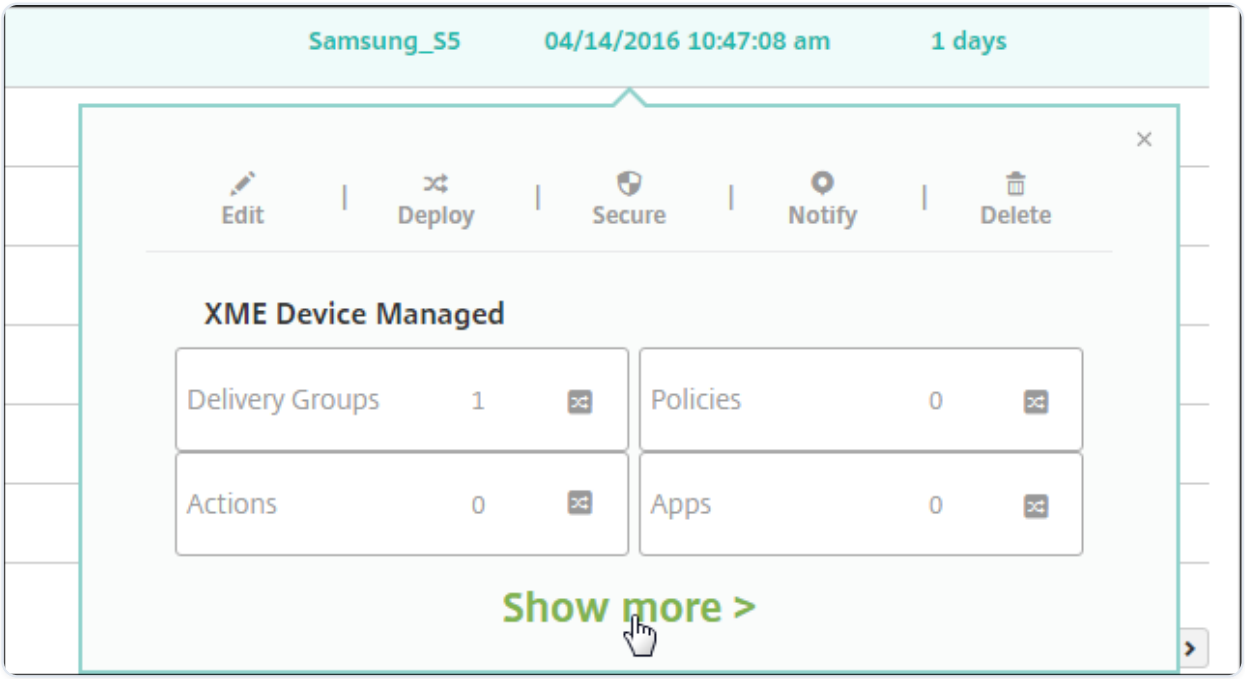
Active Directory 데이터베이스가 XenMobile과 동기화되도록 허용하기 위해 작업이 수행되기 전에 약 1시간의 추가 지연이 발생할 수 있습니다.



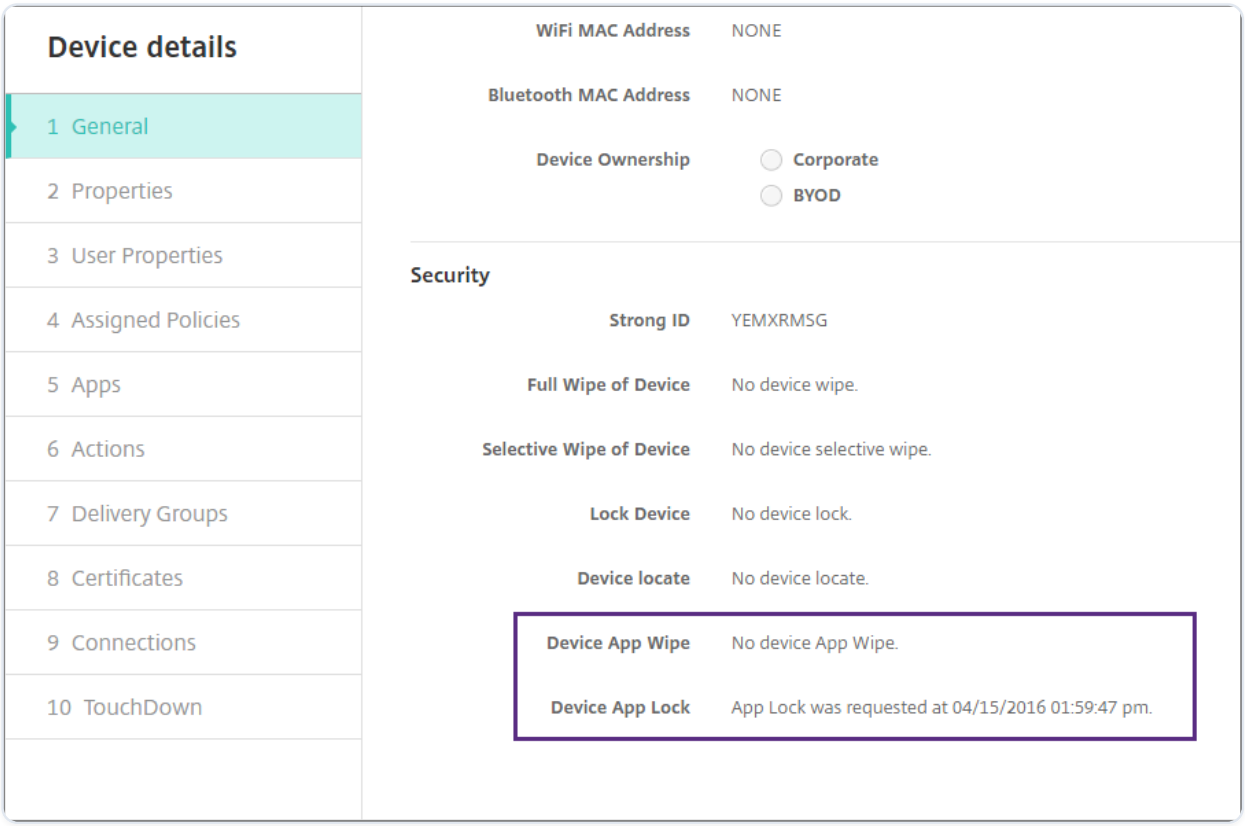
6. 배포 규칙을 구성한 다음 **다음**을 클릭합니다.
7. 배달 그룹 할당 및 배포 일정을 구성한 다음 **다음**을 클릭합니다.
8. **저장**을 클릭합니다.

앱 잠금 또는 앱 초기화 상태를 확인하려면

1. **관리 > 장치**로 이동하여 장치를 클릭한 다음 **자세히 보기**를 클릭합니다.



2. **장치 앱 초기화** 및 **장치 앱 잠금**으로 스크롤합니다.



장치가 초기화되면 사용자에게 PIN 코드를 입력하라는 메시지가 표시됩니다. 사용자가 코드를 잊어버린 경우 장치 세부 정보에서 찾을 수 있습니다.

모니터링 및 지원

XenMobile® 대시보드 및 XenMobile 지원 페이지를 사용하여 XenMobile Server를 모니터링하고 문제를 해결할 수 있습니다. XenMobile 지원 페이지를 사용하여 지원 관련 정보 및 도구에 액세스하십시오.

온프레미스 XenMobile Server의 경우 XenMobile CLI에서 작업을 수행할 수도 있습니다. 자세한 내용은 명령줄 인터페이스 옵션을 참조하십시오.

XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 렌치 아이콘을 클릭합니다.

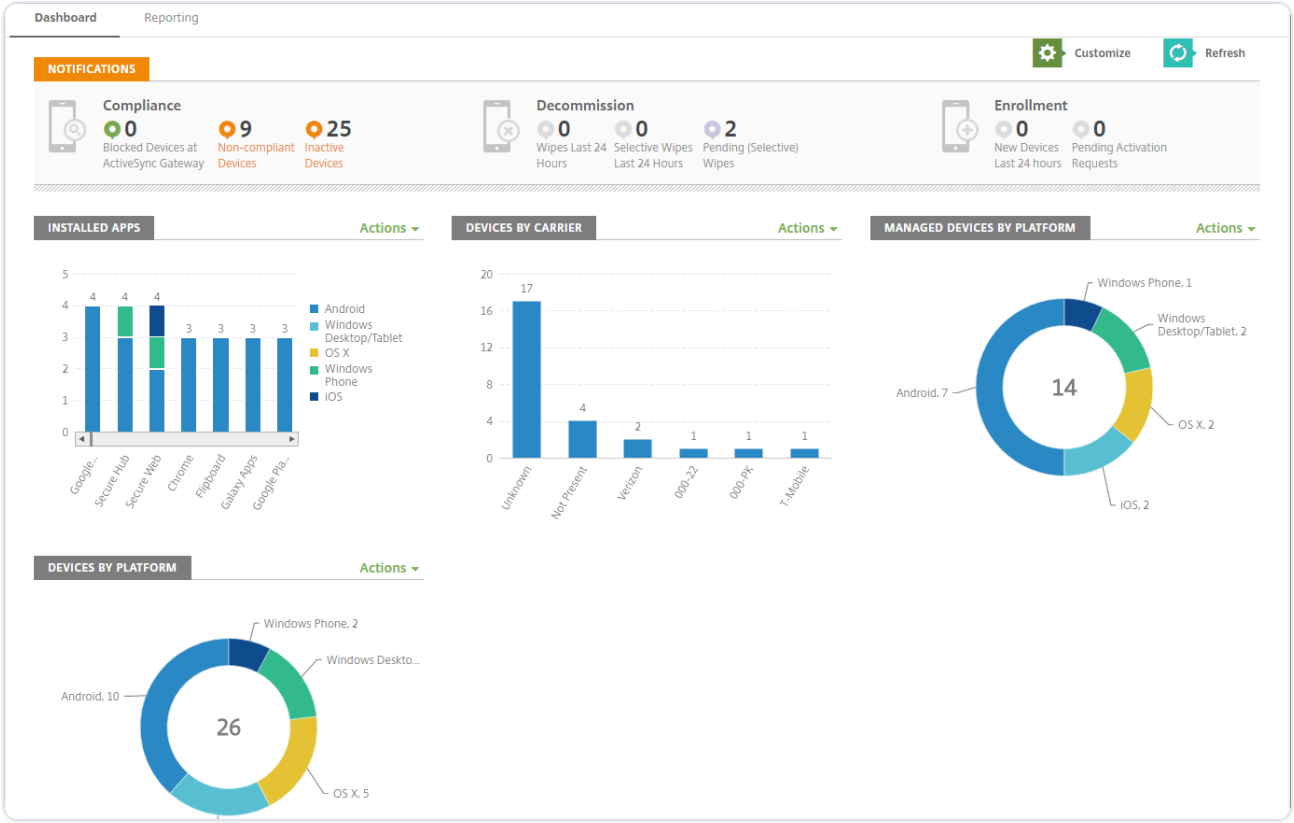


문제 해결 및 지원 페이지가 나타납니다.

XenMobile **지원** 페이지를 사용하여 다음을 수행합니다.

- 진단에 액세스합니다.
- 지원 번들을 생성합니다(온프레미스 설치에만 해당).
- Citrix 제품 설명서 및 지식 센터 링크에 액세스합니다.
- 로그 작업에 액세스합니다.
- 고급 구성 옵션을 사용합니다.
- 도구 및 유틸리티 세트에 액세스합니다.

XenMobile 콘솔 대시보드에 액세스하여 정보를 한눈에 볼 수도 있습니다. 이 정보를 통해 위젯을 사용하여 문제와 성공 여부를 빠르게 확인할 수 있습니다.



대시보드는 일반적으로 XenMobile 콘솔에 로그인할 때 처음 나타나는 페이지입니다. 콘솔의 다른 곳에서 대시보드에 액세스하려면 **분석**을 클릭합니다. 대시보드에서 **사용자 지정**을 클릭하여 페이지 레이아웃을 편집하고 표시되는 위젯을 편집합니다.

- **내 대시보드:** 최대 4개의 대시보드를 저장할 수 있습니다. 이 대시보드를 개별적으로 편집하고 저장된 대시보드를 선택하여 각 대시보드를 볼 수 있습니다.
- **레이아웃 스타일:** 이 행에서 대시보드에 표시되는 위젯 수와 위젯이 배치되는 방식을 선택할 수 있습니다 .
- **위젯 선택:** 대시보드에 표시할 정보를 선택할 수 있습니다.
  - **알림:** 왼쪽에 있는 숫자 위에 있는 확인란을 선택하여 위젯 위에 알림 표시줄을 추가합니다. 이 표시줄은 지난 24시간 동안 규정 준수 장치, 비활성 장치, 초기화되거나 등록된 장치의 수를 보여줍니다.
  - **플랫폼별 장치:** 플랫폼별 관리 및 비관리 장치 수를 표시합니다.
  - **통신사별 장치:** 통신사별 관리 및 비관리 장치 수를 표시합니다. 각 막대를 클릭하여 플랫폼별 분석을 볼 수 있습니다.
  - **플랫폼별 관리 장치:** 플랫폼별 관리 장치 수를 표시합니다.
  - **플랫폼별 비관리 장치:** 플랫폼별 비관리 장치 수를 표시합니다. 이 차트에 나타나는 장치에는 에이전트가 설치되어 있을 수 있지만, 권한이 취소되었거나 초기화되었을 수 있습니다.

- **ActiveSync Gateway 상태별 장치:** ActiveSync Gateway 상태별로 그룹화된 장치 수를 표시합니다. 정보는 차단됨, 허용됨 또는 알 수 없음 상태를 보여줍니다. 각 막대를 클릭하여 플랫폼별로 데이터를 분석할 수 있습니다.
- **소유권별 장치:** 소유권 상태별로 그룹화된 장치 수를 표시합니다. 정보는 회사 소유, 직원 소유 또는 알 수 없는 소유권 상태를 보여줍니다.
- **실패한 배달 그룹 배포:** 패키지당 실패한 배포의 총 수를 표시합니다. 배포에 실패한 패키지만 나타납니다.
- **차단 이유별 장치:** ActiveSync에 의해 차단된 장치 수를 표시합니다.
- **설치된 앱:** 앱 정보 그래프를 보려면 앱 이름을 입력합니다.
- **볼륨 구매 앱 라이선스 사용량:** Apple 볼륨 구매 앱의 라이선스 사용 통계를 표시합니다.

각 위젯에서 개별 부분을 클릭하여 더 자세한 정보를 드릴다운할 수 있습니다.

분석 대시보드 드릴다운 이미지(/en-us/xenmobile/server/media/analyze-dashboard-drill-down.png)

작업 메뉴를 클릭하여 정보를 .csv 파일로 내보낼 수도 있습니다.

분석 대시보드 메뉴 이미지(/en-us/xenmobile/server/media/analyze-dashboard-actions-menu.png)

지원 번들의 데이터 익명화

XenMobile®에서 지원 번들을 생성할 때 민감한 사용자, 서버 및 네트워크 데이터는 기본적으로 익명화됩니다. 이 동작은 익명화 및 익명 해제 페이지에서 변경할 수 있습니다. 또한 XenMobile이 데이터를 익명화할 때 저장하는 매핑 파일을 다운로드할 수 있습니다. Citrix® 지원팀은 이 파일을 요청하여 데이터를 익명 해제하고 특정 사용자 또는 장치의 문제를 찾을 수 있습니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 렌치 아이콘을 클릭합니다. **지원** 페이지가 나타납니다.
2. **지원** 페이지의 **고급** 아래에서 **익명화 및 익명 해제**를 클릭합니다. **익명화 및 익명 해제** 페이지가 나타납니다.

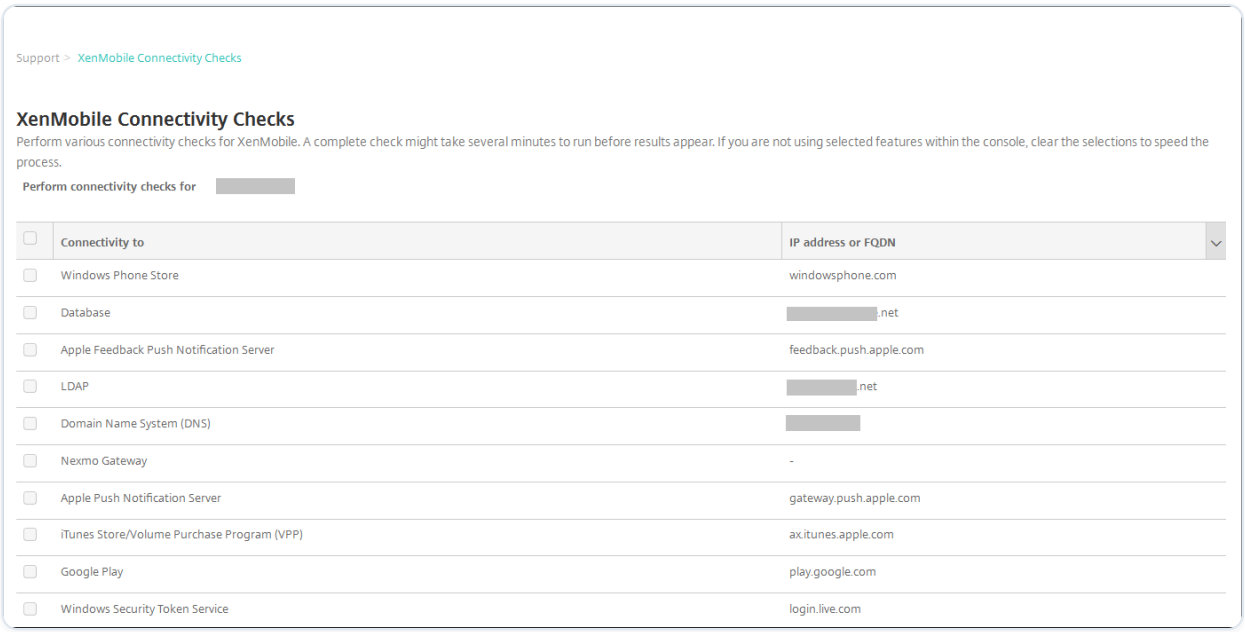
   데이터 익명화 구성 이미지(/en-us/xenmobile/server/media/anonymize-data-screen.png)
3. **지원 번들 익명화**에서 데이터가 익명화되는지 여부를 선택합니다. 기본값은 **켜짐**입니다.
4. **익명 해제** 옆에서 **익명 해제 파일 다운로드**를 클릭하여 Citrix 지원팀이 문제를 진단하기 위해 특정 장치 또는 사용자 정보가 필요할 때 보낼 매핑 파일을 다운로드합니다.

연결 확인

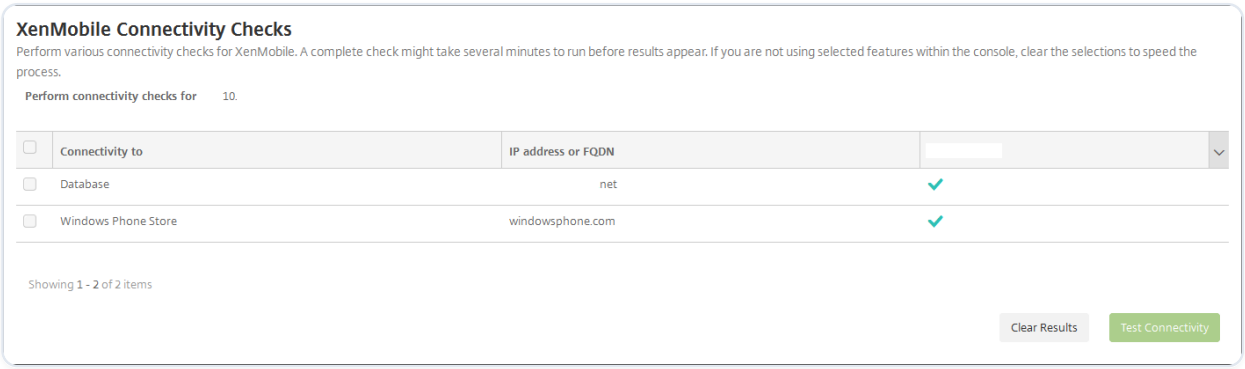
XenMobile® **Support** 페이지에서 Citrix Gateway 및 기타 서버와 위치에 대한 XenMobile 연결을 확인할 수 있습니다.

XenMobile 연결 확인 수행

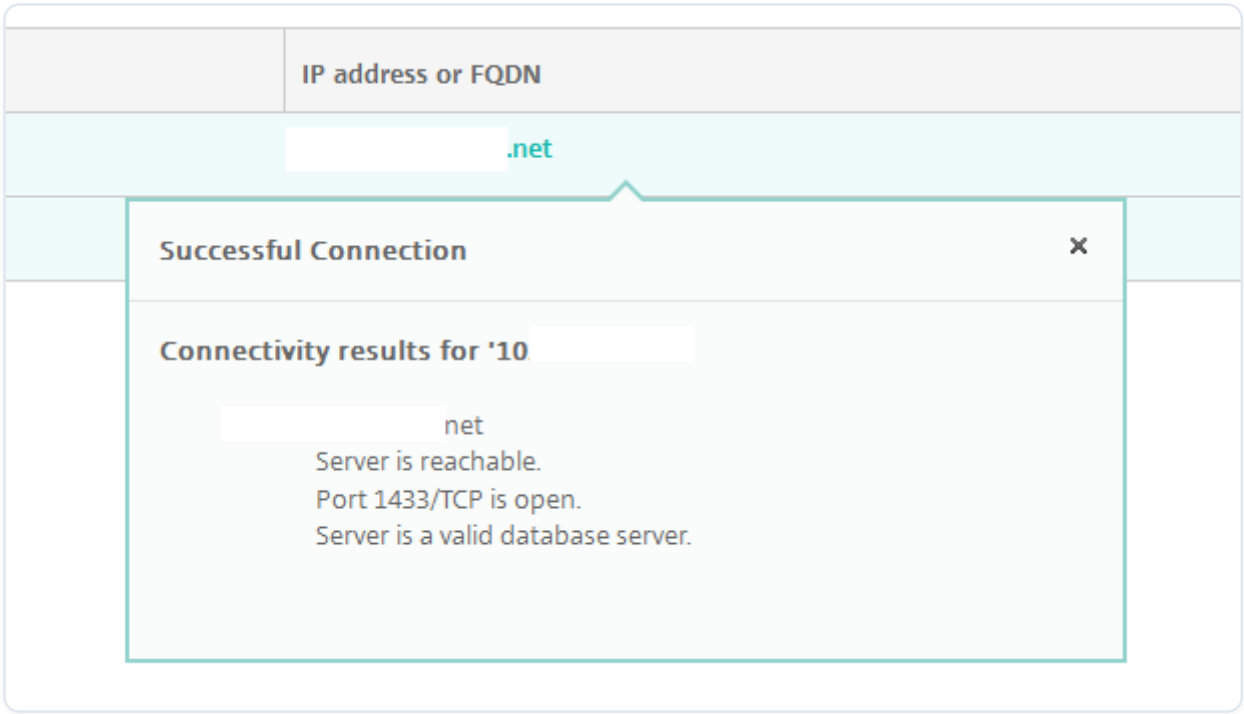
1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 렌치 아이콘을 클릭합니다. **Support** 페이지가 나타납니다.
2. **Diagnostics** 아래에서 **XenMobile Connectivity Checks**를 클릭합니다. **XenMobile Connectivity Checks** 페이지가 나타납니다. XenMobile 환경에 클러스터된 노드가 있는 경우 모든 노드가 표시됩니다.



3. 연결 테스트에 포함할 서버를 선택한 다음 **Test Connectivity**를 클릭합니다. 테스트 결과 페이지가 나타납니다.

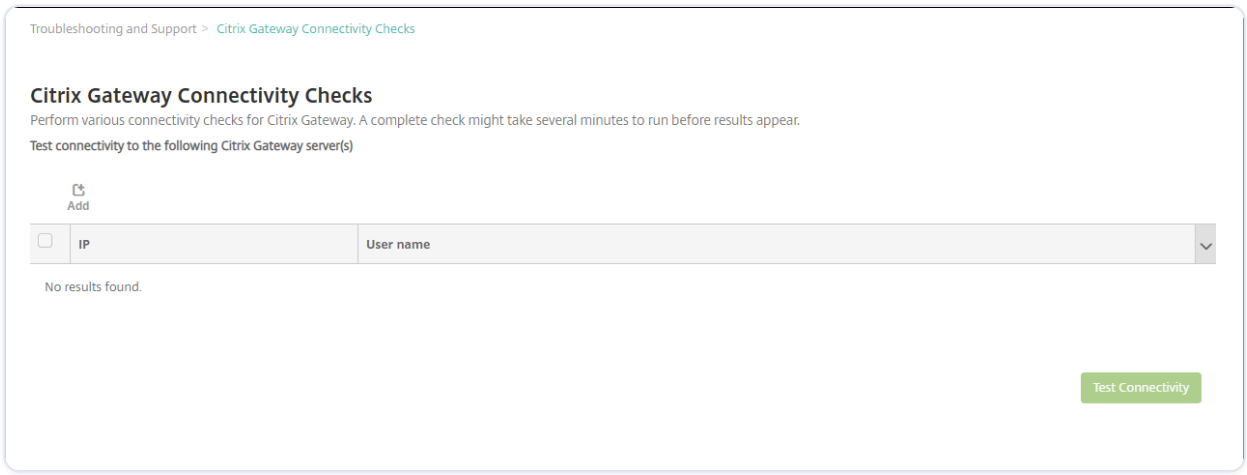


4. 테스트 결과 테이블에서 서버를 선택하여 해당 서버에 대한 자세한 결과를 확인합니다.

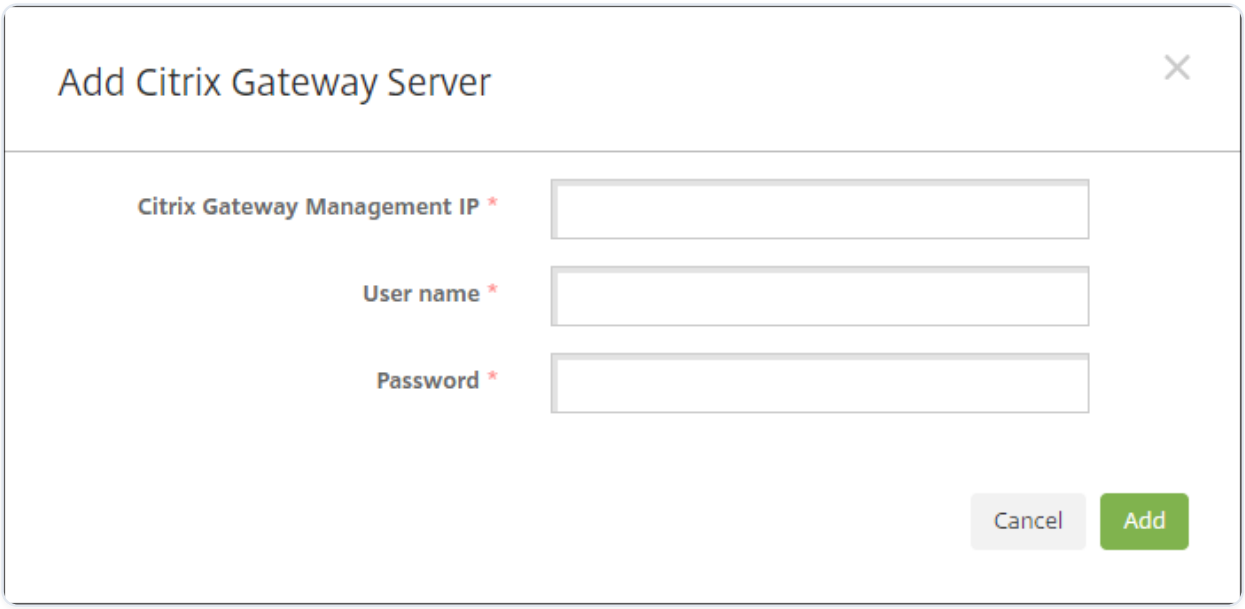


Citrix Gateway 연결 확인 수행

1. **Support** 페이지의 **Diagnostics** 아래에서 **Citrix Gateway Connectivity Checks**를 클릭합니다. **Citrix Gateway Connectivity Checks** 페이지가 나타납니다. Citrix Gateway 서버를 추가하지 않은 경우 테이블이 비어 있습니다.



2. **Add**를 클릭합니다. **Add Citrix Gateway Server** 대화 상자가 나타납니다.



3. **Citrix Gateway Management IP**에서 테스트하려는 Citrix Gateway를 실행하는 서버의 관리 IP 주소를 입력합니다.

> **참고:**
>
> 이미 추가된 Citrix Gateway 서버에 대해 연결 확인을 수행하는 경우 IP 주소가 제공됩니다.

4. 이 Citrix Gateway에 대한 관리자 자격 증명을 입력합니다.

> **참고:**
>
> 이미 추가된 Citrix Gateway 서버에 대해 연결 확인을 수행하는 경우 사용자 이름이 제공됩니다.

5. **추가**를 클릭합니다. Citrix Gateway가 **Citrix Gateway 연결 확인** 페이지의 테이블에 추가됩니다.
6. Citrix Gateway 서버를 선택한 다음 **연결 테스트**를 클릭합니다. 결과가 테스트 결과 테이블에 나타납니다.
7. 테스트 결과 테이블에서 서버를 선택하여 해당 서버에 대한 자세한 결과를 확인합니다.

고객 경험 향상 프로그램

Citrix 고객 경험 향상 프로그램(CEIP)은 XenMobile에서 익명 구성 및 사용 데이터를 수집하여 Citrix로 자동으로 전송합니다. 이 데이터는 Citrix가 XenMobile의 품질, 안정성 및 성능을 개선하는 데 도움이 됩니다. CEIP 참여는 자발적입니다. XenMobile을 처음 설치하거나 업데이트를 설치할 때 CEIP에 참여할 수 있습니

다. 참여를 선택하면 데이터는 일반적으로 매주 수집되며, 성능 및 사용 데이터는 매시간 수집됩니다. 데이터는 디스크에 저장되고 매주 HTTPS를 통해 Citrix로 안전하게 전송됩니다. XenMobile 콘솔에서 CEIP 참여 여부를 변경할 수 있습니다. CEIP에 대한 자세한 내용은 Citrix 고객 경험 향상 프로그램(CEIP) 정보를 참조하십시오.

CEIP 참여 선택

XenMobile®을 처음 설치하거나 업데이트할 때 참여를 요청하는 다음 대화 상자가 나타납니다.

CEIP 이미지(/en-us/xenmobile/server/media/ceip-first-time-use.png)

CEIP 참여 설정 변경

1. XenMobile 콘솔에서 CEIP 참여 설정을 변경하려면 콘솔의 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭하여 **설정** 페이지를 엽니다.
2. **서버** 아래에서 **경험 향상 프로그램**을 클릭합니다. **고객 경험 향상 프로그램** 페이지가 나타납니다. 표시되는 정확한 페이지는 현재 CEIP에 참여하고 있는지 여부에 따라 달라집니다.

   CEIP 설정 이미지(/en-us/xenmobile/server/media/settings-server-ceip.png)
3. 현재 CEIP에 참여하고 있으며 중단하려면 **참여 중지**를 클릭합니다.
4. 현재 CEIP에 참여하고 있지 않으며 시작하려면 **참여 시작**을 클릭합니다.
5. **저장**을 클릭합니다.

로그

XenMobile®이 생성하는 로그의 출력을 사용자 지정하도록 로그 설정을 구성할 수 있습니다. XenMobile 콘솔에서 로그 설정을 구성할 때 클러스터링된 XenMobile 서버가 있는 경우, 해당 설정은 클러스터의 다른 모든 서버와 공유됩니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단에 있는 렌치 아이콘을 클릭합니다. **지원** 페이지가 나타납니다.
2. **로그 작업** 아래에서 **로그 설정**을 클릭합니다. **로그 설정** 페이지가 나타납니다.

   로깅 구성 이미지(/en-us/xenmobile/server/media/support-log-settings.png)

   로그 설정 페이지에서 다음 옵션에 액세스할 수 있습니다.

   - **로그 크기**. 이 옵션을 사용하여 로그 파일의 크기와 데이터베이스에 보관되는 최대 로그 백업 파일 수를 제어합니다. 로그 크기는 XenMobile에서 지원하는 각 로그(디버그 로그, 관리자 활동 로그 및 사용자 활동 로그)에 적용됩니다.
   - **로그 수준**. 이 옵션을 사용하여 로그 수준을 변경하거나 설정을 유지합니다.

- **사용자 지정 로거**. 이 옵션을 사용하여 사용자 지정 로거를 생성합니다. 사용자 지정 로그에는 클래스 이름과 로그 수준이 필요합니다.

로그 크기 옵션 구성

1. **로그 설정** 페이지에서 **로그 크기**를 확장합니다.

   로깅 구성 이미지(/en-us/xenmobile/server/media/support-log-settings-log-size.png)

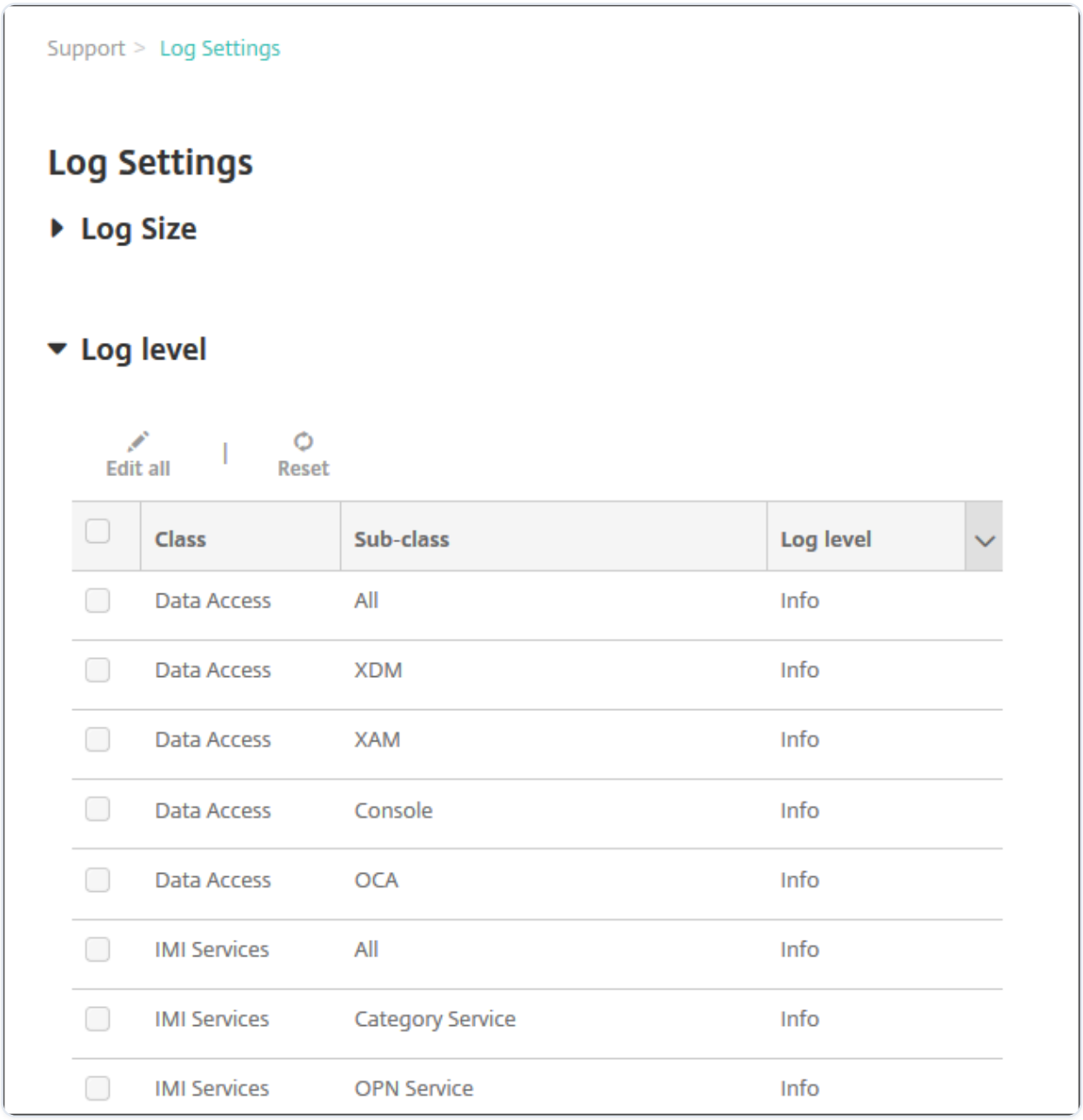
2. 다음 설정을 구성합니다.

   - **디버그 로그 파일 크기(MB):** 목록에서 5MB에서 20MB 사이의 크기를 클릭하여 디버그 파일의 최대 크기를 변경합니다. 기본 파일 크기는 **10MB**입니다.
   - **최대 디버그 백업 파일 수:** 목록에서 서버에 보관되는 최대 디버그 파일 수를 클릭합니다. 기본적으로 XenMobile은 서버에 50개의 백업 파일을 보관합니다.
   - **관리자 활동 로그 파일 크기(MB):** 목록에서 5MB에서 20MB 사이의 크기를 클릭하여 관리자 활동 파일의 최대 크기를 변경합니다. 기본 파일 크기는 **10MB**입니다.
   - **관리자 활동 백업 파일의 최대 개수:** 목록에서 서버가 보관하는 관리자 활동 파일의 최대 개수를 클릭합니다. 기본적으로 XenMobile은 서버에 300개의 백업 파일을 보관합니다.
   - **사용자 활동 로그 파일 크기(MB):** 목록에서 5MB에서 20MB 사이의 크기를 클릭하여 사용자 활동 파일의 최대 크기를 변경합니다. 기본 파일 크기는 **10MB**입니다.
   - **사용자 활동 백업 파일의 최대 개수:** 목록에서 서버가 보관하는 사용자 활동 파일의 최대 개수를 클릭합니다. 기본적으로 XenMobile은 서버에 300개의 백업 파일을 보관합니다.

로그 수준 옵션을 구성하려면

로그 수준을 통해 XenMobile이 로그에 수집하는 정보 유형을 지정할 수 있습니다. 모든 클래스에 동일한 수준을 설정하거나 개별 클래스에 특정 수준을 설정할 수 있습니다.

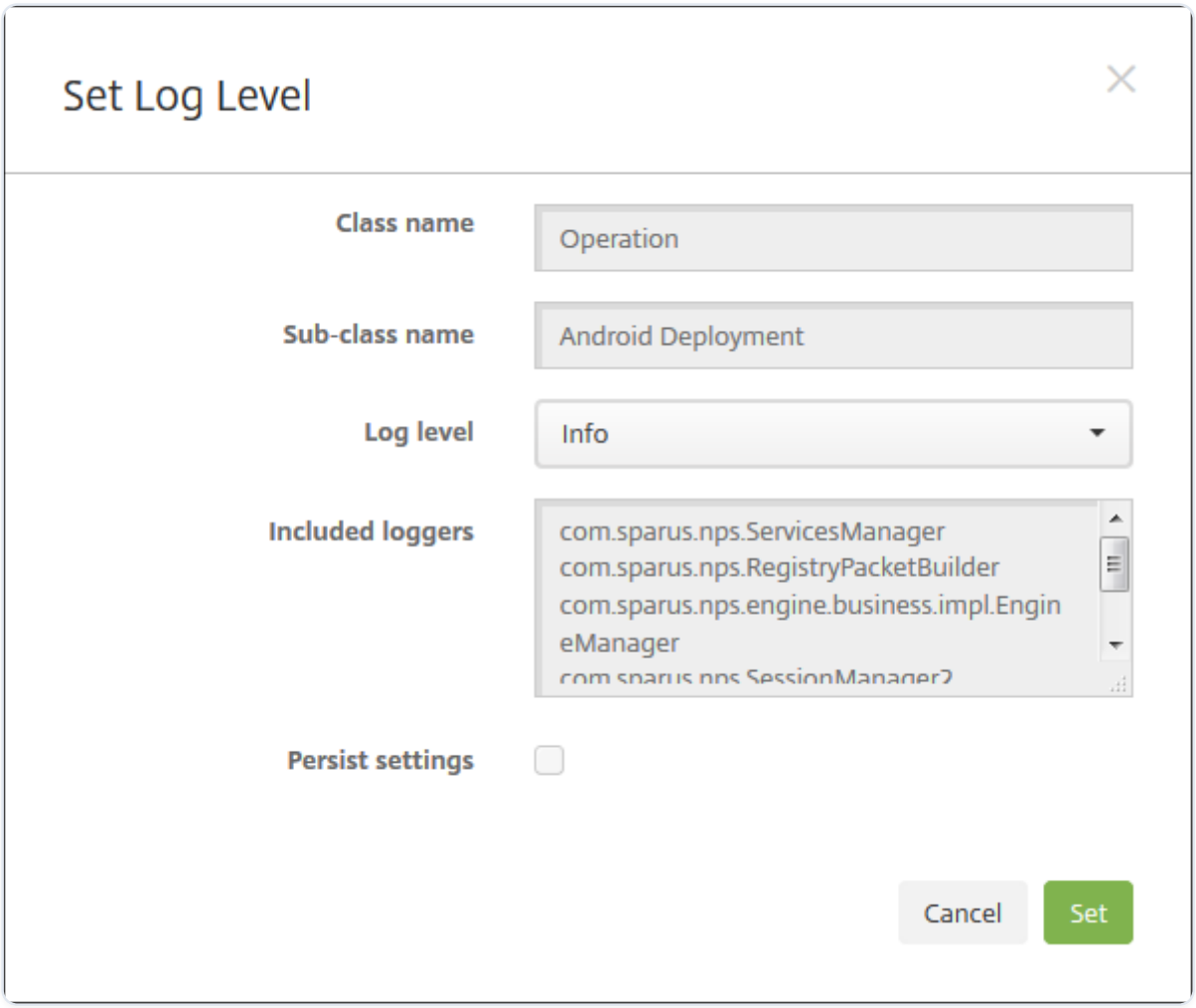
1. **로그 설정** 페이지에서 **로그 수준**을 확장합니다. 모든 로그 클래스 테이블이 나타납니다.



2. 다음 중 하나를 수행합니다.

   - 하나의 클래스 옆에 있는 확인란을 클릭한 다음 **수준 설정**을 클릭하여 이 클래스의 로그 수준만 변경합니다.
   - **모두 편집**을 클릭하여 테이블의 모든 클래스에 로그 수준 변경 사항을 적용합니다.

   로그 수준 설정 대화 상자가 나타나면 로그 수준을 설정하고 XenMobile Server를 재부팅할 때 로그 수준 설정이 유지되도록 할지 여부를 선택할 수 있습니다.



- **클래스 이름**: 이 필드는 모든 클래스의 로그 수준을 변경할 때 **모두**를 표시하거나 개별 클래스 이름을 표시합니다. 편집할 수 없습니다.
- **하위 클래스 이름**: 이 필드는 모든 클래스의 로그 수준을 변경할 때 **모두**를 표시하거나 개별 클래스 하위 클래스 이름을 표시합니다. 편집할 수 없습니다.
- **로그 수준**: 목록에서 로그 수준을 클릭합니다. 지원되는 로그 수준은 다음과 같습니다.
  - 치명적
  - 오류
  - 경고
  - 정보
  - 디버그
  - 추적
  - 끄기
- **포함된 로거**: 이 필드는 모든 클래스에 대한 로그 수준을 변경할 때 비어 있거나 개별 클래스에 대해 현재 구성된 로거를 표시합니다. 편집할 수 없습니다.

- **설정 유지**: 서버를 재부팅할 때 로그 수준 설정을 유지하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 서버를 재부팅할 때 로그 수준 설정이 기본값으로 되돌아갑니다.

3. 변경 사항을 적용하려면 **설정**을 클릭합니다.

사용자 지정 로거를 추가하려면

1. **로그 설정** 페이지에서 **사용자 지정 로거**를 확장합니다. **사용자 지정 로거** 테이블이 나타납니다. 사용자 지정 로거를 추가하지 않은 경우 테이블은 처음에는 비어 있습니다.

   로깅 구성 이미지(/en-us/xenmobile/server/media/support-log-settings-custom-logger.png)

2. **추가**를 클릭합니다. **사용자 지정 로거 추가** 대화 상자가 나타납니다.

   로깅 구성 이미지(/en-us/xenmobile/server/media/support-log-settings-custom-logger-add.png)

3. 다음 설정을 구성합니다:

   - **클래스 이름:** 이 필드에는 **사용자 지정**이 표시됩니다. 편집할 수 없습니다.
   - **로그 수준:** 목록에서 로그 수준을 클릭합니다. 지원되는 로그 수준은 다음과 같습니다:
     - 치명적
     - 오류
     - 경고
     - 정보
     - 디버그
     - 추적
     - 끄기
   - **포함된 로거:** 사용자 지정 로거에 포함할 특정 로거를 입력하거나 필드를 비워 두어 모든 로거를 포함합니다.

4. **추가**를 클릭합니다. 사용자 지정 로거가 **사용자 지정 로거** 테이블에 추가됩니다.

   로깅 구성 이미지(/en-us/xenmobile/server/media/support-log-settings-custom-logger-table.png)

사용자 지정 로거를 삭제하려면

1. **로그 설정** 페이지에서 **사용자 지정 로거**를 확장합니다.
2. 삭제하려는 사용자 지정 로거를 선택합니다.
3. **삭제**를 클릭합니다. 사용자 지정 로거를 삭제할지 묻는 대화 상자가 나타납니다. **확인**을 클릭합니다.

중요:

이 작업은 실행 취소할 수 없습니다.

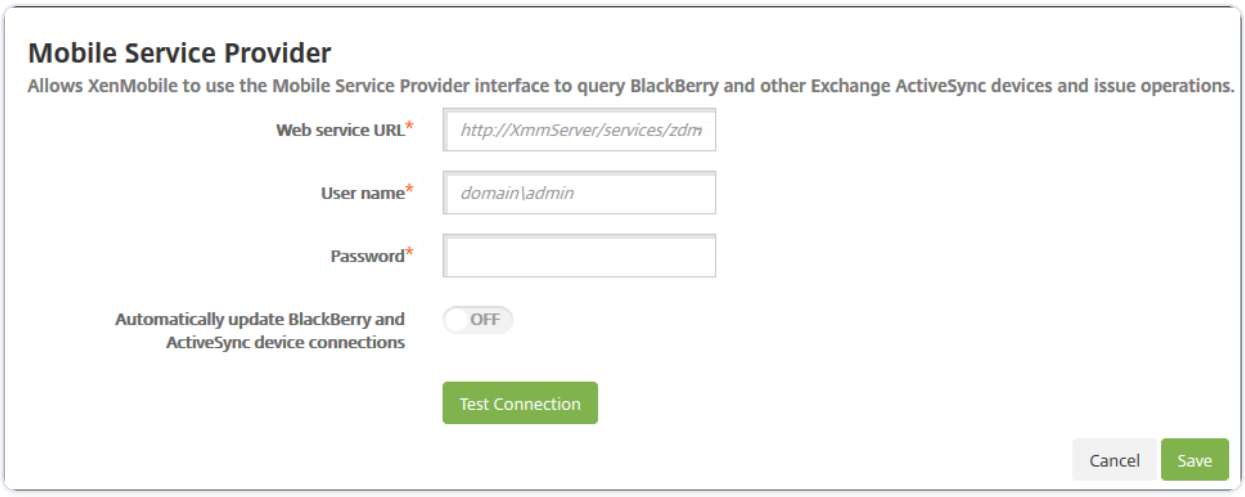
모바일 서비스 공급자

XenMobile®이 모바일 서비스 공급자 인터페이스를 사용하여 BlackBerry 및 Exchange ActiveSync 장치를 쿼리하고 작업을 발행하도록 설정할 수 있습니다.

예를 들어, 조직에 1,000명의 사용자가 있고 각 사용자가 하나 이상의 장치를 사용할 수 있습니다. 모든 사용자에게 장치를 XenMobile에 등록하여 관리해야 한다고 알린 후, XenMobile 콘솔은 사용자가 등록한 장치 수를 나타냅니다. 이 설정을 구성하면 Exchange Server에 연결된 장치 수를 확인할 수 있습니다. 이러한 방식으로 다음을 수행할 수 있습니다.

- 아직 장치를 등록해야 하는 사용자가 있는지 확인합니다.
- 데이터 삭제와 같이 Exchange Server에 연결된 사용자 장치에 명령을 발행합니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **서버** 아래에서 **모바일 서비스 공급자**를 클릭합니다. **모바일 서비스 공급자** 페이지가 나타납니다.



3. 다음 설정을 구성합니다.

- **웹 서비스 URL:** 웹 서비스의 URL을 입력합니다. 예를 들어, `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 **OFF**입니다.
- 연결을 확인하려면 **연결 테스트**를 클릭합니다.

4. **저장**을 클릭합니다.

보고서

XenMobile®은 앱 및 장치 배포를 분석할 수 있는 다음과 같은 사전 정의된 보고서를 제공합니다. 각 보고서는 표와 차트 형태로 나타납니다. 열을 기준으로 표를 정렬하고 필터링할 수 있습니다. 차트에서 요소를 선택하여 더 자세한 정보를 볼 수 있습니다.

- **총 앱 배포 시도:** 사용자가 장치에 설치하려고 시도한 배포된 앱을 나열합니다.
- **플랫폼별 앱:** 장치 플랫폼 및 버전에 따라 앱과 앱 버전을 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.threshold에 지정된 일수 동안 활동이 없었던 장치 목록입니다.
- **탈옥/루팅된 장치:** 탈옥된 iOS 장치와 루팅된 Android 장치를 나열합니다.
- **이용 약관:** 이용 약관 계약에 동의하거나 거부한 사용자를 나열합니다. 차트 영역을 선택하여 자세한 내용을 볼 수 있습니다.
- **상위 10개 앱:** 배포 실패 - 배포에 실패한 최대 10개의 앱을 나열합니다.
- **장치 및 사용자별 블랙리스트 앱:** 사용자가 장치에 가지고 있는 차단된 앱을 나열합니다.

> **참고:**
>
> XenMobile Server 콘솔에는 "blacklist" 및 "whitelist"라는 용어가 포함되어 있습니다. 다가오는 릴리스에서는 이러한 용어를 "block list" 및 "allow list"로 변경할 예정입니다.

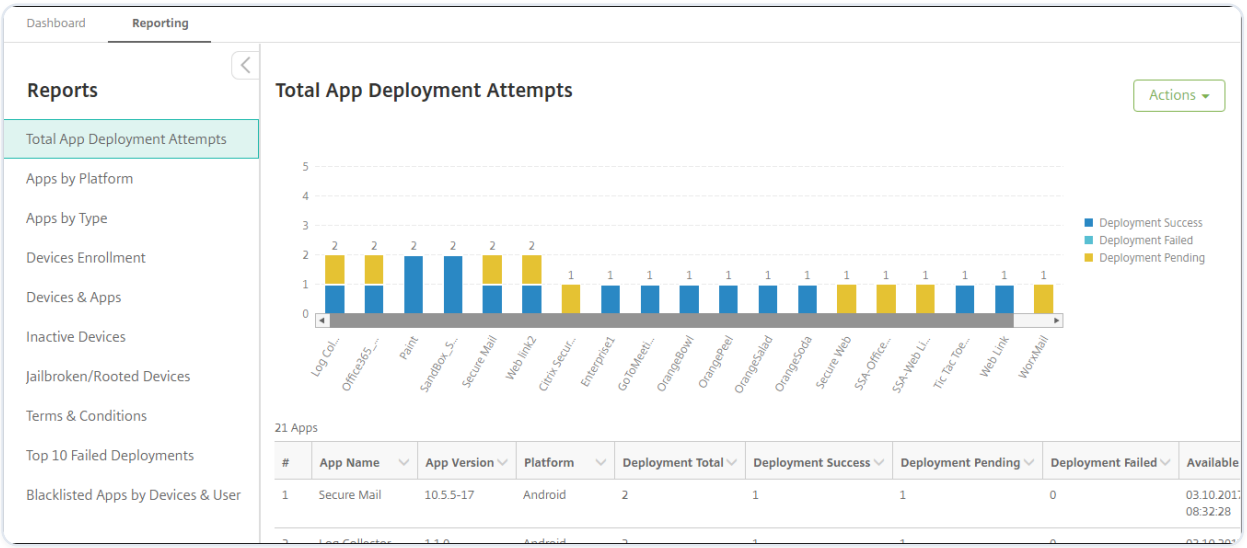
- **비규격 장치:** 장치 탈옥 여부, 실행 중인 OS 버전, 장치에 암호가 있는지 여부와 같은 규정 준수 기준을 충족하지 않는 장치를 나열합니다.

Microsoft Excel과 같은 프로그램을 사용하여 열 수 있는 .csv 형식으로 각 테이블의 데이터를 내보낼 수 있습니다. 각 보고서의 차트는 PDF 형식으로 내보낼 수 있습니다.

- **설치된 상위 100개 앱:** 각 플랫폼에 설치된 상위 100개 앱을 나열합니다. 자세한 내용은 서버 속성을 참조하십시오.

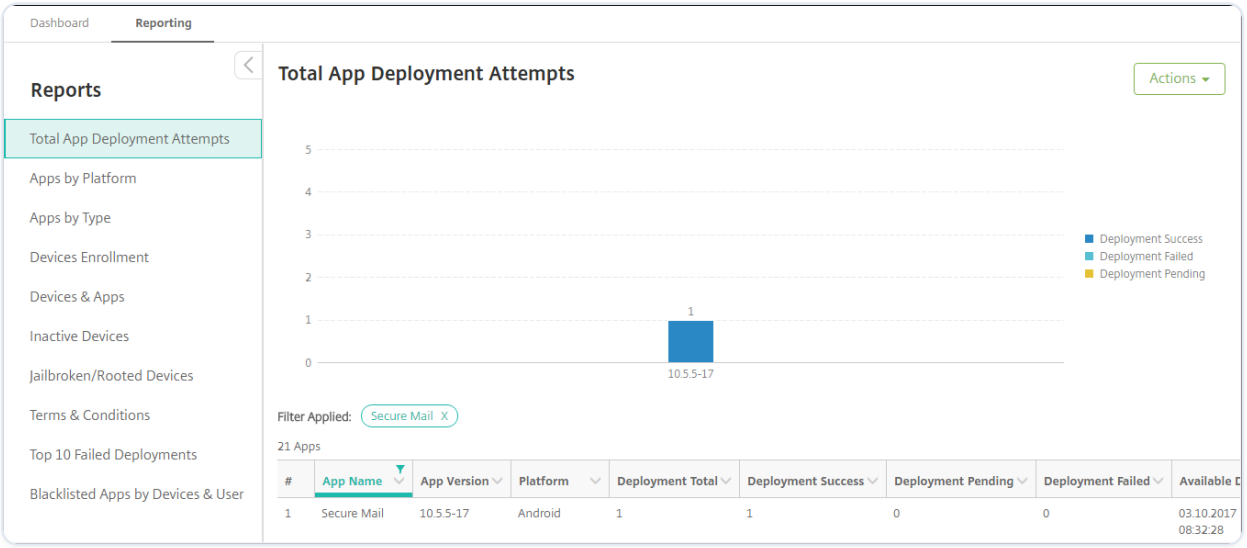
보고서 생성 방법

1. XenMobile 콘솔에서 **분석 > 보고**를 클릭합니다. **보고** 페이지가 나타납니다.
2. 생성하려는 보고서를 클릭합니다.

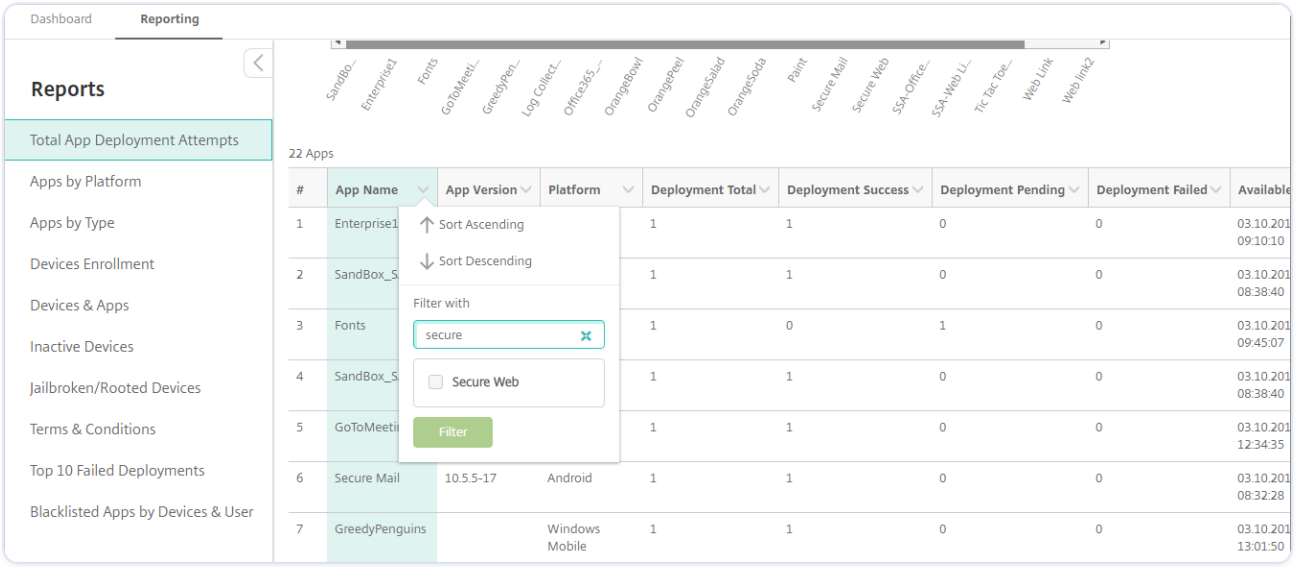


보고서의 자세한 내용 보기

1. 차트 영역을 클릭하여 드릴다운하고 자세한 정보를 확인합니다.

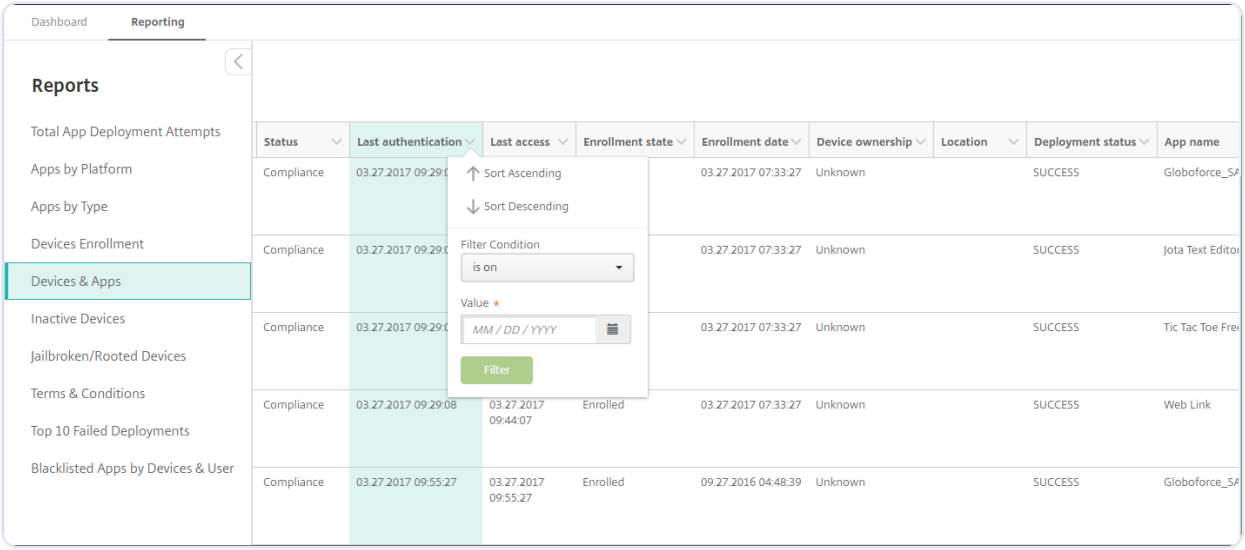


테이블 열을 정렬, 필터링 또는 검색하려면 열 머리글을 클릭합니다



날짜별로 보고서 필터링

1. 열 머리글을 클릭하여 필터 설정을 확인합니다.



2. **필터 조건**에서 보고된 날짜를 제한하는 방법을 선택합니다.

   날짜별 보고서 필터 이미지(/en-us/xenmobile/server/media/analyze-reporting-date-filter-condition.png)

3. 날짜 선택기를 사용하여 날짜를 지정합니다.

   날짜별 보고서 필터 이미지(/en-us/xenmobile/server/media/analyze-reporting-date-filter-choose-date.png)

4. 날짜 필터가 있는 열은 다음 예와 같이 표시됩니다.

날짜별 보고서 필터 이미지(/en-us/xenmobile/server/media/analyze-reporting-date-filter-indicator.png)

5. 필터를 제거하려면 열 머리글을 클릭한 다음 **필터 제거**를 클릭합니다.

   필터 제거 이미지(/en-us/xenmobile/server/media/analyze-reporting-date-filter-remove.png)

차트 또는 테이블 내보내기

- 차트를 PDF 형식으로 내보내려면 **작업**을 클릭한 다음 **그래프를 PDF로 내보내기**를 클릭합니다.
- 테이블 데이터를 CSV 형식으로 내보내려면 **작업**을 클릭한 다음 **데이터를 CVS로 내보내기**를 클릭합니다.

차트 또는 테이블 내보내기 이미지(/en-us/xenmobile/server/media/reporting-export-snip.png)

> **중요:**
>
> SQL Server를 사용하여 사용자 지정 보고서를 만들 수 있지만, Citrix®는 이 방법을 권장하지 않습니다. Citrix는 스키마를 게시하지 않으며 통지 없이 스키마를 변경할 수 있습니다. 이 보고 방법을 사용하기로 결정한 경우, SQL 쿼리가 읽기 전용 계정을 사용하여 실행되는지 확인하십시오. 실행하는 데 시간이 오래 걸리는 여러 JOIN이 있는 쿼리는 해당 시간 동안 XenMobile Server 성능에 영향을 미칩니다.

SNMP 모니터링

XenMobile Server에서 SNMP 모니터링을 활성화하여 모니터링 시스템이 XenMobile 노드에 대한 정보를 쿼리하고 가져올 수 있습니다. 쿼리는 프로세서 로드, 로드 평균, 메모리 사용량 및 연결과 같은 매개변수를 사용합니다. 인증 및 암호화 사양과 같은 SNMP v3에 대한 자세한 내용은 RFC 3414에 대한 공식 SNMP 설명서를 참조하십시오.

> **참고:**
>
> SNMP v3 모니터링은 XenMobile Server 10.8 이상에서 지원됩니다.

> SCOM과 같이 SNMP 모니터링을 지원하는 다양한 모니터링 애플리케이션을 사용할 수 있습니다. SCOM 구성에 대한 자세한 내용은 이 Citrix 지원 기술 자료 문서를 참조하십시오.

필수 구성 요소

다음 TCP 포트를 구성합니다.

- **포트 161 (UDP):** UDP 프로토콜을 사용하는 SNMP 트래픽에 사용됩니다. 소스는 SNMP 관리자이고 대상은 XenMobile입니다.
- **포트 162 (UDP):** XenMobile에서 SNMP 관리자로 SNMP 트랩 경고를 보내는 데 사용됩니다. 소스는 XenMobile이고 대상은 SNMP 관리자입니다.

XenMobile 포트 구성에 대한 자세한 내용은 포트 요구 사항을 참조하십시오.

SNMP를 포함하는 온프레미스 XenMobile 배포의 아키텍처 다이어그램을 보려면 온프레미스 배포를 위한 참조 아키텍처를 참조하십시오.

SNMP 설정의 일반적인 단계는 다음과 같습니다.

1. **사용자 추가:** 사용자는 트랩을 수신하고 XenMobile Server를 모니터링할 수 있는 권한을 상속받습니다.
2. **트랩을 수신할 SNMP 관리자 추가:** 트랩은 XenMobile 노드가 사용자 정의 최대 임계값을 초과할 때 XenMobile이 생성하는 경고입니다.
3. **SNMP 관리자가 XenMobile과 상호 작용하도록 구성:** XenMobile Server는 특정 관리 정보 베이스(MIB)를 사용하여 작업을 수행합니다. XenMobile 콘솔의 **설정 > SNMP 구성** 페이지에서 MIB를 다운로드합니다. 그런 다음 MIB 가져오기 도구를 사용하여 MIB를 SNMP 관리자로 가져옵니다.

   > **참고:**
   >
   > 모든 SNMP 관리자에는 자체 MIB 가져오기 도구가 있습니다.

4. **트랩 사용:** XenMobile 콘솔 내에서 트랩을 사용하도록 설정하고 환경에 따라 간격 및 임계값을 정의합니다.
5. **타사 SNMP 관리자 내에서 트랩 보기:** 트랩을 보려면 SNMP 관리자를 확인하십시오. 그러나 일부 관리자에서는 관리자 외부에서 알림을 사용하도록 설정을 구성할 수 있습니다. 예를 들어 이메일로 알림이 표시되도록 구성할 수 있습니다.

XenMobile에서 다음 트랩을 생성할 수 있습니다.

트랩 이름: 프로세서 로드

- **모니터링 개체 ID(OID):** .1.3.6.1.2.1.25.3.3.1.2

- **설명:** 사용자 정의 간격 동안 시스템의 CPU 로드를 모니터링합니다. 로드가 사용자 지정 임계값보다 크면 XenMobile에서 SNMP 트랩을 생성합니다.

트랩 이름: 1분 동안의 평균 로드

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.2021.10.1.5.1
- **설명:** 사용자 정의 간격 동안 1분 동안의 평균 시스템 로드를 모니터링합니다. 평균 로드가 사용자 지정 임계값보다 크면 XenMobile에서 SNMP 트랩을 생성합니다.

트랩 이름: 5분 동안의 평균 로드

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.2021.10.1.5.2
- **설명:** 사용자 정의 간격 동안 5분 동안의 평균 시스템 로드를 모니터링합니다. 평균 로드가 사용자 지정 임계값보다 크면 XenMobile에서 SNMP 트랩을 생성합니다.

트랩 이름: 15분 동안의 평균 로드

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.2021.10.1.5.3
- **설명:** 사용자 정의 간격마다 15분 동안의 평균 시스템 로드를 모니터링합니다. 로드 평균이 사용자 지정 임계값을 초과하면 XenMobile은 SNMP 트랩을 생성합니다.

트랩 이름: 총 사용 가능한 메모리

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.2021.4.11
- **설명:** 사용자 정의 간격마다 사용 가능한 메모리를 모니터링합니다. 사용 가능한 메모리가 사용자 지정 임계값 미만으로 떨어지면 XenMobile은 SNMP 트랩을 생성합니다. 참고: 총 사용 가능한 메모리에는 RAM과 스왑 메모리(가상 메모리)가 모두 포함됩니다. 총 스왑 메모리를 검색하려면 SNMP OID .1.3.6.1.4.1.2021.4.3을 사용하여 쿼리할 수 있습니다. 사용 가능한 스왑 메모리를 검색하려면 SNMP OID .1.3.6.1.4.1.2021.4.4를 사용하여 쿼리할 수 있습니다.

트랩 이름: 총 사용된 디스크 스토리지

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.2021.9.1.9.1
- **설명:** 사용자 정의 간격마다 시스템 디스크 스토리지를 모니터링합니다. 디스크 스토리지가 사용자 지정 임계값을 초과하면 XenMobile은 SNMP 트랩을 생성합니다.

트랩 이름: Java 힙 메모리 사용량

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.2.4.0
- **설명:** 사용자 정의 간격마다 XenMobile의 Java 가상 머신(JVM) 힙 메모리 사용량을 모니터링합니다. 사용량이 사용자 지정 임계값을 초과하면 XenMobile은 SNMP 트랩을 생성합니다.

트랩 이름: Java 메타스페이스 사용량

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.2.5.0
- **설명:** 사용자 정의 간격마다 XenMobile의 Java 메타스페이스 사용량을 모니터링합니다. 사용량이 임계값을 초과하면 XenMobile은 SNMP 트랩을 생성합니다.

트랩 이름: LDAP 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **설명:** LDAP 서버와 XenMobile 노드 간의 연결을 사용자 정의된 간격마다 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: DNS 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **설명:** DNS 서버와 XenMobile 노드 간의 연결을 사용자 정의된 간격마다 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Google Store 서버 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **설명:** Google Store 서버와 XenMobile 노드 간의 연결을 사용자 정의된 간격마다 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Windows Tab Store 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- **설명:** Tab Store 서버와 XenMobile 노드 간의 연결을 사용자 정의된 간격 동안 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Windows 보안 토큰 서버 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **설명:** Windows 보안 토큰 서버와 XenMobile 노드 간의 연결을 사용자 정의된 간격 동안 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Windows 알림 서버 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **설명:** 사용자 정의 간격 동안 Windows 알림 서버와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Apple 푸시 알림 서버(APNs) 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **설명:** 사용자 정의 간격 동안 APNs와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Apple 피드백 서버 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **설명:** 사용자 정의 간격 동안 Apple 피드백 서버와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Apple Store 서버 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **설명:** 사용자 정의 간격 동안 Apple Store 서버와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: XenMobile 데이터베이스 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- **설명:** 사용자 정의 간격 동안 XenMobile 데이터베이스와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Firebase 클라우드 메시징 서버 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- **설명:** 사용자 정의 간격 동안 Firebase Cloud Messaging 서버와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Citrix License Server 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **설명:** 사용자 정의 간격 동안 Citrix License Server와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: Citrix Gateway 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **설명:** 사용자 정의 간격 동안 Citrix Gateway와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: XenMobile 노드 간 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **설명:** 사용자 정의 간격 동안 XenMobile 클러스터 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

트랩 이름: XenMobile Tomcat 노드 서비스 연결

- **모니터링 개체 ID(OID):** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **설명:** 사용자 정의 간격 동안 XenMobile Tomcat 노드 서비스와 XenMobile 노드 간의 연결을 모니터링합니다. 연결에 실패하면 XenMobile이 SNMP 트랩을 생성합니다.

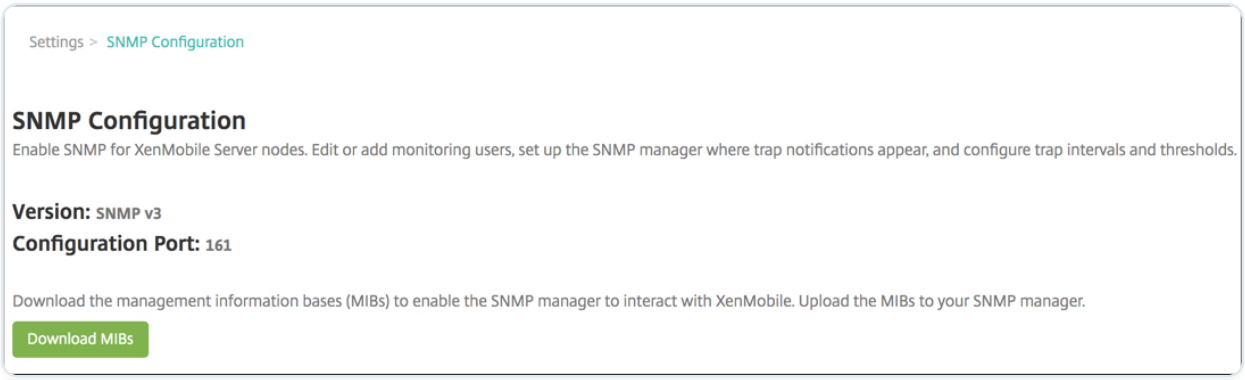
SNMP 임계값을 구성할 때 최상의 서버 성능을 위해 다음 요소를 고려하십시오.

- 호출 빈도
- 수집할 트랩 데이터 및 임계값 확인
- 노드 간 통신 메커니즘
- 연결 확인 빈도
- 확인 중 오류 발생 시 시간 초과

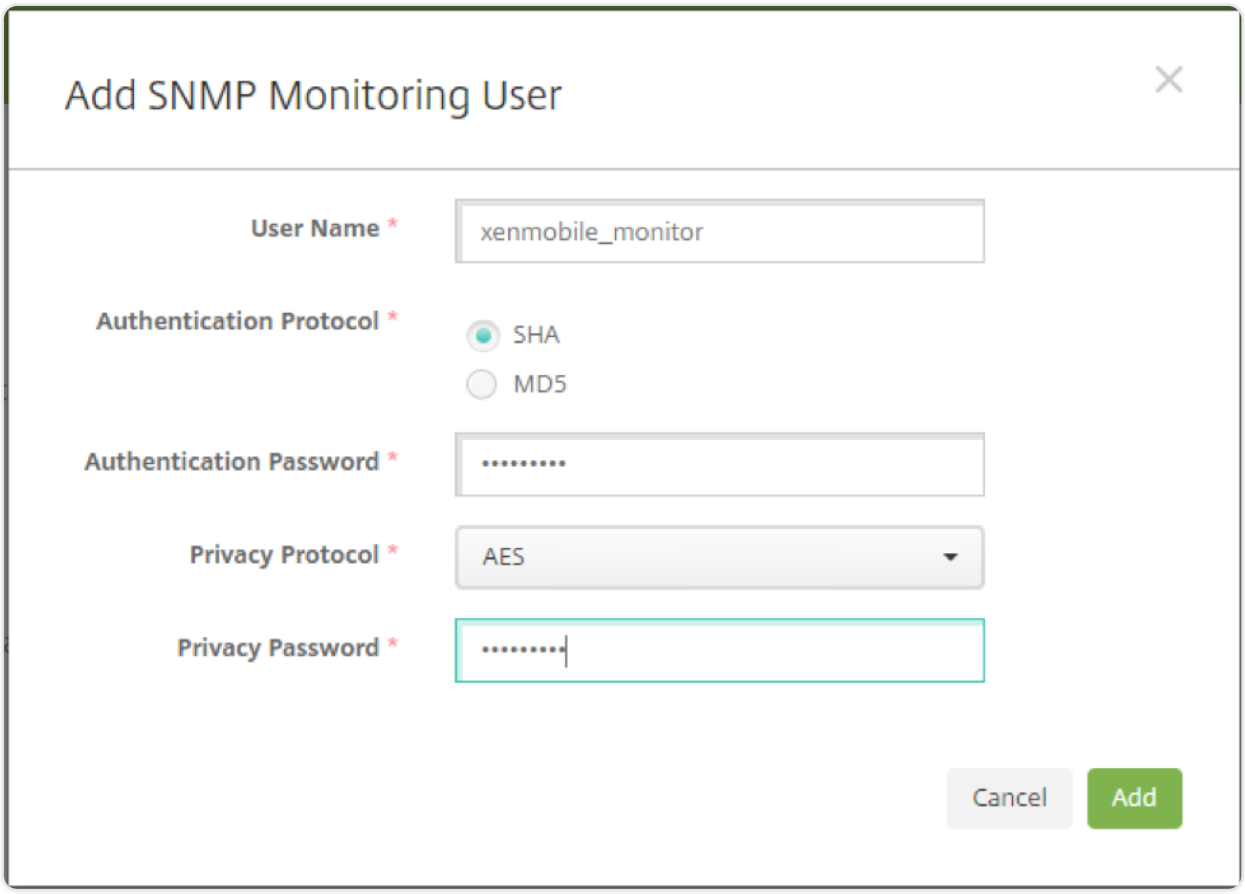
SNMP 사용자 추가

SNMP 사용자는 SNMP 관리자와 상호 작용하고 트랩을 수신합니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **모니터링** 아래에서 **SNMP 구성**을 클릭합니다. **SNMP 구성** 페이지가 나타납니다.



3. **SNMP 모니터링 사용자** 아래에서 **추가**를 클릭합니다.
4. **SNMP 모니터링 사용자 추가** 대화 상자에서 다음 설정을 구성합니다.



사용자 이름: SNMP 관리자에 로그온하는 데 사용되는 사용자 이름입니다. 영숫자, 밑줄, 하이픈을 사용할 수 있지만 공백 및 기타 특수 문자는 사용자 이름에 사용할 수 없습니다.

> **참고:**
>
> XenMobile이 내부용으로 해당 이름을 예약하므로 사용자 이름 "xmsmonitor"를 추가할 수 없습니다.

> **인증 프로토콜:**

- **SHA** (권장)
- **MD5**

인증 암호: 8~18자 암호를 입력합니다. 영숫자와 특수 문자를 포함할 수 있습니다.

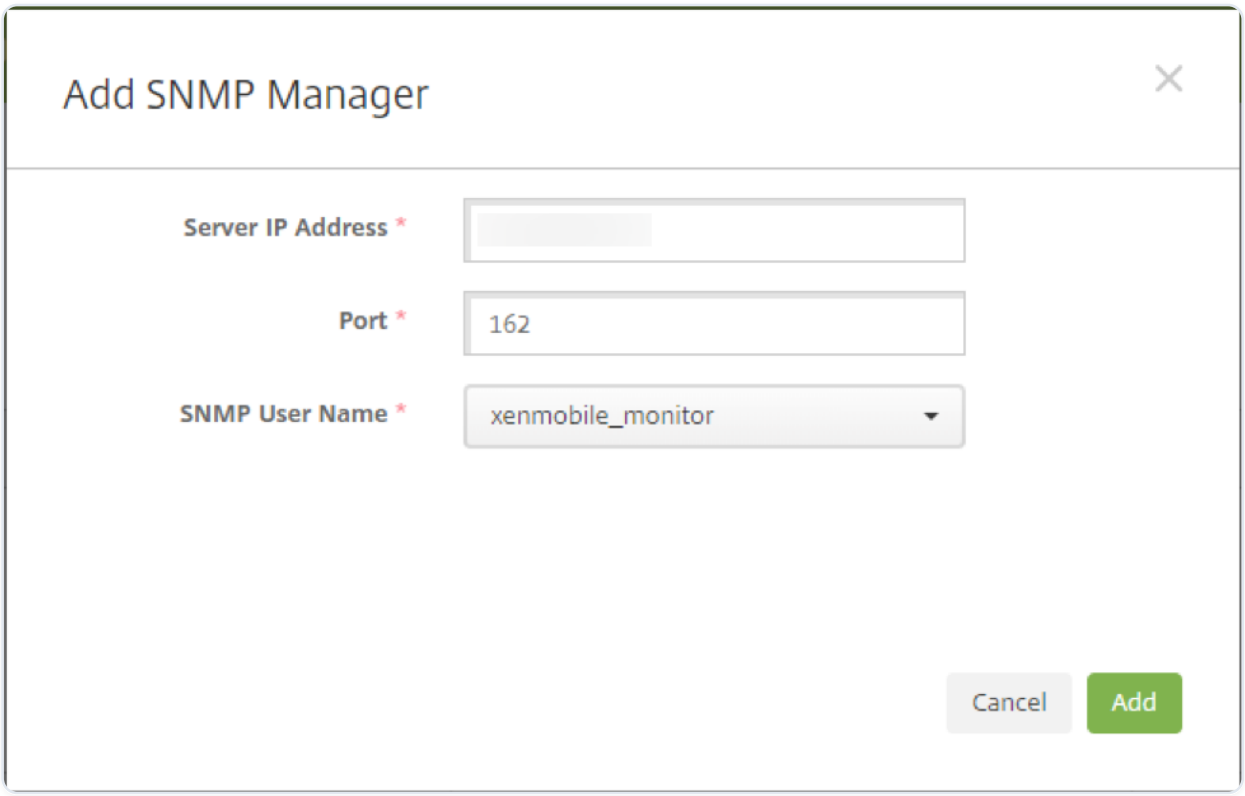
개인 정보 보호 프로토콜:

- **DES**
- **AES 128** (권장)

개인 정보 보호 암호: 8~18자 암호를 입력합니다. 영숫자와 특수 문자를 포함할 수 있습니다.

SNMP 관리자를 추가하려면

1. **SNMP 관리자**에서 **추가**를 클릭합니다.
2. **SNMP 관리자 추가** 대화 상자에서 다음 설정을 구성합니다.



서버 IP 주소: SNMP 관리자의 IP 주소를 입력합니다.

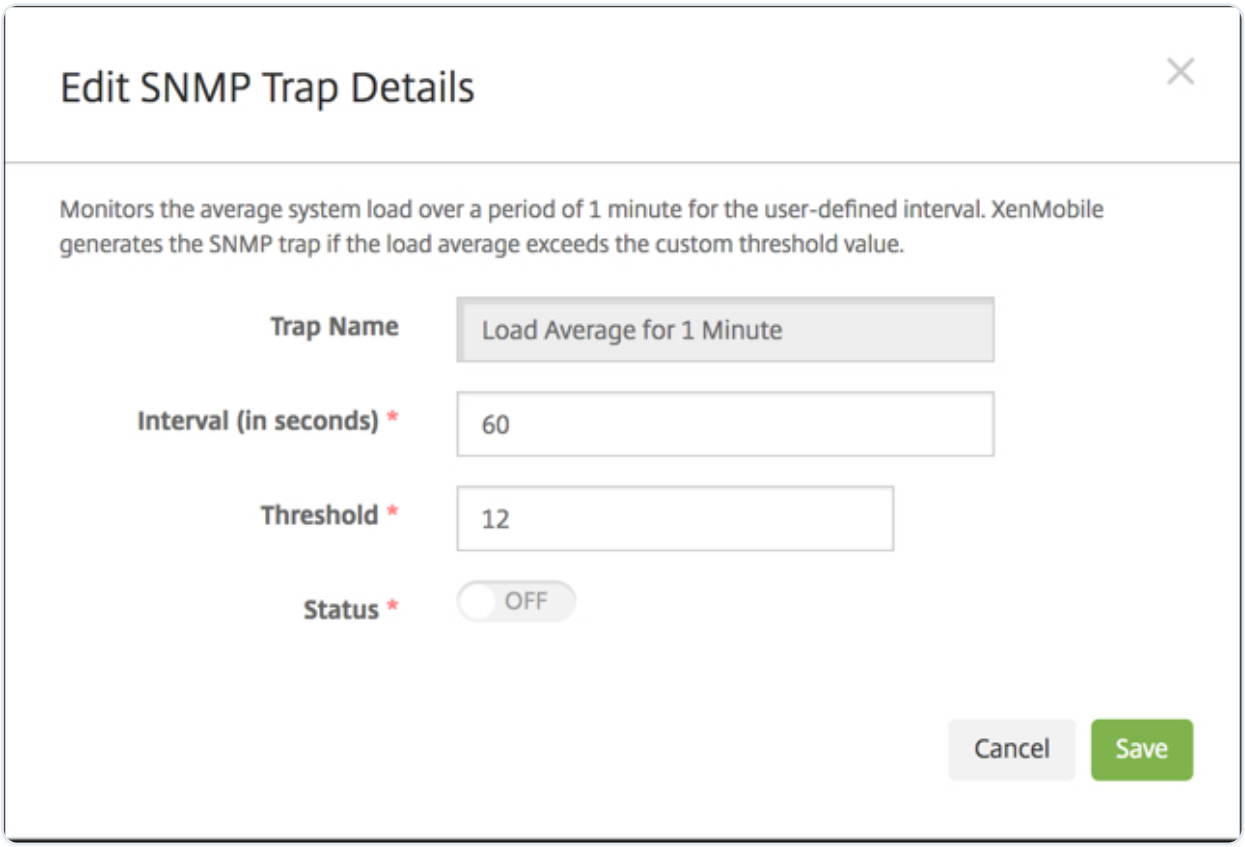
포트: 필요한 경우 포트 번호를 변경합니다. 기본값은 162입니다.

SNMP 사용자 이름: 관리자에 액세스할 수 있는 사용자 이름을 선택합니다.

SNMP 트랩을 활성화하고 구성하려면

환경에 적합한 트랩 설정을 결정하는 데 도움이 필요하면 확장성 및 성능을 참조하십시오. 예를 들어, XenMobile 로드 평균을 1분 동안 모니터링하려면 1분 로드 평균을 활성화하고 임계값(threshold value)을 제공할 수 있습니다. XenMobile Server의 1분 로드 평균이 지정된 임계값을 초과하면 구성된 SNMP 관리자에서 트랩을 수신합니다.

1. 개별 트랩을 활성화하려면 다음 중 하나를 수행합니다.
   - 매개변수 옆의 확인란을 선택한 다음 **활성화**를 클릭합니다.
   - 목록의 모든 트랩을 활성화하려면 맨 위에 있는 확인란을 선택한 다음 **활성화**를 클릭합니다.
2. 트랩을 편집하려면 매개변수를 선택한 다음 **편집**을 클릭합니다.
3. **SNMP 트랩 세부 정보 편집** 대화 상자에서 개별 트랩의 임계값(threshold value)을 편집할 수 있습니다.



트랩 이름: 트랩의 이름입니다. 이 필드는 편집할 수 없습니다.

간격(초): 허용되는 범위는 60에서 86400(24시간)입니다.

임계값: 다음 트랩에 대해서만 임계값을 변경할 수 있습니다.

- 프로세서 로드
- 1분 로드 평균
- 5분 로드 평균
- 15분 동안의 로드 평균
- 총 사용 가능한 메모리
- 총 사용된 디스크 저장소
- Java 힙 메모리 사용량
- Java 메타스페이스 사용량

상태: 트랩에 대한 SNMP 모니터링을 사용하도록 설정하려면 **ON**을 선택합니다. 모니터링을 사용하지 않도록 설정하려면 **OFF**를 선택합니다.

SNMP를 사용하여 XenMobile 모니터링에 대한 더 유용한 정보는 이 블로그 게시물을 참조하십시오.

지원 번들

Citrix에 문제를 보고하거나 문제를 해결하려면 지원 번들을 생성하십시오. 그런 다음 지원 번들을 Citrix Insight Services(CIS)에 업로드하십시오.

기본적으로 지원 번들에는 다음 파일의 백업 아카이브가 최대 100개 포함됩니다. 이러한 파일의 기본 파일 크기는 10MB입니다.

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

지원 번들에 각 범주별로 100개의 로그 아카이브 파일이 포함되면 로그 파일이 롤오버됩니다. 최대 로그 파일 수를 더 낮게 구성하면 XenMobile®은 해당 노드의 불필요한 로그 파일을 즉시 삭제합니다. 로그 파일 수를 구성하려면 **문제 해결 및 지원 > 로그 설정**으로 이동하십시오.

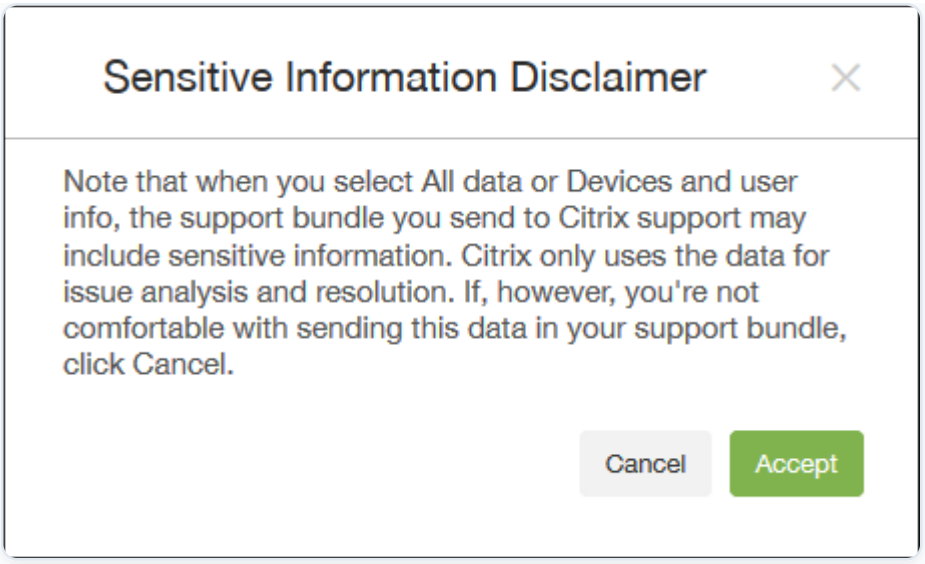
지원 번들을 생성하려면:

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 렌치 아이콘을 클릭합니다. **지원** 페이지가 나타납니다.
2. **지원** 페이지에서 **지원 번들 생성**을 클릭합니다. **지원 번들 생성** 페이지가 나타납니다. XenMobile 환경에 클러스터된 노드가 있는 경우 모든 노드가 표시됩니다.

   지원 번들(/en-us/xenmobile/server/media/create-support-bundle.png)
3. **XenMobile용 지원 번들** 확인란이 선택되어 있는지 확인하십시오.
4. XenMobile 환경에 클러스터된 노드가 있는 경우 **지원 번들 대상**에서 모든 노드 또는 데이터를 가져올 노드의 조합을 선택할 수 있습니다.
5. **데이터베이스에서 포함**에서 다음 중 하나를 수행하십시오.
   - **데이터 없음**을 클릭합니다.
   - **사용자 지정 데이터**를 클릭합니다. 기본적으로 이 모든 옵션이 선택되어 있습니다.
     - **구성 데이터:** 인증서 구성 및 장치 관리자 정책을 포함합니다.
     - **전송 그룹 데이터:** 앱 유형 및 앱 전송 정책 세부 정보를 포함하는 앱 전송 그룹 정보를 포함합니다.
     - **장치 및 사용자 정보:** 장치 정책, 앱, 작업 및 전송 그룹을 포함합니다.
   - **모든 데이터**를 클릭합니다.

참고:

장치 및 사용자 정보 또는 **모든 데이터**를 선택하고 이것이 처음으로 생성하는 지원 번들이라면 **민감한 정보 고지 사항** 대화 상자가 나타납니다. 고지 사항을 읽은 다음 **수락** 또는 **취소**를 클릭합니다. **취소**를 클릭하면 지원 번들을 Citrix에 업로드할 수 없습니다. **수락**을 클릭하면 지원 번들을 Citrix에 업로드할 수 있으며, 장치 또는 사용자 데이터를 포함하는 지원 번들을 다음에 생성할 때는 고지 사항이 표시되지 않습니다.

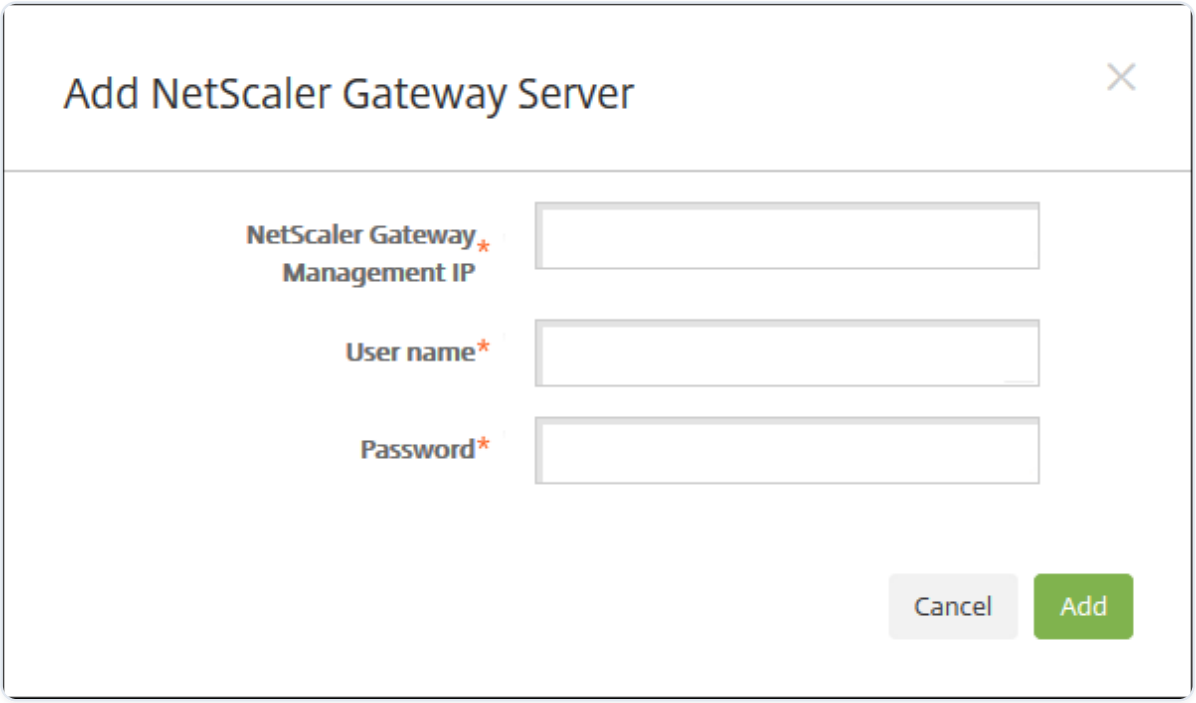


6. **지원 데이터 익명화가 켜져 있습니다** 옵션은 데이터를 익명화하는 것이 기본 설정임을 나타냅니다. 데이터 익명화는 지원 번들에서 민감한 사용자, 서버 및 네트워크 데이터가 익명으로 처리됨을 의미합니다.

   이 설정을 변경하려면 **익명화 및 익명화 해제**를 클릭합니다. 데이터 익명화에 대한 자세한 내용은 지원 번들에서 데이터 익명화를 참조하십시오.

7. Citrix Gateway에서 지원 번들을 포함하려면: **Citrix Gateway용 지원 번들** 확인란을 선택한 다음 다음 작업을 수행합니다.

   a. **추가**를 클릭합니다. **Citrix Gateway 서버 추가** 대화 상자가 나타납니다.



b. **Citrix Gateway 관리 IP**에 지원 번들 데이터를 가져올 Citrix Gateway의 Citrix ADC 관리 IP 주소를 입력합니다.

> **참고:**
>
> 이미 추가된 Citrix Gateway 서버에서 번들을 생성하는 경우, IP 주소가 제공됩니다.

c. **사용자 이름** 및 **암호**에 Citrix Gateway를 실행하는 서버에 액세스하는 데 필요한 사용자 자격 증명을 입력합니다.

> **참고:**
>
> 이미 추가된 Citrix Gateway 서버에서 번들을 생성하는 경우, 사용자 이름이 제공됩니다.

8. **추가**를 클릭합니다. 새 Citrix Gateway 지원 번들이 테이블에 추가됩니다.
9. 7단계를 반복하여 Citrix Gateway 지원 번들을 더 추가합니다.
10. **생성**을 클릭합니다. 지원 번들이 생성되고 **CIS에 업로드** 및 **클라이언트에 다운로드**라는 두 개의 새 버튼이 나타납니다.

Citrix Insight Services에 지원 번들 업로드

지원 번들을 생성한 후, 해당 번들을 Citrix Insight Services(CIS)에 업로드하거나 컴퓨터로 다운로드할 수 있습니다.

XenMobile에서 CIS로의 업로드는 SSL 아웃바운드 연결을 통해 이루어집니다. CIS 서버 IP 주소(52.88.24.76, 52.88.118.220, 52.11.72.119)에 대해 포트 443을 엽니다. HTTPS 트래픽에 대한 프록시가 있는 경우, 프록시가 CIS 서버 IP 주소에 도달할 수 있는지 확인하십시오.

다음 단계는 번들을 CIS에 업로드하는 방법을 보여줍니다. CIS에 업로드하려면 My Citrix ID와 암호가 필요합니다.

1. **지원 번들 생성** 페이지에서 **CIS에 업로드**를 클릭합니다. **Citrix Insight Services(CIS)에 업로드** 대화 상자가 나타납니다.
2. **사용자 이름**에 My Citrix ID를 입력합니다.
3. **암호**에 My Citrix 암호를 입력합니다.
4. 이 번들을 기존 서비스 요청 번호와 연결하려면 **Associate with SR#** 확인란을 선택하고 나타나는 두 개의 새 필드에서 다음을 수행합니다.
   - **SR#**에 이 번들을 연결하려는 8자리 서비스 요청 번호를 입력합니다.
   - **SR Description**에 SR에 대한 설명을 입력합니다.
5. **Upload**를 클릭합니다.

   CIS에 지원 번들을 처음 업로드하는 경우, 다른 제품을 통해 CIS에 계정을 만들지 않았고 Data Collection and Privacy agreement에 동의하지 않은 경우 다음 대화 상자가 나타납니다. 업로드를 시작하기 전에 계약에 동의해야 합니다. CIS에 계정이 있고 이전에 계약에 동의한 경우 지원 번들이 즉시 업로드됩니다.

   지원 번들 법적 계약(/en-us/xenmobile/server/media/cis-legal-agreement.png)
6. 계약을 읽은 다음 **Agree and upload**를 클릭합니다. 지원 번들이 업로드됩니다.

컴퓨터로 지원 번들 다운로드

지원 번들을 생성한 후 번들을 CIS에 업로드하거나 컴퓨터로 다운로드할 수 있습니다. 문제를 직접 해결하려면 지원 번들을 컴퓨터로 다운로드합니다.

Create Support Bundles 페이지에서 **Download to Client**를 클릭합니다. 번들이 컴퓨터로 다운로드됩니다.

지원 번들에는 분석 가치가 다양한 파일이 포함되어 있습니다. 다음 표에서 파일 목록과 해당 분석 가치를 참조하십시오.

파일 이름	유형	설명	값
DbDump.json	JSON 데이터베이스 덤프	사용자/장치/애플리케이션 정보	높음
Garbage.html	HTML 파일	Java 가비지 컬렉터	낮음
MemoryInfo.html	HTML 파일	메모리 사용량 - java 관련 메모리 사용량	높음
MultiNodeClusterInfo.html	HTML 파일	클러스터 구성	높음
Patches.html	HTML 파일	패치 정보. xmspatches.txt가 더 좋습니다.	높음
pg_dump0.sql	PG 덤프	기본 Postgress 인스턴스 덤프	중간
rt_db/*	DB 복사 (중복, pg_dump0.sql의 이진 표현)		해당 없음
sas_config/c3p0.properties	속성 파일	C3P0 DB 구성 속성	중간
sas_config/catalina.policy	정책 파일	웹 서버 Catalina 정책 - 파일은 변경되지 않습니다	낮음
sas_config/catalina.properties	속성 파일	웹 서버 Catalina 속성 - 파일은 변경되지 않습니다	낮음
sas_config/ew-config.properties	속성 파일	XM 서버 구성 정보	높음

파일 이름	유형	설명	값
sas_config/ew-config-reloadable.properties	속성 파일	보안 모델 정보	높음
sas_config/hazelcast.xml	XML 파일	Hazelcast 로그 - 크게 유용하지 않을 것으로 생각됩니다.	낮음
sas_config/pki.xml	XML 파일	타사 PKI 서버 사용 여부를 확인하는 데 사용될 수 있습니다.	높음
sas_config/push_services.xml	XML 파일	푸시 서비스 - 파일이 변경되지 않습니다.	낮음
sas_config/server.xml	XML 파일	여기에 암호 정보 - 보안 관련	높음
sas_config/sftu_config/AppC.properties	속성 파일	AppC 속성 - 파일이 변경되지 않음	낮음
sas_config/sftu_config/catalina.policy	정책 파일	Catalina 정책 - 파일이 변경되지 않음	낮음
sas_config/sftu_config/catalina.properties	속성 파일	Catalina 속성 - 파일이 변경되지 않음	낮음
sas_config/sftu_config/logging.properties	속성 파일	로깅 속성 - 파일이 변경되지 않음	낮음
sas_config/sftu_config/server.xml	XML 파일	여기에 암호 정보 - 보안 관련	높음
sas_config/sftu_config/server_migration.xml	XML 파일	마이그레이션 정보	높음

파일 이름	유형	설명	값
sas_config/sftu_config/server_sftu.xml	XML 파일	최초 사용자 설정	높음
sas_config/sftu_config/tomcat-users.xml	XML 파일	TomCat 사용자 - 파일이 변경되지 않음	낮음
sas_config/sftu_config/web.xml	XML 파일	웹 - 파일이 변경되지 않음	낮음
sas_config/sftu.properties	속성 파일	SFTU 구성 속성	높음
sas_config/variables.xml	XML 파일	변수 - 파일이 변경되지 않음	낮음
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.sh	Linux 로그 파일	지원 생성 명령 출력	낮음
sas_log/DebugLogFile.log	Linux 로그 파일	모든 기능 로그	높음
sas_log/HibernateStats.log	Linux 로그 파일	HibernateStats 로그	낮음
sas_log/kafka-consumer.log	Linux 로그 파일	Kafka 로그	낮음
sas_log/kafka-server.log	Linux 로그 파일	Kafka 로그	낮음
sas_log/kafka-topics.log	Linux 로그 파일	Kafka 로그	낮음
sas_log/LPE.log	Linux 로그 파일	LPE 로그	낮음

파일 이름	유형	설명	값
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.txt	텍스트 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	낮음
sas_log/tc1/console	Linux 로그 파일	콘솔	낮음
sas_log/tc1/host-manager.log	Linux 로그 파일	호스트 관리자	낮음
sas_log/tc1/localhost.log	Linux 로그 파일	로컬 호스트	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	낮음
snmp/snmpd_etc_netsnmp.conf	속성 파일	SNMP 구성 속성	낮음
snmp/snmpd_privileges.conf	속성 파일	SNMP 구성 속성	낮음

파일 이름	유형	설명	값
sys_info/arp_entries.txt	텍스트 파일	XMS 서버의 ARP 항목	중간
sys_info/chrony.txt	텍스트 파일	Chrony 로그	낮음
sys_info/diskspace_usage.txt	텍스트 파일	디스크 공간 사용량	높음
sys_info/firewall_rules.txt	텍스트 파일	XMS에 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_process.txt	텍스트 파일	높은 값	높음
sys_info/top.txt	텍스트 파일	시스템 명령 출력	중간
ThreadDump.html	HTML 파일	더 이상 사용되지 않습니다.	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 레벨 로그	보통
var_log/daemon.log	Linux 로그 파일	OS 레벨 로그	보통
var_log/kern.log	Linux 로그 파일	OS 레벨 로그	보통

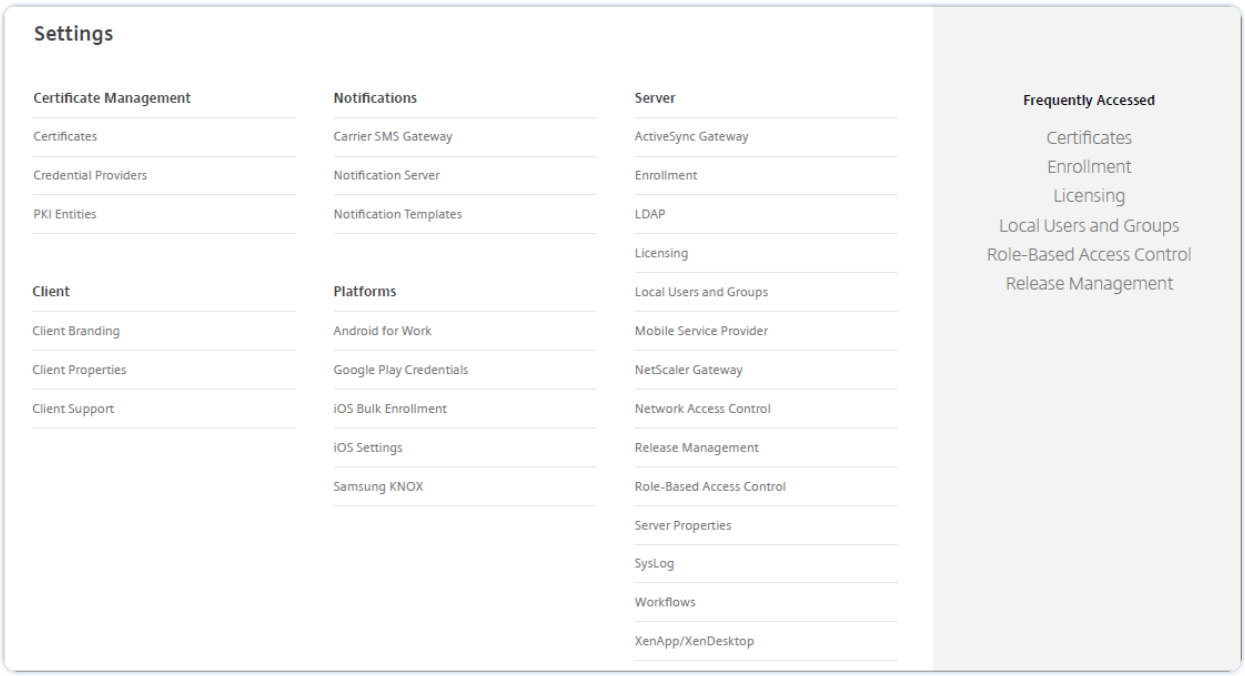
파일 이름	유형	설명	값
var_log/lastlog	Linux 로그 파일	OS 레벨 로그	보통
var_log/mail.log	Linux 로그 파일	OS 수준 로그	보통
var_log/sys.log	Linux 로그 파일	OS 수준 로그	보통
var_log/user.log	Linux 로그 파일	OS 수준 로그	보통
var_log/wtmp	Linux 로그 파일	OS 수준 로그	중간
version.txt	텍스트 파일	XM 서버 버전	중간
XENMOBILE-`<IP Address>`-ConnectivityCheckResults.xml	XML 파일	XMS 서버의 연결 확인 결과	중간
xmspatches.txt	텍스트 파일	패치 정보.	높음

지원 옵션 및 원격 지원

사용자가 지원 담당자에게 연락할 수 있도록 이메일 주소를 제공할 수 있습니다. 사용자가 장치에서 지원을 요청하면 해당 이메일 주소가 표시됩니다.

사용자가 장치에서 헬프데스크로 로그를 보내는 방법을 구성할 수도 있습니다. 로그를 직접 보내거나 이메일로 보내도록 구성할 수 있습니다.

1. XenMobile® 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.



2. **클라이언트** 아래에서 **클라이언트 지원**을 클릭합니다. **클라이언트 지원** 페이지가 나타납니다.
3. 다음 설정을 구성합니다.

   - **지원 이메일(IT 헬프데스크):** IT 헬프데스크 담당자의 이메일 주소를 입력합니다.
   - **장치 로그를 IT 헬프데스크로 보내기:** 장치 로그를 **직접** 보낼지 **이메일로** 보낼지 선택합니다. 기본값은 **이메일로**입니다.

     - **직접**을 사용하도록 설정하면 ShareFile에 로그 저장(현재 ShareFile이라고 함) 설정이 나타납니다. ShareFile에 로그 저장을 사용하도록 설정하면 로그가 Citrix Files로 직접 전송됩니다. 그렇지 않으면 로그가 XenMobile로 전송된 다음 헬프데스크로 이메일로 전송됩니다. 또한 **직접 전송에 실패하면 이메일 사용** 옵션이 나타나며, 이 옵션은 기본적으로 사용하도록 설정되어 있습니다. 서버 문제에 대한 로그를 보내기 위해 클라이언트 이메일을 사용하지 않으려면 이 옵션을 비활성화할 수 있습니다. 그러나 이 옵션을 비활성화하고 서버 문제가 발생하면 로그가 전송되지 않습니다.
     - **이메일로**를 사용하도록 설정하면 클라이언트 이메일이 항상 로그를 보내는 데 사용됩니다.

4. **저장**을 클릭합니다.

원격 지원

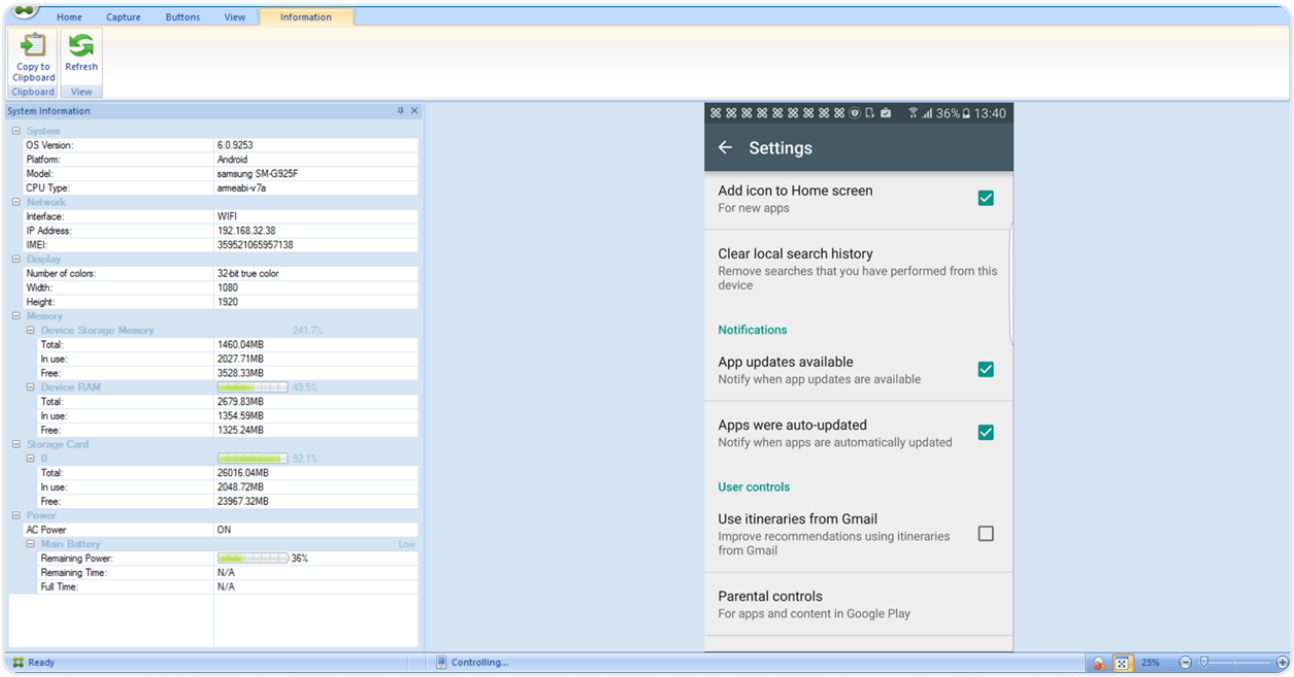
> **참고:**
>
> 원격 지원은 January 1, 2019부터 신규 고객에게 더 이상 제공되지 않습니다. 기존 고객은 계속해서 제품을 사용할 수 있지만, Citrix는 향상된 기능이나 수정 사항을 제공하지 않습니다.

> 온프레미스 XenMobile Server 배포의 경우: 원격 지원을 통해 헬프데스크 담당자가 관리되는 Android 모바일 장치를 원격으로 제어할 수 있습니다. 화면 전송은 Samsung Knox 장치에서만 지원됩니다.

클러스터링된 온프레미스 XenMobile Server 배포에서는 원격 지원을 사용할 수 없습니다.

원격 제어 세션 중:

- 사용자는 모바일 장치에서 원격 제어 세션이 활성 상태임을 나타내는 아이콘을 볼 수 있습니다.
- 원격 지원 사용자는 원격 지원 애플리케이션 창과 제어되는 장치의 렌더링을 보여주는 원격 제어 창을 볼 수 있습니다.



원격 지원을 사용하여 다음을 수행할 수 있습니다.

- 사용자 장치에 원격으로 로그인하여 화면을 제어합니다. 사용자는 화면 탐색을 볼 수 있으며, 이는 교육 목적으로도 유용할 수 있습니다.
- 원격 장치를 실시간으로 탐색하고 복구합니다. 구성을 변경하고, 운영 체제 문제를 해결하고, 문제가 있는 앱이나 프로세스를 비활성화하거나 중지할 수 있습니다.
- 네트워크 액세스를 원격으로 비활성화하고, 악성 프로세스를 중지하고, 앱 또는 맬웨어를 제거하여 위협이 다른 모바일 장치로 확산되기 전에 격리하고 차단합니다.
- 장치 벨소리를 원격으로 활성화하고 전화에 전화를 걸어 사용자가 장치를 찾도록 돕습니다. 사용자가 장치를 찾을 수 없는 경우, 중요한 데이터가 손상되지 않도록 장치를 초기화할 수 있습니다.

원격 지원을 통해 지원 담당자는 다음을 수행할 수도 있습니다.

- 하나 이상의 XenMobile 인스턴스 내에서 연결된 모든 장치 목록을 표시합니다.
- 장치 모델, 운영 체제 수준, 국제 모바일 장비 식별(IMEI), 일련 번호, 메모리 및 배터리 상태, 연결성을 포함한 시스템 정보를 표시합니다.
- XenMobile의 사용자 및 그룹을 표시합니다.
- 장치 작업 관리자를 실행하여 활성 프로세스를 표시하고, 활성 프로세스를 종료하고, 모바일 장치를 다시 시작할 수 있습니다.
- 모바일 장치와 중앙 파일 서버 간의 양방향 파일 전송을 포함하는 원격 파일 전송을 실행합니다.
- 하나 이상의 모바일 장치에 소프트웨어 프로그램을 일괄적으로 다운로드하고 설치합니다.
- 장치에서 원격 레지스트리 키 설정을 구성합니다.
- 실시간 장치 화면 원격 제어를 사용하여 낮은 대역폭의 셀룰러 네트워크에서 응답 시간을 최적화합니다.
- 대부분의 모바일 장치 브랜드 및 모델에 대한 장치 스킨을 표시합니다. 새 장치 모델을 추가하고 물리적 키를 매핑하기 위한 스킨 편집기를 표시합니다.
- 장치에서 일련의 상호 작용을 캡처하여 비디오 AVI 파일을 생성하는 기능으로 장치 화면 캡처, 기록 및 재생을 활성화합니다.
- 공유 화이트보드, VoIP 기반 음성 통신 및 모바일 사용자 및 지원 담당자 간의 채팅을 사용하여 실시간 회의를 진행합니다.

원격 지원 시스템 요구 사항

원격 지원 소프트웨어는 다음 요구 사항을 충족하는 Windows 기반 컴퓨터에 설치됩니다. 포트 요구 사항은 포트 요구 사항을 참조하십시오.

지원되는 플랫폼:

- Intel Xeon/Pentium 4 -1 GHz 최소 워크스테이션 등급
- 512MB RAM 최소
- 100MB 사용 가능한 디스크 공간 최소

지원되는 운영 체제:

- Microsoft Windows 2003 서버 스탠다드 에디션 또는 엔터프라이즈 에디션 SP1 이상
- Microsoft Windows 2000 프로페셔널 SP4
- Microsoft Windows XP SP2 이상 버전
- Microsoft Windows Vista SP1 이상 버전
- 마이크로소프트 윈도우 10 또는 윈도우 11
- 마이크로소프트 윈도우 8

- 마이크로소프트 윈도우 7

명령줄에서 원격 지원을 설치하려면

다음 명령을 실행합니다.

```
*RemoteSupport*.exe /S
```

*RemoteSupport*는 설치 프로그램의 이름입니다. 예:

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

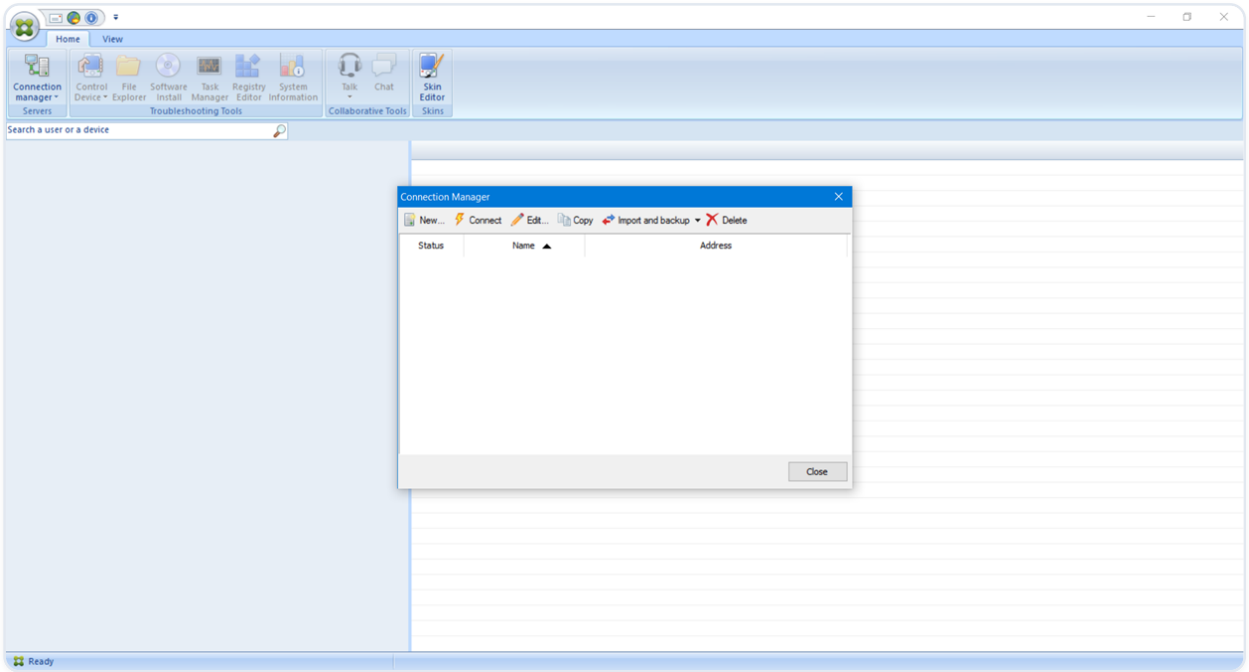
원격 지원 소프트웨어를 설치할 때 다음 변수를 사용할 수 있습니다.

- /S: 기본 매개변수로 원격 지원 소프트웨어를 자동으로 설치합니다.
- /D=dir: 사용자 지정 설치 디렉터리를 지정합니다.

원격 지원을 XenMobile에 연결하려면

관리되는 장치에 대한 원격 지원 연결을 설정하려면 원격 지원에서 장치를 관리하는 하나 이상의 XenMobile Server에 연결을 추가해야 합니다. 이 연결은 Android 장치용 장치 정책인 터널 MDM 정책에서 정의하는 앱 터널을 통해 실행됩니다. 원격 지원을 XenMobile에 연결하기 전에 앱 터널을 정의하십시오. 자세한 내용은 앱 터널링 장치 정책을 참조하십시오.

1. 원격 지원 소프트웨어를 시작하고 XenMobile 자격 증명을 사용하여 로그인합니다.
2. **연결 관리자**에서 **새로 만들기**를 클릭합니다.



3. **연결 구성** 대화 상자의 **서버** 탭에서 다음 값을 입력합니다.

   a. **구성 이름**에 구성 항목의 이름을 입력합니다.

   b. **서버 IP 주소 또는 이름**에 XenMobile Server의 IP 주소 또는 DNS 이름을 입력합니다.

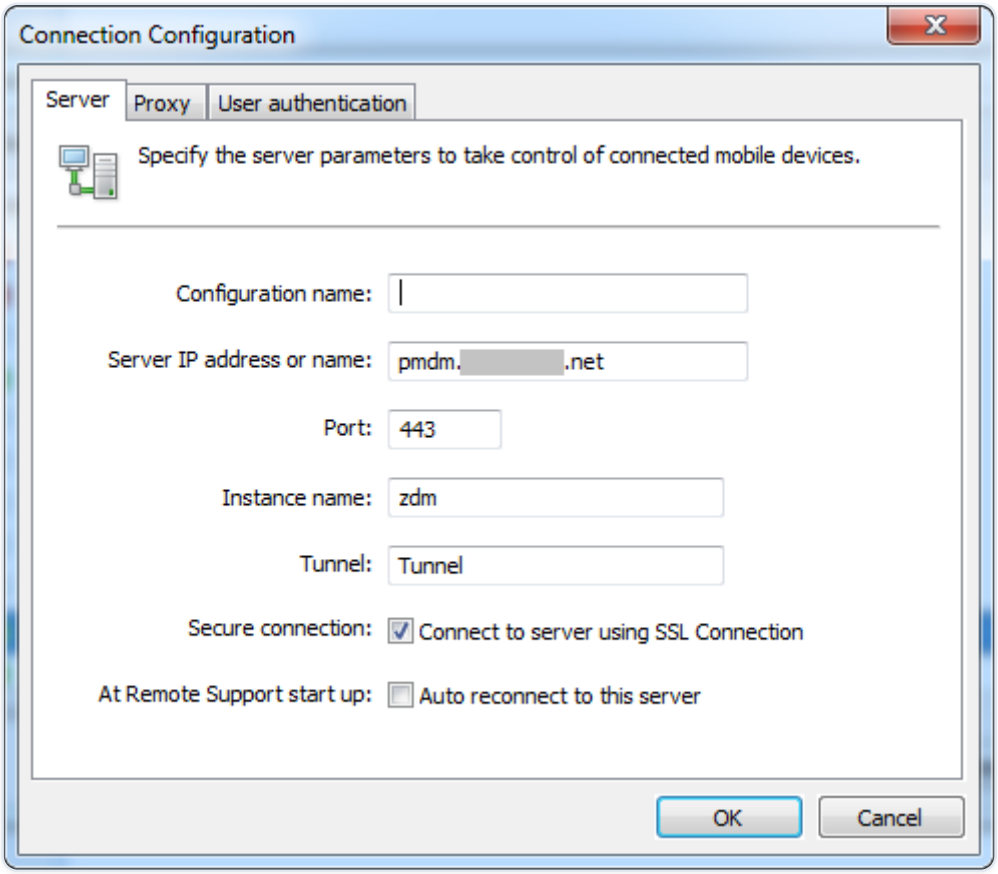
   c. **포트**에 XenMobile Server 구성에 정의된 TCP 포트 번호를 입력합니다.

   d. XenMobile이 다중 테넌트 배포의 일부인 경우 **인스턴스 이름**에 인스턴스 이름을 입력합니다.

   e. **터널**에 터널 정책의 이름을 입력합니다.

   f. **SSL 연결을 사용하여 서버에 연결** 확인란을 선택합니다.

   g. 원격 지원 애플리케이션이 시작될 때마다 구성된 XenMobile Server에 연결하려면 **이 서버에 자동으로 다시 연결** 확인란을 선택합니다.



4. **프록시** 탭에서 **HTTP 프록시 서버 사용**을 선택한 다음 다음 정보를 입력합니다.

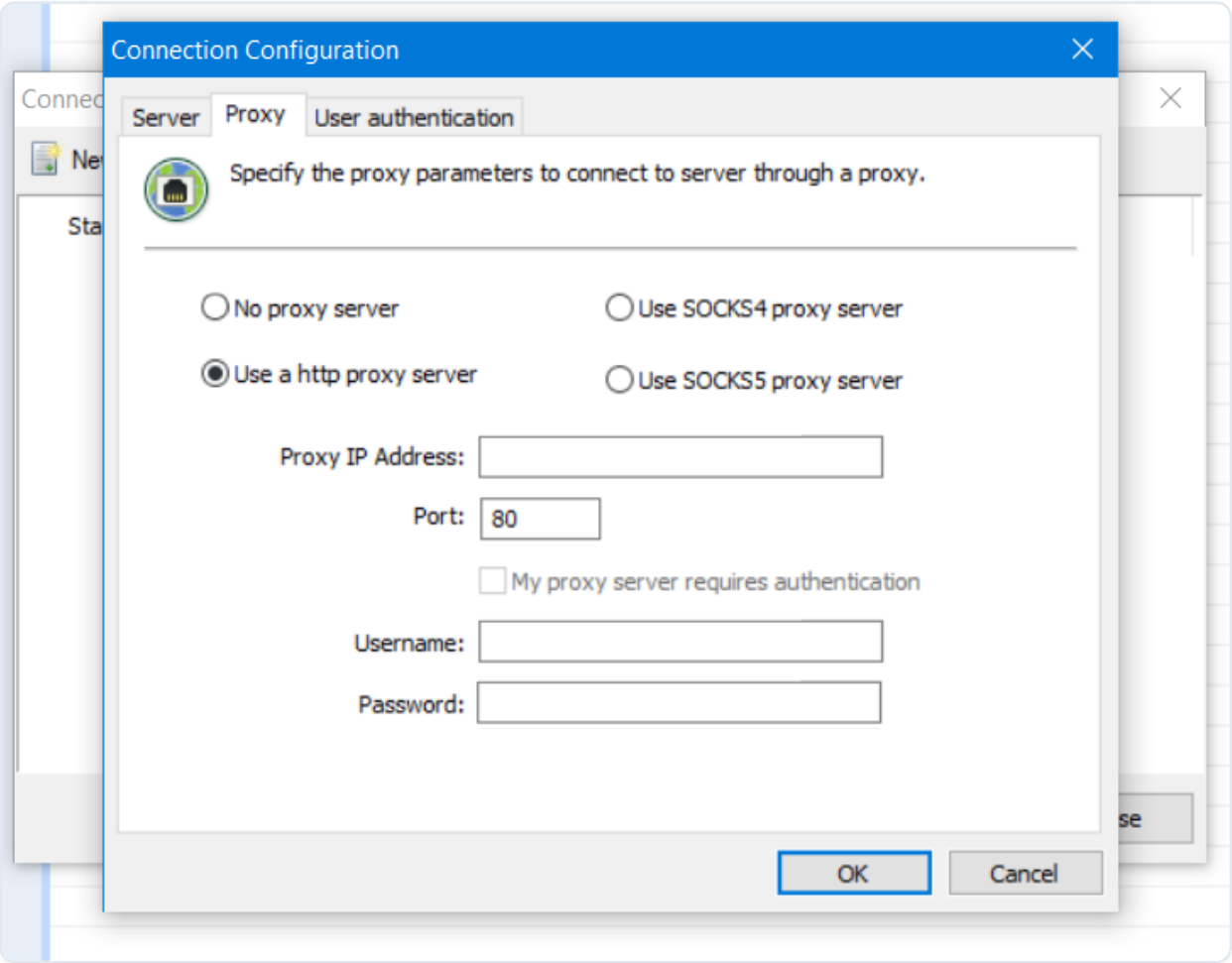
   a. **프록시 IP 주소**에 프록시 서버의 IP 주소를 입력합니다.

   b. **포트**에 프록시에서 사용하는 TCP 포트 번호를 입력합니다.

   c. 프록시 서버에서 트래픽을 허용하기 위해 인증이 필요한 경우 **내 프록시 서버에 인증 필요** 체크박스를 선택합니다.

   d. **사용자 이름**에 프록시 서버에서 인증할 사용자 이름을 입력합니다.

   e. **암호**에 프록시 서버에서 인증할 암호를 입력합니다.



5. **사용자 인증** 탭에서 **내 로그인 및 암호 기억** 체크박스를 선택하고 자격 증명을 입력합니다.
6. **확인**을 클릭합니다.

XenMobile에 연결하려면 생성한 연결을 두 번 클릭한 다음 연결에 대해 구성한 사용자 이름과 암호를 입력합니다.

Samsung Knox 장치에 대한 원격 지원을 활성화하려면

XenMobile에서 원격 지원 정책을 생성하여 Samsung Knox 장치에 대한 원격 액세스 권한을 부여합니다. 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 등이 있습니다.
- **프리미엄:** 장치 화면을 원격으로 제어할 수 있습니다. 예를 들어, 창 색상 제어, 헬프 데스크와 사용자 간의 VoIP 세션 설정, 헬프 데스크와 사용자 간의 채팅 세션 설정 등이 있습니다.

  프리미엄 지원을 사용하려면 XenMobile 콘솔에서 Samsung MDM 라이선스 키 장치 정책을 구성해야 합니다. 이 정책을 구성할 때 **Samsung KNOX** 플랫폼만 선택하십시오. Samsung SAFE 플랫폼의 경우, ELM 키는 Samsung 장치가 XenMobile에 등록될 때 자동으로 배포됩니다. 따라서 이 정책에 대해

Samsung SAFE 플랫폼을 선택하지 마십시오. 자세한 내용은 Samsung MDM 라이선스 키를 참조하십시오.

원격 지원 정책 구성에 대한 자세한 내용은 원격 지원 장치 정책을 참조하십시오.

원격 지원 세션을 사용하려면

원격 지원을 시작한 후 원격 지원 애플리케이션 창의 왼쪽에는 XenMobile 콘솔에서 정의한 XenMobile 사용자 그룹이 표시됩니다. 기본적으로 현재 연결된 사용자가 있는 그룹만 나타납니다. 각 사용자 항목 옆에 각 사용자의 장치를 볼 수 있습니다.

1. 모든 사용자를 보려면 왼쪽 열에서 각 그룹을 확장하십시오. XenMobile Server에 현재 연결된 사용자는 녹색 아이콘으로 표시됩니다.
2. 현재 연결되지 않은 사용자를 포함하여 모든 사용자를 표시하려면 **보기**를 클릭하고 **연결되지 않은 장치**를 선택합니다. 연결되지 않은 사용자는 작은 녹색 아이콘 없이 나타납니다.

XenMobile Server에 연결되어 있지만 사용자에게 할당되지 않은 장치는 익명 모드로 나타납니다. (목록에 **익명** 문자열이 나타납니다.) 로그인한 사용자의 장치와 마찬가지로 이러한 장치를 제어할 수 있습니다.

장치를 제어하려면 해당 행을 클릭한 다음 **장치 제어**를 클릭하여 장치를 선택합니다. 원격 제어 창에 장치 렌더링이 나타납니다. 제어되는 장치와 다음과 같은 방식으로 상호 작용할 수 있습니다.

- 기본 창 또는 별도의 부동 창에서 색상 제어를 포함하여 장치 화면을 제어합니다.
- 헬프 데스크와 사용자 간에 VoIP 세션을 설정합니다. VoIP 설정을 구성합니다.
- 사용자와 채팅 세션을 설정합니다.
- 장치 작업 관리자에 액세스하여 메모리 사용량, CPU 사용량 및 실행 중인 앱과 같은 항목을 관리합니다.
- 모바일 장치 로컬 디렉터리를 탐색합니다. 파일을 전송합니다.
- 장치 시스템 정보 및 설치된 모든 소프트웨어를 표시합니다.
- XenMobile Server와의 모바일 장치 연결 상태를 업데이트합니다.

시스템 로그

XenMobile® Server(온프레미스 전용)를 구성하여 로그 파일을 시스템 로그(syslog) 서버로 보낼 수 있습니다. 서버 호스트 이름 또는 IP 주소가 필요합니다.

Syslog는 두 가지 구성 요소(어플라이언스에서 실행되는 감사 모듈과 원격 시스템에서 실행될 수 있는 서버)로 구성된 표준 로깅 프로토콜입니다. Syslog 프로토콜은 데이터 전송에 사용자 데이터 프로토콜(UDP)을 사용합니다. 관리자 이벤트와 사용자 이벤트가 기록됩니다.

서버를 구성하여 다음 유형의 정보를 수집할 수 있습니다.

- XenMobile에서 수행한 작업 기록이 있는 시스템 로그.
- XenMobile의 시스템 활동에 대한 시간순 기록이 있는 감사 로그.

syslog 서버가 어플라이언스에서 수집하는 로그 정보는 메시지 형태로 로그 파일에 저장됩니다. 이러한 메시지에는 일반적으로 다음 정보가 포함됩니다.

- 로그 메시지를 생성한 어플라이언스의 IP 주소
- 타임스탬프
- 메시지 유형
- 이벤트와 관련된 로그 수준(Critical, Error, Notice, Warning, Informational, Debug, Alert 또는 Emergency)
- 메시지 정보

XenMobile은 log4j syslog 어펜더를 사용하여 RFC5424 형식의 syslog 메시지를 보냅니다. syslog 메시지 데이터는 특정 형식이 없는 일반 텍스트입니다.

이 정보를 사용하여 경고의 원인을 분석하고 필요한 경우 시정 조치를 취할 수 있습니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 톱니바퀴 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 514로 설정되어 있습니다.
    - **로그할 정보: 시스템 로그** 및 **감사**를 선택하거나 선택 취소합니다.
        - 시스템 로그에는 XenMobile에서 수행한 작업이 포함됩니다.
        - 감사 로그에는 XenMobile에 대한 시스템 활동의 시간순 기록이 포함됩니다.
        - XenMobile에 대한 디버그 로그입니다.
4. **저장**을 클릭합니다.

XenMobile®에서 로그 파일 보기

XenMobile 관리에 도움이 되도록 로그를 보고, 조작하고, 다운로드합니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 상단 모서리에 있는 렌치 아이콘을 클릭합니다. **지원** 페이지가 열립니다.

2. **로그 작업**에서 **로그**를 클릭합니다. **로그** 페이지가 나타납니다. 개별 로그가 표에 나타납니다.

   지원 로그 이미지(/en-us/xenmobile/server/media/support-logs.png)

3. 보려는 로그를 선택합니다.

   - 디버그 로그 파일에는 오류 메시지 및 서버 관련 작업과 같이 Citrix 지원에 유용한 정보가 포함되어 있습니다.
   - 관리자 감사 로그 파일에는 XenMobile 콘솔에서의 활동에 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. 표 상단의 작업을 사용하여 모두 다운로드, 보기, 회전, 단일 로그 다운로드 또는 선택한 로그 삭제를 수행합니다.

   지원 로그 분석 이미지(/en-us/xenmobile/server/media/analyze-logs.png)

   > **참고:**
   >
   > - 두 개 이상의 로그 파일을 선택하면 **모두 다운로드** 및 **회전**만 사용할 수 있습니다.
   > - 클러스터링된 XenMobile 서버가 있는 경우 연결된 서버의 로그만 볼 수 있습니다. 다른 서버의 로그를 보려면 다운로드 옵션 중 하나를 사용하십시오.

5. 다음 중 하나를 수행합니다.

   - **모두 다운로드:** 콘솔이 시스템에 있는 모든 로그(디버그, 관리자 감사, 사용자 감사, 서버 로그 등 포함)를 다운로드합니다.
   - **보기:** 선택한 로그의 내용을 테이블 아래에 표시합니다.
   - **회전:** 현재 로그 파일을 보관하고 로그 항목을 캡처할 파일을 생성합니다. 로그 파일을 보관할 때 대화 상자가 나타납니다. 계속하려면 Rotate를 클릭합니다.
   - **다운로드:** 콘솔이 선택한 단일 로그 파일 유형만 다운로드합니다. 또한 해당 유형의 보관된 로그도 다운로드합니다.
   - **삭제:** 선택한 로그 파일을 영구적으로 제거합니다.

   디버그 로그 예시 이미지(/en-us/xenmobile/server/media/debug-log-file-example.png)

XenMobile® Server 텔레메트리 데이터 요소

XenMobile Server 구성

이벤트 헤더

키	설명	예시
버전	헤더 버전을 나타냅니다.	1
id	고유 이벤트 ID(GUID)를 나타냅니다.	고유 식별자
유형	이벤트 유형 이름을 나타냅니다.	SYSTEM_CONFIGURATION
st	UTC 형식의 타임스탬프를 나타냅니다.	2011-08-12T20:17:46.384Z
제품	제품 이름을 나타냅니다.	XenMobile.OnPrem
prodVer	제품 버전을 나타냅니다.	10.16.0.10123

이벤트 페이로드

키	설명	예시
버전	XenMobile Server 구성 페이로드 버전 번호를 나타냅니다.	1.1
xmsVer	XenMobile Server 버전 번호를 나타냅니다.	10.16.0.48
xmsrpVer	XenMobile Server 롤링 패치 버전 번호를 나타냅니다.	10.16.0.10323
dbType	XenMobile Server 데이터베이스 유형을 나타냅니다.	MSSQL

키	설명	예시
dbVer	XenMobile Server 데이터베이스 버전 번호를 나타냅니다.	Microsoft SQL Server 2019 (RTM-CU8) (KB4577194) - 15.0.4073.23 (X64) Sep 23 2020 16:03:08 저작권 (C) 2019 Microsoft Corporation 표준 에디션 (64비트) Windows Server 2016 Standard 10.0 X64 (Build 14393:)에서 (하이퍼바이저)
hostType	XenMobile Server 하이퍼바이저 유형을 나타냅니다.	온프레미스 - XenServer®
instanceName	XenMobile Server 인스턴스 이름을 나타냅니다.	경로
licenseType	XenMobile Server 활성화된 라이선스 유형을 나타냅니다.	CXM_ENTU_UD
sp	수집할 모든 서버 속성을 나타냅니다.	sp: {afw_restriction_v2: 참 device_page_enhancement_new: 참 다중 모드: 참 http2_alternate_port: 거짓 playemmapi_update: 참 afw_efota: 참

키	설명	예시	
		password_strength: 참 모드: ENT WSDL: 거짓 afw_restriction_cope: 참 playemmapi: 활성화됨 mac_app_push: 활성화됨 ga: 참 zdm_pki: 참 tiffany: 거짓 ios_mdm: 참 nac_mail: 거짓 console_ceip: 참 ssl_sign: 참 wip: 참 zebra: 참 apple_apns_http2: 참 afw_hide_vpn_always_on: 참 force_push_apps: 참	

키	설명	예시	
		ftu: 거짓 afw_vpn_always_on_lockdown: 참 mfa: 참 mobile_service_provider: 참 afw_network_domain: 참 deprecate_sms: 참 cert_self_signed: 참 ios_http2_pushtype_bg: 거짓 device_update_awapppushtask: 활성화됨 android.deprecate.policy: 참 device_page_enhancement: 참 macos_http2_pushtype_bg: 거짓 edu_shared_ipad: 참 sync_license: 거짓 force_push_apps_flag: 참 shp: 거짓	

키	설명	예시
		wsapi: 거짓 aw_dg_performance: 참 애플 프로필 갱신: 참 AFW 우선순위 앱 업데이트: 참 esim: 참 wpcod: 참 knox: 참 device_report: 참 ios_app_update: 참 mspki_revert: 참}

키	설명	예시
cp	수집할 모든 클라이언트 속성을 나타냅니다.	cp: {PASSCODE_STRENGTH: 보통 ENABLE_WORXHOME_CEIP: 거짓 ENABLE_FIPS_MODE: 거짓 DEVICE_LOGS_TO_IT_HELP_DESK: 거짓 ENABLE_WORXHOME_GA: 참 ENCRYPT_SECRETS_USING_PASSCODE: 거짓 ENABLE_PASSCODE_AUTH: 거짓 ON_FAILURE_USE_EMAIL: 참 PASSCODE_TYPE: 숫자 CONTAINER_SELF_DESTRUCT_PERIOD: 0 PASSCODE_MIN_LENGTH: 6 ENABLE_CRASH_REPORTING: 예

키	설명	예시
		PASSCODE_EXPIRY: 90 INACTIVITY_TIMER: 15 ENABLE_PASSWORD_CACHING: 거짓 PASSCODE_MAX_ATTEMPTS: 15 PASSCODE_HISTORY: 5 로깅 비활성화: false Touch ID 인증 활성화: false 비콘 확인 활성화: false}
enrolledDevices	등록된 장치 수를 나타냅니다.	enrolledDevices: {ANDROID:1,iOS:2,MACOSX:1}
정규화된 도메인 이름	고객의 공용 FQDN을 나타냅니다.	zl225.xmqa.cloud.com
ladpAuthType	LDAP 인증 유형을 나타냅니다.	도메인
nodeCount	클러스터의 노드 수를 나타냅니다.	4
managedApps	XenMobile Server에서 관리하는 애플리케이션 수를 나타냅니다.	1000

키	설명	예시
usersUsingMicroVPN	MicroVPN 사용자 수를 나타냅니다.	9999
isIntuneIntegrated	Intune이 XenMobile Server와 통합되었는지 여부를 나타냅니다.	참
configuratedPolicies	XenMobile Server에서 구성한 정책 수를 나타냅니다.	7777

XenMobile Server 사용량

이벤트 헤더

키	설명	예시
버전	헤더 버전을 나타냅니다.	1
id	고유한 이벤트 ID(GUID)를 나타냅니다.	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
유형	이벤트 유형 이름을 나타냅니다.	DEVICE_CHECKIN
st	UTC 형식의 타임스탬프를 나타냅니다.	2011-08-12T20:17:46.384Z
제품	제품 이름을 나타냅니다.	XenMobile.OnPrem
prodVer	제품 버전을 나타냅니다.	10.16.0.10123
사용자	사용자 정보를 나타냅니다. 로컬 사용자의 경우 페이로드에 SID가 없습니다. **값은 스크램블됩니다.**	**AD 사용자** 사용자: {

키	설명	예시
		upn: C982F651A44B3F7 **(항상 스크램블됨)** domain: C982F651A44B3F7 **(항상 스크램블됨)** email: C982F651A44B3F7 **(항상 스크램블됨)** sid: C982F651A44B3F7 **(항상 스크램블됨)}** **로컬 사용자** 사용자: { upn: C982F651A44B3F7 **(항상 스크램블됨)** sAMAccountName: C982F651A44B3F7 **(항상 스크램블됨)**}

이벤트 페이로드

키	설명	예시
버전	XenMobile Server 사용량 페이로드의 버전 번호를 나타냅니다.	1.1
deviceType	장치 유형을 나타냅니다.	iPhone
hostName	온프레미스 배포를 위한 고객의 fqdn을 나타냅니다.	test.xmqa.cloud.com

키	설명	예시
platformInfo	장치 플랫폼을 나타냅니다.	iPhone - iPhone
jailBroken	이 키는 장치가 **탈옥**되었거나 **루팅**된 경우에만 사용할 수 있습니다. 태그가 없으면 장치는 탈옥되거나 루팅되지 않은 것입니다.	예 또는 아니요
serialNum	기본적으로 해시 처리된 장치의 일련 번호를 나타냅니다.	KsPRhShj0h9IhbVkFEU7ZQ==
os	장치의 OS 유형을 나타냅니다.	iOS
managementMode	장치 관리 모드를 나타냅니다.	mdm 또는 mam 또는 xme 또는 unmanaged
deviceId	장치의 내부 고유 ID를 나타냅니다.	41CC018E-7CC0-4697-B07E-1E8CCEF7F592
감독됨	장치가 감독 대상인지 여부를 나타냅니다.	예 또는 아니요
osVersion	장치의 OS 버전 번호를 나타냅니다.	16.4.1 (a)
아이엠이아이	사용 가능한 경우 장치의 IMEI 번호를 나타내며, 기본적으로 해시 처리됩니다.	6M6iBmcsokQxPQyeVwiaQQ==
deviceModel	장치의 모델을 나타냅니다.	iPhone
lastActivity	장치의 마지막 활동 타임스탬프를 나타냅니다.	2024-03-29 14:17:14.277
corporateOwned	장치가 회사 소유인지 여부를 나타냅니다.	아니요
enabledFeatures	여러 기능의 활성화 여부를 나타냅니다.	1
엘피이아이디	고유한 XMS 사이트를 식별하는 데 사용할 수 있는 고유 환경 ID를 나타냅니다.	95ba4968cfaf069c20949d76473ecd4f3994f556d0fef7f2fa11

키	설명	예시
		912731d720bf 또는 LAS를 사용할 수 없는 경우 공백

REST API

> **참고:**
>
> 이 문서에서는 XenMobile Server용 REST API에 대해 설명합니다. Endpoint Management용 REST API에 대한 자세한 내용은 REST API를 참조하십시오.

> XenMobile® REST API를 사용하면 XenMobile 콘솔을 통해 노출되는 서비스를 호출할 수 있습니다. 모든 REST 클라이언트를 사용하여 REST 서비스를 호출할 수 있습니다. API는 서비스를 호출하기 위해 XenMobile 콘솔에 로그인할 필요가 없습니다.

사용 가능한 API의 전체 최신 세트는 REST 서비스용 공개 API PDF를 다운로드하십시오.

REST API 액세스에 필요한 권한

REST API에 액세스하려면 다음 권한 중 하나가 필요합니다.

- 역할 기반 액세스 구성의 일부로 설정된 공개 API 액세스 권한. 자세한 내용은 RBAC를 사용하여 역할 구성을 참조하십시오.
- 슈퍼 사용자 권한

REST API 서비스 호출

REST 클라이언트 또는 cURL 명령을 사용하여 REST API 서비스를 호출할 수 있습니다. 다음 예제에서는 Chrome용 Advanced REST 클라이언트를 사용합니다.

> **참고:**
>
> 다음 예제에서 호스트 이름과 포트 번호를 사용자 환경에 맞게 변경하십시오.

로그인

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

요청: `{ "login":"administrator", "password":"password" }`

메서드 유형: POST

콘텐츠 유형: application/json

로그인 페이로드 및 요청/응답 헤더 이미지(/en-us/xenmobile/server/media/rest-1.png)

관련 정보

- XenMobile REST API

익스체인지 액티브싱크용 엔드포인트 관리 커넥터

XenMobile Mail Manager는 이제 Exchange ActiveSync용 Endpoint Management 커넥터입니다. Citrix 통합 포트폴리오에 대한 자세한 내용은 Citrix 제품 가이드를 참조하십시오.

이 커넥터는 다음과 같은 방식으로 XenMobile®의 기능을 확장합니다.

- Exchange Active Sync(EAS) 장치에 대한 동적 액세스 제어. EAS 장치는 Exchange 서비스에 대한 액세스를 자동으로 허용하거나 차단할 수 있습니다.
- XenMobile이 Exchange에서 제공하는 EAS 장치 파트너십 정보에 액세스하는 기능.
- XenMobile이 EAS 상태에 따라 모바일 장치를 초기화하는 기능.
- XenMobile이 Blackberry 장치에 대한 정보에 액세스하고 초기화(Wipe) 및 암호 재설정(ResetPassword)과 같은 제어 작업을 수행하는 기능.

EAS 상태에 따라 장치를 초기화하려면 ActiveSync 트리거로 자동화된 작업을 구성하십시오. 자동화된 작업을 참조하십시오.

Exchange ActiveSync용 Endpoint Management 커넥터를 다운로드하려면:

1. `<https://www.citrix.com/downloads>`으로 이동합니다.
2. **Citrix Endpoint Management™ (및 Citrix XenMobile Server) > XenMobile Server (온프레미스) > 제품 소프트웨어 > XenMobile Server 10 > 서버 구성 요소**로 이동합니다.
3. **Exchange ActiveSync용 Citrix Endpoint Management 커넥터** 타일에서 **파일 다운로드**를 클릭합니다.

> **중요:**
>
> 2022년 10월부터 Microsoft가 여기에서 발표한 인증 변경 사항으로 인해 Exchange ActiveSync용 Endpoint Management 및 Citrix Gateway 커넥터는 더 이상 Exchange Online을 지원하지 않습니다. Exchange용 Endpoint Management 커넥터는 Microsoft Exchange Server(온프레미스)에서 계속 작동합니다.

새로운 기능

다음 섹션에서는 이전에 XenMobile Mail Manager였던 Exchange ActiveSync용 Endpoint Management 커넥터의 새로운 기능을 나열합니다.

버전 10.1.10의 새로운 기능

버전 10.1.10에서 다음 문제가 해결되었습니다.

- 네트워크 문제가 자주 발생하는 고객은 이전에 제공된 세 번의 시도 내에 스냅샷을 완료하지 못할 수 있습니다. 이 릴리스에서는 관리자가 최대 시도 횟수(1-10)를 구성할 수 있습니다. 이 수정 사항을 통해 스냅샷 프로세스를 완전히 중단하지 않고도 통신 중단이 여러 번 발생하더라도 스냅샷을 수행할 수 있습니다. (/en-us/xenmobile/server/media/snapshot-type-exchange-activesync-connector.png)
- 이전 버전에서는 스냅샷 유형이 Exchange 구성 목록에 나타나지 않았습니다. 이제 스냅샷 유형이 나타납니다.
- PowerShell에서 보고된 PSRemotingTransport 예외는 Exchange에 대한 세션이 더 이상 유효하지 않음을 나타냅니다. 이 상태는 기본적으로 구성 파일의 중요 오류 목록에 추가됩니다. 이렇게 하면 PSRemotingTransportException이 감지될 때 연결이 나중에 폐기될 오류 상태로 표시됩니다. 다음 통신은 유효한 연결을 사용하거나 연결을 생성합니다.
- 구성 변경 사항이 저장될 때, 새 구성을 로드하기 전에 이전에 구성된 모든 내부 구성 요소가 제대로 폐기되지 않았을 수 있습니다. 이 문제는 예측할 수 없는 동작으로 이어질 수 있습니다. 동작은 특정 변경 사항과 변경 사항이 이전 구성과 충돌했는지 여부에 따라 달라집니다. 이 릴리스에서는 새 구성을 로드하기 전에 모든 내부 구성 요소가 폐기됩니다.

이전 버전의 새로운 기능

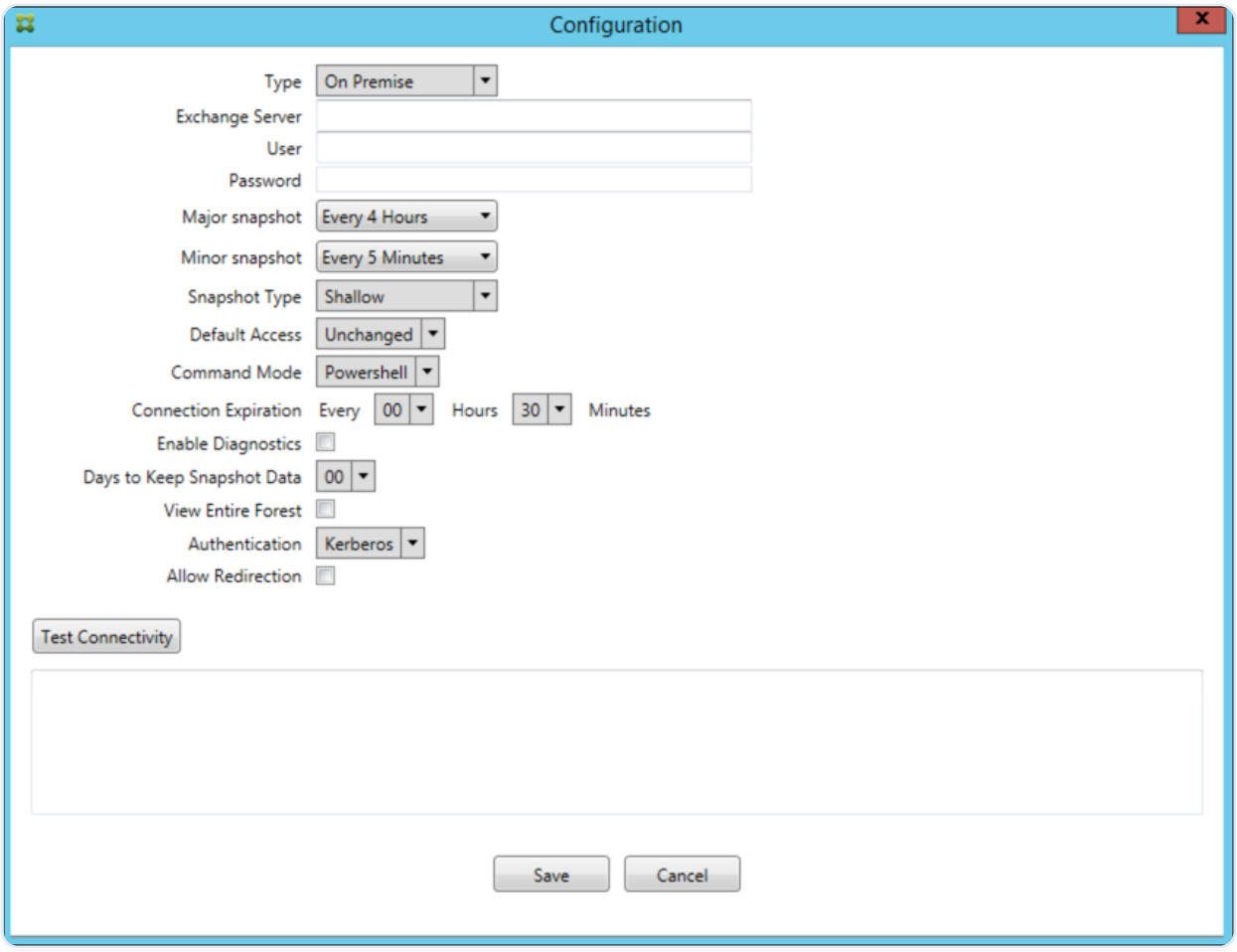
다음 섹션에서는 Exchange ActiveSync용 Endpoint Management 커넥터의 이전 버전에서 제공되는 기능 및 해결된 문제를 나열합니다.

버전 10.1.9의 새로운 기능

버전 10.1.9에서 다음 문제가 해결되었습니다.

- 이제 구성 변경 사항이 보다 일관된 방식으로 처리됩니다. 서비스가 구성 변경을 감지하면 각 내부 서브시스템이 중지되어 활성 또는 예약된 모든 처리가 중단됩니다. 다음으로 새 구성이 로드되고 서브시스템이 다시 시작되어 모든 스케줄 및 기타 내부 인프라가 새 설정으로 재설정됩니다. 이 문제는 버전 10.1.8의 알려진 문제를 수정합니다.
- 업그레이드 중에 기존 데이터베이스 구성이 새 구성 파일에 병합되지 않았습니다. 이제 데이터베이스 구성이 업그레이드된 구성 파일에 병합됩니다.

- 스냅샷 관련 진단 파일에서 열 헤더가 누락되었습니다. 헤더가 복원되었습니다.
- 이전 버전에서 업그레이드할 때 구성 파일의 기본값 섹션이 사용 중인 구성 파일의 유사한 섹션으로 덮어쓰여졌습니다. 이 문제로 인해 업그레이드 후 서비스에서 기본값 섹션에 대한 추가 또는 개선 사항이 로드되지 않았습니다. 이 버전부터 기본값 섹션은 항상 최신 구성을 반영합니다.
- 관리자는 애플리케이션 실행 시 Shift 키를 눌러 특정 옵션에 더 이상 액세스할 수 없습니다. 이러한 옵션은 이전에 Citrix 권한으로 사용할 수 있었습니다. 이제 일부 옵션(예: 리디렉션 허용)은 완전히 사용할 수 있으며, 다른 옵션(예: 중단 감지 및 개수 수정)은 더 이상 사용되지 않습니다.



버전 10.1.8의 새로운 기능

버전 10.1.8에서 다음 문제가 해결되었습니다.

- Exchange가 Exchange ActiveSync 서비스용 Citrix Endpoint Management 커넥터가 너무 자주 명령을 발행하는 것을 제한할 수 있습니다. 이는 Office 365 연결에서 흔히 발생합니다. 제한의 영향으로 인해 서비스는 다음 명령을 보내기 전에 지정된 기간 동안 일시 중지해야 합니다. 이제 구성 콘솔에 일시 중지 남은 시간이 표시됩니다.
- 구성 파일(config.xml)의 "Watchdog" 또는 "SpecialistsDefaults" 섹션을 수정해도 업그레이드 후 구성 파일에 변경 사항이 반영되지 않습니다. 이 릴리스에서는 수정 사항이 새 구성 파일에 올바르게 병합됩니다.

- Google Analytics로 전송되는 분석에 특히 스냅샷과 관련하여 더 많은 세부 정보가 추가되었습니다.
- Exchange 연결 테스트 기능은 연결을 한 번만 초기화하려고 시도했습니다. Office 365 연결은 제한될 수 있으므로, 제한될 때 연결 테스트가 실패한 것처럼 보일 수 있었습니다. Exchange ActiveSync용 Citrix Endpoint Management 커넥터는 이제 연결을 최대 세 번까지 시도합니다.
- Exchange에 정책을 적용하려면 Exchange ActiveSync용 Citrix Endpoint Management 커넥터가 각 사서함에 대한 모든 관련 장치를 허용 및 차단이라는 두 가지 목록으로 포함하는 **Set-CASMailbox** 명령을 컴파일해야 합니다. 장치가 두 목록 중 어느 하나에도 포함되지 않으면 Exchange는 기본 액세스 상태로 돌아갑니다. 해당 기본 액세스 상태가 장치에 대해 원하는 상태와 다르면 해당 장치는 규정 미준수 상태가 됩니다. 결과적으로 Exchange 기본 액세스 상태가 차단되어야 하는데 허용된 경우 사용자는 이메일 액세스 권한을 잃을 수 있습니다. 또는 이메일 액세스가 차단되어야 하는 사용자에게 액세스 권한이 부여될 수 있습니다. Exchange ActiveSync용 Citrix Endpoint Management 커넥터는 이제 유효한 원하는 상태를 가진 모든 장치가 각 **Set-CasMailbox** 명령에 포함되도록 합니다.

버전 10.1.8에서 알려진 문제는 다음과 같습니다.

관리자가 구성 데이터를 수정하는 구성 애플리케이션에서 변경 사항을 적용하는 동안 서비스가 스냅샷 또는 정책 평가와 같은 장시간 작업을 수행 중인 경우 서비스가 불확실한 상태로 전환될 수 있습니다. 가능한 증상으로는 정책 변경이 처리되지 않거나 스냅샷이 시작되지 않는 것 등이 있습니다. 서비스를 작동 상태로 되돌리려면 서비스를 다시 시작해야 합니다. 서비스를 시작하기 전에 Windows 서비스 관리자를 사용하여 서비스 프로세스를 종료해야 할 수도 있습니다.

버전 10.1.7의 새로운 기능

- XenMobile Mail Manager는 이제 Exchange ActiveSync용 Endpoint Management 커넥터입니다.
- Exchange 구성 대화 상자에서 **파이프라이닝 비활성화** 옵션은 더 이상 사용되지 않습니다. config.xml 파일에서 각 명령에 대해 여러 단계를 구성하여 동일한 기능을 구현할 수 있습니다.

버전 10.1.7에서 다음 문제가 해결되었습니다.

- 스냅샷 기록 창에서 오류 메시지가 컨텍스트 없이 표시될 수 있습니다. 이제 오류 메시지에는 발생한 위치의 컨텍스트가 접두사로 붙습니다.
- XmmGoogleAnalytics .dll에 릴리스에 해당하는 파일 버전이 없었습니다.
- 진단을 개선하기 위해 최근 사서함 허용/차단 상태를 설정하는 데 사용되는 장치 ID 목록의 문자열 형식을 변경했습니다. 그러나 너무 많은 장치를 지정하면 최대 문자열 크기를 초과했습니다. 이제 내부 배열 데이터 구조를 사용합니다. 이 구조는 크기 제한이 없으며 진단 목적에 맞게 데이터를 적절하게 포맷합니다.
- Exchange와 동기화되지 않은 장치 정책이 감지되면 해당 명령에는 관련 사서함에 속하지 않는 장치가 포함될 수 있습니다. Endpoint Management connector for Exchange ActiveSync는 이제 Exchange에 대한 명령이 해당 사서함에 속하는 장치만 나타내도록 합니다.

- 일부 환경에서는 Microsoft 어셈블리를 사용할 수 없습니다. 이제 필요한 어셈블리가 애플리케이션과 함께 명시적으로 설치됩니다.
- 장치 또는 사서함의 고유 이름에 특성 이름과 등호 사이에 공백이 있거나 등호 뒤와 값 앞에 공백이 있는 경우 Endpoint Management connector for Exchange ActiveSync는 장치를 해당 사서함과 올바르게 일치시키지 못하거나 그 반대의 경우도 마찬가지일 수 있습니다. 그 결과 스냅샷 조정 중에 일부 장치 및/또는 사서함이 거부될 수 있습니다.

> **참고:**

> 다음 섹션에서는 Endpoint Management connector for Exchange ActiveSync를 이전 이름인 XenMobile Mail Manager로 지칭합니다. 이름은 버전 10.1.7부터 변경되었습니다.

버전 10.1.6.20의 업데이트

10.1.6 업데이트에는 버전 10.1.6.20의 다음 수정 사항이 포함되어 있습니다.

- Exchange와 동기화되지 않은 장치 정책이 감지되면 해당 명령에는 관련 사서함에 속하지 않는 장치가 포함될 수 있습니다. 이제 XenMobile Mail Manager는 Exchange에 대한 명령이 해당 사서함에 속하는 장치만 나타내도록 합니다.

버전 10.1.6의 새로운 기능

XenMobile Mail Manager 버전 10.1.6에는 다음과 같은 해결된 문제 및 개선 사항이 포함되어 있습니다.

- 스냅샷 기록 창이 때때로 더 이상 업데이트되지 않는 상태가 됩니다. 창 새로 고침 메커니즘이 개선되어 더 안정적으로 업데이트됩니다.
- 분할된 스냅샷과 분할되지 않은 스냅샷에 대해 두 가지 별도의 모드와 코드 경로가 사용되었습니다. 분할되지 않은 스냅샷은 단일 "*" 파티션을 사용하는 구성의 분할된 스냅샷과 동일하므로 분할되지 않은 스냅샷 모드는 제거되었습니다. 이제 기본 스냅샷 모드는 36개의 파티션(0-9, A-Z)을 가진 분할된 스냅샷입니다.
- 스냅샷 기록 창에서 오류 메시지가 상태 메시지로 덮어쓰여집니다. 이제 XenMobile Mail Manager는 사용자가 상태와 오류를 동시에 볼 수 있도록 두 개의 별도 필드를 제공합니다.
- Exchange Online (Office 365)에 연결할 때 스냅샷 관련 쿼리로 인해 데이터 세트가 잘릴 수 있습니다. 이 문제는 XenMobile Mail Manager가 다중 명령 파이프라인 스크립트를 실행할 때 발생할 수 있습니다. 업스트림 명령이 다운스트림 명령에 데이터를 충분히 빠르게 전달할 수 없어 작업이 조기에 완료됩니다. 그 결과 불완전한 데이터가 발생합니다. 이제 XenMobile Mail Manager는 파이프라인 자체를 모방하여

업스트림 명령이 완료될 때까지 기다린 후 다운스트림 명령을 호출할 수 있습니다. 이 변경으로 모든 데이터가 처리되고 캡처되어야 합니다.

- Exchange에 대한 정책 업데이트 명령에서 해결할 수 없는 오류가 발생하면 동일한 명령이 오랫동안 작업 대기열로 반복적으로 반환됩니다. 이 상황으로 인해 명령이 Exchange로 여러 번 전송되었습니다. 이 버전의 XenMobile Mail Manager에서는 오류가 발생하는 명령이 정해진 횟수만큼만 작업 대기열로 반환됩니다.
- 특정 사서함에 대한 정책 업데이트에 모든 장치 허용 또는 차단이 포함된 경우: 발행된 **Set-CASMailbox** 명령은 빈 목록이 **NULL** 대신 빈 문자열로 변환되어 실패했습니다. 이제 올바른 데이터가 전송됩니다.
- 새 장치를 처리할 때 Exchange는 한동안 (일반적으로 15분) 상태를 "DeviceDiscovery"로 반환할 수 있습니다. XenMobile Mail Manager는 이 상태를 특별히 처리하지 않았습니다. 이제 XenMobile Mail Manager는 이 상태를 처리합니다. UI의 모니터 탭에서 사용자는 이 상태의 장치를 필터링할 수 있습니다.
- XenMobile Mail Manager는 XenMobile Mail Manager 데이터베이스에 쓸 수 있는 권한을 확인하지 않았습니다. 결과적으로 권한이 제한된 경우 동작을 예측할 수 없었습니다. 이제 XenMobile Mail Manager는 데이터베이스에서 필요한 권한을 캡처하고 유효성을 검사합니다. XenMobile Mail Manager는 연결 테스트 시 (메시지 표시) 또는 기본 구성 창 하단의 데이터베이스 표시기 (메시지를 보려면 마우스 오버)에서 권한이 축소되었음을 나타냅니다.
- 현재 워크로드에 따라 지시를 받을 때 XenMobile Mail Manager 서비스가 즉시 중지되지 않을 수 있습니다. 따라서 서비스가 응답하지 않는 상태인 것처럼 보입니다. 개선 사항을 통해 진행 중인 작업을 중단할 수 있어 보다 원활한 종료가 가능합니다.

버전 10.1.5의 새로운 기능

XenMobile Mail Manager 버전 10.1.5에는 다음과 같은 해결된 문제가 포함되어 있습니다.

- Exchange가 XenMobile Mail Manager 활동에 스로틀링을 적용할 때 (로그 외에는) 스로틀링이 발생하고 있다는 표시가 없습니다. 이 릴리스에서는 사용자가 활성 스냅샷 위에 마우스를 올리면 "스로틀링" 상태가 나타납니다. 또한 XenMobile Mail Manager가 스로틀링되는 동안 Exchange가 스로틀링 금지를 해제할 때까지 주요 스냅샷 시작이 금지됩니다.
- 주요 스냅샷 중에 XenMobile Mail Manager가 Exchange에 의해 스로틀링되는 경우: 다음 스냅샷 시도를 실행하기 전에 충분한 시간이 경과되지 않을 수 있습니다. 이 문제로 인해 추가 스로틀링 및 스냅샷 실패가 발생합니다. 이제 XenMobile Mail Manager는 Exchange가 스냅샷 시도 사이에 대기하도록 지정한 최소 시간만큼 기다립니다.
- 진단이 활성화되면 명령 파일에 각 속성 이름 앞에 하이픈이 누락된 **Set-CasMailbox** 명령이 표시됩니다. 이 문제는 진단 파일의 형식에서만 발생하며 Exchange에 대한 실제 명령에서는 발생하지 않습니다.

누락된 하이픈으로 인해 사용자가 명령을 잘라내어 테스트 또는 유효성 검사를 위해 PowerShell 프롬프트에 직접 붙여넣을 수 없었습니다. 하이픈이 추가되었습니다.

- 사서함 ID가 "성, 이름" 형식인 경우 Exchange는 쿼리에서 데이터를 반환할 때 쉼표 앞에 백슬래시를 추가합니다. XenMobile Mail Manager가 이 ID를 사용하여 추가 데이터를 쿼리할 때 이 백슬래시를 제거해야 합니다.

알려진 제한 사항

> **참고:**

> 다음 제한 사항은 버전 10.1.6에서 해결되었습니다.

> XenMobile Mail Manager에는 Exchange 명령이 실패할 수 있는 알려진 제한 사항이 있습니다. Exchange에 정책 변경 사항을 적용하기 위해 XenMobile Mail Manager에서 **Set_CASMailbox** 명령을 실행합니다. 이 명령은 허용할 장치 목록과 차단할 장치 목록, 두 가지 장치 목록을 사용할 수 있습니다. 이 명령은 사서함과 파트너 관계를 맺은 장치에 적용됩니다.

이러한 목록은 Microsoft API에 의해 각각 256자로 제한됩니다. 이 목록 중 하나라도 제한을 초과하면 명령이 전체적으로 실패하여 해당 사서함 장치에 대한 모든 정책을 설정할 수 없게 됩니다. XenMobile Mail Manager 로그에 나타나는 보고된 오류는 다음과 같습니다. 이 예는 차단된 목록에 대한 것입니다.

“메시지: '매개 변수 'ActiveSyncBlockedDeviceIDs'를 대상으로 바인딩할 수 없습니다. "ActiveSyncBlockedDeviceIDs" 설정 예외: "속성 길이가 너무 깁니다. 최대 길이는 256이고 제공된 값의 길이는 …"

장치 ID 길이는 다를 수 있지만, 약 10개 이상의 장치가 동시에 허용되거나 차단되면 제한을 초과할 수 있다는 것이 좋은 지침입니다. 특정 사서함과 연결된 장치가 그렇게 많은 경우는 드물지만, 가능성은 있습니다. XenMobile Mail Manager가 이러한 시나리오를 처리하도록 개선될 때까지 사용자 및 사서함과 연결된 장치 수를 10개 이하로 제한하는 것이 좋습니다.

버전 10.1.4의 새로운 기능

XenMobile Mail Manager 버전 10.1.4에는 다음과 같은 해결된 문제가 포함되어 있습니다.

- 보안이 약화됨에 따라 PCI 위원회에서 TLS 1.0을 더 이상 사용하지 않도록 권고하고 있습니다. XenMobile Mail Manager에 TLS 1.1 및 1.2 지원이 추가되었습니다.

- XenMobile Mail Manager에는 새로운 진단 파일이 포함되어 있습니다. Exchange 사양에서 **진단 사용**을 선택하면 새로운 스냅샷 기록 파일이 생성됩니다. 스냅샷을 시도할 때마다 스냅샷 결과와 함께 한 줄이 파일에 추가됩니다.
- 명령 진단 파일에서 **Set-CASMailbox** 명령에 대해 허용되거나 차단된 장치 목록이 나타나지 않았습니다. 대신 관련 인수에 대해 내부 클래스 이름이 파일에 표시되었습니다. 이제 XenMobile Mail Manager는 deviceID 목록을 쉼표로 구분된 목록으로 표시합니다.
- 잘못된 사양으로 인해 Exchange에 대한 연결을 시도하는 데 실패할 경우: 오류 메시지가 잘못된 메시지인 "모든 연결 사용 중"으로 덮어쓰여집니다. 이제 "모든 연결이 작동하지 않음", "연결 풀이 비어 있음", "모든 연결이 제한됨", "사용 가능한 연결 없음"과 같은 더 설명적인 메시지가 나타납니다.
- 때때로 허용/차단/초기화 명령이 XenMobile Mail Manager 내부 캐시에 여러 번 대기열에 추가됩니다. 이 문제로 인해 명령이 Exchange로 전송되는 데 지연이 발생합니다. 이제 XenMobile Mail Manager는 각 명령의 인스턴스를 하나만 대기열에 추가합니다.

버전 10.1.3의 새로운 기능

- **Google Analytics 지원:** XenMobile Mail Manager를 어떻게 사용하시는지 파악하여 제품을 개선할 수 있는 부분에 집중하고자 합니다.
- **진단 사용 설정: 구성** 대화 상자의 구성 콘솔에 **진단 사용** 확인란이 나타납니다.

Exchange ActiveSync용 엔드포인트 관리 커넥터 콘솔 이미지(/en-us/xenmobile/server/media/mail-manager-diagnostics-checkbox.png)

버전 10.1.3에서 해결된 문제

- **스냅샷 기록** 창에서 스냅샷의 현재 상태를 보여주는 도구 설명이 실제 상태를 반영하지 않습니다. 가끔 XenMobile Mail Manager가 명령 진단 파일에 쓸 수 없습니다. 이 경우 명령 기록이 전체적으로 기록되지 않습니다.
- 연결에 오류가 발생하면 연결이 "오류 발생"으로 표시되지 않을 수 있습니다. 결과적으로 후속 명령이 연결을 사용하려고 시도하여 또 다른 오류를 일으킬 수 있습니다.
- Exchange Server에서 스로틀링이 발생하면 상태 확인 루틴에서 예외가 발생할 수 있습니다. 결과적으로 오류가 발생했거나 만료된 연결이 제거되지 않을 수 있습니다. 또한 XenMobile Mail Manager는 스로틀링 시간이 만료될 때까지 연결을 생성하지 않을 수 있습니다.
- Exchange의 최대 세션 수가 초과되면 XenMobile Mail Manager는 "장치 캡처 실패"라는 오류를 보고하는데, 이는 정확한 메시지가 아닙니다. 대신, XenMobile Mail Manager가 Exchange 통신에 일반적으로 사용하는 두 세션이 사용 중임을 나타내는 메시지가 표시되어야 합니다.

버전 10.1.2의 새로운 기능

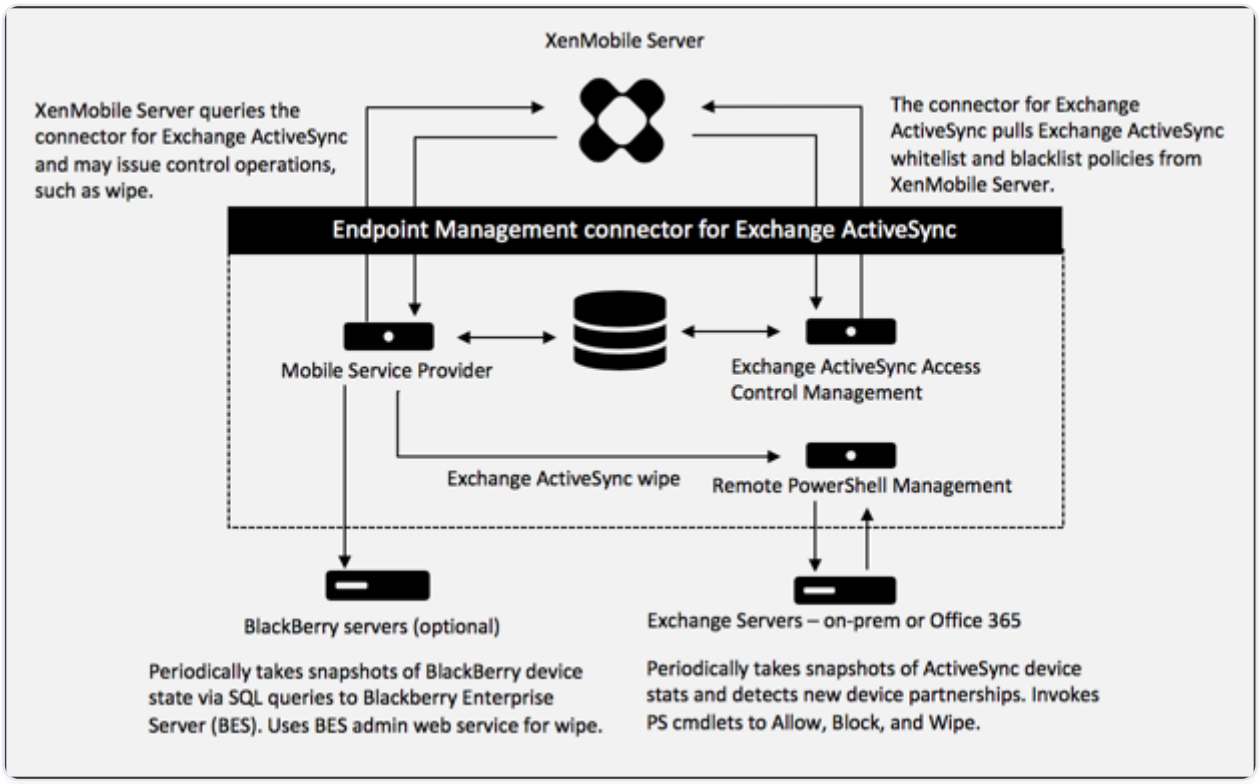
- **Exchange 연결 개선**: XenMobile Mail Manager는 PowerShell 세션을 사용하여 Exchange와 통신합니다. PowerShell 세션, 특히 Office 365를 다룰 때 시간이 지나면 불안정해져 후속 명령이 성공하지 못하게 될 수 있습니다. 이제 XenMobile Mail Manager는 연결에 대한 만료 기간을 설정할 수 있습니다. 연결이 만료 시간에 도달하면 XenMobile Mail Manager는 PowerShell 세션을 정상적으로 종료하고 새 세션을 생성합니다. 이렇게 함으로써 PowerShell 세션이 불안정해질 가능성이 줄어들어 스냅샷 실패 가능성이 크게 감소합니다.
- **스냅샷 워크플로 개선**: 주요 스냅샷은 시간이 많이 걸리고 프로세스 집약적인 작업입니다. 스냅샷 중에 오류가 발생하면 XenMobile Mail Manager는 이제 스냅샷을 완료하기 위해 여러 번(최대 3회) 시도합니다. 후속 시도는 처음부터 시작하지 않습니다. XenMobile Mail Manager는 중단된 지점부터 계속 진행합니다. 이 개선 사항은 스냅샷이 진행 중인 동안 일시적인 오류가 지나가도록 허용하여 전반적인 스냅샷 성공률을 향상시킵니다.
- **진단 기능 개선**: 스냅샷 중에 선택적으로 생성되는 세 가지 새로운 진단 파일을 통해 스냅샷 작업 문제 해결이 더 쉬워졌습니다. 이 파일은 PowerShell 명령 문제, 정보가 누락된 사서함, 사서함과 연결할 수 없는 장치를 식별하는 데 도움이 됩니다. 관리자는 이 파일을 사용하여 Exchange에서 올바르지 않을 수 있는 데이터를 식별할 수 있습니다.
- **메모리 사용량 개선**: XenMobile Mail Manager는 이제 메모리 사용에서 더 효율적입니다. 관리자는 XenMobile Mail Manager가 시스템에 깨끗한 상태를 제공하도록 자동으로 다시 시작하도록 예약할 수 있습니다.
- **Microsoft .NET Framework 4.6 필수 구성 요소**: Microsoft .NET Framework의 필수 구성 요소는 이제 버전 4.6입니다.

해결된 문제

- 자격 증명 프롬프트 오류: Office 365 세션 불안정으로 인해 이 오류가 자주 발생했습니다. Exchange 연결 개선 기능이 이 문제를 해결합니다. (XMHELP-293, XMHELP-311, XMHELP-801)
- 사서함 및 장치 수 부정확성: XenMobile Mail Manager는 개선된 사서함-장치 연결 알고리즘을 가지고 있습니다. 개선된 진단 기능은 XenMobile Mail Manager가 책임 범위 내에 있지 않다고 판단하는 사서함 및 장치를 식별하는 데 도움이 됩니다. (XMHELP-623)
- 허용/차단/초기화 명령이 인식되지 않음: XenMobile Mail Manager 허용/차단/초기화 명령이 때때로 인식되지 않는 버그가 수정되었습니다. (XMHELP-489)
- 메모리 관리: 더 나은 메모리 관리 및 완화. (XMHELP-419)

아키텍처

다음 그림은 Exchange ActiveSync용 Endpoint Management 커넥터의 주요 구성 요소를 보여줍니다. 자세한 참조 아키텍처 다이어그램은 아키텍처를 참조하십시오.



세 가지 주요 구성 요소는 다음과 같습니다.

- **Exchange ActiveSync 액세스 제어 관리:** XenMobile과 통신하여 XenMobile에서 Exchange ActiveSync 정책을 검색하고, 이 정책을 로컬로 정의된 정책과 병합하여 Exchange에 대한 액세스를 허용하거나 거부해야 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:** Exchange ActiveSync 액세스 제어 관리에서 컴파일한 정책을 실행하기 위해 원격 PowerShell 명령을 예약하고 호출하는 역할을 합니다. 주기적으로 Exchange ActiveSync 데이터베이스의 스냅샷을 생성하여 새로 추가되거나 변경된 Exchange ActiveSync 장치를 감지합니다.
- **모바일 서비스 공급자:** XenMobile이 Exchange ActiveSync를 쿼리하고, Blackberry 장치를 쿼리하며, ActiveSync 및 Blackberry 장치에 대해 초기화와 같은 제어 작업을 발행할 수 있도록 웹 서비스 인터페이스를 제공합니다.

시스템 요구 사항 및 전제 조건

Exchange ActiveSync용 Endpoint Management 커넥터를 사용하려면 다음 최소 시스템 요구 사항이 필요합니다.

- 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 지원은 January 14, 2020에 종료되며, Windows Server 2012 R2 지원은 October 10, 2023에 종료됩니다.
- Microsoft SQL Server 2016 서비스 팩 2 또는 SQL Server 2014 서비스 팩 3.
- 마이크로소프트 .NET 프레임워크 4.6.
- Blackberry Enterprise Service, 버전 5 (선택 사항).

Microsoft Exchange Server의 최소 지원 버전:

- 마이크로소프트 오피스 365
- 익스체인지 서버 2016
- 익스체인지 서버 2013 (지원 종료 April 11, 2023)
- 익스체인지 서버 2010 서비스 팩 3 (지원 종료 January 14, 2020)

사전 요구 사항

- Windows Management Framework가 설치되어 있어야 합니다.
  - PowerShell V5, V4 및 V3
- PowerShell 실행 정책은 Set-ExecutionPolicy RemoteSigned를 통해 RemoteSigned로 설정되어야 합니다.
- Endpoint Management connector for Exchange ActiveSync를 실행하는 컴퓨터와 원격 Exchange Server 간에 TCP 포트 80이 열려 있어야 합니다.
- **장치 이메일 클라이언트**: 모든 이메일 클라이언트가 장치에 대해 동일한 ActiveSync ID를 일관되게 반환하는 것은 아닙니다. Endpoint Management connector for Exchange ActiveSync는 각 장치에 대해 고유한 ActiveSync ID를 예상하므로, 각 장치에 대해 동일한 고유 ActiveSync ID를 일관되게 생성하는 이메일 클라이언트만 지원됩니다. 다음 이메일 클라이언트는 Citrix에서 테스트되었으며 오류 없이 작동했습니다.
  - Samsung 기본 이메일 클라이언트
  - iOS 기본 이메일 클라이언트
- **Exchange**: Exchange를 실행하는 온프레미스 컴퓨터에 대한 요구 사항은 다음과 같습니다.

  Exchange Configuration UI에 지정된 자격 증명은 Exchange Server에 연결할 수 있어야 하며, 다음 Exchange 관련 PowerShell cmdlet을 실행할 수 있는 모든 권한이 부여되어야 합니다.
  - **Exchange Server 2010 SP2의 경우:**

    - CAS 사서함 가져오기
    - CAS 사서함 설정
    - Get-Mailbox
    - Get-ActiveSyncDevice
    - Get-ActiveSyncDeviceStatistics
    - Clear-ActiveSyncDevice
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment
- **Exchange 서버 2013 및 Exchange 서버 2016의 경우:**
    - Get-CASMailbox
    - Set-CASMailbox
    - 겟-메일박스
    - Get-MobileDevice
    - Get-MobileDeviceStatistics
    - 클리어-모바일디바이스
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment
- Endpoint Management connector for Exchange ActiveSync가 전체 포리스트를 볼 수 있도록 구성된 경우 다음을 실행할 권한이 부여되어야 합니다: **Set-AdServerSettings -ViewEntireForest $true**
- 제공된 자격 증명에는 원격 셸을 통해 Exchange Server에 연결할 권한이 부여되어야 합니다. 기본적으로 Exchange를 설치한 사용자에게 이 권한이 있습니다.
- 원격 연결을 설정하고 원격 명령을 실행하려면 자격 증명이 원격 시스템의 관리자인 사용자와 일치해야 합니다. Set-PSSessionConfiguration을 사용하여 관리 요구 사항을 제거할 수 있지만, 해당 명령에 대한 설명은 이 문서의 범위를 벗어납니다. 자세한 내용은 Microsoft 문서 세션 구성 정보를 참조하십시오.
- Exchange Server는 HTTP를 통한 원격 PowerShell 요청을 지원하도록 구성되어야 합니다. 일반적으로 Exchange Server에서 다음 PowerShell 명령을 실행하는 관리자만 있으면 됩니다: WinRM QuickConfig.

- Exchange에는 여러 스로틀링 정책이 있습니다. 정책 중 하나는 사용자당 허용되는 동시 PowerShell 연결 수를 제어합니다. Exchange 2010에서 사용자에게 허용되는 기본 동시 연결 수는 18개입니다. 연결 제한에 도달하면 Endpoint Management connector for Exchange ActiveSync는 Exchange Server에 연결할 수 없습니다. PowerShell을 통해 허용되는 최대 동시 연결 수를 변경하는 방법이 있지만, 이는 이 문서의 범위를 벗어납니다. 관심이 있다면 PowerShell을 사용한 원격 관리와 관련된 Exchange 스로틀링 정책을 살펴보십시오.

Office 365 Exchange 요구 사항

- **권한:** Exchange 구성 UI에 지정된 자격 증명은 Office 365에 연결할 수 있어야 하며 다음 Exchange 관련 PowerShell cmdlet을 실행할 수 있는 모든 권한이 부여되어야 합니다.
  - Get-CASMailbox
  - Set-CAS메일박스
  - Get-메일박스
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - 클리어-모바일디바이스
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **권한:** 제공된 자격 증명에는 원격 셸을 통해 Office 365 서버에 연결할 수 있는 권한이 부여되어야 합니다. 기본적으로 Office 365 온라인 관리자는 필요한 권한을 가지고 있습니다.
- **스로틀링 정책:** Exchange에는 많은 스로틀링 정책이 있습니다. 정책 중 하나는 사용자당 허용되는 동시 PowerShell 연결 수를 제어합니다. Office 365에서 사용자에게 허용되는 기본 동시 연결 수는 3개입니다. 연결 제한에 도달하면 Exchange ActiveSync용 Endpoint Management 커넥터는 Exchange Server에 연결할 수 없습니다. PowerShell을 통해 허용되는 최대 동시 연결 수를 변경하는 방법이 있지만, 이는 이 설명서의 범위를 벗어납니다. 관심이 있다면 PowerShell을 사용한 원격 관리와 관련된 Exchange 스로틀링 정책을 조사하십시오.

설치 및 구성

1. XmmSetup.msi 파일을 클릭한 다음 설치 프로그램의 지시에 따라 Exchange ActiveSync용 Endpoint Management 커넥터를 설치합니다.
2. 설치 마법사의 마지막 화면에서 **구성 유틸리티 시작**을 선택된 상태로 둡니다. 또는 **시작** 메뉴에서 Exchange ActiveSync용 Endpoint Management 커넥터를 엽니다.

3. 다음 데이터베이스 속성을 구성합니다.

   - **구성 > 데이터베이스** 탭을 선택합니다.
   - SQL Server 이름을 입력합니다(기본값은 localhost입니다).
   - 데이터베이스를 기본값인 **CitrixXmm**으로 유지합니다.

4. SQL에 사용되는 다음 인증 모드 중 하나를 선택합니다.

   - **SQL:** 유효한 SQL 사용자의 사용자 이름과 암호를 입력합니다.
   - **Windows 통합:** 이 옵션을 선택하는 경우, Endpoint Management connector for Exchange ActiveSync Service의 로그온 자격 증명을 SQL Server에 액세스할 권한이 있는 Windows 계정으로 변경해야 합니다. 이렇게 하려면 **제어판 > 관리 도구 > 서비스**를 열고 Endpoint Management connector for Exchange ActiveSync Service 항목을 마우스 오른쪽 버튼으로 클릭한 다음 **로그온** 탭을 클릭합니다.

   BlackBerry 데이터베이스 연결에도 Windows 통합이 선택된 경우, 여기에 지정된 Windows 계정에도 BlackBerry 데이터베이스에 대한 액세스 권한이 부여되어야 합니다.

5. SQL Server에 연결할 수 있는지 확인하려면 **연결 테스트**를 클릭한 다음 **저장**을 클릭합니다.
6. 서비스를 다시 시작하라는 메시지가 나타납니다. **예**를 클릭합니다.

   Endpoint Management connector for Exchange ActiveSync 설정 화면 이미지(/en-us/xenmobile/server/media/xmm-install-2.png)

7. 하나 이상의 Exchange Server 구성:

   - 단일 Exchange 환경을 관리하는 경우, 단일 서버만 지정합니다. 여러 Exchange 환경을 관리하는 경우, 각 Exchange 환경에 대해 단일 Exchange Server를 지정합니다.
   - **구성 > Exchange** 탭을 클릭한 다음 **추가**를 클릭합니다.

   엔드포인트 관리용 Exchange ActiveSync 커넥터 화면 이미지(/en-us/xenmobile/server/media/connector_exchange.png)

8. Exchange Server 환경 유형을 선택합니다: **온프레미스** 또는 **Office 365**.

   - **온프레미스**를 선택하는 경우, 원격 PowerShell 명령에 사용할 Exchange Server의 이름을 입력합니다.
   - 요구 사항 섹션에 지정된 대로 Exchange Server에 적절한 권한을 가진 Windows ID의 **사용자 이름**을 입력한 다음 해당 사용자의 **암호**를 입력합니다.
   - 주요 스냅샷 실행 일정을 선택합니다. 주요 스냅샷은 모든 Exchange ActiveSync 파트너십을 감지합니다.

- 마이너 스냅샷 실행 일정을 선택합니다. 마이너 스냅샷은 새로 생성된 Exchange ActiveSync 파트너십을 감지합니다.
- 스냅샷 유형을 선택합니다. **Deep** 또는 **Shallow**. Shallow 스냅샷은 일반적으로 훨씬 빠르며 Exchange ActiveSync용 Endpoint Management 커넥터의 모든 Exchange ActiveSync 액세스 제어 기능을 수행하기에 충분합니다. Deep 스냅샷은 시간이 더 오래 걸릴 수 있으며 ActiveSync에 대해 모바일 서비스 공급자가 활성화된 경우에만 필요합니다. 이 옵션을 사용하면 XenMobile이 관리되지 않는 장치를 쿼리할 수 있습니다.
- 기본 액세스를 선택합니다. **허용(Allow)**, **차단(Block)** 또는 **변경 안 함(Unchanged)**. 이 설정은 명시적인 XenMobile 또는 로컬 규칙으로 식별된 장치 외의 모든 장치를 처리하는 방법을 제어합니다. **허용(Allow)**을 선택하면 해당 모든 장치에 대한 ActiveSync 액세스가 허용됩니다. **차단(Block)**을 선택하면 액세스가 거부됩니다. **변경 안 함(Unchanged)**을 선택하면 변경 사항이 적용되지 않습니다.
- ActiveSync 명령 모드를 선택합니다. **PowerShell** 또는 **시뮬레이션(Simulation)**.
- **PowerShell** 모드에서 Exchange ActiveSync용 Endpoint Management 커넥터는 원하는 액세스 제어를 실행하기 위해 PowerShell 명령을 발행합니다. 시뮬레이션 모드에서 Exchange ActiveSync용 Endpoint Management 커넥터는 PowerShell 명령을 발행하지 않고 의도된 명령과 의도된 결과를 데이터베이스에 기록합니다. 시뮬레이션 모드에서 사용자는 **모니터(Monitor)** 탭을 사용하여 PowerShell 모드가 활성화되었을 때 어떤 일이 발생했을지 확인할 수 있습니다.
- **연결 만료(Connection Expiration)**에서 연결 수명에 대한 시간과 분을 설정합니다. 연결이 지정된 기간에 도달하면 연결이 만료된 것으로 표시되어 다시는 사용되지 않습니다. 만료된 연결이 더 이상 사용되지 않으면 Exchange ActiveSync용 Endpoint Management 커넥터가 연결을 정상적으로 종료합니다. 연결이 다시 필요할 때 사용 가능한 연결이 없으면 새 연결이 초기화됩니다. 지정되지 않은 경우 기본값인 30분이 사용됩니다.
- **전체 포리스트 보기(View Entire Forest)**를 선택하여 Exchange 환경에서 전체 Active Directory 포리스트를 볼 수 있도록 Exchange ActiveSync용 Endpoint Management 커넥터를 구성합니다.
- 인증 프로토콜을 선택합니다. **Kerberos** 또는 **기본(Basic)**. Exchange ActiveSync용 Endpoint Management 커넥터는 온프레미스 배포를 위한 기본 인증을 지원합니다. 이를 통해 Exchange ActiveSync용 Endpoint Management 커넥터 서버가 Exchange 서버가 있는 도메인의 구성원이 아닌 경우에도 Exchange ActiveSync용 Endpoint Management 커넥터를 사용할 수 있습니다.
- **연결 테스트(Test Connectivity)**를 클릭하여 Exchange Server에 연결할 수 있는지 확인한 다음 **저장(Save)**을 클릭합니다.
- 서비스를 다시 시작하라는 메시지가 나타납니다. **예(Yes)**를 클릭합니다.

9. 액세스 규칙을 구성합니다. **구성(Configure) > 액세스 규칙(Access Rules)** 탭을 선택하고 **XMS 규칙(XMS Rules)** 탭을 클릭한 다음 **추가(Add)**를 클릭합니다.

   Exchange ActiveSync 규칙용 엔드포인트 관리 커넥터 이미지(/en-us/xenmobile/server/media/connector-access-rules.png)

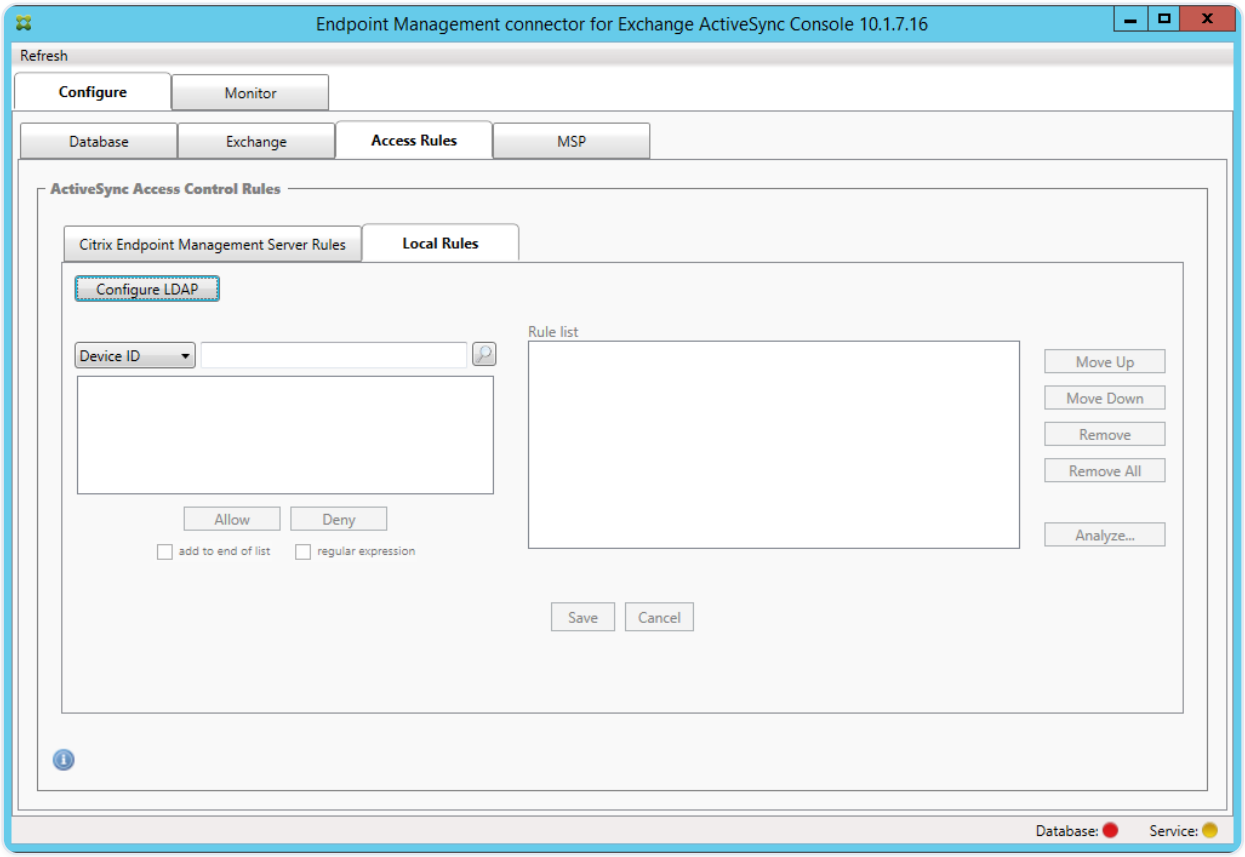
10. **XenMobile server Service Properties** 페이지에서 URL 문자열을 수정하여 XenMobile Server를 가리키도록 합니다. 예를 들어 인스턴스 이름이 **zdm**인 경우 `https://<XdmHostName>/zdm/services/MagConfigService`을 입력합니다. 이 예에서 **XdmHostName**을 XenMobile Server의 IP 또는 DNS 주소로 바꿉니다.

    Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/xmm-install-7.png)

    - 서버의 권한 있는 사용자를 입력합니다.
    - 사용자의 암호를 입력합니다.
    - **기준 간격**, **델타 간격**, **시간 초과** 값에 대한 기본값을 유지합니다.
    - 서버 연결을 확인하려면 **연결 테스트**를 클릭한 다음 **확인**을 클릭합니다.

    사용 안 함 확인란이 선택된 경우 XenMobile Mail Service는 XenMobile에서 정책을 수집하지 않습니다.

11. **로컬 규칙** 탭을 클릭합니다.

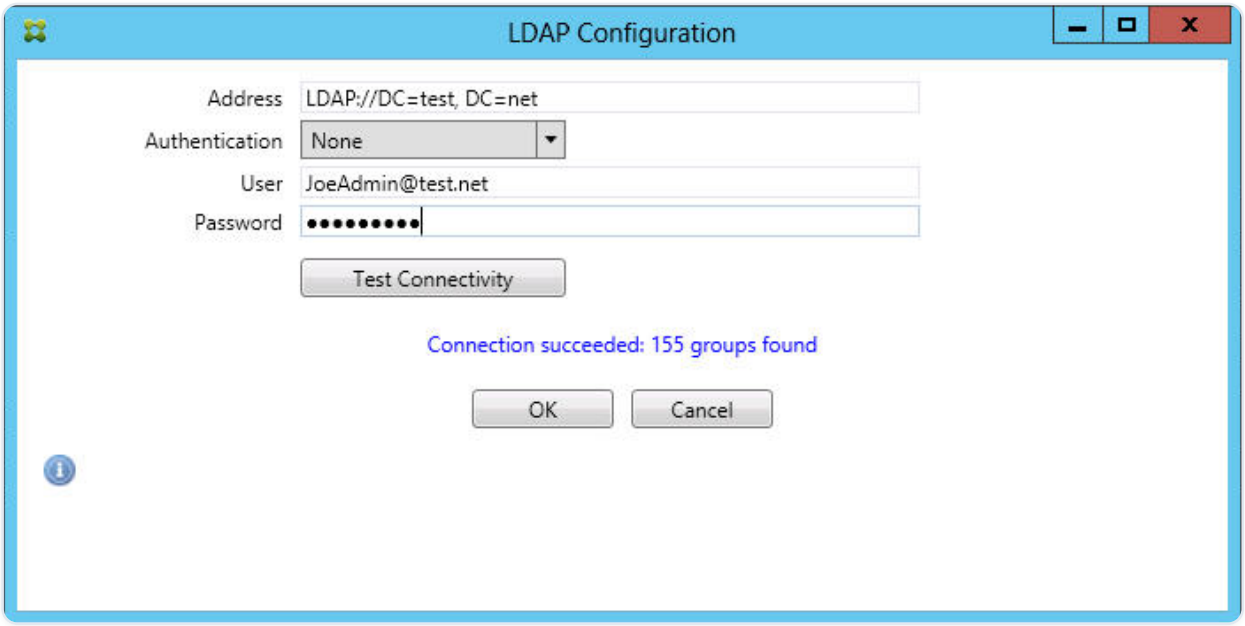


- ActiveSync 장치 ID, 장치 유형, AD 그룹, 사용자 또는 장치 UserAgent를 기반으로 로컬 규칙을 추가할 수 있습니다. 목록에서 적절한 유형을 선택합니다.
- 텍스트 상자에 텍스트 또는 텍스트 조각을 입력합니다. 필요에 따라 쿼리 버튼을 클릭하여 조각과 일치하는 엔터티를 볼 수 있습니다.

그룹을 제외한 모든 유형의 경우 시스템은 스냅샷에서 발견된 장치에 의존합니다. 따라서 이제 막 시작하여 스냅샷을 완료하지 않은 경우 사용할 수 있는 엔터티가 없습니다.

- 텍스트 값을 선택한 다음 **허용** 또는 **거부**를 클릭하여 오른쪽에 있는 **규칙 목록** 창에 추가합니다. **규칙 목록** 창 오른쪽에 있는 버튼을 사용하여 규칙 순서를 변경하거나 제거할 수 있습니다. 순서는 중요합니다. 특정 사용자 및 장치에 대해 규칙은 표시된 순서대로 평가되며, 상위 규칙(맨 위와 가까운)이 일치하면 후속 규칙은 영향을 미치지 않습니다. 예를 들어, 모든 iPad 장치를 허용하는 규칙이 있고 그 다음으로 사용자 Matt를 차단하는 규칙이 있는 경우, iPad 규칙이 Matt 규칙보다 더 높은 유효 우선순위를 가지므로 Matt의 iPad는 여전히 허용됩니다.
- 규칙 목록 내에서 규칙을 분석하여 잠재적인 재정의, 충돌 또는 보충 구성을 찾으려면 **분석**을 클릭한 다음 **저장**을 클릭합니다.

12. Active Directory 그룹에서 작동하는 로컬 규칙을 구성하려면 **LDAP 구성**을 클릭한 다음 LDAP 연결 속성을 구성합니다.



13. 모바일 서비스 공급자를 구성합니다.

모바일 서비스 공급자는 선택 사항입니다. 이 설정은 XenMobile이 관리되지 않는 장치를 쿼리하기 위해 모바일 서비스 공급자 인터페이스를 사용하도록 구성된 경우에만 필요합니다.

- **구성 > MSP** 탭을 클릭합니다.

Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector_msp.png)

- Mobile Service Provider 서비스의 서비스 전송 유형을 **HTTP** 또는 **HTTPS**로 설정합니다.
- Mobile Service Provider 서비스의 **서비스 포트**(일반적으로 80 또는 443)를 설정합니다. 포트 443을 사용하는 경우 해당 포트에는 IIS에 바인딩된 SSL 인증서가 필요합니다.
- **권한 부여 그룹** 또는 **사용자**를 설정합니다. 이 설정은 XenMobile에서 Mobile Service Provider 서비스에 연결할 수 있는 사용자 또는 사용자 집합을 지정합니다.
- ActiveSync 쿼리 사용 여부를 설정합니다. XenMobile Server에 대해 ActiveSync 쿼리가 활성화된 경우 하나 이상의 Exchange Server에 대한 스냅샷 유형을 **심층**으로 설정해야 합니다. 이 설정은 스냅샷을 찍는 데 상당한 성능 비용이 발생할 수 있습니다.
- 기본적으로 정규식 WorxMail.*와 일치하는 ActiveSync 장치는 XenMobile로 전송되지 않습니다. 이 동작을 변경하려면 필요에 따라 **ActiveSync 필터링** 필드를 변경합니다. 비어 있으면 모든 장치가 XenMobile로 전달됩니다.
- **저장**을 클릭합니다.

14. 선택적으로 BlackBerry Enterprise Server(BES) 인스턴스를 하나 이상 구성합니다. **추가**를 클릭한 다음 BES SQL Server의 서버 이름을 입력합니다.

    Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/xmm-install-10.png)

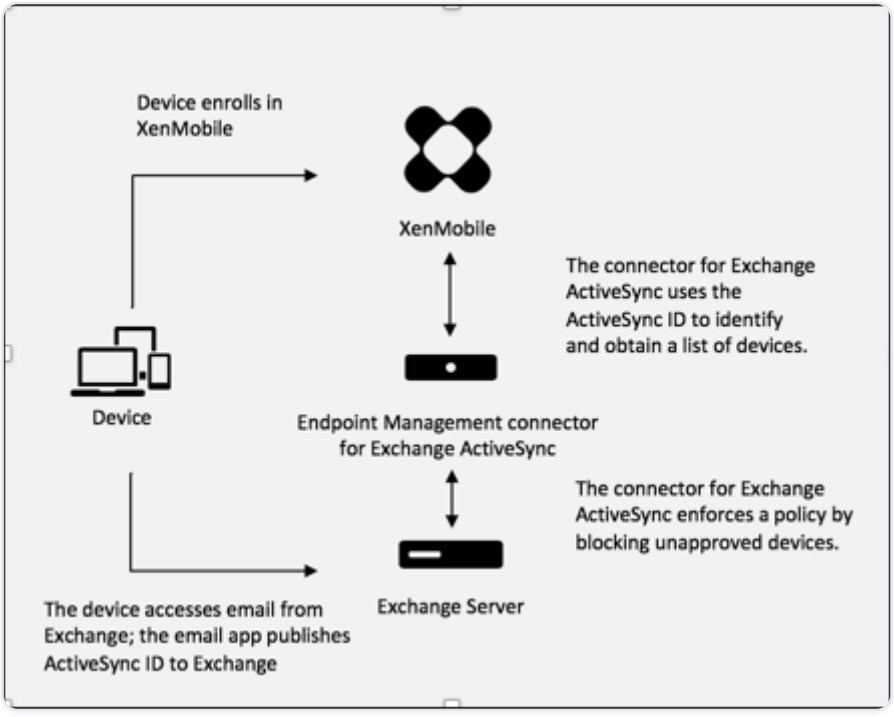
    - BES 관리 데이터베이스의 데이터베이스 이름을 입력합니다.
    - **인증** 모드를 선택합니다. Windows 통합 인증을 선택하는 경우 Endpoint Management connector for Exchange ActiveSync 서비스의 사용자 계정이 BES SQL Server에 연결하는 데 사용되는 계정입니다. Endpoint Management connector for Exchange ActiveSync 데이터베이스 연결에 Windows 통합을 선택하는 경우 여기에 지정된 Windows 계정에도 Endpoint Management connector for Exchange ActiveSync 데이터베이스에 대한 액세스 권한이 부여되어야 합니다.
    - **SQL 인증**을 선택하는 경우 사용자 이름과 암호를 입력합니다.
    - **동기화 일정**을 설정합니다. 이 일정은 BES SQL Server에 연결하여 장치 업데이트를 확인하는 데 사용됩니다.
    - **연결 테스트**를 클릭하여 SQL Server에 대한 연결을 확인합니다. Windows 통합을 선택하는 경우 이 테스트는 현재 로그인한 사용자를 사용하며 Endpoint Management connector for Exchange ActiveSync 서비스 사용자를 사용하지 않으므로 SQL 인증을 정확하게 테스트하지 않습니다.
    - XenMobile에서 BlackBerry 장치의 원격 Wipe 및 ResetPassword를 지원하려면 **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.
- BES에 대한 연결을 테스트하려면 **연결 테스트**를 클릭합니다.
- **저장**을 클릭합니다.

ActiveSync ID로 이메일 정책 적용

회사 이메일 정책에 따라 특정 장치는 회사 이메일 사용에 승인되지 않을 수 있습니다. 이 정책을 따르려면 직원이 해당 장치에서 회사 이메일에 액세스할 수 없도록 해야 합니다. Endpoint Management connector for Exchange ActiveSync와 XenMobile은 함께 작동하여 이러한 이메일 정책을 적용합니다. XenMobile은 회사 이메일 액세스에 대한 정책을 설정하고, 승인되지 않은 장치가 XenMobile에 등록되면 Endpoint Management connector for Exchange ActiveSync가 정책을 적용합니다.

장치의 이메일 클라이언트는 장치를 식별하는 데 사용되는 ActiveSync ID라고도 하는 장치 ID를 사용하여 Exchange Server(또는 Office 365)에 자신을 알립니다. Secure Hub는 유사한 식별자를 얻어 장치가 등록될 때 XenMobile로 보냅니다. 두 장치 ID를 비교하여 Endpoint Management connector for Exchange ActiveSync는 특정 장치가 회사 이메일 액세스 권한을 가져야 하는지 여부를 결정할 수 있습니다. 다음 그림은 이 개념을 보여줍니다.



XenMobile이 Endpoint Management connector for Exchange ActiveSync에 장치가 Exchange에 게시하는 ID와 다른 ActiveSync ID를 보내면 Endpoint Management connector for Exchange ActiveSync는 Exchange에 해당 장치에 대해 수행할 작업을 지시할 수 없습니다.

ActiveSync ID 일치는 대부분의 플랫폼에서 안정적으로 작동합니다. 그러나 Citrix는 일부 Android 구현에서 장치의 ActiveSync ID가 메일 클라이언트가 Exchange에 알리는 ID와 다르다는 것을 발견했습니다. 이 문제를 완화하려면 다음을 수행할 수 있습니다.

- Samsung SAFE 플랫폼에서 XenMobile에서 장치 ActiveSync 구성을 푸시합니다.

회사 이메일 액세스 정책이 제대로 적용되도록 보장하려면 방어적인 보안 태세를 취하고 Endpoint Management connector for Exchange ActiveSync를 구성하여 정적 정책을 기본적으로 거부(Deny)로 설정하여 이메일을 차단할 수 있습니다. 이는 직원이 Android 장치에서 이메일 클라이언트를 구성하고 ActiveSync ID 감지가 제대로 작동하지 않는 경우 직원이 회사 이메일 액세스를 거부당한다는 것을 의미합니다.

액세스 제어 규칙

Exchange ActiveSync용 Endpoint Management 커넥터는 Exchange ActiveSync 장치에 대한 액세스 제어를 동적으로 구성하기 위한 규칙 기반 접근 방식을 제공합니다. Exchange ActiveSync용 Endpoint Management 커넥터 액세스 제어 규칙은 일치 표현식과 원하는 액세스 상태(허용 또는 차단)의 두 부분으로 구성됩니다. 규칙은 특정 Exchange ActiveSync 장치에 적용되는지 또는 장치와 일치하는지 확인하기 위해 평가될 수 있습니다. 여러 종류의 일치 표현식이 있습니다. 예를 들어, 규칙은 특정 장치 유형의 모든 장치, 특정 Exchange ActiveSync 장치 ID 또는 특정 사용자의 모든 장치 등과 일치할 수 있습니다.

규칙 목록에서 규칙을 추가, 제거 및 재정렬하는 동안 언제든지 **취소** 버튼을 클릭하면 규칙 목록이 처음 열렸을 때의 상태로 되돌아갑니다. **저장**을 클릭하지 않으면 구성 도구를 닫을 경우 이 창에서 변경한 모든 내용이 손실됩니다.

Exchange ActiveSync용 Endpoint Management 커넥터에는 로컬 규칙, XenMobile Server 규칙(XDM 규칙이라고도 함) 및 기본 액세스 규칙의 세 가지 유형의 규칙이 있습니다.

로컬 규칙: 로컬 규칙은 가장 높은 우선순위를 가집니다. 장치가 로컬 규칙과 일치하면 규칙 평가가 중지됩니다. XenMobile Server 규칙이나 기본 액세스 규칙은 참조되지 않습니다. 로컬 규칙은 **구성 > 액세스 규칙 > 로컬 규칙** 탭을 통해 Exchange ActiveSync용 Endpoint Management 커넥터에 로컬로 구성됩니다. 일치 지원은 지정된 Active Directory 그룹 내 사용자 멤버십을 기반으로 합니다. 일치 지원은 다음 필드에 대한 정규식을 기반으로 합니다.

- 액티브 싱크 장치 ID
- ActiveSync 장치 유형
- 사용자 계정 이름(UPN)
- ActiveSync 사용자 에이전트(일반적으로 장치 플랫폼 또는 이메일 클라이언트)

주요 스냅샷이 완료되어 장치를 찾은 경우 일반 규칙 또는 정규식 규칙을 추가할 수 있습니다. 주요 스냅샷이 완료되지 않은 경우 정규식 규칙만 추가할 수 있습니다.

XenMobile 서버 규칙: XenMobile Server 규칙은 관리되는 장치에 대한 규칙을 제공하는 외부 XenMobile Server에 대한 참조입니다. XenMobile Server는 장치가 탈옥되었는지 또는 금지된 앱을 포함하는지 등 XenMobile에 알려진 속성을 기반으로 허용되거나 차단될 장치를 식별하는 자체 상위 수준 규칙으로 구성될 수 있습니다. XenMobile은 상위 수준 규칙을 평가하고 허용되거나 차단된 ActiveSync 장치 ID 세트를 생성하며, 이는 Exchange ActiveSync용 Endpoint Management 커넥터로 전달됩니다.

기본 액세스 규칙: 기본 액세스 규칙은 모든 장치와 일치할 수 있으며 항상 마지막으로 평가된다는 점에서 고유합니다. 이 규칙은 포괄적인 규칙으로, 특정 장치가 로컬 또는 XenMobile Server 규칙과 일치하지 않는 경우 장치의 원하는 액세스 상태는 기본 액세스 규칙의 원하는 액세스 상태에 따라 결정됩니다.

- **기본 액세스 – 허용:** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치는 허용됩니다.
- **기본 액세스 – 차단:** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치는 차단됩니다.
- **기본 액세스 - 변경 없음:** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치는 Exchange ActiveSync용 Endpoint Management 커넥터에 의해 액세스 상태가 어떤 식으로든 수정되지 않습니다. 장치가 Exchange에 의해 격리 모드에 배치된 경우 아무런 조치도 취해지지 않습니다. 예를 들어, 장치를 격리 모드에서 제거하는 유일한 방법은 명시적인 로컬 또는 XDM 규칙이 격리를 재정의하도록 하는 것입니다.

규칙 평가 정보

Exchange가 Endpoint Management connector for Exchange ActiveSync에 보고하는 각 장치에 대해 규칙은 다음과 같이 가장 높은 우선순위부터 가장 낮은 우선순위까지 순서대로 평가됩니다.

- 로컬 규칙
- XenMobile Server 규칙
- 기본 액세스 규칙

일치하는 항목이 발견되면 평가는 중지됩니다. 예를 들어, 로컬 규칙이 특정 장치와 일치하는 경우 해당 장치는 XenMobile Server 규칙이나 기본 액세스 규칙에 대해 평가되지 않습니다. 이는 특정 규칙 유형 내에서도 마찬가지입니다. 예를 들어, 로컬 규칙 목록에서 특정 장치에 대해 단일 일치 항목 이상이 있는 경우 첫 번째 일치 항목이 발견되면 평가는 중지됩니다.

Endpoint Management connector for Exchange ActiveSync는 장치 속성이 변경되거나, 장치가 추가 또는 제거되거나, 규칙 자체가 변경될 때 현재 정의된 규칙 집합을 다시 평가합니다. 주요 스냅샷은 구성 가능한 간격으로 장치 속성 변경 및 제거를 포착합니다. 보조 스냅샷은 구성 가능한 간격으로 새 장치를 포착합니다.

Exchange ActiveSync에도 액세스를 제어하는 규칙이 있습니다. Endpoint Management connector for Exchange ActiveSync의 컨텍스트에서 이러한 규칙이 어떻게 작동하는지 이해하는 것이 중요합니다. Exchange는 개인 예외, 장치 규칙 및 조직 설정의 세 가지 수준의 규칙으로 구성될 수 있습니다. Endpoint Management connector for Exchange ActiveSync는 원격 PowerShell 요청을 프로그래밍 방식으로 발행하여 개인 예외 목록에 영향을 줌으로써 액세스 제어를 자동화합니다. 이 목록은 특정 사서함과 연결된 허용되거나 차단된 Exchange ActiveSync 장치 ID 목록입니다. 배포되면 Endpoint Management connector for Exchange ActiveSync는 Exchange 내에서 예외 목록 기능 관리를 효과적으로 인계받습니다. 자세한 내용은 Microsoft 문서 장치 액세스 제어를 참조하십시오.

분석은 동일한 필드에 대해 여러 규칙이 정의된 상황에서 유용합니다. 규칙 간의 관계를 문제 해결할 수 있습니다. 규칙 필드의 관점에서 분석을 수행합니다. 예를 들어, ActiveSync 장치 ID, ActiveSync 장치 유형, 사용자, 사용자 에이전트와 같이 일치하는 필드를 기반으로 규칙이 그룹으로 분석됩니다.

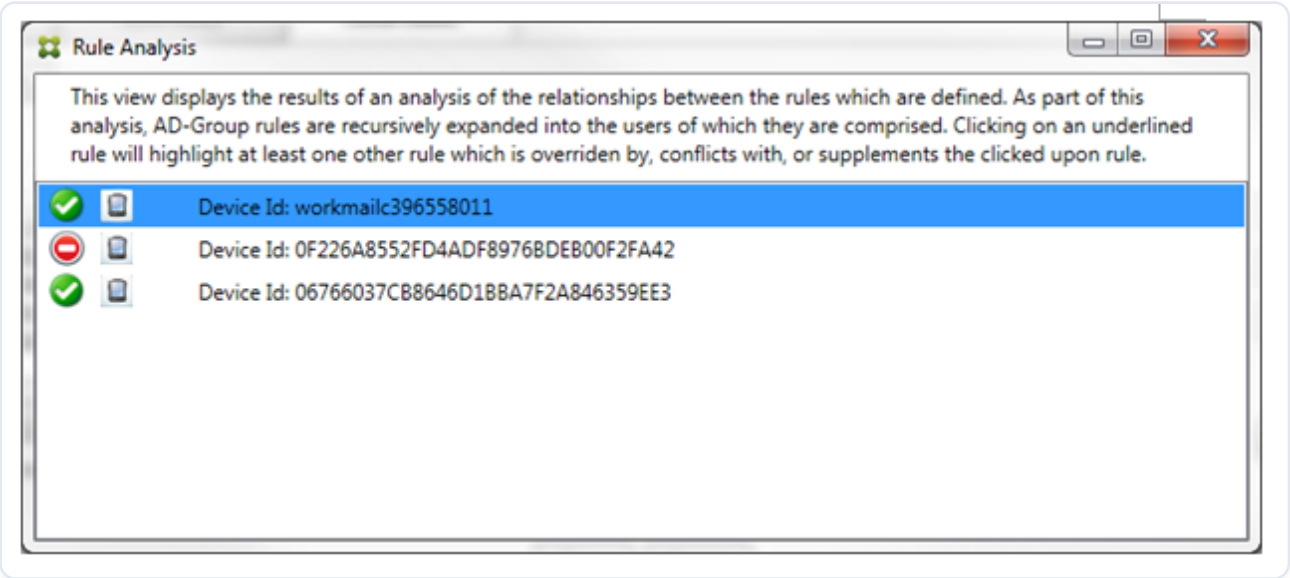
규칙 용어

- **재정의 규칙:** 재정의는 단일 규칙 이상이 동일한 장치에 적용될 수 있을 때 발생합니다. 규칙은 목록에서 우선순위에 따라 평가되므로, 나중에 적용될 수 있는 규칙 인스턴스는 평가되지 않을 수 있습니다.
- **충돌 규칙:** 충돌은 단일 규칙 이상이 동일한 장치에 적용될 수 있지만 액세스(허용/차단)가 일치하지 않을 때 발생합니다. 충돌하는 규칙이 정규식 규칙이 아닌 경우, 충돌은 항상 암묵적으로 재정의를 의미합니다 .
- **보충 규칙:** 보충은 둘 이상의 규칙이 정규식 규칙일 때 발생하며, 이 경우 두 개(또는 그 이상)의 정규식을 단일 정규식 규칙으로 결합하거나 기능이 중복되지 않도록 해야 할 필요가 있을 수 있습니다. 보충 규칙은 액세스(허용/차단)에서 충돌할 수도 있습니다.
- **기본 규칙:** 기본 규칙은 대화 상자 내에서 클릭된 규칙입니다. 이 규칙은 주위를 둘러싼 실선 테두리로 시각적으로 표시됩니다. 또한 위 또는 아래를 가리키는 하나 또는 두 개의 녹색 화살표가 있습니다. 화살표가 위를 가리키면 기본 규칙보다 선행하는 보조 규칙이 있음을 나타냅니다. 화살표가 아래를 가리키면 기본 규칙 다음에 오는 보조 규칙이 있음을 나타냅니다. 한 번에 하나의 기본 규칙만 활성화될 수 있습니다.
- **보조 규칙:** 보조 규칙은 재정의, 충돌 또는 보충 관계를 통해 기본 규칙과 어떤 식으로든 관련됩니다. 이 규칙은 주위를 둘러싼 점선 테두리로 시각적으로 표시됩니다. 각 기본 규칙에 대해 하나에서 여러 개의 보조 규칙이 있을 수 있습니다. 밑줄이 그어진 항목을 클릭하면 강조 표시된 보조 규칙은 항상 기본 규칙의 관점에서 나타납니다. 예를 들어, 보조 규칙은 기본 규칙에 의해 재정의되거나, 보조 규칙은 기본 규칙과의 액세스에서 충돌하거나, 보조 규칙은 기본 규칙을 보충합니다.

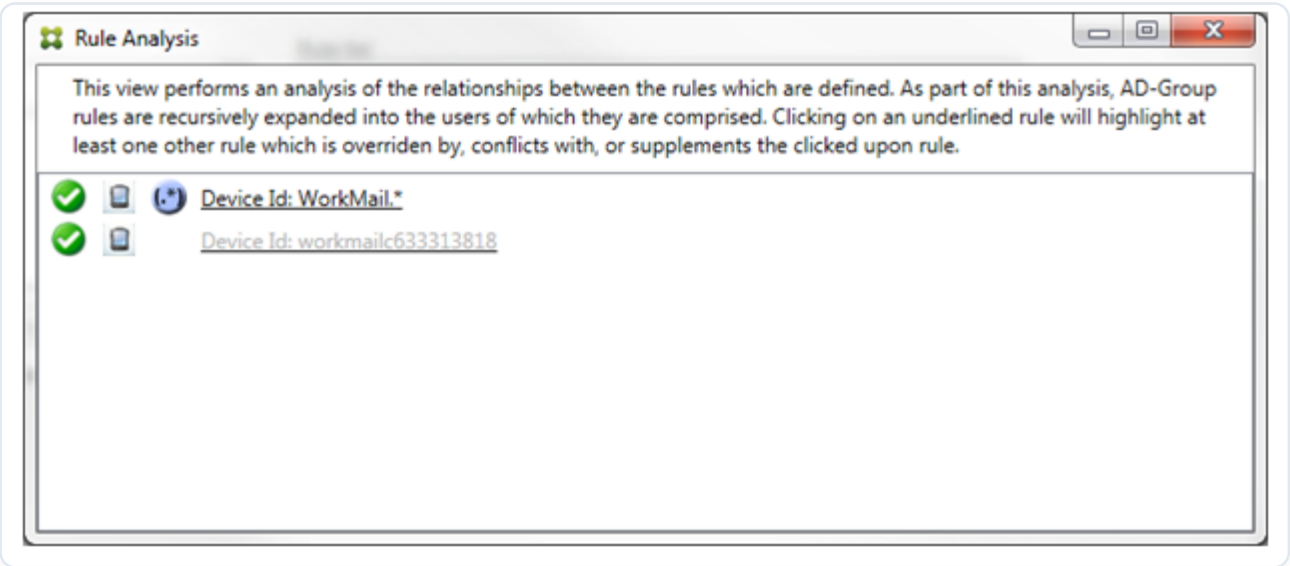
규칙 분석 대화 상자에 규칙 유형이 나타나는 방식

충돌, 재정의 또는 보완이 없는 경우 규칙 분석 대화 상자에는 밑줄이 그어진 항목이 없습니다. 항목을 클릭해도 아무런 영향이 없으며, 예를 들어 일반적인 선택된 항목 시각 효과가 나타납니다.

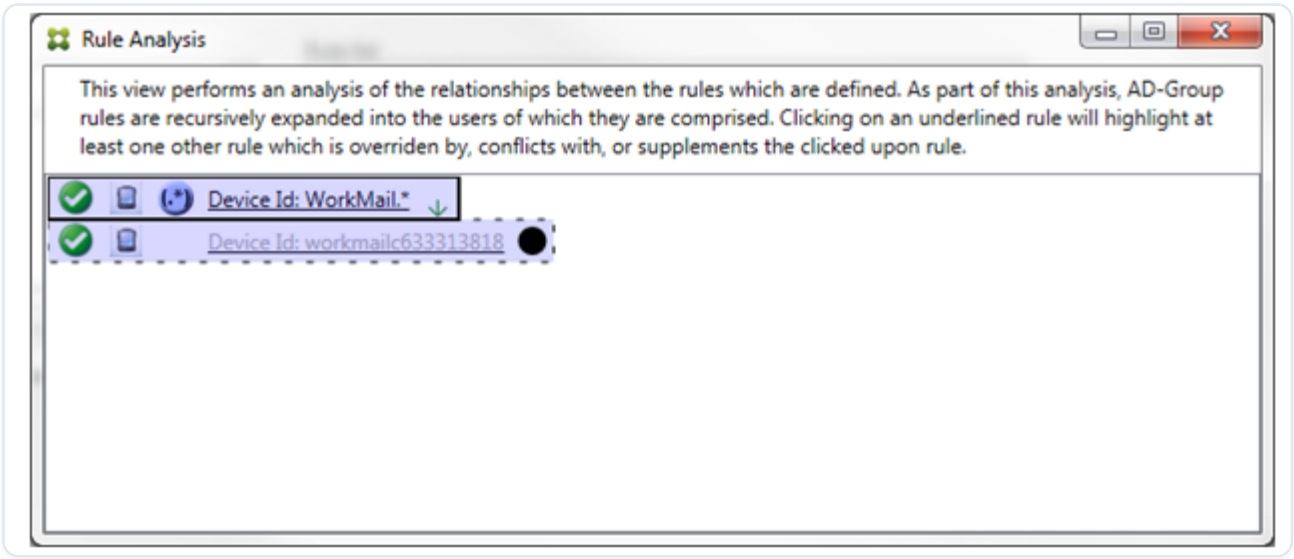
규칙 분석 창에는 확인란이 있으며, 이 확인란을 선택하면 충돌, 재정의, 중복 또는 보완인 규칙만 표시됩니다
.



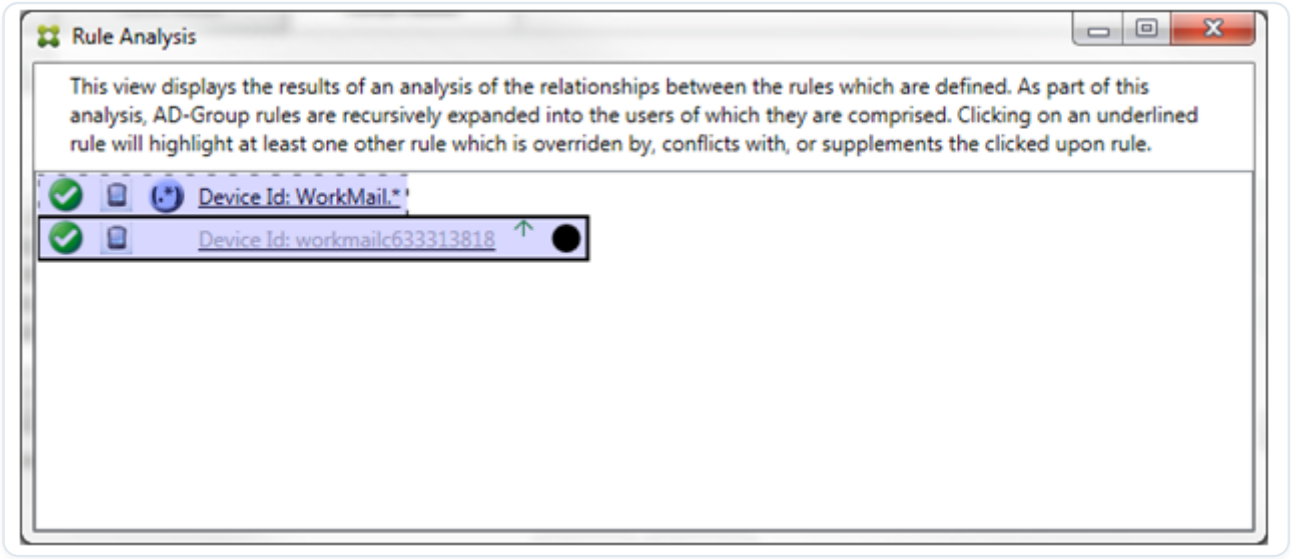
재정의가 발생하면 기본 규칙과 보조 규칙을 포함하여 최소 두 개의 규칙에 밑줄이 그어집니다. 최소 하나의 보조 규칙은 더 밝은 글꼴로 나타나 해당 규칙이 더 높은 우선순위 규칙에 의해 재정의되었음을 나타냅니다. 재정의된 규칙을 클릭하여 어떤 규칙이 해당 규칙을 재정의했는지 확인할 수 있습니다. 재정의된 규칙이 기본 규칙이거나 보조 규칙이기 때문에 강조 표시될 때마다 옆에 검은색 원이 나타나 해당 규칙이 비활성 상태임을 추가적으로 시각적으로 나타냅니다. 예를 들어, 규칙을 클릭하기 전에는 대화 상자가 다음과 같이 나타납니다
.



가장 높은 우선순위 규칙을 클릭하면 대화 상자가 다음과 같이 나타납니다.

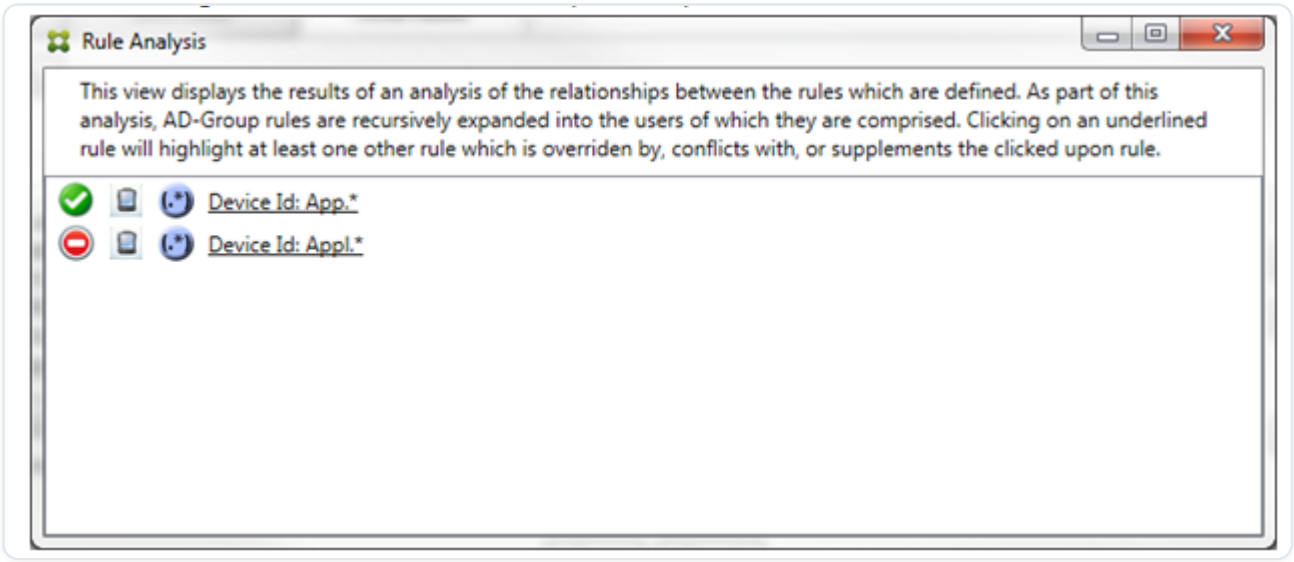


이 예에서 정규식 규칙 `WorkMail.*`은 기본 규칙(실선 테두리로 표시됨)이고 일반 규칙 `workmailc633313818`는 보조 규칙(점선 테두리로 표시됨)입니다. 보조 규칙 옆의 검은색 점은 그 앞에 오는 더 높은 우선순위 정규식 규칙 때문에 해당 규칙이 비활성 상태(절대 평가되지 않음)임을 추가적으로 나타내는 시각적 신호입니다. 재정의된 규칙을 클릭하면 대화 상자가 다음과 같이 나타납니다.

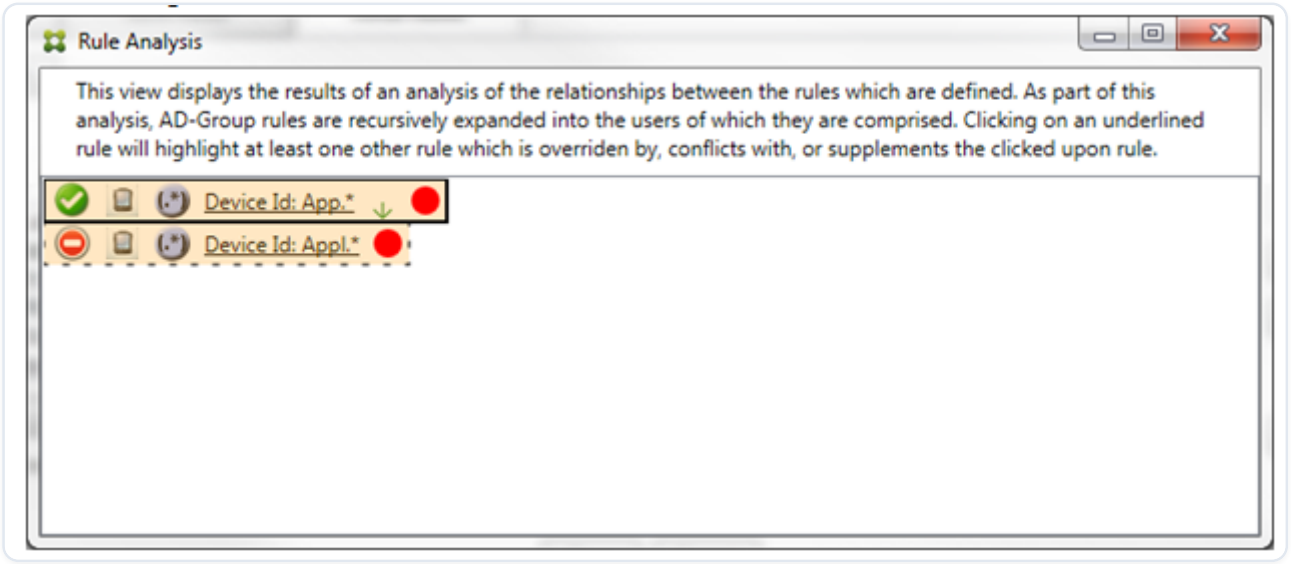


앞의 예에서 정규식 규칙 `WorkMail.*`은 보조 규칙(점선 테두리로 표시됨)이고 일반 규칙 `workmailc633313818`는 기본 규칙(실선 테두리로 표시됨)입니다. 이 간단한 예에서는 큰 차이가 없습니다. 더 복잡한 예는 이 항목의 뒷부분에 있는 복합 표현식 예제를 참조하십시오. 많은 규칙이 정의된 시나리오에서 재정의된 규칙을 클릭하면 어떤 규칙이 해당 규칙을 재정의했는지 빠르게 식별할 수 있습니다.

충돌이 발생하면 기본 규칙과 보조 규칙을 포함하여 최소 두 개의 규칙에 밑줄이 그어집니다. 충돌하는 규칙은 빨간색 점으로 표시됩니다. 서로만 충돌하는 규칙은 두 개 이상의 정규식 규칙이 정의된 경우에만 가능합니다. 다른 모든 충돌 시나리오에서는 충돌뿐만 아니라 재정의도 발생합니다. 간단한 예에서 두 규칙 중 하나를 클릭하기 전에는 대화 상자가 다음과 같이 나타납니다.

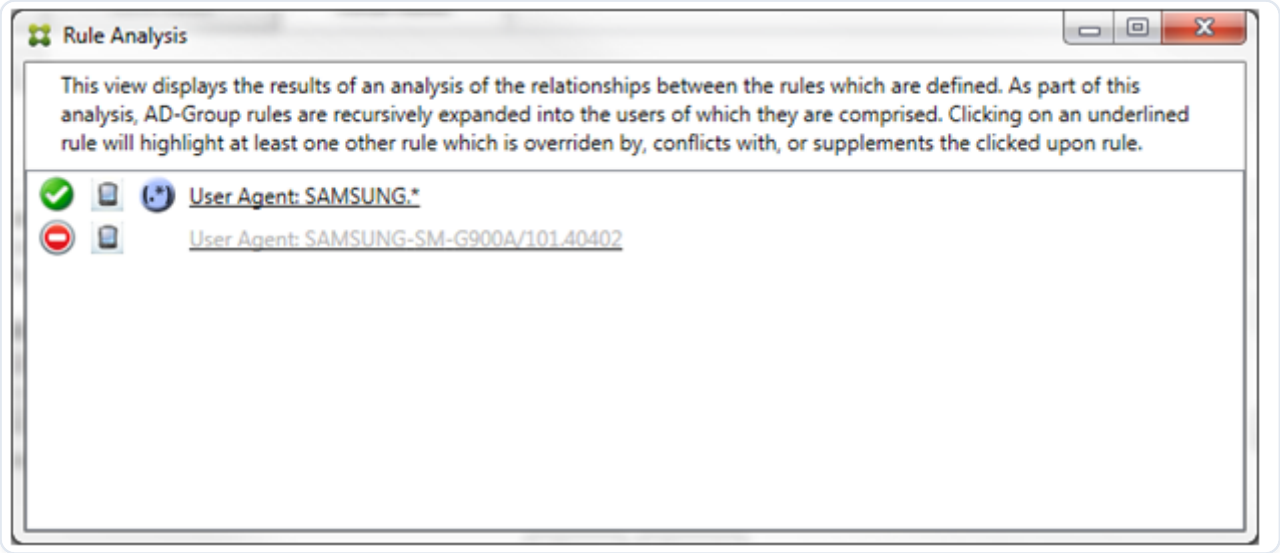


두 정규식 규칙을 검사하면 첫 번째 규칙이 "App"을 포함하는 장치 ID를 가진 모든 장치를 허용하고 두 번째 규칙이 "Appl"을 포함하는 장치 ID를 가진 모든 장치를 거부한다는 것이 분명합니다. 또한, 두 번째 규칙이 "Appl"을 포함하는 장치 ID를 가진 모든 장치를 거부하더라도, 허용 규칙의 더 높은 우선순위 때문에 해당 기준과 일치하는 장치는 결코 거부되지 않습니다. 첫 번째 규칙을 클릭하면 대화 상자가 다음과 같이 나타납니다 .



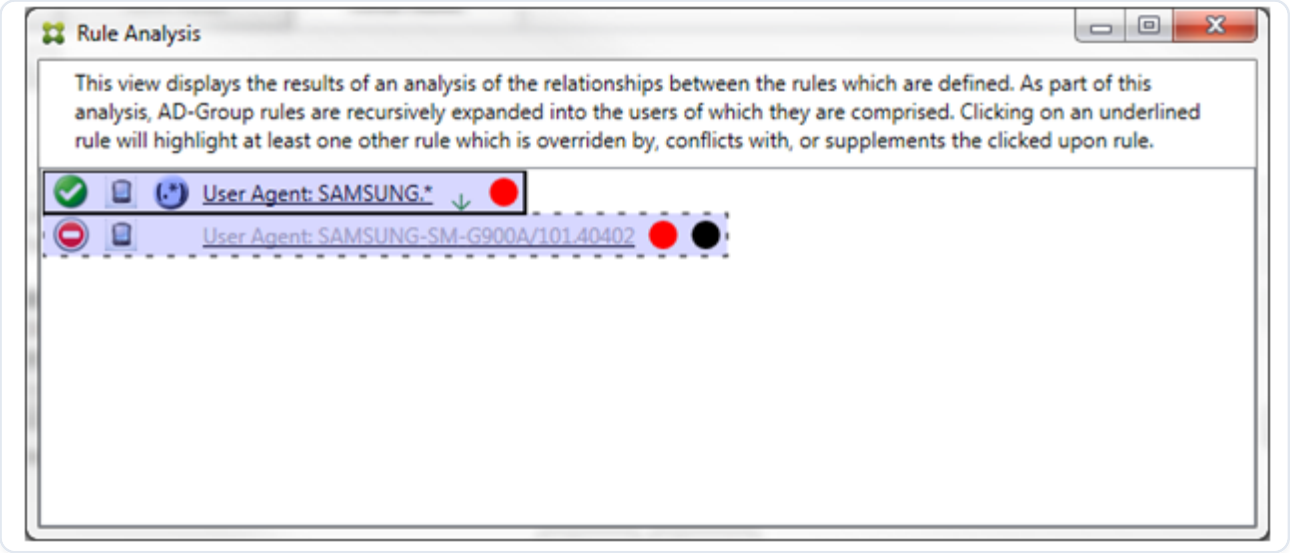
앞의 시나리오에서 기본 규칙(정규식 규칙 `App.*`)과 보조 규칙(정규식 규칙 `Appl.*`) 모두 노란색으로 강조 표시됩니다. 이는 단일 일치 가능 필드에 두 개 이상의 정규식 규칙을 적용했음을 알려주는 단순한 시각적 경고이며, 이는 중복 문제 또는 더 심각한 문제를 의미할 수 있습니다.

충돌과 재정의가 모두 있는 시나리오에서는 기본 규칙(정규식 규칙 `App.*`)과 보조 규칙(정규식 규칙 `Appl.*`)이 모두 노란색으로 강조 표시됩니다. 이는 단일 일치 가능 필드에 단일 정규식 규칙 이상을 적용했음을 알려주는 시각적 경고일 뿐이며, 이는 중복 문제 또는 더 심각한 문제를 의미할 수 있습니다.



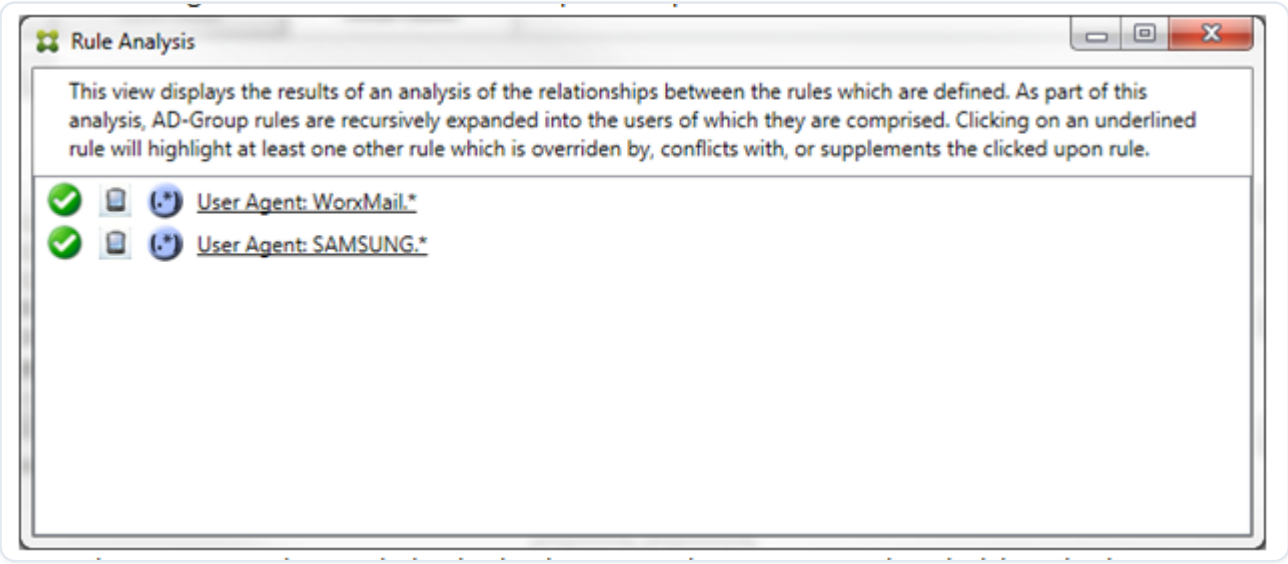
이전 예제에서 첫 번째 규칙(정규식 규칙 `SAMSUNG.*`)이 다음 규칙(일반 규칙 `SAMSUNG-SM-G900A/101.40402`)을 재정의할 뿐만 아니라 두 규칙의 액세스 권한이 다르다는 것(기본 규칙은 허용을 지정하고, 보조 규칙은 차단을 지정함)을 쉽게 알 수 있습니다. 두 번째 규칙(일반 규칙 `SAMSUNG-SM-G900A/101.40402`)은 재정의되어 비활성 상태임을 나타내기 위해 더 밝은 텍스트로 표시됩니다.

정규식 규칙을 클릭하면 대화 상자가 다음과 같이 나타납니다.

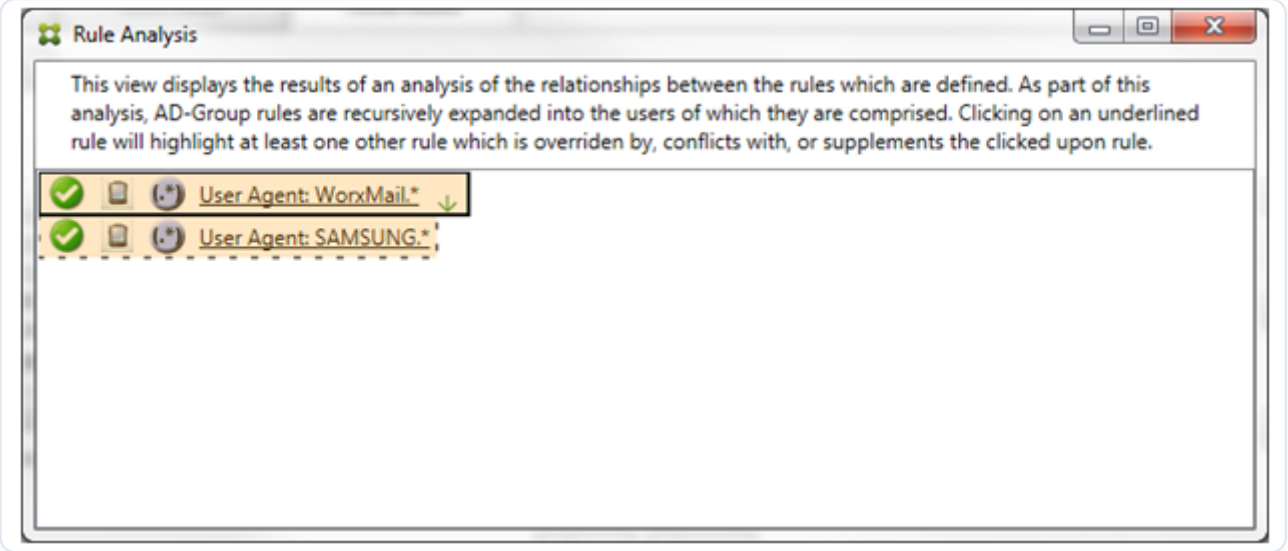


기본 규칙(정규식 규칙 `SAMSUNG.*`) 뒤에는 액세스 상태가 하나 이상의 보조 규칙과 충돌함을 나타내는 빨간색 점이 뒤따릅니다. 보조 규칙(일반 규칙 `SAMSUNG-SM-G900A/101.40402`) 뒤에는 액세스 상태가 기본 규칙과 충돌함을 나타내는 빨간색 점이 뒤따릅니다. 이 규칙 뒤에는 재정의되어 비활성 상태임을 나타내는 검은색 점도 뒤따릅니다.

최소 두 개의 규칙, 즉 기본 규칙과 보조 규칙(들)에 밑줄이 표시됩니다. 서로를 보완하는 규칙은 정규식 규칙만 포함합니다. 규칙이 서로를 보완할 때 노란색 오버레이로 표시됩니다. 간단한 예에서 두 규칙 중 하나를 클릭하기 전에 대화 상자는 다음과 같이 나타납니다.



육안 검사로 두 규칙 모두 Endpoint Management connector for Exchange ActiveSync의 ActiveSync 장치 ID 필드에 적용된 정규식 규칙임을 쉽게 알 수 있습니다. 첫 번째 규칙을 클릭하면 대화 상자가 다음과 같이 나타납니다.

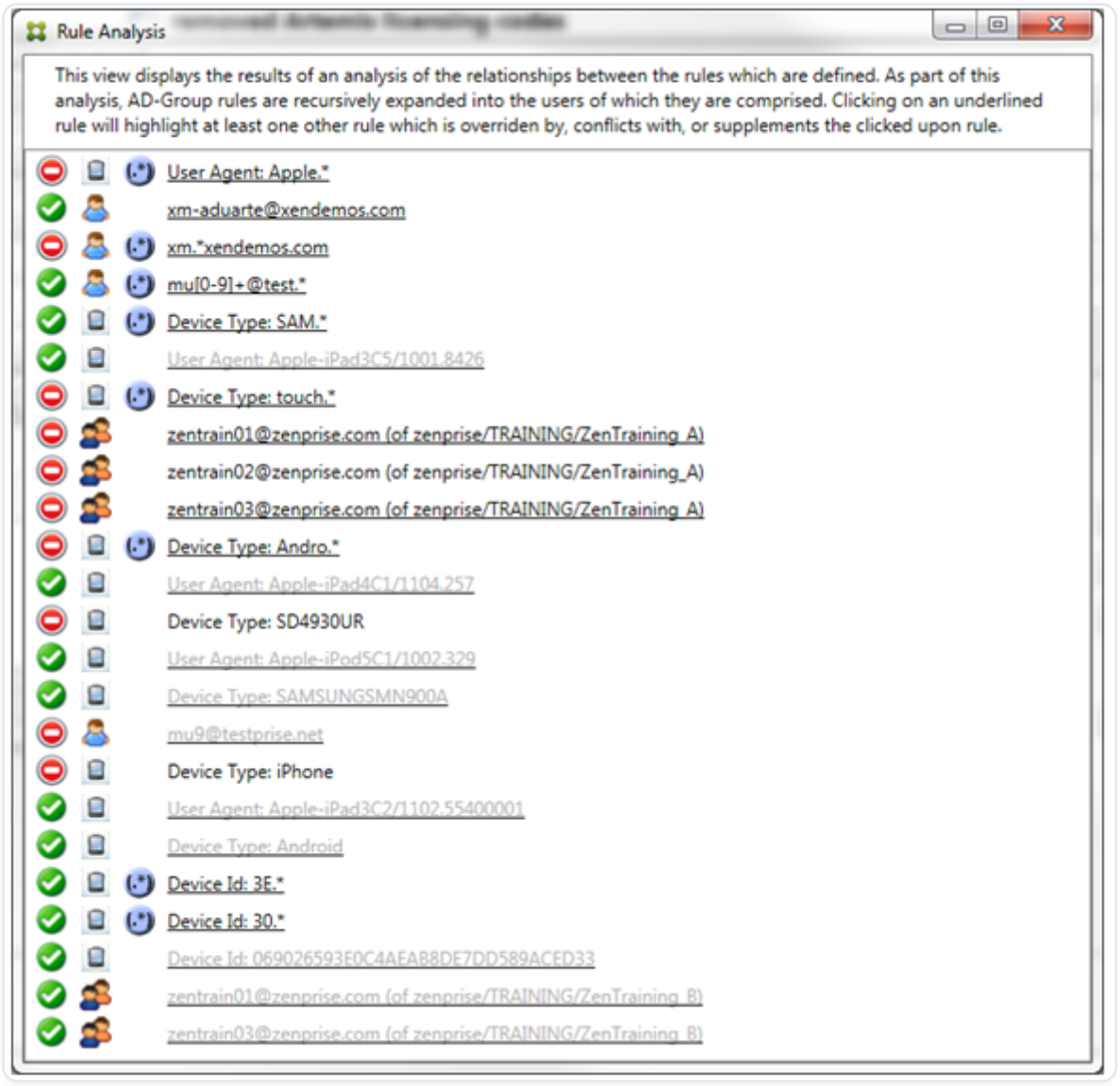


기본 규칙(정규식 규칙 `WorkMail.*`)은 정규식인 보조 규칙이 하나 이상 존재함을 나타내기 위해 노란색 오버레이로 강조 표시됩니다. 보조 규칙(정규식 규칙 `SAMSUNG.*`)은 자신과 기본 규칙 모두 Endpoint Management connector for Exchange ActiveSync 내의 동일한 필드에 적용되는 정규식 규칙임을 나타내기 위해 노란색 오버레이로 강조 표시됩니다. 이 경우 해당 필드는 ActiveSync 장치 ID입니다. 정규식이 겹칠 수도 있고 겹치지 않을 수도 있습니다. 정규식이 올바르게 작성되었는지 여부는 사용자에게 달려 있습니다.

복잡한 식의 예

많은 잠재적인 재정의, 충돌 또는 보완이 발생할 수 있으므로 모든 가능한 시나리오의 예를 제공하는 것은 불가능합니다. 다음 예제에서는 하지 말아야 할 사항을 설명하는 동시에 규칙 분석 시각적 구성의 모든 기능을 보여주는 역할도 합니다. 다음 그림에서 대부분의 항목에 밑줄이 표시됩니다. 많은 항목이 더 밝은 글꼴로 렌더링되는데, 이는 해당 규칙이 어떤 식으로든 더 높은 우선순위 규칙에 의해 재정의되었음을 나타냅니다. (/en-us/

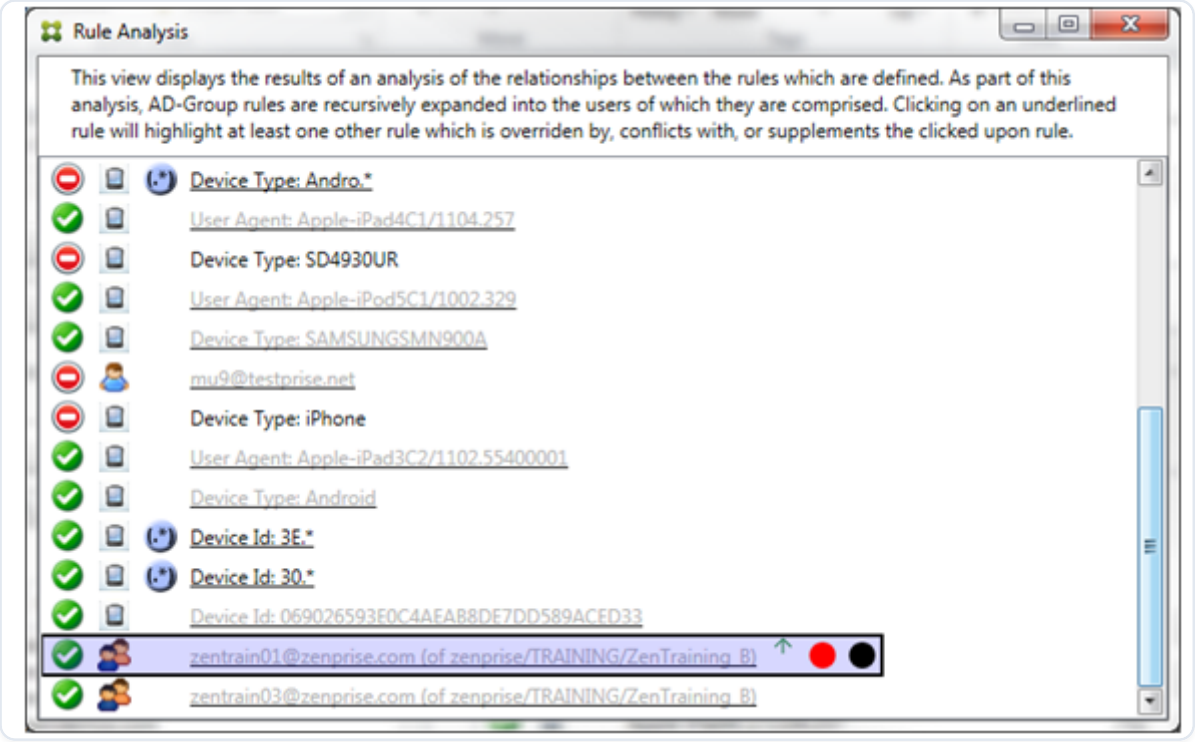
xenmobile/server/media/xenmobilemailmanager-regexpression-icon.png) 아이콘으로 표시된 다양한 정규식 규칙도 목록에 포함되어 있습니다.



재정의를 분석하는 방법

특정 규칙을 재정의한 규칙을 확인하려면 해당 규칙을 클릭합니다.

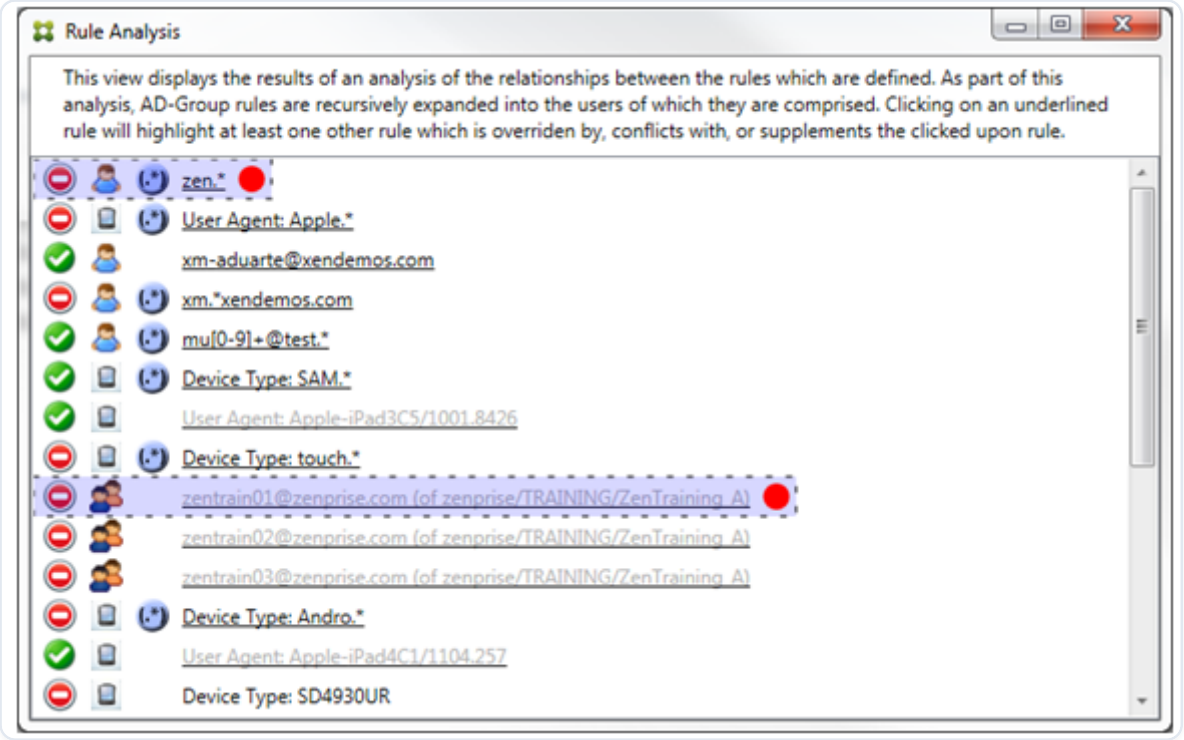
예시 1: 이 예시에서는 `zentrain01@zenprise.com`이(가) 재정의된 이유를 살펴봅니다.



기본 규칙(`zentrain01@zenprise.com`이(가) 구성원인 AD 그룹 규칙 `zenprise/TRAINING/ZenTraining B`)은 다음과 같은 특징을 가집니다.

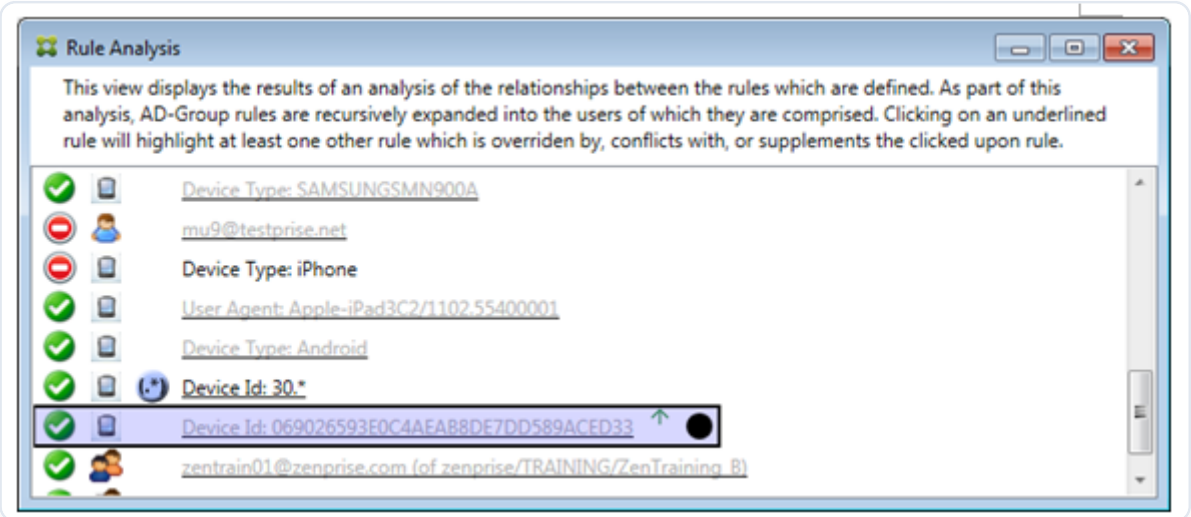
- 파란색으로 강조 표시되어 있으며 실선 테두리가 있습니다.
- 위쪽을 가리키는 녹색 화살표가 있습니다(보조 규칙이 모두 그 위에 있음을 나타냄).
- 빨간색 원과 검은색 원이 모두 뒤따르는데, 이는 각각 하나 이상의 보조 규칙이 해당 액세스와 충돌하고 기본 규칙이 재정의되어 비활성 상태임을 나타냅니다.

위로 스크롤하면 다음이 표시됩니다.



이 경우 기본 규칙을 재정의하는 두 가지 보조 규칙이 있습니다. 즉, 정규식 규칙 `zen.*`과 일반 규칙 `zentrain01@zenprise.com` (`zenprise/TRAINING/ZenTraining A`의)입니다. 후자의 보조 규칙의 경우, Active Directory 그룹 규칙 `ZenTraining A`에 사용자 `zentrain01@zenprise.com`가 포함되어 있고, Active Directory 그룹 규칙 `ZenTraining B`에도 사용자 `zentrain01@zenprise.com`이 포함되어 있습니다. 그러나 보조 규칙이 기본 규칙보다 우선순위가 높기 때문에 기본 규칙이 재정의되었습니다. 기본 규칙의 액세스는 허용(Allow)이며, 두 보조 규칙의 액세스는 모두 차단(Block)이므로, 모두 빨간색 원이 뒤따라 액세스 충돌을 추가로 나타냅니다.

예시 2: 이 예시에서는 ActiveSync 장치 ID가 `069026593E0C4AEAB8DE7DD589ACED33`인 장치가 재정의된 이유를 보여줍니다.



기본 규칙(일반 장치 ID 규칙 `069026593E0C4AEAB8DE7DD589ACED33`)은 다음과 같은 특징을 가집니다.

- 파란색으로 강조 표시되어 있으며 실선 테두리가 있습니다.

- 위쪽을 가리키는 녹색 화살표가 있습니다(보조 규칙이 그 위에 있음을 나타냄).
- 보조 규칙이 기본 규칙을 재정의하여 비활성 상태임을 나타내는 검은색 원이 뒤따릅니다.

Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules26.png)

이 경우 단일 보조 규칙이 기본 규칙을 재정의합니다. 정규식 ActiveSync 장치 ID 규칙은 `3E.*`입니다. 정규식 `3E.*`가 `069026593E0C4AEAB8DE7DD589ACED33`와 일치하므로 기본 규칙은 절대 평가되지 않습니다.

보충 및 충돌 분석 방법

이 경우 기본 규칙은 정규식 ActiveSync 장치 유형 규칙 `touch.*`입니다. 특징은 다음과 같습니다.

- 특정 규칙 필드(이 경우 ActiveSync 장치 유형)에 대해 단일 정규식 규칙 이상이 작동하고 있음을 경고하는 노란색 오버레이가 있는 실선 테두리로 표시됩니다.
- 각각 위아래를 가리키는 두 개의 화살표는 우선 순위가 더 높은 보조 규칙이 하나 이상 있고 우선 순위가 더 낮은 보조 규칙이 하나 이상 있음을 나타냅니다.
- 옆에 있는 빨간색 원은 하나 이상의 보조 규칙이 액세스를 허용으로 설정하여 기본 규칙의 액세스인 차단과 충돌함을 나타냅니다.
- 두 가지 보조 규칙이 있습니다. 정규식 ActiveSync 장치 유형 규칙 `SAM.*`과 정규식 ActiveSync 장치 유형 규칙 `Andro.*`입니다.
- 두 보조 규칙 모두 보조 규칙임을 나타내기 위해 대시로 테두리가 표시됩니다.
- 두 보조 규칙 모두 ActiveSync 장치 유형의 규칙 필드에도 적용됨을 나타내기 위해 노란색으로 오버레이됩니다.
- 이러한 시나리오에서는 정규식 규칙이 중복되지 않도록 해야 합니다.

  Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules27.png)

규칙을 추가로 분석하는 방법

이 예는 규칙 관계가 항상 기본 규칙의 관점에서 어떻게 작동하는지 보여줍니다. 이전 예에서는 `touch.*` 값을 가진 장치 유형의 규칙 필드에 적용된 정규식 규칙을 클릭하는 방법을 보여주었습니다. 보조 규칙 `Andro.*`를 클릭하면 다른 보조 규칙 세트가 강조 표시됩니다.

Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules28.png)

이 예시는 규칙 관계에 포함된 재정의된 규칙을 보여줍니다. 이 규칙은 일반 ActiveSync 장치 유형 규칙 `Android`이며, 재정의되었고(옅은 글꼴과 옆의 검은색 원으로 표시됨) 기본 규칙 정규식 ActiveSync 장치 유형 규칙 `Andro.*`와 액세스에서 충돌합니다. 이 규칙은 클릭되기 전에는 보조 규칙이었습니다. 앞의 예시에서 일반 ActiveSync 장치 유형 규칙 `Android`은 당시 기본 규칙(정규식 ActiveSync 장치 유형 규칙 `touch.*`)의 관점에서 관련이 없었기 때문에 보조 규칙으로 표시되지 않았습니다.

일반 표현식 로컬 규칙을 구성하려면

1. **액세스 규칙** 탭을 클릭합니다.

   Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector-exchangeactivesync-local-rule.png)

2. **장치 ID** 목록에서 로컬 규칙을 생성하려는 필드를 선택합니다.
3. 돋보기 아이콘을 클릭하여 선택한 필드에 대한 모든 고유 일치 항목을 표시합니다. 이 예시에서는 **장치 유형** 필드가 선택되었으며, 선택 항목은 아래 목록 상자에 표시됩니다.

   Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector-exchangeactivesync-localrules-unique.png)

4. 결과 목록 상자에서 항목 중 하나를 클릭한 다음 다음 옵션 중 하나를 클릭합니다.

   - **허용**은 일치하는 모든 장치에 대해 Exchange가 ActiveSync 트래픽을 허용하도록 구성됨을 의미합니다.
   - **거부**는 일치하는 모든 장치에 대해 Exchange가 ActiveSync 트래픽을 거부하도록 구성됨을 의미합니다.

   이 예시에서는 장치 유형이 SamsungSPhl720인 모든 장치의 액세스가 거부됩니다.

   Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-deny-samsung.png)

정규식을 추가하려면

정규식 로컬 규칙은 옆에 나타나는 아이콘으로 구별할 수 있습니다. -  .

정규식 규칙을 추가하려면, 주어진 필드의 결과 목록에서 기존 값을 사용하여 정규식 규칙을 만들거나(주요 스냅샷이 완료된 경우), 원하는 정규식을 직접 입력할 수 있습니다.

기존 필드 값에서 정규식 만들기

1. **액세스 규칙** 탭을 클릭합니다.

Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector-exchangeactivesync-local-rule.png)

2. **장치 ID** 목록에서 정규식 로컬 규칙을 만들 필드를 선택합니다.
3. 돋보기 아이콘을 클릭하여 선택한 필드에 대한 모든 고유 일치 항목을 표시합니다. 이 예에서는 **장치 유형** 필드가 선택되었으며, 선택 항목은 아래 목록 상자에 표시됩니다.

   Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector-exchangeactivesync-magnifier.png)
4. 결과 목록에서 항목 중 하나를 클릭합니다. 이 예에서는 **SAMSUNGSPHL720**이 선택되어 **장치 유형** 옆의 텍스트 상자에 나타납니다.

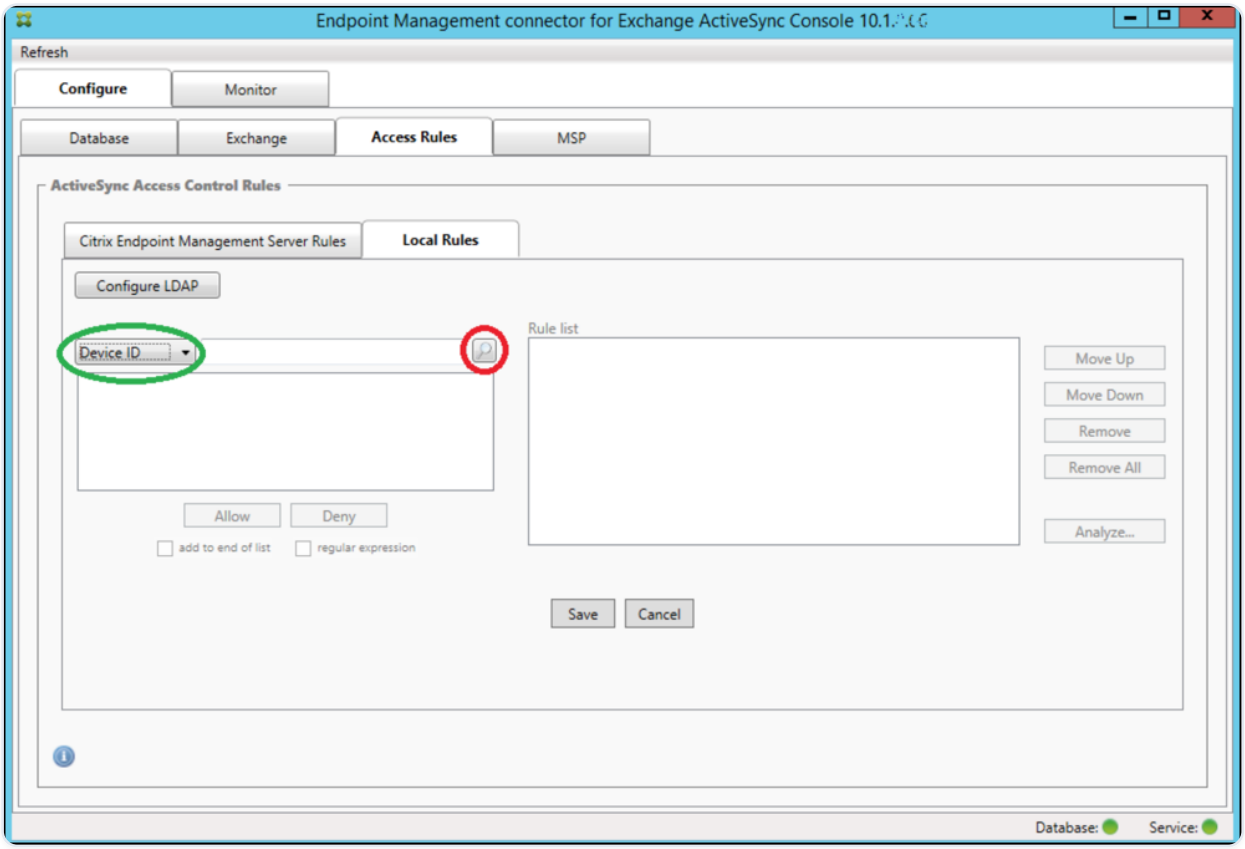
   Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector-exchangeactivesync-localrules-samsung-regex.png)
5. 장치 유형 값에 "Samsung"이 포함된 모든 장치 유형을 허용하려면 다음 단계에 따라 정규식 규칙을 추가합니다.

   a. 선택한 항목 텍스트 상자 안을 클릭합니다.
   b. 텍스트를 **SAMSUNGSPHL720**에서 **SAMSUNG.***으로 변경합니다.
   c. 정규식 확인란이 선택되어 있는지 확인합니다.
   d. **허용**을 클릭합니다.

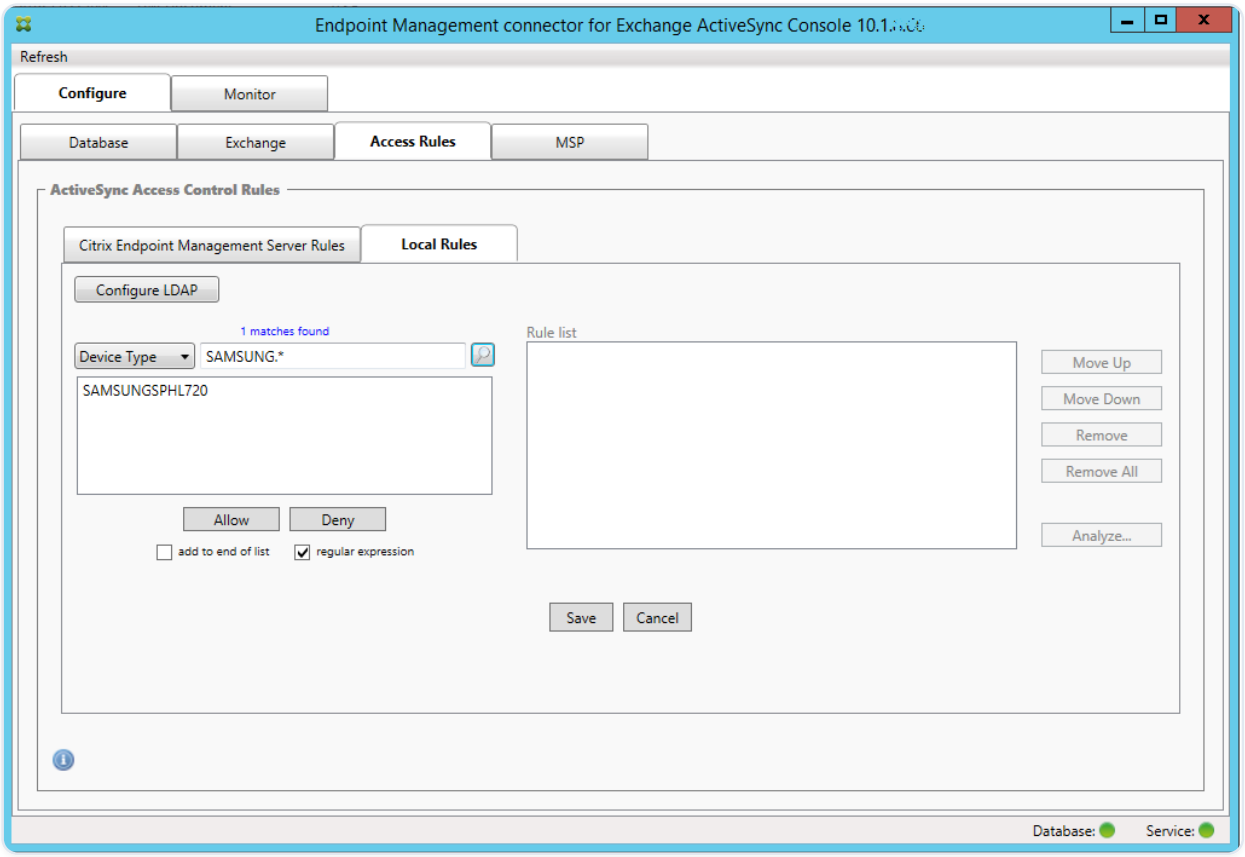
   Endpoint Management connector for Exchange ActiveSync 콘솔 페이지 이미지(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-allow-samsung.png)

액세스 규칙을 빌드하려면

1. **로컬 규칙** 탭을 클릭합니다.
2. 정규식을 입력하려면 장치 ID 목록과 선택한 항목 텍스트 상자를 모두 사용해야 합니다.



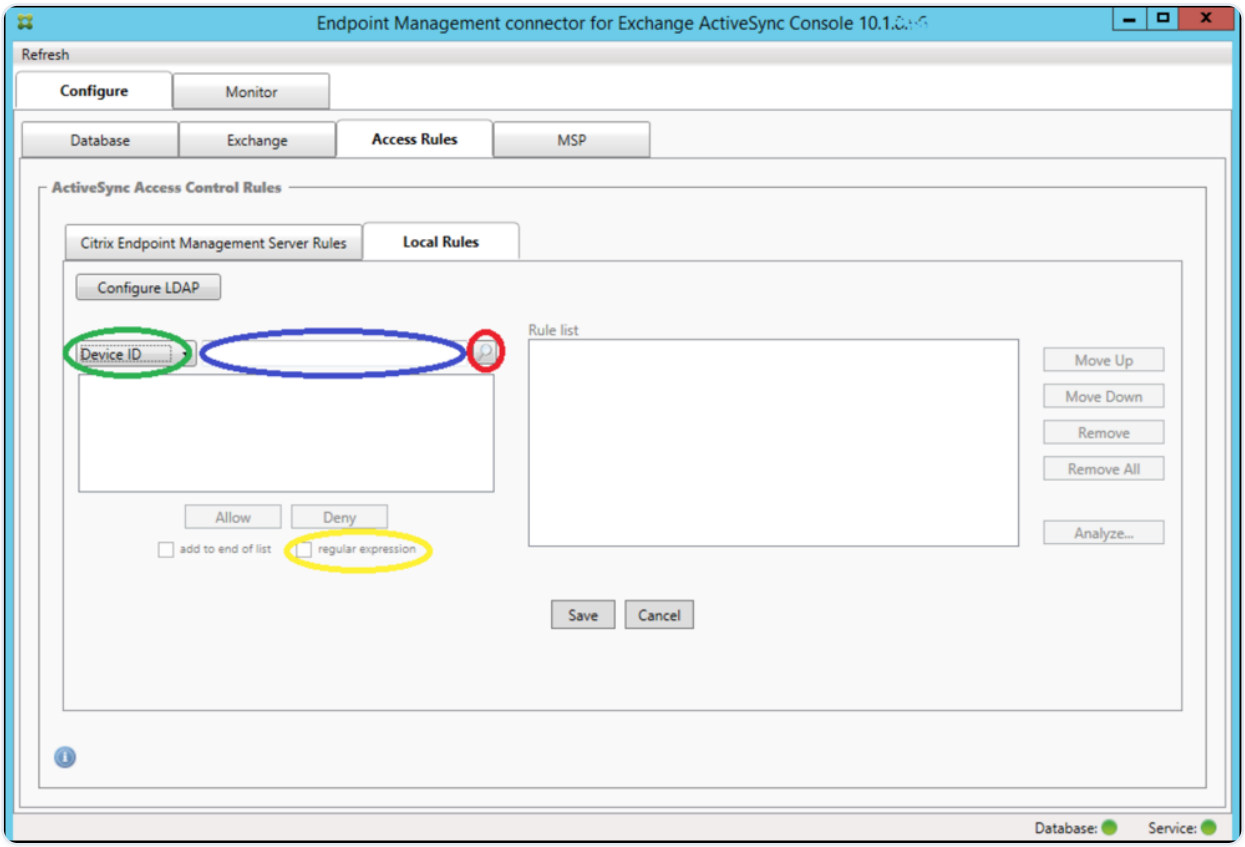
3. 일치시킬 필드를 선택합니다. 이 예시에서는 장치 유형을 사용합니다.
4. 정규식을 입력합니다. 이 예시에서는 `samsung.*`을(를) 사용합니다.
5. 정규식 확인란이 선택되어 있는지 확인한 다음 **허용** 또는 **거부**를 클릭합니다. 이 예시에서는 **허용**을 선택합니다. 최종 결과는 다음과 같습니다.



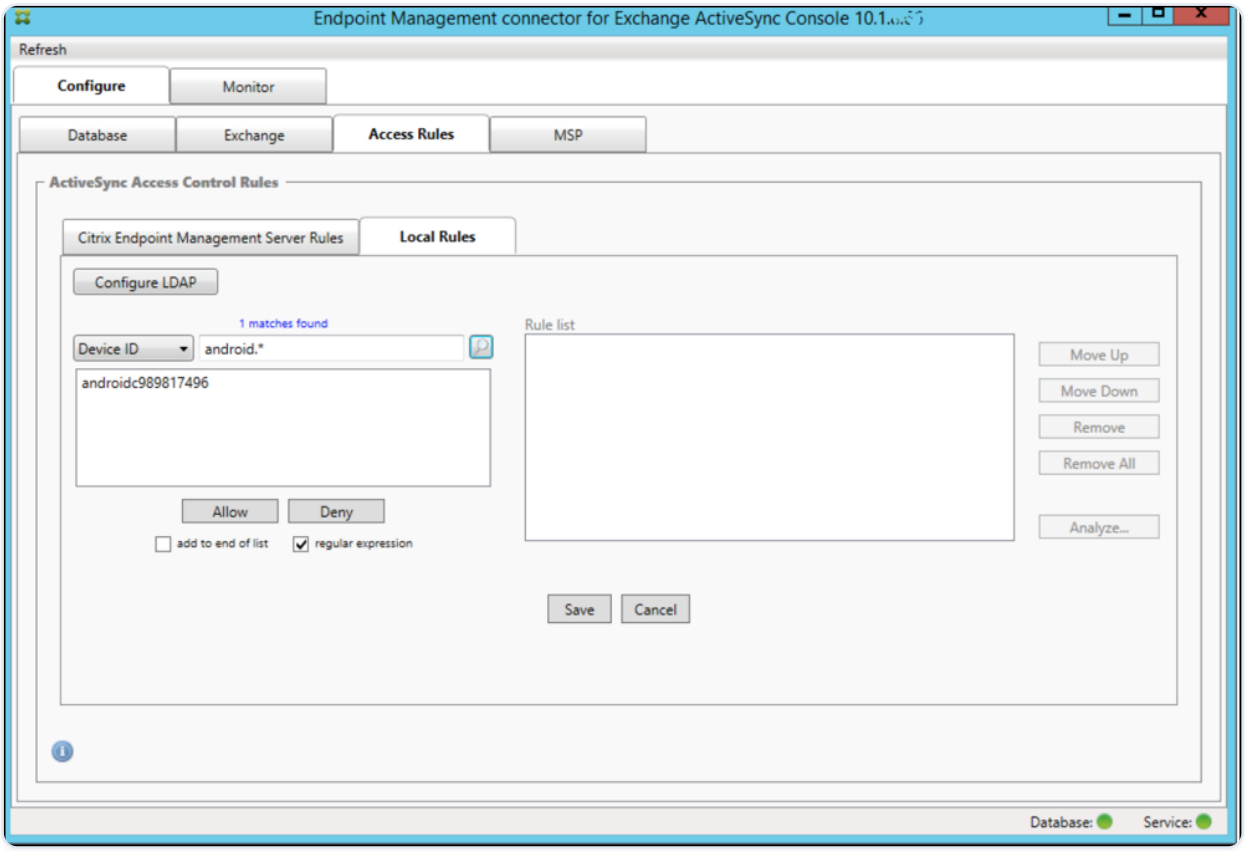
장치를 찾으려면

정규식 확인란을 선택하면 지정된 식과 일치하는 특정 장치를 검색할 수 있습니다. 이 기능은 주요 스냅샷이 성공적으로 완료된 경우에만 사용할 수 있습니다. 정규식 규칙을 사용할 계획이 없더라도 이 기능을 사용할 수 있습니다. 예를 들어, ActiveSync 장치 ID에 "workmail" 텍스트가 있는 모든 장치를 찾으려면 다음 절차를 따르십시오.

1. **액세스 규칙** 탭을 클릭합니다.
2. 장치 일치 필드 선택기가 장치 ID(기본값)로 설정되어 있는지 확인합니다.



3. 선택한 항목 텍스트 상자(앞 그림에서 파란색으로 표시됨)를 클릭한 다음 **`workmail.*`**을(를) 입력합니다.
4. 정규식 확인란이 선택되어 있는지 확인한 다음 돋보기 아이콘을 클릭하여 다음 그림과 같이 일치 항목을 표시합니다.

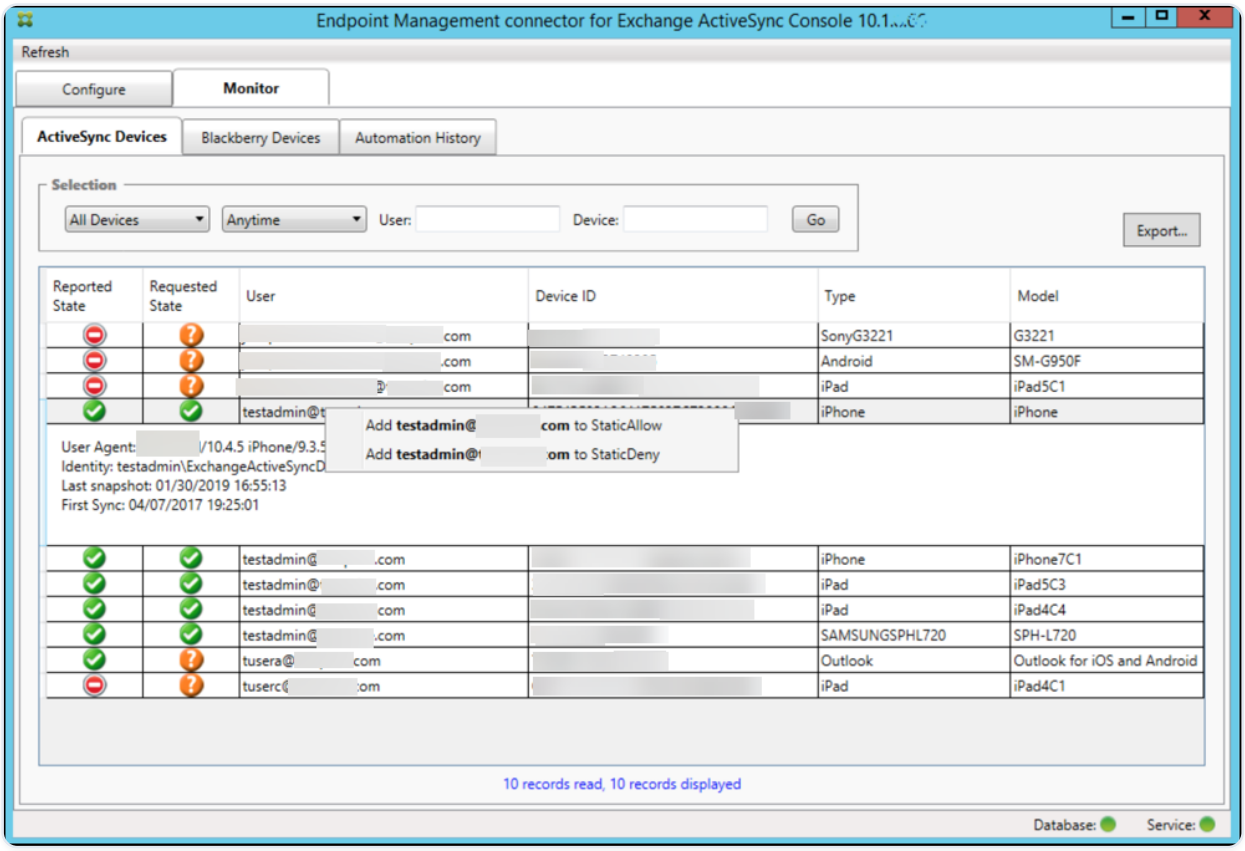


개별 사용자, 장치 또는 장치 유형을 정적 규칙에 추가하려면

사용자, 장치 ID 또는 장치 유형을 기반으로 정적 규칙을 **ActiveSync Devices** 탭에서 추가할 수 있습니다.

1. **ActiveSync Devices** 탭을 클릭합니다.
2. 목록에서 사용자, 장치 또는 장치 유형을 마우스 오른쪽 버튼으로 클릭하고 선택 항목을 허용할지 또는 거부할지 선택합니다.

   다음 이미지는 user1이 선택되었을 때 허용/거부 옵션을 보여줍니다.



장치 모니터링

Endpoint Management connector for Exchange ActiveSync의 **모니터** 탭에서는 감지된 Exchange ActiveSync 및 BlackBerry 장치와 발행된 자동 PowerShell 명령 기록을 찾아볼 수 있습니다. **모니터** 탭에는 다음 세 가지 탭이 있습니다.

- **ActiveSync 장치**:
  - **내보내기** 버튼을 클릭하여 표시된 ActiveSync 장치 파트너십을 내보낼 수 있습니다.
  - **사용자**, **장치 ID** 또는 **유형** 열을 마우스 오른쪽 버튼으로 클릭하고 적절한 허용 또는 차단 규칙 유형을 선택하여 로컬(정적) 규칙을 추가할 수 있습니다.
  - 확장된 행을 축소하려면 확장된 행을 Ctrl-클릭합니다.
- **Blackberry 장치**
- **자동화 기록**

구성 탭에는 모든 스냅샷 기록이 표시됩니다. 스냅샷 기록에는 스냅샷이 수행된 시기, 소요 시간, 감지된 장치 수 및 발생한 오류가 표시됩니다.

- **Exchange** 탭에서 원하는 Exchange Server의 정보 아이콘을 클릭합니다.
- **MSP** 탭에서 원하는 BlackBerry Server의 정보 아이콘을 클릭합니다.

문제 해결 및 진단

Endpoint Management connector for Exchange ActiveSync는 오류 및 기타 운영 정보를 로그 파일(*설치 폴더*\log\XmmWindowsService.log)에 기록합니다. Endpoint Management connector for Exchange ActiveSync는 중요한 이벤트를 Windows 이벤트 로그에도 기록합니다.

로깅 수준 변경

Endpoint Management connector for Exchange ActiveSync에는 오류(Error), 정보(Info), 경고(Warn), 디버그(Debug) 및 추적(Trace) 로깅 수준이 포함됩니다.

> **참고:**
>
> 각 후속 수준은 더 많은 세부 정보(더 많은 데이터)를 생성합니다. 예를 들어, 오류 수준은 가장 적은 세부 정보를 제공하는 반면, 추적 수준은 가장 많은 세부 정보를 제공합니다.

로깅 수준을 변경하려면 다음을 수행합니다.

1. C:\Program Files\Citrix\Citrix Endpoint Management connector에서 nlog.config 파일을 엽니다.
2. `<rules>` 섹션에서 *minilevel* 매개변수를 원하는 로깅 수준으로 변경합니다. 예를 들면 다음과 같습니다.

   ```
   <rules>


   <logger name="*" writeTo="file" minlevel="Debug" />


   </rules>
   ```

3. 파일을 저장합니다.

   변경 사항은 즉시 적용됩니다. Exchange ActiveSync용 커넥터를 다시 시작할 필요가 없습니다.

일반적인 오류

다음 목록에는 일반적인 오류가 포함되어 있습니다.

- Exchange ActiveSync 서비스용 Endpoint Management 커넥터가 시작되지 않음

  오류에 대한 로그 파일 및 Windows 이벤트 로그를 확인하십시오. 일반적인 원인은 다음과 같습니다.

  - Exchange ActiveSync 서비스용 Endpoint Management 커넥터가 SQL Server에 액세스할 수 없습니다. 이는 다음 문제로 인해 발생할 수 있습니다.
    - SQL Server 서비스가 실행되고 있지 않습니다.
    - 인증 실패.

    Windows 통합 인증이 구성된 경우, Exchange ActiveSync 서비스용 Endpoint Management 커넥터의 사용자 계정은 허용된 SQL 로그온이어야 합니다. Exchange ActiveSync 서비스용 Endpoint Management 커넥터의 계정은 기본적으로 로컬 시스템이지만, 로컬 관리자 권한이 있는 모든 계정으로 변경될 수 있습니다. SQL 인증이 구성된 경우, SQL 로그온은 SQL에서 올바르게 구성되어야 합니다.
  - MSP(Mobile Service Provider)에 대해 구성된 포트를 사용할 수 없습니다. 시스템의 다른 프로세스에서 사용하지 않는 수신 포트를 선택해야 합니다.

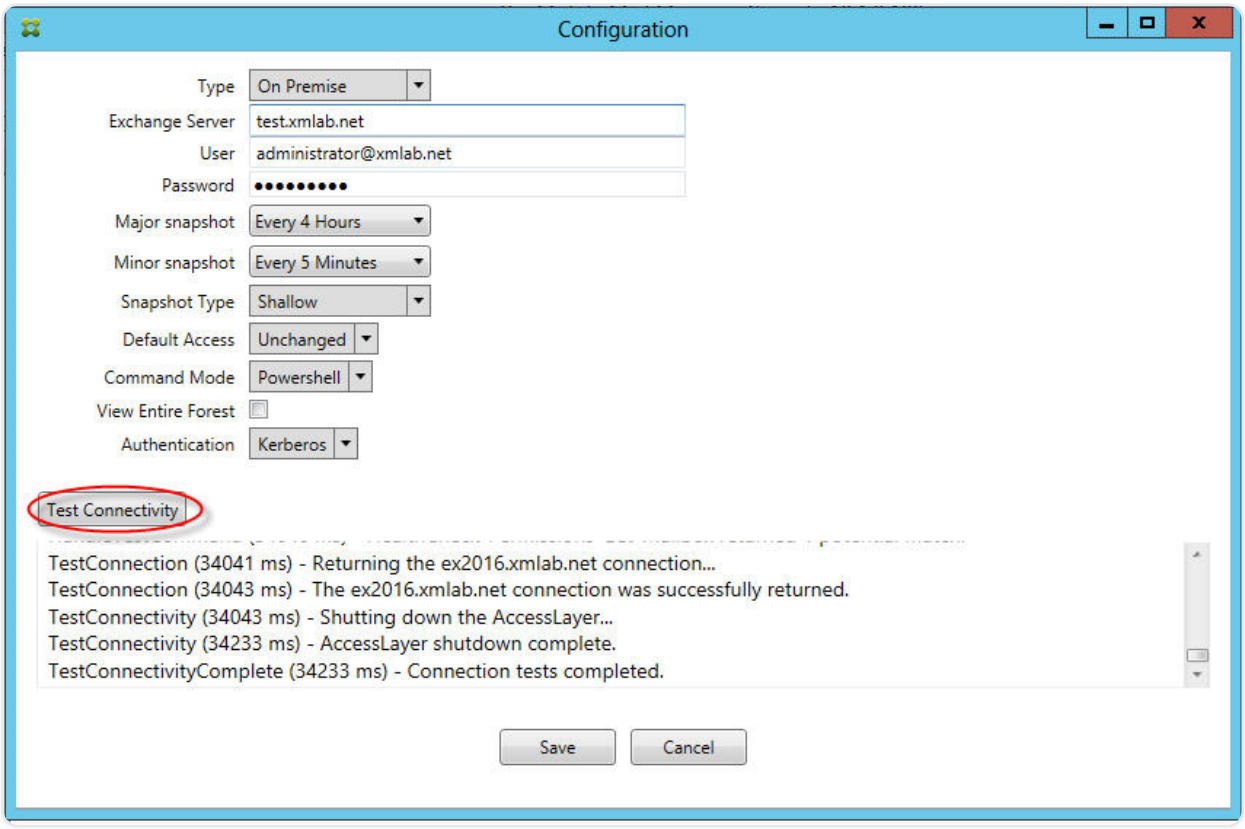
- XenMobile이 MSP에 연결할 수 없습니다.

  Exchange ActiveSync 콘솔용 Endpoint Management 커넥터의 **Configure > MSP** 탭에서 MSP 서비스 포트 및 전송이 올바르게 구성되었는지 확인하십시오. 권한 부여 그룹 또는 사용자가 올바르게 설정되었는지 확인하십시오.

  HTTPS가 구성된 경우, 유효한 SSL 서버 인증서가 설치되어야 합니다. IIS가 설치된 경우, IIS 관리자를 사용하여 인증서를 설치할 수 있습니다. IIS가 설치되지 않은 경우, 인증서 설치에 대한 자세한 내용은 SSL 인증서로 포트를 구성하는 방법을(를) 참조하십시오.

  Exchange ActiveSync용 Endpoint Management 커넥터에는 MSP 서비스 연결을 테스트하는 유틸리티 프로그램이 포함되어 있습니다. *InstallFolder*\MspTestServiceClient.exe 프로그램을 실행하고 URL 및 자격 증명을 XenMobile에 구성된 URL 및 자격 증명으로 설정한 다음 **Test Connectivity**를 클릭합니다. 이는 XenMobile Server가 발행하는 웹 서비스 요청을 시뮬레이션합니다. HTTPS가 구성된 경우, 서버의 실제 호스트 이름(SSL 인증서에 지정된 이름)을 지정해야 합니다.

  Test Connectivity를 사용할 때, 최소한 하나의 ActiveSyncDevice 레코드가 있는지 확인하십시오. 그렇지 않으면 테스트가 실패할 수 있습니다.



문제 해결 도구

문제 해결을 위한 PowerShell 유틸리티 세트는 **Support\PowerShell** 폴더에서 사용할 수 있습니다.

문제 해결 도구는 사용자 사서함 및 장치에 대한 심층 분석을 수행하여 오류 조건 및 잠재적인 실패 영역을 감지하고, 사용자에 대한 심층 RBAC 분석을 수행합니다. 모든 cmdlet의 원시 출력을 텍스트 파일로 저장할 수 있습니다.

익스체인지 액티브싱크용 시트릭스 게이트웨이 커넥터™

XenMobile Citrix ADC Connector는 이제 Exchange ActiveSync용 Citrix Gateway 커넥터입니다. Citrix 통합 포트폴리오에 대한 자세한 내용은 Citrix 제품 가이드를 참조하십시오.

Exchange ActiveSync용 커넥터는 ActiveSync 클라이언트에 대한 장치 수준 권한 부여 서비스를 Citrix ADC에 제공하며, Citrix ADC는 Exchange ActiveSync 프로토콜의 역방향 프록시 역할을 합니다. 권한 부여는 XenMobile® 내에서 정의하는 정책과 Exchange ActiveSync용 Citrix Gateway 커넥터에서 로컬로 정의하는 규칙의 조합으로 제어됩니다.

자세한 내용은 ActiveSync Gateway를 참조하십시오.

자세한 참조 아키텍처 다이어그램은 아키텍처를 참조하십시오.

Exchange ActiveSync용 Citrix Gateway 커넥터의 현재 릴리스는 버전 8.5.2입니다.

> **중요:**

> 2022년 10월부터 Microsoft에서 여기에 발표한 인증 변경 사항으로 인해 Exchange ActiveSync용 Endpoint Management 및 Citrix Gateway 커넥터는 더 이상 Exchange Online을 지원하지 않습니다. Exchange용 Endpoint Management 커넥터는 Microsoft Exchange Server(온프레미스)에서 계속 작동합니다.

새로운 기능

다음 섹션에서는 이전에는 XenMobile Citrix ADC Connector였던 Exchange ActiveSync용 Citrix Gateway 커넥터의 현재 및 이전 버전에서 새로 추가된 기능을 나열합니다.

버전 8.5.3의 새로운 기능

- 이 릴리스에서는 ActiveSync 프로토콜 16.0 및 16.1에 대한 지원이 추가되었습니다.
- Google Analytics로 전송되는 분석에 더 많은 세부 정보가 추가되었으며, 특히 스냅샷과 관련하여 그렇습니다.

버전 8.5.2의 새로운 기능

- XenMobile Citrix ADC Connector는 이제 Exchange ActiveSync용 Citrix Gateway 커넥터입니다.

이번 릴리스에서 다음 문제가 해결되었습니다:

- 정책 규칙을 정의할 때 두 개 이상의 기준이 사용되고 기준 중 하나에 사용자 ID가 포함되는 경우, 다음 문제가 발생할 수 있습니다. 사용자가 여러 별칭을 가지고 있으면 규칙을 적용할 때 해당 별칭도 확인되지 않습니다.

> **참고:**
>
> 다음 새로운 기능 섹션에서는 Citrix Gateway connector for Exchange ActiveSync를 이전 이름인 XenMobile Citrix ADC Connector로 지칭합니다. 이 이름은 버전 8.5.2부터 변경되었습니다.

버전 8.5.1.11의 새로운 기능

- **시스템 요구 사항 변경:** 현재 버전의 Citrix ADC Connector에는 Microsoft .NET Framework 4.5가 필요합니다.
- **Google Analytics 지원:** XenMobile Citrix ADC Connector 사용 방법을 파악하여 제품을 개선할 수 있는 부분에 집중하고자 합니다.
- **TLS 1.1 및 1.2 지원:** 보안이 약화됨에 따라 TLS 1.0은 PCI 위원회에서 더 이상 사용하지 않도록 권고하고 있습니다. TLS 1.1 및 1.2 지원이 XenMobile Citrix ADC Connector에 추가되었습니다.

익스체인지 액티브싱크용 시트릭스 게이트웨이 커넥터 모니터링

Exchange ActiveSync 구성 유틸리티용 Citrix Gateway connector는 Secure Mobile Gateway에서 허용되거나 차단되는 Exchange Server를 통과하는 모든 트래픽을 볼 수 있는 자세한 로깅을 제공합니다.

로그 탭을 사용하여 인증을 위해 Citrix ADC에서 Exchange ActiveSync용 커넥터로 전달된 ActiveSync 요청 기록을 볼 수 있습니다.

또한, Exchange ActiveSync 웹 서비스용 Citrix Gateway connector가 실행 중인지 확인하려면 커넥터 서버의 브라우저에 다음 URL을 로드합니다 `https://<host:port>/services/ActiveSync/Version`. URL이 제품 버전을 문자열로 반환하면 웹 서비스가 응답하는 것입니다.

Exchange ActiveSync용 Citrix Gateway connector로 ActiveSync 트래픽을 시뮬레이션하려면

Exchange ActiveSync용 Citrix Gateway connector를 사용하여 정책에 따라 ActiveSync 트래픽이 어떻게 보이는지 시뮬레이션할 수 있습니다. 커넥터 구성 유틸리티에서 **시뮬레이터** 탭을 선택합니다. 결과에는 구성한 규칙에 따라 정책이 어떻게 적용되는지 표시됩니다.

익스체인지 액티브싱크용 시트릭스 게이트웨이 커넥터 필터 선택

Citrix Gateway connector for Exchange ActiveSync 필터는 특정 정책 위반 또는 속성 설정을 위해 장치를 분석하여 작동합니다. 장치가 기준을 충족하면 장치 목록에 배치됩니다. 이 장치 목록은 허용 목록도 차단 목록도 아닙니다. 정의된 기준을 충족하는 장치 목록입니다. XenMobile 내 커넥터에서 다음 필터를 사용할 수 있습니다. 각 필터에 대한 두 가지 옵션은 **허용** 또는 **거부**입니다.

- **익명 장치:** XenMobile에 등록되었지만 사용자 ID를 알 수 없는 장치를 허용하거나 거부합니다. 예를 들어, 등록되었지만 Active Directory 암호가 만료된 사용자이거나 알 수 없는 자격 증명으로 등록한 사용자일 수 있습니다.
- **Samsung KNOX 증명 실패:** Samsung 장치에는 보안 및 진단 기능이 있습니다. 이 필터는 장치가 KNOX용으로 설정되었음을 확인합니다. 자세한 내용은 Samsung Knox를 참조하십시오.
- **금지된 앱:** 차단 목록 정책에 의해 정의된 장치 목록 및 차단된 앱의 존재 여부에 따라 장치를 허용하거나 거부합니다.
- **암시적 허용/거부:** 다른 필터 규칙 기준을 충족하지 않는 모든 장치의 장치 목록을 생성하고 해당 목록을 기반으로 허용하거나 거부합니다. 암시적 허용/거부 옵션은 장치 탭에서 Citrix Gateway connector for Exchange ActiveSync 상태가 활성화되고 장치에 대한 커넥터 상태를 표시하도록 합니다. 암시적 허용/거부 옵션은 선택되지 않은 다른 모든 커넥터 필터도 제어합니다. 예를 들어, 암시적 허용/거부 옵션이 **허용**으로 설정되어 있기 때문에 커넥터는 차단된 앱을 거부하지만 다른 모든 필터는 허용합니다.
- **비활성 장치:** 지정된 시간 내에 XenMobile과 통신하지 않은 장치의 장치 목록을 생성합니다. 이러한 장치는 비활성으로 간주됩니다. 필터는 그에 따라 장치를 허용하거나 거부합니다.
- **필수 앱 누락:** 사용자가 등록할 때 설치해야 하는 필수 앱 목록을 받습니다. 필수 앱 누락 필터는 하나 이상의 앱이 더 이상 존재하지 않음을 나타냅니다. 예를 들어, 사용자가 하나 이상의 앱을 삭제한 경우입니다.
- **권장되지 않는 앱:** 사용자가 등록할 때 설치해야 하는 앱 목록을 받습니다. 권장되지 않는 앱 필터는 해당 목록에 없는 앱에 대해 장치를 확인합니다.
- **규정 미준수 암호:** 장치에 암호가 없는 모든 장치의 장치 목록을 생성합니다.
- **규정 미준수 장치:** 자체 내부 IT 규정 준수 기준을 충족하는 장치를 거부하거나 허용할 수 있습니다. 규정 준수는 **True** 또는 **False**일 수 있는 부울 플래그인 Out of Compliance라는 장치 속성으로 정의된 임의

설정입니다. (이 속성을 수동으로 생성하고 값을 설정하거나, 장치가 특정 기준을 충족하거나 충족하지 않는 경우 자동화된 작업을 사용하여 장치에 이 속성을 생성할 수 있습니다.)

  - **규정 미준수 = True**. 장치가 IT 부서에서 설정한 규정 준수 표준 및 정책 정의를 충족하지 않으면 해당 장치는 규정 미준수 상태입니다.
  - **규정 미준수 = False**. 장치가 IT 부서에서 설정한 규정 준수 표준 및 정책 정의를 충족하면 해당 장치는 규정 준수 상태입니다.

- **해지 상태:** 해지된 모든 장치의 장치 목록을 생성하고 해지 상태를 기반으로 허용하거나 거부합니다.
- **루팅된 Android/탈옥된 iOS 장치**. 루팅된 것으로 플래그 지정된 모든 장치의 장치 목록을 생성하고 루팅 상태를 기반으로 허용하거나 거부합니다.
- **관리되지 않는 장치**. XenMobile 데이터베이스의 모든 장치에 대한 장치 목록을 생성합니다. Mobile Application Gateway는 차단 모드로 배포되어야 합니다.

Exchange ActiveSync용 Citrix Gateway 커넥터에 대한 연결 구성

Exchange ActiveSync용 Citrix Gateway 커넥터는 보안 웹 서비스를 통해 XenMobile 및 기타 원격 구성 공급자와 통신합니다.

1. 커넥터 구성 유틸리티에서 **구성 공급자** 탭을 클릭한 다음 **추가**를 클릭합니다.
2. **구성 공급자** 대화 상자의 **이름**에 관리자 권한이 있고 XenMobile Server와 기본 HTTP 인증에 사용되는 사용자 이름을 입력합니다.
3. **URL**에 XenMobile GCS의 웹 주소를 입력합니다. 일반적으로 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 형식입니다. *MagConfigService* 이름은 대소문자를 구분합니다.
4. **암호**에 XenMobile Server와 기본 HTTP 인증에 사용되는 암호를 입력합니다.
5. **관리 호스트**에 커넥터 서버 이름을 입력합니다.
6. **기준 간격**에 Device Manager에서 새로 고쳐진 동적 규칙 집합을 가져올 시간 간격을 지정합니다.
7. **델타 간격**에 동적 규칙 업데이트를 가져올 시간 간격을 지정합니다.
8. **요청 시간 초과**에 서버 요청 시간 초과 간격을 지정합니다.
9. **구성 공급자**에서 구성 공급자 서버 인스턴스가 정책 구성을 제공하는지 여부를 선택합니다.
10. **이벤트 사용**에서 장치가 차단될 때 커넥터가 XenMobile에 알리도록 하려면 이 옵션을 활성화합니다. XenMobile 자동화된 작업에서 커넥터 규칙을 사용하는 경우 이 옵션이 필요합니다.
11. **저장**을 클릭한 다음 **연결 테스트**를 클릭하여 게이트웨이-구성 공급자 연결을 테스트합니다. 연결에 실패하면 로컬 방화벽 설정이 연결을 허용하는지 확인하거나 관리자에게 문의하십시오.

12. 연결에 성공하면 **비활성화됨** 확인란을 선택 취소한 다음 **저장**을 클릭합니다.

새 구성 공급자를 추가하면 Exchange ActiveSync용 Citrix Gateway 커넥터는 공급자와 연결된 하나 이상의 정책을 자동으로 생성합니다. 이러한 정책은 NewPolicyTemplate 섹션의 `config\policyTemplates.xml`에 포함된 템플릿 정의에 의해 정의됩니다. 이 섹션 내에 정의된 각 정책 요소에 대해 새 정책이 생성됩니다.

다음 조건이 충족되면 운영자가 정책 요소를 추가, 제거 또는 수정할 수 있습니다. 정책 요소가 스키마 정의를 준수하고 표준 대체 문자열(중괄호로 묶음)이 수정되지 않은 경우. 다음으로, 공급자를 위한 새 그룹을 추가하고 정책을 업데이트하여 새 그룹을 포함합니다.

XenMobile에서 정책을 가져오려면

1. Exchange ActiveSync 구성 유틸리티용 Citrix Gateway connector에서 **구성 공급자** 탭을 클릭한 다음 **추가**를 클릭합니다.
2. **구성 공급자** 대화 상자의 **이름**에 XenMobile Server와 기본 HTTP 인증에 사용되며 관리자 권한이 있는 사용자 이름을 입력합니다.
3. **URL**에 XenMobile Gateway Configuration Service(GCS)의 웹 주소를 입력합니다. 일반적으로 `https://<xdmHost>/xdm/services/<MagConfigService>` 형식입니다. MagConfigService 이름은 대소문자를 구분합니다.
4. **암호**에 XenMobile Server와 기본 HTTP 인증에 사용되는 암호를 입력합니다.
5. 게이트웨이-구성 공급자 연결을 테스트하려면 **연결 테스트**를 클릭합니다. 연결에 실패하면 로컬 방화벽 설정이 연결을 허용하는지 확인하거나 관리자에게 문의하십시오.
6. 연결이 성공적으로 설정되면 **사용 안 함** 확인란을 선택 취소한 다음 **저장**을 클릭합니다.
7. **호스트 관리**에서 로컬 호스트 컴퓨터의 기본 DNS 이름을 그대로 둡니다. 이 설정은 여러 Forefront Threat Management Gateway(TMG) 서버가 배열로 구성될 때 XenMobile과의 통신을 조정하는 데 사용됩니다.

   설정을 저장한 후 GCS를 엽니다.

Exchange ActiveSync 정책 모드용 Citrix Gateway connector 구성

Exchange ActiveSync용 Citrix Gateway connector는 다음 6가지 모드로 실행될 수 있습니다.

- **모두 허용**. 이 정책 모드는 커넥터를 통과하는 모든 트래픽에 대한 액세스를 허용합니다. 다른 필터링 규칙은 사용되지 않습니다.

- **모두 거부**. 이 정책 모드는 커넥터를 통과하는 모든 트래픽에 대한 액세스를 차단합니다. 다른 필터링 규칙은 사용되지 않습니다.
- **정적 규칙: 차단 모드**. 이 정책 모드는 끝에 암시적 거부 또는 차단 문과 함께 정적 규칙을 실행합니다. 커넥터는 다른 필터 규칙을 통해 허용되거나 허가되지 않은 장치를 차단합니다.
- **정적 규칙: 허용 모드**. 이 정책 모드는 끝에 암시적 허용 또는 허가 문이 있는 정적 규칙을 실행합니다. 다른 필터 규칙을 통해 차단되거나 거부되지 않은 장치는 커넥터를 통해 허용됩니다.
- **정적 + ZDM 규칙**: 차단 모드. 이 정책 모드는 정적 규칙을 먼저 실행한 다음, XenMobile의 동적 규칙을 실행하며 끝에 암시적 거부 또는 차단 문이 있습니다. 장치는 정의된 필터 및 장치 관리자 규칙에 따라 허용되거나 거부됩니다. 정의된 필터 및 규칙과 일치하지 않는 모든 장치는 차단됩니다.
- **정적 + ZDM 규칙**: 허용 모드. 이 정책 모드는 정적 규칙을 먼저 실행한 다음, XenMobile의 동적 규칙을 실행하며 끝에 암시적 허용 또는 허가 문이 있습니다. 장치는 정의된 필터 및 XenMobile 규칙에 따라 허용되거나 거부됩니다. 정의된 필터 및 규칙과 일치하지 않는 모든 장치는 허용됩니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 프로세스는 XenMobile에서 수신된 iOS 및 Windows 기반 모바일 장치의 고유한 ActiveSync ID를 기반으로 동적 규칙에 대한 허용 또는 차단을 수행합니다. Android 장치는 제조업체에 따라 동작이 다르며 일부는 고유한 ActiveSync ID를 쉽게 노출하지 않습니다. 이를 보완하기 위해 XenMobile은 Android 장치에 대한 사용자 ID 정보를 전송하여 허용 또는 차단 결정을 내립니다. 결과적으로 사용자가 Android 장치를 하나만 가지고 있는 경우 허용 및 차단 기능은 정상적으로 작동합니다. 사용자가 여러 Android 장치를 가지고 있는 경우 Android 장치를 구별할 수 없으므로 모든 장치가 허용됩니다. 알려진 경우 ActiveSyncID를 통해 이러한 장치를 정적으로 차단하도록 게이트웨이를 구성할 수 있습니다. 또한 장치 유형 또는 사용자 에이전트를 기반으로 차단하도록 게이트웨이를 구성할 수도 있습니다.

정책 모드를 지정하려면 SMG 컨트롤러 구성 유틸리티에서 다음을 수행하십시오.

1. **경로 필터** 탭을 클릭한 다음 **추가**를 클릭합니다.
2. **경로 속성** 대화 상자에서 **정책** 목록에서 정책 모드를 선택한 다음 **저장**을 클릭합니다.

구성 유틸리티의 **정책** 탭에서 규칙을 검토할 수 있습니다. 규칙은 Exchange ActiveSync용 Citrix Gateway 커넥터에서 위에서 아래로 처리됩니다. 허용 정책은 녹색 확인 표시로 표시됩니다. 거부 정책은 빨간색 원에 선이 그어진 형태로 표시됩니다. 화면을 새로 고쳐 최신 규칙을 보려면 **새로 고침**을 클릭합니다. config.xml 파일에서 규칙의 순서를 수정할 수도 있습니다.

규칙을 테스트하려면 **시뮬레이터** 탭을 클릭합니다. 필드에 값을 지정합니다. 이 값은 로그에서도 얻을 수 있습니다. 허용 또는 차단을 지정하는 결과 메시지가 나타납니다.

정적 규칙 구성

ActiveSync 연결 HTTP 요청의 ISAPI 필터링이 읽는 값으로 정적 규칙을 입력합니다. 정적 규칙을 통해 Exchange ActiveSync용 Citrix Gateway 커넥터는 다음 기준에 따라 트래픽을 허용하거나 차단할 수 있습니다.

- **사용자:** Exchange ActiveSync용 Citrix Gateway 커넥터는 장치 등록 중에 캡처된 승인된 사용자 값 및 이름 구조를 사용합니다. 이는 일반적으로 LDAP를 통해 Active Directory에 연결된 XenMobile을 실행하는 서버에서 참조하는 domain\username으로 찾을 수 있습니다. 커넥터 구성 유틸리티 내의 **로그** 탭은 커넥터를 통해 전달되는 값을 보여줍니다. 값 구조를 결정해야 하거나 다른 경우 값이 전달됩니다.
- **장치 ID (ActiveSyncID):** 연결된 장치의 ActiveSyncID로도 알려져 있습니다. 이 값은 일반적으로 XenMobile 콘솔의 특정 장치 속성 페이지에서 찾을 수 있습니다. 이 값은 커넥터 구성 유틸리티의 로그 탭에서도 확인할 수 있습니다.
- **장치 유형:** 커넥터는 장치가 iPhone, iPad 또는 기타 장치 유형인지 여부를 판단하고 해당 기준에 따라 허용하거나 차단할 수 있습니다. 다른 값과 마찬가지로 커넥터 구성 유틸리티는 ActiveSync 연결에 대해 처리되는 모든 연결된 장치 유형을 표시할 수 있습니다.
- **사용자 에이전트:** 사용되는 ActiveSync 클라이언트에 대한 정보를 포함합니다. 일반적으로 지정된 값은 모바일 장치 플랫폼의 특정 운영 체제 빌드 및 버전에 해당합니다.

서버에서 실행되는 커넥터 구성 유틸리티는 항상 정적 규칙을 관리합니다.

1. SMG 컨트롤러 구성 유틸리티에서 **정적 규칙** 탭을 클릭한 다음 **추가**를 클릭합니다.
2. **정적 규칙 속성** 대화 상자에서 기준으로 사용할 값을 지정합니다. 예를 들어, 사용자 이름(예: AllowedUser)을 입력하고 **비활성화됨** 확인란을 선택 취소하여 액세스를 허용할 사용자를 입력할 수 있습니다.
3. **저장**을 클릭합니다.

   이제 정적 규칙이 적용됩니다. 또한 정규식을 사용하여 값을 정의할 수 있지만, config.xml 파일에서 규칙 처리 모드를 활성화해야 합니다.

동적 규칙을 구성하려면

XenMobile의 장치 정책 및 속성은 동적 규칙을 정의하며 동적 Citrix Gateway connector for Exchange ActiveSync 필터를 트리거할 수 있습니다. 트리거는 정책 위반 또는 속성 설정의 존재 여부에 따라 달라집니다. 커넥터 필터는 주어진 정책 위반 또는 속성 설정에 대해 장치를 분석하여 작동합니다. 장치가 기준을 충족하면 장치는 장치 목록에 배치됩니다. 이 장치 목록은 허용 목록이나 차단 목록이 아닙니다. 정의된 기준을 충족하는 장치 목록입니다. 다음 구성 옵션을 사용하면 커넥터를 사용하여 장치 목록에 있는 장치를 허용할지 또는 거부할지 정의할 수 있습니다.

참고:

동적 규칙을 구성하려면 XenMobile 콘솔을 사용해야 합니다.

1. XenMobile 콘솔에서 오른쪽 상단 모서리에 있는 기어 아이콘을 클릭합니다. **설정** 페이지가 나타납니다.
2. **서버** 아래에서 **ActiveSync Gateway**를 클릭합니다. ActiveSync Gateway 페이지가 나타납니다.
3. **다음 규칙 활성화**에서 활성화할 규칙을 하나 이상 선택합니다.
4. Android 전용에서 **Android 도메인 사용자를 ActiveSync Gateway로 보내기**에서 **예**를 클릭하여 XenMobile이 Android 장치 정보를 Secure Mobile Gateway로 보내도록 합니다.

   이 옵션을 활성화하면 XenMobile이 Android 장치 사용자의 ActiveSync 식별자를 가지고 있지 않을 때 XenMobile이 Android 장치 정보를 Citrix Gateway connector for Exchange ActiveSync로 보냅니다.

Exchange ActiveSync XML 파일용 Citrix Gateway 커넥터를 편집하여 사용자 지정 정책을 구성하려면

기본 구성의 기본 정책은 Citrix Gateway connector for Exchange ActiveSync 구성 유틸리티의 **정책** 탭에서 볼 수 있습니다. 사용자 지정 정책을 만들려면 커넥터 XML 구성 파일(config\config.xml)을 편집할 수 있습니다.

1. 파일에서 **PolicyList** 섹션을 찾아 새 **Policy** 요소를 추가합니다.
2. 다른 정적 그룹 또는 다른 GCP를 지원하는 그룹과 같이 새 그룹이 필요한 경우, 새 **Group** 요소를 **GroupList** 섹션에 추가합니다.
3. 선택적으로, **GroupRef** 요소의 순서를 재배열하여 기존 정책 내 그룹의 순서를 변경할 수 있습니다.

Exchange ActiveSync XML 파일용 Citrix Gateway 커넥터 구성

Exchange ActiveSync용 Citrix Gateway 커넥터는 XML 구성 파일을 사용하여 커넥터의 동작을 지시합니다. 다른 항목들 중에서 이 파일은 HTTP 요청을 평가할 때 필터가 수행하는 그룹 파일 및 관련 작업을 지정합니다. 기본적으로 파일 이름은 config.xml이며 다음 위치에서 찾을 수 있습니다: ..\Program Files\Citrix\XenMobile Citrix ADC Connector\config\.

GroupRef 노드

GroupRef 노드는 논리적 그룹 이름을 정의합니다. 기본값은 AllowGroup 및 DenyGroup입니다.

참고:

> GroupRefList 노드에 나타나는 GroupRef 노드의 순서는 중요합니다.

> GroupRef 노드의 ID 값은 특정 사용자 계정 또는 장치를 일치시키는 데 사용되는 논리적 컨테이너 또는 멤버 컬렉션을 식별합니다. 작업 속성은 필터가 컬렉션의 규칙과 일치하는 멤버를 처리하는 방법을 지정합니다. 예를 들어, AllowGroup 세트의 규칙과 일치하는 사용자 계정 또는 장치는 "통과"됩니다. 통과한다는 것은 Exchange CAS에 액세스하는 것이 허용됨을 의미합니다. DenyGroup 세트의 규칙과 일치하는 사용자 계정 또는 장치는 "거부"됩니다. 거부된다는 것은 Exchange CAS에 액세스하는 것이 허용되지 않음을 의미합니다.

특정 사용자 계정/장치 또는 조합이 두 그룹의 규칙을 모두 충족하는 경우, 요청의 결과를 지시하기 위해 우선순위 규칙이 사용됩니다. 우선순위는 config.xml 파일에서 GroupRef 노드의 위에서 아래로의 순서에 반영됩니다. GroupRef 노드는 우선순위 순서로 순위가 매겨집니다. Allow 그룹의 특정 조건에 대한 규칙은 Deny 그룹의 동일한 조건에 대한 규칙보다 항상 우선합니다.

그룹 노드

또한 config.xml은 그룹 노드를 정의합니다. 이 노드는 논리적 컨테이너인 AllowGroup 및 DenyGroup을 외부 XML 파일에 연결합니다. 외부 파일에 저장된 항목은 필터 규칙의 기초를 형성합니다.

> **참고:**

> 이 릴리스에서는 외부 XML 파일만 지원됩니다.

> 기본 설치는 구성에 두 개의 XML 파일(allow.xml 및 deny.xml)을 구현합니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 구성

Exchange ActiveSync용 Citrix Gateway 커넥터를 구성하여 다음 속성을 기반으로 ActiveSync 요청을 선택적으로 차단하거나 허용할 수 있습니다. **Active Sync Service ID**, **장치 유형**, **사용자 에이전트**(장치 운영 체제), **승인된 사용자** 및 **ActiveSync 명령**.

기본 구성은 정적 및 동적 그룹의 조합을 지원합니다. SMG 컨트롤러 구성 유틸리티를 사용하여 정적 그룹을 유지 관리합니다. 정적 그룹은 특정 사용자 에이전트를 사용하는 모든 장치와 같이 알려진 장치 범주로 구성될 수 있습니다.

Gateway Configuration Provider라는 외부 소스가 동적 그룹을 유지 관리합니다. Exchange ActiveSync용 Citrix Gateway 커넥터는 주기적으로 그룹을 연결합니다. XenMobile은 허용 및 차단된 장치 및 사용자 그룹을 커넥터로 내보낼 수 있습니다.

동적 그룹은 Gateway Configuration Provider라는 외부 소스에 의해 유지 관리되며 Exchange ActiveSync용 Citrix Gateway 커넥터에 의해 주기적으로 수집됩니다. XenMobile은 허용 및 차단된 장치 및 사용자 그룹을 커넥터로 내보낼 수 있습니다.

정책은 각 그룹에 연결된 작업(허용 또는 차단)과 그룹 구성원 목록이 있는 정렬된 그룹 목록입니다. 정책에는 여러 그룹이 있을 수 있습니다. 일치하는 항목이 발견되면 해당 그룹의 작업이 수행되고 후속 그룹은 평가되지 않으므로 정책 내 그룹 순서가 중요합니다.

구성원은 요청의 속성을 일치시키는 방법을 정의합니다. 장치 ID와 같은 단일 속성 또는 장치 유형 및 사용자 에이전트와 같은 여러 속성을 일치시킬 수 있습니다.

Exchange ActiveSync용 Citrix Gateway 커넥터의 보안 모델 선택

보안 모델을 설정하는 것은 모든 규모의 조직에서 성공적인 모바일 장치 배포에 필수적입니다. 기본적으로 사용자, 컴퓨터 또는 장치에 대한 액세스를 허용하기 위해 보호되거나 격리된 네트워크 제어를 사용하는 것이 일반적입니다. 이 방법이 항상 이상적인 것은 아닙니다. IT 보안을 관리하는 모든 조직은 모바일 장치 보안에 대해 약간 다르거나 맞춤화된 접근 방식을 가질 수 있습니다.

동일한 논리가 모바일 장치 보안에도 적용됩니다. 허용 모델을 사용하는 것은 수많은 모바일 장치 및 유형, 사용자당 모바일 장치, 사용 가능한 운영 체제 플랫폼 및 앱으로 인해 약한 선택입니다. 대부분의 조직에서는 제한 모델이 가장 논리적인 선택입니다.

Citrix가 Exchange ActiveSync용 Citrix Gateway 커넥터를 XenMobile과 통합하기 위해 허용하는 구성 시나리오는 다음과 같습니다.

허용 모델 (허용 모드)

허용 보안 모델은 모든 것이 기본적으로 허용되거나 액세스 권한이 부여된다는 전제하에 작동합니다. 규칙 및 필터링을 통해서만 무언가가 차단되고 제한이 적용됩니다. 허용 보안 모델은 모바일 장치에 대한 보안 우려가 비교적 느슨한 조직에 적합합니다. 이 모델은 적절한 경우(정책 규칙이 실패할 때) 액세스를 거부하기 위한 제한적인 제어만 적용합니다.

제한적 모델 (차단 모드)

제한적 보안 모델은 기본적으로 아무것도 허용되거나 액세스 권한이 부여되지 않는다는 전제에 기반합니다. 보안 검사 지점을 통과하는 모든 것은 필터링되고 검사되며, 액세스를 허용하는 규칙이 통과되지 않으면 액세스가 거부됩니다. 제한적 보안 모델은 모바일 장치에 대해 비교적 엄격한 보안 기준을 가진 조직에 적합합니다. 이 모드는 액세스를 허용하는 모든 규칙이 통과된 경우에만 네트워크 서비스 사용 및 기능에 대한 액세스 권한을 부여합니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 관리

Exchange ActiveSync용 Citrix Gateway 커넥터를 사용하여 액세스 제어 규칙을 만들 수 있습니다. 이 규칙은 관리되는 장치에서 ActiveSync 연결 요청에 대한 액세스를 허용하거나 차단합니다. 액세스는 장치 상태, 앱 허용 또는 차단 목록 및 기타 규정 준수 조건에 따라 결정됩니다.

Exchange ActiveSync 구성 유틸리티용 Citrix Gateway 커넥터를 사용하면 기업 이메일 정책을 적용하는 동적 및 정적 규칙을 만들 수 있으며, 이를 통해 규정 준수 표준을 위반하는 사용자를 차단할 수 있습니다. 또한 이메일 첨부 파일 암호화를 설정하여 Exchange Server를 통해 관리되는 장치로 전달되는 모든 첨부 파일이 암호화되고 승인된 사용자만 관리되는 장치에서 볼 수 있도록 할 수 있습니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 제거

1. 관리자 계정으로 XncInstaller.exe를 실행합니다.
2. 화면의 지시에 따라 제거를 완료합니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 설치, 업그레이드 또는 제거

1. 관리자 계정으로 XncInstaller.exe를 실행하여 커넥터를 설치하거나 기존 커넥터의 업그레이드 또는 제거를 허용합니다.
2. 화면의 지시에 따라 설치, 업그레이드 또는 제거를 완료합니다.

커넥터를 설치한 후에는 XenMobile 구성 서비스와 알림 서비스를 수동으로 다시 시작해야 합니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 설치

Exchange ActiveSync용 Citrix Gateway 커넥터는 자체 Windows Server에 설치합니다.

커넥터가 서버에 가하는 CPU 부하는 관리되는 장치 수에 따라 달라집니다. 많은 수의 장치(50,000개 이상)의 경우 클러스터 환경이 없으면 두 개 이상의 코어를 프로비저닝해야 할 수 있습니다. 커넥터의 메모리 사용량은 더 많은 메모리를 할당할 만큼 중요하지 않습니다.

Exchange ActiveSync용 Citrix Gateway Connector 시스템 요구 사항

Exchange ActiveSync용 Citrix Gateway Connector는 Citrix ADC 어플라이언스에 구성된 SSL 브리지를 통해 Citrix ADC와 통신합니다. 이 브리지를 통해 어플라이언스는 모든 보안 트래픽을 XenMobile로 직접 브리징할 수 있습니다. 이 커넥터에는 다음 최소 시스템 구성이 필요합니다.

구성 요소	요구 사항
컴퓨터 및 프로세서	733MHz Pentium III 733MHz 이상 프로세서. 2.0GHz Pentium III 이상 프로세서(권장)
시트릭스 ADC	소프트웨어 버전 10이 설치된 Citrix ADC 어플라이언스
메모리	1GB
하드 디스크	150MB의 사용 가능한 하드 디스크 공간이 있는 NTFS 형식의 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 지원은 January 14, 2020에 종료되며, Windows Server 2012 R2 지원은 October 10, 2023에 종료됩니다.
기타 장치	내부 네트워크 통신을 위한 호스트 운영 체제와 호환되는 네트워크 어댑터
마이크로소프트 .NET 프레임워크	버전 8.5.1.11에는 Microsoft .NET Framework 4.5가 필요합니다.
디스플레이	VGA 또는 고해상도 모니터

Exchange ActiveSync용 Citrix Gateway connector의 호스트 컴퓨터에는 다음 최소 사용 가능한 하드 디스크 공간이 필요합니다.

- **애플리케이션:** 10–15MB (100MB 권장)
- **로깅:** 1GB (20GB 권장)

Exchange ActiveSync용 Citrix Gateway connector의 플랫폼 지원에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오.

장치 이메일 클라이언트

모든 이메일 클라이언트가 장치에 대해 동일한 ActiveSync ID를 일관되게 반환하는 것은 아닙니다. Exchange ActiveSync용 Citrix Gateway connector는 각 장치에 대해 고유한 ActiveSync ID를 예상하므로 다음이 적용됩니다. 각 장치에 대해 동일하고 고유한 ActiveSync ID를 일관되게 생성하는 이메일 클라이

언트만 지원됩니다. Citrix는 이러한 이메일 클라이언트를 테스트했으며 클라이언트는 오류 없이 작동했습니다.

- Samsung 기본 이메일 클라이언트
- iOS 기본 이메일 클라이언트

Exchange ActiveSync용 시트릭스 게이트웨이 커넥터 배포

Exchange ActiveSync용 Citrix Gateway connector를 사용하면 Citrix ADC를 사용하여 XenMobile 관리 장치와의 XenMobile Server 통신을 프록시하고 로드 밸런싱할 수 있습니다. 커넥터는 XenMobile과 주기적으로 통신하여 정책을 동기화합니다. 커넥터와 XenMobile은 함께 또는 독립적으로 클러스터링될 수 있으며 Citrix ADC에 의해 로드 밸런싱될 수 있습니다.

Exchange ActiveSync용 Citrix Gateway 커넥터 구성 요소

- **Exchange ActiveSync용 Citrix Gateway 커넥터 서비스:** 이 서비스는 Citrix ADC가 장치에서 ActiveSync 요청이 승인되었는지 여부를 결정하기 위해 호출할 수 있는 REST 웹 서비스 인터페이스를 제공합니다.
- **XenMobile 구성 서비스:** 이 서비스는 XenMobile과 통신하여 XenMobile 정책 변경 사항을 커넥터와 동기화합니다.
- **XenMobile 알림 서비스:** 이 서비스는 승인되지 않은 장치 액세스에 대한 알림을 XenMobile로 보냅니다. 이러한 방식으로 XenMobile은 장치가 차단된 이유를 사용자에게 알리는 등 적절한 조치를 취할 수 있습니다.
- **Exchange ActiveSync용 Citrix Gateway 커넥터 구성 유틸리티:** 이 애플리케이션을 통해 관리자는 커넥터를 구성하고 모니터링할 수 있습니다.

Exchange ActiveSync용 Citrix Gateway 커넥터의 수신 주소 설정

Exchange ActiveSync용 Citrix Gateway 커넥터가 ActiveSync 트래픽을 승인하기 위해 Citrix ADC로부터 요청을 수신하려면 다음을 수행하십시오. 커넥터가 Citrix ADC 웹 서비스 호출을 수신하는 포트를 지정하십시오.

1. **시작** 메뉴에서 Exchange ActiveSync 구성 유틸리티용 Citrix Gateway 커넥터를 선택합니다.
2. **웹 서비스** 탭을 클릭한 다음 커넥터 웹 서비스의 수신 주소를 입력합니다. **HTTP** 또는 **HTTPS** 또는 둘 다를 선택할 수 있습니다. 커넥터가 XenMobile과 함께 상주하는 경우(동일한 서버에 설치된 경우) XenMobile과 충돌하지 않는 포트 값을 선택합니다.
3. 값이 구성되면 **저장**을 클릭한 다음 **서비스 시작**을 클릭하여 웹 서비스를 시작합니다.

Exchange ActiveSync용 Citrix Gateway 커넥터에서 장치 액세스 제어 정책 구성

관리 장치에 적용할 액세스 제어 정책을 구성하려면 다음을 수행하십시오.

1. Exchange ActiveSync 구성 유틸리티용 Citrix Gateway 커넥터에서 **경로 필터** 탭을 클릭합니다.
2. 첫 번째 행인 **Microsoft-Server-ActiveSync는 ActiveSync용입니다**를 선택한 다음 **편집**을 클릭합니다.
3. **정책** 목록에서 원하는 정책을 선택합니다. XenMobile 정책을 포함하는 정책의 경우 **정적 + ZDM: 허용 모드 또는 정적 + ZDM: 차단 모드**를 선택합니다. 이러한 정책은 로컬(또는 정적) 규칙과 XenMobile의 규칙을 결합합니다. 허용 모드는 규칙에 의해 명시적으로 식별되지 않은 모든 장치가 ActiveSync에 액세스하도록 허용됨을 의미합니다. 차단 모드는 이러한 장치가 차단됨을 의미합니다.
4. 정책을 설정한 후 **저장**을 클릭합니다.

XenMobile과 통신을 구성하려면

Exchange ActiveSync용 Citrix Gateway 커넥터 및 Citrix ADC와 함께 사용할 XenMobile Server(Config Provider라고도 함)의 이름과 속성을 지정합니다.

> **참고:**
>
> 이 작업은 XenMobile을 이미 설치하고 구성했다고 가정합니다.

1. Exchange ActiveSync 구성 유틸리티용 Citrix Gateway 커넥터에서 **Config Providers** 탭을 클릭한 다음 **추가**를 클릭합니다.
2. 이 배포에서 사용 중인 XenMobile Server의 이름과 URL을 입력합니다. 다중 테넌트 배포에 여러 XenMobile Server가 배포된 경우 이 이름은 각 서버 인스턴스에 대해 고유해야 합니다. 예를 들어, **이름**에 **XMS**를 입력할 수 있습니다.
3. **Url**에 XenMobile GlobalConfig Provider(GCP)의 웹 주소를 입력합니다. 일반적으로 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 형식입니다. *MagConfigService* 이름은 대소문자를 구분합니다.
4. **암호**에 XenMobile 웹 서버와의 기본 HTTP 인증에 사용되는 암호를 입력합니다.
5. **관리 호스트**에 Exchange ActiveSync용 Citrix Gateway 커넥터를 설치한 서버 이름을 입력합니다.
6. **기준 간격**에 XenMobile에서 새로 고쳐진 동적 규칙 집합을 가져오는 기간을 지정합니다.
7. **요청 시간 초과**에 서버 요청 시간 초과 간격을 지정합니다.

8. **구성 공급자**에서 구성 공급자 서버 인스턴스가 정책 구성을 제공하는지 여부를 선택합니다.
9. **이벤트 사용**에서 Secure Mobile Gateway가 장치가 차단될 때 XenMobile에 알리도록 하려면 이 옵션을 활성화합니다. 이 옵션은 Device Manager 자동화된 작업에서 Secure Mobile Gateway 규칙을 사용하는 경우 필수입니다.
10. 서버를 구성한 후 **연결 테스트**를 클릭하여 XenMobile에 대한 연결을 테스트합니다.
11. 연결이 설정되면 **저장**을 클릭합니다.

이중화 및 확장성을 위한 Exchange ActiveSync용 Citrix Gateway 커넥터 배포

Exchange ActiveSync용 Citrix Gateway 커넥터 및 XenMobile 배포를 확장하려면 여러 Windows Server에 커넥터 인스턴스를 설치하고 모두 동일한 XenMobile 인스턴스를 가리키도록 한 다음 Citrix ADC를 사용하여 서버의 로드 밸런싱을 수행할 수 있습니다.

Exchange ActiveSync 구성용 Citrix Gateway 커넥터에는 두 가지 모드가 있습니다.

- 비공유 모드에서는 각 Exchange ActiveSync용 Citrix Gateway 커넥터 인스턴스가 XenMobile Server와 통신하고 결과 정책의 자체 비공개 복사본을 유지합니다. 예를 들어, XenMobile Server 클러스터가 있는 경우 각 XenMobile Server에서 커넥터 인스턴스를 실행할 수 있으며 커넥터는 로컬 XenMobile 인스턴스에서 정책을 가져옵니다.
- 공유 모드에서는 하나의 커넥터 노드가 기본 노드로 선택되어 XenMobile과 통신합니다. 결과 구성은 Windows 네트워크 공유 또는 Windows(또는 타사) 복제를 통해 다른 노드와 공유됩니다.

전체 커넥터 구성은 단일 폴더(몇 개의 XML 파일로 구성됨)에 있습니다. 커넥터 프로세스는 이 폴더의 파일 변경 사항을 감지하고 구성을 자동으로 다시 로드합니다. 공유 모드에서는 기본 노드에 대한 페일오버가 없습니다. 그러나 마지막으로 알려진 올바른 구성이 커넥터 프로세스에 캐시되어 있으므로 시스템은 기본 서버가 몇 분 동안 다운되어도(예: 다시 시작하기 위해) 견딜 수 있습니다.

고급 개념

참고:

이 문서에서는 XenMobile Server의 고급 개념을 다룹니다. Citrix Endpoint Management에 대한 고급 정보는 고급 개념을 참조하십시오.

XenMobile® 고급 개념 문서는 XenMobile 제품 설명서에 대한 심층적인 내용을 제공합니다. 목표는 전문가 기술을 통해 배포 시간을 단축하는 것입니다. 이 문서에는 콘텐츠를 작성한 기술 전문가가 인용될 수 있습니다.

종단 간 XenMobile 환경에 대한 결정 지점, 권장 사항, 일반적인 질문 및 사용 사례는 이 섹션의 XenMobile 배포 핸드북을 참조하십시오.

XenMobile에 대한 커뮤니티 지원 포럼은 Citrix Discussions를 참조하십시오.

온프레미스 XenMobile®과 Active Directory의 상호 작용

이 문서에서는 XenMobile Server와 Active Directory 간의 상호 작용에 대해 설명합니다. XenMobile Server는 인라인 및 백그라운드에서 Active Directory와 상호 작용합니다. 다음 섹션에서는 Active Directory 상호 작용과 관련된 인라인 및 백그라운드 작업에 대한 자세한 정보를 제공합니다.

참고:

이 문서는 상호 작용에 대한 개요이며 세부적인 내용은 다루지 않습니다. XenMobile 콘솔에서 Active Directory 및 LDAP 구성에 대한 자세한 내용은 도메인 또는 도메인과 보안 토큰 인증을 참조하십시오.

인라인 상호 작용

XenMobile Server는 관리자가 구성하는 LDAP 설정을 사용하여 Active Directory와 통신합니다. 이 설정은 사용자 및 그룹에 대한 정보를 검색합니다. 다음은 XenMobile Server와 Active Directory 간의 상호 작용을 유발하는 작업입니다.

1. **LDAP 구성.** Active Directory 자체를 구성하면 Active Directory와의 상호 작용이 발생합니다. XenMobile Server는 Active Directory를 통해 정보를 인증하여 정보를 검증하려고 시도합니다. 서버는 제공된 인터넷 프로토콜, 포트 및 서비스 계정 자격 증명을 사용하여 이 작업을 수행합니다. 바인딩에 성공하면 연결이 올바르게 구성되었음을 나타냅니다.
2. **그룹 기반 상호 작용.**

   a. 역할 기반 액세스 제어(RBAC) 및 전달 그룹 정의 생성 중에 하나 이상의 그룹을 검색합니다. XenMobile Server 관리자는 XenMobile 콘솔에 검색 텍스트 문자열을 입력합니다. XenMobile Server는 제공된 하위 문자열을 포함하는 모든 그룹에 대해 선택한 도메인을 검색합니다. 그런 다음 XenMobile Server는 검색에서 식별된 그룹의 objectGUID, sAMAccountName 및 Distinguished Name 속성을 검색합니다.

   > **참고:**
   >
   > 이 정보는 XenMobile Server 데이터베이스에 저장되지 않습니다.

   b. RBAC 및 배포 그룹 정의 추가 또는 업데이트. XenMobile Server 관리자는 이전 검색을 기반으로 관심 있는 Active Directory 그룹을 선택하고 배포 그룹 정의에 포함합니다. XenMobile Server는 Active Directory에서 특정 그룹을 한 번에 하나씩 검색합니다. XenMobile Server는 objectGUID 속성을 검색하고 멤버십 정보를 포함하여 선택된 속성을 검색합니다. 그룹 멤버십 정보는 검색된 그룹과 XenMobile Server 데이터베이스의 기존 사용자 또는 그룹 간의 멤버십을 결정하는 데 도움이 됩니다. 그룹 멤버십 변경은 영향을 받는 사용자 멤버에 대한 RBAC 및 배포 그룹 파생을 초래하며, 이는 사용자 권한으로 이어집니다.

   > **참고:**
   >
   > 배포 그룹 정의 변경은 영향을 받는 사용자의 앱 또는 정책 권한 변경으로 이어질 수 있습니다.

   c. **일회용 PIN(OTP) 초대.** XenMobile Server 관리자는 XenMobile Server 데이터베이스에 있는 Active Directory 그룹 목록에서 그룹을 선택합니다. 이 그룹의 경우, 직접 및 간접 사용자 모두 Active Directory에서 검색됩니다. OTP 초대는 이전 단계에서 식별된 사용자에게 전송됩니다.

   > **참고:**

> 앞의 세 가지 상호 작용은 XenMobile Server 구성 변경에 따라 그룹 기반 상호 작용이 트리거됨을 의미합니다. 구성 변경이 없는 경우, 상호 작용은 Active Directory와의 상호 작용이 없음을 의미합니다. 또한 주기적으로 변경 사항의 그룹 측면을 캡처하기 위한 백그라운드 작업이 필요하지 않음을 의미합니다.

3. **사용자 기반 상호 작용**

   a. **사용자 인증:** 사용자 인증 워크플로는 Active Directory와의 두 가지 상호 작용을 발생시킵니다.

      - 제공된 자격 증명으로 사용자를 인증하는 데 사용됩니다.
      - objectGUID, Distinguished Name, sAMAccountName 및 그룹에 대한 직접 멤버십을 포함하여 선택한 사용자 속성을 XenMobile Server 데이터베이스에 추가하거나 업데이트합니다. 그룹 멤버십 변경은 앱, 정책 및 액세스 권한의 재평가를 초래합니다.

      사용자는 장치 또는 XenMobile Server 콘솔에서 인증할 수 있습니다. 두 시나리오 모두에서 Active Directory와의 상호 작용은 동일한 동작을 따릅니다.

   b. **앱 스토어 액세스 및 새로 고침:** 스토어를 새로 고치면 직접 그룹 멤버십을 포함한 사용자 속성이 새로 고쳐집니다. 이 작업은 사용자 권한을 재평가할 수 있도록 합니다.

   c. **장치 체크인:** 관리자는 XenMobile 콘솔에서 주기적으로 장치 체크인을 구성할 수 있습니다. 장치가 체크인될 때마다 직접 그룹 멤버십을 포함한 해당 사용자 속성이 새로 고쳐집니다. 이러한 체크인은 사용자 권한을 재평가할 수 있도록 합니다.

   d. **그룹별 OTP 초대:** XenMobile Server 관리자는 XenMobile Server 데이터베이스에 있는 Active Directory 그룹 목록에서 그룹을 선택합니다. 직접 및 간접 사용자 멤버(중첩으로 인해)는 Active Directory에서 검색되어 XenMobile Server 데이터베이스에 저장됩니다. 이전 단계에서 식별된 사용자 멤버에게 OTP 초대가 전송됩니다.

   e. **사용자별 OTP 초대:** 관리자는 XenMobile 콘솔 내에서 검색 텍스트 문자열을 입력합니다. XenMobile Server는 Active Directory를 쿼리하고 입력 텍스트 문자열과 일치하는 사용자 레코드를 반환합니다. 그런 다음 관리자는 OTP 초대를 보낼 사용자를 선택합니다. XenMobile Server는 Active Directory에서 사용자 세부 정보를 검색하고 사용자에게 초대를 보내기 전에 데이터베이스에서 동일한 세부 정보를 업데이트합니다.

백그라운드 상호 작용

Active Directory와의 인라인 통신에서 얻은 한 가지 결론은 XenMobile Server 구성에 대한 선택된 변경 사항에 따라 그룹 기반 상호 작용이 트리거된다는 것입니다. 구성 변경이 없는 경우, 그룹에 대한 Active Directory와의 상호 작용이 없음을 의미합니다.

이 상호 작용에는 Active Directory와 주기적으로 동기화하고 관련 변경 사항을 해당 그룹에 업데이트하는 백그라운드 작업이 필요합니다.

다음은 Active Directory와 상호 작용하는 백그라운드 작업입니다.

1. **그룹 동기화 작업**. 이 작업의 목적은 Active Directory에서 관심 그룹을 한 번에 하나씩 쿼리하여 고유 이름 또는 sAMAccountName 특성 변경 사항을 확인하는 것입니다. Active Directory에 대한 검색 쿼리는 관심 그룹의 objectGUID를 사용하여 고유 이름 및 sAMAccountName 특성의 현재 값을 가져옵니다. 관심 그룹의 고유 이름 또는 sAMAccountName 값 변경 사항은 데이터베이스에 업데이트됩니다.

   > **참고:**
   >
   > 이 작업은 사용자-그룹 멤버십 정보를 업데이트하지 않습니다.

2. **중첩 그룹 동기화 작업**. 이 작업은 관심 그룹의 중첩 계층 구조 변경 사항을 업데이트합니다. XenMobile Server는 관심 그룹의 직접 및 간접 구성원 모두에게 권한을 부여합니다. 사용자의 직접 멤버십은 사용자 기반 인라인 상호 작용 중에 업데이트됩니다. 백그라운드에서 실행되는 이 작업은 간접 멤버십을 추적합니다. 간접 멤버십은 사용자가 관심 그룹의 구성원인 그룹의 구성원인 경우를 의미합니다.

   이 작업은 XenMobile Server 데이터베이스에서 Active Directory 그룹 목록을 수집합니다. 이 그룹은 배포 그룹 또는 RBAC 정의의 일부입니다. 이 목록의 각 그룹에 대해 XenMobile Server는 그룹의 구성원을 가져옵니다. 그룹의 구성원은 사용자 및 그룹을 모두 나타내는 고유 이름 목록입니다.

   XenMobile Server는 관심 그룹의 사용자 구성원만 가져오기 위해 Active Directory에 다시 쿼리합니다. 두 목록의 차이는 관심 그룹에 대한 그룹 구성원만 제공합니다. 구성원 그룹의 변경 사항은 데이터베이스에 업데이트됩니다. 동일한 프로세스가 계층 구조의 모든 그룹에 대해 반복됩니다.

   중첩 변경은 권한 변경에 대해 영향을 받는 사용자를 처리하는 결과를 가져옵니다.

3. **비활성화된 사용자 확인**. 이 작업은 XenMobile 관리자가 비활성화된 사용자를 확인하는 작업을 생성할 때만 실행됩니다. 이 작업은 그룹 동기화 작업 범위 내에서 실행됩니다. 이 작업은 Active Directory를 쿼리하여 관심 있는 사용자의 비활성화 상태를 한 번에 한 사용자씩 확인합니다.

FAQ

백그라운드 작업은 기본적으로 얼마나 자주 실행됩니까?

- 그룹 동기화 작업은 현지 시간 02:00부터 5시간마다 실행됩니다.
- 중첩 그룹 동기화 작업은 현지 시간 자정에 하루에 한 번 실행됩니다.

그룹 동기화 작업이 필요한 이유는 무엇입니까?

- Active Directory의 사용자 레코드에 있는 **memberOf** 특성은 사용자가 직접 구성원인 그룹 목록을 제공합니다. 그룹이 한 OU에서 다른 OU로 이동하면 **memberOf** 특성은 고유 이름의 최신 값을 반영합니다. XenMobile Server 데이터베이스에도 마지막으로 새로 고쳐진 값이 있습니다. 그룹의 고유 이름 불일치는 사용자가 배포 그룹에 대한 액세스 권한을 잃게 만들 수 있습니다. 사용자는 해당 배포 그룹과 연결된 앱 및 정책도 잃을 수 있습니다.
- 백그라운드 작업은 XenMobile Server 데이터베이스에서 그룹 고유 이름 특성을 최신 상태로 유지하여 사용자가 자신의 권한에 액세스할 수 있도록 합니다.
- Active Directory 내의 그룹 변경이 흔하지 않다고 가정하므로 동기화 작업은 5시간마다 예약됩니다.

그룹 동기화 작업을 끌 수 있습니까?

- 관심 그룹이 한 OU에서 다른 OU로 변경되지 않는다는 것을 아는 경우 작업을 끌 수 있습니다.

중첩 그룹 처리 백그라운드 작업이 필요한 이유는 무엇입니까?

- Active Directory에서 그룹 중첩 변경은 매일 발생하는 일이 아닙니다. 관심 그룹의 중첩 계층 변경은 영향을 받는 사용자의 권한 변경으로 이어집니다. 그룹이 계층에 추가되면 해당 구성원 사용자는 각 역할에 대한 권한을 갖게 됩니다. 그룹이 중첩에서 벗어나면 해당 그룹의 구성원 사용자는 역할 기반 권한에 대한 액세스를 잃을 수 있습니다.
- 중첩 변경은 사용자 새로 고침 중에 캡처되지 않습니다. 중첩 변경은 온디맨드로 처리될 수 없으므로 백그라운드 작업을 통해 캡처됩니다.
- 중첩 변경은 흔하지 않다고 가정하므로 백그라운드 작업은 변경 사항을 확인하기 위해 하루에 한 번 실행됩니다.

중첩 그룹 처리 작업을 끌 수 있습니까?

- 관심 그룹에 중첩 변경이 발생하지 않는다는 것을 아는 경우 작업을 끌 수 있습니다.

XenMobile® 배포

XenMobile 배포를 계획할 때 고려해야 할 사항이 많습니다.

- 어떤 장치를 선택해야 합니까?
- 장치를 어떻게 관리해야 합니까?
- 뛰어난 사용자 경험을 제공하면서 네트워크를 안전하게 유지하려면 어떻게 해야 합니까?
- 어떤 하드웨어가 필요하며, 어떻게 문제를 해결해야 합니까?

이 섹션의 문서들은 이러한 질문에 답하는 데 도움이 되는 것을 목표로 합니다. 배포 관련 우려 사항을 다루는 주제에 대한 사용 사례 및 권장 사항이 포함되어 있습니다.

지침이나 권장 사항이 모든 환경이나 사용 사례에 적용되지 않을 수 있다는 점을 명심하십시오. XenMobile 배포를 시작하기 전에 테스트 환경을 설정해야 합니다.

이 섹션의 문서들은 다음 영역을 다룹니다.

- **평가:** 배포를 계획할 때 고려해야 할 일반적인 사용 사례 및 질문.
- **설계 및 구성:** 환경 설계 및 구성에 대한 권장 사항
- **운영 및 모니터링:** 실행 중인 환경의 원활한 운영을 보장합니다.

평가

모든 배포와 마찬가지로, 요구 사항을 평가하는 것이 최우선입니다. XenMobile의 주요 요구 사항은 무엇입니까? 환경의 모든 장치를 관리해야 합니까, 아니면 앱만 관리해야 합니까? 둘 다 관리해야 할 수도 있습니다. XenMobile 환경이 얼마나 안전해야 합니까? 배포를 계획할 때 고려해야 할 일반적인 사용 사례 및 질문을 살펴보겠습니다.

- 관리 모드
- 장치 요구 사항
- 보안 및 사용자 경험
- 앱
- 사용자 커뮤니티
- 이메일 전략
- XenMobile 통합
- 다중 사이트 요구 사항

설계 및 구성

배포 요구 사항 평가를 마치면 환경의 설계 및 구성을 결정할 수 있습니다. 계획해야 할 몇 가지 사항은 다음과 같습니다:

- 서버용 하드웨어 선택
- 앱 및 장치에 대한 정책 설정
- 사용자 등록

이 섹션에는 이러한 각 시나리오 및 기타 시나리오에 대한 사용 사례와 권장 사항이 포함되어 있습니다.

- Citrix ADC 및 Citrix Gateway와 통합
- MDX 앱을 위한 SSO 및 프록시 고려 사항

- 인증
- 온프레미스 배포를 위한 참조 아키텍처
- 서버 속성
- 장치 및 앱 정책
- 사용자 등록 옵션
- XenMobile 작업 튜닝

운영 및 모니터링

XenMobile 환경이 실행되면 원활한 작동을 위해 모니터링해야 합니다. 모니터링 섹션에서는 다음 내용을 다룹니다.

- XenMobile 및 해당 구성 요소가 생성하는 다양한 로그 및 메시지를 찾을 수 있는 위치
- 해당 로그를 읽는 방법

이 섹션에는 고객 지원 피드백 시간을 줄이기 위해 따를 수 있는 다양한 일반적인 문제 해결 단계도 포함되어 있습니다.

- 앱 프로비저닝 및 프로비저닝 해제
- 대시보드 기반 작업
- 역할 기반 액세스 제어 및 XenMobile 지원
- 시스템 모니터링
- 재해 복구
- Citrix 지원 프로세스

관리 모드

각 XenMobile® 인스턴스(단일 서버 또는 노드 클러스터)에 대해 장치, 앱 또는 둘 다를 관리할지 선택할 수 있습니다. XenMobile은 장치 및 앱 관리 모드에 대해 다음 용어를 사용합니다:

- 모바일 장치 관리 모드 (MDM 모드)
- 모바일 앱 관리 모드 (MAM 모드)
- MDM+MAM 모드 (엔터프라이즈 모드)

모바일 장치 관리 (MDM 모드)

> **중요:**

> MDM 모드를 구성한 후 나중에 ENT 모드로 변경하는 경우, 동일한 (Active Directory) 인증을 사용해야 합니다. XenMobile은 사용자 등록 후 인증 모드 변경을 지원하지 않습니다. 자세한 내용은 업그레이드를 참조하십시오.

> MDM을 사용하면 모바일 장치를 구성하고, 보호하며, 지원할 수 있습니다. MDM을 통해 시스템 수준에서 장치 및 장치 데이터를 보호할 수 있습니다. 정책, 작업 및 보안 기능을 구성할 수 있습니다. 예를 들어, 장치를 분실하거나 도난당했거나 규정을 준수하지 않는 경우 장치를 선택적으로 초기화할 수 있습니다. MDM 모드에서는 앱 관리를 사용할 수 없지만, 이 모드에서 공용 앱 스토어 및 엔터프라이즈 앱과 같은 모바일 앱을 제공할 수 있습니다. 다음은 MDM 모드의 일반적인 사용 사례입니다:

- MDM은 전체 초기화, 선택적 초기화 또는 지리적 위치와 같은 장치 수준 관리 정책 또는 제한이 필요한 기업 소유 장치에 대한 고려 사항입니다.
- 고객이 실제 장치 관리를 필요로 하지만, 앱 컨테이너화, 앱 데이터 공유 제어 또는 마이크로 VPN과 같은 MDX 정책을 필요로 하지 않는 경우.
- 사용자가 모바일 장치의 기본 이메일 클라이언트로 이메일을 수신하기만 하면 되고, Exchange ActiveSync 또는 클라이언트 액세스 서버가 이미 외부에서 액세스 가능한 경우. 이 사용 사례에서는 MDM을 사용하여 이메일 전송을 구성할 수 있습니다.
- 기본 엔터프라이즈 앱(비 MDX), 공용 앱 스토어 앱 또는 공용 스토어에서 제공되는 MDX 앱을 배포할 때 . MDM 솔루션만으로는 장치 내 앱 간의 기밀 정보 데이터 유출을 방지하지 못할 수 있다는 점을 고려하십시오. Office 365 앱에서 복사 및 붙여넣기 또는 다른 이름으로 저장 작업 시 데이터 유출이 발생할 수 있습니다.

모바일 앱 관리 (MAM 모드)

MAM은 앱 데이터를 보호하고 앱 데이터 공유를 제어할 수 있도록 합니다. 또한 MAM은 개인 데이터와 별도로 기업 데이터 및 리소스를 관리할 수 있도록 합니다. MAM 모드로 구성된 XenMobile을 사용하면 MDX 지원 모바일 앱을 사용하여 앱별 컨테이너화 및 제어를 제공할 수 있습니다. MAM 모드라는 용어는 MAM 전용 모드라고도 불립니다. 이 용어는 이 모드를 레거시 MAM 모드와 구별합니다.

MDX 정책을 사용하여 XenMobile은 네트워크 액세스(예: 마이크로 VPN), 앱 및 장치 상호 작용, 데이터 암호화 및 앱 액세스에 대한 앱 수준 제어를 제공합니다.

MAM은 장치가 관리되지 않더라도 회사 데이터가 보호되기 때문에 BYO(Bring-Your-Own) 장치에 적합한 경우가 많습니다. MDX에는 MDM 제어가 필요 없는 MAM 전용 정책이 많이 있습니다.

MAM은 또한 모바일 생산성 앱을 지원합니다. 이 지원에는 Citrix Secure Mail로의 보안 이메일 전송, 보안 모바일 생산성 앱 간의 데이터 공유, Citrix Files의 보안 데이터 저장이 포함됩니다. 자세한 내용은 모바일 생산성 앱을 참조하십시오.

MAM은 다음 예시에 적합한 경우가 많습니다.

- 앱 수준에서 관리되는 MDX 앱과 같은 모바일 앱을 제공합니다.
- 시스템 수준에서 장치를 관리할 필요가 없습니다.

MDM+MAM (엔터프라이즈 모드)

MDM+MAM은 하이브리드 모드로, 엔터프라이즈 모드라고도 불리며, XenMobile EMM(Enterprise Mobility Management) 솔루션에서 사용 가능한 모든 기능 세트를 활성화합니다. XenMobile을 MDM+MAM 모드로 구성하면 MDM 및 MAM 기능이 모두 활성화됩니다.

XenMobile을 사용하면 사용자가 장치 관리에서 제외할지 또는 장치 관리가 필요한지 여부를 지정할 수 있습니다. 이러한 유연성은 다양한 사용 사례가 혼합된 환경에 유용합니다. 이러한 환경에서는 MAM 리소스에 액세스하기 위해 MDM 정책을 통한 장치 관리가 필요할 수도 있고 필요하지 않을 수도 있습니다.

MDM+MAM은 다음 예시에 적합합니다.

- MDM과 MAM이 모두 필요한 단일 사용 사례가 있습니다. MAM 리소스에 액세스하려면 MDM이 필요합니다.
- 일부 사용 사례는 MDM을 필요로 하지만 일부는 그렇지 않습니다.
- 일부 사용 사례는 MAM을 필요로 하지만 일부는 그렇지 않습니다.

서버 모드 속성을 통해 XenMobile Server의 관리 모드를 지정합니다. 이 설정은 XenMobile 콘솔에서 구성합니다. 모드는 MDM, MAM 또는 ENT(MDM+MAM의 경우)가 될 수 있습니다.

라이선스를 보유한 XenMobile 에디션에 따라 다음 표에 표시된 것처럼 사용 가능한 관리 모드 및 기타 기능이 결정됩니다.

XenMobile MDM 에디션	**XenMobile Advanced 에디션**
MDM 기능	MDM 기능
-	MAM 기능
-	MAM SDK
시큐어 허브	시큐어 허브
-	시큐어 메일
-	시큐어 웹

관리 모드 및 등록 프로필

관리 모드와 등록 프로필은 함께 작동합니다. 등록 프로필을 사용하여 Android 및 iOS 장치에 대한 장치 관리 및 앱 관리 등록 옵션을 구성합니다. Android의 경우 MDM+MAM 서버 모드에 사용할 수 있는 등록 옵션은 MDM 모드 옵션과 다릅니다. 자세한 내용은 등록 프로필을 참조하십시오.

장치 관리 및 MDM 등록

XenMobile Enterprise 환경에는 다양한 사용 사례가 포함될 수 있으며, 그 중 일부는 MAM 리소스에 대한 액세스를 허용하기 위해 MDM 정책을 통한 장치 관리가 필요합니다. 사용자에게 모바일 생산성 앱을 배포하기 전에 사용 사례를 완전히 평가하고 MDM 등록을 요구할지 여부를 결정하십시오. 나중에 MDM 등록 요구 사항을 변경하기로 결정하면 사용자가 장치를 다시 등록해야 할 수 있습니다.

> **참고:**

> 사용자에게 MDM 등록을 요구할지 여부를 지정하려면 XenMobile 콘솔(**설정 > 서버 속성**)에서 XenMobile Server 속성 **등록 필요**를 사용하십시오. 이 전역 서버 속성은 XenMobile 인스턴스의 모든 사용자 및 장치에 적용됩니다. 이 속성은 XenMobile Server 모드가 ENT일 때만 적용됩니다.

> 다음은 XenMobile Enterprise 모드 배포에서 MDM 등록을 요구할 때의 장점과 단점(완화책 포함)을 요약한 것입니다.

MDM 등록이 선택 사항인 경우

장점:

- 사용자는 장치를 MDM 관리하에 두지 않고도 MAM 리소스에 액세스할 수 있습니다. 이 옵션은 사용자 채택을 늘릴 수 있습니다.
- 엔터프라이즈 데이터를 보호하기 위해 MAM 리소스에 대한 액세스를 보호할 수 있습니다.
- **앱 암호**와 같은 MDX 정책은 각 MDX 앱에 대한 앱 액세스를 제어할 수 있습니다.
- Citrix ADC, XenMobile Server 및 애플리케이션별 시간 초과를 Citrix PIN과 함께 구성하면 추가적인 보호 계층이 제공됩니다.
- MDM 작업이 장치에 적용되지 않더라도 일부 MDX 정책은 MAM 액세스를 거부하는 데 사용할 수 있습니다. 거부는 탈옥 또는 루팅된 장치와 같은 시스템 설정에 기반합니다.
- 사용자는 처음 사용할 때 MDM에 장치를 등록할지 여부를 선택할 수 있습니다.

단점:

- MDM에 등록되지 않은 장치에서도 MAM 리소스를 사용할 수 있습니다.

- MDM 정책 및 작업은 MDM에 등록된 장치에서만 사용할 수 있습니다.

완화 옵션:

- 사용자가 규정을 준수하지 않기로 선택할 경우 책임을 지도록 회사 약관에 동의하게 합니다. 관리자는 관리되지 않는 장치를 모니터링해야 합니다.
- 애플리케이션 타이머를 사용하여 애플리케이션 액세스 및 보안을 관리합니다. 시간 초과 값을 줄이면 보안이 강화되지만 사용자 경험에 영향을 미칠 수 있습니다.
- MDM 등록이 필요한 두 번째 XenMobile 환경을 사용하는 것도 한 가지 옵션입니다. 이 옵션을 고려할 때 두 환경을 관리하는 데 필요한 추가 오버헤드와 추가 리소스를 염두에 두십시오.

MDM 등록이 필요한 경우

장점:

- MAM 리소스에 대한 액세스를 MDM 관리 장치로만 제한할 수 있습니다.
- MDM 정책 및 작업은 원하는 대로 환경의 모든 장치에 적용할 수 있습니다.
- 사용자는 장치 등록을 거부할 수 없습니다.

단점:

- 모든 사용자가 MDM에 등록해야 합니다.
- 개인 장치에 대한 회사 관리에 반대하는 사용자의 채택률이 감소할 수 있습니다.

완화 옵션:

- 사용자에게 XenMobile이 장치에서 실제로 무엇을 관리하는지, 그리고 관리자가 어떤 정보에 액세스할 수 있는지 교육합니다.
- MDM 관리가 필요 없는 장치의 경우, MAM 서버 모드(MAM 전용 모드라고도 함)를 사용하는 두 번째 XenMobile 환경을 사용할 수 있습니다. 이 옵션을 고려할 때, 두 환경을 관리하는 데 드는 추가 오버헤드와 필요한 추가 리소스를 염두에 두십시오.

MAM 및 레거시 MAM 모드 정보

XenMobile 10.3.5에서는 새로운 MAM 전용 서버 모드를 도입했습니다. 이전 MAM 모드와 새로운 MAM 모드를 구분하기 위해 설명서에서는 이러한 용어를 사용합니다. 새로운 모드는 MAM 전용 또는 MA라고 하며, 이전 MAM 모드는 레거시 MAM 모드라고 합니다.

XenMobile의 **서버 모드** 속성이 MAM일 때 MAM 전용 모드가 적용됩니다. 장치는 MAM 모드로 등록됩니다.

XenMobile의 **서버 모드** 속성이 ENT이고 사용자가 장치 관리를 거부하도록 선택한 경우 레거시 MAM 기능이 적용됩니다. 이 경우 장치는 MAM 모드로 등록됩니다. MDM 관리를 거부한 사용자는 레거시 MAM 기능을 계속 받습니다.

> **참고:**
>
> 이전에는 서버 모드 속성을 MAM으로 설정하는 것이 ENT로 설정하는 것과 동일한 효과를 가졌습니다. 즉, MDM 관리를 거부한 사용자는 레거시 MAM 기능을 받았습니다.

다음 표는 특정 라이선스 유형 및 원하는 장치 모드에 사용할 **서버 모드** 설정을 요약한 것입니다.

라이선스가 적용되는 에디션	이 모드로 장치를 등록하려는 경우	서버 모드 속성을 다음으로 설정
Enterprise/ Advanced/MDM	MDM 모드	MDM
엔터프라이즈/고급	MAM 모드(MAM 전용 모드라고도 함)	MAM
엔터프라이즈/고급	MDM+MAM 모드	ENT (장치 관리에서 제외된 사용자는 레거시 MAM 모드에서 작동합니다.)

MAM 전용 모드는 이전에 ENT에서만 사용할 수 있었던 다음 기능을 지원합니다.

- **인증서 기반 인증:** MAM 전용 모드는 인증서 기반 인증을 지원합니다. 사용자는 Active Directory 암호가 만료되어도 앱에 계속 액세스할 수 있습니다. MAM 장치에 인증서 기반 인증을 사용하는 경우 Citrix Gateway를 구성해야 합니다. 기본적으로 **XenMobile 설정 > Citrix Gateway**에서 인증을 위한 사용자 인증서 전달은 **끔**으로 설정되어 있으며, 이는 사용자 이름 및 암호 인증이 사용됨을 의미합니다. 인증서 인증을 사용하도록 설정하려면 해당 설정을 **켬**으로 변경합니다.
- **셀프 도움말 포털:** 사용자가 직접 앱 잠금 및 앱 초기화를 수행할 수 있도록 합니다. 이러한 작업은 장치의 모든 앱에 적용됩니다. **구성 > 작업**에서 앱 잠금 및 앱 초기화 작업을 구성할 수 있습니다.
- **모든 등록 보안 모드:** 높은 보안, 초대 URL 및 2단계 인증을 포함하며, **관리 > 등록 초대**를 통해 구성됩니다.
- **Android 및 iOS 장치에 대한 장치 등록 제한:** 서버 속성 **사용자당 장치 수**가 **구성 > 등록 프로필**로 이동했으며 이제 모든 서버 모드에 적용됩니다.

- **MAM 전용 API:** MAM 전용 장치의 경우 모든 REST 클라이언트와 XenMobile REST API를 사용하여 XenMobile 콘솔이 노출하는 서비스를 호출할 수 있습니다.
- MAM 전용 API를 사용하면 다음을 수행할 수 있습니다.
  - 초대 URL 및 일회용 PIN을 보냅니다.
  - 장치에서 앱 잠금 및 초기화를 실행합니다.

다음 표는 레거시 MAM과 MAM 전용 기능 간의 차이점을 요약합니다.

등록 시나리오 및 기타 기능	레거시 MAM (서버 모드는 ENT)	MAM 전용 모드 (서버 모드는 MAM)
인증서 인증	지원되지 않습니다.	지원됩니다. 인증서 인증에는 Citrix Gateway가 필요합니다.
배포 요구 사항	XenMobile Server는 장치에서 직접 액세스할 필요가 없습니다.	XenMobile Server는 장치에서 직접 액세스할 필요가 없습니다.
등록 옵션	Citrix Gateway FQDN을 사용하거나, MDM FQDN을 사용하는 경우 등록하지 않도록 선택합니다.	XenMobile Server FQDN을 사용합니다.
등록 방법*	사용자 이름 + 암호	사용자 이름 + 암호, 높은 보안, 초대 URL, 초대 URL+PIN, 초대 URL + 암호, 2단계 인증, 사용자 이름 + PIN
앱 잠금 및 초기화	지원됨.	지원됨.
앱 잠금 및 초기화를 위한 셀프 서비스 포털 옵션	지원되지 않음.	지원됨.
앱 초기화 동작	앱은 장치에 남아 있지만 사용할 수 없습니다. XenMobile은 클라이언트에서만 계정을 삭제합니다.	앱은 장치에 남아 있지만 사용할 수 없습니다. XenMobile은 클라이언트에서만 계정을 삭제합니다.
MAM 전용 사용자를 위한 자동화된 작업.	이벤트, 장치 속성, 사용자 속성 작업이 지원됩니다. 설치된 앱 기반 자동화된 작업은 지원하지 않습니다.	이벤트, 장치 속성, 사용자 속성 및 일부 앱 기반 작업(앱 초기화 및 앱 잠금 포함)을 지원합니다.

Active Directory 사용자가 삭제될 때의 내장 작업	앱 초기화를 지원합니다.	앱 초기화를 지원합니다.
등록 제한	지원됨; 등록 프로필을 통해 구성됩니다.	지원됨; 등록 프로필을 통해 구성됩니다.
소프트웨어 인벤토리	지원됩니다. XenMobile은 장치에 설치된 앱을 나열합니다.	지원되지 않습니다.

*__알림 관련:__ SMTP는 등록 초대장을 보내는 유일하게 지원되는 방법입니다.

> **중요:**
>
> MAM 전용 모드의 경우, 이전에 등록된 사용자는 장치를 다시 등록해야 합니다. 사용자에게 등록에 필요한 XenMobile Server FQDN을 제공해야 합니다. MAM 전용 모드에서는 ENT 모드와 마찬가지로 장치가 XenMobile Server FQDN을 사용하여 등록됩니다. (레거시 MAM 모드에서는 장치가 Citrix Gateway FQDN을 사용하여 등록됩니다.)

장치 요구 사항

모든 배포에서 고려해야 할 중요한 사항은 배포하려는 장치입니다. iOS, Android 및 Windows 플랫폼에는 다양한 옵션이 있습니다. XenMobile이 지원하는 장치 목록은 지원되는 장치 플랫폼을 참조하십시오.

BYOD(Bring Your Own Device) 환경에서는 지원되는 플랫폼이 혼합될 수 있습니다. 그러나 사용자가 등록할 수 있는 장치에 대해 알릴 때는 지원되는 장치 플랫폼 문서의 제한 사항을 고려하십시오. 환경에서 한두 개의 장치만 허용하더라도 XenMobile®은 iOS, Android 및 Windows 장치에서 약간 다르게 작동합니다. 각 플랫폼에서 다른 기능 세트를 사용할 수 있습니다.

또한 모든 앱 디자인이 태블릿과 휴대폰 폼 팩터를 모두 대상으로 하는 것은 아닙니다. 광범위한 변경을 하기 전에 앱을 테스트하여 배포하려는 장치 화면에 맞는지 확인하십시오.

등록 요인도 고려할 수 있습니다. Apple과 Google은 기업 등록 프로그램을 제공합니다. Apple 배포 프로그램 및 Google Android Enterprise를 통해 사전 구성되어 직원이 바로 사용할 수 있는 장치를 구매할 수 있습니다.

등록에 대한 자세한 내용은 사용자 등록 옵션을 참조하십시오.

보안 및 사용자 경험

보안은 모든 조직에 중요하지만, 보안과 사용자 경험 사이의 균형을 이루어야 합니다. 예를 들어, 사용자가 사용하기 어려운 고도로 보안된 환경을 가질 수 있습니다. 또는 액세스 제어가 엄격하지 않을 정도로 사용자 친화적인 환경일 수도 있습니다. 이 가상 핸드북의 다른 섹션에서는 보안 기능을 자세히 다룹니다. 이 문서의 목적은 일반적인 보안 문제와 XenMobile에서 사용할 수 있는 보안 옵션에 대한 일반적인 개요를 제공하는 것입니다.

각 사용 사례에 대해 염두에 두어야 할 몇 가지 주요 고려 사항은 다음과 같습니다.

- 특정 앱, 전체 장치 또는 둘 다를 보호하고 싶습니까?
- 사용자가 자신의 신원을 어떻게 인증하기를 원하십니까? LDAP, 인증서 기반 인증 또는 이 둘의 조합을 사용할 계획입니까?
- 사용자 세션 시간 초과를 어떻게 처리하시겠습니까? 백그라운드 서비스, Citrix ADC 및 오프라인 상태에서 앱에 액세스할 수 있는 경우에 대한 시간 초과 값은 다르다는 점을 명심하십시오.
- 사용자가 장치 수준 암호, 앱 수준 암호 또는 둘 다를 설정하도록 하시겠습니까? 사용자에게 몇 번의 로그온 시도를 허용하시겠습니까? MAM으로 구현된 추가 앱별 인증 요구 사항이 사용자 경험에 어떤 영향을 미칠 수 있는지 염두에 두십시오.
- 사용자에게 어떤 다른 제한을 두시겠습니까? 사용자가 Siri와 같은 클라우드 서비스에 액세스하도록 하시겠습니까? 제공하는 각 앱으로 무엇을 할 수 있고 무엇을 할 수 없습니까? 사무실 공간 내에서 휴대폰 데이터 요금제 사용을 방지하기 위해 기업 Wi-Fi 정책을 배포하시겠습니까?

앱 대 장치

가장 먼저 고려해야 할 사항 중 하나는 모바일 앱 관리(MAM)를 사용하여 특정 앱만 보호할 것인지 여부입니다. 또는 모바일 장치 관리(MDM)를 사용하여 전체 장치도 관리할 것인지 여부입니다. 일반적으로 장치 수준 제어가 필요하지 않은 경우, 특히 조직이 BYOD(Bring Your Own Device)를 지원하는 경우 모바일 앱만 관리합니다.

XenMobile이 관리하지 않는 장치를 가진 사용자는 앱 스토어를 통해 앱을 설치할 수 있습니다. 선택적 또는 전체 초기화와 같은 장치 수준 제어 대신 앱 정책을 통해 앱에 대한 액세스를 제어합니다. 설정한 값에 따라 정책은 앱이 계속 실행될 수 있는지 확인하기 위해 장치가 XenMobile을 정기적으로 확인하도록 요구합니다.

MDM을 사용하면 장치의 모든 소프트웨어 재고를 파악하는 기능을 포함하여 전체 장치를 보호할 수 있습니다. 장치가 탈옥되었거나, 루팅되었거나, 안전하지 않은 소프트웨어가 설치된 경우 등록을 방지할 수 있습니다. 그러나 이러한 수준의 제어를 적용하면 사용자가 개인 장치에 대한 많은 권한을 허용하는 것을 꺼려 등록률이 감소할 수 있습니다.

인증

인증은 사용자 경험의 많은 부분이 발생하는 곳입니다. 조직이 이미 Active Directory를 실행하고 있다면 Active Directory를 사용하는 것이 사용자가 시스템에 액세스하는 가장 간단한 방법입니다.

인증 사용자 경험의 또 다른 중요한 부분은 시간 초과입니다. 높은 보안 환경에서는 사용자가 시스템에 액세스할 때마다 로그온하도록 할 수 있지만, 이 옵션이 모든 조직에 이상적인 것은 아닙니다. 예를 들어, 사용자가 이메일에 액세스할 때마다 자격 증명을 입력하도록 하면 사용자 경험에 상당한 영향을 미칠 수 있습니다.

사용자 엔트로피

보안 강화를 위해 *사용자 엔트로피*라는 기능을 활성화할 수 있습니다. Citrix Secure Hub™ 및 일부 다른 앱은 모든 기능이 제대로 작동하도록 암호, PIN, 인증서와 같은 공통 데이터를 공유하는 경우가 많습니다. 이 정보는 Secure Hub 내의 일반 볼트에 저장됩니다. **비밀 암호화** 옵션을 통해 사용자 엔트로피를 활성화하면 XenMobile은 UserEntropy라는 새 볼트를 생성합니다. XenMobile은 일반 볼트의 정보를 새 볼트로 이동합니다. Secure Hub 또는 다른 앱이 데이터에 액세스하려면 사용자가 암호 또는 PIN을 입력해야 합니다.

사용자 엔트로피를 활성화하면 여러 곳에 추가 인증 계층이 추가됩니다. 결과적으로 앱이 UserEntropy 볼트에 있는 인증서를 포함한 공유 데이터에 액세스해야 할 때마다 사용자는 암호 또는 PIN을 입력해야 합니다.

XenMobile 설명서에서 MDX Toolkit 정보를 읽고 사용자 엔트로피에 대해 자세히 알아볼 수 있습니다. 사용자 엔트로피를 켜려면 클라이언트 속성에서 관련 설정을 찾을 수 있습니다.

정책

MDX 및 MDM 정책은 조직에 많은 유연성을 제공하지만 사용자를 제한할 수도 있습니다. 예를 들어, Siri 또는 iCloud와 같이 민감한 데이터를 다양한 위치로 보낼 수 있는 클라우드 애플리케이션에 대한 액세스를 차단할 수 있습니다. 이러한 서비스에 대한 액세스를 차단하는 정책을 설정할 수 있지만, 그러한 정책이 의도하지 않은 결과를 초래할 수 있다는 점을 명심하십시오. iOS 키보드 마이크도 클라우드 액세스에 의존하므로 해당 기능에 대한 액세스도 차단할 수 있습니다.

앱

EMM(Enterprise Mobility Management)은 MDM(Mobile Device Management)과 MAM(Mobile Application Management)으로 나뉩니다. MDM은 조직이 모바일 장치를 보호하고 제어할 수 있도록 하는 반면, MAM은 애플리케이션 배포 및 관리를 용이하게 합니다. BYOD 채택이 증가함에 따라 일반적으로 MAM 솔루션을 구현하여 애플리케이션 배포, 소프트웨어 라이선싱, 구성 및 애플리케이션 수명 주기 관리를 지원할 수 있습니다.

XenMobile을 사용하면 특정 MAM 정책 및 VPN 설정을 구성하여 데이터 유출 및 기타 보안 위협을 방지함으로써 이러한 앱을 더욱 안전하게 보호할 수 있습니다. XenMobile은 조직에 다음 솔루션 중 하나를 배포할 수 있는 유연성을 제공합니다.

- MAM 전용 환경
- MDM 전용 환경
- 동일한 플랫폼에서 MDM 및 MAM 기능을 모두 제공하는 통합 XenMobile Enterprise 환경

모바일 장치에 앱을 배포하는 기능 외에도 XenMobile은 MDX 기술을 통해 앱 컨테이너화를 제공합니다. MDX는 플랫폼에서 제공하는 장치 수준 암호화와는 별개인 암호화를 통해 앱을 보호합니다. 앱을 초기화하거나 잠글 수 있으며, 앱은 세분화된 정책 기반 제어를 받습니다. 독립 소프트웨어 공급업체(ISV)는 모바일 앱 SDK를 사용하여 이러한 제어를 적용할 수 있습니다.

기업 환경에서 사용자는 업무 역할을 지원하기 위해 다양한 모바일 앱을 사용합니다. 앱에는 공개 앱 스토어의 앱, 자체 개발 앱 및 기본 앱이 포함될 수 있습니다. XenMobile은 이러한 앱을 다음과 같이 분류합니다.

공개 앱: 이러한 앱에는 Apple App Store 또는 Google Play와 같은 공개 앱 스토어에서 사용할 수 있는 무료 또는 유료 앱이 포함됩니다. 조직 외부의 공급업체는 종종 공개 앱 스토어에서 앱을 제공합니다. 이 옵션을 통해 고객은 인터넷에서 직접 앱을 다운로드할 수 있습니다. 사용자의 필요에 따라 조직에서 수많은 공개 앱을 사용할 수 있습니다. 이러한 앱의 예로는 GoToMeeting, Salesforce 및 EpicCare 앱이 있습니다.

Citrix는 공용 앱 스토어에서 앱 바이너리를 직접 다운로드한 다음, 엔터프라이즈 배포를 위해 MDX Toolkit으로 래핑하는 것을 지원하지 않습니다. 타사 애플리케이션을 MDX 지원하려면 앱 공급업체에 문의하여 앱 바이너리를 얻으십시오. MDX Toolkit을 사용하여 바이너리를 래핑하거나 MAM SDK를 바이너리와 통합할 수 있습니다.

사내 앱: 많은 조직에는 특정 기능을 제공하고 조직 내에서 독립적으로 개발 및 배포되는 앱을 만드는 사내 개발자가 있습니다. 특정 경우에 일부 조직에는 ISV가 제공하는 앱도 있을 수 있습니다. 이러한 앱을 기본 앱으로 배포하거나 XenMobile과 같은 MAM 솔루션을 사용하여 앱을 컨테이너화할 수 있습니다. 예를 들어, 의료 기관은 의사가 모바일 장치에서 환자 정보를 볼 수 있도록 하는 사내 앱을 만들 수 있습니다. 그러면 조직은 환자 정보를 보호하고 백엔드 환자 데이터베이스 서버에 대한 VPN 액세스를 활성화하기 위해 앱을 MAM SDK 지원하거나 MDM 래핑할 수 있습니다.

웹 및 SaaS 앱: 이러한 앱에는 내부 네트워크(웹 앱) 또는 공용 네트워크(SaaS)를 통해 액세스하는 앱이 포함됩니다. XenMobile을 사용하면 앱 커넥터 목록을 사용하여 사용자 지정 웹 및 SaaS 앱을 만들 수도 있습니다. 이러한 앱 커넥터는 기존 웹 앱에 대한 단일 Sign-On(SSO)을 용이하게 할 수 있습니다. 자세한 내용은 앱 커넥터 유형을 참조하십시오. 예를 들어, Google Apps에 대한 Security Assertion Markup Language(SAML) 기반 SSO에 Google Apps SAML을 사용할 수 있습니다.

모바일 생산성 앱: XenMobile 라이선스에 포함된 Citrix 개발 앱입니다. 자세한 내용은 모바일 생산성 앱 정보를 참조하십시오. Citrix는 또한 ISV가 Mobile Apps SDK를 사용하여 개발한 다른 비즈니스 준비 앱도 제공합니다.

HDX 앱: StoreFront로 게시하는 Windows 호스팅 앱입니다. Citrix Virtual Apps and Desktops™ 환경이 있는 경우 앱을 XenMobile과 통합하여 등록된 사용자가 앱을 사용할 수 있도록 할 수 있습니다.

XenMobile로 배포하고 관리하려는 모바일 앱 유형에 따라 기본 구성 및 아키텍처가 다릅니다. 예를 들어, 서로 다른 권한 수준을 가진 여러 사용자 그룹이 단일 앱을 사용하는 경우 앱의 두 가지 버전을 배포하기 위해 별도의 배달 그룹이 필요할 수 있습니다. 또한 사용자 장치에서 정책 불일치를 방지하려면 사용자 그룹 구성원이 상호 배타적인지 확인해야 합니다.

Apple 볼륨 구매를 사용하여 iOS 애플리케이션 라이선스를 관리할 수도 있습니다. 이 옵션을 사용하려면 Apple 볼륨 구매에 등록하고 XenMobile 콘솔에서 XenMobile 볼륨 구매 설정을 구성하여 볼륨 구매 라이선스로 앱을 배포해야 합니다. 이러한 다양한 사용 사례로 인해 XenMobile 환경을 구현하기 전에 MAM 전략을 평가하고 계획하는 것이 중요합니다. 다음을 정의하여 MAM 전략 계획을 시작할 수 있습니다.

앱 유형: 지원하려는 다양한 앱 유형을 나열한 다음 분류합니다. 예를 들어, 공용, 기본, 모바일 생산성 앱, 웹, 사내, ISV 앱 등입니다. 또한 iOS 및 Android와 같은 다양한 장치 플랫폼에 대한 앱을 분류합니다. 이 분류는 각 앱 유형에 필요한 XenMobile 설정을 조정하는 데 도움이 됩니다. 예를 들어, 특정 앱은 래핑에 적합하지 않거나 다른 앱과의 상호 작용을 위해 특수 API를 활성화하려면 Mobile Apps SDK가 필요할 수 있습니다.

네트워크 요구 사항: 특정 네트워크 액세스 요구 사항이 있는 앱을 적절한 설정으로 구성합니다. 예를 들어, 특정 앱은 VPN을 통해 내부 네트워크에 액세스해야 할 수 있습니다. 일부 앱은 DMZ를 통해 액세스를 라우팅하기 위해 인터넷 액세스가 필요할 수 있습니다. 이러한 앱이 필요한 네트워크에 연결할 수 있도록 하려면 다양한 설정을 그에 따라 구성해야 합니다. 앱별 네트워크 요구 사항을 정의하면 아키텍처 결정을 조기에 확정하는 데 도움이 되며, 이는 전체 구현 프로세스를 간소화합니다.

보안 요구 사항: 개별 앱 또는 모든 앱에 적용되는 보안 요구 사항을 정의하는 것이 중요합니다. 이 계획을 통해 XenMobile Server를 설치할 때 올바른 구성을 생성할 수 있습니다. MDX 정책과 같은 설정은 개별 앱에 적용되지만, 세션 및 인증 설정은 모든 앱에 적용됩니다. 일부 앱에는 배포를 단순화하기 위해 미리 개요를 설명할 수 있는 특정 암호화, 컨테이너화, 래핑, 인증, 지오펜싱, 암호 또는 데이터 공유 요구 사항이 있을 수 있습니다.

배포 요구 사항: 정책 기반 배포를 사용하여 규정을 준수하는 사용자만 게시된 앱을 다운로드하도록 허용할 수 있습니다. 예를 들어, 특정 앱에 다음 중 하나가 필요하도록 할 수 있습니다.

- 장치 플랫폼 기반 암호화가 활성화됨
- 장치가 관리됨
- 장치가 최소 운영 체제 버전을 충족함
- 특정 앱은 회사 사용자만 사용할 수 있음

특정 앱을 기업 사용자에게만 제공하고 싶을 수도 있습니다. 적절한 배포 규칙 또는 작업을 구성할 수 있도록 이러한 요구 사항을 미리 계획하십시오.

라이선스 요구 사항: 앱 관련 라이선스 요구 사항을 기록해 두십시오. 이 기록은 라이선스 사용을 효과적으로 관리하고 라이선스를 용이하게 하기 위해 XenMobile에서 특정 기능을 구성할지 여부를 결정하는 데 도움이 됩니다. 예를 들어, 무료 또는 유료 iOS 앱을 배포하는 경우 Apple은 사용자가 iTunes 계정에 로그인하도록 요구하여 앱에 대한 라이선스 요구 사항을 적용합니다. Apple 볼륨 구매에 등록하여 XenMobile을 통해 이러한 앱을 배포하고 관리할 수 있습니다. 볼륨 구매를 통해 사용자는 iTunes 계정에 로그인하지 않고도 앱을 다운로드할 수 있습니다. 또한 Samsung SAFE 및 Samsung Knox와 같은 도구에는 특별한 라이선스 요구 사항이 있으며, 이러한 기능을 배포하기 전에 완료해야 합니다.

허용 목록 및 차단 목록 요구 사항: 사용자가 일부 앱을 설치하거나 사용하지 못하도록 차단하고 싶을 수 있습니다. 장치를 규정 미준수 상태로 만드는 앱의 허용 목록을 만드십시오. 그런 다음 장치가 규정 미준수 상태가 될 때 트리거되는 정책을 설정하십시오. 반면에 앱은 사용하기에 허용될 수 있지만 어떤 이유로든 차단 목록에 포함될 수 있습니다. 이 경우 앱을 허용 목록에 추가하고 앱을 사용할 수 있지만 필수는 아님을 나타낼 수 있습니다. 또한 새 장치에 사전 설치된 앱에는 운영 체제의 일부가 아닌 일부 일반적으로 사용되는 앱이 포함될 수 있다는 점을 명심하십시오. 이러한 앱은 차단 목록 전략과 충돌할 수 있습니다.

앱 사용 사례

한 의료 기관에서 모바일 앱을 위한 MAM 솔루션으로 XenMobile을 배포할 계획입니다. 모바일 앱은 기업 및 BYOD 사용자에게 제공됩니다. IT 부서는 다음 앱을 제공하고 관리하기로 결정했습니다.

- **모바일 생산성 앱:** Citrix에서 제공하는 iOS 및 Android 앱.
- **Secure Mail:** 이메일, 캘린더 및 연락처 앱.
- **Secure Web:** 인터넷 및 인트라넷 사이트에 대한 액세스를 제공하는 보안 웹 브라우저.
- **Citrix Files:** 공유 데이터에 액세스하고 파일을 공유, 동기화 및 편집하는 앱.

공개 앱 스토어

- **Secure Hub:** 모든 모바일 장치가 XenMobile과 통신하는 데 사용되는 클라이언트입니다. IT 부서는 Secure Hub 클라이언트를 통해 보안 설정, 구성 및 모바일 앱을 모바일 장치로 푸시합니다. Android 및 iOS 장치는 Secure Hub를 통해 XenMobile에 등록됩니다.
- **Citrix Receiver™:** 사용자가 모바일 장치에서 Virtual Apps and Desktops에서 호스팅되는 애플리케이션을 열 수 있도록 하는 모바일 앱.
- **GoToMeeting:** 사용자가 인터넷을 통해 다른 컴퓨터 사용자, 고객, 클라이언트 또는 동료와 실시간으로 회의할 수 있도록 하는 온라인 회의, 데스크톱 공유 및 화상 회의 클라이언트.
- **Salesforce1:** Salesforce1을 통해 사용자는 모바일 장치에서 Salesforce에 액세스할 수 있으며, 모든 Chatter, CRM, 사용자 지정 앱 및 비즈니스 프로세스를 모든 Salesforce 사용자에게 통합된 환경으로 제공합니다.
- **RSA SecurID:** 2단계 인증을 위한 소프트웨어 기반 토큰.

- **EpicCare 앱:** 이 앱은 의료 종사자에게 환자 차트, 환자 목록, 일정 및 메시징에 대한 안전하고 휴대 가능한 액세스를 제공합니다.
  - **Haiku:** iPhone 및 Android 휴대폰용 모바일 앱.
  - **Canto:** iPad용 모바일 앱
  - **Rover:** iPhone 및 iPad용 모바일 앱.

HDX: 이 앱은 Citrix Virtual Apps™ 및 Desktops를 통해 제공됩니다.

- **Epic Hyperspace:** 전자 건강 기록 관리를 위한 Epic 클라이언트 애플리케이션.

ISV

- **Vocera:** iPhone 및 Android 스마트폰을 통해 언제 어디서나 Vocera 음성 기술의 이점을 확장하는 HIPAA 준수 VoIP 및 메시징 모바일 앱.

사내 앱

- **HCMail:** 암호화된 메시지를 작성하고, 내부 메일 서버에서 주소록을 검색하며, 이메일 클라이언트를 사용하여 암호화된 메시지를 연락처로 보내는 데 도움이 되는 앱.

사내 웹 앱

- **PatientRounding:** 여러 부서에서 환자 건강 정보를 기록하는 데 사용되는 웹 애플리케이션.
- **Outlook Web Access:** 웹 브라우저를 통해 이메일에 액세스할 수 있습니다.
- **SharePoint:** 조직 전체의 파일 및 데이터 공유에 사용됩니다.

다음 표에는 MAM 구성에 필요한 기본 정보가 나열되어 있습니다.

앱 이름	앱 유형	MDX 래핑	iOS	안드로이드
시큐어 메일	XenMobile 앱	버전 10.4.1 이상에서는 아니요	예	예
시큐어 웹	XenMobile 앱	버전 10.4.1 이상에서는 아니요	예	예
시트릭스 파일즈	XenMobile 앱	버전 10.4.1 이상에서는 아니요	예	예
시큐어 허브	공개 앱	NA	예	예
시트릭스 리시버	공개 앱	NA	예	예

GoToMeeting	공개 앱	NA	예	예
세일즈포스1	공개 앱	NA	예	예
RSA SecurID	공개 앱	NA	예	예
에픽 하이쿠	공개 앱	NA	예	예
에픽 칸토	공개 앱	NA	예	아니요
에픽 로버	공개 앱	NA	예	아니요
에픽 하이퍼스페이스	HDX™ 앱	해당 없음	예	예
보세라	ISV 앱	예	예	예
에이치씨메일	자체 개발 앱	예	예	예
PatientRounding	웹 앱	NA	예	예
아웃룩 웹 액세스	웹 앱	NA	예	예
SharePoint	웹 앱	NA	예	예

다음 표에는 XenMobile에서 MAM 정책을 구성할 때 참조할 수 있는 특정 요구 사항이 나열되어 있습니다.

앱 이름	VPN 필요	상호 작용	상호 작용	장치 플랫폼 기반 암호화
		(컨테이너 외부 앱과 함께)	(컨테이너 외부 앱에서)	
보안 메일	예	선택적으로 허용됨	허용됨	필요 없음
보안 웹	예	허용됨	허용됨	필요 없음
시트릭스 파일즈	예	허용됨	허용됨	필요 없음
시큐어 허브	예	해당 없음	해당 없음	해당 없음

앱 이름	VPN 필요	상호 작용	상호 작용	장치 플랫폼 기반 암호화
		(컨테이너 외부 앱과 함께)	(컨테이너 외부 앱에서)	
시트릭스 리시버	예	N/A	N/A	N/A
GoToMeeting	N	N/A	N/A	N/A
세일즈포스1	N	N/A	N/A	N/A
RSA SecurID	N	N/A	N/A	N/A
에픽 하이쿠	Y	N/A	N/A	N/A
에픽 칸토	Y	N/A	N/A	N/A
에픽 로버	Y	해당 없음	해당 없음	해당 없음
에픽 하이퍼스페이스	예	해당 없음	해당 없음	해당 없음
보세라	예	차단됨	차단됨	필요 없음
에이치씨메일	예	차단됨	차단됨	필수
PatientRounding	Y	N/A	N/A	필수
아웃룩 웹 액세스	Y	N/A	N/A	필수 아님
SharePoint	Y	해당 없음	해당 없음	필요 없음

앱 이름	프록시 필터링	라이선싱	지오펜싱	모바일 앱 SDK	최소 운영 체제 버전
보안 메일	필수	해당 없음	선택적으로 필요함	해당 없음	강제 적용됨
시큐어 웹	필수	해당 없음	필수 아님	해당 없음	강제 적용
시트릭스 파일	필수	해당 없음	필수 아님	해당 없음	강제 적용

앱 이름	프록시 필터링	라이선싱	지오펜싱	모바일 앱 SDK	최소 운영 체제 버전
시큐어 허브	필수 아님	볼륨 구매	필요 없음	해당 없음	강제되지 않음
시트릭스 리시버	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
GoToMeeting	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
세일즈포스1	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
RSA SecurID	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
에픽 하이쿠	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
에픽 칸토	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
에픽 로버	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
에픽 하이퍼스페이스	필요 없음	해당 없음	필요 없음	해당 없음	적용되지 않음
보세라	필수	해당 없음	필수	필수	적용됨
에이치씨메일	필수	해당 없음	필수	필수	강제 적용됨
PatientRound-ing	필수	해당 없음	필수 아님	해당 없음	강제 적용되지 않음
아웃룩 웹 액세스	필수	해당 없음	필수 아님	해당 없음	강제 적용되지 않음
SharePoint	필수	해당 없음	필수 아님	해당 없음	강제되지 않음

사용자 커뮤니티

모든 조직은 다양한 기능적 역할을 수행하는 여러 사용자 커뮤니티로 구성됩니다. 이러한 사용자 커뮤니티는 사용자의 모바일 장치를 통해 제공하는 다양한 리소스를 사용하여 여러 작업과 사무 기능을 수행합니다. 사용자는 제공된 모바일 장치를 사용하여 집이나 원격 사무실에서 작업할 수 있습니다. 또는 사용자는 개인 모바일 장치를 사용하여 특정 보안 규정 준수 규칙이 적용되는 도구에 액세스할 수 있습니다.

As more user communities use mobile devices, Enterprise Mobility Management (EMM) becomes critical to prevent data leaks and to enforce security restrictions. For efficient and more sophisticated mobile device management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and ensures that the right security policies apply to the right users.

다음 예시는 의료 기관의 사용자 커뮤니티가 EMM을 위해 어떻게 분류되는지 보여줍니다.

사용자 커뮤니티 사용 사례

이 예시 의료 기관은 네트워크 및 제휴 직원과 자원봉사자를 포함한 여러 사용자에게 기술 리소스와 액세스를 제공합니다. 이 조직은 EMM 솔루션을 비경영진 사용자에게만 배포하기로 결정했습니다.

이 조직의 사용자 역할 및 기능은 임상, 비임상 및 계약직을 포함한 하위 그룹으로 나눌 수 있습니다. 선택된 사용자 그룹은 회사 모바일 장치를 지급받고, 다른 사용자들은 개인 장치에서 제한된 회사 리소스에 액세스할 수 있습니다. 적절한 수준의 보안 제한을 적용하고 데이터 유출을 방지하기 위해, 조직은 기업 IT가 등록된 각 장치(회사 지급 또는 BYOD)를 관리하도록 결정했습니다. 또한, 사용자는 단일 장치만 등록할 수 있습니다.

다음 섹션에서는 각 하위 그룹의 역할과 기능에 대한 개요를 제공합니다.

임상

- 간호사
- 의사 (내과 의사, 외과 의사 등)
- 전문가 (영양사, 마취과 의사, 방사선과 의사, 심장 전문의, 종양 전문의 등)
- 외부 의사 (원격 사무실에서 근무하는 비직원 의사 및 사무직 직원)
- 재택 건강 서비스 (환자 방문 진료 서비스를 수행하는 사무직 및 모바일 직원)
- 연구 전문가 (의학 문제에 대한 해답을 찾기 위해 임상 연구를 수행하는 6개 연구 기관의 지식 근로자 및 파워 사용자)
- 교육 및 훈련 (교육 및 훈련 분야의 간호사, 의사 및 전문가)

비임상

- 공유 서비스 (HR, 급여, 미지급금, 공급망 서비스 등 다양한 백오피스 기능을 수행하는 사무직 직원)

- 의료 서비스 (행정 서비스, 분석 및 비즈니스 인텔리전스, 비즈니스 시스템, 고객 서비스, 재무, 관리 의료 행정, 환자 접근 솔루션, 수익 주기 솔루션 등 다양한 의료 관리, 행정 서비스 및 비즈니스 프로세스 솔루션을 제공업체에 제공하는 사무직 직원)
- 지원 서비스 (복리후생 관리, 임상 통합, 커뮤니케이션, 보상 및 성과 관리, 시설 및 자산 서비스, HR 기술 시스템, 정보 서비스, 내부 감사 및 프로세스 개선 등 다양한 비임상 기능을 수행하는 사무직 직원)
- 자선 프로그램 (자선 프로그램을 지원하는 다양한 기능을 수행하는 사무직 및 모바일 직원)

계약자

- 제조업체 및 공급업체 파트너 (현장 및 사이트 간 VPN을 통해 원격으로 연결되어 다양한 비임상 지원 기능을 제공)

앞선 정보를 바탕으로 조직은 다음 엔터티를 생성했습니다. XenMobile의 배포 그룹에 대한 자세한 내용은 리소스 배포를 참조하십시오.

액티브 디렉터리 조직 구성 단위(OU) 및 그룹

OU = XenMobile 리소스의 경우:

- OU = 임상; 그룹 =
    - XM-간호사
    - XM-의사
    - XM-전문가
    - XM-외부 의사
    - XM-재택 건강 서비스
    - XM-연구 전문가
    - XM-교육 및 훈련
- OU = 비임상; 그룹 =
    - XM-공유 서비스
    - XM-의료 서비스
    - XM-지원 서비스
    - XM-자선 프로그램

XENMOBILE 로컬 사용자 및 그룹

그룹 = 계약자, 사용자 =

- 공급업체1

- 공급업체2
- 공급업체 3
- … 공급업체 10

XENMOBILE 배달 그룹

- Clinical-간호사
- Clinical-의사
- Clinical-전문가
- Clinical-외부 의사
- Clinical-재택 건강 서비스
- Clinical-연구 전문가
- Clinical-교육 및 훈련
- Non-Clinical-공유 서비스
- 비임상-의사 서비스
- 비임상-지원 서비스
- 비임상-자선 프로그램

배달 그룹 및 사용자 그룹 매핑

액티브 디렉토리 그룹	**XenMobile 배달 그룹**
XM-간호사	임상-간호사
XM-의사	임상-의사
XM-전문가	임상-전문가
XM-외부 의사	임상-외부 의사
XM-재택 건강 서비스	임상-재택 건강 서비스
XM-연구 전문가	임상-연구 전문가
XM-교육 및 훈련	임상-교육 및 훈련
XM-공유 서비스	비임상-공유 서비스
XM-의료 서비스	비임상-의료 서비스

XM-지원 서비스	비임상-지원 서비스
XM-자선 프로그램	비임상-자선 프로그램

딜리버리 그룹 및 리소스 매핑

다음 표는 이 사용 사례에서 각 딜리버리 그룹에 할당된 리소스를 보여줍니다. 첫 번째 표는 모바일 앱 할당을 보여줍니다. 두 번째 표는 공용 앱, HDX 앱 및 장치 관리 리소스를 보여줍니다.

XenMobile 딜리버리 그룹	**Citrix 모바일 앱**	**공개 모바일 앱**	**HDX 모바일 앱**
임상-간호사	X		
임상-의사			
임상-전문가			
임상-외부 의사	X		
임상-재택 건강 서비스	X		
임상-연구 전문가	X		
임상-교육 및 훈련		X	X
비임상-공유 서비스		X	X
비임상-의료 서비스		X	X
비임상-지원 서비스	X	X	X
비임상-자선 프로그램	X	X	X
계약직 직원	X	X	X

XenMobile 배달 그룹	**공개 앱: RSA SecurID**	**공개 앱: EpicCare Haiku**	**HDX 앱: 에픽 하이퍼스페이스**	**암호 정책**	**장치 제한**	**자동화된 작업**	**Wi-Fi 정책**

임상 간호사							X
임상-의사					X		
임상-전문가							
임상-외부 의사							
임상-재택 건강 서비스							
임상-연구 전문가							
임상-교육 및 훈련		X	X				
비임상-공유 서비스		X	X				
비임상-의료 서비스		X	X				
비임상 지원 서비스		X	X				

참고 사항 및 고려 사항

- XenMobile은 초기 구성 중에 All Users라는 기본 전달 그룹을 생성합니다. 이 전달 그룹을 비활성화하지 않으면 모든 Active Directory 사용자가 XenMobile에 등록할 권한을 갖습니다.
- XenMobile은 LDAP 서버에 대한 동적 연결을 사용하여 Active Directory 사용자 및 그룹을 온디맨드로 동기화합니다.

- 사용자가 XenMobile에 매핑되지 않은 그룹에 속해 있으면 해당 사용자는 등록할 수 없습니다. 마찬가지로, 사용자가 여러 그룹의 구성원인 경우 XenMobile은 해당 사용자를 XenMobile에 매핑된 그룹에만 속하는 것으로 분류합니다.
- MDM 등록을 필수로 설정하려면 XenMobile 콘솔의 서버 속성에서 등록 필요(Enrollment Required) 옵션을 True로 설정해야 합니다. 자세한 내용은 서버 속성을 참조하십시오.
- SQL Server 데이터베이스의 dbo.userlistgrps에서 항목을 삭제하여 XenMobile 전달 그룹에서 사용자 그룹을 삭제할 수 있습니다. **주의:** 이 작업을 수행하기 전에 XenMobile 및 데이터베이스를 백업하십시오.

XenMobile의 장치 소유권 정보

사용자의 장치 소유자에 따라 사용자를 그룹화할 수 있습니다. 장치 소유권에는 회사 소유 장치와 사용자 소유 장치(BYOD(Bring Your Own Device)라고도 함)가 포함됩니다. XenMobile 콘솔의 두 곳에서 BYOD 장치가 네트워크에 연결하는 방법을 제어할 수 있습니다. 각 리소스 유형에 대한 배포 규칙과 **설정** 페이지의 서버 속성을 통해서입니다. 배포 규칙에 대한 자세한 내용은 XenMobile 설명서의 배포 규칙 구성을 참조하십시오. 서버 속성에 대한 자세한 내용은 서버 속성를 참조하십시오.

모든 BYOD 사용자가 앱에 액세스하기 전에 장치에 대한 회사 관리를 수락하도록 요구할 수 있습니다. 또는 장치를 관리하지 않고도 사용자에게 회사 앱에 대한 액세스 권한을 부여할 수 있습니다.

서버 설정 **wsapi.mdm.required.flag**를 **true**로 설정하면 XenMobile이 모든 BYOD 장치를 관리하며, 등록을 거부하는 모든 사용자는 앱에 대한 액세스가 거부됩니다. 엔터프라이즈 IT 팀이 XenMobile에 사용자 장치를 등록할 때 긍정적인 사용자 경험과 함께 높은 보안이 필요한 환경에서는 **wsapi.mdm.required.flag**를 **true**로 설정하는 것을 고려하십시오.

기본 설정인 **wsapi.mdm.required.flag**를 **false**로 두면 사용자는 등록을 거부할 수 있지만 XenMobile Store를 통해 장치의 앱에 계속 액세스할 수 있습니다. 개인 정보 보호, 법적 또는 규제 제약으로 인해 장치 관리가 필요 없고 엔터프라이즈 앱 관리만 필요한 환경에서는 **wsapi.mdm.required.flag**를 **false**로 설정하는 것을 고려하십시오.

XenMobile이 관리하지 않는 장치를 가진 사용자는 XenMobile Store를 통해 앱을 설치할 수 있습니다. 선택적 또는 전체 초기화와 같은 장치 수준 제어 대신 앱 정책을 통해 앱에 대한 액세스를 제어합니다. 정책은 설정한 값에 따라 앱이 계속 실행될 수 있는지 확인하기 위해 장치가 XenMobile Server를 정기적으로 확인하도록 요구합니다.

보안 요구 사항

XenMobile 환경을 배포할 때 고려해야 할 보안 사항이 너무 많아 금방 압도될 수 있습니다. 서로 맞물리는 많은 요소와 설정이 있습니다. 시작하는 데 도움을 드리고 허용 가능한 수준의 보호를 선택할 수 있도록 Citrix는 다음 표에 요약된 대로 높은 보안, 더 높은 보안, 최고 보안에 대한 권장 사항을 제공합니다.

배포 모드 선택은 보안 문제 그 이상을 포함합니다. 사용 사례의 요구 사항을 검토하고 배포 모드를 선택하기 전에 보안 문제를 완화할 수 있는지 결정하는 것도 중요합니다.

높음: 이 설정을 사용하면 대부분의 조직에서 허용 가능한 기본 보안 수준을 유지하면서 최적의 사용자 환경을 제공합니다.

더 높음: 이 설정은 보안과 유용성 간의 더 강력한 균형을 이룹니다.

최고: 이러한 권장 사항을 따르면 유용성과 사용자 채택을 희생하면서 높은 수준의 보안을 제공합니다.

배포 모드 보안 고려 사항

다음 표는 각 보안 수준에 대한 배포 모드를 지정합니다.

높은 보안	**더 높은 보안**	**최고 보안**
MAM 또는 MDM	MDM+MAM	MDM+MAM; FIPS 포함

참고:

- 사용 사례에 따라 MDM 전용 또는 MAM 전용 배포는 보안 요구 사항을 충족하고 우수한 사용자 환경을 제공할 수 있습니다.
- 앱 컨테이너화, 마이크로 VPN 또는 앱별 정책이 필요하지 않은 경우 MDM만으로도 장치를 관리하고 보호하기에 충분합니다.
- 앱 컨테이너화만으로 모든 비즈니스 및 보안 요구 사항을 충족할 수 있는 BYOD와 같은 사용 사례의 경우 Citrix는 MAM 전용 모드를 권장합니다.
- 높은 보안 환경(및 회사에서 발행한 장치)의 경우 Citrix는 사용 가능한 모든 보안 기능을 활용하기 위해 MDM+MAM을 권장합니다. MDM 등록을 반드시 적용하십시오.
- 연방 정부와 같이 가장 높은 보안 요구 사항이 있는 환경을 위한 FIPS 옵션.

FIPS 모드를 활성화하는 경우 SQL 트래픽을 암호화하도록 SQL Server를 구성해야 합니다.

Citrix ADC 및 Citrix Gateway 보안 고려 사항

다음 표는 각 보안 수준에 대한 Citrix ADC 및 Citrix Gateway 권장 사항을 지정합니다.

높은 보안	**더 높은 보안**	**최고 보안**

Citrix ADC가 권장됩니다. Citrix Gateway는 MAM 및 ENT에 필수이며, MDM에 권장됩니다.	XenMobile이 DMZ에 있는 경우 SSL 브리지가 포함된 XenMobile 마법사 구성용 표준 Citrix ADC. 또는 XenMobile Server가 내부 네트워크에 있는 경우 보안 표준을 충족하기 위해 필요한 경우 SSL 오프로드.	종단 간 암호화가 포함된 SSL 오프로드

참고:

- NAT 또는 기존 타사 프록시 및 로드 밸런서를 통해 XenMobile Server를 인터넷에 노출하는 것은 MDM의 옵션이 될 수 있습니다. 그러나 해당 설정은 SSL 트래픽이 XenMobile Server에서 종료되어야 하므로 잠재적인 보안 위험을 초래합니다.
- 높은 보안 환경의 경우, 기본 XenMobile 구성이 적용된 Citrix ADC는 일반적으로 보안 요구 사항을 충족하거나 초과합니다.
- 최고 수준의 보안이 필요한 MDM 환경의 경우, Citrix ADC에서 SSL을 종료하면 경계에서 트래픽 검사가 가능하며 종단 간 SSL 암호화를 유지합니다.
- SSL/TLS 암호 정의 옵션.
- SSL FIPS Citrix ADC 하드웨어도 사용할 수 있습니다.
- 자세한 내용은 Citrix Gateway 및 Citrix ADC와 통합을 참조하십시오.

등록 보안 고려 사항

다음 표는 각 보안 수준에 대한 Citrix ADC 및 Citrix Gateway 권장 사항을 지정합니다.

높은 보안	**더 높은 보안**	**최고 보안**
Active Directory 그룹 멤버십만 해당. 모든 사용자 배달 그룹 비활성화됨.	초대 전용 등록 보안 모드. Active Directory 그룹 멤버십만 해당. 모든 사용자 배달 그룹 비활성화됨.	장치 ID에 연결된 등록 보안 모드. Active Directory 그룹 멤버십만 해당. 모든 사용자 배달 그룹 비활성화됨.

참고:

- Citrix는 일반적으로 등록을 미리 정의된 Active Directory 그룹의 사용자에게만 제한할 것을 권장합니다. 이 설정은 내장된 모든 사용자 배달 그룹을 비활성화해야 합니다.

- 등록 초대를 사용하여 초대받은 사용자에게만 등록을 제한할 수 있습니다. 등록 초대는 Windows 장치에서는 사용할 수 없습니다.
- 일회용 PIN(OTP) 등록 초대를 2단계 인증 솔루션으로 사용하고 사용자가 등록할 수 있는 장치 수를 제어할 수 있습니다. OTP 초대는 Windows 장치에서는 사용할 수 없습니다.

장치 암호 보안 고려 사항

다음 표는 각 보안 수준에 대한 장치 암호 권장 사항을 지정합니다.

높은 보안	**더 높은 보안**	**최고 보안**
권장됩니다. 장치 수준 암호화에는 높은 보안이 필요합니다. MDM을 사용하여 적용됩니다. MDX 정책인 비준수 장치 동작을 사용하여 MAM 전용에 필요한 높은 보안을 설정할 수 있습니다.	MDM, MDX 정책 또는 둘 다를 사용하여 적용됩니다.	MDM 및 MDX 정책을 사용하여 적용됩니다. MDM 복잡한 암호 정책.

참고:

- Citrix는 장치 암호 사용을 권장합니다.
- MDM 정책을 통해 장치 암호를 적용할 수 있습니다.
- MDX 정책을 사용하여 관리되는 앱을 사용하는 데 장치 암호를 필수로 설정할 수 있습니다. 예를 들어, BYOD 사용 사례의 경우입니다.
- Citrix는 MDM+MAM 환경에서 보안 강화를 위해 MDM 및 MDX 정책 옵션을 결합할 것을 권장합니다.
- 최고의 보안 요구 사항을 가진 환경의 경우, 복잡한 암호 정책을 구성하고 MDM으로 이를 강제할 수 있습니다. 장치가 암호 정책을 준수하지 않을 때 관리자에게 알리거나 선택적/전체 장치 초기화를 실행하는 자동 작업을 구성할 수 있습니다.

앱

엔터프라이즈 모빌리티 관리(EMM)는 모바일 장치 관리(MDM)와 모바일 애플리케이션 관리(MAM)로 나뉩니다. MDM은 조직이 모바일 장치를 보호하고 제어할 수 있도록 하는 반면, MAM은 애플리케이션 배포 및 관리를 용이하게 합니다. BYOD 도입을 지원하기 위해 XenMobile®과 같은 MAM 솔루션을 구현하여 다음을 지원할 수 있습니다.

- 애플리케이션 배포
- 소프트웨어 라이선스
- 구성

- 애플리케이션 수명 주기 관리

사용자에게 MDM 관리를 선택하도록 요구하거나 허용할 수 있습니다.

XenMobile을 사용하면 특정 MAM 정책 및 VPN 설정을 구성하여 데이터 유출 및 기타 보안 위협을 방지함으로써 이러한 앱을 보호하기 위해 한 단계 더 나아갈 수 있습니다. XenMobile은 조직에 솔루션을 다음과 같이 배포할 수 있는 유연성을 제공합니다.

- MAM 전용 환경
- MDM 전용 환경
- MDM 및 MAM 기능을 모두 제공하는 통합 XenMobile Enterprise 환경

모바일 장치에 앱을 배포하는 기능 외에도 XenMobile은 MDX 기술을 통한 앱 컨테이너화를 제공합니다. 앱에는 세분화된 정책 기반 제어가 적용됩니다. 독립 소프트웨어 공급업체(ISV)는 Mobile Apps SDK를 사용하여 이러한 제어를 적용할 수 있습니다.

기업 환경에서 사용자는 직무를 지원하기 위해 다양한 모바일 앱을 사용합니다. 앱에는 공개 앱 스토어의 앱, 자체 개발 앱 또는 기본 앱이 포함될 수 있습니다. XenMobile은 이러한 앱을 다음과 같이 분류합니다.

- **공개 앱:** 이러한 앱에는 Apple App Store 또는 Google Play와 같은 공개 앱 스토어에서 사용할 수 있는 무료 또는 유료 앱이 포함됩니다. 조직 외부의 공급업체는 종종 공개 앱 스토어에서 앱을 제공합니다. 이 옵션을 통해 고객은 인터넷에서 직접 앱을 다운로드할 수 있습니다. 사용자의 필요에 따라 조직에서 수많은 공개 앱을 사용할 수 있습니다. 이러한 앱의 예로는 GoToMeeting, Salesforce 및 EpicCare 앱이 있습니다.
    - **MAM SDK를 사용하는 경우:** 앱 공급업체로부터 앱 바이너리를 확보합니다. 그런 다음 MAM SDK를 앱에 통합합니다.
    - **MDX Toolkit을 사용하는 경우:** Citrix®는 공개 앱 스토어에서 앱 바이너리를 직접 다운로드한 다음 MDX Toolkit으로 래핑하여 엔터프라이즈 배포하는 것을 지원하지 않습니다. 타사 애플리케이션을 래핑하려면 앱 공급업체와 협력하여 앱 바이너리를 확보하십시오. 그런 다음 MDX Toolkit을 사용하여 바이너리를 래핑할 수 있습니다.
- **사내 앱:** 많은 조직에는 특정 기능을 제공하고 조직 내에서 독립적으로 개발 및 배포되는 앱을 만드는 사내 개발자가 있습니다. 특정 경우에 일부 조직은 ISV가 제공하는 앱을 보유할 수도 있습니다. 이러한 앱은 기본 앱으로 배포하거나 XenMobile과 같은 MAM 솔루션을 사용하여 컨테이너화할 수 있습니다.

  예를 들어, 의료 기관은 의사가 모바일 장치에서 환자 정보를 볼 수 있도록 하는 사내 앱을 만들 수 있습니다. 그러면 조직은 다음 중 하나를 사용하여 환자 정보를 보호하고 환자 데이터베이스에 대한 VPN 액세스를 활성화할 수 있습니다.
    - MAM SDK

  - MDX 툴킷

- **웹 및 SaaS 앱:** 이러한 앱에는 내부 네트워크(웹 앱) 또는 공용 네트워크(SaaS)를 통해 액세스하는 앱이 포함됩니다. XenMobile은 또한 앱 커넥터 목록을 사용하여 사용자 지정 웹 및 SaaS 앱을 만들 수 있도록 합니다. 이러한 앱 커넥터는 기존 웹 앱에 대한 단일 Sign-On(SSO)을 용이하게 할 수 있습니다. 자세한 내용은 앱 커넥터 유형을 참조하십시오. 예를 들어, Google Apps에 대한 SAML(Security Assertion Markup Language) 기반 SSO를 위해 Google Apps SAML을 사용할 수 있습니다.
- **모바일 생산성 앱:** 모바일 생산성 앱은 XenMobile 라이선스에 포함된 Citrix 개발 앱입니다. 자세한 내용은 모바일 생산성 앱 정보를 참조하십시오. Citrix는 또한 ISV가 Mobile Apps SDK를 사용하여 개발하는 다른 비즈니스 준비 앱도 제공합니다.
- **HDX 앱:** HDX 앱은 StoreFront로 게시하는 Windows 호스팅 앱입니다. Citrix Virtual Apps and Desktops™ 및 Citrix Workspace™를 사용하는 경우, 등록된 사용자가 HDX 앱을 사용할 수 있습니다.

XenMobile로 배포하고 관리하려는 모바일 앱 유형에 따라 기본 구성이 다를 수 있습니다. 예를 들어, 서로 다른 권한 수준을 가진 여러 사용자 그룹이 단일 앱을 사용할 수 있습니다. 이 경우 동일한 앱의 두 가지 별도 버전을 배포하기 위해 별도의 배달 그룹을 만들 수 있습니다. 또한 사용자 장치에서 정책 불일치를 방지하려면 사용자 그룹 구성원이 상호 배타적인지 확인해야 합니다.

Apple 볼륨 구매를 사용하여 iOS 애플리케이션 라이선스를 관리할 수도 있습니다. 이 옵션을 사용하려면 볼륨 구매 프로그램에 등록하고 XenMobile 콘솔에서 볼륨 구매 설정을 구성해야 합니다. 이 구성을 통해 볼륨 구매 라이선스로 앱을 배포할 수 있습니다. 다양한 사용 사례로 인해 XenMobile 환경을 구현하기 전에 MAM 전략을 평가하고 계획하는 것이 중요합니다. 다음을 정의하여 MAM 전략 계획을 시작할 수 있습니다.

- **앱 유형:** 지원하려는 다양한 앱 유형을 나열하고 공개, 기본, 웹, 사내 또는 ISV 앱과 같이 분류합니다. 또한 iOS 및 Android와 같은 다양한 장치 플랫폼에 대한 앱을 분류합니다. 이 분류는 각 앱 유형에 필요한 다양한 XenMobile 설정을 조정하는 데 도움이 됩니다. 예를 들어, 일부 앱은 다른 앱과의 상호 작용을 위한 특수 API를 활성화하기 위해 Mobile Apps SDK를 사용해야 할 수 있습니다.
- **네트워크 요구 사항:** 특정 네트워크 액세스 요구 사항이 있는 앱의 설정을 구성합니다. 예를 들어, 특정 앱은 VPN을 통해 내부 네트워크에 액세스해야 할 수 있습니다. 일부 앱은 DMZ를 통해 액세스를 라우팅하기 위해 인터넷 액세스가 필요할 수 있습니다. 이러한 앱이 필요한 네트워크에 연결할 수 있도록 하려면 그에 따라 다양한 설정을 구성해야 합니다. 앱별 네트워크 요구 사항을 정의하면 아키텍처 결정을 조기에 확정하는 데 도움이 되며, 이는 전체 구현 프로세스를 간소화합니다.
- **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 특정 컨테이너화, MDX, 인증, 지오펜싱, 암호 또는 데이터 공유 요구 사항이 있을 수 있습니다.

배포를 간소화하려면 이러한 요구 사항을 미리 계획하십시오. Endpoint Management의 보안에 대한 자세한 내용은 보안 및 사용자 경험을 참조하십시오.

- **배포 요구 사항** - 규정을 준수하는 사용자만 게시된 앱을 다운로드하도록 허용하기 위해 정책 기반 배포를 사용하고 싶을 수 있습니다. 예를 들어, 특정 앱은 장치가 관리되거나 장치가 최소 운영 체제 버전을 충족해야 할 수 있습니다. 또한 특정 앱을 회사 사용자에게만 제공하고 싶을 수도 있습니다. 적절한 배포 규칙 또는 작업을 구성할 수 있도록 이러한 요구 사항을 미리 계획하십시오.
- **라이선스 요구 사항:** 앱 관련 라이선스 요구 사항을 기록해 두십시오. 기록은 라이선스 사용을 효과적으로 관리하고 라이선스를 용이하게 하기 위해 XenMobile에서 특정 기능을 구성할지 여부를 결정하는 데 도움이 될 수 있습니다. 예를 들어, 무료 또는 유료 iOS 앱을 배포하는 경우 Apple은 앱에 대한 라이선스 요구 사항을 적용합니다. 결과적으로 사용자는 Apple App Store 계정에 로그인해야 합니다.

  그러나 XenMobile을 사용하여 이러한 앱을 배포하고 관리하기 위해 Apple 볼륨 구매에 등록할 수 있습니다. 볼륨 구매를 통해 사용자는 Apple App Store 계정에 로그인하지 않고도 앱을 다운로드할 수 있습니다.

  Samsung SAFE 및 Samsung Knox와 같은 일부 플랫폼에는 해당 기능을 배포하기 전에 완료해야 하는 특별한 라이선스 요구 사항이 있습니다.
- **허용 목록 및 차단 목록 요구 사항:** 사용자가 설치하거나 사용하지 않기를 원하는 앱을 식별할 수 있습니다. 차단 목록을 생성하면 규정 미준수 이벤트가 정의됩니다. 그런 다음 이벤트 발생 시 트리거될 정책을 설정할 수 있습니다. 반면에 앱은 사용하기에 허용될 수 있지만 어떤 이유로든 차단 목록에 포함될 수 있습니다. 이 경우 앱을 허용 목록에 추가하고 앱이 사용하기에 허용되지만 필수는 아님을 나타낼 수 있습니다. 또한 새 장치에 사전 설치된 앱에는 운영 체제의 일부가 아닌 일반적으로 사용되는 일부 앱이 포함될 수 있음을 명심하십시오. 이러한 앱은 차단 목록 전략과 충돌할 수 있습니다.

사용 사례

한 의료 기관은 모바일 앱을 위한 MAM 솔루션으로 XenMobile을 배포할 계획입니다. 모바일 앱은 기업 및 BYOD 사용자에게 제공됩니다. IT 부서는 다음 앱을 제공하고 관리하기로 결정했습니다.

모바일 생산성 앱: Citrix에서 제공하는 iOS 및 Android 앱입니다. 자세한 내용은 모바일 생산성 앱을 참조하십시오.

Citrix Secure Hub™: 모든 모바일 장치가 XenMobile과 통신하는 데 사용되는 클라이언트입니다. Secure Hub를 사용하여 보안 설정, 구성 및 모바일 앱을 모바일 장치로 푸시합니다. Android 및 iOS 장치는 Secure Hub를 통해 XenMobile에 등록됩니다.

Citrix Receiver: 모바일 장치 사용자가 Citrix Virtual Apps에서 호스팅되는 애플리케이션을 열 수 있도록 하는 모바일 앱입니다.

GoToMeeting: 사용자가 인터넷을 통해 다른 컴퓨터 사용자, 고객, 클라이언트 또는 동료와 실시간으로 회의할 수 있도록 하는 온라인 회의, 데스크톱 공유 및 화상 회의 클라이언트입니다.

SalesForce1: Salesforce1을 통해 사용자는 모바일 장치에서 Salesforce에 액세스하고 모든 Chatter, CRM, 사용자 지정 앱 및 비즈니스 프로세스를 모든 Salesforce 사용자에게 통합된 경험으로 제공합니다.

RSA SecurID: 2단계 인증을 위한 소프트웨어 기반 토큰입니다.

EpicCare 앱: 이 앱은 의료 종사자에게 환자 차트, 환자 목록, 일정 및 메시징에 대한 안전하고 휴대 가능한 액세스를 제공합니다.

Haiku: iPhone 및 Android 휴대폰용 모바일 앱입니다.

Canto: iPad용 모바일 앱입니다.

Rover: iPhone 및 iPad용 모바일 앱입니다.

HDX™: Citrix Virtual Apps는 HDX 앱을 제공합니다.

- **Epic Hyperspace:** 전자 건강 기록 관리를 위한 Epic 클라이언트 애플리케이션입니다.

ISV:

- **Vocera:** Vocera 음성 기술의 이점을 iPhone 및 Android 스마트폰을 통해 언제 어디서나 확장하는 HIPAA 준수 VoIP(Voice-over IP) 및 메시징 모바일 앱입니다.

사내 앱:

- **HCMail:** 암호화된 메시지를 작성하고, 내부 메일 서버에서 주소록을 검색하며, 이메일 클라이언트를 사용하여 암호화된 메시지를 연락처로 보내는 데 도움이 되는 앱입니다.

사내 웹 앱:

- **PatientRounding:** 여러 부서에서 환자 건강 정보를 기록하는 데 사용되는 웹 애플리케이션입니다.
- **Outlook Web Access:** 웹 브라우저를 통해 이메일에 액세스할 수 있습니다.
- **SharePoint:** 조직 전체의 파일 및 데이터 공유에 사용됩니다.

다음 표에는 MAM 구성에 필요한 기본 정보가 나열되어 있습니다.

앱 이름	**앱 유형**	**MAM SDK 통합 또는 MDX 래핑**	**iOS**	**안드로이드**

시큐어 메일	XenMobile 앱	버전 10.4.1 이상에서는 아니요	예	예
시큐어 웹	XenMobile 앱	버전 10.4.1 이상에서는 아니요	예	예
시트릭스 파일즈	XenMobile 앱	버전 10.4.1 이상에서는 아니요	예	예
시큐어 허브	공개 앱	해당 없음	예	예
시트릭스 리시버	공개 앱	해당 없음	예	예
GoToMeeting	공개 앱	N/A	예	예
SalesForce1	공개 앱	N/A	예	예
RSA SecurID	공개 앱	N/A	예	예
에픽 하이쿠	공개 앱	해당 없음	예	예
에픽 칸토	공개 앱	해당 없음	예	아니요
에픽 로버	공개 앱	해당 없음	예	아니요
에픽 하이퍼스페이스	HDX 앱	해당 없음	예	예
보세라	ISV 앱	예	예	예
에이치씨메일	사내 앱	예	예	예
PatientRounding	웹 앱	N/A	예	예
아웃룩 웹 액세스	웹 앱	N/A	예	예
SharePoint	웹 앱	N/A	예	예

다음 표에는 XenMobile에서 MAM 정책을 구성할 때 참조할 수 있는 특정 요구 사항이 나열되어 있습니다.

앱 이름	VPN 필요	상호 작용 (컨테이너 외부 앱과)	상호 작용 (컨테이너 외부 앱으로부터)	프록시 필터링	라이선스	지오펜싱	모바일 앱 SDK	최소 운영 체제 버전
보안 메일	Y	선택적으로 허용됨	허용됨	필수	해당 없음	선택적으로 필요함	해당 없음	강제 적용됨
보안 웹	예	허용됨	허용됨	필요함	해당 없음	필요하지 않음	해당 없음	강제 적용됨
시트릭스 파일	예	허용됨	허용됨	필수	해당 없음	필요 없음	해당 없음	강제 적용
시큐어 허브	Y	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
시트릭스 리시버	예	해당 없음	해당 없음	필요 없음	대량 구매	필요 없음	해당 없음	강제되지 않음
GoTo Meeting	아니요	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
Sales Force 1	N	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
RSA SecurID	N	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
에픽 하이쿠	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
에픽 칸토	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	강제되지 않음
에픽 로버	예	해당 없음	해당 없음	필요 없음	볼륨 구매	필요 없음	해당 없음	적용되지 않음

앱 이름	VPN 필요	상호 작용 (컨테이너 외부 앱과)	상호 작용 (컨테이너 외부 앱으로부터)	프록시 필터링	라이선스	지오펜싱	모바일 앱 SDK	최소 운영 체제 버전
에픽 하이퍼스페이스	예	해당 없음	해당 없음	필요 없음	해당 없음	필요 없음	해당 없음	적용되지 않음
보세라	예	차단됨	차단됨	필수	해당 없음	필수	필수	강제 적용됨
에이치씨메일	예	차단됨	차단됨	필수	해당 없음	필수	필수	강제 적용
PatientRound-ing	예	해당 없음	해당 없음	필수	해당 없음	필수 아님	해당 없음	강제 적용 안 함
아웃룩 웹 액세스	예	해당 없음	해당 없음	필수	해당 없음	필요 없음	해당 없음	강제되지 않음
SharePoint	예	해당 없음	해당 없음	필수	해당 없음	필요 없음	해당 없음	강제되지 않음

사용자 커뮤니티

모든 조직은 다양한 기능적 역할을 수행하는 여러 사용자 커뮤니티로 구성됩니다. 이러한 사용자 커뮤니티는 사용자가 모바일 장치를 통해 제공하는 다양한 리소스를 사용하여 여러 작업과 사무 기능을 수행합니다. 사용자는 집이나 원격 사무실에서 제공된 모바일 장치를 사용하거나 개인 모바일 장치를 사용하여 특정 보안 규정 준수 규칙이 적용되는 도구에 액세스할 수 있습니다.

모바일 장치를 사용하는 사용자 커뮤니티가 증가함에 따라 엔터프라이즈 모빌리티 관리(EMM)는 데이터 유출을 방지하고 조직의 보안 제한을 적용하는 데 중요해집니다. 효율적이고 정교한 모바일 장치 관리를 위해 사용자 커뮤니티를 분류할 수 있습니다. 이렇게 하면 사용자를 리소스에 매핑하는 것이 간소화되고 올바른 보안 정책이 올바른 사용자에게 적용되도록 보장합니다.

사용자 커뮤니티 분류에는 다음 구성 요소 사용이 포함될 수 있습니다.

- Active Directory 조직 구성 단위(OU) 및 그룹

특정 Active Directory 보안 그룹에 추가된 사용자는 앱과 같은 정책 및 리소스를 받을 수 있습니다. Active Directory 보안 그룹에서 사용자를 제거하면 이전에 허용된 XenMobile® 리소스에 대한 액세스가 제거됩니다.

- XenMobile 로컬 사용자 및 그룹

  Active Directory에 계정이 없는 사용자의 경우 로컬 XenMobile 사용자로 생성할 수 있습니다. 로컬 사용자를 배달 그룹에 추가하고 Active Directory 사용자와 동일한 방식으로 리소스를 프로비저닝할 수 있습니다.

- XenMobile 배달 그룹

  다른 수준의 권한을 가진 여러 사용자 그룹이 단일 앱을 사용해야 하는 경우 별도의 배달 그룹을 생성해야 할 수 있습니다. 별도의 배달 그룹을 사용하면 동일한 앱의 두 가지 버전을 배포할 수 있습니다.

- 배달 그룹 및 사용자 그룹 매핑

  배달 그룹과 Active Directory 그룹 매핑은 일대일 또는 일대다일 수 있습니다. 일대다 배달 그룹 매핑에 기본 정책 및 앱을 할당합니다. 일대일 배달 그룹 매핑에 기능별 정책 및 앱을 할당합니다.

- 배달 그룹 및 앱 리소스 매핑

  각 배달 그룹에 특정 앱을 할당합니다.

- 배달 그룹 및 MDM 리소스 매핑

  각 배포 그룹에 앱 및 특정 장치 관리 리소스를 할당합니다. 예를 들어, 다음 항목을 혼합하여 배포 그룹을 구성할 수 있습니다. 앱 유형(공개, HDX™ 등), 앱 유형별 특정 앱, 장치 정책 및 자동화된 작업과 같은 리소스.

다음 예는 의료 기관의 사용자 커뮤니티가 EMM을 위해 어떻게 분류되는지 보여줍니다.

사용 사례

이 예시 의료 기관은 네트워크 및 계열사 직원과 자원봉사자를 포함한 여러 사용자에게 기술 리소스 및 액세스를 제공합니다. 이 기관은 EMM 솔루션을 비경영진 사용자에게만 배포하기로 결정했습니다.

이 기관의 사용자 역할과 기능은 임상, 비임상, 계약직을 포함한 하위 그룹으로 나눌 수 있습니다. 일부 사용자는 회사 모바일 장치를 지급받고, 다른 사용자는 개인 장치(BYOD)에서 제한된 회사 리소스에 액세스할 수 있습니다. 적절한 수준의 보안 제한을 적용하고 데이터 유출을 방지하기 위해, 이 기관은 등록된 각 장치를 회사 IT가 관리하도록 결정했습니다. 또한, 사용자는 단 하나의 장치만 등록할 수 있습니다.

다음 섹션에서는 각 하위 그룹의 역할과 기능에 대한 개요를 제공합니다.

임상

- 간호사

- 의사 (내과 의사, 외과 의사 등)
- 전문가 (영양사, 채혈사, 마취과 의사, 방사선과 의사, 심장 전문의, 종양 전문의 등)
- 외부 의사 (원격 사무실에서 근무하는 비직원 의사 및 사무직 직원)
- 재택 의료 서비스 (환자 방문을 위해 의료 서비스를 제공하는 사무직 및 모바일 직원)
- 연구 전문가 (의학 문제에 대한 해답을 찾기 위해 임상 연구를 수행하는 6개 연구 기관의 지식 근로자 및 파워 사용자)
- 교육 및 훈련 (교육 및 훈련 분야의 간호사, 의사 및 전문가)

비임상

- 공유 서비스 (HR, 급여, 미지급금, 공급망 서비스 등을 포함한 다양한 백오피스 기능을 수행하는 사무직 직원)
- 의료 서비스 (행정 서비스, 분석 및 비즈니스 인텔리전스, 비즈니스 시스템, 고객 서비스, 재무, 관리형 의료 관리, 환자 접근 솔루션, 수익 주기 솔루션 등을 포함하여 공급자에게 다양한 의료 관리, 행정 서비스 및 비즈니스 프로세스 솔루션을 제공하는 사무직 직원)
- 지원 서비스 (혜택 관리, 임상 통합, 커뮤니케이션, 보상 및 성과 관리, 시설 및 자산 서비스, HR 기술 시스템, 정보 서비스, 내부 감사 및 프로세스 개선 등을 포함한 다양한 비임상 기능을 수행하는 사무직 직원)
- 자선 프로그램 (자선 프로그램을 지원하는 다양한 기능을 수행하는 사무직 및 모바일 직원)

계약자

- 제조업체 및 공급업체 파트너 (현장 및 사이트 간 VPN을 통해 원격으로 연결되어 다양한 비임상 지원 기능을 제공)

앞선 정보를 바탕으로 조직은 다음 엔터티를 생성했습니다. XenMobile의 딜리버리 그룹에 대한 자세한 내용은 XenMobile 제품 설명서의 리소스 배포를 참조하십시오.

Active Directory 조직 구성 단위(OU) 및 그룹

OU = XenMobile 리소스

- OU = 임상; 그룹 =
  - XM-간호사
  - XM-의사
  - XM-전문가
  - XM-외부 의사
  - XM-재택 건강 서비스
  - XM-연구 전문가

    - XM-교육 및 훈련
- OU = 비임상; 그룹 =
    - XM-공유 서비스
    - XM-의료 서비스
    - XM-지원 서비스
    - XM-자선 프로그램

XenMobile 로컬 사용자 및 그룹

그룹 = 계약자, 사용자 =

- 공급업체1
- 공급업체2
- 공급업체 3
- … 공급업체 10

XenMobile 딜리버리 그룹

- 임상-간호사
- 임상-의사
- 임상-전문가
- 임상-외부 의사
- 임상-재택 건강 서비스
- 임상-연구 전문가
- 임상-교육 및 훈련
- 비임상-공유 서비스
- 비임상-의사 서비스
- 비임상-지원 서비스
- 비임상-자선 프로그램

전달 그룹 및 사용자 그룹 매핑

액티브 디렉터리 그룹	**XenMobile 전달 그룹**
XM-간호사	임상-간호사

XM-의사	임상-의사
XM-전문가	임상-전문가
XM-외부 의사	임상-외부 의사
XM-재택 건강 서비스	임상-재택 건강 서비스
XM-연구 전문가	임상-연구 전문가
XM-교육 및 훈련	임상-교육 및 훈련
XM-공유 서비스	비임상-공유 서비스
XM-의사 서비스	비임상-의사 서비스
XM-지원 서비스	비임상-지원 서비스
XM-자선 프로그램	비임상-자선 프로그램

앱의 딜리버리 그룹 및 리소스 매핑

	보안 메일	보안 웹	ShareFile	리시버	SalesForce 1	RSA SecurID	에픽케어 하이쿠	에픽 하이퍼스페이스
임상-간호사	X	X	X					
임상-의사								
임상-전문가								
임상-외부 의사	X		X					
임상-재택 건	X		X					

강 서비스								
임상-연구 전문가	X		X					
임상-교육 및 훈련							X	X
비임상-공유 서비스							X	X
비임상-의료 서비스							X	X
비임상-지원 서비스	X		X				X	X
비임상-자선 프로그램	X		X				X	X
계약직 직원	X		X	X	X		X	X

MDM 리소스의 배달 그룹 및 리소스 매핑

	MDM: 암호 정책	**MDM: 장치 제한**	**MDM: 자동화된 작업**	**MDM: Wi-Fi 정책**
임상-간호사				X
임상-의사		X		
임상-전문가				

임상-외부 의사				
임상-재택 건강 서비스				
임상-연구 전문가				
임상-교육 및 훈련				
비임상-공유 서비스				
비임상-의료 서비스				
비임상-지원 서비스				
비임상-자선 프로그램				
계약자				X

참고 및 고려 사항

- XenMobile은 초기 구성 중에 All Users라는 기본 Delivery Group을 생성합니다. 이 Delivery Group을 비활성화하지 않으면 모든 Active Directory 사용자가 XenMobile에 등록할 권한을 갖습니다.
- XenMobile은 LDAP 서버에 대한 동적 연결을 사용하여 Active Directory 사용자 및 그룹을 온디맨드로 동기화합니다.
- 사용자가 XenMobile에 매핑되지 않은 그룹의 일부인 경우 해당 사용자는 등록할 수 없습니다. 마찬가지로, 사용자가 여러 그룹의 구성원인 경우 XenMobile은 XenMobile에 매핑된 그룹에 있는 사용자만 분류합니다.
- MDM 등록을 필수로 설정하려면 XenMobile 콘솔의 **Server Properties**에서 **Enrollment Required** 옵션을 **True**로 설정합니다. 자세한 내용은 Server Properties를 참조하십시오.
- XenMobile Delivery Group에서 사용자 그룹을 삭제하려면 dbo.userlistgrps 아래의 SQL Server 데이터베이스에서 항목을 삭제합니다.

> **주의:**

> 이 작업을 수행하기 전에 XenMobile 및 데이터베이스를 백업하십시오.

XenMobile의 장치 소유권 정보

사용자 장치 소유자에 따라 사용자를 그룹화할 수 있습니다. 장치 소유권에는 회사 소유 장치와 BYOD(Bring Your Own Device)로도 알려진 사용자 소유 장치가 포함됩니다. XenMobile 콘솔의 두 위치, 즉 배포 규칙과 **Settings** 페이지의 XenMobile Server 속성을 통해 BYOD 장치가 네트워크에 연결하는 방식을 제어할 수 있습니다. 배포 규칙에 대한 자세한 내용은 XenMobile 설명서의 Deploy resources를 참조하십시오. 서버 속성에 대한 자세한 내용은 이 핸드북의 Server Properties를 참조하십시오.

서버 속성을 설정하여 모든 BYOD 사용자가 앱에 액세스하기 전에 장치에 대한 회사 관리를 수락하도록 요구할 수 있습니다. 또는 장치를 관리하지 않고도 사용자에게 회사 앱에 대한 액세스 권한을 부여할 수 있습니다.

wsapi.mdm.required.flag 서버 속성을 **true**로 설정하면 XenMobile이 모든 BYOD 장치를 관리하며, 등록을 거부하는 모든 사용자는 앱에 대한 액세스가 거부됩니다. 엔터프라이즈 IT 팀이 높은 보안과 등록 중 긍정적인 사용자 경험을 필요로 하는 환경에서는 **wsapi.mdm.required.flag**를 **true**로 설정하는 것을 고려하십시오.

기본 설정인 **wsapi.mdm.required.flag**를 **false**로 두면 사용자는 등록을 거부할 수 있습니다. 그러나 XenMobile Store를 통해 장치의 앱에 액세스할 수 있습니다. 개인 정보 보호, 법적 또는 규제 제약으로 인해 장치 관리가 아닌 엔터프라이즈 앱 관리만 필요한 환경에서는 **wsapi.mdm.required.flag**를 **false**로 설정하는 것을 고려하십시오.

XenMobile이 관리하지 않는 장치를 가진 사용자는 XenMobile Store를 통해 앱을 설치할 수 있습니다. 선택적 또는 전체 초기화와 같은 장치 수준 제어 대신 앱 정책을 통해 앱에 대한 액세스를 제어합니다. 일부 정책 설정은 앱이 계속 실행될 수 있는지 확인하기 위해 장치가 XenMobile Server에 정기적으로 확인하도록 요구합니다.

이메일 전략

모바일 장치에서 이메일에 대한 보안 액세스는 모든 조직의 모빌리티 관리 이니셔티브를 이끄는 주요 동인 중 하나입니다. 적절한 이메일 전략을 결정하는 것은 종종 모든 XenMobile® 설계의 핵심 구성 요소입니다. XenMobile은 보안, 사용자 경험 및 통합 요구 사항에 따라 다양한 사용 사례를 수용할 수 있는 여러 옵션을 제공합니다. 이 문서는 클라이언트 선택부터 메일 트래픽 흐름에 이르기까지 올바른 솔루션을 선택하기 위한 일반적인 설계 결정 프로세스 및 고려 사항을 다룹니다.

이메일 클라이언트 선택

클라이언트 선택은 일반적으로 전체 이메일 전략 설계에서 가장 중요한 부분입니다. Citrix Secure Mail™, 특정 모바일 플랫폼 운영 체제에 포함된 기본 메일 또는 공개 앱 스토어를 통해 제공되는 기타 타사 클라이언트

등 여러 클라이언트 중에서 선택할 수 있습니다. 필요에 따라 단일(표준) 클라이언트로 사용자 커뮤니티를 지원하거나 여러 클라이언트를 조합하여 사용해야 할 수도 있습니다.

다음 표는 사용 가능한 다양한 클라이언트 옵션에 대한 몇 가지 설계 고려 사항을 요약한 것입니다.

주제	보안 메일	기본 (예: iOS Mail)	타사 메일
최소 XenMobile 에디션	고급	MDM	MDM
구성	MDX 정책을 통해 구성된 Exchange 계정 프로필.	MDM 정책을 통해 구성된 Exchange 계정 프로필. Android 지원은 SAFE/KNOX 및 Android Enterprise로 제한됩니다. 다른 모든 클라이언트는 타사 클라이언트로 간주됩니다.	일반적으로 사용자의 수동 구성이 필요합니다.
보안	설계상 안전하며 최고 수준의 보안을 제공합니다. 추가 데이터 암호화 수준이 적용된 MDX 정책을 사용합니다. Secure Mail은 MDX 정책을 통해 완전히 관리되는 앱입니다. Citrix PIN을 통한 추가 인증 계층.	공급업체/앱 기능 세트에 기반합니다. 더 높은 보안을 제공합니다. 장치 암호화 설정을 사용합니다(MDX 정책을 통한 보안 없음). 앱 액세스를 위해 장치 수준 인증에 의존합니다.	공급업체/앱 기능 세트에 기반합니다. 높은 보안을 제공합니다.
통합	기본적으로 관리되는 (MDX) 앱과의 상호 작용을 허용합니다. Citrix Secure Web으로 웹 URL을 엽니다. Citrix Files에 파일을 저장하고 Citrix Files에서 파일을 첨부합니다. GoToMeeting에 직접 참여하고 전화로 접속합니다.	기본적으로 다른 비관리형(비MDX) 앱과만 상호 작용할 수 있습니다.	기본적으로 다른 비관리형(비MDX) 앱과만 상호 작용할 수 있습니다.

배포/라이선싱	MDM을 통해, 또는 공용 앱 스토어에서 직접 Secure Mail을 푸시할 수 있습니다. XenMobile Advanced 및 Enterprise 라이선스에 포함됩니다.	플랫폼 운영 체제에 포함된 클라이언트 앱. 추가 라이선스 요구 사항 없음.	MDM을 통해, 엔터프라이즈 앱으로 또는 공용 앱 스토어에서 직접 푸시할 수 있습니다. 앱 공급업체에 따라 관련 라이선스 모델/비용이 결정됩니다.
지원	클라이언트 및 EMM 솔루션(Citrix)에 대한 단일 공급업체 지원. Secure Hub/앱 디버그로깅 기능에 내장된 지원 연락처 정보. 지원할 클라이언트 하나.	공급업체 정의 지원(Apple/Google). 장치 플랫폼에 따라 다른 클라이언트를 지원해야 할 수도 있습니다.	공급업체 정의 지원. 타사 클라이언트가 모든 관리형 장치 플랫폼에서 지원된다고 가정할 때, 지원할 클라이언트 하나.

메일 트래픽 흐름 및 필터링 고려 사항

이 섹션에서는 XenMobile 컨텍스트에서 메일(ActiveSync) 트래픽 흐름에 대한 세 가지 주요 시나리오와 설계 고려 사항에 대해 설명합니다.

시나리오 1: 노출된 Exchange

외부 클라이언트를 지원하는 환경에서는 일반적으로 Exchange ActiveSync 서비스가 인터넷에 노출됩니다. 모바일 ActiveSync 클라이언트는 역방향 프록시(예: Citrix ADC) 또는 Edge Server를 통해 외부 연결 경로로 연결됩니다. 이 옵션은 기본 또는 타사 메일 클라이언트를 사용하는 데 필요하며, 이로 인해 이러한 클라이언트가 이 시나리오에서 인기 있는 선택이 됩니다. 일반적인 방법은 아니지만, 이 시나리오에서 Secure Mail 클라이언트를 사용할 수도 있습니다. 그렇게 하면 MDX 정책 사용 및 앱 관리에서 제공하는 보안 기능의 이점을 얻을 수 있습니다.

시나리오 2: Citrix ADC를 통한 터널링(마이크로 VPN 및 STA)

이 시나리오는 Secure Mail 클라이언트의 마이크로 VPN 기능 때문에 기본값으로 사용됩니다. 이 경우 Secure Mail 클라이언트는 Citrix Gateway를 통해 ActiveSync에 대한 보안 연결을 설정합니다. 본질적으로 Secure Mail은 내부 네트워크에서 ActiveSync에 직접 연결하는 클라이언트로 간주할 수 있습니다. Citrix 고객은 모바일 ActiveSync 클라이언트로 Secure Mail을 표준화하는 경우가 많습니다. 이러한 결정은 첫 번째 시나리오에서 설명한 대로 노출된 Exchange Server에서 ActiveSync 서비스를 인터넷에 노출하는 것을 피하기 위한 이니셔티브의 일부입니다.

MAM SDK가 활성화되었거나 MDX로 래핑된 앱만 마이크로 VPN 기능을 사용할 수 있습니다. MDX 래핑을 사용하는 경우 이 시나리오는 기본 클라이언트에는 적용되지 않습니다. MDX Toolkit으로 타사 클라이언트를 래핑하는 것이 가능할 수도 있지만, 이 방법은 일반적이지 않습니다. 기본 또는 타사 클라이언트에 대한 터널

링된 액세스를 허용하기 위해 장치 수준 VPN 클라이언트를 사용하는 것은 번거롭고 실행 가능한 솔루션이 아닌 것으로 입증되었습니다.

시나리오 3: 클라우드 호스팅 Exchange 서비스

Microsoft Office 365와 같은 클라우드 호스팅 Exchange 서비스가 점점 더 인기를 얻고 있습니다. XenMobile 컨텍스트에서 이 시나리오는 ActiveSync 서비스도 인터넷에 노출되므로 첫 번째 시나리오와 동일하게 처리할 수 있습니다. 이 경우 클라우드 서비스 공급업체 요구 사항에 따라 클라이언트 선택이 결정됩니다. 일반적으로 Secure Mail 및 기타 기본 또는 타사 클라이언트와 같은 대부분의 ActiveSync 클라이언트에 대한 지원이 포함됩니다.

XenMobile은 이 시나리오에서 세 가지 영역에서 가치를 더할 수 있습니다.

- MDX 정책 및 Secure Mail을 사용한 앱 관리가 적용된 클라이언트
- 지원되는 기본 이메일 클라이언트에서 MDM 정책을 사용한 클라이언트 구성
- Endpoint Management connector for Exchange ActiveSync를 사용하여 ActiveSync 필터링 옵션

메일 트래픽 필터링 고려 사항

대부분의 인터넷 노출 서비스와 마찬가지로, 경로를 보호하고 승인된 액세스에 대한 필터링을 제공해야 합니다. XenMobile 솔루션에는 기본 및 타사 클라이언트에 ActiveSync 필터링 기능을 제공하도록 특별히 설계된 두 가지 구성 요소가 포함되어 있습니다. Citrix Gateway connector™ for Exchange ActiveSync 및 Endpoint Management connector for Exchange ActiveSync입니다.

익스체인지 액티브싱크용 시트릭스 게이트웨이 커넥터

Citrix Gateway connector for Exchange ActiveSync는 Citrix ADC를 ActiveSync 트래픽의 프록시로 사용하여 경계에서 ActiveSync 필터링을 제공합니다. 결과적으로 필터링 구성 요소는 메일 트래픽 흐름 경로에 위치하여 메일이 환경에 들어오거나 나갈 때 가로챕니다. Citrix Gateway connector for Exchange ActiveSync는 Citrix ADC와 XenMobile Server 간의 중개자 역할을 합니다. 장치가 Citrix ADC의 ActiveSync 가상 서버를 통해 Exchange와 통신할 때, Citrix ADC는 connector for Exchange ActiveSync 서비스에 HTTP 콜아웃을 수행합니다. 이 서비스는 XenMobile을 통해 장치 상태를 확인합니다. 장치 상태에 따라 connector for Exchange ActiveSync는 Citrix ADC에 연결을 허용하거나 거부하도록 응답합니다. 사용자, 에이전트 및 장치 유형 또는 ID를 기반으로 액세스를 필터링하는 정적 규칙을 구성할 수도 있습니다.

이 설정은 Exchange ActiveSync 서비스를 인터넷에 노출시키면서 무단 액세스를 방지하기 위한 추가 보안 계층을 제공합니다. 설계 고려 사항은 다음과 같습니다.

- Windows Server: Exchange ActiveSync 구성 요소용 커넥터에는 Windows Server가 필요합니다.

- 필터링 규칙 세트: Exchange ActiveSync용 커넥터는 사용자 정보보다는 장치 상태 및 정보를 기반으로 필터링하도록 설계되었습니다. 사용자 ID로 필터링하는 정적 규칙을 구성할 수 있지만, 예를 들어 Active Directory 그룹 멤버십을 기반으로 필터링하는 옵션은 없습니다. Active Directory 그룹 필터링이 필요한 경우 Endpoint Management connector for Exchange ActiveSync를 대신 사용할 수 있습니다.
- Citrix ADC 확장성: Citrix ADC를 통해 ActiveSync 트래픽을 프록시해야 하는 요구 사항을 고려할 때, 모든 ActiveSync SSL 연결의 추가 워크로드를 지원하려면 Citrix ADC 인스턴스의 적절한 크기 조정이 중요합니다.
- Citrix ADC 통합 캐싱: Citrix ADC의 Exchange ActiveSync용 커넥터 구성은 통합 캐싱 기능을 사용하여 Exchange ActiveSync용 커넥터의 응답을 캐시합니다. 이 구성의 결과로 Citrix ADC는 주어진 세션의 모든 ActiveSync 트랜잭션에 대해 Citrix Gateway connector for Exchange ActiveSync에 요청을 발행할 필요가 없습니다. 이 구성은 적절한 성능과 확장을 위해서도 중요합니다. 통합 캐싱은 Citrix ADC Platinum Edition에서 사용할 수 있으며, Enterprise Edition의 경우 기능을 별도로 라이선스할 수 있습니다.
- 사용자 지정 필터링 정책: 표준 기본 모바일 클라이언트 외의 특정 ActiveSync 클라이언트를 제한하기 위해 사용자 지정 Citrix ADC 정책을 생성해야 할 수도 있습니다. 이 구성에는 ActiveSync HTTP 요청 및 Citrix ADC 응답기 정책 생성에 대한 지식이 필요합니다.
- Secure Mail 클라이언트: Secure Mail은 경계에서 필터링할 필요가 없는 마이크로 VPN 기능을 가지고 있습니다. Secure Mail 클라이언트는 Citrix Gateway를 통해 연결될 때 일반적으로 내부(신뢰할 수 있는) ActiveSync 클라이언트로 취급됩니다. 기본 및 타사(Exchange ActiveSync용 커넥터 포함) 클라이언트와 Secure Mail 클라이언트 모두에 대한 지원이 필요한 경우: Citrix는 Secure Mail 트래픽이 Exchange ActiveSync용 커넥터에 사용되는 Citrix ADC 가상 서버를 통해 흐르지 않도록 권장합니다. 이 트래픽 흐름은 DNS를 통해 달성할 수 있으며, Exchange ActiveSync용 커넥터 정책이 Secure Mail 클라이언트에 영향을 미치지 않도록 할 수 있습니다.

XenMobile 배포에서 Citrix Gateway connector for Exchange ActiveSync 다이어그램은 온프레미스 배포를 위한 참조 아키텍처를 참조하십시오.

익스체인지 액티브싱크용 엔드포인트 관리 커넥터

Endpoint Management connector for Exchange ActiveSync는 Exchange 서비스 수준에서 ActiveSync 필터링을 제공하는 XenMobile 구성 요소입니다. 결과적으로 필터링은 메일이 XenMobile 환경에 들어올 때가 아니라 Exchange 서비스에 도달한 후에만 발생합니다. Mail Manager는 PowerShell을 사용하여 Exchange ActiveSync에서 장치 파트너십 정보를 쿼리하고 장치 격리 작업을 통해 액세스를 제어합니다. 이러한 작업은 Endpoint Management connector for Exchange ActiveSync 규칙 기준에 따라 장치를 격리 상태로 만들거나 격리 해제합니다. Citrix Gateway connector for Exchange ActiveSync와 유사하게, Endpoint Management connector for Exchange ActiveSync는 XenMobile을 통해 장치 상태를 확인하여

장치 규정 준수 여부에 따라 액세스를 필터링합니다. 장치 유형 또는 ID, 에이전트 버전 및 Active Directory 그룹 멤버십을 기반으로 액세스를 필터링하는 정적 규칙을 구성할 수도 있습니다.

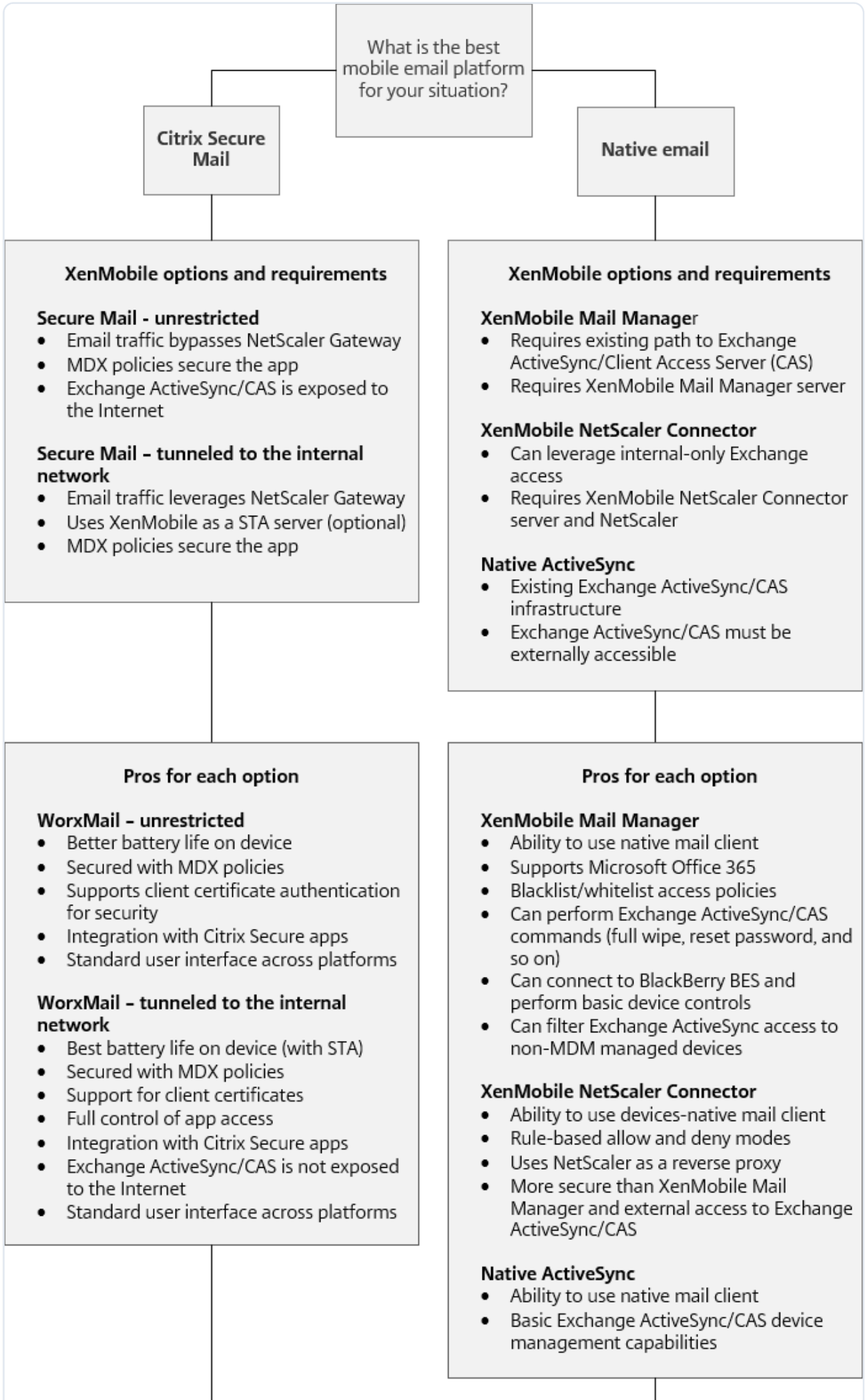
이 솔루션은 Citrix ADC 사용을 요구하지 않습니다. 기존 ActiveSync 트래픽에 대한 라우팅 변경 없이 Exchange ActiveSync용 Endpoint Management 커넥터를 배포할 수 있습니다. 설계 고려 사항은 다음과 같습니다.

- Windows Server: Exchange ActiveSync 구성 요소용 Endpoint Management 커넥터를 사용하려면 Windows Server를 배포해야 합니다.
- 필터링 규칙 세트: Exchange ActiveSync용 Citrix Gateway 커넥터와 마찬가지로, Exchange ActiveSync용 Endpoint Management 커넥터에는 장치 상태를 평가하는 필터링 규칙이 포함되어 있습니다. 또한, Exchange ActiveSync용 Endpoint Management 커넥터는 Active Directory 그룹 멤버십을 기반으로 필터링하는 정적 규칙도 지원합니다.
- Exchange 통합: Exchange ActiveSync용 Endpoint Management 커넥터는 ActiveSync 역할을 호스팅하는 Exchange 클라이언트 액세스 서버(CAS)에 대한 직접 액세스와 장치 격리 작업에 대한 제어를 필요로 합니다. 이 요구 사항은 환경 아키텍처 및 보안 상태에 따라 문제가 될 수 있습니다. 이 기술적 요구 사항을 사전에 평가하는 것이 중요합니다.
- 다른 ActiveSync 클라이언트: Exchange ActiveSync용 Endpoint Management 커넥터는 ActiveSync 서비스 수준에서 필터링하므로, XenMobile 환경 외부의 다른 ActiveSync 클라이언트를 고려해야 합니다. 다른 ActiveSync 클라이언트에 의도치 않은 영향을 미치지 않도록 Exchange ActiveSync용 Endpoint Management 커넥터 정적 규칙을 구성할 수 있습니다.
- 확장된 Exchange 기능: Exchange ActiveSync와의 직접 통합을 통해 Exchange ActiveSync용 Endpoint Management 커넥터는 XenMobile이 모바일 장치에서 Exchange ActiveSync 초기화를 수행할 수 있는 기능을 제공합니다. Exchange ActiveSync용 Endpoint Management 커넥터는 또한 XenMobile이 Blackberry 장치에 대한 정보에 액세스하고 다른 제어 작업을 수행할 수 있도록 합니다.

XenMobile 배포에서 Exchange ActiveSync용 Endpoint Management 커넥터 다이어그램은 온프레미스 배포를 위한 참조 아키텍처를 참조하십시오.

이메일 플랫폼 의사 결정 트리

다음 그림은 XenMobile 배포에서 기본 이메일 또는 Secure Mail 솔루션을 사용하는 것의 장단점을 구분하는 데 도움이 됩니다. 각 선택은 서버, 네트워크 및 데이터베이스 액세스를 활성화하기 위한 관련 XenMobile 옵션 및 요구 사항을 허용합니다. 장단점에는 보안, 정책 및 사용자 인터페이스 고려 사항에 대한 세부 정보가 포함됩니다.


What is the best mobile email platform for your situation?
Citrix Secure Mail
Native email
XenMobile options and requirements
Secure Mail - unrestricted
• Email traffic bypasses NetScaler Gateway
• MDX policies secure the app
• Exchange ActiveSync/CAS is exposed to the Internet
Secure Mail – tunneled to the internal network
• Email traffic leverages NetScaler Gateway
• Uses XenMobile as a STA server (optional)
• MDX policies secure the app
XenMobile options and requirements
XenMobile Mail Manager
• Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
• Requires XenMobile Mail Manager server
XenMobile NetScaler Connector
• Can leverage internal-only Exchange access
• Requires XenMobile NetScaler Connector server and NetScaler
Native ActiveSync
• Existing Exchange ActiveSync/CAS infrastructure
• Exchange ActiveSync/CAS must be externally accessible
Pros for each option
WorxMail – unrestricted
• Better battery life on device
• Secured with MDX policies
• Supports client certificate authentication for security
• Integration with Citrix Secure apps
• Standard user interface across platforms
WorxMail – tunneled to the internal network
• Best battery life on device (with STA)
• Secured with MDX policies
• Support for client certificates
• Full control of app access
• Integration with Citrix Secure apps
• Exchange ActiveSync/CAS is not exposed to the Internet
• Standard user interface across platforms
Pros for each option
XenMobile Mail Manager
• Ability to use native mail client
• Supports Microsoft Office 365
• Blacklist/whitelist access policies
• Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
• Can connect to BlackBerry BES and perform basic device controls
• Can filter Exchange ActiveSync access to non-MDM managed devices
XenMobile NetScaler Connector
• Ability to use devices-native mail client
• Rule-based allow and deny modes
• Uses NetScaler as a reverse proxy
• More secure than XenMobile Mail Manager and external access to Exchange ActiveSync/CAS
Native ActiveSync
• Ability to use native mail client
• Basic Exchange ActiveSync/CAS device management capabilities

XenMobile® 통합

이 문서에서는 XenMobile을 기존 네트워크 및 솔루션과 통합하는 방법을 계획할 때 고려해야 할 사항을 다룹니다. 예를 들어, Virtual Apps and Desktops에 Citrix ADC를 이미 사용하고 있는 경우:

- 기존 Citrix ADC 인스턴스를 사용하시겠습니까, 아니면 새 전용 인스턴스를 사용하시겠습니까?
- StoreFront™를 사용하여 게시된 HDX 앱을 XenMobile과 통합하시겠습니까?
- XenMobile과 함께 Citrix Files를 사용할 계획이십니까?
- XenMobile에 통합하려는 네트워크 액세스 제어 솔루션이 있습니까?
- 네트워크의 모든 아웃바운드 트래픽에 웹 프록시를 배포하십니까?

시트릭스 ADC 및 시트릭스 게이트웨이

XenMobile ENT 및 MAM 모드에는 Citrix Gateway가 필수입니다. Citrix Gateway는 모든 기업 리소스에 대한 액세스를 위한 마이크로 VPN 경로를 제공하며 강력한 다단계 인증을 지원합니다. 모든 XenMobile Server 장치 모드에는 Citrix ADC 로드 밸런싱이 필요합니다.

- 여러 XenMobile Server가 있는 경우
- 또는 XenMobile Server가 DMZ 또는 내부 네트워크 내에 있는 경우(따라서 트래픽이 장치에서 Citrix ADC를 거쳐 XenMobile로 흐르는 경우)

기존 Citrix ADC 인스턴스를 사용하거나 XenMobile용 새 인스턴스를 설정할 수 있습니다. 다음 섹션에서는 기존 또는 새 전용 Citrix ADC 인스턴스를 사용하는 것의 장점과 단점을 설명합니다.

XenMobile용으로 생성된 Citrix Gateway VIP가 있는 공유 Citrix ADC MPX

장점:

- 모든 Citrix 원격 연결(Citrix Virtual Apps and Desktops™, 전체 VPN 및 클라이언트 없는 VPN)에 공통 Citrix ADC 인스턴스를 사용합니다.
- 인증서 인증 및 DNS, LDAP, NTP와 같은 서비스 액세스를 위해 기존 Citrix ADC 구성을 사용합니다.
- 단일 Citrix ADC 플랫폼 라이선스를 사용합니다.

단점:

- 동일한 Citrix ADC에서 두 가지 다른 사용 사례를 처리할 때 확장을 계획하기가 더 어렵습니다.
- 때로는 Citrix Virtual Apps™ and Desktops 사용 사례에 특정 Citrix ADC 버전이 필요할 수 있습니다. 이 동일한 버전에는 XenMobile에 알려진 문제가 있을 수 있습니다. 또는 XenMobile에 Citrix ADC 버전에 알려진 문제가 있을 수 있습니다.
- Citrix Gateway가 이미 있는 경우, XenMobile용 Citrix ADC 구성을 생성하기 위해 XenMobile 마법사용 Citrix ADC를 두 번째로 실행할 수 없습니다.

- Citrix Gateway 11.1 이상에 Platinum 라이선스가 사용되는 경우를 제외하고: Citrix ADC에 설치되고 VPN 연결에 필요한 사용자 액세스 라이선스는 풀링됩니다. 이러한 라이선스는 모든 Citrix ADC 가상 서버에서 사용할 수 있으므로 XenMobile 이외의 서비스에서 잠재적으로 이를 사용할 수 있습니다.

전용 Citrix ADC VPX/MPX 인스턴스

장점:

Citrix는 전용 Citrix ADC 인스턴스를 사용하는 것을 권장합니다.

- 확장 계획이 더 쉽고, 이미 리소스 제약이 있을 수 있는 Citrix ADC 인스턴스에서 XenMobile 트래픽을 분리합니다.
- XenMobile과 Citrix Virtual Apps and Desktops가 다른 Citrix ADC 소프트웨어 버전을 필요로 할 때 발생하는 문제를 방지합니다. 일반적으로 XenMobile에 대해 최신 호환 Citrix ADC 버전 및 빌드를 사용하는 것이 좋습니다.
- 내장된 XenMobile 마법사용 Citrix ADC를 통해 Citrix ADC의 XenMobile 구성을 허용합니다.
- 서비스의 가상 및 물리적 분리.
- Citrix Gateway 11.1 이상에 Platinum 라이선스가 사용되는 경우를 제외하고: XenMobile에 필요한 사용자 액세스 라이선스는 Citrix ADC의 XenMobile 서비스에서만 사용할 수 있습니다.

단점:

- XenMobile 구성을 지원하기 위해 Citrix ADC에 추가 서비스 설정이 필요합니다.
- 다른 Citrix ADC 플랫폼 라이선스가 필요합니다. Citrix Gateway용 Citrix ADC 인스턴스마다 라이선스를 부여해야 합니다.

각 XenMobile Server 모드에 Citrix ADC 및 Citrix Gateway를 통합할 때 고려해야 할 사항에 대한 자세한 내용은 Citrix ADC 및 Citrix Gateway 통합을 참조하십시오.

StoreFront

Citrix Virtual Apps and Desktops 환경이 있는 경우 StoreFront를 사용하여 HDX™ 애플리케이션을 XenMobile과 통합할 수 있습니다. HDX 앱을 XenMobile과 통합할 때 다음 사항이 적용됩니다.

- XenMobile에 등록된 사용자가 앱을 사용할 수 있습니다.
- 앱은 다른 모바일 앱과 함께 XenMobile Store에 표시됩니다.
- XenMobile은 StoreFront에서 레거시 PNAgent (서비스) 사이트를 사용합니다.
- Citrix Receiver™가 장치에 설치되면 HDX 앱은 Receiver를 사용하여 시작됩니다.

StoreFront는 StoreFront 인스턴스당 하나의 서비스 사이트라는 제한이 있습니다. 여러 스토어가 있고 다른 프로덕션 사용량과 분리하려는 경우 Citrix는 일반적으로 XenMobile용 새 StoreFront 인스턴스 및 서비스 사이트를 고려할 것을 권장합니다.

고려 사항은 다음과 같습니다.

- StoreFront에 대한 다른 인증 요구 사항이 있습니까? StoreFront 서비스 사이트에는 로그온을 위한 Active Directory 자격 증명이 필요합니다. 인증서 기반 인증만 사용하는 고객은 동일한 Citrix Gateway를 사용하여 XenMobile을 통해 애플리케이션을 열거할 수 없습니다.
- 동일한 스토어를 사용합니까, 아니면 새 스토어를 만듭니까?
- 동일한 StoreFront 서버를 사용합니까, 아니면 다른 서버를 사용합니까?

다음 섹션에서는 Receiver 및 모바일 생산성 앱에 대해 별도의 또는 결합된 StoreFront를 사용하는 것의 장점과 단점을 설명합니다.

기존 StoreFront 인스턴스를 XenMobile Server와 통합

장점:

- 동일한 스토어: HDX 액세스에 동일한 Citrix ADC VIP를 사용한다고 가정할 경우, XenMobile에 대해 StoreFront의 추가 구성이 필요하지 않습니다. 동일한 스토어를 사용하고 Receiver 액세스를 새 Citrix ADC VIP로 지정하려는 경우, StoreFront에 적절한 Citrix Gateway 구성을 추가하십시오.
- 동일한 StoreFront 서버: 기존 StoreFront 설치 및 구성을 사용합니다.

단점:

- 동일한 스토어: Virtual Apps and Desktops 워크로드를 지원하기 위한 StoreFront의 재구성은 XenMobile에도 부정적인 영향을 미칠 수 있습니다.
- 동일한 StoreFront 서버: 대규모 환경에서는 앱 열거 및 시작을 위한 PNAgent의 XenMobile 사용으로 인한 추가 로드를 고려하십시오.

XenMobile Server 통합을 위해 새 전용 StoreFront 인스턴스 사용

장점:

- 새 스토어: XenMobile용 StoreFront 스토어의 구성 변경 사항은 기존 Virtual Apps and Desktops 워크로드에 영향을 주지 않아야 합니다.
- 새 StoreFront 서버: 서버 구성 변경 사항은 Virtual Apps and Desktops 워크플로에 영향을 주지 않아야 합니다. 또한 앱 열거 및 시작을 위한 PNAgent의 XenMobile 사용 외의 로드는 확장성에 영향을 주지 않아야 합니다.

단점:

- 새 스토어: StoreFront 스토어 구성.
- 새 StoreFront 서버: 새로운 StoreFront 설치 및 구성이 필요합니다.

자세한 내용은 XenMobile 설명서의 Virtual Apps and Desktops through Citrix Secure Hub를 참조하십시오.

쉐어파일 및 시트릭스 파일

> **면책 조항:**

> ShareFile(현재 Progress)이 지원을 중단하면 이 기능은 더 이상 사용되지 않습니다.

> Citrix Files를 통해 사용자는 모든 장치에서 모든 데이터에 액세스하고 동기화할 수 있습니다. Citrix Files를 사용하면 조직 내부 및 외부의 사람들과 데이터를 안전하게 공유할 수 있습니다. ShareFile을 XenMobile Advanced Edition 또는 Enterprise Edition과 통합하는 경우 XenMobile은 Citrix Files에 다음을 제공할 수 있습니다.

- XenMobile 앱 사용자를 위한 단일 Sign-On 인증.
- Active Directory 기반 사용자 계정 프로비저닝.
- 포괄적인 액세스 제어 정책.

모바일 사용자는 전체 Enterprise 계정 기능 세트의 이점을 누릴 수 있습니다.

또는 XenMobile을 스토리지 영역 커넥터와만 통합하도록 구성할 수 있습니다. 스토리지 영역 커넥터를 통해 Citrix Files는 다음 항목에 대한 액세스를 제공합니다.

- 문서 및 폴더
- 네트워크 파일 공유
- SharePoint 사이트에서: 사이트 모음 및 문서 라이브러리.

연결된 파일 공유에는 Citrix Virtual Apps and Desktops 환경에서 사용되는 것과 동일한 네트워크 홈 드라이브가 포함될 수 있습니다. XenMobile 콘솔을 사용하여 Citrix Files 또는 스토리지 영역 커넥터와의 통합을 구성합니다. 자세한 내용은 Citrix Files use with XenMobile를 참조하십시오.

다음 섹션에서는 Citrix Files에 대한 설계 결정을 내릴 때 고려해야 할 질문을 설명합니다.

Citrix Files 또는 스토리지 영역 커넥터만 통합

질문:

- Citrix 관리 스토리지 영역에 데이터를 저장하시겠습니까?
- 사용자에게 파일 공유 및 동기화 기능을 제공하시겠습니까?
- 사용자가 Citrix Files 웹사이트에서 파일에 액세스하도록 허용하시겠습니까? 아니면 모바일 장치에서 Office 365 콘텐츠 및 개인 클라우드 커넥터에 액세스하도록 허용하시겠습니까?

설계 결정:

- 이러한 질문 중 하나라도 "예"라고 답하면 Citrix Files와 통합하십시오.
- 스토리지 영역 커넥터만 통합하면 iOS 사용자에게 SharePoint 사이트 및 네트워크 파일 공유와 같은 기존 온프레미스 스토리지 리포지토리에 대한 보안 모바일 액세스를 제공합니다. 이 구성에서는 ShareFile 하위 도메인을 설정하거나, Citrix Files에 사용자를 프로비저닝하거나, Citrix Files 데이터를 호스팅하지 않습니다. XenMobile과 함께 스토리지 영역 커넥터를 사용하면 기업 네트워크 외부로 사용자 정보가 유출되는 것을 방지하는 보안 제한 사항을 준수합니다.

스토리지 영역 컨트롤러 서버 위치

질문:

- 온프레미스 스토리지 또는 스토리지 영역 커넥터와 같은 기능이 필요하십니까?
- Citrix Files의 온프레미스 기능을 사용하는 경우 스토리지 영역 컨트롤러는 네트워크의 어디에 위치합니까?

설계 결정:

- 스토리지 영역 컨트롤러 서버를 Citrix Files 클라우드, 온프레미스 단일 테넌트 스토리지 시스템 또는 지원되는 타사 클라우드 스토리지 중 어디에 배치할지 결정하십시오.
- 스토리지 영역 컨트롤러는 Citrix Files Control Plane과 통신하기 위해 일부 인터넷 액세스가 필요합니다. 직접 액세스, NAT/PAT 구성 또는 프록시 구성 등 여러 가지 방법으로 연결할 수 있습니다.

스토리지 영역 커넥터

질문 사항:

- CIFS 공유 경로는 무엇입니까?
- SharePoint URL은 무엇입니까?

설계 결정:

- 해당 위치에 액세스하는 데 온프레미스 스토리지 영역 컨트롤러가 필요한지 확인합니다.
- 파일 리포지토리, CIFS 공유 및 SharePoint와 같은 내부 리소스와의 스토리지 영역 커넥터 통신으로 인해 Citrix는 스토리지 영역 컨트롤러가 DMZ 방화벽 뒤의 내부 네트워크에 상주하고 Citrix ADC에 의해 전면에 배치될 것을 권장합니다.

XenMobile Enterprise와의 SAML 통합

질문 사항:

- Citrix Files에 Active Directory 인증이 필요합니까?
- XenMobile용 Citrix Files 앱을 처음 사용할 때 SSO가 필요합니까?
- 현재 환경에 표준 IdP가 있습니까?
- SAML을 사용하려면 몇 개의 도메인이 필요합니까?
- Active Directory 사용자를 위한 여러 이메일 별칭이 있습니까?
- 진행 중이거나 곧 예정된 Active Directory 도메인 마이그레이션이 있습니까?

설계 결정:

XenMobile Enterprise 환경에서는 Citrix Files의 인증 메커니즘으로 SAML을 사용할 수 있습니다. 인증 옵션은 다음과 같습니다.

- SAML용 IdP(Identity Provider)로 XenMobile Server를 사용합니다.

이 옵션은 탁월한 사용자 경험을 제공하고 Citrix Files 계정 생성을 자동화하며 모바일 앱 SSO 기능을 활성화할 수 있습니다.

- XenMobile Server는 이 프로세스를 위해 향상되었습니다. Active Directory 동기화가 필요하지 않습니다.
- 사용자 프로비저닝을 위해 Citrix Files 사용자 관리 도구를 사용합니다.
- 지원되는 타사 공급업체를 SAML용 IdP로 사용

기존에 지원되는 IdP가 있고 모바일 앱 SSO 기능이 필요하지 않은 경우 이 옵션이 가장 적합할 수 있습니다. 이 옵션은 계정 프로비저닝을 위해 Citrix Files 사용자 관리 도구를 사용하는 것도 필요합니다.

ADFS와 같은 타사 IdP 솔루션을 사용하면 Windows 클라이언트 측에서도 SSO 기능을 제공할 수 있습니다. Citrix Files SAML IdP를 선택하기 전에 사용 사례를 평가해야 합니다.

또한 두 가지 사용 사례를 모두 충족하기 위해 ADFS와 XenMobile을 이중 IdP로 구성할 수 있습니다.

모바일 앱

질문:

- 어떤 Citrix Files 모바일 앱을 사용할 계획입니까(공개, MDM, MDX)?

설계 결정:

- Apple App Store 및 Google Play Store에서 모바일 생산성 앱을 배포합니다. 이러한 공개 앱 스토어 배포를 통해 Citrix 다운로드 페이지에서 래핑된 앱을 얻을 수 있습니다.
- 보안 수준이 낮고 컨테이너화가 필요하지 않은 경우, 공개 Citrix Files 애플리케이션이 적합하지 않을 수 있습니다. MDM 전용 환경에서는 MDM 모드에서 XenMobile을 사용하여 Citrix Files 앱의 MDM 버전을 제공할 수 있습니다.
- 자세한 내용은 앱 및 XenMobile용 Citrix Files를 참조하십시오.

보안, 정책 및 액세스 제어

질문:

- 데스크톱, 웹 및 모바일 사용자에게 어떤 제한이 필요합니까?
- 사용자에게 어떤 표준 액세스 제어 설정을 원하십니까?
- 어떤 파일 보존 정책을 사용할 계획입니까?

설계 결정:

- Citrix Files를 사용하면 직원 권한 및 장치 보안을 관리할 수 있습니다. 자세한 내용은 직원 권한 및 장치 및 앱 관리를 참조하십시오.
- 일부 Citrix Files 장치 보안 설정 및 MDX 정책은 동일한 기능을 제어합니다. 이러한 경우 XenMobile 정책이 우선하며, 그 다음으로 Citrix Files 장치 보안 설정이 적용됩니다. 예: Citrix Files에서 외부 앱을 비활성화했지만 XenMobile에서 활성화한 경우, 외부 앱은 Citrix Files에서 비활성화됩니다. XenMobile이 PIN/암호를 요구하지 않도록 앱을 구성할 수 있지만, Citrix Files 앱은 PIN/암호를 요구합니다.

표준 스토리지 영역 대 제한된 스토리지 영역

질문:

- 제한된 스토리지 영역이 필요합니까?

설계 결정:

- 표준 스토리지 영역은 중요하지 않은 데이터를 위한 것이며 직원이 비직원과 데이터를 공유할 수 있도록 합니다. 이 옵션은 도메인 외부에서 데이터를 공유하는 워크플로를 지원합니다.
- 제한된 스토리지 영역은 중요한 데이터를 보호합니다. 인증된 도메인 사용자만 해당 영역에 저장된 데이터에 액세스할 수 있습니다.

웹 프록시

HTTP(S)/SOCKS 프록시를 통해 XenMobile 트래픽을 라우팅하는 가장 가능성 있는 시나리오는 다음과 같습니다. XenMobile Server가 있는 서브넷에 필요한 Apple, Google 또는 Microsoft IP 주소에 대한 아웃바

운드 인터넷 액세스가 없는 경우입니다. XenMobile에서 프록시 서버 설정을 지정하여 모든 인터넷 트래픽을 프록시 서버로 라우팅할 수 있습니다. 자세한 내용은 프록시 서버 사용 설정을 참조하십시오.

다음 표에서는 XenMobile과 함께 사용되는 가장 일반적인 프록시의 장점과 단점을 설명합니다.

옵션	장점	단점
XenMobile Server와 함께 HTTP(S)/SOCKS 프록시 사용.	정책에서 XenMobile Server 서브넷의 아웃바운드 인터넷 연결을 허용하지 않는 경우: HTTP(S) 또는 SOCKS 프록시를 구성하여 인터넷 연결을 제공할 수 있습니다.	프록시 서버가 실패하면 APN(iOS) 또는 Firebase Cloud Messaging(Android) 연결이 끊어집니다. 결과적으로 모든 iOS 및 Android 장치에 대한 장치 알림이 실패합니다.
Secure Web과 함께 HTTP(S) 프록시 사용.	HTTP/HTTPS 트래픽을 모니터링하여 인터넷 활동이 조직의 표준을 준수하는지 확인할 수 있습니다.	이 구성에서는 모든 Secure Web 인터넷 트래픽이 인터넷으로 다시 전송되기 전에 회사 네트워크로 다시 터널링되어야 합니다. 인터넷 연결이 브라우징을 제한하는 경우: 이 구성은 인터넷 브라우징 성능에 영향을 미칠 수 있습니다.

분할 터널링에 대한 Citrix ADC 세션 프로필 구성은 트래픽에 다음과 같이 영향을 미칩니다.

Citrix ADC 분할 터널링이 **꺼져** 있을 때:

- MDX **네트워크 액세스** 정책이 **내부 네트워크로 터널링됨**으로 설정된 경우: 모든 트래픽은 마이크로 VPN 또는 클라이언트리스 VPN(cVPN) 터널을 통해 Citrix Gateway로 강제 적용됩니다.
- 프록시 서버에 대한 Citrix ADC 트래픽 정책/프로필을 구성하고 이를 Citrix Gateway VIP에 바인딩합니다.

> **중요:**
>
> 프록시에서 Secure Hub cVPN 트래픽을 제외해야 합니다.

- 자세한 내용은 보안 브라우징 모드에서 프록시 서버를 통한 XenMobile Secure Hub 트래픽을(를) 참조하십시오.

Citrix ADC 분할 터널링이 **켜짐**으로 설정된 경우:

- MDX **네트워크 액세스** 정책이 **내부 네트워크로 터널링됨**으로 설정된 앱의 경우: 앱은 먼저 웹 리소스를 직접 가져오려고 시도합니다. 웹 리소스가 공개적으로 사용 가능하지 않은 경우, 해당 앱은 Citrix Gateway로 대체됩니다.
- 프록시 서버에 대한 Citrix ADC 트래픽 정책 및 프로필을 구성합니다. 그런 다음 해당 정책 및 프로필을 Citrix Gateway VIP에 바인딩합니다.

> **중요:**

> 프록시에서 Secure Hub cVPN 트래픽을 제외해야 합니다.

> **분할 DNS**에 대한 Citrix ADC 세션 프로필 구성(**클라이언트 환경** 아래)은 분할 터널링과 유사하게 작동합니다.

분할 DNS가 활성화되고 **모두**로 설정된 경우:

- 클라이언트는 먼저 FQDN을 로컬에서 확인하려고 시도하고 실패 시 DNS 확인을 위해 Citrix ADC로 대체됩니다.

분할 DNS가 **원격**으로 설정된 경우:

- DNS 확인은 Citrix ADC에서만 발생합니다.

Split DNS가 **로컬**로 설정된 경우:

- 클라이언트는 FQDN을 로컬에서 확인하려고 시도합니다. Citrix ADC는 DNS 확인에 사용되지 않습니다.

액세스 제어

기업은 네트워크 내부 및 외부에서 모바일 장치를 관리할 수 있습니다. XenMobile과 같은 엔터프라이즈 모빌리티 관리 솔루션은 위치에 관계없이 모바일 장치에 대한 보안 및 제어를 제공하는 데 탁월합니다. 그러나 네트워크 액세스 제어(NAC) 솔루션과 결합하면 네트워크 내부에 있는 장치에 QoS 및 보다 세분화된 제어를 추가할 수 있습니다. 이러한 조합을 통해 NAC 솔루션을 통해 XenMobile 장치 보안 평가를 확장할 수 있습니다. 그러면 NAC 솔루션은 XenMobile 보안 평가를 사용하여 인증 결정을 촉진하고 처리할 수 있습니다.

NAC 정책을 적용하려면 다음 솔루션 중 하나를 사용할 수 있습니다.

- 시트릭스 게이트웨이
- 시스코 아이덴티티 서비스 엔진 (ISE)

- ForeScout

Citrix는 다른 NAC 솔루션과의 통합을 보장하지 않습니다.

XenMobile과 NAC 솔루션 통합의 장점은 다음과 같습니다.

- 엔터프라이즈 네트워크의 모든 엔드포인트에 대한 향상된 보안, 규정 준수 및 제어.
- NAC 솔루션은 다음을 수행할 수 있습니다.
  - 장치가 네트워크에 연결을 시도하는 즉시 장치를 감지합니다.
  - 장치 속성에 대해 XenMobile에 쿼리합니다.
  - 해당 장치 정보를 사용하여 해당 장치를 허용, 차단, 제한 또는 리디렉션할지 여부를 결정합니다. 이러한 결정은 적용하려는 보안 정책에 따라 달라집니다.
- NAC 솔루션은 IT 관리자에게 관리되지 않거나 규정을 준수하지 않는 장치에 대한 가시성을 제공합니다.

XenMobile에서 지원하는 NAC 규정 준수 필터에 대한 설명과 구성 개요는 네트워크 액세스 제어를 참조하십시오.

다중 사이트 요구 사항

고가용성 및 재해 복구를 위해 여러 사이트를 포함하는 XenMobile® 배포를 설계하고 구성할 수 있습니다. 이 문서에서는 XenMobile 배포에 사용되는 고가용성 및 재해 복구 모델에 대한 개요를 제공합니다.

고가용성

- XenMobile 클러스터 노드의 경우 Citrix ADC가 로드 밸런싱을 처리합니다. 자세한 내용은 클러스터링 구성을 참조하십시오.
- XenMobile Server 노드는 활성/활성 구성으로 작동합니다.
- 용량이 필요함에 따라 더 많은 XenMobile Server 노드가 고가용성 클러스터에 추가됩니다. 하나의 노드는 최대 약 8,500개의 사용자 장치를 처리할 수 있습니다 (자세한 내용은 확장성 및 성능 참조).
- Citrix®는 "n+1" XenMobile Server 구성을 권장합니다. 즉, 8,500개의 사용자 장치당 하나의 서버와 이중화를 위한 추가 서버 하나입니다.
- Citrix는 가능한 모든 경우에 모든 Citrix ADC 인스턴스에 대해 고가용성을 구성하여 구성이 두 번째 Citrix ADC와 동기화되도록 권장합니다.
- 표준 Citrix ADC 고가용성 쌍은 활성/수동 구성으로 작동합니다.

일반적인 고가용성 XenMobile 배포에는 일반적으로 다음이 포함됩니다.

- 두 개의 Citrix ADC 인스턴스(VPX 또는 MPX). Citrix ADC SDX 플랫폼을 사용하는 경우 고가용성도 고려해야 합니다.

- 동일한 데이터베이스 설정으로 구성된 두 개 이상의 XenMobile Server.

재해 복구

하나의 활성 데이터 센터와 하나의 수동 데이터 센터를 사용하여 두 데이터 센터에 걸쳐 재해 복구를 위해 XenMobile을 구성할 수 있습니다. Citrix ADC 및 GSLB(Global Server Load Balancing)는 활성/활성 데이터 경로를 생성하는 데 사용되므로 사용자 경험은 활성/활성 설정과 동일합니다.

재해 복구를 위한 XenMobile 배포에는 다음이 포함됩니다.

- 두 개의 데이터 센터 - 각 데이터 센터에는 하나 이상의 Citrix ADC 인스턴스, XenMobile 서버 및 SQL Server 데이터베이스가 포함됩니다.
- 데이터 센터로 트래픽을 전달하는 GSLB 서버. GSLB 서버는 XenMobile 등록 URL과 사이트로 트래픽을 처리하는 Citrix Gateway URL 모두에 대해 구성됩니다.
- XenMobile 마법사용 Citrix ADC를 사용하여 Citrix Gateway를 구성할 때, 기본적으로 GSLB는 XenMobile 등록 서버로의 트래픽과 MAM 로드 밸런싱 서버로 가는 Citrix Gateway로의 트래픽을 해결하도록 설정되어 있지 않습니다. 결과적으로 추가 단계가 필요합니다. 이러한 단계를 준비하고 구현하는 방법에 대한 자세한 내용은 재해 복구를 참조하십시오.
- Always On 가용성 그룹의 클러스터형 SQL Server.
- XenMobile 서버와 SQL Server 간의 지연 시간은 5ms 미만이어야 합니다.

> **참고:**
>
> 이 핸드북에 설명된 재해 복구 방법은 액세스 계층에 대한 자동화된 재해 복구만 제공합니다. 장치가 XenMobile 서버에 연결하기 전에 장애 조치 사이트에서 모든 XenMobile 서버 노드와 SQL Server 데이터베이스를 수동으로 시작해야 합니다.

Citrix Gateway 및 Citrix ADC와 통합

XenMobile®과 통합하면 Citrix Gateway는 MAM 장치용 내부 네트워크에 대한 원격 장치 액세스를 위한 인증 메커니즘을 제공합니다. 이 통합을 통해 모바일 생산성 앱은 마이크로 VPN을 통해 인트라넷의 회사 서버에 연결할 수 있습니다. 마이크로 VPN은 모바일 장치의 앱에서 Citrix Gateway로 생성됩니다. Citrix Gateway는 모든 회사 리소스에 액세스하기 위한 마이크로 VPN 경로를 제공하고 강력한 다단계 인증을 지원합니다.

다음 경우에 모든 XenMobile Server 장치 모드에 Citrix ADC 로드 밸런싱이 필요합니다.

- 여러 XenMobile Server가 있는 경우

- 또는 XenMobile Server가 DMZ 또는 내부 네트워크 내에 있는 경우(따라서 트래픽이 장치에서 Citrix ADC를 거쳐 XenMobile로 흐르는 경우)

XenMobile Server 모드에 대한 통합 요구 사항

Citrix Gateway 및 Citrix ADC에 대한 통합 요구 사항은 XenMobile Server 모드(MAM, MDM, ENT)에 따라 다릅니다.

MAM

MAM 모드의 XenMobile Server의 경우:

- **Citrix Gateway**가 필요합니다. Citrix Gateway는 모든 회사 리소스에 액세스하기 위한 마이크로 VPN 경로를 제공하고 강력한 다단계 인증을 지원합니다.
- 로드 밸런싱을 위해 **Citrix ADC**를 권장합니다.

  Citrix는 XenMobile 앞에 로드 밸런서가 필요한 고가용성 구성으로 XenMobile을 배포할 것을 권장합니다. 자세한 내용은 MAM 및 레거시 MAM 모드 정보를 참조하십시오.

MDM

MDM 모드의 XenMobile Server의 경우:

- Citrix Gateway는 필수가 아닙니다. MDM 배포의 경우 Citrix는 모바일 장치 VPN에 Citrix Gateway를 권장합니다.
- Citrix ADC는 보안 및 로드 밸런싱에 권장됩니다.

  Citrix는 보안 및 로드 밸런싱을 위해 XenMobile Server 앞에 Citrix ADC 어플라이언스를 배포할 것을 권장합니다. DMZ에 XenMobile이 있는 표준 배포의 경우, Citrix는 SSL Bridge 모드의 XenMobile Server 로드 밸런싱과 함께 XenMobile용 Citrix ADC 마법사를 권장합니다. 다음 배포에서는 SSL 오프로드를 고려할 수도 있습니다.

  - XenMobile Server가 DMZ가 아닌 내부 네트워크에 상주하는 경우.
  - 또는 보안 팀에서 SSL Bridge 구성을 요구하는 경우.

  Citrix는 NAT 또는 기존 타사 프록시 또는 로드 밸런서를 통해 XenMobile Server를 인터넷에 노출하는 것을 MDM에 권장하지 않습니다. 이러한 구성은 SSL 트래픽이 XenMobile Server(SSL Bridge)에서 종료되더라도 잠재적인 보안 위험을 초래합니다.

  높은 보안 환경의 경우, 기본 XenMobile 구성의 Citrix ADC는 보안 요구 사항을 충족하거나 초과합니다.

최고의 보안 요구 사항을 가진 MDM 환경의 경우, Citrix ADC에서의 SSL 종료를 통해 경계에서 트래픽을 검사하면서 종단 간 SSL 암호화를 유지할 수 있습니다. 자세한 내용은 보안 요구 사항을 참조하십시오. Citrix ADC는 SSL/TLS 암호 및 SSL FIPS Citrix ADC 하드웨어를 정의하는 옵션을 제공합니다.

ENT (MAM+MDM)

ENT 모드의 XenMobile Server 사용 시:

- Citrix Gateway가 필요합니다. Citrix Gateway는 모든 회사 리소스에 대한 액세스를 위한 마이크로 VPN 경로를 제공하고 강력한 다단계 인증을 지원합니다.

  XenMobile Server 모드가 ENT이고 사용자가 MDM 등록을 거부하면 장치는 레거시 MAM 모드에서 작동합니다. 레거시 MAM 모드에서는 Citrix Gateway FQDN을 사용하여 장치를 등록합니다. 자세한 내용은 MAM 및 레거시 MAM 모드 정보를 참조하십시오.
- Citrix ADC는 로드 밸런싱에 권장됩니다. 자세한 내용은 이 문서의 앞부분에 있는 "MDM" 아래의 Citrix ADC 지점을 참조하십시오.

> **중요:**
>
> 초기 등록의 경우, 로드 밸런싱 가상 서버를 SSL 오프로드 또는 SSL Bridge로 구성했는지 여부에 관계없이 사용자 장치에서 오는 트래픽은 XenMobile Server에서 인증됩니다.

설계 결정

다음 섹션에서는 XenMobile과 Citrix Gateway 통합을 계획할 때 고려해야 할 다양한 설계 결정을 요약합니다.

라이선스 및 에디션

결정 세부 정보:

- 어떤 Citrix ADC 에디션을 사용할 계획입니까?
- Citrix ADC에 플랫폼 라이선스를 적용했습니까?
- MAM 기능을 사용해야 하는 경우 Citrix ADC Universal Access Licenses를 적용했습니까?

설계 지침:

Citrix Gateway에 적절한 라이선스를 적용했는지 확인하십시오. Exchange ActiveSync용 Citrix Gateway connector™를 사용하는 경우 통합 캐싱이 필요할 수 있습니다. 따라서 적절한 Citrix ADC Edition이 설치되어 있는지 확인해야 합니다.

Citrix ADC 기능을 활성화하기 위한 라이선스 요구 사항은 다음과 같습니다.

- XenMobile MDM 로드 밸런싱에는 최소한 Citrix ADC 표준 플랫폼 라이선스가 필요합니다.
- 스토리지 영역 컨트롤러를 사용하는 ShareFile 로드 밸런싱에는 최소한 Citrix ADC 표준 플랫폼 라이선스가 필요합니다.
- XenMobile Advanced Edition (온프레미스) 또는 Citrix Endpoint Management™ (클라우드)에는 MAM에 필요한 Citrix Gateway Universal 라이선스가 포함되어 있습니다.
- Exchange 로드 밸런싱에는 Citrix ADC Platinum 플랫폼 라이선스 또는 통합 캐싱 라이선스가 추가된 Citrix ADC Enterprise 플랫폼 라이선스가 필요합니다.

XenMobile용 Citrix ADC 버전

결정 세부 정보:

- XenMobile 환경에서 실행 중인 Citrix ADC 버전은 무엇입니까?
- 별도의 인스턴스가 필요합니까?

설계 지침:

Citrix는 Citrix Gateway 가상 서버에 전용 Citrix ADC 인스턴스를 사용할 것을 권장합니다. XenMobile 환경에 필요한 최소 Citrix ADC 버전 및 빌드가 사용 중인지 확인하십시오. 일반적으로 XenMobile에 최신 호환 Citrix ADC 버전 및 빌드를 사용하는 것이 가장 좋습니다. Citrix Gateway를 업그레이드하면 기존 환경에 영향을 미치는 경우 XenMobile용 두 번째 전용 인스턴스가 적절할 수 있습니다.

XenMobile 및 VPN 연결을 사용하는 다른 앱에 Citrix ADC 인스턴스를 공유할 계획이라면 두 가지 모두에 충분한 VPN 라이선스가 있는지 확인하십시오. XenMobile 테스트 및 프로덕션 환경은 Citrix ADC 인스턴스를 공유할 수 없다는 점을 명심하십시오.

인증서

결정 세부 정보:

- XenMobile 환경 등록 및 액세스에 더 높은 수준의 보안이 필요합니까?
- LDAP는 옵션이 아닙니까?

설계 지침:

XenMobile의 기본 구성은 사용자 이름 및 암호 인증입니다. XenMobile 환경 등록 및 액세스에 보안 계층을 추가하려면 인증서 기반 인증 사용을 고려하십시오. LDAP와 함께 인증서를 사용하여 2단계 인증을 수행하면 RSA 서버 없이도 더 높은 수준의 보안을 제공할 수 있습니다.

LDAP를 허용하지 않고 스마트 카드 또는 유사한 방법을 사용하는 경우 인증서를 구성하면 XenMobile에 스마트 카드를 나타낼 수 있습니다. 그러면 사용자는 XenMobile이 생성한 고유 PIN을 사용하여 등록합니다. 사용자가 액세스 권한을 얻으면 XenMobile은 XenMobile 환경에 인증하는 데 사용되는 인증서를 생성하고 배포합니다.

XenMobile은 타사 인증 기관에 대해서만 CRL(인증서 해지 목록)을 지원합니다. Microsoft CA가 구성된 경우 XenMobile은 Citrix ADC를 사용하여 해지를 관리합니다. 클라이언트 인증서 기반 인증을 구성할 때 Citrix ADC CRL(인증서 해지 목록) 설정인 **CRL 자동 새로 고침 사용**을 구성해야 하는지 고려하십시오. 이 단계는 MAM에만 등록된 장치 사용자가 장치의 기존 인증서를 사용하여 인증할 수 없도록 합니다. XenMobile은 사용자가 해지된 경우 사용자 인증서를 생성하는 것을 제한하지 않으므로 새 인증서를 다시 발급합니다. 이 설정은 CRL이 만료된 PKI 엔터티를 확인할 때 PKI 엔터티의 보안을 강화합니다.

네트워킹 토폴로지

결정 세부 정보:

- 어떤 Citrix ADC 토폴로지가 필요합니까?

설계 지침:

Citrix는 XenMobile에 Citrix ADC 인스턴스를 사용할 것을 권장합니다. 그러나 내부 네트워크에서 DMZ로 트래픽이 나가는 것을 원하지 않을 수도 있습니다. 이 경우 추가 Citrix ADC 인스턴스를 설정하는 것을 고려하십시오. 내부 사용자용 Citrix ADC 인스턴스 하나와 외부 사용자용 Citrix ADC 인스턴스 하나를 사용하십시오. 사용자가 내부 및 외부 네트워크 간에 전환할 때 DNS 레코드 캐싱으로 인해 Secure Hub 로그인 프롬프트가 증가할 수 있습니다.

XenMobile은 Citrix Gateway 이중 홉을 지원하지 않습니다.

전용 또는 공유 Citrix Gateway VIP

결정 세부 정보:

- 현재 Virtual Apps and Desktops에 Citrix Gateway를 사용하고 있습니까?
- XenMobile이 Virtual Apps and Desktops와 동일한 Citrix Gateway를 사용하도록 계획하고 있습니까?
- 두 트래픽 흐름에 대한 인증 요구 사항은 무엇입니까?

설계 지침:

Citrix 환경에 XenMobile과 Virtual Apps and Desktops가 모두 포함된 경우, 동일한 Citrix ADC 인스턴스와 Citrix Gateway 가상 서버를 둘 다에 사용할 수 있습니다. 잠재적인 버전 충돌 및 환경 격리 문제로 인해 각 XenMobile 환경에 전용 Citrix ADC 인스턴스와 Citrix Gateway를 사용하는 것이 좋습니다. 그러나 전용 Citrix ADC 인스턴스를 사용할 수 없는 경우, Citrix는 Secure Hub의 트래픽 흐름을 분리하기 위해 전용

Citrix Gateway 가상 서버를 사용할 것을 권장합니다. 이 구성은 XenMobile과 Virtual Apps and Desktops 간에 공유되는 가상 서버 대신 사용됩니다.

LDAP 인증을 사용하는 경우, Receiver와 Secure Hub는 문제 없이 동일한 Citrix Gateway에 인증할 수 있습니다. 인증서 기반 인증을 사용하는 경우, XenMobile은 MDX 컨테이너에 인증서를 푸시하고 Secure Hub는 이 인증서를 사용하여 Citrix Gateway에 인증합니다. Receiver는 Secure Hub와 별개이며 Secure Hub와 동일한 인증서를 사용하여 동일한 Citrix Gateway에 인증할 수 없습니다.

두 개의 Citrix Gateway VIP에 동일한 FQDN을 사용할 수 있도록 하는 다음 해결 방법을 고려할 수 있습니다.

- 동일한 IP 주소를 가진 두 개의 Citrix Gateway VIP를 생성합니다. Secure Hub용 VIP는 표준 443 포트를 사용하고 Virtual Apps and Desktops(Receiver를 배포하는)용 VIP는 444 포트를 사용합니다.
- 결과적으로 하나의 FQDN이 동일한 IP 주소로 확인됩니다.
- 이 해결 방법의 경우, 기본 포트 443 대신 포트 444에 대한 ICA 파일을 반환하도록 StoreFront™를 구성할 수 있습니다. 이 해결 방법은 사용자가 포트 번호를 입력할 필요가 없습니다.

Citrix Gateway 시간 초과

결정 세부 정보:

- XenMobile 트래픽에 대한 Citrix Gateway 시간 초과를 어떻게 구성하시겠습니까?

설계 지침:

Citrix Gateway에는 세션 시간 초과 및 강제 시간 초과 설정이 포함되어 있습니다. 자세한 내용은 권장 구성을 참조하십시오. 백그라운드 서비스, Citrix ADC 및 오프라인 상태에서 애플리케이션에 액세스하기 위한 시간 초과 값은 서로 다르다는 점을 명심하십시오.

MAM용 XenMobile 로드 밸런서 IP 주소

결정 세부 정보:

- VIP에 내부 또는 외부 IP 주소를 사용하고 있습니까?

설계 지침:

Citrix Gateway VIP에 공용 IP 주소를 사용할 수 있는 환경에서 이러한 방식으로 XenMobile 로드 밸런싱 VIP 및 주소를 할당하면 등록 실패가 발생합니다.

이 시나리오에서 등록 실패를 방지하려면 로드 밸런싱 VIP가 내부 IP를 사용하도록 하십시오. 이 가상 IP 주소는 RFC 1918 개인 IP 주소 표준을 따라야 합니다. 이 가상 서버에 비공개 IP 주소를 사용하는 경우 Citrix ADC는 인증 프로세스 중에 XenMobile Server에 성공적으로 연결할 수 없습니다. 자세한 내용은 `<https://support.citrix.com/article/CTX200430>`을 참조하십시오.

MDM 로드 밸런싱 메커니즘

결정 세부 정보:

- Citrix Gateway는 XenMobile Server의 로드 밸런싱을 어떻게 수행합니까?

설계 지침:

XenMobile이 DMZ에 있는 경우 SSL Bridge를 사용합니다. XenMobile이 내부 네트워크에 있는 경우 보안 표준을 충족하기 위해 필요한 경우 SSL Offload를 사용합니다.

- SSL Bridge 모드에서 Citrix ADC VIP를 사용하여 XenMobile Server의 로드 밸런싱을 수행하면 인터넷 트래픽이 XenMobile Server로 직접 흐르고, 여기서 연결이 종료됩니다. SSL Bridge 모드는 설정 및 문제 해결이 가장 간단한 모드입니다.
- SSL Offload 모드에서 Citrix ADC VIP를 사용하여 XenMobile Server의 로드 밸런싱을 수행하면 인터넷 트래픽이 Citrix ADC로 직접 흐르고, 여기서 연결이 종료됩니다. 그런 다음 Citrix ADC는 Citrix ADC에서 XenMobile Server로 새 세션을 설정합니다. SSL Offload 모드는 설정 및 문제 해결 시 추가적인 복잡성을 수반합니다.

SSL Offload를 사용한 MDM 로드 밸런싱을 위한 서비스 포트

결정 세부 정보:

- 로드 밸런싱에 SSL Offload 모드를 사용할 계획이라면 백엔드 서비스는 어떤 포트를 사용합니까?

설계 지침:

SSL Offload의 경우 다음과 같이 포트 80 또는 8443을 선택합니다.

- 진정한 오프로딩을 위해 XenMobile Server로 다시 포트 80을 사용합니다.
- 종단 간 암호화, 즉 트래픽 재암호화는 지원되지 않습니다. 자세한 내용은 Citrix 지원 문서인 NetScaler와 XenMobile Server 간 지원되는 아키텍처를 참조하십시오.

등록 FQDN

결정 세부 정보:

- 등록 및 XenMobile 인스턴스/로드 밸런싱 VIP에 사용할 FQDN은 무엇입니까?

설계 지침:

클러스터의 첫 번째 XenMobile Server 초기 구성에는 XenMobile Server FQDN을 제공해야 합니다. 해당 FQDN은 MDM VIP URL 및 내부 MAM LB VIP URL과 일치해야 합니다. (내부 Citrix ADC 주소 레코드가

MAM LB VIP를 확인합니다.) 자세한 내용은 이 문서의 뒷부분에 나오는 "각 관리 모드에 대한 등록 FQDN"을 참조하십시오.

또한 다음 인증서와 동일한 인증서를 사용해야 합니다.

- XenMobile SSL 수신기 인증서
- 내부 MAM LB VIP 인증서
- MDM VIP 인증서(MDM VIP에 SSL 오프로드 사용 시)

> **중요:**
>
> 등록 FQDN을 구성한 후에는 변경할 수 없습니다. 새 등록 FQDN에는 새 SQL Server 데이터베이스와 XenMobile Server 재구축이 필요합니다.

Secure Web 트래픽

결정 세부 정보:

- Secure Web을 내부 웹 브라우징으로만 제한할 계획입니까?
- Secure Web을 내부 및 외부 웹 브라우징 모두에 사용할 계획입니까?

설계 지침:

Secure Web을 내부 웹 브라우징에만 사용할 계획이라면 Citrix Gateway 구성은 간단합니다. Secure Web은 기본적으로 모든 내부 사이트에 연결되어야 합니다. 방화벽 및 프록시 서버를 구성해야 할 수도 있습니다.

Secure Web을 내부 및 외부 브라우징 모두에 사용할 계획이라면 SNIP가 아웃바운드 인터넷 액세스를 갖도록 설정해야 합니다. IT 부서는 일반적으로 등록된 장치(MDX 컨테이너 사용)를 회사 네트워크의 확장으로 간주합니다. 따라서 IT 부서는 일반적으로 Secure Web 연결이 Citrix ADC로 돌아와 프록시 서버를 거쳐 인터넷으로 나가기를 원합니다. 기본적으로 Secure Web은 모든 네트워크 액세스에 대해 애플리케이션별 VPN 터널을 사용하여 내부 네트워크로 돌아갑니다. Citrix ADC는 분할 터널 설정을 사용합니다.

Secure Web 연결에 대한 자세한 내용은 사용자 연결 구성을 참조하십시오.

Secure Mail용 푸시 알림

결정 세부 정보:

- 푸시 알림을 사용할 계획입니까?

iOS용 설계 지침:

Citrix Gateway 구성에는 스플릿 터널링이 해제된 Secure Ticket Authority (STA)가 포함될 수 있습니다. Citrix Gateway는 iOS용 Secure Mail 푸시 알림에 지정된 Citrix 수신기 서비스 URL로 Secure Mail의 트래픽을 허용해야 합니다.

Android용 설계 지침:

Android 장치가 XenMobile에 연결해야 하는 방법과 시기를 제어하려면 Firebase Cloud Messaging (FCM)을 사용하십시오. FCM이 구성되면 모든 보안 작업 또는 배포 명령은 Secure Hub에 푸시 알림을 트리거하여 사용자에게 XenMobile Server에 다시 연결하도록 요청합니다.

HDX™ STA

결정 세부 정보:

- HDX 애플리케이션 액세스를 통합할 계획이라면 어떤 STA를 사용해야 합니까?

설계 지침:

HDX STA는 StoreFront의 STA와 일치해야 하며 Virtual Apps and Desktops 팜에 유효해야 합니다.

시트릭스 파일즈 및 쉐어파일

결정 세부 정보:

- 환경에서 스토리지 영역 컨트롤러를 사용할 계획입니까?
- 어떤 Citrix Files VIP URL을 사용할 계획입니까?

설계 지침:

환경에 스토리지 영역 컨트롤러를 포함하는 경우 다음을 올바르게 구성해야 합니다.

- Citrix Files 스위치 VIP (Citrix Files 제어 평면이 스토리지 영역 컨트롤러 서버와 통신하는 데 사용됨)
- Citrix Files 로드 밸런싱 VIP
- 모든 필수 정책 및 프로필

자세한 내용은 스토리지 영역 컨트롤러 설명서를 참조하십시오.

SAML IdP

결정 세부 정보:

- Citrix Files에 SAML이 필요한 경우 XenMobile을 SAML IdP로 사용하시겠습니까?

설계 지침:

권장되는 모범 사례는 Citrix Files를 XenMobile Advanced Edition 또는 XenMobile Advanced Edition (온프레미스) 또는 Citrix Endpoint Management (클라우드)와 통합하는 것입니다. 이는 SAML 기반 페더레이션을 구성하는 것보다 간단한 대안입니다. 이러한 XenMobile 에디션과 함께 Citrix Files를 사용할 때 XenMobile은 Citrix Files에 다음을 제공합니다.

- 모바일 생산성 앱 사용자의 단일 Sign-On (SSO) 인증
- Active Directory 기반 사용자 계정 프로비저닝
- 포괄적인 액세스 제어 정책

XenMobile 콘솔을 사용하면 Citrix Files 구성을 수행하고 서비스 수준 및 라이선스 사용량을 모니터링할 수 있습니다.

Citrix Files 클라이언트에는 두 가지 유형이 있습니다. XenMobile용 Citrix Files 클라이언트(래핑된 Citrix Files라고도 함)와 Citrix Files 모바일 클라이언트(래핑되지 않은 Citrix Files라고도 함)입니다. 차이점을 이해하려면 XenMobile용 Citrix Files 클라이언트가 Citrix Files 모바일 클라이언트와 다른 점을 참조하십시오.

XenMobile 및 ShareFile을 구성하여 SAML을 사용하여 다음 항목에 대한 SSO 액세스를 제공할 수 있습니다.

- Citrix Files 모바일 앱
- 웹사이트, Outlook 플러그인 또는 동기화 클라이언트와 같은 래핑되지 않은 Citrix Files 클라이언트

XenMobile을 Citrix Files의 SAML IdP로 사용하려면 적절한 구성이 마련되어 있는지 확인하십시오. 자세한 내용은 Citrix Files와 SSO를 위한 SAML을 참조하십시오.

ShareConnect 직접 연결

결정 세부 정보:

- 사용자가 ShareConnect를 실행하는 컴퓨터 또는 모바일 장치에서 직접 연결을 사용하여 호스트 컴퓨터에 액세스해야 합니까?

설계 지침:

ShareConnect를 사용하면 사용자가 iPad, Android 태블릿 및 Android 휴대폰을 통해 컴퓨터에 안전하게 연결하여 파일 및 응용 프로그램에 액세스할 수 있습니다. 직접 연결의 경우 XenMobile은 Citrix Gateway를 사용하여 로컬 네트워크 외부의 리소스에 대한 보안 액세스를 제공합니다. 구성 세부 정보는 ShareConnect를 참조하십시오.

각 관리 모드에 대한 등록 FQDN

관리 모드	등록 FQDN
필수 MDM 등록이 포함된 엔터프라이즈(MDM+MAM)	XenMobile 서버 FQDN
선택적 MDM 등록을 포함한 엔터프라이즈(MDM+MAM)	XenMobile 서버 FQDN 또는 Citrix Gateway FQDN
MDM 전용	XenMobile 서버 FQDN
MAM 전용(레거시)	시트릭스 게이트웨이 FQDN
MAM 전용	XenMobile 서버 FQDN

배포 요약

Citrix는 올바른 구성을 위해 XenMobile 마법사용 Citrix ADC를 사용할 것을 권장합니다. 마법사는 한 번만 사용할 수 있습니다. 테스트, 개발 및 프로덕션 환경과 같이 여러 XenMobile 인스턴스가 있는 경우 추가 환경에 대해 Citrix ADC를 수동으로 구성해야 합니다. 작동하는 환경이 있으면 XenMobile용 Citrix ADC를 수동으로 구성하기 전에 설정을 기록해 두십시오.

마법사를 사용할 때 내리는 주요 결정은 XenMobile Server와의 통신에 HTTPS를 사용할지 HTTP를 사용할지 여부입니다. HTTPS는 Citrix ADC와 XenMobile 간의 트래픽이 암호화되므로 안전한 백엔드 통신을 제공합니다. 재암호화는 XenMobile Server 성능에 영향을 미칩니다. HTTP는 더 나은 XenMobile Server 성능을 제공합니다. Citrix ADC와 XenMobile 간의 트래픽은 암호화되지 않습니다. 다음 표는 Citrix ADC 및 XenMobile Server에 대한 HTTP 및 HTTPS 포트 요구 사항을 보여줍니다.

HTTPS

Citrix는 일반적으로 Citrix ADC MDM 가상 서버 구성에 SSL Bridge를 권장합니다. MDM 가상 서버와 함께 Citrix ADC SSL 오프로드를 사용하는 경우 XenMobile은 백엔드 서비스로 포트 80만 지원합니다.

관리 모드	Citrix ADC 로드 밸런싱 방식	SSL 재암호화	XenMobile 서버 포트
MDM	SSL 브리지	해당 없음	443, 8443
MAM	SSL 오프로드	사용	8443

엔터프라이즈	MDM: SSL 브리지	해당 없음	443, 8443
엔터프라이즈	MAM: SSL 오프로드	활성화됨	8443

HTTP

관리 모드	Citrix ADC 로드 밸런싱 방식	SSL 재암호화	XenMobile 서버 포트
MDM	SSL 오프로드	지원되지 않음	80
MAM	SSL 오프로드	활성화됨	8443
엔터프라이즈	MDM: SSL 오프로드	지원되지 않음	80
엔터프라이즈	MAM: SSL 오프로드	활성화됨	8443

XenMobile 배포에서 Citrix Gateway 다이어그램은 온프레미스 배포를 위한 참조 아키텍처를 참조하십시오.

MDX 앱을 위한 SSO 및 프록시 고려 사항

Citrix ADC와 XenMobile 통합을 통해 사용자에게 모든 백엔드 HTTP/HTTPS 리소스에 대한 단일 Sign-On(SSO)을 제공할 수 있습니다. SSO 인증 요구 사항에 따라 MDX 앱에 대한 사용자 연결이 다음 옵션 중 하나를 사용하도록 구성할 수 있습니다.

- 클라이언트리스 VPN의 한 유형인 Secure Browse
- 전체 VPN 터널

Citrix ADC가 환경에서 SSO를 제공하는 가장 좋은 방법이 아닌 경우, 정책 기반 로컬 암호 캐싱을 사용하여 MDX 앱을 설정할 수 있습니다. 이 문서에서는 Secure Web에 중점을 두고 다양한 SSO 및 프록시 옵션을 살펴봅니다. 이 개념은 다른 MDX 앱에도 적용됩니다.

다음 흐름도는 SSO 및 사용자 연결에 대한 의사 결정 흐름을 요약합니다.

SSO 및 사용자 연결에 대한 의사 결정 흐름도(/en-us/xenmobile/server/media/sso-proxy-decision-flow.png)

Citrix ADC 인증 방법

이 섹션에서는 Citrix ADC에서 지원하는 인증 방법에 대한 일반적인 정보를 제공합니다.

SAML 인증

Citrix ADC를 SAML(Security Assertion Markup Language)에 대해 구성하면 사용자는 단일 Sign-On을 위한 SAML 프로토콜을 지원하는 웹 앱에 연결할 수 있습니다. Citrix Gateway는 SAML 웹 앱에 대한 IdP(ID 공급자) 단일 Sign-On을 지원합니다.

필수 구성:

- Citrix ADC 트래픽 프로필에서 SAML SSO를 구성합니다.
- 요청된 서비스에 대해 SAML IdP를 구성합니다.

NTLM 인증

세션 프로필에서 웹 앱에 대한 SSO가 활성화된 경우 Citrix ADC는 NTLM 인증을 자동으로 수행합니다.

필수 구성:

- Citrix ADC 세션 또는 트래픽 프로필에서 SSO를 활성화합니다.

Kerberos 가장

XenMobile®은 Secure Web에 대해서만 Kerberos를 지원합니다. Kerberos SSO용 Citrix ADC를 구성할 때 Citrix ADC는 사용자 암호를 사용할 수 있는 경우 가장을 사용합니다. 가장은 Citrix ADC가 사용자 자격 증명을 사용하여 Secure Web과 같은 서비스에 액세스하는 데 필요한 티켓을 얻는 것을 의미합니다.

필수 구성:

- 연결에서 Kerberos Realm을 식별할 수 있도록 Citrix ADC "Worx" 세션 정책을 구성합니다.
- Citrix ADC에서 Kerberos 제한 위임(KCD) 계정을 구성합니다. 해당 계정을 암호 없이 구성하고 XenMobile 게이트웨이의 트래픽 정책에 바인딩합니다.
- 이러한 및 기타 구성 세부 정보는 Citrix 블로그: WorxWeb 및 Kerberos 가장 SSO를 참조하십시오.

Kerberos 제한 위임

XenMobile은 Secure Web에 대해서만 Kerberos를 지원합니다. Kerberos SSO용 Citrix ADC를 구성할 때 Citrix ADC는 사용자 암호를 사용할 수 없는 경우 제한 위임을 사용합니다.

제한 위임을 사용하면 Citrix ADC는 지정된 관리자 계정을 사용하여 사용자 및 서비스를 대신하여 티켓을 가져옵니다.

필수 구성:

- 필요한 권한을 가진 Active Directory의 KCD 계정과 Citrix ADC의 KCD 계정을 구성합니다.
- Citrix ADC 트래픽 프로필에서 SSO를 활성화합니다.

- Kerberos 인증을 위해 백엔드 웹사이트를 구성합니다.

양식 채우기 인증

양식 기반 단일 Sign-On을 위해 Citrix ADC를 구성하면 사용자는 한 번 로그인하여 네트워크의 모든 보호된 앱에 액세스할 수 있습니다. 이 인증 방법은 Secure Browse 또는 Full VPN 모드를 사용하는 앱에 적용됩니다.

필수 구성:

- Citrix ADC 트래픽 프로필에서 양식 기반 SSO를 구성합니다.

다이제스트 HTTP 인증

세션 프로필에서 웹 앱에 대한 SSO를 활성화하면 Citrix ADC가 다이제스트 HTTP 인증을 자동으로 수행합니다. 이 인증 방법은 Secure Browse 또는 Full VPN 모드를 사용하는 앱에 적용됩니다.

필수 구성:

- Citrix ADC 세션 또는 트래픽 프로필에서 SSO를 활성화합니다.

기본 HTTP 인증

세션 프로필에서 웹 앱에 대한 SSO를 활성화하면 Citrix ADC가 기본 HTTP 인증을 자동으로 수행합니다. 이 인증 방법은 Secure Browse 또는 Full VPN 모드를 사용하는 앱에 적용됩니다.

필수 구성:

- Citrix ADC 세션 또는 트래픽 프로필에서 SSO를 활성화합니다.

Secure Browse, Full VPN Tunnel 또는 PAC를 사용하는 Full VPN Tunnel

다음 섹션에서는 Secure Web의 사용자 연결 유형에 대해 설명합니다. 자세한 내용은 Citrix 설명서의 Secure Web 문서인 사용자 연결 구성을 참조하십시오.

전체 VPN 터널

내부 네트워크로 터널링하는 연결은 전체 VPN 터널을 사용할 수 있습니다. Secure Web 기본 VPN 모드 정책을 사용하여 전체 VPN 터널을 구성합니다. Citrix는 클라이언트 인증서 또는 내부 네트워크의 리소스에 대한 종단 간 SSL을 사용하는 연결에 전체 VPN 터널을 권장합니다. 전체 VPN 터널은 TCP를 통한 모든 프로토콜을 처리합니다. Windows, Mac, iOS 및 Android 장치에서 전체 VPN 터널을 사용할 수 있습니다.

전체 VPN 터널 모드에서는 Citrix ADC가 HTTPS 세션 내부에 대한 가시성을 갖지 않습니다.

보안 브라우징

내부 네트워크로 터널링하는 연결은 Secure Browse라고 하는 클라이언트 없는 VPN의 변형을 사용할 수 있습니다. Secure Browse는 Secure Web **기본 VPN 모드** 정책에 지정된 기본 구성입니다. Citrix는 단일 Sign-On(SSO)이 필요한 연결에 Secure Browse를 권장합니다.

Secure Browse 모드에서 Citrix ADC는 HTTPS 세션을 두 부분으로 나눕니다.

- 클라이언트에서 Citrix ADC로
- Citrix ADC에서 백엔드 리소스 서버로.

이러한 방식으로 Citrix ADC는 클라이언트와 서버 간의 모든 트랜잭션에 대한 완전한 가시성을 확보하여 SSO를 제공할 수 있습니다.

보안 브라우징 모드에서 Secure Web을 사용할 때 프록시 서버를 구성할 수도 있습니다. 자세한 내용은 블로그 XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode를 참조하십시오.

PAC를 사용한 전체 VPN 터널

iOS 및 Android 장치에서 Secure Web에 대한 전체 VPN 터널 배포와 함께 프록시 자동 구성(PAC) 파일을 사용할 수 있습니다. XenMobile은 Citrix ADC에서 제공하는 프록시 인증을 지원합니다. PAC 파일에는 웹 브라우저가 특정 URL에 액세스하기 위해 프록시를 선택하는 방법을 정의하는 규칙이 포함되어 있습니다. PAC 파일 규칙은 내부 및 외부 사이트 모두에 대한 처리를 지정할 수 있습니다. Secure Web은 PAC 파일 규칙을 구문 분석하고 프록시 서버 정보를 Citrix Gateway로 보냅니다. Citrix Gateway는 PAC 파일 또는 프록시 서버를 인식하지 못합니다.

HTTPS 웹사이트에 대한 인증의 경우: Secure Web MDX 정책 **웹 암호 캐싱 사용**을 통해 Secure Web은 MDX를 통해 프록시 서버에 인증하고 SSO를 제공할 수 있습니다.

Citrix ADC 분할 터널링

SSO 및 프록시 구성을 계획할 때 Citrix ADC 분할 터널링을 사용할지 여부도 결정해야 합니다. Citrix는 필요한 경우에만 Citrix ADC 분할 터널링을 사용할 것을 권장합니다. 이 섹션에서는 분할 터널링 작동 방식에 대한 개략적인 설명을 제공합니다. Citrix ADC는 라우팅 테이블을 기반으로 트래픽 경로를 결정합니다. Citrix ADC 분할 터널링이 켜져 있으면 Secure Hub는 내부(보호된) 네트워크 트래픽과 인터넷 트래픽을 구분합니다. Secure Hub는 DNS 접미사 및 인트라넷 애플리케이션을 기반으로 해당 결정을 내립니다. 그런 다음 Secure Hub는 VPN 터널을 통해 내부 네트워크 트래픽만 터널링합니다. Citrix ADC 분할 터널링이 꺼져 있으면 모든 트래픽이 VPN 터널을 통과합니다.

- 보안상의 이유로 모든 트래픽을 모니터링하려는 경우 Citrix ADC 분할 터널링을 비활성화합니다. 결과적으로 모든 트래픽은 VPN 터널을 통해 이동합니다.

- PAC와 함께 전체 VPN 터널을 사용하는 경우 Citrix Gateway 분할 터널링을 비활성화해야 합니다. 분할 터널링이 켜져 있고 PAC 파일을 구성하면 PAC 파일 규칙이 Citrix ADC 분할 터널링 규칙을 재정의합니다. 트래픽 정책에 구성된 프록시 서버는 Citrix ADC 분할 터널링 규칙을 재정의하지 않습니다.

기본적으로 Secure Web의 **네트워크 액세스** 정책은 **내부 네트워크로 터널링됨**으로 설정됩니다. 이 구성에서는 MDX 앱이 Citrix ADC 분할 터널 설정을 사용합니다. **네트워크 액세스** 정책 기본값은 다른 일부 모바일 생산성 앱의 경우 다릅니다.

Citrix Gateway에는 마이크로 VPN 역방향 분할 터널 모드도 있습니다. 이 구성은 Citrix ADC로 터널링되지 않는 IP 주소의 제외 목록을 지원합니다. 대신 해당 주소는 장치 인터넷 연결을 사용하여 전송됩니다. 역방향 분할 터널링에 대한 자세한 내용은 Citrix Gateway 설명서를 참조하십시오.

XenMobile에는 **역방향 분할 터널 제외 목록**이 포함되어 있습니다. 특정 웹사이트가 Citrix Gateway를 통해 터널링되는 것을 방지하려면: 대신 LAN을 사용하여 연결하는 정규화된 도메인 이름(FQDN) 또는 DNS 접미사의 쉼표로 구분된 목록을 추가합니다. 이 목록은 역방향 분할 터널링용으로 구성된 Citrix Gateway의 Secure Browse 모드에만 적용됩니다.

인증

XenMobile® 배포에서 인증 구성 방법을 결정할 때 여러 고려 사항이 작용합니다. 이 섹션에서는 다음을 논의하여 인증에 영향을 미치는 다양한 요소를 이해하는 데 도움을 줍니다.

- 인증과 관련된 주요 MDX 정책, XenMobile 클라이언트 속성 및 Citrix Gateway 설정.
- 이러한 정책, 클라이언트 속성 및 설정이 상호 작용하는 방식.
- 각 선택의 장단점.

이 문서에는 보안 수준을 높이기 위한 권장 구성 세 가지 예도 포함되어 있습니다.

일반적으로 보안이 강화될수록 사용자가 더 자주 인증해야 하므로 사용자 경험은 최적화되지 않습니다. 이러한 우려 사항의 균형을 맞추는 방법은 조직의 요구 사항과 우선순위에 따라 달라집니다. 세 가지 권장 구성을 검토함으로써 사용 가능한 인증 조치의 상호 작용과 XenMobile 환경을 가장 잘 배포하는 방법에 대해 더 깊이 이해할 수 있습니다.

인증 모드

온라인 인증: 사용자가 XenMobile 네트워크에 액세스할 수 있도록 합니다. 인터넷 연결이 필요합니다.

오프라인 인증: 장치에서 발생합니다. 사용자는 보안 볼트를 잠금 해제하고 다운로드된 메일, 캐시된 웹사이트, 메모와 같은 항목에 오프라인으로 액세스할 수 있습니다.

인증 방법

단일 요소

LDAP: XenMobile에서 Lightweight Directory Access Protocol(LDAP)을 준수하는 Active Directory와 같은 하나 이상의 디렉터리에 대한 연결을 구성할 수 있습니다. 이는 회사 환경에서 단일 Sign-On(SSO)을 제공하는 데 일반적으로 사용되는 방법입니다. 등록 시 복잡한 암호, 암호 만료 및 계정 잠금의 보안을 유지하면서 LDAP를 통한 사용자 경험을 개선하기 위해 Active Directory 암호 캐싱과 함께 Citrix PIN을 선택할 수 있습니다.

자세한 내용은 도메인 또는 도메인 + STA를 참조하십시오.

클라이언트 인증서: XenMobile은 업계 표준 인증 기관과 통합하여 인증서를 온라인 인증의 유일한 방법으로 사용할 수 있습니다. XenMobile은 사용자 등록 후 이 인증서를 제공하며, 이 등록에는 일회용 암호, 초대 URL 또는 LDAP 자격 증명이 필요합니다. 클라이언트 인증서를 기본 인증 방법으로 사용하는 경우, 장치에서 인증서를 보호하기 위해 클라이언트 인증서 전용 환경에서 Citrix PIN이 필요합니다.

XenMobile은 타사 인증 기관에 대해서만 인증서 해지 목록(CRL)을 지원합니다. Microsoft CA가 구성된 경우 XenMobile은 Citrix ADC를 사용하여 해지를 관리합니다. 클라이언트 인증서 기반 인증을 구성할 때 Citrix ADC 인증서 해지 목록(CRL) 설정인 CRL 자동 새로 고침 사용을 구성해야 하는지 고려하십시오. 이 단계는 MAM 전용 모드의 장치 사용자가 장치의 기존 인증서를 사용하여 인증할 수 없도록 합니다. XenMobile은 인증서가 해지되더라도 사용자가 사용자 인증서를 생성하는 것을 제한하지 않으므로 새 인증서를 다시 발급합니다. 이 설정은 CRL이 만료된 PKI 엔터티를 확인할 때 PKI 엔터티의 보안을 강화합니다.

사용자를 위한 인증서 기반 인증을 사용하거나 장치 인증서 발급을 위해 엔터프라이즈 인증 기관(CA)을 사용하려는 경우 필요한 배포를 보여주는 다이어그램은 온프레미스 배포를 위한 참조 아키텍처를 참조하십시오.

이중 요소

LDAP + 클라이언트 인증서: XenMobile 환경에서 이 구성은 Citrix ADC에서 이중 요소 인증으로 제공되는 보안과 결합된 최상의 SSO 가능성과 함께 보안 및 사용자 경험의 최상의 조합입니다. LDAP와 클라이언트 인증서를 모두 사용하면 사용자가 아는 것(Active Directory 암호)과 사용자가 가지고 있는 것(장치의 클라이언트 인증서) 모두를 통해 보안을 제공합니다. Secure Mail(및 기타 일부 모바일 생산성 앱)은 올바르게 구성된 Exchange 클라이언트 액세스 서버 환경에서 클라이언트 인증서 인증을 통해 원활한 첫 사용자 경험을 자동으로 구성하고 제공할 수 있습니다. 최적의 유용성을 위해 이 옵션을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다.

LDAP + 토큰: 이 구성은 RADIUS 프로토콜을 사용하여 LDAP 자격 증명과 일회용 암호의 고전적인 구성을 허용합니다. 최적의 유용성을 위해 이 옵션을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다.

인증과 관련된 중요 정책, 설정 및 클라이언트 속성

다음 정책, 설정 및 클라이언트 속성은 다음 세 가지 권장 구성과 함께 사용됩니다.

MDX 정책

앱 암호: 켜짐으로 설정하면 비활성 기간 후 앱이 시작되거나 다시 시작될 때 앱 잠금을 해제하려면 Citrix PIN 또는 암호가 필요합니다. 기본값은 **켜짐**입니다.

모든 앱에 대한 비활성 타이머를 구성하려면 **설정** 탭의 **클라이언트 속성**에서 XenMobile 콘솔의 INACTIVITY_TIMER 값을 분 단위로 설정합니다. 기본값은 15분입니다. 비활성 타이머를 비활성화하여 앱이 시작될 때만 PIN 또는 암호 프롬프트가 나타나도록 하려면 값을 0으로 설정합니다.

> **참고:**
>
> 암호화 키 정책에 대해 오프라인 보안을 선택하면 이 정책이 자동으로 활성화됩니다.

> **온라인 세션 필요: 켜짐**으로 설정하면 사용자는 장치에서 앱에 액세스하기 위해 엔터프라이즈 네트워크에 연결되어 있고 활성 세션이 있어야 합니다. **꺼짐**으로 설정하면 장치에서 앱에 액세스하기 위해 활성 세션이 필요하지 않습니다. 기본값은 **꺼짐**입니다.

최대 오프라인 기간(시간): 앱 권한을 다시 확인하고 XenMobile에서 정책을 새로 고치지 않고 앱이 실행될 수 있는 최대 기간을 정의합니다. 최대 오프라인 기간을 설정할 때 iOS용 Secure Hub에 유효한 Citrix Gateway 토큰이 있으면 앱은 사용자에게 중단 없이 XenMobile에서 MDX 앱에 대한 새 정책을 검색합니다. Secure Hub에 유효한 Citrix ADC 토큰이 없으면 사용자는 앱 정책을 업데이트하기 위해 Secure Hub를 통해 인증해야 합니다. Citrix ADC 토큰은 Citrix Gateway 세션 비활성 또는 강제 세션 시간 초과 정책으로 인해 유효하지 않게 될 수 있습니다. 사용자가 Secure Hub에 다시 로그인하면 앱을 계속 실행할 수 있습니다.

사용자는 기간이 만료되기 30분, 15분, 5분 전에 로그인하도록 알림을 받습니다. 만료 후에는 사용자가 로그인할 때까지 앱이 잠깁니다. 기본값은 **72시간(3일)**입니다. 최소 기간은 1시간입니다.

> **참고:**
>
> 사용자가 자주 여행하고 국제 로밍을 사용할 수 있는 시나리오에서는 기본값인 72시간(3일)이 너무 짧을 수 있다는 점을 명심하십시오.

> **백그라운드 서비스 티켓 만료:** 백그라운드 네트워크 서비스 티켓이 유효하게 유지되는 기간입니다. Secure Mail이 Citrix Gateway를 통해 ActiveSync를 실행하는 Exchange Server에 연결할 때, XenMobile은 Secure Mail이 내부 Exchange Server에 연결하는 데 사용하는 토큰을 발급합니다. 이

> 속성 설정은 Secure Mail이 인증 및 Exchange Server 연결을 위해 새 토큰을 요구하지 않고 토큰을 사용할 수 있는 기간을 결정합니다. 시간 제한이 만료되면 사용자는 새 토큰을 생성하기 위해 다시 로그온해야 합니다. 기본값은 **168시간(7일)**입니다. 이 시간 제한이 만료되면 메일 알림이 중단됩니다.

온라인 세션 필수 유예 기간: 온라인 세션 필수 정책이 추가 사용을 방지하기 전(온라인 세션이 유효성 검사를 받을 때까지) 사용자가 앱을 오프라인으로 사용할 수 있는 시간을 분 단위로 결정합니다. 기본값은 0(유예 기간 없음)입니다.

인증 정책에 대한 자세한 내용은 다음을 참조하십시오.

- MAM SDK를 사용하는 경우: MAM SDK 개요
- MDX Toolkit을 사용하는 경우: iOS용 MDX 정책 및 Android용 MDX 정책

XenMobile 클라이언트 속성

> **참고:**

> 클라이언트 속성은 XenMobile에 연결하는 모든 장치에 적용되는 전역 설정입니다.

> **Citrix PIN:** 간단한 로그온 환경을 위해 Citrix PIN을 활성화하도록 선택할 수 있습니다. PIN을 사용하면 사용자는 Active Directory 사용자 이름 및 암호와 같은 다른 자격 증명을 반복해서 입력할 필요가 없습니다. Citrix PIN을 독립형 오프라인 인증으로만 구성하거나, PIN을 Active Directory 암호 캐싱과 결합하여 최적의 유용성을 위해 인증을 간소화할 수 있습니다. XenMobile 콘솔의 **설정 > 클라이언트 > 클라이언트 속성**에서 Citrix PIN을 구성합니다.

다음은 몇 가지 중요한 속성에 대한 요약입니다. 자세한 내용은 클라이언트 속성을 참조하십시오.

ENABLE_PASSCODE_AUTH

표시 이름: Citrix PIN 인증 활성화

이 키를 사용하면 Citrix PIN 기능을 켤 수 있습니다. Citrix PIN 또는 암호를 사용하면 사용자에게 Active Directory 암호 대신 사용할 PIN을 정의하라는 메시지가 표시됩니다.
ENABLE_PASSWORD_CACHING이 활성화되어 있거나 XenMobile이 인증서 인증을 사용하는 경우 이 설정을 활성화해야 합니다.

가능한 값: true 또는 **false**

기본값: false

ENABLE_PASSWORD_CACHING

표시 이름: 사용자 암호 캐싱 사용

이 키를 사용하면 사용자의 Active Directory 암호를 모바일 장치에 로컬로 캐시할 수 있습니다. 이 키를 true로 설정하면 사용자에게 Citrix PIN 또는 암호를 설정하라는 메시지가 표시됩니다. 이 키를 **true**로 설정할 때 **ENABLE_PASSCODE_AUTH** 키도 true로 설정해야 합니다.

가능한 값: true 또는 **false**

기본값: false

PASSCODE_STRENGTH

표시 이름: PIN 강도 요구 사항

이 키는 Citrix PIN 또는 암호의 강도를 정의합니다. 이 설정을 변경하면 다음에 인증하라는 메시지가 표시될 때 사용자에게 새 Citrix PIN 또는 암호를 설정하라는 메시지가 표시됩니다.

가능한 값: 낮음, **보통**, 또는 **강함**

기본값: 보통

INACTIVITY_TIMER

표시 이름: 비활성 타이머

이 키는 사용자가 장치를 비활성 상태로 두었다가 Citrix PIN 또는 암호를 입력하라는 메시지 없이 앱에 액세스할 수 있는 시간을 분 단위로 정의합니다. MDX 앱에 대해 이 설정을 사용하려면 **앱 암호** 설정을 **켜기**로 설정해야 합니다. **앱 암호** 설정이 **끄기**로 설정된 경우 사용자는 Secure Hub로 리디렉션되어 전체 인증을 수행합니다. 이 설정을 변경하면 다음에 사용자에게 인증하라는 메시지가 표시될 때 값이 적용됩니다. 기본값은 15분입니다.

ENABLE_TOUCH_ID_AUTH

표시 이름: Touch ID 인증 활성화

오프라인 인증을 위해 지문 판독기(iOS에서만) 사용을 허용합니다. 온라인 인증에는 여전히 기본 인증 방법이 필요합니다.

ENCRYPT_SECRETS_USING_PASSCODE

표시 이름: 암호로 비밀 암호화

이 키를 사용하면 민감한 데이터를 iOS 키체인과 같은 플랫폼 기반 기본 저장소 대신 모바일 장치의 비밀 금고에 저장할 수 있습니다. 이 구성 키는 주요 아티팩트의 강력한 암호화를 가능하게 하며, 사용자 엔트로피(사용자만 아는 사용자 생성 임의 PIN 코드)도 추가합니다.

가능한 값: true 또는 **false**

기본값: false

Citrix ADC 설정

세션 시간 초과: 이 설정을 활성화하면 Citrix ADC가 지정된 간격 동안 네트워크 활동을 감지하지 못할 경우 Citrix Gateway가 세션을 연결 해제합니다. 이 설정은 Citrix Gateway Plug-in, Citrix Receiver™, Secure Hub 또는 웹 브라우저를 통해 연결하는 사용자에게 적용됩니다. 기본값은 **1440분**입니다. 이 값을 0으로 설정하면 설정이 비활성화됩니다.

강제 시간 초과: 이 설정을 활성화하면 사용자가 무엇을 하든 시간 초과 간격이 경과한 후 Citrix Gateway가 세션을 연결 해제합니다. 시간 초과 간격이 경과하면 사용자가 연결 해제를 방지하기 위해 취할 수 있는 조치가 없습니다. 이 설정은 Citrix Gateway Plug-in, Citrix Receiver, Secure Hub 또는 웹 브라우저를 통해 연결하는 사용자에게 적용됩니다. Secure Mail이 특수 Citrix ADC 모드인 STA를 사용하는 경우, **강제 시간 초과** 설정은 Secure Mail 세션에 적용되지 않습니다. 기본값은 **1440분**입니다. 이 값을 비워두면 설정이 비활성화됩니다.

Citrix Gateway의 시간 초과 설정에 대한 자세한 내용은 Citrix ADC 설명서를 참조하십시오.

장치에 자격 증명을 입력하여 XenMobile로 인증하도록 사용자에게 메시지를 표시하는 시나리오에 대한 자세한 내용은 인증 프롬프트 시나리오를 참조하십시오.

기본 구성 설정

다음 설정은 다음에서 제공하는 기본값입니다.

- NetScaler® for XenMobile 마법사
- MAM SDK 또는 MDX Toolkit
- XenMobile 콘솔

설정	설정 위치	기본 설정
세션 제한 시간	시트릭스 게이트웨이	1440분
강제 제한 시간	시트릭스 게이트웨이	1440분
최대 오프라인 기간	MDX 정책	72시간

설정	설정 위치	기본 설정
백그라운드 서비스 티켓 만료	MDX 정책	168시간 (7일)
온라인 세션 필요	MDX 정책	끔
온라인 세션 필요 유예 기간	MDX 정책	0
앱 암호	MDX 정책	켬
암호를 사용하여 비밀 암호화	XenMobile 클라이언트 속성	거짓
Citrix PIN 인증 사용	XenMobile 클라이언트 속성	거짓
PIN 강도 요구 사항	XenMobile 클라이언트 속성	중간
PIN 유형	XenMobile 클라이언트 속성	숫자
사용자 암호 캐싱 사용	XenMobile 클라이언트 속성	거짓
비활성 타이머	XenMobile 클라이언트 속성	15
Touch ID 인증 사용	XenMobile 클라이언트 속성	거짓

권장 구성

이 섹션에서는 최저 보안 및 최적의 사용자 경험부터 최고 보안 및 더 침해적인 사용자 경험에 이르는 세 가지 XenMobile 구성 예시를 제공합니다. 이 예시들은 사용자가 자신의 구성을 어느 수준으로 설정할지 결정하는 데 유용한 참조점을 제공해야 합니다. 이러한 설정을 수정하면 다른 설정도 변경해야 할 수 있습니다. 예를 들어, 최대 오프라인 기간은 항상 세션 시간 초과보다 짧아야 합니다.

최고 보안

이 구성은 최고 수준의 보안을 제공하지만, 상당한 사용성 절충이 따릅니다.

설정	설정 위치	권장 설정	동작 영향
세션 시간 초과	시트릭스 게이트웨이	1440	사용자는 온라인 인증이 필요한 경우(24시간마다)에만 Secure Hub 자격 증명을 입력합니다.

강제 시간 초과	시트릭스 게이트웨이	1440	온라인 인증은 24시간마다 엄격하게 요구됩니다. 활동은 세션 수명을 연장하지 않습니다.
최대 오프라인 기간	MDX 정책	23	매일 정책 새로 고침이 필요합니다.
백그라운드 서비스 티켓 만료	MDX 정책	72시간	STA 시간 초과. 이는 Citrix Gateway 세션 토큰 없이 장기 세션을 허용합니다. Secure Mail의 경우, STA 시간 초과를 세션 시간 초과보다 길게 설정하면 사용자가 세션 만료 전에 앱을 열지 않아도 메일 알림이 중단되는 것을 방지할 수 있습니다.
온라인 세션 필요	MDX 정책	해제	앱을 사용하기 위해 유효한 네트워크 연결 및 Citrix Gateway 세션을 보장합니다.
온라인 세션 필수 유예 기간	MDX 정책	0	유예 기간 없음 (온라인 세션 필수를 활성화한 경우).
앱 암호	MDX 정책	켜기	애플리케이션에 암호가 필요합니다.
암호를 사용하여 비밀 암호화	XenMobile 클라이언트 속성	예	사용자 엔트로피에서 파생된 키가 볼트를 보호합니다.
Citrix PIN 인증 사용	XenMobile 클라이언트 속성	참	간소화된 인증 환경을 위해 Citrix PIN을 활성화합니다.
PIN 강도 요구 사항	XenMobile 클라이언트 속성	강함	높은 암호 복잡성 요구 사항.

PIN 유형	XenMobile 클라이언트 속성	영숫자	PIN은 영숫자 시퀀스입니다.
암호 캐싱 활성화	XenMobile 클라이언트 속성	거짓	Active Directory 암호는 캐시되지 않으며 Citrix PIN은 오프라인 인증에 사용됩니다.
비활성 타이머	XenMobile 클라이언트 속성	15	사용자가 이 기간 동안 MDX 앱 또는 Secure Hub를 사용하지 않으면 오프라인 인증을 요청합니다.
Touch ID 인증 사용	XenMobile 클라이언트 속성	거짓	iOS에서 오프라인 인증 사용 사례에 대해 Touch ID를 비활성화합니다.

더 높은 보안

보다 절충적인 접근 방식인 이 구성은 사용자가 7일 대신 최대 3일마다 더 자주 인증하도록 요구하며, 더 강력한 보안을 제공합니다. 인증 횟수가 증가하면 컨테이너가 더 자주 잠겨 장치를 사용하지 않을 때 데이터 보안을 보장합니다.

설정	**설정 위치**	**권장 설정**	**동작 영향**
세션 시간 초과	시트릭스 게이트웨이	4320	사용자는 온라인 인증이 필요할 때만(3일마다) Secure Hub 자격 증명을 입력합니다.
강제 시간 초과	Citrix 게이트웨이	값 없음	활동이 있는 경우 세션이 연장됩니다.
최대 오프라인 기간	MDX 정책	71	3일마다 정책 새로 고침이 필요합니다. 시간 차이는 세션 시간 초과 전에 새로 고침을 허용하기 위한 것입니다.

백그라운드 서비스 티켓 만료	MDX 정책	168시간	Citrix Gateway 세션 토큰 없이 장기 세션을 허용하는 STA에 대한 시간 초과입니다. Secure Mail의 경우, STA 시간 초과를 세션 시간 초과보다 길게 설정하면 사용자가 세션 만료 전에 앱을 열지 않아도 메일 알림이 중단되는 것을 방지할 수 있습니다.
온라인 세션 필요	MDX 정책	끔	앱을 사용하기 위한 유효한 네트워크 연결 및 Citrix Gateway 세션을 보장합니다.
온라인 세션 필수 유예 기간	MDX 정책	0	유예 기간 없음(온라인 세션 필수를 활성화한 경우).
앱 암호	MDX 정책	켬	애플리케이션에 암호가 필요합니다.
암호를 사용하여 비밀 암호화	XenMobile 클라이언트 속성	거짓	볼트 암호화를 위해 사용자 엔트로피를 요구하지 않습니다.
Citrix PIN 인증 활성화	XenMobile 클라이언트 속성	참	간소화된 인증 환경을 위해 Citrix PIN을 활성화합니다.
PIN 강도 요구 사항	XenMobile 클라이언트 속성	중간	중간 수준의 암호 복잡성 규칙을 적용합니다.
PIN 유형	XenMobile 클라이언트 속성	숫자	PIN은 숫자 시퀀스입니다.
암호 캐싱 활성화	XenMobile 클라이언트 속성	참	사용자 PIN은 Active Directory 암호를 캐시하고 보호합니다.

비활성 타이머	XenMobile 클라이언트 속성	30	사용자가 이 기간 동안 MDX 앱 또는 Secure Hub를 사용하지 않으면 오프라인 인증을 요청합니다.
Touch ID 인증 활성화	XenMobile 클라이언트 속성	참	iOS에서 오프라인 인증 사용 사례에 대해 Touch ID를 활성화합니다.

높은 보안

사용자에게 가장 편리한 이 구성은 기본 수준의 보안을 제공합니다.

설정	설정 위치	권장 설정	동작 영향
세션 시간 초과	Citrix Gateway (시트릭스 게이트웨이)	10080	사용자는 온라인 인증이 필요할 때만(7일마다) Secure Hub 자격 증명을 입력합니다.
강제 시간 초과	Citrix Gateway (시트릭스 게이트웨이)	값 없음	활동이 있으면 세션이 연장됩니다.
최대 오프라인 기간	MDX 정책	167	매주(7일마다) 정책 새로 고침이 필요합니다. 시간 차이는 세션 시간 초과 전에 새로 고침을 허용하기 위함입니다.
백그라운드 서비스 티켓 만료	MDX 정책	240	STA 시간 초과. Citrix Gateway 세션 토큰 없이 장기 세션을 허용합니다. Secure Mail의 경우, STA 시간 초과를 세션 시간 초과보다 길게 설정하면 사용자가 세션 만료 전에 앱을 열지 않아도 메일 알림이

			중단되는 것을 방지할 수 있습니다.
온라인 세션 필요	MDX 정책	끔	앱을 사용하기 위한 유효한 네트워크 연결 및 Citrix Gateway 세션을 보장합니다.
온라인 세션 필요 유예 기간	MDX 정책	0	유예 기간 없음 (온라인 세션 필요를 활성화한 경우).
앱 암호	MDX 정책	켬	애플리케이션에 암호가 필요합니다.
암호를 사용하여 비밀 암호화	XenMobile 클라이언트 속성	거짓	볼트 암호화를 위해 사용자 엔트로피를 요구하지 마십시오.
Citrix PIN 인증 사용	XenMobile 클라이언트 속성	참	간소화된 인증 환경을 위해 Citrix PIN을 사용하도록 설정합니다.
PIN 강도 요구 사항	XenMobile 클라이언트 속성	낮음	암호 복잡성 요구 사항 없음
PIN 유형	XenMobile 클라이언트 속성	숫자	PIN은 숫자 시퀀스입니다.
암호 캐싱 사용	XenMobile 클라이언트 속성	예	사용자 PIN은 Active Directory 암호를 캐시하고 보호합니다.
비활성 타이머	XenMobile 클라이언트 속성	90	사용자가 이 기간 동안 MDX 앱 또는 Secure Hub를 사용하지 않으면 오프라인 인증을 요청합니다.
Touch ID 인증 사용	XenMobile 클라이언트 속성	예	iOS에서 오프라인 인증 사용 사례에 대해 Touch ID를 활성화합니다.

단계별 인증 사용

일부 앱은 향상된 인증(예: 토큰 또는 공격적인 세션 시간 초과와 같은 보조 인증 요소)을 요구할 수 있습니다. 이 인증 방법은 MDX 정책을 통해 제어합니다. 이 방법은 또한 인증 방법을 제어하기 위한 별도의 가상 서버를 필요로 합니다(동일하거나 별도의 Citrix ADC 어플라이언스에서).

설정	설정 위치	권장 설정	동작 영향
대체 시트릭스 게이트웨이	MDX 정책	보조 Citrix ADC 어플라이언스의 FQDN 및 포트가 필요합니다.	보조 Citrix ADC 어플라이언스 인증 및 세션 정책에 의해 제어되는 향상된 인증을 허용합니다.

사용자가 대체 Citrix Gateway 인스턴스에 로그온하는 앱을 열면, 다른 모든 앱은 내부 네트워크와 통신하기 위해 해당 Citrix Gateway 인스턴스를 사용합니다. 세션은 향상된 보안이 적용된 Citrix Gateway 인스턴스에서 세션 시간이 초과될 때만 낮은 보안 Citrix Gateway 인스턴스로 다시 전환됩니다.

온라인 세션 필수 사용

Secure Web과 같은 특정 애플리케이션의 경우, 사용자가 인증된 세션을 가지고 있고 장치가 네트워크에 연결되어 있을 때만 앱을 실행하도록 할 수 있습니다. 이 정책은 해당 옵션을 적용하고 사용자가 작업을 마칠 수 있도록 유예 기간을 허용합니다.

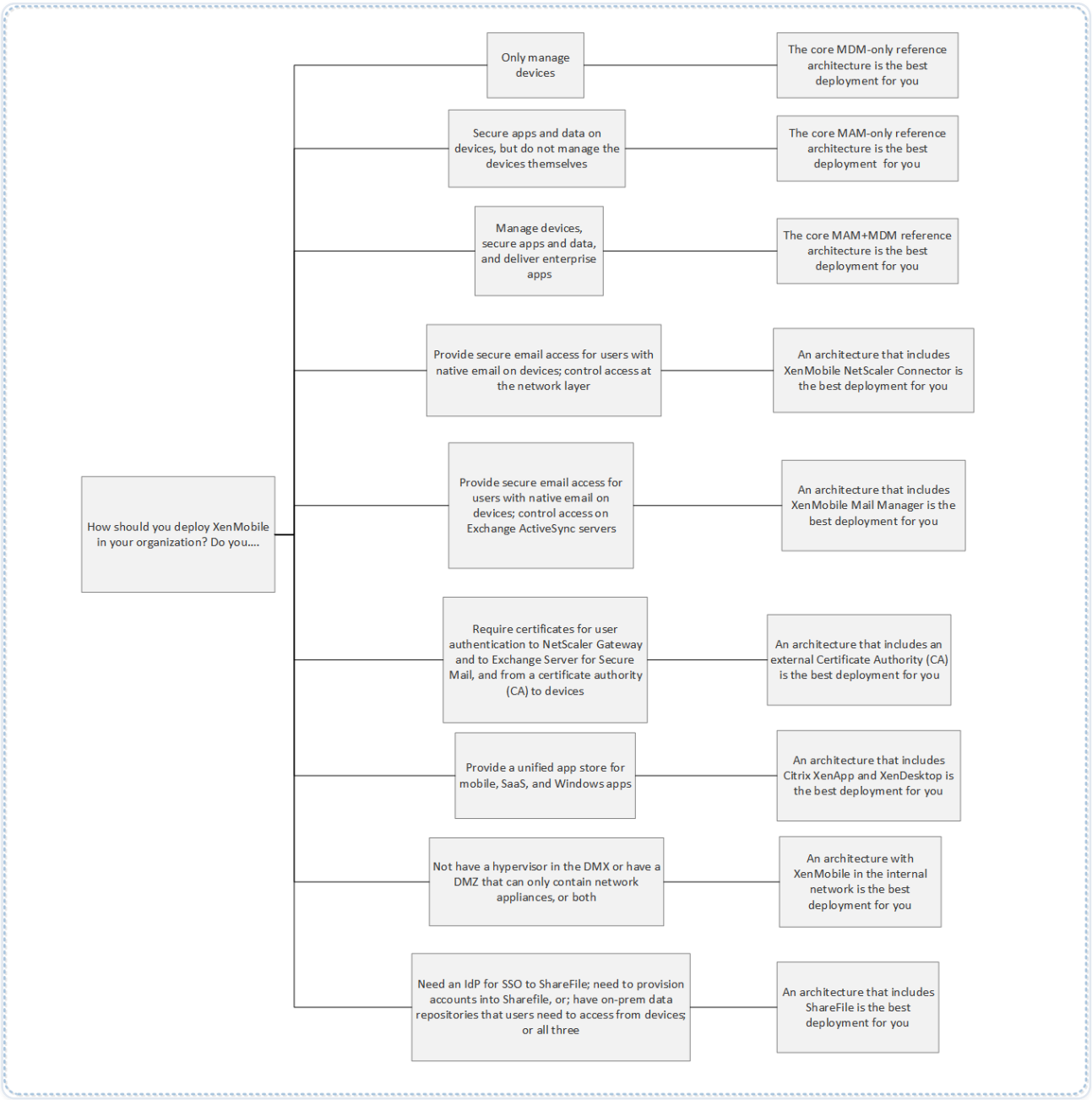
설정	설정 위치	권장 설정	동작 영향
온라인 세션 필수	MDX 정책	켜짐	장치가 온라인 상태이고 유효한 인증 토큰을 가지고 있는지 확인합니다.
온라인 세션 필수 유예 기간	MDX 정책	15	사용자가 앱을 더 이상 사용할 수 없게 되기 전에 15분간의 유예 기간을 허용합니다.

온프레미스 배포를 위한 참조 아키텍처

이 문서의 그림은 온프레미스 XenMobile 배포를 위한 참조 아키텍처를 보여줍니다. 배포 시나리오에는 핵심 아키텍처로서 MDM 전용, MAM 전용 및 MDM+MAM이 포함되며, SNMP Manager, Exchange ActiveSync용 Citrix Gateway connector™, Exchange ActiveSync용 Endpoint Management

connector, Virtual Apps and Desktops와 같은 구성 요소가 포함된 시나리오도 있습니다. 이 그림은 XenMobile에 필요한 최소 구성 요소를 보여줍니다.

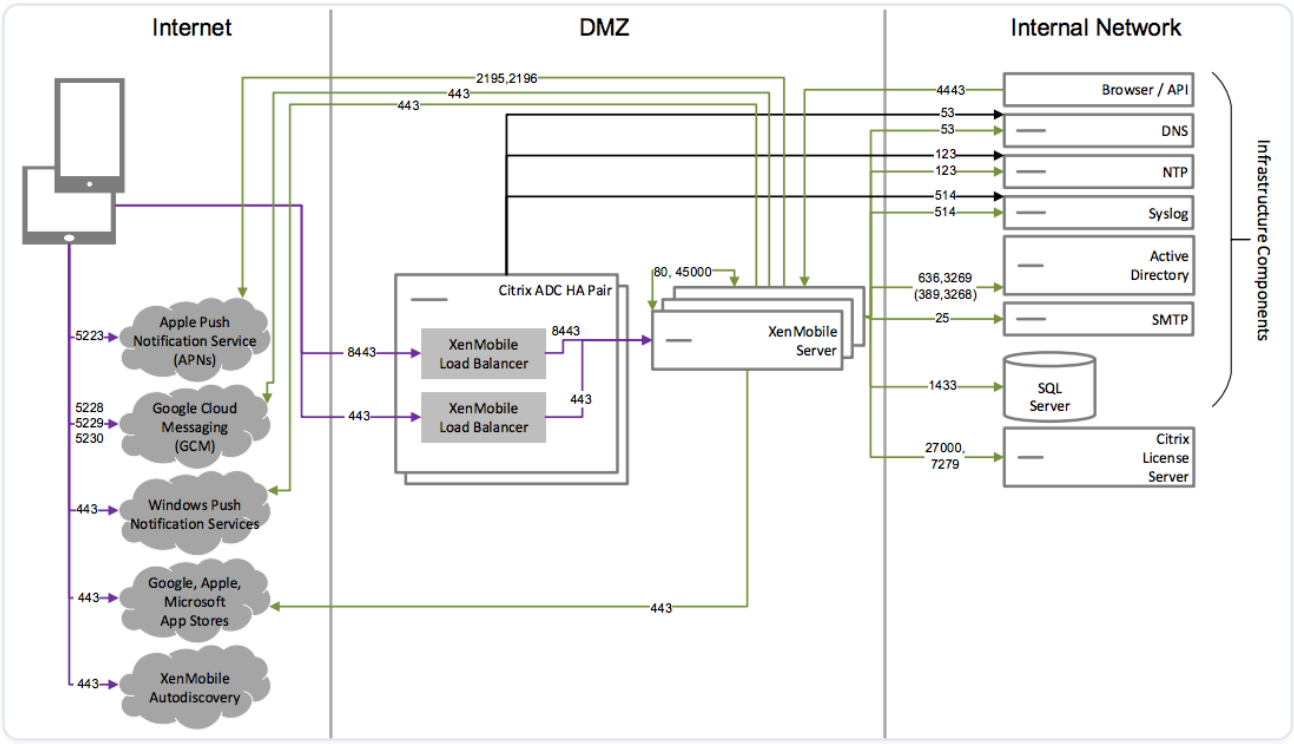
이 차트를 배포 결정에 대한 일반적인 지침으로 사용하십시오.



그림에서 커넥터의 숫자는 구성 요소 간의 연결을 허용하기 위해 열어야 하는 포트를 나타냅니다. 전체 포트 목록은 XenMobile 설명서의 포트 요구 사항을 참조하십시오.

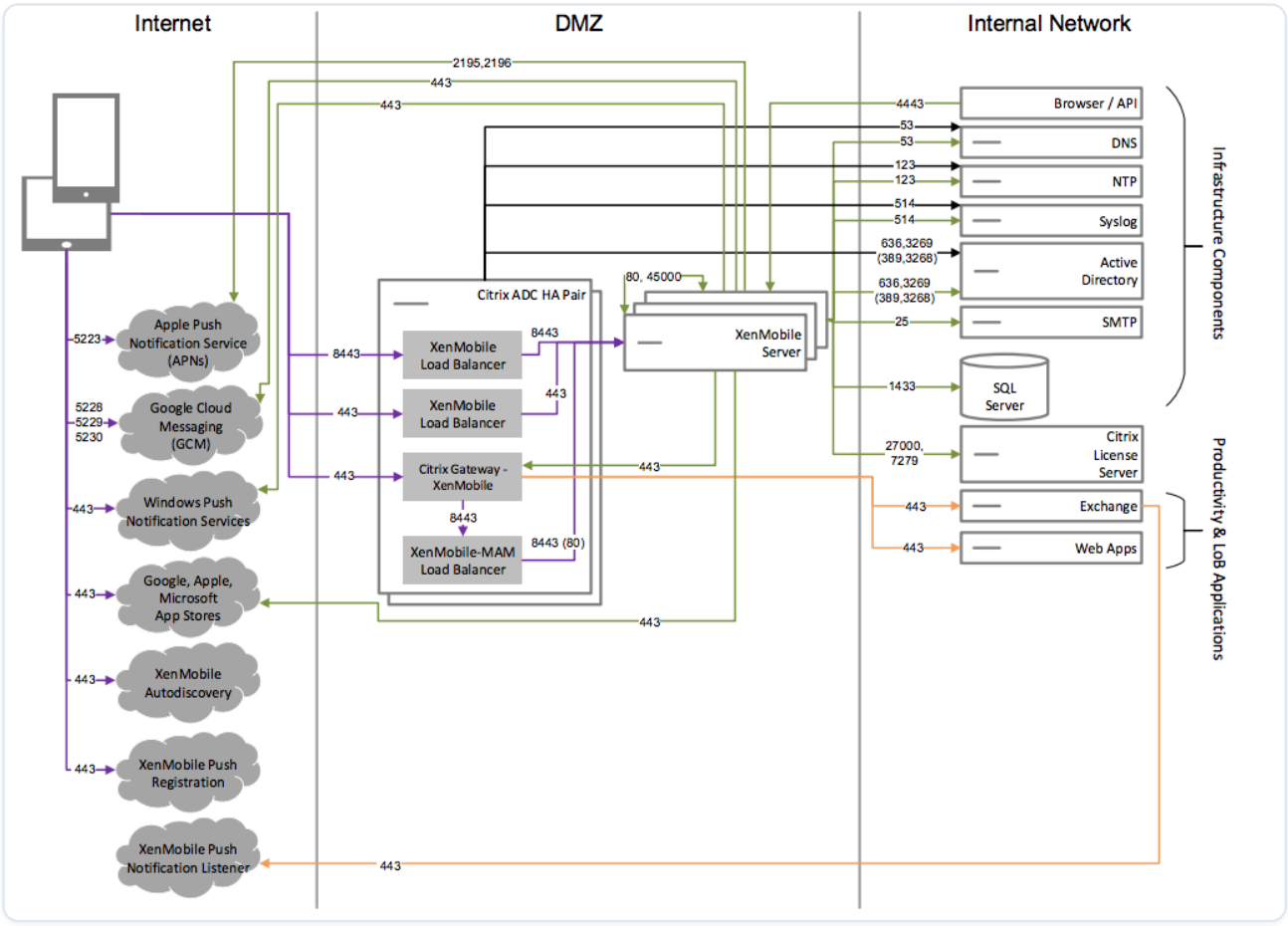
핵심 MDM 전용 참조 아키텍처

XenMobile의 MDM 기능만 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어, 장치 정책, 앱을 배포하고 자산 인벤토리를 검색하며 장치 초기화와 같은 작업을 수행하기 위해 MDM을 통해 회사에서 발행한 장치를 관리해야 하는 경우입니다.



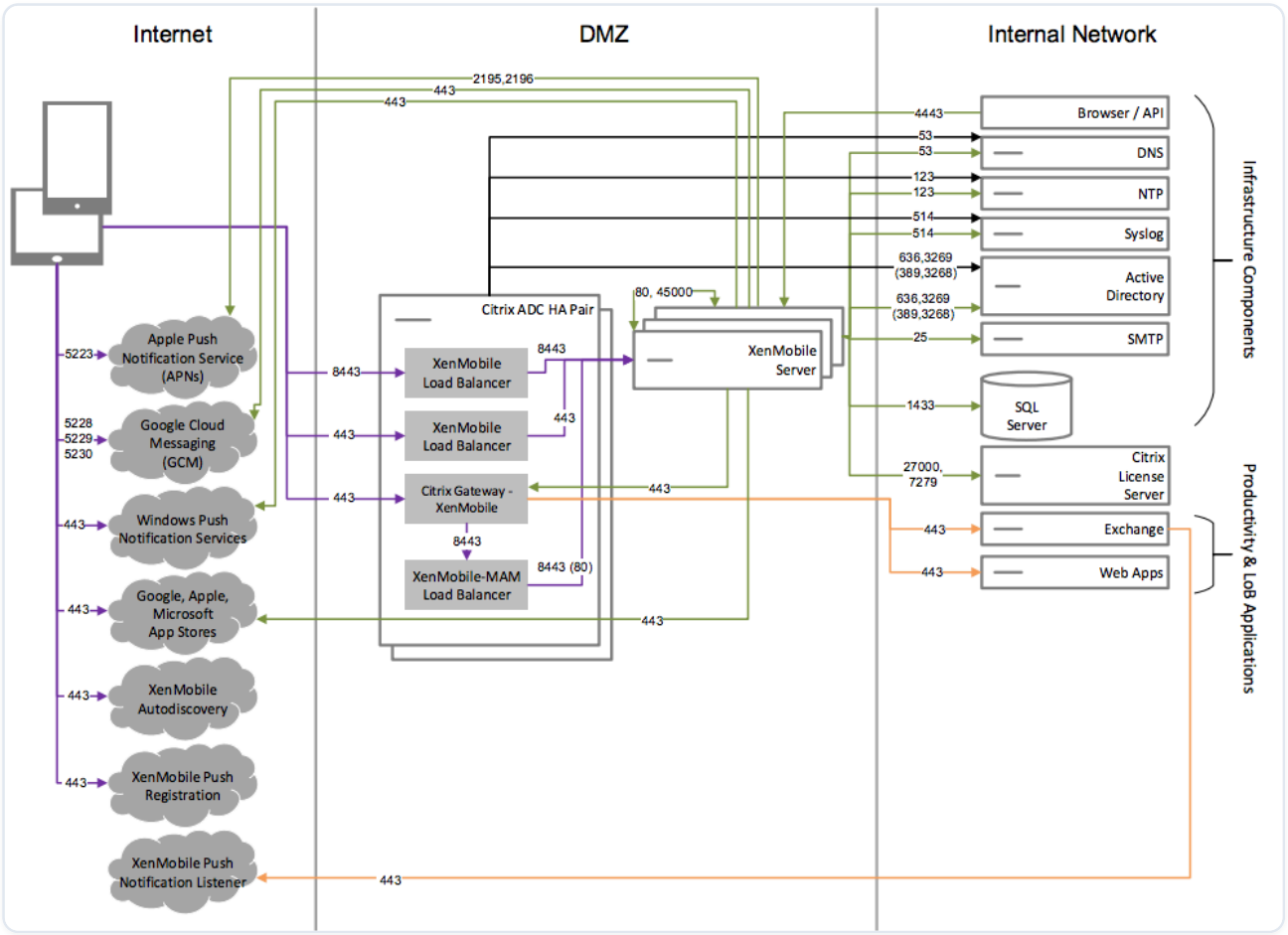
핵심 MAM 전용 참조 아키텍처

MDM에 장치를 등록하지 않고 XenMobile의 MAM 기능만 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어, BYO 모바일 장치에서 앱과 데이터를 보호하고 싶거나, 엔터프라이즈 모바일 앱을 제공하고 앱을 잠그고 데이터를 지우고 싶은 경우입니다. 이 경우 장치는 MDM에 등록할 수 없습니다.



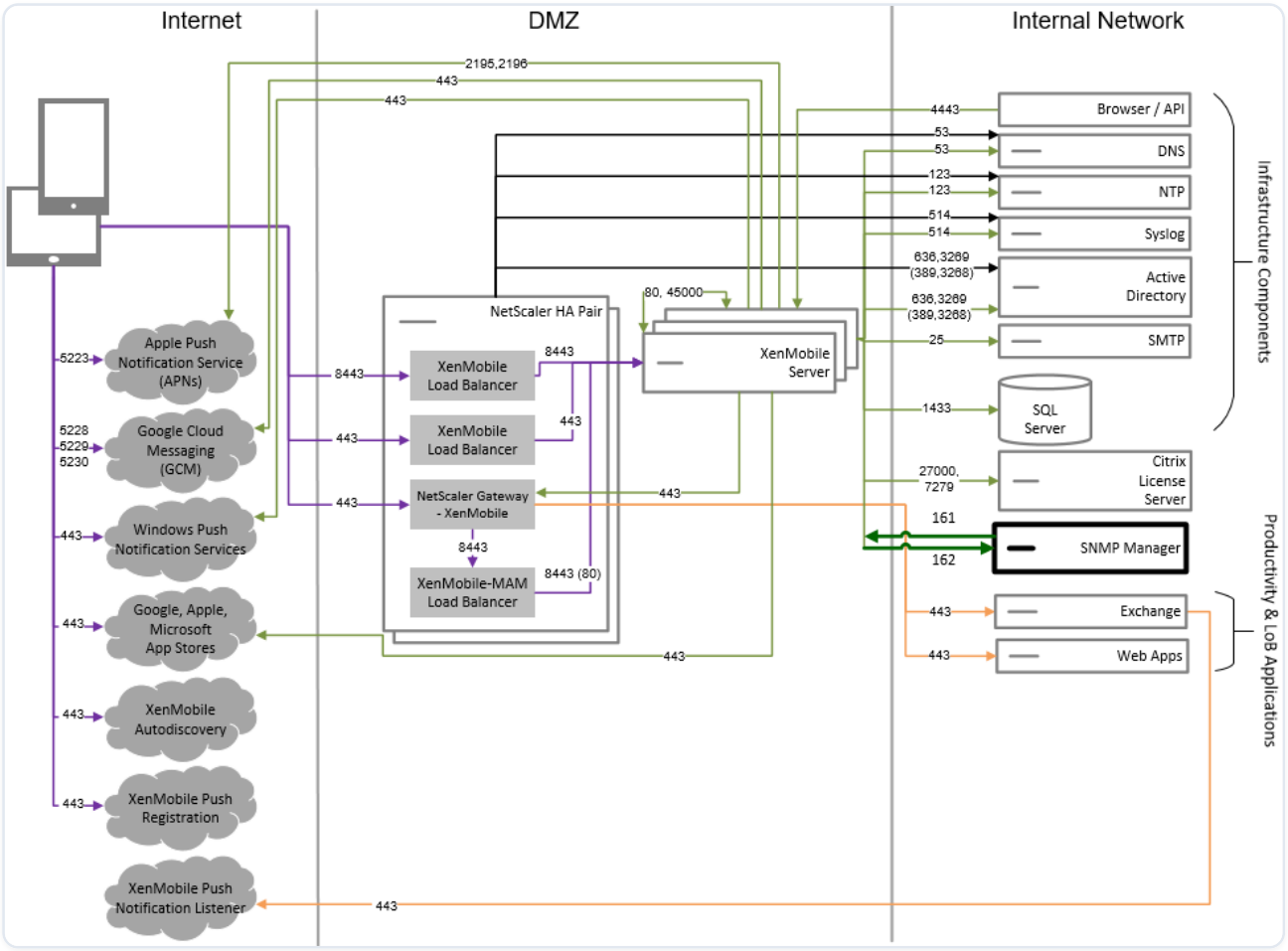
핵심 MAM+MDM 참조 아키텍처

XenMobile의 MDM+MAM 기능을 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어, MDM을 통해 회사에서 발행한 장치를 관리하고 싶거나, 장치 정책 및 앱을 배포하고, 자산 인벤토리를 검색하고, 장치를 초기화할 수 있는 경우입니다. 또한 엔터프라이즈 모바일 앱을 제공하고 앱을 잠그고 장치의 데이터를 지울 수 있습니다.



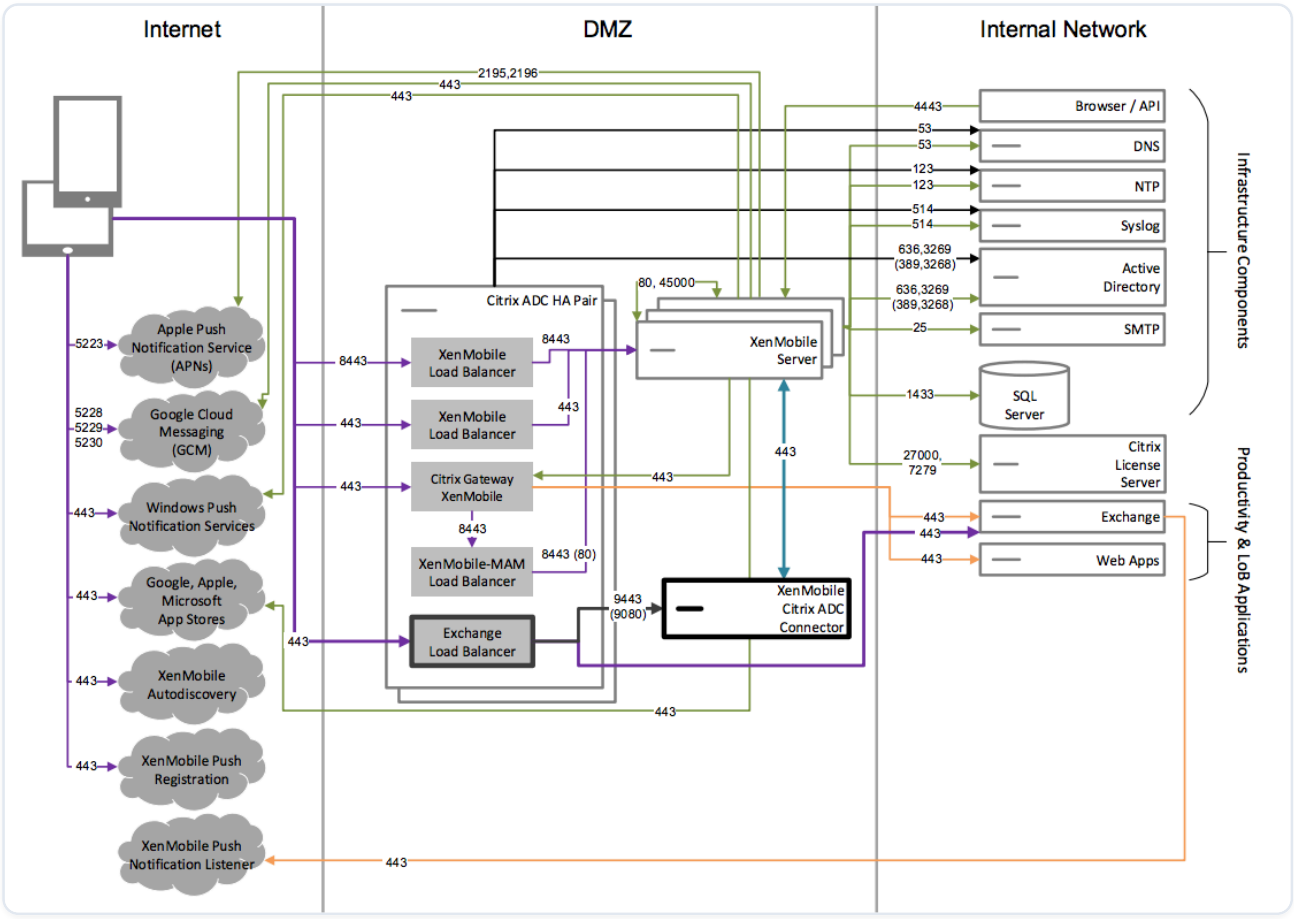
SNMP를 사용한 참조 아키텍처

XenMobile과 함께 SNMP 모니터링을 활성화할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어, 모니터링 시스템이 XenMobile 노드에 대한 정보를 쿼리하고 얻을 수 있도록 허용하려는 경우입니다. 자세한 내용은 SNMP 모니터링을 참조하십시오.



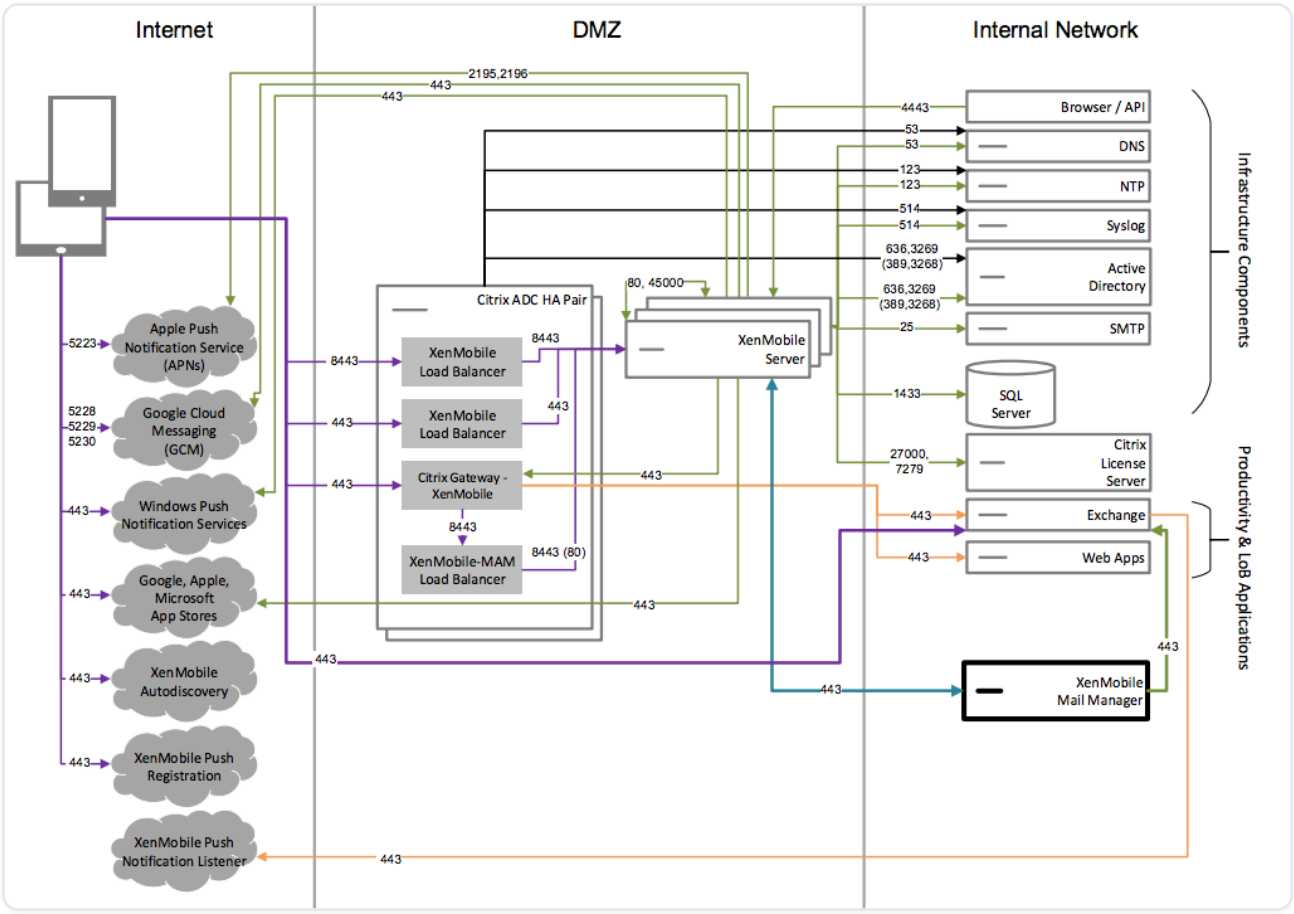
Exchange ActiveSync용 Citrix Gateway 커넥터가 포함된 참조 아키텍처

XenMobile과 함께 Exchange ActiveSync용 Citrix Gateway 커넥터를 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어, 기본 모바일 이메일 앱을 사용하는 사용자에게 안전한 이메일 액세스를 제공해야 하는 경우입니다. 이러한 사용자는 기본 앱을 통해 이메일에 계속 액세스하거나, 시간이 지남에 따라 Citrix Secure Mail로 전환할 수 있습니다. 트래픽이 Exchange Active Sync 서버에 도달하기 전에 네트워크 계층에서 액세스 제어가 이루어져야 합니다. 다이어그램에는 MDM 및 MAM 아키텍처에 배포된 Exchange ActiveSync용 커넥터가 표시되어 있지만, MDM 전용 아키텍처의 일부로 Exchange ActiveSync용 커넥터를 동일한 방식으로 배포할 수도 있습니다.



Exchange ActiveSync용 Endpoint Management 커넥터가 포함된 참조 아키텍처

XenMobile과 함께 Exchange ActiveSync용 Endpoint Management 커넥터를 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어, 기본 모바일 이메일 앱을 사용하는 사용자에게 안전한 이메일 액세스를 제공하려는 경우입니다. 이러한 사용자는 기본 앱을 통해 이메일에 계속 액세스하거나, 시간이 지남에 따라 Secure Mail로 전환할 수 있습니다. Exchange ActiveSync 서버에서 액세스 제어를 구현할 수 있습니다. 다이어그램에는 MDM 및 MAM 아키텍처에 배포된 Exchange ActiveSync용 Endpoint Management 커넥터가 표시되어 있지만, MDM 전용 아키텍처의 일부로 Exchange ActiveSync용 Endpoint Management 커넥터를 동일한 방식으로 배포할 수도 있습니다.

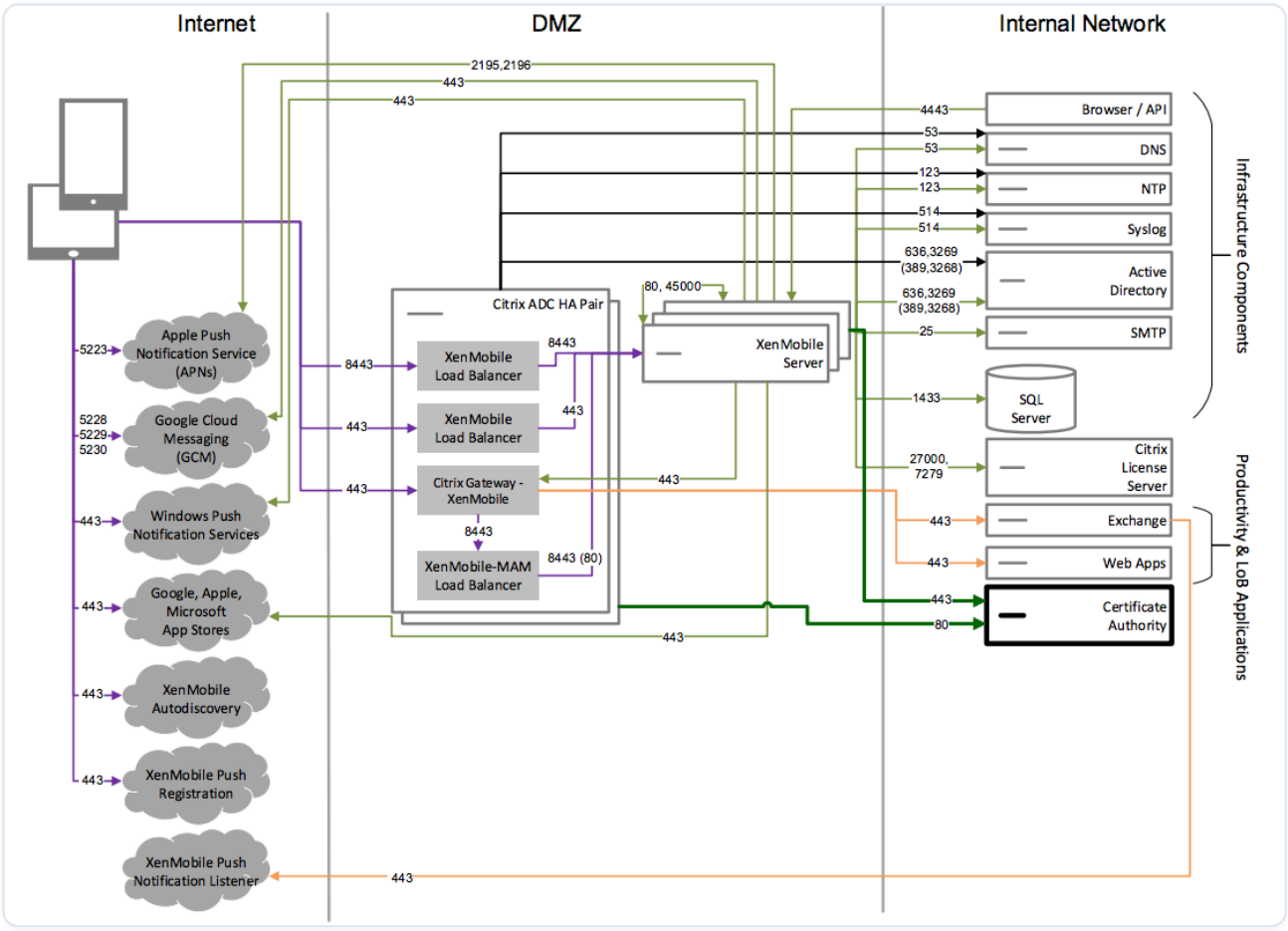


외부 인증 기관이 포함된 참조 아키텍처

외부 인증 기관을 포함하는 배포는 다음 요구 사항 중 하나 이상을 충족하기 위해 권장됩니다.

- Citrix Gateway에 대한 사용자 인증(인트라넷 액세스용)을 위해 사용자 인증서가 필요합니다.
- Secure Mail 사용자가 사용자 인증서를 사용하여 Exchange Server에 인증하도록 요구합니다.
- 예를 들어, Wi-Fi 액세스를 위해 회사 인증 기관에서 발급한 인증서를 모바일 장치로 푸시해야 합니다.

다이어그램에는 MDM+MAM 아키텍처에 배포된 외부 인증 기관이 표시되어 있지만, MDM 전용 또는 MAM 전용 아키텍처의 일부로 외부 인증 기관을 동일한 방식으로 배포할 수도 있습니다.



Virtual Apps and Desktops를 사용한 참조 아키텍처

XenMobile과 Virtual Apps and Desktops를 통합할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어, 모든 유형의 애플리케이션(모바일, SaaS 및 Windows)에 대해 모바일 사용자에게 통합 앱 스토어를 제공해야 합니다. 다이어그램은 MDM 및 MAM 아키텍처에 배포된 Virtual Desktops를 보여주지만, MAM 전용 아키텍처의 일부로 동일한 방식으로 해당 데스크톱을 배포할 수도 있습니다.

Virtual Apps and Desktops를 사용한 참조 아키텍처 다이어그램(/en-us/xenmobile/server/media/architecture-xenapp-xendesktop.png)

내부 네트워크에 XenMobile이 있는 참조 아키텍처

다음 요구 사항 중 하나 이상을 충족하기 위해 내부 네트워크에 XenMobile이 있는 아키텍처를 배포할 수 있습니다.

- DMZ에 하이퍼바이저가 없거나 허용되지 않습니다.
- DMZ에는 네트워크 어플라이언스만 포함될 수 있습니다.
- 보안 요구 사항에 SSL 오프로드 사용이 필요합니다.

내부 네트워크에 XenMobile이 있는 참조 아키텍처 다이어그램(/en-us/xenmobile/server/media/architecture-internal-network.png)

ShareFile을 사용한 참조 아키텍처

Citrix Files 또는 스토리지 영역 커넥터만 XenMobile과 통합하려면 이 아키텍처를 배포하십시오. Citrix Files 통합을 통해 다음 요구 사항 중 하나 이상을 충족할 수 있습니다.

- 사용자에게 ShareFile.com에 대한 단일 Sign-On(SSO)을 제공하려면 IdP가 필요합니다.
- ShareFile.com에 계정을 프로비저닝하는 방법이 필요합니다.
- 모바일 장치에서 액세스해야 하는 온프레미스 데이터 리포지토리가 있습니다.

스토리지 영역 커넥터만 통합하면 SharePoint 사이트 및 네트워크 파일 공유와 같은 기존 온프레미스 스토리지 리포지토리에 대한 안전한 모바일 액세스를 사용자에게 제공합니다. 이 구성에서는 ShareFile 하위 도메인을 설정하거나, Citrix Files에 사용자를 프로비저닝하거나, Citrix Files 데이터를 호스팅할 필요가 없습니다.

다이어그램에는 MDM+MAM 아키텍처에 배포된 Citrix Files가 표시되어 있지만, MAM 전용 아키텍처의 일부로 동일한 방식으로 Citrix Files를 배포할 수도 있습니다.

Citrix Files를 포함한 참조 아키텍처 다이어그램(/en-us/xenmobile/server/media/reference-architecture-sharefile-storagezones.png)

서버 속성

서버 속성은 전체 XenMobile® 인스턴스의 작업, 사용자 및 장치에 적용되는 전역 속성입니다. Citrix®는 이 문서에서 다루는 서버 속성을 사용자 환경에 맞게 평가할 것을 권장합니다. 다른 서버 속성을 변경하기 전에 반드시 Citrix에 문의하십시오.

일부 서버 속성을 변경하려면 각 노드를 다시 시작해야 합니다. XenMobile은 다시 시작이 필요할 때 사용자에게 알립니다.

일부 서버 속성은 성능과 안정성을 향상시키는 데 도움이 됩니다. 자세한 내용은 XenMobile 작업 튜닝을 참조하십시오.

레거시 Android 앱을 Android Enterprise 장치에 배포: `afw.allow.legacy.apps`이(가) `true`(으)로 설정된 경우, Android Enterprise 장치는 레거시 Android 앱과 Android Enterprise 앱을 모두 받습니다. `false`인 경우, Android Enterprise 장치는 Android Enterprise 앱만 받습니다. 기본값은 `true`입니다.

파일 정책에 대한 파일 확장명 허용: 관리자가 파일 장치 정책을 사용하여 업로드할 수 있는 파일 형식의 쉼표로 구분된 목록으로 `file.extension.allowlist`을(를) 구성합니다. 다음 파일 형식은 이 허용 목록에 추가하더라도 업로드할 수 없습니다.

- .캐브

- .앱엑스
- .아이피에이
- .에이피케이
- .엑스에이피
- .엠디엑스
- .이엑스이

기본값은 `7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,` 입니다.

관리형 Google Play 스토어의 모든 앱에 액세스: `true`인 경우, XenMobile은 공개 Google Play 스토어의 모든 앱을 관리형 Google Play 스토어에서 액세스할 수 있도록 합니다. 이 속성을 `true`(으)로 설정하면 모든 Android Enterprise 사용자가 공개 Google Play 스토어 앱을 사용할 수 있습니다. 관리자는 제한 장치 정책을(를) 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다. 기본값은 `false`입니다.

기업 소유 장치 등록 시 Android Enterprise 업무 프로필: `afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled`이(가) `true`(으)로 설정된 경우 Android 11 이상을 실행하는 장치는 기업 소유 장치(WPCOD) 모드에서 업무 프로필에 등록할 수 있습니다. 콘솔은 이 등록 모드에 대한 변경 사항을 반영합니다. `false`(으)로 설정된 경우 WPCOD 설정은 사용할 수 없습니다. 기본값은 `true`입니다.

추가 Android Enterprise 제한 설정: 속성 `afw.restriction.policy.v2`이(가) `true`(으)로 설정된 경우 Android Enterprise 장치에 대해 다음 제한 설정을 사용할 수 있습니다.

- 앱 제거 허용
- Bluetooth 공유 허용

이러한 설정에 대한 자세한 내용은 제한 장치 정책을(를) 참조하십시오.

COPE 장치에 대한 Android Enterprise 제한: 제한 장치 정책에서 **업무 프로필이 있는 완전 관리형 장치에 적용/기업 소유 장치에 대한 업무 프로필** 설정을 활성화하려면 `afw.restriction.cope`을(를) `true`(으)로 설정합니다. 기본값은 `true`입니다. 이 설정에 대한 자세한 내용은 제한 장치 정책을(를) 참조하십시오.

iOS App Store 링크에 대한 호스트 이름 허용: 속성 `ios.app.store.allowed.hostnames`은(는) 공용 API를 사용하여 공용 앱 스토어 앱을 서버에 업로드할 때 사용되는 허용된 호스트 이름 목록입니다. 서버

를 통해 앱을 업로드하는 대신 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`(으)로부터 APN 알림을 주고받을 수 있습니다. 이 포트는 HTTP/2 기반 APN 공급자 API를 사용합니다. 포트 2197을 사용하려면 속성 `apns.http2.alternate.port.enabled`를 `true`(으)로 설정하십시오. 서버 속성 `apns.http2.alternate.port.enabled`의 기본값은 `false`입니다.

약한 암호를 가진 로컬 사용자 방지를 위한 암호 유효성 검사 활성화: `enable.password.strength.validation`이(가) `true`(으)로 설정된 경우 약한 암호를 가진 로컬 사용자를 추가할 수 없습니다. `false`(으)로 설정된 경우 약한 암호를 가진 로컬 사용자를 생성할 수 있습니다. 기본값은 `true`입니다.

루팅된 Android 및 탈옥된 iOS 장치 등록 차단: 이 속성이 `true`(으)로 설정된 경우 XenMobile은 루팅된 Android 장치 및 탈옥된 iOS 장치의 등록을 차단합니다. 기본값은 `true`입니다. 모든 보안 수준에 권장되는 설정은 `true`입니다.

등록 필수: `wsapi.mdm.required.flag`(은)는 모드가 ENT일 때만 적용되며, 사용자에게 MDM 등록을 요구할지 여부를 지정합니다. 이 속성은 XenMobile 인스턴스의 모든 사용자 및 장치에 적용됩니다. 등록을 요구하면 더 높은 수준의 보안을 제공합니다. 그러나 이 결정은 MDM을 요구할지 여부에 따라 달라집니다. 기본적으로 등록은 필수가 아닙니다.

이 속성이 `false`(으)로 설정된 경우 사용자는 등록을 거부할 수 있지만 XenMobile Store를 통해 장치의 앱에 계속 액세스할 수 있습니다. 이 속성이 `true`(으)로 설정된 경우 등록을 거부하는 모든 사용자는 모든 앱에 대한 액세스가 거부됩니다.

사용자가 등록한 후 이 속성을 변경하면 사용자는 다시 등록해야 합니다.

MDM 등록을 요구할지 여부에 대한 논의는 장치 관리 및 MDM 등록을(를) 참조하십시오.

다중 모드 등록 활성화: 속성 `enable.multimode.xms`(은)는 하나의 XenMobile Server에서 Android 및 iOS 장치의 장치 및 앱 관리를 위한 등록 설정을 제어하는 등록 프로필을 생성할 수 있도록 합니다. 또한 새로운 향상된 등록 프로필 기능은 Android 전용 장치 등록과 Android 및 iOS 장치 전용 MAM 등록을 가능하게 합니다. 이 속성이 `false`(으)로 설정된 경우 등록 프로필을 설정할 때 해당 등록 옵션을 사용할 수 없습니다. 기본값은 `true`입니다. 이 속성이 `true`(으)로 설정되었을 때 등록된 장치는 속성을 `false`(으)로 변경해도 계속 작동합니다.

셀프 도움말 포털 사용: `shp.console.enable`이(가) `false`이면 셀프 도움말 포털에 대한 액세스를 방지합니다. 포트 443에서 셀프 도움말 포털로 이동하는 사용자는 404 오류를 수신합니다. 포트 4443에서 포

털로 이동하는 사용자는 "액세스 거부" 메시지를 수신합니다. `true`이면 포트 443을 통해 셀프 도움말 포털에 대한 액세스를 제공합니다. 기본값은 `false`입니다.

로컬 사용자 계정 잠금 제한: 제한 정책을 사용하여 Active Directory 사용자의 로그인 시도 횟수를 제한할 수 있습니다. 로컬 사용자 계정에 대해서도 동일하게 하려면 `local.user.account.lockout.limit` 키를 사용합니다. 사용자가 지정된 횟수만큼 로그인 시도를 한 후에는 일정 시간이 지나야 다시 시도할 수 있습니다. 해당 시간은 **로컬 사용자 계정 잠금 시간** 속성으로 구성합니다. 기본값은 `6`입니다.

로컬 사용자 계정 잠금 시간: `local.user.account.lockout.time` 속성을 사용하면 잠긴 로컬 사용자 계정이 다시 로그인하기 전에 경과해야 하는 시간을 분 단위로 설정할 수 있습니다. 기본값은 `30`분입니다.

파일 업로드 최대 크기 제한 사용: 업로드에 대한 최대 파일 크기 제한을 사용하려면 `max.file.size.upload.restriction`을(를) `true`(으)로 설정합니다. 이 제한을 사용하도록 설정하는 경우 `max.file.size.upload.allowed`을(를) 사용하여 최대 파일 크기를 구성합니다. 이 속성의 기본값은 `true`입니다.

허용되는 파일 업로드 최대 크기: `max.file.size.upload.allowed`을(를) 사용하여 모든 업로드에 대한 최대 파일 크기를 지정할 수 있습니다. 예시 값으로는 `500 B`, `1 KB`, `1 MB`, `1 MiB`, `1 G` 또는 `1 GiB`이(가) 있습니다. 기본값은 `5 MB`입니다.

비활성 시간 제한(분): XenMobile Server 공용 API를 사용하여 XenMobile 콘솔 또는 타사 앱에 액세스한 비활성 사용자를 XenMobile이 로그아웃시키는 시간(분)입니다. `0`의 시간 제한 값은 비활성 사용자가 로그인 상태를 유지함을 의미합니다. API에 액세스하는 타사 앱의 경우 로그인 상태를 유지하는 것이 일반적으로 필요합니다. 기본값은 `5`입니다.

iOS 장치 관리 등록 시 필요한 경우 루트 CA 설치: Apple의 최신 등록 워크플로는 사용자가 MDM 프로필을 수동으로 설치해야 합니다. 이 워크플로는 Apple Business Manager 또는 Apple School Manager에 할당된 서버에 대한 MDM 등록에는 적용되지 않습니다. 그러나 MDM에 수동으로 등록하는 동안 iOS 장치 사용자는 등록 중에 MDM 장치 인증서 프롬프트만 받습니다.

수동 등록 시 더 나은 사용자 환경을 제공하기 위해 Citrix는 서버 속성 `ios.mdm.enrollment.installRootCaIfRequired`을(를) **False**로 변경할 것을 권장합니다. 기본값은 **True**입니다. 이 변경으로 인해 MDM 등록 중에 Safari 창이 열려 사용자의 프로필 설치가 간소화됩니다.

VPP 기준 간격: `vpp.baseline` 속성은 XenMobile이 Apple에서 볼륨 구매 라이선스를 다시 가져오는 최소 간격을 설정합니다. 라이선스 정보를 새로 고치면 볼륨 구매에서 가져온 앱을 수동으로 삭제하는 경우와 같이 XenMobile이 모든 변경 사항을 반영하는지 확인할 수 있습니다. 기본적으로 XenMobile은 최소 `1440` 분마다 볼륨 구매 라이선스 기준을 새로 고칩니다.

많은 볼륨 구매 라이선스(예: 50,000개 이상)가 설치되어 있는 경우 Citrix는 라이선스 가져오기 오버헤드를 줄이기 위해 기준 간격을 늘릴 것을 권장합니다. Apple에서 볼륨 구매 라이선스 변경이 자주 발생할 것으로 예상되는 경우 Citrix는 변경 사항으로 XenMobile을 업데이트된 상태로 유지하기 위해 값을 낮출 것을 권장합니다. 두 기준 간의 최소 간격은 60분입니다. cron 작업이 60분마다 실행되므로 볼륨 구매 기준 간격이 60분인 경우 기준 간의 간격은 최대 119분까지 지연될 수 있습니다.

XenMobile MDM 셀프 도움말 포털 콘솔 최대 비활성 간격(분): 이 속성 이름은 이전 XenMobile 버전을 반영합니다. 이 속성은 XenMobile 콘솔의 최대 비활성 간격을 제어합니다. 이 간격은 XenMobile이 비활성 사용자를 XenMobile 콘솔에서 로그아웃시키는 시간(분)입니다. 시간 제한이 0이면 비활성 사용자가 로그인 상태를 유지함을 의미합니다. 기본값은 `30`입니다.

Nexmo SMS 게이트웨이에 대한 지원 중단: `deprecate.carrier.sms.gateway` 속성은 기본적으로 **True**로 설정된 Nexmo SMS 게이트웨이에 대한 지원을 제거합니다. Nexmo SMS는 셀프 도움말 포털에서도 더 이상 사용되지 않습니다.

MSP(모바일 서비스 공급자) 인터페이스에 대한 지원 중단: `deprecate.mobile.service.provider` 속성은 기본적으로 **True**로 설정된 MSP 인터페이스를 콘솔에서 제거합니다.

Windows 정보 보호 정책에 대한 지원 중단: Windows 공지에 따라 Windows 정보 보호(WIP)에 대한 지원이 중단되었습니다. 서버 속성 `windows.wip.deprecation`는 기본적으로 **True**로 설정된 WIP에 대한 지원을 제거합니다.

Android Enterprise용 OS 업데이트 제어 정책에서 "Control Enterprise FOTA" 필드에 대한 지원 중단: 속성 `afw.disable.osupdate.efota`이(가) **True**로 설정된 경우 Android Enterprise용 OS 업데이트 제어 정책에서 **Control Enterprise FOTA** 필드가 더 이상 사용되지 않습니다. 기본값은 **True**로 설정됩니다.

macOS 기기에서 엔터프라이즈 앱 지원: 속성 `mac.app.push`이 **True**로 설정된 경우, macOS를 실행하는 기기에 다운로드될 때 엔터프라이즈 앱이 자동으로 설치됩니다. 기본값은 **True**로 설정됩니다.

iOS 기기에서 eSIM 지원: 속성 `ios.esim.support`이 **True**로 설정된 경우, XenMobile Server는 iOS 기기에서 eSIM 정보를 가져와 사용자 인터페이스에 eSIM 관련 기기 속성을 표시합니다.

Android Enterprise용 802.1x 설정의 Wi-Fi 정책에서 "도메인" 필드 지원: 속성 `afw.network.domain.support`이 **True**로 설정된 경우, **Android Enterprise용 802.1x 설정**에 ***도메인*** 필드가 추가됩니다.

iOS에서 선택적 앱 자동 업데이트 지원: `apple.ios.optional_app_update` 속성이 **True**로 설정된 경우, Citrix Secure Hub 스토어에서 구독한 iOS의 선택적 앱도 자동으로 업데이트됩니다. 기본값은 **False**로 설정됩니다.

총 앱 배포 시도 및 상위 100개 설치된 앱에 대한 기기 보고서 개선: 속성 `device.report.enhancement.enabled`이 **True**로 설정된 경우, **총 앱 배포 시도**에 **운영 체제 버전** 및 **기기 모델** 두 개의 새 열이 추가되고, 각 플랫폼에 설치된 상위 100개 앱을 표시하는 새 기기 보고서 **상위 100개 설치된 앱**이 추가됩니다.

iPhone 및 iPad의 서비스 복귀 지원: 속성 `ios.mdm.return.to.service`이 **True**로 설정된 경우, iOS 17 이상을 실행하는 iPhone 및 iPad에서 서비스 복귀 기능을 사용할 수 있습니다. 이 속성의 기본 설정은 **True**입니다.

Android Enterprise용 VPN 정책에서 상시 VPN 옵션 지원: 속성 `afw.policy.vpn_always_on_lockdown`이 **True**로 설정된 경우, Android Enterprise 플랫폼용 **VPN** 정책에 **상시 VPN 사용** 및 **잠금 사용** 옵션이 추가됩니다. 기본값은 **True**입니다.

Android Enterprise용 옵션 정책에서 상시 VPN 옵션 지원 중단: 속성 `afw.policy.hide_vpn_always_on`은 Android Enterprise 플랫폼의 **XenMobile 옵션** 정책에서 **상시 VPN** 옵션을 제거합니다. 기본값은 **True**입니다.

레거시 MDX 사용 중단 경고: 속성 `legacy.mdx.deprecation.alert`이 **True**로 설정된 경우, 레거시 MDX 모드로 게시된 MDX 앱이 있으면 XenMobile Server 콘솔에 경고가 나타납니다. 기본값은 **True**입니다.

새 HTTP v1 API를 사용하도록 마이그레이션된 Firebase Cloud Messaging 지원: 속성 `afw.fcm.httpv1.migration`이 **True**로 설정된 경우, 새 HTTP v1 API와 함께 Firebase Cloud Messaging을 사용할 수 있습니다. 기본값은 **False**입니다.

iPhone 및 iPad의 서비스 복귀 지원: 속성 `ios.mdm.return.to.service`이 **True**로 설정된 경우, iOS 17 이상을 실행하는 iPhone 및 iPad에서 서비스 복귀 기능을 사용할 수 있습니다. 이 속성의 기본 설정은 **True**입니다.

개인 프로필에서 업무 프로필 이메일 앱에 액세스하고 사용하는 기능 지원: `afw.mailapp.crossworkprofile` 속성이 **True**로 설정된 경우, Android Enterprise 설정에서 개인 프로필에서 업무 프로필 이메일 앱에 액세스하고 사용할 수 있는 기능을 활성화합니다. 기본값은 **True**입니다.

자동 등록 시 설정 완료를 위한 최소 OS 버전 적용 지원: `ios.mdm.minimum_os_version.enrollment` 속성이 **True**로 설정된 경우, iOS 17 이상에서 자동 등록 중 설정을 완료하기 위한 최소 OS 버전 요구 사항을 적용할 수 있습니다. 기본값은 **True**입니다.

Samsung Knox 향상된 증명 v3 지원: `afw.knox.attestation.v3` 속성이 **True**로 설정된 경우, Samsung Knox 기기에서 보안 기능을 향상시킬 수 있습니다. 기본값은 **True**입니다.

Android Enterprise 관리형 구성 피드백 활성화: `afw.app_managed_configurations.feedback`이 **True**로 설정된 경우, 관리자는 관리형 구성 정책으로 구성된 Android 기기에서 앱 상태에 대한 피드백을 얻을 수 있습니다. **False**인 경우, 관리자는 피드백을 받지 못합니다. 기본값은 **False**입니다.

Android Enterprise 관리형 구성 피드백 DB 업데이트를 위한 배치 크기: `android.managed.configuration.feedback.db.update.batch.size`이(가) 설정된 경우, Android Enterprise 관리형 구성 피드백 DB를 업데이트할 배치 크기를 정의합니다. 크기는 DB 기능에 따라 구성할 수 있습니다. 기본값은 **100**이고, 최대값은 **1000**입니다.

Android Enterprise 관리형 구성 피드백 DB 업데이트 시간 간격: `android.managed.configuration.feedback.db.update.time.interval`이(가) 설정된 경우, Android Enterprise 관리형 구성 피드백 DB를 업데이트하는 시간 간격을 정의합니다. 기본값은 **6**시간입니다.

Android Enterprise 정책 규정 준수 적용: `afw.policy.compliance` 속성이 **True**로 설정된 경우, 장치 소유자 모드로 등록된 Android 장치는 관리자가 장치 규정 준수를 관리할 수 있도록 합니다. 기본값은 **False**입니다.

ABM MDM 서버에서 할당 해제된 경우 XMS에서 ABM 장치 제거: `remove.unassigned.abm.devices`이(가) **true**인 경우, XMS는 이 서버에 더 이상 할당되지 않은 장치를 제거합니다. 기본값은 **false**입니다.

인증서 기반 인증을 위한 새로운 강력한 인증서 매핑 지원: `all_platforms.certificate.strong.mapping` 속성이 **True**로 설정된 경우, XenMobile Server는 Microsoft의 새로운 강력한 인증서 매핑을 지원합니다. 기본값은 **True**입니다.

Android Enterprise 장치에서 eSIM 지원: `ae.esim.support` 속성이 **True**로 설정된 경우, XenMobile Server는 Android Enterprise 장치에서 eSIM 정보를 가져와 사용자 인터페이스에 eSIM 관련 장치 속성을 표시합니다. 기본값은 **True**입니다.

선언적 장치 관리(DDM) 지원: `ios.mdm.declarative.management` 속성이 **True**로 설정된 경우, XenMobile Server 콘솔에서 iOS 선언적 관리 정책을 구성할 수 있습니다. 기본값은 **False**입니다.

iOS 소프트웨어 업데이트 적용 지원: `ios.mdm.software.update.settings` 속성이 **True**로 설정된 경우, XenMobile Server 콘솔에서 소프트웨어 업데이트 적용 장치 정책을 구성할 수 있습니다. 기본값은 **False**입니다.

Android Enterprise 장치에서 앱 자동 실행 지원: `afw.launcher.auto_launch` 속성이 **True**로 설정된 경우, 런처 구성 장치 정책에서 Android Enterprise 장치에 대해 **앱 자동 실행** 설정이 제공됩니다. 기본값은 **False**입니다.

iOS 27 DDM 정책 지원: `ios.mdm.ios27.ddm.support` 속성이 **True**로 설정된 경우, XenMobile Server 콘솔에서 iOS 27에 도입된 iOS 선언적 관리 정책을 구성할 수 있습니다. 기본값은 **True**입니다.

장치 및 앱 정책

XenMobile® 장치 및 앱 정책을 통해 다음과 같은 요소 간의 균형을 최적화할 수 있습니다.

- 엔터프라이즈 보안
- 기업 데이터 및 자산 보호
- 사용자 개인 정보 보호
- 생산적이고 긍정적인 사용자 경험

이러한 요소 간의 최적 균형은 달라질 수 있습니다. 예를 들어, 금융과 같이 규제가 엄격한 조직은 사용자 생산성이 주요 고려 사항인 교육 및 소매와 같은 다른 산업보다 더 엄격한 보안 제어가 필요합니다.

사용자의 ID, 장치, 위치 및 연결 유형을 기반으로 정책을 중앙에서 제어하고 구성하여 기업 콘텐츠의 악의적인 사용을 제한할 수 있습니다. 장치를 분실하거나 도난당한 경우 비즈니스 애플리케이션 및 데이터를 원격으로 비활성화, 잠금 또는 초기화할 수 있습니다. 전반적인 결과는 보안 및 관리 제어를 보장하면서 직원 만족도와 생산성을 높이는 솔루션입니다.

이 문서의 주요 초점은 보안과 관련된 다양한 장치 및 앱 정책입니다.

보안 위험을 해결하는 정책

XenMobile 장치 및 앱 정책은 다음과 같이 보안 위험을 초래할 수 있는 여러 상황을 해결합니다.

- 사용자가 신뢰할 수 없는 장치 및 예측할 수 없는 위치에서 앱 및 데이터에 액세스하려고 할 때.
- 사용자가 장치 간에 데이터를 전달할 때.
- 승인되지 않은 사용자가 데이터에 액세스하려고 할 때.
- 회사를 떠난 사용자가 자신의 장치(BYOD)를 사용했을 때.
- 사용자가 장치를 분실했을 때.
- 사용자가 항상 네트워크에 안전하게 액세스해야 할 때.
- 사용자가 자신의 장치를 관리하고 업무 데이터와 개인 데이터를 분리해야 할 때.
- 장치가 유휴 상태이고 사용자 자격 증명 확인이 다시 필요할 때.
- 사용자가 민감한 콘텐츠를 보호되지 않은 이메일 시스템에 복사하여 붙여넣을 때.
- 사용자가 개인 계정과 회사 계정을 모두 보유한 장치에서 민감한 데이터가 포함된 이메일 첨부 파일 또는 웹 링크를 받을 때.

이러한 상황은 회사 데이터를 보호할 때 두 가지 주요 관심 영역과 관련이 있습니다. 즉, 데이터가 다음 상태일 때입니다.

- 저장 중
- 전송 중

XenMobile이 저장 중인 데이터를 보호하는 방법

모바일 장치에 저장된 데이터는 저장 중인 데이터라고 합니다. XenMobile은 iOS 및 Android 플랫폼에서 제공하는 장치 암호화를 사용합니다. XenMobile은 Citrix MAM SDK를 통해 제공되는 규정 준수 확인과 같은 기능으로 플랫폼 기반 암호화를 보완합니다.

XenMobile의 모바일 애플리케이션 관리(MAM) 기능은 모바일 생산성 앱, MDX 지원 앱 및 관련 데이터에 대한 완벽한 관리, 보안 및 제어를 가능하게 합니다.

Mobile Apps SDK는 Citrix MDX 앱 컨테이너 기술을 사용하여 XenMobile 배포용 앱을 활성화합니다. 컨테이너 기술은 사용자 장치에서 회사 앱 및 데이터를 개인 앱 및 데이터와 분리합니다. 데이터 분리를 통해 사용자 지정 개발, 타사 또는 BYO 모바일 앱을 포괄적인 정책 기반 제어로 보호할 수 있습니다.

XenMobile은 앱 수준 암호화도 포함합니다. XenMobile은 장치 암호가 필요 없으며 정책을 적용하기 위해 장치를 관리할 필요 없이 MDX 지원 앱 내에 저장된 데이터를 별도로 암호화합니다.

정책 및 Mobile Apps SDK를 통해 다음을 수행할 수 있습니다.

- 안전한 모바일 컨테이너에서 업무용 및 개인용 앱과 데이터를 분리합니다.
- 암호화 및 기타 모바일 데이터 손실 방지(DLP) 기술로 앱을 보호합니다.

MDX 정책은 다양한 운영 제어를 제공합니다. MAM SDK가 활성화되거나 MDX로 래핑된 앱 간의 원활한 통합을 활성화하는 동시에 모든 통신을 제어할 수 있습니다. 이러한 방식으로 데이터가 MAM SDK가 활성화되거나 MDX로 래핑된 앱에서만 액세스할 수 있도록 하는 것과 같은 정책을 적용할 수 있습니다.

장치 및 앱 정책 제어 외에도, 저장된 데이터를 보호하는 가장 좋은 방법은 암호화입니다. XenMobile은 MDX 지원 앱에 저장된 모든 데이터에 암호화 계층을 추가하여 공용 파일 암호화, 개인 파일 암호화 및 암호화 제외와 같은 기능에 대한 정책 제어를 제공합니다. Mobile Apps SDK는 보호된 Citrix Secret Vault에 저장된 키와 함께 FIPS 140-2 준수 AES 256비트 암호화를 사용합니다.

XenMobile이 전송 중인 데이터를 보호하는 방법

사용자 모바일 장치와 내부 네트워크 간에 이동하는 데이터는 전송 중인 데이터라고 합니다. MDX 앱 컨테이너 기술은 Citrix Gateway를 통해 내부 네트워크에 애플리케이션별 VPN 액세스를 제공합니다.

직원이 모바일 장치에서 보안 엔터프라이즈 네트워크에 있는 다음 리소스에 액세스하려는 상황을 고려해 보십시오.

- 회사 이메일 서버
- 회사 인트라넷에서 호스팅되는 SSL 지원 웹 애플리케이션
- 파일 서버 또는 Microsoft SharePoint에 저장된 문서

MDX는 애플리케이션별 마이크로 VPN을 통해 모바일 장치에서 이러한 모든 엔터프라이즈 리소스에 대한 액세스를 가능하게 합니다. 각 장치에는 자체 전용 마이크로 VPN 터널이 있습니다.

마이크로 VPN 기능은 신뢰할 수 없는 모바일 장치의 보안을 손상시킬 수 있는 장치 전체 VPN을 필요로 하지 않습니다. 결과적으로 내부 네트워크는 전체 기업 시스템을 감염시킬 수 있는 맬웨어 또는 공격에 노출되지 않습니다. 기업 모바일 앱과 개인 모바일 앱은 하나의 장치에서 공존할 수 있습니다.

훨씬 더 강력한 수준의 보안을 제공하기 위해, 인증 및 앱과의 마이크로 VPN 세션에 사용되는 대체 Citrix Gateway 정책으로 MDX 지원 앱을 구성할 수 있습니다. 온라인 세션 필수 정책과 함께 대체 Citrix Gateway를 사용하여 앱이 특정 게이트웨이에 다시 인증하도록 강제할 수 있습니다. 이러한 게이트웨이는 일반적으로 다른 (더 높은 보증) 인증 요구 사항 및 트래픽 관리 정책을 가집니다.

보안 기능 외에도 마이크로 VPN 기능은 압축 알고리즘을 포함한 데이터 최적화 기술도 제공합니다. 압축 알고리즘은 다음을 보장합니다.

- 최소한의 데이터만 전송됩니다.
- 전송은 가능한 한 가장 빠른 시간 내에 이루어집니다. 속도는 사용자 경험을 향상시키며, 이는 모바일 장치 채택의 핵심 성공 요인입니다.

다음과 같은 상황에서 장치 정책을 주기적으로 재평가하십시오.

- 장치 운영 체제 업데이트 릴리스로 인해 XenMobile의 새 버전에 새롭거나 업데이트된 정책이 포함될 때
- 장치 유형을 추가할 때:

  많은 정책이 모든 장치에 공통적이지만, 각 장치에는 해당 운영 체제에 특정한 정책 세트가 있습니다. 결과적으로 iOS, Android 및 Windows 장치 간에, 심지어는 다른 제조업체의 Android 장치 간에도 차이점을 발견할 수 있습니다.
- 새로운 기업 보안 정책 또는 규정 준수 규정과 같은 기업 또는 산업 변화에 맞춰 XenMobile 운영을 동기화하기 위해
- MAM SDK의 새 버전에 새롭거나 업데이트된 정책이 포함될 때
- 앱을 추가하거나 업데이트할 때
- 새로운 앱 또는 새로운 요구 사항으로 인해 사용자에게 새로운 워크플로를 통합하기 위해

앱 정책 및 사용 사례 시나리오

Secure Hub를 통해 사용할 수 있는 앱을 선택할 수 있지만, 해당 앱이 XenMobile과 상호 작용하는 방식도 정의하고 싶을 수 있습니다. 앱 정책을 사용하십시오.

- 특정 시간 기간이 경과한 후 사용자가 인증하도록 하려면.
- 사용자에게 정보에 대한 오프라인 액세스를 제공하려면.

다음 섹션에는 일부 정책 및 사용 예시가 포함되어 있습니다.

- MAM SDK를 사용하여 iOS 및 Android 앱에 통합할 수 있는 타사 정책 목록은 MAM SDK 개요를 참조하십시오.
- 플랫폼별 모든 MDX 정책 목록은 MDX 정책 개요를 참조하십시오.

인증 정책

- **장치 암호**

  이 정책을 사용하는 이유: 장치 암호 정책을 사용하도록 설정하여 장치에 장치 암호가 활성화된 경우에만 사용자가 MDX 앱에 액세스할 수 있도록 합니다. 이 기능은 장치 수준에서 iOS 암호화를 사용하도록 보장합니다.

  사용자 예시: 이 정책을 사용하도록 설정하면 사용자가 MDX 앱에 액세스하기 전에 iOS 장치에 암호를 설정해야 합니다.

- **앱 암호**

  이 정책을 사용하는 이유: 앱 암호 정책을 사용하도록 설정하여 Secure Hub가 사용자가 앱을 열고 데이터에 액세스하기 전에 관리되는 앱에 인증하도록 프롬프트를 표시하게 합니다. 사용자는 XenMobile Server 설정의 클라이언트 속성에서 구성한 내용에 따라 Active Directory 암호, Citrix PIN 또는 iOS TouchID로 인증할 수 있습니다. 클라이언트 속성에서 비활성 타이머를 설정하여 계속 사용하는 경우 타이머가 만료될 때까지 Secure Hub가 사용자에게 관리되는 앱에 다시 인증하도록 프롬프트를 표시하지 않도록 할 수 있습니다.

  앱 암호는 장치 암호와 다릅니다. 장치 암호 정책이 장치로 푸시되면 Secure Hub는 사용자에게 암호 또는 PIN을 구성하도록 프롬프트를 표시하며, 사용자는 장치를 켜거나 비활성 타이머가 만료될 때 장치에 액세스하려면 이를 잠금 해제해야 합니다. 자세한 내용은 XenMobile의 인증을 참조하십시오.

  사용자 예시: 장치에서 Citrix Secure Web™ 애플리케이션을 열 때, 비활성 기간이 만료된 경우 사용자는 웹 사이트를 탐색하기 전에 Citrix PIN을 입력해야 합니다.

- **온라인 세션 필요**

이 정책을 사용하는 이유: 애플리케이션이 실행을 위해 웹 앱(웹 서비스)에 대한 액세스를 필요로 하는 경우, XenMobile이 앱을 사용하기 전에 사용자에게 엔터프라이즈 네트워크에 연결하거나 활성 세션을 갖도록 프롬프트를 표시하도록 이 정책을 사용하도록 설정합니다.

사용자 예시: 사용자가 온라인 세션 필요 정책이 활성화된 MDX 앱을 열려고 할 때, 셀룰러 또는 Wi-Fi 서비스를 사용하여 네트워크에 연결하기 전까지는 앱을 사용할 수 없습니다.

- **최대 오프라인 기간**

이 정책을 사용하는 이유: 이 정책을 추가 보안 옵션으로 사용하여 사용자가 앱 권한을 재확인하고 XenMobile에서 정책을 새로 고치지 않고 장시간 오프라인으로 앱을 실행할 수 없도록 합니다.

사용자 예시: 최대 오프라인 기간으로 MDX 앱을 구성하면 사용자는 오프라인 타이머 기간이 만료될 때까지 앱을 오프라인으로 열고 사용할 수 있습니다. 그 시점에서 사용자는 셀룰러 또는 Wi-Fi 서비스를 통해 네트워크에 다시 연결하고, 메시지가 표시되면 다시 인증해야 합니다.

기타 액세스 정책

- **앱 업데이트 유예 기간(시간)**

이 정책을 사용하는 이유: 앱 업데이트 유예 기간은 XenMobile Store에 최신 버전이 릴리스된 앱을 사용자가 업데이트해야 하기 전까지 사용할 수 있는 시간입니다. 만료 시점에 사용자는 앱의 데이터에 액세스하기 전에 앱을 업데이트해야 합니다. 이 값을 설정할 때는 모바일 인력, 특히 해외 여행 시 장기간 오프라인 상태를 경험할 수 있는 인력의 요구 사항을 염두에 두십시오.

사용자 예시: XenMobile Store에 Secure Mail의 새 버전을 로드한 다음 앱 업데이트 유예 기간을 6시간으로 설정합니다. 모든 Secure Mail 사용자는 6시간이 만료될 때까지 Secure Mail 앱을 업데이트하라는 메시지를 받습니다. 6시간이 만료되면 Secure Hub는 사용자를 XenMobile Store로 안내합니다.

- **활성 폴링 기간(분)**

이 정책을 사용하는 이유: 활성 폴링 기간은 XenMobile이 앱 잠금 및 앱 초기화와 같은 보안 작업을 수행할 시기를 앱에서 확인하는 간격입니다.

사용자 예시: 활성 폴링 기간 정책을 60분으로 설정하면 XenMobile에서 장치로 앱 잠금 명령을 보낼 때 마지막 폴링이 발생한 시점으로부터 60분 이내에 잠금이 발생합니다.

비준수 장치 동작 정책

장치가 최소 규정 준수 요구 사항 미만으로 떨어지면 비준수 장치 동작 정책을 통해 수행할 작업을 선택할 수 있습니다. 자세한 내용은 비준수 장치 동작을 참조하십시오.

앱 상호 작용 정책

이 정책을 사용하는 이유: 앱 상호 작용 정책을 사용하여 MDX 앱에서 장치의 다른 앱으로 문서 및 데이터 흐름을 제어합니다. 예를 들어, 사용자가 컨테이너 외부의 개인 앱으로 데이터를 이동하거나 컨테이너 외부에서 컨테이너화된 앱으로 데이터를 붙여넣는 것을 방지할 수 있습니다.

사용자 예시: 앱 상호 작용 정책을 제한됨으로 설정하면 사용자는 Secure Mail에서 Secure Web으로 텍스트를 복사할 수 있지만, 컨테이너 외부에 있는 개인 Safari 또는 Chrome 브라우저로는 해당 데이터를 복사할 수 없습니다. 또한 사용자는 Secure Mail에서 첨부된 문서를 Citrix Files 또는 Quick Edit으로 열 수 있지만, 컨테이너 외부에 있는 개인 파일 보기 앱으로는 첨부된 문서를 열 수 없습니다.

앱 제한 정책

이 정책을 사용하는 이유: 앱 제한 정책을 사용하여 MDX 앱이 열려 있는 동안 사용자가 액세스할 수 있는 기능을 제어합니다. 이는 앱이 실행되는 동안 악의적인 활동이 발생하지 않도록 하는 데 도움이 됩니다. 앱 제한 정책은 iOS와 Android 간에 약간 다릅니다. 예를 들어, iOS에서는 MDX 앱이 실행되는 동안 iCloud에 대한 액세스를 차단할 수 있습니다. Android에서는 MDX 앱이 실행되는 동안 NFC 사용을 중지할 수 있습니다.

사용자 예시: MDX 앱에서 iOS의 받아쓰기를 차단하는 앱 제한 정책을 활성화하면 사용자는 MDX 앱이 실행되는 동안 iOS 키보드의 받아쓰기 기능을 사용할 수 없습니다. 따라서 사용자가 받아쓰기한 데이터는 안전하지 않은 타사 클라우드 받아쓰기 서비스로 전달되지 않습니다. 사용자가 컨테이너 외부의 개인 앱을 열면 받아쓰기 옵션은 개인 통신을 위해 사용자에게 계속 제공됩니다.

앱 네트워크 액세스 정책

이 정책을 사용하는 이유: 장치 컨테이너의 MDX 앱에서 회사 네트워크 내에 있는 데이터에 액세스할 수 있도록 앱 네트워크 액세스 정책을 사용합니다. 네트워크 액세스 정책의 경우 **내부 네트워크로 터널링** 옵션을 설정하여 MDX 앱에서 Citrix ADC를 통해 백엔드 웹 서비스 또는 데이터 저장소로 마이크로 VPN을 자동화합니다.

사용자 예시: 사용자가 터널링이 활성화된 Secure Web과 같은 MDX 앱을 열면, VPN을 시작할 필요 없이 브라우저가 열리고 인트라넷 사이트가 실행됩니다. Secure Web 앱은 마이크로 VPN 기술을 사용하여 내부 사이트에 자동으로 액세스합니다.

앱 지리적 위치 및 지오펜싱 정책

이 정책을 사용하는 이유: 앱 지리적 위치 및 지오펜싱을 제어하는 정책에는 중심점 경도, 중심점 위도 및 반경이 포함됩니다. 이러한 정책은 MDX 앱의 데이터에 대한 액세스를 특정 지리적 영역으로 제한합니다. 이 정책은 위도 및 경도 좌표의 반경으로 지리적 영역을 정의합니다. 사용자가 정의된 반경 밖에서 앱을 사용하려고 하면 앱이 잠긴 상태로 유지되고 사용자는 앱 데이터에 액세스할 수 없습니다.

사용자 예시: 사용자는 사무실 위치에 있는 동안 인수합병 데이터에 액세스할 수 있습니다. 사무실 위치를 벗어나면 이 중요한 데이터에 액세스할 수 없게 됩니다.

Secure Mail 앱 정책

- **백그라운드 네트워크 서비스**

  이 정책을 사용하는 이유: Secure Mail의 백그라운드 네트워크 서비스는 Citrix Gateway를 통해 연결하기 위해 사실상 SOCKS5 프록시인 STA(Secure Ticket Authority)를 사용합니다. STA는 마이크로 VPN에 비해 장기 연결을 지원하고 배터리 수명을 향상시킵니다. 따라서 STA는 지속적으로 연결되는 메일에 이상적입니다. Citrix는 Secure Mail에 대해 이러한 설정을 구성할 것을 권장합니다. XenMobile용 Citrix ADC 마법사는 Secure Mail용 STA를 자동으로 설정합니다.

  사용자 예시: STA가 활성화되지 않은 상태에서 Android 사용자가 Secure Mail을 열면, 장치에 계속 열려 있는 VPN을 열라는 메시지가 표시됩니다. STA가 활성화된 상태에서 Android 사용자가 Secure Mail을 열면, Secure Mail은 VPN 없이 원활하게 연결됩니다.

- **기본 동기화 간격**

  이 정책을 사용하는 이유: 이 설정은 사용자가 Secure Mail에 처음 액세스할 때 Secure Mail로 동기화되는 기본 이메일 일수를 지정합니다. 2주 분량의 이메일은 3일 분량보다 동기화하는 데 시간이 더 오래 걸리며 사용자 설정 프로세스를 지연시킵니다.

  사용자 예시: 사용자가 Secure Mail을 처음 설정할 때 기본 동기화 간격이 3일로 설정되어 있으면, 현재부터 과거 3일 이내에 받은 모든 이메일을 받은 편지함에서 볼 수 있습니다. 사용자가 3일보다 오래된 이메일을 보려면 검색을 수행할 수 있습니다. 그러면 Secure Mail은 서버에 저장된 오래된 이메일을 표시합니다. Secure Mail을 설치한 후 각 사용자는 자신의 필요에 맞게 이 설정을 변경할 수 있습니다.

장치 정책 및 사용 사례 동작

장치 정책(MDM 정책이라고도 함)은 XenMobile이 장치와 작동하는 방식을 결정합니다. 많은 정책이 모든 장치에 공통적이지만, 각 장치에는 해당 운영 체제에 특정한 정책 세트가 있습니다. 다음 목록에는 일부 장치 정책이 포함되어 있으며, 이를 사용하는 방법에 대해 설명합니다. 모든 장치 정책 목록은 장치 정책 아래의 문서를 참조하십시오.

- **앱 인벤토리 정책**

  이 정책을 사용하는 이유: 사용자가 설치한 앱을 확인해야 하는 경우 앱 인벤토리 정책을 장치에 배포합니다. 앱 인벤토리 정책을 배포하지 않으면 사용자가 XenMobile Store에서 설치한 앱만 볼 수 있으며 개인적으로 설치한 애플리케이션은 볼 수 없습니다. 회사 장치에서 특정 앱이 실행되지 않도록 차단하려면 이 정책을 사용해야 합니다.

  사용자 예시: MDM 관리 장치를 사용하는 사용자는 이 기능을 비활성화할 수 없습니다. 사용자가 개인적으로 설치한 애플리케이션은 XenMobile 관리자에게 표시됩니다.

- **앱 잠금 정책**

이 정책을 사용하는 이유: Android용 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 배포합니다. 차단된 앱에 대한 사용자 액세스를 제공하기 위해 재정의 암호를 설정할 수 있습니다.

사용자 예시: Angry Birds 앱을 차단하는 앱 잠금 정책을 배포했다고 가정해 보겠습니다. 사용자는 Google Play에서 Angry Birds 앱을 설치할 수 있지만, 앱을 열면 관리자가 앱을 차단했다는 메시지가 표시됩니다.

- **연결 예약 정책**

  이 정책을 사용하는 이유: Windows Mobile 장치가 MDM 관리, 앱 푸시 및 정책 배포를 위해 XenMobile Server에 다시 연결할 수 있도록 연결 예약 정책을 사용해야 합니다. Android, Android Enterprise 및 Chrome OS 장치의 경우 이 정책 대신 Google Firebase Cloud Messaging(FCM)을 사용하여 XenMobile Server에 대한 연결을 제어합니다. 예약 옵션은 다음과 같습니다.

  - **항상:** 연결을 영구적으로 유지합니다. Citrix는 최적화된 보안을 위해 이 옵션을 권장합니다. **항상**을 선택할 때는 연결 타이머 정책도 사용하여 연결로 인해 배터리가 소모되지 않도록 합니다. 연결을 유지함으로써 장치에 원격 초기화 또는 잠금과 같은 보안 명령을 온디맨드로 푸시할 수 있습니다. 또한 장치에 배포하는 각 정책에서 배포 일정 옵션 **항상 켜진 연결을 위해 배포**를 선택해야 합니다.
  - **안 함:** 수동으로 연결합니다. Citrix는 **안 함** 옵션이 장치에 보안 정책을 배포하는 것을 방지하므로 사용자가 새로운 앱이나 정책을 받지 못하게 되므로 프로덕션 배포에 이 옵션을 권장하지 않습니다.
  - **매번:** 지정된 간격으로 연결합니다. 이 옵션이 적용되고 잠금 또는 원격 초기화와 같은 보안 정책을 보내면 XenMobile은 장치가 다음에 연결할 때 장치에서 정책을 처리합니다.
  - **일정 정의:** 이 옵션을 사용하면 XenMobile은 네트워크 연결 손실 후 사용자 장치를 XenMobile Server에 다시 연결하려고 시도하고, 정의한 시간 내에 정기적인 간격으로 제어 패킷을 전송하여 연결을 모니터링합니다.

  사용자 예시: 등록된 장치에 암호 정책을 배포하려고 합니다. 예약 정책은 장치가 새 정책을 수집하기 위해 정기적인 간격으로 서버에 다시 연결되도록 합니다.

- **자격 증명 정책**

  이 정책을 사용하는 이유: Wi-Fi 정책과 함께 자주 사용되는 자격 증명 정책을 사용하면 인증서 인증이 필요한 내부 리소스에 대한 인증을 위해 인증서를 배포할 수 있습니다.

  사용자 예시: 장치에 무선 네트워크를 구성하는 Wi-Fi 정책을 배포합니다. Wi-Fi 네트워크는 인증을 위해 인증서가 필요합니다. 자격 증명 정책은 운영 체제 키 저장소에 저장되는 인증서를 배포합니다. 사용자는 내부 리소스에 연결할 때 해당 인증서를 선택할 수 있습니다.

- **Exchange 정책**

이 정책을 사용하는 이유: XenMobile을 사용하면 Microsoft Exchange ActiveSync 이메일을 전달하는 두 가지 옵션이 있습니다.

- **Secure Mail 앱:** 공용 앱 스토어 또는 XenMobile Store에서 배포하는 Secure Mail 앱을 사용하여 이메일을 전달합니다.
- **기본 이메일 앱:** Exchange 정책을 사용하여 장치의 기본 이메일 클라이언트에 ActiveSync 이메일을 사용하도록 설정합니다. 기본 이메일용 Exchange 정책을 사용하면 ${user.username}으로 사용자 이름을 채우고 ${user.domain}으로 사용자 도메인을 채우는 것과 같이 Active Directory 속성에서 사용자 데이터를 채우는 데 매크로를 사용할 수 있습니다.

사용자 예시: Exchange 정책을 푸시하면 Exchange Server 세부 정보를 장치로 보냅니다. Secure Hub는 사용자에게 인증을 요청하고 이메일 동기화가 시작됩니다.

- **위치 정책**

  이 정책을 사용하는 이유: 장치에 Secure Hub용 GPS가 활성화되어 있는 경우 위치 정책을 통해 지도에서 장치의 위치를 파악할 수 있습니다. 이 정책을 배포한 다음 XenMobile Server에서 위치 찾기 명령을 보내면 장치는 위치 좌표로 응답합니다.

  사용자 예시: 위치 정책을 배포하고 장치에서 GPS가 활성화된 경우, 사용자가 장치를 분실하면 XenMobile Self-Help Portal에 로그인하여 위치 찾기 옵션을 선택하여 지도에서 장치의 위치를 확인할 수 있습니다. 사용자는 Secure Hub가 위치 서비스를 사용하도록 허용할지 여부를 선택합니다. 사용자가 직접 장치를 등록할 때는 위치 서비스 사용을 강제할 수 없습니다. 이 정책을 사용하는 또 다른 고려 사항은 배터리 수명에 미치는 영향입니다.

- **암호 정책**

  이 정책을 사용하는 이유: 암호 정책을 사용하면 관리되는 장치에 PIN 코드 또는 암호를 강제 적용할 수 있습니다. 이 암호 정책을 통해 장치의 암호 복잡성과 시간 제한을 설정할 수 있습니다.

  사용자 예시: 관리되는 장치에 암호 정책을 배포하면 Secure Hub는 사용자에게 암호 또는 PIN을 구성하도록 요청하며, 사용자는 장치를 켜거나 비활성 타이머가 만료될 때 장치에 액세스하려면 이를 잠금 해제해야 합니다.

- **프로필 제거 정책**

  이 정책을 사용하는 이유: 사용자 그룹에 정책을 배포한 후 나중에 해당 정책을 일부 사용자에게서 제거해야 한다고 가정해 봅시다. 프로필 제거 정책을 생성하고 배포 규칙을 사용하여 지정된 사용자 이름에만 프로필 제거 정책을 배포함으로써 선택한 사용자에 대한 정책을 제거할 수 있습니다.

  사용자 예시: 사용자 장치에 프로필 제거 정책을 배포할 때 사용자는 변경 사항을 인지하지 못할 수 있습니다. 예를 들어, 프로필 제거 정책이 장치 카메라를 비활성화했던 제한을 제거하더라도 사용자는 카메라 사

용이 이제 허용된다는 것을 알지 못할 것입니다. 변경 사항이 사용자 경험에 영향을 미칠 때 사용자에게 알리는 것을 고려하십시오.

- **제한 정책**

  이 정책을 사용하는 이유: 제한 정책은 관리되는 장치에서 기능 및 기능을 잠그고 제어할 수 있는 다양한 옵션을 제공합니다. 장치의 카메라 또는 마이크 비활성화부터 로밍 규칙 및 앱 스토어와 같은 타사 서비스 액세스 강제 적용에 이르기까지 지원되는 장치에 대해 수백 가지 제한 옵션을 활성화할 수 있습니다.

  사용자 예시: iOS 장치에 제한을 배포하는 경우 사용자는 iCloud 또는 Apple App Store에 액세스하지 못할 수 있습니다.

- **이용 약관 정책**

  이 정책을 사용하는 이유: 장치 관리의 법적 의미에 대해 사용자에게 알려야 할 수도 있습니다. 또한 기업 데이터가 장치로 푸시될 때 사용자가 보안 위험을 인지하도록 해야 할 수도 있습니다. 사용자 지정 이용 약관 문서를 통해 사용자가 등록하기 전에 규칙 및 공지를 게시할 수 있습니다.

  사용자 예시: 사용자는 등록 과정에서 이용 약관 정보를 확인합니다. 명시된 조건을 수락하지 않으면 등록 과정이 종료되고 기업 데이터에 액세스할 수 없습니다. HR/법무/준수 팀에 제공할 보고서를 생성하여 누가 약관을 수락했는지 또는 거부했는지 보여줄 수 있습니다.

- **VPN 정책**

  이 정책을 사용하는 이유: VPN 정책을 사용하여 이전 VPN Gateway 기술을 사용하는 백엔드 시스템에 대한 액세스를 제공합니다. 이 정책은 Cisco AnyConnect, Juniper 및 Citrix VPN을 포함한 다양한 VPN 공급자를 지원합니다. VPN 게이트웨이가 이 옵션을 지원하는 경우 이 정책을 CA에 연결하고 주문형 VPN을 활성화할 수도 있습니다.

  사용자 예시: VPN 정책이 활성화되면 사용자가 내부 도메인에 액세스할 때 사용자 장치가 VPN 연결을 엽니다.

- **웹 클립 정책**

  이 정책을 사용하는 이유: 웹사이트로 직접 열리는 아이콘을 장치에 푸시하려면 웹 클립 정책을 사용하십시오. 웹 클립에는 웹사이트 링크가 포함되어 있으며 사용자 지정 아이콘을 포함할 수 있습니다. 장치에서 웹 클립은 앱 아이콘처럼 보입니다.

  사용자 예시: 사용자는 웹 클립 아이콘을 클릭하여 액세스해야 하는 서비스를 제공하는 인터넷 사이트를 열 수 있습니다. 웹 링크를 사용하는 것이 브라우저 앱을 열고 링크 주소를 입력해야 하는 것보다 편리합니다.

- **WiFi 정책**

이 정책을 사용하는 이유: Wi-Fi 정책을 사용하면 SSID, 인증 데이터 및 구성 데이터와 같은 Wi-Fi 네트워크 세부 정보를 관리되는 장치에 배포할 수 있습니다.

사용자 예시: Wi-Fi 정책을 배포하면 장치가 Wi-Fi 네트워크에 자동으로 연결되고 사용자를 인증하여 네트워크에 액세스할 수 있습니다.

- **Windows 정보 보호 정책**

  이 정책을 사용하는 이유: 기업 데이터의 잠재적인 유출을 방지하려면 Windows Information Protection(WIP) 정책을 사용하십시오. 설정한 적용 수준에서 Windows Information Protection이 필요한 앱을 지정할 수 있습니다. 예를 들어, 부적절한 데이터 공유를 차단하거나 부적절한 데이터 공유에 대해 경고하고 사용자가 정책을 재정의하도록 허용할 수 있습니다. 부적절한 데이터 공유를 기록하고 허용하면서 WIP를 자동으로 실행할 수 있습니다.

  사용자 예시: 부적절한 데이터 공유를 차단하도록 WIP 정책을 구성했다고 가정해 보겠습니다. 사용자가 보호된 파일을 보호되지 않은 위치에 복사하거나 저장하면 다음과 유사한 메시지가 나타납니다. 이 위치에 업무용으로 보호된 콘텐츠를 배치할 수 없습니다.

- **XenMobile Store 정책**

  이 정책을 사용하는 이유: XenMobile Store는 관리자가 사용자가 필요로 하는 모든 기업 앱 및 데이터 리소스를 게시할 수 있는 통합 앱 스토어입니다. 관리자는 다음을 추가할 수 있습니다.

  - 웹 앱, SaaS 앱, MAM SDK 지원 앱 또는 MDX 래핑 앱
  - Citrix 모바일 생산성 앱
  - .ipa 또는 .apk 파일과 같은 기본 모바일 앱
  - Apple 앱 스토어 및 Google 플레이 앱
  - 웹 링크
  - Citrix StoreFront를 사용하여 게시된 Citrix Virtual Apps™

  사용자 예시: 사용자가 장치를 XenMobile에 등록한 후 Citrix Secure Hub™ 앱을 통해 XenMobile Store에 액세스합니다. 그러면 사용자는 자신에게 제공되는 모든 기업 앱 및 서비스를 볼 수 있습니다. 사용자는 앱을 클릭하여 설치하고, 데이터에 액세스하고, 앱을 평가 및 검토하고, XenMobile Store에서 앱 업데이트를 다운로드할 수 있습니다.

사용자 등록 옵션

사용자는 여러 가지 방법으로 XenMobile에 장치를 등록할 수 있습니다. 세부 사항을 고려하기 전에 MDM+MAM, MDM 또는 MAM에 등록할 장치를 결정하십시오. 이러한 관리 모드에 대한 자세한 내용은 관리 모드를 참조하십시오.

가장 높은 수준에서 네 가지 등록 옵션이 있습니다.

- **등록 초대:** 사용자에게 등록 초대 또는 초대 URL을 보냅니다. 등록 초대 및 URL은 Windows 장치에서 사용할 수 없습니다.
- **셀프 도움말 포털:** 사용자가 Secure Hub를 다운로드하고 장치를 등록하거나 등록 초대를 자신에게 보낼 수 있는 포털을 설정합니다.
- **수동 등록:** 이메일, 핸드북 또는 기타 통신을 통해 사용자에게 시스템 등록이 가능함을 알립니다. 그런 다음 사용자는 Secure Hub를 다운로드하고 장치를 수동으로 등록합니다.
- **엔터프라이즈:** 장치 등록을 위한 또 다른 옵션은 Apple 배포 프로그램 및 Google Android Enterprise를 통하는 것입니다. 이러한 각 프로그램을 통해 사전 구성되어 직원이 바로 사용할 수 있는 장치를 구매할 수 있습니다. 자세한 내용은 Apple 지원의 Apple 배포 프로그램 문서와 Android Enterprise 웹사이트의 Google Android Enterprise 문서를 참조하십시오.

등록 초대

iOS, macOS, Android Enterprise 및 레거시 Android 장치 사용자에게 등록 초대를 이메일로 보낼 수 있습니다. 등록 초대 및 URL은 Windows 장치에서 사용할 수 없습니다.

또한 SMTP 또는 SMS를 통해 iOS, macOS, Android 또는 Windows 장치 사용자에게 설치 링크를 보낼 수 있습니다. 자세한 내용은 장치 등록을 참조하십시오.

등록 초대 방법을 사용하기로 선택한 경우 다음을 수행할 수 있습니다.

- **초대 URL**, **초대 URL + PIN**, 또는 **초대 URL + 암호** 등록 보안 모드를 선택합니다.
- 모드의 모든 조합을 사용합니다.
- **설정** 페이지에서 모드를 활성화하거나 비활성화합니다.

각 등록 보안 모드에 대한 자세한 내용은 등록 보안 모드 구성을 참조하십시오.

초대는 여러 용도로 사용됩니다. 초대의 가장 일반적인 용도는 시스템을 사용할 수 있으며 사용자가 등록할 수 있음을 알리는 것입니다. 초대 URL은 고유합니다. 사용자가 초대 URL을 사용하면 해당 URL은 더 이상 사용할 수 없습니다. 이 속성을 사용하여 시스템에 등록하는 사용자 또는 장치를 제한할 수 있습니다.

등록 프로필을 구성할 때 Active Directory 그룹을 기반으로 특정 사용자가 등록할 수 있는 장치 수를 제어할 수 있습니다. 예를 들어, 재무 부서에는 사용자당 하나의 장치만 허용할 수 있습니다.

특정 등록 옵션의 추가 비용과 위험을 인지하십시오. 예를 들어, SMS를 사용하여 초대를 보내려면 추가 인프라가 필요합니다. 이 옵션에 대한 자세한 내용은 알림을 참조하십시오.

이메일로 초대를 보내는 것과 함께, 사용자가 Secure Hub 외부에서 이메일에 액세스할 수 있는 방법을 가지고 있는지 확인하십시오. MDM 등록을 위해 Active Directory 암호 대신 일회용 암호(OTP) 등록 보안 모드를 사용할 수 있습니다.

셀프 서비스 포털

셀프 서비스 포털을 통해 등록 초대를 요청할 수 있습니다. 셀프 서비스 포털 설정에 대한 자세한 내용은 등록 보안 모드 구성을 참조하십시오.

수동 등록

수동 등록을 통해 사용자는 AutoDiscovery를 통하거나 서버 정보를 입력하여 XenMobile에 연결합니다. AutoDiscovery를 사용하면 사용자는 이메일 주소 또는 사용자 계정 이름 형식의 Active Directory 자격 증명으로만 로그인합니다. AutoDiscovery가 없으면 서버 주소와 Active Directory 자격 증명을 입력해야 합니다. AutoDiscovery 설정에 대한 자세한 내용은 XenMobile AutoDiscovery 서비스를 참조하십시오.

수동 등록은 여러 가지 방법으로 용이하게 할 수 있습니다. 가이드를 만들고 사용자에게 배포하여 직접 등록하게 할 수 있습니다. IT 부서에서 특정 시간대에 사용자 그룹을 수동으로 등록하게 할 수 있습니다. 사용자가 자격 증명, 서버 정보 또는 둘 다를 입력해야 하는 유사한 방법을 사용할 수 있습니다.

사용자 온보딩

환경을 설정한 후에는 사용자를 환경으로 가져오는 방법을 결정해야 합니다. 이 문서의 이전 섹션에서는 사용자 등록 보안 모드의 세부 사항에 대해 설명합니다. 이 섹션에서는 사용자에게 연락하는 방법에 대해 설명합니다.

개방형 등록 대 선택적 초대

사용자를 온보딩할 때 두 가지 기본 방법을 통해 등록을 허용할 수 있습니다.

- 개방형 등록. 기본적으로 LDAP 자격 증명과 XenMobile® 환경 정보를 가진 모든 사용자가 등록할 수 있습니다.
- 제한된 등록. 초대장을 가진 사용자만 등록하도록 허용하여 사용자 수를 제한할 수 있습니다. Active Directory 그룹별로 개방형 등록을 제한할 수도 있습니다.

초대 방식을 사용하면 사용자가 등록할 수 있는 장치 수를 제한할 수도 있습니다. 대부분의 경우 개방형 등록이 허용되지만, 고려해야 할 몇 가지 사항이 있습니다.

- MAM 등록의 경우, Active Directory 그룹 멤버십을 통해 개방형 등록을 쉽게 제한할 수 있습니다.
- MDM 등록의 경우, Active Directory 그룹 멤버십을 기반으로 등록할 수 있는 장치 수를 제한할 수 있습니다. 환경에서 회사 장치만 허용하는 경우, 이러한 제한은 일반적으로 문제가 되지 않습니다. 그러나 BYOD 환경에서 환경 내 장치 수를 제한하려는 경우 이 방법을 고려해 볼 수 있습니다.

선택적 초대는 개방형 등록보다 약간 더 많은 작업이 필요하므로 일반적으로 덜 자주 수행됩니다. 사용자가 환경에 장치를 등록하려면 각 사용자에게 고유한 초대를 보내야 합니다. 등록 초대장을 보내는 방법에 대한 자세한 내용은 등록 초대장 보내기를 참조하십시오.

Active Directory 그룹을 사용하여 일괄적으로 초대장을 만들 수 있지만, 이 접근 방식은 단계적으로 수행해야 합니다.

사용자에게 처음 연락하기

개방형 등록 또는 선택적 초대 중 하나를 결정하고 해당 환경을 설정한 후에는 사용자에게 등록 옵션을 알려야 합니다.

선택적 초대 방식을 사용하는 경우, 이메일 및 SMS 메시지가 프로세스의 일부입니다. 개방형 등록의 경우 XenMobile 콘솔을 통해 이메일을 보낼 수도 있습니다. 자세한 내용은 등록 초대장 보내기를 참조하십시오.

어떤 경우든 이메일의 경우 SMTP 서버가 필요하며, 문자 메시지의 경우 SMS 서버가 필요하다는 점을 명심하십시오. 이러한 서버는 결정을 내릴 때 고려해야 할 추가 비용이 될 수 있습니다. 방법을 선택하기 전에 새 사용자가 이메일과 같은 정보에 어떻게 액세스할 것으로 예상하는지 고려하십시오. 모든 사용자가 XenMobile을 통해 이메일에 액세스하기를 원한다면 초대 이메일을 보내는 것이 문제가 될 수 있습니다.

개방형 등록 환경의 경우 XenMobile 외부의 다른 수단을 통해 통신을 보낼 수도 있습니다. 이 옵션을 선택하는 경우 모든 관련 정보를 포함해야 합니다. 사용자에게 Secure Hub 앱을 어디서 받을 수 있는지, 등록에 어떤 방법을 사용해야 하는지 알려주십시오. 검색 기능이 꺼져 있는 경우 사용자에게 XenMobile Server 주소도 제공하십시오. AutoDiscovery에 대해 자세히 알아보려면 XenMobile AutoDiscovery Service를 참조하십시오.

XenMobile® 작업 튜닝

XenMobile 작업의 성능과 안정성은 XenMobile 전반의 다양한 설정과 관련되어 있으며, Citrix ADC 및 SQL Server 데이터베이스 구성에 따라 달라집니다. 이 문서에서는 XenMobile 튜닝 및 최적화와 관련하여 관리자가 가장 자주 구성하는 설정에 중점을 둡니다. Citrix는 XenMobile을 배포하기 전에 이 문서의 각 설정을 평가할 것을 권장합니다.

> **중요:**
>
> 이 지침은 XenMobile Server CPU 및 RAM이 장치 수에 적합하다고 가정합니다. 확장성에 대한 자세한 내용은 확장성 및 성능을 참조하십시오.

> 다음 서버 속성은 전체 XenMobile 인스턴스의 작업, 사용자 및 장치에 전역적으로 적용됩니다. 일부 서버 속성을 변경하려면 각 XenMobile Server 노드를 다시 시작해야 합니다. XenMobile은 다시 시작이 필요할 때 알려줍니다.

이러한 튜닝 지침은 클러스터링된 환경과 클러스터링되지 않은 환경 모두에 적용됩니다.

hibernate.c3p0.idle_test_period

이 XenMobile Server 속성(사용자 지정 키)은 연결이 자동으로 유효성 검사되기 전의 유휴 시간을 초 단위로 결정합니다. 키를 다음과 같이 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 유휴 테스트 기간**

hibernate.c3p0.max_size

이 사용자 지정 키는 XenMobile이 SQL Server 데이터베이스에 열 수 있는 최대 연결 수를 결정합니다. XenMobile은 이 사용자 지정 키에 지정한 값을 상한으로 사용합니다. 연결은 필요할 때만 열립니다. 데이터베이스 서버의 용량을 기준으로 설정을 지정하십시오.

클러스터 구성에서 다음 방정식을 참고하십시오. c3p0 연결 수에 노드 수를 곱한 값이 XenMobile이 SQL Server 데이터베이스에 열 수 있는 실제 최대 연결 수와 같습니다.

클러스터 및 비클러스터 구성에서, SQL Server 크기가 작은데 값을 너무 높게 설정하면 피크 로드 시 SQL 측에서 리소스 문제가 발생할 수 있습니다. 값을 너무 낮게 설정하면 사용 가능한 SQL 리소스를 활용하지 못할 수 있습니다.

키를 다음과 같이 구성하십시오. 기본값은 **1000**입니다.

- 키: **hibernate.c3p0.max_size**
- 값: **1000**
- 표시 이름: **hibernate.c3p0.max_size**
- 설명: SQL에 대한 DB 연결

hibernate.c3p0.min_size

이 사용자 지정 키는 XenMobile이 SQL Server 데이터베이스에 여는 최소 연결 수를 결정합니다. 키를 다음과 같이 구성하십시오. 기본값은 **100**입니다.

- 키: **hibernate.c3p0.min_size**
- 값: **100**
- 표시 이름: **hibernate.c3p0.min_size**
- 설명: SQL에 대한 DB 연결

hibernate.c3p0.timeout

이 사용자 지정 키는 유휴 시간 제한을 결정합니다. 데이터베이스 클러스터 장애 조치를 사용하는 경우, Citrix는 이 사용자 지정 키를 추가하고 유휴 시간 제한을 줄이도록 설정할 것을 권장합니다. 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 장치가 APNs 알림이 그동안 전달되지 않았는지 얼마나 자주 확인하는지를 결정합니다. APNs 하트비트 빈도를 늘리면 데이터베이스 통신을 최적화할 수 있습니다. 너무 큰 값은 불필요한 부하를 추가할 수 있습니다. 이 설정은 iOS에만 적용됩니다. 기본값은 **20**시간입니다.

환경에 iOS 장치가 많은 경우 하트비트 간격으로 인해 필요 이상으로 높은 부하가 발생할 수 있습니다. 선택적 초기화, 잠금, 전체 초기화와 같은 보안 작업은 이 하트비트에 의존하지 않습니다. 그 이유는 이러한 작업이 실행될 때 APNs 알림이 장치로 전송되기 때문입니다.

이 값은 Active Directory 그룹 멤버십 변경 후 정책 업데이트가 얼마나 빨리 이루어지는지를 제어합니다. 따라서 부하를 줄이기 위해 이 값을 12시간에서 20시간 사이로 늘리는 것이 종종 적합합니다.

iOS MDM APNS 연결 풀 크기

APNs 연결 풀이 너무 작으면 100대 이상의 장치가 있을 때 APNs 활동 성능에 부정적인 영향을 미칠 수 있습니다. 성능 문제에는 장치에 앱 및 정책 배포 속도 저하, 장치 등록 속도 저하가 포함됩니다. 기본값은 **1**입니다. 약 400대 장치당 이 값을 1씩 늘리는 것이 좋습니다.

auth.ldap.connect.timeout

느린 LDAP 응답을 보완하기 위해 Citrix는 다음 Custom Key에 대한 서버 속성을 추가할 것을 권장합니다.

- 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 보완하기 위해 Citrix는 다음 사용자 지정 키에 대한 서버 속성을 추가할 것을 권장합니다.

- 키: **사용자 지정 키**
- 키: **auth.ldap.read.timeout**
- 값: **60000**
- 표시 이름: **auth.ldap.read.timeout**
- 설명: **LDAP 읽기 시간 초과**

기타 서버 최적화

서버 속성	기본 설정	이 설정을 변경하는 이유?
백그라운드 배포	1,440분	백그라운드 정책 배포 빈도(분). Android 장치의 상시 연결에만 적용됩니다. 정책 배포 빈도를 늘리면 서버 로드가 줄어듭니다. 권장 설정은 **1440**(24시간)입니다.
백그라운드 하드웨어 인벤토리	1,440분	백그라운드 하드웨어 인벤토리 빈도(분). Android 장치의 상시 연결에만 적용됩니다. 하드웨어 인벤토리 빈도를 늘리면 서버 로드가 줄어듭니다. 권장 설정은 **1440**(24시간)입니다.
삭제된 Active Directory 사용자 확인 간격	15분	Active Directory의 표준 동기화 시간은 **15**분입니다. 값 **0**은 XenMobile이 삭제된 Active Directory 사용자를 확인하는 것을 방지합니다. 권장 설정은 **15**분입니다.
MaxNumberOfWorker	3	많은 볼륨 구매 라이선스를 가져올 때 사용되는 스레드 수입니다. 기본값은 **3**입니다. 추가 최적화

		가 필요한 경우 스레드 수를 늘릴 수 있습니다. 그러나 6과 같이 스레드 수가 많으면 볼륨 구매 가져오기로 인해 CPU 사용량이 높아집니다.

SQL DB에서 교착 상태를 확인하고 기록 데이터를 삭제하는 방법

교착 상태가 발생하면 다음 쿼리를 실행하여 교착 상태를 확인합니다. 그런 다음 데이터베이스 관리자 또는 Microsoft SQL 팀이 정보를 확인할 수 있습니다.

SQL 쿼리

```
SELECT


db.name DB_Service,


tl.request_session_id,


wt.blocking_session_id,


OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,


tl.resource_type,


h1.TEXT AS RequestingText,


h2.TEXT AS BlockingTest,
```

```
tl.request_mode

FROM sys.dm_tran_locks AS tl

INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id

INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address =
wt.resource_address

INNER JOIN sys.partitions AS p ON p.hobt_id =
tl.resource_associated_entity_id

INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id =
tl.request_session_id

INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id =
wt.blocking_session_id

CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1

CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2
```

```
GO
```

데이터베이스 정리

중요:

테이블을 변경하기 전에 데이터베이스를 백업하십시오.

1. 다음 쿼리를 실행하여 기록 데이터를 확인합니다.

```
select COUNT(*) as total_record from dbo.EWDEPLOY_HISTO;

select COUNT(*) as total_record from dbo.EWSESS;

select COUNT(*) as total_record from dbo.EWAUDIT;
```

2. 이전 세 테이블에서 데이터를 삭제합니다.

참고:

테이블에 기록 데이터가 표시되지 않을 수 있습니다. 이 경우 해당 테이블에 대한 잘라내기 쿼리 실행을 건너뜁니다.

```
truncate TABLE dbo.EWDEPLOY_HISTO;

truncate TABLE dbo.EWSESS;

truncate TABLE dbo.EWAUDIT;
```

3. 교착 상태로 인해 차단된 SELECT 쿼리의 차단을 해제합니다. 이 단계는 추가 교착 상태를 처리합니다.

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT ON
WITH ROLLBACK IMMEDIATE
```

4. 기본적으로 데이터베이스 정리는 세션 보존 및 감사 보존 데이터를 유지하기 위해 7일로 설정되어 있으며, 이는 많은 사용자에게 높은 값입니다. 정리 값을 1일 또는 2일로 변경합니다. 서버 속성에서 다음 변경을 수행합니다.

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day

zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day

zdm.dbcleanup.auditRetentionTimeInDays=1 day
```

KEYSTORE 테이블에서 고아 정리

XenMobile 노드의 성능이 저하되면 KEYSTORE 테이블이 너무 큰지 확인하십시오. XenMobile Server는 등록 인증서를 ENROLLMENT_CERTIFICATE 및 KEYSTORE 테이블에 저장합니다. 장치를 삭제하거나 다시 등록하면 ENROLLMENT_CERTIFICATE 테이블의 인증서가 삭제됩니다. KEYSTORE 테이블의 항목은 남아 있어 성능 문제를 일으킬 수 있습니다. 다음 절차를 수행하여 KEYSTORE 테이블에서 고아를 정리하십시오.

> **중요:**
>
> 테이블을 변경하기 전에 데이터베이스를 백업하십시오.

1. 다음 쿼리를 실행하여 기록 데이터를 확인합니다.

```
select COUNT(*) from KEYSTORE
```

2. 다음 쿼리를 사용하여 KEYSTORE 테이블에서 고아를 확인합니다.

```
WITH cte(KEYSTORE_ID)

AS (SELECT KEYSTORE_ID

    FROM ENROLLMENT_CERTIFICATE

    UNION

    SELECT CA_KEYSTORE_ID

    FROM LDAP_CONFIG
```

```
    UNION

    SELECT CLIENT_KEYSTORE_ID

    FROM LDAP_CONFIG

    UNION

    SELECT KEYSTORE_ID

    FROM SAML_SERVICE_PROVIDER

    UNION

    SELECT KEYSTORE_ID

    FROM SERVER_CERTIFICATE)
SELECT keystore.id

FROM keystore

    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID

WHERE KEYSTORE_ID IS NULL;
```

3. 다음 쿼리를 사용하여 고아를 지웁니다.

```
WITH cte(KEYSTORE_ID)

    AS (SELECT KEYSTORE_ID

        FROM ENROLLMENT_CERTIFICATE

        UNION

        SELECT CA_KEYSTORE_ID

        FROM LDAP_CONFIG

        UNION
```

```
        SELECT CLIENT_KEYSTORE_ID

        FROM LDAP_CONFIG

        UNION

        SELECT KEYSTORE_ID

        FROM SAML_SERVICE_PROVIDER

        UNION

        SELECT KEYSTORE_ID

        FROM SERVER_CERTIFICATE)

    DELETE FROM keystore

    WHERE id IN

    (

        SELECT keystore.id

        FROM keystore

            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID

        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'

    );
```

4. 검색 효율성을 향상시키기 위해 KEYSTORE 테이블에 인덱스를 추가합니다.

```
DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";

ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;

CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("ID",
"TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "DESCRIPTION",
"ALIAS", "MODIFICATION_DATE");
```

앱 프로비저닝 및 프로비저닝 해제

애플리케이션 프로비저닝은 모바일 앱 수명 주기 관리, 즉 XenMobile® 환경 내에서 모바일 앱을 준비, 구성, 제공 및 관리하는 것을 중심으로 이루어집니다. 경우에 따라 애플리케이션 코드를 개발하거나 수정하는 것도 프로비저닝 프로세스의 일부가 될 수 있습니다. XenMobile은 앱 프로비저닝에 사용할 수 있는 다양한 도구와 프로세스를 갖추고 있습니다.

앱 프로비저닝에 대한 이 문서를 읽기 전에 다음 문서를 읽어보는 것이 좋습니다.

- 앱 - 사용자 커뮤니티

조직에서 사용자에게 제공할 앱 유형을 확정한 후에는 앱의 수명 주기 전반에 걸쳐 앱을 관리하는 프로세스를 개략적으로 설명할 수 있습니다.

앱 프로비저닝 프로세스를 정의할 때 다음 사항을 고려하십시오.

- **앱 프로파일링:** 조직은 제한된 수의 앱으로 시작할 수 있습니다. 그러나 사용자 채택률이 증가하고 환경이 성장함에 따라 관리하는 앱의 수가 빠르게 증가할 수 있습니다. 앱 프로비저닝을 쉽게 관리할 수 있도록 처음부터 특정 앱 프로필을 정의하십시오. 앱 프로파일링은 비기술적인 관점에서 앱을 논리적인 그룹으로 분류하는 데 도움이 됩니다. 예를 들어, 다음 요소를 기반으로 앱 프로필을 만들 수 있습니다.
  - 버전: 추적을 위한 앱 버전
  - 인스턴스: 예를 들어, 다른 수준의 액세스 권한을 가진 다른 사용자 집합에 배포되는 여러 인스턴스
  - 플랫폼: iOS, Android 또는 Windows
  - 대상 사용자: 일반 사용자, 부서, C-레벨 임원
  - 소유권: 앱을 소유한 부서
  - 유형: MDX, 공개, 웹 및 SaaS 또는 웹 링크
  - 업그레이드 주기: 앱이 업그레이드되는 빈도
  - 라이선스: 라이선스 요구 사항 및 소유권
  - MAM SDK 또는 MDX 정책: 모바일 앱에 MDX 기능을 적용하려면
  - 네트워크 액세스: Secure Browse 또는 전체 VPN과 같은 액세스 유형

> **참고:**
>
> 터널링된 웹 SSO는 MDX 설정에서 Secure Browse의 이름입니다. 동작은 동일합니다.

예시:

요소	시큐어 메일	메일	사내	에픽 로버
버전	10.1	10.1	X.x	X.x
인스턴스	VIP	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	공용
업그레이드 주기	분기별	분기별	연간	해당 없음
라이선싱	N/A	N/A	N/A	볼륨 구매
MDX 정책	예	예	예	아니요
네트워크 액세스	VPN	VPN	VPN	공개

- **앱 버전 관리:** 앱 버전 유지 및 추적은 프로비저닝 프로세스의 중요한 부분입니다. 버전 관리는 사용자에게 투명하게 이루어집니다. 사용자는 새 버전의 앱을 다운로드할 수 있을 때만 알림을 받습니다. 귀하의 관점에서, 비프로덕션 환경에서 각 앱 버전을 검토하고 테스트하는 것도 프로덕션에 미치는 영향을 방지하는 데 중요합니다.

  특정 업그레이드가 필요한지 평가하는 것도 중요합니다. 앱 업그레이드는 일반적으로 두 가지 유형으로 나뉩니다. 하나는 특정 버그 수정과 같은 사소한 업그레이드이고, 다른 하나는 앱에 상당한 변경 사항과 개선 사항을 도입하는 주요 릴리스입니다. 어떤 경우든 업그레이드가 필요한지 평가하기 위해 앱의 릴리스 노트를 주의 깊게 검토하십시오.
- **앱 개발:** 개발하는 모바일 앱에 MAM SDK를 통합하면 해당 앱에 MDX 기능을 적용할 수 있습니다. MAM SDK 개요를 참조하십시오.

  MAM SDK는 2023년 7월에 사용 중단될 예정인 MDX Toolkit을 대체합니다. 앱 래핑에 대한 자세한 내용은 MDX Toolkit을 참조하십시오. 래핑된 앱의 앱 프로비저닝 프로세스는 표준 래핑되지 않은 앱의 프로비저닝 프로세스와 다릅니다.
- **앱 보안:** 프로비저닝 프로세스의 일부로 개별 앱 또는 앱 프로필의 보안 요구 사항을 정의합니다. 앱을 배포하기 전에 보안 요구 사항을 특정 MDM 또는 MAM 정책에 매핑할 수 있습니다. 이러한 계획은 앱 배포를 간소화하고 가속화합니다. 예를 들어:

    - 특정 앱을 다르게 배포할 수 있습니다.
    - XenMobile 환경에 아키텍처 변경을 원할 수 있습니다. 변경 사항은 앱이 요구하는 보안 규정 준수 유형에 따라 달라집니다. 예를 들어, 중요한 비즈니스 인텔리전스 앱 사용을 허용하기 위해 장치를 암호화하도록 할 수 있습니다. 또는 특정 앱에 종단 간 SSL 암호화 또는 지오펜싱이 필요할 수 있습니다.

- **앱 배포:** XenMobile을 사용하면 앱을 MDM 앱 또는 MAM 앱으로 배포할 수 있습니다. MDM 앱은 XenMobile Store에 나타납니다. 이 스토어를 통해 공개 또는 네이티브 앱을 사용자에게 편리하게 배포할 수 있습니다. 관리하는 유일한 MDM 앱 제어는 장치 수준 제한을 적용하는 것입니다. 그러나 MAM을 사용하여 앱을 배포하면 앱 배포 및 앱 자체에 대한 완전한 제어가 가능합니다. 일반적으로 MAM을 통해 앱을 배포하는 것이 더 적합합니다.
- **애플리케이션 유지 관리:**
    - 초기 감사 수행: 프로덕션 환경의 앱 버전과 마지막 업그레이드 주기를 추적합니다. 업그레이드가 필요했던 특정 기능 또는 버그 수정을 기록합니다.
    - 기준선 설정: 각 앱의 최신 안정 릴리스 목록을 유지 관리합니다. 이 앱 버전은 업그레이드 후 예기치 않은 문제가 발생할 경우를 대비한 대체 버전입니다. 롤백 계획도 개발합니다. 프로덕션 배포 전에 테스트 환경에서 앱 업그레이드를 테스트합니다. 가능하다면, 먼저 프로덕션 사용자 중 일부에게 업그레이드를 배포한 다음 전체 사용자 기반에 배포합니다.
    - Citrix® 소프트웨어 업데이트 알림 및 타사 소프트웨어 공급업체 알림 구독: 앱의 최신 릴리스를 최신 상태로 유지하는 것이 중요합니다. 조기 액세스 릴리스(EAR) 빌드를 테스트용으로 사용할 수 있습니다.
    - 사용자에게 알리는 전략 고안: 앱 업그레이드를 사용할 수 있을 때 사용자에게 알리는 전략을 정의합니다. 배포 전에 교육을 통해 사용자를 준비시킵니다. 앱을 업데이트하기 전에 여러 알림을 보낼 수 있습니다. 앱에 따라 가장 좋은 알림 방법은 이메일 알림 또는 웹사이트일 수 있습니다.

앱 수명 주기 관리는 초기 배포부터 서비스 종료까지 앱의 전체 수명 주기를 나타냅니다. 앱의 수명 주기는 다음과 같은 단계로 구성됩니다.

1. 사양 요구 사항: 비즈니스 사례 및 사용자 요구 사항부터 시작합니다.
2. 개발: 앱이 비즈니스 요구 사항을 충족하는지 확인합니다.
3. 테스트: 테스트 사용자, 문제 및 버그를 식별합니다.
4. 배포: 프로덕션 사용자에게 앱을 배포합니다.
5. 유지 관리: 앱 버전을 업데이트합니다. 프로덕션 환경에서 앱을 업데이트하기 전에 테스트 환경에 앱을 배포합니다.

Secure Mail을 사용한 애플리케이션 수명 주기 예시

1. 사양 요구 사항: 보안 요구 사항으로, 컨테이너화되고 MDX 보안 정책을 지원하는 메일 앱이 필요합니다.

2. 개발: 앱이 비즈니스 요구 사항을 충족하는지 확인합니다. 앱에 MDX 정책 제어를 적용할 수 있어야 합니다.
3. 테스트: Secure Mail을 테스트 사용자 그룹에 할당하고 XenMobile Server에서 해당 MDX 파일을 배포합니다. 테스트 사용자는 이메일을 성공적으로 보내고 받을 수 있으며, 캘린더 및 연락처에 액세스할 수 있는지 확인합니다. 또한 테스트 사용자는 문제점을 보고하고 버그를 식별합니다. 테스트 사용자의 피드백을 기반으로 프로덕션 사용을 위한 Secure Mail 구성을 최적화합니다.
4. 배포: 테스트 단계가 완료되면 Secure Mail을 프로덕션 사용자에게 할당하고 XenMobile에서 해당 MDX 파일을 배포합니다.
5. 유지 관리: Secure Mail의 새 업데이트를 사용할 수 있습니다. Citrix 다운로드에서 새 MDX 파일을 다운로드하고 XenMobile Server의 기존 MDX 파일을 교체합니다. 사용자에게 업데이트를 수행하도록 지시합니다. 참고: Citrix는 이 프로세스를 테스트 환경에서 완료하고 테스트할 것을 권장합니다. 그런 다음, 앱을 XenMobile 프로덕션 환경에 업로드하고 사용자에게 배포합니다.

자세한 내용은 iOS 모바일 앱 래핑 및 Android 모바일 앱 래핑을 참조하십시오.

대시보드 기반 작업

XenMobile® 콘솔 대시보드에 액세스하여 정보를 한눈에 볼 수 있습니다. 이 정보를 통해 위젯을 사용하여 문제와 성공을 빠르게 확인할 수 있습니다.

대시보드는 일반적으로 XenMobile 콘솔에 처음 로그인할 때 나타나는 화면입니다. 콘솔의 다른 위치에서 대시보드에 액세스하려면 **분석**을 클릭합니다. 대시보드에서 **사용자 지정**을 클릭하여 페이지 레이아웃을 편집하고 표시되는 위젯을 편집합니다.

- **내 대시보드:** 최대 4개의 대시보드를 저장할 수 있습니다. 이러한 대시보드를 개별적으로 편집하고 저장된 대시보드를 선택하여 각 대시보드를 볼 수 있습니다.
- **레이아웃 스타일:** 이 행에서 대시보드에 표시되는 위젯 수와 위젯이 배치되는 방식을 선택할 수 있습니다.
- **위젯 선택:** 대시보드에 표시할 정보를 선택할 수 있습니다.
    - **알림:** 위젯 위에 알림 표시줄을 추가하려면 왼쪽의 숫자 위에 있는 확인란을 선택합니다. 이 표시줄은 규정 준수 장치, 비활성 장치, 지난 24시간 동안 초기화되거나 등록된 장치 수를 보여줍니다.
    - **플랫폼별 장치:** 플랫폼별 관리 및 비관리 장치 수를 표시합니다.
    - **통신사별 장치:** 통신사별 관리 및 비관리 장치 수를 표시합니다. 각 막대를 클릭하여 플랫폼별 분석을 볼 수 있습니다.
    - **플랫폼별 관리 장치:** 플랫폼별 관리 장치 수를 표시합니다.
    - **플랫폼별 비관리 장치:** 플랫폼별 비관리 장치 수를 표시합니다. 이 차트에 나타나는 장치에는 에이전트가 설치되어 있을 수 있지만, 권한이 취소되었거나 초기화되었을 수 있습니다.

- **ActiveSync Gateway 상태별 장치:** ActiveSync Gateway 상태별로 그룹화된 장치 수를 표시합니다. 이 정보는 차단됨, 허용됨 또는 알 수 없음 상태를 보여줍니다. 각 막대를 클릭하여 플랫폼별로 데이터를 분석할 수 있습니다.
- **소유권별 장치:** 소유권 상태별로 그룹화된 장치 수를 표시합니다. 이 정보는 회사 소유, 직원 소유 또는 알 수 없음 소유권 상태를 보여줍니다.
- **실패한 배달 그룹 배포:** 패키지당 실패한 배포의 총 수를 표시합니다. 배포에 실패한 패키지만 표시됩니다.
- **차단 이유별 장치:** ActiveSync에 의해 차단된 장치 수를 표시합니다.
- **설치된 앱:** 이 위젯을 사용하여 앱 이름을 입력하면 해당 앱에 대한 정보가 그래프로 표시됩니다.
- **볼륨 구매 앱 라이선스 사용량:** Apple 볼륨 구매 앱의 라이선스 사용 통계를 표시합니다.

사용 사례

환경을 모니터링하기 위해 대시보드 위젯을 사용할 수 있는 다양한 방법의 몇 가지 예는 다음과 같습니다.

- 모바일 생산성 앱을 배포했으며, 모바일 생산성 앱이 장치에 설치되지 않는 문제에 대한 지원 티켓을 받고 있습니다. **규정 미준수 장치** 및 **설치된 앱** 위젯을 사용하여 모바일 생산성 앱이 설치되지 않은 장치를 확인할 수 있습니다.
- 비활성 장치를 모니터링하여 환경에서 장치를 제거하고 라이선스를 회수하려고 합니다. **비활성 장치** 위젯을 사용하여 이 통계를 추적합니다.
- 데이터가 제대로 동기화되지 않는 문제에 대한 지원 티켓을 받고 있습니다. **ActiveSync 게이트웨이 상태별 장치** 및 **차단 사유별 장치** 위젯을 사용하여 문제가 ActiveSync와 관련이 있는지 확인할 수 있습니다.

보고

환경이 설정되고 사용자가 등록되면 보고서를 실행하여 배포에 대해 알아볼 수 있습니다. XenMobile에는 환경에서 실행되는 장치에 대한 더 나은 그림을 얻는 데 도움이 되는 다양한 보고서가 내장되어 있습니다. 자세한 내용은 보고서를 참조하십시오.

> **중요:**
>
> 사용자 지정 보고서를 생성하기 위해 SQL Server를 사용할 수 있지만, Citrix®는 이 방법을 권장하지 않습니다. 이러한 방식으로 SQL Server 데이터베이스를 사용하면 XenMobile 배포에 예상치 못한 결과를 초래할 수 있습니다. 이 보고 방법을 사용하기로 결정한 경우, SQL 쿼리가 읽기 전용 계정을 사용하여 실행되는지 확인하십시오.

역할 기반 액세스 제어 및 XenMobile® 지원

XenMobile은 역할 기반 액세스 제어(RBAC)를 사용하여 XenMobile 콘솔, 원격 지원 및 공용 API와 같은 XenMobile 시스템 기능에 대한 사용자 및 그룹 액세스를 제한합니다. 이 문서에서는 XenMobile에 내장된 역할에 대해 설명하고 RBAC를 사용하는 XenMobile 지원 모델을 결정하기 위한 고려 사항을 포함합니다.

> **참고:**
>
> January 1, 2019부터 신규 고객에게는 원격 지원을 더 이상 제공하지 않습니다. 기존 고객은 계속해서 제품을 사용할 수 있지만, Citrix®는 개선 사항이나 수정 사항을 제공하지 않습니다.

내장 역할

다음 내장 역할에 부여된 액세스를 변경할 수 있으며 역할을 추가할 수도 있습니다. 각 역할과 관련된 전체 액세스 및 기능 권한 세트와 기본 설정에 대해서는 XenMobile 설명서에서 역할 기반 액세스 제어 기본값을 다운로드하십시오. 각 기능에 대한 정의는 XenMobile 설명서에서 RBAC로 역할 구성을 참조하십시오.

관리자 역할

기본 액세스 권한:

- 원격 지원을 제외한 전체 시스템 액세스.
- 기본적으로 관리자는 연결 확인 및 지원 번들 생성과 같은 일부 지원 작업을 수행할 수 있습니다.

고려 사항:

- 일부 또는 모든 관리자가 원격 지원에 액세스해야 합니까? 그렇다면 관리자 역할을 편집하거나 관리자 역할을 추가할 수 있습니다.
- 일부 관리자 또는 관리자 그룹에 대한 액세스를 추가로 제한하려면 관리자 템플릿을 기반으로 역할을 추가하고 권한을 편집하십시오.

지원

기본 액세스 권한:

- 원격 지원 액세스.

고려 사항:

- 온프레미스 XenMobile Server 배포의 경우: 원격 지원을 통해 헬프데스크 담당자가 관리되는 Android 모바일 장치를 원격으로 제어할 수 있습니다. 화면 전송은 Samsung Knox 장치에서만 지원됩니다.
- 클러스터링된 온프레미스 XenMobile Server 배포에서는 원격 지원을 사용할 수 없습니다.

사용자

부여된 기본 액세스:

- XenMobile 콘솔에 대한 제한된 액세스: 장치 기능(예: 장치 초기화, 잠금/잠금 해제, 컨테이너 잠금/잠금 해제, 위치 확인 및 지리적 제한 설정, 장치 벨소리 울리기, 컨테이너 암호 재설정), 등록 초대 추가, 제거 및 전송.

고려 사항:

- 사용자 역할을 통해 사용자가 스스로 문제를 해결할 수 있도록 할 수 있습니다.
- 공유 장치를 지원하려면 공유 장치 등록을 위한 사용자 역할을 생성하십시오.

XenMobile 지원 모델에 대한 고려 사항

채택할 수 있는 지원 모델은 매우 다양하며, 직원이 레벨 3 및 4 지원을 처리하는 동안 제3자가 레벨 1 및 2 지원을 처리하는 경우도 있습니다. 지원 부담을 어떻게 분배하든 관계없이 XenMobile 배포 및 사용자 기반에 특정한 이 섹션의 고려 사항을 염두에 두십시오.

사용자가 회사 소유 장치를 사용합니까, 아니면 BYO 장치를 사용합니까? 지원에 영향을 미치는 주요 질문은 XenMobile 환경에서 사용자 장치의 소유자가 누구인지입니다. 사용자가 회사 소유 장치를 사용하는 경우, 장치를 잠그는 방법으로 낮은 수준의 지원을 제공할 수 있습니다. 이 경우, 장치 문제 및 장치 사용 방법에 대해 사용자를 지원하는 헬프데스크를 제공할 수 있습니다. 지원해야 하는 장치 유형에 따라 헬프데스크에 RBAC 장치 프로비저닝 및 지원 역할을 어떻게 사용할지 고려하십시오.

사용자가 BYO 장치를 사용하는 경우, 조직은 사용자가 장치 지원을 위한 자체 소스를 찾을 것으로 예상할 수 있습니다. 이 경우, 조직이 제공하는 지원은 XenMobile 관련 문제에 중점을 둔 관리 역할에 가깝습니다.

데스크톱에 대한 지원 모델은 무엇입니까? 데스크톱에 대한 지원 모델이 다른 회사 소유 장치에 적합한지 고려하십시오. 동일한 지원 조직을 사용할 수 있습니까? 어떤 추가 교육이 필요합니까?

사용자에게 XenMobile 셀프 도움말 포털에 대한 액세스 권한을 부여하시겠습니까? 등록 보안 모드에 대해 셀프 도움말 포털을 활성화하려면 **설정 > 등록**을 사용하십시오. 셀프 도움말 포털에서 사용자는 장치를 등록하거나 등록 초대를 자신에게 보낼 수 있는 등록 링크를 생성할 수 있습니다. 등록 보안 모드 구성을 참조하십시오.

시스템 모니터링

앱 액세스 및 연결을 위한 최적의 가동 시간을 보장하려면 XenMobile® 환경에서 다음 핵심 구성 요소를 모니터링해야 합니다.

젠모바일 서버

XenMobile Server는 로컬 스토리지에 로그를 생성하고 저장하며, 이 로그를 시스템 로그(syslogs) 서버로 내보낼 수도 있습니다. 로그 설정을 구성하여 크기 제약 조건, 로그 수준을 지정하거나 특정 이벤트를 필터링하기 위한 사용자 지정 로거를 만들 수 있습니다. XenMobile 콘솔에서 언제든지 XenMobile Server 로그를 확인할 수 있습니다. 또한 syslog 서버를 통해 로그의 정보를 프로덕션 Splunk 로깅 서버로 내보낼 수도 있습니다.

다음 목록은 XenMobile에서 사용할 수 있는 다양한 유형의 로그 파일을 설명합니다.

디버그 로그 파일: 오류 메시지 및 서버 관련 작업을 포함하여 XenMobile의 핵심 웹 서비스에 대한 디버그 수준 정보를 포함합니다.

메시지 형식:

`<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>`

- 여기서 `<id>`은 sessionID와 같은 고유 식별자입니다.
- 여기서 `<log message>`은 애플리케이션에서 제공하는 메시지입니다.

관리자 감사 로그 파일: XenMobile 콘솔에서의 활동에 대한 감사 정보를 포함합니다.

> **참고:**
>
> 관리자 감사 로그와 사용자 감사 로그 모두 동일한 형식이 사용됩니다.
>
> 메시지 형식:

필수 날짜 및 타임스탬프 값을 제외하고 다른 모든 속성은 선택 사항입니다. 선택 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.

이벤트에 대한 관리자 감사 로그 메시지	상태
로그인	성공/실패

이벤트에 대한 관리자 감사 로그 메시지	상태
로그아웃	성공/실패
관리자 가져오기	성공/실패
관리자 업데이트	성공/실패
애플리케이션 가져오기	성공/실패
애플리케이션 추가	성공/실패
애플리케이션 업데이트	성공/실패
애플리케이션 삭제	성공/실패
애플리케이션 바인딩	성공/실패
애플리케이션 바인딩 해제	성공/실패
애플리케이션 비활성화	성공/실패
애플리케이션 활성화	성공/실패
범주 가져오기	성공/실패
범주 추가	성공/실패
범주 업데이트	성공/실패
범주 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

이벤트에 대한 관리자 감사 로그 메시지	상태
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
구성 설정 업데이트	성공/실패
워크플로 이메일 업데이트	성공/실패
워크플로 추가	성공/실패
워크플로 삭제	성공/실패

이벤트에 대한 관리자 감사 로그 메시지	상태
액티브 디렉터리 추가	성공/실패
Active Directory 업데이트	성공/실패
마스터유저리스트 추가	성공/실패
masteruserlist 업데이트	성공/실패
DNS 업데이트	성공/실패
네트워크 업데이트	성공/실패
로그 서버 업데이트	성공/실패
로그 서버에서 로그 전송	성공/실패
syslog 업데이트	성공/실패
수신기 업데이트 업데이트	성공/실패
시간 서버 업데이트	성공/실패
트러스트 업데이트	성공/실패
서비스 레코드 추가	성공/실패
서비스 레코드 업데이트	성공/실패
수신기 이메일 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

이벤트에 대한 관리자 감사 로그 메시지	상태
HDX 업데이트	성공/실패
HDX 삭제	성공/실패
브랜딩 추가	성공/실패
브랜딩 삭제	성공/실패
SSL 오프로드 업데이트	성공/실패
계정 속성 추가	성공/실패
계정 속성 삭제	성공/실패
계정 속성 업데이트	성공/실패
비콘 추가	성공/실패

사용자 감사 로그 파일: 등록된 장치의 사용자 활동과 관련된 정보를 포함합니다.

> **참고:**
>
> 사용자 감사 로그와 관리자 감사 로그 모두 동일한 형식이 사용됩니다.
>
> 메시지 형식:

필수 날짜 및 타임스탬프 값을 제외하고, 다른 모든 속성은 선택 사항입니다. 선택 필드는 메시지에서 " "로 표시됩니다. 예를 들어,

`<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.

이벤트에 대한 사용자 감사 로그 메시지	상태
로그인	성공/실패

이벤트에 대한 사용자 감사 로그 메시지	상태
세션 시간 초과	성공/실패
구독	성공/실패
구독 취소	성공/실패
사전 실행	성공/실패
AGEE SSO	성공/실패
Citrix Files용 SAML 토큰	성공/실패
장치 등록	성공/실패
장치 확인	잠금/초기화
장치 업데이트	성공/실패
토큰 새로 고침	성공/실패
비밀 저장됨	성공/실패
비밀 검색됨	성공/실패
사용자 암호 변경 시작	성공/실패
모바일 클라이언트 다운로드	성공/실패
로그아웃	성공/실패
검색 서비스	성공/실패
엔드포인트 서비스	성공/실패

MDM 기능	상태
REGHIVE	성공/실패
Cab 인벤토리	성공/실패
Cab	성공/실패

MDM 기능	상태
Cab 자동 설치	성공/실패
Cab 셸 설치	성공/실패
Cab 폴더 생성	성공/실패
Cab 파일 가져오기	성공/실패
파일 폴더 생성	성공/실패
파일 가져오기	성공/실패
파일 전송됨	성공/실패
스크립트 폴더 생성	성공/실패
스크립트 가져오기	성공/실패
스크립트 전송됨	성공/실패
스크립트 셸 실행	성공/실패
스크립트 자동 실행	성공/실패
APK 인벤토리	성공/실패
APK	성공/실패
APK 셸 설치	성공/실패
APK 자동 설치	성공/실패
APK 폴더 생성	성공/실패
APK 파일 가져오기	성공/실패
APK 앱	성공/실패
EXT 앱	성공/실패
목록 가져오기	성공/실패

MDM 기능	상태
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
애플리케이션 제거	성공/실패
관리되지 않는 애플리케이션 제거	성공/실패
관리되지 않는 프로필 제거	성공/실패
IPA 앱	성공/실패
EXT 앱	성공/실패
교환 코드 적용	성공/실패
설정 적용	성공/실패
장치 추적 활성화	성공/실패
앱 관리 정책	성공/실패
SD 카드 초기화	성공/실패
암호화된 이메일 첨부 파일	성공/실패
브랜딩	성공/실패
보안 브라우저	성공/실패
컨테이너 브라우저	성공/실패

MDM 기능	상태
컨테이너 잠금 해제	성공/실패
컨테이너 암호 재설정	성공/실패
AG 클라이언트 인증 자격 증명	성공/실패

Citrix ADC는 또한 XenMobile 웹 서비스 상태를 모니터링합니다. 이 서비스는 각 XenMobile Server 클러스터 노드에 대한 HTTP 요청을 시뮬레이션하도록 지능형 모니터링 프로브로 구성됩니다. 프로브는 서비스가 온라인 상태인지 확인한 다음 수신된 응답에 따라 응답합니다. 노드가 예상대로 응답하지 않는 경우 Citrix ADC는 서버를 다운으로 표시합니다. 또한 Citrix ADC는 노드를 로드 밸런싱 풀에서 제외하고 Citrix ADC 모니터링 솔루션을 통해 경고를 생성하는 데 사용할 이벤트를 기록합니다.

표준 하이퍼바이저 모니터링 도구를 사용하여 XenMobile 가상 머신을 모니터링하고 CPU, 메모리 및 스토리지 사용률 메트릭과 관련된 경고를 제공할 수도 있습니다.

SQL Server 및 데이터베이스

SQL Server 및 데이터베이스 성능은 XenMobile 서비스에 직접적인 영향을 미칩니다. XenMobile 인스턴스는 항상 데이터베이스에 액세스해야 하며 SQL 인프라에 장애가 발생하면 오프라인 상태가 됩니다(예: 응답 중지). XenMobile 콘솔은 SQL Server의 디스크 공간 문제 발생 후에도 한동안 계속 작동할 수 있습니다. 최대 데이터베이스 가동 시간과 XenMobile 워크로드에 대한 적절한 성능을 보장하려면 SQL Server의 상태를 사전에 모니터링해야 합니다. SQL Server 모니터링에 대한 자세한 내용은 성능 모니터링 및 튜닝 개요를 참조하십시오. 또한 XenMobile 환경이 계속 성장함에 따라 서비스 수준 계약을 보장하기 위해 CPU, 메모리 및 스토리지에 대한 리소스 할당을 조정해야 합니다.

시트릭스 ADC

Citrix ADC는 메트릭을 내부 스토리지에 기록하거나 외부 로깅 서버로 로그를 보낼 수 있는 기능을 제공합니다. syslog 서버를 구성하여 Citrix ADC 로그를 프로덕션 Splunk 로깅 서버로 내보낼 수 있습니다. Citrix ADC에서 사용할 수 있는 로깅 수준은 다음과 같습니다.

- 긴급
- 경고
- 심각
- 오류
- 경고
- 정보

로그 파일은 Citrix ADC 스토리지의 /var/log/ns.log 디렉터리에도 저장되며 newnslog로 명명됩니다. Citrix ADC는 GZIP 알고리즘을 사용하여 파일을 롤오버하고 압축합니다. 로그 파일 이름은 newnslog.xx.gz이며, 여기서 xx는 실행 번호를 나타냅니다.

Citrix ADC는 모니터링 옵션으로 SNMP 트랩 및 경고도 지원합니다. SNMP 트랩 목록은 SNMP 모니터링을 참조하십시오.

재해 복구

활성-수동 페일오버 전략을 사용하여 재해 복구를 위한 여러 사이트를 포함하는 XenMobile® 배포를 설계하고 구성할 수 있습니다.

이 문서에서 설명하는 권장 재해 복구 전략은 다음으로 구성됩니다.

- 전 세계 모든 엔터프라이즈 사용자에게 서비스를 제공하는 단일 지리적 위치의 데이터 센터에 있는 단일 XenMobile 활성 사이트로, 기본 사이트라고 합니다.
- 재해 복구 사이트라고 하는 두 번째 지리적 위치의 데이터 센터에 있는 두 번째 XenMobile 사이트. 이 재해 복구 사이트는 기본 사이트에서 사이트 전체 데이터 센터 장애가 발생하는 경우 활성-수동 사이트 페일오버를 제공합니다. 기본 사이트에는 페일오버를 용이하게 하고 기본 사이트에 대한 연결 실패 시 사용자에게 XenMobile에 대한 액세스를 제공하기 위한 XenMobile, SQL 데이터베이스 및 Citrix ADC 인프라가 포함됩니다.

재해 복구 사이트의 XenMobile 서버는 정상 작동 중에는 오프라인 상태를 유지하며, 기본 사이트에서 재해 복구 사이트로의 완전한 사이트 페일오버가 필요한 재해 복구 시나리오에서만 온라인 상태가 됩니다. 재해 복구 사이트의 XenMobile 서버를 시작하기 전에 재해 복구 사이트의 SQL 서버는 활성 상태여야 하며 연결을 처리할 준비가 되어 있어야 합니다.

이 재해 복구 전략은 중단 발생 시 MDM 및 MAM 연결을 재해 복구 사이트로 라우팅하기 위한 DNS 변경을 통해 Citrix ADC 액세스 계층의 수동 페일오버에 의존합니다.

> **참고:**
>
> 이 아키텍처를 사용하려면 데이터베이스의 비동기 백업을 위한 프로세스와 SQL 인프라의 고가용성을 보장하는 방법이 마련되어 있어야 합니다.

재해 복구 페일오버 프로세스

1. 재해 복구 페일오버 프로세스를 테스트하는 경우, 사이트 장애를 시뮬레이션하기 위해 기본 사이트의 XenMobile 서버를 종료합니다.

2. XenMobile 서버의 공용 DNS 레코드를 재해 복구 사이트의 외부 IP 주소를 가리키도록 변경합니다.
3. SQL Server의 내부 DNS 레코드를 재해 복구 사이트의 SQL Server IP 주소를 가리키도록 변경합니다.
4. 재해 복구 사이트에서 XenMobile SQL 데이터베이스를 온라인 상태로 전환합니다. SQL Server 및 데이터베이스가 활성 상태이며 해당 사이트의 XenMobile 서버로부터의 연결을 처리할 준비가 되어 있는지 확인합니다.
5. 재해 복구 사이트의 XenMobile 서버를 엽니다.

XenMobile Server 업데이트 프로세스

기본 서버와 재해 복구 서버의 코드를 일관되게 유지하려면 패치 및 릴리스로 XenMobile을 업데이트할 때마다 다음 단계를 따르십시오.

1. 기본 사이트의 XenMobile Server가 패치되거나 업그레이드되었는지 확인합니다.
2. SQL Server의 DNS 레코드가 기본 사이트의 활성 SQL Server 데이터베이스로 확인되는지 확인합니다.
3. 재해 복구 사이트의 XenMobile Server를 온라인 상태로 전환합니다. 서버는 업그레이드 프로세스 중에만 WAN을 통해 기본 사이트의 데이터베이스에 연결됩니다.
4. 모든 재해 복구 사이트의 XenMobile Server에 필요한 패치 및 업데이트를 적용합니다.
5. XenMobile Server를 다시 시작하고 패치 또는 업그레이드가 성공했는지 확인합니다.

재해 복구 참조 아키텍처 다이어그램

다음 다이어그램은 XenMobile의 재해 복구 배포를 위한 상위 수준 아키텍처를 보여줍니다.

재해 복구 참조 아키텍처 다이어그램(/en-us/xenmobile/server/media/disaster-recovery-diagram.png)

재해 복구를 위한 GSLB

이 아키텍처의 핵심 요소는 트래픽을 올바른 데이터 센터로 전달하기 위해 GSLB(Global Server Load Balancing)를 사용하는 것입니다.

기본적으로 XenMobile용 Citrix ADC 마법사는 재해 복구를 위한 GSLB 사용을 활성화하지 않는 방식으로 Citrix Gateway를 구성합니다. 따라서 추가 단계를 수행해야 합니다.

GSLB 작동 방식

GSLB는 본질적으로 DNS의 한 형태입니다. 참여하는 Citrix ADC 어플라이언스는 권한 있는 DNS 서버 역할을 하며 DNS 레코드를 올바른 IP 주소(일반적으로 트래픽을 수신해야 하는 VIP)로 확인합니다. Citrix ADC 어플라이언스는 해당 시스템으로 트래픽을 전달하는 DNS 쿼리에 응답하기 전에 시스템 상태를 확인합니다.

레코드가 확인되면 트래픽을 확인하는 GSLB의 역할은 완료됩니다. 클라이언트는 대상 가상 IP(VIP) 주소와 직접 통신합니다. DNS 클라이언트 동작은 레코드가 만료되는 방식과 시기를 제어하는 데 중요한 역할을 합니다. 이는 Citrix ADC 시스템의 경계를 크게 벗어납니다. 따라서 GSLB는 DNS 이름 확인과 동일한 제한을 받습니다. 클라이언트는 응답을 캐시하므로 이러한 방식의 로드 밸런싱은 기존 로드 밸런싱만큼 실시간이 아닙니다.

사이트, 서비스 및 모니터를 포함한 Citrix ADC의 GSLB 구성은 올바른 DNS 이름 확인을 제공하기 위해 존재합니다.

게시 서버에 대한 실제 구성(이 시나리오에서는 XenMobile 마법사용 Citrix ADC가 생성하는 구성)은 GSLB의 영향을 받지 않습니다. GSLB는 Citrix ADC의 별도 서비스입니다.

XenMobile과 함께 GSLB를 사용할 때 도메인 위임 관련 문제

XenMobile 마법사용 Citrix ADC는 XenMobile용 Citrix Gateway를 구성합니다. 이 마법사는 세 개의 로드 밸런싱 가상 서버와 하나의 Citrix Gateway 가상 서버를 생성합니다.

로드 밸런싱 가상 서버 중 두 개는 포트 443 및 8443에서 MDM 트래픽을 처리합니다. Citrix Gateway는 MAM 트래픽을 수신하여 세 번째 서버인 MAM 로드 밸런싱 가상 서버(포트 8443)로 전달합니다. MAM 로드 밸런싱 가상 서버로의 모든 트래픽은 Citrix Gateway를 통해 전달됩니다.

MAM 로드 밸런싱 가상 서버는 XenMobile 서버와 동일한 SSL 인증서를 필요로 하며, 장치 등록에 사용되는 것과 동일한 FQDN을 사용합니다. MAM 로드 밸런싱 서버는 MDM 로드 밸런싱 서버 중 하나와 동일한 포트(8443)를 사용합니다. 트래픽이 확인될 수 있도록 XenMobile 마법사용 Citrix ADC는 Citrix Gateway에 로컬 DNS 레코드를 생성합니다. DNS 레코드는 장치 등록에 사용되는 FQDN과 일치합니다.

이 구성은 XenMobile 서버 URL이 GSLB 도메인 URL이 아닐 때 효과적입니다. 재해 복구에 필요한 대로 GSLB 도메인 URL이 XenMobile 서버 URL로 사용되는 경우, 로컬 DNS 레코드는 Citrix Gateway가 MDM 로드 밸런싱 서버로 트래픽을 확인하는 것을 방지합니다.

GSLB 재해 복구를 위한 CNAME 메서드 사용

XenMobile 마법사용 Citrix ADC가 생성한 기본 구성으로 인해 발생하는 문제를 해결하려면, 상위 도메인(`company.com`)에 XenMobile 서버 FQDN에 대한 CNAME 레코드를 생성하고 Citrix ADC가 권한을 갖는 위임된 하위 영역(`gslb.company.com`)의 레코드를 가리킬 수 있습니다. 이렇게 하면 트래픽 확인에 필요한 MAM 로드 밸런싱 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 트래픽용이고 다른 하나는 MAM(Citrix Gateway) 트래픽용입니다.

   예:

`CNAME = xms.company.com IN CNAME xms.gslb.comany.com`

2. 각 사이트의 Citrix Gateway 인스턴스에서 CNAME 레코드가 가리키는 FQDN을 가진 GSLB 가상 서버를 생성합니다.

   예:

   `bind gslb vserver xms-gslb -domainName xms.gslb.company.com`

   Citrix ADC for XenMobile 마법사를 사용하여 Citrix Gateway를 배포할 때 MAM 로드 밸런싱 서버를 구성할 때 XenMobile Server URL을 사용합니다. 이렇게 하면 XenMobile Server URL에 대한 정적 DNS A 레코드가 생성됩니다.

3. XenMobile Server URL (`xms.company.com`)을 사용하여 Secure Hub에 등록하는 클라이언트로 테스트합니다.

   이 예에서는 다음 FQDN을 사용합니다.

   - `xms.company.com`은 MDM 트래픽에서 사용되고 장치 등록에 사용되는 URL이며, 이 예에서는 Citrix ADC for XenMobile 마법사를 사용하여 구성됩니다.
   - `xms.gslb.company.com`은 XenMobile Server의 GSLB 도메인 FQDN입니다.

Citrix 지원 프로세스

Citrix 제품 관련 문제에 대한 도움을 받으려면 Citrix 기술 지원 서비스를 이용할 수 있습니다. 이 그룹은 해결 방법과 해결책을 제공하며, 개발 팀과 긴밀히 협력하여 솔루션을 제공합니다.

Citrix ConsultingSM Services 또는 Citrix Education Services는 제품 교육, 제품 사용, 구성, 설치 또는 환경 설계 및 아키텍처에 대한 조언과 관련된 도움을 제공합니다.

Citrix Consulting은 개념 증명, 경제적 영향 평가, 인프라 상태 점검, 설계 요구 사항 분석, 아키텍처 설계 검증, 통합 및 운영 프로세스 개발을 포함한 Citrix 제품 관련 프로젝트를 지원합니다.

Citrix EducationSM은 Citrix 가상화, 클라우드 및 네트워킹 기술에 대한 동급 최고의 IT 교육 및 인증을 제공합니다.

Citrix는 지원 사례를 생성하기 전에 Citrix 자가 진단 리소스 및 권장 사항을 최대한 활용할 것을 권장합니다. 예를 들어, Citrix 기술 전문가가 작성한 문서 및 게시판에 액세스하거나, Citrix 솔루션 및 기술에 대한 제품 설명서를 보거나, Citrix 경영진, 제품 팀 및 기술 전문가의 솔직한 이야기를 읽을 수 있는 여러 곳이 있습니다. 각각 Knowledge Center, 제품 설명서 및 블로그 페이지를 참조하십시오.

더 많은 상호 작용 지원을 위해 토론 포럼에 참여하여 다른 고객으로부터 질문하고 실제 답변을 얻거나, 사용자 그룹 및 관심 그룹 내에서 아이디어, 의견, 기술 정보 및 모범 사례를 공유하거나, Citrix 지원 소셜 네트워킹

사이트를 모니터링하는 Citrix 지원 엔지니어와 상호 작용할 수 있습니다. 각각 지원 포럼 및 Citrix 커뮤니티 페이지를 참조하십시오.

기술을 향상시키기 위한 교육 및 인증 과정에도 액세스할 수 있습니다. Citrix Education을 참조하십시오.

Citrix Insight Services는 Citrix 환경을 위한 간단한 온라인 문제 해결 플랫폼 및 상태 검사기를 제공합니다. XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor 및 Citrix Gateway에서 사용할 수 있습니다. 분석 도구를 참조하십시오.

기술 지원을 요청하려면 전화 또는 웹을 통해 지원 사례를 생성할 수 있습니다. 웹은 심각도가 낮거나 중간인 문제에 사용하고, 전화 옵션은 심각도가 높은 문제에 사용합니다. XenMobile 문제에 대한 지원을 문의하려면 Citrix Support Services를 참조하십시오.

Citrix 솔루션 제공에 대한 광범위한 경험을 가진 고도로 훈련된 단일 연락 창구를 찾고 있다면 Citrix Services에서 기술 관계 관리자를 제공합니다. Citrix 서비스 제공 및 이점에 대한 자세한 내용은 Citrix Worldwide Services를 참조하십시오.

XenMobile®에서 그룹 등록 초대 보내기

XenMobile Server에서 그룹 및 중첩 그룹에 등록 초대를 보낼 수 있습니다. 등록 초대는 Windows 장치에서는 사용할 수 없습니다.

그룹 초대를 설정할 때 하나 이상의 장치 플랫폼을 지정할 수 있습니다. 예를 들어 회사 소유 장치와 직원 소유 장치를 구분할 수 있도록 장치에 태그를 지정할 수도 있습니다. 그런 다음 사용자 장치에 대한 인증 유형을 설정합니다.

> **참고:**
>
> 사용자 지정 알림 템플릿을 사용할 계획이라면 등록 보안 모드를 구성하기 전에 템플릿을 설정해야 합니다. 알림 템플릿에 대한 자세한 내용은 알림 템플릿 생성 및 업데이트를 참조하십시오.
>
> 사용자 계정, 역할, 등록 보안 모드 및 초대에 대한 기본 구성에 대한 자세한 내용은 사용자 계정, 역할 및 등록을 참조하십시오.

일반적인 단계

1. XenMobile 콘솔에서 **관리 > 등록 초대**로 이동합니다.
2. 화면 왼쪽 상단에 있는 **추가**를 클릭한 다음 **초대 추가**를 클릭합니다.
3. **수신자** 메뉴에서 **그룹**을 클릭합니다.

이 단계에서는 하나 이상의 플랫폼을 선택할 수 있습니다. 회사에 다양한 운영 체제 플랫폼이 혼합되어 있는 경우 모든 플랫폼을 선택합니다. 특정 플랫폼을 사용하는 사용자가 없다고 확신하는 경우에만 플랫폼 선택을 해제합니다.

4. 초대 과정에서 장치에 태그를 지정할 수 있습니다. **회사** 또는 **직원**을 선택합니다.

   태그 지정을 통해 회사 소유 장치와 직원 소유 장치를 쉽게 구분할 수 있습니다.

5. **도메인** 목록에서 그룹이 있는 도메인을 선택합니다.
6. **그룹** 목록에서 초대를 보낼 Active Directory 그룹을 선택합니다.
7. **등록 모드**를 통해 사용자가 선호하는 인증 보안 유형을 설정할 수 있습니다.

   - 사용자 이름 + 암호
   - 높은 보안
   - 초대 URL
   - 초대 URL + PIN
   - 초대 URL + 암호
   - 2단계 인증
   - 사용자 이름 + PIN

   > **참고:**
   >
   > 등록 초대를 보내려면 **초대 URL**, **초대 URL + PIN** 또는 **초대 URL + 암호** 등록 보안 모드만 사용할 수 있습니다. **사용자 이름 + 암호**, **2단계 인증** 또는 **사용자 이름 + PIN**으로 등록하는 장치의 경우 사용자는 Secure Hub에 자격 증명을 수동으로 입력해야 합니다.

8. **에이전트 다운로드**, **등록 URL**, **등록 PIN** 및 **등록 확인** 템플릿의 경우 이전에 생성한 사용자 지정 알림 템플릿을 선택하거나 나열된 기본값을 선택합니다.

   사용자 지정 알림 템플릿을 사용할 계획이라면 등록 보안 모드를 구성하기 전에 템플릿을 설정해야 합니다. 알림 템플릿에 대한 자세한 내용은 알림을 참조하십시오.

   이러한 알림 템플릿의 경우 XenMobile 내에서 구성된 SMTP 서버 설정을 사용하십시오. 진행하기 전에 먼저 SMTP 정보를 설정하십시오.

   > **참고:**

> **만료 기간** 및 **최대 시도 횟수** 옵션은 선택한 **등록 모드** 옵션에 따라 변경됩니다. 이러한 옵션은 변경할 수 없습니다.

9. **초대 보내기**를 ON으로 선택한 다음 **저장 및 보내기**를 클릭하여 프로세스를 완료합니다.

중첩 그룹 지원

중첩 그룹을 사용하여 초대를 보낼 수 있습니다. 일반적으로 중첩 그룹은 유사한 권한을 가진 그룹이 서로 연결된 대규모 환경에서 사용됩니다.

설정 > LDAP으로 이동한 다음 **중첩 그룹 지원** 옵션을 사용하도록 설정합니다.

문제 해결 및 알려진 제한 사항

문제: Active Directory 그룹에서 제거되었음에도 불구하고 사용자에게 초대가 전송됩니다.

해결 방법: Active Directory 환경의 규모에 따라 변경 사항이 모든 서버에 전파되는 데 최대 6시간이 걸릴 수 있습니다. 사용자 또는 중첩 그룹이 최근에 제거된 경우 XenMobile은 해당 사용자를 여전히 그룹의 일부로 간주할 수 있습니다.

따라서 그룹에 다른 그룹 초대를 보내기 전에 최대 6시간을 기다리는 것이 가장 좋습니다.

온프레미스 장치 상태 증명 서버 구성

온프레미스 Windows 서버를 통해 Windows 10 및 Windows 11 모바일 장치에 대해 장치 상태 증명(DHA)을 활성화할 수 있습니다. 온프레미스에서 DHA를 활성화하려면 먼저 DHA 서버를 구성해야 합니다.

DHA 서버를 구성한 후 온프레미스 DHA 서비스를 활성화하기 위한 XenMobile Server 정책을 생성합니다. 이 정책 생성에 대한 자세한 내용은 장치 상태 증명 장치 정책을 참조하십시오.

DHA 서버의 전제 조건

- Desktop Experience 설치 옵션을 사용하여 설치된 Windows Server Technical Preview 5 이상을 실행하는 서버.
- 하나 이상의 Windows 10 및 Windows 11 클라이언트 장치. 이 장치에는 최신 버전의 Windows를 실행하는 TPM 1.2 또는 2.0이 있어야 합니다.
- 다음 인증서:
  - **DHA SSL 인증서:** 내보낼 수 있는 개인 키가 있는 엔터프라이즈 신뢰할 수 있는 루트에 연결되는 x.509 SSL 인증서입니다. 이 인증서는 다음 통신을 포함하여 전송 중인 DHA 데이터 통신을 보호합니다.

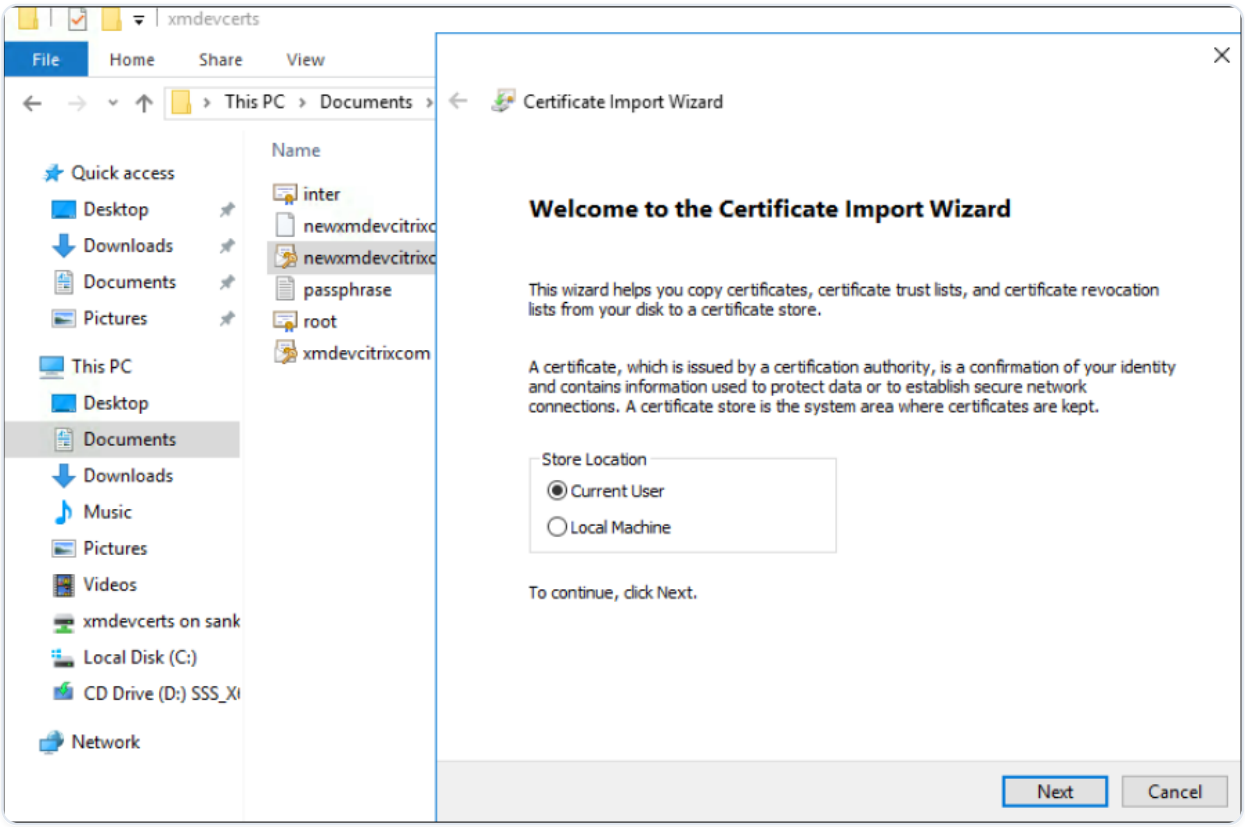
    - 서버 간 (DHA 서비스 및 MDM 서버)
    - 서버-클라이언트 (DHA 서비스 및 Windows 10 또는 Windows 11 장치)
  - **DHA 서명 인증서:** 내보낼 수 있는 개인 키가 있는 엔터프라이즈 신뢰할 수 있는 루트에 연결되는 x.509 인증서입니다. DHA 서비스는 이 인증서를 디지털 서명에 사용합니다.
  - **DHA 암호화 인증서:** 내보낼 수 있는 개인 키가 있는 엔터프라이즈 신뢰할 수 있는 루트에 연결되는 x.509 인증서입니다. DHA 서비스는 이 인증서를 암호화에도 사용합니다.
- 다음 인증서 유효성 검사 모드 중 하나를 선택합니다.
  - **EKCert:** EKCert 유효성 검사 모드는 인터넷에 연결되지 않은 조직의 장치에 최적화되어 있습니다. EKCert 유효성 검사 모드에서 실행되는 DHA 서비스에 연결하는 장치는 인터넷에 직접 액세스할 수 없습니다.
  - **AIKCert:** AIKCert 유효성 검사 모드는 인터넷에 액세스할 수 있는 운영 환경에 최적화되어 있습니다. AIKCert 유효성 검사 모드에서 실행되는 DHA 서비스에 연결하는 장치는 인터넷에 직접 액세스할 수 있어야 하며 Microsoft에서 AIK 인증서를 받을 수 있습니다.

Windows 서버에 DHA 서버 역할 추가

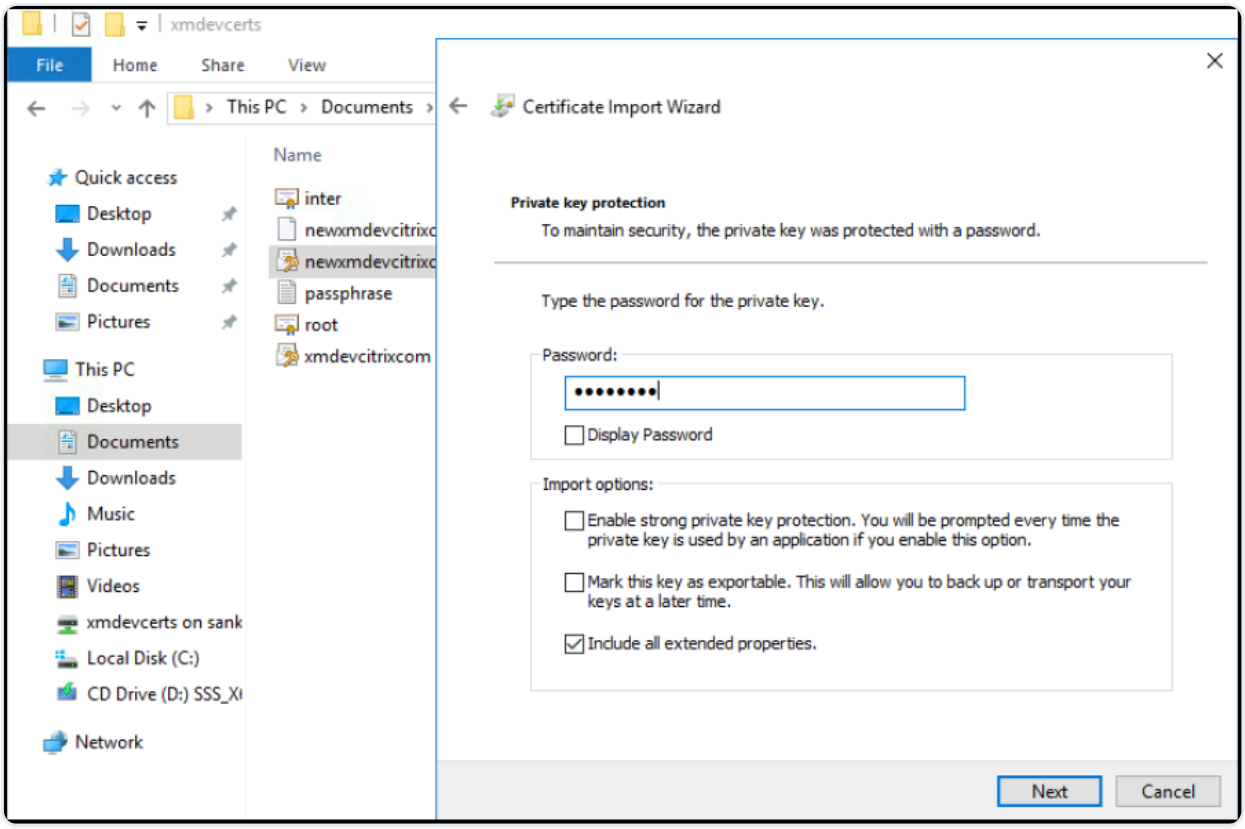
1. Windows 서버에서 서버 관리자가 아직 열려 있지 않은 경우, **시작**을 클릭한 다음 **서버 관리자**를 클릭합니다.
2. **역할 및 기능 추가**를 클릭합니다.
3. **시작하기 전** 페이지에서 **다음**을 클릭합니다.
4. **설치 유형 선택** 페이지에서 **역할 기반 또는 기능 기반 설치**를 클릭한 다음 **다음**을 클릭합니다.
5. **대상 서버 선택** 페이지에서 **서버 풀에서 서버 선택**을 클릭하고 서버를 선택한 다음 **다음**을 클릭합니다.
6. **서버 역할 선택** 페이지에서 Device Health Attestation 확인란을 선택합니다.
7. 선택 사항: **기능 추가**를 클릭하여 다른 필수 역할 서비스 및 기능을 설치합니다.
8. **다음**을 클릭합니다.
9. **기능 선택** 페이지에서 **다음**을 클릭합니다.
10. **웹 서버 역할(IIS)** 페이지에서 **다음**을 클릭합니다.
11. **역할 서비스 선택** 페이지에서 **다음**을 클릭합니다.
12. **Device Health Attestation 서비스** 페이지에서 **다음**을 클릭합니다.
13. **설치 선택 확인** 페이지에서 **설치**를 클릭합니다.
14. 설치가 완료되면 **닫기**를 클릭합니다.

서버의 인증서 저장소에 SSL 인증서를 추가합니다

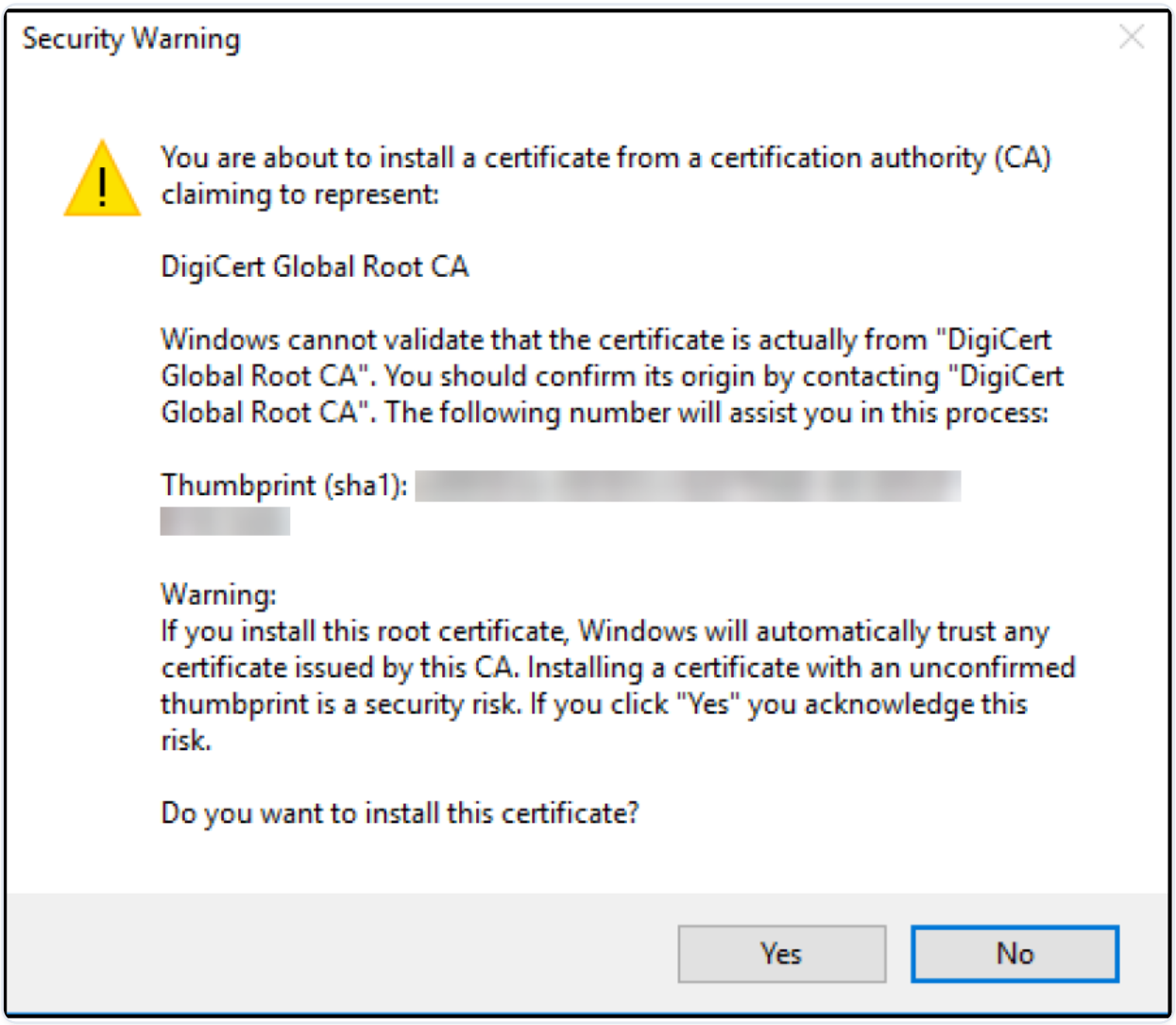
1. SSL 인증서 파일로 이동하여 선택합니다.
2. 저장소 위치로 **현재 사용자**를 선택하고 **다음**을 클릭합니다.



3. 개인 키의 암호를 입력합니다.
4. 가져오기 옵션 **모든 확장 속성 포함**이 선택되어 있는지 확인합니다. **다음**을 클릭합니다.



5. 이 창이 나타나면 **예**를 클릭합니다.



6. 인증서가 설치되었는지 확인합니다.

   a. 명령 프롬프트 창을 엽니다.

   b. **mmc**를 입력하고 Enter 키를 누릅니다. 로컬 컴퓨터 저장소의 인증서를 보려면 관리자 역할이어야 합니다.

   c. 파일 메뉴에서 **스냅인 추가/제거**를 클릭합니다.

   d. **추가**를 클릭합니다.

   e. 독립 실행형 스냅인 추가 대화 상자에서 **인증서**를 선택합니다.

   f. **추가**를 클릭합니다.

   g. **인증서 스냅인** 대화 상자에서 **내 사용자 계정**을 선택합니다. (서비스 계정 소유자로 로그인한 경우 **서비스 계정**을 선택합니다.)

   h. 컴퓨터 선택 대화 상자에서 **마침**을 클릭합니다.

   Windows Server Manager의 이미지(/en-us/xenmobile/server/media/configure-dha-thumbprint5.png)

7. **서버 관리자 > IIS**로 이동하여 아이콘 목록에서 **서버 인증서**를 선택합니다.

   Windows Server Manager의 이미지(/en-us/xenmobile/server/media/configure-dha-addcert5.png)

8. 작업 메뉴에서 **가져오기...**를 선택하여 SSL 인증서를 가져옵니다.

   Windows Server Manager의 이미지(/en-us/xenmobile/server/media/configure-dha-addcert6.png)

인증서 지문 검색 및 저장

1. 파일 탐색기 검색 창에 **mmc**를 입력합니다.
2. 콘솔 루트 창에서 **파일 > 스냅인 추가/제거...**를 클릭합니다.

   Windows 파일 탐색기 이미지(/en-us/xenmobile/server/media/configure-dha-thumbprint1.png)

3. 사용 가능한 스냅인에서 인증서를 선택하고 선택한 스냅인에 추가합니다.

   Windows 스냅인 추가 또는 제거 이미지(/en-us/xenmobile/server/media/configure-dha-thumbprint2.png)

4. **내 사용자 계정**을 선택합니다.

   Windows 스냅인 추가 또는 제거 이미지(/en-us/xenmobile/server/media/configure-dha-thumbprint3.png)

5. 인증서를 선택하고 **확인**을 클릭합니다.

   Windows 스냅인 추가 또는 제거 이미지(/en-us/xenmobile/server/media/configure-dha-thumbprint4.png)

6. 인증서를 두 번 클릭하고 **자세히** 탭을 선택합니다. 아래로 스크롤하여 인증서 지문을 확인합니다.

   Windows 스냅인 추가 또는 제거 이미지(/en-us/xenmobile/server/media/configure-dha-thumbprint5.png)

7. 지문을 파일에 복사합니다. PowerShell 명령에서 지문을 사용할 때는 공백을 제거합니다.

서명 및 암호화 인증서 설치

Windows 서버에서 다음 PowerShell 명령을 실행하여 서명 및 암호화 인증서를 설치합니다.

자리 표시자 ReplaceWithThumbprint를 바꾸고 표시된 대로 이중 따옴표 안에 넣습니다.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint
-like "ReplaceWithThumbprint"}



$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName



$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
$keyname icacls $keypath /grant IIS_IUSRS`:R
```

TPM 루트 인증서 추출 및 신뢰할 수 있는 인증서 패키지 설치

Windows 서버에서 다음 명령을 실행합니다.

```
mkdir .\TrustedTpm



expand -F:\* .\TrustedTpm.cab .\TrustedTpm



cd .\TrustedTpm



.\setup.cmd
```

DHA 서비스 구성

Windows 서버에서 이 명령을 실행하여 DHA 서비스를 구성합니다.

자리 표시자 ReplaceWithThumbprint를 바꿉니다.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
ReplaceWithThumbprint



-SigningCertificateThumbprint ReplaceWithThumbprint
```

```
-SslCertificateStoreName My -SslCertificateThumbprint
ReplaceWithThumbprint



-SupportedAuthenticationSchema "AikCertificate"
```

Windows 서버에서 다음 명령을 실행하여 DHA 서비스에 대한 인증서 체인 정책을 설정합니다.

```
$policy = Get-DHASCertificateChainPolicy



$policy.RevocationMode = "NoCheck"



Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

다음과 같이 메시지에 응답합니다.

```
  Confirm



    Are you sure you want to perform this action?



    Performing the operation "Install-DeviceHealthAttestation" on target
"WIN-N27D1FKCEBT".



    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): A
```

```
    Adding SSL binding to website 'Default Web Site'.


    Add SSL binding?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.


    Add application pool?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Adding web application 'DeviceHealthAttestation' to website 'Default
Web Site'.


    Add web application?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Adding firewall rule 'Device Health Attestation Service' to allow
inbound connections on port(s) '443'.


    Add firewall rule?
```

```
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Setting initial configuration for Device Health Attestation Service.

Set initial configuration?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Registering User Access Logging.

Register User Access Logging?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

구성 확인

DHASActiveSigningCertificate가 활성 상태인지 확인하려면 서버에서 다음 명령을 실행합니다.

`Get-DHASActiveSigningCertificate`

인증서가 활성 상태이면 인증서 유형(서명)과 지문이 표시됩니다.

DHASActiveSigningCertificate가 활성 상태인지 확인하려면 서버에서 다음 명령을 실행합니다.

자리 표시자 ReplaceWithThumbprint를 바꾸고 표시된 대로 이중 따옴표 안에 넣습니다.

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
-Force



Get-DHASActiveEncryptionCertificate
```

인증서가 활성 상태이면 지문이 나타납니다.

최종 확인을 위해 다음 URL로 이동합니다.

`https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1`

DHA 서비스가 실행 중이면 “Method not allowed”가 나타납니다.



EWS를 사용하여 Secure Mail 푸시 알림에 대한 인증서 기반 인증 구성

Vijay Kumar Kunchakuri 님이 기여했습니다.

Secure Mail 푸시 알림이 작동하도록 하려면 Exchange Server를 인증서 기반 인증용으로 구성해야 합니다. 이는 Secure Hub가 인증서 기반 인증으로 XenMobile®에 등록될 때 필요합니다.

Exchange 메일 서버에서 Active Sync 및 Exchange 웹 서비스(EWS) 가상 디렉터리를 인증서 기반 인증으로 구성해야 합니다.

이러한 구성을 완료하지 않으면 Secure Mail 푸시 알림 구독이 실패하고 Secure Mail에서 배지 업데이트가 발생하지 않습니다.

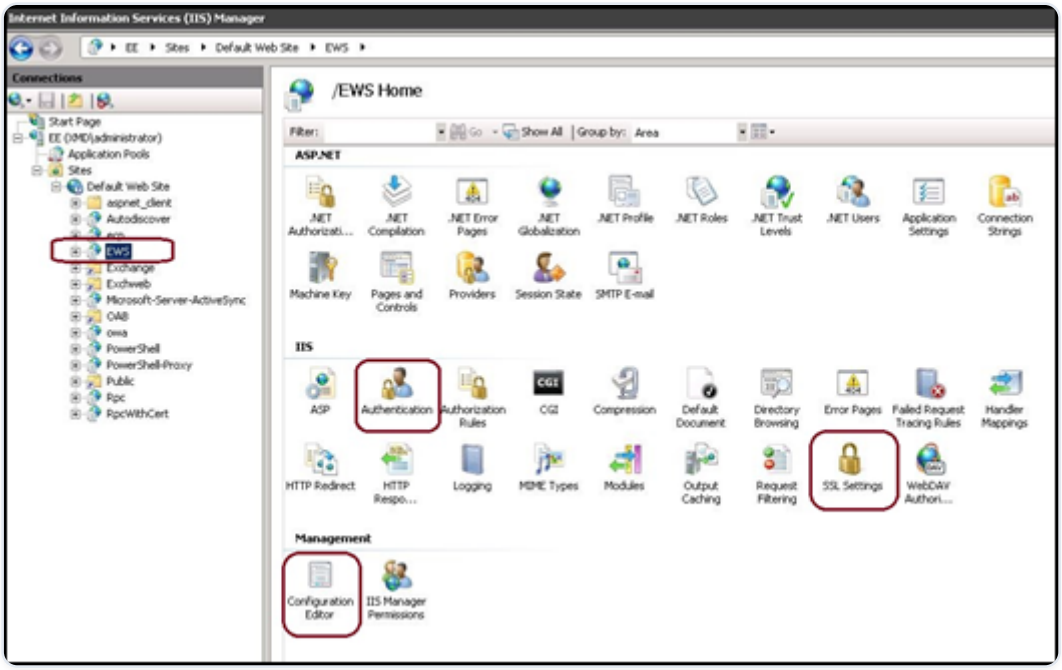
이 문서에서는 인증서 기반 인증을 구성하는 단계를 설명합니다. 구성은 특히 Exchange Server의 EWS 가상 디렉터리에 대한 것입니다.

구성을 시작하려면 다음을 수행하십시오.

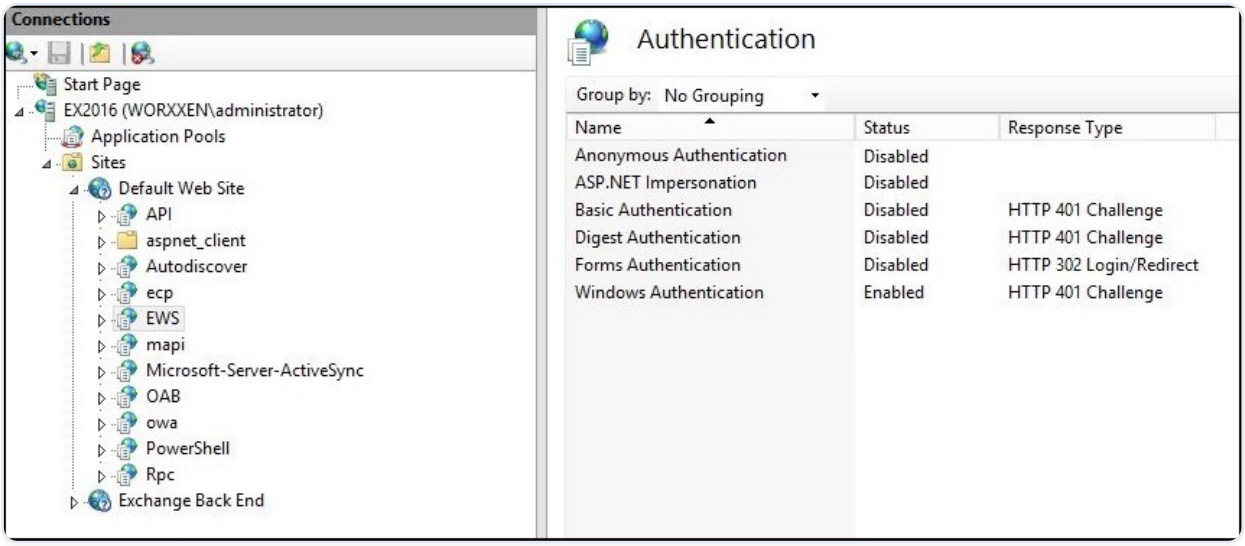
1. EWS 가상 디렉터리가 설치된 서버에 로그온합니다.

2. IIS 관리자 콘솔을 엽니다.
3. **기본 웹 사이트** 아래에서 EWS 가상 디렉터리를 클릭합니다.

   인증, SSL, 구성 편집기 스냅인은 IIS 관리자 콘솔의 오른쪽에 있습니다.



4. EWS에 대한 **인증** 설정이 다음 그림과 같이 구성되었는지 확인합니다.



5. EWS 가상 디렉터리에 대한 **SSL 설정**을 구성합니다.

   a. **Require SSL** 확인란을 선택합니다.

   b. **클라이언트 인증서**에서 **필수**를 클릭합니다. 다른 EWS 메일 클라이언트가 사용자 이름과 암호를 자격 증명으로 사용하여 Exchange Server에 인증하고 연결하는 경우 이 옵션을 **수락**으로 설정할 수 있습니다.

IIS 관리자 콘솔 이미지(/en-us/xenmobile/server/media/ews-xenmobile-ssl-settings.png)

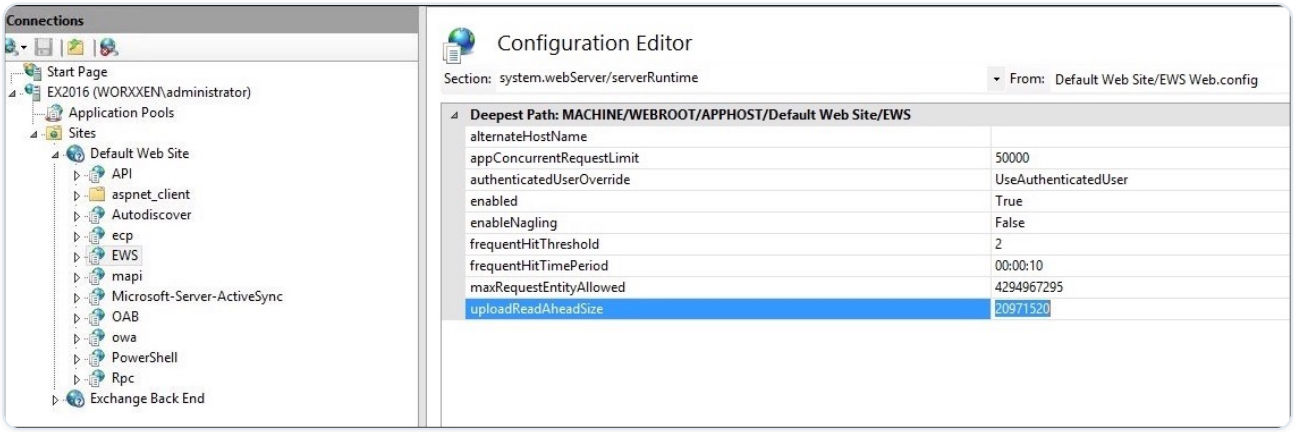
6. **구성 편집기**를 클릭합니다. **섹션** 드롭다운 목록에서 다음 섹션으로 이동합니다.
   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**
7. **enabled** 값을 **True**로 설정합니다.

   IIS 관리자 콘솔 이미지(/en-us/xenmobile/server/media/ews-xenmobile-configuration-editor.png)
8. **구성 편집기**를 클릭합니다. **섹션** 드롭다운 목록에서 다음 섹션으로 이동합니다.
   - **system.webServer/serverRuntime**
9. **uploadReadAheadSize** 값을 **10485760** (10MB) 또는 **20971520** (20MB) 또는 조직에서 요구하는 값으로 설정합니다.

> **중요:**
>
> 이 값을 올바르게 설정하지 않으면 EWS 푸시 알림을 구독하는 동안 인증서 기반 인증이 오류 코드 413으로 실패할 수 있습니다.
>
> 이 값을 **0**으로 설정하지 마십시오.

자세한 내용은 다음 타사 리소스를 참조하십시오.

- Microsoft IIS 서버 런타임
- Butsch 클라이언트 관리 블로그



iOS 푸시 알림과 관련된 Secure Mail 문제 해결에 대한 자세한 내용은 이 Citrix 지원 기술 자료 문서를 참조하십시오.

관련 정보

iOS용 Secure Mail 푸시 알림

XenMobile® 모바일 장치 관리(MDM)를 Cisco Identity Services Engine (ISE)과 통합

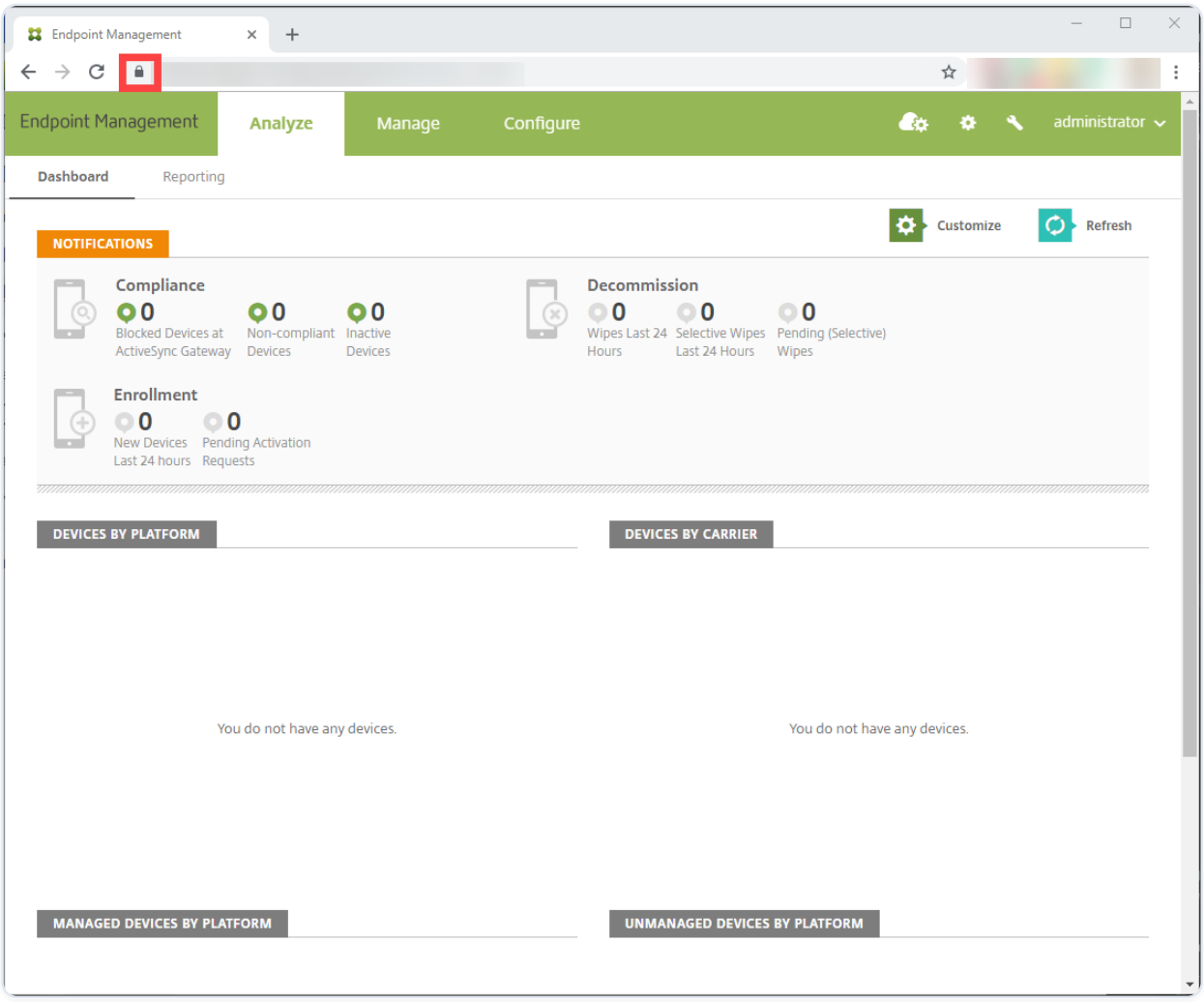
Cisco ISE는 직장에서 모바일 장치를 배포, 보호, 모니터링, 통합 및 관리하는 데 사용됩니다. 모바일 장치에 다운로드된 소프트웨어는 다음을 제어합니다.

- 애플리케이션 및 패치 배포
- 엔드포인트의 데이터 및 구성

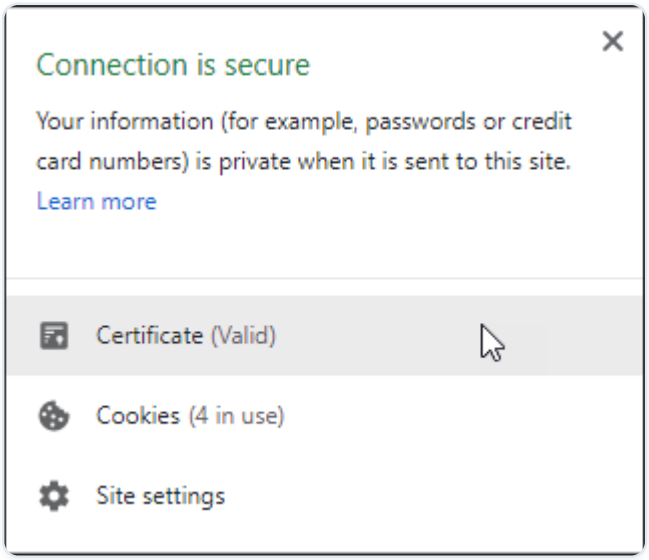
XenMobile은 Cisco ISE 콘솔에서 비준수 및 관리되지 않는 장치를 관리하기 위해 Cisco ISE와 통합할 수 있습니다. XenMobile은 또한 기업 서비스에 대한 액세스를 선택적으로 허용, 거부 또는 격리할 수 있도록 합니다.

XenMobile과 통합을 설정하려면 XenMobile Server에 관리자 RBAC 역할이 할당된 로컬 서비스 계정을 생성하십시오. 이 역할은 Cisco ISE가 XenMobile API에 액세스할 수 있도록 합니다. ISE는 XenMobile 인증서를 신뢰해야 합니다. 이 인증서를 다운로드하려면 웹 브라우저를 열고 서버 URL로 이동하여 로그인하십시오.

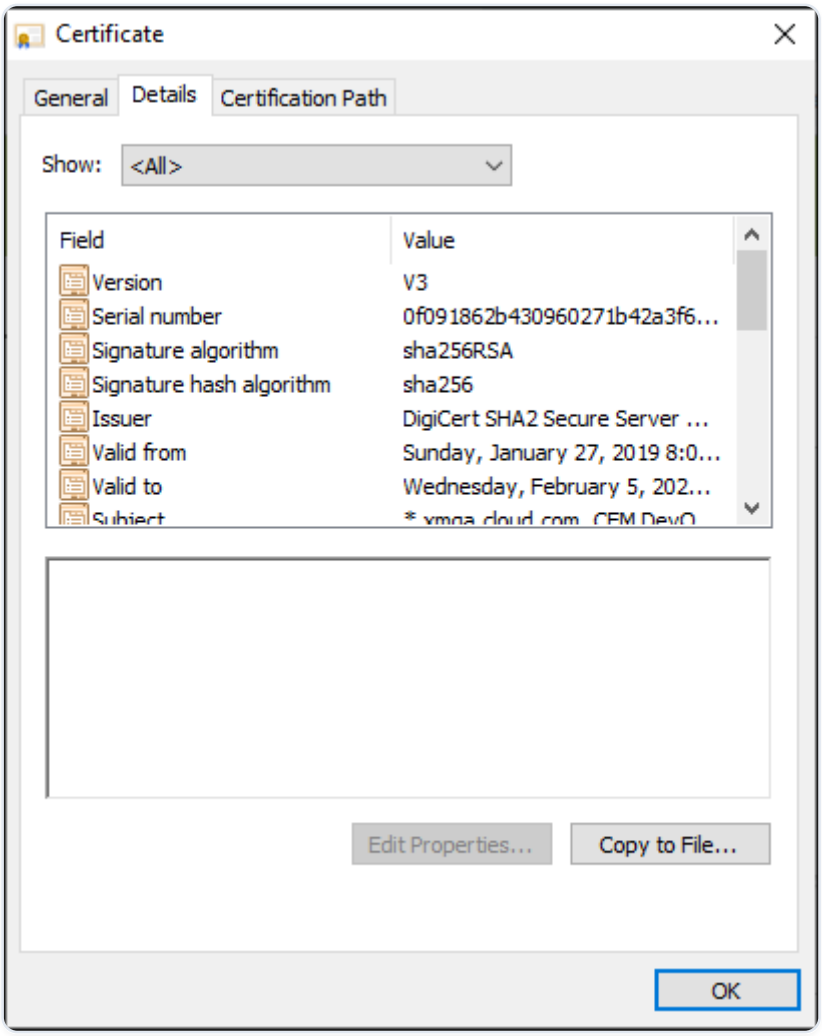
1. 로그인한 후 주소 표시줄의 URL 옆에 있는 자물쇠를 클릭합니다.



2. **인증서**를 클릭합니다.



3. **세부 정보** 탭을 선택하고 **파일로 복사**를 클릭합니다.



4. 마법사를 따라 인증서를 로컬에 저장합니다.
5. Cisco ISE 콘솔에 로그인하여 이전에 다운로드한 XenMobile 인증서를 가져옵니다. Cisco ISE의 신뢰할 수 있는 인증서 저장소로 인증서를 가져옵니다. 이는 Cisco ISE가 XenMobile Server와의 통신을 신뢰하는 데 필요합니다.

    a. **관리 > 시스템 > 인증서 > 인증서 관리 > 신뢰할 수 있는 인증서**로 이동합니다. **가져오기**를 클릭합니다.

    b. 인증서 이름을 지정하고 **ISE 내 인증을 위한 신뢰** 및 **Cisco 서비스 인증을 위한 신뢰** 확인란을 선택합니다.

6. Cisco ISE 내에서 XenMobile을 외부 MDM으로 추가합니다.

    a. **관리 > 네트워크 리소스 > 외부 MDM**으로 이동합니다. **추가**를 클릭하고 다음을 작성합니다.

    - **서버 호스트:** XenMobile FQDN
    - **포트:** 443

- **인스턴스 이름:** XenMobile Server의 인스턴스 이름입니다. 대부분의 배포에서 인스턴스 이름은 기본적으로 "zdm"입니다.
- **사용자 이름:** 이 작업을 위해 생성한 사용자 이름을 입력합니다. 사용자는 원래 관리자 RBAC 그룹의 로컬 관리자 계정이어야 합니다.
- **암호:** 방금 추가한 사용자의 암호입니다.
- **활성화**라고 표시된 곳을 확인합니다.

7. 테스트가 성공하면 **제출**을 클릭합니다.

Cisco ISE에 대한 자세한 내용은 Cisco 설명서를 참조하십시오.

> **참고:**

> ISE 통합은 호스팅된 Endpoint Management에서는 지원되지 않습니다.

Citrix XenMobile® Server 문서 변경 기록

다음 표에서는 XenMobile Server 제품 설명서의 중요한 변경 사항을 설명합니다. 이러한 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

날짜	변경 사항	설명
27 Jan 2026	XenMobile Server 10.16 롤링 패치 8 릴리스 정보	
20 Nov 2025	XenMobile Server 10.15 롤링 패치 13 릴리스 정보	
13 Nov 2025	XenMobile Server 10.16 롤링 패치 7 릴리스 정보	
23 Oct 2025	XenMobile Server 10.15 롤링 패치 12 릴리스 정보	
26 Sep 2025	XenMobile Server 10.16 롤링 패치 6 릴리스 정보	
13 May 2025	XenMobile Server 10.15 롤링 패치 11 릴리스 정보	지원 문서 CTX693257을 참조하십시오.
15 Apr 2025	XenMobile Server 10.16 롤링 패치 5 릴리스 정보	지원 문서 CTX692919를 참조하십시오.
27 Jan 2025	XenMobile Server 10.15 롤링 패치 10 릴리스 정보	지원 문서 CTX692560을 참조하십시오.
18 Dec 2024	XenMobile Server 10.16 롤링 패치 4 릴리스 정보	지원 문서 CTX692370을 참조하십시오.
04 Dec 2024	XenMobile Server 10.15 롤링 패치 9 릴리스 정보	지원 문서 CTX692268을 참조하십시오.
28 Aug 2024	XenMobile Server 10.16 롤링 패치 3 릴리스 정보	지원 문서 CTX691503을 참조하십시오.

날짜	변경 사항	설명
11 Jul 2024	XenMobile Server 10.15 롤링 패치 8 릴리스 정보	지원 문서 CTX691107을 참조하십시오.
02 Jul 2024	XenMobile Server 10.16 롤링 패치 2 릴리스 정보	지원 문서 CTX678043을 참조하십시오.
17 Jun 2024	XenMobile Server 10.16 롤링 패치 1 릴리스 정보	지원 문서 CTX677872를 참조하십시오.
06 Jun 2024	XenMobile Server 10.15 롤링 패치 7 릴리스 정보	지원 문서 CTX677079을 참조하십시오.
08 Mar 2024	XenMobile Server 10.14 롤링 패치 13 릴리스 정보	지원 문서 CTX628921을 참조하십시오.
06 Mar 2024	XenMobile Server 10.15 롤링 패치 6 릴리스 정보	지원 문서 CTX625010을 참조하십시오.
13 Nov 2023	XenMobile Server 10.15 롤링 패치 5 릴리스 정보	지원 문서 CTX583748을 참조하십시오.
19 Oct 2023	XenMobile Server 10.14 롤링 패치 12 릴리스 정보	지원 문서 CTX582535을 참조하십시오.
18 Sep 2023	XenMobile Server 10.15 롤링 패치 4 릴리스 정보	지원 문서 CTX579528을 참조하십시오.
19 Jul 2023	XenMobile Server 10.15 롤링 패치 3 릴리스 정보	지원 문서 CTX565649을 참조하십시오.
31 May 2023	XenMobile Server 10.14 롤링 패치 11 릴리스 정보	지원 문서 CTX558678을 참조하십시오.
26 Apr 2023	XenMobile Server 10.15 롤링 패치 2 릴리스 정보	지원 문서 CTX546782를 참조하십시오.
11 Apr 2023	XenMobile Server 10.14 롤링 패치 10 릴리스 정보에 수정된 문제 추가	수정된 문제를 참조하십시오.
23 Mar 2023	XenMobile Server 10.14 롤링 패치 10 릴리스 정보	지원 문서 CTX491036을 참조하십시오.

날짜	변경 사항	설명
23 Feb 2023	XenMobile Server 10.15 롤링 패치 1 릴리스 정보	지원 문서 CTX478719를 참조하십시오.
20 Dec 2022	XenMobile Server 10.14 롤링 패치 9 릴리스 정보	지원 문서 CTX477055을 참조하십시오.
16 Nov 2022	XenMobile Server 10.15 릴리스에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 XenMobile Server 10.15의 새로운 기능을 참조하십시오.
22 Sep 2022	XenMobile Server 10.14 롤링 패치 8 릴리스 정보	지원 문서 CTX464099을 참조하십시오.
08 Sep 2022	XenMobile Server 10.13 롤링 패치 10 릴리스 정보	지원 문서 CTX463922을 참조하십시오.
18 Aug 2022	XenMobile Server 10.14 롤링 패치 7 릴리스 정보	지원 문서 CTX463691을 참조하십시오.
14 Jun 2022	XenMobile Server 10.13 롤링 패치 9 릴리스 정보	지원 문서 CTX460128을 참조하십시오.
23 May 2022	XenMobile Server 10.14 롤링 패치 6 릴리스 정보	지원 문서 CTX459871을 참조하십시오.
12 Apr 2022	XenMobile Server 10.13 롤링 패치 8 릴리스 정보	지원 문서 CTX447596을 참조하십시오.
30 Mar 2022	XenMobile Server 10.14 롤링 패치 5 릴리스 정보	지원 문서 CTX399411을 참조하십시오.
01 Mar 2022	XenMobile Server 10.13 롤링 패치 7 릴리스 정보	지원 문서 CTX341602을 참조하십시오.
26 Jan 2022	XenMobile Server 10.14 롤링 패치 4 릴리스 정보	지원 문서 CTX339069을 참조하십시오.
22 Dec 2021	XenMobile Server 10.14 롤링 패치 3 릴리스 정보	지원 문서 CTX335897을 참조하십시오.
21 Dec 2021	XenMobile Server 10.13 롤링 패치 6 릴리스 정보	지원 문서 CTX335875을 참조하십시오.

날짜	변경 사항	설명
21 Dec 2021	XenMobile Server 10.12 롤링 패치 11 릴리스 정보	지원 문서 CTX335861을 참조하십시오.
16 Dec 2021	XenMobile Server 10.12 롤링 패치 10 릴리스 정보	지원 문서 CTX335785을 참조하십시오.
15 Dec 2021	XenMobile Server 10.14 롤링 패치 2 릴리스 정보	지원 문서 CTX335763을 참조하십시오.
15 Dec 2021	XenMobile Server 10.13 롤링 패치 5 릴리스 정보	지원 문서 CTX335753을 참조하십시오.
19 Nov 2021	XenMobile Server 10.14 롤링 패치 1 릴리스 정보	지원 문서 CTX335342을 참조하십시오.
08 Oct 2021	XenMobile Server 10.12 롤링 패치 9 릴리스 정보	지원 문서 CTX331040을 참조하십시오.
15 Sep 2021	XenMobile Server 10.14 릴리스에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 XenMobile Server 10.14의 새로운 기능을 참조하십시오.
11 Aug 2021	XenMobile Server 10.13 롤링 패치 4 릴리스 정보	지원 문서 CTX324159을 참조하십시오.
02 Jun 2021	XenMobile Server 10.12 롤링 패치 8 릴리스 정보	지원 문서 CTX316910을 참조하십시오.
13 May 2021	XenMobile Server 10.13 롤링 패치 3 릴리스 정보	지원 문서 CTX315034을 참조하십시오.
27 Apr 2021	찾기 보안 작업에 대한 설명 업데이트	보안 작업을 참조하십시오.
23 Apr 2021	작업 예시 추가	자동화된 작업을 참조하십시오.
01 Apr 2021	앱별 VPN 요구 사항에 대한 설명 추가	VPN 장치 정책을 참조하십시오.
24 Feb 2021	iOS 14.5로 엔드포인트를 업그레이드하기 전에 필요한 준비에 대한 공지 추가	iOS 14.5로 엔드포인트를 업그레이드하기 전을 참조하십시오.

날짜	변경 사항	설명
17 Dec 2020	Android Enterprise에서 설치된 관리되는 앱이 업데이트되는 방식을 제어하는 새로운 장치 정책	관리되는 앱 자동 업데이트 장치 정책
18 Nov 2020	온프레미스 Citrix ADC와 관련된 단일 Sign-On 문제에 대한 해결 방법 추가	온프레미스 Citrix ADC를 업그레이드하기 전을 참조하십시오.
26 Oct 2020	XenMobile Server 10.13 릴리스에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 XenMobile Server 10.13의 새로운 기능을 참조하십시오.
02 Jul 2020	MDX 암호화 사용 중단에 대한 타임라인 및 작업 계획 추가	예정된 변경 사항에 대비하여 Android 장치 준비를 참조하십시오.
19 Jun 2020	설명서에서 "blacklist" 및 "whitelist" 용어 처리. "block list" 및 "allow list"로 변경.	Endpoint Management 콘솔에는 현재 "blacklist" 및 "whitelist" 용어가 포함되어 있습니다. 설명서를 업데이트했습니다. 향후 릴리스를 위해 제품 콘솔의 용어를 변경하는 중입니다.
04 May 2020	iOS, iPadOS 및 macOS의 신뢰할 수 있는 인증서에 대한 새로운 TLS 인증서 요구 사항에 대한 참고 사항 추가	인증서를 참조하십시오.
18 Feb 2020	용어 업데이트	설명서 전체에서 NetScaler®, NetScaler Gateway, ShareFile 및 스토리지 영역 컨트롤러 용어를 업데이트했습니다. 일부 콘솔 구성 요소에는 여전히 이전 이름이 표시될 수 있습니다.
06 Feb 2020	XenMobile Server 10.12 릴리스에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 XenMobile Server 10.12의 새로운 기능을 참조하십시오.

날짜	변경 사항	설명
06 Nov 2019	Apple VPP에서 ABM 또는 ASM으로 마이그레이션에 대한 섹션 추가	Apple VPP(Volume Purchase Program)를 Apple Business Manager(ABM) 및 Apple School Manager(ASM)로 마이그레이션을 참조하십시오.
04 Sep 2019	XenMobile Server 10.11 릴리스에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 XenMobile Server 10.11의 새로운 기능을 참조하십시오.
15 May 2019	iOS 장치 등록 섹션 업데이트	iOS 12 장치 등록을 위한 비디오 및 업데이트된 단계 추가. iOS 장치 등록을 참조하십시오.
10 May 2019	Entrust PKI에 대한 새 섹션	"PKI 엔터티" 문서에 섹션 추가: PKI 엔터티.
03 Apr 2019	Apple DEP 갱신 단계에 대한 새 섹션	"Apple DEP를 통한 장치 배포"에 섹션 추가: Apple 배포 프로그램 등록 갱신.
02 Apr 2019	Exchange ActiveSync 8.5.3 릴리스용 Gateway 커넥터에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 버전 8.5.3의 새로운 기능을 참조하십시오.
26 Mar 2019	Secure Hub 스토어 이름 구문 업데이트	앱 스토어 및 Citrix Secure Hub 브랜딩에서 스토어 이름의 영숫자 요구 사항에 대한 참고 사항 추가.
06 Mar 2019	Exchange ActiveSync 10.1.9 릴리스용 Endpoint Management 커넥터에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 버전 10.1.9의 새로운 기능을 참조하십시오.
01 Feb 2019	Exchange ActiveSync 10.1.8 릴리스용 Endpoint Management 커넥터에 대한 문서 업데이트	새로운 기능 및 변경된 기능 요약은 버전 10.1.8의 새로운 기능을 참조하십시오.

날짜	변경 사항	설명
23 Jan 2019	Secure Browse 용어 업데이트	설명서 전체에서 MDX 설정 "Secure Browse"를 "터널링된 웹 SSO"로 이름을 변경했습니다. 자세한 내용은 iOS의 경우 앱 네트워크 액세스 및 Android의 경우 앱 네트워크 액세스를 참조하십시오.