AppTec360 엔터프라이즈 모바일 관리자 및 콘텐츠박스

관리 매뉴얼 | 버전 5.0 (202110)

목차

- 메시지(디바이스 수준에서만)
- 보안 구성
  - 암호
  - 암호화
  - 안티바이러스
- 수명 종료(디바이스 수준에서만)
  - 지우기(디바이스 수준에서만)
- 제한 설정
  - 제한 사항
  - AE 장치 소유자

BYOD 컨테이너

- Android 엔터프라이즈
  - Android 엔터프라이즈
  - Gmail 교환
  - AE 시스템 앱
  - 컨테이너 암호
- 삼성 KNOX
  - 활성화
  - Knox 암호
  - Knox 보안
  - Knox Exchange
  - Knox 이메일
  - Knox 앱

연결 관리

- Wi-Fi
  - 보안 유형
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- 제한 사항
- APN
- 블루투스

PIM 관리

- 교환

- 이메일
- AE Gmail 교환

앱 관리

- 엔터프라이즈 앱 관리자
  - 설치된 앱(디바이스 수준에서만)
  - 시스템 앱(디바이스 수준에서만)
  - 필수 앱
  - AE 시스템 앱
- 제한 및 설정
  - 블랙리스트 및 화이트리스트
  - 시스템 앱 제한
    - 삼성 앱
    - 화웨이 앱
  - 앱 관리 설정
- 엔터프라이즈 앱 스토어
  - Play스토어
  - 사내
- 기업용 Play 스토어
- 키오스크 모드 및 런처
  - 키오스크 모드
  - AppTec360 런처
  - AppTec360 설정

원격 제어

- 스플래시탑
- 팀뷰어

콘텐츠 관리

- 콘텐츠 상자
- 보안 브라우저

구성 Windows 10 PC

일반

- 그룹 프로필 개요(그룹 수준에서만)
- 장치 개요(장치 수준에서만)
- 설정
- 구성 수정(디바이스 수준에서만)

- 디바이스 로그(디바이스 수준에서만)
  - 명령 로그
  - 가능한 명령 상태
- 자산 관리(디바이스 수준에서만)
  - 장치 정보
  - 셀룰러
  - 동기화 정보
- 보안 관리
  - 도난 방지(디바이스 수준에서만)
    - GPS 정보(디바이스 수준에서만)
    - GPS 설정
  - 보안 구성
    - 암호
    - 바이러스 백신
    - 보안 센터
    - 방화벽 구성
    - 방화벽 규칙
  - 제한 설정
    - 디바이스 기능
  - BitLocker
    - BitLocker 구성
    - 비트락커 상태
  - 인증서 관리
    - 인증서 목록
    - 인증서 구성
    - SCEP
- 연결 관리
  - Wi-Fi
    - 보안 유형
    - 프록시 서버 사용
  - 와이파이 제한
  - VPN
    - 연결 유형
    - 일반 VPN 구성
  - VPN 제한 사항
  - 블루투스
- PIM 관리

- Exchange Active 동기화
- 이메일
- 앱 관리
  - 엔터프라이즈 앱 관리자
    - 설치된 앱
    - 필수 앱
    - 시스템 앱 제한
    - 블랙리스트 및 화이트리스트

MacOS 구성

일반

- 그룹 프로필 개요(그룹 수준에서만)
- 장치 개요(장치 수준에서만)
- 구성 수정(디바이스 수준에서만)
- 디바이스 로그(디바이스 수준에서만)
  - 명령 로그
  - 가능한 명령 상태

자산 관리(디바이스 수준에서만)

- 장치 정보
- WiFi
- 셀룰러
- 블루투스

업데이트 관리(디바이스 수준에서만)

- 정보 업데이트

보안 관리

- 도난 방지
  - 지우기 및 잠금
- 보안 구성
  - 암호
  - 인증서
- 제한 설정
  - 디바이스 기능
  - iCloud
  - 미디어 관리

연결 관리

일반 개요

AppTec360 소개

앱텍의 엔터프라이즈 모바일 관리 솔루션은 직관적인 관리 콘솔을 통해 모든 모바일 디바이스를 관리하고 구성할 수 있는 옵션을 제공합니다. 이 시나리오에서는 EMM 서버를 자체 환경에서 실행하거나 클라우드 기반 솔루션을 활용할 수 있습니다.

스마트폰에 기업용 애플리케이션을 중앙에서 설치하는 주제에 대해서도 제대로 찾아 오셨습니다. Enterprise Mobile Manager를 사용하면 몇 초 안에 기업 애플리케이션과 문서를 디바이스에 배포하거나 화이트/블랙리스트를 통해 원치 않는 애플리케이션을 차단할 수 있습니다.

회사에서 개인 디바이스를 사용함에 따라 스마트폰과 태블릿 보안에 새로운 과제가 생겼습니다. 직원들이 스마트폰을 점점 더 많이 사용하기를 원하기 때문에 IT 관리자는 다양한 유형의 디바이스를 보호해야 합니다. 모든 장치와 장치에 저장된 중요한 데이터를 보호하고 직관적인 콘솔에서 관리할 수 있도록 도와드립니다.

지원되는 장치 운영 체제

AppTec360은 iOS, Android 및 Windows 기기를 지원합니다. 언급된 플랫폼의 기능 용량은 OS마다 다를 수 있다는 점에 유의하세요.

- Apple iOS 11.0 이상*
- Apple macOS 10.11 이상
- 클라우드 버전의 Google Android 4.4 이상** 버전
- 온프레미스 버전의 Google Android 4.1 이상** 버전
- MS Windows 10 이상***(데스크톱-컴퓨터, 노트북 및 태블릿)

**iOS 10 이전 버전의 기기는 Apple에서 등록 프로세스를 대폭 변경하여 등록할 수 없습니다.*

***제조사에서 더 이상 지원하지 않는 버전을 사용하는 장치도 연결 및 구성할 수 있습니다. 특정 Android 버전이 필요한 기능이 있을 수 있습니다. 지원의 경우 제조업체의 공식 지원을 따릅니다. 제조업체에서 더 이상 지원하지 않는 오래된 버전으로 인해 발생하는 문제나 버그의 경우, 당사는 제한된 지원만 제공할 권리가 있습니다.*

****운영체제의 제한으로 인해 홈 버전의 Windows는 지원되지 않습니다. 제조업체에서 계속 지원하는 OS 버전을 사용하는 것이 좋습니다. 호환성뿐만 아니라 보안상의 이유도 있습니다. 따라서 iOS 12 이상 및 Android 9 이상을 권장합니다.*

지원되는 LDAP 디렉토리

- Microsoft Active Directory
- LDAP 열기

'지원되는 디바이스 운영 체제' 및 '지원되는 LDAP 디렉터리'에 대한 최신 정보는 여기에서 확인할 수 있습니다:

https://www.apptec360.com/products/systemrequirements/

Apple 디바이스의 '감독 모드'에 대한 설명

감독 모드는 iOS 디바이스를 위한 확장된 인터페이스를 나타냅니다.

각각 구성된 디바이스에서는 최종 사용자 디바이스의 기능과 관련된 추가 제한 사항이 적용될 수 있습니다. 이러한 내용은 관리 핸드북에도 포함되어 있으며 배너로 표시되어 있습니다.

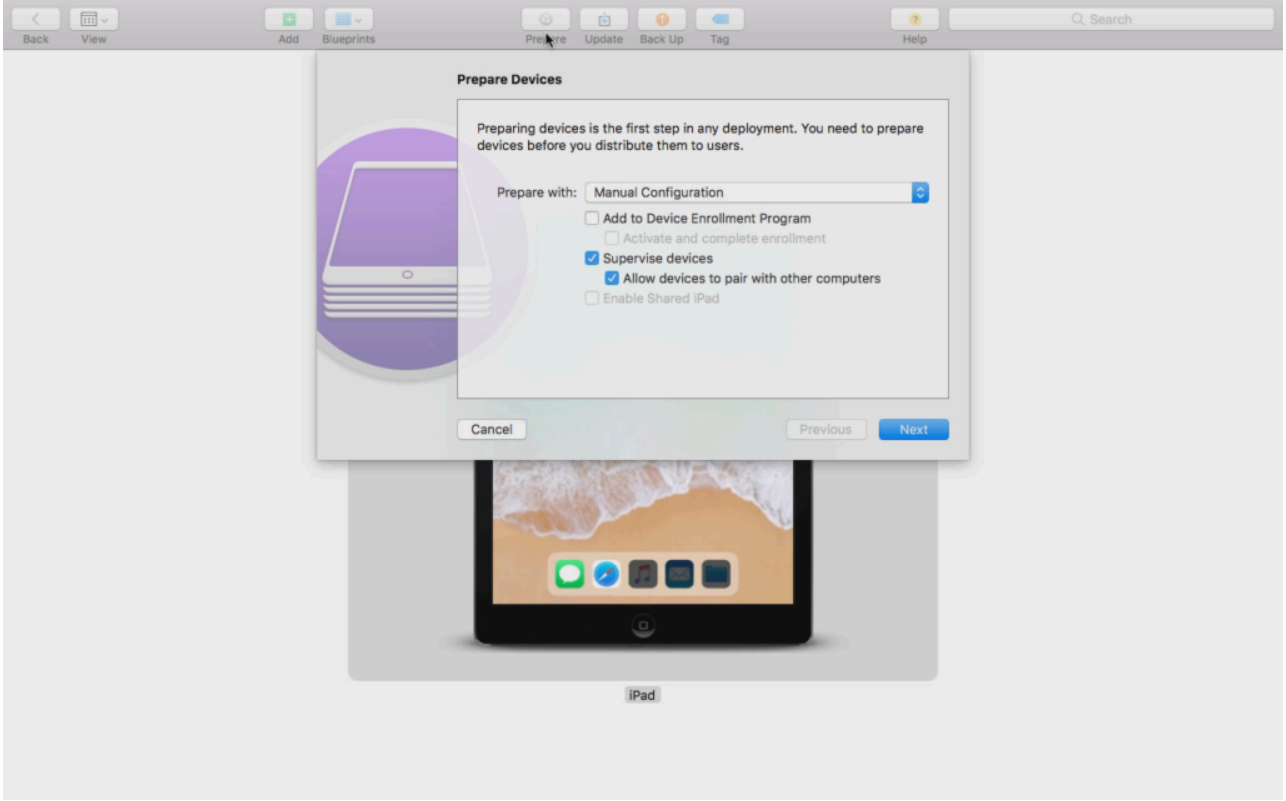
감독 모드에서 사용 가능

'감독 모드'는 'Apple 구성 관리자' 프로그램을 사용하여 활성화할 수 있습니다. Apple 구성 도구는 USB 인터페이스를 통해 새 iOS 디바이스에서 기본 설정을 설정할 수 있는 구성 도구입니다.

이 도구는 구성 프로필뿐만 아니라 앱도 설치할 수 있습니다. 무료이지만 Mac 컴퓨터가 필요합니다.

감독 모드 활성화

1. Apple 구성 관리자 열기



2. 장치를 클릭하고 "준비"를 선택합니다.
3. "수동 구성" 및 "장치 감독"을 선택합니다.
4. "다음"을 클릭합니다.
5. (선택 사항) 이제 장치를 등록할 MDM 서버를 추가할 수 있습니다. 이에 대한 링크는 "일반 설정 - iOS 구성 - 구성자 및 URL"에서 찾을 수 있습니다. 조직을 선택하거나 새 조직을 만듭니다.
6. 조직을 선택하거나 새 조직 만들기
7. 초기 설정에서 건너뛸 단계를 선택하고 "다음"을 클릭합니다(주의: 계속 진행하면 디바이스가 삭제됩니다!).

이제 디바이스가 감독 모드로 전환됩니다. 이 작업에는 몇 분 정도 걸릴 수 있습니다. 완료되면 장치가 재부팅됩니다.

이제 디바이스가 감독됩니다!

DEP에 장치 추가하기

디바이스가 iOS 11 이상 버전인 경우 Apple Configurator를 사용하여 DEP(디바이스 등록 프로그램)에 디바이스를 추가할 수도 있습니다.

DEP에 대한 자세한 정보: https://www.apple.com/business/dep/

장치를 감독할 때와 동일한 단계를 따르고 '장치 등록 프로그램에 추가'를 추가로 확인합니다. 이전에 Apple Configurator로 DEP에 로그인한 적이 없는 경우 DEP 로그인 데이터를 입력하라는 메시지가 표시됩니다.

프로세스가 완료되면 DEP 서버의 "Apple Configurator 2에 의해 추가된 장치"에서 장치를 찾을 수 있습니다. 이제 이 서버를 사용하여 관리 콘솔에 연결하거나 이미 존재하는 서버로 장치를 전송할 수 있습니다.

이제 DEP에 장치를 성공적으로 추가했습니다!

안드로이드 엔터프라이즈에 대한 설명

Android Enterprise란 무엇인가요?

Android Enterprise는 MDM으로 관리되는 업무용 기기를 더욱 효과적으로 제어할 수 있습니다. 이를 통해 관리자는 안드로이드 기기를 완전히 제어하거나 회사 데이터와 컨테이너 기기의 개인 데이터를 분리할 수 있습니다. 또한 Android Enterprise를 사용하면 디바이스를 더 쉽게 등록하고 앱을 쉽게 배포할 수 있습니다.

Android Enterprise를 사용하기 위한 요구 사항은 무엇인가요?

Android Enterprise는 누구나 무료로 사용할 수 있습니다. 모든 Android Enterprise 기능을 사용하려면 Google 계정을 MDM에 연결하기만 하면 됩니다. 이에 대한 자세한 내용은 Android Enterprise 섹션에서 확인할 수 있습니다.

안드로이드 엔터프라이즈는 향상된 업무 프로필(아래 참조)을 제외하고 안드로이드 5.1 이상의 기기에서 사용할 수 있습니다. 보다 쉽게 등록하려면 Android 7 이상, 사용 가능한 모든 기능을 사용하려면 Android 11 이상을 권장합니다.

Android Enterprise에서 사용할 수 있는 모드는 무엇인가요?

Android Enterprise를 사용할 때 사용할 수 있는 3가지 모드가 있습니다.

AE 완전 관리형 디바이스(업무용 관리형): 업무용으로만 사용되는 완전 관리형 장치입니다. 이 경우 관리자가 디바이스를 완전히 제어할 수 있습니다. 이 모드에서는 디바이스를 개인적으로 사용할 수 없습니다. 이 모드에서 디바이스를 등록하려면 디바이스를 재설정하고 QR 코드를 사용하여 등록하거나(AE 등록 참조) Knox 등록 또는 제로 터치를 통해 등록해야 합니다.

AE BYOD 컨테이너: BYOD(개인 기기 가져오기) 컨테이너를 사용하면 사용자가 별도의 컨테이너에서 개인 휴대폰으로 회사 데이터에 액세스할 수 있습니다. 이 모드에서는 개인 앱이 회사 데이터와 앱을 볼 수 없으며 그 반대의 경우도 마찬가지입니다. 이 모드에서 디바이스를 등록하려면 AppTec 앱을 다운로드하고 QR 코드를 스캔해야 합니다. 콘솔에서 디바이스를 생성하고 디바이스 유형으로 "AE 컨테이너(BYOD & Enahnced Work Profile)"를 선택합니다. 새로 생성된 디바이스에서 QR 코드를 클릭하여 QR 코드를 가져와 첫 번째 스위치를 "레거시 및 BYOD"로 설정합니다.

AE 향상된 업무 프로필: (Android 11 이상 필요) 위에서 언급한 BYOD 컨테이너는 개인 디바이스에 회사 데이터를 가져오지만, 향상된 업무 프로필은 회사 소유 디바이스에 대해 동일한 작업을 수행합니다. 동일한 컨테이너를 만들지만 관리자에게 디바이스에 대한 제어 권한이 조금 더 부여되므로 사용자가 단순히 디바이스에서 MDM을 제거할 수 없습니다. 콘솔에서 디바이스를 만들고 디바이스 유형으로 'AE 컨테이너(BYOD 및 Enahnced Work Profile)'를 선택합니다. 새로 생성된 디바이스에서 QR 코드를 클릭하여 QR 코드를 가져와 첫 번째 스위치를 '향상된 업무 프로필'로 설정합니다. 이 QR 코드는 AE 등록의 방법 1에 설명된 대로 장치를 재설정하고 화면을 6번 탭한 후 스캔할 수 있습니다.

Android Enterprise 기기에 앱을 할당하려면 어떻게 해야 하나요?

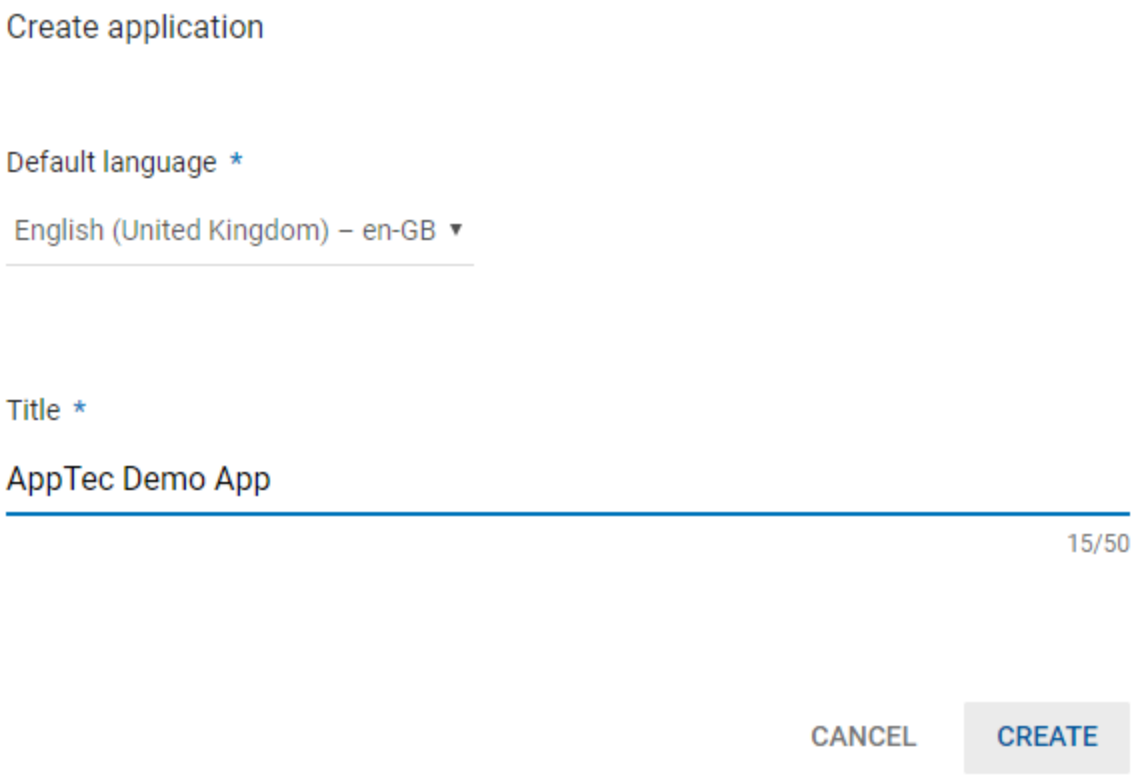
먼저 일반 설정 → 앱 관리 → AE Play 스토어 → Play 스토어 앱에서 사용하려는 앱을 승인해야 합니다. 앱을 승인한 후 '+'를 클릭하고 'AE Play 스토어' 탭에서 앱을 선택하면 프로필의 필수 앱 목록 →에 앱을 지정할 수 있습니다. 그러면 앱이 자동으로 다운로드되고 설치됩니다. 기기에 Google 계정이 필요하지 않으며 사용자가 이를 확인하거나 허용할 필요가 없습니다.

Google Play 스토어에 나만의 앱 업로드하기

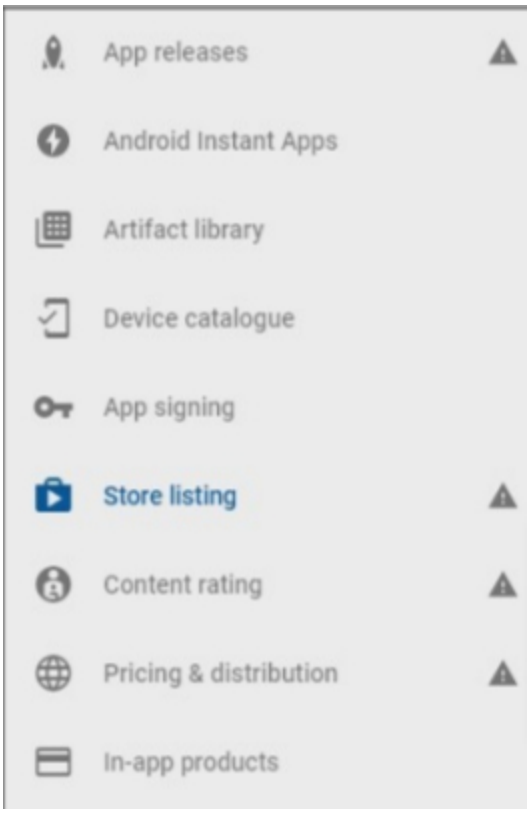
사내 앱을 Google Play 스토어에 업로드할 수 있습니다. 이렇게 하면 Play 스토어의 업데이트 메커니즘과 같은 다양한 이점을 활용할 수 있습니다.

이렇게 하려면 Google 개발자 계정이 필요합니다. Google Play 콘솔(https://play.google.com/apps/publish)을 사용하여 로그인합니다.

"애플리케이션 만들기"를 클릭합니다. 기본 언어와 앱의 제목을 선택합니다.



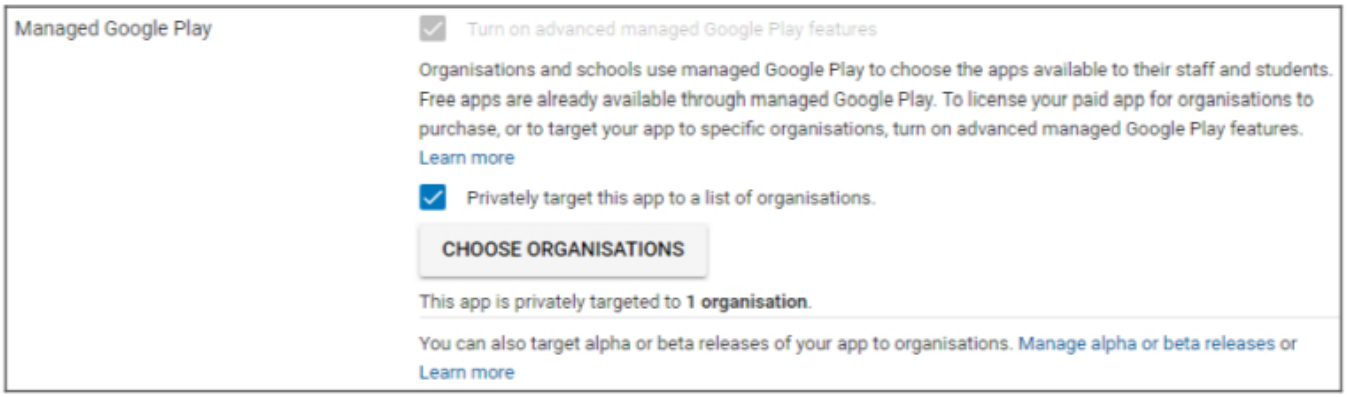
다음 페이지에서 앱에 대한 다양한 세부 정보를 입력하라는 메시지가 표시됩니다.



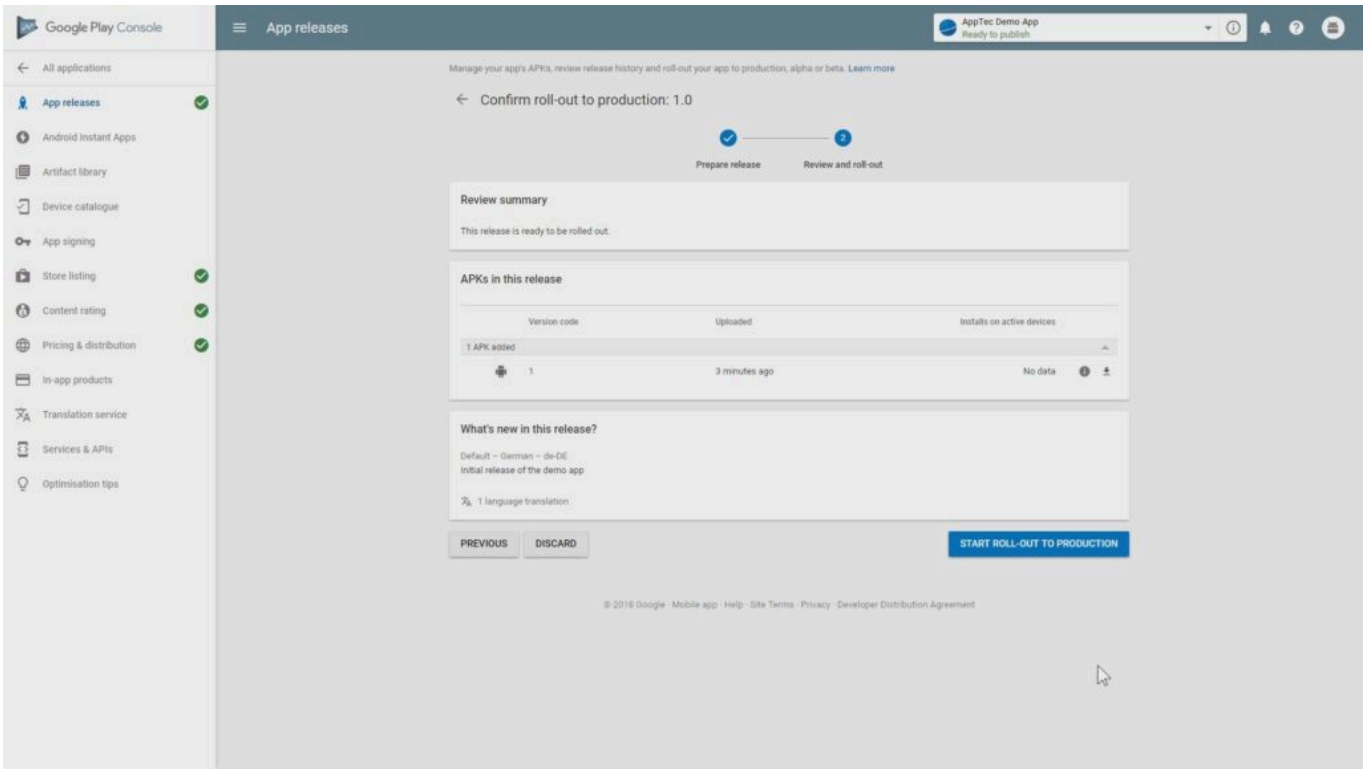
모든 세부 정보를 입력하면 왼쪽에 다양한 힌트 기호가 표시됩니다.

마우스를 가져가서 남은 단계를 확인하고 원하는 순서대로 따라하세요.

참고: '가격 및 배포' 아래의 '관리되는 Google Play'에서 두 개의 확인란을 선택해야 합니다. 그렇지 않으면 앱이 공개되어 모든 사람이 액세스할 수 있습니다. 또한 배포할 국가를 선택해야 합니다.



모든 단계를 완료했으면 "앱 릴리스"로 이동합니다. "검토" 및 "프로덕션에 롤아웃 시작"을 클릭하여 초안을 마무리하고 앱을 게시합니다.



Play 스토어에서 앱을 사용할 수 있을 때까지 시간이 다소 걸릴 수 있습니다. 프로세스가 완료되면 Play for Work 스토어에서 앱을 검색하고 승인할 수 있습니다. 그 후에는 다른 앱과 마찬가지로 EMM 콘솔을 사용하여 앱을 디바이스에 간단히 할당할 수 있습니다.

요구 사항 및 설치

요구 사항

시스템 요구 사항

가상 어플라이언스는 개방형 가상화 형식(VMWare, VirtualBox, Citrix Xen Server)과 압축된 .vhdx(Hyper-V) 파일*로 사용할 수 있습니다.

*참고: Hyper-V를 사용할 때는 1세대로 머신을 만들어야 합니다.

가상 디스크의 목표 크기는 20GB이고 컴퓨터에는 4GB의 RAM이 필요합니다.

어플라이언스는 Debian 9 64비트 기반입니다.

가져온 머신을 최신 호환성(예: VMWare)으로 업그레이드하고 하이퍼바이저에서 머신 OS 유형이 올바르게 설정되어 있는지 확인합니다.

라이선스 키

서버를 성공적으로 활성화하고 설치하려면 유효한 라이선스 파일이 필요합니다. AppTec360에서 직접 또는 각 리셀러로부터 라이선스 파일을 받을 수 있습니다.

IP 주소 및 DNS 확인

라이선스가 발급된 호스트 이름을 사용하여 기기에서 AppTec360 어플라이언스에 연결할 수 있어야 합니다.

Windows 10 디바이스를 등록하려면 어플라이언스를 가리키는 "엔터프라이즈 등록." 형식의 추가 하위 도메인을 설정해야 합니다.

SSL 인증서

장치와의 모든 연결은 SSL을 사용하여 보호되어야 하므로 장치에서 신뢰할 수 있는 인증 기관에서 발급한 호스트 이름에 대한 유효한 인증서가 필요합니다. 인증서의 개인 키는 비밀번호 보호 없이 업로드해야 합니다. 대부분의 경우 장치에서 서버 인증서를 인식하려면 CA에 대한 중간 인증서가 필요합니다.

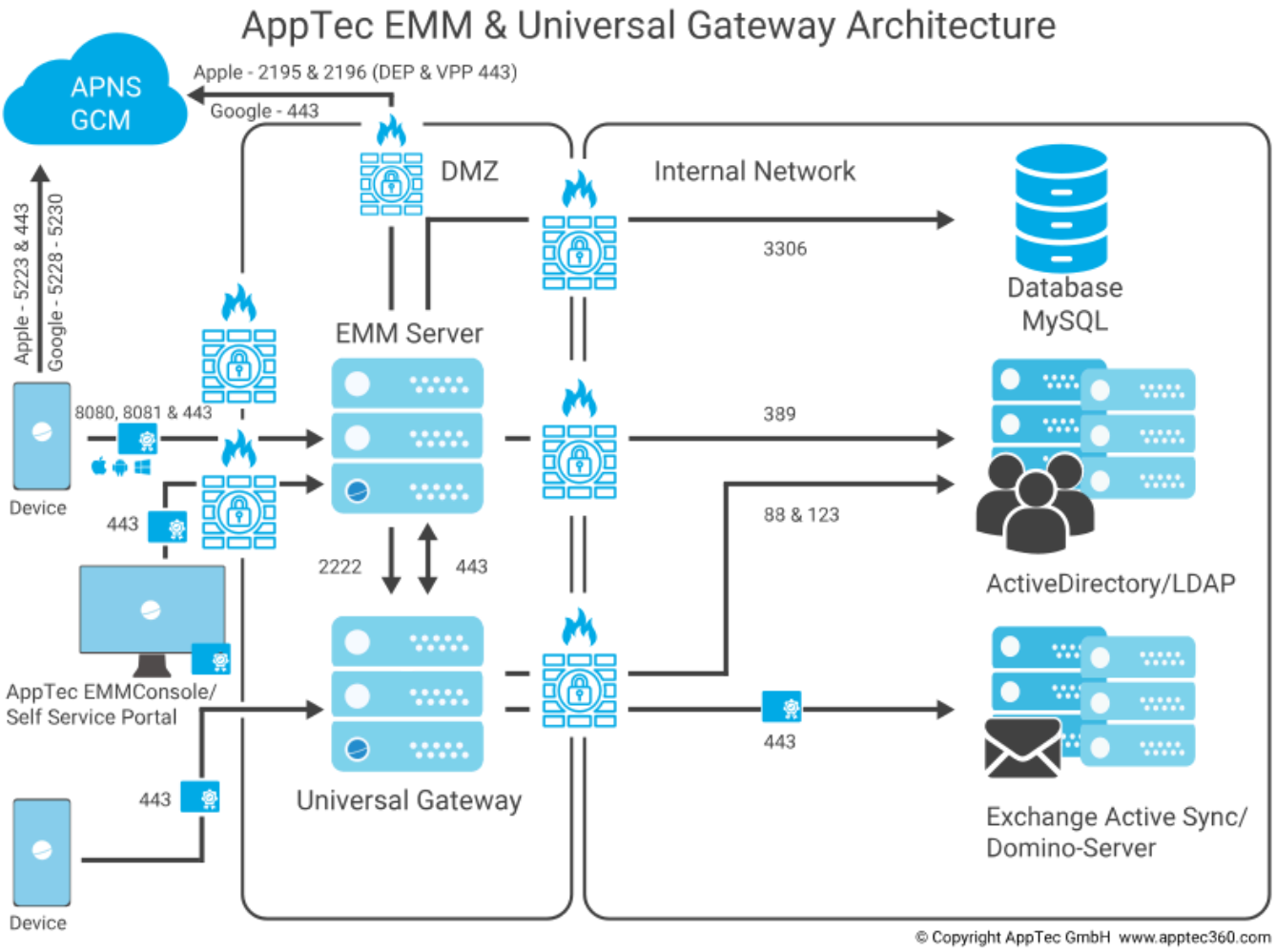
Windows 10 디바이스에는 기업 등록 하위 도메인에 대한 특정 인증서가 필요합니다.

어플라이언스 버전 202104부터는 자동으로 생성되는 Let's Encrypt 인증서를 사용할 수도 있습니다(2단계 - SSL 인증서에 설명되어 있음).

SMTP 서버

AppTec360 EMM이 이메일을 보낼 수 있도록 이메일 서버 및/또는 이메일 릴레이가 필요합니다(예: 기기 등록 및 계정 유효성 검사).

방화벽 규칙



이 다이어그램은 사용하려는 서비스에 따라 어떤 연결이 필요한지 보여줍니다.

자세한 설명은 다음 페이지의 표를 참조하세요.

모두(외부/장치)	→	**AppTec360 어플라이언스 / emmconsole.com**
포트	443	관리, 엔터프라이즈 앱스토어 및 Windows Phone 통신
	8080	Android 및 iOS 커뮤니케이션
	80	Let´s Encrypt를 처음 설정합니다. 이후에는 443을 사용합니다.
모두(디바이스)	→	**모두(외부)**
포트	5223, 443	Apple 푸시 서비스, 프록시 없이 연결 가능해야 함, 443을 폴백으로 참조(https://support.apple.com/en-us/HT203609)
	5228-5230	Android 푸시 서비스(FCM), 프록시 없이 연결 가능해야 함
AppTec360 어플라이언스	→	**도메인 컨트롤러**
포트	389, (ldaps 636)	LDAP와 사용자 동기화
AppTec360 어플라이언스	→	**모든**
포트	443	안드로이드 푸시 서비스(GCM)에 사용됩니다. 앱스토어 / 플레이스토어 검색
AppTec360 어플라이언스	→	**emmconsole.com**
포트	443	AppTec360 어플라이언스 업데이트, APNS 인증서 생성
AppTec360 어플라이언스	→	**Apple 네트워크 (17.0.0.0/8)**
포트	2195, 2196	Apple 푸시 서비스 및 피드백 서비스
	443	DEP & VPP

보안 업데이트

최신 보안 수정 사항을 적용하려면 Debian 운영 체제를 정기적으로 업데이트해야 합니다. 그러나 최신 주요 버전의 Debian으로 수동으로 업그레이드하지 않도록 주의하세요. AppTec360 EMM이 최신 주요 버전과 호환되면 어플라이언스 업데이트에서 업그레이드할 수 있는 방법을 추가할 예정입니다.

가상 어플라이언스의 기본 비밀번호

로그인 사용자(루트 로그인이 비활성화됩니다. 관리 작업에는 "sudo" 사용)

앱텍

로그인 비밀번호

앱텍

MySQL 루트 사용자

root

MySQL 루트 비밀번호

앱텍

MySQL 기본 사용자

AppTec

MySQL 기본 사용자 비밀번호

AppTec

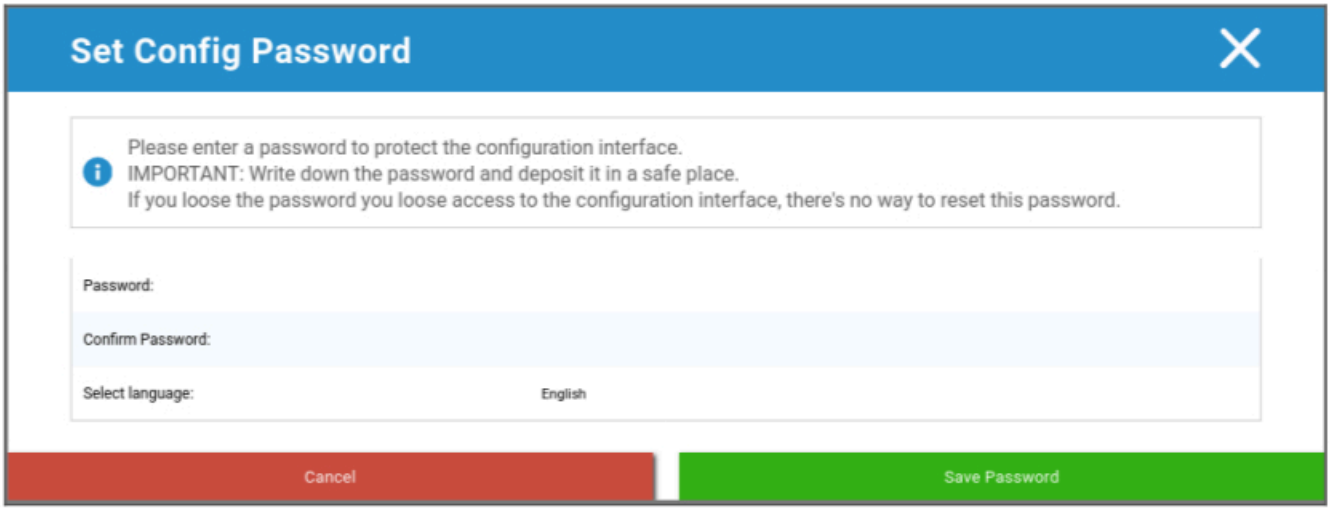
가상 어플라이언스 구성

중요: 가상 기기 구성을 시작하기 전에 디스플레이 해상도를 최소 1280 x 800픽셀로 설정해야 합니다.

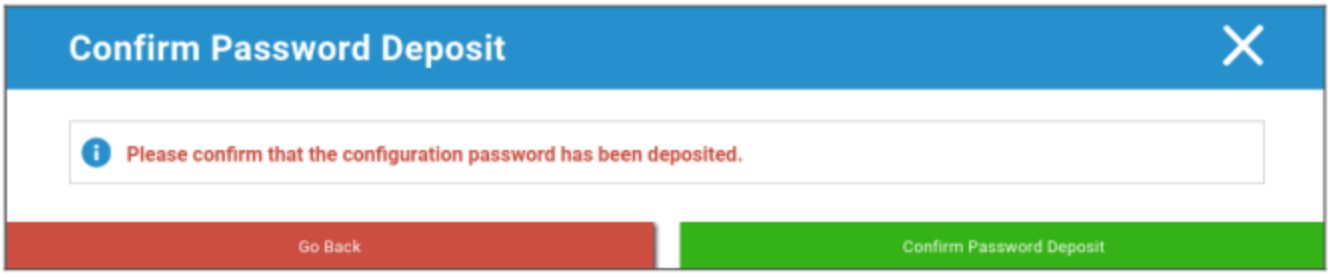
어플라이언스에 로그인하면 Firefox가 자동으로 시작되고 구성 인터페이스가 표시됩니다.

준비

먼저 구성 인터페이스의 비밀번호를 입력해야 합니다. 이 비밀번호는 구성 인터페이스에 입력한 모든 정보와 파일을 암호화하는 데 사용됩니다. 여기에서 인터페이스가 표시될 언어를 설정할 수도 있습니다(나중에 변경 가능).

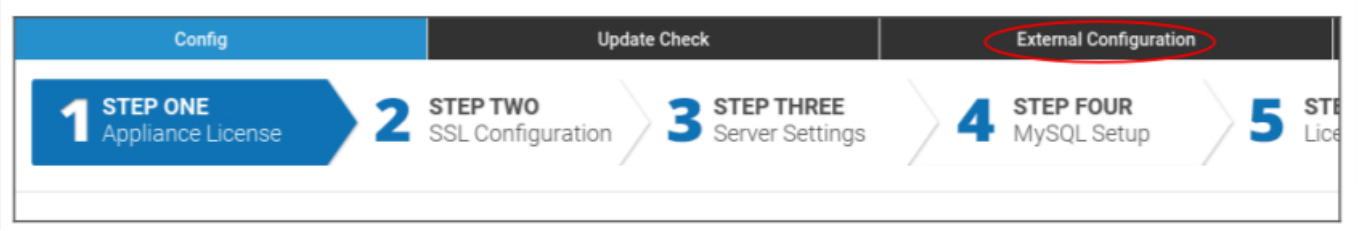


비밀번호는 앱테크360 지원팀에서만 재설정할 수 있으므로 안전한 곳에 비밀번호를 보관하고 곧 있을 팝업을 확인하세요.



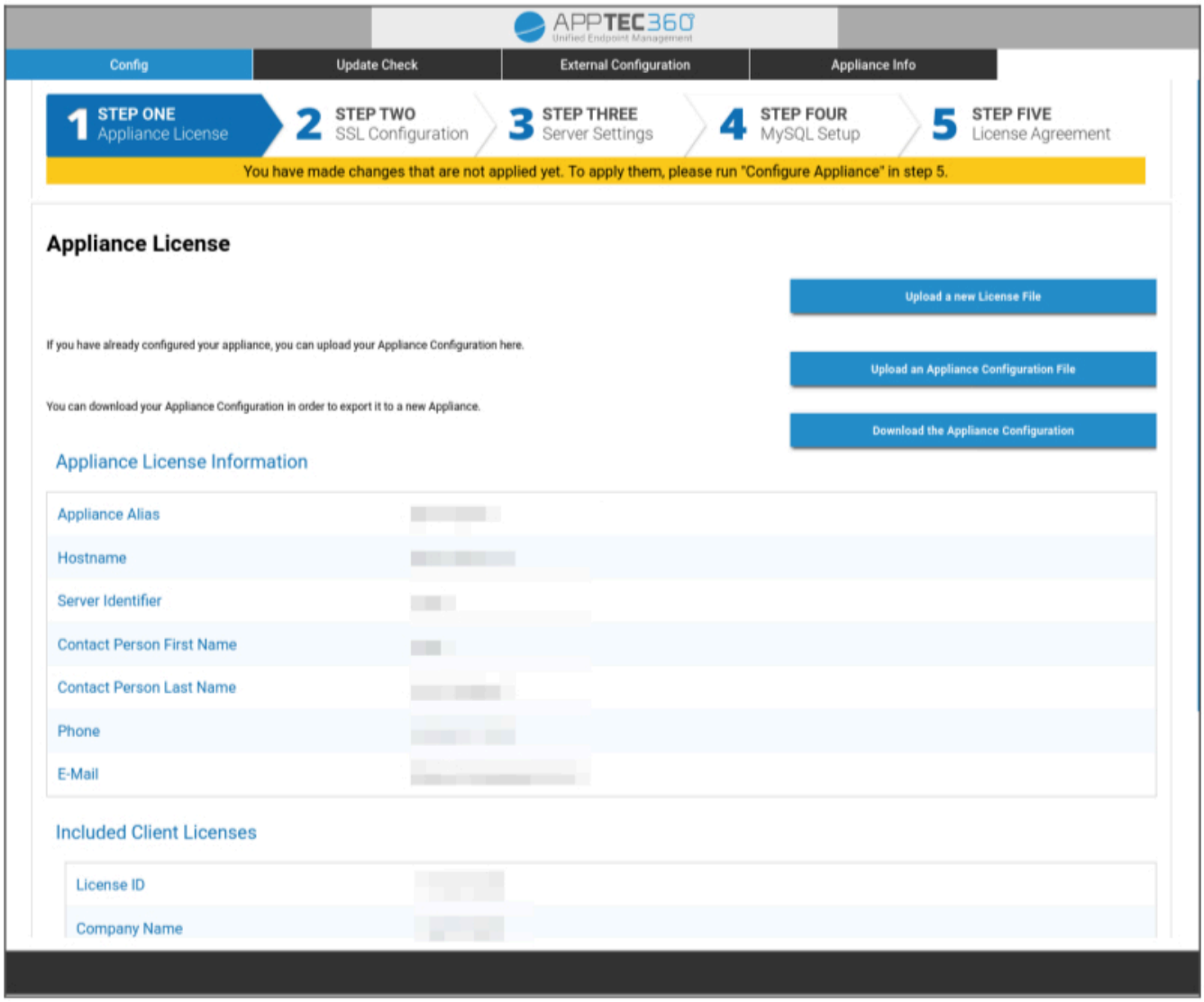
외부 호스트에서 구성

설정 프로세스를 간소화하기 위해 원격에서 구성 페이지에 액세스할 수 있도록 설정할 수 있습니다. 이렇게 하려면 '외부 호스트에서 구성하기'의 단계를 따르세요.



1단계 – 어플라이언스 라이선스

1. 앱테크에서 받은 라이선스 파일을 업로드하세요.
2. 라이선스 파일이 성공적으로 업로드되면 아래 스크린샷과 같이 어플라이언스 라이선스 정보를 확인할 수 있습니다.



2단계 – SSL 인증서

암호화하자를 사용하여 자동 인증서 설정을 사용하거나 직접 인증서를 제공할 수 있습니다(자세한 내용은 SSL-인증서 참조).

자동

인증서는 암호화하자 서비스를 사용하여 자동으로 생성됩니다.

AppTec360 EMM은 도메인 유효성 검사에 HTTP-01 챌린지를 사용하므로 인증서를 처음 요청할 때 인터넷에서 HTTP 포트가 열려 있어야 합니다. 이후 갱신 요청은 HTTPS를 통해 유효성을 검사할 수 있습니다.

라디오 버튼을 "자동(암호화하자)"로 전환하고 "값 저장"을 누릅니다. 5단계 - 라이선스 계약에서 구성을 적용할 때 인증서가 자동으로 요청됩니다. 필요한 경우 인증서가 자동으로 갱신되며, 인증서가 곧 만료될 경우(갱신에 실패했을 수 있음을 의미함) 이메일을 받게 됩니다.

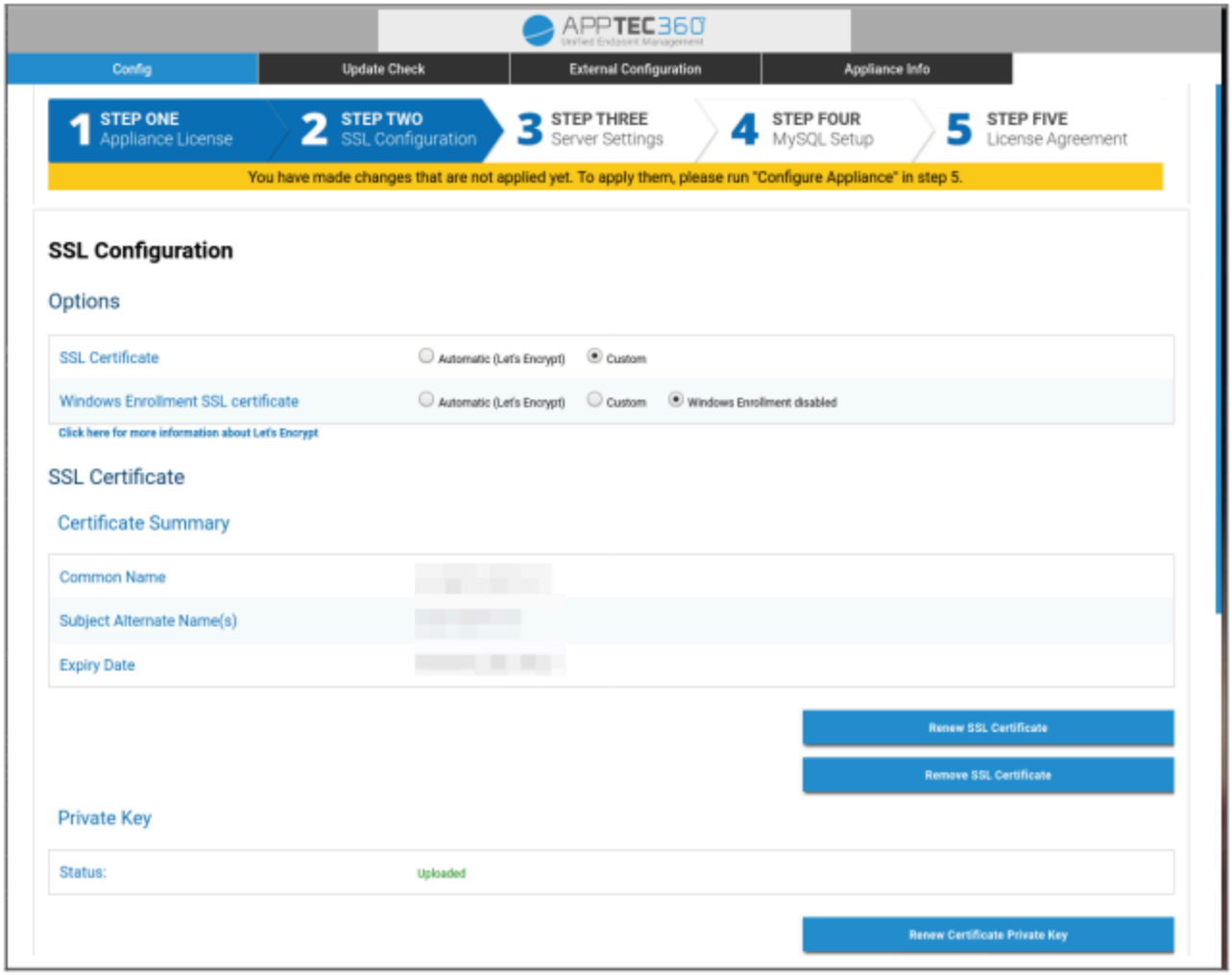
사용자 지정

1. 라이센스가 부여된 호스트 이름에 대한 SSL 인증서를 업로드합니다. 호스트 이름은 1단계 - 어플라이언스 라이선스에서 확인할 수 있습니다.

2. 인증서의 개인 키와 필요한 경우 중간 인증서도 업로드하세요.

중요: 키는 비밀번호로 보호되어 있지 않아야 합니다. 비밀번호로 보호되어 있는 경우 업로드하기 전에 비밀번호를 제거하세요.

힌트: Windows 10 디바이스도 사용하려면 'Windows 등록 SSL 인증서'를 사용 설정하고 페이지 하단의 하위 도메인용 인증서, 비공개 키 및 중간 인증서(IP 주소 및 DNS 확인에 설명되어 있음)를 업로드해야 합니다.



3단계 – 서버 설정

1. 글로벌 지원 이메일 주소를 입력하세요. 이 주소는 사용자에게 보내는 이메일에 사용되므로 사용자는 장치와 관련된 문제가 발생할 경우 누구에게 연락해야 하는지 알 수 있습니다.

2. 시스템에서 이메일을 보낼 때 사용할 이메일 설정을 입력합니다. 이 설정은 사용자에게 이메일을 보내고 버그 보고서 및 기능 요청을"support@apptec360.com"로 보내는 데 사용됩니다. 이메일 설정을 저장한 후에는 '이메일 설정 테스트'를 클릭하고 안내에 따라 설정을 확인해야 합니다.

4단계 – MySQL 설정

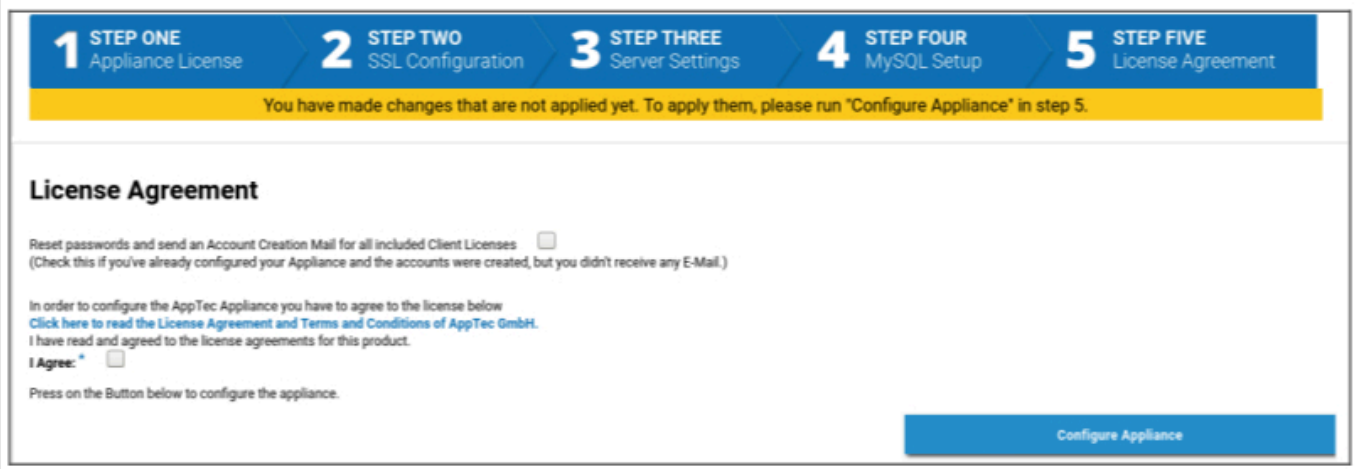
1. 내부 데이터베이스를 사용하려는 경우 이 단계를 건너뛸 수 있습니다. 그렇지 않으면 외부 데이터베이스 서버에 대한 연결 정보를 입력할 수 있습니다.


1 STEP ONE
Appliance License
2 STEP TWO
SSL Configuration
3 STEP THREE
Server Settings
4 STEP FOUR
MySQL Setup
5 STEP FIVE
License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

5단계 – 라이선스 계약

1. 라이선스 계약서를 읽어주세요.
2. "동의함"에 체크하고 "어플라이언스 구성" 버튼을 눌러 설정을 적용합니다.

힌트: 설정을 적용하려면 5단계에서 설정을 변경할 때마다 '어플라이언스 구성'을 실행해야 합니다.



축하합니다!

가상 어플라이언스의 구성을 완료했습니다.

라이선스에 대해 제공한 주소로 비밀번호가 포함된 이메일이 전송되었습니다(1단계 - 어플라이언스 라이선스의 '포함된 클라이언트 라이선스'에 표시됨).

이제 이 비밀번호와 비밀번호를 받은 이메일 주소를 사용하여 콘솔에 로그인할 수 있습니다.

콘솔에 로그인하려면 브라우저의 주소창에 콘솔의 호스트 이름을 입력하세요.

어플라이언스의 호스트 이름은 1단계 - 어플라이언스 라이선스에서 찾을 수 있습니다.

문제 해결

1. 5단계 - 라이선스 계약에서 어플라이언스를 구성할 때 이메일을 받지 못했습니다:

3단계 - 서버 설정의 이메일 설정이 올바른지 확인합니다. 비밀번호를 다시 보내려면 5단계 - 라이선스 계약에서 "포함된 모든 클라이언트 라이선스에 대한 비밀번호 재설정 및 계정 생성 메일 보내기"를 확인한 후 "어플라이언스 구성"을 다시 실행하세요.

2. 5단계 - 라이선스 계약에서 구성하는 동안 암호화 사용과 관련된 오류가 발생했습니다:

포트 80에서 해당 도메인 이름으로 어플라이언스에 연결할 수 있는지 확인하세요. 추가 문제 해결에 도움이 될 수 있도록 "/var/log/letsencrypt"에 로그도 암호화하여 기록해 보겠습니다.

보안 권장 사항

AppTec360 어플라이언스를 보호하려면 다음 단계를 수행하는 것이 좋습니다.

이는 전체 지침이 아니라 기본 구성에 대한 권장 사항일 뿐입니다.

- AppTec360 사용자의 비밀번호 변경
- MySQL 사용자 "root"와 "AppTec"의 비밀번호를 변경하고 그에 따라 4단계 - MySQL 설정을 업데이트합니다.
- 기본 SSH 서버 포트 변경
- 콘솔에서 포트 80을 차단하고 들어오는 HTTP 트래픽을 허용하지 않고 HTTPS만 사용하세요. 설정이 완료되면 HTTPS를 통한 외부 구성도 가능합니다.
- 3단계 - 서버 설정의 맨 아래에서 관리 인터페이스에 대한 액세스를 특정 IP로만 제한합니다.
- 방화벽 구성

일반 설정

계정 개요

계정 정보

개요

여기에서 AppTec360 계정의 개요를 확인할 수 있습니다.

회사 이름	회사 이름
생성 날짜	계정 생성 날짜
라이선스 유형	유료 = 유료 라이선스 무료 = 무료 라이선스 참고: 온프레미스 어플라이언스의 계정은 기술적인 이유로 항상 유료로 표시됩니다.
클라이언트 식별자	계정 식별자(고객 번호가 아님)
라이선스 만료일	AppTec360 라이선스 만료일
ContentBox 라이선스	무료 = 25개 장치에 대한 무료 라이선스 유료 = x 디바이스용 유료 라이선스
런처	Android용 사용자 지정 런처를 사용할 수 있는지 여부를 표시합니다.
디바이스	현재 사용 중인 라이선스 수/총 라이선스 수
담당자	제공된 담당자
전화	전화번호 제공
이메일*	제공된 이메일 주소
루트 사용자	로그인할 수 있는 루트 사용자
소프트웨어 버전	현재 소프트웨어 버전

**참고: 여기에 표시된 이메일 주소는 계정을 등록할 때 입력한 이메일 주소입니다. 이를 기반으로 사용자/장치 트리에 사용자가 생성되며 수정할 수 있습니다. 이 사용자를 수정하면 로그인에 사용해야 하는 이메일 주소는 변경되지만 계정 개요의 정보는 변경되지 않습니다. .*

버그 보고

버그 보고서는 문제나 버그를 보고하기 위해 지원팀에 직접 보낼 수 있으며 계정 및 설정에 대한 정보와 로그를 포함합니다.

제목	버그 보고서의 제목입니다. 기존 지원 티켓에 추가하려면 티켓 번호를 포함하세요.
예상되는 동작	수행한 작업과 예상되는 결과를 자세히 설명하세요.
실제 행동	정확히 어떤 일이 발생했는지 자세히 설명하세요. 오류 메시지를 정확히 인용하세요. 첨부 파일에 스크린샷을 추가하면 도움이 됩니다.
언제 이 문제가 발생했나요?	구체적인 오류 메시지/문제가 발생한 정확한 시간을 알려주세요. 최상의 경우 초도 포함(예: 18:55:27)
문제를 재현할 수 있나요? 그렇다면 어떻게(자세히) 재현할 수 있나요?	문제를 재현할 수 있는 방법을 자세히 설명하세요.
이 기능이 이전에 예상대로 작동했나요? 그렇다면 언제까지 작동했나요?	모르는 경우 비워 두세요.
이 문제가 발생하기 전에 시스템에 특정한 변경 사항이 있었나요? 그렇다면 어떤 변경 사항(세부 사항)이 있었나요?	관련이 없다고 생각되더라도 문제가 발생하기 전에 마지막으로 변경한 사항이나 조치가 무엇인지 항상 언급하세요.
해당되는 경우: 어떤 기기 모델과 OS 버전이 영향을 받나요?	항상 정확한 OS 버전(예: iOS 14.7.1 또는 Android 11)을 입력하세요.
해당되는 경우: 기기의 공인 IP 주소 또는 일련번호는 무엇인가요?	모든 디바이스가 영향을 받더라도 하나 이상의 이름을 지정하세요.
로그 파일 포함	버그 보고서와 함께 로그파일을 보내려면 이 옵션을 선택합니다. 이렇게 하는 것이 좋습니다.
Apple에서 현재 VPP 상태를 가져와 버그 리포트에 포함하기	VPP 라이선스 할당에 대한 정보를 포함합니다. 지원팀에서 요청을 받거나 문제가 VPP와 관련된 경우에만 활성화하세요.
첨부 파일	유용할 수 있는 파일(예: 오류 메시지의 스크린샷)을 첨부합니다.

기능 요청

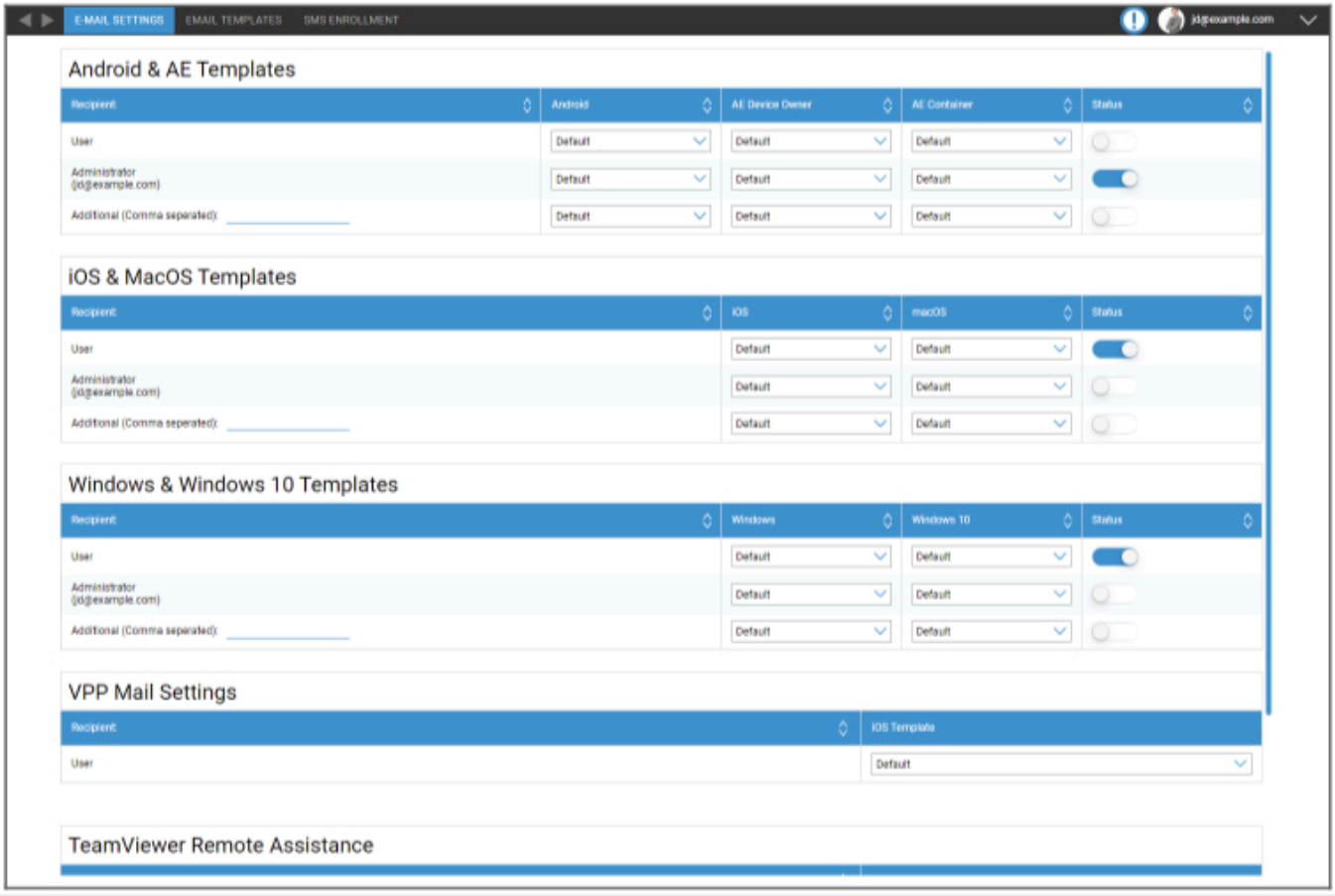
기능 요청은 지원팀에 직접 보낼 수 있습니다. 여기에는 특정 기능에 대한 요청이나 다음에 대한 개선 요청이 포함될 수 있습니다.

요약	문제에 대한 간단한 개요
설명	문제에 대한 자세한 설명, 가능한 한 구체적으로 작성해 주세요.
첨부 파일	버그 리포트에 파일 첨부하기

글로벌 구성

이메일 설정

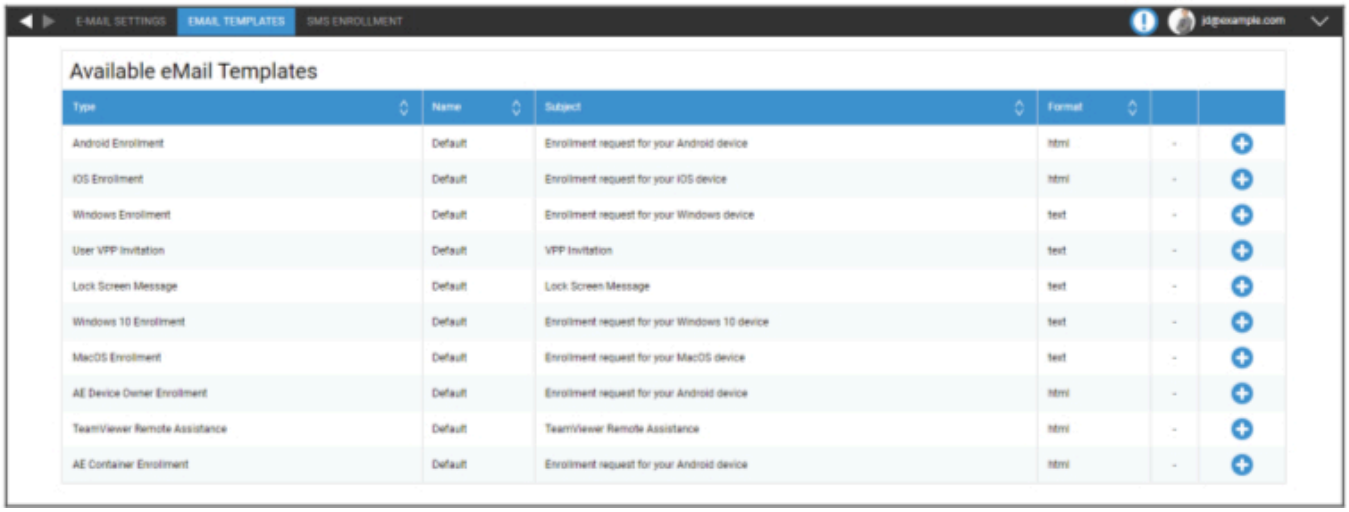
여기에서 등록 요청이 생성될 때 메일을 받을 대상과 해당 메일에 사용되는 텍스트 템플릿을 정의할 수 있습니다.



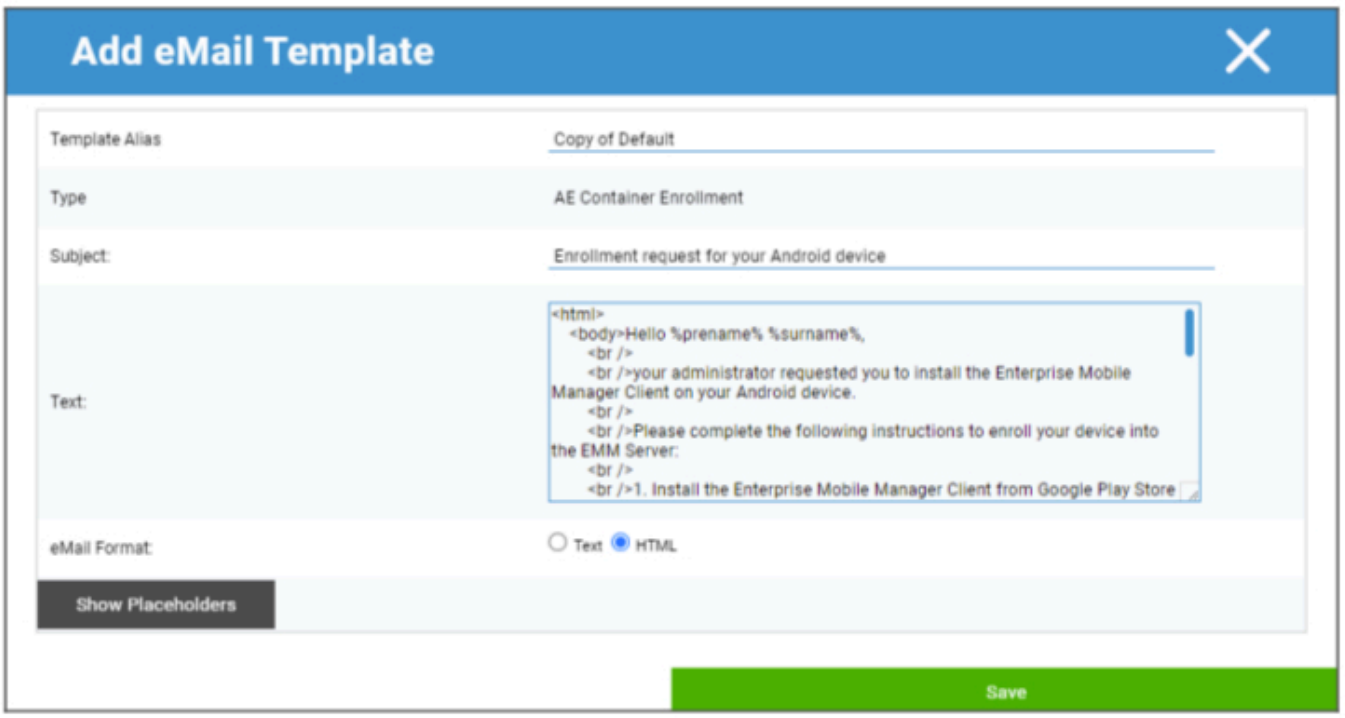
이메일 템플릿

여기에서 다양한 시나리오에 맞는 템플릿을 생성하고 편집할 수 있습니다. 템플릿은 일반 텍스트 형식 또는 HTML 형식이 될 수 있습니다. HTML을 사용하면 텍스트 서식을 더 잘 제어할 수 있습니다.

기본 템플릿은 편집하거나 지울 수 없습니다.



플레이스홀더를 자동으로 대체되는 변수로 사용할 수도 있습니다. 편집하는 동안 '플레이스홀더 표시'를 클릭하면 사용 가능한 플레이스홀더를 볼 수 있습니다. 카테고리마다 플레이스홀더가 다릅니다.



SMS 등록

여기에서 SMS 등록 프로세스를 비활성화/활성화할 수 있습니다.

(기본값: 비활성화됨)

또한 사용 가능한 SMS 크레딧의 수를 나타내는 디스플레이가 표시됩니다.

SMS 크레딧은 별도로 구매해야 합니다.

개인 정보 보호

GPS 액세스

여기에서 모든 디바이스의 GPS 보기를 1개 또는 2개의 비밀번호로 보호할 수 있습니다(네 개의 눈 원칙). 디바이스의 위치에 액세스하려고 할 때마다 비밀번호를 입력하라는 메시지가 표시됩니다.

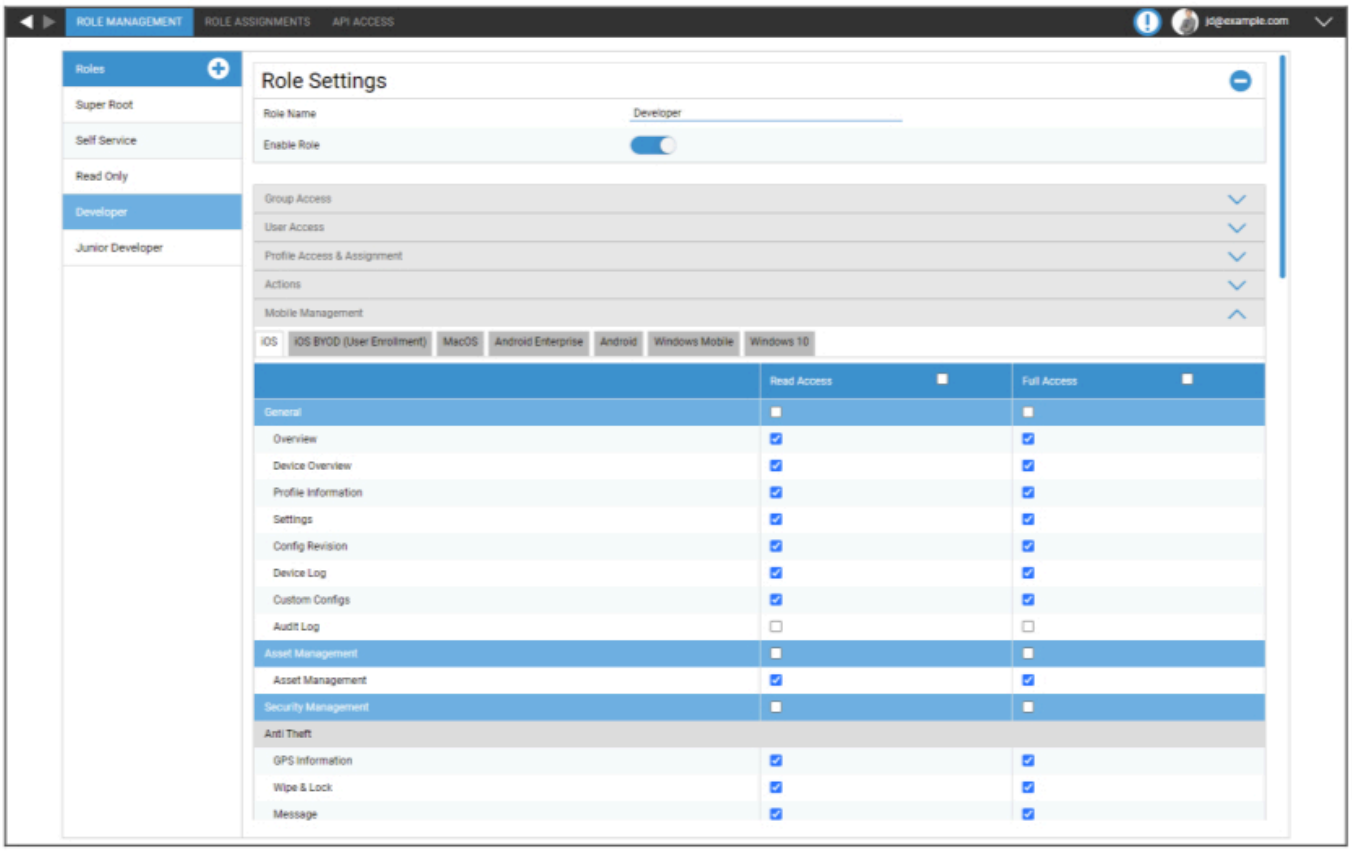
GPS 설정에 대한 액세스 제한	끄기 = 기능이 꺼져 있으며 현지화에 비밀번호가 필요하지 않습니다.
	켜짐 = 기능이 켜져 있고 현지화를 위해 비밀번호가 필요합니다.
보호 방법	하나의 비밀번호 사용 = 현지화에 하나의 비밀번호 사용
	두 개의 비밀번호 사용 = 현지화를 위해 두 개의 비밀번호 사용
비밀번호 입력 (1)	선택한 비밀번호 입력
비밀번호 반복 (1)	선택한 비밀번호 재입력
선택 사항입니다: 비밀번호 입력 2	두 번째로 선택한 비밀번호 입력
선택 사항입니다: 비밀번호 2 반복	두 번째로 선택한 비밀번호 재입력

참고: 비밀번호를 설정한 후 완전히 활성화하려면 비밀번호를 한 번 더 입력해야 합니다.

역할 기반 액세스

역할 관리

역할은 사용자가 관리 콘솔에 로그인할 때 보고 수행할 수 있는 작업을 정의합니다. 이를 통해 로그인은 가능하지만 기능이 제한된 사용자를 만들 수 있습니다.



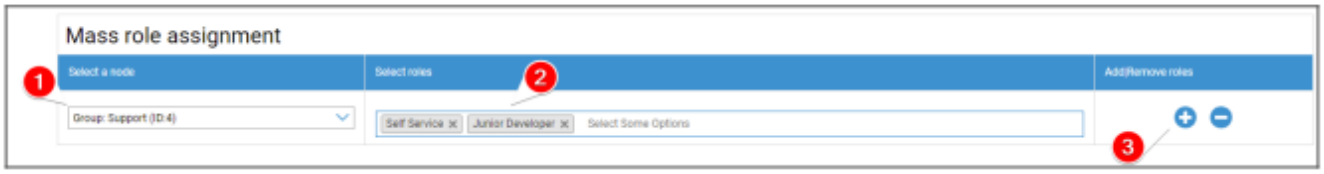
슈퍼 루트 역할은 항상 모든 것을 보고 변경할 수 있는 기본 역할입니다. 변경하거나 삭제할 수 없습니다. 셀프 서비스 역할은 자신의 사용자 및 장치만 볼 수 있습니다. 셀프 서비스와 사용자 지정 역할을 결합하여 사용자가 직접 로그인하고 해당 사용자만 장치를 등록하도록 허용하는 등의 작업을 할 수 있습니다.

사용자 지정 역할은 수동으로 활성화 또는 비활성화할 수 있습니다. 새 역할은 기본적으로 비활성화되어 있습니다. 역할이 비활성화된 사용자는 해당 역할이 없는 것처럼 작업합니다. 이를 통해 특정 역할의 작업을 일시적으로 제한할 수 있습니다.

모든 권한은 '읽기 액세스'와 '전체 액세스'로 나뉩니다. 역할에 읽기 액세스 권한을 부여하면 콘솔의 특정 부분을 볼 수 있습니다. 역할에 전체 액세스 권한을 부여하면 해당 역할이 콘솔의 특정 부분을 보고 변경할 수 있습니다.

역할 할당

여기에서 역할을 가진 모든 사용자에 대한 개요와 해당 사용자가 어떤 역할을 가지고 있는지 확인할 수 있습니다. 여기에서 사용자 또는 전체 그룹에 역할을 할당할 수도 있습니다:

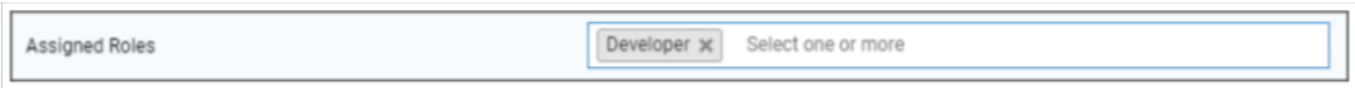


1. 역할을 추가하거나 제거할 그룹 또는 사용자를 선택합니다. 단일 사용자를 선택하거나 그룹을 선택할 수 있습니다. 그룹을 선택하면 변경 사항이 해당 그룹 내의 모든 사용자와 선택한 그룹에 속한 하위 그룹의 모든 사용자에게 영향을 미칩니다.
2. 추가하거나 제거할 역할을 선택합니다. 하나 또는 여러 개의 역할을 선택할 수 있습니다.
3. . Select what operation you want to perform. Clicking the “+” adds the selected roles if the user(s) did not have them already. Clicking the “-” removes the selected roles from the user(s). If you add roles to a user which did not yet have any role, it will automatically enable “Can Login” for the user.
4. 저장을 클릭하여 프로세스를 완료합니다. 이전에 역할이 없고 '로그인 가능'이 비활성화되어 있던 사용자에게는 비밀번호 설정 링크가 포함된 메일이 자동으로 전송됩니다.

대량 역할 할당 아래에서 할당된 역할에 대한 개요를 확인할 수 있습니다. 특정 사용자에 대한 역할을 수동으로 변경할 수도 있습니다.

역할 할당

사용자에게 역할을 할당하려면 그룹, 사용자 및 디바이스의 트리가 있는 모바일 관리로 이동해야 합니다. 사용자를 편집하여 역할을 할당합니다. 또는 위에서 언급한 방법을 단일 사용자에 대해서만 사용할 수도 있습니다.



API 액세스

AppTec360 REST API 액세스

AppTec360 REST API를 사용하려면 인증 토큰(API 키)과 개인 키가 필요하며, 이는 관리 콘솔에서 생성해야 합니다.

이렇게 하려면 AppTec360 EMM에 로그인하고 다음으로 이동합니다.

일반 설정 → 역할 기반 액세스 → API 액세스로 이동하여 새 키를 추가합니다.

API 키에 권한을 적용할 사용자를 선택해야 합니다.

개인 키는 한 번만 다운로드할 수 있습니다. 다운로드가 시작되면 키가 삭제되고 '다운로드' 버튼이 사라집니다.

개인 키를 분실한 경우 새 API 키를 생성해야 합니다.

일반 규칙

- REST API는 기본 URL 아래에서 사용할 수 있습니다:

/public/external/api

- 모든 요청은 POST를 통해 보내야 합니다.
- REST API는 HTTPS를 통한 요청만 지원합니다.
- 요청에는 다음 헤더가 포함되어야 합니다:

헤더 이름	헤더 값	설명
콘텐츠 유형	application/json	고정
auth	123...xyz	"API 액세스" 탭의 API 키
서명	Base64로 인코딩된 서명	를 사용하여 생성된 페이로드의 서명 "API 액세스" 탭에서 개인 키를 입력합니다.

- 요청 본문은 다음 값을 포함해야 하는 json 인코딩된 객체여야 합니다:

필드	필드 예제 값	설명
api	V2/장치/목록장치	API 이름
시간	1529662725	클라이언트 컴퓨터의 유닉스 타임스탬프(UTC). 허용되는 최대 시차 클라이언트와 서버 사이의 비율은 30 분.

- 성공하면 API는 요청된 데이터(아래 쿼리 참조)와 HTTP 상태 코드 200을 반환합니다.
- 오류가 발생하면 HTTP 상태 코드는 오류에 따라 4xx에서 5xx 사이가 되며 응답 객체에는 사람이 읽을 수 있는 오류 메시지 목록이 포함된 "errors" 키가 있는 배열이 포함됩니다.
- 장치에 일치하는 데이터가 없는 경우 빈 배열이 반환됩니다.
- 디바이스 ID가 존재하지 않으면 반환 데이터는 null이 됩니다.

요청 예시

```
POST /public/external/api HTTP/1.1
Host: myapptecemm.com
Accept: /
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg/
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
+q+rh6mrP1g4BCZ7Xq/wvgZkaP
b0CStBdMRvj46i3enxCXcLQQ==
Content-Length: 74
{"api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}}
```

쿼리

모든 디바이스 나열

기능: 기능: 디바이스 ID, IMEI, 시리얼이 포함된 모든 디바이스 목록을 반환합니다
API URI: v2/device/listdevices
필수 파라미터: 없음
선택 파라미터: 없음

요청 본문 예시

{
"api": "v2/device/listdevices",
"time": 1529662725
}

응답 본문 예시

{
"errors": [],
"list":[
{ "id":"10","serial":"987612345","imei":"899938455454"},
{ "id":"11","serial":"619723118","imei":"713032378599"}
]
}

(GPS) 위치 목록 가져오기

기능: 장치 ID에 대해 저장된 모든 위치 로그 항목의 목록을 반환합니다
API URI: v2/device/listposition
필수 매개변수: "ids" - 디바이스 ID 배열
선택적 매개변수: 없음

요청 본문 예시

{
"api": "device/listposition",
"params": {
"ids": [10, 11]
},
"time": 1529662725
}

응답 본문 예시

{
"errors": [],
"list":[
"10":[
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
],
"88":[],
]
}

자산 맵 가져오기

기능:
자산 데이터 가져오기를 사용하여 요청할 수 있는 저장된 모든 자산 목록을 반환합니다.
사람이 읽을 수 있는 양식 또는 자산 태그를 사용하여 데이터를 요청할 수 있습니다.
API URI: v2/device/getassetmap
필수 파라미터: 없음
선택 파라미터: 없음

요청 본문 예시

{
"api": "v2/device/getassetmap",
"time": 1529662725
}

응답 본문 예시

이 답변은 가독성을 위해 짧게 작성되었습니다.

{
"AssetKeys": {
"UDID": "AT001",
"Device Alias": "AT002",
"OS Version WinMobile iOS MacOS": "AT003",
"Model Name": "AT004",
"Serial Number": "AT005",
"Total Storage": "AT006",
"Free Storage": "AT007",
"IMEI": "AT008",
…
"apptecID": "APPTECID"
},
"errors": []
}

모든 자산 데이터 가져오기

기능: 디바이스 ID에 대해 요청된 에셋 데이터 목록을 반환합니다
API URI: v2/device/getassetdata
필수 파라미터: "ids" - 디바이스 ID 배열
선택적 매개변수:
"assetkeys" - 반환할 에셋 데이터 키. 지정하지 않으면 사용 가능한 모든 에셋 데이터가 반환됩니다. 에셋 맵 가져오기를 사용하여 에셋 키 목록을 가져올 수 있습니다.

요청 본문 예시

{
"api": "v2/device/getassetdata",
"time": 1529662725,
"params": {
"ids": [
26
],
"assetkeys": [
"imei"
]
}
}

응답 본문 예시

{
"result": {
"26": {
"imei": "349157642516427”
}
},
"errors": []
}

Python3의 예제 코드

```
! /usr/bin/python
import base64
from Crypto.Hash import SHA512
from Crypto.Signature import PKCS1_v1_5
from Crypto.PublicKey import RSA
import os
import time
import json
import urllib.request
import urllib.parse
import urllib.error
import http.client
applianceDomain = "YOURAPPLIANCE.COM"
apiURL = "https://"+applianceDomain+"/public/external/api"
privateKeyPath = "/path/to/PrivateKey-XXXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXX20"
currentTimestamp = int(time.time())
# Get Devices
#requestData = {"api": "v2/device/listdevices", "time": currentTimestamp}
# Get Positions
#requestData = {"api": "v2/device/listposition", "time": currentTimestamp,
"params":{"ids":[26]}}
# Get AssetData
requestData = {"api": "v2/device/getassetdata", "time": currentTimestamp,
"params":{"ids":[26], "assetkeys": ["imei"]}}
# encode the request data to json
print(json.dumps(requestData, indent=1))
jsonEncodedRequestData = json.dumps(requestData)
# Sign the request data json with the API private key
message = jsonEncodedRequestData.encode('utf-8')
print("Body:", message)
digest = SHA512.new()
digest.update(message)
```

```
# Read private key from file
with open(privateKeyPath, "r") as myKeyFile:
private_key = RSA.importKey(myKeyFile.read())
```

```
# Load private key and sign message
signer = PKCS1_v1_5.new(private_key)
signatureOfRequestData = signer.sign(digest)
Base64EncodedSignature = base64.b64encode(
signatureOfRequestData).decode("utf-8")

headers = {"Content-type": "application/json",
"auth": apptecAPIAuthToken, "signature": Base64EncodedSignature}
print("Headers:", headers, "\n")

# Send request to Server
httpsClient = http.client.HTTPSConnection(applianceDomain, 443, timeout=10)
httpsClient.request("POST", apiURL, jsonEncodedRequestData, headers)

# Get answer
response = httpsClient.getresponse()
status = response.status
data = response.read()

if data == False:
print("Invalid answer from the server")
else:
print("Answer:")
print(json.dumps(json.loads(data), indent=1))
if status != 200:
print("http error: lastReceivedHttpCode")
print(status)
```

Apple 구성

APNS 인증서

여기에서 APNS 인증서를 업로드할 수 있습니다. 이는 iOS 및 MacOS 장치를 관리하는 데 필요합니다.

참고: APNS 인증서는 1년 동안만 유효합니다. 만료되기 전에 갱신해야 합니다. 갱신 절차는 생성할 때와 동일하며(아래 참조) 몇 분 밖에 걸리지 않습니다.

제때 갱신하는 것을 잊은 경우 이미 등록된 디바이스를 변경할 수 없습니다. **모든 장치를 다시 등록해야 합니다.**.

1단계

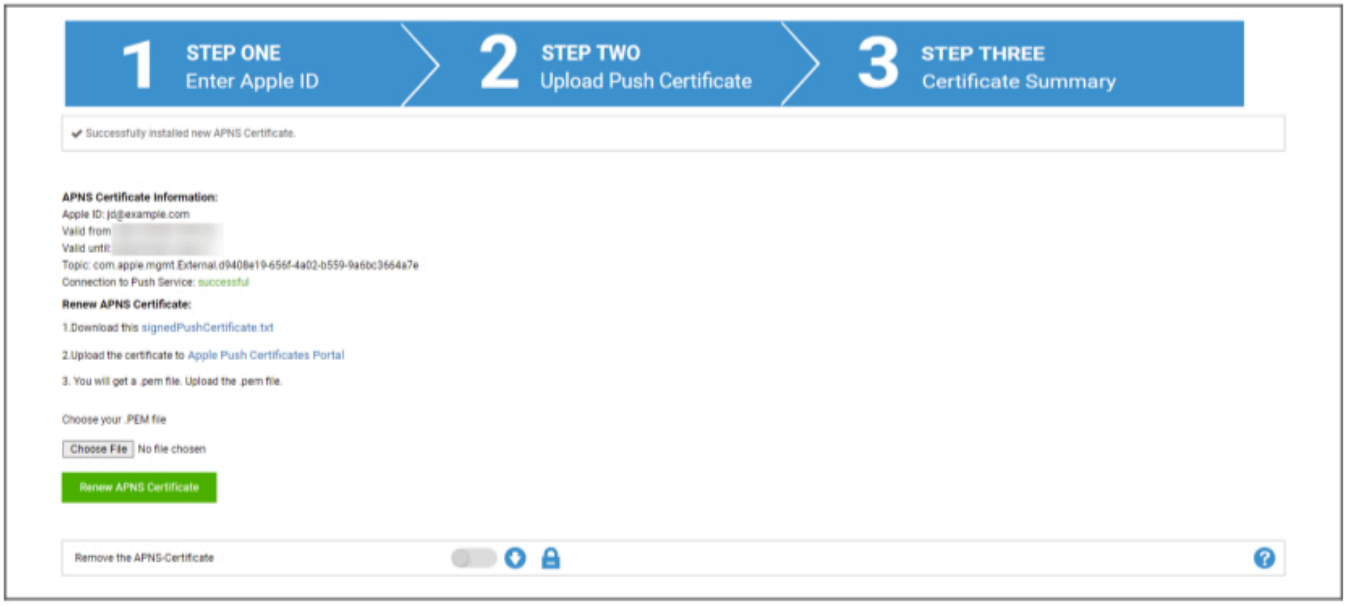
- 먼저, APNS 인증서를 만드는 데 사용할 Apple ID를 입력합니다.

참고: 이 Apple ID는 APNS 인증서 생성에만 사용됩니다. 이 Apple ID는 장치와 관련이 없으며 장치는 이 Apple ID에 대해 알지 못합니다. 또한 APNS 인증서를 갱신하려면 이 Apple ID에 대한 액세스 권한도 필요합니다. 따라서 일반 Apple ID를 사용하고 로그인 데이터를 문서화하는 것이 좋습니다. APNS 인증서가 만료되기 전에 사용한 Apple ID의 메일 주소로 리마인더가 전송됩니다.

- 계속하려면 '다음 단계'를 클릭합니다.
- (선택 사항) 실수로 삭제한 경우 이전에 삭제한 APNS 인증서를 복구할 수도 있습니다.

2단계

- 서명된 푸시 인증서.txt 다운로드
- https://identity.apple.com/pushcert/ 으로 이동하여 1단계의 Apple ID로 로그인합니다.
- "인증서 만들기"를 클릭합니다.
- (선택 사항) 메모를 입력합니다. 여러 테넌트를 관리하여 쉽게 식별할 수 있는 경우 유용할 수 있습니다.
- "파일 선택"을 클릭하여 이전에 다운로드한 서명된 푸시인증서.txt를 선택합니다.
- '업로드'를 클릭합니다.
- 이제 APNS 인증서를 만들었다는 확인 메시지가 표시됩니다.
- '다운로드'를 클릭하고 저장합니다.
- 관리 콘솔로 돌아갑니다.
- '파일 선택'을 클릭하고 업로드하려는 APNS 인증서를 선택합니다.
- "업로드"를 클릭합니다.



3단계

이제 APNS 인증서를 성공적으로 설정했으며 이제 iOS 및 MacOS 장치를 관리할 수 있습니다.

3단계에서는 현재 사용 중인 APNS 인증서에 대한 개요를 볼 수 있습니다.

또한 화면에 표시된 단계에 따라 APNS 인증서를 갱신할 수 있는 옵션도 있습니다. 만료되기 전에 갱신하는 것을 잊지 마세요.

APNS 인증서를 갱신할 때, 3단계에 표시된 Apple ID로 로그인하고 이전에 사용한 인증서를 갱신하고 새 인증서를 만들지 않도록 유의하세요. 3단계와 Apple 푸시 인증서 포털에서 "i"를 클릭하면 APNS 인증서의 "주제"를 볼 수 있습니다. 이것은 인증서를 식별하는 고유 ID입니다. 이를 통해 올바른 인증서를 식별하고 올바른 인증서를 갱신하는 데 도움이 됩니다.

갱신하는 동안 "오류: 푸시 인증서에 다른 주제가 있습니다!"라는 메시지가 표시되면 다른 인증서를 갱신했거나 새 인증서를 만들었음을 의미합니다.

이전에 사용하던 Apple ID에 더 이상 액세스할 수 없는 경우와 같이 새 인증서를 업로드하려면 먼저 현재 업로드한 인증서를 삭제해야 합니다.

어쨌든 APNS 인증서를 삭제하면 다시 등록할 때까지 현재 등록된 디바이스에 대해 더 이상 변경할 수 없습니다. 따라서 이에 대한 준비를 하고 다른 방법이 없는 경우에만 인증서를 제거하세요.

관리 액세스

여기에서 iOS 장치용 사용자 등록 및 iOS 장치용 공유 iPad를 사용하도록 설정할 수 있습니다.

사용자 등록

'사용자 등록'은 BYOD 디바이스를 위한 특수 모드를 활성화합니다.

각 사용자에 대해 Apple 비즈니스 포털에서 관리되는 Apple-ID를 생성해야 합니다.

등록 과정에서 사용자는 Apple-ID 자격 증명을 입력해야 합니다.

'사용자 등록'은 MDM에서 제한된 설정 및 제한 사항만 구성할 수 있도록 허용하므로 사용자의 안전을 최대한 보장합니다.

관리되는 도메인:

사용자의 이메일 주소를 관리되는 Apple-ID에 매핑하는 데 사용되는 도메인(반드시 '@appleid.company.com' 형식이어야 함)(예: john.doe@example.com은 john.doe@appleid.company.com에 매핑됨).

Apple 비즈니스 관리자에서 관리되는 도메인을 확인합니다.

공유 iPad

공유 iPad는 특수 DEP 프로필로 구성된 DEP 장치입니다.

이렇게 하면 여러 사용자가 관리되는 Apple-ID를 사용하여 기기에 로그인할 수 있습니다.

관리되는 Apple-ID는 Apple 비즈니스 포털 또는 Apple 학교 관리자에서 생성해야 합니다.

공유 iPad에 로그인하는 사용자에게는 관리되는 Apple-ID 자격 증명을 입력하라는 메시지가 표시됩니다.

관리되는 도메인:

사용자의 이메일 주소를 관리되는 Apple-ID에 매핑하는 데 사용되는 도메인(반드시 '@appleid.company.com' 형식이어야 함)(예: john.doe@example.com은 john.doe@appleid.company.com에 매핑됨).

Apple 비즈니스 관리자에서 관리되는 도메인을 확인합니다.

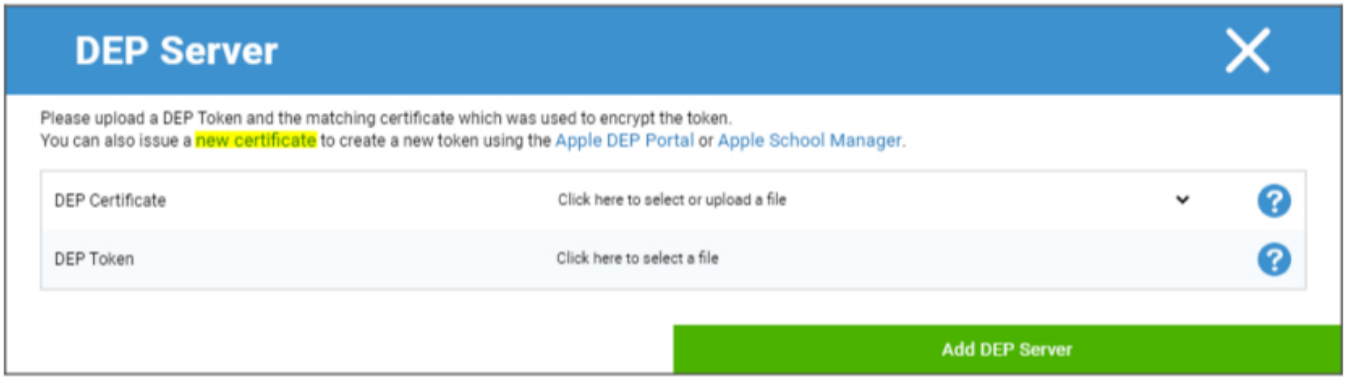
DEP

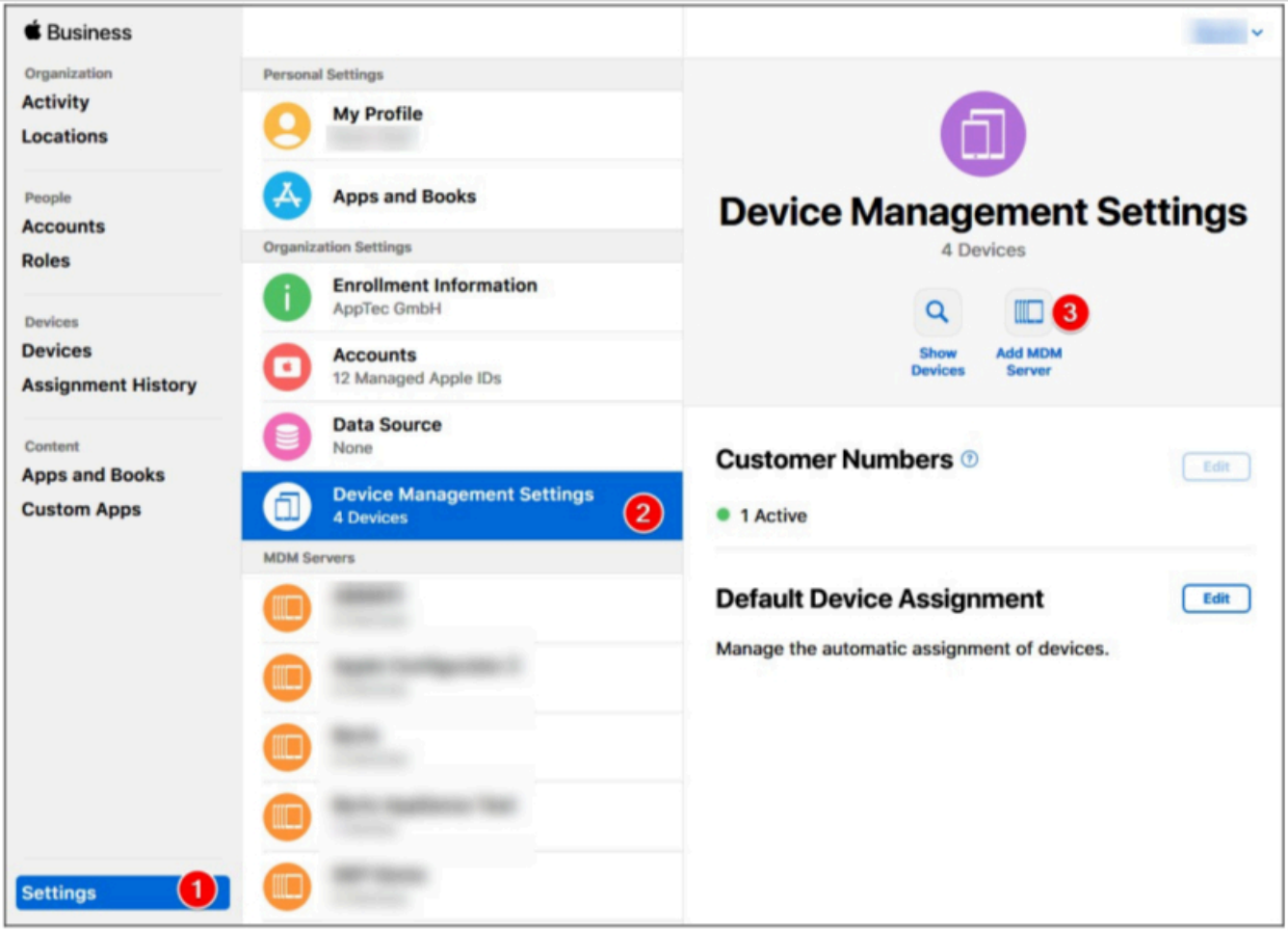
DEP(장치 등록 프로그램)를 사용하면 장치를 MDM에 쉽게 등록할 수 있습니다. DEP를 사용하면 디바이스를 설정할 때 디바이스가 자동으로 MDM에 연결됩니다. 또한 일반적으로 iOS에서 필수적으로 수행해야 하는 거의 모든 설정 단계를 건너뛸 수 있습니다.

DEP를 지원하는 리셀러를 통해 기기를 구입해야 한다는 점에 유의하세요. 자세한 내용은 리셀러 또는 Apple에 문의하세요.

DEP에 대한 자세한 정보: https://www.apple.com/business/dep/

"+"를 클릭하여 DEP 토큰을 추가합니다. 팝업에서 텍스트의 "새 인증서"를 클릭합니다(아래 이미지에서 노란색으로 표시됨). 그러면 DEP 인증서가 생성되고 다운로드됩니다. 그런 다음 Apple 비즈니스 관리자 (https://business.apple.com/) 또는 Apple 학교 관리자(https://school.apple.com/)로 이동합니다.

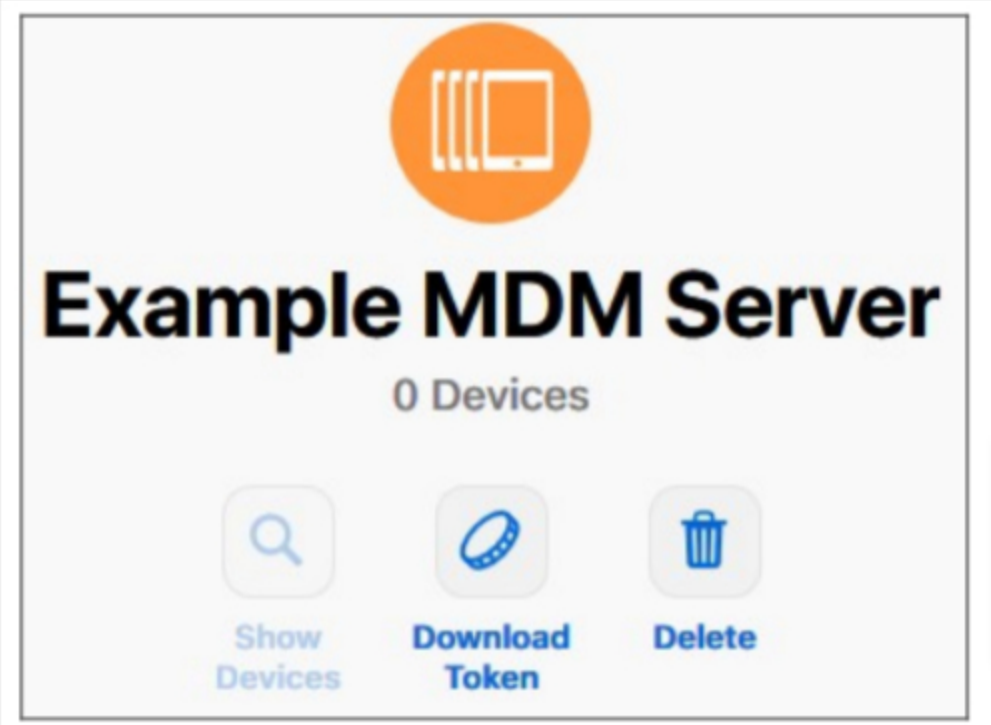




Apple 비즈니스 관리자에서 위 이미지와 같은 단계를 따릅니다. 설정 → 장치 관리 설정 → MDM 서버 추가를 선택합니다.

서버에 원하는 이름을 지정하고 MDM 서버 설정 → 공개 키 업로드에서 이전에 다운로드한 DEP 인증서를 업로드한 후 "저장"을 클릭합니다.

이제 "토큰 다운로드" 옵션이 표시됩니다. 이를 클릭하고 저장합니다. 토큰은 1년 동안만 유효합니다. 하지만 "토큰 다운로드"를 다시 클릭하면 새 토큰을 받을 수 있으므로 토큰을 매우 쉽게 갱신할 수 있습니다.



이제 이전에 DEP 인증서를 다운로드한 MDM으로 돌아갈 수 있습니다. 탭을 닫지 않았다면 DEP 서버 추가 팝업이 계속 열리고 DEP 인증서가 이미 선택되어 있을 것입니다. 이제 "DEP 토큰" 필드에 토큰을 업로드하고 DEP 서버를 클릭할 수 있습니다.

'**장치**' 열에서 이 DEP 서버에 할당된 장치 수를 확인할 수 있습니다. 이 DEP 서버에 추가된 장치는 모바일 관리의 DEP 풀에 자동으로 생성됩니다.

이 번호를 클릭하면 모든 DEP 장치와 그 상태에 대한 개요를 확인할 수 있습니다.

참고: 비즈니스 관리자의 워크플로 또는 구성에 따라 이러한 장치를 DEP 서버에 수동으로 할당해야 할 수도 있습니다. Apple 비즈니스 관리자에서 새 장치에 대한 기본 DEP 서버를 설정할 수도 있습니다.

'**프로필**' 열에서 보유한 DEP 프로필의 양을 확인할 수 있습니다. 이 번호를 클릭하면 DEP 프로필에 대한 세부 정보를 볼 수 있으며, 여기에서 오래된 프로필이나 사용하지 않는 프로필을 삭제할 수 있습니다. 현재 이러한 프로필은 변경할 수 없습니다. 변경하려면 프로필을 새로 만들어야 합니다.

'**마지막 동기화**' 열에서 DEP 서버를 수동으로 동기화하고(예: 방금 새 장치를 DEP에 추가한 경우) 마지막으로 동기화에 성공한 날짜를 확인할 수 있습니다.

'**자동 프로필**' 열에서 DEP 프로필을 자동 기본값으로 설정할 수 있습니다. 이 프로필은 새 장치에 자동으로 할당됩니다. 자동 프로필을 설정하지 않으면 매번 새 장치에 프로필을 수동으로 할당해야 합니다.

"**프로필 추가**" 열에서 새 DEP 프로필을 추가할 수 있습니다. 디바이스 설정이 시작될 때 디바이스가 이 프로필을 받게 됩니다. DEP 프로필은 장치 설정 방법과 건너뛸 설정 단계를 정의합니다.

참고: 디바이스를 등록한 후에는 공장 초기화를 수행하고 새 프로필로 디바이스를 등록해야만 이러한 설정을 변경할 수 있습니다. 이는 특히 '**이동식**' 및 '**페어링 허용**'과 관련이 있습니다. '**페어링 허용**'의 경우 MDM 제한을 통해 비활성화할 수 있지만 DEP 프로필에서 비활성화하면 다시 활성화할 수 없으므로 이 설정을 켜는 것이 좋습니다.

예를 들어 토큰을 갱신할 때 '**수정**' 열에서 새 토큰을 업로드할 수 있습니다.

구성자 및 URL

풀 등록 URL

여기에서 설정된 등록 기간과 설정된 날짜까지 유효한 등록 URL과 등록 QR 코드를 생성할 수 있습니다. 이렇게 하면 하나의 링크 또는 QR 코드만으로 여러 장치를 등록할 수 있습니다.

이 URL 또는 QR 코드로 등록한 디바이스는 모바일 관리의 풀에 등록되며 나중에 그룹이나 사용자에게 수동으로 할당해야 합니다.

참고: 이 URL은 수동 등록 전용입니다. Apple Configurator를 통해 장치를 등록하는 경우에는 이 URL을 사용하지 마세요.

MDM 프로필 – Apple 구성 관리자

여기에서 Apple Configurator를 통해 장치를 등록할 때 필요한 URL을 얻을 수 있습니다. Apple Configurator로 장치를 준비하는 동안 동일한 프로세스에서 장치를 MDM에 추가할 수 있습니다. 이를 위해서는 Apple Configurator에 이 URL이 필요합니다.

Apple Configurator를 통해 추가된 장치는 모바일 관리의 풀에 있으며 나중에 그룹이나 사용자에게 수동으로 할당해야 합니다.

또한 여기에서 Apple Configurator를 통해 장치를 등록하는 데 사용할 수 있는 .mobileconfig 파일도 찾을 수 있습니다. 어쨌든 URL 사용을 권장합니다.

Android 구성

Android 구성

보호 제거	이 기능이 활성화된 경우 사용자는 MDM 관리자가 설정한 비밀번호를 입력하지 않고는 장치 관리자를 비활성화할 수 없습니다. 비밀번호는 등록 시 설정되므로 비밀번호를 업데이트하려면 장치를 다시 등록해야 합니다. 장치 관리자를 제거하는 데는 두 가지 옵션이 있습니다: 1. 장치에서 수동으로 ◦ 기기에서 EMM 앱 열기 ◦ 상태 탭으로 전환 ◦ "보호 기능 제거"를 탭합니다. ◦ 비밀번호 입력 콘솔의 '비밀번호 기록'에서 수정본을 사용하여 올바른 비밀번호를 얻을 수 있습니다. ◦ 아래로 스크롤하여 새로 추가된 지점, "AppTec360 MDM 앱을 제거하려면 탭하세요"를 탭합니다(이 작업을 수행하는 데 20초가 주어집니다). ◦ "앱텍360 MDM 앱 제거" 대화 상자를 "확인"으로 확인합니다. 그러면 콘솔에서 디바이스의 등록이 해제됩니다. ◦ 기기에서 앱을 제거하려면 "앱텍360 MDM이 제거됩니다"라는 대화 상자를 "제거"로 확인합니다. 2. 자동(콘솔) ◦ 콘솔에서 장치를 선택합니다. ◦ 파란색 톱니바퀴 아이콘을 클릭하고 '엔터프라이즈 삭제'를 선택합니다. 참고: Android 4.x 이하 버전 또는 KNOX API가 설치된 기기(삼성 기기)에서만 사용할 수 있습니다.
비밀번호 제거 (개정 X)	사용자가 장치 관리자를 제거할 수 있는 설정된 비밀번호입니다. 개정 x = 카운터, 암호가 이미 변경된 빈도 장치가 AppTec360 서버와 통신하지 않아 최신 암호가 아직 전송되지 않았을 수 있으므로 사용자에게 필요한 암호가 중요합니다.
비밀번호 기록	파란색 버튼('기록 보기')을 클릭하면 이전에 설정한 비밀번호를 볼 수 있습니다.
확장된 제거 보호	이 옵션은 비안전 장치에 대한 보호 기능을 제공합니다.

	이 설정이 활성화되어 있는 한 장치 관리자는 쉽게 비활성화할 수 없습니다.
사용자에게 차단된 앱을 제거하라는 메시지를 표시하나요?	가능한 경우 차단된 앱은 차단될 뿐만 아니라 자동으로 제거됩니다. 자동 제거가 불가능한 경우 차단된 앱을 제거하라는 메시지가 표시됩니다.
지능형 시스템 앱 차단	화이트리스트가 활성화되면 Android MDM 클라이언트는 사용자가 설치한 모든 앱을 차단합니다. 화이트리스트 모드에서 실행 가능한 모든 시스템 앱을 차단하려면 이 설정을 활성화합니다.

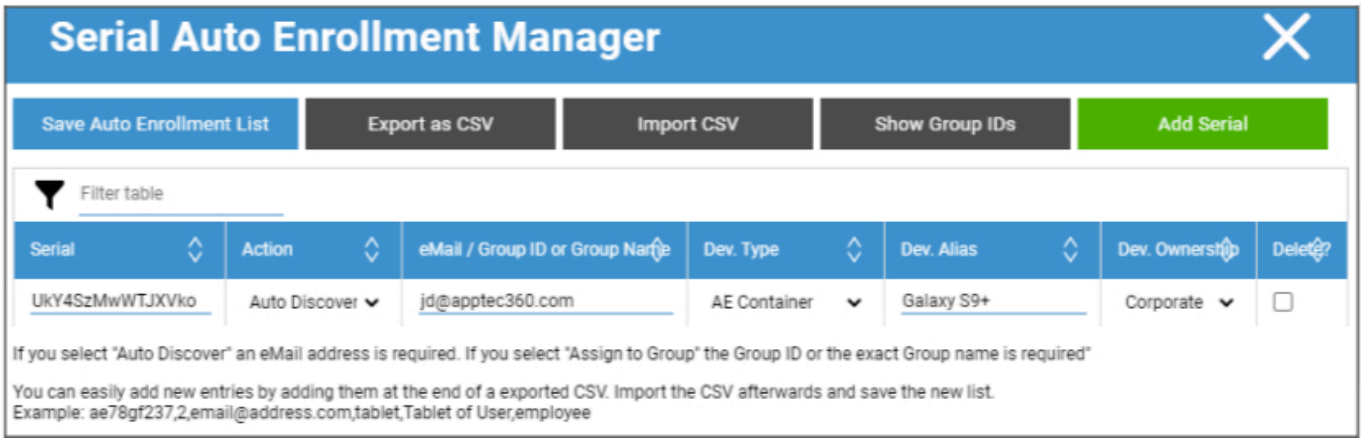
자동 등록

여기에서 자동 등록 기능을 활성화하여 기기에서 AppTec360 MDM 클라이언트를 열 때 기기를 자동으로 등록할 수 있습니다.

중요: 이 등록 방법은 더 이상 사용되지 않으며 Android 10 이상에서는 더 이상 작동하지 않습니다. 어쨌든 Android 7 이상을 사용하는 경우에는 기기를 Android Enterprise 완전 관리형으로 등록해야 합니다. Android Enterprise BYOD 컨테이너를 사용하려는 경우 Android 10 이상을 사용하는 경우 자격 증명, QR코드 또는 SMS를 통해 수동으로 장치를 등록해야 합니다. 어쨌든 자동 등록 목록은 여전히 AE 등록, Knox 등록 등의 등록 프로세스를 자동화하는 데 사용됩니다.

어쨌든 자동 등록 목록은 여전히 AE 등록, Knox 등록 등의 등록 프로세스를 자동화하는 데 사용됩니다.

'시리얼 관리자' 또는 'IMEI 관리자'를 클릭하면 각각 디바이스의 시리얼 또는 IMEI를 추가할 수 있습니다. 장치에 대해 두 가지를 모두 수행할 필요는 없으며 하나만 수행해도 충분합니다.



동작은 디바이스를 풀에 등록할지, 사용자 또는 그룹에 등록할지 정의합니다.

또한 .csv 파일을 내보내고 가져올 수 있으며 키워드로 항목을 필터링할 수도 있습니다.

Android 엔터프라이즈

여기에서 Android Enterprise를 설정할 수 있습니다. 모든 Android Enterprise 기능을 사용하려면 이 설정이 필요합니다.

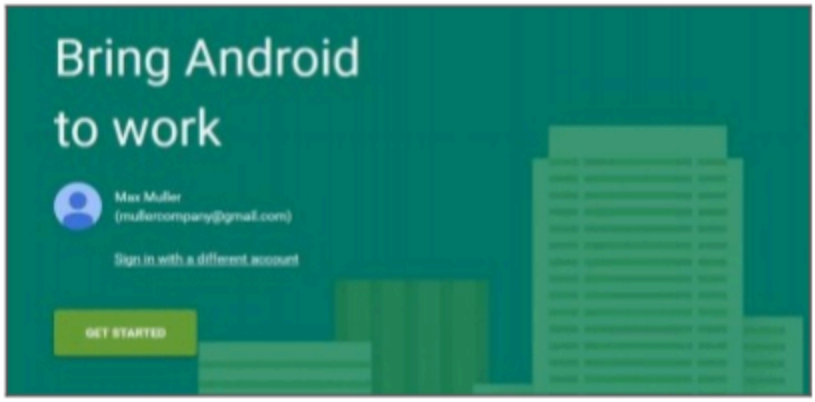
첫 번째 방법: Android 기업 계정(Google 계정)

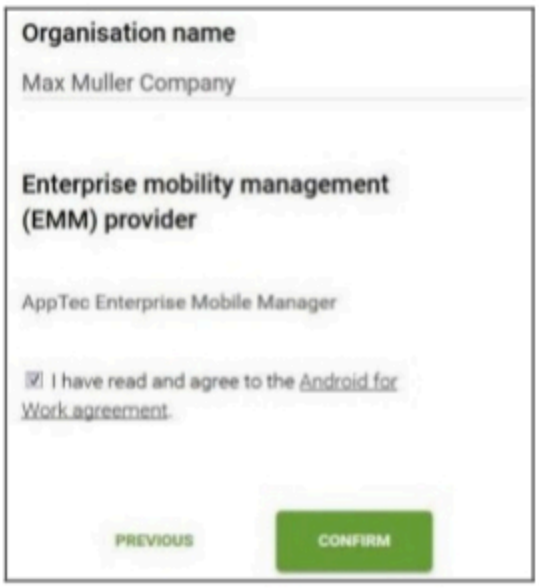
먼저 "설정 준비"를 누르면 잠시 후 "설정 시작" 버튼이 나타납니다.

그러면 Google의 Android 기업 설정 페이지로 이동합니다.

아직 로그인하지 않은 경우 사용하려는 Google 계정으로 로그인하고 '시작하기'를 누릅니다.

이제 회사 이름을 입력할 수 있습니다. 그런 다음 확인란을 선택하고 "확인"을 누릅니다.





마지막 단계에서 등록을 완료하고 콘솔로 돌아가야 합니다. 모든 것이 정상적으로 작동했다면 다음과 같이 표시되어야 합니다:

이제 Android 엔터프라이즈 컨테이너 구성을 시작할 수 있습니다.

두 번째 방법: G-Suite 계정

"G-Suite 사용"을 누르고 Google 관리자 계정에 로그인합니다. "보안" -> "더보기" -> "Android용 EMM 공급자 관리"로 이동하여 토큰을 생성합니다. 참고: G-Suite 계정에 Android 엔터프라이즈 설정이 표시되지 않으면 "더 많은 앱 및 서비스 받기"로 이동하여 Android 기기 관리를 추가해야 합니다. 이제 콘솔에 토큰과 기본 도메인을 입력하고 "변경사항 저장"을 클릭합니다. 완료했으면 "Android 엔터프라이즈 계정 사용"을 클릭합니다.

이제 "서비스 계정 만들기" 버튼이 표시됩니다. 클릭합니다. 이 과정은 몇 분 정도 걸릴 수 있습니다.

모든 것이 정상적으로 작동했다면 다음과 같이 표시되어야 합니다:

이제 Android 엔터프라이즈 컨테이너 구성을 시작할 수 있습니다.

공장 초기화 보호

공장 초기화 보호 기능을 사용하면 원하는 Google 계정에 디바이스를 바인딩할 수 있으며, 이 경우 기존의 모든 Google 계정 바인딩도 무시할 수 있습니다. 공장 초기화 보호를 사용하려면 먼저 여기에서 설정하고 나중에 프로필에서 활성화해야 합니다.

공장 초기화 보호를 설정하려면 'FRP 설정'을 클릭하고 화면의 지침을 따르세요.

참고: 단계를 주의 깊게 읽고 수행하세요. 잘못된 Google 계정에 자동으로 로그인되는 것을 방지하려면 새 시크릿 브라우저 창에서 이 작업을 수행하는 것이 좋습니다. 잘못된 아이디를 입력하거나 사용한 Google 계정에 대한 액세스 권한을 잃어버린 경우 기기에서 자신을 완전히 차단할 수 있습니다!

AE 등록

여기에서 Android 엔터프라이즈 어놀레이션을 활성화할 수 있습니다. 이 방법을 사용하면 디바이스가 Android Enterprise 디바이스 소유자 모드로 등록됩니다. 이 모드에서는 장치를 완전히 제어할 수 있습니다.

AE 등록 사용	AE 등록 주의를 활성화합니다: AE 등록을 비활성화하면 기존 QR코드와 이미 구성된 NFC 프로그래머 디바이스의 작동이 중지됩니다. AE 등록을 다시 활성화하면 NFC 푸시 구성을 다시 전송하거나 새 QR 코드를 생성해야 합니다.
자동 검색 사용	디바이스가 'AE 등록'을 통해 스스로 등록하면 시스템은 시리얼/IMEI 화이트리스트('일반 설정' > 'Android 구성' > '자동 등록')에 설정된 정보를 기반으로 사용자에게 디바이스를 할당하려고 시도합니다.
알 수 없는 장치 차단	시리얼/IMEI 화이트리스트('일반 설정' > 'Android 구성' > '자동 등록')에 화이트리스트에 등록된 디바이스만 등록할 수 있습니다.

방법 1 및 2 참고: '시작 화면'은 공장 초기화 후 처음 표시되는 화면을 말합니다. 사용 중인 Android 버전 및/또는 디바이스 모델에 따라 다르게 보일 수 있습니다.

방법 1: QR코드 등록

(안드로이드 7.0 이상 필요) 안드로이드 7 이상을 실행하는 경우 항상 이 방법을 사용하는 것이 좋습니다.

1. 기기 공장 초기화
2. 다음 두 가지 방법 중 하나를 사용하여 등록용 QR 코드를 생성합니다:
   - '일반 설정 -> 안드로이드 구성 -> AE 등록'에서 'QR코드 생성'을 클릭합니다. 저장소 암호화를 건너뛰거나 모든 시스템 앱을 제거할지 여부를 선택합니다.
   - (또는) 기존 장치를 선택합니다. '장치 개요'에서 표시된 QR 코드를 클릭합니다. 스토리지 암호화를 건너뛰거나 모든 시스템 앱을 제거할지 여부를 선택합니다.
3. 이제 디바이스의 시작 화면을 6번 탭합니다. 그러면 QR 등록 모드가 시작됩니다.
4. 이제 무선 네트워크에 연결하고 QR코드 리더가 설치될 때까지 잠시 기다립니다.
5. 이제 QR 코드를 스캔하세요.
6. 이제 끝입니다. 이제 디바이스가 Android 기업용 디바이스 모드에 등록되었습니다.
   - a. '일반 설정'에서 QR 코드를 사용한 경우 '풀 -> AE 디바이스 소유자 디바이스'에서 디바이스를 찾을 수 있습니다. (힌트: 사이트를 새로고침해야 디바이스를 확인할 수 있습니다). "자동 검색 사용"을 체크한 경우 자동 검색 사용자 내에서 찾을 수 있습니다.
   - 기존 디바이스 프로필의 QR 코드를 사용한 경우 해당 디바이스가 이 프로필에 등록됩니다.

방법 2: NFC 등록

(NFC 및 Android 6.0 이상 필요)

준비: "일반 설정 -> 안드로이드 구성 -> AE 등록 -> NFC 프로비저닝용 데이터"에서 WiFi 정보를 입력합니다. 이제 "NFC 장치"를 사용하여 프로그래머가 될 장치를 검색합니다. 이 장치는 NFC를 통해 다른 장치에 등록 정보를 전송하는 데 사용됩니다.

1. 기기 공장 초기화
2. 프로그래머에서 AppTec360의 NFC 페어링 앱을 엽니다.
3. 저장소 암호화를 건너뛰거나 모든 시스템 앱을 제거할지 여부를 선택합니다.
4. 두 장치를 연달아 잡기
5. 이제 Android 엔터프라이즈 등록이 뚜렷해집니다.
6. 이제 콘솔에서 기기를 찾을 수 있습니다.
    - a. 풀에서 자동 검색을 구성하지 않은 경우
    - b. 사용자 내에서 자동 검색을 구성한 경우
    - c. 힌트: 장치를 보려면 사이트를 다시 로드해야 할 수 있습니다.

방법 3: Google 계정

(Android 5.1 이상 필요)

(참고: 이 방법을 사용하는 경우 디바이스가 자동으로 등록되지 않습니다. 대신 수동으로 등록하거나 자동 등록을 사용하여 프로세스를 자동화해야 합니다.)

1. 기기 공장 초기화
2. Google 계정으로 로그인할 수 있을 때까지 설정 단계를 진행합니다.
3. 사용자 이름/이메일로 "afw#apptec"을 입력합니다.
4. "다음"을 탭합니다.
5. 이제 디바이스가 Android 기업용 디바이스입니다.

KNOX 등록

여기에서 KNOX 등록을 활성화하고 KNOX 배포 포털에서 KNOX 등록 프로필을 만드는 데 필요한 정보를 찾을 수 있습니다. 이를 구성하고 사용하려면 KNOX 배포 포털의 계정이 필요합니다.

(https://www.samsungknox.com/en/knox-deployment-program)

KNOX 등록 사용	KNOX 등록을 활성화합니다. 주의: KNOX 등록을 비활성화하면 기존 MDM 프로필의 작동이 중지됩니다. KNOX 등록을 다시 사용 설정하는 경우 MDM 프로필의 '사용자 지정 JSON 데이터' 필드를 업데이트해야 합니다.
자동 검색 사용	장치가 "KNOX 등록"을 통해 스스로 등록하면 시스템은 시리얼/IMEI 화이트리스트("일반 설정" > "Android 구성" > "자동 등록")에 설정된 정보를 기반으로 사용자에게 장치를 할당하려고 시도합니다.

1. 삼성 KNOX 모바일 등록 포털에 로그인 https://eukme.samsungknox.com/itadmin
2. "MDM 프로필"로 이동
3. "추가"를 클릭합니다.
4. "내 MDM에 서버 URI가 필요하지 않음"을 선택하고 "다음"을 클릭합니다.
5. 이제 관리 콘솔에 표시된 정보로 프로필을 만듭니다.

이제 삼성에서 직접 디바이스를 구입한 경우 이 KNOX 등록 프로필을 삼성에서 디바이스에 직접 설치할 수 있습니다.

또는 KNOX 배포 앱을 다운로드하고 KNOX 배포 계정으로 로그인한 다음 NFC를 통해 다른 장치로 KNOX 등록 프로필을 전송할 수 있습니다.

장치에 KNOX 등록 프로필이 설치되어 있는 경우, 인터넷 연결이 가능한 경우 앱을 다운로드하고 장치를 등록합니다.

KNOX 등록을 통한 장치 등록은 "풀 -> KNOX 등록" 또는 자동 검색에서 지정한 사용자 내에서 찾을 수 있습니다.

제로 터치

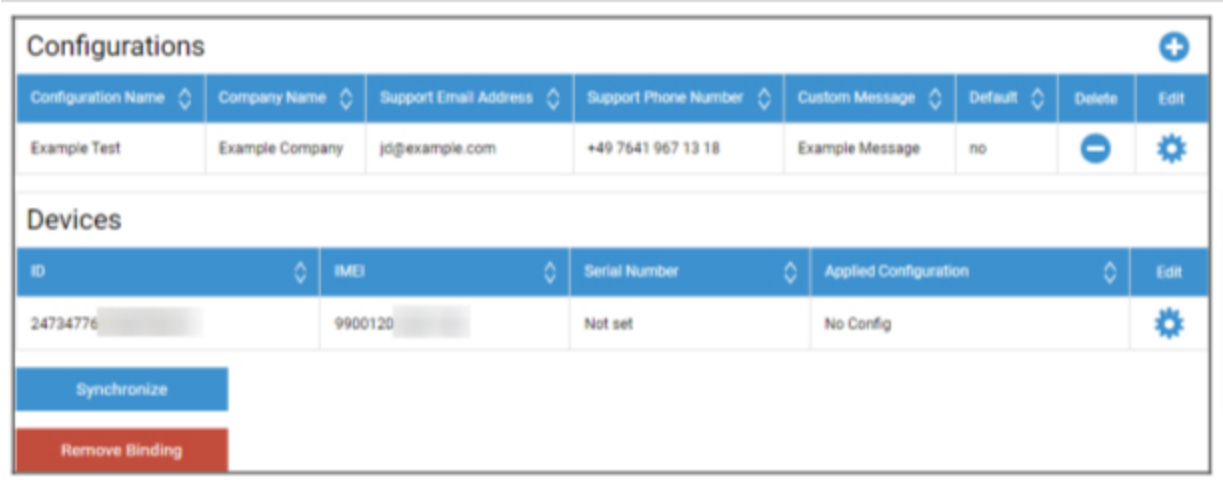
제로 터치를 사용하면 장치를 만지거나 장치 자체에서 아무것도 구성할 필요 없이 쉽게 장치를 등록할 수 있습니다. 전원을 켜고 평소와 같이 구성을 진행하기만 하면 장치가 MDM 설정 및 연결 방법에 대한 모든 정보를 완전히 자동으로 수신합니다.

제로 터치를 사용하려면 제로 터치를 지원하는 리셀러를 통해 기기를 구매해야 합니다. 동일한 리셀러가 제로 터치 포털에서 사용자를 위한 계정도 생성합니다. 절차에 대한 자세한 정보를 얻거나 제로 터치 포털에 액세스할 때 문제가 있는 경우 리셀러에게 문의하세요.

설정을 시작하려면 '설정 시작'을 클릭합니다. 제로 터치 포털에 액세스할 수 있는 Google 계정을 선택해야 하는 로그인 페이지로 리디렉션됩니다.

참고: 모든 계정을 선택할 수 있습니다. 따라서 이 단계에서 올바른 계정을 선택해야 합니다. 디바이스/구성 정보가 표시되지 않는다면 잘못된 계정을 사용했을 가능성이 높습니다.

로그인이 완료되면 다음과 같은 화면이 표시됩니다:



"+"를 클릭하여 구성을 추가하고 화면에 표시된 대로 입력란을 채웁니다. 구성을 기본 구성으로 활성화하면 새 장치에 자동으로 할당됩니다. 기본 구성을 만들거나 설정해도 이미 존재하는 장치에는 기본 구성이 할당되지 않습니다.

장치에 구성이 할당되지 않은 경우 일반 장치로 설정되고 MDM에 연결되지 않습니다. 따라서 장치에 구성이 할당되어 있는지 확인하세요.

계정을 연결하고 장치가 표시되고 장치에 구성이 할당되면 장치 설정을 시작할 수 있습니다.

장치를 자동 등록 목록에 추가하여 지정된 그룹 또는 사용자에게 자동으로 등록되도록 할 수 있습니다. 자동 등록 목록에서 아무것도 구성하지 않으면 장치가 풀에 등록됩니다.

Windows 구성

Windows 구성

여기에서 Windows 10 PC에서 다음 구성을 활성화할 수 있는 옵션이 있습니다:

즉시 DM 연결	
초기 재시도 시간	장치에 대한 첫 번째 연결 시도를 설정하며, 이 값은 기하급수적으로 증가합니다.
연결 재시도	연결 오류가 발생하는 동안 DM 클라이언트가 수행해야 하는 연결 시도 횟수를 나타냅니다.
최대 수면 시간	연결 오류 후 최대 절전 시간을 나타냅니다.
첫 번째 동기화 재시도	첫 번째 연결 후 장치가 서버와 통신하는 간격입니다.
첫 번째 재시도 간격	"첫 번째 동기화 재시도"와 관련된 내용 시간은 분 단위로 나열됩니다. 예를 들어 "첫 번째 동기화 재시도" 아래에 "2" 값이 표시되고 "첫 번째 재시도 간격" 아래에 "4분" 값이 표시되면 첫 번째 연결 후 장치가 4분마다 2번씩 통신하는 방식입니다.
두 번째 동기화 재시도	"첫 번째 동기화 재시도"를 완료한 후 장치가 서버와 통신해야 하는 간격입니다.
두 번째 재시도 간격	"첫 번째 재시도 간격"과 동일한 원칙이 여기서는 "두 번째 동기화 재시도"에 적용된다는 점만 다릅니다.
정기적인 동기화 재시도	간격, 향후 장치가 서버와 통신해야 하는 빈도를 나타냅니다. 기본값: "무한" 이 값을 변경하지 않는 것이 좋습니다. "10"을 입력하면 장치가 서버와 10 번 통신 한 다음 중지되므로 AppTec360 서버와의 통신이 끊어집니다!
정기 재시도 간격	'첫 번째/두 번째 재시도 간격'과 동일한 원리로, 여기서는 향후 설정을 적용한다는 점만 다릅니다.
정기 재시도 간격	'첫 번째/두 번째 재시도 간격'과 동일한 원리로, 여기서는 향후 설정을 적용한다는 점만 다릅니다.

콘텐츠 상자

구성

여기에서 ContentBox를 구성할 수 있습니다. 디바이스의 ContentBox 앱으로 액세스할 수 있는 그룹용 파일을 ContentBox에 배치할 수 있습니다.

콘텐츠 상자 사용	ContentBox를 활성화합니다. ContentBox를 사용하지 않는 경우 이 기능을 비활성화하면 온프레미스 머신의 리소스를 절약할 수 있습니다.
외부 ContentBox 설치 사용	ContentBox는 자체 Nextcloud로 운영할 수도 있습니다.
URL	Nextcloud 엔티티의 전체 URL
루트 사용자	Nextcloud 계정의 루트 사용자
루트 비밀번호	넥스트클라우드 계정의 루트 비밀번호
기본 그룹 폴더 권한	기본 그룹 폴더 권한은 그룹별로 개별적으로 수정할 수 있습니다(모바일 관리에서).
하위 그룹과 그룹 폴더 공유	활성화된 경우 각 하위 그룹은 메인 그룹의 모든 폴더를 읽을 수 있으며, 각 그룹에 대해 개별적으로 구성할 수도 있습니다(모바일 관리).
하위 그룹에 대한 권한	하위 그룹에 대한 권한 각 그룹에 대해 개별적으로 구성할 수 있습니다(모바일 관리).
공유 허용	링크를 통해 사용자가 콘텐츠를 공유할 수 있도록 허용하며, 각 그룹별로 개별적으로 구성할 수 있습니다.
최대 파일 업로드 크기(MB)	파일 최대 크기 표준: 512MB 최대 구성: 2048
WebDAV 자격 증명	
WebDAV URL	WebDAV로 콘텐츠 상자를 열 수도 있습니다. 어떤 경우에도 다음 폴더를 삭제하지 마세요: /apptecgroups /apptecgroups/AppTecGroup-X
루트 사용자	루트 사용자의 이름
비밀번호	루트 사용자의 비밀번호

ContentBox와의 동기화는 자동으로 수행됩니다. 그러나 "콘텐츠 상자 동기화"를 사용하여 수동으로 동기화를 수행할 수도 있습니다.

또한 여기에서 각 개별 장치에서 콘텐츠 상자를 활성화/비활성화할 수 있습니다.

콘텐츠박스를 추가로 라이선스하지 않은 경우에만 해당되며, 콘텐츠박스를 테스트할 수 있는 25개의 디바이스에 대한 액세스 권한이 있으며 여기에서 각 디바이스에 대해 활성화할 수 있습니다.

LDAP 구성

LDAP 개요

여기에서 LDAP를 통해 Active Directory에 연결하여 사용자 및 그룹을 대량으로 가져올 수 있습니다. 동기화는 수동으로 수행해야 합니다. 서로 다른 시스템 또는 서로 다른 구성/필터를 사용하여 여러 개의 LDAP 연결을 구성할 수 있습니다.

서버 이름	서버의 표시 이름
유형	현재 LDAP를 지원하는 활성 디렉터리만 지원됩니다.
LDAP 도메인	기본 LDAP 도메인(예: example.com)
LDAP 호스트	지정된 LDAP 도메인에서 LDAP 호스트에 연결할 수 없는 경우에만 필요합니다.
포트	표준 포트(SSL의 경우 389 또는 636)를 사용하려면 비워둡니다.
사용자 이름	예: CN=John,OU=사용자,DC=EXAMPLE,DC=COM 참고: 대부분의 시스템에서는 이 형식의 사용자 아이디를 요구하며 "John"을 사용자 아이디로 허용하지 않습니다.
비밀번호	
비밀번호 확인	
연결 보안	참고: SSL 또는 TLS를 사용하는 경우 Active Directory의 인증서가 확인됩니다. 자체 서명된 경우 루트 CA를 온프레미스 컴퓨터의 신뢰 저장소에 추가해야 합니다. 클라우드에 있는 경우 Active Directory에서 신뢰할 수 있는 인증서를 제공해야 하며, 그렇지 않으면 암호화 없이 연결만 작동합니다.
자동 동기화.	일반 LDAP 설정에서 지정한 시간 간격으로 LDAP 디렉터리를 자동으로 동기화할 수 있도록 설정합니다.
기본 DN	전체 디렉터리를 동기화하지 않으려면 여기에 OU를 지정할 수 있습니다(예: OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM).
회원	가져온 모든 사용자가 선택한 그룹에 추가됩니다.
활성화된 사용자만 사용하시나요?	활성화하면 userAccountControl 속성이 고려되며, 해당 속성이 없는 사용자는 가져오지 않습니다.
LDAP 필터	LDAP 필터를 사용하여 가져올 사용자를 필터링할 수 있습니다.
정규식 필터	정규식 필터를 사용하여 가져올 사용자를 필터링할 수 있습니다.
연결 테스트	구성을 저장할 때 연결을 테스트합니다.

동기화 시 디렉터리 구조를 초기화할 수 있나요?	참이면 모든 LDAP 항목이 LDAP 트리의 원래 위치로 다시 이동됩니다. 활성화하는 것이 좋습니다.
삭제된 사용자 및 그룹을 다시 가져오시겠습니까?	사용 설정하면 삭제된 사용자 및 그룹이 다시 만들어집니다. 사용하도록 설정하는 것이 좋습니다.
동기화 삭제?	이 옵션을 활성화하면 그룹과 사용자가 LDAP 서버에서 삭제될 때 삭제됩니다. 또한 삭제된 사용자의 장치도 삭제됩니다.

LDAP 구성 목록 아래에서 시스템 자동 동기화 주기를 정의할 수 있습니다. 자동 동기화에는 해당 옵션이 활성화된 LDAP 구성만 사용합니다.

앱 관리

사내 앱 DB

Android

여기에서 회사에서 개발한 Android 앱을 업로드하고 나중에 모바일 관리에서 디바이스 또는 그룹 프로필에 배포할 수 있습니다.

Google Play 스토어에서 사용할 수 없는 앱은 이 방법으로만 배포하는 것이 좋습니다.

"+"를 클릭하여 업로드하려는 앱의 APK를 업로드합니다. 현재 APK 형식만 지원됩니다.

온프레미스 어플라이언스의 업로드 제한은 어플라이언스 구성의 3단계에서 늘릴 수 있습니다. Cloud에서 업로드 한도를 늘리려면 지원팀에 문의하여 자세한 내용을 확인하세요.

일반적으로 APK는 콘텐츠보다 약간 작다는 점에 유의하세요. 이 과정에서 APK의 압축이 풀리기 때문에 업로드가 실패할 수 있습니다. 예를 들어 업로드 제한이 100MB인 경우 95MB APK가 실패할 수 있습니다. 이 경우 위에서 언급한 대로 업로드 제한을 늘리세요.

또한 먼저 USB를 통해 APK를 하나의 테스트 디바이스로 수동으로 이동하고 디바이스의 파일 앱으로 수동으로 설치를 시도하는 것이 좋습니다. 어떤 이유로든 이 방법이 작동하지 않으면 MDM을 통해서도 실패합니다.

대상 업데이트

'업데이트 대상' 기능을 사용하면 앱에 대해 '최신 버전 유지'를 활성화한 경우 설치할 앱의 버전 또는 업데이트할 앱을 선택할 수 있습니다.

업데이트 대상을 선택하지 않은 경우 가장 높은 버전이 사용됩니다.

Android는 앱을 다운그레이드할 수 없다는 점에 유의하세요. 또한 '버전 코드'에 따라 버전이 더 높은지, 더 낮은지 또는 동일한지 여부가 결정된다는 점에 유의하세요. 따라서 업데이트를 빌드할 때 앱에서 이 버전을 올바르게 높여야 합니다.

iOS

여기에서 개발한 iOS 앱을 업로드하고 나중에 장치 또는 그룹 프로필의 모바일 관리에서 배포할 수 있습니다.

"+"를 클릭하여 업로드하려는 앱의 IPA를 업로드합니다. 현재는 IPA 형식만 지원됩니다.

온프레미스 어플라이언스의 업로드 제한은 어플라이언스 구성의 3단계에서 늘릴 수 있습니다. Cloud에서 업로드 한도를 늘리려면 지원팀에 문의하여 자세한 내용을 확인하세요.

대상 업데이트

'업데이트 대상' 기능을 사용하면 앱에 대해 '최신 버전 유지'를 활성화한 경우 설치할 앱의 버전 또는 업데이트할 앱을 선택할 수 있습니다.

업데이트 대상을 선택하지 않은 경우 가장 높은 버전이 사용됩니다.

MacOS

여기에서 개발한 MacOS 앱을 업로드하고 나중에 장치 또는 그룹 프로필의 모바일 관리에서 배포할 수 있습니다.

"+"를 클릭하여 업로드하려는 앱의 PKG를 업로드합니다. 현재로서는 PKG 형식만 지원됩니다.

온프레미스 어플라이언스의 업로드 제한은 어플라이언스 구성의 3단계에서 늘릴 수 있습니다. Cloud에서 업로드 한도를 늘리려면 지원팀에 문의하여 자세한 내용을 확인하세요.

대상 업데이트

'업데이트 대상' 기능을 사용하면 앱의 '최신 버전 유지'를 활성화한 경우 설치할 앱의 버전을 선택하거나 앱을 업데이트할 버전을 선택할 수 있습니다.

업데이트 대상을 선택하지 않은 경우 가장 높은 버전이 사용됩니다.

Windows 10

여기에서 Windows 10 앱을 업로드하고 나중에 디바이스 또는 그룹 프로필의 모바일 관리에서 배포할 수 있습니다.

"+"를 클릭하여 업로드하려는 앱의 APPX, APPXBUNDLE 또는 MSI를 업로드합니다. 현재로서는 APPX, APPXBUNDLE 또는 MSI 형식만 지원됩니다.

또한 원하는 앱을 설치하기 전에 자동으로 배포 및 설치되는 앱의 종속성을 업로드하고 정의할 수도 있습니다.

온프레미스 어플라이언스의 업로드 제한은 어플라이언스 구성의 3단계에서 늘릴 수 있습니다. Cloud에서 업로드 한도를 늘리려면 지원팀에 문의하여 자세한 내용을 확인하세요.

대상 업데이트

'업데이트 대상' 기능을 사용하면 앱의 '최신 버전 유지'를 활성화한 경우 설치할 앱의 버전을 선택하거나 앱을 업데이트할 버전을 선택할 수 있습니다.

업데이트 대상을 선택하지 않은 경우 가장 높은 버전이 사용됩니다.

Win32 패키지(.exe)

.exe 파일/설치 프로그램을 장치에 배포할 수도 있습니다.

패키지 이름	MDM에 표시될 이름입니다.
설명	MDM에 표시되는 설명
패키지 파일	.zip 파일만 허용됩니다. 배포하려는 파일을 이 zip 파일에 넣습니다.
배포 컨텍스트	**System**: 설치 명령은 "사용자" 권한보다 높은 시스템 권한으로 실행됩니다. 또한 '시스템'을 사용하는 경우 프로세스에는 UI가 없으므로 무음으로 실행되며 사용자 프로필(예: %AppDat% 같은 환경 변수)에 액세스할 수 없습니다. **사용자**: 설치 명령은 사용자 프로필에 액세스할 수 있으며 필요한 경우 UI를 표시할 수 있습니다. 참고: 일부 프로세스는 하나의 컨텍스트에서만 작동할 수 있습니다. 예를 들어 소프트웨어가 앱데이터에 자체 설치되는 경우 "사용자"를 선택할 때만 작동합니다.
설치 명령	프로그램을 설치하는 데 사용되는 명령입니다. 예를 들어 루트에 "setup.exe"가 포함된 zip 파일의 설치 명령은 "/s" 매개 변수를 지원하며 자동 설치의 경우 설치 명령은 "setup.exe /s"가 됩니다. 소프트웨어마다 매개변수가 다를 수 있다는 점에 유의하세요.
제거 명령	MDM을 통해 소프트웨어를 제거하기 위해 실행할 명령입니다. 일반적으로 제거 프로그램을 가리킵니다. 예: "C:\프로그램 파일\예제 소프트웨어\uninstall.exe".
요구 사항	
참고: 소프트웨어를 설치하려면 설정된 모든 요구 사항을 충족해야 합니다. 그렇지 않으면 설치되지 않습니다. 일부 필드는 필수 항목일 수 있습니다. 요구 사항에 대해 설정된 값이 없으면 해당 요구 사항은 무시됩니다.	
OS 아키텍처	OS 아키텍처
최소 OS 버전	최소 OS 버전
최소 디스크 여유 공간(MB)	최소 디스크 여유 공간(MB)
최소 물리적 메모리(MB)	최소 물리적 메모리(MB)
최소 논리 프로세서 수	최소 논리 프로세서 수

최소 CPU 속도(MHz)	최소 CPU 속도(MHz)
추가 요구 사항	원하는 경우 여기에서 규칙을 수동으로 정의하거나 스크립트를 업로드하여 추가 요구 사항 검사를 수행할 수도 있습니다.
탐지 규칙	
감지 방법	여기에서 앱이 디바이스에 설치되었는지 여부를 감지하는 방법을 정의할 수 있습니다. 설치 명령은 이러한 규칙에 따라 앱이 설치되지 않은 것으로 감지되는 경우에만 실행됩니다. 제거 명령은 이러한 규칙에 따라 앱이 설치되지 않은 것으로 감지된 경우에만 실행됩니다. **수동으로 규칙 정의**: 하나 이상의 규칙을 수동으로 정의하여 특정 파일, 폴더, MSI 또는 레지스트리 키가 존재하는지 여부를 확인할 수 있습니다. 지정된 감지 규칙이 모두 참이면 앱이 있는 것으로 간주됩니다. **스크립트 사용**: 자체 검사가 포함된 자체 스크립트를 업로드하세요. 스크립트가 "$TRUE"를 반환하면 앱이 있는 것으로 간주됩니다.
탐지 규칙	

앱 설정

iOS 앱 설정

여기에서 필수 앱 또는 엔터프라이즈 앱 스토어에 앱을 추가하기 위한 기본 설정을 정의할 수 있습니다.

참고: 앱을 추가할 때 기본적으로 선택되는 항목만 설정합니다. 필수 앱 또는 기업 앱 스토어에 이미 추가된 앱의 기존 설정은 변경되지 않습니다.

최신 정보 확인	앱을 자동으로 최신 상태로 유지합니다. 업데이트가 릴리스된 후 앱이 업데이트될 때까지 최대 7일이 소요될 수 있다는 점에 유의하세요.
관리되지 않는 경우 추월	앱이 이미 (사용자에 의해) 관리되지 않는 상태로 설치되어 있는 경우 해당 앱은 MDM에 의해 추월되어 관리됩니다.
MDM 프로필이 제거되면 앱 제거	MDM이 제거되면 앱을 제거합니다.
앱 데이터 백업 방지	앱 데이터의 백업을 방지합니다.

Android 앱 설정

여기에서 필수 앱 또는 엔터프라이즈 앱 스토어에 앱을 추가하기 위한 기본 설정을 정의할 수 있습니다.

참고: 추가할 때 기본적으로 선택되는 항목만 설정합니다. 필수 앱 또는 기업 앱 스토어에 이미 추가되어 있는 앱의 설정은 변경되지 않습니다.

최신 정보 확인	앱을 자동으로 최신 상태로 유지합니다. 사내 앱에서만 사용할 수 있습니다.
AppTec360 EMM 클라이언트 업데이트 제어	이 기능을 활성화하면 관리자가 AppTec360 EMM 클라이언트의 업데이트 대상을 지정할 수 있습니다. "일반 설정" → "앱 관리" → "사내 앱 DB" → "안드로이드"에 사용 가능한 모든 버전의 AppTec360 EMM 클라이언트 목록이 표시됩니다.

타사 앱

Android

여기에서 이카루스 활성화 코드를 설정할 수 있습니다.

이를 '활성화 코드 사용'으로 설정하고 여기에 활성화 코드를 입력합니다.

참고: 코드를 입력하고 저장해도 디바이스로 전송되는 프로필에 코드가 아직 추가되지 않습니다. 코드를 프로필에 추가하려면 프로필에서 변경 작업을 수행해야 합니다. 예를 들어 프로필의 스위치를 끄기 → 켜기 → 끄기 - 저장 → 지금 할당으로 변경합니다.

iOS

여기에서 SecurePIM 라이선스를 입력할 수 있습니다. 라이선스를 입력한 후 '변경사항 저장'을 누르면 SecurePIM 옵션을 사용할 수 있습니다.

VPP/녹스 프리미엄

Apple 볼륨 구매 프로그램(VPP)을 사용하면 유료 및 무료 앱을 기기에 쉽게 배포할 수 있습니다. 기기에서 Apple ID가 필요하지 않고, 사용자가 설치를 확인(감독)할 필요가 없으며, 사용자가 Apple ID의 비밀번호를 입력할 필요가 없고, 모든 기기에서 유료 앱을 다시 구매하지 않고도 쉽게 배포할 수 있으므로 적극 권장합니다.

VPP를 사용하려면 Apple 비즈니스 관리자에 등록해야 합니다.

VPP 라이선스

여기에서 VPP 앱에 대한 개요, 사용 중인 라이선스 수 및 사용 가능한 라이선스 수를 확인할 수 있습니다.

휠을 클릭하면 라이선스가 할당된 장치와 이 할당의 상태를 확인할 수 있습니다.

를 클릭하면 VPP 캐시가 새로 고침되어 MDM에 할당된 라이선스와 Apples 측에 할당된 라이선스를 비교합니다. 이렇게 하면 경우에 따라 라이선스 문제가 해결될 수 있습니다.

VPP 토큰

여기에서 Apple 비즈니스 관리자의 설정 → 앱 및 책에서 찾을 수 있는 VPP 토큰을 업로드할 수 있습니다. 여러 개의 VPP 토큰을 업로드할 수 있습니다.

Apple 비즈니스 관리자에서 새 토큰을 다운로드하고 '편집' 휠을 클릭한 다음 새 토큰을 업로드하기만 하면 토큰을 갱신할 수 있습니다.

"VPP 모드"는 라이선스 할당 처리 방법을 결정합니다. 시나리오에 따라 다른 모드를 사용해야 합니다:

'장치 기반'은 QR코드, 링크, Apple Configurator 또는 DEP를 통해 장치를 등록할 때 사용해야 합니다.

"장치가 사용자 등록 또는 공유 iPad로 등록되어 있는 경우 '사용자 기반'이 필요합니다.

'자동화된 라이선스 관리'를 활성화하면 한 그룹에서 다른 그룹으로 이동한 사용자에게 이동한 그룹 프로필에 따라 Apple VPP 라이선스가 자동으로 할당됩니다.

이전한 그룹의 기존 Apple VPP 라이선스는 취소되지 않습니다.

그룹에 추가된 새 사용자에게는 해당 그룹 프로필에 따라 Apple VPP 라이선스가 자동으로 할당됩니다.

KNOX 프리미엄 키

여기에서 KNOX 프리미엄 키를 입력하여 삼성 KNOX 컨테이너를 사용할 수 있습니다.

이 기능은 Android 10부터 더 이상 지원되지 않는다는 점에 유의하세요. 대신 Android Enterprise 컨테이너를 사용하세요.

앱 스토어 설정

지역 및 언어

여기에서 앱 관리에서 앱 검색의 기본 언어 및 지역을 설정할 수 있습니다.

iTunes의 설정은 시스템이 특정 앱에 대한 정보를 가져오는 방법도 정의한다는 점에 유의하십시오. 목록에 이상한 방식으로 표시되는 앱(예: 아이콘이 없는 경우)이 있는 경우 특정 앱을 사용할 수 없는 지역을 설정했을 수 있습니다.

AE Play 스토어

여기에서 Android 기업용 기기용 Play 스토어에 대한 모든 옵션을 확인하여 앱을 승인하고, 자체 앱을 Play 스토어에 업로드하거나, 자체 웹 앱을 만들 수 있습니다.

승인된 앱

여기에서 승인한 모든 앱에 대한 개요를 확인할 수 있습니다.

Play 스토어 앱

그러면 Play 스토어가 표시된 아이프레임이 로드됩니다. 원하는 앱을 검색하여 클릭하고 승인합니다. 앱을 승인하는 동안 필요한 권한이 변경되는 경우 승인이 취소되도록 정의할 수도 있습니다. 앱을 승인할 때는 이러한 설정을 기본값으로 두는 것이 좋습니다.

앱이 승인되면 프로필에 앱을 추가할 수 있습니다.

승인 후에는 '승인' 버튼이 '승인 취소'로 변경되므로 더 이상 필요하지 않은 앱은 언제든지 삭제할 수 있습니다.

비공개 앱

여기에서 나만의 앱을 비공개 앱으로 구글 플레이 스토어에 업로드할 수 있습니다. 이렇게 하면 Google 서비스를 통해 앱을 배포하고 이를 통해 업데이트할 수 있습니다. 또한 일반적으로 필요한 사용자 확인 없이 앱을 설치할 수 있다는 장점도 있습니다.

웹 앱

여기에서 앱처럼 할당할 수 있는 특정 웹 페이지에 대한 링크인 웹 앱을 만들 수 있습니다.

사용자 지정 아이콘을 지정하고 정확히 표시되는 방식을 추가로 정의할 수도 있습니다.

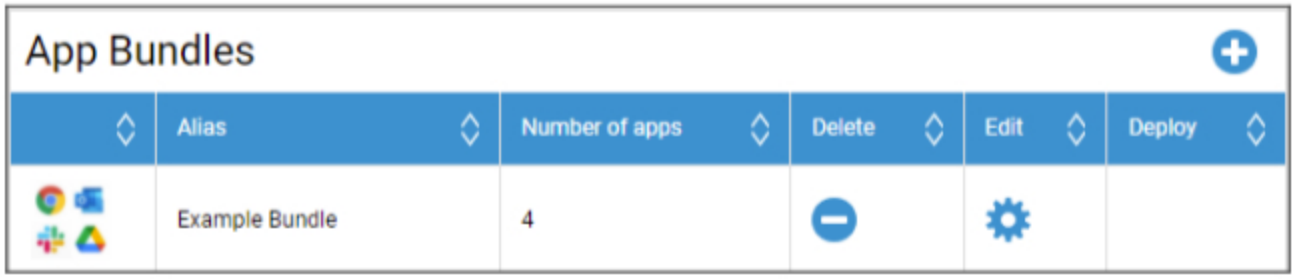
스토어 레이아웃

스토어 레이아웃은 Play 스토어에 앱이 표시되는 방식 또는 아예 표시되는지 여부를 정의합니다.

사용자가 수동으로 설치할 수 있도록 Play 스토어에 앱을 표시하려면 여기에 레이아웃 **및** 프로필에서 엔터프라이즈 Play 스토어에 추가해야 합니다. 둘 중 하나에만 앱을 추가하면 앱이 표시되지 않습니다.

앱 번들

앱 번들을 사용하면 클릭 한 번으로 디바이스 또는 그룹 프로필에 할당할 수 있는 앱 그룹을 정의할 수 있습니다.



"+"를 클릭하여 새 앱 번들을 생성합니다. 앱 번들을 생성한 후 "편집"을 클릭하여 다양한 소스의 앱을 번들에 추가할 수 있습니다.

번들은 다른 모든 앱과 마찬가지로 프로필에 추가할 수 있습니다. 앱을 추가할 때 번들이 있는 '앱 번들'이라는 탭이 추가로 표시됩니다.

앱 번들을 변경하면 '배포' 열에 버튼이 나타납니다. 이 버튼을 사용하면 해당 번들을 포함하는 모든 프로필에 변경 사항을 푸시할 수 있습니다. 따라서 번들에서 앱을 추가하거나 제거한 후에는 이 작업을 수동으로 수행해야 한다는 점에 유의하세요.

원격 제어

TeamViewer

TeamViewer 커넥터

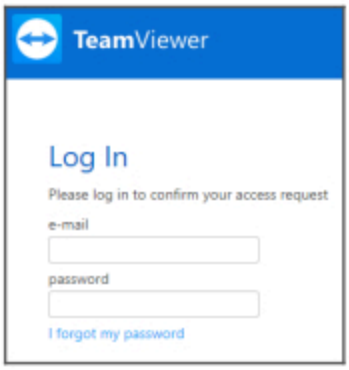
참고: 클라우드 버전의 무료 평가판에서는 TeamViewer 계정을 연결할 수 없습니다. 대신 무료 데모 계정이 자동으로 연결됩니다.

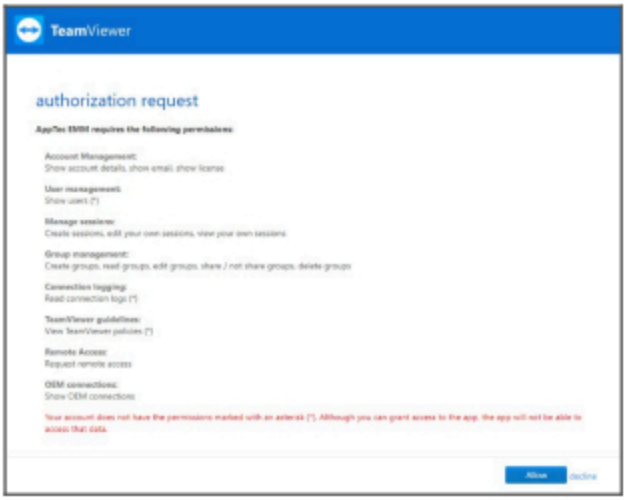
일반 설정 -> 원격 제어 -> TeamViewer로 이동합니다. 여기에서 TeamViewer 계정을 콘솔과 연결하거나 현재 연결된 계정에 대한 정보를 볼 수 있습니다. 또한 "활성 세션"으로 이동하면 현재 활성화된 모든 세션을 볼 수 있습니다.

계정을 연결하려면 '설정 시작'을 클릭합니다.

이렇게 하면 새 페이지로 이동하여 TeamViewer 계정으로 로그인해야 합니다.

로그인 후 AppTec360 MDM이 이 계정을 사용할 수 있도록 권한을 부여합니다. 이를 확인한 후 몇 초간 기다리면 계정이 연결됩니다.


TeamViewer
Log In
Please log in to confirm your access request
e-mail
password
I forgot my password


TeamViewer
authorization request

TeamViewer 퀵서포트 설치

장치 프로필 또는 그룹 프로필의 필수 앱에 "TeamViewer QuickSupport" 앱을 추가하고 "지금 할당"을 클릭합니다. 앱이 장치에 설치될 때까지 기다립니다.

앱이 설치되어 있지 않은 디바이스에서 액세스를 시도하면 디바이스 구성에 따라 앱이 설치되거나 설치하라는 메시지가 표시됩니다.

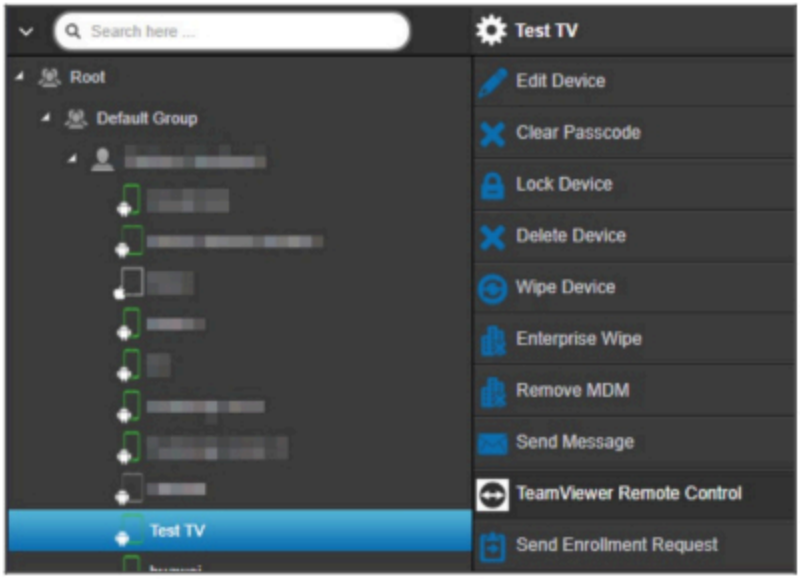
디바이스 원격 제어

장치를 원격 제어하려면 장치를 선택하고 휠을 클릭한 다음 "TeamViewer 원격 제어"를 선택하세요.

이미 활성 세션이 있는 경우 이전 세션을 사용하거나 새 세션을 만들 수 있습니다.

새 TeamViewer 세션을 만들 것인지 확인합니다.

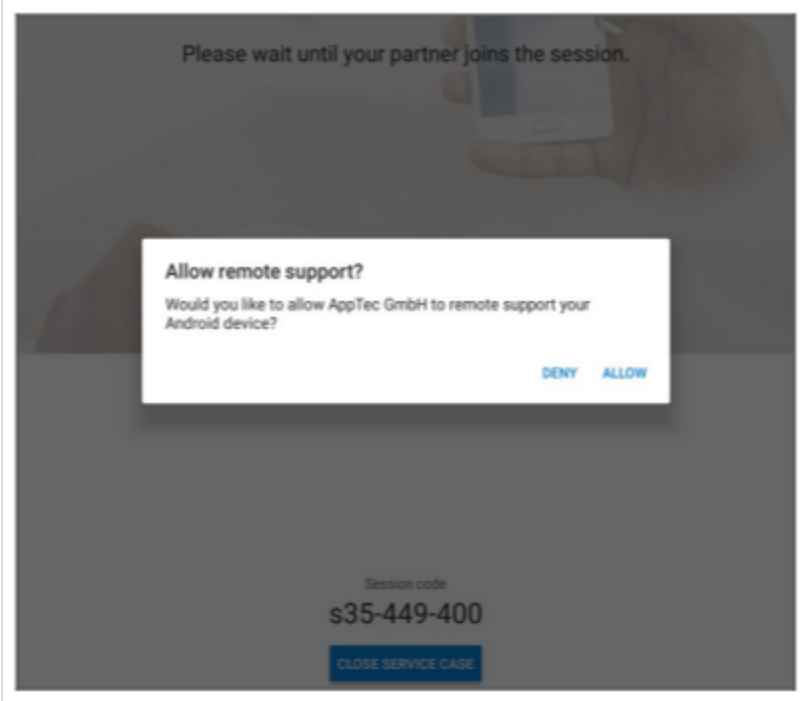
몇 초 후 TeamViewer 세션에 대한 링크가 표시됩니다. "시작"을 클릭하여 이 링크를 새 창에서 열 수 있습니다.


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

이 링크를 클릭하면 설치된 TeamViewer가 열리고 장치에 연결됩니다.

이제 원격 제어를 위해 장치 자체에서 연결을 확인해야 합니다.

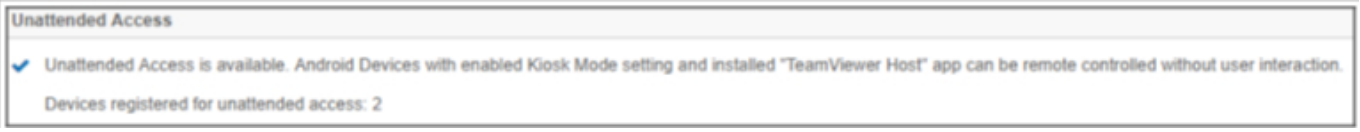


iOS를 사용하는 경우 AppTec360 MDM 클라이언트에 메시지가 표시됩니다. 해당 링크를 통해 기기가 원격 세션에 참여하게 됩니다. 장치의 알림 설정에 따라 알림을 받지 못하고 AppTec360 MDM 클라이언트를 수동으로 열어야 할 수도 있습니다.

일부 Android 기기(예: 삼성)에서는 추가 앱을 애드온으로 설치해야 합니다. 장치에서 필요한 경우 장치의 TeamViewer 앱에서 이에 대해 알려줍니다.

무인 액세스

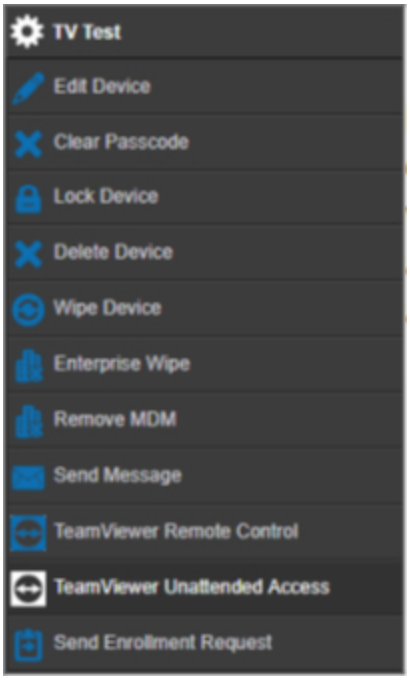
참고: 무인 액세스는 Android 디바이스에서만 가능합니다.



팀뷰어 계정에서 "텐서" 또는 "기업용" 라이선스를 사용하는 경우에만 장치에서 연결을 수락하지 않고 장치에 연결할 수 있습니다.

계정 연결 후 '일반 설정'에서 확인할 수 있습니다.

무인 액세스를 사용하려면 "TeamViewer Host" 앱을 설치하고 프로필의 "키오스크 모드 및 런처"에서 "무인 액세스 사용"을 활성화해야 합니다. 이 기능은 키오스크 모드를 사용하는 경우에만 가능하다는 점에 유의하세요.



이제 디바이스를 선택하고 휠을 클릭하면 무인 액세스를 선택할 수 있습니다. 그러면 디바이스 자체에서 확인할 필요 없이 디바이스에 연결됩니다. 장치에 액세스할 수 있는 링크를 받을 때까지 다소 시간이 걸릴 수 있다는 점에 유의하세요.

스플래시탑

스플래시탑 옵션을 활성화하면 프로필에 스플래시탑 구성 옵션이 표시됩니다.

스플래시탑을 사용하려면 프로필에서 스플래시탑 스트리머(com.splashtop.streamer.csrs)를 필수 앱으로 설정해야 합니다. 그런 다음 프로필의 '원격 제어'에서 스플래시탑 구성을 활성화할 수 있습니다. 이 기능을 활성화하면 스플래시탑 스트리머 앱이 구성됩니다. 스플래시탑 스트리머를 사용하지만 MDM과 함께 사용하지 않는 경우에는 이 옵션을 해제해야 합니다.

프로필의 '원격 제어' 아래에서 배포 코드도 설정해야 합니다. https://my.splashtop.com 으로 이동하여 Splashtop 계정에 로그인합니다. "컴퓨터 추가"를 클릭하고 결과 페이지에서 12자리 배포 코드를 복사합니다.

배포 코드가 없으면 원격 제어가 불가능합니다.

그런 다음 장치를 마우스 오른쪽 버튼으로 클릭하고 "스플래시톱 원격 제어"를 클릭하여 원격 세션을 시작할 수 있습니다.

심카드 관리

CSV 대량 가져오기

여기에는 할당된 Sim 카드에 대한 개요와 모든 정보가 표시됩니다. 이를 통해 디바이스뿐만 아니라 심 카드에 대한 모든 정보를 하나의 시스템에서 확인할 수 있습니다.

참고: 이 데이터는 수동으로 관리/문서화해야 합니다. 운영 체제의 개인정보 보호/보안 메커니즘으로 인해 디바이스에서 이 데이터를 자동으로 가져올 수 없습니다.

이 목록을 CSV로 내보내고 가져올 수도 있습니다.

이동 통신사 및 관세

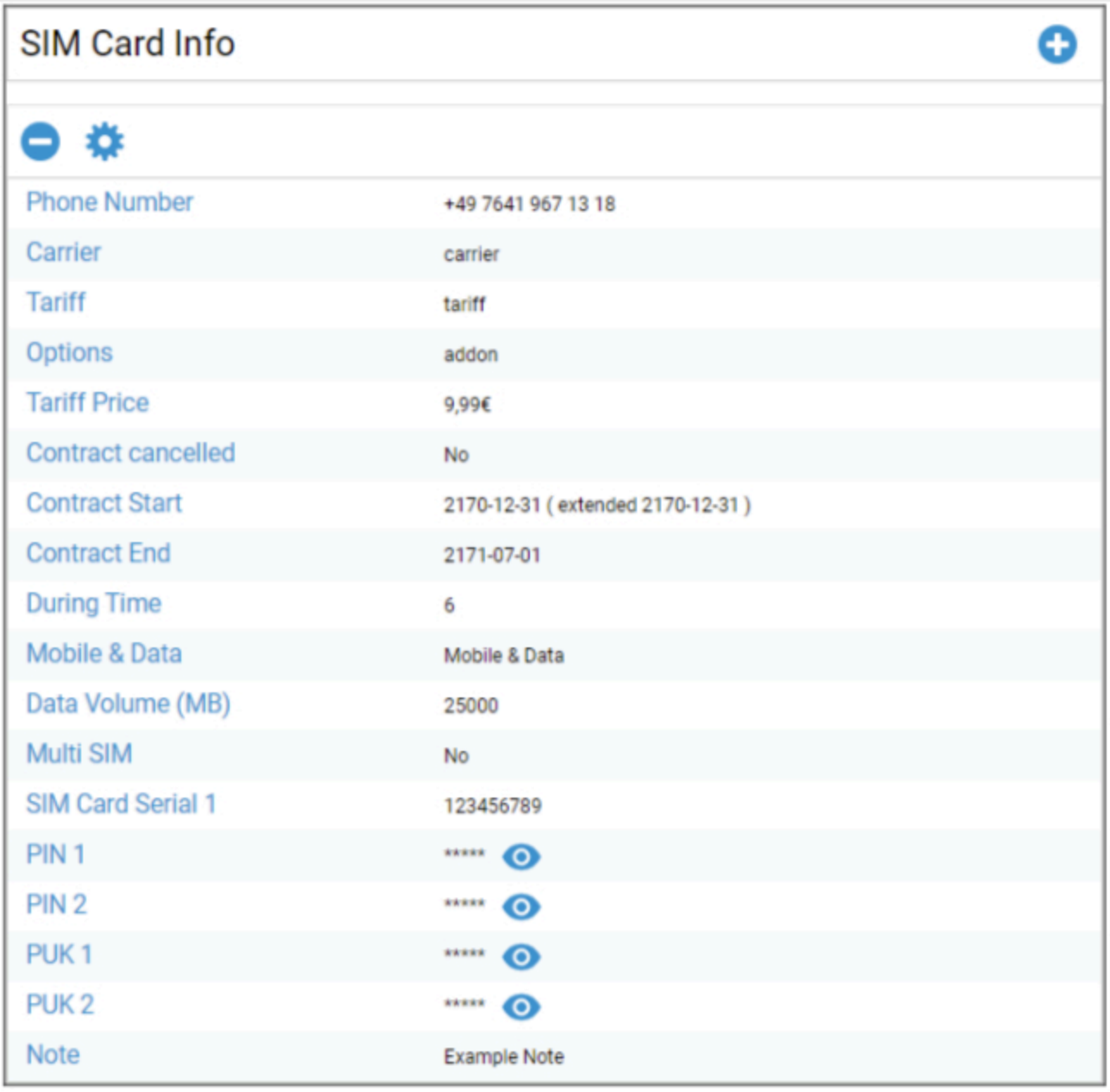
Sim 카드를 추가하려면 먼저 버튼을 클릭하여 하나 또는 여러 개의 이동 통신사를 추가하세요.

그런 다음 '관세 정보'에서 '+'를 클릭하여 배송업체에 관세를 추가합니다.

원하는 경우 아래에 선택적 애드온을 추가할 수 있습니다.

이로써 실제 심 카드를 추가하는 데 필요한 모든 것이 준비되었습니다. 심 카드는 현재 사용자에게 할당되어 있습니다. 따라서 모바일 관리로 이동하여 사용자를 선택한 다음 'Sim 카드 개요'로 이동합니다.

여기에 이 사용자의 심 카드가 표시됩니다. 심 카드가 있는 경우 편집하거나 제거할 수 있습니다. 사용자는 여러 개의 Sim 카드를 가질 수 있습니다.

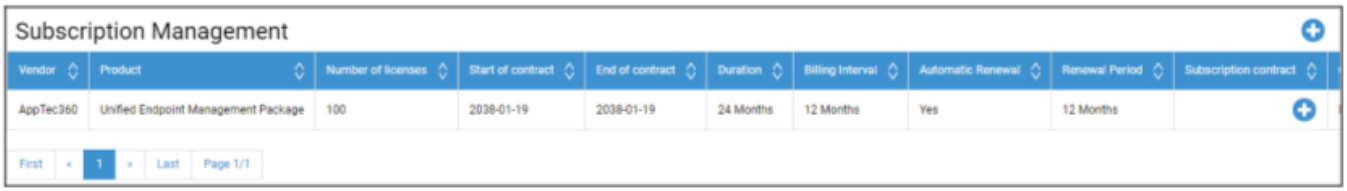


"+"를 클릭하여 Sim 카드를 추가하고 필요한 모든 정보를 추가합니다. 이 심 카드는 일반 설정 → 심 카드 관리의 모든 심 카드 목록에도 표시됩니다.

구독 관리

구독 관리

여기에서 진행 중인 구독과 세부 정보를 문서화하고 서명된 계약서, 해지 통지서 등 다양한 파일을 저장할 수 있습니다. 또한 구독이 종료되기 전에 메일별로 알림을 보내거나 자동으로 연장되도록 미리 알림을 설정할 수도 있습니다.



상단의 '+'를 클릭하여 구독을 추가합니다. 원하는 만큼 구독을 추가할 수 있습니다.

이 구독과 관련된 파일을 업로드하려면 다른 필드에서 '+'를 클릭합니다. 기술적으로는 모든 파일 유형을 업로드할 수 있지만 브라우저에서 모든 파일 유형을 미리 볼 수 있는 것은 아니라는 점에 유의하세요.

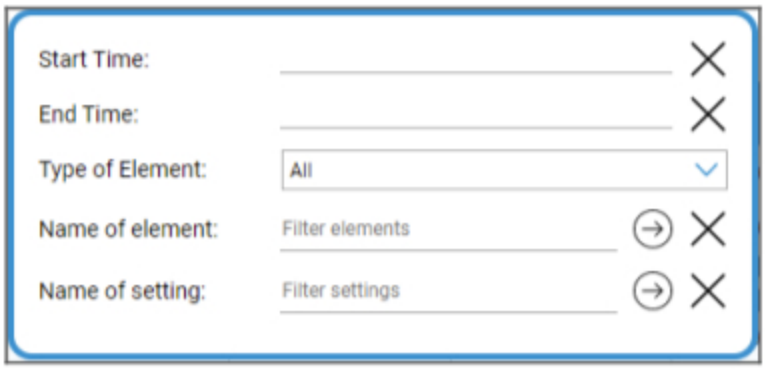
일반 감사 로그

감사 로그

여기에는 모든 변경 사항이 표시되는 일반 감사 로그가 있습니다. 사용자 또는 그룹의 감사 로그에는 해당 사용자 또는 그룹에 따른 변경 사항만 표시되지만 여기에는 콘솔의 모든 곳에서 이루어진 모든 변경 사항이 표시됩니다.

누가, 언제, 어디서, 무엇을 변경했는지 확인할 수 있습니다. 경우에 따라 항목을 확장하여 자세한 내용을 볼 수도 있습니다.

사용자 또는 '경로/유형'의 항목을 클릭하여 변경이 이루어진 위치로 이동할 수 있습니다.



오른쪽 상단에서는 많은 변화가 일어나는 환경에서 특정 변경 사항을 찾는 데 도움이 되는 필터를 정의할 수도 있습니다.

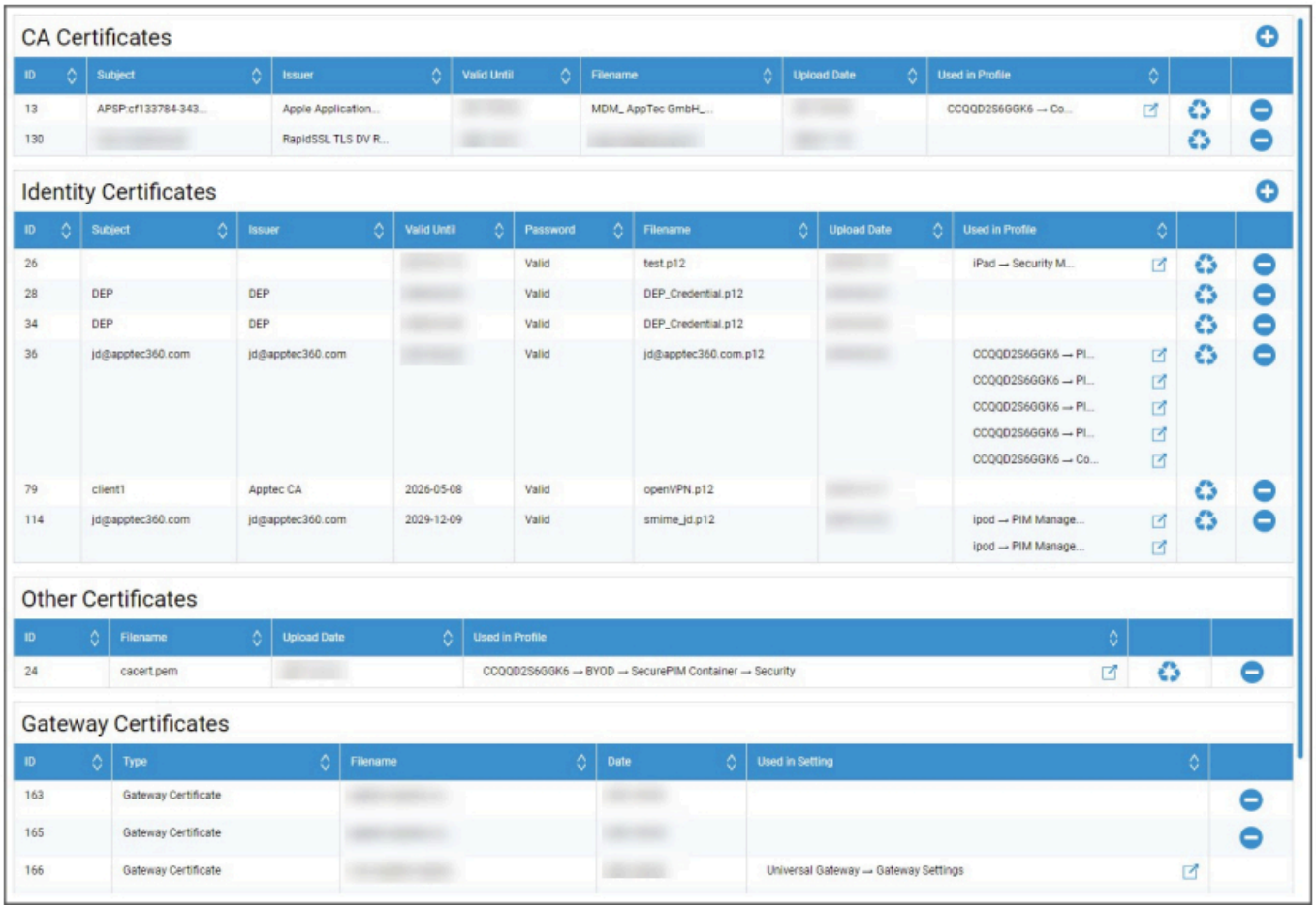
감사 로그 설정

'감사 로그 보존 기간'은 감사 로그를 삭제하기 전에 얼마나 오래 보관해야 하는지를 정의합니다.

인증서 관리

여기에서 콘솔에서 업로드하고 사용하는 모든 인증서에 대한 개요를 볼 수 있습니다. 이것은 개요일 뿐입니다. 예를 들어 Wi-Fi 인증서에 대한 실제 구성은 여전히 해당 위치의 프로필에서 이루어집니다.

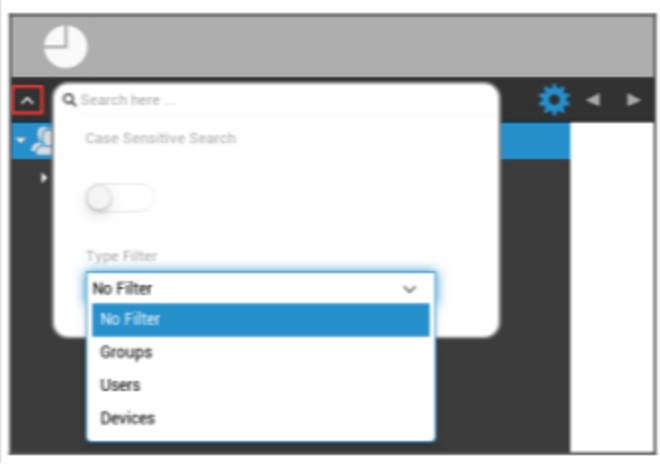
여기에서 인증서를 제거하거나 업데이트할 수도 있으며, 이는 영향을 받는 프로필에 자동으로 반영됩니다. '프로필에서 사용됨'의 정보를 클릭하여 인증서가 아직 할당된 정확한 위치를 확인합니다.



모바일 관리

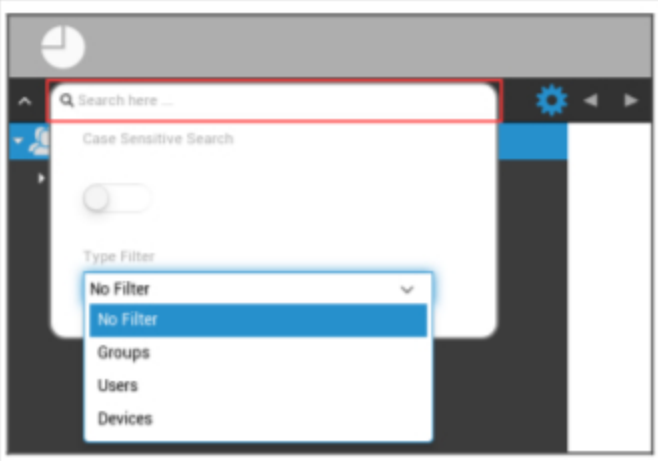
모바일 관리 화면

디바이스 필터



화면 왼쪽 상단을 클릭하면 디바이스 표시를 위한 다양한 필터를 찾을 수 있습니다.

검색 창



검색 창에서는 특정 키워드로 모든 디바이스 및/또는 사용자를 검색할 수 있습니다.

옵션 기어

각 기호를 클릭하면 사용 가능한 옵션 목록이 표시됩니다.

이는 현재 창마다 변경되며 각 장에서 설명합니다.

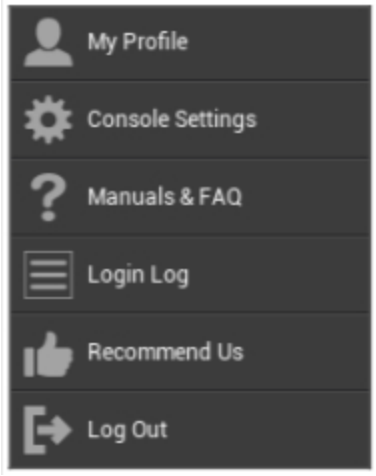
탐색 화살표

왼쪽 화살표를 클릭하면 이전 페이지로 이동합니다.

그 후 오른쪽 화살표를 클릭하면 방금 떠났던 페이지로 이동합니다.

관리 계정 설정

위와 같이 이메일 주소를 클릭하면 다음 메뉴가 표시됩니다:



내 프로필	관리자 계정 세부 정보 수정
콘솔 설정	관리자 계정에 대한 콘솔 설정 구성하기
매뉴얼 및 FAQ	'일반 설정'에서 '매뉴얼 및 FAQ' 페이지 보기
로그인 로그	"로그인 로그"에 액세스
추천하기	'일반 설정'에서 '추천하기' 페이지 보기
로그아웃	MDM 콘솔에서 로그아웃

사용자 정보

여기에서 현재 로그인한 관리자의 계정 세부 정보를 수정할 수 있습니다.

사용자 이름	계정의 사용자 이름 및/또는 이메일 주소
이름	관리자 이름
성	관리자 성
로그인 이름	관리자 로그인 이름
이메일 주소	관리자 이메일 주소
대체 이메일 주소	관리자 대체 이메일 주소
사진	프로필 사진
전화번호	관리자 전화번호
휴대폰 번호	관리자 휴대폰 번호
전화 내선 번호	전화 내선 번호
위치	위치
위치	회사 내 직급
사용자 그룹	관리자 계정을 할당할 사용자 그룹을 선택합니다.
댓글	댓글 입력
새 비밀번호 입력	비밀번호 변경 시 비밀번호를 입력합니다.
새 비밀번호 반복하기	새 비밀번호를 반복하여 확인합니다.

관리 액세스 권한은 계층 구조에서 로컬 사용자 계정으로 제출할 수도 있습니다. 추가 관리자를 설정하지 않는 한 이 계정을 삭제해서는 안 됩니다!

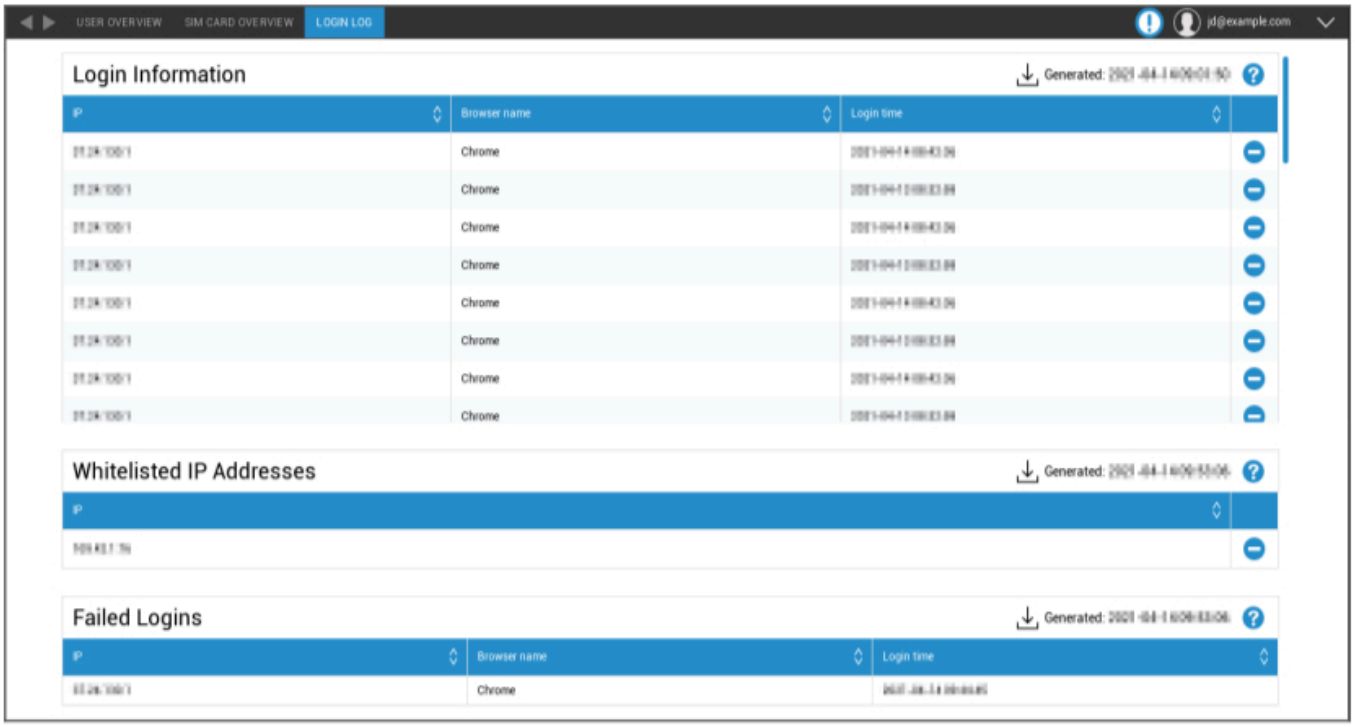
콘솔 설정

여기에서 관리자 계정에 대해 다음과 같은 콘솔 설정을 구성할 수 있습니다:

디렉토리 사용자 표시 옵션	트리에서 사용자에게 라벨을 지정하는 방법 정의하기
디렉토리 장치 표시 옵션	트리에서 디바이스에 레이블을 지정하는 방법 정의하기
세션 시간 초과	사용자가 지정된 시간 동안 아무 작업도 하지 않으면 로그아웃됩니다. 기본값은 60분입니다. 이 설정을 변경한 후 로그아웃했다가 다시 로그온하세요.
시간대	사용할 표준 시간대 선택
시간 형식	타임스탬프 표시 방법 선택
콘솔 언어	콘솔을 표시할 언어를 선택합니다. 영어와 독일어를 사용할 수 있습니다.
주요 색상	콘솔의 색 구성표에 기본으로 사용할 색상을 설정할 수 있습니다. 색상 선택기를 사용하거나 HTML HEX 표기법으로 색상을 입력할 수 있습니다. '분홍색', '노란색'과 같은 RGB 포뮬러도 작동합니다.
저장 명령	'저장' 버튼을 누르지 않고 저장을 트리거하는 키 조합입니다.
2단계 인증 사용	로그인할 때 2단계 인증을 사용하도록 설정합니다. 로그인하면 로그인할 때 입력해야 하는 코드가 포함된 이메일을 받게 됩니다.
2단계 인증 시간 초과	이미 인증에 성공한 후 2단계 인증을 요청하지 않는 기간을 설정합니다.
다음을 통해 인증 코드 보내기	인증 코드가 선택한 옵션으로 전송됩니다. 기기 메시지는 본인 소유의 모든 Android 및 iOS 기기의 AppTec360 MDM 앱에 표시됩니다.
로그인 후 로그인 메시지 보내기	활성화하면 화이트리스트에 포함되지 않은 IP 주소에서 로그인할 때마다 이메일이 전송됩니다. 이메일에는 로그인에 대한 정보(예: IP, 브라우저)가 포함되어 있습니다.

로그인 로그

여기에서 현재 로그인한 관리자 계정의 로그인 관련 정보를 볼 수 있습니다.



로그인 정보	콘솔에 기록된 현재 로그인한 관리자 계정의 로그인이 포함된 목록입니다. 이 목록에는 지난 30일 동안 로그인에 성공한 모든 내역이 표시됩니다.
화이트리스트 IP 주소	화이트리스트에 등록된 모든 IP 주소의 목록입니다. 여기에 나열된 IP에서 로그인하면 로그인 메시지가 표시되지 않습니다. 위의 '로그인 정보' 목록에서 항목 옆에 있는 버튼을 클릭하여 이 목록에 IP 주소를 추가할 수 있습니다. 이 목록 또는 위의 '로그인 정보' 목록에 있는 항목 옆의 버튼을 클릭하여 이 목록에서 IP 주소를 제거할 수 있습니다.
로그인 실패	지난 30일 동안 실패한 모든 로그인 시도의 목록입니다. 20분 동안 올바른 비밀번호를 3번 이상 입력하지 못한 경우 이 목록에 항목이 표시됩니다. 또한 로그인 시도가 실패하면 이메일을 통해 알림을 받게 됩니다.

모바일 관리의 기업 관리(루트-노드)

루트 노드(첫 번째 그룹)에 도달하면 모바일 관리와 관련하여 회사에 대한 다양한 설정을 수행할 수 있습니다.

하위 그룹 만들기	하위 그룹 만들기
루트 노드 이름 바꾸기	루트 노드 이름 변경(예: 회사 이름)
대량 등록	여러 디바이스/사용자를 동시에 등록하기
대량 할당	한 번에 각 그룹에 프로필을 할당하세요.
빠른 앱 관리	각 그룹 장치에 애플리케이션에 대한 설치 요청을 (언)설치 요청 보내기
CSV 사용자 가져오기	CSV에서 해당 그룹으로 사용자 가져오기

하위 그룹 만들기

'하위 그룹 만들기'를 사용하면 추가 하위 그룹을 만들 수 있습니다.

하위 그룹을 할당할 그룹을 설정할 수 있습니다.

(기본적으로 루트 노드에 하위 그룹으로 할당되는 새 그룹이 생성됩니다.)

루트 노드 이름 바꾸기

여기에서 루트 이름을 변경할 수 있습니다. 이 경우 회사 이름을 사용하는 것이 일반적입니다.

대량 등록

'대량 등록'을 사용하면 여러 장치와 사용자를 등록할 수 있습니다.

사용자가 등록을 수신할 방식(이메일, 대체 이메일, SMS)을 직접 선택할 수 있습니다.

사용자가 수신할 디바이스(iOS, Android, Windows Phone)에 따라 여기에 직접 표시할 수 있습니다.

스마트폰인지 태블릿인지의 구분도 여기에서 구성할 수 있으며, 확인 표시를 통해 올바르게 선택해야 합니다.

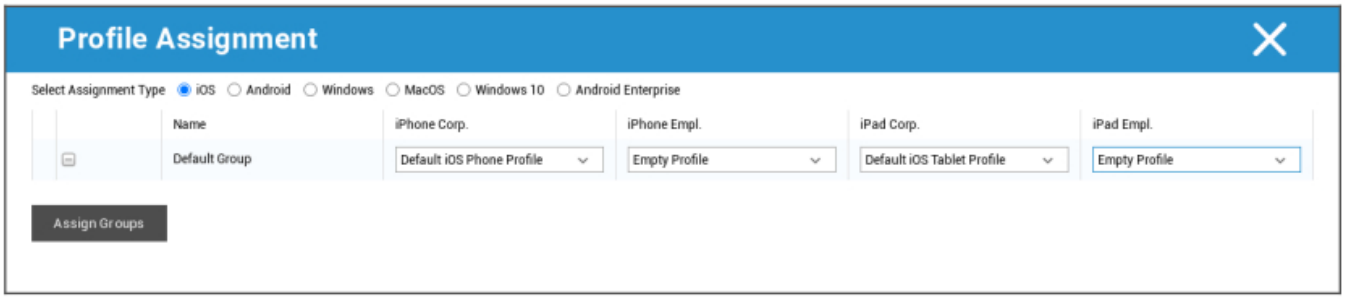
마지막 단계로 각 디바이스가 회사 디바이스인지 개인 디바이스(BYOD)인지 설정할 수 있습니다.

"CSV로 내보내기"를 사용하면 정보를 CSV 데이터 파일로 내보낼 수 있습니다. 반대로 "CSV 가져오기"를 사용하여 CSV 데이터 파일을 가져올 수도 있으며, 파일은 아래 예시와 같아야 합니다:

필립 라이스, philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;

대량 할당

대량 할당에서는 모든 그룹에 프로필을 할당할 수 있으며, 이는 iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise로 나뉩니다.

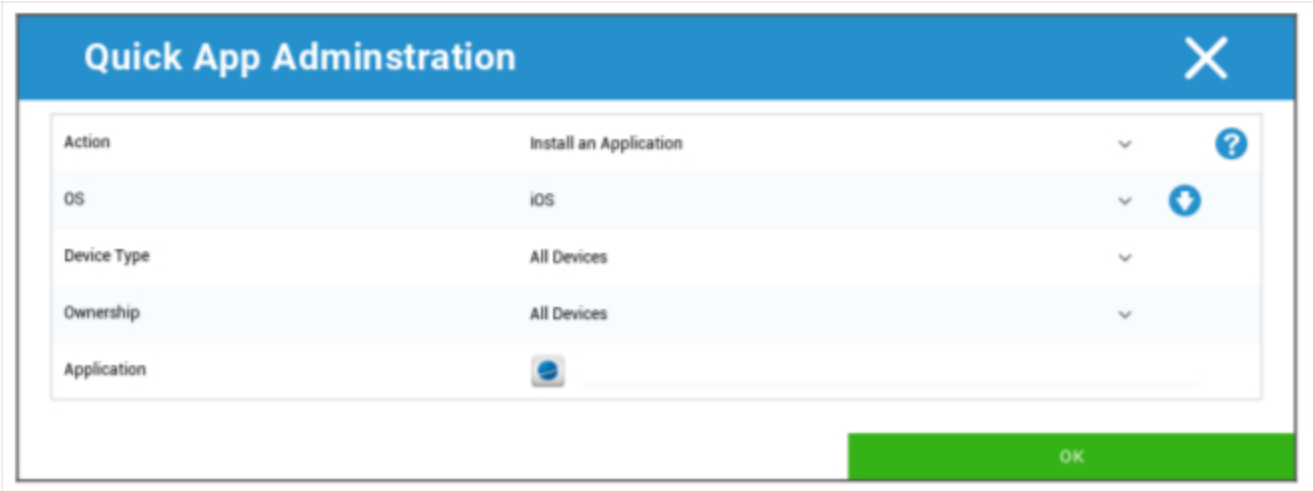


윈도우 - MacOS - 윈도우 10 - 안드로이드 엔터프라이즈

빠른 앱 관리

빠른 앱 관리에서 특정 애플리케이션에 대한 설치 또는 제거 요청을 원하는 OS로 보낼 수 있습니다.

또한 선택한 OS의 모든 디바이스 유형으로 요청을 보낼지 아니면 특정 디바이스 유형으로만 보낼지 정의할 수도 있습니다.



CSV 사용자 가져오기

CSV에서 해당 그룹으로 사용자를 가져옵니다.

'CSV 템플릿 다운로드'를 사용하면 CSV 템플릿 파일을 내보낼 수 있으며, 이를 입력하거나 참조용으로 사용할 수 있습니다.

'역할 아이디 표시' 및 '그룹 아이디 표시' 옵션을 참조로 사용하여 자신만의 CSV 파일을 만들 수도 있습니다.

CSV 파일은 "CSV 업로드"를 사용하여 MDM에 업로드할 수 있습니다.

마지막 단계로 '가져오기 시작'을 클릭하여 가져오기를 시작할 수 있습니다.

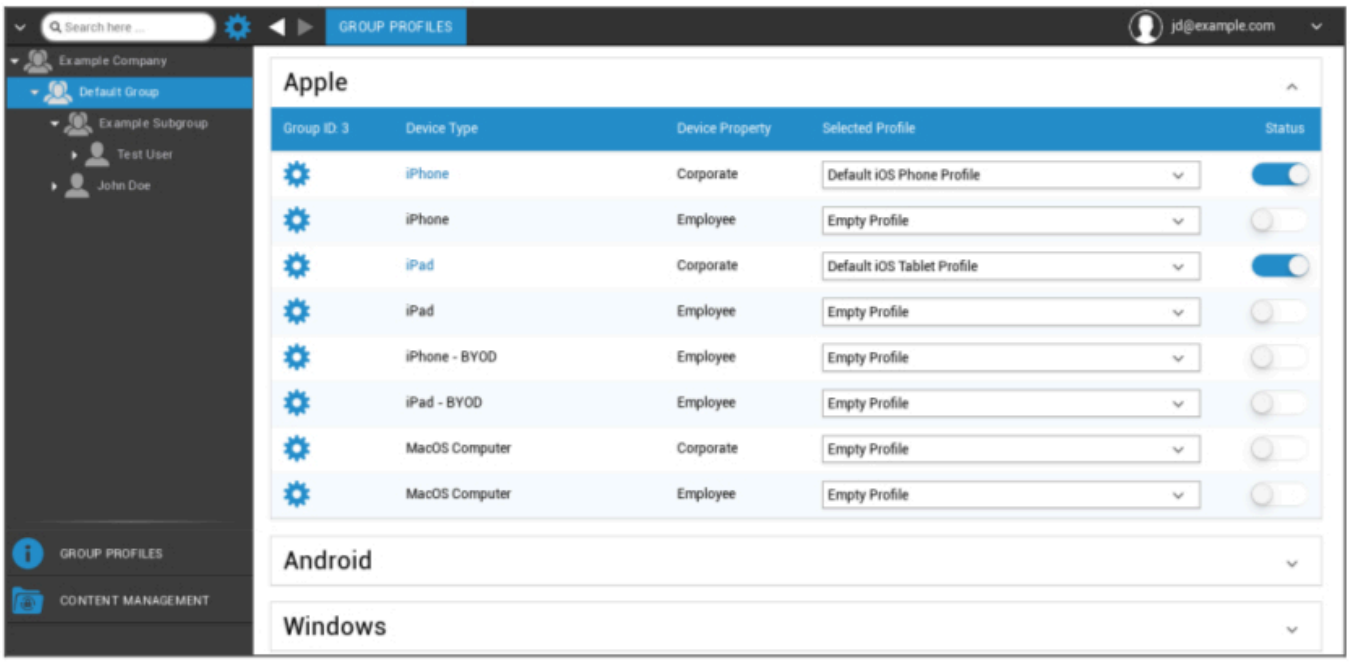
모바일 관리의 그룹 관리

개요를 한 번 클릭하면 각 플랫폼에 대한 다양한 구성 프로필이 표시됩니다.

하나의 프로필에는 최종 사용자 디바이스에서 AppTec360으로 미리 설정할 수 있는 모든 설정 옵션이 포함되어 있습니다. 각 플랫폼에서 기업용 디바이스(기업) 또는 개인 디바이스(직원) 디바이스에 대한 프로필을 만들 수 있습니다.

예를 들어 위치나 기능에 따라 디바이스 그룹의 구성을 차별화하려면 여러 개의 하위 그룹을 만드는 것이 좋습니다.

모바일 관리의 프로필 관리에 유의하세요.



기어 메뉴를 사용하여 각 (하위) 그룹에 대한 다양한 설정을 설정할 수 있습니다.

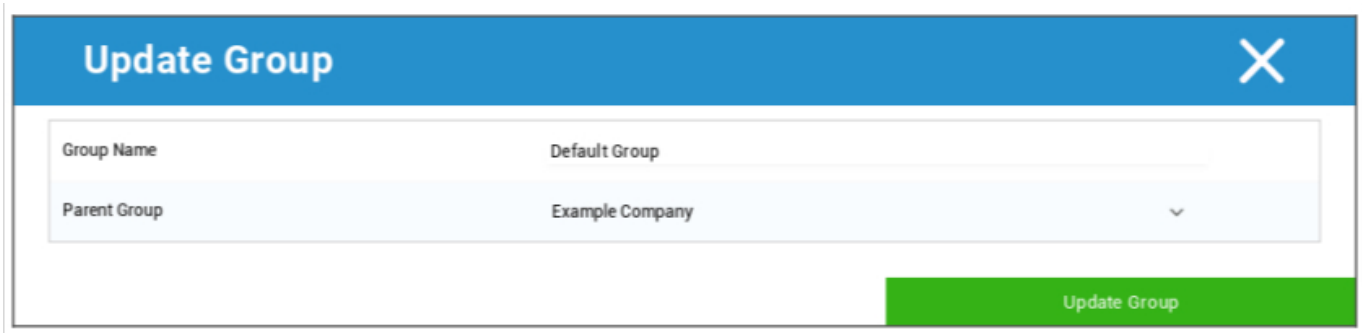
하위 그룹 만들기	해당 (하위) 그룹에 대한 하위 그룹 만들기
선택한 그룹 편집	선택한 그룹 수정
선택한 그룹 삭제	선택한 그룹 삭제
대량 등록	선택한 프로필에 대해 한 번에 많은 디바이스/사용자를 등록합니다.
대량 할당	현재 선택된 그룹에 프로필 할당하기
하위 그룹 만들기	해당 (하위) 그룹에 대한 하위 그룹 만들기
사용자 만들기	해당 (하위) 그룹에 대한 사용자 만들기

하위 그룹 만들기

'하위 그룹 만들기'를 사용하면 추가 하위 그룹을 만들 수 있습니다.

하위 그룹을 할당할 그룹을 설정할 수 있습니다(기본적으로 하위 그룹은 현재 선택되어 있는 그룹에 할당됩니다).

선택한 그룹 편집



여기에서 프로필을 편집할 수 있으며, 다음과 같은 설정이 가능합니다:

- 그룹 이름 변경 가능
- 상위 그룹 변경 가능

선택한 그룹 삭제

'선택한 그룹 삭제' 아래에 해당 그룹에 속한 모든 사용자와 디바이스가 나열됩니다. 여기에서 이들을 삭제할 수 있는 옵션이 있습니다.

한 사용자에 대해 다음과 같은 삭제 명령을 수행할 수 있습니다:

사용자 삭제	사용자가 삭제됨
사용자를 그룹으로 이동합니다:	사용자를 다른 그룹(다음 열, 예: '관리자')으로 이동할 수 있습니다.

하나의 디바이스에 대해 다음과 같은 삭제 명령을 수행할 수 있습니다:

지우기 및 삭제	디바이스 초기화 및 삭제
시스템에서 삭제	앱텍에서만 장치 제거

참조: 대량 등록

참조: 대량 할당

사용자 만들기

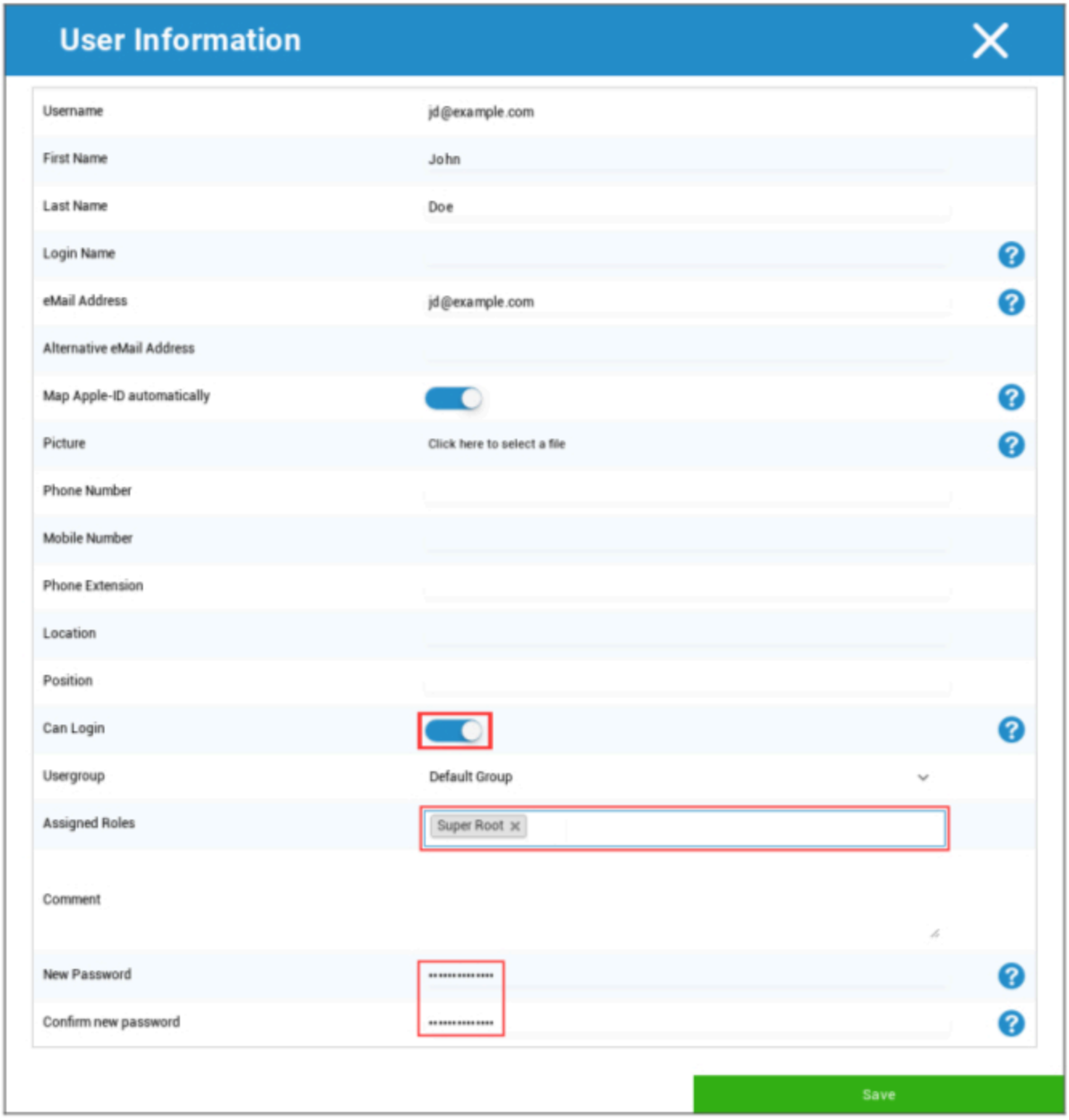
'사용자 만들기'를 사용하면 새 사용자를 추가할 수 있습니다.

새 관리자 사용자 만들기

사용자를 관리자 사용자로 설정할 수 있습니다. 이렇게 하면 콘솔에 로그인하고 사용자/그룹/기기를 변경할 수 있는 권한이 부여됩니다.

일반 사용자를 만들거나 기존 사용자를 사용합니다. 관리자 권한을 부여할 사용자를 선택하고 휠을 클릭한 다음 '사용자 수정'을 선택합니다:

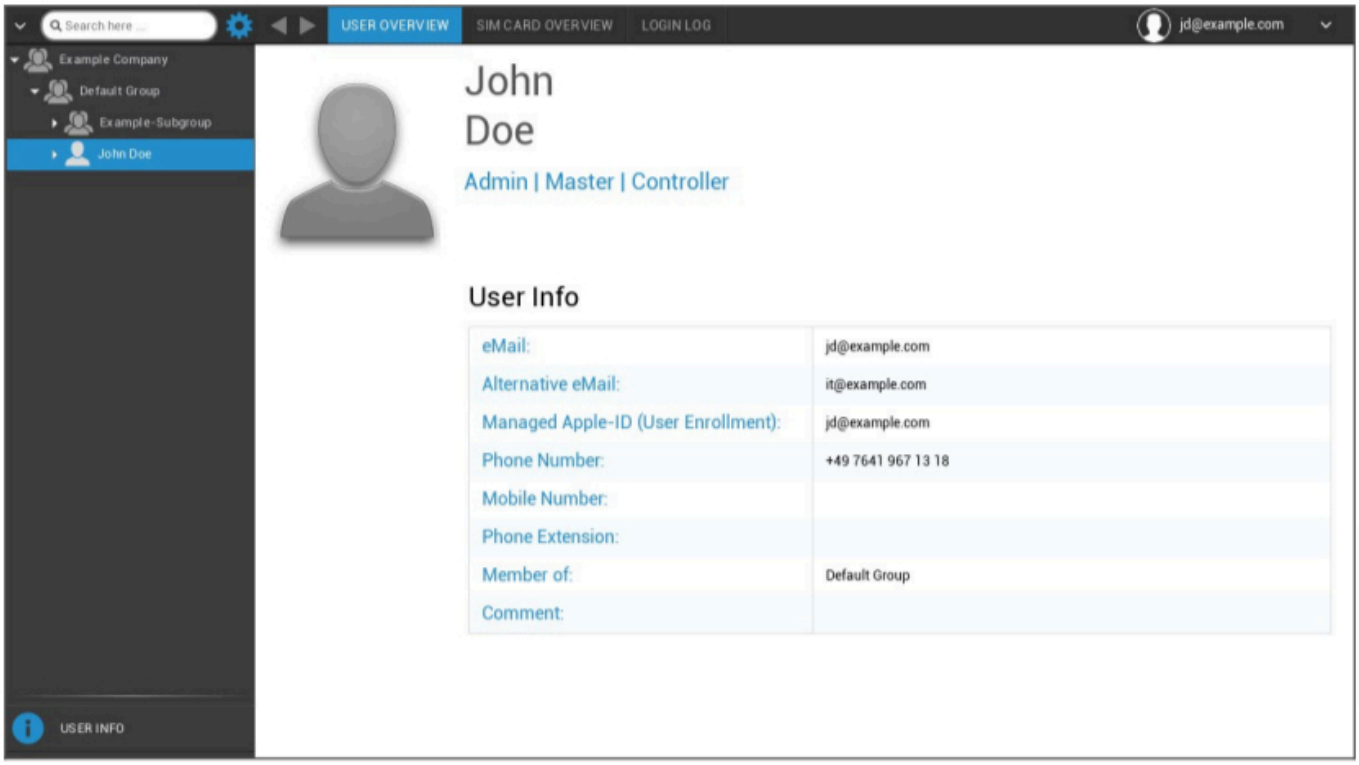
'로그인 가능' 스위치를 활성화하고 사용자에게 '슈퍼루트' 역할을 할당하고 비밀번호를 설정합니다.



이를 저장하면 이제 사용자가 사용자 아이디와 비밀번호로 로그인할 수 있습니다.

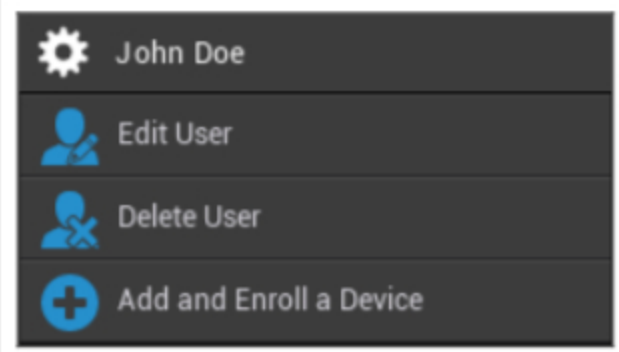
모바일 관리의 사용자 관리

특정 사용자를 선택하면 다음과 같은 개요가 표시됩니다:



앞서 '사용자 만들기'에서 입력한 모든 정보에 대한 개요를 확인할 수 있습니다.

상단에 설치된 기어를 사용하여 다음 구성을 수행할 수 있습니다:



사용자 이름	선택한 사용자의 사용자 이름
사용자 편집	사용자 정보 편집
사용자 삭제	사용자 삭제 • 시스템에서 삭제 = 앱텍에서 장치가 제거됩니다.

	• 초기화 및 삭제 = 기기가 공장 설정으로 복원되고 AppTec에서 제거됩니다.
장치 추가 및 등록	선택한 사용자에 대한 디바이스 등록

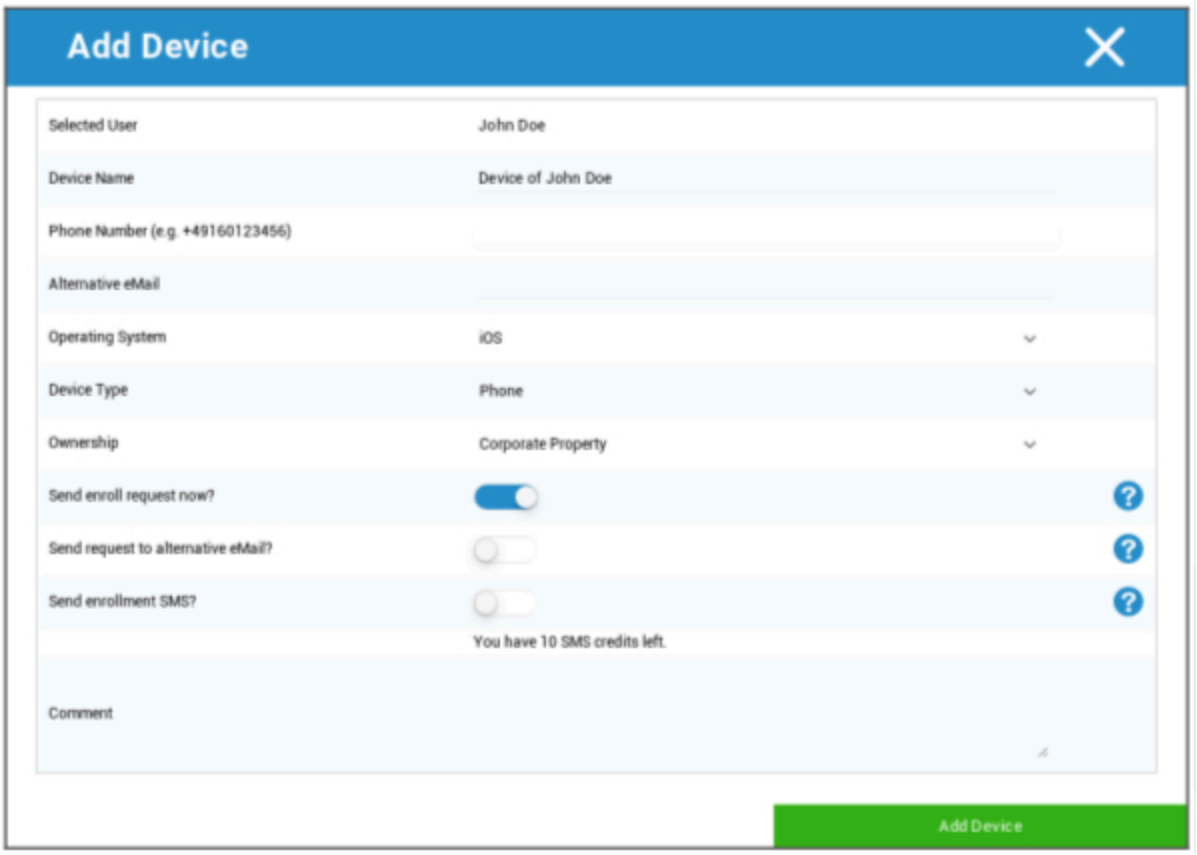
관리 액세스 권한은 계층 구조에서 로컬 사용자 계정으로 제출할 수도 있습니다. 추가 관리자를 설정하지 않는 한 이 계정을 삭제해서는 안 됩니다!

장치 추가 및 등록

여기에서 선택한 용도에 맞는 디바이스를 선택할 수 있습니다.

또는 장치를 그룹에 직접 등록할 수도 있습니다. 이렇게 하려면 그룹을 클릭하고 휠을 클릭한 다음 '디바이스 추가 및 등록'을 선택합니다.

다음과 같은 개요가 표시됩니다:



등록하려는 디바이스 종류에 따라 다음 구성을 수행해야 합니다:

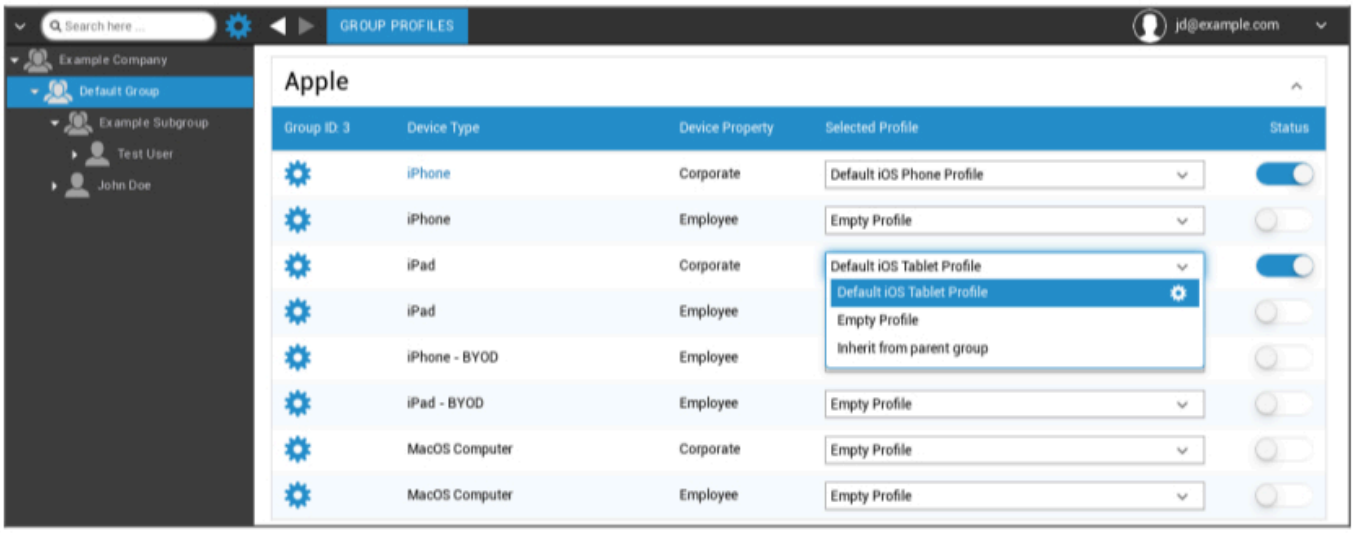
선택된 사용자	선택한 사용자(자동으로 입력됨)
장치 이름	자동으로 입력됨('사용자 이름'의 경우 디바이스) - 변경 가능
전화번호	전화번호는 사용자가 제공한 경우 자동으로 입력되지만, 여기에서 추가하거나 변경할 수 있습니다.
대체 이메일	대체 이메일은 사용자가 제공한 경우 자동으로 채워지지만 여기에서 추가하거나 변경할 수 있습니다.
디바이스 소유자	회사 자산 = 회사 디바이스 직원 자산 = BYOD 기기
운영 체제 선택	여기에서 다음 운영 체제 중에서 선택할 수 있습니다: • iOS • iOS BYOD(사용자 등록) • MacOS • Android 엔터프라이즈 • Android • Windows 모바일 • Windows 10
등록 요청을 보내시겠습니까?	이메일이 기본 이메일 주소로 즉시 전송되고 사용자에게 기기를 연결하라는 메시지가 표시됩니다.
다른 이메일로 요청을 보내시겠습니까?	대체 이메일 주소로 추가 또는 단독으로("등록 요청 보내기?"가 비활성화된 경우) 이메일을 보냅니다(이메일이 "일반" 등록 요청 이메일과 다름).
등록 SMS를 보내시겠습니까?	SMS를 통해 등록 요청을 보냅니다('전화번호'를 입력해야 함).

등록 요청이 전송되면 장치가 바로 표시(빨간색으로 표시)됩니다.

디바이스가 성공적으로 연결되면 곧바로 녹색으로 표시되어 제한 사항, 앱 등을 받을 준비가 된 것입니다.

모바일 관리의 프로필 관리

그룹을 클릭하면 구성할 모든 디바이스 플랫폼과 각각 할당된 프로필에 대한 개요를 볼 수 있습니다.



	선택한 프로필에 대한 구성을 수행합니다.
디바이스 유형	장치 유형 및/또는 모델
장치 속성	디바이스 소유자(회사 = 회사 소유, 직원 = 개인 직원 디바이스)
선택한 프로필	선택한 프로필(기어를 누르면 프로필의 구성 대화 상자가 열림)
상태	켜기/끄기(프로필이 활성화/비활성화됨)

기어를 선택하면 다음과 같은 옵션이 표시됩니다:

프로필 만들기

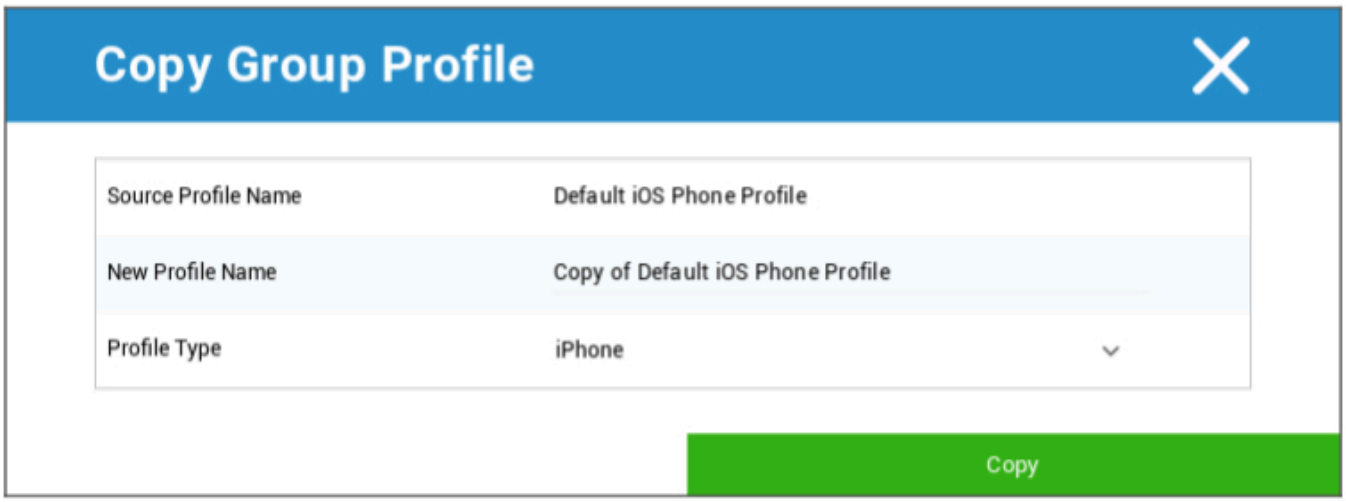
각 항목 및/또는 플랫폼에 대해 새 프로필을 생성하고 구성할 수 있습니다. 이 하위 지점을 클릭하면 프로필이 즉시 생성되며 iOS, Android 및 Windows Phone의 구성을 바로 시작할 수 있습니다.

프로필 수정

'프로필 수정'을 클릭하면 해당 프로필의 구성 화면으로 이동하여 구성을 설정할 수 있습니다.

프로필 복사

'프로필 복사' 기능을 사용하면 이미 존재하는 프로필의 설정/구성을 복사하여 새 프로필에 추가할 수 있습니다.

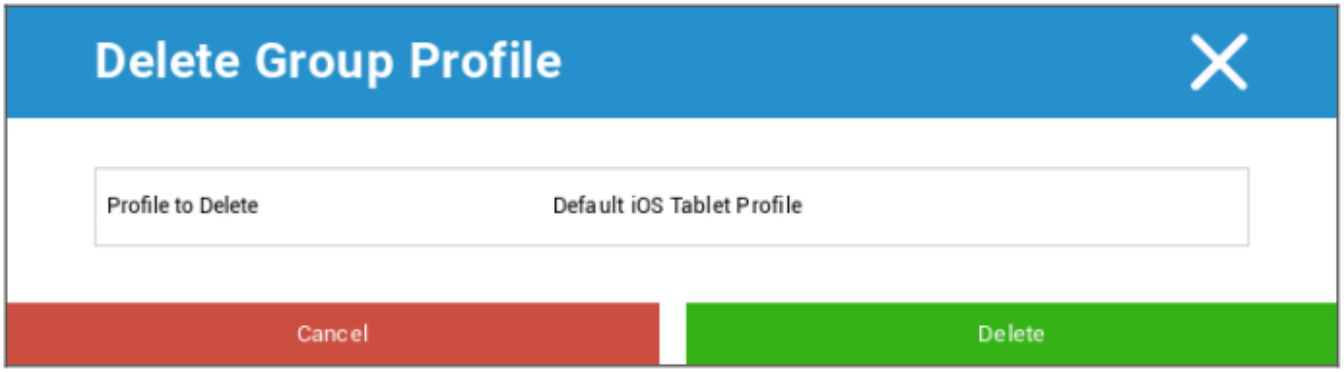


소스 프로필 이름	복사할 프로필의 이름
새 프로필 이름	새 프로필의 이름
프로필 유형	프로필 유형(휴대폰/태블릿)

"복사"를 클릭하면 프로필이 생성되고 이제 그룹에 할당할 수 있습니다.

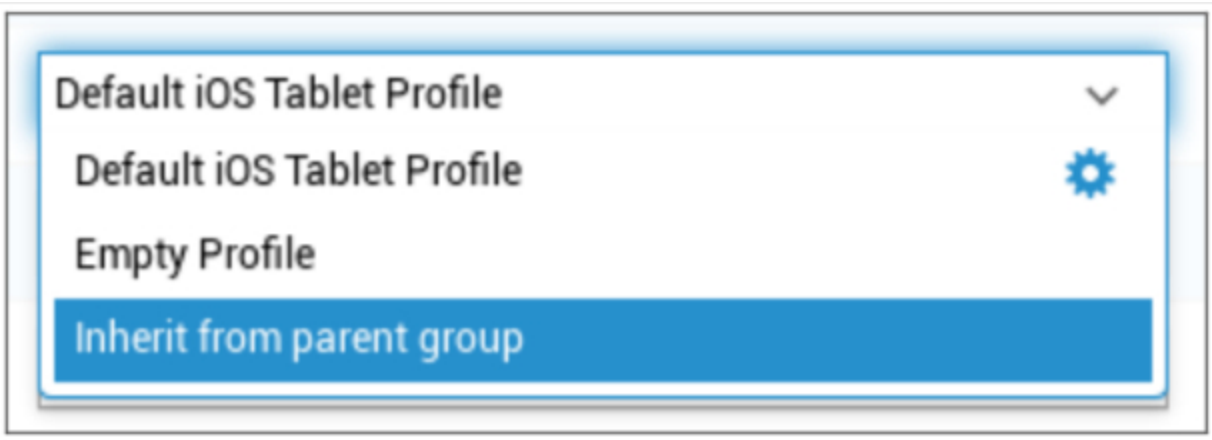
프로필 삭제

여기에서 프로필을 영구적으로 삭제할 수 있습니다. 프로필을 삭제하는 과정과 프로필에 대한 다음 '지금 할당' 프로세스 중에는 해당 그룹의 각 디바이스에서 구성이 사라지고 복구할 수 없다는 점에 유의하세요!


Delete Group Profile
Profile to Delete
Default iOS Tablet Profile
Cancel
Delete

프로필 상속

프로필을 선택하는 동안 '상위 그룹에서 상속' 옵션을 사용할 수 있습니다.



프로필이 활성화되면 상위 그룹의 프로필이 각각 선택한 디바이스(및 해당 디바이스 유형)에 사용됩니다. 또한 이 프로필을 변경하면 여러 그룹에 영향을 미칠 수 있다는 점에 유의하세요.

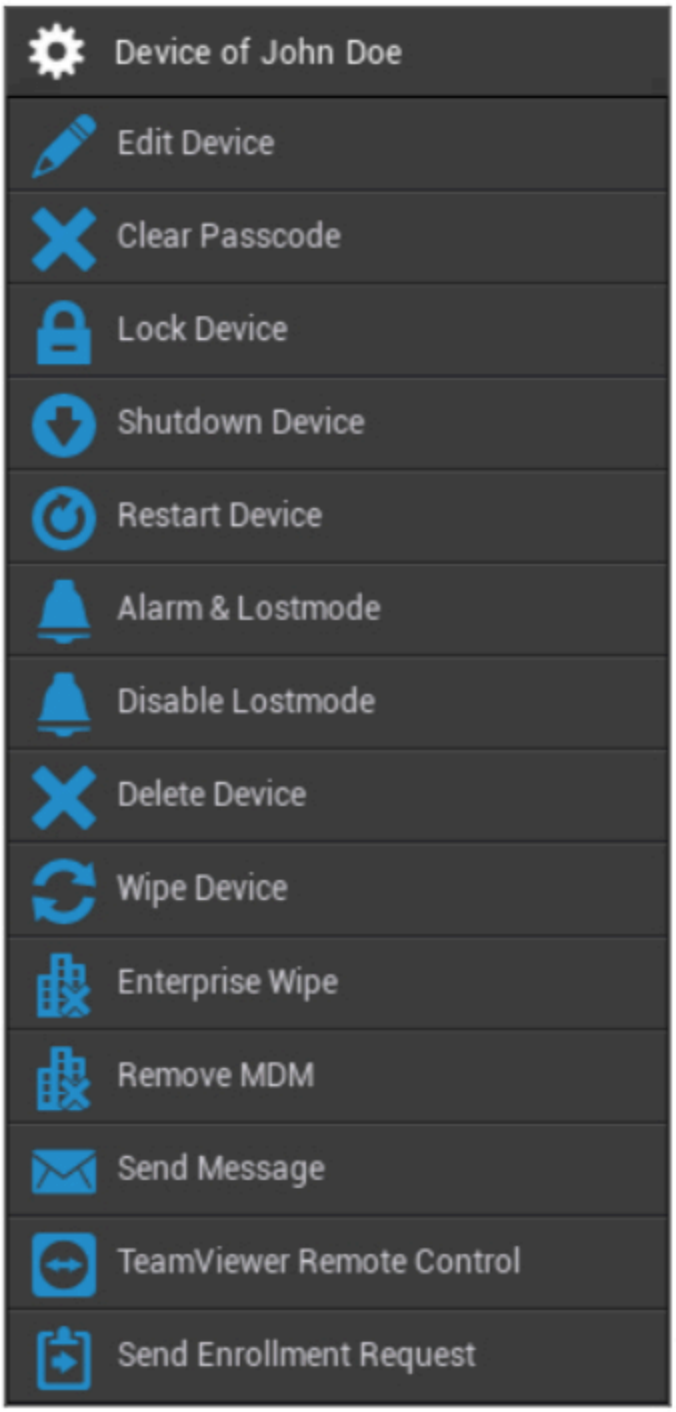
이 구성은 새 하위 그룹이 생성될 때 기본값으로 설정됩니다.

빈 프로필에 해당하는 '빈 프로필' 구성도 사용할 수 있으며, 이는 결국 최종 사용자 디바이스에서 새 구성이 수행되지 않음을 의미합니다.

모바일 관리의 디바이스 관리

디바이스를 선택하면 '기어'를 통해 다양한 작업을 수행할 수 있습니다. 이는 OS 플랫폼(iOS, Android Enterprise, Android, Windows Mobile, Windows 10)에 따라 다릅니다.

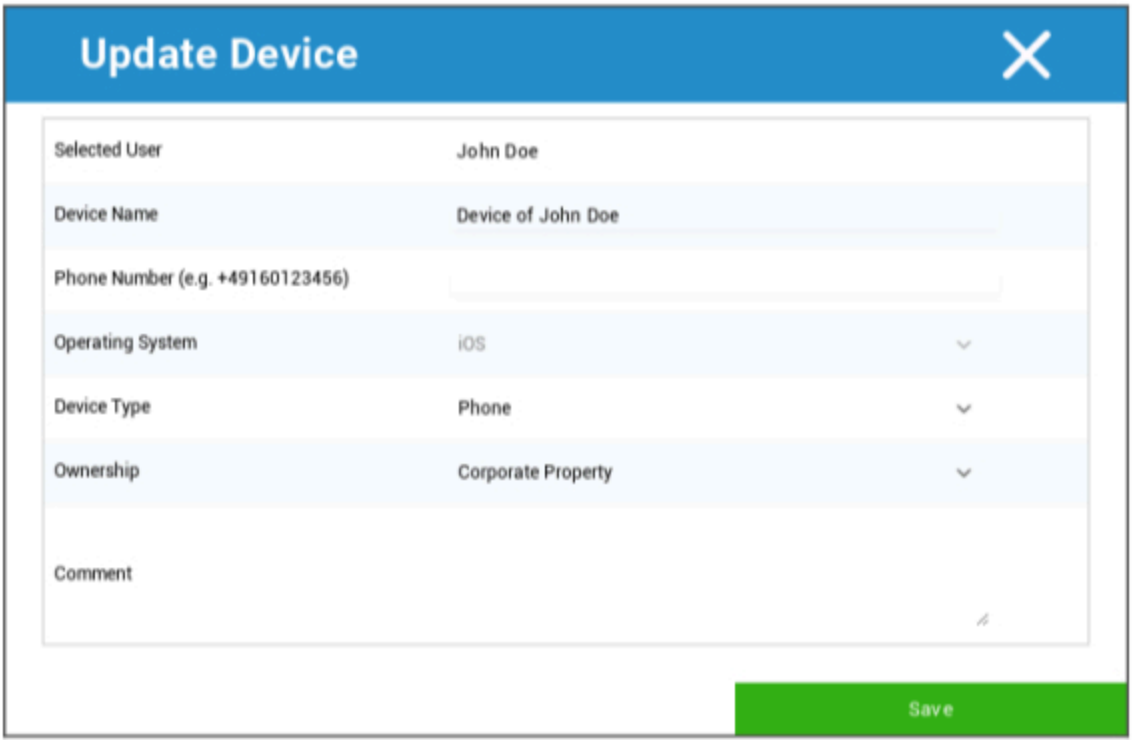
IOS



장치 편집	장치 편집
암호 지우기	장치 암호가 지워집니다.
잠금 장치	잠금 장치(잠금 화면)
장치 종료	장치 종료

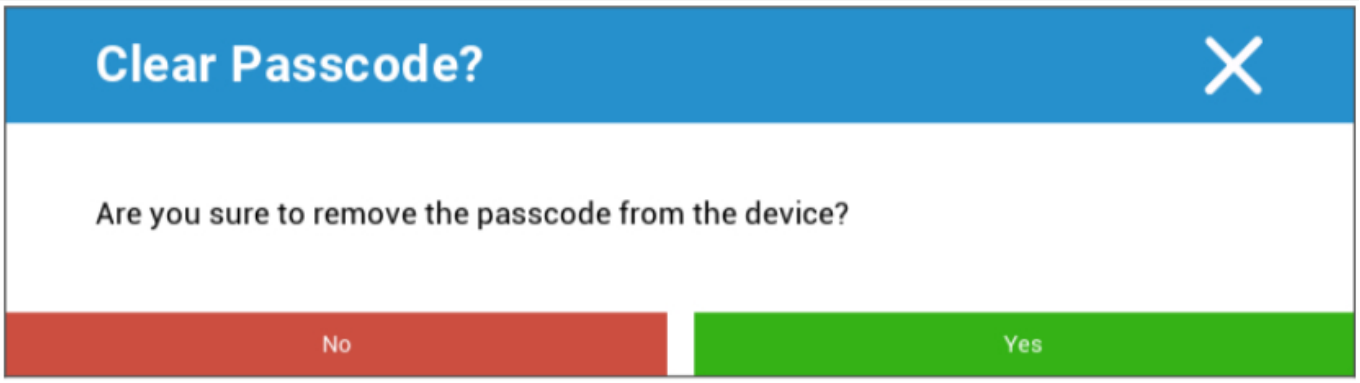
장치 다시 시작	장치 다시 시작
알람 및 분실 모드	알람 및 분실 모드 시작
로스트모드 비활성화	로스트모드 비활성화
장치 삭제	AppTec에서 장치 제거
장치 지우기	기기를 공장 출하 시 설정으로 복원
엔터프라이즈 삭제	AppTec360에서 제공하는 정보, 앱 및 프로필이 삭제됩니다(장치는 MDM에서 분리됨).
MDM 제거	
메시지 보내기	디바이스로 푸시 알림 보내기 앱텍360 앱(메시지 탭)에 메시지가 표시됩니다.
TeamViewer 원격 제어	TeamViewer를 사용하여 원격 제어 세션 시작
등록 요청 보내기	등록 요청 보내기(반복)

장치 편집



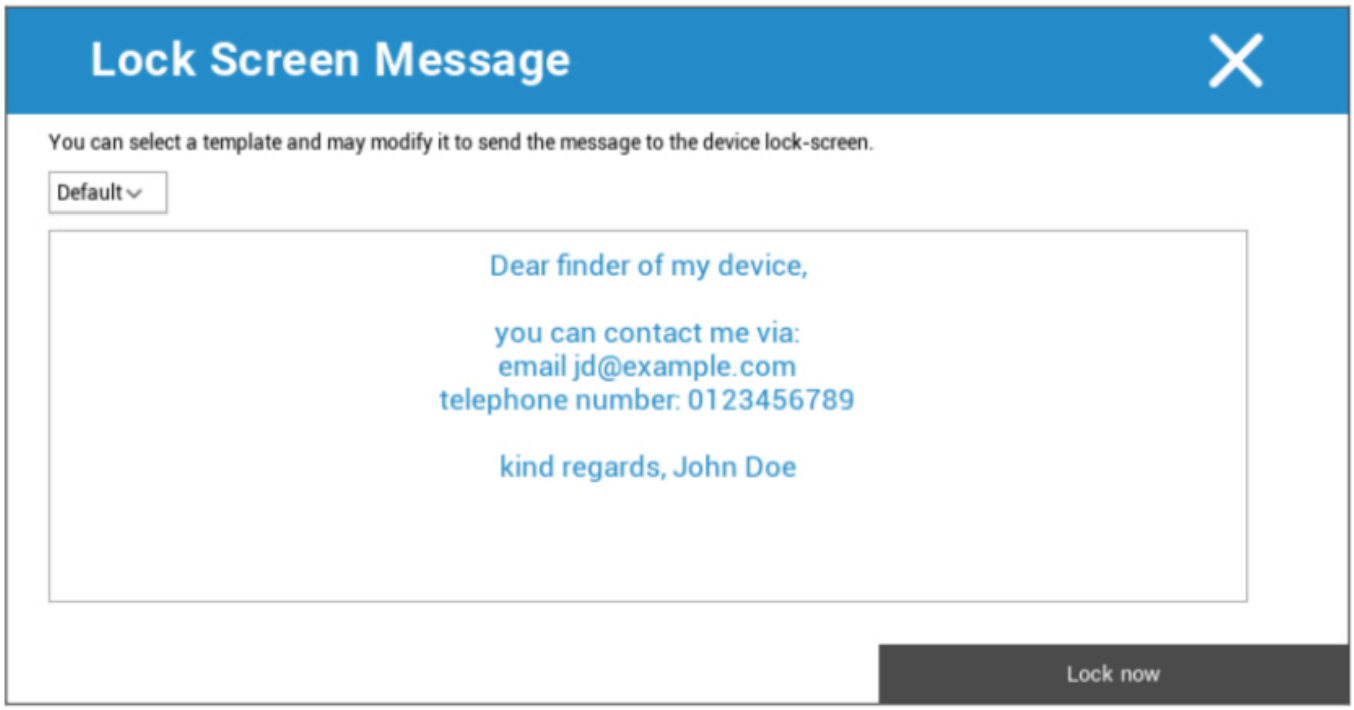
여기에서 디바이스의 다양한 정보를 업데이트할 수 있습니다.

암호 지우기



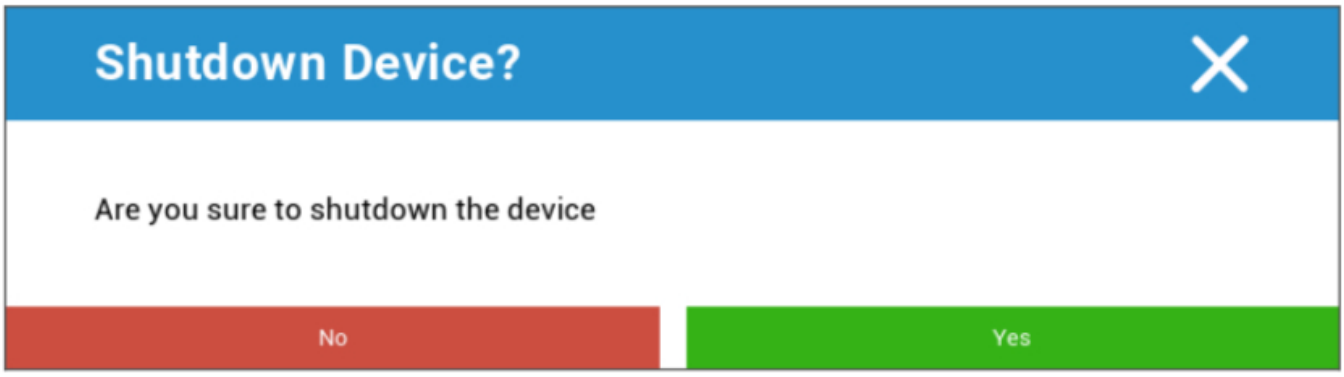
'비밀번호 지우기'에서 디바이스에서 비밀번호를 원격으로 제거할 수 있습니다. 그 후 비밀번호 지침에 따라 새 비밀번호를 발급하라는 메시지가 표시됩니다(비밀번호 지침에 따라).

잠금 장치



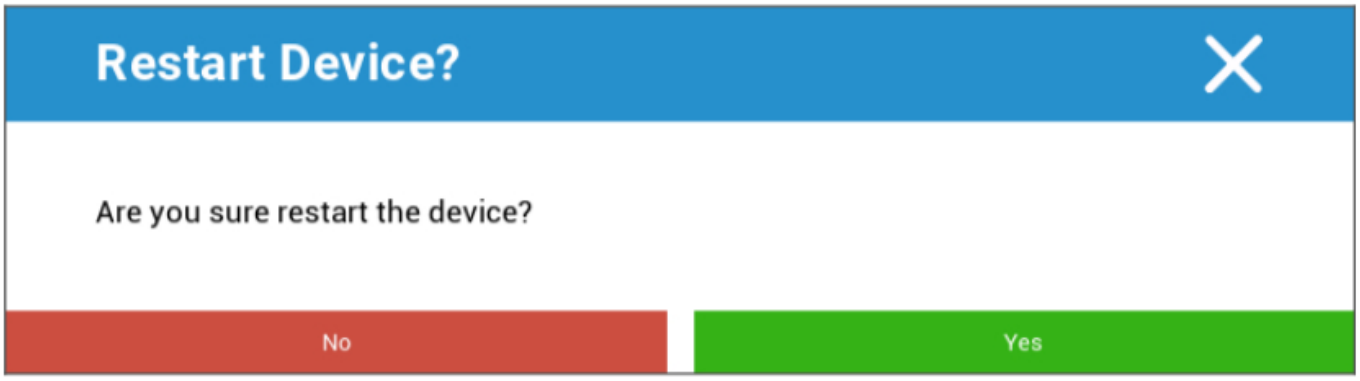
여기서 잠금 명령이 최종 사용자 디바이스(잠금 화면)로 전송됩니다.

장치 종료



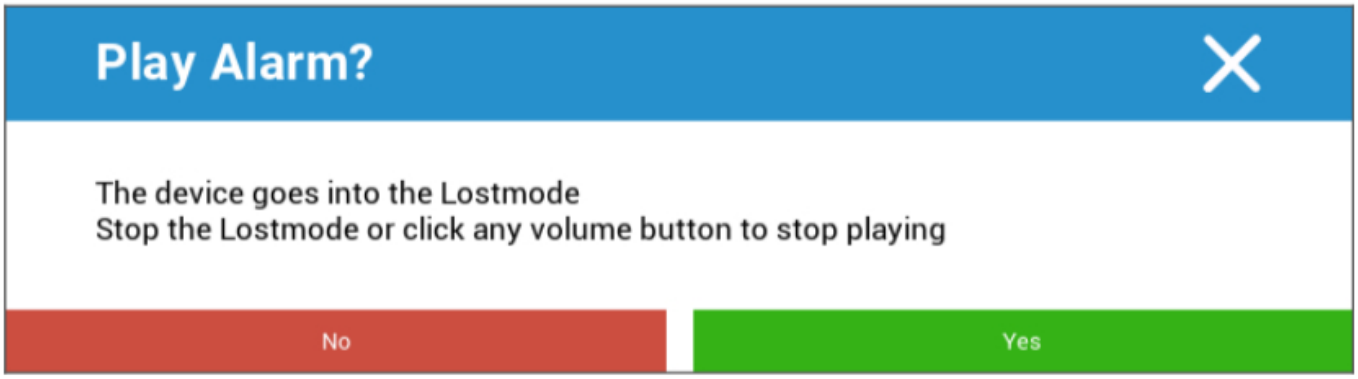
여기서 종료 명령이 최종 사용자 장치로 전송됩니다.

장치 다시 시작

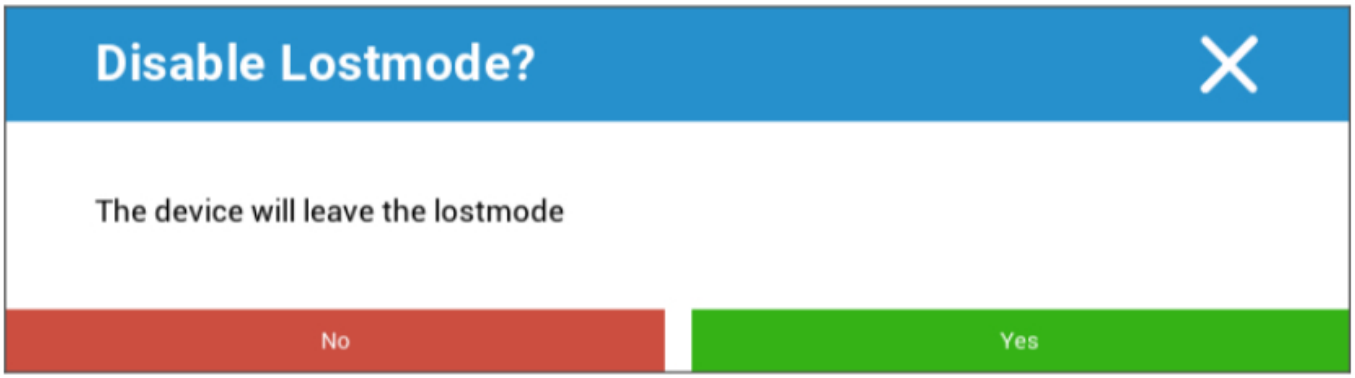


여기서 재시작 명령이 최종 사용자 장치로 전송됩니다.

알람 및 분실모드 | 분실모드 비활성화하기



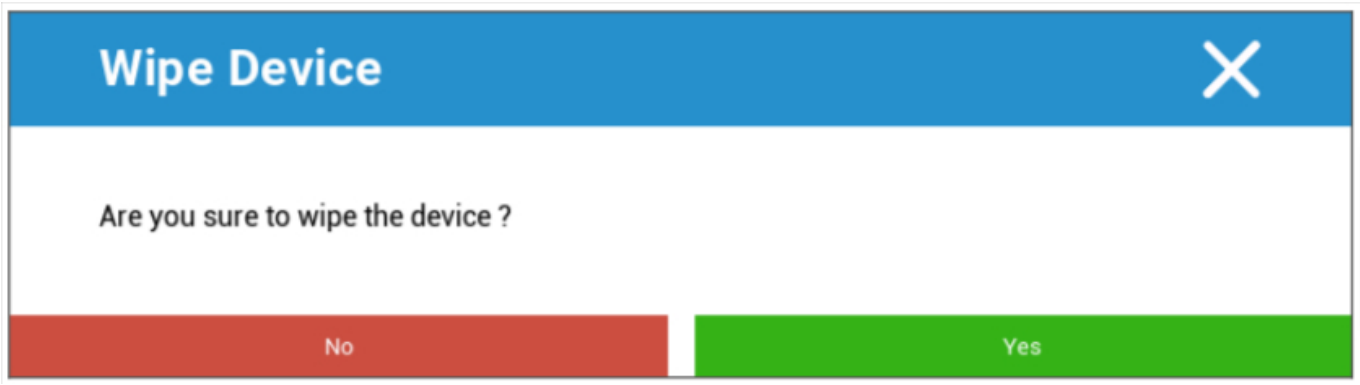
여기에서 디바이스를 분실 모드로 설정하면 디바이스에서 알람 소리가 지속적으로 재생되도록 설정할 수 있습니다. 분실 모드는 디바이스의 볼륨 버튼을 누르거나 '분실 모드 비활성화'를 클릭하여 원격으로 중지할 수 있습니다:



장치 삭제

여기에서 삭제 명령을 수행할 수 있습니다. 장치를 AppTec360에서만 제거할지("시스템에서 삭제") 또는 AppTec360에서 장치를 제거한 후 공장 설정으로 복원할지("초기화 및 삭제") 다시 한 번 결정할 수 있습니다.

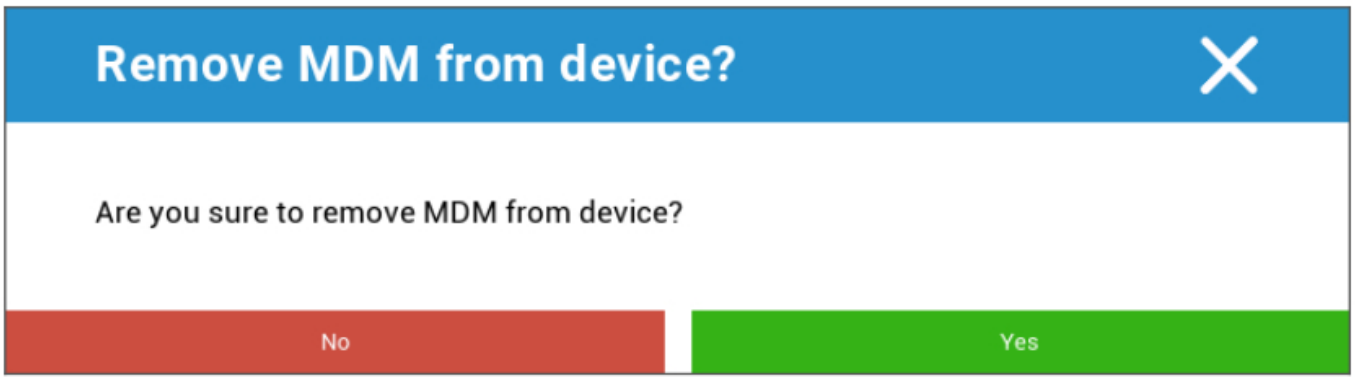
장치 지우기



'디바이스 초기화'에서 디바이스를 완전히 초기화할 수 있습니다. 장치가 공장 설정으로 복원됩니다.

엔터프라이즈 초기화 | MDM 제거

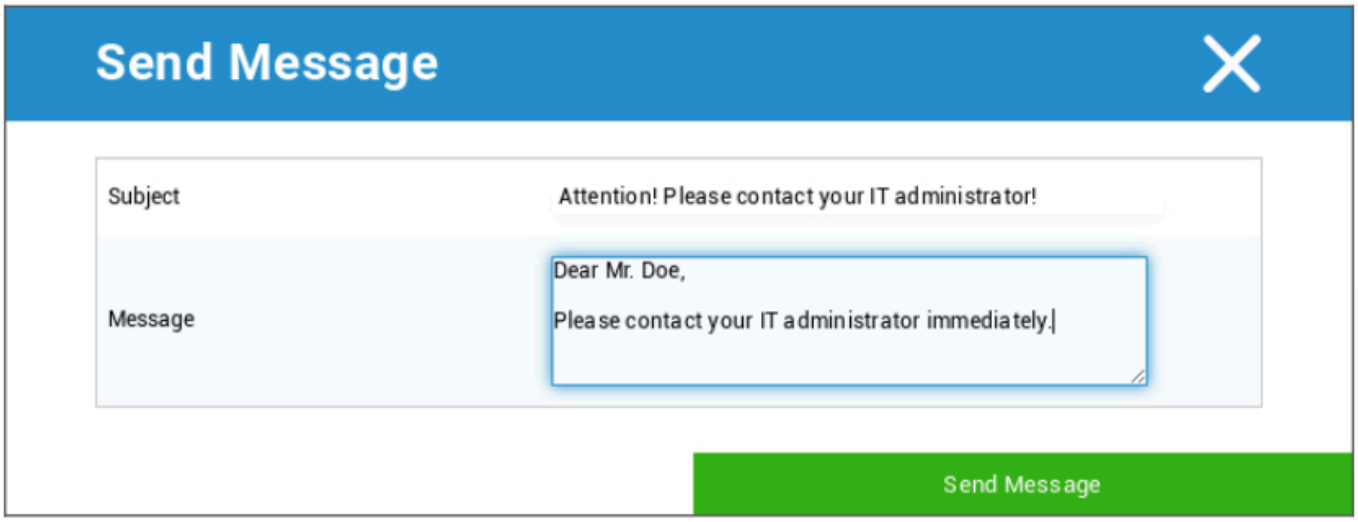
AppTec360에서 제공한 정보, 앱 및 프로필만 삭제됩니다. 이렇게 하면 최종 사용자 디바이스에서 기업 데이터를 더 이상 사용할 수 없게 됩니다. 비공개 영역은 영향을 받지 않으며 최종 사용자 디바이스에 계속 남아 있습니다.



"MDM 제거"를 사용하면 최종 사용자 기기에서 MDM 프로필과 AppTec에서 제공하는 기타 모든 항목을 제거할 수 있습니다.

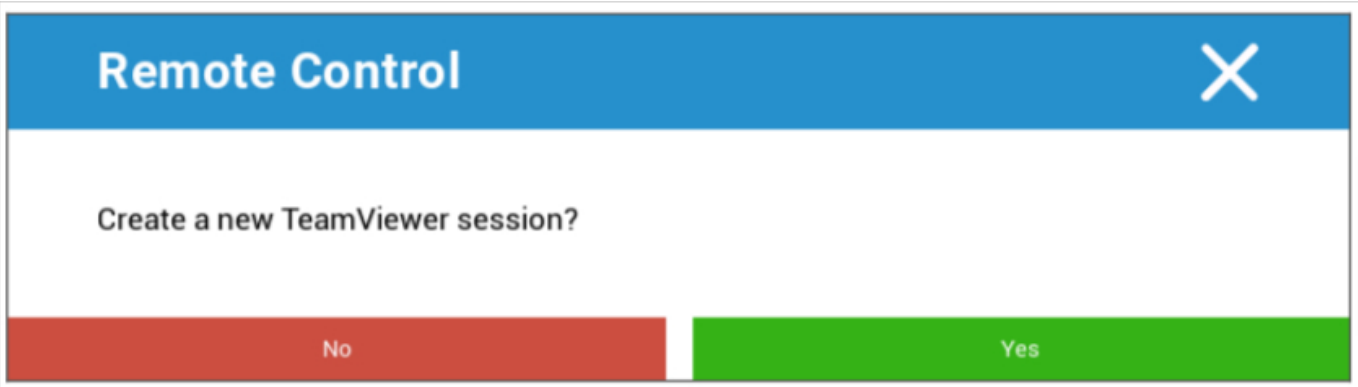
이 명령은 "엔터프라이즈 초기화"와 동일한 작업을 수행합니다.

메시지 보내기



여기에서 각 디바이스로 푸시 알림을 보낼 수 있습니다.

TeamViewer 원격 제어



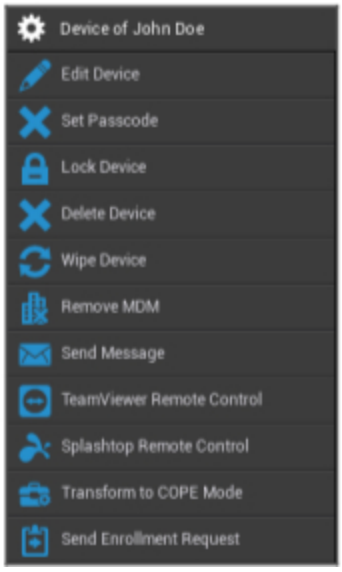
여기에서 팀뷰어 원격 제어 세션을 시작할 수 있습니다.

등록 요청 보내기

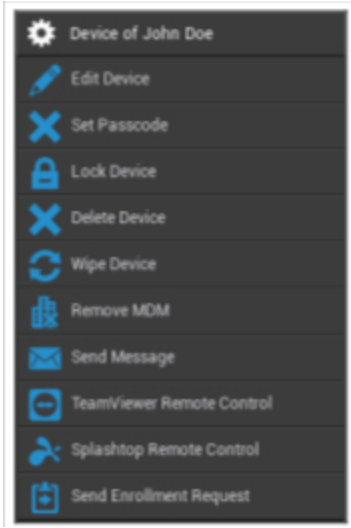
"등록 요청 보내기"를 사용하면 해당 사용자에게 등록 요청을 (다시) 보낼 수 있습니다.

Android

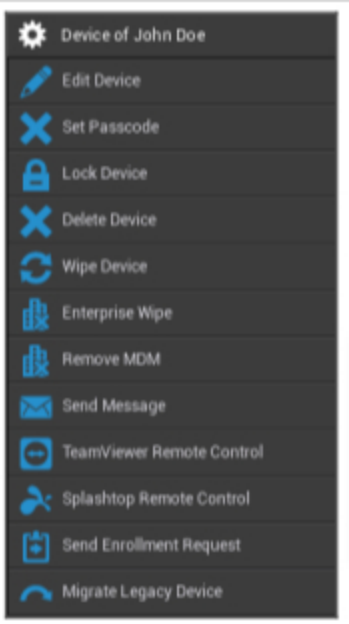
AE 완전 관리형 디바이스(업무 관리형)



AE 작업 프로필(컨테이너)



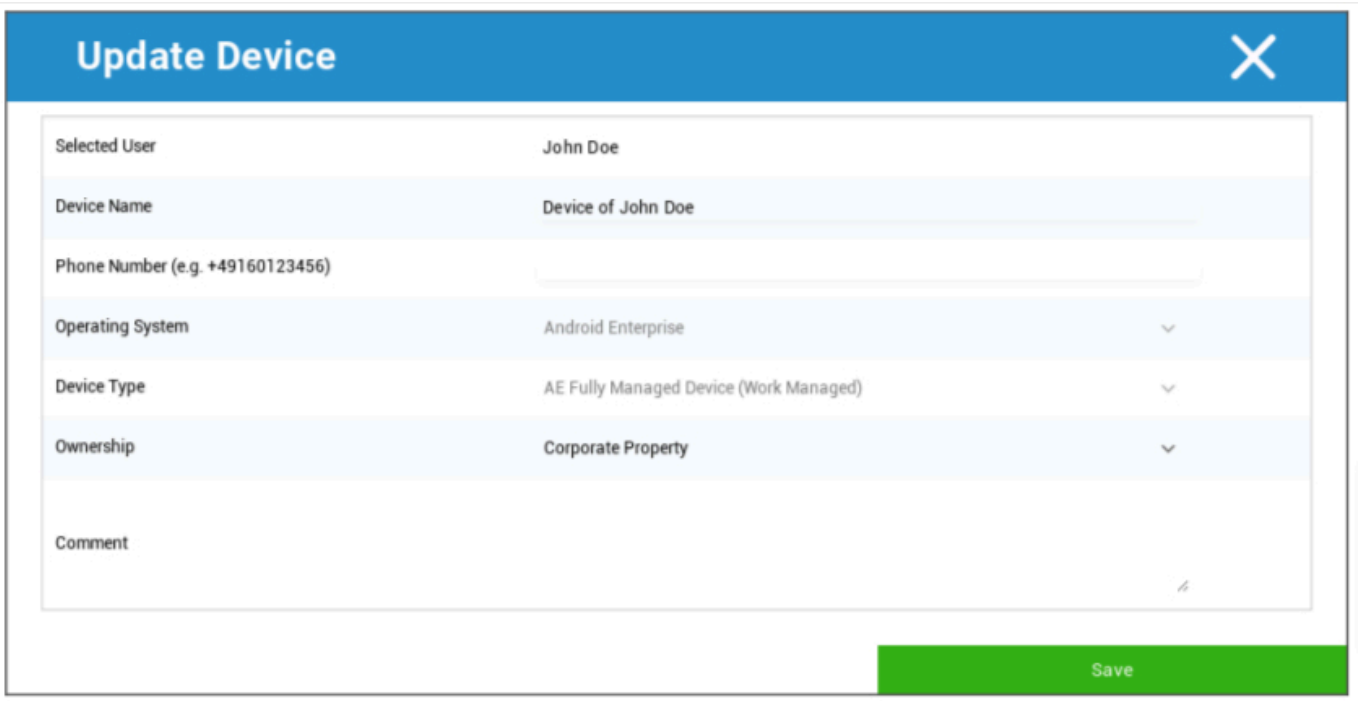
Android 휴대폰 | 태블릿



장치 편집	디바이스 정보 수정
암호 설정	디바이스의 비밀번호 설정
잠금 장치	잠금 장치(잠금 화면)
장치 삭제	AppTec에서 기기 삭제
장치 지우기	기기를 공장 출하 시 설정으로 복원
엔터프라이즈 삭제	AppTec360에서 제공하는 정보, 앱, 프로필이 삭제됩니다(장치는 MDM에서 분리됩니다).
MDM 제거	
메시지 보내기	장치에 푸시 알림 보내기 앱텍360 앱(메시지 탭)에 메시지가 표시됩니다.
TeamViewer 원격 제어	TeamViewer를 사용하여 이 장치에 대한 원격 제어 세션을 시작합니다.
스플래시탑 원격 제어	스플래시톱을 사용하여 이 장치에 대한 원격 제어 세션을 시작합니다.
COPE 모드로 전환(AE 완전 관리형 장치(작업 관리형)에서만)	이 AE 완전 관리형(작업 관리형) 장치에서 작업 프로필 만들기
등록 요청 보내기	등록 요청 보내기(반복)
레거시 디바이스 마이그레이션(디바이스 소유자 모드 프로비저닝을 사용하여 등록한 경우 Android 휴대폰/태블릿에서만 해당)	Android 휴대폰/태블릿 프로필을 AE 완전 관리형 디바이스(업무 관리형) 프로필로 마이그레이션하기

장치 편집

여기에서 다양한 디바이스 정보를 업데이트할 수 있습니다.



선택된 사용자	디바이스 사용자
장치 이름	장치 이름
전화번호	장치 전화 번호
운영 체제	Android 엔터프라이즈 Android
디바이스 유형	Android Enterprise: • AE 완전 관리형 디바이스(업무 관리형) • AE 작업 프로필 모드(컨테이너 전용) • 업무 프로필이 있는 AE 완전 관리형 디바이스(COPE) Android: • 전화 • 태블릿
소유권	기업 = 기업 자산

	직원 = 직원 자산
댓글	장치에 대한 추가 설명

암호 지우기

여기에서 선택한 디바이스의 디바이스 비밀번호를 제거할 수 있습니다. Android의 경우 기본적으로 비밀번호는 "123456"으로 설정되며, 나중에 사용자가 변경할 수 있고 변경해야 합니다.

잠금 장치

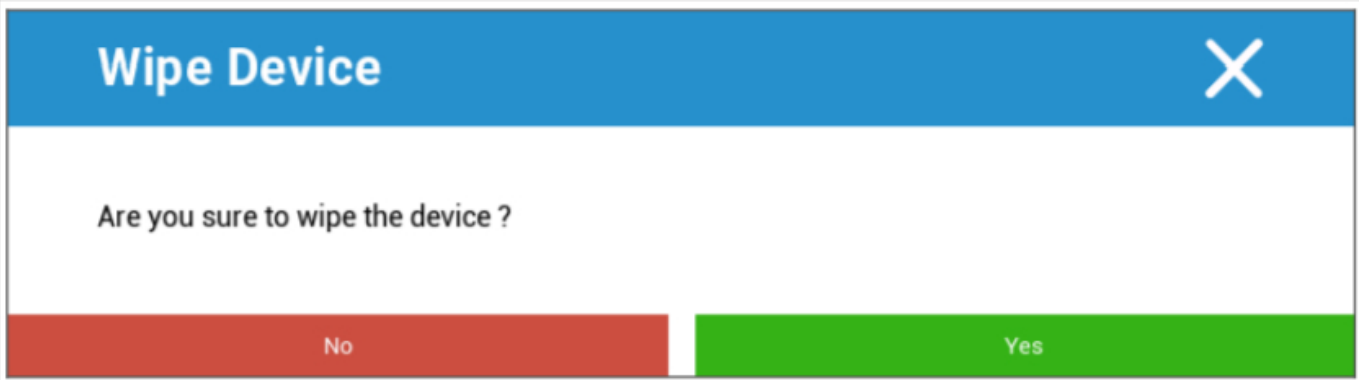
여기에서 디바이스 잠금 명령이 디바이스(잠금 화면)로 전송됩니다.

장치 삭제

여기에서 삭제 명령을 수행할 수 있습니다. 장치를 AppTec360에서만 제거할지("시스템에서 삭제") 또는 AppTec360에서 장치를 제거한 후 추가로 공장 설정으로 복원할지("초기화 및 삭제") 다시 한 번 결정할 수 있습니다.

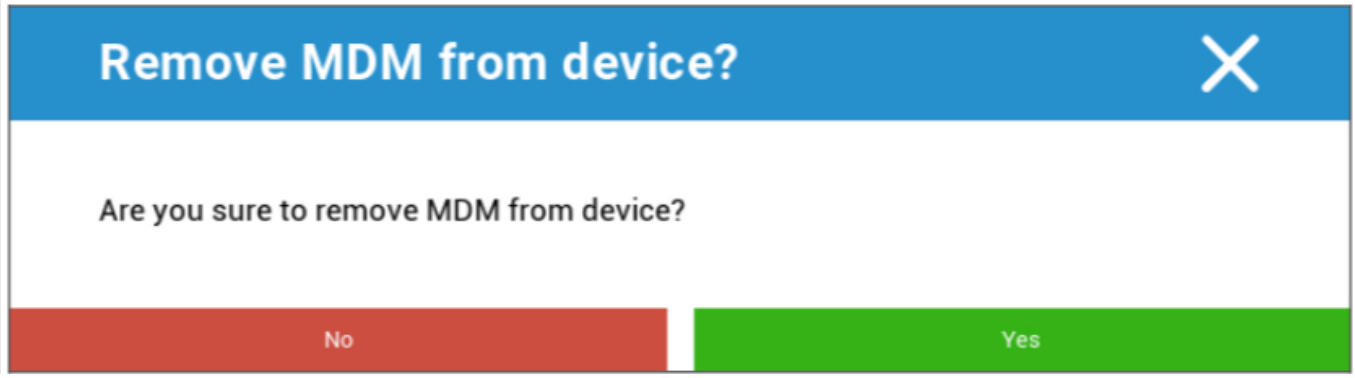
장치 지우기

'디바이스 초기화'에서 디바이스를 완전히 초기화할 수 있습니다. 그러면 디바이스가 공장 설정으로 복원됩니다.



또한 장치에 SD 카드가 포함되어 있는 경우 SD 카드를 지울 수 있습니다. "SD 카드도 지우시겠습니까?"를 "켜기"로 설정하면 이 작업을 수행할 수 있습니다. "를 "켜기"로 설정하면 됩니다.

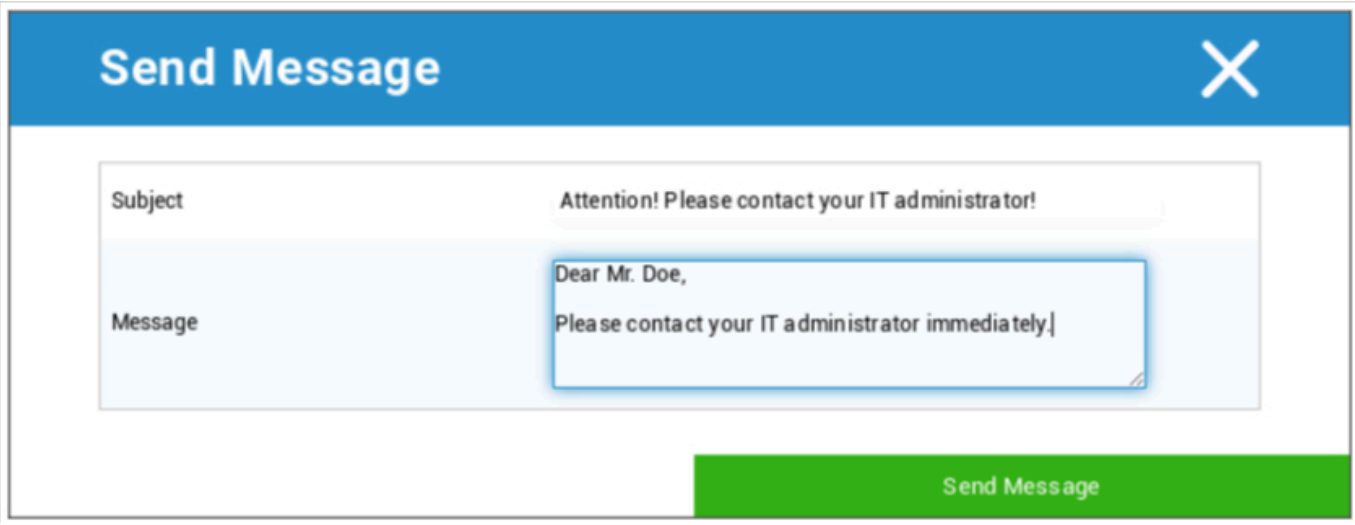
MDM 제거



이 방법은 MDM에서 분리하는 데 권장되는 방법입니다.

AppTec360에서 제공하는 정보, 앱 및 프로필만 삭제되므로 최종 사용자 디바이스에서 모든 기업 데이터를 더 이상 사용할 수 없게 됩니다. 그러나 개인 영역은 영향을 받지 않으며 최종 사용자 디바이스에 계속 남아 있습니다.

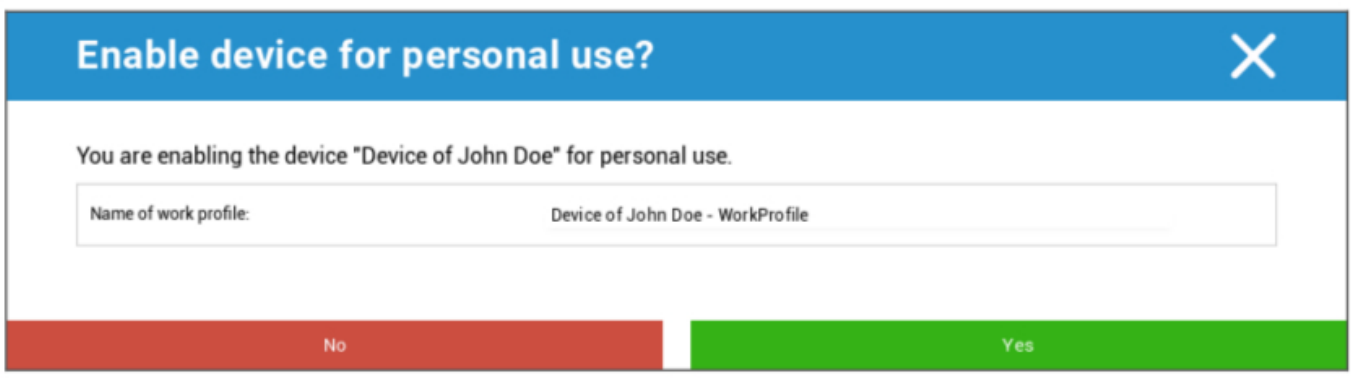
메시지 보내기



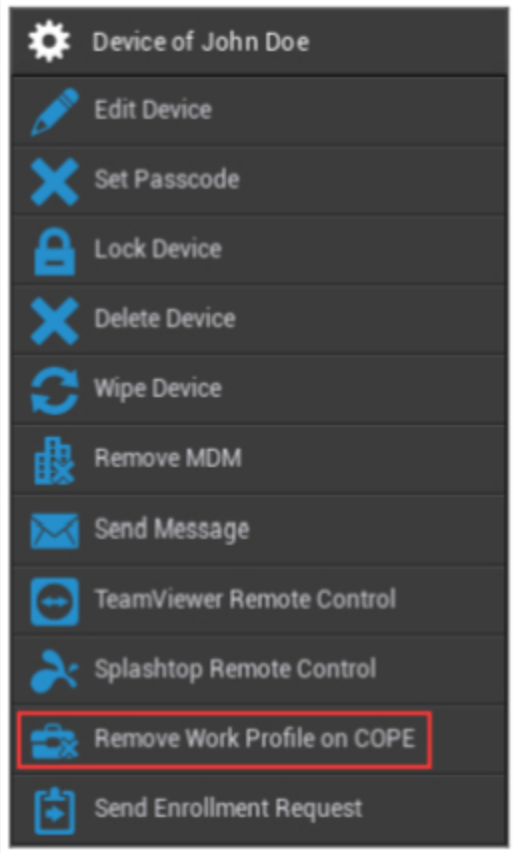
여기에서 각 최종 사용자 디바이스로 푸시 알림을 보낼 수 있습니다.

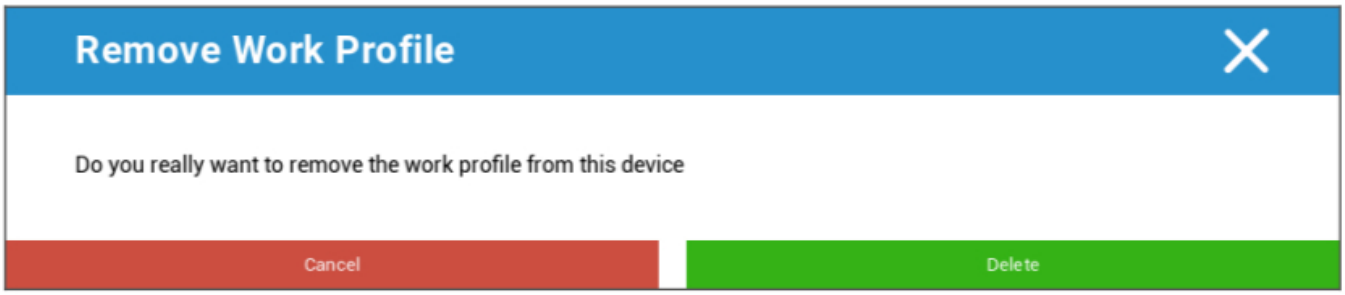
COPE 모드로 전환

이 AE 완전 관리형(작업 관리형) 장치에서 작업 프로필 만들기



장치를 COPE 모드로 전환한 후 기어 옵션인 **COPE에서 작업 프로필 제거**를 클릭하여 작업 프로필을 제거할 수 있습니다:




Remove Work Profile
Do you really want to remove the work profile from this device
Cancel
Delete

등록 요청 보내기

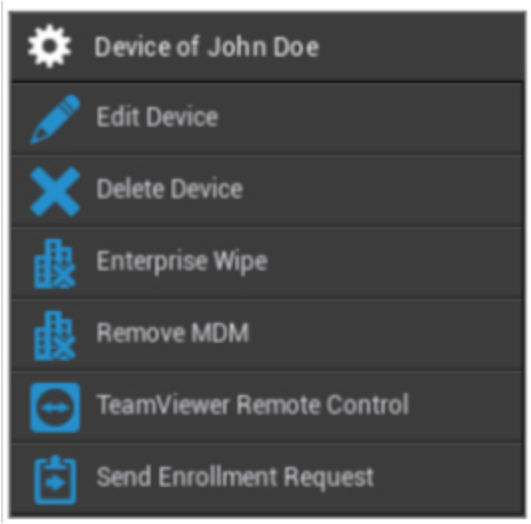
'등록 요청 보내기'를 사용하면 해당 사용자에게 등록 요청을 (다시) 보낼 수 있습니다.

최신 등록 - 요청만 유효하다는 점에 유의하세요.

레거시 디바이스 마이그레이션

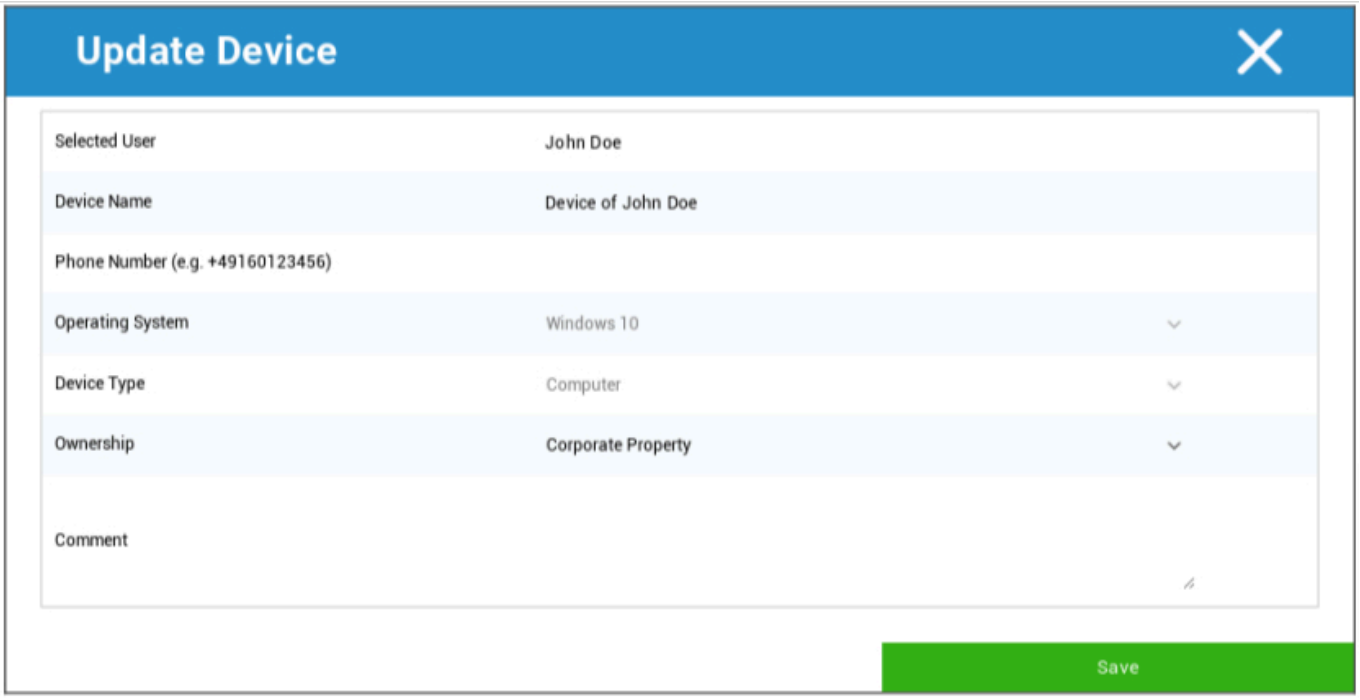
Android 휴대폰/태블릿 프로필을 AE 완전 관리형 디바이스(업무 관리형) 프로필로 마이그레이션하기

Windows



장치 이름	선택한 디바이스의 이름
장치 편집	장치 편집
장치 삭제	AppTec에서 장치 제거
엔터프라이즈 삭제	앱텍360에서 제공한 정보, 앱 및 프로필이 삭제됩니다.
MDM 제거	
TeamViewer 원격 제어	TeamViewer로 장치 원격 제어
등록 요청 보내기	등록 요청 보내기(다시)

장치 편집

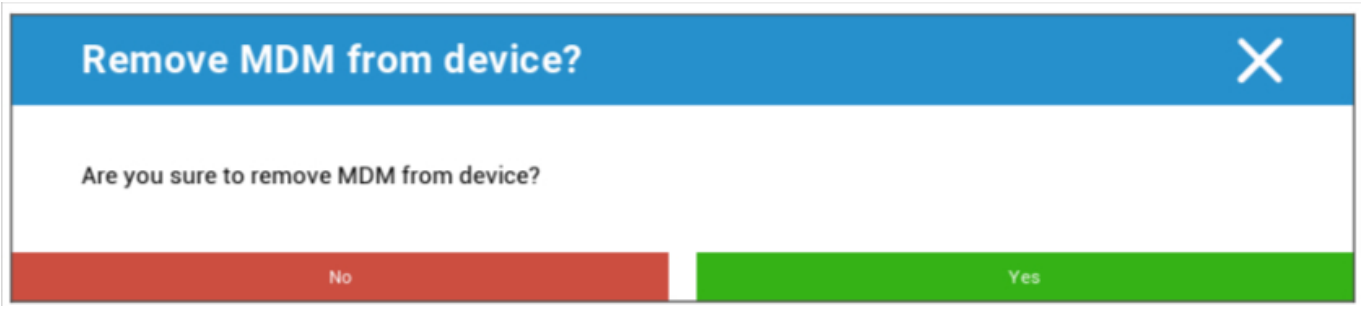


여기에서 디바이스의 다양한 정보를 업데이트할 수 있습니다.

장치 삭제

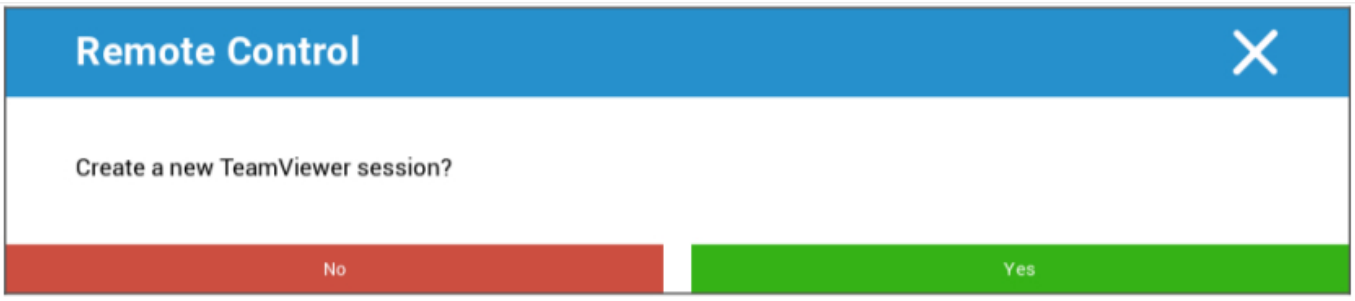
여기서 AppTec360에서 디바이스만 제거하는 삭제 명령을 수행할 수 있습니다.

엔터프라이즈 초기화 | MDM 제거



AppTec360에서 제공한 정보, 앱 및 프로필만 삭제됩니다. 이렇게 하면 최종 사용자 디바이스에서 기업 데이터를 더 이상 사용할 수 없게 됩니다. 비공개 영역은 영향을 받지 않으며 최종 사용자 디바이스에 계속 남아 있습니다.

TeamViewer 원격 제어



여기에서 이 장치에 대한 TeamViewer 원격 제어 세션을 시작할 수 있습니다.

등록 요청 보내기

"등록 요청 보내기"를 사용하면 해당 사용자에게 등록 요청을 (다시) 보낼 수 있습니다.

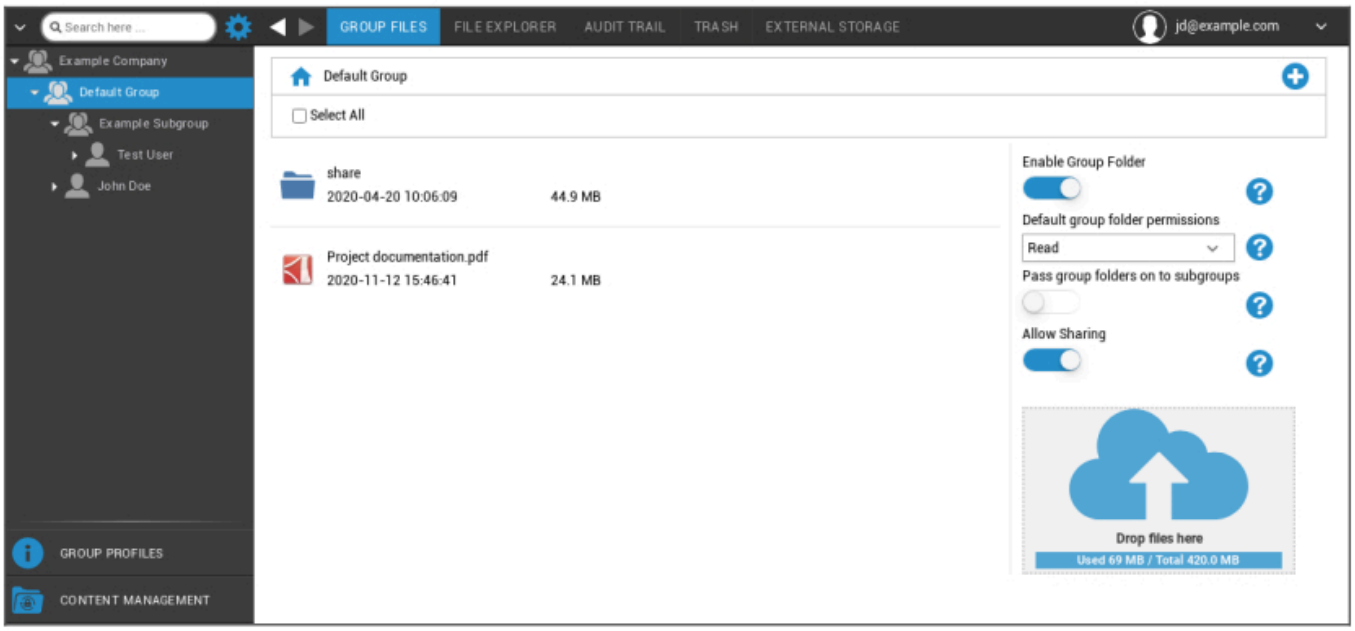
콘텐츠 관리

그룹에 속해 있는 경우 "콘텐츠 관리"를 통해 앱테크의 콘텐츠박스를 관리할 수 있습니다.

콘텐츠 상자를 사용하면 문서와 기타 기업 데이터를 최종 사용자 장치에 안전하게 배포할 수 있습니다.

그룹 파일

"그룹 파일"은 기본적인 부분인 ContentBox를 나타냅니다. 여기에서 설정을 설정하고, 문서를 업로드하고, 새 폴더를 만드는 등의 작업을 수행합니다.



오른쪽 상단 모서리에 있는 기호를 사용하여 '폴더 추가'로 해당 그룹에 지정되는 새 폴더를 만들 수 있습니다.

오른쪽 상단 모서리에 있는 기호를 사용하여 '폴더 추가'를 통해 새 폴더를 만들 수 있으며, 해당 폴더는 각 그룹에 할당되어야 합니다.

폴더 이름은 원하는 대로 지정할 수 있습니다.

'파일 업로드'를 통해 데이터를 업로드할 수 있습니다. 여기에서 표준 탐색기가 열립니다. 물론 모든 (하위) 폴더에서 이 두 가지 작업을 수행할 수 있습니다.

왼쪽 상단 모서리에 있는 기호를 클릭하면 주 메뉴로 돌아갈 수 있습니다.

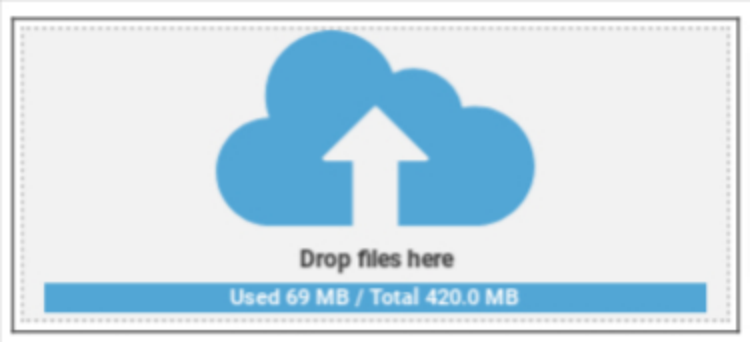
여러 폴더와 파일을 선택하고 "다운로드"로 다운로드하거나 "삭제"를 클릭하여 지울 수 있습니다.

모든 파일과 폴더를 선택하고 '다운로드' 및 '삭제' 명령을 수행할 수도 있습니다.

폴더나 파일 위로 마우스를 이동하면 다음과 같은 개요가 표시됩니다:

- '이름 바꾸기'를 사용하면 폴더/파일의 이름을 바꿀 수 있습니다.
- '다운로드'를 사용하면 폴더/파일을 다운로드할 수 있습니다.
- '삭제'를 사용하면 폴더/파일을 삭제할 수 있습니다.

그룹 폴더 사용	활성화하면 그룹의 모든 구성원이 해당 폴더에 액세스할 수 있습니다.
기본 그룹 폴더 권한	선택한 그룹에 속한 사용자의 권한입니다: 읽기 = 읽기 전용 권한 업데이트 = 업데이트 권한 만들기 = 만들기 권한 삭제 = 삭제 권한
그룹 폴더를 하위 그룹에 전달	활성화하면 각 하위 그룹이 상위 데이터 파일에 액세스할 수 있습니다.
하위 그룹에 대한 권한	선택한 하위 그룹에 속한 사용자의 권한입니다: 읽기 = 읽기 전용 권한 업데이트 = 업데이트 권한 만들기 = 만들기 권한 삭제 = 삭제 권한
공유 허용	활성화된 경우 사용자는 링크를 통해 파일을 공유할 수 있습니다.



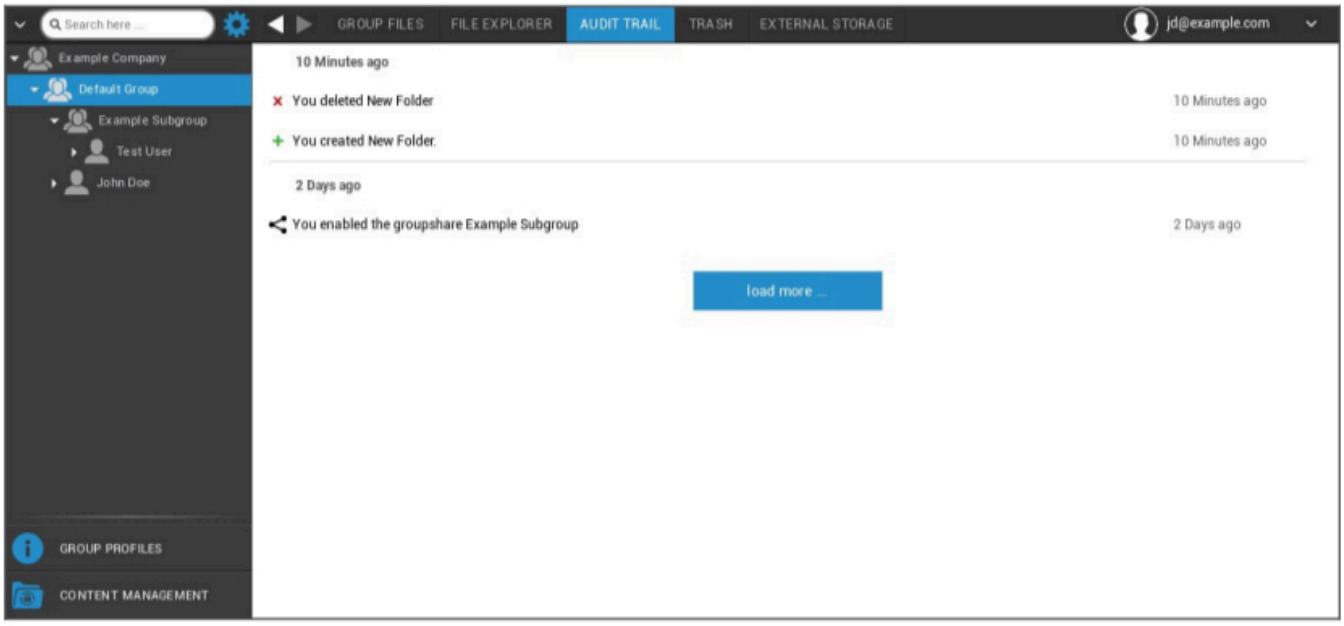
파일을 업로드하려면 드래그 앤 드롭을 통해 이 창으로 파일을 끌어와 이 필드를 사용할 수 있습니다. 이 필드를 클릭하여 인터넷 익스플로러를 사용하여 파일을 선택하고 업로드할 수도 있습니다.

파일 탐색기

'파일 탐색기'를 사용하면 파일이 저장된 그룹에 관계없이 모든 폴더와 파일을 관리할 수 있습니다.

'그룹 파일'에서 배운 설정과 버튼도 찾을 수 있습니다.

감사 추적



'감사 추적'에서는 어떤 사용자가 무엇을 만들고, 삭제하고, 공유했는지 기록을 통해 확인할 수 있습니다. 이렇게 하면 언제든지 회사 데이터로 어떤 작업이 수행되었는지 확인할 수 있습니다.

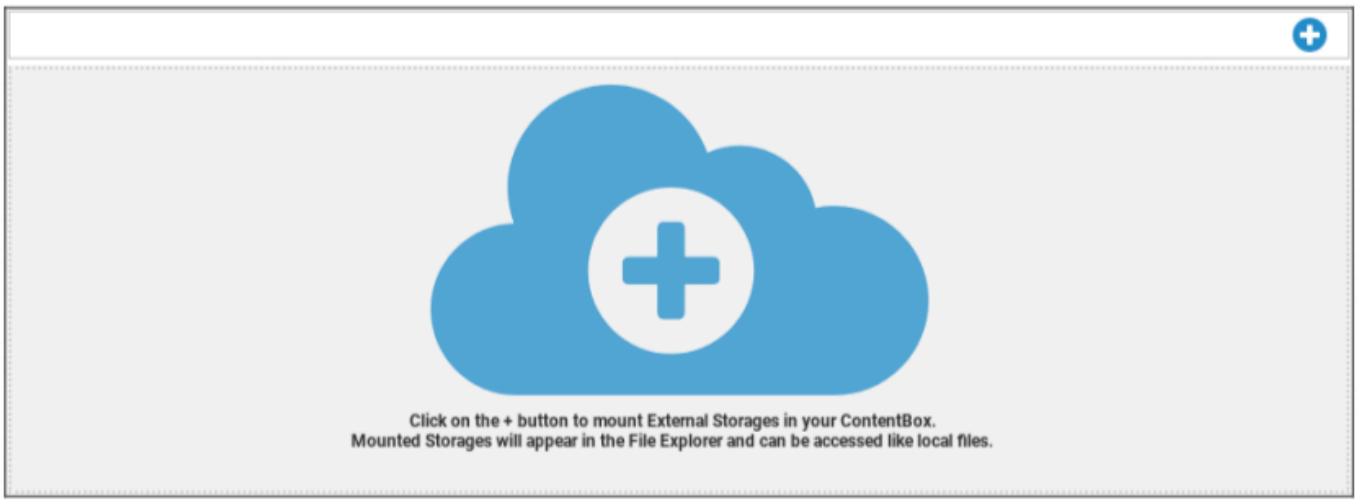
휴지통

실수로 무언가를 삭제한 경우, '휴지통'에서 폴더와 파일을 확인하고 원하는 대로 복구할 수 있습니다.

- '삭제 취소'를 사용하면 데이터/폴더를 복구할 수 있습니다.
- '삭제'를 사용하면 데이터/폴더를 영구 삭제할 수 있으며, 삭제 명령을 다시 한 번 확인해야 합니다.

휴지통에서 사용 중인 저장 용량은 사용 가능한 '총 공간'을 감소시키며, 이는 자체 클라우드 요구 사항이라는 점에 유의하세요.

외부 스토리지



'외부 저장소'라는 제목 아래에서 외부 저장소를 연결할 수 있습니다.

기호를 사용하면 (추가) 스토리지를 추가할 수 있습니다.

유형	Amazon S3, FTP, SFTP, ownCloud, WebDAV, Windows 공유, SharePoint

Amazon S3	
표시 이름	표시 이름
액세스 키	액세스 키
비밀 키	보안 키
버킷	나에게 할당된 하위 폴더의 확실한 신원 확인
호스트 이름(선택 사항)	호스트 이름(선택 사항)
포트(선택 사항)	포트(선택 사항)
지역	지역(선택 사항)
SSL 사용	SSL 사용
경로 스타일 사용	할당된 경로 주소 지우기

FTP	
표시 이름	표시 이름
호스트	호스트 주소
사용자 이름	사용자 이름
비밀번호	비밀번호
루트	메인 메뉴
보안 FTP://	

SFTP	
표시 이름	표시 이름
호스트	호스트 주소
사용자 이름	사용자 이름
비밀번호	비밀번호
루트	메인 메뉴

ownCloud	
표시 이름	표시 이름
URL	ownCloud URL
사용자 이름	사용자 이름
비밀번호	비밀번호
원격 하위 폴더	표준 폴더
보안 https://	

WebDAV	
표시 이름	표시 이름
URL	WebDAV URL
사용자 이름	사용자 이름
비밀번호	비밀번호
루트	메인 메뉴
보안 https://	
Windows 공유	Windows 공유에 대한 지원은 곧 제공될 예정입니다.
SharePoint	Microsoft SharePoint에 대한 지원은 곧 제공될 예정입니다.

감사 로그

여기에서 MDM 콘솔에서 수행된 작업에 대한 정보를 기록하는 로그를 찾을 수 있습니다.

필터 아이콘을 사용하여 표시된 목록에 필터를 적용할 수 있습니다.

드롭다운 메뉴의 **페이지당 항목** 수: 목록의 한 페이지에 표시할 항목 수를 선택할 수 있습니다.

취한 조치/설정 변경	수행한 작업 / 변경한 설정
가치	취해진 조치/변경된 설정의 값
사용자	조치를 취했거나 설정을 변경한 사용자의 이름입니다.
날짜	이 작업이 수행된 시점/이 설정이 변경된 타임스탬프
경로 / 유형	이 작업이 수행된 경로/이 설정이 변경된 경로

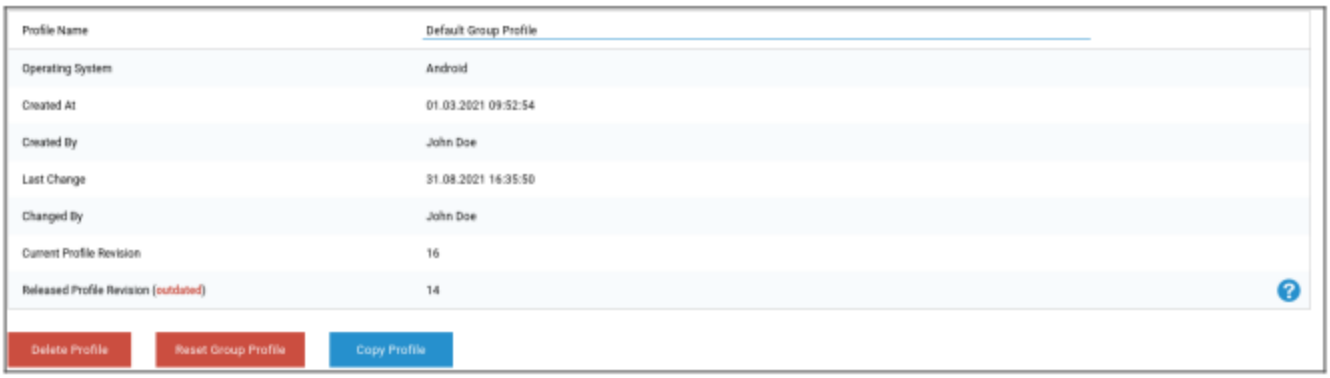
iOS 구성

일반

현재 선택한 그룹 또는 디바이스에 따라 디스플레이와 하위 포인트가 달라지니 이 점에 주의하세요!

그룹 프로필 개요(그룹 수준에서만)

그룹 프로필을 열면 프로필에 대한 간략한 개요를 볼 수 있습니다.



프로필 이름	프로필 이름(여기에서 변경 가능)
운영 체제	프로필의 운영 체제
만든 곳	생성 시간
만든 사람	프로필 작성자
마지막 변경 사항	프로필을 마지막으로 변경한 시간
변경자	마지막으로 변경한 계정
현재 프로필 수정	저장된 프로필 상태 수정
프로필 수정 버전 출시	할당된 프로필 수정본('지금 할당'). 텍스트 뒤에 '(오래된)'이라는 레이블이 표시되면 프로필을 저장했지만 아직 할당하지 않았다는 의미이므로 디바이스는 여전히 이전 버전을 받게 됩니다.

일반 정보

디바이스에 직접 접속하는 경우 선택한 디바이스에 대한 간략한 개요가 표시됩니다.

장치 이름	장치 이름
전화번호	장치 전화 번호
모델	모델 번호
운영 체제	OS
일련 번호	장치 일련 번호
디바이스 소유권	기업용 또는 개인용 디바이스 기업 = 기업용 디바이스 직원 = 개인 디바이스
디바이스 유형	디바이스 유형(태블릿 또는 휴대폰)
탈옥	기기에 탈옥이 있는 경우
감독	감독 대상 장치인지 여부를 나타냅니다.
규정 준수	가이드라인을 위반한 경우
마지막으로 본	기기가 AppTec360 서버와 마지막으로 통신한 시점의 상태

설정

이러한 설정에는 디바이스 이름과 미리 정의된 배경이 포함되어 있습니다.

장치 이름을 시스템 이름으로 지정	AppTec360 콘솔(왼쪽 계층 구조)에서 발급되는 이름은 각 최종 사용자 기기에서와 동일합니다(기기 설정에서 볼 수 있음).
사용자 지정 배경화면 사용(감독 대상 장치만 해당)	여기에서 최종 사용자 디바이스에 표시될 배경을 미리 정의할 수 있습니다 (예: 디바이스에 대한 기업 브랜딩 유형). 감독 모드에서만 사용할 수 있습니다!
자동 OS 업데이트	가능한 경우 OS 업데이트를 강제 실행합니다. 감독 모드의 DEP 장치에만 해당됩니다.
사용자 지정 글꼴	여기에서 사용자 정의 글꼴을 추가할 수 있습니다.
이름	선택 사항입니다. 글꼴의 사용자 표시 이름입니다. 이 필드는 설치 후 글꼴의 실제 이름으로 대체됩니다.
글꼴	글꼴 파일(.otf 또는 .ttf)을 업로드합니다.

구성 개정

여기에서 장치에 지정된 그룹 프로필에 대한 개요를 볼 수 있습니다.

그룹 프로필을 클릭하면 프로필에 바로 액세스하여 설정을 수행할 수 있습니다.

기호를 사용하여 할당된 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

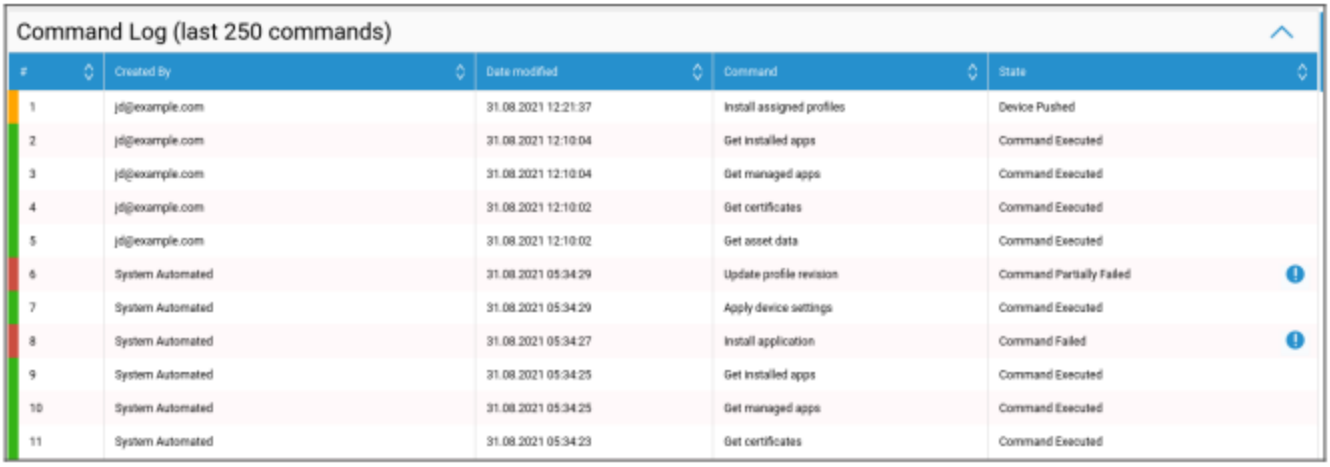
기호를 사용하면 설정이 전혀 없도록 디바이스 프로필을 초기화할 수 있습니다.

"최신 수정본 사용 가능"은 그룹 프로필이 변경되어 저장되었지만 할당되지 않았음을 나타냅니다. 변경 사항을 디바이스에 적용하려면 그룹 수준에서 '지금 할당'을 사용하여 그룹 프로필을 할당해야 합니다.

디바이스 로그(디바이스 수준에서만)

명령 로그

여기에서 디바이스에 대해 어떤 명령이 실행되었는지, 어떤 상태인지 확인할 수 있습니다.



'시스템 자동화'에 의해 생성된 명령은 시스템에 의해 자동으로 생성됩니다.

가능한 명령 상태

푸시된 장치	푸시 요청이 푸시 서비스(예: APNS)로 전송되어 디바이스가 EMM 서버에 다시 연결하도록 지시합니다.
명령 생성	이 명령은 시스템에서 생성되었습니다.
명령 전송	명령은 서버에 연결한 후 디바이스로 전송되었습니다.
명령 실행	명령이 성공적으로 실행되었습니다.
명령 실패	명령이 실패했습니다. *
명령이 부분적으로 실패했습니다.	디바이스 OS에 따라 일부 명령이 함께 그룹화될 수 있습니다. 이 경우 이 명령 그룹의 일부가 실패했습니다. *
명령 실행, 결국 실패	명령이 실행되었지만 실행되지 않았을 수도 있습니다.
명령 재푸시	명령이 사용자에 의해 다시 푸시되었습니다.
폐기됨	명령이 삭제되었습니다. 예를 들어 다른 명령으로 대체되었거나 디바이스가 다시 등록되어 이전 명령이 제거되었기 때문입니다.

메시지 뒤에 느낌표가 있는 경우 커서로 아이콘 위에 마우스를 가져가면 자세한 정보를 확인할 수 있습니다.

자산 관리(디바이스 수준에서만)

자산 관리(디바이스 수준에서만)

장치 정보

모델	디바이스 모델 번호
운영 체제	OS
OS 버전	OS 버전
일련 번호	일련 번호
UDID	디바이스 UDID
장치 이름	장치 이름
감독	장치가 감독되고 있는지 표시
배터리 상태	배터리 상태

Wi-Fi

IP 주소	디바이스 IP 주소
WiFi MAC	WiFi MAC 주소

셀룰러

상태	상태(SIM 카드 유무)
전화번호	전화 번호
로밍 상태	현재 로밍 상태
로밍(음성/데이터)	음성/데이터 로밍 상태
IP 주소	IP 주소
IMEI	IMEI-번호
사업자/이동 통신사	셀룰러 서비스 제공업체
SIM 이동 통신사 네트워크	SIM 이동 통신사 네트워크
통신사 버전	통신사 버전
모뎀 펌웨어	모뎀 펌웨어
현재 MCC/MNC	"SIM MCC/MNC" 참조
SIM MCC/MNC	모바일 국가 코드는 모바일 네트워크 코드(MNC)와 함께 셀룰러 네트워크(=국가 코드)를 식별하는 데 사용되는 E.212 표준에 따라 ITU에서 확립한 국가 식별 코드입니다. 따라서 다른 셀룰러 네트워크에 들어가면 '현재 MCC/MNC'와 'SIM MCC/MNC'가 달라집니다.

블루투스

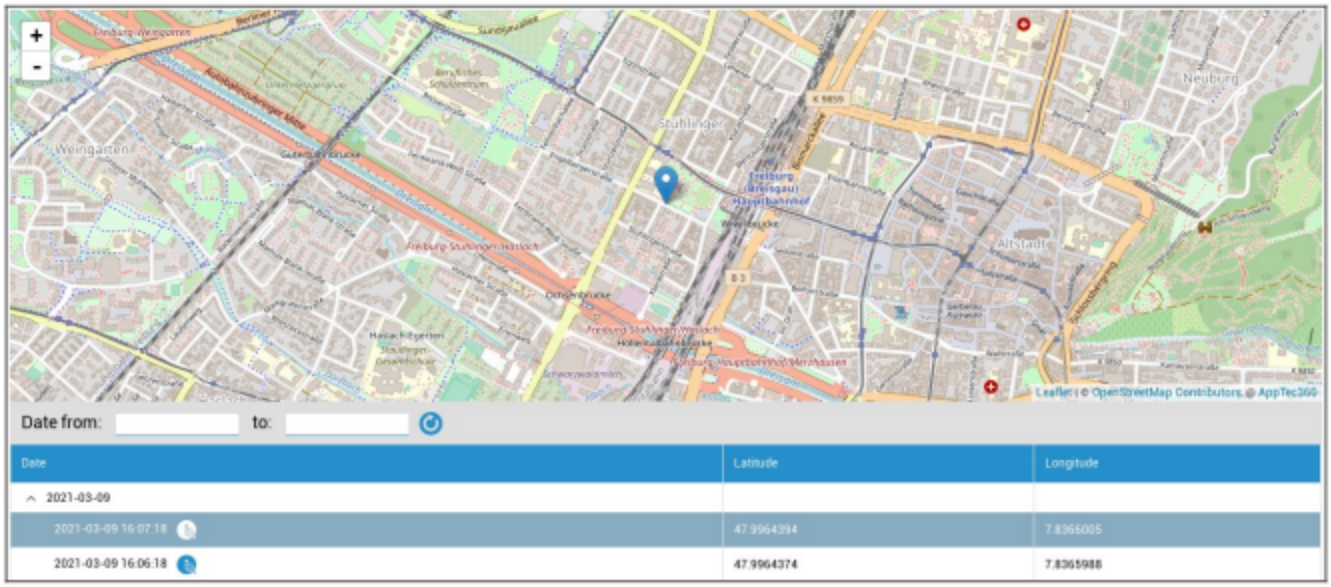
블루투스 MAC	블루투스 MAC 주소

보안 관리

도난 방지(디바이스 수준에서만)

GPS 정보(디바이스 수준에서만)

여기에서 디바이스의 현재/마지막 위치를 확인할 수 있습니다. 현지화는 하나 또는 두 개의 비밀번호로 보호할 수 있습니다(참조하세요: 일반 설정 - 개인정보 - GPS 액세스



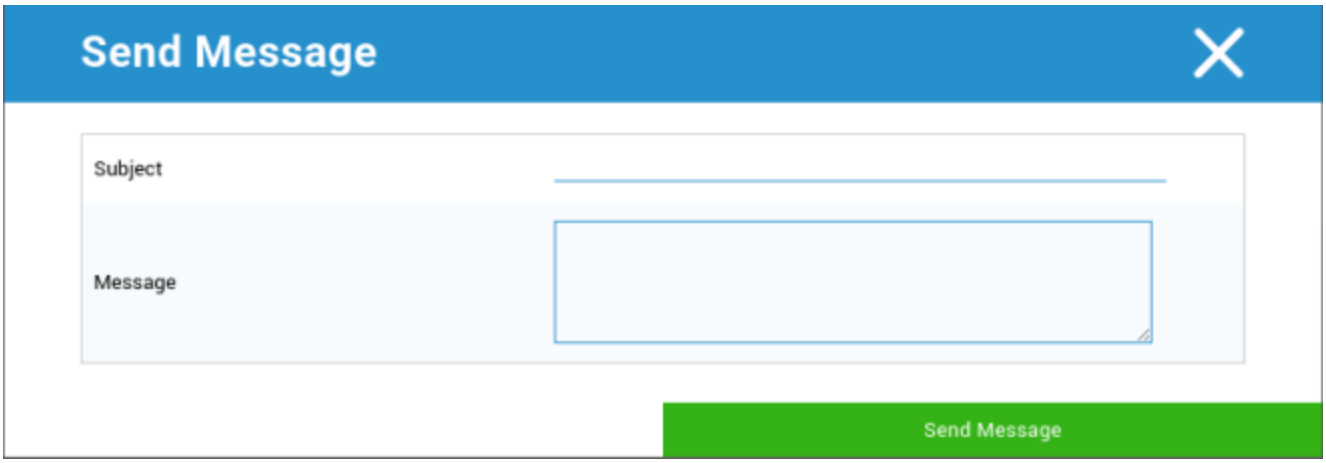
지우기 및 잠금(기기 수준에서만)

'삭제 및 잠금'에서 다음 세 가지 작업을 수행할 수 있습니다:

전체 삭제	장치가 공장 설정으로 복원됩니다(회사 및 개인 데이터가 삭제됨).
엔터프라이즈 삭제	최종 사용자 기기에서 기업 데이터만 제거됩니다(앱텍에서 제공한 모든 앱, 데이터 등).
잠금 화면	화면 잠금이 활성화되어 있으면 기기 비밀번호/PIN으로 기기 잠금을 해제하는 것으로 충분합니다.
포렌식 잠금(감독 대상 장치만 해당)	 기호를 사용하여 이 기능을 활성화하면 기기가 잠기며 닫을 수 없다는 메시지가 표시됩니다. 직원도 디바이스의 잠금을 해제할 수 없습니다. 관리자만 콘솔에서 잠금 해제() 기호를 사용하여 디바이스의 잠금을 해제할 수 있습니다.
활성화 잠금 허용(감독되는 장치만 해당)	이 기능이 활성화되면 , iCloud 설정에서 "내 iPhone 찾기"가 활성화 되 자마자 기기가 잠 깁니다.

메시지(디바이스 수준에서만)

다음 창에서 제목과 메시지를 입력하고 최종 사용자 디바이스로 보낼 수 있습니다:



보안 구성

암호

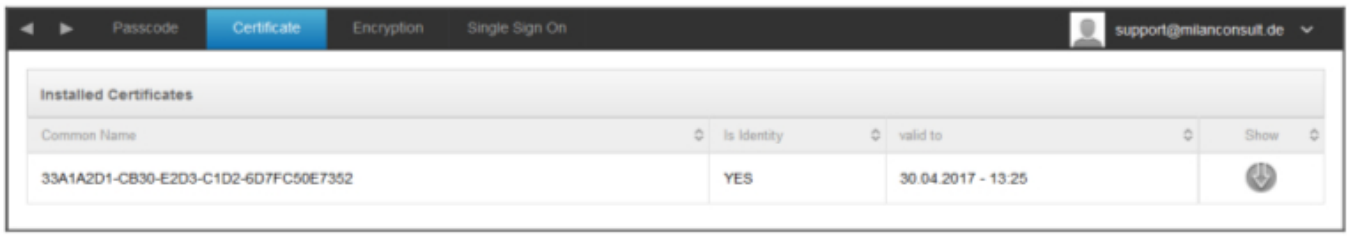
여기에서 디바이스 비밀번호 설정을 설정합니다.

코드 비활성화 허용	이 설정이 활성화되면 비밀번호를 입력하라는 메시지가 표시되지 않습니다. 비밀번호가 설정되면 비활성화할 수 없습니다.
단순 값 허용	사용자가 동일한 숫자 문자열(예: 1234, 1111)을 에스컬레이션 및 축소하여 사용할 수 있도록 허용합니다.
영숫자 값 필요	비밀번호는 하나 이상의 문자를 포함해야 합니다.
최소 암호 길이	최소 비밀번호 길이
복잡한 문자의 최소 개수	비밀번호의 영숫자 기호 최소 개수
최대 암호 사용 기간	비밀번호를 변경해야 하는 기간(일수)
최대 자동 잠금	최대 시간, 그 이후에는 장치가 잠깁니다.
기기 잠금의 최대 유예 기간	시간, 그 후 기기가 잠긴 대기 모드로 전환됩니다.
최대 실패 시도 횟수	전체 장치 초기화가 수행되기 전에 비밀번호를 잘못 입력할 수 있는 빈도를 설정합니다.
최대 암호 유효 기간 (1~730일)	최대 비밀번호 사용 기간
비밀번호 기록(1~50개 비밀번호)	이 번호 이후에는 이전 비밀번호를 사용할 수 있습니다.

휴지통을 클릭하면 비밀번호 재설정 대화 상자가 열리고, 여기서 잊어버린 장치 비밀번호를 지울 수 있습니다.

인증서(디바이스 수준에서만)

장치에서 사용할 수 있는 인증서를 표시합니다.



암호화

스토리지 암호화 필요	설치된 장치 암호화 기능 활성화

싱글 사인온

"싱글 사인온" 항목에서 Kerberos 인증을 구성할 수 있습니다.

여기에서 액세스 자격 증명과 Kerberos 토큰을 사용할 수 있는 각 URL/앱을 설정합니다.

감독 모드에서 사용 가능	
계정 이름	계정 이름
학교장 이름	Kerberos 티켓을 배포할 수 있는 고유 ID
영역	사용할 Kerberos 영역(예: 도메인)

심볼을 사용하여 추가 URL을 설정할 수 있습니다.

이 계정을 제한하는 데 사용되는 URL 패턴	Kerberos 티켓을 배포할 수 있는 URL을 결정할 수 있습니다.

심볼을 사용하여 추가 앱을 설정할 수 있습니다.

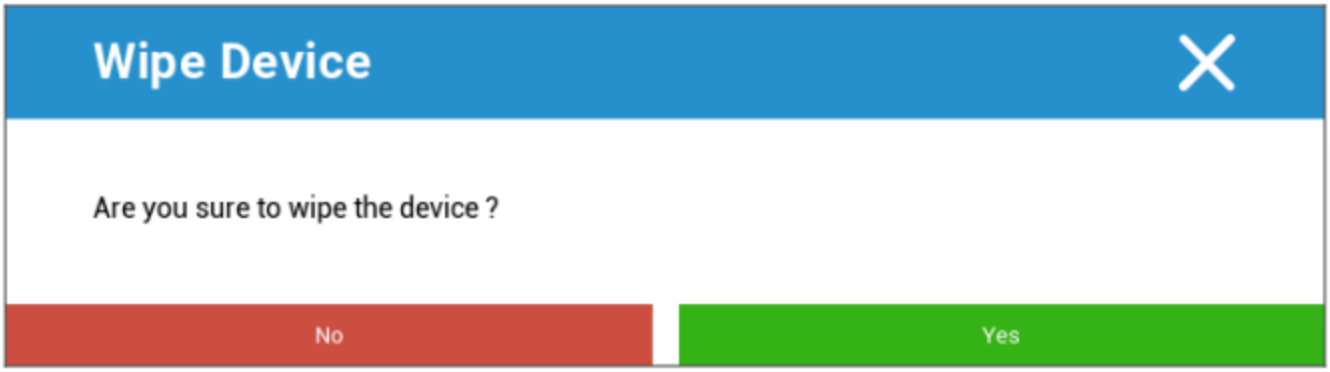
이 계정을 제한하는 앱	결정 예정, Kerberos 티켓을 배포할 수 있는 앱

수명 종료(디바이스 수준에서만)

지우기(디바이스 수준에서만)

'초기화'에서 장치를 공장 설정으로 복원할 수 있습니다. 여기에서는 회사 데이터와 개인 데이터가 최종 사용자 장치에서 삭제됩니다.

'마이너스 기호'를 클릭하면 다음과 같은 메시지가 표시됩니다.



"예"를 선택하면 지우기를 수행할 수 있습니다.

"삭제 보고서" 아래에 다음 항목이 표시될 수 있습니다.

지운 사람	삭제한 사람에 대한 기록
날짜	날짜
상태	상태(예: 초기화가 성공적으로 수행된 경우)

제한 설정

디바이스 기능

여기에서 개별 최종 사용자 디바이스 기능을 차단할 수 있습니다.

앱 설치 허용	앱 설치 허용
카메라 허용	카메라 사용 허용
FaceTime 허용	FaceTime 허용
화면 캡처 허용	화면 캡처 허용
로밍 중 자동 동기화 허용	로밍 중 자동 동기화 허용
Siri 허용	Siri 허용
음성 다이얼링 허용	음성 다이얼링 허용
인앱 구매 허용	인앱 구매 허용
모든 구매에 iTunes Store 암호 요구	모든 구매에 iTunes Store 암호 요구
멀티플레이어 게임 허용	멀티플레이어 게임 허용
게임 센터 친구 추가 허용	게임 센터 친구 추가 허용
관리되는 항목에서 관리되지 않는 항목으로 열기 허용	관리되는 앱의 콘텐츠를 관리되지 않는 앱에서 열 수 있도록 허용
비관리형에서 관리형으로 열기 허용	관리되는 앱에서 관리되지 않는 앱의 콘텐츠 열기 허용
잠금 화면에서 오늘 보기 허용	이 설정이 활성화되면 잠금 화면의 알림 센터에 '오늘' 보기가 표시됩니다.
잠금 화면에서 제어 센터 허용	잠금 화면에서 제어 센터 허용
TouchID 허용	TouchID 허용
무선 PKI 업데이트 허용	무선 PKI 업데이트 허용
잠긴 상태에서 통장 허용	기기가 잠겨 있는 동안 통장 허용
광고 추적 제한	이 기능은 광고 추적을 비활성화합니다(예: 광고주가 개인 맞춤 광고를 배포하기 위해 광고 추적을 사용할 수 없음).
핸드오프 허용	핸드오프 허용
인터넷 검색 결과에 스포트라이트 허용	인터넷 검색 결과를 스포트라이트에 표시하도록 허용(예: Bing 또는 Wikipedia)

첫 번째 AirPlay 페어링 시 암호 필요	첫 번째 AirPlay 페어링 시 암호 필요
포스 워치 손목 보호	활성화하면 Apple Watch는 "손목 보호"(손목 인식)를 강제로 사용합니다.
iCloud 사진 보관함 허용	iCloud 사진 보관함을 허용합니다. 허용하지 않으면 iCloud에서 완전히 다운로드되지 않은 모든 사진이 로컬 저장 공간에서 지워집니다.
감독 모드에서 사용 가능	
계정 수정 허용	'메일, 연락처, 캘린더' 수정 허용
에어드롭 허용	에어드롭 허용
앱 셀룰러 수정 허용	이 설정은 모바일 데이터를 사용할 수 있는 앱에 대한 설정을 차단합니다. 예를 들어 이 설정은 최종 사용자 디바이스에서 수동으로 설정한 다음 이 제한을 활성화할 수 있습니다.
Siri가 웹에서 사용자 생성 콘텐츠를 쿼리하도록 허용하기	누구나 원하는 대로 변경할 수 있기 때문에 특정 웹사이트(예: 위키피디아)의 웹 검색이 차단됩니다.
Siri 욕설 필터 활성화	Siri를 향한 욕설은 검열됩니다.
아이북 스토어 허용	아이북 스토어 허용
아이북 스토어 에로티카 허용	아이북 스토어 에로티카 허용
내 친구 찾기 설정 수정 허용	내 친구 찾기 설정 수정 허용
게임 센터 허용	게임 센터 허용
호스트 페어링 허용	컴퓨터 페어링 제어
구성 프로필 설치 허용	구성 프로필 설치 허용
앱 제거 허용	앱 제거 제어
iMessage 허용	iMessage 허용
모든 콘텐츠 및 설정 지우기 허용	모든 콘텐츠 및 설정 삭제 허용
제한 구성 허용	제한 구성 허용
팟캐스트 허용	팟캐스트 허용
정의 조회 허용	정의 조회 허용
예측 키보드 허용	예측 키보드 허용
자동 수정 허용	자동 수정 허용
UI 앱 설치 허용	비활성화하면 공용 AppStore에서 앱을 설치할 수 없습니다(아이콘이 더 이상 표시되지 않음). 그러나 iTunes 및 구성기를 통해 앱을 계속 설치할 수 있습니다.

키보드 단축키 허용	장치가 물리적 키보드에 연결된 경우 키보드 단축키를 허용합니다.
Apple Watch 페어링 허용	장치와 Apple Watch 간의 페어링을 금지하면 기존 연결이 종료됩니다.
비밀번호 수정 허용	허용되지 않으면 장치 비밀번호를 추가, 변경 또는 제거할 수 없습니다.
장치 이름 수정 허용	디바이스 이름 변경 가능 여부를 결정하는 가이드라인
배경화면 수정 허용	배경화면 변경 가능 여부를 결정하는 가이드라인
자동 앱 다운로드 허용	비활성화하면 구매한 앱이 다른 디바이스에 자동으로 설치되지 않습니다. 기존 앱의 업데이트에는 적용되지 않습니다.
뉴스 허용	iOS 기기에서 뉴스 허용
엔터프라이즈 앱 신뢰 허용	false로 설정하면 엔터프라이즈 앱을 신뢰하지 않습니다.

iCloud

iCloud 페어링 중 특정 기능 차단하기

백업 허용	백업 허용
문서 동기화 허용	문서 동기화 허용
사진 스트림 허용	사진 스트림 허용
공유 사진 스트림 허용	공유 사진 스트림 허용
클라우드 키체인 동기화 허용	클라우드 키체인 동기화 허용
관리되는 앱에서 데이터 저장 허용	관리되는 앱에서 데이터 저장 허용
엔터프라이즈 북의 노트 및 하이라이트 동기화 허용	엔터프라이즈 북에 노트 및 하이라이트 동기화 허용
엔터프라이즈 장부 백업 허용	엔터프라이즈 장부 백업 허용

보안 및 개인정보 보호

진단 데이터와 관련된 다음 기능을 차단합니다.

진단 데이터를 Apple로 전송하도록 허용	진단 데이터를 Apple로 전송하도록 허용
사용자가 신뢰할 수 없는 TLS 인증서 수락 허용	사용자가 신뢰할 수 없는 TLS 인증서 수락 허용
강제 암호화 백업	강제 암호화 백업

BYOD

기본 제공 iOS 보안(컨테이너)

iOS는 항상 관리형(비즈니스)과 비관리형(개인)을 구분할 수 있었습니다. MDM 시스템에서 제공되는 모든 것은 관리되는 것으로 취급됩니다. 예를 들어 MDM을 통해 앱을 설치하거나 Exchange 계정을 구성하는 경우 iOS에서 관리되는 것으로 취급됩니다.

그 외 장치에 수동으로 구성/설치되는 모든 항목은 관리되지 않는 것으로 처리됩니다. 예를 들어 사용자가 자체적으로 WhatsApp을 설치하거나 Exchange 계정을 추가하는 경우 등이 이에 해당합니다. 그러나 이러한 분리는 연락처에는 영향을 미치지 않았습니다. 하지만 iOS 11.3(이상)부터는 연락처에도 이 기능이 추가되었습니다.

이것은 운영 체제의 기본 기능이므로 무언가를 설치하거나 특별한 컨테이너를 설정할 필요가 없습니다.

기본 제공 기능을 활성화하여 개인용 앱과 업무용 앱/정보/파일을 분리하세요. 이 설정은 실수로 이 분리 기능의 일부를 해제할 수 있는 일부 다른 기능도 비활성화합니다.

활성화

AppTec360에서 지원하는 컨테이너 솔루션 활성화

Google 분할 컨테이너 사용	Google 분할 컨테이너 사용
SecurePIM 컨테이너 활성화	SecurePIM 컨테이너 활성화

SecurePIM 컨테이너를 활성화했다면 '활성화'에서도 다음 사항을 확인할 수 있습니다. 또한 아래에 설명된 네 개의 탭이 바로 추가로 열립니다.

지원 이메일 주소	사용자가 문제를 문의할 수 있는 지원 이메일 주소

SecurePIM 비밀번호

'SecurePIM 비밀번호'에서 비밀번호 보안 강도에 대한 가이드라인을 설정할 수 있습니다.

세션 시간 초과	여기에서 SecurePIM이 백그라운드에서 실행되면 몇 분 후에 새 비밀번호를 다시 입력해야 하는지 설정할 수 있습니다.
비밀번호 길이	SecurePIM 컨테이너에 액세스하기 위한 비밀번호 길이
대문자	최소 대문자
소문자	최소 소문자
특수 문자	최소 특수 문자
숫자	최소 숫자
애플리케이션 삭제	비밀번호를 잘못 입력한 횟수만큼 SecurePIM 콘텐츠가 삭제됩니다. (하지만 앱은 여전히 최종 사용자 디바이스에 남아 있습니다.)

SecurePIM 보안

"SecurePIM 보안"에서 다양한 보안 설정을 설정할 수 있습니다.

탈옥된 디바이스 탐지	이 설정을 활성화하면 기기가 탈옥된 것으로 감지되는 즉시 SecurePIM 컨테이너에 대한 액세스가 차단됩니다.
텍스트 필드 보안	제출 필드의 콘텐츠는 암호화되며, 어떠한 정보도 OS(iOS)에 전달되지 않습니다. 참고: 이 설정이 활성화되어 있는 한 자동 수정 기능을 더 이상 사용할 수 없습니다.
연락처 데이터를 디바이스로 내보내기	이 설정이 활성화되면 사용자는 Exchange 연락처를 로컬 장치로 내보낼 수 있습니다. 참고: 이름과 전화번호만 내보내집니다.
이벤트 위치 표시	이 설정을 활성화하면 예정된 이벤트의 위치가 알림 표시줄에 표시됩니다.
이벤트 제목 표시	이 설정을 활성화하면 예정된 이벤트 제목의 위치가 알림 표시줄에 표시됩니다.

SecurePIM 브라우저

여기에서 SecurePIM의 브라우저를 구성할 수 있습니다.

기호를 사용하여 새 URL을 정의할 수 있습니다.

기호를 사용하여 정의된 URL을 다시 제거할 수 있습니다.

"화이트리스트 URL"은 로드할 수 있는 URL입니다.

'블랙리스트에 등록된 URL'은 로드할 수 없어 차단된 URL입니다.

화이트리스트 항목은 블랙리스트 항목보다 우선순위가 높다는 점에 유의하세요. "북마크 제목"에서 제목을 지정할 수 있습니다. "북마크 URL"을 사용하면 URL 주소를 북마크 제목과 연결할 수 있으므로 각 사용자에게 개별화된 북마크를 배포할 수 있습니다.

교환

'Exchange'에서 Exchange 계정을 구성할 수 있습니다.

ActiveSync 이메일 주소	교환 이메일 주소('자리 표시자'에 유의)
ActiveSync Exchange 로그인	사용자 이름 교환('자리 표시자'에 유의)
ActiveSync Exchange Server	Exchange 서버 주소(FQDN)
ActiveSync Exchange 도메인	교환 도메인 주소
사용자 인증서	사용자 인증서
인증서 기반 인증	사용자가 인증서로 본인 인증
S/MIME 암호화 허용	사용자가 메일을 암호화할 수 있습니다.
S/MIME 서명 허용	사용자가 메일에 서명할 수 있도록 허용
CRL 확인	활성화된 경우, 개인 인증서는 CRL(인증서 해지 목록)과 비교됩니다.

연결 관리

Wi-Fi

서비스 집합 식별자(SSID)	연결할 네트워크의 SSID
자동 가입	네트워크에 가입할 때 자동 가입 활성화
숨겨진 네트워크	AP가 SSID를 브로드캐스트하지 않는 경우 활성화합니다.

프록시 설정

모든 액세스 포인트에 대한 프록시 구성

없음		프록시 설정 안 함
매뉴얼		수동 프록시 설정
	프록시 서버 URL	프록시 설정에 액세스하기 위한 주소
	포트	프록시용 포트 설정
	인증	프록시에서 인증할 사용자 이름
	비밀번호	프록시에서 인증하기 위한 비밀번호
자동		자동으로 프록시 설정
프록시 서버 URL		프록시 설정에 액세스하기 위한 URL

보안 유형

AP의 보안 유형 설정

WEP	
비밀번호	AP의 비밀번호

WPA/WPA2	
비밀번호	AP의 비밀번호

WEP 엔터프라이즈 - WPA/WPA2 엔터프라이즈 - 모든 엔터프라이즈		
프로토콜		
TLS	활성화/비활성화	
TTLS	활성화/비활성화	
LEAP	활성화/비활성화	
PEAP	활성화/비활성화	
EAP-FAST	활성화/비활성화	
EAP-SIM	활성화/비활성화	
PAC 사용		PAC(보호 액세스 제어) 사용
프로비저닝 PAC	프로비저닝 PAC 구성	
익명으로 PAC 프로비저닝	PAC의 익명 제공	
내부 인증	사용해야 하는 인증 프로토콜입니다: PAP, CHAP, MSCHAP, MSCHAPv2	
사용자 이름	인증 사용자 이름	
연결별 비밀번호를 사용하지 마세요.	연결별 비밀번호를 사용하지 마세요.	
신원 증명서	인증 인증서 업로드/선택	
외부 정체성	외부에서 볼 수 있는 신원	
신뢰		
신뢰할 수 있는 인증서 1	첫 번째 신뢰할 수 있는 인증서 업로드	
신뢰할 수 있는 인증서 2	두 번째 신뢰할 수 있는 인증서 업로드	
신뢰할 수 있는 인증서 3	신뢰할 수 있는 세 번째 인증서 업로드	
신뢰할 수 있는 서버 인증서 이름	예상 서버 인증서의 이름 (쉼표로 구분된 목록)	

없음	보안 설정 안 함

VPN

연결 이름	VPN 프로필 이름

VPN 유형

VPN

모든 기기 네트워크 트래픽은 VPN 연결을 통해 라우팅됩니다.

연결 유형	VPN 연결 유형 설정
IPsec(cisco)	시스코의 IPsec 프로토콜
PPTP	PPTP 프로토콜
L2TP	L2TP 프로토콜
Cisco AnyConnect	애니커넥트 프로토콜
주니퍼 SSL	주니퍼 SSL 프로토콜
F5 SSL	F5 SSL 프로토콜
SonicWall mConnect	SonicWall 모바일 연결
아루바 비아	아루바 VIA 프로토콜
사용자 지정 SSL	사용자 지정 SSL을 통한 연결
OpenVPN	OpenVPN 프로토콜

앱별 VPN

특정 앱을 열면 VPN 연결이 설정됩니다.

앱별 VPN 연결 자동 시작	앱별 VPN 연결 자동 시작
연결 유형	VPN 연결 유형 설정
Cisco AnyConnect	애니커넥트 프로토콜
주니퍼 SSL	주니퍼 SSL 프로토콜
F5 SSL	F5 SSL 프로토콜
SonicWall mConnect	SonicWall 모바일 연결
아루바 비아	아루바 VIA 프로토콜
사용자 지정 SSL	사용자 지정 SSL을 통한 연결
OpenVPN	OpenVPN 프로토콜

프록시 설정

VPN 연결을 위한 프록시 구성

없음	프록시 설정 안 함
매뉴얼	수동으로 프록시 설정
프록시 서버 URL	프록시 설정에 액세스할 수 있는 주소
포트	프록시용 포트 설정
인증	프록시에서 인증할 사용자 이름
비밀번호	프록시에서 인증을 위한 비밀번호
자동	자동으로 프록시 설정
프록시 서버 URL	프록시 설정에 액세스하기 위한 URL

자리 표시자 표시	AppTec360이 사용할 수 있는 모든 사용 가능한 사용자 변수를 표시합니다.

APN

액세스 포인트 이름	액세스 포인트 이름
액세스 포인트 사용자 이름	액세스 포인트 사용자 이름
액세스 포인트 비밀번호	액세스 포인트 비밀번호
프록시 서버	프록시 서버 주소
포트	각 프록시 포트

셀룰러

데이터 로밍 활성화	데이터 로밍 활성화
음성 로밍 활성화	음성 로밍 활성화
핫스팟 사용	핫스팟 사용

HTTP 프록시

프록시 유형	
매뉴얼	수동으로 프록시 설정
프록시 서버 URL	프록시 설정에 액세스할 수 있는 주소
포트	프록시 포트 설정
인증	프록시에서 인증할 사용자 이름
비밀번호	프록시에서 인증을 위한 비밀번호
자동	자동으로 프록시 설정
프록시 PAC URL	프록시 PAC URL
PAC에 연결할 수 없는 경우 직접 연결 허용	PAC에 연결할 수 없는 경우 직접 연결 허용(VPN 없이)
프록시를 우회하여 캡티브 네트워크에 액세스하도록 허용	프록시를 우회하여 종속 내부 네트워크에 액세스하도록 허용

AirPrint

IP 주소	프린터 IP 주소
리소스 경로	AirPrint 장치로 가는 확실한 경로

AirPlay

장치 이름	장치 이름
비밀번호	페어링 비밀번호
화이트리스트	디바이스가 독점적으로 페어링할 수 있는 디바이스 목록을 정의합니다.

PIM 관리

Exchange Active 동기화

계정 이름		이메일 계정 이름
Exchange ActiveSync 호스트		서버의 주소/FQDN
이동 허용		이메일 이동 허용
메일에서만 사용		기본 메일 앱에서만 상호 작용이 발생할 수 있습니다.
SSL 사용		SSL 암호화 사용
도메인		서버 도메인
사용자		사용자 이름
이메일 주소		이메일 주소(디바이스 수준에서만)
비밀번호(디바이스 수준에서만)		사용자 비밀번호
신원 증명서		서버에서 인증할 각 인증서를 선택합니다.
동기화할 메일의 지난 날짜		이메일이 다시 동기화될 때까지의 기간(일수)입니다. 제한 없음 = 무제한
S/MIME 사용		S/MIME 암호화 사용
	서명 인증서	각 서명 인증서를 업로드합니다.
	암호화 인증서	각 암호화 인증서 업로드

이메일

최종 사용자 디바이스에서 POP3 / IMAP 계정 설정

계정 설명	이메일 계정 이름		
계정 유형	IMAP	경로 접두사	특수 폴더의 경로 접두사
	POP		
사용자 표시 이름	사용자 표시 이름		
이메일 주소	사용자 이메일 주소		
이동 허용	이메일 이동 허용		
S/MIME 사용	S/MIME 암호화 사용		
서명 인증서	각 서명 인증서를 업로드합니다.		
암호화 인증서	각 암호화 인증서 업로드		

수신 메일

수신 서버 설정

메일 서버 주소	메일 서버 주소
메일 서버 포트	메일 서버 포트
사용자 이름	각 사용자 이름
인증 유형	인증 유형
없음	인증 유형 없음
비밀번호(디바이스 수준에서만)	비밀번호 프롬프트
MDM 도전 과제-대응	
NTLM	NTLM-인증
HTTP MD5 다이제스트	
SSL 사용	필요한 경우 SSL 사용

발신 메일

발신 서버 설정

메일 서버 주소	메일 서버 주소
메일 서버 포트	메일 서버 포트
사용자 이름	각 사용자 이름
인증 유형	
없음	인증 방법 없음
비밀번호(디바이스 수준에서만)	비밀번호 프롬프트
MDM 도전 과제-대응	
NTLM	NTLM-인증
HTTP MD5 다이제스트	
SSL 사용	필요한 경우 SSL 사용
수신 비밀번호와 동일한 발신 비밀번호	수신 비밀번호와 동일한 발신 비밀번호
메일에서만 사용	모든 발신 이메일을 메일 앱을 통해 보내려면 활성화합니다.

CalDav

CalDav 계정의 설정 및 배포를 구성합니다.

계정 설명	계정의 표시 이름
호스트 이름	호스트 이름 및/또는 IP 주소
포트	CalDav 계정의 포트
주요 URL	계정의 기본 URL
사용자 이름	각 CalDav 사용자 이름
비밀번호(디바이스 수준에서만)	각 CalDav 비밀번호
SSL 사용	필요한 경우 SSL 사용

구독 캘린더

구독 캘린더 설정 및 배포

설명	계정의 표시 이름
URL	캘린더 데이터베이스의 URL
사용자 이름	캘린더 구독의 사용자 이름
비밀번호(디바이스 수준에서만)	캘린더 구독의 비밀번호
SSL 사용	필요한 경우 SSL 사용

LDAP

이 영역에서 최종 사용자 장치와 Active Directory 간에 동적 인증서 교환을 허용하기 위해 LDAP 연결을 설정합니다.

선택한 사용자에게는 해당 읽기 권한이 필요합니다.

계정 설명	계정 설명
계정 사용자 이름	LDAP 액세스용 사용자
계정 비밀번호	LDAP 액세스를 위한 비밀번호
계정 호스트 이름	LDAP 서버 호스트 이름/IP 주소
SSL 사용	필요한 경우 SSL 사용

두 번째 부분에서는 LDAP 레지스트리에서 검색할 개별 필터를 정의할 수 있습니다.

설명	범위	검색 기반

필터 설명	LDAP 레지스트리의 검색 수준	개별 필터 정의

웹 관리

웹 클립

이 위치에서 웹페이지, 인트라넷 포털 등의 링크가 포함된 북마크를 정의하면 최종 사용자 장치에서 애플리케이션으로 표시됩니다.

라벨	최종 사용자 디바이스의 연결 이름
URL	각 웹사이트로 연결되는 링크
이동식	활성화된 경우 사용자는 웹 클립을 제거할 수 있습니다.
아이콘	이 대화 상자에서 연결에 사용할 로고를 업로드합니다: 크기 180x180, png 형식
미리 구성된 아이콘	활성화하면 아이콘에 추가 효과(그림자, 반사)가 표시되지 않습니다.
전체 화면	웹 클립을 열면 브라우저가 전체 화면 모드로 열립니다.

웹 콘텐츠 필터

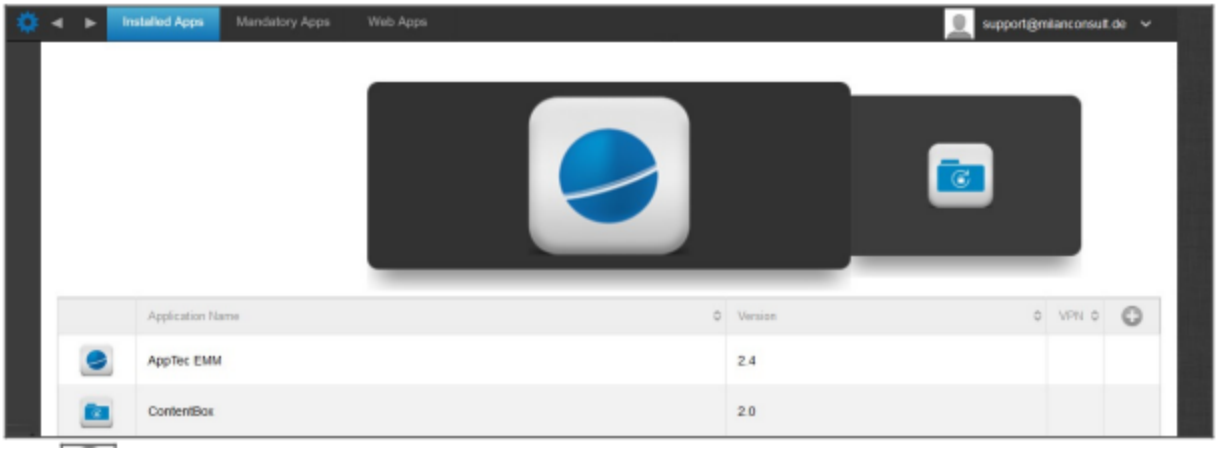
웹 콘텐츠 필터를 사용하면 특정 인터넷 페이지에 대한 액세스를 제한할 수 있습니다.

허용된 웹사이트	
성인용 콘텐츠 제한	성인용 콘텐츠에 웹 필터가 자동으로 적용됩니다.
허용된 URL	기호를 사용하여 허용된 페이지를 추가합니다.
블랙리스트 URL	기호를 사용하여 차단된 페이지 추가
특정 웹사이트만 해당	특정 콘텐츠만 표시할 수 있으며, + 기호를 사용하여 추가할 수 있습니다.

앱 관리

엔터프라이즈 앱 관리자

설치된 앱(디바이스 수준에서만)



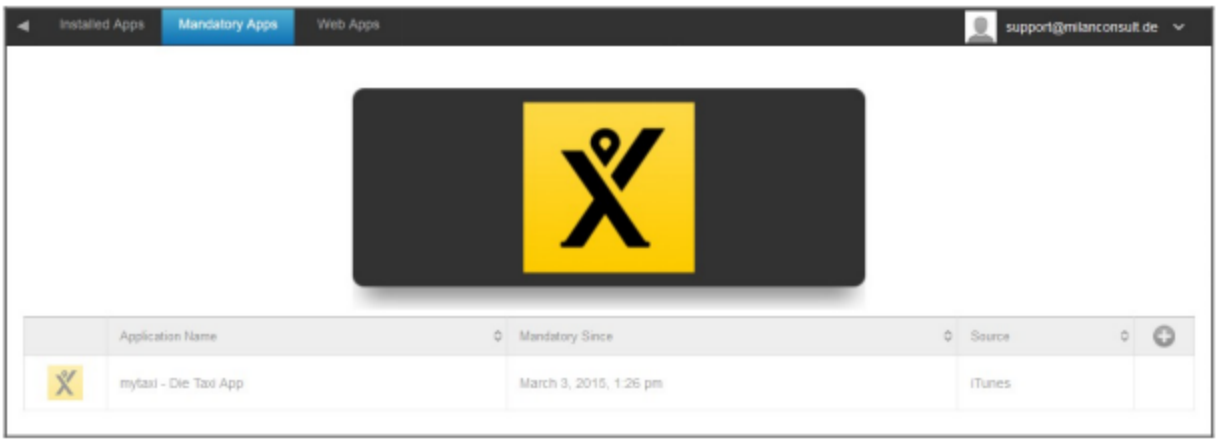
여기에서 현재 디바이스에 설치된 앱을 확인할 수 있습니다.

필수 앱

필수 앱에서 필수 앱을 지정할 수 있습니다.

언급된 앱을 설치하라는 알림이 계속 표시됩니다.

를 통해 필수 앱을 정의할 수 있습니다.



Apple 앱스토어 앱일 수도 있고 사내 앱일 수도 있습니다.

감독 대상 장치와 관련된 경우 앱이 자동으로 설치됩니다.

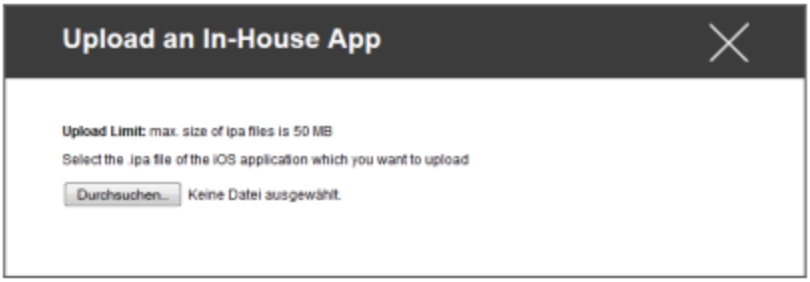
공개 앱스토어의 'Apple 앱스토어' 앱은 물론 내부적으로 개발한 사내 앱도 디바이스에 푸시할 수 있습니다.

또는 'iOS 사내 앱' 카테고리에서 일반 설정에서 업로드한 사내 앱을 선택할 수 있습니다.

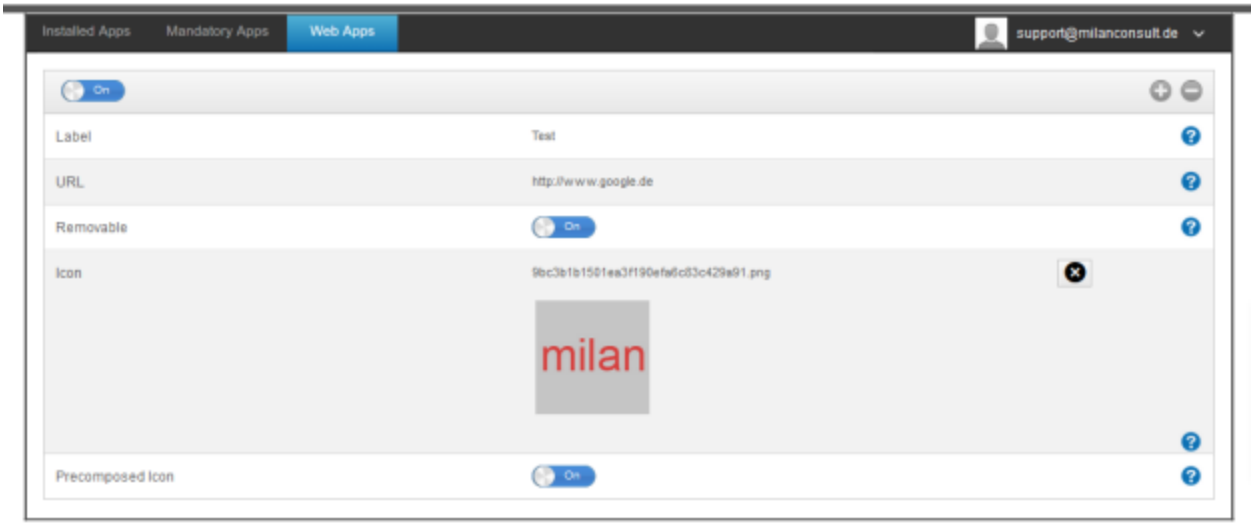
설치 옵션

최신 상태 유지(디바이스당 VPP만 지원)	일주일에 한 번 앱에 대한 업데이트가 있는지 확인합니다. 그렇다면 이 업데이트가 설치됩니다. 인하우스 앱의 경우 일반 설정에서 구성한 업데이트 대상이 업데이트 프로세스에 사용됩니다.
관리되지 않는 경우 추월	앱이 이미 설치되어 있는 경우 MDM이 앱을 인수하여 관리합니다.
MDM 프로필이 제거되면 앱 제거	기기 관리 제거의 경우 앱이 제거됩니다.
앱 데이터 백업 방지	앱별 데이터의 백업은 생성되지 않습니다.
앱 설정	'앱 설정'에서 앱에 특정 값을 포그라운드로 지정할 수 있습니다(앱이 지원하는 한, 필요한 경우 앱 개발자에게 문의하세요).

'사내 앱 업로드'를 통해 IPA 파일을 직접 선택하여 업로드할 수도 있습니다.



웹 앱



'웹 앱'에서는 '웹 클립'과 마찬가지로 웹 관리 영역에서 인터넷 페이지 또는 인트라넷 포털을 애플리케이션으로 최종 사용자 장치에 푸시할 수 있습니다. 기본적으로 웹 앱은 전체 화면 모드로 표시되며, 이는 웹 클립에서 구성할 수 있습니다.

라벨	최종 사용자 디바이스의 연결 이름
URL	각 웹사이트로 연결되는 링크
이동식	활성화된 경우 사용자는 웹클립을 제거할 수 있습니다.
아이콘	이 대화 상자에서 연결에 사용할 로고를 업로드합니다: 크기 180x180, png 형식
미리 구성된 아이콘	활성화하면 아이콘에 추가 효과(그림자, 반사)가 표시되지 않습니다.

제한 및 설정

블랙리스트/화이트 리스트 앱

여기에서 '일반 설정'의 설정에 따라 차단(또는 허용) 앱을 설정할 수 있습니다. 클릭하면 알려진 앱 검색이 나타납니다. 여기에서 추가하려는 앱을 검색할 수 있습니다.

이 기능을 사용하려면 감독 장치가 필요합니다.

SysApp 제한 사항

기기의 특정 앱 또는 기능 차단

YouTube 사용 허용	YouTube 사용 허용
iTunes Store 사용 허용	iTunes Store 사용 허용
Safari 사용 허용	Safari 사용 허용
자동 완성 사용	자동 완성 허용
강제 사기 경고	사기 경고 강제 적용
자바스크립트 사용	자바스크립트 사용 활성화
팝업 차단	모든 종류의 팝업 차단
쿠키 허용	Safari가 쿠키를 허용할 때 선택

앱-VPN

기호를 통해 시작 시 선택한 VPN 연결을 자동으로 실행하는 애플리케이션을 정의할 수 있습니다.

앱 설정

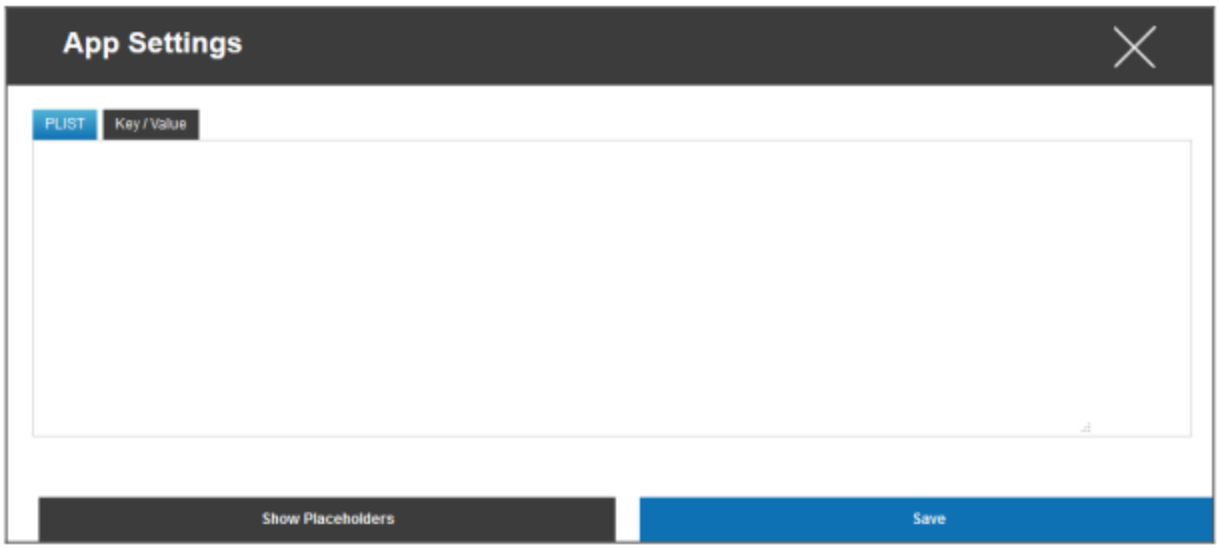
'앱 설정'에서 앱에 특정 값을 포그라운드로 지정할 수 있습니다(앱이 지원하는 한, 필요한 경우 앱 개발자에게 문의하세요).

기호를 통해 (추가) 앱을 추가합니다. 다시 한 번 익숙한 AppTec360의 앱 가져오기 표현을 찾을 수 있습니다.

여기에서 구성하려는 앱을 검색하여 선택합니다. 설정은 관리되는 앱에만 적용됩니다.

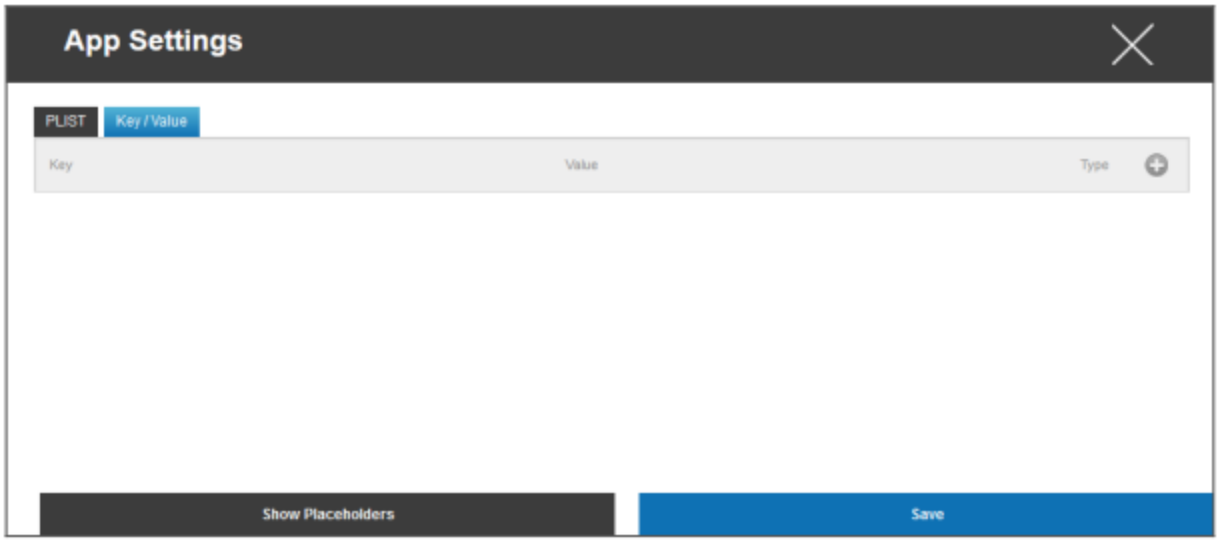
가져오기에 성공했다면 다음과 같은 화면이 표시됩니다:

이제 클릭 한 번으로 다양한 구성을 수행할 수 있습니다. 그러면 다음과 같은 개요가 표시됩니다:

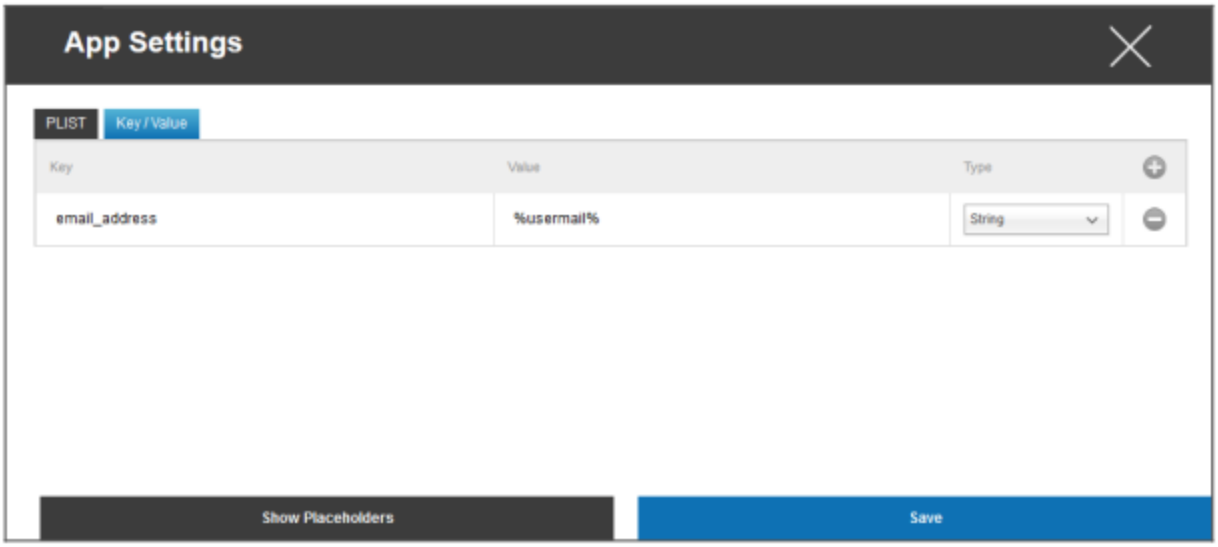


이미 PLIST(구성의 소스 텍스트)가 있는 경우 여기에 추가하고 '저장'으로 모두 저장할 수 있습니다.

"키/값"에서 앱에 특정 구성을 첨부할 수 있습니다.



여기에서 기호를 사용하여 새 키와 해당 값을 설정할 수 있습니다.



물론 앱텍의 모든 플레이스홀더를 자유롭게 사용할 수 있습니다.

"유형" 설명:

문자열	텍스트
부울	참/거짓
번호	번호

기호를 사용하여 앱을 다시 제거할 수 있습니다.

엔터프라이즈 앱 스토어

iTunes 앱

이 시점에서 사용자를 위한 선택적 앱을 배포할 수 있습니다.

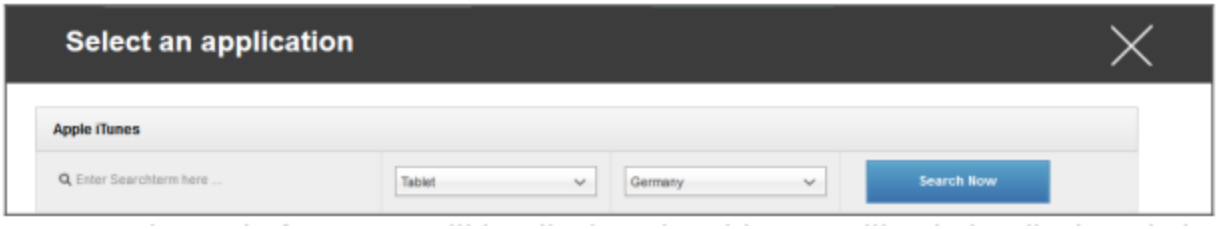
여기에 앱이 있으면 앱텍360 스토어의 최종 사용자 디바이스에 자동으로 설치됩니다.

이는 공식 Apple 앱 스토어로 연결되는 링크일 뿐입니다. 따라서 각 최종 사용자 디바이스에는 Apple ID가 있어야 합니다.

이 시점에서는 각 사용자에게 고유한 Apple ID를 사용하는 것이 좋습니다.

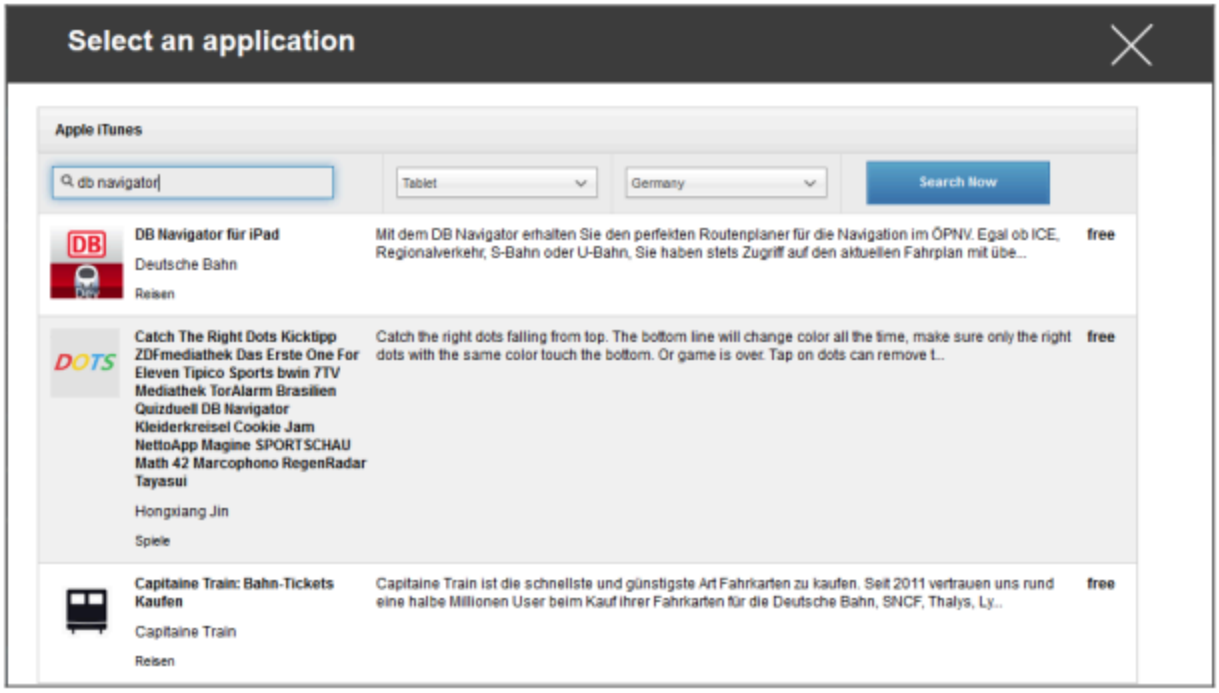
기호를 사용하여 앱을 추가할 수 있습니다.

그 후 다음과 같은 개요가 표시된 창이 열립니다.



무료 앱만 표시되며 유료 앱은 VPN을 통해서만 표시된다는 점에 유의하세요.

"여기에 검색어 입력 ..."에서 Apple 앱스토어에 있는 앱을 검색할 수 있습니다.



아이콘 또는 앱 이름을 클릭하면 추가 구성을 수행하라는 메시지가 다시 표시됩니다.

최신 정보 확인	일주일에 한 번 앱에 대한 업데이트가 있는지 확인합니다. 그렇다면 이 업데이트가 설치됩니다.
MDM 프로필이 제거되면 앱 제거	기기 관리 제거의 경우 앱이 제거됩니다.
앱 데이터 백업 방지	앱별 데이터의 백업은 생성되지 않습니다.
앱-VPN	앱을 열면 실행되는 VPN 연결을 선택합니다.

"설치"를 클릭하면 앱이 엔터프라이즈 앱 스토어에 추가되고 AppTec360 앱스토어를 통해 최종 사용자 디바이스에 설치할 수 있습니다.

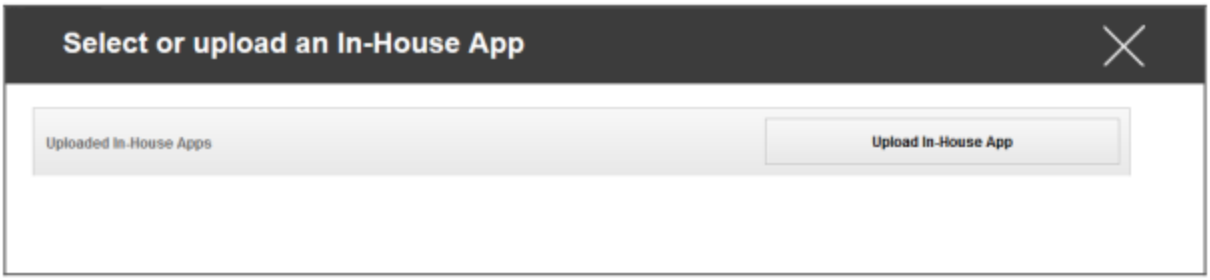
앱 스토어 가져오기가 성공적으로 완료되면 다음과 같은 개요가 표시됩니다:

사내

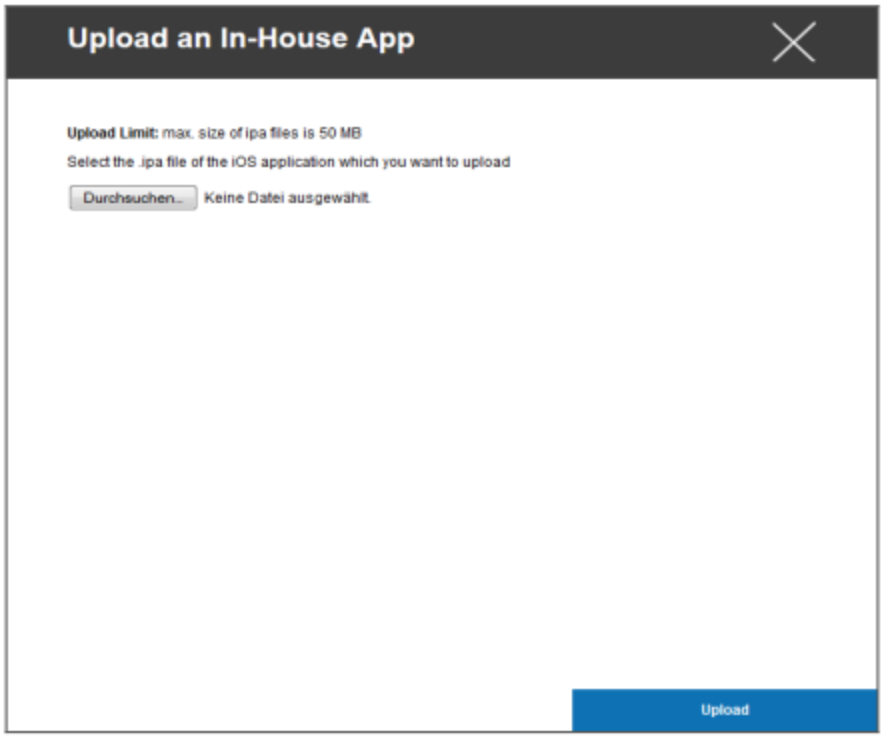
'사내' 항목에서는 내부에서 개발한 앱을 업로드하고 배포할 수 있습니다.

이 기호를 사용하면 사내 앱을 추가로 배포할 수 있습니다.

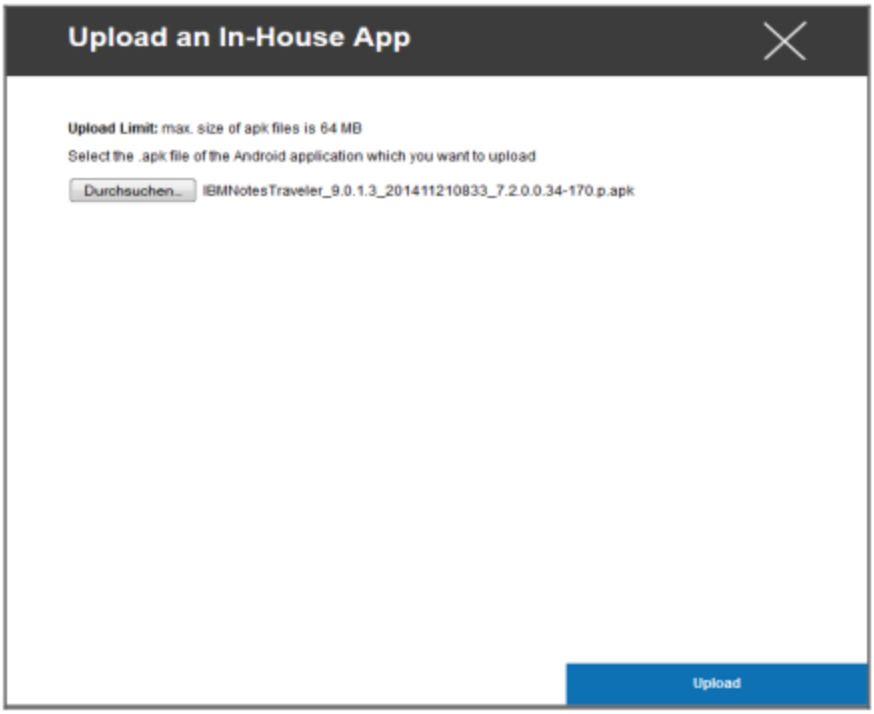
사내 앱을 배포한 적이 없는 경우 다음과 같은 개요를 받게 됩니다:



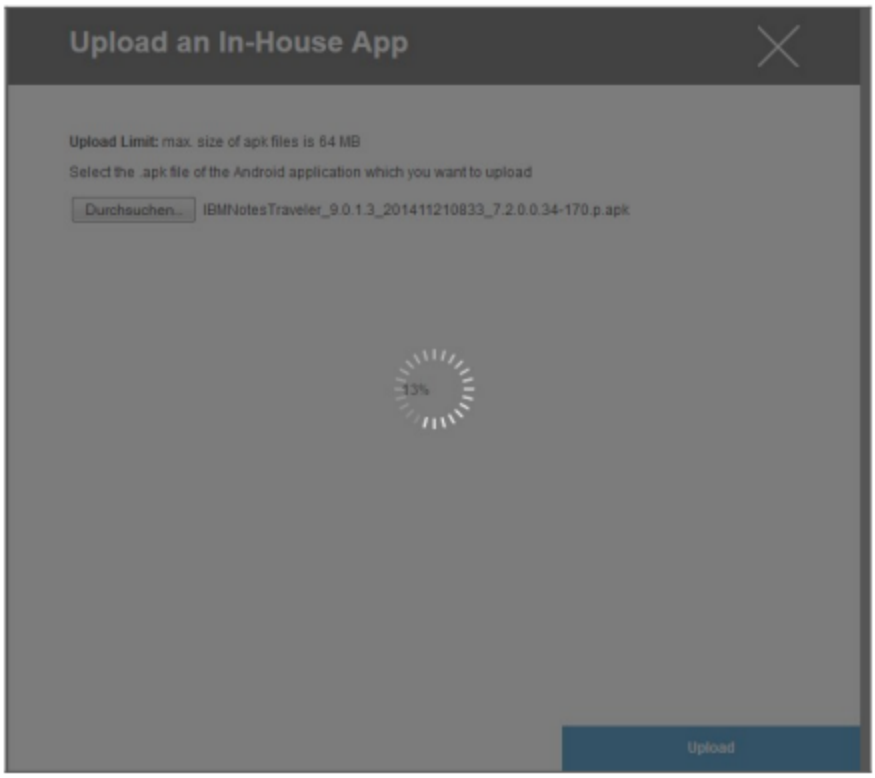
이를 위해 '사내 앱 업로드'를 클릭하면 다음과 같은 개요가 표시됩니다:



이제 "검색..."으로 .ipa 파일을 선택한 다음 "업로드"를 클릭합니다.



이제 앱이 업로드됩니다. 원 가운데에서 앱이 이미 업로드된 비율을 확인할 수 있습니다.



사내 앱 업로드가 성공적으로 완료되면 앱 카탈로그에 새로 업로드된 앱이 표시됩니다.

이제 사용자는 최종 사용자 디바이스의 AppTec360 스토어에서 '사내' 카테고리 아래에서 이 앱을 확인하고 설치할 수 있습니다.

여기에는 공개 Apple 앱스토어 앱이 포함되지 않기 때문에 최종 사용자 디바이스에 저장된 Apple ID가 필요하지 않습니다.

키오스크 모드

iOS 키오스크 모드는 감독 모드에서만 사용할 수 있습니다.

키오스크 모드에서는 앱 또는 URL을 미리 정의하여 이 앱/URL만 실행/방문할 수 있도록 할 수 있습니다.

또한 키오스크 모드에서 다양한 하드웨어 버튼을 비활성화할 수 있습니다.

애플리케이션 유형

패키지

키오스크 모드에서 앱을 실행하려면 '애플리케이션 유형' 아래에서 '패키지'를 선택합니다.

키오스크 애플리케이션	키오스크 모드에서 실행해야 하는 앱을 선택하려면 여기를 클릭하세요. 앱 관리의 현재 개요를 확인할 수 있습니다. "Apple iTunes 앱"과 "iOS 인하우스 앱" 중에서 선택할 수 있습니다.

URL

키오스크 모드에서 URL을 실행하려면 '애플리케이션 유형' 아래에서 'URL'을 선택합니다.

URL	이제 원하는 URL 주소를 정의합니다.
동일 출처 정책	이 기능이 활성화되면 사용자는 미리 정의된 URL의 하위 페이지만 서핑할 수 있습니다. 예를 들어 다음 URL을 정의한 경우입니다: www.mypage.com, 사용자는 www.mypage.com/subpage
화이트리스트 URL	여기에서 화이트리스트를 관리할 수 있으며, 다음과 같은 모든 URL이 허용됩니다. 한 줄당 최대 1개의 URL URL은 http:/ 또는 https://로 시작해야 합니다.
블랙리스트 URL	여기에서 블랙리스트를 관리할 수 있으며, 다음 URL은 모두 허용되지 않습니다. 한 줄당 최대 1개의 URL URL은 http:/ 또는 https://로 시작해야 합니다.
비활성 후 브라우저 지우기	비활성 상태가 되면 브라우저 캐시가 비워집니다.
종료 암호 사용	이 기능을 활성화하면 사용자는 미리 정의한 비밀번호를 사용하여 키오스크 모드를 종료할 수 있습니다.
종료 비밀번호	사용자가 미리 정의한 비밀번호입니다.

키오스크 모드 설정

예약된 키오스크 모드	하루 중 시간을 기준으로 키오스크 모드를 설정하여 미리 정해진 시간에 자동으로 모드가 시작되고 종료되도록 할 수 있습니다.
시작 시간	시작 시간
시간(분)	키오스크 모드가 다시 종료되어야 하는 시간(분)
터치 사용 안 함	활성화하면 터치스크린이 비활성화됩니다.
장치 회전 비활성화	활성화하면 자동 화면 조정이 비활성화됩니다.
벨소리 스위치 비활성화	활성화하면 벨소리 스위치가 비활성화됩니다. 그 이후부터는 이전에 설정한 기능에 따라 동작이 달라집니다.
볼륨 버튼 비활성화	활성화하면 볼륨 버튼이 비활성화됩니다.
절전 모드 깨우기 버튼 비활성화	활성화하면 켜기/끄기 스위치가 비활성화됩니다.
자동 잠금 비활성화	활성화하면 장치가 대기 모드로 전환되지 않습니다.
음성 해설 사용	활성화하면 보이스오버 어시스턴트가 활성화됩니다.
줌 사용	활성화하면 줌이 활성화됩니다.
색상 반전 사용	활성화하면 반전 표시 모드가 활성화됩니다.
보조 터치 활성화	활성화하면 어시스턴티브 터치가 활성화됩니다.
말하기 선택 활성화	활성화하면 말하기 선택 항목이 활성화됩니다.
모노 오디오 활성화	활성화하면 모노 오디오가 활성화됩니다.
보이스오버	활성화된 경우 사용자는 보이스오버를 활성화할 수 있습니다.
Zoom	활성화된 경우 사용자는 Zoom을 활성화할 수 있습니다.
색상 반전	활성화하면 사용자가 반전된 색상을 활성화할 수 있습니다.
보조 터치	활성화하면 사용자가 보조 터치를 활성화할 수 있습니다.

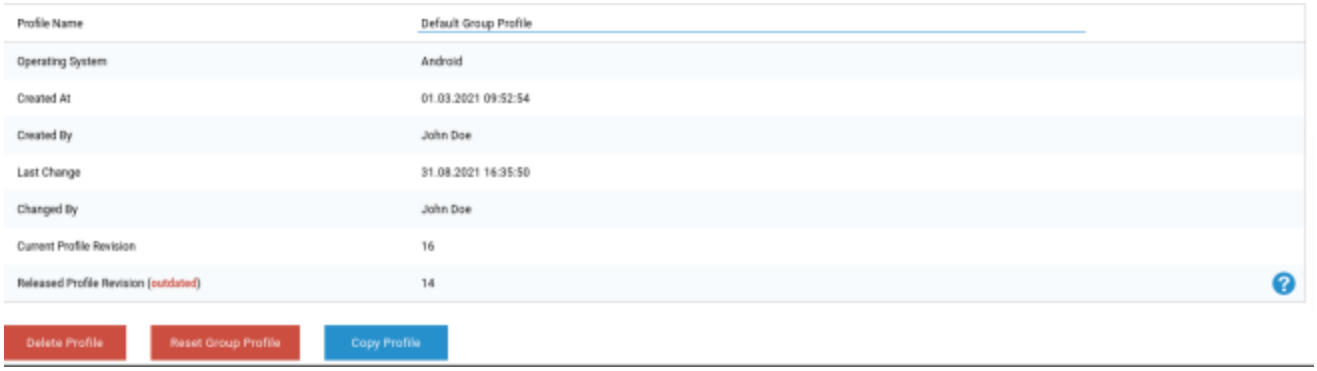
안드로이드 엔터프라이즈 – 완전 관리형 디바이스 구성

현재 그룹 프로필을 선택했는지 또는 디바이스를 선택했는지에 따라 개요와 하위 요점이 달라지므로 이를 신중하게 고려해 주세요!

일반

그룹 프로필 개요(그룹 수준에서만)

그룹 프로필을 열면 프로필에 대한 간략한 개요를 볼 수 있습니다.



프로필 이름	프로필 이름(여기에서 변경 가능)
운영 체제	프로필의 운영 체제
만든 곳	생성 시간
만든 사람	프로필 작성자
마지막 변경 사항	프로필을 마지막으로 변경한 시간
변경자	마지막으로 변경한 계정
현재 프로필 수정	저장된 프로필 상태 수정
프로필 수정 버전 출시	할당된 프로필 수정본('지금 할당'). 텍스트 뒤에 '(오래된)'이라는 레이블이 표시되면 프로필을 저장했지만 아직 할당하지 않았으므로 디바이스는 여전히 이전 버전을 받게 됩니다.

장치 개요(장치 수준에서만)

디바이스를 사용하는 경우 선택한 디바이스에 대한 개요 요약이 표시되며, 여기에는 다음과 같은 내용이 포함되어 있습니다:

장치 이름	장치 이름
위치	위치 좌표
전화번호	전화번호
필수 앱 지정	할당된 필수 앱 수
OS 버전	디바이스의 OS 버전
운영 체제	운영 체제(Android Enterprise)
일련 번호	장치 일련 번호
디바이스 소유권	기업 또는 개인 디바이스
디바이스 유형	AE 업무용 관리 디바이스
루팅	상태, 기기가 루팅되었는지 여부를 나타냅니다.
규정 준수	가이드라인 준수
IP 주소	디바이스의 IP 주소
마지막으로 본	기기가 AppTec에 마지막으로 연결한 시점
마지막 푸시	마지막 푸시가 디바이스로 전송된 시점, 특정 시점
AE 장치 소유자 모드	예
사용자 할당	이 장치가 할당된 사용자 또는 그룹

구성 수정(디바이스 수준에서만)

여기에서 장치에 어떤 그룹 프로필이 할당되었는지에 대한 개요를 볼 수 있습니다.

그룹 프로필을 클릭하면 이 프로필에 직접 액세스할 수 있으며 설정을 수행할 수 있습니다.

이 기호를 사용하면 배포된 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

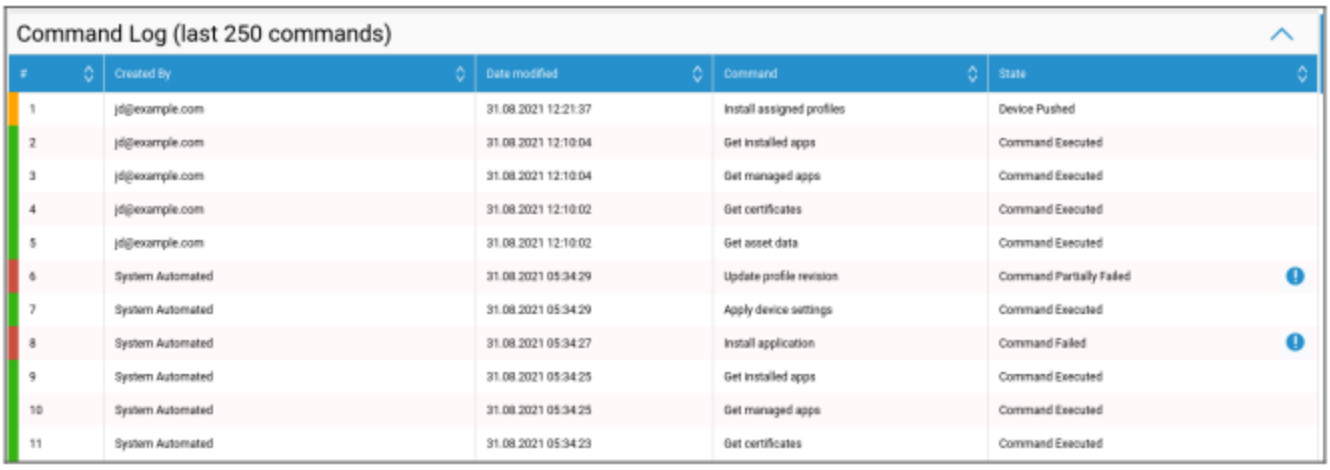
이 기호를 사용하면 사용한 모든 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

"최신 수정본 사용 가능"은 그룹 프로필이 변경되어 저장되었지만 할당되지 않았음을 나타냅니다. 변경 사항을 디바이스에 적용하려면 그룹 수준에서 '지금 할당'을 사용하여 그룹 프로필을 할당해야 합니다.

디바이스 로그(디바이스 수준에서만)

명령 로그

여기에서 디바이스에 대해 어떤 명령이 실행되었는지, 어떤 상태인지 확인할 수 있습니다.



'시스템 자동화'에 의해 생성된 명령은 시스템에 의해 자동으로 생성됩니다.

가능한 명령 상태

푸시된 장치	푸시 요청이 푸시 서비스(예: APNS)로 전송되어 디바이스가 EMM 서버에 다시 연결하도록 지시합니다.
명령 생성	이 명령은 시스템에서 생성되었습니다.
명령 전송	명령은 서버에 연결한 후 디바이스로 전송되었습니다.
명령 실행	명령이 성공적으로 실행되었습니다.
명령 실패	명령이 실패했습니다. *
명령이 부분적으로 실패했습니다.	디바이스 OS에 따라 일부 명령이 함께 그룹화될 수 있습니다. 이 경우 이 명령 그룹의 일부가 실패했습니다. *
명령 실행, 결국 실패	명령이 실행되었지만 실행되지 않았을 수도 있습니다.
명령 재푸시	명령이 사용자에 의해 다시 푸시되었습니다.
폐기됨	명령이 삭제되었습니다. 예를 들어 다른 명령으로 대체되었거나 디바이스가 다시 등록되어 이전 명령이 제거되었기 때문입니다.

메시지 뒤에 느낌표가 있는 경우 커서로 아이콘 위에 마우스를 가져가면 자세한 정보를 확인할 수 있습니다.

디바이스 설정

클라이언트 구성

여기에서 Android 디바이스에서 다음 구성을 수행할 수 있습니다:

규정 준수 시간 초과	강제 조치가 적용되는 사용자 응답 시간 제한입니다.
규정 준수 시간 초과 후 시행 조치	사용자가 규정 준수 장치 상태로 이어지는 작업을 수행하지 않을 경우 강제 조치
데이터 수집 빈도	기기/GPS 정보 수집 빈도
장치 하트비트 주파수	장치가 AppTec360 서버에 연결해야 하는 간격 Min. 1분 최대. 24시간
위치 업데이트 사용	활성화된 경우, 장치는 AppTec360 서버로 위치 업데이트를 보냅니다.
위치 업데이트 시간	장치가 AppTec360에 위치 업데이트를 전송하는 시간 간격을 결정합니다.
위치 업데이트에 Google 위치 정확도 사용	활성화하면 네트워크 위치가 위치 업데이트에 사용됩니다('제한'에서 비활성화한 경우 이 설정은 아무 영향도 미치지 않습니다).
위치 업데이트를 위해 GPS 위치 사용	활성화하면 GPS가 위치 업데이트에 사용됩니다.
모의 (가짜) 위치 허용	타사 앱을 통한 위치 정보 위조 허용
연결 끊김 조치	이 옵션을 활성화하면 장치가 하트비트 간격으로 MDM 서버에 연결되지 않는 경우에 대한 동작을 지정할 수 있습니다. 예를 들어 디바이스의 하트비트 시간이 5분인 경우 오전 10시 35분에 서버에 연결됩니다. 그 후에는 디바이스가 Wi-Fi 범위를 벗어납니다. 오전 10시 40분에 다음 하트비트가 실패하고 지정된 작업이 실행됩니다.
액션	디바이스가 규정을 준수하지 않게 되는 즉시 취해야 할 조치입니다.

	• 장치 잠금 = 장치 잠금 • 장치 초기화 = 장치가 공장 설정으로 복원됩니다. • 장치 및 SD 카드 초기화 = 장치가 공장 설정으로 복원되고 SD 카드 저장소가 삭제됩니다.
임계값	지정된 작업을 트리거하는 데 필요한 실패한 하트비트 임계값을 지정할 수 있습니다.

정책 적용 모드	기본값입니다:	사용자에게 미결 작업을 실행하라는 메시지가 주기적으로 표시됩니다.
	게으른 정책 시행:	사용자에게 미결 작업을 실행하라는 메시지가 표시되지 않습니다. 열려 있는 모든 작업은 AppTec360 클라이언트에 표시됩니다.
	적극적인 정책 집행:	사용자에게 미결 작업을 실행하라는 메시지가 계속 표시됩니다.
AppTec360 버전 잠금	이 옵션을 활성화하면 AppTec360 MDM 클라이언트의 버전 코드를 지정할 수 있습니다. AppTec360 클라이언트는 지정된 버전으로만 업데이트됩니다. 최신 버전은 무시됩니다. 다운그레이드는 불가능합니다.	
버전 코드	잠글 AppTec360 MDM 클라이언트의 버전 코드입니다.	
AppTec360 알림 비활성화	비활성화하면 AppTec360 클라이언트는 알림 표시줄에 알림을 표시하지 않습니다. 따라서 사용자는 작업 관리자를 통해 AppTec360 클라이언트를 닫을 수 있습니다. AppTec360 클라이언트가 닫히면 키오스크 모드 및 앱 블랙/화이트 리스트 등 일부 기능이 제대로 작동하지 않습니다. 삼성 기기는 AppTec360 클라이언트를 위한 보호 메커니즘을 제공합니다. KNOX API를 지원하는 삼성 디바이스에서는 기본적으로 알림이 비활성화되어 있습니다. Android 8.0 이상의 디바이스에서는 알림이 비활성화되지 않아야 합니다.	

배경 화면

사용자 지정 배경 화면 설정	사용자 지정 배경화면 활성화/비활성화
배경 화면	컬러 코드 또는 이미지를 사용하도록 배경화면 모드를 설정합니다.
색상 지정	백고라운드 색상을 16진수 값으로 지정합니다(예: 검정색은 #000000, 흰색은 #ffffff).
이미지를 배경화면으로 설정	배경화면으로 사용할 이미지 파일을 업로드합니다.

자산 관리(디바이스 수준에서만)

장치 정보

모델	디바이스 모델 지정
운영 체제	OS
OS 버전	OS 버전
일련 번호	일련 번호
장치 이름	장치 이름
배터리 상태	배터리 상태
여유 / 총 메모리	여유 / 총 메모리
삼성 금고	다양한 설정 옵션에 필요한 삼성 SAFE 인터페이스
SD 카드 사용 가능	SD 카드 사용 가능
SD 카드 에뮬레이션	SD 카드 에뮬레이션
SD 카드 이동식	SD 카드 탈착식
SD 여유 / 총 메모리	SD 무료 / 총 SD 카드 메모리

Wi-Fi

IP 주소	디바이스 IP 주소
WiFi MAC	WiFi MAC 주소

셀룰러

상태	상태(SIM 카드 설치)
전화번호	전화번호
로밍(음성/데이터)	음성/데이터 로밍
로밍 상태	현재 로밍 상태
IP 주소	IP 주소
사업자/이동 통신사	사업자/이동 통신사
셀룰러 기술	셀룰러 기술
IMEI	IMEI 번호
ICCID	SIM 카드의 ID이며, 종종 스마트카드 또는 집적 회로 카드(ICC)이기도 합니다.
IMSI	국제 모바일 가입자 신원(IMSI)은 GSM 및 UMTS 모바일 네트워크에서 네트워크 사용자를 명확하게 식별하는 기능을 제공합니다. IMSI는 최대 15자리로 구성되며 다음과 같은 방식으로 구성됩니다: • 모바일 국가 코드 (MCC), 3자리 • 모바일 네트워크 코드 (MNC), 2자리 또는 3자리 • 모바일 가입자 식별 번호(MSIN), 1~10자리
현재 MCC/MNC	"SIM MCC/MNC" 참조
SIM MCC/MNC	모바일 국가 코드는 ITU에서 E.212 표준에 따라 설정한 국가 식별자입니다. 이는 모바일 네트워크 식별을 위해 모바일 네트워크 코드(MNC)와 함께 작동합니다. SIM 카드의 국가/모바일 네트워크 코드를 의미합니다. 다른 모바일 네트워크로 로밍하는 경우 논리적으로 '현재 MCC/MNC'와 'SIM MCC/MNC'가 달라집니다.

블루투스

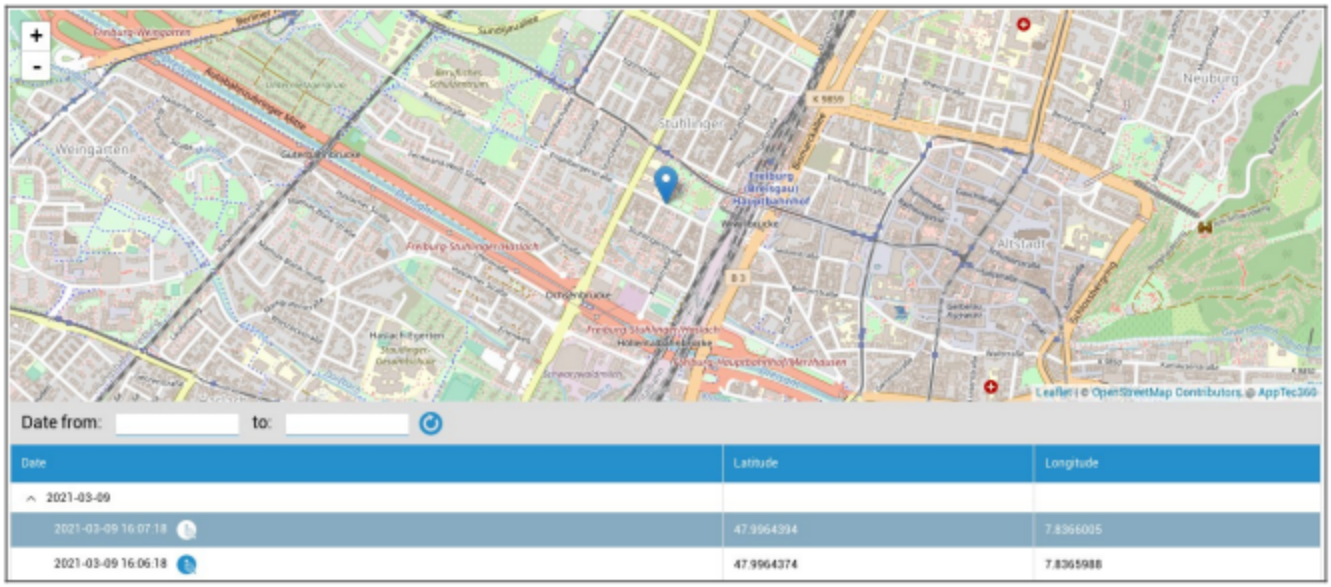
블루투스 MAC	블루투스 MAC 주소

보안 관리

도난 방지(디바이스 수준에서만)

GPS 정보(디바이스 수준에서만)

여기에서 현재/마지막 장치 위치를 설정할 수 있습니다. 현지화는 하나 또는 두 개의 비밀번호로 보호할 수 있습니다(참조: 일반 설정 - 개인정보 - GPS 액세스



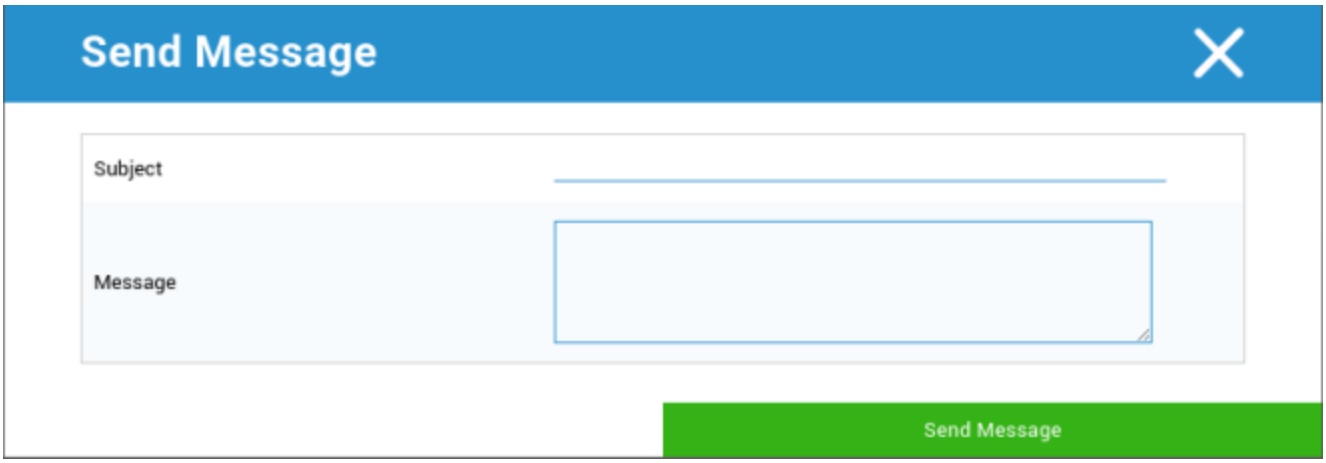
지우기 및 잠금(기기 수준에서만)

'삭제 및 잠금'에서 다음 세 가지 작업을 수행할 수 있습니다:

전체 삭제	장치가 공장 설정으로 복원됩니다(회사 및 개인 데이터가 삭제됨).
엔터프라이즈 삭제	최종 사용자 기기에서 기업 데이터만 제거됩니다(AppTec360에서 제공한 모든 앱, 데이터 등).
잠금 화면	화면 잠금이 활성화되어 있으면 기기 비밀번호/PIN으로 기기 잠금을 해제하는 것으로 충분합니다.

메시지(디바이스 수준에서만)

여기에서 제목과 메시지를 입력하고 최종 사용자 디바이스로 보낼 수 있습니다.



보안 구성

장치 암호

'비밀번호'에서 디바이스 비밀번호를 지정할 수 있으며, 다음과 같은 설정 옵션을 사용할 수 있습니다.

최소 비밀번호 길이	비밀번호에 포함되어야 하는 최소 기호 수를 설정합니다.	
비밀번호 품질	지정되지 않음	이 정책에는 비밀번호에 대한 요구 사항이 없습니다.
	생체 인식 약	이 정책은 보안 수준이 낮은 생체 인식 기술을 허용합니다. 이는 개인의 신원을 3자리 비밀번호 정도로 인식할 수 있는 기술을 의미합니다(오탐지 확률은 1,000분의 1 미만).
	무언가	이 정책은 일종의 비밀번호나 패턴을 설정하도록 요구하지만 특정 규칙을 강제하지는 않습니다.
	알파벳	사용자는 알파벳(또는 기타 기호) 이상의 문자가 포함된 비밀번호를 입력해야 합니다.
	영숫자	사용자는 숫자와 알파벳(또는 기타 기호) 문자를 모두 포함한 비밀번호를 입력해야 합니다.
	복잡한	사용자는 기본적으로 문자, 숫자 및 특수 기호가 포함된 비밀번호를 입력해야 합니다. 이 비밀번호 품질을 사용하면 최소 대문자 등 다양한 문자 집합을 포함하도록 비밀번호를 제한할 수 있습니다.
최소 비밀번호 길이	비밀번호에 필요한 글자 수를 설정합니다. 예를 들어 PIN 또는 비밀번호는 6자 이상으로 설정할 수 있습니다.	
비밀번호에 필요한 최소 숫자 자릿수	비밀번호에 필요한 최소 숫자 자릿수	
비밀번호에 필요한 최소 소문자	비밀번호에 필요한 최소 소문자	
비밀번호에 필요한 최소 대문자	비밀번호에 필요한 최소 대문자	
비밀번호에 필요한 최소 문자 이외의 문자	비밀번호에 필요한 최소 문자 이외의 문자	

비밀번호에 필요한 최소 기호	비밀번호에 필요한 최소 기호

최대 비활성 시간 잠금	시간 잠금까지 최대 사용자 비활성 상태
비밀번호 만료 시간 초과	비밀번호가 만료되고 새 비밀번호를 발급해야 하는 시간 간격을 설정합니다.
비밀번호 기록 제한	허용되지 않는 이전에 사용한 비밀번호의 개수
최대 실패한 비밀번호 시도 횟수	전체 장치 초기화가 수행되기 전에 비밀번호를 잘못 입력할 수 있는 빈도를 설정합니다.
생체 인증 허용	지문 또는 홍채 스캔을 통해 인증할 수 있습니다. 삼성 KNOX 2.1 이상에서만 사용 가능

안티바이러스

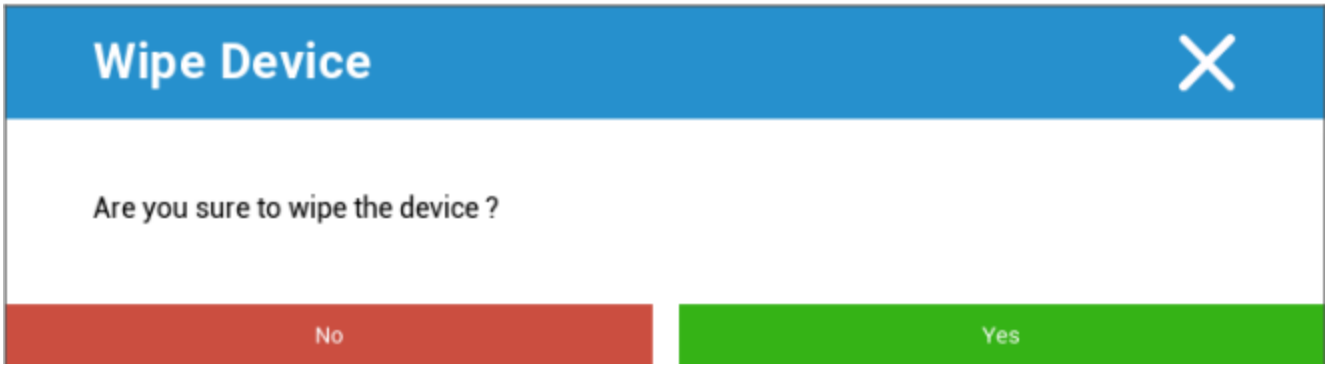
자동 스캔	주기적인 자동 스캔 사용
스캔 간격	검사 간격(빠른/전체)
완전 자동 스캔	완전 자동 스캔 사용
자동 업데이트	자동 업데이트 사용
업데이트 확인 간격	앱 및 데이터베이스의 업데이트 주기(바이러스/손상된 코드)
앱 보호	자동 앱 스캔 사용
SD 카드 보호	SD 카드 자동 스캔 활성화
Wi-Fi 전용 업데이트	이 기능을 활성화하면 장치가 Wi-Fi 네트워크에 성공적으로 연결된 경우에만 업데이트가 적용됩니다.

수명 종료(디바이스 수준에서만)

지우기(디바이스 수준에서만)

'초기화'에서 장치를 공장 설정으로 복원할 수 있습니다. 여기에서는 회사 데이터와 개인 데이터가 최종 사용자 장치에서 삭제됩니다.

'빼기 기호'를 클릭하면 다음과 같은 메시지가 표시됩니다:



"예"를 선택하면 지우기를 수행할 수 있습니다.

"삭제 보고서" 아래에 다음 항목이 표시될 수 있습니다.

지운 사람	삭제한 사람에 대한 기록
날짜	날짜
상태	상태(예: 초기화가 성공적으로 수행된 경우)

제한 설정

제한 사항

여기에서 다양한 항목을 제한하고 차단할 수 있습니다.

카메라 사용	카메라 사용 허용	
강제 자동 동기화	켜짐	동기화가 영구적으로 활성화됩니다.
	꺼짐	동기화가 영구적으로 비활성화됩니다.
	사용자 선택	사용자가 선택한 항목
강제 블루투스	켜짐	블루투스가 영구적으로 활성화됨
	꺼짐	블루투스가 영구적으로 비활성화됨
	사용자 선택	사용자가 선택한 항목
강제 GPS	켜짐	GPS가 영구적으로 활성화됨
	꺼짐	GPS가 영구적으로 비활성화됨
	사용자 선택	사용자가 선택한 항목
강제 네트워크 위치	켜짐	영구적인 인터넷 현지화
	꺼짐	인터넷 로캘라이제이션 영구 비활성화
	사용자 선택	사용자가 선택한 항목

보안		
공유 위치 허용 안 함	사용자가 위치 공유를 켤 수 없도록 허용할지 여부를 지정합니다.	
안전 부팅 허용 안 함	사용자가 장치를 안전 부팅 모드로 재부팅할 수 없도록 허용할지 여부를 지정합니다.	
네트워크 재설정 허용 안 함	사용자가 설정에서 네트워크 설정을 재설정할 수 없도록 허용할지 여부를 지정합니다.	
공장 초기화 허용 안 함	사용자가 디바이스를 재설정할 수 없도록 허용할지 여부를 지정합니다.	
ADB 사용	ADB를 통해 PC에 연결할 수 있습니다.	
키가드 비활성화	키가드 비활성화	
기기 소유자 잠금 화면 정보	잠금 화면에 표시할 기기 소유자 정보를 설정합니다.	
규정 준수 시행	모드 프롬프트 사용자	사용자에게 필요한 조치를 이행하라는 메시지가 표시됩니다.
	모드 잠금 컨테이너	모든 요구 사항이 충족될 때까지 모든 앱 숨기기

앱 관리	
교차 프로필 앱 연결 허용	상위 프로필의 앱이 관리 프로필의 웹 링크를 처리할 수 있도록 허용합니다.
앱 제어 허용 안 함	사용자가 설정 또는 런처에서 애플리케이션을 수정할 수 없도록 허용할지 여부를 지정합니다.
앱 설치 허용 안 함	사용자가 애플리케이션을 설치할 수 없도록 허용할지 여부를 지정합니다.
앱 제거 허용	사용자가 애플리케이션을 제거할 수 없도록 허용할지 여부를 지정합니다.
런타임 권한 정책	앱의 새 권한 요청을 처리하는 방법을 지정합니다.
알 수 없는 소스 허용	활성화하면 사용자는 .apk 파일을 설치하여 앱을 사이드로드할 수 있습니다.

연결성	
모바일 네트워크 구성 허용 안 함	사용자가 모바일 네트워크를 구성할 수 없도록 허용할지 여부를 지정합니다.
테더링 구성 허용 안 함	사용자가 테더링 및 휴대용 핫스팟을 구성할 수 없도록 허용할지 여부를 지정합니다.
VPN 구성 허용 안 함	사용자가 VPN을 구성할 수 없도록 허용할지 여부를 지정합니다.
Wi-Fi 구성 허용 안 함	사용자가 WiFi 액세스 포인트를 변경할 수 없도록 허용할지 여부를 지정합니다.
발신 NFC 빔 허용	사용자가 NFC를 사용하여 앱에서 데이터를 빔으로 전송할 수 없도록 허용할지 여부를 지정합니다.
WiFi 구성 잠금	이 설정은 장치 소유자 앱에서 만든 WiFi 구성을 잠글지 여부(즉, 설정 앱이 아닌 장치 소유자 앱에서만 편집하거나 제거할 수 있도록 할지 여부)를 제어합니다.
데이터 로밍 활성화	데이터 로밍 활성화

블루투스	
블루투스 허용 안 함	장치에서 블루투스를 허용하지 않을지 여부를 지정합니다. Android 8.0이 필요합니다.
블루투스 공유 허용	장치에서 발신 블루투스 공유를 허용할지 여부를 지정합니다. Android 8.0 필요
블루투스 구성 허용 안 함	사용자가 블루투스를 구성할 수 없도록 허용할지 여부를 지정합니다.

계정 관리	
관리되는 프로필 추가 허용 안 함	사용자가 관리되는 프로필을 추가할 수 없도록 허용할지 여부를 지정합니다. Android 8.0 필요
사용자 추가 허용 안 함	사용자가 새 사용자를 추가할 수 없도록 허용할지 여부를 지정합니다.
관리되는 프로필 제거 허용 안 함	프로필 소유자가 아닌 다른 사람이 이 사용자의 관리되는 프로필을 제거할 수 있는지 여부를 지정합니다. Android 8.0 필요
계정 수정 허용	인증자가 프로그래밍 방식으로 추가하지 않는 한 사용자가 계정을 추가 및 제거할 수 없도록 허용할지 여부를 지정합니다.

전화 통신	
발신 전화 허용	사용자가 발신 전화를 걸 수 없도록 지정합니다.
SMS 허용 안 함	사용자가 SMS 메시지를 보내거나 받을 수 없도록 지정합니다.

시스템	
창 생성 허용 안 함	앱 창 이외의 창을 만들지 않도록 지정합니다.
사용자 아이콘 설정 허용 안 함	사용자가 자신의 아이콘을 변경할 수 없도록 허용할지 여부를 지정합니다.
배경화면 설정 허용 안 함	배경화면 설정을 허용하지 않도록 사용자를 제한합니다.
상태 표시줄 비활성화	상태 표시줄을 비활성화하면 알림, 빠른 설정 및 기타 화면 오버레이를 차단하여 일회용 장치에서 벗어날 수 있습니다.
자동 시간 사용	시간을 자동으로 설정합니다.
자동 시간대 사용	표준 시간대를 자동으로 설정합니다.
전원이 연결된 상태에서 계속 켜두기	기기는 전원에 연결되어 있는 동안 활성 상태로 유지됩니다.

스토리지	
앱 인증 비활성화	사용자가 애플리케이션 확인을 비활성화할 수 없도록 허용할지 여부를 지정합니다.
물리적 미디어 마운트 허용	사용자가 물리적 외부 미디어를 마운트할 수 없도록 허용할지 여부를 지정합니다.
백업 서비스 사용	백업 서비스는 디바이스의 모든 백업 및 복원 메커니즘을 관리합니다. 이 옵션을 false로 설정하면 데이터가 백업 또는 복원되지 않습니다. 백업 서비스는 기본적으로 꺼져 있습니다. Android 8.0 필요
USB 대용량 저장소 사용	USB 대용량 저장소 사용을 활성화합니다.

키보드	
자동 완성 허용 안 함	사용자가 자동 완성 서비스를 사용할 수 없도록 허용할지 여부를 지정합니다. Android 8.0 필요
프로필 간 복사 및 붙여넣기 허용	이 프로필의 클립보드에 복사된 내용을 관련 프로필에 붙여넣을 수 있는지 여부를 지정합니다.

사운드	
볼륨 조정 허용 안 함	사용자가 마스터 볼륨을 조정할 수 없도록 허용할지 여부를 지정합니다.
마이크 음소거 해제 허용	사용자가 마이크 볼륨을 조정할 수 없도록 허용할지 여부를 지정합니다.
장치 음소거	디바이스 음소거.

인증서 관리

여기에서 신뢰할 수 있는 인증서 및 ID 인증서를 장치에 배포할 수 있습니다.

신뢰할 수 있는 인증서를 배포하려면 Android 8 이상이 필요하고 신원 인증서를 배포하려면 Android 9 이상이 필요합니다.

"+"를 사용하여 여러 개의 인증서를 추가할 수 있습니다.

신뢰할 수 있는 인증서는 PEM 형식이어야 합니다.

ID 인증서는 PKCS12 형식이어야 합니다.

연결 관리

Wi-Fi

이 설정의 경우 내부 Access
포인트에 액세스하기 위해 최종 사용자 디바이스의 사전 구성을 수행합니다.

서비스 집합 식별자(SSID)	연결할 네트워크의 SSID
숨겨진 네트워크	AP가 SSID를 브로드캐스트하지 않는 경우 활성화합니다.

보안 유형

AP의 보안 유형 설정

WEP

비밀번호	AP의 비밀번호

WPA/WPA2

비밀번호	AP의 비밀번호

802.1x EAP

EAP 방법

PWD	정체성	정체성
	비밀번호	비밀번호

PEAP	2단계 인증 프로토콜	없음	추가 프로토콜 없음
		MSCHAPV2	MSCHAPV2 프로토콜
		GTC	GTC 프로토콜
	CA 인증서	CA 인증서	
	정체성	정체성	
	익명 신원	익명 신원	
	비밀번호	비밀번호	

TTLS	2단계 인증 프로토콜	없음	추가 프로토콜 없음
		PAP	PAP 프로토콜
		MSCHAP	MSCHAP 프로토콜
		MSCHAPV2	MSCHAPV2 프로토콜
		GTC	GTC 프로토콜
	CA 인증서	CA 인증서	
	정체성	정체성	
	익명 신원	익명 신원	
	비밀번호	비밀번호	

TLS	CA 인증서	CA 인증서
	정체성	정체성
	비밀번호	비밀번호

VPN

연결 이름	VPN 연결 이름

VPN 유형

VPN

VPN 클라이언트

AppTec360 VPN 클라이언트	
게이트웨이 구성	게이트웨이 VPN 구성을 선택합니다(**일반 설정 > 유니버설 게이트웨이 > VPN 설정** 참조).
항상 켜져 있는 VPN	기본 잠금 사용
AppTec360 잠금 활성화	AppTec360 잠금 활성화

내장(삼성 디바이스에서만 사용 가능)			
연결 유형	PPTP	서버	서버
		PPTP 암호화 사용	PPTP 암호화 사용
	L2TP / IPSec PSK	서버	서버
		IPSec 사전 공유 키	IPSec 사전 공유 키
		L2TP 비밀 사용	L2TP 비밀 사용
		L2TP 비밀	L2TP 비밀
	IPSec XAuth PSK	서버	서버
		IPSec 식별자	IPSec 식별자
		IPSec 사전 공유 키	IPSec 사전 공유 키
DNS 검색 도메인	DNS 검색 도메인		
전문가 설정	DNS 서버	DNS 서버	
	포워딩 경로	포워딩 경로	

VPN 열기		
서버	서버	
OpenVPN 프로필	OpenVPN 프로필	
OpenVPN 앱	Android용 OpenVPN(권장)	
	OpenVPN 연결	
전문가 설정	DNS 서버	DNS 서버
	포워딩 경로	포워딩 경로

삼성 / 스트롱 스완			
연결 유형	PPTP	서버	서버
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		PPTP 암호화 사용	PPTP 암호화 사용
	L2TP / IPSec PSK	서버	서버
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		L2TP 비밀 사용	L2TP 비밀
	IPSec XAuth PSK	서버	서버
		IPSec 식별자	IPSec 식별자
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
전문가 설정	DNS 서버	DNS 서버	
	포워딩 경로	포워딩 경로	

Cisco Any Connect		
서버	서버	
인증서 모드	장애인	장애인
	자동	자동
전문가 설정	DNS 서버	DNS 서버
	포워딩 경로	포워딩 경로

앱별 VPN

VPN 클라이언트

AppTec360 VPN 클라이언트		
게이트웨이 구성	게이트웨이 VPN 구성을 선택합니다(**일반 설정 > 유니버설 게이트웨이 > VPN 설정** 참조).	
VPN 앱	VPN 앱	
항상 켜져 있는 VPN	기본 잠금 사용	항상 켜져 있는 VPN
AppTec360 잠금 활성화	AppTec360 잠금 활성화	

삼성 / 스트롱 스완			
연결 유형	PPTP	서버	서버
		VPN 앱	VPN 앱
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		PPTP 암호화 사용	PPTP 암호화 사용
	L2TP / IPSec PSK	서버	서버
		VPN 앱	VPN 앱
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		L2TP 비밀 사용	L2TP 비밀
	IPSec XAuth PSK	서버	서버
		VPN 앱	VPN 앱
		IPSec 식별자	IPSec 식별자
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
전문가 설정	DNS 서버	DNS 서버	
	포워딩 경로	포워딩 경로	

제한 사항

여기에서 연결 관리와 관련된 제한 사항을 설정할 수 있습니다.

데이터 로밍 허용	로밍 중 모바일 데이터 허용
강제 데이터 로밍	활성화하면 모바일 데이터 로밍이 영구적으로 활성화됩니다(권장하지 않습니다!). 이 설정은 "데이터 로밍 허용" 설정을 덮어씁니다!
다음 설정은 SAFE 2.x 이상에서만 사용할 수 있습니다.	
긴급 통화만 허용	긴급 통화만 허용
WiFi 허용	WiFi 허용
WiFi 네트워크 최소 보안 수준	WiFi 네트워크 최소 보안 수준 개방형 = 모든 유형의 WiFi 허용
사용자의 WiFi 네트워크 추가 금지	사용자가 직접 WiFi 네트워크를 추가할 수 없습니다. 이 설정은 '연결 관리'에서 WiFi 프로필을 정의한 경우에만 가능합니다.
SMS 및 MMS 허용	모두 = 모든 SMS 및 MMS 트래픽이 허용됨 수신 SMS만 = 수신 SMS 메시지만 허용됨 발신 SMS만 = 발신 SMS 메시지만 허용됨 없음 = SMS/MMS 트래픽이 허용되지 않음
로밍 중 동기화 허용	로밍 중 동기화 허용 켜짐 = 활성화됨 꺼짐 = 비활성화됨 사용자 선택 = 사용자의 선택
음성 로밍 허용	음성 로밍 허용 켜짐 = 활성화됨 꺼짐 = 비활성화됨 사용자 선택 = 사용자의 선택
시스템 http 프록시 서버 사용	설정에서 시스템 설정에 의해 제공되는 HTTP 프록시 서버의 사용은 연결된 네트워크(WiFi 또는 APN)에 따라 달라집니다.

PIM 관리

Gmail 교환

정보: 이 구성은 Gmail 앱에 적용됩니다. 따라서 Gmail을 승인하고 설치해야 합니다.

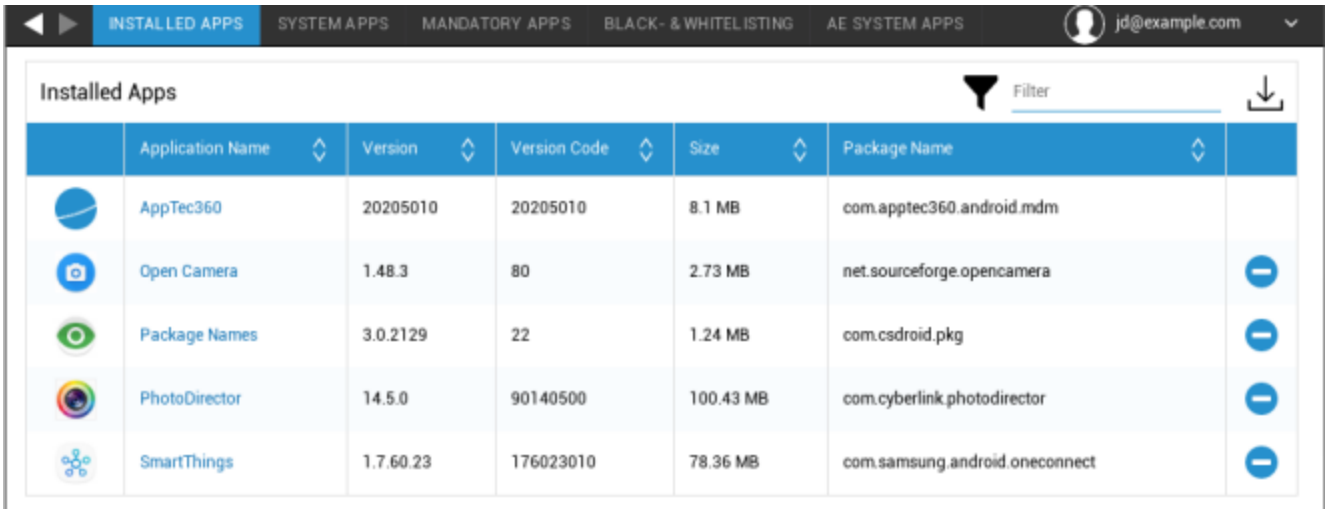
이메일 주소	제공된 사용자의 이메일 주소 자격 증명 작업에 사용할 수 있는 '자리 표시자'는 모든 기기에서 수동으로 변경을 수행하지 않습니다. 클릭 한 번으로 직접 표시할 수 있습니다.
서버 호스트 이름	Exchange 서버의 서버 주소
로그인 이름	각 최종 사용자 디바이스의 로그인 이름, 또한 "여기에 자리 표시자를 참고하세요.
서명	서명을 첨부할 수 있습니다(힌트: 일부 장치에서는 서명에 HTML 형식이 필요합니다).
동기화할 이전 일수	이메일이 다시 동기화되는 시기를 결정하는 일 수
장치 식별자	EAS 장치 ID가 포함된 문자열입니다. 이것은 EAS 프로토콜의 일부이며 특정 환경에서 필요합니다.
SSL(보안 소켓 계층) 사용	SSL 연결 사용
모든 인증서 수락	모든 인증서가 허용됩니다. Exchange Server에서 자체 서명된 인증서를 사용하는 경우 이 옵션을 선택하세요.

앱 관리

엔터프라이즈 앱 관리자

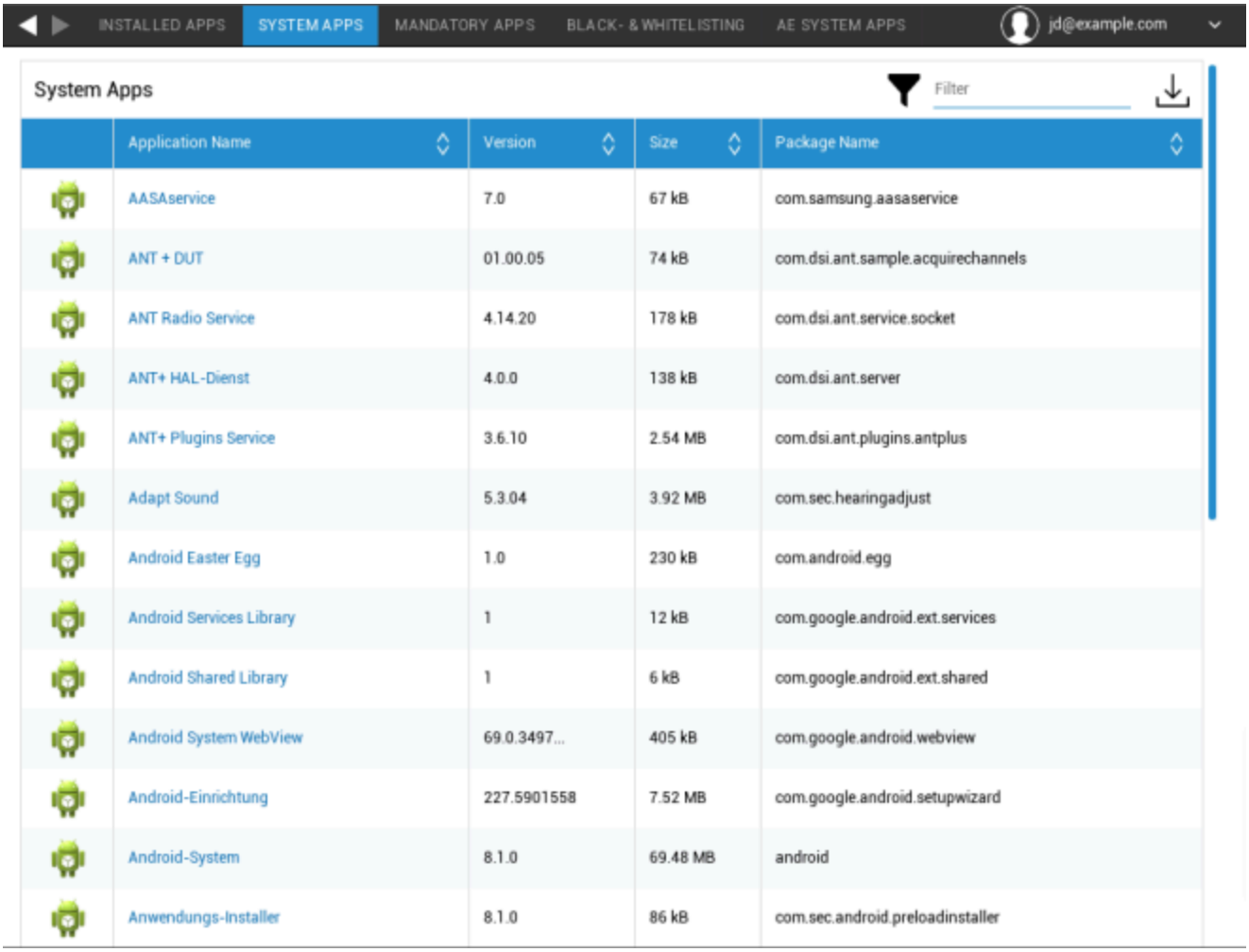
설치된 앱(디바이스 수준에서만)

현재 최종 사용자 디바이스에 설치된 모든 앱이 여기에 표시됩니다.



시스템 앱(디바이스 수준에서만)

'시스템 앱' 아래에는 디바이스 제조업체에서 최종 사용자 디바이스에 이미 설치한 모든 앱과 서비스가 나열됩니다.

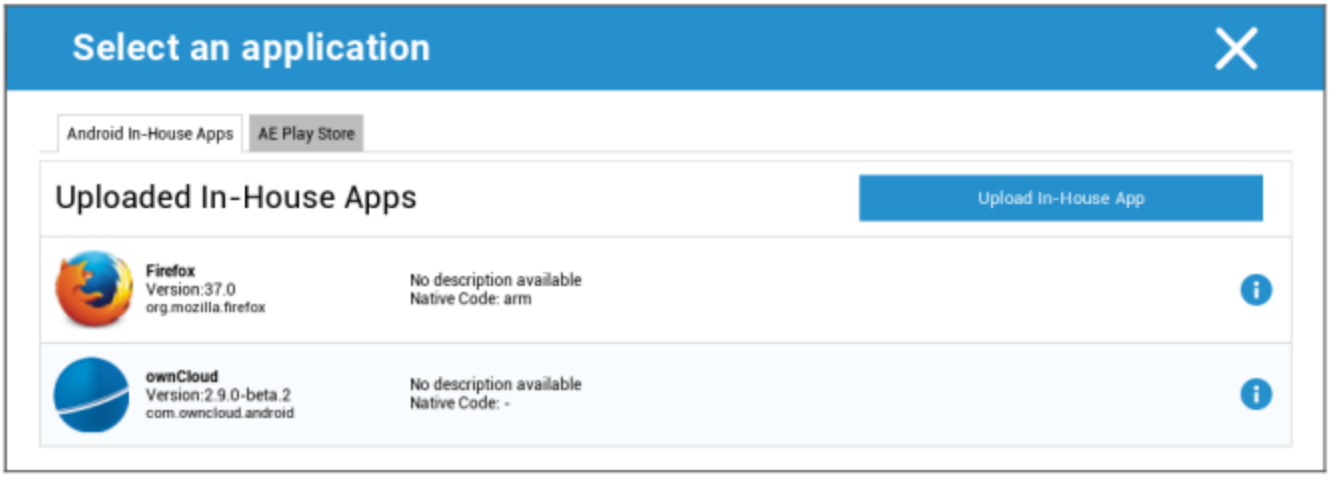


필수 앱

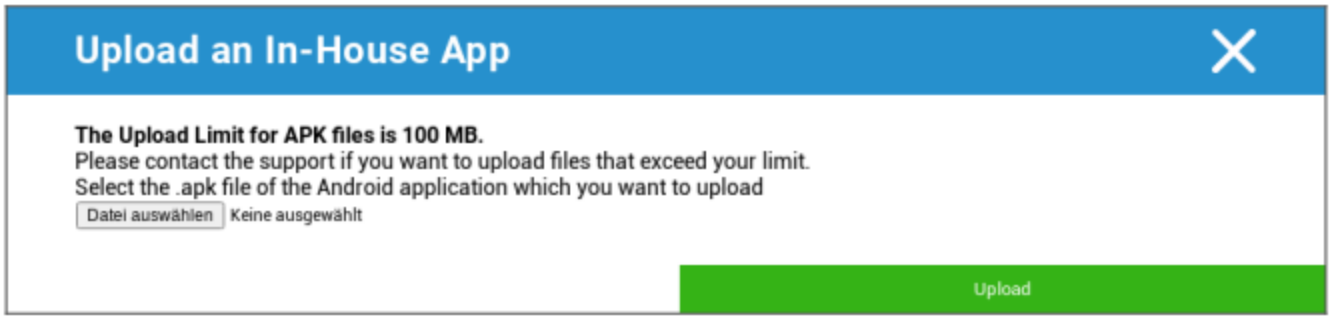
필수 앱에서 필수 앱을 설정할 수 있습니다. 사용자에게 이 지정된 앱을 설치하라는 메시지가 계속 표시됩니다.

를 통해 필수 앱을 정의할 수 있습니다.

일반 설정에서 업로드한 'Android 사내 앱'의 사내 앱이 될 수 있습니다.

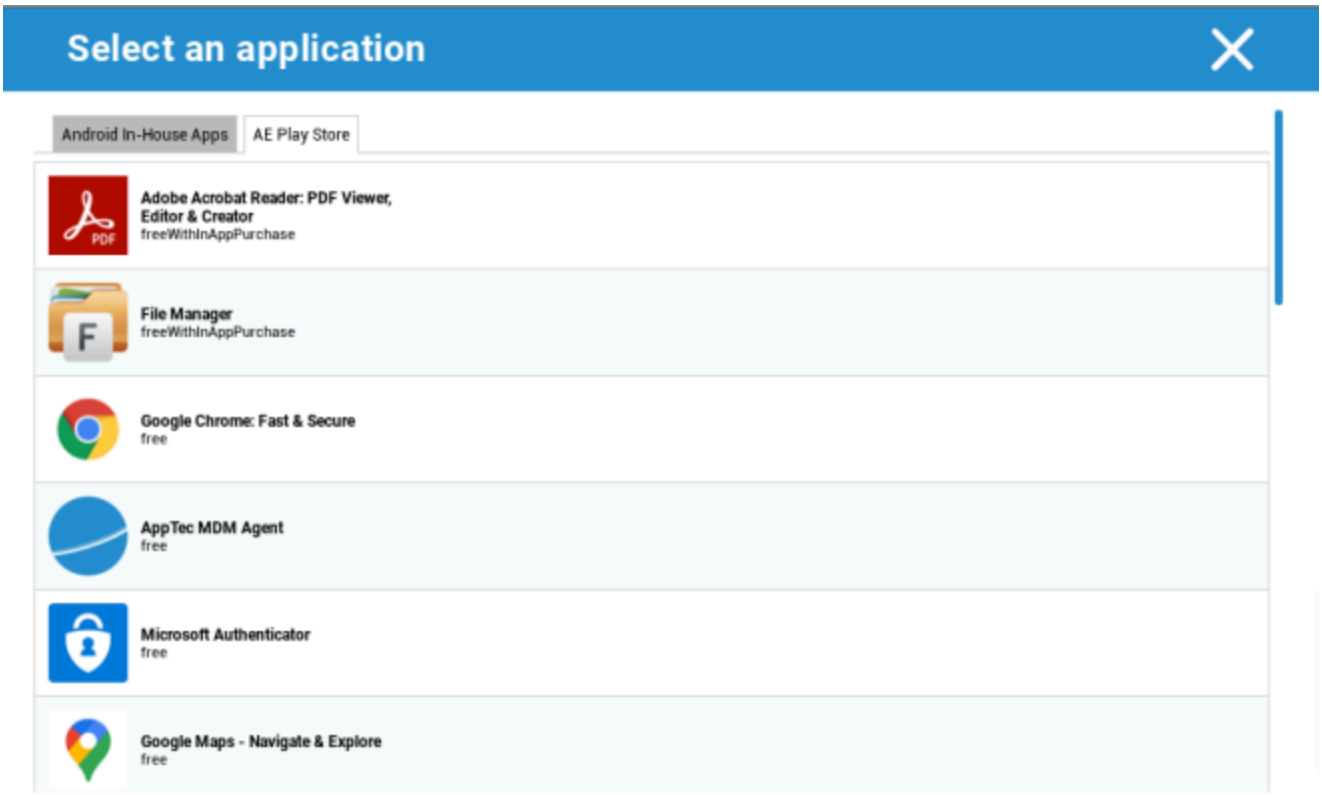


'사내 앱 업로드'를 사용하여 직접 APK 파일을 선택하여 업로드할 수도 있습니다.



사내 앱을 설치하는 경우 '최신 버전 유지'를 활성화할 수 있습니다. 이 기능을 활성화하고 사내 앱 DB에 최신 버전을 정의한 경우 디바이스에서 앱이 업데이트됩니다.

또는 Google Work Play 스토어에서 "AE Play 스토어" 앱을 사용할 수도 있습니다.



이 탭에는 승인된 'AE Play 스토어 앱'만 표시됩니다.

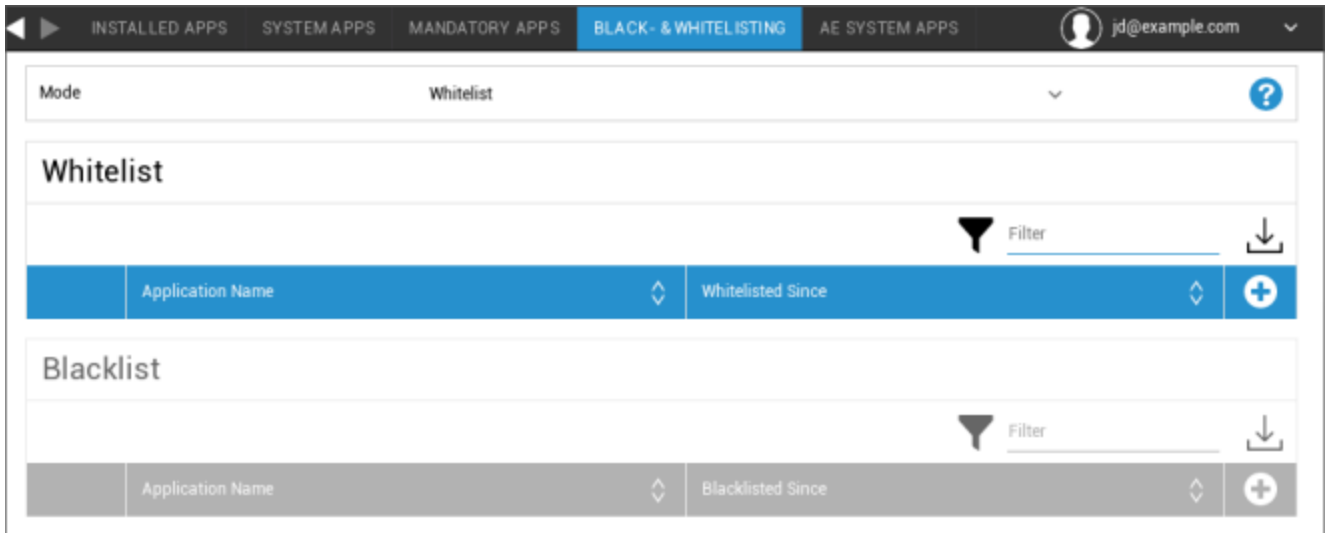
'AE Play 스토어 앱'을 승인하려면 '일반 설정' > '앱 관리' > 'AE Play'로 이동하세요.

Store"를 클릭하고 'Play 스토어 앱' 탭으로 리디렉션되는 버튼을 통해 앱을 추가합니다(또는
에서 'Play 스토어 앱' 탭으로 바로 이동할 수 있습니다).

'Play 스토어 앱' 탭에서 앱을 검색할 수 있습니다. 앱을 클릭하면 앱 페이지(
)가 열리고 여기에서 '승인'을 클릭하여 앱을 승인할 수 있습니다.

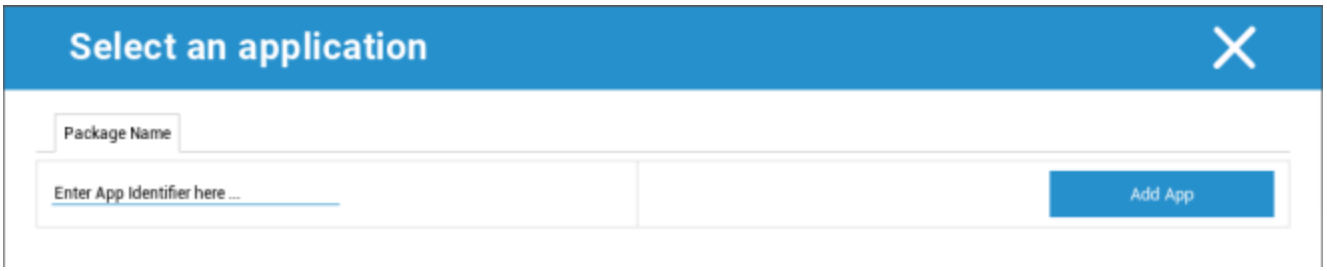
블랙리스트 및 화이트리스트

'블랙리스트 및 화이트리스트'에서 '화이트리스트' 모드와 '블랙리스트' 모드 중에서 선택할 수 있습니다.



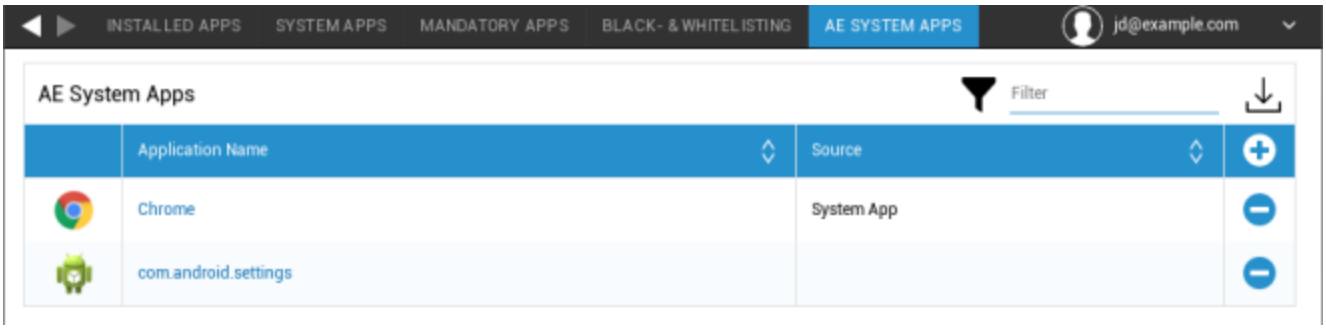
화이트리스트	목록에 추가된 앱과 서비스만 최종 사용자 디바이스에 설치할 수 있습니다. 최종 사용자 디바이스에 이미 사전 설치되어 있는 경우 사용자가 실행할 수 있도록 활성화 및 설정됩니다.
	목록에 추가되지 않은 다른 모든 앱은 최종 사용자 디바이스에 설치할 수 없습니다. 이러한 앱이 이미 최종 사용자 디바이스에 사전 설치되어 있는 경우 사용자가 실행할 수 없도록 비활성화 및 설정됩니다.
블랙리스트	목록에 추가된 앱 및 서비스는 최종 사용자 디바이스에 설치할 수 없습니다. 최종 사용자 디바이스에 이미 사전 설치되어 있는 경우 사용자가 실행할 수 없도록 비활성화 및 설정됩니다.
	목록에 추가되지 않은 다른 모든 앱은 최종 사용자 디바이스에 설치할 수 있습니다. 이러한 앱이 이미 최종 사용자 디바이스에 사전 설치되어 있는 경우 사용자가 실행할 수 있도록 활성화 및 설정됩니다.

를 통해 현재 사용 중인 목록에 앱이나 서비스를 추가합니다.
를 통해 현재 비활성화된 목록에 앱이나 서비스를 추가합니다.
"패키지 이름"을 정의할 수 있습니다:

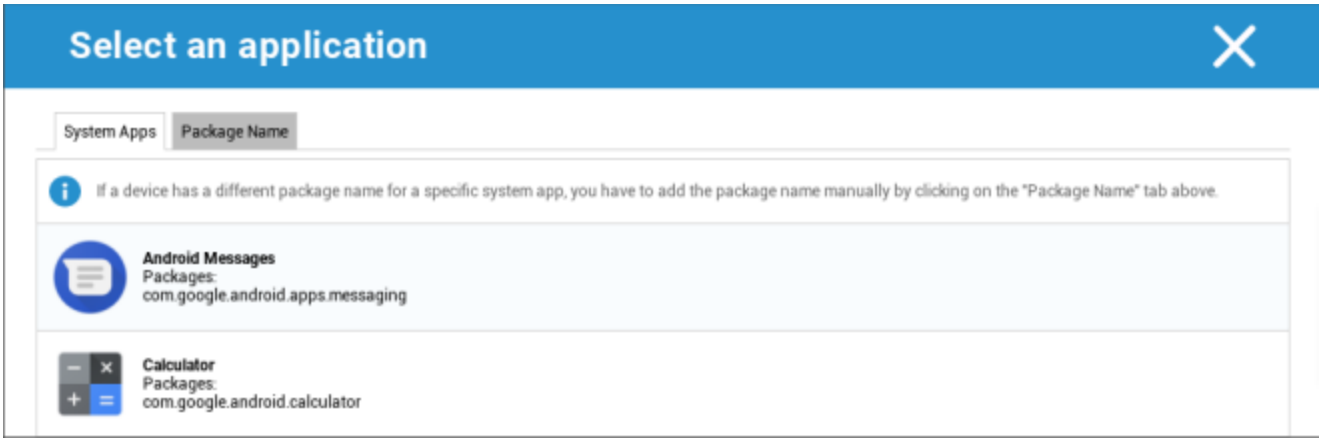


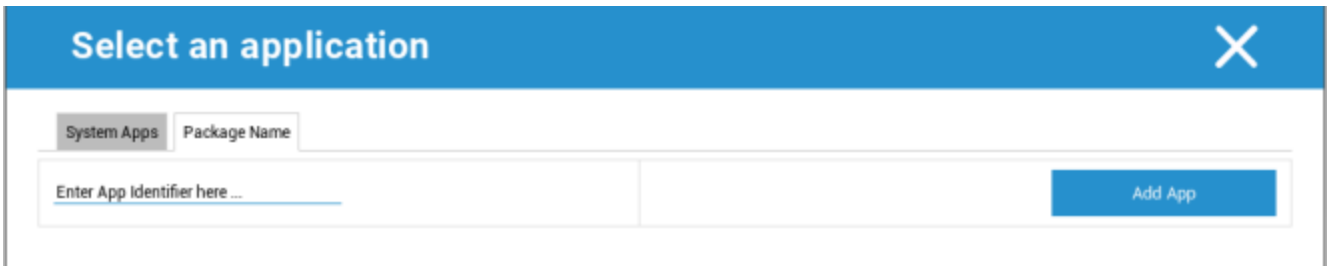
AE 시스템 앱

여기에서 디바이스에서 활성화해야 하는 특정 시스템 앱이 포함된 목록을 정의할 수 있습니다.



버튼을 클릭하면 Google에서 제공하는 가능한 시스템 앱 목록에서 선택하거나 활성화해야 하는 시스템 앱의 패키지 이름을 직접 입력할 수 있습니다.





Google에서 제공하는 목록의 시스템 앱은 시스템 앱이 될 수 있는 앱일 뿐이며, 반드시 기기에서 시스템 앱일 필요는 없다는 점에 유의하세요.

그러나 이 목록은 이미 사전 설치된 앱에만 영향을 미칩니다.

기기에 사전 설치되어 있지 않은 앱을 추가해도 Google에서 제공한 목록에 있는 앱이든 앱의 패키지 이름을 직접 입력한 앱이든 기기에 영향을 미치지 않습니다.

제한 및 설정

앱 관리 설정

여기에서 앱 업데이트와 관련된 디바이스의 동작을 구성할 수 있습니다.

업데이트 확인 빈도	AppTec360 클라이언트가 앱 업데이트를 검색할 간격을 지정합니다. 기본값은 24시간입니다.
Wi-Fi 임계값	지정된 크기보다 큰 앱은 Wi-Fi를 통해 다운로드됩니다. 'Wi-Fi 전용'을 선택하면 모든 앱이 Wi-Fi를 통해 다운로드됩니다.

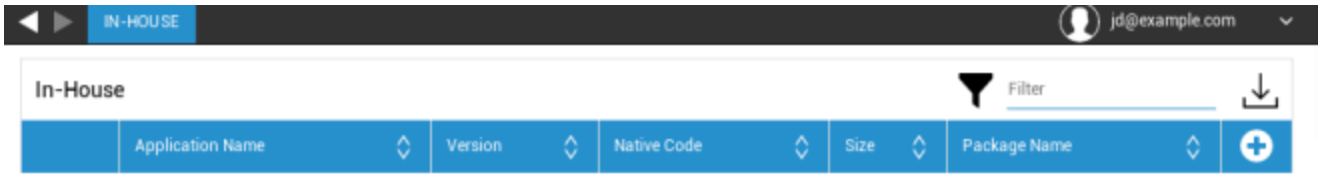
엔터프라이즈 앱 스토어

사내

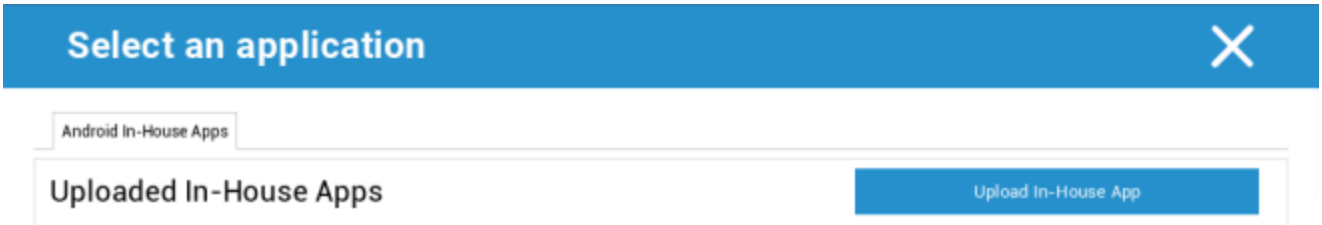
'사내' 항목에서는 내부에서 개발한 앱을 업로드하고 배포할 수 있습니다.

이 기호를 사용하면 사내 앱을 추가로 배포할 수 있습니다.

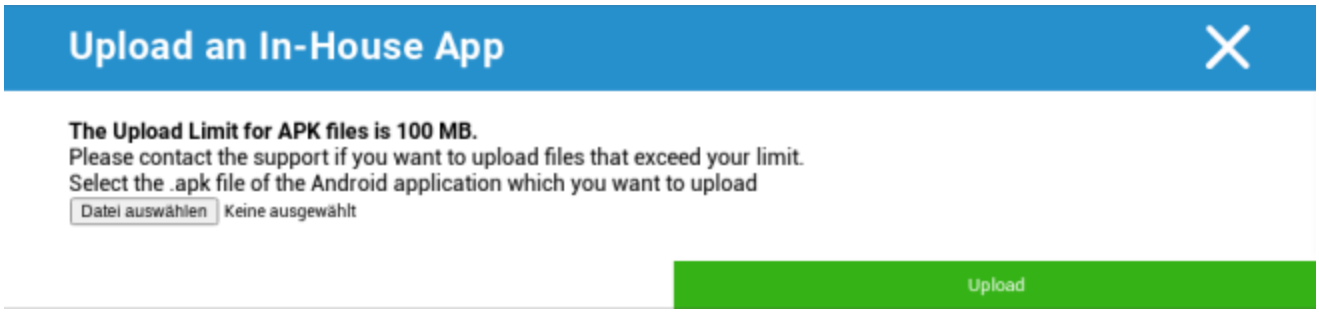
사내 앱을 설치하는 경우 '최신 버전 유지'를 활성화할 수 있습니다.
이 기능이 활성화되어 있고 사내 앱 DB에 최신 버전을 정의한 경우 앱이 디바이스에서 업데이트됩니다.



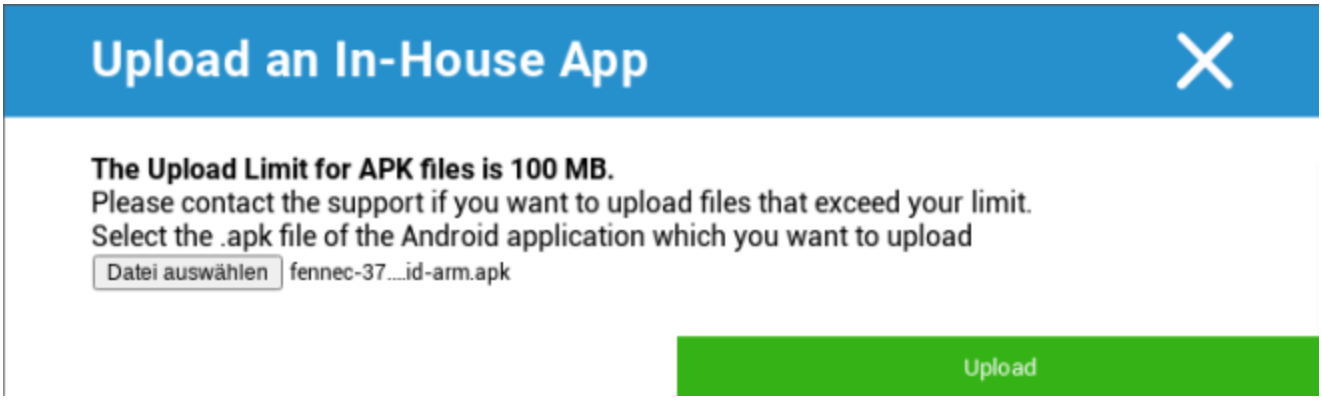
사내 앱을 배포하지 않은 경우 다음과 같은 개요를 받게 됩니다:



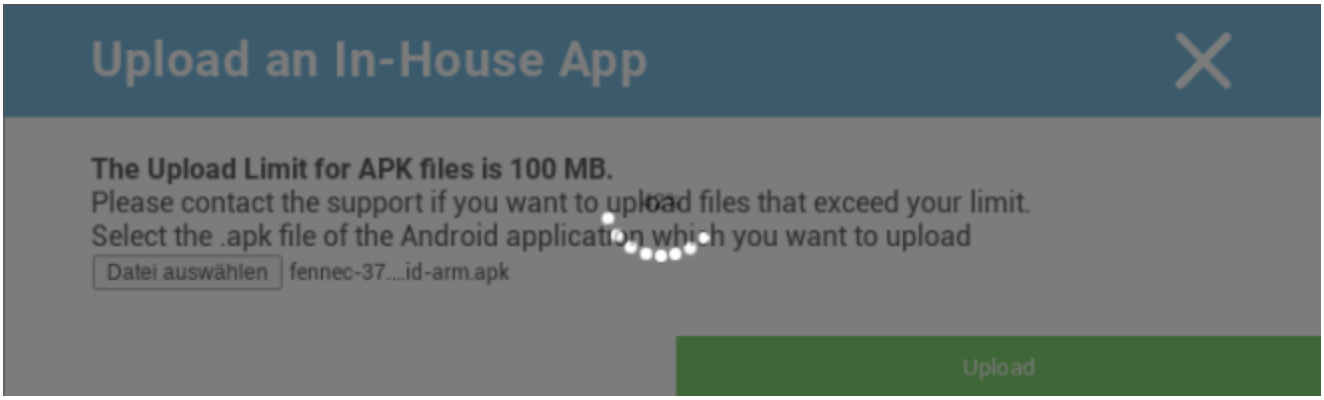
이를 위해 '사내 앱 업로드'를 클릭하면 다음과 같은 개요가 표시됩니다:



이제 "검색..."으로 .apk 파일을 선택한 다음 "업로드"를 클릭합니다.



이제 앱이 업로드되고 원 중앙에 백분율 표시기(
)가 표시되어 앱이 이미 얼마나 업로드되었는지 확인할 수 있습니다.



사내 앱 업로드가 성공적으로 완료되면 앱 카탈로그에서 업로드된 앱(
)을 찾을 수 있습니다.

이제 사용자는 최종 사용자
디바이스의 AppTec360 스토어에서 '사내' 카테고리에서 이 앱을 확인하고 설치할 수 있습니다.

여기에는 구글 플레이스토어 앱이 포함되지 않기 때문에 사용자는 각 최종 사용자 디바이스에 저장된 구글 아이디가 필요하지 않습니다.

기업용 Play 스토어

AE Play 스토어

여기에서 Android 엔터프라이즈 플레이스토어에 앱을 추가할 수 있습니다. 앱을 추가하려면 먼저 AE 관리자 계정으로
앱을 승인해야 합니다.

앱 승인에 대해서는 필수 앱의 지침을 참조하세요.

키오스크 모드 및 런처

키오스크 모드

키오스크 모드에서는 앱 또는 URL을 미리 정의할 수 있습니다. 그러면
이 앱 또는 URL을 실행/방문하는 것이 독점적으로 가능해집니다.

마찬가지로 키오스크 모드에서도 다양한 하드웨어 버튼을 비활성화할 수 있습니다.

자동 시작	프로필이 최종 사용자 디바이스에 도달하는 즉시 키오스크 모드가 자동으로 시작됩니다.
예약된 키오스크 모드?	키오스크 모드의 시간을 계획할 수 있으며, 설정한 시간에 자동으로 시작 및 종료됩니다.
시작 시간	시작 시간
시간(분)	키오스크 모드가 다시 종료되어야 하는 시간(분)

애플리케이션 유형

단일 앱	키오스크 모드에서 앱을 시작하려면 '애플리케이션 유형'에서 패키지'를 선택합니다.
키오스크 애플리케이션	키오스크 모드에서 시작해야 하는 앱을 선택하려면 여기를 클릭하세요. 일반적인 앱 관리의 개요를 확인할 수 있습니다. "구글 플레이 스토어", "안드로이드 인하우스 앱", "패키지 이름" 중에서 선택할 수 있습니다.

애플리케이션 유형

URL	키오스크 모드에서 URL을 실행하려면 '애플리케이션 유형' 아래에서 'URL'을 선택합니다. 그런 다음 원하는 URL 주소를 정의합니다.
비활성 후 브라우저 지우기	여기에서 키오스크 모드가 다시 시작될 시간 간격을 분 단위로 정의할 수 있습니다.
웹 캐시 및 쿠키 지우기	이 기능을 활성화하면 키오스크 모드를 다시 시작하면 웹 캐시(쿠키 및 캐시된 사진)가 지워집니다.
동일 출처 정책	이 기능이 활성화되어 있으면 사용자는 정의된 URL의 하위 페이지만 서핑할 수 있습니다. 예를 들어, 다음 URL을 정의했습니다:www.mypage.com 그러면 사용자는 www.mypage.com/subpage 에서 서핑을 할 수 있습니다.
화이트리스트 URL	여기에서 화이트리스트를 관리할 수 있으며, 다음과 같은 모든 URL이 허용됩니다. 한 줄당 최대 1개의 URL URL은 http:/ 또는 https://로 시작해야 합니다.
블랙리스트 URL	여기에서 블랙리스트를 관리할 수 있으며, 다음과 같은 모든 URL은 허용되지 않습니다. 한 줄당 최대 1개의 URL URL은 http:/ 또는 https://로 시작해야 합니다.
화면 방향	이 설정은 화면 조정과 관련이 있습니다. 자동 = 자동 세로 = 세로 형식 가로 = 가로 모드

멀티 앱	"멀티 앱" 키오스크 모드를 선택하면 AppTec360 런처를 사용하게 됩니다.
앱	애플리케이션을 선택합니다: 키오스크 애플리케이션으로 Play스토어 또는 사내 앱을 선택합니다. 패키지 이름을 입력할 수도 있습니다. 선택한 키오스크 애플리케이션이 장치에 설치되어 있어야 합니다. 키오스크 애플리케이션을 필수로 설정하는 것을 잊지 마세요. 홈 화면의 바로 가기: "켜기"로 설정하면 홈 화면에 바로 가기가 만들어집니다. "끄기"로 설정하면 앱이 앱 목록에 계속 표시됩니다.

종료 암호 사용	이 기능을 활성화하면 사용자가 미리 정의한 비밀번호를 사용하여 키오스크 모드를 종료할 수 있습니다.
종료 비밀번호	이것은 사용자가 미리 정의한 비밀번호입니다.
상태 표시줄 자동 접기	이 옵션을 활성화하면 상태 표시줄이 자동으로 축소됩니다. 이 옵션을 사용하면 사용자는 상태 표시줄에서 정보를 볼 수 있지만 해당 기능에는 액세스할 수 없습니다.
상태 표시줄 비활성화	상태 표시줄에는 알림, 바로 가기 및 정보가 포함되어 있습니다. SAFE 4.0 이상이 설치된 삼성 디바이스에서만 사용할 수 있습니다.
볼륨 키 비활성화	볼륨 키 비활성화(SAFE 3.0 이상이 설치된 삼성 디바이스에서만 사용 가능)
켜기/끄기 스위치 비활성화	켜기/끄기 스위치 비활성화(SAFE 3.0 이상이 설치된 삼성 디바이스에서만 사용 가능)
홈 버튼 비활성화	홈 버튼을 비활성화합니다. 이 기능이 활성화된 경우 키오스크 모드는 AppTec360 콘솔에서만 종료할 수 있습니다. (SAFE 3.0 이상이 설치된 삼성 디바이스에서만 사용 가능)
탐색 모음 비활성화	이를 통해 탐색 모음(뒤로/메뉴)을 비활성화할 수 있습니다. 이 기능이 활성화된 경우, 키오스크 모드는 AppTec360 콘솔에서만 종료할 수 있습니다. (SAFE 3.0 이상이 설치된 삼성 디바이스에서만 사용 가능)

AppTec360 런처

AppTec360 런처 활성화	켜짐: 앱테크360 런처를 활성화합니다. 사용자는 한 번 기본 런처로 설정해야 합니다. 참고: 키오스크 모드가 활성화되어 있고 키오스크 모드가 "멀티 앱"으로 설정되어 있으면 AppTec360 런처의 사용이 강제 적용됩니다.
큰 아이콘	켜짐: 켜기: 런처에서 앱 아이콘을 더 큰 버전으로 표시합니다.
AppTec360 앱 아이콘 숨기기	켜짐: 켜기: AppTec360 앱을 완전히 숨깁니다.
AppTec360 스토어 아이콘 숨기기	켜짐: 켜기: AppTec360 엔터프라이즈 앱스토어를 완전히 숨깁니다.

AppTec360 설정

AppTec360 설정 앱 활성화	AppTec360 설정 앱은 WiFi 및 블루투스 연결을 제어할 수 있습니다.
멀티 앱에서 설정 활성화 키오스크 모드	활성화된 경우, 사용자는 멀티 앱 키오스크 모드가 활성화된 상태에서 AppTec360 설정 앱에 액세스할 수 있습니다.

원격 제어

스플래시탑

기기의 원격 제어 세션을 시작하려면 **앱 관리** → **엔터프라이즈 앱 관리자** → **필수 앱에** 앱을 추가하여 기기에 '스플래시탑 스트리머' 앱을 설치해야 합니다.

그런 다음 스플래시탑에 대해 다음 설정을 구성합니다:

스플래시탑 사용	이 기능을 활성화하면 앱텍360이 원격 제어를 허용하도록 스플래시탑 앱을 구성합니다.
코드 배포	https://my.splashtop.com 으로 이동하여 Splashtop 계정에 로그인합니다. '컴퓨터 추가'를 클릭하고 결과 페이지에서 12자리 배포 코드를 복사합니다.
사용자 지정 배포 게이트웨이를 설정하시겠습니까?	게이트웨이 배포
게이트웨이 도메인/호스트 배포	게이트웨이 배포
인증서 확인	인증서 확인

그런 다음 스플래시톱 원격 제어 옵션을 사용하여 컨텍스트 메뉴(장치가 선택된 경우 검색창 옆의 기어 또는 트리에서 장치를 마우스 오른쪽 버튼으로 클릭)에서 원격 제어 세션을 시작할 수 있습니다.

TeamViewer

기기에 대한 원격 제어 세션을 시작하려면 **앱 관리** → **기업 앱 관리자** → **필수 앱에** 앱을 추가하여 기기에 "TeamViewer QuickSupport" 앱을 설치해야 합니다.

그런 다음 **TeamViewer 원격 제어** 옵션을 사용하여 컨텍스트 메뉴(장치가 선택된 경우 검색 표시줄 옆의 기어 또는 트리에서 장치를 마우스 오른쪽 버튼으로 클릭)에서 원격 제어 세션을 시작할 수 있습니다.

콘텐츠 관리

콘텐츠 상자

여기에서 콘텐츠 상자를 활성화할 수 있습니다.

'콘텐츠 박스 사용'을 '켜기'로 전환하면 별도의 콘텐츠 박스 앱(
)이 최종 사용자 장치에 자동으로 설치됩니다.

보안 브라우저

여기에서 AppTec360 보안 브라우저의 설정을 구성할 수 있습니다.

'보안 브라우저'의 섹션을 '켜기'로 전환하면 별도의 브라우저 앱(
)이 최종 사용자 디바이스에 자동으로 설치됩니다.

비밀번호 필요	사용자가 브라우저에 액세스하기 위해 비밀번호를 설정하고 사용하도록 요구합니다.
최소 필수 비밀번호 길이	비밀번호에 필요한 글자 수를 설정합니다.
필수 비밀번호 품질	필요한 비밀번호 품질 설정
다운로드 제한/열기	
업로드 제한	
화이트리스트 업로드	업로드가 항상 허용되는 URL 목록입니다.
복사 허용	웹 페이지 내의 텍스트 복사, 잘라내기 또는 공유를 허용합니다.
화면 캡처 허용	스크린샷 캡처를 허용합니다.
데이터 정리 빈도	모든 사용자 데이터(기록, 캐시 등)를 자동으로 삭제할 빈도를 선택합니다.
회사 북마크	북마크는 브라우저 북마크의 '회사 북마크' 폴더에 표시됩니다. 사용자가 편집할 수 없습니다.
주소 표시줄 숨기기	
브라우저 내 화이트리스트(유니버설 게이트웨이 제외)	클라이언트 측 URL 화이트리스트를 활성화합니다. • 회사 북마크는 항상 화이트리스트에 등록됩니다. • 100개의 URL만 지원 • 유니버설 게이트웨이를 사용하여 무제한 블랙리스트 및 화이트리스트에 액세스하세요.
화이트리스트 URL	허용된 URL 목록입니다.
게이트웨이 기반 블랙리스트 및 화이트리스트	블랙리스트에는 다음과 같은 요구 사항이 있습니다: • 작동하는 AppTec360 유니버설 게이트웨이("일반 설정" → "유니버설 게이트웨이") • 지정된 DNS 서버로 작동하는 VPN 구성("일반 설정" → "범용 게이트웨이" → "VPN 설정")

	• 블랙리스트 구성('일반 설정' → '유니버설 게이트웨이' → '도메인 블랙리스트') • 프로필의 유효한 VPN 연결("연결 관리" → "VPN")

추가 API

삼성 KNOX

제한 사항

SD 카드 허용	
SD 카드 쓰기 허용	
화면 캡처 허용	
클립보드 허용	
Google 클라우드의 설정 및 앱 데이터 백업	
앱을 다시 설치할 때 Google 클라우드에서 설정 복원하기	
USB 디버깅 허용	
Google 충돌 보고서 허용	
공장 초기화 허용	
OTA 업그레이드 허용	
USB 호스트 스토리지 허용	이 기능을 활성화하면 사용자는 펜 드라이브(휴대용 USB 저장 장치), 외장형 HD 또는 보안 디지털(SD) 카드 리더를 연결할 수 있으며, 장치에 저장 드라이브로 마운트됩니다.
USB 미디어 플레이어(MTP, PTP) 허용	
마이크 허용	타사 애플리케이션의 마이크를 비활성화합니다.
NFC(근거리 무선 통신) 허용	
알 수 없는 소스 허용(APK 사이드로드)	활성화하면 앱(APK 파일)의 사이드 로딩이 허용됩니다. 이 설정을 비활성화하면 알 수 없는 출처의 APK 설치를 허용할 때 사용자가 수동으로 활성화해야 합니다.
사용자 생성 허용	활성화하면 사용자는 장치에서 여러 계정(예: 게스트 계정)을 만들 수 있습니다.

이메일

이메일 주소	
수신 서버 프로토콜	
수신 서버 주소	
수신 서버 포트	
수신 서버 로그인/사용자 이름	
수신 서버 비밀번호	
들어오는 서버는 SSL을 사용합니다.	
수신 서버는 TLS를 사용합니다.	
수신 서버는 모든 인증서를 수락합니다.	
발신 서버 프로토콜	
발신 서버 주소	
발신 서버 포트	
발신 서버는 추가 자격 증명을 사용합니다.	비활성화하면 시스템에서 발신 서버에 대해서도 수신 자격 증명을 사용합니다.
발신 서버 로그인/사용자 이름	
발신 서버 비밀번호	
발신 서버는 SSL을 사용합니다.	
발신 서버는 TLS를 사용합니다.	
발신 서버는 모든 인증서를 수락합니다.	
서명 설정	
서명	참고: 일부 디바이스의 경우 서명을 HTML 형식으로 지정해야 합니다.
새 이메일 수신 시 사용자에게 알림	

교환

이메일 주소	
서버 호스트 이름	Exchange 서버의 호스트 이름
로그인 이름	Exchange Server에 로그인하는 데 사용되는 사용자 이름입니다.
도메인	ACL 게이트웨이 구성이 활성화되어 있고 도메인 필드가 비어 있지 않은 경우 AppTec360 유니버설 게이트웨이는 다음 이름인 "도메인\로그인 이름"으로 장치를 인증합니다.
비밀번호	
동기화할 이전 일수	
이메일 동기화 빈도	
로밍 중 동기화	
서명 설정	
서명	참고: 일부 디바이스의 경우 서명을 HTML 형식으로 지정해야 합니다.
기본 계정	
SSL(보안 소켓 계층) 사용	
TLS(전송 계층 보안) 사용	
모든 인증서 수락	

APN

APN 표시 이름	
액세스 포인트 이름	APN 이름
발신 서버 프로토콜	
MCC - 모바일 국가 코드	설치된 SIM의 MMC를 사용하려면 비워둡니다.
MNC - 모바일 네트워크 코드	설치된 SIM의 mnc를 사용하려면 비워둡니다.
서버 주소	
서버 포트 번호	
서버 프록시 주소	
MMS 서버 주소	기본값으로 비워 두기
MMS 포트 번호	기본값으로 비워 두기
MMS 프록시 주소	기본값으로 비워 두기
사용자 이름	
비밀번호	
액세스 포인트 유형	허용되는 유형은 "default", "mms", "supl"입니다.
	null 또는 빈 값을 전달하면 기본적으로 "default,supl,mms"가 사용됩니다.
	기본적으로 비워 둡니다.
기본 APN	

블루투스

블루투스를 통한 장치 검색 허용	
블루투스 페어링 허용	
블루투스 헤드셋 장치 허용	
블루투스 핸즈프리 장치 허용	
Bluetooth A2DP 장치 허용	A2DP, 고급 오디오 배포 프로필로 장치 간 오디오 스트리밍 가능
발신 전화 허용	
블루투스를 통한 데이터 전송 허용	
블루투스 테더링 허용	
블루투스를 통해 컴퓨터에 연결 허용	

연결

긴급 통화만 허용Wi-Fi 허용	
Wi-Fi 네트워크 최소 보안 수준	
사용자의 Wi-Fi 네트워크 추가 금지	이 제한은 연결 관리에서 활성 Wi-Fi 프로필이 하나 이상 정의되어 있는 경우에만 활성화할 수 있습니다.
SMS 및 MMS 허용	
로밍 중 동기화 허용	
음성 로밍 허용	

안드로이드 엔터프라이즈 – 완전 관리형 디바이스 위드-워크 프로필(COPE)

COPE에 대한 일반적인 설명

COPE는 **기업 소유 개인 사용의**약자입니다.

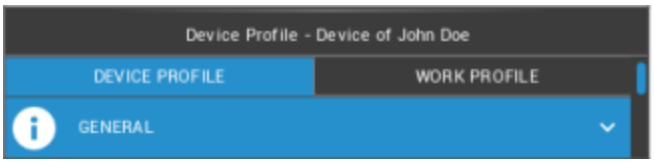
COPE 모드를 사용하면 Android 기기를 통합 **Android Enterprise - 컨테이너** 프로필이 있는 Android **Enterprise - 완전 관리형 기기로** 등록할 수 있습니다.

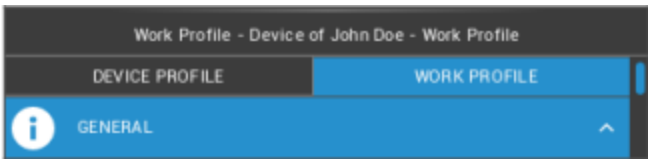
이미 **Android Enterprise - 완전 관리형 디바이** 스로 등록되어 있고 **Android Enterprise - 컨테이너가** 추가로 설정되어 있는 Android 디바이스이거나, 새로 등록한 Android 디바이스가 Android **Enterprise - 완전 관리형 디바이스로** 직접 등록되고 그 위에 **Android Enterprise - 컨테이너가** 함께 등록되어 있는 경우일 수 있습니다.

COPE 모드는 Android 8, 9 및 10이 설치된 기기에서만 사용할 수 있습니다.

COPE 장치용 프로파일 구성

COPE 모드 자체에 대한 구성 프로필이 없으므로, **Android Enterprise - 완전 관리형 디바이스** 및 **Android Enterprise - 컨테이너의** 구성은 COPE 프로필 내에서 두 개의 프로필로 분리되어 있습니다. 콘솔 왼쪽의 해당 버튼을 클릭하여 각 프로필의 구성을 위해 두 프로필 사이를 전환할 수 있습니다:





두 프로필 모두 각 개별 프로필에 대해 설명된 대로 구성할 수 있습니다:

안드로이드 엔터프라이즈 - 완전 관리형 디바이스

안드로이드 엔터프라이즈 - 컨테이너

AE 완전 관리형 디바이스로 되돌리기

Android Enterprise - 컨테이너 프로필은 **모바일 관리에** 설명된 대로 제거할 수 있습니다.

컨테이너 프로필을 제거하면 COPE 프로필이 **Android Enterprise - 완전 관리형 디바이스** 프로필로 변환됩니다.

Android Enterprise – 컨테이너 구성

현재 그룹 프로필을 선택했는지 또는 디바이스를 선택했는지에 따라 개요와 하위 요점이 달라지므로 이를 신중하게 고려해 주세요!

일반

프로필 개요(프로필 수준에서만)

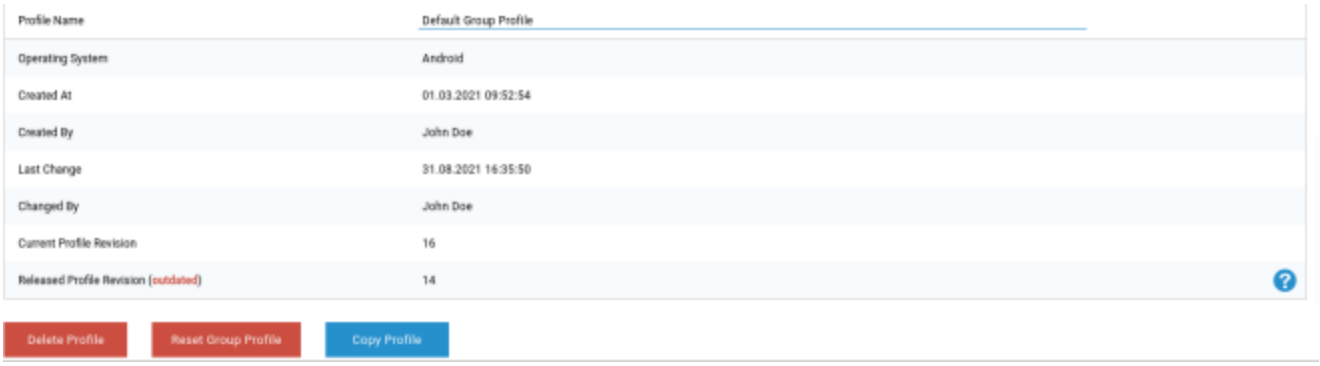
프로필에 있는 경우 이름, 운영체제, 작성 날짜, 작성자 등 프로필에 대한 간략한 개요를 볼 수 있습니다.

프로필 이름	프로필 이름 - 여기에서 직접 이름을 변경할 수 있습니다.
운영 체제	프로필에 유효한 OS
만든 곳	생성 날짜
만든 사람	만든 사람
마지막 변경 사항	마지막 변경 날짜
변경자	이 프로필을 마지막으로 변경한 사용자
현재 프로필 수정	프로필이 이미 업데이트된 횟수
프로필 수정 버전 출시	프로필이 이미 업데이트되어 디바이스가 할당된 횟수

프로필 삭제	프로필 삭제
그룹 프로필 재설정	그룹 프로필 재설정
프로필 복사	프로필 복사

그룹 프로필 개요(그룹 수준에서만)

그룹 프로필을 열면 프로필에 대한 간략한 개요를 볼 수 있습니다.



프로필 이름	프로필 이름(여기에서 변경 가능)
운영 체제	프로필의 운영 체제
만든 곳	생성 시간
만든 사람	프로필 작성자
마지막 변경 사항	프로필을 마지막으로 변경한 시간
변경자	마지막으로 변경한 계정
현재 프로필 수정	저장된 프로필 상태 수정
프로필 수정 버전 출시	할당된 프로필 수정본('지금 할당'). 텍스트 뒤에 '(오래된)'이라는 레이블이 표시되면 프로필을 저장했지만 아직 할당하지 않았으므로 디바이스는 여전히 이전 버전을 받게 됩니다.

장치 개요(장치 수준에서만)

디바이스를 사용하는 경우 선택한 디바이스에 대한 개요 요약이 표시되며, 여기에는 다음과 같은 내용이 포함되어 있습니다:

장치 이름	장치 이름
위치	위치 좌표
전화번호	전화번호
필수 앱 지정	할당된 필수 앱 수
OS 버전	디바이스의 OS 버전
운영 체제	운영 체제(Android Enterprise)
일련 번호	장치 일련 번호
디바이스 소유권	기업 또는 개인 디바이스
디바이스 유형	AE 업무용 관리 디바이스
루팅	상태, 기기가 루팅되었는지 여부를 나타냅니다.
규정 준수	가이드라인 준수
IP 주소	디바이스의 IP 주소
마지막으로 본	기기가 AppTec에 마지막으로 연결한 시점
마지막 푸시	마지막 푸시가 디바이스로 전송된 시점, 특정 시점
사용자 할당	이 장치가 할당된 사용자 또는 그룹

구성 개정

여기에서 장치에 어떤 그룹 프로필이 할당되었는지에 대한 개요를 볼 수 있습니다.

그룹 프로필을 클릭하면 이 프로필에 직접 액세스할 수 있으며 설정을 수행할 수 있습니다.

이 기호를 사용하면 배포된 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

이 기호를 사용하면 사용한 모든 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

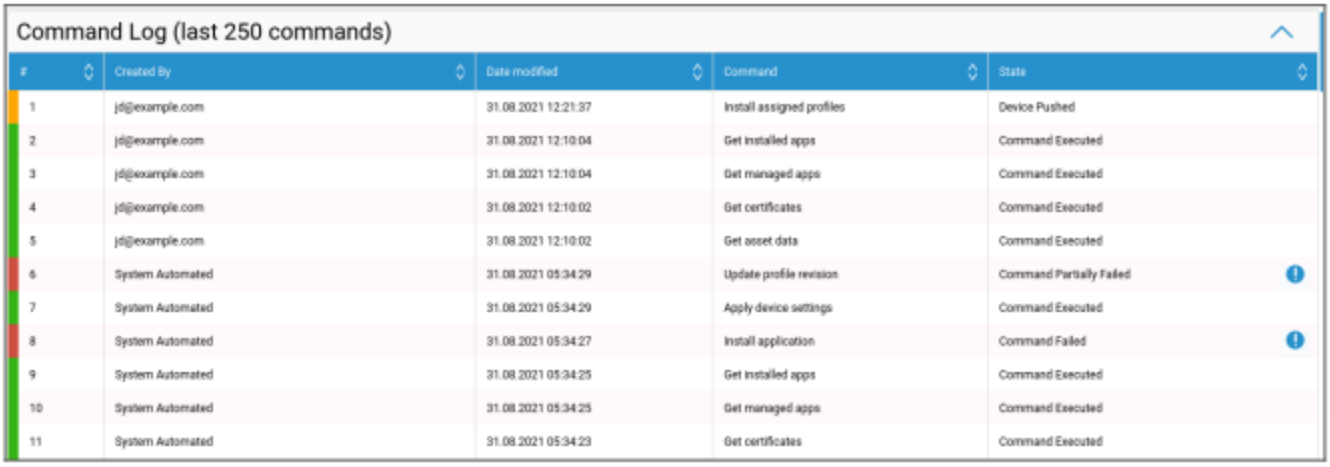
"최신 수정본 사용 가능"은 그룹 프로필이 변경되어 저장되었지만 할당되지 않았음을 나타냅니다. 변경 사항을 디바이스에 적용하려면 그룹 수준에서 '지금 할당'을 사용하여 그룹 프로필을 할당해야 합니다.

디바이스 로그(디바이스 수준에서만)

여기에서 다양한 장치 로그를 받을 수 있습니다. 필요한 경우 여기에서 오류의 원인을 직접 찾을 수 있습니다.

명령 로그

여기에서 디바이스에 대해 어떤 명령이 실행되었는지, 어떤 상태인지 확인할 수 있습니다.



가능한 명령 상태

푸시된 장치	푸시 요청이 푸시 서비스(예: APNS)로 전송되어 디바이스가 EMM 서버에 다시 연결하도록 지시합니다.
명령 생성	이 명령은 시스템에서 생성되었습니다.
명령 전송	명령은 서버에 연결한 후 디바이스로 전송되었습니다.
명령 실행	명령이 성공적으로 실행되었습니다.
명령 실패	명령이 실패했습니다. *
명령이 부분적으로 실패했습니다.	디바이스 OS에 따라 일부 명령이 함께 그룹화될 수 있습니다. 이 경우 이 명령 그룹의 일부가 실패했습니다. *
명령 실행, 결국 실패	명령이 실행되었지만 실행되지 않았을 수도 있습니다.
명령 재푸시	명령이 사용자에 의해 다시 푸시되었습니다.
폐기됨	명령이 삭제되었습니다. 예를 들어 다른 명령으로 대체되었거나 디바이스가 다시 등록되어 이전 명령이 제거되었기 때문입니다.

*메시지 뒤에 느낌표가 있는 경우 커서로 아이콘을 가리키면 자세한 정보를 확인할 수 있습니다.

디바이스 설정

클라이언트 구성

여기에서 Android 디바이스에서 다음 구성을 수행할 수 있습니다:

규정 준수 시간 초과	강제 조치가 적용되는 사용자 응답 시간 제한입니다.
규정 준수 시간 초과 후 시행 조치	사용자가 규정 준수 디바이스 상태를 초래하는 작업을 수행하지 않는 경우의 강제 조치
데이터 수집 빈도	기기/GPS 정보 수집 빈도
장치 하트비트 주파수	장치가 앱텍 서버에 연결해야 하는 간격 Min. 1분 최대. 24시간
위치 업데이트 사용	활성화된 경우, 장치는 위치 업데이트를 앱텍 서버로 전송합니다.
위치 업데이트 시간	장치가 AppTec에 위치 업데이트를 전송하는 시간 간격을 결정합니다.
위치 업데이트에 Google 위치 정확도 사용	활성화하면 네트워크 위치가 위치 업데이트에 사용됩니다('제한'에서 비활성화한 경우 이 설정은 아무 영향도 미치지 않습니다).
위치 업데이트를 위해 GPS 위치 사용	활성화하면 GPS가 위치 업데이트에 사용됩니다.
모의 (가짜) 위치 허용	타사 앱을 통한 위치 정보 위조 허용
연결 끊김 조치	이 옵션을 활성화하면 장치가 하트비트 간격으로 MDM 서버에 연결되지 않는 경우에 대한 동작을 지정할 수 있습니다. 예를 들어 디바이스의 하트비트 시간이 5분인 경우 오전 10시 35분에 서버에 연결됩니다. 그 후에는 디바이스가 Wi-Fi 범위를 벗어납니다. 오전 10시 40분에 다음 하트비트가 실패하고 지정된 작업이 실행됩니다.
액션	디바이스가 규정을 준수하지 않게 되는 즉시 취해야 할 조치입니다. • Lock 장치 = 잠금 장치 • 장치 초기화 = 장치가 공장 설정으로 복원됩니다. • 장치 및 SD 카드 초기화 = 장치가 공장 설정으로 복원되고 SD 카드 저장소가 삭제됩니다.
임계값	지정된 작업을 트리거하는 데 필요한 실패한 하트비트 임계값을 지정할 수 있습니다.

정책 적용 모드	기본값입니다:	사용자에게 미결 작업을 실행하라는 메시지가 주기적으로 표시됩니다.
	게으른 정책 시행:	사용자에게 미결 작업을 실행하라는 메시지가 표시되지 않습니다. 열려 있는 모든 작업은 AppTec 클라이언트에 표시됩니다.
	적극적인 정책 집행:	사용자에게 미결 작업을 실행하라는 메시지가 계속 표시됩니다.
앱텍 버전 잠금	활성화하면 AppTec 앱의 버전 코드를 지정할 수 있습니다. AppTec 클라이언트는 지정된 버전으로만 업데이트됩니다. 최신 버전은 무시됩니다. 다운그레이드는 불가능합니다.	
버전 코드	잠글 AppTec 앱의 버전 코드입니다.	
앱텍 알림 비활성화	비활성화하면 AppTec 클라이언트는 알림 표시줄에 알림을 표시하지 않습니다. 따라서 사용자는 작업 관리자를 통해 AppTec 클라이언트를 닫을 수 있습니다. AppTec 클라이언트가 닫히면 키오스크 모드 및 앱 블랙/화이트 리스트 등 여러 기능이 제대로 작동하지 않습니다. 삼성 기기는 앱텍 클라이언트를 위한 보호 메커니즘을 제공합니다. KNOX API를 지원하는 삼성 디바이스에서는 기본적으로 알림이 비활성화되어 있습니다. Android 8.0 이상의 디바이스에서는 알림이 비활성화되지 않아야 합니다.	

배경 화면

사용자 지정 배경 화면 설정	사용자 지정 배경화면 활성화/비활성화
배경 화면	컬러 코드 또는 이미지를 사용하도록 배경화면 모드를 설정합니다.
색상 지정	배경색을 16진수 값으로 지정합니다(예: 검정색은 #000000, 흰색은 #ffffff).
이미지를 배경화면으로 설정	배경화면으로 사용할 이미지 파일을 업로드합니다.

자산 관리(디바이스 수준에서만)

장치 정보

모델	디바이스 모델 지정
운영 체제	OS
OS 버전	OS 버전
일련 번호	일련 번호
장치 이름	장치 이름
배터리 상태	배터리 상태
여유 / 총 메모리	여유 / 총 메모리
삼성 금고	다양한 설정 옵션에 필요한 삼성 SAFE 인터페이스
SD 카드 사용 가능	SD 카드 사용 가능
SD 카드 에뮬레이션	SD 카드 에뮬레이션
SD 카드 이동식	SD 카드 탈착식
SD 여유 / 총 메모리	SD 무료 / 총 SD 카드 메모리

Wi-Fi

IP 주소	디바이스 IP 주소
WiFi MAC	WiFi MAC 주소

셀룰러

상태	상태(SIM 카드 설치)
전화번호	전화번호
로밍(음성/데이터)	음성/데이터 로밍
로밍 상태	현재 로밍 상태
IP 주소	IP 주소
사업자/이동 통신사	사업자/이동 통신사
셀룰러 기술	셀룰러 기술
IMEI	IMEI 번호
ICCID	SIM 카드의 ID이며, 종종 스마트카드 또는 집적 회로 카드(ICC)이기도 합니다.
IMSI	국제 모바일 가입자 신원(IMSI)은 GSM 및 UMTS 모바일 네트워크에서 네트워크 사용자를 명확하게 식별하는 기능을 제공합니다. IMSI는 최대 15자리로 구성되며 다음과 같은 방식으로 구성됩니다: • 모바일 국가 코드 (MCC), 3자리 • 모바일 네트워크 코드 (MNC), 2자리 또는 3자리 • 모바일 가입자 식별 번호(MSIN), 1~10자리
현재 MCC/MNC	"SIM MCC/MNC" 참조
SIM MCC/MNC	모바일 국가 코드는 ITU에서 E.212 표준에 따라 설정한 국가 식별자입니다. 이는 모바일 네트워크 식별을 위해 모바일 네트워크 코드(MNC)와 함께 작동합니다. SIM 카드의 국가/모바일 네트워크 코드를 의미합니다. 다른 모바일 네트워크로 로밍하는 경우 논리적으로 '현재 MCC/MNC'와 'SIM MCC/MNC'가 달라집니다.

블루투스

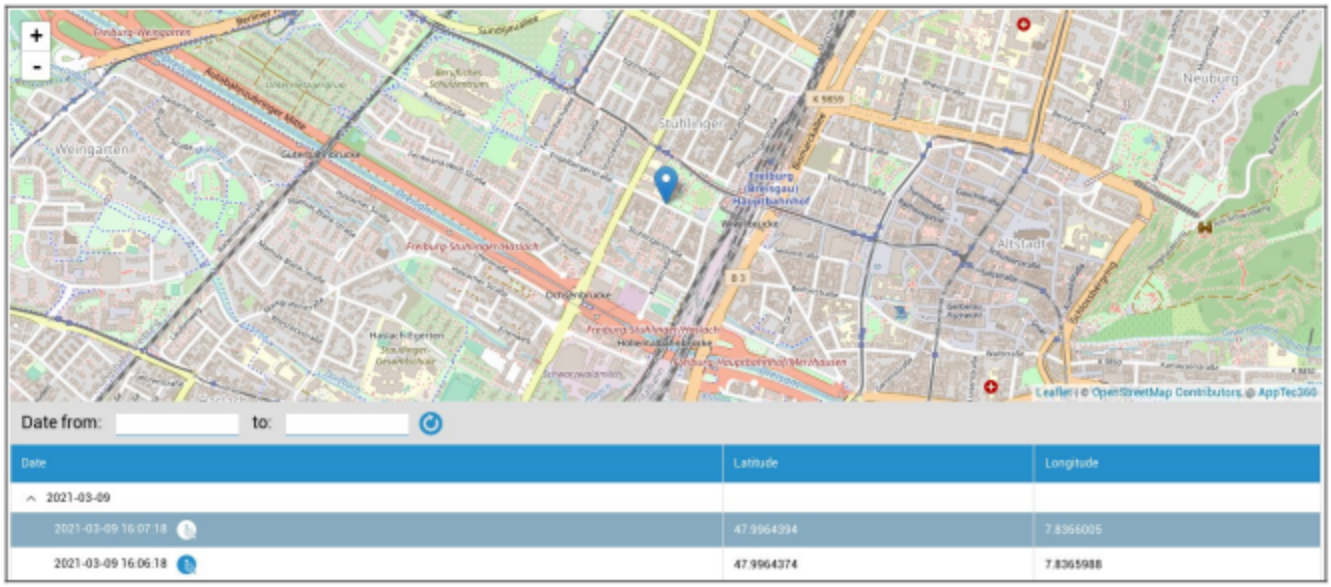
블루투스 MAC	블루투스 MAC 주소

보안 관리

도난 방지(디바이스 수준에서만)

GPS 정보(디바이스 수준에서만)

여기에서 현재/마지막 장치 위치를 설정할 수 있습니다. 현지화는 하나 또는 두 개의 비밀번호로 보호할 수 있습니다(참조: 일반 설정 - 개인정보 - GPS 액세스



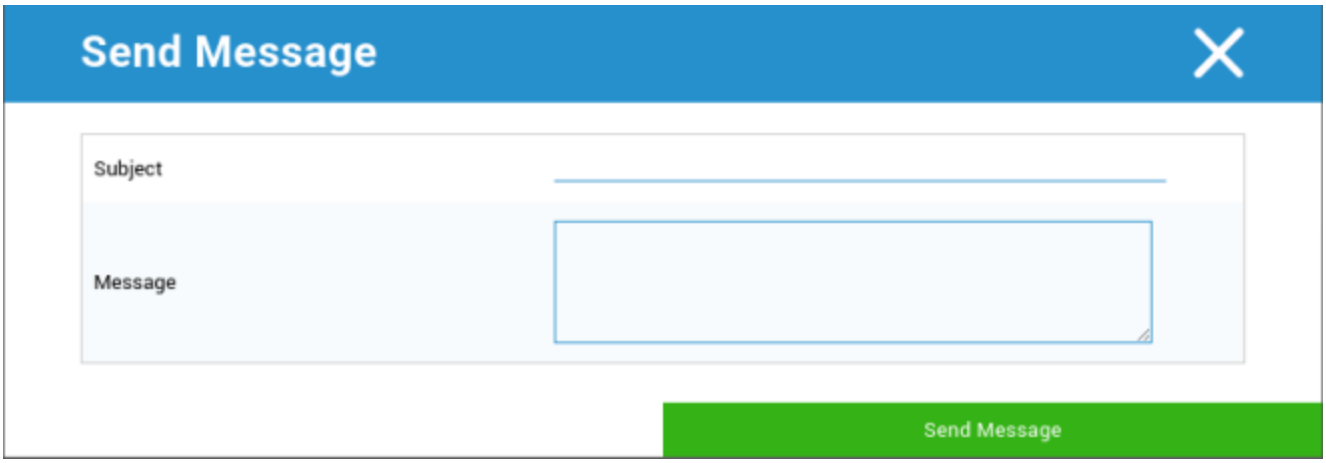
지우기 및 잠금(기기 수준에서만)

'삭제 및 잠금'에서 다음 세 가지 작업을 수행할 수 있습니다:

전체 삭제	장치가 공장 설정으로 복원됩니다(회사 및 개인 데이터는 삭제됨). 향상된 업무용 프로필에서만 작동합니다.
엔터프라이즈 삭제	최종 사용자 기기에서 기업 데이터만 제거됩니다(앱텍에서 제공한 모든 앱, 데이터 등).
잠금 화면	화면 잠금이 활성화되어 있으면 기기 비밀번호/PIN으로 기기 잠금을 해제하는 것으로 충분합니다.

메시지(디바이스 수준에서만)

여기에서 제목과 메시지를 입력하고 최종 사용자 디바이스로 보낼 수 있습니다.



보안 구성

장치 암호

'비밀번호'에서 디바이스 비밀번호를 지정할 수 있으며, 다음과 같은 설정 옵션을 사용할 수 있습니다.

최소 비밀번호 길이	비밀번호에 포함되어야 하는 최소 기호 수를 설정합니다.	
비밀번호 품질	지정되지 않음	이 정책에는 비밀번호에 대한 요구 사항이 없습니다.
	생체 인식 약	이 정책은 보안 수준이 낮은 생체 인식 기술을 허용합니다. 이는 개인의 신원을 3자리 비밀번호 정도로 인식할 수 있는 기술을 의미합니다(오탐지 확률은 1,000분의 1 미만).
	무언가	이 정책은 일종의 비밀번호나 패턴을 설정하도록 요구하지만 특정 규칙을 강제하지는 않습니다.
	알파벳	사용자는 알파벳(또는 기타 기호) 이상의 문자가 포함된 비밀번호를 입력해야 합니다.
	영숫자	사용자는 숫자와 알파벳(또는 기타 기호) 문자를 모두 포함한 비밀번호를 입력해야 합니다.
	복잡한	사용자는 기본적으로 문자, 숫자 및 특수 기호가 포함된 비밀번호를 입력해야 합니다. 이 비밀번호 품질을 사용하면 최소 대문자 등 다양한 문자 집합을 포함하도록 비밀번호를 제한할 수 있습니다.
최소 비밀번호 길이	비밀번호에 필요한 글자 수를 설정합니다. 예를 들어 PIN 또는 비밀번호는 6자 이상으로 설정할 수 있습니다.	
비밀번호에 필요한 최소 숫자 자릿수	비밀번호에 필요한 최소 숫자 자릿수	
비밀번호에 필요한 최소 소문자	비밀번호에 필요한 최소 소문자	
비밀번호에 필요한 최소 대문자	비밀번호에 필요한 최소 대문자	
비밀번호에 필요한 최소 문자 이외의 문자	비밀번호에 필요한 최소 문자 이외의 문자	

비밀번호에 필요한 최소 기호	비밀번호에 필요한 최소 기호

최대 비활성 시간 잠금	시간 잠금까지 최대 사용자 비활성 상태
비밀번호 만료 시간 초과	비밀번호가 만료되고 새 비밀번호를 발급해야 하는 시간 간격을 설정합니다.
비밀번호 기록 제한	허용되지 않는 이전에 사용한 비밀번호의 개수
최대 실패한 비밀번호 시도 횟수	전체 장치 초기화가 수행되기 전에 비밀번호를 잘못 입력할 수 있는 빈도를 설정합니다.
생체 인증 허용	지문 또는 홍채 스캔을 통해 인증할 수 있습니다. 삼성 KNOX 2.1 이상에서만 사용 가능

컨테이너 암호

"비밀번호"에서 컨테이너 비밀번호를 지정할 수 있으며, 다음 설정 옵션(
)을 사용할 수 있습니다.

최소 비밀번호 길이	비밀번호에 포함되어야 하는 최소 기호 수를 설정합니다.	
비밀번호 품질	지정되지 않음	이 정책에는 비밀번호에 대한 요구 사항이 없습니다.
	생체 인식 약	이 정책은 보안 수준이 낮은 생체 인식 기술을 허용합니다. 이는 개인의 신원을 3자리 비밀번호 정도로 인식할 수 있는 기술을 의미합니다(오탐지 확률은 1,000분의 1 미만).
	무언가	이 정책은 일종의 비밀번호나 패턴을 설정하도록 요구하지만 특정 규칙을 강제하지는 않습니다.
	알파벳	사용자는 알파벳(또는 기타 기호) 이상의 문자가 포함된 비밀번호를 입력해야 합니다.
	영숫자	사용자는 숫자와 알파벳(또는 기타 기호) 문자를 모두 포함한 비밀번호를 입력해야 합니다.
	복잡한	사용자는 기본적으로 문자, 숫자 및 특수 기호가 포함된 비밀번호를 입력해야 합니다. 이 비밀번호 품질을 사용하면 최소 대문자 등 다양한 문자 집합을 포함하도록 비밀번호를 제한할 수 있습니다.
최소 비밀번호 길이	비밀번호에 필요한 글자 수를 설정합니다. 예를 들어 PIN 또는 비밀번호는 6자 이상으로 설정할 수 있습니다.	
비밀번호에 필요한 최소 숫자 자릿수	비밀번호에 필요한 최소 숫자 자릿수	
비밀번호에 필요한 최소 소문자	비밀번호에 필요한 최소 소문자	
비밀번호에 필요한 최소 대문자	비밀번호에 필요한 최소 대문자	
비밀번호에 필요한 최소 문자 이외의 문자	비밀번호에 필요한 최소 문자 이외의 문자	
비밀번호에 필요한 최소 기호	비밀번호에 필요한 최소 기호	

최대 비활성 시간 잠금	시간 잠금까지 최대 사용자 비활성 상태
비밀번호 만료 시간 초과	비밀번호가 만료되고 새 비밀번호를 발급해야 하는 시간 간격을 설정합니다.
비밀번호 기록 제한	허용되지 않는 이전에 사용한 비밀번호의 개수
최대 실패한 비밀번호 시도 횟수	전체 장치 초기화가 수행되기 전에 비밀번호를 잘못 입력할 수 있는 빈도를 설정합니다.

안티바이러스

자동 스캔	주기적인 자동 스캔 사용
스캔 간격	검사 간격(빠른/전체)
완전 자동 스캔	완전 자동 스캔 사용
자동 업데이트	자동 업데이트 사용
업데이트 확인 간격	앱 및 데이터베이스의 업데이트 주기(바이러스/손상된 코드)
앱 보호	자동 앱 스캔 사용
SD 카드 보호	SD 카드 자동 스캔 활성화
Wi-Fi 전용 업데이트	이 기능을 활성화하면 장치가 Wi-Fi 네트워크에 성공적으로 연결된 경우에만 업데이트가 적용됩니다.

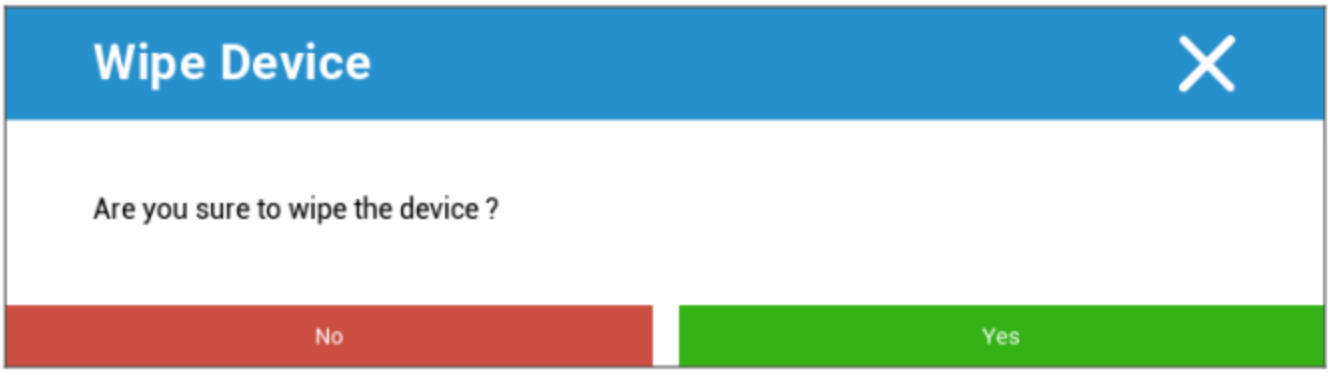
수명 종료(디바이스 수준에서만)

지우기(디바이스 수준에서만)

'초기화'에서 장치를 공장 설정으로 복원할 수 있습니다(향상된 작업 프로필에서만).

여기서 기업 데이터는 물론 개인 데이터도 최종 사용자 장치에서 삭제됩니다.

'빼기 기호'를 클릭하면 다음과 같은 메시지가 표시됩니다:



"예"를 선택하면 지우기를 수행할 수 있습니다.

"삭제 보고서" 아래에 다음 항목이 표시될 수 있습니다.

지운 사람	삭제한 사람에 대한 기록
날짜	날짜
상태	상태(예: 초기화가 성공적으로 수행된 경우)

제한 설정

제한 사항

여기에서 다양한 항목을 제한하고 차단할 수 있습니다.

규정 준수 시행	모드 프롬프트 사용자 - 사용자에게 필요한 작업을 수행하라는 메시지가 표시됩니다. 모드 잠금 컨테이너 - 모든 요구 사항이 충족될 때까지 모든 앱 숨기기
런타임 권한 정책	사용자에게 새 권한 요청에 대한 메시지 표시 항상 새로운 새 권한 요청을 허용하세요. 항상 새로운 권한 요청을 거부하세요. 경고: 일부 앱은 권한이 자동으로 설정된 경우 권한을 인식하는 데 문제가 있습니다. 항상 권한을 부여하고 있는데 앱에서 권한이 누락되었다는 문제가 발생하면 '사용자에게 확인'으로 설정하고 앱을 다시 설치하세요.
보내는 클립보드 허용	컨테이너 내부에서 외부로 복사 및 붙여넣기 허용
발신자 번호 확인 허용	컨테이너의 연락처를 기준으로 수신 전화의 이름을 표시합니다.
연락처 검색 해결 허용	전화를 걸 때 컨테이너 연락처에서 이름을 검색할 수 있습니다.
블루투스 연락처 공유 허용	차량 내 컨테이너 접촉 허용
발신 NFC 빔 허용	컨테이너에 대한 NFC 비활성화
알 수 없는 소스 허용	활성화하면 사용자는 .apk 파일을 설치하여 앱을 사이드로드할 수 있습니다.
USB 디버깅 허용	활성화하면 사용자가 USB 디버깅을 활성화할 수 있습니다.
계정 수정 허용	컨테이너의 계정에 대한 생성, 삭제 및 수정을 허용하지 않습니다. 일부 앱이 정상적으로 작동하려면 계정을 만들거나 수정해야 한다는 점에 유의하세요.

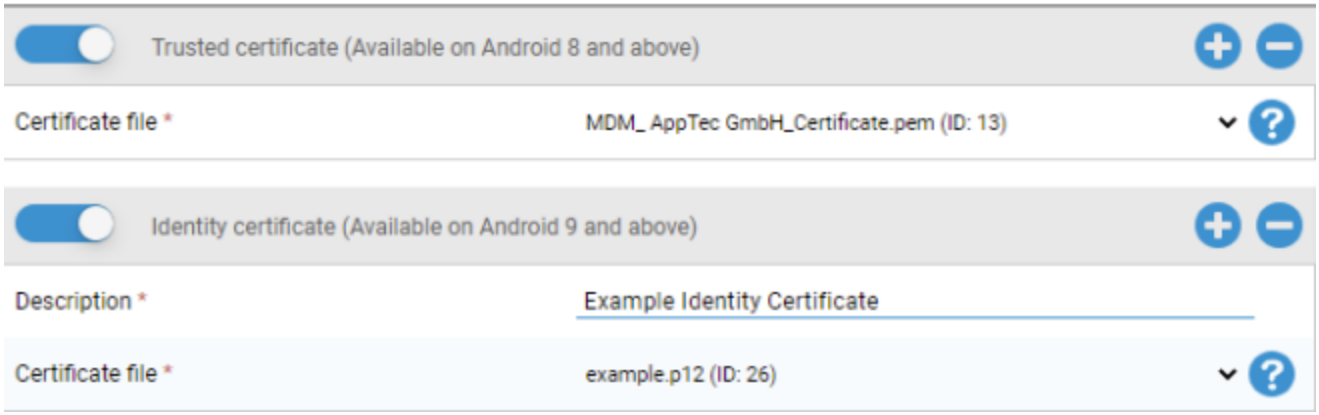
업무 프로필 제한. 향상된 작업 프로필을 사용하는 Android 11 이상 기기에서만 사용 가능	
카메라 허용 안 함	작업 프로필에서 카메라가 허용되지 않는지 여부를 지정합니다.

블루투스 허용 안 함	작업 프로필에서 블루투스를 허용할지 여부를 지정합니다.
공장 초기화 보호 활성화	이 기능을 활성화하면 '일반 설정' → 'Android 구성' → 'Android 기업' → '공장 초기화 보호'에서 정의한 Google 계정으로 Android의 공장 초기화 보호를 재정의할 수 있습니다. 이 기능을 활성화한 후 기기를 재설정하면 구성된 Google 계정을 제공해야 기기를 다시 설정할 수 있습니다.
OS 업데이트 제어	이 옵션을 활성화하면 업데이트 동작을 자동, 창 열기 또는 연기로 설정할 수 있습니다.
업데이트 정책	자동: 업데이트가 제공되는 즉시 자동으로 설치합니다. 윈도우: 일일 유지 관리 기간 내에 자동으로 설치합니다. 또한 Play 앱이 창 내에서 업데이트되도록 구성합니다. 키오스크 기기에서는 이 방법을 강력히 권장하는데, 이는 영구적으로 포그라운드에 고정된 앱을 Play에서 업데이트할 수 있는 유일한 방법이기 때문입니다. 연기: 자동 설치를 최대 30일까지 연기합니다.

개인 프로필 제한. 향상된 업무용 프로필을 사용하는 Android 11 이상 기기에서만 사용 가능	
카메라 허용 안 함	개인 프로필에서 카메라를 허용할지 여부를 지정합니다.
블루투스 허용 안 함	개인 프로필에서 블루투스를 허용할지 여부를 지정합니다.
알 수 없는 소스 허용	활성화하면 업무용 프로필 사용자는 .apk 파일을 설치하여 앱을 사이드로드할 수 있습니다.

인증서 관리

여기에서 신뢰할 수 있는 인증서 및 신원 인증서를 장치에 배포할 수 있습니다. 신뢰할 수 있는 인증서를 배포하려면 Android 8 이상이 필요하고, 신원 인증서를 배포하려면 Android 9 이상이 필요합니다.



"+"를 사용하여 여러 개의 인증서를 추가할 수 있습니다.

신뢰할 수 있는 인증서는 PEM 형식이어야 합니다.

ID 인증서는 PKCS12 형식이어야 합니다.

연결 관리

Wi-Fi

이 설정의 경우 내부 Access
포인트에 액세스하기 위해 최종 사용자 디바이스의 사전 구성을 수행합니다.

서비스 집합 식별자(SSID)	연결할 네트워크의 SSID
숨겨진 네트워크	AP가 SSID를 브로드캐스트하지 않는 경우 활성화합니다.

보안 유형

AP의 보안 유형 설정

WEP

비밀번호	AP의 비밀번호

WPA/WPA2

비밀번호	AP의 비밀번호

802.1x EAP

EAP 방법

PWD	정체성	정체성
	비밀번호	비밀번호

PEAP	2단계 인증 프로토콜	없음	추가 프로토콜 없음
		MSCHAPV2	MSCHAPV2 프로토콜
		GTC	GTC 프로토콜
	CA 인증서	CA 인증서	
	정체성	정체성	
	익명 신원	익명 신원	
	비밀번호	비밀번호	

TTLS	2단계 인증 프로토콜	없음	추가 프로토콜 없음
		PAP	PAP 프로토콜
		MSCHAP	MSCHAP 프로토콜
		MSCHAPV2	MSCHAPV2 프로토콜
		GTC	GTC 프로토콜
	CA 인증서	CA 인증서	
	정체성	정체성	
	익명 신원	익명 신원	
	비밀번호	비밀번호	

TLS	CA 인증서	CA 인증서
	정체성	정체성
	비밀번호	비밀번호

VPN

연결 이름	VPN 연결 이름

VPN 유형

VPN

VPN 클라이언트

앱텍 VPN 클라이언트	
게이트웨이 구성	게이트웨이 VPN 구성을 선택합니다(**일반 설정 > 유니버설 게이트웨이 > VPN 설정** 참조).
항상 켜져 있는 VPN	기본 잠금 사용
앱텍 잠금 활성화	앱텍 잠금 활성화

내장(삼성 디바이스에서만 사용 가능)			
연결 유형	PPTP	서버	서버
		PPTP 암호화 사용	PPTP 암호화 사용
	L2TP / IPSec PSK	서버	서버
		IPSec 사전 공유 키	IPSec 사전 공유 키
		L2TP 비밀 사용	L2TP 비밀 사용
		L2TP 비밀	L2TP 비밀
	IPSec XAuth PSK	서버	서버
		IPSec 식별자	IPSec 식별자
		IPSec 사전 공유 키	IPSec 사전 공유 키
DNS 검색 도메인	DNS 검색 도메인		
전문가 설정	DNS 서버	DNS 서버	
	포워딩 경로	포워딩 경로	

VPN 열기		
서버	서버	
OpenVPN 프로필	OpenVPN 프로필	
OpenVPN 앱	Android용 OpenVPN(권장)	
	OpenVPN 연결	
전문가 설정	DNS 서버	DNS 서버
	포워딩 경로	포워딩 경로

삼성 / 스트롱 스완			
연결 유형	PPTP	서버	서버
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		PPTP 암호화 사용	PPTP 암호화 사용
	L2TP / IPSec PSK	서버	서버
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		L2TP 비밀 사용	L2TP 비밀
	IPSec XAuth PSK	서버	서버
		IPSec 식별자	IPSec 식별자
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
전문가 설정	DNS 서버	DNS 서버	
	포워딩 경로	포워딩 경로	

Cisco Any Connect		
서버	서버	
인증서 모드	장애인	장애인
	자동	자동
전문가 설정	DNS 서버	DNS 서버
	포워딩 경로	포워딩 경로

앱별 VPN

VPN 클라이언트

앱텍 VPN 클라이언트		
게이트웨이 구성	게이트웨이 VPN 구성을 선택합니다(**일반 설정 > 유니버설 게이트웨이 > VPN 설정** 참조).	
VPN 앱	VPN 앱	
항상 켜져 있는 VPN	기본 잠금 사용	항상 켜져 있는 VPN
앱텍 잠금 활성화	앱텍 잠금 활성화	

삼성 / 스트롱 스완			
연결 유형	PPTP	서버	서버
		VPN 앱	VPN 앱
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		PPTP 암호화 사용	PPTP 암호화 사용
	L2TP / IPSec PSK	서버	서버
		VPN 앱	VPN 앱
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
		L2TP 비밀 사용	L2TP 비밀
	IPSec XAuth PSK	서버	서버
		VPN 앱	VPN 앱
		IPSec 식별자	IPSec 식별자
		IPSec 사전 공유 키	IPSec 사전 공유 키
		사용자 이름	사용자 이름
		비밀번호	비밀번호
전문가 설정	DNS 서버	DNS 서버	
	포워딩 경로	포워딩 경로	

제한 사항

여기에서 연결 관리와 관련된 제한 사항을 설정할 수 있습니다.

데이터 로밍 허용	로밍 중 모바일 데이터 허용
강제 데이터 로밍	활성화하면 모바일 데이터 로밍이 영구적으로 활성화됩니다(권장하지 않습니다!). 이 설정은 "데이터 로밍 허용" 설정을 덮어씁니다!
시스템 http 프록시 서버 사용	설정에서 시스템 설정에 의해 제공되는 HTTP 프록시 서버의 사용은 연결된 네트워크(WiFi 또는 APN)에 따라 달라집니다.

PIM 관리

Gmail 교환

정보: 이 구성은 Gmail 앱에 적용됩니다. 따라서 Gmail을 승인하고 설치해야 합니다.

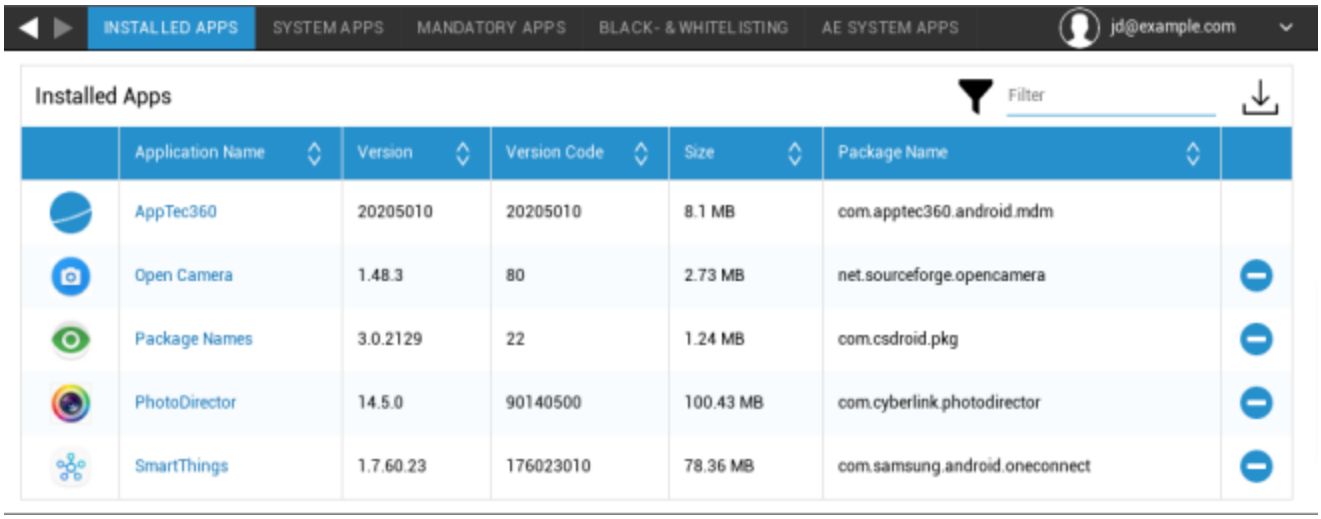
이메일 주소	제공된 사용자의 이메일 주소 자격 증명 작업에 사용할 수 있는 '자리 표시자'는 모든 기기에서 수동으로 변경을 수행하지 않습니다. 클릭 한 번으로 직접 표시할 수 있습니다.
서버 호스트 이름	Exchange 서버의 서버 주소
로그인 이름	각 최종 사용자 디바이스의 로그인 이름, 또한 "여기에 자리 표시자를 참고하세요.
서명	서명을 첨부할 수 있습니다(힌트: 일부 장치에서는 서명에 HTML 형식이 필요합니다).
동기화할 이전 일수	이메일이 다시 동기화되는 시기를 결정하는 일 수
장치 식별자	EAS 장치 ID가 포함된 문자열입니다. 이것은 EAS 프로토콜의 일부이며 특정 환경에서 필요합니다.
SSL(보안 소켓 계층) 사용	SSL 연결 사용
모든 인증서 수락	모든 인증서가 허용됩니다. Exchange Server에서 자체 서명된 인증서를 사용하는 경우 이 옵션을 선택하세요.
관리되지 않는 계정 허용	사용자가 이 관리 구성에 지정된 계정 이외의 모든 Exchange 계정을 추가하거나 제거할 수 있도록 허용합니다. 이 설정을 사용 설정하면 사용자가 다른 Exchange 계정을 Gmail에 추가하는 것을 막을 수 없습니다. 또한 다른 앱과 사용자가 추가한 Exchange 계정 간의 데이터 공유를 제어할 수 없습니다. 이 설정은 사용자가 Gmail에서 둘 이상의 업무용 Exchange 계정을 유지해야 하는 경우에만 사용하도록 설정해야 합니다.
클라이언트 인증서	클라이언트 인증서. 메일 서버에서 이 인증서가 있어야 한다고 예상하는 경우에만 필요합니다.

앱 관리

엔터프라이즈 앱 관리자

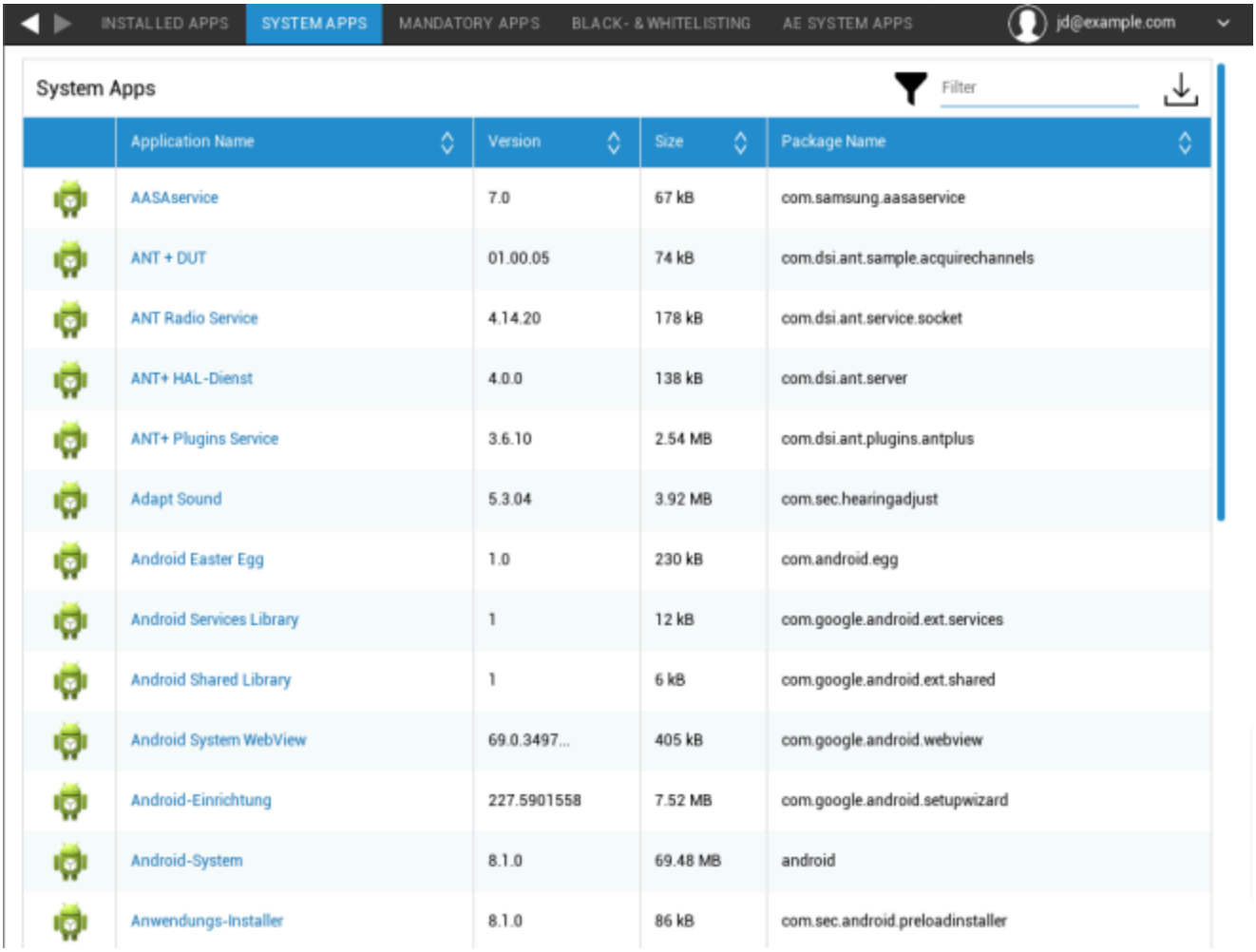
설치된 앱(디바이스 수준에서만)

현재 컨테이너에 설치된 모든 앱이 여기에 표시됩니다.



시스템 앱(디바이스 수준에서만)

'시스템 앱' 아래에는 디바이스 제조업체에서 최종 사용자 디바이스에 이미 설치한 모든 앱과 서비스가 나열됩니다.

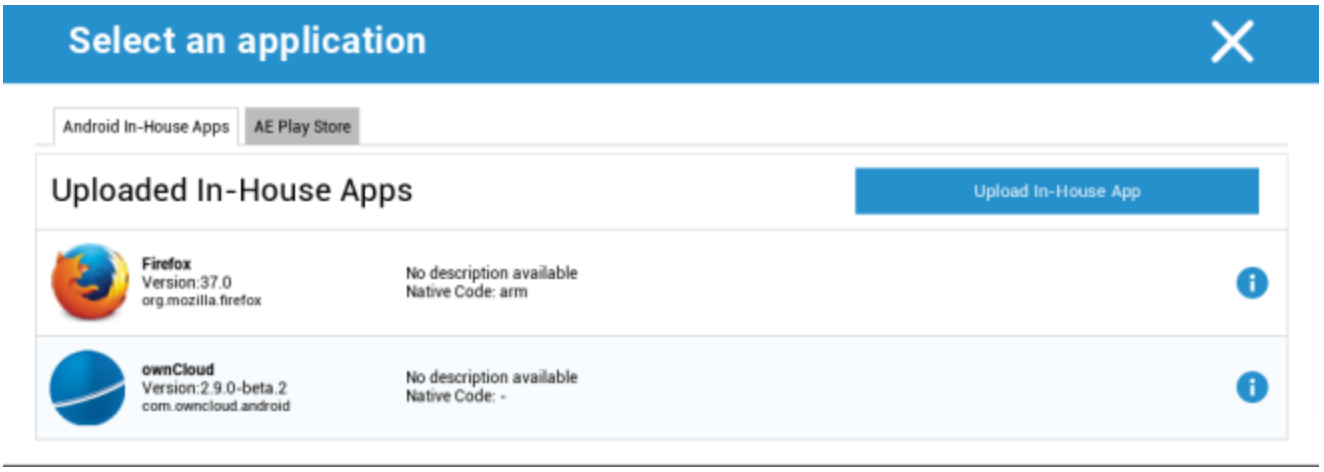


필수 앱

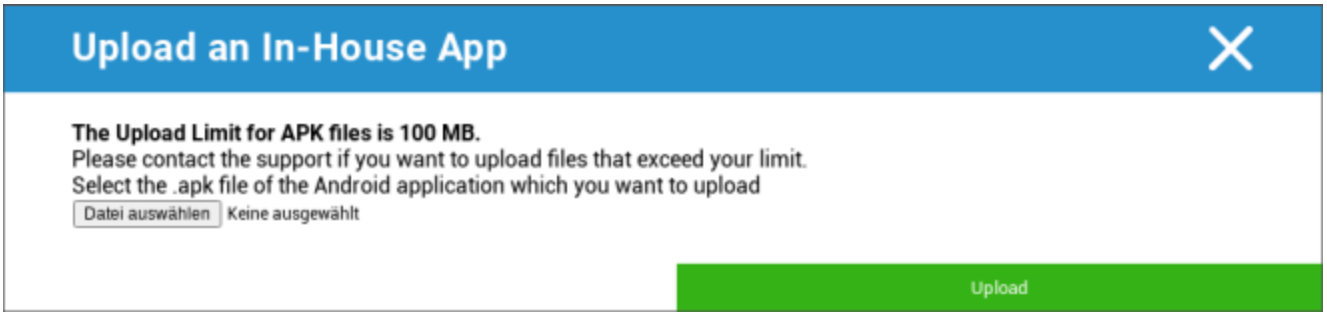
필수 앱에서 필수 앱을 설정할 수 있습니다. 지정된 앱이 사내 앱인 경우 사용자에게 이 앱을 설치하라는 메시지가 계속 표시됩니다. Play 스토어 앱은 자동으로 설치됩니다.

를 통해 필수 앱을 정의할 수 있습니다.

일반 설정에서 업로드한 'Android 사내 앱'의 사내 앱이 될 수 있습니다.

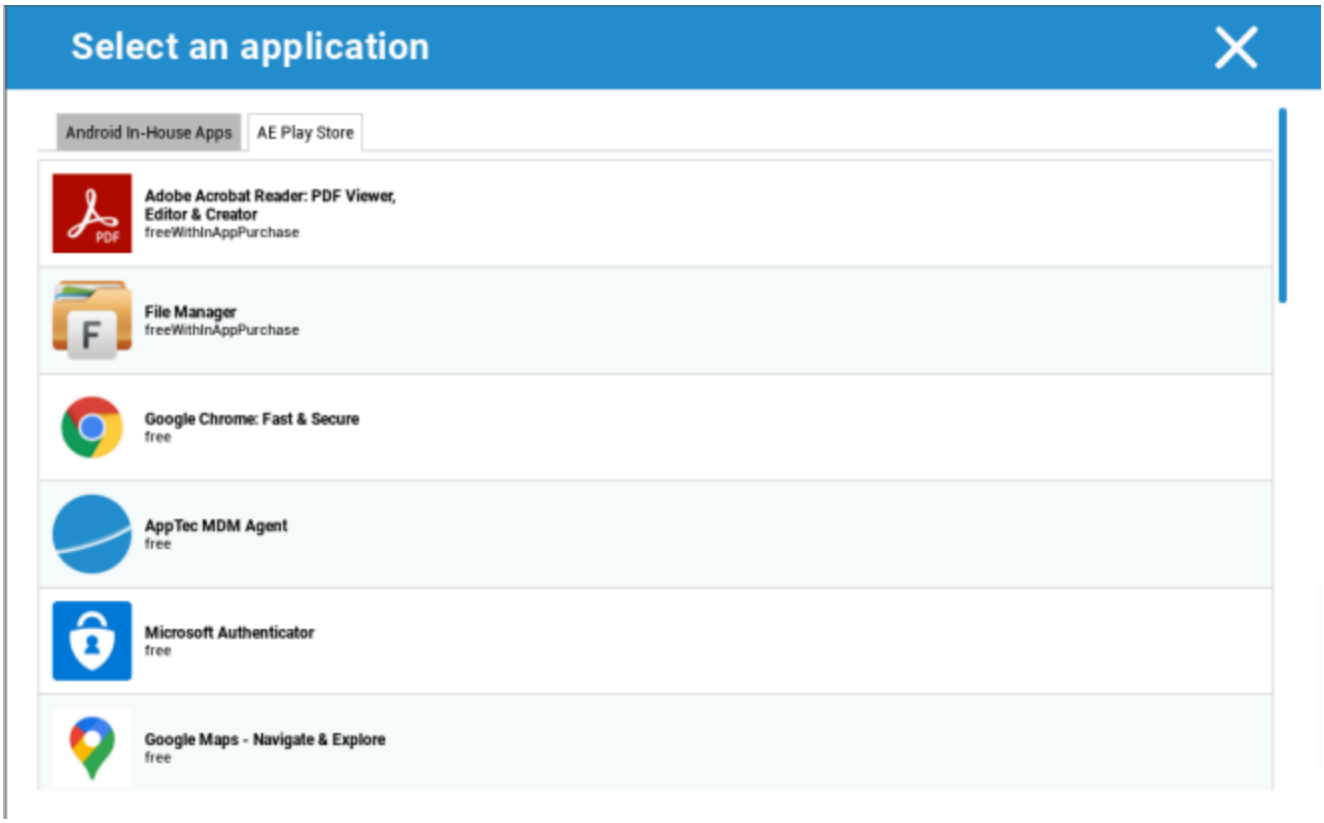


'사내 앱 업로드'를 사용하여 직접 APK 파일을 선택하여 업로드할 수도 있습니다.



사내 앱을 설치하는 경우 '최신 버전 유지'를 활성화할 수 있습니다. 이 기능을 활성화하고 사내 앱 DB에 최신 버전을 정의한 경우 디바이스에서 앱이 업데이트됩니다.

또는 Google Work Play 스토어에서 "AE Play 스토어" 앱을 사용할 수도 있습니다.



이 탭에는 승인된 'AE Play 스토어 앱'만 표시됩니다.

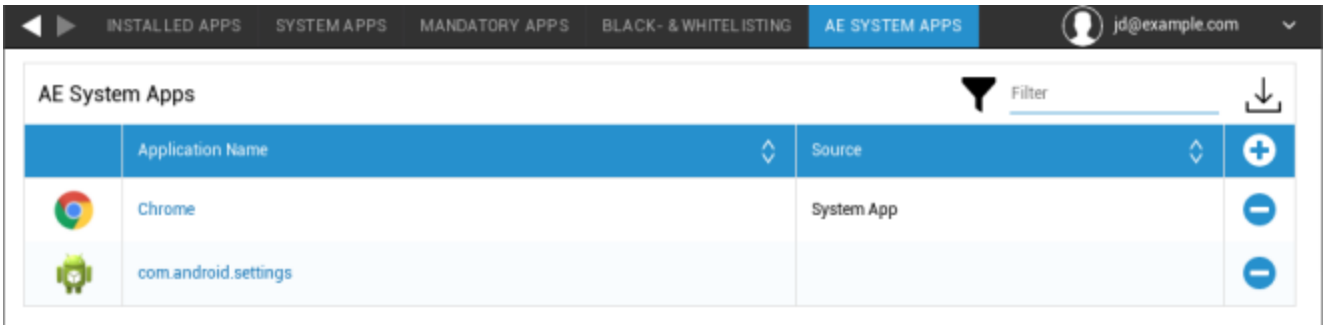
'AE Play 스토어 앱'을 승인하려면 '일반 설정' > '앱 관리' > 'AE Play'로 이동하세요.

Store"를 클릭하고 버튼을 통해 앱을 추가하면 'Play 스토어 앱' 탭으로 리디렉션됩니다(또는 'Play 스토어 앱' 탭으로 바로 이동할 수도 있습니다).

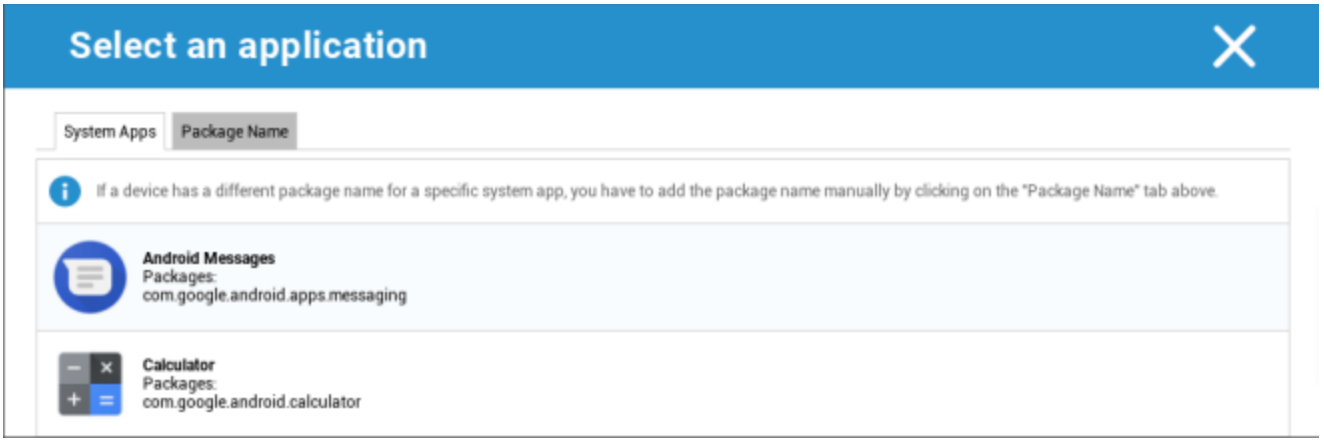
'Play 스토어 앱' 탭에서 앱을 검색할 수 있습니다. 앱을 클릭하면 앱 페이지가 열리고 여기에서 '승인'을 클릭하여 앱을 승인할 수 있습니다.

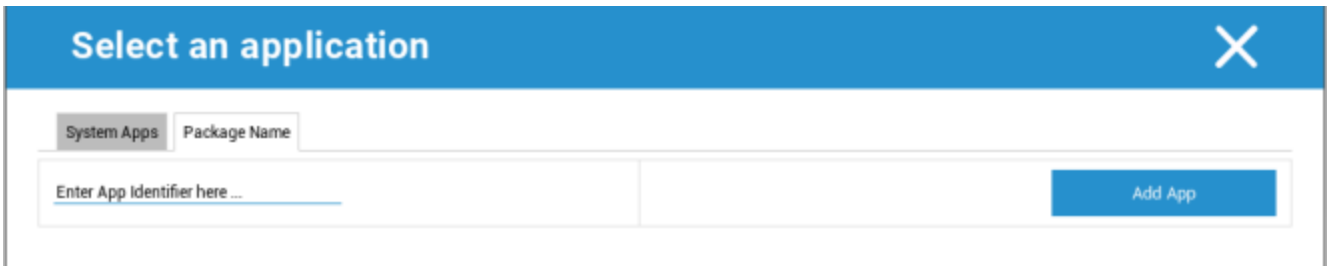
AE 시스템 앱

여기에서 디바이스에서 활성화해야 하는 특정 시스템 앱이 포함된 목록을 정의할 수 있습니다.



버튼을 클릭하면 Google에서 제공하는 가능한 시스템 앱 목록에서 선택하거나 활성화해야 하는 시스템 앱의 패키지 이름을 직접 입력할 수 있습니다.





Google에서 제공하는 목록의 시스템 앱은 시스템 앱이 될 수 있는 앱일 뿐이며, 반드시 기기에서 시스템 앱일 필요는 없다는 점에 유의하세요.

그러나 이 목록은 이미 사전 설치된 앱에만 영향을 미칩니다.

기기에 사전 설치되어 있지 않은 앱을 추가해도 Google에서 제공한 목록에 있는 앱이든 앱의 패키지 이름을 직접 입력한 앱이든 기기에 영향을 미치지 않습니다.

제한 및 설정

앱 관리 설정

여기에서 앱 업데이트와 관련된 디바이스의 동작을 구성할 수 있습니다.

업데이트 확인 빈도	앱텍 클라이언트가 앱 업데이트를 검색할 간격을 지정합니다. 기본값은 24시간입니다.
Wi-Fi 임계값	지정된 크기보다 큰 앱은 Wi-Fi를 통해 다운로드됩니다. 'Wi-Fi 전용'을 선택하면 모든 앱이 Wi-Fi를 통해 다운로드됩니다.

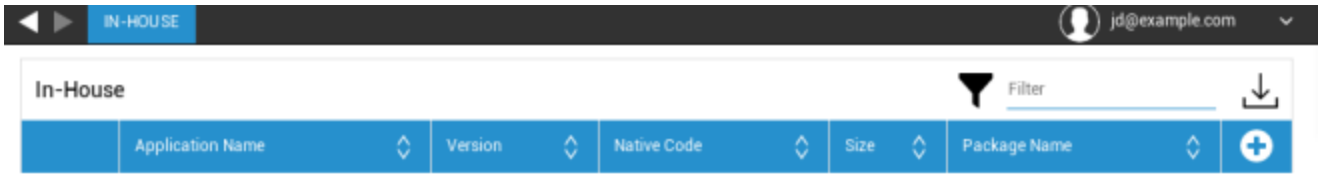
엔터프라이즈 앱 스토어

사내

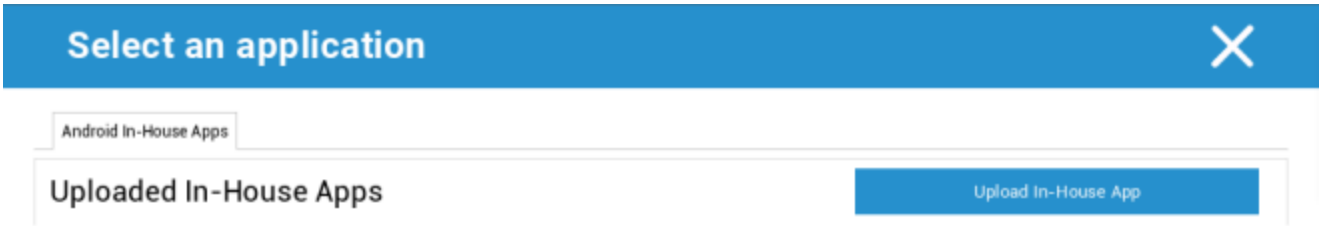
'사내' 항목에서는 내부에서 개발한 앱을 업로드하고 배포할 수 있습니다.

이 기호를 사용하면 사내 앱을 추가로 배포할 수 있습니다.

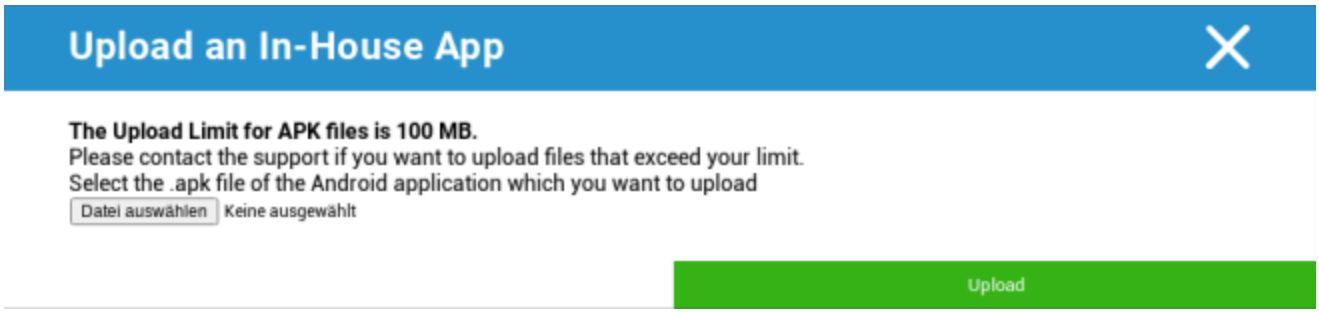
사내 앱을 설치하는 경우 '최신 버전 유지'를 활성화할 수 있습니다. 이 기능을 활성화하고 사내 앱 DB에 최신 버전을 정의한 경우 디바이스에서 앱이 업데이트됩니다.



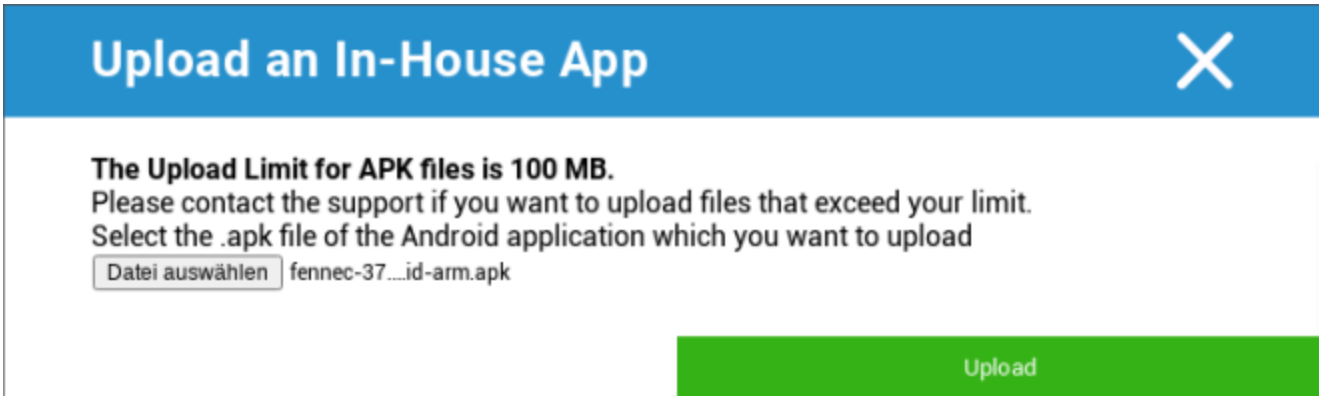
사내 앱을 배포하지 않은 경우 다음과 같은 개요를 받게 됩니다:



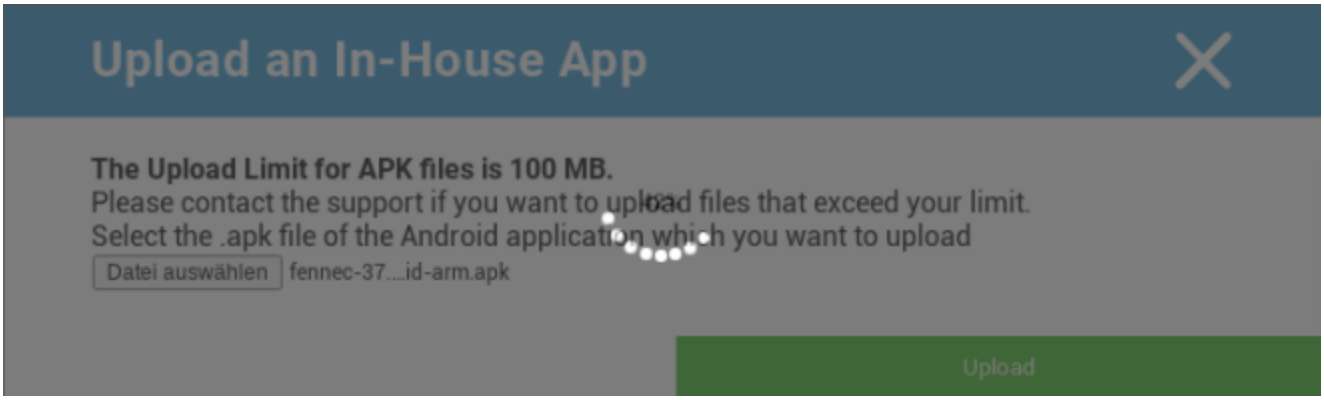
이를 위해 '사내 앱 업로드'를 클릭하면 다음과 같은 개요가 표시됩니다:



이제 "검색..."으로 .apk 파일을 선택한 다음 "업로드"를 클릭합니다.



이제 앱이 업로드되고 원 중앙에 백분율 표시기가 표시되어 이미 업로드된 앱의 양을 확인할 수 있습니다.



사내 앱 업로드가 성공적으로 완료되면 앱 카탈로그에서 업로드된 앱을 찾을 수 있습니다.

이제 사용자는 최종 사용자 디바이스의 AppTec 스토어에서 '사내' 카테고리 아래에서 이 앱을 확인하고 설치할 수 있습니다.

여기에는 구글 플레이스토어 앱이 포함되지 않기 때문에 사용자는 각 최종 사용자 디바이스에 저장된 구글 아이디가 필요하지 않습니다.

기업용 Play 스토어

AE Play 스토어

여기에서 Android 엔터프라이즈 플레이스토어에 앱을 추가할 수 있습니다. 앱을 추가하려면 먼저 AE 관리자 계정으로 앱을 승인해야 한다는 점에 유의하세요.

앱 승인에 대해서는 필수 앱의 지침을 참조하세요.

콘텐츠 관리

콘텐츠 상자

여기에서 콘텐츠 상자를 활성화할 수 있습니다.

"콘텐츠 박스 사용"을 "켜기"로 전환하면 별도의 콘텐츠 박스 앱이 최종 사용자 장치에 자동으로 설치됩니다.

보안 브라우저

여기에서 앱텍 보안 브라우저에 대한 설정을 구성할 수 있습니다.

'보안 브라우저'의 섹션을 '켜기'로 전환하면 별도의 브라우저 앱이 최종 사용자 디바이스에 자동으로 설치됩니다.

비밀번호 필요	사용자가 브라우저에 액세스하기 위해 비밀번호를 설정하고 사용하도록 요구합니다.
최소 필수 비밀번호 길이	비밀번호에 필요한 글자 수를 설정합니다.
필수 비밀번호 품질	필요한 비밀번호 품질 설정
다운로드 제한/열기	
업로드 제한	
화이트리스트 업로드	업로드가 항상 허용되는 URL 목록입니다.
복사 허용	웹 페이지 내의 텍스트 복사, 잘라내기 또는 공유를 허용합니다.
화면 캡처 허용	스크린샷 캡처를 허용합니다.
데이터 정리 빈도	모든 사용자 데이터(기록, 캐시 등)를 자동으로 삭제할 빈도를 선택합니다.
회사 북마크	북마크는 브라우저 북마크의 '회사 북마크' 폴더에 표시됩니다. 사용자가 편집할 수 없습니다.
주소 표시줄 숨기기	
브라우저 내 화이트리스트(유니버설 게이트웨이 제외)	클라이언트 측 URL 화이트리스트를 활성화합니다. • 회사 북마크는 항상 화이트리스트에 등록됩니다. • 100개의 URL만 지원 • 유니버설 게이트웨이를 사용하여 무제한 블랙리스트 및 화이트리스트에 액세스하세요.
화이트리스트 URL	허용된 URL 목록입니다.
게이트웨이 기반 블랙리스트 및 화이트리스트	블랙리스트에는 다음과 같은 요구 사항이 있습니다: • 작동하는 앱텍 유니버설 게이트웨이("일반 설정" → "유니버설 게이트웨이") • 지정된 DNS 서버로 작동하는 VPN 구성("일반 설정" → "범용 게이트웨이" → "VPN 설정")

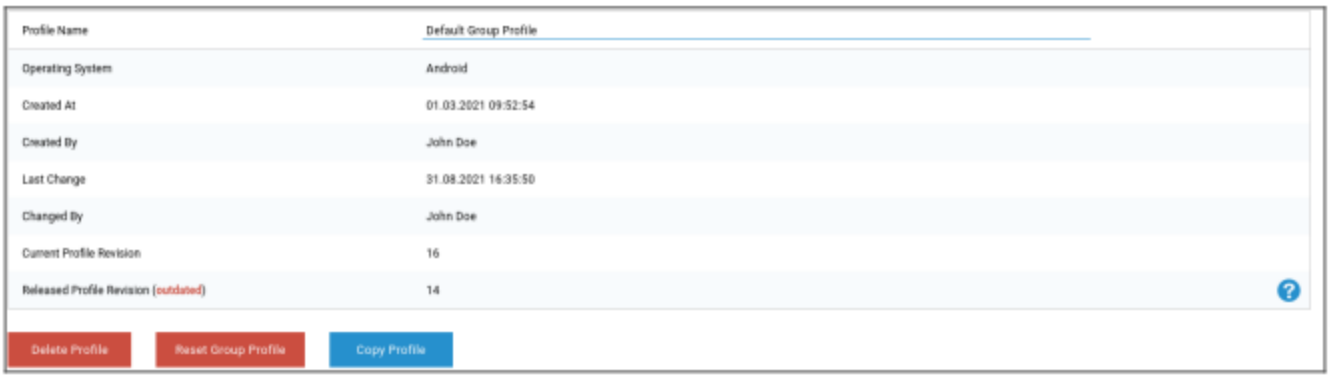
	• 블랙리스트 구성('일반 설정' → '유니버설 게이트웨이' → '도메인 블랙리스트') • 프로필의 유효한 VPN 연결("연결 관리" → "VPN")

Android 구성

일반

그룹 프로필 개요(그룹 수준에서만)

그룹 프로필을 열면 프로필에 대한 간략한 개요를 볼 수 있습니다.



프로필 이름	프로필 이름(여기에서 변경 가능)
운영 체제	프로필의 운영 체제
만든 곳	생성 시간
만든 사람	프로필 작성자
마지막 변경 사항	프로필을 마지막으로 변경한 시간
변경자	마지막으로 변경한 계정
현재 프로필 수정	저장된 프로필 상태 수정
프로필 수정 버전 출시	할당된 프로필 수정본('지금 할당'). 텍스트 뒤에 '(오래된)'이라는 레이블이 표시되면 프로필을 저장했지만 아직 할당하지 않았으므로 디바이스는 여전히 이전 버전을 받게 됩니다.

장치 개요(장치 수준에서만)

디바이스를 사용하는 경우 선택한 디바이스에 대한 개요 요약이 표시되며, 여기에는 다음과 같은 내용이 포함되어 있습니다:

장치 이름	장치 이름
마지막으로 알려진 위치	마지막으로 알려진 GPS 좌표
전화번호	전화번호
필수 앱 지정	할당된 필수 앱의 수
OS 버전	디바이스의 OS 버전
운영 체제	운영 체제(안드로이드/iOS/윈도폰)
일련 번호	장치 일련 번호
디바이스 소유권	기업 또는 개인 디바이스
디바이스 유형	전화 또는 태블릿
루팅	상태, 기기가 루팅되었는지 여부를 나타냅니다.
규정 준수	가이드라인 준수
IP 주소	IP 주소
마지막으로 본	기기가 AppTec에 마지막으로 연결한 시점
마지막 푸시	서버가 디바이스에 푸시를 보낸 시점, 특정 시점
사용자 할당	다른 사용자에게 디바이스를 할당하는 드롭다운

구성 수정(디바이스 수준에서만)

여기에서 장치에 어떤 그룹 프로필이 할당되었는지에 대한 개요를 볼 수 있습니다.

그룹 프로필을 클릭하면 프로필에 바로 액세스하여 설정을 수행할 수 있습니다.

기호를 사용하여 할당된 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

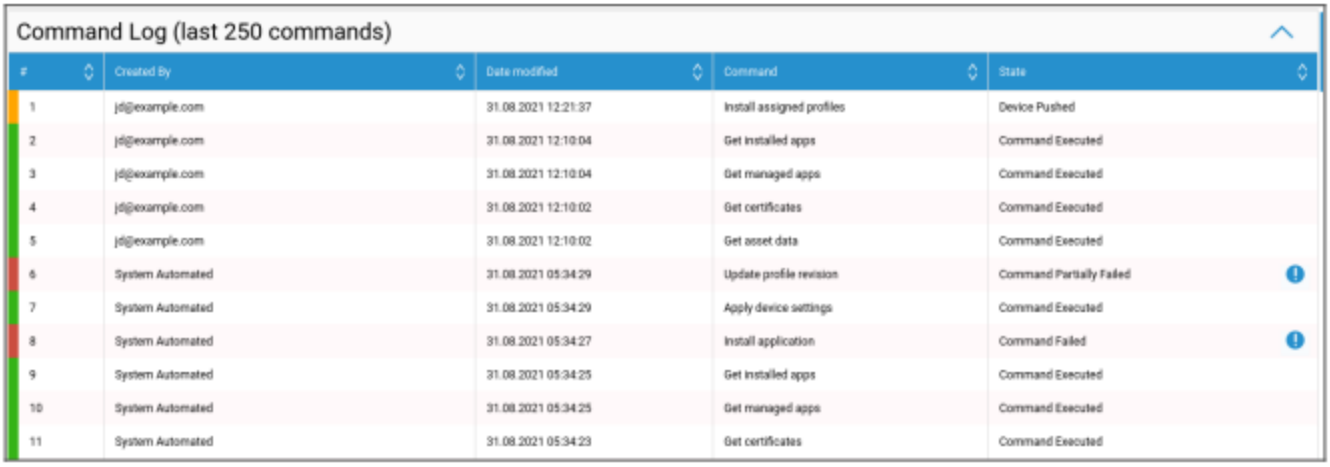
기호를 사용하면 설정이 전혀 없도록 디바이스 프로필을 초기화할 수 있습니다.

"최신 수정본 사용 가능"은 그룹 프로필이 변경되어 저장되었지만 할당되지 않았음을 나타냅니다. 변경 사항을 디바이스에 적용하려면 그룹 수준에서 '지금 할당'을 사용하여 그룹 프로필을 할당해야 합니다.

디바이스 로그(디바이스 수준에서만)

명령 로그

여기에서 디바이스에 대해 어떤 명령이 실행되었는지, 어떤 상태인지 확인할 수 있습니다.



'시스템 자동화'에 의해 생성된 명령은 시스템에 의해 자동으로 생성됩니다.

가능한 명령 상태

푸시된 장치	푸시 요청이 푸시 서비스(예: APNS)로 전송되어 디바이스가 EMM 서버에 다시 연결하도록 지시합니다.
명령 생성	이 명령은 시스템에서 생성되었습니다.
명령 전송	명령은 서버에 연결한 후 디바이스로 전송되었습니다.
명령 실행	명령이 성공적으로 실행되었습니다.
명령 실패	명령이 실패했습니다. *
명령이 부분적으로 실패했습니다.	디바이스 OS에 따라 일부 명령이 함께 그룹화될 수 있습니다. 이 경우 이 명령 그룹의 일부가 실패했습니다. *
명령 실행, 결국 실패	명령이 실행되었지만 실행되지 않았을 수도 있습니다.
명령 재푸시	명령이 사용자에 의해 다시 푸시되었습니다.
폐기됨	명령이 삭제되었습니다. 예를 들어 다른 명령으로 대체되었거나 디바이스가 다시 등록되어 이전 명령이 제거되었기 때문입니다.

*메시지 뒤에 느낌표가 있는 경우 커서로 아이콘을 가리키면 자세한 정보를 확인할 수 있습니다.

디바이스 설정

클라이언트 구성

여기에서 Android 디바이스에서 다음 구성을 수행할 수 있습니다:

장치 관리 비활성화 후 경고 메시지	장치 관리 비활성화 후 경고 메시지 설정
규정 준수 시간 초과	기한이 지나면 장치가 규정을 준수하지 않을 경우 '규정 준수 후 강제 조치'가 수행됩니다. Min. 1분 최대. 24시간
규정 준수 시간 초과 후 시행 조치	디바이스가 규정을 준수하지 않게 되는 즉시 취해야 할 조치입니다. • 아무것도 하지 않음 = 아무런 조치 없음 • 장치 잠금 = 장치 잠금 • 장치 초기화 = 장치가 공장 설정으로 복원됩니다.
데이터 수집 빈도	기기/GPS 정보 수집 빈도
장치 하트비트 주파수	장치가 AppTec360 서버에 연결해야 하는 간격 Min. 1분 최대. 24시간
위치 업데이트 사용	활성화된 경우, 장치는 AppTec360 서버로 위치 업데이트를 보냅니다.
위치 업데이트 시간	장치가 AppTec에 위치 업데이트를 전송하는 시간 간격을 결정합니다.
위치 업데이트에 Google 위치 정확도 사용	활성화하면 Google 위치 정확도(이전의 네트워크 위치)가 위치 업데이트에 사용됩니다(이 설정이 '제한'에서 비활성화되어 있는 경우 이 설정은 아무 영향도 미치지 않습니다).
위치 업데이트를 위해 GPS 위치 사용	활성화하면 GPS가 위치 업데이트에 사용됩니다.
모의 (가짜) 위치 허용	타사 앱을 통한 위치 정보 위조 허용
연결 끊김 조치	일정 횟수의 하트비트 실패 후 수행되는 특정 동작을 설정할 수 있습니다.
정책 적용 모드	AppTec360 클라이언트가 사용자 입력이 필요한 특정 작업을 수행하도록 사용자에게 얼마나 적극적으로 요청할지 정의합니다. 간격(기본값) = 간격을 두고 요청하므로 사용자가 잠시 백그라운드에 놓아둘 수 있습니다.

	경고 없음 = 필요한 상호 작용에 대한 팝업이 표시되지 않습니다. 필요한 작업이 있는지 확인하려면 AppTec360 클라이언트를 수동으로 열어야 합니다. 상시 경고 = 사용자는 필요한 작업만 수행할 수 있습니다. 사용자가 이를 피하려고 하면 AppTec360 클라이언트가 강제로 포그라운드로 이동합니다.
AppTec360 버전 잠금	클라이언트가 자체적으로 업데이트하는 최대 버전인 AppTec360 클라이언트의 버전을 정의할 수 있습니다.

배경 화면

여기에서 사용자 지정 배경 화면을 정의할 수 있습니다.

'색상 지정'을 사용하면 16진수 형식(예: #000000)으로 색상을 정의할 수 있습니다. 16진수 값만 허용됩니다.

'이미지를 배경화면으로 설정'을 사용하면 이미지를 업로드할 수 있습니다. 런처와 OS 버전이 다른 디바이스마다 다르게 작동한다는 점에 유의하세요. 크기와 비율은 디바이스에 따라 다르므로 일반적인 가이드 라인은 없습니다.

파일 형식은 JPG(또는 JPEG) 또는 PNG를 사용합니다.

자산 관리(디바이스 수준에서만)

자산 관리

장치 정보

모델	디바이스 모델 지정
운영 체제	OS
OS 버전	OS 버전
AE 지원	Android Enterprise 지원(컨테이너 및 완전 관리형)
일련 번호	일련 번호
장치 이름	장치 이름
배터리 상태	배터리 상태
여유 / 총 메모리	여유 / 총 메모리
삼성 KNOX	삼성 KNOX API 레벨
SD 카드 사용 가능	SD 카드 사용 가능
SD 카드 에뮬레이션	SD 카드 에뮬레이션
SD 카드 이동식	SD 카드 탈착식
SD 여유 / 총 메모리	SD 무료 / 총 SD 카드 메모리

Wi-Fi

IP 주소	디바이스 IP 주소
WiFi MAC	WiFi MAC 주소

셀룰러

상태	상태(SIM 카드 설치)
전화번호	전화번호
로밍(음성/데이터)	음성/데이터 로밍
로밍 상태	현재 로밍 상태
IP 주소	IP 주소
사업자/이동 통신사	사업자/이동 통신사
셀룰러 기술	셀룰러 기술
IMEI	IMEI 번호
ICCID	SIM 카드의 ID이며, 종종 스마트카드 또는 집적 회로 카드(ICC)이기도 합니다.
IMSI	국제 모바일 가입자 신원(IMSI)은 GSM 및 UMTS 모바일 네트워크에서 네트워크 사용자를 명확하게 식별하는 기능을 제공합니다. IMSI는 최대 15자리로 구성되며 다음과 같은 방식으로 구성됩니다: • 모바일 국가 코드 (MCC), 3자리 • 모바일 네트워크 코드 (MNC), 2자리 또는 3자리 • 모바일 가입자 식별 번호(MSIN), 1~10자리
현재 MCC/MNC	"SIM MCC/MNC" 참조
SIM MCC/MNC	모바일 국가 코드는 ITU에서 E.212 표준에 따라 설정한 국가 식별자입니다. 이는 모바일 네트워크 식별을 위해 모바일 네트워크 코드(MNC)와 함께 작동합니다. SIM 카드의 국가/모바일 네트워크 코드를 의미합니다. 다른 모바일 네트워크로 로밍하는 경우 논리적으로 '현재 MCC/MNC'와 'SIM MCC/MNC'가 달라집니다.

블루투스

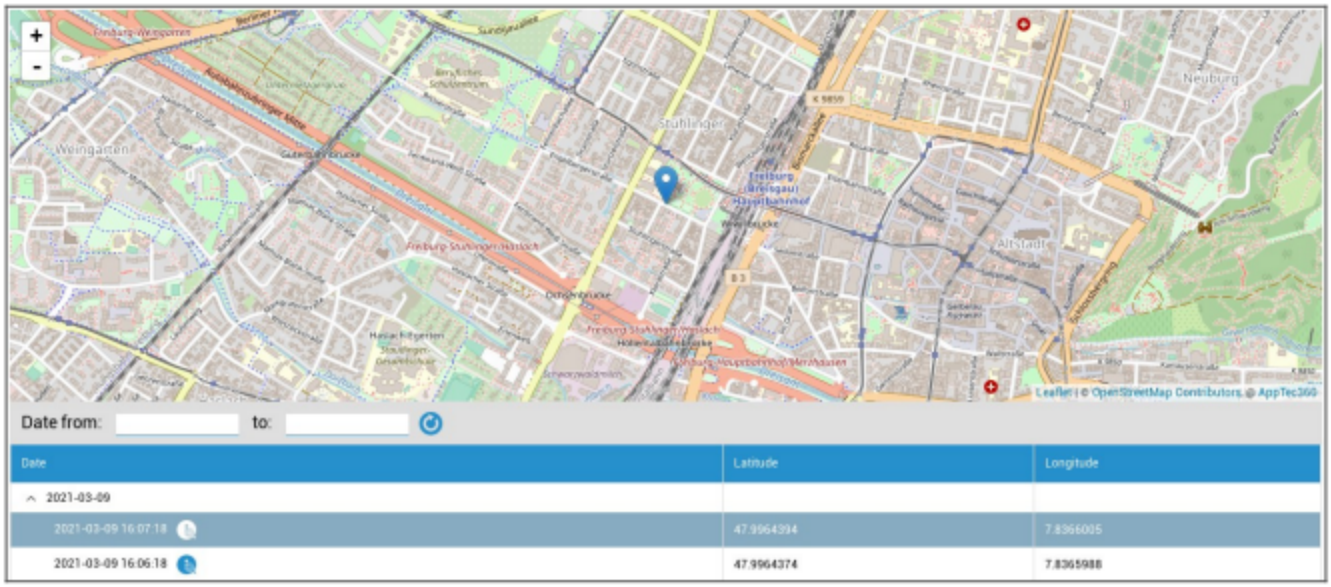
블루투스 MAC	블루투스 MAC 주소

보안 관리

도난 방지(디바이스 수준에서만)

GPS 정보(디바이스 수준에서만)

여기에서 현재/마지막 장치 위치를 설정할 수 있습니다. 현지화는 하나 또는 두 개의 비밀번호로 보호할 수 있습니다(참조: 일반 설정 - 개인정보 - GPS 액세스



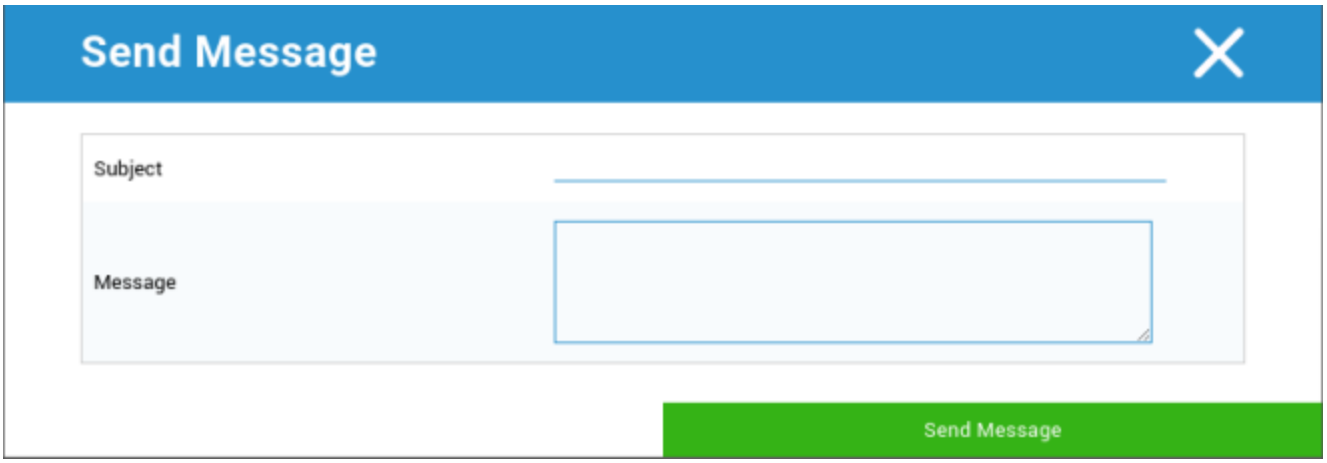
지우기 및 잠금(기기 수준에서만)

'삭제 및 잠금'에서 다음 세 가지 작업을 수행할 수 있습니다:

전체 삭제	장치가 공장 설정으로 복원됩니다(회사 및 개인 데이터가 삭제됨).
엔터프라이즈 삭제	최종 사용자 기기에서 기업 데이터만 제거됩니다(AppTec360에서 제공한 모든 앱, 데이터 등).
잠금 화면	화면 잠금이 활성화되어 있으면 기기 비밀번호/PIN으로 기기 잠금을 해제하는 것으로 충분합니다.

메시지(디바이스 수준에서만)

제목과 메시지를 입력하여 최종 사용자 디바이스로 보낼 수 있습니다. 이 메시지는 AppTec360 클라이언트에 표시됩니다.



보안 구성

암호

'비밀번호'에서 디바이스 비밀번호를 지정할 수 있으며, 다음과 같은 설정 옵션을 사용할 수 있습니다.

최소 비밀번호 길이	비밀번호에 포함되어야 하는 최소 기호 수를 설정합니다.
비밀번호 품질	비밀번호 강도 지정되지 않음 = 지정되지 않음 모든 비밀번호 사용 가능 = 모든 비밀번호 사용 가능 숫자 문자 이상 = 숫자 문자를 포함해야 합니다. 복잡한 문자 이상 = 특수 문자 이상을 포함해야 합니다. 영숫자 이상 = 영숫자 이상을 포함해야 합니다. 알파벳 문자 이상 = 알파벳 문자를 포함해야 합니다.
최대 비활성 시간 잠금	최대 화면 시간 초과. 사용자가 선택할 수 있는 최대값만 구성합니다.
비밀번호에 필요한 최소 소문자	비밀번호에 필요한 최소 소문자
비밀번호에 필요한 최소 대문자	비밀번호에 필요한 최소 대문자
비밀번호에 필요한 최소 문자 이외의 문자	비밀번호에 필요한 최소 문자 이외의 문자
비밀번호에 필요한 최소 숫자 자릿수	비밀번호에 필요한 최소 숫자 자릿수
비밀번호에 필요한 최소 기호	비밀번호에 필요한 최소 기호
비밀번호 만료 시간 초과	비밀번호가 만료되고 새 비밀번호를 발급해야 하는 시간 간격을 설정합니다.
비밀번호 기록 제한	허용되지 않는 이전에 사용한 비밀번호의 개수
최대 실패한 비밀번호 시도 횟수	전체 장치 초기화가 수행되기 전에 비밀번호를 잘못 입력할 수 있는 빈도를 설정합니다.

암호화

이 시점에서 SD 카드 메모리뿐만 아니라 내부 장치 메모리도 암호화할 수 있습니다.

스토리지 암호화 필요	이 설정을 활성화하면 디바이스가 이 기능을 지원하는 한 디바이스 메모리가 암호화됩니다. 디바이스 메모리가 처음 한 번 암호화되면 더 이상 암호화를 해제할 수 없습니다. 마찬가지로 비밀번호 정책도 6개의 영숫자 기호로 자동 전환됩니다.
SD 카드 암호화 필요	이 설정은 삼성 디바이스에만 적용됩니다! 이 설정이 활성화되면 외부 SD 카드를 암호화할 수 있으며 최종 사용자 장치에서만 수동으로 암호화를 해제할 수 있습니다. 마찬가지로 비밀번호 정책도 6개의 영숫자 기호로 자동 전환됩니다.

안티바이러스

안티바이러스를 활성화하면 디바이스에 이카루스가 설치됩니다. 이를 위해서는 일반 설정 → 앱 관리 → 타사 앱에서 입력할 수 있는 별도의 라이선스가 필요하다는 점에 유의하세요.

자동 스캔	Ikarus의 자동 스캔 여부 및 이 스캔을 수행하는 빈도를 정의합니다. '전체 자동 스캔'을 활성화하면 전체 스캔이 수행됩니다. 그렇지 않으면 빠른 스캔이 수행됩니다.
자동 업데이트	바이러스 데이터베이스의 자동 업데이트를 활성화하고 이 작업의 빈도를 설정합니다.
앱 보호	파일만 스캔하는 일반 스캔에 추가하여 앱 스캔을 활성화합니다.
SD 카드 보호	SD 카드 보호를 활성화합니다. 이 기능이 없으면 스캔이 로컬 저장소로 제한됩니다.
Wi-Fi 전용 업데이트	Wi-Fi로 업데이트 제한

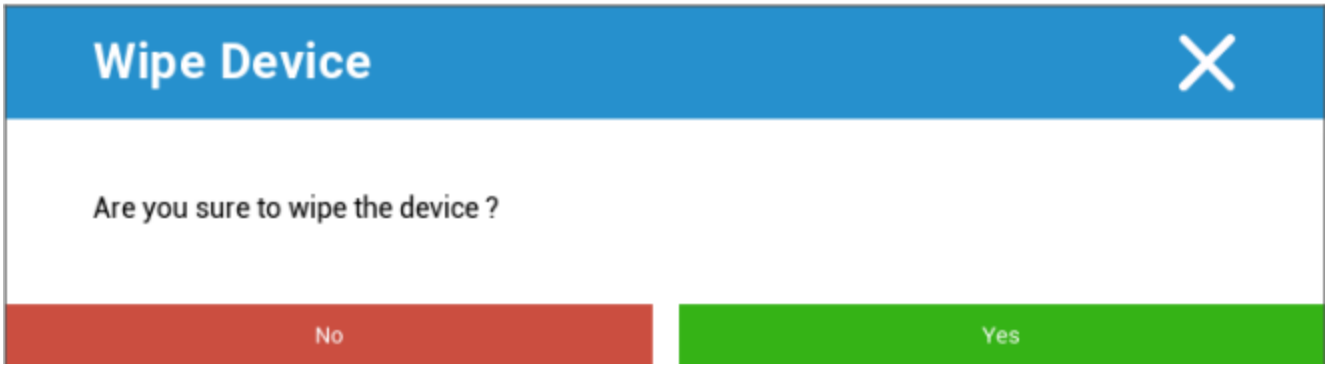
수명 종료(디바이스 수준에서만)

지우기(디바이스 수준에서만)

'초기화'에서 장치를 공장 설정으로 복원할 수 있습니다. 여기에서는 회사 데이터와 개인 데이터가 최종 사용자 장치에서 삭제됩니다.

"마이너스 기호"를 클릭하면 다음과 같은 메시지가 표시됩니다.

SD 카드도 지우시겠습니까?	SD 카드 메모리도 지워집니다.



"예"를 선택하면 지우기를 수행할 수 있습니다.

"삭제 보고서" 아래에 다음 항목이 표시될 수 있습니다.

지운 사람	삭제한 사람에 대한 기록
날짜	날짜
상태	상태(예: 초기화가 성공적으로 수행된 경우)

제한 설정

제한 사항

여기에서 다양한 항목을 제한하고 차단할 수 있습니다.

카메라 사용	카메라 사용 허용
강제 자동 동기화	'동기화' 인터페이스 관련 켜짐 = 동기화가 영구적으로 활성화됨 끄기 = 동기화가 영구적으로 비활성화됨 사용자 선택 = 사용자가 선택한 항목
강제 블루투스	켜짐 = 블루투스가 영구적으로 활성화됨 끄기 = 블루투스가 영구적으로 비활성화됨 사용자 선택 = 사용자가 선택한 항목
강제 GPS	켜짐 = GPS가 영구적으로 활성화됨 끄기 = GPS가 영구적으로 비활성화됨 사용자 선택 = 사용자가 선택한 항목
Google 위치 정확도 강제 적용	켜짐 = 영구적인 인터넷 현지화 끄기 = 인터넷 로캘라이제이션 영구 비활성화 사용자 선택 = 사용자가 선택한 항목

KNOX 1.0 이상 인터페이스가 탑재된 삼성 디바이스의 경우 다음 설정 옵션을 사용할 수 있습니다.

SD 카드 허용	SD 카드 허용
SD 카드 쓰기 허용	SD 카드에 '쓰기' 허용
화면 캡처 허용	화면 캡처 허용
클립보드 허용	클립보드 허용
Google 클라우드의 설정 및 앱 데이터 백업	끄기 = Google 백업 비활성화 켜기 = Google 백업 활성화 사용자 선택 = 사용자가 선택한 항목
USB 디버깅 허용	USB 디버깅 허용(예: 장치 로그(ADB) 생성에 사용됨)
Google 충돌 보고서 허용	앱에서 Google 충돌 보고서 전송 허용
공장 초기화 허용	사용자가 장치를 공장 설정으로 복원할 수 있습니다.
OTA 업그레이드 허용	"무선" 업데이트 허용
USB 호스트 스토리지 허용	활성화된 경우 HD 또는 SD 카드 리더기 형태의 USB 메모리를 연결할 수 있습니다.
USB 미디어 플레이어(MTP, PTP) 허용	USB 미디어 플레이어(MTP, PTP) 허용
마이크 허용	켜기 = 타사 앱에 마이크 허용 끄기 = 타사 앱용 마이크 차단 사용자 선택 = 사용자는 타사 앱이 마이크에 액세스할 수 있는 경우 다음을 선택할 수 있습니다.
NFC(근거리 무선 통신) 허용	NFC 허용
알 수 없는 소스 허용(APK 사이드로드)	활성화하면 앱(APK 파일)의 사이드 로딩이 허용됩니다. 이 설정을 비활성화하면 알 수 없는 출처의 APK 설치를 허용할 때 사용자가 수동으로 활성화해야 합니다.
사용자 생성 허용	여러 사용자를 만들 수 있습니다.

AE 장치 소유자

(디바이스가 Android Enterprise 디바이스 소유자 모드에 있어야 함) 디바이스를 'Android' 디바이스가 아닌 'Android Enterprise' 디바이스로 생성하는 것이 좋습니다.

보안	
공유 위치 허용 안 함	사용자가 위치 공유를 켤 수 없도록 허용할지 여부를 지정합니다.

안전 부팅 허용 안 함	사용자가 장치를 안전 부팅 모드로 재부팅할 수 없도록 허용할지 여부를 지정합니다.
네트워크 재설정 허용 안 함	사용자가 설정에서 네트워크 설정을 재설정할 수 없도록 허용할지 여부를 지정합니다.
공장 초기화 허용 안 함	사용자가 디바이스를 재설정할 수 없도록 허용할지 여부를 지정합니다.
ADB 사용	ADB를 통해 PC에 연결할 수 있습니다.
키가드 비활성화	키가드 비활성화
기기 소유자 잠금 화면 정보	잠금 화면에 표시할 기기 소유자 정보를 설정합니다.
규정 준수 시행	모드 프롬프트 사용자 - 사용자에게 필요한 작업을 수행하라는 메시지가 표시됩니다. 모드 잠금 컨테이너 - 모든 요구 사항이 충족될 때까지 모든 앱 숨기기

앱 관리	
교차 프로필 앱 연결 허용	상위 프로필의 앱이 관리 프로필의 웹 링크를 처리할 수 있도록 허용합니다.
앱 제어 허용 안 함	사용자가 설정 또는 런처에서 애플리케이션을 수정할 수 없도록 허용할지 여부를 지정합니다.
앱 설치 허용 안 함	사용자가 애플리케이션을 설치할 수 없도록 허용할지 여부를 지정합니다.
앱 제거 허용	사용자가 애플리케이션을 제거할 수 없도록 허용할지 여부를 지정합니다.
런타임 권한 정책	앱의 새 권한 요청을 처리하는 방법을 지정합니다.
알 수 없는 소스 허용	활성화하면 사용자는 .apk 파일을 설치하여 앱을 사이드로드할 수 있습니다.

연결성	
모바일 네트워크 구성 허용 안 함	사용자가 모바일 네트워크를 구성할 수 없도록 허용할지 여부를 지정합니다.
테더링 구성 허용 안 함	사용자가 테더링 및 휴대용 핫스팟을 구성할 수 없도록 허용할지 여부를 지정합니다.
VPN 구성 허용 안 함	사용자가 VPN을 구성할 수 없도록 허용할지 여부를 지정합니다.
Wi-Fi 구성 허용 안 함	사용자가 WiFi 액세스 포인트를 변경할 수 없도록 허용할지 여부를 지정합니다.
발신 NFC 빔 허용	사용자가 NFC를 사용하여 앱에서 데이터를 빔으로 전송할 수 없도록 허용할지 여부를 지정합니다.
WiFi 구성 잠금	이 설정은 장치 소유자 앱에서 만든 WiFi 구성을 잠글지 여부(즉, 설정 앱이 아닌 장치 소유자 앱에서만 편집하거나 제거할 수 있도록 할지 여부)를 제어합니다.
데이터 로밍 활성화	데이터 로밍 활성화

블루투스	
블루투스 허용 안 함	장치에서 블루투스를 허용하지 않을지 여부를 지정합니다. Android 8.0이 필요합니다.
블루투스 공유 허용	장치에서 발신 블루투스 공유를 허용할지 여부를 지정합니다. Android 8.0 필요
블루투스 구성 허용 안 함	사용자가 블루투스를 구성할 수 없도록 허용할지 여부를 지정합니다.

계정 관리	
관리되는 프로필 추가 허용 안 함	사용자가 관리되는 프로필을 추가할 수 없도록 허용할지 여부를 지정합니다. Android 8.0 필요
사용자 추가 허용 안 함	사용자가 새 사용자를 추가할 수 없도록 허용할지 여부를 지정합니다.
관리되는 프로필 제거 허용 안 함	프로필 소유자가 아닌 다른 사람이 이 사용자의 관리되는 프로필을 제거할 수 있는지 여부를 지정합니다. Android 8.0 필요
계정 수정 허용	인증자가 프로그래밍 방식으로 추가하지 않는 한 사용자가 계정을 추가 및 제거할 수 없도록 허용할지 여부를 지정합니다.

전화 통신	
발신 전화 허용	사용자가 발신 전화를 걸 수 없도록 지정합니다.
SMS 허용 안 함	사용자가 SMS 메시지를 보내거나 받을 수 없도록 지정합니다.

시스템	
창 생성 허용 안 함	앱 창 이외의 창을 만들지 않도록 지정합니다.
사용자 아이콘 설정 허용 안 함	사용자가 자신의 아이콘을 변경할 수 없도록 허용할지 여부를 지정합니다.
배경화면 설정 허용 안 함	배경화면 설정을 허용하지 않도록 사용자를 제한합니다.
상태 표시줄 비활성화	상태 표시줄을 비활성화하면 알림, 빠른 설정 및 기타 화면 오버레이를 차단하여 일회용 장치에서 벗어날 수 있습니다.
자동 시간 사용	시간을 자동으로 설정합니다.
자동 시간대 사용	표준 시간대를 자동으로 설정합니다.
전원이 연결된 상태에서 계속 켜두기	기기는 전원에 연결되어 있는 동안 활성 상태로 유지됩니다.

스토리지	
앱 인증 비활성화	사용자가 애플리케이션 확인을 비활성화할 수 없도록 허용할지 여부를 지정합니다.
물리적 미디어 마운트 허용	사용자가 물리적 외부 미디어를 마운트할 수 없도록 허용할지 여부를 지정합니다.
백업 서비스 사용	백업 서비스는 디바이스의 모든 백업 및 복원 메커니즘을 관리합니다. 이 옵션을 false로 설정하면 데이터가 백업 또는 복원되지 않습니다. 백업 서비스는 기본적으로 꺼져 있습니다.

	Android 8.0 필요
USB 대용량 저장소 사용	USB 대용량 저장소 사용을 활성화합니다.

키보드	
자동 완성 허용 안 함	사용자가 자동 완성 서비스를 사용할 수 없도록 허용할지 여부를 지정합니다. Android 8.0 필요
프로필 간 복사 및 붙여넣기 허용	이 프로필의 클립보드에 복사된 내용을 관련 프로필에 붙여넣을 수 있는지 여부를 지정합니다.

사운드	
볼륨 조정 허용 안 함	사용자가 마스터 볼륨을 조정할 수 없도록 허용할지 여부를 지정합니다.
마이크 음소거 해제 허용	사용자가 마이크 볼륨을 조정할 수 없도록 허용할지 여부를 지정합니다.
장치 음소거	디바이스 음소거.

시스템 업데이트 정책	
OS 업데이트 제어	이 옵션을 활성화하면 업데이트 동작을 자동, 창 열기 또는 연기로 설정할 수 있습니다.

BYOD 컨테이너

Android 엔터프라이즈

Android 엔터프라이즈

Android 엔터프라이즈 사용	Android Enterprise(AE)를 사용 설정합니다. AE는 Android 5.1 이상부터 지원됩니다.
규정 준수 시행	모드 프롬프트 사용자 - 사용자에게 필요한 작업을 수행하라는 메시지가 표시됩니다. 모드 잠금 컨테이너 - 모든 요구 사항이 충족될 때까지 모든 앱 숨기기
런타임 권한 정책	사용자에게 새 권한 요청에 대한 메시지 표시 항상 새로운 새 권한 요청을 허용하세요. 항상 새로운 권한 요청을 거부하세요. 경고: 일부 앱은 권한이 자동으로 설정된 경우 권한을 인식하는 데 문제가 있습니다. 항상 권한을 부여하고 있는데 앱에서 권한이 누락되었다는 문제가 발생하면 '사용자에게 확인'으로 설정하고 앱을 다시 설치하세요.
보내는 클립보드 허용	컨테이너 내부에서 외부로 복사 및 붙여넣기 허용
발신자 번호 확인 허용	컨테이너의 연락처를 기준으로 수신 전화의 이름을 표시합니다.
연락처 검색 해결 허용	전화를 걸 때 컨테이너 연락처에서 이름을 검색할 수 있습니다.
블루투스 연락처 공유 허용	차량 내 컨테이너 접촉 허용
발신 NFC 빔 허용	컨테이너에 대한 NFC 비활성화
알 수 없는 소스 허용	활성화하면 사용자는 .apk 파일을 설치하여 앱을 사이드로드할 수 있습니다.
USB 디버깅 허용	활성화하면 사용자가 USB 디버깅을 활성화할 수 있습니다.
계정 수정 허용	컨테이너의 계정에 대한 생성, 삭제 및 수정을 허용하지 않습니다. 일부 앱이 정상적으로 작동하려면 계정을 만들거나 수정해야 한다는 점에 유의하세요.

Gmail 교환

컨테이너에서 Gmail을 구성할 수 있습니다. 이 구성을 활성화해도 앱이 자동으로 설치되지 않는다는 점에 유의하세요. 이 앱을 필수 앱으로 추가해야 합니다.

이메일 주소	이메일 주소
서버 호스트 이름	서버 호스트 이름
로그인 이름	로그인 이름
서명	서명
동기화할 이전 일수	동기화할 이전 일수입니다.
장치 식별자	EAS 식별자. 사용 중인 환경에 필요하지 않은 경우 비워둡니다.
SSL(보안 소켓 계층) 사용	SSL 사용을 활성화합니다. 비활성화하면 보안이 저하될 수 있습니다.
모든 인증서 수락	모든 인증서를 허용합니다. 이 옵션을 활성화하면 보안이 저하될 수 있습니다.
관리되지 않는 계정 허용	사용자가 계정을 추가할 수 있습니다.
클라이언트 인증서	Exchange 서버에 필요한 경우 클라이언트 인증서 업로드

AE 시스템 앱

여기에서 Android 엔터프라이즈 컨테이너용 시스템 앱을 활성화할 수 있습니다. 지정된 앱이 시스템 스토리지에 있어야 하며, 그렇지 않으면 아무 일도 일어나지 않습니다.

컨테이너 암호

Android 7.0 이상만 해당

컨테이너에 대한 특정 비밀번호 요구 사항을 설정할 수 있습니다.

최소 비밀번호 길이	비밀번호에 포함되어야 하는 최소 기호 수를 설정합니다.
비밀번호 품질	비밀번호 강도 지정되지 않음 = 지정되지 않음 모든 비밀번호 사용 가능 = 모든 비밀번호 사용 가능 숫자 문자 이상 = 숫자 문자를 포함해야 합니다. 복잡한 문자 이상 = 특수 문자 이상을 포함해야 합니다. 영숫자 이상 = 영숫자 이상을 포함해야 합니다. 알파벳 문자 이상 = 알파벳 문자를 포함해야 합니다.
최대 비활성 시간 잠금	컨테이너가 잠길 때까지 최대 시간. 사용자가 선택할 수 있는 최대값만 구성합니다.
비밀번호에 필요한 최소 소문자	비밀번호에 필요한 최소 소문자
비밀번호에 필요한 최소 대문자	비밀번호에 필요한 최소 대문자
비밀번호에 필요한 최소 문자 이외의 문자	비밀번호에 필요한 최소 문자 이외의 문자
비밀번호에 필요한 최소 숫자 자릿수	비밀번호에 필요한 최소 숫자 자릿수
비밀번호에 필요한 최소 기호	비밀번호에 필요한 최소 기호
비밀번호 만료 시간 초과	비밀번호가 만료되고 새 비밀번호를 발급해야 하는 시간 간격을 설정합니다.
비밀번호 기록 제한	허용되지 않는 이전에 사용한 비밀번호의 개수
최대 실패한 비밀번호 시도 횟수	컨테이너가 삭제되기 전에 비밀번호를 잘못 입력할 수 있는 빈도를 설정합니다.

삼성 KNOX

활성화

여기에서 삼성 KNOX 컨테이너를 활성화할 수 있습니다. Android 10 이상에서는 더 이상 삼성에서 지원되지 않는다는 점에 유의하세요. Android 10 이상에서 Android Enterprise 컨테이너 사용

Knox 암호

디바이스 비밀번호 설정과 관련된 가이드라인을 설정합니다.

최소 비밀번호 길이	비밀번호에 포함되어야 하는 기호 수를 설정합니다.
비밀번호 품질	비밀번호 강도 모든 비밀번호 사용 가능 = 모든 비밀번호 사용 가능 숫자 문자 이상 = 최소 숫자 문자가 있어야 합니다.

	최소 복합 문자 = 최소 특수 문자가 있어야 합니다. 영숫자 이상 = 최소 영숫자 문자가 있어야 합니다. 최소 알파벳 문자 = 최소 알파벳 문자가 있어야 합니다.
최소한의 복잡한 문자 필요	최소한의 복잡한 문자가 있어야 합니다.
최대 비활성 시간 초과	키보드 잠금 전 최대 사용자 비활성 시간 제한
지문 인증 허용	지문 인증 허용
홍채 인증 허용	홍채 인식 인증 허용
최대 비밀번호 사용 기간	비밀번호가 만료되고 새 비밀번호를 발급해야 하는 시간 이후를 설정합니다.
저장된 비밀번호 기록	허용되지 않는 이전 비밀번호 수
최대 실패한 비밀번호 시도 횟수	전체 장치 삭제가 수행되기 전에 비밀번호가 잘못 제출될 수 있는 빈도를 설정합니다.

Knox 보안

특정 장치 기능 제한

카메라 사용	카메라 사용 허용
삼성 KNOX 허용 App Store	삼성 KNOX 앱 스토어 사용 허용
Google Play 서비스 허용	Google Play 서비스 허용
브라우저 허용	기본 브라우저 사용 허용
스크린샷 허용	스크린샷 생성 허용
연락처 가져오기 허용	활성화하면 KNOX 컨테이너에서 장치 연락처의 액세스가 허용됩니다.
연락처 내보내기 허용	활성화하면 장치에서 KNOX 연락처에 대한 액세스가 허용됩니다.
캘린더 가져오기 허용	활성화하면 KNOX 컨테이너에서 장치 캘린더에 대한 액세스가 허용됩니다.
캘린더 내보내기 허용	활성화하면 장치에서 KNOX 캘린더에 대한 액세스가 허용됩니다.
비보안 키패드 허용	비보안 키패드 사용 허용
파일 가져오기 사용	KNOX 컨테이너로 파일 가져오기 활성화하기
파일 내보내기 사용	KNOX 컨테이너에서 파일 내보내기 활성화하기

Knox Exchange

여기에서 KNOX 컨테이너에 대한 교환 프로필을 구성할 수 있습니다.

이메일 주소	제공된 사용자의 이메일 주소 자격 증명 작업에 사용할 수 있는 '자리 표시자'는 모든 기기에서 수동으로 변경을 수행하지 않습니다. **자리 표시자 표시** 를 클릭하면 **자리** 표시자를 직접 표시할 수 있습니다.
서버 호스트 이름	Exchange 서버의 서버 주소
로그인 이름	각 최종 사용자 디바이스의 로그인 이름, 여기에 "자리 표시자"도 참고하세요.
도메인	도메인 주소
비밀번호(디바이스 수준에서만)	선택적으로 개별 장치에 비밀번호를 제공할 수 있으며, 비밀번호가 비어 있는 경우 사용자에게 Exchange 비밀번호를 입력하라는 메시지가 표시됩니다.
동기화할 이전 일수	이메일이 다시 동기화되는 시기를 결정하는 일 수
서명	서명을 첨부할 수 있습니다.
기본 계정	이 이메일 계정을 표준 계정으로 설정합니다.
SSL(보안 소켓 계층) 사용	SSL 연결 사용
TLS(전송 계층 보안) 사용	TLS 연결 사용
모든 인증서 수락	모든 인증서가 허용됩니다. Exchange Server에서 자체 서명된 인증서를 사용하는 경우 이 옵션을 선택하세요.

Knox 이메일

이메일 주소	제공된 사용자의 이메일 주소 자격 증명 작업에 사용할 수 있는 '자리 표시자'는 모든 기기에서 수동으로 변경을 수행하지 않습니다. **자리 표시자 표시** 를 클릭하면 **자리** 표시자를 직접 표시할 수 있습니다.
수신 서버 프로토콜	수신 서버 프로토콜 IMAP 또는 POP
수신 서버 주소	수신 서버 주소
수신 서버 포트	수신 서버 포트
수신 서버 로그인/사용자 이름	수신 서버 로그인/사용자 이름
수신 서버 비밀번호	수신 서버 비밀번호
들어오는 서버는 SSL을 사용합니다.	들어오는 서버는 SSL을 사용합니다.
수신 서버는 TLS를 사용합니다.	수신 서버는 TLS를 사용합니다.
수신 서버는 모든 인증서를 수락합니다.	수신 서버는 모든 유형의 인증서를 허용합니다.
발신 서버 프로토콜	발신 서버 프로토콜 SMTP
발신 서버 포트	발신 서버 포트
발신 서버는 추가 자격 증명을 사용합니다.	발신 서버에 대한 추가 자격 증명입니다. 이 값을 "꺼짐"으로 설정하면 수신 서버 설정이 사용됩니다.
발신 서버 로그인/사용자 이름	발신 서버 로그인/사용자 이름
발신 서버 비밀번호	발신 서버 비밀번호
발신 서버는 SSL을 사용합니다.	발신 서버는 SSL을 사용합니다.
발신 서버는 TLS를 사용합니다.	발신 서버는 TLS를 사용합니다.
발신 서버는 모든 인증서를 수락합니다.	발신 서버는 모든 유형의 인증서를 허용합니다.
서명	여기에 서명을 첨부할 수 있습니다.
새 이메일 수신 시 사용자에게 알림	새 이메일 수신 시 사용자에게 알림

Knox 앱

여기에서 최종 사용자 디바이스에 배포할 앱을 설정합니다. 그러면 KNOX 컨테이너에서 사용할 수 있습니다. 앱을 추가하려면 필수 앱 메뉴에서와 같이 진행하세요.

애플리케이션 이름	애플리케이션 이름
필수 이후	앱이 추가된 시점
출처	앱의 소스(Play 스토어 | 인하우스)

기호를 클릭하면 해당 앱을 다시 제거할 수 있습니다.

연결 관리

Wi-Fi

이 설정의 경우, 내부 액세스 포인트에 액세스하기 위해 최종 사용자 디바이스의 사전 구성을 수행합니다.

서비스 집합 식별자(SSID)	연결할 네트워크의 SSID
숨겨진 네트워크	AP가 SSID를 브로드캐스트하지 않는 경우 활성화합니다.
보안 유형	AP의 보안 유형 설정

보안 유형

WEP

비밀번호	AP의 비밀번호

WPA/WPA2

비밀번호	AP의 비밀번호

802.1x EAP

EAP 방법	

PWD	정체성	정체성	
	비밀번호	비밀번호	

PEAP	2단계 인증 프로토콜	없음	추가 프로토콜 없음
		MSCHAPV2	MSCHAPV2 프로토콜
		GTC	GTC 프로토콜
	CA 인증서	CA 인증서	

	정체성	정체성
	익명 신원	익명 신원
	비밀번호	비밀번호

EAP 방법	

TTLS	2단계 인증 프로토콜	없음	추가 프로토콜 없음
		PAP	PAP 프로토콜
		MSCHAP	MSCHAP 프로토콜
		MSCHAPV2	MSCHAPV2 프로토콜
		GTC	GTC 프로토콜
	CA 인증서	CA 인증서	
	정체성	정체성	
	익명 신원	익명 신원	
	비밀번호	비밀번호	

TLS	CA 인증서	CA 인증서
	정체성	정체성
	비밀번호	비밀번호

VPN

연결 유형	**VPN 연결 유형 설정**

VPN 유형으로 "앱별 VPN"을 선택하면 사용 가능한 VPN 클라이언트가 변경됩니다. 앱별 VPN은 VPN을 특정 앱으로 제한하고 특정 앱이 시작되면 자동으로 VPN 연결을 시작합니다.

AppTec360 VPN 클라이언트	앱텍360 VPN 클라이언트를 유니버설 게이트웨이와 함께 사용합니다.
연결 이름	VPN 연결 이름
게이트웨이 구성	유니버설 게이트웨이의 VPN 구성을 선택합니다.
항상 VPN 사용	VPN을 항상 활성화하여 전체 트래픽이 VPN을 통과하도록 합니다.

기본 잠금 사용	장치가 VPN에 연결되어 있지 않을 때 모든 네트워킹을 차단합니다. 제대로 구성하지 않으면 연결이 완전히 끊어질 수 있으므로 주의해서 사용하세요. 안드로이드 7 이상의 안드로이드 엔터프라이즈에만 해당
AppTec360 잠금 활성화	VPN 연결이 시작될 때까지 모든 앱의 사용을 차단합니다.

Cisco AnyConnect	
연결 이름	VPN 연결 이름
서버	서버 주소
인증서 모드	사용 안 함 = 비활성화됨 자동 = 자동

L2TP(KNOX 전용)	삼성 기기에서만 사용 가능
연결 이름	연결 이름
서버	서버 주소
L2TP 비밀 사용	
DNS 검색 도메인	DNS 검색 도메인

연결 유형	**VPN 연결 유형 설정**

PPTP(KNOX 전용)	삼성 기기에서만 사용 가능
연결 이름	VPN 연결 이름
서버	서버 주소
암호화 사용	암호화 사용
DNS 검색 도메인	DNS 검색 도메인

L2TP/IPSec PSK(KNOX 전용)	삼성 기기에서만 사용 가능
연결 이름	VPN 연결 이름
서버	서버 주소
IPSec 사전 공유 키	인증을 위한 사전 공유 키
L2TP 비밀 사용	
L2TP 비밀	
DNS 검색 도메인	DNS 검색 도메인

IPSec XAuth PSK(KNOX 전용)	삼성 기기에서만 사용 가능
연결 이름	VPN 연결 이름
서버	서버 주소
IPSec 식별자	연결의 사용자 이름
IPSec 사전 공유 키	연결 비밀번호
DNS 검색 도메인	DNS 검색 도메인

OpenVPN	
연결 이름	연결 이름

OpenVPN 프로필	.ovpn 파일의 콘텐츠가 복사되는 위치는 다음과 같습니다.
OpenVPN 앱	OpenVPN을 사용하기 위한 두 가지 앱이 있습니다. "Android용 OpenVPN" 앱을 추천합니다. 하지만 대안으로 "OpenVPN Connect" 앱을 사용할 수 있습니다.

제한 사항

여기에서 연결 관리와 관련된 제한 사항을 설정할 수 있습니다.

데이터 로밍 허용	로밍 중 모바일 데이터 허용
강제 데이터 로밍	활성화하면 모바일 데이터 로밍이 영구적으로 활성화됩니다(권장하지 않습니다!). 이 설정은 "데이터 로밍 허용" 설정을 덮어씁니다!
다음 설정은 삼성 KNOX 2.0 이상에서만 사용할 수 있습니다.	
긴급 통화만 허용	긴급 통화만 허용
WiFi 허용	WiFi 허용
WiFi 네트워크 최소 보안 수준	WiFi 네트워크 최소 보안 수준 개방형 = 모든 유형의 WiFi 허용
사용자의 WiFi 네트워크 추가 금지	사용자가 직접 WiFi 네트워크를 추가할 수 없습니다. 이 설정은 '연결 관리'에서 WiFi 프로필을 정의한 경우에만 가능합니다.
SMS 및 MMS 허용	모두 = 모든 SMS 및 MMS 트래픽이 허용됨 수신 SMS만 = 수신 SMS 메시지만 허용됨 발신 SMS만 = 발신 SMS 메시지만 허용됨 없음 = SMS/MMS 트래픽이 허용되지 않음
로밍 중 동기화 허용	로밍 중 동기화 허용 켜짐 = 활성화됨 꺼짐 = 비활성화됨 사용자 선택 = 사용자의 선택
음성 로밍 허용	음성 로밍 허용 켜짐 = 활성화됨 꺼짐 = 비활성화됨 사용자 선택 = 사용자의 선택
시스템 http 프록시 서버 사용	설정에서 시스템 설정에 의해 제공되는 HTTP 프록시 서버의 사용은 연결된 네트워크(WiFi 또는 APN)에 따라 달라집니다.

APN

다음 설정은 삼성 SAFE 2.0 이상에서만 사용할 수 있습니다!

APN 표시 이름	APN 표시 이름	
액세스 포인트 이름	APN의 이름	
발신 서버 프로토콜	설정되지 않음	
	없음	
	PAP	PAP 프로토콜
	CHAP	CHAP 프로토콜
	PAP 또는 CHAP	PAP 또는 CHAP 프로토콜
MCC - 모바일 국가 코드	삽입된 SIM 카드의 MCC를 사용해야 하는 경우 이 입력란을 비워둡니다.	
MNC - 모바일 네트워크 코드	삽입된 SIM 카드의 MCC를 사용해야 하는 경우 이 입력란을 비워둡니다.	
서버 주소	서버 주소	
서버 포트 번호	서버 포트 번호	
서버 프록시 주소	서버 프록시 주소	
MMS 서버 주소	MMS 서버 주소, 표준의 경우 비워 두세요.	
MMS 포트 번호	MMS 포트 번호	
MMS 프록시 주소	MMS 프록시 주소	
사용자 이름	사용자 이름	
비밀번호	비밀번호	
액세스 포인트 유형	허용되는 유형은 다음과 같습니다: "기본", "MMS", "SUPL" 이 필드를 비워두면 "default,supl,mms"가 사용됩니다.	
기본 APN	APN이 선호됩니다.	

블루투스

여기에서 다양한 블루투스 설정을 수행할 수 있습니다.

다음 설정은 삼성 KNOX 1.0 이상에서만 사용할 수 있습니다!

블루투스를 통한 장치 검색 허용	블루투스를 통한 디바이스 검색 허용
블루투스 페어링 허용	블루투스 페어링 허용
블루투스 헤드셋 장치 허용	블루투스 헤드셋 장치 허용
블루투스 핸즈프리 장치 허용	블루투스 핸즈프리 장치 허용
Bluetooth A2DP 장치 허용	장치 간 Bluetooth A2DP 오디오 스트리밍 허용
발신 전화 허용	BT를 통한 발신 통화 허용
블루투스를 통한 데이터 전송 허용	블루투스를 통한 데이터 전송 허용
블루투스 테더링 허용	장치를 모뎀으로 사용할 수 있습니다(블루투스 인터넷 연결).
블루투스를 통해 컴퓨터에 연결 허용	블루투스를 통해 컴퓨터에 연결 허용

PIM 관리

교환

삼성 KNOX 1.0 이상에서만 사용 가능합니다!

이메일 주소	제공된 사용자의 이메일 주소 자격 증명 작업에 사용할 수 있는 '자리 표시자'는 모든 기기에서 수동으로 변경을 수행하지 않습니다. **자리 표시자 표시** 를 클릭하면 **자리** 표시자를 직접 표시할 수 있습니다.
서버 호스트 이름	Exchange 서버의 서버 주소
로그인 이름	각 최종 사용자 디바이스의 로그인 이름, 또한 "여기에 자리 표시자를 참고하세요.
도메인	도메인 주소
비밀번호(디바이스 수준에서만)	선택적으로 개별 장치에 비밀번호를 제공할 수 있으며, 이 비밀번호가 비어 있는 경우 사용자에게 Exchange 비밀번호를 입력하라는 메시지가 표시됩니다.
동기화할 이전 일수	이메일이 다시 동기화되는 시기를 결정하는 일 수
서명	서명을 첨부할 수 있습니다(힌트: 일부 장치에서는 서명에 HTML 형식이 필요합니다).
기본 계정	이 메일 계정을 표준 계정으로 설정합니다.
SSL(보안 소켓 계층) 사용	SSL 연결 사용
TLS(전송 계층 보안) 사용	TLS 연결 사용
모든 인증서 수락	모든 인증서가 허용됩니다. Exchange Server에서 자체 서명된 인증서를 사용하는 경우 이 옵션을 선택하세요.

이메일

여기에서 각 최종 사용자 장치에 IMAP 및 POP 계정을 배포할 수 있습니다.

다음 설정은 삼성 KNOX 1.0 이상에서만 사용할 수 있습니다!		
이메일 주소	제공된 사용자의 이메일 주소 자격 증명 작업에 사용할 수 있는 '자리 표시자'는 모든 기기에서 수동으로 변경을 수행하지 않습니다. **자리 표시자 표시** 를 클릭하면 **자리** 표시자를 직접 표시할 수 있습니다.	
수신 서버 프로토콜	수신 서버 프로토콜	IMAP 또는 POP
수신 서버 주소	수신 서버 주소	
수신 서버 포트	수신 서버 포트	
수신 서버 로그인/사용자 이름	수신 서버 로그인/사용자 이름	
수신 서버 비밀번호(디바이스 수준에서만)	수신 서버 비밀번호(디바이스 수준에서만)	
들어오는 서버는 SSL을 사용합니다.	들어오는 서버는 SSL을 사용합니다.	
수신 서버는 TLS를 사용합니다.	수신 서버는 TLS를 사용합니다.	
수신 서버는 모든 인증서를 수락합니다.	수신 서버는 모든 유형의 인증서를 허용합니다.	
발신 서버 프로토콜	발신 서버 프로토콜	SMTP
발신 서버 포트	발신 서버 포트	
발신 서버는 추가 자격 증명을 사용합니다.	발신 서버에 대한 추가 자격 증명입니다. 이 설정을 "꺼짐"으로 설정하면 수신 서버 설정이 사용됩니다.	
발신 서버 로그인/사용자 이름	발신 서버 로그인/사용자 이름	
발신 서버 비밀번호(디바이스 수준에서만)	발신 서버 비밀번호	
발신 서버는 SSL을 사용합니다.	발신 서버는 SSL을 사용합니다.	
발신 서버는 TLS를 사용합니다.	발신 서버는 TLS를 사용합니다.	
발신 서버는 모든 인증서를 수락합니다.	발신 서버는 모든 유형의 인증서를 허용합니다.	

서명	여기에 서명을 첨부할 수 있습니다(힌트: 일부 장치에서는 서명에 HTML 형식이 필요합니다).
새 이메일 수신 시 사용자에게 알림	새 이메일 수신 시 사용자에게 알림

AE Gmail 교환

정보: 이 구성은 Gmail 앱에 적용됩니다. 따라서 Gmail을 승인하고 설치해야 합니다.

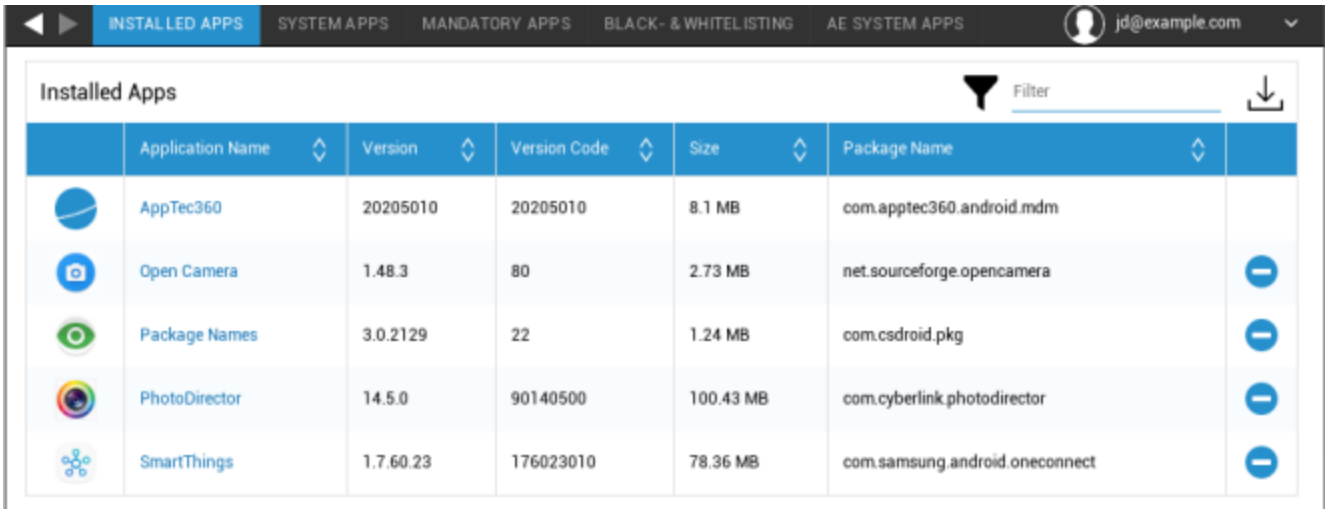
이메일 주소	제공된 사용자의 이메일 주소 자격 증명 작업에 사용할 수 있는 '자리 표시자'는 모든 기기에서 수동으로 변경을 수행하지 않습니다. 자리 표시자 표시를 클릭하면 자리 표시자를 직접 표시할 수 있습니다.
서버 호스트 이름	Exchange 서버의 서버 주소
로그인 이름	각 최종 사용자 디바이스의 로그인 이름, 또한 "여기에 자리 표시자를 참고하세요.
서명	서명을 첨부할 수 있습니다(힌트: 일부 장치에서는 서명에 HTML 형식이 필요합니다).
동기화할 이전 일수	이메일이 다시 동기화되는 시기를 결정하는 일 수
장치 식별자	EAS 식별자. 사용 중인 환경에 필요하지 않은 경우 비워둡니다.
SSL(보안 소켓 계층) 사용	SSL 연결 사용
모든 인증서 수락	모든 인증서가 허용됩니다. Exchange Server에서 자체 서명된 인증서를 사용하는 경우 이 옵션을 선택하세요.
관리되지 않는 계정 허용	사용자가 계정을 추가할 수 있습니다.
클라이언트 인증서	Exchange 서버에 필요한 경우 클라이언트 인증서 업로드

앱 관리

엔터프라이즈 앱 관리자

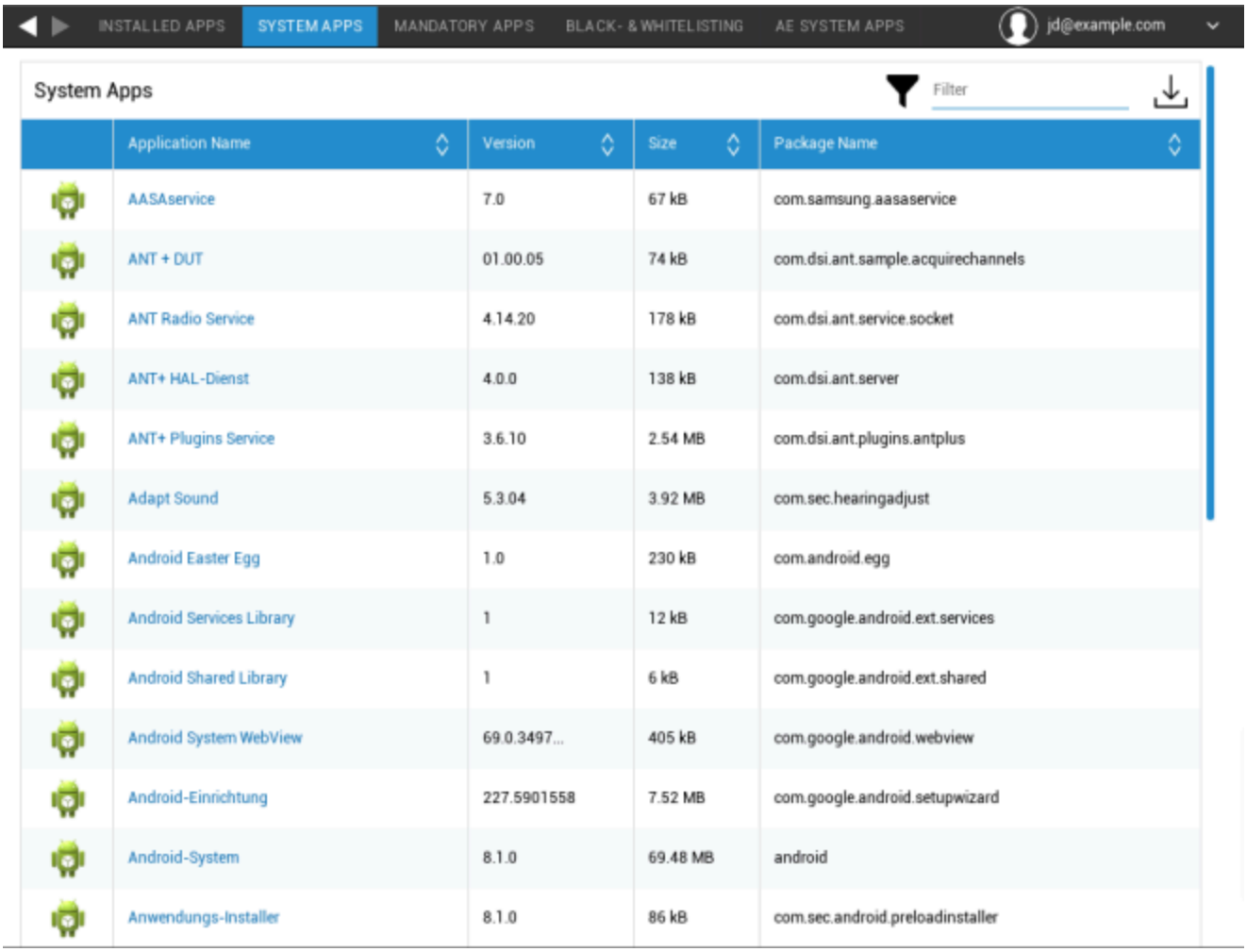
설치된 앱(디바이스 수준에서만)

여기에는 현재 최종 사용자 디바이스에 설치된 모든 앱이 표시됩니다.


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

시스템 앱(디바이스 수준에서만)

'시스템 앱' 아래에 사전 설치된 모든 시스템이 패키지 이름 및 버전과 함께 나열됩니다.



필수 앱

필수 앱에서 디바이스에 설치해야 하는 앱을 정의할 수 있습니다. 구성 및 디바이스에 따라 앱이 자동으로 설치되거나 사용자에게 설치하라는 메시지가 표시됩니다.

간편한 앱 관리를 위해 Android Enterprise를 사용하는 것이 좋습니다.

시나리오는 다음과 같습니다:

일반 Play 스토어 앱

Play스토어 앱 설치에는 항상 사용자 상호 작용이 필요합니다. 또한 기기에서 Google 계정을 구성해야 합니다.

사내 앱 설치

삼성 디바이스에서는 이러한 앱이 자동으로 설치됩니다. 사용자가 설치를 확인해야 하는 컨테이너만 예외입니다.

다른 시나리오에서는 사용자가 앱 설치를 확인해야 합니다.

Android 기업용 Play 스토어 앱

이러한 앱은 항상 사용자 상호작용 없이 자동으로 설치됩니다.

필수 앱을 추가하려면 '+'를 클릭하고 목록에서 원하는 앱을 선택합니다. 기기가 Android Enterprise로 완전 관리형 또는 컨테이너로 구성된 경우 'Google Play 스토어' 탭에서 앱을 설치할 수 없다는 점에 유의하세요.

Android Enterprise를 사용하는 경우 'AE Play 스토어' 섹션에서 앱을 선택합니다. 여기에서 앱을 사용할 수 있도록 설정하려면 일반 설정 → AE Play 스토어 → Play 스토어 앱으로 이동하여 Google Enterprise Play 스토어에서 앱을 확인합니다.

필수 앱을 제거하면 해당 앱도 기기에서 제거됩니다.

필수 앱 목록에서 앱 이름을 클릭하고 '구성' 탭으로 이동하여 앱을 구성할 수 있습니다. 이를 위해서는 Android Enterprise를 사용해야 하며 앱이 이를 지원해야 합니다. 따라서 사용 가능한 옵션은 선택한 앱에 따라 달라집니다.

AE 시스템 앱

여기에서 Android Enterprise 디바이스에 대한 시스템 앱을 활성화할 수 있습니다. 지정된 앱이 시스템 저장소에 있어야 하며, 그렇지 않으면 아무 일도 일어나지 않습니다. 296

제한 및 설정

블랙리스트 및 화이트리스트

여기에서 블랙리스트 또는 화이트리스트를 정의할 수 있습니다. 블랙리스트에 있는 모든 앱이 차단됩니다. 화이트리스트에 없는 모든 앱은 차단됩니다. 블랙리스트가 비어 있으면 아무것도 차단되지 않지만 화이트리스트가 비어 있으면 모든 앱이 차단됩니다*.

**모든 필수 앱과 기업 앱스토어의 앱은 자동으로 화이트리스트에 추가됩니다. 수동으로 추가할 필요가 없습니다.*

'+'를 클릭하면 블랙리스트 또는 화이트리스트에 추가할 앱을 검색하거나 패키지 이름을 직접 입력할 수 있습니다.

시스템 앱 제한

'시스템 앱 제한'에서는 무엇보다도 원하는 대로 사전 설치된 앱과 서비스를 차단할 수 있습니다.

브라우저 비활성화	표준 브라우저 비활성화
캘린더 비활성화	기본 캘린더 비활성화
계산기 비활성화	계산기 비활성화
Chrome 브라우저 비활성화	Chrome 브라우저 비활성화
시계 비활성화	시계 비활성화
연락처 비활성화	연락처 비활성화
다이얼러 비활성화	기본 다이얼러 비활성화
이메일 비활성화	이메일 비활성화
교환 비활성화	Exchange 계정 비활성화
Facebook 비활성화	Facebook 앱 비활성화
갤러리 비활성화	기본 갤러리 앱 비활성화
Gmail 비활성화	Gmail 비활성화
Google 북 비활성화	Google 북 비활성화
Google Play 키오스크 비활성화	Google Play 키오스크 비활성화
Google 지도 비활성화	Google 지도 비활성화
Google 뮤직 비활성화	Google 뮤직 비활성화
Google 동영상 비활성화	Google 동영상 비활성화
Google Play 스토어 비활성화	Google Play 스토어(공용 앱 스토어) 비활성화
Google 플러스 비활성화	Google 플러스 비활성화
Google 검색 비활성화	Google 검색 비활성화
Google 토크/Google 행아웃 비활성화	Google 토크/Google 행아웃 비활성화
음악 플레이어 비활성화	기본 음악 플레이어 앱 비활성화
설정 비활성화	장치 설정 비활성화
Sim 툴킷 비활성화	Sim Toolkit 서비스 비활성화
SMS/MMS 비활성화	SMS/MMS 비활성화
스트리트 뷰 비활성화	스트리트 뷰 서비스 비활성화
유튜브 비활성화	유튜브 비활성화

삼성 앱

'삼성 앱'에서 삼성 디바이스에 대한 추가 설정 및/또는 제한 사항을 정의할 수 있습니다.

올쉐어 플레이 / 삼성 링크 비활성화	올쉐어 플레이 / 삼성 링크 비활성화
ChatON 비활성화	ChatON 비활성화
게임 허브 비활성화	게임 허브 비활성화
그룹 플레이 비활성화	그룹 플레이 비활성화
도움말 사용 안 함	삼성 도움말 비활성화
KNOX 비활성화	삼성 KNOX 컨테이너 비활성화
메모 비활성화	음성 메모 비활성화
내 파일 비활성화	내 파일 비활성화
광학 리더 비활성화	광학 리더 비활성화
폴라리스 오피스 비활성화	폴라리스 오피스 비활성화
리더스 허브 / 삼성 북스 비활성화	리더스 허브 / 삼성 북스 비활성화
S 메모 비활성화	삼성 메모 앱 비활성화
S 번역기 비활성화	삼성 번역기 앱 비활성화
S 음성 비활성화	S 음성 어시스턴트 비활성화
삼성 앱 비활성화	삼성 앱 스토어 비활성화
삼성 허브 비활성화	삼성 엔터테인먼트 스토어 비활성화
비디오 플레이어 비활성화	비디오 플레이어 비활성화
음성 녹음기 비활성화	음성 녹음기 비활성화
WatchON 비활성화	WatchON 사용 안 함(리모컨 시뮬레이션)

화웨이 앱

'Huawei 앱'에서 Huawei 디바이스에 대한 추가 설정 및/또는 제한 사항을 정의할 수 있습니다.

DLNA 비활성화	DLNA 비활성화
앱 설치 관리자 비활성화	앱 설치 관리자 비활성화
파일 관리자 비활성화	파일 관리자 비활성화
백업 관리자 비활성화	백업 관리자 비활성화
시스템 업데이터 비활성화	시스템 업데이터 비활성화
도구 상자 비활성화	도구 상자 비활성화
날씨 비활성화	날씨 비활성화
FM 라디오 비활성화	FM 라디오 비활성화

앱 관리 설정

여기에서 인하우스 앱의 업데이트 동작을 정의할 수 있습니다.

업데이트 확인 빈도는 AppTec360 앱이 사내 앱의 업데이트를 찾는 빈도를 정의합니다. 새 버전이 감지되면 다운로드 및 설치됩니다.

Wi-Fi 임계값은 앱이 구성된 임계값보다 큰 경우 다운로드가 Wi-Fi 연결로 제한되어야 하는지 여부를 정의합니다. 이보다 작거나 임계값을 정의하지 않으면 앱이 Wi-Fi 및 셀룰러 네트워크에서 다운로드됩니다.

엔터프라이즈 앱 스토어

여기에서 앱(Enterprise App Store)을 추가한다고 해서 해당 앱이 디바이스에 자동으로 설치되는 것은 아닙니다. 사용자가 디바이스에서 기업용 앱 스토어를 열고 앱을 수동으로 설치해야 합니다.

기기에 앱을 자동으로 설치하려면 '앱 관리' → '기업 앱 관리자' → '필수 앱'으로 이동하여 원하는 앱을 추가하세요.

이 시점에서 사용자에게 선택적 앱을 배포할 수 있습니다.

Play스토어

"+"를 클릭하여 Play 스토어 앱을 스토어에 추가합니다. Android Enterprise를 사용하는 경우 "앱 관리 엔터프라이즈 플레이 스토어"로 이동하세요. 또한 여기에 정의된 앱을 설치하려면 → 기기에서 Google 계정을 구성해야 한다는 점에 유의하세요.

사내

'사내' 항목에서는 내부에서 개발한 앱을 업로드하고 배포할 수 있습니다.

"+"를 클릭하여 사내 앱을 기업 앱 스토어에 추가하면 사용자가 설치할 수 있습니다. 이 대화 상자에서 새 사내 앱을 업로드할 수도 있습니다.

기업용 Play 스토어

여기(기업용 Play 스토어)에 앱을 추가한다고 해서 해당 앱이 디바이스에 자동으로 설치되는 것은 아니라는 점에 유의하세요. 사용자가 기기에서 Play 스토어를 열고 앱을 수동으로 설치해야 합니다.

기기에 앱을 자동으로 설치하려면 '앱 관리' → '기업 앱 관리자' → '필수 앱'으로 이동하여 원하는 앱을 추가하세요.

이 시점에서 사용자에게 선택적 앱을 배포할 수 있습니다.

여기에서 Android 엔터프라이즈 플레이스토어에 앱을 추가할 수 있습니다. 일반 설정 → AE Play 스토어 → Play 스토어 앱에서 앱을 승인해야 한다는 점에 유의하세요. 이러한 앱은 일반 Google Play 스토어에 추가됩니다.

또한 일반 설정 → 앱 관리 → AE Play 스토어 → 스토어 레이아웃에서 앱으로 레이아웃을 먼저 정의해야 한다는 점에 유의하세요.

앱이 레이아웃에 있어야 스토어에 앱을 성공적으로 추가할 수 있습니다.

키오스크 모드 및 런처

키오스크 모드

키오스크 모드에서는 앱 또는 URL을 미리 정의할 수 있습니다. 그러면 해당 앱 또는 URL을 실행/방문하는 것이 독점적으로 가능해집니다.

마찬가지로 키오스크 모드에서도 다양한 하드웨어 버튼을 비활성화할 수 있습니다.

자동 시작	프로필이 최종 사용자 디바이스에 도달하는 즉시 키오스크 모드가 자동으로 시작됩니다.
예약된 키오스크 모드?	키오스크 모드의 시간을 계획할 수 있으며, 설정한 시간에 자동으로 시작 및 종료됩니다.
시작 시간	시작 시간
시간(분)	키오스크 모드가 다시 종료되어야 하는 시간(분)

애플리케이션 유형

단일 앱	키오스크 모드에서 앱을 시작하려면 '애플리케이션 유형'에서 패키지'를 선택합니다.
키오스크 애플리케이션	키오스크 모드에서 시작해야 하는 앱을 선택하려면 여기를 클릭하세요. 일반적인 앱 관리의 개요를 확인할 수 있습니다. "구글 플레이 스토어", "안드로이드 인하우스 앱", "패키지 이름" 중에서 선택할 수 있습니다.

애플리케이션 유형

URL	키오스크 모드에서 URL을 실행하려면 '애플리케이션 유형' 아래에서 'URL'을 선택합니다. 그런 다음 원하는 URL 주소를 정의합니다.
비활성 후 브라우저 지우기	여기에서 키오스크 모드가 다시 시작될 시간 간격을 분 단위로 정의할 수 있습니다.
웹 캐시 및 쿠키 지우기	이 기능을 활성화하면 키오스크 모드를 다시 시작하면 웹 캐시(쿠키 및 캐시된 사진)가 지워집니다.
동일 출처 정책	이 기능이 활성화되어 있으면 사용자는 정의된 URL의 하위 페이지만 서핑할 수 있습니다. 예를 들어, 다음 URL을 정의했습니다:www.mypage.com 그러면 사용자는 www.mypage.com/subpage 에서 서핑을 할 수 있습니다.
화이트리스트 URL	여기에서 화이트리스트를 관리할 수 있으며, 다음과 같은 모든 URL이 허용됩니다. 한 줄당 최대 1개의 URL URL은 http:/ 또는 https://로 시작해야 합니다.
블랙리스트 URL	여기에서 블랙리스트를 관리할 수 있으며, 다음과 같은 모든 URL은 허용되지 않습니다. 한 줄당 최대 1개의 URL URL은 http:/ 또는 https://로 시작해야 합니다.
화면 방향	이 설정은 화면 조정과 관련이 있습니다. 자동 = 자동 세로 = 세로 형식 가로 = 가로 모드

멀티 앱	"멀티 앱" 키오스크 모드를 선택하면 AppTec360 런처를 사용하게 됩니다.
앱	애플리케이션을 선택합니다: 키오스크 애플리케이션으로 Play스토어 또는 사내 앱을 선택합니다. 패키지 이름을 입력할 수도 있습니다. 선택한 키오스크 애플리케이션이 장치에 설치되어 있어야 합니다. 키오스크 애플리케이션을 필수로 설정하는 것을 잊지 마세요. 홈 화면의 바로 가기: "켜기"로 설정하면 홈 화면에 바로 가기가 만들어집니다. "끄기"로 설정하면 앱이 앱 목록에 계속 표시됩니다.

종료 암호 사용	이 기능을 활성화하면 사용자가 미리 정의한 비밀번호를 사용하여 키오스크 모드를 종료할 수 있습니다.
종료 비밀번호	이것은 사용자가 미리 정의한 비밀번호입니다.
상태 표시줄 자동 접기	이 옵션을 활성화하면 상태 표시줄이 자동으로 축소됩니다. 이 옵션을 사용하면 사용자는 상태 표시줄에서 정보를 볼 수 있지만 해당 기능에는 액세스할 수 없습니다.
상태 표시줄 비활성화	상태 표시줄에는 알림, 바로 가기 및 정보가 포함되어 있습니다. KNOX 1.0 이상이 설치된 삼성 디바이스에서만 사용할 수 있습니다.
볼륨 키 비활성화	볼륨 키 비활성화(KNOX 1.0 이상이 설치된 삼성 디바이스에서만 사용 가능)
켜기/끄기 스위치 비활성화	켜기/끄기 스위치 비활성화(KNOX 1.0 이상이 설치된 삼성 디바이스에서만 사용 가능)
홈 버튼 비활성화	홈 버튼을 비활성화합니다. 이 기능이 활성화된 경우 키오스크 모드는 AppTec360 콘솔에서만 종료할 수 있습니다. (KNOX 1.0 이상이 설치된 삼성 디바이스에서만 사용 가능)
탐색 모음 비활성화	이를 통해 탐색 모음(뒤로/메뉴)을 비활성화할 수 있습니다. 이 기능이 활성화된 경우, 키오스크 모드는 AppTec360 콘솔에서만 종료할 수 있습니다. (KNOX 1.0 이상이 설치된 삼성 디바이스에서만 사용 가능)

앱 업데이트 설정	
앱 업데이트 허용	키오스크 모드가 활성화되어 있어도 앱 업데이트를 수행하라는 메시지가 표시됩니다. 삼성 KNOX가 설치된 디바이스에서는 앱이 자동으로 업데이트됩니다.
업데이트 창	사용자에게 앱 업데이트를 설치하라는 메시지가 표시되는 간격을 설정합니다.

TeamViewer	
무인 액세스 사용	이 기능을 활성화하면 관리자는 사용자 상호 작용 없이 장치를 원격으로 제어할 수 있습니다. 장치에 TeamViewer Host 앱이 설치되어 있어야 합니다.

AppTec360 런처

AppTec360 런처 활성화	켜짐: 앱테크360 런처를 활성화합니다. 사용자는 한 번 기본 런처로 설정해야 합니다. 참고: 키오스크 모드가 활성화되어 있고 키오스크 모드가 "멀티 앱"으로 설정되어 있으면 AppTec360 런처의 사용이 강제 적용됩니다.
큰 아이콘	켜짐: 켜기: 런처에서 앱 아이콘을 더 큰 버전으로 표시합니다.
AppTec360 앱 아이콘 숨기기	켜짐: 켜기: AppTec360 앱을 완전히 숨깁니다.
AppTec360 스토어 아이콘 숨기기	켜짐: 켜기: AppTec360 엔터프라이즈 앱스토어를 완전히 숨깁니다.

AppTec360 설정

AppTec360 설정 앱 활성화	AppTec360 설정 앱은 WiFi 및 블루투스 연결을 제어할 수 있습니다.
멀티 앱에서 설정 활성화 키오스크 모드	활성화된 경우, 사용자는 멀티 앱 키오스크 모드가 활성화된 상태에서 AppTec360 설정 앱에 액세스할 수 있습니다.

원격 제어

스플래시탑

스플래시탑 설정의 현재 상태를 표시합니다. 여기에는 스플래시탑을 통해 디바이스에 원격 액세스하기 위해 수행해야 하는 단계가 표시됩니다. 여기에서 Splashtop 웹사이트에서 받을 수 있는 배포 코드도 입력해야 합니다. 배포 코드는 장치에 연결하기 위해 필요합니다.

팀뷰어

Teamviewer 설정의 현재 상태를 표시합니다. 여기에서 Teamviewer를 통해 장치에 원격으로 액세스하기 위해 수행해야 하는 단계를 확인할 수 있습니다.

콘텐츠 관리

콘텐츠 상자

여기에서 이 장치에 대해 Contentbox를 활성화할 수 있습니다. 활성화되면 콘텐츠박스 앱이 장치에 설치됩니다.

보안 브라우저

여기에서 이 디바이스에 보안 브라우저를 활성화할 수 있습니다. 활성화하면 보안 브라우저 앱이 디바이스에 설치됩니다. 이 브라우저는 필요에 따라 제한된 웹 브라우저를 디바이스에 제공하도록 구성할 수 있습니다.

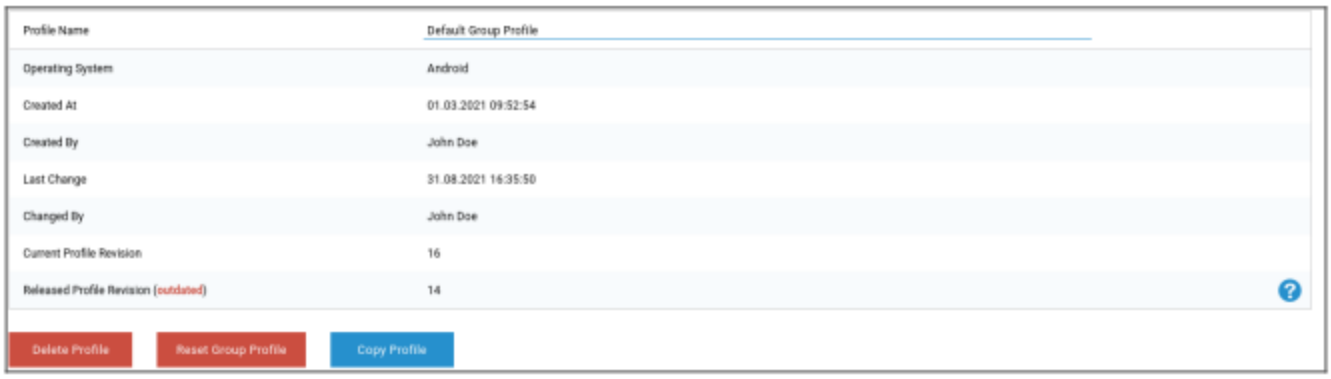
비밀번호 필요	사용자가 브라우저에 액세스하기 위해 비밀번호를 설정하고 사용하도록 요구합니다.
다운로드 제한/열기	웹 사이트에서 다운로드 차단
업로드 제한	특정 URL로 업로드를 제한합니다. 업로드를 완전히 차단하려면 URL을 입력하지 않습니다.
복사 허용	웹 페이지 내의 텍스트 복사, 잘라내기 또는 공유를 허용합니다.
화면 캡처 허용	스크린샷 캡처를 허용합니다.
데이터 정리 빈도	모든 사용자 데이터(기록, 캐시 등)를 자동으로 삭제할 빈도를 선택합니다.
회사 북마크	북마크는 브라우저 북마크의 '회사 북마크' 폴더에 표시됩니다. 사용자가 편집할 수 없습니다.
주소 표시줄 숨기기	사용자가 방문 중인 URL을 볼 수 없도록 주소 표시줄을 숨깁니다.
브라우저 내 화이트리스트(유니버설 게이트웨이 제외)	클라이언트 측 URL 화이트리스트를 활성화합니다. - 회사 북마크는 항상 화이트리스트에 포함됩니다 - 100개의 URL만 지원 - 무제한 블랙리스트 및 화이트리스트를 사용하려면 유니버설 게이트웨이를 사용하세요.
게이트웨이 기반 블랙리스트 및 화이트리스트	블랙리스트에는 다음과 같은 요구 사항이 있습니다: - 작동하는 AppTec360 유니버설 게이트웨이("일반 설정" → "유니버설 게이트웨이") - 지정된 DNS 서버로 작동하는 VPN 구성("일반 설정" → "유니버설 게이트웨이" → "VPN 설정") - 블랙리스트 구성("일반 설정" → "유니버설 게이트웨이" → "도메인 블랙리스트") - 프로필에 유효한 VPN 연결("연결 관리" → "VPN")이 있어야 합니다.

구성 Windows 10 PC

일반

그룹 프로필 개요(그룹 수준에서만)

그룹 프로필을 열면 프로필에 대한 간략한 개요를 볼 수 있습니다.



프로필 이름	프로필 이름(여기에서 변경 가능)
운영 체제	프로필의 운영 체제
만든 곳	생성 시간
만든 사람	프로필 작성자
마지막 변경 사항	프로필을 마지막으로 변경한 시간
변경자	마지막으로 변경한 계정
현재 프로필 수정	저장된 프로필 상태 수정
프로필 수정 버전 출시	할당된 프로필 수정본('지금 할당'). 텍스트 뒤에 '(오래된)'이라는 레이블이 표시되면 프로필을 저장했지만 아직 할당하지 않았으므로 디바이스는 여전히 이전 버전을 받게 됩니다.

장치 개요(장치 수준에서만)

장치의 요약된 개요에는 다음 내용이 포함되어 있습니다:

PC 이름	PC 이름
클라이언트	Windows 유형 장치
마지막으로 알려진 위치	기기의 마지막 알려진 위치의 위도 및 경도
필수 앱 지정	디바이스에 할당된 필수 앱 수
PC UID	PC의 UID
OS 에디션	Windows 버전 표시
OS 버전	현재 설치된 Windows 버전
OS 빌드	현재 Windows 빌드
운영 체제	현재 설치된 운영 체제
일련 번호	장치의 일련 번호
디바이스 소유권	구성된 소유권 유형
디바이스 유형	디바이스 유형
루팅	기기가 루팅되었는지 여부 표시
규정 준수	디바이스가 규정을 준수하는지 표시
마지막으로 본	프로필이 변경된 날짜 및 시간
사용자 할당	이 디바이스가 현재 할당된 사용자 또는 그룹을 표시합니다. 드롭다운 목록에서 다른 사용자 또는 그룹을 선택하여 디바이스를 이동할 수 있습니다.

설정

자동 업데이트 허용	자동 OS 업데이트를 허용 또는 허용하지 않습니다.

구성 수정(디바이스 수준에서만)

여기에서 장치에 어떤 그룹 프로필이 할당되었는지에 대한 개요를 볼 수 있습니다.

그룹 프로필을 클릭하면 프로필에 바로 액세스하여 설정을 수행할 수 있습니다.

기호를 사용하여 할당된 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

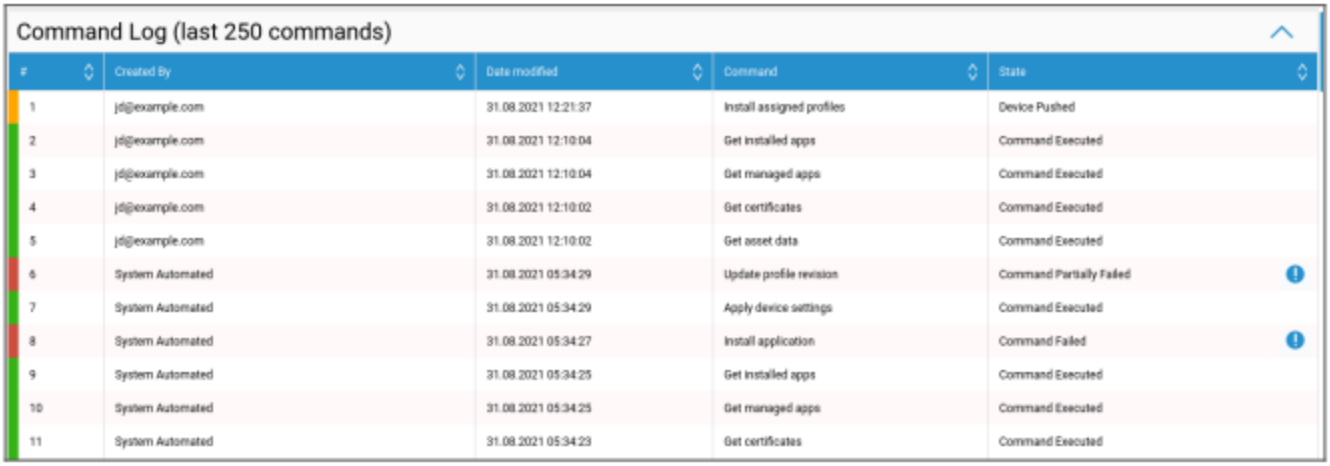
기호를 사용하면 설정이 전혀 없도록 디바이스 프로필을 초기화할 수 있습니다.

"최신 수정본 사용 가능"은 그룹 프로필이 변경되어 저장되었지만 할당되지 않았음을 나타냅니다. 변경 사항을 디바이스에 적용하려면 그룹 수준에서 '지금 할당'을 사용하여 그룹 프로필을 할당해야 합니다.

디바이스 로그(디바이스 수준에서만)

명령 로그

여기에서 디바이스에 대해 어떤 명령이 실행되었는지, 어떤 상태인지 확인할 수 있습니다.



'시스템 자동화'에 의해 생성된 명령은 시스템에 의해 자동으로 생성됩니다.

가능한 명령 상태

푸시된 장치	푸시 요청이 푸시 서비스(예: APNS)로 전송되어 디바이스가 EMM 서버에 다시 연결하도록 지시합니다.
명령 생성	이 명령은 시스템에서 생성되었습니다.
명령 전송	명령은 서버에 연결한 후 디바이스로 전송되었습니다.
명령 실행	명령이 성공적으로 실행되었습니다.
명령 실패	명령이 실패했습니다. *
명령이 부분적으로 실패했습니다.	디바이스 OS에 따라 일부 명령이 함께 그룹화될 수 있습니다. 이 경우 이 명령 그룹의 일부가 실패했습니다. *
명령 실행, 결국 실패	명령이 실행되었지만 실행되지 않았을 수도 있습니다.
명령 재푸시	명령이 사용자에 의해 다시 푸시되었습니다.
폐기됨	명령이 삭제되었습니다. 예를 들어 다른 명령으로 대체되었거나 디바이스가 다시 등록되어 이전 명령이 제거되었기 때문입니다.

*메시지 뒤에 느낌표가 있는 경우 커서로 아이콘을 가리키면 자세한 정보를 확인할 수 있습니다.

자산 관리(디바이스 수준에서만)

장치 정보

제조업체	장치 제조업체
모델	디바이스 모델
모델 번호	모델 번호
운영 체제	운영 체제
OS 버전	OS 버전
일련 번호	일련 번호
ExchangeID	ExchangeID
총 RAM	총 RAM
디스플레이 해상도	디스플레이 해상도
전화 언어	장치 언어
펌웨어 버전	펌웨어 버전
DM 클라이언트 버전	장치 관리 클라이언트 버전
하드웨어 버전	장치 하드웨어 버전
CPU 아키텍처	CPU 아키텍처(프로세서 유형)

셀룰러

SIM 이동 통신사 네트워크	통신사 네트워크
전화번호	전화번호
로밍 상태	로밍 상태
IMEI	IMEI
IMSI	IMSI
모뎀 펌웨어	모뎀 펌웨어

동기화 정보

즉시 DM 연결	장치는 즉시 AppTec에 대한 연결을 생성해야 합니다.
초기 재시도 시간	첫 번째 연결에 대한 초기 재시도 시간
연결 재시도	연결 관리자에서 연결이 끊어지거나 WinInet 수준 오류가 발생한 후 새 연결 재시도 횟수
최대 수면 시간	패키지 전송 오류 후 최대 절전 시간
첫 번째 동기화 재시도	등록 후 첫 번째 단계의 시간
첫 번째 재시도 간격	등록 후 첫 번째 단계의 시간
두 번째 동기화 재시도	등록 후 두 번째 단계의 시간
두 번째 재시도 간격	등록 후 두 번째 단계의 시간
정기적인 동기화 재시도	등록 후 추가 단계를 위한 시간
정기 재시도 간격	등록 후 추가 단계를 위한 시간

보안 관리

도난 방지(디바이스 수준에서만)

GPS 정보(디바이스 수준에서만)

여기에서 현재/마지막 장치 위치를 설정할 수 있습니다. 현지화는 하나 또는 두 개의 비밀번호로 보호할 수 있습니다(참조: "일반 설정" > "개인정보" > "GPS 액세스"를 참조하세요.

GPS 설정

GPS 추적 활성화	GPS 정보를 정기적으로 동기화할 수 있습니다.
추적 간격	GPS 정보 동기화 간격을 설정합니다.

보안 구성

암호

최소 비밀번호 길이	최소 비밀번호 길이	
비밀번호 구성	비밀번호에 포함되어야 하는 특정 문자 수를 지정합니다. 대문자, 소문자, 숫자 및 특수 기호로 구성됩니다.	
비밀번호 품질	여기에서 비밀번호 품질을 설정할 수 있습니다.	
	영숫자	숫자와 문자만
	숫자	숫자만
	숫자 또는 영숫자	숫자 또는 숫자 및 문자
최대 비활성 시간 잠금	디바이스에서 사용자가 활동하지 않은 시간(분) 이후 디바이스가 잠기는 시간입니다. 이 시간이 지나면 사용자는 디바이스 비밀번호를 입력하여 디바이스의 잠금을 해제해야 합니다.	
비밀번호 만료	새 비밀번호를 설정해야 할 때까지의 시간 설정	
비밀번호 기록 제한	허용되지 않는 이전에 사용한 비밀번호의 수	
최대 실패한 비밀번호 시도 횟수	장치를 완전히 초기화하기 전에 비밀번호를 잘못 입력할 수 있는 횟수	

바이러스 백신

바이러스 백신 설정 - 검사 구성 설정	
스캔 유형	빠른 스캔을 수행할지 전체 스캔을 수행할지 선택합니다.
스캔 시작 설정	Windows Defender가 검사를 시작할 하루 중 시간을 선택합니다.
스캔 빈도	Windows Defender 검사를 실행할 날짜를 선택합니다.
서명 업데이트 빈도	서명을 확인하는 데 사용할 간격을 시간 단위로 지정합니다.

스캔할 파일 유형 구성	
아카이브 파일 스캔 허용	액세스 시 아카이브(.zip 등)의 스캔을 허용하거나 허용하지 않습니다.
스크립트 스캔 허용	Windows Defender 스크립트 검사 기능을 허용하거나 허용하지 않습니다.
이메일 스캔 허용	이메일 스캔을 허용하거나 허용하지 않습니다.
네트워크 파일 스캔 허용	네트워크 파일 스캔을 허용하거나 허용하지 않습니다.
매핑된 네트워크 드라이브의 전체 스캔 허용	매핑된 네트워크 드라이브의 스캔을 허용 또는 허용하지 않습니다(전체 스캔이 활성화된 경우에만 활성화됨).
양방향 스캔 제어	모니터링할 파일 집합을 제어합니다.
이동식 드라이브의 전체 스캔 허용	이동식 드라이브의 전체 스캔을 허용하거나 허용하지 않습니다. 전체 스캔 중에만 시작됩니다.

검사에서 제외할 파일 유형	
스캔할 파일 형식 무시	파일 확장자 유형 집합을 정의합니다. 각 필드에 대한 각 파일 확장자를 정의합니다.
디렉토리 경로 무시	스캔하지 않으려면 디렉터리 경로 집합을 정의하세요. 필드당 하나의 경로. 예시: "C:\Example", "C:\Windows" 또는 "C:\Users".
스캔에서 프로세스 제외	특정 프로세스에서 연 파일을 Microsoft Defender 바이러스 백신 검사에서 제외합니다. . 필드당 하나의 경로. 예 "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

추가 설정	
실시간 모니터링 허용	Windows Defender 실시간 모니터링 기능 허용 또는 허용 안 함
행동 모니터링 허용	Windows 동작 모니터링 기능 허용 또는 허용 안 함
클라우드 보호 허용	Windows Defender가 발견한 문제에 대한 정보를 Microsoft에 보내도록 허용하거나 허용하지 않도록 설정합니다. Microsoft는 해당 정보를 분석하여 장치에 영향을 미치는 문제에 대해 자세히 알아보고 개선된 솔루션을 제공합니다.
	샘플을 보내는 동작
Windows Defender IOAV 보호 허용	Windows Defender IOAV 보호 허용 또는 허용 안 함
수비수에게 액세스 허용 "액세스 보호 켜기" UI	
평균 CPU 부하율	Windows Defender 검사에 대한 평균 CPU 부하율(퍼센트)을 나타냅니다.

멀웨어 처리	
낮은 심각도 보통 심각도 높은 심각도 심각도	각 심각도 수준에 따라 디바이스가 멀웨어를 처리하는 방법을 정의할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다: • 청소 • 격리 • 제거 • 허용 • 사용자 정의 • 블록
치료된 멀웨어를 보관하는 일수	격리된 파일/항목이 시스템에 저장되는 기간(일)입니다. 기본값은 0으로, 항목을 격리 상태로 유지하며 자동으로 제거하지 않습니다. 최대값은 90입니다.

보안 센터

Windows 보안 센터 - Windows 보안 설정	
바이러스 및 위협 보호 UI 비활성화	
랜섬웨어 데이터 복구 UI 숨기기	
계정 보호 비활성화 UI	
방화벽 및 네트워크 보호 UI 비활성화	
앱 및 브라우저 제어 UI 비활성화	
익스플로잇 보호에 대한 변경 허용	사용자가 익스플로잇 보호 설정을 변경할 수 없도록 허용하기
장치 보안 UI 비활성화	
TPM 문제 해결 숨기기	TPM 문제 해결 설정 숨기기
TPM 지우기 버튼 비활성화	
디바이스 성능 및 상태 UI 비활성화	
패밀리 옵션 비활성화 UI	

토스트 사용자 지정	
맞춤형 지원 정보 사용 설정	보안 센터 앱의 오른쪽 하단에 회사에 대한 사용자 지정 지원 연락처 정보를 표시하도록 설정합니다.
이메일 주소	회사 이메일 주소 설정
회사 이름	회사 이름 설정
회사 전화	회사 전화 설정
도움말 URL	회사의 도움말 URL 설정

추가 설정	
알림 비활성화	Windows Defender 보안 센터 알림 표시를 비활성화합니다.
TPM 펌웨어 업데이트 권장 사항 숨기기	취약한 펌웨어가 감지되면 TPM 펌웨어 업데이트 권장 사항을 숨깁니다.
회사명 및 연락처 옵션 표시	Windows Defender 보안 센터의 연락처 카드 플라이아웃에 회사 이름과 연락처 옵션을 표시하세요.
보안 부팅 숨기기	보안 부팅 영역 숨기기.
보안 알림 영역 제어 숨기기	Windows 보안 알림 영역 제어를 숨깁니다.

방화벽 구성

방화벽 구성 - 전역 설정	
인증 세트 무시	집합에 지정된 모든 인증 제품군을 지원하지 않는 경우 전체 인증 집합을 무시합니다.
패킷 큐잉 유형	수신 측의 소프트웨어에 대한 스케일링이 암호화된 수신과 IPsec 터널 게이트웨이 시나리오의 순방향 경로 지우기 모두에 대해 활성화되는 방법을 지정합니다.
상태 저장 FTP 필터링 수행 비활성화	이 기능을 비활성화하면 보조 연결을 허용하기 위해 상태 저장 파일 전송 프로토콜(FTP) 필터링을 수행하지 않습니다.
보안 연결 유휴 시간	이 필드는 보안 연결 유휴 시간(초)을 구성합니다. 이 지정된 시간 동안 네트워크 트래픽이 표시되지 않으면 보안 연결이 삭제됩니다.
사전 공유 키 인코딩	미리 공유한 키 인코딩 설정
IPSec 예외	인터넷 프로토콜 예외 구성
인증서 해지 목록 확인	

방화벽 프로필(도메인 프로필/개인 프로필/공용 프로필)	
이 프로필에 방화벽 사용	
알림 비활성화	애플리케이션이 포트에서 수신이 차단된 경우 사용자에게 알림을 표시하지 않도록 설정합니다.
멀티캐스트 생방송에 대한 유니캐스트 응답 차단하기	
인증된 애플리케이션 방화벽 규칙 적용	적용되지 않으면 로컬 스토어에서 권한이 부여된 애플리케이션 방화벽 규칙이 무시되고 적용되지 않습니다.
글로벌 포트 방화벽 규칙 적용	적용하지 않으면 로컬 저장소의 글로벌 포트 방화벽 규칙이 무시되고 적용되지 않습니다. 이 설정은 그룹 정책 저장소에서 설정되거나 열거된 경우에만 의미가 있으며, 그룹 정책 저장소에서 열거된 경우 또는 GroupPolicyRSoPStore에서 설정된 경우에만 의미가 있습니다.
방화벽 규칙 적용	적용되지 않으면 로컬 스토어의 방화벽 규칙이 무시되고 적용되지 않습니다.
연결 보안 규칙 적용	적용되지 않으면 로컬 스토어의 연결 보안 규칙이 무시되고 적용되지 않습니다.
기본 아웃바운드 작업	방화벽이 아웃바운드 연결에서 기본적으로 수행하는 작업
기본 인바운드 작업	방화벽이 인바운드 연결에서 기본적으로 수행하는 작업
스텔스 모드 비활성화	스텔스 모드는 악의적인 사용자가 네트워크 컴퓨터 및 실행 중인 서비스에 대한 정보를 발견하지 못하도록 도와주는 Windows 방화벽의 메커니즘입니다.
원치 않는 트래픽에 응답하지 않도록 설정하기	비활성화하는 경우 방화벽의 스텔스 모드 규칙은 해당 트래픽이 IPsec으로 보호되는 경우 호스트 컴퓨터가 원치 않는 네트워크 트래픽에 응답하는 것을 방지하지 않아야 합니다.

방화벽 규칙

방화벽 규칙	
이름	규칙 이름
설명	규칙 설명
액션	이 규칙이 트래픽을 차단할지 아니면 허용할지 지정합니다. 차단 옵션은 MDM 서버와 장치 간의 트래픽(나머지 구성에 따라 다름)도 차단할 수 있다는 점을 고려하세요.
방향	
엣지 트래버스 활성화(**방향이 인바운드 트래픽으로** 설정된 경우에만 사용 가능)	특정 인바운드 트래픽이 Teredo 터널링 기술을 사용하여 NAT 및 기타 에지 디바이스를 통해 터널링되도록 허용됨을 나타냅니다.

프로그램 및 서비스	
애플리케이션 정의, 그 외에는 모두	활성화하지 않으면 모든 애플리케이션을 고려합니다.
패키지 제품군 이름	규칙이 적용될 패키지 패밀리 이름입니다.
애플리케이션의 파일 경로	규칙이 적용될 전체 응용 프로그램(예: C:\Windows\System\Notepad.exe)
정규화된 바이너리 이름	규칙이 적용될 정규화된 바이너리 이름입니다. FQBN은 다음 형식의 문자열입니다: {발행자\제품\파일명,버전}입니다.
서비스 이름	서비스 이름을 입력합니다(예: "EventLog"). "Get-Service" 명령을 실행하여 Powershell에서 서비스 이름 목록을 가져올 수 있습니다.

<table>
<tr><th colspan="5">프로토콜 및 포트</th></tr>
<tr><td rowspan="8">프로토콜</td><td colspan="4">규칙에서 사용하는 프로토콜입니다.</td></tr>
<tr><td rowspan="7">사용 가능한 값입니다:
- 모든
- 사용자 지정
- 호포트
- ICMPv4
- IGMP
- TCP
- UDP
- IPv6
- IPv6-라우트
- IPv6-Frag
- GRE
- ICMPv6
- IPv6-NoNxt
- IPv6 옵션
- VRRP
- PGM
- L2TP</td><td>사용자 지정으로 설정한 경우</td><td>0에서 255 사이의 프로토콜 번호를 입력합니다.</td><td>프로토콜 번호</td></tr>
<tr><td rowspan="6">TCP 또는 UDP로 설정한 경우</td><td rowspan="2">로컬 포트를 지정하지 않으면 모두 사용됩니다.</td><td rowspan="2">규칙이 사용할 로컬 포트, 범위 포트도 허용됩니다.</td></tr>
<tr></tr>
<tr><td>로컬 포트</td><td>단일 포트 또는 다양한 포트. 예: 100-120,200,300-320.</td></tr>
<tr><td>원격 포트를 지정하지 않으면 모두 사용됩니다.</td><td>규칙이 사용할 원격 포트, 범위 포트도 허용됩니다.</td></tr>
<tr><td>원격 포트</td><td>단일 포트 또는 다양한 포트. 예: 100-120,200,300-320.</td></tr>
<tr></tr>
</table>

<table>
<tr><th colspan="3">범위</th></tr>
<tr><td colspan="2">로컬 IP를 지정하고, 그렇지 않은 경우 모든 IP를 지정합니다.</td><td>로 구분된 로컬 IP 집합일 수도 있으며, -로 구분된 IP 범위일 수도 있습니다.</td></tr>
<tr><td></td><td>로컬 IP 주소</td><td>로 구분된 단일 IP 또는 IP 범위의 집합입니다.</td></tr>
<tr><td colspan="2">원격 IP 지정, 그렇지 않으면 모든 원격 IP</td><td>원격 IP 집합을 지정할 수 있으며, "-"로 구분된 IP 범위일 수도 있습니다.</td></tr>
<tr><td></td><td>원격 IP 주소</td><td>단일 IP 또는 범위의 IP 지정</td></tr>
<tr><td></td><td>토큰</td><td>원격 주소와 함께 설정할 수 있는 토큰. 토큰 인트라넷, Rmt인트라넷 및 Ply2Renders는 Windows 10, 버전 1809 이상에서 지원됩니다.</td></tr>
</table>

<table>
<tr><th colspan="2">고급 설정</th></tr>
<tr><td>프로필을 지정하지 않으면 모두 사용됩니다.</td><td>비활성화하면 모든 프로필이 사용됩니다.</td></tr>
<tr><td>도메인</td><td>도메인 프로필</td></tr>
</table>

비공개	비공개 프로필
공개	공개 프로필
인터페이스를 지정하지 않으면 모두 사용됩니다.	비활성화하면 모든 인터페이스가 사용됩니다.
로컬 영역 네트워크	로컬 영역 네트워크 인터페이스
원격 액세스	원격 액세스 인터페이스
무선	무선 인터페이스

지역 교장	
인증된 로컬 사용자 추가	이 규칙을 사용할 로컬 사용자 목록을 추가하도록 허용합니다.
인증된 사용자	이 규칙에 대해 권한이 부여된 로컬 사용자 목록입니다. 사용자는 SDDL(보안 설명 정의 언어) 형식(예: PC_NAME\USERNAME)이어야 합니다. 서비스 이름이 이 규칙을 사용하도록 설정된 경우에는 이 필드를 채우지 않아야 합니다.

제한 설정

디바이스 기능

SD 카드 허용	SD 카드 사용 허용
카메라 허용	카메라 사용 허용
위치 서비스 허용	디바이스 위치 서비스 허용
앱 사이드로드 허용	알 수 없는 출처의 앱 설치 허용
개발자 모드 허용	개발자 모드 허용
셀룰러 데이터 로밍 허용	셀룰러 데이터 로밍 허용
Cortana 허용	음성 도우미 Cortana 허용
검색에서 위치 사용 허용	검색에서 위치 사용 허용
Microsoft 이외의 이메일 계정 추가 허용	사용자가 MSA 이외의 이메일 계정을 추가할 수 있도록 허용할지 여부를 지정합니다.
Microsoft 계정 연결 허용	이메일과 관련이 없는 연결 인증 및 서비스에 MSA 계정을 사용할 수 있도록 허용할지 여부를 지정합니다.
내 설정 동기화 허용	전체 장치에서 설정을 동기화할 수 있습니다.
기업 보호 도메인 이름	엔터프라이즈 도메인 이름을 ";"으로 구분하여 지정합니다.
사용자가 시스템 복원을 비활성화하도록 허용	사용자가 시스템 복원을 비활성화할 수 있습니다. **경고!** 이 기능은 기업 회사 또는 조직이 소유하거나 제공한 디바이스 또는 사용자가 기업 회사에서 디바이스를 완전히 관리하도록 허용한 사용자 소유 디바이스에서만 사용해야 합니다. 이 정책 설정을 비활성화하면 시스템 복원이 꺼지고 시스템 복원 마법사에 액세스할 수 없습니다. 시스템 복원을 구성하거나 시스템 보호를 통해 복원 지점을 만드는 옵션도 비활성화됩니다.
사용자 등록 취소 허용	사용자가 장치에서 회사 부분을 제거하여 AppTec360 서버와의 연결을 끊을 수 있습니다. 이 경우 더 이상 디바이스를 관리할 수 없습니다. **경고!** 이 기능은 기업 회사 또는 조직이 소유하거나 제공한 장치 또는 사용자가 기업 회사에서 장치를 완전히 관리하도록 허용한 사용자 소유 장치에서만 사용해야 합니다. 이 정책 설정을

	비활성화하면 사용자가 MDM 등록을 제거할 수 없습니다. 사용자가 워크플레이스 제어판을 통해 워크플레이스 계정을 삭제할 수 있도록 허용할지 여부를 지정합니다. MDM 서버는 항상 원격으로 계정을 삭제할 수 있습니다.

BitLocker

BitLocker 구성

일반 설정	
장치 암호화 필요	Windows 버전 및 시스템 구성에 따라 사용자에게 장치 암호화를 사용하도록 설정할지 묻는 메시지가 표시될 수 있습니다: - 다른 제공업체의 암호화가 활성화되어 있지 않은지 확인합니다. - BitLocker 드라이브 암호화를 껐다가 다시 켜려면 다음과 같이 하세요.
암호화 방법	
운영 체제 드라이브의 암호화 방법	
고정 데이터 드라이브의 암호화 방법	
이동식 데이터 드라이브의 암호화 방법	
타사 디스크 암호화에 대한 경고 비활성화하기	장치에서 사용 중인 타사 디스크 암호화 서비스에 대한 경고 메시지를 비활성화합니다. Windows 10, 버전 1803부터 이 설정은 Azure Active Directory 가입 디바이스에 대해서만 지원됩니다.
관리자가 아닌 사용자가 로그인한 상태에서 암호화 실행 허용	Azure Active Directory에 가입된 디바이스만 지원

AppTec360 확장 프로그램	
자동 암호화	"디바이스 암호화 필요"와 함께 선택하면 AppTec360 관리 서비스가 디바이스 드라이브의 자동 무음 암호화를 실행합니다.
사용자 자격 증명 자동 생성	암호화된 OS 드라이브는 자동으로 생성된 사용자 자격 증명으로 보호됩니다. TPM을 사용할 수 있는 경우 TPM PIN 또는 6자리 텍스트 비밀번호를 입력합니다. 생성된 자격 증명은 지정된 장치에 등록된 이메일 주소로 전송됩니다. 이 옵션을 해제하면 자동 암호화를 보호할 수 있는 유일한 방법은 TPM을 사용하는 것입니다. 이 경우 TPM이 없는 장치의 경우 자동 암호화가 실패합니다.
고정 드라이브 암호화	사용 가능한 모든 고정 데이터 드라이브도 OS 드라이브에 저장된 키를 사용하여 '자동 잠금 해제'로 암호화 및 보호됩니다.

OS 드라이브 설정

시작 시 추가 인증 필요	이 설정을 사용하면 컴퓨터를 시작할 때마다 BitLocker에 인증이 필요한지 여부를 구성할 수 있습니다. 이 설정은 BitLocker를 설정하는 동안 적용됩니다. 이 설정을 활성화하면 사용자는 BitLocker 설정 마법사에서 고급 시작 옵션을 구성할 수 있습니다.
호환되는 TPM이 없는 BitLocker 차단	
TPM 전용	
TPM 및 PIN	
TPM 및 키	
TPM, 키 및 PIN	PIN과 USB 플래시 드라이브(키)를 사용하도록 하려면 BitLocker 드라이브 암호화 설정 마법사 대신 명령줄 도구인 "manage-bde"를 사용하여 BitLocker를 설정해야 합니다.

최소 PIN 길이 필요	
	최소 문자 수

부팅 전 복구 메시지 및 URL 구성하기	전체 복구 메시지를 구성하거나 OS 드라이브가 잠겨 있을 때 부팅 전 키 복구 화면에 표시되는 기존 URL을 대체할 수 있습니다. 참고: 사전 부팅에서 모든 문자 및 언어가 지원되는 것은 아닙니다. 부팅 전 복구 화면에서 사용하는 문자가 올바르게 표시되는지 테스트하는 것이 좋습니다.
	부팅 전 복구 메시지 옵션
	사용자 지정 복구 메시지

	사용자 지정 복구 URL

OS 드라이브 복구 옵션		이 설정을 사용하면 필요한 자격 증명이 없는 경우 BitLocker로 보호된 운영 체제 드라이브가 복구되는 방법을 제어할 수 있습니다. 이 설정은 BitLocker를 설정하는 동안 적용됩니다. 기본적으로 인증서 기반 데이터 복구 에이전트가 허용되며, 복구 암호 및 복구 키를 포함하여 복구 옵션을 사용자가 지정할 수 있고 복구 정보는 AD DS에 백업되지 않습니다.
	인증서 기반 데이터 복구 에이전트 차단	데이터 복구 에이전트를 BitLocker로 보호된 운영 체제 드라이브에 사용할 수 있는지 여부를 지정합니다. 데이터 복구 에이전트를 사용하려면 먼저 그룹 정책 관리 콘솔 또는 로컬 그룹 정책 편집기의 공개 키 정책 항목에서 추가해야 합니다. 데이터 복구 에이전트 추가에 대한 자세한 내용은 Microsoft TechNet의 BitLocker 드라이브 암호화 배포 가이드를 참조하세요.
	BitLocker 복구 암호 설정	
	BitLocker 복구 키 설정	
	비트락커 복구 정보를 Active Directory 도메인 서비스에 저장하기	
	AD DS BitLocker 복구 저장소 구성	키 패키지를 저장하면 물리적으로 손상된 드라이브에서 데이터를 복구할 수 있습니다.
	복구 데이터를 AD DS에 저장해야 함	컴퓨터가 도메인에 연결되어 있지 않으면 사용자가 BitLocker를 사용하도록 설정하지 못하도록 합니다.

고정 드라이브 설정	
고정 드라이브 복구 옵션	이 설정을 사용하면 필요한 자격 증명이 없는 경우 BitLocker로 보호된 고정 드라이브가 복구되는 방법을 제어할 수 있습니다. 이 설정은 BitLocker를 설정하는 동안 적용됩니다. 기본적으로 인증서 기반 데이터 복구 에이전트가 허용되며, 복구 암호 및 복구 키를 포함하여 복구 옵션을 사용자가 지정할 수 있고 복구 정보는 AD DS에 백업되지 않습니다.
인증서 기반 데이터 복구 에이전트 차단	
BitLocker 복구 암호 설정	
BitLocker 복구 키 설정	
비트락커 복구 정보를 Active Directory 도메인 서비스에 저장하기	
AD DS BitLocker 복구 저장소 구성	키 패키지를 저장하면 물리적으로 손상된 드라이브에서 데이터를 복구할 수 있습니다.
복구 데이터를 AD DS에 저장해야 함	컴퓨터가 도메인에 연결되어 있고 BitLocker 복구 정보를 AD DS에 백업하는 데 성공하지 않으면 사용자가 BitLocker를 사용하도록 설정할 수 없도록 합니다. 참고: 복구 비밀번호는 자동으로 생성됩니다.
보호되지 않은 고정 드라이브에 대한 쓰기 액세스 거부	

이동식 드라이브 설정	
보호되지 않은 이동식 드라이브에 대한 쓰기 액세스 거부	Bitlocker로 보호되지 않는 이동식 데이터 드라이브에 대한 쓰기 액세스를 거부합니다. 참고: 그룹 정책에서 "이동식 디스크: 쓰기 액세스 거부"가 그룹 정책에서 활성화되어 있으면 이 정책 설정은 무시됩니다.
다른 조직에 구성된 장치에 대한 쓰기 액세스 거부	컴퓨터의 식별 필드와 일치하는 식별 필드가 있는 드라이브에만 쓰기 권한이 부여됩니다. 이러한 필드는 '조직의 고유 식별자 제공' 그룹 정책 설정에 의해 정의됩니다.

비트락커 상태

여기에서 BitLocker로 암호화된 드라이브의 현재 상태를 확인할 수 있습니다.

C [OS Drive]
암호화 상태
암호화(%)
보호 상태
암호화 방법
주요 보호자
복구 비밀번호

"복구 비밀번호 회전" 버튼을 클릭하면 BitLocker 복구 비밀번호를 회전할 수 있습니다.

인증서 관리

인증서 목록

다음은 표시되는 장치에 설치된 인증서 목록입니다.

인증서 구성

여기에서 인증서를 구성하고 장치에 설치하는 방법을 구성할 수 있습니다.

신뢰할 수 있는 인증서	
설명	인증서 설명
범위	인증서 배포 범위: 현재 사용자 대 장치
인증서 저장소	"신뢰할 수 없는 인증서"는 Windows 10, 버전 1803부터 사용할 수 있습니다.
인증서 파일	PKCS#1 파일 업로드

신원 인증서			
설명	인증서 설명		
범위	인증서 배포 범위: 현재 사용자 대 장치		
주요 위치	개인키를 설치할 키 저장소 공급자입니다.		
		TPM. TPM이 없는 경우 실패	
	TPM. TPM이 없는 경우, 소프트웨어 KSP로 폴백합니다.		
	소프트웨어 키 저장소 제공업체	개인 키를 내보내기 가능으로 표시	
	비즈니스용 Windows Hello	컨테이너 이름	비즈니스용 Windows Hello(이전의 업무용 Microsoft Passport) 컨테이너 이름을 지정합니다.
		PIN 프롬프트 텍스트	인증서를 등록하는 동안 비즈니스용 Windows Hello PIN 프롬프트에 표시할 사용자 지정 텍스트를 지정합니다.
자격 증명	PKCS#12 파일 업로드		

SCEP

설명	SCEP 서버 설명		
배포 범위	인증서 배포 범위: 현재 장치 대 사용자		
SCEP 서버 URL	SCEP를 통해 인증서를 발급하는 하나 이상의 서버		
제목	X.500 이름의 표현. 예: "C=미국, O=마이크로소프트 코퍼레이션, CN=푸, 1.2.5.3=바"		
제목 대체 이름	유형	이메일 주소	
		DNS	
		URI	
		사용자 계정 이름(UPN)	
CA 지문	인증 기관 인증서의 SHA1 지문입니다. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
유효 기간 단위	일, 월 또는 년		
유효 기간			
도전 과제	자동 등록을 위한 사전 공유 비밀로 사용됨		
재시도	서버가 보류 중 응답을 보내는 경우 디바이스에서 재시도할 횟수입니다. 기본값은 5입니다. 최대값은 30입니다.		
재시도 지연	재시도하기 전에 대기할 시간(분)입니다. 기본값은 5입니다. 최소값은 1입니다.		
키 크기	비트 단위의 키 크기		
해시 알고리즘	해시 알고리즘 제품군		
주요 사용법	키 사용 확장은 인증서에 포함된 키의 용도(예: 암호화, 서명)를 정의합니다. "디지털 서명" 또는 "키 암호화" 중 하나 이상을 선택해야 합니다.		
확장 키 사용	확장 키 용도를 지정합니다(SCEP 서버 구성에 따라 다름). 해당 OID 목록(예: 1.3.6.1.5.5.7.3.2(클라이언트 인증))을 지정합니다.		
주요 위치	개인키를 설치할 키 저장소 공급자입니다.		
		TPM. TPM이 없는 경우 실패	
	TPM. TPM이 없는 경우, 소프트웨어 KSP로 폴백합니다.		
	소프트웨어 키 저장소 제공업체		

	비즈니스용 Windows Hello	컨테이너 이름	비즈니스용 Windows Hello(이전의 업무용 Microsoft Passport) 컨테이너 이름을 지정합니다.	
		PIN 프롬프트 텍스트	인증서를 등록하는 동안 비즈니스용 Windows Hello PIN 프롬프트에 표시할 사용자 지정 텍스트를 지정합니다.	

연결 관리

Wi-Fi

이 설정에서 내부 액세스 포인트에 액세스할 수 있도록 최종 사용자 디바이스의 사전 구성을 수행합니다.

서비스 세트 식별자(SSID)	연결이 설정될 네트워크의 SSID입니다.
자동 가입	네트워크 자동 가입 활성화
숨겨진 네트워크	AP가 SSID를 브로드캐스트하지 않는 경우 활성화합니다.

보안 유형

AP 보안 유형 설정

WEP 개방형 시스템	
비밀번호	AP의 비밀번호

WPA PSK	
비밀번호	AP의 비밀번호

WPA EAP	
인증 유형	인증 유형, "PEAP-MSCAHPv2"로만 가능
빠른 재연결	디바이스는 다시 인증할 필요 없이 액세스 포인트 간에 전환할 수 있습니다.
게스트 액세스	사용자에게 계정이 없으므로 게스트로 등록해야 합니다.
격리 검사	클라이언트는 NAP(네트워크 액세스 보호) 검사를 수행하고 그 결과를 시스템과 공유한 다음, 클라이언트가 연결할 수 있는지 여부를 결정해야 합니다.
암호화 바인딩 필요	인증은 암호화 바인딩을 통해서만 가능합니다.
서버 유효성 검사	클라이언트는 서버 인증서가 유효한지 확인합니다. 이 경우 연결이 설정됩니다.
인증서 확인 메시지	사용자가 신뢰할 수 없는 인증서를 수락하도록 허용합니다.
서버 이름	네트워크 인증 및 권한 부여를 제공하는 RADIUS 서버의 이름을 표시하는 옵션을 제공합니다.

WPA2-PSK	
비밀번호	AP 비밀번호

WPA2 EAP	
인증 유형	인증 유형, "PEAP-MSCAHPv2"에서만 사용 가능
빠른 재연결	
게스트 액세스	
검역소 검사	네트워크 액세스 보호 NAP 활성화
암호화 바인딩 필요	인증은 암호화 바인딩을 통해서만 가능합니다.
서버 유효성 검사	
인증서 확인 메시지	유효성 검사된 서버 인증서, 이름 또는 루트 인증서 인증(CA)을 입력하라는 메시지가 표시됩니다.
서버 이름	디바이스에서 신뢰할 수 있는 서버 목록
없음	보안이 확립되지 않음
프록시 서버 사용	프록시 서버 사용
서버 주소	프록시 서버 주소
서버 포트	프록시 서버의 서버 포트

프록시 서버 사용

프록시 서버 사용을 활성화합니다.

서버 주소	이 네트워크에서 사용하는 프록시 서버 주소입니다.
서버 포트	이 네트워크에서 사용하는 프록시 서버 포트입니다.

와이파이 제한

여기에서 다양한 와이파이 제한을 정의할 수 있습니다.

WiFi 허용	WiFi 허용/거부
인터넷 공유 허용	핫스팟 사용 허용
WiFi Sense 핫스팟에 자동 연결 허용	WiFi Sense 핫스팟에 자동 연결 허용
수동 WiFi 구성 허용	앱텍에서 정의하지 않은 와이파이 네트워크에 사용자가 연결할 수 있도록 허용합니다.
무선랜 스캔 빈도	WLAN 스캔 간격을 설정합니다. 여기서 값이 클수록 와이파이 네트워크를 인식하는 기능이 향상됩니다.

VPN

VPN 연결을 구성하려면 여기에서 적절한 설정을 수행하세요.

연결 이름	표시된 연결 이름		
VPN 유형	앱별 VPN 연결은 특정 앱의 트래픽을 보호하는 데 사용됩니다.		
	VPN	항상 켜짐	이렇게 하면 로그인 시 VPN이 자동으로 연결되며 사용자가 수동으로 연결을 끊을 때까지 연결이 유지됩니다.
	앱별 VPN	VPN 앱	이 VPN 연결을 사용하는 앱 정의
		앱별 잠금	앱별 잠금을 사용하면 선택한 앱은 이 VPN 연결을 통해서만 연결할 수 있습니다. 이 기능은 Windows Defender 방화벽에 따라 다릅니다.
	WIP 프로필	이 연결에 대한 WIP 도메인	이 VPN 프로필을 WIP(Windows 정보 보호) 정책과 연결하는 데 필요한 엔터프라이즈 ID입니다.

연결 유형

AppTec360 VPN	
"AppTec360 VPN"의 경우 앱 사이드로드를 허용해야 합니다. "보안 관리" → "제한 설정" → "기기 기능"에서 "앱 사이드로드 허용"을 활성화하세요.	
게이트웨이 구성	블랙리스트가 있는 VPN 연결을 구성하려면 지정된 DNS 서버가 있는 VPN 구성을 선택하세요. VPN 구성은 '일반 설정' → '범용 게이트웨이' → 'VPN 설정'에서 설정할 수 있습니다.

IKEv2		
서버	VPN 서버 목록	
디바이스 터널	사용자 로그온 전에 연결을 사용하도록 설정합니다.	
인증 방법	EAP	EAP XML
	머신 인증서	
암호화 알고리즘		
무결성 검사 알고리즘		
디피-헬만 그룹		
암호 변환 알고리즘		
인증 변환 알고리즘		
완전 순방향 비밀(PFS) 그룹		

PPTP		
서버	VPN 서버 목록	
인증 방법	EAP	EAP XML

L2TP		
서버	VPN 서버 목록	
인증 방법	EAP	EAP XML
암호화 알고리즘		
무결성 검사 알고리즘		
디피-헬만 그룹		
암호 변환 알고리즘		
인증 변환 알고리즘		
완전 순방향 비밀(PFS) 그룹		

자동		
서버	VPN 서버 목록	
인증 방법	EAP	EAP XML

일반 VPN 구성

로그온할 때마다 자격 증명 기억하기	
내부 DNS에 IP 주소 등록	
네트워크 트래픽 필터링 규칙	정의된 규칙 집합으로 VPN 연결을 제한합니다.
DNS 접미사 검색 목록	짧은 이름을 라우팅하기 위해 DNS 검색 목록에 추가할 DNS 접미사.
NRPT(이름 확인 정책 테이블) 규칙	NRPT(이름 확인 정책 테이블) 규칙은 VPN에 연결할 때 DNS가 이름을 확인하는 방법을 정의합니다.
신뢰할 수 있는 네트워크 탐지	신뢰할 수 있는 네트워크를 식별하기 위한 DNS 접미사 목록입니다.
분할 터널링	분할 터널링은 트래픽이 네트워킹 스택에 따라 결정된 모든 인터페이스를 통해 이동할 수 있음을 의미합니다.
터널링 경로 분할	VPN 인터페이스의 라우팅 테이블에 추가할 경로 목록입니다.
프록시 설정	이 네트워크에 사용되는 프록시 구성
프록시 주소	프록시 서버 주소를 정규화된 호스트 이름 또는 IP 주소로 지정합니다.
포트	프록시 서버 포트.
프록시 자동 구성 URL	URL을 입력하면 프록시 설정이 자동으로 검색됩니다.

VPN 제한 사항

여기에서 다양한 VPN 제한을 정의할 수 있습니다.

VPN 설정 허용	이 가이드라인은 사용자가 VPN 설정을 비활성화 및 변경하는 것을 허용/금지합니다.
셀룰러를 통한 VPN 허용	디바이스가 모바일 데이터를 사용하는 경우, 디바이스의 VPN 연결을 허용/금지합니다.
셀룰러를 통한 VPN 로밍 허용	디바이스가 로밍 중인 경우 디바이스의 VPN 연결을 허용/금지합니다.

블루투스

여기에서 블루투스를 허용할지 금지할지 설정할 수 있습니다.

블루투스 허용	블루투스 활성화/비활성화

PIM 관리

Exchange Active 동기화

최종 사용자 장치에서 ActiveSync 계정 설정

계정 이름	이메일 계정 이름
서버 호스트 이름	서버 주소/FQDN
도메인 이름	서버 도메인
이메일 주소	이메일 주소
사용자 이름	사용자 이름
사용자 비밀번호	선택적으로 여기에서 사용자에게 비밀번호를 이미 첨부할 수 있습니다.
SSL 사용	SSL 연결 사용
동기화 간격	여기에서 동기화 간격을 설정할 수 있습니다. 수동 동기화 = 사용자가 이메일을 다운로드하고 수동 동기화를 수행해야 합니다.
메일 연령 필터	이메일이 동기화될 때까지의 기간(시간) 필터 없음 = 무제한
로그 레벨	ActiveSync 트래픽에 대한 로깅 수준 설정
이메일 동기화	활성화됨 = 이메일이 동기화됨
연락처 동기화	활성화됨 = 연락처가 동기화됨
캘린더 동기화	활성화됨 = 캘린더가 동기화됨
작업 동기화	활성화됨 = 작업이 동기화됨

이메일

최종 사용자 디바이스에 POP3/IMAP4 계정을 설정합니다.

계정 설명	이메일 계정 이름
발신자 이름	발신자 이름 표시
도메인 이름	이메일 계정의 도메인 이름
이메일 주소	사용자 이메일 주소
사용자 이름	사용자 이름
사용자 비밀번호	선택적으로 여기에서 사용자에게 비밀번호를 이미 첨부할 수 있습니다.
대체 발신 서버 자격 증명	발신 서버에 다른 자격 증명이 필요한 경우 여기에서 정의할 수 있습니다.
발신 도메인 이름	발신 도메인 이름
발신 서버 사용자 이름	발신 서버 사용자 이름
발신 서버 비밀번호	발신 서버 비밀번호
이메일 프로토콜	POP3 또는 IMAP4를 프로토콜로 사용할 수 있습니다.
수신 메일 서버 호스트 이름	수신 메일 서버 호스트 이름
수신 메일에 SSL 사용	수신 이메일에 SSL 사용
발신 메일 서버 호스트 이름	발신 메일 서버 호스트 이름
발신 메일에 SSL 사용	발신 이메일에 SSL 사용
발신 서버 인증	발신 서버 인증이 필요합니다.
동기화 간격	여기에서 동기화 간격을 설정할 수 있습니다. 수동 동기화 = 사용자가 이메일을 다운로드하고 수동 동기화를 수행해야 합니다.
메일 연령 필터	이메일이 동기화될 때까지의 기간(시간) 필터 없음 = 무제한

앱 관리

엔터프라이즈 앱 관리자

설치된 앱

다음은 현재 표시되는 디바이스에 설치된 앱 목록입니다.

필수 앱

여기에서 디바이스에서 필수로 설치해야 하는 앱 목록을 구성할 수 있습니다.

이 목록은 디바이스가 MDM에 연결할 때마다 확인되며, 앱이 제거되었거나 이전에 설치한 적이 없는지 여부에 관계없이 이 목록에 있는 모든 앱을 디바이스에 설치합니다.

Windows 10 사내 앱을 업로드한 다음 이 목록에 추가하거나 '일반 설정' > '앱 관리' > 'Microsoft Office'에서 미리 구성해야 하는 Microsoft Office 구성을 추가할 수 있습니다.

시스템 앱 제한

받은 편지함 앱
알람 및 시계 허용
허용 계산기
카메라 허용
연락처 지원 허용
Cortana 허용
파일 탐색기 허용
허용 시작하기
그루브 음악 허용
지도 허용
메시징 허용
Microsoft Edge 허용
영화 및 TV 허용
돈 허용
뉴스 허용
OneDrive 허용
OneNote 허용
Outlook 일정 및 메일 허용
사람 허용
전화 허용
사진 허용
파워포인트 허용
허용 설정
Skype 허용
스포츠 허용
스토어 허용
음성 녹음기 허용
지갑 허용
날씨 허용

Windows 피드백 허브 허용
Word 허용
Xbox 허용

페이지 설정
계정 허용 작업장
고급 정보 허용
앱 허용 코너
차단 및 필터 허용
색상 프로필 허용
운전 모드 허용
이메일 및 계정 허용
이퀄라이저 허용
키보드 허용
탐색 모음 허용
네트워크 비행기 모드 허용
네트워크 인터넷 공유 허용
네트워크 서비스 허용
네트워크 Wi-Fi 허용
PC 시스템 블루투스 허용
디바이스 평가 허용
업데이트 복원 허용
공유 허용
시작 허용
허용 시간 언어
허용 시간 지역
Windows 기본 잠금 화면 허용
회사 또는 학교 계정 허용

블랙리스트 및 화이트리스트

'블랙리스트 및 화이트리스트'에서 '화이트리스트' 모드와 '블랙리스트' 모드 중에서 선택할 수 있습니다.

화이트리스트	목록에 추가된 앱과 서비스만 최종 사용자 디바이스에 설치할 수 있습니다. 최종 사용자 디바이스에 이미 사전 설치되어 있는 경우 사용자가 실행할 수 있도록 활성화 및 설정됩니다.
	목록에 추가되지 않은 다른 모든 앱은 최종 사용자 디바이스에 설치할 수 없습니다. 이러한 앱이 이미 최종 사용자 디바이스에 사전 설치되어 있는 경우 사용자가 실행할 수 없도록 비활성화 및 설정됩니다.
블랙리스트	목록에 추가된 앱 및 서비스는 최종 사용자 디바이스에 설치할 수 없습니다. 최종 사용자 디바이스에 이미 사전 설치되어 있는 경우 사용자가 실행할 수 없도록 비활성화 및 설정됩니다.
	목록에 추가되지 않은 다른 모든 앱은 최종 사용자 디바이스에 설치할 수 있습니다. 이러한 앱이 이미 최종 사용자 디바이스에 사전 설치되어 있는 경우 사용자가 실행할 수 있도록 활성화 및 설정됩니다.

를 통해 현재 사용 중인 목록에 앱이나 서비스를 추가할 수 있습니다.

를 통해 현재 비활성화된 목록에 앱이나 서비스를 추가할 수 있습니다.

'Windows 앱 스토어'에서 앱을 추가하거나 '앱 식별자'를 직접 입력하여 블랙리스트 또는 화이트리스트에 추가할 수 있습니다.

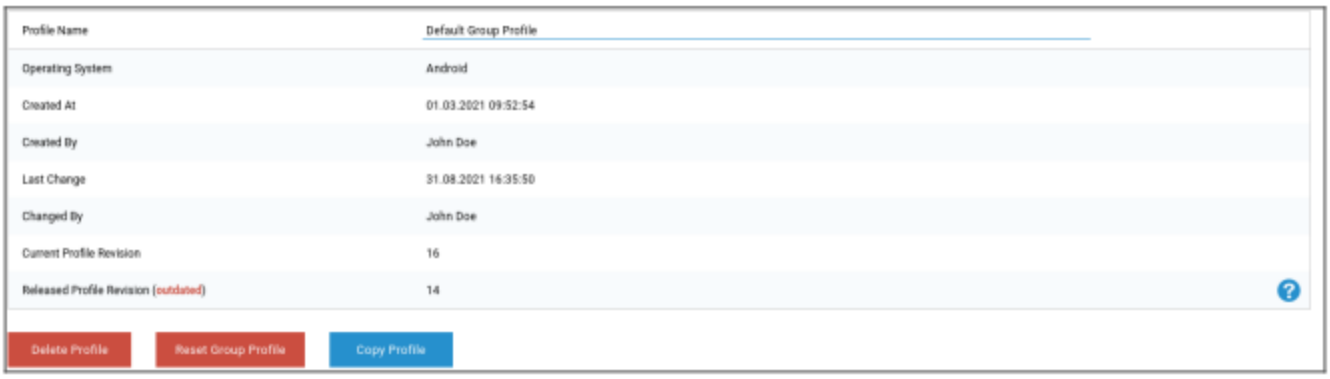
MacOS 구성

프로필 또는 디바이스를 선택했는지 여부에 따라 디스플레이와 하위 포인트가 달라지므로 이 점에 주의하세요!

일반

그룹 프로필 개요(그룹 수준에서만)

그룹 프로필을 열면 프로필에 대한 간략한 개요를 볼 수 있습니다.



프로필 이름	프로필 이름(여기에서 변경 가능)
운영 체제	프로필의 운영 체제
만든 곳	생성 시간
만든 사람	프로필 작성자
마지막 변경 사항	프로필을 마지막으로 변경한 시간
변경자	마지막으로 변경한 계정
현재 프로필 수정	저장된 프로필 상태 수정
프로필 수정 버전 출시	할당된 프로필 수정본('지금 할당'). 텍스트 뒤에 '(오래된)'이라는 레이블이 표시되면 프로필을 저장했지만 아직 할당하지 않았으므로 디바이스는 여전히 이전 버전을 받게 됩니다.

장치 개요(장치 수준에서만)

장치의 요약된 개요입니다.

장치 이름	장치 이름
모델	모델
운영 체제	운영 체제
일련 번호	장치의 일련 번호
디바이스 소유권	구성된 소유권 유형
디바이스 유형	디바이스 유형
규정 준수	디바이스가 규정을 준수하는지 표시
IP 주소	장치가 서버에 연결된 IP 주소입니다.
마지막으로 본	디바이스에서 마지막으로 연결한 시간
마지막 푸시	디바이스에 마지막으로 푸시를 보낸 시간
할당	여기에서 장치를 다른 사용자 또는 그룹으로 이동할 수 있습니다.

구성 수정(디바이스 수준에서만)

여기에서 장치에 어떤 그룹 프로필이 할당되었는지에 대한 개요를 볼 수 있습니다.

그룹 프로필을 클릭하면 프로필에 바로 액세스하여 설정을 수행할 수 있습니다.

기호를 사용하여 할당된 앱을 그룹 프로필의 설정으로 되돌릴 수 있습니다.

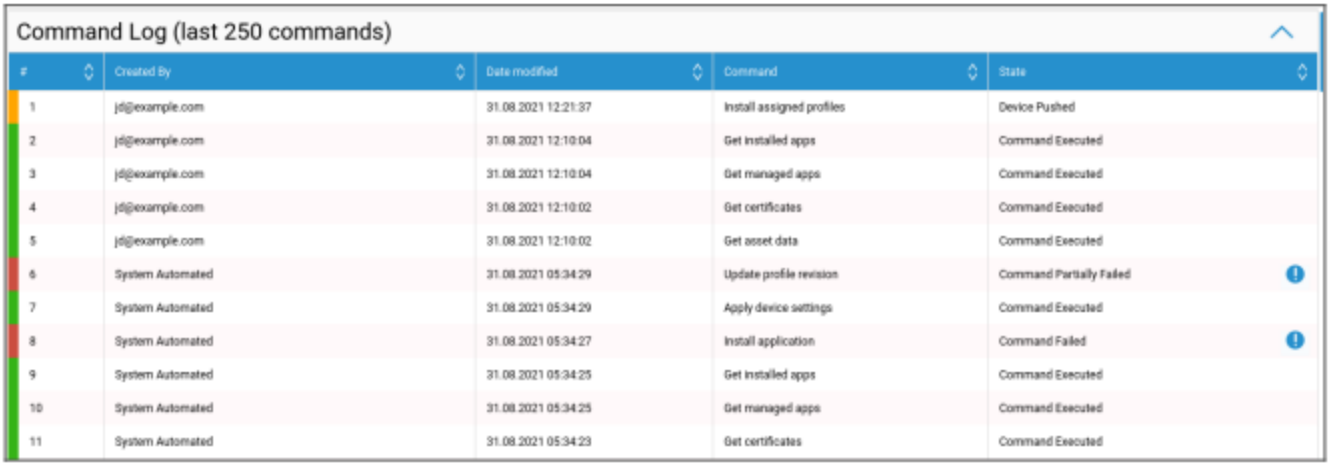
기호를 사용하면 설정이 전혀 없도록 디바이스 프로필을 초기화할 수 있습니다.

"최신 수정본 사용 가능"은 그룹 프로필이 변경되어 저장되었지만 할당되지 않았음을 나타냅니다. 변경 사항을 디바이스에 적용하려면 그룹 수준에서 '지금 할당'을 사용하여 그룹 프로필을 할당해야 합니다.

디바이스 로그(디바이스 수준에서만)

명령 로그

여기에서 디바이스에 대해 어떤 명령이 실행되었는지, 어떤 상태인지 확인할 수 있습니다.



'시스템 자동화'에 의해 생성된 명령은 시스템에 의해 자동으로 생성됩니다.

가능한 명령 상태

푸시된 장치	푸시 요청이 푸시 서비스(예: APNS)로 전송되어 디바이스가 EMM 서버에 다시 연결하도록 지시합니다.
명령 생성	이 명령은 시스템에서 생성되었습니다.
명령 전송	명령은 서버에 연결한 후 디바이스로 전송되었습니다.
명령 실행	명령이 성공적으로 실행되었습니다.
명령 실패	명령이 실패했습니다. *
명령이 부분적으로 실패했습니다.	디바이스 OS에 따라 일부 명령이 함께 그룹화될 수 있습니다. 이 경우 이 명령 그룹의 일부가 실패했습니다. *
명령 실행, 결국 실패	명령이 실행되었지만 실행되지 않았을 수도 있습니다.
명령 재푸시	명령이 사용자에 의해 다시 푸시되었습니다.
폐기됨	명령이 삭제되었습니다. 예를 들어 다른 명령으로 대체되었거나 디바이스가 다시 등록되어 이전 명령이 제거되었기 때문입니다.

*메시지 뒤에 느낌표가 있는 경우 커서로 아이콘을 가리키면 자세한 정보를 확인할 수 있습니다.

자산 관리(디바이스 수준에서만)

장치 정보

모델 번호	모델 번호
호스트 이름	호스트 이름
로컬 호스트 이름	로컬 호스트 이름
운영 체제	운영 체제
OS 버전	OS 버전
UDID	UDID
여유 / 총 메모리	여유 / 총 메모리

WiFi

IP 주소	IP 주소
WiFi MAC	WiFi MAC

셀룰러

전화번호	전화번호
로밍 상태	로밍 상태
로밍(음성/데이터)	로밍(음성/데이터)
IP 주소	IP 주소
사업자/이동 통신사	사업자/이동 통신사
SIM 이동 통신사 네트워크	통신사 네트워크
통신사 버전	통신사 버전
ICCID	ICCID
현재 MCC/MNC	현재 MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

블루투스

블루투스 MAC	블루투스 MAC

업데이트 관리(디바이스 수준에서만)

정보 업데이트

이 탭에는 디바이스의 시스템 업데이트 설정에 대한 정보가 표시됩니다.

자동 확인 사용	시스템이 자동으로 업데이트를 확인하는 경우.
자동 앱 업데이트 사용	시스템이 앱 업데이트를 자동으로 설치하는 경우.
자동 OS 업데이트 사용	시스템이 OS 업데이트를 자동으로 설치하는 경우.
자동 보안 업데이트 사용	시스템에서 보안 업데이트를 자동으로 설치하는 경우.
앱 업데이트 백그라운드 다운로드 사용	시스템이 백그라운드에서 앱 업데이트를 다운로드하는 경우.
카탈로그 URL	클라이언트가 사용 중인 소프트웨어 업데이트 카탈로그의 URL입니다.
기본 카탈로그입니다.	"예"인 경우 카탈로그가 기본 카탈로그가 됩니다.
정기 점검 수행	"예"인 경우 새 스캔을 시작합니다.
이전 스캔 날짜	마지막 소프트웨어 업데이트 검사 날짜입니다.
이전 스캔 결과	마지막 소프트웨어 업데이트 스캔의 결과 코드입니다.

보안 관리

도난 방지

지우기 및 잠금

전체 삭제	기기 초기화 명령 보내기
엔터프라이즈 삭제	장치에서 MDM을 제거하고 모든 MDM 데이터(예: 계정, 앱)를 제거합니다.
잠금 화면	기기를 잠금 화면으로 되돌리기

보안 구성

암호

코드 비활성화 허용	사용자에게 비밀번호를 강제 설정할지 여부를 결정합니다. 이 값을 설정하기만 하면 (다른 값은 설정하지 않음) 길이나 품질에 제한 없이 사용자에게 비밀번호를 입력하도록 강제합니다.
단순 값 허용	사용자가 동일한 숫자 문자열(예: 1234, 1111)을 에스컬레이션 및 축소하여 사용할 수 있도록 허용합니다.
영숫자 값 필요	비밀번호는 하나 이상의 문자를 포함해야 합니다.
최소 암호 길이	최소 비밀번호 길이
복잡한 문자의 최소 개수	비밀번호의 영숫자 기호 최소 개수
최대 암호 사용 기간	비밀번호를 변경해야 하는 기간(일수)
최대 자동 잠금	최대 시간, 그 이후에는 장치가 잠깁니다.
기기 잠금의 최대 유예 기간	잠금 해제 시 비밀번호를 입력하지 않고 장치를 잠글 수 있는 시간
최대 비밀번호 유효 기간(1~730일 또는 없음)	암호를 변경해야 하는 날짜
비밀번호 기록(1~50개 비밀번호 또는 없음)	재사용 전 고유 암호 개수

인증서

PKCS#1	
설명	인증서에 대한 설명을 입력합니다.
자격 증명	pkcs1 파일 업로드

PKCS#12	
설명	인증서에 대한 설명을 입력합니다.
자격 증명	pkcs12 파일 업로드

제한 설정

디바이스 기능

카메라 허용	카메라 사용 허용
게임 센터 허용	거짓이면 게임 센터가 비활성화되고 홈 화면에서 해당 아이콘이 제거됩니다.
멀티플레이어 게임 허용	거짓이면 멀티플레이어 게임을 금지합니다.
게임 센터 친구 추가 허용	거짓인 경우, 게임 센터에 친구 추가를 금지합니다.
iCloud 사진 보관함 허용	false로 설정하면 iCloud 사진 보관함을 비활성화합니다. iCloud 사진 보관함에서 장치로 완전히 다운로드되지 않은 사진은 로컬 저장 공간에서 제거됩니다.
터치 ID 허용	거짓이면 Touch ID가 장치의 잠금을 해제하지 못하도록 합니다.

iCloud

iCloud 페어링 중 특정 기능 차단하기

문서 동기화 허용	문서 동기화 허용
iCloud 키체인 동기화 허용	iCloud 키체인 동기화 허용
iCloud 메모 허용	거짓인 경우, MacOS iCloud Notes 서비스를 허용하지 않습니다.
iCloud BTMM 허용	거짓인 경우, MacOS 내 Mac으로 돌아가기 iCloud 서비스를 허용하지 않습니다.
iCloud FMM 허용	거짓인 경우, MacOS 나의 Mac 찾기 iCloud 서비스를 허용하지 않습니다.
iCloud 책갈피 허용	거짓인 경우, MacOS iCloud 책갈피 동기화를 허용하지 않습니다.
iCloud 메일 허용	거짓인 경우, MacOS Mail iCloud 서비스를 허용하지 않습니다.
iCloud 캘린더 허용	거짓인 경우, MacOS 클라우드 iCloud 서비스를 허용하지 않습니다.
iCloud 미리 알림 허용	거짓이면 iCloud 미리 알림 서비스를 허용하지 않습니다.
iCloud 주소록 허용	거짓인 경우, MacOS iCloud 주소록 서비스를 허용하지 않습니다.

미디어 관리

로그아웃 시 꺼내기	로그아웃 시 모든 이동식 미디어 꺼내기
네트워크 허용	네트워크 미디어에 대한 액세스 허용
내부 디스크 허용	내부 디스크에 대한 액세스를 허용합니다.
인증 필요	이 미디어를 사용하려면 인증이 필요합니다.
읽기 전용	사용자는 미디어에서 데이터만 읽을 수 있습니다.
외부 디스크 허용	외부 디스크에 대한 액세스를 허용합니다.
인증 필요	이 미디어를 사용하려면 인증이 필요합니다.
읽기 전용	사용자는 미디어에서 데이터만 읽을 수 있습니다.
디스크 이미지 사용 허용	이미지에 대한 액세스를 허용합니다.
인증 필요	이 미디어를 사용하려면 인증이 필요합니다.
읽기 전용	사용자는 미디어에서 데이터만 읽을 수 있습니다.
DVD-RAM 사용 허용	DVD-RAM 디스크에 대한 액세스를 허용합니다.
인증 필요	이 미디어를 사용하려면 인증이 필요합니다.
읽기 전용	사용자는 미디어에서 데이터만 읽을 수 있습니다.
DVD 사용 허용	DVD 디스크에 대한 액세스를 허용합니다.
인증 필요	이 미디어를 사용하려면 인증이 필요합니다.
CD 사용 허용	CD 디스크에 대한 액세스를 허용합니다.
인증 필요	이 미디어를 사용하려면 인증이 필요합니다.

연결 관리

Wi-Fi

여기에서 Wi-Fi 연결을 추가하고 구성할 수 있습니다.

서비스 세트 식별자 (SSID)	연결이 설정될 네트워크의 SSID입니다.
자동 가입	네트워크에 자동 가입 사용
숨겨진 네트워크	AP가 SSID를 브로드캐스트하지 않는 경우 활성화합니다.
프록시 설정	모든 액세스 포인트에 대한 프록시 구성
없음	프록시 서버를 사용하지 마세요.
매뉴얼	수동 프록시 설정
프록시 서버 URL	프록시 설정에 액세스하기 위한 주소
포트	프록시용 포트 설정
인증	프록시에서 인증할 사용자 이름
비밀번호	프록시에서 인증하기 위한 비밀번호
자동	자동으로 프록시 설정
프록시 서버 URL	프록시 설정 파일의 URL
보안 유형	AP의 보안 유형 설정
WEP	
비밀번호	AP의 비밀번호
WPA/WPA2	
비밀번호	AP의 비밀번호
WEP 엔터프라이즈 - WPA / WPA2 엔터프라이즈 / 모든 기업	표 오류를 참조하십시오: 아래에서 참조 소스를 찾을 수 없습니다.
없음	보안 설정 안 함
MAC 주소 무작위 지정 비활성화	네트워크에 연결되어 있는 동안 해당 Wi-Fi 네트워크에 대한 MAC 주소 무작위화를 비활성화합니다. 또한 설정에 개인정보 보호 경고가 표시되어 네트워크의 개인정보 보호 기능이 약화되었음을 나타냅니다.

엔터프라이즈 Wi-Fi 구성

참고: '보안 유형'이 기업 유형으로 설정된 경우에만 사용할 수 있습니다.

프로토콜	대상 네트워크에서 지원되는 인증 프로토콜
TLS	사용 활성화/비활성화
TTLS	사용 활성화/비활성화
내부 인증	사용해야 하는 인증 프로토콜: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	사용 활성화/비활성화
PEAP	사용 활성화/비활성화
EAP-FAST	사용 활성화/비활성화
EAP-SIM	사용 활성화/비활성화
PAC 사용	PAC(보호 액세스 제어) 사용
프로비저닝 PAC	프로비저닝 PAC 구성
익명으로 PAC 프로비저닝	PAC의 익명 제공
인증	
사용자 이름	인증 사용자 이름
사용하지 마십시오. 연결당 비밀번호	연결별 비밀번호를 사용하지 마세요.
비밀번호	사용할 비밀번호
신원 증명서	인증 인증서 업로드/선택
외부 정체성	외부에서 볼 수 있는 신원
신뢰	
신뢰할 수 있는 인증서 1	첫 번째 신뢰할 수 있는 인증서 업로드
신뢰할 수 있는 인증서 2	두 번째 신뢰할 수 있는 인증서 업로드
신뢰할 수 있는 인증서 3	신뢰할 수 있는 세 번째 인증서 업로드
신뢰할 수 있는 서버 인증서 이름	예상 서버 인증서의 이름 (쉼표로 구분된 목록)

VPN

선택한 연결 유형에 따라 다른 필드가 표시될 수 있습니다.

연결 이름	VPN 프로필 이름
VPN 유형	
VPN	모든 기기 네트워크 트래픽은 VPN 연결을 통해 라우팅됩니다.
연결 유형	VPN 연결 유형 설정
IPsec(cisco)	시스코의 IPsec 프로토콜
L2TP	L2TP 프로토콜
사용자 지정 SSL	사용자 지정 SSL을 통한 연결
IKEv2	IKEv2 프로토콜
프록시 설정	VPN 연결을 위한 프록시 구성
없음	프록시 설정 안 함
매뉴얼	수동으로 프록시 설정
프록시 서버 URL	프록시 설정에 액세스할 수 있는 주소
포트	프록시용 포트 설정
인증	프록시에서 인증할 사용자 이름
비밀번호	프록시에서 인증을 위한 비밀번호
자동	자동으로 프록시 설정
프록시 서버 URL	프록시 설정에 액세스하기 위한 URL

HTTP 프록시

프록시 유형	
매뉴얼	수동으로 프록시 설정
프록시 서버 URL	프록시 설정에 액세스할 수 있는 주소
포트	프록시 포트 설정
인증	프록시에서 인증할 사용자 이름
비밀번호	프록시에서 인증을 위한 비밀번호
자동	자동으로 프록시 설정
프록시 PAC URL	프록시 PAC URL
PAC에 연결할 수 없는 경우 직접 연결 허용	PAC에 연결할 수 없는 경우 직접 연결 허용(VPN 없이)
프록시를 우회하여 캡티브 네트워크에 액세스하도록 허용	프록시를 우회하여 종속 내부 네트워크에 액세스하도록 허용

AirPrint

IP 주소	프린터 IP 주소
리소스 경로	AirPrint 장치로 가는 확실한 경로

AirPlay

장치 이름	장치 이름
비밀번호	페어링 비밀번호
화이트리스트	디바이스가 독점적으로 페어링할 수 있는 디바이스 목록을 정의합니다.

PIM 관리

Exchange Active 동기화

계정 이름	계정 이름입니다.
이메일 주소	계정의 주소(예: max@company.com)
서버 호스트 이름	내부 호스트 이름
로그인 이름	'도메인'과 '로그인 이름'은 비워 두어야 장치에서 사용자에게 메시지를 표시합니다.
도메인	'도메인'과 '로그인 이름'은 비워 두어야 장치에서 사용자에게 메시지를 표시합니다. ACL 게이트웨이 구성이 활성화되어 있고 도메인 필드가 비어 있지 않으면 AppTec360 범용 게이트웨이는 다음 이름 "도메인\로그인 이름"으로 장치를 인증합니다.
비밀번호	계정의 비밀번호(예: 비밀사용자 비밀번호)
동기화할 메일의 지난 날짜	동기화할 메일의 과거 일수
SSL 사용	내부 Exchange 호스트에 SSL 사용
고급 옵션	고급 옵션 표시
서버 포트	내부 포트
서버 경로	내부 경로
외부 호스트 이름	외부 호스트
외부 포트	외부 포트
외부 경로	외부 경로
외부용 SSL 사용 교환 호스트	외부 Exchange 호스트에 SSL 사용

이메일

최종 사용자 디바이스에서 POP3 / IMAP 계정 설정

계정 설명	이메일 계정 이름
계정 유형	
IMAP	
경로 접두사	특수 폴더의 경로 접두사
POP	
사용자 표시 이름	사용자 표시 이름
이메일 주소	사용자 이메일 주소

수신 메일	수신 서버 설정
메일 서버 주소	메일 서버 주소
메일 서버 포트	메일 서버 포트
사용자 이름	각 사용자 이름
인증 유형	인증 유형
없음	인증 유형 없음
비밀번호(디바이스 수준에서만)	비밀번호 프롬프트
MDM 도전 과제-대응	
NTLM	NTLM-인증
HTTP MD5 다이제스트	
SSL 사용	필요한 경우 SSL 사용

발신 메일	발신 서버 설정
메일 서버 주소	메일 서버 주소
메일 서버 포트	메일 서버 포트
사용자 이름	각 사용자 이름
인증 유형	
없음	인증 방법 없음
비밀번호(디바이스 수준에서만)	비밀번호 프롬프트
MDM 도전 과제-대응	
NTLM	NTLM-인증
HTTP MD5 다이제스트	
SSL 사용	필요한 경우 SSL 사용
수신 비밀번호와 동일한 발신 비밀번호	수신 비밀번호와 동일한 발신 비밀번호
메일에서만 사용	모든 발신 이메일을 메일 앱을 통해 보내려면 활성화합니다.

CalDav

CalDav 계정의 설정 및 배포를 구성합니다.

계정 설명	계정의 표시 이름
호스트 이름	호스트 이름 및/또는 IP 주소
포트	CalDav 계정의 포트
주요 URL	계정의 기본 URL
사용자 이름	각 CalDav 사용자 이름
비밀번호(디바이스 수준에서만)	각 CalDav 비밀번호
SSL 사용	필요한 경우 SSL 사용

CardDav

CardDav 계정의 설정 및 배포를 구성합니다.

계정 설명	계정의 표시 이름
호스트 이름	호스트 이름 및/또는 IP 주소
포트	CardDav 계정의 포트
주요 URL	계정의 기본 URL
사용자 이름	각 CardDav 사용자 이름
비밀번호(디바이스 수준에서만)	각 CardDav 비밀번호
SSL 사용	필요한 경우 SSL 사용

LDAP

이 영역에서 최종 사용자 장치와 Active Directory 간에 동적 인증서 교환을 허용하기 위해 LDAP 연결을 설정합니다.

선택한 사용자에게는 해당 읽기 권한이 필요합니다.

계정 설명	계정 설명
계정 사용자 이름	LDAP 액세스용 사용자
계정 비밀번호	LDAP 액세스를 위한 비밀번호
계정 호스트 이름	LDAP 서버 호스트 이름/IP 주소
SSL 사용	필요한 경우 SSL 사용

두 번째 부분에서는 LDAP 레지스트리에서 검색할 개별 필터를 정의할 수 있습니다.

설명	범위	검색 기반
필터 설명	LDAP 레지스트리의 검색 수준	개별 필터 정의

대시보드 및 보고

대시보드 설정

여기에서 어떤 대시보드가 있는지 확인하고, 편집하거나 새 대시보드를 만들 수 있습니다. 각 대시보드에는 표시할 고유한 데이터 세트와 그래프 구성이 있습니다.

대시보드 설정 제어

공개	대시보드를 공개로 설정하여 다른 사용자가 대시보드를 볼 수 있도록 합니다. 물론 사용자는 로그인하여 대시보드를 볼 수 있어야 합니다. '공개'를 활성화하지 않으면 작성자만 대시보드를 볼 수 있습니다.
기본값	다음에 대시보드 보기에 액세스할 때 대시보드가 자동으로 열리도록 기본값으로 설정합니다.
	대시보드 및 그래프 표시
	대시보드 삭제
	대시보드 이름 및 설정 편집
	대시보드 사본 만들기
	완전히 새로운 대시보드 추가

대시보드 보기

선택한 대시보드의 데이터 및 그래프가 표시되며 이를 변경할 수도 있습니다.

대시보드 제어

	대시보드에 표시할 데이터, 표시할 데이터의 양 및 이러한 데이터를 표시할 크기를 정의할 수 있습니다.
	대시보드 개요로 돌아갑니다.
	현재 열려 있는 대시보드를 기본값으로 초기화합니다.
	현재 열려 있는 대시보드에 대한 모든 변경 사항(예: 표시할 데이터)을 저장합니다.
	차트 유형을 기둥 차트로 변경
	차트 유형을 원형 차트로 변경
	차트 유형을 도넛 차트로 변경
	차트 유형을 극좌표형 차트로 변경
	정렬 순서 변경

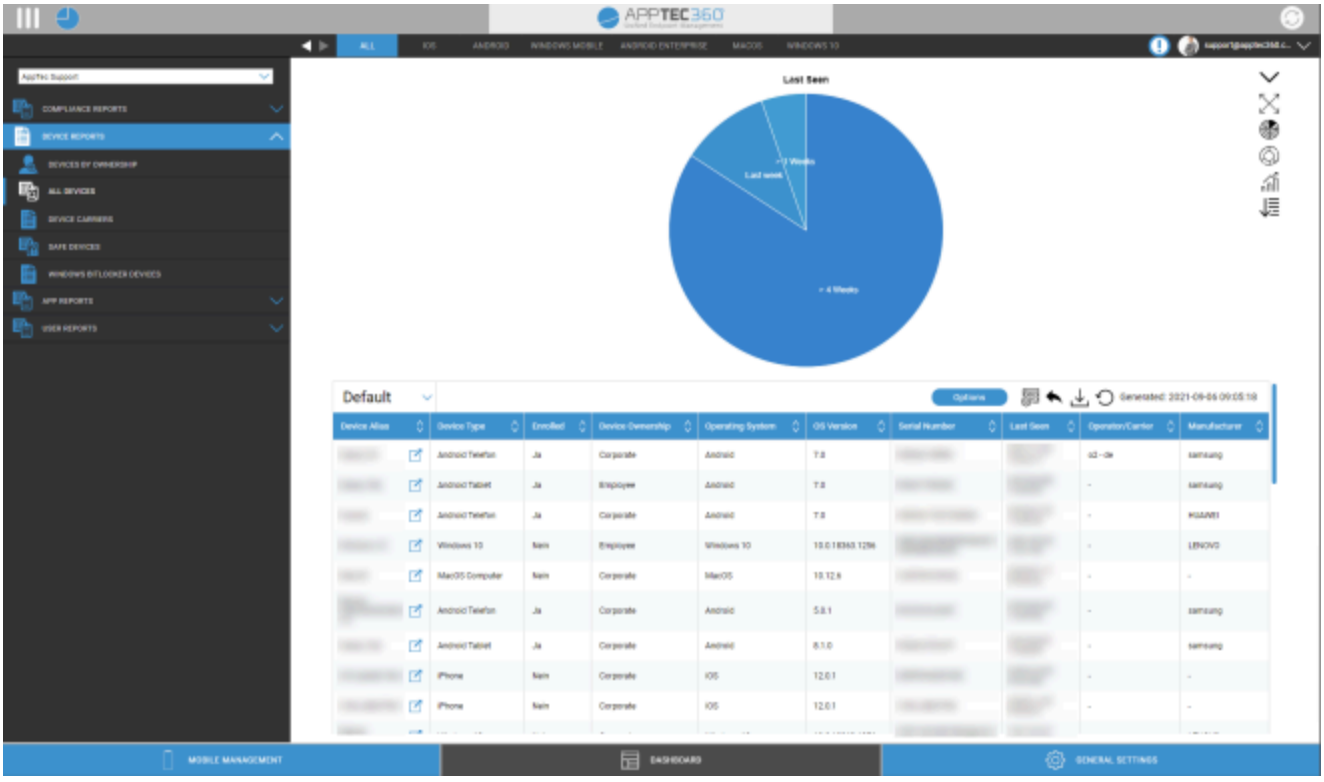
확장 보고

'확장 보고'는 디바이스 및 사용자 정보에 대한 자세한 개요와 그래프를 제공합니다.

몇 가지 기본 보고서가 있지만 모두 수동으로 변경하여 표시할 데이터를 추가하거나 제거할 수 있습니다.

표시되는 데이터는 수동으로만 변경할 수 있다는 점에 유의하세요. 선택한 보고서 카테고리에 따라 보고서의 기준이 되는 데이터가 정의됩니다. 예를 들어 디바이스 보고서 모든 디바이스 iOS의 iOS 보고서에는 Android 디바이스를 볼 수 없습니다.

왼쪽 상단에서 보고 데이터를 특정 그룹(및 모든 하위 그룹)으로 제한할 수 있습니다. 기본적으로 이 기능은 루트 노드로 설정되어 있으므로 모든 디바이스와 사용자를 고려합니다.



확장된 보고 제어

각 개요에서 다음 기능을 사용하여 원하는 방식으로 보고서를 변경할 수 있습니다:

	차트 숨기기(차트가 표시된 경우)
	차트 표시(차트가 숨겨져 있는 경우)
	차트 펼치기(차트가 접힌 경우)
	차트 축소(차트가 확장된 경우)
	차트 유형을 기둥 차트로 변경
	차트 유형을 원형 차트로 변경
	차트 유형을 도넛 차트로 변경
	차트 유형을 극좌표형 차트로 변경
	정렬 순서 변경
	표시된 개요에 대해 다음 부분을 수정합니다: • 열 추가/제거 • 열이 표시되는 순서를 지정합니다. • 표 위의 차트 표시/숨기기 • 차트에 사용되는 열을 선택합니다. • 테이블의 데이터 필터링
	설정 관리자를 열어 다양한 보고서를 저장하고 로드합니다.
	현재 열려 있는 보고서를 기본값으로 재설정합니다.
	현재 보고서를 .csv 파일로 내보내기
	데이터 재생성 및 현재 보고서 다시 로드하기

다음 페이지에서 모든 기본 보고서 목록을 확인할 수 있습니다.

규정 준수 보고서

루팅된 디바이스

루팅/탈옥된 디바이스 개요.

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일
운영 체제
전화번호
마지막으로 본
제조업체

로밍 장치

로밍 중인 모든 디바이스 개요

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일
디바이스 유형
운영 체제
전화번호
마지막으로 본

로밍 지원 장치

로밍을 활성화했지만 현재 로밍 중이 아닌 모든 장치에 대한 개요입니다.

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일
디바이스 유형
운영 체제
전화번호
마지막으로 본

감독 대상 장치

감독 모드에서 감독되는 모든 디바이스 개요(iOS만 해당)

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일
디바이스 유형
마지막으로 본

비활성 장치

지난 7일 동안 서버에 연결하지 않은 모든 디바이스 개요

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일
디바이스 유형
운영 체제
마지막으로 본

디바이스 보고서

소유권별 디바이스

여기에서 현재 회사(회사 디바이스) 및 직원(개인 디바이스)으로 배포된 디바이스 수를 확인할 수 있습니다.

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
디바이스 유형
디바이스 소유권
운영 체제

모든 디바이스

여기에서 가장 중요한 정보가 포함된 모든 디바이스의 개요를 확인할 수 있습니다.

이 보고서의 기본 열입니다:

장치 별칭
디바이스 유형
등록
디바이스 소유권
운영 체제
OS 버전
일련 번호
마지막으로 본
사업자/이동 통신사
제조업체

디바이스 이동 통신사

여기에서 이동 통신사(이동통신사)에 대한 개요를 확인할 수 있습니다.

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일
운영 체제
OS 버전
사업자/이동 통신사

안전한 장치

여기에서 SAFE 버전을 사용하는 기기에 대한 개요를 확인할 수 있습니다.

개요 및/또는 SAFE는 삼성 디바이스에서만 사용할 수 있으므로 이 시점에서는 일반적인 탭이 표시되지 않습니다.

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일
디바이스 유형
마지막으로 본
SAFE 버전

Windows BitLocker 장치

여기에서 BitLocker를 사용하는 Windows 장치에 대한 개요를 볼 수 있습니다.

이 보고서의 기본 열입니다:

장치 별칭
디바이스 소유자
이메일

비트락커 상태

앱 보고서

여기에서 앱과 관련된 다양한 개요를 확인할 수 있습니다. 이러한 모든 보고서에서 항목을 클릭하면 디바이스에 설치된 버전과 설치 빈도를 자세히 확인할 수 있습니다. 이 보기에서 특정 버전을 다시 클릭하면 특정 버전이 설치된 디바이스를 확인할 수 있습니다.

참고: 시스템이 디바이스에서 최신 정보를 가져올 때까지 다소 시간이 걸릴 수 있습니다. 또한 보고서는 매분마다 업데이트되지 않습니다. 새 앱이나 버전을 방금 할당했다면 현재 상태를 확인하려면 조금 기다려야 할 수도 있습니다. 보고서를 수동으로 다시 로드하면 보고서에 사용 가능한 가장 최신 데이터가 표시되도록 강제 적용됩니다.

설치된 앱

여기에서 설치된 모든 앱의 개요를 볼 수 있습니다.

이 보고서의 기본 열입니다:

이름	해당 앱 및/또는 서비스 이름
식별자	명확한 앱/서비스 ID
총 개수	이 앱/서비스가 최종 사용자 디바이스에 설치된 빈도

가장 많이 설치된 앱

여기에서 가장 많이 설치된 앱에 대한 개요를 확인할 수 있습니다.

이 보고서의 기본 열입니다:

이름	해당 앱 및/또는 서비스 이름
식별자	명확한 앱/서비스 ID
총 개수	이 앱/서비스가 최종 사용자 디바이스에 설치된 빈도

필수 앱

여기에서 필수(의무적으로 설치해야 하는) 앱에 대한 개요를 확인할 수 있습니다.

이 보고서의 기본 열입니다:

이름	해당 앱 및/또는 서비스 이름
식별자	명확한 앱/서비스 ID
앱 소스	어떤 앱스토어가 관련되어 있는지 확인합니다: • 구글 플레이스토어(Android) • iTunes AppStore(iOS)
OS	운영 체제

블랙리스트 앱

여기에서 정의된 모든 블랙리스트 앱의 개요를 확인할 수 있습니다.

이 보고서의 기본 열입니다:

이름	해당 앱 및/또는 서비스 이름
식별자	명확한 앱/서비스 ID
앱 소스	어떤 앱스토어가 관련되어 있는지 확인합니다: • 구글 플레이스토어(Android) • iTunes AppStore(iOS)
OS	운영 체제

사용자 보고서

관세

여기에서 사용자의 휴대폰 요금과 SIM 카드에 대한 개요를 확인할 수 있습니다.

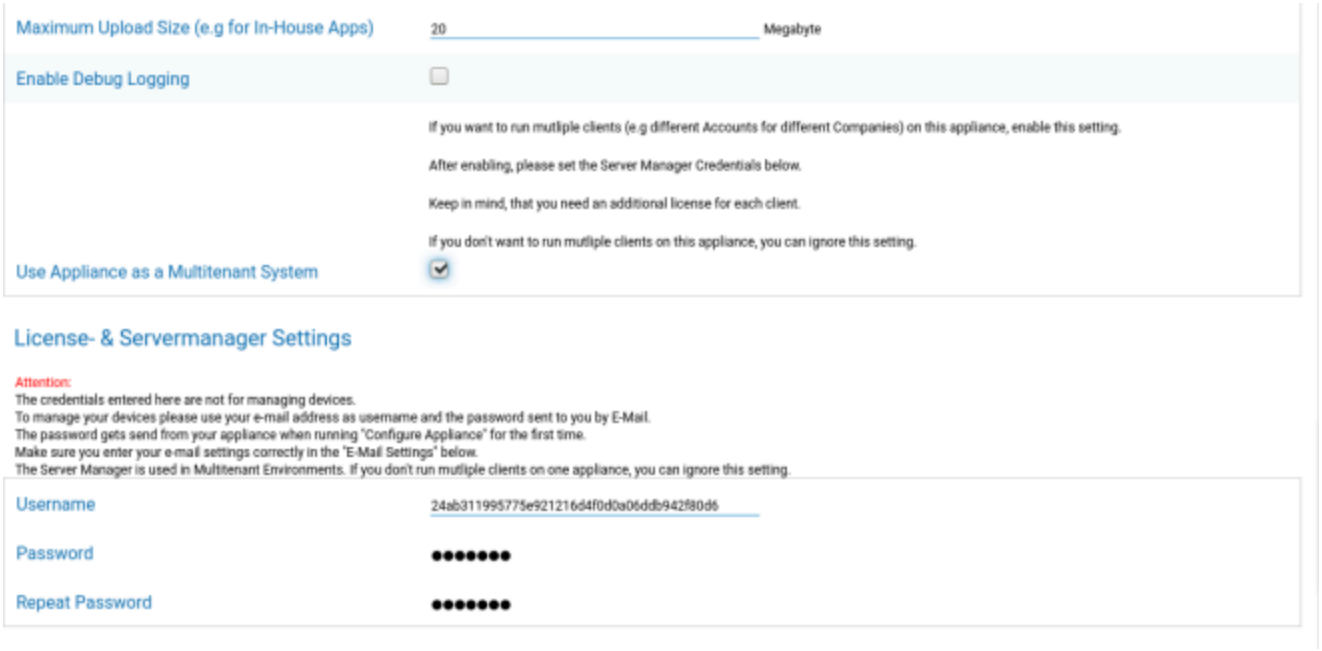
이 보고서의 기본 열입니다:

이메일
이름
전화 번호
캐리어
관세
옵션
가격
계약 취소
계약 시작
동안 시간
모바일 및 데이터
데이터 볼륨
멀티심
유형
simCardSerial1
simCardSerial2
simCardSerial3
핀1
핀2
puk1
puk2
참고

멀티테넌트 관리

AppTec360 EMM은 각각 고유한 사용자 및 그룹, 권한 및 글로벌 설정을 가진 여러 개의 개별 테넌트를 호스팅 할 수 있습니다.

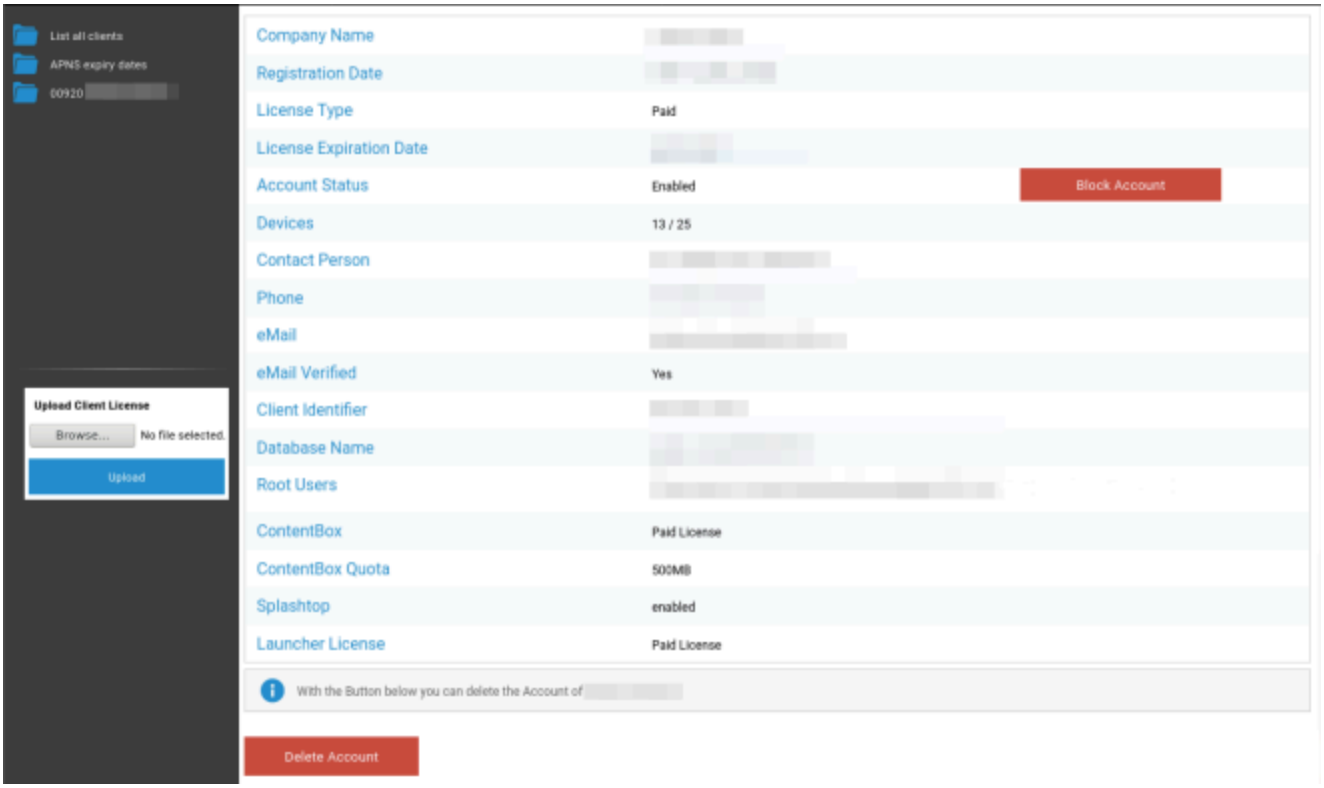
멀티테넌트 기능을 사용 설정하려면 "3단계 - 서버 설정"의 어플라이언스 구성 인터페이스에서 해당 기능을 사용 설정해야 합니다.



새 메뉴에서 Servermanager의 사용자 이름과 비밀번호를 설정합니다. 설정을 저장하고 '5단계 - 라이선스 계약'의 '어플라이언스 구성'을 실행하여 설정을 적용합니다.

구성이 완료되면 이제 일반 모바일 관리 인터페이스를 통해 설정된 자격 증명으로 로그인할 수 있습니다.

로그인하면 다음과 같은 화면을 볼 수 있습니다.



왼쪽에는 모든 테넌트(이 경우에는 ID가 920인 테넌트 하나만)가 표시되고 오른쪽에는 이 클라이언트에 대한 정보가 표시됩니다. 또한 계정에 대한 액세스를 차단하고 클라이언트를 삭제하는 옵션도 있습니다(주의: 이렇게 하면 해당 클라이언트와 관련된 모든 데이터가 제거됩니다).

왼쪽에서 기존 클라이언트의 라이선스 업데이트 또는 새 클라이언트를 자동으로 생성하는 새 라이선스 중 하나를 업로드할 수 있습니다. 새 클라이언트가 생성되면 로그인 비밀번호가 포함된 이메일이 라이선스가 발급된 이메일 주소로 자동으로 전송됩니다.

신규 또는 업데이트된 클라이언트 라이선스를 받으려면(예: 디바이스 라이선스가 더 필요한 경우) 영업 담당자에게 문의하세요.

추가 보기

모든 클라이언트 목록

시스템의 모든 클라이언트에 대한 개요를 표시합니다.

클라이언트 ID	클라이언트 ID
식별자	클라이언트 식별자
데이터베이스	데이터베이스
회사 이름	회사 이름
이메일	담당자 이메일
확인됨	담당자 이메일 확인 여부
국가	국가
디바이스	등록된 디바이스 수
등록 날짜	라이선스 할당 시점
마지막 로그인	마지막 관리자 계정 로그인
라이선스	라이선스 유형 표시(무료|유료)
CB 라이선스	ContentBox 라이선스 유형(무료|유료)
상태	현재 앱텍-클라이언트 상태
만료됨	라이선스가 만료된 경우 표시됨
iOS	iOS 기기 수
Android	Android 기기 수
Windows 모바일	Windows 모바일 장치 수
MacOS	MacOS 장치 수
Windows 10	Windows 10 장치 수
Android 엔터프라이즈	Android 기업용 디바이스 수
IOS BYOD(사용자 등록)	IOS BYOD(사용자 등록) 디바이스 수
IoT	IoT 디바이스 수

APNS 만료 날짜

모든 클라이언트의 모든 APNS 인증서 만료 날짜에 대한 개요를 표시합니다.

클라이언트 ID	클라이언트 ID
회사 이름	회사 이름
만료 날짜	Apple APNS 인증서의 만료일
정보	만료에 대한 정보

연락처

추가 질문이 있으신가요? 아래에서 문의해 주세요:

일반적인 기술 관련 질문

support@apptec360.com

+41 61 511 3210

가상 어플라이언스 설치와 관련된 질문은 다음과 같이 문의하세요.

consulting@apptec360.com

+41 61 511 3214

면책 조항