



XenMobile Server 현재릴리스

Contents

XenMobile Server 10.11 의새로운기능	3
XenMobile Server 10.10 의새로운기능	11
XenMobile Server 10.9 의새로운기능	16
타사고지사항	19
수정된문제	20
알려진문제	21
아키텍처	22
시스템요구사항및호환성	24
XenMobile 호환성	27
지원되는장치운영체제	29
포트요구사항	31
확장성및성능	39
라이선스	42
FIPS 140-2 준수	47
언어지원	48
설치및구성	50
XenMobile 을사용하여 FIPS 구성	67
클러스터링구성	70
재해복구가이드	81
프록시서버사용	81
SQL Server 구성	84
서버속성	87
CLI(명령줄인터페이스) 옵션	101

XenMobile 콘솔에대한워크플로시작하기	115
인증서및인증	119
NetScaler Gateway 및 XenMobile	129
도메인인증또는도메인및보안토큰인증	138
클라이언트인증서인증또는인증서와도메인인증	145
PKI 엔터티	166
자격증명공급자	192
APNs 인증서	198
ShareFile SSO(Single Sign-on) 용 SAML	204
IDP 역할을하는 Azure Active Directory	213
파생된자격증명	226
업그레이드	244
사용자계정, 역할및등록	248
RBAC 를사용하여역할구성	263
알림	281
장치	292
ActiveSync Gateway	299
장치관리에서 Android Enterprise 로마이그레이션	301
Android Enterprise	307
G Suite 고객을위한레거시 Android Enterprise	356
iOS 및 macOS 장치의대량등록	398
클라이언트속성	412
Apple DEP 를통해 iOS 및 macOS 장치배포	422
장치등록제한	432

장치등록	434
Firebase Cloud Messaging	462
Apple 교육기능과통합	467
네트워크액세스제어	502
Samsung KNOX	504
보안동작	505
공유장치	516
XenMobile Autodiscovery Service	520
장치정책	526
플랫폼별장치정책	540
AirPlay 미러링장치정책	541
AirPrint 장치정책	543
Android Enterprise 관리되는구성정책	544
Android Enterprise 권한	553
APN 장치정책	554
앱액세스장치정책	557
앱특성장치정책	558
앱구성장치정책	559
앱인벤토리장치정책	561
앱잠금장치정책	561
앱네트워크사용장치정책	564
앱알림장치정책	564
앱제한장치정책	565
앱터널링장치정책	566

앱제거장치정책	569
앱제거제한장치정책	570
BitLocker 장치정책	571
브라우저장치정책	575
캘린더 (CalDav) 장치정책	576
셀룰러장치정책	576
연결관리자장치정책	577
연결예약장치정책	577
연락처 (CardDAV) 장치정책	579
OS 업데이트제어장치정책	580
Samsung 컨테이너에앱복사장치정책	585
자격증명장치정책	585
사용자지정 XML 장치정책	591
Defender 장치정책	592
파일및폴더장치정책삭제	594
레지스트리키값삭제장치정책	594
장치상태증명장치정책	594
장치이름장치정책	596
교육구성장치정책	597
엔터프라이즈허브장치정책	599
Exchange 장치정책	600
파일장치정책	608
FileVault 장치정책	609
글꼴장치정책	611

휴화면레이아웃장치정책	612
iOS 및 macOS 프로필장치정책가져오기	613
키오스크장치정책	614
Android 에대한 Launcher 구성장치정책	617
LDAP 장치정책	618
위치장치정책	619
메일장치정책	624
관리되는도메인장치정책	626
MDM 옵션장치정책	628
조직정보장치정책	629
암호장치정책	630
개인핫스팟장치정책	641
프로필제거장치정책	641
프로비전프로필장치정책	642
프로비전프로필제거장치정책	643
프록시장치정책	644
레지스트리장치정책	645
원격지원장치정책	646
제한장치정책	647
로밍장치정책	675
Samsung MDM 라이선스키장치정책	676
Samsung SAFE 방화벽장치정책	678
SCEP 장치정책	679
Siri 및받아쓰기정책	681

SSO 계정장치정책	683
스토리지암호화장치정책	684
스토어장치정책	685
구독캘린더장치정책	685
약관장치정책	686
VPN 장치정책	687
배경화면장치정책	725
웹콘텐츠필터장치정책	726
웹클리프장치정책	727
WiFi 장치정책	728
Windows CE 인증서장치정책	741
Windows Information Protection 장치정책	742
XenMobile 옵션장치정책	746
XenMobile 제거장치정책	748
앱추가	748
앱커넥터유형	786
MDX 또는엔터프라이즈앱업그레이드	787
MDX 앱정책요약	788
XenMobile Store 및 Citrix Secure Hub 브랜딩	789
Citrix Launcher	790
iOS Volume Purchase Program	793
Citrix Secure Hub 를통한 Virtual Apps and Desktops	799
XenMobile 에서 ShareFile 사용	800
HDX 앱용 SmartAccess	815

미디어추가	833
리소스배포	838
매크로	851
자동화된동작	881
모니터링및지원	888
지원번들의데이터익명화	891
연결확인	892
사용자환경개선프로그램	895
로그	897
모바일서비스공급자	904
보고서	905
SNMP 모니터링	909
지원번들	917
지원옵션및원격지원	921
SysLog	928
XenMobile 에서로그파일보기	929
XenMobile Analyzer 도구	931
REST API	950
Exchange ActiveSync 용 Endpoint Management 커넥터	952
Exchange ActiveSync 용 Citrix Gateway 커넥터	998
고급개념	1010
온-프레미스 XenMobile 과 Active Directory 상호작용	1010
XenMobile 배포	1013
관리모드	1015

장치요구사항	1020
보안및사용자환경	1021
앱	1036
사용자커뮤니티	1041
전자메일전략	1047
XenMobile 통합	1054
다중사이트요구사항	1062
NetScaler Gateway 및 NetScaler 통합	1063
MDX 앱에대한 SSO 및프록시고려사항	1072
인증	1077
온-프레미스배포용참조아키텍처	1088
서버속성	1099
장치및앱정책	1100
사용자등록옵션	1109
XenMobile 작업조정	1112
앱프로비전및프로비전해제	1119
대시보드기반작업	1123
역할기반액세스제어및 XenMobile 지원	1124
시스템모니터링	1126
재해복구	1133
Citrix 지원프로세스	1137
XenMobile 에서그룹등록초대보내기	1138
온-프레미스장치상태증명서버구성	1139
Secure Mail 푸시알림을통한 EWS 의인증서기반인증구성	1149

XenMobile Server 10.11 의새로운기능

January 6, 2020

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

Apple VPP(Volume Purchase Program) 를사용하는회사및교육기관에서는 2019 년 12 월 1 일전에 Apple Business Manager 또는 Apple School Manager 의앱및서적으로마이그레이션해야합니다.

XenMobile 에서 VPP 계정을마이그레이션하기전에이 [Apple 지원문서](#)를참조하십시오.

조직또는학교에서 VPP(Volume Purchase Program) 만사용하는경우 ABM/ASM 에등록한다음기존 VPP 구매자를 새 ABM/ASM 계정으로초대할수있습니다. ASM 의경우 <https://school.apple.com>으로이동합니다. ABM 의경우 <https://business.apple.com>으로이동합니다.

XenMobile 에서볼륨구매 (이전 VPP) 계정을업데이트하려면:

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 볼륨구매를클릭합니다. 볼륨구매구성페이지가나타납니다.
3. ABM 또는 ASM 계정에이전 VPP 계정과동일한앱구성이있는지확인합니다.
4. ABM 또는 ASM 포털에서업데이트된토큰을다운로드합니다.
5. XenMobile 콘솔에서다음을수행합니다.
 - a) 해당위치에대한업데이트된토큰정보로기존볼륨구매계정을편집합니다.
 - b) ABM 또는 ASM 자격증명을편집합니다. 접미사를변경하지마십시오.
 - c) 저장을두번클릭합니다.

iOS 13 지원

중요:

iOS 12 이상으로장치를업그레이드하기위한준비: iOS 용 VPN 장치정책의 Citrix VPN 연결유형은 iOS 12 이상을지원하지않습니다. VPN 장치정책을삭제하고 Citrix SSO 연결유형으로새 VPN 장치정책을만듭니다.

VPN 장치정책을삭제한후 Citrix VPN 연결은이전에배포된장치에서계속작동합니다. 새 VPN 장치정책구성은사용자등록중에 XenMobile Server 10.11 에서적용됩니다.

XenMobile Server 는 iOS 13 으로업그레이드된장치를지원합니다. 업그레이드는사용자에게다음과같은영향을미칩니다.

- 등록하는동안몇개의새로운 iOS Setup Assistant(설정도우미) 옵션화면이나타납니다. Apple 은 iOS 13 에새로운 iOS Setup Assistant(설정도우미) 옵션화면을추가했습니다. 새옵션은이릴리스의 설정 > **Apple DEP**(장치등록프

로그) 페이지에 포함되지 않습니다. 따라서 이러한 화면을 건너뛰도록 XenMobile Server 를 구성할 수 없습니다. 이러한 페이지는 iOS 13 장치 사용자에게 나타납니다.

- iOS 13 이상에서는 이전 버전의 iOS 에 대한 감독 또는 감독되지 않은 장치에서 사용할 수 있었던 일부 제한 장치 정책 설정을 감독되는 장치에서만 사용할 수 있습니다. 현재 XenMobile Server 콘솔의 도구 설명에는 이러한 설정이 iOS 13 이상에서 감독되는 장치 전용이라는 설명이 표시되지 않습니다.
 - 하드웨어 제어 허용:
 - * FaceTime
 - * 앱 설치
 - 앱 허용:
 - * iTunes 스토어
 - * Safari
 - * Safari > 자동 채우기
 - 네트워크 - iCloud 동작 허용:
 - * iCloud 문서 및 데이터
 - 감독되는 경우에만 해당되는 설정 - 허용:
 - * 게임 센터 > 친구 추가
 - * 게임 센터 > 멀티플레이 게임
 - 미디어 콘텐츠 - 허용:
 - * 음악, 팟캐스트 및 iTunes U 의성인 등급 자료

이러한 제한은 다음과 같이 적용됩니다.

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

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

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

GCM 에서 FCM 으로 업그레이드

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

중요요구사항:

- 최신버전의 XenMobile Server 로업그레이드하십시오.
- 최신버전의 Secure Hub 로업그레이드하십시오.

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

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

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

업그레이드 단계:

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

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

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

XenMobile 마이그레이션 서비스

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

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

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

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

XenMobile 10.11 로 업그레이드하기 전에 (온-프레미스)

일부 시스템 요구사항이 변경되었습니다. 자세한 내용은 [시스템 요구사항 및 호환성](#) 및 [XenMobile 호환성](#)을 참조하십시오.

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

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

참고:

미리보기에자체라이센스를사용하려는경우 XenMobile 10.11 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2019 년 4 월 9 일이라는점을숙지하십시오. Citrix 라이선스의 Customer Success Services 날짜는이날짜보다이후여야합니다.

날짜는라이선스서버의라이선스옆에서볼수있습니다. 최신버전의 XenMobile 을이전버전의라이선스서버환경에 연결하면연결확인이실패하고라이선스서버를구성할수없게됩니다.

라이선스의날짜를갱신하려면 Citrix 포털에서최신라이선스파일을다운로드하고라이선스서버에파일을업로드하십시오. 자세한내용은 [Customer Success Services](#)에서참조하십시오.

- 클러스터된환경의경우: iOS 11 이상을실행하는장치에 iOS 정책및앱을배포하려면다음과같은요구사항이충족되어야합니다. NetScaler Gateway 에 SSL 지속성이구성되어있으면모든 XenMobile Server 노드에서포트 80 을열어야합니다.
- 업그레이드할 XenMobile Server 를실행하는가상컴퓨터의 RAM 이 4GB 미만인경우 4GB 이상으로 RAM 을늘리십시오. 프로덕션환경에권장되는최소 RAM 은 8GB 입니다.
- XenMobile 업데이트를설치하기전에 VM 의기능을사용하여시스템냅샷을생성합니다. 또한시스템구성데이터베이스를백업합니다. 업그레이드도중문제가발생하는경우전체백업을사용하여복구할수있습니다.

업그레이드하려면

XenMobile 10.10.x 또는 10.9.x 에서 XenMobile 10.11 로직접업그레이드할수있습니다. 업그레이드를수행하려면 Citrix [다운로드](#) 페이지에서제공되는최신 10.11 이진파일을사용합니다. 업그레이드를업로드하려면 XenMobile 콘솔의 릴리스관리페이지를사용합니다. 자세한내용은 [릴리스관리페이지를사용하여업그레이드하려면](#)에서참조하십시오.

업그레이드후

XenMobile 10.11 으로업그레이드한후 (온-프레미스):

연결구성을변경하지않았는데도발신연결이관련된기능이작동을중지하는경우 XenMobile Server 로그에다음과같은오류가있는지확인하십시오. “VPP Server 에연결할수없습니다. 호스트이름 ‘192.0.2.0’ 이피어가제공한인증서제목과일치하지않습니다.”

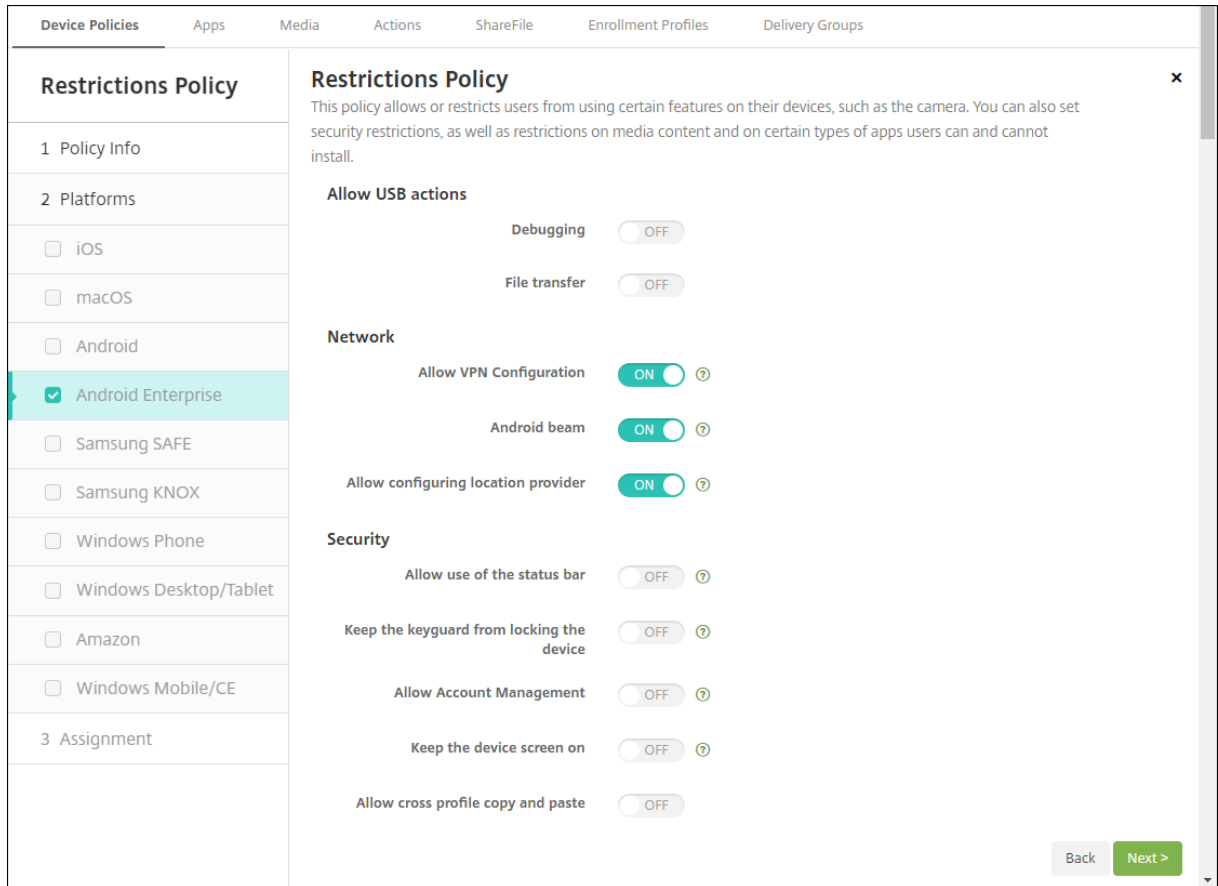
이인증서유효성검사로류는 XenMobile Server 에서호스트이름유효성검사를비활성화해야함을나타냅니다. 기본적으로호스트이름유효성검사는 Microsoft PKI 서버를제외한발신연결에대해활성화됩니다. 호스트이름유효성검사로인해배포가중단되는경우서버속성 `disable.hostname.verification` 을 `true` 로변경하십시오. 이속성의기본값은 `false` 입니다.

Android Enterprise 장치의신규및업데이트된장치정책설정

Samsung Knox 와 **Android Enterprise** 정책통합. Samsung Knox 3.0 이상과 Android 8.0 이상을실행하는 Android Enterprise 장치의경우: Knox 와 Android Enterprise 가통합장치및프로필관리솔루션으로결합됩니다.

다음장치정책의 Android Enterprise 페이지에서 Knox 설정을구성합니다.

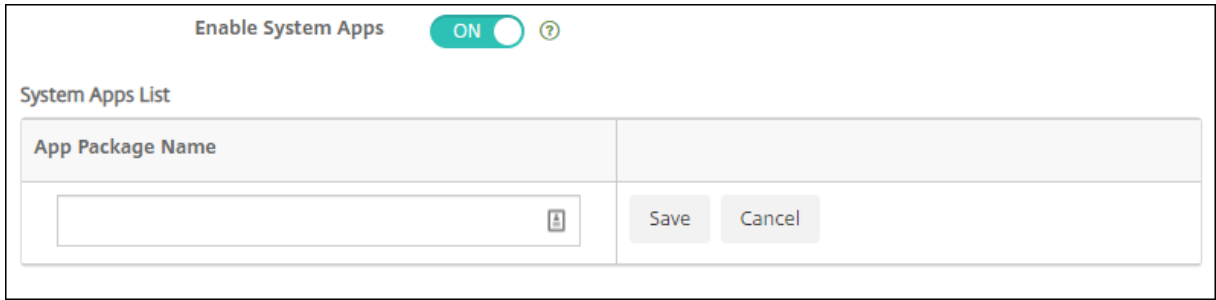
- **OS 업데이트장치정책.** Samsung Enterprise FOTA 업데이트에대한설정이포함되어있습니다.
- **암호장치정책.**
- **Samsung MDM 라이선스키장치정책.** Knox 라이선스키를구성합니다.
- **제한장치정책설정.**



Android Enterprise 의앱인벤토리장치정책. 이제관리되는장치에서 Android Enterprise 앱의인벤토리를수집할수있습니다. [앱인벤토리장치정책](#)에서자세한내용을참조하십시오.

관리되는 **Google Play Store** 의모든 **Google Play** 앱에액세스. 관리되는 **Google Play Store** 의모든앱에액세스서버속성을사용하면관리되는 Google Play Store 에서공용 Google Play Store 의모든앱에액세스할수있습니다. 이속성을 **true** 로설정하면모든 Android Enterprise 사용자에대한공용 Google Play Store 앱이화이트리스트에추가됩니다. 이후관리자는 [제한장치정책](#)을사용하여이러한앱에대한액세스를제어할수있습니다.

Android Enterprise 장치에서시스템앱사용. Android Enterprise 작업프로필모드또는완전관리되는모드에서사용자가 앱에미리설치된시스템앱을실행할수있도록하려면 [제한장치정책](#)을구성합니다. 이구성은카메라, 갤러리및기타기본장치앱에대한액세스권한을사용자에게부여합니다. 특정앱에대한액세스를제한하려면 [Android Enterprise 권한장치정책](#)을사용하여앱권한을설정합니다.



Android Enterprise 전용장치에대한지원. 이제 XenMobile 이 COSU(회사소유일회사용) 장치라고하는전용장치의관리를지원합니다.

전용 Android Enterprise 장치는단일사용사례를이행하는데전용으로사용되는완전관리되는장치입니다. 이러한장치는이사용 사례에필요한작업을수행하는데필요한단일앱또는소수의앱으로제한되어야합니다. 또한사용자가장치에서다른앱을사용하도록설정하거나다른작업을수행하지못하도록차단해야합니다.

Android Enterprise 장치프로비저닝에대한자세한내용은 [전용 Android Enterprise 장치프로비전](#)을참조하십시오.

정책이름변경. Google 용어에맞추기위해 Android Enterprise 앱제한장치정책의이름이이제 Android Enterprise 관리되는구성으로변경되었습니다. [Android Enterprise 관리되는구성장치정책](#)에서자세한내용을참조하십시오.

Android Enterprise 의잠금및암호재설정

XenMobile 은이제 Android Enterprise 장치에대한잠금및암호재설정보안동작을지원합니다. 이러한장치는 Android 8.0 이상을실행하는작업프로필모드에등록되어야합니다.

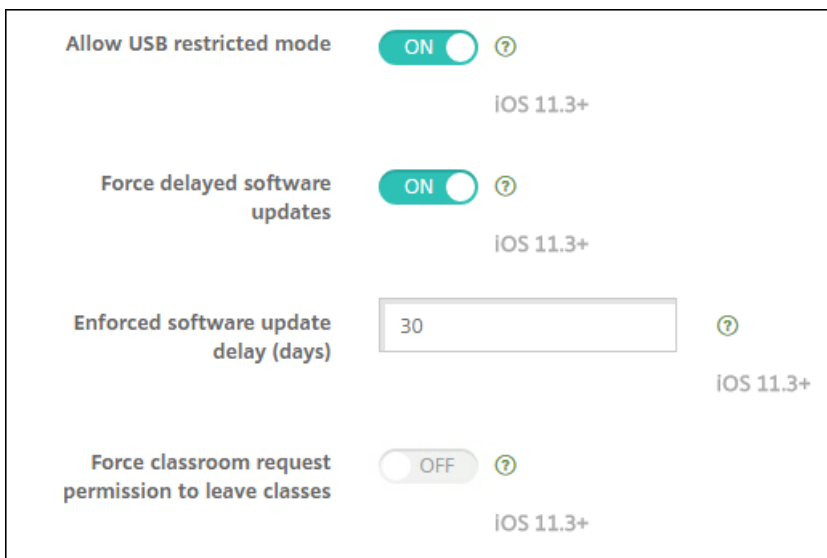
- 전송된암호로작업프로필이잠깁니다. 장치는잠기지않습니다.
- 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않는경우:
 - 작업프로필에암호가이미설정되어있지않으면장치가잠깁니다.
 - 작업프로필에암호가이미설정되어있으면작업프로필은잠기지만장치는잠기지않습니다.

잠금및암호재설정보안동작에대한자세한내용은 [보안동작](#)을참조하십시오.

iOS 또는 macOS 의새로운제한장치정책설정

- 관리되지않는앱이관리되는연락처읽기: 선택사항. 관리되지않는앱에있는관리되는앱의문서가사용되지않는경우에만사용할수있습니다. 사용하도록설정하면관리되지않는앱이관리되는계정의연락처에서데이터를읽을수있습니다. 기본값은 꺼짐입니다. iOS 12 부터사용할수있습니다.
- 관리되는앱이관리되지않는연락처쓰기: 선택사항. 사용하도록설정하면관리되는앱에서관리되지않는계정의연락처에연락처를쓸수있습니다. 관리되지않는앱에있는관리되는앱의문서를사용하는경우이제한은영향을미치지않습니다. 기본값은 꺼짐입니다. iOS 12 부터사용할수있습니다.
- 암호자동채우기: 선택사항입니다. 사용하지않는경우사용자는암호자동채우기또는강력한자동암호기능을사용할수없습니다. 기본값은 켜짐입니다. iOS 12 및 macOS 10.14 부터사용할수있습니다.

- 암호근접요청: 선택사항입니다. 사용하지않는경우사용자의장치는주변장치에서암호를요청하지않습니다. 기본값은 켜짐입니다. iOS 12 및 macOS 10.14 부터사용할수있습니다.
- 암호공유: 선택사항입니다. 사용하지않는경우사용자는 AirDrop 암호기능을사용하여암호를공유할수없습니다. 기본값은 켜짐입니다. iOS 12 및 macOS 10.14 부터사용할수있습니다.
- 자동날짜및시간적용: 감독되는장치. 사용하는경우사용자는 일반 > 날짜및시간 > 자동설정옵션을사용하지않도록설정할수없습니다. 기본값은 꺼짐입니다. iOS 12 부터사용할수있습니다.
- **USB** 제한모드허용: 감독되는장치에서만사용할수있습니다. 꺼짐인경우장치가잠겨있는동안항상 USB 액세서리에연결할수있습니다. 기본값은 켜짐입니다. iOS 11.3 부터사용할수있습니다.
- 소프트웨어업데이트강제지연: 감독되는장치에서만사용할수있습니다. 켜짐으로설정하면사용자에게소프트웨어업데이트표시가지연됩니다. 이제한을적용하면소프트웨어업데이트릴리스날짜로부터지정된기간 (일) 까지소프트웨어업데이트가표시되지않습니다. 기본값은 꺼짐입니다. iOS 11.3 및 macOS 10.13.4 부터사용할수있습니다.
- 소프트웨어업데이트시행지연 (일): 감독되는장치에서만사용할수있습니다. 관리자는이제한을사용하여장치의소프트웨어업데이트를지연할일수를설정할수있습니다. 최대값은 90 일이고기본값은 **30** 입니다. iOS 11.3 및 macOS 10.13.4 부터사용할수있습니다.
- 교실에서클래스를나갈때허가요청시행: 감독되는장치에서만사용할수있습니다. 켜짐으로설정하면교실앱을통해관리되지않는과정에등록한학생이과정을나가려면교사의허가를요청해야합니다. 기본값은 꺼짐입니다. iOS 11.3 부터사용할수있습니다.



[제한장치정책](#)에서자세한내용을참조하십시오.

iOS 또는 macOS 에대한 Exchange 장치정책업데이트

iOS 12 이상의추가 **S/MIME Exchange** 서명및암호화설정. 이제 Exchange 장치정책에 S/MIME 서명및암호화를구성하는설정이포함됩니다.

S/MIME 서명의경우:

- 서명 **ID** 자격증명: 사용할서명자격증명을선택합니다.

- **S/MIME** 서명사용자재정의가능: 쉼표로설정하면사용자가장치설정에서 S/MIME 서명을켜거나꺼낼수있습니다. 기본값은 꺼짐입니다.
- **S/MIME** 서명인증서 **UUID** 사용자재정의가능: 쉼표로설정하면사용자가장치설정에서사용할서명자격증명을선택할수있습니다. 기본값은 꺼짐입니다.

S/MIME 암호화의경우:

- 암호화 **ID** 자격증명: 사용할암호화자격증명을선택합니다.
- 메시지별 **S/MIME** 전환사용: 쉼표로설정하면작성하는각메시지에대해 S/MIME 암호화를켜거나꺼낼수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
- 기본적으로 **S/MIME** 암호화사용자재정의가능: 쉼표로설정하면사용자가장치설정에서 S/MIME 를기본적으로켜지여부를선택할수있습니다. 기본값은 꺼짐입니다.
- **S/MIME** 암호화인증서 **UUID** 사용자재정의가능: 쉼표로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나꺼낼수있습니다. 기본값은 꺼짐입니다.

iOS 12 이상의 **Exchange OAuth** 설정. 이제인증에 OAuth 를사용하도록 Exchange 연결을구성할수있습니다.

macOS 10.14 이상의 **Exchange OAuth** 설정. 이제인증에 OAuth 를사용하도록 Exchange 연결을구성할수있습니다. OAuth 를사용한인증의경우자동검색을사용하지않는설정에대한로그인 URL 을지정할수있습니다.

[Exchange 장치정책](#)에서자세한내용을참조하십시오.

iOS 용메일장치정책업데이트

iOS 12 이상의추가 **S/MIME Exchange** 서명및암호화설정. 메일장치정책에 S/MIME 서명및암호화를구성하는추가설정이 포함됩니다.

S/MIME 서명의경우:

- **S/MIME** 서명사용: 이계정이 S/MIME 서명을지원하는지여부를선택합니다. 기본값은 쉼표입니다. 쉼표로설정하면다음필드가나타납니다.
 - **S/MIME** 서명사용자재정의가능: 쉼표로설정하면사용자가장치설정에서 S/MIME 서명을켜거나꺼낼수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
 - **S/MIME** 서명인증서 **UUID** 사용자재정의가능: 쉼표로설정하면사용자가장치설정에서사용할서명자격증명을선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.

S/MIME 암호화의경우:

- **S/MIME** 암호화사용: 이계정이 S/MIME 암호화를지원하는지여부를선택합니다. 기본값은 꺼짐입니다. 쉼표로설정하면다음필드가나타납니다.
 - 메시지별 **S/MIME** 전환사용: 쉼표로설정하면작성하는각메시지에대해 S/MIME 암호화를켜거나꺼낼수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
 - 기본적으로 **S/MIME** 암호화사용자재정의가능: 쉼표로설정하면사용자가장치설정에서 S/MIME 를기본적으로켜지여부를선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.

- **S/MIME** 암호화인증서 **UUID** 사용자재정의가능: 쉼으로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나꺼낼수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.

[메일장치정책](#)에서자세한내용을참조하십시오.

iOS 용앱알림장치정책업데이트

다음앱알림설정은 iOS 12 부터사용할수있습니다.

- **CarPlay** 로표시: 쉼인경우 Apple CarPlay 에알림이표시됩니다. 기본값은 쉼입니다.
- **중요알림사용**: 쉼인경우앱이방해금지및벨소리설정을무시하는중요알림으로알림을표시할수있습니다. 기본값은 꺼짐입니다.

을참조하십시오. [앱알림장치정책](#)

Apple Education 에사용되는공유 iPad 지원

XenMobile 과 Apple Education 통합기능에서이제공유 iPad 가지원됩니다. 한교실에있는여러학생이한명또는여러명의강사가가르치는다양한과목에서 iPad 를공유할수있습니다.

관리자또는강사는공유 iPad 를등록한다음장치정책, 앱및미디어를장치에배포합니다. 그런다음수강생은관리되는 Apple ID 자격증명을제공하여공유 iPad 에로그인합니다. 이전에교육구성정책을학생에게배포한경우학생은장치를공유할때 “기타사용자” 로로그인하지않습니다.

공유 iPad 에대한사전요구사항:

- 모든 iPad Pro, iPad 5 세대, iPad Air 2 이상및 iPad 미니 4 이상
- 최소 32GB 의스토리지
- 감독됨

자세한내용은 [공유 iPad 구성](#)에서참조하십시오.

RBAC(역할기반액세스제어) 권한변경

로컬사용자추가/삭제 RBAC 권한이로컬사용자추가와로컬사용자삭제의두가지권한으로분할되었습니다.

자세한내용은 [RBAC 를사용하여역할구성](#)에서참조하십시오.

XenMobile Server 10.10 의새로운기능

January 6, 2020

[XenMobile Server 10.10](#)(PDF 다운로드)

중요:

iOS 12 로 장치를 업그레이드하기 위한 준비: iOS 용 VPN 장치정책의 Citrix VPN 연결 유형은 iOS 12 를 지원하지 않습니다. VPN 장치정책을 삭제하고 Citrix SSO 연결 유형으로 새 VPN 장치정책을 만듭니다.

VPN 장치정책을 삭제한 후 Citrix VPN 연결은 이전에 배포된 장치에서 계속 작동합니다. 새 VPN 장치정책 구성은 사용자 등록 중에 XenMobile Server 10.10 에서 적용됩니다.

GCM 에서 FCM 으로 업그레이드

2018 년 4 월 10 일 기준 Google 은 GCM(Google Cloud Messaging) 을 더 이상 사용하지 않습니다. Google 은 2019 년 5 월 29 일 이 되는 즉시 GCM 서버 및 클라이언트 API 를 제거할 것입니다.

중요 요구 사항:

- 중단을 방지하려면 5 월 29 일 이전에 XenMobile Server 10.10 으로 업그레이드하십시오.
- Secure Hub 19.3.5 이상으로 업그레이드해야 합니다.

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

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

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

업그레이드 단계:

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

다음에 XenMobile Server 로 체크인하고 정책 새로고침을 수행하면 장치가 FCM 으로 전환됩니다. Secure Hub 에서 장치를 새로고치려면: Secure Hub 에서 **기본설정 > 장치정보** 로 이동하고 정책 새로고침을 누릅니다.

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

XenMobile 마이그레이션 서비스

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

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

[New XenMobile Migration Service\(새로운 XenMobile 마이그레이션서비스\)](#)

[Making the Case for XenMobile in the Cloud\(클라우드에서 XenMobile 용사례만들기\)](#)

iOS MDM 등록워크플로변경

오해의소지가있는프로필설치를줄임으로써플랫폼보안을개선하기위해 Apple 은 MDM 에서장치를수동으로등록하는새로운워크플로를릴리스했습니다. 이새로운워크플로는 XenMobile Server 를비롯한모든 MDM 솔루션에영향을줍니다.

Apple Business Manager 또는 Apple School Manager 에서할당된서버에대한 MDM 등록은변경되지않습니다. 워크플로변경은 MDM 의수동등록에만해당됩니다.

신뢰할수있는인증서를사용하는경우이제등록을더욱간소화할수있습니다. 이전에는 iOS 장치사용자가등록중에메시지를두번 (루트 CA 에대한메시지와 MDM 장치인증서에대한메시지) 받았지만, 이제 iOS 장치사용자는등록중에 MDM 장치인증서에대한메시지만받을수있습니다. 이변경사항을지원하려면:

- 신뢰할 수 있는 인증서를 사용하는 경우 설정 > 서버 속성으로 이동하고 `ios.mdm.enrollment.installRootCaIfRequired` 속성의 값을 **false**로 변경합니다. 이 변경이 적용되면 MDM 등록 중에 사용자가 간편하게 프로필을 설치할 수 있는 Safari 창이 열립니다. iOS 장치 사용자는 등록 중에 MDM 장치 인증서에 대한 메시지만 받게 됩니다. 프롬프트의 레이블은 “XenMobile 프로필 서비스” 입니다.

<input type="checkbox"/>	Display name	Key	Value	Default value	Description
<input checked="" type="checkbox"/>	iOS Device Management Enrollment Install Root CA if Required	<code>ios.mdm.enrollment.installRootCaIfRequired</code>	true	true	Bypass installation of the root CA. Third-party public certificate required trusted by iOS.

자세한 내용은 [iOS 장치등록](#) 및 다음 YouTube 비디오를 참조하십시오.



XenMobile 10.10 로업그레이드하기전에 (온-프레미스)

일부시스템요구사항이변경되었습니다. 자세한내용은 [시스템요구사항및호환성](#) 및 [XenMobile 호환성](#)를참조하십시오.

1. 최신버전의 XenMobile Server 10.10 으로업데이트하기전에 Citrix License Server 를 11.15 이상으로업데이트하십시오.

최신버전의 XenMobile 에는 Citrix License Server 11.15(최소버전) 가필요합니다.

참고

XenMobile 10.10 의 SA(Subscription Advantage) 날짜는 2019 년 4 월 9 일입니다. Citrix 라이선스의 SA(Subscription Advantage) 날짜는이날짜보다이후여야합니다. SA 날짜는라이선스서버의라이선스옆에서 볼수있습니다. 최신버전의 XenMobile 을이전버전의라이선스서버환경에연결하면연결확인이실패하고라이선스 서버를구성할수없게됩니다.

라이선스의 SA 날짜를갱신하려면 Citrix 포털에서최신라이선스파일을다운로드하고라이선스서버에파일을업로드하십시오. 자세한내용은 <https://support.citrix.com/article/CTX134629>에서참조하십시오.

2. 클러스터된환경의경우: iOS 11 이상을실행하는장치에 iOS 정책및앱을배포하려면다음과같은요구사항이충족되어야합니다. NetScaler Gateway 에 SSL 지속성이구성되어있으면모든 XenMobile Server 노트에서포트 80 을열어야

합니다.

- 업그레이드할 XenMobile Server 를 실행하는 가상 컴퓨터의 RAM 이 4GB 미만인 경우 4GB 이상으로 RAM 을 늘리십시오. 프로덕션 환경에 권장되는 최소 RAM 은 8GB 입니다.
- XenMobile 업데이트를 설치하기 전에 VM 의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

업그레이드 파일에 대한 ShareFile 링크가 제공될 것입니다.

XenMobile 10.9 또는 10.8 에서 XenMobile Server 10.10 으로 직접 업그레이드할 수 있습니다. XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다. 자세한 내용은 [릴리스 관리 페이지를 사용하여 업그레이드하려면](#)에서 참조하십시오.

업그레이드 후

XenMobile 10.10 으로 업그레이드한 후 (온-프레미스):

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

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

관리자 그룹 권한을 제한하도록 향상된 RBAC 의 기능

관리 > 사용자 및 관리 > 등록 초대 페이지에서: RBAC 관리자의 그룹 권한에 따라 표시되는 사용자 정보가 제한됩니다. 이전에는 XenMobile Server 콘솔의 이러한 페이지에 모든 로컬 사용자 및 도메인 사용자에 대한 정보가 포함되었습니다.

RBAC 관리자가 보고 관리할 수 있는 사용자 그룹을 지정하려면: 관리자 역할을 편집하고 사용자 그룹을 지정합니다. 자세한 내용은 [RBAC 를 사용하여 역할 구성](#)에서 참조하십시오.

Android Enterprise 장치에 대한 새로운 정책

XenMobile Server 의 최신 버전에는 Android Enterprise 장치에 대한 새로운 정책이 포함됩니다.

- WiFi** 장치 정책. Android Enterprise 장치에 대한 WiFi 장치 정책을 만들 수 있습니다. [WiFi 장치 정책](#)에서 자세한 내용을 참조하십시오.
- 사용자 지정 **XML** 장치 정책. Android Enterprise 장치에 대한 사용자 지정 XML 장치 정책을 만들 수 있습니다. [사용자 지정 XML 장치 정책](#)에서 자세한 내용을 참조하십시오.

- 위치장치정책. **Android Enterprise** 장치소유자모드또는프로필소유자모드에서등록되는장치에대한위치설정을정의할수있습니다. [위치장치정책](#)에서자세한내용을참조하십시오.
- 파일장치정책. XenMobile Server 에파일을추가하여 **Android Enterprise** 장치에서기능을수행할수있습니다. [파일장치정책](#)에서자세한내용을참조하십시오.
- 새로운제한장치정책설정. 제한장치정책에대한새로운설정을사용하여 **Android Enterprise** 장치의다음과같은기능에대한사용자엑세스를허용할수있습니다. [제한장치정책](#)에서자세한내용을참조하십시오.
 - 파일전송
 - 테더링
 - Android Beam
 - 복사및붙여넣기허용
 - 앱확인사용
 - 응용프로그램설정의사용자제어허용
 - 장치연락처에작업프로필연락처허용
 - 화면캡처허용
 - 카메라사용허용
 - 홈화면에작업프로필앱위젯허용
 - 계정관리허용
 - 위치서비스허용
 - 응용프로그램사용안함

참고:

최신 Android Enterprise 정책에엑세스하려면 Secure Hub 의최신 Google Play 버전을사용해야합니다.

XenMobile Server 10.9 의새로운기능

January 6, 2020

[XenMobile Server 10.9\(PDF 다운로드\)](#)

중요:

iOS 12 로장치를업그레이드하기위한준비: iOS 용 VPN 장치정책의 Citrix VPN 연결유형은 iOS 12 를지원하지않습니다. VPN 장치정책을삭제하고 Citrix SSO 연결유형으로새 VPN 장치정책을만듭니다.

VPN 장치정책을삭제한후 Citrix VPN 연결은이전에배포된장치에서계속작동합니다. 새 VPN 장치정책구성은사용자등록중에 XenMobile Server 10.9 에서적용됩니다.

XenMobile 마이그레이션서비스

XenMobile Server 를온-프레미스에서사용하는경우 XenMobile 마이그레이션서비스를사용하여 Endpoint Management 를시작할수있습니다. XenMobile Server 에서 Citrix Endpoint Management 로마이그레이션할때장치를재등

록할필요는없습니다.

자세한내용은해당지역의 Citrix 영업사원, 시스템엔지니어또는 Citrix 파트너에게문의하십시오. 다음블로그에 XenMobile 마이그레이션서비스에대한자세한내용이나와있습니다.

[New XenMobile Migration Service\(새로운 XenMobile 마이그레이션서비스\)](#)

[Making the Case for XenMobile in the Cloud\(클라우드에서 XenMobile 용사례만들기\)](#)

콘솔에서 **XenMobile Tools** 액세스

XenMobile 콘솔에서다음과같은 XenMobile Tools 에액세스할수있습니다.

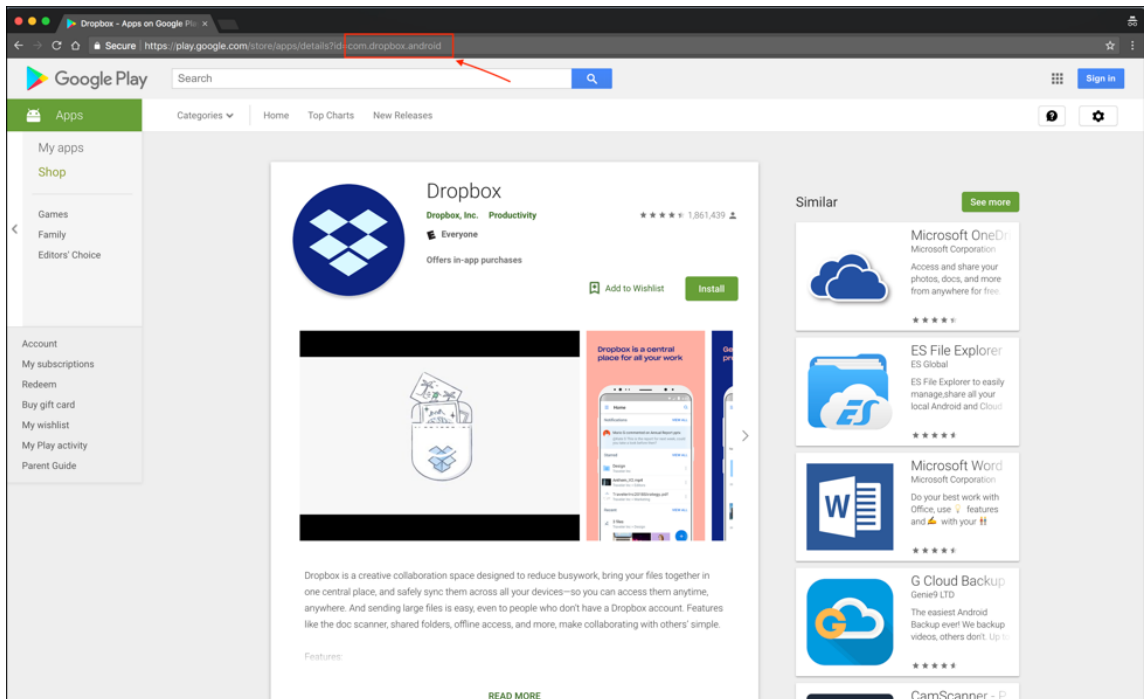
- **XenMobile Analyzer:** 배포의잠재적인문제를식별하고분류합니다.
- **APNs 포털:** APNs 인증서에서명하는요청을 Citrix 에제출합니다. 이인증서는다시 Apple 에제출합니다.
- **자동검색서비스:** 도메인에서 XenMobile 에대한자동검색을요청하고구성합니다.
- **푸시알림관리:** iOS 및 Windows 모바일생산성앱에대한푸시알림을관리합니다.
- **MDX Service:** XenMobile 을사용하여관리할수있도록앱을래핑합니다.

이러한도구에액세스하려면 설정 > **XenMobile Tools** 로이동합니다.

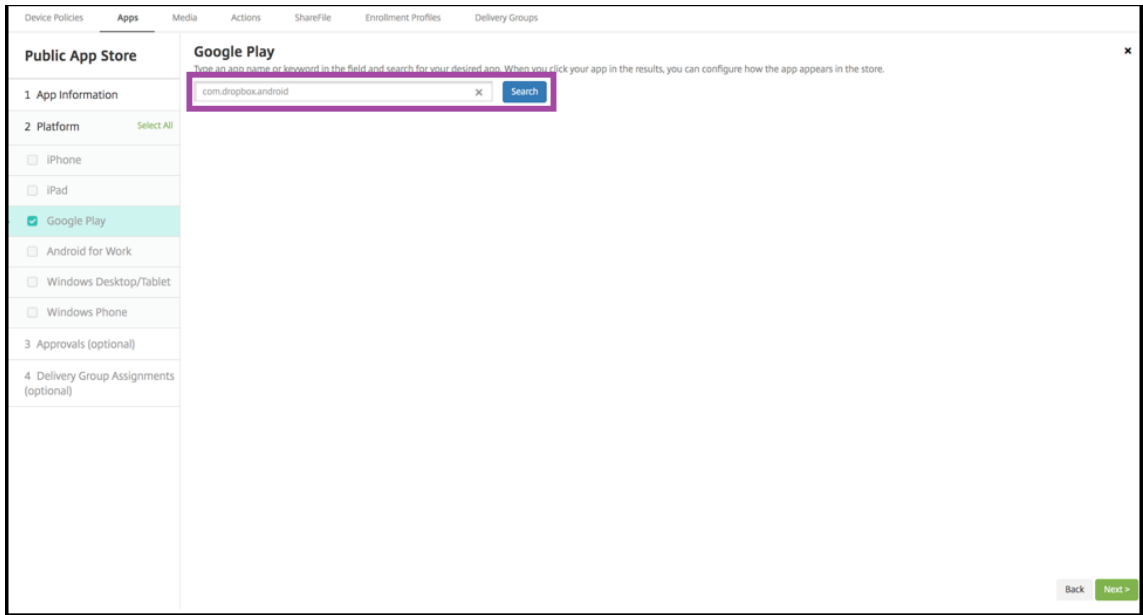
Google Play Store 에서앱을추가하기위한새워크플로

앱을추가할때 Google Play 자격증명을지정하는대신, 이제공용스토어 Android 앱의패키지 ID 를추가합니다.

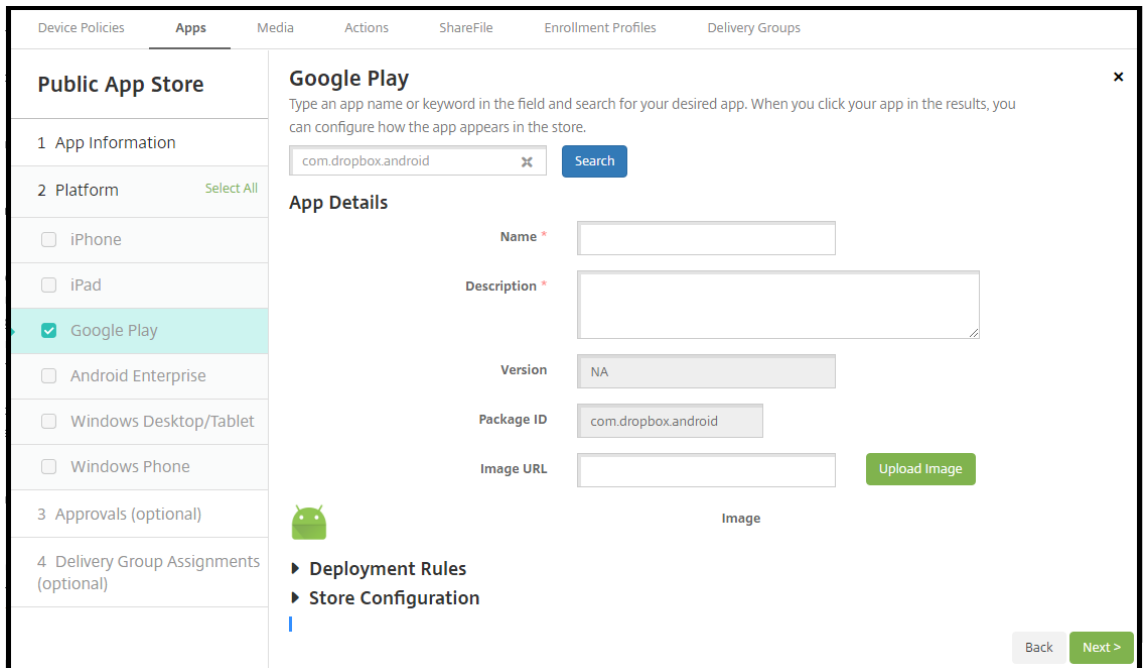
1. Google Play Store 에서패키지 ID 를복사합니다. ID 는앱의 URL 에있습니다.



2. XenMobile Server 콘솔에서공용스토어앱을추가할때검색창에패키지 ID 를붙여넣습니다.



3. 패키지 ID 가유효하면앱세부정보를입력할수있는 UI 가나타납니다.



자세한내용은 [공용앱스토어앱추가](#)에서참조하십시오.

새공용 **REST API**

- 필터로장치 가져오기 API 의새버전은장치에대한추가적인세부정보를제공합니다. 자세한내용은 [XenMobile Public API for REST Services\(REST 서비스에대한 XenMobile 공용 API\)](#) PDF 에서섹션 3.16.2 Get Devices by

Filters(필터로장치가져오기)(버전 2) 를참조하십시오.

- 루트 CA, 장치 CA, 서버 CA 를다시생성하고장치인증서를갱신하는기능

XenMobile Server 는 PKI: 루트 CA, 장치 CA 및서버 CA 에대해내부적으로다음과같은인증기관을사용합니다. 이러한 CA 는논리적그룹으로분류되며그룹이름이제공됩니다. 새 XenMobile Server 인스턴스를프로비저닝하면세계의 CA 가생성되고그룹이름 “default(기본)” 가지정됩니다.

XenMobile Server 콘솔또는공용 REST API 를사용하여지원되는 iOS, macOS 및 Android 장치에대한 CA 를갱신할수있습니다. 등록된 Windows 장치의경우새장치 CA 를받으려면사용자가장치를재등록해야합니다.

XenMobile Server 에서내부 PKI CA 를새로고치거나다시생성하고이러한인증기관에서발급한장치인증서를갱신하는데다음과같은 API 를사용할수있습니다.

- 새그룹 CA(인증기관) 를만듭니다.
- 새 CA 를활성화하고이전 CA 를비활성화합니다.
- 구성된장치목록에서장치인증서를갱신합니다. 이미등록된장치는중단없이계속작동합니다. 장치가서버에다시연결되면장치인증서가발급됩니다.
- 여전히이전 CA 를사용중인장치의목록을반환합니다.
- 모든장치가새 CA 를사용하게되면이전 CA 를삭제합니다.

자세한내용은 [XenMobile Public API for REST Services](#)(REST 서비스에대한 XenMobile 공용 API) PDF 에서다음섹션을참조하십시오.

- 섹션 3.16.58, Renew Device Certificate(장치인증서갱신)
- 섹션 3.23, Refresh XenMobile CA Group(XenMobile CA 그룹새로고침)

이기능의일부로서로보안동작인 인증서갱신을 장치관리콘솔에서사용할수있습니다. 이동작은해당장치의등록인증서를갱신합니다.

사전요구사항:

- 기본적으로이러한새인증서갱신기능은사용되지않도록설정됩니다. 인증서갱신기능을활성화하려면 **refresh.internal.ca** 서버속성값을 **True** 로설정하십시오.

중요:

NetScaler 에 SSL 오프로드가설정된경우새인증서를생성할때새 cacert.perm 으로부하분산장치를업데이트해야합니다. NetScaler Gateway 설정에대한자세한내용은 [To use SSL Offload mode for NetScaler VIPs](#)(NetScaler VIP 에 SSL 오프로드모드를사용하려면) 문서를참조하십시오.

타사고지사항

March 4, 2019

XenMobile 의이릴리스에는다음문서에정의된약관에따라사용이허가된타사소프트웨어가포함될수있습니다.

XenMobile 타사고지사항

수정된문제

October 21, 2019

XenMobile 10.11 에서는다음과같은문제가수정되었습니다.

- 모바일생산성앱과관련된수정된문제에대해서는 [Secure Hub](#), [Secure Mail](#) 및 [Secure Web](#)을참조하십시오.
- 버전 10.10.0 롤링패치릴리스의수정된문제는다음을참조하십시오.
 - [XenMobile Server 10.10.0 롤링패치 1](#)
 - [XenMobile Server 10.10.0 롤링패치 2](#)
 - [XenMobile Server 10.10.0 롤링패치 3](#)
- RBAC 관리자가신규또는기존사용자에게기본관리자역할을할당할수있습니다. 기본관리자역할할당은슈퍼관리자로제한되어야합니다. [CXM-37805]
- 이미등록된 Android Enterprise 장치에서 **AllUsers** 배달그룹에대한새필수앱이 Google Play Store 에표시되지 않습니다. [CXM-64910]
- Android 장치를등록하는동안다음과같은치명적인오류가발생합니다. **Cannot decrypt value**(값을해독할수없습니다). [CXM-65936]
- Android Enterprise 엔터프라이즈의이름및소유자가 Google Play Store 관리자콘솔에올바르게표시되지않을수 있습니다. [CXM-65996]
- XenMobile Server 에서올바른 VPP 토큰을구성하고 Apple VPP 포털에서새 VPP 서적을구입하십시오. 새로추가된미디어서적이동기화되지않고콘솔에나타나지않습니다. [CXM-66453]
- 새로가져온 CA 인증서가 PKI(공개키인터페이스) 항목에표시되지않습니다. [CXM-67960]
- VPP 계정을추가할때 (설정 > **iOS** 설정) 토큰이 350 자를초과하면다음메시지가나타납니다. “입력한회사토큰이잘못되었습니다. 새로입력하십시오.” [CXM-68113]
- StoreFront 서버에연결할수없는경우 MDX 앱이나열되기전에 iOS 용 Secure Hub 가시간초과됩니다. [CXM-68117]
- XenMobile Server 10.11 에대한 Secure Hub APNs(Apple 푸시알림서비스) 인증서가 2019 년 8 월 2 일에만료됩니다. 따라서에이전트알림이실패하고 iOS 장치에서응용프로그램푸시가 지연될수있습니다. 이번업데이트로 Secure Hub APNs 인증서가갱신되고 2020 년 7 월 12 일에만료됩니다. [CXM-68354]
- XenMobile Server 콘솔에서클라이언트속성값의문자수가 256 자로제한됩니다. [CXM-68386]
- Android 를실행하는장치에서엔터프라이즈앱을업데이트할수없는경우가있습니다. [CXM-68391]

- ‘bulk.enrollment.fetchRosterInfoDelay’ 서버속성의기간이종료되고 Apple School Manager DEP 장치가서버와동기화된후 Apple School Manager 사용자계정이서버에서삭제되고장치가익명상태로전환됩니다. [CXM-68417]
- Citrix SSO 프로토콜을사용하도록 iOS 용 VPN 장치정책을구성할때 연결할때 PIN 확인설정을사용하도록설정하고정책을저장하면이설정이 꺼짐으로되돌아갑니다. [CXM-68463]
- 이전에 REST API 를통해업데이트된엔터프라이즈앱을최신버전으로업데이트하는경우버전번호가업데이트되지않습니다. [CXM-68588]
- 앱액세스장치정책을배포한후규정을준수하지않는장치에서구성된작업이트리거되지않습니다. [CXM-69480]
- XenMobile Server 를사용하여공용 iOS 앱을업데이트하려고하면구성오류가나타납니다. [CXM-69555]
- Tomcat 서버상태를확인할때서버상태는정상이지만 0 이 아닌 1 값이반환될수있습니다. [CXM-69900]
- 이전버전에서마이그레이션한고객의경우장치의등록프로필이삭제되면콘솔에서관리탭을열때오류가표시됩니다. [CXM-70341]
- RBAC 역할 “Tier 2 techs” 는사용자수가 2,000 명을초과하는사용자그룹에대한등록초대를만들수없습니다. 전체관리자사용자만초대를만들수있습니다. [CXM-71224]

관련정보

- [XenMobile Support Knowledge Center](#)

알려진문제

January 6, 2020

XenMobile 10.11 에는다음과같은알려진문제가포함되어있습니다.

- XenMobile Server 에서 Apple 배포프로그램 (이전 DEP) 과의통신오류가발생합니다. 이문제는 XenMobile 10.11 및 10.10 에서발생합니다. 최신정보는 <https://support.citrix.com/article/CTX267079>에서확인하십시오.
- 모바일생산성앱과관련된알려진문제에대해서는 [Secure Hub](#), [Secure Mail](#) 및 [Secure Web](#)을참조하십시오.
- 버전 10.10.0 롤링패치릴리스의알려진문제는다음을참조하십시오.
 - [XenMobile Server 10.10.0 롤링패치 1](#)
 - [XenMobile Server 10.10.0 롤링패치 2](#)
 - [XenMobile Server 10.10.0 롤링패치 3](#)

관련정보

- [XenMobile Support Knowledge Center](#)

아키텍처

January 6, 2020

조직의 장치 또는 앱 관리 요구 사항에 따라 XenMobile 참조 아키텍처에서 배포할 XenMobile 구성 요소를 선택합니다. XenMobile 구성 요소는 모듈식이며 상호 기반하여 구축됩니다. 예를 들어 조직의 사용자에게 모바일 앱에 대한 원격 액세스를 제공하고 사용자 장치 유형을 추적하려면 XenMobile 과 함께 NetScaler Gateway 를 배포합니다. XenMobile 은 앱 및 장치를 관리하는데 사용되고 NetScaler Gateway 는 사용자가 조직의 네트워크에 연결할 때 사용됩니다.

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

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

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

- NetScaler Gateway. Quick Configuration(빠른 구성) 마법사를 통해 NetScaler Gateway 의 설정을 구성하여 XenMobile, StoreFront 또는 Web Interface 와의 통신을 설정할 수 있습니다. NetScaler Gateway 에서 Quick Configuration(빠른 구성) 마법사를 사용하기 전에 XenMobile, StoreFront 또는 Web Interface 중 하나를 설치하여 통신을 설정해야 합니다.
- XenMobile. XenMobile 을 설치한 후 XenMobile 콘솔에서 사용자의 모바일 장치 등록을 허용하는 정책 및 설정을 구성할 수 있습니다. 또한 모바일, 웹 및 SaaS 앱을 구성할 수 있습니다. 모바일 앱에는 Apple App Store 또는 Google Play 앱이 포함될 수 있습니다. 또한 사용자는 MDX Toolkit 을 사용하여 래핑되고 콘솔에 업로드된 모바일 앱에 연결할 수 있습니다.
- MDX Toolkit. MDX Toolkit 을 사용하면 조직 내부 또는 회사 외부에서 만들어진 모바일 앱을 안전하게 래핑할 수 있습니다. 앱을 래핑한 후에는 XenMobile 콘솔을 사용하여 앱을 XenMobile 에 추가하고 필요에 따라 정책 구성을 변경합니다. 또한 앱 범주를 추가하고, 워크플로를 적용하고, 배달 그룹에 앱을 배포할 수 있습니다. [MDX Toolkit 정보](#)에서 자세한 내용을 참조하십시오.
- StoreFront(선택 사항). Receiver 연결을 통해 StoreFront 의 Windows 기반 앱 및 가상 데스크톱에 대한 액세스를 제공할 수 있습니다.
- ShareFile Enterprise(선택 사항). ShareFile 을 배포하는 경우 XenMobile 을 통해 엔터프라이즈 디렉터리를 통합하여 SAML(Security Assertion Markup Language) ID 공급자로 사용할 수 있습니다. ShareFile 에 대한 ID 공급자 구성에 대한 자세한 내용은 ShareFile 지원 사이트를 참조하십시오.

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

프로덕션 환경에서는 확장성 및 서버 중복성을 위해 XenMobile 솔루션을 클러스터 구성으로 배포하는 것이 좋습니다. 또한

NetScaler SSL 오프로드기능을사용하면 XenMobile Server 의부하가줄고처리량이늘어납니다. NetScaler 에부하분산을위한가상 IP 주소 2 개를구성하여 XenMobile 클러스터를설정하는방법에대한자세한내용은 [클러스터링](#)을참조하십시오.

재해복구배포용으로 XenMobile 을구성하는방법에대한자세한내용은배포안내서의 [재해복구](#) 문서를참조하십시오. 이문서에는 아키텍처다이어그램이포함되어있습니다.

다음섹션에서는 XenMobile 배포의다양한참조아키텍처를설명합니다. 참조아키텍처다이어그램은 XenMobile 배포안내서문서 [온-프레미스배포용참조아키텍처](#) 및 [아키텍처](#)를참조하십시오. 전체포트목록은 [포트요구사항](#)(온프레미스) 및 [포트요구사항](#)(클라우드) 을참조하십시오.

MDM(모바일기기관리) 모드

중요:

MDM 모드를구성하고나중에 ENT 모드로변경하는경우동일한인증 (Active Directory) 을사용해야합니다. XenMobile 은사용자등록후의인증모드변경을지원하지않습니다. 자세한내용은 [XenMobile MDM Edition](#) 에서 [Enterprise Edition](#) 으로업그레이드에서참조하십시오.

XenMobile MDM Edition 은모바일기기관리를제공합니다. 플랫폼지원은 [지원되는장치운영체제](#)를참조하십시오. XenMobile 의 MDM 기능만사용하려는경우 XenMobile 을 MDM 모드로배포합니다. 예를들어다음을수행할수있습니다.

- 장치정책및앱배포
- 자산인벤토리검색
- 장치에서장치초기화및동작수행

권장모델에서 XenMobile Server 는 DMZ 에배치되며 XenMobile 의보호를개선하는 NetScaler 를선택적으로그앞에배포할수있습니다.

MAM(모바일앱관리) 모드

MAM 또는 MAM 전용모드는모바일앱관리를제공합니다. 플랫폼지원은 [지원되는장치운영체제](#)를참조하십시오. XenMobile 의 MAM 기능만사용하고 MDM 에장치를등록하지않으려는경우 XenMobile 을 MAM 모드로배포합니다. 예를들어다음을수행할수있습니다.

- BYO 모바일장치의앱및데이터보안
- 엔터프라이즈모바일앱제공
- 앱잠금및데이터초기화

장치를 MDM 에등록할수없습니다.

이배포모델에서 XenMobile Server 는 XenMobile 의보호를개선하는 NetScaler Gateway 다음에배치됩니다.

MDM+MAM 모드

MDM 과 MAM 모드를함께사용하면모바일앱및데이터관리기능과모바일기기관리기능을사용할수있습니다. 플랫폼지원은 [지원되는장치운영체제](#)를참조하십시오. XenMobile 의 MDM 기능과 MAM 기능을사용하려는경우 XenMobile 을 ENT(엔터프라이즈) 모드로배포합니다. 예를들어다음을수행할수있습니다.

- MDM 을사용하여회사에서발급한장치관리
- 장치정책및앱배포
- 자산인벤토리검색
- 장치초기화
- 엔터프라이즈모바일앱제공
- 장치의앱잠금및데이터초기화

권장배포모델에서 XenMobile Server 는 DMZ 에배치되며 XenMobile 의보호를개선하는 NetScaler Gateway 를그앞에배포합니다.

내부네트워크의 **XenMobile** - 다른배포옵션은온-프레미스 XenMobile Server 를 DMZ 가아닌내부네트워크에배치하는것입니다. 이배포는보안정책에따라 DMZ 에네트워크장비만배치해야하는경우사용됩니다. 이배포에서 XenMobile Server 는 DMZ 에배치되지않습니다. 따라서 DMZ 의 SQL Server 및 PKI 서버에대한액세스를허용하기위해내부방화벽의포트를열필요가없습니다.

시스템요구사항및호환성

January 27, 2020

참고:

이문서에서는 XenMobile Server 10.11 의시스템요구사항및호환성에대해다룹니다. Endpoint Management 의 시스템요구사항에대해서는 [시스템요구사항](#)을참조하십시오.

추가요구사항및호환성정보는다음문서를참조하십시오.

- [XenMobile 호환성](#)
- [지원되는장치운영체제](#)
- [포트요구사항](#)
- [확장성](#)
- [라이선스](#)
- [FIPS 140-2 준수](#)
- [언어지원](#)

XenMobile 10.11 을실행하려면다음과같은최소시스템요구사항이필요합니다.

- 다음중하나:

- Citrix Hypervisor 8.0 또는 Citrix XenServer(지원되는버전: 6.5.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6). 자세한내용은 [XenServer](#)를참조하십시오.
 - VMware(지원되는버전: ESXi 5.5 Update 3, ESXi 6.0, ESXi 6.5.0 Update 3 또는 ESXi 6.7 Update 2 패치 10). 자세한내용은 [VMware](#)를참조하십시오.
 - Hyper-V(지원되는 버전: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019). 자세한내용은 [Hyper-V](#)를참조하십시오.
 - Exchange ActiveSync 10.1.9.24 용 Endpoint Management 커넥터
 - Exchange ActiveSync 8.5.3.19 용 Citrix Gateway 커넥터
 - 듀얼코어프로세서
 - 가상 CPU 4 개
 - 프로덕션환경의경우 8GB RAM. POC 및테스트환경의경우 4GB RAM
 - 50GB 의디스크공간
 - Citrix License Server 11.15.x 이상
- XenMobile Server 를업그레이드하기전에라이선스서버를업데이트하십시오.

중요:

ESXi 6.7 이작동할수있도록다음해결방법을수행해야합니다.

1. VMware 에서 제공하는 OVF 도구를 사용하여 citrix.com 에서 다운로드한 OVA 파일을 추출합니다. VMware 페이지 (<https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491>) 에서 OVF 도구를연습니다.
2. 추출된세개파일중에서.vmdk 파일을데이터저장소에업로드합니다.
3. 새가상컴퓨터를만듭니다.
 - a) 가상컴퓨터이름을지정하고호환성옵션으로 **ESX/ESXi 4.x virtual machine(ESX/ESXi 4.x 가상컴퓨터)** 을선택합니다.
 - b) Guest OS family(게스트 OS 제품군) 에서 **Linux** 를선택합니다.
 - c) Guest OS version(게스트 OS 버전) 에서 **Other 2.6.x Linux (64-bit)(기타 2.6.x Linux(64 비트))** 를선택합니다.
 - d) 데이터저장소에서 **Default(기본값)** 를선택합니다.
 - e) 사용자지정하는동안기본하드디스크, USB 컨트롤러및 CD/DVD 드라이브를제거합니다.
 - f) Network(네트워크) 에서어댑터유형으로 **VMXNET3** 을선택합니다.
 - g) ESXi 에서디스크가로컬인경우 **SCSI Controller(SCSI 컨트롤러)** 및 **LSI Logic Parallel(LSI Logic 병렬)** 을선택합니다. 공유디스크를사용하는경우 **VMware Paravirtual(VMware 반가상화)** 을선택합니다.
 - h) Next(다음) 를클릭하여 VM 생성을마칩니다.
4. 데이터저장소로이동하고앞서업로드한.vmdk 파일을복사합니다. XenMobile 용으로만든 VM 디렉터리에붙여넣습니다.
5. ESXi 웹인터페이스에서 VM 을선택하고설정을편집합니다.
6. **Add Hard disk(하드디스크추가)** 를클릭합니다.
7. 앞서복사한.vmdk 파일을선택하고 VM 에파일을연결합니다.

- 8. 저장소를 클릭합니다.
- 9. VM 의전원을 켭니다.

NetScaler Gateway 시스템요구사항

XenMobile 10.11 과함께 NetScaler Gateway 를 실행하려면 다음과 같은 최소 시스템 요구사항이 필요합니다.

- NetScaler Gateway(온-프레미스). 지원되는 버전: 11.1(최신빌드), 12.0, 12.1(최신빌드), 13(최신빌드)
- 또한 Active Directory 와 통신하기 위한 서비스 계정이 있어야 합니다. 쿼리 및 읽기 권한만 있으면 됩니다.

XenMobile 10.11 데이터베이스 요구사항

XenMobile 에는 다음 데이터베이스 중 하나가 필요합니다.

- Microsoft SQL Server

XenMobile 저장소는 다음과 같은 지원되는 버전 중 하나에서 실행되는 Microsoft SQL Server 데이터베이스를 지원합니다. Microsoft SQL Server 데이터베이스에 대한 자세한 내용은 Microsoft SQL Server 를 참조하십시오.

- Microsoft SQL Server 2012 SP4
- Microsoft SQL Server 2014 SP3
- Microsoft SQL Server 2016 SP2
- Microsoft SQL Server 2017 CU 13
- Microsoft SQL Server 2019 CTP 3.2

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

Microsoft SQL 은 원격으로 사용하는 것이 좋습니다.

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

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

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

SQL Server 서비스 계정 요구사항

XenMobile 에 사용할 SQL Server 서비스 계정에 DBcreator 역할 권한이 있는지 확인합니다. XenMobile Server 설치 중에 지정하는 SQL Server 계정 암호를 기록합니다. XenMobile Server 복구 중에 XenMobile 데이터베이스를 복제해야 하는 경우가 암호가 필요합니다.

SQL Server 서비스계정에대한자세한내용은 Microsoft Developer Network 사이트의다음페이지를참조하십시오. 이러한링크는 SQL Server 2014 에대한정보를가리킵니다. 다른버전을사용하는경우 **Other Versions(다른버전)** 목록에서서버버전을선택하십시오.

- [서버구성 - 서비스계정](#)
- [Windows 서비스계정및권한구성](#)
- [서버수준역할](#)

Virtual Apps and Desktops 호환성

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

StoreFront 호환성

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906

기타호환성

- Exchange ActiveSync 10.1.9.24 용 Endpoint Management 커넥터
 - 이전버전은테스트되지않았습니다.
- Exchange ActiveSync 8.5.3.19 용 Citrix Gateway 커넥터
 - 이전버전은테스트되지않았습니다.

XenMobile 호환성

January 6, 2020

참고:

이문서에서는 XenMobile Server 의호환성에대해다룹니다. Endpoint Management 에서테스트된구성요소에대해서는 [Endpoint Management 호환성](#)을참조하십시오.

새로운기능, 수정사항및정책업데이트를사용하려면 Citrix 권장사항에따라 MDX Toolkit, Secure Hub 및모바일생산성앱의 최신버전을설치하는것이 좋습니다. MDX Toolkit 대신 MDX Service 를사용할수있습니다. 자세한내용은 [XenMobile MDX Service](#)에서참조하십시오.

중요:

2017년 12월 31일에 XenMobile 생산성앱에 대한 엔터프라이즈 배포 지원이 종료되었습니다. 자세한 내용은 [Citrix Product Matrix\(Citrix 제품 매트릭스\)](#) 문서를 참조하십시오. 이제 Citrix는 공용 앱스토어 배포만 지원합니다.

이 문서에서는 통합이 가능한 지원되는 XenMobile 구성 요소의 버전을 요약하여 보여줍니다.

지원되는 버전 및 업그레이드 경로

Secure Hub, MDX Toolkit 및 모바일 생산성 앱의 최신 버전은 XenMobile Server의 최신 버전 및 두 이전 버전과 호환됩니다. 최신 버전의 모바일 생산성 앱에는 최신 버전의 Secure Hub가 필요합니다. 이전 두 버전의 앱은 최신 Secure Hub와 호환됩니다.

XenMobile Server(온-프레미스)

- 이전 두 버전의 XenMobile Server에서 업그레이드할 수 있습니다.
- 최신 버전의 XenMobile Server:
 - XenMobile Server 10.11
- 업그레이드 원본:
 - XenMobile Server 10.10.x
 - XenMobile Server 10.9.x

모바일 생산성 앱

최신 버전의 모바일 생산성 앱에는 최신 버전의 Secure Hub가 필요합니다. 이전 두 버전의 앱은 최신 Secure Hub와 호환됩니다.

모바일 생산성 앱의 2주 릴리스 스케일업과 Secure Mail 및 Secure Web의 단계별 릴리스 프로세스에 대한 자세한 내용은 [릴리스 일정](#)을 참조하십시오. 지원 세부 정보는 [모바일 생산성 앱 지원](#)을 참조하십시오.

MDX Toolkit

- MDX Toolkit의 최신 릴리스 3개 (n.n.n)가 지원됩니다. XenMobile MDX Service를 사용하여 앱을 래핑할 수 있습니다. 자세한 내용은 [XenMobile MDX Service](#)에서 참조하십시오.
- 최신 Toolkit 버전은 타사 앱을 래핑할 수 있는 MDX Toolkit 19.9.5입니다 (iOS 및 Android용). MDX Toolkit 19.9.0 및 19.8.0에서 MDX Toolkit 19.9.5로 업그레이드할 수 있습니다.

MDX Toolkit 10.7.10은 모바일 생산성 앱 (이전의 XenMobile Apps)의 래핑을 지원하는 마지막 릴리스입니다. 사용자는 공용 앱스토어에서 모바일 생산성 앱에 액세스할 수 있습니다.

브라우저 지원

XenMobile Server 는 다음과 같은 브라우저를 지원합니다.

- Internet Explorer(버전 9 이하 제외)
- Chrome
- Firefox
- 자가지원 포털에서 사용할 수 있는 모바일 장치의 Safari

XenMobile Server 는 최신 버전의 브라우저와 호환되며 현재 버전이 이전 버전과 호환됩니다.

지원되는 장치 운영 체제

January 6, 2020

참고:

이 문서에서는 XenMobile Server 10.11 에서 지원되는 장치 운영 체제에 대해 다룹니다. Endpoint Management 에 지원되는 운영 체제는 [지원되는 장치 운영 체제](#) 를 참조하십시오.

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

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

참고:

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

운영 체제 지원 목록

Citrix XenMobile 은 다음 운영 체제를 지원합니다.

- **Android:** 6.x, 7.x, 8.x, 9.x, Android Q

참고:

Android Q 의 경우 [Android 고려 사항](#) 을 참조하십시오.

- **iOS:** 11.x, 12.x, 13.x
- **macOS:** 10.11 El Capitan, 10.12 Sierra, 10.13 High Sierra
- **Windows 10** 데스크톱 및 태블릿: Windows 10 RS4 및 RS5(MDM 전용)

- **Windows Phone:** Windows Phone 8.1, Windows Phone 10, Windows 10 RS4 및 RS5(MDM 전용)
- **Windows Mobile/CE:**(MDM 전용). 2018 년 2 분기부터 신규고객은 Windows Mobile/CE 장치에 대한 지원을 더 이상 이용할 수 없습니다.
- **Symbian 장치:** 2018 년 2 분기부터 신규고객은 Symbian 장치에 대한 지원을 더 이상 이용할 수 없습니다. 다음 목록에는 이전에 이러한 장치를 구성한 고객을 위해 XenMobile 이 지원하는 일부 Symbian 장치가 나와 있습니다.
 - Symbian 3
 - Symbian S60 5th Edition
 - Symbian S60 3rd Edition, Feature Pack 2
 - Symbian S60 3rd Edition, Feature Pack 1
 - Symbian S60 3rd Edition
 - Symbian S60 2nd Edition, Feature Pack 3
 - Symbian S60 2nd Edition, Feature Pack 2
- **Samsung SAFE 및 KNOX:** 호환되는 Samsung 장치에서 XenMobile 은 SAFE(Samsung for Enterprise) 및 Samsung Knox 정책을 지원하고 확장합니다. XenMobile 에서 SAFE 정책 및 제한을 배포하려면 먼저 SAFE API 를 사용하도록 설정해야 합니다. 이 작업을 수행하려면 기본 제공 Samsung ELM(Enterprise License Management) 키를 장치에 배포합니다. Samsung Knox API 를 사용하도록 설정하려면:
 1. Samsung KLMS(Knox License Management System) 를 사용하여 Samsung Knox 라이선스를 구입합니다.
 2. Samsung ELM 키를 배포합니다.
- **HTC:** HTC 관련 정책의 경우 XenMobile 은 HTC API 버전 0.5.0
- **Sony:** Sony 관련 정책의 경우 Sony Enterprise SDK 2.0

Android 고려사항

Android Q 플랫폼으로 업그레이드하기 전에 Google Device Administration API 의 사용 중단이 Android Q 를 실행하는 장치에 미치는 영향에 대해 [장치관리에서 Android Enterprise 로 마이그레이션](#)에서 자세한 내용을 참조하십시오.

- Android Q 장치는 레거시 장치관리 모드에서 등록하지 않는 것이 좋습니다. Google 은 Android Q 를 실행하는 장치에 영향을 미치는 장치관리 API 의 사용을 중단하고 있습니다. API 의 사용이 중단된 후에 레거시 장치관리 모드에서 Android Q 장치를 등록하면 등록이 실패합니다.
- Android Q 장치에는 Android Enterprise 를 사용하는 것이 좋습니다. 자세한 내용은 [장치관리에서 Android Enterprise 로 마이그레이션](#)에서 참조하십시오.
- Google API 변경은 MAM 전용 모드에서 등록된 장치에는 영향을 주지 않습니다.

Android P 플랫폼으로 업그레이드하기 전에:

- 서버 인프라인이 subjectAltName(SAN) 확장에 일치하는 호스트 이름을 가진 보안 인증서와 호환되는지 확인하십시오.
- 호스트 이름을 확인하려면 서버가 일치하는 SAN 이 포함된 인증서를 제공해야 합니다. Citrix 는 호스트 이름과 일치하는 SAN 이 포함된 인증서만 신뢰합니다.

- 자세한내용은 [Android P 동작변경사항](#)에서 Android Developer 사이트문서를참조하십시오.

Android O(버전 8) 릴리스관련사항:

- SSLv3 은 Android O 에서지원되지않습니다. Google 은 SSLv3 연결을더이상지원하지않습니다. 따라서 Android O 장치에서실행되는모바일생산성앱은 SSLv3 연결을사용하는내부서버에연결할수없습니다. SSLv3 을활용하는서버가 있는경우 Android O 를롤아웃하기전에이제한을해결하여사용자의연결실패를방지하는것이중요합니다.
- Citrix 모바일생산성앱의버전 10.6.20 공용앱스토어릴리스부터 Android 4.4x 에대한지원이종료되었습니다.
- Citrix 모바일생산성앱및 MDX 래핑된앱은 ARM 기반프로세서를탑재한 Android 장치에서사용할수있습니다. Intel x86 또는 x64 기반 Android 장치에서는지원되지않습니다.

BlackBerry

BlackBerry 장치의관리는 Exchange ActiveSync 용 XenMobile 커넥터를통해제공됩니다. 자세한내용은 [Exchange ActiveSync 용 XenMobile 커넥터](#)에서참조하십시오.

포트요구사항

September 27, 2019

장치및앱에서 XenMobile 과통신할수있도록하려면방화벽에서특정포트를열어야합니다. 열어야하는포트가다음표에나열되어 있습니다.

NetScaler Gateway 및 XenMobile 의앱관리를위한포트열기

Citrix Secure Hub, Citrix Receiver 및 NetScaler Gateway 플러그인사용자가 NetScaler Gateway 를통해다음구성요소에연결할수있도록하려면다음포트를열어야합니다.

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- Exchange ActiveSync 용 Citrix Gateway 커넥터
- 인트라넷웹사이트와같은다른내부네트워크리소스

NetScaler 에서 Launch Darkly 로의트래픽을활성화하려면이 [Support Knowledge Center 문서](#)에나와있는 IP 주소 를사용할수있습니다.

NetScaler Gateway 에대한자세한내용은 NetScaler Gateway 설명서를참조하십시오. 이설명서에 NSIP(NetScaler IP), VIP(가상서버 IP) 및 SNIP(서브넷 IP) 주소에대한정보가포함되어있습니다.

TCP 포트	설명	원본	대상
21 또는 22	FTP 또는 SCP 서버로 지원 번들을 보내는데 사용됩니다.	XenMobile	FTP 또는 SCP 서버
53(TCP 및 UDP)	DNS 연결에 사용됩니다.	NetScaler Gateway, XenMobile	DNS 서버
80	NetScaler Gateway 가 두 번째 방화벽을 통해 VPN 연결을 내부 네트워크 리소스 에 전달합니다. 이상 상황은 일 반적으로 사용자가 NetScaler Gateway 플 러그인으로 로그인한 경우 발 생합니다.	NetScaler Gateway	인트라넷 웹사이트
80 또는 8080, 443	열거, 티켓 생성 및 인증에서 용되는 XML 및 STA(Secure Ticket Authority) 포트입니다. 포트 443 을 사용할 것을 권 장합니다.	StoreFront 및 Web Interface XML 네트워크 트래픽, NetScaler Gateway STA	Virtual Apps 또는 Desktops
123(TCP 및 UDP)	NTP(Network Time Protocol) 서비스에 사용됩 니다.	NetScaler Gateway, XenMobile	NTP 서버
389	보안되지 않은 LDAP 연결 에 사용됩니다.	NetScaler Gateway, XenMobile	LDAP 인증 서버 또는 Microsoft Active Directory
443	Citrix Receiver 의 StoreFront 연결 또는 Receiver for Web 의 Virtual Apps and Desktops 연결에 사용됩니 다.	인터넷	NetScaler Gateway
443	웹, 모바일 및 SaaS 앱 제공 을 위해 XenMobile 에 연결 할 때 사용됩니다.	인터넷	NetScaler Gateway
443	일반 장치와 XenMobile Server 의 통신에 사용됩니 다.	XenMobile	XenMobile

TCP 포트	설명	원본	대상
443	등록을위해모바일장치에서 XenMobile 에연결할때사용됩니다.	인터넷	XenMobile
443	XenMobile 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터로의연결에사용됩니다.	XenMobile	Exchange ActiveSync 용 Citrix Gateway 커넥터
443	Exchange ActiveSync 용 Citrix Gateway 커넥터에서 XenMobile 로의연결에사용됩니다.	Exchange ActiveSync 용 Citrix Gateway 커넥터	XenMobile
443	인증서인증을사용하지않는 배포의콜백 URL 에사용됩니다.	XenMobile	NetScaler Gateway
514	XenMobile 과 syslog 서버간의연결에사용됩니다.	XenMobile	Syslog 서버
636	보안 LDAP 연결에사용됩니다.	NetScaler Gateway, XenMobile	LDAP 인증서버또는 Active Directory
1494	내부네트워크의 Windows 기반응용프로그램에대한 ICA 연결에사용됩니다. 이 포트는열어두는것이 좋습니다.	NetScaler Gateway	Virtual Apps 또는 Desktops
1812	RADIUS 연결에사용됩니다.	NetScaler Gateway	RADIUS 인증서버
2598	세션안정성을사용한내부네트워크의 Windows 기반 응용프로그램에대한연결에 사용됩니다. 이포트는열어두는것이 좋습니다.	NetScaler Gateway	Virtual Apps 또는 Desktops
3268	Microsoft 글로벌카탈로그의보안되지않은 LDAP 연결에사용됩니다.	NetScaler Gateway, XenMobile	LDAP 인증서버또는 Active Directory

TCP 포트	설명	원본	대상
3269	Microsoft 글로벌카탈로그의보안 LDAP 연결에서 사용됩니다.	NetScaler Gateway, XenMobile	LDAP 인증서버또는 Active Directory
9080	NetScaler 와 Exchange ActiveSync 용 Citrix Gateway 커넥터간의 HTTP 트래픽에서 사용됩니다.	NetScaler	Exchange ActiveSync 용 Citrix Gateway 커넥터
30001	HTTPS 서비스의초기스테이징을위한관리 API	내부 LAN	XenMobile Server
9443	NetScaler 와 Exchange ActiveSync 용 Citrix Gateway 커넥터간의 HTTPS 트래픽에서 사용됩니다.	NetScaler	Exchange ActiveSync 용 Citrix Gateway 커넥터
45000, 80	클러스터에배포된두 XenMobile VM 간의통신에 사용됩니다. 포트 80 은 노드간통신및 SSL 오프로드에 사용됩니다.	XenMobile	XenMobile
8443	등록, XenMobile Store 및 MAM(모바일앱관리) 에 사용됩니다.	XenMobile, NetScaler Gateway, 장치, 인터넷	XenMobile
4443	관리자가브라우저를통해 XenMobile 콘솔에액세스 할때 사용됩니다. 또한모든 XenMobile 클러스터노드의로그및지원번들을한노드에서다운로드하는데 사용됩니다.	액세스지점 (브라우저), XenMobile	XenMobile
27000	외부 Citrix License Server 에액세스할때 사용되는기본포트입니다.	XenMobile	Citrix License Server
7279	들어오고나가는 Citrix 라이선스를확인할때 사용되는기본포트입니다.	XenMobile	Citrix 공급업체데몬

TCP 포트	설명	원본	대상
161	UDP 프로토콜을 사용하는 SNMP 트래픽에 사용됩니다.	SNMP 관리자	XenMobile
162	XenMobile의 SNMP 트랩알림을 SNMP 관리자로 보내는데 사용됩니다. 원본은 XenMobile 이고 대상은 SNMP 관리자입니다.	XenMobile	SNMP 관리자

장치 관리를 위한 **XenMobile** 포트 열기

XenMobile 이 네트워크에서 통신할 수 있도록 하려면 다음 포트를 엽니다.

TCP 포트	설명	원본	대상
25	XenMobile 알림 서비스의 기본 SMTP 포트입니다. SMTP 서버가 다른 포트를 사용하는 경우 방화벽이 해당 포트를 차단하지 않는지 확인하십시오.	XenMobile	SMTP 서버
80 및 443	Apple iTunes App Store, Google Play(80을 사용해야 함) 또는 Windows Phone 스토어에 대한 엔터프라이즈 앱스토어 연결입니다. Apple Volume Purchase Program 에 사용됩니다. iOS 의 Citrix Mobile Self-Serve, Android 용 Secure Hub 또는 Windows Phone 용 Secure Hub 를 통해 앱스토어의 앱을 게시할 때 사용됩니다.	XenMobile	ax.apps.apple.com 및 *.mzstatic.com, vpp.itunes.apple.com, login.live.com, *.notify.windows.com, play.google.com, android.clients.google.com, android.l.google.com

TCP 포트	설명	원본	대상
80 또는 443	XenMobile 과 Nexmo SMS 알림릴레이간의아웃 바운드연결에서사용됩니다.	XenMobile	Nexmo SMS 릴레이서버
389	보안되지않은 LDAP 연결 에사용됩니다.	XenMobile	LDAP 인증서버또는 Active Directory
443	Android 및 Windows Mobile 의등록및에이전트 설정에서사용됩니다.	인터넷	XenMobile
443	Android 및 Windows 장치, XenMobile 웹콘솔및 MDM 원격지원클라이언트 의등록및에이전트설정에서 사용됩니다.	인터넷 LAN 및 Wi-Fi	XenMobile
1433	원격데이터베이스서버에대한연결에기본적으로사용됩니다 (선택사항).	XenMobile	SQL Server
2195	APNs(Apple 푸시알림서비스) 에서 iOS 장치알림및 장치정책푸시를위해 gateway.push.apple.com 에아웃바운드연결할때사용됩니다.	XenMobile	인터넷 (공용 IP 주소 17.0.0.0/8 을사용하는 APNs 호스트)
2196	APNs 에서 iOS 장치알림및장치정책푸시를위해 feedback.push.apple.com 에아웃바운드연결할때사용됩니다.		
5223	Wi-Fi 네트워크의 iOS 장치에서 *. push.apple.com 에대한 APNs 의아웃 바운드연결에서사용됩니다.	Wi-Fi 네트워크의 iOS 장치	인터넷 (공용 IP 주소 17.0.0.0/8 을사용하는 APNs 호스트)
8081	선택적 MDM 원격지원클라이언트의애플터널에서사용됩니다. 기본값은 8081 입니다.	원격지원클라이언트	XenMobile

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

자동검색서비스연결을위한포트요구사항

이 포트 구성은 Android 용 Secure Hub 로부터 연결되는 Android 장치가 내부 네트워크 내에서 Citrix ADS(자동검색서비스)에 액세스할 수 있도록 합니다. ADS 를 통해 제공되는 보안 업데이트를 다운로드하려면 ADS 에 액세스할 수 있어야 합니다.

참고:

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

인증서 고정을 사용하려는 경우 다음 사전 요구 사항을 수행합니다.

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

인증서 고정을 사용하려면 장치 등록 전에 장치가 ADS 에 연결되어야 합니다. 그렇게 해야 장치를 등록하는 환경에 대한 최신 보안 정보가 Secure Hub 에 제공됩니다. Secure Hub 에서 장치를 등록하려면 장치가 ADS 에 연결되어야 합니다. 그러므로 내부 네트워크에서 ADS 액세스를 열어야 장치를 등록할 수 있습니다.

Android 용 Secure Hub 에서 ADS 에 액세스할 수 있게 하려면 다음 FQDN 및 IP 주소에 대해 포트 443 을 엽니다.

FQDN	IP 주소	포트	IP 및 포트 사용
ads.xml.cloud.com	34.194.83.188	443	Secure Hub - ADS 통신
ads.xml.cloud.com	34.193.202.23	443	Secure Hub - ADS 통신

참고:

10.6.15 이전 Secure Hub 버전의 경우 FQDN 은 discovery.mdm.zenprise.com입니다. IP 주소 52.5.138.94 및 52.1.30.122 에 대해 포트 443 을 엽니다.

Android Enterprise 네트워크 요구 사항

Android Enterprise 용 네트워크 환경을 설정할 때 알아둘 몇 가지 아웃바운드 연결이 있습니다.

장치에대한포트요구사항

대상호스트	포트	설명
*.googleapis.com	TCP/443	Google Mobile Management, Google API, Google Play 스토어 API 에사용
play.google.com, android.com google-analytics.com, android.clients.google.com	TCP/443	Google Play 및 Android.clients.google.com 을 통한업데이트에사용. 앱, 업데이트및 Google Play 스토어 API 다운로드
cm.googleapis.com	TCP/443	Firebase Cloud Messaging 에사 용
android.apis.google.com, cm.googleapis.com	TCP/5228, 5229, 5230	장치 Wi-Fi 의 Firebase Cloud Messaging 의나가는인터넷통신에 사용
connectivitycheck.android.com www.google.com	TCP/443	CloudDPC v470 이전버전의연결확 인에사용. N MR1 로시작하는 Android 연결확인을위해 https://www.google.com/generate_204 에연결할수있거나, 지정된 Wi-Fi 네트워크가연결가능한 PAC 파일을가리켜야합니다.

XenMobile 의포트요구사항

EMM 콘솔이온프레미스에있는경우관리형 Google Play Enterprise 를만들고 [관리형 Google Play iFrame](#)에액세스하려면네트워크에서다음대상호스트에연결할수있어야합니다. Google 은앱검색및승인을간소화하기위해 EMM 개발자가관리형 Play iFrame 을사용할수있도록했습니다.

대상호스트	포트	설명
play.google.com	TCP/443	Google Play 스토어, Play Enterprise 가입에사용
accounts.youtube.com, accounts.google.com	TCP/443	계정인증에사용
apis.google.com	TCP/443	GCM 및기타 Google 웹서비스에사 용
ogs.google.com	TCP/443	iFrame UI 요소에사용

대상호스트	포트	설명
notifications.google.com	TCP/443	데스크톱및모바일알림에사용
fonts.googleapis.com, *.gstatic.com, *.googleusercontent.com	TCP/443	Google Fonts 사용자생성콘텐츠에 사용. 예: 스토어의앱아이콘
cri.pki.goog, ocsp.pki.goog	TCP/443	인증서유효성검사에사용

확장성및성능

April 11, 2019

XenMobile 인프라의규모를이해하는것은 XenMobile 을어떻게배포하고구성할지결정하는데있어중요합니다. 이문서에는확장성테스트데이터와소규모에서대규모에이르는온-프레미스 XenMobile 엔터프라이즈배포의성능과확장성을위한인프라요구사항을결정하는지침이포함되어있습니다.

여기서확장성은배포에이미등록된장치가해당배포에동시에다시연결되는능력의관점에서정의됩니다.

- 확장성은배포에등록된최대장치수로정의됩니다.
- 로그인속도는기존장치가배포에다시연결될수있는최대속도로정의됩니다.

이문서에나온데이터는 10,000~75,000 개장치규모의배포에대한테스트결과입니다. 알려진작업부하를사용하여모바일장치를테스트했습니다.

XenMobile Enterprise Edition 에서모든테스트를수행했습니다.

테스트는 NetScaler Gateway 8200 을사용하여수행되었습니다. 비슷하거나더큰용량의 NetScaler 장비에서는비슷한수준또는더뛰어난확장성과성능이나타날수있습니다.

확장성테스트결과요약은다음과같습니다.

최대 **75,000** 개장치의배포에대한확장성테스트결과요약

로그인속도 (기존사용자의다시연결속도) - 시간당최대 9,375 개장치

사용된구성:

- NetScaler Gateway
- MPX 8200
- XenMobile Enterprise Edition
- XenMobile Server 7 노드클러스터

- 데이터베이스: Microsoft SQL Server 외부데이터베이스

장치모집단및하드웨어구성을사용한테스트결과

장치수	12,500	30,000	60,000	75,000
시간당기존장치이다 시연결속도	1,250	3,750	7,500	9,375
XenMobile Server - 모드	독립실행형	클러스터	클러스터	클러스터
XenMobile Server - 클러스터	해당없음	3	5	7
XenMobile Server - 가상장비	메모리 = 8GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 6	메모리 = 24GB RAM, vCPU = 8	메모리 = 24GB RAM, vCPU = 8
Active Directory	메모리 = 4GB RAM, vCPU = 2	메모리 = 8GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 4
Microsoft SQL Server 외부데이터 베이스	메모리 = 8GB RAM, vCPU = 4	메모리 = 16GB RAM, vCPU = 8	메모리 = 24GB RAM, vCPU = 16	메모리 = 24GB RAM, vCPU = 16

확장성프로필

Active Directory 구성	사용된프로필
사용자	100,000
그룹	200,000
중첩수준	5

XenMobile Server 구성	합계	사용자당
정책	20	20
앱	270	50
공용앱	200	0
MDX	50	30
웹및 SaaS	20	20

XenMobile Server 구성	합계	사용자당
동작	50	
배달그룹	20	
배달그룹당 Active Directory 그룹	10	
SQL		
데이터베이스개수	1	

장치연결및앱작업

이러한확장성테스트를통해배포에등록된장치가 8 시간내에다시연결될수있는지에대한데이터를수집했습니다.

이테스트에서시뮬레이션한다시연결간격동안에는다시연결되는장치에모든해당보안정책이적용되기때문에 XenMobile Server 노드의부하상태가일반적인수준보다높아집니다. 이후에다시연결할때에는변경된정책또는새로운정책만 iOS 장치로푸시되므로 XenMobile Server 노드의부하가줄어듭니다.

이러한테스트에서는 iOS 장치와 Android 장치를 50% 씩섞어서사용했습니다.

이러한테스트에서는다시연결되는 Android 장치가사전 GCM 알림을받은것으로가정합니다.

8 시간의테스트기간동안다음과같은앱관련작업이이루어졌습니다.

- 권한이부여된앱을열거하기위해 Secure Hub 가한번열림
- 2 개의 SAML 웹앱이열림
- 4 개의 MAM 앱이다운로드됨
- Secure Mail 에서사용하도록 1 개의 STA 가생성됨
- Micro VPN 을통한 Secure Mail 다시연결이벤트당하나씩 240 개의 STA 티켓유효성검사가수행됨

참조아키텍처

이러한확장성테스트에사용되는배포의참조아키텍처에대한자세한내용은 [온-프리미스배포용참조아키텍처](#)의 “핵심 MAM + MDM 참조아키텍처” 를참조하십시오.

주의사항및제한사항

이문서에나온확장성테스트결과를고려할때다음사항에유의하십시오.

- Windows 플랫폼은테스트되지않았습니다.
- iOS 와 Android 장치에대한정책푸시를테스트했습니다.
- 각 XenMobile Server 노드는동시에최대 12,000 개의장치를지원합니다.

라이선스

January 6, 2020

XenMobile 은 Citrix Licensing 을사용하여라이선스를관리합니다. XenMobile Server 및 NetScaler Gateway 를사용하려면라이선스가필요합니다.

NetScaler Gateway 라이선스에대한자세한내용은 NetScaler Gateway 설명서를참조하십시오. Citrix 라이선스에대한자세한내용은 [Citrix Licensing 시스템](#)을참조하십시오.

XenMobile Server 를구입하면라이선스활성화지침이포함된주문확인전자메일메시지가전송됩니다. 신규고객은주문을제출하기전에라이선스프로그램에등록해야합니다. XenMobile 라이선스모델및프로그램에대한자세한내용은 [XenMobile licensing\(XenMobile 라이선스\)](#)을참조하십시오.

요구사항

- 최신버전의 XenMobile Server 로업데이트하기전에 Citrix License Server 를 11.15.x 이상으로업데이트하십시오. 이전라이선스서버버전은최신버전의 XenMobile 을지원하지않습니다.
- XenMobile 라이선스를다운로드하기전에 Citrix Licensing 을설치해야합니다. 라이선스파일을생성하려면 Citrix Licensing 을설치한서버의이름이필요합니다. XenMobile 을설치하면 Citrix Licensing 이기본적으로이서버에설치됩니다. 또는기존 Citrix Licensing 배포를사용하여 XenMobile 라이선스를관리할수있습니다. Citrix Licensing 설치, 배포및관리에대한자세한내용은 [제품라이선스](#)를참조하십시오.
- XenMobile 의노드또는인스턴스를클러스터하려는경우원격서버에서 Citrix Licensing 을사용해야합니다.
- 받은모든라이선스파일의로컬복사본을유지하는것이 좋습니다. 구성파일의백업복사본을저장하면모든라이선스파일백업에포함됩니다. 그러나구성파일을먼저백업하지않고 XenMobile 을다시설치하는경우원래라이선스파일이필요합니다.

XenMobile 라이선스고려사항

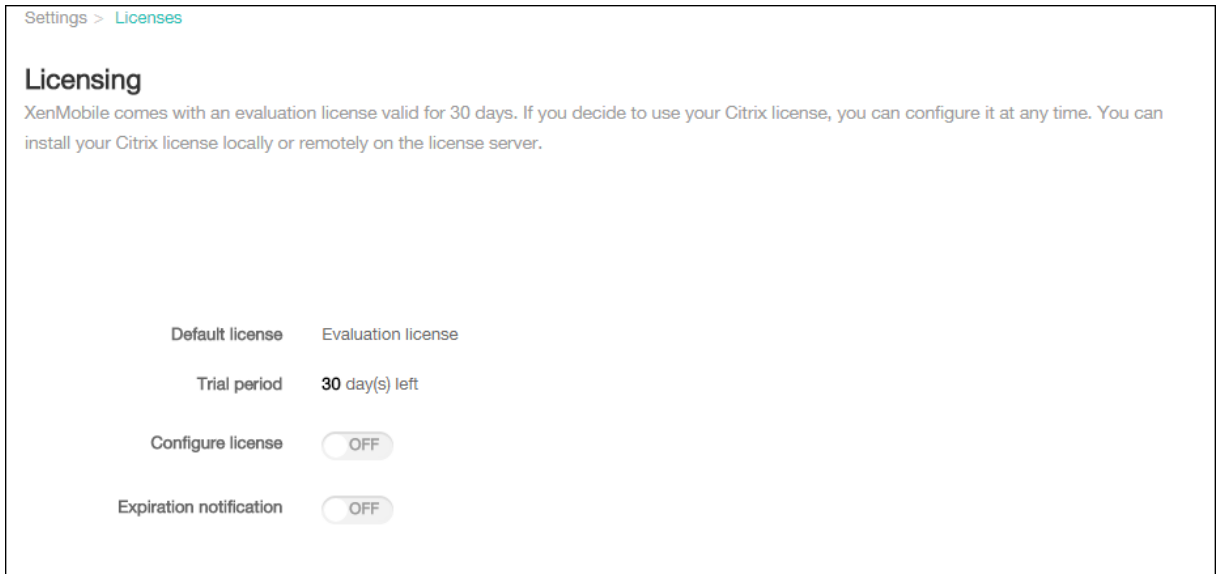
라이선스가없는경우평가모드에서 30 일의유예기간동안 XenMobile 의모든기능을사용할수있습니다. 이평가모드는한번만사용할수있으며 XenMobile 을설치한날부터 30 일간유효합니다. 유효한 XenMobile 라이선스가있는지여부와관계없이 XenMobile 웹콘솔에대한액세스는차단되지않습니다. XenMobile 콘솔에서평가기간이얼마나남았는지를확인할수있습니다.

XenMobile 에서다수의라이선스를업로드할수있지만한번에하나의라이선스만활성화할수있습니다.

XenMobile 라이선스가만료되면더이상장치관리기능을수행할수없습니다. 예를들어새사용자또는장치를등록할수없고등록된장치에배포한앱및구성을업데이트할수없습니다. XenMobile 라이선스모델및프로그램에대한자세한내용은 [XenMobile licensing\(XenMobile 라이선스\)](#)을참조하십시오.

XenMobile 콘솔에서라이센스페이지를찾으려면

XenMobile 을설치한후 라이선스페이지가처음로나타날때라이선스는기본 30 일평가모드로설정되고아직구성되지않은상태로표시됩니다. 이페이지에서라이선스를추가하고구성할수있습니다.



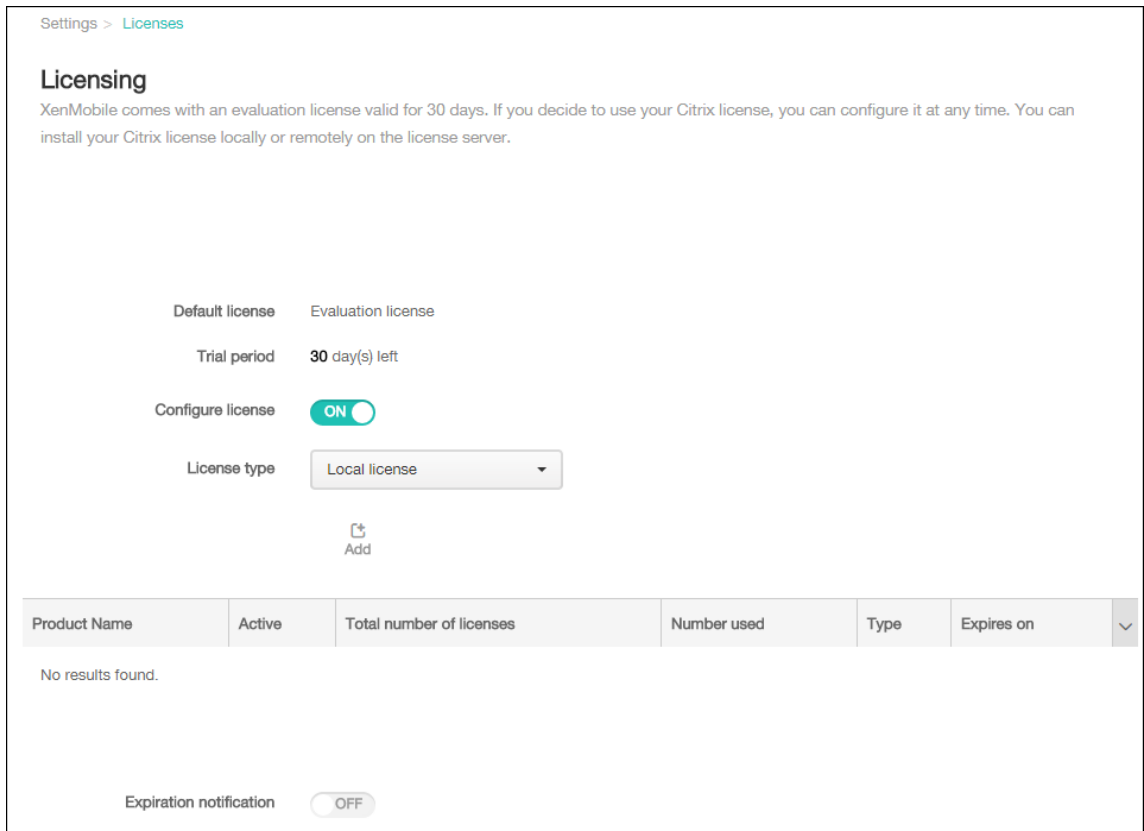
1. XenMobile 콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 라이선스를클릭합니다. 라이선스페이지가나타납니다.

로컬라이선스를추가하려면

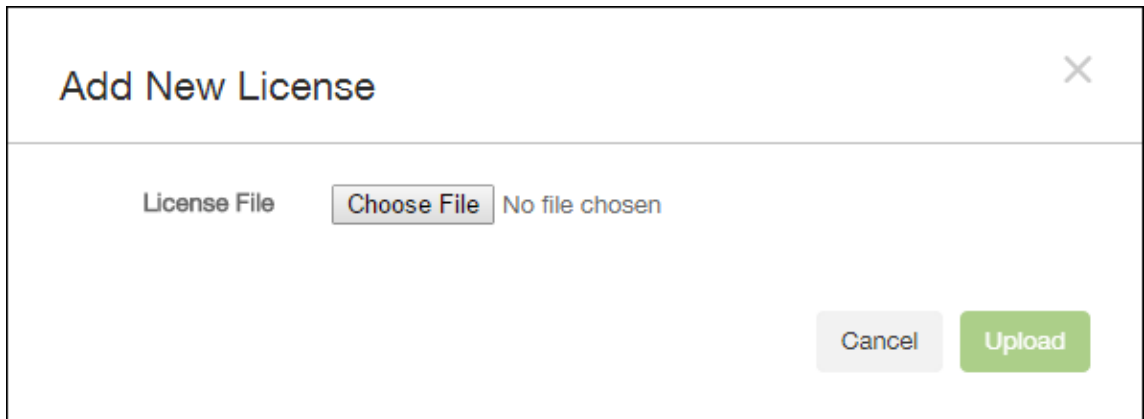
새라이선스를추가하면테이블에새라이선스가나타납니다. 추가한첫번째라이선스가자동으로활성화됩니다. 동일한범주 (예: Enterprise) 와유형의여러라이선스를추가하는경우이러한라이선스가테이블의한행에나타납니다. 이경우공통라이선스의결합된양이 총라이선스수및 사용된수에반영됩니다. 만료날짜에는공통라이선스중에서가장빠른만료날짜가표시됩니다.

모든로컬라이선스는 XenMobile 콘솔을통해관리합니다.

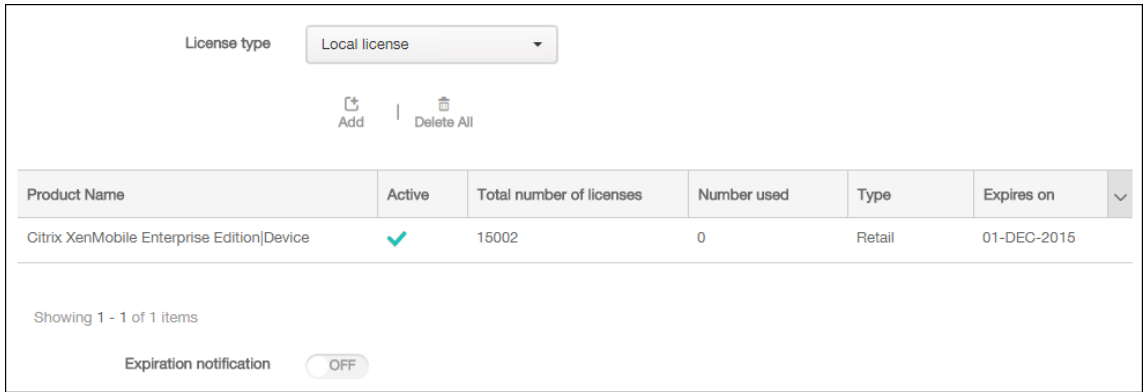
1. Simple License Service 에서 License Administration Console 을 통해라이선스파일을가져오거나 Citrix.com 계정에서직접가져옵니다. 자세한내용은 Citrix Licensing 설명서를참조하십시오.
2. XenMobile 콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
3. 라이선스를클릭합니다. 라이선스페이지가나타납니다.
4. 라이선스구성을 켜짐으로설정합니다. 라이선스유형목록, 추가단추및 라이선스테이블이표시됩니다. 라이선스테이블에는 XenMobile 에서사용한라이선스가포함됩니다. Citrix 라이선스를추가하지않은경우테이블이비어있습니다.



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



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



- 라이선스 페이지의 테이블에 나타낸 라이선스를 활성화합니다. 테이블의 첫 번째 라이선스인 경우 해당 라이선스가 자동으로 활성화됩니다.

원격 라이선스를 추가하려면

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

- 라이선스 서버 인증서를 XenMobile Server 로 가져옵니다 (설정 > 인증서).
- 기본적으로 호스트 이름 유효성 검사는 Microsoft PKI 서버를 제외 한 발신 연결에 대해 활성화됩니다. 호스트 이름 유효성 검사로 인해 배포가 중단되는 경우 서버 속성 **disable.hostname.verification** 을 **true** 로 변경하십시오. 이 속성의 기본 값은 **false** 입니다.

호스트 이름 유효성 검사가 실패하면 서버 로그에 다음과 같은 오류가 포함됩니다. “Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer(VPP 서버에 연결할 수 없습니다. 호스트 이름 ‘192.0.2.0’ 은 피어가 제공한 인증서 주체와 일치하지 않습니다.)”

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



- 다음 설정을 구성합니다.

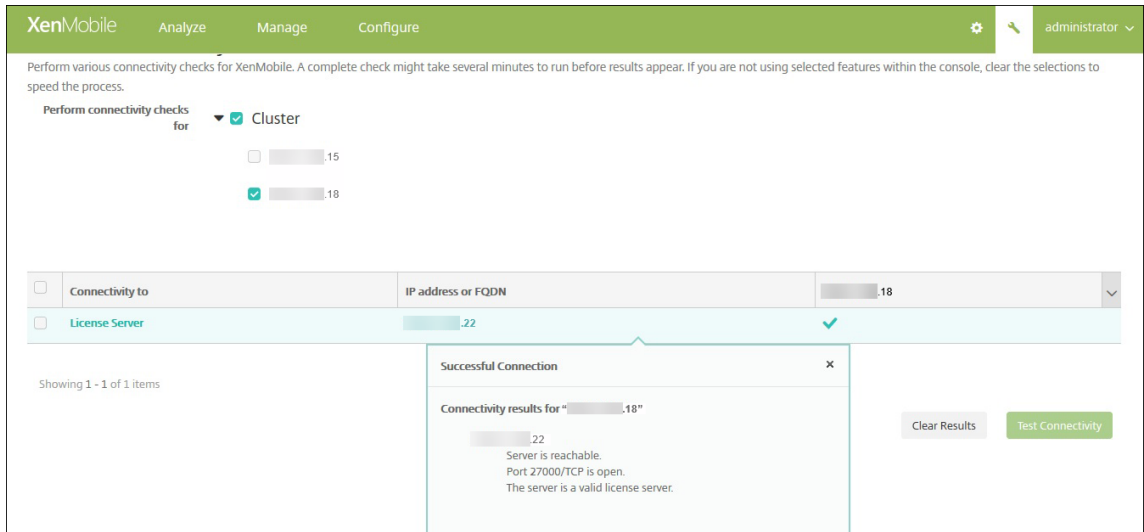
- 라이선스 서버: 원격 라이선스 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름) 을 입력합니다.
- 포트: 기본 포트를 사용하거나 라이선스 서버와의 통신에 사용할 포트 번호를 입력합니다.

6. 연결테스트를클릭합니다. 연결이성공적인경우 XenMobile 이라이센스서버에연결하고라이센스테이블이사용가능한라이센스로채워집니다. 테이블에라이센스가하나만있는경우자동으로활성화됩니다.

연결테스트를클릭하면 XenMobile 이다음을확인합니다.

- XenMobile 에서라이센스서버와통신할수있습니다.
- 라이센스서버의라이센스가유효합니다.
- 라이센스서버가 XenMobile 과호환됩니다.

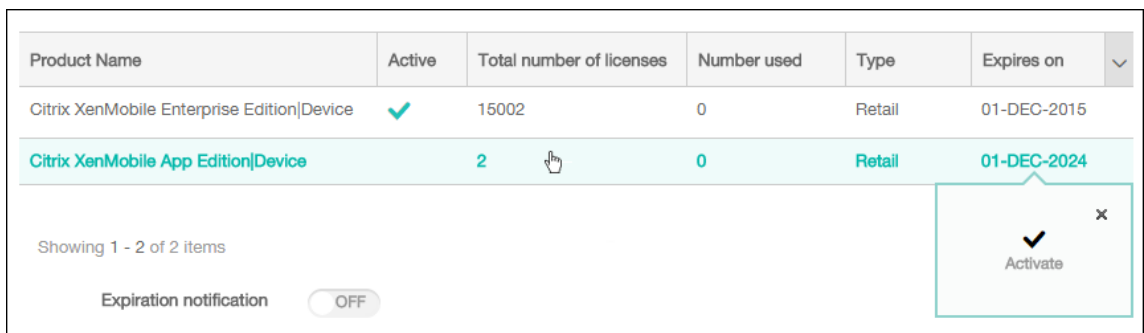
연결이실패한경우표시된오류메시지를검토하고필요한사항을수정한후 연결테스트를클릭합니다.



서로다른라이센스를활성화하려면

라이센스가여러개인경우활성화할라이센스를선택할수있습니다. 그러나한번에하나의라이센스만활성화할수있습니다.

1. 라이센스페이지의 라이센스테이블에서활성화할라이센스의행을클릭합니다. 활성화확인대화상자가행옆에나타납니다.



2. 활성화를클릭합니다. 활성화대화상자가나타납니다.

3. 활성화를클릭합니다. 선택한라이센스가활성화됩니다.

중요:

선택한라이센스를활성화하면현재라이센스가비활성화됩니다.

만료알림을자동화하려면

원격또는로컬라이센스를활성화한후라이센스만료날짜가가까워질때알림을보내도록 XenMobile 을구성할수있습니다.

1. 라이선스페이지에서 만료알림을 켜짐으로설정합니다. 새알림관련필드가나타납니다.

Expiration notification ON

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

Recipient*

Content*

2. 다음설정을구성합니다.

- 알림간격: 유형:
- 알림보낼빈도 (예: 7 일마다) 입니다.
- 알림전송을시작할시기 (예: 라이선스만료 60 일전) 입니다.
- 받는사람: 자신의전자메일주소또는라이센스담당자의전자메일주소를입력합니다.
- 내용: 받는사람이알림에서볼만료알림메시지를입력합니다.

3. 저장클릭합니다. 설정을기반으로 XenMobile 이 내용에입력된텍스트가포함된전자메일메시지를 받는사람에입력된 받는사람에게보내기시작합니다. 알림은설정빈도로전송됩니다.

FIPS 140-2 준수

May 21, 2019

미국 NIST(표준기술연구소) 에서발행한 FIPS(Federal Information Processing Standard) 는보안시스템에서사용되는 암호화모듈의보안요구사항을지정합니다. FIPS 140-2 는이표준의두번째버전입니다. NIST 가검증한 FIPS 140 모듈에대한자세한내용은 [NIST Computer Security Resource Center](#)를참조하십시오.

중요:

- XenMobile FIPS 모드는초기설치중에만설정할수있습니다.
- XenMobile 모바일기기관리전용, XenMobile 모바일앱관리전용및 XenMobile MDM+MAM 은모두 HDX 앱

을 사용하지 않는 한 FIPS 를 준수합니다.

iOS 의 모든 저장 데이터 및 전송 중 데이터 암호화 작업에는 OpenSSL 및 Apple 에서 제공하는 FIPS 인증 암호화 모듈이 사용됩니다. Android 에서 모든 저장 데이터 암호화 작업과 모바일 장치에서 NetScaler Gateway 로 전송되는 모든 전송 중 데이터 암호화 작업에는 OpenSSL 에서 제공하는 FIPS 인증 암호화 모듈이 사용됩니다.

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

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

iOS, Android 및 Windows 모바일 장치와 NetScaler Gateway 간의 모든 전송 중 데이터 암호화 작업에는 FIPS 인증 암호화 모듈이 사용됩니다. XenMobile 은 인증된 FIPS 모듈이 장착된 DMZ 호스트 NetScaler FIPS 버전 장비를 사용하여 이러한 데이터를 보호합니다. 자세한 내용은 NetScaler FIPS 설명서를 참조하십시오.

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

각 사례에 사용되는 특정 모듈을 포함한 전체 XenMobile FIPS 140-2 준수 명세서는 Citrix 담당자에게 문의하십시오.

언어 지원

October 4, 2018

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

이 문서에서는 XenMobile 의 최신 릴리스에서 지원되는 언어를 나열합니다.

XenMobile 콘솔 및 자가 지원 포털

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

모바일생산성앱

X 는 해당언어로 앱을 사용할 수 있음을 나타냅니다.

iOS 및 Android

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

Windows

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

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

오른쪽에서왼쪽으로읽는언어지원

다음표는각앱의중동언어텍스트지원을요약한것입니다. X 는해당플랫폼에서기능을사용할수있음을나타냅니다. Windows 장치에서는오른쪽에서왼쪽으로읽는언어가지원되지않습니다.

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

설치및구성

September 27, 2019

시작하기전에

다음사전설치체크리스트를사용하여온-프레미스에 XenMobile 을설치하기위한사전요구사항과설정을확인할수있습니다. 각각업또는메모에는요구사항이적용되는구성요소또는기능을나타내는열이포함되어있습니다.

XenMobile 배포를계획할때는많은요소를고려해야합니다. 전체 XenMobile 환경에대한권장사항, 일반적인질문및사용사례는 [XenMobile 배포안내서](#)를참조하십시오.

설치단계는이문서뒷부분의 [XenMobile 설치](#) 섹션을참조하십시오.

사전설치체크리스트

기본네트워크연결

다음은 XenMobile 솔루션에필요한네트워크설정입니다.

사전요구사항또는설 정	구성요소또는기능	설정메모
원격사용자가연결하 는 FQDN(정규화된 도메인이름) 을적어둡 니다.	XenMobile 및 NetScaler Gateway	
공용및로컬 IP 주소를 적어둡니다.		
방화벽을구성하여 NAT(Network Address Translation) 를설 정하려면이러한 IP 주 소가필요합니다.	XenMobile 및 NetScaler Gateway	
서브넷마스크를적어 둡니다.	XenMobile 및 NetScaler Gateway	
DNS IP 주소를적어 둡니다.	XenMobile 및 NetScaler Gateway	
WINS 서버 IP 주소 (해당하는경우) 를적 어둡니다.	NetScaler Gateway	

사전요구사항또는설 정	구성요소또는기능	설정메모	
NetScaler Gateway 호스트이름을식별하고적어둡니다.	NetScaler Gateway	이항목은 FQDN 이 아닙니다. FQDN 은 가상서버에바인딩되어있고사용자가연결하는서명된서버인증서에포함되어있습니다. NetScaler Gateway 에서설치마법사를사용하여호스트이름을구성할수 있습니다.	NetScaler Gateway
XenMobile 의 IP 주소를적어둡니다. XenMobile 의인스턴스하나를설치하는 경우 IP 주소하나를예약합니다. 클러스터를구성하는경우필요한모든 IP 주소를적어둡니다.	XenMobile		
NetScaler Gateway 에구성된공용 IP 주소 1 개	NetScaler Gateway		
NetScaler Gateway 에대한외부 DNS 항목 1 개	NetScaler Gateway		
웹프록시서버 IP 주소, 포트, 프록시호스트목록및관리자사용자이름/암호를적어둡니다. 회사네트워크(해당하는경우) 에프록시서버를배포하는경우이러한설정에선택사항입니다.	NetScaler Gateway	웹프록시에대한사용자이름을구성할때 sAMAccount-Name 또는 UPN(사용자계정이름) 을사용할수있습니다.	XenMobile 및 NetScaler Gateway

사전요구사항또는설 정	구성요소또는기능	설정메모
기본게이트웨이 IP 주 소를적어둡니다.	XenMobile 및 NetScaler Gateway	
시스템 IP(NSIP) 주 소및서브넷마스크를 적어둡니다.	NetScaler Gateway	
서브넷 IP(SNIP) 주 소및서브넷마스크를 적어둡니다.	NetScaler Gateway	
인증서에서 NetScaler Gateway 가상서버 IP 주소및 FQDN 을 적어둡니다. 다수의 가상서버를구성하려 면인증서의모든가상 IP 주소및 FQDN 을 적어둡니다.	NetScaler Gateway	
사용자가 NetScaler Gateway 를통해액 세스할수있는내부네 트워크를적어둡니다. 예: 10.10.0.0/24. 분할터널링이켜짐으 로설정된경우사용자 가 Secure Hub 또 는 NetScaler Gateway 플러그인 에연결할때액세스해 야하는모든내부네트 워크및네트워크세그 먼트를입력합니다.	NetScaler Gateway	

사전요구사항또는설

정	구성요소또는기능	설정메모
---	----------	------

XenMobile Server, NetScaler Gateway, 외부 Microsoft SQL Server 및 DNS 서버간의네트워크연결 이접속가능한지확인 합니다.	XenMobile 및 NetScaler Gateway	
--	-------------------------------	--

라이선스

XenMobile 을사용하려면 NetScaler Gateway 및 XenMobile 에대한라이선스옵션을구입해야합니다. Citrix 라이선스 에대한자세한내용은 [Citrix Licensing 시스템](#)을참조하십시오.

사전요구사항	구성요소	위치메모
--------	------	------

Citrix 웹사이트에서범용라이선스를 구입합니다. 자세한내용은 NetScaler Gateway 설명서에서 Licensing(라이선스) 을참조하십시오.	NetScaler Gateway, XenMobile 및 Citrix License Server	
---	--	--

인증서

XenMobile 및 NetScaler Gateway 를사용자장치다른 Citrix 제품및앱과연결하려면인증서가필요합니다. 자세한내용은 XenMobile 설명서의 [인증서및인증](#) 섹션을참조하십시오.

사전요구사항	구성요소	참고
--------	------	----

필요한인증서를받고설치합니다.	XenMobile 및 NetScaler Gateway	
-----------------	-------------------------------	--

포트

XenMobile 구성요소와통신할수있도록포트를열립니다.

사전요구사항	구성요소	참고
XenMobile 포트를열립니다.	XenMobile 및 NetScaler Gateway	

데이터베이스

XenMobile 에데이터베이스연결을구성해야합니다. XenMobile 저장소에는 [시스템요구사항및호환성](#)에명시된지원되는버전 중하나에서실행되는 Microsoft SQL Server 데이터베이스가필요합니다. Microsoft SQL 은원격으로사용하는것이좋습니다. PostgreSQL 은 XenMobile 에포함되어있으며 테스트환경에서만로컬또는원격으로사용할수있습니다.

기본적으로 XenMobile 은 jTDS 데이터베이스드라이버를 사용합니다. XenMobile Server 의온-프레미스설치에 Microsoft JDBC 드라이버를사용하려면 [SQL Server 드라이버](#)를참조하십시오.

사전요구사항	구성요소	참고
Microsoft SQL Server, IP 주소및 포트. XenMobile 에사용할 SQL Server 서비스계정에 DBcreator 역할권한이있는지확인합니다.	XenMobile	

Active Directory 설정

사전요구사항	구성요소	참고
주서버와보조서버의 Active Directory IP 주소및포트를적어둡니다. 포트 636 을사용하는경우 XenMobile 에서 CA 의루트인증서를설치하고보안연결사용옵션을예로변경합니다.	XenMobile 및 NetScaler Gateway	
Active Directory 도메인이름을적어둡니다.	XenMobile 및 NetScaler Gateway	

사전요구사항	구성요소	참고
Active Directory 서비스계정을 사용자 ID, 암호및도메인별칭을포함하여 적어둡니다.		
Active Directory 서비스계정은 XenMobile 이 Active Directory 에쿼리할때사용하는계정입니다.	XenMobile 및 NetScaler Gateway	
사용자가위치한디렉터리수준을나타내는사용자기본 DN 을적어둡니다. 예: <code>cn=users,dc=ace,dc=com</code> . NetScaler Gateway 및 XenMobile 은사용자기본 DN 을사용하여 Active Directory 에쿼리합니다.	XenMobile 및 NetScaler Gateway	
그룹이위치한디렉터리수준을나타내는 그룹기본 DN 을적어둡니다. NetScaler Gateway 및 XenMobile 은이 DN 을사용하여 Active Directory 에쿼리합니다.	XenMobile 및 NetScaler Gateway	

XenMobile 과 NetScaler Gateway 간연결

사전요구사항	구성요소	설정메모
XenMobile 호스트이름을적어둡니다.	XenMobile	
XenMobile 의 FQDN 또는 IP 주소 를적어둡니다.	XenMobile	
사용자가액세스할수있는앱을파악합니다.	NetScaler Gateway	
콜백 URL 을적어둡니다.	XenMobile	

사용자연결: **Citrix Virtual Apps and Desktops** 및 **Citrix Secure Hub** 액세스

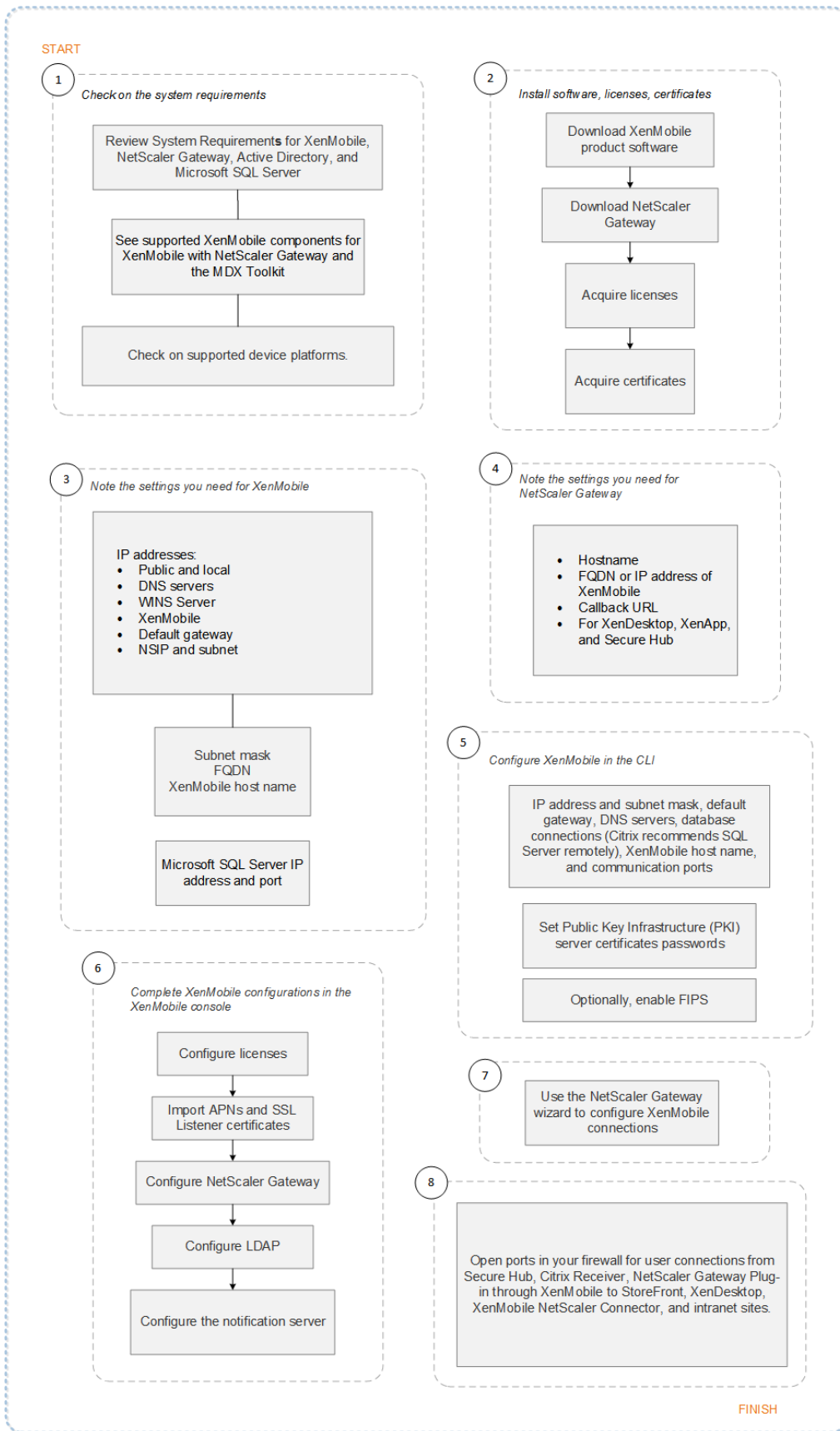
NetScaler 의 Quick Configuration(빠른구성) 마법사를사용하여 XenMobile 과 NetScaler Gateway 간의연결설정 및 XenMobile 과 Secure Hub 간의연결설정을구성하는것이 좋습니다. 두번째가상서버를생성하여 Citrix Receiver 와웹브

라우저에서사용자연결을사용하도록설정합니다. 이러한연결은 Virtual Apps and Desktops 에있는 Windows 기반응용프로그램과가상데스크톱에대한연결입니다. 이러한설정도 NetScaler 의 Quick Configuration(빠른구성) 마법사를사용하여구성하는것이 좋습니다.

사건요구사항	구성요소	설정메모
NetScaler Gateway 호스트이름및 외부 URL 을적어둡니다. 외부 URL 은사용자가연결하는웹주소입니다.	XenMobile	
NetScaler Gateway 콜백 URL 을 적어둡니다.	XenMobile	
가상서버의 IP 주소와서브넷마스크를 적어둡니다.	NetScaler Gateway	
Program Neighborhood Agent 또는 Virtual Apps and Desktops 사이트의경로를적어둡니다.	NetScaler Gateway 및 XenMobile	
STA(Secure Ticket Authority) 를실행하는 Virtual Apps and Desktops 서버의 FQDN 또는 IP 주소를적어둡니다 (ICA 연결에만해당).	NetScaler Gateway	
XenMobile 의공용 FQDN 을적어둡니다.	NetScaler Gateway	
Secure Hub 의공용 FQDN 을적어둡니다.	NetScaler Gateway	

XenMobile 배포순서도

이순서도에서는 XenMobile 을배포하는주요단계를안내합니다. 각단계에대한항목으로연결되는링크가그림다음에옵니다.



1: [시스템요구사항및호환성](#)

2: [설치및구성](#)

3 및 4: [사전설치체크리스트 \(이문서\)](#)

5: [명령프롬프트창에서 XenMobile 구성 \(이문서\)](#)

6: [웹브라우저에서 XenMobile 구성 \(이문서\)](#)

7: [XenMobile 환경에대한설정구성](#)

8: [포트요구사항](#)

XenMobile 설치

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

참고:

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

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

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

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

- 적절한 시스템 리소스가 있는 컴퓨터에 Windows Server 2008 R2, Windows Server 2012 또는 Windows Server 2012 R2 를 설치하고 Hyper-V 와 역할을 사용하도록 설정합니다. Hyper-V 역할을 설치할 때 Hyper-V 에서 가상 네트워크를 만드는 데 사용할 서버에서 NIC 를 지정해야 합니다. 일부 NIC 는 호스트용으로 남겨둘 수 있습니다.
- Virtual Machines/*<build-specific UUID>*.xml 파일을 삭제합니다.
- Legacy/*<build-specific UUID>*.exp 파일을 Virtual Machines 로 이동합니다.

Windows Server 2008 R2 또는 Windows Server 2012 를 설치하는 경우 다음을 수행합니다.

VM 구성을 나타내는 Hyper-V 매니페스트 파일에 두 가지 버전 (.exp 및 .xml) 이 있기 때문에 이러한 단계가 필요합니다. Windows Server 2008 R2 및 Windows Server 2012 릴리스는 .exp 만 지원합니다. 이러한 릴리스의 경우 설치 전에 .exp 매니페스트 파일만 있어야 합니다.

Windows Server 2012 R2 에서는 이러한 추가 단계가 필요 없습니다.

FIPS 140-2 모드. XenMobile Server 를 FIPS 모드로설치하려는 경우 [XenMobile](#) 을 사용하여 FIPS 구성에나온일련의 사전요구사항을완료합니다.

XenMobile 제품소프트웨어다운로드

[Citrix 웹사이트](#)에서제품소프트웨어를다운로드할수있습니다. 사이트에로그온한후 [Download\(다운로드\)](#) 링크를사용하여다운로드할소프트웨어가있는페이지로이동합니다.

XenMobile 소프트웨어를다운로드하려면

1. [Citrix 웹사이트](#)로이동합니다.
2. Search(검색) 상자옆에있는 **Log On(로그온)** 을클릭하여계정에로그온합니다.
3. **Downloads(다운로드)** 탭을클릭합니다.
4. Downloads(다운로드) 페이지의제품선택목록에서 **XenMobile** 을클릭합니다.



5. **Go(이동)** 를클릭합니다. XenMobile 페이지가나타납니다.
6. **XenMobile Server** 를확장합니다.
7. **Product Software(제품소프트웨어)** 를확장합니다.
8. **XenMobile Server 10** 을클릭합니다.
9. **Jump to Download(다운로드로이동)** 메뉴를클릭하고 XenMobile 을설치할때사용할가상이미지를선택합니다. 또는페이지를아래로스크롤하여설치할이미지에대한 **Download File(파일다운로드)** 단추를찾습니다.
10. 화면의지침을따라소프트웨어를다운로드합니다.

NetScaler Gateway 소프트웨어를다운로드하려면

NetScaler Gateway 가상장비또는소프트웨어업그레이드를기존 NetScaler Gateway 장비에다운로드하려면다음절차를사용합니다.

1. [Citrix 웹사이트](#)로이동합니다.
2. Citrix 웹사이트에아직로그온하지않은경우 Search(검색) 상자옆에있는 **Log On(로그온)** 을클릭하여계정에로그온합니다.

3. **Downloads**(다운로드) 탭을클릭합니다.
4. Downloads(다운로드) 페이지의제품선택목록에서 **NetScaler Gateway** 를클릭합니다.
5. **Go**(이동) 를클릭합니다. NetScaler Gateway 페이지가나타납니다.
6. NetScaler Gateway 페이지에서실행중인 NetScaler Gateway 버전을확장합니다.
7. **Firmware**(펌웨어) 아래에서다운로드할장비소프트웨어버전을클릭합니다.

참고:

Virtual Appliances(가상장비) 를클릭하여 NetScaler VPX 를다운로드할수도있습니다. 이옵션을선택하면 각하이퍼바이저에대한가상컴퓨터용소프트웨어목록이나타납니다.

8. 다운로드하려는장비소프트웨어버전을클릭합니다.
9. 다운로드하려는버전의장비소프트웨어페이지에서해당가상장비에대해 **Download**(다운로드) 를클릭합니다.
10. 화면의지침을따라소프트웨어를다운로드합니다.

처음사용을위한 **XenMobile** 구성

1. XenMobile 에대한 IP 주소와서브넷마스크, 기본게이트웨이, DNS 서버등을구성하려면 XenCenter 또는 vSphere 명령줄콘솔을사용합니다.

참고:

vSphere 웹클라이언트를사용하는경우 **Customize template**(사용자지정템플릿) 페이지에서 OVF 템플릿을배포할때네트워크속성을구성하지않는것이 좋습니다. 이렇게하면고가용성구성에서복제후두번째 XenMobile 가상컴퓨터를다시시작할때발생하는 IP 주소관련문제를방지할수있습니다.

2. XenMobile Server 의정규화된도메인이름또는노드의 IP 주소를통해서만 XenMobile 관리콘솔에액세스합니다.
3. 로그인후초기로그온화면의단계를수행합니다.

명령프롬프트창에서 **XenMobile** 구성

1. XenMobile 가상컴퓨터를 Citrix XenServer, Microsoft Hyper-V 또는 VMware ESXi 로가져옵니다. 자세한내용은 [XenServer](#), [Hyper-V](#) 또는 [VMware](#) 설명서를참조하십시오.
2. 하이퍼바이저에서, 가져온 XenMobile 가상컴퓨터를선택하고명령프롬프트보기를시작합니다. 자세한내용은해당하이퍼바이저의설명서를참조하십시오.
3. 하이퍼바이저의콘솔페이지에서명령프롬프트창에관리자의사용자이름및암호를입력하여 XenMobile 의관리자계정을만듭니다.

중요:

명령프롬프트관리자계정, PKI(공개키인프라) 서버인증서및 FIPS 의암호를만들거나변경하는경우 XenMobile 외부에서암호가관리되는 Active Directory 사용자를제외한모든사용자에대해다음규칙이적용됩니다.

- 암호는 8 자이상이어야합니다.
- 암호는다음복잡성기준중최소 3 개를충족해야합니다.
 - 대문자 (A ~ Z)
 - 소문자 (a ~ z)
 - 숫자 (0 ~ 9)
 - 특수문자 (예: ! ## \$ %)

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

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

새암호를입력할때별표와같은문자는표시되지않습니다.

4. 다음네트워크정보를입력한후 **y** 를입력하여설정을적용합니다.

- a) XenMobile Server 의 IP 주소
- b) 넷마스크
- c) 기본게이트웨이 - DMZ 에있는기본게이트웨이의 IP 주소
- d) 주 DNS 서버 - DNS 서버의 IP 주소
- e) 보조 DNS 서버 (선택사항)

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

참고:

이이미지와다음이미지에표시된주소는작동하지않는주소이며예를위해서만제공되었습니다.

5. 무작위암호화암호를생성하여보안을강화하려면 **y** 를입력하고고유한암호를제공하려면 **n** 을입력합니다. **y** 를입력하여무작위암호를생성하는것이 좋습니다.

암호는중요한데이터를보호하는데사용되는암호화키의보호차원에서사용됩니다. 데이터의암호화및암호해독시서버파일시스템에서저장된암호해시를사용하여키가검색됩니다. 암호는볼수없습니다.

참고:

환경을확장하고추가서버를구성하려는경우고유한암호를제공합니다. 무작위암호를선택하는경우암호를볼수없습니다.

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

- 필요한경우 FIPS(Federal Information Processing Standard) 를사용하도록설정합니다. FIPS 에대한자세한 내용은 FIPS를참조하십시오. 또한 XenMobile 을사용하여 FIPS 구성에설명된대로일련의사전요구사항을충족해야합니다.

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

- 다음정보를제공하여데이터베이스연결을구성합니다.

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

- 데이터베이스는로컬또는원격일수있습니다. 로컬인경우 **l** 을입력하고원격인경우 **r** 을입력합니다.
- 데이터베이스유형을선택합니다. Microsoft SQL 인경우 **mi** 를입력하고 PostgreSQL 인경우 **p** 를입력합니다.

중요:

- Microsoft SQL 은원격으로사용하는것이 좋습니다. PostgreSQL 은 XenMobile 에포함되어있으며 테스트환경에서만로컬또는원격으로사용할수있습니다.
- 데이터베이스마이그레이션은지원되지않습니다. 테스트환경에서만데이터베이스를프로덕션환경으로이동할수없습니다.

- 필요한경우 **y** 를입력하여데이터베이스에대한 SSL 인증을사용합니다.
- XenMobile 을호스트하는서버의 FQDN(정규화된도메인이름) 을입력합니다. 이하나의호스트서버에서장치관리와애플관리서비스를모두제공합니다.
- 기본포트번호와다른경우해당데이터베이스포트번호를입력합니다. Microsoft SQL 의기본포트는 1433 이고 PostgreSQL 의기본포트는 5432 입니다.
- 데이터베이스관리자의사용자이름을입력합니다.

- 데이터베이스관리자의암호를입력합니다.
- 데이터베이스이름을입력합니다.
- **Enter** 키를눌러데이터베이스설정을적용합니다.

8. 필요한경우 **y** 를입력하여 XenMobile 노드또는인스턴스의클러스터를사용하도록설정합니다.

중요:

XenMobile 클러스터를사용하도록설정하는경우시스템구성이완료된후클러스터구성원간의실시간통신이가능하도록포트 80 을열어야합니다. 모든클러스터노드에대해이설정을완료합니다.

9. XenMobile Server 의 FQDN(정규화된도메인이름) 을입력합니다.

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

10. **Enter** 키를눌러설정을적용합니다.

11. 통신포트를확인합니다. 포트와용도에대한자세한내용은 [포트요구사항](#)을참조하십시오.

참고:

Enter(Mac 의경우 Return) 키를눌러기본포트를적용합니다.

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

12. XenMobile 을처음으로설치하는것이므로이전 XenMobile 릴리스에서의업그레이드에대한다음질문은건너뛰니다.

13. 각 PKI(공개키인프라) 인증서에동일한암호를사용하려면 **y** 를입력합니다. XenMobile PKI 기능에대한자세한내용은 [인증서업로드](#)를참조하십시오.

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

중요:

XenMobile 의노드또는인스턴스를함께클러스터링하려는경우후속노드에동일한암호를제공합니다.

14. 새암호를입력한다음, 확인을위해새암호를다시입력합니다.

새암호를입력할때별표와같은문자는표시되지않습니다.

15. **Enter** 키를눌러설정을적용합니다.
16. 웹브라우저에서 XenMobile 콘솔에로그온할때사용할관리자계정을만듭니다. 이러한자격증명을기록하여나중에사용할수있도록하십시오.

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

참고:

새암호를입력할때별표와같은문자는표시되지않습니다.

17. **Enter** 키를눌러설정을적용합니다. 초기시스템구성이저장됩니다.
18. 새로운설치이므로업그레이드중인지묻는메시지가나타나면 **n** 을입력합니다.
19. 화면에나타나는전체 URL 을복사하고웹브라우저에서이초기 XenMobile 구성을계속합니다.

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

Initial system configuration complete!

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

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

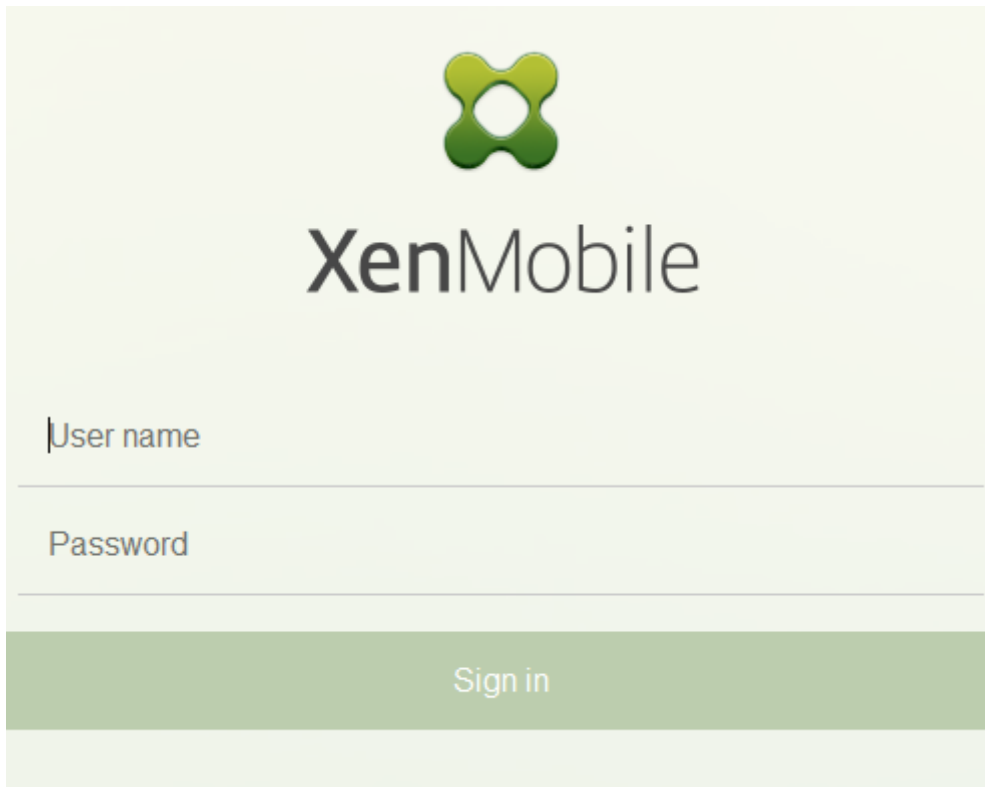
To access the console, from a web browser, go to the following location and
log on with your console credentials:
https://203.0.113.8:4443/

Starting monitoring... [ OK ]
```

웹브라우저에서 XenMobile 구성

하이퍼바이저명령프롬프트창에서 XenMobile 구성의초기부분을완료한후웹브라우저에서프로세스를완료합니다.

1. 웹브라우저에서, 명령프롬프트창구성의마지막부분에제공된위치로이동합니다.
2. 명령프롬프트창에서만든 XenMobile 콘솔관리자계정의사용자이름및암호를입력합니다.



3. 시작페이지에서 시작을클릭합니다. 라이선스페이지가나타납니다.
4. 라이선스를구성합니다. 라이선스를업로드하지않는경우 30 일동안유효한평가라이선스를사용합니다. 라이선스를추가및 구성하고만료알림을구성하는방법에대한자세한내용은 [라이선스](#)를참조하십시오.

중요:

XenMobile 의클러스터노드또는인스턴스를추가하여 XenMobile 클러스터링을사용하려는경우원격서버에서 Citrix Licensing 을사용해야합니다.

5. 인증서페이지에서 가져오기를클릭합니다. 가져오기대화상자가나타납니다.
6. APNs 및 SSL 수신기인증서를가져옵니다. iOS 장치를관리하려면 APNs 인증서가필요합니다. 인증서사용방법에대한 자세한내용은 [인증서](#)를참조하십시오.

참고:

이단계를수행하려면서버를다시시작해야합니다.

7. 환경에해당되는경우 NetScaler Gateway 를구성합니다. NetScaler Gateway 구성에대한자세한내용은 [NetScaler Gateway 및 XenMobile](#)과 [XenMobile 환경에대한설정구성](#)을참조하십시오..

참고:

- 내부네트워크경계 (또는인트라넷) 에 NetScaler Gateway 를배포할수있습니다. 이배포는내부네트워크 에잇는서버, 앱및기타네트워크리소스에대한안전한단일지점엑세스를제공합니다. 이배포에서는모든원격사용자가내부네트워크리소스에엑세스하기위해먼저 NetScaler Gateway 에연결해야합니다.

- NetScaler Gateway 는선택적인설정이지만이페이지에서데이터를입력한후에페이지에서나가려면모든필수필드를지우거나작성해야합니다.

8. Active Directory 에서사용자및그룹에엑세스하려면 LDAP 구성을완료합니다. LDAP 연결을구성하는방법에대한자세한내용은 [LDAP 구성](#)을참조하십시오.

9. 사용자에게메시지를보낼수있도록알림서버를구성합니다. 알림서버구성에대한자세한내용은 [알림](#)을참조하십시오.

사후요구사항. XenMobile Server 를다시시작하여인증서를활성화합니다.

XenMobile 을사용하여 FIPS 구성

January 6, 2020

XenMobile 의 FIPS(Federal Information Processing Standard) 모드는모든암호화작업에 FIPS 140-2 인증라이브러리만사용하여미국연방정부고객을지원합니다. FIPS 모드를사용하여 XenMobile Server 를설치하면 XenMobile 클라이언트와서버의모든데이터가 FIPS 140-2 를완벽하게준수합니다. 이러한준수는저장된데이터와전송중데이터에적용됩니다.

FIPS 모드로 XenMobile Server 를설치하기전에다음과같은사전요구사항을충족합니다.

- XenMobile 데이터베이스외부 SQL Server 2012 또는 SQL Server 2014 를사용합니다. 또한보안 SSL 통신을사용하도록 SQL Server 를구성해야합니다. SQL Server 에대한보안 SSL 통신을구성하는지침은 [SQL Server 온라인설명서](#)를참조하십시오.
- 보안 SSL 통신을사용하려면 SQL Server 에잘알려진 CA(인증기관) 의신뢰할수있는 SSL 인증서를설치해야합니다. SQL Server 2014 에는와일드카드인증서를사용할수없습니다. 따라서 SQL Server FQDN 을사용하여 SSL 인증서를요청하는것이 좋습니다.

FIPS 모드구성

FIPS 모드는 XenMobile Server 를처음설치하는동안에만사용하도록설정할수있습니다. 설치가완료된후에는 FIPS 를사용하도록설정할수없습니다. 따라서 FIPS 모드를사용하려는경우처음부터 FIPS 모드로 XenMobile Server 를설치해야합니다. 또한 XenMobile 클러스터의경우모든클러스터노드에서 FIPS 를사용해야합니다. FIPS 와비 FIPS XenMobile Server 를동일한클러스터에혼합하여배치할수없습니다.

XenMobile 명령줄인터페이스에 **Toggle FIPS mode(FIPS 모드전환)** 가있지만이는프로덕션용도가아닙니다. 이옵션은비프로덕션및진단용으로제공되며프로덕션 XenMobile Server 에서지원되지않습니다.

1. 초기설정시 **FIPS** 모드를사용하도록설정합니다.
2. SQL Server 에대한루트 CA 인증서를업로드합니다.
3. SQL Server 의서버이름및포트, SQL Server 에로그인하는데사용할자격증명, XenMobile 에대해만들데이터베이스 이름을지정합니다.

참고:

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

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

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

인증서가져오기

다음 절차는 인증서를 가져와 XenMobile 에서 FIPS 를 구성하는 방법을 설명합니다. 이는 VMware 하이퍼바이저를 사용하는데 필요합니다.

SQL 사전요구사항

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

IIS(인터넷정보서비스) 사전요구사항

1. 루트인증서 (base 64) 를다운로드합니다.
2. 루트인증서를 IIS 서버의기본사이트 (C:\inetpub\wwwroot) 로복사합니다.
3. 기본사이트에대해 인증확인란을선택합니다.
4. 익명을 사용으로설정합니다.
5. 실패한요청추적규칙확인란을선택합니다.
6. .cer 이차단되지않았는지확인합니다.
7. 로컬서버의 Internet Explorer 브라우저에서.cer 위치 (<https://localhost/certname.cer>) 로이동합
니다. 루트인증서텍스트가브라우저에나타납니다.
8. Internet Explorer 브라우저에루트인증서가표시되지않을경우다음과같이 IIS 서버에서 ASP 를사용하도록설정되어
있는지확인합니다.
 - a) 서버관리자를열니다.
 - b) 관리 > 역할및기능추가에서마법사로이동합니다.
 - c) 서버역할에서 웹서버 (IIS), 웹서버, 응용프로그램개발을차례로확장한후 **ASP** 를선택합니다.
 - d) 설치가완료될때까지 다음을클릭합니다.
9. Internet Explorer 를열고 <https://localhost/cert.cer>로이동합니다.

자세한내용은 [웹서버 \(IIS\)](#)에서참조하십시오.

참고:

이절차에 CA 의 IIS 인스턴스를사용할수있습니다.

초기 FIPS 구성시루트인증서가져오기

명령줄콘솔에서처음으로 XenMobile 구성단계를완료하는경우다음설정을완료하여루트인증서를가져와야합니다. 설치단계에
대한자세한내용은 [XenMobile 설치](#)를참조하십시오.

- Enable FIPS: Yes
- Upload Root Certificate: Yes
- Copy(c) or Import(i): i
- Enter HTTP URL to import: <https://<FQDN of IIS server>/cert.cer>
- Server: *SQL Server* 의 *FQDN*
- Port: 1433
- User name: 데이터베이스를만들수있는서비스계정 (domain\username)
- Password: 서비스계정의암호
- Database Name: 원하는이름

모바일장치에서 **FIPS** 모드사용

기본적으로모바일장치에서는 **FIPS** 모드가사용되지않습니다. **FIPS** 모드를사용하려면 설정 > 클라이언트속성으로이동하고 **FIPS** 모드사용속성을편집하여값을 **true** 로설정합니다. 자세한내용은 [클라이언트속성](#)에서참조하십시오.

클러스터링구성

January 6, 2020

클러스터링을구성하려면 NetScaler 에다음두부하분산가상 IP 주소를구성합니다.

- **MDM(모바일기기관리) 부하분산가상 IP 주소:** 클러스터로구성된 XenMobile 노드와통신하려면 MDM 부하분산가상 IP 주소가필요합니다. 이부하분산은 SSL 브리지모드에서수행됩니다.
- **MAM(모바일앱관리) 부하분산가상 IP 주소:** NetScaler Gateway 에서클러스터로구성된 XenMobile 노드와통신하려면 MAM 부하분산가상 IP 주소가필요합니다. XenMobile 에서는기본적으로 NetScaler Gateway 의모든트래픽이포트 8443 의부하분산가상 IP 주소로전달됩니다.

이문서에나와있는절차는새로운 XenMobile VM(가상컴퓨터) 을만들고새 VM 을기존 VM 에연결하는방법을설명합니다. 이러한단계를수행하면클러스터설정이만들어집니다.

사전요구사항

- 필요한 XenMobile 노드가완전히구성되어있어야합니다.
- 모든클러스터노드와 XenMobile 데이터베이스에 NTP 를구성합니다. 클러스터링이올바르게작동하려면이러한모든서버의시간이동일해야합니다.
- MDM 부하분산장치용공용 IP 주소하나와 MAM 용사설 IP 주소하나
- 서버인증서
- NetScaler Gateway 가상 IP 주소에사용할가용 IP 주소하나
- 클러스터설치및 MDM 전용또는엔터프라이즈모드 (MDM+MAM) 에서 XenMobile 을배포한경우: 모든 NetScaler MDM 부하분산장치, 즉포트 8443 및 443 에대해설정된가상서버에 **Source IP persistence(소스 IP 지속성)** 를사용하도록 NetScaler 부하분산장치구성을수정합니다. 이구성은사용자장치를 iOS 11 로업그레이드하기전에완료되어야합니다. 자세한내용은이 Citrix Knowledge Center 문서 (<https://support.citrix.com/article/CTX227406>) 를참조하십시오.
- iOS 11 장치의 XenMobile Store 에서앱을설치하려면 XenMobile Server 에서포트 80 을사용하도록설정해야합니다.

클러스터링된구성의 XenMobile 10.x 에대한참조아키텍처다이어그램은 [아키텍처](#)를참조하십시오.

XenMobile 클러스터노드설치

필요한노드수에따라 XenMobile VM 을만듭니다. 새 VM 이동일한데이터베이스를가리키도록하고동일한 PKI 인증서암호를제 공합니다.

1. 새 VM 의명령줄콘솔을열고관리자계정에대한새암호를입력합니다.

```

*****
*           Citrix XenMobile           *
*   (in First Time Use mode)         *
*****

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

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

2. 다음그림에표시된것과같이네트워크구성세부정보를제공합니다.

```

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

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

3. 데이터보호를위해기본암호를사용하려면 **y** 를입력합니다. 또는 **n** 을입력한후새암호를입력합니다.

```

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

4. FIPS 를사용하려면 **y** 를입력하고그렇지않으면 **n** 을입력합니다.

```

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

5. 이전에완벽하게구성된 VM 이가리키는동일한데이터베이스를가리키도록데이터베이스를구성합니다. “Database already exists(데이터베이스가이미있습니다)” 라는메시지가표시됩니다.

```

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

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

Commit settings (y/n) [y]:
Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..
    
```

6. 첫번째 VM 에 대해 제공한 것과 동일한 인증서 암호를 입력합니다.

```

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

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

Commit settings (y/n) [y]:

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

Saving server and client certificate passwords..

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

- 암호를 입력하면 두번째 노드에 대한 초기 구성이 완료됩니다.


```

Saving server and client certificate passwords..

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

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

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

7. 구성이 완료되면서 서버가 다시 시작되고 로그인 대화상자가 나타납니다.

```

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

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

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

Starting monitoring... [ OK ]

xms51.wg.lab login:
    
```

참고:

로그인 대화상자는 첫 번째 VM 의 로그인 대화상자와 동일합니다. 두 대화상자가 일치하는 것을 통해 두 VM 이동 일한 데 이터베이스 서버를 사용한다는 것을 확인할 수 있습니다.

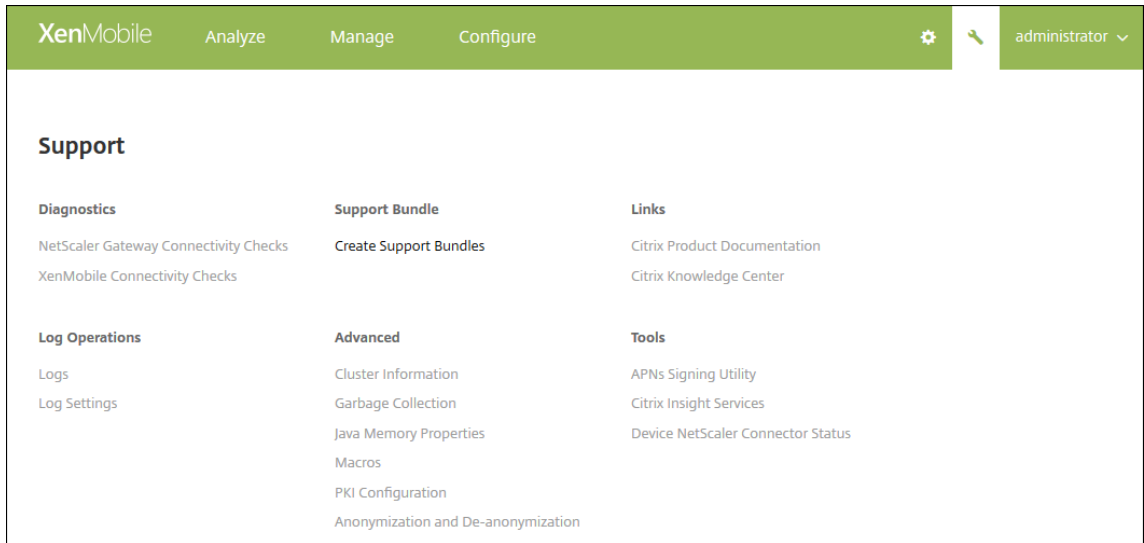
8. XenMobile 의 FQDN(정규화된 도메인 이름) 을 사용하여 웹 브라우저에서 XenMobile 콘솔을 엽니다.

9. XenMobile 콘솔에서 오른쪽 위 모서리의 렌치 아이콘을 클릭합니다.

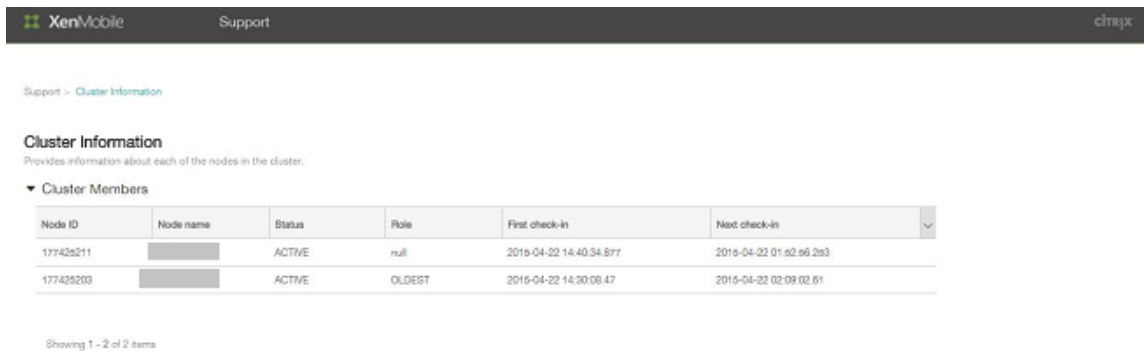


지원 페이지가 열립니다.

10. 고급아래에서 클러스터정보를클릭합니다.



클러스터구성원, 장치연결정보, 작업등을포함하여클러스터에대한모든정보가나타납니다. 이제새노드가클러스터의구성원이됩니다.

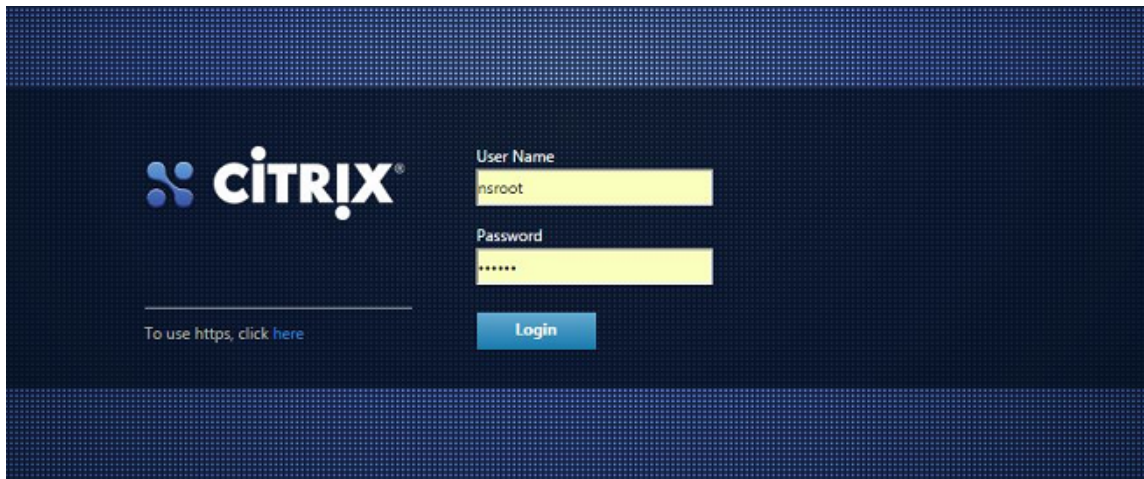


동일한단계를수행하여다른노드를추가할수있습니다. 클러스터에추가된첫번째노드는 **OLDEST** 역할을갖습니다. 그후에추가된노드에는 **NONE** 또는 **null** 역할이표시됩니다.

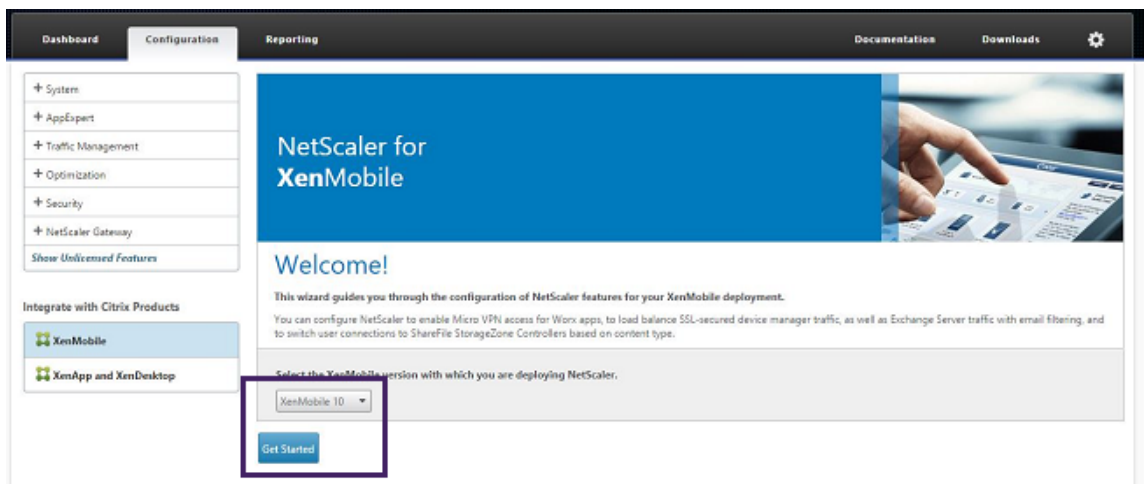
NetScaler 에서 XenMobile 클러스터에대한부하분산을구성하려면

필요한노드를 XenMobile 클러스터의구성원으로추가한후에는노드가클러스터에액세스할수있도록부하를분산합니다. 부하분산을수행하려면 NetScaler 에서사용할수있는 XenMobile 마법사를실행합니다. 다음단계는마법사를실행하여 XenMobile 의부하를분산하는방법을설명합니다.

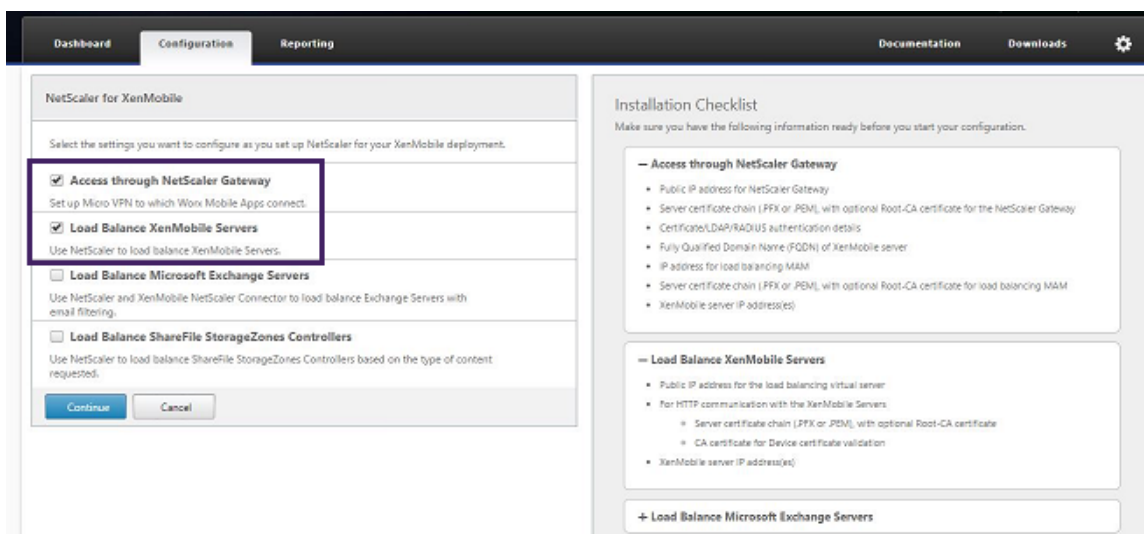
1. NetScaler 에로그온합니다.



2. Configuration(구성) 탭에서 **XenMobile** 을클릭하고 **Get Started(시작)** 를클릭합니다.



3. **Access through NetScaler Gateway(NetScaler Gateway 를통해액세스)** 확인란과 **Load Balance XenMobile Servers(XenMobile Server 부하분산)** 확인란을선택한후 **Continue(계속)** 를클릭합니다.



4. NetScaler Gateway 의 IP 주소를입력하고 **Continue(계속)** 를클릭합니다.

The screenshot shows the 'NetScaler Gateway Configuration' page. Under the 'NetScaler Gateway Settings' section, there are three input fields: 'NetScaler Gateway IP Address*' with the value '10 . 147 . 75 . 54', 'Port*' with the value '443', and 'Virtual Server Name*' with the value 'XenMobileGateway'. At the bottom of this section are 'Continue' and 'Cancel' buttons.

5. 다음중하나를수행하여서버인증서를 NetScaler Gateway 가상 IP 주소에바인딩한후 **Continue(계속)** 를클릭합니다.

- **Use existing certificate(기존인증서사용)** 에서, 목록에서해당서버인증서를선택합니다.
- **Install Certificate(인증서설치)** 탭을클릭하여새서버인증서를업로드합니다.

The screenshot shows the 'NetScaler Gateway Configuration' page. The 'NetScaler Gateway Settings' section is now a table with the following data:

Virtual Server Name	IP Address	Port
XenMobileGateway	10.147.75.54	443

Below this is the 'Server Certificate for NetScaler Gateway' section. It contains a text block explaining server certificates. There are two radio buttons: 'Use existing certificate' (which is selected) and 'Install Certificate'. Under 'Use existing certificate', there is a dropdown menu for 'Server Certificate*' with the value 'wildcert-wg-lab.pfx_CERT_KEY'. At the bottom are 'Continue' and 'Do It Later' buttons.

6. 인증서세부정보를입력하고 **Continue(계속)** 를클릭합니다.

Authentication Settings

Select a primary authentication method for client connections. Primary authentication can be configured to use Active Directory/LDAP, RADIUS, or client certificate methods. For two-factor authentication, configure a secondary method from either RADIUS or Active Directory/LDAP methods.

Primary authentication method*
Active Directory/LDAP

IP Address*
10 . 147 . 75 . 240 IPv6

Port*
389

Base DN*
dc=wg,dc=lab

Service account*
administrator@wg.lab

Password*

Confirm Password*

Time out (seconds)*
3

Server Logon Name Attribute*
userPrincipalName

Secondary authentication method*
None

참고:

Server Logon Name Attribute(서버로그온이름특성) 가 XenMobile LDAP 구성에서지정된것과동일해야 합니다.

7. XenMobile settings(XenMobile 설정) 아래에서 Load Balancing FQDN for MAM(MAM 의 FQDN 부하분산) 을입력하고 **Continue(계속)** 를클릭합니다.

XenMobile Settings

Load Balancing FQDN for MAM*
xm51.wg.lab

Load Balancing IP address for MAM*
10 . 147 . 75 . 55

Port*
8443

SSL Traffic Configuration*
 HTTPS communication to XenMobile Server HTTP communication to XenMobile Server

Split DNS mode for Micro VPN*
BOTH

Enable split tunneling

참고:

MAM 부하분산가상 IP 주소의 FQDN 과 XenMobile 의 FQDN 이동일해야합니다.

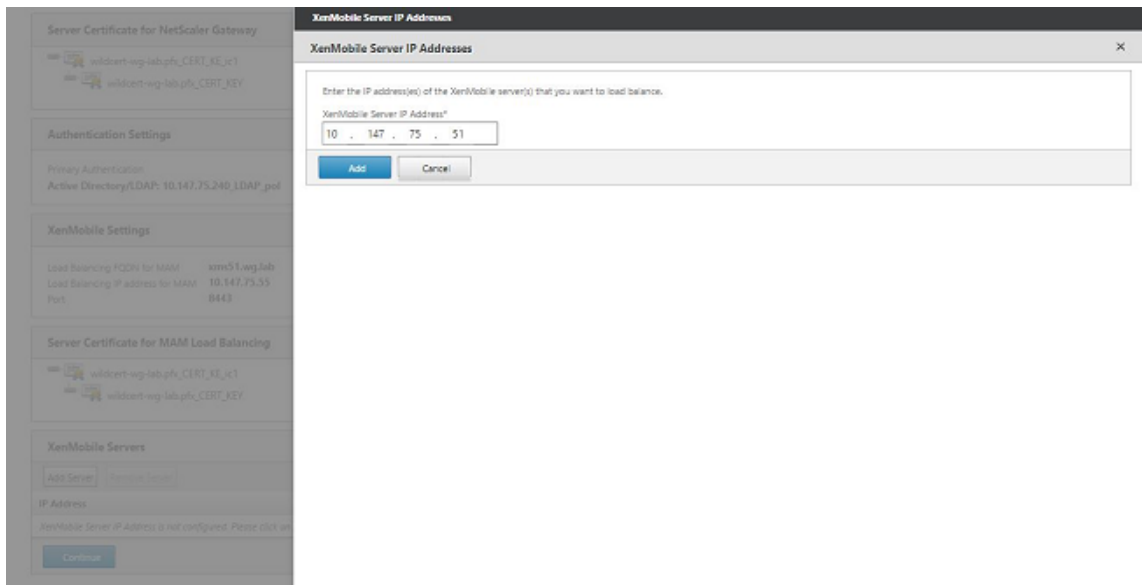
8. SSL 브리지모드 (HTTPS) 를사용하려는경우 **HTTPS communication to XenMobile Server(XenMobile 서버에대한 HTTPS 통신)** 를선택합니다. 그러나 SSL 오프로드를사용하려는경우앞의그림에나온것처럼 **HTTP communication to XenMobile Server(XenMobile Server 에대한 HTTP 통신)** 를선택합니다. 이 문서에 서는 SSL 브리지모드 (HTTPS) 를선택했습니다.
9. MAM 부하분산가상 IP 주소에대한서버인증서를바인딩하고 Continue(계속) 를클릭합니다.



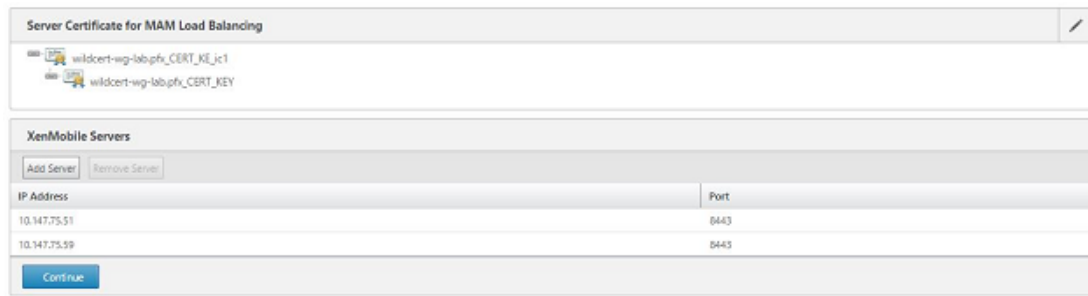
10. XenMobile Servers 아래에서 **Add Server**(서버추가) 를클릭하고 XenMobile 노드를추가합니다.



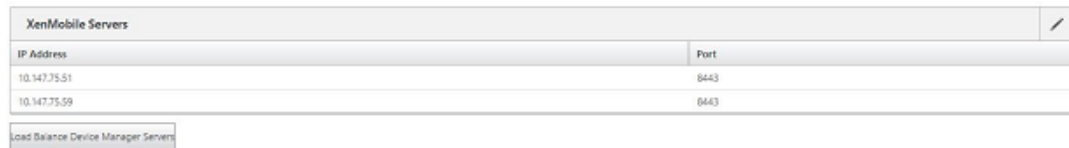
11. XenMobile 노드의 IP 주소를입력하고 Add(추가) 를클릭합니다.



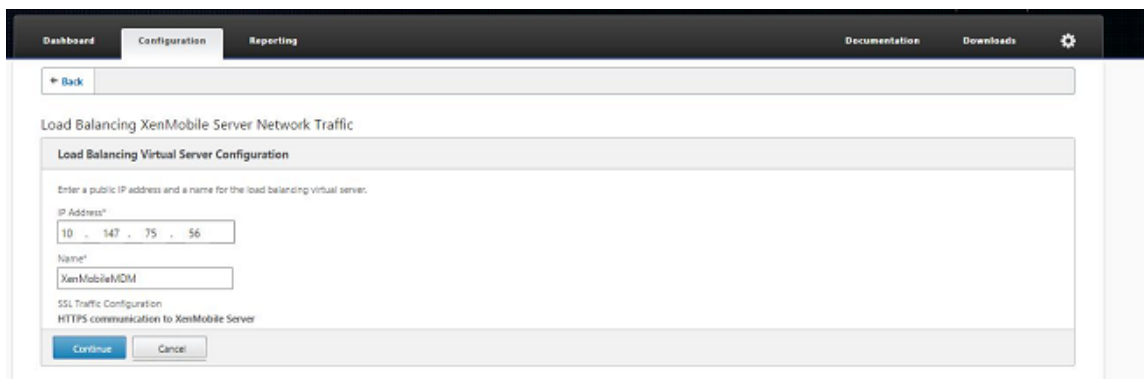
12. 10-11 단계를반복하여 XenMobile 클러스터의일부인 XenMobile 노드를추가합니다. 추가한모든 XenMobile 노드 가표시됩니다. Continue(계속) 를클릭합니다.



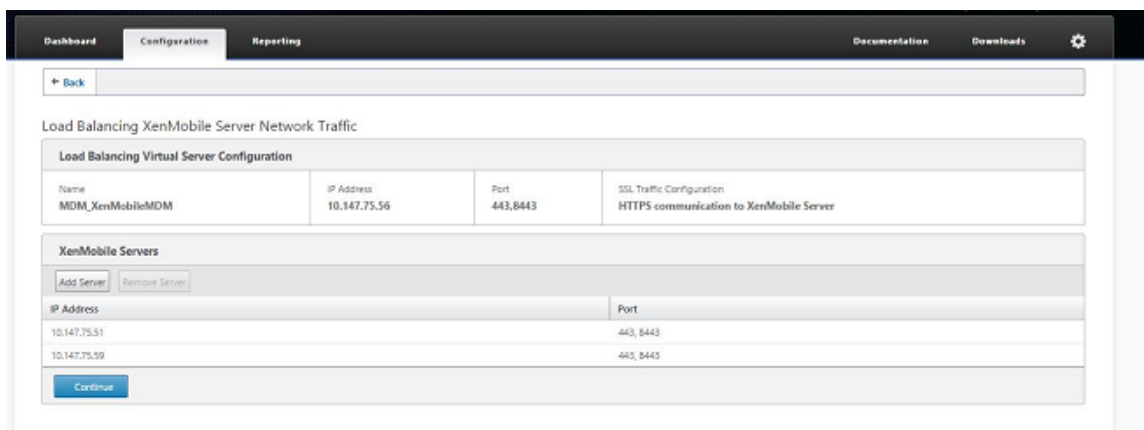
13. **Load Balance Device Manager Servers**(부하분산장치관리자서버) 를 클릭하여 MDM 부하분산구성을계속합니다.



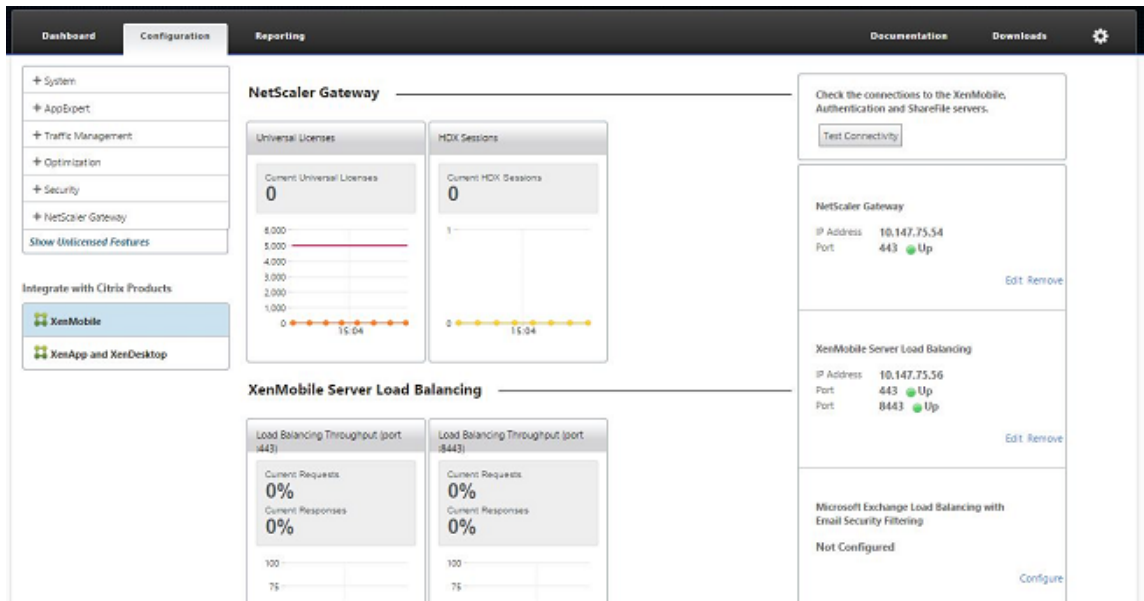
14. MDM 부하분산 IP 주소에사용할 IP 주소를입력하고 **Continue(계속)** 를 클릭합니다.



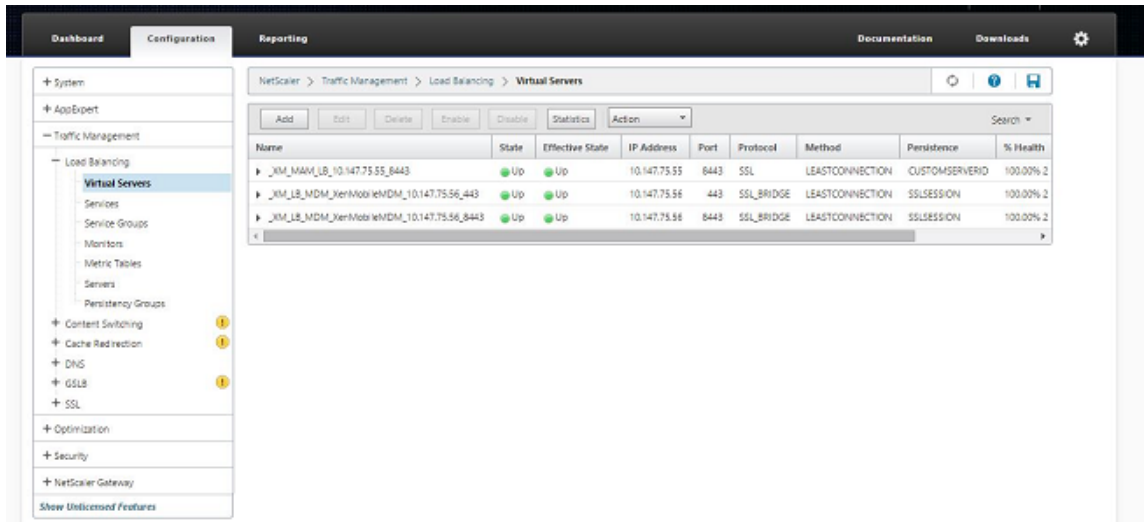
15. XenMobile 노드가목록에표시되면 **Continue(계속)** 를 누른다음 **Done(완료)** 을 클릭하여프로세스를마칩니다.



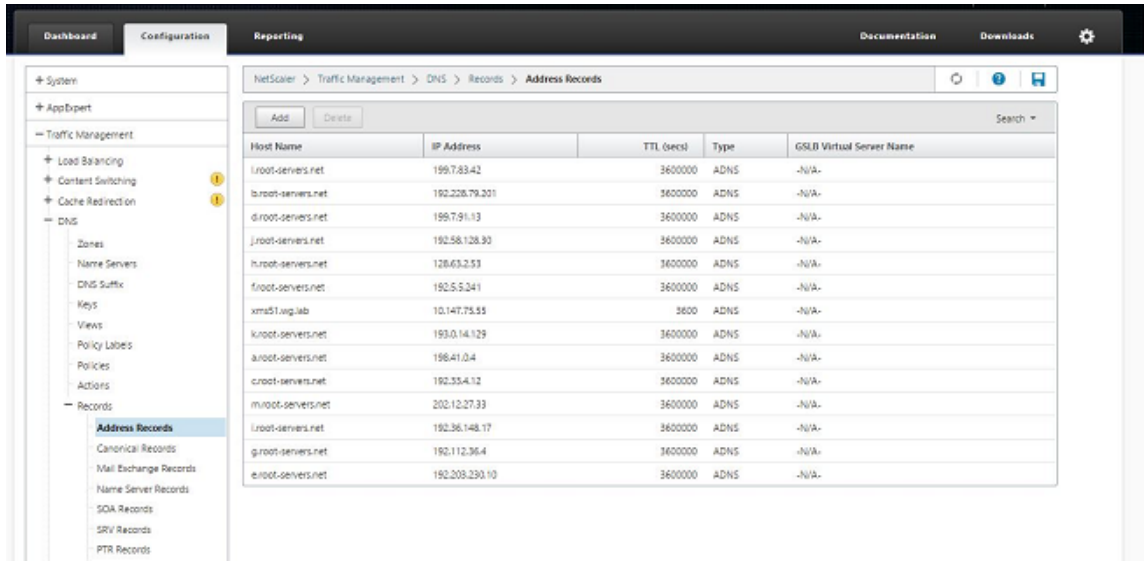
XenMobile 페이지에가상 IP 주소상태가표시됩니다.



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



NetScaler 의 DNS 항목이 MAM 부하분산가상 IP 주소를 가리키는 것을 볼 수 있습니다.



재해복구가이드

August 24, 2018

재해복구를위해활성/수동장애조치 (failover) 전략을사용하여여러사이트가포함된 XenMobile 배포를설계하고구성할수있습니다. 자세한내용은 XenMobile 배포안내서 [재해복구](#) 문서를참조하십시오.

프록시서버사용

January 6, 2020

아웃바운드인터넷트래픽을제어하려면 XenMobile 에서해당트래픽을처리할프록시서버를설정하면됩니다. 프록시서버는 CLI(명령줄인터페이스) 를통해설정합니다. 프록시서버를설정하려면시스템을다시시작해야합니다.

1. XenMobile CLI 메인메뉴에서 **2** 를입력하여시스템메뉴를선택합니다.
2. 시스템메뉴에서 **6** 을입력하여프록시서버메뉴를선택합니다.

```

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

3. 프록시구성메뉴에서 **1** 을입력하여 SOCKS 를선택합니다.

이설정을저장하기전에 HTTPS 도구성해야합니다. 동일한구성에서 SOCKS 및 HTTPS 설정을저장하지않으면프록시가작동하지않습니다.

```

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

4. 프록시서버 IP 주소, 포트번호및대상을입력합니다. 각프록시서버유형에대해지원되는대상유형은다음표를참조하십시오.

프록시유형	지원되는대상
SOCKS	APNS
HTTP	APNS, 웹, PKI
HTTPS	웹, PKI

인증을사용하는 HTTP	웹, PKI
인증을사용하는 HTTPS	웹, PKI

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

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

5. **n** 을입력하고 **2** 를입력하여 HTTPS 를선택한다음프록시서버 IP 주소, 포트번호및대상을입력합니다.
6. 프록시서버인증에사용할사용자이름과암호를구성하도록선택하는경우 **y** 를입력한후사용자이름과암호를입력합니다.

```

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

Enter https proxy information

Address []: 203.0.113.23

Port[]: 4443

Configure username & password [y/n]: y
Username: Justaname
Password:

Target - WEB
WEB proxy configured. Override proxy settings?[y/n]: █

```

7. **y** 를 입력하여 설정을 저장합니다.

SQL Server 구성

May 21, 2019

온-프레미스 XenMobile Server 에서 SQL Server 에 연결할 때 기본 드라이버인 jTDS 또는 Microsoft JDBC (Java Database Connectivity) 드라이버를 사용할 수 있습니다. 다음의 경우 jTDS 드라이버가 기본 드라이버입니다.

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

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

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

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

Microsoft JDBC 로 전환 (SQL Server 인증)

이러한 단계를 완료하려면 SQL Server 사용자 이름과 암호가 필요합니다.

1. 모든 XenMobile Server 노드에 SSH 로연결합니다.
2. XenMobile CLI 메인메뉴에서 **2** 를 입력하여 시스템메뉴를 선택합니다.
3. **12** 를 입력하여 고급설정을 선택합니다.
4. **7** 을 입력하여 JDBC 드라이버 전환을 선택한 후 **m** 을 입력하여 Microsoft 를 선택합니다.

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

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

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
[7] Switch JDBC driver
-----
Choice: [0 - 7] 7
JDBC driver type (JTDS or Microsoft) [1]:
```

5. 메시지가 표시되면 **y** 를 입력하여 SQL 인증을 선택하고 SQL Server 사용자 이름과 암호를 입력합니다.
6. 각 XenMobile Server 노드에 대해 단계를 반복합니다.
7. 각 XenMobile Server 노드를 다시 시작합니다.

Microsoft JDBC 로 전환 (SSL 꺼짐, Windows 인증)

이러한 단계를 완료하려면 Active Directory 사용자 이름 및 암호 Kerberos KDC 영역 및 KDC 사용자 이름이 필요합니다.

1. 모든 XenMobile Server 노드에 SSH 로 연결합니다.
2. XenMobile CLI 메인메뉴에서 **2** 를 입력하여 시스템메뉴를 선택합니다.
3. **12** 를 입력하여 고급설정을 선택합니다.
4. **7** 을 입력하여 JDBC 드라이버 전환을 선택한 후 **m** 을 입력합니다.
5. SQL Server 인증의 사용 여부를 묻는 메시지가 표시되면 **n** 을 입력합니다.
6. 메시지가 표시되면 SQL Server 에 구성된 Active Directory 사용자 이름과 암호를 입력합니다.

7. XenMobile 에서 Kerberos KDC 영역이자동으로검색되지않으면 SQL Server FQDN 을비롯한 KDC 세부정보를 묻는메시지가표시됩니다.
8. SSL 사용여부를묻는메시지가표시되면 **n** 을입력합니다. XenMobile 구성 XenMobile 에서오류로인해구성이저장되지않으면오류메시지와입력한세부정보가표시됩니다.
9. 각 XenMobile Server 노드에대해단계를반복합니다.
10. 각 XenMobile Server 노드를다시시작합니다.

XenMobile 데이터베이스암호를변경하려면

다음지침에따라 XenMobile 데이터베이스암호를변경합니다. 예를들어 Citrix 지원에서암호변경을요청하는경우암호를변경해야합니다.

중요:

- 데이터베이스암호변경을위해예약된유지관리기간을계획합니다. 암호는시스템중단시간에변경해야합니다.
- 암호를변경할때는모든 XenMobile 노드가네트워크에연결되어있는지확인하십시오. 암호를변경한후 XenMobile 을다시시작합니다.

암호를변경한후 XenMobile 을다시시작하지않으면 XenMobile 이복구모드로전환됩니다. 그러면 SQL Server 에서이전암호로되돌린후 XenMobile 을다시시작하고암호를다시변경해야합니다.

- SQL Server 에서 Windows 인증을사용하는경우 Windows Active Directory 에서데이터베이스암호를변경해야합니다.

1. 모든 XenMobile Server 노드가실행중인지확인합니다. 클러스터링된환경의경우모든노드를가동합니다.
2. Netscaler 부하분산장치에서 vServer 를사용하지않도록설정하여 XenMobile 에대한수신장치트래픽을차단합니다.
3. SQL Server 에서데이터베이스암호를변경하려면: XenMobile CLI 에로그인하고 **Configuration > Database** 로이동한다음메시지가표시되면변경된암호를입력합니다.

```
1 Server []: <ipAddress>
2 Port [1433]: 1433
3 Username [sa]: <userName>
4 Password: <****>
```

4. **Y** 를입력하여서버를다시시작합니다.
5. 클러스터의다른모든노드에대해 3 단계와 4 단계를반복합니다.
6. NetScaler 부하분산장치에서 vServer 를사용하도록설정하여수신장치트래픽의차단을해제합니다.

서버속성

January 6, 2020

XenMobile 에는 서버전체작업에 적용되는 다수의 속성이 있습니다. 이 문서에서는 여러 서버속성을 설명하고 서버속성을 추가, 편집 또는 삭제하는 방법을 자세히 설명합니다.

일부 속성은 사용자 지정 키입니다. 사용자 지정 키를 추가하려면 추가를 클릭한 다음 키에서 사용자 지정 키를 선택합니다.

일반적으로 구성되는 속성에 대한 자세한 내용은 XenMobile 가상 안내서에서 [서버속성](#)을 참조하십시오.

서버속성 정의

Add Device Always(항상 장치 추가)

- **true** 인 경우 XenMobile 이 등록에 실패한 장치도 XenMobile 콘솔에 추가합니다. 따라서 등록을 시도한 장치를 볼 수 있습니다. 기본값은 **false** 입니다.

AG Client Cert Issuing Throttling Interval(AG 클라이언트 인증서 발급 제한 간격)

- 인증서 생성 사이의 여유 기간입니다. 이 간격은 XenMobile 이 짧은 기간에 장치용 인증서를 여러 개 생성하는 것을 방지합니다. 이 값은 변경하지 않는 것이 좋습니다. 기본값은 **30** 분입니다.

Audit Log Cleanup Execution Time(감사 로그 정리 실행 시간)

- 감사 로그 정리를 시작하는 시간이며 HH:MM AM/PM 형식을 사용합니다. 예: 04:00 AM. 기본값은 **02:00 AM** 입니다.

Audit Log Cleanup Interval (in Days)(감사 로그 정리 간격 (일))

- XenMobile 에 감사 로그가 유지되는 일수입니다. 기본값은 **1** 입니다.

Audit Logger(감사 로거)

- **False** 인 경우 UI(사용자 인터페이스) 이벤트를 기록하지 않습니다. 기본값은 **False** 입니다.

Audit Log Retention (in Days)(감사 로그 유지 (일))

- XenMobile 에 감사 로그가 유지되는 일수입니다. 기본값은 **7** 입니다.

auth.ldap.connect.timeout and auth.ldap.read.timeout

- 느린 LDAP 응답을 보완하려면 다음 사용자 지정 키의 서버 속성을 추가하는 것이 좋습니다.
 - 키: 사용자 지정 키
 - 키: **auth.ldap.connect.timeout**
 - 값: **60000**
 - 표시 이름: **auth.ldap.connect.timeout**
 - 설명: **LDAP** 연결 시간 초과
 - 키: 사용자 지정 키
 - 키: **auth.ldap.read.timeout**
 - 값: **60000**
 - 표시 이름: **auth.ldap.read.timeout**
 - 설명: **LDAP** 읽기 시간 제한

인증서 갱신 (초)

- XenMobile 이인증서 갱신을 시작하는 인증서가 만료되기 전의 시간 (초)입니다. 예를 들어 인증서가 12 월 30 일에 만료될 예정이고 이 속성이 30 일로 설정된 경우 장치가 12 월 1 일에서 12 월 30 일 사이에 연결하면 XenMobile 이인증서 갱신을 시작합니다. 기본값은 **2592000** 초 (30 일)입니다.

연결 시간 제한

- XenMobile 이 장치에 대한 TCP 연결을 종료하기 전까지의 세션 비활성 시간 제한 (분)입니다. 세션은 열린 상태로 유지됩니다. Android 및 Windows CE 장치와 원격 지원에 적용됩니다. 기본값은 **5** 분입니다.

Connection Timeout to Microsoft Certification Server(Microsoft 인증서 서버에 대한 연결 시간 제한)

- XenMobile 이인증서 서버의 응답을 대기하는 시간 (초)입니다. 인증서 서버가 느리고 트래픽이 많은 경우 이 값을 60 초 이상으로 늘립니다. 120 초 후에 응답하지 않는 인증서 서버는 유지 관리가 필요합니다. 기본값은 **15000** 밀리초 (15 초)입니다.

기본 배포 채널

- XenMobile 이리소스를 장치에 배포하는 방법을 사용자 수준 (**DEFAULT_TO_USER**) 또는 장치 수준에서 결정합니다. 기본값은 **DEFAULT_TO_DEVICE**입니다.

Deploy Log Cleanup (in Days)(배포로그정리 (일))

- XenMobile 에배포로그가유지되는일수입니다. 기본값은 **7** 입니다.

Disable Hostname Verification(호스트이름유효성검사비활성화)

- 기본적으로호스트이름유효성검사는 Microsoft PKI 서버를제외한발신연결에대해활성화됩니다. 호스트이름유효성검사가실패하면서버로그에다음과같은오류가포함됩니다. “Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer(VPP 서버에연결할수없습니다. 호스트이름 ‘192.0.2.0’ 은피어가제공한인증서주체와일치하지않습니다.)” 호스트이름유효성검사로인해배포가중단되는경우이속성을 **true** 로변경하십시오. 기본값은 **false** 입니다.

SSL 서버확인사용안함

- **True** 인경우다음모든조건이충족되면 SSL 서버인증서유효성검사가사용되지않습니다.
 - XenMobile Server 에서인증서기반인증을사용합니다.
 - Microsoft CA 서버가인증서발급자입니다.
 - XenMobile Server 가루트를신뢰하지않는내부 CA 에서인증서를서명했습니다.

기본값은 **true** 입니다.

Enable Console(콘솔사용)

- **true** 인경우사용자가자가지원포털콘솔에액세스할수있습니다. 기본값은 **true** 입니다.

Enable Crash Reporting(크래시보고사용)

- **true** 인경우 Citrix 는 iOS 및 Android 용 Secure Hub 의문제를해결하는데도움이되는충돌보고서및진단을수집합니다. **false** 인경우데이터가수집되지않습니다. 기본값은 **true** 입니다.

Enable/Disable Hibernate statistics logging for diagnostics(진단에 Hibernate 통계로깅사용/사용안함)

- **True** 인경우 Hibernate 통계로깅을사용하여응용프로그램성능문제해결을지원합니다. Hibernate 는 XenMobile 에서 Microsoft SQL Server 에연결할때사용되는구성요소입니다. 기본적으로로깅은응용프로그램성능에영향을미치므로사용하지않도록설정됩니다. 매우큰로그파일이만들어지는것을방지하려면짧은기간동안만로깅을사용하십시오. XenMobile 은 /opt/sas/logs/hibernate_stats.log 에로그를기록합니다. 기본값은 **False** 입니다.

Enable macOS OTAЕ(macOS OTAЕ 사용)

- **false** 인 경우 macOS 장치에 대한 등록 링크의 사용을 차단합니다. 즉, macOS 사용자는 등록 초대를 통해서만 등록할 수 있습니다. 기본값은 **true** 입니다.

Enable Notification Trigger(알림 트리거 사용)

- Secure Hub 클라이언트 알림을 사용하거나 사용하지 않도록 설정합니다. **true** 값은 알림을 사용합니다. 기본값은 **true** 입니다.

force.server.push.required.apps

- 다음과 같은 경우에 Android 및 iOS 장치에서 필수 앱의 강제 배포를 사용하도록 설정합니다.
 - 사용자가 새 앱을 업로드하고 필수 앱으로 표시합니다.
 - 사용자가 기존 앱을 필수 앱으로 표시합니다.
 - 사용자가 필수 앱을 삭제합니다.
 - Secure Hub 업데이트가 제공됩니다.

필수 앱의 강제 배포는 기본적으로 **false** 로 설정됩니다. 강제 배포를 사용하도록 설정하려면 사용자 지정 키를 만들고 값을 **true** 로 설정하십시오. 강제 배포 중에는 엔터프라이즈 앱 및 공용 앱 스토어 앱을 포함한 MDX 지원 필수 앱이 즉시 업그레이드됩니다. 관리자가 앱 업데이트 유예 기간에 대한 MDX 정책을 구성하고 사용자가 앱을 나중에 업그레이드하도록 선택하는 경우에도 업그레이드가 수행됩니다.

- 키: 사용자 지정 키
- 키: **force.server.push.required.apps**
- 값: **false**
- 표시 이름: **force.server.push.required.apps**
- 설명: 필수 앱을 강제로 배포

ActiveSync 가 허용 및 거부된 사용자 전체 목록 끌어들이기

- XenMobile 이 ActiveSync 가 허용 및 거부된 사용자의 전체 목록 (기준) 을 가져오는 간격 (초) 입니다. 기본값은 **28800** 초입니다.

hibernate.c3p0.idle_test_period

- XenMobile Server 속성인 사용자 지정 키는 연결 유효성이 자동으로 검사되기까지의 유휴 시간 (초) 을 결정합니다. 다음과 같이 키를 구성합니다. 기본값은 **30** 입니다.
- 키: 사용자 지정 키

- 키: **hibernate.c3p0.idle_test_period**
- 값: **30**
- 표시이름: **hibernate.c3p0.idle_test_period=nnn**
- 설명: **Hibernate** 유틸테스트기간

hibernate.c3p0.max_size

- 이사용자지정키는 XenMobile 에서 SQL Server 데이터베이스에대해열수있는최대연결수를결정합니다. XenMobile 은이사용자지정키에지정한값을상한으로사용합니다. 필요한경우에만연결이열립니다. 데이터베이스서버의용량에 따라설정을결정합니다. 자세한내용은 [XenMobile 작업조정](#)에서참조하십시오. 다음과같이키를구성합니다. 기본값은 **1000** 입니다.
- 키: **hibernate.c3p0.max_size**
- 값: **1000**
- 표시이름: **hibernate.c3p0.max_size**
- 설명: **SQL** 에대한 **DB** 연결

hibernate.c3p0.min_size

- 이사용자지정키는 XenMobile 에서 SQL Server 데이터베이스에대해여는최소연결수를결정합니다. 다음과같이키를 구성합니다. 기본값은 **100** 입니다.
- 키: **hibernate.c3p0.min_size**
- 값: **100**
- 표시이름: **hibernate.c3p0.min_size**
- 설명: **SQL** 에대한 **DB** 연결

hibernate.c3p0.timeout

- 이사용자지정키는유틸시간초과 (초) 를결정합니다. 기본값은 **120** 입니다.
- 키: 사용자지정키
- 키: **hibernate.c3p0.timeout**
- 값: **120**
- 표시이름: **hibernate.c3p0.timeout**
- 설명: 데이터베이스유틸시간초과

원격분석의사용여부를식별합니다

- 원격분석 (사용자환경개선프로그램또는 CEIP) 이사용되는지여부를식별합니다. XenMobile 을설치하거나업그레이드 할때 CEIP 에참여할수있습니다. XenMobile 서 15 번연속으로업로드에실패할경우원격분석이사용되지않습니다. 기본값은 **false** 입니다.

Inactivity Timeout in Minutes(비활성시간제한 (분))

- 웹서비스시간제한유형서버속성이 **INACTIVITY_TIMEOUT** 인경우: 이속성은 XenMobile 이다음을수행한비활성관리자로그아웃하기전까지의시간 (분) 을정의합니다.
 - REST 서비스에대한 XenMobile 공용 API 를사용한 XenMobile 콘솔액세스
 - REST 서비스에대한 XenMobile 공용 API 를사용하여타사앱에액세스. 시간제한이 **0** 인경우비활성사용자로그인한상태로유지됩니다.

기본값은 **5** 입니다.

iOS Device Management Enrollment Auto-Install Enabled(iOS 장치관리등록자동설치사용)

- true 인경우이속성은장치등록시필요한사용자상호작용의수를줄입니다. 사용자는 **Root CA install(루트 CA 설치)(필요한경우)** 및 **MDM Profile install(MDM 프로파일설치)** 을클릭해야합니다.

iOS Device Management Enrollment First Step Delayed(iOS 장치관리등록의첫번째단계지연)

- 장치등록시사용자가자격증명을입력한후루트 CA 에대한메시지에응답하기까지대기해야하는시간을지정합니다. 이속성은네트워크대기시간또는속도문제가있는경우에만편집하는것이 좋습니다. 이경우 5000 밀리초 (5 초) 를초과하는값을설정하지마십시오. 기본값은 **1000** 밀리초 (1 초) 입니다.

iOS Device Management Enrollment First Step Delayed(iOS 장치관리등록의마지막단계지연)

- 이속성값은장치등록중에 MDM 프로파일설치된후장치의에이전트가시작되기까지대기해야하는시간을지정합니다. 이속성은네트워크대기시간또는속도문제가있는경우에만편집하는것이 좋습니다. 이경우 5000 밀리초 (5 초) 를초과하는값을설정하지마십시오. 기본값은 **1000** 밀리초 (1 초) 입니다.

iOS Device Management Identity Delivery Mode(iOS 장치관리 ID 배달모드)

- XenMobile 이장치에 MDM 인증서를배포할때 **SCEP**(보안상의이유로권장됨) 또는 **PKCS12** 를사용할지여부를지정합니다. PKCS12 모드에서는서버에키쌍이생성되고협상이수행되지않습니다. 기본값은 **SCEP** 입니다.

iOS Device Management Identity Key Size(iOS 장치관리 ID 키크기)

- MDM ID, iOS 프로필서비스 및 XenMobile iOS 에이전트 ID 에대한 개인키의 크기를 정의합니다. 기본값은 **1024** 입니다.

iOS Device Management Identity Renewal Days(iOS 장치관리 ID 갱신일수)

- XenMobile 이인증서 갱신을 시작하는 인증서가 만료되기 전의 시간 (일) 을 지정합니다. 예를 들어 인증서가 10 일 후에 만료 되고 이 속성이 **10** 일인 경우 장치가 만료 9 일 전에 연결하면 XenMobile 이 새 인증서를 발급합니다. 기본값은 **30** 일입니다.

iOS MDM APNS Private Key Password(iOS MDM APNS 개인키 암호)

- 이 속성에는 XenMobile 에서 Apple 서버로 알림을 푸시할 때 필요한 APNs 암호가 포함됩니다.

Length of Inactivity Before Device Is Disconnected(장치 연결을 해제하기 전 비활성화 시간)

- XenMobile 이 연결을 해제하기 전에 장치가 마지막 인증부터 비활성화 상태로 있을 수 있는 시간을 지정합니다. 기본값은 **7** 일입니다.

MAM Only Device Max

- 이 사용자 지정 키는 각 사용자가 등록할 수 있는 MAM 전용 장치의 수를 제한합니다. 다음과 같이 키를 구성합니다. 값이 **0** 이면 장치를 무제한 등록할 수 있습니다.
- 키 = **number.of.mam.devices.per.user**
- 값 = **5**
- 표시 이름 = **MAM Only Device Max**
- 설명 = 각 사용자가 등록할 수 있는 **MAM** 장치 수를 제한합니다.

MaxNumberOfWorker

- 많은 수의 VPP 라이선스를 가져올 때 사용되는 스레드 수입니다. 기본값은 **3** 입니다. 추가 최적화가 필요한 경우 스레드 수를 늘릴 수 있습니다. 그러나 예를 들어 6 과 같이 스레드 수가 커지면 VPP 를 가져올 때 CPU 사용량이 매우 높아집니다.

NetScaler Single Sign-On

- **False** 인 경우 NetScaler 에서 XenMobile 로의 SSO 중에 XenMobile 콜백 기능이 사용되지 않습니다. NetScaler Gateway 구성에 콜백 URL 이 포함되는 경우 XenMobile 이 콜백 기능을 사용하여 NetScaler Gateway 세션 ID 를 확인합니다. 기본값은 **False** 입니다.

Number of consecutive failed uploads(연속 업로드 실패 수)

- CEIP(사용자 환경 개선 프로그램) 업로드 중에 연속적으로 실패한 횟수를 표시합니다. 업로드가 실패하면 값이 증가합니다. 업로드가 15 회 실패하면 XenMobile 이 원격 분석이라고도 하는 CEIP 를 사용하지 않도록 설정합니다. 자세한 내용은 원격 분석의 사용 여부를 식별합니다 서버 속성을 참조하십시오. 업로드가 성공하면 값이 **0** 으로 재설정됩니다.

Number of Users Per Device(장치당 사용자 수)

- 동일한 장치를 MDM 에 등록할 수 있는 사용자의 최대 수입니다. **0** 값은 무제한의 사용자가 동일한 장치를 등록할 수 있음을 의미합니다. 기본값은 **0** 입니다.

Pull of Incremental Change of Allowed and Denied Users(허용 및 거부된 사용자의 증분 변경 끌어오기)

- XenMobile 이 PowerShell 명령을 실행하여 ActiveSync 장치의 델타를 가져올 때 도메인의 응답을 대기하는 시간 (초)입니다. 기본값은 **60** 초입니다.

Read Timeout to Microsoft Certification Server(Microsoft 인증 서버에 대한 읽기 시간 제한)

- XenMobile 이 읽기를 수행할 때 인증서 서버의 응답을 대기하는 시간 (초)입니다. 인증서 서버가 느리고 트래픽이 많은 경우 이 값을 60 초 이상으로 늘릴 수 있습니다. 120 초 후에 응답하지 않는 인증서 서버는 유지 관리가 필요합니다. 기본값은 **15000** 밀리초 (15 초)입니다.

REST Web Services(REST 웹 서비스)

- REST 웹 서비스를 사용합니다. 기본값은 **true** 입니다.

지정된 키의 청크로 장치 정보를 검색합니다

- 이 값은 장치 내보내기 중 내부적으로 다중 스레드 처리에 사용됩니다. 값이 클수록 단일 스레드가 더 많은 장치를 구문 분석합니다. 값이 작을수록 더 많은 스레드가 장치를 가져옵니다. 값을 줄이면 내보내기 및 장치 목록 가져오기 성능이 향상되지만 사용 가능한 메모리가 줄어들 수 있습니다. 기본값은 **1000** 입니다.

Session Log Cleanup (in Days)(세션로그정리 (일))

- XenMobile 에세션로그가유지되는일수입니다. 기본값은 **7** 입니다.

Server Mode(서버모드)

- XenMobile 이앱관리, 장치관리또는앱및장치관리에해당하는 MAM, MDM 또는 ENT(엔터프라이즈) 모드에서실행되는지확인합니다. Server Mode(서버모드) 속성은아래표에설명된것과같이장치등록방법에따라설정합니다. 서버모드의기본값은라이선스유형에관계없이 **ENT** 입니다.

XenMobile MDM Edition 라이선스가있는경우유효한서버모드는서버속성에서설정한서버모드와관계없이항상 MDM 입니다. MDM Edition 라이선스가있는경우서버모드를 MAM 또는 ENT 로설정하여앱관리를사용할수없습니다.

라이선스버전	장치등록에사용할모드	Server Mode(서버모드) 속성을다음으로설정
Enterprise/Advanced	MDM 모드	MDM
Enterprise/Advanced	MDM+MAM 모드	ENT
MDM	MDM 모드	MDM

유효한서버모드는라이선스유형과서버모드의조합입니다. MDM 라이선스에유효한서버모드는서버모드설정과관계없이항상 MDM 입니다. Enterprise 및 Advanced 라이선스의경우유효한서버모드는서버모드가 **ENT** 또는 **MDM** 인경우서버모드와 일치합니다. 서버모드가 **MAM** 인경우유효한서버모드는 ENT 입니다.

XenMobile 온라인라이선스활성화, 라이선스삭제및서버속성에서서버모드변경작업에대한서버로그에서서버모드를추가합니다. 로그파일만들기및보기에대한자세한내용은 [로그](#) 및 [XenMobile 의로그파일보기및분석](#)을참조하십시오.

ShareFile configuration type(ShareFile 구성유형)

- ShareFile 스토리지유형을지정합니다. **ENTERPRISE** 는 ShareFile Enterprise 모드를사용합니다. **CONNECTORS** 는 XenMobile 콘솔을통해만든 StorageZone 커넥터에대한액세스만제공합니다. 기본값은 **NONE** 이며 구성 > **ShareFile** 화면의초기보기에서 ShareFile Enterprise 와커넥터중에서선택할수있습니다. 기본값은 **NONE** 입니다.

Static Timeout in Minutes(정적시간제한 (분))

- 웹서비스시간제한유형서버속성이 **STATIC_TIMEOUT** 인경우: 이속성은 XenMobile 이다음을사용한후관리자들로 그아웃하기전의시간 (분) 을정의합니다.

- REST 서비스에대한 XenMobile 공용 API 를사용하여 XenMobile 콘솔에액세스
- REST 서비스에대한 XenMobile 공용 API 를사용하여타사앱에액세스.

기본값은 **60** 입니다.

Trigger Agent Message Suppression(에이전트메시지트리거억제)

- Secure Hub 클라이언트메시지를사용하거나사용하지않도록설정합니다. **false** 값은메시지를사용합니다. 기본값은 **true** 입니다.

Trigger Agent Sound Suppression(에이전트사운드트리거억제)

- Secure Hub 클라이언트사운드를사용하거나사용하지않도록설정합니다. **false** 값은사운드를사용합니다. 기본값은 **true** 입니다.

Unauthenticated App Download for Android Devices(Android 장치에대한인증되지않은앱다운로드)

- **True** 인경우자체호스팅된앱을 Android Enterprise 를실행하는 Android 장치에다운로드할수있습니다. 이속성은 Google Play Store 의다운로드 URL 을정적으로제공하는 Android Enterprise 옵션이사용되는경우필요합니다. 이경우다운로드 URL 에는인증토큰이있는일회용티켓 (**XAM One-Time Ticket server**(XAM 일회용티켓서버) 속성으로정의됨) 이포함될수없습니다. 기본값은 **False** 입니다.

Unauthenticated App Download for Windows Devices(Windows 장치에대한인증되지않은앱다운로드)

- 일회용티켓의유효성을검사하지않는이전버전의 Secure Hub 에만사용됩니다. **False** 인경우 XenMobile 에서인증되지않은앱을 Windows 장치에다운로드할수있습니다. 기본값은 **False** 입니다.

Use ActiveSync ID to Conduct an ActiveSync Wipe Device(ActiveSync ID 를사용하여 ActiveSync 장치 초기화수행)

- **true** 인경우 Exchange ActiveSync 용 Endpoint Management 커넥터가 ActiveSync 식별자를 asWipeDevice 메서드의인수로사용합니다. 기본값은 **false** 입니다.

사용자정의장치속성 **N**

- Windows CE 장치에만사용됩니다. 이사용자지정키를사용하면 Windows CE 장치의레지스트리에서만드는속성을가져올수있습니다. 해당속성이 XenMobile 데이터베이스에추가되면속성의값에기반하여배포규칙을만들수있습니다.
- 키: 사용자지정키

- 키: **device.properties.userDefinedN**
- 값: 관리자가정의
- 표시이름: 관리자가정의
- 설명: 관리자가정의

Exchange 의사용자만

- **true** 인경우 ActiveSync Exchange 사용자에게사용자인증을사용하지않습니다. 기본값은 **false** 입니다.

VPP baseline interval(VPP 기준간격)

- XenMobile 이 Apple 에서 VPP 라이선스를다시 가져오는최소간격입니다. 라이선스정보를새로고치면 VPP 에서가져온앱을수동으로삭제하는것과같은모든변경내용을 XenMobile 에반영할수있습니다. 기본적으로 XenMobile 은 VPP 라이선스기준을최소 **720** 분마다새로고칩니다.

설치된 VPP 라이선스가많은경우 (예: 50,000 개초과) 기준간격을늘려라이선스가져오기의빈도및오버헤드를줄이는것이 좋습니다. Apple 에서 VPP 라이선스가 자주변경될것으로예상되는경우값을낮춰 XenMobile 에변경내용이업데이트되도록하는것이 좋습니다. 두기준사이의최소간격은 60 분입니다. 또한 XenMobile 은 60 분마다델타가져오기를수행하여마지막가져오기 이후의변경내용을캡처합니다. 그러므로 VPP 기준간격이 60 분인경우기준사이의간격이최대 119 분까지지연될수있습니다.

웹서비스시간제한유형

- 공용 API 에서검색되는인증토큰의만료방법을지정합니다. **STATIC_TIMEOUT** 인경우 정적시간제한 (분) 서버속성에 지정된값이지나면인증토큰이만료된것으로간주합니다.

INACTIVITY_TIMEOUT 인경우 비활성시간제한 (분) 서버속성에지정된값동안비활성상태이면인증토큰이만료된것으로간주합니다. 기본값은 **STATIC_TIMEOUT** 입니다.

Windows Phone MDM Certificate Extended Validity (5y)(Windows Phone MDM 인증서연장유효성 (5년))

- Windows Phone 및태블릿용 MDM 에서발급된장치인증서의유효기간입니다. 장치관리중에장치는장치인증서를사용하여 MDM 서버에인증합니다. **true** 인경우유효기간은 5 년입니다. **false** 인경우유효기간은 2 년입니다. 기본값은 **true** 입니다.

Windows WNS 채널 - 갱신전일수

- ChannelURI 의갱신빈도입니다. 기본값은 **10** 일입니다.

Windows WNS 하트비트간격

- XenMobile 이 3 분마다 5 번장치에연결한후장치에연결하기전까지 기다릴 시간입니다. 기본값은 **6** 시간입니다.

XAM 일회용티켓

- OTT(일회용인증토큰) 로 앱을 다운로드할 수 있는 시간 (밀리초) 입니다. 이 속성은 **Android** 장치의 인증되지 않은 앱 다운로드 및 **Windows** 장치의 인증되지 않은 앱 다운로드 속성과 함께 사용됩니다. 이러한 속성은 인증되지 않은 앱 다운로드를 허용할지 여부를 지정합니다. 기본값은 **3600000** 입니다.

XenMobile MDM Self Help Portal console max inactive interval (minutes)(XenMobile MDM 자가지원포털콘솔최대비활성간격 (분))

- XenMobile 자가지원포털에서 비활성 사용자가 로그아웃되기까지의 시간 (분) 입니다. 시간제한이 **0** 인 경우 비활성 사용자 로그아웃 상태로 유지됩니다. 기본값은 **30** 입니다.

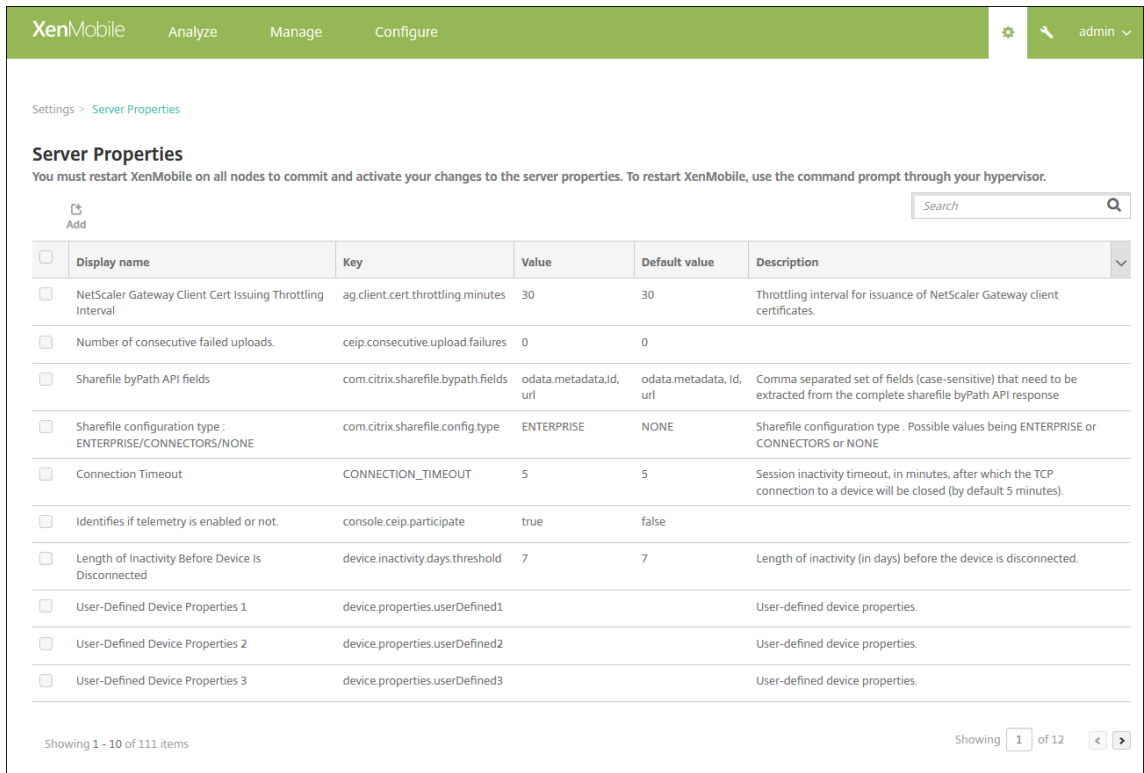
서버속성추가, 편집또는삭제

XenMobile 에서 서버에 속성을 적용할 수 있습니다. 변경한 후에는 모든 노드에서 XenMobile 을 다시 시작하여 변경 내용을 커밋하고 활성화해야 합니다.

참고:

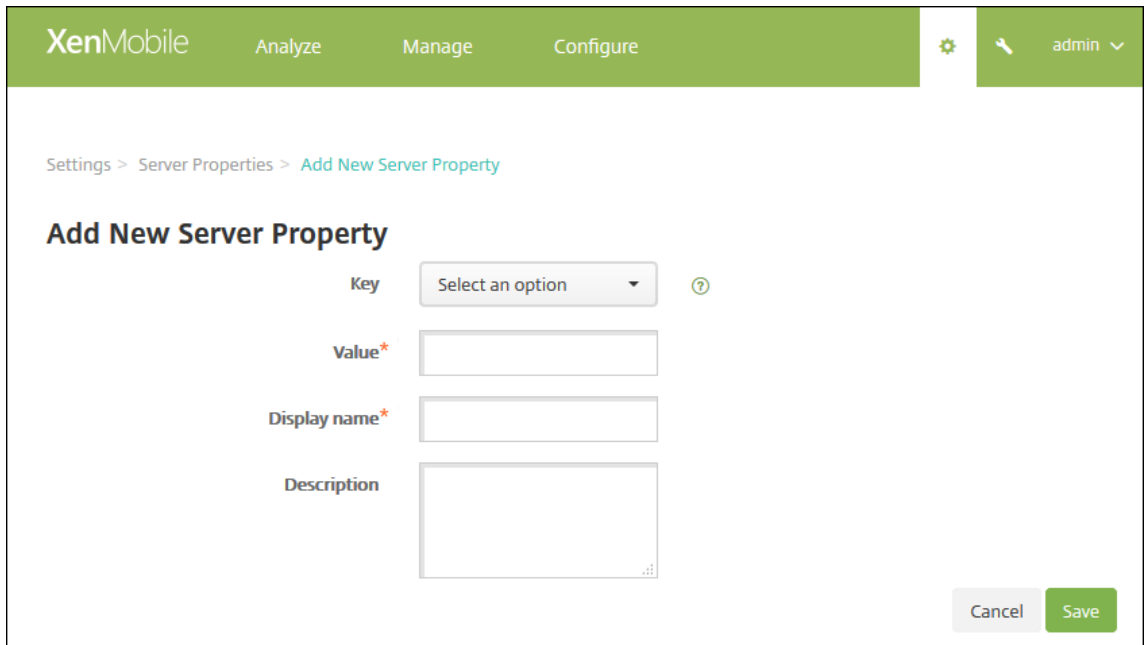
XenMobile 을 다시 시작하려면 하이퍼바이저를 통해 명령 프롬프트를 사용합니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버 아래에서 서버 속성을 클릭합니다. 서버 속성 페이지가 나타납니다. 이 페이지에서 서버 속성을 추가, 편집 또는 삭제할 수 있습니다.



서버속성을추가하려면

1. 추가를클릭합니다. 새서버속성추가페이지가나타납니다.



2. 다음설정을구성합니다.

- 키: 목록에서해당하는키를선택합니다. 키는대/소문자를구분합니다. 속성값을편집하기전또는특수키를요청하려는경우 Citrix 지원에문의하십시오.
- 값: 선택한키에따른값을입력합니다.
- 표시이름: 서버속성테이블에표시되는새속성값의이름을입력합니다.
- 설명: 필요한경우새서버속성의설명을입력합니다.

3. 저장을클릭합니다.

서버속성을편집하려면

1. 서버속성테이블에서편집할서버속성을선택합니다.

서버속성옆의확인란을선택하면서버속성목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하여목록오른쪽의옵션메뉴를열립니다.

2. 편집을클릭합니다. 새서버속성편집페이지가나타납니다.

The screenshot shows the 'Edit New Server Property' interface in the XenMobile console. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs, along with a settings icon and a user profile 'admin'. The breadcrumb trail is 'Settings > Server Properties > Edit New Server Property'. The main form area contains the following fields:

- Key:** ag.client.cert.throttling.mi
- Value*:** 30
- Display name*:** NetScaler Gateway Client
- Description:** Throttling interval for issuance of NetScaler Gateway client certificates.

At the bottom right of the form, there are 'Cancel' and 'Save' buttons.

3. 다음정보를적절하게변경합니다.

- 키: 이필드는변경할수없습니다.
- 값: 속성값입니다.
- 표시이름: 속성이름입니다.
- 설명: 속성설명입니다.

4. 저장을클릭하여변경내용을저장하거나 취소를클릭하여속성을변경하지않고그대로유지합니다.

서버속성을삭제하려면

1. 서버속성테이블에서삭제할서버속성을선택합니다.
각속성옆에있는확인란을선택하여삭제할속성을돌이상선택할수있습니다.
2. 삭제를클릭합니다. 확인대화상자가나타납니다. 삭제를다시클릭합니다.

CLI(명령줄인터페이스) 옵션

May 21, 2019

XenMobile Server 온-프레미스설치의경우다음과같은방법으로 CLI 옵션에액세스할수있습니다.

- **XenMobile** 이설치된하이퍼바이저사용: 하이퍼바이저에서, 가져온 XenMobile 가상컴퓨터를선택하고명령프롬프트 보기를시작한후 XenMobile 의관리자계정으로그은합니다. 자세한내용은해당하이퍼바이저의설명서를참조하십시오.
- 방화벽에 **SSH** 가사용되는경우 **SSH** 사용: XenMobile 에대한관리자계정으로그은합니다.

CLI 를사용하여다양한구성및문제해결작업을수행할수있습니다. 다음그림은 CLI 의최상위메뉴를보여줍니다.

```
Main Menu
-----
[0] Configuration
[1] Clustering
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
```

구성옵션

다음은 **Configuration Menu** 의샘플과각옵션에대해표시되는설정입니다.

```
Configuration Menu
-----
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----
```

[1] Network

```
Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: y
IP address [10.207.87.75]: 10.200.87.75
Netmask [255.255.254.0]: 255.255.254.0
Default gateway [10.207.86.1]: 10.200.86.1
Primary DNS server [10.207.86.50]: 10.200.86.50
Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]: █
```

[2] Firewall

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
- comma separated list of hosts or networks
- e.g. 10.20.5.3, 10.20.6.0/24
- an empty value means no access restriction
- enter c as value to clear list

HTTP service
Port: 80
Enable access (y/n) [y]: y
Access white list []:

Management HTTPS service
Port: 4443
Enable access (y/n) [y]:
Access white list []:

SSH service
Port [22]:
Enable access (y/n) [y]:
Access white list []:

Management API (for initial staging) HTTPS service
Port [30001]:
Enable access (y/n) [n]:

Remote support tunnel
Port [8081]:
Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```

[3] Database

```
Type: [mi]
Use SSL (y/n) [n]:
Server [10.207.86.64]:
Port [1433]:
Username [sa]:
Password:
Database name [RC]:

Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: █
```

[4] Listener Ports

```
Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: y
HTTP [80]:
HTTPS with certificate authentication [443]:
HTTPS with no certificate authentication [8443]:
HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]: █
```

클러스터링 옵션

다음은 **Clustering Menu** 의 샘플과 각 옵션에 대해 표시되는 설정입니다.

```
-----
Clustering Menu
-----
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----
```

[1] Show Cluster Status

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75 status: ACTIVE role: OLDEST
node: 10.207.87.77 status: ACTIVE role: NONE
node: 10.207.87.88 status: ACTIVE role: NONE
```

[2] Enable/Disable cluster

클러스터링을사용하도록선택할경우다음과같은메시지가나타납니다.

To enable real-time communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings **for** restricted access.

클러스터링을사용하지않도록선택할경우다음과같은메시지가나타납니다.

You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.

[3] Cluster member white list

```
Current White List:
- comma separated list of hosts or networks
- e.g. 10.20.5.3, 10.20.6.0/24
- an empty value means no access restriction

Please enter hosts or networks to be white listed:
```

[4] Enable or disable SSL offload

SSL 오프로딩을사용할지여부를선택하면다음과같은메시지가나타납니다.

Enabling SSL offload opens port 80 **for** everyone. Please configure Access white list under Firewall settings **for** restricted access.

[5] Display Hazelcast Cluster

Hazelcast 클러스터를표시하도록선택하면다음과같은옵션이나타납니다.

Hazelcast Cluster Members:

[IP 주소나열됨]

참고:

구성된노드가클러스터의일부가아닌경우해당노드를다시시작하십시오.

시스템옵션

System Menu에서는시스템수준정보를표시또는설정하거나, 서버를다시시작또는종료하거나, **Advanced Settings**에액세스할수있습니다.

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

NTP 서버설정을통해 NTP 서버정보를지정할수있습니다. XenMobile 시간을하이퍼바이저와동기화할때표준시간대관련문제가나타나는경우 XenMobile 이 NTP 서버를가리키도록하면이문제를방지할수있습니다. 이옵션을변경한후에도모든클러스터서버를다시시작합니다.

[5]Display System Disk Usage 메뉴항목에서디스크공간을확인할수도있습니다.

[12] Advanced Settings

```

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

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

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
[7] Switch JDBC driver
-----

```

SSL protocols 옵션은 기본적으로 허용된 모든 프로토콜로 설정됩니다. **New SSL protocols to enable** 프롬프트가 표시되면 사용할 프로토콜을 입력합니다. XenMobile 은 응답에 포함되지 않은 모든 프로토콜을 사용하지 않습니다. 예를 들어 TLSv1 을 사용하지 않으려면 **TLSv1.2,TLSv1.1** 을 입력한 다음 **y** 를 입력하여 XenMobile Server 를 다시 시작합니다.

Server Tuning 옵션에는 서버 연결 시간 초과, 최대 연결 수 (포트별) 및 최대 스레드 수 (포트별) 가 포함됩니다.

Switch JDBC driver 옵션은 **JTDS** 와 **Microsoft** JDBC 입니다. 기본 드라이버는 JTDS 입니다. Microsoft JDBC 드라이버 전환에 대한 자세한 내용은 [SQL Server 드라이버](#) 를 참조하십시오.

문제 해결 옵션

다음은 **Troubleshooting Menu** 의 샘플과 각 옵션에 대해 표시되는 설정입니다.

```

-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----

```

[1] Network Utilities

```
-----
Network Menu
-----
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
-----
```

[2] 로그

```
-----
Logs Menu
-----
[0] Back to Troubleshooting Menu
[1] Display Log File
-----
```

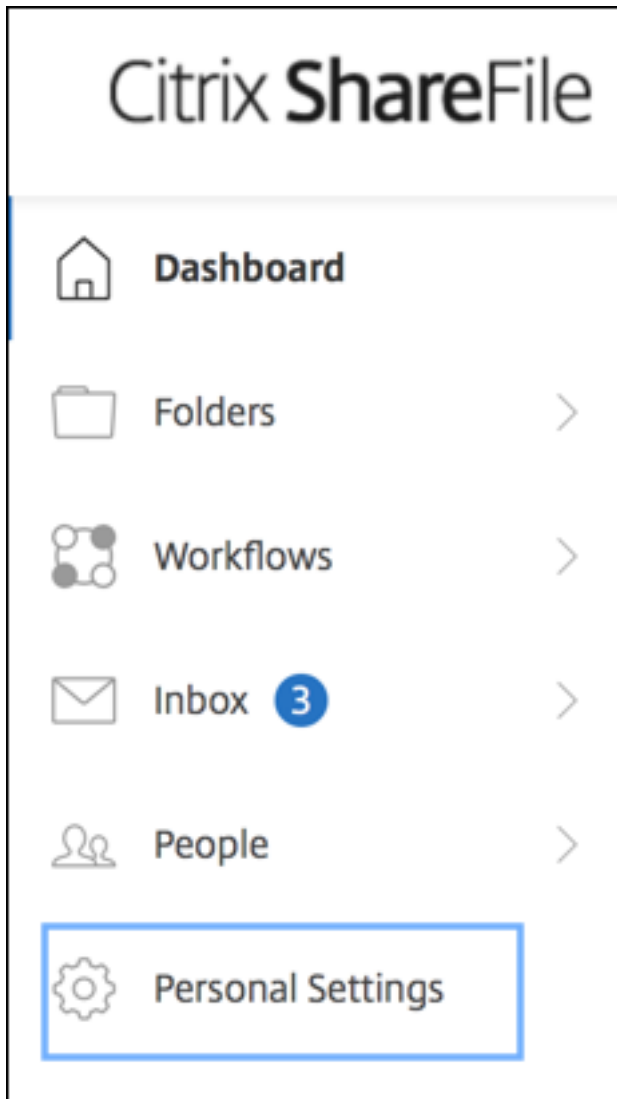
[3] Support Bundle

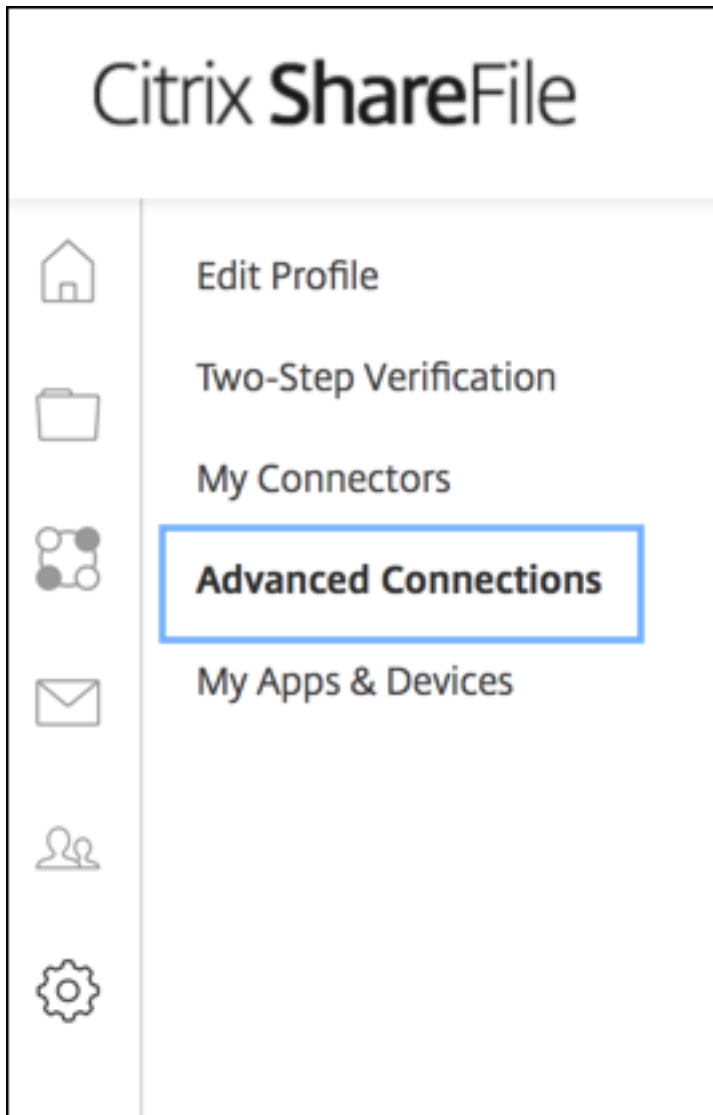
```
-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----
```

ShareFile 을 **FTP** 사이트로 사용하여 지원본들을 업로드하려면

지원본들업로드를 시작하기 전에 ShareFile 에서 다음 필수 구성요소를 구성합니다.

1. FTP 로그인 세부 정보를 확인합니다.
 - a. 웹브라우저에서 <https://citrix.sharefile.com> 을 엽니다.
 - b. **Personal Settings**(개인설정) 를 클릭한 후 **Advanced connections**(고급연결) 를 클릭합니다.





c. FTP 서버정보에서사용자이름에대한영숫자사용자 ID 가기본하위도메인/사용자이름세부정보와함께나타나는지확인합니다.

You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the / and @ characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

[Detailed Set-up Instructions](#)

FTP Server Information

Security: Standard (Port 21) or Implicit SSL/TLS (Port 990)
FTP Server: citrite.sharefileftp.com
User name: [redacted].com or [redacted]
Password: (your ShareFile password)

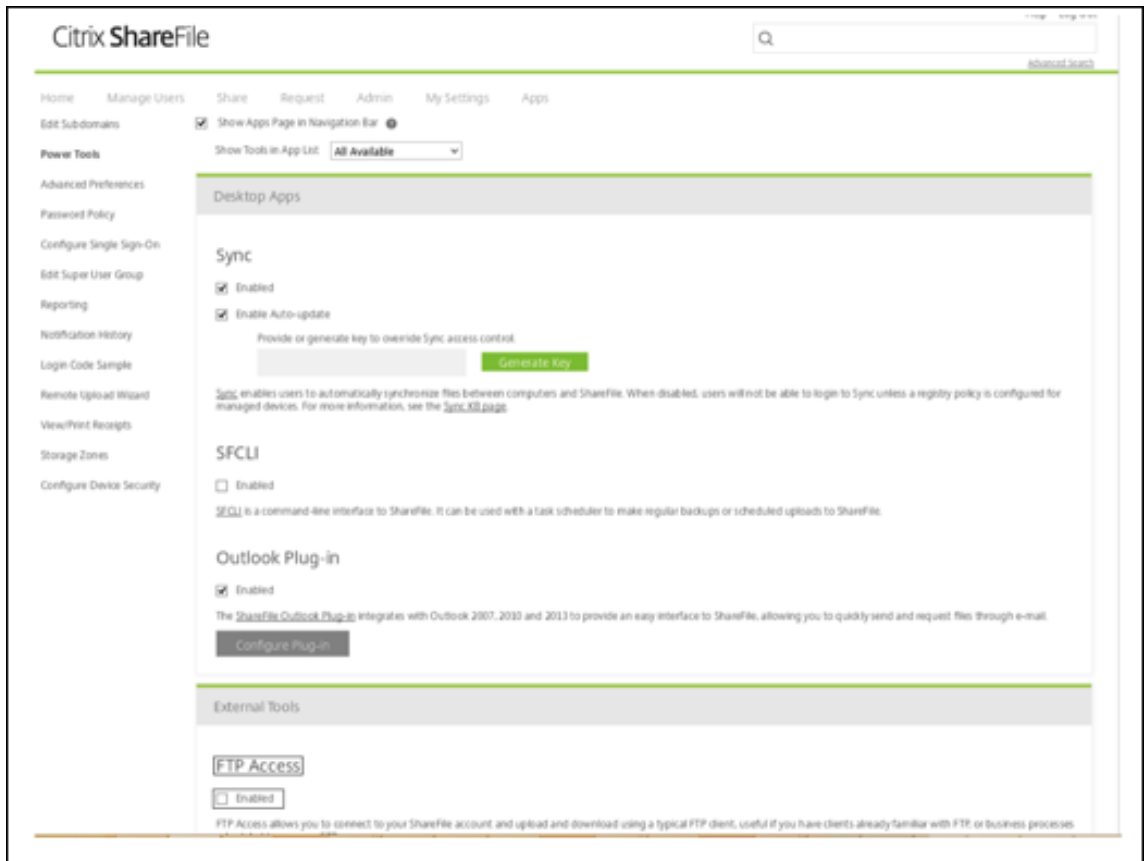
Both secure and standard FTP are enabled for your account.

참고:

- Linux CLI 기반 FTP 클라이언트인 XenMobile 에서 파일을 업로드하는 것이므로 백슬래시 (/) 와 단가 기호 (@) 문자를 사용자 이름의 일부로 입력할 수 없습니다.
- 영숫자 사용자 ID 가 보이지 않으면 ShareFile 관리자 또는 ShareFile 지원으로부터 사용자 ID 를 요청할 수 있습니다.

2. ShareFile 서버에서 FTP 통신 및 FTPS 를 사용할 수 있는지 확인합니다. 이상적으로는 ShareFile 관리자가 FTP 통신에서 사용자 계정을 여는 것을 허용합니다. 그러나 가끔은 FTPS 통신만 허용됩니다.

관리자 권한이 있는 사용자는 **Settings(설정)**, **Admin Settings(관리자 설정)**, **Advanced Preferences(고급 기본 설정)** 를 클릭한 후 **Enable ShareFile Tools(ShareFile 도구 사용)** 를 클릭하여 이 설정을 확인하고 사용하도록 설정할 수 있습니다. **External Apps(외부 앱)**, **FTP Access(FTP 액세스)** 에서 **Enable(사용)** 확인란을 선택해야 합니다.



3. FTP 클라이언트에서파일업로드에대한디렉터리로사용할공유폴더를만듭니다. **Home(홈)**, **Folders(폴더)** 를차례로 클릭한후 **Personal Folders(개인폴더)** 를클릭합니다.
4. 맨오른쪽에서더하기 (+) 아이콘을클릭하고 **Create Folder(폴더만들기)** 를클릭한다음폴더이름을입력합니다.

Create Folder [X]

* Required

Name: *

Description:

Add Users: Add People to Folder

Storage Zone: [v] [?]

5. XenMobile Server CLI 의 **Main Menu**(메인메뉴) 에서 **Troubleshooting**(문제해결) > **Support Bundle**(지원번들) 을 선택합니다. 그런다음 **Support Bundle Menu**(지원번들메뉴) 에서 **Generate Support Bundle**(지원번들생성) 을 선택합니다.



참고:

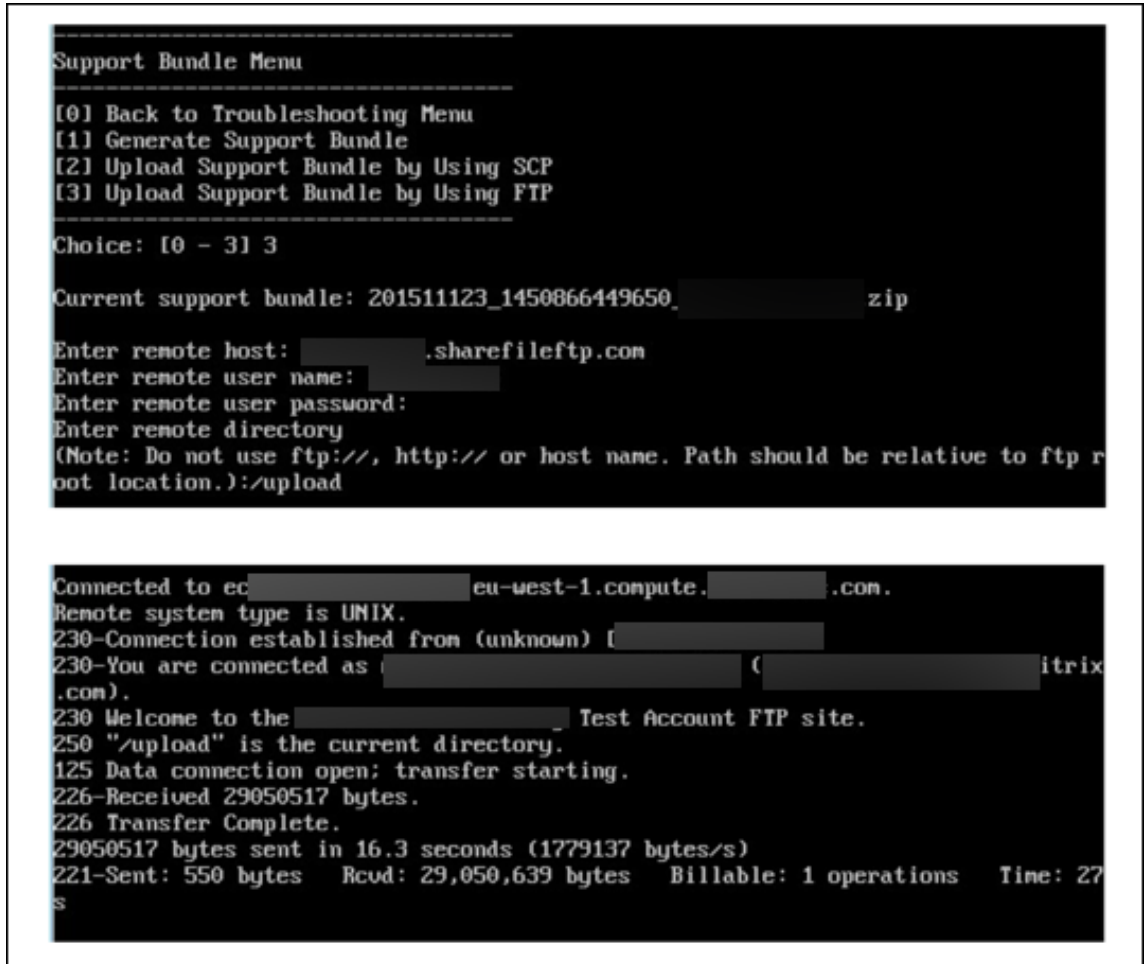
기존지원번들이있는경우메시지가표시되면 **y** 를입력하여번들을재정의합니다.

6. 지원번들을 FTP 서버에업로드합니다.

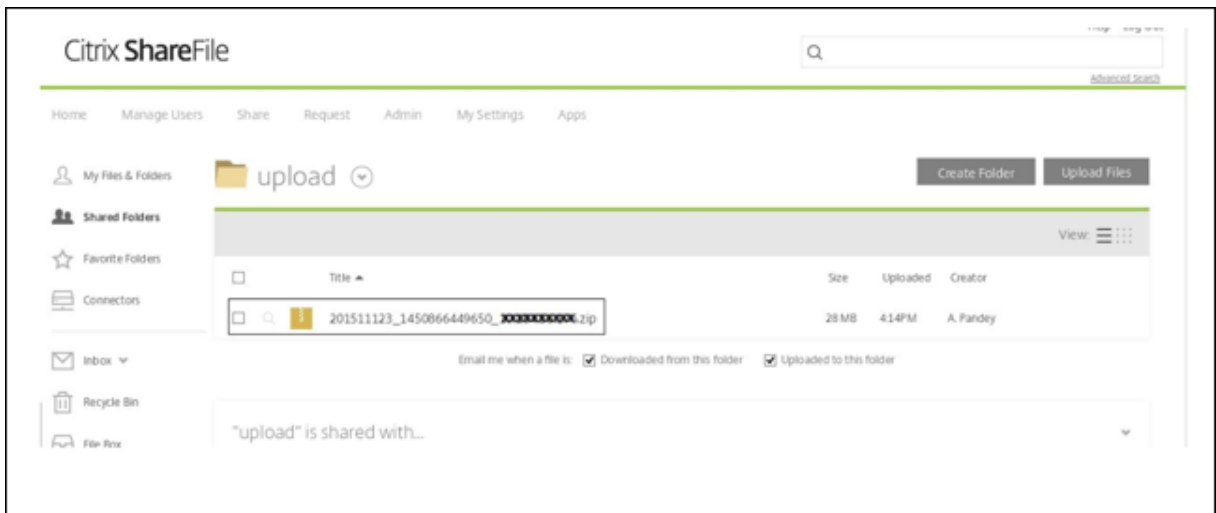
- a. **Upload Support Bundle by using FTP**(FTP 를사용하여지원번들업로드) 를선택합니다.
- b. **Enter remote host**(원격호스트입력) 메시지가표시되면 FTP 서버이름을입력합니다. ShareFile 이 FTP 서버로사용되는경우회사이름다음에 Sharefile FTP 사이트이름을입력합니다. 예: citrix.sharefileftp.com
- c. **Enter remote user name**(원격사용자이름입력) 메시지가표시되면영숫자사용자 ID 를입력합니다.

d. **Enter remote user password**(원격사용자암호입력) 메시지가표시되면암호를입력합니다.

e. **Enter remote directory**(원격디렉터리입력) 메시지가표시되면 ShareFile 에서만든공유폴더이름을입력한후 **Enter** 키를누릅니다.



업로드한지원번들을 ShareFile 에서만든공유폴더에서볼수있습니다.



XenMobile 및 ShareFile 에대한자세한내용은 [Citrix Support Knowledge Center 문서](#)를참조하십시오.

디스크공간을확인하려면

CLI 에서다음과같이시스템디스크공간을확인할수있습니다.

1. 메인메뉴에서 **System** 메뉴를선택합니다.
2. **System** 메뉴에서 **Display System Disk Usage** 옵션을선택합니다.

파일시스템정보가나타납니다.

```
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----
Choice: [0 - 12] 5

filesystem      1K-blocks      Used Available Use% Mounted on
dev/             49431012 3786556 43133500   9% /
mpfs             8191176    156 8191020    1% /run
evtmpfs         8190888      0 8190888    0% /dev
dev/             101086    10094 85773    11% /boot
```

XenMobile 콘솔에대한워크플로시작하기

January 6, 2020

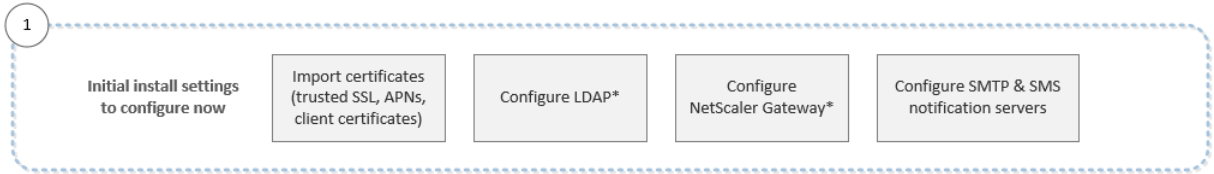
XenMobile 콘솔은 XenMobile 의통합된관리도구입니다. 이문서에서는 XenMobile 를설치했고콘솔에서작업할수있는상태 인것으로가정합니다. XenMobile 을아직설치하지않은경우 [XenMobile 설치](#)를참조하십시오. XenMobile 콘솔의브라우저 지원에대한자세한내용은 XenMobile 호환성문서를참조하십시오.

초기설정워크플로

명령줄콘솔과 XenMobile 콘솔에서차례로 XenMobile 을구성하고나면대시보드가열립니다. 초기구성화면으로돌아갈수없습니다. 일부설치구성을건너뛴경우콘솔에서다음설정을구성할수있습니다. 사용자, 앱및장치를추가하기전에다음설치설정을완료 해야합니다. 먼저콘솔의오른쪽맨위에있는기어아이콘을클릭합니다.

참고:

별표가있는항목은선택적요소입니다.



각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

- 인증
- [NetScaler Gateway](#) 및 [XenMobile](#)
- 알림

Android, iOS 및 Windows 플랫폼을지원하려면다음과같은계정관련설정을완료해야합니다.

Android

- Google Play 자격증명을만듭니다. 자세한내용은 [Google Play Launch\(시작\)](#)를참조하십시오.
- Android Enterprise 관리자계정을만듭니다. 자세한내용은 [Android Enterprise](#)에서참조하십시오.
- Google 의도메인이름을확인합니다. 자세한내용은 [G Suite 도메인확인](#)에서참조하십시오.
- API 를사용하도록설정하고 Android Enterprise 의서비스계정을만듭니다. 자세한내용은 [Android Enterprise 도움말](#)에서참조하십시오.

iOS

- Apple ID 와개발자계정을만듭니다. 자세한내용은 [Apple Developer Program](#) 웹사이트를참조하십시오.
- APNs(Apple 푸시알림서비스) 인증서를만듭니다. XenMobile Server 배포를사용하여 iOS 장치를관리하려는경우 Apple APNs 인증서가필요합니다. Secure Mail 배포에푸시알림을사용하는경우 Apple APNs 인증서도필요합니다. Apple APNs 인증서를얻는방법에대한자세한내용은 [Apple Push Certificates Portal](#)을참조하십시오. XenMobile 및 APNs 에대한자세한내용은 [APNs 인증서](#) 및 [iOS 용 Secure Mail 의푸시알림](#)을참조하십시오.
- VPP(Volume Purchase Program) 회사토큰을만듭니다. 자세한내용은 [Apple Volume Purchasing Program](#)에서참조하십시오.

Windows

- Microsoft Windows 스토어개발자계정을만듭니다. 자세한내용은 [계정유형, 위치및수수료를참조하십시오.](#)에서참조하십시오.
- Microsoft Windows 스토어게시자 ID 를가져옵니다. 자세한내용은 [계정설정및프로필정보관리](#)에서참조하십시오.
- DigiCert 의엔터프라이즈인증서를얻습니다. 자세한내용은 [배포할 Windows Phone 용업무용배포](#)를참조하십시오. 문서를참조하십시오.

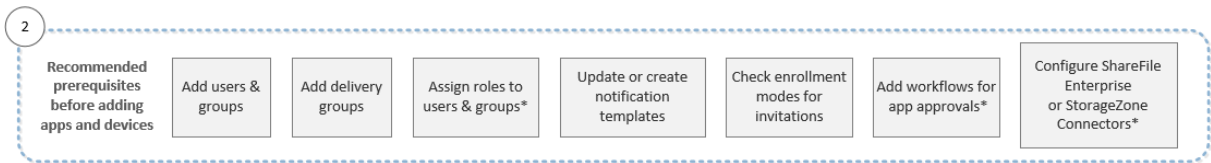
- Windows Phone 등록에 XenMobile 자동검색을사용하려는경우공용 SSL 인증서를사용할수있는지확인합니다. 자세한내용은 [XenMobile Autodiscovery Service](#)에서참조하십시오.
- AET(응용프로그램등록토큰) 를만듭니다. 자세한내용은 [Windows Phone 응용프로그램등록토큰을생성하는방법](#) 문서를참조하십시오.

콘솔사전요구사항워크플로

이워크플로에서는앱및장치를추가하기전에구성해야할사전요구사항을보여줍니다.

참고:

별표가있는항목은선택적요소입니다.



각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

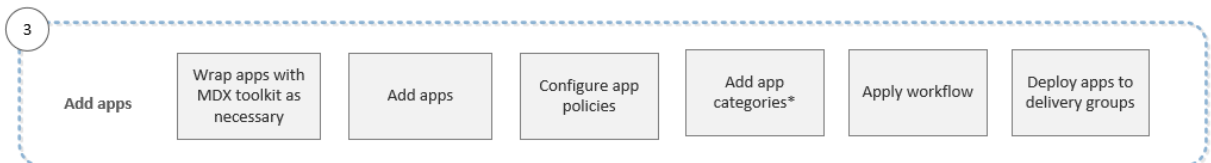
- [사용자계정, 역할및등록](#)
- [리소스배포](#)
- [RBAC 를사용하여역할구성](#)
- [알림](#)
- [워크플로만들기및관리](#)
- [XenMobile 에서 ShareFile 사용](#)

앱워크플로추가

이워크플로는 XenMobile 에앱을추가하는경우따라야할권장순서를보여줍니다.

참고:

별표가있는항목은선택적요소입니다.



각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

- [MDX Toolkit 정보](#)
- [앱추가](#)
- [MDX 정책요약](#)

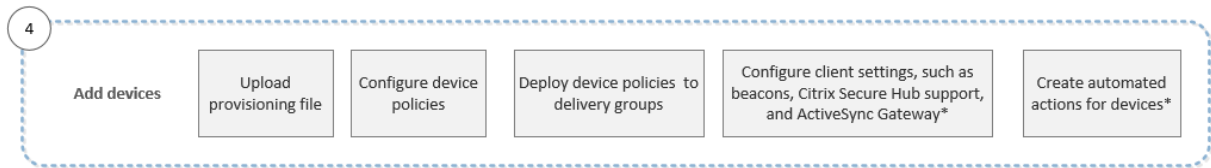
- [워크플로만들기및관리](#)
- [리소스배포](#)

장치워크플로추가

이워크플로는 XenMobile 에서장치를추가하고등록하는경우따라야할권장순서를보여줍니다.

참고:

별표가있는항목은선택적요소입니다.

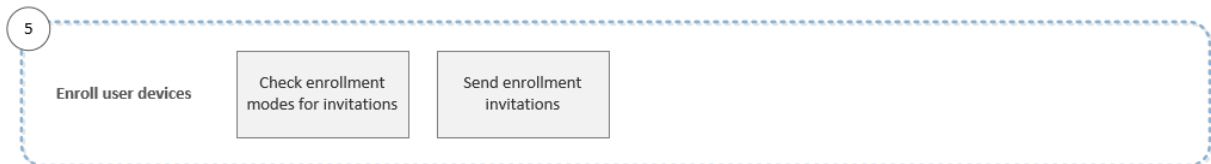


각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

- [장치](#)
- [지원되는장치운영체제](#)
- [리소스배포](#)
- [모니터링및지원](#)
- [자동화된동작](#)

사용자장치워크플로등록

이워크플로는 XenMobile 에서사용자장치를등록하는경우따라야할권장순서를보여줍니다.



각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서를참조하십시오.

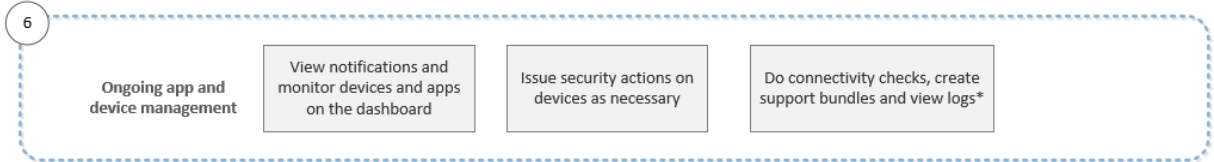
- [사용자계정, 역할및등록](#)
- [알림](#)

진행중인앱및장치관리워크플로

이워크플로는콘솔에서수행할수있는앱및장치관리작업을보여줍니다.

참고:

별표가있는항목은선택적요소입니다.



콘솔의오른쪽맨위에있는렌치아이콘을클릭하면표시되는지원옵션에대한자세한내용은 [모니터링및지원을참조하십시오](#).

인증서및인증

January 6, 2020

XenMobile 작동중에다음과같은다양한구성요소가인증에관여합니다.

- **XenMobile Server:** XenMobile Server 는등록보안및등록환경을정의하는위치입니다. 사용자등록에대한옵션은 다음과 같습니다.
 - 등록을모두에게공개할지초대전용으로할지여부.
 - 2 단계인증을요구할지 3 단계인증을요구할지여부. XenMobile 의클라이언트속성을통해 Citrix PIN 인증을사용하도록설정하고 PIN 의복잡성과만료시간을구성합니다.
- **NetScaler:** NetScaler 는 Micro VPN SSL 세션의종료기능을제공합니다. 또한 NetScaler 는네트워크전송중보안기능을제공하며사용자가앱에액세스할때마다사용되는인증환경을정의할수있게해줍니다.
- **Secure Hub:** 등록작업에서 Secure Hub 와 XenMobile Server 가함께작동합니다. Secure Hub 는장치에서 NetScaler 와통신하는엔터티입니다. 세션이만료되면 Secure Hub 가 NetScaler 로부터인증티켓을받아 MDX 앱에해당티켓을전달합니다. 메시지가로채기 (man-in-the-middle) 공격을방지할수있도록인증서고정기능을사용하는것이 좋습니다. 자세한내용은 Secure Hub 문서에서 [인증서고정](#)을참조하십시오.

또한 Secure Hub 를통해 MDX 보안컨테이너를쉽게사용할수있습니다. Secure Hub 를사용하여정책을푸시하고, 앱이시간초과되면 NetScaler 를통해세션을만들고, MDX 시간초과및인증환경을정의할수있습니다. 또한 Secure Hub 는탈옥감지, 지오로케이션확인및사용자가적용한모든정책을관리합니다.
- **MDX 정책:** MDX 정책은장치에서데이터저장소를만듭니다. MDX 정책은 Micro VPN 연결을다시 NetScaler 로리디렉션하고, 오프라인모드제한을적용하고, 시간초과같은클라이언트정책을적용합니다.

1 단계인증및 2 단계인증방법의개요를비롯한인증구성에대한자세한내용은배포안내서에서 [인증](#) 문서를참조하십시오.

XenMobile 의인증서를사용하여보안연결을만들고사용자를인증할수있습니다. 이문서의나머지부에서인증서에대해설명합니다. 다른구성세부정보에대해서는다음과같은문서를참조하십시오.

- [도메인인증또는도메인및보안토큰인증](#)

- 클라이언트인증서인증또는인증서와도메인인증
- PKI 엔터티
- 자격증명공급자
- APNs 인증서
- ShareFile SSO(Single Sign-on) 용 SAML
- Microsoft Azure Active Directory 서버설정
- WiFi 서버인증을위한인증서를장치로보내려면: [WiFi 장치정책](#)
- 인증에사용되지않는고유인증서또는특정정책을푸시하려면: [자격증명장치정책](#)

인증서

XenMobile 은서버로전달되는통신을보호하기위해자체서명된 SSL(Secure Sockets Layer) 인증서를설치중에생성합니다. 이 SSL 인증서를잘알려진 CA(인증기관) 의신뢰할수있는 SSL 인증서로교체해야합니다.

또한 XenMobile 은자체 PKI(공개키인프라) 서비스를사용하거나클라이언트인증서에대한 CA 로부터인증서를가져옵니다. 모든 Citrix 제품은와일드카드인증서와 SAN(주체대체이름) 인증서를지원합니다. 대부분의배포에서와일드카드또는 SAN 인증서 두개만있으면됩니다.

클라이언트인증서인증에는모바일앱을위한추가보안계층이제공되기때문에사용자가 HDX 앱에원활하게액세스할수있습니다. 클라이언트인증서인증이구성된경우사용자가 XenMobile 지원앱에액세스하려면 SSO(Single Sign-on) 용 Citrix PIN 을 입력해야합니다. 또한 Citrix PIN 은사용자인증환경을간소화합니다. Citrix PIN 은클라이언트인증서를보호하거나 Active Directory 자격증명을장치에로컬로저장하는데사용됩니다.

XenMobile 에서 iOS 장치를등록하고관리하려면 Apple 에서 APNs(Apple 푸시알림서비스) 인증서를설정하고만드십시오. 단계는 [APNs 인증서](#) 을참조하십시오.

다음표에서는각 XenMobile 구성요소에대한인증서형식및유형을보여줍니다.

XenMobile 구성요소	인증서형식	필요한인증서유형
NetScaler Gateway	PEM(BASE64), PFX(PKCS #12)	SSL, 루트 (NetScaler Gateway 가 PFX 를자동으로 PEM 으로변환함)
XenMobile Server	.p12(Windows 기반컴퓨터의경우.pfx)	SSL, SAML, APNs(XenMobile 이 설치프로세스중에전체 PKI 도생성함) 중요: XenMobile Server 는.pem 확장인증서를지원하지않습니다. .pem 인증서를사용하려면.pem 파일인증서와키로분할하고각각을 XenMobile Server 로가져옵니다.
StoreFront	PFX(PKCS #12)	SSL, 루트

XenMobile 은비트길이가 4096, 2048 및 1024 인 SSL 수신기인증서및클라이언트인증서를지원합니다. 1024 비트인증서는쉽게손상될수있습니다.

NetScaler Gateway 및 XenMobile Server 의경우 Verisign, DigiCert, Thawte 등과같은공용 CA 로부터서버인증서를받는것이 좋습니다. NetScaler Gateway 또는 XenMobile 구성유틸리티에서 CSR(인증서서명요청) 을만들수있습니다. CSR 을만든후 CA 에제출하여서명을받을수있습니다. CA 가서명된인증서를반환하면해당인증서를 NetScaler Gateway 또는 XenMobile 에설치할수있습니다.

중요: iOS 13 및 macOS 15 의신뢰할수있는인증서에대한요구사항

Apple 은 TLS 서버인증서에대한새로운요구사항을도입했습니다. 모든인증서가새로운 Apple 요구사항을따르는지확인하십시오. Apple 게시물 <https://support.apple.com/en-us/HT210176>를참조하십시오.

XenMobile 에서인증서업로드

업로드하는인증서에는인증서콘텐츠를포함하여인증서테이블의항목이포함됩니다. 인증서가필요한 PKI 통합구성요소를구성할때컨텍스트에종속적인조건을충족하는서버인증서를선택하십시오. 예를들어 Microsoft CA 와통합되도록 XenMobile 을구성한다고가정합니다. Microsoft CA 에대한연결은클라이언트인증서를사용하여인증되어야합니다.

이섹션에서는인증서를업로드하는일반적인절차를제공합니다. 클라이언트인증서만들기, 업로드및구성에대한자세한내용은 [클라이언트인증서인증또는인증서와도메인인증](#)을참조하십시오.

개인키요구사항

XenMobile 은지정된인증서에대한개인키를소유하거나소유하지않을수있습니다. 마찬가지로사용자가업로드한인증서에대해 XenMobile 이개인키를요구하거나요구하지않을수있습니다.

콘솔에인증서업로드

콘솔에인증서를업로드할때주요옵션두가지가있습니다.

- 키저장소가저오기를클릭할수있습니다. PKCS #12 형식을업로드하려는경우가아니라면계속해서설치하려는키저장소의항목을식별합니다.
- 인증서가저오기를클릭할수있습니다.

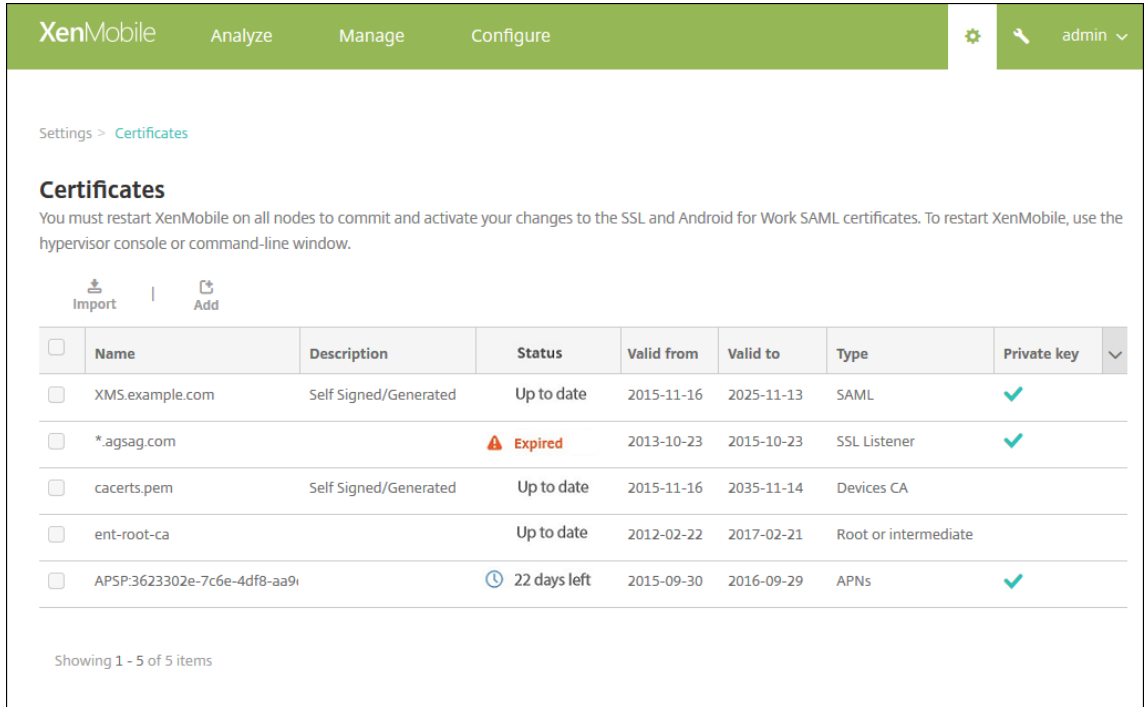
CA 가요청에서명하기위해사용하는 CA 인증서 (개인키포함안함) 를업로드할수있습니다. 또한클라이언트인증을위해 SSL 클라이언트인증서 (개인키포함) 를업로드할수있습니다.

Microsoft CA 엔터티를구성할때 CA 인증서를지정합니다. CA 인증서인모든서버인증서목록에서 CA 인증서를선택합니다. 마찬가지로, 클라이언트인증을구성할때 XenMobile 에개인키가있는모든서버인증서의목록에서선택할수있습니다.

키저장소를가져오려면

보안인증서저장소인키저장소는여러항목을포함할수있도록설계되어있습니다. 따라서키저장소에서로드할경우로드할항목을식별하는항목별칭을지정하라는메시지가나타납니다. 별칭을지정하지않으면저장소의첫번째항목이로드됩니다. PKCS #12 파일은대개항목하나만포함하기때문에 PKCS #12 를키저장소유형으로선택하면별칭필드가나타나지않습니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 인증서를클릭합니다. 인증서페이지가나타납니다.



3. 가져오기를클릭합니다. 가져오기대화상자가나타납니다.
4. 다음설정을구성합니다.
 - 가져오기: 목록에서 키저장소를클릭합니다. 가져오기대화상자가변경되어사용가능한키저장소옵션이나타납니다.

Import ✕

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import Keystore ▾

Keystore type PKCS#12 ▾

Use as Server ▾

Keystore file* Browse

Password*

Description

Cancel
Import

- 키저장소유형: 목록에서 **PKCS #12** 를클릭합니다.
- 용도: 목록에서인증서사용방법을클릭합니다. 사용가능한옵션은다음과같습니다.
 - 서버. 서버인증서는 XenMobile 웹콘솔에업로드되어 XenMobile Server 에서기능적으로사용되는인증서입니다. 여기에는 CA 인증서, RA 인증서및클라이언트인증용인증서와인프라의다른구성요소가포함됩니다. 또한서버인증서를장치에배포할인증서의저장소로사용할수있습니다. 이용도는특히장치에서신뢰를형성하는데사용되는 CA 에적용됩니다.
 - **SAML**. SAML(Security Assertion Markup Language) 인증을사용하면서버, 웹사이트및앱에대한 SSO 액세스를제공할수있습니다.
 - **APNs**. Apple 의 APNs 인증서를사용하면 Apple Push Network 를통해모바일장치를관리할수있습니다.
 - **SSL** 수신기. SSL(Secure Sockets Layer) 수신기는 XenMobile 에 SSL 암호화활동을알립니다.
- 키저장소파일: 찾아보기로가져올.p12(또는 Windows 기반컴퓨터의경우.pfx) 파일형식의키저장소를찾습니다.
- 암호: 인증서에할당된암호를입력합니다.
- 설명: 필요한경우서로다른키저장소를구분하는데도움이되는설명을입력합니다.

5. 가져오기를클릭합니다. 키저장소가인증서테이블에추가됩니다.

인증서를 가져오려면

파일 또는 키저장소 항목에서 인증서를 가져오면 XenMobile 이 입력에서 인증서 체인을 구성합니다. XenMobile 은 해당 체인의 모든 인증서를 가져와 각 인증서에 대한 서버 인증서 항목을 만듭니다. 이 작업은 파일 또는 키저장소 항목의 인증서가 체인을 형성하는 경우에만 작동합니다. 예를 들어 체인의 각 후속 인증서가 이전 인증서의 발급자여야 합니다.

필요한 경우 가져온 인증서에 대한 설명을 추가할 수 있습니다. 설명은 체인의 첫 번째 인증서에만 첨부됩니다. 나중에 나머지 인증서의 설명을 업데이트할 수 있습니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭한 다음 인증서를 클릭합니다.
2. 인증서 페이지에서 가져오기를 클릭합니다. 가져오기 대화상자가 나타납니다.
3. 가져오기 대화상자의 가져오기에서 인증서가 선택되어 있지 않은 경우 인증서를 클릭합니다.
4. 가져오기 대화상자가 변경되어 사용 가능한 인증서 옵션이 나타납니다. 용도에서 키저장소를 사용할 방법을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - 서버. 서버 인증서는 XenMobile 웹 콘솔에 업로드되어 XenMobile Server 에서 기능적으로 사용되는 인증서입니다. 여기에는 CA 인증서, RA 인증서 및 클라이언트 인증용 인증서와 인프라의 다른 구성 요소가 포함됩니다. 또한 서버 인증서를 장치에 배포할 인증서의 저장소로 사용할 수 있습니다. 이 옵션은 특히 장치에서 신뢰를 형성하는 데 사용되는 CA 에 적용됩니다.
 - **SAML**. SAML(Security Assertion Markup Language) 인증을 사용하면 서버, 웹 사이트 및 앱에 대한 SSO(Single Sign-On) 액세스를 제공할 수 있습니다.
 - **SSL** 수신기. SSL(Secure Sockets Layer) 수신기는 XenMobile 에 SSL 암호화 활동을 알립니다.
5. 찾아보기로 가져올.p12(또는 Windows 기반 컴퓨터의 경우.pfx) 파일 형식의 키저장소를 찾습니다.
6. 찾아보기로 인증서에 대한 선택적인 개인 키 파일을 찾습니다. 개인 키는 인증서의 암호화 및 암호 해독에 사용됩니다.
7. 필요한 경우 서로 다른 인증서를 구분할 때 도움이 되도록 인증서에 대한 설명을 입력합니다.
8. 가져오기를 클릭합니다. 인증서가 인증서 테이블에 추가됩니다.

인증서 업데이트

XenMobile 은 특정 시점에 공개 키당 하나의 인증서만 시스템에 존재하도록 허용합니다. 이미 가져온 인증서와 동일한 키쌍의 인증서를 가져오려고 하면 기존 항목을 바꾸거나 항목을 삭제할 수 있습니다.

인증서가 가장 효과적으로 업데이트하려면 XenMobile 콘솔에서 다음을 수행하십시오. 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭하여 설정 페이지를 연 다음 인증서를 클릭합니다. 가져오기 대화상자에서 새 인증서를 가져옵니다.

서버 인증서를 업데이트할 경우 이전 인증서를 사용하는 구성 요소가 자동으로 새 인증서를 사용하도록 전환됩니다. 마찬가지로, 장치에 서버 인증서를 배포한 경우 인증서가 다음 번 배포에서 자동으로 업데이트됩니다.

인증서 새로고침

XenMobile Server 는 PKI: 루트 CA, 장치 CA 및 서버 CA 에 대해 내부적으로 다음과 같은 인증기관을 사용합니다. 이러한 CA 는 논리적 그룹으로 분류되며 그룹 이름이 제공됩니다. 새 XenMobile Server 인스턴스를 프로비저닝하면 세계의 CA 가 생성되고 그룹 이름 “default(기본)” 가 지정됩니다.

XenMobile Server 콘솔 또는 공용 REST API 를 사용하여 지원되는 iOS, macOS 및 Android 장치에 대한 CA 를 갱신할 수 있습니다. 등록된 Windows 장치의 경우 새 장치 CA 를 받으려면 사용자가 장치를 재등록해야 합니다.

XenMobile Server 에서 내부 PKI CA 를 새로 고치거나 다시 생성하고 이러한 인증기관에서 발급한 장치 인증서를 갱신하는 데 다음과 같은 API 를 사용할 수 있습니다.

- 새 그룹 CA(인증기관) 를 만듭니다.
- 새 CA 를 활성화하고 이전 CA 를 비활성화합니다.
- 구성된 장치 목록에서 장치 인증서를 갱신합니다. 이미 등록된 장치는 중단 없이 계속 작동합니다. 장치가 서버에 다시 연결되면 장치 인증서가 발급됩니다.
- 여전히 이전 CA 를 사용 중인 장치의 목록을 반환합니다.
- 모든 장치가 새 CA 를 사용하게 되면 이전 CA 를 삭제합니다.

자세한 내용은 [XenMobile Public API for REST Services\(REST 서비스에 대한 XenMobile 공용 API\)](#) PDF 에서 다음 섹션을 참조하십시오.

1	-	섹션 3.16.58, Renew Device Certificate(장치 인증서 갱신)
2	-	섹션 3.23, Refresh XenMobile CA Group(XenMobile CA 그룹 새로 고침)

이 기능의 일부로 새로운 보안 동작인 인증서 갱신을 장치 관리 콘솔에서 사용할 수 있습니다. 이동작은 해당 장치의 등록 인증서를 갱신합니다.

사전 요구 사항

- 기본적으로 이 인증서 새로 고침 기능은 사용되지 않도록 설정됩니다. 인증서 새로 고침 기능을 활성화하려면 **refresh.internal.ca** 서버 속성 값을 **True** 로 설정하십시오.

중요:

NetScaler 에 SSL 오프로드가 설정된 경우 새 인증서를 생성할 때 cacert.perm 으로 부하 분산 장치를 업데이트해야 합니다. NetScaler Gateway 설정에 대한 자세한 내용은 [To use SSL Offload mode for NetScaler VIPs\(NetScaler VIP 에 SSL 오프로드 모드를 사용하려면\)](#) 문서를 참조하십시오.

클러스터 노드에 대한 서버 CA 인증서 암호를 재설정하는 CLI 옵션

한 XenMobile Server 노드에서 서버 CA 인증서를 생성한 후 XenMobile CLI 를 사용하여 다른 클러스터 노드의 인증서 암호를 재설정합니다. CLI 기본 메뉴에서 **System(시스템) > Advanced Settings(고급 설정) > Reset CA certs password(CA 인증서 암호 재설정)** 를 선택합니다. 새 CA 인증서가 없는 경우 암호를 재설정하면 XenMobile 이 암호를 재설정하지 않습니다.

```

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

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

*****

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
[7] Switch JDBC driver
-----

```

XenMobile 인증서관리

특히만료날짜와관련암호에대해, XenMobile 배포에서사용하는인증서를기록해두는것이 좋습니다. 이 섹션에서는 XenMobile 에서인증서를보다쉽게관리할수있도록도와줍니다.

환경에다음과같은인증서중일부또는전체가포함될수있습니다.

- XenMobile Server
 - MDM FQDN 에대한 SSL 인증서
 - SAML 인증서 (ShareFile 의경우)
 - 이전인증서및다른모든내부리소스 (StoreFront/프록시등) 에대한루트및중간 CA 인증서
 - iOS 장치관리용 APN 인증서
 - XenMobile Server Secure Hub 알림을위한내부 APNs 인증서
 - PKI 연결을위한 PKI 사용자인증서
- MDX Toolkit
 - Apple Developer 인증서
 - Apple 프로비전프로필 (응용프로그램별)
 - Apple APNs 인증서 (Citrix Secure Mail 용)
 - Android 키저장소파일
 - Windows Phone - DigiCert 인증서
- NetScaler
 - MDM FQDN 에대한 SSL 인증서
 - Gateway FQDN 에대한 SSL 인증서

- ShareFile SZC FQDN 에대한 SSL 인증서
- Exchange 부하분산에대한 SSL 인증서 (오프로드구성)
- StoreFront 부하분산에대한 SSL 인증서
- 이전인증서에대한루트및중간 CA 인증서

XenMobile 인증서만료정책

인증서가만료되도록허용하는경우인증서가무효화됩니다. 더이상환경에서보안트랜잭션을실행할수없으며 XenMobile 리소스에액세스할수없습니다.

참고:

만료날짜전에 CA(인증기관) 에서 SSL 인증서를갱신하라는메시지를표시합니다.

Citrix Secure Mail 용 APNs 인증서

APNs(Apple 푸시알림서비스) 인증서는매년만료됩니다. 인증서가만료되기전에 APNs SSL 인증서를만들고 Citrix 포털에서업데이트하십시오. 인증서가만료되면 Secure Mail 푸시알림에서불일치가발생합니다. 또한더이상업에대한푸시알림을보낼수없습니다.

iOS 장치관리를 APNs 인증서

XenMobile 에서 iOS 장치를등록하고관리하려면 Apple 에서 APNs 인증서를설정하고만드십시오. 인증서가만료되면사용자가 XenMobile 에등록할수없으며사용자의 iOS 장치를관리할수없게됩니다. 자세한내용은 [APNs 인증서](#)에서참조하십시오.

Apple Push Certificates Portal 에로그온하여 APNs 인증서상태및만료날짜를확인할수있습니다. 인증서를만든동일사용자로로그온해야합니다.

또한만료날짜 30 일전과 10 일전에 Apple 로부터전자메일알림을받게됩니다. 알림에는다음정보가포함되어있습니다.

```
1 The following Apple Push Notification Service certificate, created for
  Apple ID CustomerID will expire on Date. Revoking or allowing this
  certificate to expire will require existing devices to be re-
  enrolled with a new push certificate.
2
3 Please contact your vendor to generate a new request (a signed CSR),
  then visit https://identity.apple.com/pushcert to renew your Apple
  Push Notification Service certificate.
4
5 Thank You,
6
7 Apple Push Notification Service
```

MDX Toolkit(iOS 배포인증서)

물리적 iOS 장치에서 실행되는 앱 (Apple App Store 의 앱 제외) 은 다음과 같은 서명 요구 사항을 충족해야 합니다.

- 프로비전 프로파일 앱을 서명합니다.
- 해당하는 배포 인증서로 앱을 서명합니다.

유효한 iOS 배포 인증서가 있는지 확인하려면 다음을 수행하십시오.

1. Apple Enterprise Developer 포털에서 MDX Toolkit 으로 래핑할 작업에 대한 명시적 앱 ID 를 만듭니다. 사용할 수 있는 앱 ID 의 예는 다음과 같습니다. `com.CompanyName.ProductName`.
2. Apple Enterprise Developer 포털에서 **Provisioning Profiles(프로비전 프로파일) > Distribution(배포)** 으로 이동하고 사내 프로비전 프로파일 만듭니다. 이전 단계에서 만든 각 앱 ID 에 대해 이 단계를 반복합니다.
3. 모든 프로비전 프로파일을 다운로드합니다. 자세한 내용은 [iOS 모바일 앱 래핑](#)에서 참조하십시오.

모든 XenMobile Server 인증서가 유효한지 확인하려면 다음을 수행하십시오.

1. XenMobile 콘솔에서 **설정 > 인증서**를 클릭합니다.
2. APNs, SSL 수신기, 루트 및 중간 인증서를 비롯한 모든 인증서가 유효한지 확인합니다.

Android 키저장소

키저장소는 Android 앱에서 명하는 데 사용된 인증서가 들어 있는 파일입니다. 키 유효 기간이 만료되면 사용자가 더 이상 새 버전의 앱으로 원활하게 업그레이드할 수 없습니다.

Windows Phone 용 DigiCert 엔터프라이즈 인증서

DigiCert 는 Microsoft App Hub 서비스용 코드 서명 인증서의 독점적 공급자입니다. 개발자 및 소프트웨어 게시자는 App Hub 에 가입하여 Windows Marketplace 에 Windows Phone 및 Xbox 360 응용 프로그램을 배포하고 다운로드하게 만들 수 있습니다. 자세한 내용은 DigiCert 설명서에서 [DigiCert Code Signing Certificates for Windows Phone\(Windows Phone 용 DigiCert 코드 서명 인증서\)](#)을 참조하십시오.

인증서가 만료되면 Windows Phone 사용자가 등록할 수 없게 됩니다. 사용자는 회사가 게시하고 서명한 앱을 설치할 수 없거나 휴대폰에 설치된 회사 앱을 시작할 수 없습니다.

NetScaler

NetScaler 에서 인증서 만료를 처리하는 방법에 대한 자세한 내용은 Citrix Support Knowledge Center 에서 [How to handle certificate expiry on NetScaler\(NetScaler 에서 인증서 만료를 처리하는 방법\)](#)를 참조하십시오.

만료된 NetScaler 인증서를 통해서 는 사용자 가 스토어에 등록 및 액세스 할 수 없으며, Secure Mail 사용 시 Exchange Server 에 연결 할 수 없습니다. 또한 사용자가 HDX 앱을 나열하고 열 수 없습니다 (만료된 인증서에 따라 다름).

Expiry Monitor 및 Command Center 를 사용하면 NetScaler 인증서를 추적 할 수 있습니다. 인증서 만료 시 Center 로부터 알림을 받게 됩니다. 이러한 도구를 사용하여 다음과 같은 NetScaler 인증서를 모니터링 할 수 있습니다.

- MDM FQDN 에대한 SSL 인증서
- Gateway FQDN 에대한 SSL 인증서
- ShareFile SZC FQDN 에대한 SSL 인증서
- Exchange 부하분산에대한 SSL 인증서 (오프로드구성)
- StoreFront 부하분산에대한 SSL 인증서
- 이전인증서에대한루트및중간 CA 인증서

NetScaler Gateway 및 XenMobile

January 6, 2020

XenMobile 을사용하여 NetScaler Gateway 를구성할때내부네트워크에대한원격장치엑세스를위한인증메커니즘을설정합니다. 이기능을사용하면모바일장치의앱이인트라넷에위치한회사서버에엑세스할수있습니다. XenMobile 은장치의앱에서 NetScaler Gateway 로 Micro VPN 을만들수있습니다.

NetScaler Gateway 에서실행되는 XenMobile 에서스크립트를내보내어 XenMobile Server 와함께사용할 NetScaler Gateway 를구성합니다.

NetScaler Gateway 구성스크립트사용을위한필수구성요소

NetScaler 요구사항:

- NetScaler(최소버전 11.0, 빌드 70.12).
- LDAP 가부하분산되는경우이외에는 NetScaler IP 주소가구성되고 LDAP 서버에연결됩니다.
- NetScaler 서브넷 (SNIP) IP 주소가구성되어있고필요한백엔드서버에연결되며포트 8443/TCP 를통해공용네트워크 액세스가가능합니다.
- DNS 가공용도메인을확인할수있습니다.
- NetScaler 가플랫폼/범용또는평가판라이선스로라이선스허가되었습니다. 자세한내용은 <https://support.citrix.com/article/CTX126049>에서참조하십시오.
- NetScaler Gateway SSL 인증서가 NetScaler 에업로드되고설치되었습니다. 자세한내용은 <https://support.citrix.com/article/CTX136023>을참조하십시오.

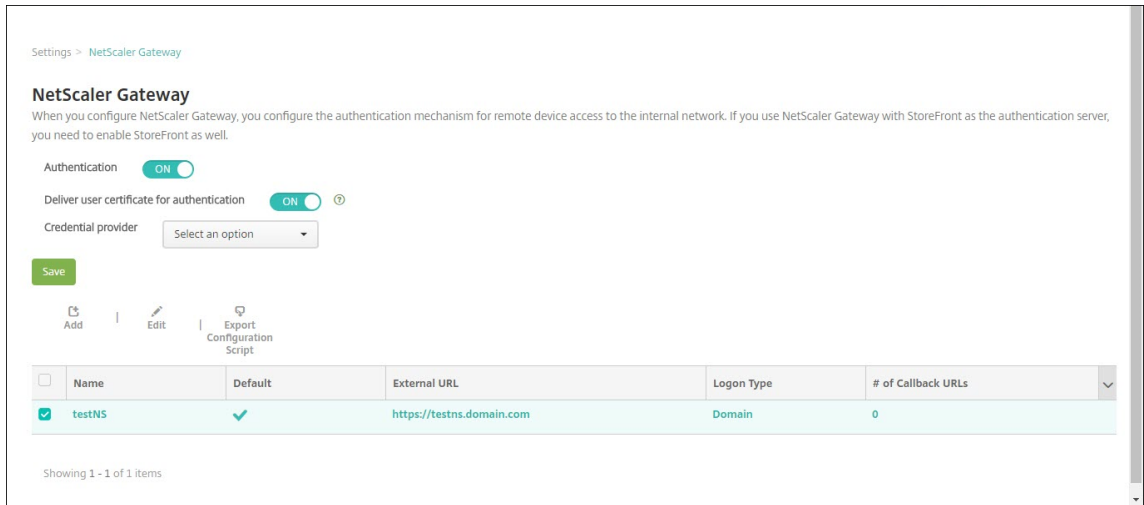
XenMobile 요구사항:

- XenMobile Server(최소버전 10.6).
- LDAP 서버가구성되었습니다.

내부네트워크에대한원격장치엑세스를위한인증구성

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.

2. 서버아래에서 **NetScaler Gateway** 를 클릭합니다. **NetScaler Gateway** 페이지가 나타납니다. 다음예제에서는 NetScaler Gateway 인스턴스가 존재합니다.



3. 다음설정을구성합니다.

- 인증: 인증을사용하도록설정하지여부를선택합니다. 기본값은 켜짐입니다.
- 인증을위한사용자인증서제공: NetScaler Gateway 가클라이언트인증서인증을처리하도록, XenMobile 에 서인증인증서를 Secure Hub 와공유하도록할지를선택합니다. 기본값은 꺼짐입니다.
- 자격증명공급자: 목록에서사용할자격증명공급자를클릭합니다. 자세한내용은 [자격증명공급자](#)에서참조하십시오.

4. 저장을클릭합니다.

NetScaler Gateway 인스턴스추가

인증설정을저장한후 NetScaler Gateway 인스턴스를 XenMobile 에추가합니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가열립니다.
2. 서버아래에서 **NetScaler Gateway** 를 클릭합니다. **NetScaler Gateway** 페이지가 나타납니다.
3. 추가를클릭합니다. 새 **NetScaler Gateway** 추가페이지가 나타납니다.

Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name*

Alias

External URL*

Logon Type

Password Required ON

Set as Default OFF

[Export Configuration Script](#)

Callback URL* Virtual IP* [Add](#)

[Cancel](#) [Save](#)

4. 다음설정을구성합니다.

- 이름: NetScaler Gateway 인스턴스의이름을입력합니다.
- 별칭: 원하는경우 NetScaler Gateway 의별칭이름을포함합니다.
- 외부 URL: NetScaler Gateway 의공개적으로액세스가능한 URL 을입력합니다. 예를들어 <https://receiver.com>입니다.
- 로그인유형: 로그인유형을선택합니다. 유형에는 도메인만, 보안토큰만, 도메인및보안토큰, 인증서, 인증서및도메인, 인증서및보안토큰이포함됩니다. 암호필요필드의기본설정은선택한 로그인유형에따라달라집니다. 기본값은도메인만입니다.

여러개의도메인이있는경우 인증서및도메인을사용합니다. XenMobile 및 NetScaler Gateway 를통한여러도메인인증구성에대한자세한내용은여러도메인에대한인증구성을참조하십시오.

인증서및보안토큰을사용하는경우 Secure Hub 를지원하기위해 NetScaler Gateway 에서몇가지추가구성이필요합니다. 자세한내용은 [Configuring XenMobile for Certificate and Security Token Authentication\(인증서및보안토큰인증을사용하기위한 XenMobile 구성\)](#)에서참조하십시오.

자세한내용은배포안내서의 인증을참조하십시오.

- 암호필요: 암호인증을요구할지여부를선택합니다. 기본값은선택한 로그인유형에따라달라집니다.
- 기본값으로설정: 이 NetScaler Gateway 를기본값으로사용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 구성스크립트내보내기: 단추를클릭하면 NetScaler Gateway 에업로드하는구성본들을내보내서 XenMobile 설정으로구성할수있습니다. 자세한내용은이단계위의 “XenMobile Server 와함께사용할온-프레미스 NetScaler Gateway 구성” 을참조하십시오.
- 콜백 URL 및 가상 IP: 이러한필드를추가하기전에설정을저장하십시오. 자세한내용은이문서에서콜백 URL 및 NetScaler Gateway VPN 가상 IP 추가를참조하십시오.

5. 저장을클릭합니다.

새 NetScaler Gateway 가추가되고테이블에나타납니다. 인스턴스를편집하거나삭제하려면목록에서이름을클릭합니다.

XenMobile Server 와함께사용할 NetScaler Gateway 구성

XenMobile Server 와함께사용할온-프레미스 NetScaler Gateway 를구성하려면이문서에서자세히설명하는다음일반단계를수행하십시오.

1. XenMobile Server 에서스크립트및관련파일을다운로드합니다. 최신의상세지침을보려면스크립트와함께제공되는추가정보파일을참조하십시오.
2. 환경이필수구성요소를충족하는지확인합니다.
3. 스크립트를환경에맞게업데이트합니다.
4. NetScaler 에서스크립트를실행합니다.
5. 구성을테스트합니다.

이스크립트로 XenMobile 에필요한 NetScaler Gateway 설정을구성합니다.

- MDM 및 MAM 에필요한 NetScaler Gateway 가상서버
- NetScaler Gateway 가상서버의세션정책
- XenMobile Server 세부정보
- NSG 가상서버의인증정책및동작 스크립트에 LDAP 구성설정이설명됩니다.
- 프록시서버의트래픽동작및정책
- 클라이언트없는액세스프로필
- NetScaler 의정적로컬 DNS 레코드
- 기타바인딩: 서비스정책, CA 인증서

다음구성은스크립트에서처리되지않습니다.

- Exchange 부하분산
- ShareFile 부하분산
- ICA 프록시구성
- SSL 오프로드

스크립트를다운로드, 업데이트및실행하려면

1. NetScaler Gateway 를추가하는경우 새 **NetScaler Gateway** 추가페이지에서 구성스크립트내보내기를클릭합니다.

Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name*

Alias

External URL*

Logon Type

Password Required

Set as Default

[Export Configuration Script](#)

Callback URL*	Virtual IP*	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

[Cancel](#) [Save](#)

또는 NetScaler Gateway 인스턴스를 추가하며스크립트를내보내기전에 저장을클릭하는경우: 설정 > **NetScaler Gateway** 로돌아가서 NetScaler 를선택한다음 구성스크립트내보내기과 다운로드를차레로클릭합니다.

Settings > NetScaler Gateway

NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication

Deliver user certificate for authentication

Credential provider

[Save](#)

[Add](#) | [Edit](#) | [Export Configuration Script](#)

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs
<input checked="" type="checkbox"/>	testNS	<input checked="" type="checkbox"/>	https://testns.domain.com	Domain	0

Showing 1 - 1 of 1 items

구성스크립트내보내기를클릭하면 XenMobile 에서.tar.gz 스크립트번들이만들어집니다. 스크립트번들에는다음이포함됩니다.

- 상세지침이포함된추가정보파일
- NetScaler 에서필요한구성요소를구성하는데사용되는 NetScaler CLI 명령이포함된스크립트
- 공용루트 CA 인증서와 XenMobile Server 의중간 CA 인증서 (현재릴리스에서는 SSL 오프로드에대해이러한 인증서가필요하지않음)
- NetScaler 구성을제거하는데사용되는 NetScaler CLI 명령이포함된스크립트

2. 스크립트 (NSGConfigBundle_CREATESCRIPT.txt) 를편집하여모든자리표시자를환경의세부정보로바꿉니다.

```
# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <NSG_ROOT_CA_CERT_TAG> -- NetScaler ROOT CA Tag.
# <RADIUS_KEY> -- Radius Key.
# <XMS_CERT_TAG> -- XenMobile Certificate Tag.
# <MAM_LB_IP> -- Virtual IP Address to be assigned for MAM Load-Balancer and this IP must follow the RFC 1918 standard of private IP addresses.
# <MDM_LB_IP> -- Virtual IP Address to be assigned for MDM Load-Balancer and this IP must follow the RFC 1918 standard of private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <NSG_VIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
```

3. 스크립트번들에포함된추가정보파일의설명에따라, 편집된스크립트를 NetScaler bash 셸 (shell) 에서실행합니다. 예를들면다음과같습니다.

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

```
login as: nsroot
#####
#
#          WARNING: Access to this system is for authorized users only          #
#          Disconnect IMMEDIATELY if you are not an authorized user!          #
#
#####

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.

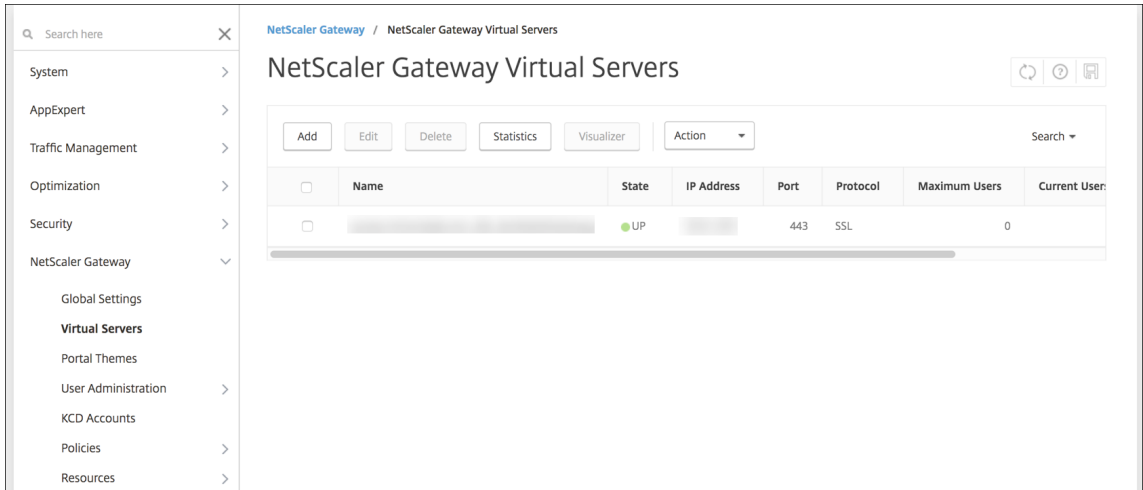
root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

스크립트가완료되면다음줄이나타납니다.

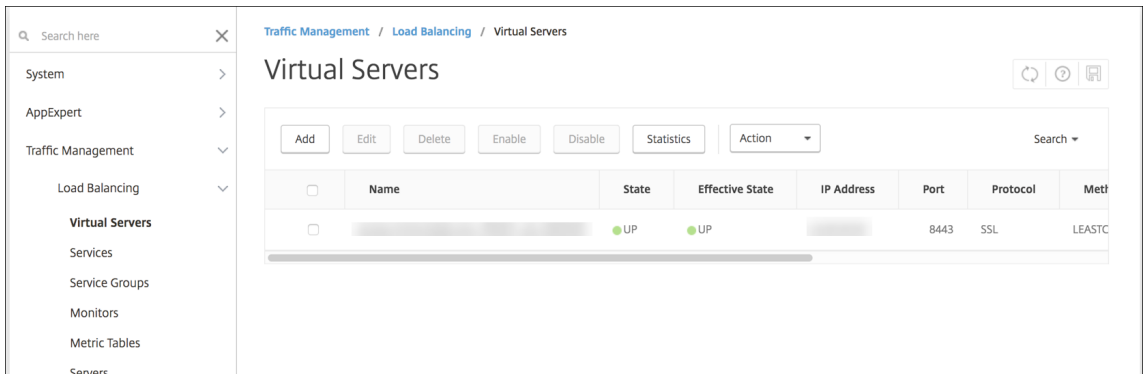
```
exec: save ns config
Done
Done
root@ns#
```

구성테스트

1. NetScaler Gateway 가상서버의상태가 작동인지확인합니다.



2. 프록시부하분산가상서버의상태가 작동인지확인합니다.



3. 브라우저를 열고 NetScaler Gateway URL 에 연결하여 인증을 시도합니다. 인증이 실패하면 HTTP 상태 404 - 찾을 수 없음 메시지가 나타납니다.

4. 장치를 등록하고 MDM 및 MAM 모두에 등록되었는지 확인합니다.

콜백 URL 및 NetScaler Gateway VPN 가상 IP 추가

NetScaler Gateway 인스턴스를 추가한 후 콜백 URL 을 추가하고 NetScaler Gateway 가상 IP 주소 를 지정할 수 있습니다. 이 설정은 선택 사항이지만 특히 XenMobile Server 가 DMZ 에 있는 경우 보안을 강화하기 위해 구성할 수 있습니다.

1. 설정 > **NetScaler Gateway** 에서 NetScaler Gateway 를 선택하고 편집을 클릭합니다.
2. 테이블에서 추가를 클릭합니다.
3. 콜백 **URL** 로 FQDN(정규화된 도메인 이름) 을 입력합니다. 콜백 URL 은 요청이 NetScaler Gateway 에서 온 요청인지 확인합니다.

콜백 URL 이 XenMobile Server 에서 연결 가능한 IP 주소로 확인되는지 확인합니다. 콜백 URL 은 외부 NetScaler Gateway URL 또는 다른 URL 일 수 있습니다.

4. NetScaler Gateway 가상 **IP** 주소를 입력한 다음 저장을 클릭합니다.

여러도메인에대한인증구성

테스트, 개발및프로덕션환경을위한다수의 XenMobile Server 인스턴스가있는경우추가환경에대한 NetScaler Gateway 를수동으로구성합니다. NetScaler for XenMobile 마법사는한번만사용할수있습니다.

NetScaler Gateway 구성

여러도메인환경에대한 NetScaler Gateway 인증정책및세션정책을구성하려면:

1. NetScaler Gateway 구성유틸리티의왼쪽탐색창에서 **Configuration(구성)** 탭으로이동하고 **NetScaler Gateway > Policies(정책) > Authentication(인증)** 을확장합니다.
2. 탐색창에서 **LDAP** 를클릭합니다.
3. LDAP 프로필을클릭하여편집합니다. **Server Logon Name Attribute(서버로그온이름특성)** 를 **userPrincipalName** 또는검색에사용하려는특성으로변경합니다. 지정한특성을기록합니다. XenMobile 콘솔에서 LDAP 설정을구성할때이특성을제공해야합니다.

The screenshot shows the 'Other Settings' section of the NetScaler Gateway configuration interface. It contains four dropdown menus for LDAP configuration:

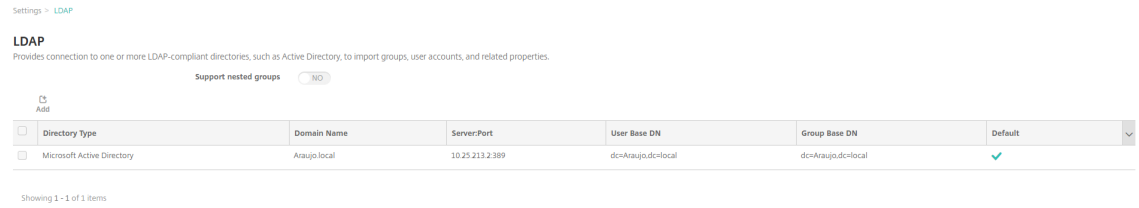
- Server Logon Name Attribute:** Set to 'sAMAccountName'.
- Search Filter:** An empty text input field.
- Group Attribute:** Set to 'memberOf'.
- Sub Attribute Name:** Set to 'cn'.

4. 각 LDAP 정책에대해이러한단계를반복합니다. 각도메인에는개별 LDAP 정책이필요합니다.
5. NetScaler Gateway 가상서버에바인딩된세션정책에서 **Edit session profile(세션프로필편집) > Published Applications(게시된응용프로그램)** 로이동합니다. **Single Sign-On Domain(Single Sign-On 도메인)** 이비어있는지확인합니다.

XenMobile Server 구성

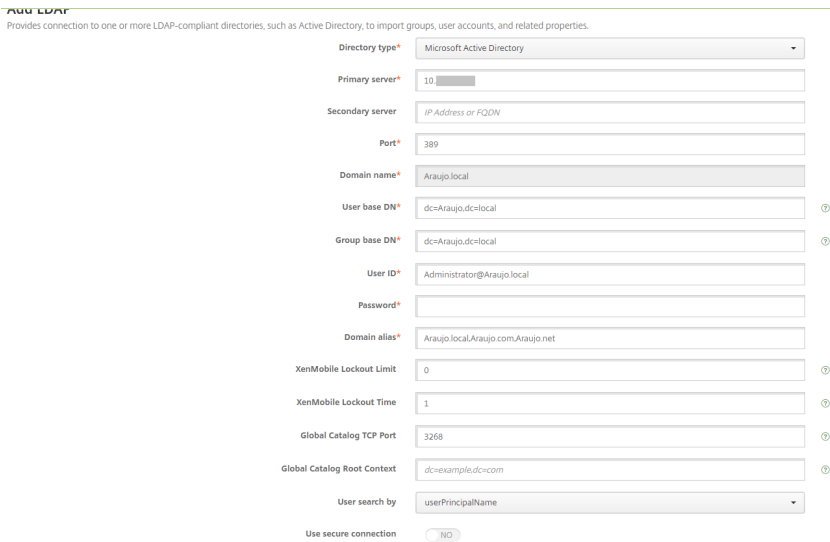
여러도메인의 XenMobile 환경에대한 LDAP 를구성하려면:

1. XenMobile 콘솔에서 설정 > **LDAP** 로이동하고디렉터리를추가하거나편집합니다.



2. 다음정보를제공합니다.

- 도메인별칭에서사용자인증에사용할각도메인을지정합니다. 도메인을심표로구분하십시오. 도메인사이에공백을사용하지하십시오. 예: domain1.com,domain2.com,domain3.com
- 사용자검색기준필드가 NetScaler Gateway LDAP 정책에서지정한 **Server Logon Name Attribute**(서버로그온이름특성) 와일치하는지확인합니다.



특정 **URL** 에대한인바운드연결요청삭제

사용자환경의 Citrix Gateway 에 SSL 오프로드가구성된경우게이트웨이에서특정 URL 에대한인바운드연결요청을삭제하는것이좋습니다.

추가보안을원하는경우 Citrix Gateway 에서두개의 MDM 부하분산장치 vServer(포트 443 용및포트 8443 용) 를구성합니다. 설정시다음정보를템플릿으로활용합니다.

중요:

다음업데이트는 SSL 오프로드가구성된 Citrix Gateway 에만적용됩니다.

1. XMS_DropURLs라는이름의패턴집합을만듭니다.

```
1 add policy patset XMS_DropURLs
```

2. 이새로운패턴집합에다음 URL 을추가합니다. 필요에따라이목록을사용자지정합니다.

```
1 bind policy patset XMS_DropURLs /zdm/shp/console -index 6
2
3 bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5
4
5 bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4
6
7 bind policy patset XMS_DropURLs /zdm/log.jsp -index 3
8
9 bind policy patset XMS_DropURLs /zdm/login.jsp -index 2
10
11 bind policy patset XMS_DropURLs /zdm/console -index 1
```

3. 연결요청이 지정된서브넷에서시작되지않는한이러한 URL 에대한모든트래픽을삭제하는정책을만듭니다.

```
1 add responder policy XMS_DROP_pol "CLIENT.IP.SRC.IN_SUBNET
(192.168.0.0/24).NOT &&
2 HTTP.REQ.URL.CONTAINS_ANY(" XMS_DropURLs ") " DROP -comment "Allow
only subnet 192.168.0.0/24 to access these URLs. All other
connections are DROPed"
```

4. 새정책을두 MDM 부하분산장치 vServer(포트 443 및 8443) 에바인딩합니다.

```
1 bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
REQUEST
2
3 bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
REQUEST
```

도메인인증또는도메인및보안토큰인증

January 6, 2020

XenMobile 은 LDAP(Lightweight Directory Access Protocol) 와호환되는하나이상의디렉터리에대한도메인기반인증을지원합니다. XenMobile 에서하나이상의디렉터리에대한연결을구성한다면다음 LDAP 구성을사용하여그룹, 사용자계정및관련속성을가져올수있습니다.

LDAP 는 IP(인터넷프로토콜) 네트워크를통한분산디렉터리정보서비스액세스및유지관리를지원하는공급업체중립적인오픈소스 응용프로그램프로토콜입니다. 디렉터리정보서비스는네트워크에서사용가능한사용자, 시스템, 네트워크, 서비스및응용프로그램에대한정보를공유하는데사용됩니다.

LDAP 는일반적으로다수의서비스에서하나의암호 (사용자당) 를공유하는 SSO(Single Sign-on) 를사용자에게제공할때사용됩니다. SSO(Single Sign-on) 를사용하면사용자가회사웹사이트에한번로그온하여회사인트라넷에대한액세스를인증할수있습니다.

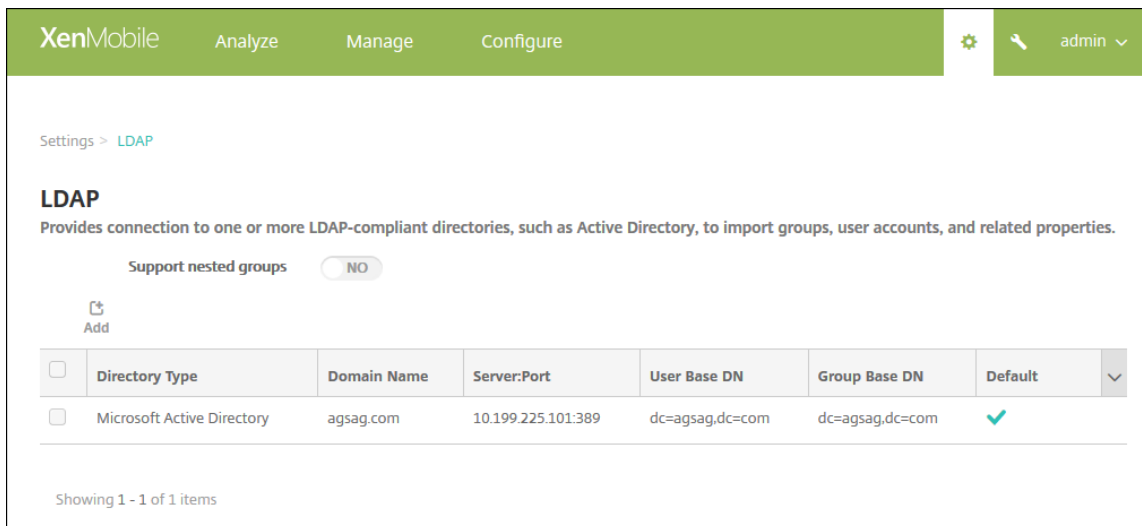
클라이언트는 DSA(Directory System Agent) 라고하는 LDAP 서버에연결하여 LDAP 세션을시작합니다. 그런다음클라이언트는서버에작업요청을보내고서버는적절한인증으로응답합니다.

중요:

XenMobile 은사용자가 XenMobile 에서장치를등록한후도메인인증에서다른인증모드로의인증모드변경을지원하지않습니다.

XenMobile 에서 LDAP 연결을추가하려면

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버에서 **LDAP** 를클릭합니다. **LDAP** 페이지가나타납니다. 이문서에설명된대로 LDAP 호환디렉터리를추가, 편집또는삭제할수있습니다.



LDAP 호환디렉터리를추가하려면

1. **LDAP** 페이지에서 추가를클릭합니다. **LDAP** 추가페이지가나타납니다.

The screenshot displays the 'Add LDAP' configuration interface in the XenMobile console. The breadcrumb trail is 'Settings > LDAP > Add LDAP'. The main heading is 'Add LDAP' with a sub-description: 'Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.' The form contains the following fields and values:

- Directory type*: Microsoft Active Directory (dropdown)
- Primary server*: IP Address or FQDN (text input)
- Secondary server: IP Address or FQDN (text input)
- Port*: 389 (text input)
- Domain name*: (text input)
- User base DN*: dc=example,dc=com (text input)
- Group base DN*: dc=example,dc=com (text input)
- User ID*: (text input)
- Password*: (text input)
- Domain alias*: (text input)
- XenMobile Lockout Limit: 0 (text input)
- XenMobile Lockout Time: 1 (text input)
- Global Catalog TCP Port: 3268 (text input)
- Global Catalog Root Context: dc=example,dc=com (text input)
- User search by: userPrincipalName (dropdown)
- Use secure connection: NO (radio button)

Buttons for 'Cancel' and 'Save' are located at the bottom right of the form.

2. 다음설정을구성합니다.

- 디렉터리유형: 목록에서적절한디렉터리유형을클릭합니다. 기본값은 **Microsoft Active Directory** 입니다.
- 주서버: LDAP 에사용되는주서버를입력합니다. IP 주소또는 FQDN(정규화된도메인이름) 을입력할수있습니다.
- 보조서버: 보조서버가구성된경우선택적으로보조서버의 IP 주소또는 FQDN 을입력합니다. 이서버는주서버에연결할수없을때사용되는장애조치 (failover) 서버입니다.
- 포트: LDAP 서버가사용하는포트번호를입력합니다. 기본적으로포트번호는보안되지않은 LDAP 연결의경우 **389** 로설정됩니다. 보안 LDAP 연결에는포트번호 **636** 을사용하고, Microsoft 비보안 LDAP 연결에는 **3268** 을사용하고, Microsoft 보안 LDAP 연결에는 **3269** 를사용하십시오.
- 도메인이름: 도메인이름을입력합니다.
- 사용자기본 **DN**: 고유식별자를통해 Active Directory 의사용자위치를입력합니다. 구문의예로는 `ou=users, dc=example` 또는 `dc=com`이있습니다.

- 그룹기본 **DN**: Active Directory 의그룹위치를입력합니다. 예를들어 **cn=users**, **dc=domain**, **dc=net**를입력합니다. 여기서, **cn=users**는그룹의컨테이너이름을나타내고 **dc**는 Active Directory 의도메인 구성요소를나타냅니다.
- 사용자 **ID**: Active Directory 계정과연관된사용자 ID 를입력합니다.
- 암호: 사용자와연관된암호를입력합니다.
- 도메인별칭: 도메인이름의별칭을입력합니다.
- **XenMobile** 잠금제한: 실패한로그온시도횟수를 **0** 에서 **999** 사이의숫자로입력합니다. **0** 값은 XenMobile 이실패한로그온시도를기준으로사용자를잠그지않음을의미합니다.
- **XenMobile** 잠금시간: 잠금제한을초과한후사용자가대기해야하는시간 (분) 을나타내는 **0** 에서 **99999** 사이의 숫자를입력합니다. **0** 값은잠금후사용자가대기하지않아도됨을의미합니다.
- 글로벌카탈로그 **TCP** 포트: 글로벌카탈로그서버의 TCP 포트번호를입력합니다. 기본적으로 TCP 포트번호는 **3268** 로설정됩니다. SSL 연결의경우포트번호 **3269** 를사용하십시오.
- 글로벌카탈로그루트컨텍스트: 필요한경우 Active Directory 의글로벌카탈로그검색을사용하도록설정하는데 사용되는글로벌루트컨텍스트값을입력합니다. 이검색은실제도메인이름을지정할필요가없는모든도메인에서표준 LDAP 검색에추가됩니다.
- 사용자검색기준: 목록에서 **userPrincipalName** 또는 **sAMAccountName** 을클릭합니다. 기본값은 **userPrincipalName** 입니다.
- 보안연결사용: 보안연결을사용할지여부를선택합니다. 기본값은 아니요입니다.

3. 저장을클릭합니다.

LDAP 호환디렉터리를편집하려면

1. **LDAP** 테이블에서편집하려는디렉터리를선택합니다.

디렉터리옆에있는확인란을선택하면 LDAP 목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.

2. 편집을클릭합니다. **LDAP** 편집페이지가나타납니다.

Settings > LDAP > Add LDAP

Edit LDAP
Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type* Microsoft Active Directory

Primary server* 10.61

Secondary server IP Address or FQDN

Port* 389

Domain name* .net

User base DN* dc=.dcnet

Group base DN* dc=.dcnet

User ID* administrator@.net

Password*

Domain alias* .net

XenMobile Lockout Limit 0

XenMobile Lockout Time 1

Global Catalog TCP Port 3268

Global Catalog Root Context dc=example,dc=com

User search by userPrincipalName

Use secure connection NO

3. 다음정보를적절하게변경합니다.

- 디렉터리유형: 목록에서적절한디렉터리유형을클릭합니다.
- 주서버: LDAP 에사용되는주서버를입력합니다. IP 주소또는 FQDN(정규화된도메인이름) 을입력할수있습니다.
- 보조서버: 필요한경우보조서버의 IP 주소또는 FQDN 을입력합니다 (보조서버가구성된경우).
- 포트: LDAP 서버가사용하는포트번호를입력합니다. 기본적으로포트번호는보안되지않은 LDAP 연결의경우 **389** 로설정됩니다. 보안 LDAP 연결에는포트번호 **636** 을사용하고, Microsoft 비보안 LDAP 연결에는 **3268** 을사용하고, Microsoft 보안 LDAP 연결에는 **3269** 를사용하십시오.
- 도메인이름: 이필드를편집할수없습니다.
- 사용자기본 **DN**: 고유식별자를통해 Active Directory 의사용자위치를입력합니다. 구문의예로는 **ou=users, dc=example** 또는 **dc=com**이있습니다.
- 그룹기본 **DN**: **cn=groupname** 형식으로지정된그룹기본 DN 그룹이름을입력합니다. 예: **cn=users, dc=servername, dc=net**. 여기서 **cn=users**는그룹이름입니다. DN 및 **servername** 은 Active Directory 를실행하는서버의이름을나타냅니다.
- 사용자 **ID**: Active Directory 계정과연관된사용자 ID 를입력합니다.
- 암호: 사용자와연관된암호를입력합니다.
- 도메인별칭: 도메인이름의별칭을입력합니다.
- **XenMobile** 잠금제한: 실패한로그온시도횟수를 **0** 에서 **999** 사이의숫자로입력합니다. **0** 값은 XenMobile 이실패한로그온시도를기준으로사용자를잠그지않음을의미합니다.
- **XenMobile** 잠금시간: 잠금제한을초과한후사용자가대기해야하는시간 (분) 을나타내는 **0** 에서 **99999** 사이의 숫자를입력합니다. **0** 값은잠금후사용자가대기하지않아도됨을의미합니다.
- 글로벌카탈로그 **TCP** 포트: 글로벌카탈로그서버의 TCP 포트번호를입력합니다. 기본적으로 TCP 포트번호는 **3268** 로설정됩니다. SSL 연결의경우포트번호 **3269** 를사용하십시오.
- 글로벌카탈로그루트컨텍스트: 필요한경우 Active Directory 의글로벌카탈로그검색을사용하도록설정하는데사용되는글로벌루트컨텍스트값을입력합니다. 이검색은실제도메인이름을지정할필요가없는모든도메인에서표준

LDAP 검색에추가됩니다.

- 사용자검색기준: 목록에서 **userPrincipalName** 또는 **sAMAccountName** 을클릭합니다.
- 보안연결사용: 보안연결을사용할지여부를선택합니다.

4. 저장을클릭하여변경내용을저장하거나 취소를클릭하여속성을변경하지않고그대로유지합니다.

LDAP 호환디렉터리를삭제하려면

1. **LDAP** 테이블에서삭제하려는디렉터리를선택합니다.

각속성옆에있는확인란을선택하여삭제할속성을둘이상선택할수있습니다.

2. 삭제를클릭합니다. 확인대화상자가나타납니다. 삭제를다시클릭합니다.

여러도메인에대한인증구성

LDAP 구성에서여러도메인접미사를사용하도록 XenMobile Server 를구성하려면 Citrix Endpoint Management 설명서에서 [여러도메인에대한인증구성](#)의절차를참조하십시오. 이러한단계는온-프레미스버전의 XenMobile Server 와 Endpoint Management 클라우드릴리스에서동일합니다.

도메인과보안토큰인증구성

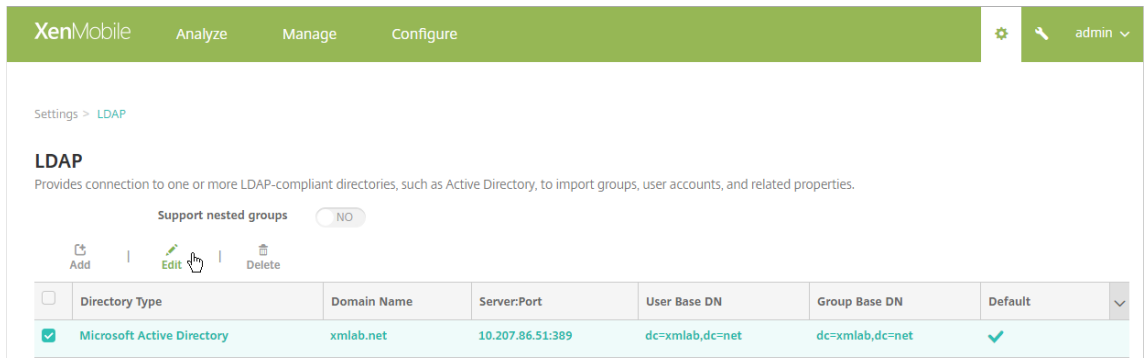
RADIUS 프로토콜을사용하여사용자가 LDAP 자격증명과일회용암호를사용하여인증하도록 XenMobile 을구성할수있습니다.

사용편의성을최적화하기위해이구성을 Citrix PIN 및 Active Directory 암호캐싱과결합할수있습니다. 이구성에서는사용자가 LDAP 사용자이름과암호를반복적으로입력하지않아도됩니다. 등록, 암호만료및계정잠금의경우사용자가사용자이름과암호를입력합니다.

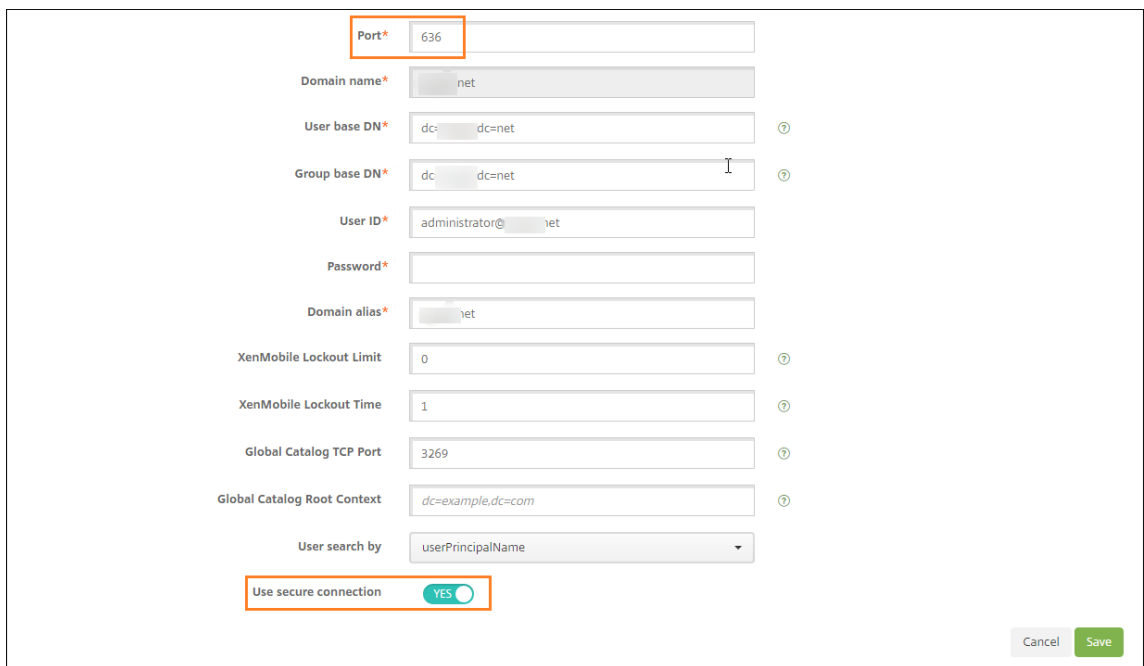
LDAP 설정구성

인증에 LDAP 를사용하려면 XenMobile 에인증기관에서발급한 SSL 인증서를설치해야합니다. 자세한내용은 [XenMobile 에서인증서업로드](#)에서참조하십시오.

1. 설정에서 **LDAP** 를클릭합니다.
2. **Microsoft Active Directory** 를선택한다음 편집을클릭합니다.



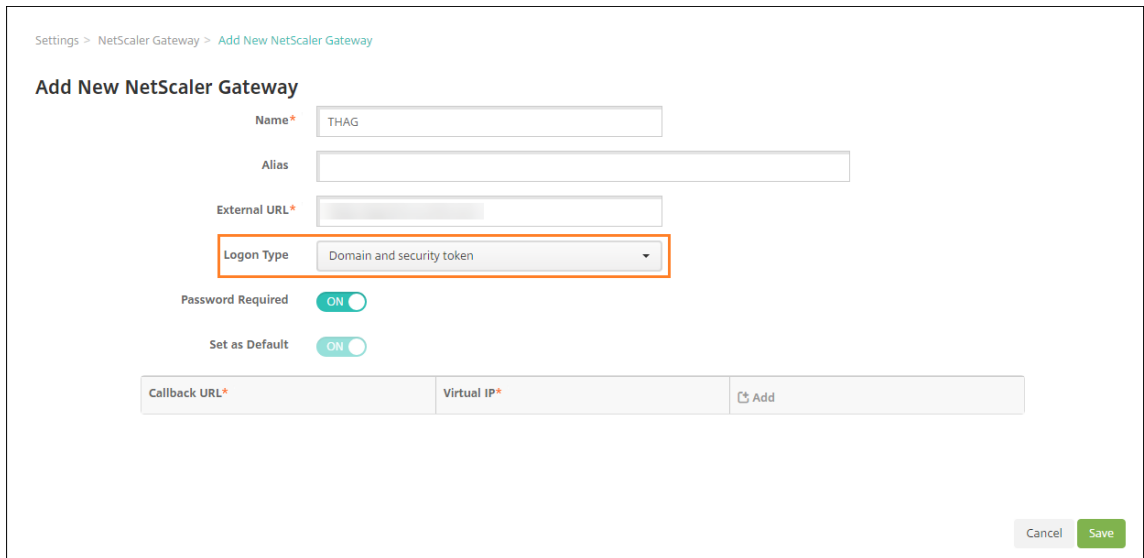
3. 포트가 **636**(보안 LDAP 연결의 경우) 또는 **3269**(Microsoft 보안 LDAP 연결의 경우) 인지 확인합니다.
4. 보안연결사용을 예로 변경합니다.



NetScaler Gateway 설정구성

다음단계에서는 이미 NetScaler Gateway 인스턴스를 XenMobile 에 추가했다고 가정합니다. 새 NetScaler Gateway 인스턴스를 추가하려면 [NetScaler Gateway 인스턴스 추가](#)를 참조하십시오.

1. 설정에서 **NetScaler Gateway** 를 클릭합니다.
2. **NetScaler Gateway** 를 선택한 다음 편집을 클릭합니다.
3. 로그인 유형에서 도메인 및 보안 토큰을 선택합니다.



Citrix PIN 및 사용자 암호 캐싱 사용

Citrix PIN 및 사용자 암호 캐싱을 사용하도록 설정하려면 설정 > 클라이언트 속성으로 이동하여 **Enable Citrix PIN Authentication (Citrix PIN 인증 사용)** 및 **Enable User Password Caching (사용자 암호 캐싱 사용)** 확인란을 선택합니다. 자세한 내용은 [클라이언트 속성](#)에서 참조하십시오.

도메인 및 보안 토큰 인증을 위해 NetScaler Gateway 구성

XenMobile 과 함께 사용되는 가상 서버에 대한 NetScaler Gateway 세션 프로필 및 정책을 구성합니다. 자세한 내용은 NetScaler Gateway 설명서를 참조하십시오.

클라이언트 인증서 인증 또는 인증서와 도메인 인증

January 6, 2020

XenMobile 에 대한 기본 구성은 사용자 이름 및 암호 인증입니다. XenMobile 환경에 대한 등록 및 액세스 시 추가 보안 계층을 추가하려면 인증서 기반 인증을 사용하는 것이 좋습니다. XenMobile 환경에서 이 구성은 보안과 사용자 환경을 모두 고려한 최고의 조합입니다. 인증서 인증과 도메인 인증을 함께 사용하면 SSO 를 사용하는 동시에 NetScaler 의 2 단계 인증을 통해 강화된 보안이 적용됩니다.

사용 편의성을 최적화하기 위해 인증서 및 도메인 인증을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다. 그러면 사용자가 LDAP 사용자 이름과 암호를 반복적으로 입력하지 않아도 됩니다. 등록, 암호 만료 및 계정 잠금의 경우 사용자가 사용자 이름과 암호를 입력합니다.

중요:

XenMobile 은 사용자가 XenMobile 에서 장치를 등록한 후 도메인 인증에서 다른 인증 모드로의 인증 모드 변경을 지원하지 않습니다.

LDAP 를 허용하지 않고 스마트카드 또는 유사한 방법을 사용하는 경우 인증서를 구성하면 XenMobile 에 스마트카드를 나타낼 수 있습니다. 그런 다음 사용자는 XenMobile 에서 생성된 고유한 PIN 을 사용하여 등록합니다. 사용자가 액세스 권한을 획득하면 XenMobile 이 XenMobile 환경에 인증하는 데 사용될 인증서를 만들어 배포합니다.

NetScaler 인증서 단독 인증 또는 인증서 및 도메인 인증을 사용하는 경우 NetScaler for XenMobile 마법사를 통해 XenMobile 에 필요한 구성을 수행할 수 있습니다. NetScaler for XenMobile 마법사는 한번만 실행할 수 있습니다.

보안이 매우 중요한 환경에서는 조직 외부의 공용 네트워크 또는 보안되지 않은 네트워크에서 LDAP 자격 증명을 사용하는 것이 조직에 큰 보안 위협으로 간주됩니다. 이러한 환경에서는 클라이언트 인증서와 보안 토큰을 사용하는 2 단계 인증을 선택할 수 있습니다. 자세한 내용은 [Configuring XenMobile for Certificate and Security Token Authentication\(인증서 및 보안 토큰 인증을 사용하기 위한 XenMobile 구성\)](#)에서 참조하십시오.

클라이언트 인증서 인증은 XenMobile MAM 모드 (MAM 단독) 및 ENT 모드 (사용자가 MDM 으로 등록시) 에 사용할 수 있습니다. 하지만 사용자가 레거시 MAM 모드로 등록하는 경우 클라이언트 인증서 인증을 XenMobile ENT 모드에 사용할 수 없습니다. XenMobile ENT 및 MAM 모드로 클라이언트 인증서 인증을 사용하려면 Microsoft 서버와 XenMobile Server 를 구성한 후 NetScaler Gateway 를 구성해야 합니다. 이 문서에 설명된 대로 다음의 일반적인 단계를 따릅니다.

Microsoft 서버:

1. Microsoft Management Console 에 인증서 스냅인을 추가합니다.
2. CA(인증기관) 에 템플릿을 추가합니다.
3. CA 서버에서 PFX 인증서를 만듭니다.

XenMobile Server:

1. XenMobile 에 인증서를 업로드합니다.
2. 인증서 기반 인증을 위한 PKI 엔터티를 만듭니다.
3. 자격 증명 공급자를 구성합니다.
4. 인증을 위한 사용자 인증서를 제공하도록 NetScaler Gateway 를 구성합니다.

NetScaler Gateway 구성에 대한 자세한 내용은 Citrix ADC 설명서 [Client authentication\(클라이언트 인증\)](#), [SSL profile infrastructure\(SSL 프로파일 인프라\)](#) 및 [Configuring and Binding a Client Certificate Authentication Policy\(클라이언트 인증서 인증 구성 및 바인딩\)](#)를 참조하십시오.

사전 요구 사항

- Microsoft 인증서 서비스 엔터티 템플릿을 생성할 때는 특수 문자를 제외하여 등록된 장치와 관련된 인증 문제를 방지하십시오. 예를 들어 템플릿 이름에 다음 문자를 사용하지 마십시오. : ! \$ () ## % + * ~ ? | { } []

- 인증서인증 및 SSL 오프로드를 사용하는 Windows Phone 8.1 장치의 경우 NetScaler 의 두 부분 산 가상 서버에서 포트 443 에 대한 SSL 세션 재사용을 사용하지 않도록 설정합니다. 그렇게 하려면 가상 서버에서 포트 443 에 대해 다음 명령을 실행합니다.

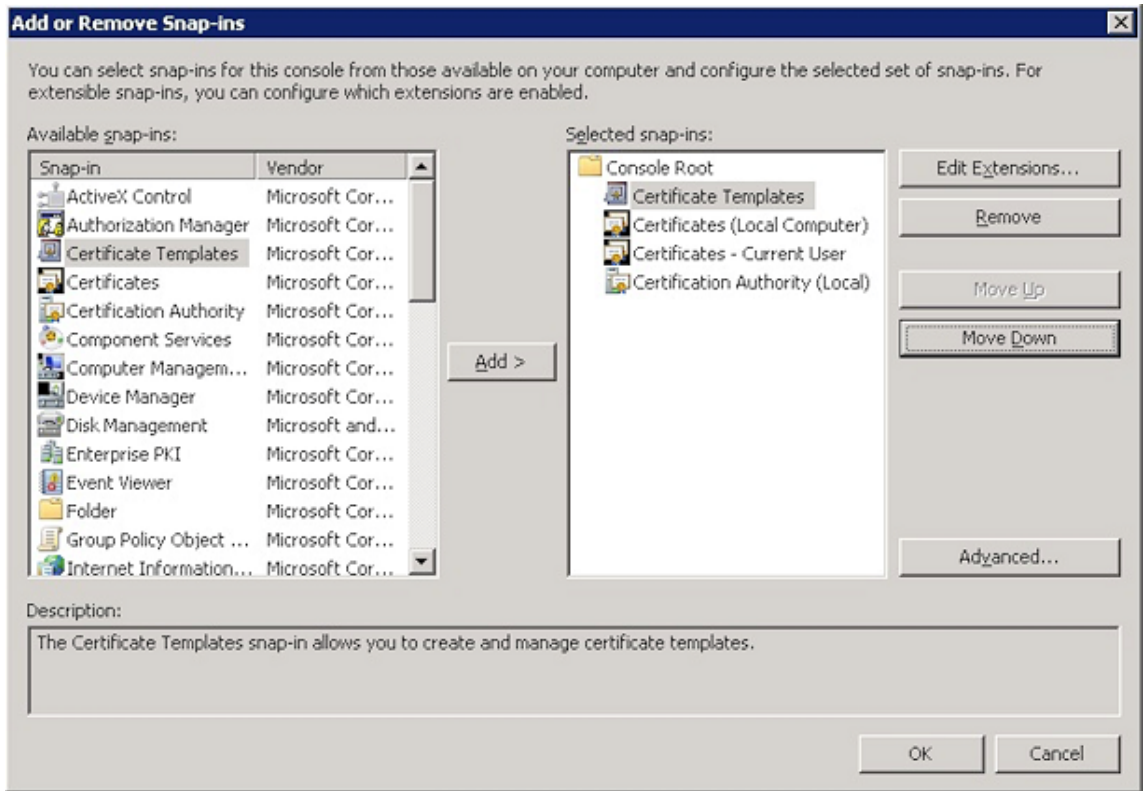
```
set ssl vserver <ssl lb vserver> sessReuse DISABLE
```

SSL 세션 재사용을 사용하지 않도록 설정하면 NetScaler 가 제공하는 일부 최적화 기능이 해제되어 NetScaler 의 성능이 저하될 수 있습니다.

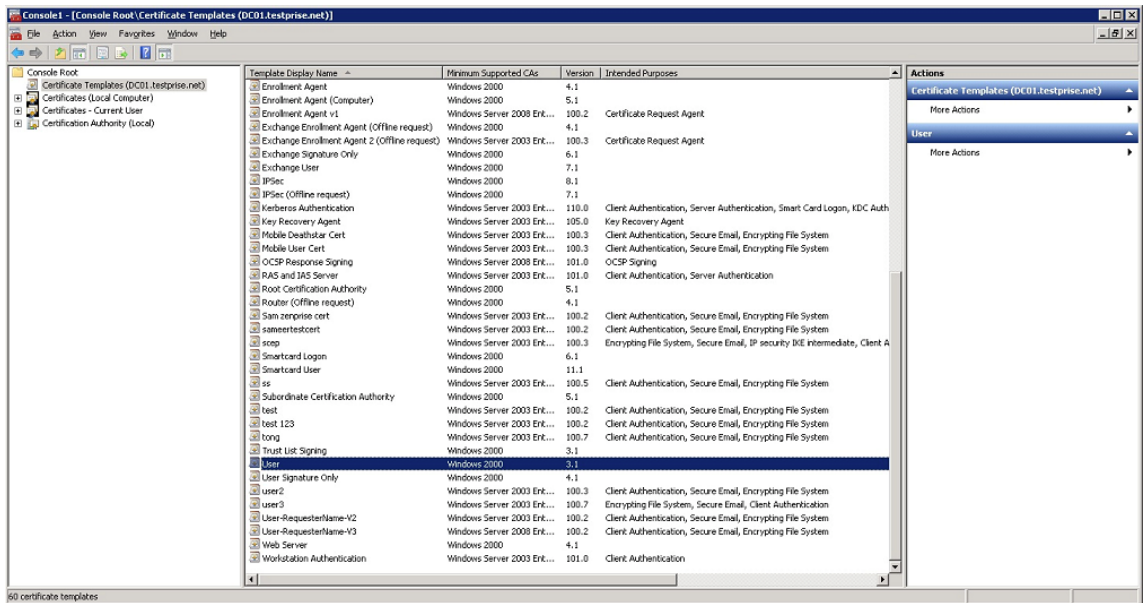
- Exchange ActiveSync 에 대한 인증서 기반 인증을 구성하려면 이 [Microsoft 블로그](#) 를 참조하십시오.
- Exchange Server 로의 ActiveSync 트래픽을 보안하기 위해 개인 서버 인증서를 사용하는 경우, 모든 루트 및 중간 인증서가 모바일 장치에 있어야 합니다. 그렇지 않으면 Secure Mail 에서 사서함을 설정하는 동안 인증서 기반 인증이 실패합니다. Exchange IIS 콘솔에서 다음 작업을 수행해야 합니다.
 - Exchange 와 함께 XenMobile 을 사용하기 위한 웹사이트를 추가하고 웹 서버 인증서를 바인딩합니다.
 - 포트 9443 을 사용합니다.
 - 해당 웹사이트에 대해 “Microsoft Server ActiveSync” 용 하나와 “EWS” 용 하나의 두 가지 응용 프로그램을 추가해야 합니다. 이러한 응용 프로그램 모두에 대해 **SSL** 설정 아래에서 **SSL** 필요를 선택합니다.
- 배포 방법에 필요한 경우 Secure Mail 이 최신 MDX Toolkit 으로 래핑되어 있는지 확인합니다.

Microsoft Management Console 에 인증서 스냅인을 추가합니다

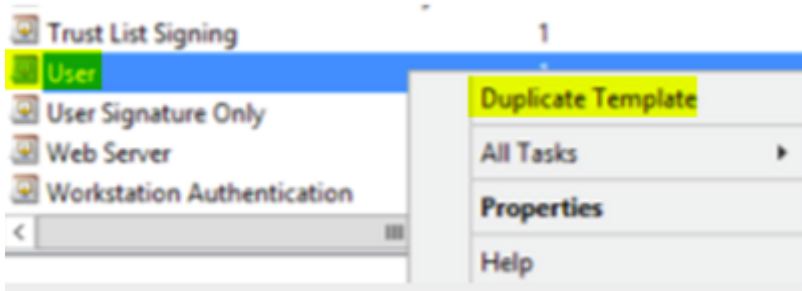
1. 콘솔을 열고 스냅인 추가/제거를 클릭합니다.
2. 다음과 같은 스냅인을 추가합니다.
 - 인증서 템플릿
 - 인증서 (로컬 컴퓨터)
 - 인증서 - 현재 사용자
 - 인증기관 (로컬)



3. 인증서 템플릿을 확장합니다.



4. 사용자 템플릿과 템플릿 복제를 선택합니다.

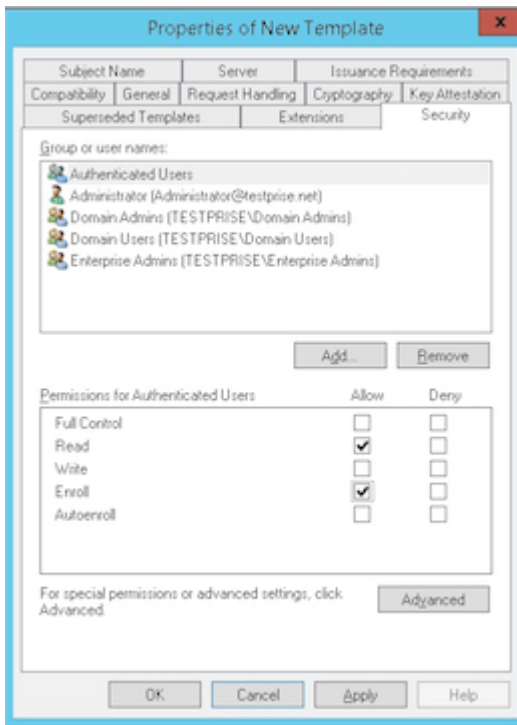


5. 템플릿표시이름을제공합니다.

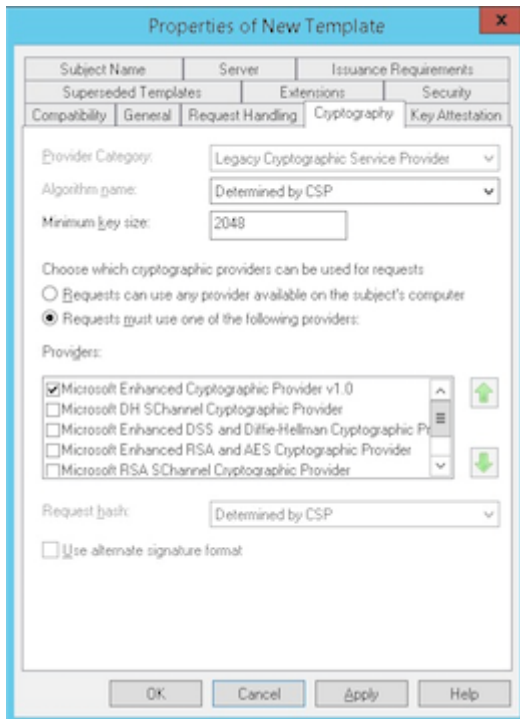
중요:

필요한경우에만 **Active Directory** 에인증서게시확인란을선택합니다. 이옵션을선택하면모든사용자클라이언트인증서가 Active Directory 에서생성되어 Active Directory 데이터베이스가복잡해질수있습니다.

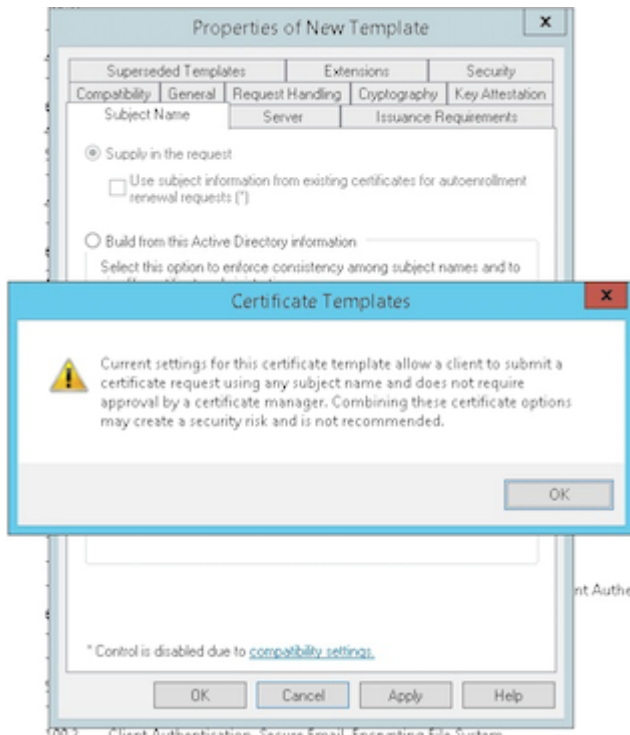
6. 템플릿유형으로 **Windows 2003 Server** 를선택합니다. Windows 2012 R2 서버에서 호환성아래에있는 인증기관을선택하고받는사람을 **Windows 2003** 으로설정합니다.
7. 보안아래에서인증된사용자에대해 허용열의 등록옵션을선택합니다.



8. 암호화아래에서키키기를제공하는지확인합니다. 키키는나중에 XenMobile 을구성할때입력합니다.



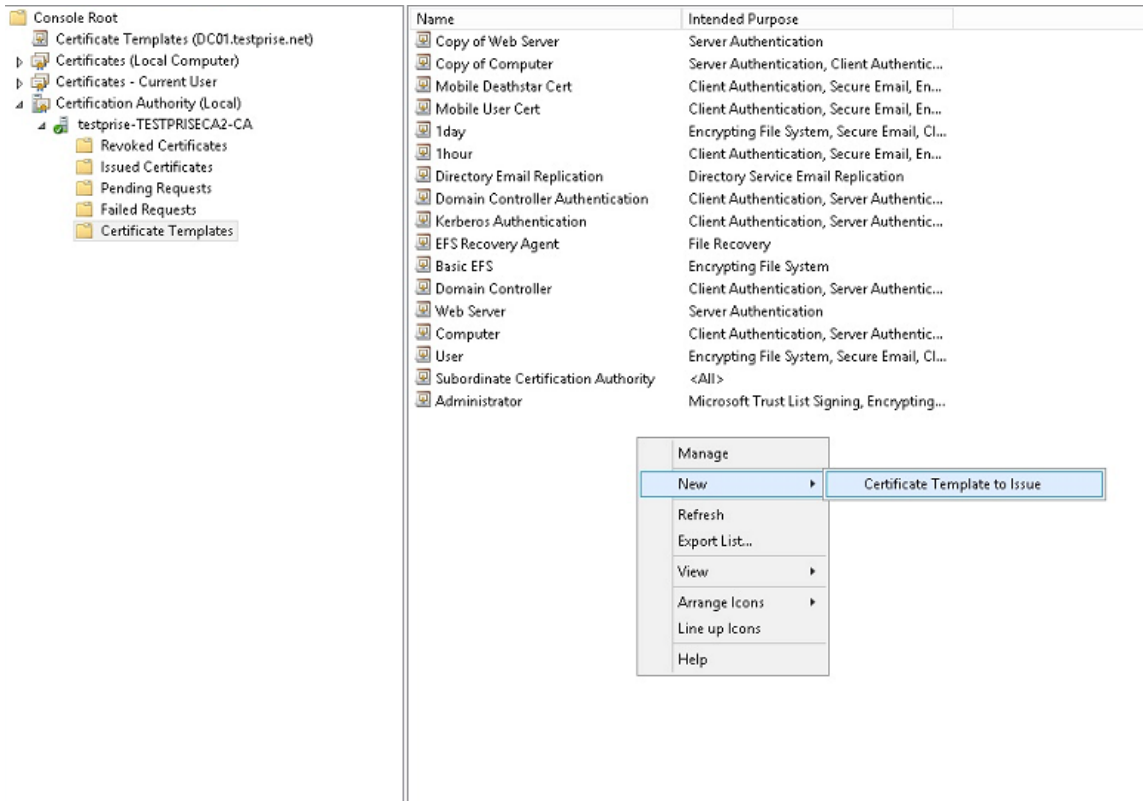
9. 주체이름아래에서 요청에서제공을선택합니다. 변경내용을적용한후저장합니다.



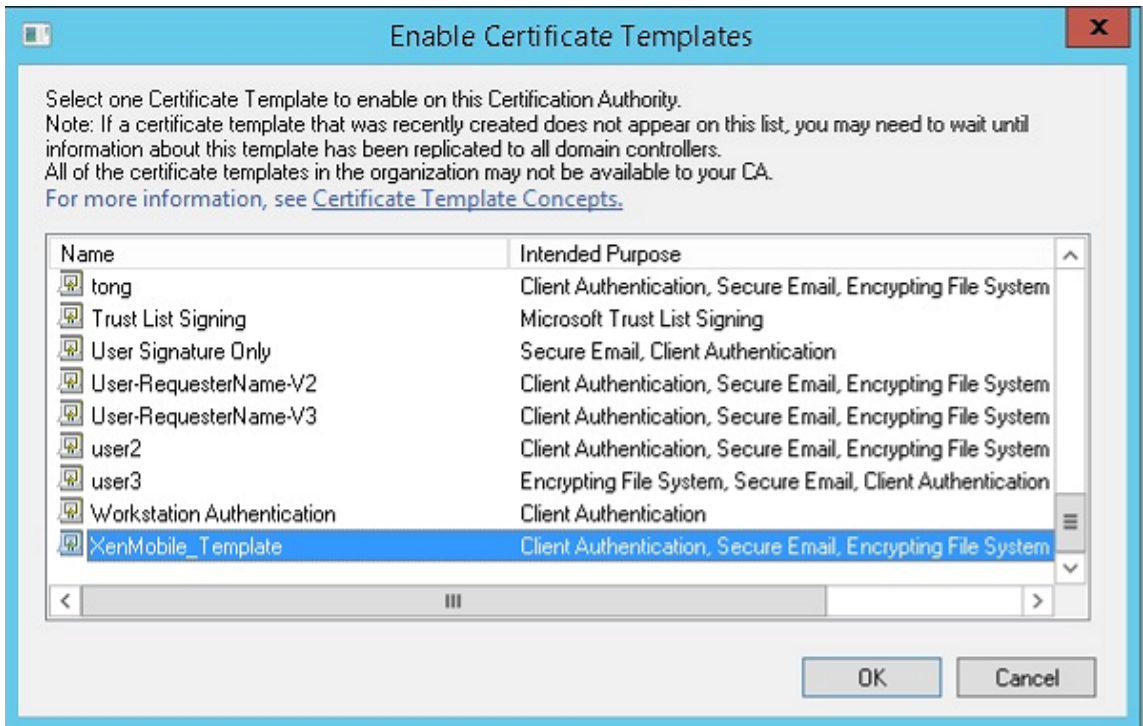
인증기관에템플릿추가

1. 인증기관으로이동하여 인증서템플릿을선택합니다.

2. 오른쪽창에서마우스오른쪽단추를클릭한후 새로만들기 > 발급할인증서템플릿을선택합니다.

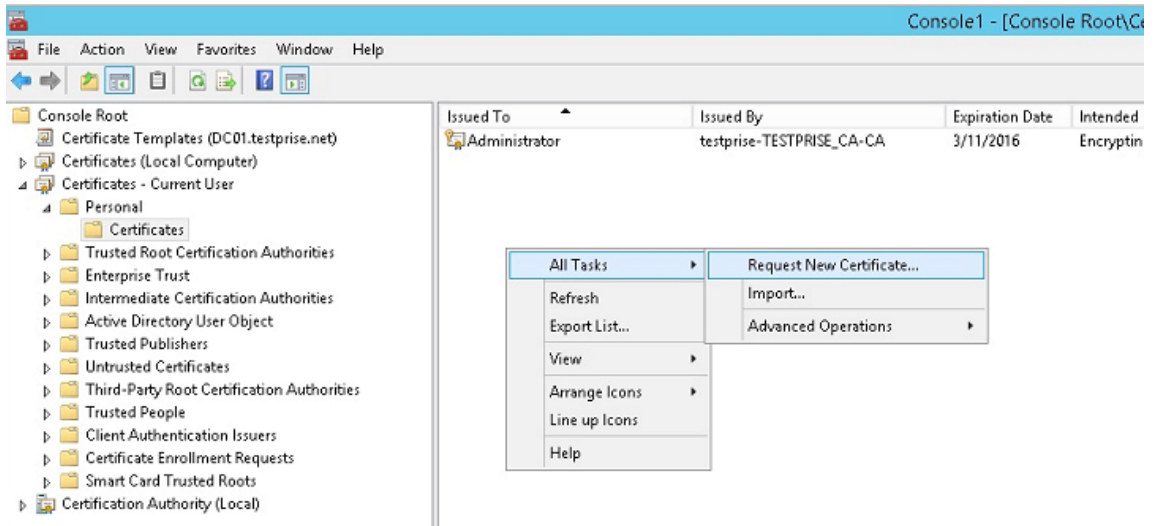


3. 이전단계에서만든템플릿을선택한다음 확인을클릭하여 인증기관에추가합니다.

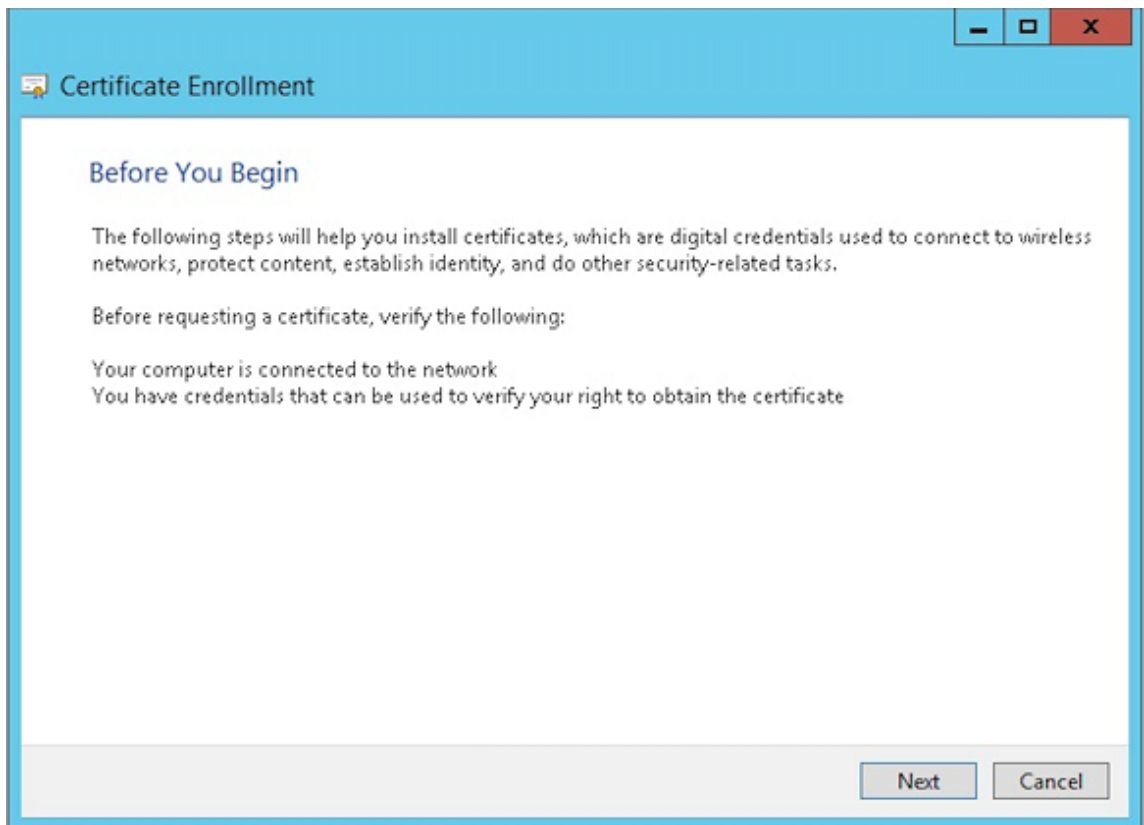


CA 서버에서 PFX 인증서만들기

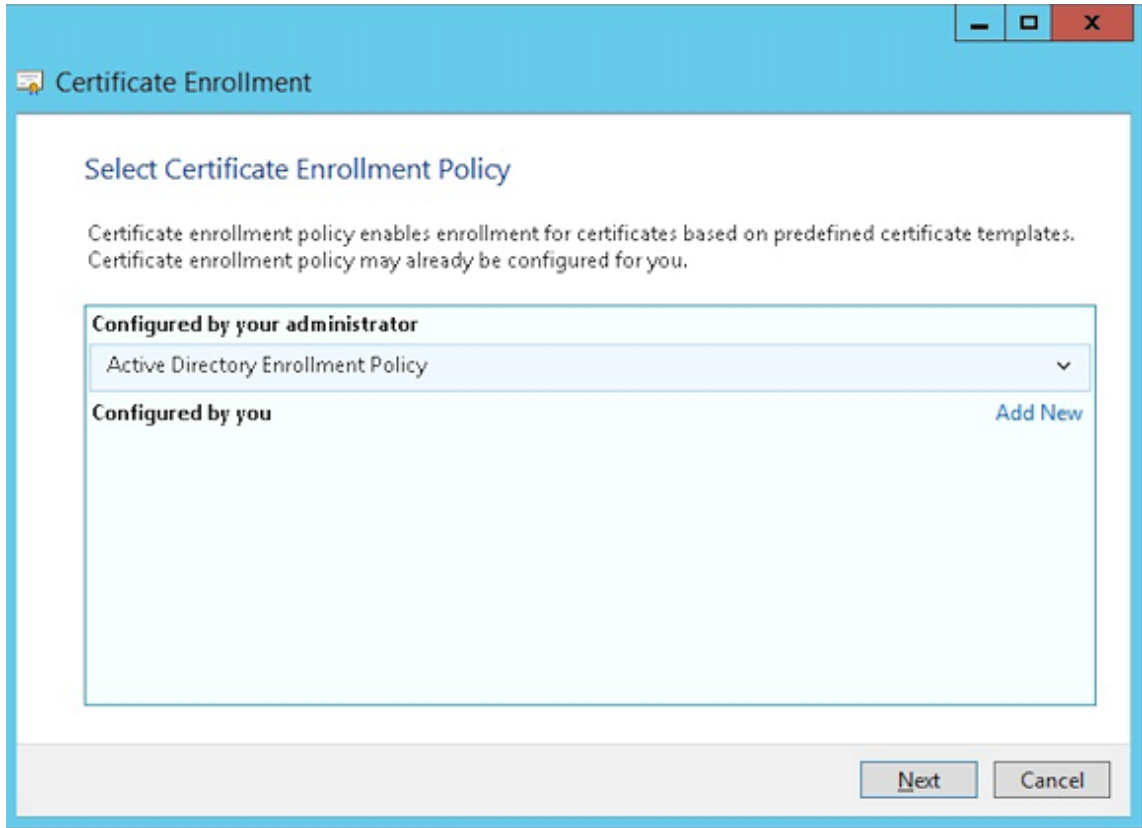
1. 로그인한서비스계정을사용하여사용자.pfx 인증서를만듭니다. .pfx 를 XenMobile 에업로드하면 XenMobile 이장치를등록하는사용자에대해서사용자인증서를요구하게됩니다.
2. 현재사용자아래에서 인증서를확장합니다.
3. 오른쪽창을마우스오른쪽단추로클릭하고 새인증서요청을클릭합니다.



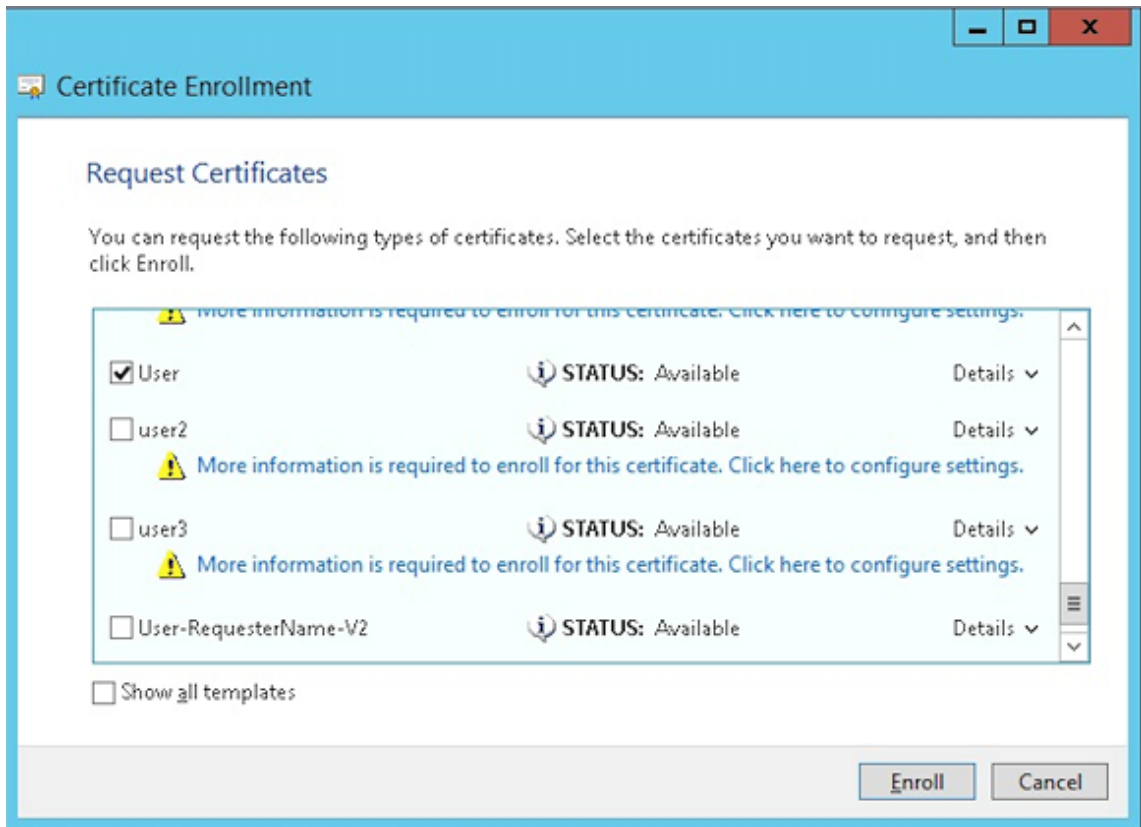
4. 인증서등록화면이나타납니다. 다음을클릭합니다.



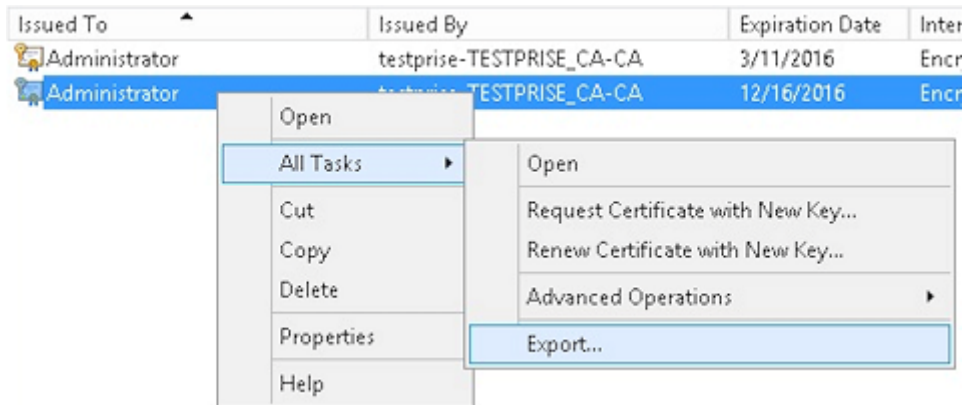
5. **Active Directory** 등록정책을선택하고 다음을클릭합니다.



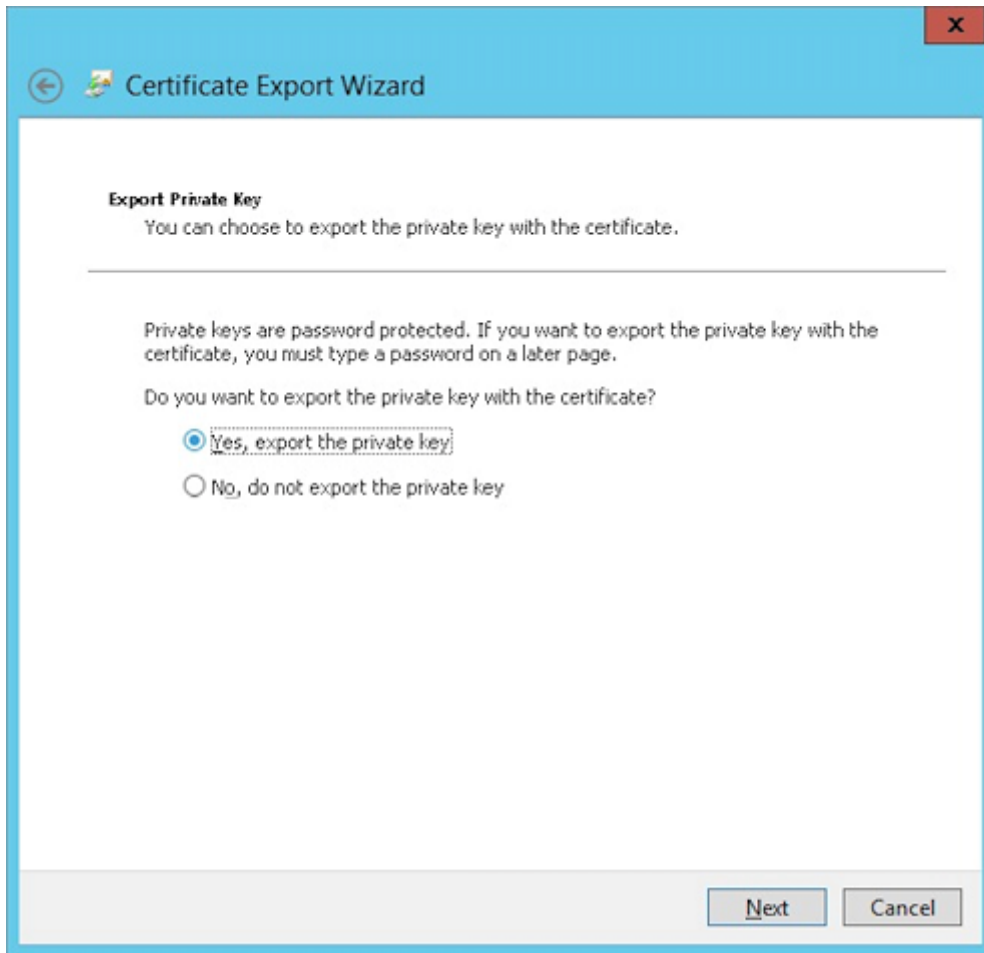
6. 사용자템플릿을선택한후 등록을클릭합니다.



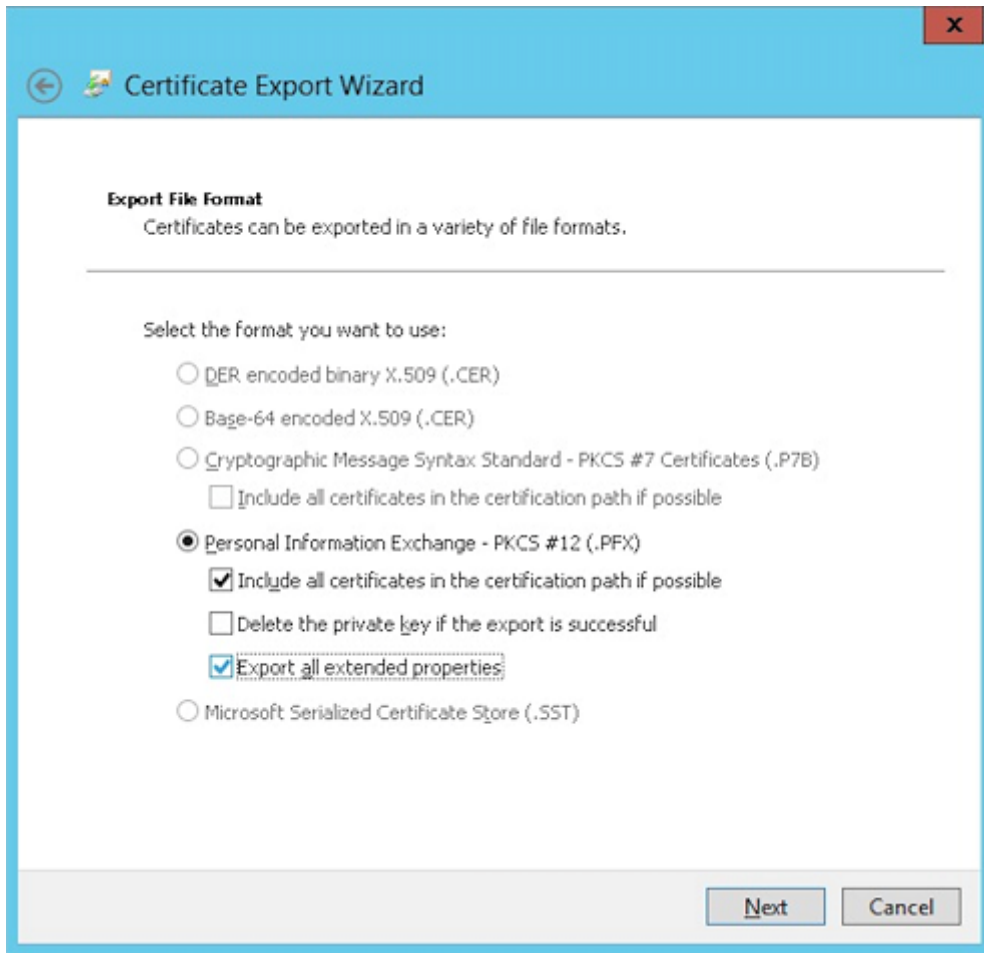
7. 이전단계에서만든.pfx 파일을내보냅니다.



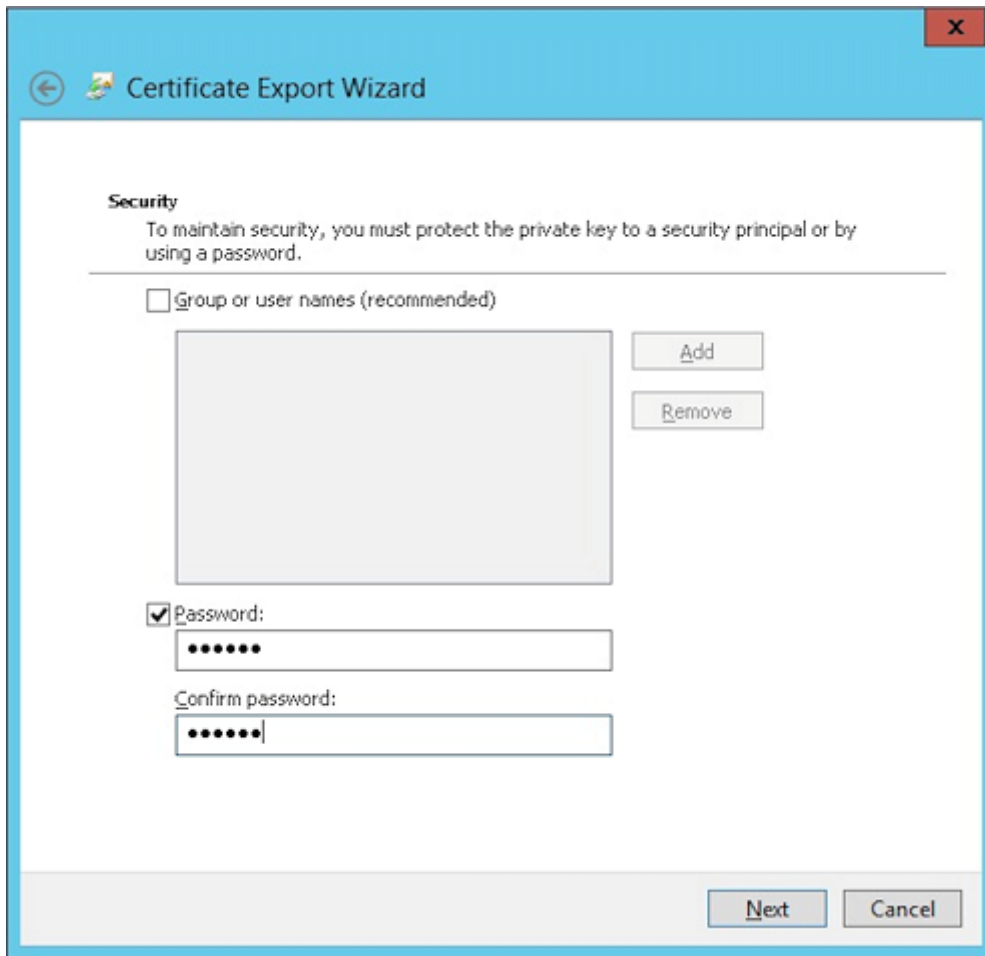
8. 예, 개인키를내보냅니다를클릭합니다.



9. 가능하면인증경로에있는인증서모두포함및 확장속성모두내보내기확인란을선택합니다.



10. XenMobile 에이전트를 업로드할 때 사용할 암호를 설정합니다.



11. 하드드라이브에인증서를저장합니다.

XenMobile 에인증서업로드

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정화면이나타납니다.
2. 인증서를클릭한후 가져오기를클릭합니다.
3. 다음매개변수를입력합니다.
 - 가져오기: 키저장소
 - 키저장소유형: PKCS #12
 - 용도: 서버
 - 키저장소파일: 찾아보기를클릭하여방금만든.pfx 인증서를선택합니다.
 - 암호: 이인증서에대해만든암호를입력합니다.

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import ▼
Keystore

Keystore type ▼
PKCS#12

Use as ▼
Server

Keystore file* Browse

Password*

Description

Cancel
Import

4. 가져오기를 클릭합니다.
5. 인증서가 올바르게 설치되었는지 확인합니다. 올바르게 설치된 인증서가 사용자 인증서로 표시됩니다.

인증서 기반 인증을 위한 PKI 엔터티 만들기

1. 설정에서 자세히 > 인증서 관리 > PKI 엔터티로 이동합니다.
2. 추가를 클릭한 후 **Microsoft** 인증서 서비스 엔터티를 클릭합니다. **Microsoft** 인증서 서비스 엔터티: 일반 정보 화면이나 타납니다.
3. 다음 매개변수를 입력합니다.
 - 이름: 원하는 이름을 입력합니다.
 - 웹 등록 서비스 루트 URL: <https://RootCA-URL/certsrv/> URL 경로에서 마지막 슬래시 (/) 를 반드시 추가해야 합니다.
 - **certnew.cer** 페이지 이름: certnew.cer (기본값)
 - **certfnsh.asp**: certfnsh.asp (기본값)
 - 인증 유형: 클라이언트 인증서
 - **SSL** 클라이언트 인증서: XenMobile 클라이언트 인증서를 발급하는 데 사용할 사용자 인증서를 선택합니다.

4. 템플릿아래에서 Microsoft 인증서를구성할때만든템플릿을추가합니다. 공백을추가하지마십시오.

5. HTTP 매개변수를생략하고 **CA** 인증서를클릭합니다.

6. 사용자환경에해당하는루트 CA 이름을선택합니다. 이루트 CA 는 XenMobile 클라이언트인증서에서가져온체인의일부입니다.

7. 저장을클릭합니다.

자격증명공급자구성

1. 설정에서 자세히 > 인증서관리 > 자격증명공급자로이동합니다.
2. 추가를클릭합니다.
3. 일반아래에서다음매개변수를입력합니다.
 - 이름: 원하는이름을입력합니다.
 - 설명: 원하는설명을입력합니다.
 - 발급엔터티: 이전에만든 PKI 엔터티를선택합니다.
 - 발급방법: 서명
 - 템플릿: PKI 엔터티아래에서추가한템플릿을선택합니다.

Credential Providers	Credential Providers: General Information
1 General	<p>You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for this certificate renewal or revocation, if any.</p> <p>Name* XenMobile_PKI</p> <p>Description XenMobile PKI Configuration</p> <p>Issuing entity MS PKI</p> <p>Issuing method SIGN</p> <p>Templates XMTemplate</p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	
5 Revocation PKI	
6 Renewal	

4. CSR 을클릭한후다음매개변수를입력합니다.

- 키알고리즘: RSA
- 키크기: 2048
- 서명알고리즘: SHA1withRSA
- 주체이름 `cn=$user.username`

주체대체이름에대해 추가를클릭한후다음매개변수를입력합니다.

- 유형: 사용자계정이름
- 값: `$user.userprincipalname`

Credential Providers	Credential Providers: Certificate Signing Request						
1 General	<p>Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.</p> <p>Key algorithm RSA</p> <p>Key size* 2048</p> <p>Signature algorithm SHA1withRSA</p> <p>Subject name* cn=\$user.username</p> <p>Subject alternative names</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Value*</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>User Principal name</td> <td>\$user.userprincipalname</td> <td></td> </tr> </tbody> </table>	Type	Value*	Add	User Principal name	\$user.userprincipalname	
Type		Value*	Add				
User Principal name		\$user.userprincipalname					
2 Certificate Signing Request							
3 Distribution							
4 Revocation XenMobile							
5 Revocation PKI							
6 Renewal							

5. 배포를클릭한후다음매개변수를입력합니다.

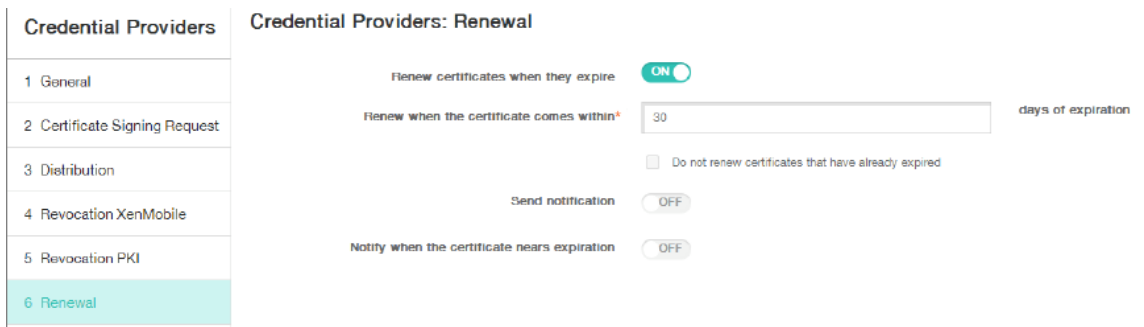
- CA 인증서발급: XenMobile 클라이언트인증서에서명한발급 CA 를선택합니다.
- 배포모드선택: 중앙집중식번호: 서버측키생성을선택합니다.

Credential Providers	Credential Providers: Distribution
1 General	<p>Issuing CA certificate CN-training-AD-CA, Serial: [dropdown]</p> <p>Select distribution mode</p> <p><input checked="" type="radio"/> Prefer centralized: Server-side key generation</p> <p><input type="radio"/> Prefer distributed: Device-side key generation</p> <p><input type="radio"/> Only distributed: Device-side key generation</p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	

6. 그다음의두섹션, 즉 해지 XenMobile 및 해지 PKI 에대해필요에따라매개변수를설정합니다. 이에에서는두옵션을모두 건너뛴니다.

7. 갱신을클릭합니다.

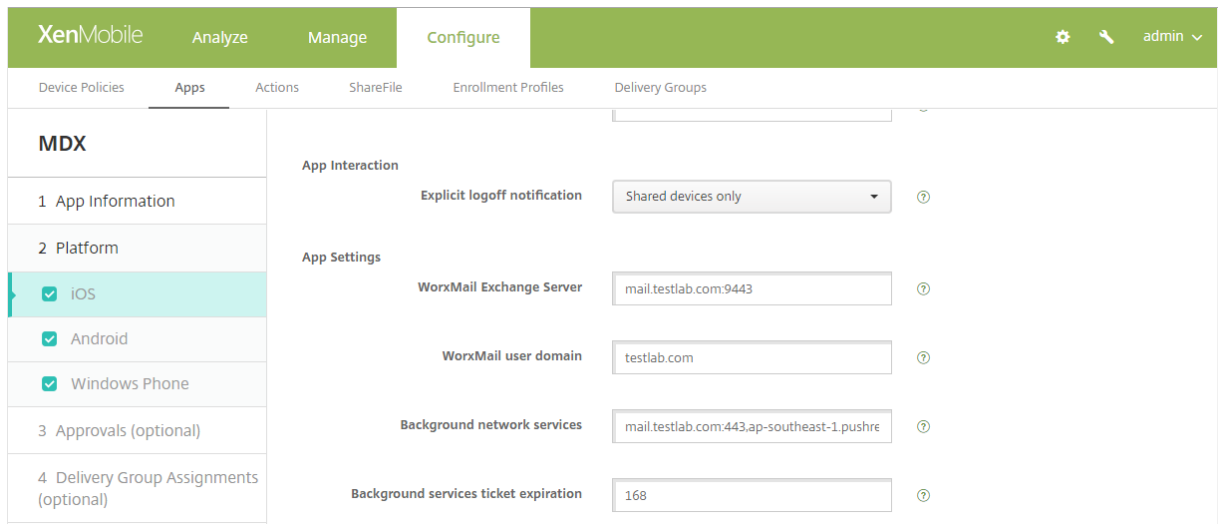
8. 인증서가만료될때갱신에대해 켜짐을선택합니다.
9. 다른모든설정을기본값으로그대로두거나필요에따라변경합니다.



10. 저장을클릭합니다.

인증서기반인증을사용하도록 **Secure Mail** 구성

Secure Mail 을 XenMobile 에추가할경우, 앱설정아래에서 Exchange 설정을구성해야합니다.



XenMobile 에서 **NetScaler** 인증서제공구성

1. XenMobile 콘솔에로그온하고오른쪽위모서리의기어아이콘을클릭합니다. 설정화면이나타납니다.
2. 서버아래에서 **NetScaler Gateway** 를클릭합니다.
3. NetScaler Gateway 가아직추가되지않은경우 추가를클릭하고설정을지정합니다.
 - 외부 **URL**: <https://YourNetScalerGatewayURL>
 - 로그인유형: 인증서및도메인
 - 암호필요: 꺼짐
 - 기본값으로설정: 켜짐

- 인증을위한사용자인증서제공에서 커짐을선택합니다.

Settings > NetScaler Gateway

NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication

Deliver user certificate for authentication ⓘ

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs
<input type="checkbox"/>					

- 자격증명공급자에서공급자를선택한다음 저장을클릭합니다.
- 사용자인증서에서 UPN(사용자계정이름) 대신 sAMAccount 특성을사용하려면 XenMobile 에서 LDAP 커넥터를다음과같이구성합니다. 설정 > **LDAP** 로이동한후디렉터리를선택하고 편집을클릭한다음 사용자검색기준에서 **sAMAccountName** 을선택합니다.

XenMobile Analyze Manage Configure admin

User base DN* ⓘ

Group base DN* ⓘ

User ID*

Password*

Domain alias*

XenMobile Lockout Limit ⓘ

XenMobile Lockout Time ⓘ

Global Catalog TCP Port ⓘ

Global Catalog Root Context ⓘ

User search by

Use secure connection

Citrix PIN 및 사용자 암호 캐싱 사용

Citrix PIN 및 사용자 암호 캐싱을 사용하도록 설정하려면 **설정 > 클라이언트 속성**으로 이동하여 **Enable Citrix PIN Authentication(Citrix PIN 인증 사용)** 및 **Enable User Password Caching(사용자 암호 캐싱 사용)** 확인란을 선택합니다. 자세한 내용은 [클라이언트 속성](#)에서 참조하십시오.

Windows Phone 대한 엔터프라이즈 허브 정책 만들기

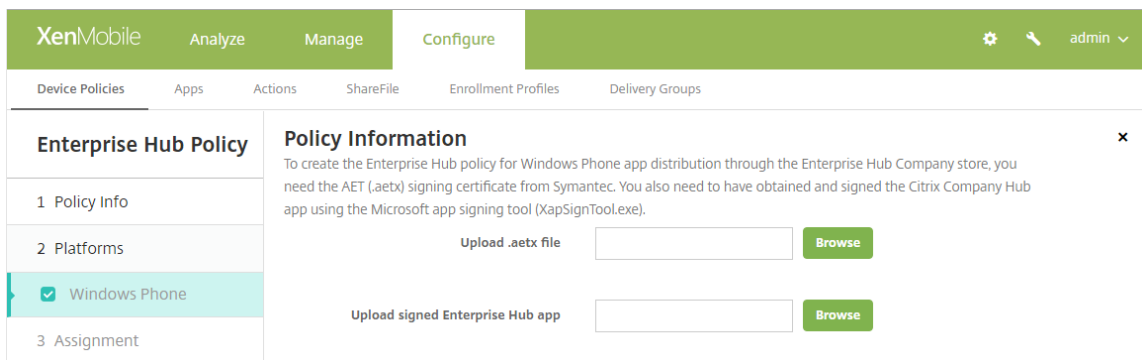
Windows Phone 장치에 대해 AETX 파일 및 Secure Hub 클라이언트를 제공하기 위한 엔터프라이즈 허브 장치 정책을 만들어야 합니다.

참고:

AETX 파일과 Secure Hub 파일이 다음을 사용하는지 확인합니다.

- 인증서 공급자의 동일한 엔터프라이즈 인증서.
- Windows 스토어 개발자 계정의 동일한 게시자 ID.

1. XenMobile 콘솔에서 **구성 > 장치 정책**을 클릭합니다.
2. 추가를 클릭한 후 자세히 **> XenMobile** 에이전트 아래에서 엔터프라이즈 허브를 클릭합니다.
3. 정책 이름을 지정 한 후 엔터프라이즈 허브에 대한 올바른 AETX 파일과 서명된 Secure Hub 앱을 선택해야 합니다.



4. 배달 그룹에 정책을 할당 한 후 저장합니다.

클라이언트 인증서 구성 문제 해결

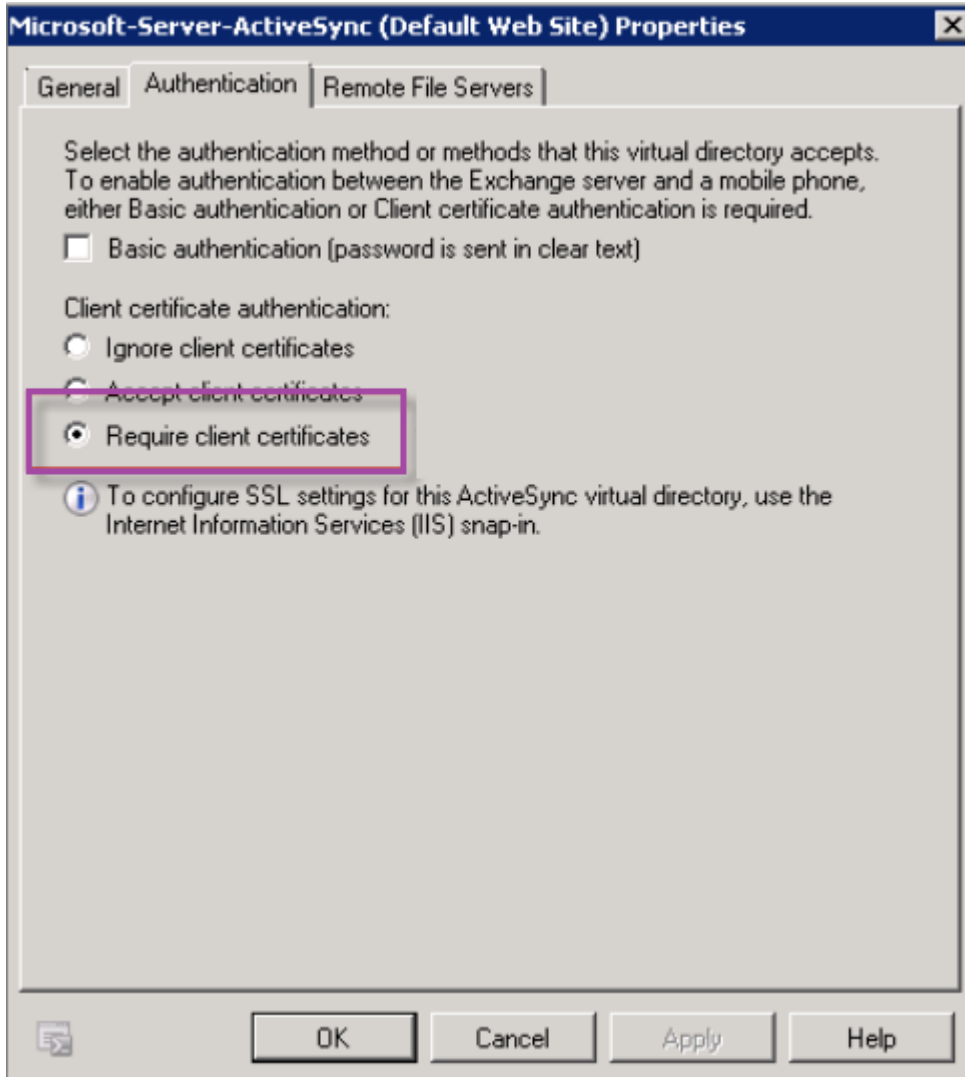
위의 구성과 NetScaler Gateway 구성을 성공적으로 완료 한 후 사용자 워크플로는 다음과 같습니다.

1. 사용자가 모바일 장치를 등록합니다.
2. XenMobile 에서 Citrix PIN 을 만들라는 메시지를 사용자에게 표시합니다.
3. 그런 다음 사용자가 XenMobile Store 로 리디렉션됩니다.
4. 사용자가 Secure Mail 을 시작할 때는 XenMobile 이 사서함 구성을 위한 사용자 자격 증명을 입력하라는 메시지를 표시하지 않습니다. 대신 Secure Mail 이 Secure Hub 에서 클라이언트 인증서를 요청하고 인증을 위해 Microsoft Exchange

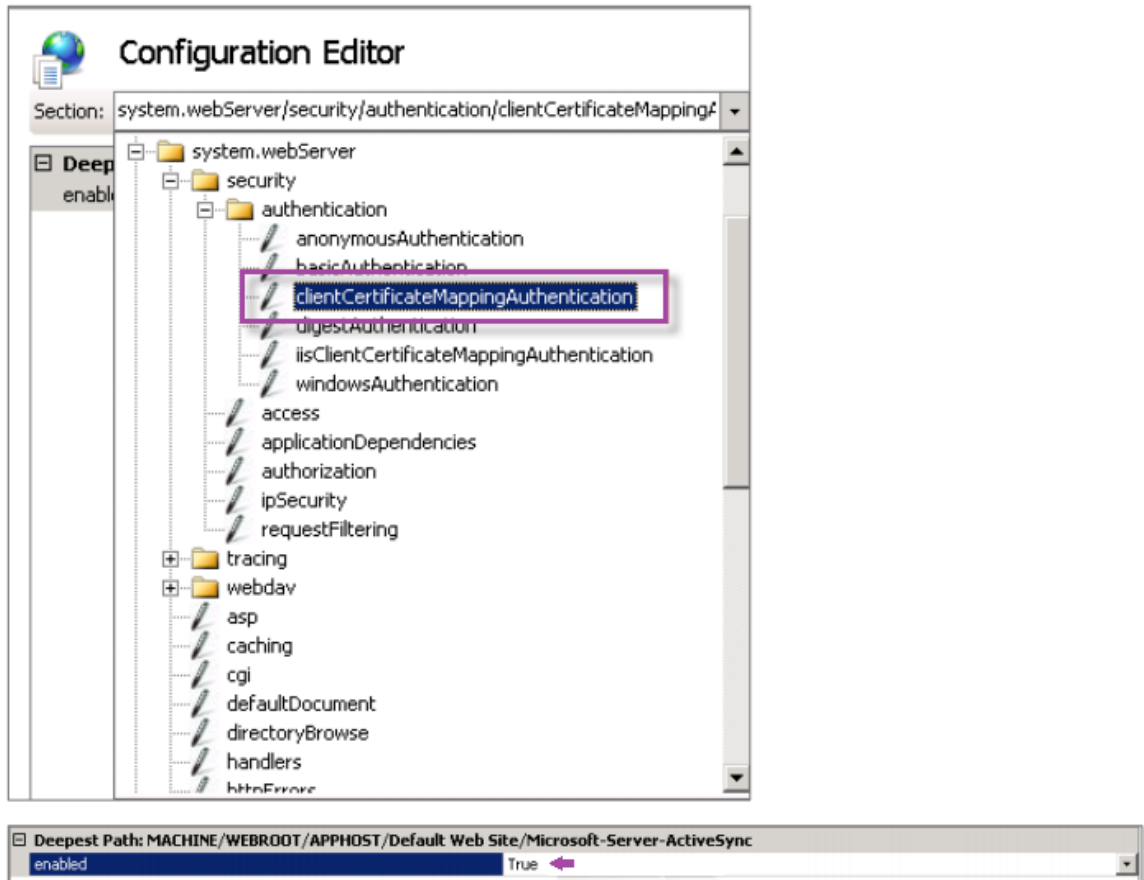
Server 에제출합니다. 사용자가 Secure Mail 을 시작할 때 자격 증명을 입력 하라는 메시지가 표시 될 경우 구성을 확인 하십시오.

사용자가 Secure Mail 을 다운로드 하고 설치 할 수 있지만 사서함 구성 중에 Secure Mail 이 구성을 완료 하지 못 할 경우:

1. Microsoft Exchange Server ActiveSync 에서 트래픽을 보안 하기 위해 개인 SSL 서버 인증서를 사용하는 경우, 모든 루트 및 중간 인증서가 모바일 장치에 설치 되어 있는지 확인 합니다.
2. ActiveSync 에 대해 선택 한 인증 유형이 클라이언트 인증서 필요 인지 확인 합니다.



3. Microsoft Exchange Server 에서 **Microsoft-Server-ActiveSync** 사이트를 확인 하여 클라이언트 인증서 매핑 인증이 사용하도록 설정 되어 있는지 검토 합니다. 기본적으로 클라이언트 인증서 매핑은 사용 되지 않습니다. 이 옵션은 구성편 집기 > 보안 > 인증 아래에 있습니다.



True 를 선택한 후에 적용을 클릭해야 변경 내용이 적용됩니다.

4. XenMobile 콘솔에서 NetScaler Gateway 설정을 확인합니다. 인증을 위한 사용자 인증서 제공이 켜짐이고 자격 증명 공급자에 올바른 프로필이 선택되어 있는지 확인합니다.

클라이언트 인증서가 모바일 장치에 제공되었는지 확인하려면

1. XenMobile 콘솔에서 관리 > 장치로 이동하여 장치를 선택합니다.
2. 편집 또는 자세한 표시를 클릭합니다.
3. 배달 그룹 섹션으로 이동하여 다음 항목을 검색합니다.

NetScaler Gateway Credentials: Requested credential, CertId=

클라이언트 인증서 협상을 사용하도록 설정했는지 확인하려면

1. 다음 `netsh` 명령을 실행하여 IIS 웹사이트에 바인딩된 SSL 인증서 구성을 표시합니다.

```
netsh http show sslcert
```

2. 클라이언트인증서협상의값이 사용안함인경우다음명령을실행하여사용하도록설정합니다.

```
netsh http delete sslcert iport=0.0.0.0:443
```

```
netsh http add sslcert iport=0.0.0.0:443 certhash=cert_hash appid={  
  app_id } certstorename=store_name verifyclientcertrevocation=Enable  
  VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
  clientcertnegotiation=Enable
```

예를들면다음과같습니다.

```
netsh http add sslcert iport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c54  
  appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam  
  verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly  
  =Disable UsageCheck=Enable clientcertnegotiation=Enable
```

XenMobile 을통해 Windows Phone 8.1 장치에루트/중간인증서를제공할수없는경우:

- 루트/중간인증서 (.cer) 파일을전자메일을통해 Windows Phone 8.1 장치로보낸다음직접설치합니다.

Windows Phone 8.1 에서 Secure Mail 이성공적으로설치되지않는경우다음을확인합니다.

- 응용프로그램등록토큰 (.AETX 파일) 이엔터프라이즈허브장치정책을사용하여 XenMobile 를통해제공됩니다.
- Secure Mail 을래핑하고 Secure Hub 앱을서명하는데사용된인증서공급자의엔터프라이즈인증서를동일하게사용하여응용프로그램등록토큰이만들어졌습니다.
- Secure Hub, Secure Mail, 응용프로그램등록토큰을서명하고래핑하는데동일한게시자 ID 가사용되었습니다.

PKI 엔터티

January 6, 2020

XenMobile PKI(공개키인프라) 엔터티구성은실제 PKI 작업 (발급, 해지및상태정보) 을수행하는구성요소를나타냅니다. 이러한구성요소는 XenMobile 의내부또는외부구성요소입니다. 내부구성요소는임의구성요소라고합니다. 외부구성요소는기업인프라의일부입니다.

XenMobile 은다음과같은 PKI 엔터티유형을지원합니다.

- GPKI(제네릭 PKI)
XenMobile Server GPKI 지원에는 DigiCert 관리 PKI 가포함됩니다.
- Microsoft 인증서서비스
- 임의의 CA(인증기관)

XenMobile 은다음과같은 CA 서버를지원합니다.

- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2

일반적인 PKI 개념

유형에 관계없이 모든 PKI 엔터티는 다음과 같은 하위 집합의 기능을 갖습니다.

- 서명: CSR(인증서 서명 요청) 을 기반으로 새 인증서 발급
- 가져오기: 기존 인증서 및 키 쌍 복구
- 해지: 클라이언트 인증서 해지

CA 인증서 정보

PKI 엔터티를 구성하는 경우 해당 엔터티에 의해 발급 (또는 복구) 되는 인증서의 서명자가 어느 CA 인증서인지를 XenMobile 에 알립니다. 이 PKI 엔터티는 개수 제한 없이 서로 다른 CA 가서명한 (가져오거나 새로 서명된) 인증서를 반환할 수도 있습니다.

PKI 엔터티 구성의 일환으로 이러한 각 CA 의 인증서를 제공합니다. 이를 위해 인증서를 XenMobile 에 업로드한 후 PKI 엔터티에서 참조해야 합니다. 임의 discretionary CA 의 경우 인증서는 묵시적으로서명 CA 인증서이지만 외부 엔터티의 경우 인증서를 수동으로 지정해야 합니다.

중요:

Microsoft 인증서 서비스 엔터티 템플릿을 생성할 때 등록된 장치와 관련된 인증 문제를 방지하려면 특수 문자를 템플릿 이름에서 사용하지 마십시오. 예를 들어 다음을 사용하지 마십시오. ! : \$ () ## % + * ~ ? | { } []

제네릭 PKI

GPKI(제네릭 PKI) 프로토콜은 다양한 PKI 솔루션과의 일관된 인터페이스를 제공하기 위해 SOAP 웹 서비스 계층을 통해 실행되는 XenMobile 고유 프로토콜입니다. GPKI 프로토콜은 다음 세 가지 기본 PKI 작업을 정의합니다.

- 서명: 어댑터가 CSR 을 생성하고, 이를 PKI 에 전송하고, 새로 서명된 인증서를 반환할 수 있습니다.
- 가져오기: 어댑터가 입력 매개변수에 따라 PKI 에서 기존 인증서 및 키 쌍을 검색 (복구) 할 수 있습니다.
- 해지: 어댑터가 PKI 로 하여금 해당 인증서를 해지하도록 할 수 있습니다.

GPKI 프로토콜을 받는 측은 GPKI 어댑터입니다. 어댑터는 기본 작업을 해당 응용별 PKI 유형으로 변환합니다. 예를 들어 RSA 용 GPKI 어댑터와 Entrust 용 GPKI 어댑터가 있습니다.

GPKI 어댑터는 SOAP 웹 서비스 끝점이며, 자체 설명형 WSDL(Web Services Description Language) 을 게시합니다. GPKI PKI 엔터티를 만들어 URL 을 사용하거나 파일 자체를 업로드함으로써 XenMobile 에 WSDL 정의를 제공할 수 있습니다.

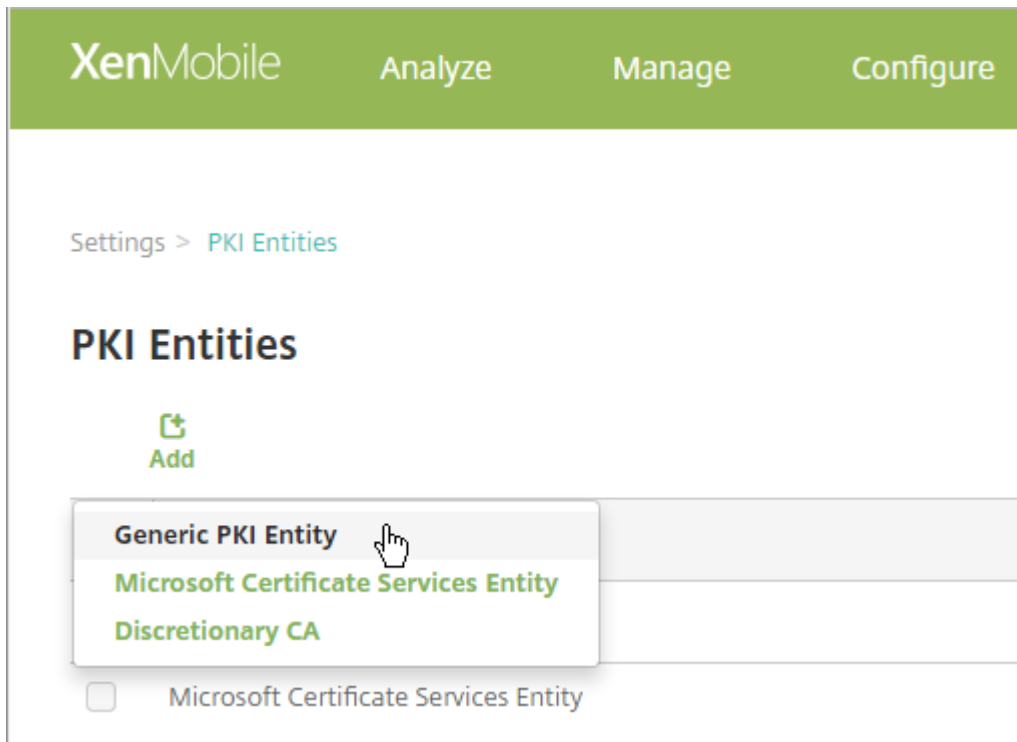
어댑터에서 각 PKI 작업에 대한 지원은 선택 사항입니다. 어댑터가 지정된 작업을 지원하는 경우 어댑터가 해당 기능 (서명, 가져오기 또는 해지) 을 갖는다고 합니다. 이러한 각 기능은 일련의 사용자 매개변수에 연결할 수 있습니다.

사용자매개변수는 특정작업을 위해 GPKI 어댑터에서 정의되었으며 XenMobile 에 해당값을 제공해야 하는 매개변수입니다. XenMobile 은 WSDL 파일을 구문 분석하여 어댑터가 지원하는 작업과 각 작업을 위해 어댑터에 필요한 매개변수를 결정합니다. 원할 경우 SSL 클라이언트 인증을 사용하여 XenMobile 과 GPKI 어댑터 간의 연결을 보호할 수 있습니다.

제네릭 PKI 를 추가하려면

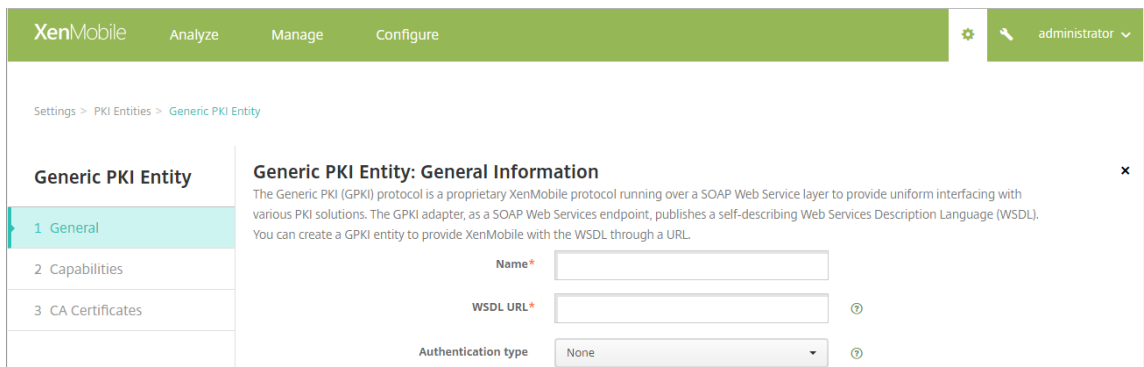
1. XenMobile 콘솔에서 설정 > PKI 엔터티를 클릭합니다.
2. PKI 엔터티 페이지에서 추가를 클릭합니다.

PKI 엔터티 유형에 대한 메뉴가 나타납니다.



3. 제네릭 PKI 엔터티를 클릭합니다.

제네릭 PKI 엔터티: 일반 정보 페이지가 나타납니다.



4. 제네릭 **PKI** 엔터티: 일반정보페이지에서다음을수행합니다.

- 이름: PKI 엔터티를설명하는이름을입력합니다.
- **WSDL URL**: 어댑터를설명하는 WSDL 의위치를입력합니다.
- 인증유형: 사용하려는인증방법을클릭합니다.
- 없음
- **HTTP 기본**: 어댑터에연결하는데필요한사용자이름및암호를입력합니다.
- 클라이언트인증서: 올바른 SSL 클라이언트인증서를선택합니다.

5. 다음을클릭합니다.

제네릭 PKI 엔터티: 어댑터기능페이지가나타납니다.

6. 제네릭 **PKI** 엔터티: 어댑터기능페이지에서어댑터와관련된기능과매개변수를검토하고 다음을클릭합니다.

제네릭 **PKI** 엔터티: **CA** 인증서발급페이지가나타납니다.

7. 제네릭 PKI 엔터티: CA 인증서발급페이지에서엔터티에사용할인증서를선택합니다.

엔터티에서서로다른 CA 가서명한인증서를반환하더라도주어진인증서공급자를통해얻은모든인증서는동일한 CA 가서명해야합니다. 따라서여기에서구성한인증서중하나를 자격증명공급자설정의 배포페이지에서선택해야합니다.

8. 저장을클릭합니다.

PKI 엔터티테이블에해당엔터티가나타납니다.

DigiCert 관리 PKI

XenMobile Server GPKI 지원에는 DigiCert 관리 PKI(MPKI 라고도함) 가포함됩니다. 이섹션에서는 DigiCert 관리 PKI 에대한 Windows Server 및 XenMobile Server 를설정하는방법을설명합니다.

사전요구사항

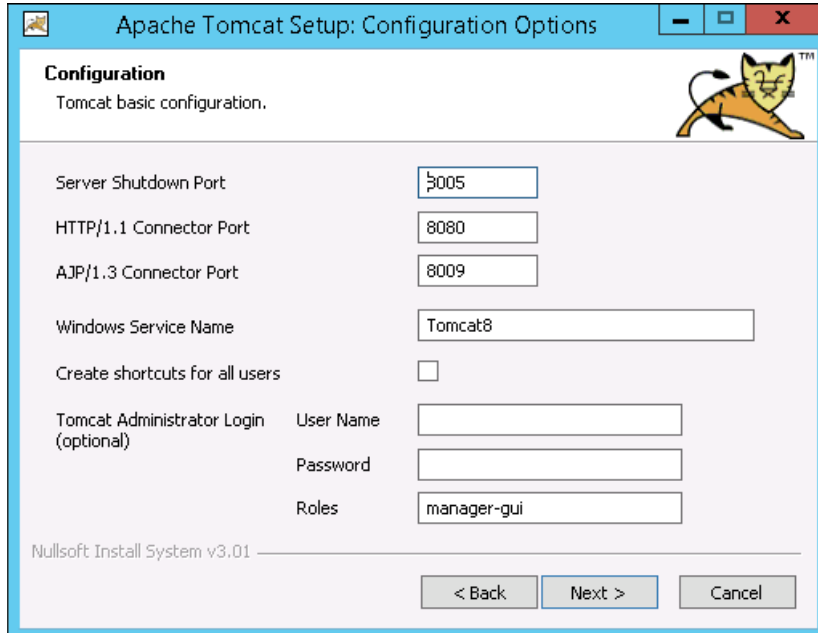
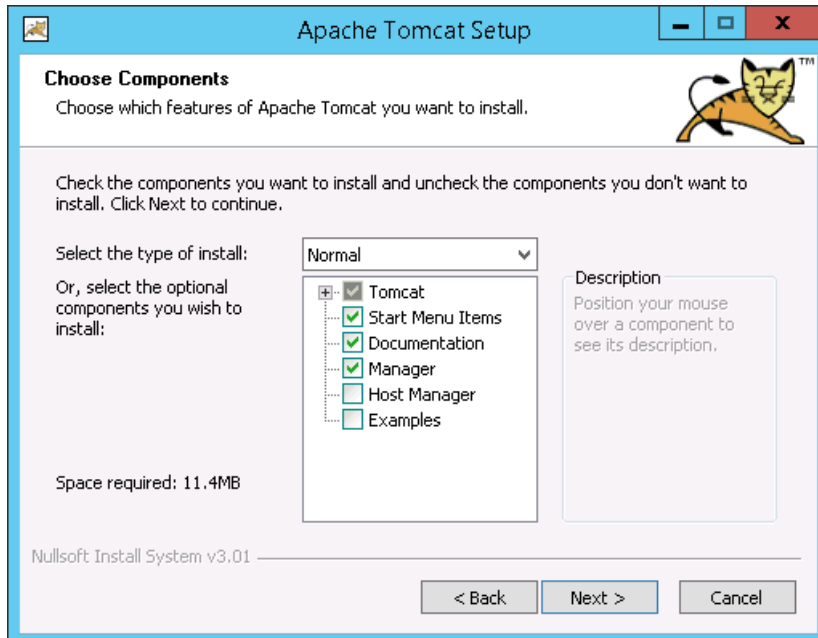
- DigiCert 관리 PKI 인프라에대한액세스권한
- 이문서에설명된대로다음구성요소가설치된 Windows Server 2012 R2 서버:
 - Java
 - Apache Tomcat
 - DigiCert PKI 클라이언트
 - Portecle
- XenMobile 다운로드사이트에대한액세스권한

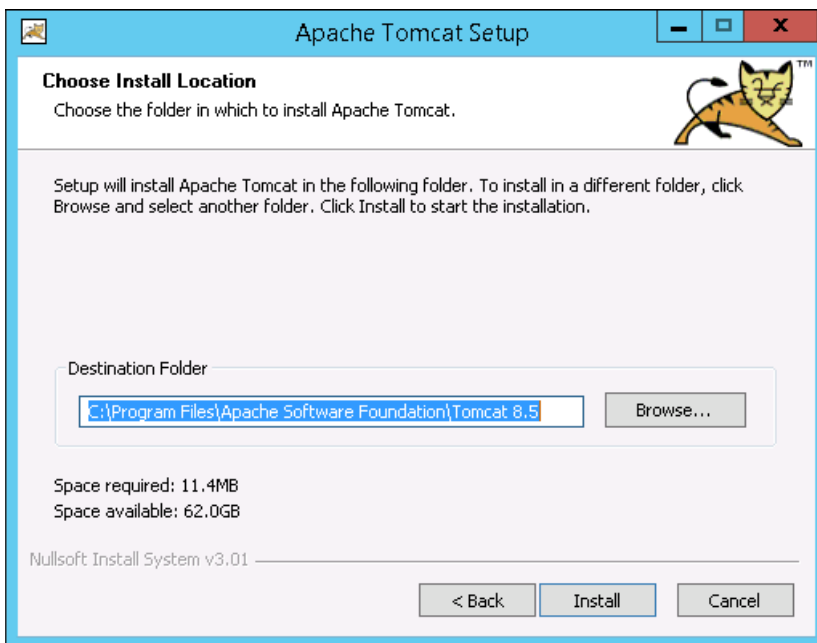
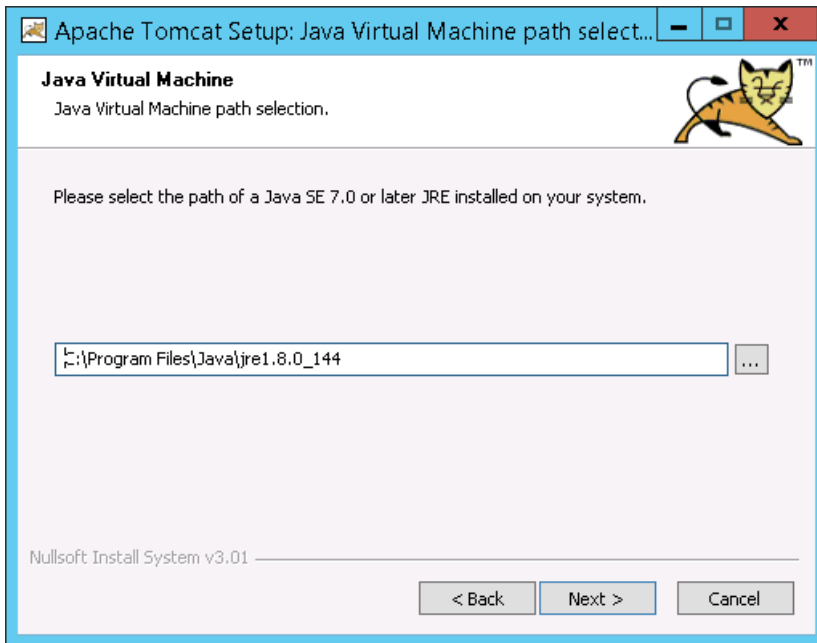
Windows Server 에 Java 설치

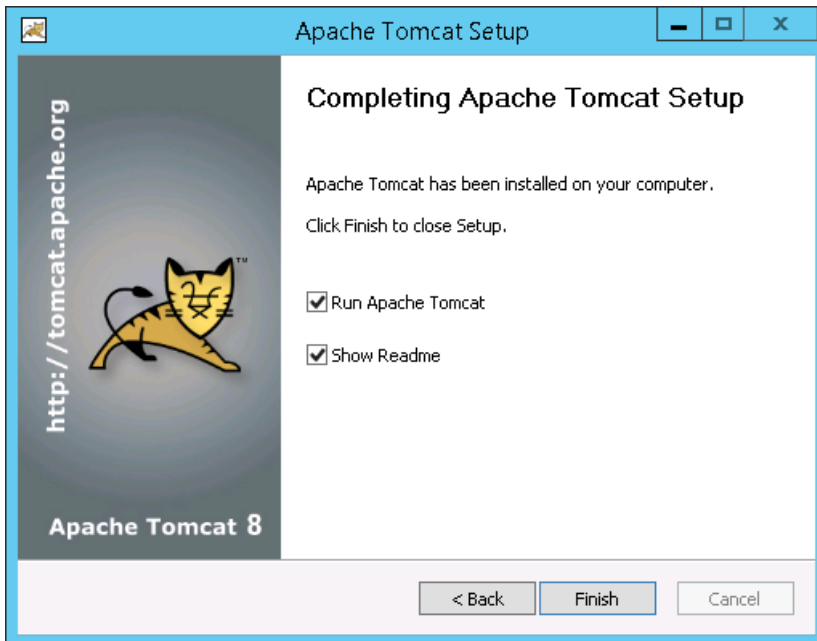
https://java.com/en/download/faq/java_win64bit.xml에서 Java 를다운로드한다음설치합니다. 보안경고대화상자에서 실행을클릭합니다.

Windows Server 에 Apache Tomcat 설치

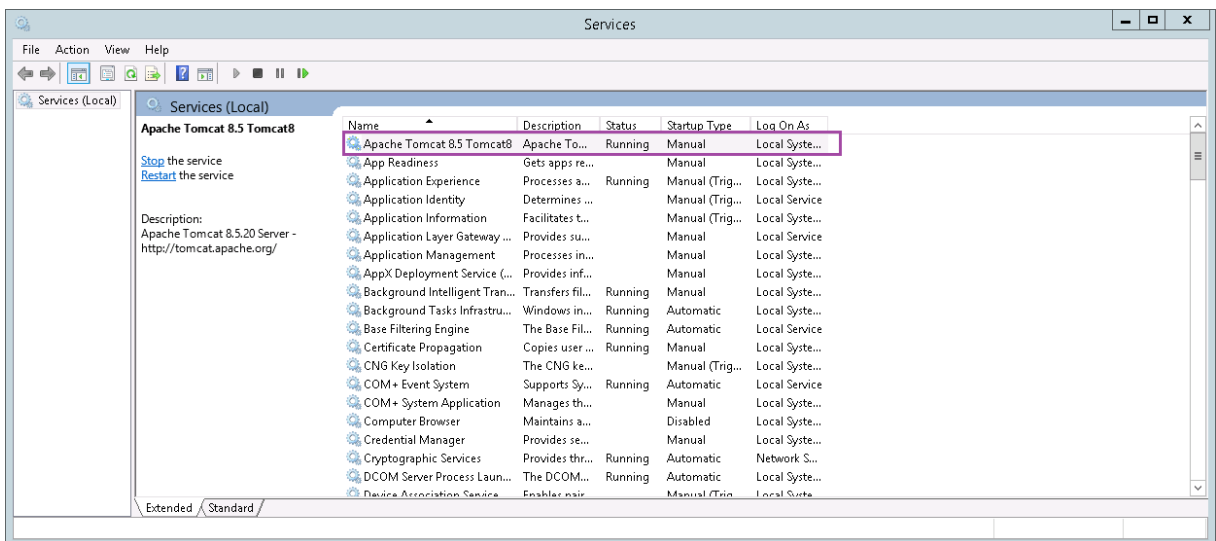
<https://tomcat.apache.org/download-80.cgi>에서 Apache Tomcat 32 비트/64 비트 Windows 서비스설치 프로그램을 다운로드하고 설치합니다. 보안 경고 대화상자에서 실행을 클릭합니다. 다음 예제를 가이드로 사용하여 Apache Tomcat 설정을 완료합니다.

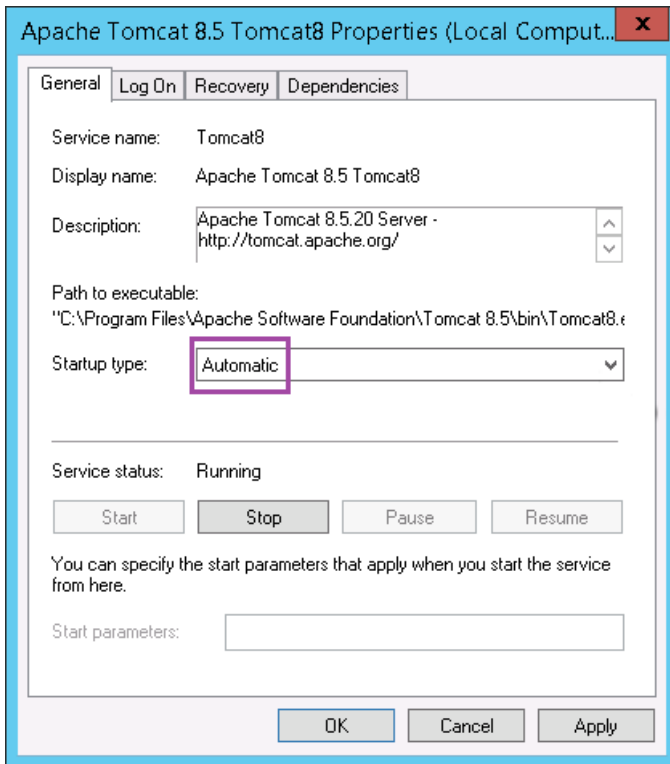






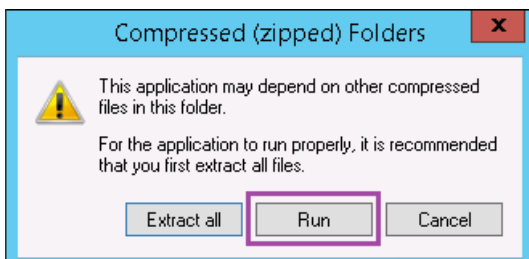
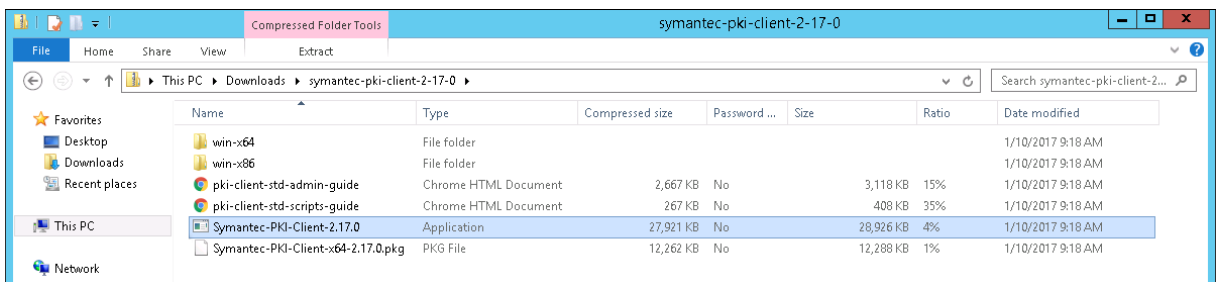
다음으로 Windows 서비스로 이동하고 시작유형을 수동에서 자동으로 변경합니다.





Windows Server 에 DigiCert PKI 클라이언트설치

PKI Manager 콘솔에서설치프로그램을다운로드합니다. 콘솔에엑세스할수없는경우 DigiCert 지원페이지의 [How to download DigiCert PKI Client\(DigiCert PKI 클라이언트다운로드방법\)](#)에서설치프로그램을다운로드합니다. 설치프로그램의압축을풀고실행합니다.



보안경고대화상자에서 실행을클릭해야합니다. 설치프로그램의지침에따라설치를완료합니다. 설치프로그램이완료되면다시시작하라는메시지가표시됩니다.

Windows Server 에 Portecle 설치

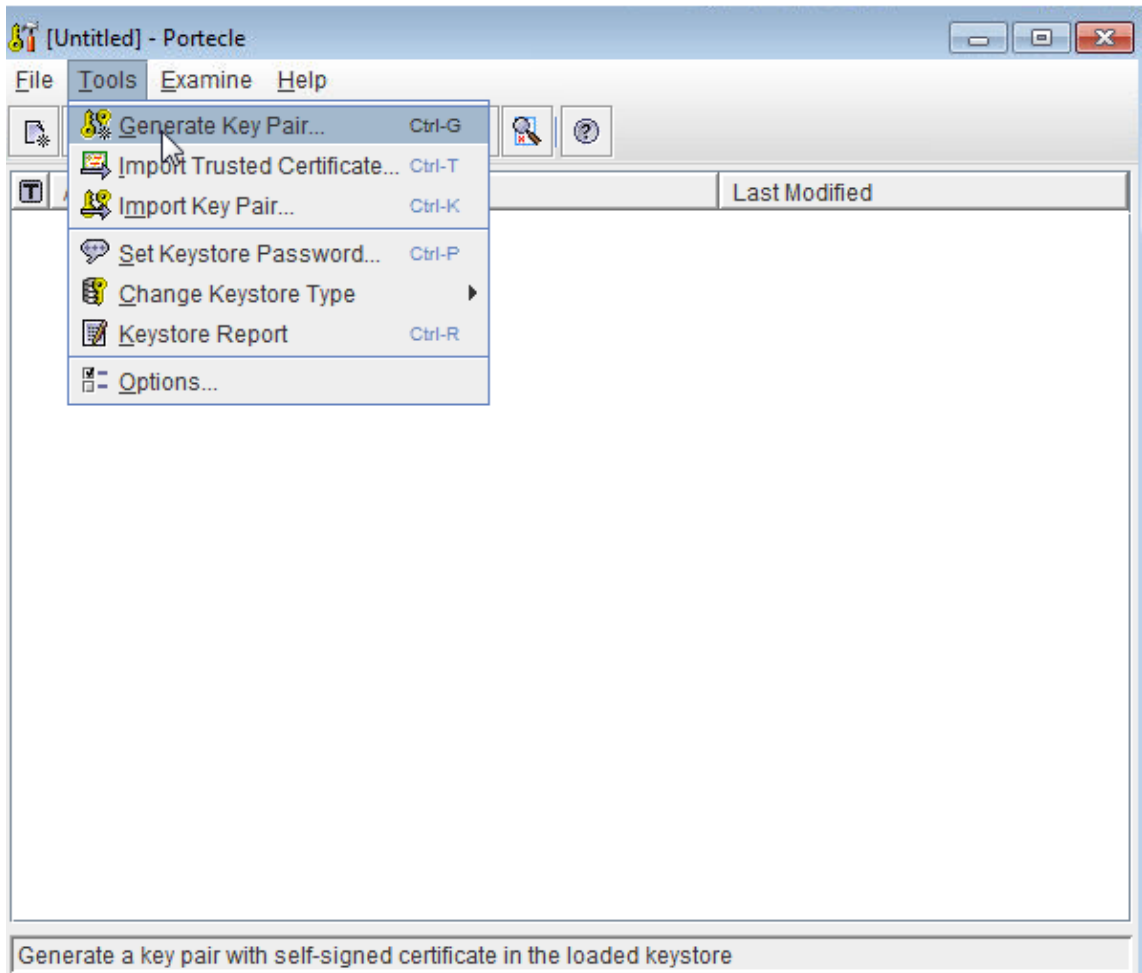
<https://sourceforge.net/projects/portecleinstall/files/>에서설치프로그램을다운로드한후압축을풀고실행합니다.

DigiCert 관리 PKI 에대한 RA(등록기관) 인증서생성

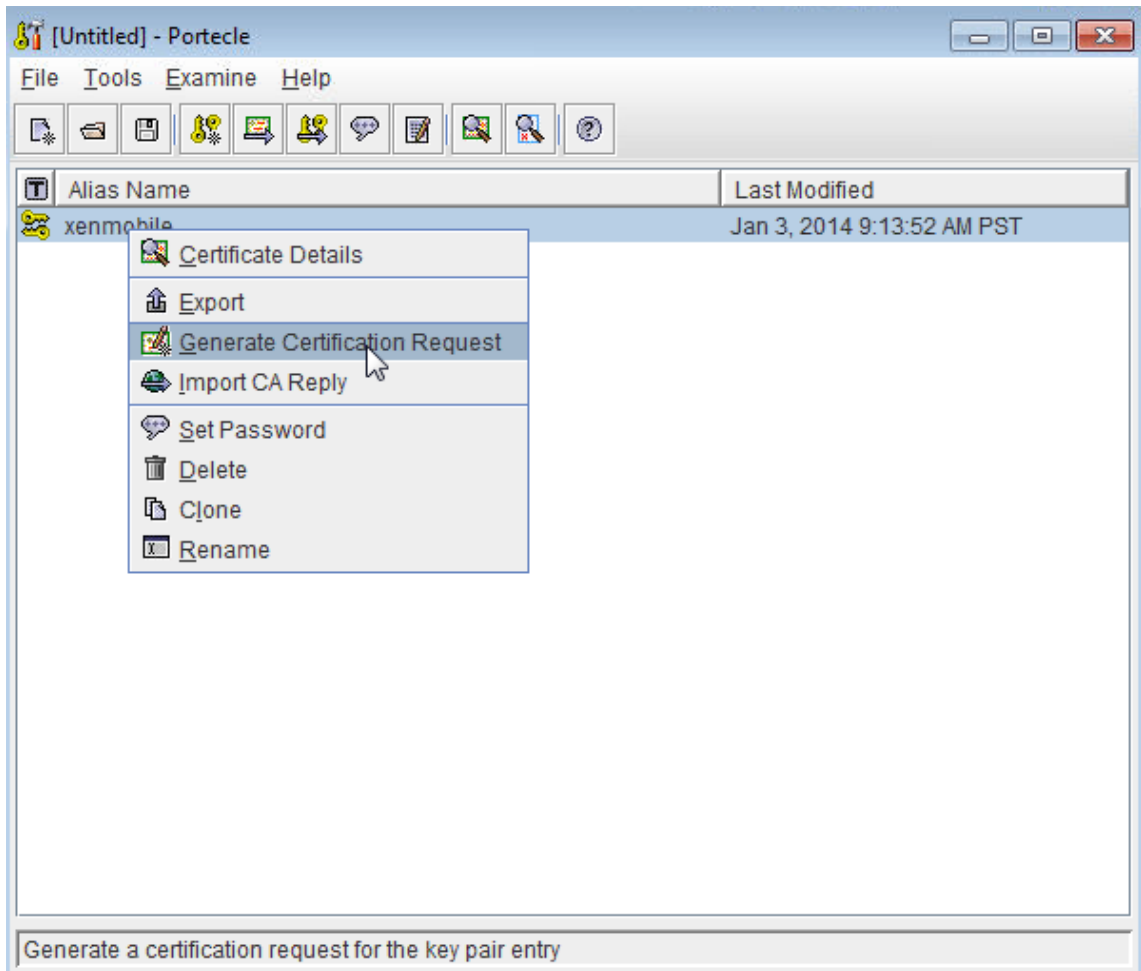
클라이언트인증서인증의키저장소는 RA.jks 라는 RA(등록기관) 인증서에포함되어있습니다. 다음단계에서는 Portecle 을사용하여이인증서를생성하는방법을설명합니다. Java CLI 를사용하여 RA 인증서를생성할수도있습니다.

또한이문서에서는 RA 인증서와공용인증서를업로드하는방법을설명합니다.

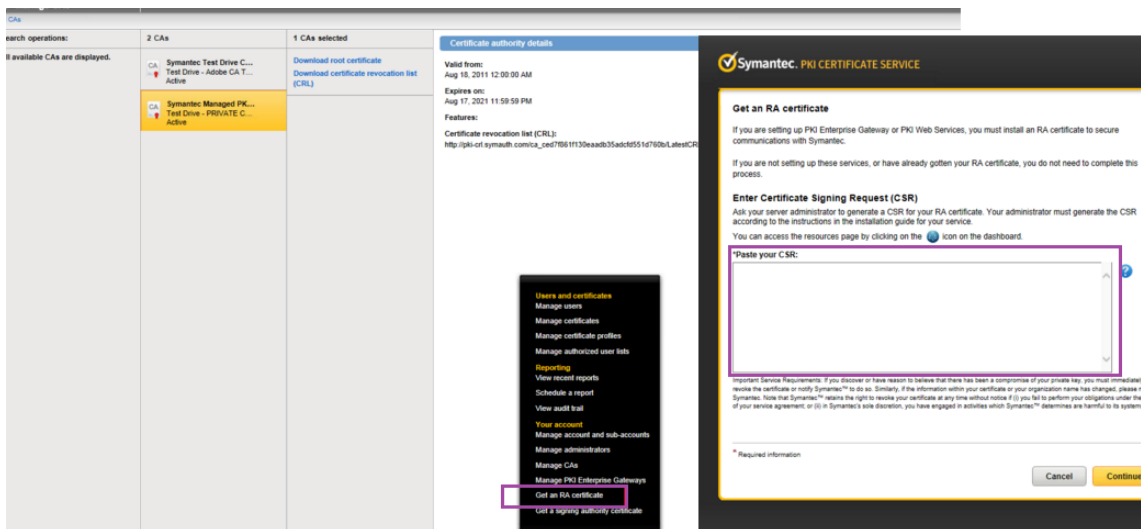
1. Portecle 에서 **Tools(도구) > Generate Key Pair(키쌍생성)** 로이동하여필요한정보를입력하고키쌍을생성합니다.



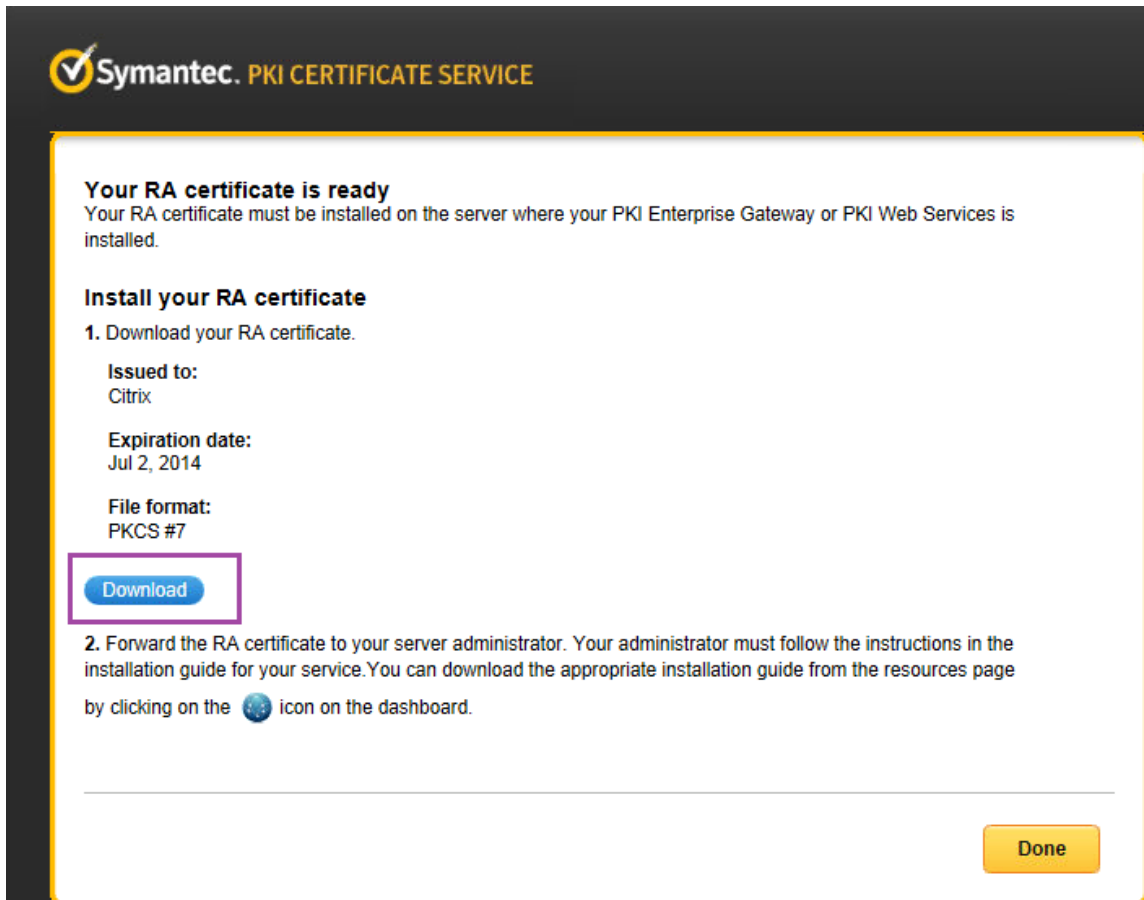
2. 키쌍을마우스오른쪽단추로클릭한후 **Generate Certification Request(인증서요청생성)** 를클릭합니다.



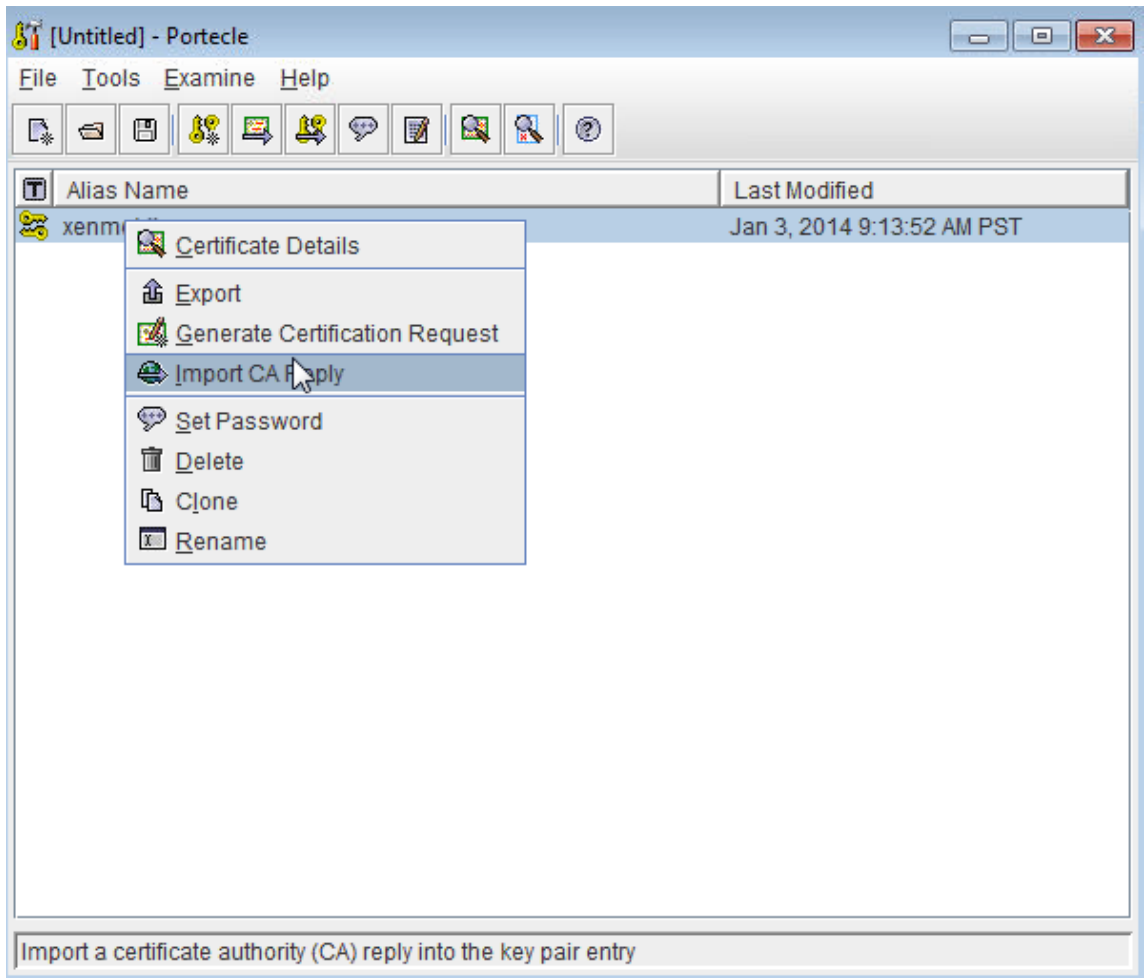
3. CSR 을복사합니다.
4. DigiCert PKI Manager 에서 RA 인증서를생성합니다. **Settings(설정)**, **Get a RA Certificate(RA 인증서가져 오기)** 를차례로클릭하고 CSR 을붙여넣은후 **Continue(계속)** 를클릭합니다.



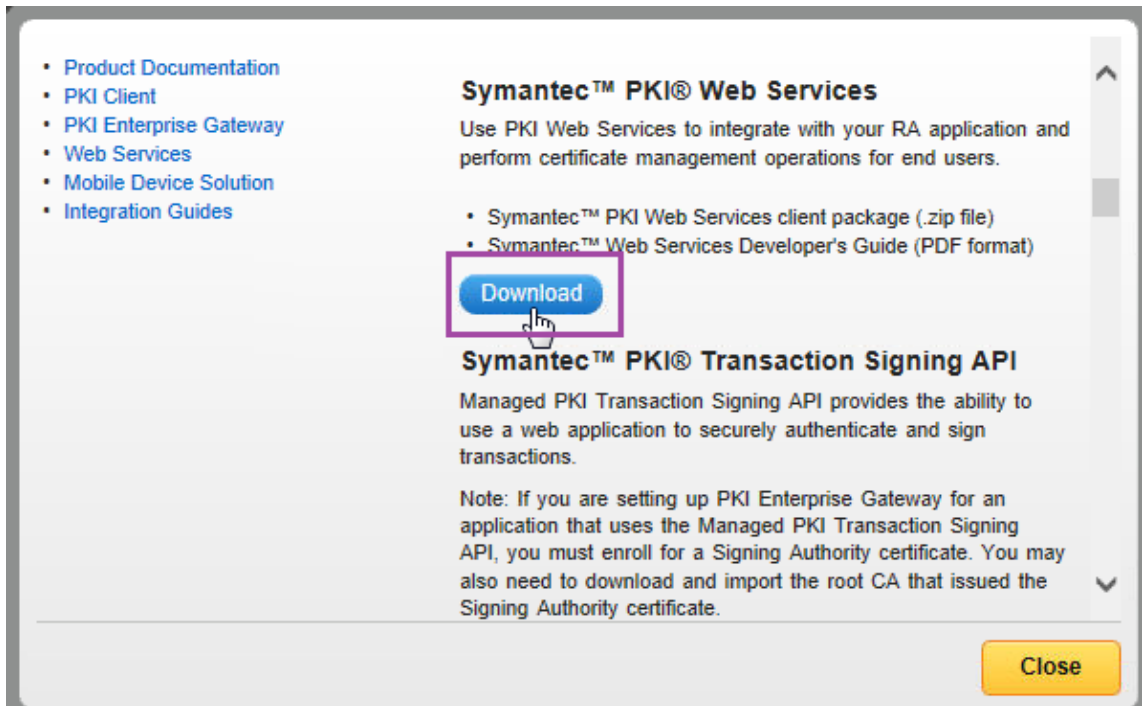
5. **Download(다운로드)** 를 클릭하여 생성된 RA 인증서를 다운로드합니다.



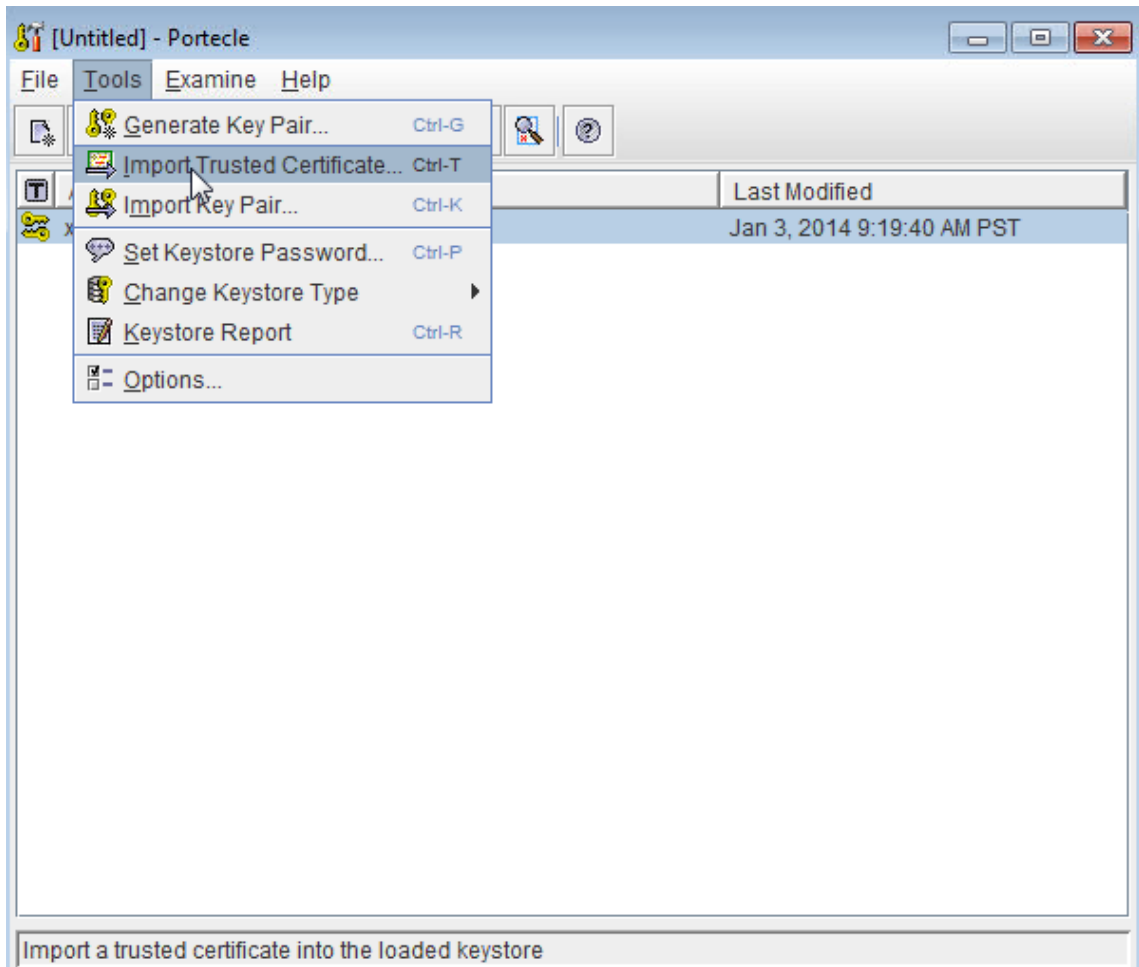
6. Portecle 에서 RA 인증서를 가져옵니다. 키쌍을 마우스 오른쪽 단추로 클릭하고 **Import CA Reply(CA 응답 가져오기)** 를 클릭합니다.



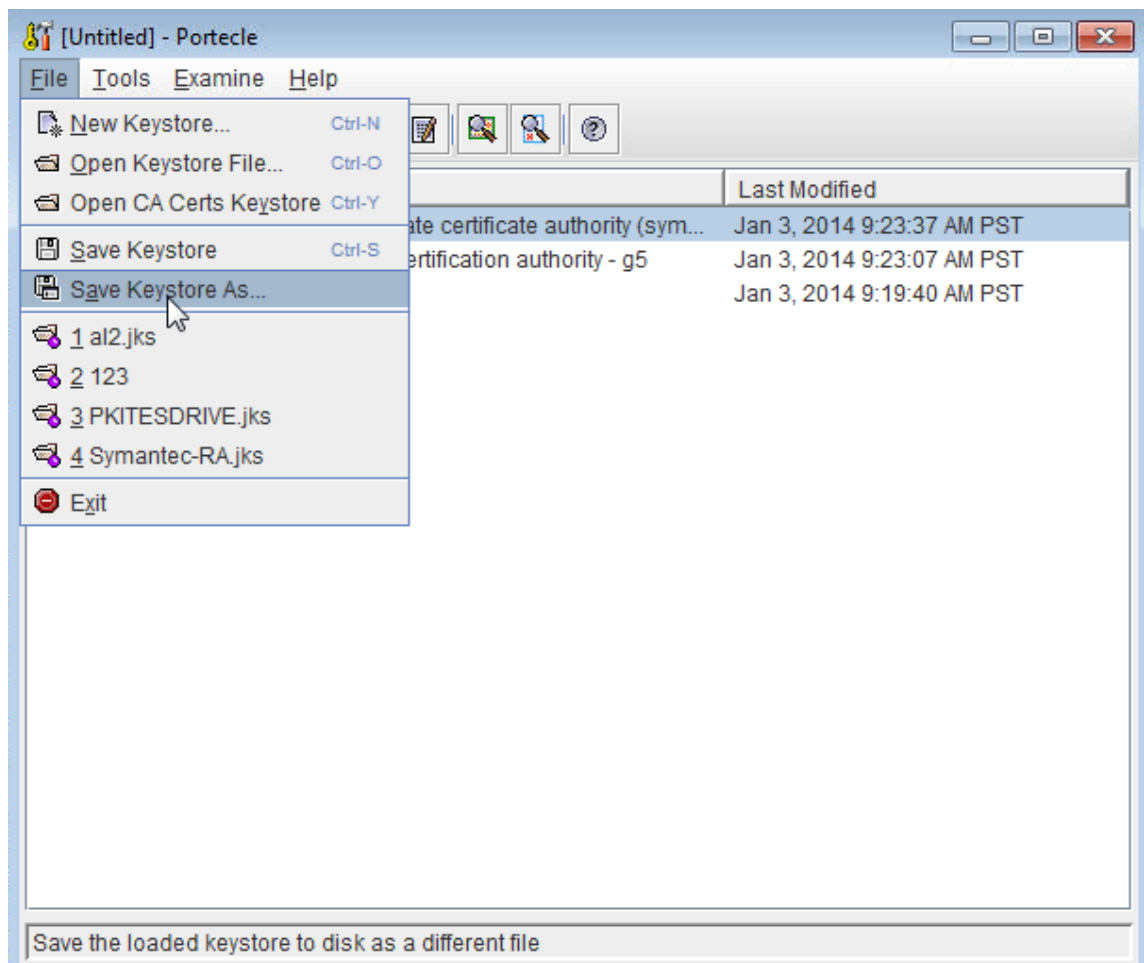
7. DigiCert PKI Manager 에서 **Resources(리소스) > Web Services(웹서비스)** 로 이동한후 CA 인증서를 다운로드합니다.



8. Portecle 에서 RA 중간인증서및루트인증서를키저장소로가져옵니다. **Tools(도구) > Import Trusted Certificates(신뢰할수있는인증서가져오기)** 로이동합니다.



9. CA 를 가져온후 Windows Server 의 C:\DigiCert 폴더에 RA.jks 로키저장소를저장합니다.



Windows Server 에서 DigiCert PKI 어댑터구성

1. Windows Server 에관리자로로그온합니다.
2. 이전섹션에서생성한 RA.jks 파일을업로드합니다. 또한 Symantec MPKI 서버에대한공용인증서 (cacerts.jks) 를업로드합니다.
3. [XenMobile Server 10 download\(XenMobile Server 10 다운로드\)](#) 페이지에서 **Tools(도구)** 를확장한후 Symantec PKI Adapter 파일을다운로드합니다. 파일이름은 XenMobile_Symantec_PKI_Adapter.zip 입니다. 파일의압축을풀고다음파일을 Windows Server C: 드라이브에복사합니다.
 - custom_gpki_adapter.properties
 - Symantec.war
4. custom_gpki_adapter.properties 를메모장에서열고다음값을편집합니다.

```

1 Gpki.CaSvc.Url=https://<managed PKI URL>
2
3 # keystore for client-cert auth

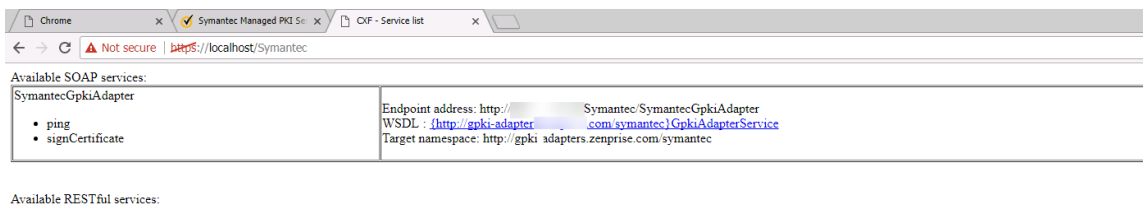
```

```
4
5 keyStore=C:\Symantec\RA.jks
6
7 # truststore for server with self-signed root CA
8
9 trustStore=C:\Symantec\cacerts.jks
```

5. Symantec.war 을 <tomcat dir>\webapps 폴더에 복사하고 Tomcat 을 시작합니다.
6. 응용 프로그램이 배포되었는지 확인합니다. 웹 브라우저를 열고 <https://localhost/Symantec> 으로 이동합니다.
7. <tomcat dir>\webapps\Symantec\WEB-INF\classes 폴더로 이동하고 gpki_adapter.properties 를 편집합니다. **CustomProperties** 속성을 C:\Symantec 폴더의 custom_gpki_adapter 파일을 가리키도록 편집합니다.

CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties

8. Tomcat 을 다시 시작하고 <https://localhost/Symantec> 으로 이동한 후 끝점 주소를 복사합니다. 다음 섹션에서 PKI 어댑터를 구성할 때 이 주소를 붙여 넣습니다.

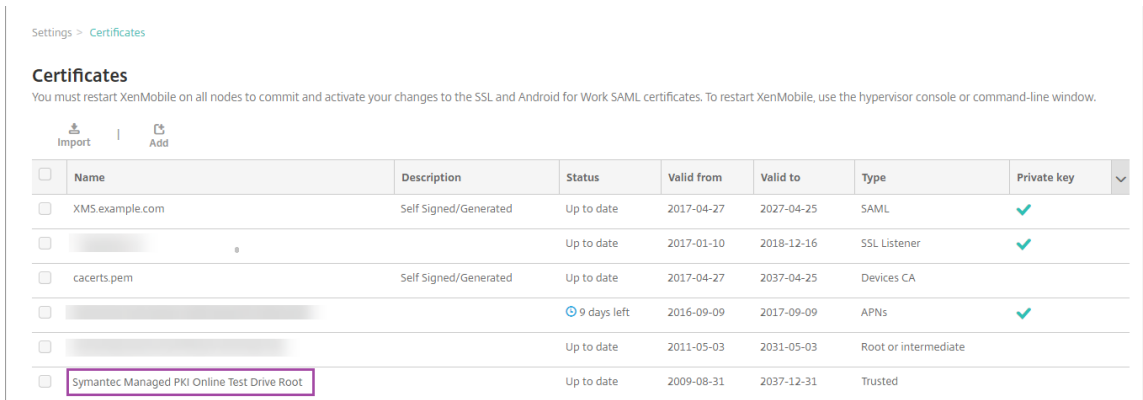


DigiCert 관리 PKI 를 사용하도록 XenMobile Server 구성

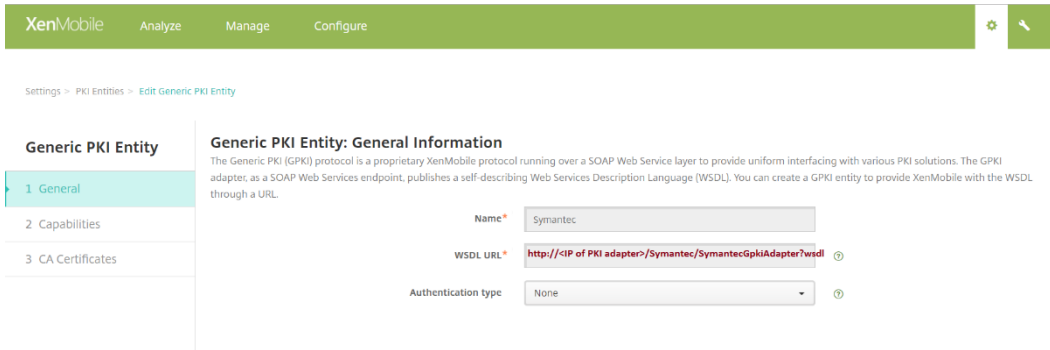
다음 XenMobile Server 구성을 수행하기 전에 Windows Server 설정을 완료합니다.

DigiCert CA 인증서를 가져오고 PKI 엔터티를 구성하려면

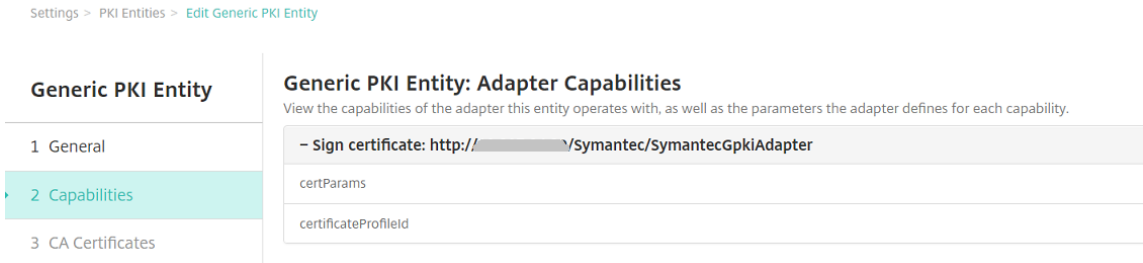
1. 최종 사용자 인증서를 발급하는 DigiCert CA 인증서를 가져옵니다. XenMobile Server 콘솔에서 설정 > 인증서로 이동하고 가져오기를 클릭합니다.



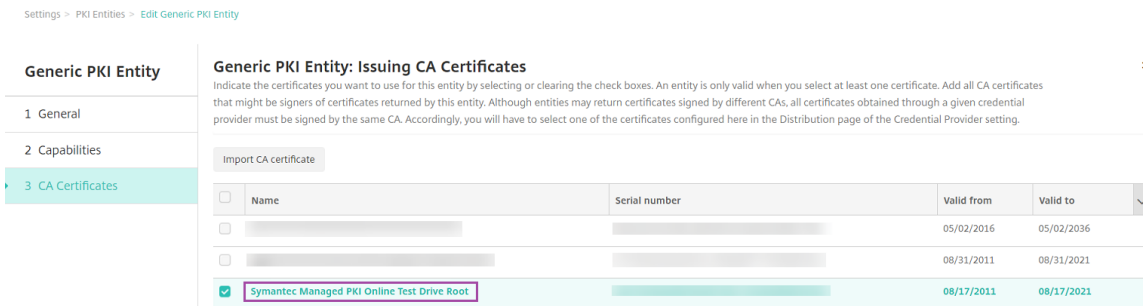
- PKI 엔터티를 추가하고 구성합니다. 설정 > PKI 엔터티에서 추가를 클릭한 후 제네릭 PKI 엔터티를 선택합니다. 이전 섹션에서 PKI 어댑터를 구성할 때 복사한 끝점 주소를 WSDL URL 에 붙여 넣고 아래와 같이 ?wsdl 을 추가합니다.



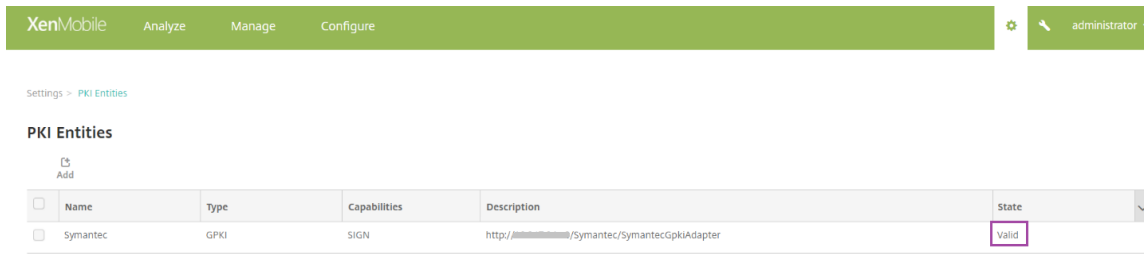
- 다음을 클릭합니다. XenMobile 이 WSDL 의 매개변수를 입력합니다.



- 다음을 클릭하고 올바른 CA 인증서를 선택한 후 저장을 클릭합니다.

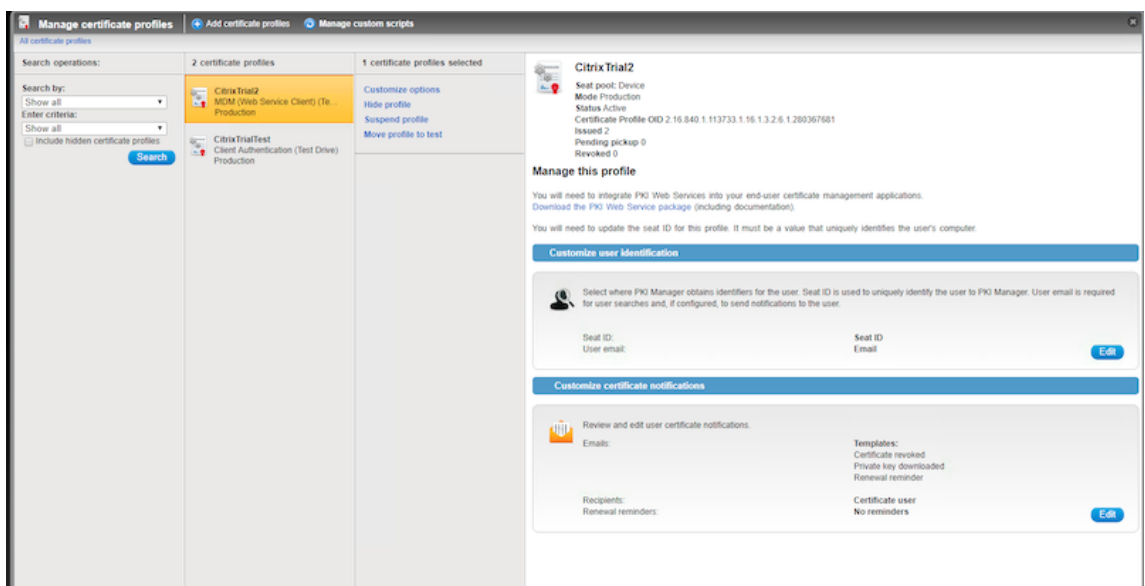


- 설정 > PKI 엔터티 페이지에서 추가한 PKI 엔터티의 상태가 유효함인지 확인합니다.



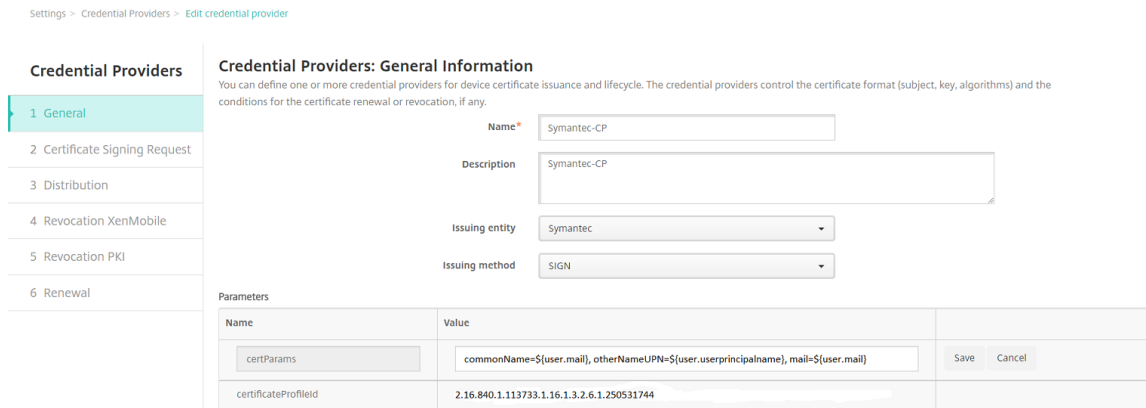
DigiCert 관리 PKI 에 대한 자격증명 공급자를 만들려면

1. DigiCert PKI Manager 콘솔에서 인증서 템플릿의 **Certificate Profile OID(인증서 프로필 OID)** 를 복사합니다.



2. XenMobile Server 콘솔에서 설정 > 자격증명 공급자로 이동하고 추가를 클릭한 후 다음과 같이 설정을 구성합니다.

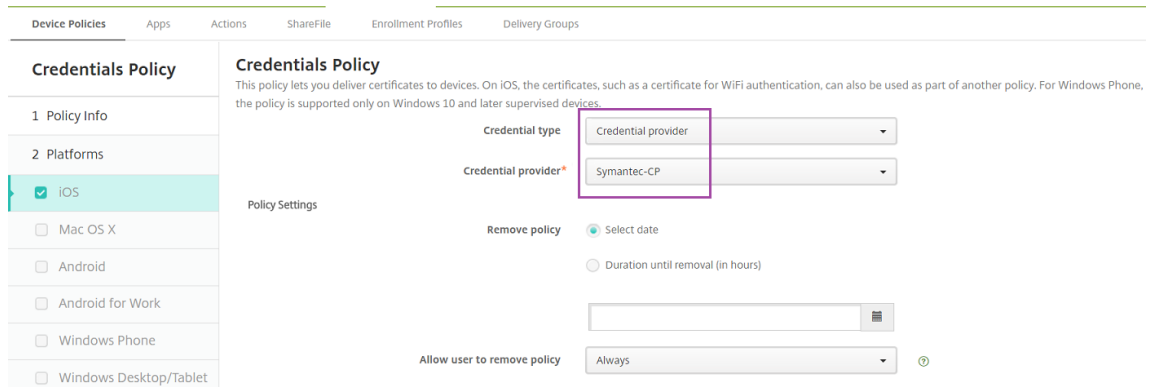
- 이름: 새 공급자 구성의 고유한 이름을 입력합니다. 이름은 XenMobile 콘솔의 다른 부분에서 구성을 참조할 때 사용 됩니다.
- 설명: 자격증명 공급자를 설명합니다. 이 필드는 선택 사항이지만 이 자격증명 공급자에 대한 세부 정보가 필요할 경우 설명 이 유용할 수 있습니다.
- 발급 엔터티: 인증서 발급 엔터티를 선택합니다.
- 발급 방법: 시스템이 구성된 엔터티에서 클라이언트 인증서를 가져올 때 사용할 방법으로 서명을 선택합니다.
- certParams: 다음 값을 추가합니다. **commonName=\${user.mail},otherNameUPN=\${user.userprincipalname}**
- certificateProfileid: 1 단계에서 복사한 인증서 프로필 OID 를 붙여넣습니다.



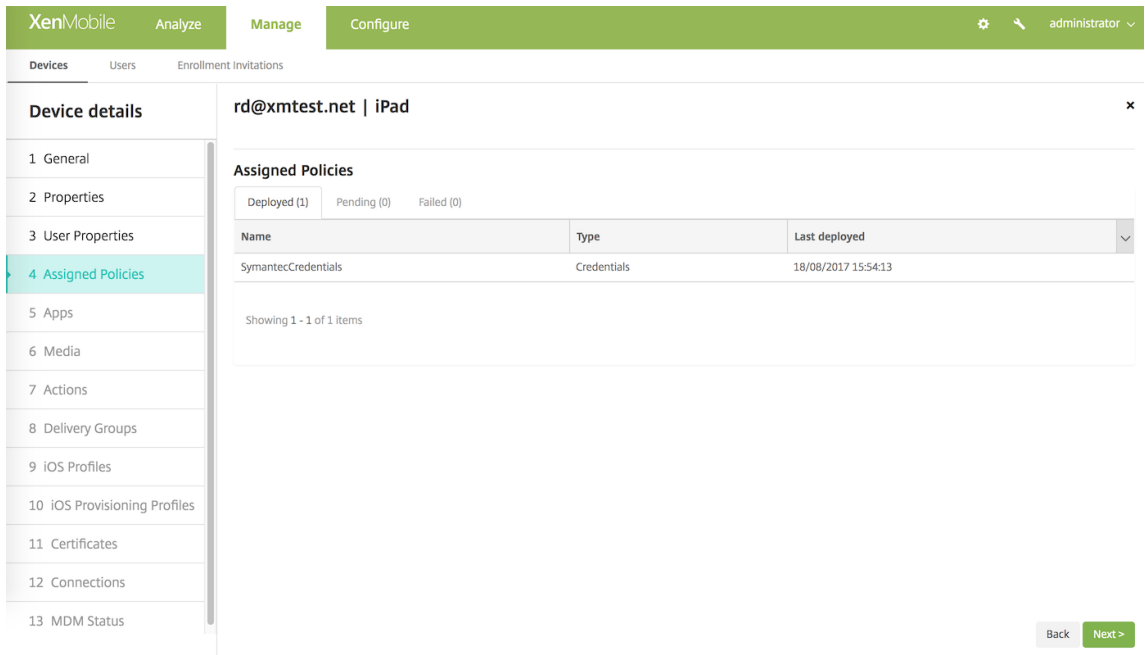
3. 다음을 클릭합니다. 나머지 각 페이지에서 (갱신을 통한 인증서 서명 요청) 기본 설정을 사용합니다. 완료되면 저장을 클릭합니다.

구성을 테스트하고 문제 해결을 수행하려면

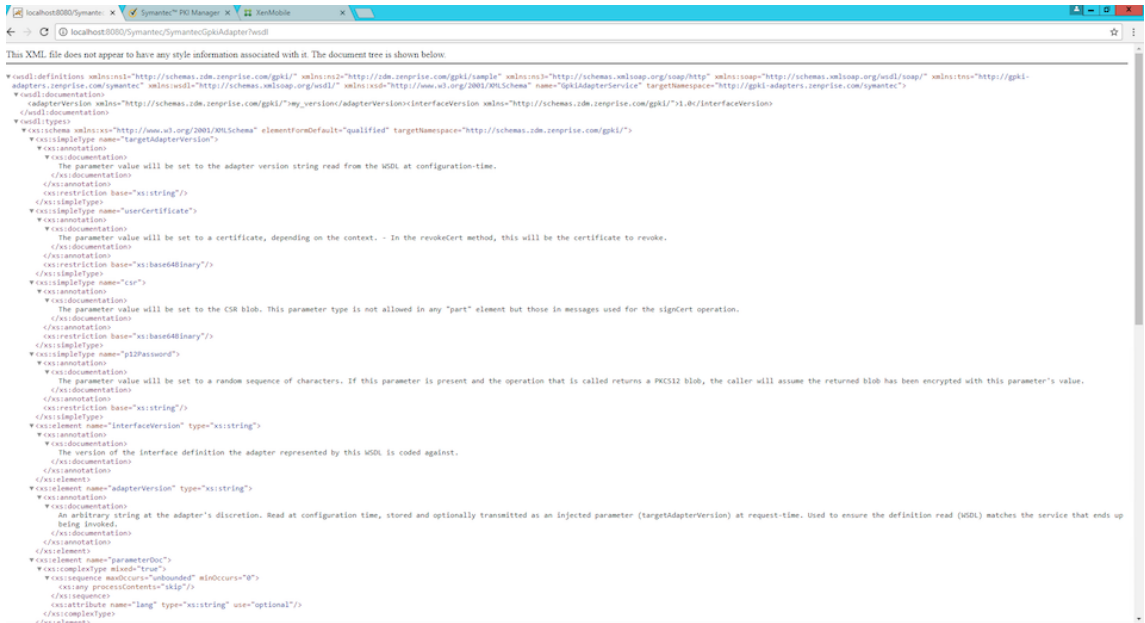
1. 자격 증명 장치 정책을 생성합니다. 구성 > 장치 정책에서 추가를 클릭하고 자격 증명 입력을 시작한 후 자격 증명을 클릭합니다.
2. 정책 이름을 지정합니다.
3. 다음과 같이 플랫폼 설정을 구성합니다.
 - 자격 증명 유형: 자격 증명 공급자를 선택합니다.
 - 자격 증명 공급자: DigiCert 공급자를 선택합니다.



4. 플랫폼 설정을 완료한 후 할당 페이지에서 배달 그룹에 정책을 할당하고 저장을 클릭합니다.
5. 정책이 장치에 배포되었는지 확인하려면 관리 > 장치에서 장치를 선택하고 편집을 클릭한 후 할당된 정책을 클릭합니다. 다음 예제는 성공적으로 배포된 정책을 보여줍니다.



정책이 배포되지 않은 경우 Windows Server 에 로그인하고 WSDL 이 올바르게 로드되는지 확인합니다.



자세한 문제 해결 정보는 <tomcat dir>\logs\catalina.<current date>에서 Tomcat 로그를 확인하십시오.

Entrust PKI 어댑터

DigiCert 관리 PKI 대신 Entrust PKI 어댑터를 설치할 수 있습니다. 이어댑터를 설치하기 전에, 이 문서의 DigiCert 관리 PKI 섹션에서 Windows 서버에 Java 및 Apache Tomcat 을 설치하는 단계를 참조하십시오.

Entrust PKI 어댑터설치

1. <https://www.citrix.com/downloads/citrix-endpoint-management/product-software/xenmobile-10-server.html>의 **Entrust Adapter(Entrust 어댑터)** 섹션에서 Entrust PKI 어댑터를다운로드합니다.
2. 다운로드한.zip 파일에서 entrust.war 파일을추출하여 C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps 디렉터리에배치합니다.
3. C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes 에서 entrust_adapter.properties 를편집하여 CustomProperties 를 c:\\zenprise\\custom_entrust_adapter.properties로설정합니다.

```
entrust_adapter - Notepad
File Edit Format View Help
# $Id: entrust_adapter.properties 31447 2013-04-17 17:17:34Z bsafinejad $
# custom deployment properties override the settings in this file
CustomProperties=c:\\zenprise\\custom_entrust_adapter.properties
```

4. C: 드라이브에서 zenprise 디렉터를만들고그안에 custom_entrust_adapter.properties 라는새파일을만듭니다.
5. 이파일을다음과같은내용으로편집합니다. Entrust.MdmSvc.URL, AdminUserId 및 AdminPassword 를적절히대체했는지확인하십시오.

```
~
# 다음을 AS/IG 에대한적절한 URL 로설정
Entrust.MdmSvc.Url=https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8
```

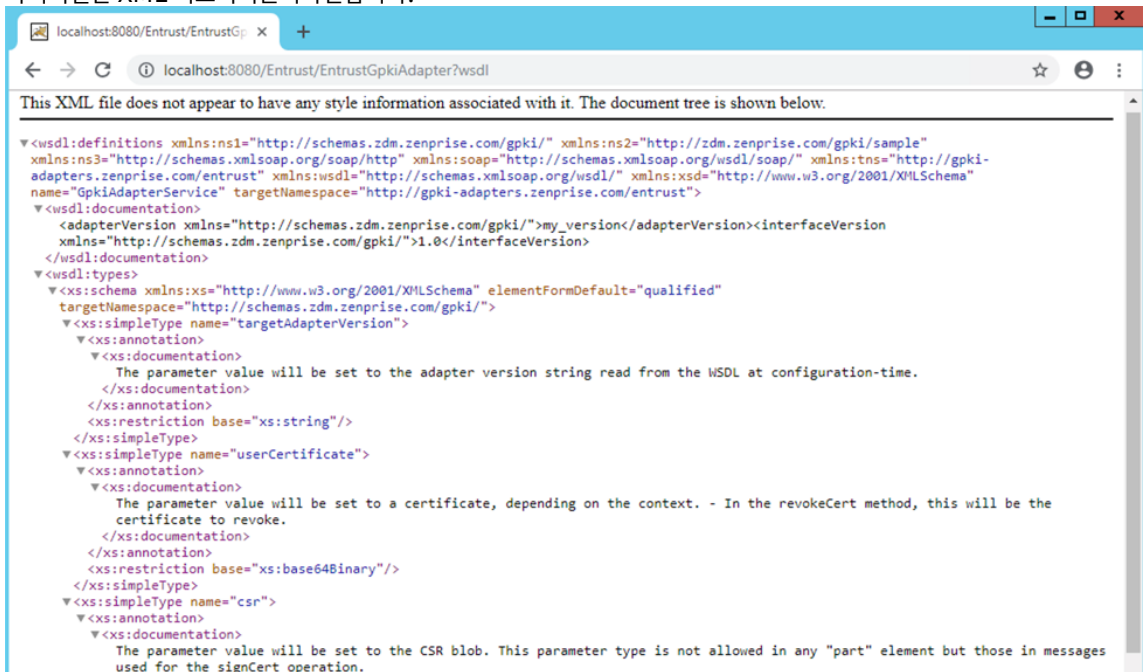
```
1 # IG를 사용하고 사용자가 존재하지 않는 경우 전달된 사용자 및 그룹
   매개 변수에서 사용자를 생성하려면 1 또는 true로 설정
2 CreateUser=
3
4 # 끝점의 자격 증명 설정
5 AdminUserId='[User ID]'
6 AdminPassword='[password]'
7
8
9 # keystore for client-cert auth
10 #keyStore=
11 #keyStorePassword=
12 #keyStoreType: JKS, JCEKS 및 PKCS12 -- .p12 및 .jks 파일에는 필요
   하지 않음
13
14 # truststore for server with self-signed root CA
```

```

15 #trustStore=
16 #trustStorePassword=
17 #trustStoreType: JKS, JCEKS 및 PKCS12 -- .p12 및 .jks 파일에는 필
    요하지 않음
18 ~
    
```

6. Tomcat 서비스를 다시 시작합니다. C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\logs 로 이동하여 Catalina_201x-MM-DD.log 를 엽니다. 오류가 없으며 다음과 같은 줄이 표시되는지 확인합니다.


```
13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf
.endpoint.ServerImpl.initDestination Setting the server's publish
address to be /EntrustGpkiAdapter
```
7. <http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl> 또는 서버의 공개 URL 로 이동하여 적절한 XML 이 표시되는지 확인합니다.



Entrust PKI 어댑터에 대해 XenMobile 구성

1. XenMobile 콘솔에 로그인하고 설정 > PKI 엔터티로 이동합니다. 추가 > 제네릭 PKI 엔터티를 클릭합니다.
2. 다음 정보를 입력합니다.
 - 이름: PKI 엔터티의 이름을 입력합니다.
 - WSDL URL: 서버의 공개 URL 을 입력합니다.
 - 인증 유형: 사용하려는 인증 방법을 선택합니다.
 - 없음
 - HTTP 기본: 연결하는데 필요한 사용자 이름 및 암호를 입력합니다.
 - 클라이언트 인증서: 올바른 SSL 클라이언트 인증서를 선택합니다.

- 리소스위치: **My Resource Location(내리소스위치)** 을선택합니다.
 - 허용된상대경로: `/Entrust/*`를입력합니다.
3. PKI 엔터티구성을마쳤으면 설정페이지가돌아가 자격증명공급자를추가합니다.
 4. 일반탭에서 Entrust 엔터티를 발급엔터티로, 서명을 발급방법으로선택합니다.
 5. **CSR** 탭에서다음과같이설정을구성합니다.
 - 키알고리즘: **RSA**
 - 키크기: 2048
 - 서명알고리즘 **SHA1withRSA**
 - 주체이름: `cd=$user.username`
 - 주체대체이름: 선택사항입니다. 다음을권장합니다.
 - 유형: 사용자계정이름
 - 값: `$user.userprincipalname`

참고:
어댑터의설정을변경한경우이러한단계에따라자격증명공급자를다시구성하십시오.
 6. 자격증명공급자구성을마친후 구성 > 장치정책으로이동하여자격증명정책을추가합니다.
 7. 사용하려는 OS 에대한정책을구성합니다. 각 OS 구성페이지에서 자격증명유형으로 자격증명공급자를선택합니다. 자격증명공급자메뉴에서앞서구성한자격증명공급자를선택합니다.

Microsoft 인증서서비스

XenMobile 은웹등록인터페이스를통해 Microsoft 인증서서비스와상호작용합니다. XenMobile 은그인터페이스를통해 새인증서발급만지원합니다 (GPKI 서명기능에해당). Microsoft CA 에서 NetScaler Gateway 사용자인증서를생성하면 NetScaler Gateway 가해당인증서의갱신과해지를지원합니다.

XenMobile 에서 Microsoft CA PKI 엔터티를만들려면인증서서비스웹인터페이스의기본 URL 을지정해야합니다. 원할경우 SSL 클라이언트인증을사용하여 XenMobile 과인증서서비스웹인터페이스간의연결을보호할수있습니다.

Microsoft 인증서서비스엔터티추가

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭하고 **PKI** 엔터티를클릭합니다.
2. **PKI** 엔터티페이지에서 추가를클릭합니다.
PKI 엔터티유형에대한메뉴가나타납니다.
3. **Microsoft** 인증서서비스엔터티를클릭합니다.
Microsoft 인증서서비스엔터티: 일반정보페이지가나타납니다.
4. **Microsoft** 인증서서비스엔터티: 일반정보페이지에서다음설정을구성합니다.
 - 이름: 나중에엔터티를참조하는데사용할새엔터티이름을입력합니다. 엔터티이름은고유해야합니다.
 - 웹등록서비스루트 **URL**: Microsoft CA 웹등록서비스의기본 URL(예: `https://192.0.2.13/certsrv/`) 을입력합니다. URL 은일반 HTTP 또는 HTTP-over-SSL 을사용할수있습니다.

- **certnew.cer** 페이지이름: certnew.cer 페이지의이름입니다. 어떤이유로이름을변경한경우가아니면기본이름을사용합니다.
 - **certfnsh.asp**: certfnsh.asp 페이지의이름입니다. 어떤이유로이름을변경한경우가아니면기본이름을사용합니다.
 - 인증유형: 사용하려는인증방법을선택합니다.
 - 없음
 - **HTTP** 기본: 연결하는데필요한사용자이름및암호를입력합니다.
 - 클라이언트인증서: 올바른 SSL 클라이언트인증서를선택합니다.
5. 연결테스트를클릭하여서버에액세스할수있는지확인합니다. 액세스할수없는경우연결에실패했음을알리는메시지가나타납니다. 구성설정을확인합니다.
6. 다음을클릭합니다.
- Microsoft** 인증서서비스엔터티: 템플릿페이지가나타납니다. 이페이지에서는해당 Microsoft CA 가지원하는템플릿의내부이름을지정합니다. 자격증명공급자를만들때여기에정의된목록에서템플릿을선택합니다. 이엔터티를사용하는모든자격증명공급자가해당템플릿하나만사용합니다.
- Microsoft 인증서서비스템플릿요구사항은해당 Microsoft 서버버전에대한 Microsoft 설명서를참조하십시오. XenMobile 에는 [인증서](#)에명시된인증서형식을제외하고배포하는인증서에대한요구사항이없습니다.
7. **Microsoft** 인증서서비스엔터티: 템플릿페이지에서 추가를클릭하고템플릿이름을입력한후 저장을클릭합니다. 추가할각템플릿에대해이단계를반복합니다.
8. 다음을클릭합니다.
- Microsoft** 인증서서비스엔터티: **HTTP** 매개변수페이지가나타납니다. 이페이지에서는 XenMobile 이 Microsoft 웹등록인터페이스에대한 HTTP 요청에추가해야하는사용자지정매개변수를지정합니다. 사용자지정매개변수는 CA 에서실행되는사용자지정스크립트에만유용합니다.
9. **Microsoft** 인증서서비스엔터티: **HTTP** 매개변수페이지에서 추가를클릭하고추가할 HTTP 매개변수의이름과값을입력한후 다음을클릭합니다.
- Microsoft** 인증서서비스엔터티: **CA** 인증서페이지가나타납니다. 이페이지에서는시스템이엔터티를통해얻는인증서의서명자를 XenMobile 에알려야합니다. CA 인증서가갱신되면 XenMobile 에서인증서를업데이트합니다. XenMobile 이변경내용을투명하게엔터티에적용합니다.
10. **Microsoft** 인증서서비스엔터티: **CA** 인증서페이지에서엔터티에사용할인증서를선택합니다.
11. 저장을클릭합니다.
- PKI 엔터티테이블에해당엔터티가나타납니다.

NetScaler CRL(인증서해지목록)

XenMobile 은타사인증기관에대해서만 CRL(인증서해지목록) 을지원합니다. Microsoft CA 가구성된경우 XenMobile 은 NetScaler 를사용하여해지를관리합니다.

클라이언트인증서기반인증을구성하는경우 NetScaler CRL(인증서해지목록) 설정인 **Enable CRL Auto Refresh(CRL 자동새로고침사용)** 을구성해야하는지여부를고려합니다. 이단계는 MAM 전용모드의장치사용자가장치의기존인증서를사용하여 인증할수없도록합니다.

XenMobile 에서는인증서가해지된경우사용자가사용자인증서를생성할수있으므로새인증서가다시발급됩니다. 이설정을사용하면 CRL 이만료된 PKI 엔터티를확인하는경우 PKI 엔터티의보안이강화됩니다.

임의의 CA

임의의 CA 는 CA 인증서와연결된개인키를 XenMobile 에제공하는경우만들어집니다. XenMobile 은지정된매개변수에따라 인증서발급, 해지및상태정보를내부적으로처리합니다.

임의의 CA 를구성하는경우해당 CA 에대한 OCSP(온라인인증서상태프로토콜) 지원을활성화할수있습니다. OCSP 지원을사용하도록설정된경우에한해 CA 는 `id-pe-authorityInfoAccess` 확장을 CA 가발급한인증서에추가합니다. 이확장은 다음위치의 XenMobile 내부 OCSP Responder 를가리킵니다.

<https://<server>/<instance>/ocsp>

OCSP 서비스를구성하는경우해당임의의엔터티에대한 OCSP 서명인증서를지정합니다. CA 인증서자체를서명자로사용할수있습니다. CA 개인키의불필요한노출을방지하려면 (권장) CA 인증서로서명된위임자 OCSP 서명인증서를만들고 `id-kp-OCSPSigning extendedKeyUsage` 확장을포함합니다.

XenMobile OCSP 응답자서비스는기본 OCSP 응답과다음해시알고리즘을요청에지원합니다.

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

응답은 SHA-256 및서명인증서키알고리즘 (DSA, RSA 또는 ECDSA) 으로서명됩니다.

임의의 CA 추가

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭하고 자세히 > **PKI** 엔터티를클릭합니다.
2. **PKI** 엔터티페이지에서 추가를클릭합니다.
PKI 엔터티유형에대한메뉴가나타납니다.
3. 임의의 **CA** 를클릭합니다.
임의의 **CA**: 일반정보페이지가나타납니다.
4. 임의의 **CA**: 일반정보페이지에서다음을수행합니다.
 - 이름: 임의의 CA 를설명하는이름을입력합니다.

- 인증서요청에서명할 **CA** 인증서: 인증서요청에서명하는데사용할임의의 CA 용인증서를클릭합니다.

XenMobile 에서 구성 > 설정 > 인증서를통해업로드한개인키를사용하여 CA 인증서에서인증서목록이생성됩니다.

5. 다음을클릭합니다.

임의의 **CA**: 매개변수페이지가나타납니다.

6. 임의의 **CA**: 매개변수페이지에서다음을수행합니다.

- 일련번호생성기: 임의의 CA 가발급한인증서에대한일련번호를생성합니다. 이목록에서 순차적또는 비순차적을클릭하여숫자가생성되는방식을지정합니다.
- 다음일련번호: 다음번발급될번호를지정하는값을입력합니다.
- 인증서유효기간: 인증서가유효한일수를입력합니다.
- 키사용: 해당키를 켜짐으로설정하여임의의 CA 에서발급하는인증서의용도를지정합니다. 이항목을설정하면해당 CA 가지정된용도로만인증서를발급할수있게됩니다.
- 확장키사용: 매개변수를더추가하려면 추가를클릭하고키이름을입력한후 저장을클릭합니다.

7. 다음을클릭합니다.

임의의 **CA**: 배포페이지가나타납니다.

8. 임의의 **CA**: 배포페이지에서배포모드를선택합니다.

- 중앙집중식: 서버측키생성. 중앙집중식옵션을사용하는것이 좋습니다. 개인키가생성되어서버에저장되고사용자장치에배포됩니다.
- 분산: 장치측키생성. 개인키가사용자장치에생성됩니다. 이분산모드에서는 SCEP 를사용하며 **keyUsage keyEncryption** 확장의 RA 암호화인증서와 **keyUsage digitalSignature** 확장의 RA 서명인증서가필요합니다. 암호화와서명에모두동일한인증서를사용할수있습니다.

9. 다음을클릭합니다.

임의의 **CA**: **OCSP**(온라인인증서상태프로토콜) 페이지가나타납니다.

임의의 **CA**: **OCSP**(온라인인증서상태프로토콜) 페이지에서다음을수행합니다.

- 이 CA 가서명한인증서에 **AuthorityInfoAccess**(RFC2459) 확장을추가하려면 이 **CA** 에 **OCSP** 지원 사용을 켜짐으로설정합니다. 이확장은 CA OCSP Responder(<https://<server>/<instance>/ocsp>) 를가리킵니다.
- OCSP 지원을사용하도록설정할경우 OSCP 서명 CA 인증서를선택합니다. XenMobile 에업로드한 CA 인증서에서인증서목록이생성됩니다.

10. 저장을클릭합니다.

PKI 엔터티테이블에임의의 CA 가나타납니다.

자격증명공급자

October 21, 2019

자격증명공급자는 XenMobile 시스템의 다양한 부분에서 사용하는 실제 인증서 구성입니다. 자격증명공급자는 인증서의 원본, 매개 변수 및 수명 주기를 정의합니다. 이러한 작업은 인증서가 장치 구성의 일부인지 독립 실행형 (즉, 있는 그대로 장치에 푸시됨) 인지에 따라 발생합니다.

장치 등록은 인증서 수명 주기를 제한합니다. 즉, XenMobile 은 등록 과정에서 일부 인증서를 발급할 수 있지만 등록 전에는 인증서를 발급하지 않습니다. 또한 등록이 해지되면 하나의 등록 컨텍스트 내에서 내부 PKI 에 의해 발급된 인증서가 해지됩니다. 관리 관계가 종료된 후에는 유효한 인증서가 남아 있지 않습니다.

단일 구성이 동시에 여러 개의 인증서를 관리할 수 있도록 여러 곳에서 단일 자격증명공급자 구성을 사용할 수 있습니다. 통일성은 배포 리소스 및 배포에 기반합니다. 예를 들어 자격증명공급자 P 가 구성 C 의 일부로 장치 D 에 배포된 경우 P 에 대한 발급 설정은 D 에 배포된 인증서를 결정합니다. 마찬가지로 D 에 대한 갱신 설정은 C 가 업데이트될 때 적용됩니다. D 에 대한 해지 설정도 C 가 삭제되거나 D 가 해지될 때 적용됩니다.

이 규칙에 따라 XenMobile 의 자격증명공급자 구성은 다음을 결정합니다.

- 인증서의 원본.
- 인증서를 얻는 방법: 새 인증서에서 명하거나 기존 인증서 및 키 쌍을 가져옵니다 (복구).
- 발급 또는 복구를 위한 매개 변수. 예: 키 크기, 키 알고리즘 및 인증서 확장 같은 CSR (인증서 서명 요청) 매개 변수.
- 인증서가 장치로 전달되는 방식.
- 해지 조건. XenMobile 에서 관리 관계가 끊어지면 모든 인증서가 해지되지만 구성에서 만료 이전에 해지되도록 지정할 수 있습니다. 예를 들어 연결된 장치 구성이 삭제된 경우 인증서가 해지되도록 구성할 수 있습니다. 또한 특정 조건에서는 XenMobile 에서 관련된 인증서의 해지가 백엔드 PKI (공개 키 인프라) 로 전송될 수 있습니다. 즉, XenMobile 에서 인증서가 해지되면 PKI 에서 인증서가 해지될 수 있습니다.
- 갱신 설정. 지정된 자격증명공급자를 통해 받은 인증서는 만료 날짜가 가까워질 때 자동으로 갱신될 수 있습니다. 또는 이러한 상황과 별개로 만료 날짜가 다가올 때 알림을 실행할 수 있습니다.

사용 가능한 구성 옵션은 주로 자격증명공급자에 대해 선택한 PKI 엔터티 및 발급 방법의 유형에 따라 다릅니다.

인증서 발급 방법

발급 방법이라고 하는 두 가지 방법으로 인증서를 얻을 수 있습니다.

- 서명: 이 방법을 사용할 경우 발급에 새 개인 키를 만들고, CSR 을 만들고, 서명을 위해 CSR 을 CA (인증 기관) 에 제출하는 과정이 포함됩니다. XenMobile 은 세 가지 PKI 엔터티 (MS 인증서 서비스 엔터티, 제네릭 PKI 및 임의의 CA) 에 대한 서명 방법을 지원합니다.
- 가져오기: 이 방법을 사용할 경우 XenMobile 에서 발급은 기존 키 쌍을 복구하는 것입니다. XenMobile 은 제네릭 PKI 에 대해서만 가져오기 방법을 지원합니다.

자격증명공급자는서명또는가져오기발급방법을사용합니다. 선택한방법에따라사용가능한구성옵션이달라집니다. 특히 CSR 구성및분산전달은발급방법이서명인경우에만사용할수있습니다. 가져온인증서는항상 PKCS #12 로장치에전송되며, 이형식은서명방법에대한중앙집중식전달모드와동일합니다.

인증서제공

XenMobile 에서는중앙집중식모드와분산모드의두가지인증서전달모드를사용할수있습니다. 분산모드는 SCEP(단순인증서등록프로토콜) 를사용하며클라이언트가프로토콜을지원하는경우에만사용할수있습니다 (iOS 만해당). 일부상황에서는분산모드가필수입니다.

자격증명공급자가분산 (SCEP 지원) 전달을지원하려면 RA(등록기관) 인증서설정이라는특수한구성단계가필요합니다. SCEP 프로토콜을사용하는경우 XenMobile 이실제인증기관의대리인 (등록기관) 역할을하기때문에 RA 인증서가필요합니다. XenMobile 은클라이언트에게인증기관의역할을수행할권한이있음을인증해야합니다. 이권한은앞서언급한인증서를XenMobile 에업로드하여설정됩니다.

단일인증서로두가지요구사항을모두충족시킬수있지만, 두가지고유한인증서역할 (RA 서명및 RA 암호화) 이필요합니다. 이러한역할에대한제약조건은다음과같습니다.

- RA 서명인증서에는 X.509 키사용디지털서명이있어야합니다.
- RA 암호화인증서에는 X.509 키사용키암호화가있어야합니다.

자격증명공급자 RA 인증서를구성하려면 XenMobile 에인증서를업로드한다음자격증명공급자에서인증서에연결합니다.

자격증명공급자는인증서역할에대해구성된인증서가있는경우에만분산전달을지원하는것으로간주됩니다. 중앙집중식모드를선택하거나, 분산모드를선택하거나또는분산모드를요구하도록각자격증명공급자를구성할수있습니다. 실제결과는컨텍스트에따라달라집니다. 컨텍스트가분산모드를지원하지않지만자격증명공급자가이모드를요구하면배포가실패합니다. 마찬가지로컨텍스트에서분산모드를요구하지만자격증명공급자가분산모드를지원하지않으면배포가실패합니다. 다른모든경우에는기본설정이적용됩니다.

다음표에서는 XenMobile 의 SCEP 배포를보여줍니다.

컨텍스트	SCEP 지원	SCEP 필요
iOS 프로필서비스	예	예
iOS 모바일기기관리등록	예	아니요
iOS 구성프로필	예	아니요
SHTP 등록	아니요	아니요
SHTP 구성	아니요	아니요
Windows Phone 및 Tablet 등록	아니요	아니요
Windows Phone 및 Tablet 구성	아니요 (Windows Phone 8.1 및최신 Windows 10 릴리스에서지원되는 WiFi 장치정책제외)	아니요

인증서해지

해지에는세가지유형이있습니다.

- **내부적해지:** 내부적해지는 XenMobile 에서유지관리하는인증서상태에영향을줍니다. XenMobile 은제시된인증서를 평가하거나인증서에대한 OCSP 상태정보를제공할때이상태를고려합니다. 자격증명공급자구성에따라다양한조건에서이러한상태가영향을받는방식이결정됩니다. 예를들어자격증명공급자는인증서가장치에서삭제된경우인증서에해지플래그를지정하도록지정할수있습니다.
- **외부에서전파된해지:** 해지 XenMobile 이라고알려진이해지유형은외부 PKI 에서취득한인증서에적용됩니다. 자격증명공급자구성에정의된조건에따라 XenMobile 에서내부적으로인증서가해지되는경우 PKI 에서인증서가해지됩니다. 해지를수행하는요청에는해지가가능한일반 PKI(GPKI) 엔터티가필요합니다.
- **외부에서유도된해지:** 해지 PKI 라고알려진이해지유형도외부 PKI 에서취득한인증서에만적용됩니다. XenMobile 이지정된인증서상태를평가할때마다 XenMobile 은해당상태에대해 PKI 를쿼리합니다. 인증서가해지된경우에는 XenMobile 이내부적으로인증서를해지합니다. 이메커니즘에서 OCSP 프로토콜을사용합니다.

이세가지유형은배타적이지않으며함께적용됩니다. 외부해지또는독립적결과로인해내부해지가발생할수있습니다. 내부해지는외부해지에영향을미칠수있습니다.

인증서갱신

인증서갱신은기존인증서의해지와다른인증서발급의조합입니다.

XenMobile 은발급실패로인한서비스중단을방지하기위해이전인증서를해지하기전에먼저새인증서를얻으려고시도합니다. 분산(SCEP 지원) 제공의경우해지는인증서가장치에설치된후에만발생합니다. 그렇지않은경우해지는새인증서가장치에전송되기전에발생합니다. 이해지는인증서설치의성공또는실패와관계가없습니다.

해지구성에서특정기간(일)을지정해야합니다. 장치가연결되면서서는인증서 NotAfter 날짜가현재날짜에서지정된기간을뺀날짜보다이후인지여부를확인합니다. 인증서가조건을충족하면 XenMobile 이인증서갱신을시도합니다.

자격증명공급자생성

자격증명공급자구성은주요자격증명공급자에대해선택한발급엔터티및발급방법의요인에따라달라집니다. 내부엔터티또는외부엔터티를사용하는자격증명공급자를구분할수있습니다.

- XenMobile 에대해내부인임의의엔터티는내부엔터티입니다. 임의의엔터티에대한발급방법은항상서명입니다. 서명은발급작업을수행할때마다 XenMobile 이엔터티에대해선택된 CA 인증서로새키쌍을서명한다는것을의미합니다. 키쌍이장치에서생성되는지, 아니면서버에서생성되는지는선택한배포방법에따라다릅니다.
- 회사인프라의일부인외부엔터티에는 Microsoft CA 또는 GPKI 가포함됩니다.

자격증명공급자생성을포함한 DigiCert 관리 PKI 설정에대한자세한내용은 PKI 엔터티의 “DigiCert 관리 PKI” 를참조하십시오.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭하고 설정 > 자격증명공급자를클릭합니다.

2. 자격증명공급자페이지에서 추가를클릭합니다.

자격증명공급자: 일반정보페이지가나타납니다.

3. 자격증명공급자: 일반정보페이지에서다음을수행합니다.

- 이름: 새공급자구성의고유한이름을입력합니다. 이이름은나중에 XenMobile 콘솔의다른부분에서구성을식별할 때사용됩니다.
- 설명: 자격증명공급자를설명합니다. 이필드는선택사항이지만설명을사용하면이자격증명공급자에대한유용한세부 정보를제공할수있습니다.
- 발급엔터티: 인증서발급엔터티를클릭합니다.
- 발급방법: 시스템이구성된엔터티에서인증서를가져올때사용할방법으로 서명또는 가져오기를클릭합니다. 클라이언트인증서인증의경우 서명을사용합니다.
- 템플릿목록을사용할수있는경우자격증명공급자에대한 PKI 엔터티아래에추가한템플릿을선택합니다.
설정 > PKI 엔터티에서 Microsoft 인증서서비스엔터티를추가하면이러한템플릿을사용할수있게됩니다.

4. 다음을클릭합니다.

자격증명공급자: **CSR** 페이지가나타납니다.

5. 자격증명공급자: **CSR** 페이지에서인증서구성에따라다음을구성합니다.

- 키알고리즘: 새키쌍에대한키알고리즘을선택합니다. 사용가능한값은 **RSA**, **DSA** 및 **ECDSA** 입니다.
- 키크기: 키쌍의크기 (비트) 를입력합니다. 이것은필수필드입니다.
허용되는값은키유형에따라다릅니다. 예를들어 DSA 키의최대크기는 1024 비트입니다. 기본하드웨어및소프트웨어에따라달라질수있는거짓응성반응을방지하기위해 XenMobile 은키크기를강제하지않습니다. 자격증명공급자 구성을프로덕션환경에서활성화하기전에항상테스트환경에서테스트해야합니다.
- 서명알고리즘: 새인증서에대한값을클릭합니다. 값은키알고리즘에따라달라집니다.
- 주체이름: 필수항목입니다. 새인증서주체의 DN(고유이름) 을입력합니다. 예를들면다음과같습니다.
`CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

예를들어클라이언트인증서인증의경우다음설정을사용합니다.

- 키알고리즘: RSA
- 키크기: 2048
- 서명알고리즘: SHA1withRSA
- 주체이름: `cn=${ user.username }`

- 주체대체이름테이블에항목을추가하려면 추가를클릭합니다. 대체이름의유형을선택하고두번째열에값을입력합니다.

클라이언트인증서인증의경우다음을지정합니다.

- 유형: 사용자계정이름
- 값: `$user.userprincipalname`

주체이름과 마찬가지로 값 필드에 XenMobile 매크로를 사용할 수 있습니다.

6. 다음을 클릭합니다.

자격증명공급자: 배포페이지가 나타납니다.

7. 자격증명공급자: 배포페이지에서 다음을 수행합니다.

- **CA** 인증서 발급 목록에서 제공된 CA 인증서를 클릭합니다. 자격증명공급자가 임의의 CA 엔터티를 사용하기 때문에 자격증명공급자에 대한 CA 인증서는 항상 엔터티 자체에서 구성된 CA 인증서입니다. 여기에 나온 CA 인증서는 외부 엔터티를 사용하는 구성과의 일관성을 위한 것입니다.
- 배포 모드 선택에서 다음과 같은 키 생성 및 배포 방법 중 하나를 클릭합니다.
 - 중앙 집중식 번호: 서버 측 키 생성: 이중 양 집중식 옵션을 사용하는 것이 좋습니다. 이 옵션은 XenMobile 에서 지원하는 모든 플랫폼을 지원하며 NetScaler Gateway 인증을 사용할 때 필요합니다. 개인 키가 생성되어 서버에 저장되고 사용자 장치에 배포됩니다.
 - 분산식 번호: 장치 측 키 생성: 개인 키가 생성되고 사용자 장치에 저장됩니다. 이 분산 모드에서는 SCEP 를 사용하며 keyUsage keyEncryption 이 포함된 RA 암호화 인증서와 KeyUsage digitalSignature 가 포함된 RA 서명 인증서가 필요합니다. 암호화와 서명에도 모두 동일한 인증서를 사용할 수 있습니다.
 - 분산 전용: 장치 측 키 생성: 이 옵션은 “선택” 가 아닌 “전용” 이기 때문에 장치 측 키 생성이 실패하거나 사용할 수 없는 경우 사용할 수 있는 옵션이 없다는 것을 제외하면 분산식 번호: 장치 측 키 생성과 동일하게 작동합니다.

분산식 번호: 장치 측 키 생성 또는 분산 전용: 장치 측 키 생성을 선택한 경우 RA 서명 인증서 및 RA 암호화 인증서를 클릭합니다. 둘 모두에 동일한 인증서를 사용할 수 있습니다. 인증서에 대한 새 필드가 나타납니다.

8. 다음을 클릭합니다.

자격증명공급자: 해지 **XenMobile** 페이지가 나타납니다. 이 페이지에서 XenMobile 이이 공급자 구성을 통해 발급된 인증서를 어떤 조건일 때 내부적으로 해지된 것으로 플래그 지정해야 하는지를 구성합니다.

9. 자격증명공급자: 해지 **XenMobile** 페이지에서 다음을 수행합니다.

- 발급된 인증서 해지에서 인증서를 해지할 시기를 나타내는 옵션 중 하나를 선택합니다.
- 인증서가 해지될 때 XenMobile 의 알림을 받으려면 알림 보내기의 값을 켜짐으로 설정하고 알림 템플릿을 선택합니다.
- XenMobile 에서 인증서가 해지될 때 PKI 에서 인증서를 해지하려면 **PKI** 에 대한 인증서 해지를 켜짐으로 설정하고 엔터티 목록에서 템플릿을 클릭합니다. 엔터티 목록에 해지 기능이 있는 모든 사용 가능한 GPKI 엔터티가 표시됩니다. XenMobile 에서 인증서가 해지되면 해지 요청이 엔터티 목록에서 선택된 PKI 로 전송됩니다.

10. 다음을 클릭합니다.

자격증명공급자: 해지 **PKI** 페이지가 나타납니다. 이 페이지에서 인증서가 해지된 경우 PKI 에서 수행할 동작을 식별합니다. 알림 메시지를 생성하는 옵션도 사용할 수 있습니다.

11. PKI 에서 인증서를 해지하려면 자격증명공급자: 해지 **PKI** 페이지에서 다음을 수행합니다.

- 외부 해지 확인 사용 설정을 켜짐으로 변경합니다. 해지 PKI 와 관련된 추가 필드가 나타납니다.

- **OCSP** 응답자 **CA** 인증서목록에서인증서주체의 DN(고유이름) 을클릭합니다.
DN 필드값에 XenMobile 매크로를 사용할 수 있습니다. 예를 들면 다음과 같습니다. `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`
- 인증서가해지된경우목록에서다음동작중하나를클릭하여인증서가해지될때 PKI 엔터티에서수행되게합니다.
 - 아무작업도하지않습니다.
 - 인증서를갱신합니다.
 - 장치를해지및초기화합니다.
- 인증서가해지될때 XenMobile 의알림을받으려면 알림보내기의값을 켜짐으로설정합니다.
두알림옵션중에서선택할수있습니다.
- 알림템플릿선택을선택한경우미리작성된알림메시지를선택하여사용자지정할수있습니다. 이러한템플릿은알림템플릿목록에있습니다.
- 알림세부정보입력을선택한경우고유한알림메시지를작성할수있습니다. 받는사람의전자메일주소와메시지를제공하는것외에도알림을보내는빈도를설정할수있습니다.

12. 다음을클릭합니다.

자격증명공급자: 갱신페이지가나타납니다. 이페이지에서다음을수행하도록 XenMobile 을구성할수있습니다.

- 인증서를갱신합니다. 필요한경우갱신시알림을보내고, 이미만료된인증서를필요에따라작업에서제외할수있습니다.
- 만료가임박한인증서에대한알림을실행합니다 (갱신전알림).

13. 인증서가만료될경우인증서를갱신하려면 자격증명공급자: 갱신페이지에서다음을수행합니다.

인증서가만료될때갱신에대해 켜짐을선택합니다. 추가필드가나타납니다.

- 인증서가다음기간내에있는경우갱신필드에인증서를갱신해야하는만료전까지남은일수를입력합니다.
- 필요한경우 이미만료된인증서는갱신하지않음을선택합니다. 이경우 “이미만료” 되었다는의미는인증서가해지되었다는것이아니라 **NotAfter** 날짜가지났다는것입니다. XenMobile 은내부적으로해지된인증서를갱신하지않습니다.

인증서가갱신되었을때 XenMobile 의알림을받으려면 알림보내기를 켜짐으로설정합니다. 인증서의만료가임박한경우 XenMobile 의알림을받으려면 인증서만료가다가오면알림을 켜짐으로설정합니다.

어느항목을선택하든두알림옵션중에서선택할수있습니다.

- 알림템플릿선택: 미리작성된알림메시지를선택한후사용자지정합니다. 이러한템플릿은알림템플릿목록에있습니다.
- 알림세부정보입력: 고유한알림메시지를작성합니다. 받는사람의전자메일주소, 메시지및알림을보낼빈도를제공합니다.

인증서가다음기간내에있는경우알림필드에알림을보낼인증서의만료전일수를입력합니다.

14. 저장을클릭합니다.

자격증명공급자가자격증명공급자테이블에표시됩니다.

APNs 인증서

October 21, 2019

XenMobile 에서 iOS 장치를등록하고관리하려면 Apple 의 APNs(Apple 푸시알림서비스) 인증서를설정합니다.

참고:

- Apple 의 APNs 인증서를사용하면 Apple Push Network 를통해모바일장치를관리할수있습니다. 실수로또는 의도적으로인증서를해지하면장치를관리할수없게됩니다.
- 또한 XenMobile 에서 iOS 용 Secure Mail 에대한푸시알림을사용하려면 APNs 인증서가필요합니다.
- iOS 개발자기업프로그램을사용하여모바일기기관리자푸시인증서를만든경우기존인증서를 Apple Push Certificates Portal 로마이그레이션해야하기때문에조치가필요할수있습니다.

이섹션에는단계별절차를개략적으로설명하는항목이나열되어있습니다. 다음은프로세스를요약한것입니다.

1 단계: Windows 의경우 Windows Server 2012 R2 또는 Windows 2008 R2 Server 와 Microsoft IIS 를사용하여 CSR 을생성합니다. Mac 의경우 Mac 컴퓨터에서 CSR 을생성합니다. Citrix 에서는이방법을권장합니다.

2 단계: Citrix 에 CSR 을제출합니다. Citrix 는모바일기기관리서명인증서로 CSR 에서명하고서명된파일을.plist 형식으로반환합니다.

3 단계: 서명된 CSR 을 Apple 에제출한다음 Apple 에서 APNs 인증서를다운로드합니다.

4 단계: (IIS, Mac 또는 SSL 에서) APNs 인증서를 PCKS #12(.pfx) 인증서로내보냅니다.

5 단계: APNs 인증서를 XenMobile 로가져옵니다.

중요:

인증서를만드는데사용된 Apple ID 를기록하고유지해야합니다. 또한 Apple ID 는개인 ID 가아닌회사 ID 여야합니다.

Microsoft IIS 를사용하여 CSR 을만들려면

iOS 장치에대한 APNs 인증서요청을생성하기위한첫번째단계는 CSR(인증서서명요청) 을만드는것입니다. Windows 2012 R2 또는 Windows 2008 R2 서버에서는 Microsoft IIS 를사용하여 CSR 을만들수있습니다.

1. Microsoft IIS 를업니다.
2. IIS 에대한서버인증서아이콘을두번클릭합니다.
3. 서버인증서창에서 인증서요청만들기를클릭합니다.
4. 해당하는 DN(고유이름) 정보를입력하고 다음을클릭합니다.

5. 암호화서비스공급자로 **Microsoft RSA SChannel Cryptographic Provider** 를선택하고비트길이로 **2048** 을선택한후 다음을클릭합니다.
6. 파일이름을입력하고 CSR 을저장할위치를지정한다음 마침을클릭합니다.

Mac 컴퓨터에서 CSR 을만들려면

1. macOS 를실행하는 Mac 컴퓨터의 응용프로그램 > 유틸리티에서키체인접근응용프로그램을시작합니다.
2. 키체인접근메뉴를열고 환경설정을클릭합니다.
3. 인증탭을클릭하고, **OCSP** 및 **CRL** 에대한옵션을 끄므로변경한다음환경설정창을닫습니다.
4. 키체인접근메뉴에서 인증지원 > 인증기관에서인증서요청을클릭합니다.
5. 다음과같은정보를입력하라는메시지가나타납니다.
 - 전자메일주소: 인증서관리를담당하는개인또는역할계정의전자메일주소입니다.
 - 일반이름: 호스트이름과도메인이름으로일반이름을지정합니다. 일반적으로 “www.website.com” 또는 “website.com” 과같은형식입니다. 일반이름은사이트에연결할때액세스하는웹주소와같아야합니다.
 - **CA** 전자메일주소: 인증기관의전자메일주소입니다.
6. 디스크에저장됨및 본인이키쌍정보지정옵션을선택하고 계속을클릭합니다.
7. CSR 파일의이름을입력하고컴퓨터에파일을저장한다음 저장을클릭합니다.
8. 키쌍정보를지정합니다. 2048 비트의 키크기와 **RSA** 알고리즘을선택한다음 계속을클릭합니다. APNs 인증서프로세스 의일부로 CSR 파일을업로드할준비가되었습니다.
9. 인증지원의 CSR 프로세스가완료되면 완료를클릭합니다.

OpenSSL 을사용하여 CSR 을만들려면

Mac 컴퓨터또는지원되는 Windows Server 및 Microsoft IIS 를사용하여 CSR 을생성할수없는경우 OpenSSL 을대신사용할수있습니다.

OpenSSL 을사용하여 CSR 을생성하려면먼저 OpenSSL 웹사이트에서 OpenSSL 을다운로드하고설치합니다.

1. OpenSSL 을설치한컴퓨터의명령프롬프트또는셸에서다음명령을실행합니다.

```
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.  
csr -newkey rsa:2048
```

2. 인증서이름지정정보에대한다음과같은메시지가나타납니다. 요청에따라정보를입력합니다.

```
1 You are about to be asked to enter information that will be  
   incorporated into your certificate request.  
2 What you are about to enter is what is called a Distinguished Name  
   or a DN.  
3 There are quite a few fields but you can leave some blank  
4 For some fields there will be a default value,  
5 If you enter '.', the field will be left blank.  
6 -----
```

```
7 Country Name (2 letter code) [AU]:US
8 State or Province Name (full name) [Some-State]:CA
9 Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    Customer
11 Organizational Unit Name (eg, section) [:Marketing
12 Common Name (eg, YOUR name) []:John Doe
13 Email Address []:john.doe@customer.com
```

3. 다음메시지가나타나면 CSR 개인키의암호를입력합니다.

```
1 Please enter the following 'extra' attributes
2 to be sent with your certificate request
3 A challenge password []:
4 An optional company name []:
```

CSR 서명

Apple 에인증서를제출하려면먼저 Citrix 에인증서를제출하고 XenMobile 에서사용할수있도록서명을받아야합니다.

1. 브라우저에서 [XenMobile APNs CSR 서명](#) 웹사이트로이동합니다.
2. **Upload the CSR(CSR 업로드)** 을클릭합니다.
3. 인증서를찾아선택합니다.
인증서는.pem/txt 형식이어야합니다.
4. **XenMobile APNs CSR Signing(XenMobile APNs CSR 서명)** 페이지에서 **Sign(서명)** 을클릭합니다. CSR 이서명되고구성된다운로드폴더에자동으로저장됩니다.

Apple 에서서명된 CSR 을제출하여 APNs 인증서를받으려면

Citrix 에서서명된 CSR(인증서서명요청) 을받았으면 Apple 에 CSR 을제출하여 APNs 인증서를받습니다.

참고:

일부사용자가 Apple Push Portal 로그인과관련된문제를보고했습니다. 다른방법으로, 1 단계에서 [identity.apple.com](#) 링크로이동하기전에 [Apple Developer Portal](#)에로그온할수있습니다.

1. 브라우저에서 <https://identity.apple.com/pushcert>로이동합니다.
2. **Create a Certificate(인증서생성)** 를클릭합니다.
3. Apple 에서인증서를만드는것이처음이라면 **I have read and agree to these terms and conditions(이용 약관을읽었고이에동의합니다.)** 확인란을선택하고 **Accept(동의)** 를클릭합니다.

4. **Choose File**(파일선택) 을클릭하고컴퓨터에서서명된 CSR 을찾아선택한다음 **Upload**(업로드) 를클릭합니다. 업로드가성공했다는확인메시지가나타납니다.
5. **Download**(다운로드) 를클릭하여.pem 인증서를검색합니다.
Internet Explorer 를사용중이고파일이름확장명이없는경우 **Cancel**(취소) 을두번클릭한후다음창에서다운로드하십시오.

Microsoft IIS 를사용하여.pfx APNs 인증서만들기

XenMobile 에서 Apple 의 APNs 인증서를사용하려면 Microsoft IIS 에서인증서요청을완료하고인증서를 PKCS #12(.pfx) 파일로내보낸다음 APNs 인증서를 XenMobile 로가져옵니다.

중요:

이작업에는 CSR 을생성하는데사용한 IIS 서버와동일한서버를사용합니다.

1. Microsoft IIS 를열니다.
2. 서버인증서아이콘을클릭합니다.
3. 서버인증서창에서 인증서요청완료를클릭합니다.
4. Apple 의 Certificate.pem 파일을찾아선택합니다. 그런다음친숙한이름이나인증서이름을입력하고 확인을클릭합니다. 이름에공백문자를사용하지마십시오.
5. 4 단계에서식별한인증서를선택하고 내보내기를클릭합니다.
6. .pfx 인증서의위치및파일이름과암호를지정한다음 확인을클릭합니다.
XenMobile 을설치하는동안인증서의암호가필요합니다.
7. XenMobile 을설치할서버에.pfx 인증서를복사합니다.
8. XenMobile 콘솔에관리자로로그온합니다.
9. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
10. 인증서를클릭합니다. 인증서페이지가나타납니다.
11. 가져오기를클릭합니다. 가져오기대화상자가나타납니다.
12. 가져오기메뉴에서 키저장소를선택합니다.
13. 용도에서 **APNs** 를선택합니다.
14. 키저장소파일에서 찾아보기를클릭하고파일의위치로이동하여가져올키저장소파일을선택합니다.
15. 암호에인증서에할당된암호를입력합니다.
16. 가져오기를클릭합니다.

Mac 컴퓨터에서 .pfx APNs 인증서 만들기

.p12 와 .pfx 파일은 동일하며 서로 바꿔 사용할 수 있습니다.

1. macOS 를 실행하며 CSR 을 생성하는데 사용한 Mac 컴퓨터와 동일한 컴퓨터에서 Apple 에서 받은 프로덕션 ID (.pem) 인증서를 찾습니다.
2. 인증서 파일을 두 번 클릭하여 파일을 키집합으로 가져옵니다.
3. 인증서를 특정 키집합에 추가하라는 메시지가 표시되면 기본 로그인 키집합을 선택된 상태로 두고 확인을 클릭합니다. 새로 추가한 인증서가 인증서 목록에 나타납니다.
4. 인증서를 클릭한 다음 파일 메뉴에서 내보내기를 클릭하여 인증서를 PKCS #12 (.pfx) 인증서로 내보내기 시작합니다.
5. 인증서 파일에 XenMobile Server 에서 사용할 고유 이름을 지정합니다. 이름에 공백 문자를 사용하지 마십시오. 저장된 인증서의 폴더 위치를 선택하고 .pfx 파일 형식을 선택한 후 저장을 클릭합니다.
6. 인증서를 내보낼 암호를 입력합니다. 고유하고 강력한 암호를 사용하는 것이 좋습니다. 또한 나중에 사용하고 참조할 수 있도록 인증서와 암호를 안전하게 보관하십시오.
7. 키체인 접근 응용 프로그램으로 로그인 암호 또는 선택한 키체인을 묻는 메시지가 나타납니다. 암호를 입력하고 확인을 클릭합니다. 이제 저장된 인증서를 XenMobile Server 에서 사용할 수 있습니다.

참고:

원래 CSR 을 생성하고 인증서 내보내기 프로세스를 완료하는데 사용한 컴퓨터 및 사용자 계정을 유지하지 않으려는 경우 로컬 시스템에서 개인 및 공개 키를 저장하거나 내보내는 것이 좋습니다. 그렇지 않으면 재사용이 필요한 경우 APNs 인증서에 액세스할 수 없게 되므로 전체 CSR 및 APNs 프로세스를 반복해야 합니다.

OpenSSL 을 사용하여 .pfx APNs 인증서를 만들려면

OpenSSL 을 사용하여 CSR (인증서 서명 요청) 을 만든 후에 OpenSSL 을 사용하여 .pfx APNs 인증서를 만들 수도 있습니다.

1. 명령 프롬프트 또는 셸에서 다음 명령을 실행합니다. 여기서 `Customer.privatekey.pem` 은 CSR 의 개인 키이고 `APNs_Certificate.pem` 은 방금 Apple 에서 받은 인증서입니다.

```
openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
```

2. .pfx 인증서 파일의 암호를 입력합니다. XenMobile 에 인증서를 업로드 할 때 암호를 다시 사용하므로 암호를 기억하고 있어야 합니다.
3. .pfx 인증서 파일의 위치를 기록합니다. 콘솔을 사용하여 파일을 업로드 할 수도 있도록 파일을 XenMobile Server 에 복사합니다.

XenMobile 로 APNs 인증서를 가져오려면

새 APNs 인증서를 요청하여 받은 후 APNs 인증서를 XenMobile 로 가져와 인증서를 처음으로 추가하거나 인증서를 바꿉니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 인증서를 클릭합니다. 인증서 페이지가 나타납니다.
3. 가져오기를 클릭합니다. 가져오기 대화상자가 나타납니다.
4. 가져오기 메뉴에서 키저장소를 선택합니다.
5. 용도에서 **APNs** 를 선택합니다.
6. 컴퓨터에서 .pfx 또는 .p12 파일을 찾습니다.
7. 암호를 입력하고 가져오기를 클릭합니다.

XenMobile 의 인증서에 대한 자세한 내용은 [인증서](#) 를 참조하십시오.

APNs 인증서를 갱신하려면

APNs 인증서를 갱신하려면 인증서를 만들 때와 동일한 단계를 수행합니다. 그런 다음 [Apple Push Certificates Portal](#) 을 방문하여 새 인증서를 업로드합니다. 로그인하면 기존 인증서가 표시되거나 이전 Apple Developers 계정에서 가져온 인증서를 볼 수 있습니다.

Certificates Portal 에서 인증서를 갱신할 때 유일한 차이점은 **Renew(갱신)** 를 클릭한다는 것입니다. 사이트에 액세스하려면 Certificates Portal 에 개발자 계정이 있어야 합니다. 인증서를 갱신할 때 동일한 조직 이름과 Apple ID 를 사용하는지 확인하십시오.

APNs 인증서 만료 시기를 확인하려면 XenMobile 콘솔에서 구성 > 설정 > 인증서를 클릭합니다. 인증서가 만료된 경우에도 인증서를 해지하지 마십시오.

1. IIS(Microsoft), OpenSSL 또는 키체인 접근 (macOS) 을 사용하여 CSR 을 생성합니다.
2. [XenMobile APNs CSR 서명](#) 웹사이트에서 **Request push notification certificate signature(푸시 알림 인증서 서명 요청)** 를 선택합니다.
3. **+ Upload the CSR(+ CSR 업로드)** 을 클릭합니다. 대화상자에서 CSR 로 이동하고 **Open(열기)** 을 클릭하고 **Sign(서명)** 을 클릭합니다.
4. .plist 파일이 표시되면 저장합니다.
5. **Apple Push Certificates Portal** 을 클릭하고 로그인합니다.
6. 갱신할 인증서를 선택하고 **Renew(갱신)** 를 클릭합니다.
7. .plist 파일을 업로드합니다. .pem 파일이 출력으로 표시됩니다. .pem 파일을 저장합니다.
8. 이 .pem 파일을 사용하여 CSR 을 완료합니다 (1 단계에서 CSR 을 생성할 때 사용한 방법에 따라).
9. 인증서를 .pfx 파일로 내보냅니다.

XenMobile 콘솔에서 .pfx 파일을 가져오기 다음과 같이 구성을 완료합니다.

1. 설정 > 인증서 관리로 이동합니다.
2. 인증서 페이지에서 가져오기를 클릭합니다.
3. 가져오기 메뉴에서 키저장소를 선택합니다.
4. 키저장소 유형에서 **PKCS#12** 를 선택합니다.
5. 용도에서 **APNs** 를 선택합니다.
6. 키저장소 파일에 대해 찾아보기를 클릭하고 해당 파일로 이동합니다.

7. 암호에인증서암호를입력합니다.
8. 필요한경우 설명을입력합니다.
9. 가져오기를클릭합니다.

XenMobile 의 인증서페이지로리디렉션됩니다. 이름, 상태, 유효기간시작일및 유효기간종료일필드가업데이트됩니다.

ShareFile SSO(Single Sign-on) 용 SAML

January 6, 2020

SAML(Security Assertion Markup Language) 을 사용하여 ShareFile Mobile 앱에대한 SSO(Single Sign-On) 액세스를제공하도록 XenMobile 및 ShareFile 을구성할수있습니다. 이기능에는 MDX Toolkit 으로래핑된 ShareFile 앱과 웹사이트, Outlook 플러그인또는동기화클라이언트같은래핑되지않은 ShareFile 클라이언트가포함됩니다.

- 래핑된 **ShareFile** 앱의 경우. ShareFile Mobile 앱을 통해 ShareFile 에 로그인하는 사용자는 사용자 인증과 SAML 토큰 획득을 위해 Secure Hub 로 리디렉션됩니다. 인증이 성공하면 ShareFile Mobile 앱이 SAML 토큰을 ShareFile 로 전송합니다. 초기 로그인 후 사용자는 SSO 를 통해 ShareFile Mobile 앱에 액세스할 수 있습니다. 또한 매번 로그인하지 않고도 ShareFile 의 문서를 Secure Mail 메일에 첨부할 수 있습니다.
- 래핑되지 않은 **ShareFile** 클라이언트의 경우. 웹 브라우저 또는 다른 ShareFile 클라이언트를 사용하여 ShareFile 에 로그인하는 사용자가 XenMobile 로 리디렉션됩니다. XenMobile 이 사용자를 인증하면 인증된 사용자가 받은 SAML 토큰이 ShareFile 로 전송됩니다. 초기 로그인 후 사용자는 매번 로그인하지 않고 SSO 를 통해 ShareFile 클라이언트에 액세스할 수 있습니다.

XenMobile 을 ShareFile 에 대한 SAML IdP(ID 공급자) 로 사용하려면 이 문서에 설명된 대로 ShareFile Enterprise 를 사용하여 XenMobile 을 구성해야 합니다. 또한 StorageZone 커넥터에서만 작동하도록 XenMobile 을 구성할 수 있습니다. 자세한 내용은 [XenMobile 에서 ShareFile 사용](#)에서 참조하십시오.

자세한 참조 아키텍처 다이어그램은 [아키텍처](#)를 참조하십시오.

사전 요구 사항

XenMobile 및 ShareFile 앱에서 SSO 를 구성하려면 먼저 다음과 같은 사전 요구 사항을 충족해야 합니다.

- MDX Service 또는 호환되는 버전의 MDX Toolkit(ShareFile Mobile 앱용).
자세한 내용은 [XenMobile 호환성](#)에서 참조하십시오.
- 호환되는 버전의 ShareFile Mobile 앱 및 Secure Hub
- ShareFile 관리자 계정
- XenMobile 과 ShareFile 간의 연결이 확인됨

ShareFile 액세스구성

ShareFile 를위한 SAML 을설정하기전에다음과같이 ShareFile 액세스정보를제공합니다.

1. XenMobile 웹콘솔에서 구성 > **ShareFile** 을클릭합니다. **ShareFile** 구성페이지가나타납니다. 콘솔에 ShareFile 대신 Content Collaboration 이라는용어가표시될수있습니다.

The screenshot shows the 'Content Collaboration' configuration page in the XenMobile console. The page is organized into several sections:

- Content Collaboration**: This section is currently selected. It includes a 'Domain' field with the value '.sharefile.com'. Below it is an 'Assign to delivery groups' search box with the placeholder text 'Type to search' and a search icon. A list of groups is displayed below the search box, including 'AllUsers', 'Local Policy', 'o87', and 'Local', each with an unchecked checkbox.
- Content Collaboration Administrator Account Logon**: This section contains a 'User name' field with a placeholder ending in '.com', a 'Password' field with the placeholder 'Enter new password', a green 'Test Connection' button, and a 'User account provisioning' toggle switch set to 'OFF'.
- App Internal name**: This field contains the value 'ShareFile_SAML'.
- SAML certificate**: This section includes a 'Name' field with the value 'example.com'.

At the bottom of the page, there is a footer that reads 'Advanced Content Collaboration Configuration'.

2. 다음설정을구성합니다.

- **도메인:** ShareFile 하위도메인이름을입력합니다. 예: `example.sharefile.com`.
- **배달그룹에할당:** ShareFile 에서 SSO 를사용할수있게하려는배달그룹을선택하거나검색합니다.
- **ShareFile** 관리자계정로그온
- **사용자이름:** ShareFile 관리자사용자이름을입력합니다. 이사용자는관리자권한을가지고있어야합니다.
- **암호:** ShareFile 관리자암호를입력합니다.
- **사용자계정프로비전:** XenMobile 에서사용자계정프로비전을사용하려면이설정을사용하도록설정합니다. ShareFile 사용자관리도구를사용자프로비전에서사용하려면이설정을사용하지않도록설정합니다.

참고:

ShareFile 계정이 없는 사용자가 선택한 역할에 포함되어 있는 경우 사용자 계정 프로비전을 사용하도록 설정하면 XenMobile 이해당사자의 ShareFile 계정을 자동으로 프로비전합니다. 소규모의 구성원이 있는 역할을 사용하여 구성을 테스트하는 것이 좋습니다. 이 테스트를 통해 ShareFile 계정이 없는 많은 사용자로 인한 문제를 방지할 수 있습니다.

3. 연결 테스트를 클릭하여 ShareFile 관리자 계정이 지정된 ShareFile 계정으로 인증하는 사용자 이름과 암호를 확인합니다.
4. 저장 버튼을 클릭합니다.
 - XenMobile 이 ShareFile 과 동기화되고 ShareFile 설정인 **ShareFile** 발급자/엔터티 ID 및 로그인 URL 이 업데이트됩니다.
 - 구성 > **ShareFile** 페이지에 앱 내부 이름이 표시됩니다. ShareFile.com SSO 설정 수정의 뒷부분에 설명된 단계를 완료하려면 이 이름이 필요합니다.

래핑된 **ShareFile MDX** 앱을 위한 **SAML** 설정

다음 단계는 iOS 및 Android 앱 및 장치에 적용됩니다.

1. MDX Toolkit 을 사용하여 ShareFile Mobile 앱을 래핑합니다. MDX Toolkit 으로 앱을 래핑하는 것에 대한 자세한 내용은 [Wrapping Apps with the MDX Toolkit\(MDX Toolkit 으로 앱 래핑\)](#) 을 참조하십시오.
2. XenMobile 콘솔에서 래핑된 ShareFile Mobile 앱을 업로드합니다. MDX 앱 업로드에 대한 자세한 내용은 [XenMobile 에 MDX 앱을 추가하려면](#) 을 참조하십시오.
3. 위에서 구성된 관리자 사용자 이름과 암호로 ShareFile 에 로그인하여 SAML 설정을 확인합니다.
4. ShareFile 및 XenMobile 이동일한 표준 시간대로 구성되어 있는지 확인합니다. XenMobile 이 구성된 표준 시간대를 기준으로 정확한 시간을 표시하는지 확인합니다. 그렇지 않은 경우 SSO 가 실패할 수 있습니다.

ShareFile Mobile 앱의 유효성 검사

1. 사용자 장치에서 Secure Hub 를 설치하고 구성합니다.
2. XenMobile Store 에서 ShareFile Mobile 앱을 다운로드하고 설치합니다.
3. ShareFile Mobile 앱을 시작합니다. ShareFile 은 사용자 이름이나 암호를 묻지 않고 시작됩니다.

Secure Mail 로 유효성 검사

1. 아직 완료하지 않은 경우 사용자 장치에서 Secure Hub 를 설치하고 구성합니다.
2. XenMobile Store 에서 Secure Mail 을 다운로드하여 설치하고 설정합니다.
3. 새 전자 메일 양식을 열고 **ShareFile** 에서 첨부 버튼을 누릅니다. 사용자 이름이나 암호를 묻지 않고 전자 메일에 첨부할 수 있는 파일이 표시됩니다.

다른 **ShareFile** 클라이언트를위해 **NetScaler Gateway** 구성

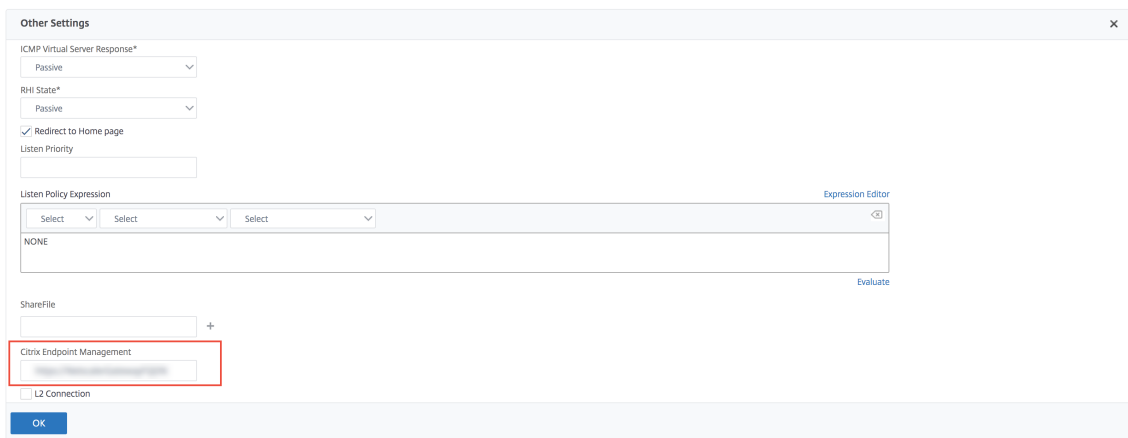
웹사이트, Outlook 플러그인또는동기화클라이언트와같이래핑되지않은 ShareFile 클라이언트에대한액세스권한을구성하려 면다음과같이 XenMobile 을 SAML ID 공급자로사용하는것을지원하도록 NetScaler Gateway 를구성합니다.

- 홈페이지리디렉션을사용하지않도록설정합니다.
- ShareFile 세션정책및프로필을만듭니다.
- NetScaler Gateway 가상서버에서정책을구성합니다.

홈페이지리디렉션사용안함

/cginfra 경로를통해수신되는요청의기본동작을사용하지않도록설정합니다. 이렇게하면사용자가구성된홈페이지대신원래요청 된내부 URL 을볼수있습니다.

1. XenMobile 로그인에사용되는 NetScaler Gateway 가상서버의설정을편집합니다. NetScaler 에서 **Other Settings**(기타설정) 로이동한다음 **Redirect to Home Page**(홈페이지로리디렉션) 확인란을선택취소합니다.



2. **ShareFile** 에서 XenMobile 내부서버의이름과포트번호를입력합니다.
3. **Citrix Endpoint Management** 아래에 XenMobile URL 을입력합니다. 사용중인 Citrix Gateway 버전에이 전제품이름인 **AppController** 가표시될수있습니다.

이구성은 /cginfra 경로를통해입력된 URL 에대한요청을인증합니다.

ShareFile 세션정책및요청프로필만들기

다음과같은설정을구성하여 ShareFile 세션정책및요청된프로필을만듭니다.

1. NetScaler Gateway 구성유틸리티의왼쪽탐색창에서 **NetScaler Gateway > Policies(정책) > Session(세션)** 을클릭합니다.
2. 세션정책을만듭니다. **Policies(정책)** 탭에서 **Add(추가)** 를클릭합니다.
3. **Name(이름)** 필드에 **ShareFile_Policy** 를입력합니다.

4. + 단추를 클릭하여 동작을 만듭니다. **Create NetScaler Gateway Session Profile(NetScaler Gateway 세션프로필 만들기)** 페이지가 나타납니다.

The screenshot shows the configuration page for a NetScaler Gateway Session Profile. The 'Name' field contains 'Sharefile_Profile'. Below this, there is a note: 'Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.' The 'Client Experience' tab is active, showing various settings: 'Accounting Policy' (dropdown), 'Display Home Page' (checked), 'Home Page' (none), 'URL for Web-Based Email' (text field), 'Split Tunnel*' (OFF), 'Session Time-out (mins)' (1), 'Client Idle Time-out (mins)' (text field), 'Clientless Access*' (Allow), 'Clientless Access URL Encoding*' (Obscure), 'Clientless Access Persistent Cookie*' (DENY), 'Plug-in Type*' (Windows/MAC OS X), 'Single Sign-on to Web Applications' (checked), 'Credential Index*' (PRIMARY), and 'KCD Account' (text field).

다음 설정을 구성합니다.

- **Name(이름): ShareFile_Profile** 을 입력합니다.
- **Client Experience(클라이언트환경)** 탭을 클릭하고 다음과 같은 설정을 구성합니다.
 - **Home Page(홈페이지): none** 을 입력합니다.
 - **Session Time-out (mins)(세션시간제한 (분)): 1** 을 입력합니다.
 - **Single Sign-on to Web Applications(웹응용프로그램에 대한 SSO):** 이 설정을 선택합니다.
 - **Credential Index(자격증명색인):** 목록에서 **PRIMARY** 를 클릭합니다.
- **Published Applications(게시된 응용 프로그램)** 탭을 클릭합니다.

Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security **Published Applications**

Override Global

ICA Proxy*
ON

Web Interface Address
https://xms.citrix.lab:8443 ?

Web Interface Address Type*
IPV4

Web Interface Portal Mode*
NORMAL

Single Sign-on Domain
citrix

Citrix Receiver Home Page

Account Services Address

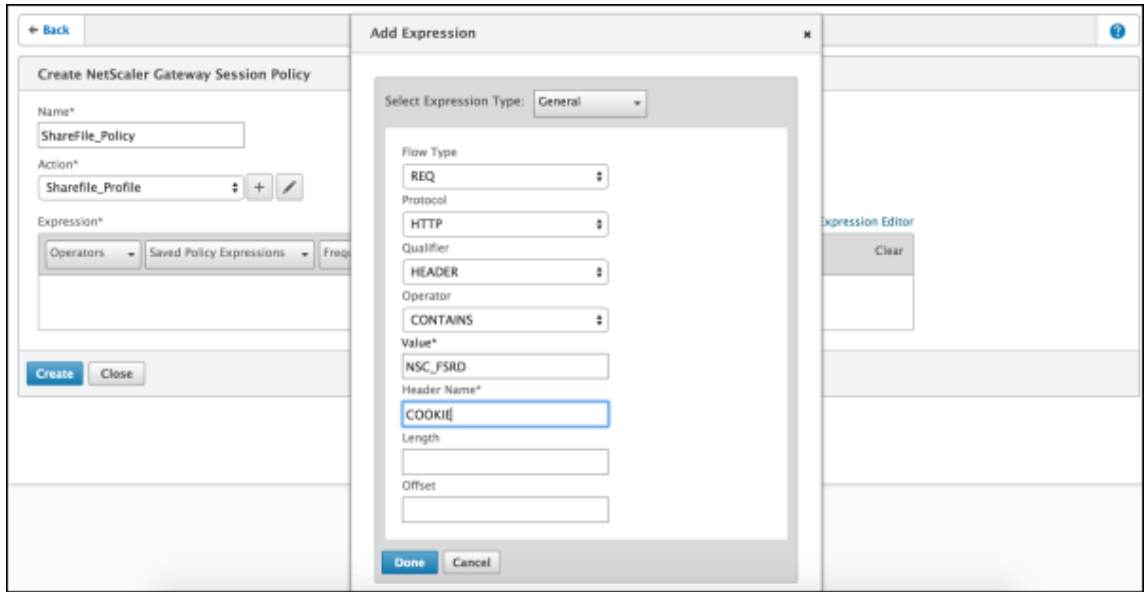
OK Close

다음설정을구성합니다.

- **ICA Proxy(ICA 프록시): ON(켜짐)** 을클릭합니다.
- **Web Interface Address(웹인터페이스주소):** XenMobile Server URL 을입력합니다.
- **Single Sign-on Domain(SSO 도메인):** Active Directory 도메인이름을입력합니다.

NetScaler Gateway 세션프로필을구성할때 **Single Sign-on Domain(SSO 도메인)** 의도메인접미사는 LDAP 에정의된 XenMobile 도메인별칭과일치해야합니다.

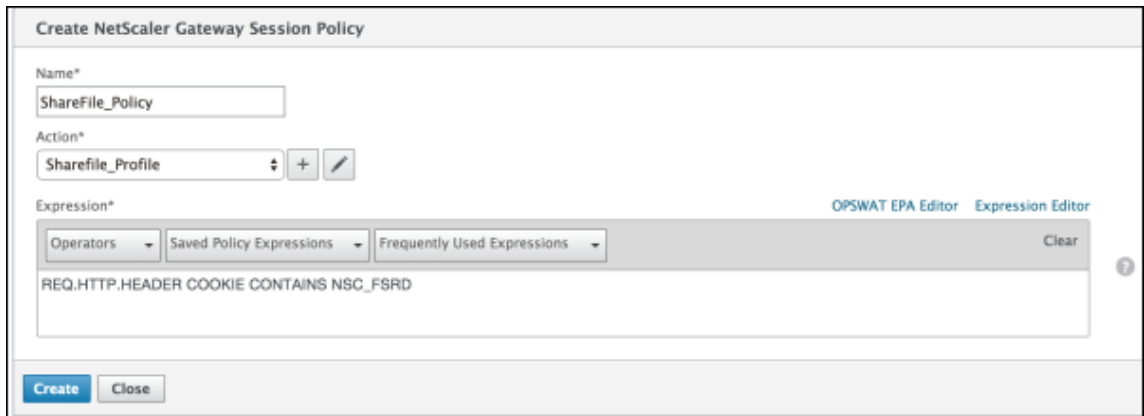
5. **Create(만들기)** 를클릭하여세션프로필을정의합니다.
6. **Expression Editor(식편집기)** 를클릭합니다.



다음설정을구성합니다.

- **Value(값): NSC_FSRD** 를입력합니다.
- **Header Name(헤더이름): COOKIE** 를입력합니다.

7. **Create(만들기)** 를클릭한다음 **Close(닫기)** 를클릭합니다.



NetScaler Gateway 가상서버에서정책구성

NetScaler Gateway 가상서버에서다음과같은설정을구성합니다.

1. NetScaler Gateway 구성유틸리티의왼쪽탐색창에서 **NetScaler Gateway > Virtual Servers(가상서버)** 를 클릭합니다.
2. **Details(세부정보)** 창에서 NetScaler Gateway 가상서버를클릭합니다.
3. 편집을클릭합니다.

4. **Configured policies**(구성된정책) > **Session policies**(세션정책) 를클릭한다음 **Add binding**(바인딩추가) 을클릭합니다.
5. **ShareFile_Policy** 를선택합니다.
6. 선택한정책의자동생성된 **Priority**(우선순위) 번호를편집하여나열된다른정책과비교하여가장높은우선순위 (가장작은 숫자) 를갓도록설정합니다. 예를들면다음과같습니다.

Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_AG_PLG_10.217.232.36_A_

7. **Done**(완료) 을클릭한다음실행중인 NetScaler 구성을저장합니다.

ShareFile.com SSO 설정수정

MDX 및비 MDX ShareFile 앱을다음과같이변경합니다.

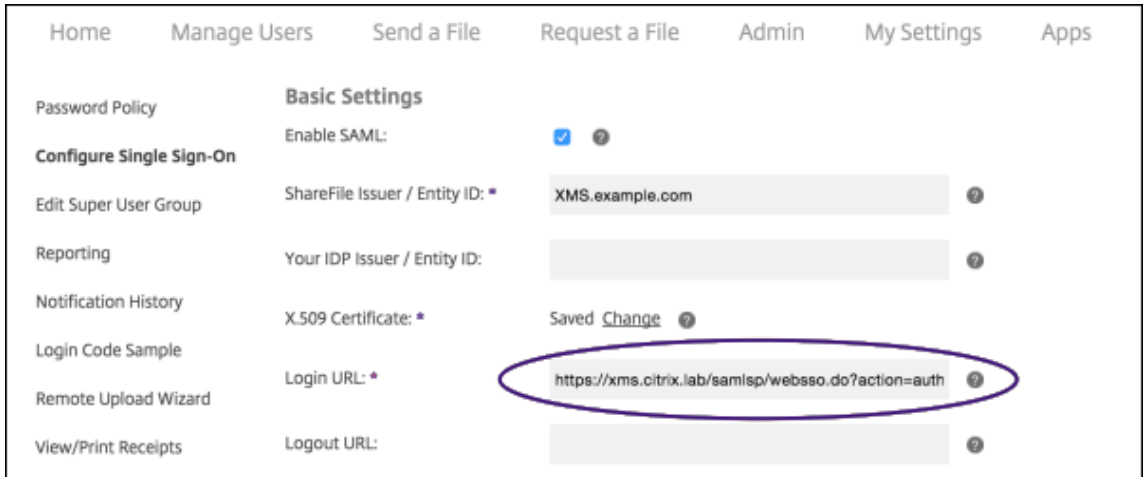
중요:

ShareFile 앱을편집또는재생성하거나 XenMobile 에서 ShareFile 설정을변경할때마다내부응용프로그램이름에새번호가추가됩니다. 그러므로 ShareFile 웹사이트에서로그인 URL 을업데이트하여업데이트된앱이름을반영해야합니다.

ShareFile 은더이상 Chrome 또는 FireFox 에서참조페이지헤더를전송하지않습니다. 자세한내용은 [릴리스정보](#), [ShareFile 웹응용프로그램 v19.17](#)에서참조하십시오.

1. ShareFile 계정 (<https://<subdomain>.sharefile.com>) 에 ShareFile 관리자로그온합니다.
2. ShareFile 웹인터페이스에서 관리를클릭한다음 **Single Sign-On** 설정구성을선택합니다.
3. **Login URL**(로그인 URL) 을다음과같이편집합니다.

다음은편집전의 로그인 URL 샘플입니다. https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



- XenMobile Server FQDN 앞에 NetScaler Gateway 가상서버외부 FQDN 과 **/cginfra/https/**를 삽입한다음 XenMobile FQDN 뒤에 **8443** 을추가합니다.

다음은 편집된 URL 의 샘플입니다. https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/webssso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

- **&app=ShareFile_SAML_SP** 매개변수를내부 ShareFile 응용프로그램이름으로변경합니다. 내부이름은기본적으로 ShareFile_SAML입니다. 그러나구성을변경할때마다내부이름에번호가추가됩니다 (ShareFile_SAML_2, ShareFile_SAML_3 등). 구성 > **ShareFile** 페이지에서 앱내부이름을찾을 수있습니다.

다음은 편집된 URL 의 샘플입니다. https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/webssso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1

- URL 끝에 **&nssso=true**를추가합니다.

다음은 최종 URL 의 샘플입니다. https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/webssso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true.

4. 옵션설정에서 웹인증사용확인란을선택합니다.

Optional Settings

Require SSO Login: ?

SSO IP Range: ?

SP-Initiated SSO certificate: HTTP Redirect with no signature ?

Enable Web Authentication: ?

SP-Initiated Auth Context: User Name and Password Minimum ?

Active Profile Cookies: ?

Save Cancel

구성유효성검사

다음을수행하여구성의유효성을검사합니다.

1. 브라우저를 <https://<subdomain>sharefile.com/saml/login>으로가리킵니다.
NetScaler Gateway 로그인양식으로리디렉션됩니다. 리디렉션되지않으면이전구성설정을확인하십시오.
2. 구성된 NetScaler Gateway 및 XenMobile 환경의사용자이름과암호를입력합니다.
ShareFile 폴더 (<subdomain>.sharefile.com) 가나타납니다. ShareFile 폴더가보이지않으면적절하로
그온자격증명을입력했는지확인하십시오.

IDP 역할을하는 Azure Active Directory

January 6, 2020

Azure AD(Active Directory) 를 IDP(ID 공급자) 로구성하면사용자가 Azure 자격증명을사용하여 XenMobile 에등록할 수있습니다.

iOS, Android 및 Windows 10 장치가지원됩니다. iOS 및 Android 장치는 Secure Hub 를통해등록됩니다.

설정 > 인증 > IDP 에서 Azure 를 IDP 로구성합니다. IDP 페이지는이버전의 XenMobile 에새롭게추가된페이지입니다. 이
전버전의 XenMobile 에서는 설정 > Microsoft Azure 에서 Azure 를추가했습니다.

요구사항

- 버전및라이선스

- iOS 또는 Android 장치를등록하려면 Secure Hub 10.5.5 가필요합니다.
- Windows 10 장치를등록하려면 Microsoft Azure Premium 라이선스가필요합니다.
- 디렉터리서비스및인증
 - XenMobile Server 가인증서기반인증을사용하도록구성해야합니다.
 - NetScaler 를인증에사용중인경우 NetScaler 가인증서기반인증을사용하도록구성해야합니다.
 - Secure Hub 인증은 Azure AD 를사용하며 Azure AD 에서정의된인증모드를따릅니다.
 - XenMobile Server 는 LDAP 를사용하여 Windows AD(Active Directory) 에연결해야합니다. 로컬 LDAP 서버가 Azure AD 와동기화되도록구성합니다.

인증흐름

장치가 Secure Hub 를통해등록되며 XenMobile 이 Azure 를 IDP 로사용하도록구성된경우:

1. 사용자가자신의장치를사용하여 Secure Hub 에서표시되는 Azure AD 로그인화면에서사용자이름과암호를입력합니다.
2. Azure AD 가사용자를확인하고 ID 토큰을보냅니다.
3. Secure Hub 는 ID 토큰을 XenMobile Server 와공유합니다.
4. XenMobile 이 ID 토큰및 ID 토큰에있는사용자정보를확인합니다. XenMobile 이세션 ID 를반환합니다.

Azure 계정설정

Azure AD 를 IDP 로사용하려면먼저 Azure 계정에로그인하고다음과같이변경합니다.

1. 사용자지정도메인을등록하고도메인을확인합니다. 자세한내용은 [Azure Active Directory 에서사용자지정도메인이름 추가](#)에서참조하십시오.
2. 디렉터리통합도구를사용하여온-프레미스디렉터리를 Azure Active Directory 로확장합니다. 자세한내용은 [Directory 통합](#) 문서를참조하십시오.

Azure AD 를사용하여 Windows 10 장치를등록하려면 Azure 계정을다음과같이변경합니다.

1. MDM 을 Azure AD 의신뢰할수있는당사자로설정합니다. 이를위해 **Azure Active Directory** > 응용프로그램을클릭한다음 추가를클릭합니다.
2. 갤러리에서 응용프로그램추가를선택합니다. 모바일기기관리로이동하고 온-프레미스 **MDM** 응용프로그램을선택합니다. 설정을저장합니다.

Citrix XenMobile Cloud 에등록한경우에도온-프레미스응용프로그램을선택합니다. Microsoft 용어에서다중테넌트가아닌모든응용프로그램은온-프레미스 MDM 응용프로그램입니다.
3. 응용프로그램에서 XenMobile Server 검색, 사용약관끝점, 앱 ID URI 를구성합니다.
 - **MDM** 검색 **URL**: <https://<FQDN>:8443/<instanceName>/wpe>
 - **MDM** 사용약관 **URL**: <https://<FQDN>:8443/<instanceName>/wpe/tou>

- 앱 ID URI: <https://<FQDN>:8443/>

4. 2 단계에서만든 온-프레미스 MDM 응용 프로그램을 선택합니다. 이 사용자의 장치 관리 옵션을 선택하여 모든 사용자 또는 특정 사용자 그룹에 대한 MDM 관리를 사용하도록 설정합니다.

Windows 10 장치에 Azure AD 를 사용하는 방법에 대한 자세한 내용은 Microsoft 문서 [Azure Active Directory 와 MDM 통합](#) 을 참조하십시오.

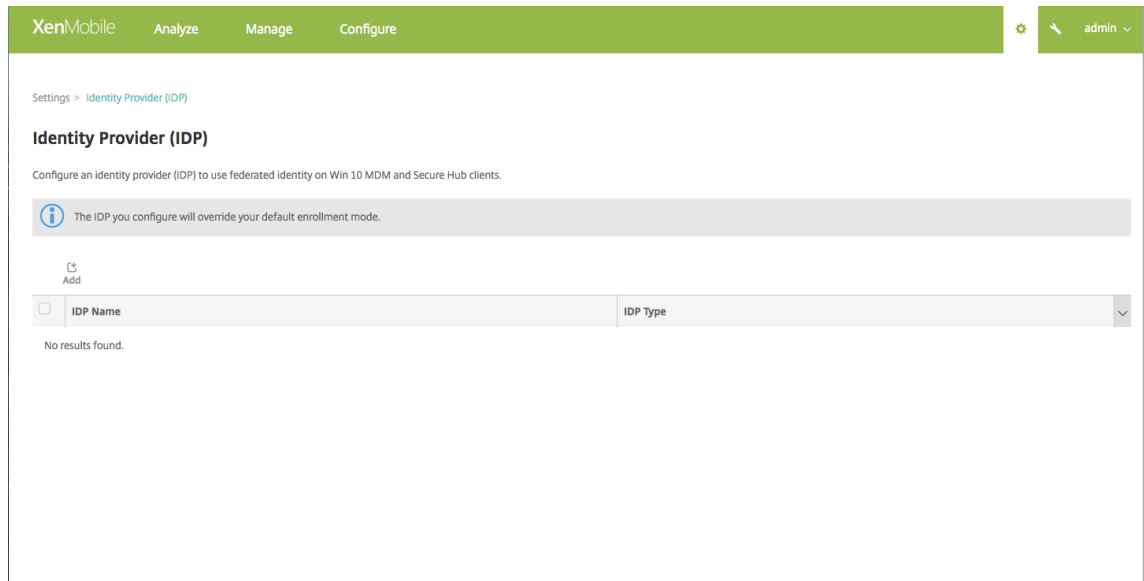
Azure AD 를 IDP 로 구성

1. Azure 계정에서 필요한 다음 정보를 찾거나 메모합니다.

- Azure 응용 프로그램 설정 페이지의 테넌트 ID.
- Azure AD 를 사용하여 Windows 10 장치를 등록하려는 경우 다음도 필요합니다.
 - 앱 ID URI: XenMobile 을 실행하는 서버의 URL 입니다.
 - 클라이언트 ID: Azure 구성 페이지에서 앱의 고유 식별자입니다.
 - 키: Azure 응용 프로그램 설정 페이지에서 확인할 수 있습니다.

2. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.

3. 인증 아래에서 **IDP (ID 공급자)** 를 클릭합니다. ID 공급자 페이지가 나타납니다.



4. 추가를 클릭합니다. IDP 구성 페이지가 나타납니다.

5. IDP 에 대한 다음 정보를 구성합니다.

- **IDP 이름:** 만들려는 IDP 연결의 이름을 입력합니다.
- **IDP 유형:** Azure Active Directory 를 IDP 유형으로 선택합니다.
- **테넌트 ID:** Azure 응용 프로그램 설정 페이지에서 이 값을 복사합니다. 브라우저 주소 표시줄에서 숫자와 문자로 구성된 섹션을 복사합니다.

예를 들어 <https://manage.windowsazure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...>에서 테넌트 ID는 abc123-abc123-abc123입니다.

6. 나머지 필드는 자동으로 입력됩니다. 입력되면 다음을 클릭합니다.

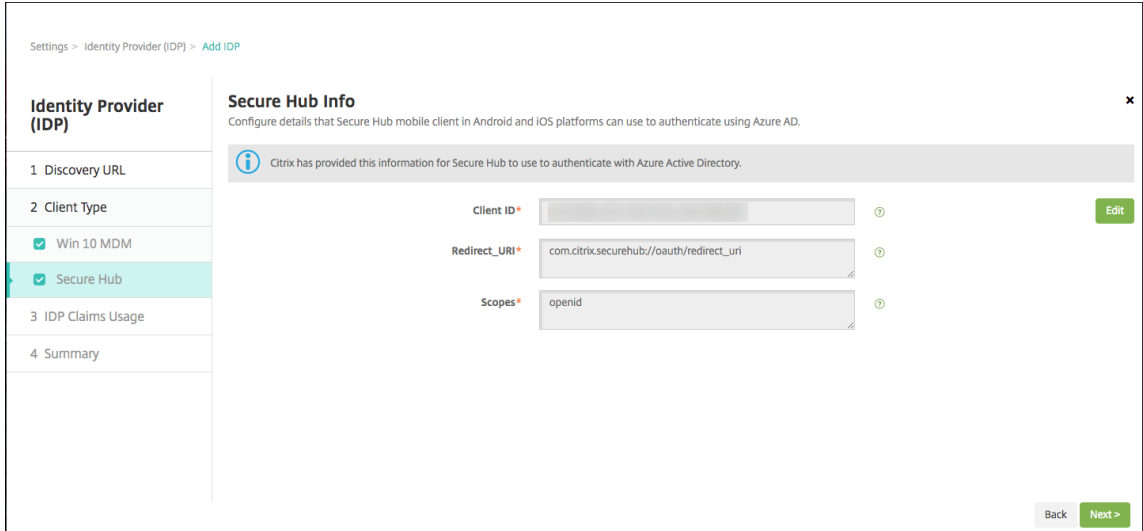
7. MDM 등록에 대해 Azure AD를 사용하여 Windows 10 장치를 등록하도록 XenMobile을 구성하려면 다음 설정을 구성하십시오. 이 선택적 단계를 건너뛰려면 **Win 10 MDM**을 선택 취소합니다.

- **앱 ID URI:** Azure 설정을 구성할 때 입력한 XenMobile Server의 URL을 입력합니다.
- **클라이언트 ID:** Azure 구성 페이지에서 값을 복사하여 붙여넣습니다. 클라이언트 ID는 앱의 고유 식별자입니다.
- **키:** Azure 응용 프로그램 설정 페이지에서 값을 복사합니다. 키 아래에 있는 목록에서 기간을 선택하고 설정을 저장합니다. 그런 다음 키를 복사하여 이 필드에 붙여넣을 수 있습니다. 앱이 Microsoft Azure AD에서 데이터를 읽거나 쓸 때 키가 필요합니다.

8. 다음을 클릭합니다.

Citrix 는 Secure Hub 를 Microsoft Azure 에등록했으며정보를유지합니다. 이화면에는 Secure Hub 가 Azure Active Directory 와통신하는데사용하는세부정보가표시됩니다. 이페이지는향후이러한정보를변경해야할때사용됩니다. Citrix 에서편집하도록안내하는경우에만이페이지를편집하십시오.

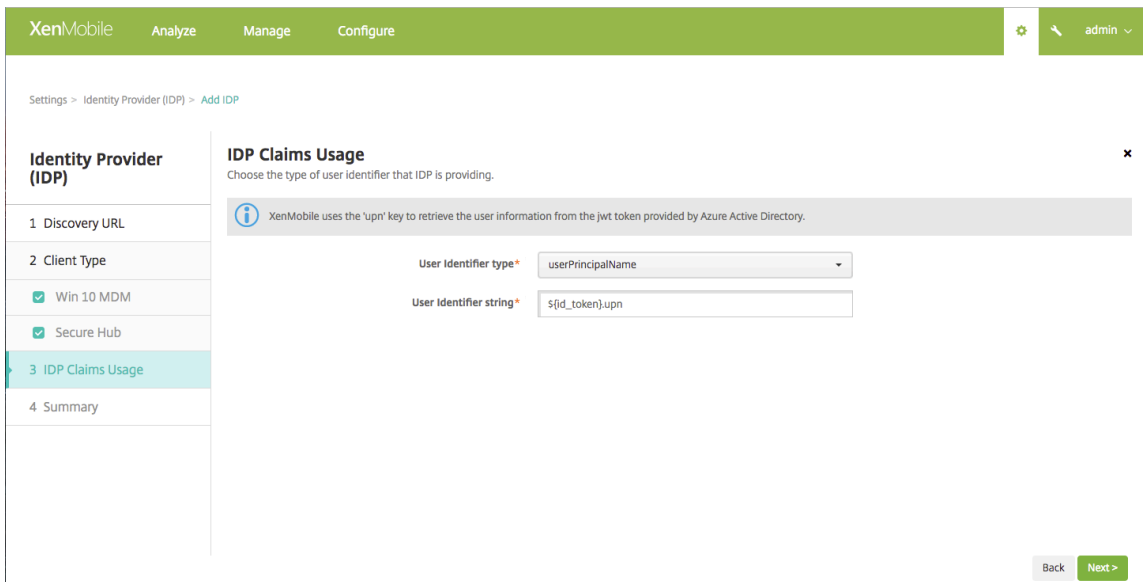
9. 다음을클릭합니다.



10. IDP 가제공하는사용자식별자유형을구성합니다.

- 사용자식별자유형: 드롭다운목록에서 **userPrincipalName** 을선택합니다.
- 사용자식별자문자열: 이필드는자동으로입력됩니다.

11. 다음을클릭합니다.



12. 요약페이지를검토하고 저장을클릭합니다.

Identity Provider (IDP)	
1 Discovery URL	
2 Client Type	
<input checked="" type="checkbox"/> Win 10 MDM	
<input checked="" type="checkbox"/> Secure Hub	
3 IDP Claims Usage	
4 Summary	

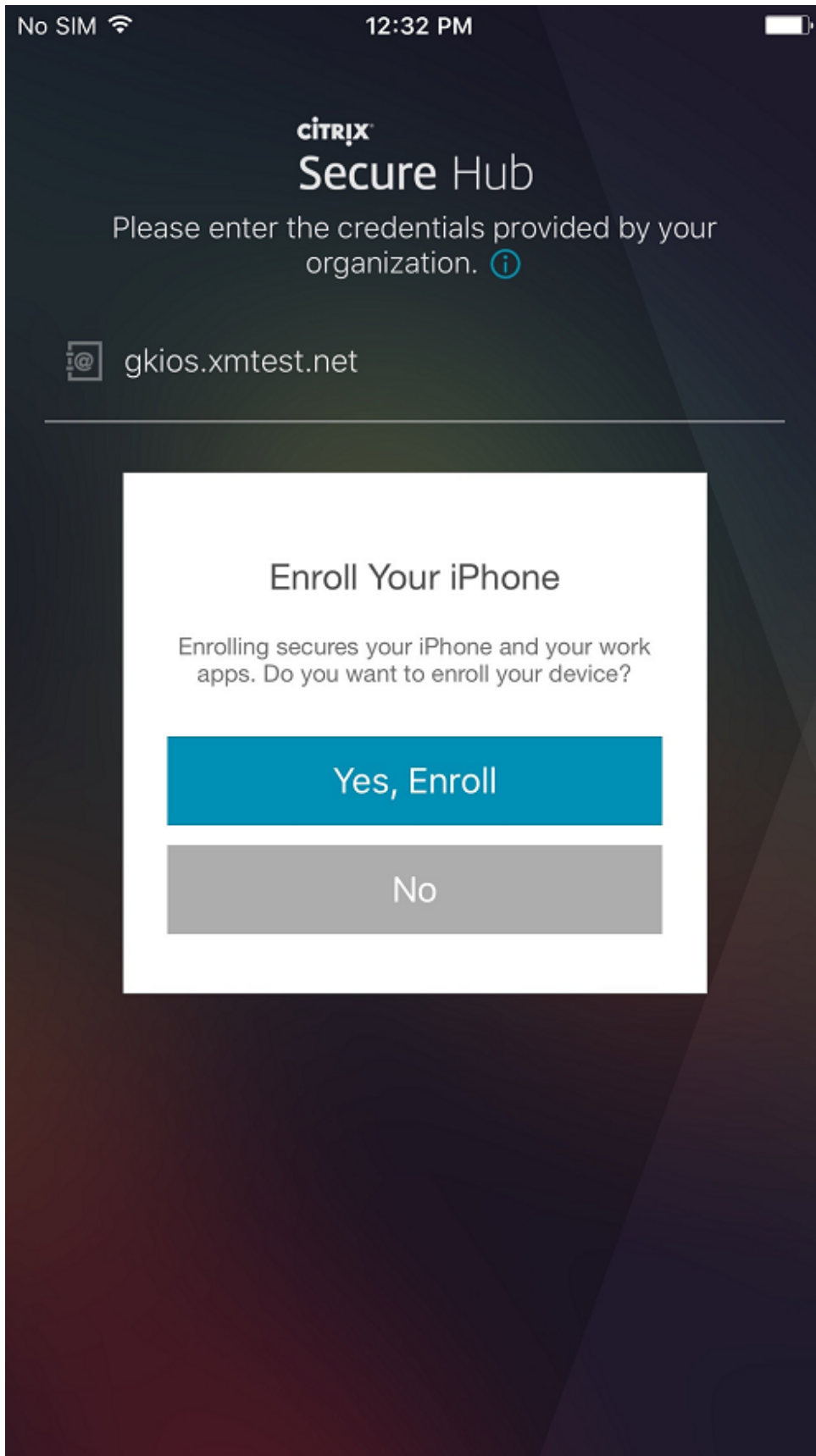
Win 10 MDM	
Token endpoint (URL)	https://login.windows.net/.../oauth2/token
jwks_uri (JSON Web Key Set URI)	https://login.windows.net/common/discovery/keys
End Session endpoint (URL)	https://login.windows.net/.../oauth2/logout

Secure Hub Info	
App ID URI	http://www.example.com
Client ID	asdf-123-example-client-id
Key	*****
Client ID	...
Client Secret (optional)	N/A
Redirect_URI	com.citrix.securehub://oauth/redirect_uri
Scopes	openid

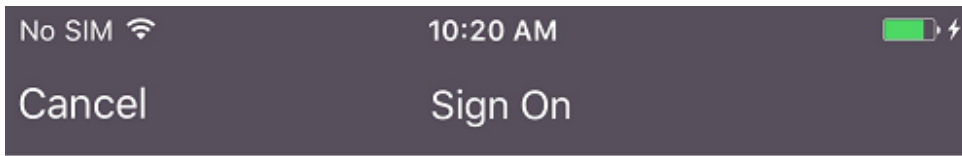
IDP Claims Usage	
User Identifier type	userPrincipalName
User Identifier string	{fid_token}.upn

사용자가 경험하는 환경

1. 사용자가 Secure Hub 를 시작합니다. 그런 다음 사용자는 XenMobile Server 의 FQDN(정규화된 도메인 이름), UPN(사용자 계정 이름) 또는 전자 메일 주소를 입력합니다.



2. 그리고 예. 등록하겠습니다를클릭합니다.



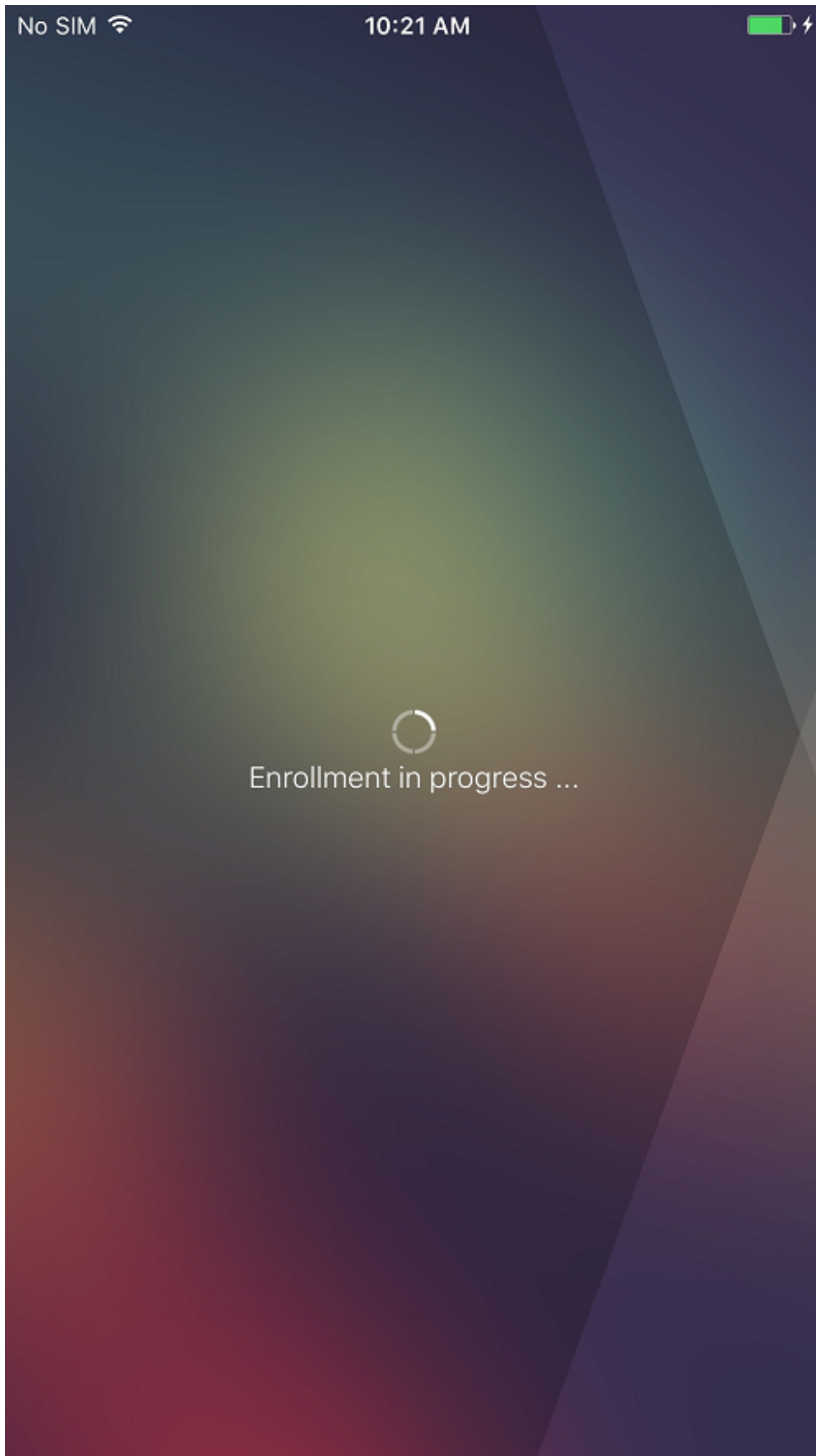
xmslab

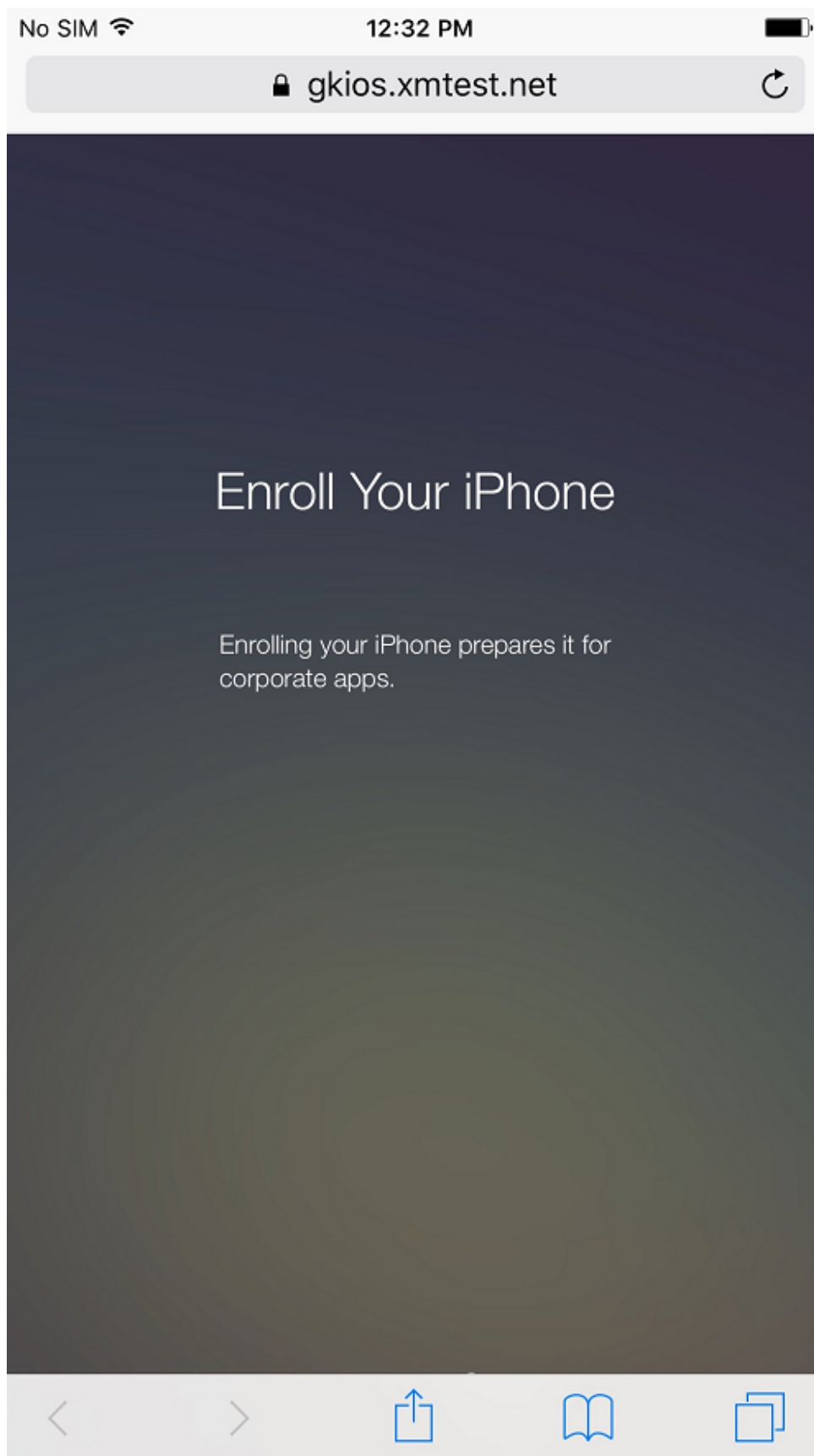
Sign in with your organizational account

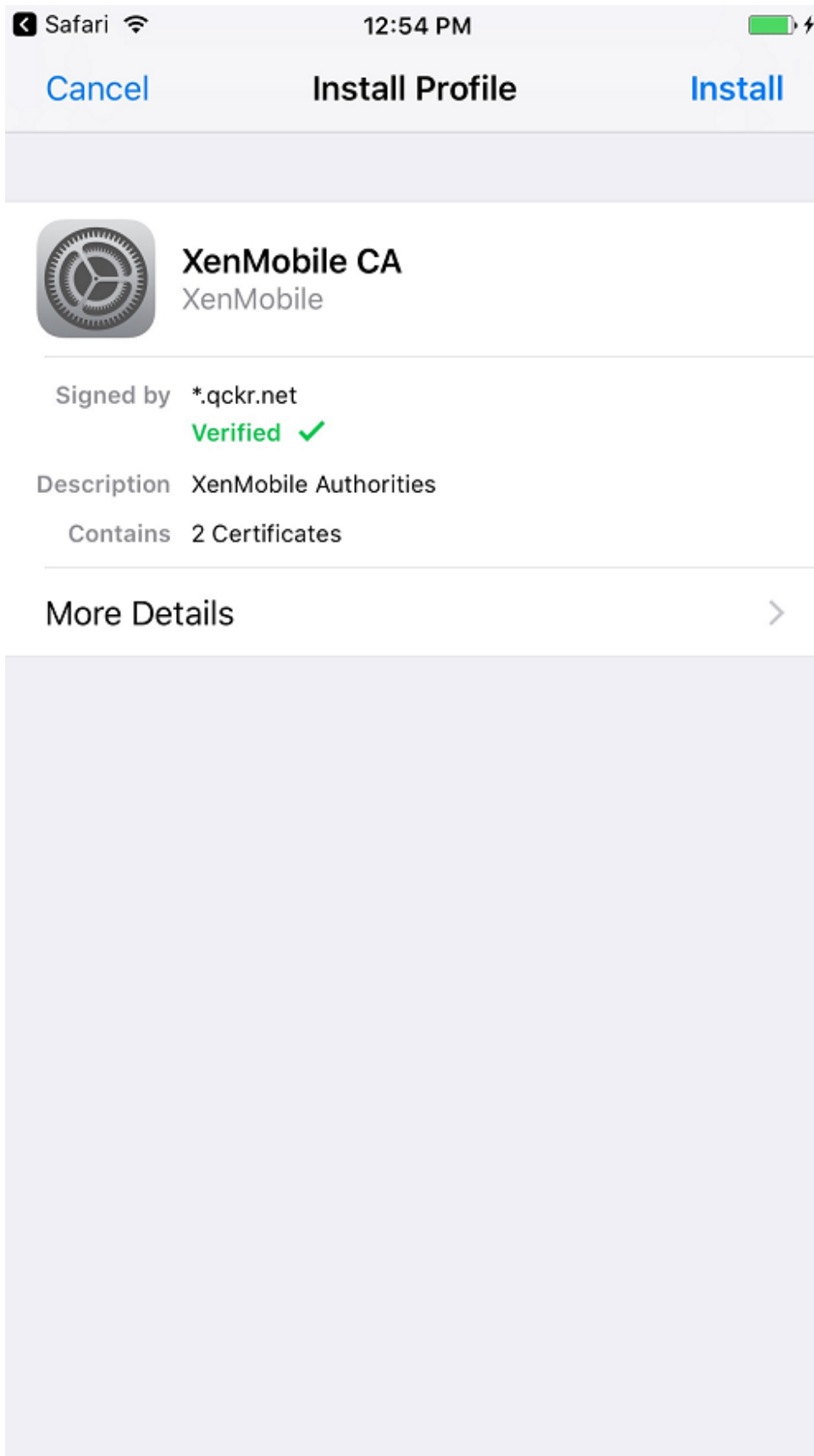
Sign in

© 2016 Microsoft

3. 사용자는 자신의 Azure AD 자격증명을 사용하여 로그인합니다.







4. 사용자는 Secure Hub 를 통한 다른 등록과 동일한 방법으로 등록 단계를 완료합니다.

참고:

XenMobile 은 등록 초대에 대해 Azure AD 를 통한 인증을 지원하지 않습니다. 사용자에게 등록 URL 이 포함된 등록 초대를 보내는 경우 사용자는 Azure AD 대신 LDAP 를 통해 인증합니다.

파생된 자격 증명

May 21, 2019

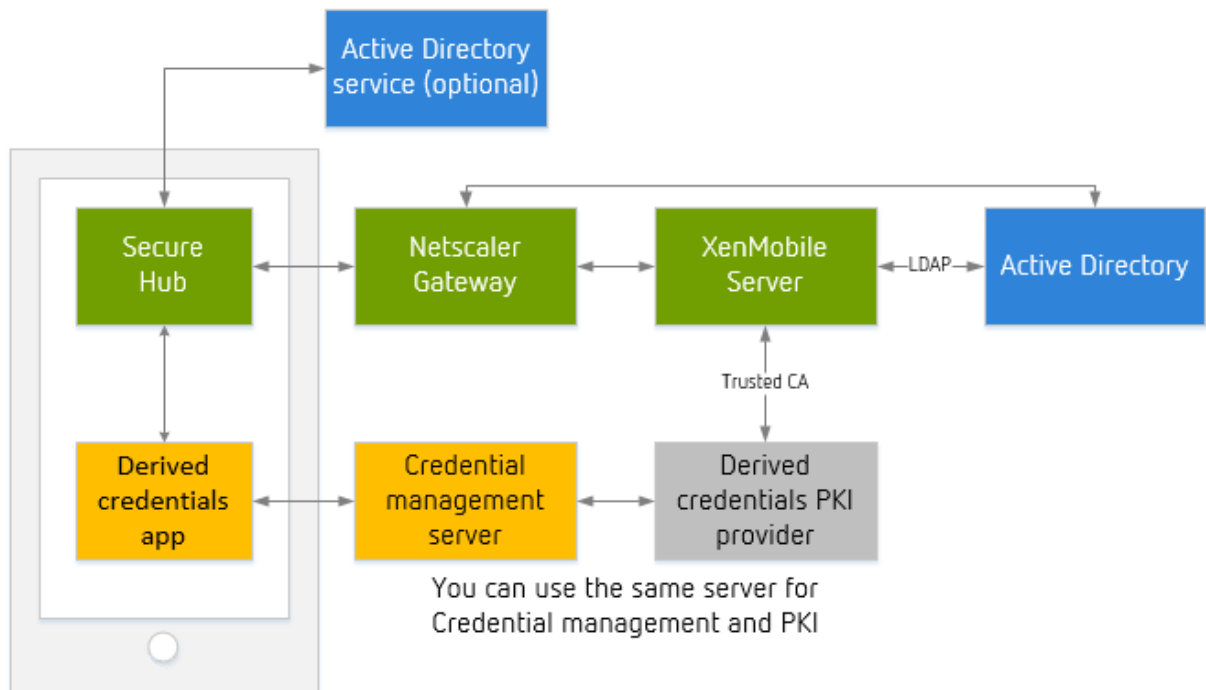
파생된 자격 증명은 모바일 장치를 위한 강력한 인증을 제공합니다. 이 자격 증명은 스마트 카드로부터 파생되어 카드가 아닌 모바일 장치에 상주합니다. 스마트 카드는 PIV(Personal Identity Verification) 카드입니다.

파생된 자격 증명은 UPN 같은 사용자 식별자가 포함된 등록 인증서입니다. XenMobile 은 자격 증명 공급자로부터 받은 자격 증명을 장치의 보안 저장소에 저장합니다.

XenMobile 은 파생된 자격 증명을 장치 등록 및 인증에 사용할 수 있습니다. 파생된 자격 증명을 사용하도록 구성하면 XenMobile 이 등록 초대 또는 기타 등록 모드를 지원하지 않습니다. iOS 를 등록하는 동안 파생된 자격 증명 앱을 사용할 수 있습니다.

아키텍처

등록을 위해 XenMobile Server 는 다음 다이어그램에서와 같이 구성 요소에 연결합니다.



- 장치 등록 도중 Secure Hub 는 파생된 자격 증명 앱에서 인증서를 가져옵니다.

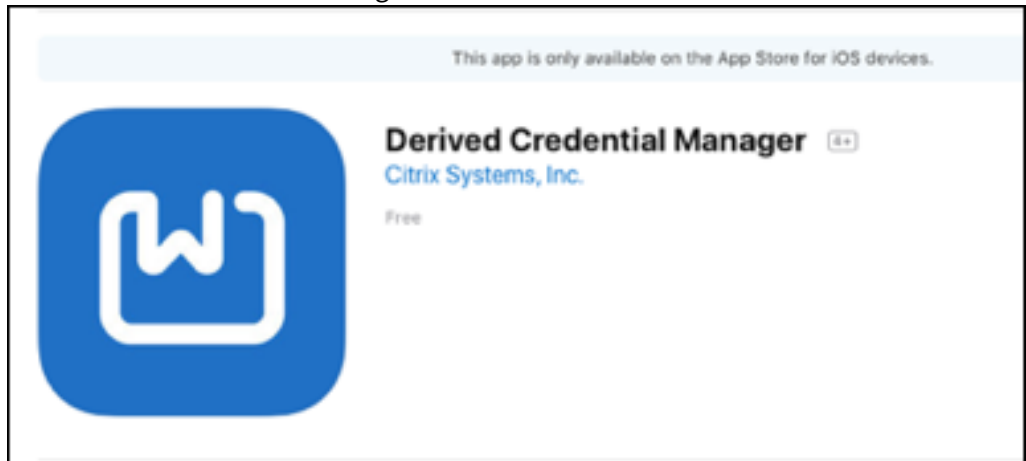
- 파생된자격증명앱은등록도중자격증명관리서버와통신합니다.
- 자격증명관리서버와타사 PKI 공급자에갈거나다른서버를사용할수있습니다.
- XenMobile Server 는타사 PKI 서버에연결하여인증서를가져옵니다.

요구사항

- Citrix Secure Hub 를다운로드하고설치합니다.
- 파생된자격증명솔루션에따라앱을다운로드하고구성합니다.

- Entrust Datacard 의경우:

- * XenMobile 에등록하기 전에 Citrix Derived Credential Manager 앱을장치에다운로드하고설치합니다. Derived Credentials Manager 앱은 Citrix 의 ID 공급자앱입니다. 해당앱의로고가나타납니다.



참고:

Citrix Derived Credential Manager 앱은신규등록만지원합니다. 장치사용자는재등록해야합니다.

- * XenMobile Server 버전 10.8 이상.
- * XenMobile Server 를엔터프라이즈모드에적합하게구성해야합니다.
- 기타파생된자격증명공급자: 다른자격증명솔루션대부분은 XenMobile 과호환될가능성이높지만운영환경에배포하기전에통합을테스트하십시오.
- 자격증명공급자서버에인증서를발급하는기관의루트인증서가있어야합니다. 이렇게설정하면 XenMobile 이등록도중디지털서명된인증서를수락할수있습니다. 인증서추가에대한자세한내용은 [인증서및인증](#)을참조하십시오.
 - 사용자전자메일도메인이 LDAP 도메인과다른경우 설정 > **LDAP** 의 도메인별칭설정에전자메일도메인을포함하십시오. 예를들어전자메일주소의도메인이 `citrix.com`이고 LDAP 도메인이름은 `sample.com`인경우 도메인별칭을 **sample.com**, **citrix.com**으로설정하십시오.
 - XenMobile 은공유장치에서파생된자격증명을사용하는것을지원하지않습니다.
- 사용자 ID 인증서:
 - 주체대체이름필드의사용자이름은 SubjectAltName 확장외 otherName, rfc822Name 또는 dNSName

필드 유형 지정되어야 합니다. 다른 필드는 지원되지 않습니다. 주체 대체 이름에 대한 자세한 내용은 RFC(<https://www.ietf.org/rfc/rfc5280.txt>) 를 참조하십시오.

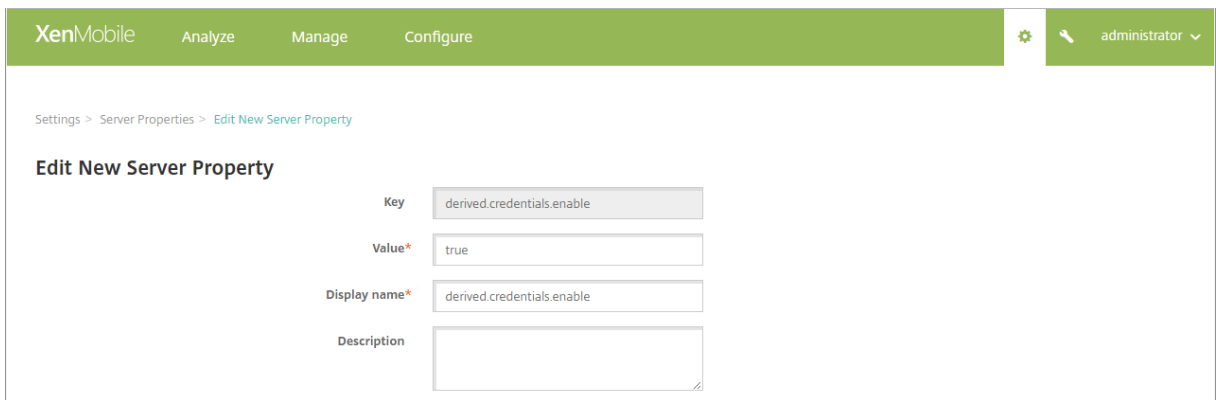
- 전자 메일 또는 CN 에서 주체 필드의 사용자 ID 는 지원되지 않습니다.
- 인증서 인증 또는 인증서와 보안 토큰 인증에 대해 구성된 Citrix Gateway

파생된 자격 증명을 사용하도록 설정

기본적으로 XenMobile 콘솔에는 설정 > 파생된 자격 증명 페이지가 포함되지 않습니다.

파생된 자격 증명에 대한 인터페이스를 사용하려면:

- 설정 > 서버 속성에서 **derived.credentials.enable** 을 서버 속성으로 추가하고 속성 값을 **true** 로 설정합니다.



파생된 자격 증명 구성

여기서는 XenMobile 과 통합할 계획인 파생된 자격 증명 공급자에 대한 작동하는 구성이 있는 것으로 가정합니다. 그러면 해당 서버와 통신하도록 XenMobile 을 구성할 수 있습니다. 이미 XenMobile 에 추가된 파생된 자격 증명 CA 인증서를 선택하거나 인증서를 가져올 수도 있습니다.

해당 CA 인증서에 대한 OCSP(Online Certificate Status Protocol) 지원을 활성화할 수 있습니다. OCSP 에 대한 자세한 내용은 [PKI 엔터티](#)의 “임의의 CA” 를 참조하십시오.

1. XenMobile 콘솔에서 설정 > **iOS** 용 파생된 자격 증명으로 이동하십시오.
2. Entrust Datacard 의 경우 파생된 자격 증명 공급자 선택에서 기타를 선택합니다. 앱 **URL(iOS)** 에 `dcapp://mode=SecureHub` 를 입력합니다.

Derived Credentials for iOS
Configure a derived credentials provider to enable iOS users to enroll with a smart card.

Provider

Choose derived credentials provider *

Intercede
 Other (tech preview)

App URL (iOS) *

Optional parameters

Name *	Value *	Add
		<input type="button" value="Add"/>

Details

Issuer CA *

CA Info
Name: C=US,O=Entrust.OU=Demonstration and Evaluation,OU=Certificate Authorities,OU=Entrust Demonstration and Evaluation Issuing CA
Expire: 2024-08-14

User Identifier field *

Subject name
 Subject alternative name

User Identifier type *

OCSP

OCSP Check OFF

3. 선택적매개변수: 일부파생된자격증명공급자의경우연결을위한매개변수를제공해야할수있습니다. 예를들어공급업체에서 백엔드서버의 URL 을지정하도록요구할수있습니다. 추가를클릭하여매개변수를제공합니다.
4. 파생된자격증명의인증서지정: 인증서가이미 XenMobile 에업로드된경우 발급자 **CA** 에서해당인증서를선택합니다. 그렇지않은경우에는 가져오기를클릭하여인증서를추가합니다. 인증서가져오기대화상자가나타납니다.
5. 인증서가져오기대화상자에서 찾아보기를클릭하여인증서로이동합니다. 그런다음 찾아보기를클릭하여개인키파일로이동합니다.

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import

Use as

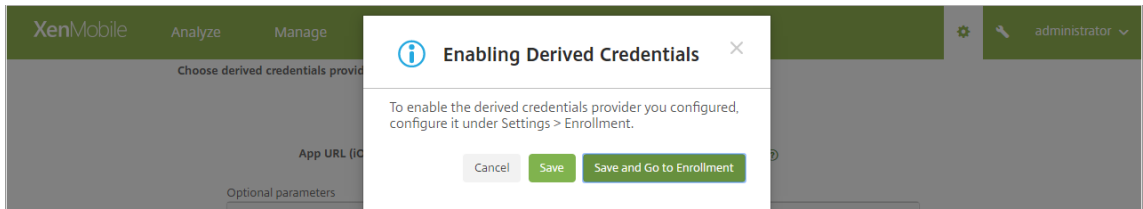
Certificate import*

Private key file

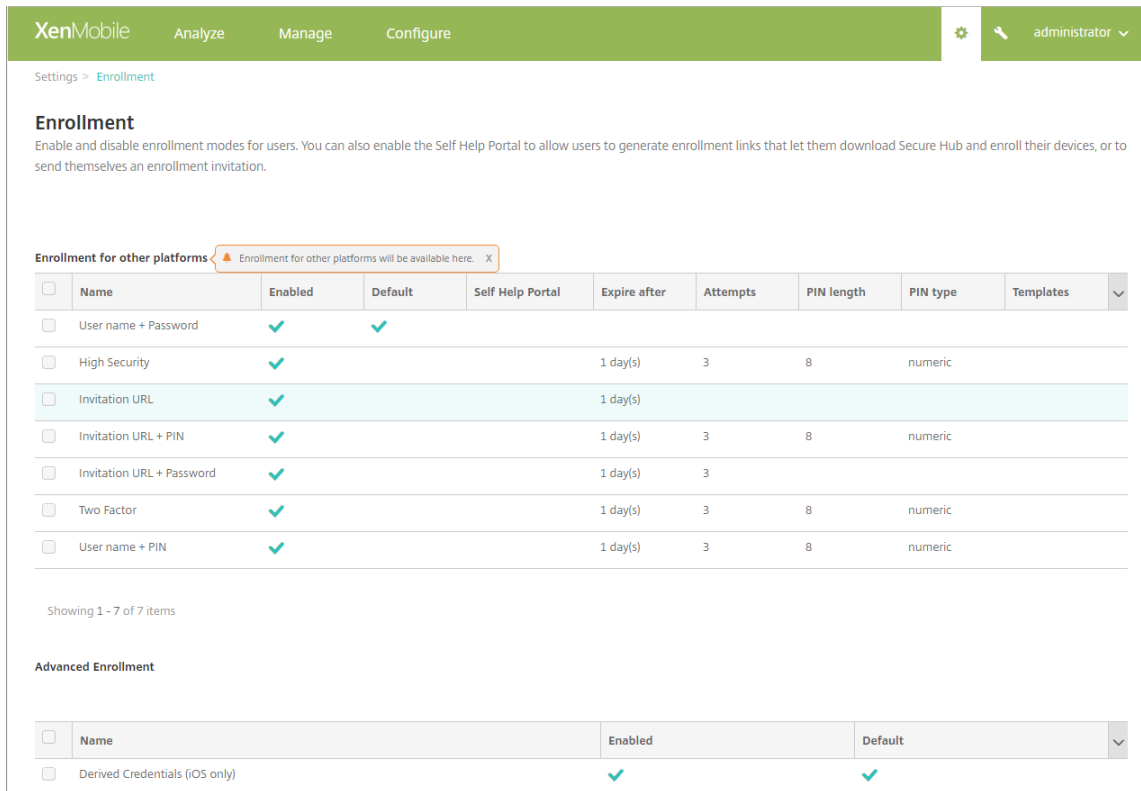
Description

6. 설정을구성합니다.
 - Citrix Derived Credential Manager 앱의경우 사용자식별자필드는 주체대체이름이고 사용자식별자유형은 **userPrincipalName** 입니다.

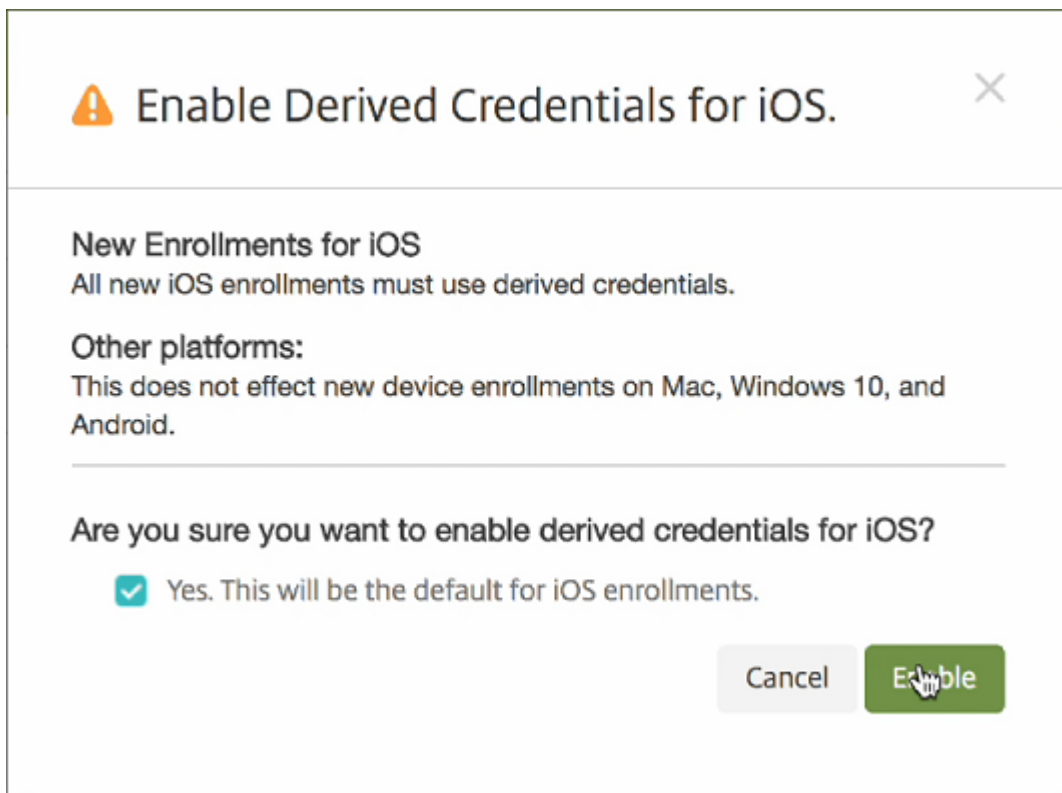
- 다른파생된자격증명공급자의경우해당공급자에정보를요청하십시오.
7. 원하는 경우 OCSP 응답자를 사용하여 인증서 해제를 확인할 수 있습니다. 보안을 위해 OCSP 응답자를 사용하는 것이 좋습니다. 기본적으로 OSP 확인은 꺼짐입니다.
- CA 인증서에 대한 OCSP 지원을 활성화하는 경우 사용자 지정 **OCSP URL** 사용에 대한 옵션을 선택합니다. 기본적으로 XenMobile 은 인증서에서 OCSP URL 을 추출합니다 (해지를 위해 인증서 정의 사용 옵션). 응답자 URL 을 지정하려면 사용자 지정 사용을 클릭하고 URL 을 입력합니다.
 - 응답자 **CA**: 응답자 **CA** 에서 인증서를 선택합니다. 또는 가져오기를 클릭한 다음 인증서가 가져오기 대화상자를 사용하여 인증서를 찾습니다.
8. 저장을 클릭합니다. 파생된 자격 증명 사용 대화상자가 나타납니다.



- 파생된 자격 증명 구성을 사용하도록 설정하려면 저장을 클릭합니다. 파생된 자격 증명을 사용하려면 등록 설정도 구성해야 합니다.
 - 파생된 자격 증명 구성을 사용하도록 설정한 다음 곧바로 설정 > 등록으로 이동하려면 저장하고 등록으로 이동을 클릭하십시오.
9. 등록에 파생된 자격 증명을 사용하도록 설정하려면: 설정 > 등록 페이지의 고급 등록 아래에서 파생된 자격 증명 (**ios 전용**) 을 선택하고 사용을 클릭합니다.



10. 확인대화상자가 나타납니다. 파생된 자격증명을 사용하도록 설정하려면 확인란을 선택하고 사용을 클릭합니다.



11. 파생된 자격증명 등록에 대한 옵션을 편집하려면 설정 > 등록으로 이동하고 파생된 자격증명 (iOS 전용) 을 선택한 다음 편집

을 클릭합니다.

파생된 자격증명을 사용하도록 설정한 후: 장치 등록 보고서의 등록 모드 열에 **derived_credentials** 가 표시됩니다.

중요:

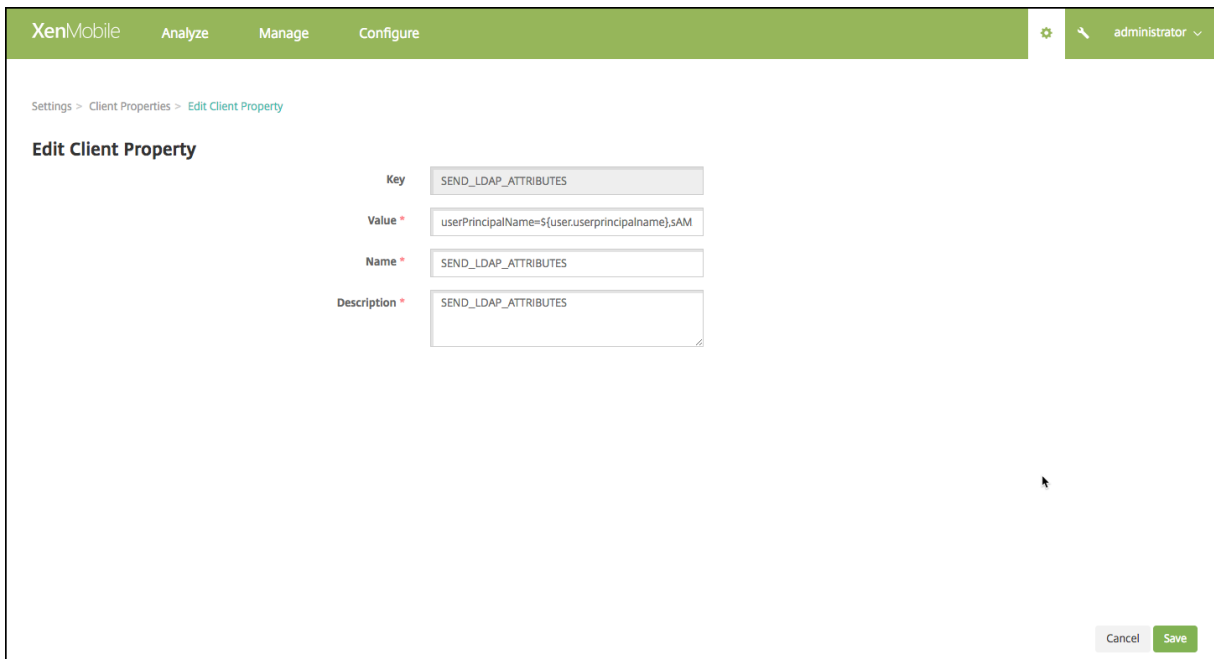
파생된 자격 증명 공급자를 추가한 후 XenMobile Server 를 다시 시작합니다.

XenMobile Server 에서 Secure Mail 구성

Secure Mail 에서 파생된 자격 증명 이 올바르게 작동하려면 LDAP 특성 클라이언트 속성을 추가해야 합니다. 클라이언트 속성 추가에 대한 자세한 내용은 [클라이언트 속성](#) 을 참조하십시오.

클라이언트 속성에 대한 다음 정보를 사용합니다.

- 키: SEND_LDAP_ATTRIBUTES
- 값: `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



iOS 장치에서 Entrust Datacard 의 파생된 자격 증명 활성화

참고:

Entrust 웹사이트를 사용하는 동안 다음을 수행합니다.

- PIV 카드를 프로그래밍하는 경우 Internet Explorer 브라우저에 Java 가 사용되는지 확인합니다.
 - PIV 카드를 변경하는 경우 브라우저 캐시를 지웁니다.
1. 새로운 스마트 자격 증명을 요청하려면 데스크톱 또는 장치를 사용하여 Entrust 사이트에 로그인합니다. 페이지 하단의 **Smart Credential Log In**(스마트 자격 증명 로그인) 버튼을 사용하여 로그인할 수 있습니다. 사용자 데스크톱에 부착된 판독기에 스마트 카드를 삽입해야 합니다.

The screenshot displays the Entrust login page. At the top, there is a 'Log In' section with a 'Sign In Using:' dropdown menu currently set to 'Corporate Domain Password'. Below this are fields for '* User Name:' and '* Password:', followed by a 'Log In' button. Underneath are four links: 'Forgot your password?', 'Perform SAML login', 'Forgot your smart credential PIN?', and 'Let me use an OTP to log in.'. The bottom section is titled 'Smart Credential Log In' and contains the instruction: 'Ensure your smart credential can be read by your computer, then click this button to log in.' A 'Log In' button in this section is highlighted with a red box. Below this button, it says 'Close your web browser when you are done.'

2. **Self-Administration Actions**(자체 관리 작업) 에서 **I'd like to enroll for a derived mobile smart credential**(파생된 모바일 스마트 자격 증명 등록) 을 선택하고 **Done**(완료) 을 클릭합니다.

Self-Administration Actions

Please select one of the actions below or click Done if you're finished:

- [I'd like to update my personal information.](#)
- [I'd like to change my question and answer pairings.](#)
- [I'd like to request a grid.](#)
- [I'd like to change my Entrust IdentityGuard password.](#)
- [I've forgotten my Entrust IdentityGuard password.](#)
- [I'd like to request a soft token.](#)
- [I'd like to unblock my smart credential.](#)
- [I'd like to activate or update my smart credential.](#)
- [I've permanently lost my smart credential or it has been compromised.](#)
- [I've temporarily forgotten or misplaced my smart credential.](#)
- [I'd like to enroll for a derived mobile smart credential.](#)

3. **Derived Mobile Smart Credential**(파생된모바일스마트자격증명) 화면에서 **Identity Name**(ID 이름) 을제 공합니다. 사용자는사용자이름또는 ID 번호와같은고유이름을선택할수있습니다.
4. Derived credential app(파생된자격증명앱) 메뉴에서 **Citrix DCAPP** 를선택하고 **Ok**(확인) 를클릭합니다.

Derived Mobile Smart Credential

Enter any name you would like to use to identify your new derived mobile smart credential identity.

* Identity Name:

Choose which app you want to associate with your new derived mobile smart credential.

* Derived Mobile Smart Credential App:

You will receive an email message, to be opened on your mobile device, that contains a link that will launch the derived mobile smart credential app with the appropriate activation data.

To unlock the activation data, you will be required to enter a password that will be provided on the next page.

The activation email message will be delivered to the account associated with citrix.com.

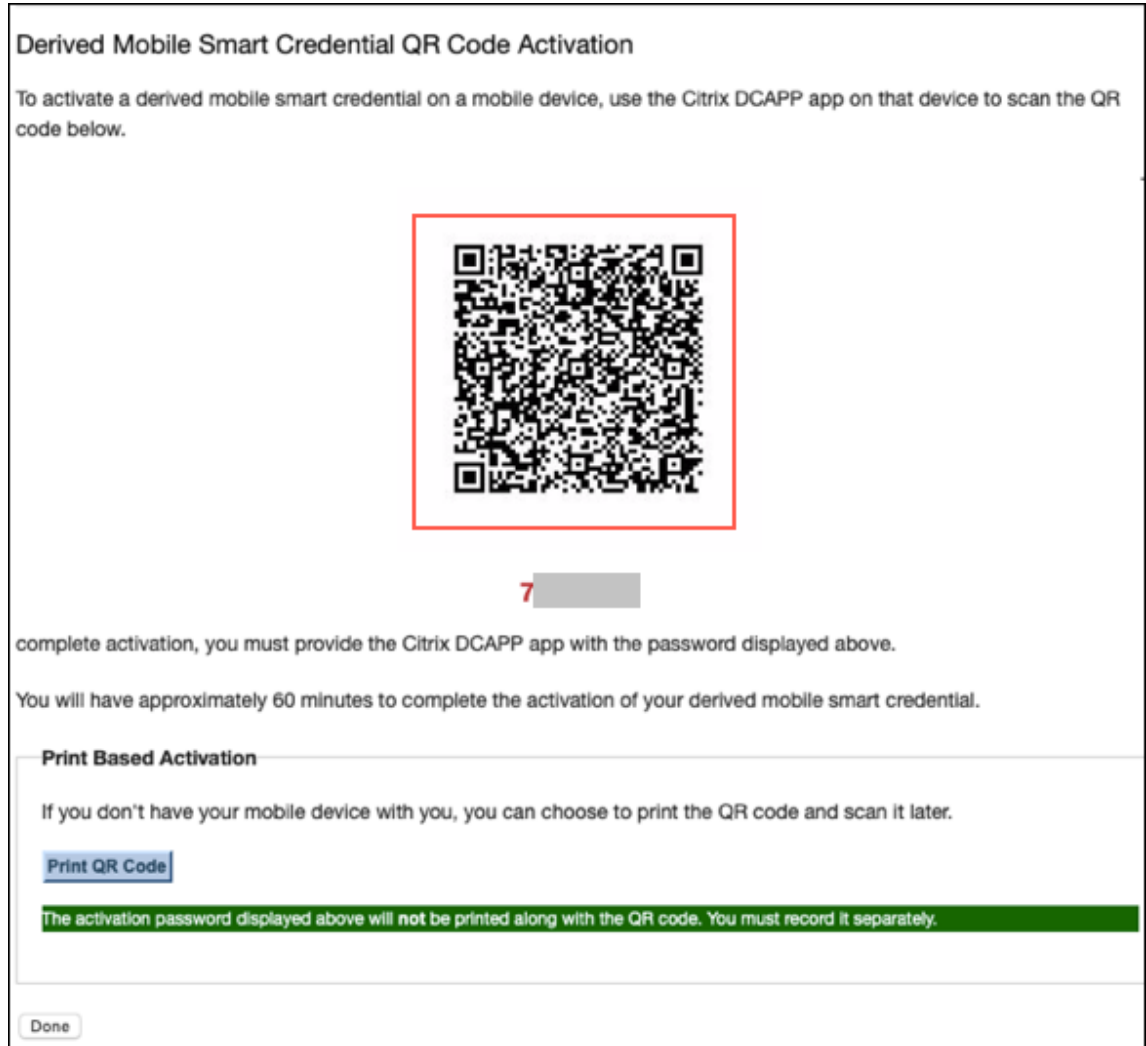
You will have approximately 60 minutes to complete the activation of your derived mobile smart credential.

QR 코드 활성화 화면이 나타나고 모바일 장치로 코드를 스캔하라는 메시지가 표시됩니다.

참고:

기본적으로 파생된 자격 증명 QR 코드는 3 분 후에 만료됩니다.

5. 장치에서 **Derived Credential Manager** 앱을 사용하여 QR 코드를 스캔하고 활성화를 완료합니다.



장치등록

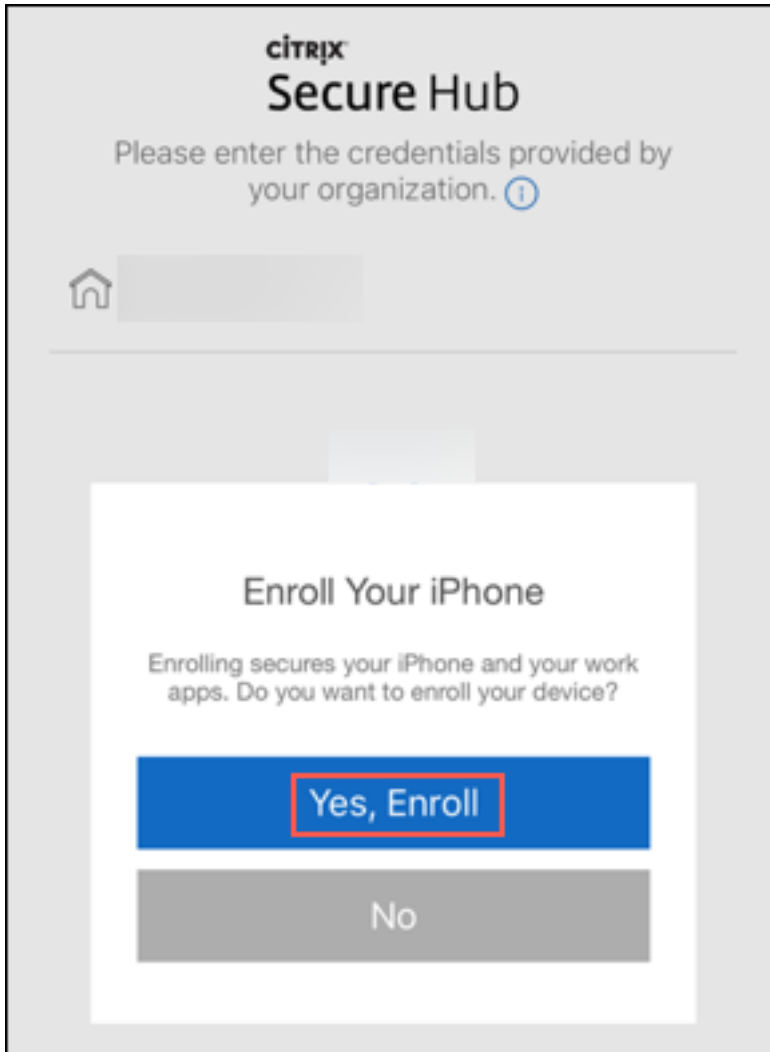
이 문서의 앞부분에 설명된 설정을 완료하면 사용자가 파생된 자격 증명을 사용하여 장치를 등록할 수 있습니다.

참고:

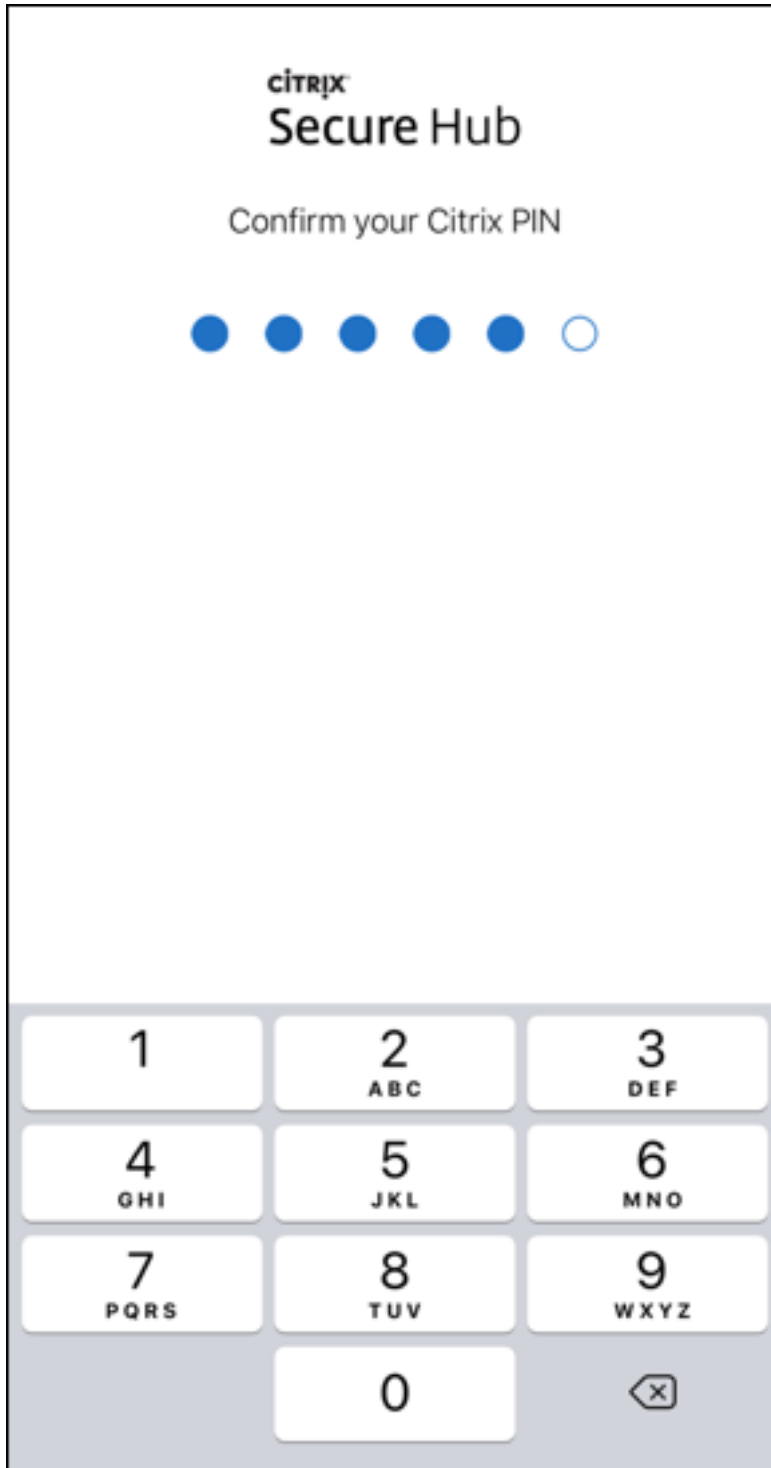
이 섹션의 스크린샷에는 Entrust Datacard 가 예로 사용되었습니다.

1. **Secure Hub** 를 눌러서 엽니다. 메시지가 나타나면 XenMobile Server FQDN(정규화된 도메인 이름) 을 입력하고 **Next(다음)** 를 클릭합니다.

2. **Yes, Enroll**(예. 등록하겠습니다) 를 클릭합니다. Secure Hub 에서장치등록이시작됩니다.

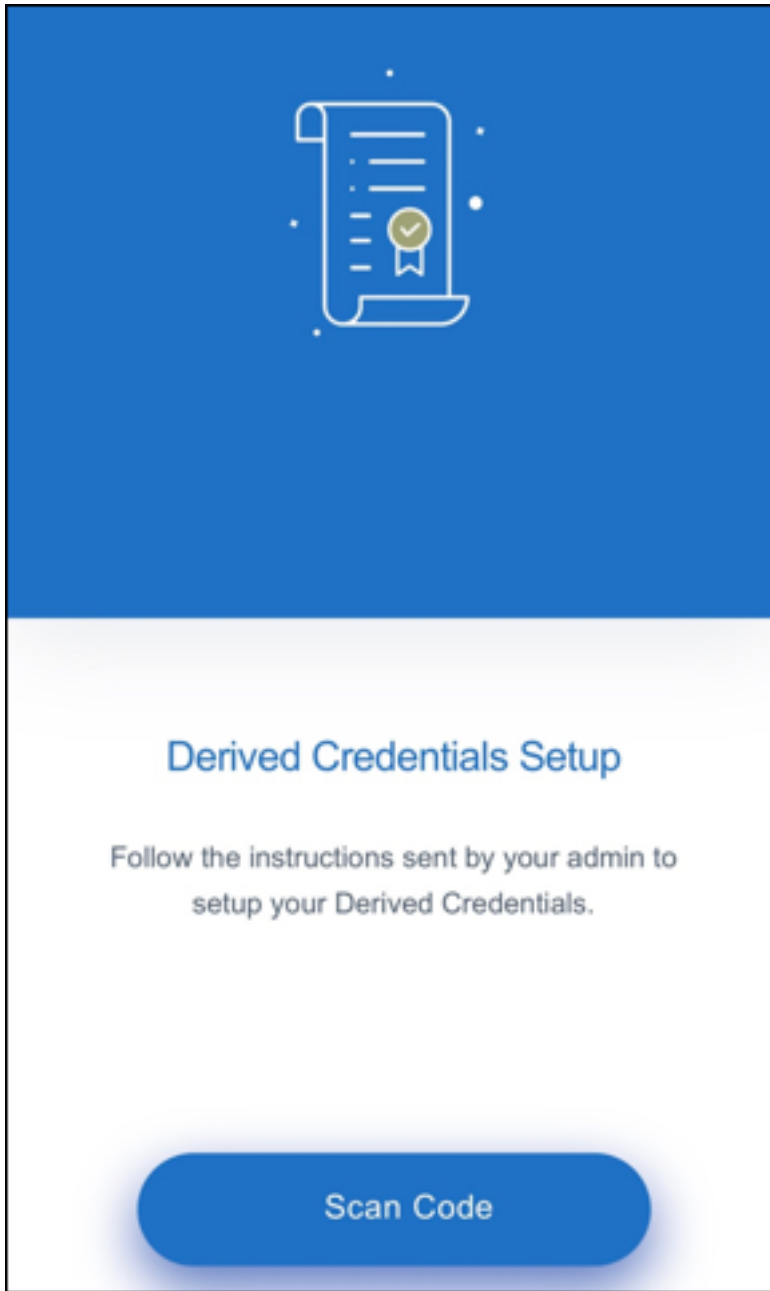


XenMobile Server 에서파생된자격증명을지원하는경우 Secure Hub 에서사용자가 Citrix PIN 을생성하고확인하도록요청하는메시지가표시됩니다.



Citrix PIN 을확인하면파생된자격증명설정시작화면이나타납니다. 지침에따라스마트자격증명을활성화합니다.

3. **Scan code(코드스캔)** 를누릅니다. 휴대폰카메라가활성화됩니다.




참고:

QR 코드를 스캔하려면 카메라와 마이크가 사용되도록 설정되었고 필요한 액세스 권한이 있는지 확인하십시오.

4. 파생 자격 증명 앱에서 이전 단계에서만 QR 코드를 스캔합니다.

Derived Mobile Smart Credential QR Code Activation

To activate a derived mobile smart credential on a mobile device, use the Citrix DCAPP app on that device to scan the QR code below.



7 [REDACTED]

complete activation, you must provide the Citrix DCAPP app with the password displayed above.

You will have approximately 60 minutes to complete the activation of your derived mobile smart credential.

Print Based Activation

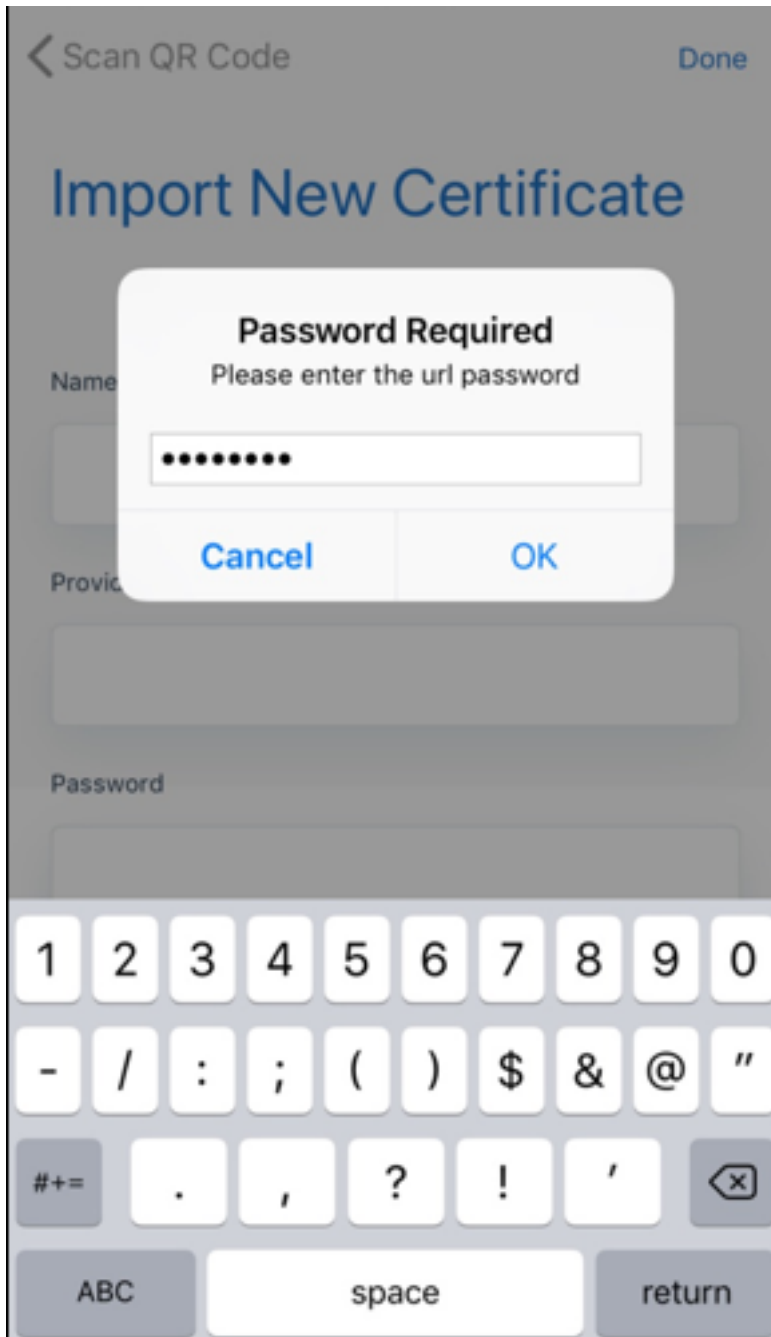
If you don't have your mobile device with you, you can choose to print the QR code and scan it later.

[Print QR Code](#)

The activation password displayed above will not be printed along with the QR code. You must record it separately.

[Done](#)

5. QR 코드를 스캔한 후 **Import New Certificate**(새인증서가져오기) 화면에서 암호 대화상자가 나타나면 암호를 입력하고 **OK**(확인) 를 클릭합니다.



Import New Certificate(새인증서가져오기) 화면이 나타나고 필드가 자동으로 채워집니다.

Import Certificates

Below are the details of certificate that you are importing into the app. Click done to confirm.

Name

DCDemo

Provider

sede

Credential ID

ET91

Import Certificates

6. 인증서가 성공적으로 추가되면 **Derived Credentials**(파생된 자격 증명) 화면에서 **Continue to Secure Hub**(Secure Hub 로 계속) 를 클릭합니다.

Derived Credentials

You have three authentication and signing certificate for authentication

🕒 23 December 2018

Enrollment Cert

Authentication

🕒 23 December 2018

SMIME Cert

Signing

🕒 23 December 2018

Encryption Cert

Encryption

[Continue to Secure Hub](#)

7. Secure Hub 에서메시지가표시되면새 PIN 을입력합니다.

PIN 인증후 Secure Hub 가인증서를다운로드합니다. 메시지에따라등록을완료합니다.

XenMobile 콘솔에서장치정보를보려면:

- 관리 > 장치로이동한다음명령상자를표시할장치를선택합니다. 자세히표시를클릭합니다.
- 분석 > 대시보드로이동합니다.

업그레이드

January 6, 2020

팁: XenMobile 마이그레이션서비스

XenMobile Server 를온-프레미스에서사용하는경우 XenMobile 마이그레이션서비스를사용하여 Endpoint Management 를시작할수있습니다. XenMobile Server 에서 Citrix Endpoint Management 로마이그레이션 할때장치를재등록할필요는없습니다.

자세한내용은해당지역의 Citrix 영업사원, 시스템엔지니어또는 Citrix 파트너에게문의하십시오. 다음블로그에 XenMobile 마이그레이션서비스에대한자세한내용이나와있습니다.

[New XenMobile Migration Service\(새로운 XenMobile 마이그레이션서비스\)](#)

[Making the Case for XenMobile in the Cloud\(클라우드에서 XenMobile 용사례만들기\)](#)

XenMobile 10.11 로업그레이드하기전에

1. 최신버전의 XenMobile Server 10.11 로업데이트하기전에 Citrix License Server 를 11.15 이상으로업데이트하십시오.

최신버전의 XenMobile 에는 Citrix License Server 11.15(최소버전) 가필요합니다.

XenMobile 10.11 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2019 년 4 월 9 일입니다. Citrix 라이선스의 Customer Success Services 날짜는이날짜보다이후여야합니다. 날짜는라이선스서버의라이선스옆에서볼수있습니다. 최신버전의 XenMobile 을이전버전의라이선스서버환경에연결하면연결확인 이실패하고라이선스서버를구성할수없게됩니다.

라이선스의날짜를갱신하려면 Citrix 포털에서최신라이선스파일을다운로드하고라이선스서버에파일을업로드하십시오. 자세한내용은 [Customer Success Services](#)에서참조하십시오.

2. 클러스터된환경의경우: iOS 11 이상을실행하는장치에 iOS 정책및앱을배포하려면다음과같은요구사항이충족되어야합니다. NetScaler Gateway 에 SSL 지속성이구성되어있으면모든 XenMobile Server 노트에서포트 80 을열어야합니다.

- 업그레이드할 XenMobile Server 를 실행하는 가상 컴퓨터의 RAM 이 4GB 미만인 경우 4GB 이상으로 RAM 을 늘리십시오. 프로덕션 환경에 권장되는 최소 RAM 은 8GB 입니다.
- XenMobile 업데이트를 설치하기 전에 VM 의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 도중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

업그레이드하려면

XenMobile 10.10.x 또는 10.9.x 에서 XenMobile 10.11 로 직접 업그레이드할 수 있습니다. 업그레이드를 수행하려면 Citrix [다운로드](#) 페이지에서 제공되는 최신 10.11 이진 파일을 사용합니다. 업그레이드를 업로드하려면 XenMobile 콘솔의 릴리스 관리 페이지를 사용합니다.

릴리스 관리 페이지를 사용하여 업그레이드하려면

릴리스 관리 페이지를 사용하여 최신 버전의 XenMobile Server 로 업그레이드합니다.

사전 요구 사항:

- 시스템 요구 사항을 검토합니다.

클러스터링된 배포의 경우 이 문서의 끝 부분에 나오는 지침을 참조하십시오.

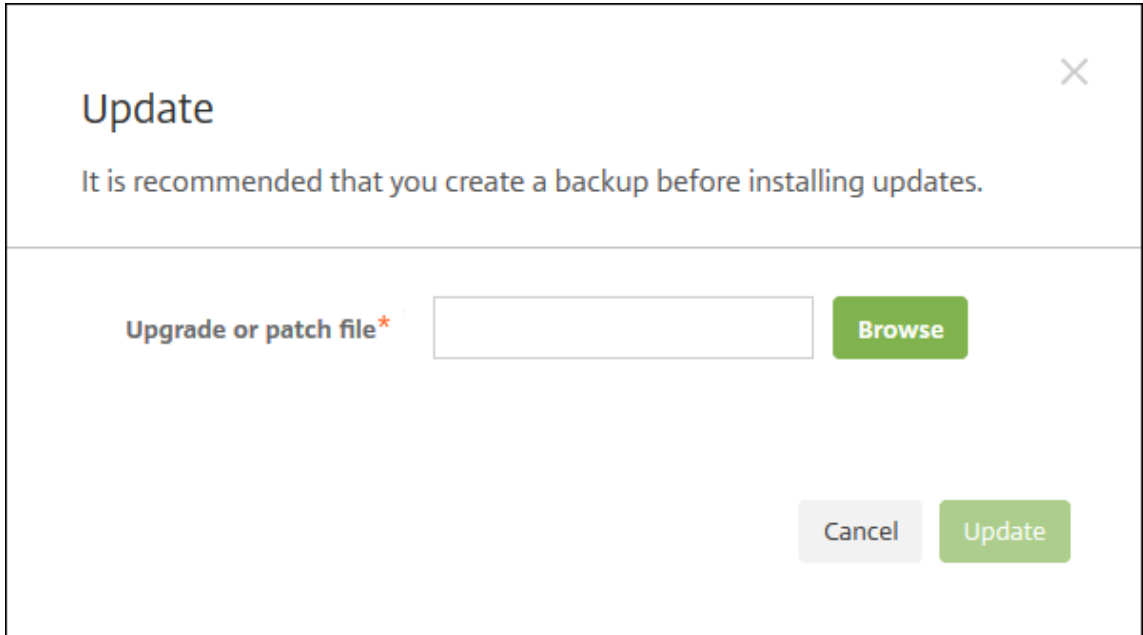
- Citrix 웹사이트에 본인 계정으로 로그인하고 [다운로드](#) 페이지로 이동합니다. XenMobile 업그레이드 (.bin) 파일을 해당 하는 위치에 다운로드합니다.
- XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
- 릴리스 관리를 클릭합니다. 릴리스 관리 페이지가 나타납니다.

The screenshot displays the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs, and a user profile 'admin'. The main content area is titled 'Release Management' and includes a sub-header 'Settings > Release Management'. Below this, there is a description: 'View the current installed release, as well as a list of all updates, patches, and upgrades to the XenMobile server up to the current date and time.' The current release information is shown as follows:

Current Release	10
Name	Release 10
Description	Software release build 10
Install date and time	Oct 26, 20 12:41 PM

Below the release information, there is an 'Updates' section with a refresh icon and the text 'Update'. At the bottom, there is a table with the following columns: Name, Release, Description, Install date and time, and Type. The table is currently empty, with the text 'No results found.' displayed below it.

- 업데이트아래에서 업데이트를클릭합니다. 업데이트대화상자가나타납니다.



- 찾아보기를클릭하고파일위치로이동하여 Citrix.com 에서다운로드한 XenMobile 업그레이드파일을선택합니다.

- 업데이트를클릭한후메시지가표시되면 XenMobile 을다시시작합니다.

몇가지이유로업데이트를성공적으로완료할수없는경우문제를나타내는오류메시지가표시됩니다. 그런다음업데이트시도 이전의상태로시스템이되돌려집니다.

업그레이드후

업그레이드한후 XenMobile 을다시시작해야합니다. XenMobile CLI 를사용하여 XenMobile Server 를다시시작합니다. 시스템을다시시작한후에는브라우저캐시를지워야합니다.

연결구성을변경하지않았는데도발신연결이관련된기능이작동을중지하는경우 XenMobile Server 로그에다음과같은오류가있는지확인하십시오. “VPP Server 에연결할수없습니다. 호스트이름 ‘192.0.2.0’ 이피어가제공한인증서제목과일치하지않습니다.”

이인증서유효성검사오류는 XenMobile Server 에서호스트이름유효성검사를비활성화해야함을나타냅니다. 기본적으로호스트이름유효성검사는 Microsoft PKI 서버를제외한발신연결에대해활성화됩니다. 호스트이름유효성검사소인해배포가중단되는 경우서버속성 **disable.hostname.verification** 을 **true** 로변경하십시오. 이속성의기본값은 **false** 입니다.

Citrix 는 XenMobile 의최신버전또는중요업데이트를 Citrix.com 에게시합니다. 또한각고객의기록된연락처로알림을전송합니다.

클러스터된 **XenMobile** 배포를업그레이드하려면

중요:

XenMobile 업데이트를 설치하기 전에 VM(가상컴퓨터) 의 기능을 사용하여 시스템 스냅샷을 생성합니다. 또한 시스템 구성 데이터베이스를 백업합니다. 업그레이드 중 문제가 발생하는 경우 전체 백업을 사용하여 복구할 수 있습니다.

시스템이 클러스터 모드로 구성된 경우 다음 단계에 따라 XenMobile 10 릴리스의 각 노드를 업데이트합니다.

1. 설정 > 릴리스 관리에서 모든 노드에 .bin 파일을 업로드합니다.
2. CLI 의 시스템 메뉴에서 모든 노드를 종료합니다.
3. CLI 의 시스템 메뉴에서 노드 하나를 시작하고 서비스가 실행되는지 확인합니다.
4. 다른 노드를 하나씩 시작합니다.

XenMobile 에서 업데이트를 성공적으로 완료할 수 없는 경우 문제를 나타내는 오류 메시지가 표시됩니다. 그런 다음 XenMobile 이 업데이트 시도 이전의 상태로 시스템을 되돌립니다.

XenMobile MDM Edition 에서 Enterprise Edition 으로 업그레이드

XenMobile MDM Edition 을 iOS 및 Android 장치용 XenMobile Enterprise Edition 으로 업그레이드할 수 있습니다.

사전 요구 사항

- 올바른 Enterprise 라이선스.
- NetScaler Gateway 가 구성되어 있음.

업그레이드하려면

1. 설정 > 라이선스로 이동하고 올바른 Enterprise Edition 라이선스 유형이 업로드되었는지 확인합니다.
2. 설정 > 서버 속성으로 이동하고 서버 모드 속성을 **MDM** 에서 **ENT** 로 변경합니다.
3. 설정 > **NetScaler Gateway** 로 이동하고 NetScaler Gateway 세부 정보를 구성합니다. 인증 모드를 MDM Edition 과 동일한 모드, 즉 도메인 인증 (Active Directory) 으로 설정합니다. XenMobile 은 사용자 등록 후의 인증 모드 변경을 지원하지 않습니다.
4. 선택 사항: 설정 > 클라이언트 속성으로 이동하고 Citrix PIN 인증을 사용하도록 설정합니다.

이 단계를 완료한 후에는 사용자가 다음 단계를 수행하여 장치를 엔터프라이즈 모드로 전환해야 합니다.

iOS 사용자

1. Secure Hub 닫기: 장치 홈 단추를 빠르게 두 번 누르고 Secure Hub 앱을 위로 밀습니다.
2. Secure Hub 를 엽니다.

Android 사용자

1. Secure Hub 를 엽니다.
2. 기본설정 > 장치정보로 이동합니다.
3. 정책새로고침을 클릭합니다.

Citrix PIN 인증을 사용하도록 설정한 경우 Secure Hub 가 PIN 을 만드라는 메시지를 사용자에게 표시합니다. 사용자가 PIN 을 생성하면 XenMobile 이 장치를 엔터프라이즈 모드로 구성합니다. 그러면 XenMobile 콘솔의 관리 > 장치 페이지에 MDM 과 MAM 이 장치의 활성 모드로 표시됩니다.

사용자 계정, 역할 및 등록

January 6, 2020

XenMobile 콘솔의 관리 탭 및 설정 페이지에서 사용자 계정, 역할 및 등록을 구성합니다. 별도로 지정되지 않은 한, 다음 작업에 대한 단계는 이 문서에서 제공됩니다.

- 사용자 계정 및 그룹:
 - 관리 > 사용자 에서 수동으로 사용자 계정을 추가하거나.csv 프로비저닝 파일을 사용하여 계정을 가져오거나 그룹을 관리합니다.
 - 설정 > 워크플로 에서 워크플로를 사용하여 사용자 계정의 생성 및 제거를 관리합니다.
- 사용자 계정 및 그룹의 역할
 - 설정 > 역할 기반 액세스 제어 에서 미리 정의된 역할 또는 권한 집합을 사용자 및 그룹에 할당합니다. 이러한 권한은 시스템 기능에 대한 사용자 액세스 수준을 제어합니다. 자세한 내용은 [RBAC 를 사용하여 역할 구성](#) 에서 참조하십시오.
 - 설정 > 알림 템플릿 에서 자동화 동작, 등록 및 사용자에게 보내는 표준 알림 메시지에 사용할 알림 템플릿을 만들거나 업데이트합니다. 세 가지 채널 (Secure Hub, SMTP 또는 SMS) 을 통해 메시지를 보내는 알림 템플릿을 구성합니다. 자세한 내용은 [알림 템플릿 만들기 및 업데이트](#) 를 참조하십시오.
- 등록 모드 및 초대
 - 설정 > 등록 에서 최대 7 개 등록 모드를 구성하고 등록 초대를 보냅니다. 각 등록 모드별로 사용자가 장치를 등록할 때 수행해야 하는 보안 수준과 단계 수가 다릅니다.
 - [XenMobile 에서 사용자 등록에 자동 검색 사용](#)

로컬 사용자 계정을 추가, 편집 또는 삭제하려면

로컬 사용자 계정을 XenMobile 에 수동으로 추가하거나 프로비저닝 파일을 사용하여 계정을 가져올 수 있습니다. 프로비저닝 파일에서 사용자 계정을 가져오는 단계는 사용자 계정 가져오기를 참조하십시오.

1. XenMobile 콘솔에서 관리 > 사용자를 클릭합니다. 사용자 페이지가 나타납니다.

<input type="checkbox"/>	User name	First name	Last name	User type	Roles	Created	Last authenticated
<input type="checkbox"/>	administrator				ADMIN	11/08/2017 08:11:00	14/08/2017 20:02:00
<input type="checkbox"/>		awsuser15	testuser	AD	USER	11/08/2017 10:27:00	11/08/2017 18:14:00
<input type="checkbox"/>		awsuser10	testuser	AD	USER	11/08/2017 18:23:00	18/08/2017 12:00:00
<input type="checkbox"/>		awsuser78	testuser	AD	USER	12/08/2017 00:40:00	12/08/2017 06:41:00

2. 필터표시를클릭하여목록을필터링합니다.

로컬사용자계정을추가하려면

1. 사용자페이지에서 로컬사용자추가를클릭합니다. 로컬사용자추가페이지가나타납니다.

Add Local User

User name*

Password

Role*

Membership

- local\Device Enrollment Program Group
- local\MSP

[Manage Groups](#)

- User Properties [Add](#)

2. 다음설정을구성합니다.

- **사용자이름:** 이름을입력합니다. 필수필드입니다. 이름에공백과대/소문자를포함할수있습니다.
- **암호:** 선택적사용자암호를입력합니다.
- **역할:** 목록에서사용자역할을클릭합니다. 역할에대한자세한내용은 [RBAC 를 사용하여역할구성](#)을참조하십시오. 사용가능한옵션은다음과같습니다.

- ADMIN
- DEVICE_PROVISIONING
- SUPPORT
- USER

- 구성원자격: 목록에서사용자를추가할그룹을클릭합니다.
- 사용자속성: 선택적사용자속성을추가합니다. 추가할각사용자속성에대해 추가를클릭하고다음을수행합니다.
 - 사용자속성: 목록에서속성을클릭하고속성옆의필드에사용자속성특성을입력합니다.
 - 완료를클릭하여사용자속성을저장하거나 취소를클릭합니다.

기존사용자속성을삭제하려면속성이포함된줄위로마우스포인터를이동하고오른쪽의 X 아이콘을클릭합니다. 속성이즉시 삭제됩니다.

기존사용자속성을편집하려면속성을클릭하고변경합니다. 완료를클릭하여변경된목록을저장하거나 취소를클릭하여목록을변경되지않은상태로유지합니다.

3. 저장을클릭합니다.

로컬사용자계정을편집하려면

1. 사용자페이지의사용자목록에서사용자를선택한후 편집을클릭합니다. 로컬사용자편집페이지가나타납니다.

2. 다음정보를적절하게변경합니다.

- 사용자이름: 사용자이름은변경할수없습니다.
- 암호: 사용자암호를변경하거나추가합니다.
- 역할: 목록에서사용자역할을클릭합니다.
- 구성원자격: 목록에서사용자계정을추가하거나편집할그룹을클릭합니다. 그룹에서사용자계정을제거하려면그룹이름옆의확인란을선택취소합니다.
- 사용자속성: 다음중하나를수행합니다.
 - 변경하려는각사용자속성에대해속성을클릭하고변경합니다. 완료를클릭하여변경된목록을저장하거나 취소를클릭하여목록을변경되지않은상태로유지합니다.
 - 추가할각사용자속성에대해 추가를클릭하고다음을수행합니다.
 - * 사용자속성: 목록에서속성을클릭하고속성옆의필드에사용자속성특성을입력합니다.
 - * 완료를클릭하여사용자속성을저장하거나 취소를클릭합니다.
 - 삭제할각기존사용자속성에대해속성이포함된줄위로마우스포인터를이동하고오른쪽의 **X** 아이콘을클릭합니다. 속성이즉시삭제됩니다.

3. 저장을클릭하여변경내용을저장하거나 취소를클릭하여사용자를변경되지않은상태로유지합니다.

로컬사용자계정을삭제하려면

1. 사용자페이지의사용자목록에서사용자계정을클릭하여선택합니다.

각사용자계정옆의확인란을선택하여둘이상의사용자계정을선택하고삭제할수있습니다.

1. 삭제를클릭합니다. 확인대화상자가나타납니다.
2. 삭제를클릭하여사용자계정을삭제하거나 취소를클릭합니다.

Active Directory 사용자삭제

한번에한명이상의 Active Directory 사용자를삭제하려면사용자를선택하고 삭제를클릭합니다.

장치가등록되어있는사용자를삭제한후해당장치를재등록하려면재등록하기전에해당장치를삭제하십시오. 장치를삭제하려면 관리 > 장치에서장치를선택한다음 삭제를클릭합니다.

사용자계정가져오기

프로비저닝파일이라고하는.csv 파일을수동으로만들어로컬사용자계정및속성을가져올수있습니다. 프로비저닝파일형식에대한 자세한내용은프로비저닝파일형식을참조하십시오.

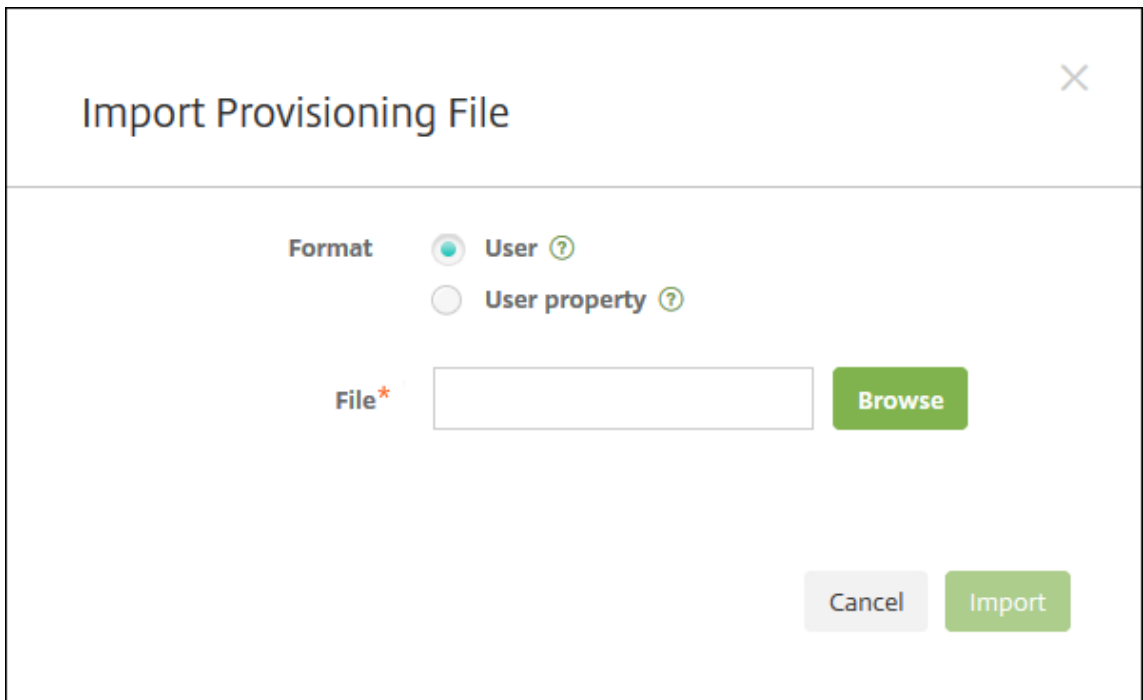
참고:

- 로컬사용자의경우가져오기파일에서사용자이름과함께도메인이름을사용합니다. 예를들어 username@domain 을지정합니다. 만들거나가져오는로컬사용자가 XenMobile 에서관리되는도메인에대한사용자인경우해당사용자는해당하는 LDAP 자격증명을사용하여등록할수없습니다.

- XenMobile 내부사용자디렉터리로사용자계정을가져오는경우기본도메인을사용하지않으면가져오기프로세스속도가빨라집니다. 도메인을사용하지않도록설정하면등록에영향을미치므로내부사용자가가져오기가완료된후기본도메인을다시사용하도록설정해야합니다.
- 로컬사용자는 UPN(사용자계정이름) 형식을사용할수있습니다. 그러나관리되는도메인은사용하지않는것이 좋습니다. 예를들어 example.com 이관리되는경우이 UPN 형식 (user@example.com) 으로로컬사용자를만들지 마십시오.

프로비저닝파일을준비한후다음단계에따라 XenMobile 로파일을가져옵니다.

1. XenMobile 콘솔에서 관리 > 사용자를클릭합니다. 사용자페이지가나타납니다.
2. 로컬사용자가가져오기를클릭합니다. 프로비저닝파일가져오기대화상자가나타납니다.



3. 가져오는프로비저닝파일의형식으로 사용자또는 속성을선택합니다.
4. 찾아보기를클릭하고파일위치로이동하여사용할프로비저닝파일을선택합니다.
5. 가져오기를클릭합니다.

프로비저닝파일형식

XenMobile 로사용자계정및속성을가져오기위해수동으로만들어사용하는프로비저닝파일은다음형식중하나여야합니다.

- 사용자프로비저닝파일필드: user;password;role;group1;group2
- 사용자특성프로비저닝파일필드: user;propertyName1;propertyValue1;propertyName2;propertyValue2

참고:

- 프로비저닝파일내의필드는세미콜론 (;) 으로구분합니다. 필드자체에세미콜론이포함되는경우백슬래시문자 (\) 로 이스케이프처리합니다. 예를들어 **propertyV;test;1;2** 속성은프로비저닝파일에 **propertyV\;test\;1\;2** 로 입력합니다.
- 역할의유효한값은미리정의된 USER, ADMIN, SUPPORT 및 DEVICE_PROVISIONING 과정의된다른역할입니다.
- 그룹계층을만들때는마침표문자 (.) 를구분기호로사용합니다. 그룹이름에는마침표를사용하지마십시오.
- 특성프로비저닝파일의속성특성에는소문자를사용합니다. 데이터베이스는대/소문자를구분합니다.

사용자프로비저닝콘텐츠의예

`user01;pwd\\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` 항목은다음의의미합니다.

- 사용자: user01
- 암호: pwd;01
- 역할: USER
- 그룹:
 - myGroup.users01
 - myGroup.users02
 - myGroup.users.users01

또다른예로 `AUser0;1.password;USER;ActiveDirectory.test.net`은다음의의미합니다.

- 사용자: AUser0
- 암호: 1.password
- 역할: USER
- 그룹: ActiveDirectory.test.net

사용자특성프로비저닝콘텐츠의예

`user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` 항목은다음의의미합니다.

- 사용자: user01
- 속성 1
 - 이름: propertyN
 - 값: propertyV;test;1;2
- 속성 2:
 - 이름: prop 2
 - 값: prop2 value

등록모드를구성하려면

장치등록모드를구성하여사용자가 XenMobile 에장치를등록하는것을허용할수있습니다. XenMobile 은사용자가장치를등록할때수행해야하는보안수준과단계가다른 7 개모드를제공합니다. 일부모드는자가지원포털에서사용할수있도록제공할수있습니다. 사용자는포털에로그온하여장치를등록하거나등록초대를보내는데사용되는등록링크를생성할수있습니다. XenMobile 콘솔의 [설정 > 등록페이지](#)에서등록모드를구성할수있습니다.

등록초대는 [관리 > 등록초대페이지](#)에서보낼수있습니다. 자세한내용은 [등록초대보내기](#)에서참조하십시오.

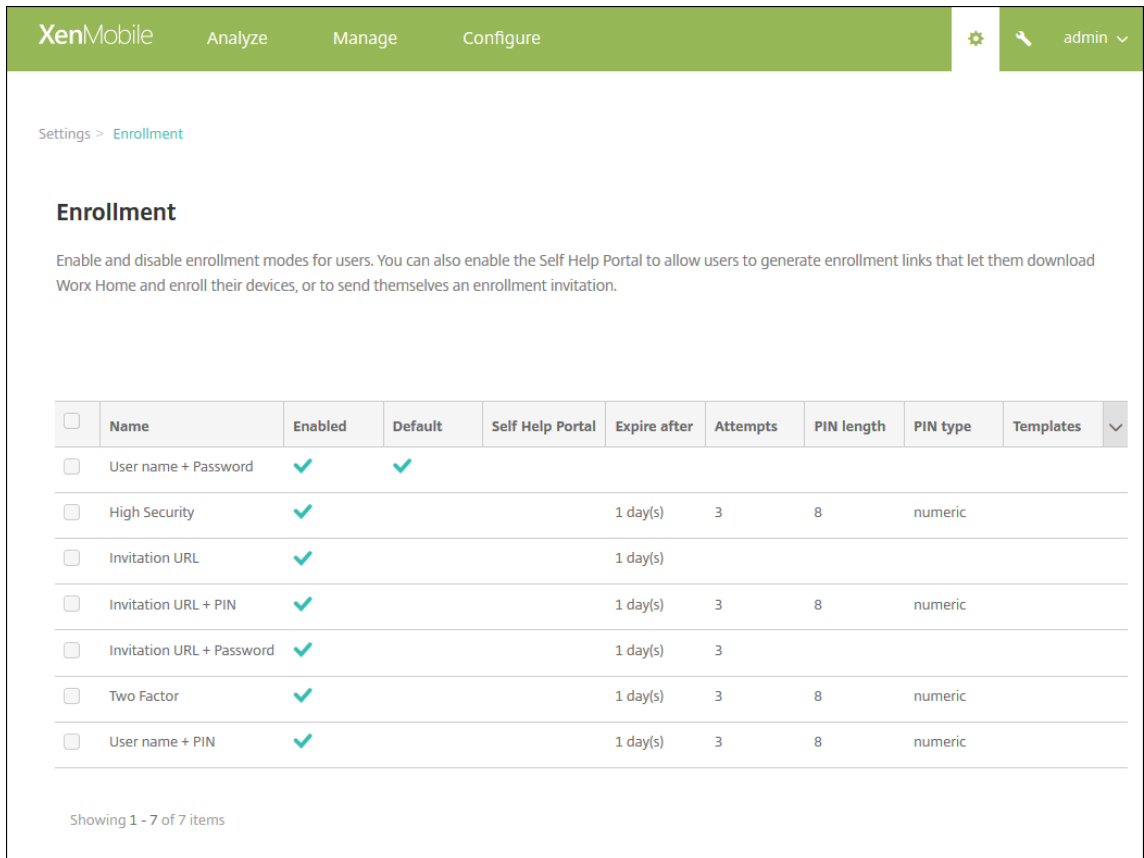
참고:

사용자지정알림플릿을사용하려는경우등록모드를구성하기전에템플릿을설정해야합니다. 알림플릿에대한자세한내용은 [알림플릿만들기또는업데이트](#) 문서를참조하십시오.

1. XenMobile 콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 등록을클릭합니다. 사용가능한모든등록모드레이블이포함된 등록페이지가나타납니다. 기본적으로모든등록모드가사용됩니다.
3. 목록에서등록모드를선택하여편집합니다. 그런다음모드를기본값으로설정하거나모드를사용하지않도록설정하거나자가지원포털을 통한 사용자 액세스를 허용합니다.

참고:

등록모드옆의확인란을선택하면등록모드목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.



다음등록모드중에서선택합니다.

- 사용자이름 + 암호
- 높은수준의보안
- 초대 URL
- 초대 URL + PIN
- 초대 URL + 암호
- 2 단계
- 사용자이름 + PIN

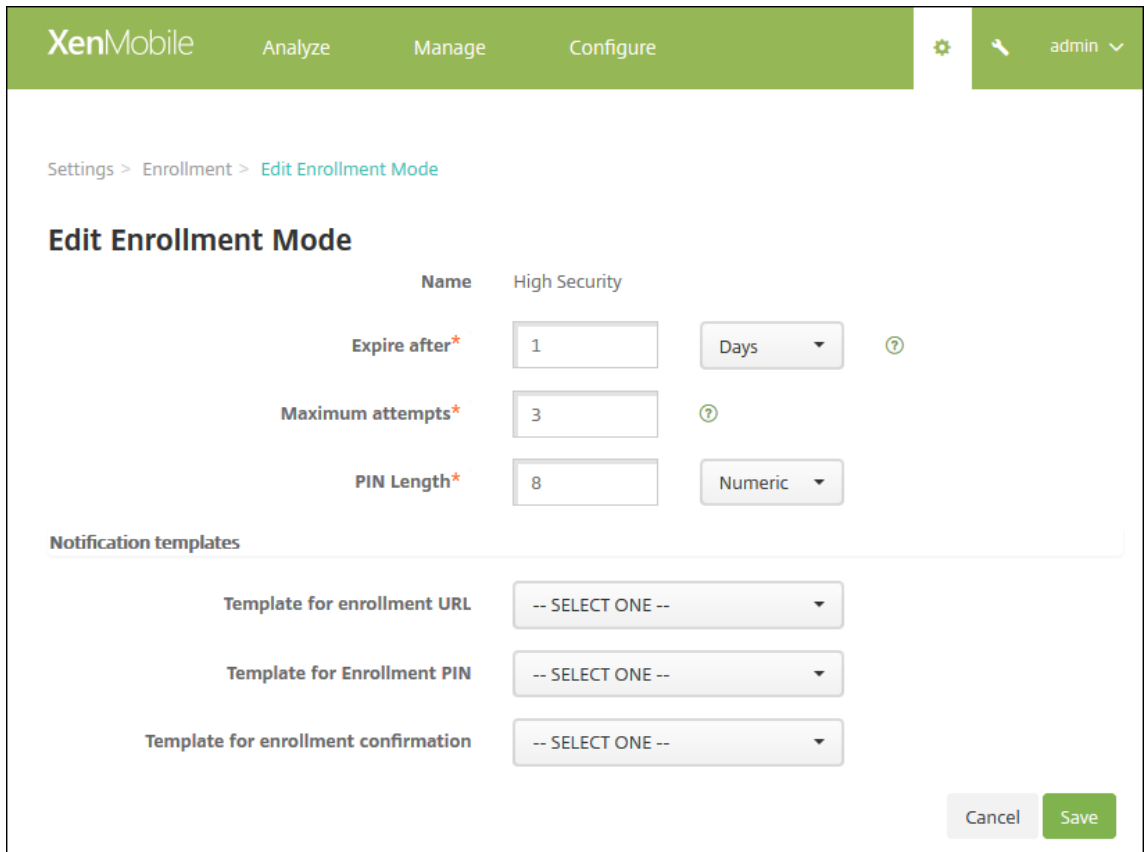
등록초대를사용하여초대를받은사용자로등록을제한할수있습니다.

OTP(일회용 PIN) 등록초대를 2 단계솔루션으로사용할수있습니다. OTP 등록초대는사용자가등록할수있는장치의수를 제어합니다.

보안수준이가장높은환경의경우등록초대를 SN/UDID/IMEI 로장치에연결할수있습니다. 2 단계옵션을사용하여 Active Directory 암호및 OTP 를요구할수도있습니다.

등록모드를편집하려면

1. 등록목록에서등록모드를선택한후 편집을클릭합니다. 등록모드편집페이지가나타납니다. 선택한모드에따라표시되는 옵션이다를수있습니다.



2. 다음정보를적절하게변경합니다.

- 다음이후에만료: 사용자가장치를등록할수없는만료기한을입력합니다. 이값은사용자및그룹등록초대구성페이지에 나타납니다.
초대가만료되지않도록하려면 **0** 을입력하십시오.
- 일: 목록에서 다음이후에만료에입력한만료기한에해당하는 일또는 시간을클릭합니다.
- 최대시도횟수: 등록프로세스가잠기기전까지사용자가등록을시도할수있는횟수를입력합니다. 이값은사용자및그룹 등록초대구성페이지에나타납니다.
시도횟수를제한하지않으려면 **0** 을입력하십시오.
- **PIN** 길이: 생성된 PIN 의길이를설정할숫자를입력합니다.
- 숫자: 목록에서 숫자또는 영숫자를 PIN 유형으로클릭합니다.
- 알림템플릿:
 - 등록 **URL** 용템플릿: 목록에서등록 URL 에서사용할템플릿을클릭합니다. 예를들어등록초대템플릿은사용자 에게전자메일또는 SMS 를보냅니다. 방법은사용자가 XenMobile 에장치를등록할때사용할수있는템플릿 의구성방법에따라다릅니다. 알림템플릿에대한자세한내용은 [알림템플릿만들기또는업데이트](#)를참조하십시오.
 - 등록 **PIN** 용템플릿: 목록에서등록 PIN 에서사용할템플릿을클릭합니다.

- 등록확인용템플릿: 목록에서사용자가성공적으로등록되었음을알릴때사용할템플릿을클릭합니다.

3. 저장을클릭합니다.

등록모드를기본값으로설정하려면

등록모드를기본값으로설정하면다른등록모드를선택하지않는한모든장치등록요청에해당모드가사용됩니다. 기본값으로설정된등록모드가없는경우장치를등록할때마다등록요청을만들어야합니다.

참고:

사용자이름 + 암호, 2 단계또는 사용자이름 + PIN 등록모드만기본값으로사용할수있습니다.

1. 사용자이름 + 암호, 2 단계또는 사용자이름 + PIN 중에서기본등록모드를선택합니다.
모드를기본값으로사용하려면먼저사용하도록설정해야합니다.
2. 기본값을클릭합니다. 이제선택한모드가기본값입니다. 이전에기본값으로설정된다른등록모드는더이상기본값이아닙니다.

등록모드를사용하지않으려면

등록모드를사용하지않도록설정하면그룹등록초대와자가지원포털에서등록모드를사용할수없게됩니다. 한등록모드를사용하지않도록설정하고다른등록모드를사용하도록설정하여사용자가장치를등록하는방법을변경할수있습니다.

1. 등록모드를선택합니다.
기본등록모드는사용하지않도록설정할수없습니다. 기본등록모드를사용하지 않으려면먼저기본값상태를제거해야합니다.
2. **Disable** 을클릭합니다. 등록모드가더이상사용되지않습니다.

자가지원포털에서등록모드를사용하도록설정하려면

자가지원포털에서등록모드를사용하도록설정하면사용자가개별적으로 XenMobile 에장치를등록할수있습니다.

참고:

- 등록모드를자가지원포털에서사용할수있으려면등록모드를사용하도록설정하고알림템플릿에연결해야합니다.
- 자가지원포털에는한번에하나의등록모드만사용하도록설정할수있습니다.

1. 등록모드를선택합니다.
2. 자가지원포털을클릭합니다. 이제사용자가자가지원포털에서선택한등록모드를사용할수있습니다. 자가지원포털에서사용하도록설정된다른모드는더이상사용자에게제공되지않습니다.

그룹추가또는제거

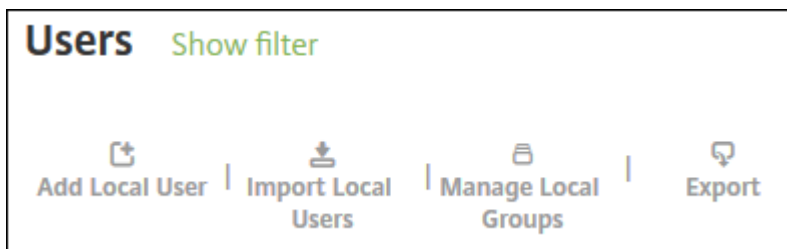
XenMobile 콘솔에서 사용자, 로컬사용자추가, 로컬사용자편집페이지의 그룹관리대화상자에서그룹을관리할수있습니다. 그룹 편집명령은없습니다.

그룹을제거하는경우그룹제거가사용자계정에영향을주지않는다는점을기억하십시오. 그룹을제거하면해당그룹에대한사용자연결만제거됩니다. 또한사용자가해당그룹에연결된배달그룹에서제공하는앱또는프로필에액세스할수없게됩니다. 그러나다른모든그룹연결은그대로유지됩니다. 다른로컬그룹에연결되지않은사용자는상위수준에연결됩니다.

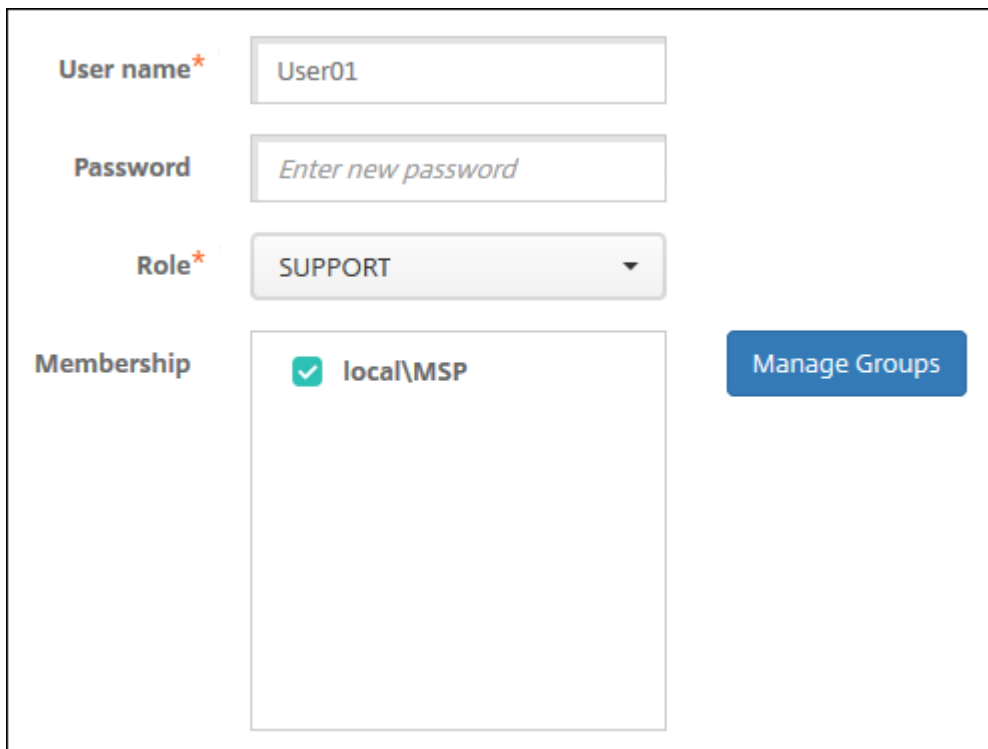
로컬그룹을추가하려면

1. 다음중하나를수행합니다.

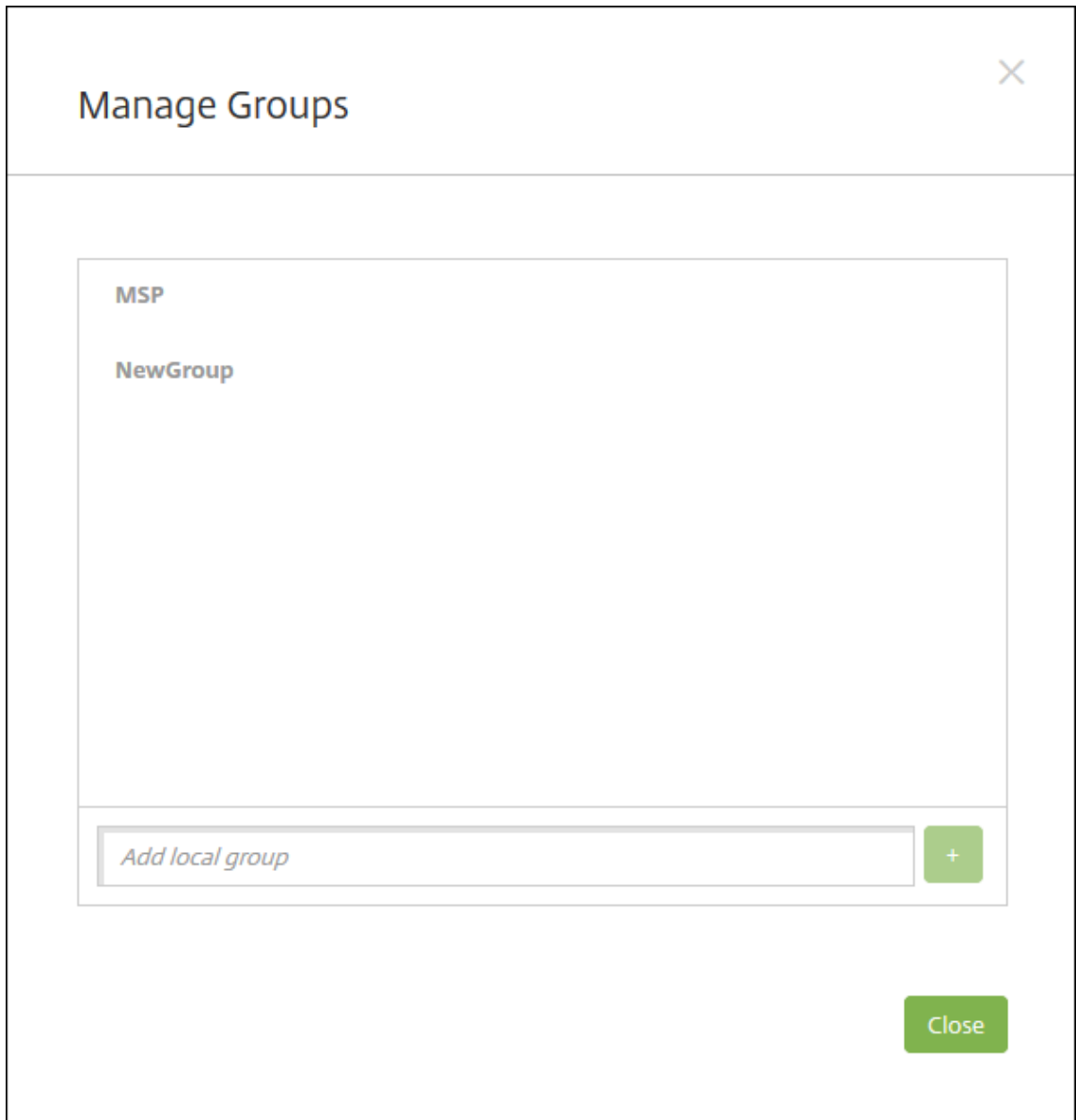
- 사용자페이지에서 로컬그룹관리를클릭합니다.



- 로컬사용자추가페이지또는 로컬사용자편집페이지에서 그룹관리를클릭합니다.



그룹관리대화상자가나타납니다.



2. 그룹목록아래에새그룹이름을입력한후더하기기호 (+) 를클릭합니다. 사용자그룹이목록에추가됩니다.
3. **Close**(닫기) 를클릭합니다.

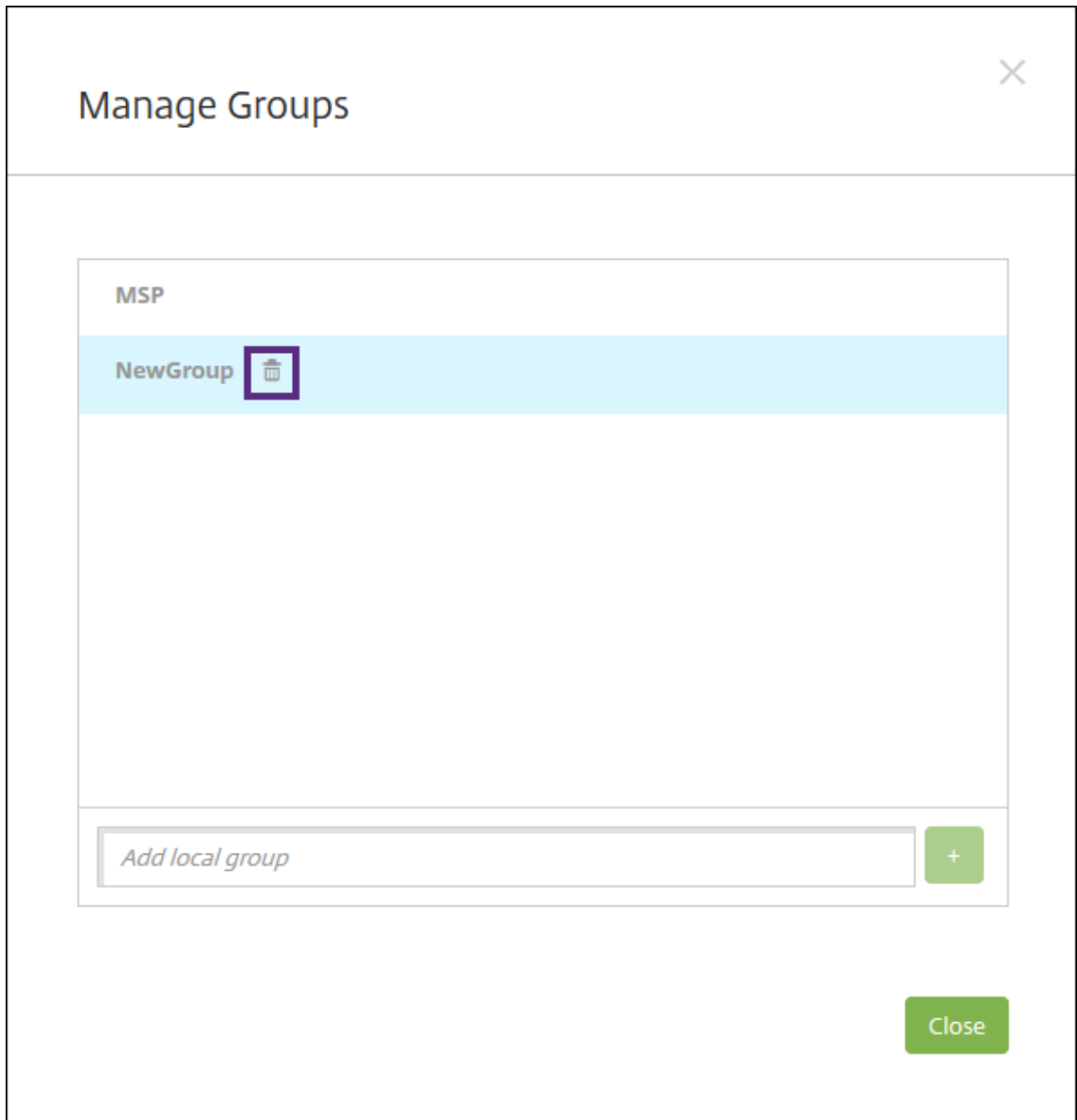
그룹을제거하려면

그룹을제거해도사용자계정에는영향을주지않습니다. 그룹을제거하면해당그룹에대한사용자연결만제거됩니다. 또한사용자가해당그룹에연결된배달그룹에서제공하는앱또는프로필에액세스할수없게됩니다. 그러나다른모든그룹연결은그대로유지됩니다. 다른로컬그룹에연결되지않은사용자는상위수준에연결됩니다.

1. 다음중하나를수행합니다.
 - 사용자페이지에서 로컬그룹관리를클릭합니다.

- 로컬사용자추가페이지또는 로컬사용자편집페이지에서 그룹관리를클릭합니다.

그룹관리대화상자가나타납니다.



2. 그룹관리대화상자에서삭제할그룹을클릭합니다.
3. 그룹이름오른쪽의휴지통아이콘을클릭합니다. 확인대화상자가나타납니다.
4. 삭제를클릭하여작업을확인하고그룹을제거합니다.

중요:

이작업은실행취소할수없습니다.

5. 그룹관리대화상자에서 닫기를클릭합니다.

워크플로만들기및관리

워크플로를사용하여사용자계정의생성및제거를관리할수있습니다. 워크플로를사용하려면먼저조직에서사용자계정요청을승인할 권한이있는담당자를식별합니다. 그런다음워크플로템플릿을사용하여사용자계정요청을만들고승인할수있습니다.

XenMobile 을처음으로설정하는경우워크플로를사용하기전에먼저워크플로전자메일설정을구성해야합니다. 워크플로전자메일 설정은언제든지변경할수있습니다. 이러한설정에는전자메일서버, 포트, 전자메일주소및사용자계정생성요청에승인이필요한지여부가포함됩니다.

XenMobile 의두위치에서워크플로를구성할수있습니다.

- XenMobile 콘솔의 워크플로페이지. 워크플로페이지에서앱구성에사용할여러워크플로를구성할수있습니다. 워크플로 페이지에서워크플로를구성하는경우앱을구성할때워크플로를선택할수있습니다.
- 앱의응용프로그램커넥터를구성할때워크플로이름을입력한다음사용자계정요청을승인할수있는사용자를구성합니다. [XenMobile 에앱추가](#)에서자세한내용을참조하십시오.

사용자계정에대한관리자승인을최대 3 개수준까지할당할수있습니다. 사용자계정을승인할다른사용자가필요한경우해당사용자의 이름또는전자메일주소를사용하여검색하고선택할수있습니다. XenMobile 에서해당사용자가검색되면워크플로에추가하면됩니다. 새사용자계정에대한승인또는거부를위한전자메일이워크플로의모든사용자에게전송됩니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 워크플로를클릭합니다. 워크플로페이지가나타납니다.
3. 추가를클릭합니다. 워크플로추가페이지가나타납니다.

4. 다음설정을구성합니다.

- 이름: 워크플로의고유한이름을입력합니다.
- 설명: 필요한경우워크플로의설명을입력합니다.
- 전자메일승인템플릿: 목록에서할당할전자메일승인템플릿을선택합니다. XenMobile 콘솔의 설정아래 알림템플릿섹션에서전자메일템플릿을만들수있습니다. 이필드의오른쪽에있는눈아이콘을클릭하면구성중인템플릿의미리보기가표시됩니다.
- 관리자승인수준: 목록에서이워크플로에필요한관리자승인수준의번호를선택합니다. 기본값은 1 수준입니다. 사용가능한옵션은다음과같습니다.
 - 필요없음
 - 1 수준
 - 2 수준
 - 3 수준
- **Active Directory** 도메인선택: 목록에서워크플로에사용할적절한 Active Directory 도메인을선택합니다.
- 추가로필요한승인자찾기: 검색필드에이름을입력하고 검색을클릭합니다. 이름은 Active Directory 에서가져옴

니다.

- 필드에이름이나타나면해당하는이름옆의확인란을선택합니다. 이름과전자메일주소가 추가로필요한승인자선택됨 목록에나타납니다.
 - 목록에서이름을제거하려면다음중하나를수행합니다.
 - * 검색을클릭하여선택한도메인의모든사용자목록을표시합니다.
 - * 검색결과를제한하려면검색상자에이름전체또는일부를입력한다음 검색을클릭합니다.
 - * 추가로필요한승인자선택됨목록에있는사용자는검색결과목록에서해당이름옆에확인표시가있습니다. 목록을스크롤하고제거할각이름옆의확인란을선택취소합니다.

5. 저장을클릭합니다. 생성된워크플로가 워크플로페이지에표시됩니다.

워크플로를만든후워크플로세부정보를보거나워크플로에연결된앱을보거나워크플로를삭제할수있습니다. 워크플로를만든후에는 워크플로를편집할수없습니다. 승인수준또는승인자가다른워크플로가필요한경우다른워크플로를만듭니다.

세부정보를보고워크플로를삭제하려면

1. 워크플로페이지의기존워크플로목록에서특정워크플로를선택합니다. 이렇게하려면테이블의행을클릭하거나워크플로옆의확인란을선택합니다.
2. 워크플로를삭제하려면 삭제를클릭합니다. 확인대화상자가나타납니다. 삭제를다시클릭합니다.

중요:

이작업은실행취소할수없습니다.

RBAC 를사용하여역할구성

January 6, 2020

사전정의된각 RBAC(역할기반액세스제어) 역할에는특정액세스및기능권한이연결되어있습니다. 이문서에서는각사용권한이 수행하는작업에대해설명합니다. 각기본제공역할에대하기본사용권한의전체목록을보려면 [Role-Based Access Control Defaults\(역할기반액세스제어기본값\)](#)를다운로드하십시오.

사용권한을적용할때 RBAC 역할에관리권한이있는사용자그룹을정의합니다. 기본관리자는적용된사용권한설정을변경할수없습니다. 기본적으로, 적용된사용권한은모든사용자그룹에적용됩니다.

할당을수행할때 RBAC 역할을그룹에할당하면사용자그룹이 RBAC 관리자권한을소유하게됩니다.

이문서의섹션은다음과같습니다.

- [관리역할](#)
- [장치프로비저닝역할](#)
- [지원역할](#)
- [사용자역할](#)
- [RBAC 를사용하여역할구성](#)

관리역할

미리정의된관리자역할을가진사용자는 XenMobile 에서다음기능에액세스하거나액세스할수없습니다. 기본적으로, 허가된엑세스 (자가지원포털제외), 콘솔기능및 권한적용을사용할수있습니다.

허가된엑세스

관리자콘솔엑세스	관리자는 XenMobile 콘솔의모든기능에액세스할수있습니다.
자가지원포털엑세스	관리자에게는자가지원포털엑세스권한이없습니다.
공유장치등록자	관리자에게는공유장치등록자엑세스권한이없습니다. 이기능은공유장치를등록해야하는사용자를위한것입니다.
원격지원엑세스	관리자는원격지원엑세스를소유합니다.*
공용 API 액세스	관리자는공용 API 에액세스하여 XenMobile 콘솔에서사용할수있는동작을프로그래밍방식으로수행할수있습니다. 이러한동작에는인증서, 앱, 장치, 배달그룹및로컬사용자관리가포함됩니다.

* 원격지원을사용하면지원센터담당자가관리되는 Windows CE 및 Android 모바일장치를원격으로제어할수있습니다. 스크린캐스트는 Samsung KNOX 장치에서만지원됩니다. 원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다. 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.

콘솔기능

관리자는 XenMobile 콘솔에대한무제한엑세스권한을갖습니다.

대시보드	대시보드는관리자가 XenMobile 콘솔에로그온한후표시되는첫번째페이지입니다. 대시보드에는알림및장치에대한기본정보가표시됩니다.
보고	분석 > 보고페이지에는앱및장치배포를분석할수있는미리정의된보고서가제공됩니다.

장치	관리 > 장치페이지에서는사용자장치를관리할수있습니다. 관리자는페이지에서개별장치를추가하거나장치프로비저닝 파일을가져와한번에여러장치를추가할수있습니다.
로컬사용자및그룹	관리 > 사용자페이지에서는로컬사용자및로컬사용자그룹을 추가, 편집또는삭제할수있습니다.
등록	관리 > 등록초대페이지는 XenMobile 에장치를등록할사용자를초대하는방법을관리하는곳입니다.
정책	구성 > 장치정책페이지는 VPN 및 WiFi 와같은장치정책을 관리하는곳입니다.
앱	구성 > 앱페이지는관리자가사용자가장치에설치할수있느냐양한앱을관리하는곳입니다.
미디어	구성 > 미디어페이지는관리자가사용자가장치에설치할수있느냐다양한미디어를관리하는곳입니다.
스마트동작	구성 > 동작페이지는이벤트를트리거하는응답을관리하는곳입니다.
등록프로필	구성 > 등록프로필페이지에서관리자는사용자가장치를등록할때사용할등록프로필 (모드) 을구성할수있습니다.
배달그룹	구성 > 배달그룹페이지는관리자가배달그룹및배달그룹과관련된리소스를관리하는곳입니다.
설정	설정페이지에서는클라이언트및서버속성, 인증서및자격증명 공급자같은시스템설정을관리할수있습니다.
지원	문제해결및지원페이지에서는진단실행및로그생성등문제해결작업을수행할수있습니다.

장치

관리자는장치제한사항을설정하고, 장치에대한알림을설정및전송하고, 장치의앱을관리하는등콘솔을통해장치기능에액세스합니다.

장치전체초기화	장치에서모든데이터와앱을초기화하며, 장치에메모리카드가 있는경우메모리카드도초기화합니다.
제한사항지우기	하나이상의장치제한사항을제거합니다.

장치선택적초기화	개인데이터및앱은그대로유지하고장치에서모든회사데이터및앱을초기화합니다.
위치보기	장치의위치를확인하고지리적제한사항을설정합니다. 포함사항: 장치찾기, 장치의위치보기, 장치추적, 시간대별장치위치추적
장치잠금	사용자가장치를사용할수없도록원격으로장치를잠금니다.
장치잠금해제	사용자가장치를사용할수있도록원격으로장치의잠금을해제합니다.
컨테이너잠금	장치에서회사컨테이너를원격으로잠금니다.
컨테이너잠금해제	장치에서회사컨테이너를원격으로잠금해제합니다.
컨테이너암호재설정	회사컨테이너암호를재설정합니다.
ASM DEP 사용/활성화잠금바이패스	활성화잠금을사용하면감독되는 iOS 장치에바이패스코드가저장됩니다. 장치를지워야하는경우이코드를사용하여활성화잠금을자동으로지웁니다.
장치벨울림	원격으로 Windows 장치의벨을 5 분동안최대볼륨으로울립니다.
장치다시부팅	XenMobile 콘솔에서 Windows 장치를다시시작합니다.
장치에배포	장치에앱, 알림, 제한사항등을보냅니다.
장치편집	장치의설정을변경합니다.
장치에알림	장치에알림을보냅니다.
장치추가/삭제	XenMobile 에서장치를추가하거나제거합니다.
장치가져오기	파일에서 XenMobile 로장치그룹을가져옵니다.
장치테이블내보내기	장치페이지에서장치정보를수집하여.csv 파일로내보냅니다.
장치해지	장치가 XenMobile 에연결하는것을금지합니다.
앱잠금	장치의모든앱에대한엑세스를거부합니다. Android 에서는사용자가 XenMobile 에로그인할수없게됩니다. iOS 에서는사용자가로그인할수있지만앱에엑세스할수없게됩니다.
앱초기화	Android 에서는사용자의 XenMobile 계정이삭제됩니다. iOS 에서는 XenMobile 기능에엑세스할때필요한암호화키가삭제됩니다.
소프트웨어인벤토리보기	어떤소프트웨어가장치에설치되어있는지확인합니다.
AirPlay 미러링요청	AirPlay 스트리밍을시작하도록요청합니다.

AirPlay 미러링중지	AirPlay 스트리밍을중지합니다.
분실모드활성화	관리페이지의장치에서감독되는장치를분실모드로설정하여 잠금화면에서감독되는장치를차단하고장치를분실하거나도 난당한경우장치를찾습니다.
분실모드비활성화	장치의관리페이지에서분실모드로설정된장치의분실모드를 비활성화할수있습니다.
OS 업데이트장치	OS 업데이트제어장치정책을장치에배포할수있습니다.
장치종료	XenMobile 콘솔에서 iOS 장치를종료합니다.
장치다시시작	XenMobile 콘솔에서 iOS 장치를다시시작합니다.

로컬사용자및그룹

관리자는 XenMobile 의 관리 > 사용자페이지에서로컬사용자및로컬사용자그룹을관리합니다.

로컬사용자추가
로컬사용자삭제
로컬사용자편집
로컬사용자가져오기
로컬사용자내보내기
로컬사용자그룹

등록

관리자는등록초대를추가및삭제하고, 사용자에게알림을보내고, 등록테이블을.csv 파일로내보낼수있습니다.

등록추가/삭제	사용자또는사용자그룹에대한등록초대를추가하거나제거합니다.
사용자알림	사용자또는사용자그룹에대한등록초대를보냅니다.
등록초데이터이블내보내기	등록페이지에서등록정보를수집하여.csv 파일로내보냅니다.

정책

정책추가/삭제	장치또는앱정책을추가하거나제거합니다.
정책편집	장치또는앱정책을변경합니다.
정책업로드	장치또는앱정책을업로드합니다.
정책복제	장치또는앱정책을복사합니다.
정책사용안함	기존앱정책을사용하지않도록설정합니다.
정책내보내기	장치정책페이지에서장치정책정보를수집하여.csv 파일로내보냅니다.
정책할당	장치정책을하나이상의배달그룹에할당합니다.

앱

관리자는 XenMobile 의 구성 > 앱페이지에서앱을관리합니다.

앱스토어또는엔터프라이즈앱추가/삭제	공용앱스토어앱또는 MDX Toolkit 으로래핑되지않은앱을추가하거나제거합니다.
앱스토어또는엔터프라이즈앱편집	공용앱스토어앱또는 MDX Toolkit 으로래핑되지않은앱을변경합니다.
MDX, 웹및 SaaS 앱추가/삭제	MDX Toolkit(MDX 앱) 으로래핑된앱, 내부네트워크의앱(웹앱) 또는공용네트워크 (SaaS) 의앱을 XenMobile 에추가하거나제거합니다.
MDX, 웹및 SaaS 앱편집	MDX Toolkit(MDX 앱) 으로래핑된앱, 내부네트워크의앱(웹앱) 또는공용네트워크 (SaaS) 의앱을 XenMobile 에서변경합니다.
범주추가/삭제	XenMobile Store 에서앱을표시할수있는범주를추가하거나삭제합니다.
공용/엔터프라이즈앱을배달그룹에할당	공용앱스토어앱또는 MDX Toolkit 으로래핑되지않은앱을배포를위해배달그룹에할당합니다.
MDX/WebLink/SaaS 앱을배달그룹에할당	MDX Toolkit 으로래핑된앱 (MDX 앱), Single Sign-on 이필요없는앱 (WebLink) 또는공용네트워크의앱 (SaaS) 을사용자장치에배포하기위해배달그룹에할당합니다.

애플리케이션 배포

애플리케이션에서 애플리케이션 정보를 수집하여.csv 파일로 배포합니다.

미디어

공용 앱 스토어 또는 VPP 라이선스를 통해 취득한 미디어를 관리합니다.

앱 스토어 또는 엔터프라이즈 서적 추가/삭제

공용/엔터프라이즈 서적을 배달 그룹에 할당

앱 스토어 또는 엔터프라이즈 서적 편집

스마트 동작

스마트 동작 추가/삭제

트리거 (이벤트, 장치/사용자 속성 또는 설치된 앱 이름) 및 관련 응답에 의해 정의된 동작을 추가하거나 제거합니다.

스마트 동작 편집

트리거 (이벤트, 장치/사용자 속성 또는 설치된 앱 이름) 및 관련 응답에 의해 정의된 동작을 변경합니다.

스마트 동작을 배달 그룹에 할당

사용자 장치에 배포하기 위해 배달 그룹에 동작을 할당합니다.

스마트 동작 배포

동작 페이지에서 동작 정보를 수집하여.csv 파일로 배포합니다.

배달 그룹

관리하는 구성 > 배달 그룹 페이지에서 배달 그룹을 관리합니다.

배달 그룹 추가/삭제

지정된 사용자 및 선택적인 정책, 앱 및 동작을 추가하는 배달 그룹을 만들거나 제거합니다.

배달 그룹 편집

기존 배달 그룹을 변경하여, 사용자 및 선택적인 정책, 앱 및 동작을 수정합니다.

배달 그룹 배포

배달 그룹을 사용할 수 있게 만듭니다.

배달그룹내보내기

배달그룹페이지에서배달그룹정보를수집하고이를.csv 파일로내보냅니다.

등록프로필

등록프로필을관리합니다.

등록프로필추가/삭제

등록프로필편집

배달그룹에등록프로필할당

설정

관리자는 설정페이지에서다양한설정을구성합니다.

RBAC

RBAC 할당, 역할할당

LDAP

그룹, 사용자계정및관련속성을가져올수있도록하나이상의 LDAP 호환디렉터리 (예: Active Directory) 를관리합니다.

라이선스

온-프레미스 XenMobile Server 에해당합니다. Citrix 라이선스를관리합니다.

등록

사용자및자가지원포털에대해등록모드를사용하도록설정합니다.

릴리스관리

현재설치된릴리스를확인합니다. 포함사항: 릴리스관리업데이트

인증서

APNS 인증서편집, 인증서 SSL 수신기

알림템플릿

자동화동작이나등록에서, 아니면사용자에게표준알림메시지를제공할때사용할알림템플릿을만듭니다.

워크플로

앱구성에서사용할수있도록사용자계정의만들기, 승인및제거를관리합니다.

자격증명공급자	장치인증서를발급하도록승인된하나이상의자격증명공급자를추가합니다. 자격증명공급자는인증서형식과인증서를갱신하거나해지하기위한조건을제어합니다.
PKI 엔터티	공개키인프라엔터티 (일반, Microsoft 인증서서비스또는 임의의 CA) 를관리합니다.
PKI 연결테스트	설정 > PKI 엔터티페이지의연결테스트단추를사용하여서버에액세스할수있는지확인합니다.
클라이언트속성	암호유형, 강도, 만료등과같은사용자장치의다양한속성을관리합니다.
클라이언트지원	사용자가지원서비스에연락할수있는방법 (전자메일, 전화또는지원티켓전자메일) 을설정합니다.
클라이언트브랜딩	XenMobile Store 의사용자지정스토어이름과기본스토어보기를생성합니다. XenMobile Store 또는 Secure Hub 예표시되는사용자지정로그를추가합니다.
이동통신사업자 SMS 게이트웨이	이동통신사업자의 SMS 게이트웨이를설정하여이동통신사업자의 SMS 게이트웨이를통해 XenMobile 이전송하는알림을구성합니다.
알림서버	사용자에게전자메일을보내도록 SMTP 게이트웨이서버를설정합니다.
ActiveSync Gateway	규칙및속성을통해사용자및장치에대한사용자엑세스를관리합니다.
Apple DEP(장치등록프로그램)	XenMobile 에 Apple DEP 계정을추가합니다.
Apple Configurator 장치등록	XenMobile 에서 Apple Configurator 설정을구성합니다.
iOS/VPP 설정	Apple Volume Purchase Program 계정을추가합니다.
모바일서비스공급자	모바일서비스공급자인터페이스를사용하여 BlackBerry 및기타 Exchange ActiveSync 장치를쿼리하고작업을실행합니다.
NetScaler Gateway	온-프레미스 XenMobile Server 에해당합니다. NetScaler Gateway 를추가합니다. 인증을사용할지여부와인증시사용자인증서를푸시할지여부를선택합니다. 자격증명공급자를선택합니다.

네트워크액세스제어	장치가규정을준수하지않는지확인하고네트워크에대한엑세스를거부하는조건을설정합니다.
Samsung KNOX	XenMobile 이 Samsung KNOX 증명서버 REST API 를취리하거나취리하지않도록설정합니다.
서버속성	서버속성을추가하거나수정합니다. 모든노드에서 XenMobile 을다시시작해야합니다.
Syslog	온-프레미스 XenMobile Server 에해당합니다. 서버호스트이름또는 IP 주소를사용하여시스템로그 (syslog) 서버로로그파일을보냅니다.
XenApp/XenDesktop	사용자가 Citrix Secure Hub 를통해 Virtual Apps and Desktops 를추가할수있습니다.
ShareFile	XenMobile 을 ShareFile Enterprise 와함께사용할경우: ShareFile 계정및관리자서비스계정에연결하여사용자계정을관리하는설정을구성합니다. 기존 ShareFile 도메인및관리자자격증명이필요합니다. XenMobile 과함께 StorageZone 커넥터를사용하는경우: ShareFile StorageZones 커넥터에정의된네트워크공유및 SharePoint 위치를가리키도록 XenMobile 을구성합니다.
환경개선프로그램	온-프레미스 XenMobile Server 에해당합니다. Citrix 로익명통계및사용현황정보를보내거나보내지않도록선택합니다.
Microsoft Azure	온-프레미스 XenMobile Server 에해당합니다. XenMobile 과 Microsoft Azure 를통합합니다.
Android Enterprise	Android Enterprise 서버설정을구성합니다.
IDP(ID 공급자)	ID 공급자를구성합니다.
파생된자격증명	iOS 장치등록을위한파생된자격증명을구성합니다.
XenMobile Tools	XenMobile Tools 페이지에엑세스합니다.
SNMP 구성	XenMobile Server 노드에대해 SNMP 를사용하도록설정합니다. 모니터링사용자를편집또는추가하고, 트랩알림이 나타나는 SNMP 관리자를설정하고, 트랩간격과임계값을구성합니다.

지원

관리자는 다양한 지원 작업을 수행할 수 있습니다.

NetScaler Gateway 연결확인	IP 주소로 NetScaler Gateway 에 대한 다양한 연결 확인을 수행합니다. 사용자 이름 및 암호가 필요합니다.
XenMobile 연결확인	선택한 XenMobile 기능 (예: 데이터베이스, DNS, Google Plan 등) 에 대한 연결 확인을 수행합니다.
지원 번들 만들기	온-프레미스 XenMobile Server 에 해당합니다. 문제 해결을 위해 Citrix 지원에 보낼 파일을 생성합니다. XenMobile 또는 NetScaler Gateway 에 대한 시스템 정보, 로그, 데이터베이스 정보, 핵심 정보, 추적 파일 및 최신 구성 정보가 포함됩니다.
Citrix 제품 설명서	공개 Citrix XenMobile 설명서 사이트에 액세스합니다.
Citrix Knowledge Center	Citrix 지원 사이트에 액세스하여 기술 자료 문서를 검색합니다.
로그	디버그, 관리자 감사 및 사용자 감사에 대한 로그 파일 세부 정보에 액세스하고 분석합니다.
클러스터 정보	온-프레미스 XenMobile Server 에 해당합니다. 클러스터된 환경의 각 노드에 대한 정보에 액세스합니다.
가비지 수집	온-프레미스 XenMobile Server 에 해당합니다. 더 이상 사용하지 않는 메모리 개체에 대한 정보에 액세스합니다.
Java 메모리 속성	온-프레미스 XenMobile Server 에 해당합니다. Java 메모리 사용 현황, 메모리 세부 정보 및 메모리 풀 세부 정보의 스냅샷에 액세스합니다.
매크로	프로필, 정책, 알림 또는 등록 템플릿의 텍스트 필드에서 사용자 또는 장치 속성 데이터를 채웁니다. 단일 정책을 구성하여 대규모 사용자 기반에 정책을 배포하고 각 대상 사용자에게 사용자 관련 값이 표시되게 합니다.
PKI 구성	PKI 구성 정보를 가져오고 내보냅니다.
APNS 서명 유틸리티	APNs (Apple Push Network signing) 인증서에 대한 요청을 제출하거나 iOS 용 Secure Mail APNs 인증서를 업로드합니다.
Citrix Insight Services	다양한 문제에 대한 도움을 받으려면 CIS (Citrix Insight Services) 에 로그를 업로드하십시오.
Exchange ActiveSync 용 Citrix Gateway 커넥터 장치 상태	장치 ActiveSync ID 를 기반으로 Exchange ActiveSync 용 Citrix Gateway 커넥터로 전송된 장치의 상태를 XenMobile 에 쿼리합니다.

익명화및익명화취소	온-프레미스 XenMobile Server 에해당합니다. XenMobile 에서지원번들을만드는경우중요한사용자, 서버및네트워크데이터가기본적으로익명으로만들어집니다. 지원의익명화및익명화취소페이지에있는고급에서이동작을변경할수있습니다.
로그설정	로그수준을사용자지정하거나사용자지정로그를추가합니다.

그룹액세스제한

관리사용자는모든사용자그룹에권한을적용할수있습니다.

장치프로비저닝역할

중요:

장치프로비저닝역할은 Windows CE 장치에만적용됩니다.

미리정의된장치프로비저닝역할이있는사용자는콘솔기능에제한적으로액세스할수있습니다. 기본적으로이러한사용자는권한이모든사용자그룹으로설정되고이설정을변경할수없습니다.

콘솔기능

장치프로비저닝사용자는 XenMobile 콘솔에대해다음과같은제한적인액세스권한을갖습니다. 기본적으로, 다음기능각각이사용하도록설정됩니다.

장치

장치편집	장치의설정을변경합니다.
장치추가/삭제	XenMobile 에서장치를추가하거나제거합니다.

설정

장치프로비저닝사용자는 설정페이지에액세스할수있지만기능을구성하는권한이없습니다.

지원역할

지원역할을 가진 사용자는 원격 지원에 액세스할 수 있습니다. 이러한 사용자의 권한은 기본적으로 모든 사용자에게 적용되며 이 설정을 편집할 수 없습니다.

사용자역할

사용자역할을 가진 사용자는 다음과 같이 XenMobile 에 제한적으로 액세스할 수 있습니다.

허가된 액세스

자가지원포털	사용자는 XenMobile 에서 자가지원포털에만 액세스할 수 있습니다.
--------	---

콘솔기능

사용자는 XenMobile 콘솔에 대해 다음과 같은 제한적인 액세스 권한을 갖습니다.

장치

장치전체초기화	장치에서 모든 데이터와 앱을 초기화하며, 장치에 메모리 카드가 있는 경우 메모리 카드도 초기화합니다.
장치선택적초기화	개인 데이터 및 앱은 그대로 유지하고 장치에서 모든 회사 데이터 및 앱을 초기화합니다.
위치보기	장치의 위치를 확인하고 지리적 제한 사항을 설정합니다. 포함 사항: 장치 찾기, 장치의 위치 보기, 장치 추적, 시간대별 장치 위치 추적
장치잠금	장치를 원격으로 잠가 사용할 수 없게 만듭니다.
장치잠금해제	장치를 원격으로 잠금 해제하여 사용할 수 있게 만듭니다.
컨테이너잠금	장치에서 회사 컨테이너를 원격으로 잠급니다.
컨테이너잠금해제	장치에서 회사 컨테이너를 원격으로 잠금 해제합니다.
컨테이너암호재설정	회사 컨테이너 암호를 재설정합니다.

ASM DEP 사용/활성화잠금바이패스	활성화잠금을사용하면감독되는 iOS 장치에바이패스코드가 저장됩니다. 장치를지워야하는경우이코드를사용하여활성화잠금을자동으로지웁니다.
장치벨울림	원격으로 Windows 장치의벨을 5 분동안최대볼륨으로울립니다.
장치다시부팅	Windows 장치를다시시작합니다.
소프트웨어인벤토리보기	어떤소프트웨어가장치에설치되어있는지확인합니다.

등록

등록추가/삭제	사용자또는사용자그룹에대한등록초대를추가하거나제거합니다.
사용자알림	사용자또는사용자그룹에대한등록초대를보냅니다.

그룹액세스제한

네가지기본역할모두에대해이권한은기본적으로설정되며모든사용자그룹에적용할수있습니다. 이역할은편집할수없습니다.

RBAC 를사용하여역할구성

XenMobile 의 RBAC(역할기반액세스제어) 를사용하여미리정의된역할또는권한집합을사용자및그룹에할당할수있습니다. 이러한권한은시스템기능에대한사용자액세스수준을제어합니다.

XenMobile 은네가지기본사용자역할을구현하여시스템기능에대한액세스권한을논리적으로분리합니다.

- 관리자: 전체시스템액세스권한을부여합니다.
- 장치프로비저닝: Windows CE 장치에대한기본적인장치관리액세스권한을부여합니다.
- 지원: 원격지원에대한액세스권한을부여합니다.
- 사용자: 장치를등록할수있고자가지원포털에액세스할수있는사용자가사용합니다.

또한기본역할을템플릿으로사용하고, 이템플릿을사용자지정하여기본역할에정의된기능이외의특정시스템기능에액세스할수있는권한이있는새로운사용자역할을만들수있습니다.

역할은로컬사용자 (사용자수준) 또는 Active Directory 그룹 (해당그룹의모든사용자가동일한권한을가짐) 에할당할수있습니다. 사용자가여러 Active Directory 그룹에속하는경우모든권한이병합되어해당사용자의권한을정의합니다. 예를들어

ADGroupA 사용자가관리자장치를찾을수있고, ADGroupB 사용자가직원장치를초기화할수있는경우두그룹에도두속한사용자는관리자및직원의장치를찾고초기화할수있습니다.

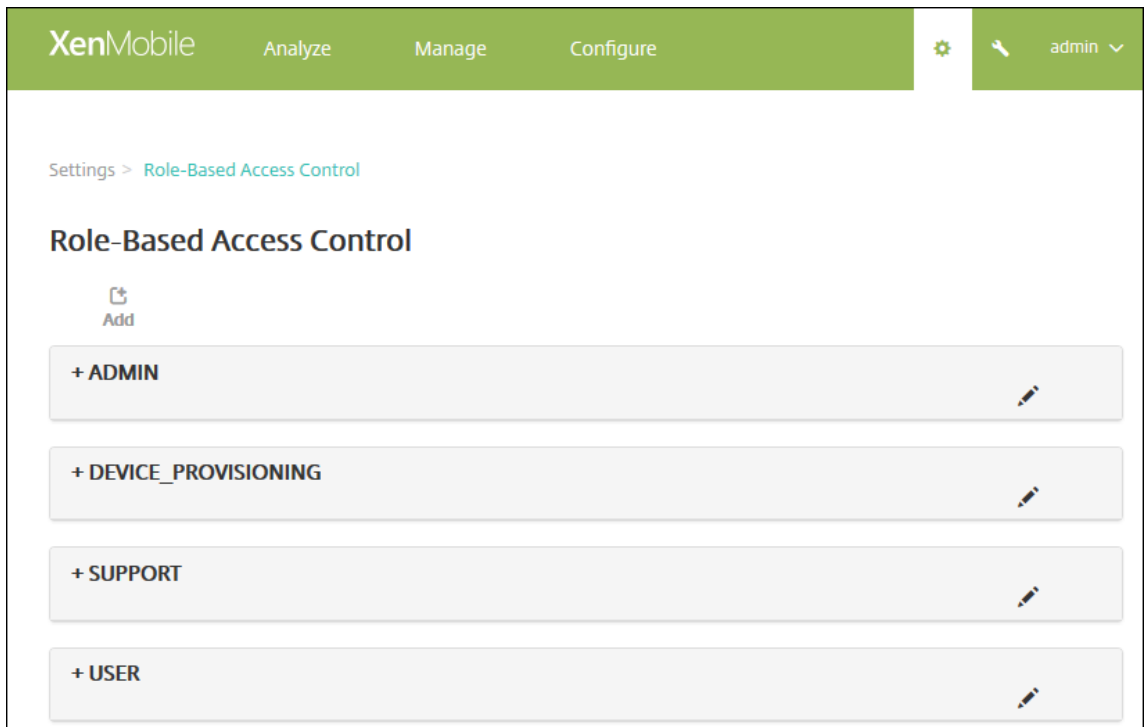
참고:

로컬사용자에게는하나의역할만할당될수있습니다.

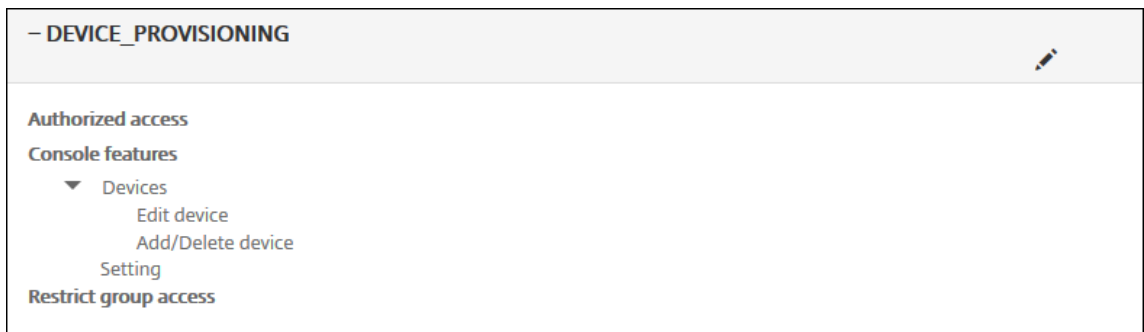
XenMobile 의 RBAC 기능을사용하여다음을수행할수있습니다.

- 새역할을만듭니다.
- 역할에그룹을추가합니다.
- 로컬사용자를역할에연결합니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 역할기반액세스제어를클릭합니다. 역할기반액세스제어페이지가나타납니다. 이페이지에는네개의기본사용자역할과앞서 추가한모든역할이표시됩니다.

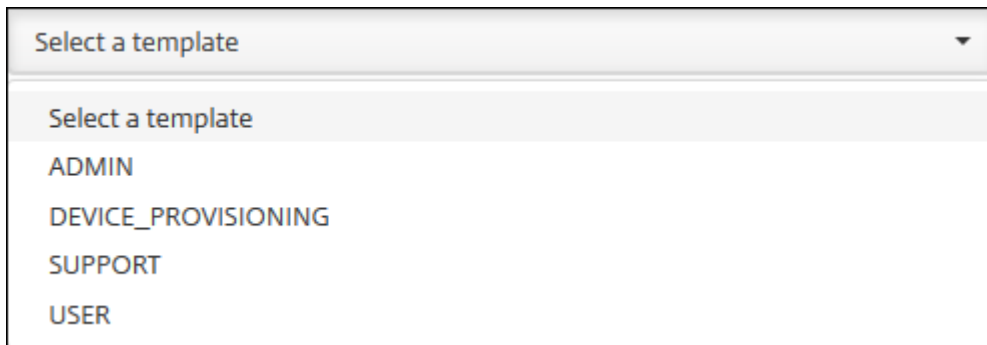


역할옆에있는더하기기호 (+) 를클릭하면다음그림과같이역할이확장되어해당역할에대한모든권한이표시됩니다.

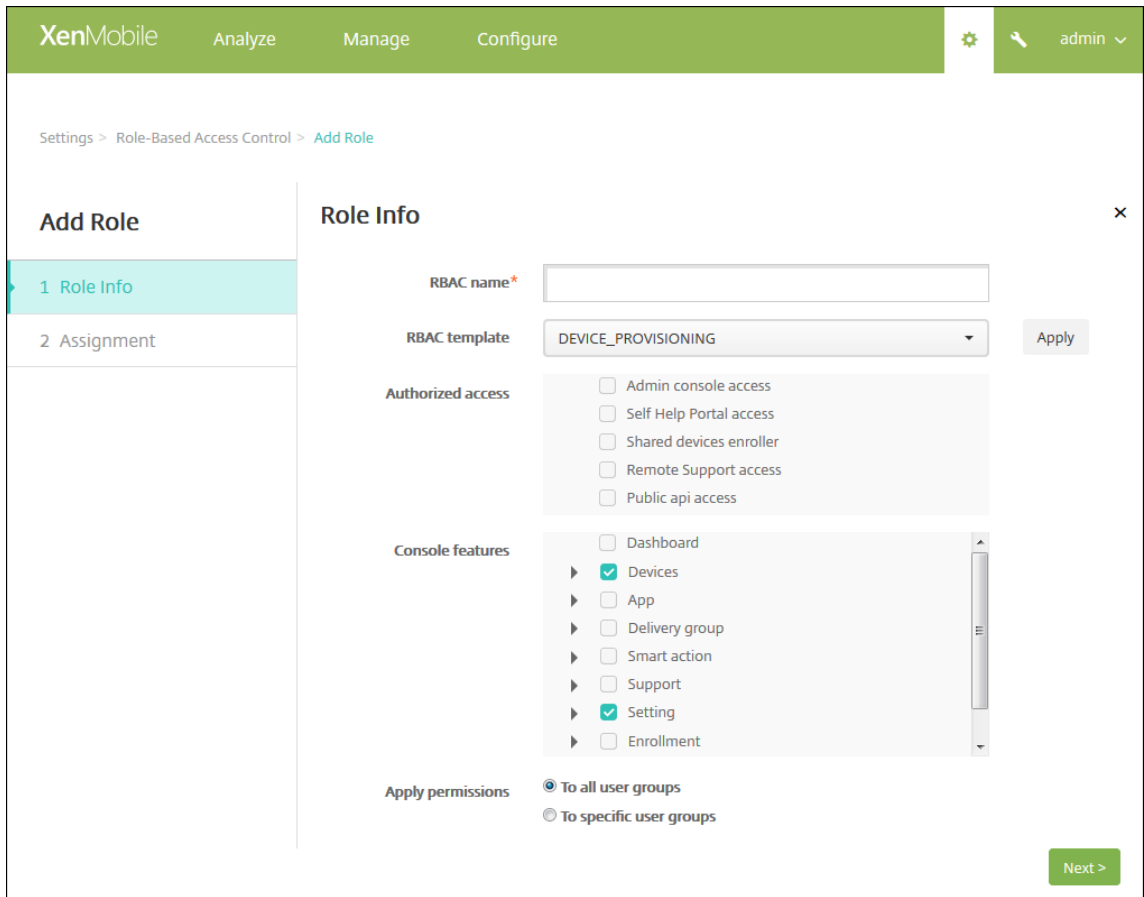


3. 추가를 클릭하여 새 사용자 역할을 추가하거나, 기존 역할 오른쪽에 있는 연필 아이콘을 클릭하여 역할을 편집하거나, 이전에 정의한 역할 오른쪽에 있는 휴지통 아이콘을 클릭하여 역할을 삭제합니다. 기본 사용자 역할은 삭제할 수 없습니다.
 - 추가 또는 연필 아이콘을 클릭하면 역할 추가 또는 역할 편집 페이지가 나타납니다.
 - 휴지통 아이콘을 클릭하면 확인 대화상자가 나타납니다. 선택한 역할을 제거하려면 삭제를 클릭합니다.
4. 다음과 같은 정보를 입력하여 새 사용자 역할을 만들거나 기존 사용자 역할을 편집합니다.
 - **RBAC 이름:** 새 사용자 역할을 설명하는 이름을 입력합니다. 기존 역할의 이름은 변경할 수 없습니다.
 - **RBAC 템플릿:** 선택적으로, 새 역할의 시작점으로 사용할 템플릿을 클릭합니다. 기존 역할을 편집하는 경우 템플릿을 선택할 수 없습니다.

RBAC 템플릿은 기본 사용자 역할입니다. 이러한 템플릿은 해당 역할과 연결된 사용자가 갖는 시스템 기능에 대한 액세스 권한을 정의합니다. RBAC 템플릿을 선택한 후 허가된 액세스 및 콘솔 기능 필드에서 해당 역할과 연결된 모든 권한을 확인할 수 있습니다. 템플릿 사용은 선택적입니다. 허가된 액세스 및 콘솔 기능 필드에서 역할에 할당할 옵션을 직접 선택할 수 있습니다.

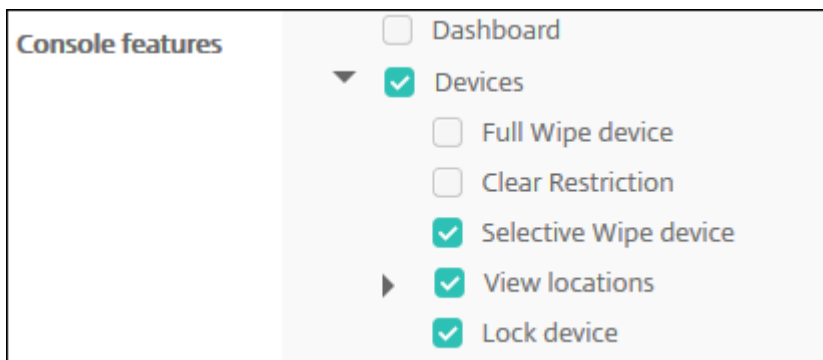


5. **RBAC** 템플릿 필드 오른쪽에 있는 적용을 클릭하여 허가된 액세스 및 콘솔 기능 확인란을 선택한 템플릿의 미리 정의된 액세스 권한과 기능 권한으로 채웁니다.



6. 허가된 액세스 및 콘솔 기능의 확인란을 선택하고 선택 취소하여 역할을 사용자 지정합니다.

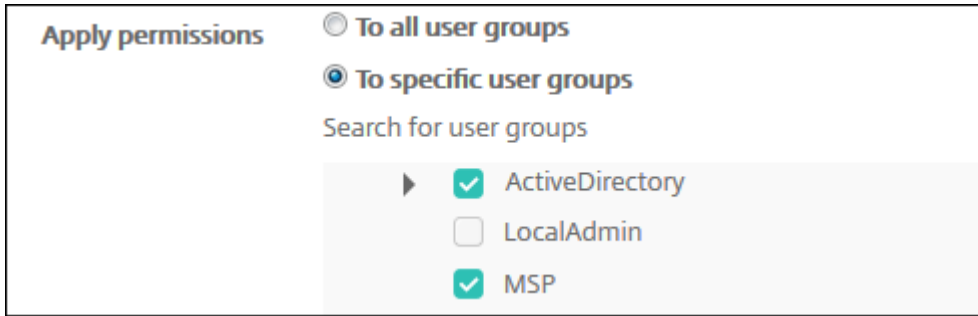
콘솔 기능 옆에 있는 삼각형을 클릭하면 해당 기능과 관련된 권한이 선택하거나 선택 취소할 수 있도록 나타납니다. 최상위 수준 확인란을 클릭하면 해당 콘솔 부분에 대한 액세스가 차단됩니다. 따라서 최상위 수준 아래의 개별 옵션을 선택하여 해당 옵션을 사용하도록 설정해야 합니다. 예를 들어 다음 그림에서 역할에 할당된 사용자의 콘솔에 장치 전체 초기화 및 제한 사항 지우기 옵션은 나타나지 않지만 확인란이 선택된 옵션은 나타납니다.



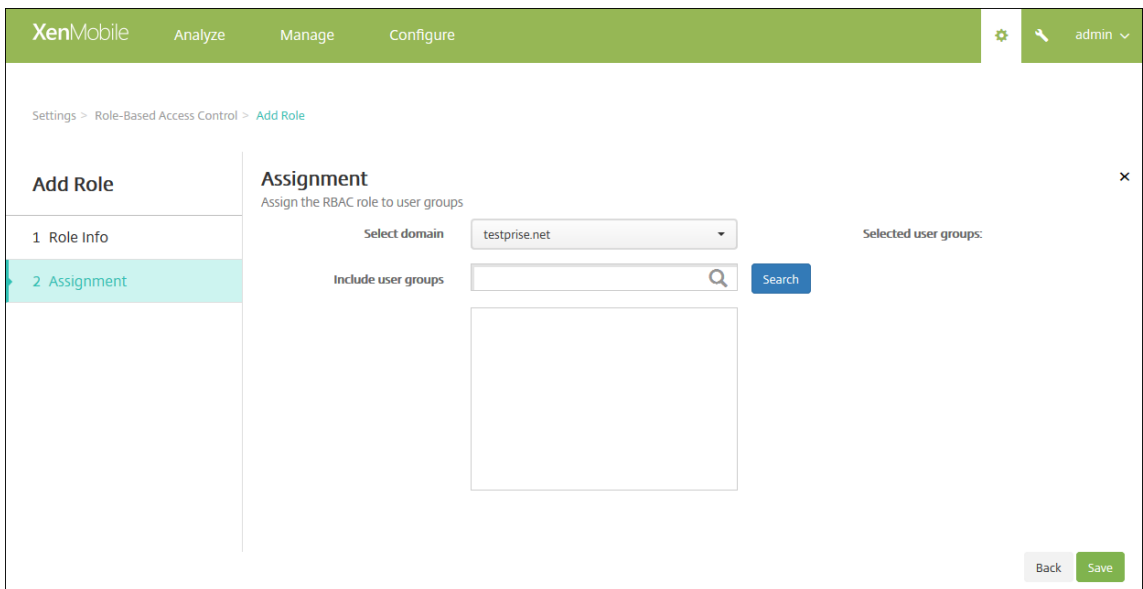
7. 권한 적용: 하나 이상의 사용자 그룹을 선택하여 관리자가 관리할 수 있는 그룹을 제한합니다. 특정 사용자 그룹을 클릭하면 하나 이상의 그룹을 선택할 수 있는 그룹 목록이 나타납니다.

예를 들어 RBAC 관리자에게 ActiveDirectory 및 MSP 사용자 그룹에 대한 권한이 있는 경우:

- 관리자는 ActiveDirectory 그룹, MSP 그룹또는두그룹모두에있는사용자에대한정보에만액세스할수있습니다.
- 관리자는다른로컬또는 AD 사용자를볼수없습니다. 관리자는이러한그룹중하나이하위그룹에속하는사용자를볼수 있습니다.
- 관리자는다음으로초대장을보낼수있습니다.
 - 권한그룹및해당하위그룹
 - 권한그룹및하위그룹의구성원인사용자

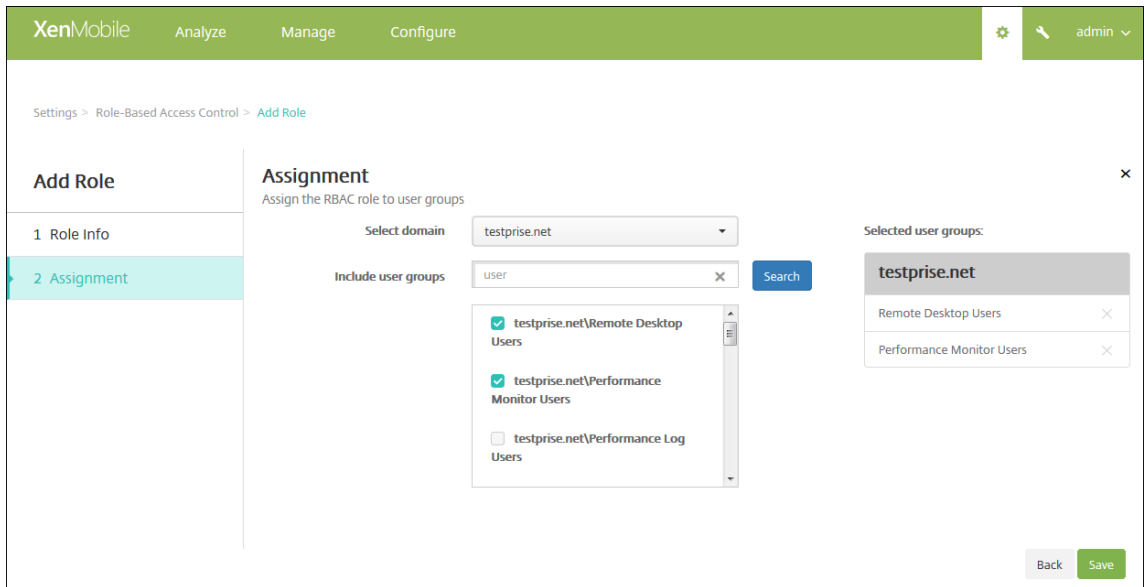


8. 다음을클릭합니다. 할당페이지가나타납니다.



9. 다음정보를입력하여사용자그룹에역할을할당합니다.

- 도메인선택: 목록에서도메인을클릭합니다.
- 사용자그룹포함: 검색을클릭하여사용가능한모든그룹의목록을보거나, 그룹이름전체또는일부를입력하여해당이름 을포함하는그룹으로만목록을제한합니다.
- 나타나는목록에서역할을할당할사용자그룹을선택합니다. 사용자그룹을선택하면해당그룹이 선택된사용자그룹목 록에나타납니다.



참고:

선택된 사용자 그룹 목록에서 사용자 그룹을 제거하려면 사용자 그룹 이름 옆에 있는 X 를 클릭합니다.

10. 저장을 클릭합니다.

알림

January 6, 2020

XenMobile 에서 다음과 같은 용도로 알림을 사용할 수 있습니다.

- 선택적인 사용자 그룹에게 다양한 시스템 관련 기능을 전달합니다. 특정 사용자를 대상으로 이러한 알림을 보낼 수도 있습니다. 예를 들어 모든 iOS 장치 사용자, 장치가 규정 위반 상태인 사용자, 직원 소유의 장치 사용자 등을 대상으로 할 수 있습니다.
- 사용자 및 장치를 등록합니다.
- 특정 조건이 충족될 때 사용자에게 자동으로 알림을 보냅니다 (자동화 동작 사용). 예를 들면 다음과 같습니다.
 - 규정문제로 인해 기업 도메인에서 사용자 장치를 차단할 예정인 경우
 - 장치가 탈옥 또는 루팅된 경우

자동화 동작에 대한 자세한 내용은 [자동화된 동작](#) 을 참조하십시오.

XenMobile 에서 알림을 보내려면 게이트웨이 및 알림 서버를 구성해야 합니다. XenMobile 에서 알림 서버를 설정하고 SMTP(Simple Mail Transfer Protocol) 및 SMS(Short Message Service) 게이트웨이 서버를 구성하여 사용자에게 전자 메일 및 텍스트 (SMS) 알림을 보낼 수 있습니다. 알림을 사용하여 SMTP 또는 SMS 의 두 개 채널로 메시지를 보낼 수 있습니다.

- SMTP 는 연결 지향적인 텍스트 기반 프로토콜로, 일반적으로 TCP(Transmission Control Protocol) 연결을 통해 명령문 자열을 실행하고 필요한 데이터를 제공하는 방식으로 메일을 보낸 사람과 메일을 받는 사람이 통신합니다. SMTP 세션은 SMTP 클라이언트 (메시지를 보내는 사람) 에서 시작된 명령과 이에 대한 SMTP 서버의 응답으로 구성됩니다.

- SMS 는전화, 웹또는모바일통신시스템의문자메시지서비스구성요소입니다. SMS 는표준화된통신프로토콜을사용하여 유선전화또는휴대폰장치에서 SMS 를교환할수있도록합니다.

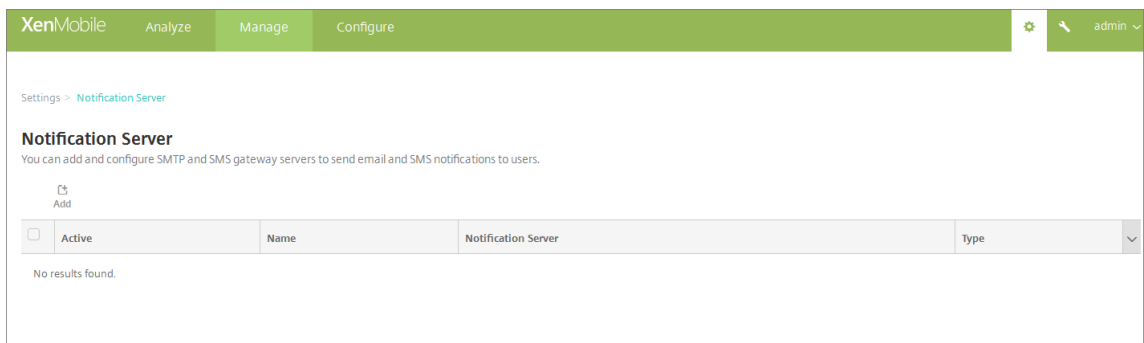
또한 XenMobile 에서이동통신사업자 SMS 게이트웨이를설정하여이동통신사업자의 SMS 게이트웨이를통해전송되는알림을 구성할수있습니다. 이동통신사업자는통신네트워크를통한 SMS 전송의송수신에 SMS 게이트웨이를사용합니다. 이러한텍스트 기반메시지는표준화된통신프로토콜을사용하여유선전화또는휴대폰장치에서 SMS 를교환할수있도록합니다.

사전요구사항

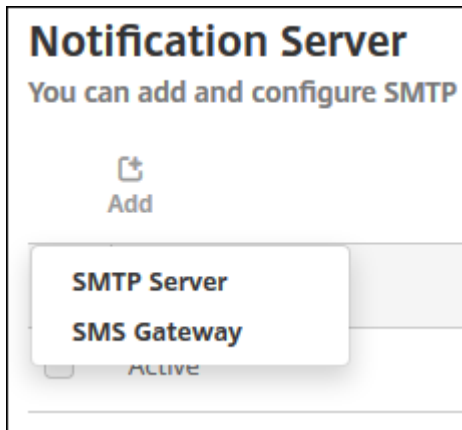
- SMS 게이트웨이를구성하기전에시스템관리자에게문의하여서버정보를확인하십시오. SMS 서버가내부회사서버에서호스트되는지, 호스트되는전자메일서비스의일부인지를확인해야합니다. 후자의경우서비스공급자의웹사이트에서정보를얻어야합니다.
- 사용자에게메시지를보내도록 SMTP 알림서버를구성합니다. 서버가내부서버에서호스트되는경우시스템관리자에게구성정보를문의하십시오. 서버가호스트되는전자메일서비스인경우서비스공급자의웹사이트에서해당하는구성정보를찾으십시오.
- 한번에하나의 SMTP 서버와하나의 SMS 서버만활성화되어야합니다.
- 네트워크 DMZ 에위치한 XenMobile 에서포트 25 를열어내부네트워크의 SMTP 서버를다시가라키도록합니다. 이렇게하면 XenMobile 에서성공적으로알림을보낼수있습니다.

SMTP 서버및 SMS 게이트웨이구성

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 알림에서 알림서버를클릭합니다. 알림서버페이지가나타납니다.



3. 추가를클릭합니다. SMTP 서버또는 SMS 게이트웨이를구성하는옵션이포함된메뉴가나타납니다.



- SMTP 서버를추가하려면 **SMTP** 서버를클릭하고 [SMTP 서버를추가하려면](#)의단계에따라이설정을구성합니다.
- SMS 게이트웨이를추가하려면 **SMS** 게이트웨이를클릭하고 [SMS 게이트웨이를추가하려면](#)의단계에따라이설정을구성합니다.

SMTP 서버추가

Settings > Notification Server > Add SMTP Server

Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*

Description

SMTP Server*

Secure channel protocol

SMTP server port*

Authentication

Microsoft Secure Password Authentication (SPA)

From name*

From email*

▶ **Advanced Settings**

1. 다음설정을구성합니다.

- **이름:** SMTP 서버계정에연결된이름을입력합니다.
- **설명:** 필요한경우서버의설명을입력합니다.
- **SMTP 서버:** 서버의호스트이름을입력합니다. 호스트이름은 FQDN(정규화된도메인이름) 또는 IP 주소일수있습니다.
- **보안채널프로토콜:** 목록에서서버가사용하는보안채널프로토콜에대해 **SSL, TLS** 또는 **없음**을클릭합니다 (보안인증을사용하도록서버가구성된경우). 기본값은 **없음**입니다.

- **SMTP** 서버포트: SMTP 서버에서 사용하는 포트를 입력합니다. 기본적으로 포트는 25 로 설정됩니다. SMTP 연결에 SSL 보안 채널 프로토콜이 사용되는 경우 포트는 465 로 설정됩니다.
 - 인증: 커짐 또는 꺼짐을 선택합니다. 기본값은 꺼짐입니다.
 - 인증을 사용하는 경우 다음 설정을 구성합니다.
 - 사용자 이름: 인증에 사용할 사용자 이름을 입력합니다.
 - 암호: 인증 사용자의 암호를 입력합니다.
 - **Microsoft SPA(보안 암호 인증)**: SMTP 서버에서 SPA 를 사용하는 경우 커짐을 클릭합니다. 기본값은 꺼짐입니다.
 - 발신자 이름: 클라이언트에서 서버의 알림 전자 메일을 수신할 때 보낸 사람 상자에 표시되는 이름을 입력합니다. 예를 들어, 회사 IT 를 입력합니다.
 - 발신자 전자 메일: 전자 메일 받는 사람이 SMTP 서버에서 보낸 알림에 회신할 때 사용하는 전자 메일 주소를 입력합니다.
2. 구성 테스트를 클릭하여 테스트 전자 메일 알림을 보냅니다.
3. 고급 설정을 확장하고 다음 설정을 구성합니다.
- **SMTP** 재시도 횟수: SMTP 서버에서 보낸 실패한 메시지를 재시도 할 횟수를 입력합니다. 기본값은 5 입니다.
 - **SMTP** 시간 제한: SMTP 요청을 보낼 때 대기할 시간 (초) 을 입력합니다. 시간 제한으로 인해 메시지 전송이 지속적으로 실패하는 경우 이 값을 늘립니다. 이 값을 줄일 때는 주의하십시오. 시간 초과로 인해 배달되지 않은 메시지의 수가 늘어날 수 있습니다. 기본값은 30 초입니다.
 - 최대 **SMTP** 받는 사람 수: SMTP 서버에서 보내는 전자 메일 메시지당 최대 받는 사람 수를 입력합니다. 기본값은 100 입니다.
4. 추가를 클릭합니다.

SMS 게이트웨이추가

참고:

XenMobile 은 Nexmo SMS 메시지만지원합니다. Nexmo 메시지사용을위한계정이없는경우 [웹사이트](#)를방문하여계정을만드십시오.

1. 다음설정을구성합니다.

- **이름:** SMS 게이트웨이구성의이름을입력합니다. 이것은필수필드입니다.
- **설명:** 필요한경우구성의설명을입력합니다.
- **키:** 계정을활성화할때시스템관리자가제공한숫자식별자를입력합니다. 이것은필수필드입니다.
- **암호:** 암호분실또는도난시계정에액세스하는데사용할시스템관리자가제공한암호를입력합니다. 이것은필수필드입니다.
- **가상전화번호:** 이필드는북미전화번호 (+1 접두사사용) 로보낼때사용합니다. 이필드에는 Nexmo 가상전화번호를입력해야하며숫자만사용해야합니다. Nexmo 웹사이트에서가상전화번호를구입할수있습니다.
- **HTTPS:** SMS 요청을 Nexmo 에전송할때 HTTPS 를사용할지여부를선택합니다. 기본값은 꺼짐입니다.

중요:

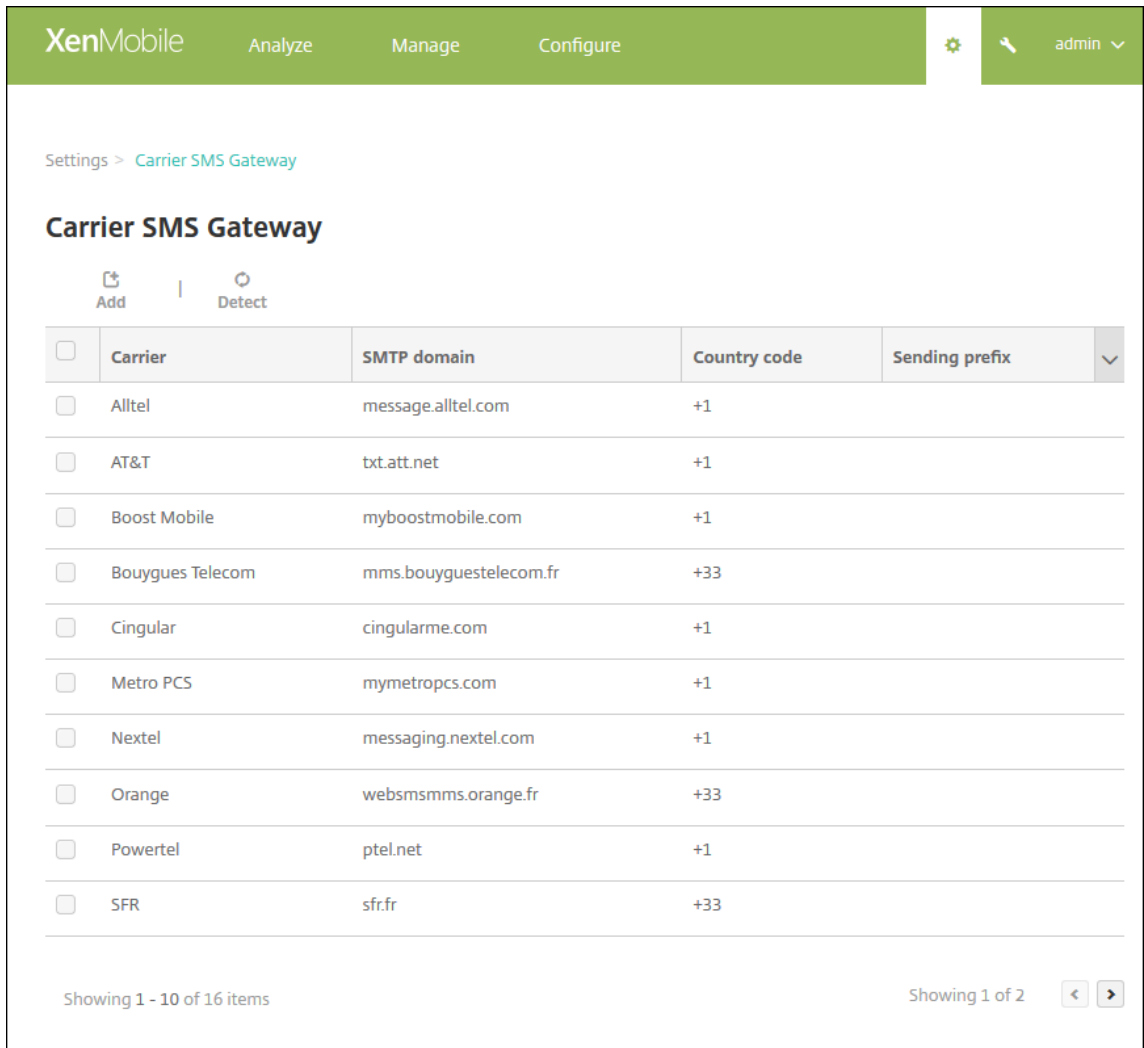
HTTPS 는 꺼짐으로설정하라는 Citrix 지원의지침이없는한 켜짐으로설정하십시오.

- 국가코드: 목록에서조직의받는사람에대한기본 SMS 국가코드접두사를클릭합니다. 이필드는항상 + 기호로시작됩니다. 기본값은 아프가니스탄 **+93** 입니다.
2. 구성테스트를클릭하여현재구성으로테스트메시지를보냅니다. 인증, 가상전화번호오류등과같은연결오류는즉시감지되고 표시됩니다. 휴대폰간에전송된메시지와같은시간내에메시지가수신됩니다.
 3. 추가를클릭합니다.

이동통신사업자 **SMS** 게이트웨이추가

XenMobile 에서이동통신사업자의 SMS 게이트웨이를설정하여이동통신사업자의 SMS 게이트웨이를통해전송되는알림을구성할수있습니다. 이동통신사업자는 SMS(Short Message Service) 게이트웨이를사용하여통신네트워크에서 SMS 전송을보내거나받습니다. 이러한텍스트기반메시지는표준화된통신프로토콜을사용하여유선전화또는휴대폰장치에서 SMS 를교환할수있도록합니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 알림에서 이동통신사업자 **SMS** 게이트웨이를클릭합니다. 이동통신사업자 **SMS** 게이트웨이페이지가열립니다.



3. 다음중하나를수행합니다.

- 검색을클릭하여자동으로게이트웨이를검색합니다. 새로운이동통신사업자가검색되지않았음을나타내거나등록된 장치중에서검색된새이동통신사업자를나열하는대화상자가나타납니다.
- 추가를클릭합니다. 이동통신사업자 **SMS** 게이트웨이추가대화상자가나타납니다.

Add a Carrier SMS Gateway ✕

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

Carrier*	<input type="text"/>
Gateway SMTP domain*	<input type="text"/>
Country code*	United States +1 ▼
Email sending prefix	<input type="text"/>

Cancel
Add

참고:

XenMobile 은 Nexmo SMS 메시지만지원합니다. Nexmo 메시지사용을위한계정이없는 경우 [웹사이트](#)를방문하여계정을만드십시오.

4. 다음설정을구성합니다.

- **이동통신사업자:** 이동통신사업자의이름을입력합니다.
- **게이트웨이 SMTP 도메인:** SMTP 게이트웨이에연결된도메인을입력합니다.
- **국가코드:** 목록에서이동통신사업자의국가코드를클릭합니다.
- **전자메일전송접두사:** 필요한경우전자메일전송접두사를지정합니다.

5. 추가를클릭하여새이동통신사업자를추가하거나 취소를클릭하여새이동통신사업자를추가하지않습니다.

알림템플릿만들기및업데이트

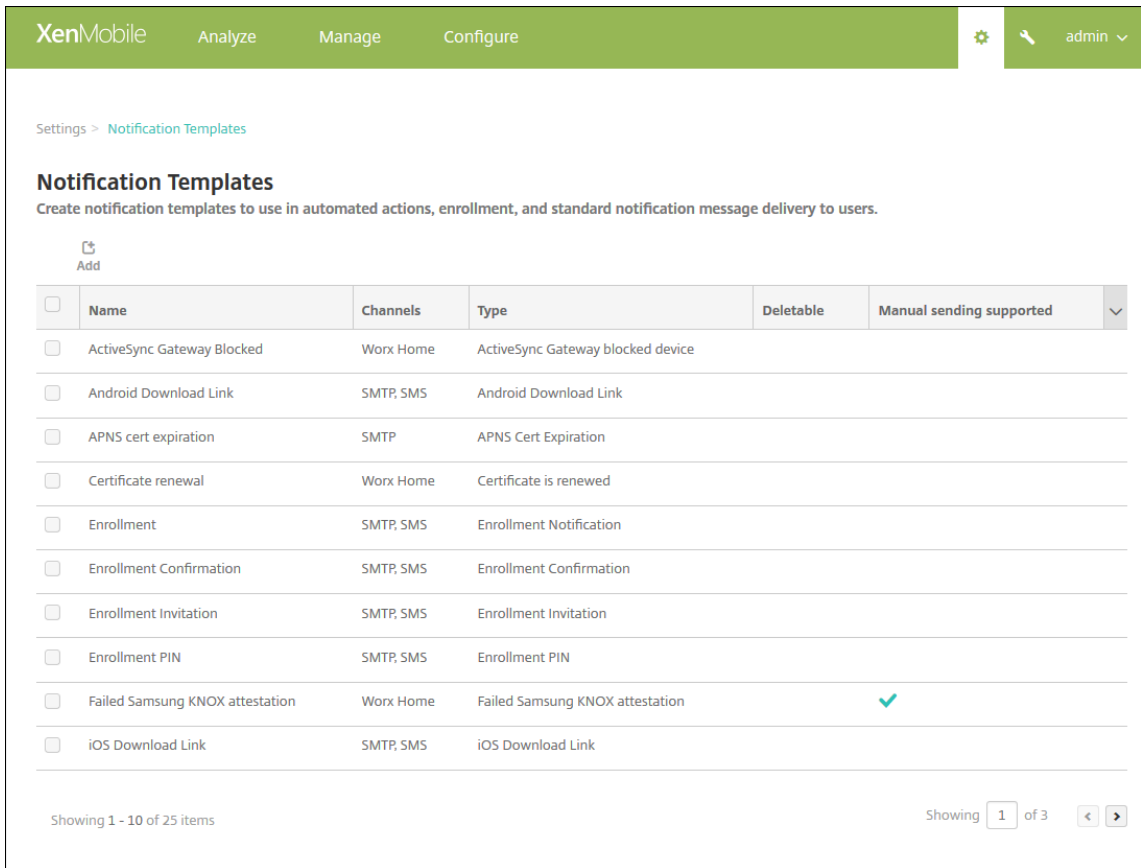
XenMobile 에서자동화동작, 등록및사용자에게보내는표준알림메시지에서사용할알림템플릿을만들거나업데이트할수있습니다. 세가지채널 (Secure Hub, SMTP 또는 SMS) 을통해메시지를보내는알림템플릿을구성합니다.

XenMobile에는 시스템의 모든 장치에서 자동으로 응답하는 서로 다른 이벤트 유형을 반영하는 다수의 미리 정의된 알림 템플릿이 있습니다.

참고:

SMTP 또는 SMS 채널을 사용하여 사용자에게 알림을 보내려는 경우 채널을 설정한 후 활성화해야 합니다. 채널이 설정되지 않은 경우 알림 템플릿을 추가할 때 채널을 설정하라는 메시지가 표시됩니다.

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 알림 템플릿을 클릭합니다. 알림 템플릿 페이지가 나타납니다.



알림 템플릿 추가

1. 추가를 클릭합니다. SMS 게이트웨이 또는 SMTP 서버가 설정되지 않은 경우 SMS 및 SMTP 알림의 사용에 관한 메시지가 표시됩니다. SMTP 서버 또는 SMS 게이트웨이를 지금 설정하거나 나중에 설정하도록 선택할 수 있습니다.

SMS 또는 SMTP 서버 설정을 지금 설정하도록 선택하는 경우 설정 페이지의 알림 서버 페이지로 리디렉션됩니다. 사용할 채널을 설정한 후 알림 템플릿 페이지로 돌아가서 알림 템플릿 추가 또는 수정을 계속할 수 있습니다.

중요:

SMS 또는 SMTP 서버 설정을 나중에 설정하도록 선택하는 경우 알림 템플릿을 추가하거나 편집할 때 이러한 채널을 활성화

화할수없으므로사용자알림을보낼때이러한채널을사용할수없게됩니다.

2. 다음설정을구성합니다.

- 이름: 템플릿에대한설명적이름을입력합니다.
- 설명: 템플릿에대한설명을입력합니다.
- 유형: 목록에서알림유형을클릭합니다. 선택한유형에대해지원되는채널만표시됩니다. 미리정의된템플릿인 APNS 인증서만료템플릿만허용됩니다. 즉, 이유형의새템플릿을추가할수없습니다.

참고:

일부템플릿유형의경우유형아래에 '수동보내기지원' 이라는구가표시됩니다. 이구는 대시보드및 장치페이지의 알림목록에있는템플릿을사용하여사용자에게수동으로알림을보낼수있음을의미합니다. 모든채널에서제목또는메시지필드에다음매크로를사용하는템플릿에는수동보내기를사용할수없습니다.

- `{outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `{outofcompliance.reason(smg_block)}`

3. 채널에서이알림에사용할각채널에대한정보를구성합니다. 일부또는모든채널을선택할수있습니다. 알림을보내는방법에따라다른채널을선택합니다.

- **Secure Hub** 를선택하는경우 iOS 및 Android 장치만알림을수신하며장치의알림트레이에표시됩니다.
- **SMTP** 를선택하는경우전자메일주소를등록한대부분의사용자가메시지를수신합니다.
- **SMS** 를선택하는경우 SIM 카드가있는장치를사용하는사용자만알림을수신합니다.

Secure Hub:

- 활성화: 알림채널을사용하려면클릭합니다.
- 메시지: 사용자에게보낼메시지를입력합니다. Secure Hub 를사용하는경우필수필드입니다. 메시지에서매크로를사용하는방법에대한자세한내용은 매크로를참조하십시오.
- 사운드파일: 목록에서알림이수신될때울릴알림사운드를클릭합니다.

SMTP:

- 활성화: 알림채널을사용하려면클릭합니다.
SMTP 서버를설정후에만 SMTP 알림을활성화할수있습니다.
- 보낸사람: 알림을보낸사람을선택적으로입력합니다. 이름, 전자메일주소또는둘다를입력할수있습니다.
- 받는사람: 이필드에는올바른 SMTP 받는사람주소로알림이전송되도록임시알림을제외한모든알림에대해미리작성된매크로가포함됩니다. 템플릿의매크로는수정하지않는것이 좋습니다. 세미콜론 (;) 으로주소를구분하여사용자 외에받는사람을추가할수있습니다 (예: 회사관리자). 임시알림을보내려면이페이지에서특정받는사람을입력하거나 관리 > 장치페이지에서장치를선택하고거기에서알림을보낼수있습니다. 자세한내용은 장치에서참조하십시오.
- 제목: 알림에대한설명적인제목을입력합니다. 이것은필수필드입니다.
- 메시지: 사용자에게보낼메시지를입력합니다. 메시지에서매크로를사용하는방법에대한자세한내용은 매크로를참조하십시오.

SMS:

- **활성화:** 알림채널을사용하려면클릭합니다.

SMTP 서버를설정후에만 SMTP 알림을활성화할수있습니다.

- **받는사람:** 이필드에는올바른 SMS 받는사람주소로알림이전송되도록임시알림을제외한모든알림에대해미리작성된매크로가포함됩니다. 템플릿의매크로는수정하지않는것이 좋습니다. 임시알림을보내려면특정받는사람을입력하거나 **관리 > 장치페이지**에서장치를선택할수있습니다.
- **메시지:** 사용자에게보낼메시지를입력합니다. 이것은필수필드입니다. 메시지에서매크로를사용하는방법에대한자세한내용은 [매크로](#)를참조하십시오.

4. 추가를클릭합니다. 모든채널이올바르게구성되면 알림템플릿페이지에 SMTP, SMS 및 Secure Hub 순서로표시됩니다. 올바르게구성되지않은채널은올바르게구성된채널뒤에표시됩니다.

알림템플릿편집

1. 알림템플릿을선택합니다. 해당템플릿에관련된편집페이지가나타나고거기에서 유형필드를제외한모든항목을변경할수있으며채널을활성화하거나비활성화할수있습니다.
2. 저장을클릭합니다.

알림템플릿삭제

자신이추가한알림템플릿만삭제할수있습니다. 미리정의된알림템플릿은삭제할수없습니다.

1. 기존의알림템플릿을선택합니다.
2. 삭제를클릭합니다. 확인대상자가나타납니다.
3. 삭제를클릭하여알림템플릿을삭제하거나 취소를클릭하여알림템플릿삭제를취소합니다.

장치

September 27, 2019

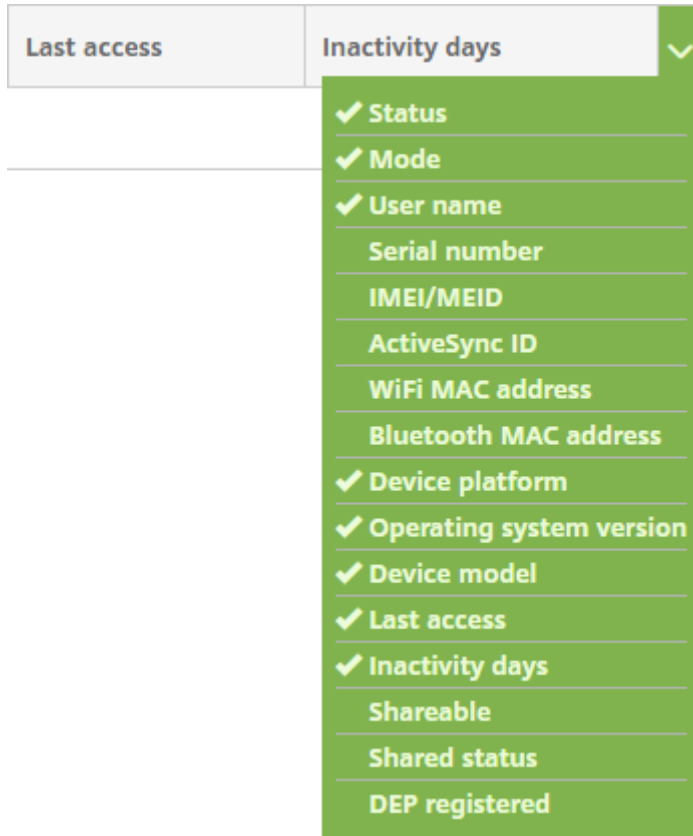
Citrix XenMobile 은단일관리콘솔에서다양한유형의장치를프로비저닝, 관리, 보안및인벤토리를수행할수있습니다.

XenMobile 서버데이터베이스는모바일장치목록을저장합니다. 고유일련번호또는 IMEI(International Mobile Station Equipment Identity)/MEID(Mobile Equipment Identifier) 각각모바일장치를고유하게정의합니다. XenMobile 콘솔에장치를채우려면수동으로장치를추가하거나파일에서장치목록을가져올수있습니다. 장치프로비저닝파일형식에대한자세한내용은이문서뒷부분에서장치프로비저닝파일형식을참조하십시오.

XenMobile 콘솔의 장치페이지에는각장치와다음과같은정보가나열됩니다.

- 상태: 장치의탈옥상태, 관리되는상태, Active Sync Gateway 를사용할수있는지여부및배포상태가아이콘으로나타납니다.
- 모드: 장치모드가 MDM 또는 MAM 인지, 아니면둘모두인지.
- 사용자이름, 장치플랫폼, 운영체제버전, 장치모델, 마지막엑세스및 비활성일수같은장치에대한기타정보. 이러한머리글은 기본적으로표시됩니다.

장치테이블을사용자지정하려면마지막머리글의아래쪽화살표를클릭하십시오. 그런다음테이블에표시할추가머리글을선택하거나 제거할머리글을선택취소합니다.



수동으로장치를추가하고, 장치프로비저닝파일에서장치를가져오고, 장치세부정보를편집하고, 보안작업을수행하고, 장치에알림을보낼수있습니다. 모든장치테이블데이터를.csv 파일로내보내사용자지정보고서를만들수도있습니다. 서버는모든장치특성을내보냅니다. 필터를적용한경우.csv 파일을만들때 XenMobile 이필터를사용합니다.

수동으로장치추가

1. XenMobile 콘솔에서 관리 > 장치를클릭합니다. 장치페이지가나타납니다.

Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>	MDM MAM		Android	5.0.2
<input type="checkbox"/>	MDM MAM		iOS	8.4.1

2. 추가를 클릭합니다. 장치추가페이지가 나타납니다.

3. 다음설정을구성합니다.

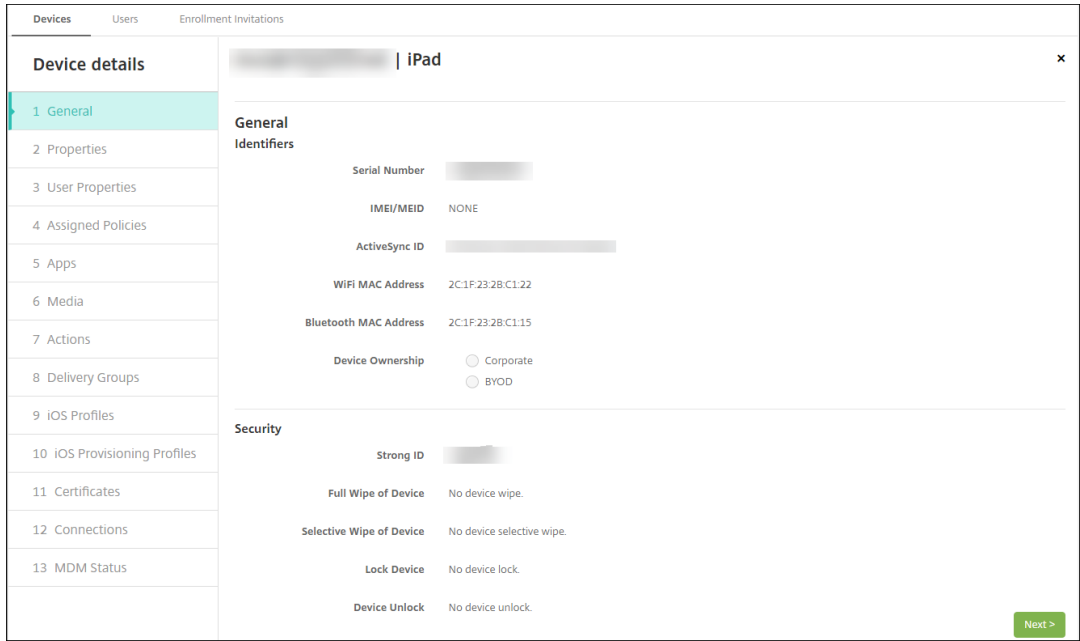
- 플랫폼선택: **iOS** 또는 **Android** 를클릭합니다.
- 일련번호: 장치일련번호를입력합니다.
- **IMEI/MEID:** Android 장치에만해당하며, 필요한경우장치 IMEI/MEID 정보를입력합니다.

4. 추가를 클릭합니다. 장치테이블이 나타나고 목록 맨 아래에 장치가 추가되어 있습니다. 추가한 장치를 선택한 다음 나타나는 메뉴에서 편집을 클릭하여 장치 세부 정보를 보고 확인합니다.

참고:

장치 옆에 있는 확인란을 선택하면 장치 목록 위에 옵션 메뉴가 표시됩니다. 목록에서 아무 위치를 클릭하면 목록의 오른쪽에 옵션 메뉴가 나타납니다.

- 엔터프라이즈 (XME) 또는 MDM 모드로 구성된 XenMobile Server
- 구성된 LDAP
- 로컬 그룹 및 로컬 사용자를 사용 중인 경우:
 - 하나 이상의 로컬 그룹.
 - 로컬 그룹에 할당된 로컬 사용자.
 - 배달 그룹은 로컬 그룹과 연결됩니다.
- Active Directory 를 사용 중인 경우:
 - 배달 그룹은 Active Directory 그룹과 연결됩니다.



5. 일반페이지에는일련번호, ActiveSync ID 및플랫폼유형에대한기타정보같은장치 식별자가나열됩니다. 장치소유권의경우 회사또는 **BYOD** 를선택합니다.

일반페이지에는강력한 ID, 장치잠금, 활성화잠금바이패스및플랫폼유형에대한기타정보같은장치 보안속성도나열됩니다. 장치전체초기화필드에는사용자 PIN 코드가포함됩니다. 장치가초기화된후사용자는이코드를입력해야합니다. 사용자가코드를잊은경우여기서코드를조회할수있습니다.

6. 속성페이지에는 XenMobile 이프로비저닝장치속성이나열됩니다. 이목록에는장치를추가하는데사용된프로비저닝파일에포함된모든장치속성이표시됩니다. 속성을추가하려면 추가를클릭한다음목록에서속성을선택합니다. 각속성에유효한값에대해서는 [장치속성이름및값 PDF](#) 를참조하십시오.

속성을추가하면처음에는속성을추가한범주아래에나타납니다. 다음을클릭한후 속성페이지로돌아가면속성이해당목록에 나타납니다.

속성을삭제하려면목록위에마우스포인트를이동하고오른쪽에있는 **X** 를클릭합니다. 항목이즉시삭제됩니다.

7. 나머지 장치세부정보섹션에는장치에대한요약정보가포함되어있습니다.

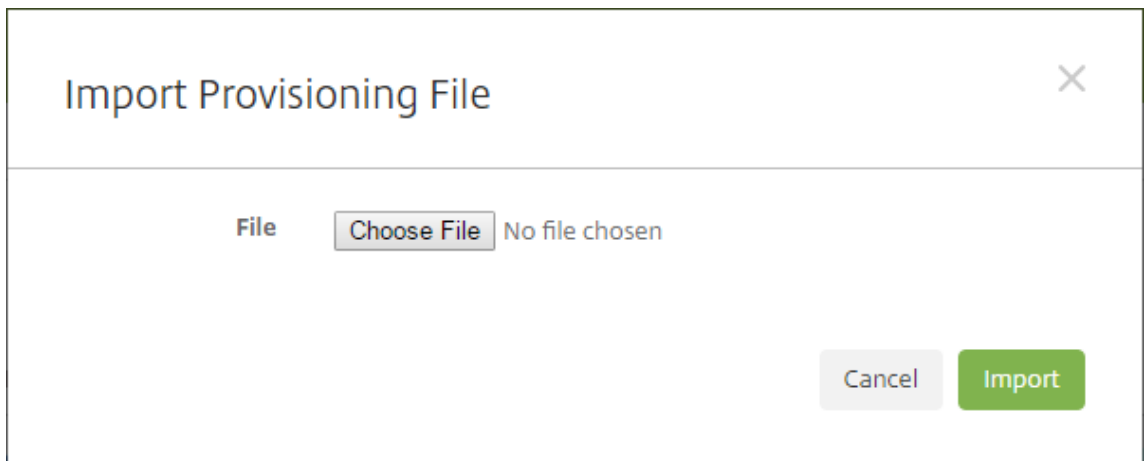
- 사용자속성: RBAC 역할, 그룹구성원자격, VPP 계정및사용자속성을표시합니다. 이페이지에서 VPP 계정을사용 중지할수있습니다.
- 할당된정책: 배포된정책, 보류중인정책및실패한정책의수를포함하여할당된정책의수를표시합니다. 각정책에대해 정책이름, 유형및마지막배포정보를제공합니다.
- 앱: 마지막인벤토리에대한설치된앱배포, 보류중인앱배포및실패한앱배포의수를표시합니다. 앱이름, 식별자, 유형 및기타정보를제공합니다.
- 미디어: 마지막인벤토리에대해배포된미디어배포, 보류중인미디어배포및실패한미디어배포의수를표시합니다.
- 동작: 배포된동작, 보류중인동작및실패한동작의수를표시합니다. 마지막배포의동작이름및시간을제공합니다.
- 배달그룹: 성공한배달그룹, 보류중인배달그룹및실패한배달그룹의수를표시합니다. 각배포에대해배달그룹이름및 배포시간을제공합니다. 배달그룹을선택하여상태, 동작및채널또는사용자를비롯한자세한정보를확인합니다.

- **iOS** 프로필: 이름, 유형, 조직및설명을비롯한마지막 iOS 프로필인벤토리를표시합니다.
- **iOS** 프로비전프로필: UUID, 만료날짜및관리여부와같은엔터프라이즈배포프로비전프로필정보를표시합니다.
- **인증서:** 유효하거나, 만료되거나, 해지된인증서에대해유형, 공급자, 발급자, 일련번호및만료전까지남은날짜와같은정보를표시합니다.
- **연결:** 첫번째연결상태및마지막연결상태를표시합니다. 각연결에대해사용자이름, 마지막두번째 (끝에서두번째) 인증시간및마지막인증시간을제공합니다.
- **MDM** 상태: MDM 상태, 마지막푸시시간및마지막장치회신시간같은정보를표시합니다.
- **TouchDown:** (Android 장치만해당) 마지막장치인증및마지막으로인증된사용자에대한정보를표시합니다. 적용가능한각정책이름및정책값을제공합니다.

프로비저닝파일에서장치가져오기

이동통신사업자또는장치제조업체가제공한파일을가져오거나고유한장치프로비저닝파일을만들수있습니다. 자세한내용은이문서 뒷부분에서장치프로비저닝파일형식을참조하십시오.

1. 관리 > 장치로이동하여 가져오기를클릭합니다. 프로비저닝파일가져오기대화상자가나타납니다.



2. 파일선택을클릭한다음가져오려는파일을찾습니다.
3. 가져오기를클릭합니다. 장치테이블에가져온파일이나열됩니다.
4. 장치정보를편집하려면장치를선택한다음 편집을클릭합니다. 장치세부정보페이지에대한자세한내용은수동으로장치추가를참조하십시오.

장치에알림보내기

장치페이지에서장치에알림을보낼수있습니다. 알림에대한자세한내용은 [알림](#)을참조하십시오.

1. 관리 > 장치페이지에서알림을보낼하나이상의장치를선택합니다.
2. 알림을클릭합니다. 알림대화상자가나타납니다. 받는사람필드에알림을받을모든장치가나열됩니다.

Notification
✕

Recipients

Templates Ad Hoc ▾

Channels SMTP SMS

SMTP

SMS

Sender

Subject

Message

Cancel
Notify

3. 다음설정을구성합니다.

- **템플릿:** 목록에서보내려는알림유형을클릭합니다. 임시템플릿을제외한각템플릿의경우 제목및 메시지필드에선택한템플릿에구성된텍스트가표시됩니다.
- **채널:** 메시지를보내는방법을선택합니다. 기본값은 **SMTP** 및 **SMS** 입니다. 각채널의메시지형식을확인하려면탭을클릭합니다.
- **보낸사람:** 선택적보낸사람을입력합니다.
- **제목:** 임시메시지의경우 제목을입력합니다.
- **메시지:** 임시메시지의경우메시지를입력합니다.

4. 알림을클릭합니다.

장치테이블내보내기

1. 내보내기파일에나타날항목에따라 장치테이블을필터링합니다.
2. 장치테이블위에서 내보내기단추를클릭합니다. 필터링된 장치테이블의정보가추출되어.csv 파일로변환됩니다.
3. 메시지가표시되면.csv 파일을열거나저장합니다.

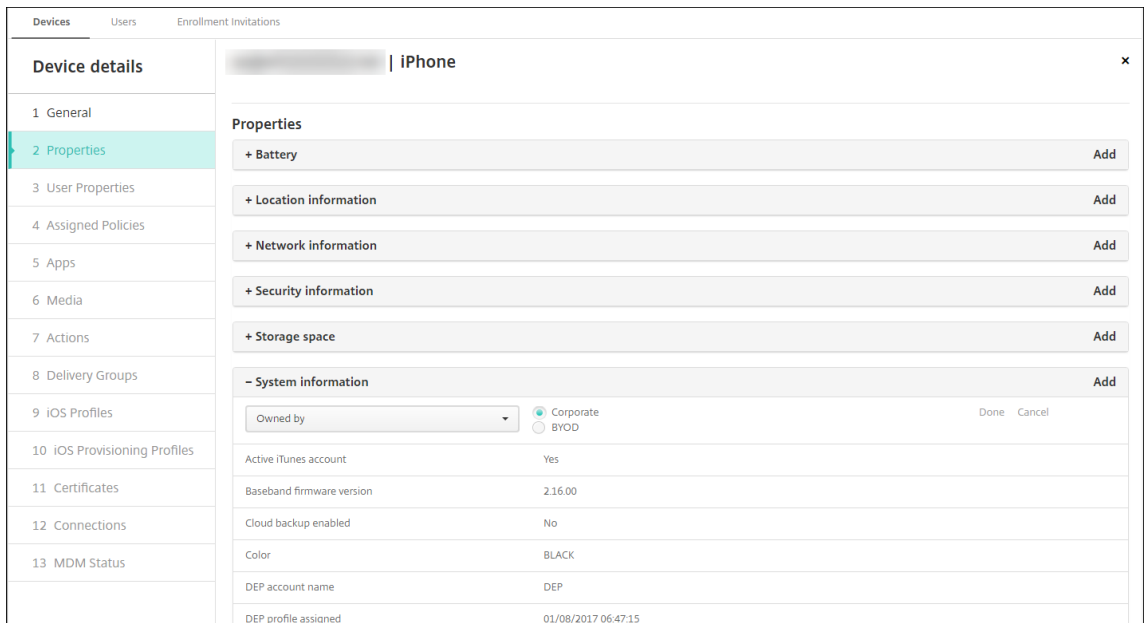
사용자장치에수동으로태그지정

다음과같은방법으로 XenMobile 에서장치에수동으로태그를지정할수있습니다.

- 초대기반등록프로세스도중
- 자가지원포털등록프로세스도중
- 장치소유권을장치속성으로추가

장치에회사소유또는직원소유태그를지정하는옵션도있습니다. 자가지원포털을사용하여장치를자가등록할때장치에회사소유또는 직원소유태그를지정할수있습니다. 다음과같이장치에수동으로태그를지정할수도있습니다.

1. XenMobile 콘솔의 장치탭에서장치에속성을추가합니다.
2. 이름이 소유자인속성을추가하고 회사또는 **BYOD**(직원소유) 중에서선택합니다.



장치프로비저닝파일형식

여러모바일운영자또는장치제조업체에서인증된모바일장치의목록을제공합니다. 이러한목록을사용하면긴모바일장치목록을수동으로입력할필요가없습니다. XenMobile 은지원되는세가지장치유형 (Android, iOS 및 Windows) 모두에공통되는가져오기파일형식을지원합니다.

수동으로만들며장치를 XenMobile 로가져오기위해사용하는프로비저닝파일은다음과같은형식이여야합니다.

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2;  
... propertyNameN;propertyValueN
```

다음사항에유의하십시오.

- 각속성에유효한값에대해서는 [장치속성이름및값 PDF](#) 를참조하십시오.
- UTF-8 문자집합을사용합니다.
- 프로비저닝파일내에서필드를구분하려면세미콜론 (;) 을사용합니다. 필드자체에세미콜론이포함되는경우백슬래시문자 (\) 로이스케이프처리합니다.

다음속성을예로들겠습니다.

```
propertyV;test;1;2
```

이경우다음과같이이스케이프처리합니다.

```
propertyV\;test\;1\;2
```

- 일련번호는 iOS 장치식별자이므로 iOS 장치에는일련번호가필수입니다.
- 다른장치플랫폼의경우일련번호또는 IMEI 를포함해야합니다.
- **OperatingSystemFamily** 의유효한값은 **WINDOWS, ANDROID** 또는 **iOS** 입니다.

장치프로비저닝파일의예:

```
1 '1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyName;  
   propertyV\;test\;1\;2;prop 2  
2 2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyName;  
   propertyV$*&&éétest  
3 3050BF3F517301081610065510590393;35244201625379903;iOS;test;  
4 4050BF3F517301081610065510590393;;iOS;test;  
5 ;55244201625379903;ANDROID;test.testé;value;'
```

파일의각줄은장치하나를기술합니다. 위샘플에서첫번째항목은다음과같은의미입니다.

- SerialNumber: 1050BF3F517301081610065510590391
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- ProertyName: propertyName
- PropertyValue: propertyV\;test\;1\;2;prop 2

ActiveSync Gateway

January 6, 2020

ActiveSync 는 Microsoft 에서개발한모바일데이터동기화프로토콜입니다. ActiveSync 는핸드헬드장치및데스크톱 (또는 랩톱) 컴퓨터와데이터를동기화합니다.

XenMobile 에서 ActiveSync Gateway 규칙을구성할수있습니다. 이러한규칙에따라장치에서 ActiveSync 데이터에대한 액세스를허용하거나거부할수있습니다. 예를들어누락된필수앱규칙을활성화하면 XenMobile 은필수앱에대해앱액세스정책을 확인하고필수앱이누락된경우 ActiveSync 데이터에대한액세스를거부합니다. 각규칙에대해 허용또는 거부중하나를선택할수있습니다. 기본설정은 허용입니다.

앱액세스장치정책에대한자세한내용은 [앱액세스장치정책](#)을참조하십시오.

XenMobile 은다음규칙을지원합니다.

익명장치: 장치가익명모드인지확인합니다. 이확인인장치гада시연결할때 XenMobile 이사용자를다시인증할수없는경우사용할수있습니다.

Samsung KNOX 증명실패: 장치가 Samsung KNOX 증명서버의쿼리에실패했는지확인합니다.

금지된앱: 장치에앱액세스정책에정의된금지된앱이있는지확인합니다.

암시적허용및거부: 이동작이 ActiveSync Gateway 의기본값입니다. 게이트웨이는다른필터규칙기준을충족시키지않는모든 장치의장치목록을만들고해당목록을기반으로연결을허용하거나거부합니다. 일치하는규칙이없으면기본값은암시적허용입니다.

비활성장치: Server Properties(서버속성) 의 Device Inactivity Days Threshold(장치비활성일수임계값) 설정에정의된대로장치가비활성상태인지확인합니다.

누락된필수앱: 앱액세스정책에정의된대로, 장치에필수앱이누락되었는지확인합니다.

비추천앱: 앱액세스정책에정의된대로, 장치에비추천앱이있는지확인합니다.

규정을준수하지않는암호: 사용자암호가규정을준수하는지확인합니다. iOS 및 Android 장치에서 XenMobile 은현재장치에 있는암호가장치로보낸암호정책을준수하는지여부를확인할수있습니다. 예를들어 iOS 에서 XenMobile 이암호정책을장치에 보내는경우 60 분내에암호를설정해야합니다. 사용자가암호를설정하기전에암호가규정을준수하지않을수있습니다.

규정위반장치: 규정위반장치속성에따라장치가규정을위반하는지여부를확인합니다. 이속성은대개자동화된동작이나 XenMobile API 를활용하는제 3 자에의해변경됩니다.

해지된상태: 장치인증서가해지되었는지여부를확인합니다. 해지된장치는다시권한이부여될때까지다시등록할수없습니다.

루팅된 Android 및탈옥 iOS 장치: Android 또는 iOS 장치가탈옥되어있는지확인합니다.

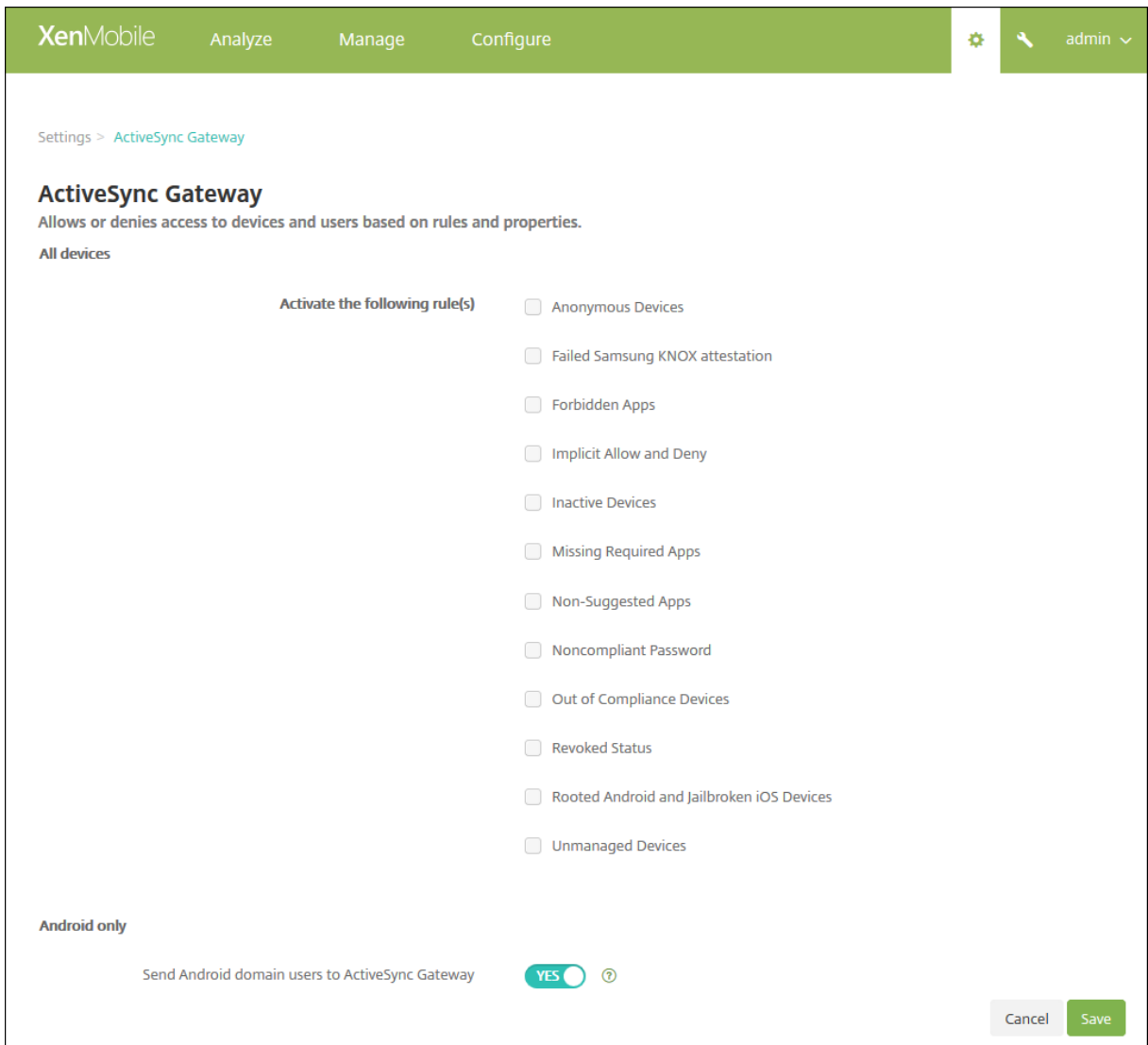
관리되지않는장치: 장치가여전히 XenMobile 제어하에관리되는상태에있는지확인합니다. 예를들어 MAM 모드에서실행중인 장치나등록되지않은장치는관리되지않습니다.

Android 도메인사용자를 ActiveSync Gateway 로보내기: XenMobile 이 Android 장치정보를 ActiveSync Gateway 로보내도록하려면 예를클릭합니다.

ActiveSync Gateway 설정을구성하려면

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.

2. 서버아래에서 **ActiveSync Gateway** 를 클릭합니다. **ActiveSync Gateway** 페이지가 나타납니다.



1. **Activate the following rules(다음규칙활성화)** 에서활성화하려는하나이상의규칙을선택합니다.
2. **Android** 만의 **Android** 도메인사용자를 **ActiveSync Gateway** 로보내기에서 예를 클릭하여 XenMobile 이 Android 장치정보를 ActiveSync Gateway 로보내도록합니다.
3. 저장을클릭합니다.

장치관리에서 **Android Enterprise** 로마이그레이션

September 27, 2019

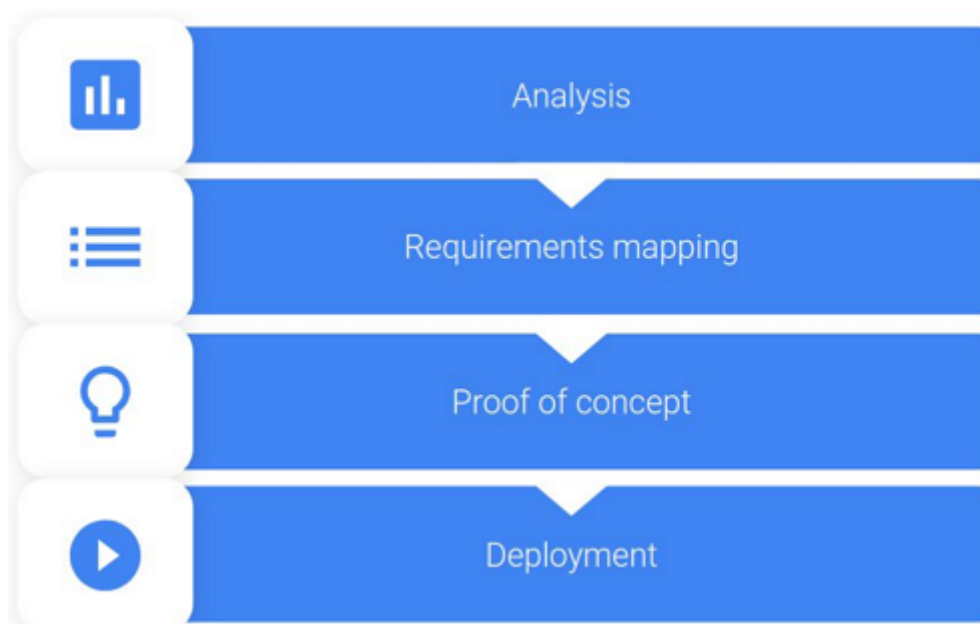
이문서에서는레거시 Android 장치관리에서 Android Enterprise 로마이그레이션할때의고려사항및권장사항에대해설명함

니다. Google 은 Android 장치관리 API 를더이상사용하지않습니다. 이 API 는 Android 장치에서엔터프라이즈앱을지원했습니다. Android Enterprise 는 Google 과 Citrix 가권장하는최신관리솔루션입니다.

XenMobile 은 Android Enterprise 를 Android 장치에대한기본등록방법으로변경하는중입니다. Google 에서이 API 의 사용을중단한후에는장치등록모드에서 Android Q 장치에대한등록이실패합니다.

Android Enterprise 에는완전관리되는장치및작업프로필장치모드에대한지원이포함됩니다. Google 게시물 [Android Enterprise Migration Bluebook\(Android Enterprise 마이그레이션지침서\)](#)에레거시장치관리와 Android Enterprise 의차이점이자세히설명되어있습니다. Google 에서마이그레이션정보를읽어보시기바랍니다.

또한이게시물은장치관리마이그레이션의 4 단계에대해설명하며다음다이어그램을포함하고있습니다. 이문서에는마이그레이션단계에서 XenMobile 과관련된권장사항이포함되어있습니다.



[Android Enterprise Migration Bluebook \(Android Enterprise 마이그레이션지침서\)](#)의다이어그램. Google 의허가하에다시게시되었습니다.

장치관리사용중단의영향

Google 은다음장치관리 API 의사용을중단할예정입니다. Android Q API 수준을대상으로 Secure Hub 를업그레이드한후에는 Android Q 를실행하는장치에서이러한 API 가작동하지않습니다.

- 카메라사용안함: 장치카메라에대한엑세스를제어합니다.
- Keyguard 기능: 생체인식및패턴과같은장치잠금과관련된기능을제어합니다.
- 암호만료: 구성가능한기간이지난후사용자에게암호를변경하도록강제합니다.
- 암호제한: 제한적인암호요구사항을설정합니다.

API 사용중단은 Citrix MAM 전용모드에등록된장치에는영향을주지않습니다.

권장사항

다음은 Android 레거시장치관리모드에이미등록된장치, 등록되지않은장치및 Citrix MAM 전용모드에등록된장치에대한권장 사항입니다.

장치등록상태	권장작업
기존장치가장치관리모드에등록되었으며 Android Q 로업 그레이드할수있습니다.	장치를 Android Q 로업그레이드하기전에장치관리모드 에서 Android Enterprise 로마이그레이션하십시오.
기존장치가장치관리모드로등록되어있습니다. 장치를 Android Q 로업그레이드할수없습니다.	장치를장치관리모드로유지할수있습니다. 그러나장치새로고 침시 Android Enterprise 로장치를이동할계획을세우십 시오.
기존장치가장치관리모드에등록되었으며 Android Q 로업 그레이드되었습니다.	Google 이 API 의사용을중단하기전에장치관리모드에서 Android Enterprise 로마이그레이션하십시오. XenMobile 콘솔에이러한장치에대한경고메시지가나타납 니다.
새로운장치가 Android Q 와함께제공되었고장치관리모드 에등록되었습니다.	Google 이 API 의사용을중단하기전에장치관리모드에서 Android Enterprise 로마이그레이션하십시오. XenMobile 콘솔에이러한장치에대한경고메시지가나타납 니다.
Android Q 와함께제공되거나업그레이드할수있는새장치 입니다. 장치는등록되지않았습니다.	모든새로운장치에대해 Android Enterprise 를사용하십 시오.
Android Q 의새장치또는기존장치는 Google 이 API 의 사용을중단한후장치관리모드에등록됩니다.	Google API 사용중단의영향을방지하려면 Google 에서 API 사용을중단하기전에 Android Enterprise 로마이그 레이션하는것이 좋습니다. 이날짜이후에는이러한장치의등록 이실패합니다.
Citrix MAM 전용모드에등록된새장치또는기존장치	따로수행해야할작업은없습니다. Google API 사용중단은 MAM 전용모드의장치에는영향을주지않습니다.

분석

마이그레이션의분석단계는다음으로구성됩니다.

- 레거시 Android 설정파악
- 레거시기능을 Android Enterprise 기능에매핑할수있도록레거시설정문서화

권장되는분석

1. XenMobile 에서 Android Enterprise 평가: 완전관리되는장치, 작업프로필로완전관리되는장치, 더이상사용되지않는장치, 작업프로필 (BYOD).
2. Android Enterprise 를기준으로현재장치관리기능을분석합니다.
3. 장치관리사용사례를문서화합니다.

장치관리사용사례를문서화하려면:

1. 스프레드시트를만들고 XenMobile 콘솔에서현재정책그룹을나열합니다.
2. 기존정책그룹을기반으로별도의사용사례를생성합니다.
3. 각사용사례에대해다음을문서화합니다.

- 이름
- 비즈니스소유자
- 사용자 ID 모델
- 장치요구사항
 - 보안
 - 관리
 - 유용성
- 장치인벤토리
 - 제조사및모델
 - OS 버전
- 앱

4. 각앱에대해다음을나열합니다.

- 앱이름
- 패키지이름
- 호스팅방법
- 앱이공개또는비공개인지여부
- 앱이필수인지여부 (true/false)

요구사항매핑

완료된분석을바탕으로 Android Enterprise 기능요구사항을결정합니다.

권장되는요구사항매핑

1. 관리모드및등록방법을결정합니다.
 - 작업프로필 (BYOD): 재등록이필요합니다. 공장기본값으로재설정할필요가없습니다.

- 완전관리형: 공장기본값으로 재설정해야 합니다. QR 코드, NFC(근거리통신) 범프, DPC(장치정책컨트롤러) 식별자, 제로터치를 사용하여 장치를 등록합니다.
2. 앱 마이그레이션 전략을 만듭니다.
 3. 사용 사례 요구 사항을 Android Enterprise 기능에 매핑합니다. 요구 사항 및 해당 Android 버전과 가장 일치하는 각 장치 요구 사항에 대한 기능을 문서화합니다.
 4. 기능 요구 사항에 따라 최소 Android OS(7.0, 8.0, 9.0)를 결정합니다.
 5. ID 모델을 선택합니다.
 - 권장: 관리되는 Google Play 계정
 - Google Cloud Identity 고객인 경우에만 Google G-Suite 계정 사용
 6. 장치 전략 만들기:
 - 작업 없음: 장치가 최소 OS 수준을 충족하는 경우
 - 업그레이드: 장치가 지원되고 지원되는 OS로 업데이트할 수 있는 경우
 - 교체: 장치를 지원되는 OS 수준으로 업데이트할 수 없는 경우

권장되는 앱 마이그레이션 전략

요구 사항 매핑을 완료한 후 Android 플랫폼에서 Android Enterprise 플랫폼으로 앱을 이동합니다. 앱 게시에 대한 자세한 내용은 [앱 추가](#)를 참조하십시오.

- 공용 스토어 앱
 1. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 Google Play 설정을 지우고 **Android Enterprise**를 플랫폼으로 선택합니다.
 2. 배달 그룹을 선택합니다. 앱이 필수인 경우 앱을 배달 그룹의 필수 앱 목록으로 이동합니다.앱을 저장하면 Google Play Store에 나타납니다. 작업 프로필이 있는 경우 Google Play Store의 작업 프로필에 앱이 표시됩니다.
- 비공개 (엔터프라이즈) 앱

비공개 앱은 사내에서 개발하거나 타사 개발자가 개발합니다. Google Play를 사용하여 비공개 앱을 게시하는 것이 좋습니다.

 1. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 **Android Enterprise**를 플랫폼으로 선택합니다.
 2. APK 파일을 업로드한 다음 앱 설정을 구성합니다.
 3. 앱을 필수 배달 그룹에 게시합니다.
- MDX 앱
 1. 마이그레이션할 앱을 선택한 다음 앱을 편집하여 **Android Enterprise**를 플랫폼으로 선택합니다.
 2. MDX 파일을 업로드합니다. 앱 승인 프로세스를 진행합니다.

3. MDX 정책을선택합니다.

Enterprise MDX 앱의경우 MDX SDK 모드래핑된앱으로변경하는것이 좋습니다.

- 옵션 1: 조직에비공개로할당된개발자계정을사용하여 Google Play 에서 APK 를호스팅합니다. MDX 파일을 XenMobile 에게시합니다.
- 옵션 2: XenMobile 에서엔터프라이즈앱으로앱을게시합니다. XenMobile 에서 APK 를게시하고 MDX 파일에대해 **Android Enterprise** 플랫폼을선택합니다.

Citrix 장치정책마이그레이션

Android 및 Android Enterprise 플랫폼모두에사용할수있는정책의경우: 정책을편집하고 **Android Enterprise** 플랫폼을선택합니다.

Android Enterprise 의경우등록모드를고려하십시오. 일부정책옵션은작업프로필모드또는완전관리되는모드의장치에만사용할수있습니다.

개념증명

앱을 Android Enterprise 로마이그레이션한후마이그레이션테스트를설정하여기능이의도한대로작동하는지확인할수있습니다.

권장되는개념증명설정

1. 배포인프라설정:
 - Android Enterprise 테스트를위한배달그룹을만듭니다.
 - XenMobile 에서 Android Enterprise 를구성합니다.
2. 사용자앱을설정합니다.
3. Android Enterprise 기능을구성합니다.
4. Android Enterprise 배달그룹에정책을할당합니다.
5. 기능을테스트하고확인합니다.
6. 각사용사례에대해장치설정연습을완료합니다.
7. 사용자설정단계를문서화합니다.

배포

이제 Android Enterprise 설정을배포하고사용자마이그레이션을준비할수있습니다.

권장되는배포전략

Citrix 에서권장하는배포전략은 Android Enterprise 의모든프로덕션시스템을테스트한다음나중에장치마이그레이션을완료하는것입니다.

- 이시나리오에서사용자는현재구성으로계속해서러거시장치를사용합니다. 관리자는 Android Enterprise 관리를위한새장치를설정합니다.
- 기존장치는업그레이드또는교체가필요한경우에만마이그레이션합니다.
- 일반적인수명주기가끝나면기존장치를 Android Enterprise 관리로마이그레이션합니다. 또는손실이나파손으로인해교체가필요한경우이러한장치를마이그레이션할수있습니다.

Android Enterprise

January 6, 2020

Android Enterprise 는 Google 이 Android 장치를위한엔터프라이즈관리솔루션으로제공하는도구및서비스집합입니다. Android Enterprise 에서는 XenMobile 을사용하여회사소유의 Android 장치와 BYOD(bring your own device) Android 장치를관리합니다. 전체장치를관리하거나장치의개별프로필을관리할수있습니다. 개별프로필은개인계정, 앱및데이터로부터비즈니스계정, 앱및데이터를분리합니다. 또한인벤토리관리와같은일회성전용장치를관리할수도있습니다.

XenMobile 에대해지원되는 Android 운영체제는 [지원되는장치운영체제](#)를참조하십시오.

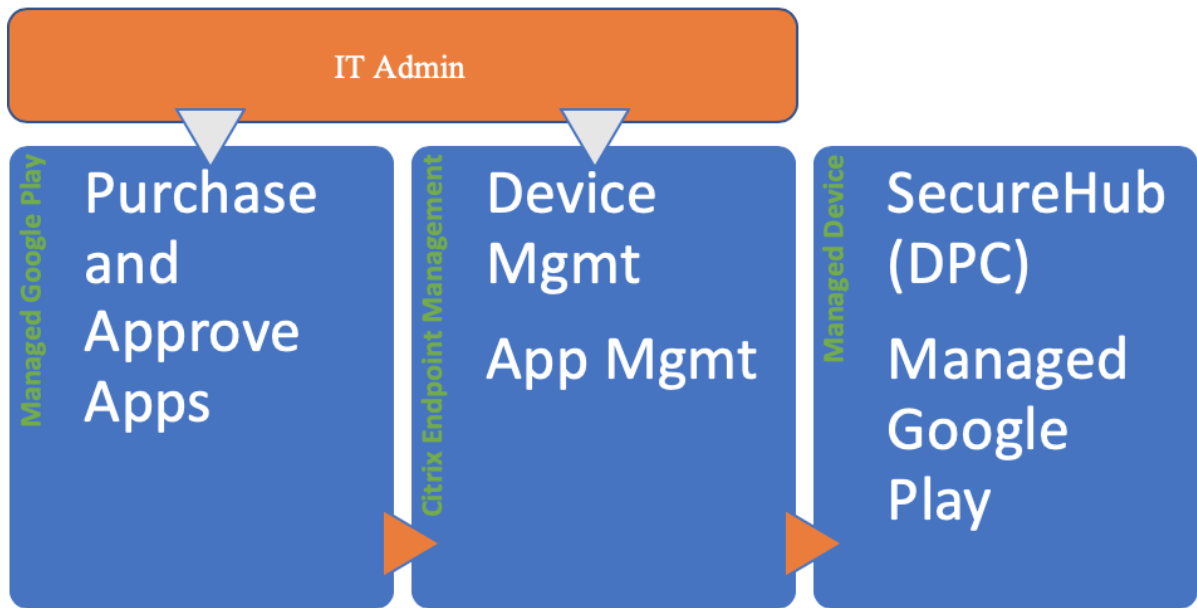
Android Enterprise 와관련된용어및정의목록은 Google Android Enterprise 개발자 가이드에서 [Android Enterprise 용어](#)를참조하십시오. Google 은이러한용어를자주업데이트합니다.

XenMobile 을관리되는 Google Play 와통합하여 Android Enterprise 를사용하는경우엔터프라이즈를만들게됩니다. Google 에서는엔터프라이즈조직과 EMM(엔터프라이즈모바일관리) 솔루션간의바인딩으로정의합니다. 조직에서솔루션을통해관리하는모든사용자및장치는해당엔터프라이즈에속합니다.

Android Enterprise 의엔터프라이즈에는 EMM 솔루션, DPC(장치정책컨트롤러) 앱및 Google 엔터프라이즈애플랫폼의세가지구성요소가있습니다. XenMobile 을 Android Enterprise 와통합하는경우전체솔루션에는다음과같은구성요소가포함됩니다.

- **XenMobile:** Citrix EMM 입니다. XenMobile 은안전한디지털작업공간을위한통합엔드포인트관리솔루션입니다. XenMobile 은 IT 관리자가조직의장치및앱을관리할수있는수단을제공합니다.
- **Citrix Secure Hub:** Citrix DPC 앱입니다. Secure Hub 는 XenMobile 의실행패드입니다. Secure Hub 는 장치에서정책을적용합니다.
- 관리되는 **Google Play:** XenMobile 과통합되는 Google 엔터프라이즈애플랫폼입니다. Google Play EMM API 는앱정책을설정하고앱을배포합니다.

다음그림은관리자가이러한구성요소와상호작용하는방식과구성요소가서로상호작용하는방식을보여줍니다.



XenMobile 에서관리되는 Google Play 사용

참고:

관리되는 Google Play 또는 G Suite 를 사용하여 Citrix 를 EMM 공급자로 등록할 수 있습니다. 이 문서에서는 관리되는 Google Play 와 함께 Android Enterprise 를 사용하는 방법에 대해 설명합니다. 조직에서 G Suite 를 사용하여 앱에 대한 액세스를 제공하는 경우 Android Enterprise 를 함께 사용할 수 있습니다. [G Suite 고객을 위한 레거시 Android Enterprise](#)에서 자세한 내용을 참조하십시오.

관리되는 Google Play 를 사용하는 경우 장치와 최종 사용자에게 관리형 Google Play 계정을 프로비전합니다. 관리되는 Google Play 계정을 통해 사용자가 관리되는 Google Play 에 액세스하여 제공되는 앱을 설치하고 사용할 수 있습니다. 조직에서 타사 ID 서비스를 사용하는 경우 관리형 Google Play 계정을 기존 ID 계정과 연결할 수 있습니다.

이 유형의 엔터프라이즈는 도메인에 연결되지 않으므로 단일 조직에 대해 둘 이상의 엔터프라이즈를 만들 수 있습니다. 예를 들어 조직 내의 각 부서 또는 리전을 서로 다른 엔터프라이즈로 등록하여 별도의 장치 및 앱 집합을 관리할 수 있습니다.

관리되는 Google Play 는 XenMobile 관리자에게 Google Play 의 사용자 환경 및 앱 스토어 기능과 함께 기업을 위해 설계된 관리 기능을 제공합니다. 관리형 Google Play 를 사용하여 장치의 Android Enterprise 작업 공간에 배포할 앱을 추가, 구매 및 승인합니다. Google Play 를 사용하여 공용 앱, 개인 앱 및 타사 앱을 배포할 수 있습니다.

관리되는 장치의 사용자에게 있어서 관리되는 Google Play 는 엔터프라이즈 앱 스토어입니다. 사용자는 앱을 탐색하고, 앱 세부 정보를 보고, 앱을 설치할 수 있습니다. 공개 버전의 Google Play 와 달리 관리형 Google Play 에서는 사용자에게 별도로 제공되는 앱만 설치할 수 있습니다.

장치배포시나리오및작동모드

장치배포시나리오는배포한장치의소유자와장치의관리방법을나타냅니다. 작동모드는 DPC 가장치에서정책을관리하고적용하는 방법을나타냅니다. 작동모드는장치배포시나리오를지원합니다.

작업프로필: BYOD 장치배포, 프로필소유자모드

BYOD 배포시나리오에서는직원이개인소유의장치를회사에가져오고해당장치를사용하여회사정보및응용프로그램에액세스할수 있습니다.

프로필소유자작동모드는 BYOD 배포를지원합니다. 기업은 DPC 를통해작업프로필을장치의기본사용자계정에추가하여개인장치의업무용사용을지원할수있습니다. 작업프로필은개인계정, 앱및데이터로부터비즈니스계정, 앱및데이터를분리합니다. 작업프로필은별도의프로필로기본사용자와연결됩니다. DPC 는프로필소유자로서장치의작업프로필만관리하고작업프로필외부에서는제한된제어권한을갖습니다. 작업프로필에대한자세한내용은 Google Android Enterprise 도움말함목 [작업프로필이란무엇인가요?](#)를참조하십시오.

프로필소유자모드는장치가 XenMobile 에서등록된경우사용됩니다. DPC 는전체장치가아닌작업프로필만관리하므로프로필소유자모드에서등록된장치가새장치이거나공장기본값으로재설정된장치일필요는없습니다.

프로필소유자모드의장치를작업프로필장치라고도합니다. 프로필소유자모드를작업프로필모드또는관리되는프로필모드라고도합니다.

참고:

XenMobile 은프로필소유자모드에서와같이 Zebra 장치를지원하지않습니다. XenMobile 은 Zebra 장치를완전관리되는장치및장치레거시모드 (장치관리모드라고도함) 로지원합니다.

완전관리형: 회사소유장치배포, 장치소유자모드

회사소유배포시나리오에서는기업이장치의사용을완벽하게제어합니다. 일반적으로조직은전체장치를엄격하게모니터링하고관리해야할때회사소유장치를배포합니다.

장치소유자작동모드는회사소유배포를지원합니다. 장치소유자모드에서 DPC 는전체장치를관리합니다. DPC 는장치소유자로서장치전체연결구성, 글로벌설정구성및공장기본값으로재설정과같은장치전체작업을수행할수있습니다.

장치소유자모드의장치는완전관리되는장치입니다.

장치소유자모드는초기장치설정중에사용되도록설정됩니다. 장치소유자모드에서는새장치또는공장기본값으로재설정된장치만 XenMobile 에등록할수있습니다.

전용장치: 회사소유장치배포, 장치소유자모드

전용장치는완전관리되는장치유형입니다. 전용장치는장치소유자모드에서실행되는회사소유장치입니다. 전용장치는디지털서명, 티켓인쇄또는인벤토리관리와같은전용용으로사용되는제한된앱집합을제공합니다. 전용장치를프로비전하는경우필수앱만제공하고사용자가다른앱을추가하지못하도록합니다.

전용장치를 COSU(회사소유일회사용) 장치또는키오스크모드장치라고도합니다.

레거시장치배포, 레거시모드

레거시배포시나리오는 5.0 이전의 Android 버전을실행하는장치를위한시나리오입니다. 5.0 이전의 Android 버전은장치소유자모드또는프로필소유자모드를지원하지않습니다. Android 버전 5.1 은장치소유자모드를지원하지만프로필소유자모드는지원하지않습니다.

장치관리모드라고도하는 레거시작동모드는레거시장치배포를지원합니다. 레거시모드에서는 DPC 가장치를제한적으로제어할 수있습니다. DPC 는장치를초기화하고, 암호를요구하거나, 일부정책을적용할 수있습니다. 레거시장치에서앱관리를제공하려면 Google Play 를사용하고사용자가 Google 계정을추가하도록허용합니다. DPC 를통해레거시장치에관리되는 Google Play 계정을추가할 수도있습니다.

장치소유자모드또는프로필소유자모드를구현할수있는배포의경우레거시모드를사용하지않는것이 좋습니다. Google 은대규모 환경전체에서공통점이가장없는솔루션을사용하는대신가장높은수준의장치관리를사용할것을권장합니다. 레거시모드에서장치소유자모드또는프로필소유자모드로마이그레이션하는방법에대한자세한내용은 [장치관리에서 Android Enterprise 로마이그레이션을참조하십시오.](#)

참고:

Citrix 에서는 레거시라는 용어를 관리되는 Google play 대신 XenMobile 및 G Suite 를 관리되는 Android Enterprise 장치에 사용하는 고객을 나타낼 때에도 사용합니다.

인증방법

XenMobile 은 Android 장치를 MDM+MAM 또는 MDM 모드로 등록합니다. 사용자에게는 MAM 전용모드로 등록할 수 있는 옵션이 제공됩니다. XenMobile 은 MDM+MAM 모드에서 Android 장치에 대해 다음과 같은 인증방법을 지원합니다. 자세한 내용은 [인증서 및 인증](#) 의 문서를 참조하십시오.

- 도메인
- 도메인 및 보안토큰
- 클라이언트 인증서
- 클라이언트 인증서와 도메인
- ID 공급자:
 - Azure Active Directory
 - Citrix ID 공급자

거의 사용되지 않는 또 다른 인증 방법은 클라이언트 인증서와 보안토큰입니다. 자세한 내용은 <https://support.citrix.com/article/CTX215200> 에서 참조하십시오.

요구사항

Android Enterprise 사용을 시작하기 전에 다음이 필요합니다.

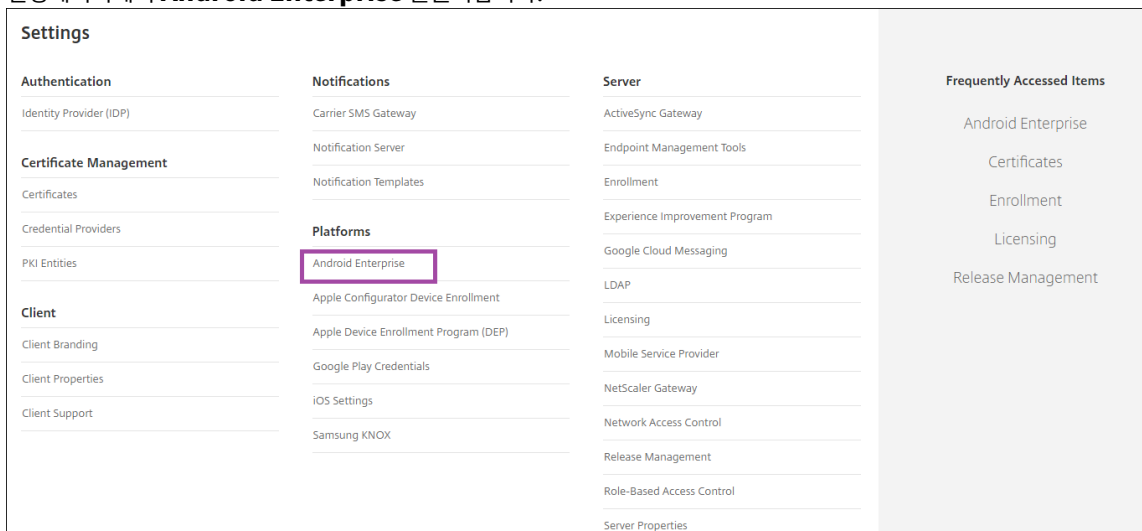
- 계정및자격증명:
 - 관리되는 Google Play 로 Android Enterprise 를설정하려면회사의 Google 계정
 - 최신 MDX 파일을다운로드하려면 Citrix 고객계정
 - 비공개앱을배포하려면 (선택사항) Google 개발자계정
- Samsung Knox 모바일등록 (선택사항) 의경우 Knox 프리미엄라이센스

Google Play 에 XenMobile 연결

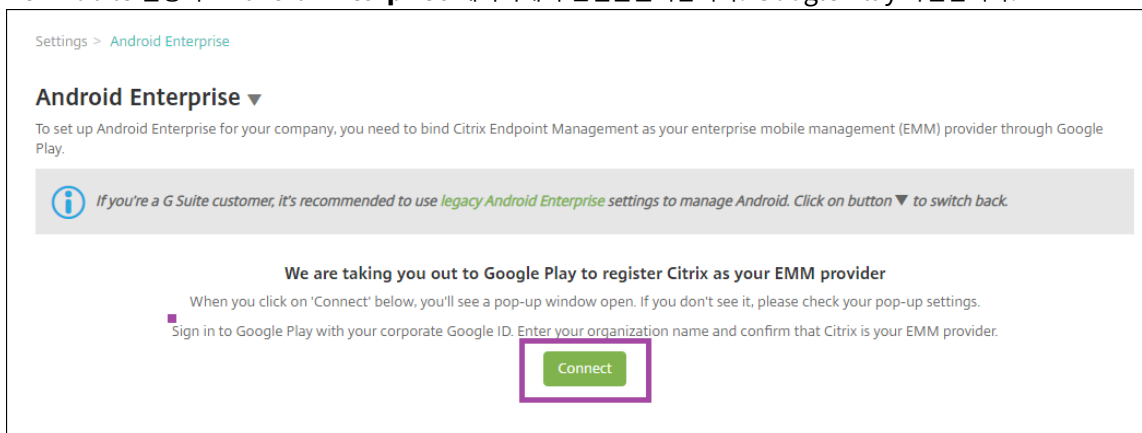
조직에대한 Android Enterprise 를설정하려면관리되는 Google Play 를통해 Citrix 를 EMM 공급자로등록합니다. 이설정은관리되는 Google Play 를 XenMobile 에연결하고 XenMobile 에 Android Enterprise 의엔터프라이즈를만듭니다.

Google Play 에로그인하려면회사 Google 계정이필요합니다.

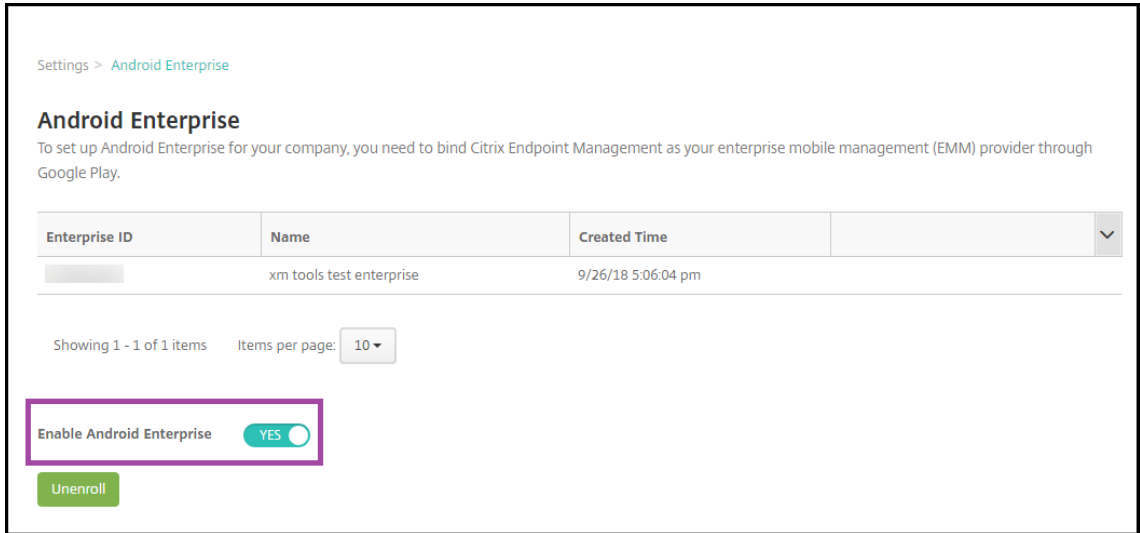
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 설정페이지에서 **Android Enterprise** 를클릭합니다.



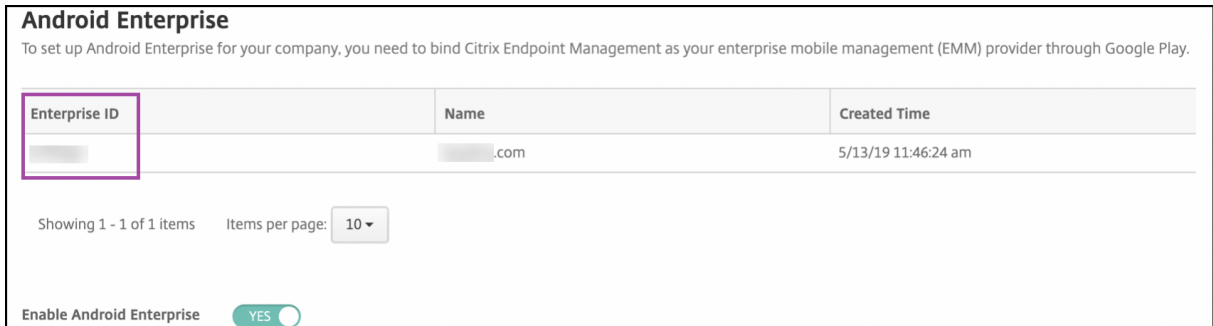
3. XenMobile 설정의 **Android Enterprise** 페이지에서 연결을클릭합니다. Google Play 가열립니다.



4. 회사 Google 계정자격증명을 사용하여 Google Play 에 로그인합니다. 조직이름을 입력하고 Citrix 가 EMM 공급자인지 확인합니다.
5. Android Enterprise 에 대한 엔터프라이즈 ID 가 추가되었습니다. Android Enterprise 를 사용하려면 **Android Enterprise** 사용을 예로합니다.



엔터프라이즈 ID 가 XenMobile 콘솔에 나타납니다.



환경이 Google 에 연결되었고 장치 관리할 준비가 되었습니다. 이제 사용자를 위한 앱을 제공할 수 있습니다.

XenMobile 을 사용하여 사용자에게 Citrix 모바일 생산성 앱, MDX 앱, 공용 앱 스토어 앱, 웹 및 SaaS 앱, 엔터프라이즈 앱 및 웹 링크를 제공할 수 있습니다. 이러한 유형의 앱 및 사용자에게 제공하는 방법에 대한 자세한 내용은 [앱 추가](#) 를 참조하십시오.

다음 섹션에서는 모바일 생산성 앱을 제공하는 방법을 보여줍니다.

Android Enterprise 사용자에게 Citrix 모바일 생산성 앱 제공

Android Enterprise 사용자에게 Citrix 모바일 생산성 앱을 제공하려면 다음 단계가 필요합니다.

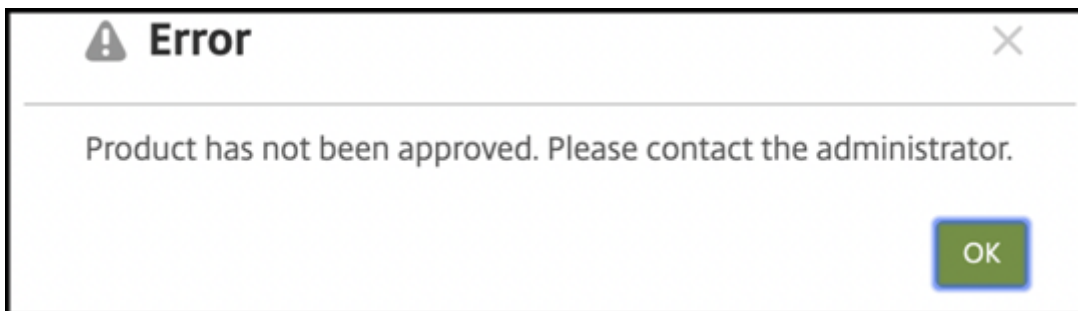
1. 관리되는 Google Play Store 에서 사용자에게 제공할 앱을 승인합니다. 관리되는 Google Play 에서 앱 승인에서 자세한 내용을 참조하십시오.
2. XenMobile 콘솔에서 앱을 공용 앱 스토어 앱으로 게시합니다. 앱을 공용 앱 스토어 앱으로 구성을 참조하십시오.

3. XenMobile 콘솔에서 동일한 앱을 MDX 앱으로 다시 게시하여 앱이 MDX 정책을 수신할 수 있도록 합니다. 앱을 MDX 앱으로 구성에서 자세한 내용을 참조하십시오.
4. XenMobile 콘솔에서 사용자가 장치의 작업 프로필에 액세스할 때 사용할 보안 챌린지에 대한 규칙을 구성합니다. 보안 챌린지 정책 구성에서 자세한 내용을 참조하십시오.

게시한 앱은 Android Enterprise 엔터프라이즈에 등록된 장치에 제공됩니다.

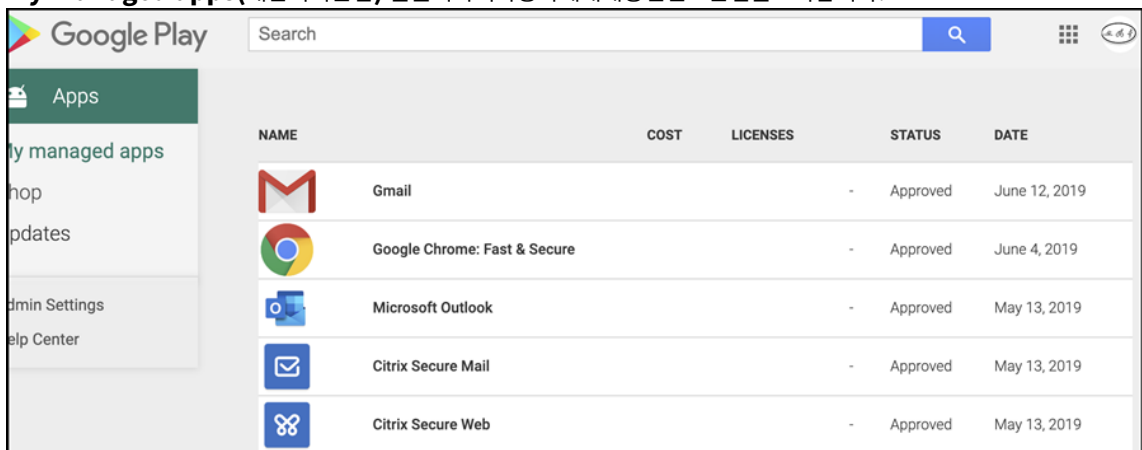
관리되는 **Google Play** 에서 앱 승인

XenMobile 에 앱을 추가하려면 먼저 관리되는 Google Play Store 에서 앱을 승인합니다. 관리되는 Google Play Store 에서 앱을 승인하지 않은 경우 앱을 추가하려고 할 때 XenMobile 콘솔에서 다음 오류가 발생합니다.



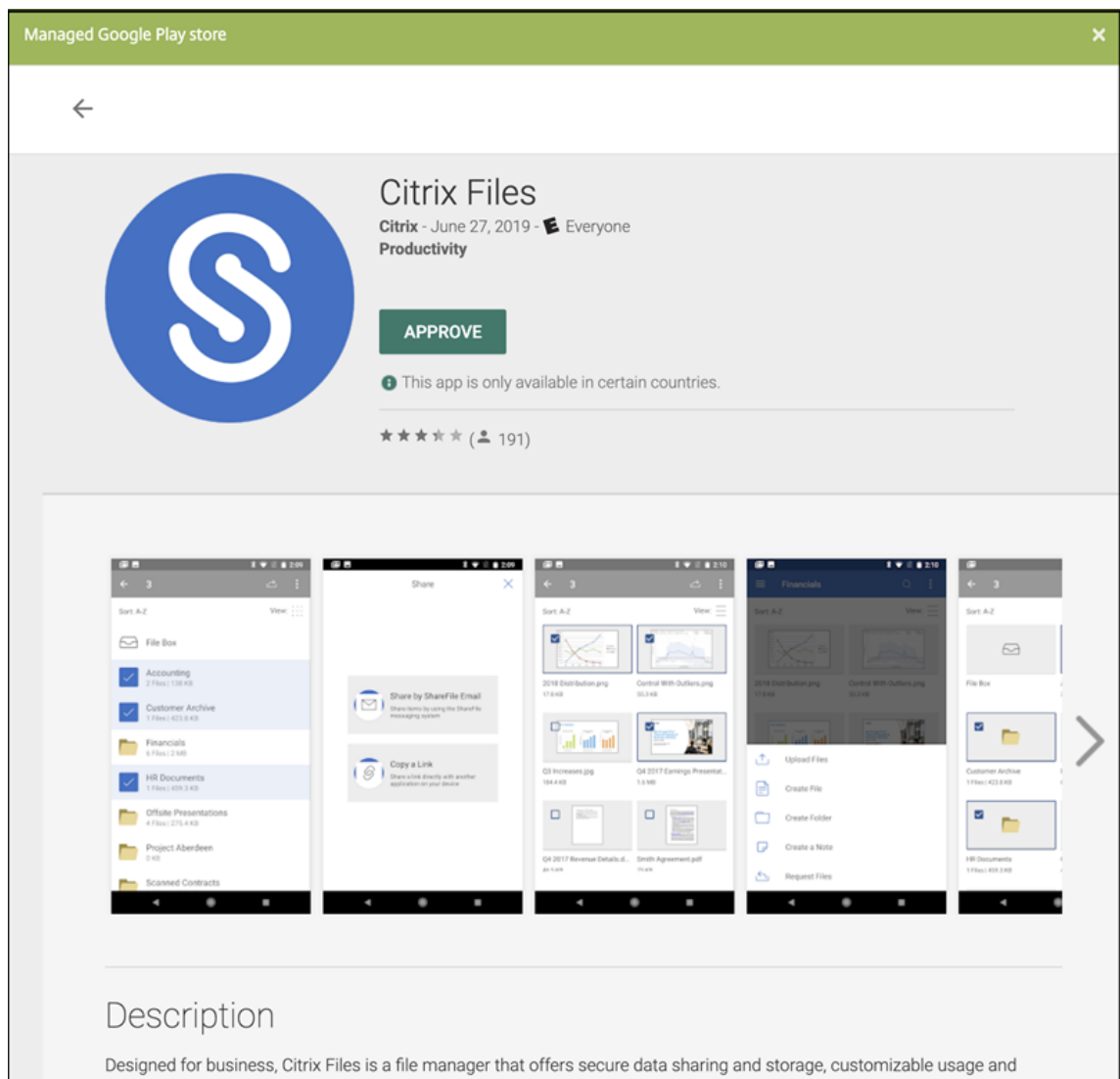
관리되는 Google Play Store 로 이동하여 기업에서 이미 사용할 수 있는 앱과 사용이 승인된 앱을 확인합니다.

1. Google 계정 자격 증명을 사용하여 <https://play.google.com/work> 에 로그인합니다.
2. **My managed apps**(내 관리되는 앱) 을 클릭하여 사용자에 대해 승인된 모든 앱을 표시합니다.

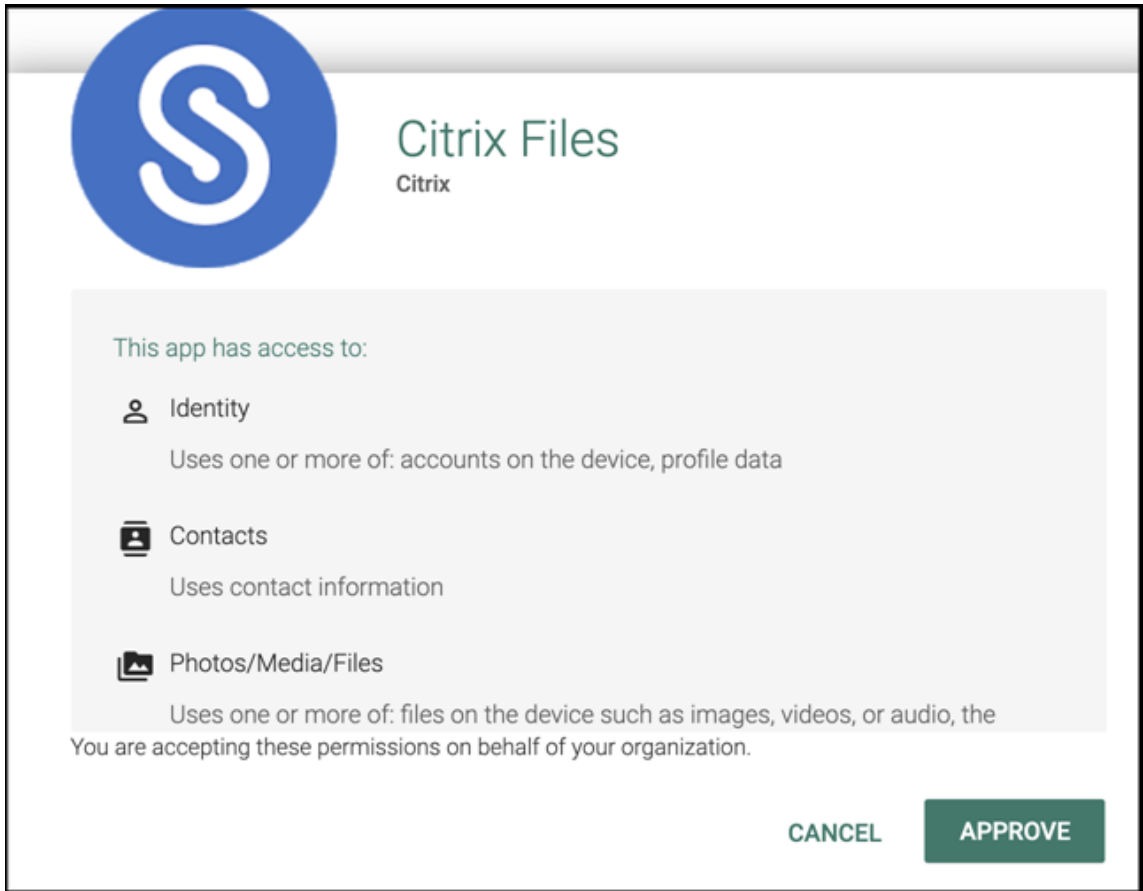


관리되는 Google Play Store 에서 앱을 승인하려면:

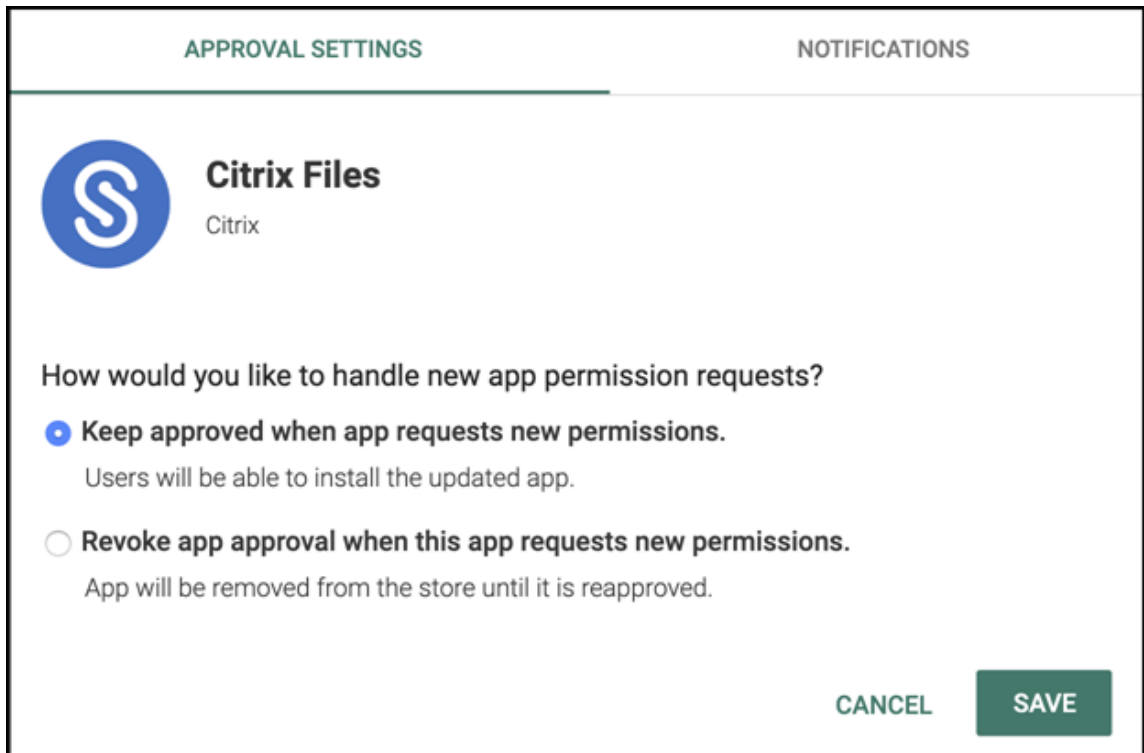
1. 관리되는 Google Play 에 로그인한 상태에서 승인하려는 앱을 선택합니다. 앱 페이지에 **Approve**(승인) 단추가 나타납니다.



2. **Approve(승인)** 를 클릭합니다.



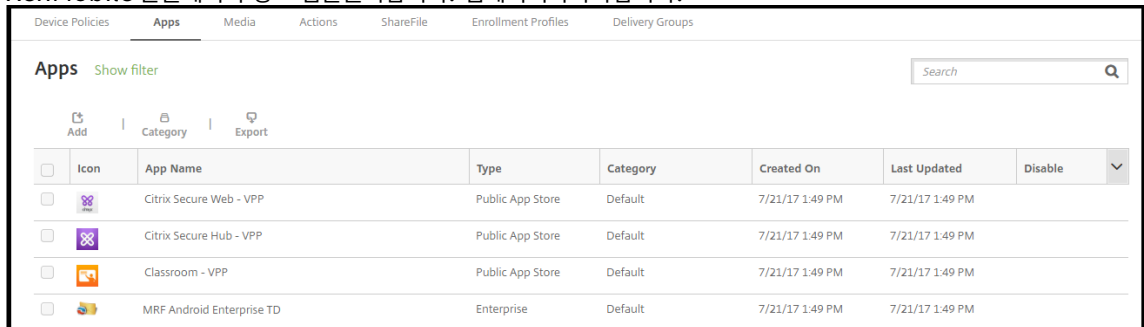
3. **Approve**(승인) 를 다시클릭합니다.
4. **Keep approved when app requests new permissions**(앱이새권한을요청할때승인된상태로유지) 를선택합니다. 저장을클릭합니다.



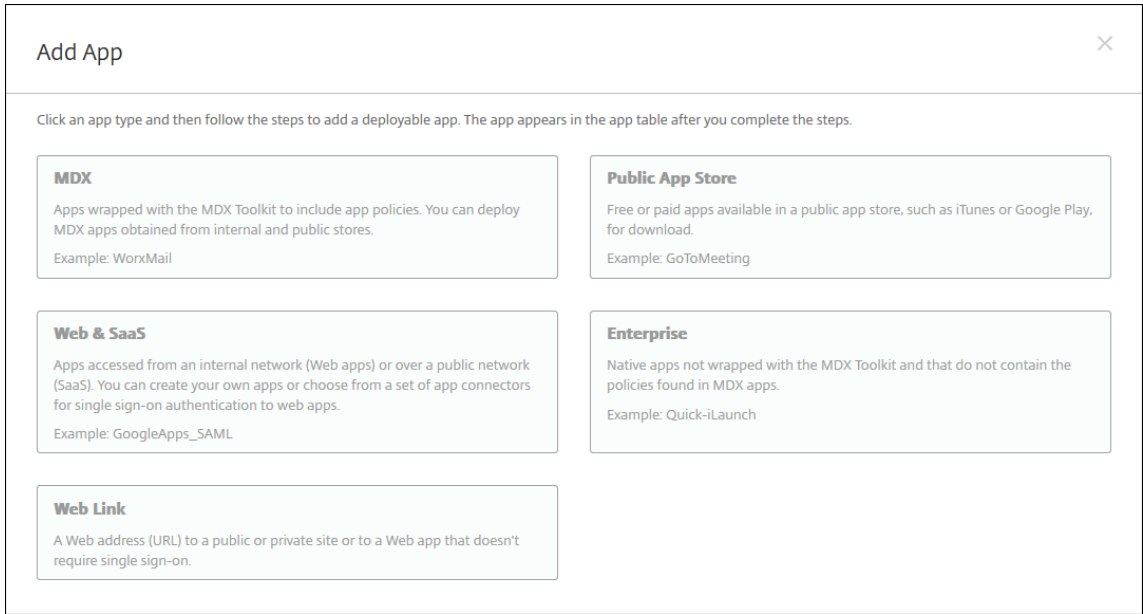
앱을공용앱스토어앱으로구성

Citrix ShareFile 을 Android Enterprise 공용앱스토어앱으로구성하려면:

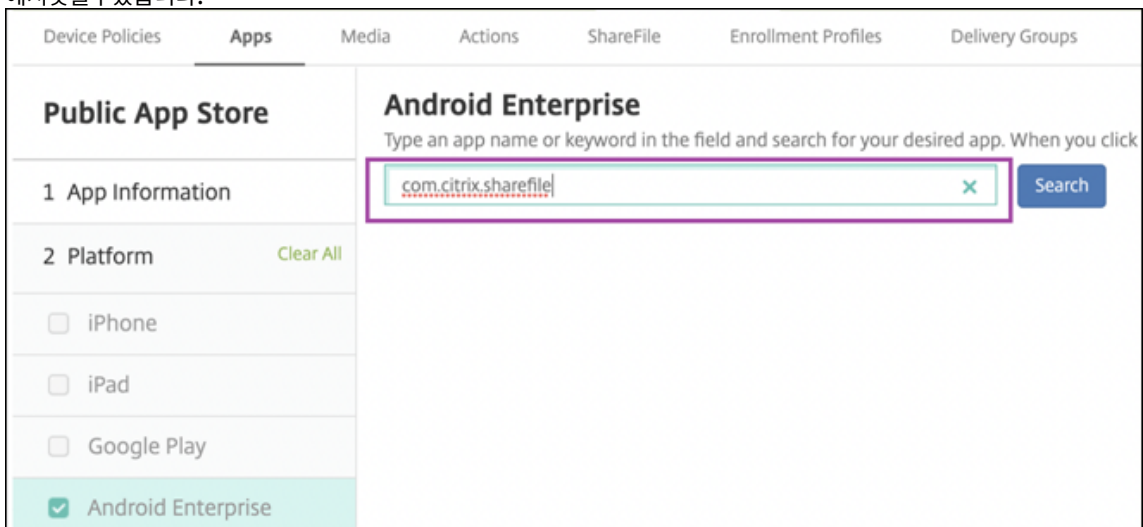
1. XenMobile 콘솔에서 구성 > 앱을클릭합니다. 앱페이지가나타납니다.



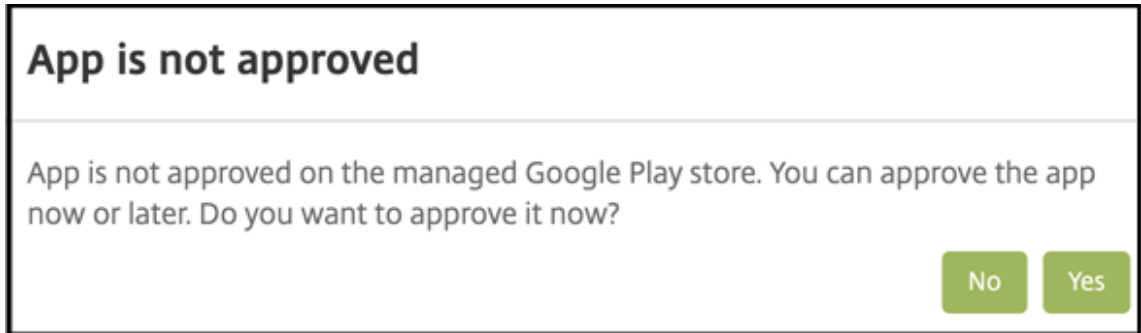
2. 추가를클릭합니다. 앱추가대화상자가나타납니다.



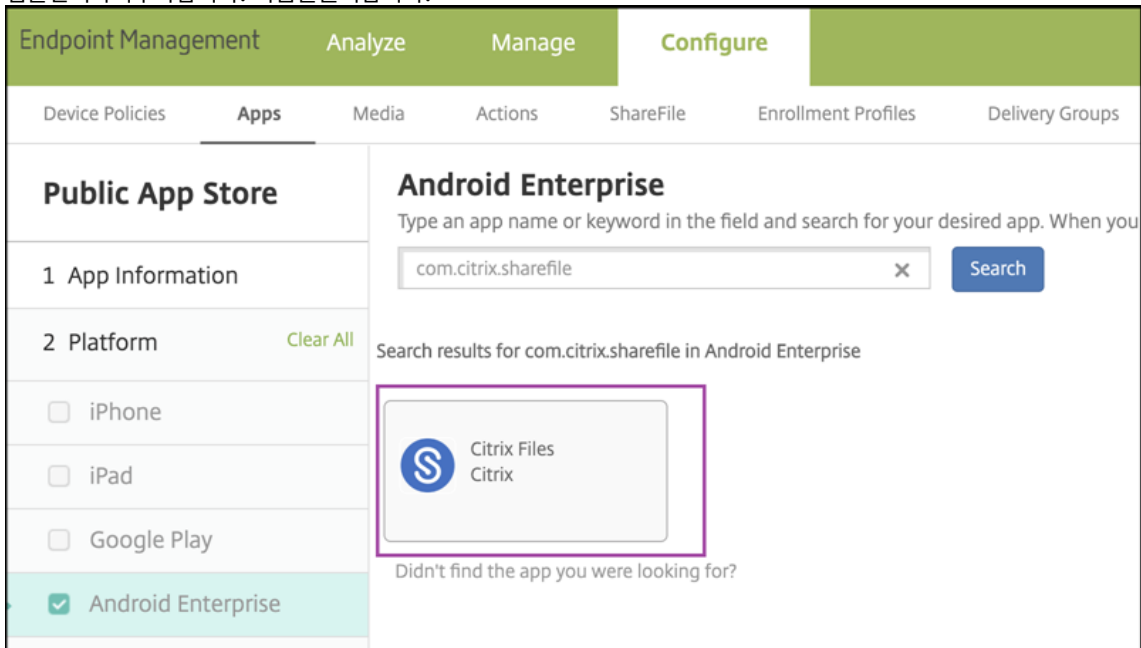
3. 공용앱스토어를 클릭합니다. 앱정보페이지가 나타납니다.
4. 앱정보페이지에서 다음 정보를 입력합니다.
 - 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱테이블의 앱 이름 아래에 표시됩니다.
 - 설명: 앱의 선택적 설명을 입력합니다.
 - 앱범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 [앱 범주 만들기](#)를 참조하십시오.
5. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.
6. 플랫폼에서 **Android Enterprise** 를 선택합니다. 다른 플랫폼을 지웁니다.
7. **Android Enterprise** 에서 앱의 번들 ID 를 입력하고 검색을 클릭합니다. 앱 식별자는 Google Play Store 의 앱 URL 에서 찾을 수 있습니다.



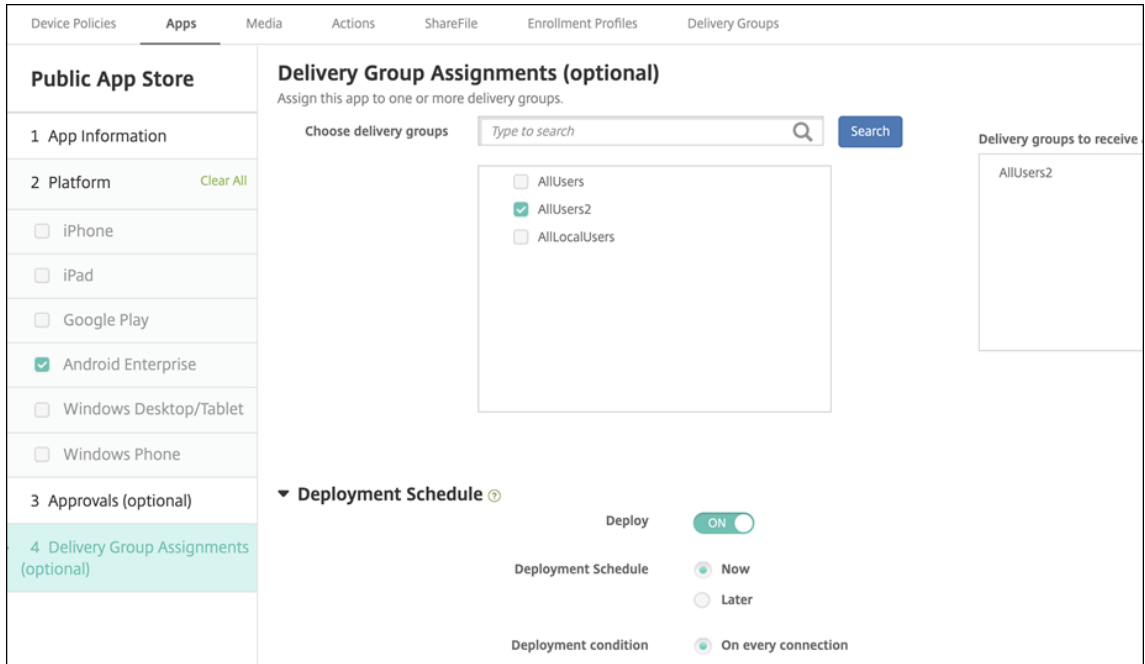
8. Google Play Store 에서 앱이 승인되지 않은 것으로 콘솔에 표시되면 예를 클릭하여 지금 승인합니다.



9. 앱을 선택하여 추가합니다. 다음을 클릭합니다.



10. 이 앱을 하나 이상의 배달 그룹에 할당합니다.



11. 저장을 클릭합니다.

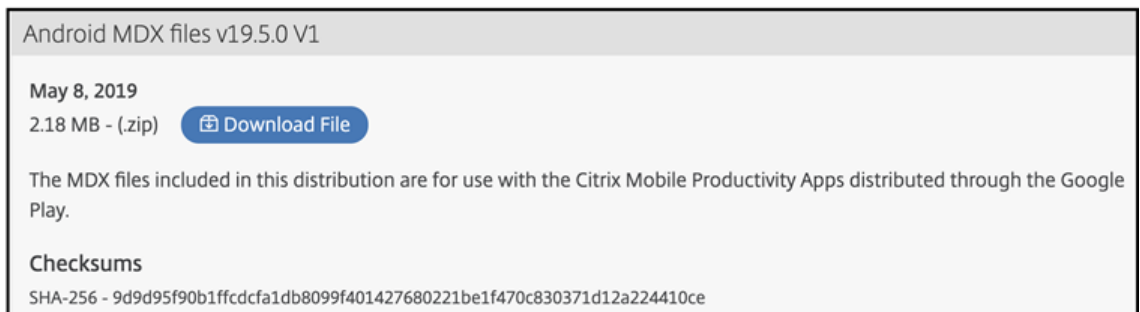
Citrix Secure Mail 및 Citrix Secure Web 에 대해 이러한 단계를 반복합니다.

앱을 MDX 앱으로 구성

모바일 생산성 앱에는 기본 Android 매니페스트가 사용되지 않습니다. 사용자에게 앱을 배포하기 전에 이러한 앱을 MDX 앱으로 추가하고 MDX 정책을 구성해야 합니다.

MDX 앱을 추가하기 전에 최신 Android MDX 파일을 다운로드하십시오.

1. XenMobile 다운로드 페이지로 이동하여 Citrix 고객 자격 증명으로 로그인합니다. <https://www.citrix.com/downloads/citrix-endpoint-management/product-software/xenmobile-enterprise-edition-worx-apps-and-mdx-toolkit.html>.



2. 다운로드한 파일의 압축을 풀고 콘텐츠를 추출합니다.

MDX 앱을 추가하고 구성하려면:

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱페이지가 나타납니다.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
<input type="checkbox"/>		Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
<input type="checkbox"/>		Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	

2. 추가를 클릭합니다. 앱추가대화상자가 나타납니다.

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

- MDX**
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail
- Public App Store**
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting
- Web & SaaS**
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML
- Enterprise**
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch
- Web Link**
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. MDX 를 클릭합니다. MDX 앱정보페이지가 나타납니다.

4. 응용프로그램의 이름을 지정하고 다음을 클릭합니다.

MDX

- 1 App Information
- 2 Platform
- iOS
- Android
- Windows Phone

App Information

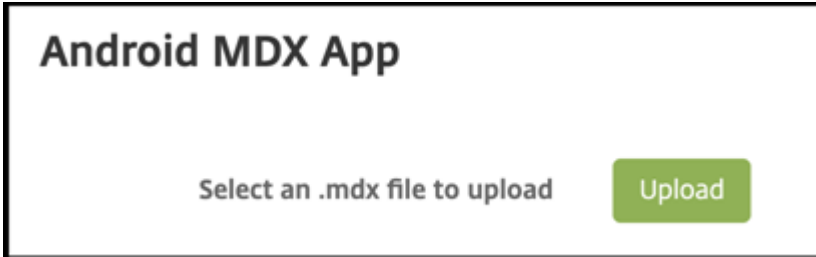
Name * ?

Description ?

App category

5. 다음을 클릭하여 Android 플랫폼 구성으로 이동합니다.

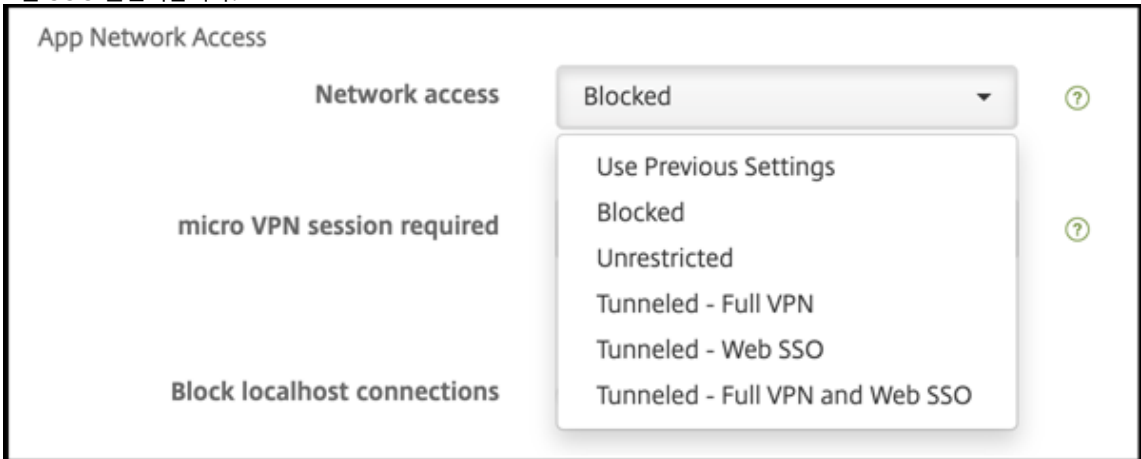
6. 업로드를 클릭합니다.



7. MDX 파일 위치로 이동하고 설치할 MDX 파일을 선택합니다.

Android_19.5.0_PlayStoreMDX_V1	May 13, 2019 at 10:39 AM	--	Folder
securemail-playstore-19.5.0.mdx	May 2, 2019 at 1:08 PM	306 KB	Micros...DX File
secureweb-playstore-19.5.0.mdx	May 2, 2019 at 1:07 PM	304 KB	Micros...DX File
QuickEdit_for_XenMobile_7.6.2_19.3.5.mdx	Apr 23, 2019 at 3:53 PM	303 KB	Micros...DX File
CitrixFiles_for_XenMobile_7.6.2_19.3.5.mdx	Apr 23, 2019 at 3:53 PM	329 KB	Micros...DX File
ShareFile_Workflows-playstore-1.10.1.5.mdx	Oct 30, 2018 at 4:51 PM	284 KB	Micros...DX File
SecureNotes-Playstore-10.8.5.2.mdx	Mar 22, 2018 at 1:08 PM	295 KB	Micros...DX File
SecureTasks-Playstore-10.8.5.2.mdx	Mar 22, 2018 at 1:08 PM	324 KB	Micros...DX File
ShareConnect_PlayStore_3.5.1863.mdx	Oct 12, 2017 at 11:27 PM	255 KB	Micros...DX File

8. 일부 앱의 네트워크 액세스는 기본적으로 차단됩니다. 네트워크 액세스를 사용하도록 설정합니다. 메뉴를 클릭하고 터널링됨 - 웹 SSO 를 선택합니다.



9. 배달 그룹 할당 페이지에도 달할 때까지 기본값을 제외 한 페이지에서 다음을 클릭합니다.

10. 앱을 공용 앱 스토어 앱으로 게시할 때 할당 한 것과 동일한 배달 그룹에 앱을 할당합니다.

11. 저장을 클릭합니다.

단계를 반복하여 각 모바일 생산성 앱에 대해 MDX 앱을 구성합니다.

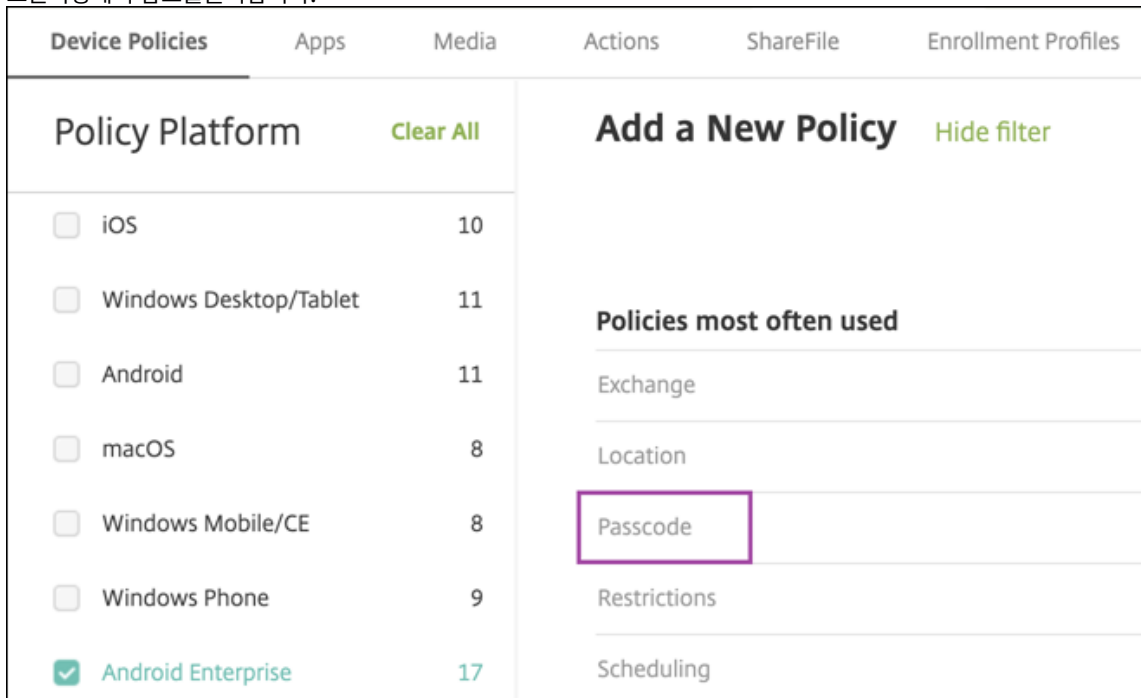
보안 챌린지 정책 구성

XenMobile 암호 장치 정책은 사용자가 자신의 장치 또는 장치의 Android Enterprise 작업 프로필에 액세스하도록 하는 보안 챌린지 정책에 대한 규칙 집합을 구성합니다. 보안 챌린지는 암호 또는 생체 인식일 수 있습니다. 암호 정책에 대한 자세한 내용은 [암호 장치 정책](#) 을 참조하십시오.

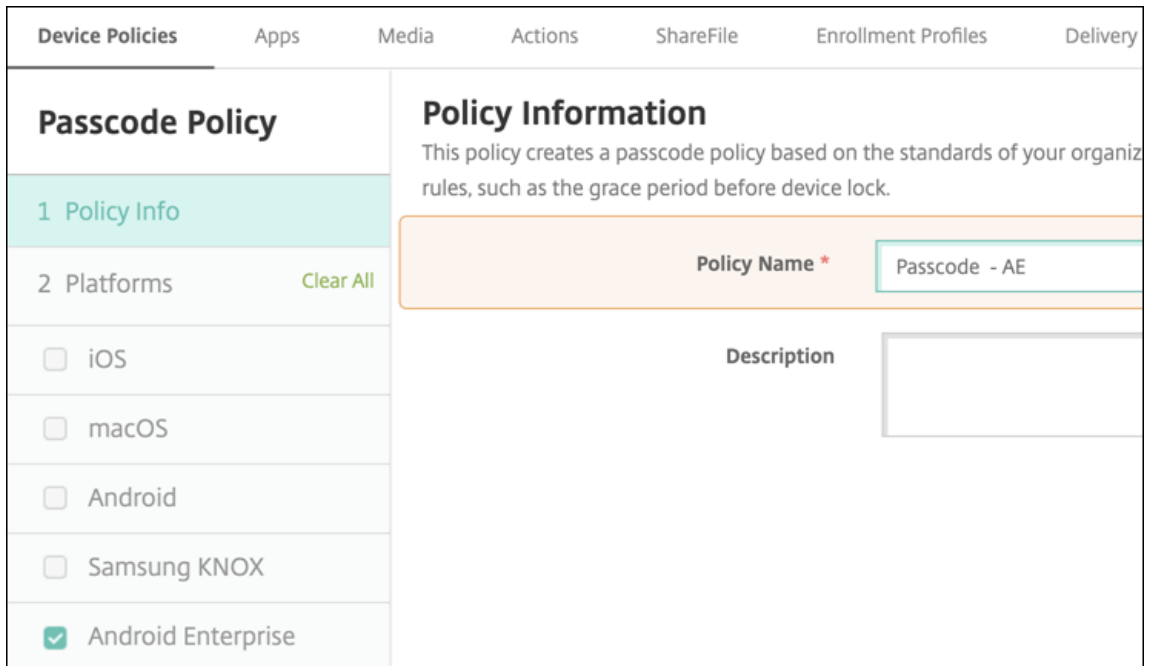
Android Enterprise 배포에 BYOD 장치가 포함되는 경우 작업 프로필에 대한 암호 정책을 구성합니다. 배포에 회사 소유의 완전 관리되는 장치가 포함되는 경우 장치 자체에 대한 암호 정책을 구성합니다. 배포에 두 가지 유형의 장치가 모두 포함되는 경우 두 유형의 암호 정책을 모두 구성합니다.

암호 정책을 구성하려면:

1. XenMobile 콘솔에서 구성 > 장치 정책으로 이동합니다.
2. 추가를 클릭합니다.
3. 필터 표시를 클릭하여 정책 플랫폼 창을 표시합니다. 정책 플랫폼 창에서 **Android Enterprise** 를 선택합니다.
4. 오른쪽 창에서 암호를 클릭합니다.



5. 정책 이름을 입력합니다. 다음을 클릭합니다.



6. 암호정책설정을구성합니다.
 - 장치자체의보안챌린지에사용할수있는설정을보려면 장치암호필요를 켜짐으로설정합니다.
 - 작업프로필보안챌린지에사용할수있는설정을보려면 작업프로필보안챌린지를 켜짐으로설정합니다.
7. 다음을클릭합니다.
8. 정책을하나이상의배달그룹에할당합니다.
9. 저장을클릭합니다.

Android Enterprise 작업프로필장치프로비전

Android Enterprise 작업프로필장치는프로필소유자모드에서등록됩니다. 이러한장치는새장치가거나출고기본값이설정된장치일필요가없습니다. BYOD 장치는작업프로필장치로등록됩니다. 등록환경은 XenMobile 의 Android 등록과비슷합니다. 사용자가 Google Play 에서 Secure Hub 를다운로드하고장치를등록합니다.

Android Enterprise 에서작업프로필장치로장치를등록하는경우 USB 디버깅및알수없는소스설정은기본적으로사용되지않도록설정됩니다.

Android Enterprise 에서작업프로필장치로장치를등록하는경우항상 Google Play 로이동하십시오. 거기서사용자의개인프로필에 Secure Hub 가표시되도록설정합니다.

Android Enterprise 완전관리되는장치프로비전

이전섹션에서설정해포에서완전관리되는장치를등록할수있습니다. 완전관리되는장치는회사소유의장치이며장치소유자모드에서등록됩니다. 장치소유자모드에서는새장치또는공장기본값으로재설정된장치만등록할수있습니다.

다음등록방법중하나를사용하여장치소유자모드에서장치를등록할수있습니다.

- **DPC** 식별자토큰이등록방법에서는사용자가장치를설정할때 `afw##xenmobile` 문자를입력합니다. `afw##xenmobile`은 Citrix DPC 식별자토큰입니다. 이토큰은 XenMobile 이관리하는장치로장치를식별하고 Google Play Store 에서 Secure Hub 를다운로드합니다. Citrix DPC 식별자토큰을사용하여장치등록에서자세한내용을참조하십시오.
- **NFC**(근거리통신) 범프: NFC 범프등록방법은근거리통신을사용하여두장치간데이터를전송합니다. 새장치또는공장기본값으로재설정된장치에서는 Bluetooth, Wi-Fi 및기타통신모드를사용할수없습니다. NFC 는이상태에서장치가사용할수있는유일한통신프로토콜입니다. NFC 범프를사용하여장치등록에서자세한내용을참조하십시오.
- **QR 코드**: QR 코드등록은태블릿과같이 NFC 를지원하지않는분산된제품군의장치를등록할때사용될수있습니다. QR 코드등록방법은설치마법사에서 QR 코드를스캔하여장치프로필모드를설정하고구성합니다. QR 코드를사용하여장치등록에서자세한내용을참조하십시오.
- **제로터치**: 제로터치등록을사용하면장치전원을처음켄때자동으로등록하도록장치를구성할수있습니다. 제로터치등록은 Android 8.0 이상을실행하는일부 Android 장치에서지원됩니다. 제로터치등록에서자세한내용을참조하십시오.
- **Google 계정**: 사용자가 Google 계정자격증명을입력하여프로비저닝프로세스를시작합니다. 이옵션은 G Suite 를사용하는엔터프라이즈용입니다.

Citrix DPC 식별자토큰을사용하여장치등록

새장치또는공장기본값으로재설정된장치의초기설정을위해전원을켄후 Google 계정을입력하라는메시지가표시되면 “afw#xenmobile” 을입력합니다. 이동작을수행하면 Secure Hub 가다운로드되고설치됩니다. 그런다음사용자는 Secure Hub 설정메시지에따라등록을완료합니다.

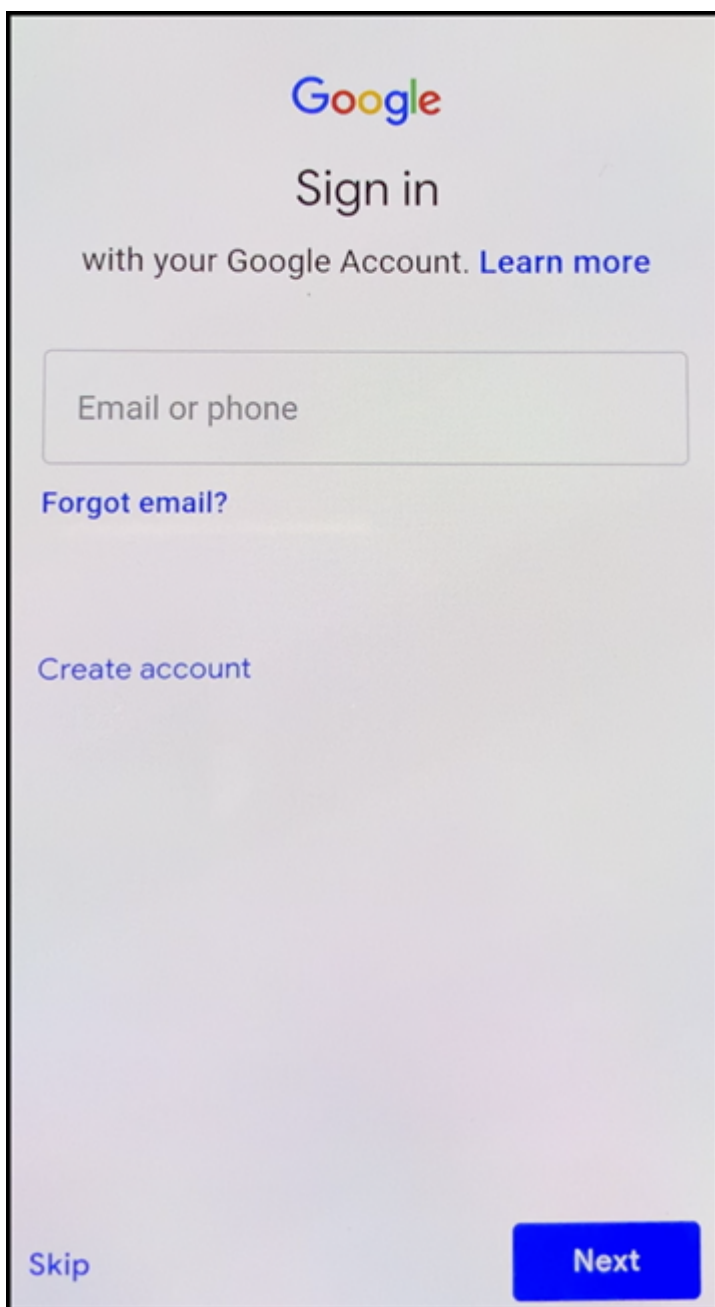
최신버전의 Secure Hub 가 Google Play Store 에서다운로드되므로이등록방법이대부분의고객에게권장됩니다. 다른등록방법과달리, XenMobile 서버에서다운로드하기위해 Secure Hub 를제공하지않습니다.

시스템요구사항

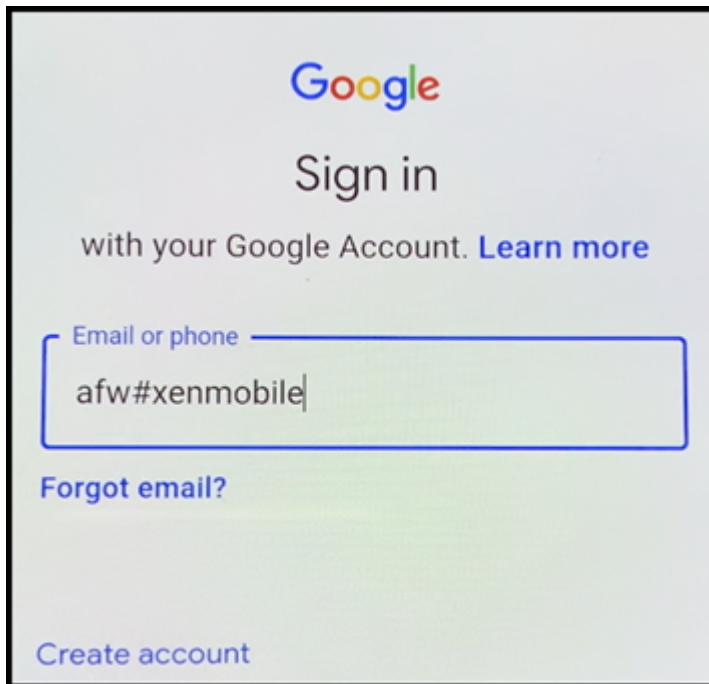
- Android OS 를실행하는모든 Android 장치에서지원됩니다.

장치를등록하려면

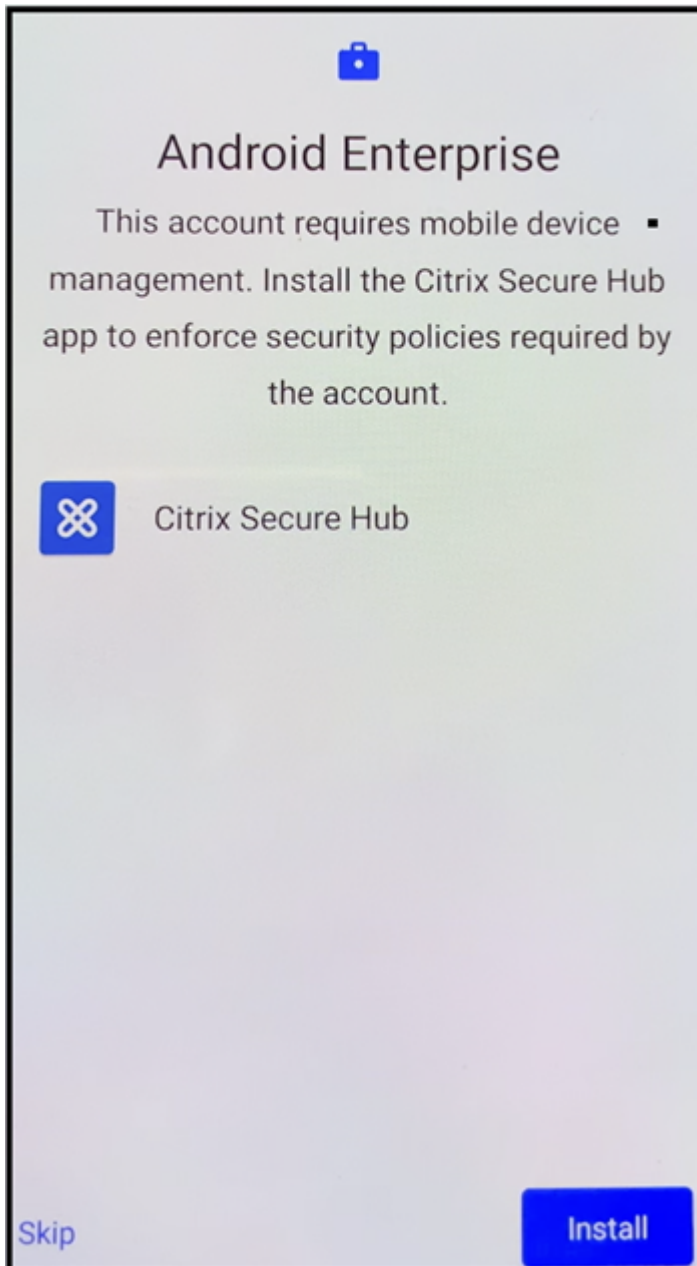
1. 새장치또는공장기본값으로재설정된장치의전원을켂니다.
2. 초기장치설정이로드되고 Google 계정을입력하라는메시지가표시됩니다. 장치에장치의홈화면이로드되는경우알림표시줄에서 설정완료알림을확인합니다.



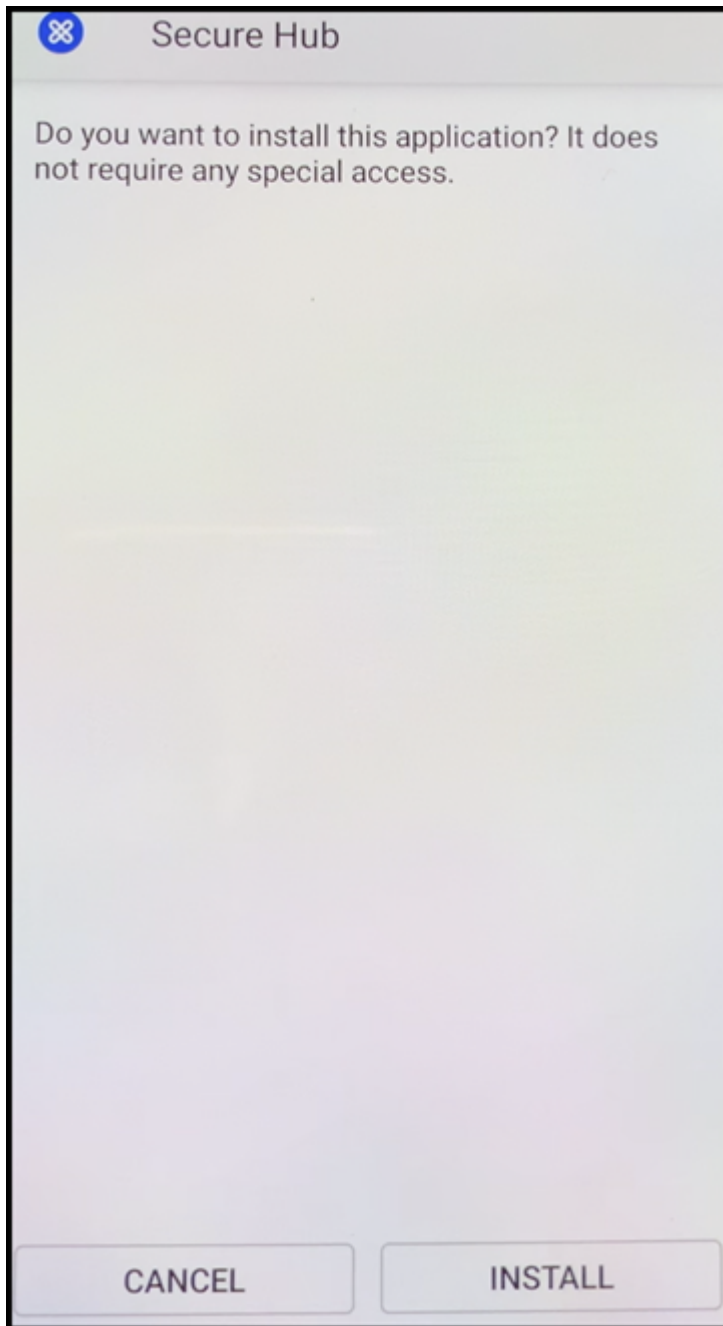
3. 전자메일또는전화필드에 `afw##xenmobile`을입력합니다.



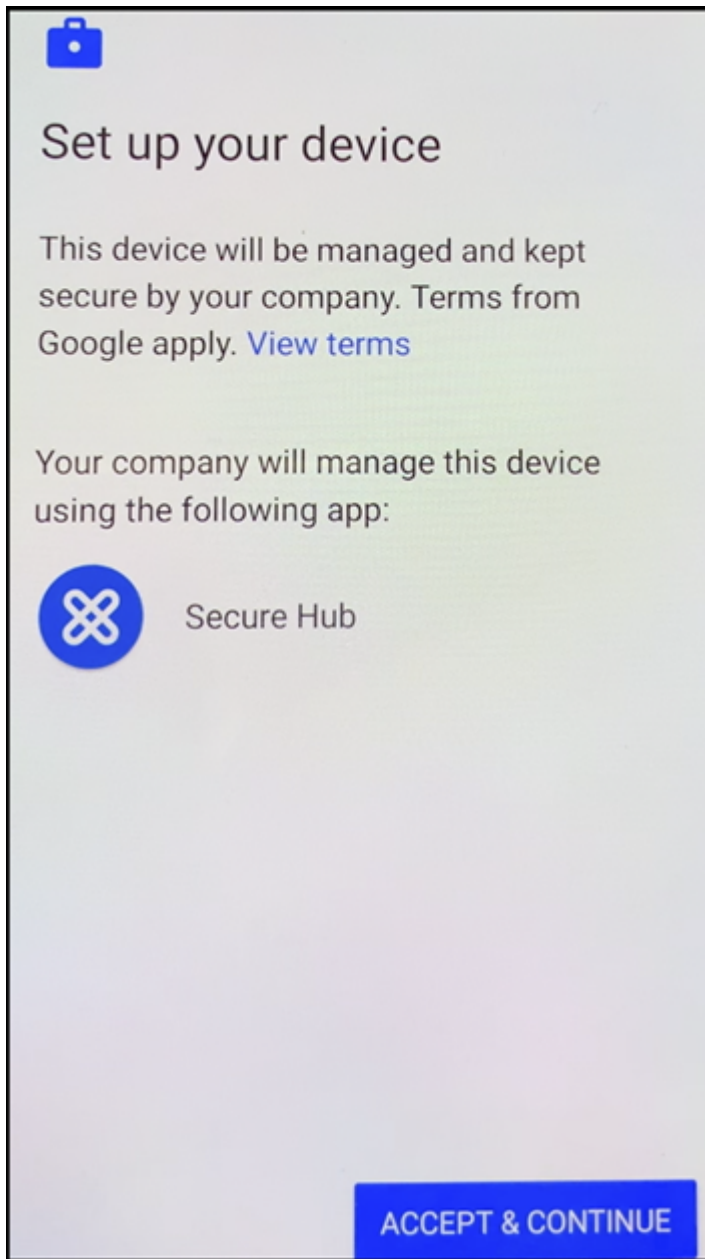
4. Android Enterprise 화면에서 Secure Hub 를설치하라는메시지가표시되면 설치를누릅니다.



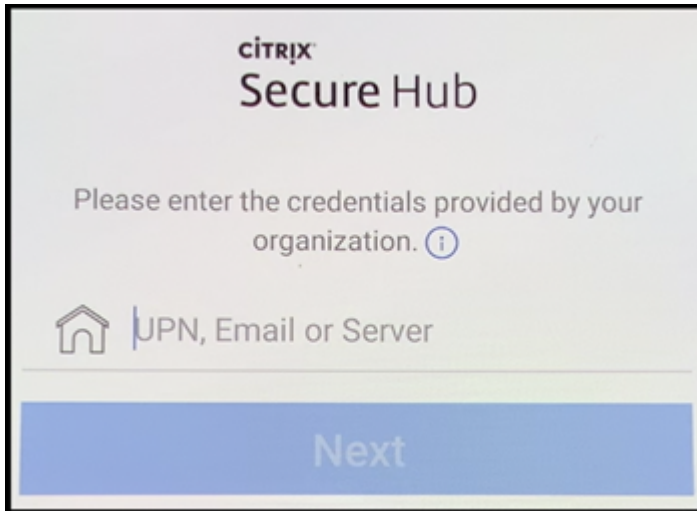
5. Secure Hub 설치관리자화면에서 **Install**(설치) 을누릅니다.



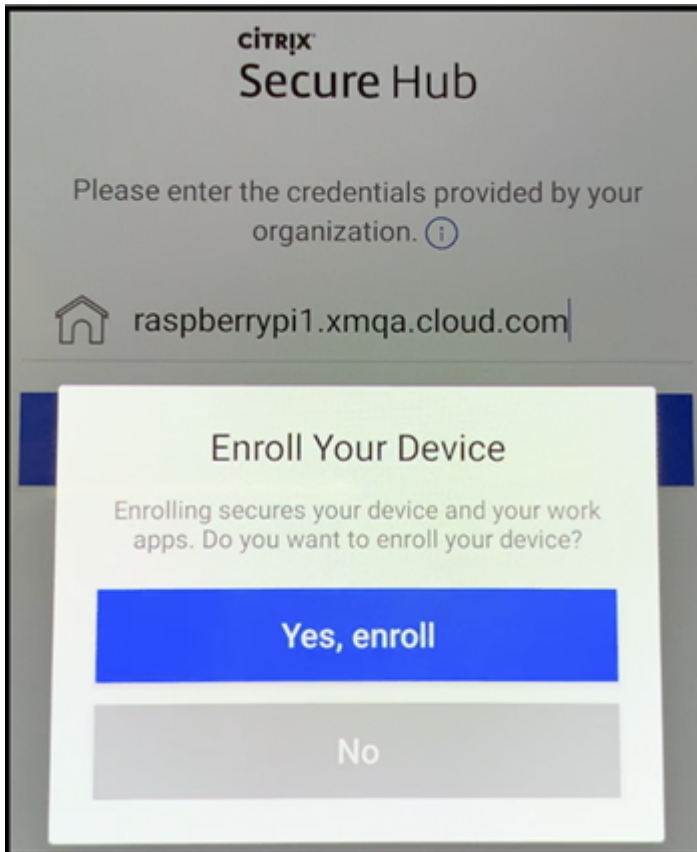
6. 모든앱권한요청에대해 **Allow**(허용) 를누릅니다.
7. **Accept & Continue**(동의및계속) 를눌러 Secure Hub 를설치하고장치관리를허용합니다.



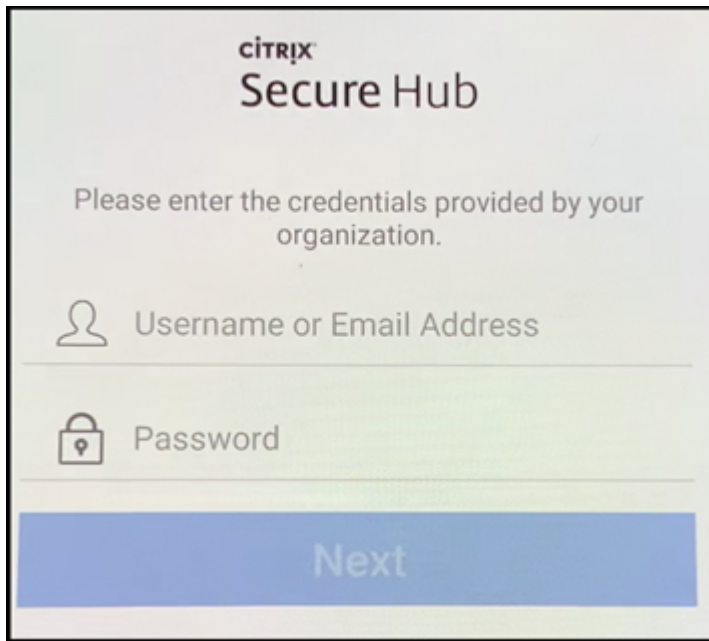
8. 이제 Secure Hub 가설치되었고기본등록화면에표시됩니다. 이에에서는자동검색을설정하지않았습니다. 자동검색을설정했다면사용자가사용자이름/전자메일을입력하고서버를찾을수있습니다. 대신환경에대한등록 URL 을입력하고 다음을 누릅니다.



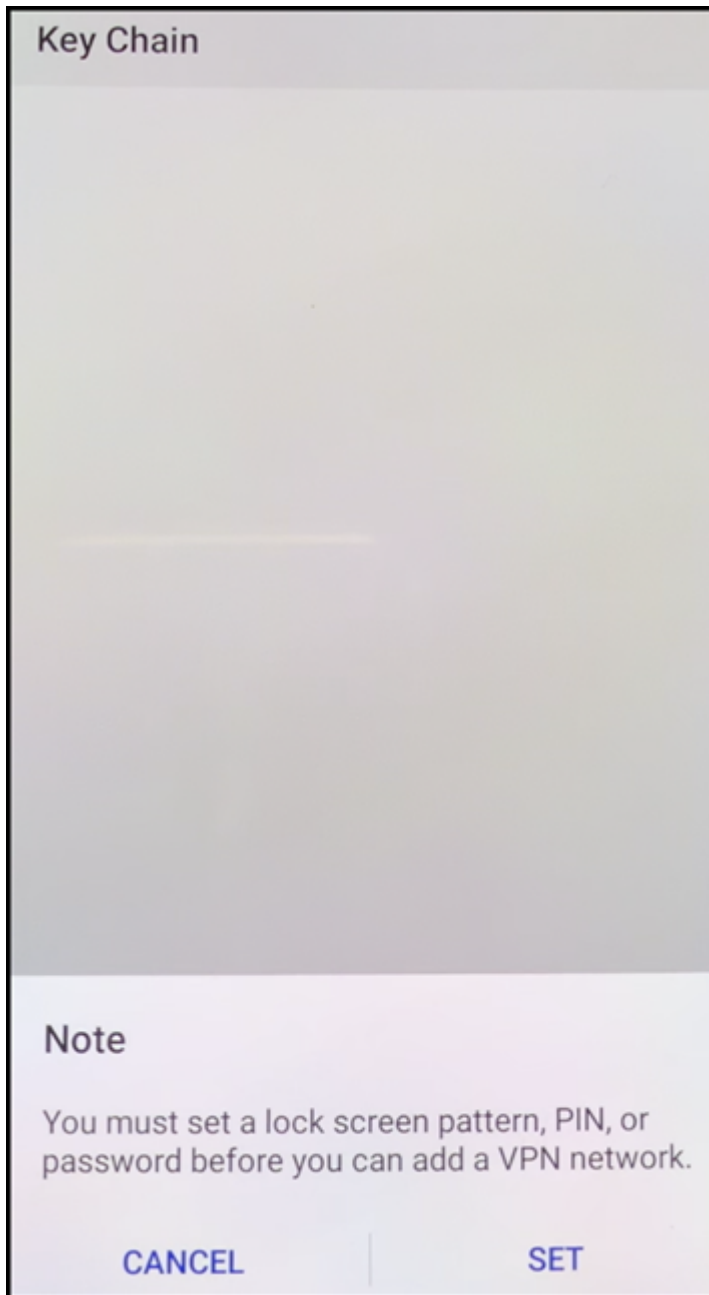
9. XenMobile 의기본구성에서는사용자가 MAM 을사용할지아니면 MDM+MAM 을사용할지를선택할수있습니다. 이와 같은메시지가표시되면 예. 등록을눌러 MDM+MAM 을선택합니다.



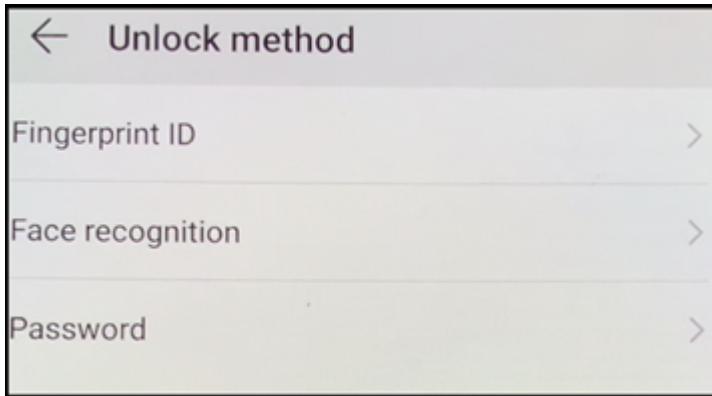
10. 사용자이름과암호를입력하고 다음을누릅니다.



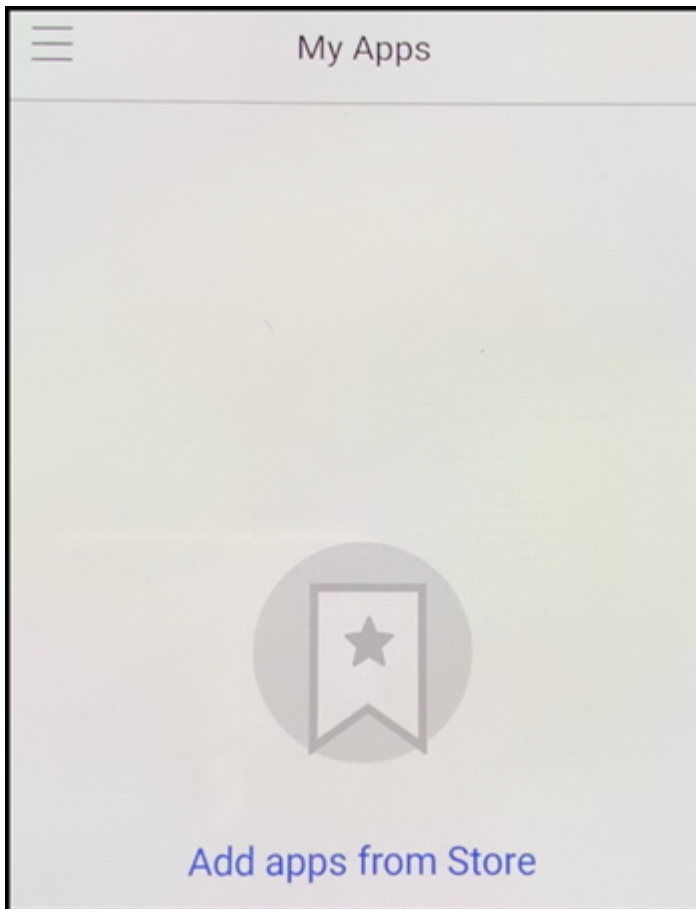
11. 장치암호를구성하라는메시지가표시됩니다. 설정을누르고암호를입력합니다.



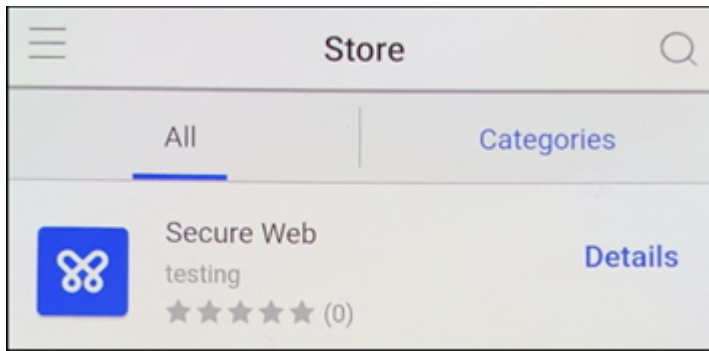
12. 작업프로필잠금해제방법을구성하라는메시지가표시됩니다. 이에에서는 암호를누르고 **PIN** 을누른다음 PIN 을입력합니다.



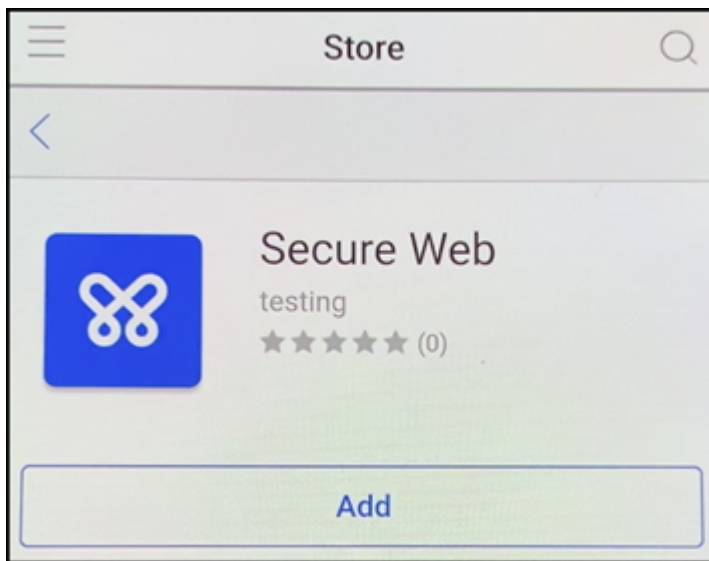
13. 이제 Secure Hub **My Apps**(내앱) 소개화면에장치가표시됩니다. 스토어의앱추가를누릅니다.



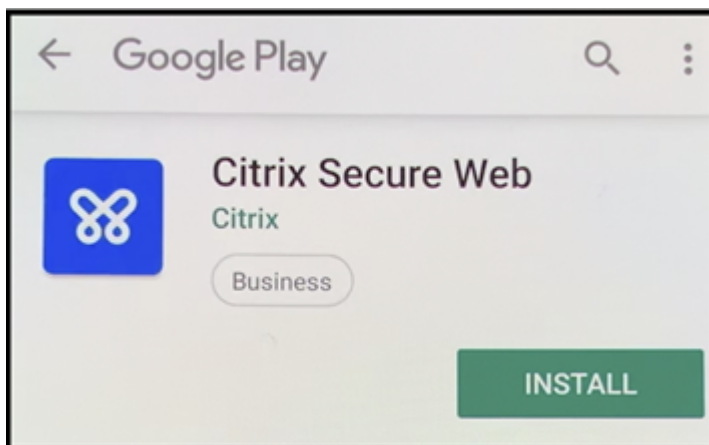
14. Secure Web 을추가하려면 **Secure Web** 을누릅니다.



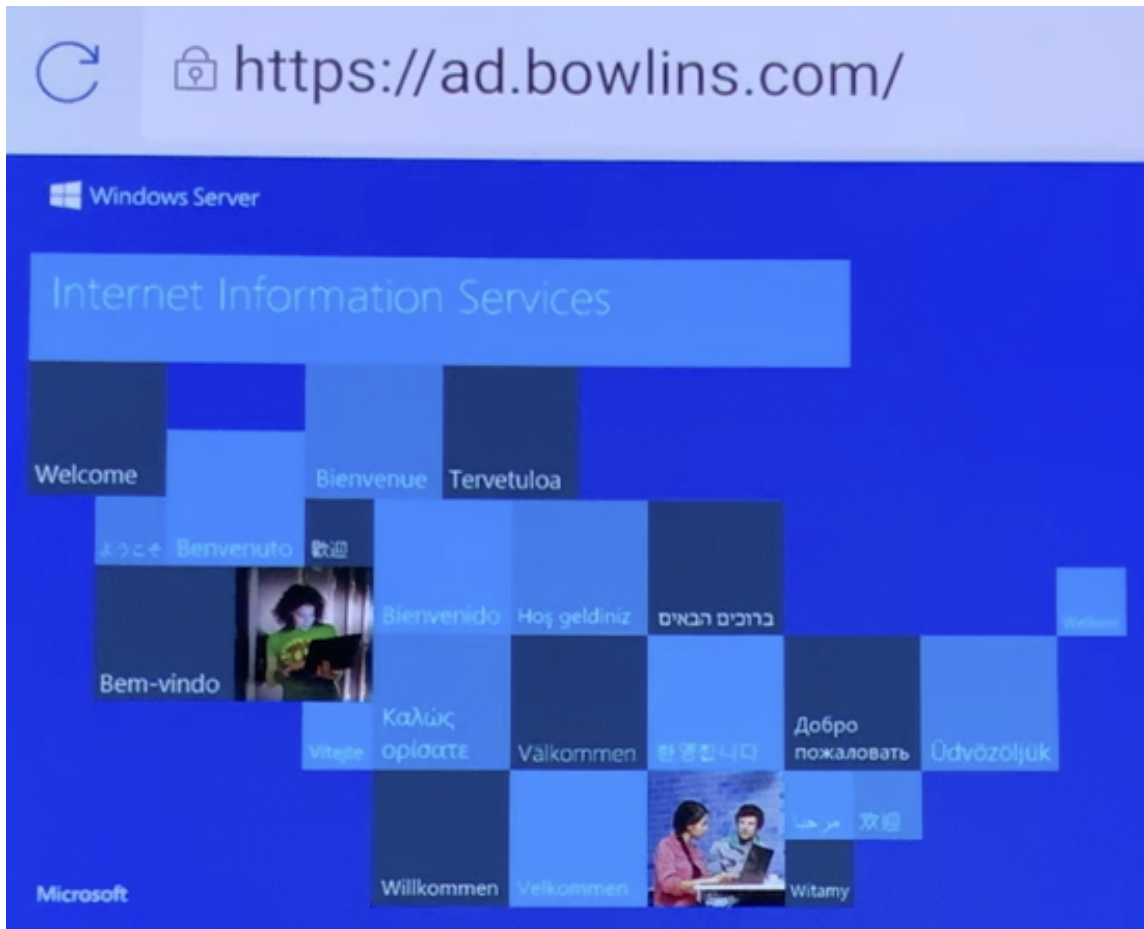
15. 추가를누릅니다.



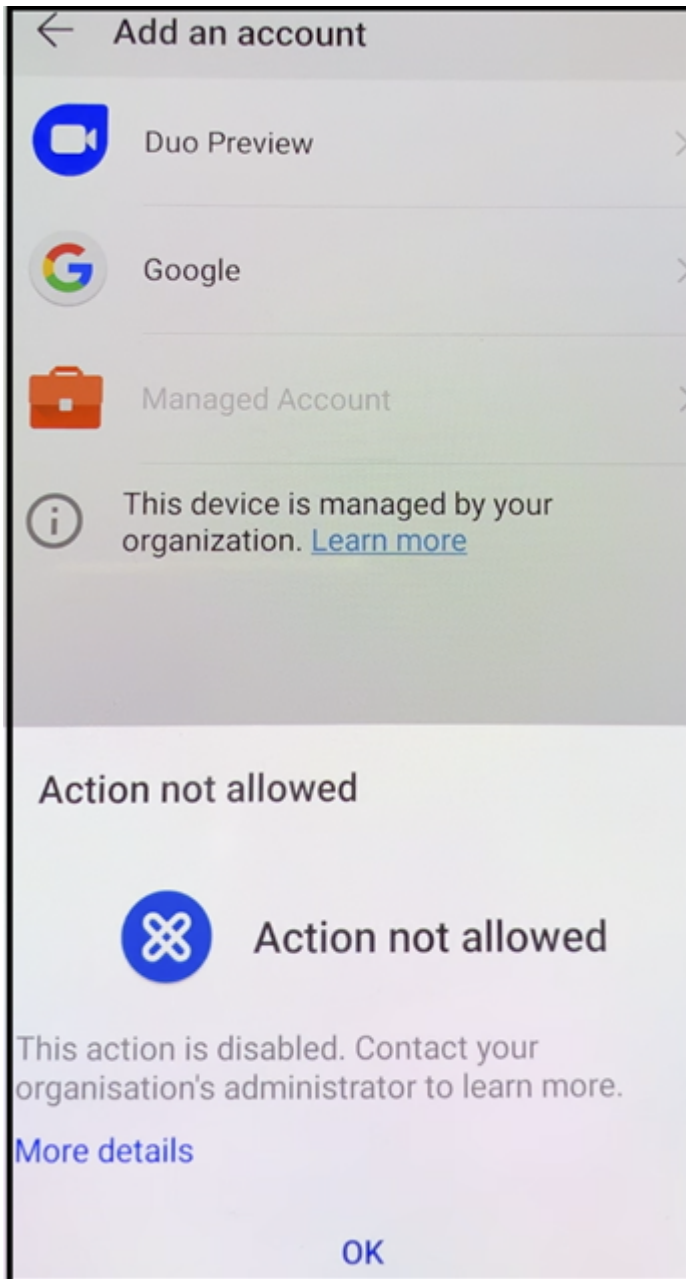
16. Secure Hub 가사용자를 Google Play Store 로보내 Secure Web 을설치하도록합니다. 설치를누릅니다.



17. Secure Web 이설치된후 열기를누릅니다. 주소표시줄에내부사이트의 URL 을입력하고페이지가로드되는지확인합니다.



18. 장치의 설정 > 계정으로이동합니다. 관리되는계정을수정할수없음을확인합니다. 화면공유또는원격디버깅을위한개발자 옵션도차단됩니다.



NFC 범프를 사용하여 장치 등록

NFC 범프를 사용하여 안전하게 관리되는 장치로 장치를 등록하려면 두 장치, 즉 출고 기본값으로 재설정된 장치와 XenMobile Provisioning Tool 을 실행하는 장치가 필요합니다.

시스템 요구 사항 및 사전 요구 사항

- 지원되는 Android 장치.

- 완전하게관리되는장치로서 Android Enterprise 용으로프로비전된새장치또는출고기본값으로재설정된장치. 이사전 요구사항을완료하는단계는이문서의뒷부분에서찾을수있습니다.
- NFC 호환성이있으며구성된 Provisioning Tool 이실행되고있는또다른장치. Provisioning Tool 은 Secure Hub 또는 [Citrix 다운로드페이지](#)에서사용할수있습니다.

각장치에는하나의 Android Enterprise 프로필인관리되는 Secure Hub 만있어야합니다. 각장치에는하나의프로필만허용됩니다. 두번째 DPC 앱을추가하려고하면설치된 Secure Hub 가제거됩니다.

NFC 범프를통해전송된데이터

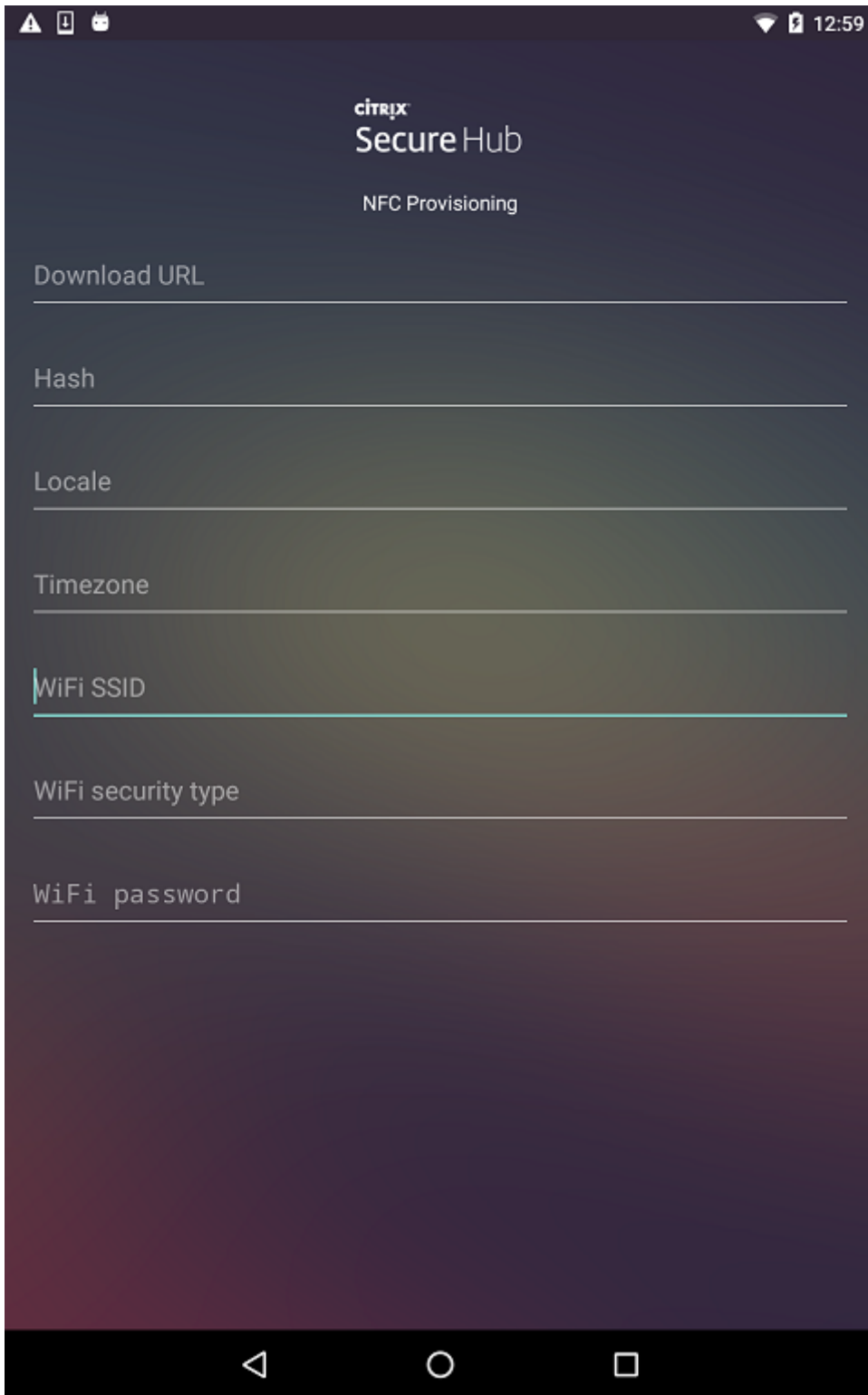
출고기본값으로재설정된장치를프로비저닝하려면 NFC 범프를통해다음데이터를전송하여 Android Enterprise 를초기화해야합니다.

- 장치소유자 (이경우 Secure Hub) 역할을하는 DPC 앱의패키지이름.
- 장치가 DPC 앱을다운로드할수있는인트라넷/인터넷위치.
- 다운로드가성공했는지확인하기위한 DPC 앱의 SHA1 해시.
- 공장기본값으로재설정된장치가연결하여 DPC 앱을다운로드할수있는 Wi-Fi 연결세부정보. 참고: 이단계에서 Android 는 802.1x Wi-Fi 를지원하지않습니다.
- 장치의표준시간대 (선택사항)
- 장치의지리적위치 (선택사항)

두장치가범프되면 Provisioning Tool 의데이터가출고기본값으로재설정된장치로전송됩니다. 이데이터는관리자설정으로 Secure Hub 를다운로드하는데사용됩니다. 표준시간대및위치값을입력하지않으면 Android 가자동으로새장치에서이러한값을구성합니다.

XenMobile Provisioning Tool 구성

NFC 범프를수행하기전에 Provisioning Tool 을구성해야합니다. 이구성은 NFC 범프중에출고기본값으로재설정된장치로전송됩니다.



필요한필드에데이터를입력하거나텍스트파일을통해데이터를채울수있습니다. 다음절차의단계에서는텍스트파일을구성하고각필드에대한설명을포함시키는방법에대해설명합니다. 입력한정보가앱에저장되지않으므로나중에사용할수있도록정보를유지하려면텍스트파일을만들수있습니다.

텍스트파일을 사용하여 **Provisioning Tool** 을 구성하려면

파일의 이름을 nfcprovisioning.txt 로 지정하고 장치의 SD 카드에 있는 /sdcard/ 폴더에 파일을 저장합니다. 그러면 앱에서 텍스트파일을 읽고 값을 채울 수 있습니다.

텍스트파일에는 다음과 같은 데이터가 포함되어야 합니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>
```

이 줄은 EMM 공급자 앱의 인터넷/인터넷 위치입니다. NFC 범프 후에 출고 기본값으로 재설정된 장치가 Wi-Fi 에 연결되면 장치가 이 위치에 액세스하여 다운로드할 수 있어야 합니다. URL 은 특수한 형식이 필요하지 않은 일반 URL 입니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```

이 줄은 EMM 공급자 앱의 체크섬입니다. 이 체크섬은 다운로드가 성공했는지 확인하는 데 사용됩니다. 체크섬을 얻는 단계에 대해서는 이 문서 뒷부분에서 설명합니다.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

이 줄은 Provisioning Tool 이 실행되고 있는 장치의 연결된 Wi-Fi SSID 입니다.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

지원되는 값은 WEP 및 WPA2 입니다. Wi-Fi 가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Wi-Fi 가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

언어 및 국가 코드를 입력합니다. 언어 코드는 [ISO 639-1](#)에 정의된 대로 소문자 두 자로 구성된 ISO 언어 코드입니다 (예: en). 국가 코드는 [ISO 3166-1](#)에 정의된 대로 대문자 두 자로 구성된 ISO 국가 코드입니다 (예: US). 예를 들어, 미국에서 사용하는 영어의 경우 en_US 를 입력합니다. 코드를 입력하지 않으면 국가 및 언어가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

장치가 실행되는 표준 시간대입니다. [지역/위치 형식의 Olson 이름](#)을 입력합니다. 예를 들어 태평양 표준 시의 경우 America/Los_Angeles 를 입력합니다. 이름을 입력하지 않으면 표준 시간대가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

값이 앱에 Secure Hub 로 하드코딩되어 있기 때문에 이 데이터는 필요하지 않습니다. 여기서는 완결성을 위해 언급되었습니다.

예를 들어 WPA2 를 사용하여 보호되는 Wi-Fi 가 있는 경우 완성된 nfcprovisioning.txt 파일은 다음과 같습니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

예를들어보호되지않는 Wi-Fi 가있는경우완성된 nfcprovisioning.txt 파일은다음과같습니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\n\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Secure Hub 체크섬을얻으려면

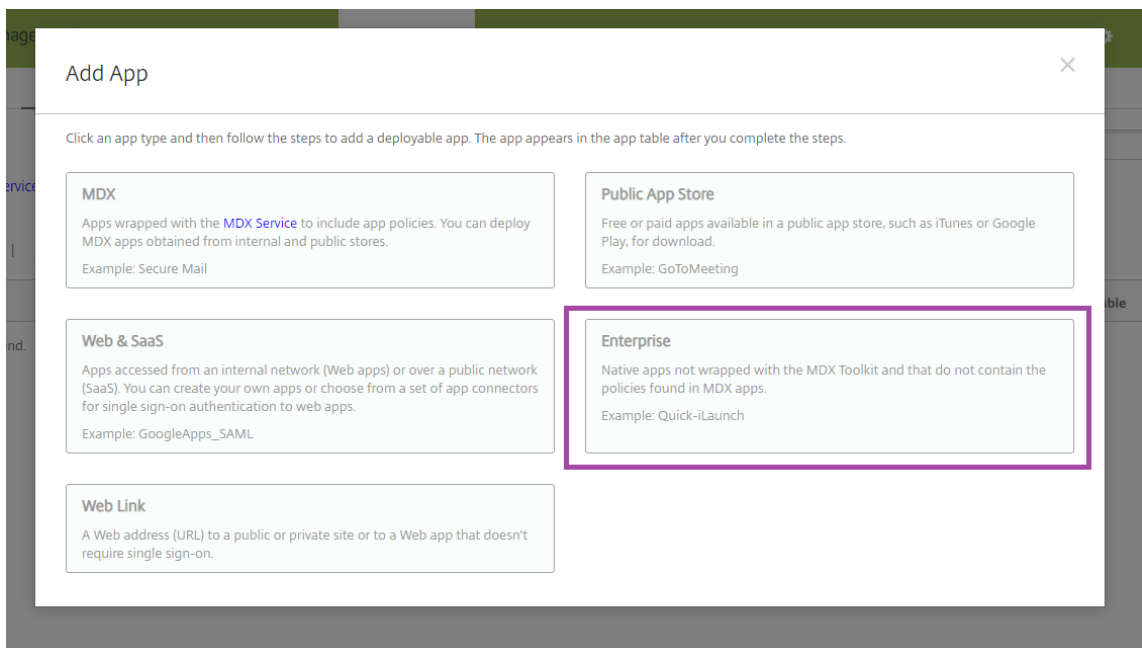
특정앱의체크섬을얻으려면앱을엔터프라이즈앱으로추가합니다.

1. XenMobile 콘솔에서 구성 > 앱으로이동한후 추가를클릭합니다.

앱추가창이나타납니다.

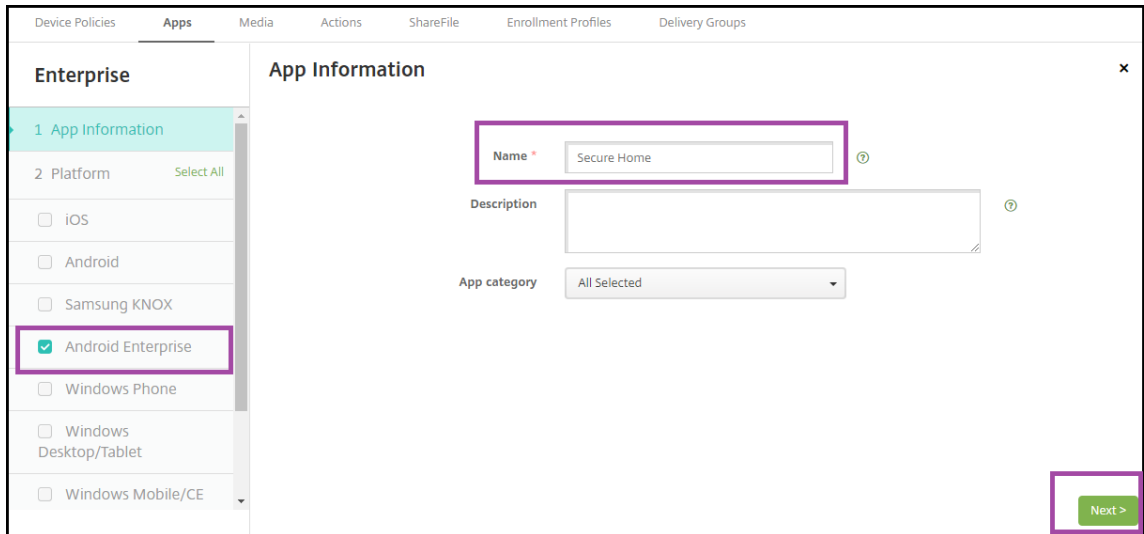
2. 엔터프라이즈를클릭합니다.

앱정보페이지가나타납니다.



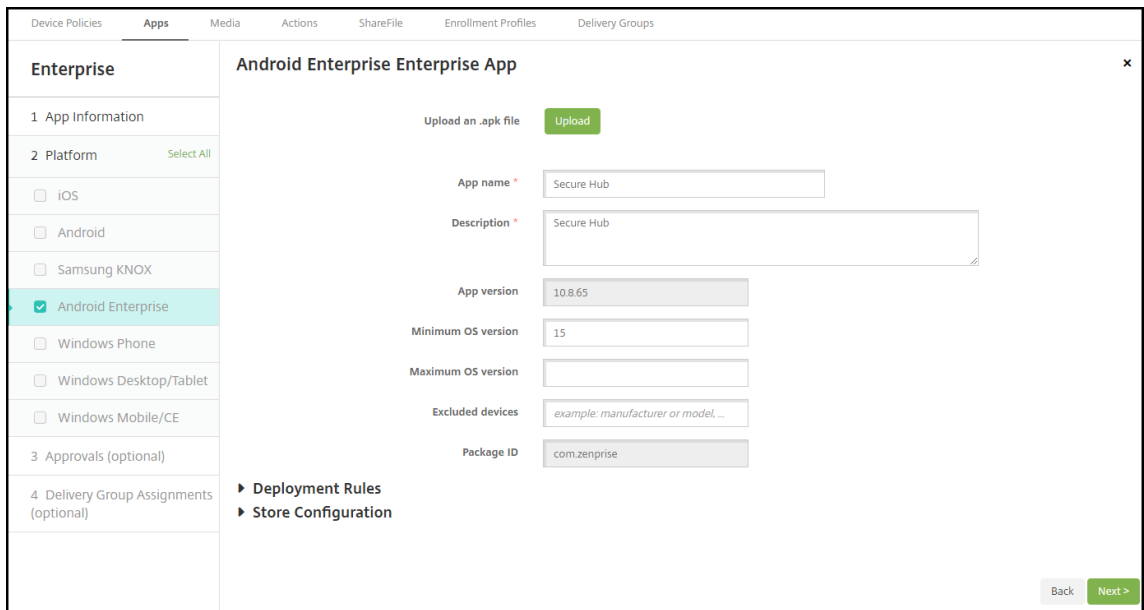
3. 다음과같은구성을선택한후 다음을클릭합니다.

Android Enterprise 엔터프라이즈앱페이지가나타납니다.

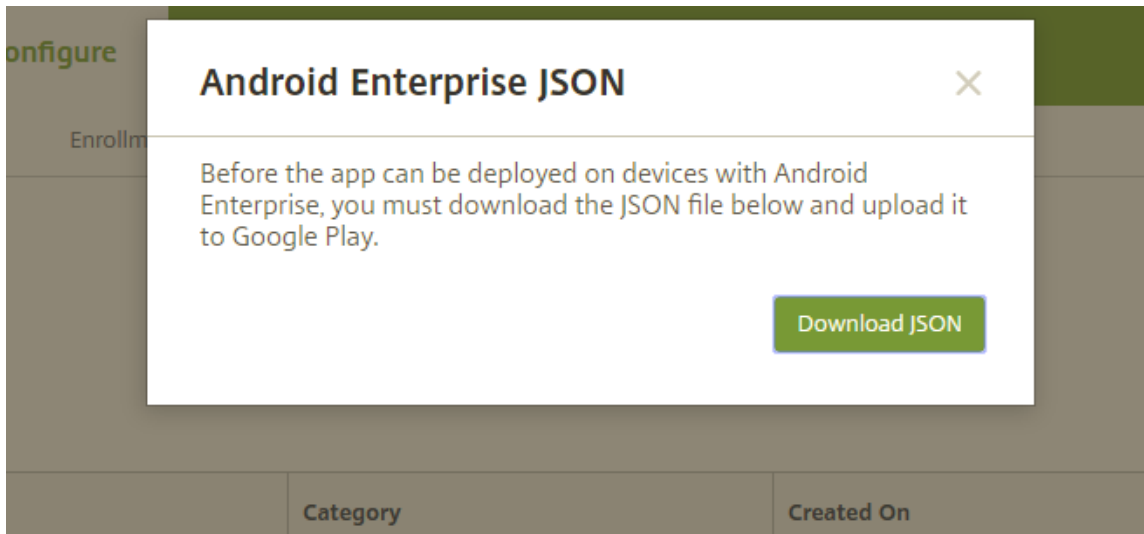


4. .apk 에대한경로를제공한후 다음을클릭하고파일을업로드합니다.

업로드가완료되면업로드된패키지의세부정보가나타납니다.



5. 다음을클릭합니다. **JSON** 다운로드를클릭하여 JSON 파일을다운로드하는페이지를열니다. 이파일을사용하여 Google Play 에업로드할수있습니다. Secure Hub 의경우 Google Play 에업로드할필요가없지만 SHA1 값을읽으려면 JSON 파일이필요합니다.



일반적인 JSON 파일은 다음과 같은 형식입니다.

```

1  {"icon_filename":"48_48_launcher.png","file_sha256_base64":
2  "01MZ86TLGd9Txis1NfE8W0i1Q0uV80xvLA003P3Av9Vw09d", "file_sha1_base64":
3  "154vulWtkzf1x8mT3Cntap3g0\u003d", "package_name":"com.zenprise",
4  "application_label":"Worx Home", "icon_base64":
5  "iVBORw0KGgoAAAANSUkEUgAAADAAAAwCAYAAABXAmHAAAPK1EQVRo3u2aaZSU1ZnHf/e+71vV1dXdfHQ03U2zHgATYgKTLJko0E50YU4S181MjkeNZ1Q0a1yZicLoJkxaojHJGJHMJYn8XFB4gIaSNjM85ZuICagrn3NQLP8B?
6  "version_code":"352975", "certificate_base64": [
7  "H1BqzCCARSpAwZBqIE5/pjDAN0qkqk1G9w0B4UfADAAmRgwfYDVO0KEv9TcFydXgU29mdHdcmUghdMfTAwNTI00EYhcnNDAAwNTEZHT180DEYmJAaMRgwfYDVO0KEv9TcFydXgU29mdHdcmUghZ0v0QY.
8  "file_size":"25916262", "externally_hosted_url":
9  "https://afwtest.xmdev.citrix.com:4443/Citrix/v1/download/app/MobileApp23",
10 "version_name":"10.3.0", "minimum_sdk":"14"}
11
    
```

6. **file_sha1_base64** 값을 복사한 후 Provisioning Tool의 해시 필드에 이 값을 사용합니다.

참고: 해시는 URL로 사용할 수 있는 형식이어야 합니다.

- 모든 + 기호를 -로 변환합니다.
- 모든 / 기호를 _로 변환합니다.
- 끝에 있는 \u003d 를 =로 바꿉니다.

장치의 SD 카드에 있는 nfcprovisioning.txt 파일에 해시를 저장하면 앱에서 안전을 위한 변환을 수행합니다. 하지만 수동으로 해시를 입력하는 경우 URL 안전성을 보장하는 것은 사용자의 책임입니다.

사용된 라이브러리

Provisioning Tool의 소스 코드에는 다음과 같은 라이브러리가 사용되었습니다.

- Apache 라이선스 2.0에 따라 Google이 제작한 v7 appcompat 라이브러리, 디자인 지원 라이브러리와 v7 Palette 라이브러리
자세한 내용은 [지원 라이브러리 기능 가이드](#)에서 참조하십시오.
- Apache 라이선스 2.0에 따라 Jake Wharton이 제작한 [Butter Knife](#)

QR 코드를 사용하여 장치 등록

QR 코드를 사용하여 완전하게 관리되는 장치를 등록하려면 JSON 을 생성하고 JSON 을 QR 코드로 변환하여 QR 코드를 생성합니다. QR 코드가 장치 카메라로 스캔되어 장치가 등록됩니다.

시스템 요구 사항

- Android 8.0 이상을 실행하는 모든 Android 장치에서 지원됩니다.

JSON 에서 QR 코드 생성

다음 필드를 사용하여 JSON 을 생성합니다.

다음 필드는 필수입니다.

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

값: com.zenprise/com.zenprise.configuration.AdminFunction

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

값: qn7oZUtheu3JBAinzZRrjCQv6LOO6Ll1OjcxT3-yKM

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

값: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>

다음 필드는 선택 사항입니다.

- **android.app.extra.PROVISIONING_LOCALE:** 언어 및 국가 코드를 입력합니다.
언어 코드는 ISO 639-1에 정의된 대로 소문자 두 자로 구성된 ISO 언어 코드입니다 (예: en). 국가 코드는 ISO 3166-1에 정의된 대로 대문자 두 자로 구성된 ISO 국가 코드입니다 (예: US). 예를 들어, 미국에서 사용하는 영어의 경우 en_US 를 입력합니다.
- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가 실행되고 있는 표준 시간대입니다.
지역/위치 형식의 Olson 이름을 입력합니다. 예를 들어 태평양 표준 시의 경우 America/Los_Angeles 를 입력합니다. 입력하지 않으면 표준 시간대가 자동으로 입력됩니다.
- **android.app.extra.PROVISIONING_LOCAL_TIME:** Epoch 이후의 시간 (밀리초)입니다.
Unix Epoch (즉 Unix 시간 또는 POSIX 시간 Unix 타임스탬프) 는 1970 년 1 월 1 일 (자정 UTC/GMT) 이후 경과한 시간이며, 윤초는 계산되지 않습니다 (ISO 8601: 1970-01-01T00:00:00Z).
- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 프로필 생성 시 암호화를 건너뛰려면 true 로 설정합니다. 프로필 생성 시 암호화를 적용하려면 false 로 설정합니다.

일반적인 JSON 은 다음과 같은 형식입니다.

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": " ",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

JSON 유효성검사도구 (예: <https://jsonlint.com>) 를 사용하여 생성된 JSON 의 유효성을 검사하고 온라인 QR 코드 생성기 (예: <https://goqr.me>) 를 사용하여 해당 JSON 문자열을 QR 코드로 변환합니다.

이 QR 코드는 공장 기본값으로 재설정된 장치에서 스캔되어 해당 장치를 완전 관리되는 장치로 등록하는 데 사용됩니다.

장치를 등록하려면

새 장치 또는 공장 기본값으로 재설정된 장치의 전원을 켜 후:

1. 시작 화면에서 화면을 6 번 눌러 QR 코드 등록 흐름을 시작합니다.
2. 메시지가 표시되면 Wi-Fi 에 연결합니다. QR 코드에 있는 Secure Hub 의 다운로드 위치 (JSON 으로 인코딩됨) 는 이 Wi-Fi 네트워크를 통해 액세스할 수 있습니다.
장치가 Wi-Fi 에 연결되면 Google 에서 QR 코드 판독기를 다운로드 하고 카메라를 시작합니다.
3. 카메라로 QR 코드를 가리키고 코드를 스캔합니다.

Android 는 QR 코드에 있는 다운로드 위치에서 Secure Hub 를 다운로드 하고 서명 인증서 서명의 유효성을 검사한 후 Secure Hub 를 설치하고 장치 소유자로 설정합니다.

자세한 내용은 Android EMM 개발자용 Google 가이드 (https://developers.google.com/android/work/prov-devices#qr_code_method) 를 참조하십시오.

제로터치 등록

제로터치 등록을 사용하면 장치 전원을 처음 켤 때 완전 관리되는 장치로 프로비전하도록 설정할 수 있습니다.

장치에 구성을 적용할 때 사용할 수 있는 온라인 도구인 Android 제로터치 포털에서 장치 리셀러를 통해 계정을 만들 수 있습니다. 그런 다음 Android 제로터치 포털에서 하나 이상의 제로터치 등록 구성을 만들고 계정에 할당된 장치에 구성을 적용합니다. 사용자가 이러한 장치의 전원을 켜면 장치가 자동으로 XenMobile 에 등록됩니다. 장치에 할당된 구성에 따라 자동 등록 프로세스가 정의됩니다.

시스템 요구 사항

- 제로터치 등록에 대한 지원은 Android 8.0 부터 시작됩니다.

리셀러의 장치 및 계정 정보

- 제로터치 등록이 가능한 장치는 엔터프라이즈 리셀러 또는 Google 파트너로부터 구입할 수 있습니다. Android Enterprise 제로터치 파트너 목록은 [Android 웹사이트](#) 를 참조하십시오.

- 리셀러를통해만든 Android Enterprise 제로터치포털계정.
- 리셀러가제공하는 Android Enterprise 제로터치포털계정로그인정보.

제로터치구성만들기

제로터치구성을만들때는구성세부정보를지정하는사용자지정 JSON 을포함합니다.

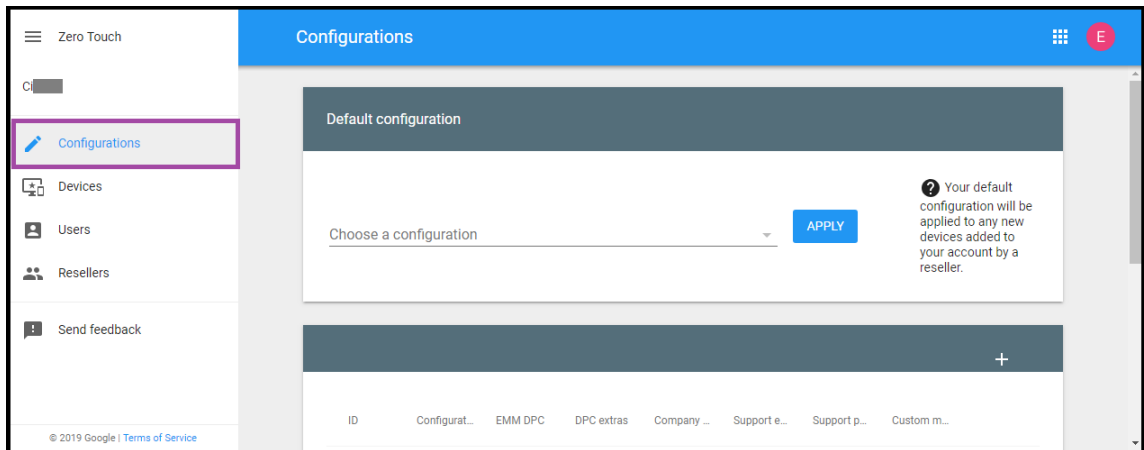
이 JSON 을사용하여지정한 XenMobile 서버에등록할장치를구성합니다. 이에에서는 'URL' 을서버의 URL 로대체하십시오.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7      }
8
9      }
```

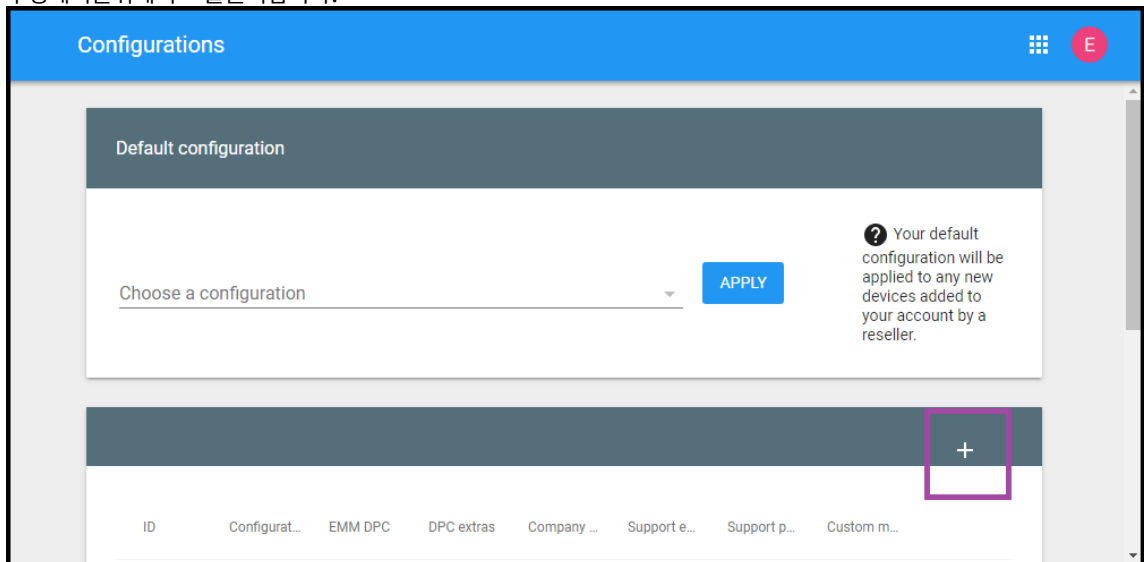
매개변수가더많은선택적 JSON 을사용하여구성을추가로사용자지정할수있습니다. 이에에서는 XenMobile 서버와이구성을사용하는장치가서버에로그인할때사용하는사용자이름과암호를지정합니다.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7          "xm_username": "username",
8          "xm_password": "password"
9      }
10
11     }
```

1. Android 제로터치포털 (<https://partner.android.com/zerotouch>) 로이동합니다. 제로터치장치리셀러의계정정보를사용하여로그인합니다.
2. 구성을클릭합니다.



3. 구성테이블위에서 + 를클릭합니다.



4. 구성창이표시되면구성정보를입력합니다.

Add a new configuration

Configuration name

EMM DPC

Select

DPC extras

Company name

Support email address

Support phone number

CANCEL ADD

- **Configuration name(구성이름):** 이 구성에 대해 선택한 이름을 입력합니다.
- **EMM DPC: Citrix Secure Hub** 를 선택합니다.
- **DPC extras(DPC 추가항목):** 이 필드에 사용자 지정 JSON 텍스트를 붙여넣습니다.
- **Company name(회사이름):** 장치 프로비전 중에 Android Enterprise 제로 터치 장치에 표시할 이름을 입력합니다.
- **Support email address(지원 전자 메일 주소):** 사용자가 지원 문의할 수 있는 전자 메일 주소를 입력합니다. 이

주소는장치프로비전전에 Android Enterprise 제로터치장치에나타납니다.

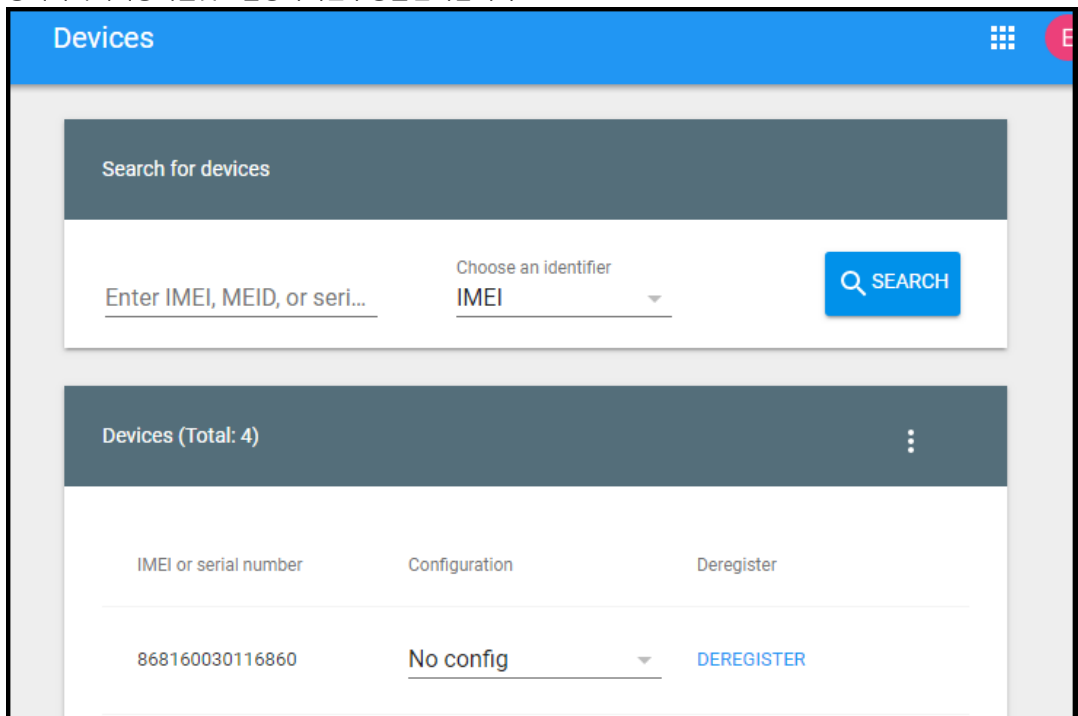
- **Support phone number(지원전화번호):** 사용자가지원을문의할수있는전화번호를입력합니다. 이전화번호는장치프로비전전에 Android Enterprise 제로터치장치에나타납니다.
- **Custom Message(사용자지정메시지):** 필요에따라사용자가문의하는데도움이되거나사용자에게장치에대한추가정보를제공하는데도움이되는하나또는두개의문장을추가합니다. 이사용자지정메시지는장치프로비전전에 Android Enterprise 제로터치장치에나타납니다.

5. 추가를클릭합니다.

6. 구성을추가로만들려면 2~4 단계를반복합니다.

7. 장치에구성을적용하려면:

- a) Android 제로터치포털에서 **Devices(장치)** 를클릭합니다.
- b) 장치목록에서장치를찾고할당하려는구성을선택합니다.



- c) **Update(업데이트)** 를클릭합니다.

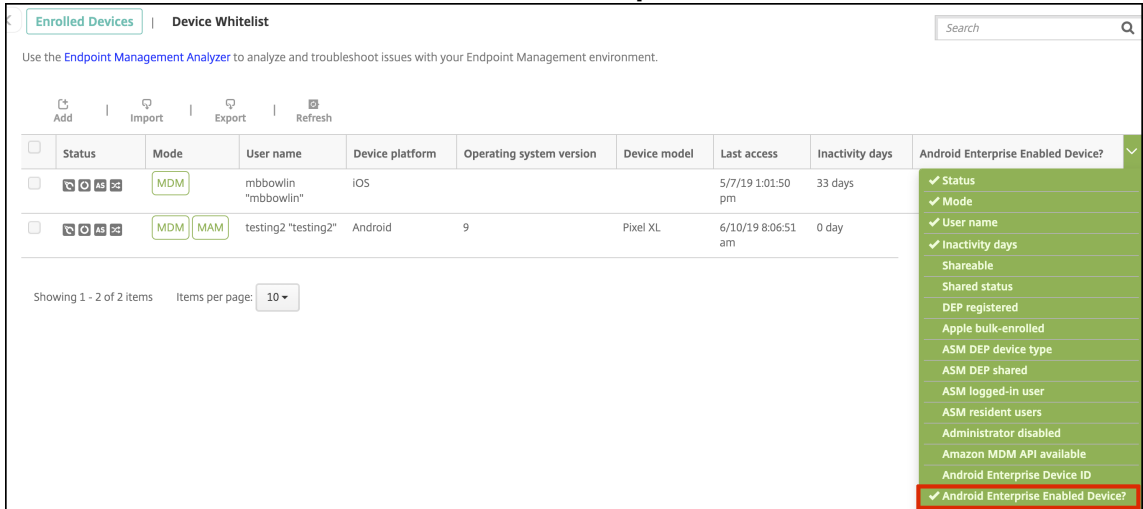
CSV 파일을사용하여여러장치에구성을적용할수있습니다.

여러장치에구성을적용하는방법에대한자세한내용은 Android Enterprise 도움말항목 [IT 관리자의제로터치등록](#)을참조하십시오. 이 Android Enterprise 도움말항목에는구성을관리하고장치에구성을적용하는방법에대한자세한정보가나와있습니다.

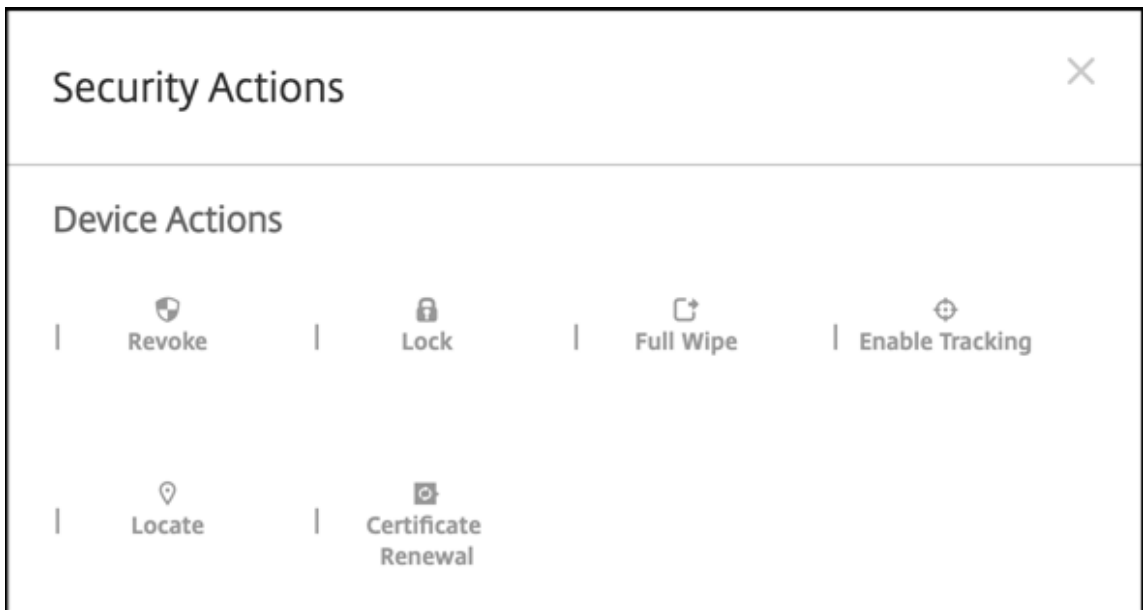
XenMobile 콘솔에서안전관리되는장치보기

1. XenMobile 콘솔에서 관리 > 장치로이동합니다.

2. 이 페이지의 테이블 오른쪽에 있는 메뉴를 클릭하여 **Android Enterprise** 에서 활성화된 장치? 열을 추가합니다.



3. 사용 가능한 보안 동작을 보려면 완전 관리되는 장치를 선택하고 보안을 클릭합니다. 장치가 완전 관리되는 경우 전체 초기화 작업을 사용할 수 있지만 선택적 초기화는 사용할 수 없습니다. 이차이는 장치가 관리되는 Google Play Store 의 앱만 허용하기 때문입니다. 사용자가 공용 스토어에서 응용 프로그램을 설치할 수 있는 옵션은 없습니다. 장치의 모든 콘텐츠는 조직에서 관리합니다.



전용 Android Enterprise 장치 프로비전

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

전용 장치는 Android Enterprise 완전 관리되는 장치 프로비전에 설명된 대로 완전 관리되는 다른 장치에서 사용되는 등록 방법 중 하나

를 사용하여 등록됩니다. 전용장치를 프로비전하려면 등록하기 전에 추가 설정이 필요합니다.

전용장치를 COSU(회사소유일회사용) 장치라고도 합니다.

참고:

완전관리되는 다른 장치와 달리 전용장치는 Active Directory 계정을 가진 사용자만 등록할 수 있습니다. 로컬 사용자는 전용 장치를 등록할 수 없습니다.

전용장치를 프로비전하려면:

- XenMobile 관리자가 XenMobile 배포에 전용장치를 등록하는데 필요한 RBAC(역할기반액세스제어) 역할을 추가합니다. 전용장치를 등록할 사용자에게 이 역할을 할당합니다.
- XenMobile 배포에 전용장치를 등록할 수 있도록 허용하는 XenMobile 관리자용 등록 프로필을 추가합니다.
- 전용장치에서 액세스할 앱을 화이트리스트에 추가합니다.
- 필요한 경우 작업 잠금 모드를 허용하도록 화이트리스트의 앱을 설정합니다. 앱이 작업 잠금 모드에 있으면 사용자가 앱을 열 때 앱이 장치 화면에 고정됩니다. 홈 단추 가나 나타나지 않고 뒤로 단추 가 비활성화됩니다. 사용자는 로그아웃과 같이 앱에 프로그래밍된 작업을 사용하여 앱을 종료할 수 있습니다.
- 각 장치를 완전관리되는 장치로 등록합니다.

시스템 요구 사항

- 전용장치 등록 지원은 Android 6.0 부터 시작됩니다.

전용장치에 대한 RBAC 역할 추가

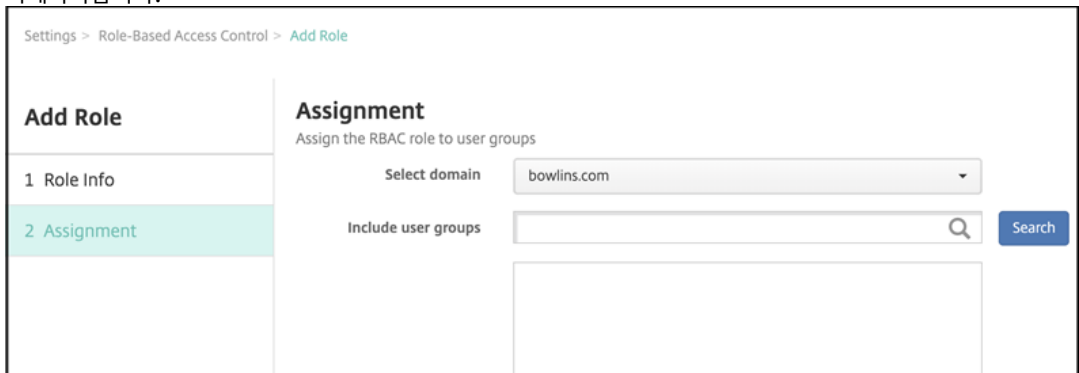
전용장치 등록을 위한 RBAC 역할이 있으면 XenMobile 이 관리되는 Google Play 계정을 장치에 자동으로 프로비전하고 활성화할 수 있습니다. 관리되는 Google Play 사용자 계정과 달리 이러한 장치 계정은 사용자와 연결되지 않은 장치를 식별합니다.

이 RBAC 역할을 XenMobile 관리자에게 할당하면 이러한 관리자가 전용장치를 등록할 수 있습니다.

전용장치 등록을 위한 RBAC 역할을 추가하려면:

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 역할기반액세스제어를 클릭합니다. 역할기반액세스제어 페이지가 나타납니다. 이 페이지에는 네 개의 기본 사용자 역할과 앞서 추가한 모든 역할이 표시됩니다.
3. 추가를 클릭합니다. 역할 추가 페이지가 나타납니다.
4. 다음 정보를 입력합니다.
 - **RBAC 이름:** "COSU" 또는 역할을 설명하는 이름을 입력합니다. 역할 이름은 변경할 수 없습니다.
 - **RBAC 템플릿:** ADMIN 템플릿을 선택합니다.
 - **허가된 액세스:** 관리자 콘솔 액세스 및 **COSU** 장치 등록자를 선택합니다.
 - **콘솔 기능:** 장치를 선택합니다.

- 권한적용: COSU 역할을적용할그룹을선택합니다. 특정사용자그룹을클릭하면하나이상의그룹을선택할수있는그룹목록이나타납니다.
5. 다음을클릭합니다. 할당페이지가나타납니다.
 6. 다음정보를입력하여 Active Director 그룹에역할을할당합니다.
 - 도메인선택: 목록에서도메인을클릭합니다.
 - 사용자그룹포함: 검색을클릭하여사용가능한모든그룹목록을표시합니다. 또는전체또는부분그룹이름을입력하여해당이름을가진그룹으로목록을제한합니다.
 - 나타나는목록에서역할을할당할사용자그룹을선택합니다. 사용자그룹을선택하면해당그룹이 선택된사용자그룹목록에나타납니다.

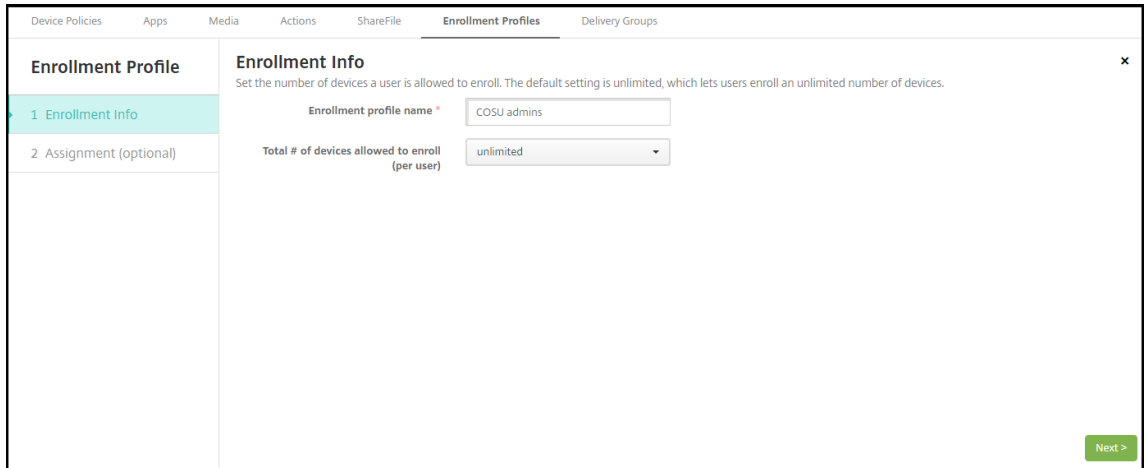


7. 저장을클릭합니다.

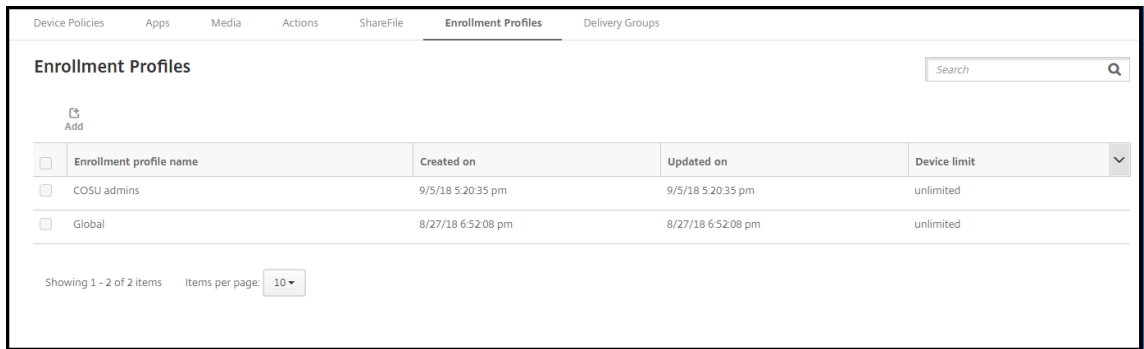
전용 (COSU) 등록프로필추가

XenMobile 배포에전용장치가포함되는경우단일 XenMobile 관리자또는소규모관리자그룹이다수의전용장치를등록합니다. 이러한관리자가필요한모든장치를등록할수있도록하려면사용자당무제한의장치가허용되는관리자용등록프로필을만듭니다. 전용장치를등록하는관리자가포함된배달그룹에이프로필을할당합니다. 이렇게하면기본글로벌프로필에서사용자당허용되는장치수가제한되어있더라도관리자가장치를무제한으로등록할수있습니다. 이러한관리자는전용 (COSU) 등록프로필에포함되어야합니다.

1. XenMobile 콘솔에서 구성 > 등록프로필로이동합니다. 기본 Global 프로필이표시됩니다.
2. 등록프로필을추가하려면 추가를클릭합니다. 등록정보페이지에서등록프로필의이름을입력합니다. 이프로필을가진구성원이등록할수있는장치수가무제한으로설정되어있는지확인합니다.



3. 다음을 클릭합니다. 배달그룹할당화면이 나타납니다.
4. 전용장치를 등록하는 관리자가 포함된 배달 그룹을 선택합니다. 그런 다음 저장을 클릭합니다.
추가한 프로필과 함께 등록 프로필 페이지가 나타납니다.



화이트리스트에 앱 추가 및 작업 잠금 모드 설정

키오스크 장치 정책을 사용하면 앱을 화이트리스트에 추가하고 작업 잠금 모드를 설정할 수 있습니다. 기본적으로 Secure Hub 와 Google Play 서비스는 화이트리스트에 포함됩니다.

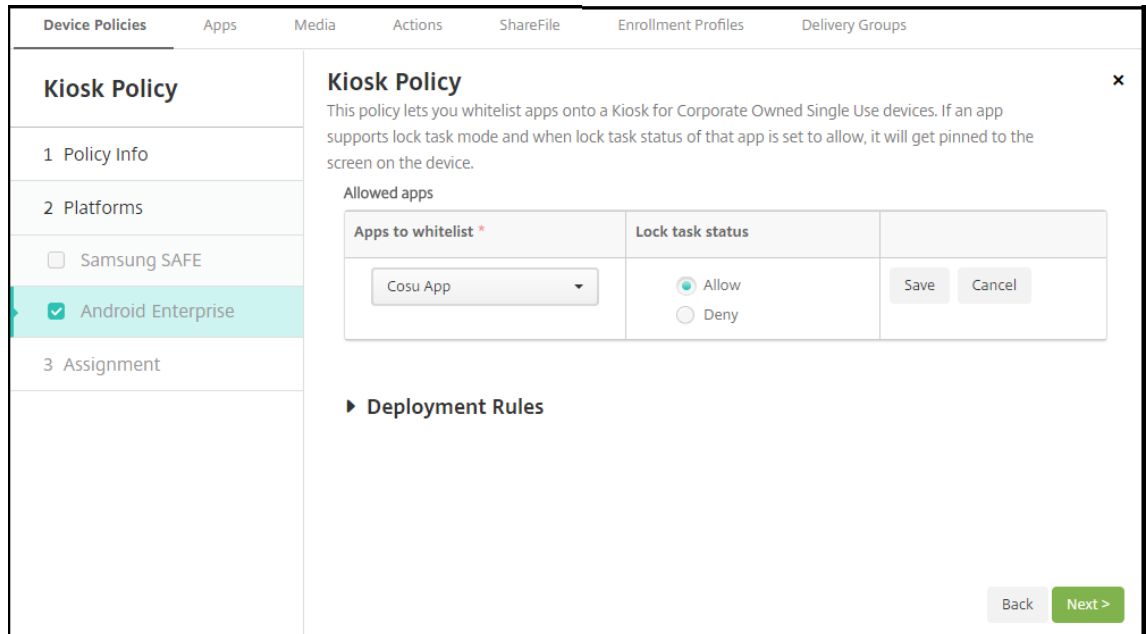
키오스크 정책을 추가하려면:

1. XenMobile 콘솔에서 구성 > 장치 정책을 클릭합니다. 장치 정책 페이지가 나타납니다.
2. 추가를 클릭합니다. 새 정책 추가 대화 상자 나타납니다.
3. 자세히를 확장한 후보안 아래에서 키오스크를 클릭합니다. 키오스크 정책 페이지가 나타납니다.
4. 플랫폼에서 **Android Enterprise** 를 선택합니다. 다른 플랫폼을 지웁니다.
5. 정책 정보 창에서 정책 이름과 필요한 경우 설명을 입력합니다.
6. 다음을 클릭한 후 추가를 클릭합니다.

7. 앱을 화이트리스트에 추가하고 해당 앱에 대한 작업 잠금 모드를 허용 또는 거부하려면:

목록에서 화이트리스트에 추가할 앱을 선택합니다.

사용자가 앱을 시작할 때 장치 화면에 앱이 고정되도록 설정하려면 허용을 선택합니다. 앱이 고정되지 않도록 설정하려면 거부를 선택합니다. 기본값은 허용입니다.



8. 저장을 클릭합니다.

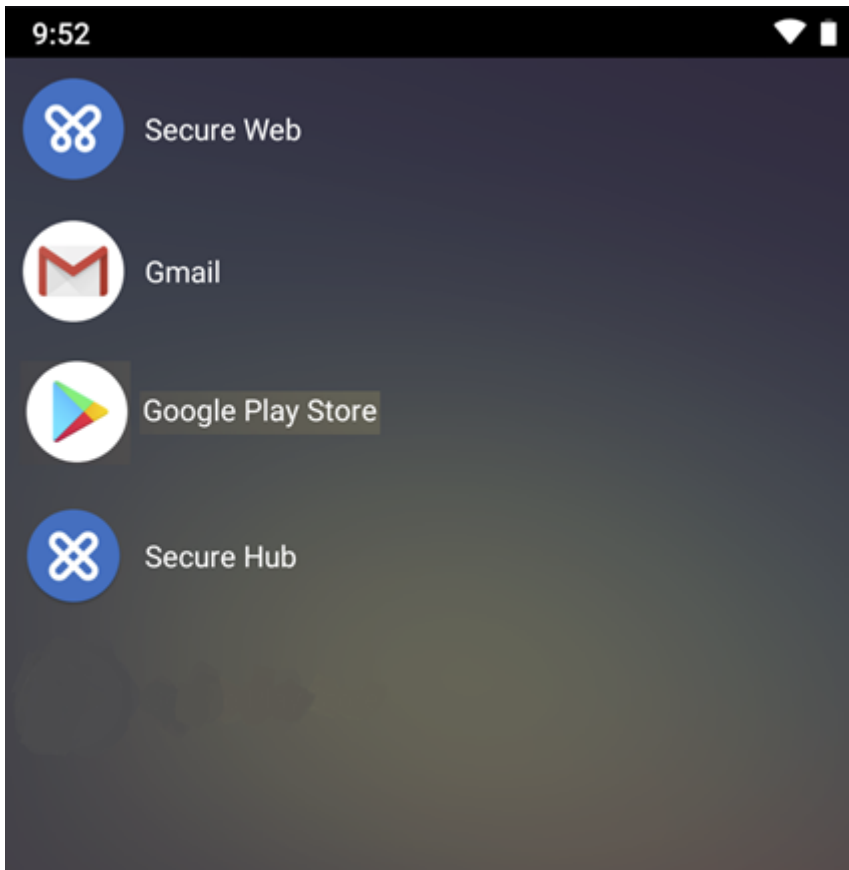
9. 다른 앱을 화이트리스트에 추가하고 해당 앱에 대한 작업 잠금 모드를 허용 또는 거부하려면 추가를 클릭합니다.

10. 배포 규칙을 구성하고 배포 그룹을 선택합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

장치를 등록하려면

1. 새 장치 또는 공장 기본값으로 재설정된 장치의 전원을 켭니다.
2. 장치를 완전 관리되는 장치로 등록하여 전용 장치 RBAC 역할이 있는 사용자에게 할당합니다.

장치가 등록되면 사용자가 실행하고 잠글 수 있는 앱 목록이 화면에 표시됩니다.



이 예제에서는 Gmail 이 장치에 있지만 실행할 수 없음을 보여줍니다.

Android Enterprise 장치 정책 구성

이러한 정책을 사용하여 XenMobile 이 Android Enterprise 를 실행하는 장치와 상호 작용하는 방식을 구성할 수 있습니다. 다음 표에는 Android Enterprise 장치에 사용할 수 있는 모든 장치 정책이 나열되어 있습니다.

중요:

Android Enterprise 에 등록하고 MDX 앱을 사용하는 장치의 경우: MDX 및 Android Enterprise 를 통해 일부 설정을 제어할 수 있습니다. MDX 에 대해 제한이 최소한인 정책 설정을 사용하고 Android Enterprise 를 통해 정책을 제어합니다.

Android Enterprise 관리되는 구성	앱 인벤토리	앱 제거
OS 업데이트 제어	자격 증명	사용자 지정 XML
Exchange	파일 장치 정책	키오스크
위치	암호	제한 사항

Samsung MDM 라이선스키

예약

Wi-Fi

보안동작

Android Enterprise 는다음과같은보안동작을지원합니다. 각보안동작에대한설명은 [보안동작](#)을참조하십시오.

보안동작	Android Enterprise(BYOD)	Android Enterprise(회사소유)
인증서갱신	예	예
전체초기화	아니요	예
찾기	예	예
잠금	예	예
Lock and Reset Password(잠금 및암호재설정)	아니요	예
Notify (Ring)(알림 (벨울림))	예	예
해지	예	예
선택적초기화	예	아니요

참고:

[위치장치정책](#)에서장치에대한위치모드를 높은정확도또는 배터리절약으로설정하지않으면찾기보안동작이실패합니다.

Android 8.0 이전버전의 Android 를 실행하는작업프로필장치에서는잠금및암호재설정명령이지원되지않습니다. Android 8.0 이상을실행하는장치작업프로필장치에서전송된암호는작업프로필을잠그지만장치는잠기지않습니다. 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않고작업프로필에암호가이미설정되지않은경우장치가잠깁니다. 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않지만작업프로필에암호가이미설정되어있는경우에는 작업프로필이잠기지만장치는잠기지않습니다.

Android Enterprise 엔터프라이즈등록취소

Android Enterprise 엔터프라이즈를더이상사용하지않으려면엔터프라이즈등록을취소하면됩니다.

경고:

엔터프라이즈등록이취소되면엔터프라이즈를통해이미등록된장치의 Android Enterprise 앱이기본상태로재설정됩니다. Google 은더이상장치를관리하지않습니다. Android Enterprise 엔터프라이즈에다시등록하는경우추가구성을수

행하지 않으면 이전 기능이 복원되지 않을 수 있습니다.

Android Enterprise 엔터프라이즈 등록 취소 후:

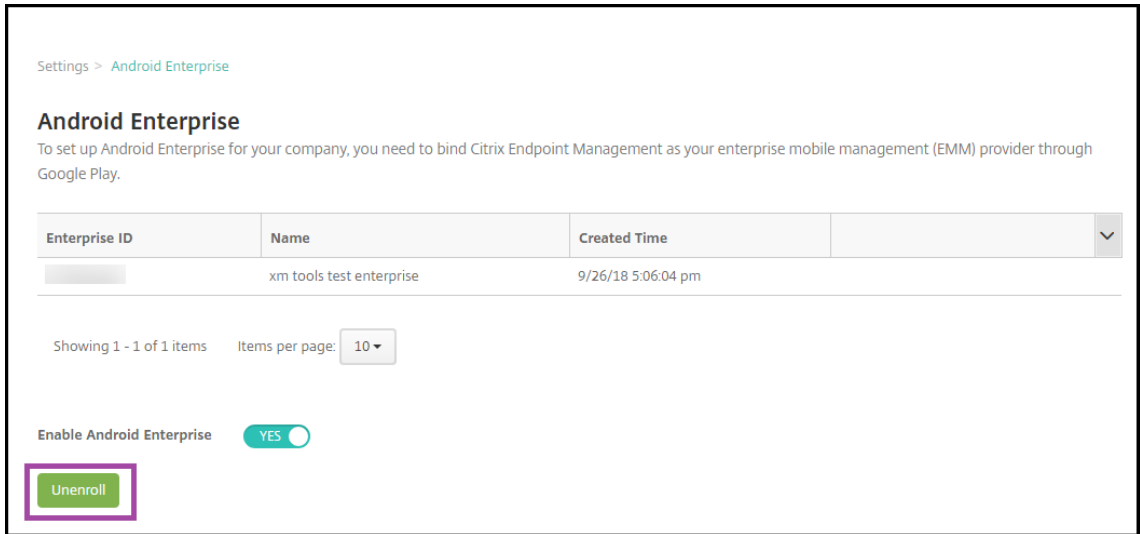
- 엔터프라이즈를 통해 등록된 장치 및 사용자의 Android Enterprise 앱이 기본 상태로 재 설정됩니다. 이전에 적용된 Android Enterprise 관리되는 구성 정책은 더 이상 작업에 영향을 미치지 않습니다.
- XenMobile 은 엔터프라이즈를 통해 등록된 장치를 관리합니다. Google 의 관점에서 이러한 장치는 관리되지 않는 장치입니다. 새로운 Android Enterprise 앱을 추가할 수 없습니다. Android Enterprise 관리되는 구성 정책을 적용할 수 없습니다. 예약, 암호 및 제한 같은 다른 정책을 이러한 장치에 적용할 수 있습니다.
- Android Enterprise 에 장치를 등록하려고 하면 Android Enterprise 장치가 아닌 Android 장치로 등록됩니다.

XenMobile 서버 콘솔 및 XenMobile Tools 를 사용하여 Android Enterprise 엔터프라이즈를 등록 취소합니다.

이 작업을 수행하면 XenMobile 서버에서 XenMobile Tools 에 대한 팝업창이 열립니다. 시작하기 전에 사용하는 브라우저에서 팝업창을 여는 데 필요한 권한이 XenMobile 서버에 있는지 확인하십시오. Google Chrome 같은 일부 브라우저의 경우 팝업 차단 을 사용하지 않도록 설정하고 XenMobile 사이트 주소를 팝업 차단 화이트리스트에 추가해야 합니다.

Android Enterprise 엔터프라이즈를 등록 취소하려면:

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 설정 페이지에서 **Android Enterprise** 를 클릭합니다.
3. 등록 취소를 클릭합니다.



G Suite 고객을 위한 레거시 Android Enterprise

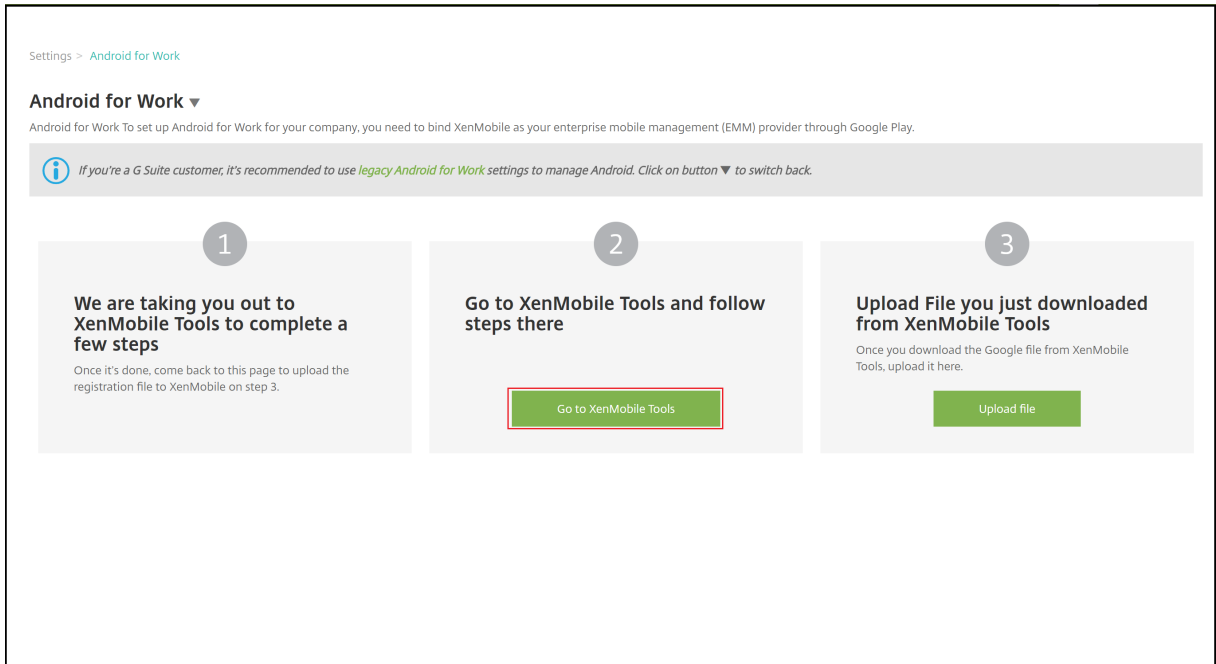
January 6, 2020

G Suite 고객은 레거시 Android Enterprise 설정을 사용하여 레거시 Android Enterprise 를 구성해야 합니다.

레거시 Android Enterprise 요구 사항:

- 공개적으로 액세스할 수 있는 도메인
- Google 관리자 계정
- 관리되는 프로필을 지원하고 Android 5.0 Lollipop 이상을 실행 중인 장치
- Google Play 가 설치된 Google 계정
- 장치에 설정된 작업 프로필

레거시 Android Enterprise 를 구성하려면 XenMobile 설정의 **Android Enterprise** 페이지에서 레거시 **Android Enterprise** 를 클릭합니다.



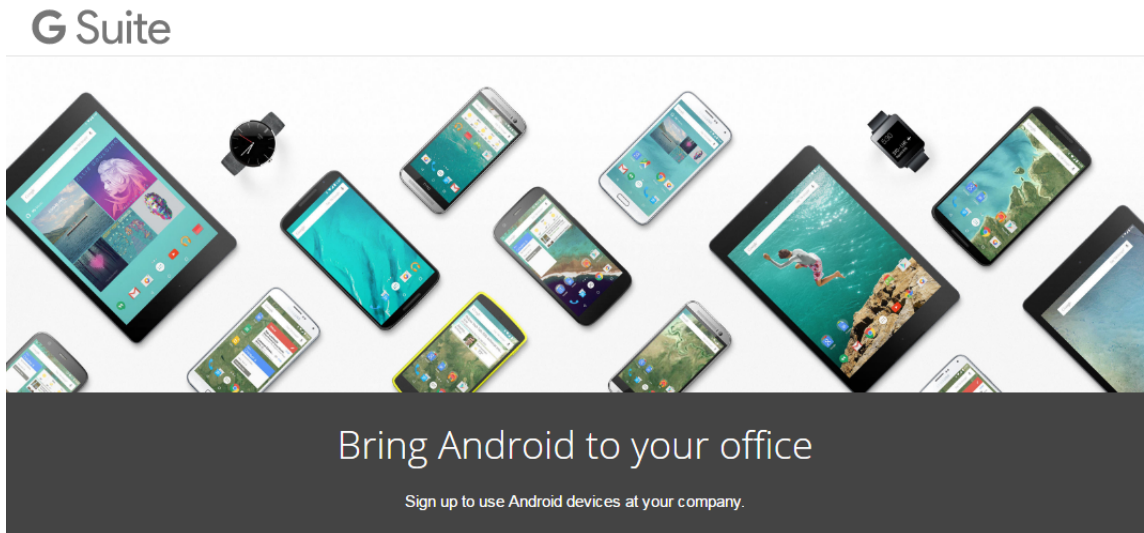
Android Enterprise 계정만들기

Android Enterprise 계정을 설정하려면 먼저 Google 에서도메인 이름을 확인해야 합니다.

Google 을 사용하여도메인 이름이 이미 확인한 경우 Android Enterprise 서비스 계정 설정 및 Android Enterprise 인증서 다운로드 단계로 건너뛸 수 있습니다.

1. https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK 로 이동합니다.

관리자 및 회사 정보를 입력하는 다음과 같은 페이지가 표시됩니다.



① About you

Name

First Name Last Name

Current work email

Doesn't have to be an official business email.

e.g. john@mydomain.com

Phone

+1

2. 관리자사용자정보를입력합니다.

① About you

Name

Justa User

Current work email

justa.user@gmail.com

Phone

+15551234567

3. 관리자계정정보와더불어회사정보를입력합니다.

② About your business

Business name
EXAMPLE CORP ✓

Business domain address You'll need to verify that you own this domain.
example.com ✓

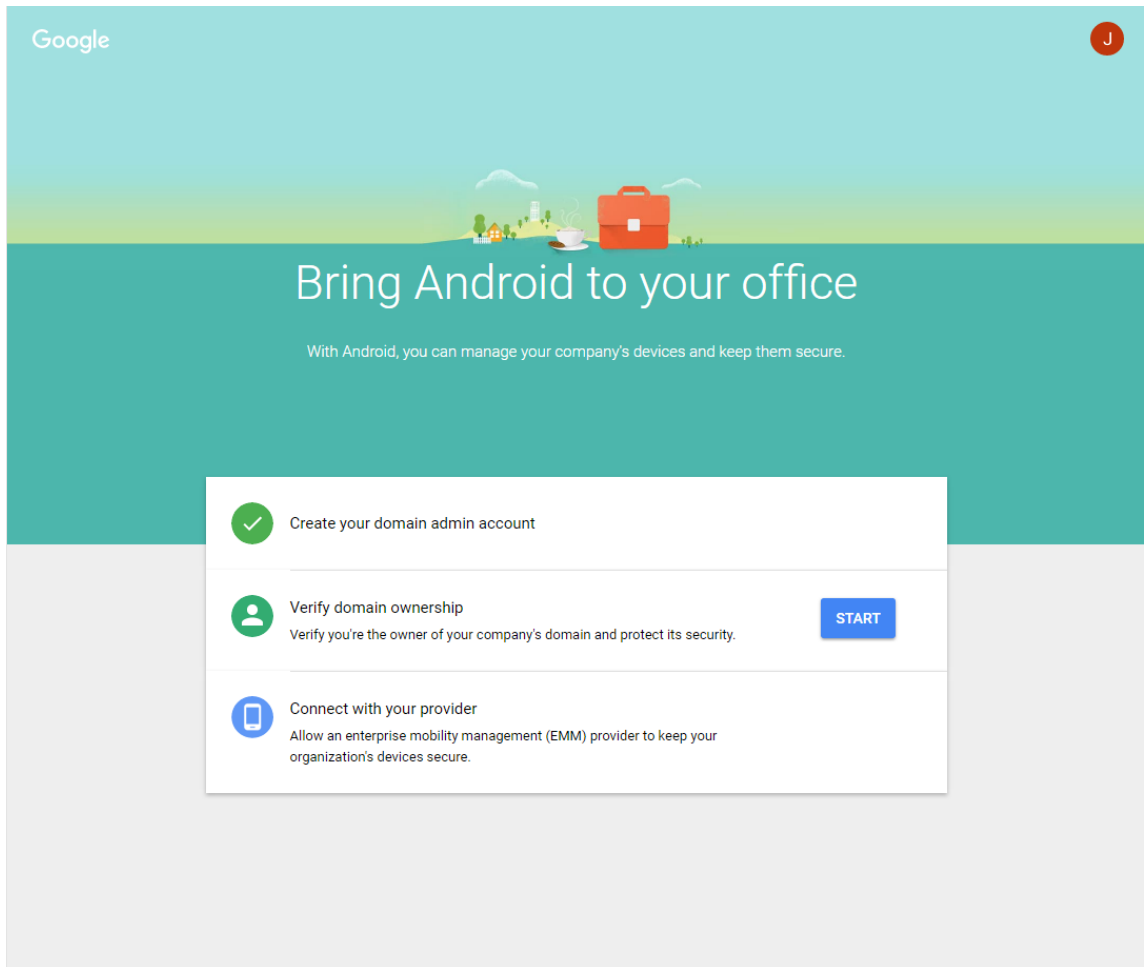
Number of employees: 1 employee ▾
Country/Region: United States ▾

③ Your Google admin account Why do I need this?

Username Create an account to manage Android for Work
justa.user ✓ @ example.com

Create a password 8-character minimum; case sensitive
..... ✓
..... ✓

프로세스의 첫 번째 단계를 완료되면 다음 페이지가 표시됩니다.



도메인소유권확인


다음방법중하나를사용하여 Google 이도메인을확인할수있게만듭니다.

- TXT 또는 CNAME 레코드를도메인호스트의웹사이트에추가합니다.
- 도메인의웹서버에 HTML 파일을업로드합니다.
- 홈페이지에 <meta> 태그를추가합니다. 첫번째방법을사용하는것이 좋습니다. 이문서에서는도메인소유권을확인하는단계를다루지않습니다. 필요한정보는 <https://support.google.com/a/answer/6248925>에서찾을수있습니다.

1. **Start(시작)** 를클릭하여도메인확인을시작합니다.

Verify domain ownership(도메인소유권확인) 페이지가나타납니다. 페이지의지침에따라도메인을확인합니다.

2. **Verify(확인)** 를클릭합니다.




Verify domain ownership


Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)

After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

Note: Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

 Need help? Search the [Help Center](#) or call **844-390-7627** and provide your unique PIN **12345678**



Verify domain ownership

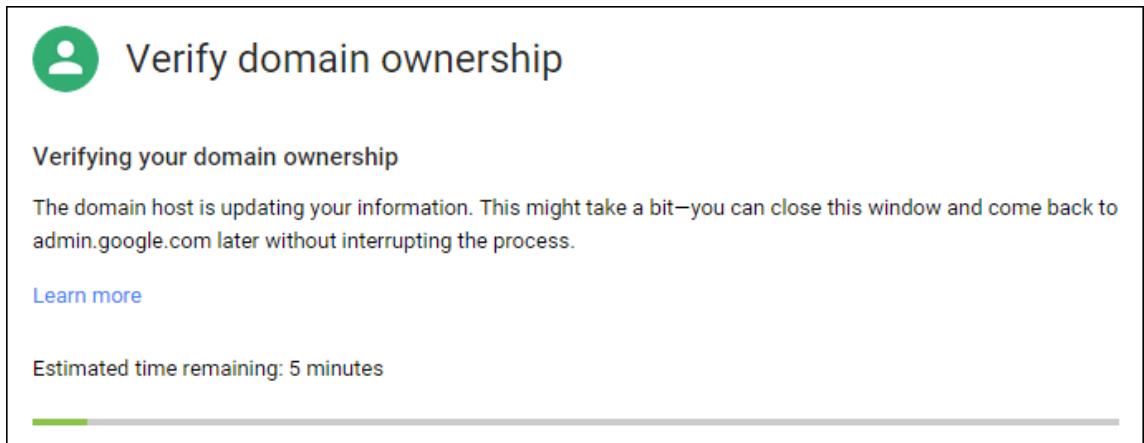
Verification checklist

Follow these steps to help Google verify that you own the domain **example.com**.

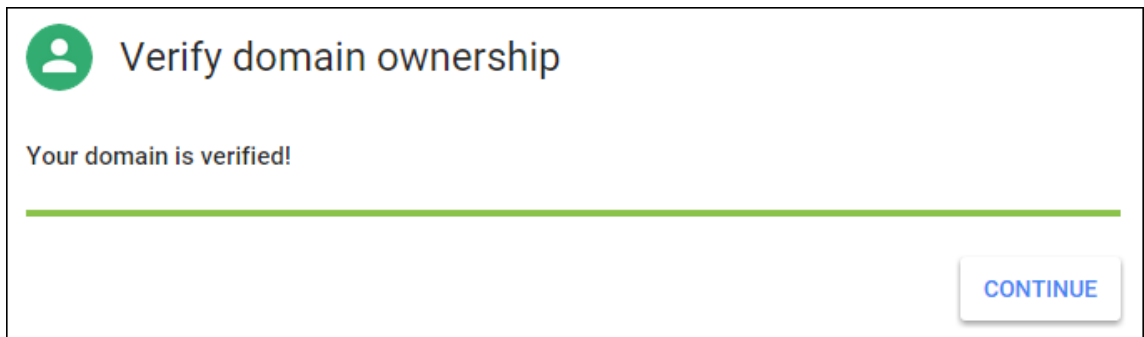
[Learn more](#)

- I have successfully logged in.
- I have opened the control panel for my domain.
- I have created the CNAME record.
- I have saved the CNAME record.

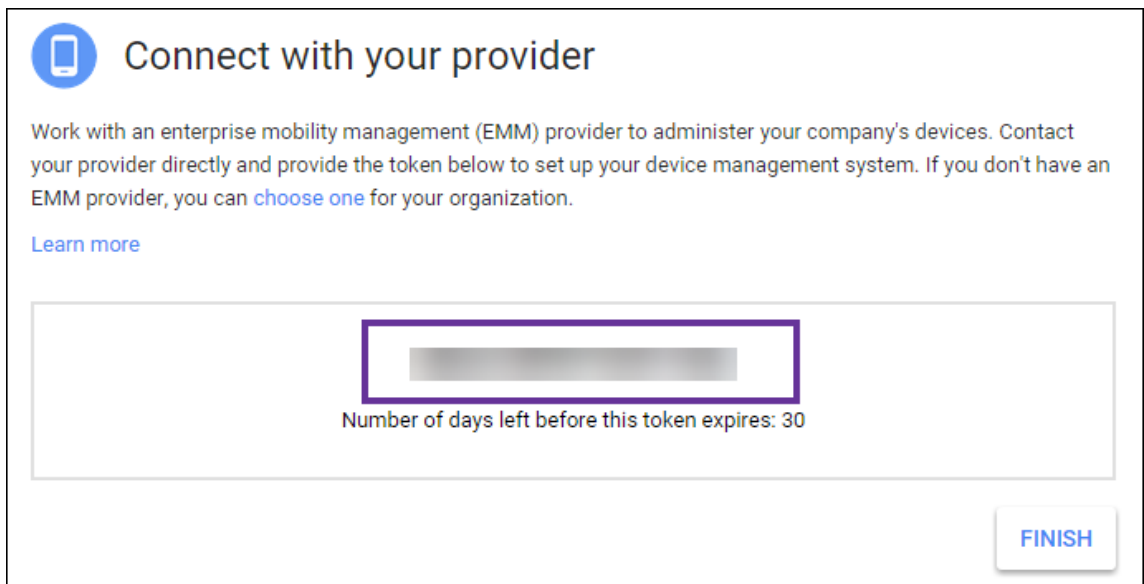
3. Google 이도메인소유권을확인합니다.



4. 확인이 성공하면 다음 페이지가 나타납니다. **Continue**(계속) 를 클릭합니다.



5. Citrix 에 제공하고 Android Enterprise 설정을 구성할 때 사용하는 EMM 바인딩 토큰이 만들어집니다. 토큰을 복사하여 저장합니다. 나중에 설정 절차에서 이 토큰이 필요합니다.



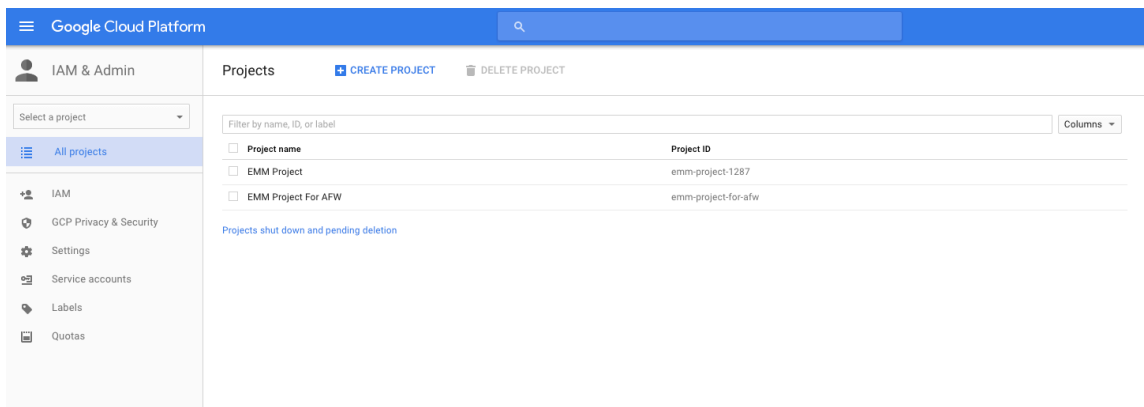
6. **Finish**(마침) 를 클릭하여 Android Enterprise 설정을 완료합니다. 도메인을 확인했음을 나타내는 페이지가 나타납니다.

Android Enterprise 서비스 계정을 만든 후 Google 관리 콘솔에 로그인하여 모바일 관리 설정을 관리할 수 있습니다.

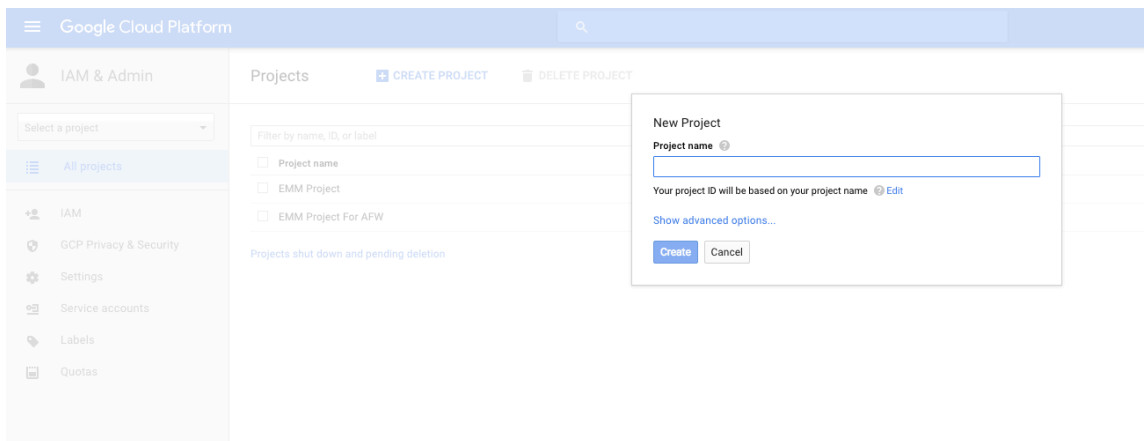
Android Enterprise 서비스계정설정및 Android Enterprise 인증서다운로드

XenMobile 이 Google Play 및 디렉터리 서비스에 액세스할 수 있게 하려면 개발자를 위한 Google 프로젝트 포털을 사용하여 서비스 계정을 만들어야 합니다. 이 서비스 계정은 XenMobile 과 Android 용 Google 서비스 사이의 서버 간 통신에 사용됩니다. 사용되는 인증 프로토콜에 대한 자세한 내용은 <https://developers.google.com/identity/protocols/OAuth2ServiceAccount> 를 참조하십시오.

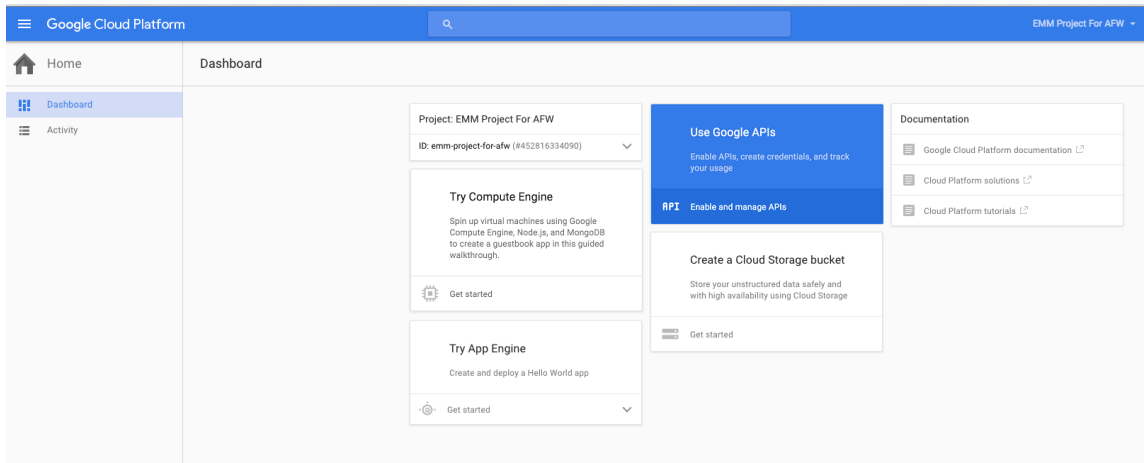
1. 웹 브라우저에서 <https://console.cloud.google.com/project> 로 이동하여 Google 관리자 자격 증명으로 로그인합니다.
2. **Projects(프로젝트)** 목록에서 **Create Project(프로젝트 만들기)** 를 클릭합니다.



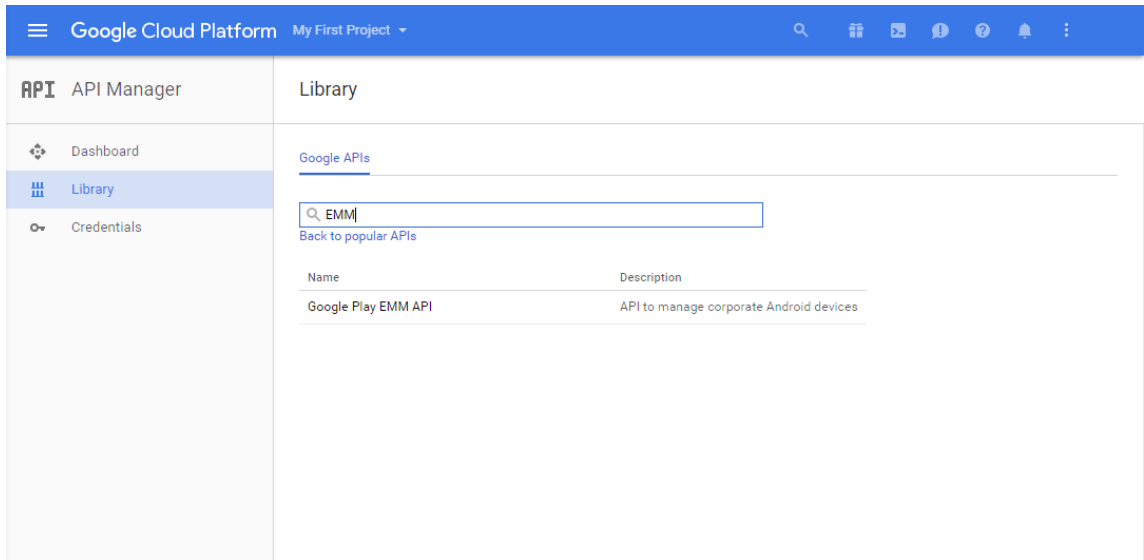
3. **Project name(프로젝트 이름)** 에 프로젝트 이름을 입력합니다.



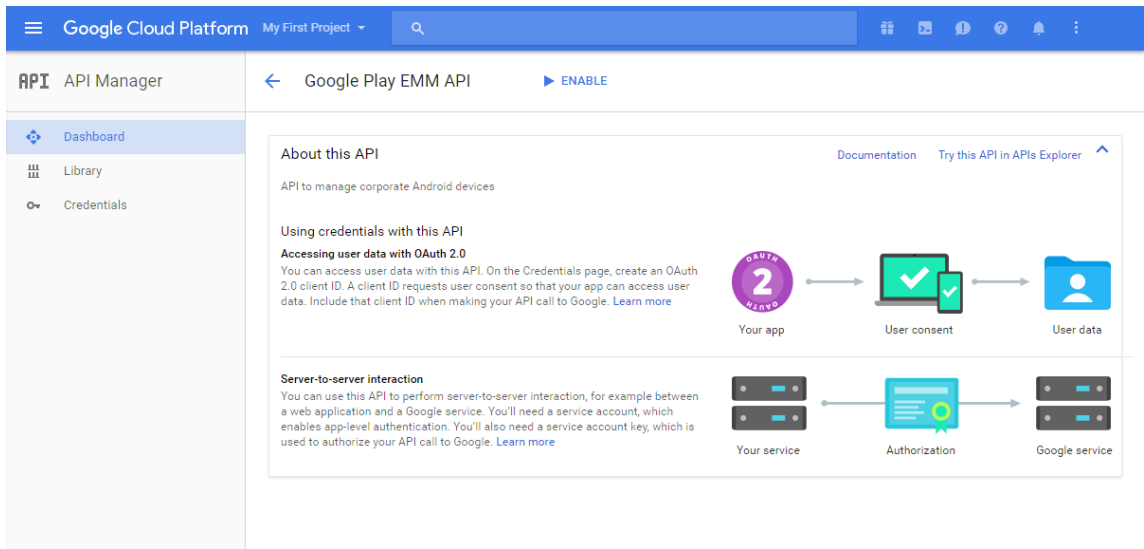
4. 대시보드에서 **Use Google APIs(Google API 사용)** 를 클릭합니다.



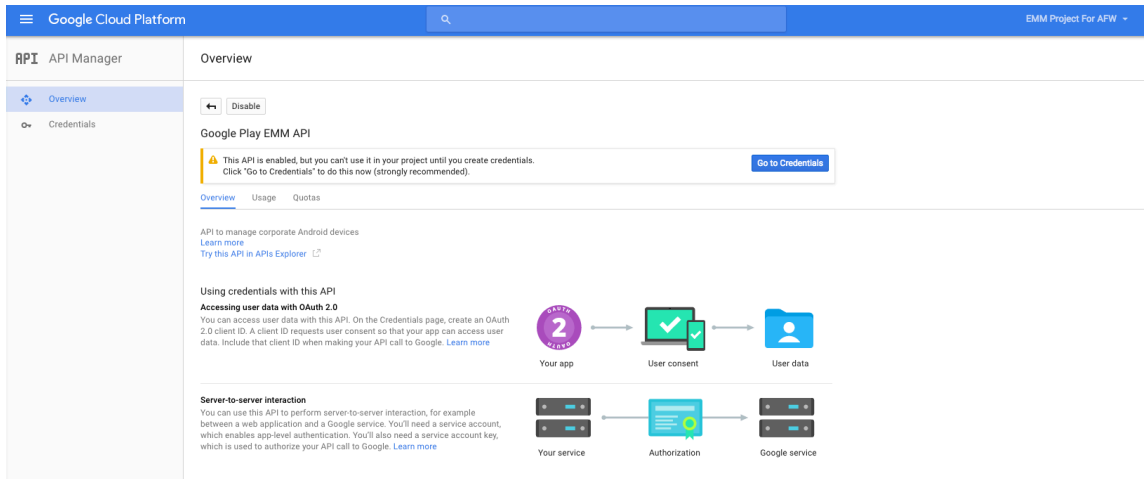
5. **Library**(라이브러리) 를 클릭하고 **Search**(검색) 에 **EMM** 을 입력한다음 검색결과를 클릭합니다.



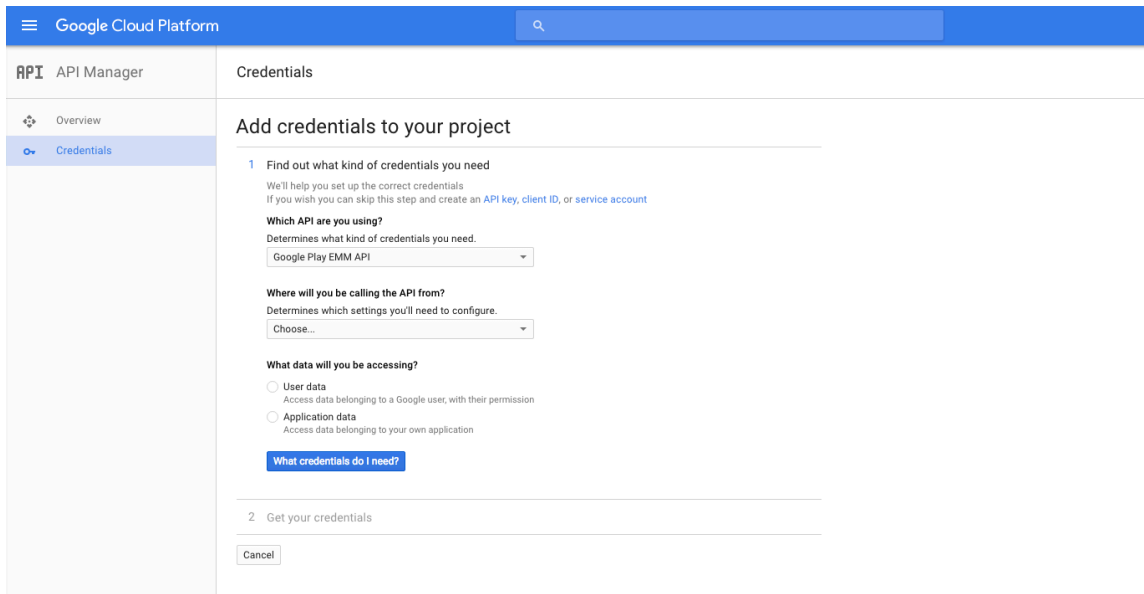
6. **Overview**(개요) 페이지에서 **Enable**(사용) 을 클릭합니다.



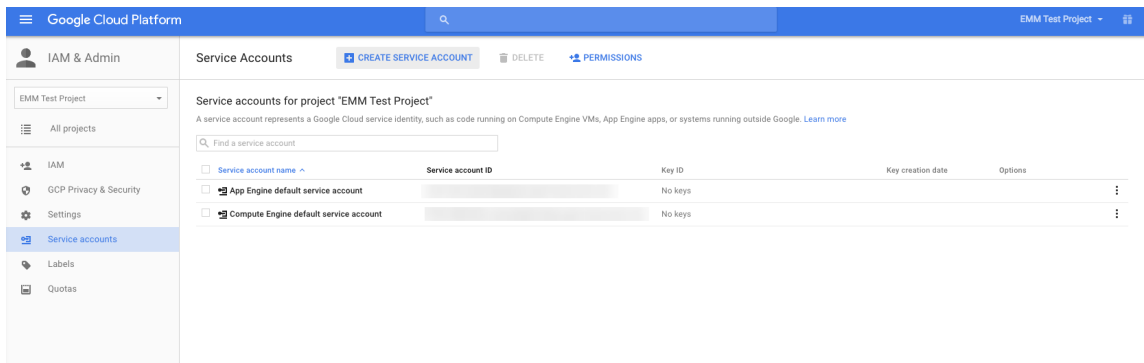
7. **Google Play EMM API** 옆에서 **Go to Credentials(자격증명으로이동)** 를클릭합니다.



8. **Add credentials to our project(프로젝트에자격증명추가)** 목록의 1 단계에서 **service account(서비스계정)** 를클릭합니다.



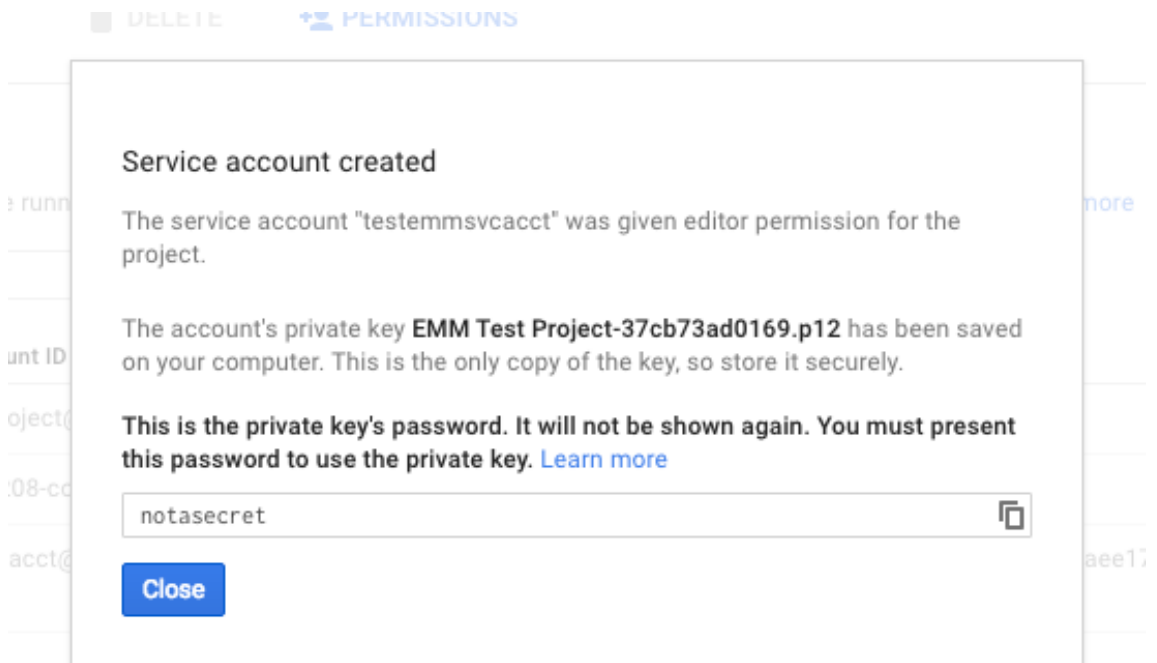
9. **Service Accounts(서비스계정) 페이지에서 Create Service Account(서비스계정만들기) 를 클릭합니다.**



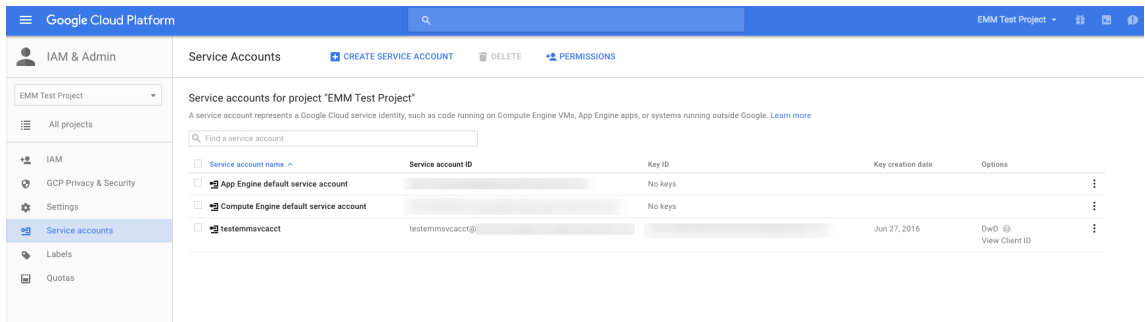
10. **Create service account(서비스계정만들기) 에서계정이름을지정하고 Furnish a new private key(새개인 키준비) 확인란을선택합니다. P12 를 클릭하고 Enable Google Apps Domain-wide Delegation(Google Apps 도메인전체위임사용) 확인란을선택한후 Create(만들기) 를 클릭합니다.**

인증서 (P12 파일) 가컴퓨터에다운로드됩니다. 인증서를안전한위치에저장합니다.

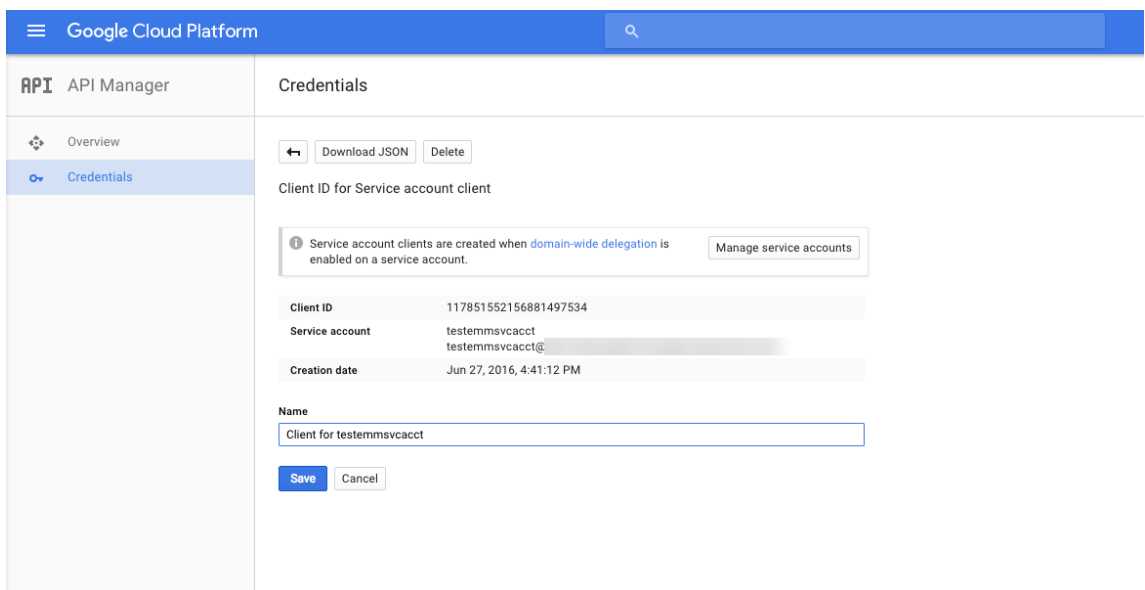
11. **Service account created**(서비스계정만들어짐) 확인페이지에서 **Close**(닫기) 를클릭합니다.



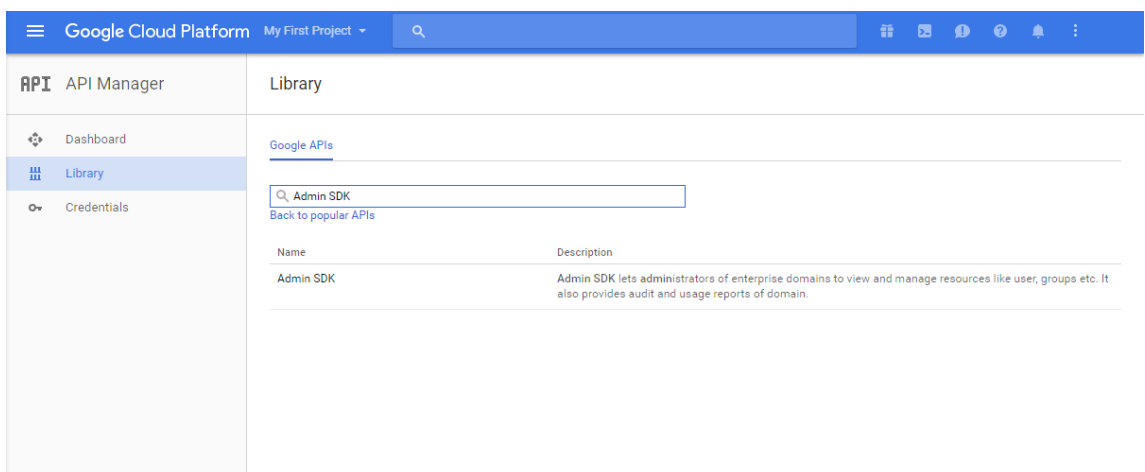
12. **Permissions**(권한) 에서 **Service accounts**(서비스계정) 를클릭한다음서비스계정의 **Options**(옵션) 에서 **View Client ID**(클라이언트 ID 보기) 를클릭합니다.



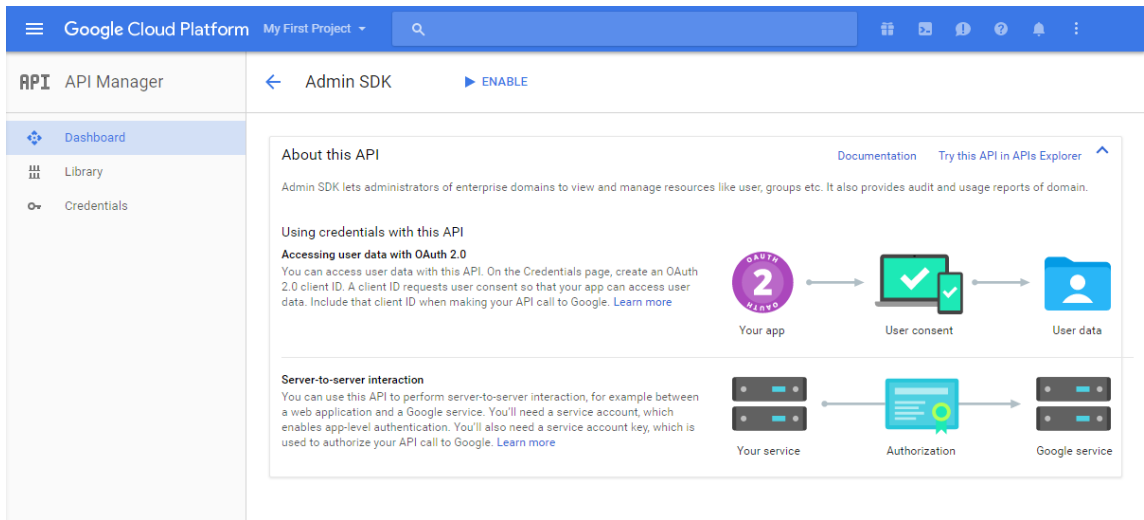
13. Google 관리콘솔의계정승인에필요한세부정보가표시됩니다. **Client ID(클라이언트 ID)** 및 **Service account ID(서비스계정 ID)** 를나중에정보를검색할수있는위치에복사합니다. 허용목록에등록하기위해 Citrix 지원에도메인이름을보낼때이정보가필요합니다.



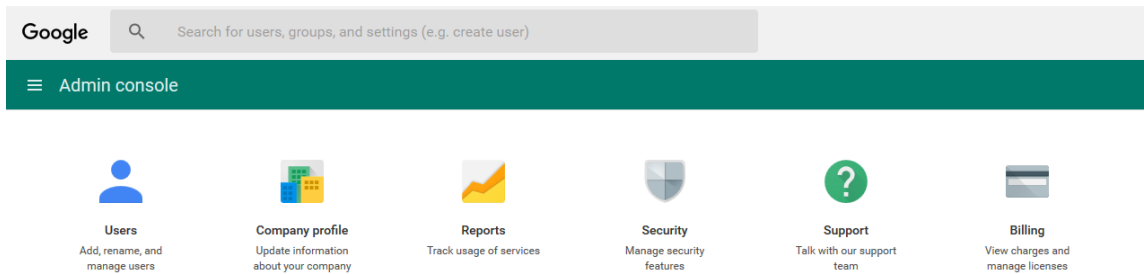
14. **Library(라이브러리)** 페이지에서 **Admin SDK** 를검색한다음검색결과를클릭합니다.



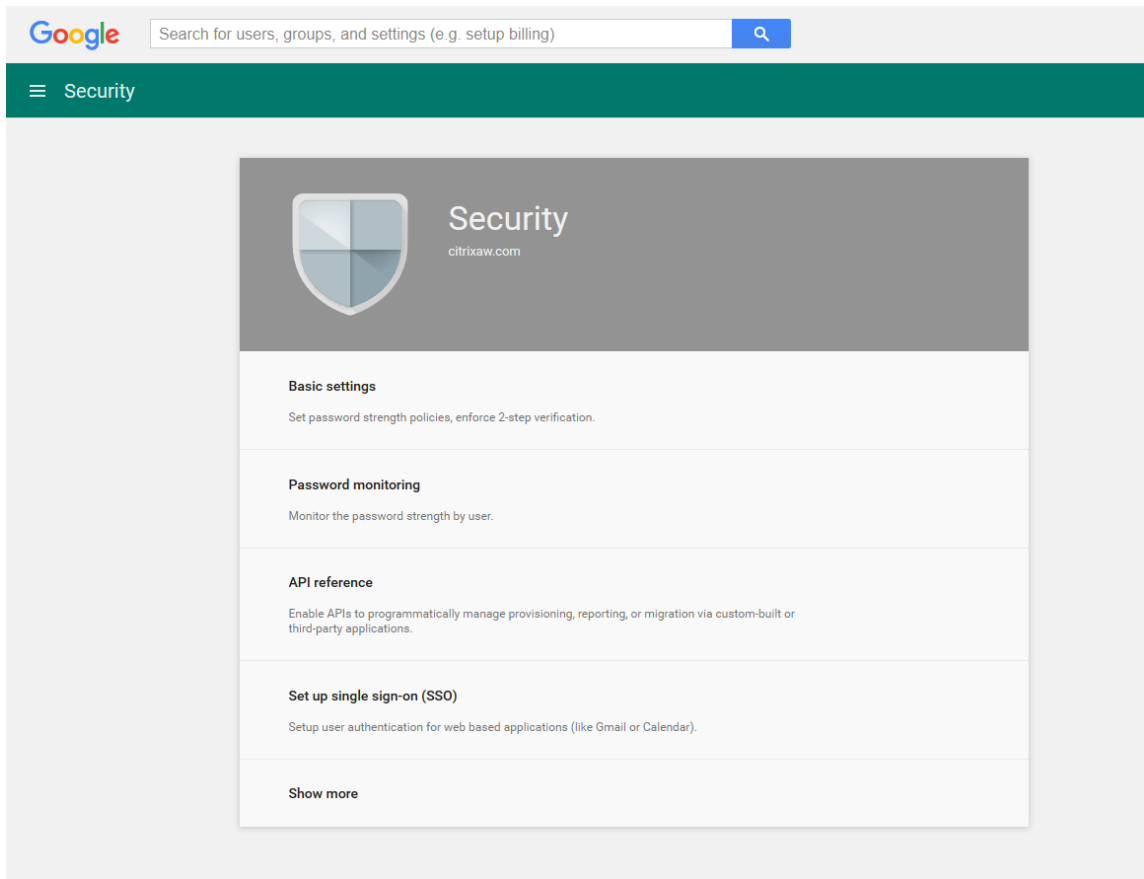
15. **Overview(개요)** 페이지에서 **Enable(사용)** 을클릭합니다.

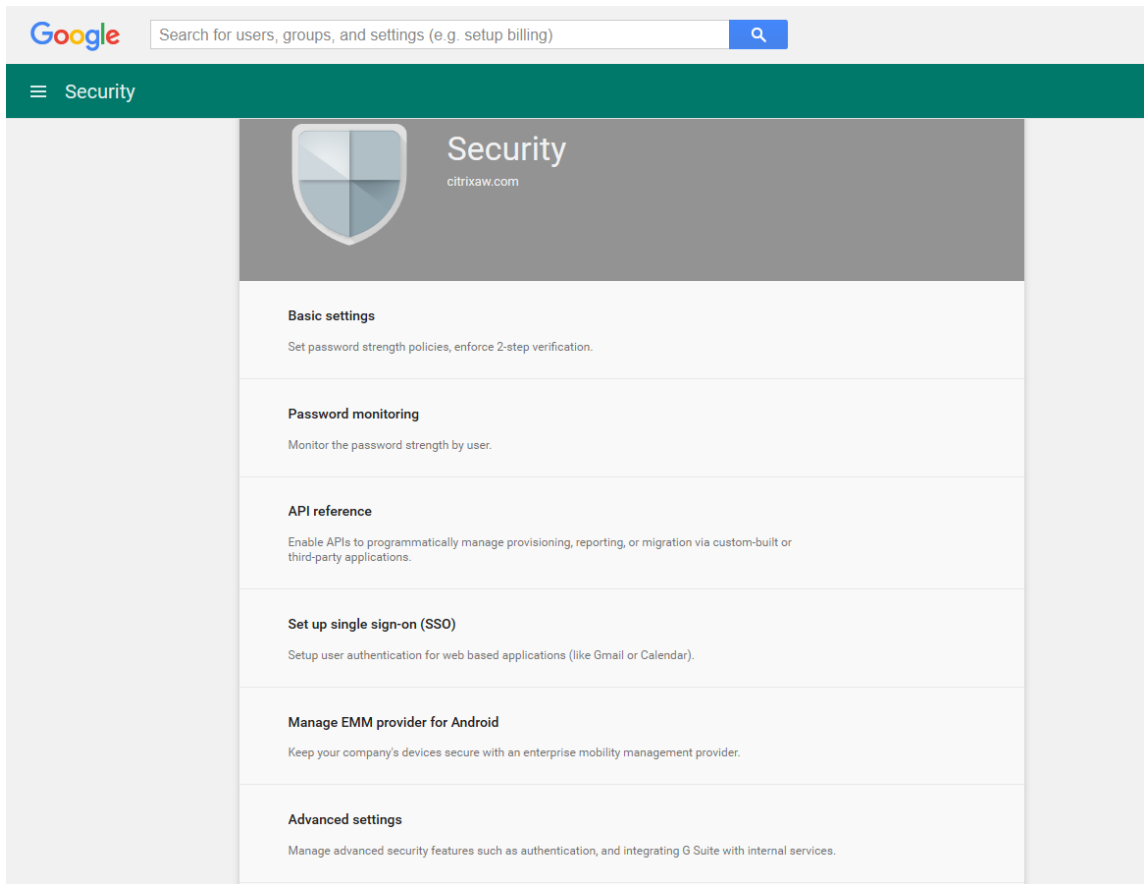


16. 도메인에대한 Google 관리콘솔을연다음 **Security(보안)** 를클릭합니다.

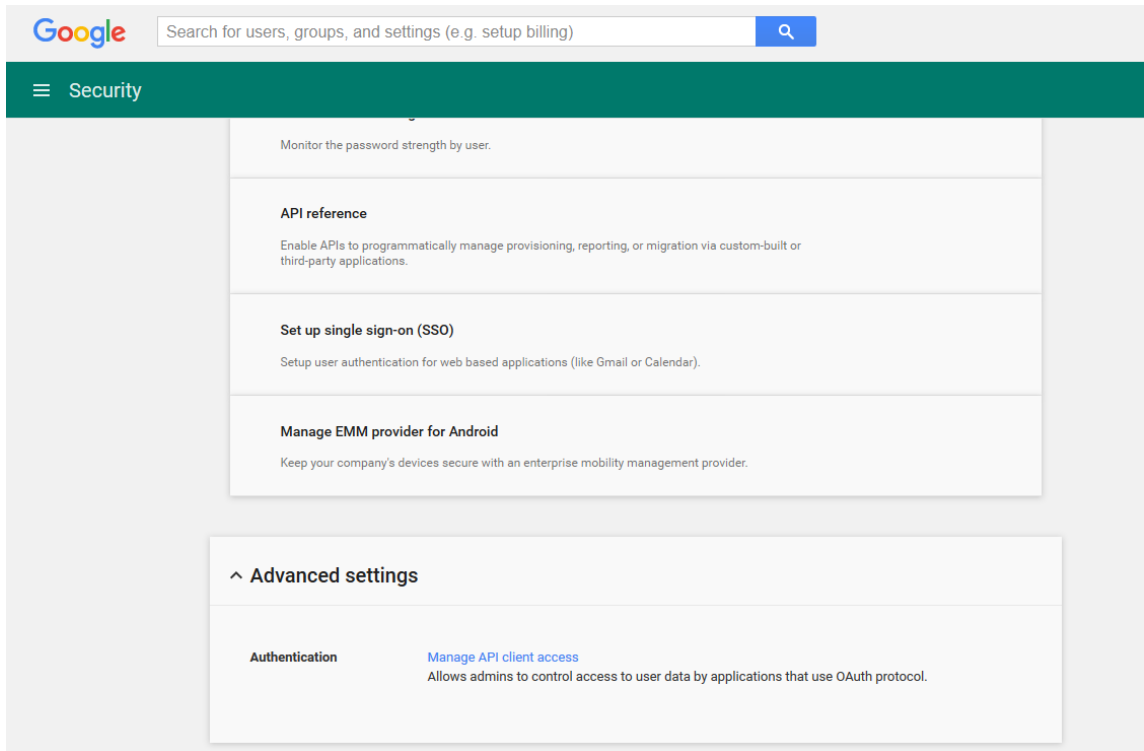


17. **Settings(설정)** 페이지에서 **Show more(자세히표시)** 를클릭한다음 **Advanced settings(고급설정)** 를클릭합니다.

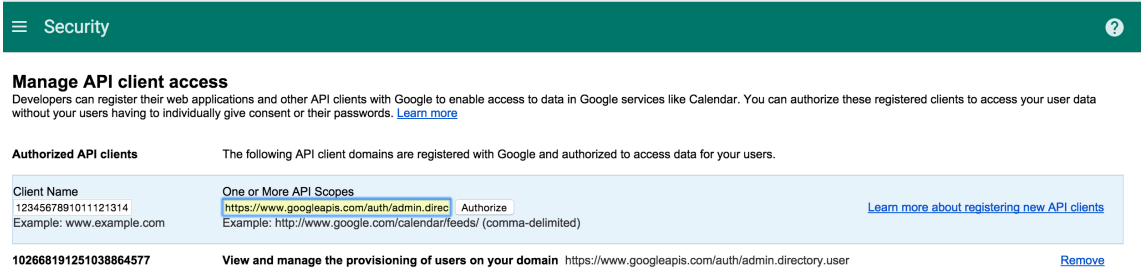




18. **Manage API client access(API 클라이언트액세스관리)** 를 클릭합니다.



- Client Name**(클라이언트이름) 에앞서저장한클라이언트 ID 를입력하고, **One or More API Scopes**(하나이상의 **API 범위**) 에 <https://www.googleapis.com/auth/admin.directory.user>를입력한다음 **Authorize**(승인) 를클릭합니다.



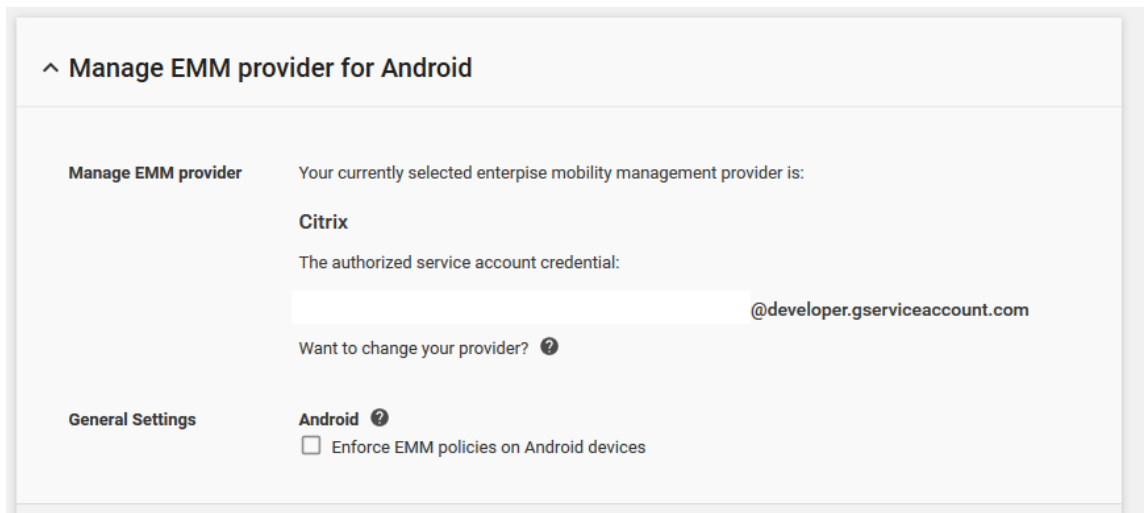
EMM 바인딩

XenMobile 을사용하여 Android 장치를관리하려면먼저 Citrix 기술지원팀에연락하여도메인이름, 서비스계정및바인딩토큰을제공해야합니다. Citrix 는해당토큰을사용자의 EMM(엔터프라이즈모빌리티관리) 공급자로 XenMobile 에바인딩합니다. Citrix 기술지원의연락처정보는 [Citrix Technical Support\(Citrix 기술지원\)](#)를참조하십시오.

- 바인딩을확인하려면 Google Admin 포털에로그인한다음 **Security**(보안) 를클릭합니다.
- Manage EMM provider for Android(Android 용 EMM 공급자관리)** 를클릭합니다.

Google Android Enterprise 계정이 EMM 공급자로 Citrix 에바인딩되었음을확인할수있습니다.

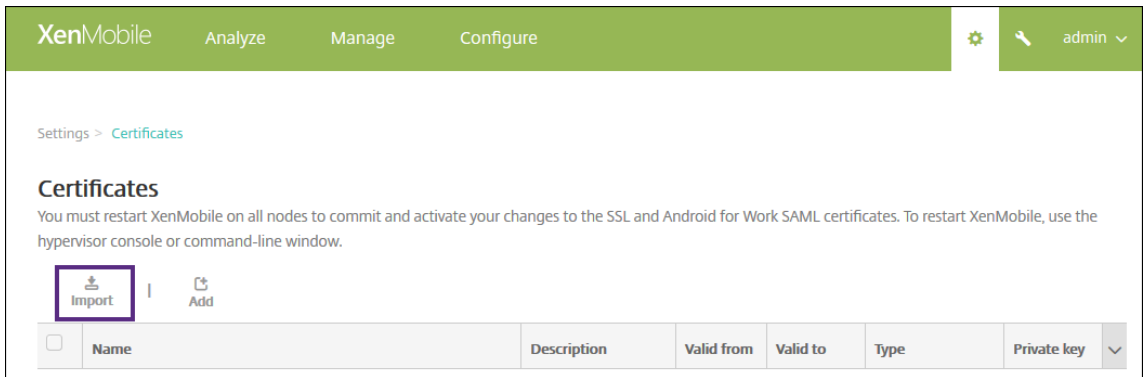
토큰바인딩을확인한후 XenMobile 콘솔을사용하여 Android 장치를관리할수있습니다. 14 단계에서생성한 P12 인증서를가져옵니다. Android Enterprise 서버설정을지정하고, SAML 기반 SSO(Single Sign On) 를사용하도록설정하고, Android Enterprise 장치정책을하나이상정의합니다.



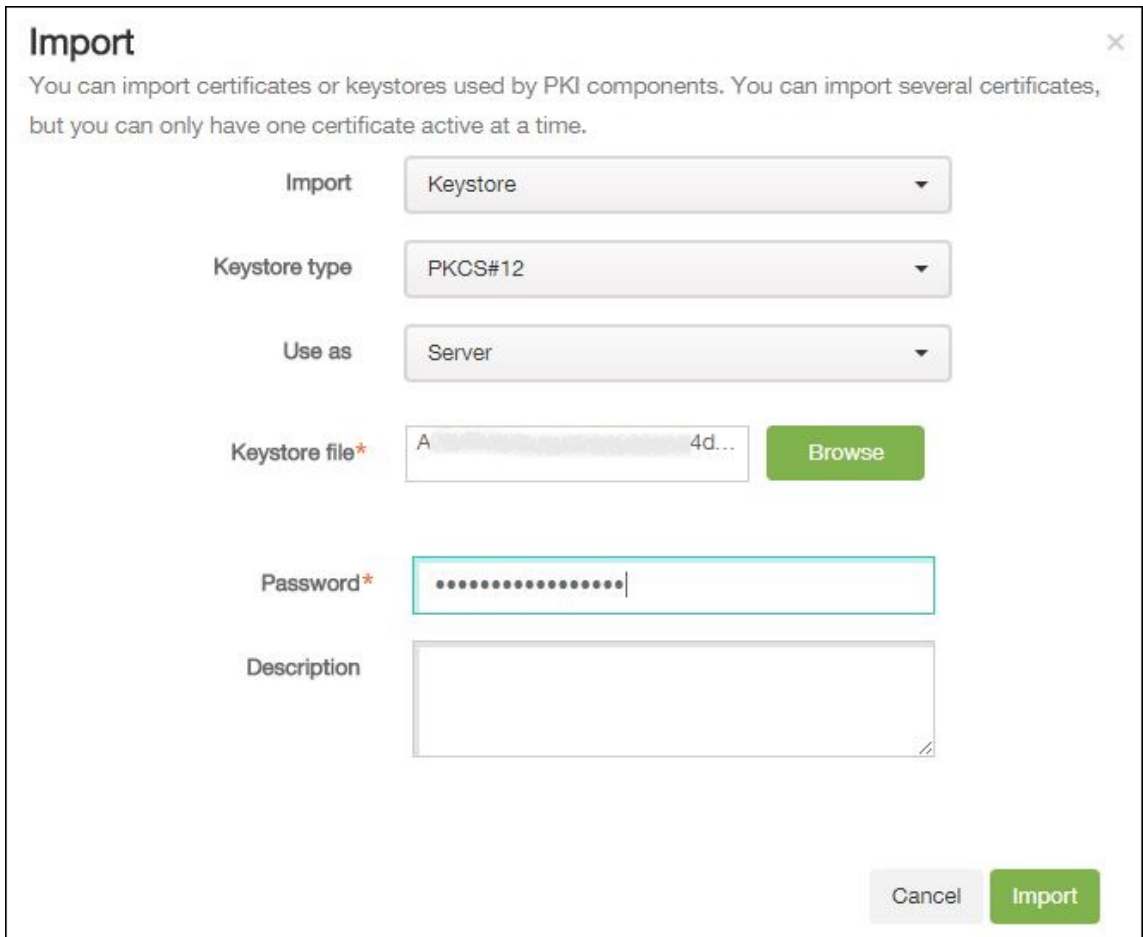
P12 인증서가져오기

Android Enterprise P12 인증서를가져오려면다음단계를따르십시오.

1. XenMobile 콘솔에로그인합니다.
2. 콘솔의오른쪽맨위에있는기어아이콘을클릭하여 설정페이지를연다음 인증서를클릭합니다. 인증서페이지가나타납니다.



3. 가져오기를클릭합니다. 가져오기대화상자가나타납니다.



다음설정을구성합니다.

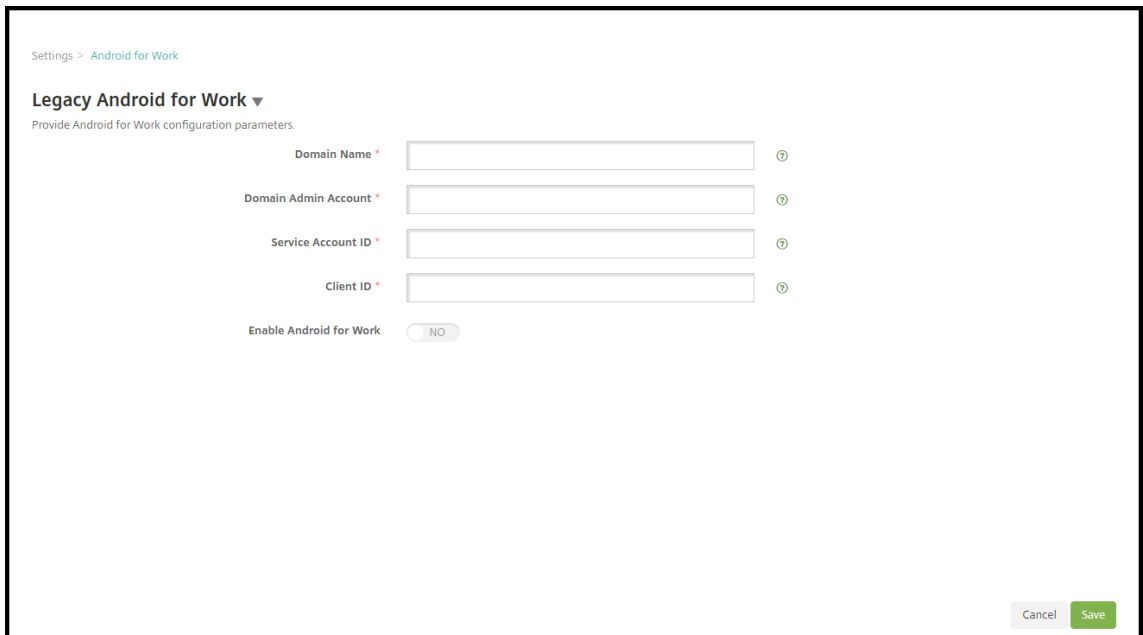
- 가져오기: 목록에서 키저장소를클릭합니다.
- 키저장소유형: 목록에서 **PKCS#12** 를클릭합니다.
- 용도: 목록에서 서버를클릭합니다.

- 키저장소파일: 찾아보기를클릭하고 P12 인증서를찾아선택합니다.
- 암호: 키저장소암호를입력합니다.
- 설명: 인증서에대한선택적설명을입력합니다.

4. 가져오기를클릭합니다.

Android Enterprise 서버설정

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버아래에서 **Android Enterprise** 를클릭합니다. **Android Enterprise** 페이지가나타납니다.



Settings > Android for Work

Legacy Android for Work ▾

Provide Android for Work configuration parameters.

Domain Name * ⓘ

Domain Admin Account * ⓘ

Service Account ID * ⓘ

Client ID * ⓘ

Enable Android for Work NO

Cancel Save

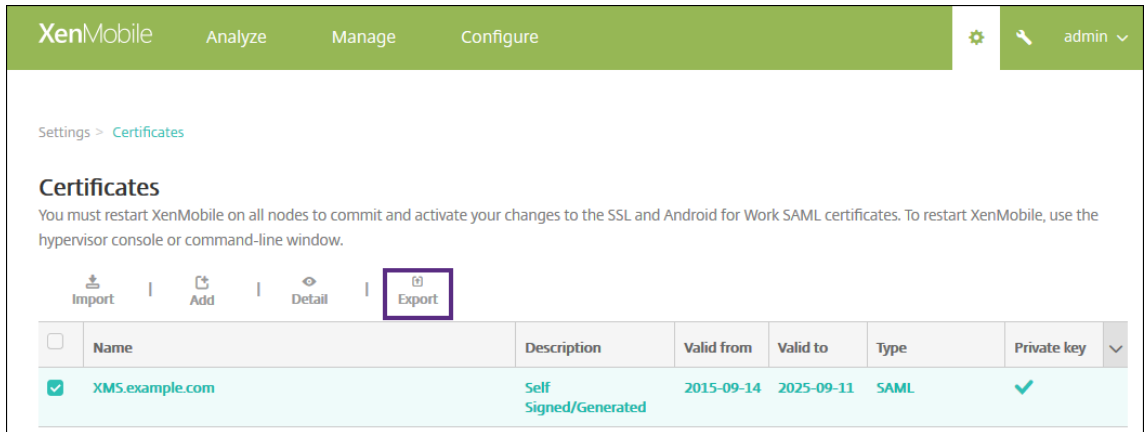
다음설정을구성한후 저장을클릭합니다.

- 도메인이름: Android Enterprise 도메인이름을입력합니다 (예: domain.com).
- 도메인관리자계정: 도메인관리자사용자이름을입력합니다 (예: Google 개발자포털에서사용되는전자메일계정).
- 서비스 계정 ID: 서비스 계정 ID 를 입력 합니다. 예를 들어 Google 서비스 계정에 연결된 전자 메일 (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com) 을입력합니다.
- 클라이언트 ID: Google 서비스계정의클라이언트 ID(숫자) 를입력합니다.
- **Android Enterprise** 사용: Android Enterprise 를사용하거나사용하지않도록선택합니다.

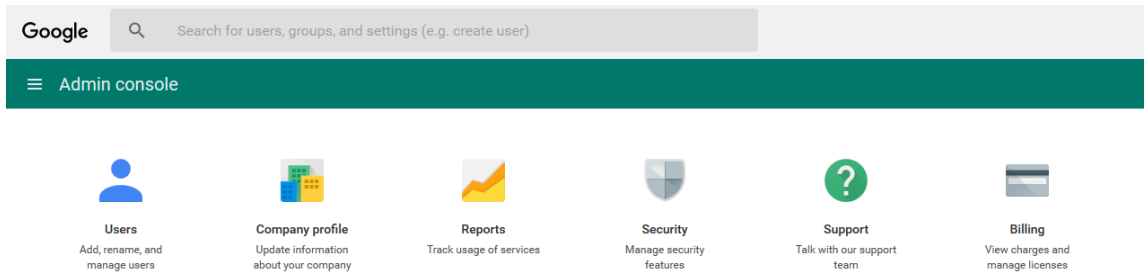
SAML 기반 SSO(Single Sign On) 사용

1. XenMobile 콘솔에로그인합니다.
2. 콘솔오른쪽위모서리에서기어아이콘을클릭합니다. 설정페이지가나타납니다.

3. 인증서를클릭합니다. 인증서페이지가나타납니다.



4. 인증서목록에서 SAML 인증서를클릭합니다.
5. 내보내기를클릭하고인증서를컴퓨터에저장합니다.
6. Android Enterprise 관리자자격증명을사용하여 Google Admin 포털에로그인합니다. 포털액세스에대한자세한내용은 [Google Admin 포털](#)을참조하십시오.
7. **Security(보안)** 를클릭합니다.



8. **Security(보안)** 아래에서 **Set up single sign-on (SSO)(SSO(Single Sign-On) 설정)** 을클릭한후다음과같은설정을구성합니다.

^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL	https://example.com/aw/saml/signin
	<small>URL for signing in to your system and Google Apps</small>
Sign-out page URL	https://example.com/aw/saml/signout
	<small>URL for redirecting users to when they sign out</small>
Change password URL	https://example.com/aw/saml/changepassword
	<small>URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled</small>
Verification certificate	<div style="display: flex; gap: 5px;"> CHOOSE FILE UPLOAD </div>
	<small>The certificate file must contain the public key for Google to verify sign-in requests. ?</small>

Use a domain specific issuer ?

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

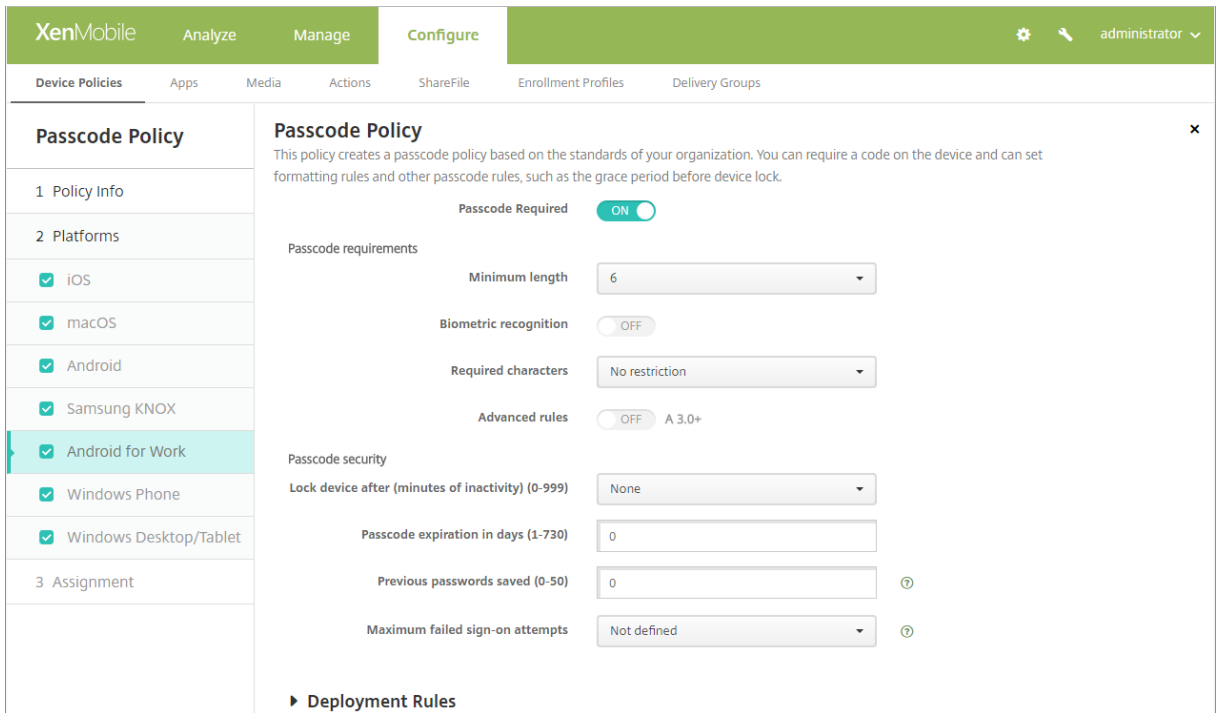
DISCARD CHANGES SAVE CHANGES

- **Sign-in page URL(로그인페이지 URL):** 사용자가시스템및 Google Apps 에로그인할수있는 URL 을입력합니다. 예: <https://<Xenmobile-FQDN>/aw/saml/signin>.
- **Sign out page URL(로그아웃페이지 URL):** 사용자가로그아웃한경우리디렉션되는 URL 을입력합니다. 예: <https://<Xenmobile-FQDN>/aw/saml/signout>.
- **Change password URL(암호변경 URL):** 사용자가시스템의암호를변경할수있는 URL 을입력합니다. 예: <https://<Xenmobile-FQDN>/aw/saml/changepassword>. 이필드가정의되어있으면 SSO 를사용할수없는경우에도이메시지가표시됩니다.
- **Verification certificate(확인인증서):** **CHOOSE FILE(파일선택)** 을클릭한다음 XenMobile 에서내보낸 SAML 인증서를찾아선택합니다.

9. **SAVE CHANGES(변경내용저장)** 를클릭합니다.

Android Enterprise 장치정책설정

사용자가처음등록할때장치에대한암호를설정해야하도록암호정책을설정하십시오.



모든장치정책을설정하는기본단계는다음과같습니다.

1. XenMobile 콘솔에로그온합니다.
2. 구성을클릭한다음 장치정책을클릭합니다.
3. 추가를클릭한다음 새정책추가대화상자에서추가하려는정책을선택합니다. 이예제에서는 암호를클릭합니다.
4. 정책정보페이지를완성합니다.
5. **Android Enterprise** 를클릭한다음정책에대한설정을구성합니다.
6. 배달그룹에정책을할당합니다.

지원되는장치정책및 **MDX** 정책

다음표에는 Android Enterprise 컨테이너가지원하는장치정책과 MDX 정책이나와있습니다. 장치정책및 MDX 정책에대한 자세한내용은각각 [장치정책](#) 및 [MDX 정책요약](#)을참조하십시오.

인증정책	지원됨	지원되는값	참고
앱암호	X	모두	
온라인세션필요		꺼짐만	
최대오프라인기간	X	모두	
대체 NetScaler Gateway		공백만	

앱네트워크액세스정책	지원됨	지원되는값	참고
네트워크액세스	X	모두	
인증서레이블		공백만	
기본설정 VPN 모드	X	모두	
VPN 모드전환허용	X	모두	
PAC 파일 URL 또는프록시 서버	X	모두	
기본로그출력	X	모두	
기본로그수준	X	모두	
최대로그파일	X	모두	
최대로그파일크기	X	모두	
앱로그리디렉션	X	모두	
로그암호화	X	모두	
허용된 WiFi 네트워크		공백만	

장치보안정책	지원됨	지원되는값	참고
탈옥또는루팅차단	X	모두	
장치암호화필요	X	모두	
장치잠금필요	X	모두	

네트워크요구사항정책	지원됨	지원되는값	참고
WiFi 필요	X	꺼짐	

기타액세스정책	지원됨	지원되는값	참고
앱업데이트유예기간 (시간)	X	모두	
잠금시앱데이터지우기	X	모두	
활성폴링기간 (분)	X	모두	

암호화정책	지원됨	지원되는값	참고
암호화키	X	오프라인액세스허용됨	Android Enterprise 정책을통해지원됨
개인파일암호화	X	사용안함만	Android Enterprise 정책을통해지원됨
개인파일암호화제외	X	해당없음 (비우기)	Android Enterprise 정책을통해지원됨
공용파일에대한액세스제한	X	해당없음 (비우기)	Android Enterprise 정책을통해지원됨
공개파일암호화	X	사용안함만	Android Enterprise 정책을통해지원됨
공개파일암호화제외	X	해당없음 (비우기)	Android Enterprise 정책을통해지원됨
공개파일마이그레이션	X	사용안함만	Android Enterprise 정책을통해지원됨

앱상호작용정책	지원됨	지원되는값	참고
보안그룹	X	비우기	Android Enterprise 정책을통해지원됨
잘라내기및복사	X	제한없음만	Android Enterprise 정책을통해지원됨
붙여넣기	X	제한없음만	Android Enterprise 정책을통해지원됨
문서교환 (열기)	X	제한없음만	Android Enterprise 정책을통해지원됨
인바운드문서교환 (열기)	X	모두	Android Enterprise 정책을통해지원됨
인바운드문서교환화이트리스트	X	비우기	Android Enterprise 정책을통해지원됨
제한된열기제외목록	X	비우기	Android Enterprise 정책을통해지원됨

앱제한정책	지원됨	지원되는값	참고
카메라차단	X	켜짐만	Android Enterprise 정책을통해지원됨
갤러리차단	X	켜짐만	Android Enterprise 정책을통해지원됨
로컬호스트연결차단	X	모두	
마이크녹음차단	X	꺼짐만	Android Enterprise 정책을통해지원됨
위치서비스차단	X	꺼짐만	Android Enterprise 정책을통해지원됨
SMS 작성차단	X	꺼짐만	Android Enterprise 정책을통해지원됨
화면캡처차단	X	꺼짐만	Android Enterprise 정책을통해지원됨
장치센서차단	X	모두	
NFC 차단	X	꺼짐만	Android Enterprise 정책을통해지원됨
인쇄차단	X	모두	
앱로그차단	X	모두	

앱지오픈스정책	지원됨	지원되는값	참고
중심점경도	X	모두	
중심점위도	X	모두	
반경	X	모두	

Android Enterprise 계정설정구성

장치에서 Android 앱및정책관리를 시작하려면 먼저 XenMobile 에서 Android Enterprise 도메인및계정정보를 설정해야 합니다. 먼저 Google 에서 Android Enterprise 설정작업을 완료하여도메인관리자를 설정하고 서비스계정 ID 및바인딩토큰을 얻습니다.

1. XenMobile 웹콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버아래에서 **Android Enterprise** 를클릭합니다. **Android Enterprise** 구성페이지가나타납니다.

Settings > Android for Work

Legacy Android for Work ▼

Provide Android for Work configuration parameters.

Domain Name * ⓘ

Domain Admin Account * ⓘ

Service Account ID * ⓘ

Client ID * ⓘ

Enable Android for Work NO

Cancel Save

1. **Android Enterprise** 페이지에서다음설정을구성합니다.

- 도메인이름: 도메인이름을입력합니다.
- 도메인관리자계정: 도메인관리자사용자이름을입력합니다.
- 서비스계정 **ID**: Google 서비스계정 ID 를입력합니다.
- 클라이언트 **ID**: Google 서비스계정의클라이언트 ID 를입력합니다.
- **Android Enterprise** 사용: Android Enterprise 를사용할지여부를선택합니다.

2. 저장을클릭합니다.

XenMobile 에대한 G Suite 파트너액세스설정

일부 Chrome 용엔드포인트관리기능은 Google 파트너 API 를사용하여 XenMobile 과 G Suite 도메인간에통신합니다. 예를들어 XenMobile 에는시크릿모드와게스트모드같은 Chrome 기능을관리하기위한장치정책용 API 가필요합니다.

파트너 API 를사용하려면 XenMobile 콘솔에서 G Suite 도메인을설정한다음 G Suite 계정을구성합니다.

XenMobile 에서 G Suite 도메인설정

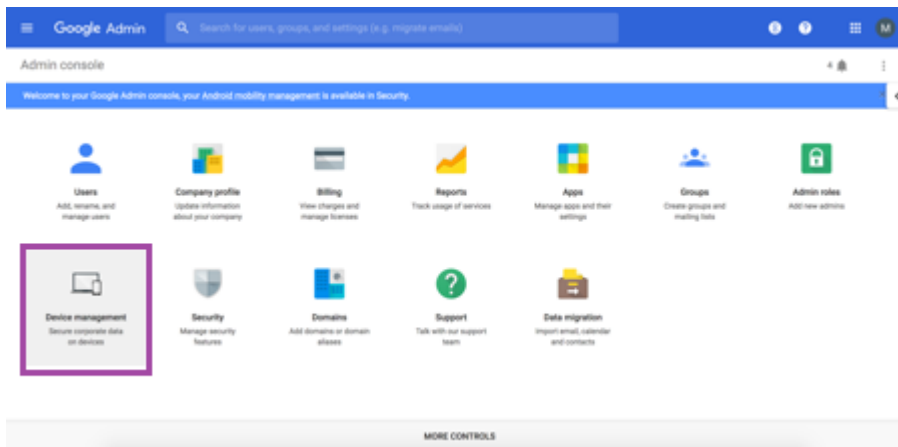
XenMobile 이 G Suite 도메인의 API 와통신하도록설정하려면 설정 > **Google Chrome** 구성으로이동하여설정을구성합니다.

G-Suite Domain *	xms [redacted]
G-Suite Admin *	ma [redacted]@xms [redacted]
G-Suite Client ID	105 [redacted]
G-Suite Enterprise ID	C01 [redacted]

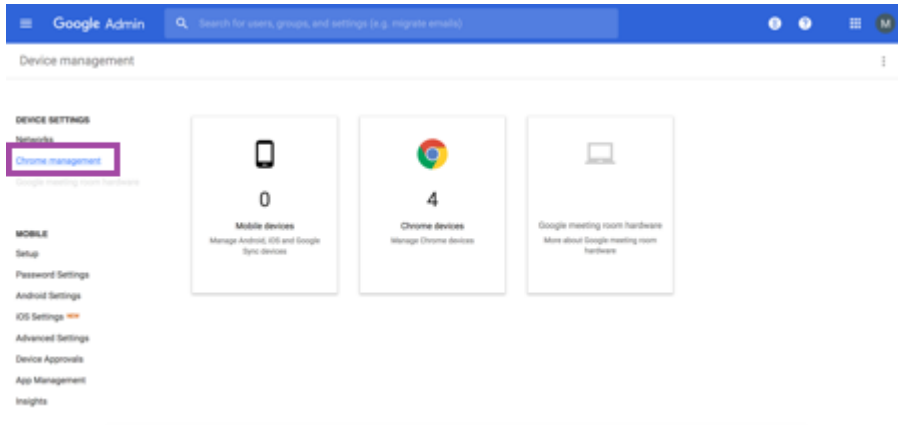
- **G Suite** 도메인: XenMobile 에필요한 API 를호스팅하는 G Suite 도메인입니다.
- **G Suite** 관리도메인: G Suite 도메인의관리자계정입니다.
- **G Suite** 클라이언트 ID: Citrix 의클라이언트 ID 입니다. G Suite 도메인에대한파트너엑세스를구성하려면이값을사 용합니다.
- **G Suite** 엔터프라이즈 ID: 계정의엔터프라이즈 ID 로, Google Enterprise 계정에서채워집니다.

G Suite 도메인의장치와사용자에대한파트너엑세스설정

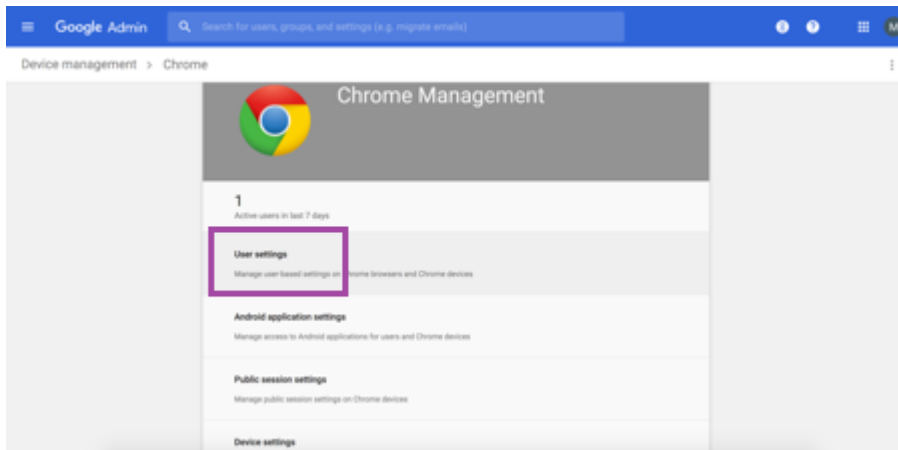
1. Google 관리자콘솔에로그인합니다. <https://admin.google.com>
2. **Device Management(장치관리)** 를클릭합니다.



3. **Chrome management(Chrome 관리)** 를클릭합니다.



4. **User settings(사용자설정)** 를 클릭합니다.



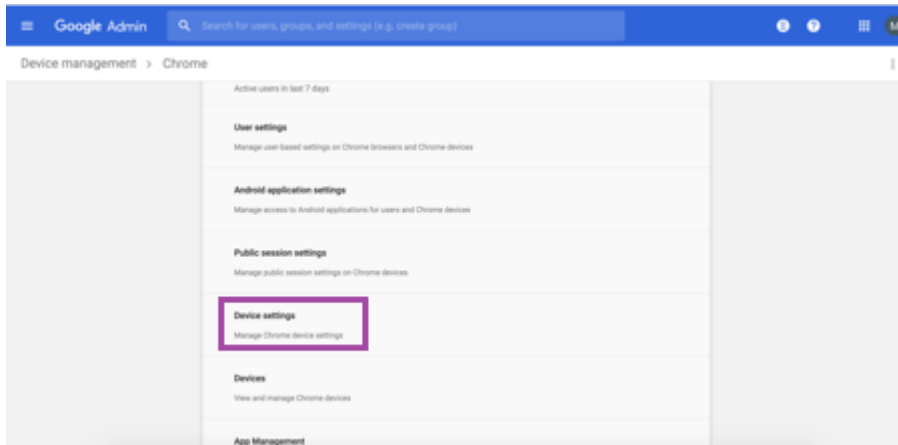
5. **Chrome Management - Partner Access(Chrome 관리 - 파트너 액세스)** 를 검색합니다.



6. **Enable Chrome Management - Partner Access(Chrome 관리 - 파트너 액세스사용)** 확인란을 선택합니다.

7. 파트너 액세스를 이해하고 사용하길 원한다는 데 동의합니다. 저장을 클릭합니다.

8. Chrome 관리페이지에서 **Device Settings(장치설정)** 를클릭합니다.



9. **Chrome Management - Partner Access(Chrome 관리 - 파트너액세스)** 를검색합니다.



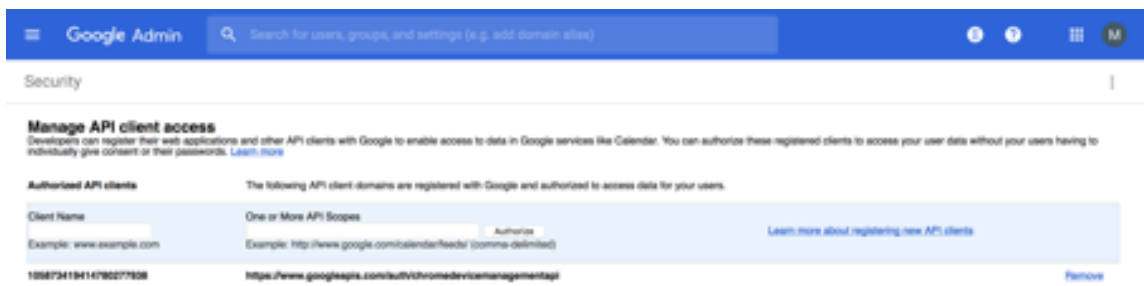
10. **Enable Chrome Management - Partner Access(Chrome 관리 - 파트너액세스사용)** 확인란을선택합니다.

11. 파트너액세스를이해하고사용하길원한다는데동의합니다. 저장을클릭합니다.

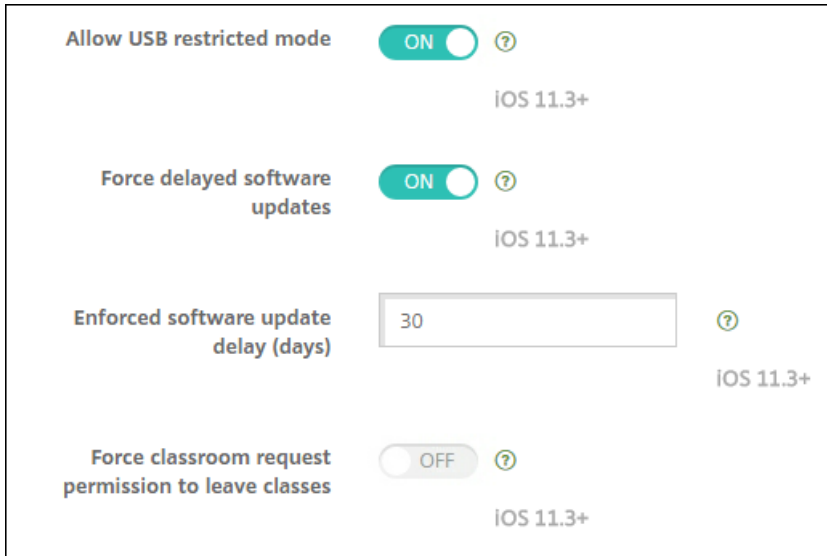
12. **Security(보안)** 페이지로이동한다음 **Advanced Settings(고급설정)** 를클릭합니다.



13. **Manage API client access**(API 클라이언트액세스관리) 를클릭합니다.
14. XenMobile 콘솔에서 설정 > **Google Chrome** 구성으로이동하여 G Suite Client ID 의값을복사합니다. 그런다음 **Manage API client Access**(API 클라이언트액세스관리) 페이지로돌아가서복사한값을 **Client Name**(클라이언트이름) 필드에붙여넣습니다.
15. **One or More API Scopes**(하나이상의 API 범위) 에서 URL(<https://www.googleapis.com/auth/chromedevicemanagementapi>) 을추가합니다.



16. **Authorize**(승인) 을클릭합니다.
 “Your settings have been saved(설정이저장되었습니다)” 라는메시지가표시됩니다.



Android Enterprise 장치등록

장치등록프로세스동안사용자가사용자이름또는사용자 ID 를입력해야하는경우 XenMobile 서버가무엇 (UPN(사용자계정이름) 또는 SAM 계정이름) 으로사용자를검색하도록구성되었는지에따라사용가능한형식이달라집니다.

XenMobile 서버가 UPN 으로사용자를검색하도록구성된경우다음형식으로 UPN 을입력해야합니다.

- *username@domain*

XenMobile 서버가 SAM 으로사용자를검색하도록구성된경우다음형식으로 SAM 을입력해야합니다.

- *username@domain*
- *domain\username*

XenMobile 서버가어떤사용자이름유형으로구성되었는지확인하려면:

1. XenMobile 서버콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. **LDAP** 를클릭하여 LDAP 연결구성을봅니다.
3. 페이지하단가까이에있는 사용자검색기준필드를확인합니다.
 - **userPrincipalName** 으로설정된경우 XenMobile 서버가 UPN 으로검색하도록설정된것입니다.
 - **sAMAccountName** 으로설정된경우 XenMobile 서버가 SAM 으로검색하도록설정된것입니다.

Android Enterprise 엔터프라이즈등록취소

XenMobile Server 콘솔및 XenMobile Tools 를사용하여 Android Enterprise 엔터프라이즈를등록취소할수있습니다.

이작업을수행하면 XenMobile Server 에서 XenMobile Tools 에대한팝업창이열립니다. 시작하기전에사용하는브라우저에서팝업창을여는데필요한권한이 XenMobile Server 에있는지확인하십시오. Google Chrome 같은일부브라우저의경우팝업차단을사용하지않도록설정하고 XenMobile 사이트주소를팝업차단화이트리스트에추가해야합니다.

경고:

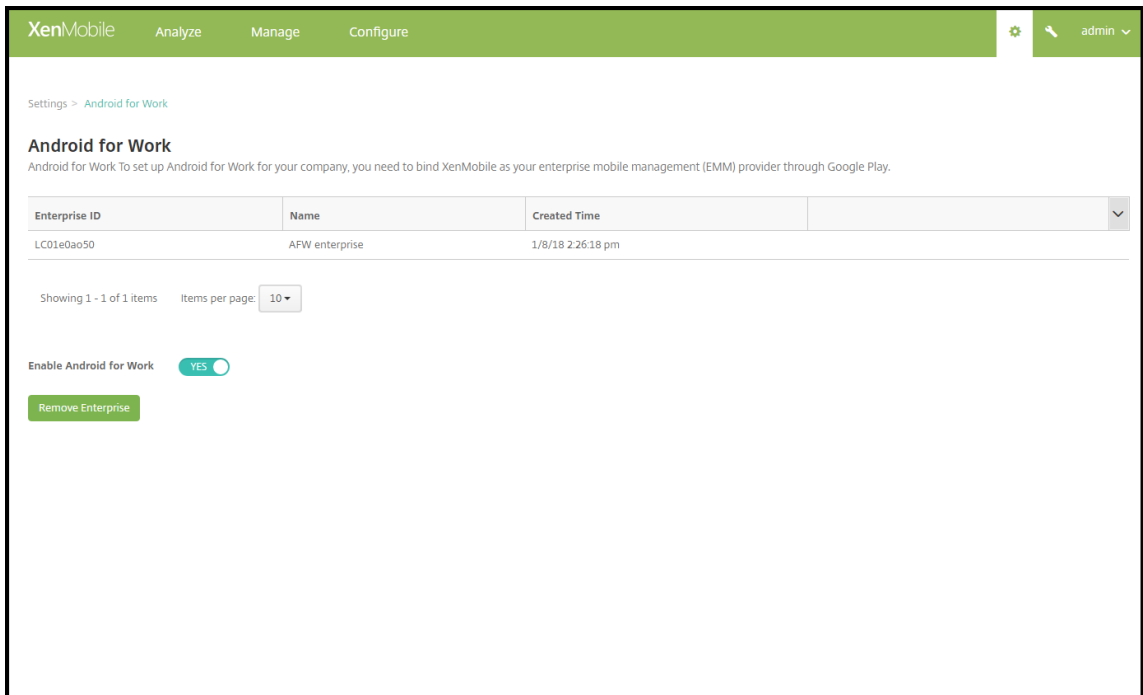
엔터프라이즈등록이취소되면엔터프라이즈를통해이미등록된장치의 Android Enterprise 앱이기본상태로재설정됩니다. 장치가더이상 Google 을통해관리되지않습니다. Android Enterprise 엔터프라이즈에다시등록하는경우추가구성을수행하지않으면이전기능이복원되지않을수있습니다.

Android Enterprise 엔터프라이즈등록취소후:

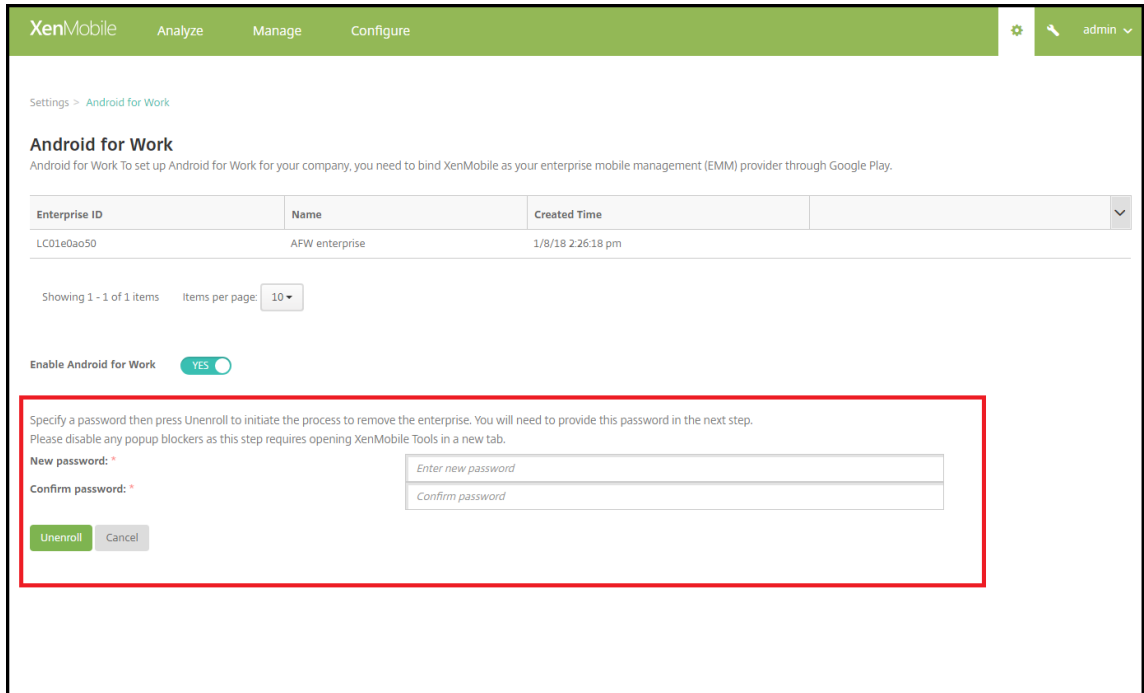
- 엔터프라이즈를통해등록된장치및사용자의 Android Enterprise 앱이기본상태로재설정됩니다. 이전에적용된 Android Enterprise 앱권한및 Android Enterprise 앱제한정책이더이상유효하지않습니다.
- 엔터프라이즈를통해등록된장치는 XenMobile 을통해관리되지만 Google 측면에서는관리되지않습니다. 새로운 Android Enterprise 앱을추가할수없습니다. 새로운 Android Enterprise 앱권한또는 Android Enterprise 앱제한정책을적용할수없습니다. 예약, 암호및제한같은다른정책은계속해서이러한장치에적용할수있습니다.
- Android Enterprise 에장치를등록하려고하면 Android Enterprise 장치가아닌 Android 장치로등록됩니다.

Android Enterprise 엔터프라이즈를등록취소하려면:

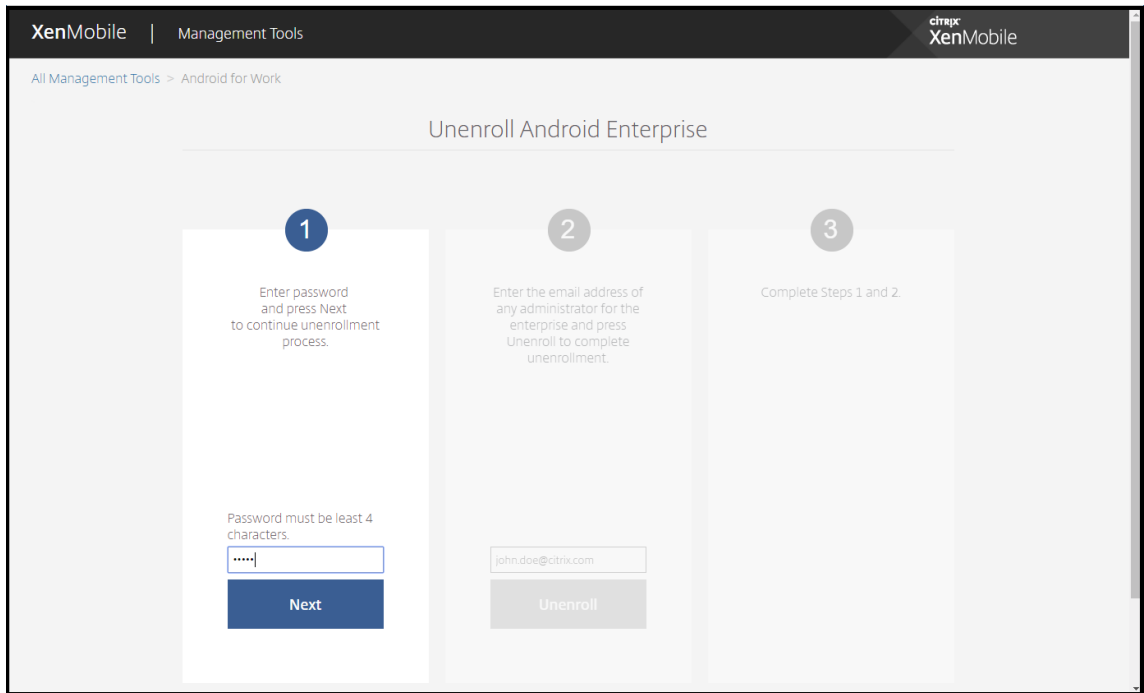
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 설정페이지에서 **Android Enterprise** 를클릭합니다.
3. 엔터프라이즈제거를클릭합니다.



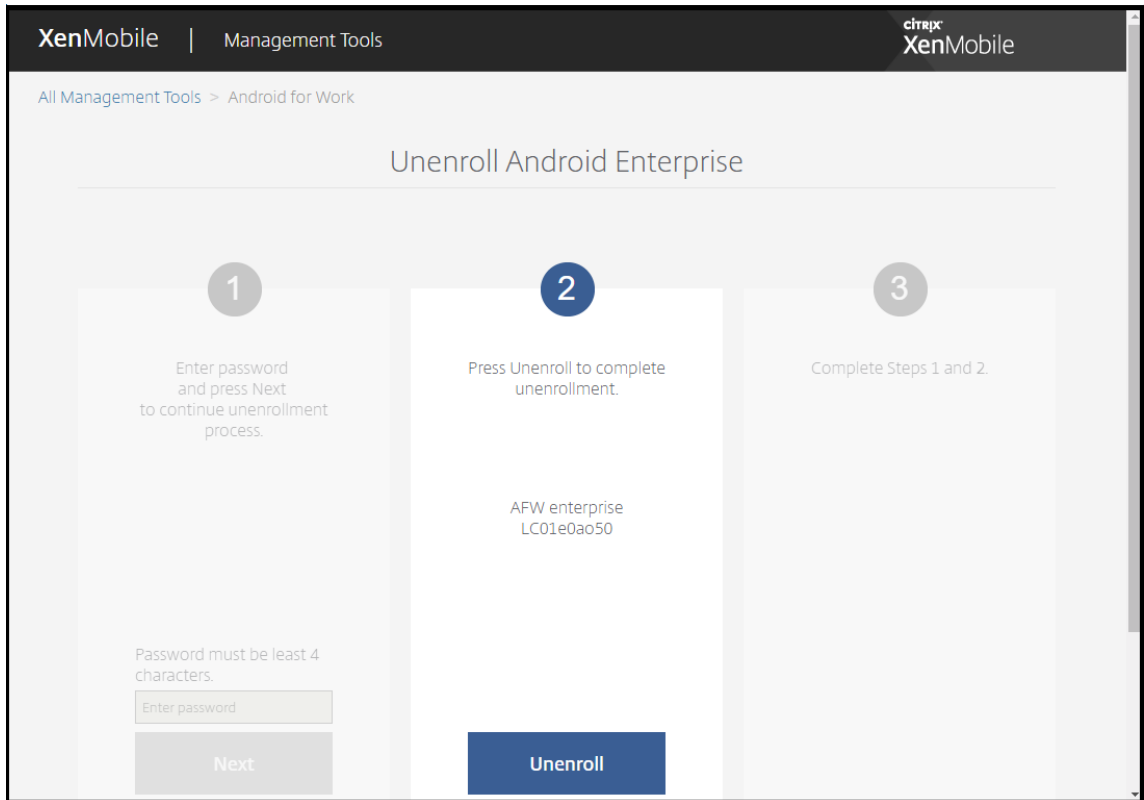
4. 암호를지정합니다. 그다음단계에서등록취소를완료하려면암호가필요합니다. 그런다음 등록취소를클릭합니다.



5. XenMobile Tools 페이지가열리면이전단계에서만든암호를입력합니다.



6. 등록취소를클릭합니다.



Android Enterprise 에서완전하게관리되는장치프로비전

회사소유장치만 Android Enterprise 에서완전하게관리되는장치가될수있습니다. 완전하게관리되는장치에서는작업프로필뿐만아니라전체장치가회사또는조직에의해제어됩니다. 완전하게관리되는장치를작업관리장치라고도합니다.

XenMobile 은완전하게관리되는장치에대해다음과같은등록방법을지원합니다.

- **afw#xenmobile:** 이등록방법을사용하는경우사용자가장치를설정할때 “afw#xenmobile” 문자를입력합니다. 이 토큰은 XenMobile 이관리하는장치로장치를식별하고 Secure Hub 를다운로드합니다.
- **QR 코드:** QR 코드프로비저닝을통해태블릿과같이 NFC 를지원하지않는분산된제품군장치간편하게프로비저닝할수있습니다. QR 코드등록방법은출고기본값으로재설정된제품군장치에서사용할수있습니다. QR 코드등록방법은설치마법사에서 QR 코드를스캔하여완전하게관리되는장치를설정하고구성합니다.
- **NFC(근거리통신) 범프:** NFC 범프등록방법은출고기본값으로재설정된제품군장치에서사용할수있습니다. NFC 범프는근거리통신을사용하여두장치간데이터를전송합니다. 출고기본값으로재설정된장치에서는 Bluetooth, Wi-Fi 및기타통신모드를사용할수없습니다. NFC 는이상태에서장치가사용할수있는유일한통신프로토콜입니다.

afw#xenmobile

이등록방법은새장치또는출고기본값으로재설정된장치의전원을켄후초기설정시사용됩니다. Google 계정을입력하라는메시지가표시되면사용자가 “afw#xenmobile” 을입력합니다. 이동작을수행하면 Secure Hub 가다운로드되고설치됩니다. 그런다음사용자는 Secure Hub 설정메시지에따라등록을완료합니다.

최신버전의 Secure Hub 가 Google Play Store 에서다운로드되므로이등록방법이대부분의고객에게권장됩니다. 다른등록방법과달리, XenMobile 서버에서다운로드하기위해 Secure Hub 를제공하지않습니다.

사전요구사항:

- Android 5.0 이상을실행하는모든 Android 장치에서지원됩니다.

QR 코드

장치모드에서 QR 코드를사용하여장치를등록하려면 JSON 을생성하고 JSON 을 QR 코드로변환하여 QR 코드를생성합니다. QR 코드가장치카메라로스캔되어장치가등록됩니다.

사전요구사항:

- Android 7.0 이상을실행하는모든 Android 장치에서지원됩니다.

JSON 에서 QR 코드생성

다음필드를사용하여 JSON 을생성합니다.

다음필드는필수입니다.

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

값: com.zenprise/com.zenprise.configuration.AdminFunction

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

값: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll10jcxT3-yKM

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

값: <https://path/to/securehub.apk>

참고:

Secure Hub 가엔터프라이즈앱으로 Citrix XenMobile 서버에업로드된경우 https://<fqdn>:4443/*instanceName*/worxhome.apk에서다운로드할수있습니다. Secure Hub APK 의경로는프로비저닝장치 가연결되는 Wi-Fi 연결을통해액세스할수있어야합니다.

다음필드는선택사항입니다.

- **android.app.extra.PROVISIONING_LOCALE:** 언어및국가코드를입력합니다.

언어코드는 [ISO 639-1](#)에정의된대문자두자구조성된 ISO 언어코드입니다 (예: en). 국가코드는 [ISO 3166-1](#)에정의된대문자두자구조성된 ISO 국가코드입니다 (예: US). 예를들어, 미국에서사용하는영어의경우 en_US 를입력합니다.

- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가실행되고있는표준시간대입니다.

[지역/위치형식의 Olson 이름](#)을입력합니다. 예를들어태평양표준시의경우 America/Los_Angeles 를입력합니다. 입력하지않으면표준시간대가자동으로입력됩니다.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Epoch 이후의시간 (밀리초) 입니다.
Unix Epoch(즉 Unix 시간또는 POSIX 시간 Unix 타임스탬프) 는 1970 년 1 월 1 일 (자정 UTC/GMT) 이후경과한 시간이며, 윤초는계산되지않습니다 (ISO 8601: 1970-01-01T00:00:00Z).
- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 프로필생성시암호화를건너뛰려면 **true** 로설정합니다. 프로필생성시암호화를적용하려면 **false** 로설정합니다.

일반적인 JSON 은다음과같은형식입니다.

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": " ",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

JSON 유효성검사도구 (예: <https://jsonlint.com>) 를사용하여생성된 JSON 의유효성을검사하고온라인 QR 코드생성기 (예: <https://goqr.me>) 를사용하여해당 JSON 문자열을 QR 코드로변환합니다.

이 QR 코드는출고기본값으로재설정된장치에서스캔되어해당장치가작업관리장치모드로등록됩니다.

장치를등록하려면

완전하게관리되는장치로장치를등록하려면장치가출고기본값으로재설정된상태여야합니다.

1. 시작화면에서화면을 6 번눌러 QR 코드등록흐름을시작합니다.
2. 메시지가표시되면 Wi-Fi 에연결합니다. QR 코드에있는 Secure Hub 의다운로드위치 (JSON 으로인코딩됨) 는이 Wi-Fi 네트워크를통해액세스할수있습니다.
장치가 Wi-Fi 에연결되면 Google 에서 QR 코드판독기를다운로드하고카메라를시작합니다.
3. 카메라로 QR 코드를가리키고코드를스캔합니다.

Android 는 QR 코드에있는다운로드위치에서 Secure Hub 를다운로드하고서명인증서서명의유효성을검사한후 Secure Hub 를설치하고장치소유자로설정합니다.

자세한내용은 Android EMM 개발자용 Google 가이드 (https://developers.google.com/android/work/prov-devices#qr_code_method) 를참조하십시오.

NFC 범프

NFC 범프를사용하여완전하게관리되는장치로장치를등록하려면두장치, 즉출고기본값으로재설정된장치와 XenMobile Provisioning Tool 을실행하는장치가필요합니다.

사전요구사항:

- Android 5.0, Android 5.1, Android 6.0 이상을실행하는모든 Android 장치에서지원됩니다.
- Android Enterprise 를사용하도록설정된 XenMobile Server 버전 10.4

- 완전하게관리되는장치로서 Android Enterprise 용으로프로비전된새장치또는출고기본값으로재설정된장치. 이사전 요구사항을완료하는단계는이문서의뒷부분에서찾을수있습니다.
- NFC 호환성이있으며구성된 Provisioning Tool 이실행되고있는또다른장치. Provisioning Tool 은 Secure Hub 10.4 또는 [Citrix 다운로드페이지](#)에서사용할수있습니다.

각장치에는 EMM(엔터프라이즈모빌리티관리) 앱으로관리되는 Android Enterprise 프로필이하나만있을수있습니다. XenMobile 에서 Secure Hub 는 EMM 앱입니다. 각장치에는하나의프로필만허용됩니다. 두번째 EMM 앱을추가하면첫번째 EMM 앱이제거됩니다.

NFC 범프를통해전송된데이터

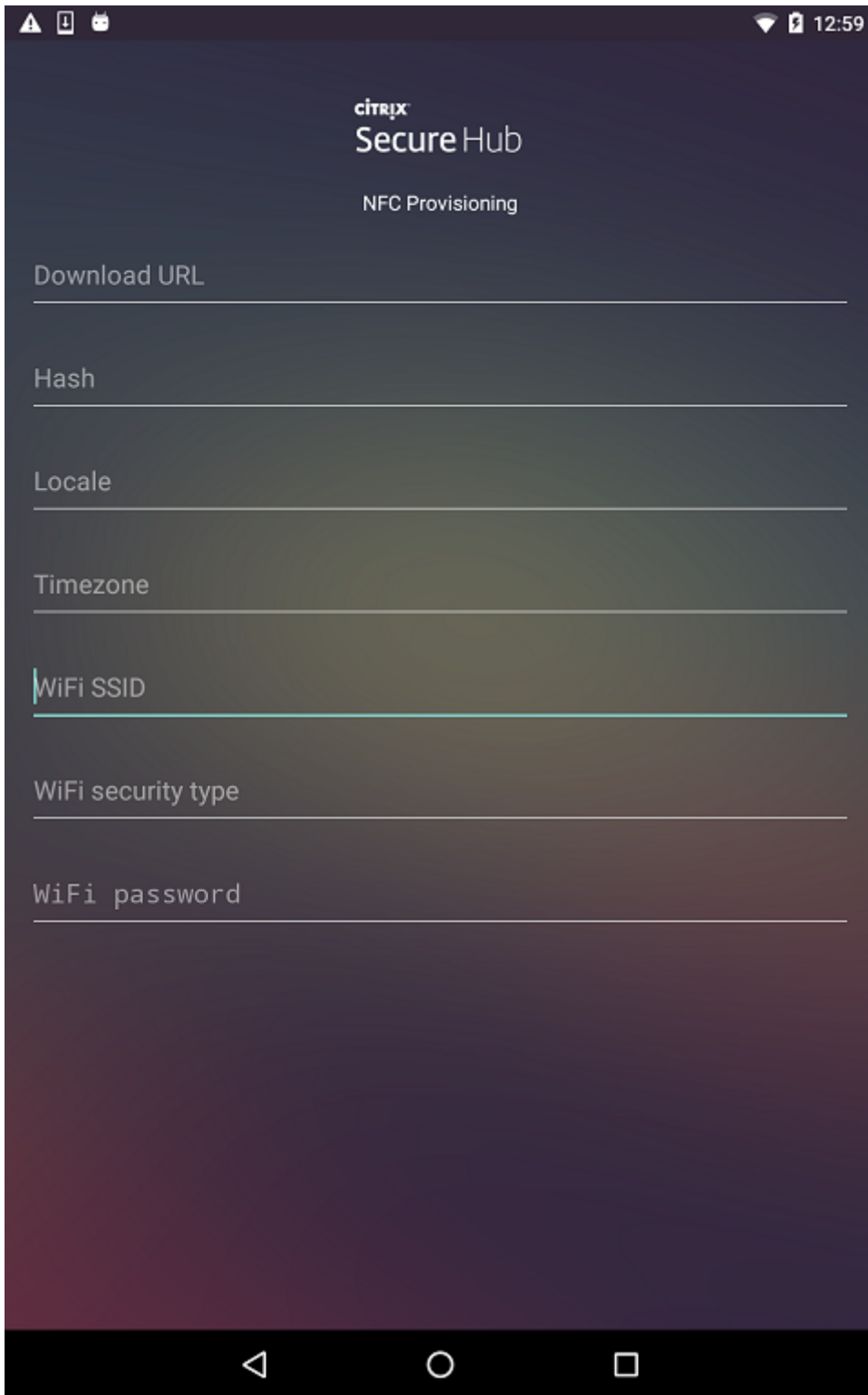
출고기본값으로재설정된장치를프로비저닝하려면 NFC 범프를통해다음데이터를전송하여 Android Enterprise 를초기화해야합니다.

- 장치소유자 (이경우 Secure Hub) 역할을하는 EMM 공급자앱의패키지이름
- 장치가 EMM 공급자앱을다운로드할수있는인트라넷/인터넷위치
- 다운로드가성공했는지확인하기위한 EMM 공급자앱의 SHA1 해시
- 출고기본값으로재설정된장치가연결하여 EMM 공급자앱을다운로드할수있는 Wi-Fi 연결세부정보. 참고: 이단계에서 Android 는 802.1x Wi-Fi 를지원하지않습니다.
- 장치의표준시간대 (선택사항)
- 장치의지리적위치 (선택사항)

두장치가범프되면 Provisioning Tool 의데이터가출고기본값으로재설정된장치로전송됩니다. 이데이터는관리자설정으로 Secure Hub 를다운로드하는데사용됩니다. 표준시간대및위치값을입력하지않으면 Android 가자동으로새장치에서이러한값을구성합니다.

XenMobile Provisioning Tool 구성

NFC 범프를수행하기전에 Provisioning Tool 을구성해야합니다. 이구성은 NFC 범프중에출고기본값으로재설정된장치로전송됩니다.



필요한필드에데이터를입력하거나텍스트파일을통해데이터를채울수있습니다. 다음절차의단계에서는텍스트파일을구성하고각필드에대한설명을포함시키는방법에대해설명합니다. 입력한정보가앱에서저장되지않으므로나중에사용할수있도록정보를유지하려면텍스트파일을만들수있습니다.

텍스트파일을 사용하여 **Provisioning Tool** 을 구성하려면

파일의 이름을 nfcprovisioning.txt 로 지정하고 장치의 SD 카드에 있는 /sdcard/ 폴더에 파일을 저장합니다. 그러면 앱에서 텍스트 파일을 읽고 값을 채울 수 있습니다.

텍스트 파일에는 다음과 같은 데이터가 포함되어야 합니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>
```

이 줄은 EMM 공급자 앱의 인터넷/인터넷 위치입니다. NFC 범프 후에 출고 기본값으로 재설정된 장치가 Wi-Fi 에 연결되면 장치가 이 위치에 액세스하여 다운로드할 수 있어야 합니다. URL 은 특수한 형식이 필요하지 않은 일반 URL 입니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```

이 줄은 EMM 공급자 앱의 체크섬입니다. 이 체크섬은 다운로드가 성공했는지 확인하는 데 사용됩니다. 체크섬을 얻는 단계에 대해서는 이 문서 뒷부분에서 설명합니다.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

이 줄은 Provisioning Tool 이 실행되고 있는 장치의 연결된 Wi-Fi SSID 입니다.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

지원되는 값은 WEP 및 WPA2 입니다. Wi-Fi 가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Wi-Fi 가 보호되지 않는 경우 이 필드는 비어 있어야 합니다.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

언어 및 국가 코드를 입력합니다. 언어 코드는 [ISO 639-1](#)에 정의된 대로 소문자 두 자로 구성된 ISO 언어 코드입니다 (예: en). 국가 코드는 [ISO 3166-1](#)에 정의된 대로 대문자 두 자로 구성된 ISO 국가 코드입니다 (예: US). 예를 들어, 미국에서 사용하는 영어의 경우 en_US 를 입력합니다. 코드를 입력하지 않으면 국가 및 언어가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

장치가 실행되는 표준 시간대입니다. [지역/위치 형식의 Olson 이름](#)을 입력합니다. 예를 들어 태평양 표준 시의 경우 America/Los_Angeles 를 입력합니다. 이름을 입력하지 않으면 표준 시간대가 자동으로 입력됩니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

값이 앱에 Secure Hub 로 하드코딩되어 있기 때문에 이 데이터는 필요하지 않습니다. 여기서는 완결성을 위해 언급되었습니다.

예를 들어 WPA2 를 사용하여 보호되는 Wi-Fi 가 있는 경우 완성된 nfcprovisioning.txt 파일은 다음과 같습니다.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

예를들어보호되지않는 Wi-Fi 가있는경우완성된 nfcprovisioning.txt 파일은다음과같습니다.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\n\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Secure Hub 체크섬을얻으려면

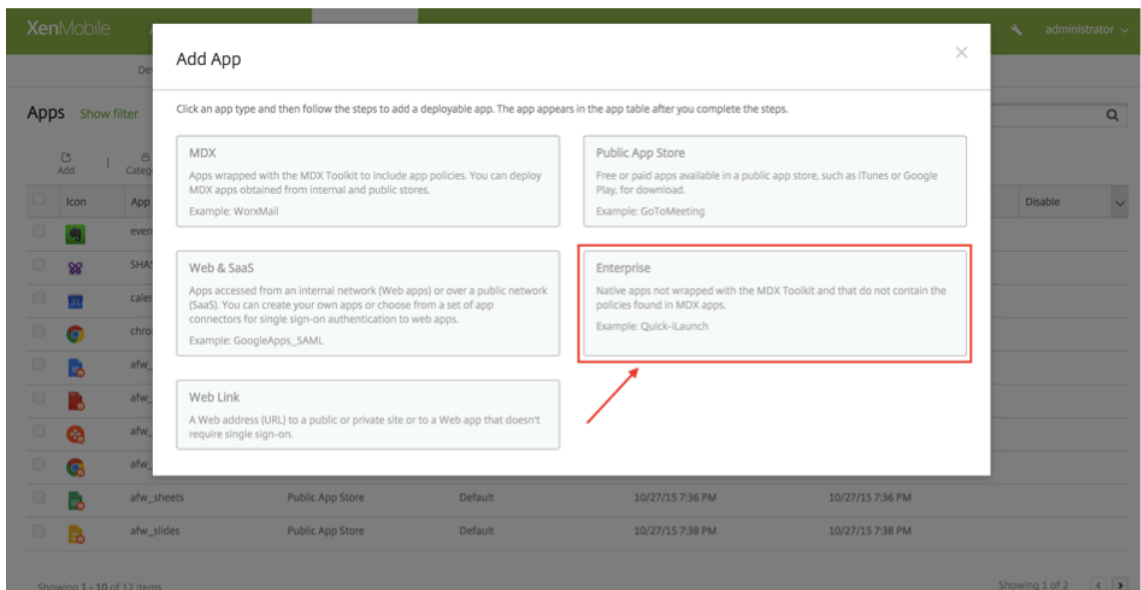
특정앱의체크섬을얻으려면앱을엔터프라이즈앱으로추가합니다.

1. XenMobile 콘솔에서 구성 > 앱으로이동한후 추가를클릭합니다.

앱추가창이나타납니다.

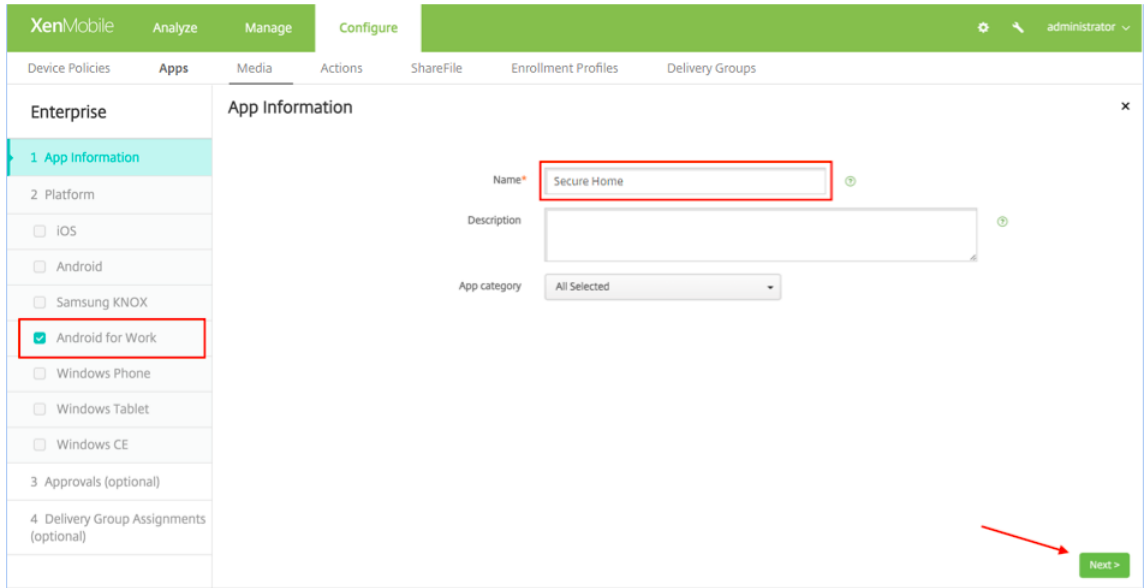
2. 엔터프라이즈를클릭합니다.

앱정보페이지가나타납니다.



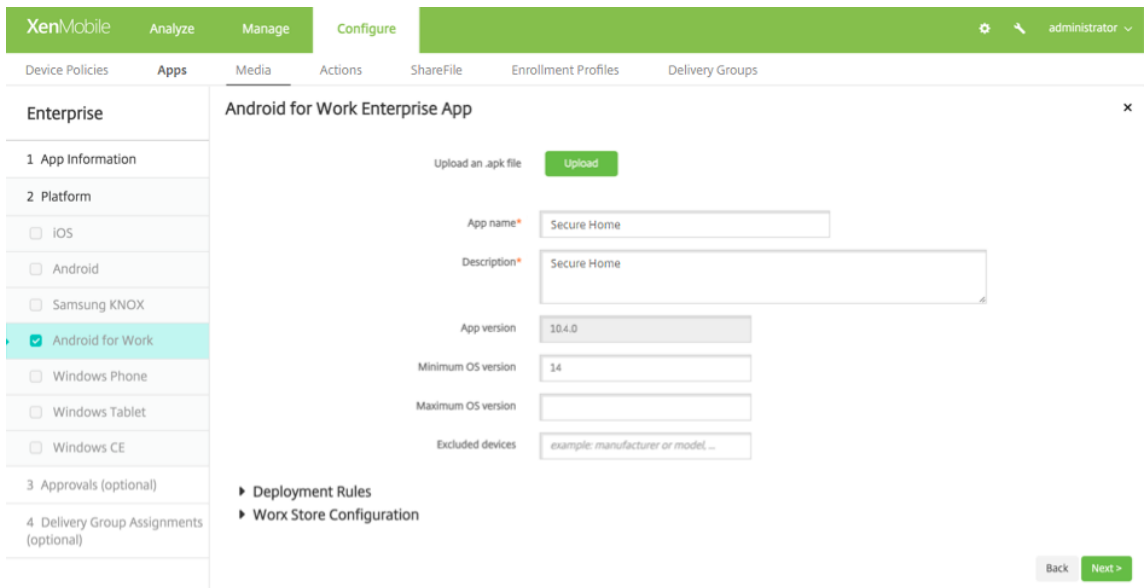
3. 다음과같은구성을선택한후 다음을클릭합니다.

Android Enterprise 엔터프라이즈앱페이지가나타납니다.

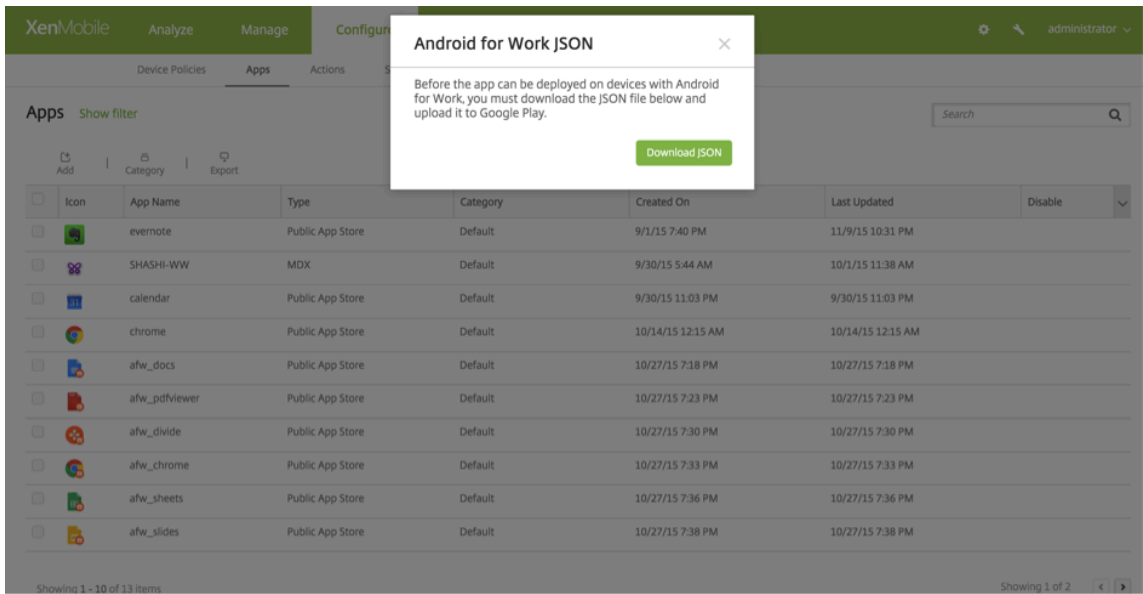


4. .apk 에대한경로를제공한후 다음을클릭하고파일을업로드합니다.

업로드가완료되면업로드된패키지의세부정보가나타납니다.



5. 다음을클릭하여 JSON 파일을다운로드하는페이지를엽니다. 이파일을사용하여 Google Play 에업로드할수있습니다. Secure Hub 의경우 Google Play 에업로드할필요없지만 SHA1 값을읽으려면 JSON 파일이필요합니다.



일반적인 JSON 파일은 다음과 같은 형식입니다.

```
1 { "icon_filename": "48_48_launcher.png", "file_sha256_base64":  
2 "0IMZ86TLGd9TxsINF8wC1Q0uAVkKvLA00JP3Avs\u003d", "file_sha1_base64":  
3 "154vuW1tkzfx8mT3CnmpM3o8\u003d", "package_name": "com.zenprise",  
4 "application_label": "Work Home", "icon_base64":  
5 "iVBORw0KGpAAANSUhEUgAAADAAwAAQAAIAAABIAAAAPFkLEQVRo3u2aaZSU1Znhf/e+71vV1dXdFHQD3U2zHqgTYgKILko0ESDYU4S18IMjkehN21Q8s1YzicIojkxaojHJGJmYrnxFB4gJaSNjM05ZuICogrn3NQLP8B  
6 "version_code": "352975", "certificate_base64": "  
7 "MTIBqzCCAR5GawIBagIES/p1DANBokohkIG9w8BAQJFADAAMRgwfFgYDV0QKew9TcGFydXQgl29mdHhcmU4hchMTAAMTIT800EYhcnNDAAWATE2MTI800EYmJAAARgwfFgYDV0QKew9TcGFydXQgl29mdHhcmU4hchMT8wODQY  
8 "file_size": "25916262", "externally_hosted_url":  
9 "https://afwtest.xmdev.citrix.com:4443/Citrix/v1/download/app/MobileApp23",  
10 "version_name": "10.3.0", "minimum_sdk": "14"}  
11
```

6. file_sha1_base64 값을 복사한 후 Provisioning Tool 의 해시 필드에 이 값을 사용합니다.

참고:

해시는 URL 로 사용할 수 있는 형식이어야 합니다.

- 모든 + 기호를 -로 변환합니다.
- 모든 / 기호를 _로 변환합니다.
- 끝에 있는 \u003d 를 =로 바꿉니다.

장치의 SD 카드에 있는 nfcprovisioning.txt 파일에 해시를 저장하면 앱에서 안전을 위한 변환을 수행합니다. 하지만 수동으로 해시를 입력하는 경우 URL 안전성을 보장하는 것은 사용자의 책임입니다.

사용된 라이브러리

Provisioning Tool 의 소스 코드에는 다음과 같은 라이브러리가 사용되었습니다.

- Apache 라이선스 2.0 에 따라 Google 이 제작한 v7 appcompat 라이브러리, 디자인 지원 라이브러리 및 v7 Palette 라이브러리

자세한 내용은 [지원 라이브러리 기능 가이드](#)에서 참조하십시오.

- Apache 라이선스 2.0 에 따라 Jake Wharton 이 제작한 [Butter Knife](#)

Android Enterprise 에서작업프로필장치프로비전

Android Enterprise 에서작업프로필장치에대해회사영역과개인영역을안전하게분리할수있습니다. 예를들어 BYOD 장치는작업프로필장치가될수있습니다. 작업프로필장치의등록환경은 XenMobile 의 Android 등록과비슷합니다. 사용자가 Google Play 에서 Secure Hub 를다운로드하고장치를등록합니다.

Android Enterprise 에서작업프로필장치로장치를등록하는경우 USB 디버깅및알수없는소스설정은기본적으로사용되지않도록설정됩니다.

팁:

Android Enterprise 에서작업프로필장치로장치를등록하는경우항상 Google Play 로이동하십시오. 거기서사용자의 개인프로필에 Secure Hub 가표시되도록설정합니다.

iOS 및 macOS 장치의대량등록

January 27, 2020

XenMobile 에서는두가지방법을사용하여많은수의 iOS 및 macOS 장치를등록할수있습니다.

- Apple DEP(장치등록프로그램) 를사용하여 Apple, 참여 Apple 공인리셀러또는이동통신사업자로부터직접구입한 iOS 및 macOS 장치를등록할수있습니다. XenMobile 은비즈니스를위한장치등록프로그램과교육기관을위한 Apple School Manager 를지원합니다. 이문서에는비즈니스 DEP 계정통합이설명되어있습니다. Apple School Manager DEP 계정에대한자세한내용은 [Apple 교육기능과통합](#)을참조하십시오.

DEP 를사용하여 macOS 장치를등록하려면 XenMobile 에서해당장치가 macOS 10.10 이상을실행해야합니다.

- 또는 Apple Configurator 를사용하여 Apple 에서직접구입했는지여부와관계없이 iOS 장치를등록할수있습니다.

Business DEP 를사용하는경우:

- 장치를터치하거나준비할필요가없습니다. 대신, DEP 를통해장치일련번호또는구매주문번호를제출하여장치를구성하고등록할수있습니다.
- XenMobile 에장치가등록된후에는장치를사용자에게제공하여바로사용하도록할수있습니다. 또한 DEP 를사용하여장치를설정하면장치를처음시작할때완료해야하는설정도우미의몇몇단계를제거할수있습니다.
- DEP 설정에대한자세한내용은 Apple [Business Support](#) 페이지를참조하십시오.

Apple Configurator 를사용하는경우:

- iOS 장치를 macOS 10.7.2 이상을실행하는 Apple 컴퓨터와 Apple Configurator 2 앱에연결합니다. Apple Configurator 2 를통해 iOS 장치를준비하고정책을구성할수있습니다.
- 필요한정책으로장치를프로비전후장치에서처음으로 XenMobile 에연결하면 XenMobile 의정책이장치에수신됩니다. 그런다음장치관리를시작할수있습니다.
- Apple Configurator 사용에대한자세한내용은 Apple [Configurator Support\(Configurator 지원\)](#)를참조하십시오.

사전요구사항

- Apple DEP(장치등록프로그램) 를 사용하여 Apple, 참여 Apple 공인리셀러또는이동통신사업자로부터직접구입한 iOS 및 macOS 장치를등록할수있습니다. XenMobile 은비즈니스를위한장치등록프로그램과교육기관을위한 Apple School Manager 를지원합니다. 이문서에는비즈니스 DEP 계정통합이설명되어있습니다. Apple School Manager DEP 계정에대한자세한내용은 [Apple 교육기능과통합](#)을참조하십시오.

XenMobile 과 Apple 간의연결에필요한포트를열어야합니다. 자세한내용은 [포트요구사항](#)에서참조하십시오.

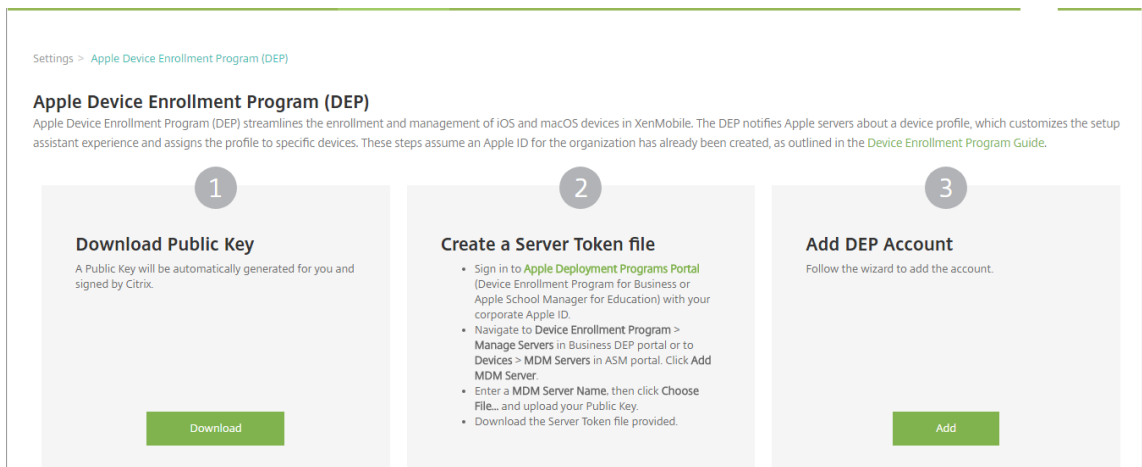
비즈니스 Apple DEP 계정과 XenMobile 통합

Apple Business DEP 계정이없는경우 [Apple DEP](#) 를통해 iOS 및 macOS 장치배포를참조하십시오.

Apple 비즈니스 DEP 계정을 XenMobile 서버배포에연결하려면다음단계에설명된것과같이 XenMobile 콘솔과 Apple DEP 포털에서정보를입력합니다.

1 단계: XenMobile 서버에서공개키를다운로드

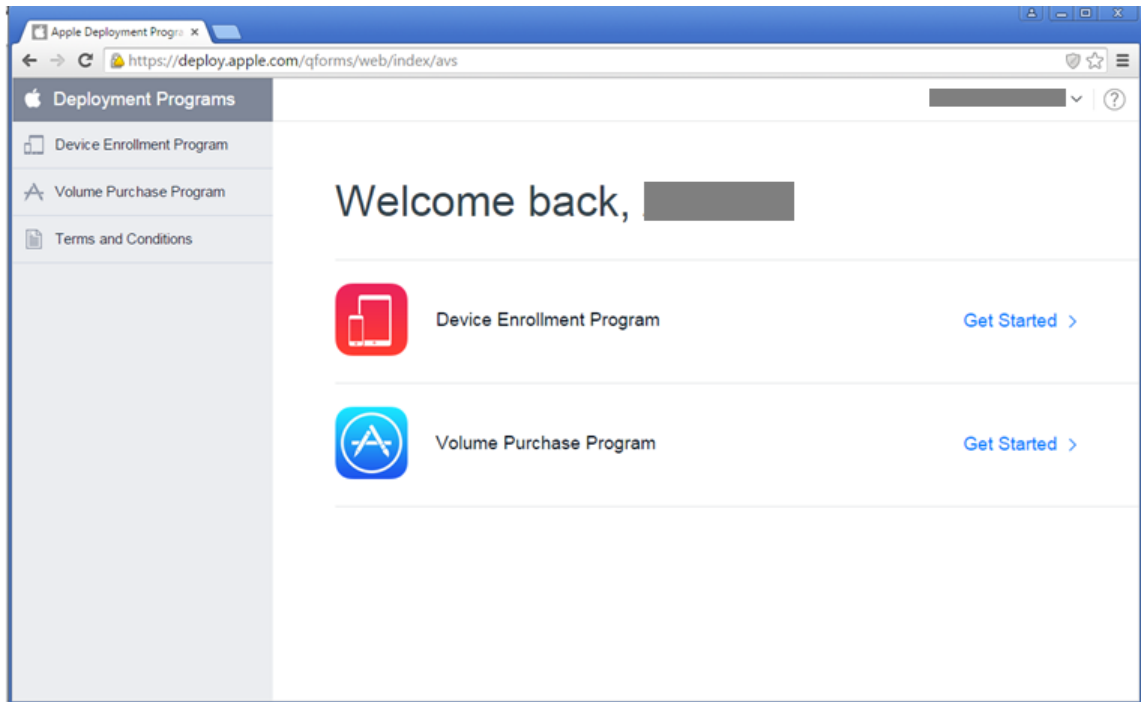
1. XenMobile 콘솔에로그온하고 설정 > **Apple DEP(장치등록프로그램)** 로이동합니다.



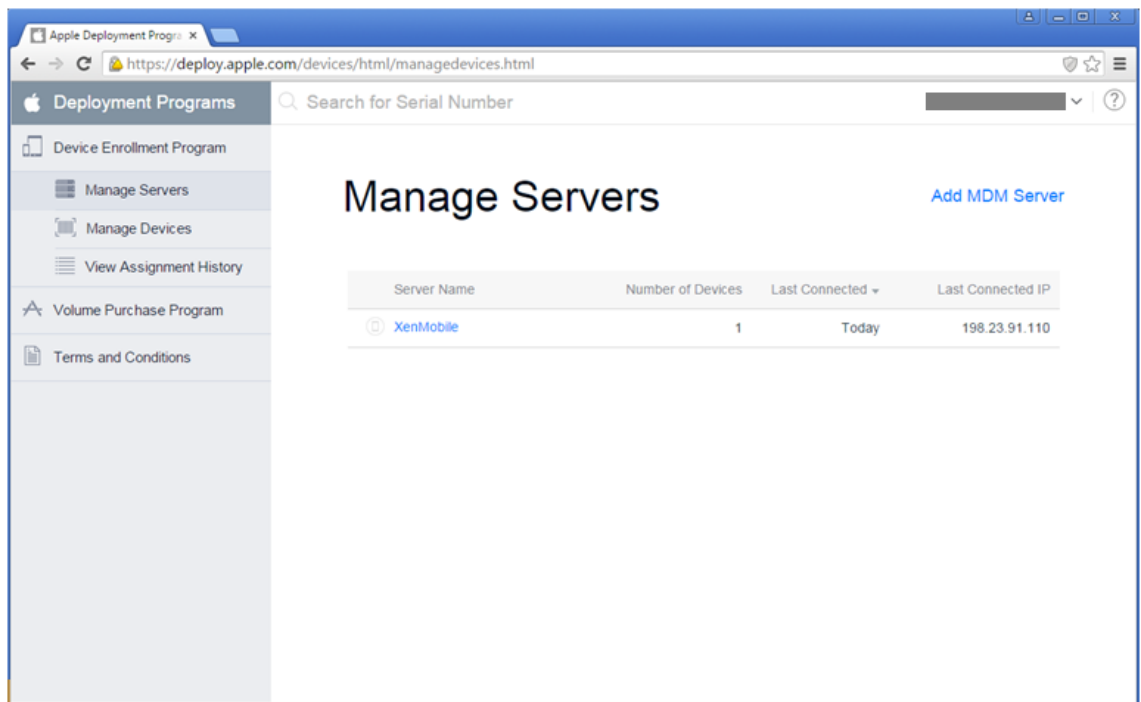
2. 공개키다운로드에서 다운로드를클릭합니다.

2 단계: Apple 계정에서서버토큰파일을만들고다운로드

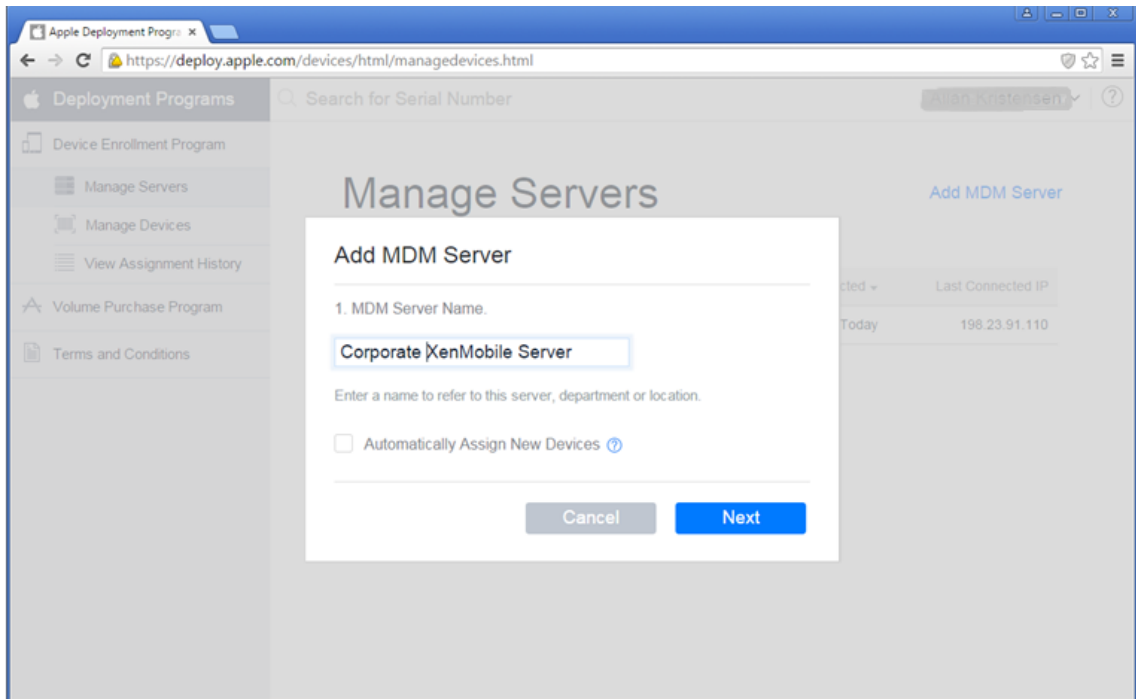
1. 회사 Apple ID 를사용하여 [Apple Deployment Program Portal\(Apple 배포프로그램포털\)](#)에로그온합니다.
2. Apple DEP 포털에서 **Device Enrollment Program(장치등록프로그램)** 을클릭합니다.



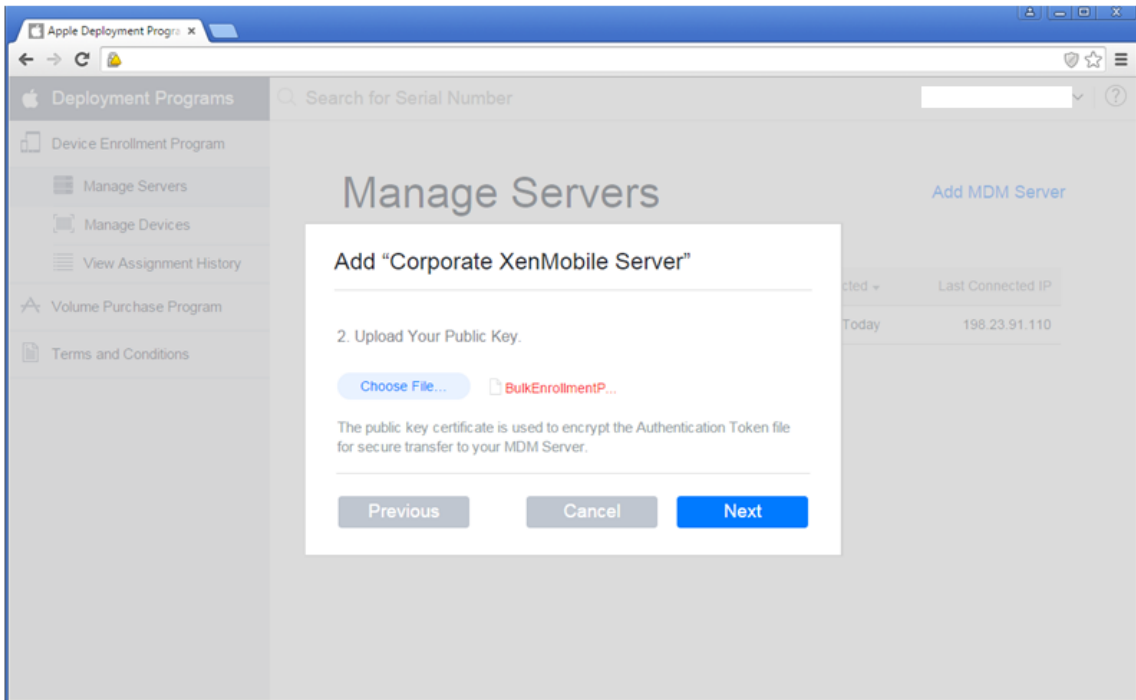
3. **Manage Servers**(서버관리) 를클릭한후오른쪽에서 **Add MDM Server**(MDM 서버추가) 를클릭합니다.



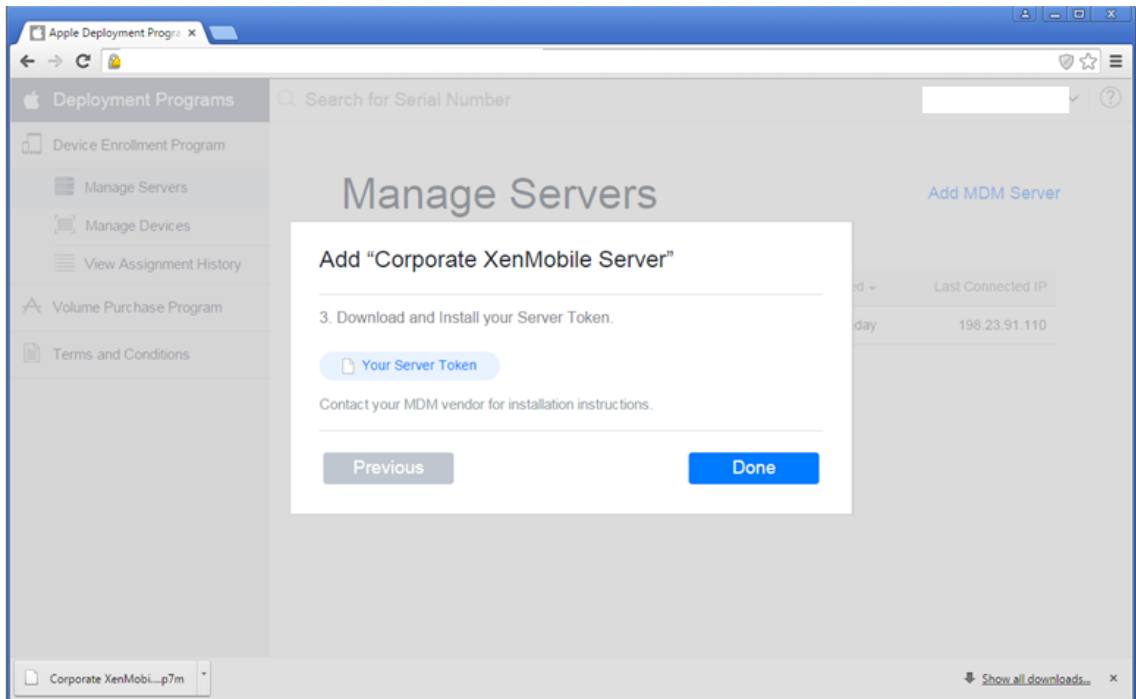
4. **Add MDM Server**(MDM 서버추가) 에서 XenMobile 서버이름을입력한후 **Next**(다음) 를클릭합니다.



5. Apple DEP 포털에서 **Choose file**(파일선택) 을클릭하고 XenMobile 에서다운로드한공개키를선택한후 **Next**(다음) 를클릭합니다.



6. **Your Server Token**(서버토큰) 을클릭하여서버토큰을생성하고브라우저에서다운로드한후 **Done**(완료) 을클릭합니다.



토큰파일을 가져오면 Apple DEP 토큰정보가 XenMobile 콘솔에 표시됩니다. 서버토큰파일은 DEP 계정을 XenMobile 에 추가할때 업로드합니다.

3 단계: XenMobile 에 DEP 계정 추가

여러개의 DEP 계정을 XenMobile 에 추가할 수 있습니다. 이 기능을 사용하면 서로 다른 등록 설정 및 설정 도우미 옵션을 국가, 부서별로 사용할 수 있습니다. 그런 다음 DEP 계정을 여러 장치 정책에 연결할 수 있습니다.

예를 들어 여러 국가에 있는 동일한 XenMobile 서버의 모든 DEP 계정을 중앙 집중화하여 모든 DEP 장치를 가져오고 감독할 수 있습니다. 등록 설정 및 설정 도우미 옵션을 부서, 조직 계층 또는 다른 구조별로 사용자 지정하면 정책을 통해 조직 전체에 적절한 기능을 제공하고 장치 사용자가 적절한 설정 지원을 받을 수 있습니다.

1. XenMobile 콘솔에서 설정 > **Apple DEP**(장치 등록 프로그램) 로 이동하고 **DEP** 계정 추가에서 추가를 클릭합니다.

Apple Device Enrollment Program (DEP)
 Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization (Business or Education) has already been created, as outlined in the [Device Enrollment Program Guide](#).

- 1 Download Public Key**
 A Public Key will be automatically generated for you and signed by Citrix.
 [Download]
- 2 Create a Server Token file**
 - Sign in to [Apple Deployment Programs Portal](#) (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
 - Navigate to [Device Enrollment Program > Manage Servers](#) in Business DEP portal or to [Devices > MDM Servers](#) in ASM portal. Click [Add MDM Server](#).
 - Enter a [MDM Server Name](#), then click [Choose File...](#) and upload your Public Key.
 - Download the Server Token file provided.
- 3 Add DEP Account**
 Follow the wizard to add the account.
 [Add]

<input type="checkbox"/>	DEP account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
<input checked="" type="checkbox"/>	ASM	citrixus1	Enabled	Education	xenmobileschool@outlook.com	21/07/2017 14:41:27	21/07/2018 21:39:48
<input type="checkbox"/>	DEP	citrixus1	Enabled	Business	CitrixXenmobileVPP@outlook.com		

Showing 1 - 2 of 2 items

2. 계정정보페이지에서다음설정을지정합니다.

XenMobile Analyze Manage Configure

Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account

DEP Account

- 1 Account Info
- 2 Server Tokens
- 3 Settings
- 4 Setup Assistant Options
- IOS

Account Info
 Specify your Apple DEP account information.

DEP account name* DEP Account US

Business unit* CITRIX SYSTEMS US (dev.paris)

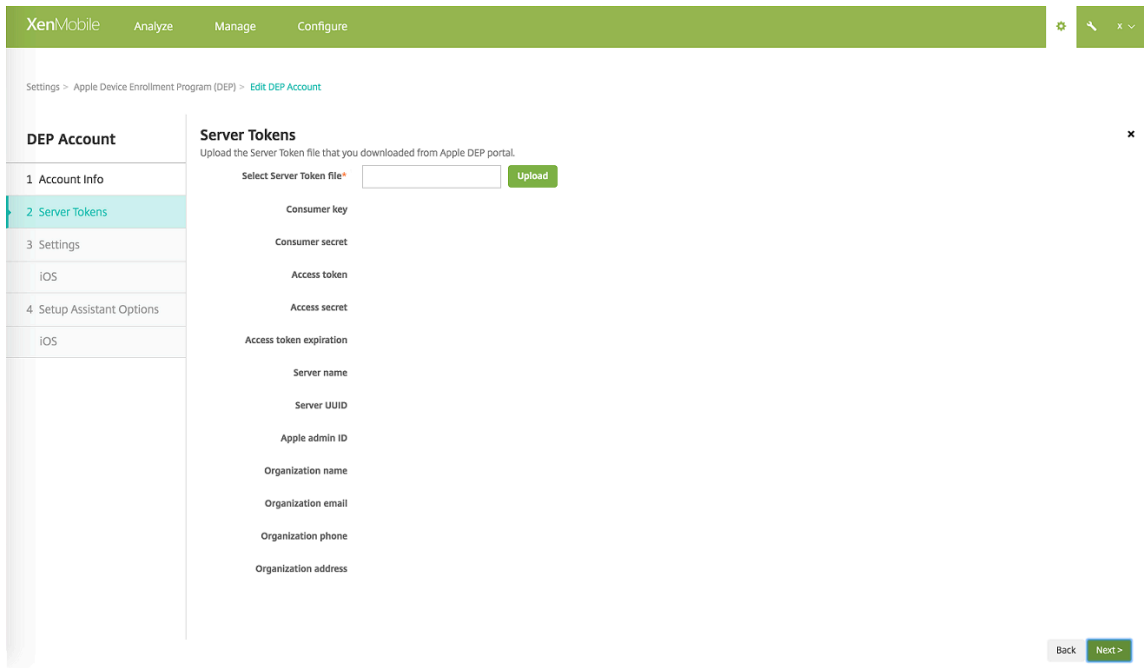
Unique service ID Santa Clara Dev

Support phone number* 408 790 8000

Support email address citrixxenmobilevpp@outlook.com

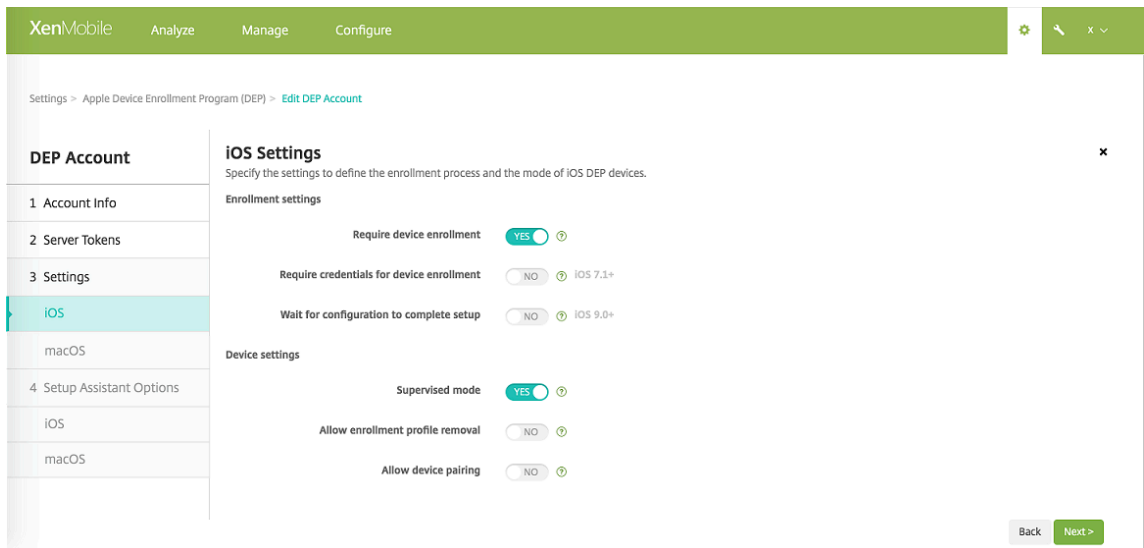
- **DEP 계정 이름:** 이 DEP 계정의 고유한 이름입니다. 국가 또는 조직 계층 구조별과 같이 DEP 계정을 구성하는 방식을 반영하는 이름을 사용합니다.
- **Business/Education unit(비즈니스/교육단위):** 장치를 할당할 비즈니스 단위 또는 부서입니다. 이것은 필수 필드입니다.
- **고유 서비스 ID:** 계정을 식별하는데 도움이 되는 선택적 고유 ID입니다.
- **지원전화번호:** 사용자가 설정 중에 전화할 수 있는 지원전화번호입니다. 이것은 필수 필드입니다.
- **지원전자메일주소:** 최종 사용자에게 제공되는 선택적 지원전자메일주소입니다.

3. 서버토큰페이지에서서버토큰파일을지정하고 업로드를클릭합니다.



서버토큰정보가 표시됩니다.

4. **iOS** 설정에서 다음 설정을 지정합니다.



등록 설정:

- **장치등록필요:** 사용자가 장치를 등록해야 하는지 여부를 설정합니다. 기본값은 예입니다.
- **장치등록에 자격증명필요:** DEP 설정 중에 사용자가 자격증명을 입력해야 하는지 여부를 설정합니다. 모든 사용자에게 장치등록 중에 자격증명을 입력하도록 요구하는 것이 좋습니다. 즉, 권한이 있는 사용자만 장치를 등록할 수 있도록 허용합니다. 기본값은 예입니다.

처음 설정할 때 DEP 를 켜고 이 옵션을 선택하지 않으면 DEP 사용자, Secure Hub, 소프트웨어 인벤토리 및 DEP 배포 그룹과 같은 DEP 구성 요소가 만들어집니다. 이 옵션을 선택하면 XenMobile 이 구성 요소를 만들지 않습니다.

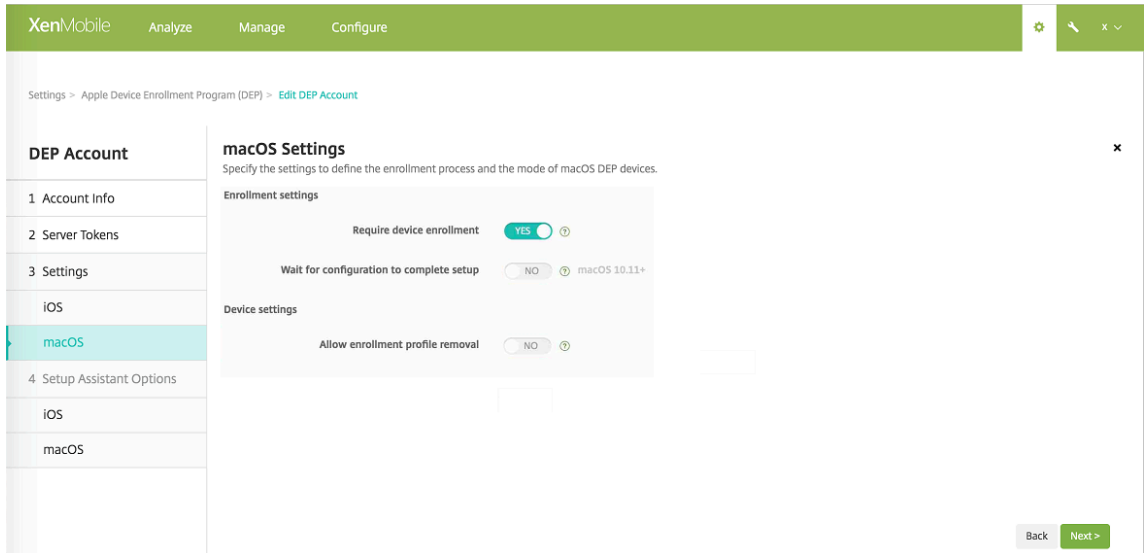
DEP 구성요소가없으므로나중에이옵션을선택취소하면자격증명을입력하지않은사용자가 DEP 등록을수행할수없습니다. DEP 구성요소를추가하려면 DEP 계정을사용하지않도록설정한다음사용하도록설정해야합니다.

- 구성에서설정을완료할때까지대기: 모든 MDM 리소스가장치에배포될때까지사용자가설정도우미모드에있어야하는지여부를설정합니다. 이옵션은감독모드의 iOS 9.0 이상장치에서사용할수있습니다. 기본값은 아니요입니다.
- Apple 설명서에따르면장치가설정도우미모드에있는동안에는다음명령이작동하지않을수있습니다.
 - InviteToProgram
 - InstallApplication
 - ApplyRedemptionCode
 - InstallMedia
 - RequestMirroring
 - DeviceLock

장치설정:

- 감독모드: Apple Configurator 를사용하여 DEP 등록장치를관리하거나 구성에서설정을완료할때까지대기를 사용하는경우 예로설정해야합니다. 기본값은 예입니다. iOS 장치의감독모드전환에대한자세한내용은Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.
- 등록프로필제거허용: 원격으로제거할수있는프로필을장치에서사용하도록할지여부를설정합니다. 기본값은 아니요입니다.
- 장치페어링허용: DEP 를통해등록한장치를 iTunes 및 Apple Configurator 를통해관리할지여부를설정합니다. 기본값은 아니요입니다.

5. macOS 설정에서다음설정을지정합니다.



등록설정:

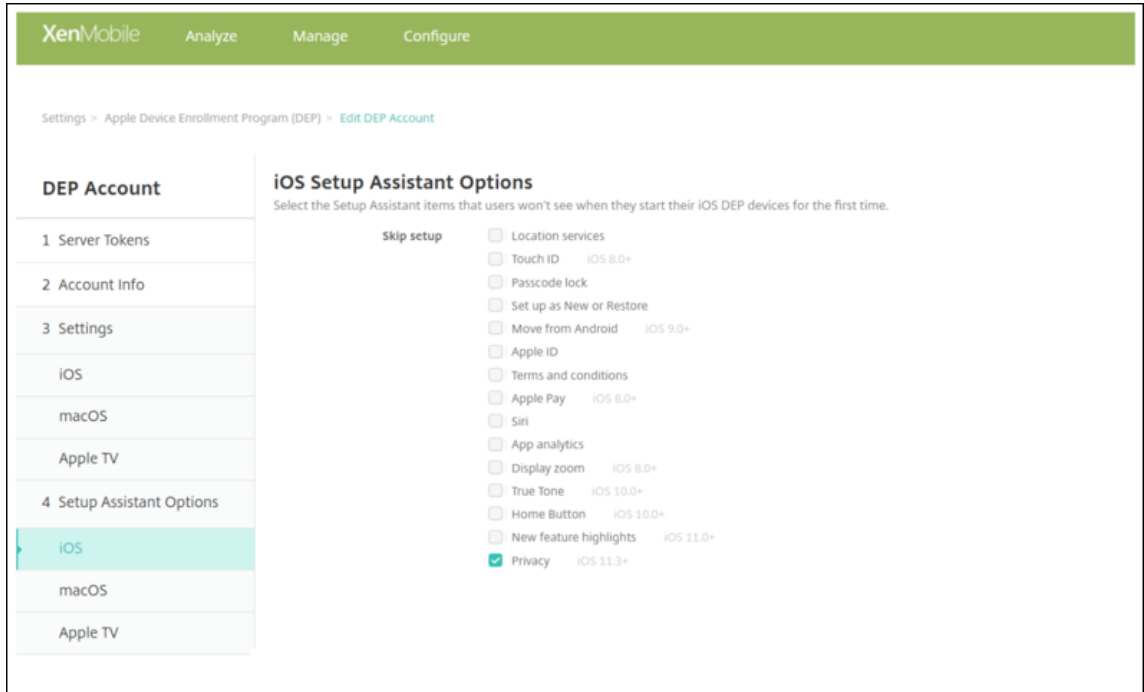
- 장치등록필요: 사용자가장치를등록해야하는지여부를설정합니다. 기본값은 예입니다.
- 구성에서설정을완료할때까지대기: 예인경우 MDM 리소스암호가장치에배포되기전까지설정도우미에서 macOS 장치가계속되지않습니다. 해당배포는로컬계정이만들어지기전에발생합니다. 이설정은 macOS 10.11 이상장치

에서사용할수있습니다. 기본값은 아니요입니다.

장치설정:

- 등록프로필제거허용: 원격으로제거할수있는프로필을장치에서사용하도록할지여부를설정합니다. 기본값은 아니요입니다.

6. **iOS** 설정도우미옵션에서사용자가장치를처음으로시작할때건너뛸 iOS 설정도우미단계를선택합니다. 모든항목에대한 기본값은선택되어있지않습니다.

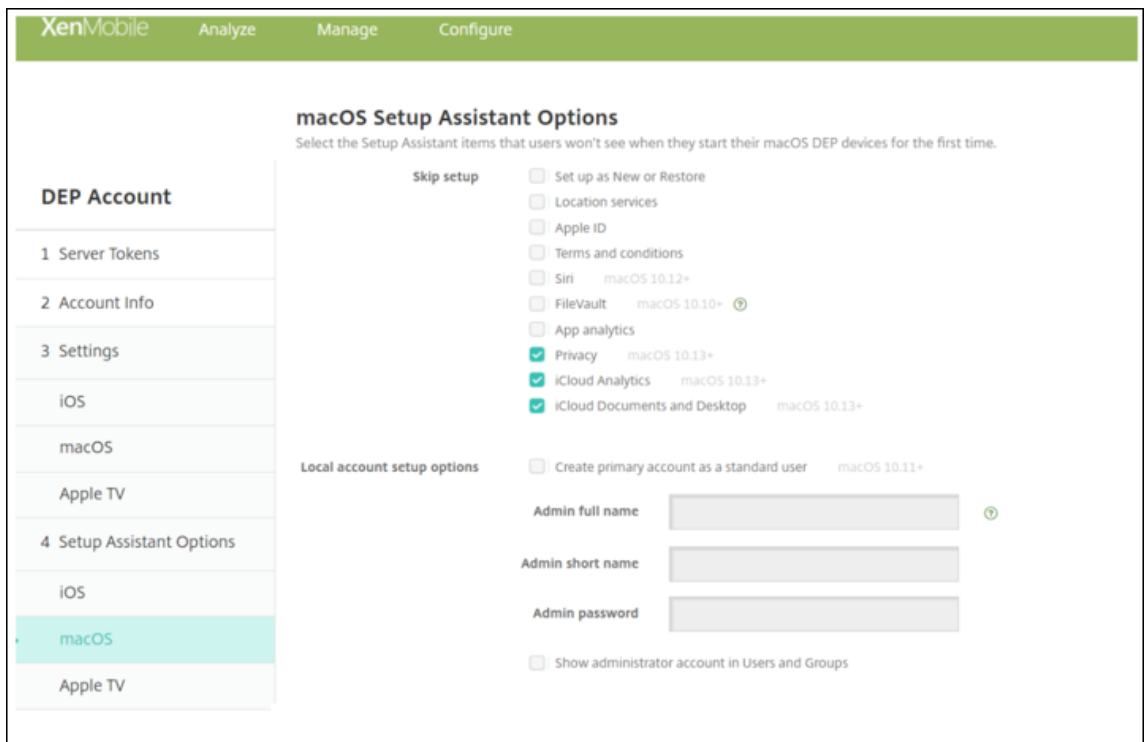


- 위치서비스: 장치에위치서비스를설정합니다.
- **Touch ID:** iOS 8.0 이상장치에서 Touch ID 를설정합니다.
- 암호잠금: 장치에대한암호를만듭니다.
- 새로설정또는복원: 장치를새로설정하거나 iCloud 또는 iTunes 백업에서복원합니다.
- **Android** 에서이동: Android 장치의데이터를 iOS 9 이상장치로전송할수있도록합니다. 이옵션은 새로설정또는복원을선택한경우에만사용할수있습니다 (즉, 단계가생략됨).
- **Apple ID:** 장치에대한 Apple ID 계정을설정합니다.
- 약관: 사용자가장치사용에대한약관에동의해야합니다.
- **Apple Pay:** iOS 8.0 이상장치에 Apple Pay 를설정합니다.
- **Siri:** 장치에서 Siri 를사용하거나사용하지않습니다.
- 앱분석: 총데이터및사용현황통계를 Apple 과공유할지여부를설정합니다.
- 표시확대/축소: iOS 8.0 이상장치에서디스플레이해상도 (표준또는확대) 를설정합니다.
- **True Tone:** iOS 10.0 장치 (최소버전) 에서 True Tone 디스플레이를설정합니다.
- 홈버튼: iOS 10.0 장치 (최소버전) 에서홈버튼화면민감도를설정합니다.
- 새로운기능하이라이트: iOS 11.0 장치 (최소버전) 에서어디서든 Dock 에접근하기와최근앱간전환이라는은보딩 정보제공용화면을설정합니다.

- **개인정보보호:** DEP 장치를 설정하는 동안 사용자에게 데이터 및 개인정보 보호 창을 표시하지 않습니다. iOS 11.3 이상에서 사용할 수 있습니다.
- **표시 형식:** DEP 장치를 설정하는 동안 사용자에게 Choose Your Look(보기 선택) 화면을 표시하지 않습니다. iOS 12.0 이상에서 사용할 수 있습니다.
- **Software Update:** DEP 장치를 설정하는 동안 사용자에게 필수 소프트웨어 업데이트 화면을 표시하지 않습니다. iOS 12.0 이상에서 사용할 수 있습니다.
- **Screen Time:** DEP 장치를 설정하는 동안 사용자에게 Screen Time(화면 시간) 화면을 표시하지 않습니다. iOS 12.0 이상에서 사용할 수 있습니다.
- **SIM Setup(SIM 설정):** DEP 장치를 설정하는 동안 사용자에게 Add Cellular Plan(데이터 요금제 추가) 화면을 표시하지 않습니다. iOS 12.0 이상에서 사용할 수 있습니다.
- **iMessage & FaceTime:** DEP 장치를 설정하는 동안 사용자에게 iMessage and FaceTime(iMessage 및 FaceTime) 화면을 표시하지 않습니다. iOS 12.0 이상에서 사용할 수 있습니다.

DEP 계정이 설정 > **Apple DEP**(장치 등록 프로그램) 에 표시됩니다.

1. **macOS** 설정 도우미 옵션에서 사용자가 장치를 처음으로 시작할 때 건너뛴 macOS 설정 도우미 단계를 선택합니다. 모든 항목에 대한 기본값은 선택되어 있지 않습니다.



- **새로 설정 또는 복원:** 장치를 새로 설정하거나 iCloud 또는 iTunes 백업에서 복원합니다.
- **위치 서비스:** 장치에 위치 서비스를 설정합니다.
- **Apple ID:** 장치에 대한 Apple ID 계정을 설정합니다.
- **약관:** 사용자가 장치 사용에 대한 약관에 동의해야 합니다.
- **Siri:** 장치에서 Siri 를 사용하거나 사용하지 않습니다.

- **FileVault:** FileVault 를 사용하여 시동 디스크를 암호화합니다. XenMobile 은 iCloud 에 로그인한 로컬 사용자 계정이거나 인 경우에만 FileVault 설정을 적용합니다.

macOS FileVault 디스크 암호화 기능으로 시스템 볼륨 콘텐츠를 암호화하여 시스템 볼륨을 보호할 수 있습니다 (<https://support.apple.com/en-us/HT204837>). FileVault 가 꺼져 있는 최신 휴대용 Mac 에서 설정도 우미를 실행하면 이 기능을 켜라는 메시지가 표시될 수 있습니다. 새 시스템과 OS X 10.10 또는 10.11 로 업그레이드한 시스템에 메시지가 표시되지만 시스템에 로컬 관리자 계정이 하나이고 이 계정으로 iCloud 에 로그인한 경우에만 표시됩니다.

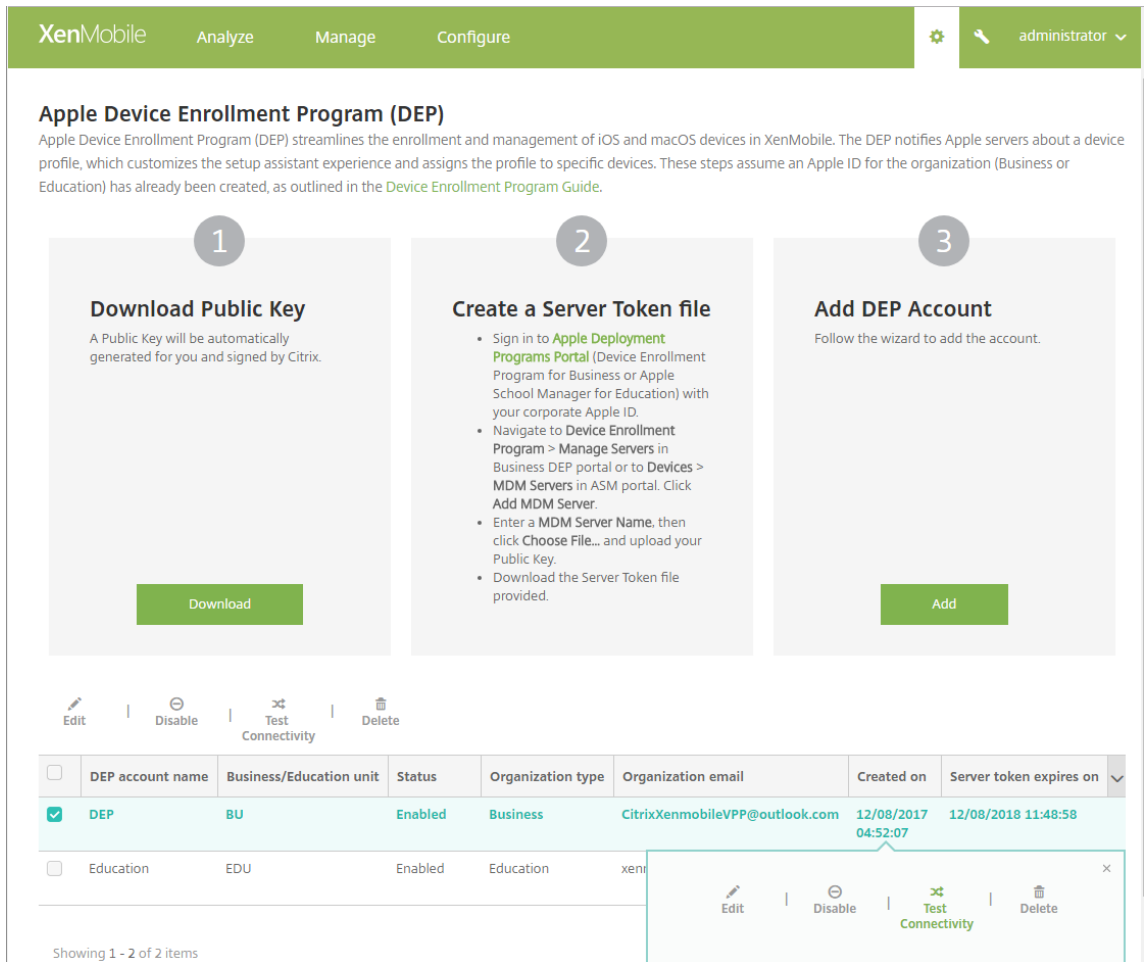
- **앱 분석:** 충돌 데이터 및 사용 현황 통계를 Apple 과 공유할지 여부를 설정합니다.
- **등록:** 사용자가 장치를 등록해야 합니다.

등록 정보 설정은 OS X 10.9 를 통해 제공되었습니다. 등록 프로세스를 수행하여 시스템 등록 정보를 Apple 에 보낼 수 있었습니다. 이 정보는 관리자의 연락처 정보를 Mac 하드웨어와 연결합니다. Apple 은 주로 이 정보를 AppleCare 지원을 용이하게 하는데 사용했습니다. 이전에 Apple ID 를 입력한 경우 설정도 우미가 관리자의 Apple ID 계정에 따라 선택적으로 등록을 제출했습니다. Apple ID 를 입력하지 않은 경우 수동으로 연락처 정보를 입력할 수 있었습니다.

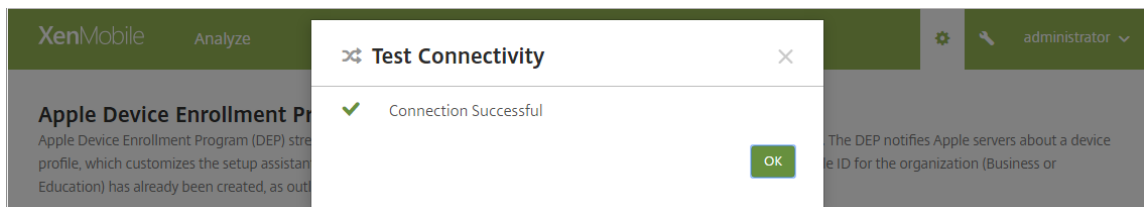
로컬 계정 설정 옵션에서 macOS 에 필요한 관리자 계정을 만들 때 사용할 설정을 지정합니다. XenMobile 이 지정된 정보를 사용하여 계정을 만듭니다.

- **개인정보 보호:** DEP 장치를 설정하는 동안 사용자에게 데이터 및 개인정보 보호 창을 표시하지 않습니다. macOS 10.13 이상에서 사용할 수 있습니다.
- **iCloud Analytics:** DEP 장치를 설정하는 동안 사용자에게 iCloud Analytics 화면을 표시하지 않습니다. macOS 10.13 이상에서 사용할 수 있습니다.
- **iCloud 문서 및 데스크톱:** DEP 장치를 설정하는 동안 사용자에게 iCloud 문서 및 데스크톱 화면을 표시하지 않습니다. macOS 10.13 이상에서 사용할 수 있습니다.
- **표시 형식:** DEP 장치를 설정하는 동안 사용자에게 Choose Your Look(보기 선택) 화면을 표시하지 않습니다. macOS 10.14 이상에서 사용할 수 있습니다.

2. XenMobile 과 Apple 간의 연결을 테스트하려면 계정을 선택하고 연결 테스트를 클릭합니다.



상태메시지가나타납니다.



DEP 계정에대한장치정책및앱의배포규칙구성

구성 > 장치정책및 구성 > 앱아래의 배포규칙색선을 사용하여 서로 다른 장치정책및 앱에 DEP 계정을 연결할 수 있습니다. 다음과 같은 정책 또는 앱을 지정할 수 있습니다.

- 특정 Apple DEP 계정에만 배포합니다.
- 선택한 계정을 제외하고 모든 Apple DEP 계정에 배포합니다.

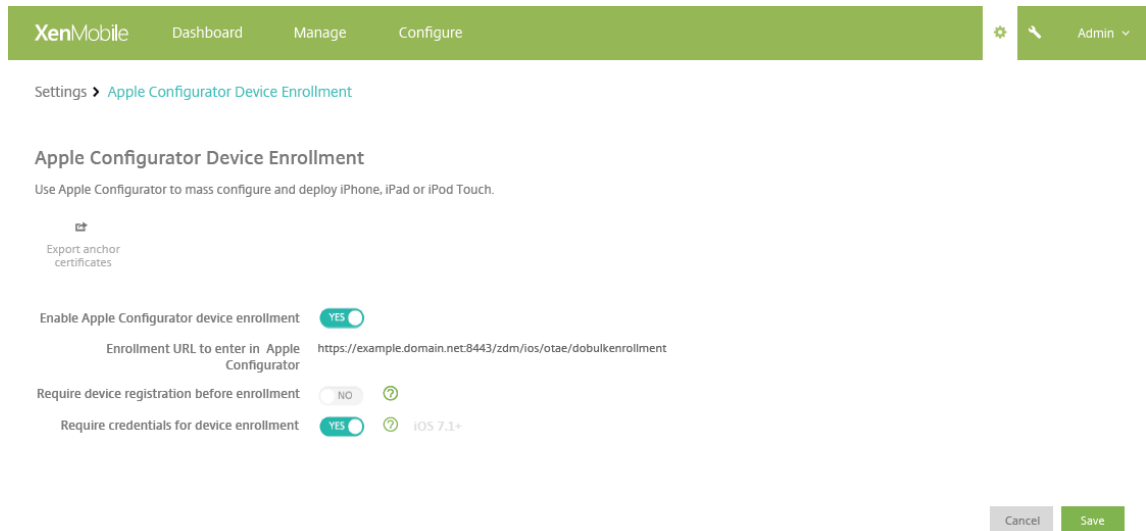
DEP 계정 목록에 상태가 사용 또는 사용 안함 상태인 계정만 포함됩니다. 사용되지 않는 DEP 계정에는 DEP 장치가 속하지 않습니다. 따라서 해당 장치에는 앱 또는 정책이 배포되지 않습니다.

다음 예에서 장치 정책은 Apple DEP 계정 이름이 “DEP Account NR” 인 장치에만 배포됩니다.

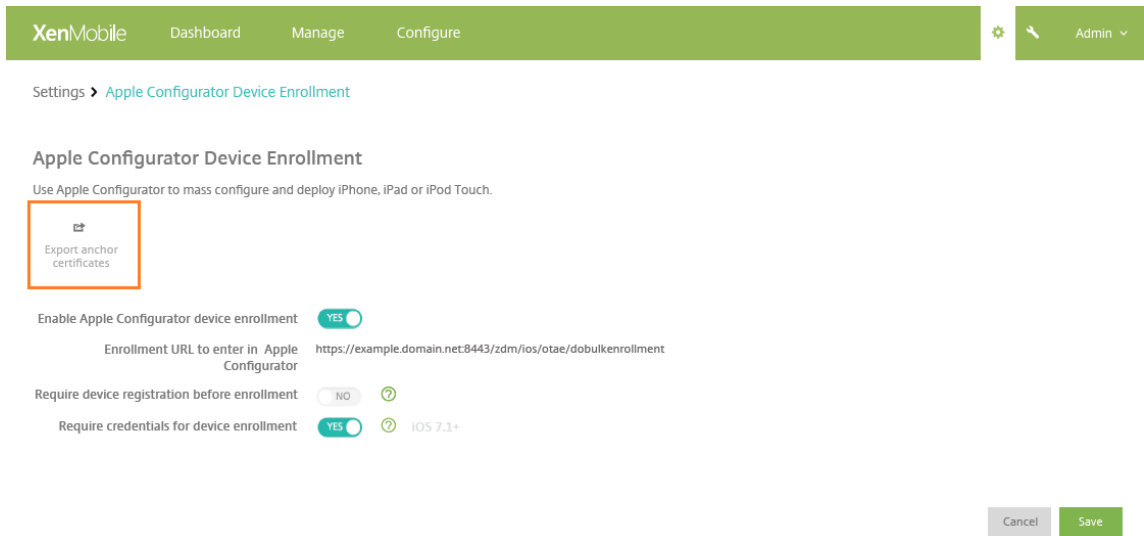
1 ![Apple DEP 설정 화면의 이미지](/ko-kr/xenmobile/server/media/apple-dep-deployment-rule-policy-example.png)

Apple Configurator 설정구성

1. XenMobile 콘솔에서 설정 > **Apple Configurator** 장치등록으로이동합니다.



2. **Apple Configurator** 장치등록허용을 예로설정합니다.
3. **Apple Configurator** 에입력할등록 URL 은읽기전용필드입니다. Apple 과통신하는 XenMobile 서버의 URL 입니다. 이단계의나중에 URL 을복사하여 Apple Configurator 에붙여넣습니다. Apple Configurator 2 에서등록 URL 은 XenMobile 서버의 FQDN(정규화된도메인이름)(예: `mdm.server.url.com`) 또는 IP 주소입니다.
4. 알수없는장치의등록을방지하려면 등록전에장치등록필요를 예로설정합니다. 참고: 이설정이 예인경우등록전에구성된장치를 XenMobile 의 관리 > 장치에수동으로추가하거나 CSV 파일을통해추가해야합니다.
5. iOS 장치사용자가등록할때자격증명을입력하도록하려면 장치등록에자격증명필요를 예로설정합니다. 기본값은등록에서 자격증명을요구하지않는것입니다.
6. 참고: XenMobile 서버에서신뢰할수있는 SSL 인증서를사용하는경우이단계를건너뛵니다. 앵커인증서내보내기를클릭하고 `certchain.pem` 파일을 macOS 키집합 (로그인또는시스템) 에저장합니다.



7. Apple Configurator 를 시작하고 준비 > 설정 > 구성설정으로 이동합니다.
8. 장치등록설정에서 4 단계의 MDM 서버 URL 을 Configurator 의 **MDM** 서버 **URL** 상자에 붙여넣습니다.
9. XenMobile 에서 신뢰할 수 있는 SSL 인증서를 사용하지 않는 경우 장치등록설정에서 루트인증기관 및 SSL 서버인증기관을 앵커인증서에 복사합니다.
10. Dock 커넥터-USB 케이블을 사용하여 Apple Configurator 를 실행하는 Mac 에 장치들을 연결하고 최대 30 개의 연결된 장치들을 동시에 구성합니다. Dock 커넥터가 없는 경우 전원선이 연결된 하나 이상의 USB 2.0 고속허브를 사용하여 장치에 연결합니다.
11. **Prepare(준비)** 를 클릭합니다. Apple Configurator 로 장치를 준비하는 방법에 대한 자세한 내용은 Apple Configurator 도움말페이지 [Prepare devices\(장치준비\)](#) 를 참조하십시오.
12. Apple Configurator 에서 필요한 장치 정책을 구성합니다.
13. 각 장치를 준비할 때 장치를 켜서 iOS 설정 도우미를 시작하면 장치를 처음으로 사용할 수 있도록 준비됩니다.

Apple DEP 를 사용하여 인증서를 갱신하거나 업데이트하려면

XenMobile SSL(Secure Sockets Layer) 인증서가 갱신되면 XenMobile 콘솔의 설정 > 인증서에서 새 인증서를 업로드합니다. 가져오기 대화상자의 용도에서 **SSL** 수신기를 클릭해야 인증서가 SSL 에 사용됩니다. 서버를 다시 시작하면 XenMobile 이 새 SSL 인증서를 사용합니다. XenMobile 의 인증서에 대한 자세한 내용은 [XenMobile 에서 인증서 업로드](#) 를 참조하십시오.

SSL 인증서를 갱신하거나 업데이트할 때 Apple DEP 와 XenMobile 간의 트러스트 관계를 다시 설정할 필요는 없습니다. 그러나 이 문서의 이전 단계에 따라 언제든지 DEP 설정을 다시 구성할 수 있습니다.

Apple DEP 에 대한 자세한 내용은 [Apple 설명서](#) 를 참조하십시오.

Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 전환

중요:

감독모드로장치를설정하면선택한버전의 iOS 가장치에설치되어이전에저장된사용자데이터또는앱이장치에서완전히초기화됩니다.

1. iTunes에서 Apple Configurator 를설치합니다.
2. Apple 컴퓨터에 iOS 장치를연결합니다.
3. Apple Configurator 를시작합니다. 감독을위해준비할장치가있다고표시됩니다.
4. 감독할장치를준비하려면:
 - **Supervision(감독) 컨트롤을 On(켜짐) 으로설정합니다.** 주기적으로구성을다시적용하여장치의제어를유지하려는경우이설정을선택하는것이 좋습니다.
 - 필요에따라장치에이름을지정합니다.
 - iOS 에서 **Latest(최신)** 를클릭하여설치할최신버전의 iOS 를검색합니다.
5. 장치를감독하도록준비할수있는상태가되면 **Prepare(준비)** 를클릭합니다.

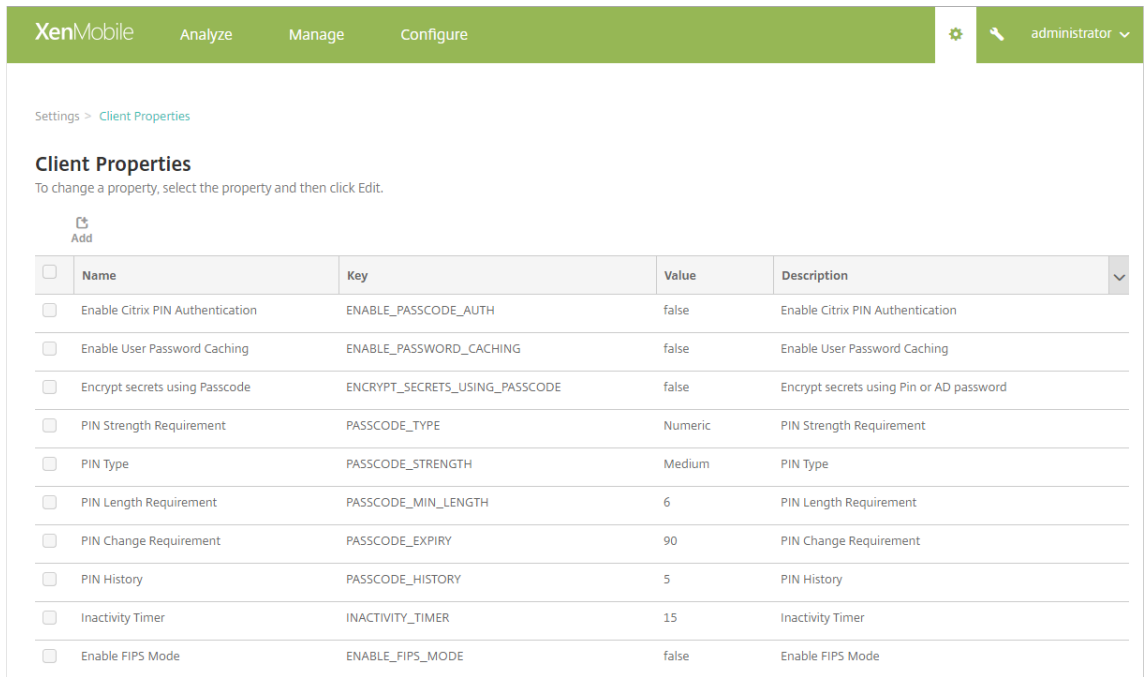
클라이언트속성

January 6, 2020

클라이언트속성은사용자장치에서 Secure Hub 에직접제공되는정보를포함합니다. 이러한속성을사용하여 Citrix PIN 같은고급설정을구성할수있습니다. Citrix 지원에서클라이언트속성을가져옵니다.

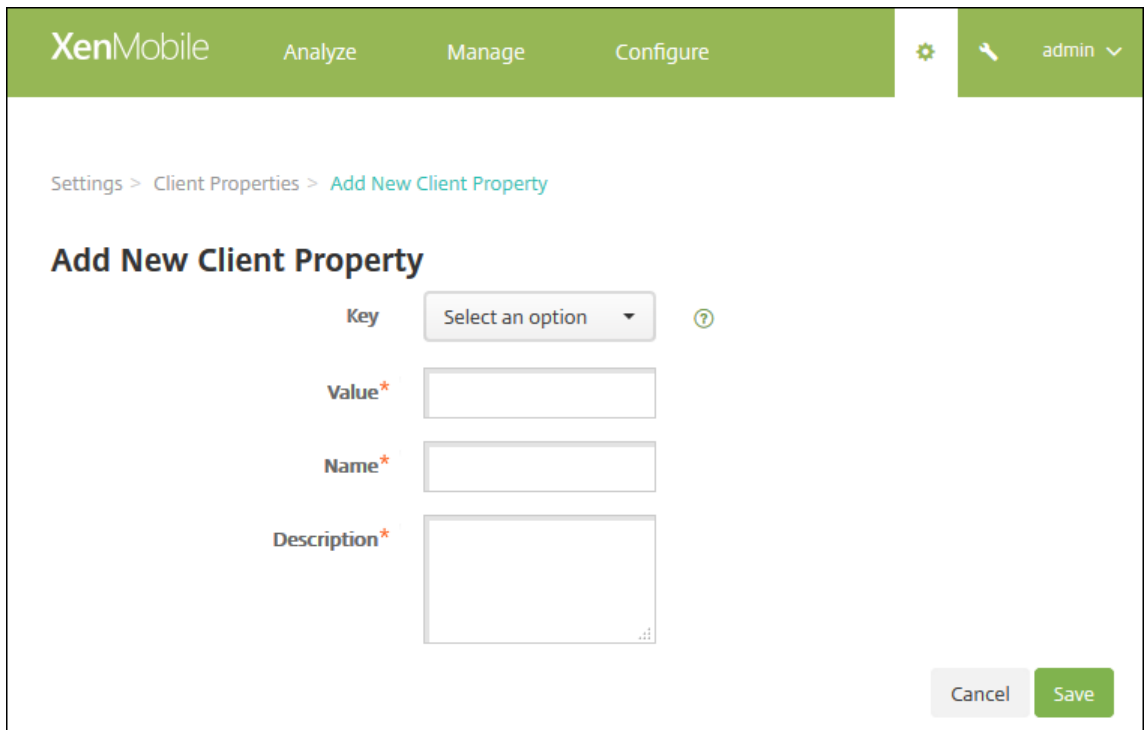
클라이언트속성은 Secure Hub 가릴리스될때마다변경될수있으며클라이언트앱의경우가끔변경될수있습니다. 보다일반적으로구성된클라이언트속성에대한자세한내용은이문서뒷부분에서클라이언트속성참조를참조하십시오.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 클라이언트에서 클라이언트속성을클릭합니다. 클라이언트속성페이지가나타납니다. 이페이지에서클라이언트속성을추가, 편집또는삭제할수있습니다.



클라이언트속성을 추가하려면

1. 추가를 클릭합니다. 새 클라이언트 속성 추가 페이지가 나타납니다.



2. 다음 설정을 구성합니다.

- 키: 목록에서추가하려는속성을클릭합니다. 중요: 이설정을업데이트하기전에 Citrix 지원에문의하십시오. 특수키를요청할수있습니다.
- 값: 선택한속성값입니다.
- 이름: 속성의이름입니다.
- 설명: 속성의설명입니다.

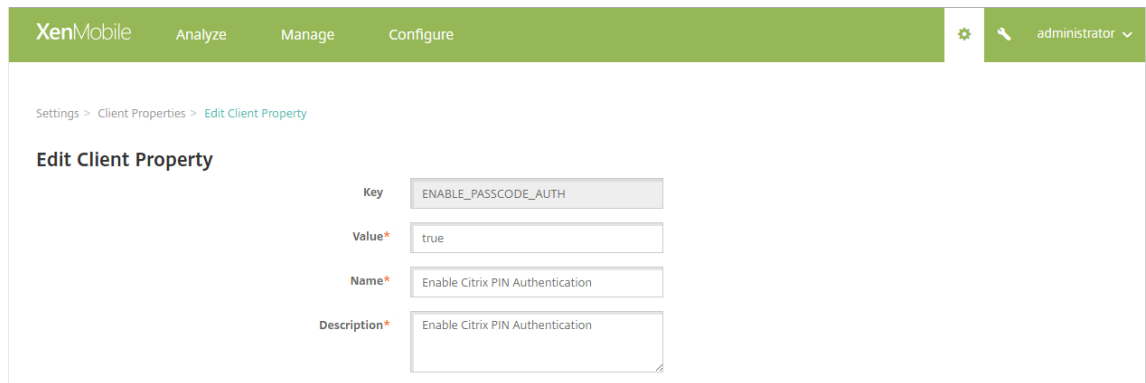
3. 저장을클릭합니다.

클라이언트속성을편집하려면

1. 클라이언트속성테이블에서편집할클라이언트속성을선택합니다.

클라이언트속성옆의확인란을선택하면서버속성목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.

2. 편집을클릭합니다. 클라이언트속성편집페이지가나타납니다.



3. 다음정보를적절하게변경합니다.

- 키: 이필드는변경할수없습니다.
- 값: 속성값입니다.
- 이름: 속성이름입니다.
- 설명: 속성설명입니다.

4. 저장을클릭하여변경내용을저장하거나 취소를클릭하여속성을변경하지않고그대로유지합니다.

클라이언트속성을삭제하려면

1. 클라이언트속성테이블에서삭제할클라이언트속성을선택합니다.

각속성옆에있는확인란을선택하여삭제할속성을둘이상선택할수있습니다.

2. 삭제를클릭합니다. 확인대화상자가나타납니다. 삭제를다시클릭합니다.

클라이언트속성참조

XenMobile 의미리정의된클라이언트속성과해당기본설정은다음과같습니다.

• CONTAINER_SELF_DESTRUCT_PERIOD

- 표시이름: MDX Container Self Destruct Period(MDX 컨테이너자체폐기기간)
- 자체폐기는지정된비활성화기간 (일) 이지난후 Secure Hub 및관리되는앱에액세스할수없도록합니다. 시간제한 후에는앱을더이상사용할수없습니다. 데이터초기화에는설치된각앱의앱데이터 (앱캐시및사용자데이터등) 를지우는작업이포함됩니다.

비활성화시간은서버가특정시간동안사용자검증을위한인증요청을수신하지않는기간을의미합니다. 예를들어이속성이 30 일인경우사용자가앱을 30 일넘게사용하지않으면정책이적용됩니다.

이글로벌보안정책은 iOS 및 Android 플랫폼에적용되며기존의앱잠금및초기화정책의향상된버전입니다.

- 이 글로벌 정책을 구성하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **CONTAINER_SELF_DESTRUCT_PERIOD** 를추가합니다.
- 값: 일수

• DEVICE_LOGS_TO_IT_HELP_DESK

- 표시이름: 장치로그를 IT 지원센터에보내기
- 이속성을사용하여 IT 지원센터로로그를보내는기능의사용여부를설정합니다.
- 가능한값: **true** 또는 **false**
- 기본값: **false**

• DISABLE_LOGGING

- 표시이름: 로깅사용안함
- 사용자가장치의로그를수집하고업로드할수없도록하려면이속성을사용합니다. 이속성은 Secure Hub 및모든설치된 MDX 앱에대한로깅을사용하지않도록설정합니다. 사용자는지원페이지에서앱의로그를전송할수없습니다. 메일작성대화상자가표시되지만로그는첨부되지않습니다. 로깅이비활성화되었다는메시지가표시됩니다. 또한이설정을사용하면 XenMobile 콘솔에서 Secure Hub 및 MDX 앱에대한로그설정을업데이트할수없습니다.

이속성을 **true** 로설정하면 Secure Hub 에서 **Block application logs**(응용프로그램로그차단) 이 **true** 로설정됩니다. 따라서새정책이적용될때 MDX 앱이로깅을중지합니다.

- 가능한값: **true** 또는 **false**
- 기본값: **false**(로깅사용)

• ENABLE_CRASH_REPORTING

- 표시이름: Enable Crash Reporting(크래시보고사용)
- **true** 인경우 Citrix 는 iOS 및 Android 용 Secure Hub 의문제를해결하는데도움이되는충돌보고서및진단을수집합니다. **false** 인경우데이터가수집되지않습니다.
- 가능한값: **true** 또는 **false**

- 기본값: **true**

• **ENABLE_CREDENTIAL_STORE**

- 표시이름: Enable Credential Store(자격증명저장소사용)
- 자격증명저장소를 사용하면 Android 또는 iOS 사용자가 모바일생산성앱에 액세스할 때 암호를 한번만 입력하면 됩니다. Citrix PIN 사용여부와 상관없이 자격증명저장소를 사용할 수 있습니다. Citrix PIN 을 사용하지 않는 경우 사용자는 Active Directory 암호를 입력합니다. XenMobile 은 Secure Hub 및 공용 스토어 앱에 대해서만 자격 증명 저장소와 함께 Active Directory 암호를 사용하도록 지원합니다. 자격 증명 저장소와 함께 Active Directory 암호를 사용하는 경우 XenMobile 에서 PKI 인증을 지원하지 않습니다.
- Secure Mail 에 자동 등록하려면 이 속성을 **true** 로 설정해야 합니다.
- 이 사용자 지정 클라이언트 정책을 구성하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **ENABLE_CREDENTIAL_STORE** 를 추가하고 값을 **true** 로 설정합니다.

• **ENABLE_FIPS_MODE**

- 표시이름: Enable FIPS Mode(FIPS 모드 사용)
- 이 속성은 모바일 장치에서 FIPS 모드의 사용 여부를 설정합니다. 값을 변경하면 Secure Hub 가 다음 번 온라인 인증을 수행할 때 새 값을 장치로 전달합니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

• **ENABLE_NETWORK_EXTENSION**

- 표시이름: ENABLE_NETWORK_EXTENSION
- 기본적으로 XenMobile 은 Secure Hub 가 설치될 때 Apple Network Extension 프레임워크를 사용하도록 설정합니다. Network Extension 을 사용하지 않도록 설정하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **ENABLE_NETWORK_EXTENSION** 을 추가하고 값을 **false** 로 설정합니다.
- 기본값: **true**

• **ENABLE_PASSCODE_AUTH**

- 표시이름: Enable Citrix PIN Authentication(Citrix PIN 인증 사용)
- 이 속성을 사용하여 Citrix PIN 기능을 활성화할 수 있습니다. Citrix PIN 또는 암호를 사용하는 경우 Active Directory 암호 대신 사용할 PIN 을 정의하라는 메시지가 나타납니다. 이 설정은 ENABLE_PASSWORD_CACHING 이 활성화되거나 XenMobile 이 인증서 인증을 사용하는 경우 자동으로 활성화됩니다.

오프라인 인증의 경우 로컬에서 Citrix PIN 의 유효성이 검사되고 사용자가 요청한 앱이나 콘텐츠에 액세스하도록 허용됩니다. 온라인 인증의 경우 Citrix PIN 또는 암호를 사용하여 Active Directory 암호 또는 인증서를 잠금 해제한 다음 이를 XenMobile 로 전송하여 인증을 수행합니다.

ENABLE_PASSCODE_AUTH 가 true 이고 ENABLE_PASSWORD_CACHING 이 false 인 경우 Secure Hub 에 암호가 저장되지 않으므로 온라인 인증 시 항상 암호 입력 메시지가 표시됩니다.

- 가능한 값: **true** 또는 **false**
- 기본값: **false**

• **ENABLE_PASSWORD_CACHING**

- 표시이름: Enable User Password Caching(사용자암호캐싱사용)
- 이속성을 사용하면 Active Directory 암호가 모바일장치에 로컬로 캐싱됩니다. 이속성을 **true** 로 설정하는 경우 **ENABLE_PASSCODE_AUTH** 속성도 **true** 로 설정해야 합니다. 사용자암호캐싱을 사용하도록 설정한 경우 Citrix PIN 또는 암호를 설정하라는 메시지가 나타납니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

• **ENABLE_TOUCH_ID_AUTH**

- 표시이름: Enable Touch ID Authentication(Touch ID 인증사용)
- Touch ID 인증을 지원하는 장치의 경우 이속성은 장치에서 Touch ID 인증의 사용 여부를 설정합니다. 요구사항:
사용자 장치가 Citrix PIN 또는 LDAP 를 사용하도록 설정되어 있어야 합니다. LDAP 인증이 해제된 경우 (예: 인증서 기반 인증만 사용되는 경우) 사용자가 Citrix PIN 을 설정해야 합니다. 이 경우 클라이언트 속성 **ENABLE_PASSCODE_AUTH** 가 **false** 인 경우에도 XenMobile 에 Citrix PIN 이 필요합니다.
사용자가 앱을 시작할 때 Touch ID 를 사용하라는 메시지에 응답해야 하도록 **ENABLE_PASSCODE_AUTH** 를 **false** 로 설정합니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **false**

• **ENABLE_WORXHOME_CEIP**

- 표시이름: Enable Worx Home CEIP(Worx Home CEIP 사용)
- 이속성은 CEIP(사용자 환경 개선 프로그램) 를 활성화합니다. 이 기능은 익명의 구성 및 사용 현황 데이터를 Citrix 에 정기적으로 전송합니다. 이 데이터는 Citrix 가 XenMobile 의 품질, 안정성 및 성능을 개선하는데 도움이 됩니다.
- 값: **true** 또는 **false**
- 기본값: **false**

• **ENABLE_WORXHOME_GA**

- 표시이름: Enable Google Analytics in Worx Home(Worx Home 에서 Google Analytics 사용)
- 이속성은 Secure Hub 에서 Google Analytics 를 사용하여 데이터를 수집하는 기능의 사용 여부를 설정합니다. 이 설정을 변경할 경우 새 값은 사용자가 다음 번에 Secure Hub(이전의 Worx Home) 에 로그인할 때 설정됩니다.
- 가능한 값: **true** 또는 **false**
- 기본값: **true**

• **ENCRYPT_SECRETS_USING_PASSCODE**

- 표시이름: Encrypt secrets using Passcode(암호를 사용하여 암호암호화)
- 이속성은 민감한 데이터를 iOS 키집합과 같은 플랫폼 기반 기본 저장소가 아닌 장치의 기밀 저장소에 저장합니다. 이속성을 사용하면 키앤티팩트의 암호화가 강화되고 사용자 엔트로피가 추가됩니다. 사용자 엔트로피는 사용자가 생성한 임의의 PIN 코드로, 이 PIN 코드는 사용자만 알고 있습니다.

사용자장치에서높은수준을보안을제공하려면이속성을활성화하는것이 좋습니다. 이경우사용자에게 Citrix PIN 에대한인증프롬프트가더많이나타납니다.

- 가능한값: **true** 또는 **false**

- 기본값: **false**

• **INACTIVITY_TIMER**

- 표시이름: Inactivity Timer(비활성타이머)

- 이속성은사용자가장치를비활성상태로둔후에 Citrix PIN 또는암호를입력하라는메시지없이앱에액세스할수있는 시간을정의합니다. MDX 앱에대해이설정을사용되도록설정하려면앱암호설정을켜짐으로설정합니다. 앱암호설정이꺼짐으로설정된경우, 사용자는전체인증을수행하기위해 Secure Hub 로리디렉션됩니다. 이설정을변경하면다음에사용자에게인증하라는메시지가표시될때값이적용됩니다.

iOS 에서비활성타이머는 MDX 및비 MDX 앱의 Secure Hub 액세스권한도제어합니다.

- 가능한값: 양의정수

- 기본값: **15** 분

• **ON_FAILURE_USE_EMAIL**

- 표시이름: On failure Use Email to Send device logs to IT help desk(장애시전자메일을사용하여장치 로그를 IT 지원센터에보내기)

- 이속성은전자메일을사용하여 IT 에장치로그를보내는기능의사용여부를설정합니다.

- 가능한값: **true** 또는 **false**

- 기본값: **true**

• **PASSCODE_EXPIRY**

- 표시이름: PIN Change Requirement(PIN 변경요구사항)

- 이속성은 Citrix PIN 또는암호가유효한기간을정의합니다. 이기간이 지나면사용자가 Citrix PIN 또는암호를변경하도록강제합니다. 이설정을변경하면현재 Citrix PIN 또는암호가만료된경우에만새값이설정됩니다.

- 가능한값: **1 ~ 99**(권장) 입니다. PIN 재설정을 제거하려면 값을 매우 높은 숫자로 설정합니다 (예: 100,000,000,000). 원래만료기간을 1 일에서 99 일사이로설정할경우해당기간동안이기간을큰수로변경하면 PIN 은초기기간이끝날때만료되지만이후에는다시만료되지않습니다.

- 기본값: **90** 일

• **PASSCODE_HISTORY**

- 표시이름: PIN History(PIN 기록)

- 이속성은사용자가 Citrix PIN 또는암호를변경할때재사용할수없는이전에사용된 Citrix PIN 또는암호의수를정의합니다. 이설정을변경하면새값은다음번에사용자가 Citrix PIN 또는암호를재설정할때설정됩니다.

- 가능한값: **1~99**

- 기본값: **5**

• **PASSCODE_MAX_ATTEMPTS**

- 표시이름: PIN Attempts(PIN 시도횟수)
- 이속성은전체인증메시지를표시하기전에사용자가시도할수있는잘못된 Citrix PIN 또는암호횟수를정의합니다. 사용자가전체인증을성공적으로수행하면 Citrix PIN 또는암호를만들라는메시지가표시됩니다.
- 가능한값: 양의정수
- 기본값: **15**

• **PASSCODE_MIN_LENGTH**

- 표시이름: PIN Length Requirement(PIN 길이요구사항)
- 이속성은 Citrix PIN 의최소길이를정의합니다.
- 가능한값: **4 ~ 10**
- 기본값: **6**

• **PASSCODE_STRENGTH**

- 표시이름: PIN Strength Requirement(PIN 강도요구사항)
- 이속성은 Citrix PIN 또는암호의강도를정의합니다. 이설정을변경하면사용자가다음번에인증을수행할때 Citrix PIN 또는암호를생성하라는메시지가나타납니다.
- 가능한값: **Low(낮음), Medium(중간) 또는 Strong(강함)**
- 기본값: **Medium(중간)**
- PASSCODE_TYPE 설정을기반으로각강도설정에대한암호규칙은다음과같습니다.

숫자암호에대한규칙:

암호강도	숫자암호유형에대한규칙	허용	허용안함
Low(낮음)	모든숫자, 모든순서가허용됨	444444, 123456, 654321	
Medium(중간)(기본설정)	모든숫자가동일하거나연속해서는안됩니다.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
High(높음)	중간암호강도와동일합니다.		
Strong(강함)	중간암호강도와동일합니다.		

영숫자암호에대한규칙:

암호강도	영숫자암호유형에대한규칙	허용	허용안함
Low(낮음)	하나이상의숫자와하나의문자가있어야합니다.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef

암호강도	영숫자암호유형에대한규칙	허용	허용안함
Medium(중간)(기본설정)	낮음암호강도에대한규칙에 더해문자와모든숫자가동일해서는안됩니다. 문자가연속해서는안되며숫자가연속해서는안됩니다.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, or cba123
High(높음)	최소한대문자하나와소문자 하나를포함해야합니다.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Strong(강함)	최소한숫자하나, 특수기호 하나, 대문자하나및소문자 하나를포함해야합니다.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgH12, jkrtA2

• **PASSCODE_TYPE**

- 표시이름: PIN Type(PIN 유형)
- 이속성은사용자가숫자 Citrix PIN 또는영숫자암호를정의할수있는지여부를정의합니다. **Numeric(숫자)** 를선택하면사용자가숫자만 (Citrix PIN) 사용할수있습니다. **Alphanumeric(영숫자)** 를선택하면사용자가문자와 숫자조합 (암호) 을사용할수있습니다.
이설정을변경하면사용자가다음번에인증을수행할때새 Citrix PIN 또는암호를설정해야합니다.
- 가능한값: **Numeric(숫자)** 또는 **Alphanumeric(영숫자)**
- 기본값: **Numeric(숫자)**

• **REFRESHINTERVAL**

- 표시이름: REFRESHINTERVAL
- 기본적으로 XenMobile 은 3 일마다고정된인증서에대해 ADS(자동검색서버) 에 ping 을수행합니다. 새로고침 간격을변경하려면 설정 > 클라이언트속성으로이동한다음사용자지정키 **REFRESHINTERVAL** 를추가하고 값을숫자 (시간) 로설정합니다.
- 기본값은 **72** 시간 (3 일) 입니다.

• **SEND_LDAP_ATTRIBUTES**

- Android, iOS 또는 macOS 장치의 MAM 전용배포의경우, 전자메일자격증명으로 Secure Hub 에등록한사용자가자동으로 Secure Mail 에등록되도록 XenMobile 을구성할수있습니다. 이렇게하면사용자가추가정보를 제공하거나추가단계를수행하지않고 Secure Mail 에등록할수있습니다.
- 이글로벌클라이언트정책을구성하려면 설정 > 클라이언트속성으로이동한다음사용자지정키 **SEND_LDAP_ATTRIBUTES** 를추가하고 값을다음과같이설정합니다.
- 값: `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${`

```
user.mail }
```

- 속성값은 MDM 정책과 유사하게 매크로로 지정됩니다.
- 다음은 이 속성의 샘플 계정 서비스 응답입니다.

```
<property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,email=user@site.com\,user@site.com" name="SEND_LDAP_ATTRIBUTES"/>
```

- 이 속성의 경우 XenMobile 은 심표문자를 문자열 종결자로 취급합니다. 그러므로 특성값에 심표가 포함되는 경우 그 앞에 백슬래시를 추가해야 합니다. 백슬래시를 추가하면 클라이언트가 포함된 심표를 특성값의 끝으로 해석하지 않습니다. 백슬래시 문자는 "`\\`"로 표현합니다.

• HIDE_THREE_FINGER_TAP_MENU

- 이 속성이 설정되지 않거나 **false** 로 설정된 경우 사용자가 장치에서 세 손가락 누르기를 수행하여 숨겨진 기능 메뉴에 액세스할 수 있습니다. 숨겨진 기능 메뉴를 사용하면 사용자가 응용 프로그램 데이터를 재설정할 수 있습니다. 이 속성을 **true** 로 설정하면 사용자가 숨겨진 기능 메뉴에 액세스할 수 없습니다.
- 이 글로벌 클라이언트 정책을 구성하려면 설정 > 클라이언트 속성으로 이동하고 사용자 지정 키 **HIDE_THREE_FINGER_TAP_MENU** 를 추가한 다음 값을 설정합니다.

• TUNNEL_EXCLUDE_DOMAINS

- 표시 이름: Tunnel Exclude Domains
- 기본적으로 MDX 는 Micro VPN 터널링에서 XenMobile SDK 및 앱이 여러 기능에서 사용하는 일부 서비스 끝점을 제외합니다. 예를 들어 이러한 끝점에는 Google Analytics, Citrix Cloud Services, Active Directory 서비스 등 엔터프라이즈 네트워크를 통한 라우팅이 필요하지 않은 서비스가 포함됩니다. 제외되는 도메인의 기본 목록을 재정의하려면 클라이언트 속성을 사용합니다.
- 이 글로벌 클라이언트 정책을 구성하려면 설정 > 클라이언트 속성으로 이동한 다음 사용자 지정 키 **TUNNEL_EXCLUDE_DOMAINS** 를 추가하고 값을 설정합니다.
- 값: 터널링에서 제외할 도메인으로 기본 목록을 바꾸려면 심표로 구분된 도메인 접미사 목록을 입력합니다. 터널링에 모든 도메인을 포함하려면 **none** 을 입력합니다. 기본값은 다음과 같습니다.

```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net ,mobile.launchdarkly.com,pushreg.xml.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com
```

Apple DEP 를 통해 iOS 및 macOS 장치 배포

August 23, 2019

Apple 에는 비즈니스 및 교육 계정을 위한 장치 등록 프로그램이 있습니다. 비즈니스 계정의 경우 XenMobile 에서 Apple DEP(장치 등록 프로그램) 를 사용하여 장치를 등록하고 관리하려면 Apple 배포 프로그램에 등록해야 합니다. 이 프로그램은 iOS 및 macOS 장치를 위한 것입니다. 비즈니스용 Apple 배포 프로그램 계정 등록에 대한 자세한 내용은 Apple 의 [이 PDF](#) 를 참조하십시오.

Apple Deployment Program 은 조직을 위한 프로그램이며 개인 사용자는 사용할 수 없습니다. Apple Deployment Program 계정을 만들려면 해당 양의 회사 세부 정보를 제공해야 합니다. 계정을 요청하고 승인을 받는 데 시간이 걸릴 수 있습니다.

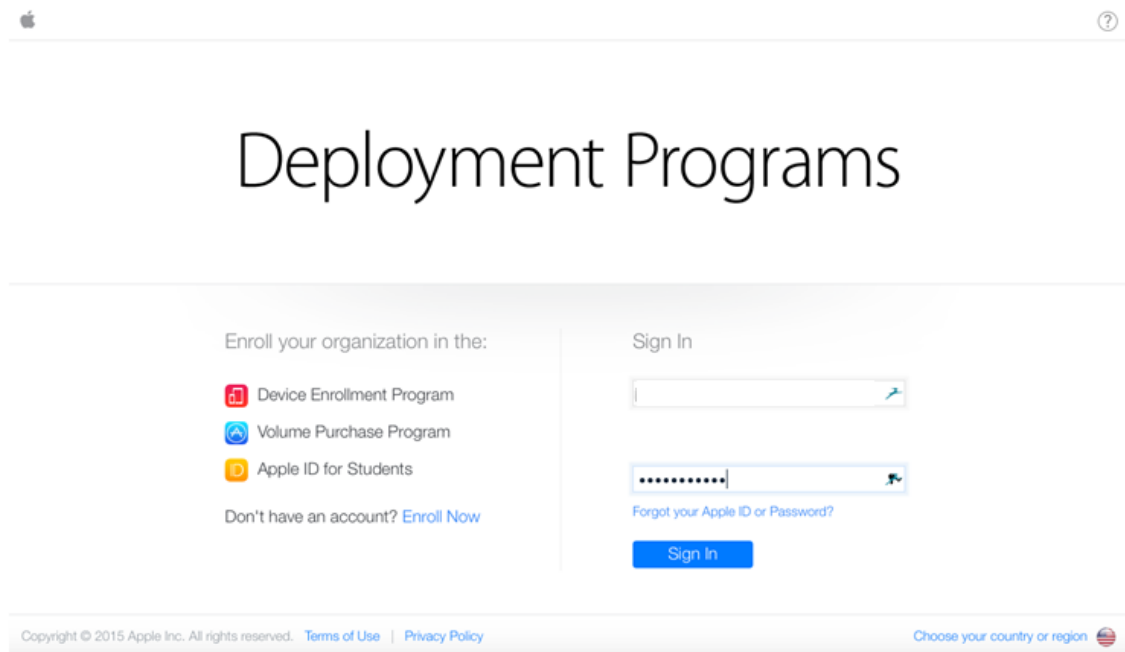
교육 계정의 경우 Apple School Manager 계정을 생성합니다. Apple School Manager 는 DEP(장치 등록 프로그램) 와 VPP(Volume Purchase Program) 를 통합합니다. Apple School Manager 는 교육 DEP 의 한 유형입니다. Apple School Manager 계정을 생성하려면 <https://school.apple.com/> 으로 이동합니다.

Apple 배포 프로그램 등록

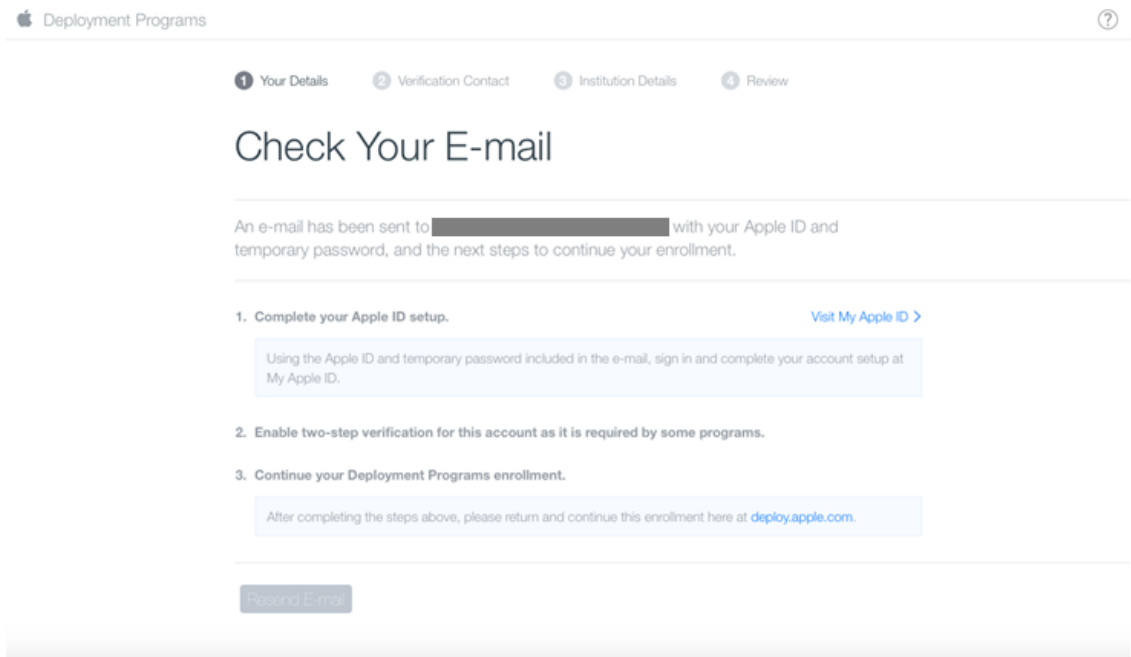
1. deploy.apple.com 으로 이동하여 Apple 배포 프로그램 계정을 신청합니다. DEP 계정을 신청할 때는 조직의 전자 메일 주소 (예: dep@company.com) 를 사용하는 것이 가장 좋습니다.

참고:

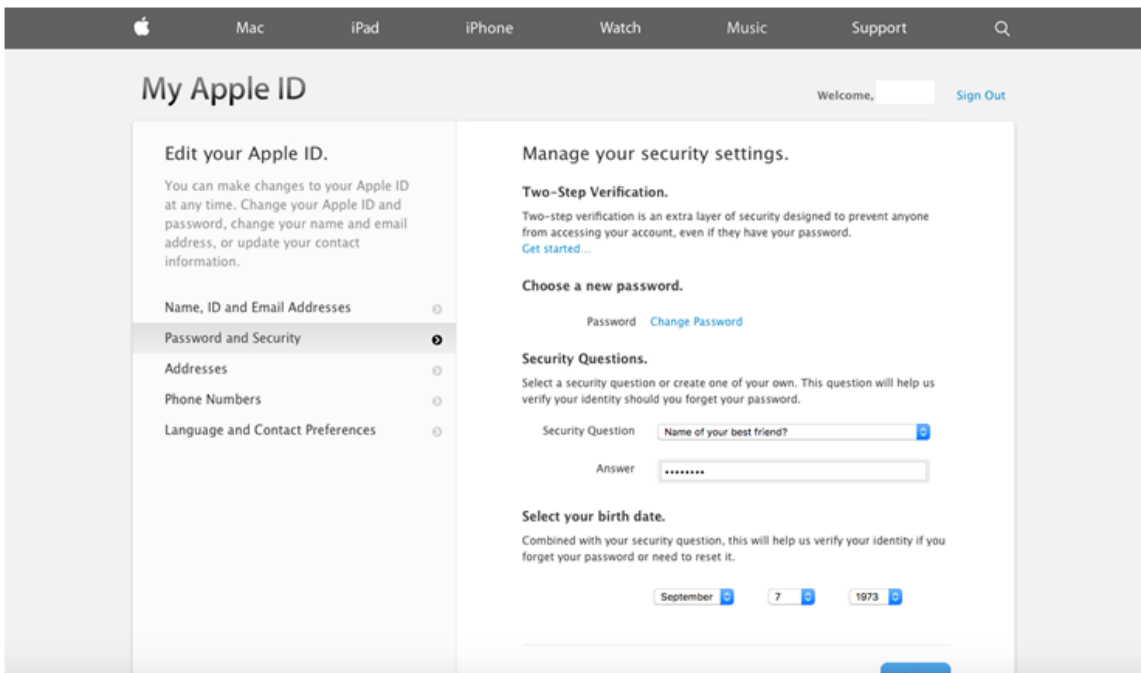
교육용 계정인 경우 <https://school.apple.com/> 으로 이동하십시오.



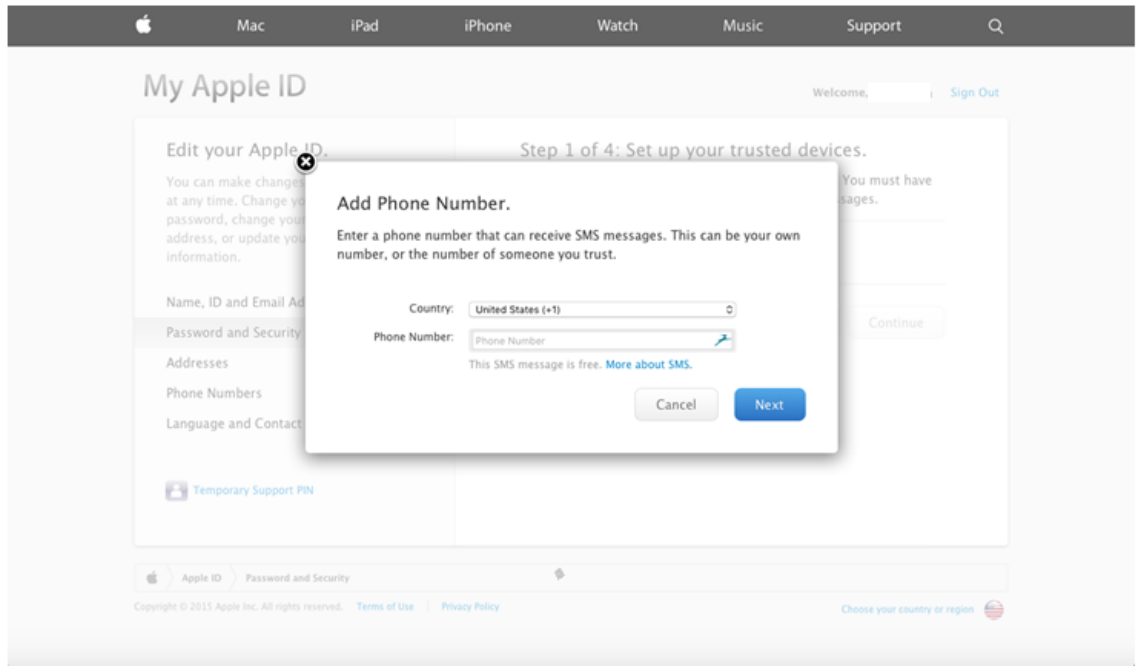
2. 조직 정보를 입력한 후 새 Apple ID 에 대한 임시 암호가 전자 메일을 통해 전송됩니다.



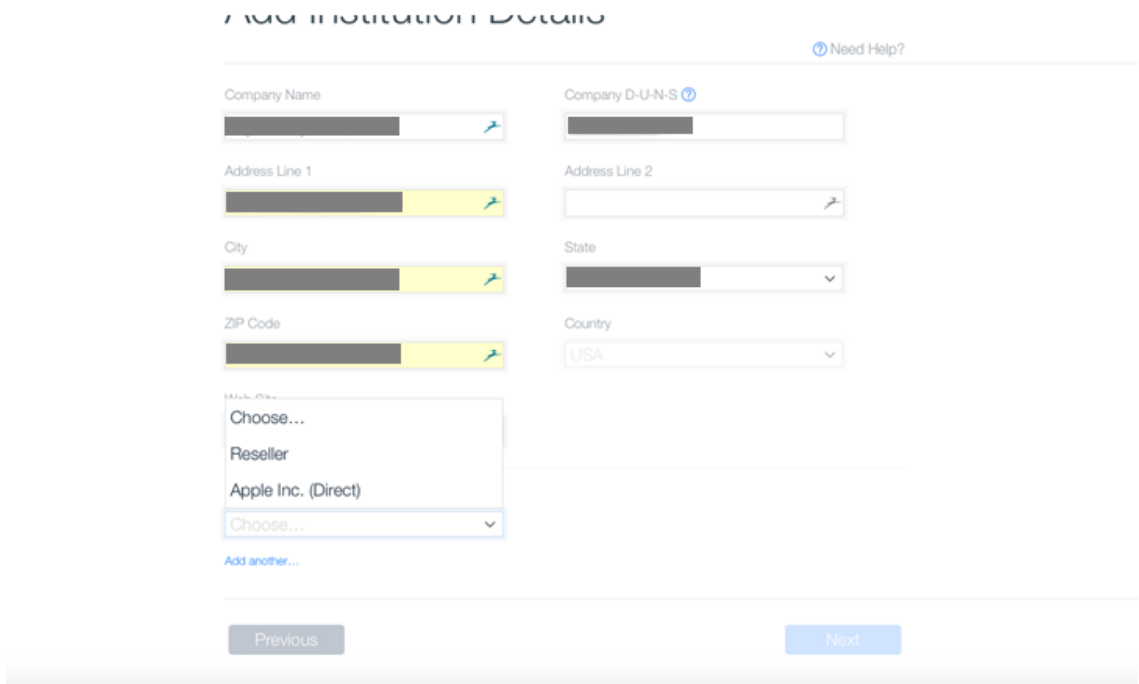
3. Apple ID 로그인하고계정의보안설정을완료합니다.



4. DEP 포털에서사용해야하는 2 단계인증을구성하고사용하도록설정합니다. 이단계에서전화번호를추가하면 2 단계인증에사용할 4 자리 PIN 을받게됩니다.



5. DEP 포털에 로그인하고 앞서 설정한 2 단계 인증을 사용하여 계정 구성을 완료합니다.
6. 회사 세부 정보를 추가한 후 장치를 구입한 위치를 선택합니다. 구입 옵션에 대한 자세한 내용은 다음 섹션인 DEP 지원 장치 주문을 참조하십시오.



7. Apple 고객 번호 또는 DEP 리셀러 ID 를 추가한 후 등록 세부 정보를 확인하고 Apple 이 계정을 승인할 때까지 기다립니다.

ADD INSTITUTION DETAILS

[Need Help?](#)

Company Name	Company D-U-N-S
Address Line 1	Address Line 2
City	State
ZIP Code	Country
Web Site	
Devices Purchased From	DEP Reseller ID
Reseller	CDW

[Add another...](#)

[Previous](#) [Next](#)

Deployment Programs

1 Your Details 2 Verification Contact 3 Institution Details 4 Review

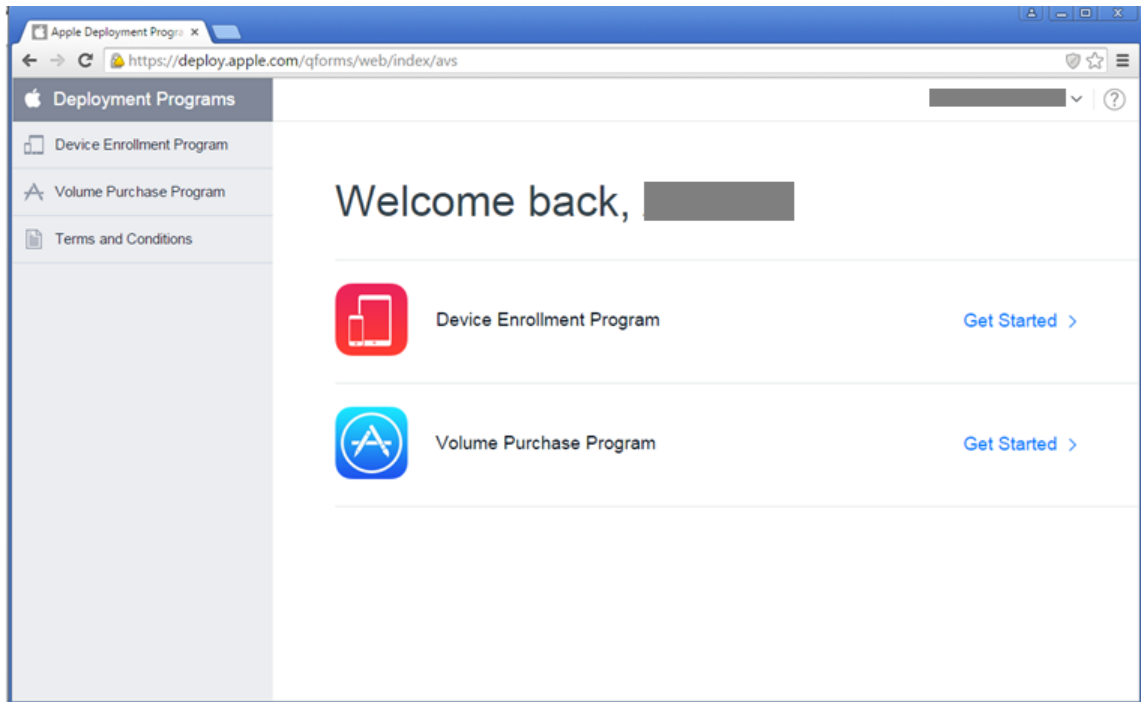
Review Your Enrollment Details

[Need Help?](#)

Your Details	Verification Contact	Institution Details
Your Name	Verification Contact Name	Company Name
Your Work E-mail	Verification Contact Work E-mail	Web Site
Your Work Phone	Verification Contact Work Phone	Address
Your Title / Position General Manager	Title / Position General Manager	Devices Purchased From

[Edit](#) [Submit](#)

8. Apple 로부터로그온자격증명을받은후 Apple DEP 포털에로그인합니다.



XenMobile 에계정을연결하려면 iOS 및 macOS 장치의대량등록에서 “Apple DEP 계정과 XenMobile 통합” 을참조하십시오.

DEP 지원장치주문

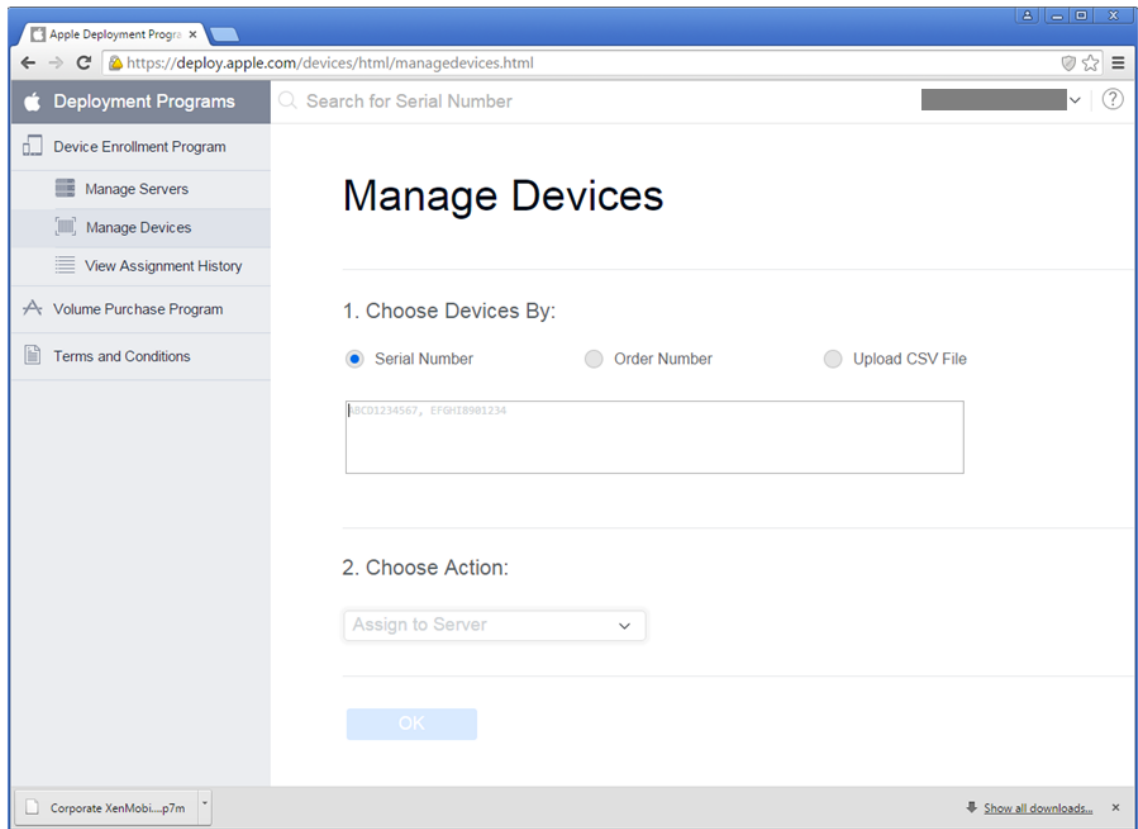
Apple 또는 DEP 지원공인리셀러또는통신사에서직접 DEP 지원장치를주문할수있습니다. Apple 에서주문하려면 Apple DEP 포털에서 Apple Customer ID(Apple 고객 ID) 를제공합니다. 고객 ID 를통해구입한장치가 Apple DEP 계정과연결될수있습니다.

리셀러또는이동통신사업자에서주문하려면 Apple 리셀러또는이동통신사업자에연락하여 Apple DEP 에참여하는지여부문의해야합니다. 장치를구입할때리셀러의 Apple DEP ID 를요청하십시오. Apple DEP 리셀러를 Apple DEP 계정에추가할때이정보가필요합니다. 리셀러의 Apple DEP ID 를추가한후 DEP 고객 ID 를받게됩니다. DEP 고객 ID 를리셀러에게제공하면리셀러에서이 ID 를사용하여장치구매정보를 Apple 에제출합니다. 자세한내용은 [Apple 웹사이트](#)를참조하십시오.

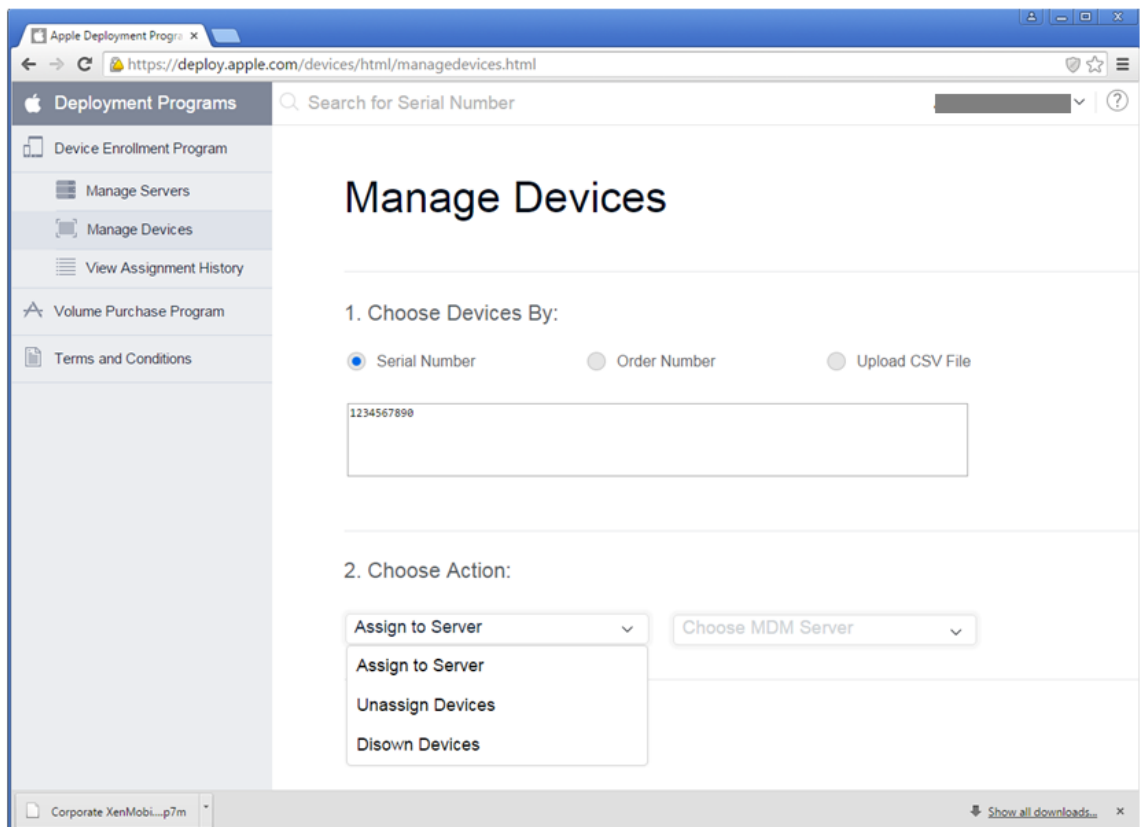
DEP 지원장치관리

DEP 포털을사용하여 Apple DEP 계정을업데이트하려면다음단계에따라 XenMobile Server 에장치를연결합니다.

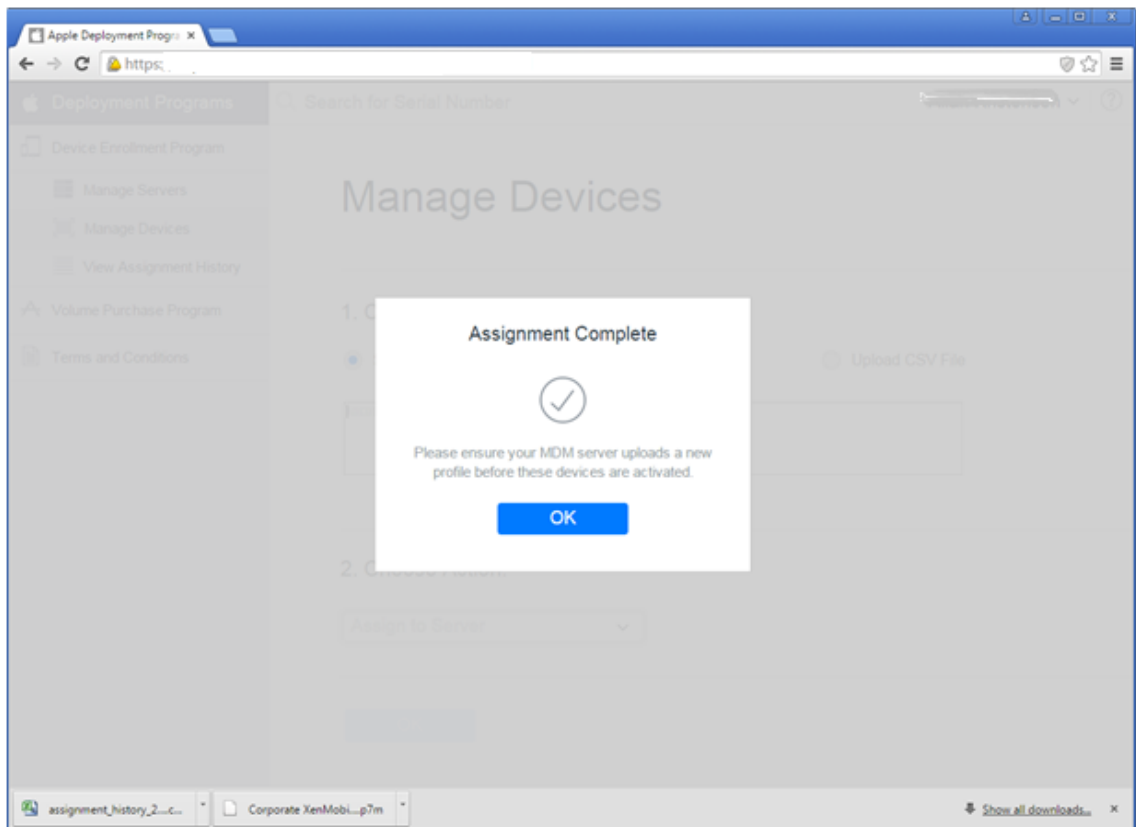
1. Apple DEP 포털에로그온합니다.
2. **Device Enrollment Program**(장치등록프로그램) 을클릭한다음 **Manage Devices**(장치관리) 를클릭합니다. **Choose Devices By**(장치기준선택) 에서 Apple DEP 지원장치를업로드하고정의할때사용할옵션 (**Serial Number**(일련번호), **Order Number**(주문번호) 또는 **Upload CSV File**(CSV 파일업로드)) 을선택합니다.



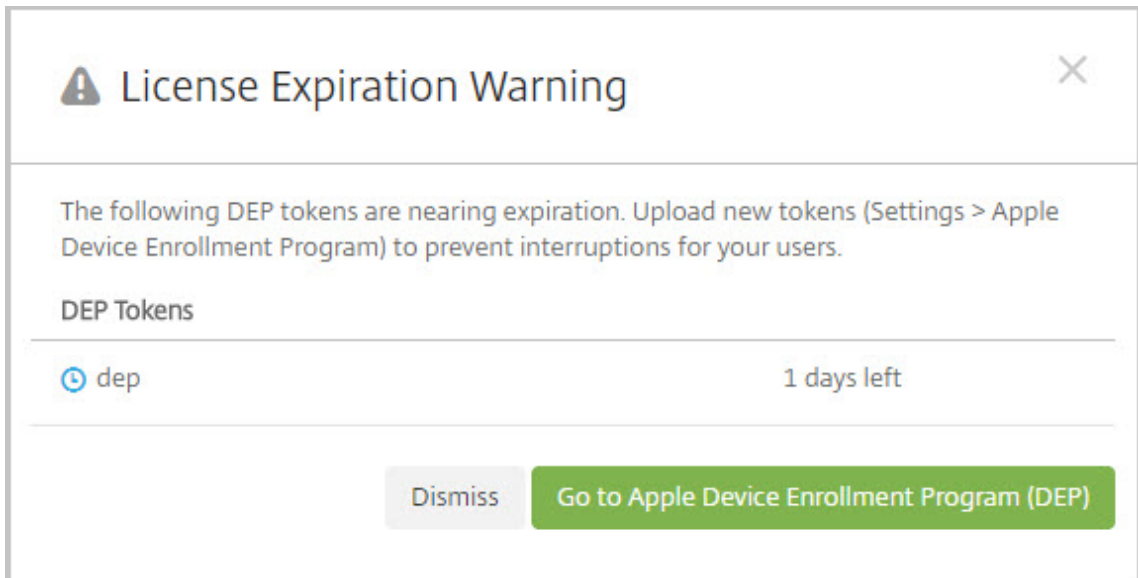
3. 장치를 XenMobile Server 에 할당하려면 **Choose Action**(작업선택) 에서 **Assign to Server**(서버에 할당) 를 선택합니다. 목록에서 XenMobile Server 의 이름을 선택합니다. **OK**(확인) 를 클릭합니다.



이제 Apple DEP 장치가선택한 XenMobile Server 에연결됩니다.



Apple DEP 토큰의 만료일이 가까워지거나 만료된 경우 XenMobile 이라이센스 만료 경고를 표시합니다.



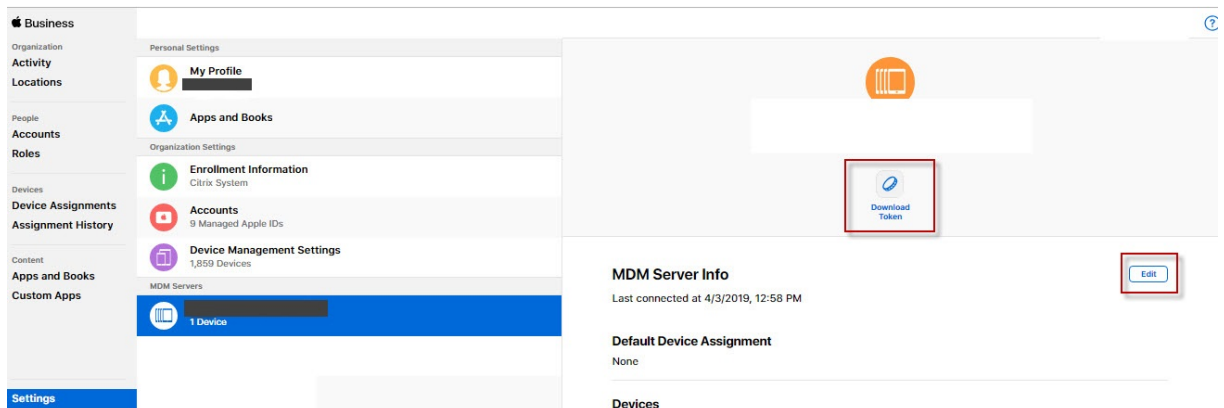
Apple 배포프로그램등록갱신

1 단계: XenMobile 서버에서공개키를다운로드

1. XenMobile 콘솔에서 설정 > **Apple DEP**(장치등록프로그램) 로이동하여새공개키를다운로드합니다.

2 단계: Apple 계정에서서버토큰파일을만들고다운로드

1. [Apple Deployment Program Portal](#)(Apple 배포프로그램포털)에로그인하여토큰을갱신합니다.
2. 설정 > **MDM Server Info**(MDM 서버정보) 를열고 편집을클릭합니다. XenMobile 에서다운로드한새공개키를업로드하고변경사항을저장합니다.
3. 설정으로돌아가서새토큰을다운로드합니다.



3 단계: XenMobile 에서서버토큰파일업로드

1. XenMobile 에서 설정 > **Apple DEP**(장치등록프로그램) 로이동합니다. DEP 계정을선택하고 편집을클릭한다음서버토큰파일을업로드합니다.
2. 다음을클릭하고변경사항을저장합니다.

Apple DEP 지원장치등록시사용자환경

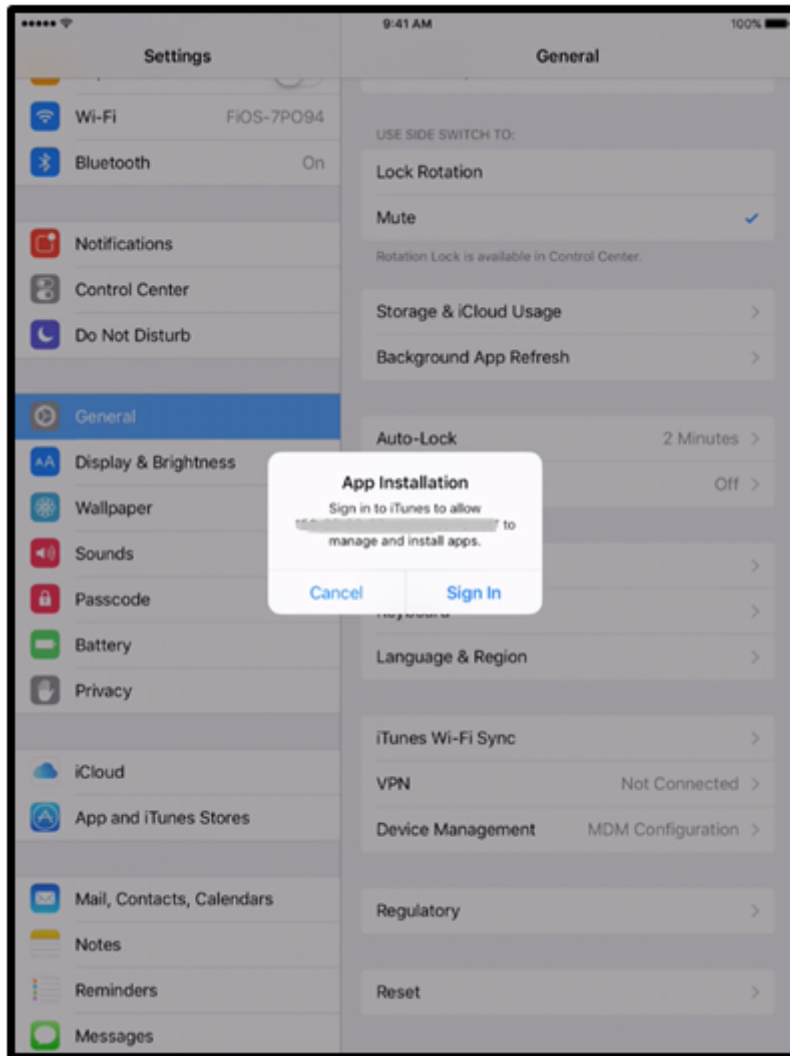
Apple DEP 지원장치를등록할때의사용자환경은다음과같습니다.

1. 사용자가 Apple DEP 지원장치를시작합니다.
2. XenMobile 은 XenMobile 콘솔에서구성한 Apple DEP 구성을 Apple DEP 지원장치에제공합니다.
3. 사용자가장치에서초기설정을구성합니다.
4. 장치에서 XenMobile 장치등록프로세스가자동으로시작됩니다.

5. 사용자가장치에서다른초기설정을계속구성합니다.
6. 홈화면에 Citrix Secure Hub 를다운로드할수있도록 iTunes 에로그인하라는메시지가나타날수있습니다.

참고:

XenMobile 이장치기반 VPP(Volume Purchase Program) 애플당을사용하여 Secure Hub 앱을배포하도록구성된경우이단계는선택사항입니다. 이경우 iTunes 계정을만들거나기존계정을사용할필요가없습니다.



7. Secure Hub 를열고자격증명을입력합니다. 정책에의해요구되는경우 Citrix PIN 을생성하고확인하라는메시지가표시될수있습니다.

나머지필수앱이장치에배포됩니다.

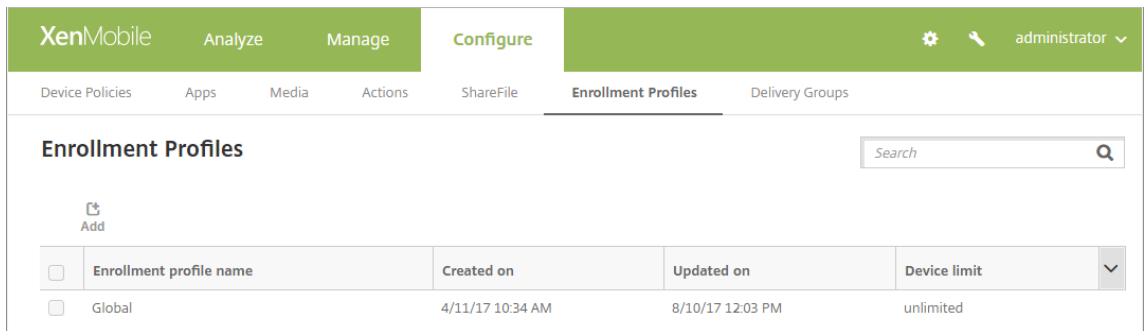
장치등록제한

August 23, 2019

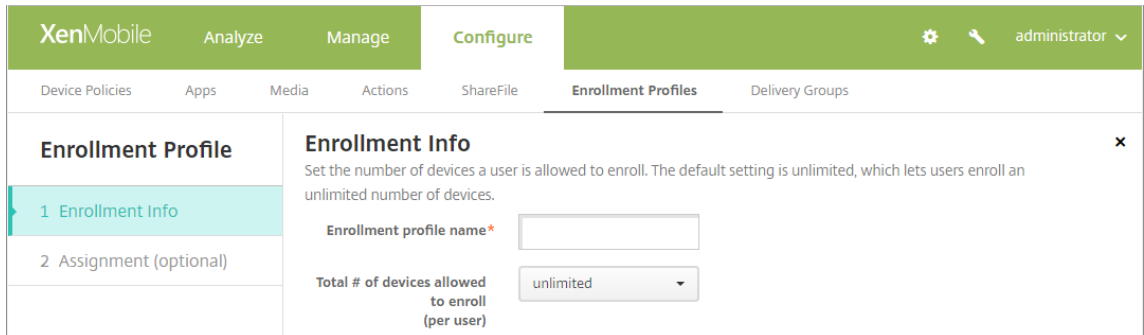
XenMobile에는 사용자가 제한 없는 수의 장치를 등록할 때 사용할 수 있는 기본 등록 프로필이 포함되어 있습니다. 기본 프로필의 이름은 Global입니다. 등록 프로필은 사용자가 등록할 수 있는 장치의 수를 제한하려는 경우에만 생성합니다. 등록 프로필을 배달 그룹에 연결할 수 있습니다.

장치 등록 제한은 ENT, MDM 및 MAM 서버 모드에 적용됩니다. 이 기능은 iOS 및 Android 장치에서만 사용할 수 있습니다.

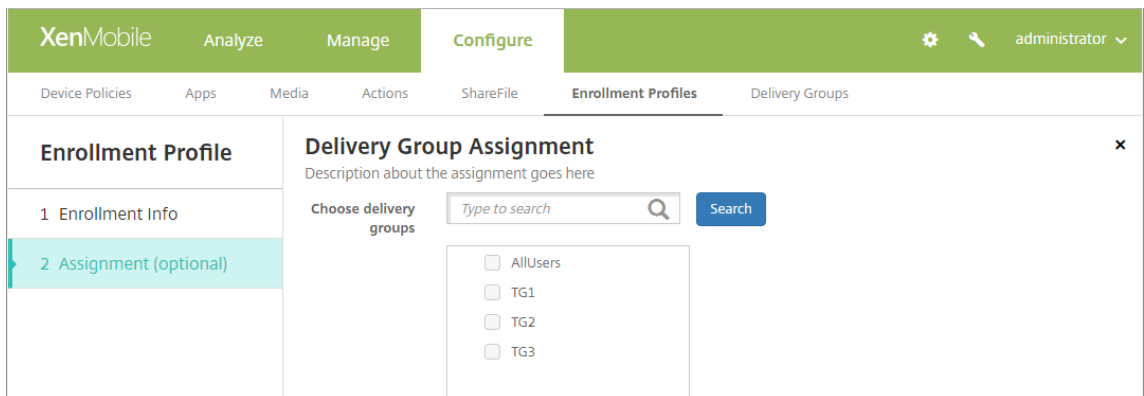
1. 구성 > 등록 프로필로 이동합니다. 기본 Global 프로필이 표시됩니다.



2. 등록 프로필을 추가하려면 추가를 클릭합니다. 등록 정보 페이지에서 등록 프로필의 이름을 입력하고 이 프로필의 구성원이 등록할 수 있는 장치 수를 선택합니다.

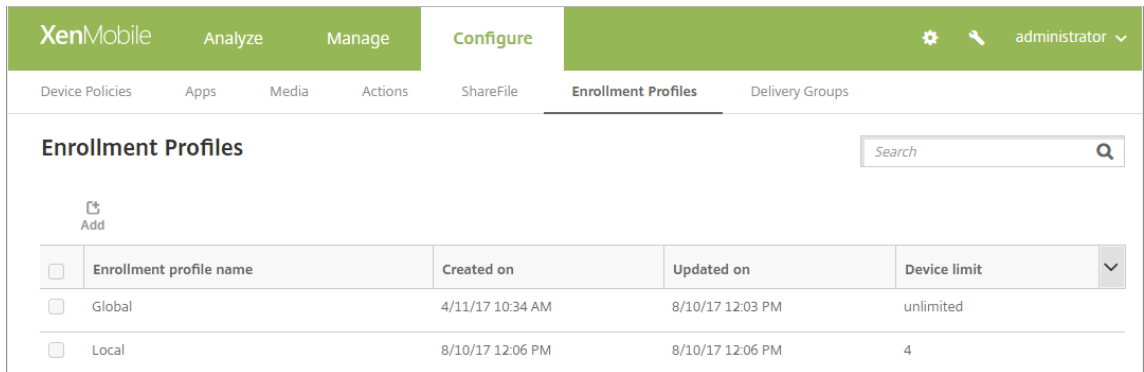


3. 다음을 클릭합니다. 배달 그룹 할당 화면이 나타납니다.

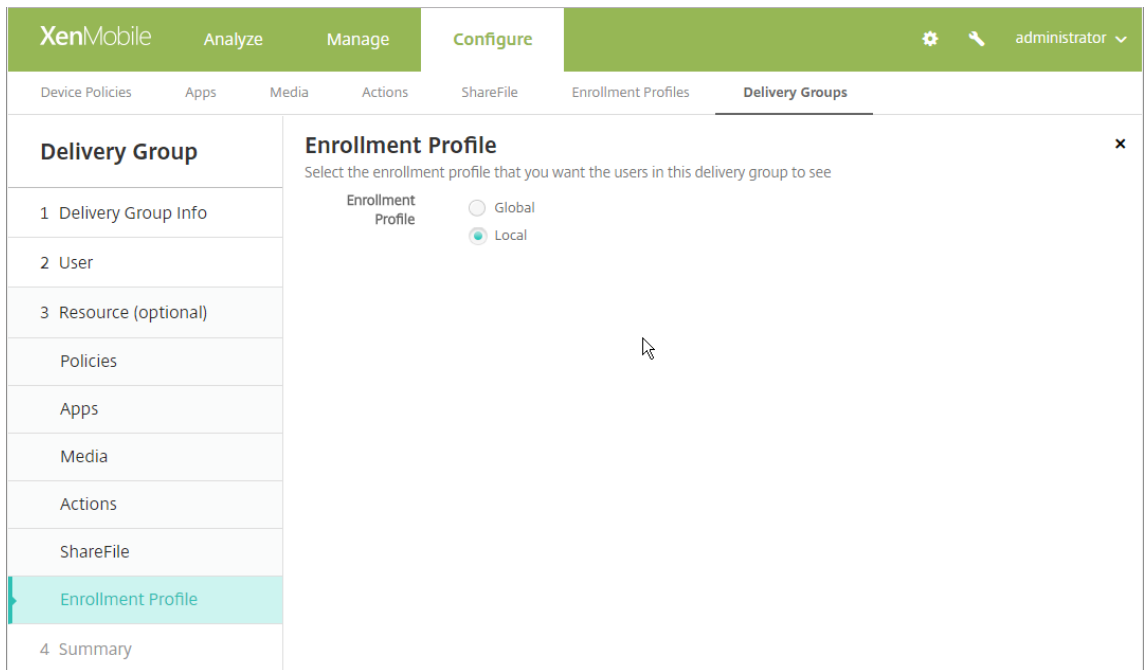


4. 이등록프로필에대한배달그룹을선택하고 저장을클릭합니다.

배달그룹페이지가나타납니다.



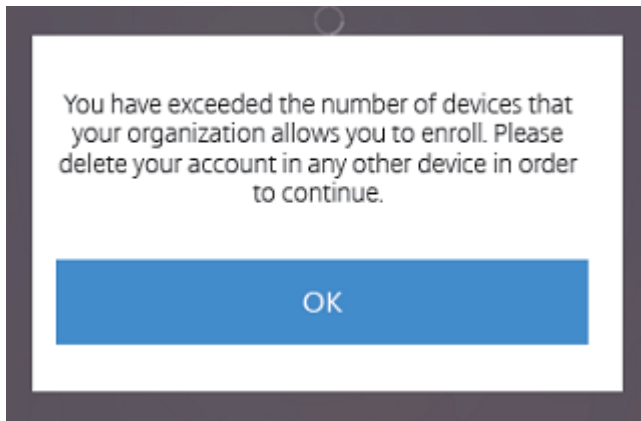
배달그룹에연결된등록프로필을변경하려면 구성 > 배달그룹으로이동하고 등록프로필을클릭합니다.



장치등록제한이있는사용자환경

장치등록제한을설정환경우새장치를등록하려는사용자는다음단계를수행하게됩니다.

1. Secure Hub 에로그온합니다.
2. 등록할서버주소를입력합니다.
3. 자격증명을입력합니다.
4. 장치제한에도달하면사용자에게장치등록제한이초과되었음을설명하는오류메시지가표시됩니다.



Secure Hub 등록화면이 다시 나타납니다.

장치등록

January 6, 2020

사용자장치를 원격으로 안전하게 관리하기 위해 사용자장치를 XenMobile 에 등록합니다. XenMobile 클라이언트 소프트웨어가 사용자 장치에 설치되며 사용자의 ID 가 인증됩니다. 그런 다음 XenMobile 과 사용자 프로필이 설치됩니다. 다음으로, XenMobile 콘솔에서 장치 관리 작업을 수행할 수 있습니다. 정책을 적용하고, 앱을 배포하고, 장치에 데이터를 푸시하고, 분실 또는 도난된 장치를 잠그고 초기화하고 찾을 수 있습니다.

iOS, Android 및 Windows 10 장치에서 Azure Active Directory 등록이 지원됩니다. Azure 를 IDP(ID 공급자) 로 구성하는 방법에 대한 자세한 내용은 [Azure Active Directory 를 IDP 로 XenMobile 과 통합](#)을 참조하십시오.

참고:

iOS 장치 사용자를 등록하려면 APNs 인증서를 요청해야 합니다. 자세한 내용은 [인증서 및 인증](#)에서 참조하십시오.

사용자 및 장치에 대한 구성 옵션을 업데이트하려면 [관리 > 등록](#) 초대 페이지로 이동합니다. 자세한 내용은 [이 문서에서 등록 초대 보내기](#)를 참조하십시오.

Android 장치

참고:

Android Enterprise 장치 등록에 대한 자세한 내용은 [Android Enterprise](#)를 참조하십시오.

1. Android 장치의 Google Play 스토어로 이동하여 Citrix Secure Hub 앱을 다운로드한 후 앱을 누릅니다.
2. 앱을 설치할 것인지 묻는 메시지가 나타나면 다음을 클릭한 후 설치를 클릭합니다.
3. Secure Hub 가 설치된 후에 **Open(열기)** 을 누릅니다.
4. XenMobile Server 이름, UPN(사용자 계정 이름) 또는 전자 메일 주소와 같은 회사 자격 증명을 입력합니다. 그리고 **Next(다음)** 를 클릭합니다.

5. **Activate device administrator**(장치관리자활성화) 화면에서 **Activate**(활성화) 를 누릅니다.
6. 회사암호를 입력한 다음 **Sign On**(로그온) 을 누릅니다.
7. XenMobile 이 구성된 방식에 따라 Citrix PIN 을 생성하라는 메시지가 나타날 수 있습니다. PIN 을 사용하여 Secure Hub 및 Secure Mail 과 ShareFile 등의 다른 XenMobile 사용 앱에 로그인할 수 있습니다. Citrix PIN 을 두 번 입력합니다. **Create Citrix PIN**(Citrix PIN 만들기) 화면에서 PIN 을 입력합니다.
8. PIN 을 다시 입력합니다. Secure Hub 가 열립니다. 이제 XenMobile Store 에 액세스하여 Android 장치에 설치할 수 있는 앱을 볼 수 있습니다.
9. 등록 후 앱을 장치에 자동으로 푸시하도록 XenMobile 을 구성한 경우 사용자에게 앱을 설치하라는 메시지가 나타납니다. 또한 XenMobile 에서 구성된 정책이 장치에 배포됩니다. 설치를 눌러 앱을 설치합니다.

Android 장치를 등록 취소하고 다시 등록하려면

사용자가 Secure Hub 내에서 등록을 취소할 수 있습니다. 사용자가 다음 절차를 사용하여 등록을 취소하는 경우 XenMobile 콘솔의 장치 인벤토리에 장치가 계속 나타납니다. 하지만 장치에 대한 작업을 수행할 수 없습니다. 장치를 추적하고 장치 규정 준수 여부를 모니터링할 수 없습니다.

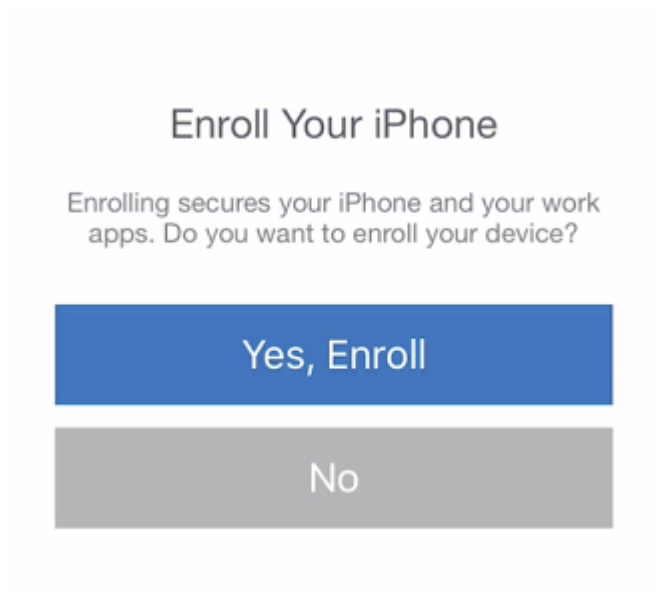
1. Secure Hub 앱을 눌러서 엽니다.
2. 휴대폰인지 태블릿인지에 따라 다음 절차를 수행합니다.
휴대폰에서:
 - 화면 왼쪽에서 살짝 밀어 설정창을 엽니다.
 - **Preferences**(기본 설정), **Accounts**(계정), **Delete Account**(계정 삭제) 를 차례로 누릅니다.태블릿에서:
 - 오른쪽 맨 위의 전자 메일 주소 옆에 있는 화살표를 누릅니다.
 - **Preferences**(기본 설정), **Accounts**(계정), **Delete Account**(계정 삭제) 를 차례로 누릅니다.
3. **Re-Enroll**(재등록) 을 누릅니다. 장치를 재등록할 것인지 확인하는 메시지가 표시됩니다.
4. 확인을 누릅니다.
장치가 등록 취소됩니다.
5. 화면의 지침에 따라 장치를 다시 등록합니다.

iOS 장치 등록

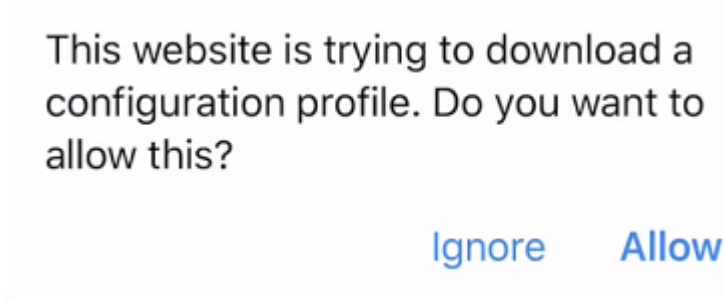
이 섹션에서는 사용자가 iOS 장치 (12.2 이상) 를 XenMobile Server 에 등록하는 방법을 보여줍니다. iOS 등록에 대한 자세한 내용을 보려면 다음 비디오를 시청하십시오.



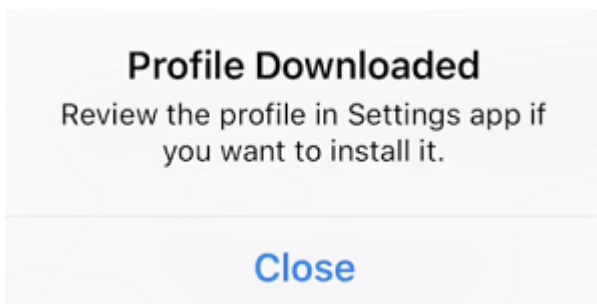
1. iOS 장치의 Apple Store 로이동하여 Citrix Secure Hub 앱을다운로드한후이앱을누릅니다.
2. 앱을설치하라는메시지가표시되면 다음을누른후 설치를누릅니다.
3. Secure Hub 가설치된후에 **Open(열기)** 을누릅니다.
4. XenMobile Server 이름, UPN(사용자계정이름) 또는전자메일주소와같은회사자격증명을입력합니다. 그리고 **Next(다음)** 를클릭합니다.
5. 예, 등록을눌러 iOS 장치를등록합니다.



6. 자격증명을 입력한 후 메시지가 표시되면 허용을 눌러 구성 프로필을 다운로드합니다.

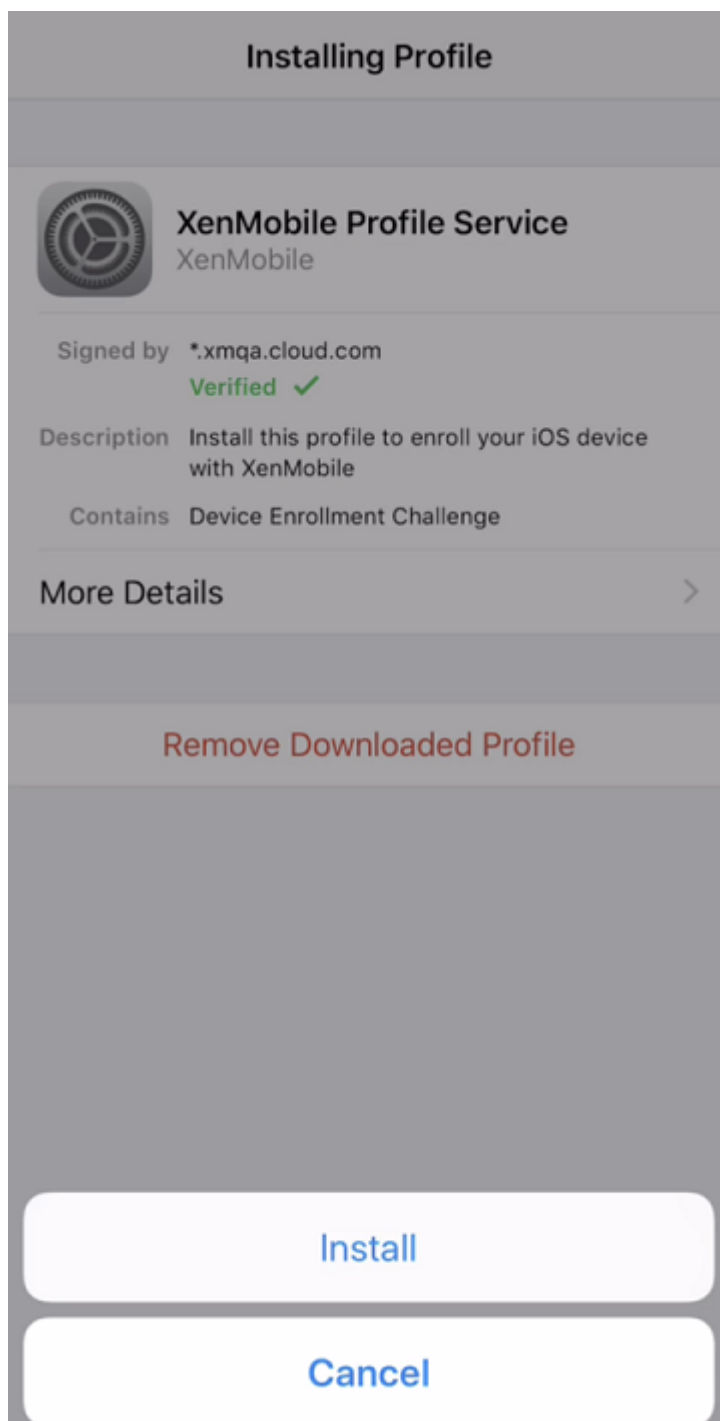


7. 구성 프로필을 다운로드한 후 닫기를 누릅니다.

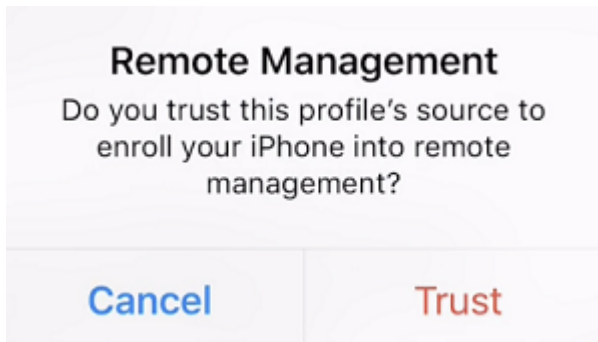


8. 장치 설정에서 iOS 인증서를 설치하고 장치를 신뢰할 수 있는 목록에 추가합니다.

- 설정 > 일반 > 프로필 > **XenMobile** 프로필 서비스로 이동하고 설치를 눌러 프로필을 추가합니다.



- 알림창에서 신뢰를눌러장치를원격관리에등록합니다.

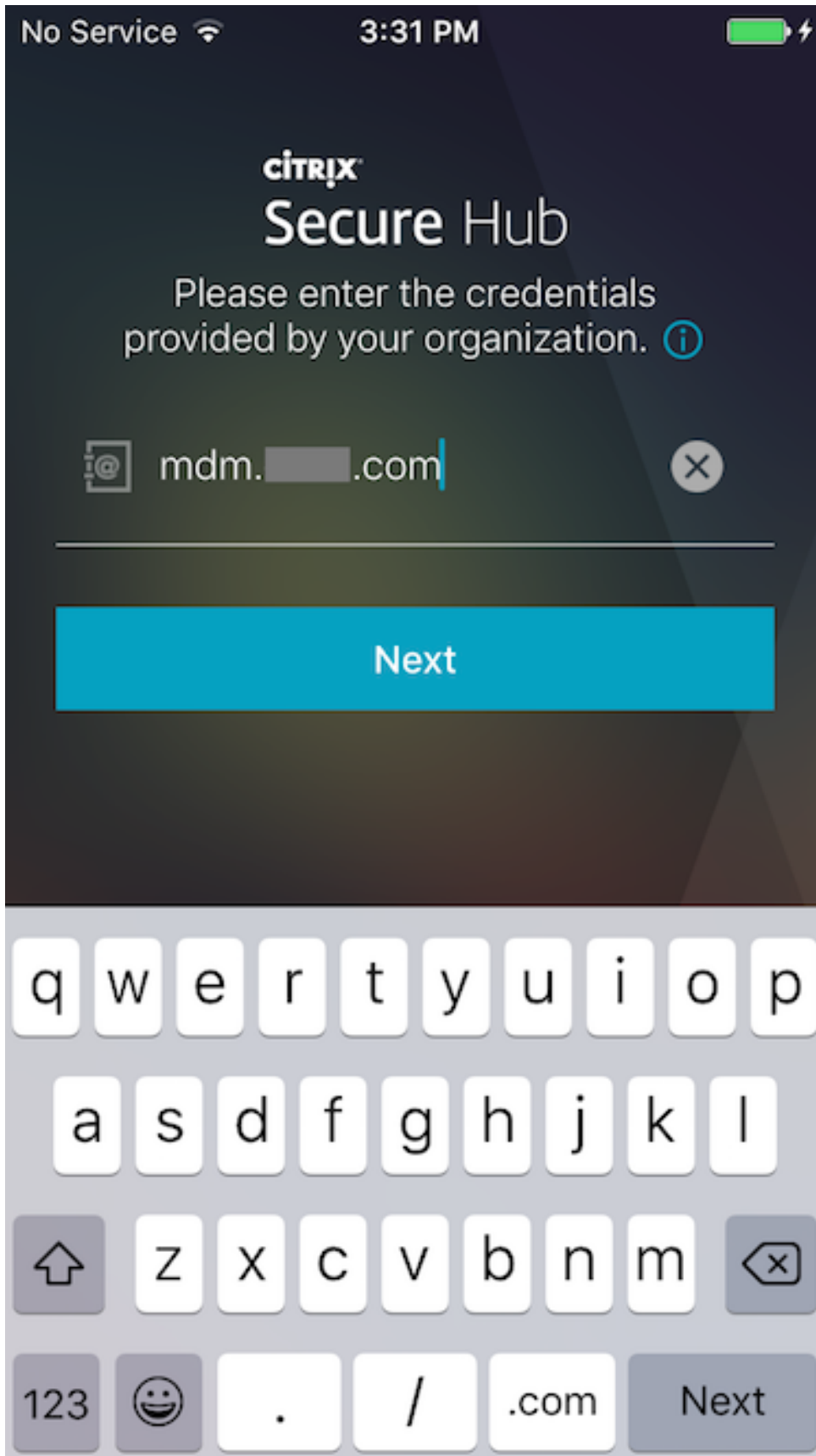


9. Secure Hub 에로그인합니다. MDM+MAM 에등록하는경우: 자격증명의유효성이확인된후메시지가표시되면 Citrix PIN 을만들고확인합니다.
10. 워크플로가완료되면장치가등록됩니다. 이제 App Store 에액세스하여 iOS 장치에설치할수있는앱을볼수있습니다.

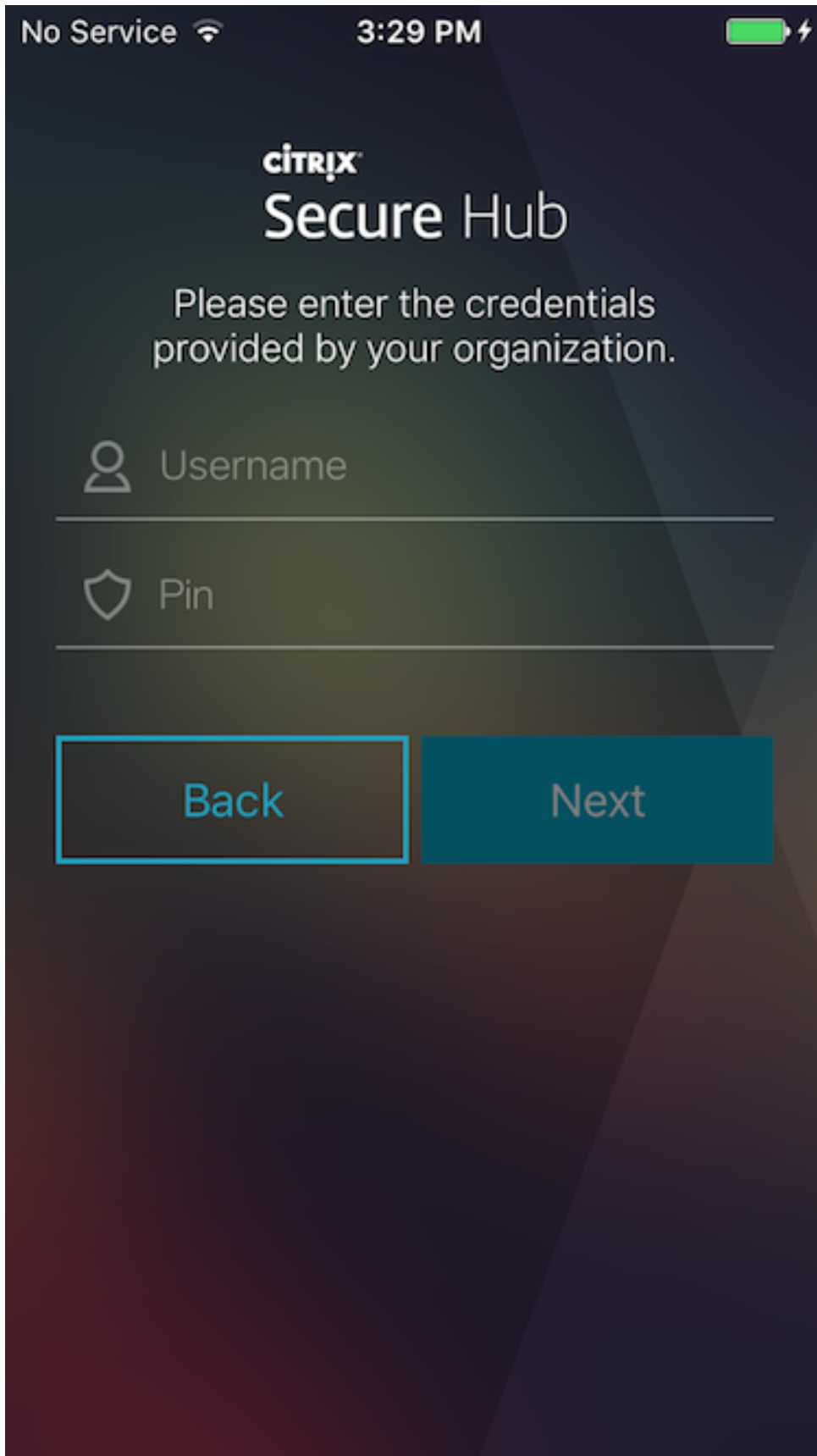
사용자가제공한자격증명을사용하는 **iOS** 장치

1. 장치에서 Apple iTunes App Store 로부터 Secure Hub 앱을다운로드한후앱을설치합니다.
2. iOS 장치의홈화면에서 Secure Hub 앱을누릅니다.
3. Secure Hub 앱이열리면지원센터에서제공한서버주소를입력합니다.

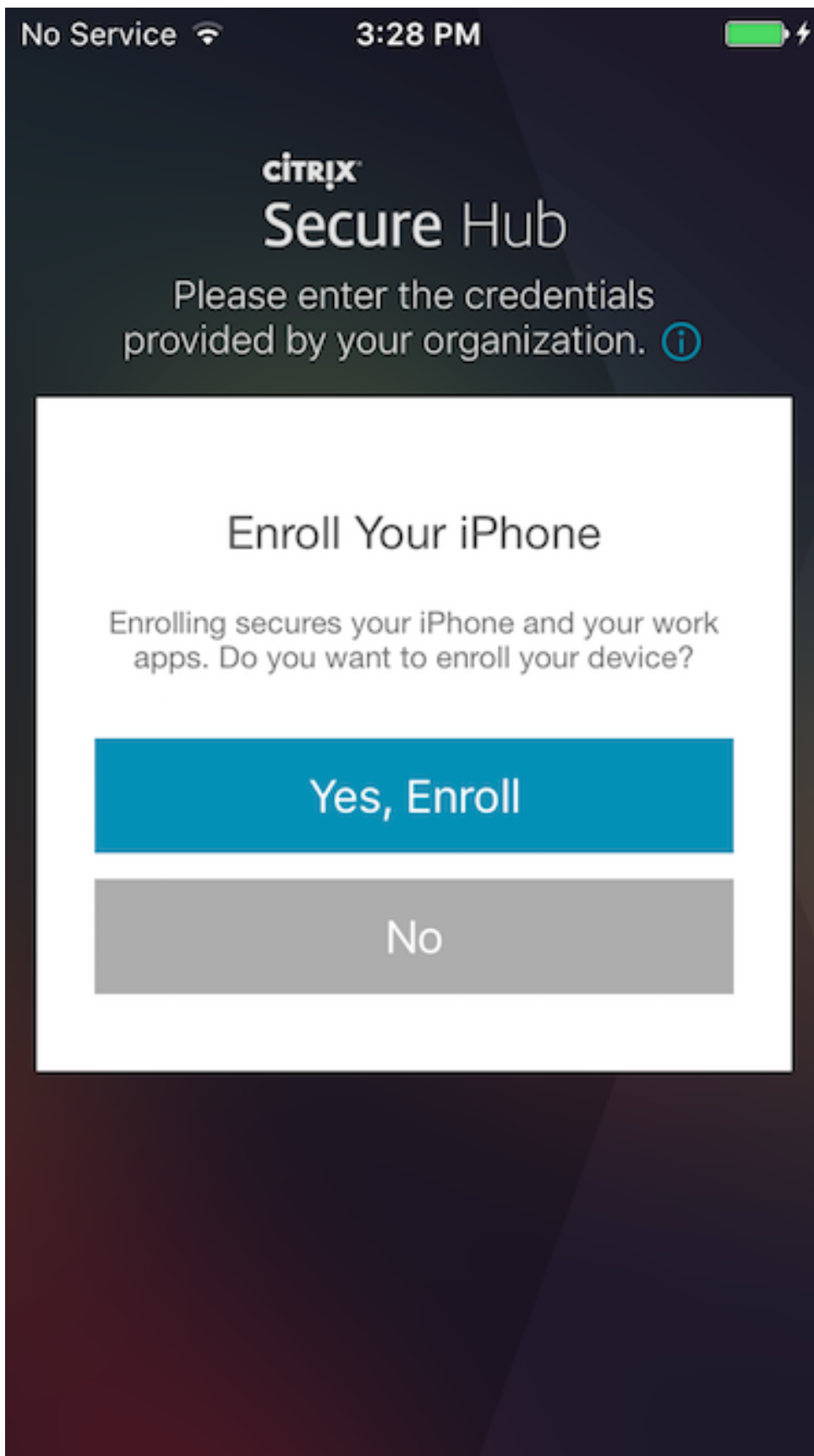
XenMobile 의구성방식에따라이러한예와다른화면이표시될수있습니다.



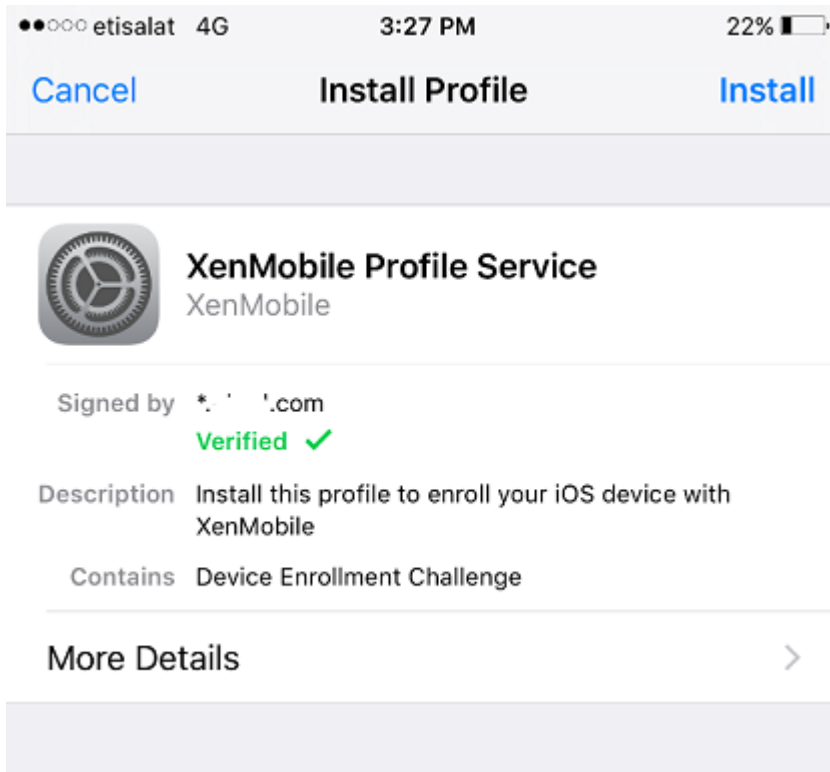
4. 메시지가 표시되면 사용자 이름과 암호 또는 PIN 을 입력합니다. 다음을 클릭합니다.



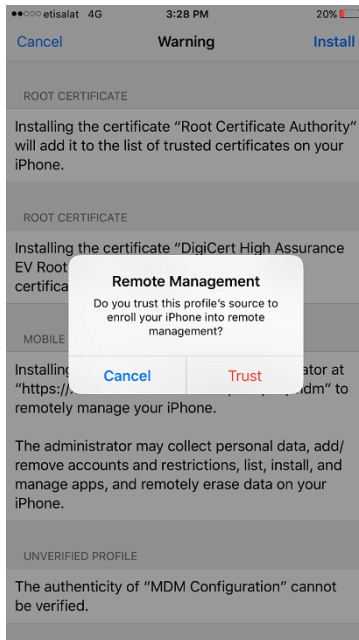
5. 등록하라는 메시지가 표시되면 **Yes, Enroll**(예, 등록) 을 클릭하고 메시지가 표시되면 자격 증명을 입력합니다.



6. 설치를 눌러 Citrix Profile Services 를설치합니다.



7. 신뢰를 누릅니다.



8. 열기를 누르고 자격증명을 입력합니다.

파생된자격증명을사용하는 iOS 장치

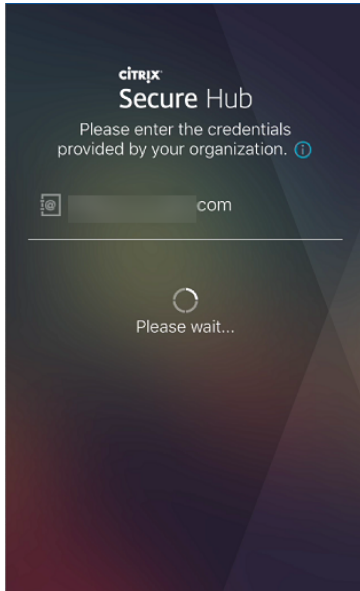
등록하려면사용자데스크톱에부착된판독기에스마트카드를삽입해야합니다.

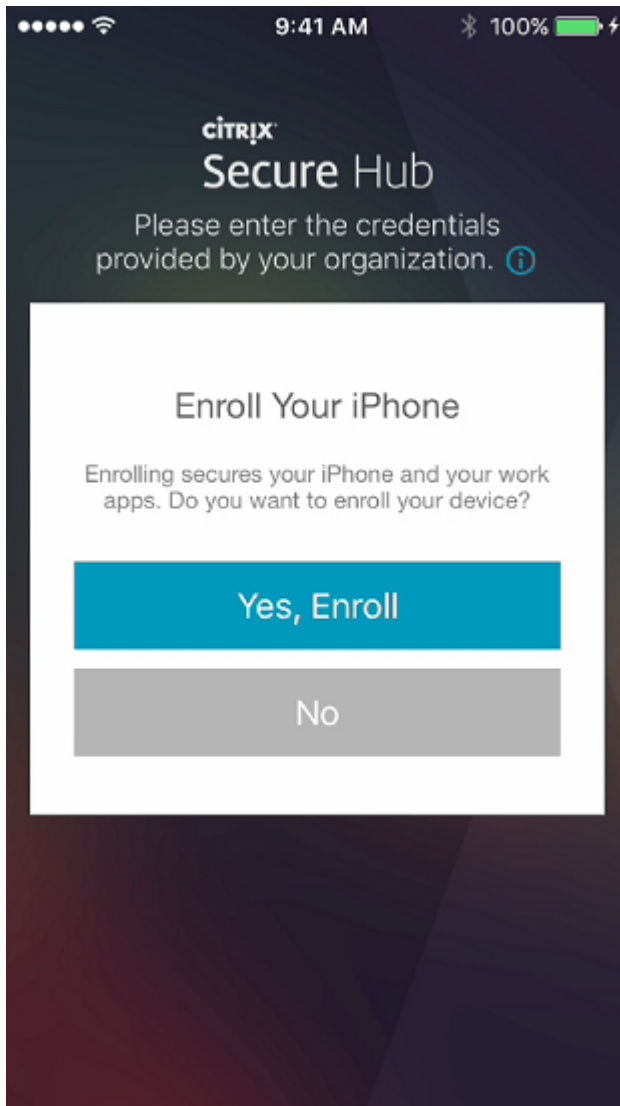
1. 사용자가 Secure Hub 와파생된자격증명공급자로부터받은앱을설치합니다.

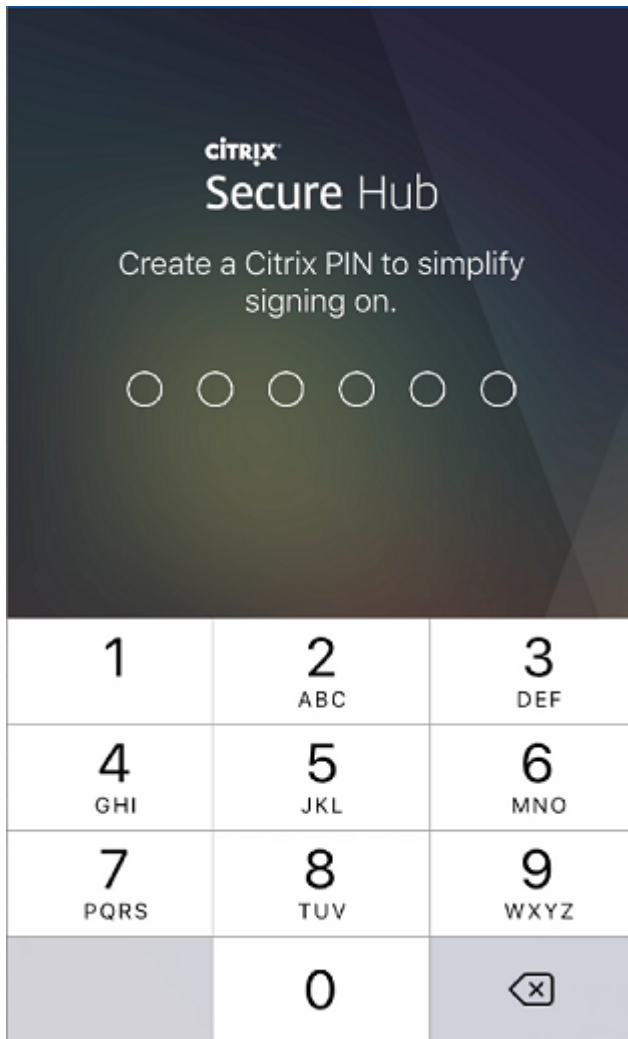
Intercede 의 ID 공급자앱은 MyID for Citrix 입니다. 해당앱의로고가나타납니다.



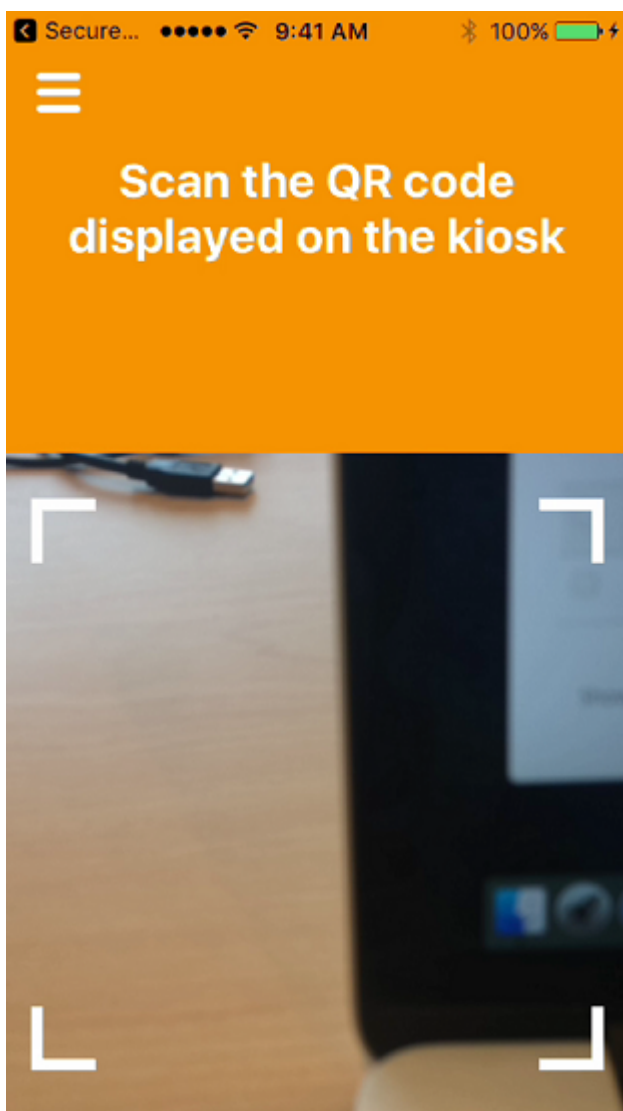
2. 사용자가 Secure Hub 를시작합니다. 메시지가나타나면사용자가 XenMobile Server FQDN(정규화된도메인이름)을입력하고 다음을클릭합니다. Secure Hub 에서등록이시작됩니다. XenMobile Server 에서파생된자격증명을지원하는경우 Secure Hub 에서사용자가 Citrix PIN 을생성하도록요청하는메시지가표시됩니다.



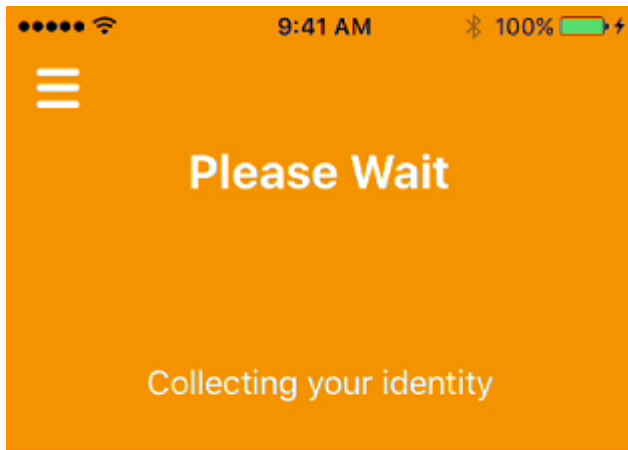




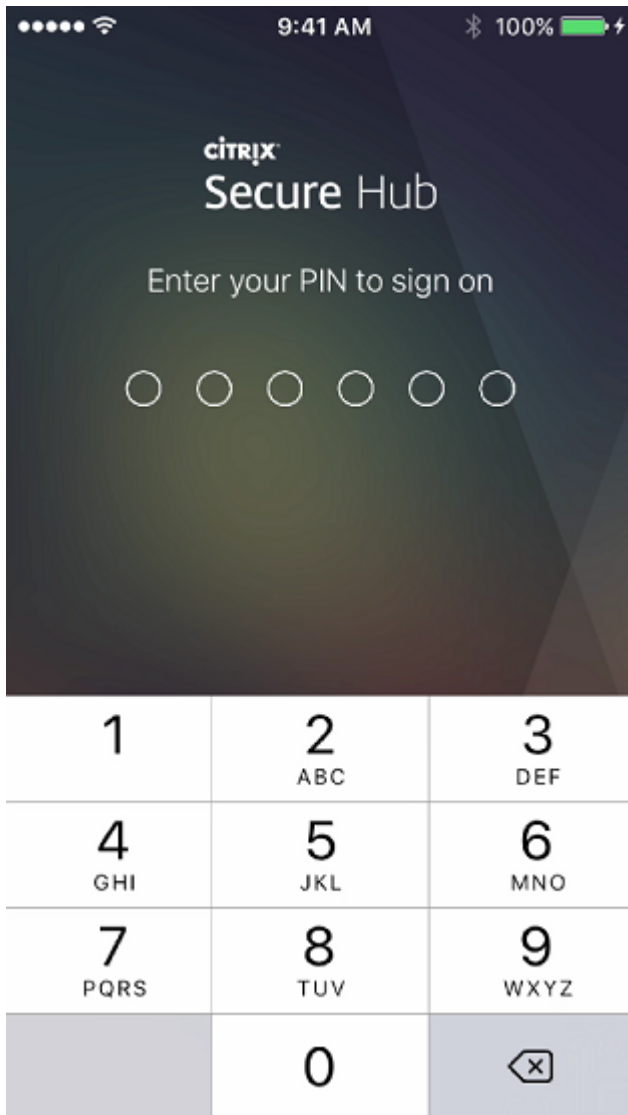
3. 사용자가 화면의 안내에 따라 스마트자격증명을 활성화합니다. 시작 화면이 나타나고 이어서 QR 코드를 스캔하라는 메시지가 나타납니다.



4. 사용자가 데스크톱에 부착된 스마트카드판독기에 카드를 삽입합니다. 그러면 데스크톱 앱에 QR 코드가 표시되고 사용자에게 모바일 장치를 사용하여 코드를 스캔하라는 메시지가 표시됩니다.



5. 메시지가 나타나면 사용자가 Secure Hub PIN 을 입력합니다.



6. PIN 인증후 Secure Hub 가인증서를다운로드합니다. 그런다음사용자는메시지에따라등록을완료합니다.

XenMobile 콘솔에서장치정보를보려면:

- 관리 > 장치로이동한다음명령상자를표시할장치를선택합니다. 자세히표시를클릭합니다.
- 분석 > 대시보드로이동합니다.

macOS 장치

XenMobile 에서 macOS 를실행하는장치를등록하는두가지방법을제공합니다. 두방법모두 macOS 사용자가장치에서직접온라인으로등록할수있습니다.

- 사용자에게등록초대보내기: 이등록방법을이용하면 macOS 장치에대해다음등록모드를설정할수있습니다.
 - 사용자이름 + 암호

- 사용자이름 + PIN
- 2 단계

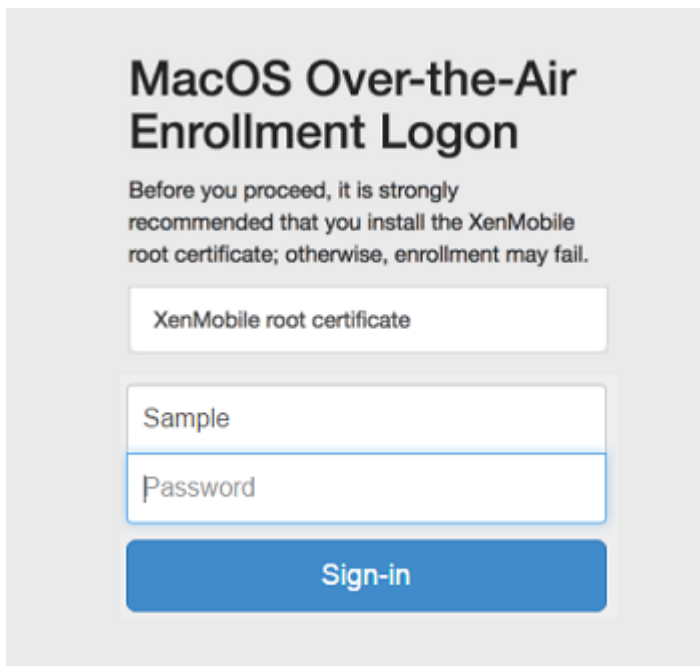
사용자가등록초대의지침을따르면사용자이름이입력된로그온화면이표시됩니다.

- 사용자에게설치링크보내기: macOS 장치를등록하는이방법은사용자에게등록링크를보냅니다. 사용자는이링크를 Safari 또는 Chrome 브라우저에서열수있습니다. 그런다음사용자이름과암호를제공하여등록합니다.

서버속성인 **Enable macOS OTAE** 를 **false** 로설정하여 macOS 장치에대한등록링크를사용하지못하도록할수있습니다. 이렇게하면 macOS 사용자가등록초대만사용하여등록할수있습니다.

사용자에게등록초대보내기

1. 필요에따라 XenMobile 콘솔에서 macOS 장치정책을설정합니다. 장치정책에대한자세한내용은 [장치정책](#)을참조하십시오.
2. macOS 사용자등록을위한초대를추가합니다. 자세한내용은이문서에서등록초대보내기를참조하십시오.
3. 사용자가초대를수신하고링크를클릭하면다음화면이 Safari 브라우저에표시됩니다. XenMobile 이사용자이름을채웁니다. 등록모드를 **2** 단계로선택한경우다른필드가나타납니다.



4. 사용자는필요에따라인증서를설치합니다. 사용자에게인증서를설치할것인지묻는메시지가표시되는지여부는 macOS 에 대해공개적으로신뢰할수있는 SSL 인증서와공개적으로신뢰할수있는디지털서명인증서를구성했는지여부에따라달라집니다. 인증서에대한자세한내용은 [인증서및인증](#)을참조하십시오.

5. 사용자가요청된자격증명을제공합니다.

Mac 장치정책이설치됩니다. 이제모바일장치를관리하듯이 XenMobile 로 Mac 을관리할수있습니다.

사용자에게설치링크보내기

1. 필요에따라 XenMobile 콘솔에서 macOS 장치정책을설정합니다. 장치정책에대한자세한내용은 [장치정책](#)을참조하십시오.
2. Safari 또는 Chrome 브라우저에서열수있는등록링크 (<https://serverFQDN:8443/instanceName/macos/otae>) 를사용자에게보냅니다.
 - **serverFQDN** 은 XenMobile 을실행하는서버의 FQDN(정규화된도메인이름) 입니다.
 - 기본보안포트는포트 **8443** 입니다. 다른포트를구성한경우 8443 대신해당포트를사용하십시오.
 - 주로 zdm 으로표시되는 **instanceName** 은서버설치중에지정된이름입니다.

설치링크를전송하는방법에대한자세한내용은설치링크를보내려면을참조하십시오.

3. 사용자는필요에따라인증서를설치합니다. iOS 와 macOS 에대해공개적으로신뢰할수있는 SSL 인증서및디지털서명인증서를구성한경우사용자에게인증서를설치하라는메시지가표시됩니다. 인증서에대한자세한내용은 [인증서및인증](#)을참조하십시오.
4. 사용자가자신의 Mac 에로그온합니다.

Mac 장치정책이설치됩니다. 이제모바일장치를관리하듯이 XenMobile 로 Mac 을관리할수있습니다.

Windows 장치

참고:

이섹션에는 Microsoft 가 2017 년 7 월 11 일에지원을종료한 Windows Phone 8.1 장치에대한참조가포함되어있습니다. XenMobile 은 Windows Phone 8.1 장치를 MDM 등록모드에서만지원합니다.

Windows 10 을실행하는장치는페더레이션된 Active Directory 인증수단으로 Azure 를사용하여등록됩니다. 다음방법중하나로 Windows 10 장치를 Microsoft Azure AD 에가입시킬수있습니다.

- 장치의전원을처음켜때 Azure AD 기본가입의일환으로 MDM 에등록합니다.
- 장치를구성한다음 Windows 설정페이지에서 Azure AD 가입의일환으로 MDM 에등록합니다.

XenMobile 에는다음 Windows 운영체제를실행하는장치를등록할수있습니다.

- Windows 10 Phone 및태블릿
- Windows Phone 8.1

사용자가자신의장치를통해직접등록할수있습니다.

참고:

Windows 10 RS2 휴대폰및태블릿의경우재등록도중사용자에게서버 URL 을입력하라는메시지가표시되지않습니다. 이문제를해결하려면장치를다시시작하십시오. 또는전자메일주소화면에서 서비스에연결하는중맞은편에있는 X 를눌러서버 URL 페이지로이동합니다. 이것은타사문제입니다.

관리자는지원되는 Windows 장치를관리할수있도록사용자등록에대한 Windows 검색서비스및자동검색을구성해야합니다.

Windows 장치사용자가 Azure 를 사용하여 등록할 수 있게 하려면 먼저 XenMobile 에서 Microsoft Azure 서버설정을 구성해야 합니다. 자세한 내용은 [Microsoft Azure Active Directory 서버설정](#)에서 참조하십시오.

자체검색을 사용하여 **Windows** 장치를 등록하려면

Windows 장치관리를 사용하려면 자동 검색 서비스 및 Windows 검색 서비스를 구성하는 것이 좋습니다. 자세한 내용은 [XenMobile Autodiscovery Service](#)에서 참조하십시오.

1. 장치에서 사용 가능한 모든 Windows 업데이트를 확인하고 설치합니다.
2. Windows 10 의 경우: 참메뉴에서 설정을 누른 후에 계정 > 회사 또는 학교 액세스 > 회사 또는 학교에 연결을 누릅니다. Windows 8.1 Phone 의 경우: **PC** 설정 > 네트워크 > 회사를 누릅니다.
3. 회사 전자메일 주소를 입력한 후 Windows 10 의 경우 계속을 누르고 Windows 8.1 의 경우 장치관리를 클릭합니다. 로컬 사용자 등록하려면 올바른 도메인 이름을 사용하여 존재하지 않는 전자메일 주소를 입력합니다 (예: `foo@mydomain.com`). 이를 통해 Windows 의 기본 제공 장치관리를 통해 등록이 수행되는 알려진 Microsoft 제한 사항을 바이패스할 수 있습니다. 서비스에 연결 중 대화상자에서 로컬 사용자와 연결된 사용자 이름 및 암호를 입력합니다. 장치에서 XenMobile Server 가 자동으로 검색되고 등록 프로세스가 시작됩니다.
4. 암호를 입력합니다. XenMobile 의 사용자 그룹에 속하는 계정과 연결된 암호를 사용합니다.
5. Windows 10 의 경우: 사용 약관 대화상자에서 장치가 관리되는 것에 동의함을 나타내고 동의를 누릅니다. Windows 8.1 의 경우: **IT** 관리자의 앱 및 서비스 허용 대화상자에서 장치가 관리되는 것에 동의함을 나타내고 커기를 누릅니다.

자체검색을 사용하지 않고 **Windows** 장치를 등록하려면

자동검색을 사용하지 않고 Windows 장치를 등록할 수 있습니다. 그러나 자동검색을 구성하는 것이 좋습니다. 자동검색을 사용하지 않고 등록하면 원하는 URL 에 연결하기 전에 포트 80 이 호출됩니다. 따라서 이는 프로덕션 배포를 위한 최선의 방법으로 간주되지 않습니다. 이 프로세스는 테스트 환경과 POC 배포에서만 사용하는 것이 좋습니다.

1. 장치에서 사용 가능한 모든 Windows 업데이트를 확인하고 설치합니다.
2. Windows 10 의 경우: 참메뉴에서 설정을 누른 후에 계정 > 회사 또는 학교 액세스 > 회사 또는 학교에 연결을 누릅니다. Windows 8.1 의 경우: **PC** 설정 > 네트워크 > 회사를 누릅니다.
3. 회사 전자메일 주소를 입력합니다.
4. Windows 10 의 경우: 자동검색이 구성되지 않은 경우 5 단계에 설명된 대로 서버 세부 정보를 입력할 수 있는 옵션이 표시됩니다. Windows 8.1 의 경우: 자동으로서버주소 검색이 켜짐으로 설정된 경우 꺼짐 옵션을 눌러서 설정합니다.
5. Windows 10 의 경우: 서버주소 입력 필드에 `https://serverfqdn:8443/serverInstance/wpe` 주소를 입력합니다.

8443 이외의 포트가 인증되지 않은 SSL 연결에 사용된 경우 주소에서 8443 대신 해당 포트 번호를 사용합니다.

Windows 8.1 의 경우: `https://serverfqdn:8443/serverInstance/Discovery.svc` 형식으로 서버주소를 입력합니다.

8443 이외의 포트가 인증되지 않은 SSL 연결에 사용된 경우 이 주소에서 8443 대신 해당 포트 번호를 사용합니다.

6. 암호를 입력합니다.
7. Windows 10 의 경우: 사용 약관 대화 상자에서 장치가 관리되는 것에 동의함을 나타내고 동의를 누릅니다. Windows 8.1 의 경우: **IT** 관리자의 엡 및 서비스 허용 대화 상자에서 장치가 관리되는 것에 동의함을 나타내고 켜기를 누릅니다.

Windows Phone 장치를 등록하려면

XenMobile 에서 Windows Phone 장치를 등록하려면 사용자에게 Active Directory 또는 내부 네트워크 전자 메일 주소 및 암호가 필요합니다. 또한 자동 검색이 설정되지 않은 경우 XenMobile Server 의 웹 주소도 필요합니다. 그런 다음 이 절차를 따라 장치를 등록합니다.

참고:

Windows Phone 회사 스토어를 통해 앱을 배포하려면 사용자가 등록하기 전에 [엔터프라이즈 허브](#) 정책 (지원되는 각 플랫폼에 대해서 명된 Secure Hub, Windows Phone 앱 사용) 을 구성해야 합니다.

1. Windows Phone 의 메인 화면에서 설정 아이콘을 누릅니다.
 - Windows 10 의 경우: 버전 에 따라 계정 > 회사 또는 학교 액세스 > 회사 또는 학교 연결을 누르거나 계정 > 회사 액세스 > 디바이스 관리에서만 등록을 누릅니다.
 - Windows 8.1 의 경우: **PC** 설정 > 네트워크 > 회사를 누른 후에 계정 추가를 누릅니다.
2. 다음 화면에서 전자 메일 주소와 암호를 입력한 후 로그인을 누릅니다.

도메인 자동 검색이 구성된 경우 다음 몇 단계에서 요청된 정보가 자동으로 입력됩니다. 8 단계로 이동합니다.

도메인에 대한 자동 검색이 구성되지 않은 경우 다음 단계를 계속합니다. 로컬 사용자로 등록하려면 올바른 도메인 이름을 사용하여 존재하지 않는 전자 메일 주소를 입력합니다 (예: `foo@mydomain.com`). 이를 통해 알려진 Microsoft 제한 사항을 바이패스할 수 있습니다. 서비스에 연결 중 대화 상자에서 로컬 사용자와 연결된 사용자 이름 및 암호를 입력합니다.
3. 다음 화면에서 XenMobile Server 의 웹 주소 (예: `https://<xenmobile_server>:<portnumber>/<instancename>/wpe`) 를 입력합니다. 예를 들어 `https://mycompany.mdm.com:8443/zdm/wpe` 입니다.

참고:

포트 번호는 각 구현에 맞게 수정해야 합니다. iOS 등록에 사용한 포트와 동일한 포트여야 합니다.

4. 사용자 이름과 도메인을 통해 인증을 검증하는 경우 사용자 이름과 도메인을 입력하고 로그인을 누릅니다.
5. Windows Phone 8.1 에서는 계정을 추가할 때 회사 앱 설치를 선택할 수 있습니다. 관리자가 회사 앱 스토어를 구성한 경우 이 옵션을 선택하고 완료를 누릅니다. 이 옵션의 선택을 취소하면 회사 앱 스토어를 받기 위해 장치를 다시 등록해야 합니다.
6. Windows Phone 8.1 의 경우 계정 추가 완료 화면에서 완료를 누릅니다.
7. 서버에 강제로 연결하려면 새로 고침 아이콘을 누릅니다. 장치가 서버에 자동으로 연결되지 않을 경우 XenMobile 이 다시 연결을 시도합니다. XenMobile 은 3 분마다 연속 5 회 장치에 연결하고 그 후로 2 시간 간격으로 장치에 연결합니다. 서버 속성을

에있는 **Windows WNS** 하트비트간격에서이연결속도를변경할수있습니다. 등록이완료되면백그라운드에서 **Secure Hub** 가등록됩니다. 설치가완료될때관련알림이표시되지않습니다. 모든앱화면에서 **Secure Hub** 를누릅니다.

등록초대보내기

XenMobile 콘솔에서 iOS, macOS 및 Android 장치사용자에게등록초대를보낼수있습니다. 또한 iOS 또는 Android 장치사용자에게설치링크를보낼수있습니다.

등록초대는다음과같이보냅니다.

- 한명의로컬사용자또는 Active Directory 사용자에게등록초대를보내는경우: 지정한휴대폰번호및통신회사이름의 SMS 를통해사용자에게초대가발송됩니다.
- 그룹에대한등록초대인경우: 사용자에게 SMS 로초대가발송됩니다. Active Directory 사용자에게 Active Directory 의전자메일주소및휴대폰번호가있는경우해당사용자는초대를받습니다. 로컬사용자는사용자속성에지정된전자메일및전화번호로초대를받습니다.

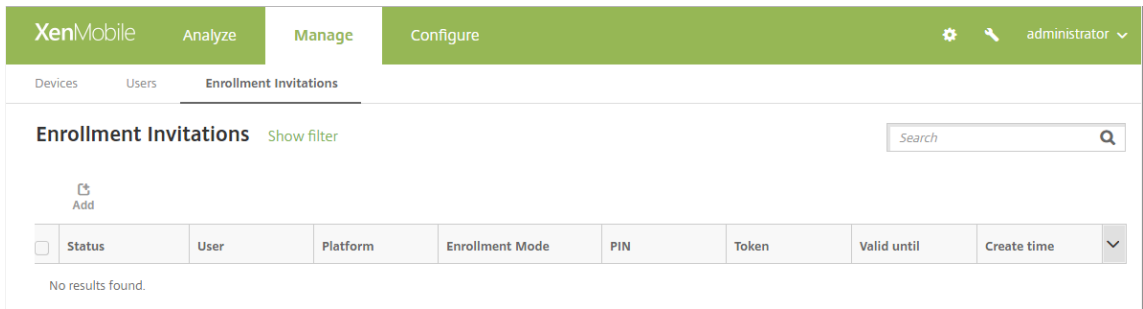
사용자가등록하면해당사용자의장치는 **관리 > 장치에관리되는장치**로표시됩니다. 초대 URL 의상태는 **상환됨**으로표시됩니다.

사전요구사항

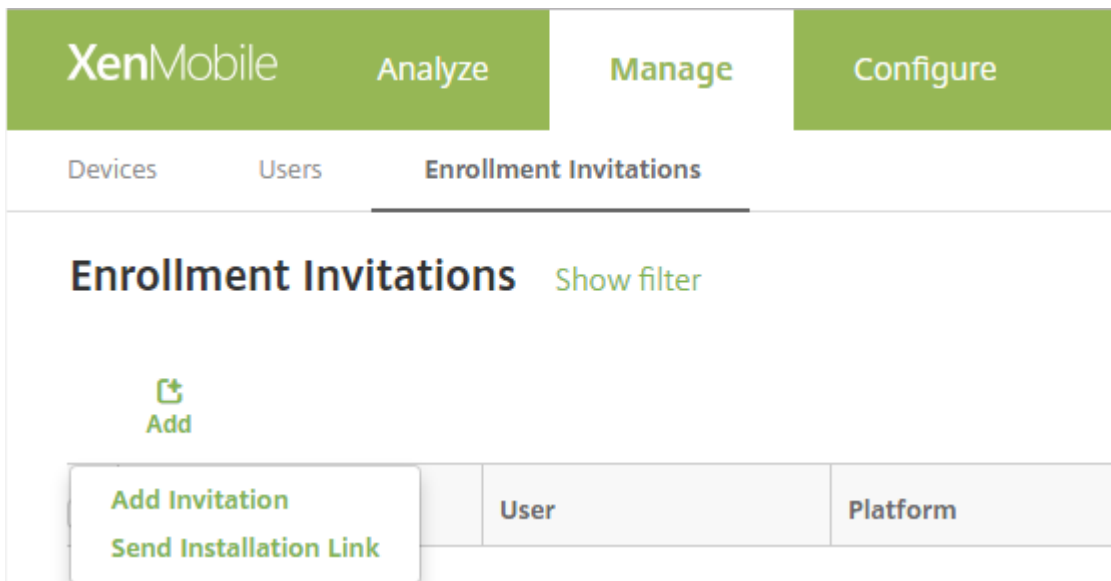
- 엔터프라이즈 (XME) 또는 MDM 모드로구성된 XenMobile Server
- 구성된 LDAP
- 로컬그룹및로컬사용자를사용중인경우:
 - 하나이상의로컬그룹.
 - 로컬그룹에할당된로컬사용자.
 - 배달그룹은로컬그룹과연결됩니다.
- Active Directory 를사용중인경우:
 - 배달그룹은 Active Directory 그룹과연결됩니다.

등록초대만들기

1. XenMobile 콘솔에서 **관리 > 등록초대**를클릭합니다. 등록초대페이지가나타납니다.



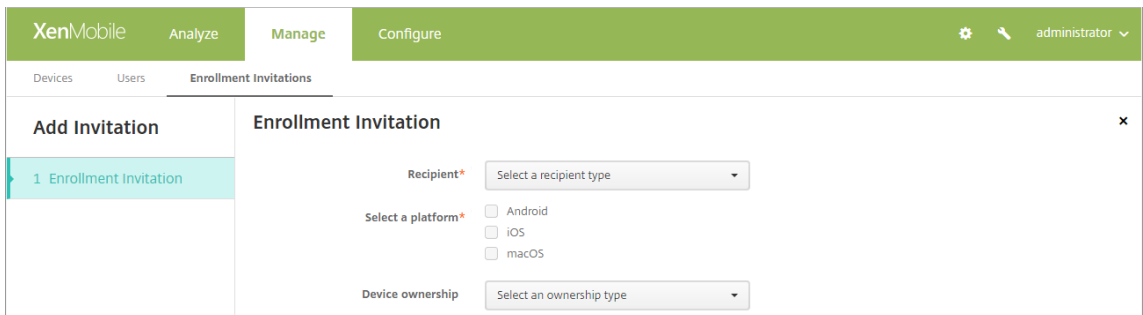
2. 추가를 클릭합니다. 등록옵션메뉴가 나타납니다.



- 사용자 또는 그룹에 등록 초대 보내려면 초대 추가를 클릭합니다.
- SMTP 또는 SMS 를 통해 받는 사람 목록에 등록 설치 링크 보내려면 설치 링크 보내기를 클릭합니다.

이후 단계에서는 등록 초대 및 설치 링크 보내기에 대해 설명합니다.

3. 초대 추가를 클릭합니다. 등록 초대 화면이 나타납니다.



4. 다음 설정을 구성합니다.

- 받는 사람: 그룹 또는 사용자를 선택합니다.
- 플랫폼 선택: 받는 사람이 그룹인 경우 모든 플랫폼이 선택됩니다. 플랫폼 선택은 변경할 수 있습니다. 받는 사람이 사용자인 경우 플랫폼이 선택되지 않습니다. 플랫폼을 선택합니다.

- 장치소유권: 회사또는 직원을선택합니다.

사용자또는그룹에대한설정이나타납니다. 다음섹션에서이에대해설명합니다.

사용자에게등록초대를보내려면

1. 다음 사용자설정을구성합니다.

- 사용자이름: 사용자이름을입력합니다. 사용자는 Active Directory 의사용자또는로컬사용자로 XenMobile Server 에있어야합니다. 로컬사용자인경우사용자에게알림을보낼수있도록사용자의전자메일속성이설정되어있는지확인하십시오. Active Directory 사용자인경우 LDAP 가구성되어있는지확인하십시오.
- 장치정보: 여러플랫폼을선택하거나 macOS 만선택한경우에는이설정이나타나지않습니다. 일련번호, **UDID** 또는 **IMEI** 를선택합니다. 옵션을선택하면장치에대한해당값을입력할수있는필드가표시됩니다.
- 전화번호: 여러플랫폼을선택하거나 macOS 만선택한경우에는이설정이나타나지않습니다. 필요에따라사용자의 전화번호를입력합니다.
- 통신회사: 여러플랫폼을선택하거나 macOS 만선택한경우에는이설정이나타나지않습니다. 사용자의전화번호에 연결할통신회사를선택합니다.
- 등록모드: 사용자를등록할방식을선택합니다. 기본값은 사용자이름 + 암호입니다. 일부플랫폼에서는다음옵션중 일부를사용할수없습니다.
 - 사용자이름 + 암호
 - 높은수준의보안
 - 초대 URL
 - 초대 URL + PIN
 - 초대 URL + 암호

- 2 단계
- 사용자이름 + PIN

선택한각플랫폼에유�효한등록모드만표시됩니다. 등록용 PIN 을일회용 PIN 이라고도합니다. 이러한 PIN 은사용자가등록할때만유효합니다.

참고:

PIN 이포함된등록모드를선택하면 등록 PIN 용템플릿필드가나타납니다. 여기서 등록 PIN 을클릭합니다.

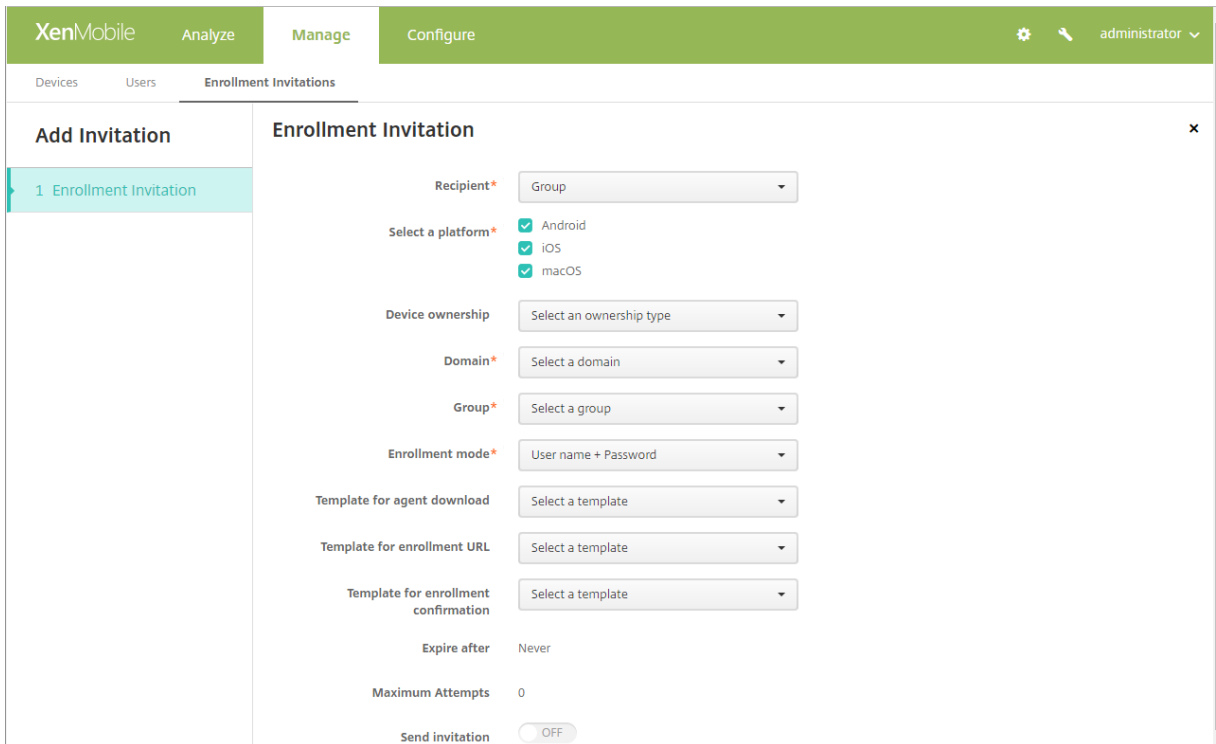
- 에이전트다운로드용템플릿: 다운로드링크라는이름의다운로드링크템플릿을선택합니다. 이템플릿은지원되는모든 플랫폼용템플릿입니다.
- 등록 URL 용템플릿: 등록초대를선택합니다.
- 등록확인용템플릿: 등록확인을선택합니다.
- 다음이후에만료: 이필드는등록모드를구성한경우설정되며등록이완료되는시기를나타냅니다. 등록모드를구성하는방법에대한자세한내용은 [등록모드를구성하려면](#)을참조하십시오.
- 최대시도횟수: 이필드는 등록모드를구성할때설정되며등록프로세스가진행되는최대횟수를나타냅니다. 등록모드를구성하는방법에대한자세한내용은 [등록모드를구성하려면](#)을참조하십시오.
- 초대보내기: 초대를즉시보내려면 켜짐을선택합니다. 초대를 등록초대페이지의테이블에추가하되보내지않으려면 꺼짐을선택합니다.

2. 초대보내기를사용하도록설정할경우 저장및보내기를클릭합니다. 그렇지않은경우 저장을클릭합니다. 등록초대페이지의테이블에초대가표시됩니다.

<input type="checkbox"/>	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time
<input type="checkbox"/>	PENDING	[Redacted]	Android	User name + Password	[Redacted]	[Redacted]	[Redacted]	05/03/2017 10:32:24 am
<input type="checkbox"/>	PENDING	[Redacted]	macOS	User name + Password	[Redacted]	[Redacted]	[Redacted]	05/01/2017 07:33:38 pm
<input type="checkbox"/>	PENDING	[Redacted]	iOS	User name + Password	[Redacted]	[Redacted]	[Redacted]	05/01/2017 07:29:02 pm

그룹에등록초대를보내려면

다음그림에서는그룹에대한등록초대를구성하기위한설정을보여줍니다.



1. 다음설정을구성합니다.

- 도메인: 초대받을그룹의도메인을선택합니다.
- 그룹: 초대받을그룹을선택합니다.
- 등록모드: 그룹의사용자를등록할방식을선택합니다. 기본값은 사용자이름 + 암호입니다. 일부플랫폼에서는다음 옵션중일부를사용할수없습니다.
 - 사용자이름 + 암호
 - 높은수준의보안
 - 초대 URL
 - 초대 URL + PIN
 - 초대 URL + 암호
 - 2 단계
 - 사용자이름 + PIN

선택한각플랫폼에유효한등록모드만표시됩니다.

참고:

PIN 이포함된등록모드를선택하면 등록 PIN 용템플릿필드가나타납니다. 여기서 등록 PIN 을클릭합니다.

- 에이전트다운로드용템플릿: 다운로드링크: 라는이름의다운로드링크템플릿을선택합니다. 이템플릿은지원되는모 든플랫폼용템플릿입니다.
- 등록 URL 용템플릿: 등록초대를선택합니다.
- 등록확인용템플릿: 등록확인을선택합니다.
- 다음이후에만료: 이필드는등록모드를구성한경우설정되며등록이만료되는시기를나타냅니다. 등록모드를구성하는

방법에대한자세한내용은 [등록모드를구성하려면](#)을참조하십시오.

- **최대시도횟수:** 이필드는등록모드를구성할때설정되며등록프로세스가진행되는최대횟수를나타냅니다. 등록모드를 구성하는방법에대한자세한내용은 [등록모드를구성하려면](#)을참조하십시오.
- **초대보내기:** 초대를즉시보내려면 **꺼짐**을선택합니다. 초대를 등록초대페이지의테이블에추가하되보내지않으려면 **꺼짐**을선택합니다.

2. 초대보내기를사용하도록설정한경우 저장및보내기를클릭합니다. 그렇지않은경우 저장을클릭합니다. 등록초대페이지의 테이블에초대가표시됩니다.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days	
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days	

설치링크를보내려면

등록설치링크를보내기전에 설정페이지에서알림서버의채널 (SMTP 또는 SMS) 을구성해야합니다. 자세한내용은 [알림](#)을참조하십시오.

Send Installation Link

Recipients*

Channels

SMTP ⚠ Channel cannot be activated until you define the SMTP server in the [Notification Server](#) section in Settings.

Sender:

Subject:

Message:

SMS ⚠ Channel cannot be activated until you define the SMS server in the [Notification Server](#) section in Settings.

Message:

1. 다음설정을구성한후 저장을클릭합니다.

- 받는사람: 추가하려는 각 받는 사람에 대해 추가를 클릭한 후 다음 작업을 수행합니다.
 - 전자메일: 받는 사람의 전자메일 주소를 입력합니다. 이것은 필수 필드입니다.
 - 전화번호: 받는 사람의 전화번호를 입력합니다. 이것은 필수 필드입니다.

참고:

기존의 받는 사람을 삭제하려면 목록이 포함된 줄 위로 마우스 포인터를 이동한 후 오른쪽의 휴지통 아이콘을 클릭합니다. 확인 대화 상자 가 나타납니다. 삭제를 클릭하여 목록을 삭제하거나 취소를 클릭하여 목록을 유지합니다.

기존의 받는 사람을 편집하려면 목록이 포함된 줄 위로 마우스 포인터를 이동한 후 오른쪽의 펜 아이콘을 클릭합니다. 목록을 업데이트한 후 저장을 클릭하여 변경된 목록을 저장하거나 취소를 클릭하여 목록을 변경되지 않은 상태로 유지합니다.

- 채널: 등록 설치 링크를 보내는데 사용할 채널을 선택합니다. **SMTP** 또는 **SMS** 를 통해 알림을 보낼 수 있습니다. 설정 페이지의 알림 서버에서 서버 설정을 구성할 때까지 이러한 채널을 활성화할 수 없습니다. 자세한 내용은 [알림](#)에서 참조하십시오.
- **SMTP**: 다음과 같은 선택적 설정을 구성합니다. 이러한 필드에 아무 것도 입력하지 않으면 선택한 플랫폼에 구성된 알림 템플릿에 지정되어 있는 기본값이 사용됩니다.
 - 보낸 사람: 선택적 보낸 사람을 입력합니다.
 - 제목: 선택적 메시지 제목을 입력합니다. 예를 들어, “장치를 등록하십시오.” 를 사용할 수 있습니다.
 - 메시지: 받는 사람에게 보낼 선택적 메시지를 입력합니다. 예를 들어 “조직의 앱과 전자메일에 대한 액세스 권한을 얻으려면 장치를 등록하십시오.” 를 사용할 수 있습니다.
- **SMS**: 다음 설정을 구성합니다. 이 필드에 아무 것도 입력하지 않으면 선택한 플랫폼에 구성된 알림 템플릿에 지정되어 있는 기본값이 사용됩니다.
 - 메시지: 받는 사람에게 보낼 메시지를 입력합니다. 이 필드는 SMS 기반 알림에 필요합니다.

참고: 북미 지역의 경우 160 자를 초과하는 SMS 메시지는 여러 메시지로 배달됩니다.

2. Send(보내기) 를 클릭합니다.

참고:

해당 환경에서 sAMAccountName 을 사용하는 경우 초대 링크를 클릭한 사용자가 사용자 이름을 편집해야 인증이 완료됩니다. 사용자 이름은 sAMAccountName@domainname.com 의 형식으로 표시됩니다. 사용자는 @domainname.com 부분을 제거해야 합니다.

Firebase Cloud Messaging

January 6, 2020

참고:

FCM(Firebase Cloud Messaging) 은 이전의 GCM(Google Cloud Messaging) 입니다. 일부 XenMobile 콘솔레이블 및 메시지는 GCM 용어가 사용됩니다.

FCM(Firebase Cloud Messaging) 을 사용하여 Android 장치의 XenMobile 연결방법 및 시기를 제어하는 것이 좋습니다. FCM 예구성된 XenMobile 은 FCM 을 사용하도록 설정된 Android 장치에 연결 알림을 전송합니다. 모든 보안 동작 또는 배포 명령이 실행되면 사용자에게 XenMobile 서버에 다시 연결하라는 메시지를 표시하는 푸시 알림이 트리거됩니다.

이 문서의 구성 단계를 완료하고 장치를 체크인하면 장치가 XenMobile Server 의 FCM 서비스에 등록됩니다. 이 연결은 FCM 을 사용하여 XenMobile Service 에서 장치로 거의 실시간 통신을 가능하게 합니다. FCM 등록은 새로운 장치 등록 및 이전에 등록된 장치에서 작동합니다.

장치에 대한 연결을 시작해야 하는 XenMobile 이 FCM 서비스에 연결하면 FCM 서비스가 연결 알림을 장치에 제공합니다. 이 유형의 연결은 Apple 이 푸시 알림 서비스에 사용하는 연결과 유사합니다.

사전 요구 사항

- 최신 Secure Hub 클라이언트
- Google 개발자 계정 자격 증명
- FCM 지원 Android 장치에 설치된 Google Play 서비스

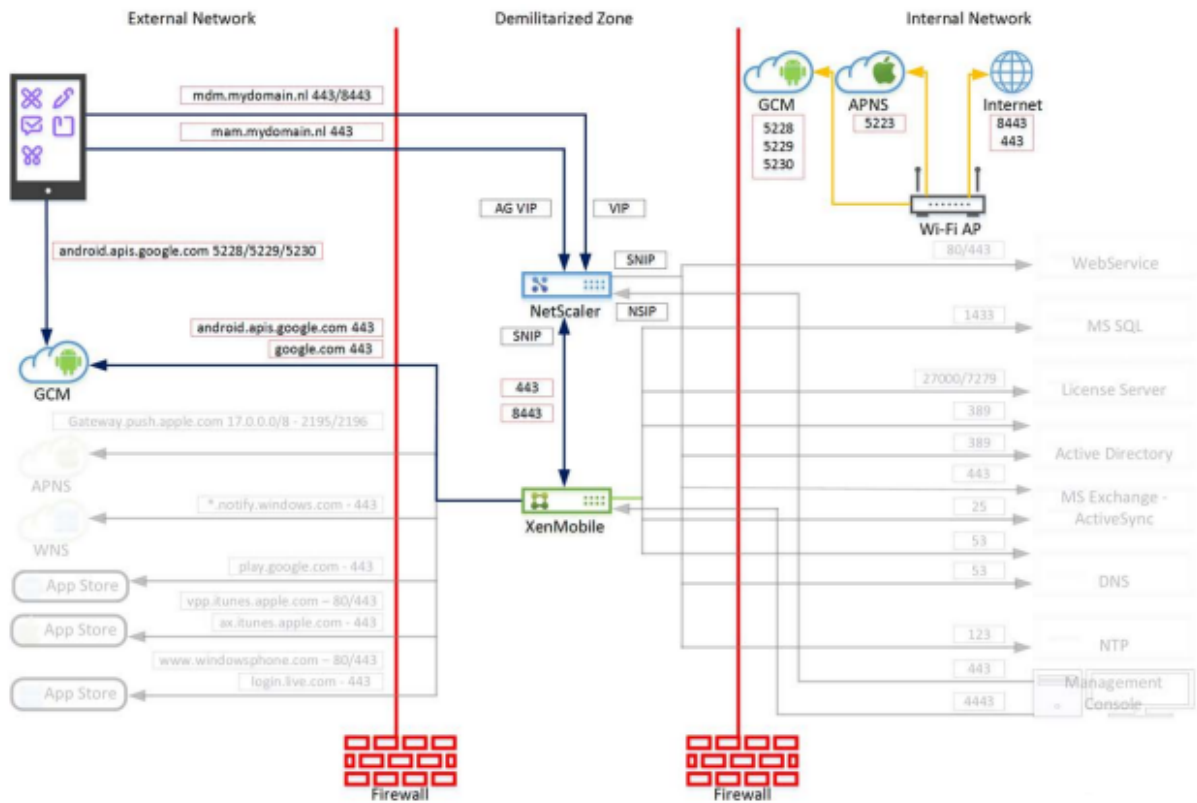
방화벽 포트

- XenMobile 에서 fcm.googleapis.com 및 [Google.com](https://google.com) 에 대해 포트 443 을 엽니다.
- 장치 Wi-Fi 에서 나가는 인터넷 통신을 위해 포트 5228, 5229 및 5230 을 엽니다.
- 나가는 연결을 허용하려면 IP 제한 없이 포트 5228~5230 을 화이트리스트에 추가하는 것이 좋습니다. IP 제한이 필요한 경우에는 IPv4 및 IPv6 블록의 모든 IP 주소를 화이트리스트에 추가하는 것이 좋습니다. 이러한 블록은 [Google ASN of 15169](#) 에 나와 있습니다. 해당 목록을 매월 업데이트하십시오.

자세한 내용은 [포트 요구 사항](#) 에서 참조하십시오.

아키텍처

이 다이어그램은 외부 및 내부 네트워크의 FCM 에 대한 통신 흐름을 보여줍니다.

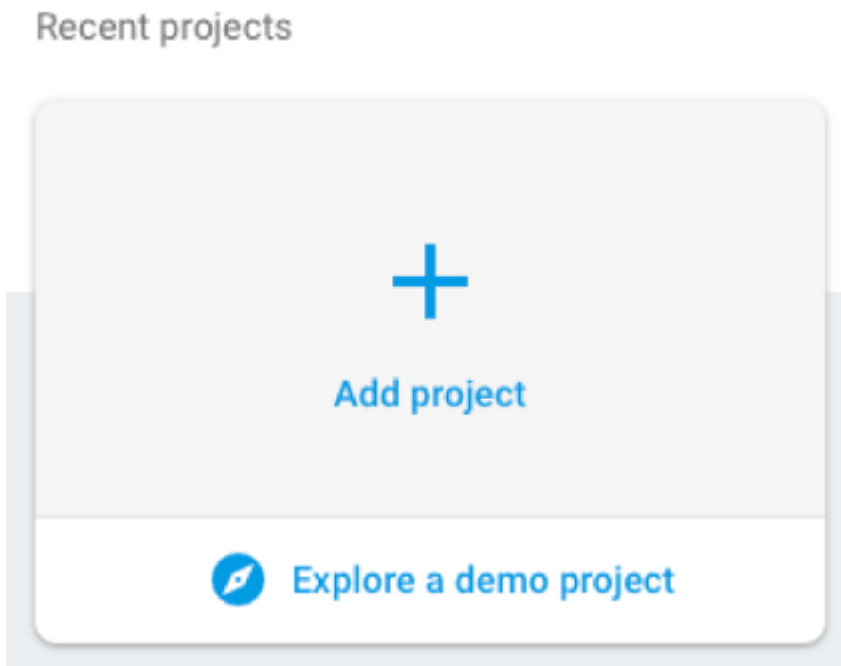


FCM 에 대해 Google 계정을 구성하려면

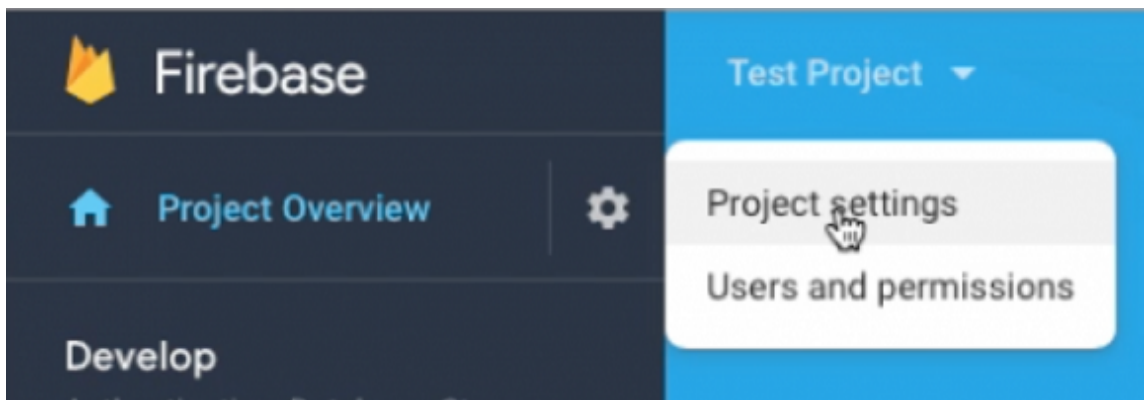
1. Google 개발자계정자격증명을 사용하여 다음 URL 에 로그인합니다.

<https://console.firebase.google.com/>

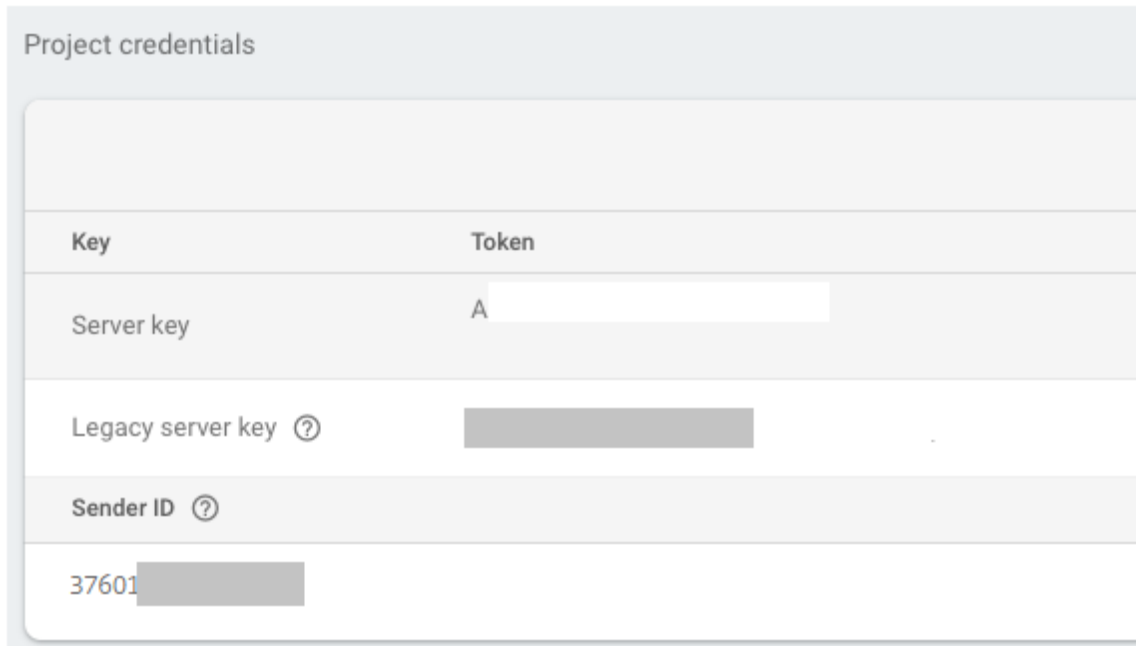
2. **Add project(프로젝트 추가)** 를 클릭합니다.



3. 프로젝트를 만든 후 **Project settings**(프로젝트설정) 를 클릭합니다.



4. **Cloud Messaging**(클라우드메시징) 탭을 클릭합니다. **Server key**(서버키) 와 **Sender ID**(보낸사람 ID) 값을 복사합니다. 다음절차에서 XenMobile 콘솔에 이러한 값을 붙여넣습니다. 2016 년 10 월부터는 Firebase 콘솔에서 서버 키를 만들어야 합니다.

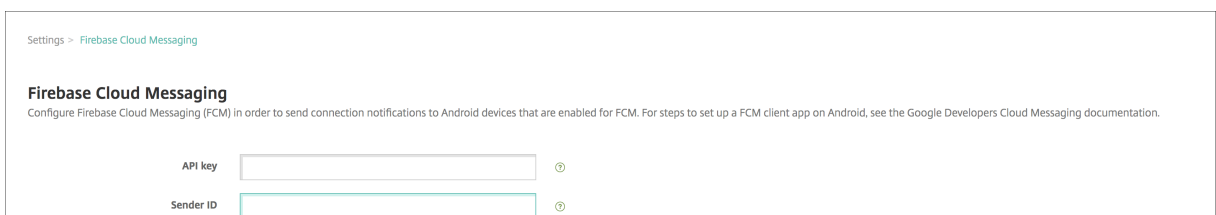


Android 에서 FCM 클라이언트 앱을 설정하는 단계는 이 Google Developers Cloud Messaging 문서 (<https://firebase.google.com/docs/cloud-messaging/android/client>) 를 참조하십시오.

XenMobile 을 FCM 에 대해 구성하려면

XenMobile 콘솔에서 설정 > **Firebase Cloud Messaging** 으로 이동합니다.

- **API** 키를 편집하고 Firebase Cloud Messaging 구성 마지막 단계에서 복사한 Firebase Cloud Messaging 서버 키를 입력합니다.
- 보낸 사람 **ID** 를 편집하고 이전 절차에서 복사한 보낸 사람 **ID** 값을 입력합니다.



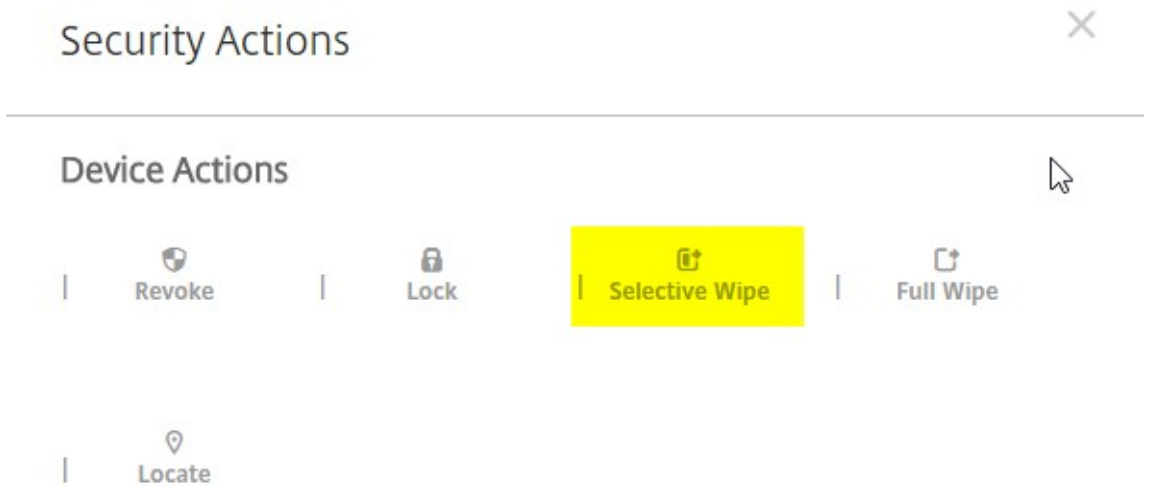
설정을 완료한 후 예약 장치 정책을 제거하거나 해당 정책을 변경하여 연결 빈도를 줄일 수 있습니다.

구성을 테스트하려면

1. Android 장치를 등록합니다.
2. XenMobile 에서 연결이 끊기기도 등록 장치를 유휴 상태로 잠시 둡니다.
3. XenMobile 콘솔에 로그인하고 관리를 클릭하고 Android 장치를 선택한 후 보안을 클릭합니다.

	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered	Activation
<input checked="" type="checkbox"/>		MDM MAM	[Redacted]	Android	6.0.1	Nexus 9	07/27/2016 06:05:25 pm	2 days	No	

4. 장치동작에서 선택적초기화를클릭합니다.



구성이성공적인경우장치에서선택적초기화가수행됩니다.

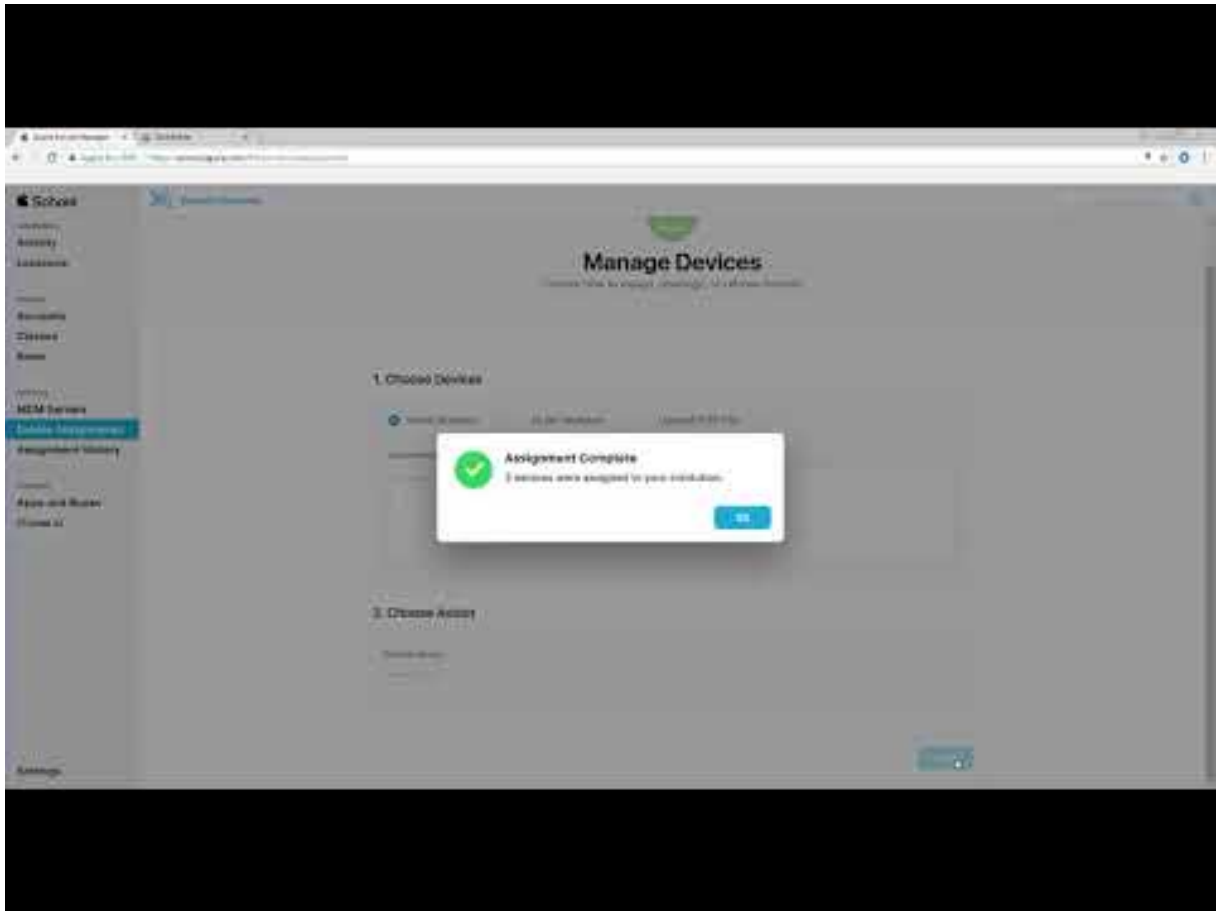
Apple 교육기능과통합

October 21, 2019

Apple 교육을사용하는환경에서 XenMobile Server 를 MDM(모바일기기관리) 솔루션으로사용할수있습니다. XenMobile 지원에는 Apple School Manager 및 iPad 용교실앱이포함됩니다. 새로운 XenMobile 교육구성장치정책은 Apple 교육을사용할강사및학생장치를구성합니다.

사전구성을마친감독되는 iPad 를강사와학생에게제공하십시오. 이구성에는 Apple School Manager DEP 의 XenMobile 등록, 새암호로구성된관리되는 Apple ID 계정과필수 VPP 앱및 iBooks 가포함됩니다.

다음비디오에서 Apple School Manager 와 XenMobile Server 에수행할수있는변경사항을간략히살펴볼수있습니다.



다음은 Apple 교육기능에대한 XenMobile 의주요지원입니다.

Apple School Manager

Apple School Manager 는교육기관에서사용되는 iOS 장치와 macOS 노트북을설정, 배포및관리할수있도록하는서비스입니다. Apple School Manager 에는 IT 관리자가다음을수행할수있는웹기반포털이포함되어있습니다.

- DEP 장치를여러 MDM 서버에할당합니다.
- 앱및 iBooks 를위한 VPP 라이선스를구매합니다.
- 관리되는 **Apple ID** 를대량으로생성합니다. 이사용자지정된 Apple ID 를사용하면 Apple 서비스에액세스하여 iCloud Drive 에문서를저장하고 iTunes 교육과정에등록하는등의작업을수행할수있습니다.

Apple School Manager 는교육 DEP 의한유형입니다. XenMobile 은비즈니스 DEP 와 Apple School Manager 등록을모두지원합니다.

여러개의 Apple School Manager DEP 계정을 XenMobile Server 에추가할수있습니다. 예를들어이기능을사용하면서로다른등록설정및설정도우미옵션을교육단위또는부서별로사용할수있습니다. 그런다음 DEP 계정을여러장치정책에연결할수있습니다.

Apple School Manager DEP 계정을 XenMobile 콘솔에 추가하면 XenMobile 이클래스 및 명단 정보를 검색합니다. 장치 설정시 XenMobile Server 는 다음을 수행합니다.

- 장치를 등록합니다.
- 배포에 구성된 리소스를 설치합니다 (예: 장치 정책, 교육 구성, 홈 화면 레이아웃 등). VPP 를 통해 구매한 앱과 iBooks 를 설치합니다.

사전 구성을 마친 장치를 강사와 학생에게 제공합니다. 분실 또는 도난 장치의 경우 MDM 분실 모드 기능을 사용하여 장치를 잠그고 찾을 수 있습니다.

iPad 용 Classroom 앱

iPad 용 Classroom 앱은 강사가 학생 장치에 연결하여 관리할 수 있도록 합니다. 장치 화면을 보고, iPad 에서 앱을 열고, 웹 링크를 공유하고, 앱을 열고, 학생 화면을 Apple TV 에 표시할 수 있습니다.

Classroom 은 App Store 에서 무료로 사용할 수 있습니다. XenMobile 콘솔에 앱을 업로드한 다음 교육 구성 장치 정책을 사용하여 강사 장치에 배포할 Classroom 앱을 구성합니다.

Apple 교육 기능에 대한 자세한 내용은 Apple [Education\(교육\)](#) 사이트 및 Apple [Education Deployment Guide\(교육 배포 가이드\)](#) 를 참조하십시오.

사전 요구 사항

- NetScaler Gateway
- 엔터프라이즈 (XME, MDM+MAM) 또는 MDM 모드로 구성된 XenMobile Server XenMobile Server 를 이미 XME 또는 MDM 모드로 구성한 경우 Apple School Manager 를 사용할 수 있습니다.
- Apple iPad 3 세대 (최소 버전) 또는 iPad Mini (iOS 9.3 이상)

참고:

- XenMobile Server 는 Apple School Manager 사용자 계정의 유효성을 LDAP 또는 Active Directory 에 대해 검사하지 않습니다. 그러나 XenMobile Server 를 LDAP 또는 Active Directory 에 연결하여 Apple School Manager 강사나 학생과 관련되지 않는 사용자 및 장치를 관리할 수 있습니다. 예를 들어 Active Directory 를 사용하여 Secure Mail 및 Secure Web 을 다른 Apple School Manager 구성원 (예: IT 관리자) 에게 제공할 수 있습니다.
- Apple School Manager 강사 및 학생은 로컬 사용자이므로 Citrix Secure Hub 를 강사 및 학생의 장치에 배포할 필요가 없습니다.
- NetScaler Gateway 인증이 포함되는 MAM 등록은 로컬 사용자를 지원하지 않습니다 (Active Directory 사용자만 지원). 따라서 XenMobile 은 필수 VPP 앱과 iBooks 만 강사와 학생의 장치에 배포합니다.

공유 iPad 에대한사전요구사항

- 모든 iPad Pro, iPad 5 세대, iPad Air 2 이상및 iPad 미니 4 이상
- 최소 32GB 의스토리지
- 감독됨

Apple School Manager 및 XenMobile Server 구성

Apple 또는 Apple 공인리셀러/통신사를통해 iPad 를구입한후이섹션의워크플로에따라 Apple School Manager 계정및 장치를설정하십시오. 이워크플로에는 Apple School Manager 포털과 XenMobile 콘솔에서수행하는단계가포함되어있습 니다.

다음지침에따라일대일모델 (학생당 iPad 1 대) 에서사용하는모든 iPad 또는강사 iPad(비공유) 에대한통합을구성합니다. 공유 iPad 를구성하려면공유 iPad 구성을참조하십시오.

1 단계: Apple School Manager 계정생성및설정도우미완료

Apple 배포프로그램에서업그레이드하려는경우 Apple 지원문서 [Prepare to upgrade to Apple School Manager\(Apple School Manager 로업그레이드준비하기\)](#)를참조하십시오. Apple School Manager 계정을생성하려면 <https://school.apple.com/>으로이동하고지침에따라등록합니다. Apple School Manager 에처음로그인하면설정도우 미가열립니다.

- Apple School Manager 사전요구사항, 설정도우미및관리작업에대한자세한내용은 [Apple School Manager help\(Apple School Manager 도움말\)](#)를참조하십시오.
- Apple School Manager 를설정할때는 Active Directory 도메인이름과다른도메인이름을사용합니다. 예를들어 Apple School Manager 도메인이름에 **appleid** 같은접두사를추가합니다.
- Apple School Manager 를명단데이터에연결하면 Apple School Manager 가강사및학생이사용할, 관리되는 Apple ID 를생성합니다. 명단데이터에는강사, 학생및클래스가포함됩니다. Apple School Manager 에명단데 이터를추가하는방법에대한자세한내용은 [Apple School Manager help\(Apple School Manager 도움말\)](#)에서 “Find staff, students and classes(직원, 학생및클래스찾기)” 아래의문서를참조하십시오.
- [Apple School Manager help\(Apple School Manager 도움말\)](#)의 “Managed Apple IDs(관리되는 Apple ID)” 에나온설명에따라관리되는 Apple ID 형식을해당교육기관에맞게사용자지정할수있습니다.

중요:

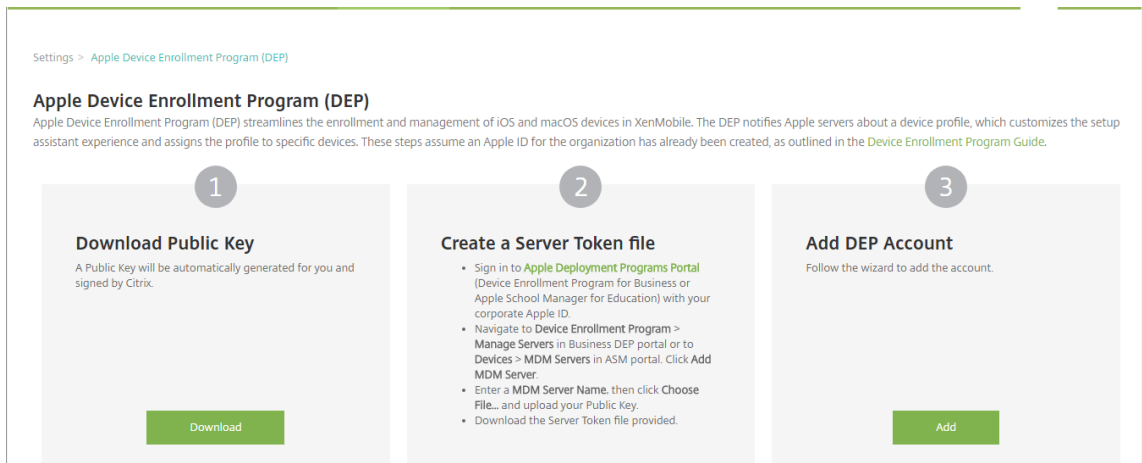
Apple School Manager 정보를 XenMobile Server 로가져온후에는관리되는 Apple ID 를변경하지마십 시오.

- 리셀러또는통신사를통해장치를구매한경우이러한장치를 Apple School Manager 에연결합니다. 자세한내용은 [Apple School Manager help\(Apple School Manager 도움말\)](#)에서 “Manage devices(장치관리)” 아래문 서를참조하십시오.

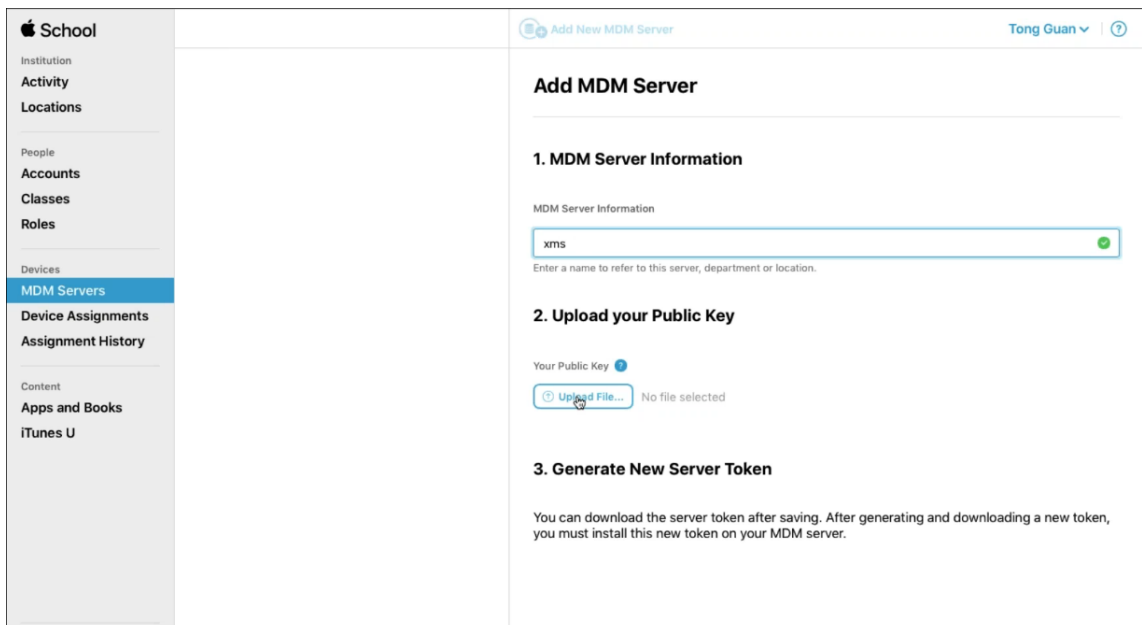
2 단계: XenMobile Server 를 Apple School Manager 의 MDM 서버로구성하고장치할당구성

Apple School Manager 포털에는 **MDM Servers(MDM 서버)** 탭이있습니다. 이설정을완료하려면 XenMobile Server 의공개키파일이필요합니다.

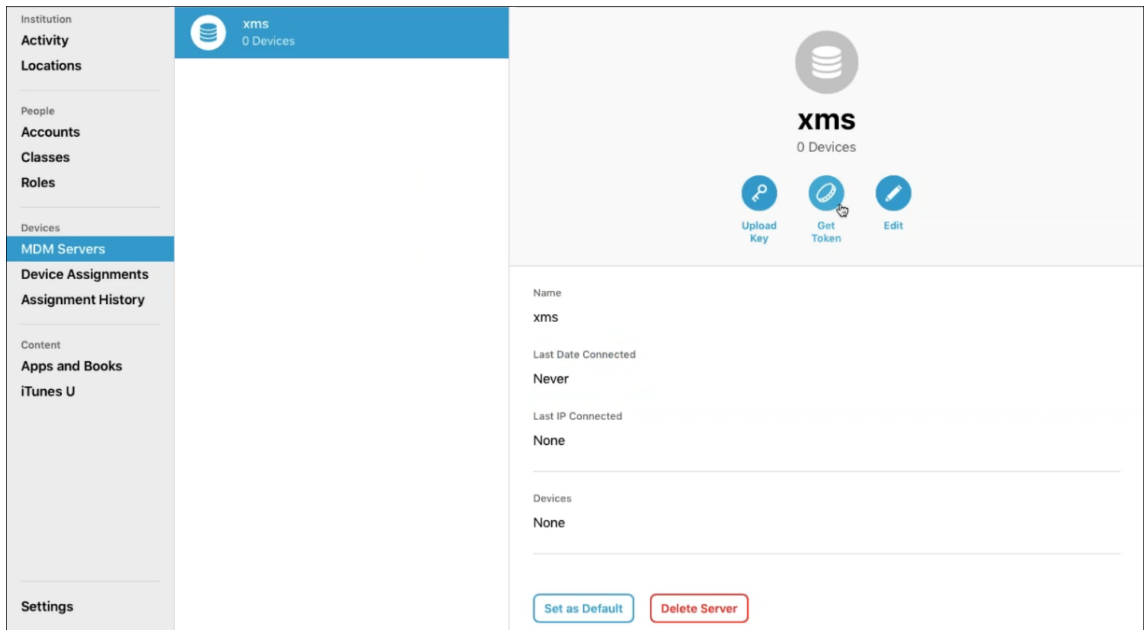
1. XenMobile Server 에대한공개키를로컬컴퓨터에다운로드합니다. XenMobile 콘솔에로그온하고 설정 > **Apple DEP(장치등록프로그램)** 로이동합니다.



2. 공개키다운로드에서 다운로드를클릭하고 PEM 파일을저장합니다.
3. Apple School Manager 포털에서 **MDM Servers(MDM 서버)** 를클릭하고 XenMobile Server 이름을입력합
니다. 입력하는서버이름은참조용이며서버의 URL 또는이름이아닙니다.
4. **Upload your Public Key(공개키업로드)** 에서 **Upload File(파일업로드)** 을클릭합니다.



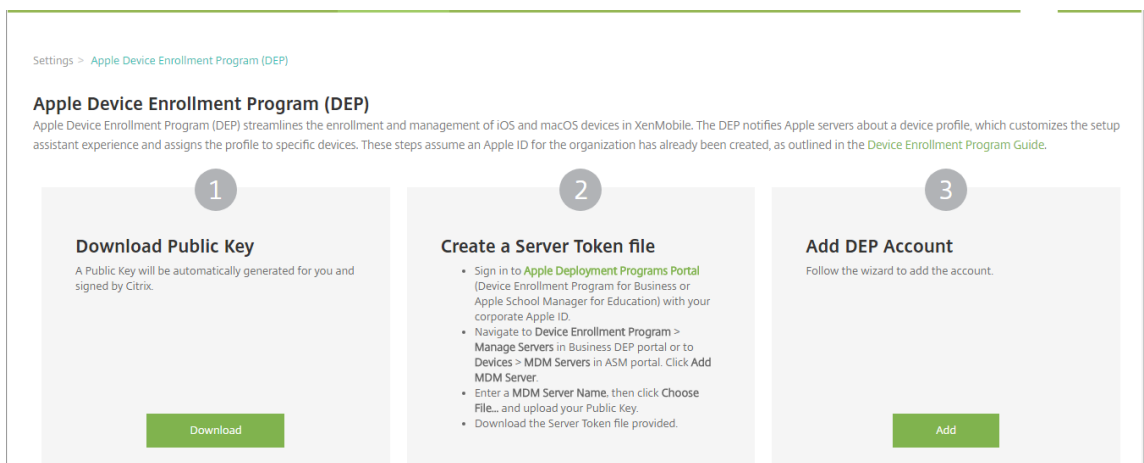
5. XenMobile Server 에서다운로드한서버키를업로드하고 **Save(저장)** 를클릭합니다.
6. 서버토큰을생성합니다. **Get Token(토큰가져오기)** 을클릭하고서버토큰파일을컴퓨터에다운로드합니다.



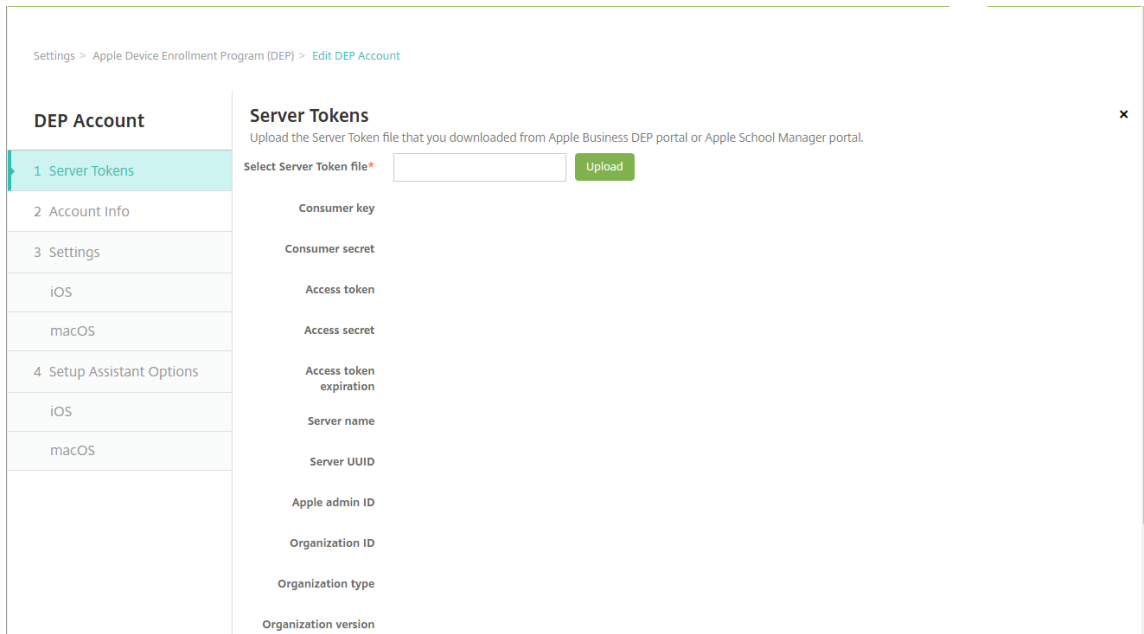
7. **Device Assignments(장치할당)** 를 클릭하고 장치할당 방법을 선택한 후 요청된 정보를 제공합니다. 자세한 내용은 [Apple School Manager help\(Apple School Manager 도움말\)](#)에서 Assign devices(장치할당) 섹션을 참조하십시오.
8. **Choose Action(동작선택)** 아래 **Perform Action(동작수행)** 메뉴에서 **Assign to Server(서버에할당)** 를 클릭합니다. **MDM Server(MDM 서버)** 메뉴에서 장치를 관리할 XenMobile Server 를 클릭하고 **Done(완료)** 을 클릭합니다.

3 단계: XenMobile Server 에 Apple School Manager 계정 추가

1. XenMobile 콘솔에서 설정 > **Apple DEP(장치등록프로그램)** 로 이동하고 **DEP** 계정 추가에서 추가를 클릭합니다.



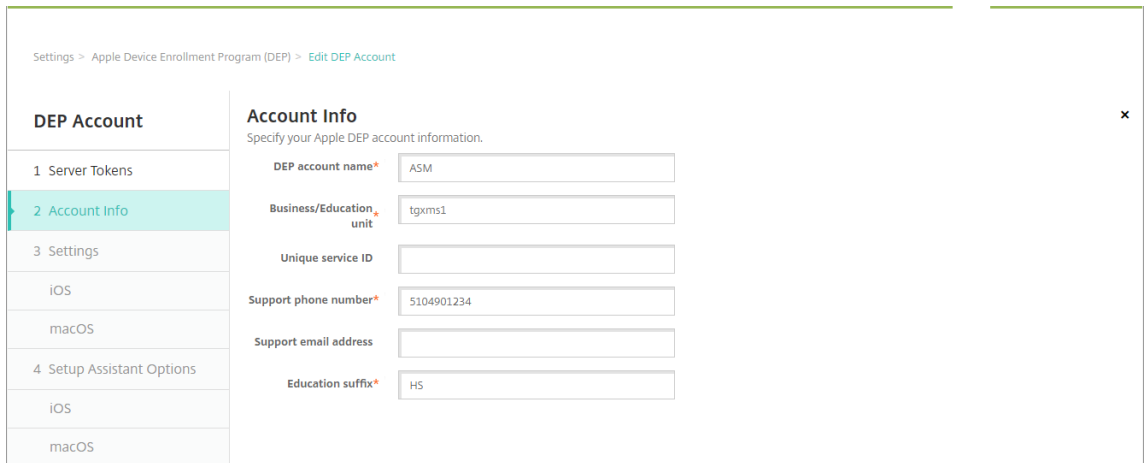
2. 서버토큰페이지에서 업로드를 클릭하고 Apple School Manager 포털에서 다운로드한 서버토큰파일 (.p7m) 을 선택합니다. 토큰정보페이지가 나타납니다.



참고:

- 조직 ID 는 DEP 의고객 ID 입니다.
- Apple School Manager 계정의 조직유형은 교육이고 조직버전은 v2 입니다.

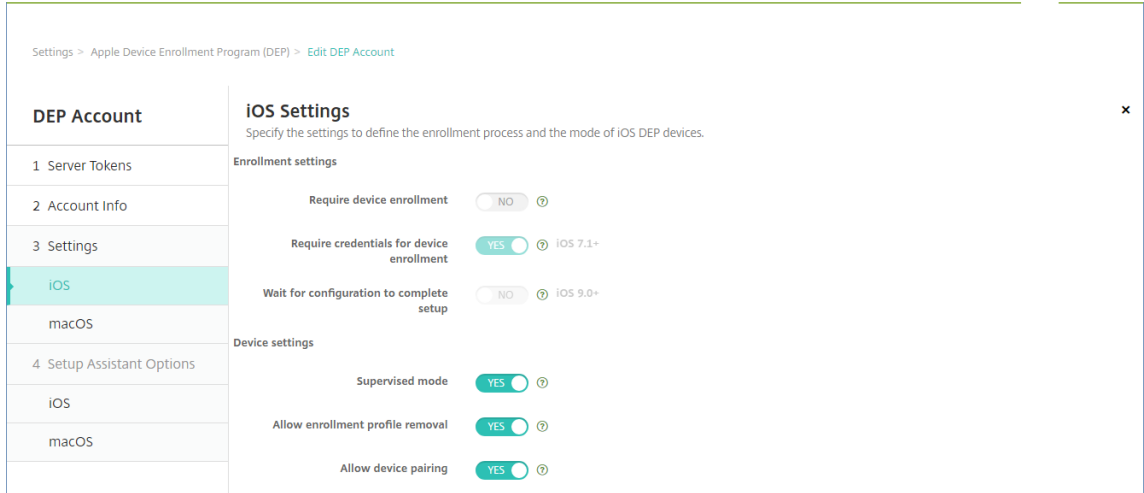
3. 계정정보페이지에서다음설정을지정합니다.



- **DEP 계정 이름:** 이 DEP 계정의 고유한 이름입니다. 국가 또는 조직 계층 구조별과 같이 DEP 계정을 구성하는 방식을 반영하는 이름을 사용합니다.
- **Business/Education unit(비즈니스/교육 단위):** 장치를 할당할 교육 단위 또는 부서입니다. 이것은 필수 필드입니다.
- **고유 서비스 ID:** 계정을 식별하는데 도움이 되는 선택적 고유 ID 입니다.
- **지원전화번호:** 사용자가 설정 중에 전화할 수 있는 지원전화번호입니다. 이것은 필수 필드입니다.
- **지원전자메일주소:** 최종 사용자에게 제공되는 선택적 지원전자메일주소입니다.

- **교육접미사:** 지정된 Apple School Manager DEP 계정의클래스에플래그를지정합니다. VPP 접미사는지정된 VPP 계정의앱및 iBooks 에플래그를지정합니다. Apple School Manager DEP 와 Apple School Manager VPP 의두계정에동일한접미사를사용하는것이 좋습니다.

4. 다음을클릭합니다. **iOS** 설정에서다음설정을지정합니다.



• 등록설정

- 장치등록필요: 사용자가장치를등록해야합니다. 이설정을 아니요로변경합니다.
- 장치등록에자격증명필요: DEP 설정중에서사용자가자격증명을입력해야합니다. Apple School Manager 를 XenMobile Server 와통합하는경우이설정은기본적으로 예입니다.
- 구성에서설정을완료할때까지대기: 모든 MDM 리소스가장치에배포될때까지사용자가설정도우미모드에있어야하는지여부를설정합니다. Apple School Manager 를 XenMobile Server 와통합하는경우이설정은기본적으로 아니요입니다. Apple 설명서에따르면장치가설정도우미모드에있는동안에는다음명령이작동하지않을수 있습니다.

- * InviteToProgram
- * InstallApplication
- * InstallMedia
- * ApplyRedemptionCode

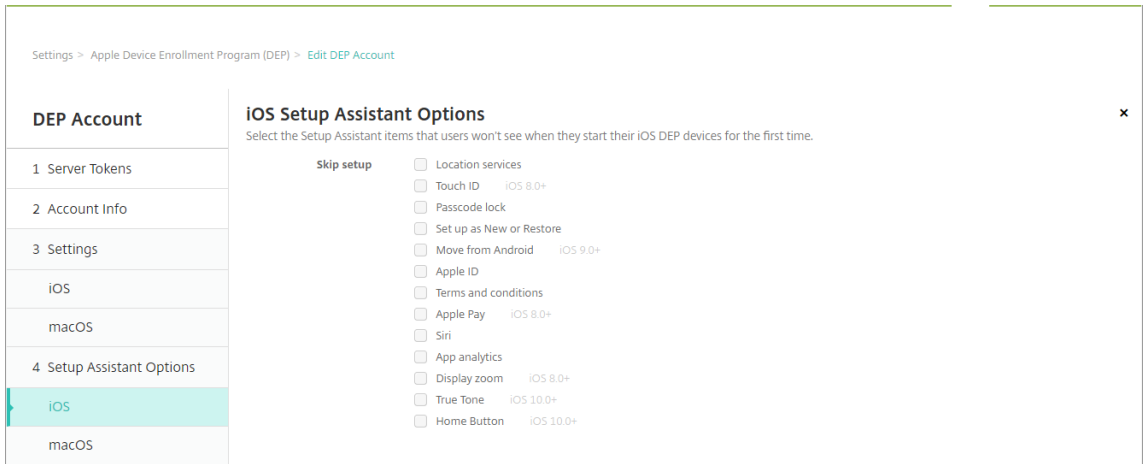
• 장치설정

- 감독모드: iOS 장치를감독모드로전환합니다. 기본값인 예를변경하지마십시오. iOS 장치의감독모드전환에 대한자세한내용은 [Apple Configurator](#) 를 사용하여 **iOS 장치를감독모드로전환**을참조하십시오.
- 등록프로필제거허용: Apple School Manager 통합의경우사용자가장치에서등록프로필을제거할수있도록합니다. 이설정을 예로변경합니다.
- 장치페어링허용: Apple School Manager 통합의경우 iTunes 및 Apple Configurator 를통해관리할수있도록장치페어링을허용합니다. 이설정을 예로변경합니다.

5. **iOS** 설정도우미옵션에서사용자가장치를처음으로시작할때건너뛴 iOS 설정도우미단계를선택합니다. 기본적으로설정도우미에는모든단계가포함됩니다. 설정도우미에서단계를제거하면사용자환경이간소화됩니다.

중요:

Apple ID 및 약관단계는포함하는것이 좋습니다. 이단계는강사와학생이관리되는 Apple ID 의새암호를입력하고필수약관에동의하는데사용됩니다.



- **위치서비스:** 장치에위치서비스를설정합니다.
- **Touch ID:** iOS 8.0 이상장치에서 Touch ID 를설정합니다.
- **암호잠금:** 장치에대한암호를만듭니다.
- **새로설정또는복원:** 장치를새로설정하거나 iCloud 또는 iTunes 백업에서복원합니다.
- **Android** 에서이동: Android 장치의데이터를 iOS 9 이상장치로전송할수있도록합니다. 이옵션은 새로설정또는복원을선택한경우에만사용할수있습니다 (즉, 단계가생략됨).
- **Apple ID:** 장치에대한 Apple ID 계정을설정합니다. 확인란을선택하여이단계를포함하는것이 좋습니다.
- **약관:** 사용자가장치사용에대한약관에동의해야합니다. 확인란을선택하여이단계를포함하는것이 좋습니다.
- **Apple Pay:** iOS 8.0 이상장치에 Apple Pay 를설정합니다.
- **Siri:** 장치에서 Siri 를사용하거나사용하지않습니다.
- **앱분석:** 충돌데이터및사용현황통계를 Apple 과공유할지여부를설정합니다.
- **표시확대/축소:** iOS 8.0 이상장치에서디스플레이해상도 (표준또는확대) 를설정합니다.
- **True Tone:** iOS 10.0 장치 (최소버전) 에서 True Tone 디스플레이를설정합니다.
- **홈버튼:** iOS 10.0 장치 (최소버전) 에서홈버튼화면민감도를설정합니다.

6. DEP 계정이 설정 > **Apple DEP**(장치등록프로그램) 에 표시됩니다. XenMobile Server 와 Apple School Manager 계정간의연결을테스트하려면계정을선택하고 연결테스트를클릭합니다.

Apple Device Enrollment Program (DEP)
 Apple Device Enrollment Program (DEP) streamlines the enrollment and management of iOS and macOS devices in XenMobile. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. These steps assume an Apple ID for the organization (Business or Education) has already been created, as outlined in the [Device Enrollment Program Guide](#).

- 1 Download Public Key**
 A Public Key will be automatically generated for you and signed by Citrix.
 [Download]
- 2 Create a Server Token file**
 - Sign in to [Apple Deployment Programs Portal](#) (Device Enrollment Program for Business or Apple School Manager for Education) with your corporate Apple ID.
 - Navigate to [Device Enrollment Program > Manage Servers](#) in Business DEP portal or to [Devices > MDM Servers](#) in ASM portal. Click [Add MDM Server](#).
 - Enter a [MDM Server Name](#), then click [Choose File...](#) and upload your Public Key.
 - Download the Server Token file provided.
- 3 Add DEP Account**
 Follow the wizard to add the account.
 [Add]

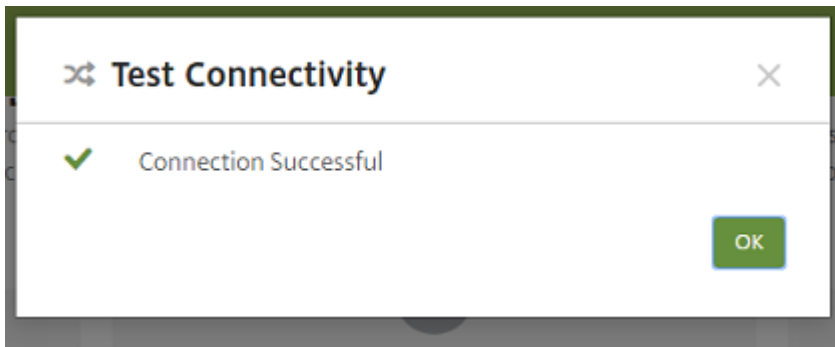
Edit | Disable | Test Connectivity | Delete

<input type="checkbox"/>	DEP account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
<input checked="" type="checkbox"/>	ASM	bxms1	Enabled	Education	xenmobileschool@outlook.com	21/07/2017 14:41:27	21/07/2018 21:39:48
<input type="checkbox"/>	DEP	t...	Enabled	Business	CitrixXenmobileVPP@out...		

Showing 1 - 2 of 2 items

Edit | Disable | Test Connectivity | Delete

상태메시지가나타납니다.



몇분후 Apple School Manager 의사용자계정이 관리 > 사용자페이지에나타납니다. XenMobile Server 는각사용자에대해가져온, 관리되는 Apple ID 를바탕으로로컬사용자계정을생성합니다. 다음예에서사용자계정에대해사용자지정된 Apple ID 도메인이름접두사는 **appleid** 입니다.

Devices | **Users** | Enrollment Invitations

Users [Show filter](#)

| | |

<input type="checkbox"/>	User name	First name	Last name	User type	Roles	Groups	Domain	Created	Last authenticated	ASM DEP account name
<input type="checkbox"/>	[blurred]	Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Lucas	Leong	ASM	USER	SAMPLE-CLASS-1013,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Alex	Mieuli	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Savannah	Cashman	ASM	USER	SAMPLE-CLASS-1010,SAMPLE-CLASS-1011	local	6/6/17 3:21 PM	6/13/17 6:46 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Aiden	Westover	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Ava	Meinerth	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Liam	Willson	ASM	USER	SAMPLE-CLASS-1013,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Brayden	Anderson	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Gabriel	Zeifman	ASM	USER	SAMPLE-CLASS-1012,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account
<input type="checkbox"/>	[blurred]	Gavin	Tien	ASM	USER	SAMPLE-CLASS-1012,SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM DEP account

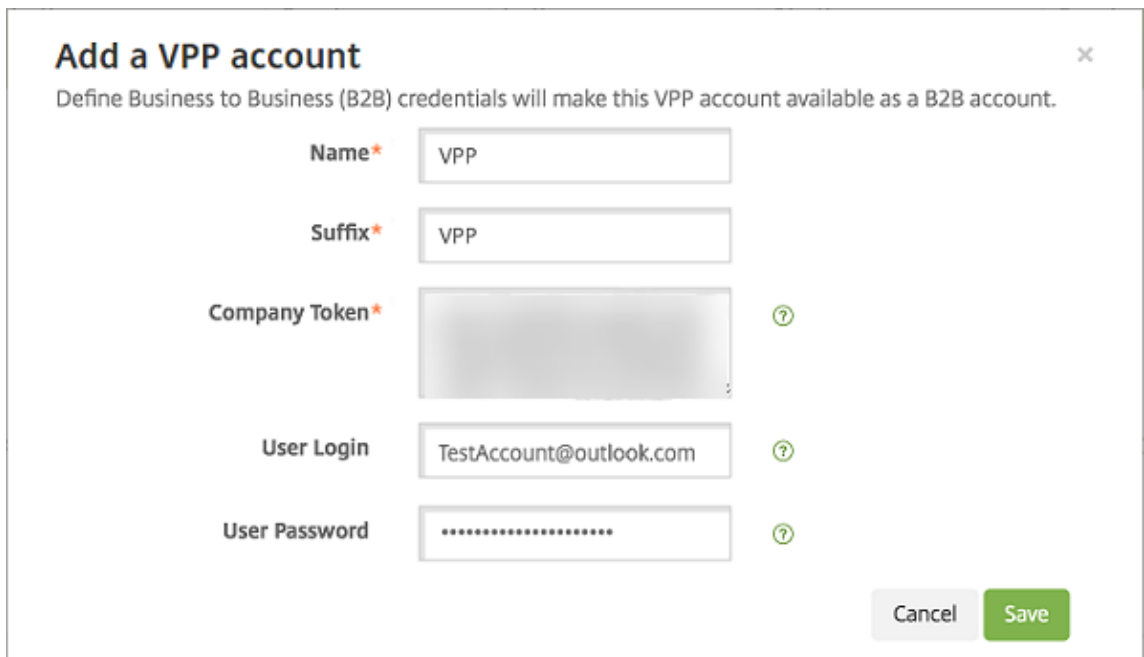
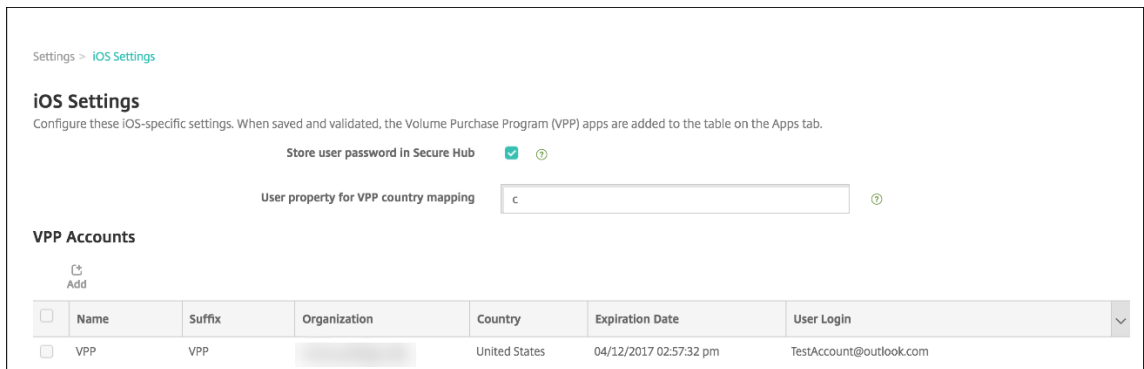
Showing 51 - 60 of 83 items | Items per page: 10 | Page: 6 of 9

지정된 Apple School Manager DEP 계정에대한모든사용자를찾으려면사용자검색필터에게정 이름을입력합니다.

4 단계: Apple School Manager 의교육 VPP 계정구성

이섹션에서는앱및 iBooks 용 VPP 라이선스를구매할때사용한 VPP 계정을 XenMobile 에지정합니다.

1. Apple School Manager 에대한교육 VPP 계정을구성하려면 [iOS Volume Purchase Program](#)의지침을따르십시오. VPP 계정추가화면에서회사토큰을입력해야합니다. 교육 VPP 계정 (<https://volume.apps.apple.com/us/store>) 에서직접토큰을다운로드하고 **VPP** 계정추가화면에붙여넣습니다.



2. VPP 라이선스를 XenMobile Server 로가져오는동안몇분정도가다리십시오.

5 단계: Apple School Manager 사용자의암호추가

Apple School Manager DEP 계정을추가하면 XenMobile Server 가 Apple School Manager 의클래스와사용자를가져옵니다. XenMobile 에서클래스는로컬그룹으로처리되며콘솔에서 “그룹” 이라는용어가사용됩니다. Apple

School Manager 에서그룹이름이있는클래스의경우 XenMobile 이해당그룹이름을클래스에할당합니다. 그렇지않은경우 XenMobile 은소스시스템 ID 를그룹이름으로사용합니다. 과정이름은 Apple School Manager 에서고유하지않으므로 XenMobile 은과정이름을클래스이름으로사용하지않습니다.

XenMobile 은관리되는 Apple ID 를사용하여사용자유형이 **ASM** 인로컬사용자를생성합니다. 사용자가로컬인이유는 Apple School Manager 가모든외부데이터원본과별개로자격증명을생성하기때문입니다. 따라서 XenMobile 은이러한사용자를인 증할때디렉터리서버를사용하지않습니다.

Apple School Manager 는 XenMobile Server 에임시사용자암호를보내지않습니다. CSV 파일로가져오거나수동으로추 가해야합니다. 임시사용자암호를가져오려면:

1. 관리되는 Apple ID 의임시암호를생성할때 Apple School Manager 에서생성된 CSV 파일을가져옵니다.
2. CSV 파일을편집하여임시암호를사용자가 XenMobile Server 에등록할때제공한새암호로바꿉니다. 이목적으로사용 하는암호유형에는제한이없습니다.

CSV 파일의입력형식은다음과같습니다. `firslast@appleid.citrix.com,Firstname,Middle, Lastname,Citrix123!`

여기서:

사용자: `firstlast@appleid.citrix.com`

이름: `Firstname`

중간이름: `Middle`

성: `Lastname`

암호: `Citrix123!`

3. XenMobile 콘솔에서 관리 > 사용자를클릭합니다. 사용자페이지가나타납니다.

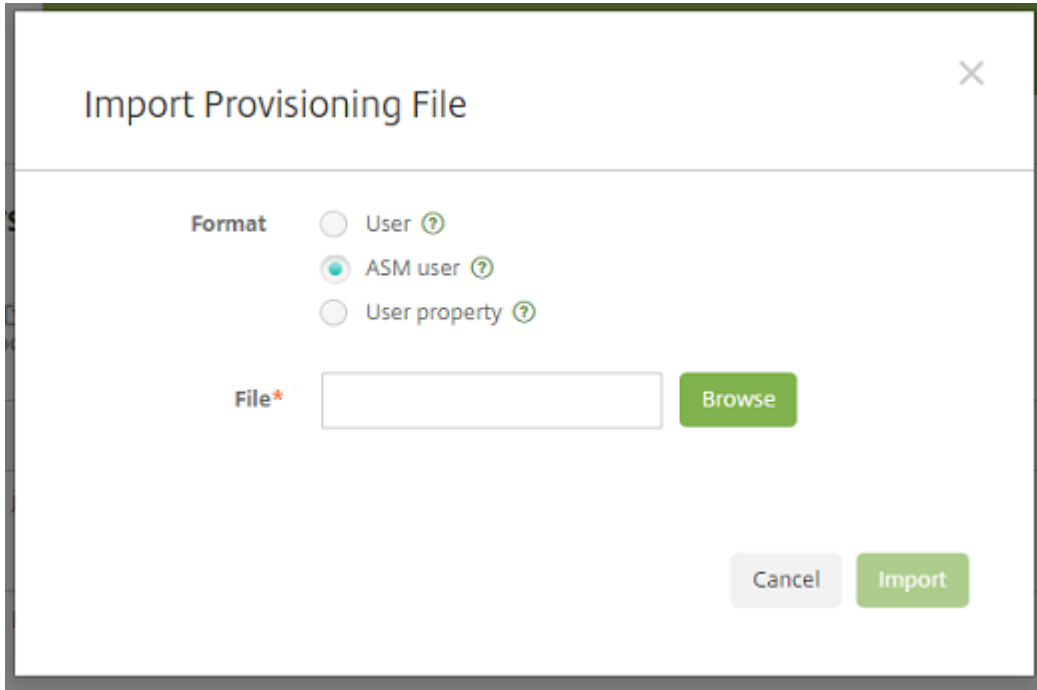
다음 관리 > 사용자화면샘플에는 Apple School Manager 에서가져온사용자목록이나와있습니다. 사용자목록에서:

- 사용자이름에는관리되는 Apple ID 가표시됩니다.
- 사용자유형은 **ASM** 이고 Apple School Manager 에서생성된계정임을나타냅니다.
- 그룹에는클래스가표시됩니다.

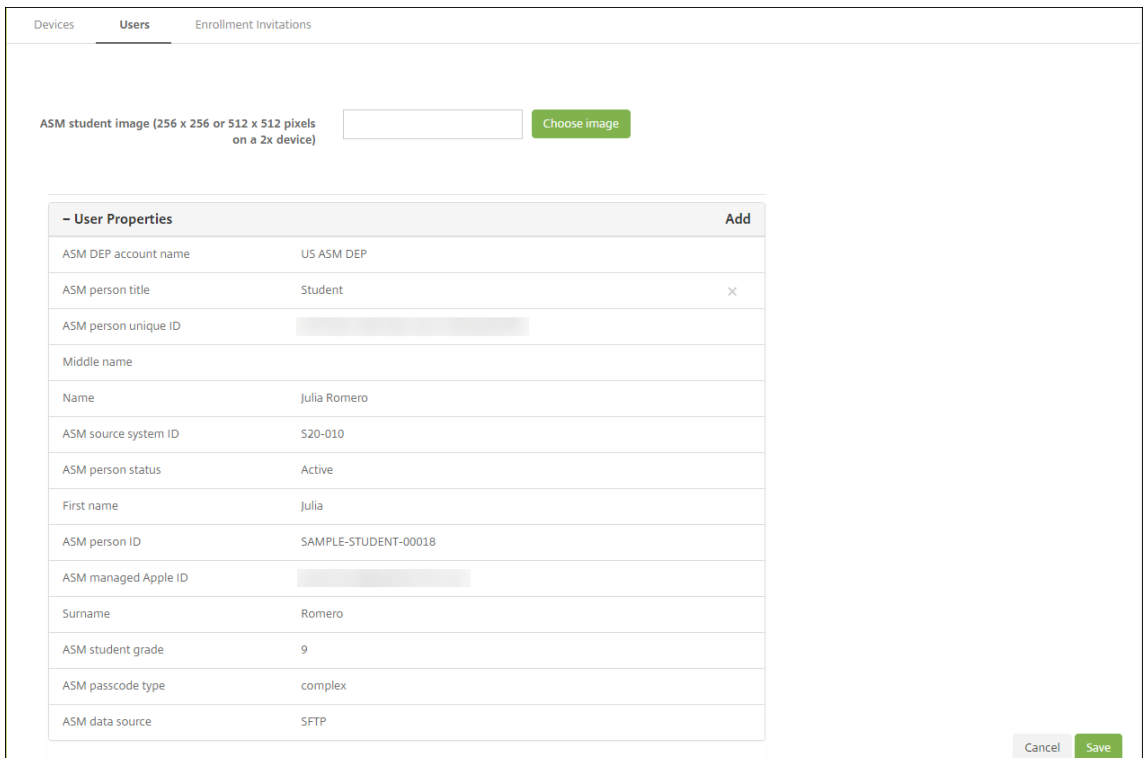
User name	First name	Last name	User type	Roles	Groups	Domain	Created
[Redacted]	Julia	Romero	ASM	USER	SAMPLE-CLASS-1013 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00
[Redacted]	Kaelyn	Lazzara	ASM	USER	SAMPLE-CLASS-1013 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00
[Redacted]	Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010 - HS,SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00

4. 로컬사용자가져오기를클릭합니다. 프로비저닝파일가져오기대화상자가나타납니다.

5. 형식으로 **ASM** 사용자를선택하고, 2 단계에서준비한 CSV 파일로이동한후 가져오기를클릭합니다.



6. 로컬사용자의속성을보려면사용자를선택하고 편집을클릭합니다.



이름속성에더해다음과같은 Apple School Manager 속성이나타납니다.

- **ASM DEP** 계정: XenMobile Server 에서계정에지정한이름입니다.

- **ASM 사용자직위:** 강사, 학생또는기타입니다.
- **ASM 사용자고유 ID:** 사용자의고유식별자입니다.
- **ASM 소스시스템 ID:** 조직에서사용자에게구성한식별자입니다.
- **ASM 사용자상태:** 관리되는 Apple ID 가 활성화또는 비활성인지여부를지정합니다. 사용자가관리되는 Apple ID 계정에대한새암호를제공하면이상태가활성으로전환됩니다.
- **ASM 관리되는 Apple ID:** 관리되는 Apple ID 에는교육기관이름과 **appleid** 가포함될수있습니다. 예를들어 ID 는 johnappleseed@appleid.myschool.edu 와유사할수있습니다. XenMobile Server 는관리되는 Apple ID 를인증에사용합니다.
- **ASM 학생학년:** 학생의학년정보입니다 (강사에게는사용되지않음).
- **ASM 암호유형:** 사용자의암호정책으로, 복합형식 (학생암호가아닌암호로, 8 자이상숫자및문자로구성됨), 4(자리) 또는 6(자리) 입니다.
- **ASM 데이터원본:** 클래스의데이터원본입니다 (예: **CSV** 또는 **SFTP**).

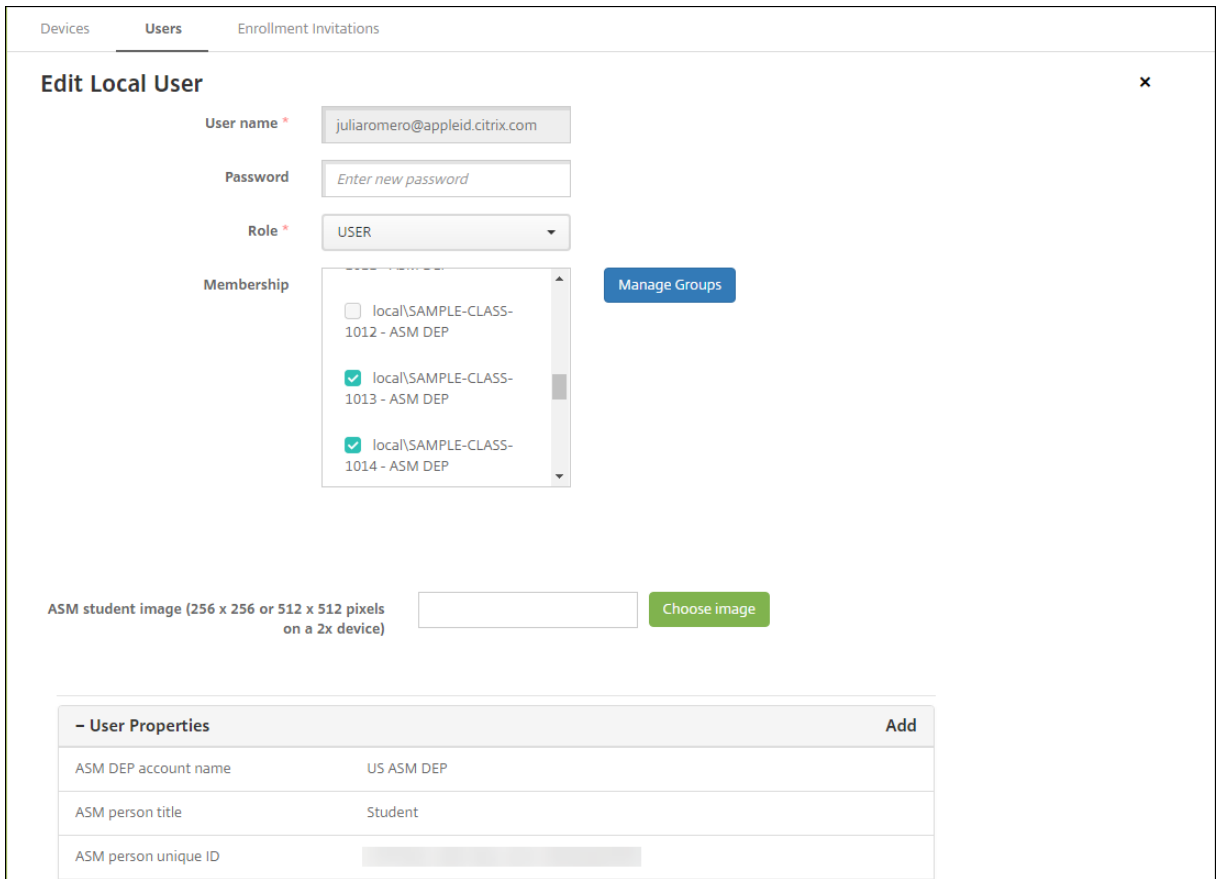
6 단계: 학생의사진추가 (선택사항)

각학생의사진을추가할수있습니다. 강사가 Apple Classroom 앱을사용하는경우이앱에서사진이나타납니다.

사진권장사항:

- 해상도: 256 x 256 픽셀 (2x 장치의경우 512 x 512 픽셀)
- 형식: JPEG, PNG 또는 TIFF

사진을추가하려면 관리 > 사용자에서사용자를선택하고 편집을클릭한후 이미지선택을클릭합니다.



7 단계: 리소스및배달그룹을계획하고 **XenMobile Server** 에추가

배달그룹은사용자범주에배포할리소스를정의합니다. 예를들어강사와학생에대한배달그룹하나를생성하거나여러배달그룹을생성하여여러강사또는학생에게전송되는앱, 미디어및정책을사용자지정할수있습니다. 클래스당하나이상의배달그룹을생성할수있습니다. 또한관리자 (교육기관의다른직원) 를위한하나이상의배달그룹을생성할수있습니다.

사용자장치에배포하는리소스에는장치정책, VPP 앱및 iBooks 가포함됩니다.

- 장치정책:

강사가 Classroom 앱을사용하는경우교육구성장치정책이필요합니다. 다른장치정책을검토하여강사및학생의 iPad 를 구성하고제한하는방법을결정하십시오.

- VPP 앱:

XenMobile 을사용하려면 VPP 앱을교육사용자의필수앱으로배포해야합니다. XenMobile Server 는 VPP 앱의선택적배포를지원하지않습니다.

Apple Classroom 앱을사용하는경우강사장치에만앱을배포하십시오.

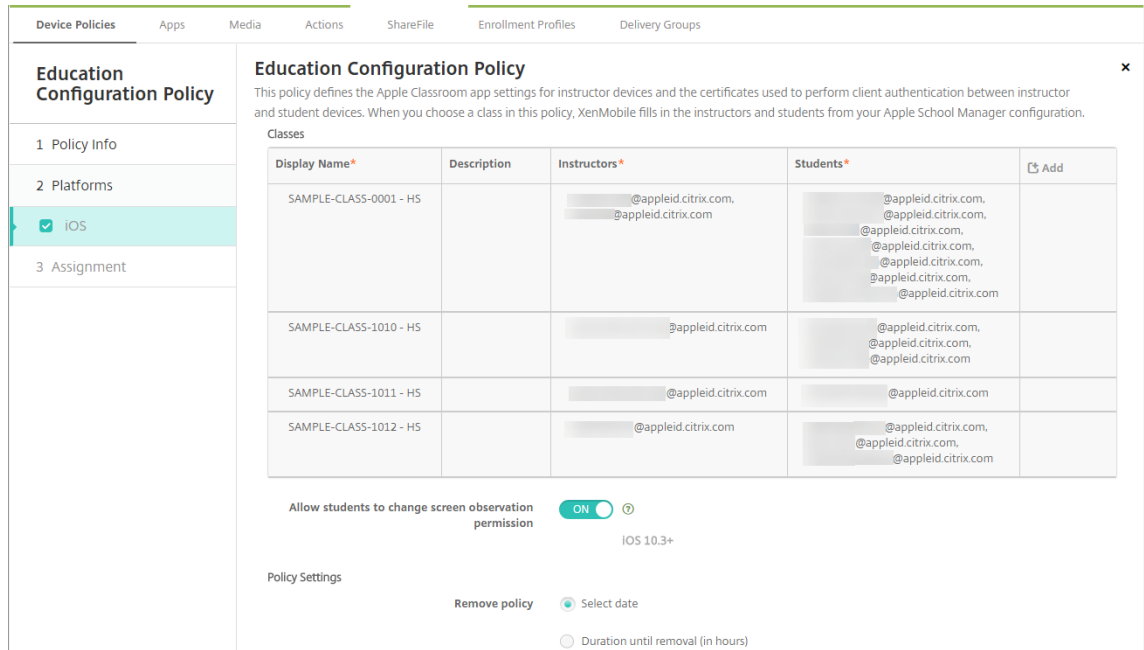
강사또는학생에게제공하려는다른앱을배포합니다. 이솔루션은 Citrix Secure Hub 앱을사용하지않으므로강사또는학생에게이앱을배포하지않아도됩니다.

• VPP iBooks:

XenMobile Server 가 Apple School Manager VPP 계정에연결하면구매한 iBooks 가 XenMobile 콘솔의 구성 > 미디어에나타납니다. 이페이지에나열되는 iBooks 는배달그룹에추가할수있습니다. XenMobile Server 는 iBooks 를필수미디어로만지원합니다.

강사및학생을위한리소스및배달그룹을계획한후에는이러한항목을 XenMobile 콘솔에서생성할수있습니다.

1. 강사또는학생장치에배포할장치정책을생성합니다. 교육구성장치정책에대한자세한내용은 [교육구성장치정책](#)을참조하십시오.

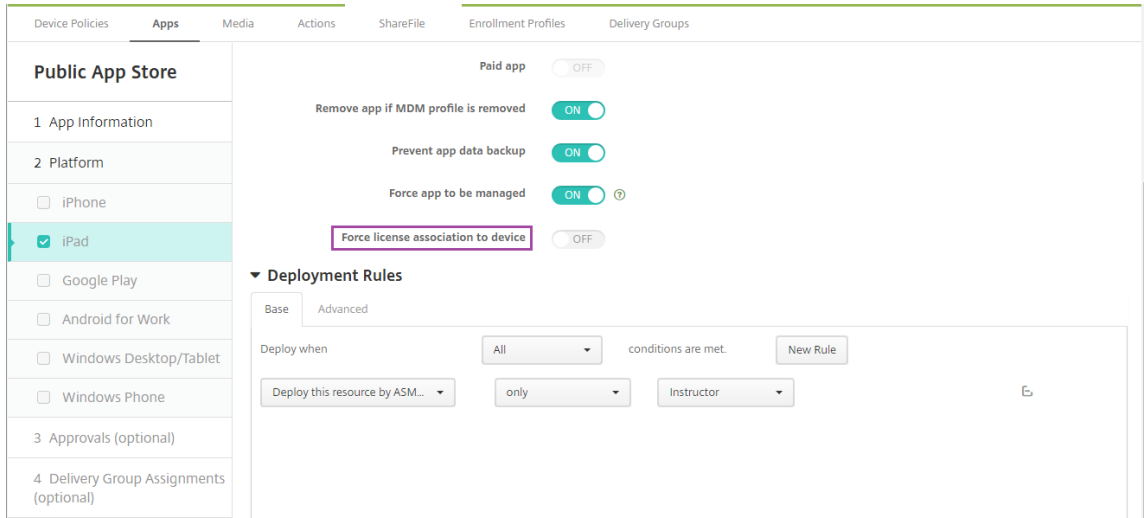


장치정책에대한자세한내용은 [장치정책](#)과개별정책문서를참조하십시오.

2. 앱 (구성 > 앱) 과 iBooks(구성 > 미디어) 를구성합니다.

- 기본적으로 XenMobile 은앱및 iBooks 를사용자수준에서할당합니다. 첫배포시강사및학생에게는 VPP 등록메시지가표시됩니다. 사용자가초대를수락하면다음배포 (6 시간이내) 시 VPP 앱과 iBooks 가전송됩니다. 새 VPP 사용자에게앱및 iBooks 의배포를강제하는것이 좋습니다. 그러려면배달그룹을선택하고 배포를클릭합니다.

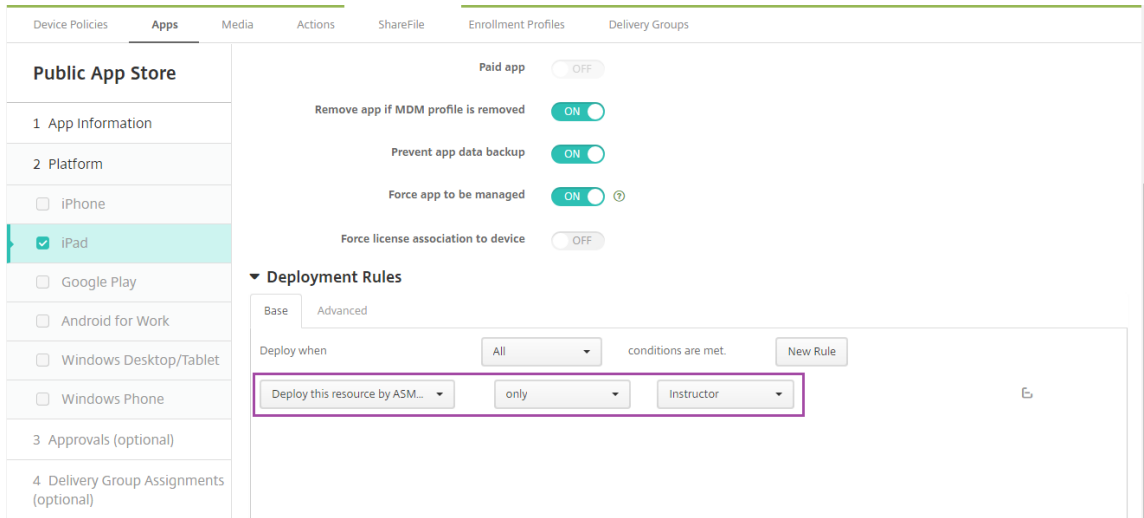
장치수준에서앱 (iBooks 제외) 을할당하도록선택할수있습니다. 그러려면 장치에강제로라이선스연결설정을켜짐으로변경합니다. 장치수준에서앱을할당하면사용자에게 VPP 프로그램가입을위한초대가전송되지않습니다.



- 강사에게만 앱을 배포하려면 강사만 포함된 배달 그룹을 선택하거나 다음 배포 규칙을 사용합니다.

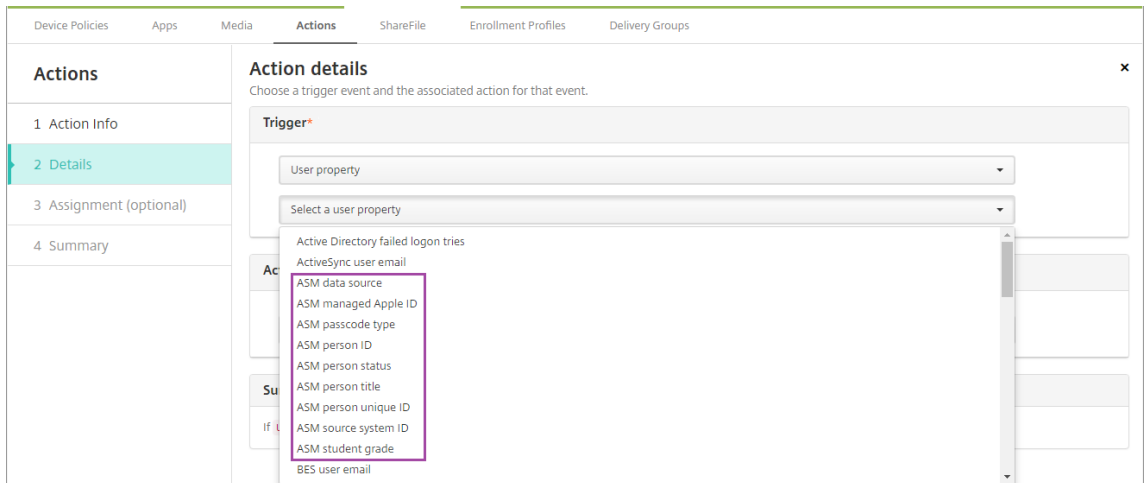
```

1 Deploy this resource by ASM DEP device type
2 only
3 Instructor
    
```



- VPP 앱 추가 관련 도움말은 [공용 앱 스토어 앱 추가](#)를 참조하십시오.

3. 선택 사항입니다. Apple School Manager 사용자 속성을 기반으로 동작을 생성합니다. 예를 들어 새 앱이 설치될 때 학생 장치에 알림을 보내는 동작을 생성할 수 있습니다. 또는 다음 예제에 표시된 것과 같이 사용자 속성이 트리거하는 동작을 생성할 수 있습니다.



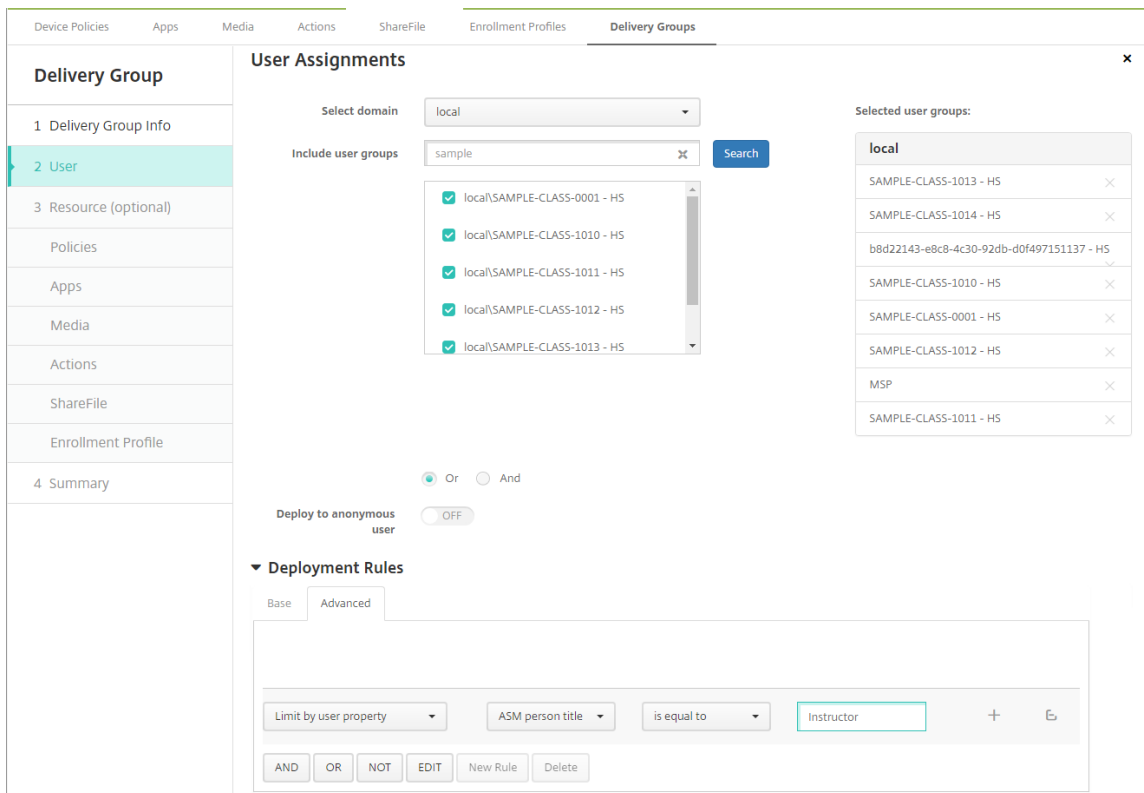
동작을 생성하려면 구성 > 동작으로 이동합니다. 동작 구성에 대한 자세한 내용은 [자동화된 동작](#)을 참조하십시오.

4. 구성 > 배달 그룹에서 강사 및 학생을 위한 배달 그룹을 생성합니다. Apple School Manager 에서 가져온 클래스를 선택합니다. 또한 강사 및 학생에 대한 배포 규칙을 생성합니다.

예를 들어 다음은 강사에 대한 사용자 할당입니다. 배포 규칙은 다음과 같습니다.

```

1 Limit by user property
2 ASM person title
3 is equal to
4 Instructor
    
```



다음은학생에대한사용자할당입니다. 배포규칙은다음과같습니다.

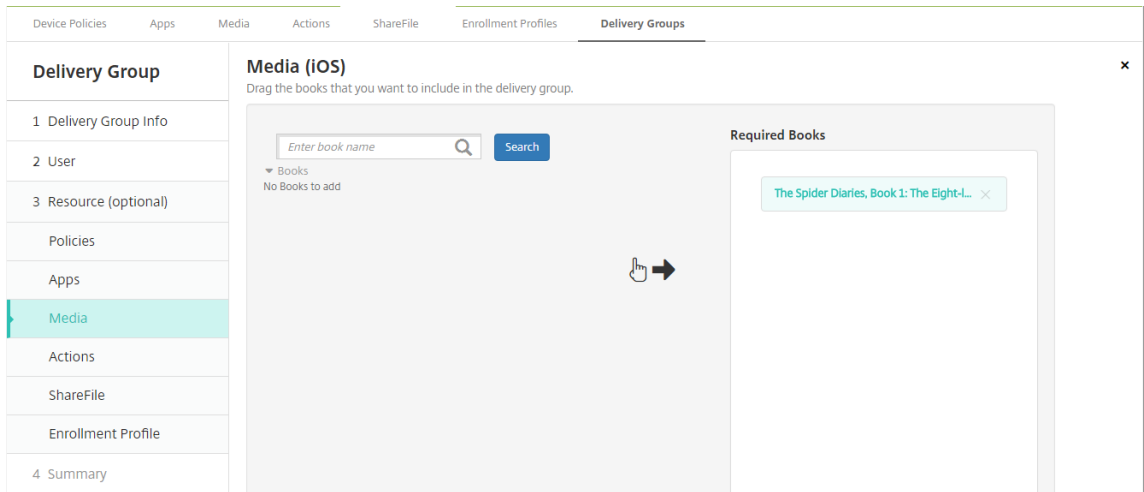
- 1 Limit by user property
- 2 ASM person title
- 3 is equal to
- 4 Student

The screenshot shows the 'User Assignments' configuration page in the XenMobile console. On the left, a navigation pane shows 'Delivery Group' with sub-items: '1 Delivery Group Info', '2 User' (selected), '3 Resource (optional)', 'Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profile', and '4 Summary'. The main area is titled 'User Assignments' and includes a 'Select domain' dropdown set to 'local'. Below it, the 'Include user groups' section shows a search box with 'sample' and a list of selected user groups: local\SAMPLE-CLASS-0001 - HS, local\SAMPLE-CLASS-1010 - HS, local\SAMPLE-CLASS-1011 - HS, local\SAMPLE-CLASS-1012 - HS, and local\SAMPLE-CLASS-1013 - HS. To the right, a 'Selected user groups' table lists: SAMPLE-CLASS-1013 - HS, SAMPLE-CLASS-1014 - HS, b8d22143-e8c8-4c30-92db-d0f497151137 - HS, SAMPLE-CLASS-1010 - HS, SAMPLE-CLASS-0001 - HS, SAMPLE-CLASS-1012 - HS, MSP, and SAMPLE-CLASS-1011 - HS. At the bottom, the 'Deployment Rules' section is expanded to 'Advanced' mode, showing a rule: 'Limit by user property' is 'ASM person title' 'is equal to' 'Student'. Buttons for 'AND', 'OR', 'NOT', 'EDIT', 'New Rule', and 'Delete' are visible.

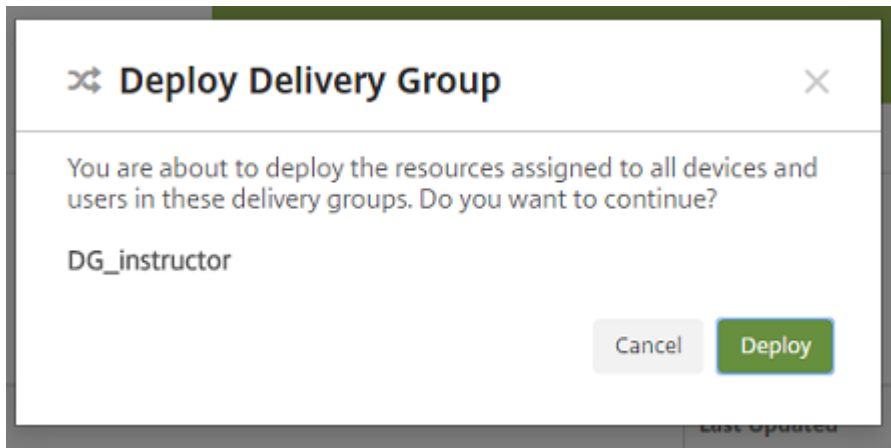
Apple School Manager DEP 계정이름에기반한배포규칙을사용하여배달그룹을필터링할수도있습니다.

The screenshot shows the 'Deployment Rules' configuration page in the XenMobile console. The left navigation pane is the same as in the previous screenshot. The main area shows the 'Deployment Rules' section expanded to 'Advanced' mode. It displays a rule configuration: 'Deploy when' is set to 'All' conditions are met. The rule itself is 'ASM DEP account name' is 'only' 'ASM'. There is a 'New Rule' button to the right.

5. 배달그룹에리소스를할당합니다. 다음예제는배달그룹에포함된 iBooks 를보여줍니다.



다음예제는배달그룹을선택하고 배포를클릭할때표시되는확인대화상자를보여줍니다.



자세한내용은 리소스배포의 “배달그룹을편집하려면” 과 “배달그룹을배포하려면” 을참조하십시오.

8 단계: 강사및학생장치등록테스트

다음방법중하나를사용하여장치를등록할수있습니다.

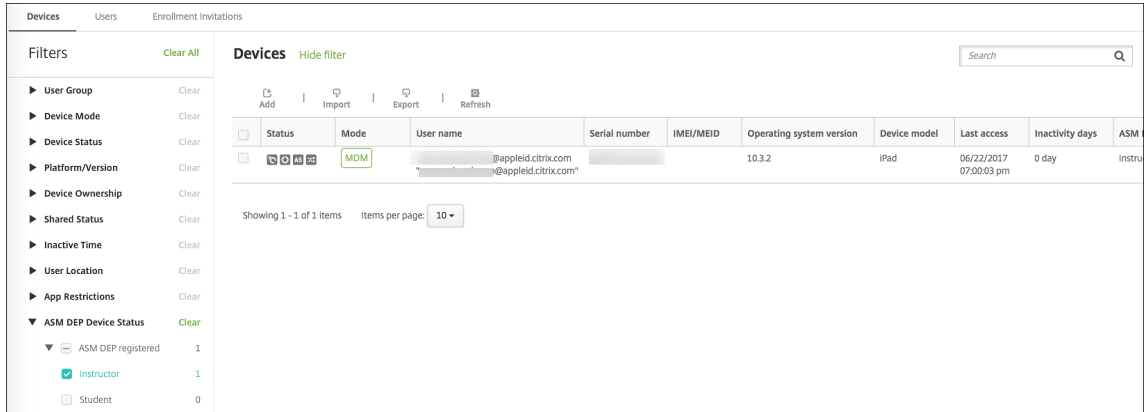
- 학교관리자는 XenMobile 콘솔에서설정할수있는사용자암호를사용하여강사및학생장치를등록할수있습니다. 따라서업과미디어가이미설정된장치를사용자에게제공할수있습니다.
- 사용자는장치를받은후관리자가제공한사용자암호를사용하여등록합니다. 등록이완료되면 XenMobile Server 가장치정책, 앱및미디어를장치에전송합니다.

등록을테스트하려면 Apple School Manager 에연결된 DEP 장치를사용합니다.

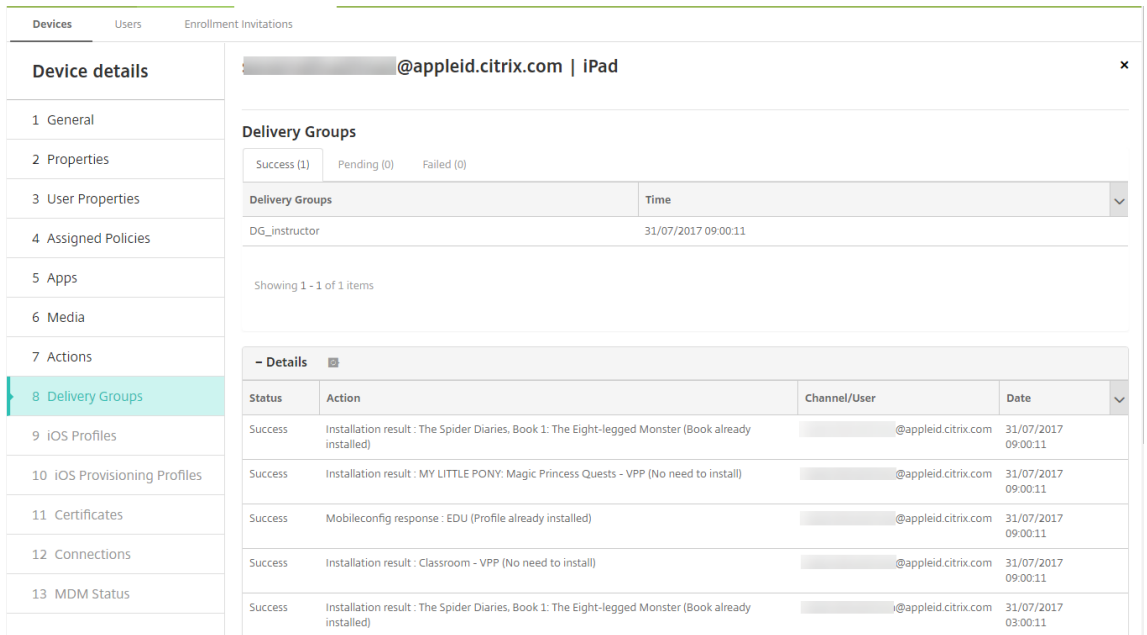
1. 장치가 Apple School Manager 에연결되지않은경우하드리셋을수행하여장치콘텐츠및설정을지웁니다.
2. 강사용 Apple School Manager DEP 장치를등록합니다. 그런다음학생용 Apple School Manager DEP 장치를등록합니다.

3. 관리 > 장치페이지에서두 Apple School Manager DEP 장치가 MDM 전용으로등록되었는지확인합니다.

장치페이지를 Apple School Manager DEP 장치상태인 **ASM DEP** 에등록됨, 강사및 학생으로필터링할수있습니다.



4. 각장치에대한 MDM 리소스가올바르게배포되었는지확인하려면: 장치를선택하고 편집을클릭한후여러페이지를확인합니다.



9 단계: 장치배포

강사와학생에게장치를배포할수있도록이벤트를호스트하는것이좋습니다.

사전등록된장치를배포하지않는경우에는사용자에게다음항목도제공하십시오.

- DEP 등록을위한 XenMobile Server 암호
- 관리되는 Apple ID 에대한 Apple School Manager 임시암호

첫번째사용자환경은다음과같습니다.

1. 하드리셋후사용자가처음으로장치를시작하면 XenMobile 이장치등록을위한 DEP 등록화면을표시합니다.
2. 사용자는관리되는 Apple ID 와인증에사용되는 XenMobile Server 암호를 XenMobile Server 에제공합니다.
3. Apple ID 설정단계에서관리되는 Apple ID 와 Apple School Manager 임시암호를제공하라는메시지가사용자에게 표시됩니다. 이러한항목은 Apple 서비스에대해사용자를인증하는데사용됩니다.
4. 관리되는 Apple ID 의암호 (iCloud 의데이터를보호하는데사용됨) 를생성하라는메시지가표시됩니다.
5. 설정도우미를마치면 XenMobile Server 가장치에정책, 앱및미디어를설치하기시작합니다. 사용자수준에서할당된앱 및 iBooks 의경우강사및학생에게 VPP 등록메시지가표시됩니다. 사용자가초대를수락하면다음배포 (6 시간이내) 시 VPP 앱과 iBooks 가전송됩니다.

공유 iPad 구성

한교실에있는여러학생이한명또는여러명의강사가가르치는다양한과목에서 iPad 를공유할수있습니다.

관리자또는강사는공유 iPad 를등록한다음장치정책, 앱및미디어를장치에배포합니다. 그런다음수강생은관리되는 Apple ID 자격증명을제공하여공유 iPad 에로그인합니다. 이전에교육구성정책을학생에게배포한경우학생은장치를공유할때 “기타사용자” 로로그인하지않습니다.

XenMobile Server 는공유 iPad 에대해두가지통신채널을사용합니다. 장치소유자 (강사) 에게는시스템채널을사용하고현재 상주사용자 (학생) 에게는사용자채널을사용합니다. XenMobile Server 는이러한채널을사용하여 Apple 이지원하는리소스에대해해당하는 MDM 명령을보냅니다.

시스템채널을통해배포되는리소스는다음과같습니다.

- 교육구성, 잠금화면메시지, 최대상주사용자수및암호잠금유예기간과같은장치정책
- 장치기반 VPP 앱

Apple 은공유 iPad 에서엔터프라이즈앱또는사용자기반 VPP 앱을지원하지않습니다. 공유 iPad 에설치된앱은사용자 별로적용되는것이아니라장치에글로벌로적용됩니다.

- 사용자기반 VPP iBooks

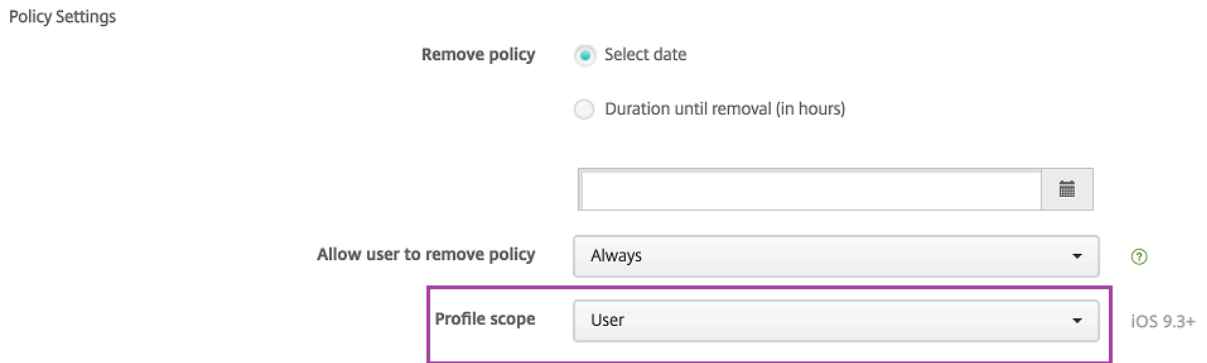
Apple 은공유 iPad 에서사용자기반 VPP iBooks 를할당하는것을지원합니다.

사용자채널을통해배포되는리소스는다음과같습니다.

- 장치정책: 앱알림, 홈화면레이아웃및제한사항

XenMobile Server 는사용자채널을통해이러한장치정책만지원합니다.

장치정책을구성할때정책설정 프로필범위에서배포채널을지정합니다.



사용자채널을통해배포한장치정책을제거하려면프로필제거정책에대해 배포범위를 사용자로선택해야합니다.

일반적인워크플로

일반적으로사전구성을마친감독되는공유 iPad 를강사에게제공합니다. 그런다음강사가학생에게장치를배포합니다. 강사에게사전등록된공유 iPad 를배포하지않는경우: 강사에게 XenMobile Server 서버암호를제공하여장치를등록할수있도록해야합니다.

공유 iPad 를구성과등록하는일반적인워크플로는다음과같습니다.

1. XenMobile Server 서버콘솔을사용하여 ASM DEP 계정을추가하고 (설정 > **Apple DEP(장치등록프로그램)**) 공유 모드를사용하도록설정합니다. 자세한내용은다음의 “공유 iPad 에대한 ASM DEP 계정관리” 를참조하십시오.
2. 이섹션에설명된대로 XenMobile Server 에필요한장치정책, 앱및미디어를추가합니다. 이러한리소스를배달그룹에할당합니다.
3. 강사로하여금공유 iPad 에대해하드리셋을수행하도록합니다. DEP 등록에대한원격관리화면이나타납니다.
4. 강사가공유 iPad 를등록합니다.
XenMobile Server 가등록된각공유 iPad 에구성된리소스를배포합니다. 자동으로다시시작된후강사는학생과장치를공유할수있습니다. iPad 에로그인페이지가나타납니다.
5. 학생이클래스를선택한다음관리되는 Apple ID 와임시 ASM(Apple School Manager) 암호를입력합니다.
공유 iPad 가 ASM 에인증하고학생에게 ASM 암호를생성하라는메시지를표시합니다. 학생은다음번에공유 iPad 에로그인할때새 ASM 암호를제공합니다.
6. iPad 를공유하는다른학생은이전단계를반복하여로그인할수있습니다.

공유 iPad 에대한 **ASM DEP** 계정관리

Apple Education 에서 XenMobile Server 를이미사용하는경우: 강사가사용하는장치와같이공유되지않는장치에대한 기존 ASM DEP 계정이 XenMobile Server 에구성되어있습니다. 공유장치와비공유장치모두에동일한 ASM 및동일한 XenMobile Server 서버를사용할수있습니다.

XenMobile 은다음과같은배포시나리오를지원합니다.

- 클래스별공유 iPad 그룹

이시나리오에서는공유 iPad 를클래스학생에게할당합니다. iPad 는교실에있습니다. 해당클래스다른과목을가르치는강사는동일한 iPad 세트를사용합니다.

- 강사별공유 iPad 그룹

이시나리오에서는공유 iPad 를강사에게할당합니다. 강사는강사가가르치는다양한클래스에서해당 iPad 를사용합니다.

공유 iPad 를장치그룹으로구성

ASM 을사용하면여러 MDM 서버를만들어장치를그룹으로구성할수있습니다. MDM 서버에공유 iPad 를할당할때공유 iPad 의 각그룹에대한장치그룹을클래스별또는강사별로만듭니다.

- 공유 iPad 의그룹 1 > 장치그룹 1 MDM 서버
- 공유 iPad 의그룹 2 > 장치그룹 2 MDM 서버
- 공유 iPad 의그룹 N > 장치그룹 N MDM 서버

각장치그룹에대한 **ASM DEP** 계정추가

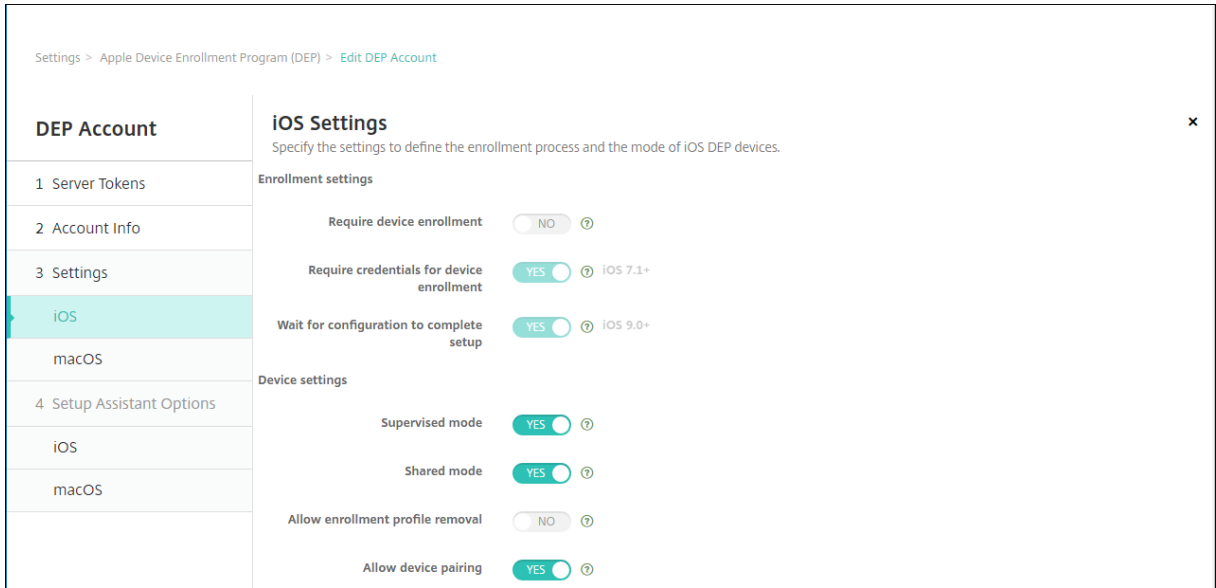
XenMobile Server 서버콘솔에서여러 ASM DEP 계정을생성하는경우공유 iPad 그룹을자동으로가져옵니다 (각클래스또는 강사당 1 대).

- 장치그룹 1 MDM 서버 > 장치그룹 1 DEP 계정
- 장치그룹 2 MDM 서버 > 장치그룹 2 DEP 계정
- 장치그룹 N MDM 서버 > 장치그룹 N DEP 계정

공유 iPad 와관련된요구사항은다음과같습니다.

- 다음설정이사용되는각장치그룹에대해 ASM DEP 계정 1 개:
 - 장치등록필요
 - 감독모드
 - 공유모드
- 지정된교육조직의경우모든 ASM DEP 계정에동일한 교육접미사를사용해야합니다.

DEP 계정을추가하려면 설정 > **Apple DEP**(장치등록프로그램) 로이동합니다.

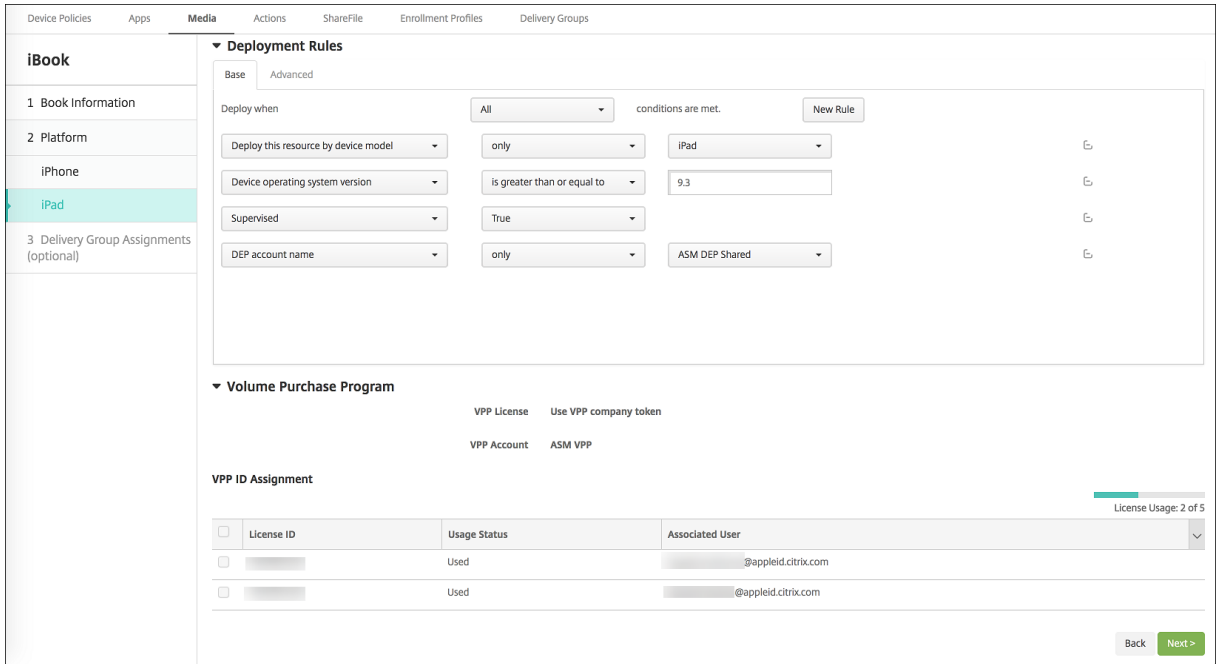


공유 iPad 의앱

공유 iPad 는장치기반 VPP 앱할당을지원합니다. 공유 iPad 에앱을배포하기전에 XenMobile Server 는장치에 VPP 라이선스를할당하라는요청을 Apple VPP 서버에보냅니다. VPP 할당을확인하려면 구성 > 앱 > iPad 로이동하고 **Volume Purchase Program** 을확장합니다.

공유 iPad 의미디어

공유 iPad 는사용자기반 VPP iBooks 할당을지원합니다. 공유 iPad 에 iBooks 를배포하기전에 XenMobile Server 는학생에게 VPP 라이선스를할당하라는요청을 Apple VPP 서버에보냅니다. VPP 할당을확인하려면 구성 > 미디어 > iPad 로이동하고 **Volume Purchase Program** 을확장합니다.



공유 iPad 에대한배포규칙

공유 iPad 배포의 경우 배달 그룹 수준의 규칙은 사용자 속성과 관련이 있으므로 적용되지 않습니다. 각 장치 그룹에 대한 정책, 앱 및 미디어를 필터링하려면 DEP 계정 이름을 기준으로 리소스에 대한 배포 규칙을 추가합니다. 예를 들면 다음과 같습니다.

- 장치 그룹 1 DEP 계정의 경우 다음 배포 규칙을 설정합니다.

1	DEP account name
2	Only
3	Device Group 1 DEP account

- 장치 그룹 2 DEP 계정의 경우 다음 배포 규칙을 설정합니다.

1	DEP account name
2	Only
3	Device Group 2 DEP account

- 장치 그룹 N DEP 계정의 경우 다음 배포 규칙을 설정합니다.

1	DEP account name
2	Only
3	Device Group N DEP account

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups			
Calendar	True	True	True	True	True	True	None		
Mail	True	True	True	True	True	True	None		
Maps	True	True	True	True	True	True	None		
Wallet	True	True	True	True	True	True	None		

Policy Settings

Remove policy Select date
 Duration until removal (in hours)

Allow user to remove policy

Profile scope iOS 9.3+

▼ Deployment Rules

Base Advanced

Deploy when conditions are met.

Deploy this resource by device model

Device operating system version

Supervised

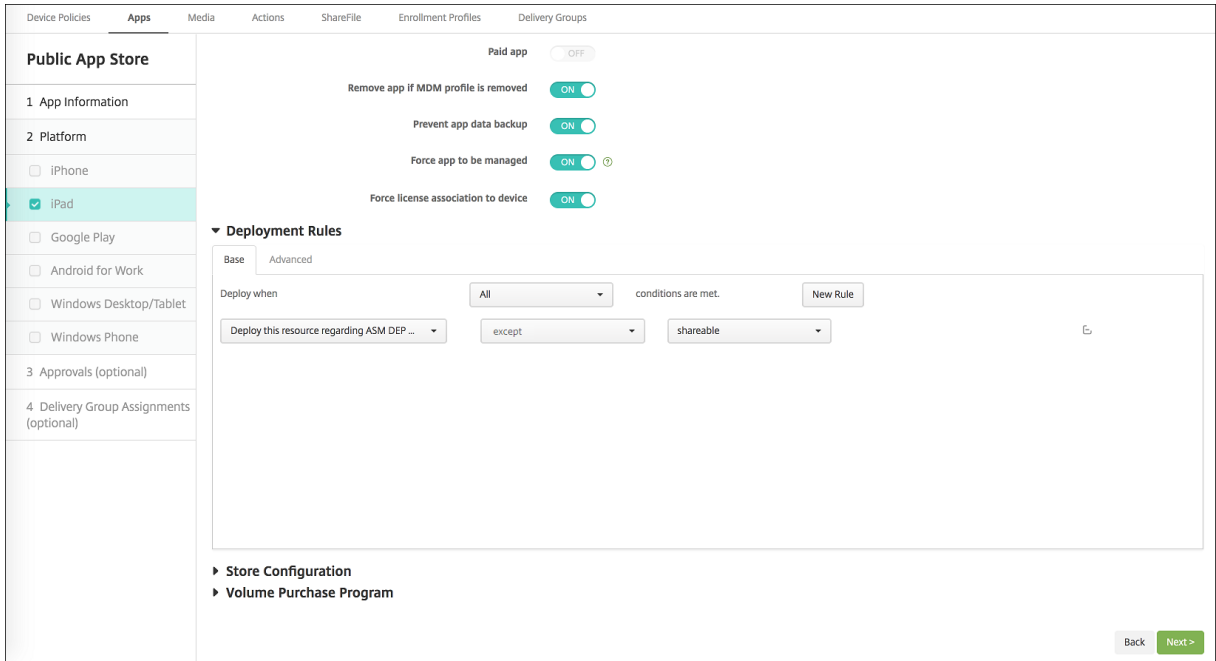
DEP account name

Apple 교실애플을강사에게만배포하려면 (공유되지않는 iPad 사용) 다음배포규칙을사용하여 ‘ASM DEP 에공유됨’ 상태로리소스를필터링합니다.

- 1 Deploy **this** resource regarding ASM DEP shared mode
- 2 only
- 3 unshared

또는:

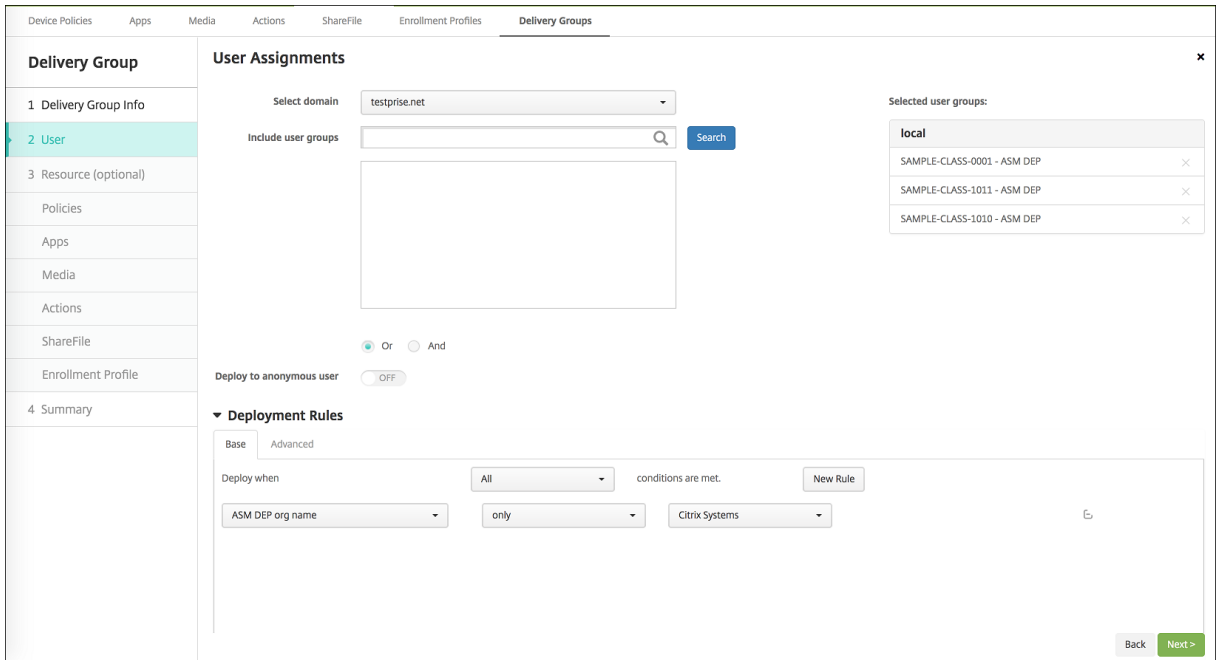
- 1 Deploy **this** resource regarding ASM DEP shared mode
- 2 except
- 3 shareable



공유 iPad 의배달그룹

각강사의장치그룹에대해

- 하나의배달그룹을구성합니다. 강사의경우교육구성정책에서정의하는모든클래스를할당합니다.



- 해당배달그룹에는다음과같은 MDM 리소스가포함되어야합니다.
 - 장치정책:

- * 교육구성
 - * 잠금화면메시지
 - * 앱알림
 - * 홈화면레이아웃
 - * 제한사항
 - * 최대상주사용자수
 - * 암호잠금유예기간
- 필수 VPP 앱
 - 필수 VPP iBooks

The screenshot displays the 'Delivery Groups' configuration interface. On the left is a sidebar with a 'Delivery Group' section containing a list of items: 1 Delivery Group Info, 2 User, 3 Resource (optional), Policies, Apps, Media, Actions, ShareFile, Enrollment Profile, and 4 Summary (highlighted). The main area shows the 'Summary' page for a delivery group, including a 'General' section with fields for Name and Description, and a 'Resource' section with a 'Deployment Order' table. The table lists various resources: Policies (2) with 'DEP Software Inventory' and 'EDU'; Apps (4) with 'Classroom - VPP', 'Citrix Secure Hub - VPP', 'Citrix Secure Web - VPP', and 'AV Player Demo'; Media (0); Actions (1) with 'Wipe device'; ShareFile (Disabled); and Enrollment Profile (Global).

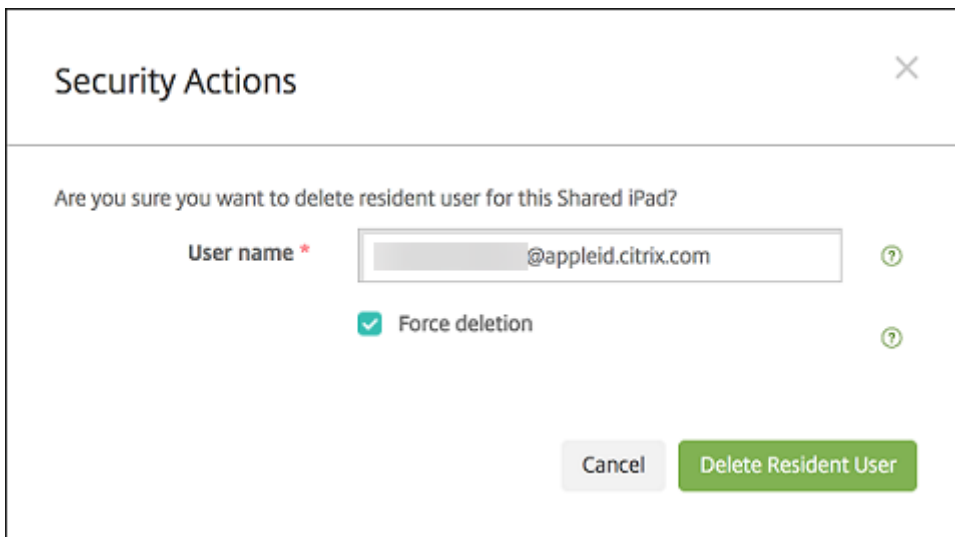
공유 iPad 의보안동작

기존보안동작외에공유 iPad 에대해다음보안동작을사용할수있습니다.

- 상주사용자가져오기: 현재장치에활성계정이있는사용자를나열합니다. 이동작은장치와 XenMobile Server 콘솔간에 강제로동기화됩니다.
- 상주사용자로그아웃: 현재사용자의로그아웃을강제수행합니다.
- 상주사용자삭제: 특정사용자에대한현재세션을삭제합니다. 사용자는다시로그인할수있습니다.



상주사용자삭제를클릭한후사용자이름을지정할수있습니다.



보안동작결과는 관리 > 장치 > 일반및 관리 > 장치 > 배달그룹페이지에나타납니다.

공유 iPad 에대한정보얻기

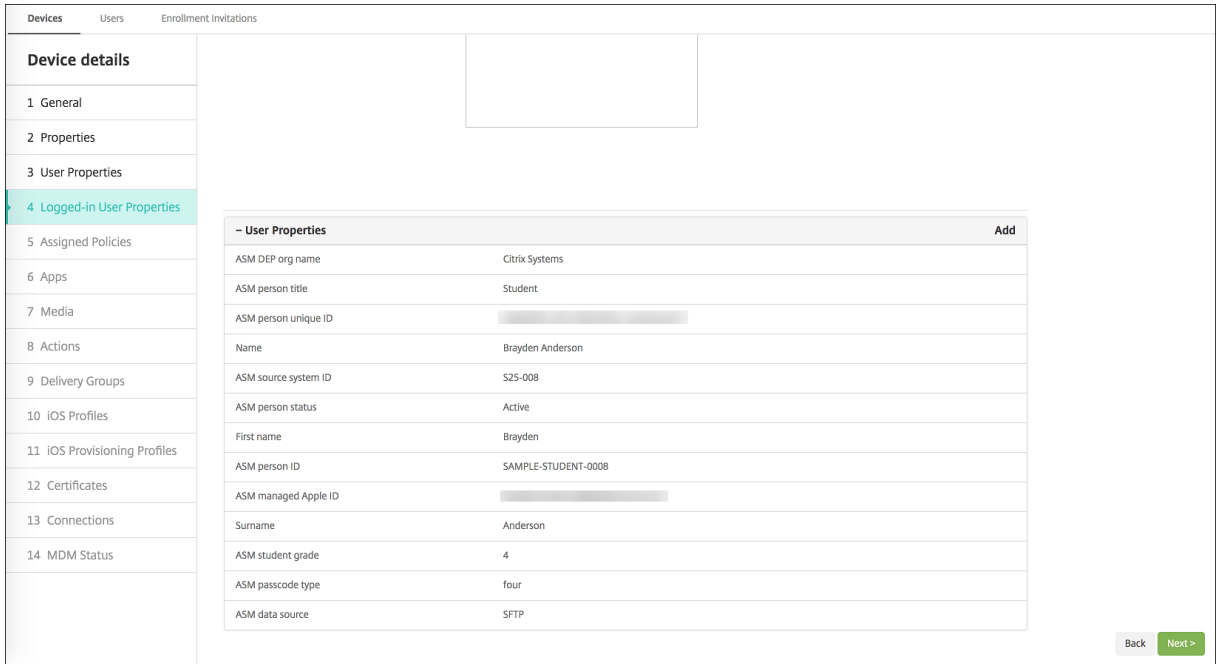
관리 > 장치페이지에서공유 iPad 와관련된정보를찾습니다.

- 다음을조회할수있습니다.
 - 장치의공유여부 (**ASM DEP** 에공유됨)
 - 공유장치에로그인한사용자 (**ASM** 에로그인한사용자)
 - 공유장치에할당된모든사용자 (**ASM** 상주사용자)

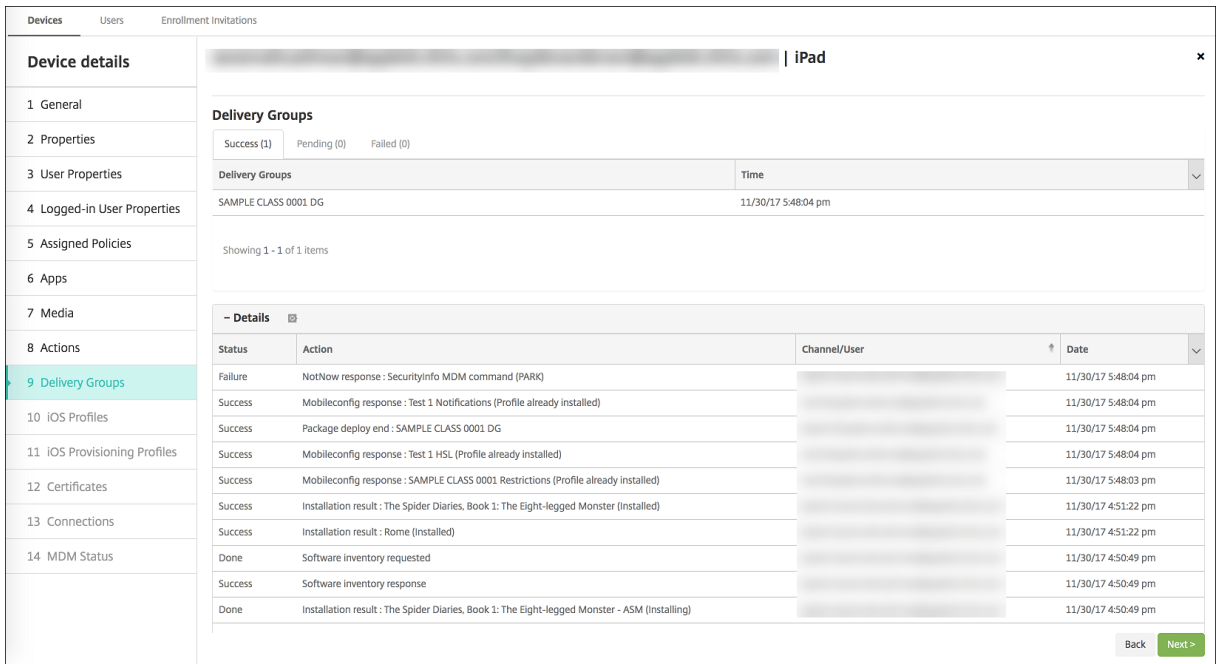
Serial number	Device platform	Operating system version	Device model	ASM DEP device type	ASM DEP shared	ASM logged-in user	ASM resident users
id.citrix.com	iOS	11.2.2	iPad	Instructor	Yes		

- **ASM DEP** 장치상태로장치목록을필터링합니다.

- 관리 > 장치 > 로그인한사용자속성페이지에서공유 iPad 에로그인한사용자에대한세부정보를봅니다.



- 관리 > 장치 > 배달그룹페이지에서배달그룹의강사및사용자에게리소스를배포할때사용되는채널을확인합니다. 채널/사용자열에는유형 (시스템또는 사용자) 과받는사람 (강사또는학생) 이표시됩니다.



- 상주사용자에대한정보를확인합니다.
 - 동기화할데이터있음: 사용자에게클라우드에동기화할데이터가있는지여부를나타냅니다.
 - 데이터할당량: 사용자에게설정된데이터할당량 (바이트) 입니다. 사용자할당량이일시적으로꺼져있거나사용자에게적용되지않는경우할당량이표시되지않을수있습니다.
 - 사용한데이터: 사용자가사용한데이터의양 (바이트) 입니다. 시스템에서정보를수집할때오류가발생하면값이나타나지않을수있습니다.

- 로그인되어있음: 사용자가장치에로그온했는지여부를나타냅니다.

Device details | iPad

Connections

First connection: 8/30/17 12:42:38 pm
 Status: Active
 Last connection: 11/30/17 5:48:04 pm

User name	Penultimate authentication	Last authentication	Has data to sync	Data quota	Data used	Is logged-in
ios	10/12/17 10:15:34 am	10/12/17 10:19:00 am				
	11/23/17 3:45:28 pm	11/23/17 3:45:29 pm				
	11/23/17 5:48:03 pm	11/23/17 5:48:03 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm	Yes			Yes
	11/29/17 7:02:32 pm	11/29/17 7:02:32 pm	No		120.82 MB	No

Showing 1 - 6 of 6 items

Back Next >

• 두채널의푸시상태를확인합니다.

Device details | iPad

System channel

Push status: Active
 Last push initiation: 1/24/18 1:00:03 pm
 Last notification completion: 1/24/18 1:00:03 pm
 Last reply time: 1/24/18 1:00:03 pm

User channel

Push status: Active
 Last push initiation: 1/24/18 1:00:03 pm
 Last notification completion: 1/24/18 1:00:03 pm
 Last reply time: 1/24/18 1:00:03 pm

Refresh

Back Save

강사, 학생및클래스데이터관리

강사, 학생및클래스데이터를관리하는경우다음참고하십시오.

- Apple School Manager 정보를 XenMobile Server 로가져온후에는관리되는 Apple ID 를변경하지마십시오. XenMobile 은 Apple School Manager 사용자식별자를사용하여사용자를식별합니다.

- 하나이상의교육구성장치정책을생성한후 Apple School Manager 의클래스데이터를추가하거나변경하는경우: 정책을편집하고다시배포합니다.
- 교육구성장치정책을배포한후클래스의강사가변경되는경우: 정책을검토하여 XenMobile 콘솔에서업데이트되는지확인한후정책을다시배포합니다.
- Apple School Manager 포털에서사용자속성을업데이트하면 XenMobile 이이러한속성을콘솔에도업데이트합니다. 그러나 ASM 사용자직위속성 (강사, 학생또는기타) 은다른속성과같은방법으로 XenMobile 에전송되지않습니다. 그러므로 Apple School Manager 에서 ASM 사용자직위를변경하는경우다음단계를수행하여 XenMobile 에변경내용이반영될수있도록하십시오.

데이터를관리하려면:

1. Apple School Manager 포털에서학생학년을업데이트하고강사학년을지웁니다.
2. 학생계정을강사계정으로변경한경우클래스의학생목록에서해당사용자를제거합니다. 그런다음동일한클래스또는다른클래스의강사목록에서사용자를추가합니다.

강사계정을학생계정으로변경한경우클래스에서해당사용자를제거합니다. 그런다음동일한클래스또는다른클래스의학생목록에서사용자를추가합니다. 다음동기화 (기본적으로 5 분마다) 또는가져오기 (기본적으로 24 시간마다) 중에업데이트내용이 XenMobile 콘솔에표시됩니다.

3. 변경내용을적용하도록교육구성장치정책을편집하고다시배포합니다.
 - Apple School Manager 포털에서사용자를삭제하면 XenMobile Server 가가져오기후 XenMobile 콘솔에서도해당사용자를삭제합니다.

다음서버속성값을변경하여두기준사이의간격을줄일수있습니다. **bulk.enrollment.fetchRosterInfoDelay**(기본값은 **1440** 분)
 - 리소스배포후: 학생이클래스에참여하면해당학생만포함된배달그룹을생성하고리소스를학생에게배포합니다.
 - 학생또는강사가임시암호를잊은경우 Apple School Manager 관리자에게문의하도록하십시오. 관리자는임시암호를제공하거나새암호를생성할수있습니다.

Apple School Manager DEP 에등록된분실또는도난장치관리

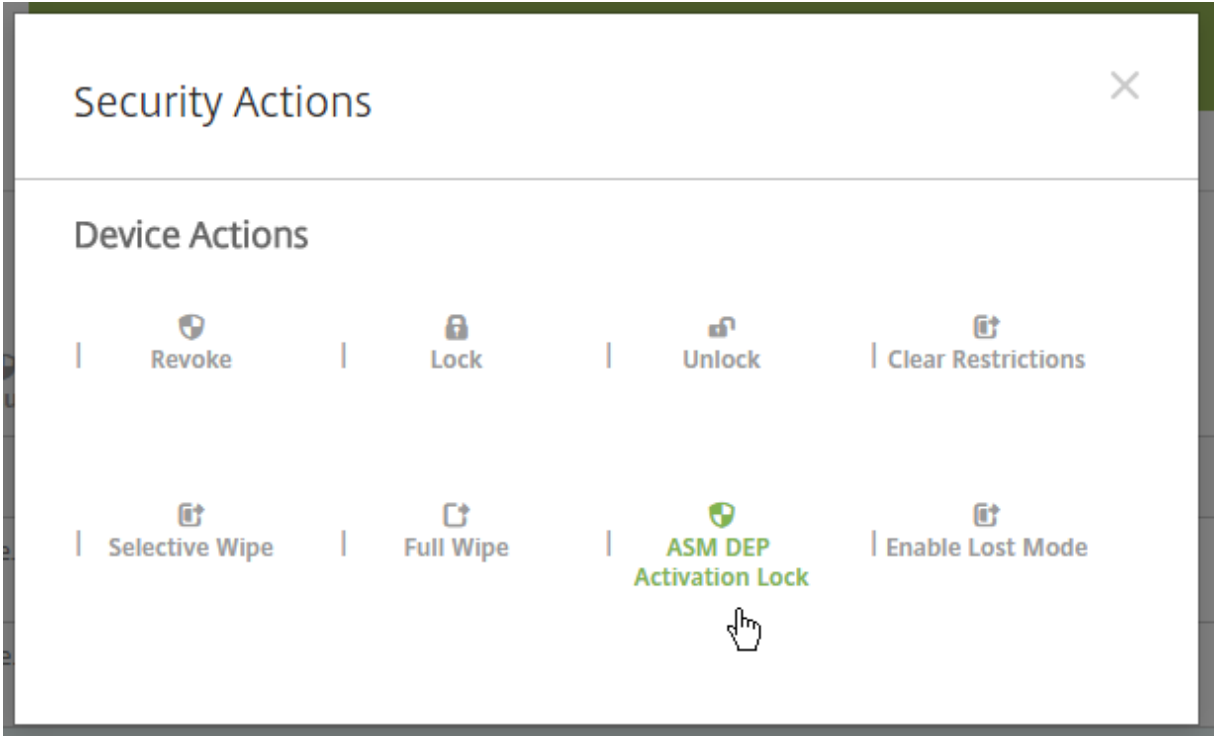
Apple 의내 iPhone/iPad 찾기서비스에는활성화잠금기능이포함되어있습니다. 활성화잠금기능은권한이없는사용자가 DEP 에등록된분실또는도난장치를사용하거나재판매할수없도록합니다.

XenMobile 에포함된 **ASM DEP** 활성화잠금보안동작을사용하면 Apple School Manager DEP 등록장치에잠금코드를전송할수있습니다.

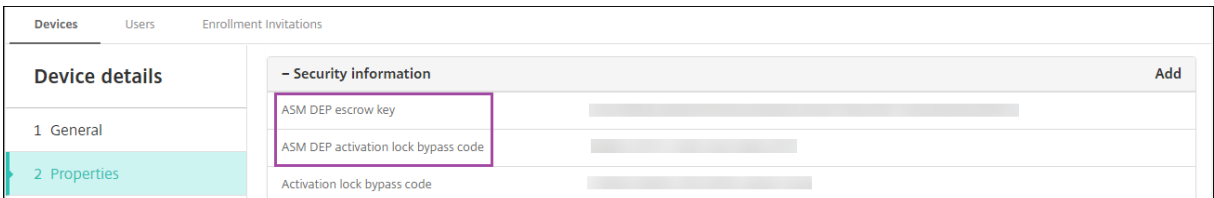
ASM DEP 활성화잠금보안동작을사용하면사용자가내 iPhone/iPad 찾기서비스를사용하지않고 XenMobile 을통해장치를 찾을수있습니다. Apple School Manager 장치가하드리셋되거나전체초기화된경우사용자는관리되는 Apple ID 와암호를제공하여장치잠금을해제할수있습니다.

콘솔에서잠금을해제하려면 활성화잠금바이패스보안동작을클릭합니다. 활성화잠금바이패스에대한자세한내용은보안동작문서에서 [iOS 활성화잠금바이패스](#)를참조하십시오. 또한로그인을비워두고 **ASM DEP** 활성화잠금바이패스코드를암호로입력할수도있습니다. 이정보는 장치세부정보의 속성탭에나와있습니다.

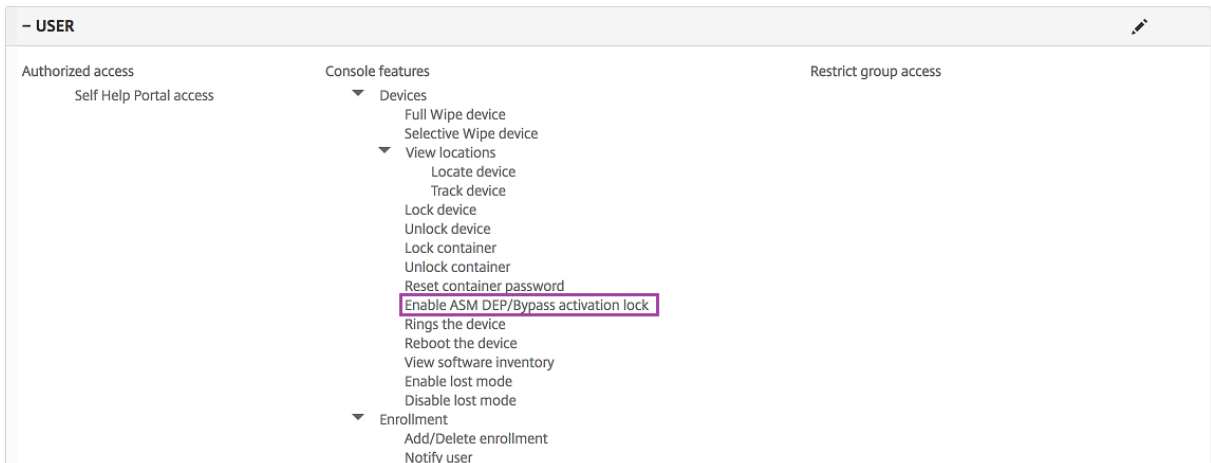
활성화잠금을설정하려면 관리 > 장치에서장치를선택하고 보안을클릭한후 **ASM DEP** 활성화잠금을클릭합니다.



ASM DEP 에스크로키와 **ASM DEP** 활성화잠금바이패스코드속성은 장치세부정보에표시됩니다.



ASM DEP 활성화잠금에대한 RBAC 권한은 장치 >**ASM DEP** 사용/활성화잠금바이패스입니다.



네트워크액세스제어

January 6, 2020

Cisco ISE 와같은 NAC(네트워크액세스제어) 장비가 XenMobile 네트워크에 설정되어있는 경우 규칙 또는 속성에 따라 장치를 NAC 준수 또는 비준수로 설정하는 필터를 사용할 수 있습니다. XenMobile 의 관리되는 장치가 지정된 기준을 충족하지 않고 그 결과 비준수로 표시되는 경우 NAC 장비가 네트워크에서 해당 장치를 차단합니다. iOS 장치의 경우 VPN 정책을 배포하고 NAC 필터를 사용하여 설정하여 규정을 준수하지 않는 앱이 설치된 장치의 VPN 연결을 차단할 수 있습니다. 자세한 내용은 아래에서 “iOS NAC 구성” 섹션을 참조하십시오.

XenMobile 콘솔에서 장치를 비준수로 설정할 때 사용할 하나 이상의 기준을 목록에서 선택합니다.

XenMobile 은 다음과 같은 NAC 준수 필터를 지원합니다.

익명 장치: 장치가 익명 모드인지 확인합니다. 이 확인은 장치가 다시 연결할 때 XenMobile 이 사용자를 다시 인증할 수 없는 경우 사용할 수 있습니다.

Samsung KNOX 증명 실패: 장치가 Samsung KNOX 증명 서버의 쿼리에 실패했는지 확인합니다.

금지된 앱: 장치에 앱 액세스 정책에 정의된 금지된 앱이 있는지 확인합니다. 앱 액세스 정책에 대한 자세한 내용은 [앱 액세스 장치 정책](#)을 참조하십시오.

비활성 장치: Server Properties(서버 속성) 의 Device Inactivity Days Threshold(장치 비활성 일 수 임계값) 설정에 정의된 대로 장치가 비활성 상태인지 확인합니다. 자세한 내용은 [서버 속성](#)에서 참조하십시오.

누락된 필수 앱: 앱 액세스 정책에 정의된 대로, 장치에 필수 앱이 누락되었는지 확인합니다.

비추천 앱: 앱 액세스 정책에 정의된 대로, 장치에 비추천 앱이 있는지 확인합니다.

규정을 준수하지 않는 암호: 사용자 암호가 규정을 준수하는지 확인합니다. iOS 및 Android 장치에서 XenMobile 은 현재 장치에 있는 암호가 장치로 보낸 암호 정책을 준수하는지 여부를 확인할 수 있습니다. 예를 들어 iOS 에서는 XenMobile 이 암호 정책을 장치에 보내는 경우 60 분 내에 암호를 설정해야 합니다. 사용자가 암호를 설정하기 전에 암호가 규정을 준수하지 않을 수 있습니다.

규정위반장치: 규정위반장치 속성에 따라 장치가 규정을 위반하는지 여부를 확인합니다. 이 속성은 일반적으로 자동화 동작 또는 XenMobile API 를 활용하는 타사 애플리케이션에 의해 변경됩니다.

해지된 상태: 장치 인증서가 해지되었는지 여부를 확인합니다. 해지된 장치는 다시 권한이 부여될 때까지 다시 등록할 수 없습니다.

루팅된 Android 및 탈옥 iOS 장치: Android 또는 iOS 장치가 탈옥되어 있는지 확인합니다.

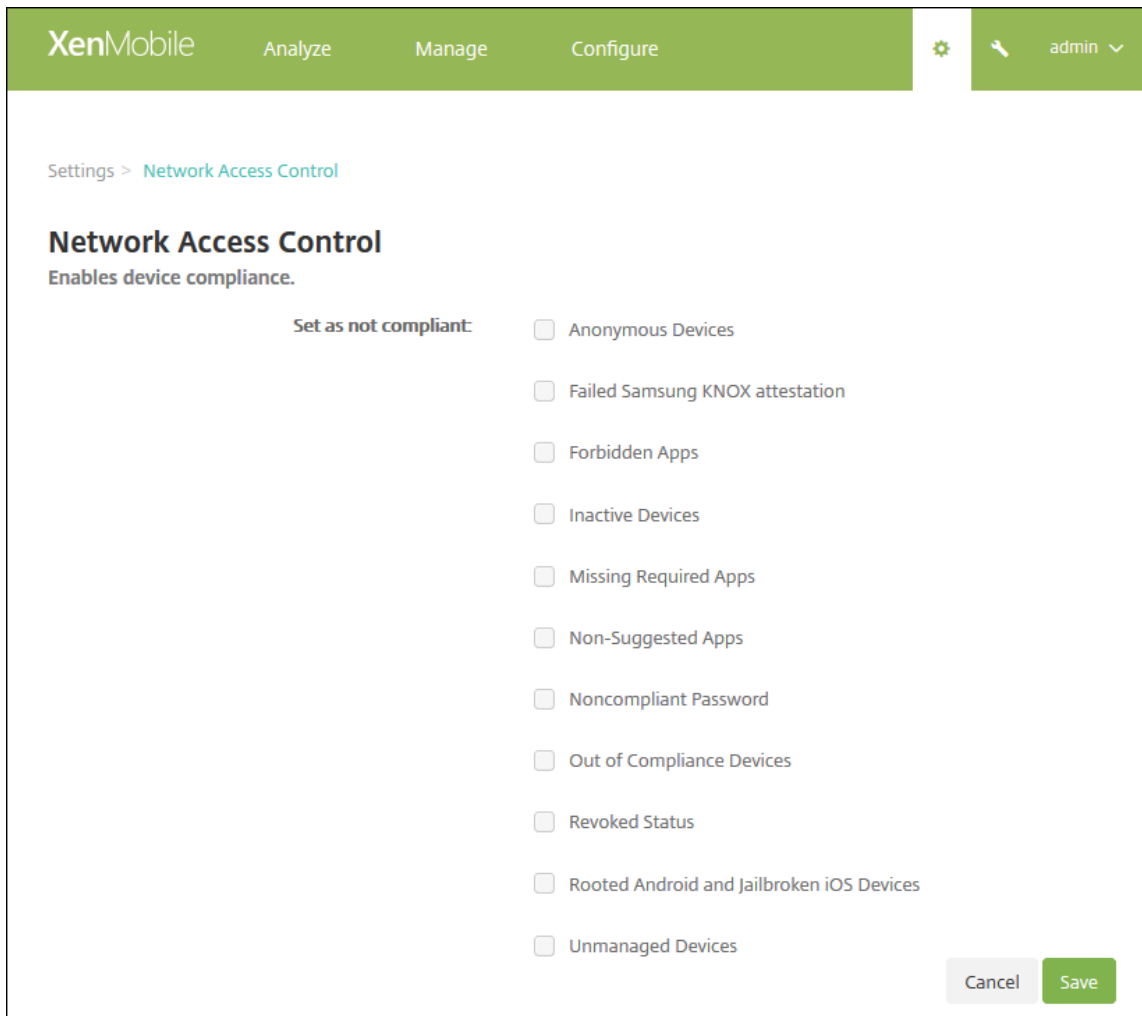
관리되지 않는 장치: 장치가 여전히 XenMobile 제어 하에 관리되는 상태에 있는지 확인합니다. 예를 들어 MAM 모드에서 실행 중인 장치나 등록되지 않은 장치는 관리되지 않습니다.

참고:

목시적 준수/비준수 필터는 XenMobile 로 관리되는 장치에만 기본값을 설정합니다. 예를 들어 블랙리스트 앱이 설치되거나 등록되지 않은 장치는 비준수로 표시되고 NAC 장비에 의해 네트워크에서 차단됩니다.

네트워크 액세스 제어 구성

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 서버에서 네트워크 액세스 제어를 클릭합니다. 네트워크 액세스 제어 페이지가 나타납니다.



3. 사용하려는 규정비준수상태로설정필터에대한확인란을선택합니다.
4. 저장을클릭합니다.

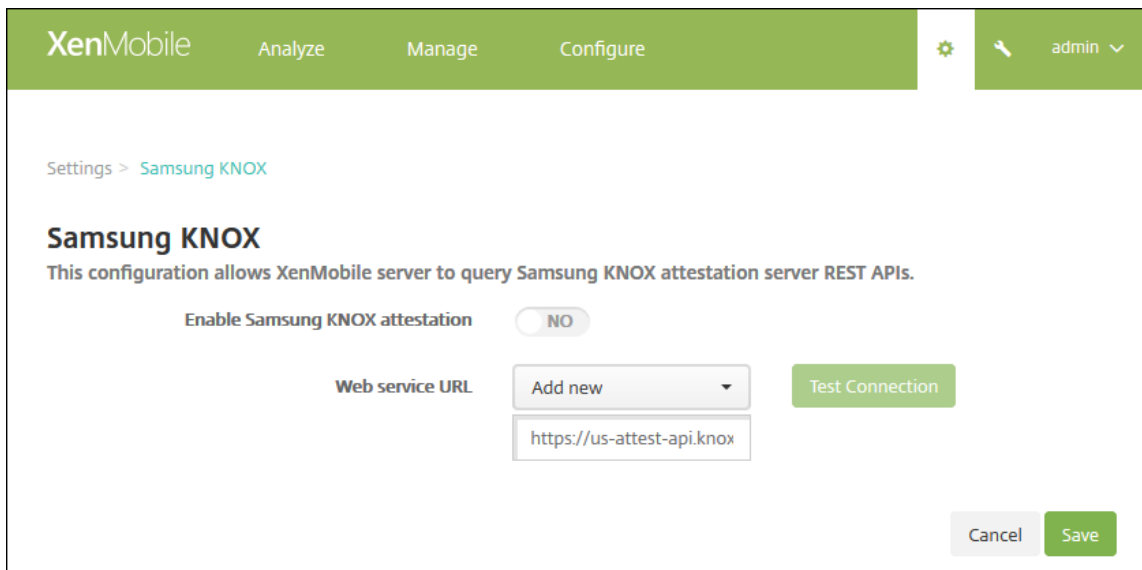
Samsung KNOX

January 6, 2020

XenMobile 에서 Samsung KNOX 증명서버 REST API 를쿼리하도록구성할수있습니다.

Samsung KNOX 는하드웨어보안기능을활용하여운영체제및응용프로그램에대한여러수준의보호를제공합니다. 이중한수준의 보안기능이증명을통해플랫폼에서제공됩니다. 증명서버는모바일장치핵심시스템소프트웨어 (예: 부팅로더및커널) 에대한확인을 수행합니다. 확인은신뢰할수있는부팅시수집된데이터를기반으로런타임에이루어집니다.

1. XenMobile 웹콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 플랫폼아래에서 **Samsung KNOX** 를클릭합니다. **Samsung KNOX** 페이지가나타납니다.



3. **Samsung KNOX** 증명사용에서 Samsung KNOX 증명을사용할지여부를선택합니다. 기본값은 아니요입니다.
4. **Samsung KNOX** 증명사용을 예로설정하는경우 웹서비스 **URL** 옵션이사용됩니다. 그런다음목록에서다음중하나를 수행합니다.
 - 적절한증명서버를클릭합니다.
 - 새로추가를클릭하고웹서비스 URL 을입력합니다.
5. 연결테스트를클릭하여연결을확인합니다. 성공또는실패메시지가나타납니다.
6. 저장을클릭합니다.

참고:

Samsung KNOX Mobile Enrollment 를 사용하여 여러 Samsung KNOX 장치를 각 장치에 대한 수동 구성 없이 XenMobile 또는 원하는 모바일 장치 관리자에 등록할 수 있습니다. 자세한 내용은 [Samsung KNOX 대량등록](#)에서 참조하십시오.

보안동작

January 6, 2020

관리 > 장치 페이지에서 장치 및 앱 보안 동작을 수행합니다. 장치 동작에는 해지, 잠금, 잠금 해제 및 초기화가 포함됩니다. 앱 보안 동작에는 앱 잠금 및 앱 초기화가 포함됩니다.

- **활성화 잠금 바이패스:** 장치 활성화 전에 감독되는 iOS 장치에서 활성화 잠금을 제거합니다. 이 명령은 개인 Apple ID 또는 암호가 없어도 사용할 수 있습니다.
- **앱 잠금:** 장치의 모든 앱에 대한 액세스를 거부합니다. Android에서는 앱이 잠기면 사용자가 XenMobile 에 로그인할 수 없습니다. iOS에서는 사용자가 로그인할 수는 있지만 앱에 액세스할 수 없습니다.
- **앱 초기화:** Android에서 앱 초기화는 XenMobile에서 사용자 계정을 삭제합니다. iOS에서는 Secure Hub에서 사용자 계정을 삭제합니다.
- **ASM DEP 활성화 잠금:** Apple School Manager DEP에 등록된 iOS 장치에 대한 활성화 잠금 바이패스 코드를 생성합니다.
- **제한 사항 지우기:** 감독되는 iOS 장치에서 이 명령을 사용하면 사용자가 구성한 제한 암호 및 제한 설정을 XenMobile Server 가지울 수 있습니다.
- **분실 모드 활성화/비활성화:** 감독되는 iOS 장치를 분실 모드로 전환하고 장치에 표시할 메시지, 전화번호 및 각주를 보냅니다. 이 명령을 두 번째로 보내면 장치가 분실 모드에서 해제됩니다.
- **추적 활성화:** Android 또는 iOS 장치에서 이 명령을 사용하면 XenMobile에서 특정 장치의 위치를 정의된 빈도로 폴링할 수 있습니다. 지도에서 장치의 좌표 및 위치를 보려면 관리 > 장치로 이동하고 장치를 선택한 다음 편집을 클릭합니다. 장치 정보는 일반 탭의 보안 아래에 있습니다.
- **전체 초기화:** 모든 메모리 카드를 포함하여 장치에서 모든 데이터와 앱을 즉시 지웁니다.
 - Android 장치의 경우 이 요청에 메모리 카드를 초기화하는 옵션도 포함될 수 있습니다.
 - iOS 및 macOS 장치의 경우 장치가 잠겨 있더라도 초기화가 수행됩니다. iOS 11 장치 (최소 버전)의 경우: 전체 초기화를 확인할 때 장치의 셀룰러 데이터 요금제가 보존되도록 선택할 수 있습니다.
 - Windows Phone 장치의 경우 전체 초기화는 앱, 전자 메일, 연락처 및 미디어와 같은 개인 콘텐츠를 포함하여 모든 XenMobile 정보와 모든 사용자 데이터를 제거합니다.
 - Windows Mobile 6 이하를 실행하는 Windows 모바일 장치의 경우: 초기화 후 장치를 제조업체에 반환하여 원래 운영 체제, 소프트웨어 또는 둘 다를 다시 로드해야 할 수 있습니다.

- 메모리카드콘텐츠가삭제되기전에장치사용자가장치전원을끄면사용자의장치데이터액세스가가능할수있습니다.
- 요청이장치로전송되기전까지는초기화요청을취소할수있습니다.
- **위치:** 관리 > 장치페이지의 장치세부정보 > 일반에서장치를찾고지도를포함한장치위치를보고할수있습니다. Android Enterprise 장치의경우 **위치장치정책**에서장치에대한위치모드를 높은정확도또는 배터리절약으로설정하지않으면이요청이실패합니다. iOS 장치의경우이명령은장치가 MDM 분실모드에있는경우에만성공합니다. 찾기는 추적활성화의지속적인추적과달리한번만수행되는작업입니다. Secure Hub 는실행중일때주기적으로위치를보고합니다.
- **잠금:** 장치를원격으로잠급니다. 이기능은장치가분실된경우그리고도난당했는지여부가불확실한경우에유용합니다. 그러면 XenMobile 이 PIN 코드를생성하여장치에이코드를설정합니다. 장치에액세스하려면사용자는 PIN 코드를입력해야합니다. 잠금을제거하려면 XenMobile 콘솔에서 잠금취소를사용합니다.
- **Lock and Reset Password(잠금및암호재설정):** 원격으로장치를잠그고암호를재설정합니다.
 - Android 8.0 이전버전의 Android 버전을실행하는작업프로필모드에서 Android Enterprise 에등록된장치의경우지원되지않습니다.
 - Android 8.0 이상을실행하는작업프로필모드에서 Android Enterprise 에등록된장치에서:
 - * 전송된암호로작업프로필이잠깁니다. 장치는잠기지않습니다.
 - * 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않고작업프로필에암호가미설정되지않은경우장치가잠깁니다.
 - * 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않지만작업프로필에암호가미설정되어있는경우에는작업프로필이잠기지만장치는잠기지않습니다.
- **Notify (Ring)(알림 (벨울림)):** Android 장치에서사운드를울립니다.
- **다시부팅:** Windows 10 장치를다시시작합니다. Windows 태블릿및 PC 의경우 “System will reboot soon(시스템이곧다시부팅됩니다.)” 라는메시지가표시되고 5 분안에다시부팅됩니다. Windows Phone 의경우경고메시지가표시되지않으며몇분후에다시부팅됩니다.
- **AirPlay** 미러링요청/중지: 감독되는 iOS 장치에서 AirPlay 미러링을시작및중지합니다.
- **다시시작/종료:** 감독되는 iOS 장치를즉시다시시작하거나종료합니다.
- **해지:** 장치가 XenMobile Server 에연결할수없도록합니다.
- **Revoke/Authorize(해지/권한부여)(iOS, macOS):** 선택적초기화와동일한동작을수행합니다. 해지후에는장치에권한을다시부여하여다시등록할수있습니다.
- **벨울림:** 장치가분실모드에있는경우감독되는 iOS 장치의벨의사운드가재생됩니다. 사운드는장치를분실모드에서제거하거나사용자가사운드를비활성화할때까지재생됩니다.
- **선택적초기화:** 장치에서모든회사데이터및앱을지우고개인데이터및앱은그대로유지합니다. 선택적초기화후에는사용자가장치를다시등록할수있습니다.
 - Android 장치의선택적초기화가수행되어도 Device Manager 및회사네트워크에서장치가분리되지않습니다. 장치가 Device Manager 에액세스하는것을방지하려면장치인증서도해지해야합니다.
 - Samsung KNOX API 를사용하도록설정된경우장치를선택적으로초기화하면 Samsung KNOX 컨테이너도제거됩니다.

- iOS 및 macOS 장치의 경우 이 명령은 MDM 을 통해 설치된 모든 프로필을 제거합니다.
 - Windows 장치에서의 선택적 초기화는 현재 로그인된 모든 사용자의 프로필 폴더 내용도 제거합니다. 선택적 초기화는 구성을 통해 사용자에게 배달하는 웹 클립은 제거하지 않습니다. 웹 클립을 제거하려면 사용자가 자신의 장치를 수동으로 등록 취소해야 합니다. 선택적으로 초기화된 장치를 다시 등록할 수 없습니다.
 - Windows Phone 장치를 선택적으로 초기화하면 XenMobile 이 장치에 앱을 설치하도록 허용하는 엔터프라이즈 토큰이 제거됩니다. 또한 초기화는 장치에 배포된 모든 XenMobile 인증서 및 구성도 제거합니다. 선택적으로 초기화된 Windows Phone 장치를 다시 등록할 수 없습니다.
 - Android 장치의 선택적 초기화를 수행하면 장치가 해지되며 장치를 다시 등록하려면 먼저 장치를 다시 승인하거나 콘솔에서 삭제해야 합니다.
- **잠금 해제:** 잠겨 있을 때 장치로 전송된 암호를 지웁니다. 이 명령은 장치를 잠금 해제하지 않습니다.

관리 > 장치의 장치 세부 정보 페이지에도 장치 보안 속성이나 열립니다. 이러한 속성에는 강력한 ID, 장치 잠금, 활성화 잠금 바이패스 및 플랫폼 유형에 대한 기타 정보 등이 포함됩니다. 장치 전체 초기화 필드에는 사용자 PIN 코드가 포함됩니다. 장치가 초기화된 후 사용자는 이 코드를 입력해야 합니다. 사용자가 코드를 잊은 경우 여기서 코드를 조회할 수 있습니다.

Android 장치에 대한 보안 동작

보안 동작	Android(Android Enterprise 장치 제외)	Android Enterprise(BYOD)	Android Enterprise(회사 소유)
앱 잠금	예	아니요	아니요
앱 초기화	예	아니요	아니요
전체 초기화	예	아니요	예
찾기	예: Android 6.0 이상을 실행하는 장치의 경우 위치를 사용하려면 사용자가 등록도중 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록도중 권한을 부여하지 않으면 XenMobile 은 위치 명령을 전송할 때 다시 위치 권한을 요청합니다.	예: Android 6.0 이상을 실행하는 장치의 경우 위치를 사용하려면 사용자가 등록도중 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록도중 권한을 부여하지 않으면 XenMobile 은 위치 명령을 전송할 때 다시 위치 권한을 요청합니다.	예: Android 6.0 이상을 실행하는 장치의 경우 위치를 사용하려면 사용자가 등록도중 위치 권한을 부여해야 합니다. 사용자는 위치 권한을 부여하지 않도록 선택할 수 있습니다. 사용자가 등록도중 권한을 부여하지 않으면 XenMobile 은 위치 명령을 전송할 때 다시 위치 권한을 요청합니다.
잠금	예	예	예
Lock and Reset Password(잠금 및 암호 재설정)	예	아니요	예

보안동작	Android(Android Enterprise 장치제외)	Android Enterprise(BYOD)	Android Enterprise(회사소유)
Notify (Ring)(알림 (벨울림))	예	예	예
해지	예	예	예
선택적초기화	예	예	아니요

iOS 및 macOS 장치에대한보안동작

보안동작	iOS	macOS
활성화잠금바이패스	예	아니요
앱잠금	예	아니요
앱초기화	예	아니요
ASM DEP 활성화잠금	예	아니요
제한사항지우기	예	아니요
분실모드활성화/비활성화	예	아니요
추적활성화/비활성화	예	아니요
전체초기화	예	예
찾기	예	아니요
잠금	예	예
벨울림	예	예
AirPlay 미러링요청/중지	예	아니요
다시시작/종료	예	아니요
Revoke/Authorize(해지/권한부여)	예	예
선택적초기화	예	예
잠금해제	예	아니요

Windows 장치에대한보안동작

보안동작	Windows Phone 10	Windows 태블릿 10	Windows Phone 8.1
찾기	예	예	아니요
잠금	예	예	예
Lock and Reset Password(잠금및암호재 설정)	예	아니요	예
다시부팅	예	예	아니요
해지	예	예	예
벨올림	예	아니요	예
선택적초기화	예	예	예
초기화	예	예	예

이문서의나머지부분에서는다양한보안동작을수행하는단계를설명합니다. 일부동작은자동화할수도있습니다. 자세한내용은 [자동화된동작](#)에서참조하십시오.

iOS 장치잠금

분실된 iOS 장치를잠그고장치잠금화면에메시지와전화번호를표시할수있습니다. 이기능은 iOS 7 이상을실행하는장치에서지원됩니다.

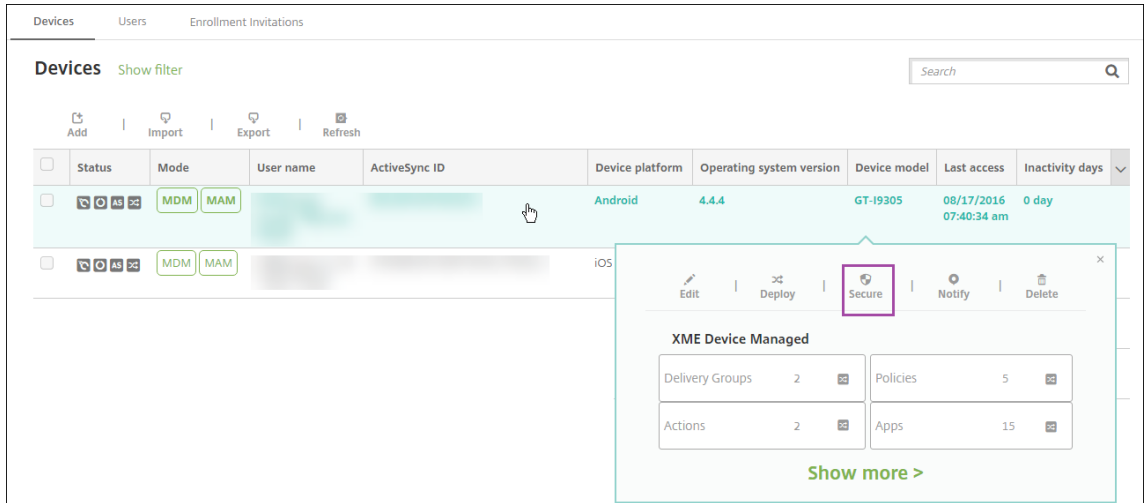
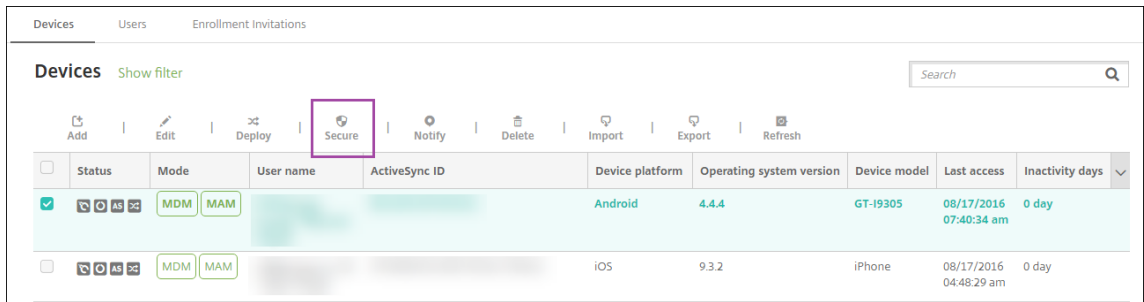
잠겨있는장치에메시지와전화번호를표시하려면 XenMobile 콘솔에서 [암호](#) 정책을 **true** 로설정합니다. 또는사용자가수동으로장치에서암호를사용하도록설정할수있습니다.

1. 관리 > 장치를클릭합니다. 장치페이지가나타납니다.

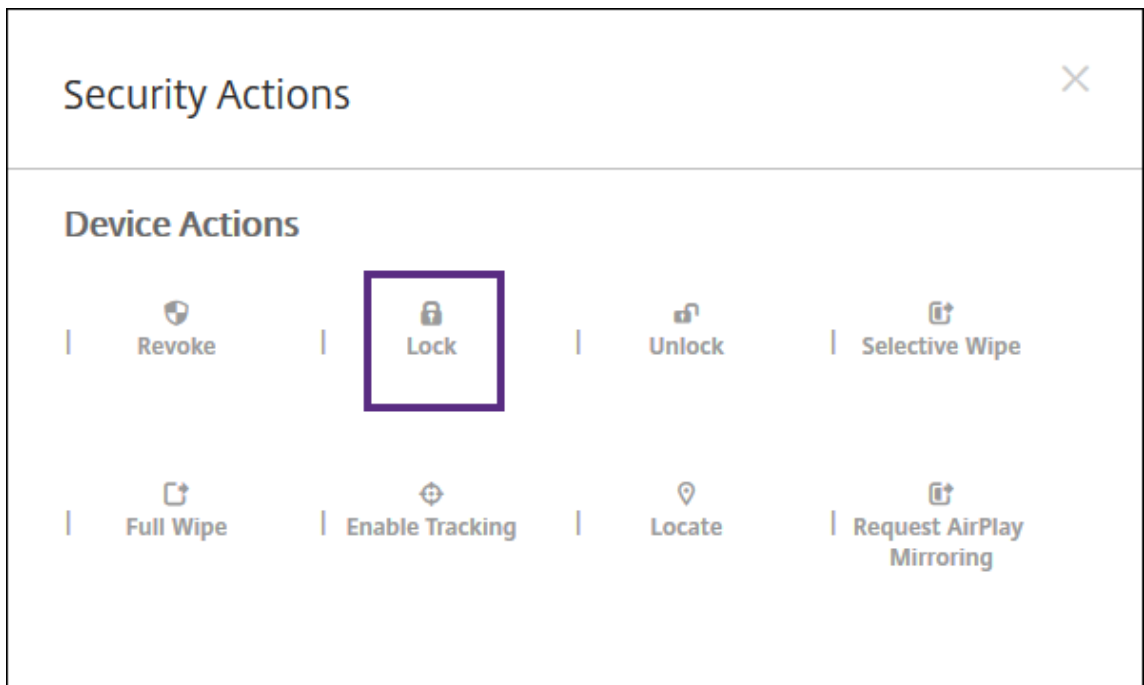


2. 잠글 iOS 장치를선택합니다.

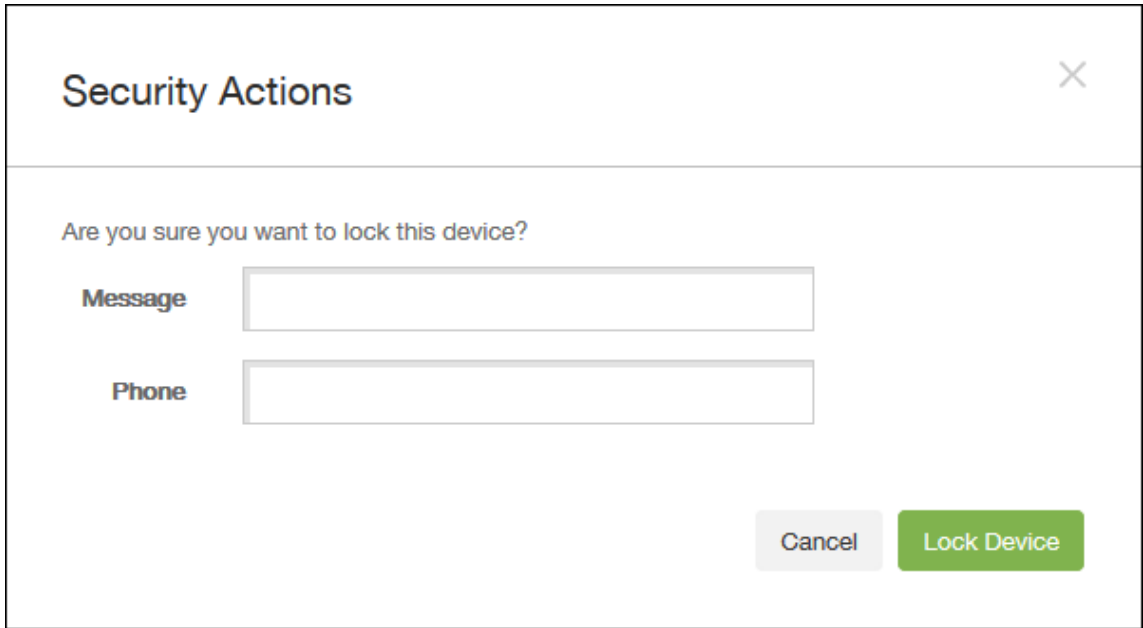
장치옆에있는확인란을선택하면장치목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.



3. 옵션메뉴에서 보안을클릭합니다. 보안동작대화상자가나타납니다.



4. 잠금을클릭합니다. 보안동작확인대화상자가표시됩니다.



5. 필요에 따라 장치 잠금 화면에 표시되는 메시지와 전화번호를 입력합니다.

iOS 7 이상을 실행하는 iPad 의 경우: 메시지 필드에 입력하는 내용에 “iPad 분실” 이라는 단어가 추가됩니다.

iOS 7 이상을 실행하는 iPhone 의 경우: 메시지 필드를 비워두고 전화번호를 입력할 경우 장치 잠금 화면에 “소유자에게 통화” 라는 메시지가 표시됩니다.

6. 장치 잠금을 클릭합니다.

XenMobile 콘솔에서 장치 제거

중요:

XenMobile 콘솔에서 장치를 제거하는 경우 관리되는 애플릿 데이터는 장치에 남습니다. 관리되는 애플릿 데이터를 장치에서 제거하려면 이 문서 뒷부분의 “장치 삭제” 를 참조하십시오.

XenMobile 콘솔에서 장치를 제거하려면 **관리 > 장치** 로 이동하여 관리되는 장치를 선택한 다음 삭제를 클릭합니다.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
<input checked="" type="checkbox"/>	MDM MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

장치를 선택적으로 초기화

1. **관리 > 장치** 로 이동하고 관리되는 장치를 선택한 다음 **보안** 을 클릭합니다.

2. 보안 동작에서 **선택적 초기화** 를 클릭합니다.

3. Android 장치의 경우에만 회사네트워크에서 장치를 분리합니다. 이렇게 하려면 장치가 초기화된 후 보안 동작에서 해지를 클릭하십시오.

초기화가 수행되기 전에 선택적 초기화 요청을 철회하려면 보안 동작에서 선택적 초기화 취소를 클릭합니다.

장치 삭제

이 절차는 관리되는 앱 및 데이터를 장치에서 제거하고 XenMobile 콘솔의 장치 목록에서 장치를 삭제합니다.

1. 관리 > 장치로 이동하고 관리되는 장치를 선택한 다음 보안을 클릭합니다.
2. 선택적 초기화를 클릭합니다. 메시지가 나타나면 선택적 초기화 수행을 클릭합니다.
3. 초기화 명령이 성공했는지 확인하려면 관리 > 장치를 새로고치십시오. 모드 열에서 MDM 및 MAM 의색이 황색이면 초기화 명령이 성공한 것입니다.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
	MDM MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

4. 관리 > 장치에서 장치를 선택한 다음 삭제를 클릭합니다. 메시지가 나타나면 삭제를 다시 클릭합니다.

앱 잠금, 잠금 해제, 초기화 또는 초기화 취소

1. 관리 > 장치로 이동하고 관리되는 장치를 선택한 다음 보안을 클릭합니다.
2. 보안 동작에서 앱 동작을 클릭합니다.

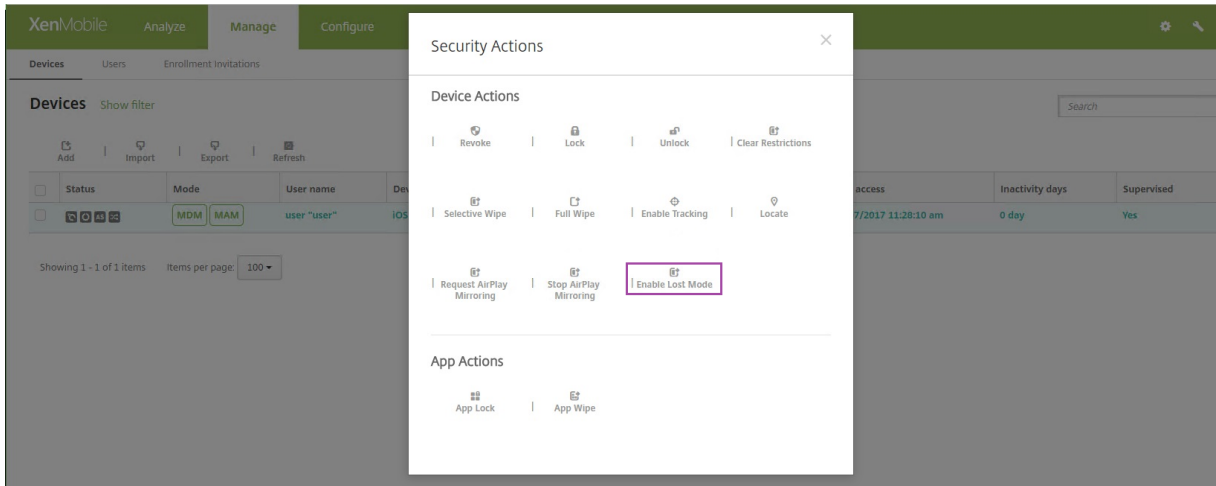
보안 동작 상자를 사용하여 Active Directory 에서 계정이 사용하지 않도록 설정되었거나 삭제된 사용자의 장치 상태를 확인할 수 있습니다. 앱 잠금 해제 또는 앱 초기화 취소 동작이 나타나면 앱이 잠겼거나 초기화되었음을 나타냅니다.

iOS 장치를 분실 모드로 전환

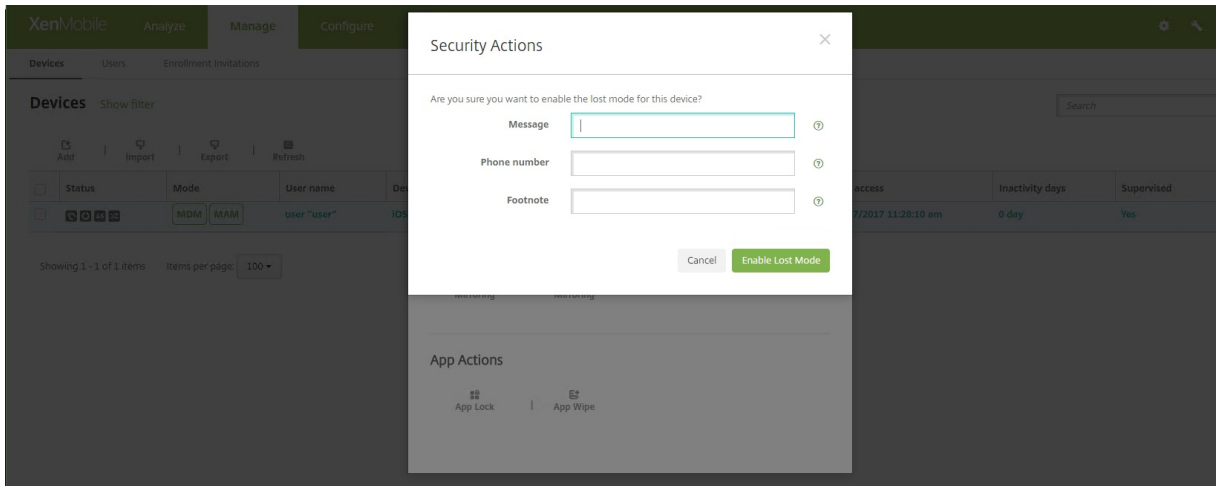
XenMobile 분실 모드 장치 속성은 iOS 장치를 분실 모드로 전환합니다. Apple 의 관리되는 분실 모드와 달리 XenMobile 의 분실 모드에서는 다음 동작 중 하나를 수행하여 사용자 가나 의 iPhone/iPad 찾기 설정을 구성하거나 Citrix Secure Hub 의 위치 서비스를 사용하지 않아도 장치 위치를 찾을 수 있습니다.

XenMobile 분실 모드에서는 XenMobile Server 만 장치 잠금을 해제할 수 있습니다. 이와 반대로 XenMobile 장치 잠금 기능을 사용하는 경우에는 사용자가 제공된 PIN 코드를 사용하여 장치를 직접 잠금 해제할 수 있습니다.

분실 모드를 사용하거나 사용하지 않으려면: 관리 > 장치로 이동하고 감도되는 iOS 장치를 선택한 후 보안을 클릭합니다. 분실 모드 활성화 또는 분실 모드 비활성화를 클릭합니다.

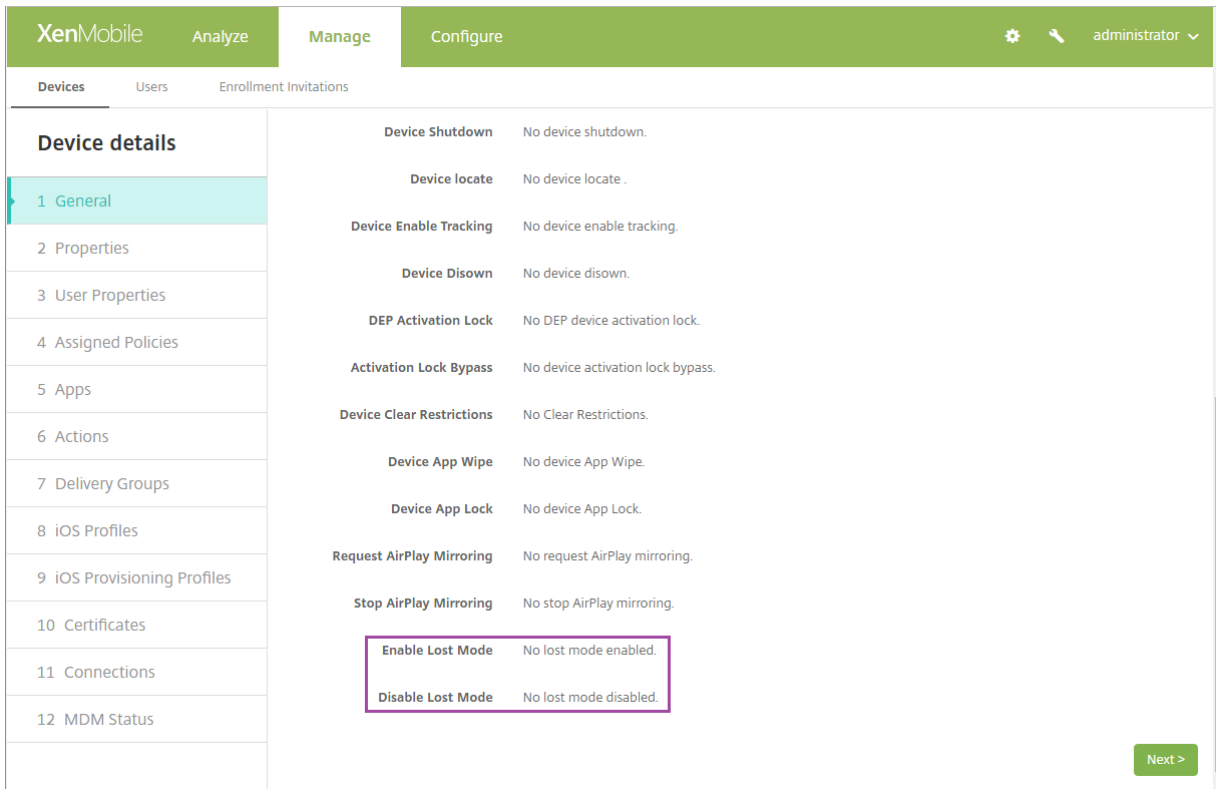


분실모드활성화를클릭하고장치가분실모드가될때장치에표시할정보를입력합니다.

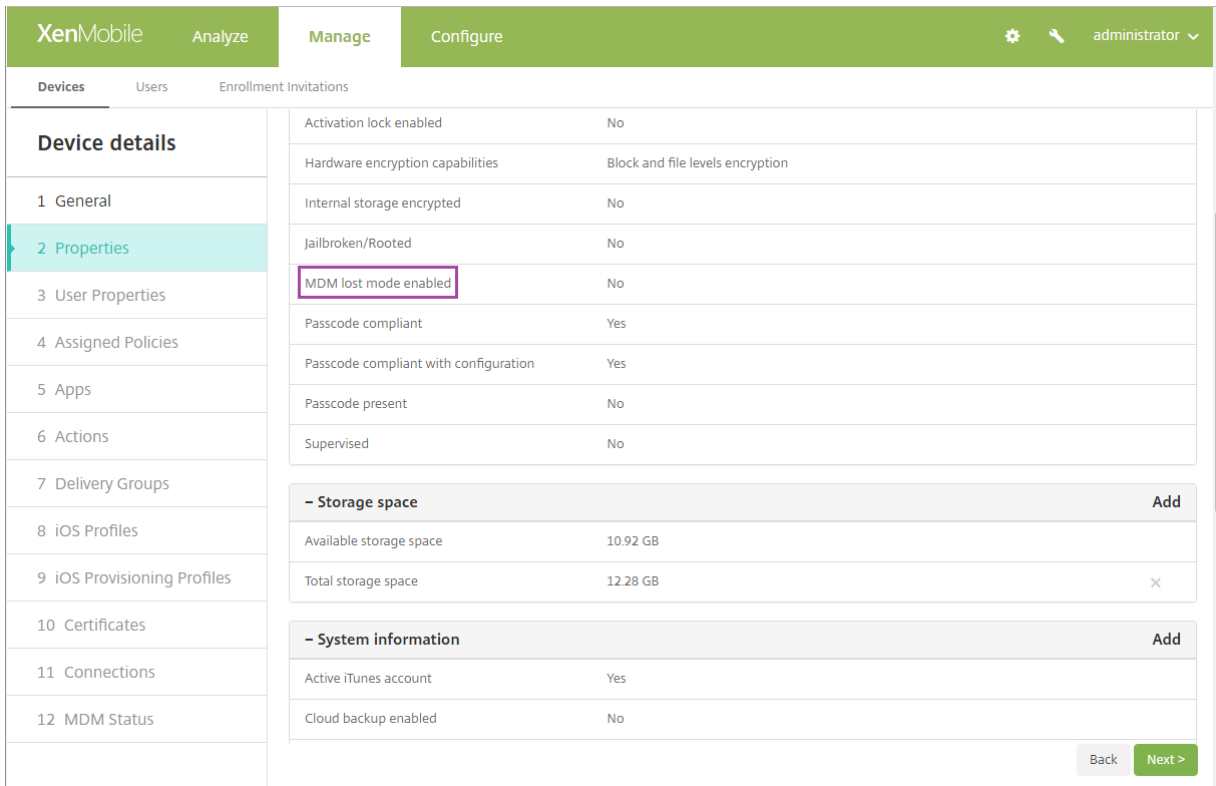


다음방법중하나를사용하여분실모드상태를확인합니다.

- 보안동작창에서단추가 분실모드비활성화인지확인합니다.
- 관리 > 장치에서 일반탭의 보안아래에서마지막분실모드활성화또는분실모드비활성화동작을확인합니다.



- 관리 > 장치의 속성탭에서 **MDM** 분실모드활성화설정의값이올바른지확인합니다.



iOS 장치에서 XenMobile 분실모드를사용하는경우 XenMobile 콘솔이다음과같이변경됩니다.

- 구성 > 동작에서 동작목록에 장치해지, 장치를선택적으로초기화및 장치를완전히초기화자동화동작이포함되지않습니다.
- 관리 > 장치에서 보안동작목록에 해지및 장치선택적초기화동작이더이상포함되지않습니다. 필요한경우보안동작을사용하여 전체초기화를수행할수있습니다.

iOS 7 이상을실행하는 iPad 의경우: 보안동작화면의 메시지에무엇을입력하든지관계없이끝에 “iPad 분실” 이라는단어가추가됩니다.

iOS 7 이상을실행하는 iPhone 의경우: 메시지를비워둔경우전화번호를입력하면장치잠금화면에 “소유자에게통화” 메시지가표시됩니다.

iOS 활성화잠금바이패스

활성화잠금은분실되거나도난당한장치의재활성화를방지하는내 iPhone/iPad 찾기기능입니다. 활성화잠금은누군가가내 iPhone/iPad 찾기를끄고장치를지우거나장치를재활성화하여사용하려고할경우사용자의 Apple ID 와암호를요구합니다. 조직이소유한장치의경우예를들어장치를재설정하거나재할당하기위해활성화잠금을바이패스해야합니다.

활성화잠금을사용하도록설정하려면 XenMobile MDM 옵션장치정책을구성하고배포합니다. 그러면사용자의 Apple 자격증명없이도 XenMobile 콘솔에서장치를관리할수있습니다. 활성화잠금의 Apple 자격증명요구사항을바이패스하려면 XenMobile 콘솔에서활성화잠금바이패스보안동작을실행합니다.

예를들어사용자가분실된휴대폰을반환하거나전체초기화전후에장치를설정하는경우 iTunes 계정자격증명을묻는메시지가표시될때 XenMobile 콘솔에서활성화잠금바이패스보안동작을실행하여이단계를바이패스할수있습니다.

활성화잠금바이패스를위한장치요구사항

- iOS 7.1(최소버전)
- Apple Configurator 또는 Apple DEP 를통해감독됨
- iCloud 계정을사용하여구성됨
- 내 iPhone/iPad 찾기를사용하도록설정됨
- XenMobile 에서등록됨
- 활성화잠금을사용하도록설정된 MDM 옵션장치정책이장치에배포됨

장치의전체초기화를실행하기전에활성화잠금을바이패스하려면:

1. 관리 > 장치에서장치를선택하고 보안을클릭한다음 활성화잠금바이패스를클릭합니다.
2. 장치를초기화합니다. 장치설정중에활성화잠금화면이표시되지않습니다.

장치의전체초기화를실행한후에활성화잠금을바이패스하려면:

1. 장치를재설정하거나초기화합니다. 장치설정중에활성화잠금화면이표시됩니다.
2. 관리 > 장치에서장치를선택하고 보안을클릭한다음 활성화잠금바이패스를클릭합니다.
3. 장치에서뒤로단추를누릅니다. 홈화면이나타납니다.

다음사항에유의하십시오.

- 사용자에게 내 iPhone/iPad 찾기를 끄지말라고일러두십시오. 장치에서전체초기화를수행하지마십시오. 두경우모두사용자에게 iCloud 계정암호를입력하라는메시지가표시됩니다. 계정유효성검사후모든콘텐츠와설정을지운다음사용자에게 iPhone/iPad 활성화화면이표시되지않습니다.
- 활성화잠금바이패스코드가생성되고활성화잠금을사용하도록설정장치경우전체초기화후 iPhone/iPad 활성화페이지를바이패스할수없으면 XenMobile 에서장치를삭제할필요가없습니다. 관리자또는사용자가 Apple 지원팀에연락하여직접장치의차단을해제할수있습니다.
- 하드웨어인벤티리중에 XenMobile 은장치에서활성화잠금바이패스코드를취리합니다. 바이패스코드를사용할수있는경우장치가해당코드를 XenMobile 에전송합니다. 그런다음장치에서바이패스코드를제거하려면 XenMobile 콘솔에서활성화잠금바이패스보안동작을전송합니다. 이때장치의차단을해제하려면 XenMobile Server 와 Apple 에바이패스코드가있어야합니다.
- 활성화잠금바이패스보안동작은 Apple 서비스의이용가능성에따라달라집니다. 이동작이작동하지않는경우다음과같이장치의차단을해제할수있습니다. 장치에서수동으로 iCloud 계정의자격증명을입력합니다. 또는사용자이름필드를비워두고암호필드에바이패스코드를입력합니다. 바이패스코드를조회하려면 관리 > 장치로이동하여장치를선택하고 편집, 속성을차례로클릭합니다. 활성화잠금바이패스코드는 보안정보아래에있습니다.

공유장치

January 6, 2020

XenMobile 을통해여러사용자가공유할수있는장치를구성할수있습니다. 공유장치기능을사용하면, 예를들어병원의임상의사가 특정장치를가지고다닐필요없이주변에있는장치를사용하여앱과데이터에액세스할수있습니다. 법집행, 소매및제조와같은분야의 교대근무자가장치를공유하여장비비용을절감할수도있습니다.

공유장치에대한주요사항

지원되는모든 iOS 및 Android 장치를공유장치로사용할수있습니다. 지원되는장치목록은 [지원되는장치운영체제](#)를참조하십시오.

MDM 모드

- iOS 및 Android 태블릿과스마트폰에서모두사용할수있습니다. XenMobile Enterprise 공유장치에는기본 DEP(장치등록프로그램) 등록이지원되지않습니다. 승인된 DEP 를사용하여이모드의공유장치를등록해야합니다.
- 클라이언트인증서인증, Citrix PIN, Touch ID, 사용자엔트로피및 2 단계인증은지원되지않습니다.

MDM+MAM 모드

- iOS 및 Android 태블릿에서만사용할수있습니다.

- Active Directory 사용자이름및암호인증만지원됩니다.
- 클라이언트인증서인증, Worx PIN, Touch ID, 사용자엔트로피및 2 단계인증은지원되지않습니다.
- MAM 전용모드는지원되지않습니다. MDM 에서장치를등록해야합니다.
- Secure Mail, Secure Web 및 ShareFile Mobile 앱만지원됩니다. HDX 앱은지원되지않습니다.
- Active Directory 사용자만지원됩니다. 로컬사용자및그룹은지원되지않습니다.
- 기존 MDM 전용공유장치를 MDM+MAM 모드로업데이트하려면재등록이필요합니다.
- 사용자는장치의기본앱을공유할수없습니다.
- 처음등록할때다운로드된후에는새사용자가장치에로그온해도모바일생산성앱이다시다운로드되지않습니다. 새로운사용자는원하는장치를가져와로그온하고작업을수행할수있습니다.
- Android 에서보안을위해각사용자의데이터를격리하려면 XenMobile 콘솔의 **Disallow rooted devices**(루팅된 장치허용안함) 정책이 켜짐이어야합니다.

공유장치등록을위한사전요구사항

공유장치를등록하려면먼저다음을수행해야합니다.

- 공유장치등록사용자역할을만듭니다. [RBAC 를사용하여역할구성](#)에서자세한내용을참조하십시오.
- 공유장치사용자를만듭니다. [로컬사용자계정을추가, 편집또는삭제하려면](#)에서자세한내용을참조하십시오.
- 공유장치등록사용자에게적용할기본정책, 앱및동작을포함하는배달그룹을만듭니다. [리소스배포](#)에서자세한내용을참조하십시오.

MDM+MAM 모드를위한사전요구사항

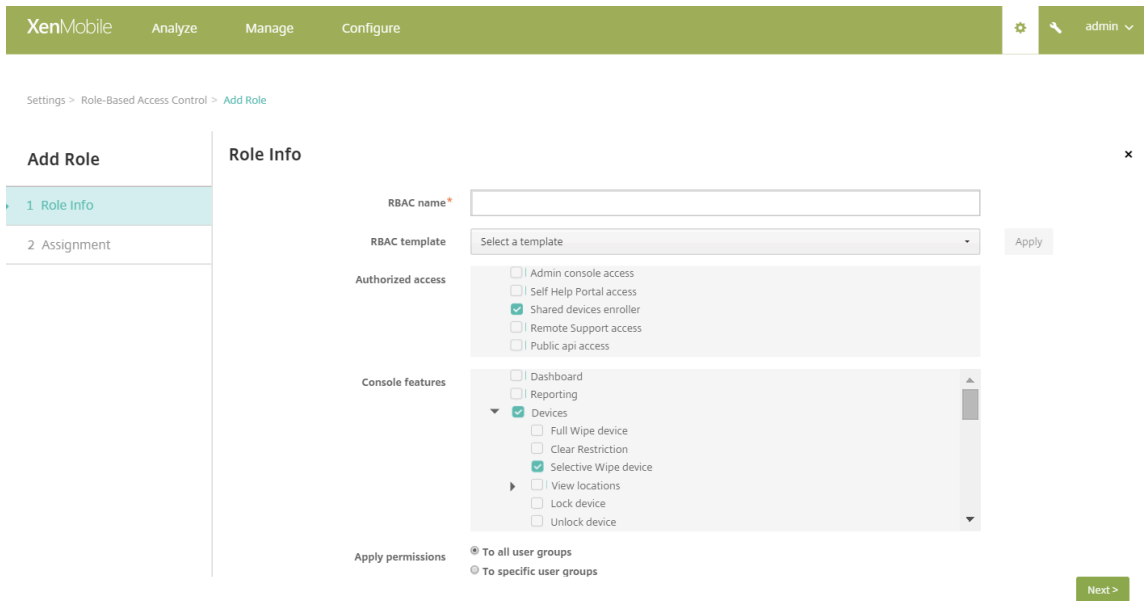
1. **Shared Device Enrollers** 같은이름으로 Active Directory 그룹을만듭니다.
2. 공유장치를등록할 Active Directory 사용자를이그룹에추가합니다. 이용도로세계정을사용하려면새 Active Directory 사용자 (예: **sdenroll**) 를만들고해당사용자를 Active Directory 그룹에추가합니다.

공유장치구성

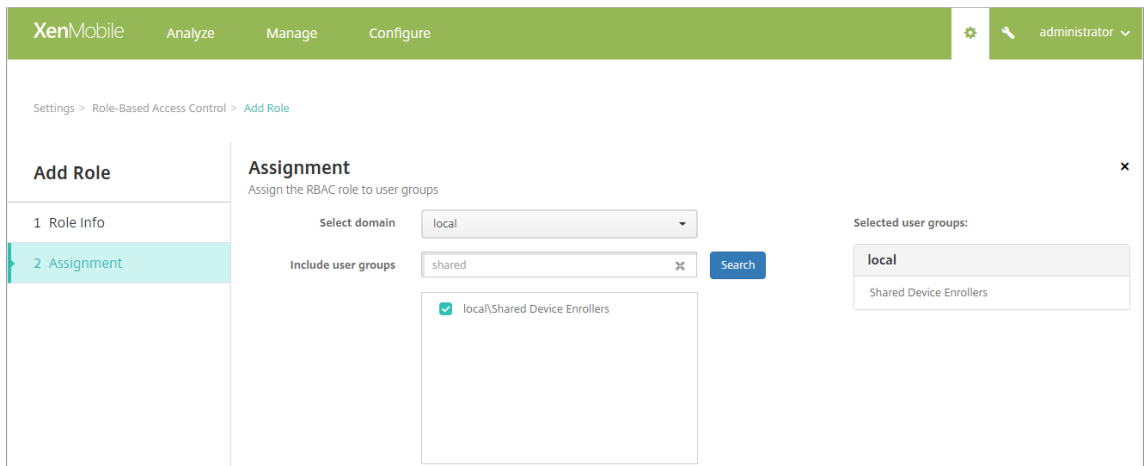
다음단계에따라공유장치를구성합니다.

1. XenMobile 콘솔에서오른쪽위모서리의기어를클릭합니다. 설정페이지가나타납니다.
2. 역할기반액세스제어를클릭한다음 추가를클릭합니다. 역할추가화면이나타납니다.
3. 허가된엑세스아래에서 공유장치등록자권한이있는 **Shared Device Enrollment User** 라는공유장치등록사용자역할을만듭니다. 콘솔기능에서 장치를확장한다음 장치선택적초기화를선택하십시오. 이설정을사용하면장치가등록취소될때공유장치등록자계정을통해프로비저닝된앱및정책이 Secure Hub 를통해삭제됩니다.

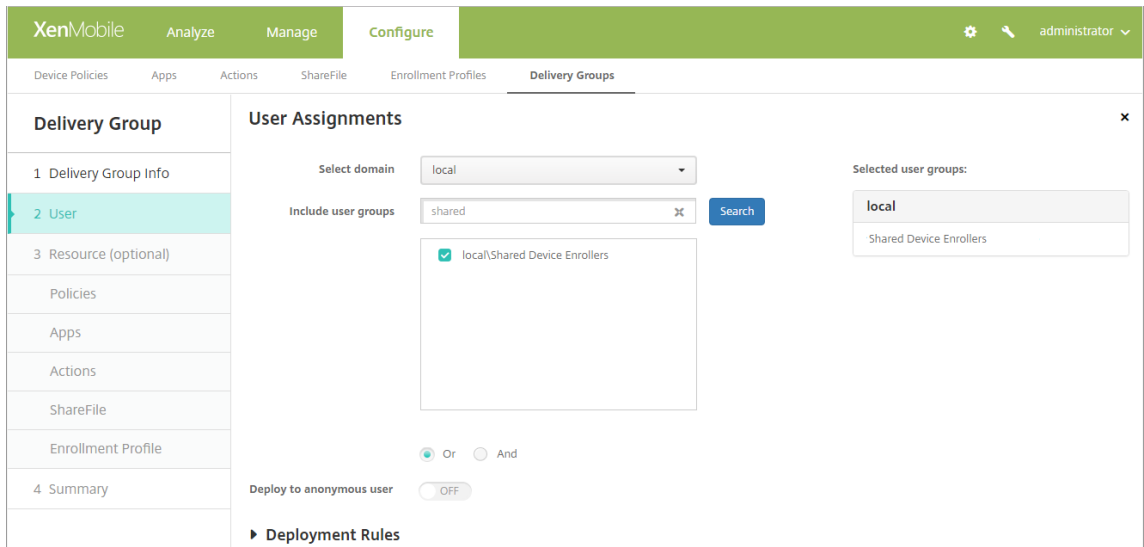
권한적용은기본설정인 모든사용자그룹으로유지하거나, 특정사용자그룹을사용하여특정 Active Directory 사용자그룹에권한을할당합니다.



다음클릭하여 할당화면으로이동합니다. 방금생성한공유장치등록역할을 1 단계의사전요구사항에서공유장치등록사용자용으로만든 Active Directory 그룹에할당합니다. 아래이미지에서 **citrix.lab** 은 Active Directory 도메인이고 **Shared Device Enrollers** 는 Active Directory 그룹입니다.



4. 사용자가로그온하지않은상태에서장치에적용할기본정책, 앱및동작을포함하는배달그룹을만든다음해당배달그룹을공유장치등록사용자 Active Directory 그룹과연결합니다.



5. 공유장치에 Secure Hub 를 설치하고 공유장치 등록 사용자 계정을 사용하여 XenMobile 에 장치를 등록합니다. 이제 XenMobile 콘솔을 통해 장치를 보고 관리할 수 있습니다. 자세한 내용은 [장치 등록](#)에서 참조하십시오.
6. 서로 다른 정책을 적용하거나 인증된 사용자를 위한 추가 앱을 제공하려면 해당 사용자 와 연결되고 공유장치에만 배포된 배달 그룹을 만들어야 합니다. 그룹을 만들 때 배포 규칙을 구성하여 패키지가 공유장치에 배포되도록 합니다. 자세한 내용은 [리소스 배포](#)에서 참조하십시오.
7. 장치 공유를 중지하려면 선택적 초기화를 수행하여 장치에서 공유장치 등록 사용자 계정과 함께 장치에 배포된 모든 앱 및 정책을 제거합니다.

공유장치 사용자 환경

MDM 모드

사용자는 자신이 사용할 수 있는 리소스만 보며 모든 공유장치에서 동일한 환경을 사용합니다. 공유장치 등록 정책 및 앱이 항상 장치에 유지됩니다. 공유장치에 등록되어 있지 않은 사용자가 Secure Hub 에 로그인하면 해당 사용자의 정책 및 앱이 장치에 배포됩니다. 해당 사용자가 로그오프하면 공유장치 등록의 정책 및 앱과 다른 정책 및 앱이 제거되지만 공유장치 등록 리소스는 그대로 유지됩니다.

MDM+MAM 모드

공유장치 등록 사용자가 등록할 때 장치에 Secure Mail 및 Secure Web 이 배포됩니다. 사용자 데이터는 장치에서 안전하게 유지 관리됩니다. Secure Mail 또는 Secure Web 에 로그인하는 다른 사용자에게 데이터가 노출되지 않습니다.

한 번에 한 사용자만 Secure Hub 에 로그인할 수 있습니다. 다음 사용자가 로그인하려면 이전 사용자가 로그오프해야 합니다. 보안상의 이유로 Secure Hub 는 공유장치에 사용자 자격 증명을 저장하지 않으므로 사용자는 로그인할 때마다 자격 증명을 입력해야 합니다. 새로운 사용자가 이전 사용자를 위해 만들어진 리소스에 액세스할 수 없도록 하기 위해 Secure Hub 는 이전 사용자와 관련된 정책, 앱 및 데이터가 제거되는 동안 새 사용자가 로그인하는 것을 허용하지 않습니다.

공유장치등록은앱업그레이드하는프로세스를변경하지않습니다. 이전과마찬가지로, 공유장치사용자에게업그레이드를푸시할 수있으며공유장치사용자가장치에서바로앱업그레이드할수있습니다.

권장 **Secure Mail** 정책

- 최상의 Secure Mail 성능을얻으려면장치를공유할사용자의수를기반으로 **Max sync period(최대동기화기간)** 를설정합니다. 무제한동기화를허용하는것은권장하지않습니다.

장치를공유하는사용자수	권장최대동기화기간
21~25 명	1 주이하
6~20 명	2 주이하
5 명이하	1 개월이하

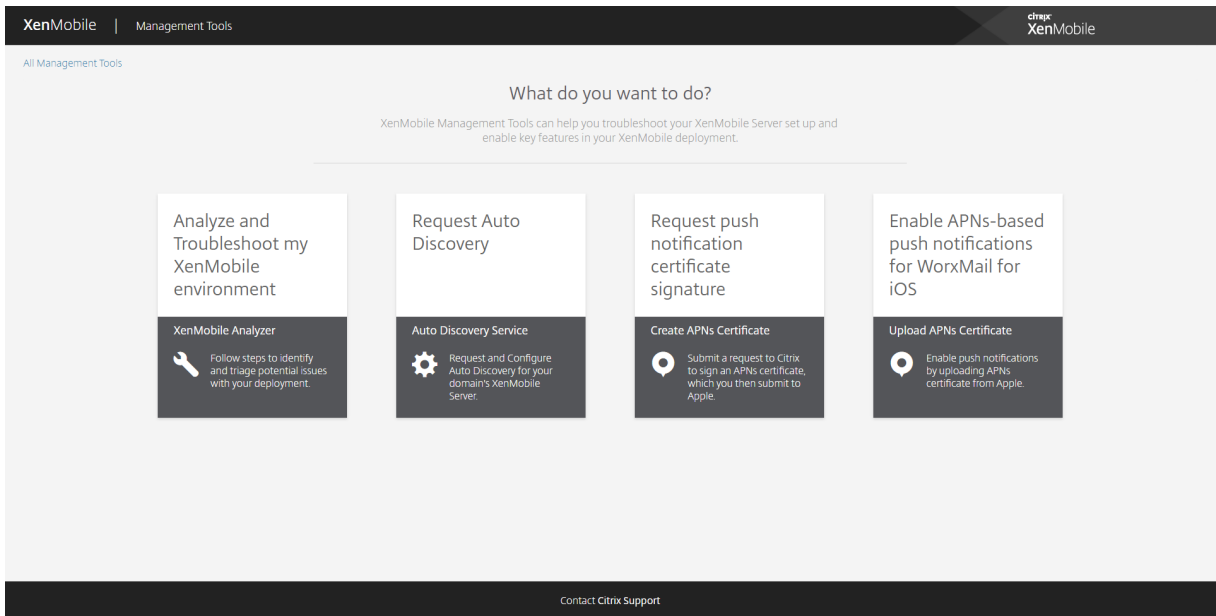
- 장치를공유하는다른사용자에게연락처가노출되는것을방지하려면 **Enable contact export(연락처내보내기사용)** 를차단합니다.
- iOS 에서는사용자별로다음과같은설정만설정할수있습니다. 다른모든설정은장치를공유하는모든사용자에게공통입니다.
 - 알림
 - 서명
 - 부재중
 - 메일동기화기간
 - S/MIME
 - 맞춤법검사

XenMobile Autodiscovery Service

August 23, 2019

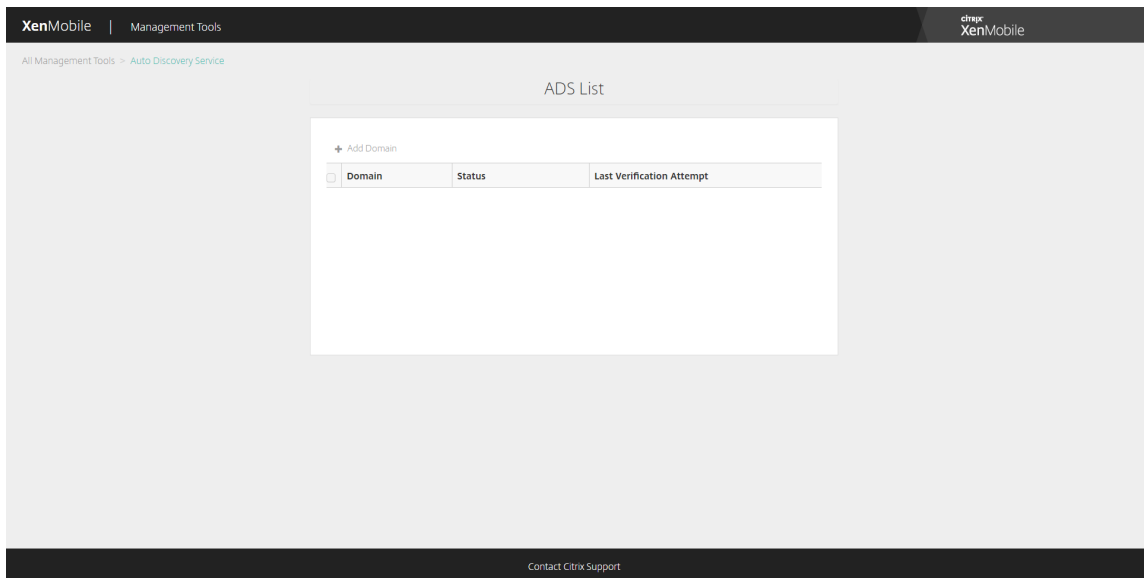
자동검색은많은 XenMobile 배포에서중요한부분입니다. 자동검색은사용자의등록프로세스를간소화합니다. 사용자는 XenMobile 서버에대한세부정보를입력할필요없이네트워크사용자이름과 Active Directory 암호를사용하여장치를등록할수있습니다. 사용자이름은 UPN(사용자계정이름) 형식 (예: user@mycompany.com) 으로입력합니다. XenMobile AutoDiscovery Service 를사용하면 Citrix 지원의도움없이자동검색레코드를만들거나편집할수있습니다.

XenMobile AutoDiscovery Service 에액세스하려면 <https://xenmobiletools.citrix.com>으로이동하고 **Request Auto Discovery(자동검색요청)** 를클릭합니다.

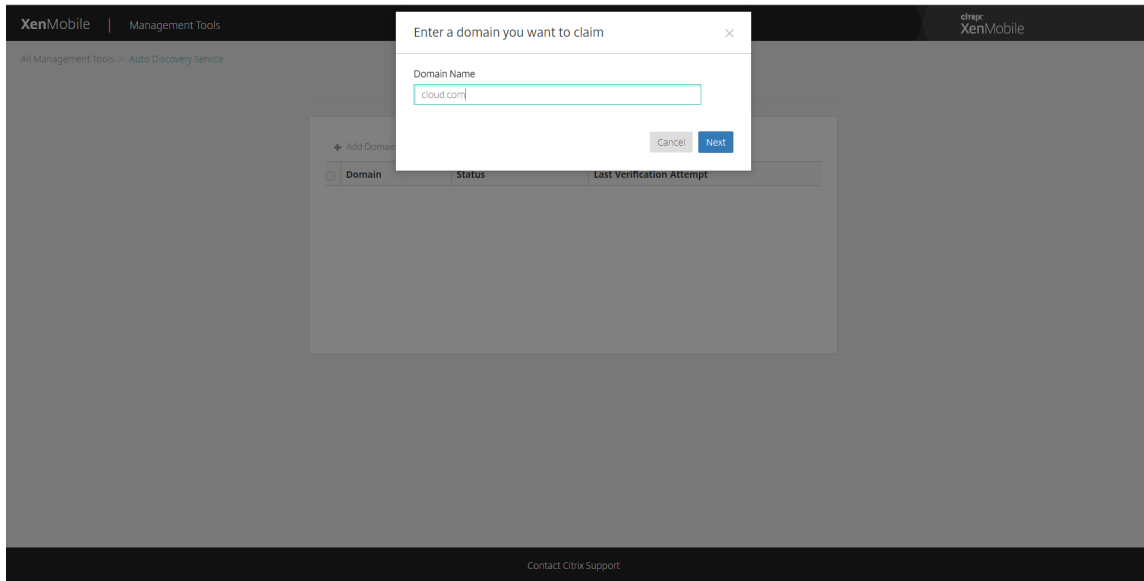


AutoDiscovery 요청

1. AutoDiscovery Service 페이지에서먼저도메인을요청해야합니다. **Add Domain(도메인추가)** 을클릭합니다.



2. 대화상자가열리면 XenMobile 환경의도메인이름을입력하고 **Next(다음)** 를클릭합니다.



3. 다음단계에서도메인을소유하고있는지확인하는방법에대한지침이제공됩니다.

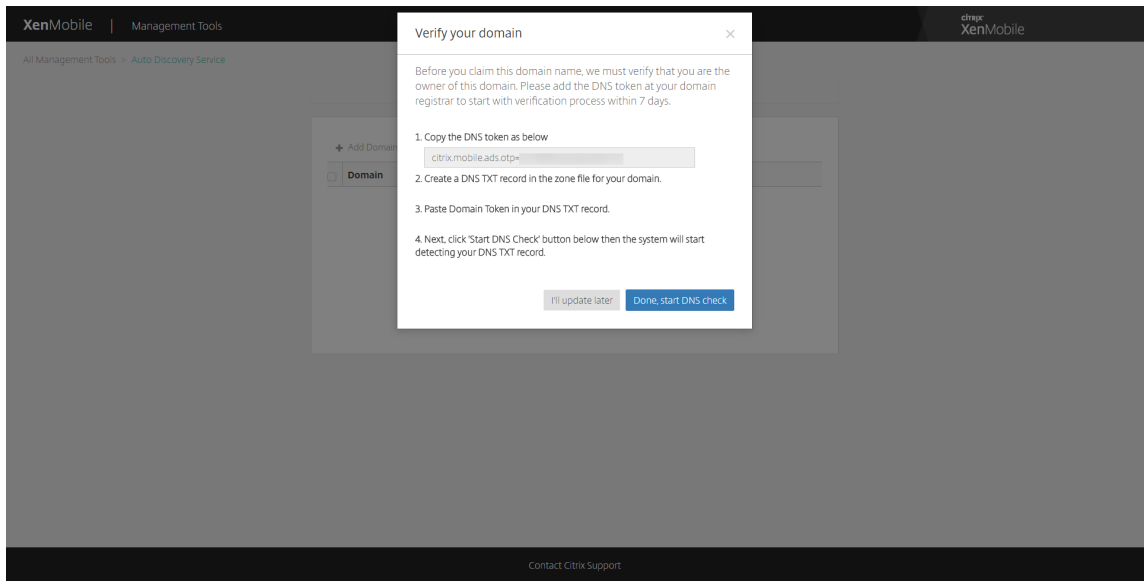
- XenMobile Tools 포털에서제공되는 DNS 토큰을복사합니다.
- 도메인호스팅공급자포털에서도메인에대한영역파일에 DNS TXT 레코드를만듭니다.

DNS TXT 레코드를만들려면위의 2 단계에서추가한도메인의도메인호스팅공급자포털에로그인해야합니다. 도메인호스팅포털에서도메인이름서버레코드를편집하고사용자지정 TXT 레코드를추가할수있습니다. 아래예제는호스팅포털에서샘플도메인 domain.com 에대한 DNS TXT 항목을추가하는방법에대한것입니다.

- 도메인토큰을 DNS TXT 레코드에붙여넣고도메인이름서버레코드를저장합니다.
- XenMobile Tools 포털에서 **Done(완료)** 을클릭하고 DNS 검사를시작합니다.

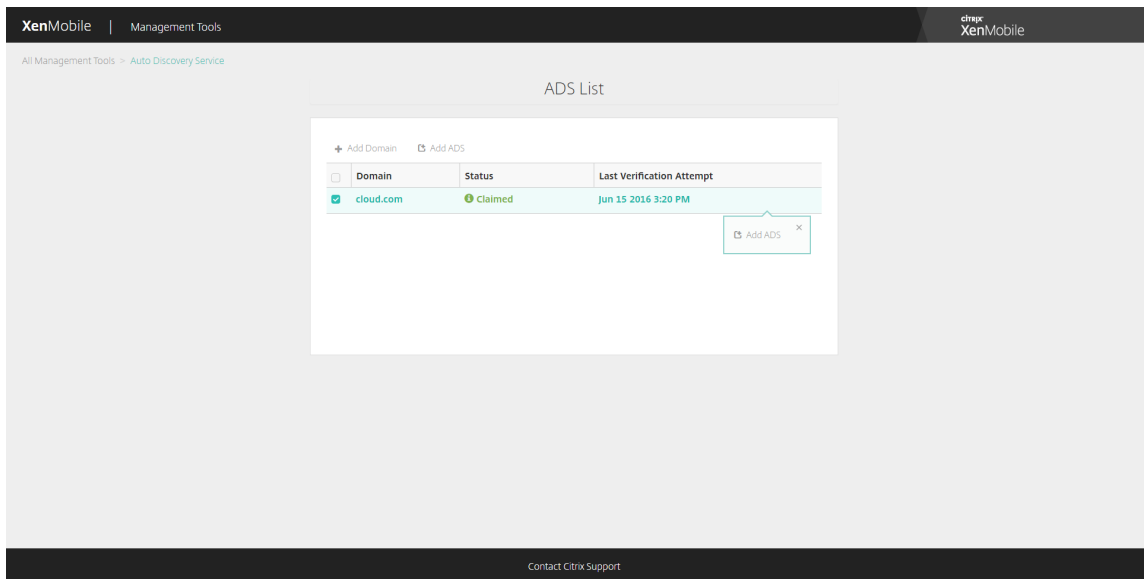
시스템에서 DNS TXT 레코드가감지됩니다. 또는 **I'll update later(나중에업데이트)** 를클릭하면레코드가저장됩니다. **Waiting record(레코드대기)** 를선택하고 **DNS Check(DNS 검사)** 를클릭하지않으면 DNS 검사가시작되지않습니다.

이검사는원래한시간가량소요되지만응답을반환하는데최대 2 일까지소요될수있습니다. 또한상태변경사항을보려면포털을나간후다시방문해야합니다.

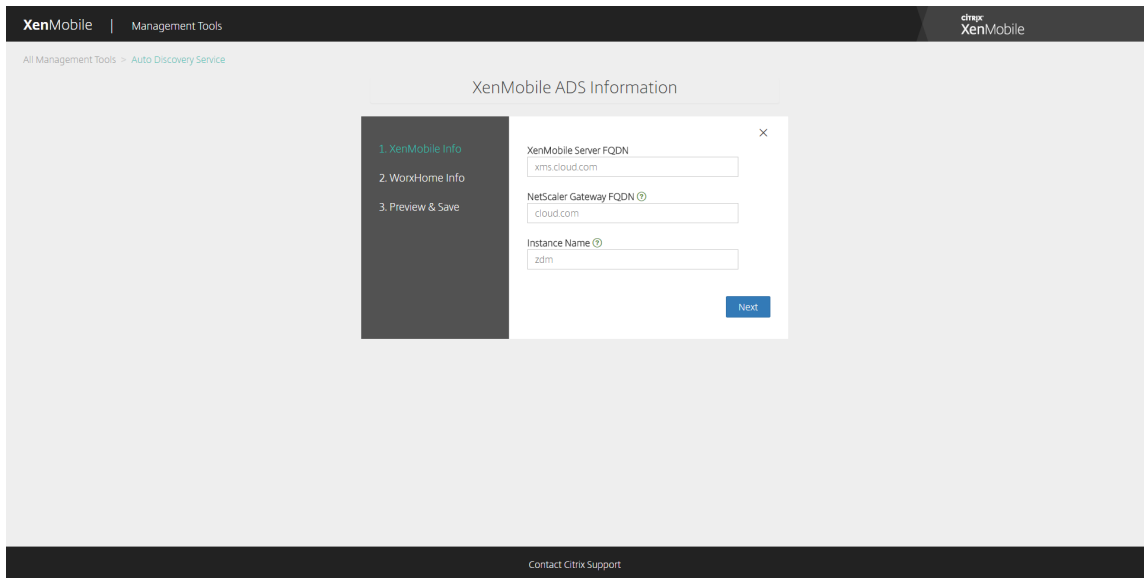


4. 도메인을요청한후 AutoDiscovery Service 정보를입력할수있습니다. 자동검색을요청할도메인레코드를마우스오른쪽단추로클릭하고 **Add ADS(ADS 추가)** 를클릭합니다.

도메인에 AutoDiscovery 레코드가있는경우 Citrix 기술지원에사례를기록하여필요에따라세부정보를수정합니다.



5. **XenMobile Server FQDN, NetScaler Gateway FQDN** 및 인스턴스이름을입력하고 **Next(다음)** 를클릭합니다. 확실하지않은경우기본인스턴스인 "zdm" 을추가합니다.



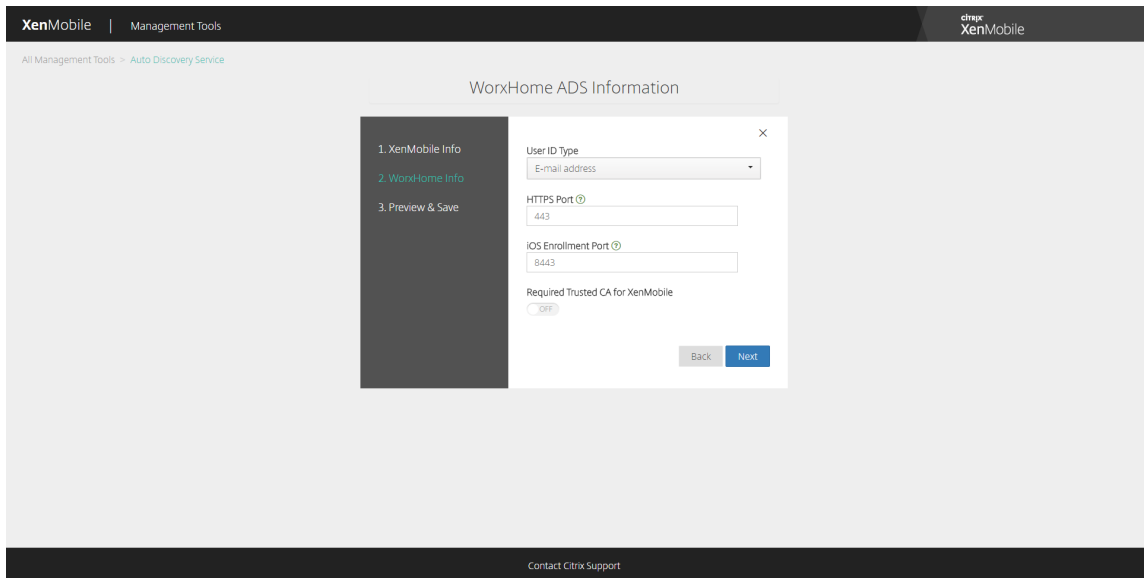
참고:

이전스크린샷에서 Worx Home 의이름이 Secure Hub 로바뀌었습니다.

6. Secure Hub 에대한다음정보를입력하고 **Next(다음)** 를클릭합니다.

- **User ID Type(사용자 ID 유형): E-mail address(전자메일주소) 또는 UPN** 중에서사용자가로그온할때사용할 ID 유형을선택합니다.

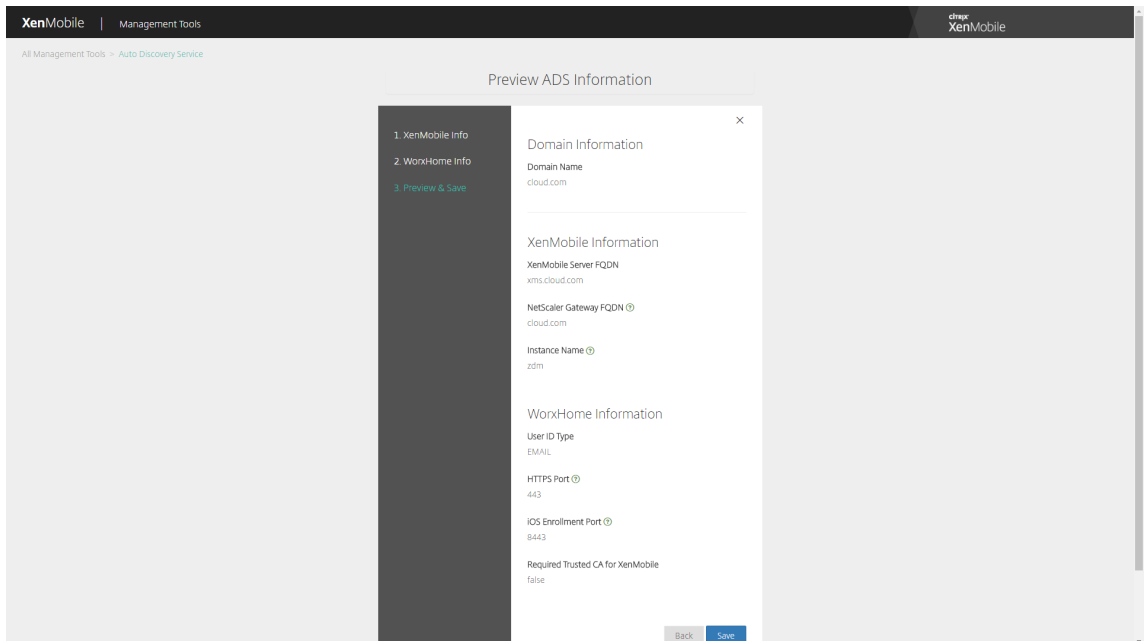
UPN 은사용자의 UPN(사용자계정이름) 이전자메일주소와동일한경우사용됩니다. 두방법모두입력된도메인을사용하여서버주소를찾습니다. **E-mail address(전자메일주소)** 를사용하는경우사용자이름및암호를입력하라는메시지가표시되며 **UPN** 을사용하는경우암호를입력하라는메시지가표시됩니다.
- **HTTPS Port(HTTPS 포트):** HTTPS 를통해 Secure Hub 에액세스할때사용할포트를입력합니다. 일반적으로이포트는포트 443 입니다.
- **iOS Enrollment Port(iOS 등록포트):** iOS 등록시 Secure Hub 에액세스할때사용할포트를입력합니다. 일반적으로이포트는포트 8443 입니다.
- **Required Trusted CA for XenMobile(XenMobile 에신뢰할수있는 CA 필요):** XenMobile 에액세스할때신뢰할수있는인증서가필요한지여부를나타냅니다. 이옵션은 **OFF(꺼짐)** 또는 **ON(켜짐)** 일수있습니다. 신뢰할수있는인증서를사용하려면 Citrix 지원에문의하여인증서를업로드하십시오. 인증서고정에대한자세한내용은모바일생산성업설명서에서 [Secure Hub](#)의인증서고정섹션을참조하십시오. 인증서고정이작동하는데필요한포트에대한자세한내용은 [XenMobile Port Requirements for ADS Connectivity\(ADS 연결을위한 XenMobile 포트요구사항\)](#)의지원문서를참조하십시오.



참고:

이전스크린샷에서 Worx Home 의이름이 Secure Hub 로바뀌었습니다.

7. 이전단계에서입력한모든정보가요약페이지에표시됩니다. 데이터가올바른지확인하고 **Save(저장)** 를클릭합니다.



참고:

이전스크린샷에서 Worx Home 의이름이 Secure Hub 로바뀌었습니다.

장치정책

January 6, 2020

정책을 만들어 XenMobile 이장치와 상호작용하는 방식을 구성할 수 있습니다. 많은 정책이 모든 장치에 공통적으로 적용되지만 각 장치에 해당 운영체제와 관련된 일련의 정책이 있습니다. 따라서 플랫폼간에는 물론 Android 장치 제조업체 사이에서도 차이가 있을 수 있습니다.

각 장치 정책에 대한 요약 설명은 이 문서의 장치 정책 요약을 참조하십시오.

참고:

환경에 GPO(그룹 정책 개체)가 구성되어 있는 경우:

Windows 10용 XenMobile 장치 정책을 구성할 때 다음 규칙을 고려하십시오. 하나 이상의 등록된 Windows 10 장치에 서 정책이 충돌하는 경우 GPO와 일치하는 정책이 우선합니다.

Android Enterprise 컨테이너가 지원되는 정책은 [Android Enterprise](#)를 참조하십시오.

사전 요구 사항

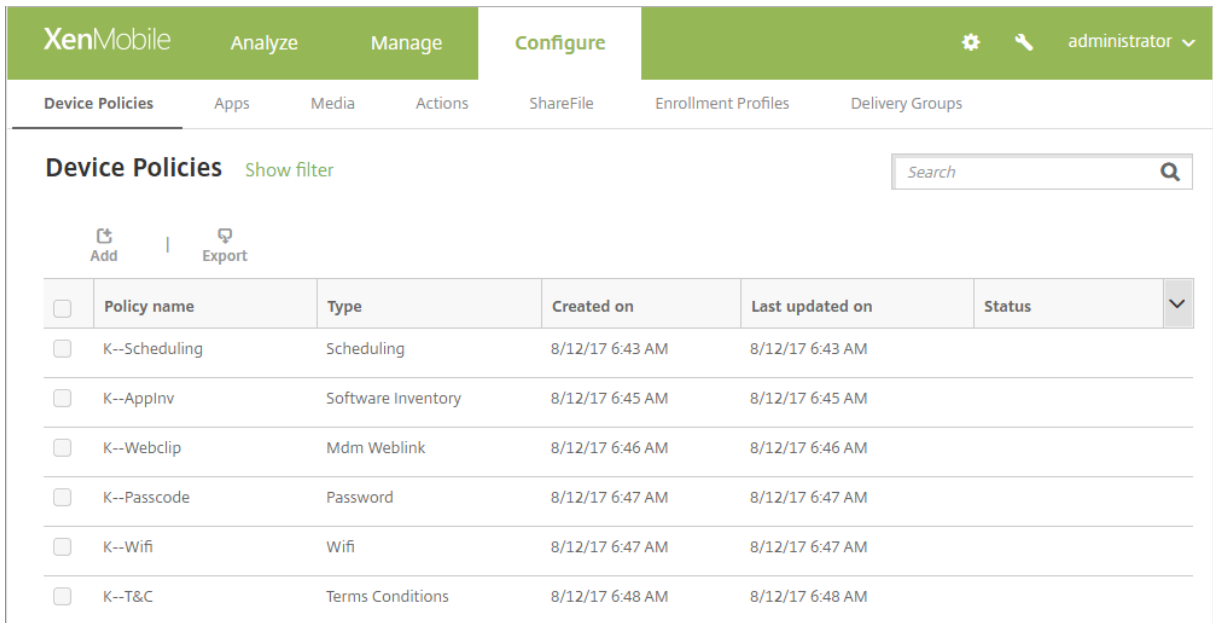
- 사용하려는 배달 그룹을 만듭니다.
- 필요한 모든 CA 인증서를 설치합니다.

장치 정책 추가

장치 정책을 만드는 기본 단계는 다음과 같습니다.

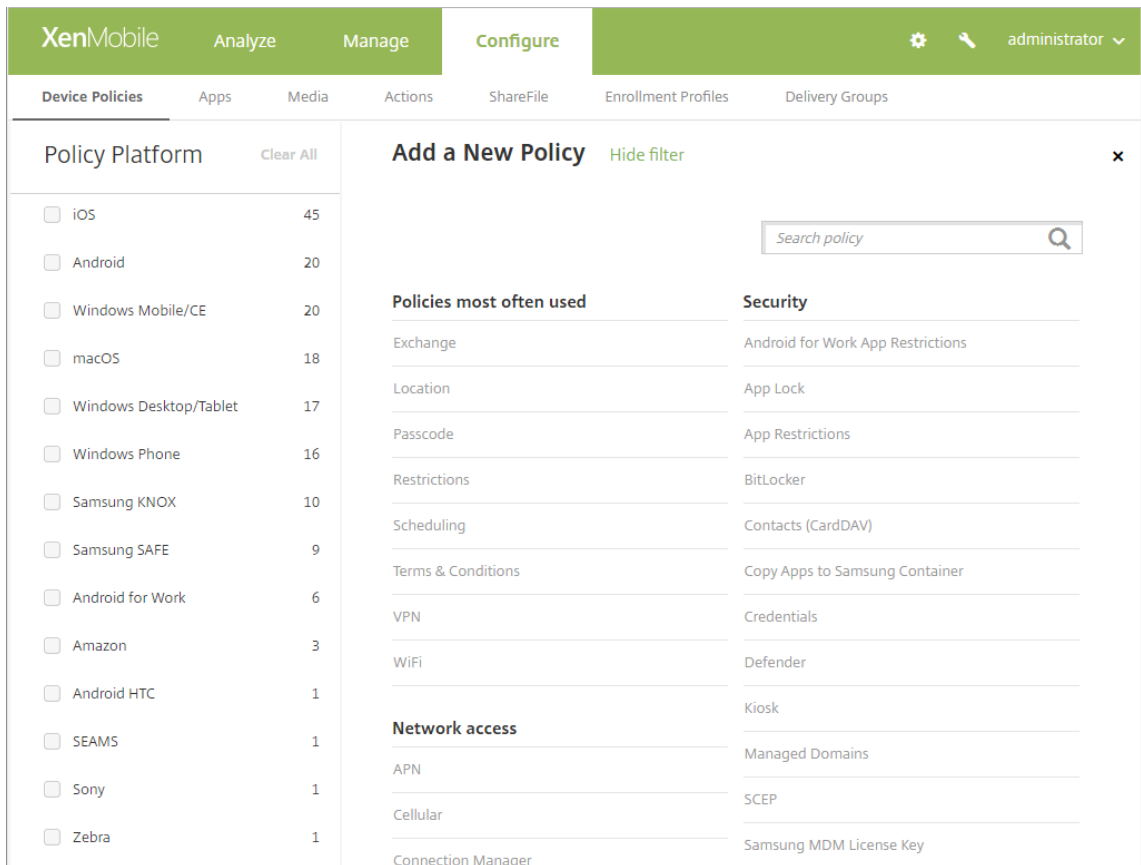
1. 정책의 이름을 지정하고 관련 설명을 입력합니다.
2. 하나 이상의 플랫폼에 대한 정책을 구성합니다.
3. 배포 규칙을 만듭니다 (선택 사항).
4. 배달 그룹에 정책을 할당합니다.
5. 배포 일정을 구성합니다 (선택 사항).

장치 정책을 만들고 관리하려면 구성 > 장치 정책으로 이동합니다.

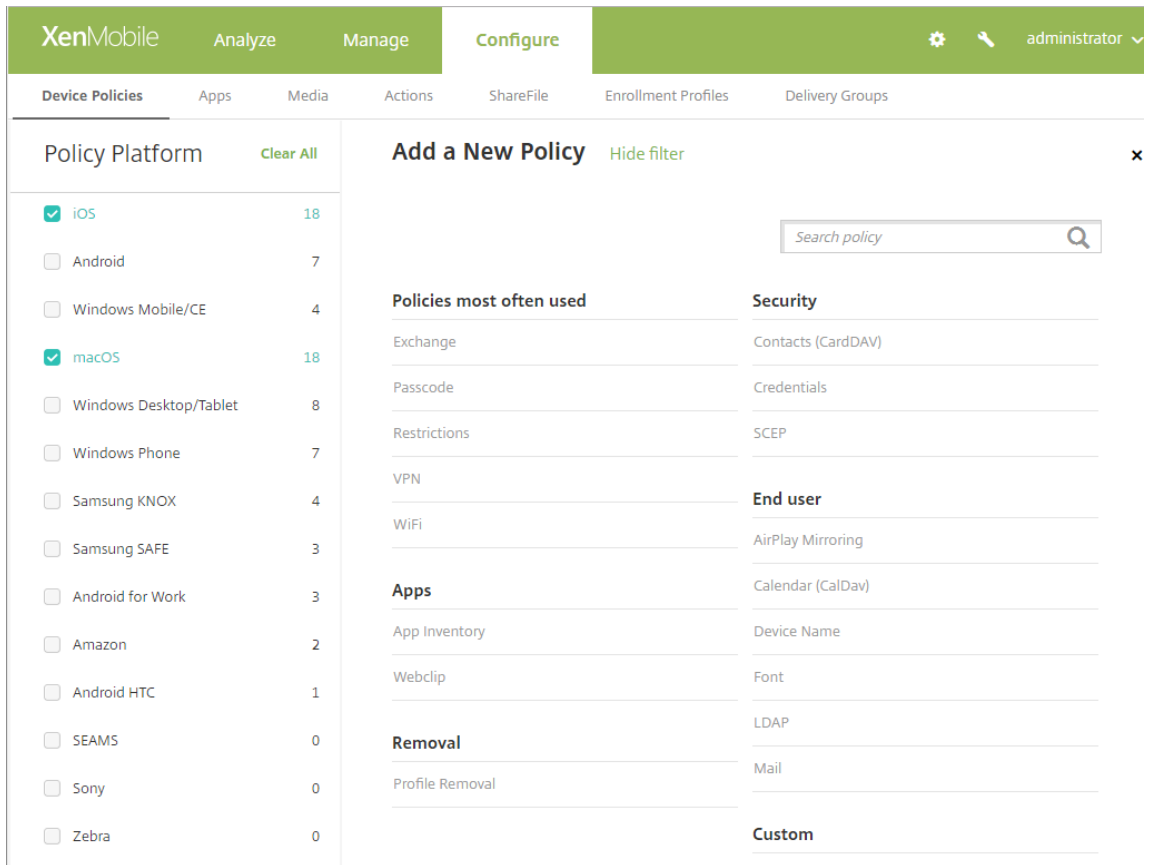


정책을추가하려면:

1. 장치정책페이지에서 추가를클릭합니다. 새정책추가페이지가나타납니다.



2. 하나이상의플랫폼을클릭하여선택한플랫폼에대한장치정책목록을봅니다. 정책추가를계속하려면정책이름을클릭합니다.



검색상자에 정책 이름을 입력할 수도 있습니다. 입력할 때 잠재적 검색 결과가 나타납니다. 목록에 해당 정책이 있으면 정책을 클릭합니다. 선택한 정책만 결과에 유지됩니다. 해당 정책을 클릭하여 정책에 대한 정책 정보 페이지를 엽니다.

3. 정책에 포함할 플랫폼을 선택합니다. 5 단계에서 선택한 플랫폼에 대한 구성 페이지가 나타납니다.
4. 정책 정보 페이지를 작성한 후 다음을 클릭합니다. 정책 정보 페이지에서는 정책을 식별하고 추적하는 데 도움이 되는 정책 이름과 같은 정보를 수집합니다. 이 페이지는 모든 정책에 대해 유사합니다.
5. 플랫폼 페이지를 작성합니다. 3 단계에서 선택한 각 플랫폼에 대해 플랫폼 페이지에 나타납니다. 이러한 페이지는 각 정책에 따라 다릅니다. 정책은 플랫폼마다 차이가 있을 수 있습니다. 모든 정책이 모든 플랫폼에 적용되는 것은 아닙니다.

일부 페이지에는 항목 표가 포함되어 있습니다. 기존의 항목을 삭제하려면 목록이 포함된 줄위로 마우스 포인터를 이동한 후 오른쪽의 휴지통 아이콘을 클릭합니다. 확인 대화 상자에서 삭제를 클릭합니다.

기존의 항목을 편집하려면 목록이 포함된 줄위로 마우스 포인터를 이동한 후 오른쪽의 펜 아이콘을 클릭합니다.

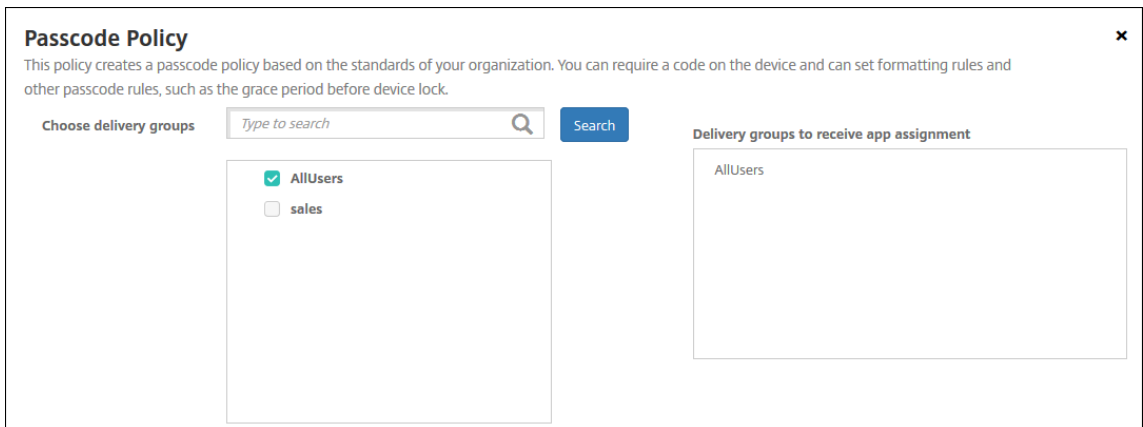
배포 규칙, 할당 및 일정을 구성하려면

배포 규칙을 구성하는 방법에 대한 자세한 내용은 [리소스 배포](#)를 참조하십시오.

1. 플랫폼 페이지에서 배포 규칙을 확장하고 다음 설정을 구성합니다. 기본적으로 기본 탭이 표시됩니다.
 - 목록에서 어떤 경우에 정책을 배포할지 지정하는 옵션을 클릭합니다. 모든 조건이 충족된 경우 또는 조건 중 하나라도 충족된 경우 정책을 배포하도록 선택할 수 있습니다. 기본 옵션은 모두입니다.

- 조건을정의하려면 새규칙을클릭합니다.
 - 목록에서 장치소유권및 **BYOD** 와같은조건을클릭합니다.
 - 조건을더추가하려면 새규칙을다시클릭합니다. 원하는만큼많은조건을추가할수있습니다.
2. 고급탭을클릭하여규칙을부울옵션과결합합니다. 기본탭에서선택한조건이표시됩니다.
 3. 추가고급부울논리를사용하여규칙을결합하거나, 편집하거나, 추가할수있습니다.
 - 그리고, 또는이나 아님을클릭합니다.
 - 목록에서규칙에추가할조건을선택합니다. 그런다음오른쪽의더하기기호 (+) 를클릭하여규칙에조건을추가합니다. 언젠든지조건을클릭하여선택한다음 편집을클릭하여조건을변경하거나 삭제를클릭하여조건을제거할수있습니다.
 - 새규칙을클릭하여다른조건을추가합니다.
 4. 다음을클릭하여다음플랫폼페이지로이동하거나, 모든플랫폼페이지가완료된경우 할당페이지로이동합니다.
 5. 할당페이지에서정책을적용할배달그룹을선택합니다. 배달그룹을클릭하면 앱할당을받을배달그룹상자에해당그룹이표시됩니다.

앱할당을받을배달그룹은배달그룹을선택하기전까지표시되지않습니다.

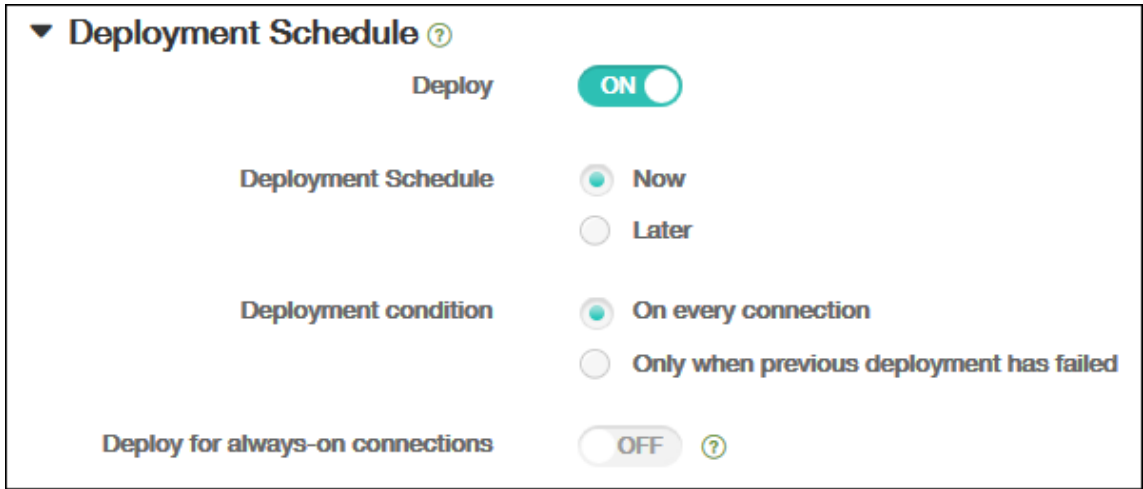


6. 할당페이지에서 배포일정을확장하고다음설정을구성합니다.
 - 배포옆에서 켜짐을클릭하여배포를예약하거나 꺼짐을클릭하여배포를차단합니다. 기본옵션은 켜짐입니다.
 - 배포일정옆에서 지금또는 나중에를클릭합니다. 기본옵션은 지금입니다.
 - 나중에를클릭하는경우달력아이콘을클릭하고배포날짜와시간을선택합니다.
 - 배포조건옆에서 모든연결에서를클릭하거나 이전배포가실패한경우에만을클릭합니다. 기본옵션은 모든연결에서입니다.
 - 상시연결에대해배포옆에서 켜짐또는 꺼짐을클릭합니다. 기본옵션은 꺼짐입니다.

참고:

설정 > 서버속성에서백그라운드배포예약키를구성한경우에만이옵션이적용됩니다. iOS 장치에는상시연결 옵션을사용할수없습니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 모든 플랫폼에 적용되지만 상시 연결에 대해 배포를 선택한 경우 iOS에는 적용되지 않습니다.

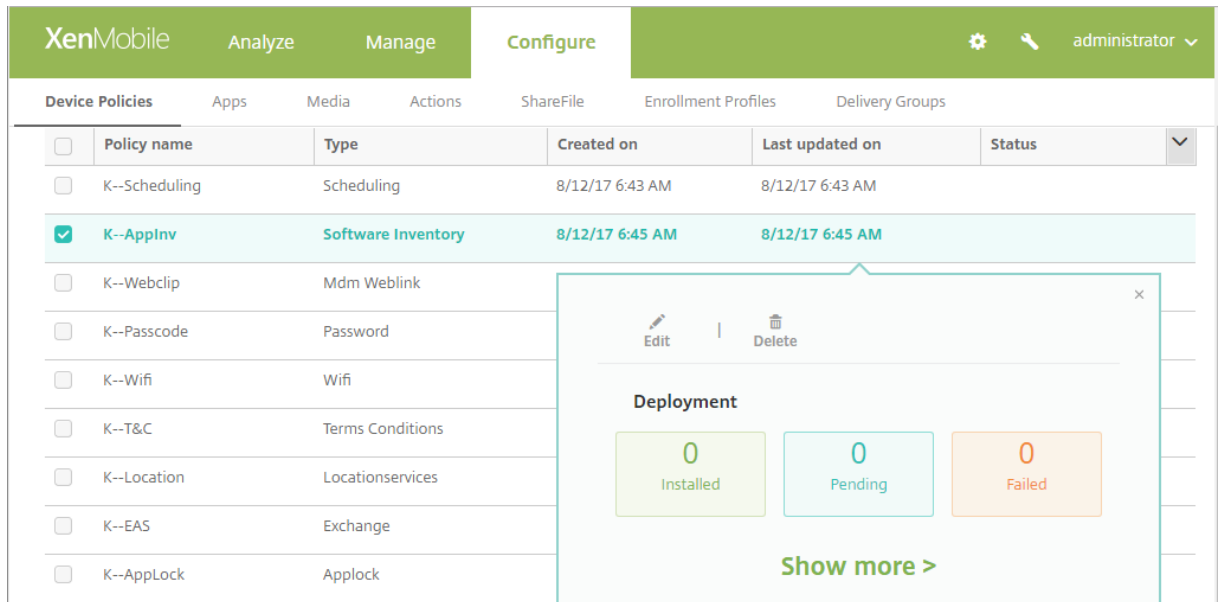


7. 저장을 클릭합니다.

장치 정책 테이블에 정책이 표시됩니다.

장치 정책 편집 또는 삭제

정책을 편집하거나 삭제하려면 정책 옆에 있는 확인란을 선택하여 정책 목록 위에 옵션 메뉴를 표시합니다. 또는 목록에서 정책을 클릭하여 목록 오른쪽에 옵션 메뉴를 표시합니다.



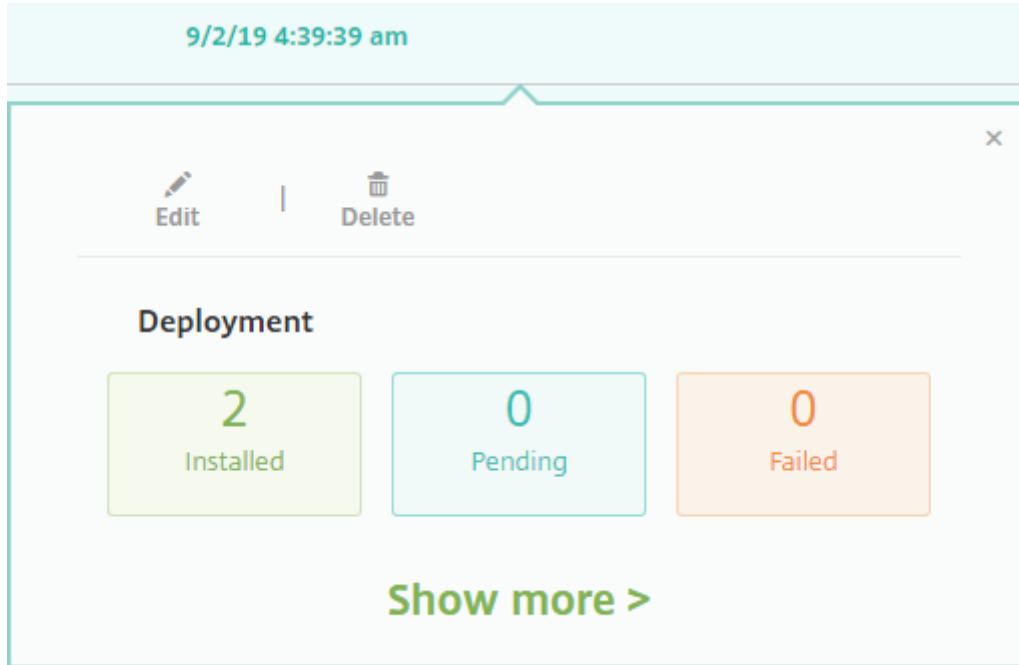
정책 세부 정보를 보려면 자세히 표시를 클릭합니다.

장치 정책에 대한 모든 설정을 편집하려면 편집을 클릭합니다.

삭제를 클릭하면 확인 대화상자가 나타납니다. 삭제를 다시 클릭합니다.

정책배포상태확인

구성 > 장치정책페이지에서정책행을클릭하여배포상태를확인합니다.



정책배포가보류중인경우사용자는 기본설정 > 장치정보 > 정책새로고침을눌러 Secure Hub 에서정책을새로고칠수있습니다.

장치에서장치정책제거

장치에서장치정책을제거하는단계는플랫폼에따라다릅니다.

- Android

Android 장치에서장치정책을제거하려면 XenMobile 제거장치정책을사용합니다. 자세한내용은 [XenMobile 제거장치정책](#)에서참조하십시오.

- iOS 및 macOS

iOS 또는 macOS 장치에서장치정책을제거하려면프로필제거장치정책을사용합니다. iOS 및 macOS 장치에서모든정책은 MDM 프로필의일부입니다. 따라서제거할정책에대해서만프로필제거장치정책을만들수있습니다. 나머지정책과프로필은장치에유지됩니다. 자세한내용은 [프로필제거장치정책](#)에서참조하십시오.

- Windows 10

Windows 10 데스크톱또는태블릿장치에서장치정책을직접제거할수는없습니다. 그러나다음방법중하나를사용할수있습니다.

- 장치의등록을취소한다음새정책집합을장치에푸시합니다. 그런다음사용자가재등록하여계속합니다.

- 보안작업을푸시하여특정장치를선택적으로초기화합니다. 이렇게하면장치에서모든회사앱및데이터가제거됩니다. 그러면해당장치만포함하는배달그룹에서장치정책을제거하고배달그룹을장치로푸시할수있습니다. 그런다음사용자가재등록하여계속합니다.

• Chrome OS

Chrome OS 장치에서장치정책을제거하려면해당장치만포함하는배달그룹에서장치정책을제거하면됩니다. 그런다음배달그룹을장치에푸시합니다.

추가된장치정책목록필터링

추가된정책목록을정책유형, 플랫폼및관련배달그룹으로필터링할수있습니다. 구성 > 장치정책페이지에서 필터표시를클릭합니다. 목록에서보려는항목의확인란을선택합니다.

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Device Policies', there are filter options for 'Policy Type' and 'Policy Platform'. The 'Policy Platform' filter is expanded, showing options for iOS (14), macOS (5), Android (13), Samsung KNOX (3), and Android for Work (1). Below the filters is a table of device policies.

Policy name	Type	Created on	Last updated on	Status
K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM	
K--Applnv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM	
K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM	
K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM	
K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM	
K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM	

필터를저장하려면 이보기저장을클릭합니다. 그러면해당필터이름이 이보기저장단추아래의단추에표시됩니다.

장치정책요약

장치정책이름	장치정책설명
AirPlay 미러링	특정 AirPlay 장치 (예: Apple TV 또는다른 Mac 컴퓨터)를 iOS 장치에추가합니다. 감독되는장치의화이트리스트에 장치를추가하는옵션도있습니다. 이옵션은사용자를화이트리스트의 AirPlay 장치로만제한합니다.

장치정책이름	장치정책설명
AirPrint	iOS 장치의 AirPrint 프린터목록에 AirPrint 프린터를 추가합니다. 이정책을사용하면프린터와장치가서로다른서브넷에있는환경을보다쉽게지원할수있습니다.
Android Enterprise 앱권한	작업프로필내의 Android Enterprise 앱에대한요청에서 Google 이 “위험한” 권한이라고하는권한을처리하는방법을구성합니다.
Android Enterprise 앱제한	Android 앱과관련된제한사항을업데이트합니다.
APN	특정전화이동통신사업자의 GPRS(General Packet Radio Service) 에장치를연결하는데사용되는설정을지정합니다. 이설정년대부분의최신휴대폰에이미정의되어있습니다. 조직이모바일장치에서인터넷에연결하는데소비자 APN 을사용하지않는경우이정책을사용합니다.
앱액세스	장치의필수앱, 선택적앱또는차단앱목록을정의합니다. 그런다음자동화된동작을만들어장치가앱목록을따르는데대응할수있습니다.
앱특성	iOS 장치에대한관리되는앱번들 ID 또는앱별 VPN 식별자와같은특성을지정합니다.
앱구성	관리되는구성을지원하는앱의다양한설정및동작을원격으로구성합니다. 이렇게하려면 iOS 장치에 XML 구성파일 (속성목록또는 plist) 을배포합니다. 또는 Windows 10 Phone, 데스크톱, 태블릿장치에키/값쌍을배포합니다.
앱인벤토리	관리되는장치에서앱의인벤토리를수집합니다. 그러면 XenMobile 이해당장치에배포된앱액세스정책과인벤토리를비교합니다. 이런방식으로앱액세스블랙리스트또는화이트리스트에있는앱을감지하고적절한조치를수행할수있습니다.
앱잠금	사용자가 iOS 또는특정 Android 장치에서실행할수있거나실행할수없는앱의목록을정의합니다.
앱네트워크사용	iOS 장치에서관리되는앱이셀룰러데이터네트워크와같은네트워크를사용하는방식을지정하는네트워크사용규칙을설정합니다. 이러한규칙은관리되는앱에만적용됩니다. 관리되는앱은 XenMobile 을통해사용자장치에배포되는앱입니다.
앱제한	사용자가 Samsung KNOX 장치에설치할수없도록방지할앱의블랙리스트를만듭니다. 또한사용자가설치할수있도록할앱의화이트리스트를만들수있습니다.
앱제거	사용자장치에서앱을제거합니다.

장치정책이름	장치정책설명
앱제거제한	사용자가제거할수있는앱과제거할수없는앱을지정합니다.
앱알림	iOS 사용자가지정된앱의알림을수신하는방법을제어합니다.
BitLocker	Windows 10 장치의 BitLocker 인터페이스에서사용할수있는설정을구성합니다.
브라우저	사용자장치가브라우저를사용할수있는지여부또는장치가사용할수있는브라우저기능을정의합니다.
일정 (CalDav)	iOS 또는 macOS 장치에일정 (CalDAV) 계정을추가합니다. CalDAV 계정을사용하면 CalDAV 를지원하는모든서버와일정데이터를동기화할수있습니다.
셀룰러	셀룰러네트워크설정을구성합니다.
연결관리자	인터넷및사설망에자동으로연결되는앱에대한연결설정을지정합니다. 이정책은 Windows Pocket PC 에서만사용할수있습니다.
연락처 (CardDAV)	iOS 또는 macOS 장치에 iOS 연락처 (CardDAV) 계정을추가합니다. CardDAV 계정을사용하면 CardDAV 를지원하는모든서버와연락처데이터를동기화할수있습니다.
OS 업데이트제어	감독되는지원장치에최신 OS 업데이트를배포합니다.
Samsung 컨테이너에앱복사	지원되는 Samsung 장치에서장치에이미설치된앱을 SEAMS 또는 KNOX 컨테이너로복사합니다. SEAMS 컨테이너에복사된앱은장치홈화면에서사용할수있습니다. KNOX 컨테이너에복사된앱은사용자가 KNOX 컨테이너에로그인하는경우에만사용할수있습니다.
자격증명	XenMobile 의 PKI 구성에대한통합된인증을수행할수있습니다. 예를들어 PKI 엔터티, 키저장소, 자격증명공급자또는서버인증서에대한인증이가능합니다.
사용자지정 XML	장치프로비전, 장치기능사용, 장치구성및장애편리같은기능을최적화합니다.
Defender	데스크톱과태블릿에설치된 Windows 10 의 Windows Defender 설정을구성합니다.
파일및폴더삭제	Windows Mobile/CE 장치에서특정파일또는폴더를삭제합니다.
레지스트리키및값삭제	Windows Mobile/CE 장치에서특정레지스트리키및값을삭제합니다.

장치정책이름	장치정책설명
장치상태증명	Windows 10 장치가해당상태를보고하도록합니다. 이를위해장치에서특정데이터및런타임정보를분석을위해 HAS(상태증명서비스) 로전송합니다. HAS 에서상태증명인증을생성하고반환하면장치가이를 XenMobile 에보냅니다. XenMobile 은상태증명인증을받은후인증서의내용에따라이전에구성된자동동작을배포할수있습니다.
장치이름	장치를식별할수있도록 iOS 와 macOS 장치에이름을설정합니다. 매크로, 텍스트또는둘의조합을사용하여장치이름을정의할수있습니다.
교육구성	Apple 교육을사용할강사및학생장치를구성합니다. 강사가 Classroom 앱을사용하는경우교육구성장치정책이필요합니다.
엔터프라이즈허브	Enterprise Hub Company 스토어를통해 Windows Phone 에앱을배포합니다. XenMobile 은 Windows Phone Secure Hub 모드마다엔터프라이즈허브정책을하나만지원합니다. 예를들어, XenMobile Enterprise Edition 의다양한 Secure Home 버전을사용하여여러 Enterprise Hub 정책을만들지마십시오. 초기엔터프라이즈허브정책은장치를등록하는동안에만배포할수있습니다.
Exchange	장치의기본전자메일클라이언트에서 ActiveSync 전자메일을사용하도록설정합니다.
파일	사용자에대한특정기능을수행하는스크립트파일을 XenMobile 에추가합니다. 또는 Android 장치사용자가장치에서액세스할수있는문서파일을추가할수있습니다. 파일을추가하는경우장치에서파일이저장될디렉터리를지정할수도있습니다.
FileVault	이정책을사용하면등록된 macOS 장치에서 FileVault 장치암호화를사용하도록설정할수있습니다. 사용자가로그인할때 FileVault 설정을건너뛸수있는횟수를제어할수있습니다. macOS 10.7 이상에서사용할수있습니다.
방화벽	방화벽설정을구성합니다. 장치에서허용하거나차단할 IP 주소, 포트및호스트이름을지정합니다. 또한프록시및프록시경로조정설정을구성할수있습니다.

장치정책이름	장치정책설명
글꼴	iOS 와 macOS 장치에추가글꼴을추가합니다. 글꼴은트루타입 (.TTF) 또는오픈타입 (.OFT) 형식이어야합니다. XenMobile 은글꼴모음 (.TTC 또는.OTC) 을지원하지않습니다.
홈화면레이아웃	iOS 9.3 이상의감독되는장치에서 iOS 홈화면의앱및폴더레이아웃을지정합니다.
iOS 및 macOS 프로필가져오기	XenMobile 로 iOS 와 macOS 장치를위한장치구성 XML 파일을가져옵니다. 이파일에는 Apple Configurator 로작성한장치보안정책및제한사항이포함되어있습니다.
키오스크	Samsung SAFE 장치에서앱사용을제한합니다. 사용가능한앱을하나이상의특정앱으로제한할수있습니다. 이정책은특정유형또는클래스의앱만실행하도록마련된회사장치에유용합니다. 또한이정책을사용하면키오스크모드의장치홈화면및잠금화면배경에대한사용자지정이미지를선택할수있습니다.
Launcher 구성	허용되는앱및 Launcher 아이콘의사용자지정로고이미지 등 Android 장치의 Citrix Launcher 에대한설정을지정합니다.
LDAP	LDAP 서버호스트이름등필요한모든계정정보를비롯하여 iOS 장치에사용할 LDAP 서버에대한정보를제공합니다. 또한 LDAP 서버를쿼리할때사용할 LDAP 검색정책집합을제공합니다.
위치	장치에 Secure Hub 에대한 GPS 가설정된경우지도에서 장치의위치를찾을수있습니다. 장치에이정책을배포한후 XenMobile Server 에서찾기명령을보낼수있습니다. 그러면장치가해당위치좌표를사용하여응답합니다. 또한 XenMobile 은지오편스및추적정책을지원합니다.
메일	iOS 또는 macOS 장치에대한전자메일계정을구성합니다.
관리되는도메인	전자메일및 Safari 브라우저에적용되는관리되는도메인을 정의합니다. 관리되는도메인을사용하면 Safari 를사용하여도메인에서다운로드한문서를열수있는앱을제어함으로써회사데이터를보호할수있습니다. iOS 8 이상의감독되는장치 의경우 URL 또는하위도메인을지정하여사용자가브라우저에서문서, 첨부파일및다운로드를열수있는방법을제어할수있습니다.

장치정책이름	장치정책설명
MDM 옵션	감독되는 iOS 7.0 이상의전화장치에서내전화찾기및 iPad 활성화잠금을관리합니다.
조직정보	XenMobile 이 iOS 장치에배포하는알림메시지에대한조직 정보를지정합니다.
암호	관리되는장치에 PIN 코드또는암호를적용합니다. 장치서암호복잡성과시간초과를설정할수있습니다.
개인핫스팟	사용자가 WiFi 네트워크범위내에없는경우인터넷에연결할수있습니다. 사용자는개인핫스팟기능을사용하여 iOS 장치에서셀룰러데이터연결을통해연결합니다.
프로필제거	사용자의 iOS 또는 macOS 장치에서앱프로필을제거합니다.
프로비전프로필	장치에보낼엔터프라이즈배포프로비전프로필을지정합니다. iOS 엔터프라이즈앱을개발하고코드서명하는경우일반적으로프로비전프로필을포함합니다. Apple iOS 장치에서앱을실행하려면이프로필이필요합니다. 프로비전프로필이누락되었거나만료된경우사용자가앱을눌러서열때앱의작동이중단됩니다.
프로비전프로필제거	iOS 프로비전프로필을제거합니다.
프록시	Windows Mobile/CE 및 iOS 를실행하는장치에대한글로벌 HTTP 프록시설정을지정합니다. 장치당하나의글로벌 HTTP 프록시정책만배포할수있습니다.
레지스트리	Windows Mobile/CE 장치를관리할수있도록레지스트리키및값을정의합니다. Windows Mobile/CE 레지스트리에는앱, 드라이버, 사용자기본설정및구성설정에대한데이터가저장됩니다.
원격지원	Samsung KNOX 장치에원격으로액세스할수있습니다. 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.
제한사항	관리되는장치의기능을잠그고제어하기위한수백개의옵션을제공합니다. 제한옵션의예로는카메라또는마이크를사용하지않도록설정, 로밍규칙적용, 앱스토어를비롯한타사서비스에대한액세스적용등이있습니다.

장치정책이름	장치정책설명
로밍	iOS 및 Windows Mobile/CE 장치에서음성및데이터로 밍을허용할것인지여부를구성합니다. 음성로밍을사용하지않 도록설정하면데이터로밍이자동으로비활성화됩니다.
Samsung MDM 라이선스키	SAFE 정책및제한사항을배포하기전에장치에배포해야하는 기본제공 Samsung ELM(엔터프라이즈라이선스관리) 키 를지정합니다. XenMobile 은 Samsung E-FOTA(Enterprise Firmware-Over-The-Air) 서비 스도지원합니다. XenMobile 은 SAFE(Samsung for Enterprise) 와 Samsung KNOX 정책을모두지원하고 확장합니다.
예약	MDM 관리, 앱주시및정책배포를위해 Android 및 Windows Mobile 장치에서 XenMobile Server 에다 시연결하는데필요합니다. 이정책을장치에보내지않고 Google FCM 을사용하도록설정하지않을경우장치에서서 버에다시연결할수없습니다.
SCEP	외부 SCEP 서버에서인증서를검색하도록 iOS 및 macOS 장치를구성합니다. 또한 XenMobile 에연결되어있는 PKI 의 SCEP 를사용하여장치에인증서를제공할수있습니다. 이 를위해분산모드에서 PKI 엔터티와 PKI 공급자를만듭니다.
SSO 계정	사용자가 XenMobile 과회사내부리소스에액세스하기위해 한번만로그온하도록 SSO(Single Sign-On) 계정을만들 니다. 사용자가장치에자격증명을저장할필요가없습니다. XenMobile 은 App Store 의앱을포함한앱전반의 SSO 계정에엔터프라이즈사용자자격증명을사용합니다. 이정책은 Kerberos 인증과호환됩니다. iOS 에서사용할수있습니다.
스토리지암호화	내부및외부스토리지를암호화합니다. 일부장치의경우이정책 으로인해사용자가해당장치에서스토리카드를사용하지못 하게됩니다.
구독중인일정	iOS 장치의캘린더목록에구독일정을추가합니다. 사용자장 치의구독일정목록에추가하기전에일정을구독해야합니다.
약관	사용자가회사네트워크에대한연결을제어하는특정회사정책 에동의하도록요구합니다. 사용자가 XenMobile 에장치를 등록할때약관에동의해야만장치를등록할수있습니다. 약관에 동의하지않으면등록프로세스가취소됩니다.

장치정책이름	장치정책설명
터널	원격지원에만사용됩니다. 원격지원을사용하면지원센터담당자가관리되는 Windows CE 및 Android 모바일장치를원격으로제어할수있습니다. 원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다. 2019년 1월 1일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix는개선사항이나수정사항을제공하지않습니다.
VPN	레거시 VPN 게이트웨이기술을사용하는백엔드시스템에대한액세스를제공합니다. 이정책은장치에배포할수있는 VPN 게이트웨이연결세부정보를제공합니다. XenMobile은 Cisco AnyConnect, Juniper, Citrix VPN을비롯한여러 VPN 공급자를지원합니다. VPN 게이트웨이가이 옵션을지원하는경우이정책을 CA에연결하고주문형 VPN을사용하도록설정할수있습니다.
배경화면	iOS 장치잠금화면, 홈화면또는돌다에배경화면을설정하기 위해.png 또는.jpg 파일을추가합니다. iPad 및 iPhone에서서로다른배경화면을사용하려면서로다른배경화면정책을만들어해당사용자에게배포합니다.
웹콘텐츠필터	iOS 장치에서웹콘텐츠를필터링합니다. XenMobile은 Apple 자동필터기능과화이트리스트및블랙리스트에추가된 사이트를사용합니다. 감독되는 iOS 장치에서만사용할수있습니다.
웹클리프	웹사이트에대한바로가기또는웹클리프를배치하여앱과나란히 사용자장치에표시합니다. iOS, macOS X 및 Android 장치의웹클리프를나타내는사용자지정아이콘을지정할수있습니다. Windows 태블릿에는레이블과 URL만필요합니다.
WiFi	관리자가관리되는장치에 WiFi 라우터세부정보를배포할수있습니다. 라우터세부정보에는 SSID, 인증데이터및구성데이터가포함됩니다.
Windows CE 인증서	외부 PKI에서 Windows Mobile/CE 인증서를만들어사용자장치에제공합니다.
Windows Information Protection	정책에대해설정된적용수준에서 Windows Information Protection이필요한앱을지정합니다. Windows 10 버전 1607 이상의감독되는장치용정책입니다.
XenMobile Store	XenMobile Store 웹클리프를사용자장치의홈화면에표시할지여부를지정합니다.

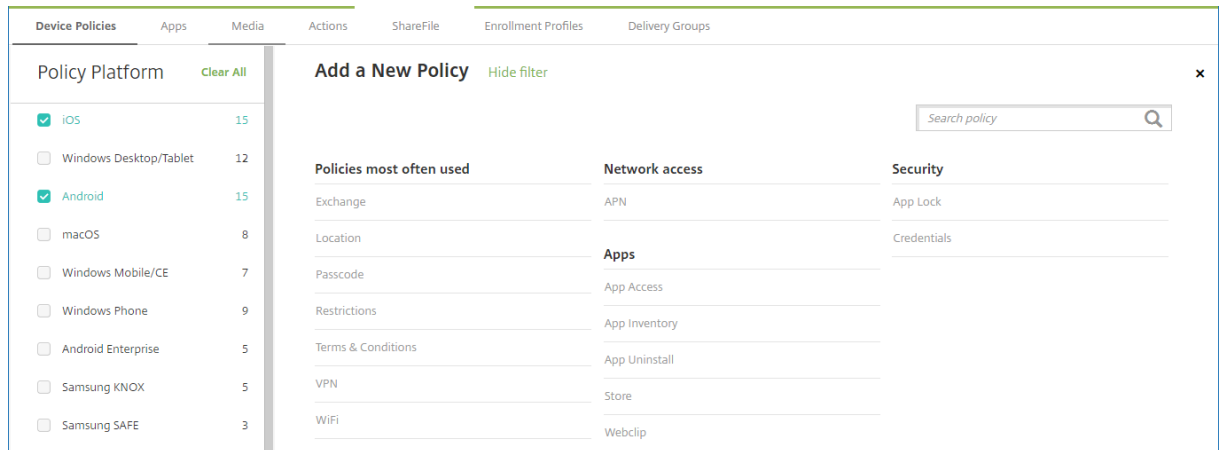
장치정책이름	장치정책설명
XenMobile 옵션	Android 및 Windows Mobile/CE 장치에서 XenMobile 에 연결할 때 Secure Hub 동작을 구성합니다.
XenMobile 제거	Android 및 Windows Mobile/CE 장치에서 XenMobile 을 제거합니다. 이 정책을 배포하면 배포 그룹에 있는 모든 장치에서 XenMobile 이 제거됩니다.

플랫폼별장치정책

January 6, 2020

플랫폼별로 사용 가능한 정책을 보려면:

1. XenMobile 콘솔에서 구성 > 장치정책으로 이동합니다.
2. 추가를 클릭합니다.
3. 정책 플랫폼 창의 목록에 각 장치 플랫폼이 나타납니다. 해당 창이 열리지 않으면 필터 표시를 클릭합니다.
4. 단일 플랫폼에서 사용할 수 있는 모든 정책 목록을 보려면 해당 플랫폼을 선택합니다. 여러 플랫폼에서 사용할 수 있는 정책 목록을 보려면 각 플랫폼을 선택합니다. 정책은 선택한 각 플랫폼에 적용되는 경우에만 목록에 나타납니다.



XenMobile 의 최신 릴리스는 다음과 같은 플랫폼에 대한 장치 정책을 지원합니다.

- Amazon
- Android
- Android HTC
- Android Sony
- Android TouchDown
- Android Enterprise
- Android Zebra

- Chrome OS
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Samsung SEAMS
- Windows 10 데스크톱/태블릿
- Windows 10 Phone
- Windows Mobile/CE

XenMobile 의최신릴리스에서지원되는장치에대한자세한내용은 [지원되는장치플랫폼](#)을참조하십시오.

참고:

환경에 GPO(그룹정책개체) 가구성되어있는경우:

Windows 10 용 XenMobile 장치정책을구성할때다음규칙을고려하십시오. 하나이상의등록된 Windows 10 장치에 서정책이충돌하는경우 GPO 와일치하는정책이우선합니다.

AirPlay 미러링장치정책

January 6, 2020

Apple AirPlay 기능을사용하면 iOS 장치의콘텐츠를 Apple TV 를통해 TV 화면에무선으로스트리밍하거나장치디스플레이에 표시되는내용을 TV 화면또는 Mac 컴퓨터에정확히미러링할수있습니다.

XenMobile 에서특정 AirPlay 장치 (예: Apple TV 또는다른 Mac 컴퓨터) 를 iOS 장치에추가하는장치정책을추가할수있습니다. 또한감독되는장치의경우화이트리스트에장치를추가할수있습니다. 그러면화이트리스트에있는 AirPlay 장치로만사용자가 제한됩니다. 장치를감독모드로전환하는방법에대한자세한내용은 [Apple Configurator 를사용하여 iOS 장치를감독모드로전환](#)을참조하십시오.

참고:

계속하기전에추가할모든장치에대한장치 ID 와암호가있는지확인하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

The screenshot shows the XenMobile configuration interface for an AirPlay Mirroring Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows the 'AirPlay Mirroring Policy' configuration steps: 1 Policy Info, 2 Platforms, 3 Assignment. The 'Platforms' section has checkboxes for 'iOS' and 'macOS', both of which are checked. The main configuration area is titled 'AirPlay Mirroring Policy' and includes a description: 'This policy lets you specify specific AirPlay devices to add to users' iOS and macOS devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.' Below the description are three main sections: 'AirPlay Password' with 'Device Name' and 'Password' input fields and an 'Add' button; 'Whitelist ID' with a 'Device ID' input field and an 'Add' button; and 'Policy Settings' with radio buttons for 'Remove policy' (selected 'Select date') and 'Duration until removal (in hours)', and a dropdown for 'Allow user to remove policy' set to 'Always'.

- **AirPlay 암호:** 추가할각장치에대해 추가를클릭하고다음을수행합니다.
 - 장치 **ID:** 하드웨어주소 (Mac 주소) 를 xx:xx:xx:xx:xx:xx 형식으로입력합니다. 이필드는대/소문자를구분하지 않습니다.
 - 암호: 장치에대한선택적암호를입력합니다.
 - 추가를클릭하여장치를추가하거나 취소를클릭하여장치추가를취소합니다.
- 화이트리스트 **ID:** 감독되지않는장치의경우이목록이무시됩니다. 이목록의장치 ID 는사용자장치에제공되는유일한 AirPlay 장치입니다. 목록에추가할각 AirPlay 장치에대해 추가를클릭하고다음을수행합니다.
 - 장치 **ID:** 장치 ID 를 xx:xx:xx:xx:xx:xx 형식으로입력합니다. 이필드는대/소문자를구분하지않습니다.
 - 추가를클릭하여장치를추가하거나 취소를클릭하여장치추가를취소합니다.

macOS 설정

The screenshot shows the 'AirPlay Mirroring Policy' configuration page in XenMobile. The left sidebar has three sections: '1 Policy Info', '2 Platforms' (with 'iOS' and 'macOS' checkboxes, 'macOS' is checked), and '3 Assignment'. The main area is titled 'AirPlay Mirroring Policy' and includes a description: 'This policy lets you specify specific AirPlay devices to add to users' iOS and macOS devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.' Below this are three sections: 'AirPlay Password' with 'Device Name' and 'Password' fields and an 'Add' button; 'Whitelist ID' with a 'Device ID' field and an 'Add' button; and 'Policy Settings' with radio buttons for 'Remove policy' (selected 'Select date', 'Duration until removal (in hours)' is unselected), a dropdown for 'Allow user to remove policy' (set to 'Always'), and a dropdown for 'Profile scope' (set to 'User') with 'macOS 10.7+' displayed next to it.

- **AirPlay 암호:** 추가할각장치에대해 추가를클릭하고다음을수행합니다.
 - 장치 ID: 하드웨어주소 (Mac 주소) 를 xx:xx:xx:xx:xx:xx 형식으로입력합니다. 이필드는대/소문자를구분하지 않습니다.
 - 암호: 장치에대한선택적암호를입력합니다.
 - 추가를클릭하여장치를추가하거나 취소를클릭하여장치추가를취소합니다.
- **화이트리스트 ID:** 감독되지않는장치의경우이목록이무시됩니다. 이목록의장치 ID 는사용자장치에제공되는유일한 AirPlay 장치입니다. 목록에추가할각 AirPlay 장치에대해 추가를클릭하고다음을수행합니다.
 - 장치 ID: 장치 ID 를 xx:xx:xx:xx:xx:xx 형식으로입력합니다. 이필드는대/소문자를구분하지않습니다.
 - 추가를클릭하여장치를추가하거나 취소를클릭하여장치추가를취소합니다.

AirPrint 장치정책

January 6, 2020

XenMobile 에서장치정책을추가하여 AirPrint 프린터를 iOS 장치에있는 AirPrint 프린터목록에추가할수있습니다. 이정책을사용하면프린터와장치가서로다른서브넷에있는환경을보다쉽게지원할수있습니다.

이정책은 iOS 7.0 이상에적용됩니다.

참고:

각프린터의 IP 주소와리소스경로를알고있는지확인하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

- **AirPrint 대상:** 추가하려는 각 AirPrint 대상에 대해 추가를 클릭한 후 다음을 수행합니다.
 - **IP 주소:** AirPrint 프린터 IP 주소를 입력합니다.
 - **리소스 경로:** 프린터와 연결된 리소스 경로를 입력합니다. 이 값은 _ipps.tcp Bonjour 레코드의 매개변수에 해당합니다. 예를 들어 printers/Canon_MG5300_series 또는 printers/Xerox_Phaser_7600 과 같습니다.
 - 저장을 클릭하여 프린터를 추가하거나 취소를 클릭하여 프린터 추가를 취소합니다.

Android Enterprise 관리되는 구성 정책

January 6, 2020

Android Enterprise 관리되는 구성 장치 정책은 다양한 앱 구성 옵션과 앱 제한을 제어합니다. 앱 개발자는 앱에서 사용할 수 있는 옵션과 도구 설명을 정의합니다. 도구 설명에 “템플릿값” 사용이 언급되는 경우 해당하는 XenMobile 매크로를 대신 사용합니다. 자세한 내용은 [원격 구성 개요](#) (Android 개발자 사이트) 및 [매크로](#) 를 참조하십시오.

앱 구성 설정에는 다음과 같은 항목이 포함될 수 있습니다.

- 앱 전자 메일 설정
- 웹 브라우저의 화이트리스트 또는 블랙리스트 URL
- 셀룰러 연결을 통해 또는 Wi-Fi 연결을 통해서만 앱 콘텐츠 동기화를 제어하는 옵션

앱에 대해 표시되는 설정에 대한 자세한 내용은 앱 개발자에게 문의하십시오.

사전 요구 사항

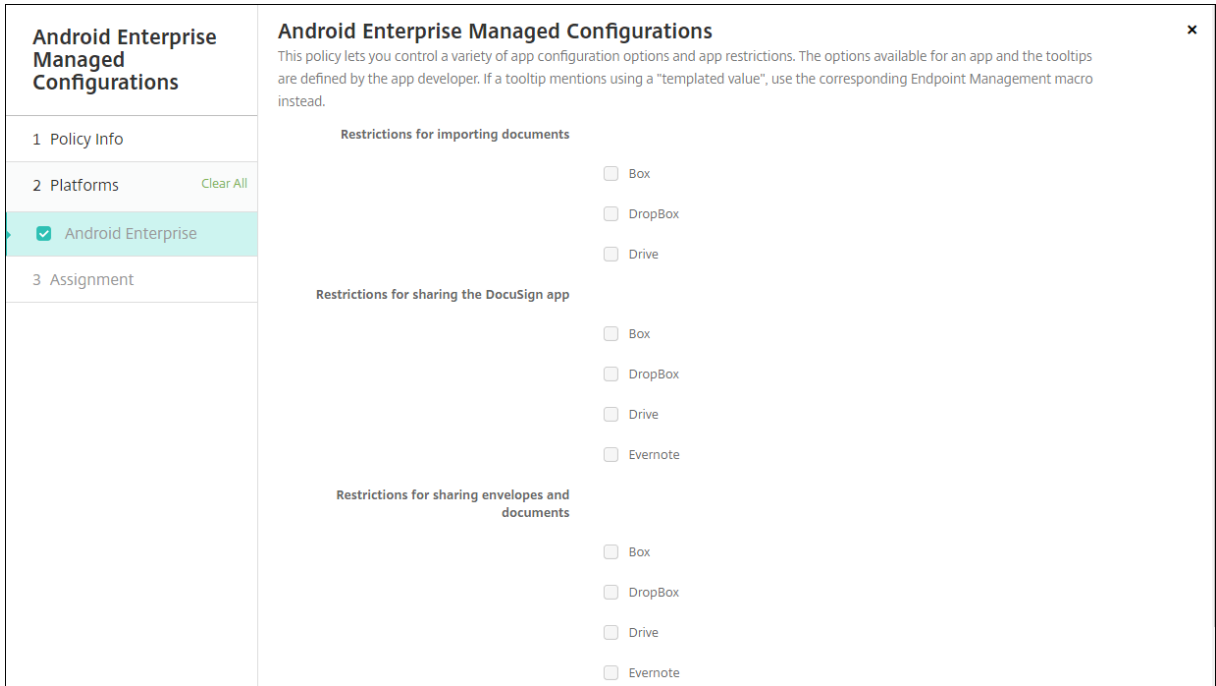
- Google 에서 Android Enterprise 설정 작업을 완료하고 Android Enterprise 를 관리되는 Google Play 에 연결합니다. 자세한 내용은 [Android Enterprise](#) 에서 참조하십시오.
- XenMobile 에 Android Enterprise 앱을 추가합니다. 자세한 내용은 [XenMobile 에 앱 추가](#) 에서 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책 으로 이동합니다. 자세한 내용은 [장치 정책](#) 에서 참조하십시오.

Android Enterprise 설정

Android Enterprise 관리되는 구성 장치 정책을 추가하도록 선택하면 앱을 선택하라는 메시지가 나타납니다. XenMobile 에 추가된 Android Enterprise 앱이 없는 경우 계속 진행할 수 없습니다.

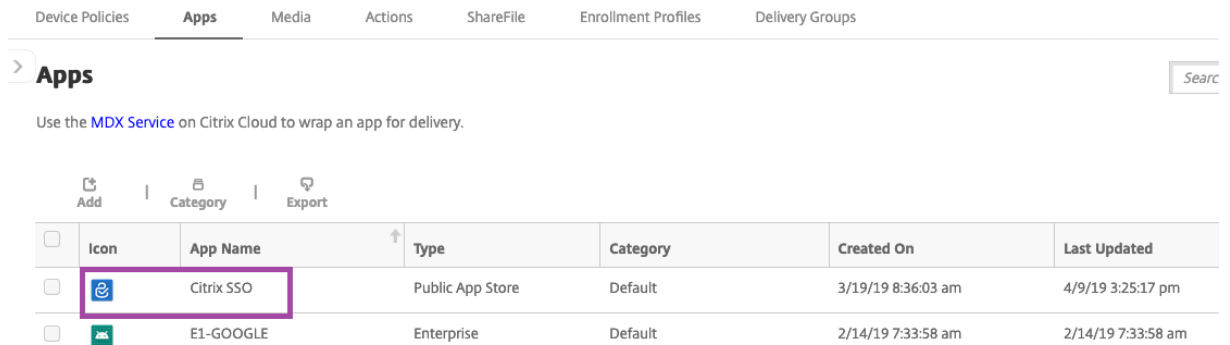
앱을 선택한 후 정책 설정을 구성합니다. 설정은 각 앱마다 다릅니다.



Android Enterprise 에대한 VPN 프로필구성

Citrix SSO 앱과 Android Enterprise 관리되는구성장치정책을 사용하여 Android Enterprise 장치에서사용할수있는 VPN 프로필을제공합니다.

먼저 Citrix SSO 를 Google Play Store 앱으로 XenMobile 콘솔에추가합니다. [공용앱스토어앱추기](#)를참조하십시오.



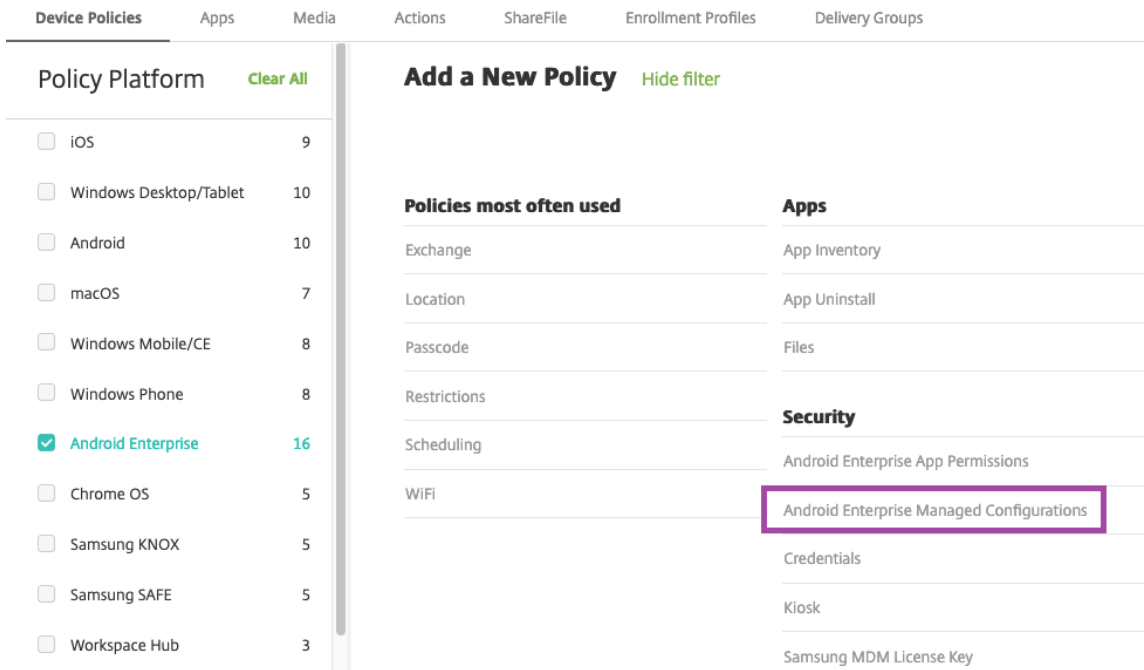
Citrix SSO 에대한 Android Enterprise 관리되는구성만들기

Citrix SSO 에대한 Android Enterprise 관리되는구성장치정책을구성하여 VPN 프로필을만듭니다. 만든 VPN 프로필에는 Citrix SSO 앱이설치되고정책이배포된장치에서액세스할수있습니다.

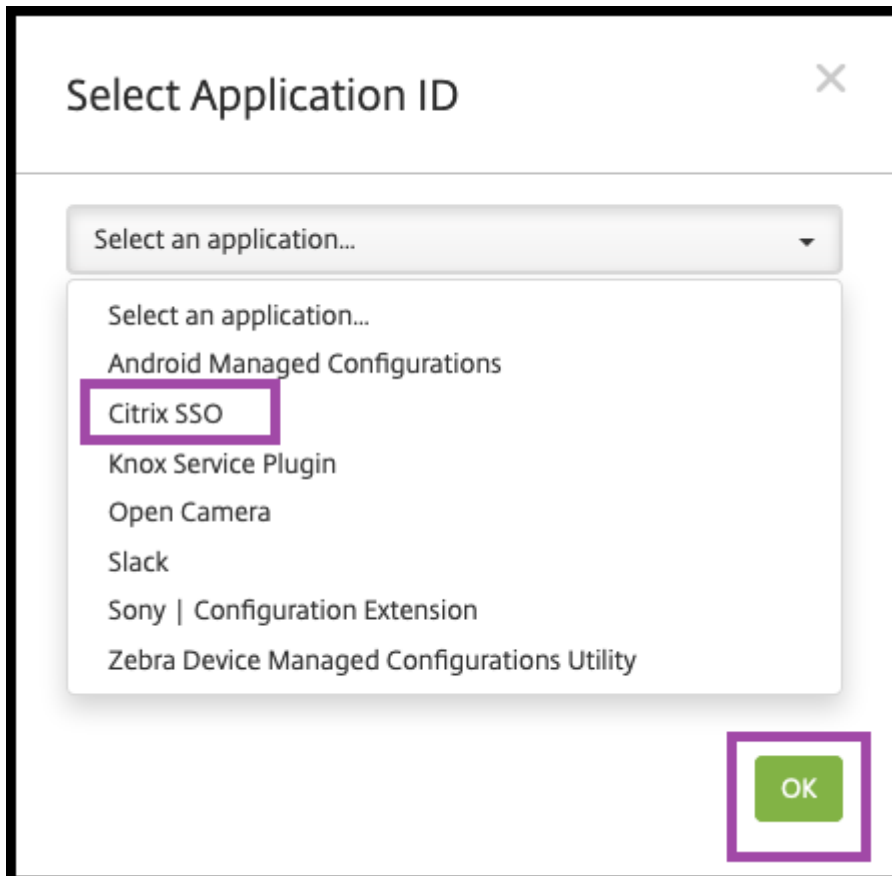
Citrix Gateway FQDN 및포트가필요합니다.

1. XenMobile 콘솔에서 구성 > 장치정책을클릭합니다. 추가를클릭합니다.

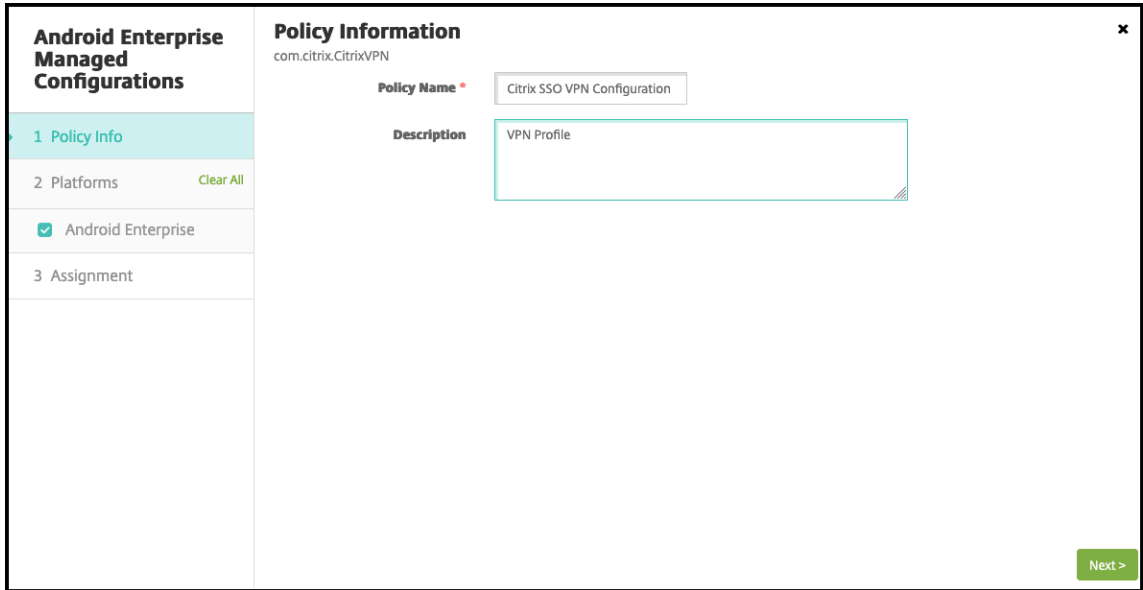
2. **Android Enterprise** 를선택합니다. **Android Enterprise** 관리되는구성을클릭합니다.



3. 응용프로그램 ID 선택창이나타나면목록에서 **Citrix SSO** 를선택하고 확인을클릭합니다.



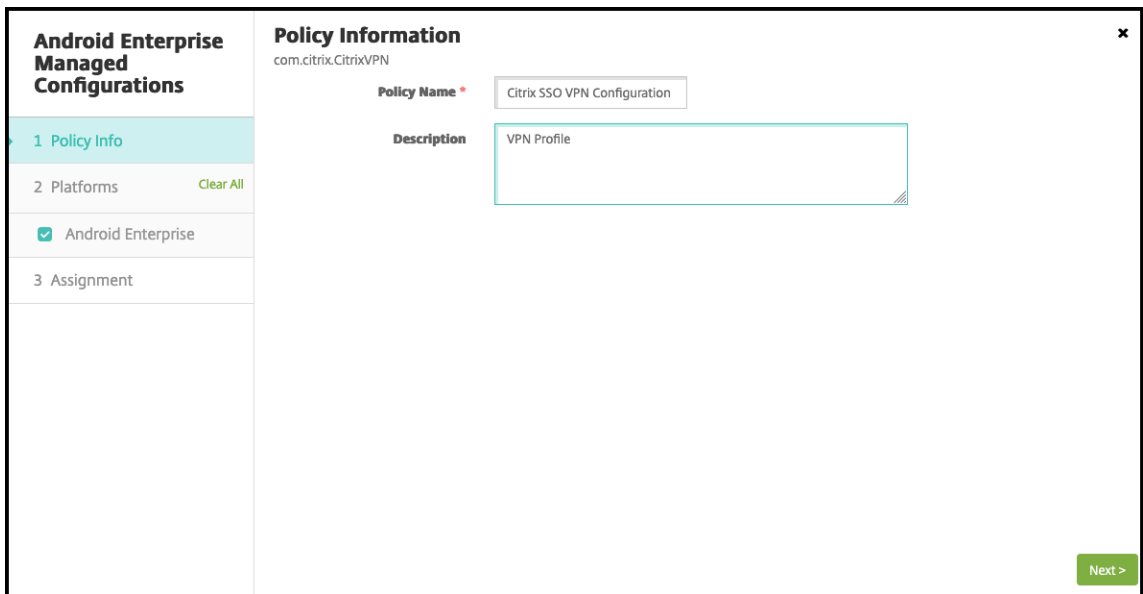
4. Citrix SSO VPN 구성에대한이름과설명을입력합니다. 다음을클릭합니다.



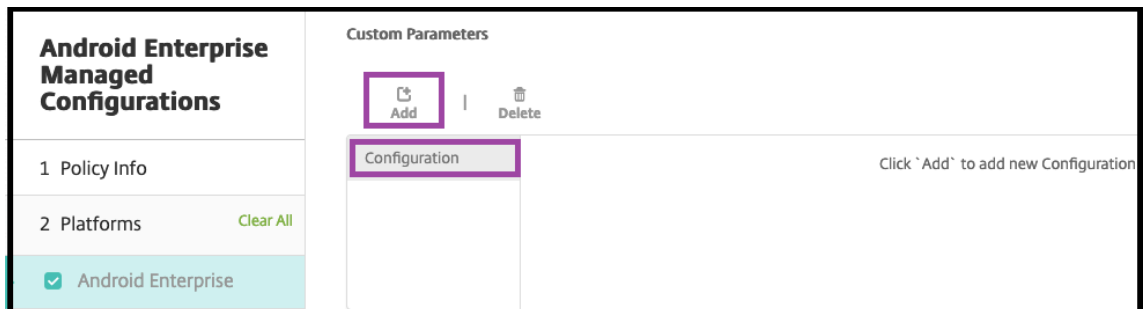
5. VPN 프로필매개변수를구성합니다.

- **VPN** 프로필이름. VPN 프로필이름을입력합니다. 둘이상의 VPN 프로필을만드는경우각각에대해고유한이름을사용합니다. 이름을제공하지않으면 서버주소필드에입력한주소가 VPN 프로필이름으로사용됩니다.
- 서버주소 (*). Citrix Gateway FQDN 을입력합니다. Citrix Gateway 포트가 443 이아닌경우해당포트를입력합니다. URL 형식을사용합니다. 예:https://gateway.mycompany.com:8443.
- 사용자이름 (선택사항). 최종사용자가 Citrix Gateway 에인증할때사용하는사용자이름을제공합니다. 이필드에 XenMobile 매크로 {user.username} 을사용할수있습니다. 매크로를참조하십시오. 사용자이름을제공하지 않으면사용자가 Citrix Gateway 에연결할때사용자이름을제공하라는메시지가표시됩니다.
- 암호 (선택사항). 최종사용자가 Citrix Gateway 에인증할때사용하는암호를제공합니다. 암호를제공하지 않으면 사용자 Citrix Gateway 에연결할때암호를제공하라는메시지가표시됩니다.
- 인증서별칭 (선택사항). 클라이언트인증서인증에사용할 Android 키저장소의인증서별칭을제공합니다. 인증서 기반인증을사용하는경우이인증서는사용자에대해미리선택됩니다.
- 앱별 VPN 유형 (선택사항). 앱별 VPN 을사용하여이 VPN 을사용하는앱을제한하는경우이설정을구성할수있습니다. 허용을선택하면 **PerAppVPN** 앱목록에나열된앱패키지이름에대한네트워크트래픽이 VPN 을통해라우팅됩니다. 다른모든앱의네트워크트래픽은 VPN 외부에서라우팅됩니다. 허용안함을선택하면 **PerAppVPN** 앱목록에나열된앱패키지이름에대한네트워크트래픽이 VPN 외부에서라우팅됩니다. 다른모든앱의네트워크트래픽은 VPN 을통해라우팅됩니다. 기본값은 허용입니다.
- **PerAppVPN** 앱목록. 앱별 VPN 유형의값에따라 VPN 에서트래픽이허용되거나허용하지않는앱의목록입니다. 심표또는세미콜론으로구분하여앱패키지이름을나열합니다. 앱패키지이름은대소문자를구분하며이목록에나타나는이름은 Google Play Store 에나타나는것과정확히일치해야합니다. 이목록은선택사항입니다. 장치전체 VPN 을프로비전하려면이목록을비워두십시오.

- 기본 **VPN** 프로필. 사용자가 특정 프로필을 누르지 않고 Citrix SSO 앱의 사용자 인터페이스에서 연결 스위치를 누를 때 사용할 VPN 프로필의 이름을 입력합니다. 이 필드를 비워두면 기본 프로필이 연결에 사용됩니다. 하나의 프로필만 구성된 경우 기본 프로필로 표시됩니다. 항상 VPN 연결의 경우 항상 VPN 연결을 설정하는데 사용할 VPN 프로필의 이름으로 이 필드를 설정해야 합니다.
- 사용자 프로필 사용 안 함. 이 설정이 꺼짐인 경우 사용자는 장치에서 자체 VPN 을 만들 수 없습니다. 이 설정이 꺼짐인 경우 사용자는 장치에서 자체 VPN 을 만들 수 있습니다. 기본값은 꺼짐입니다.
- 신뢰할 수 없는 서버 차단. Citrix Gateway 에 대해 자체 서명된 인증서를 사용하는 경우 또는 Citrix Gateway 인증서를 발급하는 CA 의 루트 인증서가 시스템 CA 목록에 없는 경우 이 설정은 꺼짐입니다. 이 설정이 꺼짐인 경우 Android 운영 체제에서는 Citrix Gateway 인증서의 유효성이 검사됩니다. 유효성 검사에 실패하면 연결이 허용되지 않습니다. 기본값은 꺼짐입니다.



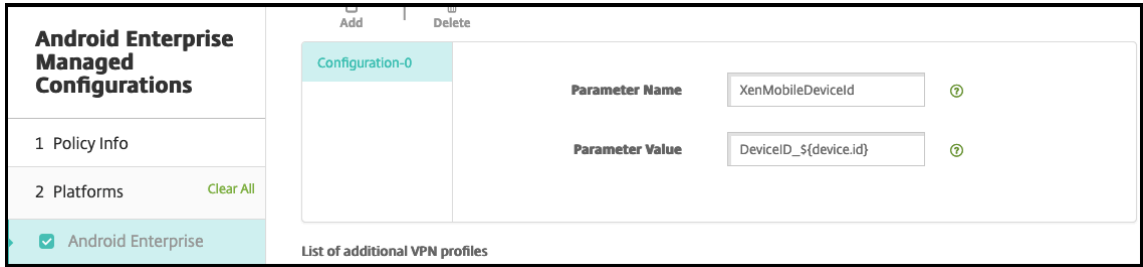
6. 필요한 경우 사용자 지정 매개변수를 만듭니다. 사용자 지정 매개변수 **XenMobileDeviceId** 와 **UserAgent** 가 지원됩니다. 현재 VPN 구성을 선택하고 추가를 클릭합니다.



- a) 사용자 지정 매개변수를 만듭니다.

- 매개변수 이름. **XenMobileDeviceId** 를 입력합니다. 이 필드는 XenMobile 의 장치 등록을 기준으로 네트워크 액세스 검사에 사용할 장치 ID 입니다. XenMobile 에서 장치를 등록하고 관리하는 경우 VPN 연결이 허용됩니다. 그렇지 않으면 VPN 설정시 인증이 거부됩니다.

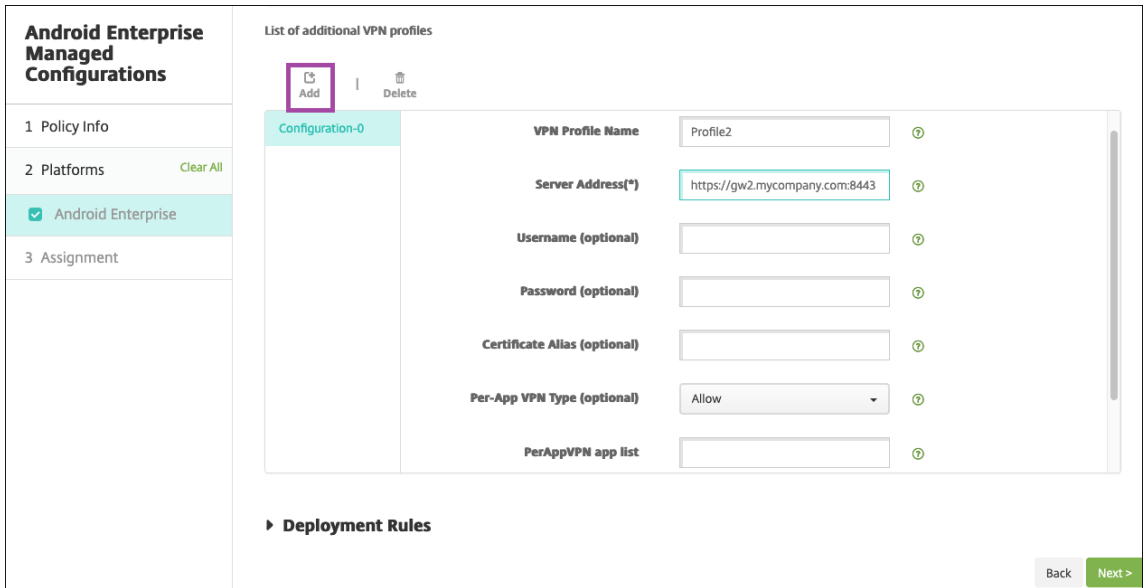
- 매개변수값 XenMobile 에서 장치의 등록 및 관리 상태를 결정하려면 XenMobileDeviceID 의 값을 `DeviceID_${ device.id }` 로 설정합니다.



a) 다른 사용자 지정 매개변수를 만들려면 추가를 다시 클릭합니다. 이 사용자 지정 매개변수를 만듭니다.

- 매개변수 이름. **UserAgent** 를 입력합니다. 이 텍스트는 Citrix Gateway 에서 추가 검사를 수행하기 위해 사용자 에이전트 HTTP 헤더에 추가됩니다. 이 텍스트의 값은 Citrix 게이트웨이와 통신하는 동안 Citrix SSO 앱을 통해 사용자 에이전트 HTTP 헤더에 추가됩니다.
- 매개변수 값. 사용자 에이전트 HTTP 헤더에 추가할 텍스트를 입력합니다. 이 텍스트는 HTTP 사용자 에이전트 사양을 준수해야 합니다.

7. 필요한 경우 VPN 프로필 구성을 추가로 만듭니다. 구성 목록에서 추가를 클릭합니다. 새 구성이 목록에 나타납니다. 새 구성을 선택하고 5 단계와 6 단계를 반복합니다 (선택 사항).



8. 원하는 VPN 프로필을 모두 만들었으면 다음을 클릭합니다.

9. Citrix SSO 의이 관리되는 구성에 대한 배포 규칙을 구성합니다.

10. 저장을 클릭합니다.

이제 Citrix SSO 에 대한 이러한 관리되는 구성이 구성된 장치 정책 목록에 나타납니다.

구성한 VPN 프로필에 대해 항상 켜기를 사용하려면 [XenMobile 옵션 장치 정책](#) 을 설정합니다.

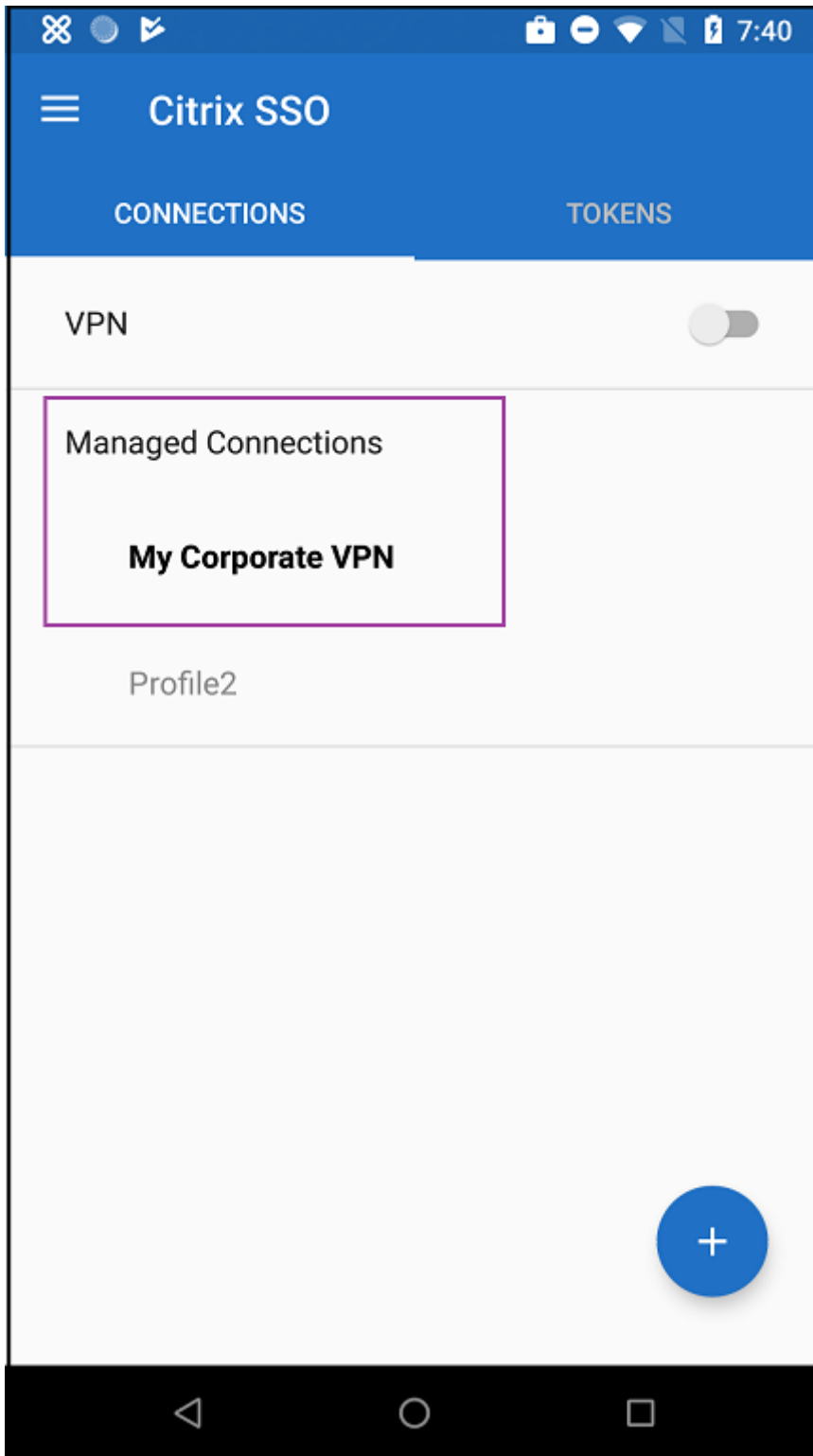
참고:

Android Enterprise 의항상 VPN 연결에는 Citrix Secure Hub 19.5.5 이상이필요합니다.

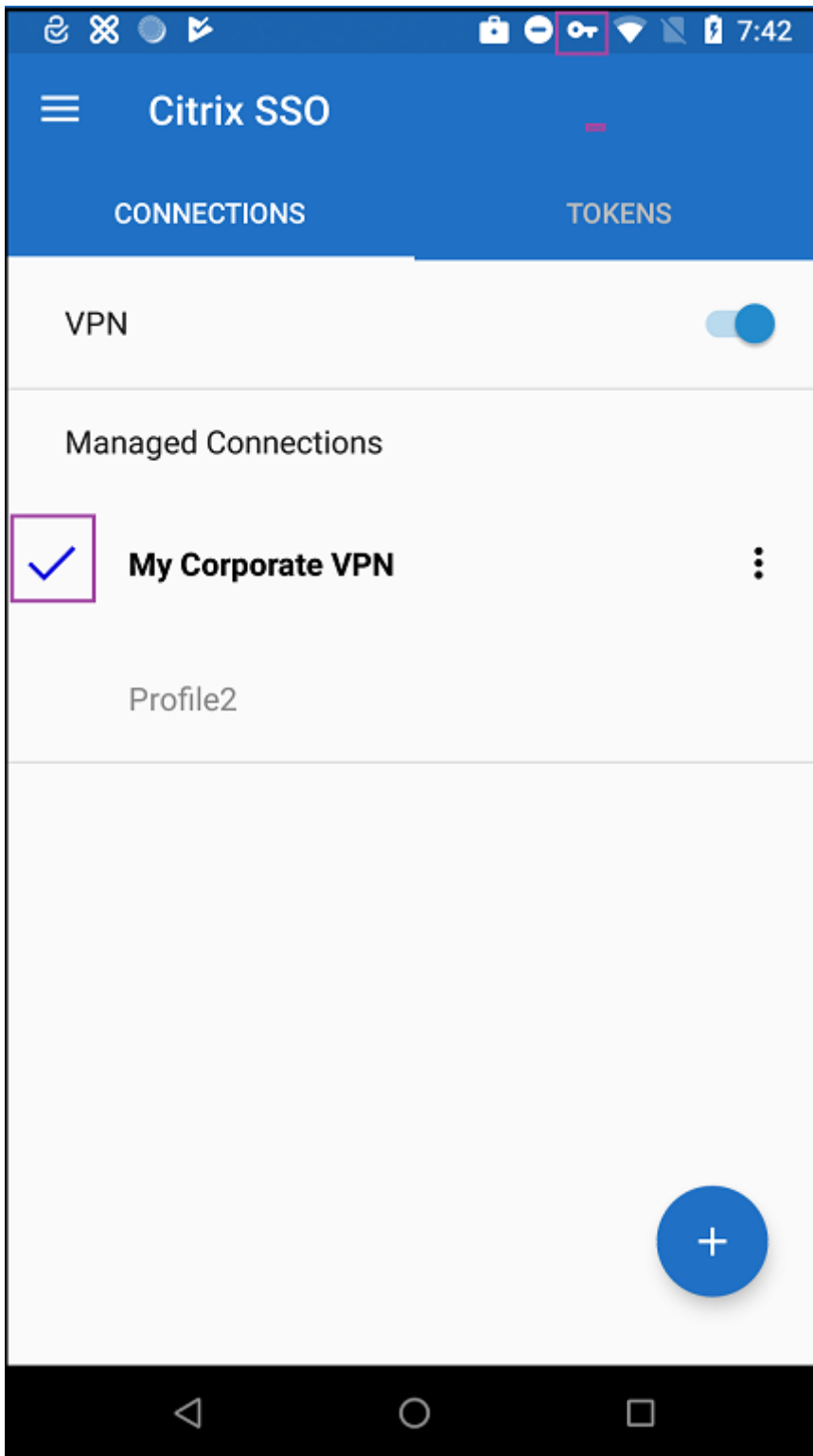
장치에서 **VPN** 프로필에액세스

만든 VPN 프로필에액세스하려면 Android Enterprise 사용자가 Google Play Store 에서 Citrix SSO 를설치해야합니
다.

구성한 VPN 프로필은앱의 **Managed Connections(관리되는연결)** 영역에나타납니다. 사용자는 VPN 프로필을사용하여
연결하려는 VPN 프로필을누릅니다.



사용자가 인증되고 연결되면 VPN 프로필 옆에 확인 표시가 나타납니다. 열쇠 아이콘은 VPN 이 연결되어 있음을 나타냅니다.



Android Enterprise 권한

January 6, 2020

작업프로필내의 Android Enterprise 앱에대한요청에서 Google 이 “위험한” 권한이라고하는권한을처리하는방법을구성할수있습니다. 앱의권한요청에대한부여또는거부를확인하는메시지를사용자에게표시할지여부를제어할수있습니다. 이기능은 Android 7.0 이상을실행하는장치에적용됩니다.

Google 에서위험한권한이란사용자의개인정보와관련되거나사용자의저장된데이터또는다른앱의작동에영향을미칠수있는데이터또는리소스에대한액세스권한을앱에제공하는권한을뜻합니다. 예를들어사용자의연락처를읽을수있는권한은위험한권한입니다.

작업프로필안에있는 Android Enterprise 앱에대한모든위험한권한요청의동작을제어하는글로벌상태를구성할수있습니다. 또한 Google 이정의한대로개별권한그룹에대한위험한권한요청의동작을각앱에대해제어할수있습니다. 이러한개별설정은글로벌상태를재정의합니다.

Google 이권한그룹을정의하는방법에대한자세한내용은이 [Android 개발자 가이드](#)에서 “권한그룹” 을참조하십시오.

기본적으로위험한권한요청을부여하거나거부하라는메시지가사용자에게표시됩니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Android Enterprise 설정

The screenshot shows the 'Configure' page for 'Android for Work App Permissions'. The 'Global State' is set to 'Prompt'. The permissions table is as follows:

Category	App	Grant Status	Action
Calendar	Gmail	Grant	Add
	WhatsApp Messenger	Deny	Add
Camera	Gmail	Prompt	Add
	WhatsApp Messenger	Deny	Add
Contacts	Gmail	Prompt	Add
	WhatsApp Messenger	Deny	Add
Location	Gmail	Prompt	Add
	WhatsApp Messenger	Deny	Add
Microphone	Gmail	Prompt	Add
	WhatsApp Messenger	Deny	Add

- 글로벌상태: 모든위험한권한요청의동작을제어합니다. 목록에서 프롬프트, 부여또는 거부를클릭합니다.

- 프롬프트: 위험한권한요청을부여하거나거부하라는메시지가사용자에게표시됩니다.
- 부여: 모든위험한권한요청이부여됩니다. 사용자에게메시지가표시되지않습니다.
- 거부: 모든위험한권한요청이거부됩니다. 사용자에게메시지가표시되지않습니다.

기본값은 프롬프트입니다.

- 각앱의각권한그룹에대한개별동작을설정합니다. 권한그룹의동작을구성하려면: 추가를클릭하고 앱에서목록의앱을선택합니다. Android Enterprise 시스템앱을구성하는경우 새로추가를클릭하고제한장치정책에서사용하도록설정하응용 프로그램패키지이름을입력합니다. 부여상태에서 프롬프트, 부여또는 거부를선택합니다. 이부여상태는글로벌상태를재정의합니다.

- 프롬프트: 이앱의이권한그룹에서위험한권한요청을부여하거나거부하라는메시지가사용자에게표시됩니다.
- 부여: 이앱의이권한그룹에서위험한권한요청이부여됩니다. 사용자에게메시지가표시되지않습니다.
- 거부: 이앱의이권한그룹에서위험한권한요청이거부됩니다. 사용자에게메시지가표시되지않습니다.

기본값은 프롬프트입니다.

- 앱및부여상태옆의 저장을클릭합니다.
- 권한그룹의앱을추가하려면 추가를다시클릭하고이단계를반복합니다.
- 모든권한그룹에대한부여상태설정이완료되면 다음을클릭합니다.

APN 장치정책

January 6, 2020

iOS, Android 및 Windows Mobile/CE 장치에대한사용자지정 APN(엑세스포인트이름) 장치정책을추가할수있습니다. 조직에서모바일장치로부터인터넷에연결하는데소비자 APN 을사용하지않을경우이정책을사용하십시오. APN 정책은특정이동통신사업자의 GPRS(General Packet Radio Service) 에장치를연결하는데사용되는설정을결정합니다. 이설정엔대부분의최신휴대폰에이미정의되어있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

The screenshot shows the XenMobile configuration interface for an APN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows 'APN Policy' selected, with sub-sections for '1 Policy Info', '2 Platforms' (where 'iOS', 'Android', and 'Windows Mobile/CE' are checked), and '3 Assignment'. The main content area is titled 'APN Policy' and contains the following fields and options:

- APN ***: A text input field.
- User name**: A text input field containing 'administrator'.
- Password**: A password input field with masked characters.
- Server proxy address**: A text input field.
- Server proxy port**: A text input field.
- Remove policy**: Two radio button options:
 - Select date
 - Duration until removal (in hours)

At the bottom right of the form, there are 'Back' and 'Next >' buttons.

- **APN:** 액세스지점의 이름을 입력합니다. 이 이름은 허용된 iOS APN 과 일치해야 합니다. 그렇지 않으면 정책이 실패합니다.
- **사용자 이름:** 이 문자열은 이 APN 의 사용자 이름을 지정합니다. 사용자 이름이 누락된 경우 프로필 설치 중에 문자열을 입력하라는 메시지가 표시됩니다.
- **암호:** 이 APN 에 대한 사용자의 암호입니다. 쉽게 알 수 없도록 암호는 암호화됩니다. 암호가 페이로드에서 누락된 경우 프로필 설치 중에 암호를 묻는 메시지가 표시됩니다.
- **서버 프록시 주소:** APN 프록시의 IP 주소 또는 URL 입니다.
- **서버 프록시 포트:** APN 프록시의 포트 번호입니다. 서버 프록시 주소를 입력한 경우 포트가 필수입니다.
- **정책 설정의 정책 제거 옆에서 날짜 선택 또는 제거할 때까지의 기간 (시간) 을 클릭합니다.**
 - 날짜 선택을 클릭하는 경우 달력을 클릭하여 제거할 날짜를 선택합니다.
 - 사용자가 정책을 제거하도록 허용 목록에서 항상, 암호 필요 또는 안함을 클릭합니다.
 - 암호 필요를 클릭하는 경우 제거 암호 옆에 필요한 암호를 입력합니다.

Android 설정

The screenshot shows the XenMobile configuration interface for an APN Policy. The 'Configure' tab is active, and the 'APN Policy' section is selected in the sidebar. The main content area displays the configuration form for the APN Policy, which includes fields for APN, User name (set to 'administrator'), Password, Server, APN type, Authentication type (set to 'None'), Server proxy address, Server proxy port, and MMSC. The 'Platforms' section shows 'Android' selected with a checked checkbox, while 'iOS' and 'Windows Mobile/CE' are unselected. The 'Assignment' section is currently empty.

- **APN:** 액세스지점의 이름을 입력합니다. 이 이름은 허용된 Android APN 과 일치해야 합니다. 그렇지 않으면 정책이 실패합니다.
- **사용자 이름:** 이 문자열은 이 APN 의 사용자 이름을 지정합니다. 사용자 이름이 누락된 경우 프로필 설치 중에 문자열을 입력하라는 메시지가 표시됩니다.
- **암호:** 이 APN 에 대한 사용자의 암호입니다. 쉽게 알 수 없도록 암호는 암호화됩니다. 암호가 페이로드에서 누락된 경우 프로필 설치 중에 암호를 묻는 메시지가 표시됩니다.
- **서버:** 스마트폰을 대상으로 하는 이 설정은 대개 비어 있습니다. 표준 웹사이트에 액세스하거나 렌더링 수 없는 휴대폰의 경우 WAP(Wireless Application Protocol) 게이트웨이 서버를 참조합니다.
- **APN 유형:** 이 설정은 액세스 지점에 대한 이동통신사업자의 의도된 용도와 일치해야 합니다. 이것은 심표로 구분된 APN 서비스 지정자 문자열이며 이동통신사업자의 공표된 정의와 일치해야 합니다. 다음 예를 참조하십시오.
 - *. 모든 트래픽은 이 액세스 지점을 통과합니다.
 - mms. 멀티미디어 트래픽은 이 액세스 지점을 통과합니다.
 - default. 멀티미디어를 비롯한 모든 트래픽은 이 액세스 지점을 통과합니다.
 - supl. SUPL(Secure User Plane Location) 은 보조 GPS(A-GPS) 와 연결됩니다.
 - dun. 전화 접속 네트워크는 시대에 뒤떨어져 거의 사용되지 않습니다.
 - hipri. 우선 순위가 높은 네트워크입니다.
 - fota. FOTA(Firmware Over The Air) 는 펌웨어 업데이트를 수신하는 데 사용됩니다.
- **인증 유형:** 목록에서 사용할 인증 유형을 클릭합니다. 기본값은 없음입니다.
- **서버 프록시 주소:** 이동통신사업자 APN HTTP 프록시의 IP 주소 또는 URL 입니다.
- **서버 프록시 포트:** APN 프록시의 포트 번호입니다. 서버 프록시 주소를 입력한 경우 포트가 필수입니다.
- **MMSC:** 이동통신사업자가 제공한 MMS 게이트웨이 서버 주소입니다.
- **MMS(멀티미디어 메시징 서버) 프록시 주소:** MMS 트래픽을 위한 멀티미디어 메시징 서비스 서버입니다. MMS 는 SMS 의 후신으로, 사진이나 비디오와 같은 멀티미디어 콘텐츠가 포함된 더 큰 메시지를 보낼 수 있습니다. 이러한 서버에는 특정 프로토콜 (예: MM1, ... MM11) 이 필요합니다.

- **MMS 포트:** MMS 프록시에서 사용되는 포트입니다.

Windows Mobile/CE 설정

The screenshot shows the XenMobile configuration interface for an APN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'APN Policy' and includes a description: 'This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.' The configuration fields are: 'APN' (text input), 'Network' (dropdown menu set to 'Built-in office'), 'User name' (text input), and 'Password' (text input). A 'Deployment Rules' section is also visible. At the bottom right, there are 'Back' and 'Next >' buttons.

- **APN:** 액세스지점의 이름을 입력합니다. 이 이름은 허용된 Android APN 과 일치해야 합니다. 그렇지 않으면 정책이 실패합니다.
- **네트워크:** 목록에서 사용할 네트워크 유형을 클릭합니다. 기본값은 기본제공사입니다.
- **사용자 이름:** 이 문자열은 이 APN 의 사용자 이름을 지정합니다. 사용자 이름이 누락된 경우 프로필 설치 중에 문자열을 입력하라는 메시지가 표시됩니다.
- **암호:** 이 APN 에 대한 사용자의 암호입니다. 쉽게 알 수 없도록 암호는 암호화됩니다. 암호가 페이로드에서 누락된 경우 프로필 설치 중에 암호를 묻는 메시지가 표시됩니다.

앱 액세스 장치 정책

January 6, 2020

XenMobile 의 앱 액세스 장치 정책을 사용하면 장치에 설치해야 하거나, 장치에 설치할 수 있거나, 장치에 설치해서는 안 되는 앱의 목록을 정의할 수 있습니다. 그런 다음 자동화된 동작을 만들어 장치가 앱 목록을 따르는 데 대응할 수 있습니다. iOS, Android 및 Windows Mobile/CE 장치에 대한 앱 액세스 정책을 만들 수 있습니다.

한 번에 한 가지 유형의 액세스 정책만 구성할 수 있습니다. 필수 앱, 추천 앱 또는 금지된 앱 목록 중 하나에 대한 정책을 추가할 수 있지만 동일한 앱 액세스 정책 내에서 목록을 혼합할 수는 없습니다. 각 유형의 목록에 대한 정책을 만드는 경우 XenMobile 의 정책이 어떤 앱 목록에 적용되는지 알 수 있도록 각 정책의 이름을 신중하게 지정하는 것이 좋습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

플랫폼설정

- 액세스정책: 필수, 추천또는 금지를클릭합니다. 기본값은 필수입니다.
- 하나이상의앱을목록에추가하려면 추가를클릭한후다음을수행합니다.
 - 앱이름: 앱이름을입력합니다.
 - 앱식별자: 선택적인앱식별자를입력합니다.
 - 저장또는 취소를클릭합니다.
 - 추가할각앱에대해이단계를반복합니다.

앱특성장치정책

January 6, 2020

앱특성장치정책을사용하면 iOS 장치에대한관리되는앱번들 ID 또는앱별 VPN 식별자와같은특성을지정할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

The screenshot shows the XenMobile web interface. At the top, there's a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below that, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'App Attributes Policy' and has a sub-section 'Policy Information'. Under 'Policy Information', there are two input fields: 'Policy Name *' and 'Description'. A checkbox for 'iOS' is checked. On the left side, there's a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. A 'Next >' button is at the bottom right.

- 관리되는앱번들 ID: 목록에서앱번들 ID 또는 새로추가를클릭합니다.
 - 새로추가를클릭하는경우표시되는필드에앱번들 ID 를입력합니다.
- 앱별 VPN 식별자: 목록에서앱별 VPN 식별자를클릭합니다.

앱구성장치정책

January 6, 2020

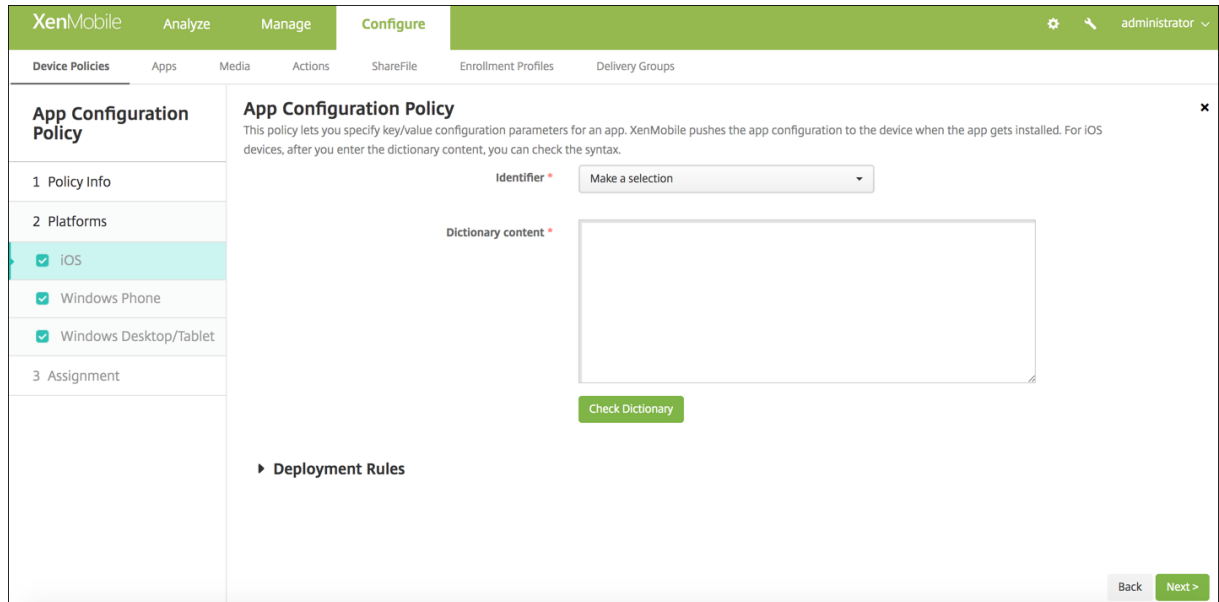
다음은배포하여관리되는구성을지원하는앱을원격으로구성할수있습니다.

- iOS 장치에 XML 구성파일 (속성목록또는 plist 라고함) 을배포합니다.
- 또는 Windows 10 전화, 태블릿또는데스크톱장치에대한키/값쌍을배포합니다.

구성은앱의다양한설정및동작을지정합니다. 사용자가앱을설치하면 XenMobile 이장치로구성을푸시합니다. 구성할수있는실제 설정및동작은앱에따라다르며이문서에서다루지않습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정



- 식별자: 목록에서구성할앱을클릭하거나 새로추가를클릭하여새앱을목록에추가합니다.
 - 새로추가를클릭하는경우표시되는필드에앱식별자를입력합니다.
- 사전내용: XML 속성목록 (plist) 구성정보를입력하거나복사하여붙여넣습니다.
- 사전확인을클릭합니다. XenMobile 이 XML 을확인합니다. 오류가없으면콘텐츠상자아래에 올바른 **XML** 이표시됩니다. 콘텐츠상자아래에구문오류가표시되면계속하기전에해당오류를수정해야합니다.

Windows Phone 또는데스크톱/태블릿설정

The screenshot shows the 'App Configuration Policy' configuration page in XenMobile. The left sidebar has '2 Platforms' selected, with 'Windows Phone' and 'Windows Desktop/Tablet' checked. The main area shows a 'Make a selection' dropdown, a table for 'Parameter name' and 'Value', and a 'Deployment Rules' section. 'Back' and 'Next >' buttons are at the bottom right.

This screenshot is similar to the one above, but in the '2 Platforms' section, 'Windows Desktop/Tablet' is selected (checked), while 'Windows Phone' is not. The rest of the interface remains the same.

- 선택목록에서구성할앱을클릭하거나 새로추가를클릭하여새앱을목록에추가합니다.
 - 새로추가를클릭하는경우표시되는필드에패키지제품군이름을입력합니다.
- 추가할각구성매개변수에대해 추가를클릭하고다음을수행합니다.
 - 매개변수이름: Windows 장치에대한응용프로그램설정의키이름을입력합니다. Windows 앱설정에대한자세한 내용은 Microsoft 설명서를참조하십시오.
 - 값: 지정된매개변수의값을입력합니다.
 - 추가를클릭하여매개변수를추가하거나 취소를클릭하여매개변수추가를취소합니다.

앱인벤토리장치정책

January 6, 2020

앱인벤토리정책을 사용하면 관리되는 장치에서 앱의 인벤토리를 수집할 수 있습니다. 그러면 XenMobile 이해당장치에 배포된 앱 액세스 정책과 인벤토리를 비교합니다. 이 방법으로 앱 블랙리스트 (앱 액세스 정책에서 금지됨) 또는 화이트리스트 (앱 액세스 정책에서 필요함)에 표시되는 앱을 검색하고 적절히 조치를 취할 수 있습니다.

iOS, macOS, Android, Android Enterprise, Windows Desktop/Tablet, Windows Phone 또는 Windows Mobile/CE 장치에 대한 앱 액세스 정책을 만들 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

플랫폼 설정

App Inventory Policy

This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.

ios

► Deployment Rules

Back Next >

- 선택한 각 플랫폼에 대해 기본 설정을 그대로 사용하거나 설정을 꺼짐으로 변경합니다. 기본값은 켜짐입니다.

앱 잠금 장치 정책

January 6, 2020

앱 잠금 장치 정책은 장치에서 실행될 수 있는 앱 목록 또는 장치에서 실행을 차단할 앱 목록을 정의합니다. iOS 및 Android 장치에 대해 이 정책을 구성할 수 있지만 정책이 작동하는 정확한 방식은 각 플랫폼마다 다릅니다. 예를 들어 iOS 장치에서는 여러 앱을 차단할 수 없습니다.

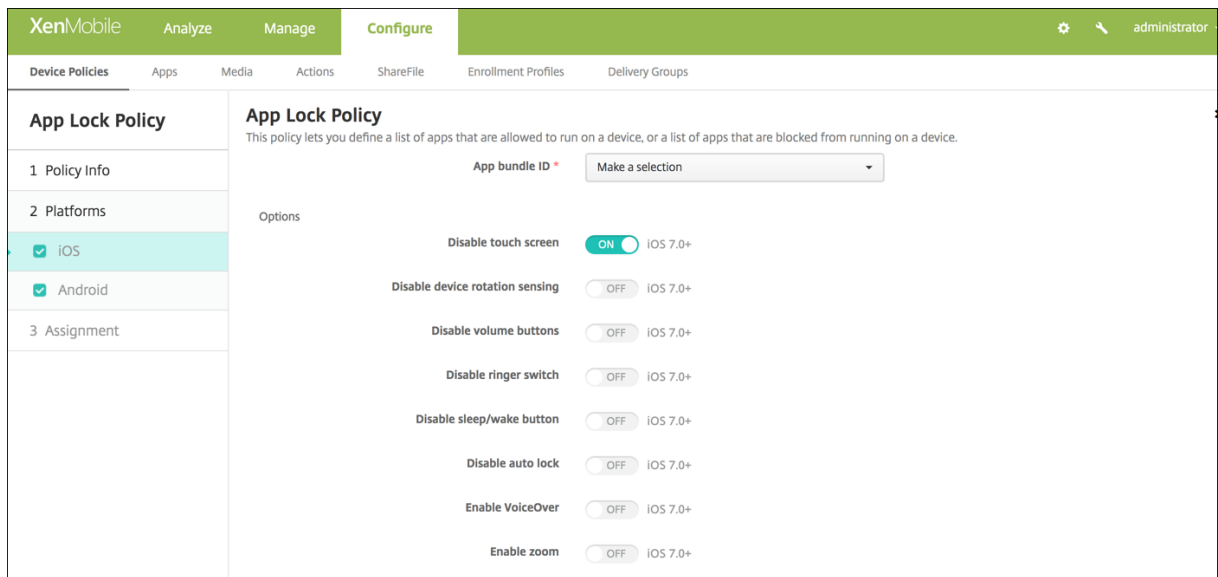
마찬가지로, iOS 장치에서는정책당하나의 iOS 앱만선택할수있습니다. 즉, 사용자는장치를사용하여하나의앱만실행할수있습니다. 앱잠금정책이시행될때관리자가구체적으로허용한옵션외의다른어떤작업도장치에서수행할수없습니다.

또한 iOS 장치에서앱잠금정책을푸시하려면장치가감독되어야합니다.

장치정책은대부분의 Android L 및 M 장치에서작동하지만앱잠금의경우필요한 API 를 Google 이더이상제공하지않기때문에 Android N 이상장치에서작동하지않습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정



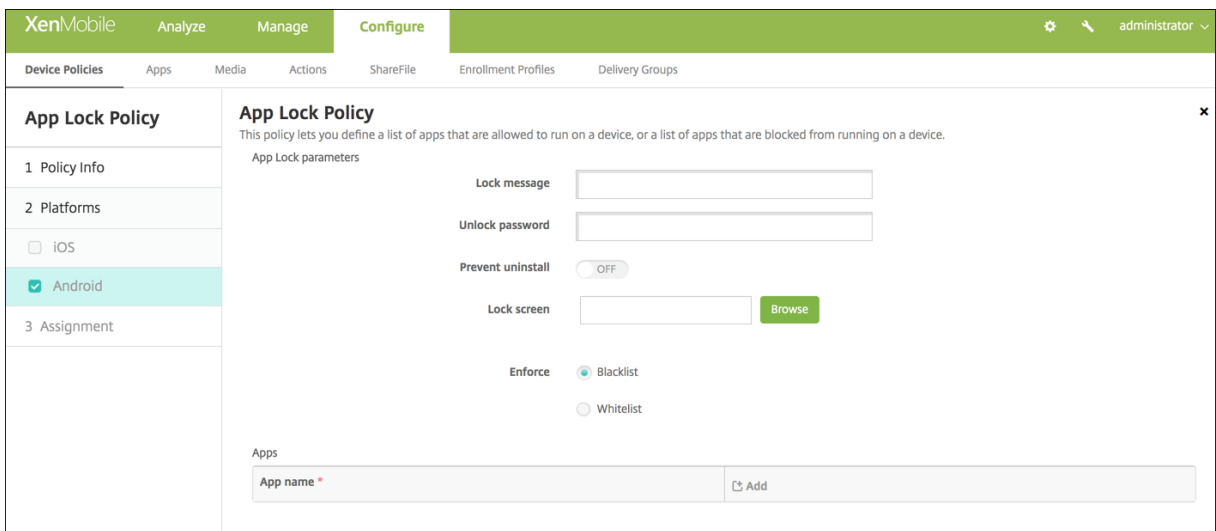
- 앱번들 ID: 목록에서이정책을적용할앱을클릭하거나 새로추가를클릭하여새앱목록에추가합니다. 새로추가를선택하는 경우표시되는필드에앱이름을입력합니다.
- 옵션: 다음각옵션은 iOS 7.0 이상에만적용됩니다. 각옵션의기본값은 꺼짐이며터치스크린사용안함은예외적으로기본값이 켜짐입니다.
 - 터치스크린사용안함
 - 장치회전감지사용안함
 - 볼륨단추사용안함
 - 벨소리전환사용안함
벨소리전환사용안함이 켜짐인경우벨소리동작은처음벨소리를사용안함으로설정할때스위치의위치에따라다릅니다.
 - 절전단추사용안함
 - 자동잠금사용안함
 - VoiceOver 사용안함
 - 확대/축소사용
 - 색반전사용
 - AssistiveTouch 사용

- 선택항목말하기사용
- 모노오디오사용
- 사용자가설정할수있는옵션: 다음각옵션은 iOS 7.0 이상에만적용됩니다. 각옵션의기본값은 꺼짐입니다.
 - VoiceOver 조정허용
 - 확대/축소조정허용
 - 색반전조정허용
 - AssitiveTouch 조정허용

Android 설정

참고:

앱잠금장치정책을사용하여 Android 설정앱을차단할수없습니다.



- 앱잠금매개변수
 - 잠금메시지: 사용자가잠긴앱을열려고할때표시할메시지를입력합니다.
 - 잠금해제암호: 앱잠금을해제하는암호를입력합니다.
 - 제거금지: 사용자가앱을제거하도록허용할지여부를선택합니다. 기본값은 꺼짐입니다.
 - 잠금화면: 찾아보기를클릭하고파일의위치가이동하여장치의잠금화면에표시할이미지를선택합니다.
 - 적용: 블랙리스트를클릭하여장치에서실행될수없는앱목록을만들거나 화이트리스트를클릭하여장치에서실행될수 있는앱목록을만듭니다.
- 앱: 추가를클릭하고다음을수행합니다.
 - 앱이름: 목록에서앱이름을클릭하여화이트리스트또는블랙리스트에추가하거나 새로추가를클릭하여사용가능한앱 목록에새앱을추가합니다.
 - 새로추가를선택하는경우표시되는필드에앱이름을입력합니다.
 - 저장또는 취소를클릭합니다.
 - 화이트리스트또는블랙리스트에추가할각앱에이러한단계를반복합니다.

앱네트워크사용장치정책

January 6, 2020

iOS 장치에서 관리되는 앱이 셀룰러 데이터 네트워크와 같은 네트워크를 사용하는 방식을 지정하는 네트워크 사용 규칙을 설정할 수 있습니다. 이러한 규칙은 관리되는 앱에만 적용됩니다. 관리되는 앱은 XenMobile 을 통해 사용자 장치에 배포되는 앱입니다. XenMobile 을 통해 배포되지 않고 사용자가 장치에 직접 다운로드한 앱이나 장치를 XenMobile 에 등록할 때 장치에 이미 설치되어 있던 앱은 여기에 해당되지 않습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

- 로밍 셀룰러 데이터 허용: 지정된 앱이 로밍 중에 셀룰러 데이터 연결을 사용할 수 있는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 셀룰러 데이터 허용: 지정된 앱이 셀룰러 데이터 연결을 사용할 수 있는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 앱 식별자 일치: 목록에 추가할 각 앱에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 앱 식별자: 앱 식별자를 입력합니다.
 - 목록에 앱을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.

앱 알림 장치 정책

January 6, 2020

앱 알림 정책을 사용하여 iOS 사용자가 지정된 앱의 알림을 수신하는 방법을 제어할 수 있습니다. 이 정책은 iOS 9.3 이상을 실행하는 장치에서 지원됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

App Bundle Identifier	Allow Notifications	Show in Notification Center	Badge App Icon	Sounds	Show on Lock Screen	Show in Car Play	Enable Critical Alert	Unlocked Alert Style
App Store	ON	ON	ON	ON	ON	ON	OFF	Alerts

Policy Settings

Remove policy: Select date, Duration until removal (in hours)

Allow user to remove policy: Always

Profile scope: System

- 앱번들 ID: 이정책을적용할앱을지정합니다.
- 알림허용: 알림을허용하려면 켜짐을선택합니다.
- 알림센터에표시: 사용자장치의알림센터에알림을표시하려면 켜짐을선택합니다.
- 배지앱아이콘: 알림과함께배지앱아이콘을표시하려면 켜짐을선택합니다.
- 사운드: 알림과함께사운드를포함하려면 켜짐을선택합니다.
- 잠금화면에표시: 사용자장치의잠금화면에알림을표시하려면 켜짐을선택합니다.
- **CarPlay** 로표시: 켜짐인경우 Apple CarPlay 에알림이표시됩니다. iOS 12 이상에서사용할수있습니다. 기본값은 켜짐입니다.
- 중요알림사용: 켜짐인경우앱이방해금지및벨소리설정을무시하는중요알림으로알림을표시할수있습니다. iOS 12 이상에서사용할수있습니다. 기본값은 꺼짐입니다.
- 잠금해제경고스타일: 목록에서 없음, 배너또는 경고를선택하여잠금해제경고의모양을구성합니다.

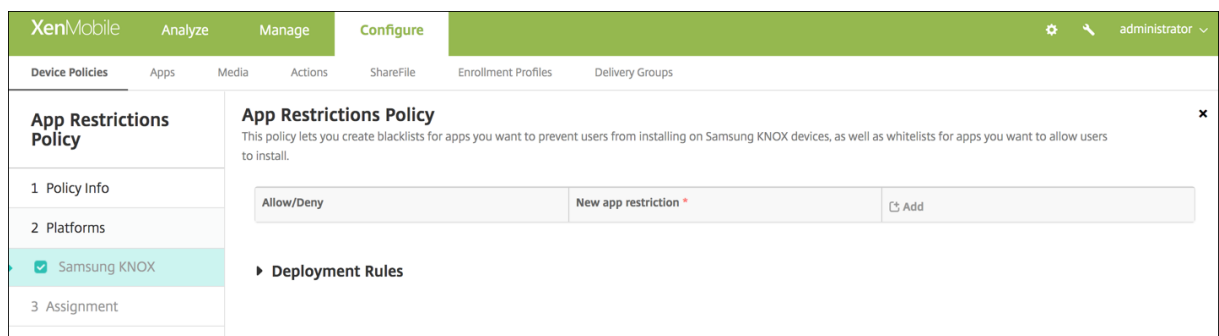
앱제한장치정책

January 6, 2020

사용자가 Samsung KNOX 장치에설치할수없는앱에대한블랙리스트를만들고사용자가설치할수있는앱에대한화이트리스트를 만들수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Samsung KNOX 설정



허용/거부목록에추가할각앱에대해 추가를클릭하고다음을수행합니다.

- 허용/거부: 사용자가앱을설치하도록허용할지여부를선택합니다.
- 새앱제한: 앱패키지 ID 를입력합니다 (예: com.kmdm.af.crackle).
- 저장을클릭하여허용/거부목록에앱을저장하거나 취소를클릭하여허용/거부목록에앱을저장하지않습니다.

애틀러닝장치정책

January 6, 2020

중요:

애틀러닝장치정책은 원격지원에만 사용됩니다. 원격지원에 대한 자세한 내용은 [지원 옵션 및 원격 지원을 참조하십시오](#). 2019년 1월 1일부터 신규 고객에게는 더 이상 원격 지원이 제공되지 않습니다. 기존 고객은 제품을 계속 사용할 수 있지만 Citrix는 개선 사항이나 수정 사항을 제공하지 않습니다.

응용 프로그램 터널 (애틀러닝)은 모바일 앱의 무중단 서비스 및 데이터 전송 안정성을 개선하도록 설계되었습니다. 애틀러닝은 모든 모바일 장치 앱의 클라이언트 구성 요소와 서버 구성 요소 간의 프로세스 매개 변수를 정의합니다. 또한 관리 지원을 위해 애틀러닝을 사용하여 장치에 대한 원격 지원 터널을 만들 수 있습니다. Android 및 Windows Mobile/CE 장치에 대한 애틀러닝 정책을 구성할 수 있습니다.

이 정책에서 정의한 터널을 통해 전송되는 모든 앱 트래픽은 앱을 실행하는 서버로 리디렉션되기 전에 XenMobile 을 통과합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

Android 설정

- 이터널을 원격 지원에 사용: 원격 지원에 터널을 사용할지 여부를 선택합니다.
구성 단계는 원격 지원을 선택하는지 여부에 따라 다릅니다.
- 원격 지원을 선택하지 않은 경우 다음을 수행합니다.
 - 연결을 시작한 원본: 장치를 또는 서버를 클릭하여 연결을 시작하는 원본을 지정합니다.

- 장치당최대연결수: 숫자를입력하여앱에서설정할수있는동시 TCP 연결수를지정합니다. 이필드는장치에서시작된연결에만적용됩니다.
 - 연결시간제한정의: 터널이닫히기전까지앱이유휴상태로있을수있는시간을설정할지여부를선택합니다.
 - * 연결시간제한: 연결시간제한정의를 켜짐으로설정한경우터널이닫히기전까지앱이유휴상태로있을수있는시간을초로입력합니다.
 - 이터널을통과하는셀룰러연결차단: 로밍중에이터널을차단할지여부를선택합니다.
 - 참고:
WiFi 및 USB 연결은차단되지않습니다.
 - 클라이언트포트: 클라이언트포트번호를입력합니다. 대부분의경우이값은서버포트와동일합니다.
 - IP 주소또는서버이름: 앱서버의 IP 주소또는이름을입력합니다. 이필드는장치에서시작된연결에만적용됩니다.
 - 서버포트: 서버포트번호를입력합니다.
- 원격지원을선택한경우다음을수행합니다.
 - 이터널을원격지원에사용: 켜짐으로설정합니다.
 - 연결시간제한정의: 터널이닫히기전까지앱이유휴상태로있을수있는시간을설정할지여부를선택합니다.
 - * 연결시간제한: 연결시간제한정의를 켜짐으로설정한경우터널이닫히기전까지앱이유휴상태로있을수있는시간을초로입력합니다.
 - **SSL** 연결사용: 이터널에보안 SSL 연결을사용할지여부를선택합니다.
 - 이터널을통과하는셀룰러연결차단: 로밍중에이터널을차단할지여부를선택합니다. 이설정은 WiFi 및 USB 연결을차단하지않습니다.

Windows Mobile/CE 설정

The screenshot shows the XenMobile configuration interface for a Tunnel Policy. The left sidebar has 'Tunnel Policy' selected, with sub-items for '1 Policy Info', '2 Platforms' (including 'Windows Mobile/CE'), and '3 Assignment'. The main area is titled 'Tunnel Policy' and contains the following settings:

- Use this tunnel for remote support:** OFF
- Connection configuration:**
 - Connection initiated by:** Device
 - Protocol:** Generic TCP
 - Maximum connections per device *:** 1
 - Define connection time out:** OFF
 - Block cellular connections passing by this tunnel:** OFF
- App device parameters:**
 - Redirect to XenMobile:** Through app settings
 - Client port *:** (empty field)
- App server parameters:**
 - IP address or server name *:** (empty field)

- 이터널을원격지원에서사용: 원격지원에터널을사용할지여부를선택합니다.

구성단계는원격지원을선택하는지여부에따라다릅니다.

- 원격지원을선택하지않은경우다음을수행합니다.
 - 연결을시작한원본: 장치또는 서버를클릭하여연결을시작하는원본을지정합니다.
 - 프로토콜: 목록에서사용할프로토콜을클릭합니다. 기본값은 제네릭 **TCP** 입니다.
 - 장치당최대연결수: 숫자를입력하여앱에서설정할수있는동시 TCP 연결수를지정합니다. 이필드는장치에서시작된 연결에만적용됩니다.
 - 연결시간제한정의: 터널이달하기전까지앱이유휴상태로있을수있는시간을설정할지여부를선택합니다.
 - * 연결시간제한: 연결시간제한정의를 켜짐으로설정할경우터널이달하기전까지앱이유휴상태로있을수있는시간을초로입력합니다.
 - 이터널을통과하는셀룰러연결차단: 로밍중에이터널을차단할지여부를선택합니다.
 - 참고:
WiFi 및 USB 연결은차단되지않습니다.
 - **XenMobile** 로리디렉션: 목록에서장치가 XenMobile 에연결하는방법을클릭합니다. 기본값은 앱설정을통해입니다.
 - * 로컬별칭사용을선택하는경우 로컬별칭에별칭을입력합니다. 기본값은 로컬호스트입니다.
 - * **IP** 주소범위를선택하는경우 **IP** 주소범위시작에서작 **IP** 주소를입력하고 **IP** 주소범위끝에종료주소범위를입력합니다.
 - 클라이언트포트: 클라이언트포트번호를입력합니다. 대부분의경우이값은서버포트와동일합니다.
 - **IP** 주소또는서버이름: 앱서버의 IP 주소또는이름을입력합니다. 이필드는장치에서시작된연결에만적용됩니다.

- 서버포트: 서버포트번호를입력합니다.
- 원격지원을선택한경우다음을수행합니다.
 - 이터널을원격지원에사용: 켜짐으로설정합니다.
 - 연결시간제한정의: 터널이닫히기전까지앱이유휴상태로있을수있는시간을설정할지여부를선택합니다.
 - * 연결시간제한: 연결시간제한정의를 켜짐으로설정할경우터널이닫히기전까지앱이유휴상태로있을수있는시간을초로입력합니다.
 - **SSL** 연결사용: 이터널에보안 SSL 연결을사용할지여부를선택합니다.
 - 이터널을통과하는셀룰러연결차단: 로밍중에이터널을차단할지여부를선택합니다. WiFi 및 USB 연결은차단되지않습니다.

앱제거장치정책

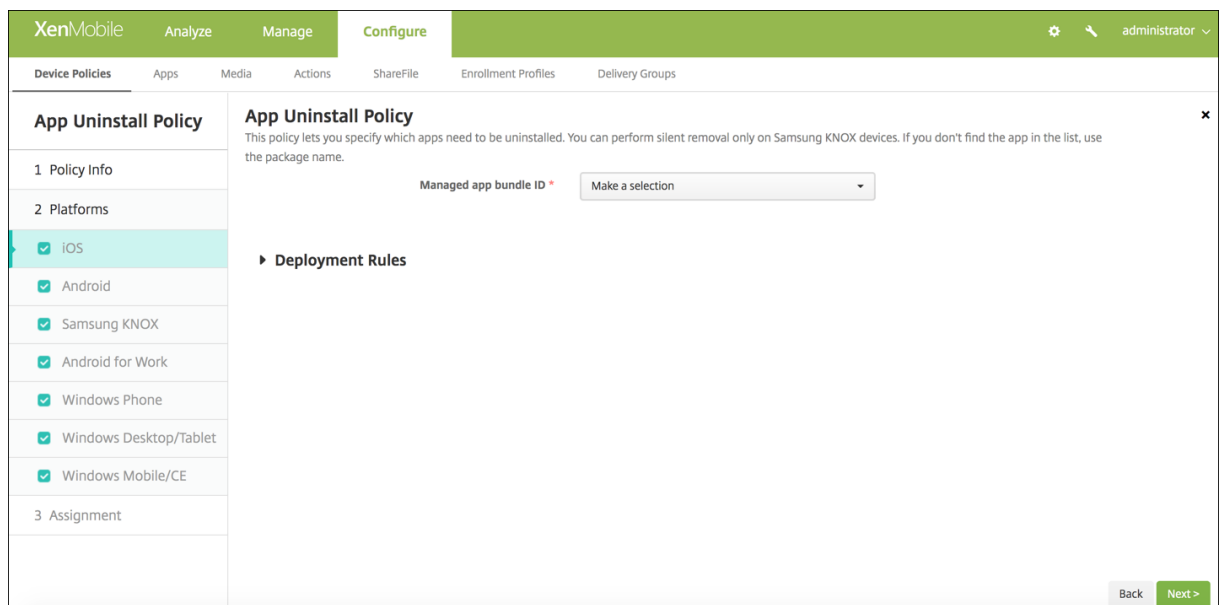
January 6, 2020

iOS, Android, Samsung KNOX, Android Enterprise, Windows Desktop/Tablet 및 Windows Mobile/CE 플랫폼에대한앱제거정책을만들수있습니다. 앱제거정책을사용하면여러가지이유로사용자장치에서앱을제거할수있습니다. 예를들어특정앱을더이상지원하지않으려하거나회사가기존앱을다른공급업체의유사한앱으로교체하려고할수있습니다.

이정책이사용자장치에배포되면해당앱이제거됩니다. Samsung KNOX 장치를제외하고사용자에게앱을제거할것인지묻는메시지가표시됩니다. Samsung KNOX 장치사용자에게는앱을제거할것인지묻는메시지가나타나지않습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정



- 관리되는 앱 번들 **ID**: 목록에서 기존 앱을 클릭하거나 새로 추가를 클릭합니다. 이 플랫폼에 구성된 앱이 없는 경우 목록은 비어 있을 것이므로 새 앱을 추가해야 합니다.
 - 추가를 클릭하면 앱 이름을 입력할 수 있는 필드가 나타납니다.

다른 모든 플랫폼 설정

- 제거할 앱: 추가하려는 각 앱에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 앱 이름: 목록에서 기존 앱을 클릭하거나 새로 추가를 클릭하여 새 앱 이름을 입력합니다. 이 플랫폼에 구성된 앱이 없는 경우 목록은 비어 있을 것이므로 새 앱을 추가해야 합니다.
 - 추가를 클릭하여 앱을 추가하거나 취소를 클릭하여 앱 추가를 취소합니다.

해당 공용 앱 스토어 앱을 설치한 후 자동으로 엔터프라이즈 앱을 제거합니다

공용 앱 스토어 버전이 설치될 때 Citrix 앱의 엔터프라이즈 버전을 제거하도록 XenMobile 을 구성할 수 있습니다. 이 기능을 사용하면 공용 앱 스토어 버전이 설치된 후 사용자 장치에 두 개의 동일한 앱 아이콘이 나타나는 것이 방지됩니다.

앱 제거 장치 정책의 배포 조건은 새 버전 설치 시 이전 앱을 사용자 장치에서 제거하도록 XenMobile 을 트리거합니다. 이 기능은 XenMobile Server 에 엔터프라이즈 모드 (XME) 로 연결되어 관리되는 iOS 장치에서만 사용할 수 있습니다.

설치된 앱 이름 조건을 사용하여 배포 규칙을 구성하려면:

- 엔터프라이즈 앱에 대한 관리되는 앱 번들 **ID** 를 지정합니다.
- 규칙 추가: 새 규칙을 클릭한 다음 샘플에 표시된 것과 같이 설치된 앱 이름 및 같음을 선택합니다. 공용 앱 스토어 앱의 앱 번들 ID 를 입력합니다.

예제에서 공용 앱 스토어 앱 (com.citrix.mail.ios) 이 지정된 배달 그룹의 장치에 설치될 때 XenMobile 이 엔터프라이즈 버전 (com.citrix.mail) 을 제거합니다.

앱 제거 제한 장치 정책

January 6, 2020

Samsung SAFE 또는 Amazon 장치에서 사용자가 제거할 수 있거나 제거할 수 없는 앱을 지정할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

Samsung SAFE 또는 Amazon 설정

- 앱 제거 제한 설정: 추가하려는 각 앱 규칙에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 앱 이름: 목록에서 앱을 클릭하거나 새로 추가를 클릭하여 새 앱을 추가합니다.

- 규칙: 사용자가 앱을 제거할 수 있는지 여부를 선택합니다. 기본값은 설치 제거를 허용하는 것입니다.
- 저장 또는 취소를 클릭합니다.

BitLocker 장치 정책

January 6, 2020

Windows 10에는 BitLocker라는 디스크 암호화 기능이 포함되어 있습니다. BitLocker는 분실 또는 도난 장치의 파일 및 시스템에 대한 무단 액세스를 추가로 보호합니다. BitLocker를 TPM(신뢰할 수 있는 플랫폼 모듈) 칩 버전 1.2 이상과 함께 사용하면 추가 보호를 적용할 수 있습니다. TPM 칩은 암호화 작업을 처리하고 암호화 키를 생성 및 저장하고 키 사용을 제한합니다.

Windows 10 빌드 1703부터 MDM 정책을 통해 BitLocker를 제어할 수 있습니다. XenMobile에서 BitLocker 장치 정책을 사용하여 Windows 10 장치의 BitLocker 마법사에서 제공되는 설정을 구성할 수 있습니다. 예를 들어 BitLocker가 활성화된 장치에서는 시작시 드라이브 잠금을 해제하는 방법, 복구 키를 백업하는 방법 및 고정 드라이브의 잠금을 해제하는 방법에 대한 메시지를 사용자에게 표시할 수 있습니다. BitLocker 장치 정책 설정을 통해 다음을 구성할 수도 있습니다.

- TPM 칩이 없는 장치에서 BitLocker를 활성화할지 여부
- BitLocker 인터페이스에 복구 옵션을 표시할지 여부
- BitLocker가 활성화되지 않은 경우 고정 또는 이동식 드라이브에 대한 쓰기 액세스를 거부할지 여부

참고:

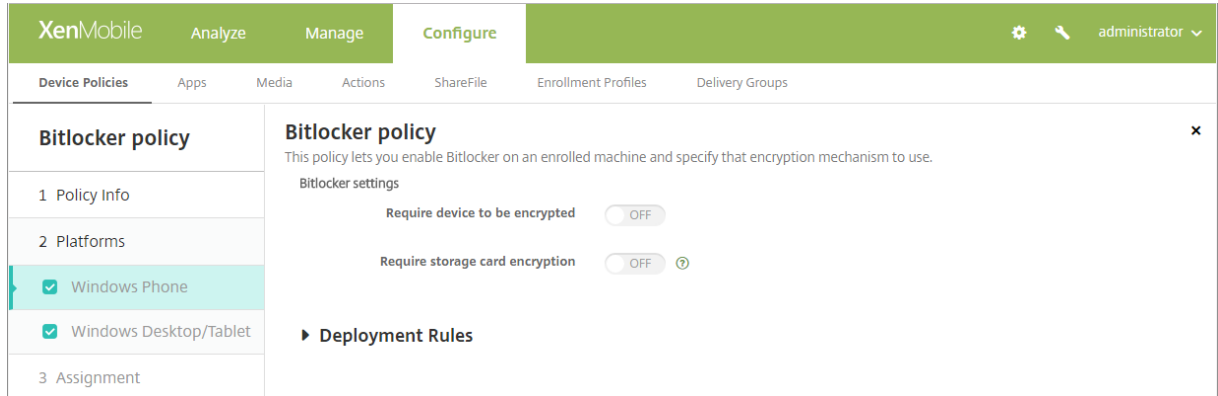
장치에서 BitLocker 암호화가 시작된 후에는 장치에 업데이트된 BitLocker 장치 정책을 배포하여 BitLocker 설정을 변경할 수 없습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

요구 사항

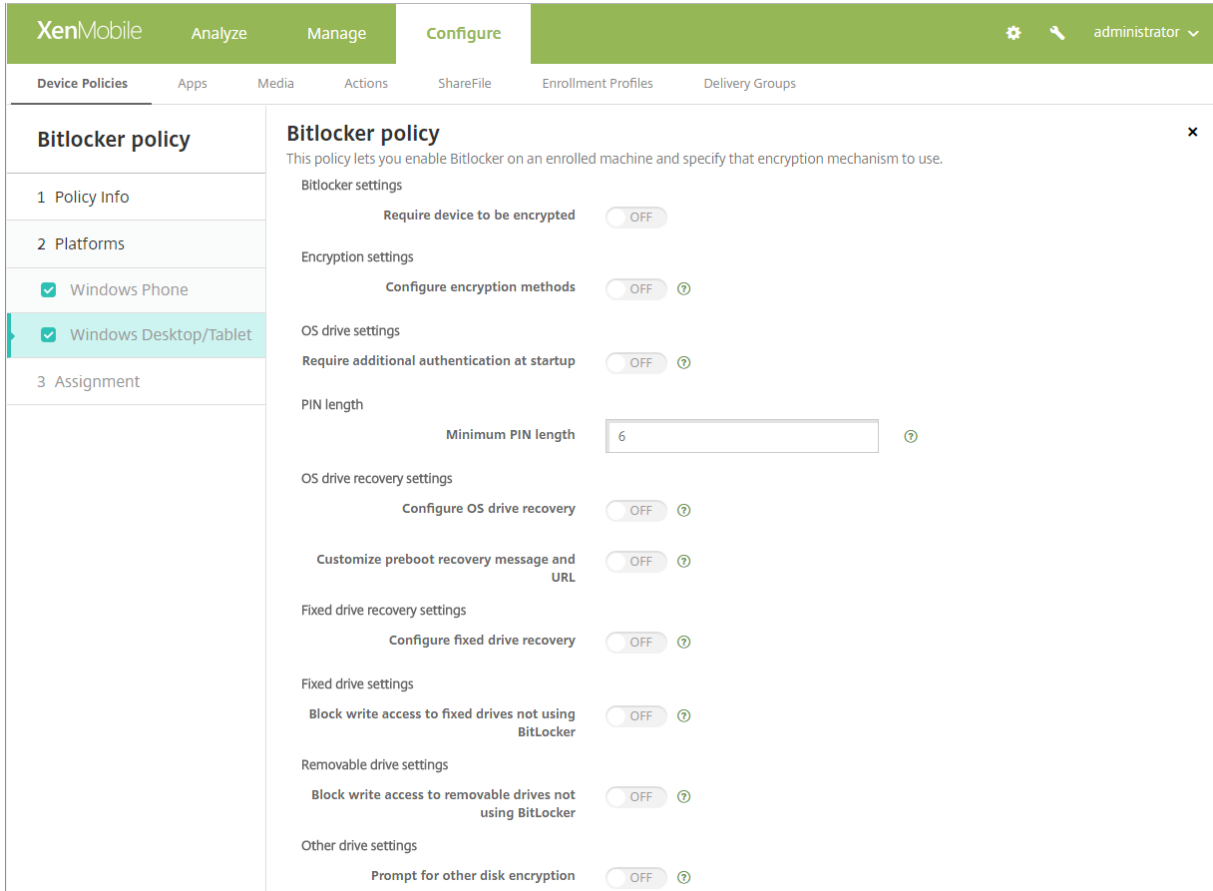
- BitLocker 장치 정책을 사용하려면 Windows 10 Enterprise 버전이 필요합니다.
- BitLocker 장치 정책을 배포하기 전에 BitLocker를 사용할 수 있도록 환경을 준비하십시오. BitLocker 시스템 요구 사항 및 설정을 포함한 Microsoft 의사 제한 정보는 [BitLocker](#) 및 해당 노드 아래의 문서를 참조하십시오.

Windows Phone 설정



- **장치암호화필요:** Windows Phone 시스템카드의 BitLocker 암호화사용설정에대한메시지를사용자에게표시할지여부를결정합니다. 꺼짐인경우등록이완료되면장치암호화가필요함을나타내는메시지가표시됩니다. 사용자가장치암호화를선택하지않으면시스템카드에대한쓰기액세스권한이제공되지않습니다. 꺼짐인경우사용자에게메시지가표시되지않으며 BitLocker 정책에따라장치의암호화여부가결정됩니다. 기본값은 꺼짐입니다.
- **스토리지카드암호화필요:** Windows Phone 스토리지카드의 BitLocker 암호화사용설정에대한메시지를사용자에게표시할지여부를결정합니다. 꺼짐인경우스토리지카드암호화를수행해야카드에대한쓰기권한이제공됩니다. 기본값은 꺼짐입니다.

Windows Desktop 및태블릿설정



- **장치암호화필요:** Windows 데스크톱 또는 태블릿의 BitLocker 암호화 사용 설정에 대한 메시지를 사용자에게 표시할지 여부를 결정합니다. 켜짐인 경우 등록이 완료되면 장치 암호화가 필요함을 나타내는 메시지가 표시됩니다. 꺼짐인 경우 사용자에게 메시지가 표시되지 않으며 BitLocker에는 정책 설정이 사용됩니다. 기본값은 꺼짐입니다.
- **암호화방법구성:** 특정 드라이브 유형에 사용할 암호화 방법을 결정합니다. 꺼짐인 경우 BitLocker 마법사에 드라이브 유형에 사용할 암호화 방법을 선택하라는 메시지가 표시됩니다. 모든 드라이브의 암호화 방법은 기본적으로 XTS-AES 128 비트입니다. 이동식 드라이브의 암호화 방법은 기본적으로 AES-CBC 128 비트입니다. 켜짐인 경우 정책에 지정된 암호화 방법이 BitLocker에 사용됩니다. 켜짐인 경우 운영체제 드라이브, 고정 드라이브 및 이동식 드라이브의 추가 설정이 나타납니다. 각 드라이브 유형에 대해 기본 암호화 방법을 선택합니다. 기본값은 꺼짐입니다.
- **시작시추가인증필요:** 장치 시작시 추가로 필요한 인증을 지정합니다. TPM 칩이 없는 장치에서 BitLocker를 허용할지 여부도 지정합니다. 꺼짐인 경우 TPM이 없는 장치에서 BitLocker 암호화를 사용할 수 없습니다. 자세한 내용은 Microsoft 문서 [TPM\(신뢰할 수 있는 플랫폼 모듈\) 기술 개요](#)를 참조하십시오. 켜짐인 경우 다음 추가 설정이 나타납니다. 기본값은 꺼짐입니다.

 - **TPM 칩이 없는 장치에서 BitLocker 차단:** TPM 칩이 없는 장치에서 BitLocker를 사용하려면 잠금 해제 암호 또는 시작키를 생성해야 합니다. 시작키는 USB 드라이브에 저장되며 사용자는 시작 전에 USB 드라이브를 장치에 연결해야 합니다. 잠금 해제 암호는 8 자 이상입니다. 기본값은 꺼짐입니다.

- **TPM 시작:** TPM 이있는장치에는 TPM 전용, TPM + PIN, TPM + 키및 TPM + PIN + 키의네가지잠금해제모드가있습니다. TPM 시작은암호화키가 TPM 칩에저장되는 TPM 전용모드를위한설정입니다. 이모드에서는사용자가추가잠금해제데이터를제공하지않아도됩니다. 사용자장치를다시시작하면 TPM 칩의암호화키를사용하여장치가자동으로잠금해제됩니다. 기본값은 **TPM** 허용입니다.
- **TPM 시작 PIN:** 이설정은 TPM + PIN 잠금해제모드입니다. PIN 은최대 20 자리일수있습니다. 최소 PIN 길이를지정하려면 최소 **PIN** 길이설정을사용합니다. PIN 은 BitLocker 를설정할때사용자가구성하며장치를시작할때이 PIN 을제공해야합니다.
- **TPM 시작키:** 이설정은 TPM + 키잠금해제모드입니다. 시작키는 USB 또는기타이동식드라이브에저장되며사용자는시작전에장치에드라이브를연결해야합니다.
- **TPM 시작키및 PIN:** 이설정은 TPM + PIN + 키잠금해제모드입니다.
잠금해제에성공하면운영체제가로딩을시작합니다. 잠금해제에실패하면장치가복구모드로전환됩니다.
- **최소 PIN 길이:** TPM 시작 PIN 의최소길이입니다. 기본값은 **6** 입니다.
- **OS 드라이브복구구성:** 잠금해제단계가실패하면 BitLocker 가구성된복구키에대한메시지를표시합니다. 이설정은잠금해제암호또는 USB 시작키가없는경우사용자에게제공되는운영체제드라이브복구옵션을구성합니다. 기본값은 꺼짐입니다.
 - **인증서기반데이터복구에이전트허용:** 인증서기반데이터복구에이전트를허용할지여부를지정합니다. GPMC(그룹정책관리콘솔) 또는로컬그룹정책편집기에위치한공개키정책에서데이터복구에이전트를추가합니다. 데이터복구에이전트에대한자세한내용은 Microsoft 문서 [BitLocker 그룹정책설정](#)을참조하십시오. 기본값은 꺼짐입니다.
 - **OS 드라이브복구용 48 비트복구암호만들기:** 사용자에게복구암호사용을허용할지, 아니면필수로할지를지정합니다. BitLocker 는암호를생성하고파일또는 Microsoft Cloud 계정에저장합니다. 기본값은 **48** 비트암호허용입니다.
 - **256 비트복구키만들기:** 복구키사용을허용할지, 아니면필수로할지를지정합니다. 복구키는 BEK 파일로, USB 드라이브에저장됩니다. 기본값은 **256** 비트복구키허용입니다.
 - **OS 드라이브복구옵션숨기기:** BitLocker 인터페이스에복구옵션을표시할지, 숨길지여부를지정합니다. 켜짐인경우 BitLocker 인터페이스에복구옵션이표시되지않습니다. 이경우장치를 Active Directory 에등록하고복구옵션을 Active Directory 에저장하고 **AD DS** 에복구정보저장을 켜짐으로설정하십시오. 기본값은 꺼짐입니다.
 - **AD DS 에복구정보저장:** Active Directory 도메인서비스에복구옵션을저장할지여부를지정합니다. 기본값은 꺼짐입니다.
 - **AD DS 에저장된복구정보구성:** BitLocker 복구암호또는복구암호및키패키지를 Active Directory 도메인서비스에저장할지여부를지정합니다. 키패키지를저장하면물리적으로손상된드라이브에서데이터를복구할수있습니다. 기본값은 복구암호백업입니다.
 - **AD DS 에복구정보저장후 BitLocker 사용:** 장치가도메인에연결되고 BitLocker 복구정보가 Active Directory 에백업된경우에만 BitLocker 를사용할수있도록할지여부를지정합니다. 켜짐인경우 BitLocker 를시작하려면장치가도메인에연결되어있어야합니다. 기본값은 꺼짐입니다.

- 사전부팅복구메시지 및 **URL** 사용자 지정: 복구 화면에 BitLocker 의 사용자 지정된 메시지 및 URL 을 표시할지 여부를 지정합니다. 켜짐인 경우 기본 복구 메시지 및 **URL** 사용, 빈 복구 메시지 및 **URL** 사용, 사용자 지정 복구 메시지 사용 및 사용자 지정 복구 **URL** 사용의 추가 설정이 나타납니다. 꺼짐인 경우 기본 복구 메시지 및 **URL** 이 표시됩니다. 기본값은 꺼짐입니다.
- 고정 드라이브 복구 구성: BitLocker 로 암호화된 고정 드라이브에 대한 사용자 복구 옵션을 구성합니다. BitLocker 는 고정 드라이브 암호화에 대한 메시지를 사용자에게 표시하지 않습니다. 시작시 드라이브 잠금을 해제하려면 사용자가 암호 또는 스마트카드를 제공해야 합니다. 사용자가 고정 드라이브의 BitLocker 암호화를 사용하도록 설정한 경우 이 정책에 포함되지 않은 시작 잠금 해제 설정이 BitLocker 인터페이스에 표시됩니다. 관련 설정에 대한 자세한 내용은 이 목록의 앞부분에 있는 **OS** 드라이브 복구 구성을 참조하십시오. 기본값은 꺼짐입니다.
- **BitLocker** 를 사용하지 않는 고정 드라이브에 대한 쓰기 액세스 차단: 켜짐인 경우 BitLocker 로 암호화된 고정 드라이브에 만 쓰기 작업을 수행할 수 있습니다. 기본값은 꺼짐입니다.
- **BitLocker** 를 사용하지 않는 이동식 드라이브에 대한 쓰기 액세스 차단: 켜짐인 경우 BitLocker 로 암호화된 이동식 드라이브에 만 쓰기 작업을 수행할 수 있습니다. 이 설정은 조직에서 다른 이동식 드라이브에 대한 쓰기 액세스를 허용하는지 여부에 따라 구성하십시오. 기본값은 꺼짐입니다.
- 다른 디스크 암호화 인 경우 메시지 표시: 장치의 다른 디스크 암호화에 대한 경고 메시지를 표시하지 않도록 설정할 수 있습니다. 기본값은 꺼짐입니다.

브라우저 장치 정책

January 6, 2020

Samsung SAFE 또는 Samsung KNOX 장치에 대한 브라우저 장치 정책을 만들어 사용자 장치에서 브라우저를 사용할 수 있는지 여부를 정의하거나 장치에서 사용할 수 있는 브라우저 기능을 제한할 수 있습니다.

Samsung 장치에서 브라우저를 완전히 사용하지 않도록 설정하거나 팝업, JavaScript, 쿠키, 자동 채우기 및 부정 행위 경고 시행을 사용하거나 사용하지 않도록 설정할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

Samsung SAFE 및 Samsung KNOX 설정

- 브라우저 사용 안 함: 사용자의 장치에서 Samsung 브라우저를 완전히 사용하지 않을지 여부를 선택합니다. 기본값은 꺼짐이고 사용자가 브라우저를 사용할 수 있습니다. 브라우저를 사용하지 않도록 설정하면 다음 옵션이 사라집니다.
- 팝업 사용 안 함: 브라우저에서 팝업 메시지를 허용할지 여부를 선택합니다.
- **Javascript** 사용 안 함: 브라우저에서 JavaScript 실행을 허용할지 여부를 선택합니다.
- 쿠키 사용 안 함: 쿠키를 허용할지 여부를 선택합니다.
- 자동 채우기 사용 안 함: 사용자가 브라우저의 자동 채우기 기능을 끄는 것을 허용할지 여부를 선택합니다.
- 부정 행위 경고 시행: 사용자가 사기를 목적으로 하는 웹사이트 또는 손상된 웹사이트를 방문할 때 경고를 표시할지 여부를 선택합니다.

캘린더 (CalDav) 장치정책

January 6, 2020

XenMobile 에서사용자의 iOS 또는 macOS 장치에캘린더 (CalDAV) 계정을추가하는장치정책을추가할수있습니다. 이정책을사용하면해당사용자가 CalDAV 를지원하는모든서버와일정데이터를동기화할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

- **계정설명:** 계정설명을입력합니다. 이것은필수필드입니다.
- **호스트이름:** CalDAV 서버의주소를입력합니다. 이것은필수필드입니다.
- **포트:** CalDAV 서버에연결하는데사용할포트를입력합니다. 이것은필수필드입니다. 기본값은 **8443** 입니다.
- **보안주체 URL:** 사용자의일정에대한기본 URL 을입력합니다.
- **사용자이름:** 사용자의로그온이름을입력합니다. 이것은필수필드입니다.
- **암호:** 선택적사용자암호를입력합니다.
- **SSL 사용:** CalDAV 서버에대한 SSL 연결을사용할것인지여부를선택합니다. 기본값은 켜짐입니다.

macOS 설정

- **계정설명:** 계정설명을입력합니다. 이것은필수필드입니다.
- **호스트이름:** CalDAV 서버의주소를입력합니다. 이것은필수필드입니다.
- **포트:** CalDAV 서버에연결하는데사용할포트를입력합니다. 이것은필수필드입니다. 기본값은 **8443** 입니다.
- **보안주체 URL:** 사용자의일정에대한기본 URL 을입력합니다.
- **사용자이름:** 사용자의로그온이름을입력합니다. 이것은필수필드입니다.
- **암호:** 선택적사용자암호를입력합니다.
- **SSL 사용:** CalDAV 서버에대한 SSL 연결을사용할것인지여부를선택합니다. 기본값은 켜짐입니다.

셀룰러장치정책

January 6, 2020

이정책을사용하면 iOS 장치에대한셀룰러네트워크설정을구성할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

- **APN 연결**

- 이름: 이구성의이름입니다.
- 인증유형: 목록에서 **CHAP**(Challenge Handshake 인증프로토콜) 또는 **PAP**(암호인증프로토콜) 를클릭합니다. 기본값은 **PAP** 입니다.
- 사용자이름및 암호: 인증에사용할사용자이름과암호입니다.

- **APN**

- 이름: APN(엑세스포인트이름) 구성의이름입니다.
- 인증유형: 목록에서 **CHAP** 또는 **PAP** 를클릭합니다. 기본값은 **PAP** 입니다.
- 사용자이름및 암호: 인증에사용할사용자이름과암호입니다.
- 프록시서버: 프록시서버네트워크주소입니다.
- 프록시서버포트: 프록시서버포트입니다.

연결관리자장치정책

January 6, 2020

XenMobile 에서인터넷및사설망에자동으로연결되는앱에대한연결설정을지정할수있습니다. 이정책은 Windows Pocket PC 에서만사용할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Windows Mobile/CE 설정

참고:

기본제공사무실은모두회사인트라넷에연결되어있음을의미합니다. 기본제공인터넷은모두인터넷에연결되어있음을의미합니다.

- 사설망에연결되는앱이자동으로사용: 목록에서 기본제공사무실또는 기본제공인터넷을클릭합니다. 기본값은 기본제공사무실입니다.
- 인터넷에연결되는앱이자동으로사용: 목록에서 기본제공사무실또는 기본제공인터넷을클릭합니다. 기본값은 기본제공사무실입니다.

연결예약장치정책

January 6, 2020

중요:

FCM(Firebase Cloud Messaging) 을 사용하여 Android, Android Enterprise 및 Chrome OS 장치의 Xen-Mobile Server 연결을 제어하는 것이 좋습니다. FCM 사용에 대한 자세한 내용은 [Firebase Cloud Messaging](#)을 참조하십시오.

FCM 을 사용하지 않도록 선택한 경우 연결 예약 정책을 만들어 사용자 장치에서 XenMobile Server 에 연결하는 방법과 시기를 제어할 수 있습니다.

사용자가 수동으로 장치에 연결하거나 장치가 정의된 시간 내에 연결하도록 지정할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

플랫폼 설정

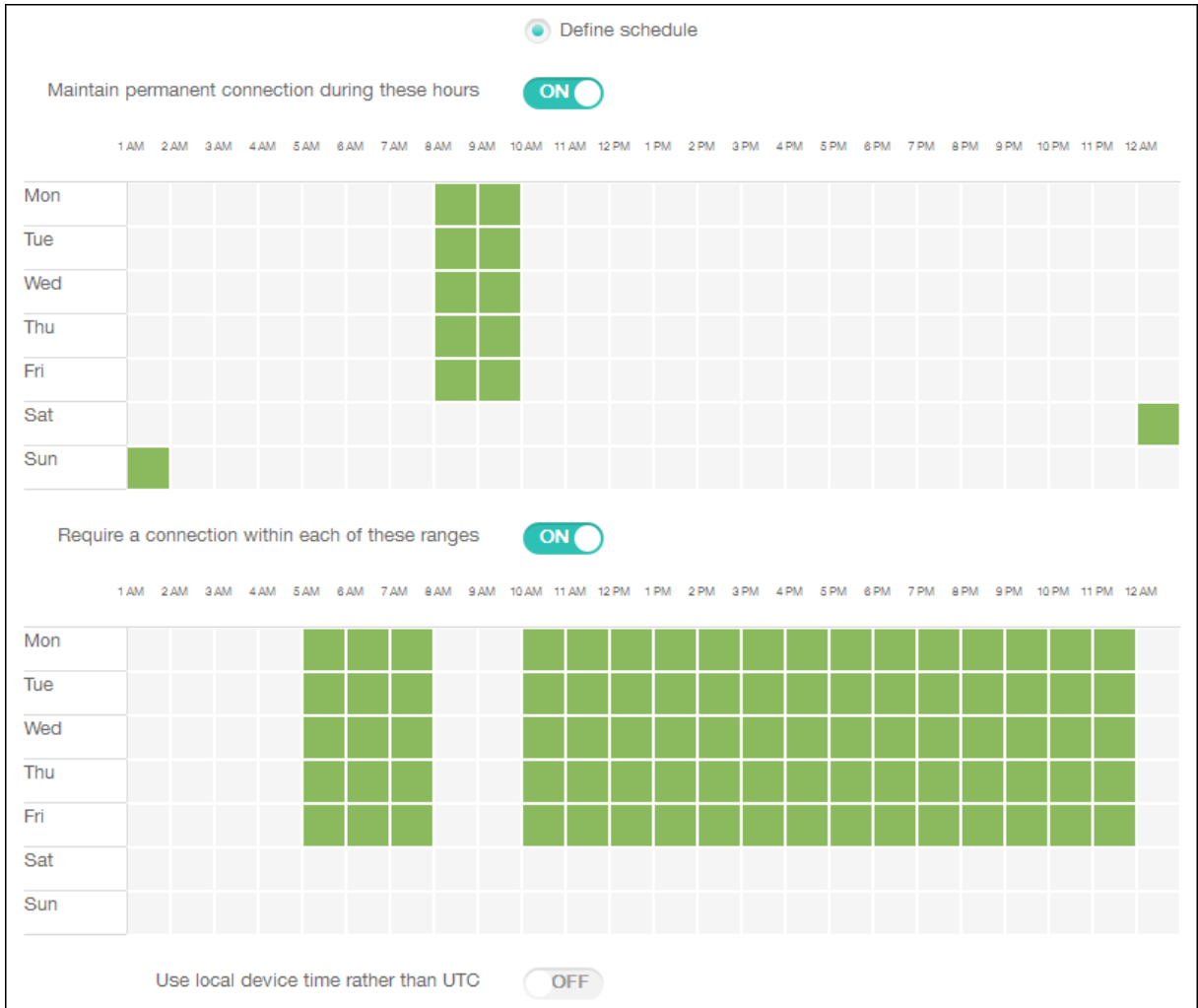
- 장치에서 연결하도록 요구: 이 설정에 대해 설정할 옵션을 클릭합니다.
 - **항상:** 연결을 영구적으로 활성화 상태로 유지합니다. 네트워크 연결이 끊긴 후 사용자 장치의 XenMobile 이 XenMobile 서버에 다시 연결을 시도하고 제어 패킷을 정기적으로 전송하여 연결을 모니터링합니다. 보안을 최적화하려면 이 옵션을 사용하는 것이 좋습니다.항상을 선택하는 경우 장치 터널 정책인 연결 시간 제한 정의 설정을 사용하여 연결로 인해 배터리가 소진되지 않도록 하십시오. 연결을 활성화 상태로 유지하면 초기화 또는 잠금과 같은 보안 명령을 주문형으로 장치에 푸시할 수 있습니다. 또한 장치에 배포하는 각 정책에서 배포 일정 옵션 상시 연결에 대해 배포를 선택해야 합니다.
 - **안함:** 수동으로 연결합니다. 사용자가 장치의 XenMobile 에서 연결을 시작해야 합니다. 이 옵션을 사용하면 보안 정책을 장치에 배포할 수 없어 사용자가 새 앱 또는 정책을 받을 수 없으므로 프로덕션 배포에 사용하지 않는 것이 좋습니다.
 - **간격:** 지정된 간격으로 연결합니다. 이 옵션이 적용될 때 잠금 또는 초기화 와 같은 보안 정책을 전송하면 다음에 장치가 연결할 때 동작이 처리됩니다. 이 옵션을 선택하면 **N** 분마다 연결 필드 가 나타납니다. 이 필드에 장치를 다시 연결하기 전까지의 시간 (분) 을 입력해야 합니다. 기본값은 **20** 입니다.
 - **일정 정의:** 사용하면 네트워크 연결이 끊긴 후 사용자 장치의 XenMobile 이 XenMobile 서버에 다시 연결을 시도하고 제어 패킷을 정의된 시간 내에 정기적으로 전송하여 연결을 모니터링합니다. 연결 시간을 정의하는 방법은 다음에 나오는 연결 시간 정의를 참조하십시오.
 - * 다음 시간 동안 고정된 연결 유지: 사용자 장치가 정의된 시간 동안 연결되어야 합니다.
 - * 다음 각 범위 내에서 연결하도록 요구: 사용자 장치가 정의된 시간 동안 한 번 이상 연결되어야 합니다.
 - * **UTC** 가 아닌 로컬 장치 시간 사용: 정의된 시간을 UTC(협정 세계시) 가 아닌 로컬 장치 시간과 동기화합니다.

연결 시간 정의

다음 옵션을 사용하면 원하는 시간을 정의할 수 있는 시간 표시 줄이 나타납니다. 특정 시간 동안 영구적으로 연결하도록 하거나 특정 시간에 연결하도록 하는 옵션 중에서 하나를 선택하거나 둘 다를 선택할 수 있습니다. 시간 표시 줄의 각 사각형은 30 분입니다. 주중 오전 8 시부터 오전 9 시 사이에 연결하도록 하려면 주중 오전 8 시와 오전 9 시 사이의 시간 표시 줄 사각형 두 개를 클릭합니다.

예를 들어 다음 그림에서 시간 표시 줄 2 개는 주중 오전 8 시부터 오전 9 시까지 영구적으로 연결해야 하고 토요일 오전 12 시부터 일요일 오전 1 시까지 영구적으로 연결해야 하며 주중 매일 오전 5 시부터 오전 8 시 또는 오전 10 시부터 오후 11 시 사이에 한 번 이상 연결해야 함

을 나타냅니다.



연락처 (CardDAV) 장치정책

January 6, 2020

XenMobile 에서장치정책을추가하여 iOS 연락처 (CardDAV) 계정을사용자의 iOS 또는 macOS 장치에추가하고이러한장치의연락처데이터를 CardDAV 를지원하는모든서버와동기화할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

- **계정설명:** 계정설명을입력합니다. 이것은필수필드입니다.
- **호스트이름:** CardDAV 서버의주소를입력합니다. 이것은필수필드입니다.

- 포트: CardDAV 서버를연결할포트를입력합니다. 이것은필수필드입니다. 기본값은 **8443** 입니다.
- 보안주체 **URL**: 사용자의일정에대한기본 URL 을입력합니다.
- 사용자이름: 사용자의로그온이름을입력합니다. 이것은필수필드입니다.
- 암호: 선택적사용자암호를입력합니다.
- **SSL** 사용: CardDAV 서버에대한 Secure Socket Layer 연결을사용할지여부를선택합니다. 기본값은 켜짐입니다.

macOS 설정

- 계정설명: 계정설명을입력합니다. 이것은필수필드입니다.
- 호스트이름: CardDAV 서버의주소를입력합니다. 이것은필수필드입니다.
- 포트: CardDAV 서버를연결할포트를입력합니다. 이것은필수필드입니다. 기본값은 **8443** 입니다.
- 보안주체 **URL**: 사용자의일정에대한기본 URL 을입력합니다.
- 사용자이름: 사용자의로그온이름을입력합니다. 이것은필수필드입니다.
- 암호: 선택적사용자암호를입력합니다.
- **SSL** 사용: CardDAV 서버에대한 Secure Socket Layer 연결을사용할지여부를선택합니다. 기본값은 켜짐입니다.

OS 업데이트제어장치정책

January 6, 2020

OS 업데이트제어장치정책을사용하여다음을배포할수있습니다.

- 감독되는 iOS 장치에최신 OS 업데이트를배포할수있습니다.

iOS 10.3 이상을실행하는장치의경우 OS 업데이트제어정책이감독되는장치에서만작동합니다. iOS 10.3 이전버전을실행하는장치의경우 OS 업데이트제어정책이감독되는장치와 DEP 등록장치에서모두작동합니다.

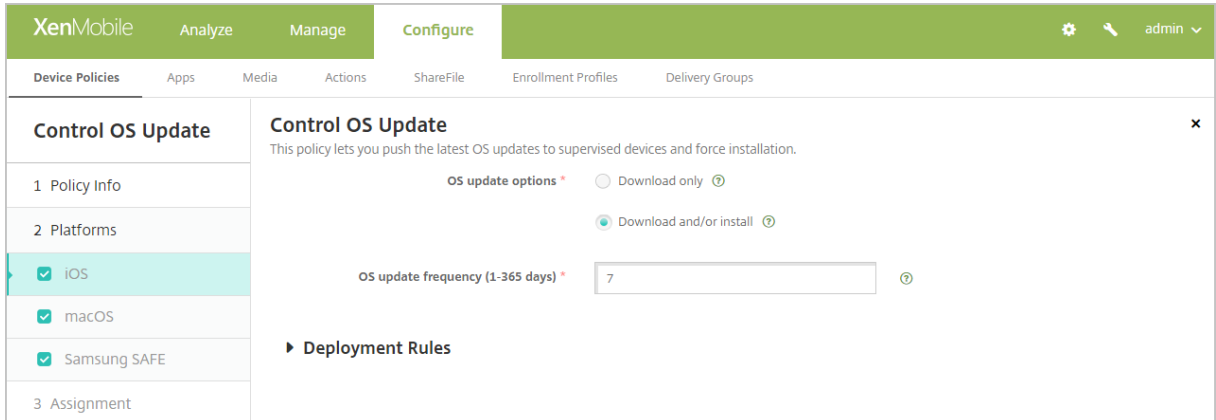
- macOS 10.11.5 이상을실행하는 DEP 등록 macOS 장치에최신 OS 및앱업데이트를배포할수있습니다.

- 감독되는 Samsung SAFE 장치에최신 OS 업데이트를배포할수있습니다.

Samsung SAFE 장치의경우 XenMobile 이 OS 업데이트제어정책을 Secure Hub 로전송하면 Secure Hub 가장치에정책을적용합니다. XenMobile Server 가정책을전송하고장치에정책이수신되면 관리 > 장치페이지가표시됩니다.

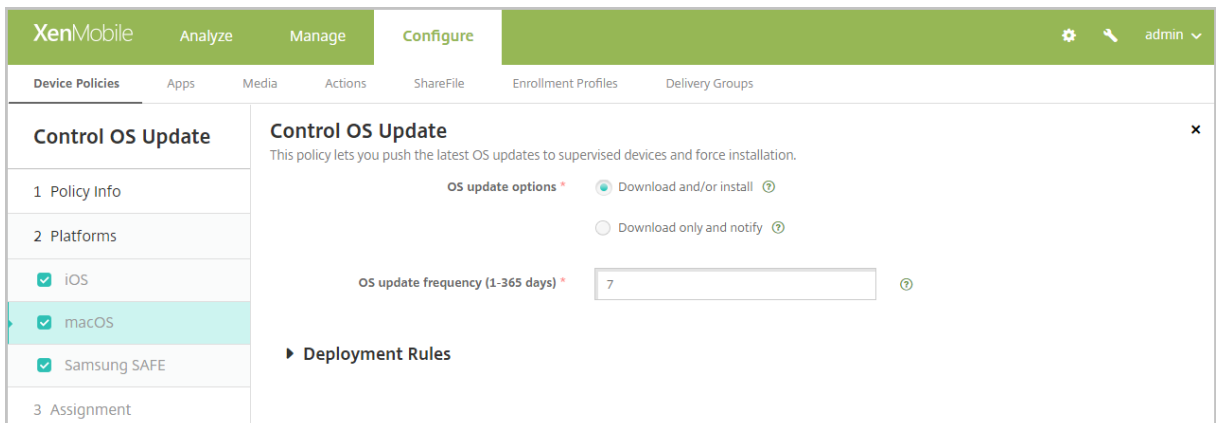
이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정



- **OS 업데이트옵션:** 두 옵션 모두 OS 업데이트 빈도에 따라 최신 OS 업데이트를 감독되는 장치에 다운로드합니다. 장치에 업데이트를 설치하라는 메시지가 표시됩니다. 이 메시지는 사용자가 장치를 잠금 해제한 후 표시됩니다.
- **OS 업데이트 빈도:** XenMobile 이 장치 OS 를 확인하고 업데이트 할 빈도를 결정합니다. 기본값은 7 일입니다.

macOS 설정



- **OS 업데이트 옵션:** 두 옵션 모두 OS 업데이트 빈도에 따라 최신 macOS 업데이트를 다운로드합니다. 선택에 따라, 업데이트를 설치하거나 App Store 를 통해 업데이트를 사용할 수 있음을 사용자에게 알릴 수 있습니다.
- **OS 업데이트 빈도:** XenMobile 이 장치 OS 를 확인하고 업데이트 할 빈도를 결정합니다. 기본값은 7 일입니다.

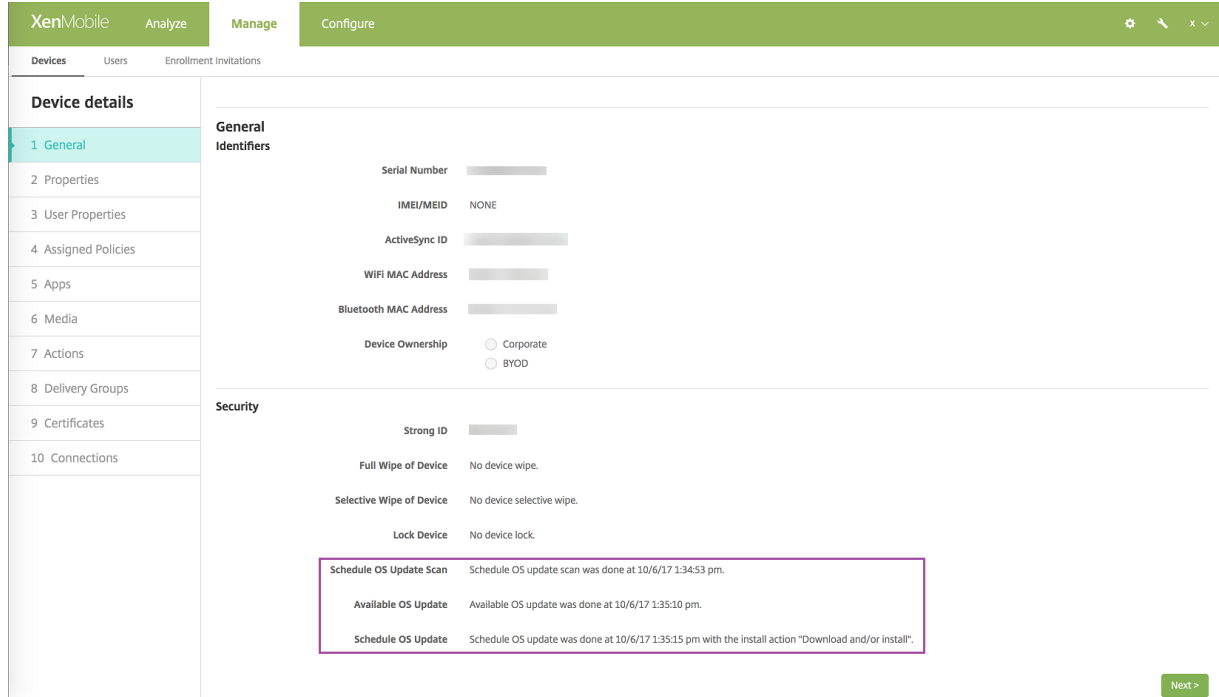
iOS 및 macOS 업데이트 작업의 상태 확인

iOS 및 macOS 의 경우 XenMobile 이 OS 업데이트 제어 정책을 장치에 배포하지 않습니다. 대신 XenMobile 은 정책을 사용하여 다음과 같은 MDM 명령을 장치에 전송합니다.

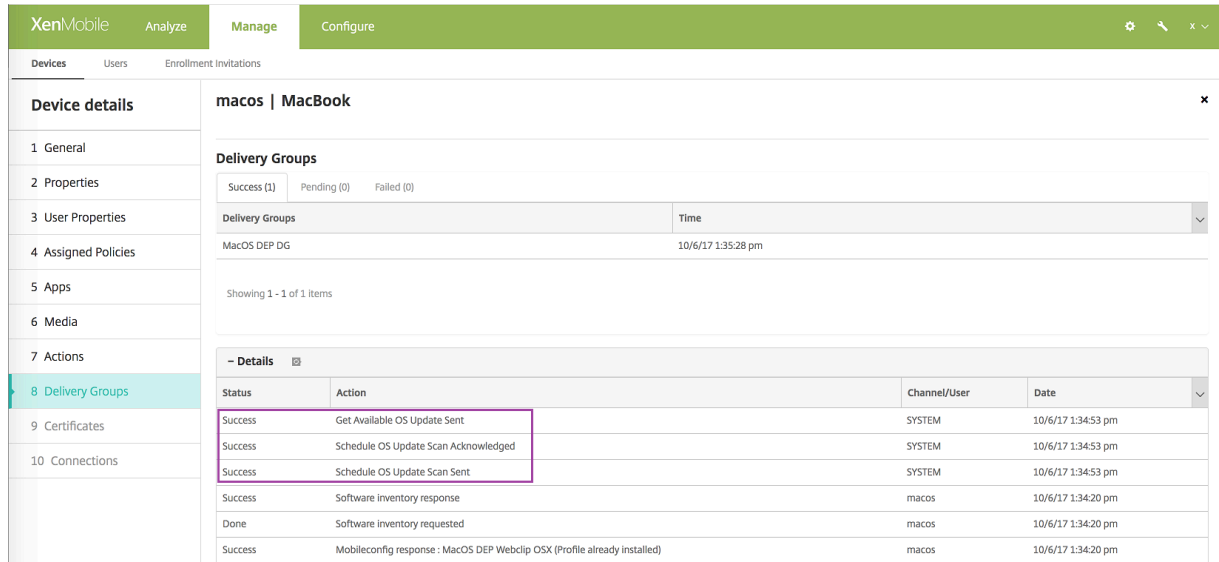
- OS 업데이트 검사 예약: OS 업데이트에 대한 백그라운드 검사를 수행하도록 장치에 요청합니다 (iOS 의 경우 선택 사항).
- 사용 가능한 OS 업데이트: 장치를 관리하여 사용 가능한 OS 업데이트 목록을 확인합니다.

- OS 업데이트예약: macOS 업데이트, 앱업데이트또는둘다를수행하도록장치에요청합니다. OS 및앱업데이트를다운로드하거나설치하는시기는장치 OS 에따라결정됩니다.

관리 > 장치 > 장치세부정보 (일반) 페이지에예약된 OS 업데이트검사와사용가능한 OS 업데이트검사, 예약된 macOS 및앱업데이트의상태가표시됩니다.



업데이트작업의상태에대한자세한내용을보려면 관리 > 장치 > 장치세부정보 (배달그룹) 페이지로이동합니다.



사용가능한 OS 업데이트및마지막설치시도등의세부정보를보려면 관리 > 장치 > 장치세부정보 (속성) 페이지로이동합니다.

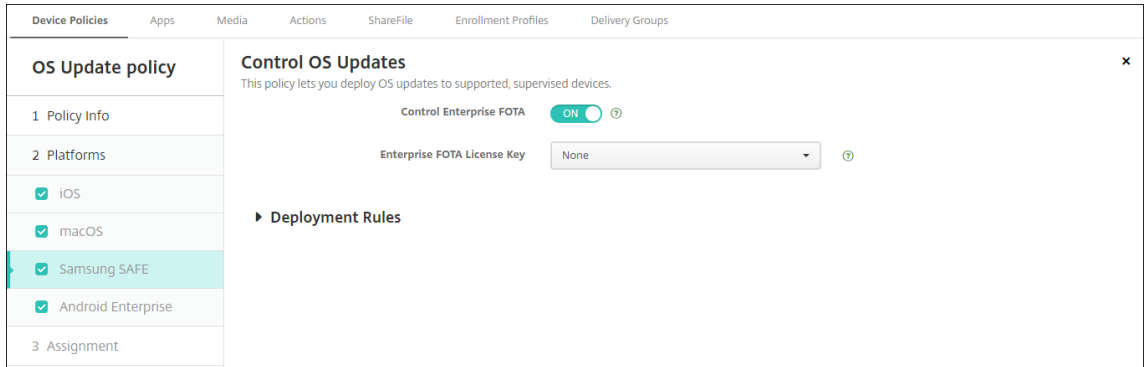
XenMobile		Analyze	Manage	Configure																														
Devices Users Enrollment Invitations																																		
Device details		<table border="1"> <tr><td>DEP account name</td><td>DEP Account FR</td></tr> <tr><td>DEP profile assigned</td><td>10/6/17 1:08:16 pm</td></tr> <tr><td>DEP profile pushed</td><td>10/6/17 1:08:16 pm</td></tr> <tr><td>DEP registration by</td><td>[redacted]@outlook.com</td></tr> <tr><td>DEP registration date</td><td>1/20/17 4:42:06 pm</td></tr> <tr><td>Description</td><td>MB 12.0 SPACE GRAY/1.1GHZ/8GB/256GB-FRA</td></tr> <tr><td>Device model</td><td>MacBook</td></tr> <tr><td>Device name</td><td>FranckD MacBook</td></tr> <tr><td>Model ID</td><td>MacBook8,1</td></tr> <tr><td>OS Update Install Failure Message</td><td></td></tr> <tr><td>OS Update Install Status</td><td>Success</td></tr> <tr><td>OS Update Is Critical</td><td>No</td></tr> <tr><td>OS Update Last Install Attempt</td><td>10/6/17 1:35:15 pm</td></tr> <tr><td>OS Update Version</td><td>macOS Sierra Update, iTunes</td></tr> <tr><td>Operating system build</td><td>16B2657</td></tr> </table>			DEP account name	DEP Account FR	DEP profile assigned	10/6/17 1:08:16 pm	DEP profile pushed	10/6/17 1:08:16 pm	DEP registration by	[redacted]@outlook.com	DEP registration date	1/20/17 4:42:06 pm	Description	MB 12.0 SPACE GRAY/1.1GHZ/8GB/256GB-FRA	Device model	MacBook	Device name	FranckD MacBook	Model ID	MacBook8,1	OS Update Install Failure Message		OS Update Install Status	Success	OS Update Is Critical	No	OS Update Last Install Attempt	10/6/17 1:35:15 pm	OS Update Version	macOS Sierra Update, iTunes	Operating system build	16B2657
DEP account name	DEP Account FR																																	
DEP profile assigned	10/6/17 1:08:16 pm																																	
DEP profile pushed	10/6/17 1:08:16 pm																																	
DEP registration by	[redacted]@outlook.com																																	
DEP registration date	1/20/17 4:42:06 pm																																	
Description	MB 12.0 SPACE GRAY/1.1GHZ/8GB/256GB-FRA																																	
Device model	MacBook																																	
Device name	FranckD MacBook																																	
Model ID	MacBook8,1																																	
OS Update Install Failure Message																																		
OS Update Install Status	Success																																	
OS Update Is Critical	No																																	
OS Update Last Install Attempt	10/6/17 1:35:15 pm																																	
OS Update Version	macOS Sierra Update, iTunes																																	
Operating system build	16B2657																																	
1 General																																		
2 Properties																																		
3 User Properties																																		
4 Assigned Policies																																		
5 Apps																																		
6 Media																																		
7 Actions																																		
8 Delivery Groups																																		
9 Certificates																																		
10 Connections																																		

XenMobile		Analyze	Manage	Configure																																				
Devices Users Enrollment Invitations																																								
Device details		<table border="1"> <tr> <th colspan="2">Properties</th> <th>Add</th> </tr> <tr> <td colspan="3">- Custom</td> </tr> <tr> <td>AutoCheckEnabled</td> <td>true</td> <td></td> </tr> <tr> <td>AutomaticAppInstallationEnabled</td> <td>false</td> <td></td> </tr> <tr> <td>AutomaticOSInstallationEnabled</td> <td>false</td> <td></td> </tr> <tr> <td>AutomaticSecurityUpdatesEnabled</td> <td>true</td> <td></td> </tr> <tr> <td>BackgroundDownloadEnabled</td> <td>true</td> <td></td> </tr> <tr> <td>CatalogURL</td> <td>https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-snowleopard-leopard.merged-1.sucatalog.gz</td> <td></td> </tr> <tr> <td>IsDefaultCatalog</td> <td>true</td> <td></td> </tr> <tr> <td>PerformPeriodicCheck</td> <td>true</td> <td></td> </tr> <tr> <td>PreviousScanDate</td> <td>2017-10-06T11:28:41Z</td> <td></td> </tr> <tr> <td>PreviousScanResult</td> <td>0</td> <td></td> </tr> </table>			Properties		Add	- Custom			AutoCheckEnabled	true		AutomaticAppInstallationEnabled	false		AutomaticOSInstallationEnabled	false		AutomaticSecurityUpdatesEnabled	true		BackgroundDownloadEnabled	true		CatalogURL	https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-snowleopard-leopard.merged-1.sucatalog.gz		IsDefaultCatalog	true		PerformPeriodicCheck	true		PreviousScanDate	2017-10-06T11:28:41Z		PreviousScanResult	0	
Properties		Add																																						
- Custom																																								
AutoCheckEnabled	true																																							
AutomaticAppInstallationEnabled	false																																							
AutomaticOSInstallationEnabled	false																																							
AutomaticSecurityUpdatesEnabled	true																																							
BackgroundDownloadEnabled	true																																							
CatalogURL	https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-snowleopard-leopard.merged-1.sucatalog.gz																																							
IsDefaultCatalog	true																																							
PerformPeriodicCheck	true																																							
PreviousScanDate	2017-10-06T11:28:41Z																																							
PreviousScanResult	0																																							
1 General																																								
2 Properties																																								
3 User Properties																																								
4 Assigned Policies																																								
5 Apps																																								
6 Media																																								
7 Actions																																								
8 Delivery Groups																																								
9 Certificates																																								
10 Connections																																								

Samsung SAFE 설정

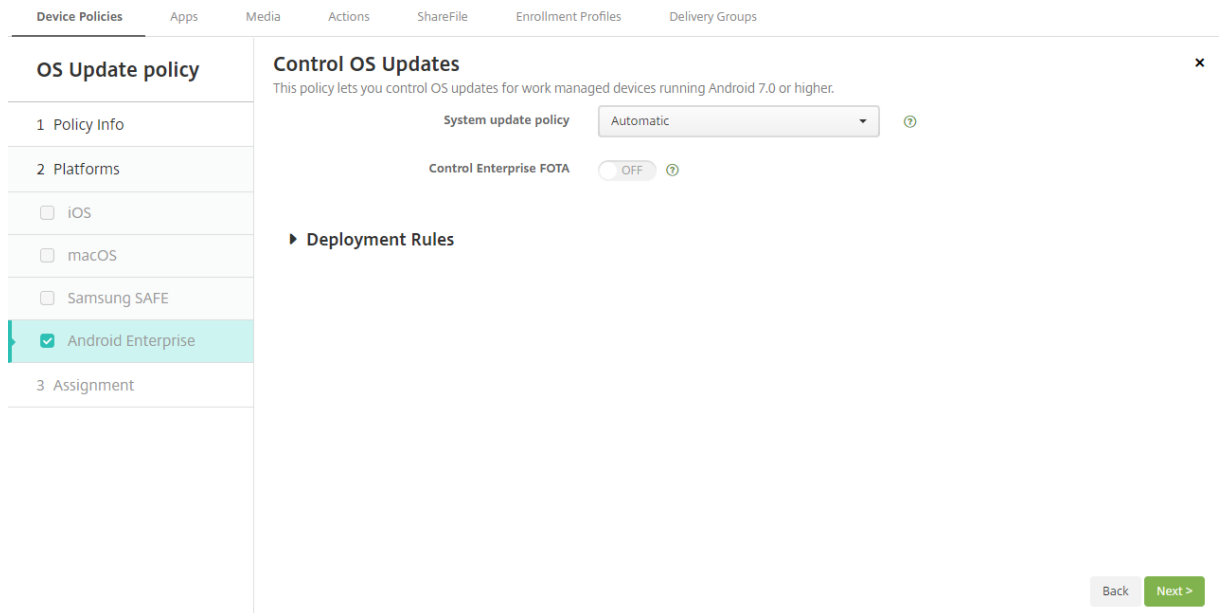
Samsung E-FOTA(Enterprise FOTA) 는 장치의 업데이트 시기 및 사용할 펌웨어 버전을 알려줍니다. E-FOTA 를 사용하려면:

1. Samsung 에서 받은 키 및 라이선스 정보를 사용하여 Samsung MDM 라이선스 키 장치 정책을 만듭니다. 자세한 내용은 [Samsung MDM 라이선스 키 장치 정책](#) 에서 참조하십시오.
2. Enterprise FOTA 를 사용하려면 OS 업데이트 제어 장치 정책을 만듭니다.



- **Enable Enterprise FOTA(Enterprise FOTA 사용):** 켜짐으로설정합니다.
- **Enterprise FOTA 라이선스키:** Samsung MDM 라이선스키장치정책이름을선택합니다.

Android Enterprise 설정



- **시스템업데이트정책.** 시스템업데이트시기를결정합니다. 자동은업데이트를사용할수있을때설치합니다. 기간내는 시작시간과 종료시간에지정된일일유지관리기간내에업데이트를자동으로설치합니다. 연기의경우사용자가최대 30 일까지업데이트를연기할수있습니다.
 - 시작시간. 유지관리기간의시작시간으로, 장치의로컬시간을기준으로자정이후의분수 (**0~1440**) 로측정됩니다. 기본값은 **0** 입니다.
 - 종료시간. 유지관리기간의종료시간으로, 장치의로컬시간을기준으로자정이후의분수 (**0~1440**) 로측정됩니다. 기본값은 **120** 입니다.
- **Enterprise FOTA 제어.** Samsung Enterprise FOTA(Firmware-Over-the-Air) 서비스를사용하는 Samsung 장치에대한업데이트를제어할수있습니다. Samsung Knox 3.0 이상을실행하는 Android Enterprise 장치를위한설정입니다. 기본값은 꺼짐입니다.

- **Enterprise FOTA** 라이선스키. **Enterprise FOTA** 제어가 켜짐인 경우 **Enterprise FOTA** 라이선스키에서 Samsung FOTA 업데이트에 사용할 라이선스키를 지정할 수 있습니다. Samsung Knox 3.0 이상을 실행하는 Android Enterprise 장치를 위한 설정입니다. 기본값은 없습니다. **Samsung MDM** 라이선스키 장치 정책을 사용하여 키를 설정할 수 있습니다. [Samsung MDM 라이선스키 장치 정책](#)에서 자세한 내용을 참조하십시오.

Samsung 컨테이너에 앱 복사 장치 정책

January 6, 2020

장치에 이미 설치된 앱의 경우 해당 앱을 지원되는 Samsung 장치에서 SEAMS 컨테이너 또는 KNOX 컨테이너로 복사하도록 지정할 수 있습니다. 지원되는 장치에 대한 자세한 내용은 Samsung 문서 [Knox에서 구축한 디바이스](#)를 참조하십시오.

SEAMS 컨테이너에 복사된 앱은 사용자의 홈 화면에서 사용할 수 있습니다. KNOX 컨테이너에 복사된 앱은 사용자가 KNOX 컨테이너에 로그인하는 경우에만 사용할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

사전 요구 사항

- XenMobile 에장치를 등록합니다.
- Samsung MDM 키 (ELM 및 KLM) 를 배포합니다. 이 작업을 수행하는 방법은 [Samsung MDM 라이선스키 장치 정책](#)을 참조하십시오.
- 장치에 앱을 설치합니다.
- 장치에서 KNOX 를 초기화하여 앱을 KNOX 컨테이너에 복사합니다.

플랫폼 설정

- 새 앱: 목록에 추가하려는 각 앱에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 패키지 ID 를 입력합니다 (예: LacingArt 앱의 경우 com.mobiwolf.lacingart).
 - 저장 또는 취소를 클릭합니다.

자격 증명 장치 정책

January 6, 2020

XenMobile 에서 자격 증명 장치 정책을 만들어 PKI 엔터티, 키 저장소, 자격 증명 공급자 또는 서버 인증서와 같은 XenMobile 의 PKI 구성과 통합된 인증을 사용할 수 있습니다. 자격 증명에 대한 자세한 내용은 [인증서 및 인증](#) 문서를 참조하십시오.

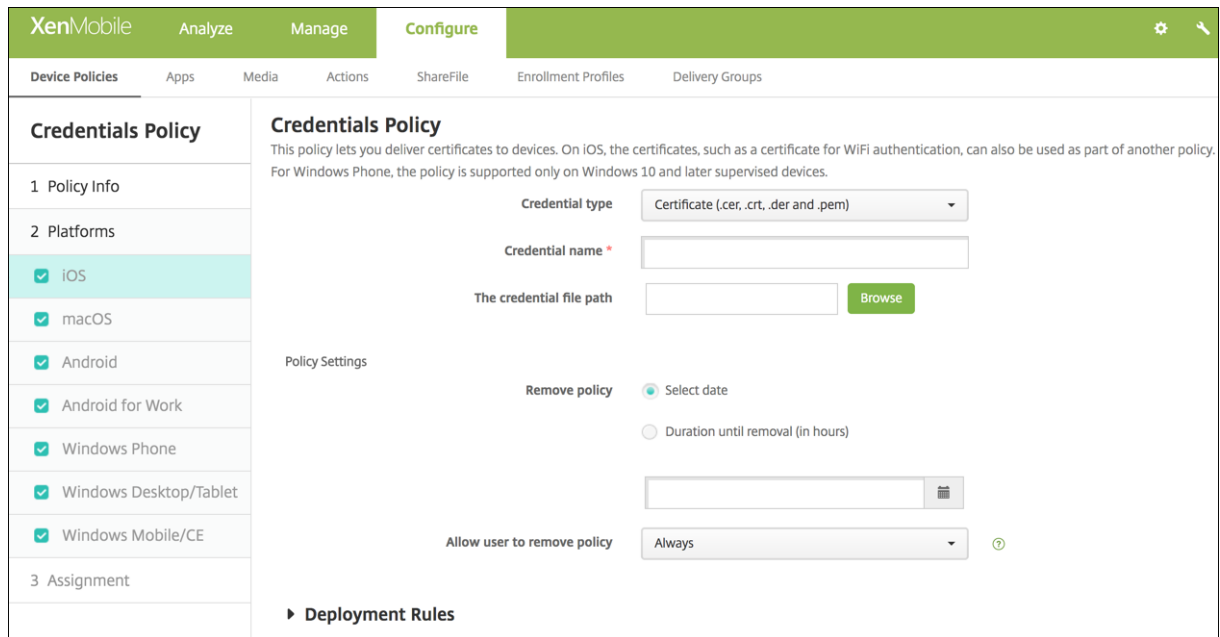
iOS, macOS, Android, Android Enterprise, Windows Desktop/Tablet, Windows Mobile/CE 및 Windows Phone 장치에 대한 자격 증명 정책을 만들 수 있습니다. 각 플랫폼마다 문서에서 설명되어 있는 서로 다른 값 집합이 필요합니다.

참고:

이 정책을 만들기 전에 각 플랫폼에서 사용할 자격 증명 정보와 모든 인증서 및 암호가 필요합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정



다음 설정을 구성합니다.

- 자격 증명 유형: 목록에서 이 정책에서 사용할 자격 증명 유형을 클릭하고 선택한 자격 증명에 대해 다음 정보를 입력합니다.
 - 인증서
 - * 자격 증명 이름: 자격 증명의 고유 이름을 입력합니다.
 - * 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - 키저장소
 - * 자격 증명 이름: 자격 증명의 고유 이름을 입력합니다.
 - * 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.
 - * 암호: 자격 증명에 대한 키저장소 암호를 입력합니다.
 - 서버인증서
 - * 서버인증서: 목록에서 사용할 인증서를 클릭합니다.
 - 자격 증명 공급자
 - * 자격 증명 공급자: 목록에서 자격 증명 공급자의 이름을 클릭합니다.

macOS 설정

Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

1 Policy Info

2 Platforms

- iOS
- macOS
- Android
- Android for Work
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

3 Assignment

Policy Settings

Credential type: Certificate (.cer, .crt, .der and .pem)

Credential name *: [Text Input]

The credential file path: [Text Input] **Browse**

Remove policy: Select date Duration until removal (in hours)

[Text Input] [Calendar Icon]

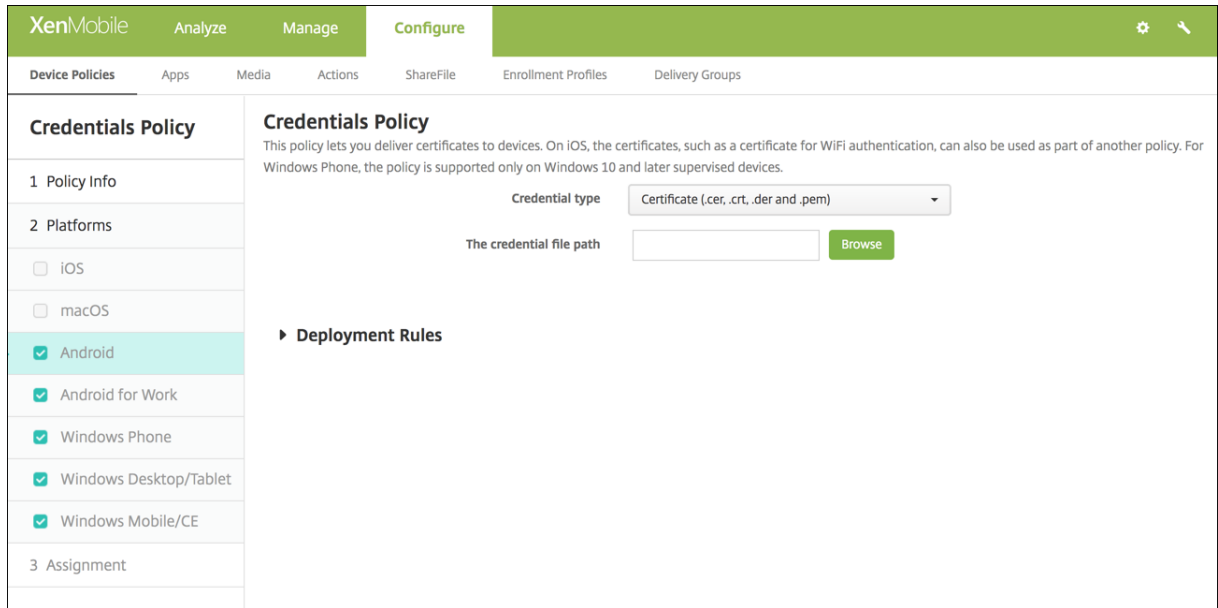
Allow user to remove policy: Always [Help Icon]

Profile scope: User macOS 10.7+

다음설정을구성합니다.

- 자격증명유형: 목록에서이정책에사용할자격증명유형을클릭하고선택한자격증명에대해다음정보를입력합니다.
 - 인증서
 - * 자격증명이름: 자격증명의고유한이름을입력합니다.
 - * 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
 - 키저장소
 - * 자격증명이름: 자격증명의고유한이름을입력합니다.
 - * 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
 - * 암호: 자격증명에대한키저장소암호를입력합니다.
 - 서버인증서
 - * 서버인증서: 목록에서사용할인증서를클릭합니다.
 - 자격증명공급자
 - * 자격증명공급자: 목록에서자격증명공급자의이름을클릭합니다.

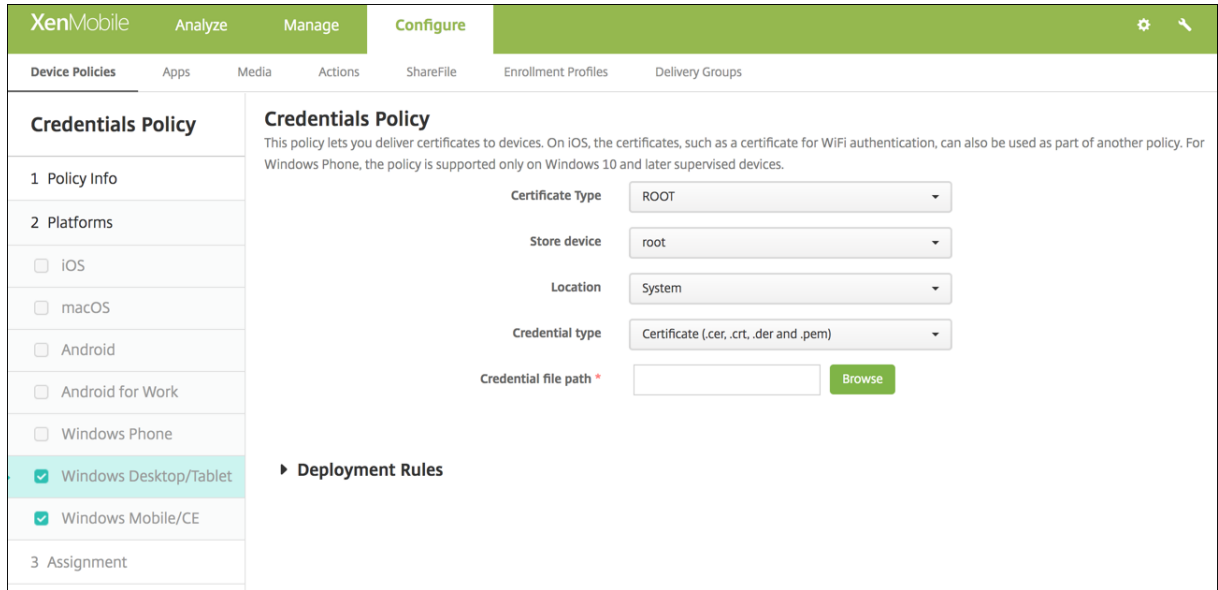
Android 및 Android Enterprise 설정



다음설정을구성합니다.

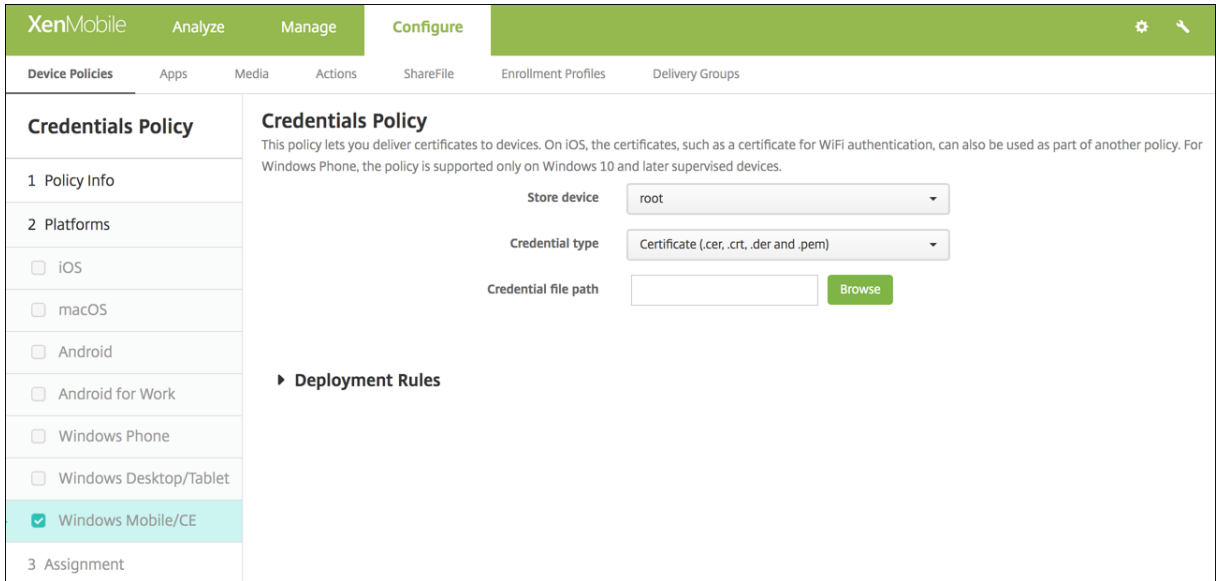
- 자격증명유형: 목록에서이정책에사용할자격증명유형을클릭하고선택한자격증명에대해다음정보를입력합니다.
 - 인증서
 - * 자격증명이름: 자격증명의고유한이름을입력합니다.
 - * 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
 - 키저장소
 - * 자격증명이름: 자격증명의고유한이름을입력합니다.
 - * 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
 - * 암호: 자격증명에대한키저장소암호를입력합니다.
 - 서버인증서
 - * 서버인증서: 목록에서사용할인증서를클릭합니다.
 - 자격증명공급자
 - * 자격증명공급자: 목록에서자격증명공급자의이름을클릭합니다.

Windows 데스크톱/태블릿설정



- 인증서유형: 목록에서 루트또는 클라이언트를클릭합니다.
- 루트를클릭하는경우다음설정을구성합니다.
 - 스토어장치: 목록에서자격증명의인증서저장소위치로 루트, 내또는 **CA** 를클릭합니다. 내의경우사용자의인증서저장소에인증서가저장됩니다.
 - 위치: Windows 10 태블릿의경우 시스템이유일한위치입니다.
 - 자격증명유형: Windows 10 태블릿의경우 인증서가유일한자격증명유형입니다.
 - 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여인증서파일을선택합니다.
- 클라이언트를클릭하는경우다음설정을구성합니다.
- 위치: Windows 10 태블릿의경우 시스템이유일한위치입니다.
- 자격증명유형: Windows 10 태블릿의경우 키저장소가유일한자격증명유형입니다.
- 자격증명이름: 자격증명의이름을입력합니다. 이것은필수필드입니다.
- 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여인증서파일을선택합니다.
- 암호: 자격증명과관련된암호를입력합니다. 이것은필수필드입니다.

Windows Mobile/CE 설정



- 스토어장치: 목록에서 자격증명의 인증서 저장소 위치를 클릭합니다. 기본값은 루트입니다. 옵션은 다음과 같습니다.
 - 권한 있는 실행 신뢰 기관: 이 저장소에 속한 인증서로서 명된 응용 프로그램은 권한 있는 신뢰 수준으로 실행됩니다.
 - 권한 없는 실행 신뢰 기관: 이 저장소에 속한 인증서로서 명된 응용 프로그램은 일반 신뢰 수준으로 실행됩니다.
 - **SPC(소프트웨어 게시자 인증서):** SPC(소프트웨어 게시자 인증서)는 .cab 파일 서명에서 사용됩니다.
 - 루트: 루트 인증서를 포함하는 인증서 저장소입니다.
 - **CA:** 중간 인증 기관을 비롯한 암호화 정보를 포함하는 인증서 저장소입니다.
 - 내: 최종 사용자의 개인 인증서를 포함하는 인증서 저장소입니다.
- 자격 증명 유형: Windows Mobile/CE 장치의 경우 인증서가 유일한 자격 증명 유형입니다.
- 자격 증명 파일 경로: 찾아보기를 클릭하고 파일 위치로 이동하여 자격 증명 파일을 선택합니다.

Windows Phone 설정

- 인증서유형: 목록에서 루트또는 클라이언트를클릭합니다.
- 루트를클릭하는경우다음설정을구성합니다.
 - 스토어장치: 목록에서자격증명의인증서저장소위치로 루트, 내또는 **CA** 를클릭합니다. 내의경우사용자의인증서저장소에인증서가저장됩니다.
 - 위치: Windows Phone 의경우시스템이유일한위치입니다.
 - 자격증명유형: Windows Phone 의경우인증서가유일한자격증명유형입니다.
 - 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여인증서파일을선택합니다.
- 클라이언트를클릭하는경우다음설정을구성합니다.
 - 위치: Windows Phone 의경우 시스템이유일한위치입니다.
 - 자격증명유형: Windows Phone 의경우 키저장소가유일한자격증명유형입니다.
 - 자격증명이름: 자격증명의이름을입력합니다. 이것은필수필드입니다.
 - 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여인증서파일을선택합니다.
 - 암호: 자격증명과연관된암호를입력합니다. 이것은필수필드입니다.

사용자지정 XML 장치정책

January 6, 2020

XenMobile 에서사용자지정 XML 정책을만들어지원되는 Windows 및 Zebra Android 와 Android Enterprise 장치에 서다음기능을사용자지정할수있습니다.

- 장치구성을비롯한프로비저닝, 기능을사용하거나사용하지않도록설정
- 사용자가설정및장치매개변수를변경하도록허용하는것을비롯한장치구성

- 앱및시스템소프트웨어를비롯하여장치에로드할새소프트웨어또는버그수정을제공하는것을포함하는소프트웨어업그레이드
- 장치에서오류및상태보고서를받는것을비롯한오류관리

Windows 장치의경우: OMA DM(Open Mobile Alliance Device Management) API 를사용하여사용자지정 XML 구성을만듭니다. OMA DM API 로사용자지정 XML 을만드는것은이항목의범위를벗어납니다. OMA DM API 를사용하는방법에 대한자세한내용은 Microsoft Developer Network 사이트에있는 [OMA Device Management\(OMA 장치관리\)](#)를참조하십시오.

Zebra Android 및 Android Enterprise 장치의경우: MXMS(MX Management System) 를사용하여사용자지정 XML 구성을만듭니다. MXMS API 로사용자지정 XML 을만드는것은이문서의범위를벗어납니다. MXMS 사용에대한자세한내용은 Zebra 사이트의 [About MX\(MX 정보\)](#)를참조하십시오.

참고:

Windows 10 RS2 휴대폰: Internet Explorer 를사용하지않는사용자지정 XML 정책또는제한정책을휴대폰에배포한 후브라우저가사용되는상태로유지됩니다. 이문제를해결하려면휴대폰을다시시작하십시오. 이것은타사문제입니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Windows Phone, Windows Desktop/Tablet, Zebra Android 및 Android Enterprise 설정

- **XML 콘텐츠:** 정책에추가할사용자지정 XML 코드를입력하거나잘라내붙여넣습니다.

다음클릭하면 XenMobile 이 XML 콘텐츠구문을확인합니다. 모든구문오류가콘텐츠상자아래에나타납니다. 계속하려면먼저모든오류를해결합니다.

구문오류가없으면 사용자지정 **XML** 정책할당페이지가나타납니다.

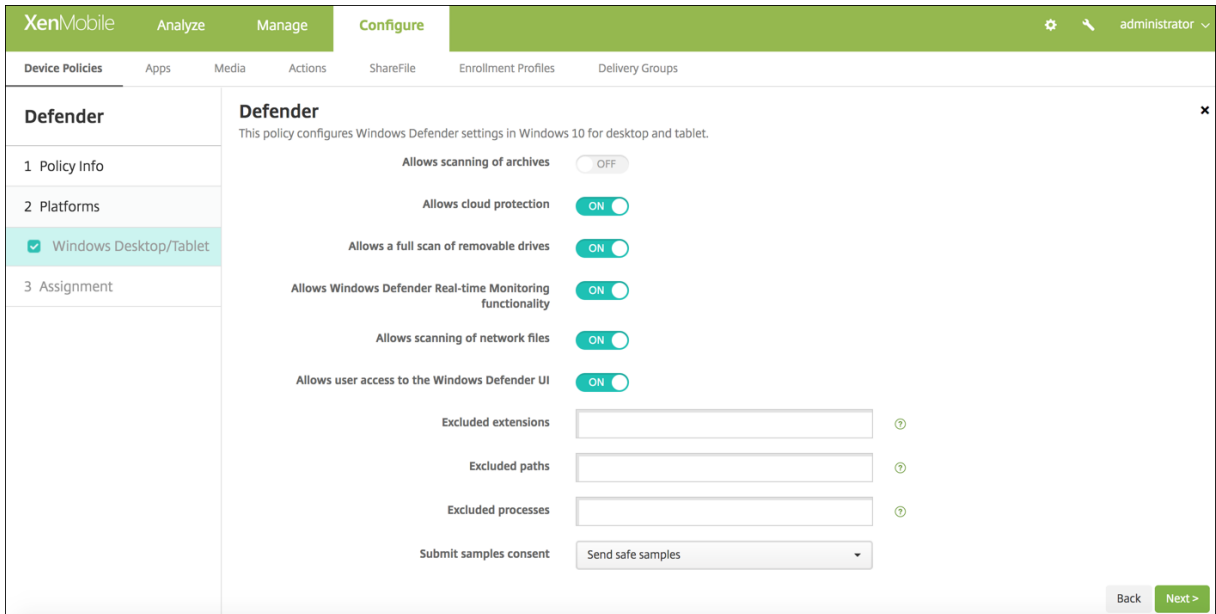
Defender 장치정책

January 6, 2020

Windows Defender 는 Windows 10 에포함된맬웨어방지프로그램입니다. XenMobile 장치정책인 Defender 를사용하여 Windows 10 데스크톱및태블릿에대한 Microsoft Defender 정책을구성할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Windows Desktop 및태블릿설정



- 보관파일에대한검사허용: Defender 가보관파일을검사하는것을허용하거나허용하지않습니다. 기본값은 꺼짐입니다.
- 클라우드보호허용: Defender 가 Microsoft 로맬웨어활동과관련된정보를보내는것을허용하거나허용하지않습니다. 기본값은 켜짐입니다.
- 이동식드라이브에대한전체검사허용: Defender 가 USB 스틱같은이동식드라이브를검사하는것을허용하거나허용하지 않습니다. 기본값은 켜짐입니다.
- **Windows Defender** 실시간모니터링기능허용: 기본값은 켜짐입니다.
- 네트워크파일에대한검사허용: Defender 가네트워크파일을검사하는것을허용하거나허용하지않습니다. 기본값은 켜짐입니다.
- **Windows Defender UI** 에대한사용자액세스허용: 사용자가 Windows Defender 사용자인터페이스에액세스할 수있는지여부를지정합니다. 이설정은다음번에사용자장치가시작될때적용됩니다. 이설정이 꺼짐이면사용자가어떠한 Windows Defender 알림도받지않습니다. 기본값은 켜짐입니다.
- 제외된확장명: 실시간또는예약검사에서제외할확장명입니다. 확장명을구분하려면 | 문자를사용합니다. 예를들어 “lib|obj” 를사용합니다.
- 제외된경로: 실시간또는예약검사에서제외할경로입니다. 경로를구분하려면 | 문자를사용합니다. 예를들어 “C:\Example\C:\Example1” 을사용합니다.
- 제외된프로세스: 실시간또는예약검사에서제외할프로세스입니다. 프로세스를구분하려면 | 문자를사용합니다. 예를들어 “C:\Example.exe\C:\Example1.exe” 를사용합니다.
- 샘플동의제출: 악성인지확인하려면추가적인분석이필요할수있는파일을 Microsoft 로보낼지여부를제어합니다. 옵션: 항상확인, 안전한샘플보내기, 보내지않음, 모든샘플보내기. 기본값은 안전한샘플보내기입니다.

파일및폴더장치정책삭제

January 6, 2020

Windows Mobile/CE 장치에서특정파일또는폴더를삭제하는정책을 XenMobile 에서만들수있습니다. 이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Windows Mobile/CE 설정

- 삭제할파일및폴더: 삭제할각파일또는폴더에대해추가를클릭한후다음을수행합니다.
 - 경로: 파일또는폴더의경로를입력합니다.
 - 유형: 목록에서파일또는폴더를클릭합니다. 기본값은파일입니다.
 - 파일또는폴더를저장하려면 저장을클릭하고저장하지않으려면 취소를클릭합니다.

레지스트리키및값삭제장치정책

January 6, 2020

XenMobile 에서정책을만들어 Windows Mobile/CE 장치에서특정레지스트리키및값을삭제할수있습니다. 이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Windows Mobile/CE 설정

- 삭제할레지스트리키및값: 삭제할각레지스트리키및값에대해 추가를클릭하고다음을수행합니다.
 - 키: 레지스트리키경로를입력합니다. 이필드는필수필드입니다. 레지스트리키경로는 HKEY_CLASSES_ROOT\ 또는 HKEY_CURRENT_USER\ 또는 HKEY_LOCAL_MACHINE\ 또는 HKEY_USERS\로시작되어야합니다.
 - 값: 삭제할값이름을입력합니다. 또는전체레지스트리키를삭제하려면이필드를비워둡니다.
 - 저장을클릭하여키및값을저장하거나 취소를클릭하여키및값을저장하지않습니다.

장치상태증명장치정책

January 6, 2020

XenMobile 에서 Windows 10 장치가 분석을 위해 특정 데이터 및 런타임 정보를 HAS(상태증명서비스)에 전송하여 해당 상태를 보고하도록 할 수 있습니다. HAS 에서 상태증명인증을 생성하고 반환하면 장치가 이를 XenMobile 에 보냅니다. XenMobile 은 상태증명인증을 받은 후 상태증명인증서의 내용에 따라 이전에 설정된 자동 동작을 배포할 수 있습니다.

HAS 에 의해 확인되는 데이터는 다음과 같습니다.

- AIK 존재
- Bit Locker 상태
- 부팅 디버깅 사용
- 부팅 관리자 수정 목록 버전
- 코드 무결성 사용
- 코드 무결성 수정 목록 버전
- DEP 정책
- ELAM 드라이버 로드
- 실행 시간
- 커널 디버깅 사용
- PCR
- 재설정 횟수
- 다시 시작 횟수
- 안전 모드 사용
- SBCP 해시
- 보안 부팅 사용
- 테스트 서명 사용
- VSM 사용
- WinPE 사용

자세한 내용은 Microsoft [HealthAttestation CSP](#) 페이지를 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

Microsoft Cloud 를 사용하여 DHA 를 구성하려면

장치 상태 증명 정책을 추가하고 선택한 각 플랫폼에 대해 다음 설정을 구성합니다.

- 장치 상태 증명 사용: 장치 상태 증명을 요구할 것인지 선택합니다. 기본값은 꺼짐입니다.

온프레미스 Windows DHA 서버를 사용하여 DHA 를 구성하려면

DHA 온-프레미스를 사용하려면 먼저 DHA 서버를 구성해야 합니다. 그런 다음 온-프레미스 DHA 서비스를 활성화하는 XenMobile Server 정책을 생성합니다.

1. DHA 를 구성하려면 Windows Server 2016 Technical Preview 5 이상을 실행하는 컴퓨터에 DHA 서버 역할을 설치해야 합니다. 지침은 [온프레미스 장치 상태 증명 서버 구성](#)을 참조하십시오.

2. 장치상태증명정책을추가하고다음설정을구성합니다.

- 장치상태증명사용: 켜짐으로설정합니다.
- 온프레미스 **Health Attestation Service** 구성: 켜짐으로설정합니다.
- **On-prem DHA Service FQDN(온-프레미스 DHA 서비스 FQDN):** 설정하는 DHA 서버의정규화된도메인 이름을입력합니다.
- **On-prem DHA API version(온-프레미스 DHA API 버전):** DHA 서버에설치된 DHA 서비스의버전을선택 합니다.

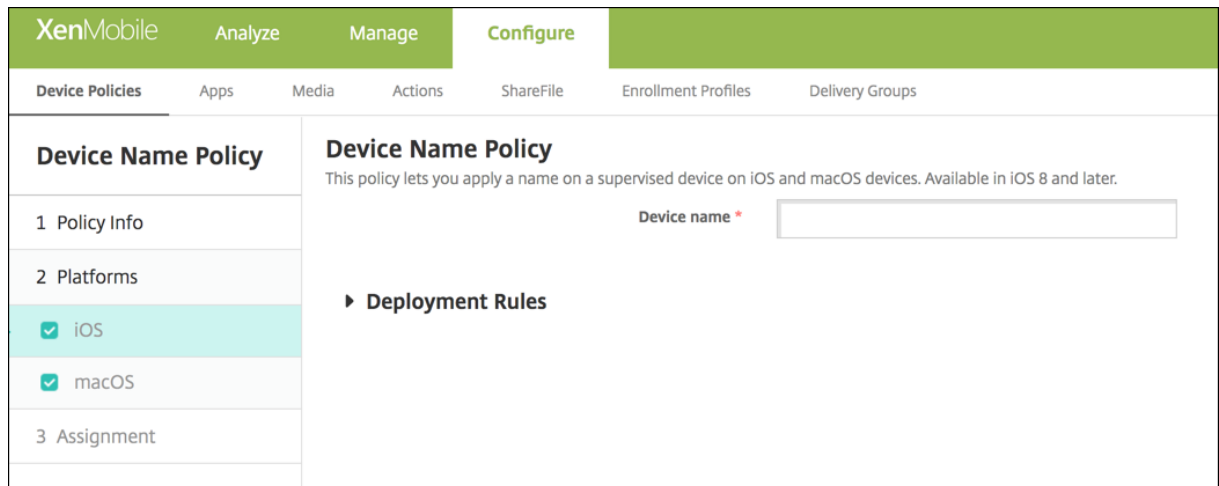
장치이름장치정책

January 6, 2020

감독되는 iOS 및 macOS 장치에장치를쉽게식별할수있도록하는이름을설정할수있습니다. 매크로, 텍스트또는둘다를사용하여 장치이름을정의할수있습니다. 예를들어장치일련번호로장치이름을설정하려는경우 `${device.serialnumber}` 를사용할수 있습니다. 사용자이름과도메인의조합으로장치이름을설정하려면 `${user.username}@example.com` 을사용할수있습니다. 매크로에대한자세한내용은 [XenMobile 의매크로](#)를참조하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 및 macOS 설정



- 장치이름: 매크로, 매크로조합또는매크로와텍스트조합을입력하여각장치에고유한이름을지정합니다. 예를들어 `${device.serialnumber}` 를사용하여장치이름을각장치의일련번호로설정하거나 `${device.serialnumber} ${user.username}` 을사용하여장치이름에사용자이름을포함합니다.

교육구성장치정책

January 6, 2020

교육구성장치정책은다음을정의합니다.

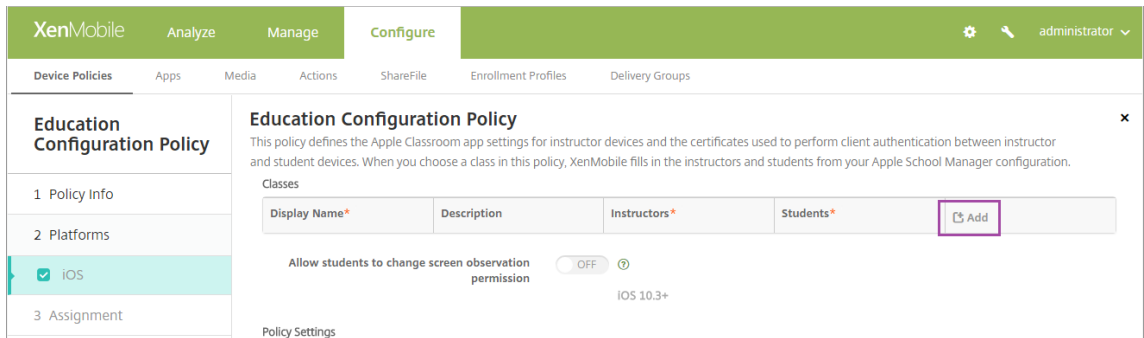
- 강사장치의 Apple Classroom 앱설정
- 강사장치와학생장치간의클라이언트인증을수행하는데사용되는인증서

이정책에서클래스를선택하면 XenMobile 콘솔에 Apple School Manager 구성의강사및학생이입력됩니다. 이정책의 Apple Classroom 앱설정이모든클래스에대해동일한경우하나의정책을생성합니다.

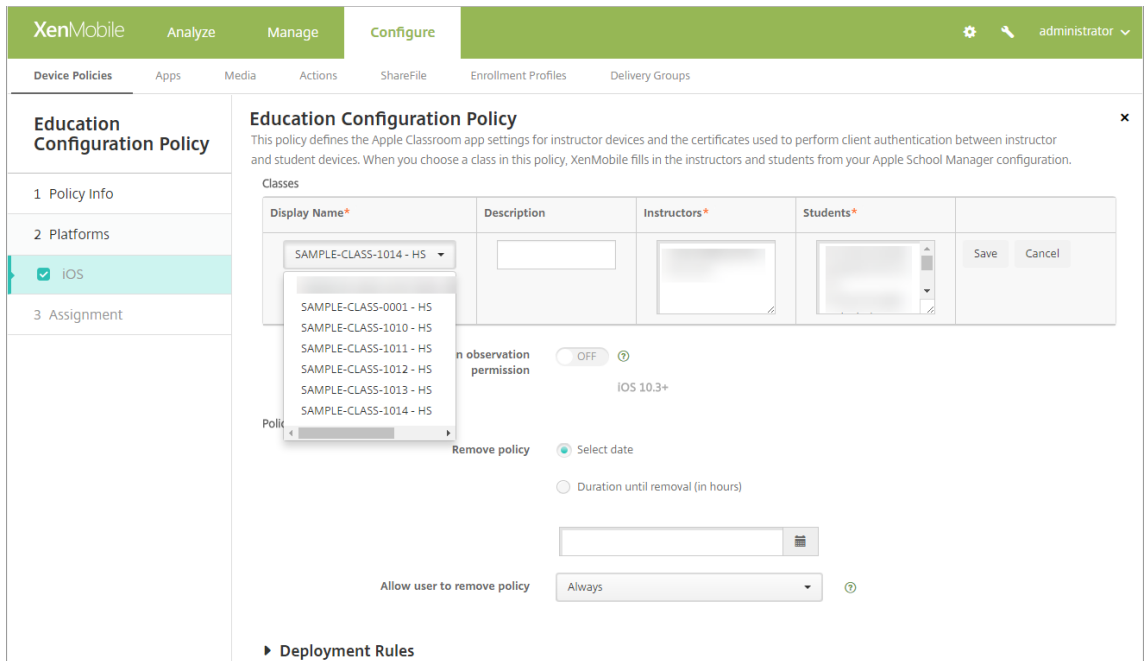
이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

정책을구성하려면

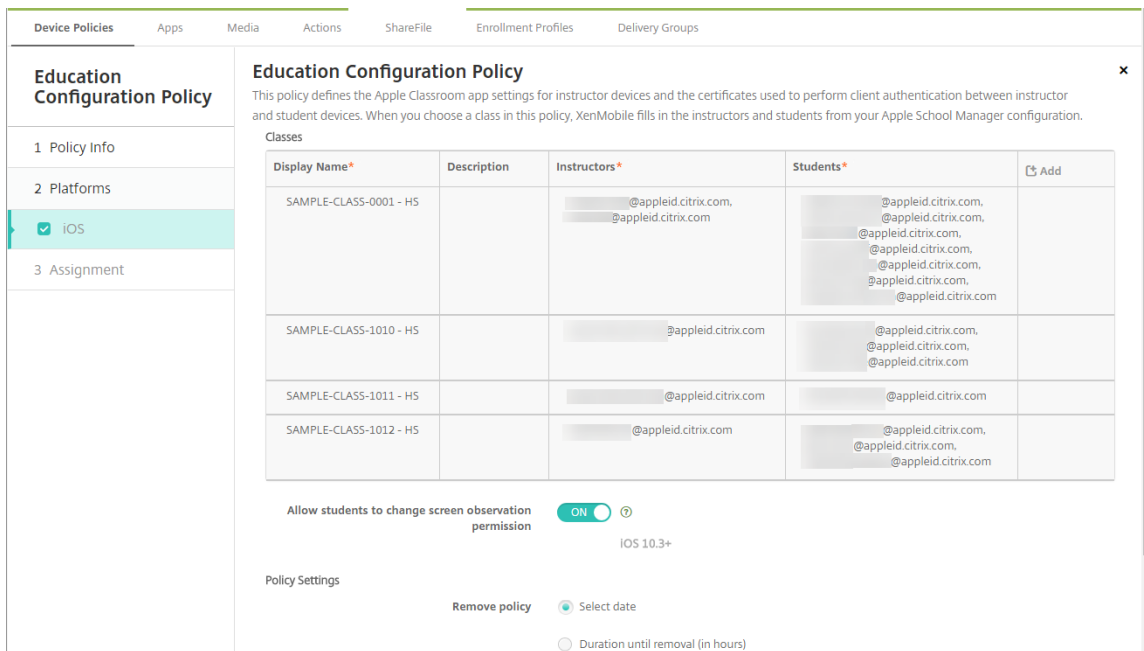
1. 교육구성정책을추가한후 추가를클릭합니다.



2. 표시이름목록을클릭합니다. 연결된 Apple School Manager 계정에서가져온클래스목록이타납니다.



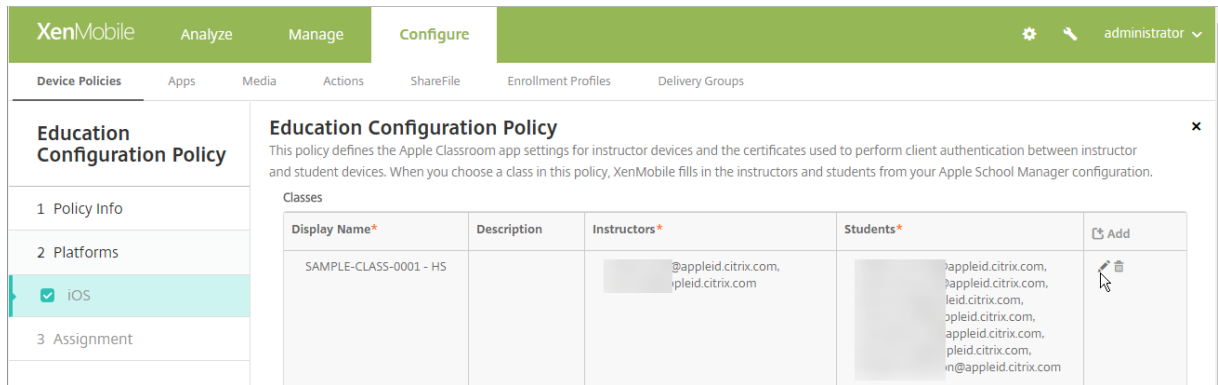
표시이름에서 클래스를 선택하면 XenMobile 이강사와 학생을 입력합니다. 클래스 추가를 계속합니다.



정책의 클래스 정보를 편집하려면

클래스에 설명을 추가할 수 있습니다 (Classroom 앱의 “표시이름”). 또한 강사와 학생을 추가하거나 제거할 수 있습니다. XenMobile Server 는 이러한 변경 내용을 Apple School Manager 계정에 저장하지 않습니다. 자세한 내용은 [Apple 교육기능과 통합](#)의 “강사, 학생 및 클래스 데이터 관리” 를 참조하십시오.

편집할 클래스의 추가 열 위로 마우스를 이동하고 연필 아이콘을 클릭합니다.



정책에서 클래스를 삭제하려면 삭제할 클래스의 추가 열 위로 마우스를 이동하고 휴지통 아이콘을 클릭합니다.

엔터프라이즈 허브 장치 정책

January 6, 2020

Windows Phone 에 대한 엔터프라이즈 허브 장치 정책을 사용하면 Enterprise Hub Company 스토어를 통해 앱을 배포할 수 있습니다.

정책을 만들려면 먼저 다음이 필요합니다.

- DigiCert 의 AET(.aetx) 서명인증서
- Microsoft 앱서명 도구 (XapSignTool.exe) 를 사용하여 서명한 Citrix Company Hub 앱

참고:

XenMobile 은 Windows Phone Secure Hub 모드마다 엔터프라이즈 허브 정책을 하나만 지원 합니다. 예를 들어, XenMobile Enterprise Edition 의 Windows Phone Secure Hub 를 업로드 하려면 XenMobile Enterprise Edition 의 다양한 Work Home 버전을 사용하여 여러 Enterprise Hub 정책을 만들어서는 안 됩니다. 초기 엔터프라이즈 허브 정책은 장치를 등록하는 동안에만 배포할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#) 에서 참조하십시오.

Windows Phone 설정

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Enterprise Hub Policy' and contains the following text: 'To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe)'. There are two 'Browse' buttons for uploading files: 'Upload .aetx file' and 'Upload signed Enterprise Hub app'. A 'Deployment Rules' section is also visible. The sidebar on the left has 'Enterprise Hub Policy' selected, with sub-sections for '1 Policy Info', '2 Platforms' (where 'Windows Phone' is checked), and '3 Assignment'. At the bottom right, there are 'Back' and 'Next >' buttons.

- **.aetx** 파일업로드: 찾아보기를클릭하고파일위치로이동하여.aetx 파일을선택합니다.
- 서명된엔터프라이즈허브앱업로드: 찾아보기를클릭하고앱위치로이동하여엔터프라이즈허브앱을선택합니다.

Exchange 장치정책

January 6, 2020

Exchange ActiveSync 장치정책을사용하여 Exchange 에서호스팅되는회사전자메일에액세스할수있도록사용자장치의전자메일클라이언트를구성할수있습니다. iOS, macOS, Android HTC, Android TouchDown, Android Enterprise, Samsung SAFE, Samsung KNOX, Windows Phone 및 Windows 태블릿에대한정책을만들수있습니다. 각플랫폼마다다른값집합이필요합니다. 값집합에대해서는이후섹션에서자세히설명합니다.

이정책을만들려면 Exchange Server 의호스트이름또는 IP 주소가필요합니다. ActiveSync 설정에대한자세한내용은 Microsoft 문서 [ActiveSync CSP](#)를참조하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

The screenshot shows the 'Exchange Policy' configuration page in XenMobile. The left sidebar lists various platforms, with 'iOS' selected. The main area is titled 'Exchange Policy' and contains the following fields and options:

- Exchange ActiveSync account name ***: Text input field.
- Exchange ActiveSync host name ***: Text input field.
- Use SSL**: Toggle switch set to 'ON'.
- Domain**: Text input field.
- User**: Text input field.
- Email address**: Text input field.
- Password**: Text input field.
- Email sync interval**: Dropdown menu set to '3 days'.
- Identity credential (keystore or PKI credential)**: Dropdown menu set to 'None'.
- Authorize email move between accounts**: Toggle switch set to 'OFF'.

- **Exchange ActiveSync** 계정 이름: 사용자 장치에 표시되는 전자 메일 계정에 대한 설명을 입력합니다.
- **Exchange ActiveSync** 호스트 이름: 전자 메일 서버의 주소를 입력합니다.
- **SSL** 사용: 사용자의 장치와 Exchange Server 간의 연결을 보호할지 여부를 선택합니다. 기본값은 켜짐입니다.
- **도메인**: Exchange Server 가상 주소는 도메인을 입력합니다. 이 필드에서 \$user.domainname 시스템 매크로를 사용하여 사용자 도메인 이름을 자동으로 조회할 수 있습니다.
- **사용자**: Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 \$user.username 시스템 매크로를 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- **전자 메일 주소**: 전체 전자 메일 주소를 지정합니다. 이 필드에서 \$user.mail 시스템 매크로를 사용하여 사용자 전자 메일 계정을 자동으로 조회할 수 있습니다.
- **OAuth** 사용: 켜짐으로 설정된 경우 연결 인증에 OAuth가 사용됩니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에 적용됩니다.
- **암호**: Exchange 사용자 계정에 대한 선택적 암호를 입력합니다. **OAuth** 사용이 켜짐인 경우 이 설정이 나타나지 않습니다.
- **전자 메일 동기화 간격**: 목록에서 전자 메일이 Exchange Server와 동기화되는 빈도를 선택합니다. 기본값은 3일입니다.
- **ID 자격 증명 (키저장소 또는 PKI)**: XenMobile에 대한 ID 공급자를 구성한 경우 목록에서 선택적인 ID 자격 증명을 클릭합니다. 이 필드는 Exchange가 클라이언트 인증서 인증을 요구하는 경우에만 필요합니다. 기본값은 없음입니다.
- **계정 간 전자 메일 이동 승인**: 사용자가 이 계정에서 다른 계정으로 전자 메일을 이동하고 다른 계정에서 전자 메일을 전달하고 회신할 수 있도록 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **전자 메일 앱에서만 전자 메일 보내기**: 전자 메일을 보낼 사용자를 iOS 메일 앱으로 제한할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **최근 전자 메일 동기화 사용 안 함**: 사용자가 최근 주소를 동기화하지 못하도록 할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 6.0 이상에만 적용됩니다.
- **S/MIME** 서명 사용: 이 계정이 S/MIME 서명을 지원하는지 여부를 선택합니다. 기본값은 켜짐입니다. 켜짐으로 설정하면 다음 필드가 나타납니다.

- 서명 **ID** 자격증명: 사용할서명자격을선택합니다.
- **S/MIME** 서명사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서 S/MIME 서명을켜거나꺼낼수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.
- **S/MIME** 서명인증서 **UUID** 사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서사용할서명자격을선택할수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.
- **S/MIME** 암호화사용: 이계정이 S/MIME 암호화를지원하는지여부를선택합니다. 기본값은 꺼짐입니다. 켜짐으로설정하면다음필드가나타납니다.
 - 암호화 **ID** 자격증명: 사용할암호화자격증을선택합니다.
 - 메시지별 **S/MIME** 전환사용: 켜짐으로설정하면작성하는각메시지에대해 S/MIME 암호화를켜거나꺼낼수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
 - 기본적으로 **S/MIME** 암호화사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서 S/MIME 를기본적으로켜지여부를선택할수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.
 - **S/MIME** 암호화인증서 **UUID** 사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나꺼낼수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.

macOS 설정

The screenshot shows the 'Configure' tab in XenMobile. Under 'Device Policies', 'Exchange Policy' is selected. The configuration form includes the following fields:

- Exchange ActiveSync account name *
- User *
- Email address *
- Password
- Internal Exchange host
- Internal server port
- Internal server path
- Use SSL for Internal Exchange host: ON
- External Exchange host
- External server port
- External server path

- **Exchange ActiveSync** 계정이름: 사용자장치에표시되는전자메일계정에대한설명을입력합니다.
- 사용자: Exchange 사용자계정의사용자이름을지정합니다. 이필드에서 \$user.username 시스템매크로를사용하여 사용자이름을자동으로조회할수있습니다.
- 전자메일주소: 전체전자메일주소를지정합니다. 이필드에서 \$user.mail 시스템매크로를사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **OAuth** 사용: 켜짐으로설정된경우연결인증에 OAuth 가사용됩니다. 기본값은 꺼짐입니다. 이 옵션은 macOS 10.14

이상에적용됩니다.

- **OAuth** 로그인 **URL**: 자동검색서비스가사용되지않을때 OAuth 를사용한인증을위해웹뷰에로드할 URL 을지정합니다. 이필드는 **OAuth** 사용이 켜짐으로설정된경우나타납니다.
- **암호**: Exchange 사용자계정에대한선택적암호를입력합니다. **OAuth** 사용이 켜짐인경우이설정이나타나지않습니다.
- **내부 Exchange** 호스트: 내부및외부 Exchange 호스트이름을서로다르게만들려면선택적인내부 Exchange 호스트 이름을입력합니다.
- **내부서버포트**: 내부및외부 Exchange Server 포트를서로다르게만들려면선택적인내부 Exchange Server 포트번호를입력합니다.
- **내부서버경로**: 내부및외부 Exchange Server 경로를서로다르게만들려면선택적인내부 Exchange Server 경로를입력합니다.
- **내부 Exchange** 호스트에 **SSL** 사용: 사용자장치와내부 Exchange 호스트간의연결을보호할지여부를선택합니다. 기본값은 켜짐입니다.
- **외부 Exchange** 호스트: 내부및외부 Exchange 호스트이름을서로다르게만들려면선택적인외부 Exchange 호스트 이름을입력합니다.
- **외부서버포트**: 내부및외부 Exchange Server 포트를서로다르게만들려면선택적인외부 Exchange Server 포트번호를입력합니다.
- **외부서버경로**: 내부및외부 Exchange Server 경로를서로다르게만들려면선택적인외부 Exchange Server 경로를입력합니다.
- **외부 Exchange** 호스트에 **SSL** 사용: 사용자장치와내부 Exchange 호스트간의연결을보호할지여부를선택합니다. 기본값은 켜짐입니다.
- **메일삭제허용**: 사용자가기존네트워크에연결할필요없이두대의 Mac 간에서무선으로파일을공유하도록허용할지여부를선택합니다. 기본값은 꺼짐입니다.

Android HTC 설정

The screenshot shows the XenMobile 'Configure' interface for an 'Exchange Policy'. The left sidebar lists policy categories: 1 Policy Info, 2 Platforms, and several platform options: iOS, macOS, Android HTC (checked), Android TouchDown (checked), Android for Work (checked), and Samsung SAFE (checked). The main configuration area includes a description: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' Below this are input fields for 'Configuration display name', 'Server address', 'User ID', 'Password', 'Domain', and 'Email address'. At the bottom, there is a 'Use SSL' toggle switch which is currently turned 'ON'.

- 구성표이름: 사용자장치에표시되는이정책의이름을입력합니다.
- 서버주소: Exchange Server 의호스트이름또는 IP 주소를입력합니다.

- 사용자 **ID**: Exchange 사용자계정의사용자이름을지정합니다. 이필드에서 \$user.username 시스템매크로를사용하여사용자이름을자동으로조회할수있습니다.
- 암호: Exchange 사용자계정에대한선택적암호를입력합니다.
- 도메인: Exchange Server 가상주하는도메인을입력합니다. 이필드에서 \$user.domainname 시스템매크로를사용하여사용자도메인이름을자동으로조회할수있습니다.
- 전자메일주소: 전체전자메일주소를지정합니다. 이필드에서 \$user.mail 시스템매크로를사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **SSL** 사용: 사용자의장치와 Exchange Server 간의연결을보호할지여부를선택합니다. 기본값은 켜짐입니다.

Android TouchDown 설정

The screenshot shows the 'Exchange Policy' configuration page in the XenMobile console. The left sidebar lists various policies, with 'Exchange Policy' selected. The main content area contains the following fields and sections:

- Server name or IP address ***: Text input field.
- Domain**: Text input field.
- User ID ***: Text input field.
- Password**: Text input field.
- Email address**: Text input field.
- Identity credential (keystore or PKI)**: Dropdown menu with 'None' selected.
- Policies and Apps**: Section with a table for 'App Setting' and 'Policy'.

- 서버이름또는 **IP** 주소: Exchange Server 의호스트이름또는 IP 주소를입력합니다.
- 도메인: Exchange Server 가상주하는도메인을입력합니다. 이필드에서 \$user.domainname 시스템매크로를사용하여사용자도메인이름을자동으로조회할수있습니다.
- 사용자 **ID**: Exchange 사용자계정의사용자이름을지정합니다. 이필드에서 \$user.username 시스템매크로를사용하여사용자이름을자동으로조회할수있습니다.
- 암호: Exchange 사용자계정에대한선택적암호를입력합니다.
- 전자메일주소: 전체전자메일주소를지정합니다. 이필드에서 \$user.mail 시스템매크로를사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **ID** 자격증명 (키저장소또는 **PKI**): XenMobile 에대한 ID 공급자를구성한경우목록에서선택적인 ID 자격증명을클릭합니다. 이필드는 Exchange 가클라이언트인증서인증을요구하는경우에만필요합니다. 기본값은 없음입니다.
- 앱설정: 필요한경우이정책에대한 TouchDown 앱설정을추가합니다.
- 정책: 필요한경우이정책에대한 TouchDown 정책을추가합니다.

Android Enterprise

The screenshot shows the XenMobile 'Configure' interface for an 'Exchange Policy'. The sidebar on the left lists various policy categories, with 'Exchange Policy' selected. The main content area is titled 'Exchange Policy' and includes a descriptive note: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' Below this, there are several input fields: 'Server name or IP address *', 'Domain', 'User ID *', 'Password', 'Email address', and 'Identity credential (keystore or PKI)' which is a dropdown menu currently set to 'None'. A 'Deployment Rules' section is partially visible at the bottom.

- 서버이름 또는 **IP 주소**: Exchange Server 의 호스트이름 또는 IP 주소를 입력합니다.
- 도메인: Exchange Server 가상주하는 도메인을 입력합니다. 이 필드에서 \$user.domainname 시스템매크로를 사용하여 사용자도메인 이름을 자동으로 조회할 수 있습니다.
- 사용자 **ID**: Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 \$user.username 시스템매크로를 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- 암호: Exchange 사용자 계정에 대한 선택적 암호를 입력합니다.
- 전자메일 주소: 전체 전자메일 주소를 지정합니다. 이 필드에서 \$user.mail 시스템매크로를 사용하여 사용자 전자메일 계정 을 자동으로 조회할 수 있습니다.
- **ID 자격증명 (키저장소 또는 PKI)**: XenMobile 에 대한 ID 공급자를 구성한 경우 목록에서 선택적인 ID 자격증명을 클릭합니다. 이 필드는 Exchange 가 클라이언트 인증서 인증을 요구하는 경우에만 필요합니다. 기본값은 없음입니다.

Samsung SAFE 및 Samsung KNOX 설정

The screenshot shows the 'Exchange Policy' configuration page in the XenMobile console. The left sidebar lists various platforms, with 'Samsung SAFE', 'Samsung KNOX', 'Windows Phone', and 'Windows Desktop/Tablet' selected. The main configuration area includes the following fields and options:

- Server name or IP address ***: Text input field.
- Domain**: Text input field.
- User ID ***: Text input field.
- Password**: Text input field.
- Email address ***: Text input field.
- Identity credential (keystore or PKI)**: Dropdown menu with 'None' selected.
- Use SSL connection**: Toggle switch (ON).
- Sync contacts**: Toggle switch (ON).
- Sync calendar**: Toggle switch (ON).
- Default account**: Toggle switch (ON).

- 서버이름또는 **IP 주소**: Exchange Server 의호스트이름또는 IP 주소를입력합니다.
- 도메인: Exchange Server 가상주하는도메인을입력합니다. 이필드에서 \$user.domainname 시스템매크로를 사용하여사용자도메인이름을자동으로조회할수있습니다.
- 사용자 **ID**: Exchange 사용자계정의사용자이름을지정합니다. 이필드에서 \$user.username 시스템매크로를 사용하여사용자이름을자동으로조회할수있습니다.
- 암호: Exchange 사용자계정에대한선택적암호를입력합니다.
- 전자메일주소: 전체전자메일주소를지정합니다. 이필드에서 \$user.mail 시스템매크로를 사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **ID 자격증명 (키저장소또는 PKI)**: XenMobile 에대한 ID 공급자를구성한경우목록에서선택적인 ID 자격증명을클릭합니다. 이필드는 Exchange 가클라이언트인증서인증을요구하는경우에만필요합니다.
- **SSL 연결사용**: 사용자장치와 Exchange Server 간의연결을보호할지여부를선택합니다. 기본값은 켜짐입니다.
- **연락처동기화**: 장치와 Exchange Server 간에사용자연락처동기화를사용할지여부를선택합니다. 기본값은 켜짐입니다.
- **캘린더동기화**: 장치와 Exchange Server 간에사용자캘린더동기화를사용할지여부를선택합니다. 기본값은 켜짐입니다.
- **기본계정**: 사용자 Exchange 계정을장치에서전자메일을보내기위한기본값으로만들지여부를선택합니다. 기본값은 켜짐입니다.

Windows Phone 및 Windows 데스크톱/태블릿설정

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The left sidebar lists various platforms, with 'Windows Desktop/Tablet' selected. The main area contains the following fields and options:

- Account name or display name ***: Text input field.
- Server name or IP address ***: Text input field.
- Domain**: Text input field.
- User ID or user name ***: Text input field.
- Email address ***: Text input field.
- Use SSL connection**: Toggle switch set to OFF.
- Sync items**: Section header.
- Past days to sync**: Dropdown menu set to 'All content'.
- Frequency**: Dropdown menu set to 'When item arrives'.
- Logging level**: Dropdown menu set to 'Disabled'.

참고:

이 정책에서는 사용자 암호를 설정하도록 허용하지 않습니다. 사용자는 정책이 푸시된 후 장치에서 해당 매개변수를 설정해야 합니다.

- **계정 이름 또는 표시 이름:** Exchange ActiveSync 계정 이름을 입력합니다.
- **서버 이름 또는 IP 주소:** Exchange Server 의 호스트 이름 또는 IP 주소를 입력합니다.
- **도메인:** Exchange Server 가상주하는 도메인을 입력합니다. 이 필드에서 \$user.domainname 시스템 매크로를 사용하여 사용자 도메인 이름을 자동으로 조회할 수 있습니다.
- **사용자 ID 또는 사용자 이름:** Exchange 사용자 계정의 사용자 이름을 지정합니다. 이 필드에서 \$user.username 시스템 매크로를 사용하여 사용자 이름을 자동으로 조회할 수 있습니다.
- **전자메일 주소:** 전체 전자메일 주소를 지정합니다. 이 필드에서 \$user.mail 시스템 매크로를 사용하여 사용자 전자메일 계정을 자동으로 조회할 수 있습니다.
- **SSL 연결 사용:** 사용자 장치와 Exchange Server 간의 연결을 보호할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **동기화 할 과거 일수:** 목록에서 장치의 모든 콘텐츠를 Exchange Server 와 동기화 할 과거 일수를 클릭합니다. 기본값은 모든 콘텐츠입니다.
- **빈도:** 목록에서 Exchange Server 에서 장치로 보낸 데이터를 동기화 할 때 사용할 일정을 클릭합니다. 기본값은 항목이 도착할 때입니다.
- **로그 수준:** 목록에서 사용 안함, 기본 또는 고급을 클릭하여 Exchange 활동을 로깅 할 때 사용할 세부 정보 수준을 지정합니다. 기본값은 사용 안함입니다.

파일장치정책

January 6, 2020

사용자에대한특정기능을수행하는스크립트파일을 XenMobile 에추가하거나, Android 장치사용자가장치에서액세스할수있는 문서파일을추가할수있습니다. 파일을추가하는경우장치에서파일이저장될디렉터리를지정할수도있습니다. 예를들어, Android 사용자가회사문서또는.pdf 파일을받기를원할경우해당장치에파일을배포하고파일위치를사용자에게알릴수있습니다.

이정책에는다음과같은파일형식을추가할수있습니다.

- 텍스트기반파일 (.xml, .html, .py 등)
- 문서, 그림, 스프레드시트또는프레젠테이션등의기타파일
- Windows Mobile 및 Windows CE 에만해당: MortScript 를사용하여만든스크립트파일

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Android Enterprise 설정

Files Policy X

This policy lets you upload files and executable scripts to devices.

File to be imported *

File type File Script

Replace macro expressions OFF ?

Destination folder ?

Destination file name ?

If file exists ?

▶ **Deployment Rules**

-
-

- 가져올파일: 가져올파일을선택하려면 찾아보기를클릭하고파일의위치로이동합니다.
- 파일형식: 파일또는 스크립트를선택합니다. 스크립트를선택하는경우 즉시실행이표시됩니다. 파일을업로드하는즉시 스크립트를실행할지여부를선택합니다. 즉시실행기본값은 꺼짐입니다.
- 매크로식바꾸기: 스크립트의매크로토큰이름을장치또는사용자속성으로바꾸지여부를선택합니다. 매크로구문은매크로를 참조하십시오. 기본값은 꺼짐입니다.
- 대상폴더: 목록에서업로드된파일을저장할위치를선택하거나 새로추가를클릭하여나열되지않은파일위치를선택합니다. %XenMobile Folder%\ 또는%Flash Storage%\ 매크로를경로식별자의시작부분으로사용할수있습니다.

- 대상파일 이름: 선택사항입니다. 장치에 배포하기 전에 파일 이름을 변경해야 하는 경우 파일 이름을 입력합니다.
- 파일이 있는 경우: 목록에서 기존 파일을 복사할지 여부를 선택합니다. 기본값은 파일이 다른 경우에만 복사입니다.

Android 설정

- 가져올 파일: 찾아보기를 클릭하고 파일의 위치로 이동하여 가져올 파일을 선택합니다.
- 파일 형식: 파일 또는 스크립트를 선택합니다. 스크립트를 선택하는 경우 즉시 실행이 표시됩니다. 파일을 업로드하는 즉시 스크립트를 실행할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 매크로 식바꾸기: 스크립트의 매크로 토큰 이름을 장치 또는 사용자 속성으로 바꿀지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 대상 폴더: 목록에서 업로드된 파일을 저장할 위치를 선택하거나 새로 추가를 클릭하여 열리지 않은 파일 위치를 선택합니다. 또는 %XenMobile Folder% \ 또는 %Flash Storage% \ 매크로를 경로 식별자의 시작 부분으로 사용할 수 있습니다.
- 대상 파일 이름: 필요에 따라 장치에 배포하기 전에 이름을 변경해야 할 경우 파일에 다른 이름을 입력합니다.
- 파일이 다른 경우에만 복사: 목록에서 기존 파일과 다른 경우 파일을 복사할 것인지 여부를 선택합니다. 기본값은 다른 경우에 파일을 복사하는 것입니다.

Windows Mobile/CE 설정

- 가져올 파일: 찾아보기를 클릭하고 파일의 위치로 이동하여 가져올 파일을 선택합니다.
- 파일 형식: 파일 또는 스크립트를 선택합니다. 스크립트를 선택하는 경우 즉시 실행이 표시됩니다. 파일을 업로드하는 즉시 스크립트를 실행할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 매크로 식바꾸기: 스크립트의 매크로 토큰 이름을 장치 또는 사용자 속성으로 바꿀지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 대상 폴더: 목록에서 업로드된 파일을 저장할 위치를 선택하거나 새로 추가를 클릭하여 열리지 않은 파일 위치를 선택합니다. 또한 경로 식별자의 시작 부분으로 다음 매크로 중 하나를 사용할 수 있습니다.
 - %Flash Storage%\
 - %XenMobile Folder%\
 - %Program Files%\
 - %My Documents%\
 - %Windows%\
- 대상 파일 이름: 필요에 따라 장치에 배포하기 전에 이름을 변경해야 할 경우 파일에 다른 이름을 입력합니다.
- 파일이 다른 경우에만 복사: 목록에서 기존 파일과 다른 경우 파일을 복사할 것인지 여부를 선택합니다. 기본값은 다른 경우에 파일을 복사하는 것입니다.
- 읽기 전용 파일: 파일이 읽기 전용인지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 숨겨진 파일: 파일 목록에 파일을 표시하지 않을지 여부를 선택합니다. 기본값은 꺼짐입니다.

FileVault 장치 정책

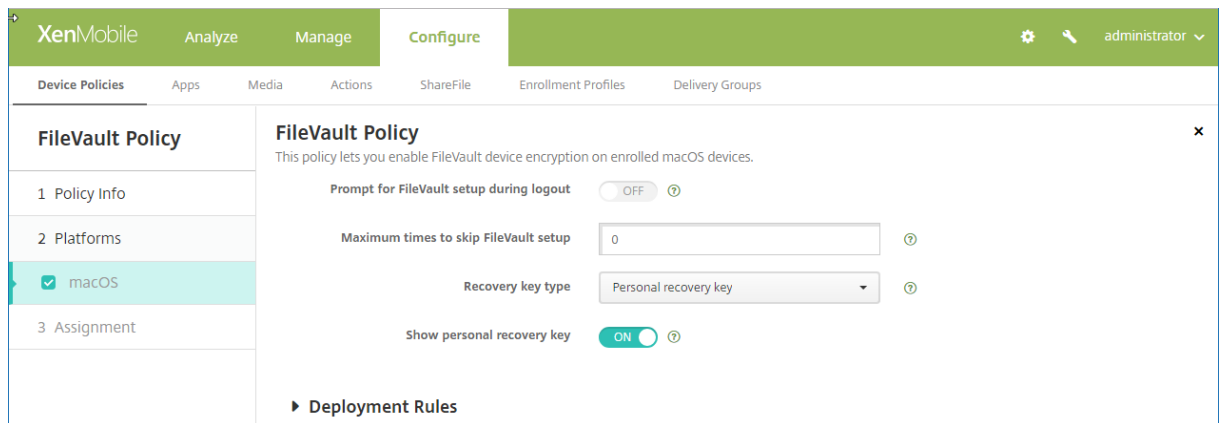
August 24, 2018

macOS FileVault 디스크암호화기능은시스템볼륨콘텐츠를암호화하여시스템볼륨을보호합니다. macOS 장치에서 FileVault 를사용하도록설정하면장치를시작할때마다사용자가계정암호를사용하여로그인해야합니다. 사용자가암호를잊은경우 복구키를사용하여디스크잠금을해제하고암호를재설정할수있습니다.

XenMobile 장치정책인 FileVault 는 FileVault 사용자설치화면을사용하도록설정하고복구키같은설정을구성합니다. FileVault 에대한자세한내용은 Apple 지원사이트 (<https://support.apple.com>) 를참조하십시오.

FileVault 정책을추가하려면 구성 > 장치정책으로이동합니다.

macOS 설정

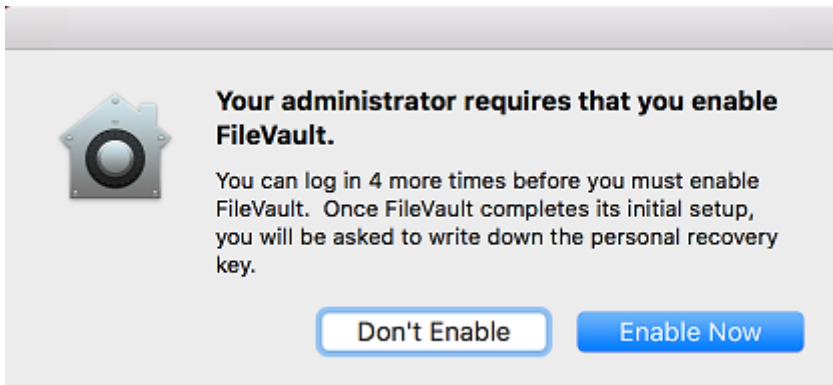


- 로그아웃도중 **FileVault** 설정에대해문기: 꺼짐인경우 **FileVault** 설정을건너뛴최대횟수옵션에지정된대로다음 N 번째로그아웃시 FileVault 를사용할지여부를묻는메시지를표시합니다. 꺼짐인경우 FileVault 암호확인메시지가표시되지않습니다.

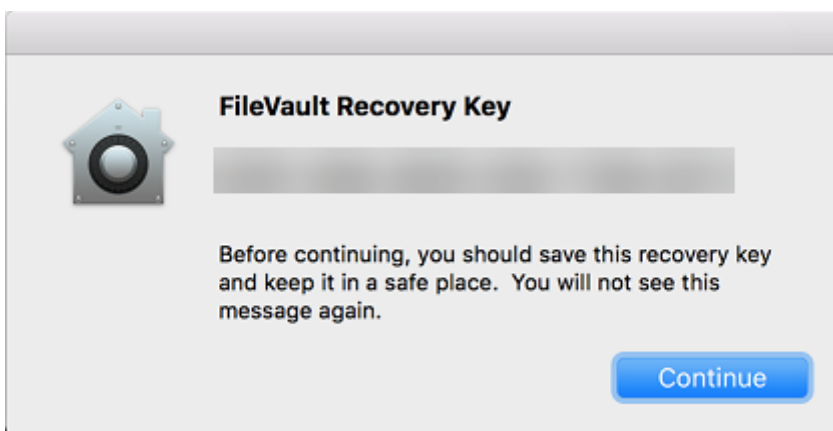
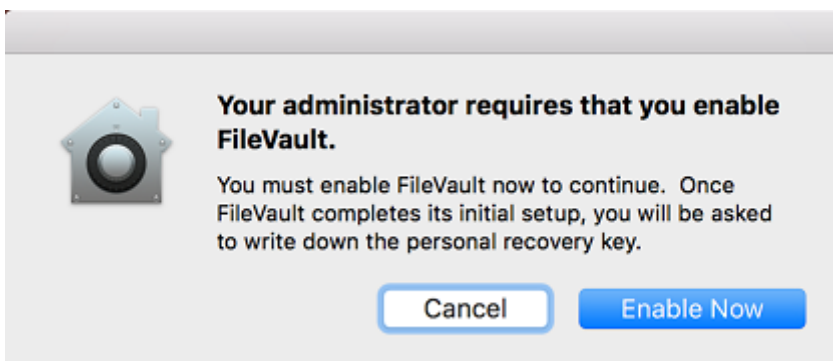
이설정을켜고 FileVault 정책을배포하면사용자가장치에서로그아웃할때다음화면이나타납니다. 이화면에는사용자가로그오프전에 FileVault 를사용하도록설정할수있는옵션이표시됩니다.



FileVault 설정을건너뛴최대횟수값이 0 이아닌경우: 이설정을끄고 FileVault 정책을배포하면사용자가로그온할때다음화면이나타납니다.



FileVault 설정을 건너뛸 때 횟수 값이 0 이거나 사용자가 최대 횟수로 설정을 건너뛴 경우 다음 화면이 나타납니다.



글꼴 장치 정책

January 6, 2020

iOS 및 macOS 장치에 글꼴을 더 추가하는 장치 정책을 XenMobile 에서 추가할 수 있습니다. 글꼴은 트루타입 (.ttf) 또는 오픈타입 (.oft) 형식이어야 합니다. 글꼴 모음 (.ttc 또는 .otc) 은 지원되지 않습니다.

iOS 의 경우, 이 정책은 iOS 7.0 이상의 버전에만 적용됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

- 사용자에게 표시되는 이름: 글꼴 목록에서 사용자에게 표시되는 이름을 입력합니다.
- 글꼴 파일: 찾아보기를 클릭하고 파일의 위치로 이동하여 사용자 장치에 추가할 글꼴 파일을 선택합니다.

macOS 설정

- 사용자에게 표시되는 이름: 글꼴 목록에서 사용자에게 표시되는 이름을 입력합니다.
- 글꼴 파일: 찾아보기를 클릭하고 파일의 위치로 이동하여 사용자 장치에 추가할 글꼴 파일을 선택합니다.

홈 화면 레이아웃 장치 정책

January 6, 2020

iOS 홈 화면의 앱 및 폴더 레이아웃을 지정할 수 있습니다. 홈 화면 레이아웃 장치 정책은 iOS 9.3 이상의 감독되는 장치에 적용됩니다.

중요:

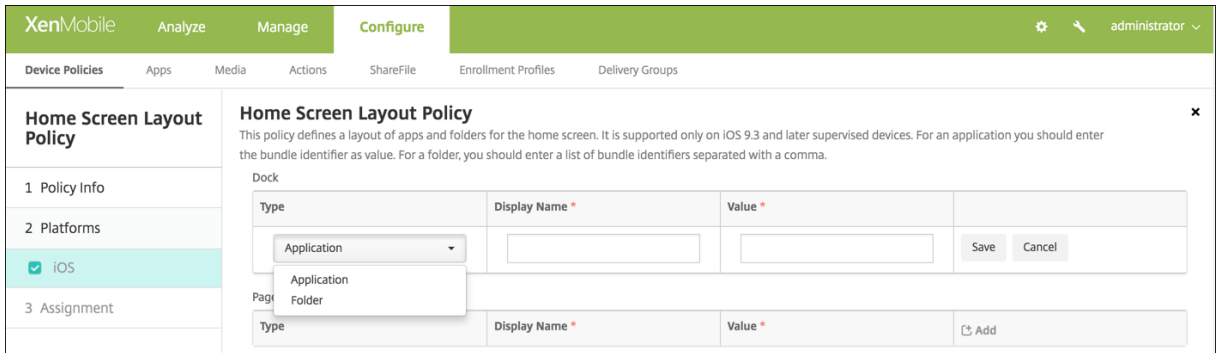
한 장치에 여러 개의 홈 화면 레이아웃 정책을 배포하면 장치에서 iOS 오류가 발생합니다. 제한은 이 XenMobile 정책 또는 Apple Configurator 를 통해 홈 화면을 정의할 때 적용됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing a sidebar with 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Home Screen Layout Policy' and includes a description: 'This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.' Below this, there are sections for 'Dock', 'Page 1', 'Page 2', 'Page 3', 'Page 4', and 'Page 5'. Each section contains a table with columns for 'Type', 'Display Name', and 'Value', along with an 'Add' button. The 'iOS' option is selected in the sidebar. At the bottom right, there are 'Back' and 'Next >' buttons.

- 구성할각화면영역 (예: **Dock** 또는 **1 페이지**) 에대해 추가를클릭합니다.
- 유형: 응용프로그램또는 폴더를선택합니다.



- 표시이름: 홈화면에표시되는앱또는폴더의이름입니다.
- 값: 앱의경우번들식별자입니다. 폴더의경우심표로구분된번들식별자목록입니다.

iOS 및 macOS 프로필장치정책가져오기

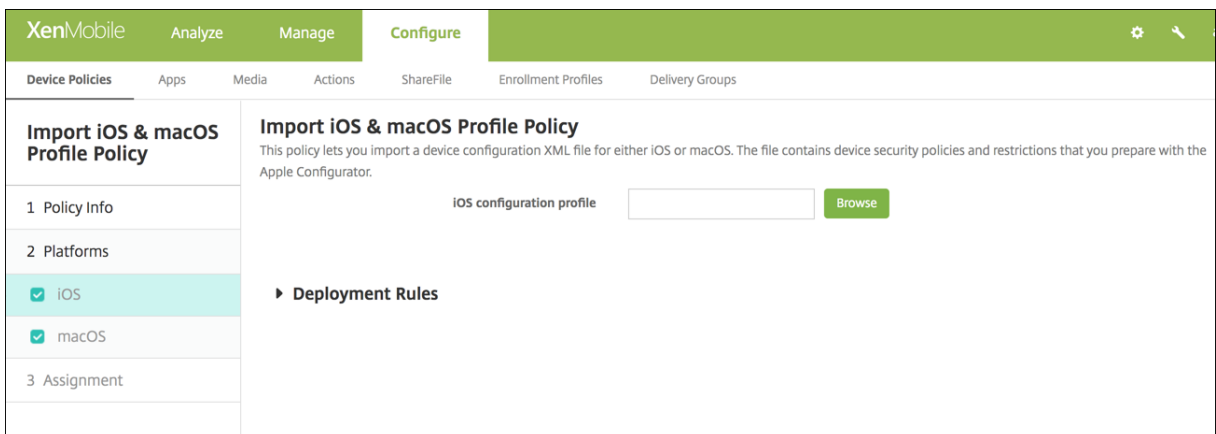
January 6, 2020

XenMobile 로 iOS 와 macOS 장치를위한장치구성 XML 파일을가져올수있습니다. 이파일에는 Apple Configurator 로 작성한장치보안정책및제한사항이포함되어있습니다.

이문서의뒷부분에 설명된대로 Apple Configurator 를 사용하여 iOS 장치를감독모드로설정 할수있습니다. Apple Configurator 를 사용하여구성파일을만드는방법에대한자세한내용은 [Apple Configurator Support\(Configurator 지원\)](#) 페이지를참조하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 및 macOS 설정



- **iOS** 구성프로필 또는 **macOS** 구성프로필: 가져올 구성파일을 선택하려면 찾아보기를 클릭하고 해당 파일 위치로 이동합니다.

Apple Configurator 를 사용하여 iOS 장치를 감독모드로 설정

Apple Configurator 를 사용하려면 macOS 10.7.2 이상을 실행하는 Apple 컴퓨터가 필요합니다.

중요:

감독모드로 장치를 설정하면 선택한 버전의 iOS 가 장치에 설치되어 이전에 저장된 사용자 데이터 또는 앱이 장치에서 완전히 초기화됩니다.

1. iTunes 에서 Apple Configurator 를 설치합니다.
2. Apple 컴퓨터에 iOS 장치를 연결합니다.
3. Apple Configurator 를 시작합니다. 감독을 위해 준비할 장치가 있다고 표시됩니다.
4. 감독할 장치를 준비하려면:
 - a) 감독 컨트롤을 켜짐으로 전환합니다. 정기적으로 구성을 다시 적용하여 장치에 대한 제어를 지속적으로 유지하려는 경우 이 설정을 선택하는 것이 좋습니다.
 - b) 필요에 따라 장치에 이름을 지정합니다.
 - c) iOS 에서 최신을 클릭하여 설치할 최신 버전의 iOS 를 검색합니다.
5. 장치를 감독하도록 준비할 수 있는 상태가 되면 **Prepare(준비)** 를 클릭합니다.

키오스크 장치 정책

January 6, 2020

키오스크 정책을 사용하면 다음과 같이 실행할 수 있는 앱을 제한하여 장치를 키오스크 모드로 제한할 수 있습니다.

- **Samsung SAFE** 장치의 경우: 특정 앱만 사용할 수 있도록 지정할 수 있습니다. 이 정책은 특정 유형 또는 클래스의 앱만 실행하도록 마련된 회사 장치에 유용합니다. 또한 이 정책을 사용하면 장치가 키오스크 모드 상태일 때 장치 홈 화면 및 잠금 화면 배경에 대한 사용자 지정 이미지를 선택할 수 있습니다.
- **COSU(회사 소유일회사용)** 장치라고도 하는 전용 **Android Enterprise** 장치의 경우: 앱을 화이트리스트에 추가하고 작업 잠금 모드를 설정할 수 있습니다. 기본적으로 **Secure Hub** 와 **Google Play** 서비스는 화이트리스트에 포함됩니다.

키오스크 모드에서 잠기는 장치의 일부는 XenMobile 을 통해 제어되지 않습니다. 정책을 배포한 후 장치에서 키오스크 모드 설정을 관리할 수 있습니다. 이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#) 에서 참조하십시오.

Samsung SAFE 장치를키오스크모드로만들려면

1. [Samsung MDM 라이선스키장치정책](#)에설명된대로모바일장치에서 Samsung SAFE API 키를사용하도록설정합니다. 이단계를통해 Samsung SAFE 장치에서정책을사용하도록설정할수있습니다.
2. [Firebase Cloud Messaging](#)에설명된대로 Android 장치에서 Firebase Cloud Messaging 을사용하도록설정합니다. 이단계를통해 Android 장치가다시 XenMobile 에연결될수있습니다.
3. 다음섹션에설명된대로키오스크장치정책을추가합니다.
4. 이세가지장치정책을적절한배달그룹에할당합니다. 배달그룹에앱인벤토리와같은다른정책을포함할지여부를고려합니다.

키오스크모드에서장치를제거하려면 키오스크모드가 사용안함으로설정된키오스크장치정책을만듭니다. 배달그룹을업데이트하여키오스크모드를사용하도록설정한키오스크정책을제거하고키오스크모드를사용하지않도록설정된키오스크정책을추가합니다.

키오스크장치정책을추가하려면

키오스크모드에서지정하는모든앱은사용자의장치에이미설치되어있어야합니다.

일부옵션은 Samsung MDM(모바일기기관리) API 4.0 이상에만적용됩니다.

Samsung SAFE 설정

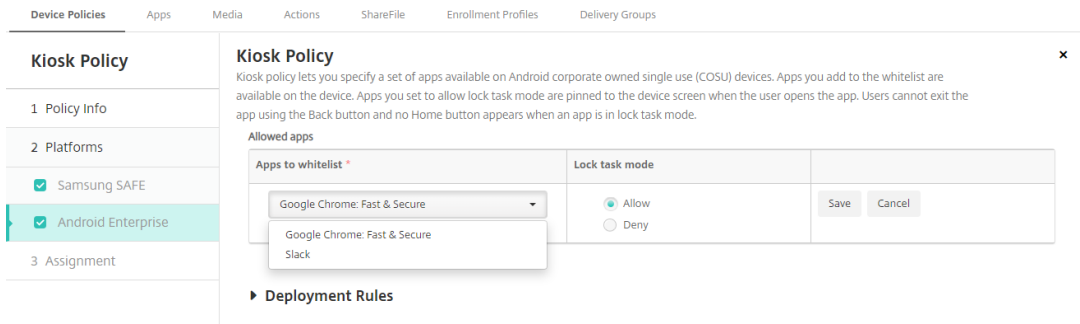
- 키오스크모드: 사용또는 사용안함을클릭합니다. 기본값은 사용입니다. 사용안함을클릭하면다음옵션이모두사라집니다.
- **Launcher** 패키지: 사용자가하나이상의키오스크앱을열수있는사내 Launcher 를개발하지않는경우이필드를비워두는것이 좋습니다. 사내 Launcher 를사용하는경우 Launcher 응용프로그램패키지의전체이름을입력합니다.
- 긴급전화번호: 선택적인전화번호를입력합니다. 분실한장치를찾기위해누구나이번호를사용하여회사에연락할수있습니다. MDM 4.0 이상에만적용됩니다.
- 탐색모음허용: 키오스크모드인동안사용자가탐색막대를보고사용하도록허용할지여부를선택합니다. MDM 4.0 이상에만적용됩니다. 기본값은 켜짐입니다.
- 다중창모드허용: 키오스크모드인동안사용자가다중창을사용하도록허용할지여부를선택합니다. MDM 4.0 이상에만적용됩니다. 기본값은 켜짐입니다.
- 상태표시줄허용: 키오스크모드인동안사용자가상태표시줄을표시하도록허용할지여부를선택합니다. MDM 4.0 이상에만적용됩니다. 기본값은 켜짐입니다.
- 시스템표시줄허용: 키오스크모드인동안사용자가시스템표시줄을표시하도록허용할지여부를선택합니다. 기본값은 켜짐입니다.
- 작업관리자허용: 키오스크모드인동안사용자가작업관리자를보고사용하도록허용할지여부를선택합니다. 기본값은 켜짐입니다.
- 공통 **SAFE** 암호변경: 이설정을사용하면공통 SAFE 암호필드의부주의한변경을방지할수있습니다. 이설정을 꺼짐으로 설정하면공통 SAFE 암호필드를변경할수없습니다. 기본값은 꺼짐입니다.
- 공통 **SAFE** 암호: 모든 Samsung SAFE 장치에대해일반암호정책을설정할경우이필드에해당암호를입력합니다.

- 배경화면
 - 홈배경화면정의: 키오스크모드인동안홈화면용사용자지정이미지를사용할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 홈이미지: 홈배경화면정의를사용하도록설정한경우 찾아보기를클릭하고파일의위치로이동하여이미지파일을선택합니다.
 - 잠금배경화면정의: 키오스크모드인동안잠금화면용사용자지정이미지를사용할지여부를선택합니다. 기본값은 꺼짐입니다. MDM 4.0 이상에만적용됩니다.
 - * 잠금이미지: 잠금배경화면정의를사용하도록설정한경우 찾아보기를클릭하고파일의위치로이동하여이미지파일을선택합니다.
- 앱: 키오스크모드에추가하려는각앱에대해 추가를클릭하고다음을수행합니다.
 - 추가할새앱: 추가할앱의전체이름을입력합니다. 예를들어 Android 일정앱을사용할수있게하려면 com.android.calendar 를입력합니다.
 - 저장을클릭하여앱을추가하거나 취소를클릭하여앱추가를취소합니다.

Android Enterprise 설정

앱을화이트리스트에포함하려면 추가를클릭합니다. 여러앱을화이트리스트에포함할수있습니다. 자세한내용은 [Android Enterprise](#)에서참조하십시오.

- 화이트리스트에추가할앱: 화이트리스트에추가할앱의패키지이름을입력하거나목록에서앱을선택합니다.
 - 새로추가를클릭하여목록에표시할승인된앱의패키지이름을입력합니다.
 - 목록에서기존앱을선택합니다. 목록에는 XenMobile 에업로드된앱이표시됩니다. 기본적으로 Secure Hub 와 Google Play 서비스는화이트리스트에포함됩니다.



- 작업잠금모드: 사용자가앱을시작할때장치화면에앱이고정되도록설정하려면 허용을선택합니다. 앱이고정되지않도록설정하려면 거부를선택합니다. 기본값은 허용입니다.

앱이작업잠금모드에있으면사용자가앱을열때앱이장치화면에고정됩니다. 홈단추가나타나지않고뒤로단추가비활성화됩니다. 사용자는로그아웃과같이앱에프로그래밍된작업을사용하여앱을종료할수있습니다.

Android 에대한 Launcher 구성장치정책

January 6, 2020

Citrix Launcher 를사용하면 XenMobile 에의해배포되는 Android 장치의사용자환경을사용자지정할수있습니다. Citrix Launcher 및 Launcher 구성장치정책은 Android Enterprise 와호환되지않습니다.

Launcher 구성정책을추가하여이러한 Citrix Launcher 기능을제어할수있습니다.

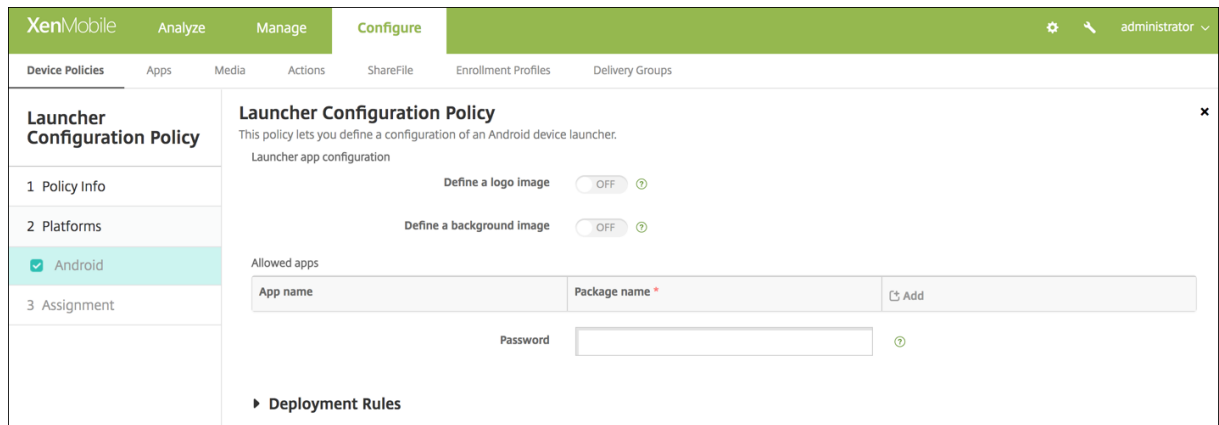
- 사용자가지정된앱에만액세스할수있도록 Android 장치를관리합니다.
- 필요에따라 Citrix Launcher 아이콘의사용자지정로고이미지와 Citrix Launcher 의사용자지정배경이미지를지정합니다.
- 사용자가 Launcher 를종료할때입력해야하는암호를지정합니다.

Citrix Launcher 를사용하면이러한장치수준제한을적용하는동시에사용자가 WiFi 설정, Bluetooth 설정및장치암호설정과같은장치설정에기본적으로액세스하여유연하게운영할수있습니다. Citrix Launcher 는장치플랫폼이이미제공하는보안에추가적인보안계층을더하기위한것이아닙니다.

Citrix Launcher 를배포하면 XenMobile 이 Launcher 를설치하고기본 Android Launcher 를대체합니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Android 설정



- 로고이미지정의: Citrix Launcher 아이콘에대한사용자지정로고이미지를사용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 로고이미지: 로고이미지정의를사용하는경우 찾아보기를클릭하고파일의위치로이동하여이미지파일을선택합니다. 지원되는파일형식은 PNG, JPG, JPEG 및 GIF 입니다.
- 배경이미지정의: Citrix Launcher 배경에대한사용자지정이미지를사용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 배경이미지: 배경이미지정의를사용하는경우 찾아보기를클릭하고파일의위치로이동하여이미지파일을선택합니다. 지원되는파일형식은 PNG, JPG, JPEG 및 GIF 입니다.
- 허용되는앱: Citrix Launcher 에서허용하려는각앱에대해 추가를클릭하고다음을수행합니다.

- 추가할 새 앱: 추가할 앱의 전체 이름을 입력합니다. 예를 들어 Android 일정 앱의 경우 `com.android.calendar` 를 입력합니다.
- 저장을 클릭하여 앱을 추가하거나 취소를 클릭하여 앱을 추가를 취소합니다.
- 암호: Citrix Launcher 를 종료할 때 사용자가 입력해야 하는 암호입니다.

LDAP 장치정책

January 6, 2020

XenMobile 에서 iOS 장치에 대한 LDAP 정책을 만들어 사용할 LDAP 서버에 대한 정보 (예: 필요한 계정 정보 등) 를 제공할 수 있습니다. 또한 LDAP 서버를 쿼리할 때 사용할 LDAP 검색 정책 집합을 제공합니다.

이 정책을 구성하려면 LDAP 호스트 이름이 필요합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치정책으로 이동합니다. 자세한 내용은 [장치정책](#)에서 참조하십시오.

iOS 설정

- 계정 설명: 선택적 계정 설명을 입력합니다.
- 계정 사용자 이름: 선택적 사용자 이름을 입력합니다.
- 계정 암호: 선택적 암호를 입력합니다. 이 필드는 암호화된 프로필에만 사용됩니다.
- **LDAP** 호스트 이름: LDAP 서버 호스트 이름을 입력합니다. 이것은 필수 필드입니다.
- **SSL** 사용: LDAP 서버에 대한 Secure Socket Layer 연결을 사용할지 여부를 선택합니다. 기본값은 켜져 있습니다.
- 검색 설정: LDAP 서버에 쿼리할 때 사용할 검색 설정을 추가합니다. 원하는 수의 검색 설정을 추가할 수 있지만 계정을 유용하게 사용하려면 적어도 하나 이상의 검색 설정을 추가해야 합니다. 추가를 클릭하고 다음을 수행합니다.
 - 설명: 검색 설정의 설명을 입력합니다. 이것은 필수 필드입니다.
 - 범위: 기준, 한 수준 또는 하위 트리를 선택하여 검색할 LDAP 트리의 깊이를 정의합니다. 기본값은 기준입니다.
 - * 기준은 검색 기준이 가리키는 노드를 검색합니다.
 - * 한 수준은 기준 노드와 한 수준 아래 노드를 검색합니다.
 - * 하위 트리는 기준 노드와 모든 하위 노드를 깊이에 관계없이 검색합니다.
 - 검색 기준: 검색을 시작할 노드에 대한 경로를 입력합니다. 예를 들어 `ou=people` 또는 `0=example corp` 을 입력합니다. 이것은 필수 필드입니다.
 - 저장을 클릭하여 검색 설정을 추가하거나 취소를 클릭하여 검색 설정 추가를 취소합니다.
 - 추가할 각 검색 설정에 대해 이 단계를 반복합니다.

macOS 설정

- 계정 설명: 선택적 계정 설명을 입력합니다.
- 계정 사용자 이름: 선택적 사용자 이름을 입력합니다.

- **계정암호:** 선택적암호를입력합니다. 이필드는암호화된프로필에만사용합니다.
- **LDAP 호스트이름:** LDAP 서버호스트이름을입력합니다. 이것은필수필드입니다.
- **SSL 사용:** LDAP 서버에대한 Secure Socket Layer 연결을사용할지여부를선택합니다. 기본값은 켜짐입니다.
- **검색설정:** LDAP 서버에쿼리할때사용할검색설정을추가합니다. 원하는수의검색설정을추가할수있지만계정을유용하게 사용하려면적어도하나이상의검색설정을추가해야합니다. 추가를클릭하고다음을수행합니다.
 - **설명:** 검색설정의설명을입력합니다. 이것은필수필드입니다.
 - **범위:** 기준, 한수준또는 하위트리를선택하여검색할 LDAP 트리의깊이를정의합니다. 기본값은 기준입니다.
 - * 기준은검색기준이가리키는노드를검색합니다.
 - * 한수준은기준노드와한수준아래노드를검색합니다.
 - * 하위트리는기준노드와모든하위노드를깊이에관계없이검색합니다.
 - **검색기준:** 검색을시작할노드에대한경로를입력합니다. 예를들어 ou=people 또는 0=example corp 을입력 합니다. 이것은필수필드입니다.
 - **저장을클릭하여검색설정을추가하거나 취소를클릭하여검색설정추가를취소합니다.**
 - **추가할각검색설정에대해이단계를반복합니다.**

위치장치정책

January 6, 2020

XenMobile 에서위치장치정책을만들어지리적경계를적용할수있습니다. 사용자가정의된경계 (지오펜스라고도함) 를위반하면 XenMobile 이특정동작을수행할수있습니다. 예를들어사용자가정의된경계를위반할경우사용자에게경고메시지를보내도록정책 을구성할수있습니다. 사용자가경계를위반할경우즉시또는지연후에사용자의회사데이터를초기화하는정책을구성할수있습니다. 장치추적및찾기사용여부와같은보안조치에대한자세한내용은 [보안동작](#)을참조하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

The screenshot shows the XenMobile Configuration console interface. The 'Configure' tab is active, and the 'Location Policy' is selected. The policy is configured for iOS. The settings are as follows:

Setting	Value	Unit
Location Timeout	1	Minutes
Tracking duration	6	Hours
Accuracy	328	Feet
Report if Location Services are disabled	OFF	
Geofencing	OFF	

Deployment Rules are also visible at the bottom of the configuration page.

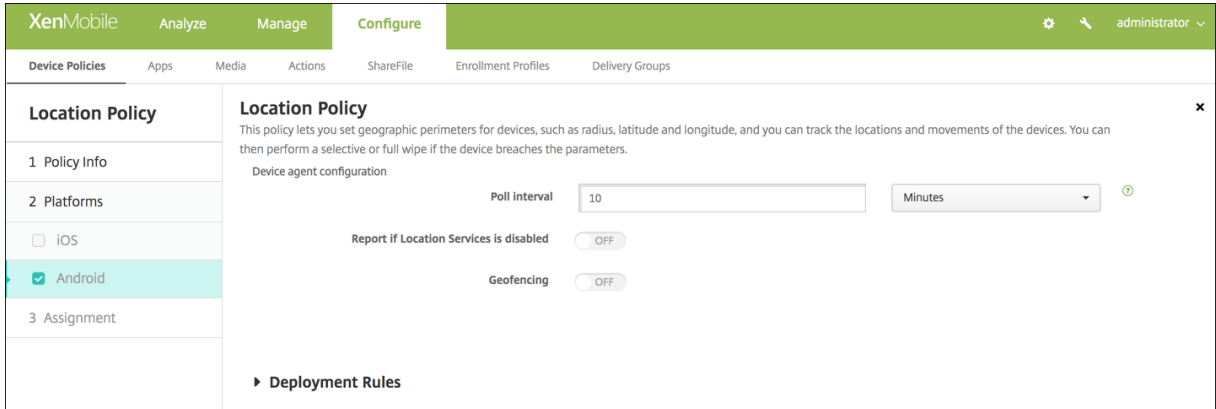
- **위치시간제한:** 숫자를입력한다음목록에서 초또는 분을클릭하여 XenMobile 이장치의위치를수정하려고시도하는빈도를설정합니다. 유효한값은 60~900 초또는 1~15 분입니다. 기본값은 1 분입니다.
- **추적기간:** 숫자를입력한다음목록에서 시간또는 분을클릭하여 XenMobile 이장치를추적하는기간을설정합니다. 유효한값은 1~6 시간또는 10~360 분입니다. 기본값은 6 시간입니다.
- **정확도:** 숫자를입력한다음목록에서 미터, 피트또는 야드를클릭하여 XenMobile 이장치를추적하는정확도를설정합니다. 유효한값은 10~5000 야드 (또는미터) 또는 30~15000 피트입니다. 기본값은 328 피트입니다.
- **위치서비스가사용하지않도록설정될경우보고: GPS 를사용하지않을때장치가 XenMobile 에보고서를보낼지여부를선택합니다. 기본값은 꺼짐입니다.**
- 지오펜스

The screenshot shows the Geofencing configuration screen. At the top, the 'Geofencing' toggle is turned ON. Below it, the 'Radius' is set to 16400, with a unit dropdown menu currently set to 'Feet'. The 'Center point latitude' and 'Center point longitude' fields are both set to 0.000000. At the bottom, there are two more toggles: 'Warn user on perimeter breach' and 'Wipe corporate data on perimeter breach', both of which are currently turned OFF.

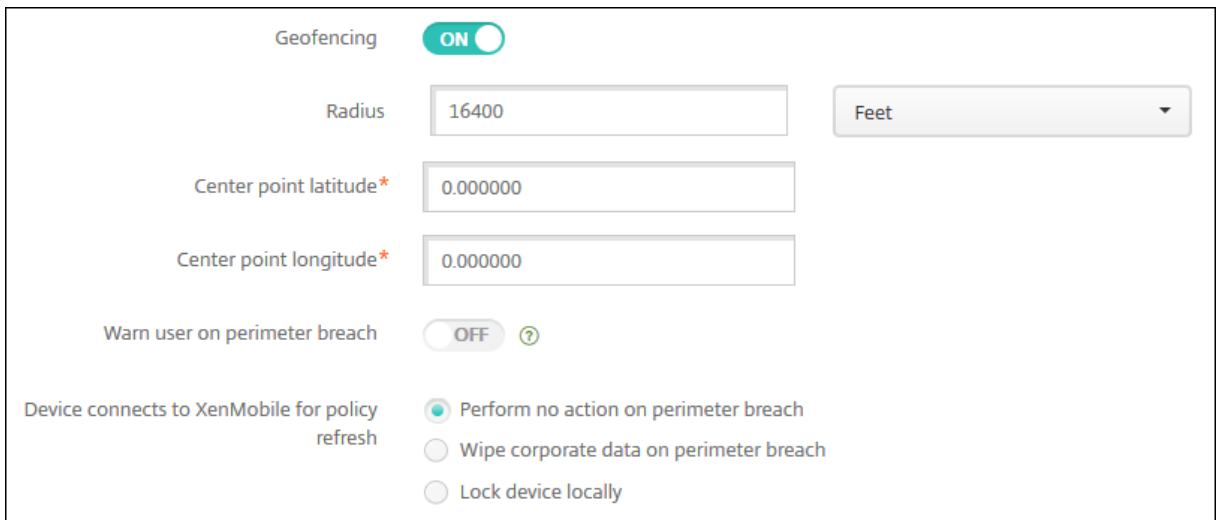
지오펜스를사용하도록설정할경우다음설정을구성합니다.

- **반경:** 숫자를입력한다음목록에서반경을측정하는데사용할단위를클릭합니다. 기본값은 16,400 피트입니다. 유효한반경은다음과같습니다.
 - 164~164000 피트
 - 50~50000 미터
 - 54~54680 야드
 - 1~31 마일
- **중심점위도:** 위도 (예: 37.787454) 를입력하여지오펜스중심점의위도를정의합니다.
- **중심점경도:** 경도 (예: 122.402952) 를입력하여지오펜스중심점의경도를정의합니다.
- **경계위반시사용자에게경고표시:** 사용자가정의된경계를위반할경우경고메시지를발행할지여부를선택합니다. 기본값은 꺼짐입니다. 경고메시지를표시하는데에는 XenMobile 연결이필요하지않습니다.
- **경계위반시회사데이터초기화:** 사용자의장치가경계를위반한경우장치를초기화할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을사용하도록설정하면 로컬초기화시지연필드가나타납니다.
 - 숫자를입력한다음목록에서 초또는 분을클릭하여사용자의장치에서회사데이터를초기화하기전에대기할기간을설정합니다. 이기간은 XenMobile 이사용자의장치를선택적으로초기화하기전에사용자가허용된위치로돌아갈수있는기회를제공합니다. 기본값은 0 초입니다.

Android 설정



- **폴링간격:** 숫자를입력한다음목록에서 분, 시간또는 일을클릭하여 XenMobile 이장치의위치를수정하려고시도하는빈도를설정합니다. 유효한값은 1~1440 분, 1~24 시간또는일수입니다. 기본값은 10 분입니다. 이값을 10 분미만으로설정하면장치의배터리수명이저하될수있습니다.
- **위치서비스가사용하지않도록설정될경우보고:** GPS 를사용하지않을때장치가 XenMobile 에보고서를보낼지여부를선택합니다. 기본값은 꺼짐입니다.
- **지오펠스**

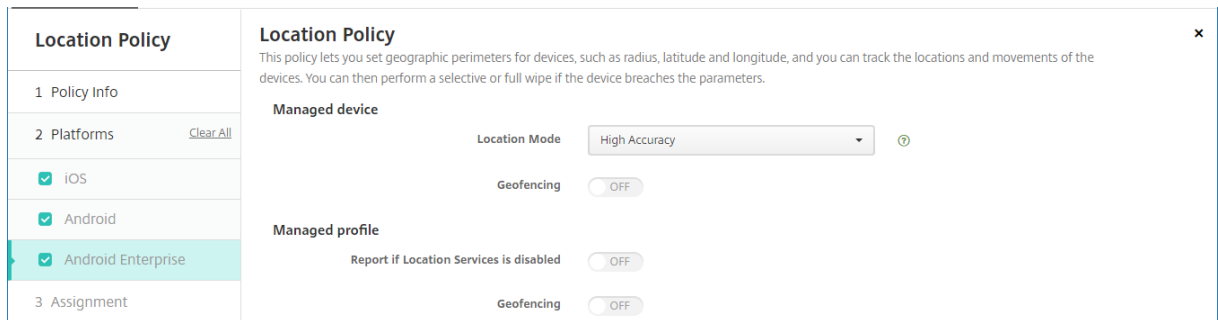


지오펠스를사용하도록설정할경우다음설정을구성합니다.

- **반경:** 숫자를입력한다음목록에서반경을측정하는데사용할단위를클릭합니다. 기본값은 16,400 피트입니다. 유효한반경은다음과같습니다.
 - 164~164000 피트
 - 1~50 킬로미터
 - 50~50000 미터
 - 54~54680 야드
 - 1~31 마일
- **중심점위도:** 위도 (예: 37.787454) 를입력하여지오펠스중심점의위도를정의합니다.

- **중심점경도:** 경도 (예: 122.402952) 를 입력하여 지오펜스 중심점의 경도를 정의합니다.
- **경계위반시 사용자에게 경고 표시:** 사용자가 정의된 경계를 위반할 경우 경고 메시지를 발행할지 여부를 선택합니다. 기본값은 꺼짐입니다. 경고 메시지를 표시하는데에는 XenMobile 연결이 필요하지 않습니다.
- **정책 새로고침을 위해 장치가 XenMobile 에 연결:** 사용자가 경계를 위반한 경우에 대해 다음 옵션 중 하나를 선택합니다.
 - **경계위반시 아무런 동작을 수행하지 않음:** 아무 작업도 하지 않습니다. 이것이 기본값입니다.
 - **경계위반시 회사 데이터 초기화:** 지정된 시간 이후 회사 데이터를 초기화합니다. 이 옵션을 사용하도록 설정하면 로컬 초기화 시 지연 필드가 나타납니다.
 - * 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 사용자의 장치에서 회사 데이터를 초기화하기 전에 대기할 시간을 설정합니다. 이 시간은 XenMobile 이 사용자의 장치를 선택적으로 초기화하기 전에 사용자가 허용된 위치로 돌아갈 수 있는 기회를 제공합니다. 기본값은 0 초입니다.
 - **잠금 시 지연:** 지정된 시간 이후 사용자의 장치를 잠급니다. 이 옵션을 사용하도록 설정하면 잠금 시 지연 필드가 나타납니다.
 - * 숫자를 입력한 다음 목록에서 초 또는 분을 클릭하여 사용자의 장치를 잠그기 전에 대기할 시간을 설정합니다. 이 시간은 XenMobile 이 사용자의 장치를 잠그기 전에 사용자가 허용된 위치로 돌아갈 수 있는 기회를 제공합니다. 기본값은 0 초입니다.

Android Enterprise 설정



관리되는 장치

- **위치 모드:** 사용할 위치 검색의 수준을 지정합니다. 위치 모드가 높은 정확도 또는 배터리 절약으로 설정된 경우에만 찾기도 사용할 수 있습니다. 기본값은 높은 정확도입니다.
 - **높은 정확도:** GPS, 네트워크 및 기타 센서를 포함한 모든 위치 검색 방법을 사용하도록 설정합니다.
 - **센서만:** GPS 및 기타 센서만 사용하도록 설정합니다.
 - **배터리 절약:** 네트워크 위치 공급자만 사용하도록 설정합니다.
 - **꺼짐:** 위치 검색을 사용하지 않습니다.
- **지오펜스:**

Geofencing ON

Poll interval *
 ⓘ

Radius *

Center point latitude *

Center point longitude *

Warn user on perimeter breach OFF ⓘ

Device connects to Endpoint Management for policy refresh

- Perform no action on perimeter breach
- Wipe corporate data on perimeter breach
- Lock device locally

지오펜스를 사용하도록 설정한 경우 다음 설정을 구성합니다.

- **폴링간격:** 숫자를 입력한 다음 분, 시간 또는 일을 클릭하여 XenMobile Server 가 장치의 위치를 수정하려고 시도하는 빈도를 설정합니다. 유효한 값은 1~1440 분, 1~24 시간 또는 일수입니다. 기본값은 **10** 분입니다. 이 값을 10 분 미만으로 설정하면 장치의 배터리 수명이 저하될 수 있습니다.
- **반경:** 숫자를 입력한 다음 반경을 측정하는 데 사용할 단위를 클릭합니다. 기본값은 **5,000 미터 (16,400 피트)** 입니다. 유효한 반경은 다음과 같습니다.
 - 164~164,000 피트
 - 1~50 킬로미터
 - 50~50,000 미터
 - 54~54,680 야드
 - 1~31 마일
- **중심점 위도:** 위도 (예: 37.787454) 를 입력하여 지오펜스 중심점의 위도를 정의합니다. 값을 조회하려면 관리 > 장치에서 장치를 선택하고 보안을 클릭한 다음 찾기를 클릭합니다. 장치를 찾은 후 XenMobile Server 는 보안 아래의 장치 세부 정보 > 일반 페이지에 장치 위치를 보고합니다.
- **중심점 경도:** 경도 (예: 122.402952) 를 입력하여 지오펜스 중심점의 경도를 정의합니다.
- **경계 위반 시 사용자에게 경고 표시:** 사용자가 정의된 경계를 위반할 경우 경고 메시지를 발행할 지 여부를 선택합니다. 기본값은 꺼짐입니다. 경고 메시지를 표시하는데에는 XenMobile Server 연결이 필요하지 않습니다.
- **정책 새로고침을 위해 장치가 XenMobile Server 에 연결:** 사용자가 경계를 위반한 경우에 대해 다음 옵션 중 하나를 선택합니다.
 - **경계 위반 시 아무런 동작을 수행하지 않음:** 아무 작업도 하지 않습니다. 이 설정은 기본값입니다.

- 경계위반시회사데이터초기화: 지정된시간이지난후회사데이터를초기화합니다. 이옵션을사용하도록설정하면 로컬초기화시지연필드가나타납니다.
 - * 숫자를입력한다음 초또는 분을클릭하여사용자의장치에서회사데이터를초기화하기전에초기화를지연할기간을설정합니다. 이지연기간은 XenMobile Server 가사용자의장치를선택적으로초기화하기전에사용자가허용된위치로돌아갈수있는기회를제공합니다. 기본값은 0 초입니다.
- 로컬에서장치잠금: 지정된시간이지난후사용자의장치를잠급니다. 이옵션을사용하도록설정하면 잠금시지연필드가나타납니다.
 - * 숫자를입력한다음 초또는 분을클릭하여사용자의장치를잠그기전에잠금을지연할기간을설정합니다. 이지연기간은 XenMobile Server 가사용자의장치를잠그기전에사용자가허용된위치로돌아갈수있는기회를제공합니다. 기본값은 0 초입니다.

관리되는프로필

- 위치서비스가사용하지않도록설정될경우보고: 사용자가 GPS 를꺼낸장치에서 XenMobile Server 에보고서를보낼지여부를선택합니다. 기본값은 꺼짐입니다.
- 지오펜스: [관리되는장치](#)에서이문서의설정을참조하십시오.

메일장치정책

January 6, 2020

XenMobile 에서메일장치정책을추가하여 iOS 또는 macOS 장치에서전자메일계정을구성할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 및 macOS 설정

The screenshot shows the 'Configure' section for 'Mail Policy'. The sidebar on the left has 'Mail Policy' selected, with sub-items '1 Policy Info', '2 Platforms' (containing 'iOS' and 'macOS' checkboxes), and '3 Assignment'. The main area contains the following configuration fields:

- Account description *
- Account type: IMAP (dropdown)
- Path prefix
- User display name *
- Email address *
- Incoming email section:
 - Email server host name *
 - Email server port *: 143
 - User name *
 - Authentication type: Password (dropdown)
 - Password

- 계정설명: 메일및설정앱에나타나는계정설명을입력합니다. 이것은필수필드입니다.
- 계정유형: **IMAP** 또는 **POP** 를선택하여사용자계정에사용할프로토콜을선택합니다. 기본값은 **IMAP** 입니다. **POP** 를 선택하면다음 경로접두사옵션이사라집니다.
- 경로접두사: **INBOX** 또는 **IMAP** 메일계정경로접두사를입력합니다. 이것은필수필드입니다.
- 사용자표시이름: 메시지및기타용도로사용할전체사용자이름을입력합니다. 이것은필수필드입니다.
- 전자메일주소: 계정의전체전자메일주소를입력합니다. 이것은필수필드입니다.
- 들어오는전자메일설정
 - 전자메일서버호스트이름: 들어오는메일서버호스트이름또는 IP 주소를입력합니다. 이것은필수필드입니다.
 - 전자메일서버포트: 들어오는메일서버포트번호를입력합니다. 기본값은 **143** 입니다. 이것은필수필드입니다.
 - 사용자이름: 전자메일계정의사용자이름을입력합니다. 이이름은일반적으로전자메일주소에서 @ 문자까지의부분과같습니다. 이것은필수필드입니다.
 - 인증유형: 사용할인증유형을선택합니다. 기본값은 암호입니다. 없음을선택하면다음 암호필드가사라집니다.
 - 암호: 들어오는메일서버에대한선택적암호를입력합니다.
 - **SSL** 사용: 들어오는메일서버가 **SSL(Secure Socket Layer)** 인증을사용하는지여부를선택합니다. 기본값은 꺼짐입니다.
- 나가는전자메일설정
 - 전자메일서버호스트이름: 나가는메일서버호스트이름또는 IP 주소를입력합니다. 이것은필수필드입니다.
 - 전자메일서버포트: 나가는메일서버포트번호를입력합니다. 포트가없는경우포트번호를입력하지않으면지정된프로토콜의기본포트가사용됩니다.
 - 사용자이름: 전자메일계정의사용자이름을입력합니다. 이이름은일반적으로전자메일주소에서 @ 문자까지의부분과같습니다. 이것은필수필드입니다.
 - 인증유형: 사용할인증유형을선택합니다. 기본값은 암호입니다.
 - 암호: 나가는메일서버에대한선택적암호를입력합니다.

- 나가는암호와들어오는암호가같음: 들어오는암호와나가는암호가같은지여부를선택합니다. 기본값은 꺼짐이며, 이는암호가다르다는의미입니다.
- **SSL** 사용: 나가는메일서버가 SSL(Secure Socket Layer) 인증을사용하는지여부를선택합니다. 기본값은 꺼짐입니다.
- 정책
 - 계정간전자메일이동승인: 사용자가이계정에서다른계정으로전자메일을이동하고다른계정에서전자메일을전달하고회신할수있도록허용할지여부를선택합니다. 기본값은 꺼짐입니다.
 - 메일앱에서만전자메일보내기: 전자메일을보낼사용자를 iOS 메일앱으로제한할지여부를선택합니다.
 - 최근메일동기화사용안함: 사용자가최근주소를동기화하지못하도록할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 6.0 이상에만적용됩니다.
 - 메일삭제허용: iOS 9.2 이상을실행하는장치에서 Apple Mail Drop 의사용을허용할지여부를선택합니다. 기본값은 꺼짐입니다.
 - **S/MIME** 서명사용: 이계정이 S/MIME 서명을지원하는지여부를선택합니다. 기본값은 켜짐입니다. 켜짐으로설정하면다음필드가나타납니다.
 - * 서명 ID 자격증명: 사용할서명자격증명을선택합니다.
 - * **S/MIME** 서명사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서 S/MIME 서명을켜거나꺼낼수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.
 - * **S/MIME** 서명인증서 UUID 사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서사용할서명자격증명을선택할수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.
 - **S/MIME** 암호화사용: 이계정이 S/MIME 암호화를지원하는지여부를선택합니다. 기본값은 꺼짐입니다. 켜짐으로설정하면다음필드가나타납니다.
 - * 암호화 ID 자격증명: 사용할암호화자격증명을선택합니다.
 - * 메시지별 **S/MIME** 전환사용: 켜짐으로설정하면작성하는각메시지에대해 S/MIME 암호화를켜거나꺼낼수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
 - * 기본적으로 **S/MIME** 암호화사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서 S/MIME 를기본적으로켜지여부를선택할수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.
 - * **S/MIME** 암호화인증서 UUID 사용자재정의가능: 켜짐으로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나꺼낼수있습니다. 기본값은 꺼짐입니다. 이 옵션은 iOS 12.0 이상에적용됩니다.
- 정책설정
 - 정책제거: 나중에정책을제거하려면 날짜선택또는 제거할때까지의기간 (시간) 에서정책을제거하도록이설정을구성하면됩니다.
 - 사용자가정책을제거하도록허용: 사용자가메일정책을제거하는것을 항상허용하거나, 암호필요로만허용하거나 안함으로설정합니다.
 - 프로필범위: macOS 에한해정책을 사용자수준별로적용할지전체 시스템에적용할지를선택합니다.

관리되는도메인장치정책

January 6, 2020

전자메일 및 Safari 브라우저에 적용되는 관리되는 도메인을 정의할 수 있습니다. 관리되는 도메인을 사용하면 Safari 를 사용하여 도메인에서 다운로드한 문서를 열 수 있는 앱을 제어함으로써 회사 데이터를 보호할 수 있습니다.

iOS 8 이상의 감독되는 장치의 경우 URL 또는 하위도메인을 지정하여 사용자가 브라우저에서 문서, 첨부파일 및 다운로드를 열 수 있는 방법을 제어할 수 있습니다. iOS 9.3 이상의 감독되는 장치의 경우 사용자가 Safari 에서 암호를 저장할 수 있는 URL 을 지정할 수 있습니다.

iOS 장치를 감독 모드로 설정하는 단계는 [Apple Configurator 를 사용하여 iOS 장치를 감독 모드로 전환](#)을 참조하십시오.

사용자가 관리되는 전자메일 도메인 목록에 없는 도메인의 받는 사람에게 전자메일을 보낼 경우 사용자 장치에서 회사 도메인 외부의 사람에게 메시지를 보낸다는 경고가 표시됩니다.

문서, 첨부파일 또는 다운로드 등의 항목: 사용자가 관리되는 웹도메인 목록에 있는 웹도메인에서 Safari 를 사용하여 항목을 열면 관련 회사 앱에서 항목이 열립니다. 해당 항목이 관리되는 웹도메인 목록의 웹도메인에 없는 경우 사용자가 회사 앱으로 항목을 열 수 없고 관리되지 않는 개인 앱을 사용해야 합니다.

감독되는 장치의 경우 Safari 암호 자동 채우기도메인을 지정하지 않더라도 장치가 임시 다중 사용자로 구성된 경우 사용자가 암호를 저장할 수 없습니다. 그러나 임시 다중 사용자로 구성되지 않은 장치에서는 사용자가 모든 암호를 저장할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

도메인을 지정하려면:

형식	설명
<code>example.com</code>	<code>site.example.com/</code> 을 제외하고, <code>example.com</code> 아래의 모든 경로를 관리되는 경로로 처리합니다.
<code>foo.example.com</code>	<code>example.com/</code> 또는 <code>bar.example.com/</code> 을 제외하고, <code>foo.example.com</code> 아래의 모든 경로를 관리되는 경로로 처리합니다.
<code>*.example.com</code>	<code>example.com/</code> 을 제외하고, <code>foo.example.com</code> 또는 <code>bar.example.com</code> 아래의 모든 경로를 관리되는 경로로 처리합니다.
<code>example.com/sub</code>	<code>example.com/</code> 을 제외하고, <code>example.com/sub</code> 와 그 아래 모든 경로를 관리되는 경로로 처리합니다.
<code>foo.example.com/sub</code>	<code>example.com</code> , <code>example.com/sub</code> , <code>foo.example.com/</code> 또는 <code>bar.example.com/sub</code> 를 제외하고, <code>foo.example.com/sub</code> 아래의 모든 경로를 관리되는 경로로 처리합니다.

형식	설명
*.example.com/sub	example.com 또는 foo.example.com/을 제외하고, foo.example.com/sub 또는 bar.example.com/sub 아래의 모든 경로를 관리되는 경로로 처리합니다.

규칙:

- 도메인 비교시 URL 의 선행 “www” 와 후행 슬래시는 무시됩니다.
- 포트 번호가 포함된 항목의 경우 해당 포트 번호를 지정하는 주소만 관리되는 주소로 간주됩니다. 그 외 항목의 경우 표준 포트 (http 의 경우 포트 80, https 의 경우 포트 443) 만 관리되는 것으로 간주됩니다. 예를 들어 *.example.com:8080 패턴은 https://site.example.com:8080/page.html 과 일치하지만 https://site.example.com/page.html 과는 일치하지 않는 한편, *.example.com 패턴은 https://site.example.com/page.html 및 https://site.example.com/page.html 과 일치하지만 https://site.example.com:8080/page.html 과는 일치하지 않습니다.
- 관리되는 Safari 웹도메인 정의는 누적됩니다. 관리되는 Safari 웹도메인 페이로드에 의해 정의되는 패턴은 모두 URL 요청과 일치시키는 데 사용됩니다.

설정:

- 관리되는 도메인
 - 표시되지 않은 전자메일도메인: 목록에 포함하려는 각 전자메일도메인에 대해 추가를 클릭한 후 다음을 수행합니다.
 - * 관리되는 전자메일도메인: 전자메일도메인을 입력합니다.
 - * 전자메일도메인을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.
 - 관리되는 Safari 웹도메인: 목록에 포함하려는 각 웹도메인에 대해 추가를 클릭한 후 다음을 수행합니다.
 - * 관리되는 웹도메인: 웹도메인을 입력합니다.
 - * 웹도메인을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.
 - Safari 암호 자동 채우기도메인: 목록에 포함하려는 각 자동 채우기도메인에 대해 추가를 클릭한 후 다음을 수행합니다.
 - * Safari 암호 자동 채우기도메인: 자동 채우기도메인을 입력합니다.
 - * 자동 채우기도메인을 저장하려면 저장을 클릭하고 저장하지 않으려면 취소를 클릭합니다.

MDM 옵션 장치 정책

January 6, 2020

감독되는 iOS 7.0 이상의 전화 장치에서 내 전화 찾기 및 iPad 활성화 잠금을 관리하는 장치 정책을 XenMobile 에서 만들 수 있습니다. iOS 장치를 감독 모드로 설정하는 단계는 [Apple Configurator](#) 를 사용하여 iOS 장치를 감독 모드로 전환을 참조하십시오.

활성화 잠금은 분실되거나 도난당한 장치의 재활성화를 방지하는 내 iPhone/iPad 찾기 기능입니다. 활성화 잠금은 누군가가 내

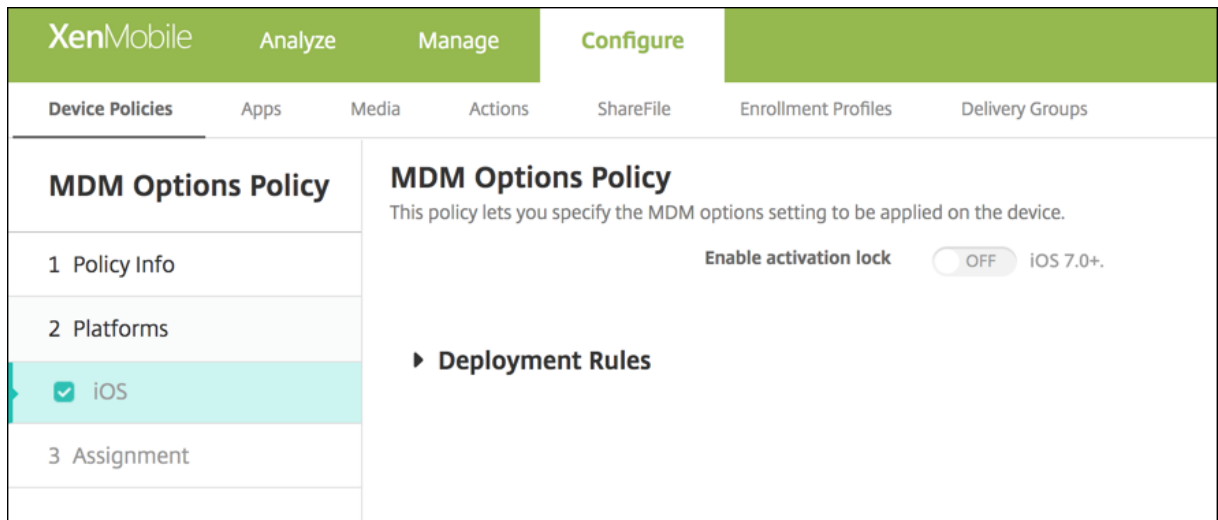
iPhone/iPad 찾기를 끄고 장치를 지우거나 장치를 재활성화하여 사용하려고 할 경우 사용자의 Apple ID 와 암호를 요구합니다. 조직이 소유한 장치의 경우 예를 들어 장치를 재설정하거나 재할당하기 위해 활성화 잠금을 바이패스해야 합니다.

활성화 잠금을 사용하도록 설정하려면 XenMobile MDM 옵션 장치 정책을 구성하고 배포합니다. 그러면 사용자의 Apple 자격 증명 없이도 XenMobile 콘솔에서 장치를 관리할 수 있습니다. 활성화 잠금의 Apple 자격 증명 요구 사항을 바이패스하려면 XenMobile 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행합니다.

예를 들어 사용자가 분실된 휴대폰을 반환하거나 전체 초기화 전후에 장치를 설정하는 경우 iTunes 계정 자격 증명을 묻는 메시지가 표시될 때 XenMobile 콘솔에서 활성화 잠금 바이패스 보안 동작을 실행하여 이 단계를 바이패스할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정



- 활성화 잠금 사용: 이 정책을 배포할 장치에서 활성화 잠금을 사용했는지 선택합니다. 기본값은 꺼짐입니다.

MDM 옵션 장치 정책을 배포하여 활성화 잠금을 사용하도록 설정하면 관리 > 장치 페이지에서 해당 장치를 선택하고 보안을 클릭할 때 보안 동작 활성화 잠금 바이패스가 표시됩니다. 활성화 잠금 바이패스를 사용하면 장치 사용자의 Apple ID 및 암호를 몰라도 장치 활성화 전에 감독되는 장치에서 활성화 잠금을 해제할 수 있습니다. 전체 초기화 전후에 활성화 잠금 바이패스를 장치에 전송할 수 있습니다. 자세한 내용은 보안 동작 문서에서 [iOS 활성화 잠금 바이패스](#)를 참조하십시오.

조직 정보 장치 정책

January 6, 2020

XenMobile 에서 iOS 장치에 푸시되는 알림 메시지에 대한 조직 정보를 지정하는 장치 정책을 XenMobile 에서 추가할 수 있습니다. iOS 7 이상의 장치에서 이 정책을 사용할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

- 이름: XenMobile 을 실행하는 조직의 이름을 입력합니다.
- 주소: 조직의 주소를 입력합니다.
- 전화: 조직의 지원 전화번호를 입력합니다.
- 전자메일: 지원 전자메일 주소를 입력합니다.
- 매직: 조직에서 관리하는 서비스를 설명하는 단어 나 구절을 입력합니다.

암호장치정책

January 6, 2020

조직의 표준에 따라 XenMobile 에서 암호정책을 만듭니다. 사용자의 장치에 암호를 요구할 수 있으며 다양한 형식 및 암호 규칙을 설정할 수 있습니다. iOS, macOS, Android, Samsung KNOX, Android Enterprise, Windows Phone 및 Windows Desktop/Tablet 에 대한 정책을 만들 수 있습니다. 각 플랫폼마다 이 문서에서 설명되어 있는 서로 다른 값 집합이 필요합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치정책으로 이동합니다. 자세한 내용은 [장치정책](#)에서 참조하십시오.

iOS 설정

The screenshot shows the XenMobile configuration interface for a Passcode Policy. The 'Configure' tab is active, and the 'Passcode Policy' section is selected in the left sidebar. The main content area displays the following settings:

- Passcode required:** ON (toggle)
- Passcode requirements:**
 - Minimum length:** 6 (dropdown)
 - Allow simple passcodes:** ON (toggle)
 - Required characters:** OFF (toggle)
 - Minimum number of symbols:** 0 (dropdown)
- Passcode security:**
 - Device lock grace period (minutes of inactivity):** None (dropdown)
 - Lock device after (minutes of inactivity) (0-999):** None (dropdown)
 - Passcode expiration in days (1-730):** 0 (input field)
 - Previous passcodes saved (0-50):** 0 (input field)

- 암호필요: 암호를 요구하고 iOS 암호장치정책의 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안 및 정책 설정에 대한 설정을 구성할 수 있게 됩니다.
- 암호 요구 사항

- 최소길이: 목록에서최소암호길이를클릭합니다. 기본값은 **6** 입니다.
- 단순암호허용: 단순암호를허용할지여부를선택합니다. 단순암호는반복적또는순차적문자집합입니다. 기본값은 켜짐입니다.
- 필수문자: 암호에적어도문자가하나있어야하는지여부를선택합니다. 기본값은 꺼짐입니다.
- 최소기호개수: 목록에서암호에포함되어야하는기호의수를클릭합니다. 기본값은 **0** 입니다.
- 암호보안
 - 장치잠금유예기간 (비활성시간 (분)): 목록에서잠긴장치의잠금을해제하려는사용자가암호를입력해야하는기간을클릭합니다. 기본값은 없음입니다.
 - 다음비활성시간 (분) 이후장치잠금: 목록에서장치가잠기지않고비활성상태를유지할수있는기간을클릭합니다. 기본값은없음입니다.
 - 암호만료 (일)(1-730): 암호가만료되기전까지남은일수를입력합니다. 유효한값은 1 부터 730 까지입니다. 기본값은 **0** 이며, 암호가만료되지않는다는의미입니다.
 - 이전암호저장 (0-50): 저장할이전암호수를입력합니다. 사용자는이목록에있는암호를사용할수없습니다. 유효한값은 0 부터 50 까지입니다. 기본값은 **0** 이며, 사용자가암호를재사용할수있다는의미입니다.
 - 최대로그온시도실패횟수: 목록에서사용자가로그인에실패할수있는횟수를클릭합니다. 이횟수를넘으면장치가전체초기화됩니다. 기본값은 정의되지않음입니다.
- 정책설정
 - 정책제거옆에서 날짜선택또는 제거할때까지의기간 (시간) 을클릭합니다.
 - 날짜선택을클릭하는경우달력을클릭하여제거할날짜를선택합니다.
 - 사용자가정책을제거하도록허용목록에서 항상, 암호필요또는 안함을클릭합니다.
 - 암호필요를클릭하는경우 제거암호옆에필요한암호를입력합니다.

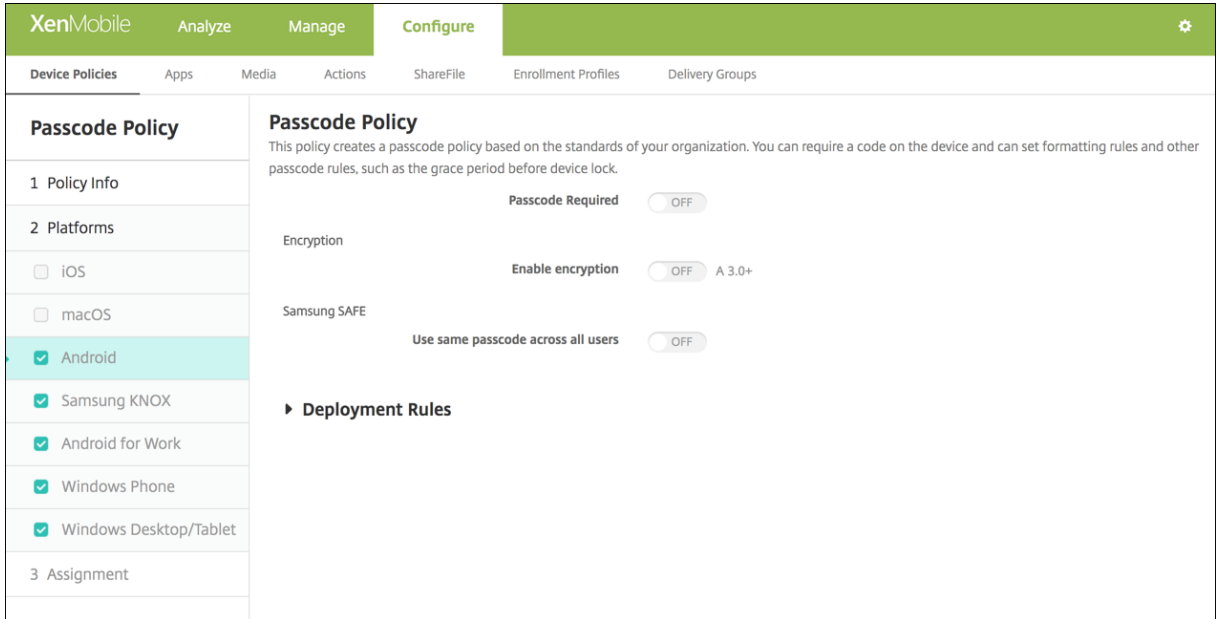
macOS 설정

The screenshot shows the XenMobile Configure interface for a Passcode Policy. The left sidebar lists various platforms, with macOS selected. The main content area shows the following settings:

- Passcode Policy**: This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
- Passcode required**: OFF (toggle)
- Passcode security**:
 - Delay after failed sign-on attempts, in minutes**: [Empty input field]
- Policy Settings**:
 - Profile scope**: User (dropdown menu)
 - macOS 10.7+
- Deployment Rules**: (Expandable section)

- **암호필요:** 암호를 요구하고 iOS 암호장치정책의 구성 옵션을 표시하려면 이 옵션을 선택합니다. 페이지가 확장되어 암호 요구 사항, 암호 보안 및 정책 설정에 대한 설정을 구성할 수 있게 됩니다.
- **암호필요를 사용하지 않으려면 로그인 시도에 실패한 후 지연 시간 (분) 옆에 사용자가 암호를 다시 입력할 수 있게 될 때까지 대기하는 시간 (분) 을 입력합니다.**
- **암호필요를 사용하도록 설정한 경우 다음 설정을 구성합니다.**
- **암호 요구 사항**
 - **최소 길이:** 목록에서 최소 암호 길이를 클릭합니다. 기본값은 **6** 입니다.
 - **단순 암호 허용:** 단순 암호를 허용할지 여부를 선택합니다. 단순 암호는 반복적 또는 순차적 문자 집합입니다. 기본값은 켜짐입니다.
 - **필수 문자:** 암호에 적어도 문자가 하나 있어야 하는지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **최소 기호 개수:** 목록에서 암호에 포함되어야 하는 기호의 수를 클릭합니다. 기본값은 **0** 입니다.
- **암호 보안**
 - **장치 잠금 유예 기간 (비활성 시간 (분)):** 목록에서 잠긴 장치의 잠금을 해제하려는 사용자가 암호를 입력해야 하는 기간을 클릭합니다. 기본값은 없음입니다.
 - **다음의 비활성 시간 (분) 이후 장치 잠금:** 목록에서 장치가 잠기지 않고 비활성 상태를 유지할 수 있는 기간을 클릭합니다. 기본값은 없음입니다.
 - **암호 만료 (일)(1-730):** 암호가 만료되기 전까지 남은 일수를 입력합니다. 유효한 값은 1 부터 730 까지입니다. 기본값은 **0** 이며, 암호가 만료되지 않는다는 의미입니다.
 - **이전 암호 저장 (0-50):** 저장할 이전 암호 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0 부터 50 까지입니다. 기본값은 **0** 이며, 사용자가 암호를 재사용할 수 있다는 의미입니다.
 - **최대 로그인 시도 실패 횟수:** 목록에서 사용자가 로그인에 실패할 수 있는 횟수를 클릭합니다. 이 횟수를 넘으면 장치가 잠깁니다. 기본값은 정의되지 않음입니다.
 - **로그인 시도에 실패한 후 지연 시간 (분):** 사용자가 암호를 다시 입력할 수 있게 될 때까지 대기하는 시간 (분) 을 입력합니다.
- **정책 설정**
 - 정책 제거 옆에서 날짜 선택 또는 제거할 때까지의 기간 (시간) 을 클릭합니다.
 - 날짜 선택을 클릭하는 경우 달력을 클릭하여 제거할 날짜를 선택합니다.
 - 사용자가 정책을 제거하도록 허용 목록에서 항상, 암호 필요 또는 안함을 클릭합니다.
 - 암호 필요를 클릭하는 경우 제거 암호 옆에 필요한 암호를 입력합니다.
 - 프로필 범위 옆에서 사용자 또는 시스템을 클릭합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.

Android 설정



참고:

Android 의기본설정은 꺼짐입니다.

- **암호필요:** 암호를요구하고 Android 암호장치정책의구성옵션을표시하려면이옵션을선택합니다. 페이지가확장되어암호요구사항, 암호보안, 암호화및 Samsung SAFE 에대한설정을구성할수있게됩니다.
- **암호요구사항**
 - **최소길이:** 목록에서최소암호길이를클릭합니다. 기본값은 6 입니다.
 - **생체인식:** 생체인식을사용할지여부를선택합니다. 이옵션을사용하도록설정하면필수문자필드가숨겨집니다. 기본값은 꺼짐입니다.
 - **필수문자:** 목록에서제한없음, 숫자와문자모두, 숫자만또는문자만을클릭하여암호가구성되는방식을구성합니다. 기본값은제한없음입니다.
 - **고급규칙:** 고급암호규칙을적용할지여부를선택합니다. 이옵션은 Android 3.0 이상에서사용할수있습니다. 기본값은 꺼짐입니다.
 - **고급규칙을사용하도록설정**한경우다음과같은목록각각에서암호에포함되어야하는각문자유형의최소수를클릭합니다.
 - * **기호:** 기호의최소수입니다.
 - * **문자:** 문자의최소수입니다.
 - * **소문자:** 소문자의최소수입니다.
 - * **대문자:** 대문자의최소수입니다.
 - * **숫자또는기호:** 숫자또는기호의최소수입니다.
 - * **숫자:** 숫자의최소수입니다.
- **암호보안**

- 다음의비활성시간 (분) 이후장치잠금: 목록에서장치가잠기지않고비활성상태를유지할수있는기간을클릭합니다. 기본값은 없음입니다.
- 암호만료 (일)(1-730): 암호가만료되기전까지남은일수를입력합니다. 유효한값은 1 부터 730 까지입니다. 기본값은 0 이며, 암호가만료되지않는다는의미입니다.
- 이전암호저장 (0-50): 저장할이전암호수를입력합니다. 사용자는이목록에있는암호를사용할수없습니다. 유효한값은 0 부터 50 까지입니다. 기본값은 0 이며, 사용자가암호를재사용할수있다는의미입니다.
- 최대로그온시도실패횟수: 목록에서사용자가로그인에실패할수있는횟수를클릭합니다. 이횟수를넘으면장치가초기화됩니다. 기본값은 정의되지않음입니다.

• 암호화

- 암호화사용: 암호화를사용하도록설정하지여부를선택합니다. 이옵션은 Android 3.0 이상에서사용할수있습니다. 이옵션은 암호필요설정과관계없이사용할수있습니다.

장치를암호화하려면충전된배터리로시작하고암호화가실행되는수시간동안장치를꽂힌상태로유지해야합니다. 암호화프로세스가중단되면장치데이터중일부또는전부가손실될수있습니다. 장치를암호화한후에는프로세스를되돌릴수없으며, 암호화를취소하는유일한방법은장치의모든데이터를지우고공장기본값으로재설정하는것입니다.

• Samsung SAFE

참고:

Samsung SAFE 장치에서얼굴또는홍채인식을사용하지않도록설정할경우해결방법: Samsung SAFE 용제한장치정책을만듭니다. 제한정책에서 응용프로그램사용안함을켜고테이블에 com.samsung.android.bio.face.service 또는 com.samsung.android.server.iris를추가합니다. 그런다음제한정책을배포합니다.

- 모든사용자가동일한암호사용: 모든사용자에게동일한암호를사용하지여부를선택합니다. 기본값은 꺼짐입니다. 이 설정은 Samsung SAFE 장치에만적용되며 암호필요설정과관계없이사용할수있습니다.
- 모든사용자가동일한암호사용을사용하도록설정할경우 암호필드에모든사용자가사용할암호를입력합니다.
- 암호필요를사용하도록설정할경우다음과같은 Samsung SAFE 설정을구성합니다.
 - * 변경된문자: 사용자가이전암호에서변경해야하는문자수를입력합니다. 기본값은 0 입니다.
 - * 한문자의최대사용횟수: 한문자가암호에서발생할수있는최대횟수를입력합니다. 기본값은 0 입니다.
 - * 연속영문자길이: 암호에서연속될수있는영문자의최대길이를입력합니다. 기본값은 0 입니다.
 - * 연속숫자길이: 암호에서연속될수있는숫자의최대길이를입력합니다. 기본값은 0 입니다.
 - * 사용자에게암호표시허용: 사용자가암호를볼수있는지여부를선택합니다. 기본값은 켜짐입니다.
 - * 생체인증구성. 생체인증을사용하도록설정하지여부를선택합니다. 기본값은 꺼짐입니다. 켜짐으로설정하는경우다음과같은옵션을설정할수있습니다.
 - 지문허용. 사용자가지문을사용하여인증할수있도록하려면이옵션을선택합니다.
 - 홍채허용. 사용자가홍채를사용하여인증할수있도록하려면이옵션을선택합니다.
 - * 금지된문자열: 금지된 문자열을만들어사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등과같이쉽게추측할수있는안전하지않은문자열을사용하지못하게합니다. 거부하려는각문자열에 대해 추가를클릭한후다음을수행합니다.
 - 금지된문자열: 사용자가사용할수없는문자열을입력합니다.

- 저장을클릭하여문자열을추가하거나 취소를클릭하여문자열추가를취소합니다.

Samsung KNOX 설정

- 암호요구사항
 - 최소길이: 목록에서최소암호길이를클릭합니다. 기본값은 **6** 입니다.
 - 사용자에게암호표시허용: 사용자가암호를볼수있는지여부를선택합니다.
 - 금지된문자열: 금지된문자열을만들어사용자가 “password”, “pwd”, “welcome”, “123456”, “11111” 등 과같이쉽게추측할수있는안전하지않은문자열을사용하지못하게합니다. 거부하려는각문자열에대해추가를클릭한 후다음을수행합니다.
 - * 금지된문자열: 사용자가사용할수없는문자열을입력합니다.
 - * 저장을클릭하여문자열을추가하거나 취소를클릭하여문자열추가를취소합니다.
- 최소개수
 - 변경된문자: 사용자가이전암호에서변경해야하는문자수를입력합니다. 기본값은 **0** 입니다.
 - 기호: 암호에필요한기호의최소개수를입력합니다. 기본값은 **0** 입니다.
- 최대개수
 - 한문자의최대사용횟수: 한문자가암호에서발생할수있는최대횟수를입력합니다. 기본값은 **0** 입니다.
 - 연속영문자길이: 암호에서연속될수있는영문자의최대길이를입력합니다. 기본값은 **0** 입니다.
 - 연속숫자길이: 암호에서연속될수있는숫자의최대길이를입력합니다. 기본값은 **0** 입니다.
- 암호보안
 - 다음의비활성시간 (분) 이후장치잠금: 목록에서장치가잠기지않고비활성상태를유지할수있는기간 (초) 을클릭합니다. 기본값은 없음입니다.
 - 암호만료 (일)(1-730): 암호가만료되기전까지남은일수를입력합니다. 유효한값은 1 부터 730 까지입니다. 기본값은 **0** 이며, 암호가만료되지않는다는의미입니다.

- 이전암호저장 (**0-50**): 저장할이전암호수를입력합니다. 사용자는이목록에있는암호를사용할수없습니다. 유효한 값은 0 부터 50 까지입니다. 기본값은 0 이며, 사용자가암호를재사용할수있다는의미입니다.
- 지정한로그온시도실패횟수를초과하면장치가잠깁니다: 목록에서사용자가로그온에실패할수있는횟수를클릭합니다. 이횟수를넘으면장치가잠깁니다. 기본값은 정의되지않음입니다.
- 지정한로그온시도실패횟수를초과하면장치가초기화됩니다: 목록에서사용자가로그온에실패할수있는횟수를클릭합니다. 이횟수를넘으면장치에서 KNOX 컨테이너 (KNOX 데이터포함) 가초기화됩니다. 초기화가실행된후사용자가 KNOX 컨테이너를다시초기화해야합니다. 기본값은 정의되지않음입니다.

Android Enterprise 설정

The screenshot displays the 'Passcode Policy' configuration interface. On the left, a sidebar lists various policy categories, with 'Android Enterprise' selected under the 'Platforms' section. The main content area is titled 'Passcode Policy' and includes a descriptive paragraph. Below this, several settings are visible: 'Device passcode required' is turned ON; 'Passcode requirements for device passcode' includes a 'Minimum length' of 6 and 'Required characters' set to 'Numbers only'; 'Allow users to make password visible (Knox 3.0+)' is OFF; 'Biometric recognition' is OFF; 'Forbidden Strings (Knox 3.0+)' has an 'Add' button; 'Advanced rules' is OFF; 'Passcode security for device passcode' includes 'Wipe the device after (failed sign-on attempts)' set to 'Not defined' and 'Lock device after (minutes of inactivity) (0-' set to 'None'. At the bottom right, there are 'Back' and 'Next >' buttons.

Android Enterprise 장치의경우장치의암호또는 Android Enterprise 작업프로필의보안철크린지를요구하거나둘다를요구할수있습니다.

Android 8.0 이상및 Samsung Knox 3.0 이상을실행하는장치경우 **Android Enterprise** 페이지에서 Samsung Knox 에대한설정을구성합니다. 이전버전의 Android 또는 Samsung Knox 를실행하는장치경우 **Samsung Knox** 페이지를사용합니다.

참고:

Samsung Knox 3.0 을실행하는장치를작업프로필장치로등록한경우 Knox 3.0 이상에대한장치암호설정은구성된경우라하더라도장치암호에적용되지않습니다.

- **장치암호필요:** 장치에암호가필요합니다. 이설정이 켜짐인경우 장치암호의암호요구사항및 장치암호의암호보안에서설정을구성합니다. 기본값은 꺼짐입니다.

- 장치암호의암호요구사항:
 - 최소길이: 최소암호길이를지정합니다. 기본값은 6 입니다.
 - 사용자에게암호표시허용: 올바른 Knox 라이선스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한 설정입니다. 완전히관리되는장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다. 사용자가암호를표시할수있습니다. 기본값은 꺼짐입니다.
 - 생체인식: 생체인식을사용하도록설정합니다. 이설정이 켜짐인경우 필수문자필드가숨겨집니다. 기본값은 꺼짐입니다.
 - 필수문자: 암호에필요한문자의유형을지정합니다. 목록에서 제한없음, 숫자와문자모두, 숫자만또는 문자만을선택합니다. 제한없음은 Android 7.0 을실행하는장치에만사용합니다. Android 7.1 이상은 제한없음설정을따르지 않습니다. 기본값은 숫자와문자모두입니다.
 - 금지된문자열: 올바른 Knox 라이선스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전히관리되는장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다. 사용자가암호로사용할수없는문자열을지정합니다. 금지된문자열을만들어사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등과같이쉽게추측할수있는안전하지않은문자열을사용하지못하게합니다. 거부할각문자열에대해 추가를클릭하고사용금지하려는문자열을입력한다음 저장을클릭하여문자열을추가하거나 취소를클릭하여 문자열추가를취소합니다.
 - 고급규칙: 암호에서발생할수있는문자유형에대해고급규칙을적용합니다. 이설정이 켜짐인경우 최소개수및 최대개수에서설정을구성합니다. Android 5.0 이전의 Android 장치에서는이설정을사용할수없습니다. 기본값은 꺼짐입니다.
 - 최소개수:
 - * 기호: 기호의최소수를지정합니다. 기본값은 0 입니다.
 - * 문자: 문자의최소수를지정합니다. 기본값은 0 입니다.
 - * 소문자: 소문자의최소수를지정합니다. 기본값은 0 입니다.
 - * 대문자: 대문자의최소수를지정합니다. 기본값은 0 입니다.
 - * 숫자또는기호: 숫자또는기호의최소수를지정합니다. 기본값은 0 입니다.
 - * 숫자: 숫자의최소수를지정합니다. 기본값은 0 입니다.
 - * 변경된문자: 올바른 Knox 라이선스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전히관리되는장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다. 사용자가이전암호에서변경해야하는문자수를지정합니다. 기본값은 0 입니다.
 - 최대개수: 올바른 Knox 라이선스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전히관리되는장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다.
 - * 한문자의최대사용횟수: 한문자가암호에서발생할수있는최대횟수를지정합니다. 기본값은 0 이며최대제한이없음을의미합니다.
 - * 연속영문자길이: 암호에서연속될수있는영문자의최대길이를지정합니다. 기본값은 0 이며최대제한이없음을의미합니다.
 - * 연속숫자길이: 암호에서연속될수있는숫자의최대길이를지정합니다. 기본값은 0 이며최대제한이없음을의미합니다.
- 장치암호의암호보안:
 - 다음로그온시도실패후장치초기화: 사용자가로그인에실패할수있는횟수를지정합니다. 이횟수를넘으면장치가전체

초기화됩니다. 기본값은 정의되지않음입니다.

- 다음의비활성시간 (분) 이후장치잠금 (0-999): 장치가잠기지않고비활성상태를유지할수있는기간 (분) 을지정합니다. 기본값은 없음입니다.
- 암호만료 (일)(1-730): 암호가만료되기전까지남은일수를지정합니다. 유효한값은 1 부터 730 까지입니다. 기본값은 0 이며, 암호가만료되지않는다는의미입니다.
- 이전암호저장 (0-50): 저장할이전암호수를지정합니다. 사용자는이목록에있는암호를사용할수없습니다. 유효한값은 0 부터 50 까지입니다. 기본값은 0 이며, 사용자가암호를재사용할수있다는의미입니다.
- 다음로그온시도실패후장치잠금올바른 Knox 라이선스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전히관리되는장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다. 사용자가로그온에실패할수있는횟수를지정합니다. 그후장치가잠깁니다. 기본값은 정의되지않음입니다.
- 작업프로필보안챌린지: 사용자가 Android Enterprise 작업프로필에서실행되는앱에액세스할때보안챌린지를완료하도록합니다. Android 7.0 이상을실행하는장치를위한설정입니다. 이설정이 켜짐인경우 작업프로필보안과제에대한암호요구사항및 작업프로필보안과제에대한암호보안에서설정을구성합니다. 기본값은 꺼짐입니다.
- 작업프로필보안과제에대한암호요구사항:
 - 최소길이: 최소암호길이를지정합니다. 기본값은 6 입니다.
 - 사용자에게암호표시허용: 올바른 Knox 라이선스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다. 사용자가암호를표시할수있습니다. 기본값은 꺼짐입니다.
 - 생체인식: 생체인식을사용하도록설정합니다. 이설정이 켜짐인경우 필수문자필드가숨겨집니다. 기본값은 꺼짐입니다.
 - 필수문자: 암호에필요한문자의유형을지정합니다. 목록에서 제한없음, 숫자와문자모두, 숫자만또는 문자만을선택합니다. 제한없음은 Android 7.0 을실행하는장치에만사용합니다. Android 7.1 이상은 제한없음설정을따르지않습니다. 기본값은 숫자와문자모두입니다.
 - 금지된문자열: 올바른 Knox 라이선스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다. 사용자가암호로사용할수없는문자열을지정합니다. 금지된문자열을만들어사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등과같이쉽게추측할수있는안전하지않은문자열을사용하지못하게합니다. 거부할각문자열에대해 추가를클릭하고사용금지하려는문자열을입력한다음 저장을클릭하여문자열을추가하거나 취소를클릭하여문자열추가를취소합니다.
 - 고급규칙: 암호에서발생할수있는문자유형에대해고급규칙을적용합니다. 이설정이 켜짐인경우 최소개수및 최대개수에서설정을구성합니다. Android 5.0 이전의 Android 장치에서는이설정을사용할수없습니다. 기본값은 꺼짐입니다.
 - 최소개수:
 - * 기호: 기호의최소수를지정합니다. 기본값은 0 입니다.
 - * 문자: 문자의최소수를지정합니다. 기본값은 0 입니다.
 - * 소문자: 소문자의최소수를지정합니다. 기본값은 0 입니다.
 - * 대문자: 대문자의최소수를지정합니다. 기본값은 0 입니다.
 - * 숫자또는기호: 숫자또는기호의최소수를지정합니다. 기본값은 0 입니다.
 - * 숫자: 숫자의최소수를지정합니다. 기본값은 0 입니다.
 - * 변경된문자: 올바른 Knox 라이선스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다. 사용자가이전암호에서변경해야하는문자수를지정합니다. 기본값은 0 입니다.

- 최대개수: 올바른 Knox 라이선스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다.
 - * 한문자의최대사용횟수: 한문자가암호에서발생할수있는최대횟수를지정합니다. 기본값은 0 이며최대제한이없음을의미합니다.
 - * 연속영문자길이: 암호에서연속될수있는영문자의최대길이를지정합니다. 기본값은 0 이며최대제한이없음을의미합니다.
 - * 연속숫자길이: 암호에서연속될수있는숫자의최대길이를지정합니다. 기본값은 0 이며최대제한이없음을의미합니다.
- 작업프로필보안과제에대한암호보안
 - 다음로그온시도실패후컨테이너초기화: 사용자가로그인에실패할수있는횟수를지정합니다. 이횟수를넘으면장치에서작업프로필및해당데이터가초기화됩니다. 사용자는초기화가발생한후작업프로필을다시초기화해야합니다. 기본값은 정의되지않음입니다.
 - 다음비활성시간 (분) 이후컨테이너잠금: 작업프로필이잠기지않고장치가비활성상태를유지할수있는기간 (분) 을지정합니다. 기본값은 없음입니다.
 - 암호만료 (일)(1-730): 암호가만료되기전까지남은일수를지정합니다. 유효한값은 1 부터 730 까지입니다. 기본값은 0 이며, 암호가만료되지않는다는의미입니다.
 - 이전암호저장 (0-50): 저장할이전암호수를지정합니다. 사용자는이목록에있는암호를사용할수없습니다. 유효한값은 0 부터 50 까지입니다. 기본값은 0 이며, 사용자가암호를재사용할수있다는의미입니다.
 - 다음로그온시도실패후컨테이너잠금올바른 Knox 라이선스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다. 사용자가로그온에실패할수있는횟수를지정합니다. 그후장치가잠깁니다. 기본값은 정의되지않음입니다.

Windows Phone 설정

The screenshot shows the 'Configure' page for XenMobile, specifically the 'Passcode Policy' configuration. The 'Passcode required' toggle is turned ON. Under 'Passcode requirements', 'Allow simple passcodes' is OFF, 'Minimum length' is 6, 'Characters required' is 'Letters only', and 'Minimum number of symbols' is 1. Under 'Passcode security', 'Lock device after (minutes of inactivity) (0-999)' is 0, 'Passcode expiration in 0-730 days *' is 0, 'Previous passwords saved (0-50)' is 0, and 'Maximum failed sign-on attempts before wipe (0-999) *' is 0. On the left, the 'Assignment' section shows 'Windows Phone' and 'Windows Desktop/Tablet' selected.

- 암호필요: Windows Phone 장치에대해암호를요구하지않으려면이옵션을선택합니다. 기본설정은 켜짐이며, 암호를

요구합니다. 이 설정을 사용하지 않으면 페이지가 축소되고 다음 옵션이 사라집니다.

- **단순 암호 허용:** 단순 암호를 허용할지 여부를 선택합니다. 단순 암호는 반복적이거나 순차적 문자 집합입니다. 기본값은 꺼짐입니다.
- **암호 요구 사항**
 - **최소 길이:** 목록에서 최소 암호 길이를 클릭합니다. 기본값은 **6**입니다.
 - **문자 필요:** 목록에서 숫자 또는 영숫자, 문자만 또는 숫자만을 클릭하여 암호가 구성되는 방식을 구성합니다. 기본값은 문자만입니다.
 - **최소 기호 개수:** 목록에서 암호에 포함되어야 하는 기호의 수를 클릭합니다. 기본값은 **1**입니다.
- **암호 보안**
 - **다음의 비활성 시간 (분) 이후 장치 잠금:** 장치가 잠기지 않고 비활성 상태를 유지할 수 있는 시간 (분) 을 입력합니다. 기본값은 **0**입니다.
 - **0-730 일 후 암호 만료:** 암호가 만료되기 전까지 남은 일수를 입력합니다. 유효한 값은 0 부터 730 까지입니다. 기본값은 **0**이며, 암호가 만료되지 않는다는 의미입니다.
 - **이전 암호 저장 (0-50):** 저장할 이전 암호 수를 입력합니다. 사용자는 이 목록에 있는 암호를 사용할 수 없습니다. 유효한 값은 0 부터 50 까지입니다. 기본값은 **0**이며, 사용자가 암호를 재 사용할 수 있다는 의미입니다.
 - **초기화하기 전까지의 최대 로그인 시도 실패 횟수 (0-999):** 사용자가 로그인에 실패할 수 있는 횟수를 입력합니다. 이 횟수를 넘으면 장치에서 데이터가 초기화됩니다. 기본값은 **0**입니다.

Windows 데스크톱/태블릿 설정

The screenshot shows the 'Configure' tab in the XenMobile console, specifically the 'Passcode Policy' configuration page for 'Windows Desktop/Tablet'. The 'Passcode required' toggle is turned ON. Under 'Passcode security', the 'Lock device after (minutes of inactivity) (0-999)' field is set to 0, 'Passcode expiration in 0-730 days' is set to 0, and 'Previous passwords saved (0-24)' is set to 0. Under 'Passcode requirements', the 'Minimum length' dropdown is set to 6. The 'Deployment Rules' section is expanded.

- **간편 로그인 허용 안 함:** 사용자가 사전 암호 또는 생체 인식 로그인을 사용하여 장치에 액세스할 수 있도록 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **최소 암호 길이:** 목록에서 최소 암호 길이를 클릭합니다. 기본값은 **6**입니다.
- **초기화하기 전까지의 최대 암호 시도 횟수:** 목록에서 사용자가 로그인에 실패할 수 있는 횟수를 클릭합니다. 이 횟수를 넘으면 장치

에서데이터가초기화됩니다. 기본값은 **4** 입니다.

- 암호만료 (**일**)(**0-730**): 암호가만료되기전까지남은일수를입력합니다. 유효한값은 0 부터 730 까지입니다. 기본값은 **0** 이며, 암호가만료되지않는다는의미입니다.
- 암호기록 (**1-24**): 저장할이전암호수를입력합니다. 사용자는이목록에있는암호를사용할수없습니다. 유효한값은 1 부터 24 까지입니다. 이필드에 1 에서 24 사이의숫자를입력해야합니다. 기본값은 **0** 입니다.
- 장치를잠그기전까지의최대비활성시간 (**분**)(**1-999**): 장치가잠기지않고비활성상태를유지할수있는기간 (분) 을입력합니다. 유효한값은 1 부터 999 까지입니다. 이필드에 1 에서 999 사이의숫자를입력해야합니다. 기본값은 **0** 입니다.

개인핫스팟장치정책

January 6, 2020

사용자가 WiFi 네트워크범위외부에있을때 iOS 장치의개인핫스팟기능을통해셀룰러데이터연결을사용하여인터넷에연결하도록 허용할수있습니다. iOS 7.0 이상에서사용가능합니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

- 개인핫스팟사용안함: 사용자의장치에서개인핫스팟기능을사용하지않도록설정할지여부를선택합니다. 기본값은사용자의 장치에서개인핫스팟을끄는 꺼짐입니다. 이정책은기능을사용하지않도록설정하지않습니다. 사용자는여전히자신의장치에서개인핫스팟을사용할수있지만정책이배포될때개인핫스팟이해제되어기본적으로켜져있지않습니다.

프로필제거장치정책

January 6, 2020

XenMobile 에서앱프로필제거장치정책을만들수있습니다. 정책을배포하면사용자의 iOS 또는 macOS 장치에서앱프로필이 제거됩니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

The screenshot shows the 'Configure' page for a 'Profile Removal Policy' in XenMobile. The left sidebar has a navigation menu with 'Profile Removal Policy' selected. The main content area shows the policy configuration for iOS. The 'Profile ID' field is a dropdown menu with the text 'This field is mandatory.' The 'Comment' field is a text input box. Below the configuration fields is a section for 'Deployment Rules'.

- **프로필 ID:** 목록에서 앱프로필 ID 를 클릭합니다. 이것은 필수필드입니다.
- **설명:** 선택적 설명을 입력합니다.

macOS 설정

The screenshot shows the 'Configure' page for a 'Profile Removal Policy' in XenMobile. The left sidebar has a navigation menu with 'Profile Removal Policy' selected. The main content area shows the policy configuration for macOS. The 'Profile ID' field is a dropdown menu with the text 'This field is mandatory.' The 'Deployment scope' field is a dropdown menu with 'User' selected and 'macOS 10.7+' next to it. The 'Comment' field is a text input box. Below the configuration fields is a section for 'Deployment Rules'.

- **프로필 ID:** 목록에서 앱프로필 ID 를 클릭합니다. 이것은 필수필드입니다.
- **배포범위:** 목록에서 사용자 또는 시스템을 클릭합니다. 기본값은 사용자입니다. 이 옵션은 macOS 10.7 이상에서만 사용할 수 있습니다.
- **설명:** 선택적 설명을 입력합니다.

프로비전프로필장치정책

August 23, 2019

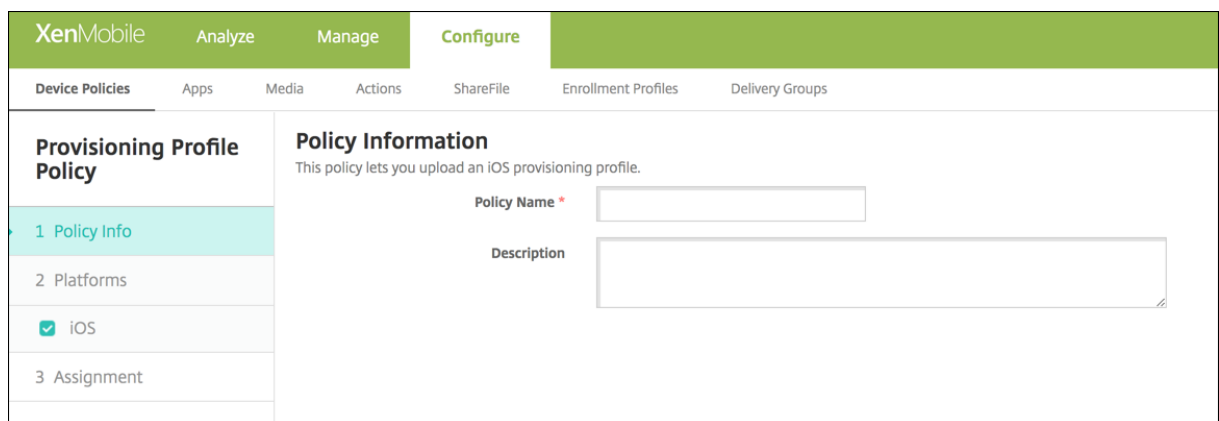
iOS 엔터프라이즈 앱을 개발하고 코드 서명하는 경우 일반적으로 엔터프라이즈 배포 프로비전 프로필을 포함합니다. Apple iOS 장치에서 앱을 실행하려면 이 프로필이 필요합니다. 프로비전 프로필이 누락되었거나 만료된 경우 사용자가 앱을 눌러서 열 때 앱의 작동이 중단됩니다.

프로비전 프로필의 주요 문제는 Apple Developer Portal에서 생성된 후 1년 지나면 만료된다는 것입니다. 따라서 사용자의 해당 등록된 모든 iOS 장치에서 모든 프로비전 프로필의 만료 날짜를 추적해야 합니다. 만료 날짜를 추적하는 작업에는 실제 만료 날짜뿐 아니라 어떤 사용자가 어떤 앱 버전을 사용하는지를 지속적으로 파악하는 것도 포함됩니다. 두 가지 해결 방법은 프로비전 프로필을 사용자에게 전자 메일로 보내거나 웹 포털에 게시해 다운로드하여 설치하도록 하는 것입니다. 이러한 해결 방법은 효과가 있지만 오류가 발생하기 쉽습니다. 사용자가 전자 메일의 지침에 대응하거나 웹 포털에서 올바른 프로필을 다운로드하여 설치해야 하기 때문입니다.

이 프로세스를 사용자에게 투명하게 진행하려면 XenMobile에서 장치 정책을 사용하여 프로비전 프로필을 설치하거나 제거할 수 있습니다. 누락되었거나 만료된 프로필은 필요에 따라 제거되고 최신 프로필이 사용자의 장치에 설치되므로 앱을 누르기만 하면 열어서 사용할 수 있습니다.

프로비전 프로필 정책을 만들려면 먼저 프로비전 프로필 파일을 만들어야 합니다. 자세한 내용은 Apple Developer 사이트의 [개발 프로비전 프로필 만들기](#)를 참조하십시오.

iOS 설정



- **iOS** 프로비전 프로필: 찾아보기를 클릭하고 파일 위치로 이동하여 가져올 프로비전 프로필 파일을 선택합니다.

프로비전 프로필 제거 장치 정책

January 6, 2020

장치 정책을 사용하여 iOS 프로비전 프로필을 제거할 수 있습니다. 프로비전 프로필에 대한 자세한 내용은 [프로비전 프로필 장치 정책](#)을 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

- **iOS** 프로비전프로필: 목록에서 제거할 프로비전프로필을 클릭합니다.
- 설명: 필요한 경우 설명을 추가합니다.

프록시장치정책

January 6, 2020

XenMobile 에서장치정책을 추가하여 Windows Mobile/CE 및 iOS 6.0 이상을 실행하는 장치에 대한 글로벌 HTTP 프록시 설정을 지정할 수 있습니다. 장치당 하나의 글로벌 HTTP 프록시 정책만 배포할 수 있습니다.

참고:

이 정책을 배포하기 전에 글로벌 HTTP 프록시를 설정할 모든 iOS 장치를 감독 모드로 설정해야 합니다. 자세한 내용은 [Apple Configurator](#) 를 사용하여 [iOS 장치를 감독 모드로 전환](#) 에서 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#) 에서 참조하십시오.

iOS 설정

- **프록시 구성:** 사용자의 장치에서 프록시를 구성하는 방법에 대해 수동 또는 자동으로 클릭합니다.
 - 수동으로 클릭하는 경우 다음 설정을 구성합니다.
 - * **프록시 서버의 호스트 이름 또는 IP 주소:** 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - * **프록시 서버 포트:** 프록시 서버 포트 번호를 입력합니다. 이것은 필수 필드입니다.
 - * **사용자 이름:** 프록시 서버 인증에 사용할 선택적 사용자 이름을 입력합니다.
 - * **암호:** 프록시 서버 인증에 사용할 선택적 암호를 입력합니다.
 - 자동으로 클릭하는 경우 다음 설정을 구성합니다.
 - * **프록시 PAC URL:** 프록시 구성을 정의하는 PAC 파일의 URL 을 입력합니다.
 - * **PAC** 에 연결할 수 없는 경우 직접 연결 허용: PAC 파일에 연결할 수 없는 경우 대상에 직접 연결할 수 있도록 할지 여부를 선택합니다. 기본값은 켜짐입니다. 이 옵션은 iOS 7.0 이상에서만 사용할 수 있습니다.
- **중속 네트워크에 액세스하기 위한 프록시 바이패스 허용:** 중속 네트워크에 액세스하기 위한 프록시 바이패스를 허용할 것인지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **정책 설정**
 - 정책 제거 옆에서 날짜 선택 또는 제거할 때까지의 기간 (시간) 을 클릭합니다.
 - 날짜 선택을 클릭하는 경우 달력을 클릭하여 제거할 날짜를 선택합니다.
 - 사용자가 정책을 제거하도록 허용 목록에서 항상, 암호 필요 또는 안함을 클릭합니다.
 - 암호 필요를 클릭하는 경우 제거 암호 옆에 필요한 암호를 입력합니다.

Windows Mobile/CE 설정

- 네트워크: 목록에서 사용할 네트워크 유형을 클릭합니다. 기본값은 기본제공사무실입니다. 사용가능한 옵션은 다음과 같습니다.
 - 사용자정의사무실
 - 사용자정의인터넷
 - 기본제공사무실
 - 기본제공인터넷
- 네트워크: 목록에서 사용할 네트워크 연결 프로토콜을 클릭합니다. 기본값은 **HTTP** 입니다. 사용가능한 옵션은 다음과 같습니다.
 - HTTP
 - WAP
 - Socks 4
 - Socks 5
- 프록시 서버의 호스트 이름 또는 **IP** 주소: 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
- 프록시 서버용 포트: 프록시 서버 포트 번호를 입력합니다. 이것은 필수 필드입니다. 기본값은 **80** 입니다.
- 사용자 이름: 프록시 서버 인증에 사용할 선택적 사용자 이름을 입력합니다.
- 암호: 프록시 서버 인증에 사용할 선택적 암호를 입력합니다.
- 도메인 이름: 선택적 도메인 이름을 입력합니다.
- 사용: 프록시 사용 여부를 선택합니다. 기본값은 켜짐입니다.

레지스트리 장치 정책

January 6, 2020

Windows Mobile/CE 레지스트리에는 앱, 드라이버, 사용자 기본 설정 및 구성 설정에 대한 데이터가 저장됩니다. XenMobile 에서 Windows Mobile/CE 장치를 관리할 수 있는 레지스트리 키 및 값을 정의할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

Windows Mobile/CE 설정

추가할 각 레지스트리 키 또는 레지스트리 키/값 쌍에 대해 추가를 클릭하고 다음을 수행합니다.

- 레지스트리 키 경로: 레지스트리 키의 전체 경로를 입력합니다. 예를 들어 **HKEY_LOCAL_MACHINE** 루트 키에서 **Windows** 키에 대한 경로를 지정하려면 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows 를 입력합니다.
- 레지스트리 값 이름: 레지스트리 값의 이름을 입력합니다. 예를 들어 **ProgramFilesDir** 을 입력하여 해당 값 이름을 레지스트리 키 경로 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion 에 추가합니다. 이 필드를 비워 두면 레지스트리 키/값 쌍이 아닌 레지스트리 키를 추가한다는 의미입니다.

- 유형: 목록에서값의데이터유형을클릭합니다. 기본값은 **DWORD** 입니다. 사용가능한옵션은다음과같습니다.
 - **DWORD**: 32 비트부호없는정수
 - 문자열: 모든문자열
 - 확장문자열: %TEMP% 또는%USERPROFILE% 같은환경변수를포함할수있는문자열값
 - 이진: 임의의이진데이터
- 값: 레지스트리값이름과연결된값을입력합니다. 예를들어 ProgramFilesDir 의값을지정하려면 **C:\Program Files** 를입력합니다.
- 저장을클릭하여레지스트리키정보를저장하거나 취소를클릭하여레지스트리키정보를저장하지않습니다.

원격지원장치정책

January 6, 2020

참고:

온-프레미스 XenMobile Server 배포의 경우: 원격지원을 사용하면 지원센터 담당자가 관리되는 Windows CE 및 Android 모바일 장치를 원격으로 제어할 수 있습니다. 스크린캐스트는 Samsung KNOX 장치에서만 지원됩니다.

원격지원은 클러스터링된 온-프레미스 XenMobile Server 배포에서 지원되지 않습니다.

자세한 내용은 [지원 옵션 및 원격 지원](#)에서 참조하십시오.

XenMobile 에서 지원되는 Windows 및 Android 장치에 대한 원격 액세스를 제공하는 원격 지원 정책을 만듭니다. 두 가지 유형의 지원을 구성할 수 있습니다.

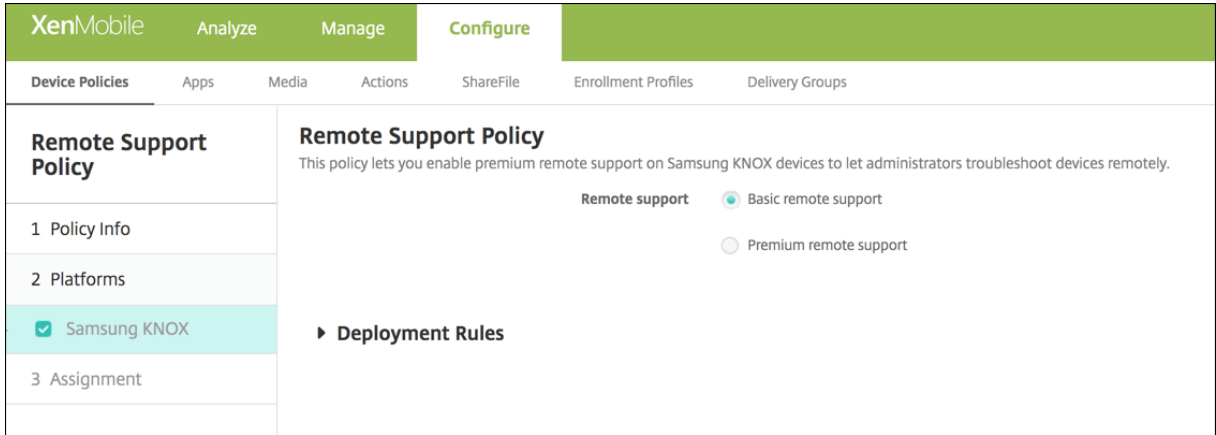
- 기본 - 시스템 정보, 실행 중인 프로세스, 작업 관리자 (메모리 및 CPU 사용량), 설치된 소프트웨어 폴더 내용 등과 같은 장치에 대한 진단 정보를 볼 수 있습니다.
- 프리미엄 - 원격으로 장치 화면을 제어할 수 있습니다.
 - 색상 제어 (주창 또는 개별적인 부동창에서)
 - 지원센터와 사용자 간의 VoIP (Voice-over-IP) 세션 설정
 - 설정 구성
 - 지원센터와 사용자 간의 채팅 세션 설정

이 정책을 구현하려면 다음을 수행해야 합니다.

- 사용자 환경에서 XenMobile Remote Support 앱을 설치합니다.
- Remote Support 앱 터널을 구성합니다. 자세한 내용은 [애플리케이션 장치 정책](#)에서 참조하십시오.
- 이 항목에 설명된 대로 Samsung KNOX 원격 지원 장치 정책을 구성합니다.
- 애플리케이션 장치 정책과 Samsung KNOX 원격 지원 정책을 모두 사용자 장치에 배포합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

Android 및 Windows CE 설정



- 원격지원: 기본원격지원또는 프리미엄원격지원을선택합니다. 기본값은 기본원격지원입니다.

제한장치정책

January 6, 2020

제한장치정책은사용자장치에서카메라와같은특정기능을허용하거나제한합니다. 또한보안제한을설정하고미디어콘텐츠에대한제한과사용자가설치할수있는앱유형및설치할수없는앱유형에대한제한을설정할수있습니다. 대부분의제한설정은기본적으로 꺼짐또는 허용입니다. 주요예외사항은 iOS 보안 - 시행기능및모든 Windows 태블릿기능입니다. 이러한기능은기본적으로 꺼짐또는 제한으로설정됩니다.

Windows 10 RS2 휴대폰: Internet Explorer 를사용하지않는사용자지정 XML 정책또는제한정책을휴대폰에배포한후브라우저가사용되는상태로유지됩니다. 이문제를해결하려면휴대폰을다시시작하십시오. 이것은타사문제입니다.

팁:

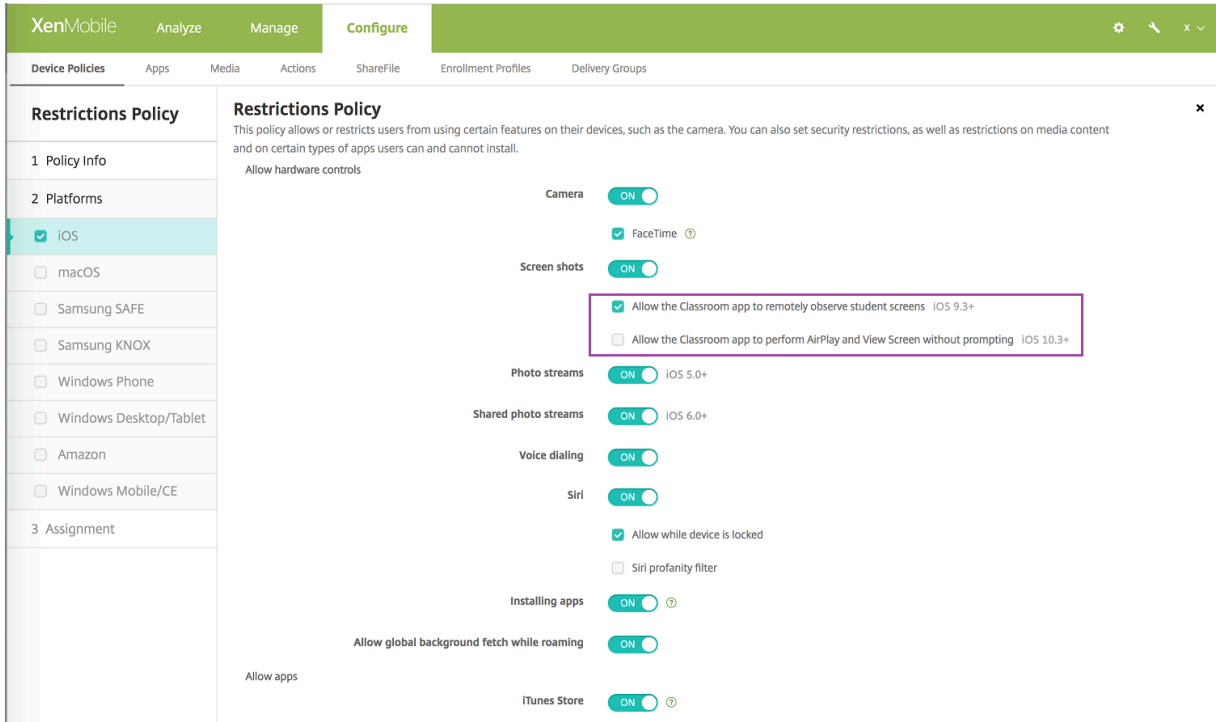
꺼짐을선택한모든옵션은사용자가해당작업을수행하거나기능을사용할수있다는의미입니다. 예를들면다음과같습니다.

카메라. 꺼짐이면사용자가장치에서카메라를사용할수있습니다. 꺼짐이면사용자가장치에서카메라를사용할수없습니다.

스크린샷. 꺼짐이면사용자가장치에서스크린샷을만들수있습니다. 꺼짐이면사용자가장치에서스크린샷을만들수없습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정



일부 iOS 제한정책설정은여기와 XenMobile Server 콘솔제한정책페이지에설명된대로특정버전의 iOS 에만적용됩니다.

모든 iOS 제한정책설정은장치가감독모드에서등록된경우적용됩니다. iOS 장치를감독모드로설정하는방법에대한자세한내용은 [Apple Configurator](#) 를사용하여 iOS 장치를감독모드로전환을참조하십시오.

일부 iOS 제한정책설정은장치가사용자등록모드또는감독되지않는모드 (전체 MDM) 에서등록된경우에도적용됩니다. 다음표에는 iOS 13 이상을실행하는장치의사용자등록모드또는감독되지않는모드에서설정을사용할수있는지여부나와있습니다.

설정	사용자등록	감독되지않음	감독됨
하드웨어제어허용			
카메라	아니요	예	예
FaceTime	아니요	아니요 (iOS 13 의새로운기능)	예
스크린샷	예	아니요	예
교실앱이학생화면을원격으로관찰할수있도록허용	아니요	아니요	예
메시지를표시하지않고교실 앱이 AirPlay 및화면보기를수행할수있도록허용	아니요	아니요	예
사진스트림	아니요	예	예

설정	사용자등록	감독되지않음	감독됨
공유사진스트림	아니요	예	예
음성전화걸기	아니요	예	예
Siri	예	예	예
장치가잠겨있는동안허용	예	예	예
Siri 비속어필터	아니요	아니요	예
앱설치	아니요	아니요 (iOS 13 의새로운기능)	예
로밍중에글로벌배경가져오기허용	아니요	예	예
앱허용			
iTunes 스토어	아니요	아니요 (iOS 13 의새로운기능)	예
앱에서바로구매	아니요	예	예
구매시 iTunes 암호필요	아니요	예	예
Safari	아니요	아니요 (iOS 13 의새로운기능)	예
자동채우기	아니요	아니요 (iOS 13 의새로운기능)	예
부정행위경고시행	예	예	예
JavaScript 사용	아니요	예	예
팝업차단	아니요	예	예
쿠키적용	아니요	예	예
네트워크 - iCloud 동작허용			
iCloud 문서및데이터	아니요	아니요 (iOS 13 의새로운기능)	예
iCloud 백업	아니요	예	예
iCloud 사진키집합	아니요	예	예
iCloud 사진라이브러리	아니요	예	예
보안 - 시행			
암호화된백업	예	예	예

설정	사용자등록	감독되지않음	감독됨
제한된 AD 추적	아니요	예	예
첫번째 AirPlay 페어링의 암호	예	예	예
Wrist Detect 를사용하기 위해페어링된 Apple Watch	예	예	예
AirDrop 을사용하여관리 되는문서공유	예	예	예
보안 - 허용			
신뢰할수없는 SSL 인증서 수락	아니요	예	예
인증서신뢰설정에대한자동 업데이트	아니요	예	예
관리되지않는앱에있는관리 되는앱의문서	예	예	예
관리되지않는앱이관리되는 연락처읽기	아니요	아니요	예
관리되는앱이관리되지않는 연락처쓰기	아니요	아니요	예
관리되는앱에있는관리되지 않는앱의문서	예	예	예
Apple 에진단제출	예	예	예
장치의잠금을해제하기위한 Touch ID	아니요	예	예
잠겨있을경우 Passbook 알림	아니요	예	예
핸드오프	아니요	예	예
관리되는앱에대한 iCloud 동기화	예	예	예
엔터프라이즈북에대한백업	예	예	예
엔터프라이즈북동기화에대한메모및하이라이트	예	예	예

설정	사용자등록	감독되지않음	감독됨
Spotlight 에대한인터넷결 과	아니요	예	예
엔터프라이즈앱신뢰	아니요	예	예
감독되는경우에만해당되는 설정 - 허용			
모든내용및설정지우기	아니요	아니요	예
제한구성	아니요	아니요	예
팟캐스트	아니요	아니요	예
구성프로필설치	아니요	아니요	예
지문수정	아니요	아니요	예
장치에서앱설치	아니요	아니요	예
바로가기키	아니요	아니요	예
페어링된 Apple Watch	아니요	아니요	예
암호수정	아니요	아니요	예
장치이름수정	아니요	아니요	예
배경화면수정	아니요	아니요	예
자동으로앱다운로드	아니요	아니요	예
AirDrop	아니요	아니요	예
iMessage	아니요	아니요	예
Siri 사용자생성콘텐츠	아니요	아니요	예
iBooks	아니요	아니요	예
앱제거	아니요	예	예
게임센터	아니요	아니요 (iOS 13 의새로운기 능)	예
친구추가	아니요	아니요	예
멀티플레이게임	아니요	아니요 (iOS 13 의새로운기 능)	예
계정설정수정	아니요	아니요	예
앱셀룰러데이터설정수정	아니요	아니요	예
앱셀룰러데이터설정수정	아니요	아니요	예

설정	사용자등록	감독되지않음	감독됨
내친구찾기설정수정	아니요	아니요	예
비 Configurator 호스트 와페어링	아니요	아니요	예
키보드자동완성	아니요	아니요	예
키보드자동수정	아니요	아니요	예
키보드맞춤법검사	아니요	아니요	예
정의조회	아니요	아니요	예
단일앱번들 ID			
뉴스	아니요	아니요	예
Apple Music 서비스	아니요	아니요	예
iTunes Radio	아니요	아니요	예
알림수정	아니요	아니요	예
제한된앱사용	아니요	아니요	예
진단체출수정	아니요	아니요	예
Bluetooth 수정	아니요	아니요	예
받아쓰기허용	아니요	아니요	예
WiFi 정책에따라설치된 WiFi 네트워크에만참가	아니요	아니요	예
메시지를표시하지않고교실 앱이 AirPlay 및화면보기 를수행할수있도록허용	아니요	아니요	예
메시지를표시하지않고교실 앱이앱및장치를잠글수있도 록허용	아니요	아니요	예
메시지를표시하지않고교실 애플클래스에자동참가	아니요	아니요	예
AirPrint 허용	아니요	아니요	예
키집합에 AirPrint 자격증 명저장허용	아니요	아니요	예
iBeacon 을사용하여 AirPrint 프린터검색허용	아니요	아니요	예

설정	사용자등록	감독되지않음	감독됨
신뢰할수있는인증서가있는 대상에만 AirPrint 허용	아니요	아니요	예
VPN 구성추가	아니요	아니요	예
셀룰러요금제설정수정	아니요	아니요	예
시스템앱제거	아니요	아니요	예
새로운주변장치설정	아니요	아니요	예
USB 제한모드허용	아니요	아니요	예
소프트웨어업데이트강제지 연	아니요	아니요	예
소프트웨어업데이트시행지 연	아니요	아니요	예
교실에서클래스를나갈때허 가요청시행	아니요	아니요	예
자동날짜맞시간적용	아니요	아니요	예
암호자동채우기	아니요	아니요	예
암호근접요청	아니요	아니요	예
암호공유	아니요	아니요	예
보안 - 잠금화면에표시			
제어센터	예	예	예
알림	예	예	예
오늘의보기	예	예	예
미디어콘텐츠 - 허용			
음악, 팟캐스트및 iTunes U 의성인등급자료	아니요	아니요 (iOS 13 의새로운기 능)	예
iBooks 의성관련성인등급 콘텐츠	아니요	예	예
평가지역	아니요	예	예
영화	아니요	예	예
TV 쇼	아니요	예	예
앱	아니요	예	예

- 하드웨어제어허용
 - 카메라: 사용자가장치에서카메라를사용할수있도록허용합니다.
 - * **FaceTime**: 사용자가장치에서 FaceTime 을사용할수있도록허용합니다. 감독되는 iOS 장치를위한설정입니다.
 - 스크린샷: 사용자가장치에서스크린샷을찍을수있도록허용합니다.
 - * 교실앱이학생화면을원격으로관찰할수있도록허용: 이제한을선택취소하면강사가교실앱을사용하여학생화면을원격으로관찰할수없습니다. 기본설정은선택되어있으며강사는교실앱을사용하여학생화면을관찰할수있습니다. 메시지를표시하지않고교실앱이 **AirPlay** 및화면보기를수행할수있도록허용설정예따라강사에게권한을제공할지여부를묻는메시지가학생에게표시됩니다. 감독되는 iOS 장치를위한설정입니다.
 - * 메시지를표시하지않고교실앱이 **AirPlay** 및화면보기를수행할수있도록허용: 이제한을선택하면권한에대한메시지표시없이강사가학생장치에서 AirPlay 및화면보기를수행할수있습니다. 기본설정은선택취소되어있습니다. 감독되는 iOS 장치를위한설정입니다.
 - 사진스트림: 사용자가 MyPhotoStream 을사용하여 iCloud 를통해사진을모든 iOS 장치에공유할수있도록허용합니다.
 - 공유사진스트림: 사용자가 iCloud 사진공유를사용하여동료, 친구및가족과사진을공유할수있도록허용합니다.
 - 음성전화걸기: 사용자의장치에서전화걸기를사용하도록설정합니다.
 - **Siri**: 사용자가 Siri 를사용할수있도록허용합니다.
 - * 장치가잠겨있는동안허용: 사용자가장치가잠겨있는동안 Siri 를사용할수있도록허용합니다.
 - * **Siri** 비속어필터: Siri 비속어필터를사용하도록설정합니다. 기본값은이기능을제한하는것이며, 비속어를필터링하지않습니다.
Siri 및보안에대한자세한내용은 [Siri 및받아쓰기정책](#)을참조하십시오.
 - 앱설치: 사용자가앱을설치하도록허용합니다. 감독되는 iOS 장치를위한설정입니다.
 - 로밍중에글로벌배경가져오기허용: 장치가로밍중인동안장치가 iCloud 에메일계정을자동으로동기화하도록허용합니다. 꺼짐으로설정하면 iOS 휴대폰이로밍중일때배경가져오기활동이비활성화됩니다. 기본값은 켜짐입니다.
- 앱허용
 - **iTunes** 스토어: 사용자가 iTunes 스토어에액세스할수있도록허용합니다. 감독되는 iOS 장치를위한설정입니다.
 - 앱에서바로구매: 사용자가앱내에서구입할수있도록허용합니다.
 - * 구매시 **iTunes** 암호필요: 앱에서바로구매시암호를묻습니다. 기본값은이기능을제한하는것이며, 앱에서바로구매시암호가필요하지않습니다.
 - **Safari**: 사용자가 Safari 에액세스할수있도록허용합니다. 감독되는 iOS 장치를위한설정입니다.
 - * 자동채우기: 사용자가 Safari 에서사용자이름및암호에대한자동채우기를설정할수있도록허용합니다.
 - * 부정행위경고시행: 이설정을사용하는경우사용자의심스러운피싱웹사이트를방문하면 Safari 경고가나타납니다. 기본값은이기능을제한하는것이며, 경고가실행되지않습니다.
 - * **JavaScript** 사용: Safari 에서 JavaScript 를실행하도록허용합니다.
 - * 팝업차단: 웹사이트를보는동안팝업을차단합니다. 기본값은이기능을제한하는것이며, 팝업을차단하지않습니다.
 - 쿠키적용: 쿠키가허용되는범위를설정합니다. 목록에서쿠키를허용하거나제한하는옵션을선택합니다. 기본옵션은 항상이며, Safari 에서모든웹사이트가쿠키를저장하도록허용합니다. 다른옵션은 현재웹사이트만, 안함및 방문한

웹사이트에서만입니다.

• 네트워크 - **iCloud** 동작허용

- **iCloud** 문서및데이터: 사용자가문서및데이터를 iCloud 에동기화하도록허용합니다. 감독되는 iOS 장치를위한 설정입니다.
- **iCloud** 백업: 사용자가장치를 iCloud 에백업하도록허용합니다.
- **iCloud** 키집합: 사용자가입호, WiFi 네트워크, 신용카드및기타정보를 iCloud 키집합에서저장하도록허용합니다.
- **iCloud** 사진라이브러리: 사용자가 iCloud 사진라이브러리에액세스할수있도록허용합니다.

• 보안 - 시행

기본값은다음과같은기능을제한하는것이며, 보안기능이사용되지않습니다.

- 암호화된백업: iCloud 에대한백업을암호화합니다.
- 제한된 **AD** 추적: 표적광고추적을차단합니다.
- 첫번째 **AirPlay** 페어링의암호: AirPlay 지원장치는 AirPlay 를사용하기전에화면상의일회용코드로확인받아야합니다.
- **Wrist Detect** 를사용하기위해페어링된 **Apple Watch**: 손목인식을사용하려면페어링된 Apple Watch 가 있어야합니다.
- **AirDrop** 을사용하여관리되는문서공유: AirDrop 액세스는감독되는옵션입니다. 이옵션을 켜짐으로설정하면감독되는장치가 AirDrop 을사용하여인접한 iOS 장치와데이터및미디어를공유하도록허용됩니다.

• 보안 - 허용

- 신뢰할수없는 **SSL** 인증서수락: 사용자가웹사이트의신뢰할수없는 SSL 인증서를수락하도록허용합니다.
- 인증서신뢰설정에대한자동업데이트: 신뢰할수있는인증서가자동으로업데이트되도록허용합니다.
- 관리되지않는앱에있는관리되는앱의문서: 사용자가관리되는 (기업) 앱에서관리되지않는 (개인) 앱으로데이터를이동할수있도록허용합니다.
- 관리되는앱에있는관리되지않는앱의문서: 사용자가관리되지않는 (개인) 앱에서관리되는 (회사) 앱으로데이터를이동할수있도록허용합니다.
- **Apple** 에진단제출: 사용자의장치에대한익명의진단데이터를 Apple 에보내도록허용합니다.
- 장치의잠금을해제하기위한 **Touch ID**: 사용자가지문을사용하여장치의잠금을해제하도록허용합니다.
- 잠겨있을경우 **Passbook** 알림: 잠금화면에 Passbook 알림이표시되도록허용합니다.
- 핸드오프: 사용자가한 iOS 장치에서근처의다른 iOS 장치로활동을전송할수있도록허용합니다.
- 관리되는앱에대한 **iCloud** 동기화: 사용자가관리되는앱을 iCloud 와동기화하도록허용합니다.
- 엔터프라이즈북에대한백업: 엔터프라이즈북을 iCloud 에백업하도록허용합니다.
- 엔터프라이즈북동기화에대한메모및하이라이트: 사용자가엔터프라이즈북에추가한메모및하이라이트를 iCloud 와동기화할수있도록허용합니다.
- **Spotlight** 에대한인터넷결과: Spotlight 가인터넷뿐만아니라장치의검색결과를표시하도록허용합니다.
- 엔터프라이즈앱신뢰: 엔터프라이즈응용프로그램을신뢰할수있도록허용합니다.
- 관리되지않는앱이관리되는연락처읽기: 선택사항. 관리되지않는앱에있는관리되는앱의문서가사용되지않는경우에만사용할수있습니다. 사용하도록설정하면관리되지않는앱이관리되는계정의연락처에서데이터를읽을수있습니다. 기본값은 꺼짐입니다. iOS 12 부터사용할수있습니다.

- 관리되는앱이관리되지않는연락처쓰기: 선택사항. 사용하도록설정하면관리되는앱에서관리되지않는계정의연락처에연락처를쓸수있습니다. 관리되지않는앱에있는관리되는앱의문서를사용하는경우이제한은영향을미치지않습니다. 기본값은 꺼짐입니다. iOS 12 부터사용할수있습니다.

- 감독되는경우에만해당되는설정 - 허용

이러한설정은감독되는장치에만적용됩니다. iOS 장치를감독모드로설정하는단계는 [Apple Configurator](#) 를사용하여 [iOS 장치를감독모드로전환](#)을참조하십시오.

- 모든내용및설정지우기: 사용자가장치에서모든콘텐츠및설정을지울수있도록허용합니다.
- 제한구성: 사용자가장치에서자녀보호기능을구성하도록허용합니다.
- 팟캐스트: 사용자가팟캐스트를다운로드하고동기화하도록허용합니다.
- 구성프로필설치: 사용자가배포된구성프로필과다른구성프로필을설치하도록허용합니다.
- 지문수정: 사용자가 Touch ID 지문을변경하거나삭제하도록허용합니다.
- 장치에서앱설치: 사용자가앱을설치하도록허용합니다.
- 바로가기키: 사용자가자주사용하는단어나구에대한사용자지정바로가기키를만들수있도록허용합니다.
- 페어링된 **Apple Watch**: 사용자가 Apple Watch 를감독되는장치와페어링할수있도록허용합니다.
- 암호수정: 사용자가감독되는장치에서암호를변경할수있도록허용합니다.
- 장치이름수정: 사용자가장치이름을변경할수있도록허용합니다.
- 배경화면수정: 사용자가장치에서배경화면을변경할수있도록허용합니다.
- 자동으로앱다운로드: 앱다운로드를허용합니다.
- **AirDrop**: 사용자가인접한 iOS 장치와사진, 비디오, 웹사이트, 위치등을공유할수있도록허용합니다.
- **iMessage**: 사용자가 iMessage 를사용하여 Wi-Fi 를통한텍스트를사용하도록허용합니다.
- **Siri** 사용자생성콘텐츠: Siri 가웹에서사용자생성콘텐츠를쿼리하도록허용합니다. 전통적인저널리스트가아닌소비가사용자생성콘텐츠를제작합니다. 예를들어 Twitter 또는 Facebook 에서찾은콘텐츠가사용자가생성한콘텐츠입니다.
- **iBooks**: 사용자가 iBooks 앱을사용할수있도록허용합니다.
- 앱제거: 사용자가장치에서앱을삭제하도록허용합니다.
- 게임센터: 사용자가장치에서 Game Center 를통해온라인게임을플레이할수있도록허용합니다.
 - * 친구추가: 사용자가게임을할친구에게알림을보낼수있도록허용합니다.
 - * 멀티플레이게임: 사용자가장치에서멀티플레이게임을시작할수있도록허용합니다.
- 계정설정수정: 사용자가장치계정설정을수정할수있도록허용합니다.
- 앱셀러레이터설정수정: 앱이셀러레이터를사용하는방식을사용자가수정할수있도록허용합니다.
- 내친구찾기설정수정: 사용자가내친구찾기설정을변경할수있도록허용합니다.

- 비 **Configurator** 호스트와 페어링: 관리자가 사용자 장치가 페어링할 수 있는 장치를 제어할 수 있도록 허용합니다. 이 설정을 사용하지 않도록 설정하면 Apple Configurator 를 실행하는 감독되는 호스트 이외에는 페어링할 수 없습니다. 감독 호스트 인증서가 구성되어 있지 않으면 모든 페어링을 사용할 수 없습니다.
- 키보드 자동 완성: 사용자 장치가 키보드 자동 완성 기능을 사용하여 입력하는 단어를 제안할 수 있도록 허용합니다. 사용자가 추천 단어를 액세스하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 키보드 자동 수정: 사용자 장치가 키보드 자동 수정을 사용할 수 있도록 허용합니다. 사용자가 자동 수정에 액세스하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 키보드 맞춤법 검사: 입력하는 동안 사용자 장치가 맞춤법 검사를 사용할 수 있도록 허용합니다. 사용자가 맞춤법 검사에 액세스하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 정의 조회: 입력하는 동안 사용자 장치가 정의 조회를 사용할 수 있도록 허용합니다. 사용자가 입력하는 동안 정의를 조회하지 못하도록 하는 표준화된 테스트 관리와 같은 상황에서는 이 옵션을 비활성화하십시오.
- 단일 앱 번들 **ID**: 장치에 대한 제어 권한을 유지하고 다른 앱 또는 기능과의 상호 작용을 방지하도록 허용된 앱 목록을 만듭니다. 앱을 추가하려면 추가를 클릭하고 앱 이름을 입력한 후 저장을 클릭합니다. 추가할 각 앱에 대해 이 프로세스를 반복합니다.
- 뉴스: 사용자가 뉴스 앱을 사용할 수 있도록 허용합니다.
- **Apple Music** 서비스: 사용자가 Apple Music 서비스를 사용할 수 있도록 허용합니다. Apple Music 서비스를 허용하지 않는 경우 Music 앱이 클래식 모드에서 실행됩니다.
- **iTunes Radio**: 사용자가 iTunes Radio 를 사용할 수 있도록 허용합니다.
- 알림 수정: 사용자가 알림 설정을 수정할 수 있도록 허용합니다.
- 암호 자동 채우기: 선택 사항입니다. 사용하지 않는 경우 사용자는 암호 자동 채우기 또는 강력한 자동 암호 기능을 사용할 수 없습니다. 기본값은 켜짐입니다. iOS 12 부터 사용할 수 있습니다.
- 암호 근접 요청: 선택 사항입니다. 사용하지 않는 경우 사용자의 장치는 주변 장치에서 암호를 요청하지 않습니다. 기본값은 켜짐입니다. iOS 12 부터 사용할 수 있습니다.
- 암호 공유: 선택 사항입니다. 사용하지 않는 경우 사용자는 Airdrop 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 켜짐입니다. iOS 12 부터 사용할 수 있습니다.
- 제한된 앱 사용: 사용자가 제공된 번들 ID 를 기반으로 모든 앱을 사용하거나 일부 앱을 사용하거나 사용하지 않도록 허용합니다. 감독되는 장치에만 적용됩니다.

참고:

iOS 11 부터 앱 제한에서 사용할 수 있는 Apple 정책이 변경되었습니다. Apple 의 경우 더 이상 적절한 iOS 응용 프로그램 번들을 제한하여 설정 앱과 전화 앱에 대한 액세스를 제거할 수 없습니다.

일부 앱을 차단하는 제한 장치 정책을 구성한 후 정책 배포: 나중에 해당 앱 중 일부 또는 전부를 허용하려는 경우 제한 장치 정책을 변경하고 배포해도 제한이 변경되지 않습니다. 이 경우 iOS 가 변경 내용을 iOS 프로필에 적용하지 않습니다. 계속하려면 프로필 제거 정책을 사용하여 iOS 프로필을 제거한 후 업데이트된 제한 장치 정책을 배포해야 합니다.

이 설정을 **Only allow some apps**(일부 앱만 허용) 로 변경하는 경우: 이 정책을 배포하기 전에 Apple DEP 를 사용하여 등록된 장치의 사용자가 설정 도우미에서 Apple 계정으로 로그인할 수 있도록 해당 사용자에게 알려줘야 합니다. 그렇지 않으면 사용자가 장치에서 2 단계 인증을 사용하지 않도록 설정해야 Apple 계정으로 로그인하고 허용된 앱에 액세스할 수 있습니다.

- 진단 제출 수정: 사용자가 설정 > 진단 및 사용 현황 창의 설정에서 진단 제출 및 앱 분석 설정을 변경할 수 있도록 허용합니다.
- **Bluetooth** 수정: 사용자가 Bluetooth 설정을 수정할 수 있도록 허용합니다.
- 받아쓰기 허용: 감독되는 경우에만 해당. 이 제한을 꺼짐으로 설정하면 받아쓰기 입력이 허용되지 않습니다. 기본 설정은 켜짐입니다.
- **WiFi** 정책에 따라 설치된 **WiFi** 네트워크에만 참가: 선택 사항입니다. 감독되는 경우에만 해당. 이 제한을 꺼짐으로 설정하면 구성 프로필을 통해 설정된 장치만 WiFi 네트워크에 참여할 수 있습니다. 기본 설정은 꺼짐입니다.
- 메시지를 표시하지 않고 교실 앱이 앱 및 장치를 잠글 수 있도록 허용: 이 제한을 꺼짐으로 설정하면 교실 앱이 사용자에게 메시지를 표시하지 않고 자동으로 사용자 장치와 앱을 잠급니다. 기본 설정은 꺼짐입니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- 메시지를 표시하지 않고 교실 앱 클래스에 자동 참가: 이 제한을 꺼짐으로 설정하면 교실 앱이 사용자에게 메시지를 표시하지 않고 사용자를 자동으로 클래스에 참가시킵니다. 기본 설정은 꺼짐입니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- **AirPrint** 허용: 이 제한을 꺼짐으로 설정하면 사용자가 AirPrint 를 사용하여 인쇄할 수 없습니다. 기본 설정은 켜짐입니다. 이 제한이 켜짐인 경우 다음과 같은 추가 제한이 표시됩니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
 - * 키집합에 **AirPrint** 자격 증명 저장 허용: 이 제한을 선택 취소하면 AirPrint 사용자 이름과 암호가 키집합에 저장되지 않습니다. 기본 설정은 선택되어 있습니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
 - * **iBeacon** 을 사용하여 **AirPrint** 프린터 검색 허용: 이 제한을 선택 취소하면 AirPrint 프린터에 대한 iBeacon 검색이 사용되지 않습니다. 이렇게 하면 위장한 AirPrint Bluetooth 알림의 네트워크 트래픽 피싱이 방지됩니다. 기본 설정은 선택되어 있습니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
 - * 신뢰할 수 있는 인증서가 있는 대상에만 **AirPrint** 허용: 이 제한을 선택하면 사용자가 AirPrint 를 사용하여 신뢰할 수 있는 인증서가 있는 대상에만 인쇄할 수 있습니다. 기본 설정은 선택 취소되어 있습니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- **VPN** 구성 추가: 이 제한을 꺼짐으로 설정하면 사용자가 VPN 구성을 만들 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- 셀룰러 요금제 설정 수정: 이 제한을 꺼짐으로 설정하면 사용자가 셀룰러 요금제 설정을 수정할 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전) 을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- 자동 날짜 및 시간 적용: 감독되는 장치에서 날짜와 시간을 자동으로 설정할 수 있습니다. 켜짐인 경우 장치 사용자는 일반 > 날짜 및 시간에서 자동으로 설정을 끌 수 없습니다. 장치의 표준 시간대는 장치가 해당 위치를 확인할 수 있는 경우에만 업

데이트됩니다. 즉, 장치에 위치 서비스가 활성화된 셀룰러 연결 또는 WiFi 연결이 있는 경우입니다. 기본값은 꺼짐입니다. iOS 12 이상의 감독되는 장치에서만 사용할 수 있습니다.

- 시스템업제거: 이 제한을 꺼짐으로 설정하면 사용자가 시스템업 장치를 제거할 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- 새로운 주변장치 설정: 이 제한을 꺼짐으로 설정하면 사용자가 새로운 주변 장치를 설정할 수 없습니다. 기본 설정은 켜짐입니다. iOS 11(최소 버전)을 실행하는 감독되는 장치에서 사용할 수 있습니다.
- **USB** 제한 모드 허용: 꺼짐인 경우 장치가 잠겨 있는 동안 항상 USB 액세스 리에 연결할 수 있습니다. 기본값은 켜짐입니다. iOS 11.3 이상의 감독되는 장치에서만 사용할 수 있습니다.
- 소프트웨어 업데이트 강제 지연: 켜짐인 경우 사용자에게 소프트웨어 업데이트 표시가 지연됩니다. 이 제한을 적용하면 소프트웨어 업데이트 릴리스 날짜로부터 지정된 기간 (일) 까지 소프트웨어 업데이트가 표시되지 않습니다. 기본값은 꺼짐입니다. iOS 11.3 및 macOS 10.13.4 부터 사용할 수 있습니다.
- 소프트웨어 업데이트 시행 지연 (일): 장치에서 소프트웨어 업데이트를 지연할 일수를 지정할 수 있습니다. 최대 지연은 **90** 일입니다. 기본값은 **30** 일입니다. iOS 11.3 및 macOS 10.13.4 부터 사용할 수 있습니다.
- 교실에서 클래스를 나갈 때 허가 요청 시행: 켜짐인 경우 교실 앱을 통해 관리되지 않는 과정에 등록한 학생이 과정을 나가려면 교사의 허가를 요청해야 합니다. 기본값은 꺼짐입니다. iOS 11.3 부터 사용할 수 있습니다.

• 보안 - 잠금 화면에 표시

- 제어 센터: 잠금 화면에서 제어 센터에 액세스할 수 있습니다. 사용자는 제어 센터에서 비행기 모드, WiFi, Bluetooth, 방해 금지 모드 및 회전 잠금 설정을 쉽게 수정할 수 있습니다.
- 알림: 잠금 화면에서 알림을 허용합니다.
- 오늘의 보기: 날씨 및 오늘날짜의 일정 항목과 같은 정보를 잠금 화면에 집계하는 [오늘의 보기] 를 허용합니다.

• 미디어 콘텐츠 - 허용

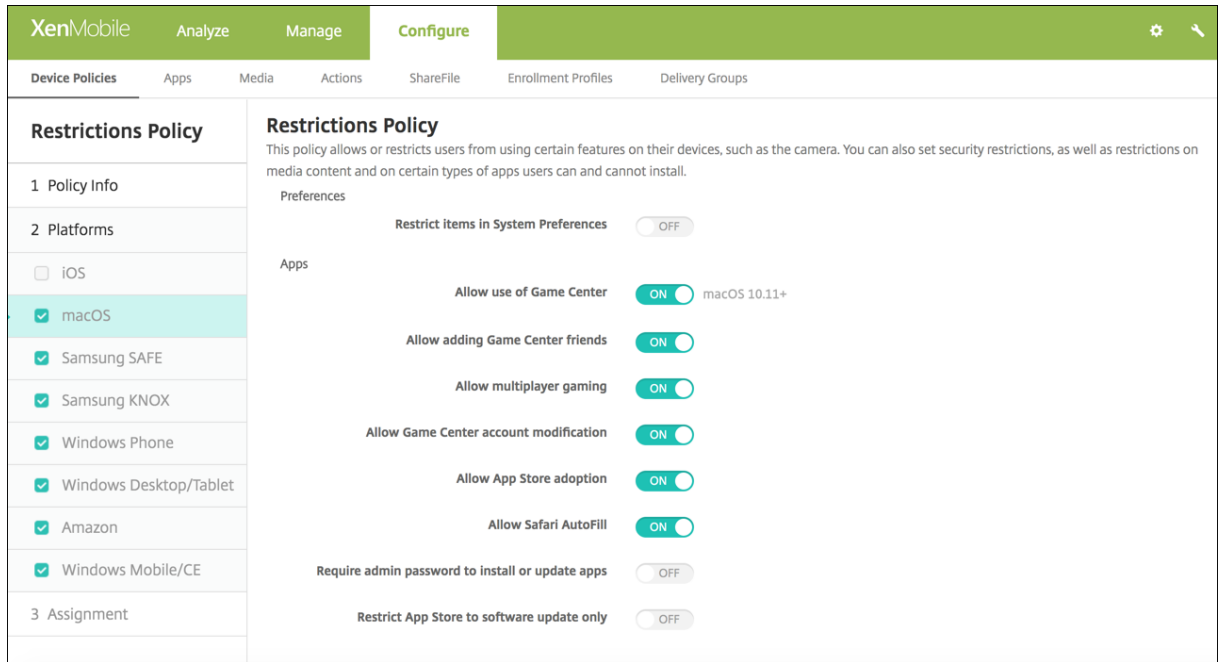
- 음악, 팟캐스트 및 iTunes U 의 성인 등급 자료: 사용자의 장치에 무삭제 판 자료를 허용합니다.
- iBooks 의 성인 관련 성인 등급 콘텐츠: iBooks 에서 무삭제 판 자료를 다운로드하도록 허용합니다.
- 평가 지역: 유해 콘텐츠 차단 등급을 얻는 지역을 설정합니다. 목록에서 평가 지역을 설정할 국가를 클릭합니다. 기본값은 미국입니다.
- 영화: 사용자 장치에서 영화를 허용할지 여부를 설정합니다. 영화가 허용된 경우 선택적으로 영화 등급을 설정합니다. 목록에서 장치에 영화를 허용하거나 제한하는 옵션을 선택합니다. 기본값은 모든 영화 허용입니다.
- TV 쇼: 사용자 장치에서 TV 쇼를 허용할지 여부를 설정합니다. TV 쇼가 허용된 경우 선택적으로 TV 쇼 등급을 설정합니다. 목록에서 장치에 TV 쇼를 허용하거나 제한하는 옵션을 선택합니다. 기본값은 모든 TV 쇼 허용입니다.
- 앱: 사용자 장치에서 앱을 허용할지 여부를 설정합니다. 앱이 허용된 경우 선택적으로 앱 등급을 설정합니다. 목록에서 장치에 앱을 허용하거나 제한하는 옵션을 선택합니다. 기본값은 모든 앱 허용입니다.

• 정책 설정

- 정책 제거: 이 정책을 장치에서 제거할 시기를 선택할 수 있습니다. 날짜 선택을 선택하면 날짜 선택기를 사용하여 정책이 제거되는 시기를 선택할 수 있습니다. 제거할 때까지 기간 (시간) 을 선택하면 정책이 제거될 때까지의 시간을 입력할 수 있습니다.

- 사용자정책을제거하도록허용: 사용자가제한정책을제거할수있습니다. 옵션은 항상, 암호필요또는 안함입니다.
- 프로필범위: 제한정책을 시스템또는 사용자에게적용할수있습니다.

macOS 설정



- 기본설정

- 시스템기본설정에서항목제한: 시스템기본설정에대사용자액세스를허용하거나제한합니다. 기본값은시스템기본 설정에대사용자의전체액세스를허용하는 꺼짐입니다. 사용하는경우다음설정을구성합니다.

* 시스템기본설정창: 선택한설정을사용할지여부를선택합니다. 기본값은모든설정을사용하도록설정하는것이 며, 기본적으로 꺼짐입니다.

- 사용자및그룹
- 일반
- 내게필요한옵션
- App Store
- 소프트웨어업데이트
- Bluetooth
- CD 및 DVD
- 날짜및시간
- 데스크톱및화면보호기
- 디스플레이
- 고정
- 절전
- 확장
- FibreChannel

- iCloud
 - 잉크
 - 인터넷계정
 - 키보드
 - 언어및텍스트
 - Mission Control
 - 마우스
 - 네트워크
 - 알림
 - 자녀보호
 - 프린터및스캐너
 - 프로필
 - 보안및개인정보
 - 공유
 - 사운드
 - 받아쓰기및음성
 - Spotlight
 - 시동디스크
 - Time Machine
 - 트랙패드
 - Xsan
- 앱
 - 게임센터사용허용: 사용자가 Game Center 를통해온라인게임을할수있도록허용합니다. 기본값은 켜짐입니다.
 - 게임센터친구추가허용: 사용자가게임을할친구에게알림을보낼수있도록허용합니다. 기본값은 켜짐입니다.
 - 멀티플레이게임허용: 사용자가멀티플레이어게임을시작할수있도록허용합니다. 기본값은 켜짐입니다.
 - 게임센터계정수정허용: 사용자가 Game Center 계정설정을수정할수있도록허용합니다. 기본값은 켜짐입니다.
 - **App Store** 채택허용: App Store 에서 OS X 의기존앱을채택하는것을허용하거나제한합니다. 기본값은 켜짐입니다.
 - **Safari** 자동채우기허용: Safari 가암호, 주소및다른저장된기본정보로웹사이트의필드를자동으로채우도록허용합니다. 기본값은 켜짐입니다.
 - 앱을설치또는업데이트하려면관리자암호가필요함: 앱을설치하거나업데이트하려면관리자암호가필요합니다. 기본값은 꺼짐이며, 관리자암호가필요하지않습니다.
 - **App Store** 를소프트웨어업데이트전용제한: App Store 를업데이트전용으로제한합니다. 업데이트를제외한 App Store 의모든탭이비활성화됩니다. 기본값은전체 App Store 액세스권한을허용하는 꺼짐입니다.
 - 열기가허용된앱제한: 사용자가사용할수있는앱을제한하거나허용합니다. 기본값은모든앱을사용하도록허용하는꺼짐입니다. 사용하는경우다음설정을구성합니다.
 - * 허용되는앱: 추가를클릭하고시작하도록허용된앱의번들 ID 와이름을입력한다음 저장을클릭합니다. 시작하도록허용할각앱에대해이단계를반복합니다.
 - * 허용되지않은폴더: 추가를클릭하고사용자엑세스를제한할폴더의파일경로 (예: /Applications/Utilities)

를 입력한 다음 저장을 클릭합니다. 사용자가 액세스할 수 없게 하려는 모든 폴더에 대해 이 단계를 반복합니다.

- * 허용되는 폴더: 추가를 클릭하고 사용자에게 액세스하도록 허가할 폴더의 파일 경로를 입력한 다음 저장을 클릭합니다. 사용자가 액세스할 수 있게 하려는 모든 폴더에 대해 이 단계를 반복합니다.

- 위젯

- 다음 대시보드 위젯만 실행되도록 허용: 세계시계 또는 계산기와 같이 사용자에게 실행하도록 허용된 대시보드 위젯을 허용하거나 제한합니다. 기본값은 사용자가 모든 위젯을 실행하도록 허용하는 것입니다. 사용하는 경우 다음 설정을 구성합니다.

- * 허용되는 위젯: 추가를 클릭하고 실행하도록 허용된 위젯의 이름 및 ID 를 입력한 다음 저장을 클릭합니다. 대시보드에서 실행하려는 각 위젯에 대해 이 단계를 반복합니다.

- 미디어

- **AirDrop** 허용: 사용자가 인접한 iOS 장치와 사진, 비디오, 웹사이트, 위치 등을 공유할 수 있도록 허용합니다.

- 공유

- 새 공유 서비스를 자동으로 사용: 공유 서비스를 자동으로 사용할지 여부를 선택합니다.
- 메일: 공유 사서함을 허용할지 여부를 선택합니다.
- **Facebook**: 공유 Facebook 계정을 허용할지 여부를 선택합니다.
- 비디오 서비스 - **Flickr, Vimeo, Tudou** 및 **Youku**: 공유 비디오 서비스를 허용할지 여부를 선택합니다.
- **Aperture** 에 추가: Aperture 에 공유 기능을 추가하도록 허용할지 여부를 선택합니다.
- **Sina Weibo**: 공유 Sina Weibo 마이크로블로그 계정을 허용할지 여부를 선택합니다.
- **Twitter**: 공유 Twitter 계정을 허용할지 여부를 선택합니다.
- 메시지: 메시지에 대한 공유 액세스를 허용할지 여부를 선택합니다.
- **iPhoto** 에 추가: iPhoto 에 공유 기능을 추가하도록 허용할지 여부를 선택합니다.
- 읽기 목록에 추가: 읽기 목록에 공유 기능을 추가하도록 허용할지 여부를 선택합니다.
- **AirDrop**: 공유 AirDrop 계정을 허용할지 여부를 선택합니다.

- 기능

- 데스크톱 바탕화면 잠금: 사용자가 바탕화면 사진을 변경할 수 있는지 여부를 선택합니다. 기본값은 사용자가 바탕화면 사진을 변경할 수 있는 것입니다.
- 카메라 사용 허용: 사용자가 Mac 에서 카메라를 사용할 수 있는지 여부를 선택합니다. 기본값은 사용자가 카메라를 사용할 수 없는 것입니다.
- **Apple Music** 허용: 사용자가 Apple Music 서비스를 사용할 수 있도록 허용합니다 (macOS 10.12 이상). Apple Music 서비스를 허용하지 않는 경우 Music 앱이 클래식 모드에서 실행됩니다. 감독되는 장치에만 적용됩니다. 기본값은 켜집니다.
- **Spotlight** 제안 허용: 사용자가 Spotlight 제안을 사용하여 Mac 을 검색하고 인터넷, iTunes 및 App Store 의 Spotlight 제안을 제공할 수 있는지 여부를 선택합니다. 기본값은 사용자가 Spotlight 제안을 사용하지 못하게 하는 것입니다.
- 조회 허용: 사용자가 상황에 맞는 메뉴 또는 Spotlight 검색 메뉴를 사용하여 단어의 정의를 조회할 수 있는지 여부를 선택합니다. 기본값은 사용자가 Mac 에서 조회를 사용하지 못하게 하는 것입니다.
- 로컬 계정에 **iCloud** 암호 사용 허용: 사용자가 Apple ID 및 iCloud 암호를 사용하여 Mac 에 로그인할 수 있는지 여부를 선택합니다. 이 정책을 사용하도록 설정하면 사용자가 Mac 의 모든 로그인 화면에서 하나의 ID 와 암호만 사용할 수 있습니다. 기본값은 사용자가 Apple ID 및 iCloud 암호를 사용하여 Mac 에 액세스할 수 있도록 허용하는 것입니다.

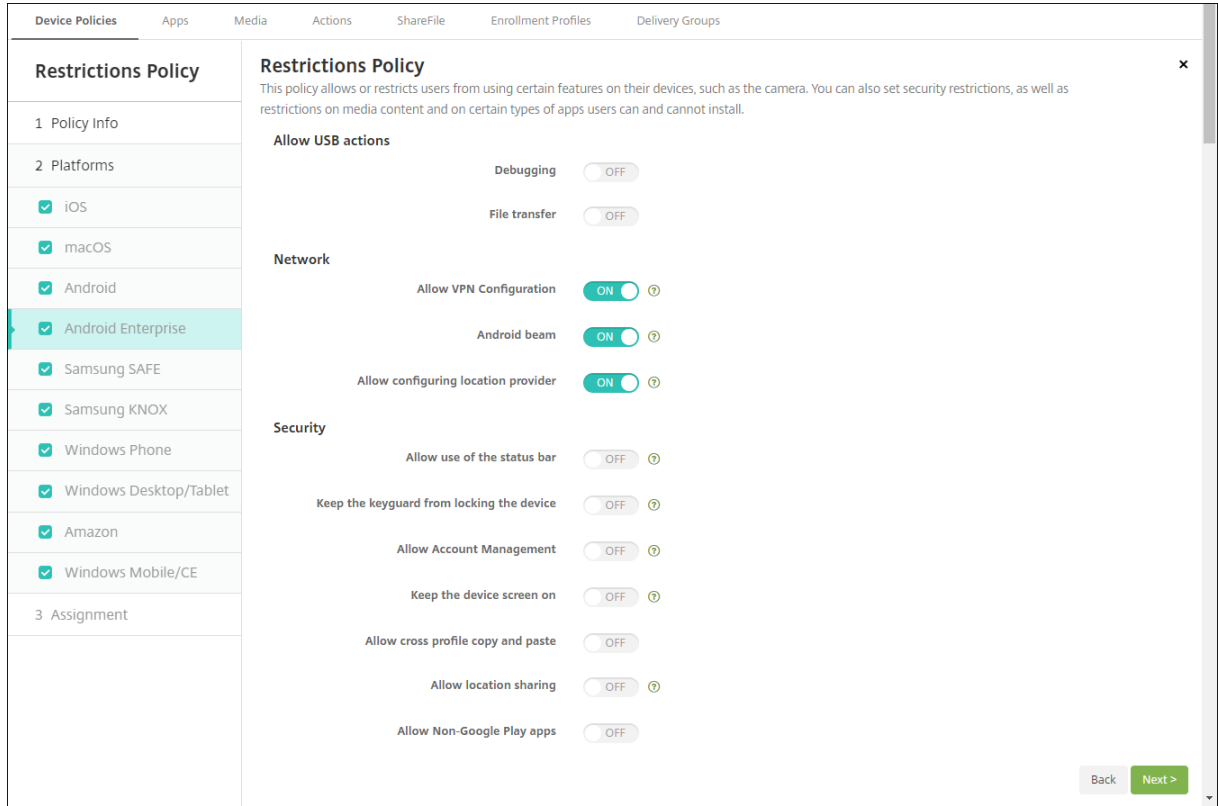
니다.

- **iCloud** 문서및데이터허용: 사용자가 Mac 에서 iCloud 에저장된문서및데이터에엑세스할수있도록허용할지여부를선택합니다. 기본값은사용자가 Mac 에서 iCloud 문서및데이터를사용하지못하게하는 꺼짐입니다.
 - * **iCloud** 바탕화면및문서허용: (macOS 10.12.4 이상) 기본적으로선택됩니다.
- **iCloud** 키집합동기화허용: iCloud 키집합동기화를허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 메일허용: 사용자가 iCloud 메일을사용할수있도록허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 연락처허용: 사용자가 iCloud 연락처를사용할수있도록허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 일정허용: 사용자가 iCloud 일정을사용할수있도록허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 미리알림허용: 사용자가 iCloud 미리알림을사용할수있도록허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 책갈피허용: 사용자가 iCloud 책갈피를동기화할수있도록허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 메모허용: 사용자가 iCloud 메모를사용할수있도록허용합니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **iCloud** 사진허용: 이설정을 꺼짐으로변경하면 iCloud 사진라이브러리에서완벽하게다운로드되지않은모든사진이로컬장치스토리지에서제거됩니다 (macOS 10.12 이상). 기본값은 켜짐입니다.
- 자동잠금해제허용: 이 옵션 및 Apple Watch 에 대한 자세한 내용은 <https://www.imore.com/autounlock>을참조하십시오 (macOS 10.12 이상). 기본값은 켜짐입니다.
- **Touch ID** 를 통한 **Mac** 잠금해제허용: (macOS 10.12.4 이상). 기본값은 켜짐입니다.
- 소프트웨어업데이트강제지연: 켜짐인 경우사용자에게소프트웨어업데이트표시가 지연됩니다. 소프트웨어업데이트 릴리스날짜로부터지정된기간 (일) 까지소프트웨어업데이트가 표시되지 않습니다. 기본값은 꺼짐입니다. macOS 10.13.4 이상을 실행하는 감독되는 장치에만 사용할 수 있습니다.
- 소프트웨어업데이트시행지연 (일): 장치에서 소프트웨어업데이트를 지연할 일수를 지정합니다. 최대값은 90 일입니다. 기본값은 30 입니다. macOS 10.13.4 이상을 실행하는 감독되는 장치에만 사용할 수 있습니다.
- 암호자동채우기: 선택사항입니다. 사용하지 않는 경우 사용자 암호 자동 채우기 또는 강력한 자동 암호 기능을 사용할 수 없습니다. 기본값은 켜짐입니다. macOS 10.14 부터 사용할 수 있습니다.
- 암호근접요청: 선택사항입니다. 사용하지 않는 경우 사용자의 장치는 주변 장치에서 암호를 요청하지 않습니다. 기본값은 켜짐입니다. macOS 10.14 부터 사용할 수 있습니다.
- 암호공유: 선택사항입니다. 사용하지 않는 경우 사용자 암호 기능을 사용하여 암호를 공유할 수 없습니다. 기본값은 켜짐입니다. macOS 10.14 부터 사용할 수 있습니다.

Android 설정

- 카메라: 사용자가 장치에서 카메라를 사용할 수 있도록 허용합니다. 꺼짐인 경우 카메라가 사용되지 않습니다. 기본값은 켜짐입니다.

Android Enterprise 설정



Android Enterprise 의작업프로필모드에서장치등록하는경우 **USB** 디버깅및알수없는소스설정은기본적으로사용되지않도록설정됩니다.

Android 8.0 이상및 Samsung Knox 3.0 이상을실행하는장치의경우 **Android Enterprise** 페이지에서 Samsung Knox 및 Samsung SAFE 에대한설정을구성합니다. 이전버전의 Android 또는 Samsung Knox 를실행하는장치의경우 **Samsung Knox** 페이지및 **Samsung SAFE** 페이지를사용합니다.

- **USB** 동작허용
 - 디버깅. USB 를통한디버깅을허용합니다. 기본값은 꺼짐입니다.
 - 파일전송. USB 를통한파일전송을허용합니다. 기본값은 꺼짐입니다.
- 네트워크
 - **VPN** 구성허용. 사용자가 VPN 구성을만들수있습니다. Android 6 이상을실행하는작업프로필장치와완전관리되는장치를위한설정입니다. 기본값은 켜짐입니다.
 - **Android Beam**. 사용자가 NFC(근거리통신) 를사용하여장치의웹페이지, 사진, 비디오또는기타콘텐츠를다른장치로보낼수있도록허용합니다. MDM 4.0 이상에서사용할수있습니다. 기본값은 꺼짐입니다.
 - 위치제공자구성허용. 사용자가장치에서 GPS 를켜줄수있도록허용합니다. Android API 28 이상을위한설정입니다. 기본값은 켜짐입니다.
- 보안
 - 상태표시줄의사용허용. 켜짐으로설정하는경우관리되는장치및전용장치 (COSU 장치라고도함) 에서상태표시줄이사용됩니다. 이렇게하면알림, 빠른설정및전체화면모드에서벗어날수있는기타화면오버레이가사용되지않습니

- 다. 사용자는 시스템 설정으로 이동하여 알림을 볼 수 있습니다. Android 6.0 이상을 위한 설정입니다. 기본값은 꺼짐입니다.
- **Keyguard** 가장치를 잠그지 않도록 방지. 켜짐으로 설정하는 경우 관리되는 장치 및 전용 장치 (COSU 장치라고도 함) 의 잠금 화면에서 Keyguard 가 사용되지 않습니다. 기본값은 꺼짐입니다.
 - 계정 관리 허용. 작업 프로필 및 관리되는 장치에 계정을 추가할 수 있습니다. 기본값은 꺼짐입니다.
 - 장치 화면을 켜진 상태로 유지. 이 설정을 켜짐으로 설정하면 장치를 연결할 때 장치 화면이 켜진 상태로 유지됩니다. 기본값은 꺼짐입니다.
 - 상호 프로필 복사 및 붙여넣기 허용. Android Enterprise 프로필의 앱과 개인 영역의 앱 간에 클립 보드를 사용한 복사 및 붙여넣기를 허용하거나 차단합니다. 기본값은 꺼짐입니다.
 - 위치 공유 허용. 위치 공유를 허용합니다. 관리되는 프로필의 경우 장치 소유자가 이 설정을 재정의할 수 있습니다. 기본값은 꺼짐입니다.
 - **Google Play** 이외의 앱 허용. Google Play 이외의 스토어에서 앱을 설치할 수 있도록 합니다. 기본값은 꺼짐입니다.
 - 화면 캡처 허용. 사용자가 장치 화면의 화면 캡처를 기록하거나 생성할 수 있습니다. 기본값은 꺼짐입니다.
 - 카메라 사용 허용. 사용자가 장치 카메라로 사진을 찍고 비디오를 만들 수 있습니다. 기본값은 꺼짐입니다.
 - 응용 프로그램 설정의 사용자 제어 허용. 사용자가 앱 제거, 앱 비활성화, 캐시 및 데이터 지우기, 원하는 앱 강제 중지 및 기본값 지우기를 할 수 있습니다. 기본값은 꺼짐입니다.
 - 홈 화면에 작업 프로필 위젯 허용. 이 설정이 켜짐인 경우 사용자가 작업 프로필 위젯을 장치 홈 화면에 배치할 수 있습니다. 이 설정이 꺼짐인 경우 사용자가 작업 프로필 위젯을 장치 홈 화면에 배치할 수 없습니다. 기본값은 꺼짐입니다.
 - * 위젯을 허용할 앱. 홈 화면에 허용할 앱 목록입니다. 홈 화면에 작업 프로필 위젯 허용을 켜짐으로 설정하고 앱을 추가합니다. 추가를 클릭하고 목록에서 홈 화면에 허용할 위젯의 앱을 선택합니다. 저장을 클릭합니다. 더 많은 앱 위젯을 허용하려면 이 프로세스를 반복합니다.
 - 장치 연락처에 작업 프로필 연락처 허용. 수신 전화에 대해 관리되는 Android Enterprise 프로필에 있는 연락처가 상 위 프로필에 표시됩니다 (Android 7.0 이상). 기본값은 꺼짐입니다.
 - 시스템 앱 사용. 사용자가 사전 설치된 장치 앱을 실행할 수 있도록 허용합니다. 기본값은 꺼짐입니다. 특정 앱을 사용하려면 시스템 앱 목록 테이블에서 추가를 클릭합니다.
 - * 시스템 앱 목록. 장치에서 사용할 시스템 앱 목록입니다. 시스템 앱을 켜짐으로 설정하고 앱 패키지 이름을 추가합니다. 시스템 앱의 패키지 이름을 조회하려면 Android Debug Bridge(adb) 를 사용하여 Android PM(패키지 관리자) 명령을 호출하면 됩니다. 예: `adb shell "pm list packages -f name"`. 여기서 "name" 은 패키지 이름의 일부입니다. 자세한 내용은 <https://developer.android.com/studio/command-line/adb>에서 참조하십시오. Android Enterprise 장치의 경우 **Android Enterprise 관리되는 구성 정책** 정책을 사용하여 앱 권한을 제한할 수 있습니다.
 - 응용 프로그램 사용 안 함. 장치에서 지정된 목록의 앱이 실행되지 않도록 차단합니다. 기본값은 꺼짐입니다. 설치된 앱을 사용하지 않도록 설정하려면 설정을 켜짐으로 변경한 다음 응용 프로그램 목록 테이블에서 추가를 클릭합니다.
 - * 응용 프로그램 목록. 차단하려는 앱의 목록입니다. 응용 프로그램 사용 안 함을 켜짐으로 설정하고 앱을 추가합니다. 앱 패키지 이름을 입력합니다. 앱 목록을 변경하고 배포하면 이전 앱 목록을 덮어 씩습니다. 예: com.example1 및 com.example2 를 사용하지 않도록 설정하고 나중에 com.example1 및 com.example3 으로 목록을 변경하는 경우 XenMobile 은 com.example.2 를 사용하도록 설정합니다.
 - 앱 확인 사용. OS 에서 앱을 검사하여 악성 동작을 감지할 수 있도록 합니다. 기본값은 켜짐입니다.

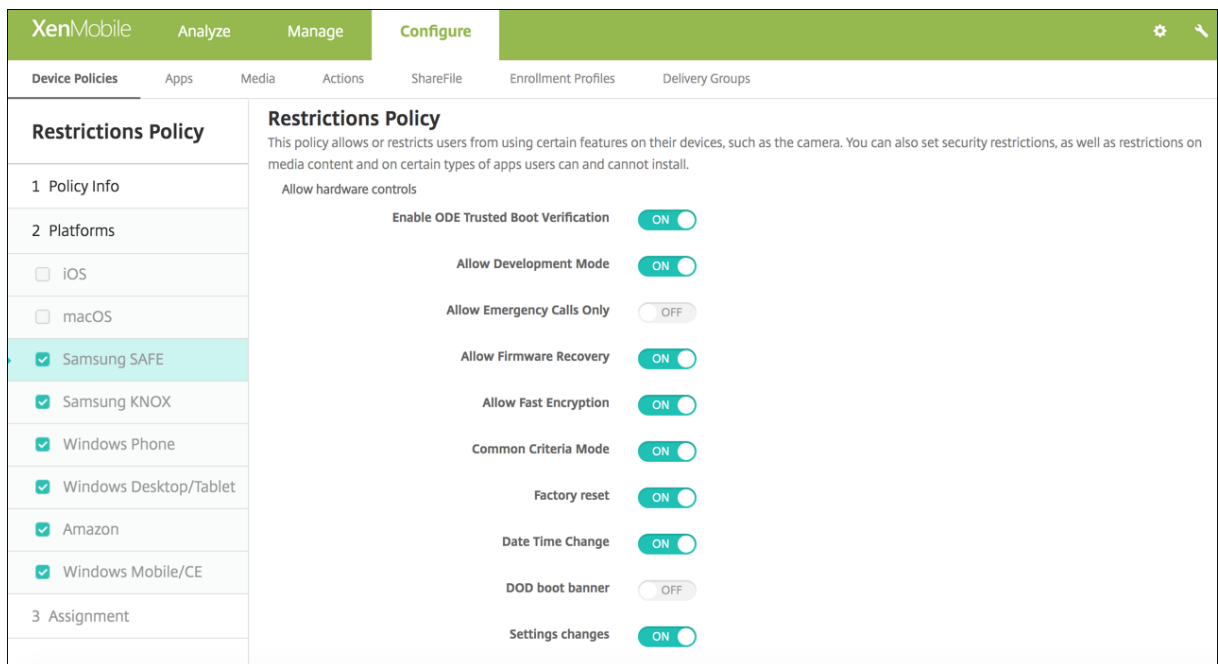
- **Google** 앱사용. 사용자가 Google Mobile Services 의앱을장치로다운로드할수있습니다. 기본값은 켜짐입니다.
- 완전히관리되는장치
 - 여러사용자허용. 여러사용자가장치를사용할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
 - 로밍허용. 로밍하는동안사용자가셀룰러데이터를사용할수있도록허용합니다. 기본값은사용자의장치에서로밍을비활성화하는꺼짐입니다. 기본값은 꺼짐입니다.
 - **SMS** 허용. 사용자가 SMS 메시지를보내고받을수있습니다. 기본값은 꺼짐입니다.
 - 백업. 사용자가장치에서응용프로그램및시스템데이터를백업할수있도록허용합니다. 기본값은 켜짐입니다.
 - **Bluetooth**. 사용자가 Bluetooth 를사용할수있도록허용합니다. 기본값은 켜짐입니다.
 - 셀룰러데이터. 사용자가데이터에해셀룰러연결을사용할수있도록허용합니다. 기본값은 켜짐입니다.
 - 일별제한 (**MB**). 사용자가하루에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
 - 주별제한 (**MB**). 사용자가한주에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
 - 월별제한 (**MB**). 사용자가한달에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
 - 날짜시간변경. 사용자가장치에서날짜및시간을변경할수있도록허용합니다. 기본값은 켜짐입니다.
 - 공장기본값으로재설정. 사용자가장치에서공장기본값으로재설정을수행할수있도록허용합니다. 기본값은 켜짐입니다.
 - 호스트스토리지. USB 장치가연결될때사용자의장치가 USB 호스트로작동할수있도록허용합니다. 그러면사용자의장치가 USB 장치에전원을공급합니다. 기본값은 켜짐입니다.
 - 대용량스토리지. USB 연결을통해사용자의장치와컴퓨터간에서대용량데이터파일을전송하도록허용합니다. 기본값은 켜짐입니다.
 - 마이크. 사용자가장치에서마이크를사용할수있도록허용합니다. 기본값은 켜짐입니다.
 - 테더링. 사용자가휴대용핫스팟을구성하고데이터를테더링할수있습니다. 기본값은 꺼짐입니다. 이설정이켜져있으면 Samsung 장치에서다음설정을사용할수있습니다.
 - * **USB**. 사용자가 USB 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다.
 - * **Bluetooth**. 사용자가 Bluetooth 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다.
 - * **WiFi**. 사용자가 WiFi 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다.
 - **WiFi**. 사용자가 WiFi 네트워크에연결할수있도록허용합니다. 기본값은 켜짐입니다. 이설정이켜져있으면다음설정을사용할수있습니다.
 - * 직접. 사용자가 WiFi 연결을통해다른장치에직접연결할수있도록허용합니다. Samsung 장치에만해당됩니다. MDM 4.0 이상에서사용할수있습니다.
 - * 상태변경. 앱이 WiFi 연결상태를변경할수있도록허용합니다.
- **Samsung SAFE**: 하드웨어제어허용
 - **ODE** 신뢰할수있는부팅확인사용. ODE 신뢰할수있는부팅확인을사용하여 bootloader 에서시스템이미지까지신뢰체인을설정합니다. 기본값은 켜짐입니다.
 - 긴급호출만허용. 사용자가장치에서긴급통화전용모드를사용할수있도록허용합니다. 기본값은 꺼짐입니다.

- 펌웨어복구허용. 사용자가장치에서펌웨어를복구할수있도록허용합니다. 기본값은 켜짐입니다.
- 빠른암호화허용. 사용된메모리공간의암호화만허용합니다. 반대로, 전체디스크암호화는설정, 응용프로그램데이터, 다운로드한파일및응용프로그램, 미디어및기타파일을비롯한모든데이터를암호화합니다. 기본값은 켜짐입니다.
- **Common Criteria** 모드. 장치를 Common Criteria 모드로전환합니다. Common Criteria 구성은엄격한보안프로세스를적용합니다. 기본값은 켜짐입니다.
- **DOD** 부팅배너. 사용자의장치가다시시작되면 DoD 에서승인시스템사용알림메시지또는배너를표시합니다. 기본값은 꺼짐입니다.
- 설정변경사항. 사용자가완전관리되는장치의설정을변경할수있습니다. 기본값은 켜짐입니다.
- 무선업그레이드: 사용자의장치가무선으로소프트웨어업데이트를수신하도록허용합니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- 백그라운드데이터. 완전히관리되는장치의경우앱이백그라운드에서데이터를동기화할수있습니다. 기본값은 켜짐입니다.
- 클립보드. 사용자가장치의클립보드에데이터를복사할수있도록허용합니다.
 - * 클립보드공유. 사용자가장치와컴퓨터간에서클립보드내용을공유할수있도록허용합니다 (MDM 4.0 이상).
- 홈키. 사용자가완전관리되는장치에서 홈키를사용할수있습니다. 기본값은 켜짐입니다.
- 모의위치. 사용자가 GPS 위치를조작할수있습니다. 완전히관리되는장치에서사용할수있습니다. 기본값은 켜짐입니다.
- **NFC**. 사용자가완전관리되는장치에서 NFC 를사용할수있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- 전원끄기. 사용자가완전관리되는장치를꺼낼수있도록허용합니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- **SD** 카드. 가능한경우사용자가장치에서 SD 카드를사용할수있도록허용합니다. 기본값은 켜짐입니다.
- 음성다이얼. 사용자가장치에서음성다이얼을사용할수있도록허용합니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **SBeam**. 사용자가 NFC 및 Wi-Fi Direct 를사용하여다른사용자와콘텐츠를공유할수있도록허용합니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **SVoice**. 사용자가장치에서지능형개인비서및지식탐색기를사용할수있도록허용합니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **Samsung SAFE: 앱허용**
 - 얼굴인식: 사용자가얼굴인식앱을사용할수있습니다. 기본값은 켜짐입니다.
 - 브라우저. 사용자가웹브라우저를사용할수있도록허용합니다. 기본값은 켜짐입니다.
 - **Youtube**. 사용자가 YouTube 에액세스할수있도록허용합니다. 기본값은 켜짐입니다.
 - **Google Play/Marketplace**. 사용자가 Google Play 및 Google Apps Marketplace 에액세스할수있도록허용합니다. 기본값은 켜짐입니다.
 - 시스템앱중지. 사용자가미리설치된시스템앱을비활성화할수있도록허용합니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **Samsung SAFE: 네트워크**
 - 들어오는 **MMS**. 사용자가 MMS 메시지를받을수있습니다. 기본값은 켜짐입니다.
 - 나가는 **MMS**. 사용자가 MMS 메시지를보낼수있습니다. 기본값은 켜짐입니다.
 - 보안통신만. 사용자가보안연결만사용할수있도록허용합니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
 - 오디오녹음. 사용자가장치에서오디오를녹음할수있도록허용합니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
 - 비디오녹음. 사용자가장치에서비디오를녹음할수있도록허용합니다 (MDM 4.0 이상). 기본값은 켜짐입니다.

• **Samsung Knox**

- 해지확인사용. 해지된인증서에대한확인을사용하도록설정합니다. 기본값은 켜짐입니다.
- 앱을컨테이너로이동. 사용자가 Knox 컨테이너와장치의개인영역간에서앱을이동할수있도록허용합니다. 기본값은 켜짐입니다.
- 다중단계인증적용. 사용자는지문과함께암호또는 PIN 과같은다른인증방법을사용하여장치를열어야합니다. 기본값은 켜짐입니다.
- **TIMA** 키저장소사용. TIMA 키저장소는대칭키에대한 TrustZone 기반의보안키저장소를제공합니다. RSA 키쌍및인증서는저장을위해기본키저장소공급자로라우팅됩니다. 기본값은 켜짐입니다.
- 컨테이너에대한인증적용. 장치의잠금을해제할때사용한 Knox 컨테이너를열려면별도의다른인증을사용하십시오. 기본값은 켜짐입니다.
- 공유목록. 사용자가공유방법목록의앱간에서콘텐츠를공유할수있도록허용합니다. 기본값은 켜짐입니다.
- 감사로그사용. 장치의법의학분석을위한이벤트감사로그만들기를사용하도록설정합니다. 기본값은 켜짐입니다.
- 보안키패드사용. 사용자가 Knox 컨테이너내부의보안키보드를사용하도록강제합니다. 기본값은 켜짐입니다.
- 인증스마트카드브라우저. 스마트카드판독기가탑재된장치에서브라우저인증을사용하도록설정합니다.

Samsung SAFE 설정



일부 옵션은 특정 Samsung 모바일 기기 관리 API 에서만 사용할 수 있습니다. 이러한 옵션에는 관련 버전 정보가 표시되어 있습니다.

• 하드웨어 제어 허용

- **ODE** 신뢰할 수 있는 부팅 확인 사용: ODE 신뢰할 수 있는 부팅 확인을 사용하여 bootloader 에서 시스템 이미지까지 신뢰 체인을 설정합니다.
- 개발 모드 허용: 사용자가 장치에서 개발자 설정을 사용할 수 있도록 허용합니다.
- 긴급 호출만 허용: 사용자가 장치에서 긴급 통화 전용 모드를 사용할 수 있도록 허용합니다.

- 펌웨어복구허용: 사용자가장치에서펌웨어를복구할수있도록허용합니다.
- 빠른암호화허용: 사용된메모리공간의암호화만허용합니다. 반대로, 전체디스크암호화는설정, 응용프로그램데이터, 다운로드한파일및응용프로그램, 미디어및기타파일을비롯한모든데이터를암호화합니다.
- **Common Criteria** 모드: 장치를 Common Criteria 모드로만듭니다. Common Criteria 구성은엄격한보안프로세스를적용합니다.
- 공장기본값으로재설정: 사용자가장치에서공장기본값으로재설정을수행할수있도록허용합니다.
- 날짜시간변경: 사용자가장치에서날짜및시간을변경할수있도록허용합니다.
- **DOD** 다시부팅배너: 사용자의장치가다시시작되면 DoD 에서승인시스템사용알림메시지또는배너를표시합니다.
- 설정변경사항: 사용자가장치에서설정을변경할수있도록허용합니다.
- 백업: 사용자가장치에서응용프로그램및시스템데이터를백업할수있도록허용합니다.
- 무선업그레이드: 사용자의장치가무선으로소프트웨어업데이트를수신하도록허용합니다 (MDM 3.0 이상).
- 백그라운드데이터: 앱이백그라운드에서데이터를동기화하도록허용합니다.
- 카메라: 사용자가장치에서카메라를사용할수있도록허용합니다.
- 클립보드: 사용자가장치의클립보드에데이터를복사할수있도록허용합니다.
 - * 클립보드공유: 사용자가장치와컴퓨터간에서클립보드콘텐츠를공유할수있도록허용합니다 (MDM 4.0 이상).
- 홈키: 사용자가장치에서홈키를사용할수있도록허용합니다.
- 마이크: 사용자가장치에서마이크를사용할수있도록허용합니다.
- 모의위치: 사용자가 GPS 위치를조작할수있도록허용합니다.
- **NFC**: 사용자가장치에서 NFC(근거리통신) 를사용할수있도록허용합니다 (MDM 3.0 이상).
- 전원끄기: 사용자가장치를끌수있도록허용합니다 (MDM 3.0 이상).
- 스크린샷: 사용자가장치에서스크린샷을찍을수있도록허용합니다.
- **SD** 카드: 가능한경우사용자가장치에서 SD 카드를사용할수있도록허용합니다.
- 음성다이얼: 사용자가장치에서음성다이얼을사용할수있도록허용합니다 (MDM 4.0 이상).
- **SBeam**: 사용자가 NFC 및 Wi-Fi Direct 를사용하여다른사용자와콘텐츠를공유할수있도록허용합니다 (MDM 4.0 이상).
- **SVoice**: 사용자가장치에서지능형개인비서및지식탐색기를사용할수있도록허용합니다 (MDM 4.0 이상).
- 여러사용자허용: 여러사용자가장치를사용할수있습니다 (MDM 4.0 이상). 기본값은 꺼짐입니다.
- 앱허용
 - 브라우저: 사용자가웹브라우저를사용할수있도록허용합니다.
 - **Youtube**: 사용자가 YouTube 에액세스할수있도록허용합니다.
 - **Google Play/Marketplace**: 사용자가 Google Play 및 Google Apps Marketplace 에액세스할수있도록허용합니다.
 - **Google Play** 이외의앱허용: 사용자가 Google Play 및 Google Apps Marketplace 이외의사이트에서앱을다운로드할수있도록허용합니다. 켜짐인경우사용자가장치의보안설정을사용하여알수없는원본의앱을신뢰할수있습니다.
 - 시스템앱중지: 사용자가미리설치된시스템앱을비활성화할수있도록허용합니다 (MDM 4.0 이상).
 - 응용프로그램사용안함: 켜짐인경우 Samsung SAFE 장치에서지정된목록의앱이실행되지않도록차단합니다.
- 네트워크

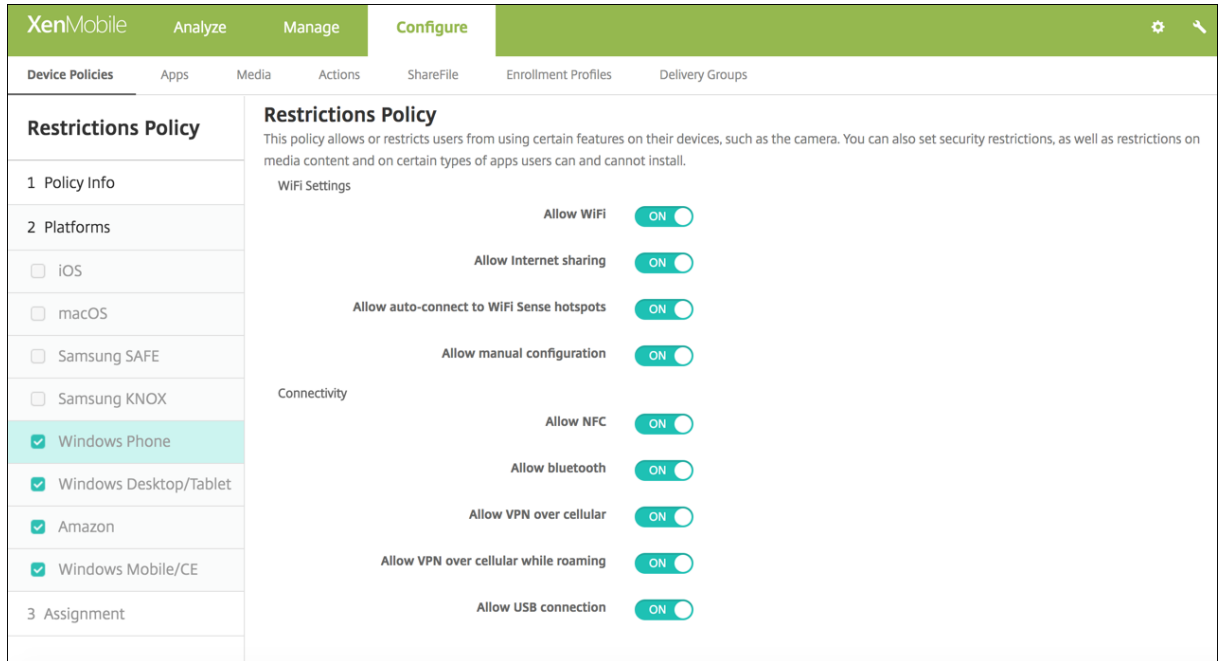
- 들어오는 **MMS**: 사용자가 MMS 메시지를받을수있도록허용합니다.
- 들어오는 **SMS**: 사용자가 SMS 메시지를받을수있도록허용합니다.
- 나가는 **MMS**: 사용자가 MMS 메시지를보낼수있도록허용합니다.
- 나가는 **SMS**: 사용자가 SMS 메시지를보낼수있도록허용합니다.
- 사용자추가프로필 **VPN**:
- **Bluetooth**: 사용자가 Bluetooth 를사용할수있도록허용합니다.
 - * 테더링: 사용자가 Bluetooth 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다.
- **WiFi**: 사용자가 WiFi 네트워크에연결할수있도록허용합니다.
 - * 테더링: 사용자가 WiFi 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다.
 - * 직접: 사용자가 WiFi 연결을통해다른장치에직접연결할수있도록허용합니다 (MDM 4.0 이상).
 - * 상태변경: 앱이 WiFi 연결상태를변경할수있도록허용합니다.
 - * 사용자정책변경사항: 사용자가 WiFi 정책을변경할수있도록허용합니다. 선택하지않은경우사용자는 WiFi 사용자이름및암호만변경할수있습니다. 선택한경우사용자가모든 WiFi 정책을변경할수있습니다.
- 테더링: 사용자가다른장치와모바일데이터연결을공유할수있도록허용합니다.
- 셀룰러데이터: 사용자가데이터에대해셀룰러연결을사용할수있도록허용합니다.
- 로밍허용: 로밍하는동안사용자가셀룰러데이터를사용할수있도록허용합니다. 기본값은사용자의장치에서로밍을비활성화하는꺼짐입니다.
- 보안통신만: 사용자가보안연결만사용할수있도록허용합니다 (MDM 4.0 이상).
- **Android Beam**: 사용자가 NFC 를사용하여장치의웹페이지, 사진, 비디오또는기타콘텐츠를다른장치로보낼수있도록허용합니다 (MDM 4.0 이상).
- 오디오녹음: 사용자가장치에서오디오를녹음할수있도록허용합니다 (MDM 4.0 이상).
- 비디오녹음: 사용자가장치에서비디오를녹음할수있도록허용합니다 (MDM 4.0 이상).
- 위치서비스: 사용자가장치에서 GPS 를결수있도록허용합니다.
- 일별제한 (**MB**): 사용자가하루에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
- 주별제한 (**MB**): 사용자가한주에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
- 월별제한 (**MB**): 사용자가한달에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
- **USB** 동작허용사용자의장치와컴퓨터간에서 USB 연결을허용합니다.
 - 디버깅: USB 를통한디버깅을허용합니다.
 - 호스트스토리지: USB 장치가연결될때사용자의장치가 USB 호스트로작동할수있도록허용합니다. 그러면사용자의장치가 USB 장치에전원을공급합니다.
 - 대용량스토리지: USB 연결을통해사용자의장치와컴퓨터간에서대용량데이터파일을전송하도록허용합니다.
 - **Kies** 미디어플레이어: 사용자가 Samsung Kies 도구를사용하여장치와컴퓨터간에서파일을동기화할수있도록허용합니다.
 - 테더링: 사용자가 USB 연결을통해다른장치와모바일데이터연결을공유할수있도록허용합니다.

Samsung KNOX 설정

이러한 옵션은 Samsung KNOX Premium(KNOX 2.0) 에서만 사용할 수 있습니다.

- **카메라 사용 허용:** 사용자가 장치에서 카메라를 사용할 수 있도록 허용합니다.
- **해지 확인 허용:** 해지된 인증서를 확인하도록 설정합니다.
- **앱 컨테이너 이동:** 사용자가 KNOX 컨테이너와 장치의 개인 영역 간에 앱을 이동할 수 있도록 허용합니다.
- **다중 단계 인증 적용:** 사용자는 지문과 함께 암호 또는 PIN 과 같은 다른 인증 방법을 사용하여 장치를 열어야 합니다.
- **TIMA 키 저장소 사용:** TIMA 키 저장소는 대칭 키에 대한 TrustZone 기반의 보안 키 저장소를 제공합니다. RSA 키 쌍 및 인증서는 저장을 위해 기본 키 저장소 공급자로 라우팅됩니다.
- **컨테이너에 대한 인증 적용:** 장치의 잠금을 해제할 때 사용한 KNOX 컨테이너를 열려면 별도의 다른 인증을 사용하십시오.
- **공유 목록:** 사용자가 공유 방법 목록의 앱 간에 콘텐츠를 공유할 수 있도록 허용합니다.
- **감사 로그 사용:** 장치의 법의학 분석을 위한 이벤트 감사 로그만들기를 사용하도록 설정합니다.
- **보안 키패드 사용:** 사용자가 KNOX 컨테이너 내부의 보안 키보드를 사용하도록 강제합니다.
- **Google 앱 사용:** 사용자가 Google 모바일 서비스에서 KNOX 컨테이너로 앱을 다운로드할 수 있도록 허용합니다.
- **인증 스마트카드 브라우저:** 스마트카드 판독기가 탑재된 장치에서 브라우저 인증을 사용하도록 설정합니다.

Windows Phone 및 Windows 데스크톱/태블릿설정



• WiFi 설정

- **WiFi 허용:** 장치가 WiFi 네트워크에 연결할 수 있도록 허용합니다. Windows Phone에만 해당합니다.
- **인터넷 공유 허용:** 장치가 WiFi 핫스팟으로 전환되어 다른 장치와 인터넷 연결을 공유할 수 있도록 허용합니다.
- **WiFi 감지 핫스팟에 자동 연결 허용:** 장치가 WiFi Sense 핫스팟에 자동으로 연결할 수 있도록 허용합니다. 이 옵션이 작동하려면 위치 서비스를 사용하도록 설정해야 합니다. WiFi Sense에 대한 자세한 내용은 [Windows Phone WiFi Sense FAQ](#)를 참조하십시오.
- **수동 구성 허용:** 사용자가 WiFi 연결을 수동으로 구성할 수 있도록 허용합니다. Windows Phone에만 해당합니다.

• 연결

- **NFC 허용:** 장치가 NFC(근거리 통신) 태그 또는 다른 NFC 지원 전송 장치와 통신할 수 있도록 허용합니다. Windows Phone에만 해당합니다.
- **Bluetooth 허용:** 장치가 Bluetooth를 통해 연결할 수 있도록 허용합니다. Windows Phone에만 해당합니다.
- **셀룰러를 통한 VPN 허용:** 장치가 VPN을 통해 셀룰러 네트워크에 연결할 수 있도록 허용합니다.
- **로밍하는 동안 셀룰러를 통한 VPN 허용:** 장치가 셀룰러 네트워크를 통해 로밍할 때 장치가 VPN을 통해 연결할 수 있도록 허용합니다.
- **USB 연결 허용:** 데스크톱이 USB 연결을 통해 장치의 저장소에 액세스할 수 있도록 허용합니다. Windows Phone에만 해당합니다.
- **셀룰러 데이터 로밍 허용:** 로밍하는 동안 사용자가 셀룰러 데이터를 사용할 수 있도록 허용합니다.

• 계정

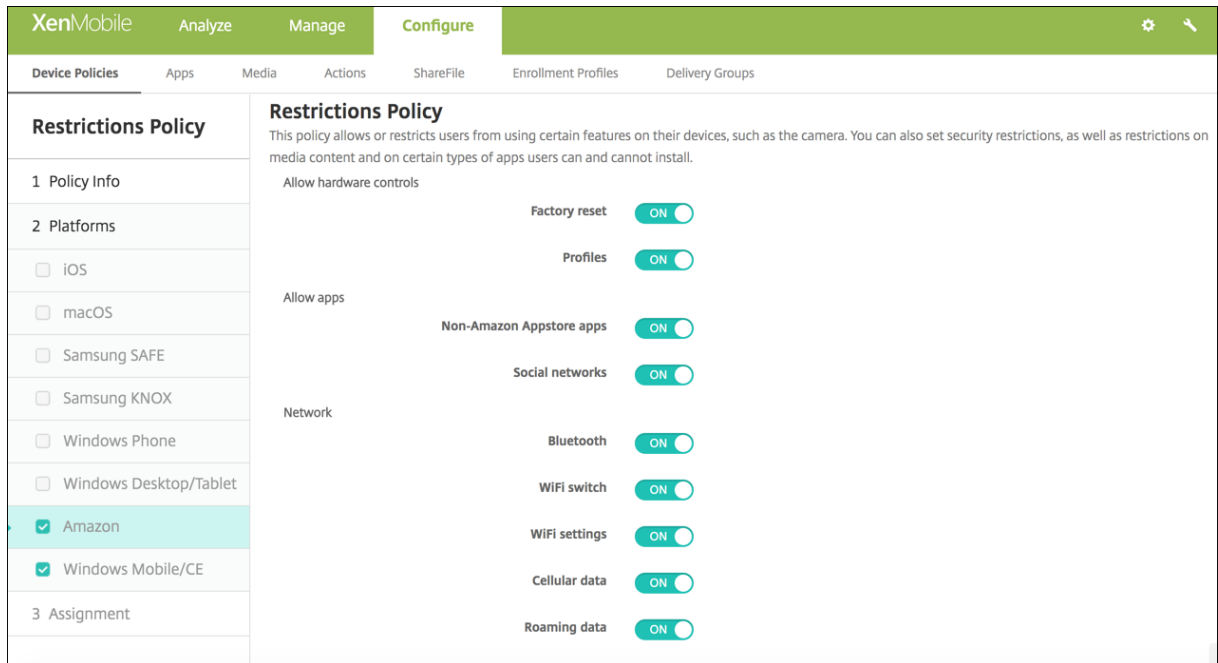
- **Microsoft 계정 연결 허용:** 장치가 전자 메일과 관련이 없는 연결 인증 및 서비스에 대해 Microsoft 계정을 사용할 수 있도록 허용합니다.
- **Microsoft 이외의 전자 메일 허용:** 사용자가 Microsoft 이외의 전자 메일 계정을 추가할 수 있도록 허용합니다.

- 검색: Windows Phone에만 해당합니다.
 - 검색에서 위치를 사용하도록 허용: 검색에서 장치의 위치 서비스를 사용할 수 있도록 허용합니다.
 - 성인 콘텐츠 필터링: 성인 콘텐츠를 허용합니다. 기본값은 성인 콘텐츠를 필터링하지 않는 꺼짐입니다.
 - **Bing Vision** 에서 이미지를 저장하도록 허용: Bing Vision 검색을 수행할 때 Bing Vision 이 캡처한 이미지를 저장할 수 있도록 허용합니다.
- 시스템
 - 스토리지 카드 허용: 장치가 스토리지 카드를 사용할 수 있도록 허용합니다.
 - 원격 분석: 목록에서 옵션을 클릭하여 장치가 원격 분석 정보를 보내는 것을 허용하거나 제한합니다. 기본값은 허용입니다. 다른 옵션은 허용 안 함 및 허용, 보조 데이터 요청 제외입니다.
 - 위치 서비스 허용: 위치 서비스를 허용합니다.
 - 내부 빌드에 대한 미리 보기 허용: 사용자가 Microsoft 내부 빌드를 미리 볼 수 있도록 허용합니다.
- 카메라: Windows 데스크톱/태블릿에만 해당합니다.
 - 카메라 사용 허용: 사용자가 장치의 카메라를 사용할 수 있도록 허용합니다.
- **Bluetooth**: Windows 데스크톱/태블릿에만 해당합니다.
 - 검색 가능 모드 허용: Bluetooth 장치가 로컬 장치를 찾을 수 있도록 허용합니다.
 - 로컬 장치 이름: 로컬 장치의 이름입니다.
- 보안: Windows Phone에만 해당합니다.
 - 수동 루트 인증서 설치 허용: 사용자가 루트 인증서를 수동으로 설치하도록 허용합니다.
 - 장치 암호화 필요: 장치 암호화를 요구합니다. 장치에서 암호화를 사용하도록 설정한 후에는 다시 사용하지 않도록 설정할 수 없습니다. 기본값은 꺼짐입니다.
 - 복사 및 붙여넣기 허용: 사용자가 장치에서 데이터를 복사하여 붙여넣을 수 있도록 허용합니다.
 - 화면 캡처 허용: 사용자가 장치에서 화면 캡처를 만들 수 있도록 허용합니다.
 - 음성 녹음 허용: 사용자가 장치에서 음성 녹음을 사용할 수 있도록 허용합니다.
 - **Office** 파일을 다른 이름으로 저장하도록 허용: 사용자가 다른 이름으로 저장을 사용하여 Office 파일을 저장할 수 있도록 허용합니다.
 - 관리 센터 알림 허용: 장치 잠금 화면에 관리 센터 알림을 허용합니다.
 - **Cortana** 허용: 사용자가 지능형 개인 비서 및 지식 탐색기인 Cortana 에 액세스할 수 있도록 허용합니다.
 - 장치 설정 동기화 허용: 로밍 중에 사용자가 Windows Phone 8.1 장치 간에 설정을 동기화할 수 있도록 허용합니다.
- 환경: Windows 데스크톱/태블릿에만 해당합니다.
 - **Cortana** 허용: 사용자가 지능형 개인 비서 및 지식 탐색기인 Cortana 에 액세스할 수 있도록 허용합니다.
 - 장치 검색 허용: 네트워크를 통한 장치 검색을 허용합니다.
 - **MDM** 수동 등록 해제 허용: 사용자가 수동으로 XenMobile MDM 에서 장치의 등록을 해제할 수 있도록 허용합니다.
 - 장치 설정 동기화 허용: 로밍 중에 사용자가 Windows 10 장치 간에 설정을 동기화할 수 있도록 허용합니다.
- 위쪽 잠금: Windows 데스크톱/태블릿에만 해당합니다.
 - 알림 허용: 잠금 화면에 알림 메시지를 허용합니다. Windows 데스크톱/태블릿에만 해당합니다.
- 앱
 - 스토어 액세스 허용: 사용자가 Microsoft Store 에 액세스할 수 있도록 허용합니다. Windows Phone에만 해당합니다.
 - 개발자 잠금 해제 허용: 사용자가 장치를 Microsoft 에 등록하고 Windows Phone 앱 스토어에 없는 앱을 개발하거나

나설치할수있도록허용합니다. Windows Phone 에만해당합니다.

- 웹브라우저액세스허용: 장치에서 Internet Explorer 를허용합니다. Windows Phone 에만해당합니다.
- 앱스토어자동업데이트허용: 앱스토어에서앱이자동으로업데이트되도록허용합니다. Windows 데스크톱/태블릿 에만해당합니다.
- 개인정보보호: Windows 데스크톱/태블릿에만해당합니다.
 - 개인설정입력허용: 입력개인설정서비스가실행되어사용자의입력내용에따라펜및터치키보드등의예측입력을개선 할수있도록허용합니다.
- 설정: Windows 데스크톱/태블릿에만해당합니다.
 - 자동재생허용: 사용자가자동재생설정을변경할수있도록허용합니다.
 - 데이터센스허용: 사용자가데이터센스설정을변경할수있도록허용합니다.
 - 날짜/시간허용: 사용자가날짜및시간설정을변경할수있도록허용합니다.
 - 언어허용: 사용자가언어설정을변경할수있도록허용합니다.
 - 절전모드허용: 사용자가전원및절전모드설정을변경할수있도록허용합니다.
 - 지역허용: 사용자가지역설정을변경할수있도록허용합니다.
 - 로그인옵션허용: 사용자가로그인설정을변경할수있도록허용합니다.
 - 회사허용: 사용자가회사설정을변경할수있도록허용합니다.
 - 사용자계정허용: 사용자가계정설정을변경할수있도록허용합니다.

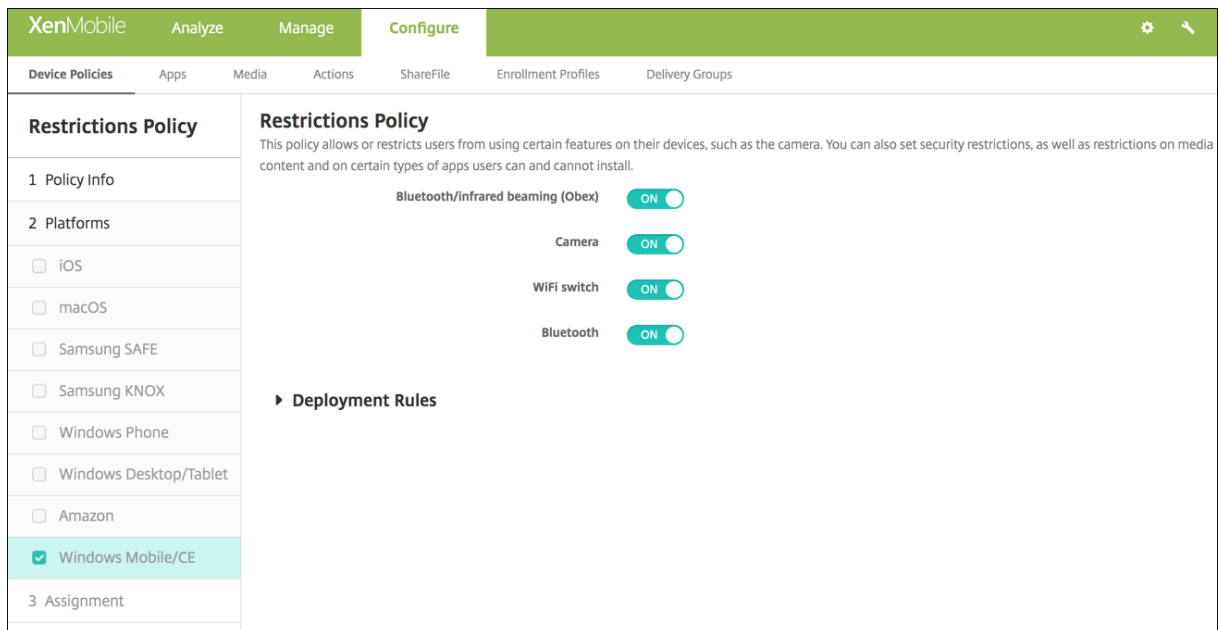
Amazon 설정



- 하드웨어제어허용
 - 공장기본값으로재설정: 사용자가장치에서공장기본값으로재설정을수행할수있도록허용합니다.
 - 프로필: 사용자가장치의하드웨어프로필을변경할수있도록허용합니다.
- 앱허용

- **Amazon Appstore** 이외의앱: 사용자가 Amazon Appstore 이외의앱을장치에설치할수있도록허용합니다.
- 소셜네트워크: 사용자가장치에서소셜네트워크에액세스할수있도록허용합니다.
- 네트워크
 - **Bluetooth**: 사용자가 Bluetooth 를사용할수있도록허용합니다.
 - **WiFi 전환**: 앱이 WiFi 연결상태를변경할수있도록허용합니다.
 - **WiFi 설정**: 사용자가 WiFi 설정을변경할수있도록허용합니다.
 - 셀룰러데이터: 사용자가데이터에대해셀룰러연결을사용할수있도록허용합니다.
 - 데이터로밍: 로밍하는동안사용자가셀룰러데이터를사용할수있도록허용합니다.
 - 위치서비스: 사용자가 GPS 를사용할수있도록허용합니다.
- **USB 동작**:
 - 디버깅: 사용자의장치가디버깅을위해 USB 를통해컴퓨터에연결할수있도록허용합니다.

Windows Mobile/CE 설정



- **Bluetooth/적외선빔 (Obex)**: Bluetooth 또는적외선기반 OBEX(Object EXchange 프로토콜) 를사용하여장치간에서데이터를교환할수있습니다.
- 카메라: 사용자장치에서카메라를사용하도록설정합니다.
- **WiFi 전환**: 사용자가 WiFi 네트워크를전환할수있도록허용합니다.
- **Bluetooth**: 사용자의장치에서 Bluetooth 를사용하도록설정합니다.

로밍장치정책

January 6, 2020

사용자의 iOS 및 Windows Mobile/CE 장치에서 음성 및 데이터 로밍을 허용할 것인지 여부를 구성하는 장치 정책을 XenMobile에서 추가할 수 있습니다. 음성 로밍을 사용하지 않도록 설정하면 데이터 로밍이 자동으로 비활성화됩니다. iOS의 경우 iOS 5.0 이상의 장치에서만 이 정책을 사용할 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

- 음성 로밍 사용 안 함: 음성 로밍을 사용하지 않을 것인지 여부를 선택합니다. 이 옵션을 사용하도록 설정하면 데이터 로밍이 자동으로 비활성화됩니다. 기본값은 꺼짐, 즉 음성 로밍을 사용하는 것입니다.
- 데이터 로밍 사용 안 함: 데이터 로밍을 사용하지 않을 것인지 여부를 선택합니다. 이 옵션은 음성 로밍이 활성화된 경우에만 사용할 수 있습니다. 기본값은 꺼짐, 즉 데이터 로밍을 사용하는 것입니다.

Windows Mobile/CE 설정

- 로밍하는 동안
 - 주문형 연결만 사용: 사용자가 장치에서 수동으로 연결을 트리거하거나 모바일 응용 프로그램이 강제 연결을 요청 (예: Exchange Server가 그렇게 설정된 경우 푸시 메일 요청) 하는 경우에만 XenMobile에 연결합니다. 이 옵션을 선택하면 기본 장치 연결 일정 정책을 일시적으로 사용할 수 없습니다.
 - **XenMobile**이 관리하는 연결을 제외한 모든 셀룰러 연결 차단: XenMobile 응용 프로그램 터널 또는 다른 XenMobile 장치 관리 작업에서 공식적으로 선언된 데이터 트래픽을 제외하고 다른 데이터는 장치에서 보내거나 받지 않습니다. 예를 들어, 이 옵션을 선택하면 장치의 웹 브라우저를 통한 모든 인터넷 연결을 사용할 수 없습니다.
 - **XenMobile**이 관리하는 모든 셀룰러 연결 차단: XenMobile 터널을 통해 전송되는 모든 응용 프로그램 데이터 (XenMobile Remote Support 포함)가 차단됩니다. 하지만 순수한 장치 관리와 관련된 데이터 트래픽은 차단되지 않습니다.
 - **XenMobile**에 대한 모든 셀룰러 연결 차단: 이 경우 장치가 USB, WiFi 또는 해당 기본 이동통신사업자 셀룰러 네트워크를 통해 다시 연결될 때까지 장치와 XenMobile 간에 트래픽이 전송되지 않습니다.
- 국내 로밍하는 동안
 - 국내 로밍 무시: 사용자가 국내 로밍하는 동안 데이터가 차단되지 않습니다.

Samsung MDM 라이선스 키 장치 정책

January 6, 2020

SAFE 정책 및 제한 사항을 배포하기 전에 장치에 배포해야 하는 기본 제공 Samsung ELM(엔터프라이즈 라이선스 관리) 키를 지정합니다. XenMobile은 Samsung E-FOTA(Enterprise Firmware-Over-The-Air) 서비스도 지원합니다. XenMobile은 SAFE(Samsung for Enterprise)와 Samsung KNOX 정책을 모두 지원하고 확장합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

Samsung SAFE 설정

- **ELM** 라이선스키: XenMobile 은 ELM 라이선스키를 생성하는 매크로로 이 필드를 미리 채웁니다. 필드가 비어있는 경우 매크로 `#{elm.license.key}` 를 입력합니다.

Samsung E-FOTA 설정구성

E-FOTA 정책을 구성하려면:

1. Samsung 에서 받은 키 및 라이선스 정보를 사용하여 Samsung MDM 라이선스키 장치 정책을 만듭니다. 그러면 XenMobile Server 가 정보의 유효성을 확인하고 정보를 등록합니다.

ELM 라이선스키를 입력합니다. XenMobile 은 ELM 라이선스키를 생성하는 매크로로 이 필드를 미리 채웁니다. 필드가 비어있는 경우 매크로 `#{elm.license.key}` 를 입력합니다.

E-FOTA 패키지를 구입할 때 Samsung 에서 제공한 다음 정보를 입력합니다.

- **Enterprise FOTA** 고객 ID
- **Enterprise FOTA** 라이선스
- 클라이언트 ID
- 클라이언트 암호

2. 필요한 경우 OS 업데이트 제어 장치 정책을 만듭니다.

- **Enable Enterprise FOTA(Enterprise FOTA 사용):** 커짐으로설정합니다.
- **Enterprise FOTA** 라이선스키: 1 단계에서만든 Samsung MDM 라이선스키정책이름을선택합니다.

3. OS 업데이트제어정책을 Secure Hub 에배포합니다.

Android Enterprise 및 Samsung KNOX 설정

The screenshot shows the configuration interface for a Samsung MDM License Key Policy. The left sidebar has sections for Policy Info, Platforms (with checkboxes for Samsung SAFE, Android Enterprise, and Samsung KNOX), and Assignment. The main area displays the policy name, a description, a text input field for the KNOX license key, and a Deployment Rules section.

- **KNOX** 라이선스키: Samsung 에서받은 KNOX 라이선스키를입력합니다.

Samsung SAFE 방화벽장치정책

January 6, 2020

이정책을사용하면 Samsung 장치에대한방화벽설정을구성할수있습니다. 허용하거나차단할 IP 주소, 포트및호스트이름을입력합니다. 프록시및프록시경로조정설정도구성할수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책>로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Samsung SAFE 설정

- 호스트허용/거부: 액세스를허용하거나거부할각호스트에대해 추가를클릭하고다음을구성합니다.
 - 호스트이름/IP 범위: 영향을줄사이트의호스트이름또는 IP 주소범위입니다.
 - 포트/포트범위: 포트또는포트범위입니다.
 - 허용/거부규칙필터: 화이트리스트를클릭하여사이트액세스를허용하거나 블랙리스트를클릭하여사이트액세스를거부합니다.
- 경로조정구성: 구성할각프록시에대해 추가를클릭하고다음을구성합니다.
 - 호스트이름/IP 범위: 프록시경로조정의호스트이름또는 IP 주소범위입니다.
 - 포트/포트범위: 프록시경로조정의포트또는포트범위입니다.
 - 프록시 IP: 프록시경로조정의프록시 IP 주소입니다.
 - 프록시포트: 프록시경로조정의프록시포트입니다.

- 프록시구성
 - 프록시 **IP**: 프록시서버의 IP 주소입니다.
 - 포트: 프록시서버포트입니다.

SCEP 장치정책

January 6, 2020

이정책을사용하면 SCEP(단순인증서등록프로토콜) 를사용하여외부 SCEP 서버에서인증서를검색하도록 iOS 및 macOS 장치를구성할수있습니다. XenMobile 에연결된 PKI 에서 SCEP 를사용하여장치에인증서를제공하려면분산모드에서 PKI 엔터티및 PKI 공급자를만들어야합니다. 자세한내용은 [PKI 엔터티](#)에서참조하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

The screenshot shows the 'SCEP Policy' configuration page in the XenMobile interface. The left sidebar has a 'SCEP Policy' section with sub-items: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' and 'macOS' are both checked. The main content area is titled 'SCEP Policy' and includes a description: 'This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.' Below this are several configuration fields:

- URL base ***: Text input field.
- Instance name ***: Text input field.
- Subject X.500 name (RFC 2253)**: Text input field.
- Subject alternative names type**: Dropdown menu set to 'None'.
- Maximum retries**: Text input field with value '3'.
- Retry delay**: Text input field with value '10'.
- Challenge password**: Text input field.
- Key size (bits)**: Dropdown menu set to '1024'.
- Use as digital signature**: Toggle switch set to 'OFF'.
- Use for key encipherment**: Toggle switch set to 'OFF'.
- SHA1/MD5 fingerprint (hexadecimal string)**: Text input field.

- **URL 기준**: HTTP 또는 HTTPS 를통해 SCEP 요청을전송할 SCEP 서버주소를입력합니다. 개인키는 CSR(인증서서명요청) 로전송되지않으므로요청을암호화되지않은상태로보내도안전할수있습니다. 그러나일회용암호를재사용하는것이 허용되므로 HTTPS 를사용하여암호를보호해야합니다. 이단계는필수단계입니다.
- **인스턴스이름**: SCEP 서버가인식하는문자열을입력합니다. 예를들어 **example.org** 와같은도메인이름을입력할수있습니다. CA 에여러 CA 인증서가있는경우이필드를사용하여필요한도메인을구분할수있습니다. 이단계는필수단계입니다.
- **주체 X.500 이름 (RFC 2253)**: OID(개체식별자) 및값배열로나타나는 X.500 이름의표현을입력합니다. 예를들어 /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 는 [[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”,

“bar”]] 로 변환될 수 있습니다. 국가 (C), 지역 (L), 시/도 (ST), 조직 (O), 조직구성단위 (OU) 및 일반이름 (CN) 에 대한 바가 포함된 점형식 문자로 OID 를 표현할 수 있습니다.

- 주체 대체 이름 유형: 목록에서 대체 이름 유형을 클릭합니다. SCEP 정책은 CA 의 인증서 발급에 필요한 값을 제공하는 선택적 대체 이름 유형을 지정할 수 있습니다. 없음, **RFC 822** 이름, **DNS** 이름 또는 **URI** 를 지정할 수 있습니다.
- 최대 재시도 횟수: SCEP 서버가 PENDING 응답을 보내는 경우 장치에서 재시도 횟수를 입력합니다. 기본값은 **3** 입니다.
- 재시도 지연: 다음 재시도 전에 대기할 시간을 초로 입력합니다. 첫 번째 재시도는 지연 없이 시도됩니다. 기본값은 **10** 입니다.
- 챌린지 암호: 미리 공유한 암호를 입력합니다.
- 키 크기 (비트): 목록에서 키 크기 (비트) 를 **1024** 또는 **2048** 중에서 클릭합니다. 기본값은 **1024** 입니다.
- 디지털 서명 사용: 인증서를 디지털 서명으로 사용할지 여부를 지정합니다. 인증서를 사용하여 디지털 서명을 확인하는 경우, 예를 들어 CA 에서 발급된 인증서인지 여부를 확인하는 경우 SCEP 서버가 공개 키를 사용하여 해독하기 전에 이 방식으로 인증서를 사용할 수 있는지 여부를 확인합니다.
- 키 암호화에 사용: 인증서를 키 암호화에 사용할지 여부를 지정합니다. 서버에서 클라이언트가 제공한 인증서의 공개 키를 사용하여 데이터가 개인 키를 사용하여 암호화되었는지 확인하는 경우 인증서를 키 암호화에 사용할 수 있는지 여부를 먼저 확인할 수 있습니다. 그렇지 않은 경우 작업에 실패합니다.
- **SHA1/MD5** 지문 (**16** 진수 문자열): CA 에서 HTTP 를 사용하는 경우 필드를 사용하여 CA 인증서 지문을 제공합니다. 이 지문은 등록 장치에서 CA 응답의 진위를 확인하는 데 사용됩니다. SHA1 또는 MD5 지문을 입력하거나 서명을 가져올 인증서를 선택할 수 있습니다.

macOS 설정

The screenshot shows the 'Configure' tab in XenMobile, specifically the 'SCEP Policy' configuration page. The sidebar on the left has 'SCEP Policy' selected, with sub-sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'macOS' is checked. The main configuration area includes the following fields:

- URL base ***: Text input field.
- Instance name ***: Text input field.
- Subject X.509 name (RFC 2253)**: Text input field.
- Subject alternative names type**: Dropdown menu set to 'None'.
- Maximum retries**: Text input field with value '3'.
- Retry delay**: Text input field with value '10'.
- Challenge password**: Text input field.
- Key size (bits)**: Dropdown menu set to '1024'.
- Use as digital signature**: Toggle switch set to 'OFF'.
- Use for key encipherment**: Toggle switch set to 'OFF'.
- SHA1/MD5 fingerprint (hexadecimal string)**: Text input field.

- **URL** 기준: HTTP 또는 HTTPS 를 통해 SCEP 요청을 전송할 SCEP 서버 주소를 입력합니다. 개인 키는 CSR(인증서 서명 요청) 로 전송되지 않으므로 요청을 암호화되지 않은 상태로 보내도 안전할 수 있습니다. 그러나 일회용 암호를 재사용하는 것이

허용되므로 HTTPS 를 사용하여 암호를 보호해야 합니다. 이 단계는 필수 단계입니다.

- 인스턴스 이름: SCEP 서버가 인식하는 문자열을 입력합니다. 예를 들어 example.org 와 같은 도메인 이름을 입력할 수 있습니다. CA 에 여러 CA 인증서가 있는 경우 이 필드를 사용하여 필요한 도메인을 구분할 수 있습니다. 이 단계는 필수 단계입니다.
- 주체 **X.500** 이름 (**RFC 2253**): OID(개체식별자) 및 값 배열로 나타나는 X.500 이름의 표현을 입력합니다. 예를 들어 /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 는 [[[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”, “bar”]]] 로 변환될 수 있습니다. 국가 (C), 지역 (L), 시/도 (ST), 조직 (O), 조직구성단위 (OU) 및 일반 이름 (CN) 에 대한 바로가기가 포함된 점형식 숫자로 OID 를 표현할 수 있습니다.
- 주체 대체 이름 유형: 목록에서 대체 이름 유형을 클릭합니다. SCEP 정책은 CA 의 인증서 발급에 필요한 값을 제공하는 선택적 대체 이름 유형을 지정할 수 있습니다. 없음, **RFC 822** 이름, **DNS** 이름 또는 **URI** 를 지정할 수 있습니다.
- 최대 재시도 횟수: SCEP 서버가 PENDING 응답을 보내는 경우 장치에서 재시도 횟수를 입력합니다. 기본값은 **3** 입니다.
- 재시도 지연: 다음 재시도 전에 대기할 시간을 초로 입력합니다. 첫 번째 재시도는 지연 없이 시도됩니다. 기본값은 **10** 입니다.
- 챌린지 암호: 미리 공유한 암호를 입력합니다.
- 키 크기 (비트): 목록에서 키 크기 (비트) 를 **1024** 또는 **2048** 중에서 클릭합니다. 기본값은 **1024** 입니다.
- 디지털 서명 사용: 인증서를 디지털 서명으로 사용할지 여부를 지정합니다. 인증서를 사용하여 디지털 서명을 확인하는 경우, 예를 들어 CA 에서 발급된 인증서인지 여부를 확인하는 경우 SCEP 서버가 공개 키를 사용하여 해독하기 전에 이 방식으로 인증서를 사용할 수 있는지 여부를 확인합니다.
- 키 암호화에 사용: 인증서를 키 암호화에 사용할지 여부를 지정합니다. 서버에서 클라이언트가 제공한 인증서의 공개 키를 사용하여 데이터가 개인 키를 사용하여 암호화되었는지 확인하는 경우 인증서를 키 암호화에 사용할 수 있는지 여부를 먼저 확인할 수 있습니다. 그렇지 않은 경우 작업에 실패합니다.
- **SHA1/MD5** 지문 (**16** 진수 문자열): CA 에서 HTTP 를 사용하는 경우 이 필드를 사용하여 CA 인증서 지문을 제공합니다. 이 지문은 등록 시 장치에서 CA 응답의 진위를 확인하는 데 사용됩니다. SHA1 또는 MD5 지문을 입력하거나 서명을 가져올 인증서를 선택할 수 있습니다.

Siri 및 받아쓰기 정책

April 11, 2019

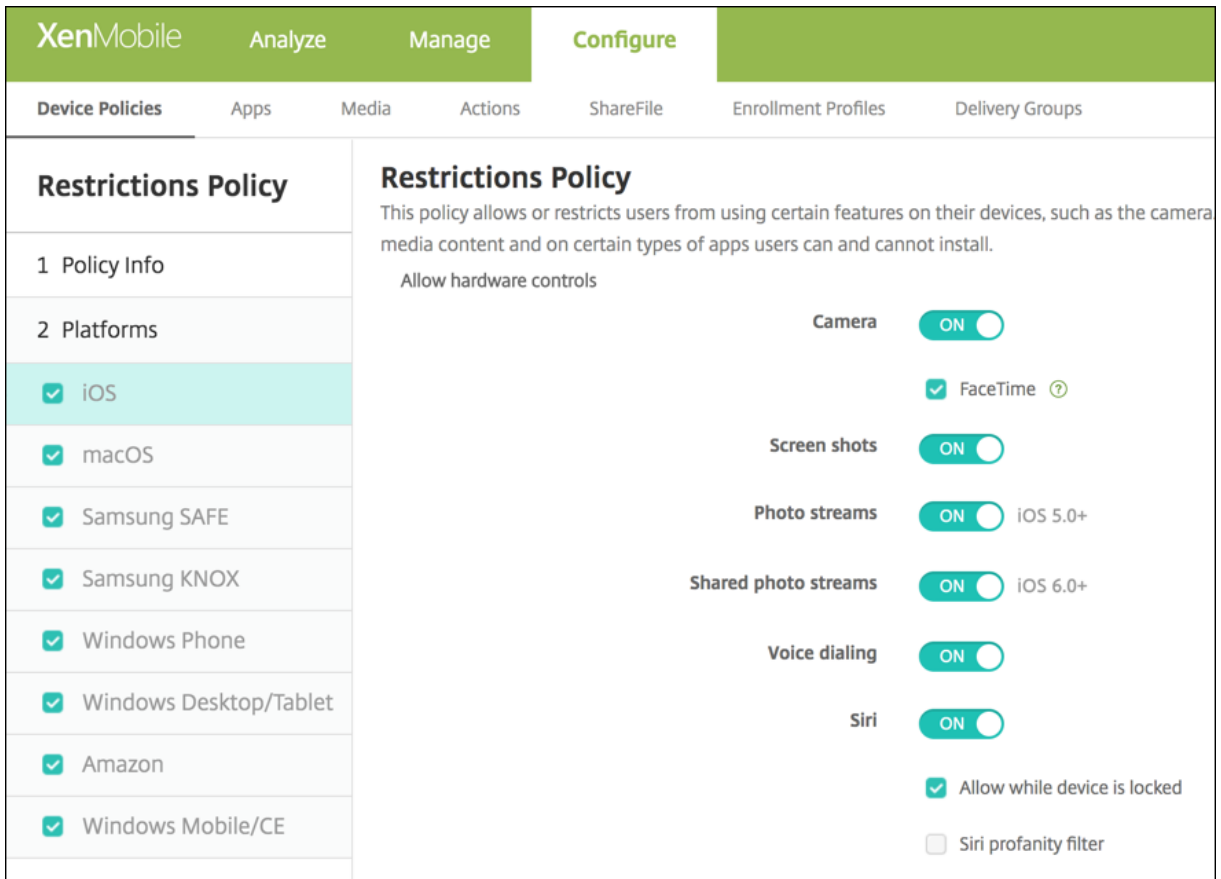
사용자가 Siri 에 무언가를 요청하거나 관리되는 iOS 장치에서 텍스트를 받아쓰면 Apple 이 Siri 를 개선하기 위해 음성 데이터를 수집합니다. 이 음성 데이터는 Apple 의 클라우드 기반 서비스를 통과하므로 보안 XenMobile 컨테이너 외부에 있게 됩니다. 그러나 받아쓰기 결과인 텍스트는 컨테이너 내에서 그대로 유지됩니다.

보안 요구에 따라 XenMobile 에서 Siri 및 받아쓰기 서비스를 차단할 수 있습니다.

MAM 배포에서 각 앱에 대한 받아쓰기 차단 정책은 기본적으로 켜져 있습니다. 즉, 장치의 마이크가 사용되지 않습니다. 받아쓰기를 허용하려면 이 정책을 꺼짐으로 설정합니다. 이 정책은 XenMobile 콘솔의 구성 > 앱에서 찾을 수 있습니다. 앱을 선택하고 편집을 클릭한 후 **iOS** 를 클릭합니다.

XenMobile		Analyze	Manage	Configure		
Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
MDX		App Restrictions				
1 App Information		Block camera <input checked="" type="checkbox"/> ON ?				
2 Platform		Block Photo Library <input checked="" type="checkbox"/> ON ?				
<input checked="" type="checkbox"/> iOS		Block mic record <input checked="" type="checkbox"/> ON ?				
<input type="checkbox"/> Android		Block dictation <input type="checkbox"/> OFF ?				
<input type="checkbox"/> Windows Phone		Block location services <input checked="" type="checkbox"/> ON ?				
<input type="checkbox"/> Windows Desktop/Tablet		Block SMS compose <input checked="" type="checkbox"/> ON ?				
3 Approvals (optional)						
4 Delivery Group Assignments (optional)						

또한 MDM 배포에서 구성 > 장치정책의 Siri 정책을 통해 Siri 를 사용하지 않도록 설정할 수 있습니다. Siri 사용은 기본적으로 허용됩니다.



Siri와 받아쓰기를 허용할지 여부를 결정할 때 주의해야 할 몇 가지 사항은 다음과 같습니다.

- Apple이 공개한 정보에 따르면 Apple은 Siri 및 받아쓰기 음성 클립 데이터를 최대 2년간 유지합니다. 이 데이터에는 사용자 연락처를 나타내는 무작위 값이 할당되며 이 무작위 번호에 음성 파일이 연결되어 있습니다. 자세한 내용은 이 문서에서 [Apple reveals how long Siri keeps your data \(Apple, Siri 사용자 데이터를 유지하는 기간 공개\)](#)를 참조하십시오.
- iOS 장치에서 설정 > 일반 > 키보드로 이동하고 받아쓰기 활성화 아래의 링크를 눌러 Apple의 개인정보 보호 정책을 검토할 수 있습니다.

SSO 계정 장치 정책

January 6, 2020

사용자가 다양한 앱에서 XenMobile 과회사내부 리소스에 액세스하기 위해 한 번만 로그인하도록 XenMobile에서 SSO(Single Sign-On) 계정을 만듭니다. 사용자가 장치에 자격 증명을 저장할 필요가 없습니다. App Store의 앱을 포함하여 앱 전반에 걸쳐 SSO 계정 엔터프라이즈 사용자 자격 증명 사용이 사용됩니다. 이 정책은 Kerberos 인증 백엔드와 함께 작동하도록 설계되었습니다.

이 정책은 iOS 7.0 이상에만 적용됩니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

- **계정이름:** 사용자의장치에나타나는 Kerberos SSO 계정이름을입력합니다. 이것은필수필드입니다.
- **Kerberos** 보안주체이름: Kerberos 보안주체이름을입력합니다. 이것은필수필드입니다.
- **ID** 자격증명 (키저장소또는 **PKI** 자격증명): 목록에서사용자상호작용없이 Kerberos 자격증명을갱신하는데사용할수 있는선택적인 ID 자격증명을클릭합니다.
- **Kerberos** 영역: 이정책의 Kerberos 영역을입력합니다. 일반적으로도메인이름은모두대문자입니다 (예: EXAMPLE.COM). 이것은필수필드입니다.
- 허용 **URL:** SSO 가필요한각 URL 에대해 추가를클릭한후다음을수행합니다.
 - 허용 **URL:** 사용자가 iOS 장치에서 URL 을방문할때 SSO 를요구할 URL 을입력합니다.
예를들어사용자가사이트를탐색하려고할때웹사이트가 Kerberos 챌린지를시작하는경우해당사이트가 URL 목록에없으면 iOS 장치는이전 Kerberos 로그인에서장치에캐시되었을수있는 Kerberos 토큰을제공하며 SSO 를시도하지않습니다. 일치항목은 URL 의호스트부분에서정확히일치해야합니다. 예를들어 <https://shopping.apple.com>은유효하지만 https://*.apple.com은유효하지않습니다. 또한호스트일치에따라 Kerberos 가활성화되지않는경우 URL 은여전히표준 HTTP 호출로대체됩니다. 이호출은 URL 이 Kerberos 를사용하는 SSO 에대해서만구성되어있는경우표준암호챌린지또는 HTTP 오류를포함한 거의모든수단을의미할수있습니다.
 - 추가를클릭하여 URL 을추가하거나 취소를클릭하여 URL 추가를취소합니다.
- **앱식별자:** 이로그인을사용하도록허용된각앱에대해 추가를클릭한후다음을수행합니다.
 - **앱식별자:** 이로그인을사용하도록허용된앱의앱식별자를입력합니다. 앱식별자를추가하지않으면이로그인은 모든 앱식별자와일치합니다.
 - 추가를클릭하여앱식별자를추가하거나 취소를클릭하여앱식별자추가를취소합니다.

스토리지암호화장치정책

January 6, 2020

XenMobile 에서스토리지암호화장치정책을만들어내부및외부스토리지를암호화하고장치에따라사용자로서로다른장치에서스토리카드를사용하지못하도록합니다.

Samsung SAFE, Windows Phone 및 Android Sony 장치에대해정책을만들수있습니다. 플랫폼마다서로다른값이필요합니다. 이에대해서는이문서에자세히설명되어있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

사전요구사항

Samsung SAFE 장치의경우이정책을구성하기전에다음요구사항을충족해야합니다.

- 사용자의장치에서화면잠금옵션을설정합니다.

- 사용자의장치를연결하고 80% 이상충전합니다.
- 장치에서숫자및문자또는기호를모두포함하는암호를요구하는지확인합니다.

Samsung SAFE 설정구성

- 내부스토리지암호화: 사용자장치의내부스토리지를암호화할것인지를선택합니다. 내부스토리지에는장치메모리와내부스
토리지가포함됩니다. 기본값은 켜짐입니다.
- 외부스토리지암호화: 사용자장치의외부스토리지를암호화할것인지를선택합니다. 기본값은 켜짐입니다.

Windows Phone 설정

- 장치암호화필요: 사용자장치를암호화할것인지를선택합니다. 기본값은 꺼짐입니다.
- 스토리지카드사용안함: 사용자가장치에서스토리지카드를사용하지못하게할지여부를선택합니다. 기본값은 꺼짐입니다.

Android Sony 설정구성

- 외부스토리지암호화: 사용자장치의외부스토리지를암호화할것인지를선택합니다. 장치에서숫자및문자또는기호를포함하
는암호를요구해야합니다. 기본값은 켜짐입니다.

스토어장치정책

January 6, 2020

iOS, Android 또는 Windows 태블릿 장치의 홈 화면에 XenMobile Store 웹클립을 표시할지 여부를 지정하는 정책을 XenMobile 에서 만들 수 있습니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

플랫폼 설정

구성하는 각 플랫폼에 대해 XenMobile Store 웹클립을 사용자 장치에 표시할지 여부를 선택합니다. 기본값은 켜짐입니다.

구독 캘린더 장치 정책

January 6, 2020

XenMobile 에장치정책을추가하여 iOS 장치에있는캘린더목록에구독캘린더를추가할수있습니다. 구독할수있는공개캘린더목록이 www.apple.com/downloads/macosx/calendars에나와있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

사전요구사항

사용자장치에있는구독캘린더목록에캘린더를추가하려면먼저캘린더를구독해야합니다.

iOS 설정

- **설명:** 캘린더의설명을입력합니다. 이것은필수필드입니다.
- **URL:** 캘린더 URL 을입력합니다. `webcal://` URL 또는 iCalendar 파일 (.ics) 에대한 `https://` 링크를입력할수있습니다. 이것은필수필드입니다.
- **사용자이름:** 사용자의로그온이름을입력합니다. 이것은필수필드입니다.
- **암호:** 선택적사용자암호를입력합니다.
- **SSL 사용:** 캘린더에대한 SSL 연결을사용할것인지여부를선택합니다. 기본값은 꺼짐입니다.

약관장치정책

January 6, 2020

사용자가회사네트워크에대한연결을통제하는회사의특정정책에동의하도록하려면 XenMobile 에서약관장치정책을만듭니다. 사용자가 XenMobile 에장치를등록할때약관이표시되며약관에동의해야만장치를등록할수있습니다. 약관에동의하지않으면등록프로세스가취소됩니다.

회사에다양한국가의사용자가있고사용자의모국어로약관에동의하게하려면약관에대한정책을여러언어로만들수있습니다. 배포하려는각플랫폼및언어조합에대한파일을제공해야합니다. Android 및 iOS 장치의경우 PDF 파일을제공해야합니다. Windows 장치의경우텍스트 (.txt) 파일및동반이미지파일을제공해야합니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 및 Android 설정

- **가져올파일:** 찾아보기를클릭하고파일의위치로이동하여가져올약관파일을선택합니다.
- **기본약관:** 이파일에서다른약관을사용하는여러그룹의구성원인사용자의기본문서인지여부를선택합니다. 기본값은 꺼짐입니다.

Windows Phone 및 Windows 태블릿설정

- **가져올파일:** 찾아보기를클릭하고파일의위치로이동하여가져올약관파일을선택합니다.
- **이미지:** 찾아보기를클릭하고파일위치로이동하여가져올이미지파일을선택합니다.
- **기본약관:** 이파일에서로다른약관을사용하는여러그룹의구성원인사용자의기본문서인지여부를선택합니다. 기본값은 꺼짐입니다.

VPN 장치정책

January 6, 2020

VPN 장치정책은사용자장치에서회사리소스에안전하게연결할수있게하는 VPN(가상사설망) 설정을구성합니다. 다음플랫폼에 대한 VPN 장치정책을구성할수있습니다. 플랫폼마다서로다른값이필요합니다. 이에대해서는이문서에자세히설명되어있습니다.

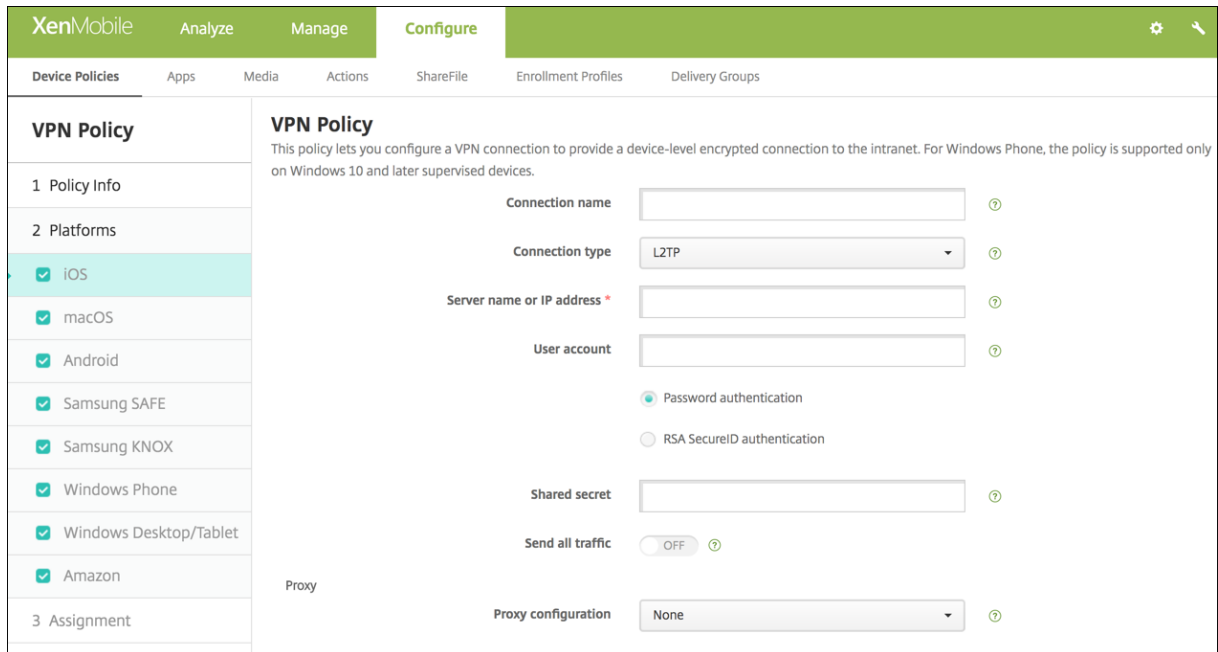
이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

iOS 12 로장치업그레이드를준비하려면:

iOS 용 VPN 장치정책의 Citrix VPN 연결유형은 iOS 12 를지원하지않습니다. 다음단계를수행하여기존 VPN 장치정책을삭제하고 Citrix SSO 연결유형으로 VPN 장치정책을만듭니다.

1. iOS 용 VPN 장치정책을삭제합니다.
2. iOS 용 VPN 장치정책을추가합니다. 중요설정:
 - 연결유형 = **Citrix SSO**
 - 앱별 VPN 사용 = 켜짐
 - 공급자유형 = 패킷터널
3. iOS 에대한앱특성장치정책을추가합니다. 앱별 VPN 식별자의경우 **iOS_VPN** 을선택합니다.



- **연결이름:** 연결이름을 입력합니다.
- **연결유형:** 목록에서 이 연결에 사용할 프로토콜을 선택합니다. 기본값은 **L2TP**입니다.
 - **L2TP:** 미리 공유한 키 인증을 사용하는 계층 2 터널링 프로토콜입니다.
 - **PPTP:** 지점간 터널링입니다.
 - **IPSec:** 회사 VPN 연결입니다.
 - **Cisco Legacy AnyConnect:** 이 연결 유형을 사용하려면 Cisco Legacy AnyConnect VPN 클라이언트가 사용자 장치에 설치되어 있어야 합니다. 이제는 사용되지 않는 VPN 프레임워크에 기반하는 Cisco Legacy AnyConnect 클라이언트는 단계적으로 중단됩니다. 자세한 내용은 지원 문서 <https://support.citrix.com/article/CTX227708>에서 참조하십시오.
 - 현재 Cisco AnyConnect 클라이언트를 사용하려면 연결 유형에서 사용자 지정 **SSL**을 선택합니다. 필요한 설정은 이 섹션에서 “사용자 지정 SSL 프로토콜 구성”을 참조하십시오.
 - **Juniper SSL:** Juniper Networks SSL VPN 클라이언트입니다.
 - **F5 SSL:** F5 Networks SSL VPN 클라이언트입니다.
 - **SonicWALL Mobile Connect:** iOS용 Dell 통합 VPN 클라이언트입니다.
 - **Ariba VIA:** Ariba Networks Virtual Internet Access 클라이언트입니다.
 - **IKEv2(iOS에만 해당):** iOS 전용 Internet Key Exchange 버전 2입니다.
 - **AlwaysOn IKEv2:** IKEv2를 사용하여 상시 액세스를 제공합니다.
 - **AlwaysOn IKEv2 이중구성:** IKEv2 이중 구성을 사용하여 상시 액세스를 제공합니다.
 - **Citrix SSO:** iOS 12 이상을 위한 Citrix SSO 클라이언트입니다.
 - 사용자 지정 **SSL:** 사용자 지정 Secure Socket Layer입니다. 이 연결 유형은 번들 ID가 **com.cisco.anyconnect**인 Cisco AnyConnect 클라이언트에 필요합니다. 연결 이름을 **Cisco AnyConnect**로 지정합니다. VPN 정책을 배포하고 iOS 장치에 대해 NAC(네트워크 액세스 제어) 필터를 사용하도록 설정할 수도 있습니다. 이 필터는 호환되지 않는 앱이 설치된 장치에 대한 VPN 연결을 차단합니다. 이 구성에는 다음 iOS 섹션에 설명된 대로 iOS VPN 정책에 대한 특정 설정이 필요합니다. NAC 필터를 사용하는 데 필요한 기타 설정에 대한 자세한 내용은 [네트워크 액세스 제](#)

어를참조하십시오.

다음섹션에는이전에설명한각연결유형에대한구성옵션이나열되어있습니다.

iOS 용 L2TP 프로토콜구성

- 서버이름또는 **IP 주소**: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 암호인증또는 **RSA SecurID** 인증을선택합니다.
- 공유암호: IPsec 공유암호키를입력합니다.
- 모든트래픽보내기: VPN 을통해모든트래픽을보낼지여부를선택합니다. 기본값은 꺼짐입니다.

iOS 용 PPTP 프로토콜구성

- 서버이름또는 **IP 주소**: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 암호인증또는 **RSA SecurID** 인증을선택합니다.
- 암호화수준: 목록에서암호화수준을선택합니다. 기본값은 없음입니다.
 - 없음: 암호화를사용하지않습니다.
 - 자동: 서버에서지원하는가장강력한암호화수준을사용합니다.
 - 최대 (**128 비트**): 항상 128 비트암호화를사용합니다.
- 모든트래픽보내기: VPN 을통해모든트래픽을보낼지여부를선택합니다. 기본값은 꺼짐입니다.

iOS 용 IPsec 프로토콜구성

- 서버이름또는 **IP 주소**: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 공유암호또는 인증서를선택합니다. 기본값은 공유암호입니다.
- 공유암호를사용하는경우다음설정을구성합니다.
 - 그룹이름: 선택적그룹이름을입력합니다.
 - 공유암호: 선택적공유암호키를입력합니다.
 - 하이브리드인증사용: 하이브리드인증을사용할지여부를선택합니다. 하이브리드인증을사용하면서버가먼저클라이언트에서자체인증된후클라이언트가서버에서자체인증됩니다. 기본값은 꺼짐입니다.
 - 암호확인: 사용자가네트워크에연결할때암호확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
- 인증서를사용하는경우다음설정을구성합니다.
 - ID 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 을입력하도록할지여부를선택합니다. 기본값은 꺼짐입니다.

- 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다. 기본값은 꺼짐입니다.
- **Safari** 도메인: 추가를클릭하여 Safari 도메인이름을추가합니다.

iOS 용 Cisco Legacy AnyConnect 프로토콜구성

Cisco Legacy AnyConnect 클라이언트에서새로운 Cisco AnyConnect 클라이언트로전환하려면사용자지정 SSL 프로토콜을사용합니다.

- 공급자번들식별자: Legacy AnyConnect 클라이언트의번들 ID 는 com.cisco.anyconnect.gui 입니다.
- 서버이름또는 IP 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 그룹: 선택적그룹이름을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * ID 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 PIN 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을사용하는경우다음설정을구성합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다. 기본값은 꺼짐입니다.
 - 공급자유형: 앱별 VPN 을 앱프록시로제공할지, 아니면 패킷터널로제공할지를선택합니다. 기본값은 앱프록시입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

iOS 용 Juniper SSL 프로토콜구성

- 공급자변들식별자: **앱별 VPN** 프로필에앱의변들식별자와동일한유형의여러 VPN 공급자가포함되는경우여기서사용할 공급자를지정합니다.
- 서버이름또는 **IP 주소**: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 영역: 선택적영역이름을입력합니다.
- 역할: 선택적역할이름을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * **ID 자격증명**: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은iOS 용주문형 VPN 사용설정구성을참조하십시오.
- **앱별 VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을사용하는경우다음설정을구성합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다. 기본값은 꺼짐입니다.
 - 공급자유형: 앱별 VPN 을 앱프로시로제공할지, 아니면 패킷터널로제공할지를선택합니다. 기본값은 앱프로시입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

iOS 용 F5 SSL 프로토콜구성

- 공급자변들식별자: **앱별 VPN** 프로필에앱의변들식별자와동일한유형의여러 VPN 공급자가포함되는경우여기서사용할 공급자를지정합니다.
- 서버이름또는 **IP 주소**: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.

- * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 꺼짐인경우설정구성에대한자세한내용은iOS 용주문형 VPN 사용설정구성을참조하십시오.
- **앱별 VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을사용하는경우다음설정을구성합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다.
 - 공급자유형: 앱별 VPN 을 앱프록시로제공할지, 아니면 패킷터널로제공할지를선택합니다. 기본값은 앱프록시입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

iOS 용 SonicWALL 프로토콜구성

- 공급자변들식별자: 앱별 VPN 프로필에앱의변들식별자와동일한유형의여러 VPN 공급자가포함되는경우여기서사용할공급자를지정합니다.
- 서버이름또는 IP 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 로그온그룹또는도메인: 선택적로그온그룹또는도메인을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * ID 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 PIN 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 VPN 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 VPN 사용이 꺼짐인경우설정구성에대한자세한내용은iOS 용주문형 VPN 사용설정구성을참조하십시오.
- **앱별 VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을켜짐으로설정하는경우다음설정을구성합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다.
 - 공급자유형: 앱별 VPN 을 앱프록시로제공할지, 아니면 패킷터널로제공할지를선택합니다. 기본값은 앱프록시입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
 - * 도메인: 추가할도메인을입력합니다.

* 저장을 클릭하여도 도메인을 저장하거나 취소를 클릭하여도 도메인을 저장하지 않습니다.

iOS 용 Ariba VIA 프로토콜 구성

- 공급자 번들 식별자: 앱별 VPN 프로필에 앱의 번들 식별자와 동일한 유형의 여러 VPN 공급자가 포함되는 경우 여기서 사용할 공급자를 지정합니다.
- 서버 이름 또는 IP 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * ID 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 PIN 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 VPN 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 VPN 사용이 꺼짐인 경우 설정 구성에 대한 자세한 내용은 iOS 용 주문형 VPN 사용 설정 구성을 참조하십시오.
- 앱별 VPN 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - Safari 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * 도메인: 추가할 도메인을 입력합니다.
 - * 저장을 클릭하여도 도메인을 저장하거나 취소를 클릭하여도 도메인을 저장하지 않습니다.

iOS 용 IKEv2 프로토콜 구성

이 섹션에는 IKEv2, AlwaysOn IKEv2 및 AlwaysOn IKEv2 이중 구성 프로토콜에 사용되는 설정이 포함되어 있습니다. AlwaysOn IKEv2 이중 구성 프로토콜의 경우 셀룰러 및 Wi-Fi 네트워크에 대해 이러한 모든 설정을 구성합니다.

- 사용자가 자동 연결을 비활성화하도록 허용: AlwaysOn 프로토콜용입니다. 사용자가 자신의 장치에서 네트워크 자동 연결을 끌 수 있게 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 서버의 호스트 이름 또는 IP 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 로컬 식별자: IKEv2 클라이언트의 FQDN 또는 IP 주소입니다. 이것은 필수 필드입니다.
- 원격 식별자: VPN 서버의 FQDN 또는 IP 주소입니다. 이것은 필수 필드입니다.
- 컴퓨터 인증: 이 연결에 대한 인증 유형으로 공유 암호 또는 인증서를 선택합니다. 기본값은 공유 암호입니다.
 - 공유 암호를 선택하는 경우 선택적 공유 암호 키를 입력합니다.

- 인증서를선택하는경우사용할 **ID** 자격증명을선택합니다. 기본값은 없음입니다.
 - 확장인증사용: EAP(확장인증프로토콜) 를사용할지여부를선택합니다. 커짐을선택하는경우 사용자계정과 인증암호를입력합니다.
 - 데드피어감지간격: 피어장치에접속하여피어장치가연결가능한상태로유지되는지를확인할빈도를선택합니다. 기본값은 없음입니다. 옵션은다음과같습니다.
 - 없음: 데드피어감지를사용하지않습니다.
 - 낮음: 30 분마다피어에접속합니다.
 - 중간: 10 분마다피어에접속합니다.
 - 높음: 1 분마다피어에접속합니다.
 - 모바일및다중홈사용안함: 이기능을사용하지않도록설정할지여부를선택합니다.
 - **IPv4/IPv6** 내부서브넷특성사용: 이기능을사용하도록설정할지여부를선택합니다.
 - 리디렉션사용안함: 리디렉션을사용하지않도록설정할지여부를선택합니다.
 - 장치가절전상태일때 **NAT Keepalive** 사용: AlwaysOn 프로토콜용입니다. Keepalive 패킷에 IKEv2 연결에대한 NAT 매핑이유지됩니다. 칩은장치가활성상태일때이러한패킷을정기적인간격으로전송합니다. 이설정이켜짐인경우장치가절전상태일때도칩이 Keepalive 패킷을전송합니다. 기본간격은 Wi-Fi 를사용하면 20 초이고셀룰러를사용하면 110 초입니다. 간격은 NAT keepalive 간격매개변수를사용하여변경할수있습니다.
 - **NAT keepalive** 간격 (초): 기본값은 20 초입니다.
 - **PFS(Perfect Forward Secrecy)** 사용: 이기능을사용하도록설정할지여부를선택합니다.
 - **DNS** 서버 **IP** 주소: 선택사항입니다. DNS 서버 IP 주소문자열의목록입니다. 이러한 IP 주소에는 IPv4 주소및 IPv6 주소가혼합되어포함될수있습니다. 추가를클릭하여주소를입력합니다.
 - 도메인이름: 선택사항입니다. 터널의기본도메인입니다.
 - 검색도메인: 선택사항입니다. 단일레이블호스트이름을정규화하는데사용되는도메인문자열의목록입니다.
 - 추가일치도메인을확인자목록에추가합니다: 선택사항입니다. 보조일치도메인목록을확인자의검색도메인목록에추가할지 여부를결정합니다. 기본값은 켜짐입니다.
 - 보조일치도메인: 선택사항입니다. DNS 서버주소에포함된 DNS 확인자설정을사용할 DNS 쿼리를결정하는데사용되는도메인문자열목록입니다. 이키는특정도메인의호스트만터널의 DNS 확인자를사용하여확인되는분할 DNS 구성을생성합니다. 이목록의도메인중하나에포함되지않은호스트는시스템의기본확인자를사용하여확인됩니다.
- 이매개변수에빈문자열이포함된경우해당문자열이기본도메인입니다. 분할터널구성은이방법으로먼저모든 DNS 쿼리를직접 VPN DNS 서버로전달한후기본 DNS 서버로전달할수있습니다. VPN 터널이네트워크의기본경로인경우나열된 DNS 서버가기본확인자가됩니다. 이경우보조일치도메인목록이무시됩니다.
- **IKE SA** 매개변수및 하위 **SA** 매개변수. 각 SA(보안연결) 매개변수옵션에대해다음설정을구성합니다.
 - 암호화알고리즘: 목록에서사용할 IKE 암호화알고리즘을선택합니다. 기본값은 **3DES** 입니다.

- 무결성알고리즘: 목록에서 사용할 무결성알고리즘을 선택합니다. 기본값은 **SHA1-96** 입니다.
- **Diffie Hellman** 그룹: 목록에서 Diffie Hellman 그룹번호를 선택합니다. 기본값은 **2** 입니다.
- **IKE 수명 (분): SA 수명** (키다시지정간격) 을 나타내는 10 에서 1440 사이의 정수를 입력합니다. 기본값은 **1440** 분입니다.
- 서비스예외: **AlwaysOn** 프로토콜용입니다. 서비스예외는 **AlwaysOn VPN** 에서 제외되는 시스템 서비스입니다. 다음 서비스예외 설정을 구성합니다.
 - 음성사서함: 목록에서 음성사서함예외의 처리방법을 선택합니다. 기본값은 트래픽이 터널을 통해 전달되도록 허용입니다.
 - **AirPrint**: 목록에서 AirPrint 예외의 처리방법을 선택합니다. 기본값은 트래픽이 터널을 통해 전달되도록 허용입니다.
 - 종속 웹사이트의 트래픽이 **VPN** 터널외부로 전달되도록 허용: 사용자가 VPN 터널외부의 공용 핫스팟에 연결할 수 있게 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 모든 종속 네트워크 애플리케이션의 트래픽이 **VPN** 터널외부로 전달되도록 허용: VPN 터널외부에 있는 모든 핫스팟 네트워크 애플리케이션을 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 종속 네트워크 애플리케이션 식별자: 사용자 액세스가 허용되는 각 핫스팟 네트워크 애플리케이션 식별자에 대해 추가를 클릭하고 핫스팟 네트워크 애플리케이션 식별자를 입력합니다. 저장을 클릭하여 애플리케이션 식별자를 저장합니다.
- **앱별 VPN**. IKEv2 연결 유형에 대한 설정을 구성합니다.
 - **앱별 VPN** 사용: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 추가를 클릭하여 Safari 도메인 이름을 추가합니다.
- **프록시 구성**: 프록시 서버를 통해 VPN 연결을 라우팅하는 방법을 선택합니다. 기본값은 없음입니다.

iOS 용 Citrix SSO 프로토콜 구성

Citrix SSO 클라이언트는 Apple Store(<https://apps.apple.com/us/app/citrix-ss0/id1333396910>) 에서 제공됩니다.

- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.

- * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 꺼짐인경우설정구성에대한자세한내용은iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을켜짐으로설정하는경우다음설정을구성합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다.
 - 공급자유형: 앱별 VPN 을 앱프록시로제공할지, 아니면 패킷터널로제공할지를선택합니다. 기본값은 앱프록시입니다.
 - 공급자유형: 패킷터널로설정합니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.
- 사용자지정 **XML**: 추가할각사용자지정 XML 매개변수에대해 추가를클릭하고키/값쌍을지정합니다. 사용가능한매개변수는다음과같습니다.
 - **disableL3**: 시스템수준 VPN 을사용하지않습니다. 앱별 VPN 만허용합니다. 값이필요하지않습니다.
 - **useragent**: 이장치정책에 VPN 플러그인클라이언트를대상으로하는모든 Citrix Gateway 정책을연결합니다. 플러그인에서시작된요청의경우이키의 값이 VPN 플러그인에자동으로추가됩니다.

iOS 용사용자지정 SSL 프로토콜구성

Cisco Legacy AnyConnect 클라이언트에서 Cisco AnyConnect 클라이언트로전환하려면:

1. 사용자지정 SSL 프로토콜을사용하여 VPN 장치정책을구성합니다. 정책을 iOS 장치에배포합니다.
2. <https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>에서 Cisco AnyConnect 클라이언트를업로드하고앱을 XenMobile 에추가한다음 iOS 장치에앱을배포합니다.
3. iOS 장치에서이전 VPN 장치정책을제거합니다.

설정:

- 사용자지정 **SSL** 식별자 (역방향 **DNS** 형식): 번들식별자로설정합니다. Cisco AnyConnect 클라이언트의경우 **com.cisco.anyconnect** 를사용합니다.
- 공급자번들식별자: 사용자지정 **SSL** 식별자에서지정한앱에동일한유형 (앱프록시또는패킷터널) 의여러 VPN 공급자가있는경우이번들식별자를지정합니다. Cisco AnyConnect 클라이언트의경우 **com.cisco.anyconnect** 를사용합니다.
- 서버이름또는 **IP** 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.

- * **ID 자격증명:** 목록에서 사용할 ID 자격증명을 선택합니다. 기본값은 없음입니다.
- * **연결할 때 PIN 확인:** 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- * **주문형 VPN 사용:** 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 VPN 사용이 꺼짐인 경우 설정 구성에 대한 자세한 내용은 iOS 용 주문형 VPN 사용 설정 구성을 참조하십시오.
- **앱별 VPN 사용:** 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 꺼짐으로 설정하는 경우 다음 설정을 구성합니다.
 - **주문형 일치 앱 사용:** 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - **공급자 유형:** 공급자가 VPN 서비스인지 프록시 서비스인지를 나타내는 공급자 유형입니다. VPN 서비스의 경우 패킷 터널을 선택합니다. 프록시 서비스의 경우 앱 프록시를 선택합니다. Cisco AnyConnect 클라이언트의 경우 패킷 터널을 선택합니다.
 - **Safari 도메인:** 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **도메인:** 추가할 도메인을 입력합니다.
 - * **저장을 클릭하여도 도메인을 저장하거나 취소를 클릭하여도 도메인을 저장하지 않습니다.**
- **사용자 지정 XML:** 추가할 각 사용자 지정 XML 매개변수에 대해 추가를 클릭하고 다음을 수행합니다.
 - **매개변수 이름:** 추가할 매개변수의 이름을 입력합니다.
 - **값:** 매개변수 이름에 연결된 값을 입력합니다.
 - **저장을 클릭하여 매개변수를 저장하거나 취소를 클릭하여 매개변수를 저장하지 않습니다.**

NAC 를 지원하도록 VPN 장치 정책을 구성하려면

1. NAC 필터를 구성하려면 연결 유형이 사용자 지정 **SSL** 이어야 합니다.
2. **VPN** 의 연결 이름을 지정합니다.
3. 사용자 지정 **SSL** 식별자에는 **com.citrix.NetScalerGateway.ios.app** 를 입력합니다.
4. 공급자 번들 식별자에는 **com.citrix.NetScalerGateway.ios.app.vpnplugin** 을 입력합니다.

3 단계와 4 단계의 값은 NAC 필터링에 필요한 Citrix SSO 설치에서 가져옵니다. 인증 암호는 구성하지 않습니다. NAC 기능 사용에 대한 자세한 내용은 [네트워크 액세스 제어](#) 를 참조하십시오.

iOS 용 주문형 VPN 사용 옵션 구성

- **주문형 도메인:** 각 도메인과 사용자가 연결할 때 수행할 관련 작업에 대해 추가를 클릭하고 다음을 수행합니다.
- **도메인:** 추가할 도메인을 입력합니다.
- **동작:** 목록에서 가능한 동작 중 하나를 선택합니다.
 - **항상 설정:** 도메인에서 항상 VPN 연결이 트리거됩니다.
 - **설정 안 함:** 도메인에서 VPN 연결이 트리거되지 않습니다.

- 필요한 경우 설정: 도메인 이름 확인에 실패하는 경우 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버에서 도메인을 확인할 수 없거나 다른 서버로 리디렉션되거나 시간 초과되는 경우 발생합니다.
- 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
- 주문형 규칙
 - 동작: 목록에서 수행할 동작을 선택합니다. 기본값은 **EvaluateConnection** 입니다. 가능한 동작은 다음과 같습니다.
 - * 허용: 트리거 시 주문형 VPN 연결을 허용합니다.
 - * 연결: VPN 연결을 무조건 시작합니다.
 - * 연결 끊기: VPN 연결을 제거하고 규칙이 일치하지 않는 한 주문형 VPN 에 다시 연결하지 않습니다.
 - * **EvaluateConnection**: 각 연결에 대한 ActionParameters 배열을 평가합니다.
 - * 무시: 기존 VPN 연결을 유지하지만 규칙이 일치하지 않는 한 주문형 VPN 에 다시 연결하지 않습니다.
 - **DNSDomainMatch**: 장치의 검색도메인 목록과 일치할 수 있는 추가할 각 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **DNS 도메인**: 도메인 이름을 입력합니다. 와일드카드 "*" 접두사를 사용하여 여러 도메인을 일치할 수 있습니다. 예를 들어 *.example.com 은 mydomain.example.com, yourdomain.example.com 및 herdomain.example.com 과 일치합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
 - **DNSServerAddressMatch**: 네트워크의 지정된 DNS 서버와 일치할 수 있는 추가할 각 IP 주소에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **DNS 서버 주소**: 추가할 DNS 서버 주소를 입력합니다. 와일드카드 "*" 접미사를 사용하여 DNS 서버를 일치할 수 있습니다. 예를 들어 17. 는 클래스 A 서브넷의 모든 DNS 서버와 일치합니다.
 - * 저장을 클릭하여 DNS 서버 주소를 저장하거나 취소를 클릭하여 DNS 서버 주소를 저장하지 않습니다.
 - **InterfaceTypeMatch**: 목록에서 사용하는 기본 네트워크 인터페이스 하드웨어 유형을 선택합니다. 기본값은 지정되지 않음입니다. 가능한 값은 다음과 같습니다.
 - * 지정되지 않음: 모든 네트워크 인터페이스 하드웨어와 일치합니다. 이 옵션은 기본값입니다.
 - * 이더넷: 이더넷 네트워크 인터페이스 하드웨어만 일치합니다.
 - * **WiFi**: Wi-Fi 네트워크 인터페이스 하드웨어만 일치합니다.
 - * 셀룰러: 셀룰러 네트워크 인터페이스 하드웨어만 일치합니다.
 - **SSIDMatch**: 현재 네트워크와 일치할 추가할 각 SSID 에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **SSID**: 추가할 SSID 를 입력합니다. 네트워크가 Wi-Fi 네트워크가 아닌 경우 또는 SSID 가 표시되지 않는 경우 일치하지 않습니다. 모든 SSID 와 일치하려면 이 목록을 비워둡니다.
 - * 저장을 클릭하여 SSID 를 저장하거나 취소를 클릭하여 SSID 를 저장하지 않습니다.
 - **URLStringProbe**: 가져올 URL 을 입력합니다. 이 URL 을 리디렉션 없이 성공적으로 가져온 경우 이 규칙이 일치합니다.
 - **ActionParameters : Domains**: EvaluateConnection 이 검사하는 추가할 각 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - * 도메인: 추가할 도메인을 입력합니다.
 - * 저장을 클릭하여 도메인을 저장하거나 취소를 클릭하여 도메인을 저장하지 않습니다.
 - **ActionParameters : DomainAction**: 목록에서 지정된 **ActionParameters : Domains** 도메인에

대한 VPN 동작을선택합니다. 기본값은 **ConnectIfNeeded** 입니다. 가능한동작은다음과같습니다.

* **ConnectIfNeeded**: 도메인이름확인예실패하는경우도메인이 VPN 연결시도를트리거합니다. 실패는 DNS 서버에서도메인을확인할수없거나다른서버로리디렉션되거나시간초과되는경우발생합니다.

* **NeverConnect**: 도메인에서 VPN 연결이트리거되지않습니다.

- **ActionParameters : RequiredDNSServers**: 지정된도메인을확인할때사용할각 DNS 서버 IP 주소에 대해 추가를클릭하고다음을수행합니다.

* **DNS 서버: ActionParameters : DomainAction = ConnectIfNeeded** 인경우에만유효합니다. 추가할 DNS 서버를입력합니다. 이서버는장치의현재네트워크구성에포함된서버가아니어도됩니다. DNS 서버에연결할수없는경우 VPN 연결이대신설정됩니다. 이 DNS 서버는내부 DNS 서버또는신뢰할수 있는외부 DNS 서버여야합니다.

* 저장을클릭하여 DNS 서버를저장하거나 취소를클릭하여 DNS 서버를저장하지않습니다.

- **ActionParameters : RequiredURLStringProbe**: 필요한경우 GET 요청을사용하여검색할 HTTP 또는 HTTPS(기본설정) URL 을입력합니다. URL 의호스트이름을확인할수없거나서버에연결할수없거나서버가응답하지않는경우 VPN 연결이설정됩니다. **ActionParameters : DomainAction = ConnectIfNeeded** 인경우에만유효합니다.

- **OnDemandRules : XML** 콘텐츠: XML 구성주문형규칙을입력하거나복사후붙여넣습니다.

* 사전확인을클릭하여 XML 코드의유효성을검사합니다. XML 이올바른경우 **XML** 콘텐츠텍스트상자아래에올바른 XML 이녹색텍스트로표시됩니다. 올바르지않은경우오류를설명하는오류메시지가주황색텍스트로표시됩니다.

• 프록시

- 프록시구성: 목록에서프록시서버를통해 VPN 연결을라우팅하는방법을선택합니다. 기본값은 없음입니다.

* 수동을사용하는경우다음설정을구성합니다.

· 프록시서버의호스트이름또는 **IP 주소**: 프록시서버의호스트이름또는 IP 주소를입력합니다. 이것은필수필드입니다.

· 프록시서버용포트: 프록시서버포트번호를입력합니다. 이것은필수필드입니다.

· 사용자이름: 선택적프록시서버사용자이름을입력합니다.

· 암호: 선택적프록시서버암호를입력합니다.

* 자동을구성하는경우다음설정을구성합니다.

· 프록시서버 **URL**: 프록시서버의 URL 을입력합니다. 이것은필수필드입니다.

• 정책설정

- 정책설정의 정책제거옆에서 날짜선택또는 제거할때까지의기간 (시간) 을선택합니다.

- 날짜선택을선택하는경우달력을클릭하여제거할특정날짜를선택합니다.

- 사용자가정책을제거하도록허용목록에서 항상, 암호필요또는 안함을선택합니다.

- 암호필요를선택하는경우 제거암호옆에필요한암호를입력합니다.

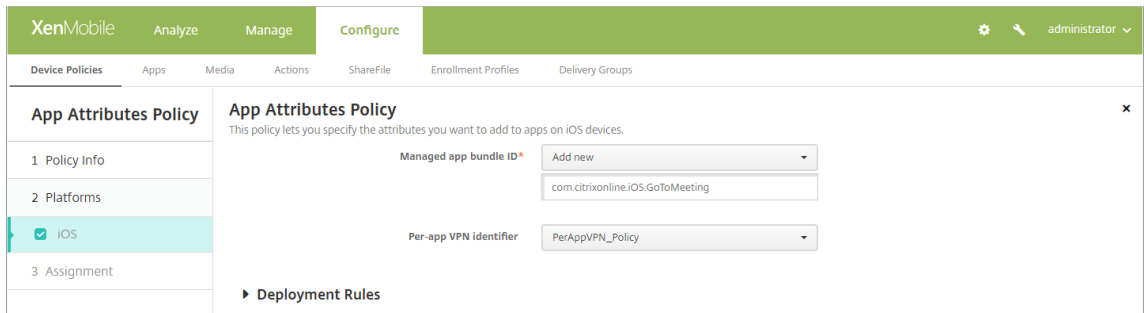
앱별 VPN 구성

iOS 에대한앱별 VPN 옵션은 Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Arriba VIA, Citrix VPN, Citrix SSO 및사용자지정 SSL 연결유형에사용할수있습니다.

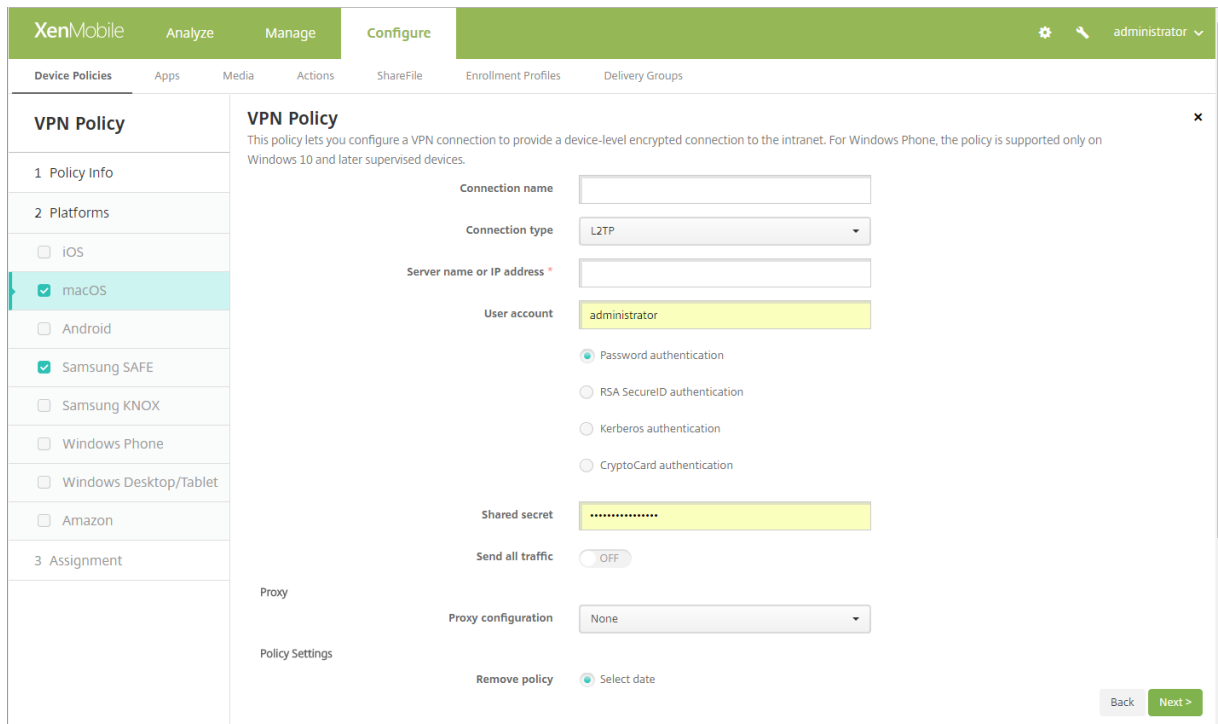
앱별 VPN 을구성하려면:

1. 구성 > 장치정책에서 VPN 정책을생성합니다. 예를들면다음과같습니다.

2. 구성 > 장치정책에서앱을앱별 VPN 정책에연결하는앱특성정책을생성합니다. 앱별 VPN 식별자에대해 1 단계에서생성한 VPN 정책의이름을선택합니다. 관리되는앱번들 ID 에대해앱목록에서선택하거나앱번들 ID 를입력합니다. (iOS 앱인벤토리정책을배포하는경우앱목록에앱이포함됩니다.)



macOS 설정



- **연결이름:** 연결이름을 입력합니다.
- **연결유형:** 목록에서 이 연결에 사용할 프로토콜을 선택합니다. 기본값은 L2TP입니다.
 - **L2TP:** 미리공유한키인증을사용하는계층 2 터널링프로토콜입니다.
 - **PPTP:** 지점간터널링입니다.
 - **IPSec:** 회사 VPN 연결입니다.
 - **Cisco AnyConnect:** Cisco AnyConnect VPN 클라이언트입니다.
 - **Juniper SSL:** Juniper Networks SSL VPN 클라이언트입니다.
 - **F5 SSL:** F5 Networks SSL VPN 클라이언트입니다.
 - **SonicWALL Mobile Connect:** iOS 용 Dell 통합 VPN 클라이언트입니다.
 - **Ariba VIA:** Ariba Networks Virtual Internet Access 클라이언트입니다.
 - **Citrix VPN:** Citrix VPN 클라이언트입니다.
 - 사용자지정 **SSL:** 사용자지정 Secure Socket Layer 입니다.

다음 섹션에는 이전에 설명한 각 연결 유형에 대한 구성 옵션이 나열되어 있습니다.

macOS 용 L2TP 프로토콜 구성

- 서버 이름 또는 **IP 주소**: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 암호 인증, **RSA SecurID** 인증, **Kerberos** 인증 또는 **CryptoCard** 인증을 선택합니다. 기본값은 암호 인증입니다.
- 공유 암호: IPsec 공유 암호 키를 입력합니다.
- 모든 트래픽 보내기: VPN 을 통해 모든 트래픽을 보낼지 여부를 선택합니다. 기본값은 꺼짐입니다.

macOS 용 PPTP 프로토콜 구성

- 서버 이름 또는 **IP 주소**: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 암호 인증, **RSA SecurID** 인증, **Kerberos** 인증 또는 **CryptoCard** 인증을 선택합니다. 기본값은 암호 인증입니다.
- 암호화 수준: 원하는 암호화 수준을 선택합니다. 기본값은 없음입니다.
 - 없음: 암호화를 사용하지 않습니다.
 - 자동: 서버에서 지원하는 가장 강력한 암호화 수준을 사용합니다.
 - 최대 (128 비트): 항상 128 비트 암호화를 사용합니다.
- 모든 트래픽 보내기: VPN 을 통해 모든 트래픽을 보낼지 여부를 선택합니다. 기본값은 꺼짐입니다.

macOS 용 IPsec 프로토콜 구성

- 서버 이름 또는 **IP 주소**: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
- 연결에 대한 인증 유형: 목록에서 이 연결에 대한 인증 유형으로 공유 암호 또는 인증서를 선택합니다. 기본값은 공유 암호입니다.
 - 공유 암호 인증을 사용하는 경우 다음 설정을 구성합니다.
 - * 그룹 이름: 선택적 그룹 이름을 입력합니다.
 - * 공유 암호: 선택적 공유 암호 키를 입력합니다.
 - * 하이브리드 인증 사용: 하이브리드 인증을 사용할지 여부를 선택합니다. 하이브리드 인증을 사용하면 서버가 먼저 클라이언트에서 자체 인증된 후 클라이언트가 서버에서 자체 인증됩니다. 기본값은 꺼짐입니다.
 - * 암호 확인: 사용자가 네트워크에 연결할 때 암호 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 인증서 인증을 사용하는 경우 다음 설정을 구성합니다.
 - * ID 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 PIN 확인: 사용자가 네트워크에 연결할 때 PIN 을 입력하도록 할지 여부를 선택합니다. 기본값은 꺼짐입니다.

- * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 꺼짐인경우설정구성에대한자세한내용은주문형 VPN 사용옵션구성을참조 하십시오.

macOS 용 Cisco AnyConnect 프로토콜구성

- 서버이름또는 **IP** 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 그룹: 선택적그룹이름을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 꺼짐인경우설정구성에대한자세한내용은주문형 VPN 사용옵션구성을참조 하십시오.
 - 앱별 **VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을사용하는경우다음설정을구성합니다.
 - * 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
 - 도메인: 추가할도메인을입력합니다.
 - 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

macOS 용 Juniper SSL 프로토콜구성

- 서버이름또는 **IP** 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 영역: 선택적영역이름을입력합니다.
- 역할: 선택적역할이름을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.

- * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은주문형 VPN 사용설정구성을참조 하십시오.
- **앱별 VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을사용하는경우다음설정을구성 합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할 지여부를선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수 행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

macOS 용 F5 SSL 프로토콜구성

- 서버이름또는 **IP** 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은주문형 VPN 사용설정구성을참조 하십시오.
- **앱별 VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을사용하는경우다음설정을구성 합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할 지여부를선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수 행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

macOS 용 SonicWALL Mobile Connect 프로토콜구성

- 서버이름또는 **IP** 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 로그온그룹또는도메인: 선택적로그온그룹또는도메인을입력합니다.

- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은주문형 VPN 사용설정구성을참조 하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을사용하는경우다음설정을구성 합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할 지여부를선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수 행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

macOS 용 Ariba VIA 프로토콜구성

- 서버이름또는 **IP** 주소: VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정: 선택적사용자계정을입력합니다.
- 연결에대한인증유형: 목록에서이연결에대한인증유형으로 암호또는 인증서를선택합니다. 기본값은 암호입니다.
 - 암호를사용하는경우 인증암호필드에선택적인증암호를입력합니다.
 - 인증서를사용하는경우다음설정을구성합니다.
 - * **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
 - * 연결할때 **PIN** 확인: 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은주문형 VPN 사용설정구성을참조 하십시오.
- 앱별 **VPN** 사용: 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 옵션을사용하는경우다음설정을구성 합니다.
 - 주문형일치앱사용: 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할 지여부를선택합니다. 기본값은 꺼짐입니다.
 - **Safari** 도메인: 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수 행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

macOS 용 사용자 지정 SSL 프로토콜 구성

- 사용자 지정 **SSL** 식별자 (역방향 **DNS** 형식): SSL 식별자를 역방향 DNS 형식으로 입력합니다. 이것은 필수 필드입니다.
- 서버 이름 또는 **IP** 주소: VPN 서버의 서버 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
- 사용자 계정: 선택적 사용자 계정을 입력합니다.
 - 연결에 대한 인증 유형: 목록에서 연결에 대한 인증 유형으로 암호 또는 인증서를 선택합니다. 기본값은 암호입니다.
 - 암호를 사용하는 경우 인증 암호 필드에 선택적 인증 암호를 입력합니다.
 - 인증서를 사용하는 경우 다음 설정을 구성합니다.
 - * **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
 - * 연결할 때 **PIN** 확인: 사용자가 네트워크에 연결할 때 PIN 확인 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - * 주문형 **VPN** 사용: 사용자가 네트워크에 연결할 때 VPN 연결 트리거를 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인 경우 설정 구성에 대한 자세한 내용은 주문형 VPN 사용 설정 구성을 참조하십시오.
 - 앱별 **VPN**: 앱별 VPN 을 사용할지 여부를 선택합니다. 기본값은 꺼짐입니다. 이 옵션을 사용하는 경우 다음 설정을 구성합니다.
 - * 주문형 일치 앱 사용: 앱별 VPN 서비스에 연결된 앱이 네트워크 통신을 시작할 때 앱별 VPN 연결을 자동으로 트리거할지 여부를 선택합니다.
 - * **Safari** 도메인: 포함하려는 앱별 VPN 연결을 트리거할 수 있는 각 Safari 도메인에 대해 추가를 클릭하고 다음을 수행합니다.
 - 도메인: 추가할 도메인을 입력합니다.
 - 저장을 클릭하여도메인을 저장하거나 취소를 클릭하여도메인을 저장하지 않습니다.
- 사용자 지정 **XML**: 추가할 각 사용자 지정 XML 매개변수에 대해 추가를 클릭하고 다음을 수행합니다.
 - 매개변수 이름: 추가할 매개변수의 이름을 입력합니다.
 - 값: 매개변수 이름에 연결된 값을 입력합니다.
 - 저장을 클릭하여도메인을 저장하거나 취소를 클릭하여도메인을 저장하지 않습니다.

주문형 VPN 사용 옵션 구성

- 주문형 도메인: 추가할 각 도메인 및 사용자가 도메인에 연결할 때 수행할 동작에 대해 추가를 클릭하고 다음을 수행합니다.
 - 도메인: 추가할 도메인을 입력합니다.
 - 동작: 목록에서 가능한 동작 중 하나를 선택합니다.
 - * 항상 설정: 도메인에서 항상 VPN 연결이 트리거됩니다.
 - * 설정 안함: 도메인에서 VPN 연결이 트리거되지 않습니다.
 - * 필요한 경우 설정: 도메인 이름 확인에 실패하는 경우 도메인이 VPN 연결 시도를 트리거합니다. 실패는 DNS 서버에서도 도메인을 확인할 수 없거나 다른 서버로 리디렉션되거나 시간 초과되는 경우 발생합니다.
 - 저장을 클릭하여도메인을 저장하거나 취소를 클릭하여도메인을 저장하지 않습니다.
- 주문형 규칙
 - 동작: 목록에서 수행할 동작을 선택합니다. 기본값은 **EvaluateConnection** 입니다. 가능한 동작은 다음과 같습니다.

- * 허용: 트리거시주문형 VPN 연결을허용합니다.
 - * 연결: VPN 연결을무조건시작합니다.
 - * 연결끊기: VPN 연결을제거하고규칙이일치하지않는한주문형 VPN 에다시연결하지않습니다.
 - * **EvaluateConnection**: 각연결에대한 **ActionParameters** 배열을평가합니다.
 - * 무시: 기존 VPN 연결을유지하지만규칙이일치하지않는한주문형 VPN 에다시연결하지않습니다.
- **DNSDomainMatch**: 사용자장치의검색도메인목록과일치할수있는추가할각도메인에대해 추가를클릭하고다음을수행합니다.
 - * **DNS** 도메인: 도메인이름을입력합니다. 와일드카드 "*" 접두사를사용하여여러도메인을일치할수있습니다. 예를들어 *.example.com 은 mydomain.example.com, yourdomain.example.com 및 herdomain.example.com 과일치합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.
 - **DNSServerAddressMatch**: 네트워크의지정된 DNS 서버와일치할수있는추가할각 IP 주소에대해 추가를클릭하고다음을수행합니다.
 - * **DNS** 서버주소: 추가할 DNS 서버주소를입력합니다. 와일드카드 "*" 접미사를사용하여 DNS 서버를일치할수있습니다. 예를들어 17. 는클래스 A 서브넷의모든 DNS 서버와일치합니다.
 - * 저장을클릭하여 DNS 서버주소를저장하거나 취소를클릭하여 DNS 서버주소를저장하지않습니다.
 - **InterfaceTypeMatch**: 목록에서사용하는기본네트워크인터페이스하드웨어유형을클릭합니다. 기본값은 지정되지않음입니다. 가능한값은다음과같습니다.
 - * 지정되지않음: 모든네트워크인터페이스하드웨어와일치합니다. 이 옵션은기본값입니다.
 - * 이더넷: 이더넷네트워크인터페이스하드웨어만일치합니다.
 - * **WiFi**: Wi-Fi 네트워크인터페이스하드웨어만일치합니다.
 - * 셀룰러: 셀룰러네트워크인터페이스하드웨어만일치합니다.
 - **SSIDMatch**: 현재네트워크와일치할추가할각 SSID 에대해 추가를클릭하고다음을수행합니다.
 - * **SSID**: 추가할 SSID 를입력합니다. 네트워크가 Wi-Fi 네트워크가아닌경우또는 SSID 가표시되지않는경우 일치가실패합니다. 모든 SSID 와일치하려면이목록을비워둡니다.
 - * 저장을클릭하여 SSID 를저장하거나 취소를클릭하여 SSID 를저장하지않습니다.
 - **URLStringProbe**: 가져올 URL 을입력합니다. 이 URL 을리디렉션없이성공적으로가져온경우이규칙이일치합니다.
 - **ActionParameters : Domains**: EvaluateConnection 이검사하는추가할각도메인에대해 추가를클릭하고다음을수행합니다.
 - * 도메인: 추가할도메인을입력합니다.
 - * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.
 - **ActionParameters : DomainAction**: 목록에서지정된 **ActionParameters : Domains** 도메인에 대한 VPN 동작을선택합니다. 기본값은 **ConnectIfNeeded** 입니다. 가능한동작은다음과같습니다.
 - * **ConnectIfNeeded**: 도메인이름확인에실패하는경우도메인이 VPN 연결시도를트리거합니다. 실패는 DNS 서버에서도메인을확인할수없거나다른서버로리디렉션되거나시간초과되는경우발생합니다.
 - * **NeverConnect**: 도메인에서 VPN 연결이트리거되지않습니다.
 - **ActionParameters : RequiredDNSServers**: 지정된도메인을확인할때사용할각 DNS 서버 IP 주소에 대해 추가를클릭하고다음을수행합니다.

* **DNS 서버: ActionParameters : DomainAction = ConnectIfNeeded** 인 경우에만 유효합니다. 추가할 DNS 서버를 입력합니다. 이 서버는 장치의 현재 네트워크 구성에 포함된 서버가 아니어도 됩니다. DNS 서버에 연결할 수 없는 경우 VPN 연결이 대신 설정됩니다. 이 DNS 서버는 내부 DNS 서버 또는 신뢰할 수 있는 외부 DNS 서버여야 합니다.

* 저장을 클릭하여 DNS 서버를 저장하거나 취소를 클릭하여 DNS 서버를 저장하지 않습니다.

- **ActionParameters : RequiredURLStringProbe:** 필요한 경우 GET 요청을 사용하여 검색할 HTTP 또는 HTTPS(기본 설정) URL 을 입력합니다. URL 의 호스트 이름을 확인할 수 없거나 서버에 연결할 수 없거나 서버가 응답하지 않는 경우 VPN 연결이 설정됩니다. **ActionParameters : DomainAction = ConnectIfNeeded** 인 경우에만 유효합니다.

- **OnDemandRules : XML 콘텐츠:** XML 구성 주문형 규칙을 입력하거나 복사 후 붙여넣습니다.

* 사전 확인을 클릭하여 XML 코드의 유효성을 검사합니다. XML 이 올바른 경우 **XML** 콘텐츠 텍스트 상자 아래 올바른 XML 이 녹색 텍스트로 표시됩니다. 올바르지 않은 경우 오류를 설명하는 오류 메시지가 주황색 텍스트로 표시됩니다.

• 프록시

- 프록시 구성: 목록에서 프록시 서버를 통해 VPN 연결을 라우팅하는 방법을 선택합니다. 기본값은 없음입니다.

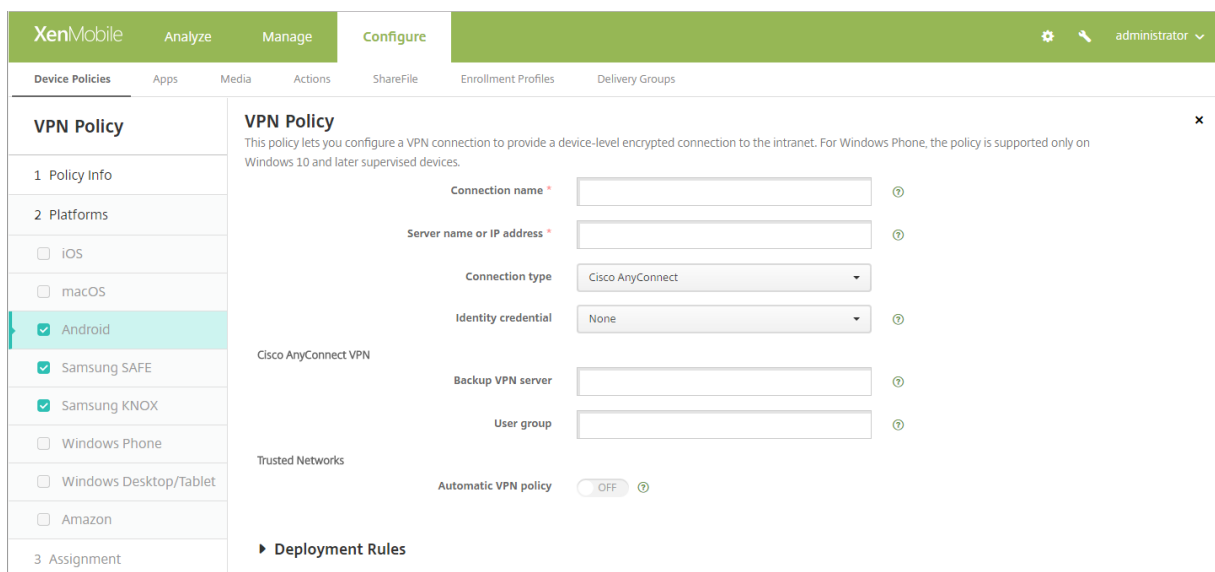
* 수동을 사용하는 경우 다음 설정을 구성합니다.

- 프록시 서버의 호스트 이름 또는 **IP** 주소: 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
- 프록시 서버용 포트: 프록시 서버 포트 번호를 입력합니다. 이것은 필수 필드입니다.
- 사용자 이름: 선택적 프록시 서버 사용자 이름을 입력합니다.
- 암호: 선택적 프록시 서버 암호를 입력합니다.

* 자동 구성하는 경우 다음 설정을 구성합니다.

- 프록시 서버 **URL**: 프록시 서버의 URL 을 입력합니다. 이것은 필수 필드입니다.

Android 설정



Android 용 Cisco AnyConnect VPN 프로토콜구성

- **연결이름:** Cisco AnyConnect VPN 연결의이름을입력합니다. 이것은필수필드입니다.
- **서버이름또는 IP 주소:** VPN 서버의이름또는 IP 주소를입력합니다. 이것은필수필드입니다.
- **ID 자격증명:** 목록에서 ID 자격증명을선택합니다.
- **백업 VPN 서버:** 백업 VPN 서버정보를입력합니다.
- **사용자그룹:** 사용자그룹정보를입력합니다.
- **신뢰할수있는네트워크**
 - **자동 VPN 정책:** 이 옵션을사용하거나사용하지않도록설정하여 VPN 이신뢰할수있는네트워크및신뢰할수없는네트워크에반응하는방법을설정합니다. 사용하는경우다음설정을구성합니다.
 - * **신뢰할수있는네트워크정책:** 목록에서원하는정책을선택합니다. 기본값은 연결끊기입니다. 사용가능한옵션은다음과같습니다.
 - **연결끊기:** 클라이언트가신뢰할수있는네트워크에서 VPN 연결을종료합니다. 이 설정은기본값입니다.
 - **연결:** 클라이언트가신뢰할수있는네트워크에서 VPN 연결을시작합니다.
 - **아무작업도하지않음:** 클라이언트가아무런동작을수행하지않습니다.
 - **일시중지:** 사용자가신뢰할수있는네트워크외부에서 VPN 세션을설정후신뢰할수있는네트워크로구성된네트워크로들어가면 VPN 세션이일시중지됩니다. 사용자가신뢰할수있는네트워크에서다시나가면 세션이다시시작됩니다. 이 설정을사용하면신뢰할수있는네트워크에서나간후새 VPN 세션을설정할필요가없습니다.
 - * **신뢰할수없는네트워크정책:** 목록에서원하는정책을선택합니다. 기본값은 연결입니다. 사용가능한옵션은다음과같습니다.
 - **연결:** 클라이언트가신뢰할수없는네트워크에서 VPN 연결을시작합니다.
 - **아무작업도하지않음:** 클라이언트가신뢰할수없는네트워크에서 VPN 연결을시작합니다. 이 옵션을사용하면항상 VPN 연결이사용되지않습니다.
 - **신뢰할수있는도메인:** 클라이언트가신뢰할수있는도메인에있을때네트워크인터페이스에포함되는각도메인접미사에대해 추가를클릭하고다음을수행합니다.
 - * **도메인:** 추가할도메인을입력합니다.
 - * **저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.**
 - **신뢰할수있는서버:** 클라이언트가신뢰할수있는도메인에있을때네트워크인터페이스에포함되는각서버주소에대해 추가를클릭하고다음을수행합니다.
 - * **서버:** 추가할서버를입력합니다.
 - * **저장을클릭하여서버를저장하거나 취소를클릭하여서버를저장하지않습니다.**

Android 용 Citrix SSO 프로토콜구성

- **연결이름:** VPN 연결의이름을입력합니다. 이것은필수필드입니다.
- **서버이름또는 IP 주소:** Citrix Gateway 의 FQDN 또는 IP 주소를입력합니다.
- **연결에대한인증유형:** 인증유형을선택하고유형에대해나타나는다음필드를모두작성합니다.

- 사용자이름 및 암호: 암호 또는 암호 및 인증서의 인증 유형에 대한 VPN 자격 증명을 입력합니다. 선택 사항입니다. VPN 자격 증명을 입력하지 않으면 Citrix VPN 앱에서 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
- ID 자격 증명: 인증 유형이 인증서 또는 암호 및 인증서인 경우 표시됩니다. 목록에서 ID 자격 증명을 선택합니다.
- **앱별 VPN 사용:** 앱별 VPN 을 사용할지 여부를 선택합니다. 앱별 VPN 을 사용하지 않는 경우 모든 트래픽이 Citrix VPN 터널을 통과합니다. 앱별 VPN 을 사용하는 경우 다음 설정을 지정합니다. 기본값은 꺼짐입니다.
 - 화이트리스트 또는 블랙리스트: 화이트리스트인 경우 화이트리스트의 모든 앱이 VPN 터널을 통과합니다. 블랙리스트인 경우 블랙리스트의 앱을 제외한 모든 앱이 VPN 터널을 통과합니다.
 - 응용 프로그램 목록: 화이트리스트 또는 블랙리스트 앱을 지정합니다. 추가를 클릭한 다음 앱 패키지 이름의 심볼로 구분된 목록을 입력합니다.
- 사용자 지정 **XML:** 추가를 클릭한 다음 사용자 지정 매개 변수를 입력합니다. XenMobile 은 Citrix VPN 에 대해 다음 매개 변수를 지원합니다.
 - **DisableUserProfiles:** 선택 사항입니다. 이 매개 변수를 사용하려면 값에 예를 입력합니다. 사용하도록 설정한 경우 XenMobile 은 사용자가 추가한 VPN 연결을 표시하지 않으며 사용자가 연결을 추가할 수 없습니다. 이 설정은 글로벌 제한이며 모든 VPN 프로필에 적용됩니다.
 - **userAgent:** 문자열 값입니다. 각 HTTP 요청에 보낼 사용자 지정 사용자 에이전트 문자열을 지정할 수 있습니다. 지정한 사용자 에이전트 문자열이 기존 Citrix VPN 사용자 에이전트에 추가됩니다.

Android Enterprise 에 대한 VPN 구성

Android Enterprise 장치에 대한 VPN 을 구성하려면 Citrix SSO 앱에 대한 Android Enterprise 관리되는 구성 장치 정책을 만듭니다. [Android Enterprise 에 대한 VPN 프로필 구성](#) 을 참조하십시오.

Samsung SAFE 설정

The screenshot shows the XenMobile Configure interface. The 'VPN Policy' configuration page is active, showing a list of platforms on the left and configuration fields on the right. The 'Platforms' section has 'Android', 'Samsung SAFE', and 'Samsung KNOX' selected. The configuration fields include:

- Connection name: K--PPTP
- Vpn Type: PPTP
- Host name: (empty)
- User name: testuser
- Password: (masked with dots)
- Enable encryption: OFF

Below the configuration fields, there is a section for 'Deployment Rules'.

- **연결이름:** 연결이름을 입력합니다.
- **VPN 유형:** 목록에서이연결에사용할프로토콜을선택합니다. 기본값은 미리공유한키를사용하는 **L2TP** 입니다. 사용가능한옵션은다음과같습니다.
 - 미리공유한키를사용하는 **L2TP:** 미리공유한키인증을포함하는계층 2 터널링프로토콜입니다. 이설정은기본값입니다.
 - 인증서를사용하는 **L2TP:** 인증서를사용하는계층 2 터널링프로토콜입니다.
 - **PPTP:** 지점간터널링입니다.
 - **엔터프라이즈:** 회사 VPN 연결입니다. SAFE 2.0 이전버전에적용됩니다.
 - **제네릭:** 제네릭 VPN 연결입니다. SAFE 2.0 이상버전에적용됩니다.

Samsung SAFE 용미리공유한키프로토콜을사용하는 **L2TP** 구성

- **호스트이름:** VPN 호스트의이름을입력합니다. 이옵션은필수입니다.
- **사용자이름:** 선택적사용자이름을입력합니다.
- **암호:** 선택적암호를입력합니다.
- **미리공유한키:** 미리공유한키를입력합니다. 이옵션은필수입니다.

Samsung SAFE 용인증서프로토콜을사용하는 **L2TP** 프로토콜구성

- **호스트이름:** VPN 호스트의이름을입력합니다. 이옵션은필수입니다.
- **사용자이름:** 선택적사용자이름을입력합니다.
- **암호:** 선택적암호를입력합니다.
- **ID 자격증명:** 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.

Samsung SAFE 용 **PPTP** 프로토콜구성

- **호스트이름:** VPN 호스트의이름을입력합니다. 이옵션은필수입니다.
- **사용자이름:** 선택적사용자이름을입력합니다.
- **암호:** 선택적암호를입력합니다.
- **암호화사용:** VPN 연결에암호화를사용할지여부를선택합니다.

Samsung SAFE 용엔터프라이즈프로토콜구성

- **호스트이름:** VPN 호스트의이름을입력합니다. 이옵션은필수입니다.
- **백업서버사용:** 백업 VPN 서버를사용할지여부를선택합니다. 사용하는경우 백업 **VPN** 서버에백업 VPN 서버의 FQDN 또는 IP 주소를입력합니다.
- **사용자인증사용:** 사용자인증이필요한지여부를선택합니다. 사용하는경우다음설정을구성합니다.
 - **사용자이름:** 사용자이름을입력합니다.
 - **암호:** 사용자암호를입력합니다.

- 그룹이름: 선택적그룹이름을입력합니다.
- 인증방법: 목록에서사용할인증방법을선택합니다. 사용가능한옵션은다음과같습니다.
 - 인증서: 인증서인증을사용합니다. 이설정은기본값입니다. 선택한경우 ID 자격증명목록에서사용할자격증명을선택합니다. 기본값은 없음입니다.
 - 미리공유한키: 미리공유한키를사용합니다. 선택한경우 미리공유한키필드에공유암호키를입력합니다.
 - 하이브리드 **RSA**: RSA 인증서를사용한하이브리드인증을사용합니다.
 - **EAP MD5**: EAP 피어를 EAP 서버로인증하지만상호인증은수행하지않습니다.
 - **EAP MSCHAPv2**: Microsoft 의 Challenge Handshake 인증을상호인증에서사용합니다.
- **CA** 인증서: 목록에서사용할인증서를선택합니다. 기본값은 없음입니다.
- 기본경로사용: VPN 서버에대한기본경로를사용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 스마트카드인증사용: 스마트카드를사용한사용자인증을허용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 모바일옵션사용: 모바일옵션을사용할지여부를선택합니다. 기본값은 꺼짐입니다.
- **Diffie-Hellman** 그룹값 (키강도): 목록에서사용할키강도를선택합니다. 기본값은 0 입니다.
- 분할터널유형: 목록에서사용할분할터널유형을선택합니다. 기본값은 자동입니다. 사용가능한옵션은다음과같습니다.
 - 자동: 분할터널링이자동으로사용됩니다.
 - 수동: VPN 서버에지정된 IP 주소및포트를통해분할터널링이사용됩니다.
 - 사용안함: 분할터널링이사용되지않습니다.
- **SuiteB** 유형: 목록에서사용할 NSA Suite B 암호화수준을선택합니다. 기본값은 **GCM-128** 입니다. 사용가능한옵션은다음과같습니다.
 - **GCM-128**: 128 비트 AES-GCM 암호화를사용합니다.
 - **GCM-256**: 256 비트 AES-GCM 암호화를사용합니다.
 - **GMAC-128**: 128 비트 AES-GMAC 암호화를사용합니다.
 - **GMAC-256**: 256 비트 AES-GMAC 암호화를사용합니다.
 - 없음: 암호화를사용하지않습니다.
- 전달경로: 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
 - 전달경로: 전달경로의 IP 주소를입력합니다.
 - 저장클릭하여경로를저장하거나 취소클릭하여경로를저장하지않습니다.

Samsung SAFE 용제네릭프로토콜구성

- 호스트이름: VPN 호스트의이름을입력합니다. 이옵션은필수입니다.
- 사용자인증사용: 사용자인증이필요한지여부를선택합니다. 사용하는경우 암호에사용자암호를입력합니다.
- 사용자이름: 사용자이름을입력합니다.
- 패키지이름에이전트 **VPN**: 장치에설치된 VPN 의패키지이름또는 ID 입니다 (예: Mocana 또는 Pulse Secure).
- **VPN** 연결유형: 목록에서사용할연결유형으로 **IPSEC** 또는 **SSL** 을선택합니다. 기본값은 **IPSEC** 입니다. 다음섹션에서는각연결유형에대한구성설정을설명합니다.

Samsung SAFE 용 IPSEC 연결유형설정구성

- **ID:** 이 구성에 대한 선택적 식별자를 입력합니다.
- **IPsec 그룹 ID 유형:** 목록에서 사용할 IPsec 그룹 ID 유형을 선택합니다. 기본값은 기본값입니다. 사용 가능한 옵션은 다음과 같습니다.
 - 기본값
 - **IPv4** 주소
 - **FQDN**(정규화된 도메인 이름)
 - 사용자 **FQDN**
 - **IKE 키 ID**
- **IKE 버전:** 목록에서 사용할 Internet Key Exchange 버전을 선택합니다. 기본값은 **IKEv1**입니다.
- **인증 방법:** 목록에서 사용할 인증 방법을 선택합니다. 기본값은 인증서입니다. 사용 가능한 옵션은 다음과 같습니다.
 - **인증서:** 인증서 인증을 사용합니다. 선택한 경우 **ID** 자격 증명 목록에서 사용할 자격 증명을 선택합니다. 기본값은 없음입니다.
 - **미리 공유한 키:** 미리 공유한 키를 사용합니다. 선택한 경우 미리 공유한 키 필드에 공유 암호 키를 입력합니다.
 - **하이브리드 RSA:** RSA 인증서를 사용한 하이브리드 인증을 사용합니다.
 - **EAP MD5:** EAP 피어를 EAP 서버로 인증하지만 상호 인증은 수행하지 않습니다.
 - **EAP MSCHAPv2:** Microsoft의 Challenge Handshake 인증을 상호 인증에 사용합니다.
 - **CAC 기반 인증:** CAC(Common Access Card)를 인증에 사용합니다.
- **ID 자격 증명:** 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
- **CA 인증서:** 목록에서 사용할 인증서를 선택합니다.
- **데드 피어 감지 사용:** 피어에 접속하여 활성 상태를 확인할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **기본 경로 사용:** VPN 서버에 대한 기본 경로를 사용할지 여부를 선택합니다.
- **모바일 옵션 사용:** 모바일 옵션을 사용할지 여부를 선택합니다.
- **IKE 수명 (분):** VPN 연결을 다시 설정하기 전까지의 시간 (분)을 입력합니다. 기본값은 1440 분 (24 시간)입니다.
- **ipsec 수명 (분):** VPN 연결을 다시 설정하기 전까지의 시간 (분)을 입력합니다. 기본값은 1440 분 (24 시간)입니다.
- **Diffie-Hellman 그룹값 (키강도):** 목록에서 사용할 키 강도를 선택합니다. 기본값은 0입니다.
- **IKE 단계 1 키 교환 모드:** IKE 단계 1 교환 모드에 대해 기본 또는 적극적 선택합니다. 기본값은 기본입니다.
 - **기본:** 협상 중에 잠재적 공격자에게 정보가 노출되지만 적극적 모드보다 느립니다.
 - **적극적:** 협상 중에 일부 정보 (예: 협상 중인 피어의 ID)가 잠재적 공격자에게 노출되지만 기본 모드보다 빠릅니다.
- **PFS(Perfect Forward Secrecy) 값:** 연결을 재협상할 때 PFS를 사용하여 새 키 교환을 요구할지 여부를 선택합니다.
- **분할터널 유형:** 목록에서 사용할 분할터널 유형을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - **자동:** 분할터널링이 자동으로 사용됩니다.
 - **수동:** VPN 서버에 지정된 IP 주소 및 포트를 통해 분할터널링이 사용됩니다.
 - **사용 안 함:** 분할터널링이 사용되지 않습니다.
- **IPSEC 암호화 알고리즘:** IPsec 프로토콜이 사용하는 VPN 구성입니다.
- **IKE 암호화 알고리즘:** IPsec 프로토콜이 사용하는 VPN 구성입니다.
- **IKE 무결성 알고리즘:** IPsec 프로토콜이 사용하는 VPN 구성입니다.
- **공급 업체:** Knox API와 통신하는 일반 에이전트의 개인 프로필입니다.

- 전달경로: 회사 VPN 서버가 전달경로를 지원하는 경우 사용할 각 전달 경로에 대해 추가를 클릭하고 다음을 수행합니다.
 - 전달경로: 전달경로의 IP 주소를 입력합니다.
 - 저장을 클릭하여 경로를 저장하거나 취소를 클릭하여 경로를 저장하지 않습니다.
- 앱별 VPN: 추가할 각 앱별 VPN 에 대해 추가를 클릭하고 다음을 수행합니다.
 - 앱별 VPN: 앱이 통신에 사용하는 VPN 구성입니다.
 - 저장을 클릭하여 앱별 VPN 을 저장하거나 취소를 클릭하여 앱별 VPN 을 저장하지 않습니다.

Samsung SAFE 용 SSL 연결 유형 설정 구성

- 인증방법: 목록에서 사용할 인증 방법을 선택합니다. 기본값은 해당 없음입니다. 사용 가능한 옵션은 다음과 같습니다.
 - 해당 없음
 - 인증서: 인증서 인증을 사용합니다. 선택한 경우 ID 자격 증명 목록에서 사용할 자격 증명을 선택합니다. 기본값은 없음입니다.
 - CAC 기반 인증: CAC(Common Access Card) 를 인증에 사용합니다.
- CA 인증서: 목록에서 사용할 인증서를 선택합니다.
- 기본 경로 사용: VPN 서버에 대한 기본 경로를 사용할지 여부를 선택합니다.
- 모바일 옵션 사용: 모바일 옵션을 사용할지 여부를 선택합니다.
- 분할 터널 유형: 목록에서 사용할 분할 터널 유형을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - 자동: 분할 터널링이 자동으로 사용됩니다.
 - 수동: VPN 서버에 지정된 IP 주소 및 포트를 통해 분할 터널링이 사용됩니다.
 - 사용 안 함: 분할 터널링이 사용되지 않습니다.
- SSL 알고리즘: 클라이언트-서버 협상에 사용할 SSL 알고리즘을 입력합니다.
- 공급업체: Knox API 와 통신하는 일반 에이전트의 개인 프로필입니다.
- 전달경로: 회사 VPN 서버가 전달경로를 지원하는 경우 사용할 각 전달 경로에 대해 추가를 클릭하고 다음을 수행합니다.
 - 전달경로: 전달경로의 IP 주소를 입력합니다.
 - 저장을 클릭하여 경로를 저장하거나 취소를 클릭하여 경로를 저장하지 않습니다.
- 앱별 VPN: 추가할 각 앱별 VPN 에 대해 추가를 클릭하고 다음을 수행합니다.
 - 앱별 VPN: 앱이 통신에 사용하는 VPN 구성입니다.
 - 저장을 클릭하여 앱별 VPN 을 저장하거나 취소를 클릭하여 앱별 VPN 을 저장하지 않습니다.

Samsung Knox 설정

The screenshot shows the 'Configure' page for a 'VPN Policy'. The left sidebar has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Samsung KNOX' is selected. The main configuration area includes:

- Vpn Type:** Enterprise (dropdown)
- Connection name *:** (text input)
- Host name *:** (text input)
- Enable backup server:** OFF (toggle)
- Enable user authentication:** OFF (toggle)
- Group name:** (text input)
- Authentication method:** Certificate (dropdown)
- Identity credential:** None (dropdown)
- CA certificate:** Select certificate (dropdown)
- Enable default route:** OFF (toggle)
- Enable smartcard authentication:** OFF (toggle)
- Enable mobile option:** OFF (toggle)

Samsung Knox 에대한정책을구성하는경우 Samsung Knox 컨테이너내부에만적용됩니다.

- **VPN 유형:** 목록에서구성할 VPN 연결유형을선택합니다. 연결은 엔터프라이즈 (Knox 2.0 이전버전에해당) 또는 제네릭 (Knox 2.0 이상버전에해당) 일수있습니다. 기본값은 엔터프라이즈입니다.

다음섹션에는이전에설명한각연결유형에대한구성옵션이나열되어있습니다.

Samsung Knox 용엔터프라이즈프로토콜구성

- **연결이름:** 연결이름을입력합니다. 이것은필수필드입니다.
- **호스트이름:** VPN 호스트의이름을입력합니다. 이옵션은필수입니다.
- **백업서버사용:** 백업 VPN 서버를사용할지여부를선택합니다. 사용하는경우 백업 **VPN** 서버에백업 VPN 서버의 FQDN 또는 IP 주소를입력합니다.
- **사용자인증사용:** 사용자인증이필요한지여부를선택합니다. 사용하는경우다음설정을구성합니다.
 - **사용자이름:** 사용자이름을입력합니다.
 - **암호:** 사용자암호를입력합니다.
- **그룹이름:** 선택적그룹이름을입력합니다.
- **인증방법:** 목록에서사용할인증방법을선택합니다. 사용가능한옵션은다음과같습니다.
 - **인증서:** 인증서인증을사용합니다. 인증서인증의경우 **ID** 자격증명목록에서사용할자격증명도선택합니다.
 - **미리공유한키:** 미리공유한키를사용합니다. 선택한경우 미리공유한키필드에공유암호키를입력합니다.
 - **하이브리드 RSA:** RSA 인증서를사용하이브리드인증을사용합니다.
 - **EAP MD5:** EAP 피어를 EAP 서버로인증하지만상호인증은수행하지않습니다.

- **EAP MSCHAPv2:** Microsoft 의 Challenge Handshake 인증을 상호인증에 사용합니다.
- **CA 인증서:** 목록에서 사용할 인증서를 선택합니다.
- **기본 경로 사용:** VPN 서버에 대한 기본 경로를 사용하지 여부를 선택합니다.
- **스마트카드 인증 사용:** 스마트카드를 사용한 사용자 인증을 허용할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **모바일 옵션 사용:** 모바일 옵션을 사용할지 여부를 선택합니다.
- **Diffie-Hellman 그룹값 (키강도):** 목록에서 사용할 키 강도를 선택합니다. 기본값은 **0**입니다.
- **분할터널 유형:** 목록에서 사용할 분할터널 유형을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - **자동:** 분할터널링이 자동으로 사용됩니다.
 - **수동:** VPN 서버에 지정된 IP 주소 및 포트를 통해 분할터널링이 사용됩니다.
 - **사용 안함:** 분할터널링이 사용되지 않습니다.
- **Suite B 유형:** 목록에서 사용할 NSA Suite B 암호화 수준을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - **GCM-128:** 128 비트 AES-GCM 암호화를 사용합니다. 이 설정은 기본값입니다.
 - **GCM-256:** 256 비트 AES-GCM 암호화를 사용합니다.
 - **GMAC-128:** 128 비트 AES-GMAC 암호화를 사용합니다.
 - **GMAC-256:** 256 비트 AES-GMAC 암호화를 사용합니다.
 - **없음:** 암호화를 사용하지 않습니다.
- **전달 경로:** 회사 VPN 서버가 다수의 경로로 테이블을 지원하는 경우 추가를 클릭하여 선택적 전달 경로를 추가합니다.

Samsung Knox 용 제네릭 프로토콜 구성

- **연결 이름:** 연결 이름을 입력합니다. 이것은 필수 필드입니다.
- **패키지 이름 에이전트 VPN:** 장치에 설치된 VPN 의 패키지 이름 또는 ID 입니다 (예: Mocana 또는 Pulse Secure).
- **호스트 이름:** VPN 호스트의 이름을 입력합니다. 이 옵션은 필수입니다.
- **사용자 인증 사용:** 사용자 인증이 필요한지 여부를 선택합니다. 사용하는 경우 다음 설정을 구성합니다.
 - **사용자 이름:** 사용자 이름을 입력합니다.
 - **암호:** 사용자 암호를 입력합니다.
- **ID:** 이 구성에 대한 선택적 식별자를 입력합니다. **Vpn 연결 유형 = IPSEC** 인 경우에만 적용됩니다.
- **VPN 연결 유형:** 목록에서 사용할 연결 유형으로 **IPSEC** 또는 **SSL** 을 선택합니다. 기본값은 **IPSEC** 입니다. 다음 섹션에서 각 연결 유형에 대한 구성 설정을 설명합니다.
- **IPSEC 연결 설정 구성**
 - **IPsec 그룹 ID 유형:** 목록에서 사용할 IPsec 그룹 ID 유형을 선택합니다. 기본값은 기본값입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * 기본값
 - * **IPv4** 주소
 - * **FQDN**(정규화된 도메인 이름)
 - * 사용자 **FQDN**
 - * **IKE** 키 ID
 - **IKE 버전:** 목록에서 사용할 Internet Key Exchange 버전을 선택합니다. 기본값은 **IKEv1** 입니다.
 - **인증 방법:** 목록에서 사용할 인증 방법을 선택합니다. 기본값은 인증서입니다. 사용 가능한 옵션은 다음과 같습니다.

- * 인증서: 인증서인증을 사용합니다. 선택한 경우 **ID** 자격증명목록에서 사용할 자격증명을 선택합니다. 기본값은 없습니다.
 - * 미리공유한키: 미리공유한키를 사용합니다. 선택한 경우 미리공유한키필드에 공유암호키를 입력합니다.
 - * 하이브리드 **RSA**: RSA 인증서를 사용한 하이브리드 인증을 사용합니다.
 - * **EAP MD5**: EAP 피어를 EAP 서버로 인증하지만 상호인증은 수행하지 않습니다.
 - * **EAP MSCHAPv2**: Microsoft의 Challenge Handshake 인증을 상호인증에 사용합니다.
 - * **CAC** 기반인증: CAC(Common Access Card)를 인증에 사용합니다.
- **CA** 인증서: 목록에서 사용할 인증서를 선택합니다.
 - 데드피어감지사용: 피어에 접속하여 활성 상태를 확인할지 여부를 선택합니다. 기본값은 꺼짐입니다.
 - 기본경로사용: VPN 서버에 대한 기본 경로를 사용할지 여부를 선택합니다.
 - 모바일 옵션사용: 모바일 옵션을 사용할지 여부를 선택합니다.
 - **IKE** 수명 (분): VPN 연결을 다시 설정하기 전까지의 시간 (분)을 입력합니다. 기본값은 1440 분 (24 시간)입니다.
 - **ipsec** 수명 (분): VPN 연결을 다시 설정하기 전까지의 시간 (분)을 입력합니다. 기본값은 1440 분 (24 시간)입니다.
 - **Diffie-Hellman** 그룹값 (키강도): 목록에서 사용할 키 강도를 선택합니다. 기본값은 **0**입니다.
 - **IKE** 단계 1 키교환모드: IKE 단계 1 교환모드에 대해 기본 또는 적극적 선택합니다. 기본값은 기본입니다.
 - * 기본: 협상 중에 잠재적 공격자에게 정보가 노출되지 않지만 적극적 모드보다 느립니다.
 - * 적극적: 협상 중에 일부 정보 (예: 협상 중인 피어의 ID)가 잠재적 공격자에게 노출되지만 기본 모드보다 빠릅니다.
 - **PFS(Perfect Forward Secrecy)** 값: 연결을 재협상할 때 PFS를 사용하여 새 키 교환을 요구할지 여부를 선택합니다.
 - 분할터널 유형: 목록에서 사용할 분할터널 유형을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - * 자동: 분할터널링이 자동으로 사용됩니다.
 - * 수동: VPN 서버에 지정된 IP 주소 및 포트를 통해 분할터널링이 사용됩니다.
 - * 사용안함: 분할터널링이 사용되지 않습니다.
 - **SuiteB** 유형: 목록에서 사용할 NSA Suite B 암호화 수준을 선택합니다. 기본값은 **GCM-128**입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **GCM-128**: 128 비트 AES-GCM 암호화를 사용합니다.
 - * **GCM-256**: 256 비트 AES-GCM 암호화를 사용합니다.
 - * **GMAC-128**: 128 비트 AES-GMAC 암호화를 사용합니다.
 - * **GMAC-256**: 256 비트 AES-GMAC 암호화를 사용합니다.
 - * 없음: 암호화를 사용하지 않습니다.
 - **IPSEC** 암호화 알고리즘: IPsec 프로토콜이 사용하는 VPN 구성입니다.
 - **IKE** 암호화 알고리즘: IPsec 프로토콜이 사용하는 VPN 구성입니다.
 - **IKE** 무결성 알고리즘: IPsec 프로토콜이 사용하는 VPN 구성입니다.
 - **Knox**: Samsung Knox 전용 구성입니다.
 - 공급업체: Knox API와 통신하는 일반 에이전트의 개인 프로필입니다.
 - 전달 경로: 회사 VPN 서버가 전달 경로를 지원하는 경우 사용할 각 전달 경로에 대해 추가를 클릭하고 다음을 수행합니다.
 - * 전달 경로: 전달 경로의 IP 주소를 입력합니다.
 - * 저장: 저장할 클릭하여 경로를 저장하거나 취소를 클릭하여 경로를 저장하지 않습니다.

- **앱별 VPN:** 추가할 각 앱별 VPN 에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **앱별 VPN:** 앱이 통신에 사용하는 VPN 구성입니다.
 - * **저장을 클릭하여 앱별 VPN 을 저장하거나 취소를 클릭하여 앱별 VPN 을 저장하지 않습니다.**
- **SSL 연결 설정 구성**
 - **인증 방법:** 목록에서 사용할 인증 방법을 클릭합니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **해당 없음:** 인증 방법이 적용되지 않습니다. 이 설정은 기본값입니다.
 - * **인증서:** 인증서 인증을 사용합니다. 이 설정은 기본값입니다. 선택한 경우 ID 자격 증명 목록에서 사용할 자격 증명 을 선택합니다. 기본값은 없음입니다.
 - * **CAC 기반 인증:** CAC(Common Access Card) 를 인증에 사용합니다.
 - **CA 인증서:** 목록에서 사용할 인증서를 선택합니다.
 - **기본 경로 사용:** VPN 서버에 대한 기본 경로를 사용할지 여부를 선택합니다.
 - **모바일 옵션 사용:** 모바일 옵션을 사용할지 여부를 선택합니다.
 - **분할터널 유형:** 목록에서 사용할 분할터널 유형을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **자동:** 분할터널링이 자동으로 사용됩니다.
 - * **수동:** 지정된 IP 주소 및 포트를 통해 분할터널링이 사용됩니다.
 - * **사용 안함:** 분할터널링이 사용되지 않습니다.
 - **SuiteB 유형:** 목록에서 사용할 NSA Suite B 암호화 수준을 선택합니다. 기본값은 GCM-128 입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **GCM-128:** 128 비트 AES-GCM 암호화를 사용합니다.
 - * **GCM-256:** 256 비트 AES-GCM 암호화를 사용합니다.
 - * **GMAC-128:** 128 비트 AES-GMAC 암호화를 사용합니다.
 - * **GMAC-256:** 256 비트 AES-GMAC 암호화를 사용합니다.
 - * **없음:** 암호화 사용 안함: 클라이언트-서버 협상에 사용할 SSL 알고리즘을 입력합니다.
 - **SSL 알고리즘:** 클라이언트-서버 협상에 사용할 SSL 알고리즘을 입력합니다.
 - **Knox:** Samsung Knox 전용 구성입니다.
 - **공급 업체:** Knox API 와 통신하는 일반 에이전트의 개인 프로필입니다.
 - **전달 경로:** 회사 VPN 서버가 전달 경로를 지원하는 경우 사용할 각 전달 경로에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **전달 경로:** 전달 경로의 IP 주소를 입력합니다.
 - * **저장을 클릭하여 경로를 저장하거나 취소를 클릭하여 경로를 저장하지 않습니다.**
 - **앱별 VPN:** 추가할 각 앱별 VPN 에 대해 추가를 클릭하고 다음을 수행합니다.
 - * **앱별 VPN:** 앱이 통신에 사용하는 VPN 구성입니다.
 - * **저장을 클릭하여 앱별 VPN 을 저장하거나 취소를 클릭하여 앱별 VPN 을 저장하지 않습니다.**

Windows Phone 설정

이러한 설정은 Window 10 이상의 감독되는 전화에서만 지원됩니다.

- **연결이름:** 연결이름을 입력합니다. 이것은 필수 필드입니다.
- **프로필 유형:** 목록에서 기본 또는 플러그인을 선택합니다. 기본값은 기본입니다. 다음 섹션에서는 이러한 각 옵션에 대한 설정을 설명합니다.
- **기본 프로필 유형 설정 구성:** 사용자의 Windows Phone 에 기본 제공되는 VPN 에 적용되는 설정입니다.
 - **VPN 서버 이름:** VPN 서버의 FQDN 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - **터널링 프로토콜:** 목록에서 사용할 VPN 터널 유형을 선택합니다. 기본값은 **L2TP** 입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **L2TP:** 미리 공유한 키 인증을 사용하는 계층 2 터널링 프로토콜입니다.
 - * **PPTP:** 지점간 터널링입니다.
 - * **IKEv2:** Internet Key Exchange 버전 2 입니다.
 - **인증 방법:** 목록에서 사용할 인증 방법을 선택합니다. 기본값은 **EAP** 입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **EAP:** Extended Authentication Protocol 의 약어로 확장 인증 프로토콜을 의미합니다.
 - * **MSChapV2:** Microsoft 의 Challenge Handshake 인증을 상호 인증에 사용합니다. IKEv2 를 터널 유형으로 선택하는 경우 이 옵션을 사용할 수 없습니다. MSChapV2 를 선택하면 자동으로 **Windows** 자격 증명 사용 옵션이 나타납니다. 기본값은 꺼짐입니다.
 - **EAP 방법:** 목록에서 사용할 EAP 방법을 선택합니다. 기본값은 **TLS** 입니다. MSChapV2 인증을 사용하는 경우 이 필드를 사용할 수 없습니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **TLS:** 전송 계층 보안
 - * **PEAP:** 보호되는 확장 인증 프로토콜

- **DNS 접미사:** DNS 접미사를 입력합니다.
- **신뢰할 수 있는 네트워크:** 액세스시 VPN 연결이 필요하지 않은 네트워크 목록을 심표로 구분하여 입력합니다. 예를 들어 회사무선네트워크에 있는 사용자는 보호되는 리소스에 직접 액세스할 수 있습니다.
- **스마트카드 인증서 필요:** 스마트카드 인증서가 필요한지 여부를 선택합니다. 기본값은 꺼짐입니다.
- **자동으로 클라이언트 인증서 선택:** 인증에 사용할 클라이언트 인증서를 자동으로 선택할지 여부를 선택합니다. 기본값은 꺼짐입니다. 스마트카드 인증서 필요를 사용하는 경우 옵션을 사용할 수 없습니다.
- **자격 증명 저장:** 자격 증명을 캐시할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하면 가능한 경우 항상 자격 증명이 캐시됩니다.
- **항상 VPN 연결:** VPN 을 항상 연결할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하는 경우 사용자가 수동으로 연결을 끊기 전까지 VPN 연결이 연결된 상태로 유지됩니다.
- **로컬에 대해서는 바이패스:** 로컬 리소스의 프록시 서버 바이패스를 허용할 주소 및 포트 번호를 입력합니다.
- **플러그인 프로토콜 유형 구성:** Windows 스토어에서 가져와 사용자 장치에 설치한 VPN 플러그인에 적용되는 설정입니다.
 - **서버 주소:** VPN 서버의 URL, 호스트 이름 또는 IP 주소를 입력합니다.
 - **클라이언트 앱 ID:** VPN 플러그인의 패키지 제품군 이름을 입력합니다.
 - **플러그인 프로필 XML:** 찾아보기를 클릭하고 파일 위치로 이동하여 사용할 사용자 지정 VPN 플러그인을 선택합니다. 형식 및 세부 정보는 플러그인 공급자에게 문의하십시오.
 - **DNS 접미사:** DNS 접미사를 입력합니다.
 - **신뢰할 수 있는 네트워크:** 액세스시 VPN 연결이 필요하지 않은 네트워크 목록을 심표로 구분하여 입력합니다. 예를 들어 회사무선네트워크에 있는 사용자는 보호되는 리소스에 직접 액세스할 수 있습니다.
 - **자격 증명 저장:** 자격 증명을 캐시할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하면 가능한 경우 항상 자격 증명이 캐시됩니다.
 - **항상 VPN 연결:** VPN 을 항상 연결할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하는 경우 사용자가 수동으로 연결을 끊기 전까지 VPN 연결이 연결된 상태로 유지됩니다.
 - **로컬에 대해서는 바이패스:** 로컬 리소스의 프록시 서버 바이패스를 허용할 주소 및 포트 번호를 입력합니다.

Windows 데스크톱/태블릿설정

The screenshot shows the 'Configure' page for a 'VPN Policy'. The left sidebar has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Windows Desktop/Tablet' is selected. The main area contains the following settings:

- Connection name: [Text Input]
- Profile type: Native (Dropdown)
- Server address: [Text Input]
- Remember credential: OFF (Toggle)
- DNS suffix: [Text Input]
- Tunnel type: L2TP (Dropdown)
- Authentication method: EAP (Dropdown)
- EAP method: TLS (Dropdown)
- Trusted networks: [Text Input]
- Require smart card certificate: OFF (Toggle)
- Automatically select client certificate: OFF (Toggle)
- Always-on VPN: OFF (Toggle)

- **연결이름:** 연결이름을 입력합니다. 이것은 필수 필드입니다.
- **프로필유형:** 목록에서 기본 또는 플러그인을 선택합니다. 기본값은 기본입니다.
- **기본프로필유형구성:** 사용자의 Windows 장치에 기본 제공되는 VPN에 적용되는 설정입니다.
 - **서버주소:** VPN 서버의 FQDN 또는 IP 주소를 입력합니다. 이것은 필수 필드입니다.
 - **자격증명저장:** 자격증명을 캐시할지 여부를 선택합니다. 기본값은 꺼짐입니다. 사용하면 가능한 경우 항상 자격증명이 캐시됩니다.
 - **DNS 접미사:** DNS 접미사를 입력합니다.
 - **터널유형:** 목록에서 사용할 VPN 터널유형을 선택합니다. 기본값은 **L2TP**입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **L2TP:** 미리 공유한 키 인증을 사용하는 계층 2 터널링 프로토콜입니다.
 - * **PPTP:** 지점간 터널링입니다.
 - * **IKEv2:** Internet Key Exchange 버전 2입니다.
 - **인증방법:** 목록에서 사용할 인증방법을 선택합니다. 기본값은 **EAP**입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **EAP:** Extended Authentication Protocol 의약어로 확장 인증 프로토콜을 의미합니다.
 - * **MSChapV2:** Microsoft의 Challenge Handshake 인증을 상호 인증에 사용합니다. **IKEv2** 터널 유형으로 선택하는 경우 이 옵션을 사용할 수 없습니다.
 - **EAP 방법:** 목록에서 사용할 EAP 방법을 선택합니다. 기본값은 **TLS**입니다. MSChapV2 인증을 사용하는 경우 이 필드를 사용할 수 없습니다. 사용 가능한 옵션은 다음과 같습니다.
 - * **TLS:** 전송 계층 보안
 - * **PEAP:** 보호되는 확장 인증 프로토콜
 - **신뢰할 수 있는 네트워크:** 액세스 시 VPN 연결이 필요하지 않은 네트워크 목록을 쉼표로 구분하여 입력합니다. 예를 들어

회사무선네트워크에있는사용자는보호되는리소스에직접액세스할수있습니다.

- 스마트카드인증서필요: 스마트카드인증서가필요한지여부를선택합니다. 기본값은 꺼짐입니다.
- 자동으로클라이언트인증서선택: 인증에사용할클라이언트인증서를자동으로선택할지여부를선택합니다. 기본값은 꺼짐입니다. 스마트카드인증서필요를사용하는경우이옵션을사용할수없습니다.
- 항상 VPN 연결: VPN 을항상연결할지여부를선택합니다. 기본값은 꺼짐입니다. 사용하는경우사용자가수동으로 연결을끊기전까지 VPN 연결이연결된상태로유지됩니다.
- 로컬에대해서는바이패스: 로컬리소스의프록시서버바이패스를허용할주소및포트번호를입력합니다.
- 플러그인프로필유형구성: Windows 스토어에서가져와사용자장치에설치한 VPN 플러그인에적용되는설정입니다.
 - 서버주소: VPN 서버의 FQDN 또는 IP 주소를입력합니다. 이것은필수필드입니다.
 - 자격증명저장: 자격증명을캐시할지여부를선택합니다. 기본값은 꺼짐입니다. 사용하면가능한경우항상자격증명이 캐시됩니다.
 - DNS 접미사: DNS 접미사를입력합니다.
 - 클라이언트앱 ID: VPN 플러그인의패키지제품군이름을입력합니다.
 - 플러그인프로필 XML: 찾아보기를클릭하고파일위치로이동하여사용할사용자지정 VPN 플러그인을선택합니다. 형식및세부정보는플러그인공급자에게문의하십시오.
 - 신뢰할수있는네트워크: 액세스시 VPN 연결이필요하지않은네트워크목록을선택하여구분하여입력합니다. 예를들어 회사무선네트워크에있는사용자는보호되는리소스에직접액세스할수있습니다.
 - 항상 VPN 연결: VPN 을항상연결할지여부를선택합니다. 기본값은 꺼짐입니다. 사용하는경우사용자가수동으로 연결을끊기전까지 VPN 연결이연결된상태로유지됩니다.
 - 로컬에대해서는바이패스: 로컬리소스의프록시서버바이패스를허용할주소및포트번호를입력합니다.

Amazon 설정

The screenshot shows the 'VPN Policy' configuration screen in the XenMobile console. The left sidebar lists various platforms, with 'Amazon' selected. The main area contains the following configuration fields:

- Connection name *
- Vpn Type: L2TP P5K
- Server address *
- User name: administrator
- Password: [Redacted]
- L2TP Secret
- IPsec Identifier
- IPsec pre-shared key
- DNS search domains
- DNS servers
- Forwarding routes

At the bottom, there are 'Deployment Rules' and navigation buttons for 'Back' and 'Next >'.

- **연결이름:** 연결이름을입력합니다.
- **VPN 유형:** 연결유형을선택합니다. 사용가능한옵션은다음과같습니다.
 - **L2TP PSK:** 미리공유한키인증을사용하는계층 2 터널링프로토콜입니다. 이설정기본값입니다.
 - **L2TP RSA:** RSA 인증을사용하는계층 2 터널링프로토콜입니다.
 - **IPSEC XAUTH PSK:** 미리공유한키및확장인증을사용하는인터넷프로토콜보안입니다.
 - **IPSEC HYBRID RSA:** 하이브리드 RSA 인증을사용하는인터넷프로토콜보안입니다.
 - **PPTP:** 지점간터널링입니다.

다음섹션에는이전에설명한각연결유형에대한구성옵션이나열되어있습니다.

Amazon 용 L2TP PSK 설정구성

- **서버주소:** VPN 서버의 IP 주소를입력합니다.
- **사용자이름:** 선택적사용자이름을입력합니다.
- **암호:** 선택적암호를입력합니다.
- **L2TP 암호:** 공유암호키를입력합니다.
- **IPSec 식별자:** 연결할때장치에표시되는 VPN 연결이름을입력합니다.
- **미리공유한 IPSec 키:** 암호키를입력합니다.
- **DNS 검색도메인:** 사용자장치의검색도메인목록과일치할수있는도메인을입력합니다.
- **DNS 서버:** 지정된도메인을확인하는데사용할 DNS 서버의 IP 주소를입력합니다.
- **전달경로:** 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
 - **전달경로:** 전달경로의 IP 주소를입력합니다.
 - **저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.**

Amazon 용 L2TP RSA 설정구성

- **서버주소:** VPN 서버의 IP 주소를입력합니다.
- **사용자이름:** 선택적사용자이름을입력합니다.
- **암호:** 선택적암호를입력합니다.
- **L2TP 암호:** 공유암호키를입력합니다.
- **DNS 검색도메인:** 사용자장치의검색도메인목록과일치할수있는도메인을입력합니다.
- **DNS 서버:** 지정된도메인을확인하는데사용할 DNS 서버의 IP 주소를입력합니다.
- **서버인증서:** 목록에서사용할서버인증서를선택합니다.
- **CA 인증서:** 목록에서사용할 CA 인증서를선택합니다.
- **ID 자격증명:** 목록에서사용할 ID 자격증명을선택합니다.
- **전달경로:** 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
 - **전달경로:** 전달경로의 IP 주소를입력합니다.
 - **저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.**

Amazon 용 IPSEC XAUTH PSK 설정구성

- 서버주소: VPN 서버의 IP 주소를입력합니다.
- 사용자이름: 선택적사용자이름을입력합니다.
- 암호: 선택적암호를입력합니다.
- **IPSec** 식별자: 연결할때장치에표시되는 VPN 연결이름을입력합니다.
- 미리공유한 **IPSec** 키: 공유암호키를입력합니다.
- **DNS** 검색도메인: 사용자장치의검색도메인목록과일치할수있는도메인을입력합니다.
- **DNS** 서버: 지정된도메인을확인하는데사용할 DNS 서버의 IP 주소를입력합니다.
- 전달경로: 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
 - 전달경로: 전달경로의 IP 주소를입력합니다.
 - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.

Amazon 용 IPSEC AUTH RSA 설정구성

- 서버주소: VPN 서버의 IP 주소를입력합니다.
- 사용자이름: 선택적사용자이름을입력합니다.
- 암호: 선택적암호를입력합니다.
- **DNS** 검색도메인: 사용자장치의검색도메인목록과일치할수있는도메인을입력합니다.
- **DNS** 서버: 지정된도메인을확인하는데사용할 DNS 서버의 IP 주소를입력합니다.
- 서버인증서: 목록에서사용할서버인증서를선택합니다.
- **CA** 인증서: 목록에서사용할 CA 인증서를선택합니다.
- **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다.
- 전달경로: 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
 - 전달경로: 전달경로의 IP 주소를입력합니다.
 - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.

Amazon 용 IPSEC HYBRID RSA 설정구성

- 서버주소: VPN 서버의 IP 주소를입력합니다.
- 사용자이름: 선택적사용자이름을입력합니다.
- 암호: 선택적암호를입력합니다.
- **DNS** 검색도메인: 사용자장치의검색도메인목록과일치할수있는도메인을입력합니다.
- **DNS** 서버: 지정된도메인을확인하는데사용할 DNS 서버의 IP 주소를입력합니다.
- 서버인증서: 목록에서사용할서버인증서를선택합니다.
- **CA** 인증서: 목록에서사용할 CA 인증서를선택합니다.
- 전달경로: 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
 - 전달경로: 전달경로의 IP 주소를입력합니다.
 - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.

Amazon 용 PPTP 설정구성

- 서버주소: VPN 서버의 IP 주소를입력합니다.
- 사용자이름: 선택적사용자이름을입력합니다.
- 암호: 선택적암호를입력합니다.
- DNS 검색도메인: 사용자장치의검색도메인목록과일치할수있는도메인을입력합니다.
- DNS 서버: 지정된도메인을확인하는데사용할 DNS 서버의 IP 주소를입력합니다.
- PPP 암호화 (MPPE): Microsoft MPPE(지점간암호화) 로데이터암호화를사용할지여부를선택합니다. 기본값은 꺼
짐입니다.
- 전달경로: 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
 - 전달경로: 전달경로의 IP 주소를입력합니다.
 - 저장클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.

배경화면장치정책

January 6, 2020

iOS 장치잠금화면, 홈화면또는돌다에배경화면을설정할.png 또는.jpg 파일을추가할수있습니다. iOS 7.1.2 이상에서사용할수
있습니다. iPad 및 iPhone 에서서로다른배경화면을사용하려면서로다른배경화면정책을만들어해당사용자에게배포해야합니
다.

다음표에는 iOS 장치에대한 Apple 의권장이미지크기가나와있습니다.

장치	이미지크기 (픽셀)
iPhone 5, 5c, 5s	640 x 1136
iPhone 6, 6s	750 x 1334
iPhone 6 Plus	1080 x 1920
iPad Air, 2	1536 x 2048
iPad 4, 3	1536 x 2048
iPad Mini 2, 3	1536 x 2048

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

- 적용대상: 목록에서 잠금화면, 홈 (아이콘목록) 화면또는 잠금및홈화면을선택하여배경화면이나타날위치를설정합니다.

- 배경화면파일: 찾아보기를클릭하고파일위치로이동하여배경화면파일을선택합니다.

웹콘텐츠필터장치정책

January 6, 2020

화이트리스트및블랙리스트에추가한특정사이트와함께 Apple 의자동필터기능을사용하여 iOS 장치에서웹콘텐츠를필터링하는장치정책을 XenMobile 에서추가할수있습니다. 감독모드에서 iOS 7.0 이상의장치에서만이정책을사용할수있습니다. iOS 장치감독모드로전환하는방법에대한자세한내용은 [Apple Configurator 를사용하여 iOS 장치를감독모드로전환](#)을참조하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

iOS 설정

- 필터유형: 목록에서 기본제공또는 플러그인을클릭한후선택한옵션에대한절차를따릅니다. 기본값은 기본제공입니다.

기본제공필터유형

- 웹콘텐츠필터
 - 자동필터사용: Apple 의자동필터기능을사용하여웹사이트의부적절한콘텐츠를분석할지여부를선택합니다. 기본값은 꺼짐입니다.
 - 허용 **URL**: 자동필터사용이 꺼짐으로설정된경우이목록이무시됩니다. 자동필터사용이 켜짐으로설정된경우자동필터가액세스를허용하는지여부에관계없이항상이목록의항목에액세스할수있습니다. 화이트리스트에추가할각 URL 에대해 추가를클릭하여다음을수행합니다.
 - * 허용된웹사이트의 URL 을입력합니다. 웹주소앞에 **http://** 또는 **https://** 를추가해야합니다.
 - * 웹사이트를화이트리스트에저장하려면 저장을클릭하고, 저장하지않으려면 취소를클릭합니다.
 - 블랙리스트 **URL**: 이목록의항목은항상차단됩니다. 블랙리스트에추가할각 URL 에대해 추가를클릭하여다음을수행합니다.
 - * 차단할웹사이트의 URL 을입력합니다. 웹주소앞에 **http://** 또는 **https://** 를추가해야합니다.
 - * 웹사이트를블랙리스트에저장하려면 저장을클릭하고, 저장하지않으려면 취소를클릭합니다.
- 책갈피화이트리스트
 - 책갈피화이트리스트: 사용자가액세스할수있는사이트를지정합니다. 웹사이트에액세스할수있도록하려면해당웹사이트의 URL 을추가합니다.
 - * **URL**: 사용자가액세스할수있는각웹사이트의 URL 입니다. 예를들어 Secure Hub 스토어에액세스할수있도록하려면 **URL** 목록에 XenMobile Server URL 을 추가합니다. 웹주소앞에 **http://** 또는 **https://** 를추가해야합니다. 이것은필수필드입니다.
 - * 책갈피폴더: 선택적책갈피폴더이름을입력합니다. 이필드를비워두면책갈피책갈피기본디렉터리에추가됩니다.

- * 제목: 웹사이트를 설명하는 제목을 입력합니다. 예를 들어, URL 이 <https://google.com>인 경우 “Google” 을 입력합니다.
- * 웹사이트를 화이트리스트에 저장하려면 저장을 클릭하고, 저장하지 않으려면 취소를 클릭합니다.

플러그인 필터 유형

- 필터 이름: 필터에 대한 고유한 이름을 입력합니다.
- 식별자: 필터링 서비스를 제공하는 플러그인의 번들 ID 를 입력합니다.
- 서비스 주소: 선택적 서버 주소를 입력합니다. 올바른 형식은 IP 주소, 호스트 이름 또는 URL 입니다.
- 사용자 이름: 서비스에 대한 선택적 사용자 이름을 입력합니다.
- 암호: 서비스에 대한 선택적 암호를 입력합니다.
- 인증서: 목록에서 서비스에 사용자를 인증하는데 사용할 선택적 ID 인증서를 클릭합니다. 기본값은 없음입니다.
- **WebKit** 트래픽 필터링: WebKit 트래픽을 필터링할 것인지 선택합니다.
- 소켓 트래픽 필터링: 소켓 트래픽을 필터링할 것인지 선택합니다.
- 사용자 지정 데이터: 웹 필터에 추가할 각 사용자 지정 키에 대해 추가를 클릭한 후 다음을 수행합니다.
 - 키: 사용자 지정 키를 입력합니다.
 - 값: 사용자 지정 키 값을 입력합니다.
 - 사용자 지정 키를 저장하려면 저장을 클릭하고, 저장하지 않으려면 취소를 클릭합니다.

웹 클립 장치 정책

January 6, 2020

웹사이트에 대한 바로가기 또는 웹 클립을 배치하여 앱과 나란히 사용자 장치에 표시할 수 있습니다. iOS, macOS 및 Android 장치에서는 웹 클립을 나타내는 고유한 아이콘을 지정할 수 있습니다. Windows 태블릿에는 레이블 및 URL 만 필요합니다.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#)에서 참조하십시오.

iOS 설정

- 레이블: 웹 클립과 함께 표시할 레이블을 입력합니다.
- **URL**: 웹 클립과 관련된 URL 을 입력합니다. URL 은 프로토콜 (예: <https://server>) 로 시작해야 합니다.
- 제거 가능: 사용자가 웹 클립을 제거할 수 있는지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 업데이트 할 아이콘: 찾아보기를 클릭하고 파일의 위치로 이동하여 웹 클립에 사용할 아이콘을 선택합니다.
- 미리 작성된 아이콘: 아이콘에 적용된 효과 (둥근 모서리, 그림자 및 반사광택) 가 있는지 여부를 선택합니다. 기본값은 효과를 추가하는 꺼짐입니다.
- 전체 화면: 링크된 웹 페이지를 전체 화면 모드로 열지 여부를 선택합니다. 기본값은 꺼짐입니다.

macOS 설정

- 레이블: 웹클립과함께표시할레이블을입력합니다.
- **URL:** 웹클립과연관된 URL 을입력합니다. URL 은프로토콜 (예: <https://server>) 로시작해야합니다.
- 업데이트할아이콘: 찾아보기를클릭하고파일의위치로이동하여웹클립에사용할아이콘을선택합니다.

Android 설정

- 규칙: 이정책으로웹클립을추가하지아니면제거할지선택합니다. 기본값은 추가입니다.
- 레이블: 웹클립과함께표시할레이블을입력합니다.
- **URL:** 웹클립과연관된 URL 을입력합니다.
- 아이콘정의: 아이콘파일사용여부를선택합니다. 기본값은 꺼짐입니다.
- 아이콘파일: 아이콘정의가 켜짐인경우 찾아보기를클릭하고파일위치로이동하여사용할아이콘파일을선택합니다.

Windows 데스크톱/태블릿설정

- 이름: 웹클립과함께표시할레이블을입력합니다.
- **URL:** 웹클립과연관된 URL 을입력합니다.

WiFi 장치정책

January 6, 2020

XenMobile 에서 WiFi 장치정책을새로만들거나기존 WiFi 장치정책을편집하려면 구성 > 장치정책페이지를사용합니다. WiFi 정책을사용하면다음항목을정의하여사용자가장치를 WiFi 네트워크에연결하는방식을관리할수있습니다.

- 네트워크이름및유형
- 인증및보안정책
- 프록시서버사용
- 기타 WiFi 관련정보

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

사전요구사항

정책을만들려면먼저다음단계를완료해야합니다.

- 사용하려는배달그룹을만듭니다.
- 네트워크이름과유형을파악합니다.

- 사용할인증또는보안유형을파악합니다.
- 필요할수있는프록시서버정보를파악합니다.
- 필요한모든 CA 인증서를설치합니다.
- 필요한공유키를확보합니다.
- 인증서기반인증을위한 PKI 엔터티를만듭니다.
- 자격증명공급자를구성합니다.

자세한내용은 [인증](#) 및그하위문서를참조하십시오.

iOS 설정

The screenshot displays the 'Configure' section for 'WiFi Policy' in XenMobile. The left sidebar shows a list of platforms with 'iOS' selected. The main configuration area includes the following settings:

- Network type:** Standard
- Network name:** (Empty text field)
- Hidden network (enable if network is open or off):** OFF
- Auto join (automatically join this wireless network):** ON
- Disable Captive Network Detection:** OFF
- Security type:** None
- Proxy configuration:** None
- Fast Lane QoS Marking:** Do not restrict QoS marking
- Remove policy:** Select date

- 네트워크유형: 목록에서 표준, 레거시핫스팟또는 **Hotspot 2.0** 을선택하여사용할네트워크유형을설정합니다.
- 네트워크이름: 장치의사용가능한네트워크목록에표시되는 SSID 를입력합니다. **Hotspot 2.0** 에는적용되지않습니다.
- 숨겨진네트워크 (네트워크가열려있거나꺼져있는경우에사용): 네트워크를숨길지여부를선택합니다.
- 자동참가 (이무선네트워크에자동참가): 네트워크를자동으로참가시킬지여부를선택합니다. iOS 장치가이미다른네트워크에연결되어있으면이네트워크에연결되지않습니다. 장치가자동으로연결되기전에사용자가이전네트워크와의연결을끊어야합니다. 기본값은 켜짐입니다.
- 보안유형: 목록에서사용하려는보안유형을선택합니다. **Hotspot 2.0** 에는적용되지않습니다.
 - 없음 - 추가구성이필요없습니다.
 - WEP
 - WPA/WPA2 개인
 - 임의 (개인)

- WEP 엔터프라이즈
- WPA/WPA2 엔터프라이즈: 최신 Windows 10 릴리스에서는 WPA-2 엔터프라이즈를사용하려면 SCEP 를구 성해야합니다. 그다음 XenMobile 에서장치에인증서를보내 WiFi 서버인증을수행할수있습니다. SCEP 를구 성하려면 설정 > 자격증명공급자의배포페이지로이동합니다. 자세한내용은 [자격증명공급자](#)에서참조하십시오.
- 임의 (엔터프라이즈)

다음섹션에는위의각연결유형에대해구성하는옵션이나열되어있습니다.

iOS 의 WPA, WPA 개인, 임의 (개인) 설정

암호: 선택적암호를입력합니다. 이필드를공백으로두면사용자가로그온할때암호를입력하라는메시지가표시될수있습니다.

iOS 의 WEP 엔터프라이즈, WPA 엔터프라이즈, WPA2 엔터프라이즈, 임의 (엔터프라이즈) 설정

이러한설정중하나를선택하면해당설정이 프록시서버설정뒤에나열됩니다.

- 프로토콜, 허용되는 EAP 유형: 지원할 EAP 유형을사용하도록설정후관련설정을구성합니다. 사용가능한각 EAP 유 형에서기본값은 꺼짐입니다.
- 내부인증 (TTLS): TTLS 를사용하는경우에만필요합니다. 목록에서사용할내부인증방법을선택합니다. 사용가능한옵 션 은 PAP, CHAP, MSCHAP 또는 MSCHAPv2 입니다. 기본값은 MSCHAPv2 입니다.
- 프로토콜, EAP-FAST: PAC(보호액세스자격증명) 를사용할지여부를선택합니다.
 - PAC 사용을선택하는경우프로비저닝 PAC 를사용할지여부를선택합니다.
 - * PAC 프로비전을선택하는경우최종사용자클라이언트와 XenMobile 간에익명 TLS 핸드셰이크를허용할것 인지선택합니다.
 - 익명으로 PAC 프로비전
- 인증:
 - 사용자이름: 사용자이름을입력합니다.
 - 연결별암호: 사용자가로그온할때마다암호를요구할지여부를선택합니다.
 - 암호: 선택적암호를입력합니다. 이필드를공백으로두면사용자가로그온할때암호를입력하라는메시지가표시될수있 습니다.
 - ID 자격증명 (키저장소또는 PKI 자격증명): 목록에서 ID 자격증명의유형을선택합니다. 기본값은 없음입니다.
 - 외부 ID: PEAP, TTLS 또는 EAP-FAST 를 사용하도록설정하는경우에만필요합니다. 외부에표시되는사용자이 름을입력합니다. 사용자이름이표시되지않도록 “익명” 같은일반용어를입력하여보안을강화할수있습니다.
 - TLS 인증서필요: TLS 인증서를요구할지여부를선택합니다.
- 신뢰
 - 신뢰할수있는인증서: 신뢰할수있는인증서를추가하려면 추가를클릭하고추가하려는각인증서에대해다음을수행합 니다.
 - * 응용프로그램: 목록에서추가하려는응용프로그램을선택합니다.
 - * 저장을클릭하여인증서를저장하거나 취소를클릭합니다.
 - 신뢰할수있는서버인증서이름: 신뢰할수있는인증서의일반이름을추가하려면 추가를클릭하고추가하려는각이름에 대해다음을수행합니다.

- * 인증서: 서버인증서의이름을입력합니다. 와일드카드를사용하여 `wpa*.example.com` 과같은이름을지정할수있습니다.
- * 저장을클릭하여인증서이름을저장하거나 취소를클릭합니다.
- 신뢰예외허용: 인증서를신뢰할수없는경우사용자장치에인증서신뢰대화상자를표시할것인지선택합니다. 기본값은 켜짐입니다.
- 프록시서버설정
 - 프록시구성: 목록에서 없음, 수동또는 자동을선택하여 VPN 연결이프록시서버를통해라우팅되는방법을설정한다음추가적인옵션을모두구성합니다. 기본값은 없음이며이경우추가적인구성이필요하지않습니다.
 - 수동을선택하는경우다음설정을구성합니다.
 - * 호스트이름/IP 주소: 프록시서버의호스트이름또는 IP 주소를입력합니다.
 - * 포트: 프록시서버포트번호를입력합니다.
 - * 사용자이름: 프록시서버인증에사용할선택적사용자이름을입력합니다.
 - * 암호: 프록시서버인증에사용할선택적암호를입력합니다.
 - 자동을선택하는경우다음설정을구성합니다.
 - * 서버 URL: 프록시구성을정의하는 PAC 파일의 URL 을입력합니다.
 - * PAC 에연결할수없는경우직접연결허용: PAC 파일에연결할수없는경우대상에직접연결할수있도록할지여부를선택합니다. 기본값은 켜짐입니다. 이옵션은 iOS 7.0 이상에서만사용할수있습니다.

macOS 설정

The screenshot shows the 'Configure' page for a 'WiFi Policy'. The left sidebar has sections for '1 Policy Info', '2 Platforms' (with 'Mac OS X' selected), and '3 Assignment'. The main content area is titled 'WiFi Policy' and includes the following settings:

- Network type:** Standard
- Network name*:** (empty text input)
- Hidden network (enable if network is open or off):** OFF
- Auto join (automatically join this wireless network):** ON
- Security type:** None
- Proxy server settings:** Proxy configuration: None
- Policy Settings:**
 - Remove policy:** Select date (selected), Duration until removal (in days)
 - Allow user to remove policy:** Always
 - Profile scope:** User (OS X 10.7+)

At the bottom, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

- 네트워크유형: 목록에서 표준, 레거시핫스팟또는 **Hotspot 2.0** 을선택하여사용할네트워크유형을설정합니다.
- 네트워크이름: 장치의사용가능한네트워크목록에표시되는 SSID 를입력합니다. **Hotspot 2.0** 에는적용되지않습니다.
- 숨겨진네트워크 (네트워크가열려있거나꺼져있는경우에사용): 네트워크를숨길지여부를선택합니다.
- 자동참가 (이무선네트워크에자동참가): 네트워크를자동으로참가시킬지여부를선택합니다. 장치가이다른네트워크에 연결되어있으면이네트워크에연결되지않습니다. 장치가자동으로연결되기전에사용자가이전네트워크와의연결을끊어야 합니다. 기본값은 켜짐입니다.
- 보안유형: 목록에서사용하려는보안유형을선택합니다. **Hotspot 2.0** 에는적용되지않습니다.
 - 없음 - 추가구성이필요없습니다.
 - WEP
 - WPA/WPA2 개인
 - 임의 (개인)
 - WEP 엔터프라이즈
 - WPA/WPA2 엔터프라이즈
 - 임의 (엔터프라이즈)

다음섹션에는위의각연결유형에대해구성하는옵션이나열되어있습니다.

macOS 의 WPA, WPA 개인, WPA 2 개인, 임의 (개인) 설정

- 암호: 선택적암호를입력합니다. 이필드를공백으로두면사용자가로그온할때암호를입력하라는메시지가표시될수있습니다.

macOS 의 WEP 엔터프라이즈, WPA 엔터프라이즈, WPA2 엔터프라이즈, 임의 (엔터프라이즈) 설정

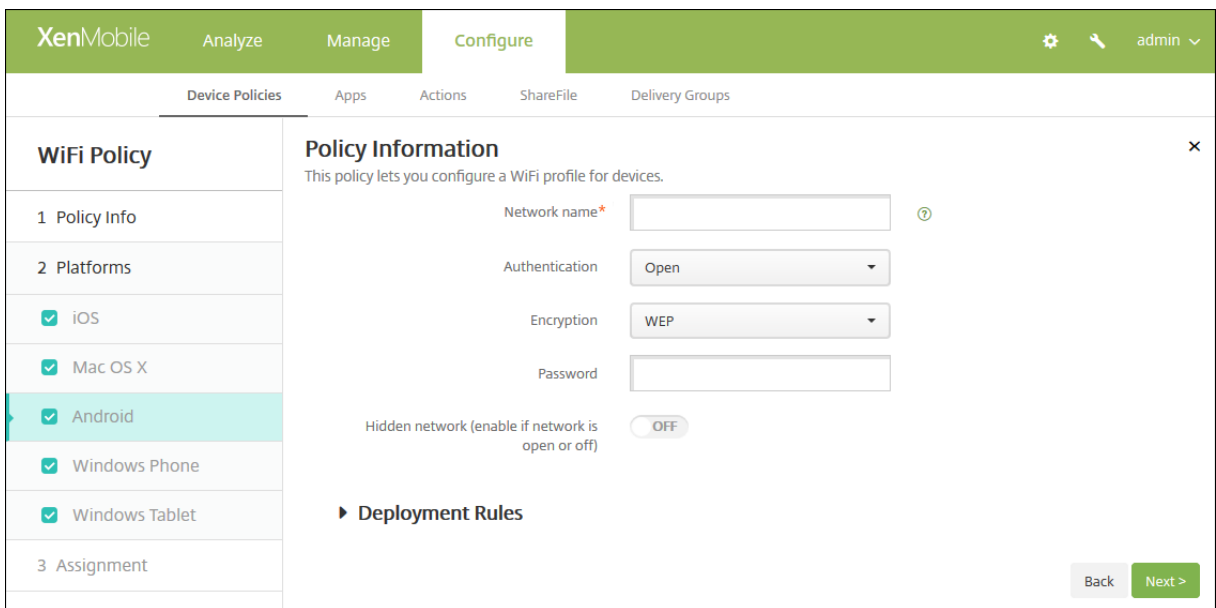
이러한설정중하나를선택하면해당설정이 프록시서버설정뒤에나열됩니다.

- 프로토콜, 허용되는 EAP 유형: 지원할 EAP 유형을사용하도록설정한후관련설정을구성합니다. 사용가능한각 EAP 유형에서기본값은 꺼짐입니다.
- 내부인증 (TTLS): TTLS 를사용하는경우에만필요합니다. 목록에서사용할내부인증방법을선택합니다. 사용가능한옵션은 PAP, CHAP, MSCHAP 또는 MSCHAPv2 입니다. 기본값은 MSCHAPv2 입니다.
- 프로토콜, EAP-FAST: PAC(보호엑세스자격증명) 를사용할지여부를선택합니다.
 - PAC 사용을선택하는경우프로비저닝 PAC 를사용할지여부를선택합니다.
 - * PAC 프로비전을선택하는경우최종사용자클라이언트와 XenMobile 간에익명 TLS 핸드셰이크를허용할것인지선택합니다.
 - 익명으로 PAC 프로비전
- 인증:
 - 사용자이름: 사용자이름을입력합니다.
 - 연결별암호: 사용자가로그온할때마다암호를요구할지여부를선택합니다.
 - 암호: 선택적암호를입력합니다. 이필드를공백으로두면사용자가로그온할때암호를입력하라는메시지가표시될수있습니다.
 - ID 자격증명 (키저장소또는 PKI 자격증명): 목록에서 ID 자격증명의유형을선택합니다. 기본값은 없음입니다.
 - 외부 ID: PEAP, TTLS 또는 EAP-FAST 를 사용하도록설정하는경우에만필요합니다. 외부에표시되는사용자이름을입력합니다. 사용자이름이표시되지않도록 “익명” 같은일반용어를입력하여보안을강화할수있습니다.
 - TLS 인증서필요: TLS 인증서를요구할지여부를선택합니다.
- 신뢰
 - 신뢰할수있는인증서: 신뢰할수있는인증서를추가하려면 추가를클릭하고추가하려는각인증서에대해다음을수행합니다.
 - * 응용프로그램: 목록에서추가하려는응용프로그램을선택합니다.
 - * 저장을클릭하여인증서를저장하거나 취소를클릭합니다.
 - 신뢰할수있는서버인증서이름: 신뢰할수있는인증서의일반이름을추가하려면 추가를클릭하고추가하려는각이름에대해다음을수행합니다.
 - * 인증서: 추가할서버인증서의이름을입력합니다. 와일드카드를사용하여 wpa*.example.com 과같은이름을지정할수있습니다.
 - * 저장을클릭하여인증서이름을저장하거나 취소를클릭합니다.
- 신뢰예외허용: 인증서를신뢰할수없는경우사용자장치에인증서신뢰대화상자를표시할것인지선택합니다. 기본값은 꺼짐입니다.
- 로그인윈도우구성으로사용: 로그인창에입력한자격증명을동일하게사용하여사용자를인증할지여부를선택합니다.

• 프록시서버설정

- 프록시구성: 목록에서 없음, 수동또는 자동을선택하여 VPN 연결이프록시서버를통해라우팅되는방법을설정한다
음추가적인옵션을모두구성합니다. 기본값은 없음이며이경우추가적인구성이필요하지않습니다.
- 수동을선택하는경우다음설정을구성합니다.
 - * 호스트이름/IP 주소: 프록시서버의호스트이름또는 IP 주소를입력합니다.
 - * 포트: 프록시서버포트번호를입력합니다.
 - * 사용자이름: 프록시서버인증에사용할선택적사용자이름을입력합니다.
 - * 암호: 프록시서버인증에사용할선택적암호를입력합니다.
- 자동을선택하는경우다음설정을구성합니다.
 - * 서버 URL: 프록시구성을정의하는 PAC 파일의 URL 을입력합니다.
 - * PAC 에연결할수없는경우직접연결허용: PAC 파일에연결할수없는경우대상에직접연결할수있도록할지여부를선택합니다. 기본값은 켜짐입니다. 이옵션은 iOS 7.0 이상에서만사용할수있습니다.

Android 설정



- 네트워크이름: 사용자장치의사용가능한네트워크목록에있는 SSID 를입력합니다.
- 인증: 목록에서 WiFi 연결에사용할보안유형을선택합니다.
 - 공개
 - 공유
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK
 - 802.1x EAP

다음섹션에는위의각연결유형에대해구성하는옵션이나열되어있습니다.

Android 의공개, 공유설정

- 암호화: 목록에서 사용안함또는 **WEP** 를선택합니다. 기본값은 **WEP** 입니다.
- 암호: 선택적암호를입력합니다.

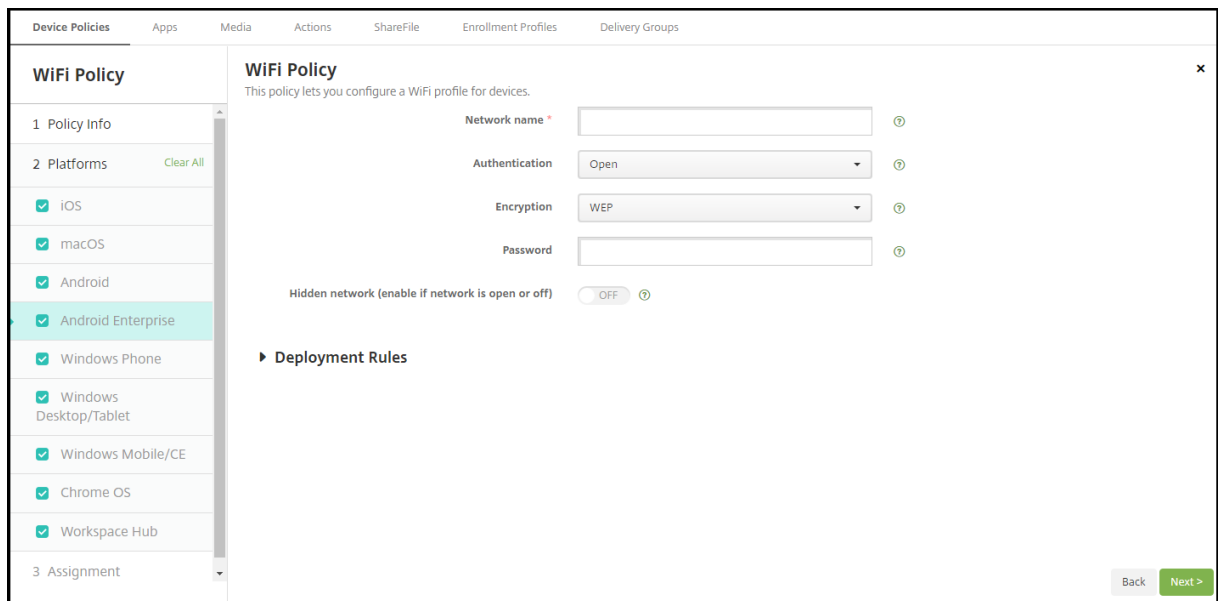
Android 의 WPA, WPA-PSK, WPA2, WPA2-PSK 설정

- 암호화: 목록에서 **TKIP** 또는 **AES** 를선택합니다. 기본값은 **TKIP** 입니다.
- 암호: 선택적암호를입력합니다.

Android 의 802.1x 설정

- **EAP** 유형: 목록에서 **PEAP**, **TLS** 또는 **TTLS** 를선택합니다. 기본값은 **PEAP** 입니다.
- 암호: 선택적암호를입력합니다.
- 인증단계 **2**: 목록에서 없음, **PAP**, **MSCHAP**, **MSCHAPPv2** 또는 **GTC** 를선택합니다. 기본값은 **PAP** 입니다.
- **ID**: 선택적사용자이름및도메인을입력합니다.
- 익명: 외부에표시되는사용자이름을입력합니다. 사용자이름이표시되지않도록 “익명” 같은일반용어를입력하여보안을강화할수있습니다.
- **CA** 인증서: 목록에서사용할인증서를선택합니다.
- **ID** 자격증명: 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
- 숨겨진네트워크 (네트워크가열려있거나꺼져있는경우에사용): 네트워크를숨길지여부를선택합니다.

Android Enterprise 설정



- 네트워크이름: 사용자장치의사용가능한네트워크목록에있는 SSID 를입력합니다.

- 인증: 목록에서 WiFi 연결에 사용할 보안 유형을 선택합니다.
 - 공개
 - 공유
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK
 - 802.1x EAP

다음 섹션에는 위의 각 연결 유형에 대해 구성하는 옵션이 열거되어 있습니다.

Android 의 공개, 공유 설정

- 암호화: 목록에서 사용 안 함 또는 **WEP** 를 선택합니다. 기본값은 **WEP** 입니다.
- 암호: 선택적 암호를 입력합니다.

Android 의 WPA, WPA-PSK, WPA2, WPA2-PSK 설정

- 암호화: 목록에서 TKIP 또는 AES 를 선택합니다. 기본값은 TKIP 입니다.
- 암호: 선택적 암호를 입력합니다.

Android 의 802.1x 설정

- **EAP** 유형: 목록에서 **PEAP**, **TLS** 또는 **TTLS** 를 선택합니다. 기본값은 **PEAP** 입니다.
- 암호: 선택적 암호를 입력합니다.
- 인증단계 **2**: 목록에서 없음, **PAP**, **MSCHAP**, **MSCHAPPv2** 또는 **GTC** 를 선택합니다. 기본값은 **PAP** 입니다.
- **ID**: 선택적 사용자 이름 및 도메인을 입력합니다.
- 익명: 외부에 표시되는 사용자 이름을 입력합니다. 사용자 이름이 표시되지 않도록 “익명” 같은 일반 용어를 입력하여 보안을 강화할 수 있습니다.
- **CA** 인증서: 목록에서 사용할 인증서를 선택합니다.
- **ID** 자격 증명: 목록에서 사용할 ID 자격 증명을 선택합니다. 기본값은 없음입니다.
- 숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용): 네트워크를 숨길지 여부를 선택합니다.

Windows Phone 설정

The screenshot shows the XenMobile configuration interface for a WiFi Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'WiFi Policy' and includes a description: 'This policy lets you configure a WiFi profile for devices.' The configuration fields are as follows:

- Network name ***: A text input field.
- Authentication**: A dropdown menu set to 'Open'.
- Connect if hidden**: A toggle switch set to 'OFF'.
- Connect automatically**: A toggle switch set to 'OFF'.
- Host name or IP address**: A text input field.
- Port**: A text input field.

On the left sidebar, under '1 Policy Info', '2 Platforms', and '3 Assignment', the following options are visible:

- iOS
- macOS
- Android
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

At the bottom of the sidebar, there is a 'Deployment Rules' section with a right-pointing arrow.

- 네트워크이름: 사용자장치의사용가능한네트워크목록에있는 SSID 를입력합니다.
- 인증: 목록에서 WiFi 연결에사용할보안유형을선택합니다.
 - 공개
 - WPA 개인
 - WPA-2 개인
 - WPA-2 엔터프라이즈: 최신 Windows 10 릴리스에서는 WPA-2 엔터프라이즈를사용하려면 SCEP 를구성해야합니다. SCEP 구성을사용하면 XenMobile 에서장치에인증서를보내 WiFi 서버인증을수행할수있습니다. SCEP 를구성하려면 설정 > 자격증명공급자의 배포페이지로이동합니다. 자세한내용은 [자격증명공급자](#)에서참조하십시오.

다음섹션에는위의각연결유형에대해구성하는옵션이나열되어있습니다.

Windows Phone 의공개설정

- 숨겨진경우연결: 숨겨져있는네트워크에연결할지여부를선택합니다.
- 자동연결: 네트워크에자동으로연결할지여부를선택합니다.

Windows Phone 의 WPA 개인, WPA-2 개인설정

- 암호화: 목록에서 **AES** 또는 **TKIP** 를선택하여암호화유형을설정합니다. 기본값은 **AES** 입니다.
- 숨겨진경우연결: 숨겨져있는네트워크에연결할지여부를선택합니다.
- 자동연결: 네트워크에자동으로연결할지여부를선택합니다.

Windows Phone 의 WPA-2 엔터프라이즈설정

- 암호화: 목록에서 **AES** 또는 **TKIP** 를선택하여암호화유형을설정합니다. 기본값은 **AES** 입니다.
- **EAP** 유형: 목록에서 **PEAP-MSCHAPv2** 또는 **TLS** 를선택하여 EAP 유형을설정합니다. 기본값은 **PEAP-MSCHAPv2** 입니다.
- 숨겨진경우연결: 숨겨져있는네트워크에연결할지여부를선택합니다.
- 자동연결: 네트워크에자동으로연결할지여부를선택합니다.
- **SCEP** 를통해인증서푸시: SCEP(단순인증서등록프로토콜) 를통해사용자장치에인증서를푸시할지여부를선택합니다.
- **SCEP** 의자격증명공급자: 목록에서 SCEP 자격증명공급자를선택합니다. 기본값은 없음입니다.
- 프록시서버설정
 - 호스트이름또는 **IP** 주소: 프록시서버의이름또는 IP 주소를입력합니다.
 - 포트: 프록시서버포트번호를입력합니다.

Windows 10 설정

The screenshot shows the XenMobile configuration interface for a WiFi Policy. The left sidebar lists policy sections: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', 'Windows Desktop/Tablet' and 'Windows Mobile/CE' are selected. The main content area shows the 'WiFi Policy' configuration for these platforms. It includes fields for 'Network name', 'Authentication' (set to 'Open'), 'Hidden network' (set to 'OFF'), 'Connect automatically' (set to 'OFF'), 'Host name or IP address', and 'Port'. There is also a 'Deployment Rules' section at the bottom.

- 인증: 목록에서 WiFi 연결에사용할보안유형을클릭합니다.
 - 공개
 - WPA 개인
 - WPA-2 개인
 - WPA 엔터프라이즈
 - WPA-2 엔터프라이즈: 최신 Windows 10 릴리스에서는 WPA-2 엔터프라이즈를사용하려면 SCEP 를구성해야합니다. SCEP 구성을사용하면 XenMobile 에서장치에인증서를보내 WiFi 서버인증을수행할수있습니다. SCEP 를구성하려면 설정 > 자격증명공급자의 배포페이지로이동합니다. 자세한내용은 [자격증명공급자](#)에서참조하십시오.

다음 섹션에는 위의 각 연결 유형에 대해 구성하는 옵션이 열거되어 있습니다.

Windows 10 의 공개 설정

- 숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용): 네트워크를 숨길지 여부를 선택합니다.
- 자동 연결: 네트워크에 자동으로 연결할지 여부를 선택합니다.

Windows 10 의 WPA 개인, WPA-2 개인 설정

- 암호화: 목록에서 **AES** 또는 **TKIP** 를 선택하여 암호화 유형을 설정합니다. 기본값은 **AES** 입니다.
- 숨겨진 네트워크 (네트워크가 열려 있거나 꺼져 있는 경우에 사용): 네트워크를 숨길지 여부를 선택합니다.
- 자동 연결: 네트워크에 자동으로 연결할지 여부를 선택합니다.

Windows 10 의 WPA-2 엔터프라이즈 설정

- 암호화: 목록에서 **AES** 또는 **TKIP** 를 선택하여 암호화 유형을 설정합니다. 기본값은 **AES** 입니다.
- **EAP** 유형: 목록에서 **PEAP-MSCHAPv2** 또는 **TLS** 를 선택하여 EAP 유형을 설정합니다. 기본값은 **PEAP-MSCHAPv2** 입니다.
- 숨겨진 경우 연결: 네트워크를 숨길지 여부를 선택합니다.
- 자동 연결: 네트워크에 자동으로 연결할지 여부를 선택합니다.
- **SCEP** 를 통해 인증서 푸시: SCEP(단순 인증서 등록 프로토콜) 를 통해 사용자 장치에 인증서를 푸시할지 여부를 선택합니다.
- **SCEP** 의 자격 증명 공급자: 목록에서 SCEP 자격 증명 공급자를 선택합니다. 기본값은 없음입니다.

Windows Mobile/CE 설정

The screenshot shows the XenMobile configuration interface for a WiFi Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'WiFi Policy' and includes a description: 'This policy lets you configure a WiFi profile for devices.' The configuration fields are as follows:

- Network name ***: A text input field.
- Device-to-device connection (ad-hoc)**: A toggle switch set to 'OFF'.
- Network**: A dropdown menu set to 'Internet'.
- Authentication**: A dropdown menu set to 'Open'.
- Encryption**: A dropdown menu set to 'WEP'.
- Key provided (automatic)**: A toggle switch set to 'OFF'.
- Password**: A text input field.
- Key index**: A dropdown menu set to '1'.

On the left sidebar, under '1 Policy Info', '2 Platforms', and '3 Assignment', the 'Windows Mobile/CE' checkbox is checked. At the bottom of the main area, there is a 'Deployment Rules' section.

- 네트워크이름: 사용자장치의사용가능한네트워크목록에있는 SSID 를입력합니다.
- 장치간연결 (임시): 두장치를직접연결할수있도록합니다. 기본값은 꺼짐입니다.
- 네트워크: 장치가외부인터넷소스에연결되어있는지, 아니면사무실인트라넷에연결되어있는지를선택합니다.
- 인증: 목록에서 WiFi 연결에사용할보안유형을선택합니다.
 - 공개
 - WPA 개인
 - WPA-2 개인
 - WPA-2 엔터프라이즈

다음섹션에는위의각연결유형에대해구성하는옵션이나열되어있습니다.

Windows Mobile/CE 의공개설정

- 숨겨진네트워크 (네트워크가열려있거나꺼져있는경우에사용): 네트워크를숨길지여부를선택합니다.
- 자동연결: 네트워크에자동으로연결할지여부를선택합니다.

Windows Mobile/CE 의 WPA 개인, WPA-2 개인설정

- 암호화: 목록에서 AES 또는 TKIP 를선택하여암호화유형을설정합니다. 기본값은 AES 입니다.
- 숨겨진네트워크 (네트워크가열려있거나꺼져있는경우에사용): 네트워크를숨길지여부를선택합니다.
- 자동연결: 네트워크에자동으로연결할지여부를선택합니다.

Windows Mobile/CE 의 WPA-2 엔터프라이즈설정

- 암호화: 목록에서 **AES** 또는 **TKIP** 를 선택하여 암호화 유형을 설정합니다. 기본값은 **AES** 입니다.
- **EAP** 유형: 목록에서 **PEAP-MSCHAPv2** 또는 **TLS** 를 선택하여 EAP 유형을 설정합니다. 기본값은 **PEAP-MSCHAPv2** 입니다.
- 숨겨진 경우 연결: 네트워크를 숨길지 여부를 선택합니다.
- 자동 연결: 네트워크에 자동으로 연결할지 여부를 선택합니다.
- **SCEP** 를 통해 인증서 푸시: SCEP(단순 인증서 등록 프로토콜) 를 통해 사용자 장치에 인증서를 푸시할지 여부를 선택합니다.
- **SCEP** 의 자격 증명 공급자: 목록에서 SCEP 자격 증명 공급자를 선택합니다. 기본값은 없음입니다.
- 키 제공 (자동): 자동으로 키를 제공할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 암호: 이 필드에 암호를 입력합니다.
- 키 인덱스: 키 인덱스를 선택합니다. 사용 가능한 옵션은 **1, 2, 3** 및 **4** 입니다.

Windows CE 인증서 장치 정책

January 6, 2020

XenMobile 에서 장치 정책을 만들어 외부 PKI 에서 Windows Mobile/CE 인증서를 만들고 사용자 장치에 제공할 수 있습니다. 인증서 및 PKI 엔터티에 대한 자세한 내용은 [인증서](#) 를 참조하십시오.

이 정책을 추가하거나 구성하려면 구성 > 장치 정책으로 이동합니다. 자세한 내용은 [장치 정책](#) 에서 참조하십시오.

Windows CE 설정

- 자격 증명 공급자: 목록에서 자격 증명 공급자를 클릭합니다. 기본값은 없음입니다.
- 생성된 **PKCS#12** 의 암호: 자격 증명을 암호화하는 데 사용되는 암호를 입력합니다.
- 대상 폴더: 목록에서 자격 증명의 대상 폴더를 클릭하거나 새로 추가를 클릭하여 아직 목록에 없는 폴더를 추가합니다. 미리 정의된 옵션은 다음과 같습니다.
 - %Flash Storage%\
 - %XenMobile Folder%\
 - %Program Files%\
 - %My Documents%\
 - %Windows%\
- 대상 파일 이름: 자격 증명 파일의 이름을 입력합니다.

Windows Information Protection 장치정책

January 6, 2020

이전의 EDP(엔터프라이즈데이터보호) 인 WIP(Windows Information Protection) 는엔터프라이즈데이터의잠재적유출을차단하는 Windows 기술입니다. 데이터유출은엔터프라이즈에서보호되지않는앱, 앱간또는조직네트워크외부로엔터프라이즈데이터를공유하는과정에서발생할수있습니다. 자세한내용은 Microsoft TechNet 에서 [Protect your enterprise data using Windows Information Protection \(WIP\)](#)(WIP(Windows Information Protection) 를사용하여엔터프라이즈데이터보호)을참조하십시오.

XenMobile 에서장치정책을생성하여설정한적용수준의 Windows Information Protection 이필요한앱을지정할수있습니다. Windows Information Protection 정책은 Windows 10 버전 1607 이상의감독되는휴대폰, 태블릿및데스크톱을위한것입니다.

XenMobile 에는자주사용되는앱몇가지가포함되어있으며다른앱도추가할수있습니다. 사용자환경에영향을미치는정책적용수준을지정할수있습니다. 예를들어다음수행할수있습니다.

- 부적절한데이터공유차단
- 부적절한데이터공유에대해경고하고사용자가정책을재정의할수있도록허용
- 부적절한데이터공유를로그하고허용하는동안 WIP 를자동으로실행

Windows Information Protection 에서앱을제외하려면 Microsoft AppLocker XML 파일에서앱을정의한다음이파일을 XenMobile 로가져옵니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Windows 10 설정

File name *	Publisher *	Product name *	Version *	Allowed	Add
iexplore.exe	O=... L=... S=...	*	*	Allowed	
notepad.exe	O=... L=... S=...	*	*	Allowed	

- 데스크톱앱 (Windows 10 태블릿), 스토어앱 (Windows 10 Phone 및태블릿): XenMobile 에는위의샘플처럼몇가지자주사용되는앱이포함되어있습니다. 필요에따라이러한앱을편집하거나제거할수있습니다.
다른앱을추가하려면: 데스크톱앱또는 스토어앱테이블에서 추가를클릭하고앱정보를제공합니다.

허용되는 앱은 엔터프라이즈 데이터를 읽고, 만들고, 업데이트할 수 있습니다. 거부되는 앱은 엔터프라이즈 데이터에 액세스할 수 없습니다. 예외 앱은 엔터프라이즈 데이터를 읽을 수 있지만 데이터를 만들거나 수정할 수는 없습니다.

- **AppLocker XML:** Microsoft 는 WIP 와 호환성 문제가 있는 것으로 알려진 Microsoft 앱의 목록을 제공합니다. 이러한 앱을 WIP 에서 제외하려면 찾아보기를 클릭하고 목록을 업로드합니다. XenMobile 은 업로드된 AppLocker XML 과 구성된 데스크톱 및 스토어 앱을 장치로 전송된 정책에서 결합합니다. 자세한 내용은 [Recommended deny list for Windows Information Protection\(Windows Information Protection 에 대한 권장 거부 목록\)](#)에서 참조하십시오.
- **적용 수준:** Windows Information Protection 이 데이터 공유를 보호하고 관리할 방식을 지정하는 옵션을 선택합니다. 기본값은 꺼짐입니다.
 - * **0-꺼짐:** WIP 가 꺼지면 데이터를 보호 또는 감사하지 않습니다.
 - * **1-무음:** WIP 가 자동으로 실행되면 서부적절한 데이터 공유를 기록하고 아무 것도 차단하지 않습니다. [Reporting CSP\(보고 CSP\)](#)를 통해 로그에 액세스할 수 있습니다.
 - * **2-재정의:** WIP 가 잠재적으로 안전하지 않은 데이터 공유에 대해 사용자에게 경고합니다. 사용자는 경고를 재정의하고 데이터를 공유할 수 있습니다. 이 모드는 사용자 재정의의 포함 작업을 감사 로그에 기록합니다.
 - * **3-차단:** WIP 는 사용자가 안전하지 않을 수 있는 데이터 공유를 수행하는 것을 차단합니다.
- **보호되는 도메인 이름:** 엔터프라이즈가 사용자 ID 에 사용하는 도메인입니다. 관리되는 ID 도메인의 목록은 기본 도메인과 함께 관리 엔터프라이즈의 ID 를 구성합니다. 목록에서 첫 번째 도메인은 Windows UI 에 사용되는 기본 회사 ID 입니다. “|”를 사용하여 목록 항목을 구분합니다. 예를 들면 다음과 같습니다. `domain1.com | domain2.com`
- **데이터 복구 인증서:** 찾아보기를 클릭한 다음 암호화된 파일의 데이터 복구에서 사용할 복구 인증서를 선택합니다. 이 인증서는 그룹 정책이 아니라 MDM 을 통해 배달된다는 점 이외에는 EFS(암호화 파일 시스템) 에 대한 DRA(데이터 복구 에이전트) 와 동일합니다. 복구 인증서를 사용할 수 없는 경우 새로 만듭니다. 자세한 내용은 이 섹션의 “데이터 복구 인증서 만들기” 를 참조하십시오.
- **네트워크 도메인 이름:** 엔터프라이즈의 경계를 구성하는 도메인의 목록입니다. WIP 는 목록의 정규화된 도메인에 대한 모든 트래픽을 보호합니다. 이 설정은 **IP** 범위 설정과 함께 사용되어 네트워크 끝점이 엔터프라이즈 인지가 아니면 사설망의 개인 인지를 감지합니다. 심표를 사용하여 목록 항목을 구분합니다. 예: `corp.example.com, region.example.com`
- **IP 범위:** 엔터프라이즈 네트워크의 컴퓨터를 정의하는 엔터프라이즈 IPv4 및 IPv6 범위의 목록입니다. WIP 는 이러한 위치를 엔터프라이즈 데이터를 공유해도 안전한 대상으로 고려합니다. 심표를 사용하여 목록 항목을 구분합니다. 예를 들면 다음과 같습니다.
`10.0.0.0-10.255.255.255, 2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **IP 범위 목록을 신뢰할 수 있음:** Windows 에 의한 IP 범위의 자동 감지를 방지하려면 이 설정을 켜짐으로 변경합니다. 기본값은 꺼짐입니다.

- **프록시서버:** 엔터프라이즈가회사리소스에서사용할수있는프록시서버의목록입니다. 네트워크에서프록시를사용하는 경우가설정이필요합니다. 프록시서버가없으면프록시뒤에있는클라이언트가엔터프라이즈리소스를사용하지못할 수있습니다. 예를들어호텔및식당의특정 WiFi 핫스팟에서리소스를사용하지못할수있습니다. 심표를사용하여목록 항목을구분합니다. 예를들면다음과같습니다.

`proxy.example.com:80;157.54.11.118:443`

- **내부프록시서버:** 장치가클라우드리소스에연결하기위해통과하는프록시서버의목록입니다. 이서버유형을사용하면, 연결하는클라우드리소스가엔터프라이즈리소스임을나타냅니다. 이목록에 WIP 비보호트래픽에사용되는 프록시서버설정의서버를포함하지마십시오. 심표를사용하여목록항목을구분합니다. 예를들면다음과같습니다.

`example.internalproxy1.com;10.147.80.50`

- **클라우드리소스:** WIP 로보호되는클라우드리소스의목록입니다. 원하는경우각클라우드리소스에대해, 이클라우드리소스에대한트래픽을라우팅할 프록시서버목록의프록시서버를지정할수도있습니다. 프록시서버를통해라우팅되는모든트래픽은엔터프라이즈트래픽으로취급됩니다. 심표를사용하여목록항목을구분합니다. 예를들면다음과같습니다.

`domain1.com:InternalProxy.domain1.com, domain2.com:InternalProxy.domain2.com`

- **잠금보호필요설정:** Windows 10 Phone 전용입니다. 커짐인경우암호장치정책도필요합니다. 그렇지않으면 Windows Information Protection 정책배포가실패합니다. 또한정책이 커짐이면 잠금을통한보호필요설정이나타납니다. 기본값은 꺼짐입니다.
- **잠금을통한보호필요:** Windows 10 Phone 전용입니다. 잠긴장치에서직원 PIN 으로보호되는키를사용하여엔터프라이즈데이터를암호화할지여부를지정합니다. 앱은잠긴장치의회사데이터를읽을수없습니다. 기본값은 꺼짐입니다.
- **등록취소할때 WIP 인증서해지:** Windows Information Protection 에서등록취소될때사용자장치에서로컬암호화키를해지할지여부를지정합니다. 암호화키가해지되면사용자는암호화된회사데이터에액세스할수없습니다. 꺼짐인경우키가해지되지않으며사용자는등록취소후에도보호된파일에계속액세스할수있습니다. 기본값은 꺼짐입니다.
- **오버레이아이콘표시:** 탐색기의회사파일및시작메뉴의엔터프라이즈전용앱타일에 Windows Information Protection 아이콘오버레이를포함할지여부를지정합니다. 기본값은 꺼짐입니다.

데이터복구인증서만들기

Windows Information Protection 정책을사용하도록설정하려면데이터복구인증서가필요합니다.

1. XenMobile Server 에서명령프롬프트를열고인증서를만들려는폴더 (Windows\System32 이외의폴더) 로이동합니다.
2. 다음명령을실행합니다.

`cipher /r:ESFDRA`

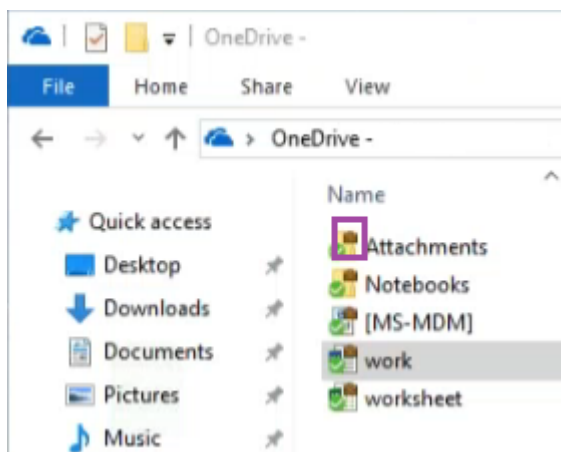
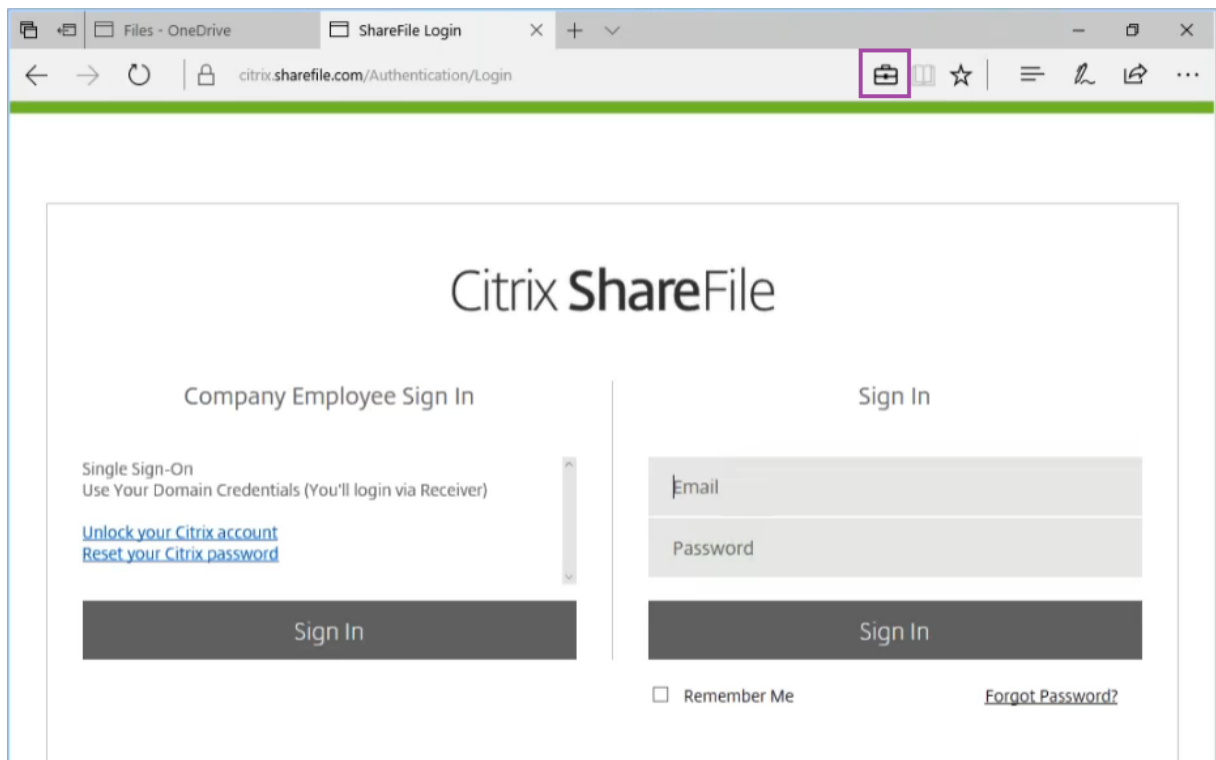
3. 메시지가 나타나면 개인키 파일을 보호하기 위한 암호를 입력합니다.

암호화 명령은 .cer 및 .pfx 파일을 생성합니다.

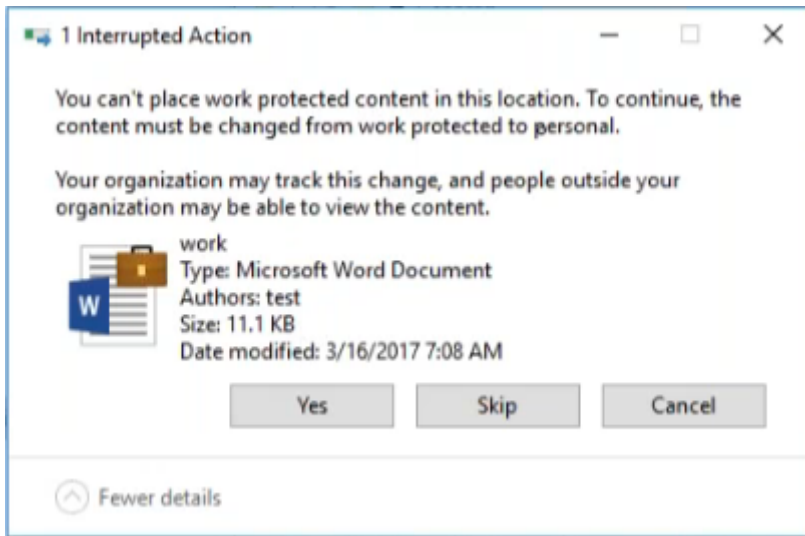
4. XenMobile 콘솔에서 설정 > 인증서로 이동하고 Windows 10 태블릿과 휴대폰 모두에 적용되는 .cer 파일을 가져옵니다.

사용자 환경

Windows Information Protection 이 적용될 때는 앱과 파일에 다음 아이콘이 포함됩니다.



사용자가 보호되는 파일을 보호되지 않는 위치로 복사하거나 저장할 경우 구성된 적용 수준에 따라 다음 알림이 나타납니다.



XenMobile 옵션장치정책

January 6, 2020

Android 및 Windows Mobile/CE 장치에서 XenMobile 에연결할때 Secure Hub 동작을구성하는 XenMobile 옵션정책을추가합니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Android 설정

- 트레이표시줄알림 - 트레이표시줄아이콘숨기기: 트레이표시줄아이콘을표시할지, 아니면숨길지를선택합니다. 기본값은 꺼짐입니다.
- 연결시간제한: 연결시간이초과되기전에연결이유휴상태로있을수있는시간 (초) 을입력합니다. 기본값은 20 초입니다.
- 연결유지간격: 연결을유지할시간 (초) 을입력합니다. 기본값은 120 초입니다.
- 원격제어를허용하기전에사용자에게확인: 원격지원제어를허용하기전에사용자에게물어볼지여부를선택합니다. 기본값은 꺼짐입니다.
- 파일전송이전: 목록에서사용자에게파일전송에대해경고할지, 아니면사용자에게허락을요청할지를클릭합니다. 사용가능한값은 사용자에게경고표시안함, 사용자에게경고표시및 사용자권한요청입니다. 기본값은 사용자에게경고표시안함입니다.

Windows Mobile/CE 설정

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'XenMobile Options Policy' and includes a description: 'This policy lets you configure parameters for connections to XenMobile.' The configuration is divided into three main sections: 'Device agent configuration', 'Remote support', and 'Deployment Rules'. The 'Device agent configuration' section includes:

- XenMobile backup configuration: Disabled (dropdown)
- Connect to the office network: ON (toggle)
- Connect to the Internet network: ON (toggle)
- Connect to the built-in office network: ON (toggle)
- Connect to the built-in Internet network: ON (toggle)
- Traybar notification - hide traybar icon: OFF (toggle)
- Connection time-out(s)*: 20 (input field)
- Keep-alive interval(s)*: 120 (input field)

 The 'Remote support' section includes:

- Prompt the user before allowing remote control: OFF (toggle)
- Before a file transfer: Do not warn the user (dropdown)

 The 'Deployment Rules' section is currently collapsed. At the bottom right, there are 'Back' and 'Next >' buttons.

- 장치에이전트구성
 - **XenMobile** 백업구성: 목록에서, 사용자장치에서 XenMobile 구성을백업하는것에대한옵션을클릭합니다. 기본값은 사용안함입니다. 다음과같은옵션을사용할수있습니다.
 - * 사용안함
 - * XenMobile 설치후첫번째연결시
 - * 각장치다시시작후첫번째연결시

- 사무실네트워크에연결
- 인터넷네트워크에연결
- 기본제공사무실네트워크에연결: 커짐으로설정된경우 XenMobile 이네트워크를자동으로감지합니다.
- 기본제공인터넷네트워크에연결: 커짐으로설정된경우 XenMobile 이네트워크를자동으로감지합니다.
- 트레이표시줄알림 - 트레이표시줄아이콘숨기기: 트레이표시줄아이콘을표시할지, 아니면숨길지를선택합니다. 기본값은 꺼짐입니다.
- 연결시간제한: 연결시간이초과되기전에연결이유휴상태로있을수있는시간 (초) 을입력합니다. 기본값은 20 초입니다.
- 연결유지간격: 연결을유지할시간 (초) 을입력합니다. 기본값은 120 초입니다.
- 원격지원
 - 원격제어를허용하기전에사용자에게확인: 원격지원제어를허용하기전에사용자에게물어볼지여부를선택합니다. 기본값은 꺼짐입니다.
 - 파일전송이전: 목록에서사용자에게파일전송에대해경고할지, 아니면사용자에게허락을요청할지를클릭합니다. 사용가능한값은 사용자에게경고표시안함, 사용자에게경고표시및 사용자권한요청입니다. 기본값은 사용자에게경고표시안함입니다.

XenMobile 제거장치정책

January 6, 2020

XenMobile 에서장치정책을추가하여 Android and Window Mobile/CE 장치에서 XenMobile 을제거할수있습니다. 이 정책을배포하면배포그룹에있는모든장치에서 XenMobile 이제거됩니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 [장치정책](#)에서참조하십시오.

Android 및 Windows Mobile/CE 설정구성

- 장치에서 **XenMobile** 제거: 이정책을배포할모든장치에서 XenMobile 을제거할지여부를선택합니다. 기본값은 꺼짐입니다.

앱추가

January 6, 2020

XenMobile 에관리할앱을추가합니다. XenMobile 콘솔에앱을추가한다음앱을범주로정렬하고사용자에게배포할수있습니다.

다음유형의앱을 XenMobile 에추가할수있습니다.

- **MDX.** MDX Toolkit 으로래핑된앱입니다. 내부및공용스토어에서얻은 MDX 앱을배포할수있습니다.

- 공용앱스토어, iTunes 또는 Google Play 와같은공용앱스토어에서무료또는유료로제공되는앱이포함됩니다. 예를들여 GoToMeeting 이포함됩니다.
- 웹및 **SaaS**. 내부네트워크에서액세스되는앱 (웹앱) 또는공용네트워크를통해액세스되는앱 (SaaS) 이포함됩니다. 자체앱을만들거나기존웹앱에대한 Single Sign-On 인증을위해앱커넥터집합에서선택할수있습니다. GoogleApps_SAML 을예로들수있습니다.
- 엔터프라이즈. MDX Toolkit 으로래핑되지않고 MDX 앱과관련된정책이포함되지않은기본앱입니다.
- 웹링크. 이러한앱은 Single Sign-On 이필요없는웹앱이나공용또는개인사이트에대한웹주소 (URL) 입니다.

자동설치정보

Citrix 는 iOS 및 Samsung Android 앱의자동설치를지원합니다. 자동설치에서는장치에배포한앱을설치하라는메시지가사용자에게표시되지않습니다. 앱이백그라운드에서자동으로설치됩니다.

자동설치를구현하기위한필수구성요소:

- iOS 앱의경우관리되는 iOS 장치를감독모드로전환합니다. 자세한내용은 [iOS 및 macOS 프로필장치정책가져오기](#)에 참조하십시오.
- Android 앱의경우장치에서 SAFE(Samsung for Enterprise) 또는 KNOX 정책을사용하도록설정합니다. 이작업을수행하려면 Samsung MDM 라이선스키장치정책을설정하여 Samsung ELM 및 KNOX 라이선스키를생성합니다. 자세한내용은 [Samsung MDM 라이선스키장치정책](#)에서참조하십시오.

모바일및 MDX 앱의작동방식

XenMobile 은 Secure Hub, Secure Mail 및 Secure Web 과같은모바일생산성앱을포함하여 iOS 및 Android 앱을지원하며 MDX 정책사용도지원합니다. XenMobile 콘솔에서앱을업로드한다음사용자장치에제공할수있습니다. 모바일생산성앱에더해다음유형의앱을추가할수있습니다.

- 사용자용으로개발한앱
- MDX 정책을사용하여장치기능을허용하거나제한하려는앱

모바일생산성앱을배포하려면다음일반단계를수행하십시오.

1. <https://www.citrix.com/downloads/citrix-endpoint-management/product-software/xenmobile-enterprise-edition-worx-apps-and-mdx-toolkit.html>에서공용스토어 MDX 파일을다운로드합니다.
2. 필요에따라 MDX 정책을업데이트하고이러한파일을 XenMobile 콘솔에업로드합니다 (구성 > 앱).
3. MDX 파일을공용앱스토어에업로드합니다. 자세한내용은이문서에서MDX 앱추가를참조하십시오.

MDX Toolkit 은 iOS 및 Android 장치용앱을 Citrix 로직및정책으로래핑합니다. 이도구를사용하면조직내에서만들거나회사외부에서만들어진앱을안전하게래핑할수있습니다.

필수앱과선택적앱정보

배달그룹에앱을추가하는경우선택적앱인지, 아니면필수앱인지를선택해야합니다. 필수로표시된앱의경우사용자는다음과같은경우에곧바로업데이트를받을수있습니다.

- 사용자가새앱을업로드하고필수앱으로표시합니다.
- 사용자가기존앱을필수앱으로표시합니다.
- 사용자가필수앱을삭제합니다.
- Secure Hub 업데이트가제공됩니다.

필수앱의강제배포를위한요구사항

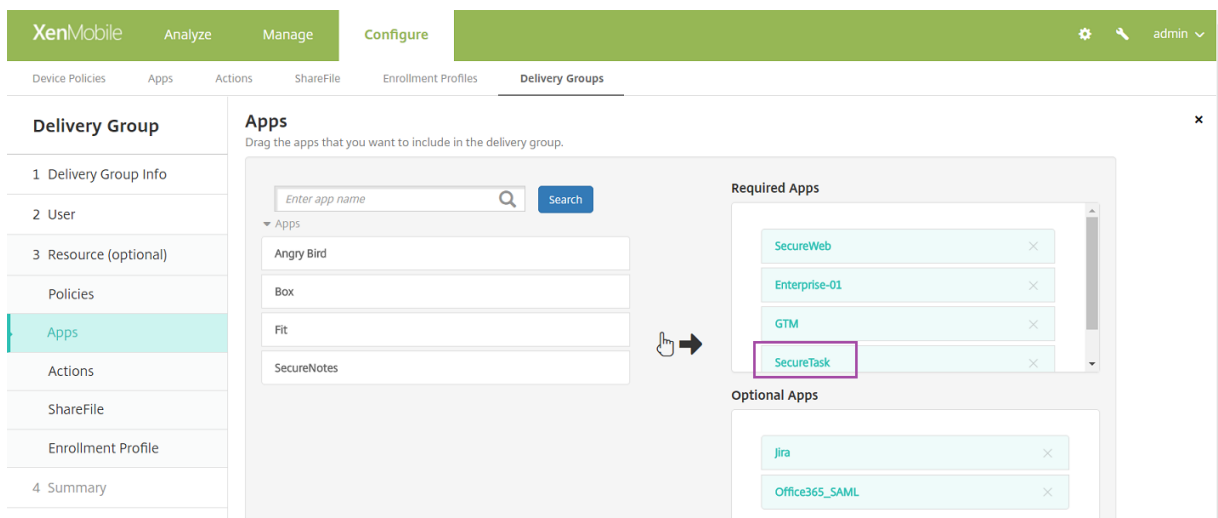
- XenMobile Server 10.6(최소버전)
- Secure Hub 10.5.15(iOS 의경우) 및 10.5.20(Android 의경우)(최소버전)
- MDX Toolkit 10.6(최소버전)
- 사용자지정서버속성, `force.server.push.required.apps`.

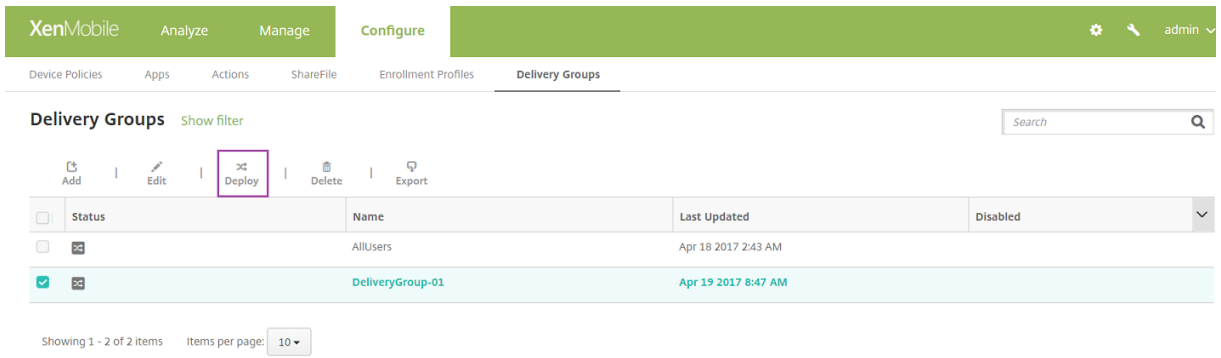
필수앱의강제배포가기본적으로사용되지않도록설정됩니다. 이기능을사용하도록설정하려면사용자지정키서버속성을만드십시오. 키및 표시이름을 **force.server.push.required.apps** 로설정하고 값을 **true** 로설정합니다.

- XenMobile Server 및 Secure Hub 업그레이드후: 등록된장치가있는사용자는로그오프후 Secure Hub 에로그온하여필수앱배포업데이트를받아야합니다.

예제

다음예제에는 Secure Tasks 앱을배달그룹에추가한후배달그룹을배포하는작업의순서가나와있습니다.





샘플앱인 **Secure Tasks** 가사용자장치에배포되면 **Secure Hub** 가앱을설치하라는메시지를표시합니다.

중요:

엔터프라이즈앱과공용앱스토어앱을포함하여 MDX 를사용하도록설정된필수앱의경우 MDX 정책예업데이트유예기간을구성하고사용자가앱을나중에업그레이드하기로선택한경우에도즉시업그레이드하십시오.

엔터프라이즈및공용스토어앱을위한 **iOS** 필수앱워크플로

1. 초기등록중에 XenMobile App 을배포합니다. 필수앱이장치에설치됩니다.
2. XenMobile 콘솔에서앱을업데이트합니다.
3. XenMobile 콘솔에서필수앱을배포합니다.
4. 홈화면의앱이업데이트됩니다. 또한공용스토어앱의경우업그레이드가자동으로시작됩니다. 사용자에게업데이트하라는메시지가표시되지않습니다.
5. 사용자가홈화면에서앱을업니다. 앱업데이트유예기간을설정했다라도사용자가나중에앱을업그레이드하기위해누르면앱이곧바로업그레이드됩니다.

엔터프라이즈앱을위한 **Android** 필수앱워크플로

1. 초기등록중에 XenMobile App 을배포합니다. 필수앱이장치에설치됩니다.
2. XenMobile 콘솔에서필수앱을배포합니다.
3. 앱이업그레이드됩니다. (Nexus 장치에서는업데이트를설치하라는메시지가표시되지만 Samsung 장치에서는자동설치됩니다.)
4. 사용자가홈화면에서앱을업니다. 앱업데이트유예기간을설정했다라도사용자가나중에앱을업그레이드하기위해누르면앱이곧바로업그레이드됩니다. (Samsung 장치에서는자동설치가수행됩니다.)

공용스토어앱을위한 **Android** 필수앱워크플로

1. 초기등록중에 XenMobile App 을배포합니다. 필수앱이장치에설치됩니다.
2. XenMobile 콘솔에서앱을업데이트합니다.

3. XenMobile 콘솔에서 필수 앱을 배포합니다. 또는 장치에서 Secure Hub 스토어를 엽니다. 스토어에 업데이트 아이콘이 나타납니다.
4. 앱 업그레이드가 자동으로 시작됩니다. (Nexus 장치에서는 업데이트를 설치하라는 메시지가 표시됩니다.)
5. 홈 화면에서 앱을 엽니다. 앱이 업그레이드됩니다. 유예 기간 동안 사용자에게 메시지가 표시되지 않습니다. (Samsung 장치에서는 자동 설치가 수행됩니다.)

웹 및 SaaS 앱의 작동 방식

XenMobile 은 웹 및 SaaS 앱에 대한 SSO(Single Sign-On) 에 구성할 수 있는 템플릿 인 응용 프로그램 커넥터 집합과 함께 제공됩니다. 경우에 따라 템플릿을 구성하여 사용자 계정 생성 및 관리에 사용할 수 있습니다. XenMobile 에는 SAML(Security Assertion Markup Language) 커넥터가 포함됩니다. SAML 커넥터는 SSO 및 사용자 계정 관리에 SAML 프로토콜을 지원하는 웹 응용 프로그램에 사용됩니다. XenMobile 은 SAML 1.1 및 SAML 2.0 을 지원합니다.

또한 회사 고유의 SAML 커넥터를 만들 수도 있습니다.

엔터프라이즈 앱의 작동 방식

엔터프라이즈 응용 프로그램은 일반적으로 내부 네트워크에 상주합니다. 사용자는 Secure Hub 를 사용하여 앱에 연결할 수 있습니다. 엔터프라이즈 앱을 추가하면 XenMobile 이 앱에 대한 앱 커넥터를 만듭니다.

공용 앱 스토어의 작동 방식

Apple App Store 및 Google Play 에서 앱 이름 및 설명을 검색하는 설정을 구성할 수 있습니다. 스토어에서 앱 정보를 검색하면 XenMobile 이 기존 이름과 설명을 덮어 씁니다.

웹 링크의 작동 방식

웹 링크는 인터넷 또는 인트라넷 사이트에 대한 웹 주소입니다. 웹 링크는 SSO 가 필요하지 않은 웹 응용 프로그램을 가리킬 수도 있습니다. 웹 링크 구성을 마치면 링크가 XenMobile Store 에서 아이콘으로 표시됩니다. 사용자가 Secure Hub 에 로그인하면 사용 가능한 앱 및 데스크톱의 목록과 함께 링크가 표시됩니다.

MDX 앱 추가

iOS 또는 Android 장치에서 사용할 수 있는 래핑된 MDX 모바일 앱을 받은 경우 해당 앱을 XenMobile 에 업로드할 수 있습니다. 앱을 업로드한 후 앱 세부 및 정책 설정을 구성할 수 있습니다. 각 장치 플랫폼 유형에서 사용할 수 있는 앱 정책에 대한 자세한 내용은 [MDX 정책 요약](#) 을 참조하십시오. 해당 섹션에서 자세한 정책 설명도 확인할 수 있습니다.

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 나타납니다.

Apps Show filter <input type="text" value="Search"/>							
<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable <input type="checkbox"/>
<input type="checkbox"/>		Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
<input type="checkbox"/>		Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
<input type="checkbox"/>		Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>

2. 추가를 클릭합니다. 앱추가대화상자가 나타납니다.

Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. **MDX** 를 클릭합니다. **MDX** 앱정보페이지가 나타납니다.

4. 앱정보창에서 다음정보를 입력합니다.

- 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱테이블의 앱이름아래에 표시됩니다.
- 설명: 앱의 선택적 설명을 입력합니다.
- 앱범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 만들기를 참조하십시오.

5. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.

6. 플랫폼 아래에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼에 대해서만 구성하는 경우 다른 플랫폼의 선택을 취소합니다.

플랫폼 설정 구성을 마치면 11 단계에서 플랫폼 배포 규칙을 설정하는 방법을 참조하십시오.

7. 업로드할 MDX 파일을 선택하려면 업로드를 클릭하고 파일의 위치로 이동합니다.

- iOS VPP B2B 앱을 추가하는 경우 응용 프로그램이 **VPP B2B** 응용 프로그램입니까? 를 클릭합니다. 그런 다음 목록에서 사용할 B2B VPP 계정을 클릭합니다.

8. 다음을 클릭합니다. 앱 세부 정보 페이지가 나타납니다.

9. 다음설정을구성합니다.

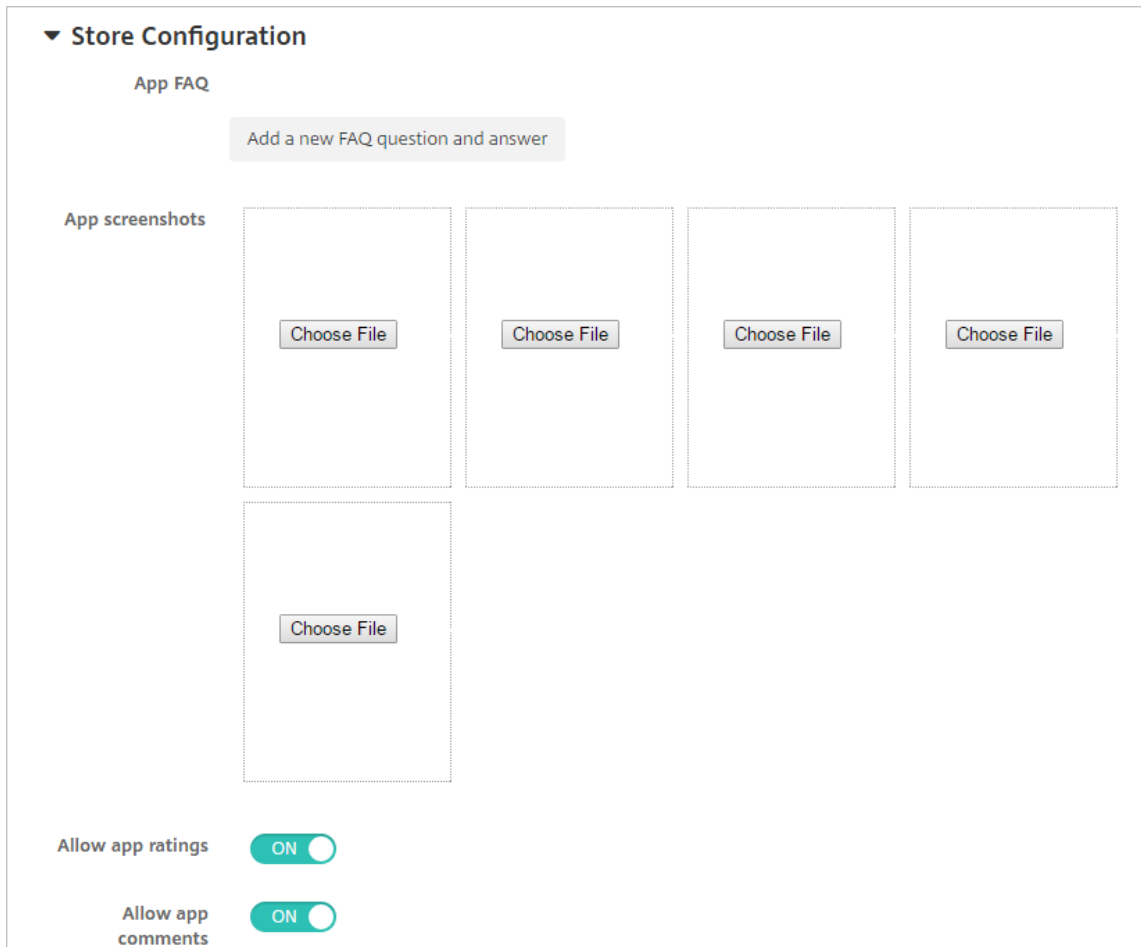
- 파일이름: 앱에연결된파일이름을입력합니다.
- 앱설명: 앱에대한설명을입력합니다.
- 앱버전: 필요한경우앱버전번호를입력합니다.
- 최소 OS 버전: 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
- 최대 OS 버전: 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
- 제외된장치: 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.
- MDM 프로필이제거된경우앱제거: MDM 프로필이제거된경우장치에서앱을제거할지여부를선택합니다. 기본값은 켜짐입니다.
- 업데이트백업방지: 사용자가업데이트를백업하는것을방지할지여부를선택합니다. 기본값은 켜짐입니다.
- 강제로앱관리: 앱이관리되지않는앱으로설치될경우감독되지않는장치에서해당앱의관리를허용할것인지문는메시지를표시할지여부를선택합니다. 기본값은 켜짐입니다. iOS 9.0 이상에서사용할수있습니다.
- VPP 를통해배포된앱: VPP 를사용하여앱을배포할지여부를선택합니다. 켜짐인경우앱의 MDX 버전을배포하고 VPP 를사용하여앱을배포하면 Secure Hub 에 VPP 인스턴스만표시됩니다. 기본값은 꺼짐입니다.

10. MDX 정책을구성합니다. MDX 정책은플랫폼별로다르며인증, 장치보안, 암호화, 앱상호작용및앱제한과같은정책영역에 대한옵션이포함됩니다. 콘솔에서각정책에는정책을설명하는도구설명이포함됩니다.

MDX 앱에대한앱정책에대해서는 [MDX 정책요약](#)을참조하십시오. 이문서에는각플랫폼에적용할정책이표시된표가포함되어있습니다.

11. 배포규칙을구성합니다. 자세한내용은 [리소스배포](#)에서참조하십시오.

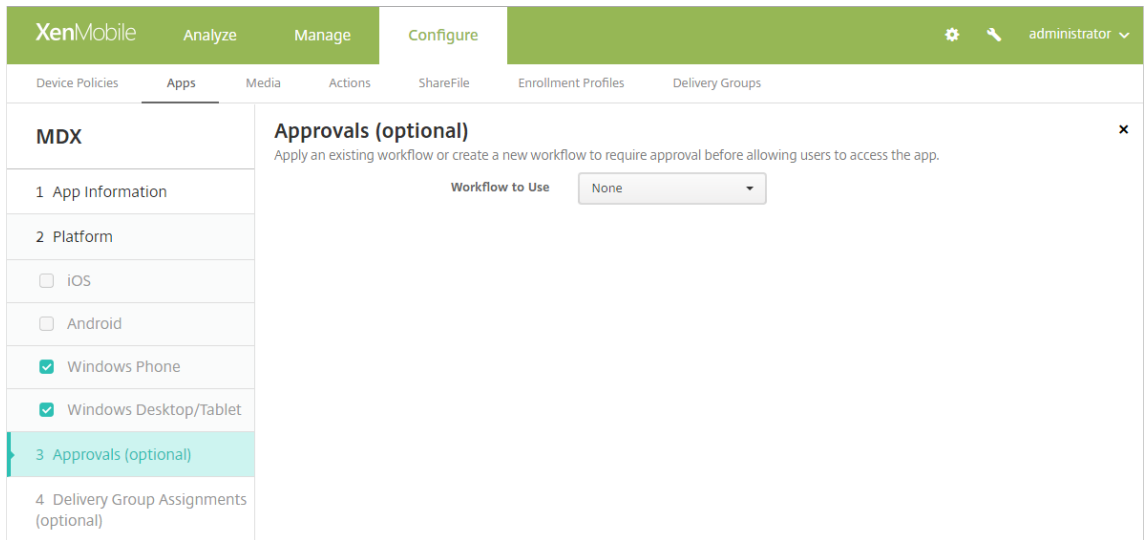
12. XenMobile Store 구성을확장합니다.



필요한 경우 XenMobile Store 에 나타나는 앱 또는 화면 캡처에 대한 FAQ 를 추가할 수 있습니다. 또한 사용자의 앱 평가 또는 설명 추가를 허용할지 여부를 설정할 수 있습니다.

- 다음 설정을 구성합니다.
 - 앱 **FAQ**: 앱에 대한 FAQ(질문과 답변) 를 추가합니다.
 - 앱 스크린샷: XenMobile Store 의 앱을 분류하는데 도움이 되는 화면 캡처를 추가합니다. 업로드하는 그래픽은 PNG 여야 합니다. GIF 또는 JPEG 이미지는 업로드할 수 없습니다.
 - 앱 등급 허용: 사용자의 앱 평가를 허용할지 여부를 선택합니다. 기본값은 켜져 있습니다.
 앱 설명 허용: 선택한 앱에 대한 사용자의 설명을 허용할지 여부를 선택합니다. 기본값은 켜져 있습니다.

13. 다음을 클릭합니다. 승인 페이지가 나타납니다.

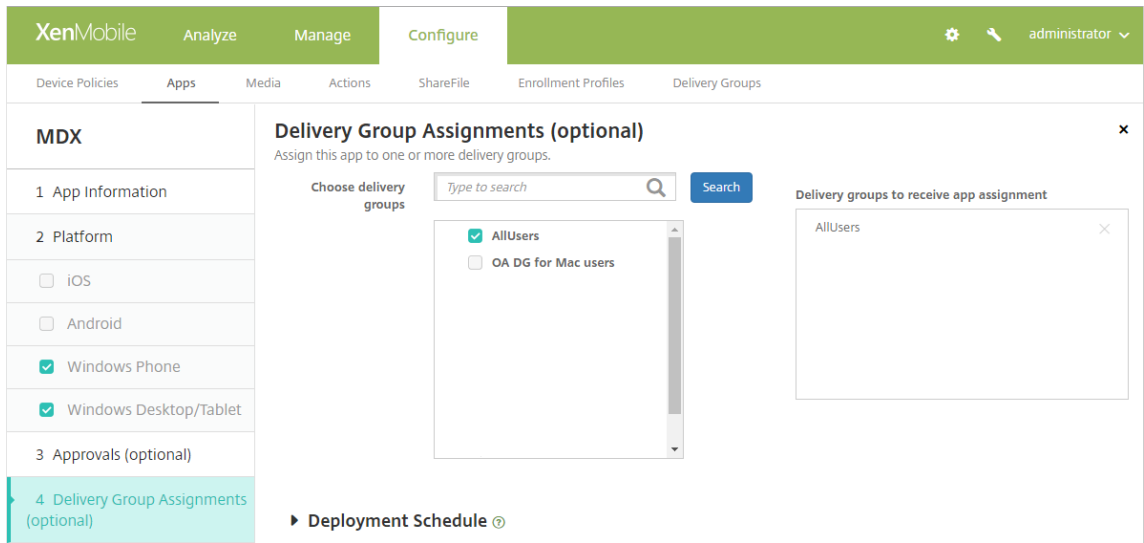


사용자계정을 만들때 승인이 필요한 경우 워크플로를 사용합니다. 승인 워크플로를 설정하지 않아도 되는 경우 15 단계로 건너뛸 수 있습니다.

다음 설정을 구성하여 워크플로를 할당하거나 만듭니다.

- 사용할 워크플로: 목록에서 기존 워크플로를 클릭하거나 새 워크플로 만들기를 클릭합니다. 기본값은 없음입니다.
- 새 워크플로 만들기를 선택하는 경우 다음 설정을 구성합니다. 자세한 내용은 워크플로 만들기 및 관리에서 참조하십시오.
- 이름: 워크플로의 고유한 이름을 입력합니다.
- 설명: 필요한 경우 워크플로의 설명을 입력합니다.
- 전자메일 승인 템플릿: 목록에서 할당할 전자메일 승인 템플릿을 선택합니다. 이 필드 오른쪽에 있는 눈모양 아이콘을 클릭하면 템플릿을 미리 볼 수 있는 대화상자가 나타납니다.
- 관리자 승인 수준: 목록에서 이 워크플로에 필요한 관리자 승인 수준의 번호를 선택합니다. 기본값은 1 수준입니다. 가능한 옵션은 다음과 같습니다.
 - 필요없음
 - 1 수준
 - 2 수준
 - 3 수준
- **Active Directory** 도메인 선택: 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
- 추가로 필요한 승인자 찾기: 검색 필드에 추가로 필요한 사람의 이름을 입력하고 검색을 클릭합니다. 이름은 Active Directory 에서 가져옵니다.
- 필드에 이름이 나타나면 해당하는 이름 옆의 확인란을 선택합니다. 이름과 전자메일 주소가 추가로 필요한 승인자 선택된 목록에 나타납니다.
 - 추가로 필요한 승인자 선택된 목록에서 사용자를 제거하려면 다음 중 하나를 수행합니다.
 - * 선택한 도메인에 있는 모든 사용자의 목록을 표시하려면 검색을 클릭합니다.
 - * 검색 결과를 제한하려면 검색 상자에 이름 전체 또는 일부를 입력한 다음 검색을 클릭합니다.
 - * 추가로 필요한 승인자 선택된 목록에 있는 사용자는 검색 결과 목록에서 해당 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하고 제거하려는 각 이름 옆에 있는 확인란의 선택을 취소합니다.

14. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.



15. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.
16. 배포일정을확장하고다음설정을구성합니다.

- 배포옆에서 켜짐을클릭하여배포를예약하거나 꺼짐을클릭하여배포를차단합니다. 기본옵션은 켜짐입니다.
- 배포일정옆에서 지금또는 나중에를클릭합니다. 기본옵션은 지금입니다.
- 나중에를클릭하는경우달력아이콘을클릭하고배포날짜와시간을선택합니다.
- 배포조건옆에서 모든연결에서를클릭하거나 이전배포가실패한경우에만을클릭합니다. 기본옵션은 모든연결에서입니다.
- 상시연결에대해배포옆에서 켜짐또는 꺼짐을클릭합니다. 기본옵션은 꺼짐입니다.

참고:

설정 > 서버속성에서백그라운드배포예약키를구성한경우에만이옵션이적용됩니다. iOS 장치에는상시연결옵션을 사용할수없습니다.

구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은모든플랫폼에적용되지만 상시연결에대해배포를선택한경우 iOS 에는적용되지않습니다.

17. 저장을클릭합니다.

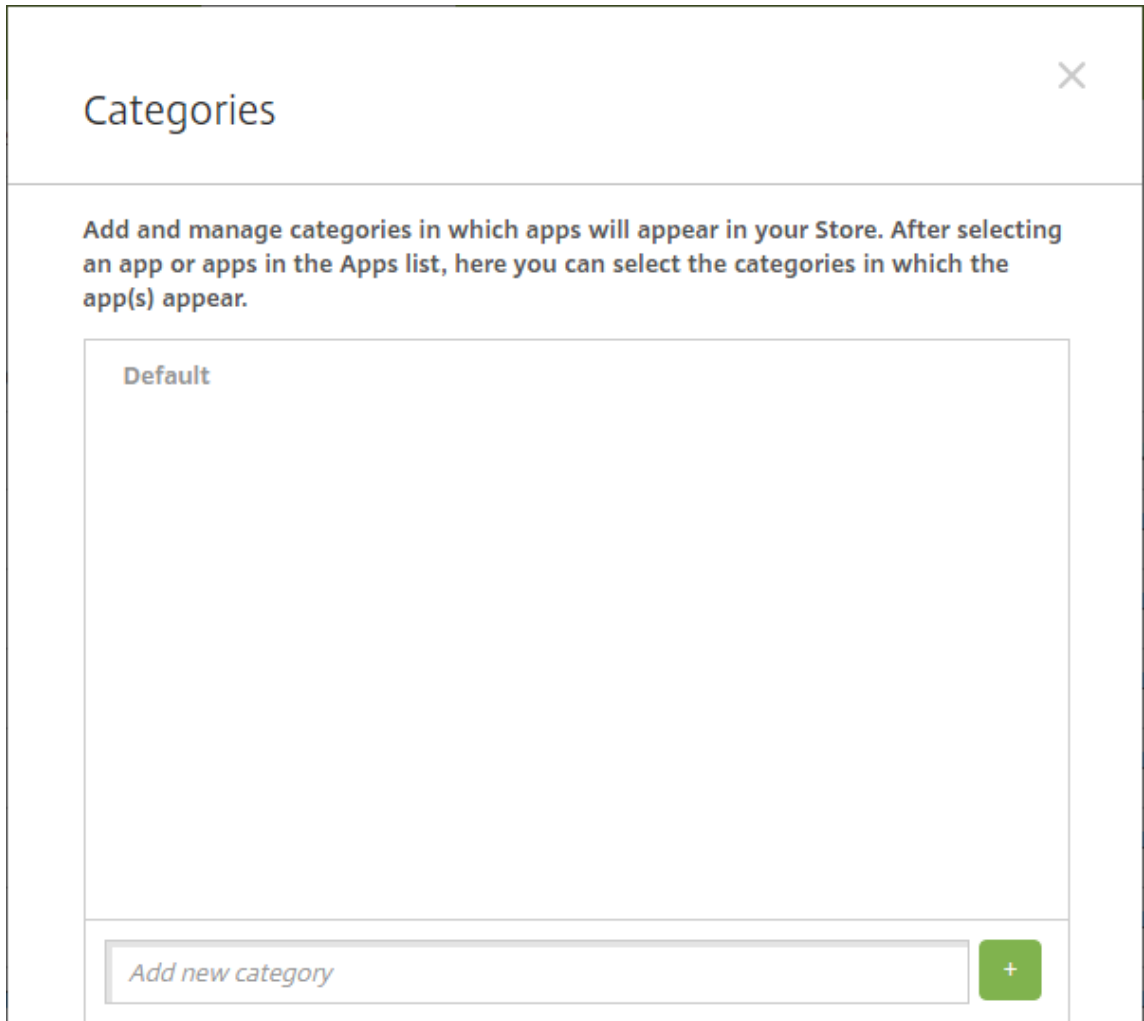
앱범주만들기

사용자가 Secure Hub 에로그온하면 XenMobile 에서설정해 앱, 웹링크및스토어목록이표시됩니다. 앱범주를사용하면사용자가액세스할수있는특정앱, 스토어또는웹링크를지정할수있습니다. 예를들어재무범주를만든후재무와관련된앱만범주에추가할수 있습니다. 또는영업범주를구성하여영업앱을할당할수있습니다.

XenMobile 콘솔의 앱페이지에서범주를구성할수있습니다. 그런다음앱, 웹링크또는스토어를추가하거나편집할때이전에구성한 하나이상의범주에앱을추가할수있습니다.

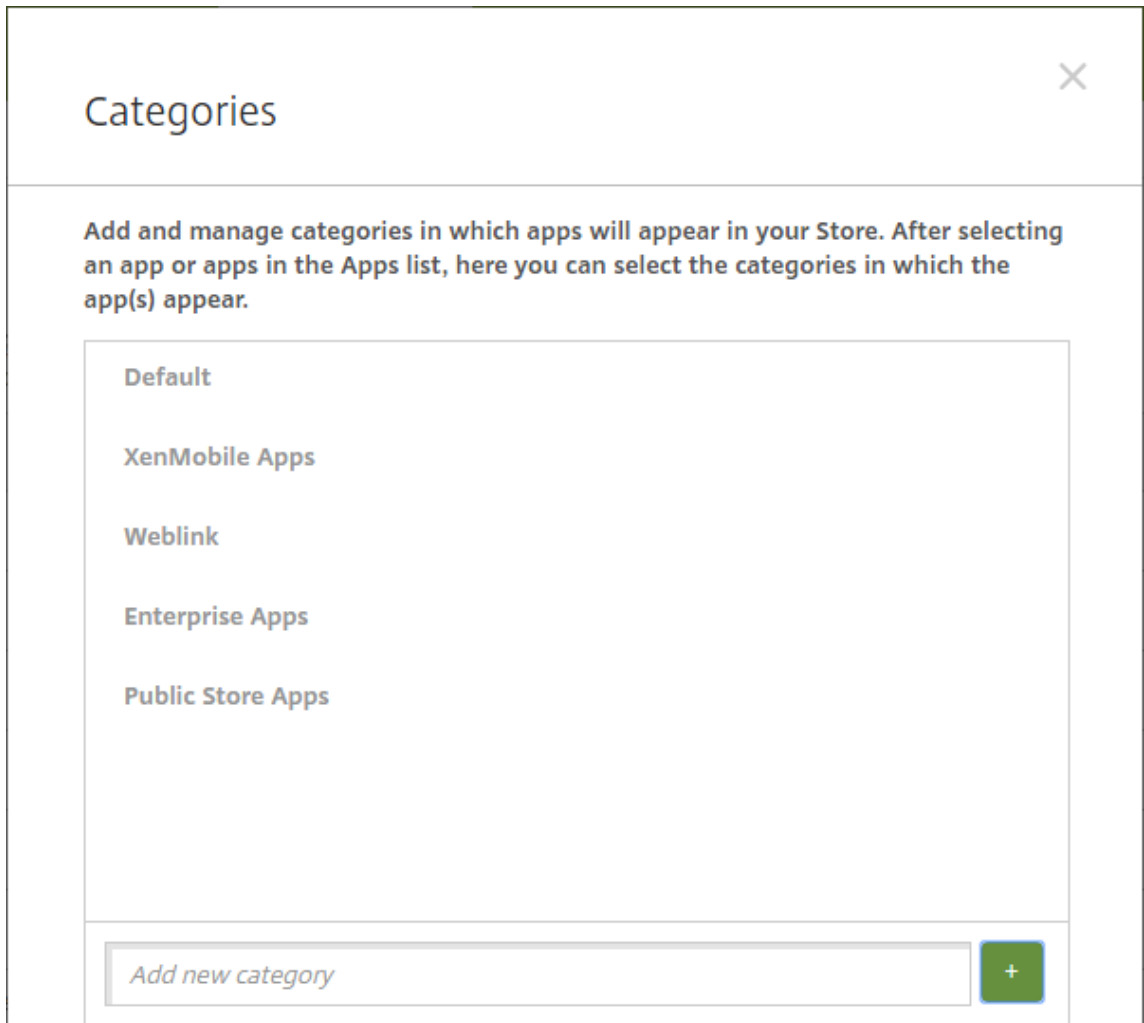
1. XenMobile 콘솔에서 구성 > 앱을클릭합니다. 앱페이지가나타납니다.

2. 범주를 클릭합니다. 범주대화상자가 나타납니다.



3. 추가할 각 범주에 대해 다음을 수행합니다.

- 대화상자의 맨 아래쪽에 있는 새 범주 추가 필드에 추가할 범주의 이름을 입력합니다. 예를 들어 엔터프라이즈 앱에 대한 범주를 만들려는 경우 엔터프라이즈 앱을 입력할 수 있습니다.
- 더하기 기호 (+) 를 클릭하여 범주를 추가합니다. 새로 만들어진 범주가 추가되고 범주 대화상자에 표시됩니다.



4. 범주추가가완료되면 범주대화상자를닫습니다.
5. 앱페이지에서기존앱을새범주에배치할수있습니다.
 - 범주로분류할앱을선택합니다.
 - 편집을클릭합니다. 앱정보페이지가나타납니다.
 - 앱범주목록에서범주확인란을선택하여새범주를적용합니다. 앱에적용하지않을기존범주에대한확인란을선택취소합니다.
 - 배달그룹할당탭을클릭하거나다음페이지에서 다음을클릭하여나머지앱설정페이지단계를이동합니다.
 - 배달그룹할당페이지에서 저장을클릭하여새범주를적용합니다. 새범주가앱에적용되고 앱테이블에표시됩니다.

공용앱스토어앱추가

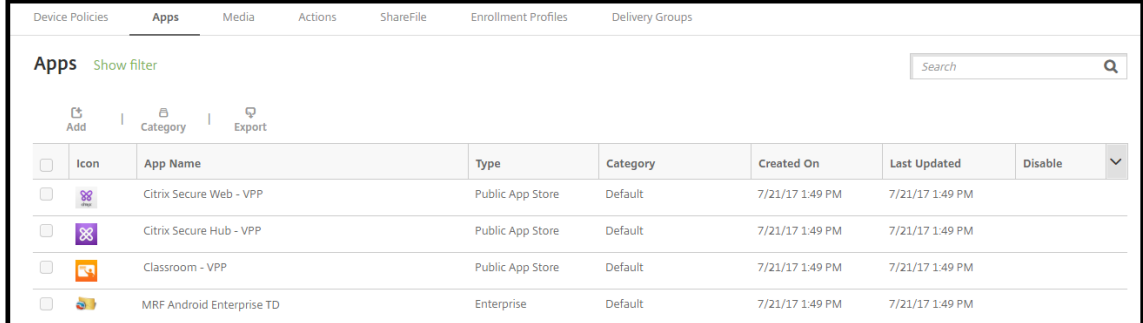
iTunes 또는 Google Play 와같은공용앱스토어에서무료또는유료로제공되는앱을 XenMobile 에추가할수있습니다.

Android Enterprise 용으로유료공용앱스토어앱을추가할경우대량구매라이선스상태를검토할수있습니다. 이상태는사용가능한총라이선스수, 현재사용중인라이선스수및라이선스를사용하고있는각사용자의전자메일주소입니다. Android Enterprise

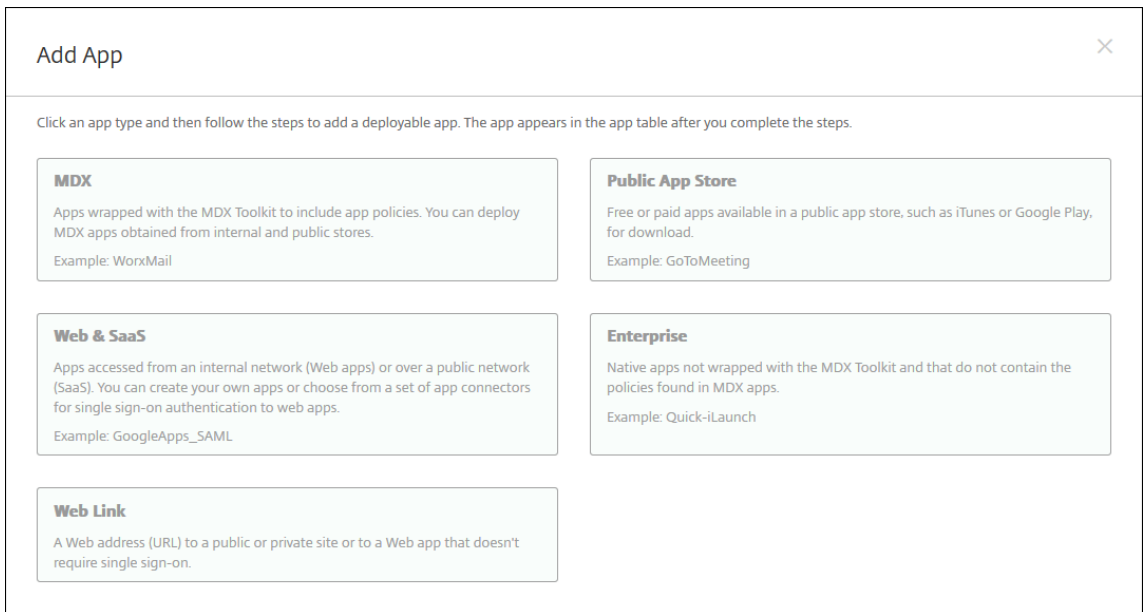
의대량구매프로그램은조직의앱및기타데이터를대량으로찾고, 구입하고, 배포하는프로세스를간소화합니다.

앱정보를구성하고앱을전달할플랫폼선택

1. XenMobile 콘솔에서 구성 > 앱을클릭합니다. 앱페이지가나타납니다.



2. 추가를클릭합니다. 앱추가대화상자가나타납니다.



3. 공용앱스토어를클릭합니다. 앱정보페이지가나타납니다.

4. 앱정보창에서다음정보를입력합니다.

- 이름: 앱의설명적이름을입력합니다. 이이름은 앱테이블의 앱이름아래에표시됩니다.
- 설명: 앱의선택적설명을입력합니다.
- 앱범주: 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은앱범주만들기를참조하십시오.

5. 다음을클릭합니다. 앱플랫폼페이지가나타납니다.

6. 플랫폼아래에서추가할플랫폼을선택합니다. 하나의플랫폼에대해서만구성하는경우다른플랫폼의선택을취소합니다.

각플랫폼에대한앱설정을구성합니다. 플랫폼설정구성을마치면플랫폼배포규칙을설정하고구성을저장합니다.

각플랫폼에대한앱설정을구성합니다. 플랫폼설정구성을마치면플랫폼배포규칙을설정하고구성을저장합니다.

중요: Google Play Store 앱을 설정하려면 다른 플랫폼과 다른 단계를 수행해야 합니다. Google Play Store 앱 정보를 수동으로 구성해야 합니다.

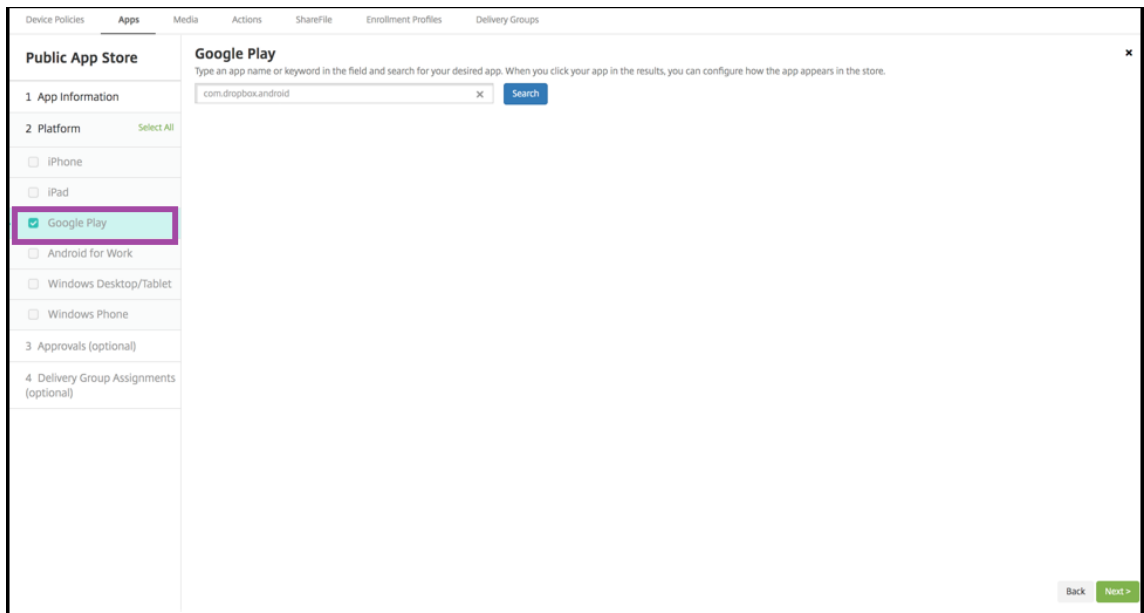
Google Play 앱에 대한 앱 설정 구성

참고:

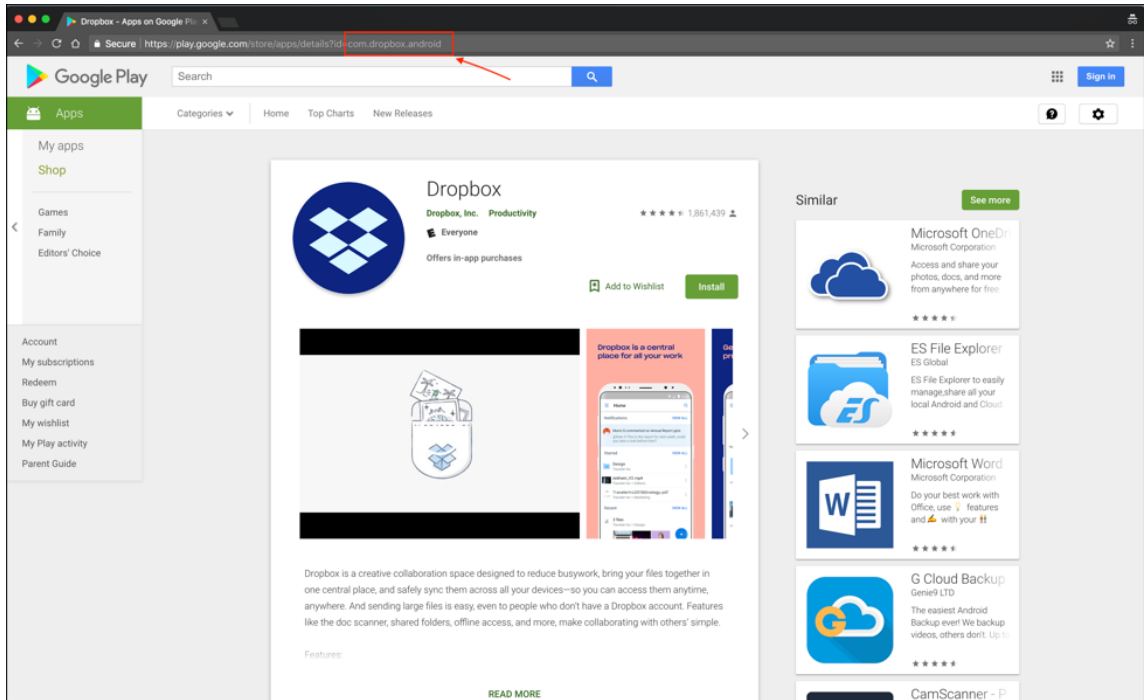
관리되는 Google Play에서 Google Play Store의 모든 앱에 액세스하려면 XenMobile 서버 속성 관리되는 **Google Play Store**의 모든 앱에 액세스를 사용합니다. **서버 속성**에서 자세한 내용을 참조하십시오. 이 속성을 **true**로 설정하면 모든 Android Enterprise 사용자에게 대공용 Google Play Store 앱이 화이트리스트에 추가됩니다. 그런 다음 **제한 장치 정책**을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다.

Google Play Store 앱 설정을 구성하려면 다른 플랫폼과 다른 단계를 수행해야 합니다. Google Play Store 앱 정보를 수동으로 구성해야 합니다.

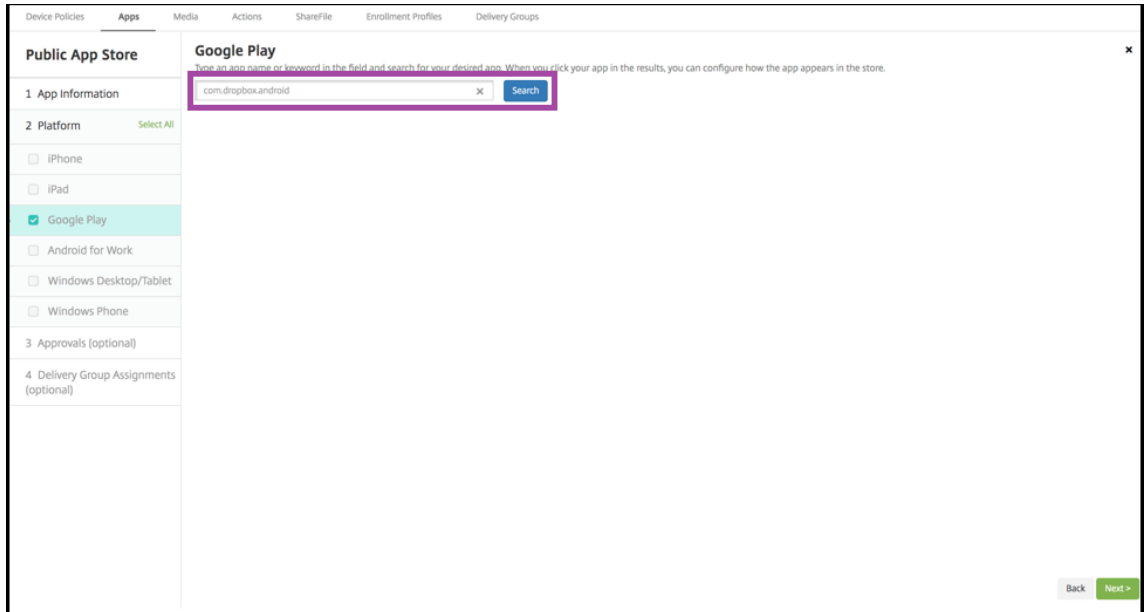
1. 플랫폼에서 **Google Play**가 선택되어 있는지 확인합니다.



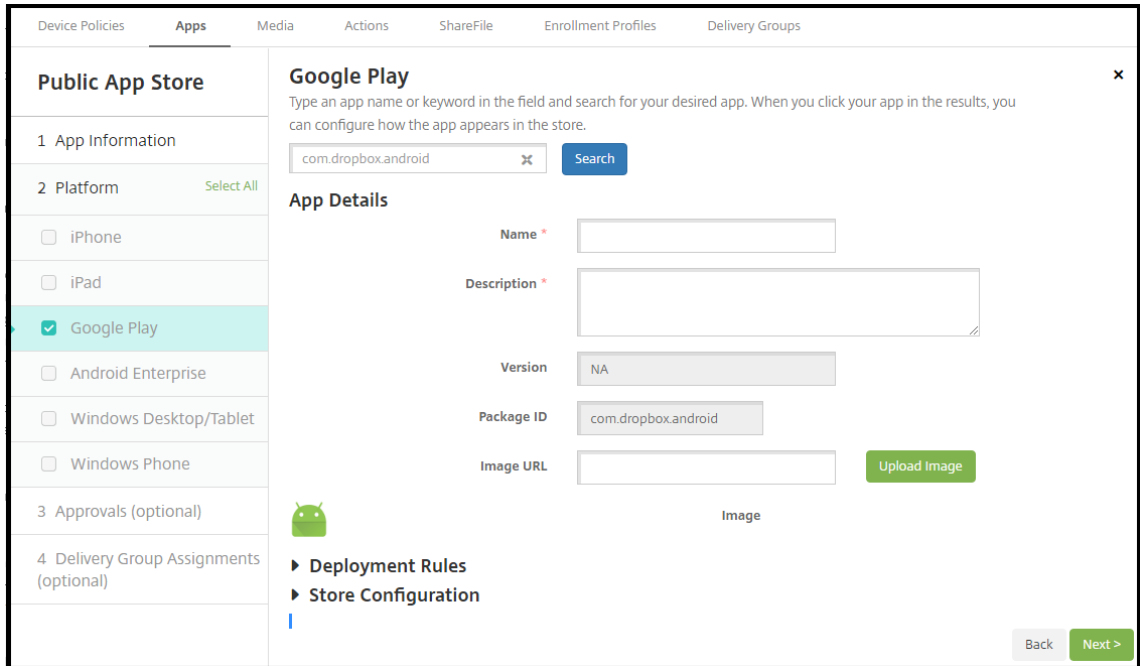
2. Google Play Store로 이동합니다. Google Play Store에서 패키지 ID를 복사합니다. ID는 앱의 URL에서 찾을 수 있습니다.



3. XenMobile Server 콘솔에서공용스토어앱을추가할때검색창에패키지 ID 를붙여넣습니다. **Search(검색)** 를클릭합니다.



4. 패키지 ID 가유효하면앱세부정보를입력할수있는 UI 가나타납니다.



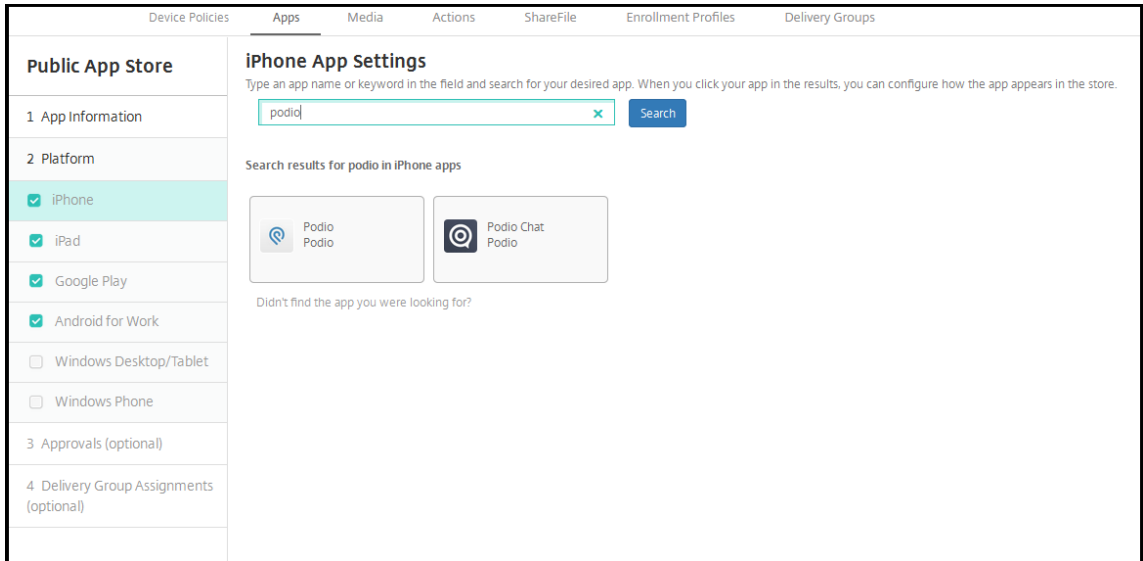
5. 스토어의 앱과 함께 표시되도록 이미지의 URL 을 구성할 수 있습니다. Google Play Store 의 이미지를 사용하려면:

- a) Google Play Store 로 이동합니다. 앱 이미지를 마우스 오른쪽 버튼으로 클릭하고 이미지 주소를 복사합니다.
- b) **Image URL(이미지 URL)** 필드에 이미지 주소를 붙여넣습니다.
- c) **Upload Image(이미지 업로드)** 를 클릭합니다. **Image(이미지)** 옆에 이미지가 나타납니다.

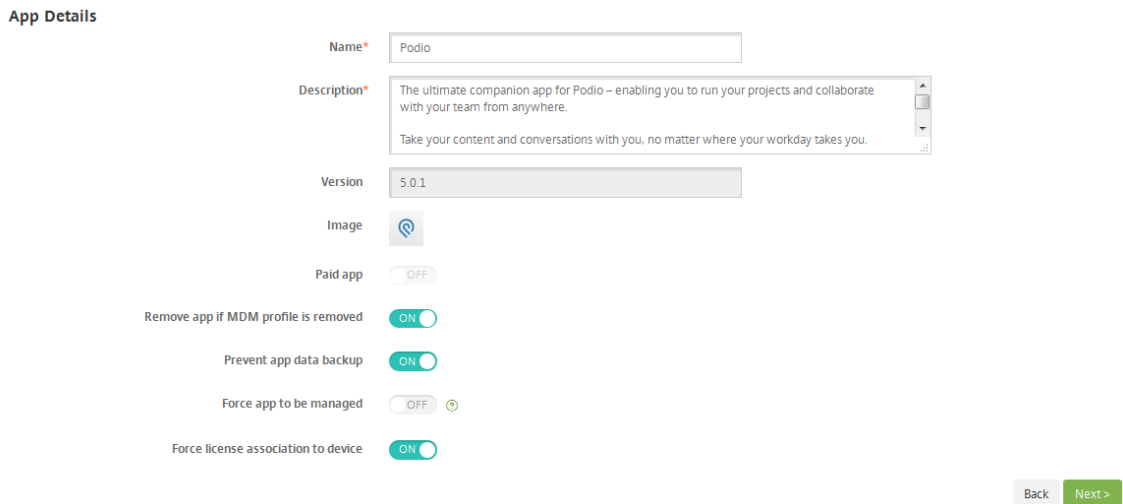
이미지를 구성하지 않으면 일반 Android 이미지가 앱과 함께 나타납니다.

Google Play 외 다른 플랫폼에 대한 앱 설정 구성

1. 검색 상자에 앱 이름을 입력하고 검색을 클릭하여 추가할 앱을 선택합니다. 검색 기준과 일치하는 앱이 표시됩니다. 다음 그림은 iPhone 앱에서 **podio** 에 대한 검색 결과를 보여줍니다.



2. 추가할 앱을 클릭합니다. 선택한 앱과 관련된 정보 (이름, 설명, 버전번호, 관련 이미지 등) 로 앱 세부정보 필드를 채웁니다.



3. 다음 설정을 구성합니다.

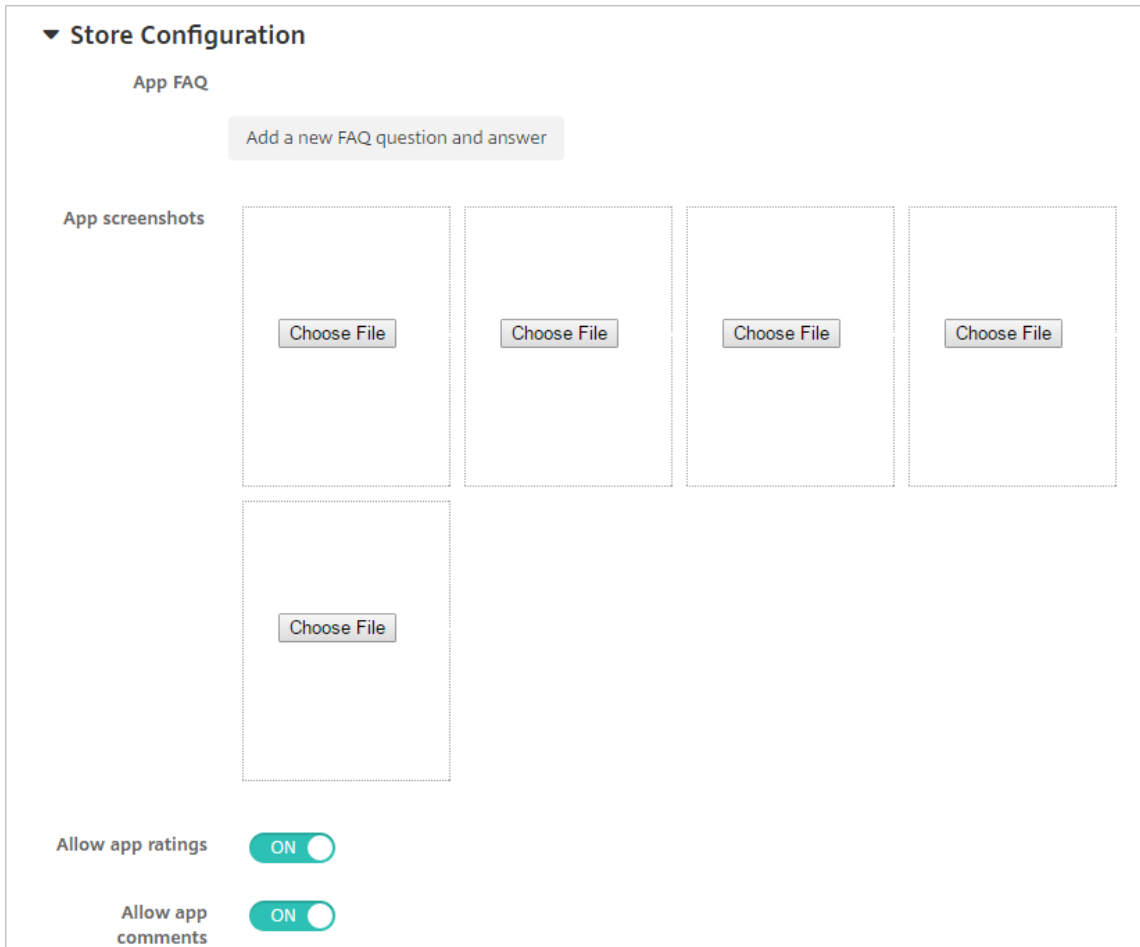
- 필요한 경우 앱의 이름 및 설명을 변경합니다.
- 유료 앱: 이 필드는 미리 구성되며 변경할 수 없습니다.
- **MDM** 프로파일 제거된 경우 앱 제거: MDM 프로파일 제거된 경우 앱을 제거할지 여부를 선택합니다. 기본값은 켜짐입니다.
- 앱 데이터 백업 방지: 앱 데이터를 백업하는 것을 방지할지 여부를 선택합니다. 기본값은 켜짐입니다.
- 강제로 앱 관리: 앱이 관리되지 않는 앱으로 설치될 경우 감독되지 않는 장치에서 해당 앱의 관리를 허용할 것인지 묻는 메시지를 표시할지 여부를 선택합니다. 기본값은 꺼짐입니다. iOS 9.0 이상에서 사용할 수 있습니다.
- 장치에 강제로 라이선스 연결: 장치 연결을 사용하는 상태에서 개발된 앱을 사용자가 아닌 장치에 연결할지 여부를 선택합니다. iOS 9 이상에서 사용할 수 있습니다. 선택한 앱이 장치할당을 지원하지 않는 경우 이 필드를 변경할 수 없습니다.

배포규칙을구성합니다

자세한내용은 [리소스배포](#)에서참조하십시오.

스토어구성설정

1. **XenMobile Store** 구성을확장합니다.



필요한경우 XenMobile Store 에나타나는앱또는화면캡처에대한 FAQ 를추가할수있습니다. 또한사용자의앱평가또는 설명추가를허용할지여부를설정할수있습니다.

- 다음설정을구성합니다.
 - 앱 **FAQ**: 앱에대한 FAQ(질문과답변) 를추가합니다.
 - 앱스크린샷: XenMobile Store 의앱을분류하는데도움이되는화면캡처를추가합니다. 업로드하는그래픽 은 PNG 여야합니다. GIF 또는 JPEG 이미지는업로드할수없습니다.
 - 앱등급허용: 사용자의앱평가를허용할지여부를선택합니다. 기본값은켜짐입니다.
 - 앱설명허용: 선택한앱에대한사용자의설명을허용할지여부를선택합니다.

2. **Volume Purchase Program** 을확장하거나 Android Enterprise 의경우 대량구매를확장합니다.

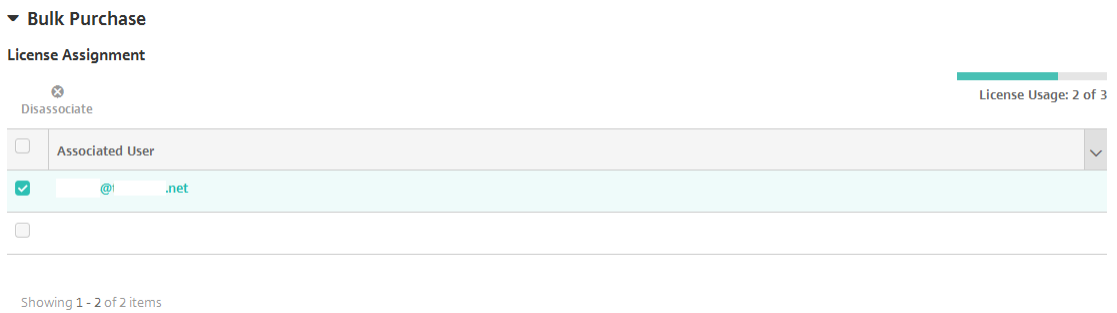
Volume Purchase Program 의 경우 다음 단계를 완료합니다.

- a) XenMobile 을 사용하여 VPP 라이선스를 앱에 적용하려는 경우 **VPP** 라이선스 목록에서 **VPP** 라이선스 파일 업로드를 클릭합니다.
- b) 표시되는 대화상자에서 라이선스를 가져옵니다.

Android Enterprise 대량구매의 경우 대량구매 섹션을 확장합니다.

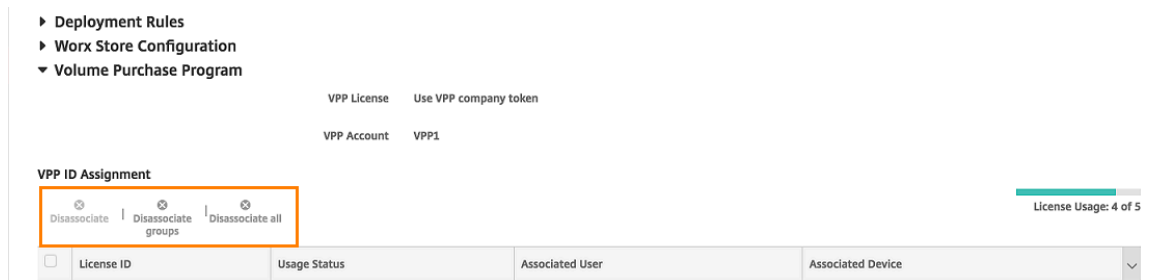
라이선스 할당 테이블에서 사용 가능한 총 라이선스 수와 앱에서 사용 중인 라이선스 수가 표시됩니다.

Android Enterprise 의 경우 사용자를 선택하고 연결 해제를 클릭하여 라이선스 할당을 종료하고 다른 사용자를 위한 라이선스를 확보할 수 있습니다. 그러나 사용자가 특정 앱이 포함된 배달 그룹에 속하지 않는 경우에만 라이선스 연결을 해제할 수 있습니다.

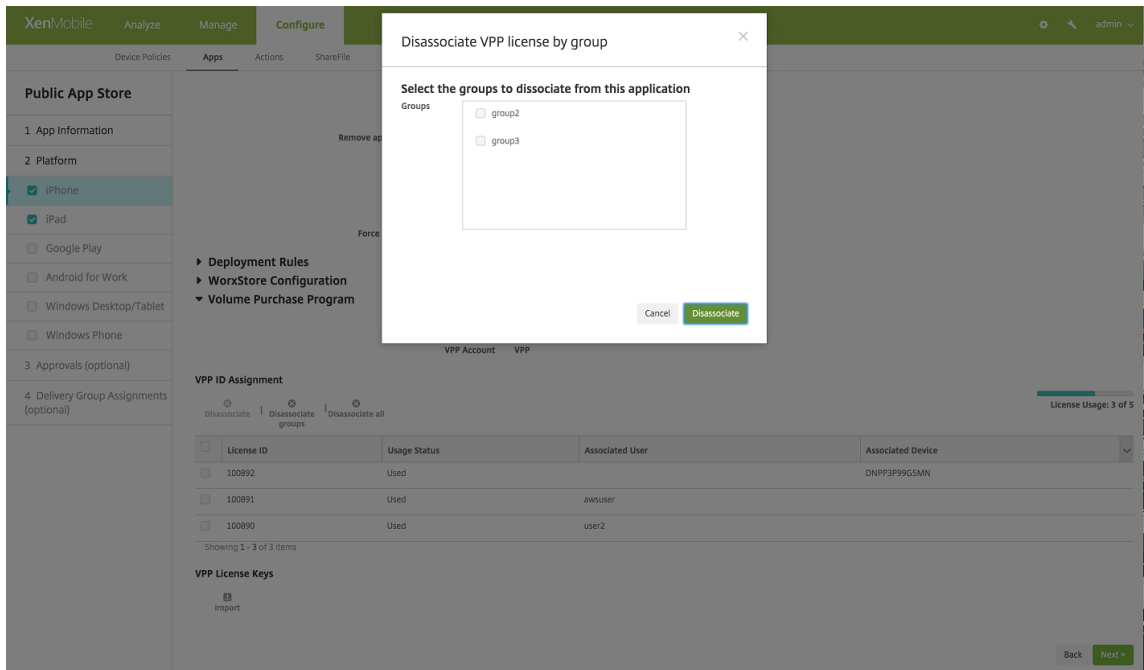


Android Enterprise 의 경우 사용자가 특정 앱이 포함된 배달 그룹에 속하지 않는 경우에만 라이선스 연결을 해제할 수 있습니다.

iOS 의 경우 개별 사용자, 사용자 그룹 또는 모든 할당의 VPP (Volume Purchase Program) 라이선스 연결을 해제할 수 있습니다. 이렇게 하면 라이선스 할당이 종료되고 라이선스가 확보됩니다.



그룹 연결 해제를 클릭하면 그룹을 선택하는 대화상자가 열립니다.



3. **Volume Purchase Program** 또는 대량구매설정을완료한후 다음을클릭합니다. 승인페이지가나타납니다.

사용자계정을만들때승인이필요한경우워크플로를사용합니다. 승인워크플로를설정하지않아도되는경우다음단계로건너
될수있습니다.

워크플로를할당하거나만들어야하는경우다음설정을구성합니다.

- 사용할워크플로: 목록에서기존워크플로를클릭하거나 새워크플로만들기를클릭합니다. 기본값은 없음입니다.
- 새워크플로만들기를선택하는경우다음설정을구성합니다.
 - 이름: 워크플로의고유한이름을입력합니다.
 - 설명: 필요한경우워크플로의설명을입력합니다.
 - 전자메일승인템플릿: 목록에서할당할전자메일승인템플릿을선택합니다. 이필드오른쪽에있는눈모양아이콘
을클릭하면템플릿을미리볼수있는대화상자가나타납니다.
 - 관리자승인수준: 목록에서이워크플로에필요한관리자승인수준의번호를선택합니다. 기본값은 **1** 수준입니다.
사용가능한옵션은다음과같습니다.
 - * 필요없음
 - * 1 수준
 - * 2 수준
 - * 3 수준
 - **Active Directory** 도메인선택: 목록에서워크플로에사용할적절한 Active Directory 도메인을선택합
니다.
 - 추가로필요한승인자찾기: 검색필드에추가로필요한사람의이름을입력하고 검색을클릭합니다. 이름은
Active Directory 에서가져옵니다.
 - 필드에이름이나타나면해당하는이름옆의확인란을선택합니다. 이름과전자메일주소가 추가로필요한승인자
선택됨목록에나타납니다.
 - * 추가로필요한승인자선택됨목록에서사용자를제거하려면다음중하나를수행합니다.

- * 선택한도메인에있는모든사용자의목록을표시하려면 검색을클릭합니다.
- * 검색결과를제한하려면검색상자에이름전체또는일부를입력한다음 검색을클릭합니다.
- * 추가로필요한승인자선택됨목록에있는사용자는검색결과목록에서해당이름옆에확인표시가있습니다. 목록을스크롤하고제거하려는각이름옆에있는확인란의선택을취소합니다.

4. 다음을클릭합니다. 배달그룹할당페이지가나타납니다.

5. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.

6. 배포일정을확장하고다음설정을구성합니다.

- 배포옆에서 켜짐을클릭하여배포를예약하거나 꺼짐을클릭하여배포를차단합니다. 기본옵션은 켜짐입니다.
- 배포일정옆에서 지금또는 나중에를클릭합니다. 기본옵션은 지금입니다.
- 나중에를클릭하는경우달력아이콘을클릭하고배포날짜와시간을선택합니다.
- 배포조건옆에서 모든연결에서를클릭하거나 이전배포가실패한경우에만을클릭합니다. 기본옵션은 모든연결에서입니다.
- 상시연결에대해배포옆에서 켜짐또는 꺼짐을클릭합니다. 기본옵션은 꺼짐입니다.

참고:

설정 > 서버속성에서백그라운드배포예약기를구성한경우에만이옵션이적용됩니다. iOS 장치에는상시연결옵션을 사용할수없습니다.

구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은모든플랫폼에적용되지만 상시연결에대해배포를선택한경우 iOS 에는적용되지않습니다.

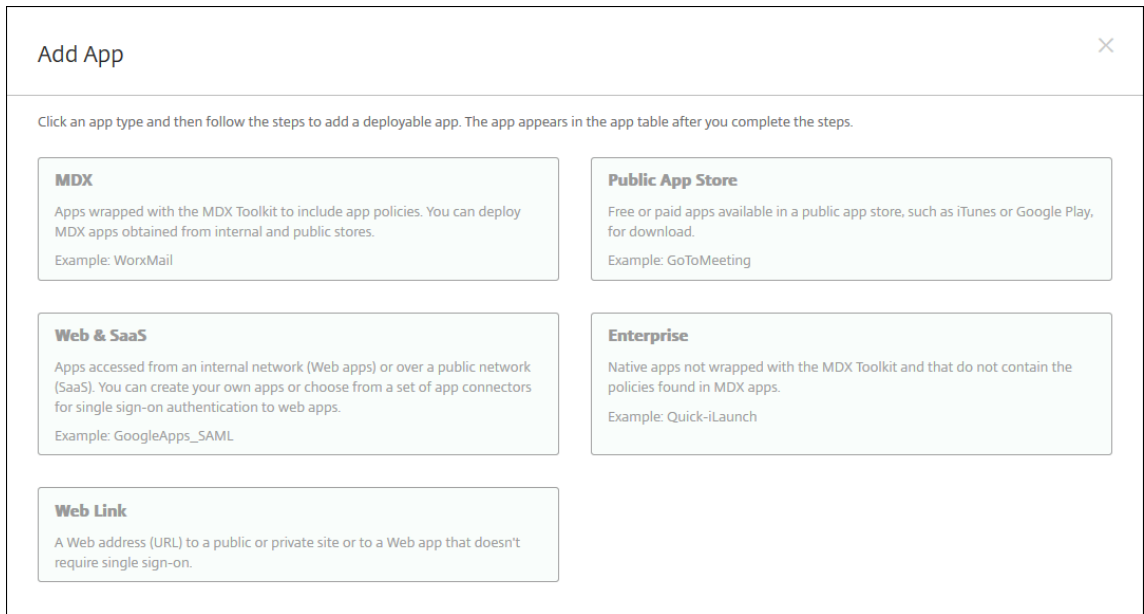
7. 저장을클릭합니다.

웹또는 SaaS 앱추가

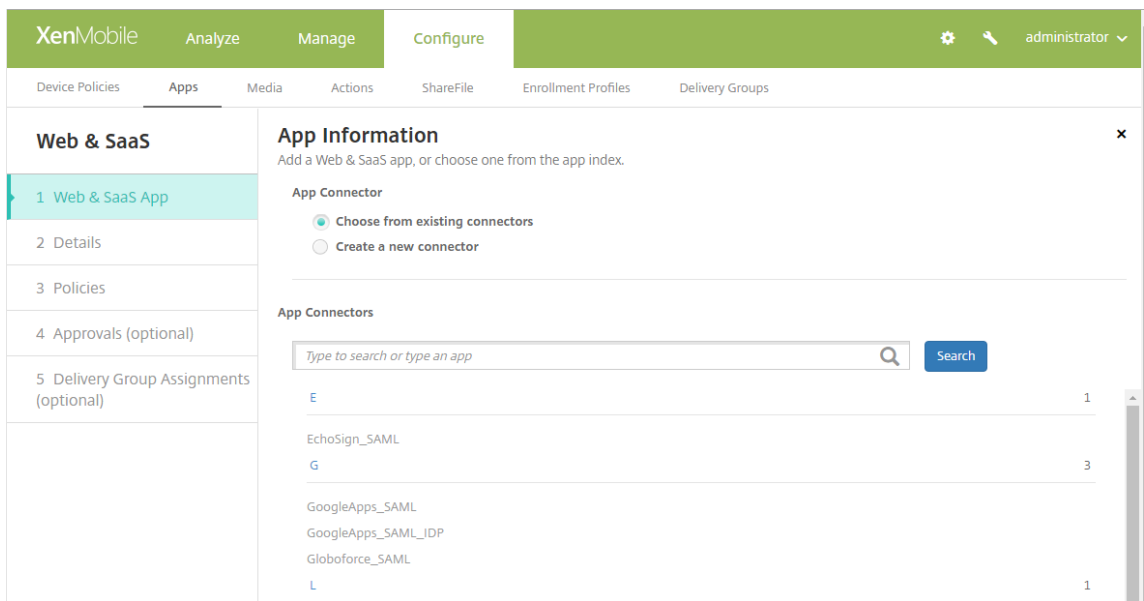
XenMobile 콘솔에서사용자에게모바일, 엔터프라이즈, 웹및 SaaS 앱에대한 SSO(Single Sign-On) 인증을제공할수있습니다. 응용프로그램커넥터플릿을사용하여앱에서 SSO 를사용하도록할수있습니다. XenMobile 에서제공되는커넥터 유형의 목록은 [응용프로그램커넥터 유형](#)을참조하십시오. XenMobile 에서웹또는 SaaS 앱을추가할때직접커넥터를만들수도있습니다.

SSO 전용으로제공되는앱의경우설정을저장하면 XenMobile 콘솔의 앱탭에앱이표시됩니다.

1. XenMobile 콘솔에서 구성 > 앱을클릭합니다. 앱페이지가열립니다.
2. 추가를클릭합니다. 앱추가대화상자가나타납니다.



3. 웹 및 **SaaS** 를 클릭합니다. 앱정보페이지가 나타납니다.



4. 다음과 같이 기존 또는 새 앱커넥터를 구성합니다.

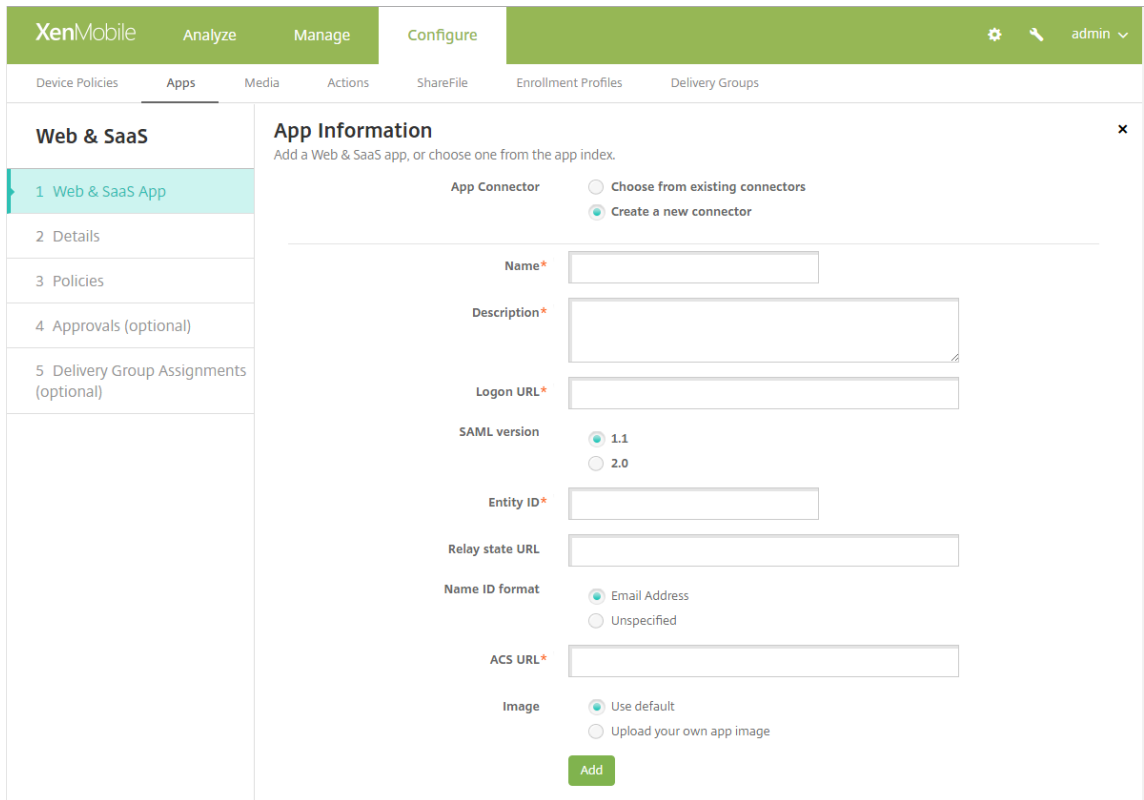
기존 앱커넥터를 구성하려면

1. 위에 표시된 것과 같이 앱정보페이지에서 기존 커넥터에서 선택이 이미 선택되어 있습니다. 앱커넥터 목록에서 사용할 커넥터를 클릭합니다. 앱커넥터 정보 페이지가 나타납니다.
2. 다음 설정을 구성합니다.
 - **앱 이름:** 미리 채워진 이름을 사용하거나 새 이름을 입력합니다.

- **앱설명:** 미리채워진설명을사용하거나직접설명을입력합니다.
- **URL:** 미리채워진 URL 을사용하거나앱의웹주소를입력합니다. 선택한커넥터에따라다음페이지로이동하기전에 바꿔야하는자리표시자가이필드에포함될수있습니다.
- **도메인이름:** 해당하는경우앱의도메인이름을입력합니다. 이필드는필수입니다.
- **앱이내부네트워크에서호스트됨:** 앱이내부네트워크의서버에서실행되는지여부를선택합니다. 원격위치에서내부업에연결하는사용자의경우 NetScaler Gateway 를통해연결해야합니다. 이옵션을 꺼짐으로설정하면 VPN 키워드가앱에추가되고사용자가 NetScaler Gateway 를통해연결할수있습니다. 기본값은 꺼짐입니다.
- **앱범주:** 목록에서앱에적용할선택적범주를클릭합니다.
- **사용자계정프로비전:** 응용프로그램에대한사용자계정을만들지여부를선택합니다. Globoforce_SAML 커넥터를사용하는경우이옵션을사용하여 SSO 가원활하게통합되도록해야합니다.
- **사용자계정프로비전을사용하는경우다음설정을구성합니다.**
 - 서비스계정
 - * **사용자이름:** 앱관리자의이름을입력합니다. 이것은필수필드입니다.
 - * **암호:** 앱관리자암호를입력합니다. 이것은필수필드입니다.
 - 사용자계정
 - * **사용자권한부여가종료된경우:** 목록에서사용자가앱에더이상액세스할수없을때수행할동작을클릭합니다. 기본값은 계정사용안함입니다.
 - 사용자이름규칙
 - * **추가할각사용자이름규칙에대해다음을수행합니다.**
 - **사용자특성:** 목록에서규칙에추가할사용자특성을클릭합니다.
 - **길이 (문자):** 목록에서사용자이름규칙에서사용할사용자특성의문자수를클릭합니다. 기본값은 모두입니다.
 - **규칙:** 추가한각사용자특성이사용자이름규칙에자동으로추가됩니다.
- **암호요구사항**
 - **길이:** 최소사용자암호길이를입력합니다. 기본값은 **8** 입니다.
- **암호만료**
 - **유효기간 (일):** 암호가유효한일수를입력합니다. 유효한값은 **0-90** 입니다. 기본값은 90 입니다.
 - **만료후자동으로암호재설정:** 암호만료시암호를자동으로재설정할지여부를선택합니다. 기본값은 꺼짐입니다. 이필드를사용하지않는경우암호가만료된사용자가앱을열수없습니다.

새앱커넥터를구성하려면

1. 앱정보페이지에서 새커넥터만들기를선택합니다. 앱커넥터필드가나타납니다.

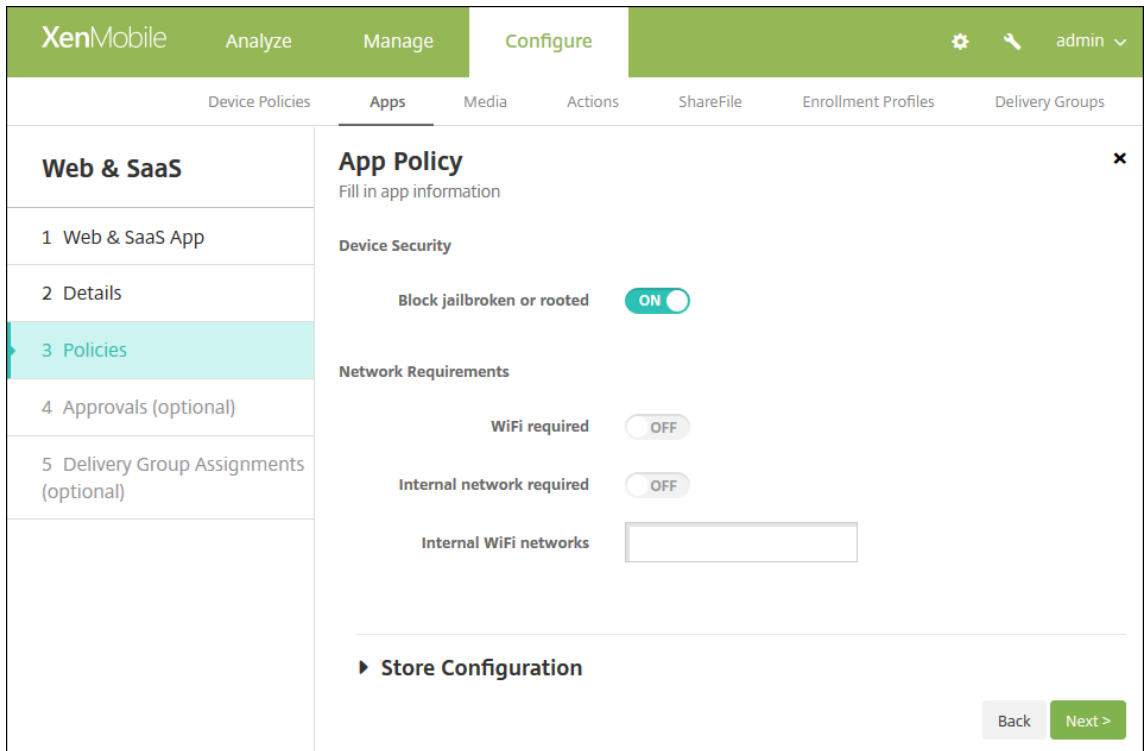


2. 다음설정을구성합니다.

- 이름: 커넥터이름을입력합니다. 이것은필수필드입니다.
- 설명: 커넥터에대한설명을입력합니다. 이것은필수필드입니다.
- 로그인 URL: 사용자가사이트에로그온하는 URL 을입력하거나복사후붙여넣습니다. 예를들어추가하려는앱으로 그온페이지가있는경우웹브라우저를열고앱의로그온페이지 (예: <https://www.example.com/login>) 로이동합니다. 이것은필수필드입니다.
- SAML 버전: 1.1 또는 2.0 을선택합니다. 기본값은 1.1 입니다.
- 엔터티 ID: SAML 앱의 ID 를입력합니다.
- 릴레이상태 URL: SAML 응용프로그램의웹주소를입력합니다. 릴레이상태 URL 은앱의응답 URL 입니다.
- 이름 ID 형식: 전자메일주소또는 지정되지않음을선택합니다. 기본값은 전자메일주소입니다.
- ACS URL: ID 공급자또는서비스공급자의 Assertion Consumer Service URL 을입력합니다. ACS URL 은사용자에게 SSO 기능을제공합니다.
- 이미지: 기본 Citrix 이미지를사용할지, 고유한이미지를업로드할지여부를선택합니다. 기본값은기본값사용입 니다.
 - 고유한이미지를업로드하려면 찾아보기를클릭하고파일의위치로이동합니다. 파일은.PNG 파일이어야합니 다. JPEG 또는 GIF 파일은업로드할수없습니다. 사용자지정그래픽을추가하면나중에변경할수없습니다.

3. 완료되면 추가를클릭합니다. 세부정보페이지가나타납니다.

4. 다음을클릭합니다. 앱정책페이지가나타납니다.



5. 다음설정을구성합니다.

- 장치보안
- 탈옥또는루팅차단: 탈옥또는루팅장치가앱에엑세스하는것을차단할지여부를선택합니다. 기본값은 켜짐입니다.
- 네트워크요구사항
- **WiFi 필요:** 앱을실행하는데 WiFi 연결이필요한지여부를선택합니다. 기본값은 꺼짐입니다.
- 내부네트워크필요: 앱을실행하는데내부네트워크가필요한지여부를선택합니다. 기본값은 꺼짐입니다.
- 내부 **WiFi** 네트워크: WiFi 필요를사용하는경우사용할내부 WiFi 네트워크를입력합니다.

6. 스토어구성을확장합니다.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

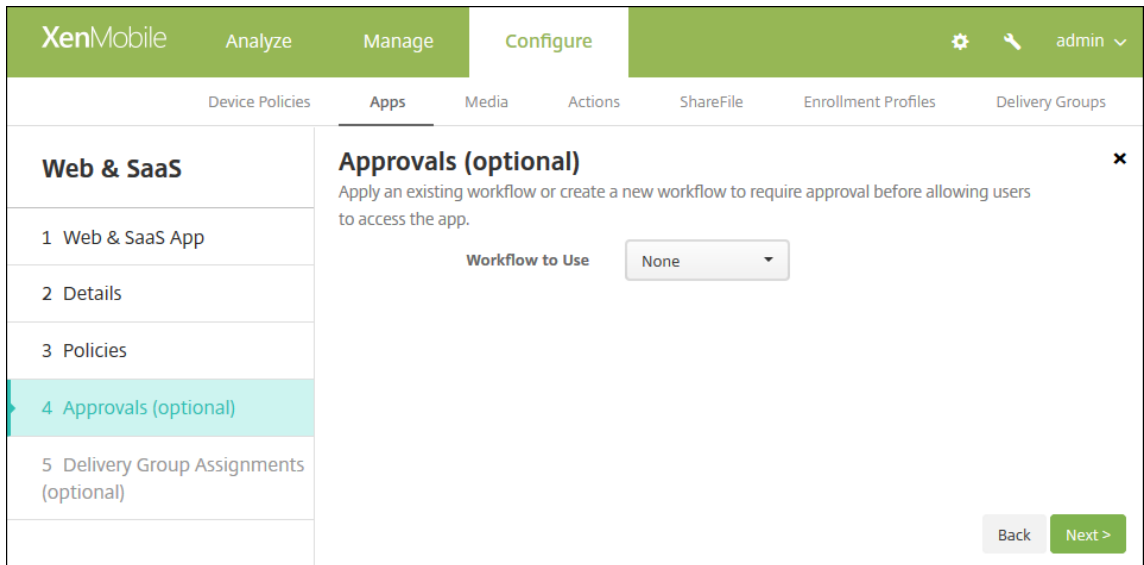
Allow app ratings ON

Allow app comments ON

필요한 경우 XenMobile Store 에 나타나는 앱 또는 화면 캡처에 대한 FAQ 를 추가할 수 있습니다. 또한 사용자의 앱 평가 또는 설명 추가를 허용할지 여부를 설정할 수 있습니다.

- 다음 설정을 구성합니다.
 - 앱 **FAQ**: 앱에 대한 FAQ(질문과 답변) 를 추가합니다.
 - 앱 스크린샷: XenMobile Store 의 앱을 분류하는데 도움이 되는 화면 캡처를 추가합니다. 업로드하는 그래픽은 PNG 여야 합니다. GIF 또는 JPEG 이미지는 업로드할 수 없습니다.
 - 앱 등급 허용: 사용자의 앱 평가를 허용할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 앱 설명 허용: 선택한 앱에 대한 사용자의 설명을 허용할지 여부를 선택합니다. 기본값은 켜짐입니다.

7. 다음을 클릭합니다. 승인 페이지가 나타납니다.



사용자계정을 만들때승인이 필요한 경우 워크플로를 사용합니다. 승인 워크플로를 설정하지 않아도 되는 경우 8 단계로 건너뛸 수 있습니다.

워크플로를 할당하거나 만들어야 하는 경우 다음 설정을 구성합니다.

- 사용할 워크플로: 목록에서 기존 워크플로를 클릭하거나 새 워크플로 만들기를 클릭합니다. 기본값은 없음입니다.
- 새 워크플로 만들기를 선택하는 경우 다음 설정을 구성합니다.
 - 이름: 워크플로의 고유한 이름을 입력합니다.
 - 설명: 필요한 경우 워크플로의 설명을 입력합니다.
 - 전자메일 승인 템플릿: 목록에서 할당할 전자메일 승인 템플릿을 선택합니다. 이 필드 오른쪽에 있는 눈모양 아이콘을 클릭하면 템플릿을 미리 볼 수 있는 대화상자가 나타납니다.
- 관리자 승인 수준: 목록에서 이 워크플로에 필요한 관리자 승인 수준의 번호를 선택합니다. 기본값은 **1** 수준입니다. 가능한 옵션은 다음과 같습니다.
 - 필요없음
 - 1 수준
 - 2 수준
 - 3 수준
- **Active Directory** 도메인 선택: 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
- 추가로 필요한 승인자 찾기: 검색 필드에 추가로 필요한 사람의 이름을 입력하고 검색을 클릭합니다. 이름은 Active Directory 에서 가져옵니다.
- 필드에 이름이 나타나면 해당하는 이름 옆의 확인란을 선택합니다. 이름과 전자메일 주소가 추가로 필요한 승인자 선택된 목록에 나타납니다.
 - 추가로 필요한 승인자 선택된 목록에서 사용자를 제거하려면 다음 중 하나를 수행합니다.
 - * 선택한 도메인에 있는 모든 사용자의 목록을 표시하려면 검색을 클릭합니다.
 - * 검색 결과를 제한하려면 검색 상자에 이름 전체 또는 일부를 입력한 다음 검색을 클릭합니다.
 - * 추가로 필요한 승인자 선택된 목록에 있는 사용자는 검색 결과 목록에서 해당 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하고 제거하려는 각 이름 옆에 있는 확인란의 선택을 취소합니다.

8. 다음을 클릭합니다. 배달그룹할당페이지가 나타납니다.
9. 배달그룹선택옆에서 배달그룹을 입력하여 찾거나 그룹을 하나 이상 선택합니다. 선택한 그룹이 애플당을 받을 배달그룹 목록에 나타납니다.
10. 배포일정을 확장하고 다음 설정을 구성합니다.
 - 배포옆에서 켜짐을 클릭하여 배포를 예약하거나 꺼짐을 클릭하여 배포를 차단합니다. 기본 옵션은 켜짐입니다.
 - 배포일정 옆에서 지금 또는 나중에를 클릭합니다. 기본 옵션은 지금입니다.
 - 나중에를 클릭하는 경우 달력 아이콘을 클릭하고 배포 날짜와 시간을 선택합니다.
 - 배포 조건 옆에서 모든 연결에서를 클릭하거나 이전 배포가 실패한 경우에만을 클릭합니다. 기본 옵션은 모든 연결에서입니다.
 - 상시 연결에 대해 배포 옆에서 켜짐 또는 꺼짐을 클릭합니다. 기본 옵션은 꺼짐입니다.

참고:

설정 > 서버 속성에서 백그라운드 배포 예약기를 구성한 경우에만이 옵션이 적용됩니다. iOS 장치에는 상시 연결 옵션을 사용할 수 없습니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 모든 플랫폼에 적용되지만 상시 연결에 대해 배포를 선택한 경우 iOS 에는 적용되지 않습니다.

11. 저장을 클릭합니다.

엔터프라이즈 앱 추가

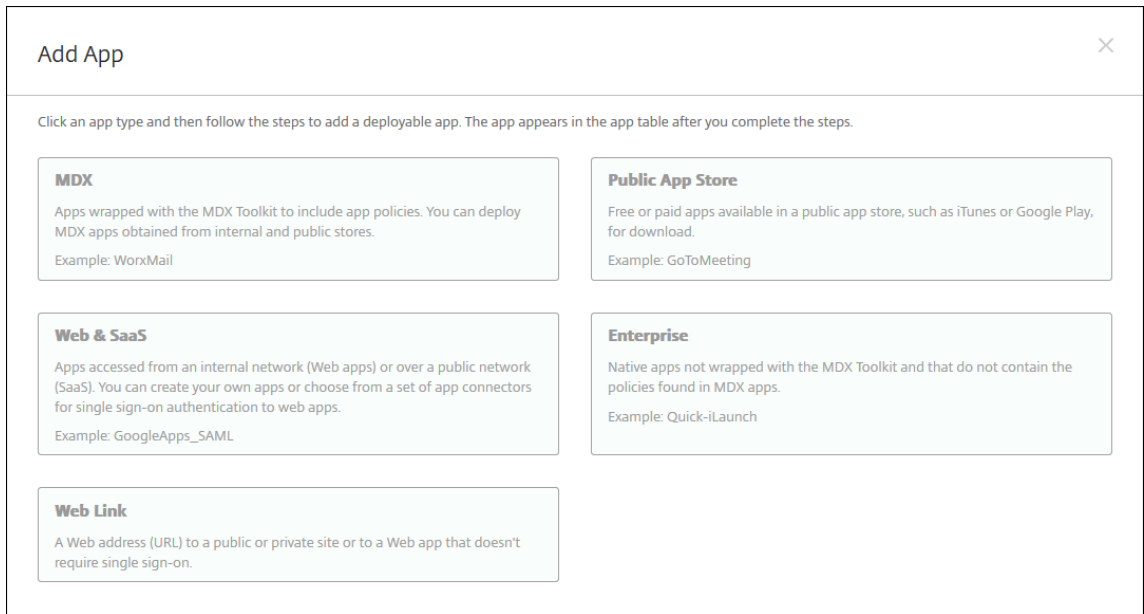
XenMobile 에서 엔터프라이즈 앱은 MDX Toolkit 으로 래핑되지 않고 MDX 앱과 관련된 정책이 포함되지 않은 기본 앱을 나타냅니다. XenMobile 콘솔의 앱 탭에서 엔터프라이즈 앱을 업로드할 수 있습니다. 엔터프라이즈 앱은 다음 플랫폼 (맞해당하는 파일 형식)을 지원합니다.

- iOS (.ipa 파일)
- Android (.apk 파일)
- Samsung Knox (.apk 파일)
- Android Enterprise (.apk 파일)

참고:

Google Play Store 에서 엔터프라이즈 앱으로 다운로드한 앱을 추가하는 작업은 지원되지 않습니다. 대신, Google Play Store 의 앱을 공용 앱 스토어 앱으로 추가하십시오. 공용 앱 스토어 앱 추가에서 자세한 내용을 참조하십시오.

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 열립니다.
2. 추가를 클릭합니다. 앱 추가 대화상자가 나타납니다.

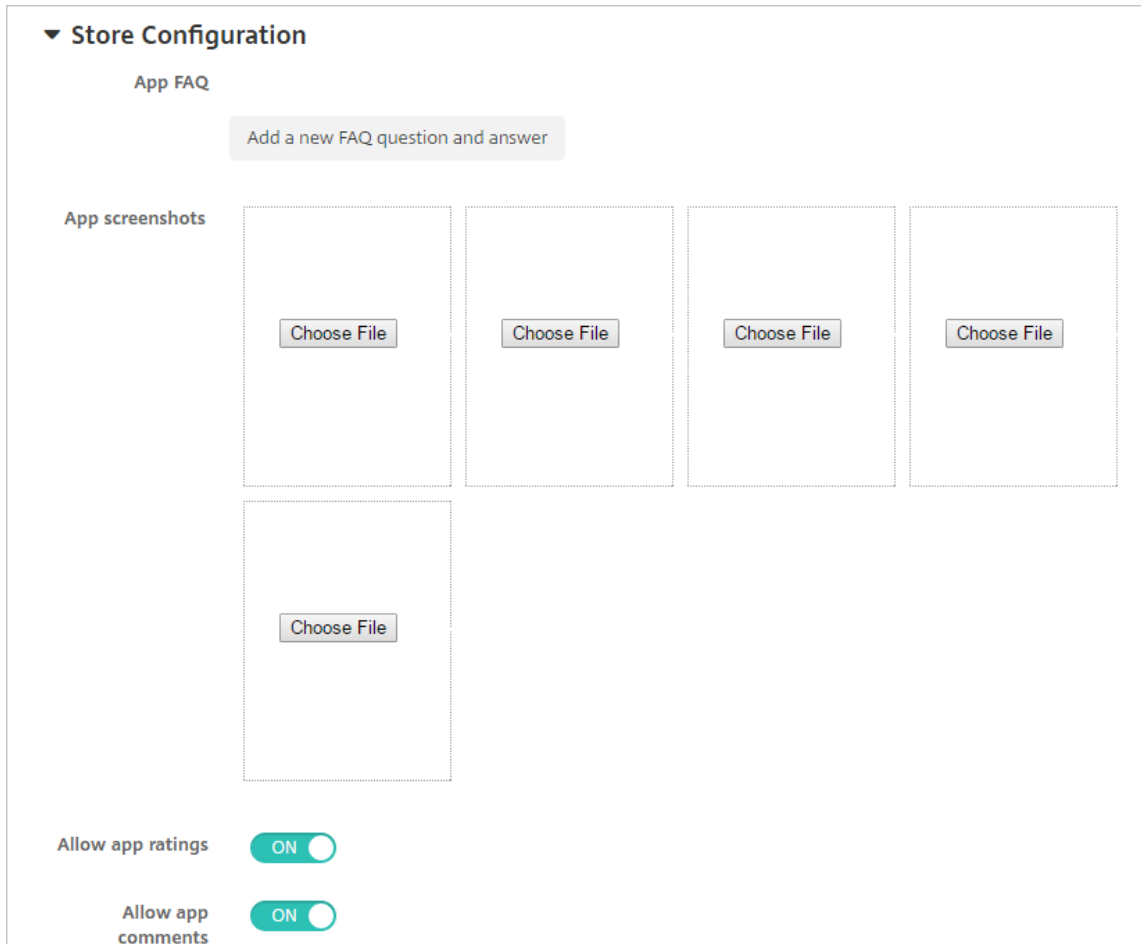


3. 엔터프라이즈를 클릭합니다. 앱정보페이지가 나타납니다.
4. 앱정보창에서 다음 정보를 입력합니다.
 - 이름: 앱의 설명적 이름을 입력합니다. 이 이름은 앱 테이블의 앱 이름 아래에 나타납니다.
 - 설명: 앱의 선택적 설명을 입력합니다.
 - 앱 범주: 필요한 경우 목록에서 앱을 추가할 범주를 클릭합니다. 앱 범주에 대한 자세한 내용은 앱 범주 만 들 기 를 참조하십시오.
5. 다음을 클릭합니다. 앱 플랫폼 페이지가 나타납니다.
6. 플랫폼 아래에서 추가할 플랫폼을 선택합니다. 하나의 플랫폼에 대해서만 구성하는 경우 다른 플랫폼의 선택을 취소합니다. 플랫폼 설정 구성을 마치면 10 단계에서 플랫폼 배포 규칙을 설정하는 방법을 참조하십시오.
7. 선택한 각 플랫폼에 대해 찾아보기를 클릭하고 파일의 위치로 이동하여 업로드할 파일을 선택합니다.
8. 다음을 클릭합니다. 플랫폼에 대한 앱 정보 페이지가 나타납니다.
9. 다음과 같은 플랫폼 유형에 대한 설정을 구성합니다.
 - 파일 이름: 필요한 경우 앱의 새 이름을 입력합니다.
 - 앱 설명: 필요한 경우 앱에 대한 새 설명을 입력합니다.
 - 앱 버전: 이 필드는 변경할 수 없습니다.
 - 최소 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행할 수 있는 운영체제의 가장 이전 버전을 입력합니다.
 - 최대 OS 버전: 필요한 경우 장치에서 앱을 사용할 때 실행해야 하는 운영체제의 가장 최신 버전을 입력합니다.
 - 제외된 장치: 필요한 경우 앱을 실행할 수 없는 장치의 제조업체 또는 모델을 입력합니다.
 - MDM 프로파일 제거된 경우 제거: MDM 프로파일 제거된 경우 장치에서 앱을 제거할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 앱 데이터 백업 방지: 앱 데이터를 백업하는 것을 방지할지 여부를 선택합니다. 기본값은 켜짐입니다.

- 강제로앱관리: 관리되지않는앱을설치하는경우감독되지않는장치의사용자에게앱관리를허용하라는메시지를표시하려면 켜짐을선택합니다. 사용자가메시지를수락하면앱이관리됩니다. 이설정은 iOS 9.x 장치에적용됩니다.

10. 배포규칙을구성합니다. 자세한내용은 [리소스배포](#)에서참조하십시오.

11. **XenMobile Store** 구성을확장합니다.



필요한경우 XenMobile Store 에나타나는앱또는화면캡처에대한 FAQ 를추가할수있습니다. 또한사용자의앱평가또는 설명추가를허용할지여부를설정할수있습니다.

다음설정을구성합니다.

- 앱 **FAQ**: 앱에대한 FAQ(질문과답변) 를추가합니다.
- 앱스크린샷: XenMobile Store 의앱을분류하는데도움이되는화면캡처를추가합니다. 업로드하는그래픽은 PNG 여야합니다. GIF 또는 JPEG 이미지는업로드할수없습니다.
- 앱등급허용: 사용자의앱평가를허용할지여부를선택합니다. 기본값은 켜짐입니다.
- 앱설명허용: 선택한앱에대한사용자의설명을허용할지여부를선택합니다. 기본값은 켜짐입니다.

12. 다음을클릭합니다. 승인페이지가나타납니다.

사용자계정을만들때승인이필요한경우워크플로를사용합니다. 승인워크플로를설정하지않아도되는경우 13 단계로건너뚫 수있습니다.

워크플로를 할당하거나 만들어야 하는 경우 다음 설정을 구성합니다.

- 사용할 워크플로: 목록에서 기존 워크플로를 클릭하거나 새 워크플로 만들기 버튼을 클릭합니다. 기본값은 없음입니다.
- 새 워크플로 만들기 선택하는 경우 다음 설정을 구성합니다.
 - 이름: 워크플로의 고유한 이름을 입력합니다.
 - 설명: 필요한 경우 워크플로의 설명을 입력합니다.
 - 전자메일 승인 템플릿: 목록에서 할당할 전자메일 승인 템플릿을 선택합니다. 이 필드 오른쪽에 있는 눈모양 아이콘을 클릭하면 템플릿을 미리 볼 수 있는 대화상자가 나타납니다.
 - 관리자 승인 수준: 목록에서 이 워크플로에 필요한 관리자 승인 수준의 번호를 선택합니다. 기본값은 **1** 수준입니다. 사용 가능한 옵션은 다음과 같습니다.
 - * 필요 없음
 - * 1 수준
 - * 2 수준
 - * 3 수준
 - **Active Directory** 도메인 선택: 목록에서 워크플로에 사용할 적절한 Active Directory 도메인을 선택합니다.
 - 추가로 필요한 승인자 찾기: 검색 필드에 추가로 필요한 사람의 이름을 입력하고 검색을 클릭합니다. 이름은 Active Directory 에서 가져옵니다.
 - 필드 이름이 나타나면 해당하는 이름 옆의 확인란을 선택합니다. 이름과 전자메일 주소가 추가로 필요한 승인자 선택된 목록에 나타납니다.
 - * 추가로 필요한 승인자 선택된 목록에서 사용자를 제거하려면 다음 중 하나를 수행합니다.
 - 선택한 도메인에 있는 모든 사용자의 목록을 표시하려면 검색을 클릭합니다.
 - 검색 결과를 제한하려면 검색 상자에 이름 전체 또는 일부를 입력한 다음 검색을 클릭합니다.
 - 추가로 필요한 승인자 선택된 목록에 있는 사용자는 검색 결과 목록에서 해당 이름 옆에 확인 표시가 있습니다. 목록을 스크롤하고 제거하려는 각 이름 옆에 있는 확인란의 선택을 취소합니다.

13. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.

14. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.

15. 배포 일정을 확장하고 다음 설정을 구성합니다.

- 배포 옆에서 켜짐을 클릭하여 배포를 예약하거나 꺼짐을 클릭하여 배포를 차단합니다. 기본 옵션은 켜짐입니다.
- 배포 일정 옆에서 지금 또는 나중에를 클릭합니다. 기본 옵션은 지금입니다.
- 나중에를 클릭하는 경우 달력 아이콘을 클릭하고 배포 날짜와 시간을 선택합니다.
- 배포 조건 옆에서 모든 연결에서를 클릭하거나 이전 배포가 실패한 경우에만 클릭합니다. 기본 옵션은 모든 연결에서입니다.
- 상시 연결에 대해 배포 옆에서 켜짐 또는 꺼짐을 클릭합니다. 기본 옵션은 꺼짐입니다.

참고:

설정 > 서버 속성에서 백그라운드 배포 예약 기능을 구성한 경우에만 이 옵션이 적용됩니다. iOS 장치에는 상시 연결 옵션을 사용할 수 없습니다.

구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 모든 플랫폼에 적용되지만 상시 연결에 대해 배포를 선택한 경우 iOS 에는 적용되지 않습니다.

16. 저장을 클릭합니다.

웹링크 추가

XenMobile 에서 SSO(Single Sign-On) 가 필요 없는 웹 앱이나 공용 또는 개인 사이트에 대한 웹 주소 (URL) 를 설정할 수 있습니다.

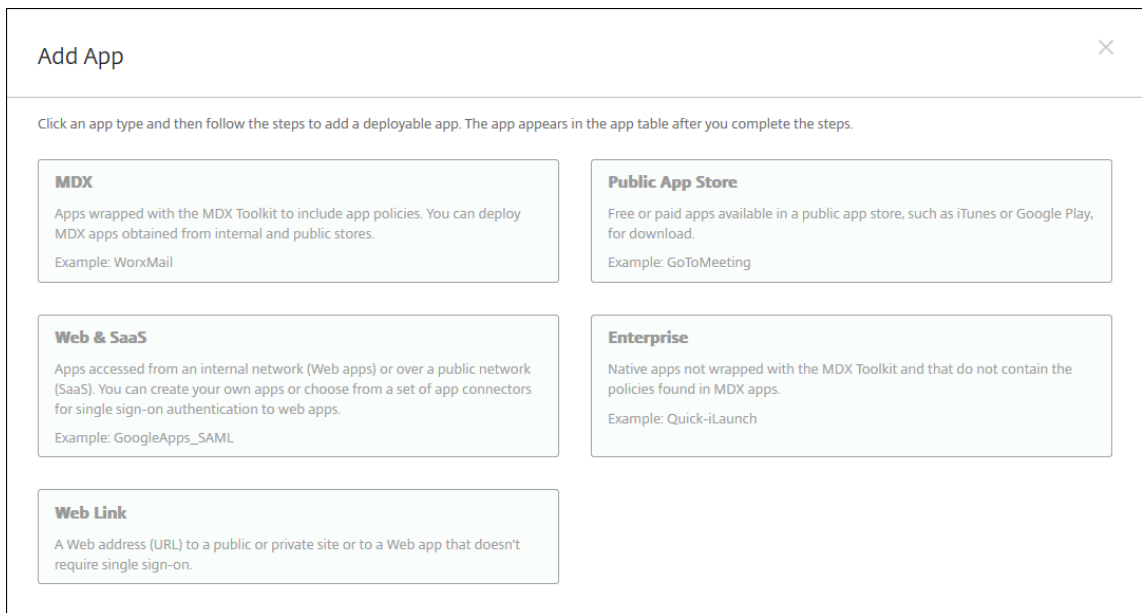
XenMobile 콘솔의 앱 탭에서 웹 링크를 구성할 수 있습니다. 웹 링크 구성을 마치면 링크가 앱 테이블의 목록에 링크 아이콘으로 나타납니다. 사용자가 Secure Hub 에 로그인하면 사용 가능한 앱 및 데스크톱의 목록과 함께 링크가 표시됩니다.

링크를 추가하려면 다음 정보를 제공합니다.

- 링크 이름
- 링크 설명
- 웹 주소 (URL)
- 범주
- 역할
- .png 형식의 이미지 (선택 사항)

1. XenMobile 콘솔에서 구성 > 앱을 클릭합니다. 앱 페이지가 나타납니다.

2. 추가를 클릭합니다. 앱 추가 대화상자가 나타납니다.



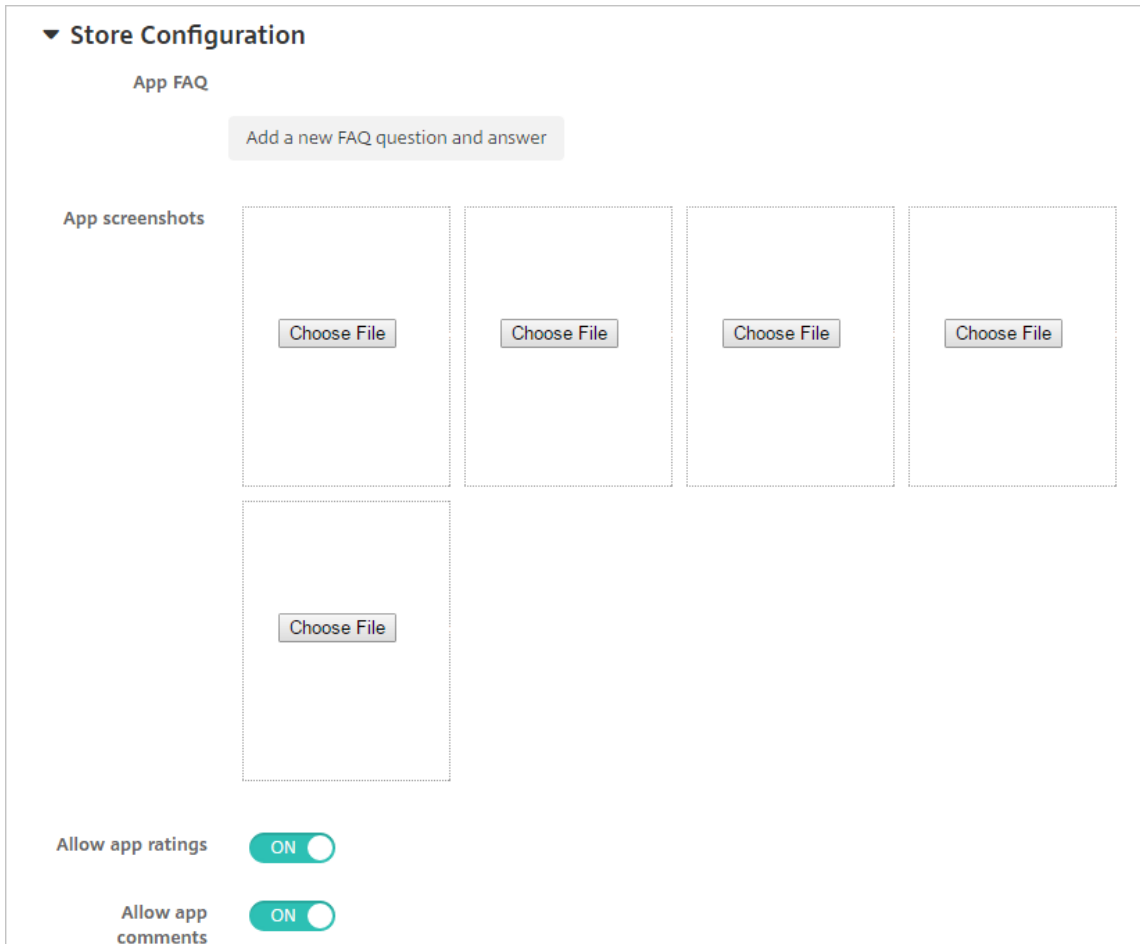
3. 웹 링크를 클릭합니다. 앱 정보 페이지가 나타납니다.

4. 다음 설정을 구성합니다.

- 앱 이름: 미리 채워진 이름을 사용하거나 새 이름을 입력합니다.

- 앱설명: 미리채워진설명을사용하거나직접설명을입력합니다.
- **URL:** 미리채워진 URL 을사용하거나앱의웹주소를입력합니다. 선택한커넥터에따라다음페이지로이동하기전에 바꿔야하는자리표시자가이필드에포함될수있습니다.
- 앱이내부네트워크에서호스트됨: 앱이내부네트워크의서버에서실행되는지여부를선택합니다. 원격위치에서내부앱에연결하는사용자의경우 NetScaler Gateway 를통해연결해야합니다. 이옵션을 켜짐으로설정하면 VPN 키워드가앱에추가되고사용자가 NetScaler Gateway 를통해연결할수있습니다. 기본값은 꺼짐입니다.
- 앱범주: 목록에서앱에적용할선택적범주를클릭합니다.
- 이미지: 기본 Citrix 이미지를사용할지, 고유한앱이미지를업로드할지여부를선택합니다. 기본값은기본값사용입니다.
 - 고유한이미지를업로드하려면 찾아보기를클릭하고파일의위치로이동합니다. 파일은.PNG 파일이어야합니다. JPEG 또는 GIF 파일은업로드할수없습니다. 사용자지정그래픽을추가하면나중에변경할수없습니다.

5. XenMobile Store 구성을확장합니다.



필요한경우 XenMobile Store 에나타나는앱또는화면캡처에대한 FAQ 를추가할수있습니다. 또한사용자의앱평가또는 설명추가를허용할지여부를설정할수있습니다.

다음설정을구성합니다.

- 앱 **FAQ:** 앱에대한 FAQ(질문과답변) 를추가합니다.

- 앱스크린샷: XenMobile Store 의 앱을 분류하는데 도움이 되는 화면 캡처를 추가합니다. 업로드하는 그래픽은 PNG 여야합니다. GIF 또는 JPEG 이미지는 업로드할 수 없습니다.
 - 앱등급허용: 사용자의 앱 평가를 허용할지 여부를 선택합니다. 기본값은 켜짐입니다.
 - 앱설명허용: 선택한 앱에 대한 사용자의 설명을 허용할지 여부를 선택합니다. 기본값은 켜짐입니다.
6. 다음을 클릭합니다. 배달 그룹 할당 페이지가 나타납니다.
 7. 배달 그룹 선택 옆에서 배달 그룹을 입력하여 찾거나 목록에서 그룹을 하나 이상 선택합니다. 선택한 그룹이 앱 할당을 받을 배달 그룹 목록에 나타납니다.
 8. 배포 일정을 확장하고 다음 설정을 구성합니다.
 - 배포 옆에서 켜짐을 클릭하여 배포를 예약하거나 꺼짐을 클릭하여 배포를 차단합니다. 기본 옵션은 켜짐입니다.
 - 배포 일정 옆에서 지금 또는 나중에를 클릭합니다. 기본 옵션은 지금입니다.
 - 나중에를 클릭하는 경우 달력 아이콘을 클릭하고 배포 날짜와 시간을 선택합니다.
 - 배포 조건 옆에서 모든 연결에서를 클릭하거나 이전 배포가 실패한 경우에만을 클릭합니다. 기본 옵션은 모든 연결에서입니다.
 - 상시 연결에 대해 배포 옆에서 켜짐 또는 꺼짐을 클릭합니다. 기본 옵션은 꺼짐입니다.
- 참고:
- 설정 > 서버 속성에서 백그라운드 배포 예약 키를 구성한 경우에만이 옵션이 적용됩니다. iOS 장치에는 상시 연결 옵션을 사용할 수 없습니다.
- 구성하는 배포 일정은 모든 플랫폼에 동일하게 적용됩니다. 변경 사항은 모든 플랫폼에 적용되지만 상시 연결에 대해 배포를 선택한 경우 iOS 에는 적용되지 않습니다.
9. 저장을 클릭합니다.

Microsoft 365 앱 사용

MDX 컨테이너를 열어 Secure Mail, Secure Web 및 ShareFile 에서 Microsoft Office 365 앱으로 문서 및 데이터를 전송할 수 있습니다. 자세한 내용은 [Office 365 앱과 보안 상호 작용 허용](#)에서 참조하십시오.

워크플로 만들기 및 관리

워크플로를 사용하여 사용자 계정의 생성 및 제거를 관리할 수 있습니다. 워크플로를 사용하려면 먼저 조직에서 사용자 계정 요청을 승인할 권한이 있는 담당자를 식별합니다. 그런 다음 워크플로 템플릿을 사용하여 사용자 계정 요청을 만들고 승인할 수 있습니다.

XenMobile 을 처음으로 설정하는 경우 워크플로를 사용하기 전에 먼저 워크플로 전자 메일 설정을 구성해야 합니다. 워크플로 전자 메일 설정은 언제든지 변경할 수 있습니다. 이러한 설정에는 전자 메일 서버, 포트, 전자 메일 주소 및 사용자 계정 생성 요청에 승인이 필요한지 여부도 포함됩니다.

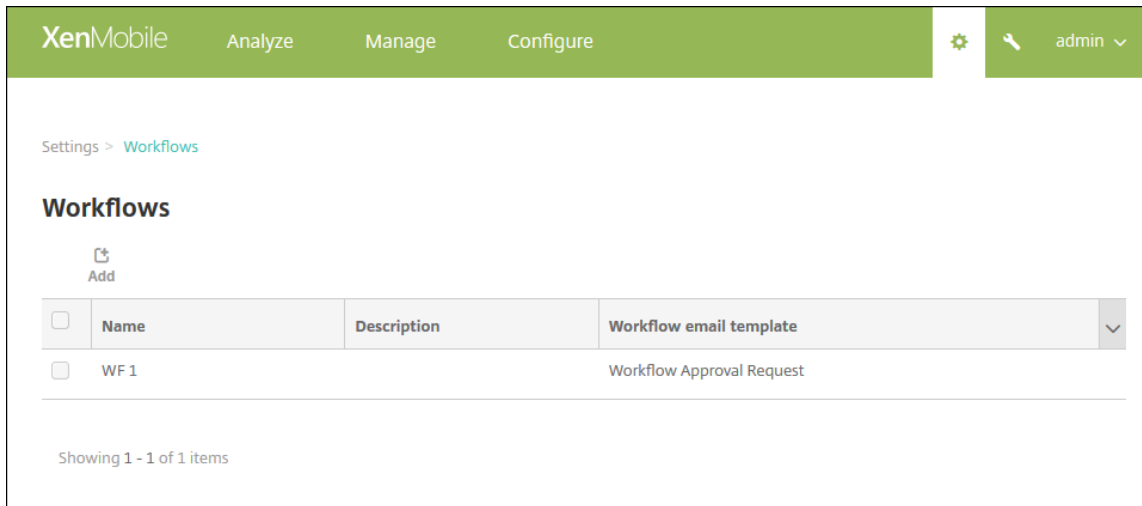
XenMobile 의 두 위치에서 워크플로를 구성할 수 있습니다.

- XenMobile 콘솔의 워크플로 페이지. 워크플로 페이지에서 앱 구성에 사용할 여러 워크플로를 구성할 수 있습니다. 워크플로 페이지에서 워크플로를 구성하는 경우 앱을 구성할 때 워크플로를 선택할 수 있습니다.

- 앱의응용프로그램커넥터를구성할때워크플로이름을입력한다음사용자계정요청을승인할수있는사용자를구성합니다.

사용자계정에대한관리자승인을최대 3 개수준까지할당할수있습니다. 사용자계정을승인할다른사용자가필요한경우이름또는전자메일주소를사용하여해당사용자를검색하고선택할수있습니다. XenMobile 에서해당사용자가검색되면워크플로에추가하면됩니다. 새사용자계정에대한승인또는거부를위한전자메일이워크플로의모든사용자에게전송됩니다.

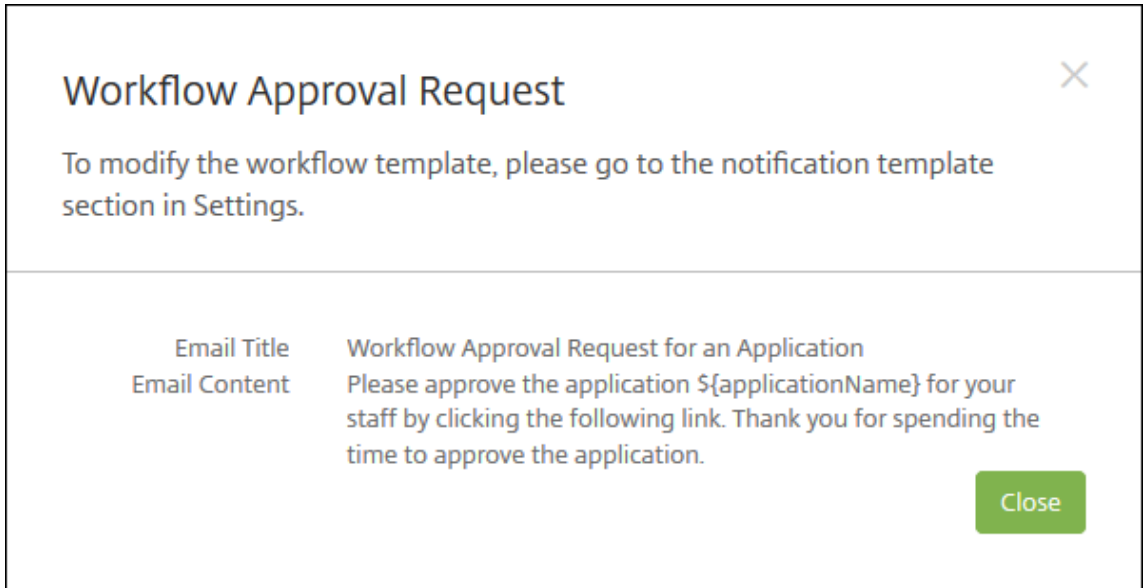
1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 워크플로를클릭합니다. 워크플로페이지가나타납니다.



3. 추가를클릭합니다. 워크플로추가페이지가나타납니다.

4. 다음설정을구성합니다.

- 이름: 워크플로의고유한이름을입력합니다.
- 설명: 필요한경우워크플로의설명을입력합니다.
- 전자메일승인템플릿: 목록에서할당할전자메일승인템플릿을선택합니다. XenMobile 콘솔의설정아래알림플릿섹션에서전자메일템플릿을만들수있습니다. 이필드의오른쪽에있는눈아이콘을클릭하면다음대화상자가나타납니다.



- 관리자승인수준: 목록에서이워크플로에필요한관리자승인수준의번호를선택합니다. 기본값은 1 수준입니다. 사용 가능한옵션은다음과같습니다.
 - 필요없음
 - 1 수준
 - 2 수준
 - 3 수준
- **Active Directory** 도메인선택: 목록에서이워크플로에사용할적절한 Active Directory 도메인을선택합니다.
- 추가로필요한승인자찾기: 검색필드에추가로필요한사람의이름을입력하고 검색을클릭합니다. 이름은 Active Directory 에서가져옵니다.
- 필드에이름이나타나면해당하는이름옆의확인란을선택합니다. 이름과전자메일주소가 추가로필요한승인자선택됨 목록에나타납니다.
- 추가로필요한승인자선택됨목록에서사용자를제거하려면다음중하나를수행합니다.
 - 선택한도메인에있는모든사용자의목록을표시하려면 검색을클릭합니다.
 - 검색결과를제한하려면검색상자에이름전체또는일부를입력한다음 검색을클릭합니다.
 - 추가로필요한승인자선택됨목록에있는사용자는검색결과목록에서해당이름옆에확인표시가있습니다. 목록을 스크롤하고제거하려는각이름옆에있는확인란의선택을취소합니다.

5. 저장을클릭합니다. 생성된워크플로가 워크플로페이지에표시됩니다.

워크플로를만든후워크플로세부정보를보거나워크플로연결된앱을보거나워크플로를삭제할수있습니다. 워크플로를만든후에는워크플로를편집할수없습니다. 승인수준또는승인자가다른워크플로가필요한경우다른워크플로를만들어야합니다.

세부정보를보고워크플로를삭제하려면

1. 워크플로페이지에서테이블의행을클릭하거나워크플로옆의확인란을선택하여워크플로를선택합니다.

2. 워크플로를 삭제하려면 삭제를 클릭합니다. 확인 대화상자가 나타납니다. 삭제를 다시 클릭합니다.

중요:

이 작업은 실행 취소할 수 없습니다.

앱스토어 및 Citrix Secure Hub 브랜딩

앱스토어에 나타나는 방식을 설정하고 Secure Hub 및 앱스토어 브랜드를 나타내는 로고를 추가할 수 있습니다. 이러한 브랜드 기능은 iOS 및 Android 장치에서 사용할 수 있습니다.

참고:

시작하기 전에 사용자 지정 이미지가 준비되었으며 액세스할 수 있는지 확인하십시오.

사용자 지정 이미지는 다음과 같은 요구 사항을 충족해야 합니다.

- 파일은 .png 형식이어야 합니다.
- 72dpi 의 투명한 배경에 순수한 흰색 로고 또는 텍스트를 사용합니다.
- 회사 로고는 높이 또는 너비가 170px x 25px(1x) 및 340px x 50px(2x) 를 초과해서는 안 됩니다.
- 파일의 이름을 Header.png 및 Header@2x.png 로 지정합니다.
- .zip 파일을 만듭니다. 이 파일 내부에 파일이 포함된 폴더가 있어서서는 안 됩니다.

1. XenMobile Server 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.

2. 클라이언트에서 클라이언트 브랜딩을 클릭합니다. 클라이언트 브랜딩 페이지가 나타납니다.

The screenshot shows the 'Client Branding' configuration page in the XenMobile console. The page has a green header with navigation tabs: XenMobile, Analyze, Manage, and Configure. On the right, there are icons for settings, a user profile, and the name 'admin'. The main content area is titled 'Client Branding' and includes a sub-header: 'You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.' Below this, there are several configuration options: 'Store name*' with a text input field containing 'Store'; 'Default store view' with radio buttons for 'Category' and 'A-Z' (selected); 'Device' with radio buttons for 'Phone' (selected) and 'Tablet'; and 'Branding file' with a text input field and a 'Browse' button. A 'Note' section at the bottom provides the following details: 'The file must be in .png format (pure white logo/text with transparent background at 72 dpi).', 'The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).', 'Files should be named as Header.png and Header@2x.png.', and 'A zip file should be created from the files, not a folder with the files inside of it.'

다음 설정을 구성합니다.

- 스토어 이름: 사용자 계정 정보에 나타나는 스토어 이름입니다. 이름을 변경하면 스토어 서비스에 액세스하는 데 사용되는 URL 도 변경됩니다. 일반적으로 기본 이름을 변경할 필요가 없습니다.

중요:

스토어이름에는영숫자만사용할수있습니다.

- 기본스토어보기: 범주또는 **A-Z** 를선택합니다. 기본값은 **A-Z** 입니다.
- 장치옵션: 전화또는 태블릿을선택합니다. 기본값은 전화입니다.
- 브랜딩파일: 찾아보기를클릭하고파일위치로이동하여브랜딩에사용할이미지또는이미지의.zip 파일을선택합니다.

3. 저장을클릭합니다.

이패키지를사용자장치에배포하려면배포패키지를만든다음패키지를배포합니다.

앱커넥터유형

August 24, 2018

다음표에는웹또는 SaaS 앱을추가할때 XenMobile 에서사용할수있는커넥터와커넥터유형이나와있습니다. 또한웹또는 SaaS 앱을추가할때새커넥터를 XenMobile 에추가할수도있습니다.

이표에는커넥터가사용자계정관리를지원하는지여부도나타나있습니다. 지원되는경우세계정을자동으로또는워크플로를사용하여 만들수있습니다.

커넥터이름	SSO SAML	사용자계정관리지원
EchoSign_SAML	예	예
Globoforce_SAML		참고: 이커넥터를사용하는경우원활한 SSO 통합을위해 User Management for Provisioning 을사용하도록설정해야합니다.
GoogleApps_SAML	예	예
GoogleApps_SAML_IDP	예	예
Lynda_SAML	예	예
Office365_SAML	예	예
Salesforce_SAML	예	예
Salesforce_SAML_SP	예	예
SandBox_SAML	예	
SuccessFactors_SAML	예	
ShareFile_SAML	예	

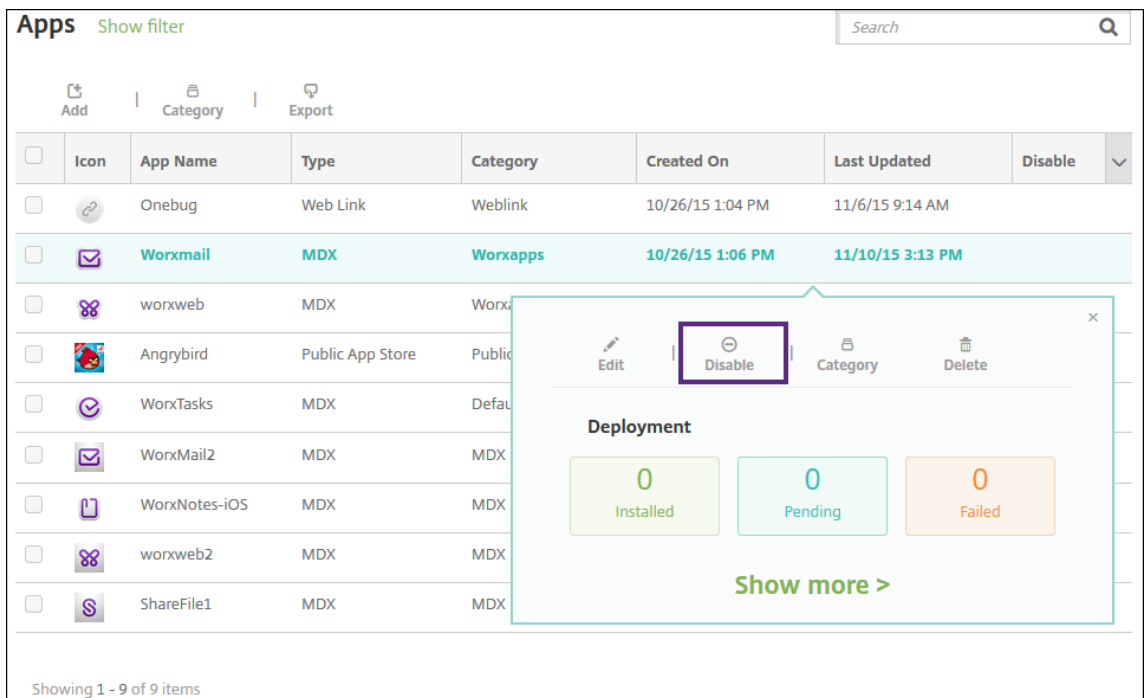
커넥터이름	SSO SAML	사용자계정관리지원
ShareFile_SAML_SP	예	
WebEx_SAML_SP	예	예

MDX 또는엔터프라이즈앱업그레이드

August 23, 2019

XenMobile 에서 MDX 또는엔터프라이즈앱업그레이드하려면 XenMobile 콘솔에서앱을사용하지않도록설정한다음새버전의앱을업로드합니다.

1. XenMobile 콘솔에서 구성 > 앱을클릭합니다. 앱페이지가나타납니다.
2. 관리되는장치 (모바일장치관리를위해 XenMobile 에등록된장치) 인경우 3 단계로건너뛰십시오. 관리되지않는장치 (엔터프라이즈앱관리용도로만 XenMobile 에등록된장치) 인경우다음을수행하십시오.
 - 앱테이블에서앱옆에있는확인란을선택하거나업데이트하려는앱이포함된라인을클릭합니다.
 - 나타나는메뉴에서 사용안함을클릭합니다.



- 확인대상자에서 사용안함을클릭합니다. 앱의 사용안함열에 사용안함이나타납니다.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
<input type="checkbox"/>		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

참고:

앱을 사용하지 않도록 설정하면 앱이 유지관리 모드가 됩니다. 앱을 사용하지 않도록 설정한 동안 로그오프하면 앱에 다시 연결할 수 없습니다. 앱을 사용하지 않도록 설정하는 것은 선택적인 설정이지만 앱 기능에 문제가 발생하지 않도록 앱을 사용하지 않도록 설정하는 것이 좋습니다. 예를 들어 정책 업데이트 또는 사용자가 XenMobile 에 앱을 업로드하는 동시에 다운로드를 요청하면 문제가 발생할 수 있습니다.

3. 앱 테이블에서 앱 옆에 있는 확인란을 클릭하거나 업데이트하려는 앱이 포함된 라인을 클릭합니다.
4. 나타나는 메뉴에서 편집을 클릭합니다. 선택한 앱에 대해 원래 선택한 플랫폼을 보여주는 앱 정보 페이지가 나타납니다.
5. 다음 설정을 구성합니다.
 - 이름: 필요한 경우 앱 이름을 변경합니다.
 - 설명: 필요한 경우 앱 설명을 변경합니다.
 - 앱 범주: 필요한 경우 앱 범주를 변경합니다.
6. 다음을 클릭합니다. 선택한 첫 번째 플랫폼 페이지가 나타납니다. 선택한 각 플랫폼에 대해 다음을 수행합니다.
 - 업로드를 클릭하고 파일 위치로 이동하여 업로드하려는 대체 파일을 선택합니다. XenMobile 에 앱이 업로드됩니다.
 - 필요한 경우 세부 정보 및 플랫폼에 대한 정책 설정을 변경합니다.
 - 필요한 경우 배포 규칙 및 XenMobile Store 구성을 구성합니다. 자세한 내용은 [앱 추가](#)에서 MDX 앱 추가를 참조하십시오.
7. 저장을 클릭합니다. 앱 페이지가 나타납니다.
8. 2 단계에서 앱을 사용하지 않도록 설정한 경우 다음을 수행하십시오.
 - 앱 테이블에서 업데이트한 앱을 클릭하여 선택한 다음 나타나는 메뉴에서 사용을 클릭합니다.
 - 나타나는 확인 대화 상자에서 사용을 클릭합니다. 이제 사용자가 앱에 액세스하여 앱을 업그레이드 하라는 알림을 받을 수 있습니다.

MDX 앱 정책 요약

April 11, 2019

iOS 및 Android 에 대한 MDX 앱 정책 과제 한 사항 및 Citrix 권장 사항이나와 있는 표를 보려면 MDX Toolkit 설명서에서 [MDX Apps 정책 요약](#) 을 참조하십시오.

XenMobile Store 및 Citrix Secure Hub 브랜딩

January 6, 2020

앱이스토어에나타나는방식을설정하고 Secure Hub 및 XenMobile Store 브랜드를나타내는로고를추가할수있습니다. 이러한브랜드기능은 iOS 및 Android 장치에서사용할수있습니다.

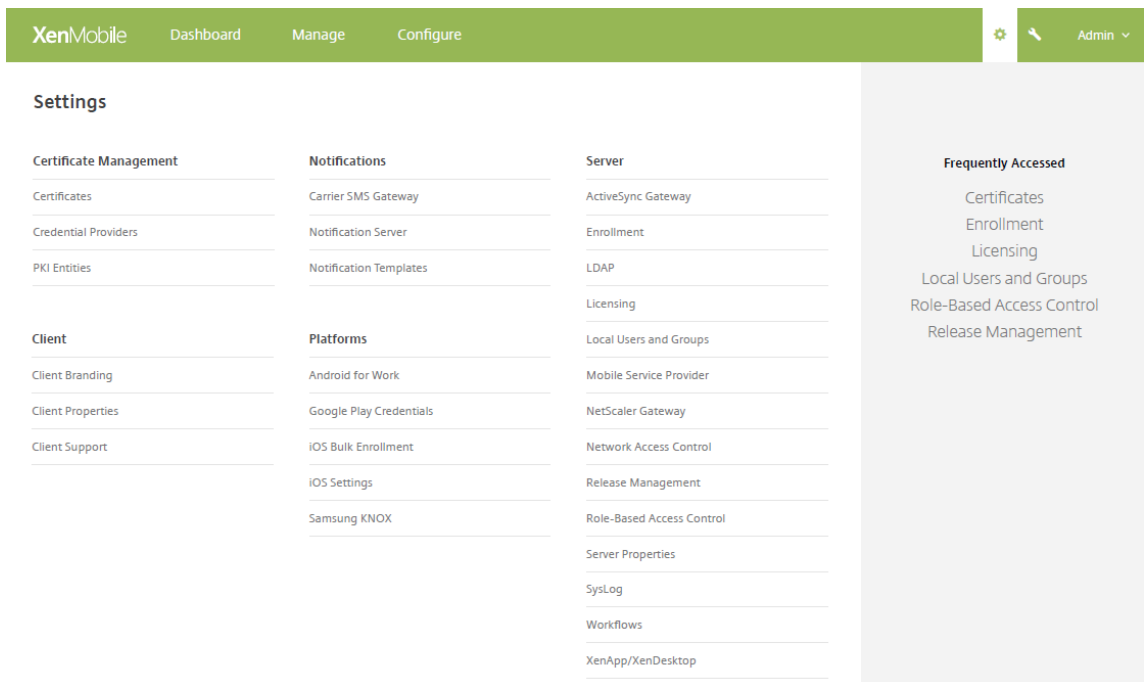
참고:

시작하기전에사용자지정이미지가준비되었으으며액세스할수있는지확인하십시오.

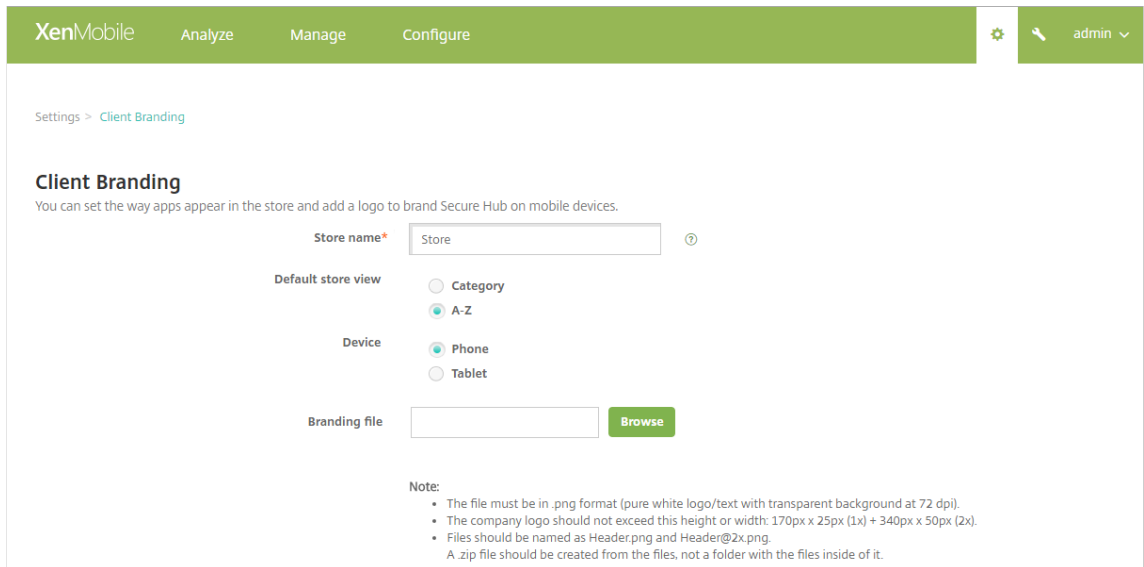
사용자지정이미지는다음과같은요구사항을충족해야합니다.

- 파일은 .png 형식이여야합니다.
- 72dpi 의투명한배경에순수한흰색로고또는텍스트를사용합니다.
- 회사로고는높이또는너비가 170px x 25px(1x) 및 340px x 50px(2x) 를초과해서는안됩니다.
- 파일의이름을 Header.png 및 Header@2x.png 로지정합니다.
- .zip 파일을만듭니다. 이파일내부에파일이포함된폴더가있어서는안됩니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.



2. 클라이언트에서 클라이언트브랜딩을클릭합니다. 클라이언트브랜딩페이지가나타납니다.



다음설정을구성합니다.

- **스토어이름:** 사용자계정정보에나타나는스토어이름입니다. 이름을변경하면스토어서비스에액세스하는데사용되는 URL 도변경됩니다. 일반적으로기본이름을변경할필요가없습니다.

중요:

스토어이름에는영숫자만사용할수있습니다.

- **기본스토어보기:** 범주또는 **A-Z** 를선택합니다. 기본값은 **A-Z** 입니다.
- **장치옵션:** 전화또는 태블릿을선택합니다. 기본값은 전화입니다.
- **브랜딩파일:** 찾아보기를클릭하고파일위치가이동하여브랜딩에사용할이미지또는이미지의.zip 파일을선택합니다.

3. 저장을클릭합니다.

이패키지를사용자장치에배포하려면배포패키지를만든다음패키지를배포합니다.

Citrix Launcher

January 6, 2020

Citrix Launcher 를사용하면 XenMobile 에의해배포되는 Android 장치의사용자환경을사용자지정할수있습니다. Citrix Launcher 의 Secure Hub 관리를위해지원되는최소 Android 버전은 Android 4.0.3 입니다. Citrix Launcher 및 Launcher 구성장치정책은 Android Enterprise 와호환되지않습니다.

이러한 Citrix Launcher 기능을제어하는 **Launcher** 구성정책을추가할수있습니다.

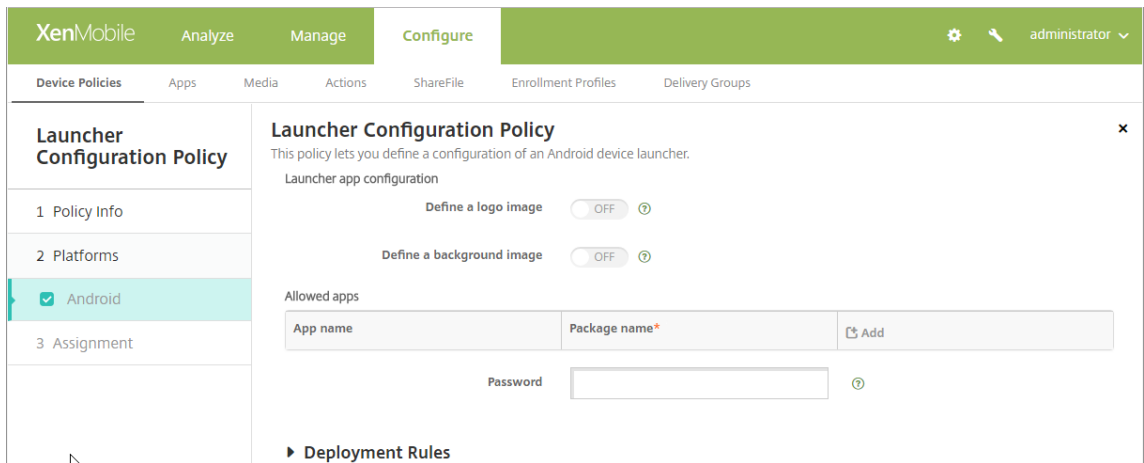
- 사용자가지정된앱에만액세스할수있도록 Android 장치를관리합니다.

- 필요에 따라 Citrix Launcher 아이콘의 사용자 지정 로고 이미지와 Citrix Launcher 의 사용자 지정 배경 이미지를 지정합니다.
- 사용자가 Launcher 를 종료할 때 입력해야 하는 암호를 지정합니다.

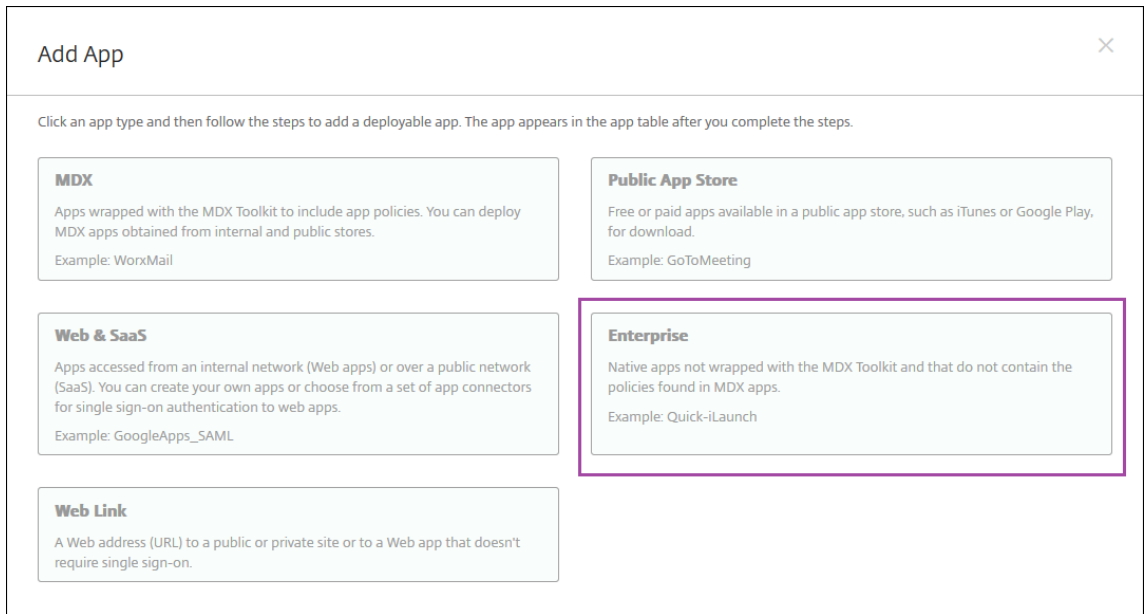
Citrix Launcher 를 사용하면 이러한 장치 수준의 제한을 적용할 수 있는 동시에 사용자에게 Wi-Fi 설정, Bluetooth 설정 및 장치 암호 설정과 같은 장치 설정에 대한 기본 제공 액세스를 부여할 수 있습니다. Citrix Launcher 는 장치 플랫폼 이미지가 제공하는 보안에 추가적인 보안 계층을 더하기 위한 것이 아닙니다.

Android 장치에 Citrix Launcher 를 제공하려면 다음과 같은 일반 단계를 따르십시오.

1. 해당 XenMobile 버전의 [Citrix XenMobile 다운로드](#) 페이지에서 Citrix Launcher 앱을 다운로드합니다. 파일 이름은 CitrixLauncher.apk 입니다. 이 파일은 XenMobile 에 업로드 가능하며 래핑이 필요 없습니다.
2. 장치 정책 **Launcher** 구성 정책을 추가합니다. 구성 > 장치 정책으로 이동한 후 추가를 클릭하고 새 정책 추가 대화 상자에서 **Launcher** 를 입력합니다. 자세한 내용은 [Launcher 구성 정책](#)에서 참조하십시오.

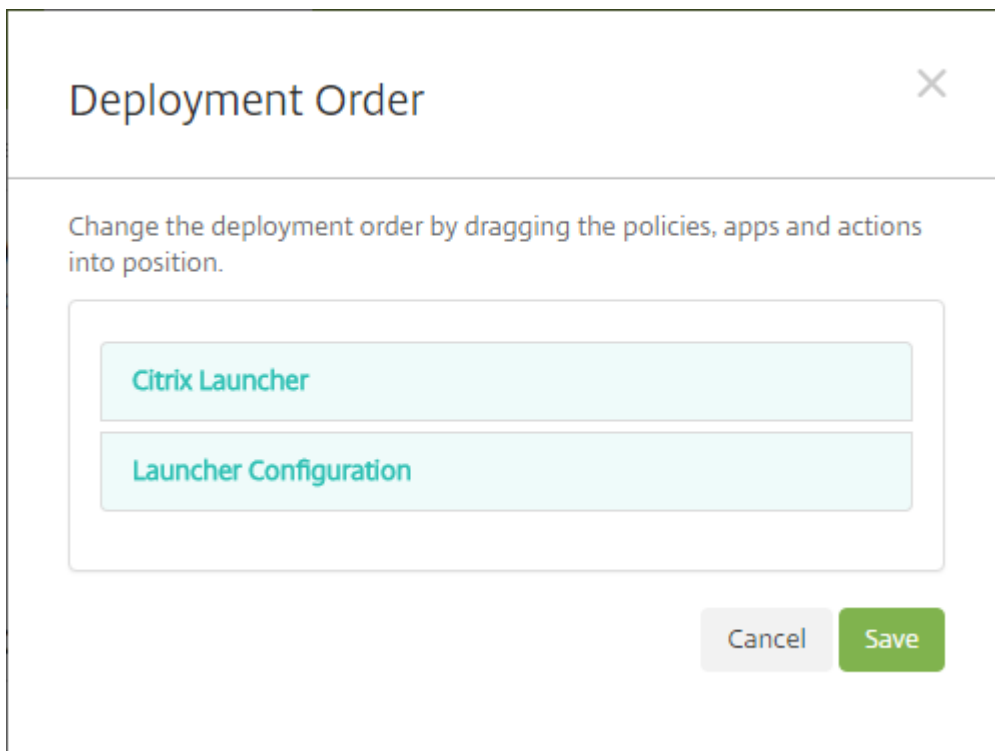


3. Citrix Launcher 앱을 XenMobile 에 엔터프라이즈 앱으로 추가합니다. 구성 > 앱에서 추가를 클릭한 후 엔터프라이즈를 클릭합니다. 자세한 내용은 [엔터프라이즈 앱 추가](#)에서 참조하십시오.



4. 구성 > 배달그룹에서다음구성을사용하여 Citrix Launcher 에대한배달그룹을만듭니다.

- 정책페이지에서 **Launcher** 구성정책을추가합니다.
- 앱페이지에서 **Citrix Launcher** 를 필수앱으로끌어옵니다.
- 요약페이지에서 배포순서를클릭하고 **Citrix Launcher** 앱이 **Launcher** 구성정책보다앞에있는지확인합니다.



자세한내용은 리소스배포에서참조하십시오.

iOS Volume Purchase Program

January 6, 2020

Apple iOS VPP (Volume Purchase Program) 를 사용하여 iOS 앱 라이선스를 관리할 수 있습니다. VPP 솔루션은 조직의 앱 및 기타 데이터를 대량으로 찾고, 구입하고, 배포하는 프로세스를 간소화합니다.

VPP 를 사용하면 XenMobile 에서 공용 앱 스토어 앱을 배포할 수 있습니다. 모바일 생산성 앱 또는 MDX Toolkit 으로 래핑된 앱에는 VPP 가 지원되지 않습니다. XenMobile 공용 스토어 앱을 VPP 로 배포할 수는 있지만 최적화된 배포가 아닙니다. 이러한 제한을 해결하려면 XenMobile Server 와 Secure Hub 스토어가 더 개선되어야 합니다. VPP 를 통한 XenMobile 공용 스토어 앱 배포와 관련된 알려진 문제 및 가능한 해결 방법의 목록은 Citrix [Knowledge Center](#) 의 이 문서를 참조하십시오.

VPP 를 사용하여 해당하는 앱을 장치에 직접 배포할 수 있습니다. 또는 상환 가능한 코드를 사용하여 사용자에게 콘텐츠를 할당할 수 있습니다. XenMobile 에서 iOS VPP 와 관련된 설정을 구성할 수 있습니다.

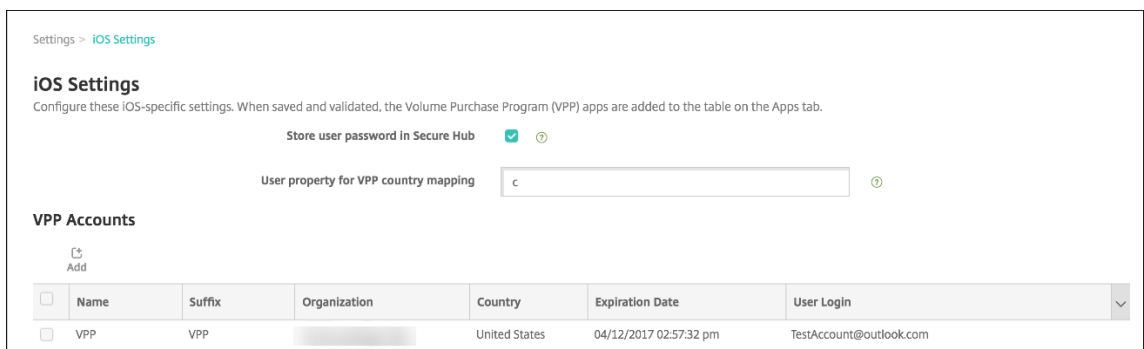
XenMobile 은 Apple 에서 VPP 라이선스를 주기적으로 다시 가져와 해당 라이선스에 모든 변경 내용이 반영되었는지 확인합니다. VPP 에서 가져온 앱을 수동으로 삭제하는 경우가 이러한 변경에 포함됩니다. 기본적으로 XenMobile 은 VPP 라이선스 기준을 최소 720 분마다 새로고칩니다. 새 서버 속성인 VPP 기준 간격 (vpp.baseline) 을 사용하여 기준 간격을 변경할 수 있습니다. 자세한 내용은 [서버 속성](#) 에서 참조하십시오.

이 문서에서는 관리되는 라이선스로 VPP 를 사용하여 XenMobile 에서 앱을 배포하는 방법을 집중적으로 설명합니다. 상환 코드를 사용하고 있고 관리되는 배포로 변경하려는 경우 Apple 지원 문서 ([Volume Purchase Program 을 통해 사용권 코드로서 관리 배포로 마이그레이션하기](#)) 를 참조하십시오.

iOS VPP 에 대한 자세한 내용은 <https://vpp.itunes.apple.com/us/store> 를 참조하십시오. VPP 에 등록하려면 <https://deploy.apple.com/qforms/open/register/check/avs> 로 이동합니다. iTunes 에서 VPP 스토어 액세스하려면 <https://vpp.itunes.apple.com/?l=en> 으로 이동합니다.

이러한 iOS VPP 설정을 XenMobile 에 저장하면 구입한 앱이 XenMobile 콘솔의 구성 > 앱 페이지에 나타납니다.

1. XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 플랫폼에서 **iOS** 설정을 클릭합니다. **iOS** 설정 구성 페이지가 나타납니다.



3. 다음 설정을 구성합니다.

- **Secure Hub** 에서 사용자 암호 저장: XenMobile 인증을 위한 사용자 이름과 암호를 Secure Hub 에 저장할지 여부를 선택합니다. 기본값은 이 보안 방법을 사용하여 정보를 저장하는 것입니다.

- **VPP** 국가매핑을위한사용자속성: 사용자가국가별앱스토어에서앱을다운로드할수있도록하는코드를입력합니다.

XenMobile 은이매핑을사용하여 VPP 의속성폴을선택합니다. 예를들어미국에있는사용자는 VPP 코드가영국인앱을다운로드할수없습니다. 국가매핑코드에대한자세한내용은 VPP 프로그램관리자에게문의하십시오.

4. 추가할각 VPP 계정에대해 추가를클릭합니다. **VPP** 계정추가대화상자가나타납니다.

5. 추가하는각계정에대해다음설정을구성합니다.

참고:

Apple Configurator 1 을사용하는경우라이센스파일을업로드합니다. 구성 > 앱으로이동하고플랫폼페이지에서 **Volume Purchase Program** 을확장합니다.

- 이름: VPP 계정이름을입력합니다.
- 접미사: VPP 계정을통해받은앱이름과함께표시할접미사를입력합니다. 예를들어 **VPP** 를입력하면 Secure Mail 앱이앱목록에 **Secure Mail - VPP** 로표시됩니다.
- 회사토큰: Apple 에서받은 VPP 서비스토큰을복사하고붙여넣습니다. 토큰을받으려면: Apple VPP 포털의 계정요약페이지에서 다운로드단추를클릭하여 VPP 파일을생성하고다운로드합니다. 이파일에는서비스토큰및기타 정보 (예: 국가코드및만료일) 가포함되어있습니다. 파일을안전한위치에서저장합니다.
- 사용자로그인: 사용자지정 B2B 앱을가져올때사용할권한이있는 VPP 계정관리자이름을선택적으로입력합니다.
- 사용자암호: VPP 계정관리자암호를입력합니다.

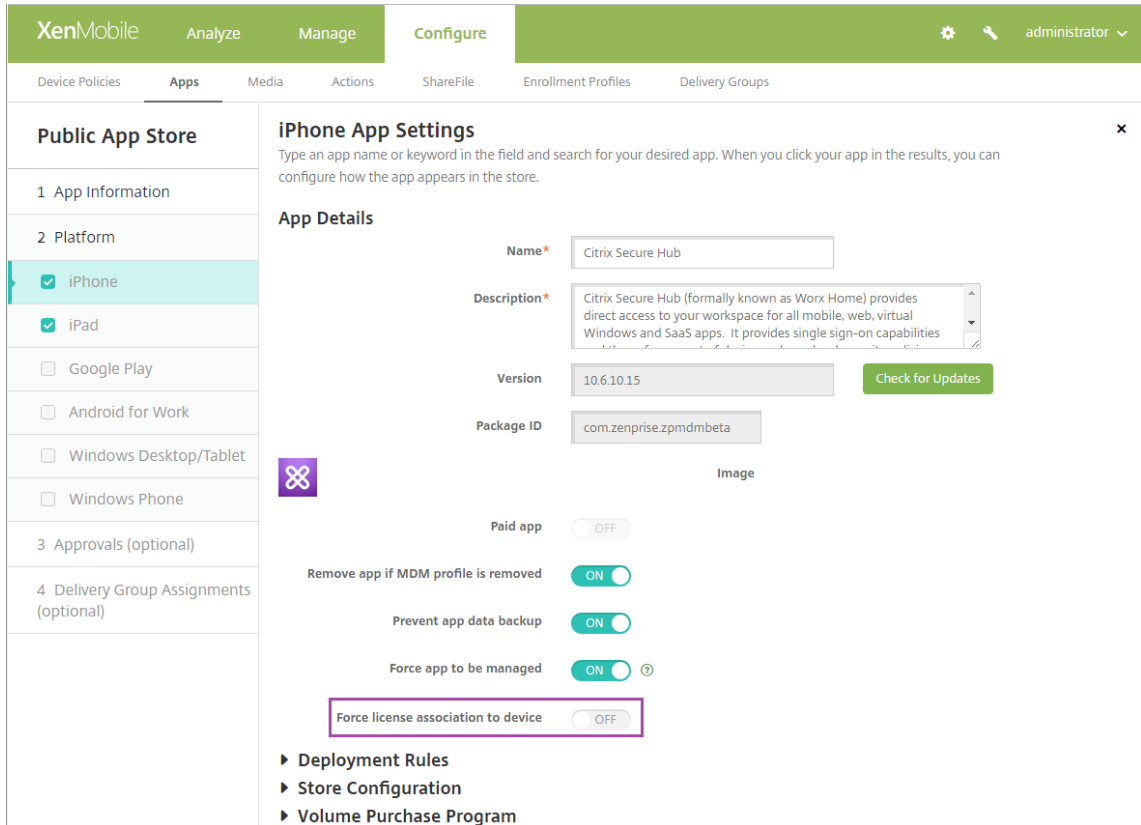
6. 저장을클릭하여대화상자를닫습니다.

7. 저장을클릭하여 iOS 설정을저장합니다.

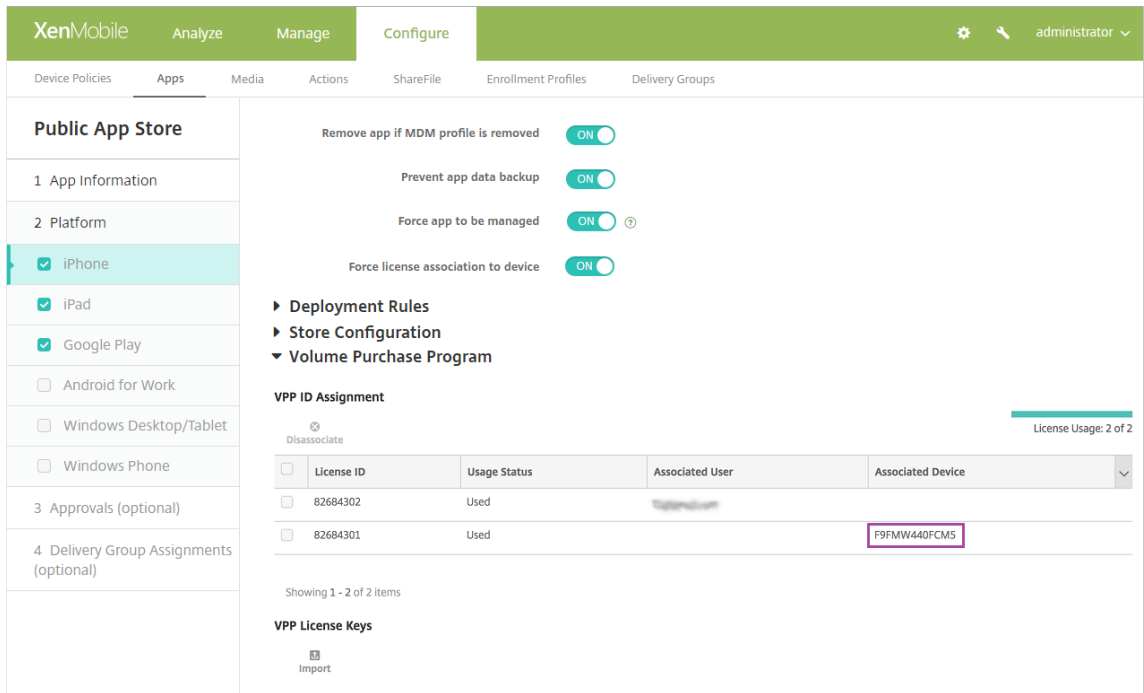
XenMobile 의 구성 > 앱페이지의목록에앱이추가된다는메시지가표시됩니다. 이페이지에서 VPP 계정의앱이름에이전 구성에입력한접미사가포함된것을알수있습니다.

이제 VPP 앱설정을구성하고 VPP 앱에대한배달그룹및배달정책설정을조정할수있습니다. 이러한구성이완료되면사용자가장치를등록할수있습니다. 다음참고는이러한프로세스에대한고려사항을제공합니다.

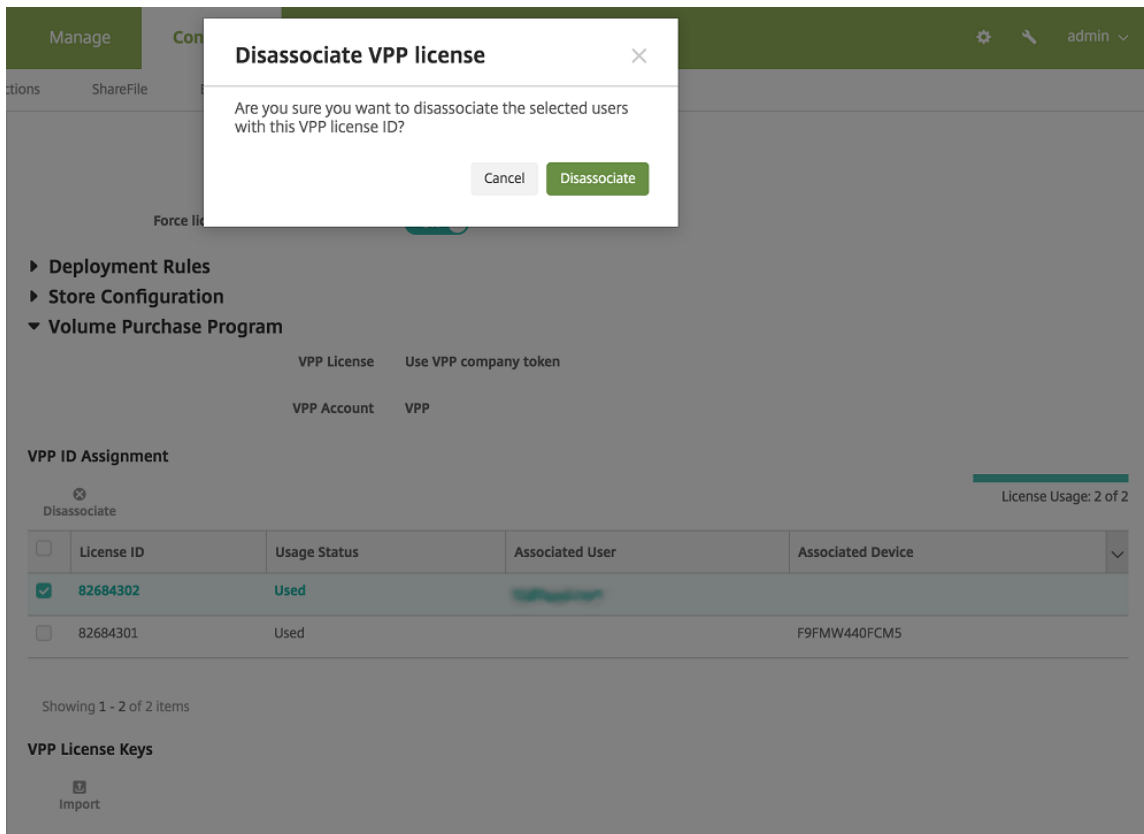
- VPP 앱설정을구성할때 (구성 > 앱) 장치에강제로라이센스연결을사용합니다. Apple VPP 및 DEP 를감독되는장치에서사용할경우 XenMobile 을사용하여사용자수준이아닌장치수준에서앱을할당할수있다는장점이있습니다. 따라서 Apple ID 장치를사용하지않아도됩니다. 또한사용자에게 VPP 프로그램가입을위한초대가전송되지않습니다. 사용자또한 iTunes 계정에로그인하지않고앱을다운로드할수있습니다.



해당앱에대한 VPP 정보를보려면 **Volume Purchase Program** 을확장합니다. **VPP ID** 할당테이블에서라이센스가장치에연결된것을볼수있습니다. 연결된장치열에장치일련번호가표시됩니다. 사용자가토큰을제거한후다시가져오면 Apple 개인정보보호제한으로인해일련번호대신 숨김단어가표시됩니다.

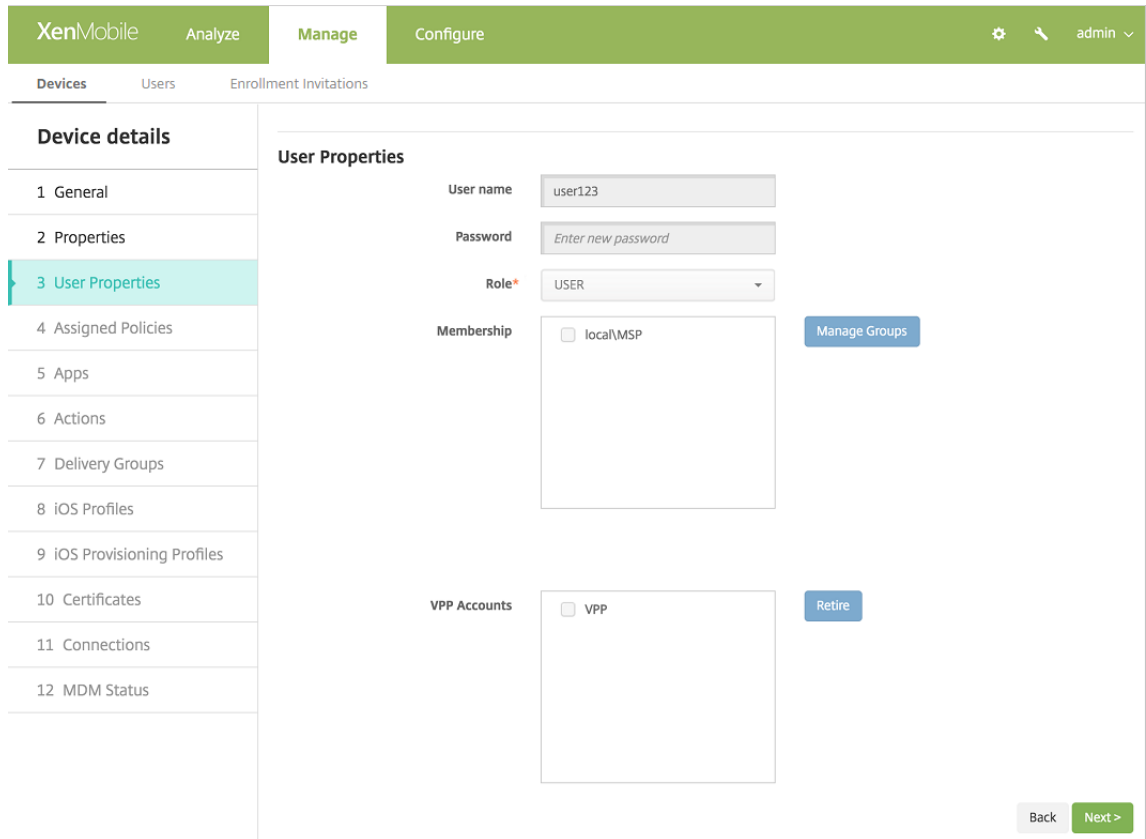


라이선스연결을해제하려면라이선스에대한행을클릭한후 연결해제를클릭합니다.

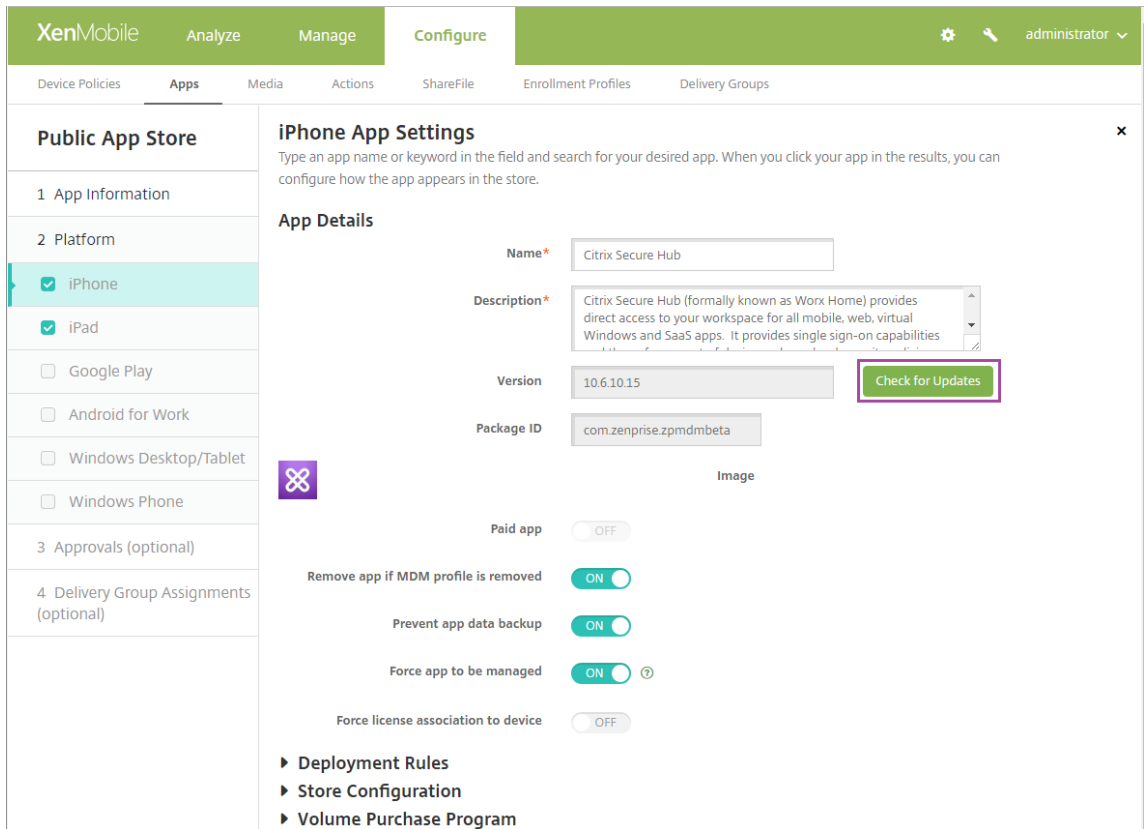


VPP 라이선스를사용자와연결하면 XenMobile 이사용자를 VPP 계정에통합하고사용자의 iTunes ID 를 VPP 계정에 연결합니다. 사용자의 iTunes ID 는회사또는 XenMobile Server 에절대표시되지않습니다. Apple 은이연결을투명

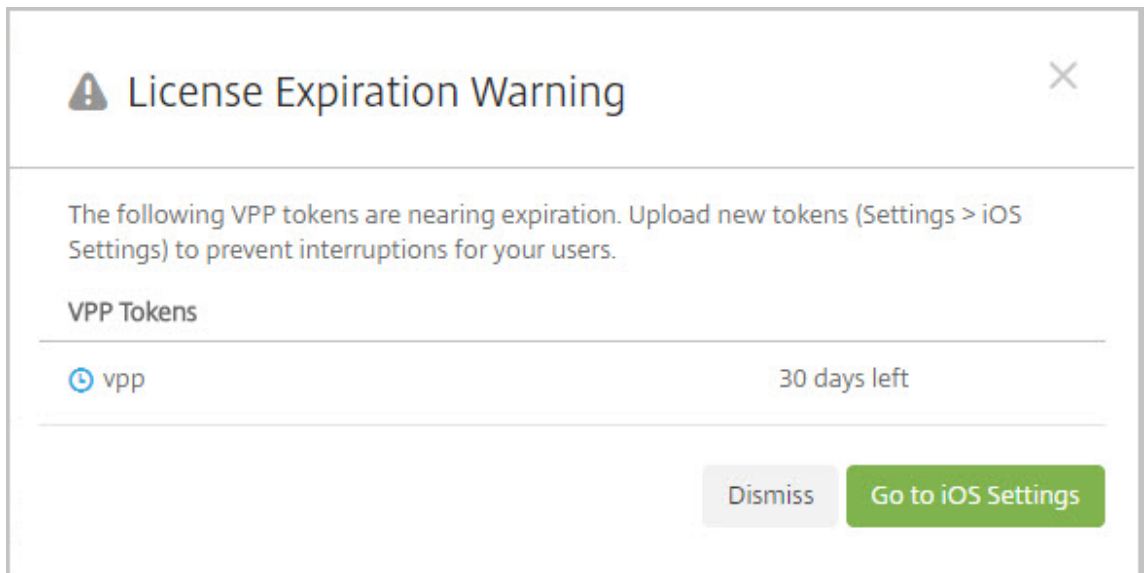
하게 생성하여 사용자 개인정보를 보호합니다. 사용자의 VPP 프로그램 사용을 중지하여 사용자 계정에서 모든 라이선스 연결을 해제할 수 있습니다. 사용자를 사용 중지하려면 관리 > 장치로 이동합니다.



- XenMobile 에서 앱을 배달 그룹에 할당하면 기본적으로 앱이 선택적 앱으로 식별됩니다. XenMobile 이 앱을 장치에 배포하도록하려면 구성 > 배달 그룹으로 이동합니다. 앱 페이지에서 앱을 필수 앱 목록으로 이동합니다.
- 공용 앱스토어 앱에 대한 업데이트가 제공되고 VPP 가 앱을 푸시할 때 장치의 앱은 업데이트를 확인하고 적용하기 전까지 자동으로 업데이트되지 않습니다. 사용자가 아닌 장치에 할당된 Secure Hub 에 대한 업데이트를 푸시하려면 다음을 수행합니다. 구성 > 앱의 플랫폼 페이지에서 업데이트 확인을 클릭하고 업데이트를 적용합니다.



Apple VPP 토큰의 만료일이 가까워지거나 만료된 경우 XenMobile 이라이센스 만료 경고를 표시합니다.



Citrix Secure Hub 를 통한 Virtual Apps and Desktops

September 27, 2019

참고:

Citrix XenApp and XenDesktop 의 이름이 Citrix Virtual Apps and Desktops 로 바뀌었습니다. 일부 문서 및 인터페이스에는 아직 이름 변경이 반영되지 않았습니다.

XenMobile 에서는 Virtual Apps and Desktops 에서 앱을 수집하고 XenMobile Store 를 통해 이러한 앱을 모바일 장치 사용자에게 제공할 수 있습니다. 사용자는 XenMobile Store 내에서 직접 앱을 구독하고 Secure Hub 에서 앱을 시작할 수 있습니다. 앱을 시작하려면 Citrix Receiver 를 사용자 장치에 설치해야 하지만 이를 구성할 필요는 없습니다.

이 설정을 구성하려면 Web Interface 사이트나 StoreFront 의 FQDN(정규화된 도메인 이름) 또는 IP 주소 및 포트 번호가 필요합니다.

1. XenMobile 웹 콘솔에서 오른쪽 위 모서리의 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. **XenApp/XenDesktop** 을 클릭합니다. **XenApp/XenDesktop** 페이지가 나타납니다.

The screenshot shows the 'XenApp/XenDesktop' configuration page. The breadcrumb is 'Settings > XenApp/XenDesktop'. The title is 'XenApp/XenDesktop' with a subtitle 'Allows users to add XenApp and XenDesktop through Secure Hub.' The configuration fields are: Host* (value: net), Port* (value: 80), and Relative Path* (value: /Citrix/StoreAG3/PNAgent/config.xml). There is a 'Use HTTPS' toggle set to 'OFF' and a green 'Test Connection' button. Below the button, a green checkmark indicates 'Connection succeeded'.

3. 다음 설정을 구성합니다.
 - **호스트:** Web Interface 사이트나 StoreFront 의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 입력합니다.
 - **포트:** Web Interface 사이트나 StoreFront 의 포트 번호를 입력합니다. 기본값은 80 입니다.
 - **상대 경로:** 경로를 입력합니다. 예를 들어, /Citrix/PNAgent/config.xml 을 입력할 수 있습니다.
 - **HTTPS 사용:** Web Interface 사이트 또는 StoreFront 와 클라이언트 장치 사이에 보안 인증을 사용할 것인지를 선택합니다. 기본값은 꺼짐입니다.
4. 연결 테스트를 클릭하여 XenMobile 에서 지정된 Virtual Apps and Desktops 서버에 연결할 수 있는지 확인합니다.
5. 저장을 클릭합니다.

XenMobile 에서 ShareFile 사용

January 6, 2020

XenMobile 에는 ShareFile 을통합할수있는두가지옵션즉, ShareFile Enterprise 와 StorageZone 커넥터가있습니다. ShareFile Enterprise 또는 StorageZone 커넥터통합에는 XenMobile Enterprise Edition 이필요합니다.

ShareFile Enterprise

XenMobile Enterprise Edition 을사용하는경우 ShareFile Enterprise 계정에대한엑세스를제공하도록 XenMobile 을구성할수있습니다. 이구성은다음과같습니다.

- 모바일사용자에게파일공유, 파일동기화및 StorageZone 커넥터와같은전체 ShareFile 기능집합에대한엑세스권한을 부여합니다.
- ShareFile 에 XenMobile App 사용자의 Single Sign-on 인증, AD 기반사용자계정프로비전및포괄적인엑세스제어정책을제공할수있습니다.
- XenMobile 콘솔을통해 ShareFile 구성, 서비스수준모니터링및라이선스사용현황모니터링을제공합니다.

ShareFile Enterprise 에대해 XenMobile 을 구성하는방법에자세한내용은 [ShareFile SSO\(Single Sign-on\) 용 SAML](#)을참조하십시오.

StorageZone 커넥터

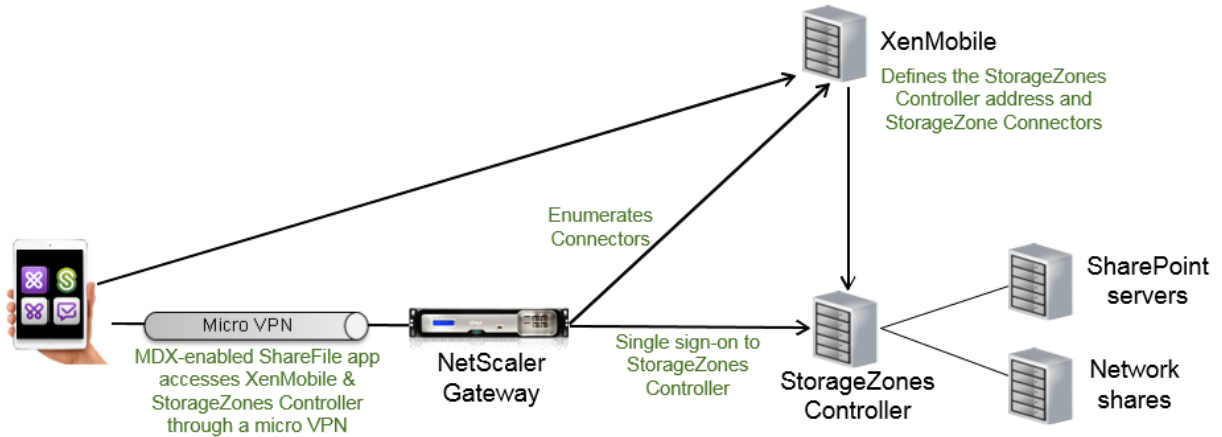
XenMobile 콘솔을통해만든 StorageZone 커넥터에대한엑세스만제공하도록 XenMobile 을구성할수있습니다. 이구성은 다음과같습니다.

- SharePoint 사이트및네트워크파일공유등의기존은-프레미스스토리지저장소에대한보안모바일엑세스를제공합니다.
- ShareFile 하위도메인을설정하거나사용자를 ShareFile 에프로비전하거나 ShareFile 데이터를호스트할필요가없습니다.
- 사용자가모바일에서 iOS 및 Android 용 ShareFile 모바일생산성앱을통해데이터에모바일엑세스할수있습니다. 사용자가 Microsoft Office 문서를편집할수있습니다. 또한모바일장치에서 Adobe PDF 파일을미리보고주석을달수있습니다.
- 사용자정보가회사네트워크밖으로유출되지않도록하는보안제한사항을준수합니다.
- XenMobile 콘솔을통해 StorageZone 커넥터를간단하게설치할수있습니다. 나중에전체 ShareFile 기능을 XenMobile 에서사용하기로결정한경우 XenMobile 콘솔에서구성을변경할수있습니다.
- XenMobile Enterprise Edition 이필요합니다.

XenMobile 과 StorageZone 커넥터전용통합의경우:

- ShareFile 은 NetScaler Gateway 에대한 Single Sign-On 구성을사용하여 StorageZones Controller 에인 중합합니다.
- ShareFile 제어부가사용되지않기때문에 XenMobile 이 SAML 을통해인증하지않습니다.

다음 다이어그램은 XenMobile 과 StorageZone 커넥터를 함께 사용할 때의 아키텍처 개요를 보여줍니다.



요구사항

- 최소구성요소버전:
 - XenMobile Server 10.5(온-프레미스)
 - ShareFile for iOS(MDX) 5.3
 - ShareFile for Android(MDX) 5.3
 - ShareFile StorageZones Controller 5.0
 이 문서에는 ShareFile StorageZones Controller 5.0 구성방법에 대한 지침이 포함되어 있습니다.
- StorageZones Controller 를 실행하는 서버가 시스템 요구사항을 충족하는지 확인하십시오. 요구사항은 [시스템요구사항](#) 을 참조하십시오.

ShareFile 데이터용 StorageZone 및 제한된 StorageZone 에 대한 요구사항은 XenMobile 과 StorageZone 커넥터 전용 통합에는 적용되지 않습니다.

XenMobile 은 Documentum 커넥터를 지원하지 않습니다.

- PowerShell 스크립트를 실행하려면:
 - 32 비트 (x86) 버전의 PowerShell 에서 스크립트를 실행합니다.

설치작업

나와있는 순서대로 다음 작업을 완료하여 StorageZones Controller 를 설치하고 설정합니다. 이러한 단계는 XenMobile 과 StorageZone 커넥터 전용 통합에만 적용됩니다. 이러한 문서 중 일부는 StorageZones Controller 설명서에 포함되어 있습니다.

1. StorageZones Controller 를 위한 NetScaler 구성

NetScaler 를 StorageZones Controller 의 DMZ 프록시로 사용할 수 있습니다.

2. SSL 인증서 설치

표준영역을호스팅하는 StorageZones Controller 에는 SSL 인증서가필요합니다. 제한된영역을호스팅하고내부주소를사용하는 StorageZones Controller 에는 SSL 인증서가필요하지않습니다.

3. 서버준비

StorageZone 커넥터에는 IIS 및 ASP.NET 설정이필요합니다.

4. StorageZones Controller 설치

5. StorageZone 커넥터전용으로사용하도록 StorageZones Controller 준비

6. StorageZone 의프록시서버지정

StorageZones Controllers 콘솔을사용하여 StorageZones Controllers 의프록시서버를지정할수있습니다. 다른방법을사용하여프록시서버를지정할수도있습니다.

7. 위임을위해 StorageZones Controller 를신뢰하도록도메인컨트롤러구성

네트워크공유또는 SharePoint 사이트에서 NTLM 또는 Kerberos 인증을지원하도록도메인컨트롤러를구성합니다.

8. StorageZone 예보조 StorageZones Controller 가입

StorageZone 예고가용성을구성하려면영역에적어도두개의 StorageZones Controller 를연결합니다.

StorageZones Controller 설치

1. StorageZones Controller 소프트웨어다운로드및설치:

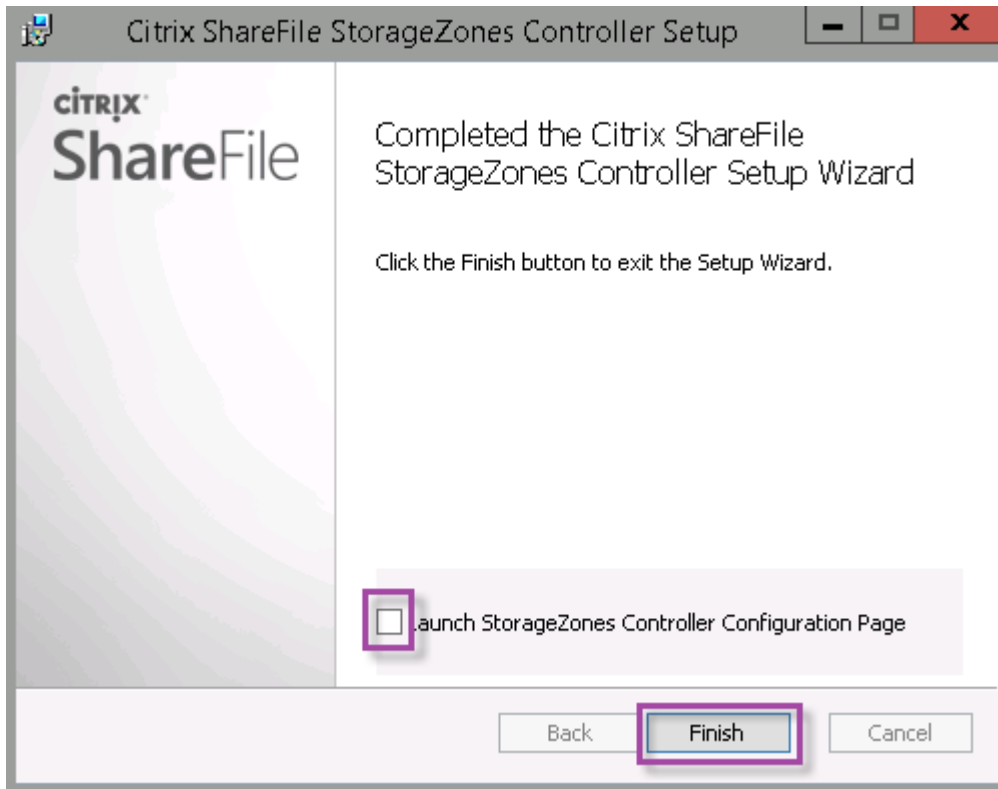
- ShareFile 다운로드페이지 (<https://www.citrix.com/downloads/sharefile.html>) 에서로그온한다음 최신 StorageZones Controller 설치관리자를다운로드합니다.
- StorageZones Controller 를설치하면서버의기본웹사이트가컨트롤러의설치경로로변경됩니다. 기본웹사이트에서 익명인증을사용하도록설정합니다.

2. StorageZones Controller 를설치하려는서버에서 StorageCenter.msi 를실행합니다.

ShareFile StorageZones Controller Setup(설치) 마법사가시작됩니다.

3. 프롬프트에응답합니다.

- IIS(Internet Information Services) 가기본위치에설치되어있는경우 **Destination Folder(대상폴더)** 페이지에서기본값을그대로유지합니다. 그렇지않은경우 IIS 설치위치를찾아선택합니다.
- 설치가완료되면 **Launch StorageZones Controller Configuration Page(StorageZones Controller 구성페이지시작)** 확인란을선택취소한다음 **Finish(마침)** 를클릭합니다.



4. 메시지가 나타나면 StorageZones Controller 를 다시 시작합니다.
5. 설치가 성공적이었는지 테스트하려면 <https://localhost/> 로 이동합니다. 설치가 성공적이면 ShareFile 로고가 나타납니다.

ShareFile 로고가 나타나지 않으면 브라우저 캐시를 지우고 다시 시도하십시오.

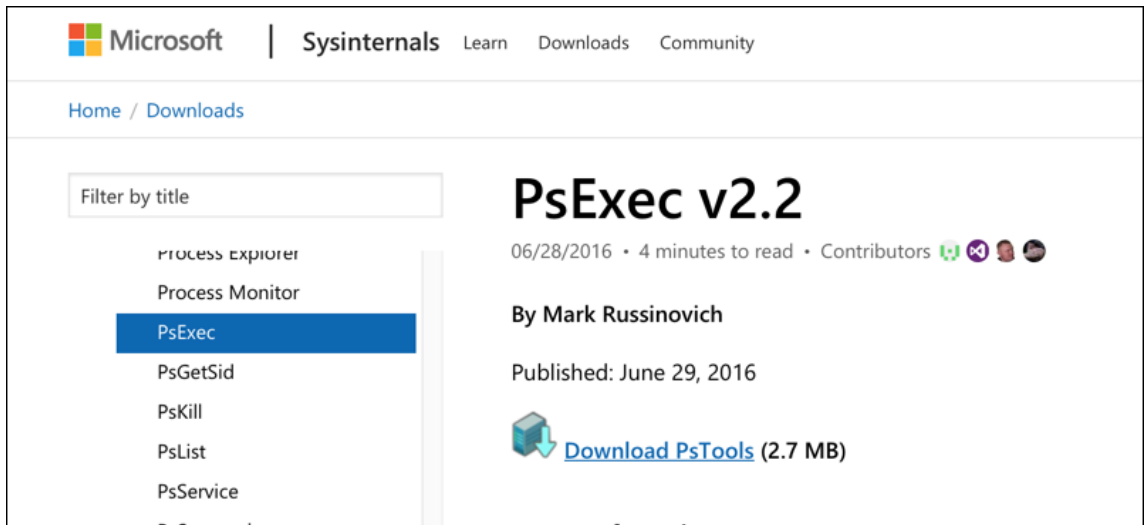
중요:

StorageZones Controller 를 복제하려는 경우 StorageZones Controller 구성을 계속하기 전에 디스크 이미지를 캡처하십시오.

StorageZone 커넥터 전용으로 사용하도록 StorageZones Controller 준비

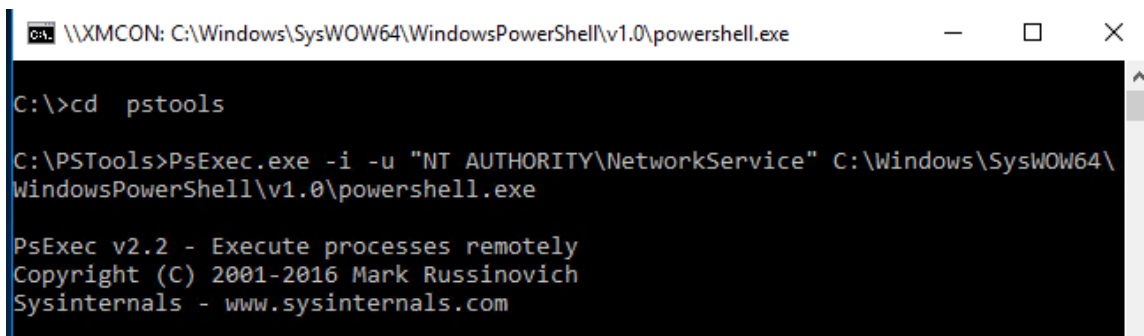
StorageZone 커넥터 전용 통합의 경우 StorageZones Controller 관리 콘솔을 사용하지 않습니다. 인터페이스에는 이 솔루션에 필요하지 않은 ShareFile 관리자 계정이 필요합니다. 따라서 PowerShell 스크립트를 실행하여 ShareFile 제어부 없이 사용하도록 StorageZones Controller 를 준비합니다. 스크립트는 다음을 수행합니다.

- 현재 StorageZones Controller 를 기본 StorageZones Controller 로 다시 시작합니다. 나중에 보조 StorageZones Controller 를 기본 컨트롤러에 가입시킬 수 있습니다.
 - 영역을 만들고 사용할 암호를 설정합니다.
1. StorageZone Controller 서버에서 PsExec 도구 다운로드: Microsoft [Windows Sysinternals](#) 로 이동한 다음 **Download PsTools(PsTools 다운로드)** 를 클릭합니다. C 드라이브 루트에도구의 압축을 풉니다.

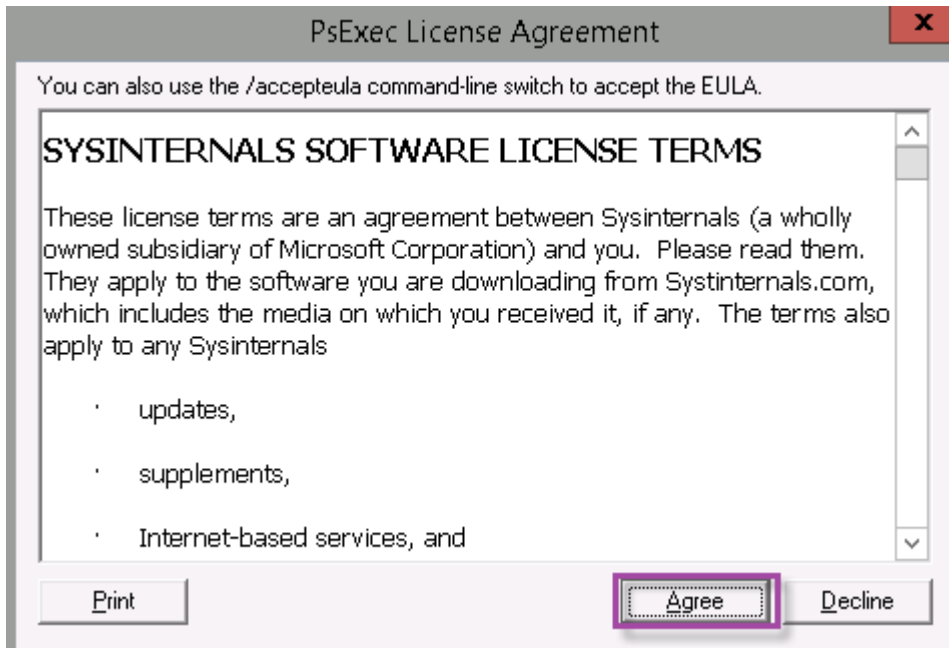


2. PsExec 도구실행: 관리자사용자로명령프롬프트를열고다음을입력합니다.

```
1 cd c:\pstools
2 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. 메시지가나타나면 **Agree**(동의) 를클릭하여 Sysinternals 도구를실행합니다.



PowerShell 창이열립니다.

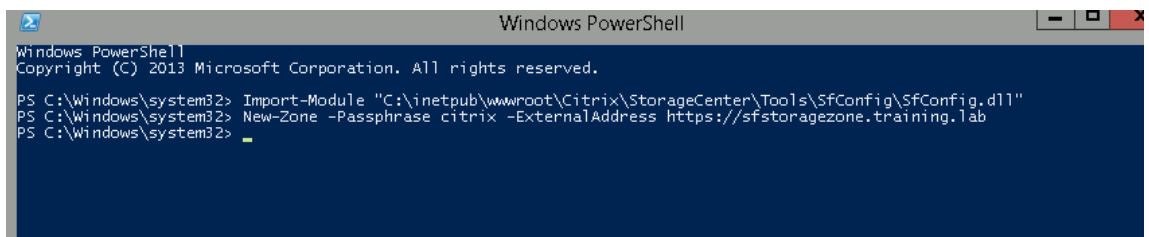
4. PowerShell 창에서다음을입력합니다.

```
1 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"
2 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

여기서:

Passphrase: 사이트에할당할암호입니다. 암호를기록합니다. 컨트롤러에서암호를복구할수없습니다. 암호를분실하면 StorageZone 을다시설치하거나, StorageZone 에추가적인 StorageZones Controller 를가입시키거나, 서버장애가발생한경우 StorageZone 을복구할수없습니다.

ExternalAddress: StorageZones Controller 서버의외부 FQDN(정규화된도메인이름) 입니다.



이제기본 StorageZones Controller 가준비되었습니다.

StorageZone 커넥터를만들기위해 XenMobile 에로그인하기전: 해당되는경우다음구성을완료합니다.

[StorageZone 의프록시서버지정](#)

[위임을위해 StorageZones Controller 를신뢰하도록도메인컨트롤러구성](#)

StorageZone 예보조 StorageZones Controller 가입

StorageZone 커넥터를 생성하려면 XenMobile 에서 StorageZones Controller 연결정의 참조하십시오.

StorageZone 예보조 StorageZones Controller 가입

StorageZone 예고가용성을 구성하려면 영역에 적어도 두개의 StorageZones Controller 를 연결합니다. 보조 StorageZones Controller 를 영역에 가입시키려면 보조 서버에 StorageZones Controller 를 설치합니다. 그런 다음 해당 컨트롤러를 기본 컨트롤러의 영역에 가입시킵니다.

1. 주 서버에 가입시키려는 StorageZones Controller 서버에서 PowerShell 창을 엽니다.
2. PowerShell 창에서 다음을 입력합니다.

```
Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
```

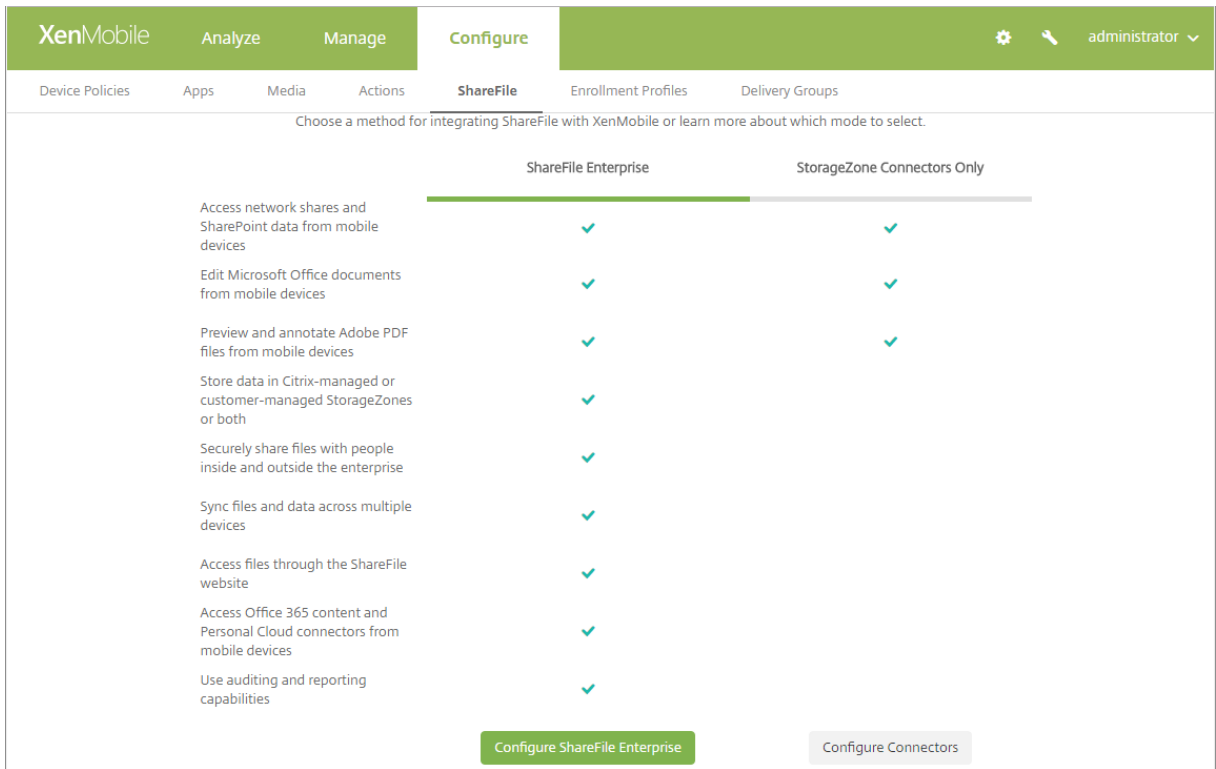
예를 들면 다음과 같습니다.

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

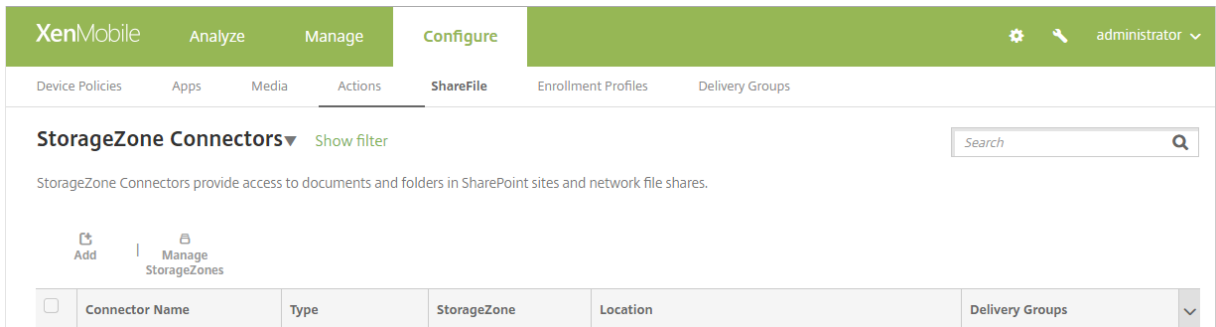
XenMobile 에서 StorageZones Controller 연결정의

StorageZone 커넥터를 추가하기 전에 StorageZone 커넥터에 사용하도록 설정된 각 StorageZones Controller 에 대한 연결정보를 구성합니다. 이 섹션에 설명된 대로 또는 커넥터를 추가할 때 StorageZones Controller 를 정의할 수 있습니다.

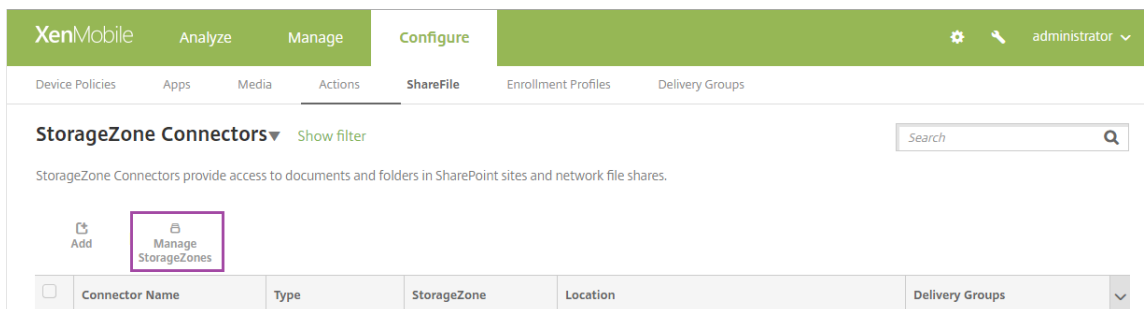
구성 > **ShareFile** 페이지를 처음 방문하면 페이지에 XenMobile 에서 ShareFile Enterprise 를 사용할 때와 StorageZone 커넥터를 사용할 때의 차이점이 요약되어 있습니다.



커넥터구성을 클릭하여이 문서의 구성 단계를 계속 수행합니다.



1. 구성 > ShareFile 에서 **StorageZone** 관리를 클릭합니다.



2. **StorageZone** 관리에서 연결정보를 추가합니다.

- 이름: XenMobile 에서 StorageZone 을 식별하는데 사용되는 StorageZone 의 설명적인 이름입니다. 이름에 공백이나 특수문자를 사용하지 마십시오.
- FQDN 및 포트: XenMobile Server 에서 연결할 수 있는 StorageZones Controller 의 FQDN(정규화된 도메인 이름) 및 포트 번호입니다.
- 보안 연결: StorageZones Controller 에 연결하기 위해 SSL 을 사용하는 경우 기본 설정인 켜짐을 사용합니다. 연결에 SSL 을 사용하지 않는다면 이 설정을 꺼짐으로 변경합니다.
- 관리자 사용자 이름 및 관리자 암호: 관리자 서비스 계정 사용자 이름 (domain\admin 형식) 및 암호입니다. 또는 StorageZones Controller 에 대한 읽기 및 쓰기 권한이 있는 사용자 계정입니다.

3. 저장을 클릭합니다.

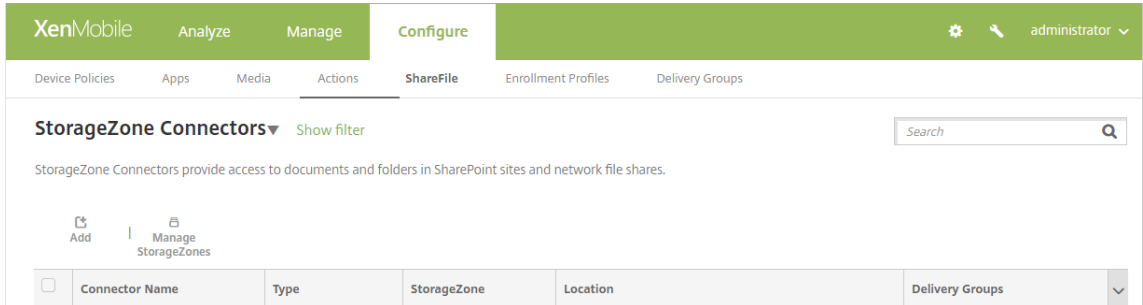
4. 연결을 테스트하려면 XenMobile Server 가 포트 443 에서 StorageZones Controller 의 정규화된 도메인 이름에 연결할 수 있는지 확인합니다.

5. 다른 StorageZones Controller 연결을 정의하려면 **StorageZone** 관리에서 추가 단추를 클릭합니다.

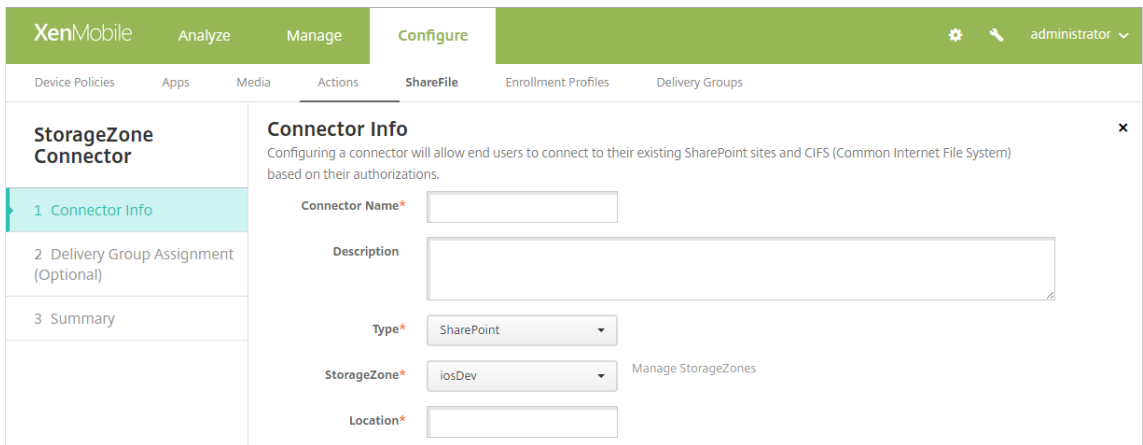
StorageZones Controller 연결에 대한 정보를 편집하거나 삭제하려면 **StorageZone** 관리에서 연결 이름을 선택합니다. 그런 다음 편집 또는 삭제를 클릭합니다.

XenMobile 에서 StorageZone 커넥터추가

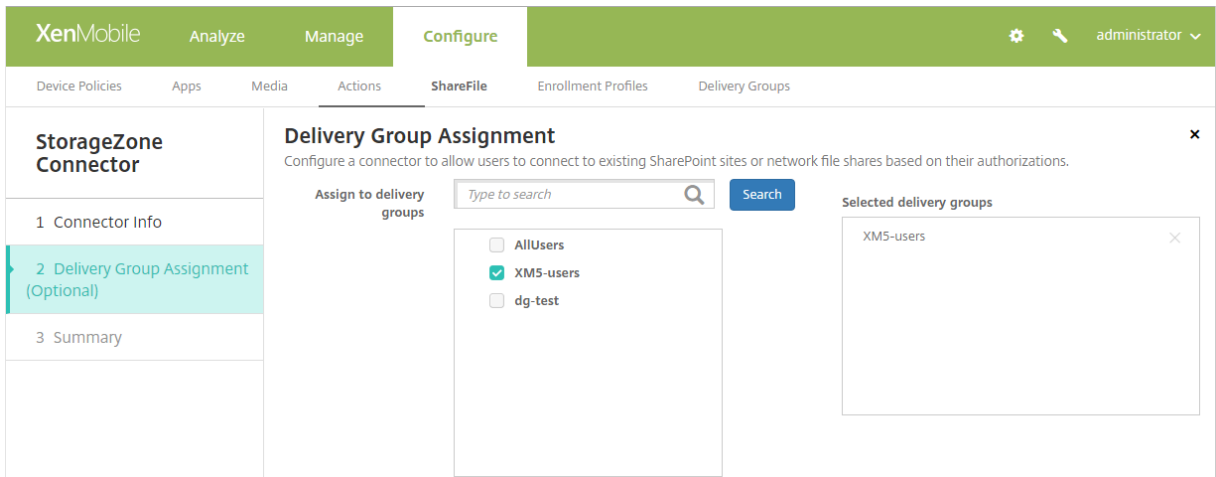
1. 구성 > **ShareFile** 로이동한다음 추가를클릭합니다.



2. 커넥터정보페이지에서다음설정을구성합니다.



- 커넥터이름: XenMobile 에서 StorageZone 커넥터를식별하는이름입니다.
 - 설명: 이커넥터에대한선택적인메모입니다.
 - 유형: **SharePoint** 또는 네트워크를선택합니다.
 - **StorageZone:** 커넥터와연결된 StorageZone 을선택합니다. StorageZone 이나열되지않으면 **StorageZone** 관리를클릭하여 StorageZones Controller 를정의합니다.
 - 위치: SharePoint 의 경우 SharePoint 루트수준사이트, 사이트컬렉션또는문서라이브러리의 URL 을 <https://sharepoint.company.com> 형식으로지정합니다. 네트워크공유의 경우 UNC(Uniform Naming Convention) 경로의정규화된도메인이름을 \\server\share 형식으로지정합니다.
3. 배달그룹할당페이지에서선택적으로커넥터를배달그룹에할당합니다. 또는 구성 > 배달그룹을사용하여커넥터를배달그룹에연결할수있습니다.



1. 요약페이지에서구성한옵션을검토할수있습니다. 구성을조정하려면 뒤로를클릭합니다.
2. 저장을클릭하여커넥터를저장합니다.
3. 커넥터를테스트합니다.

a) ShareFile 클라이언트를래핑하는경우다음을수행합니다.

- 네트워크액세스정책을 내부네트워크로터널링됨으로설정합니다.

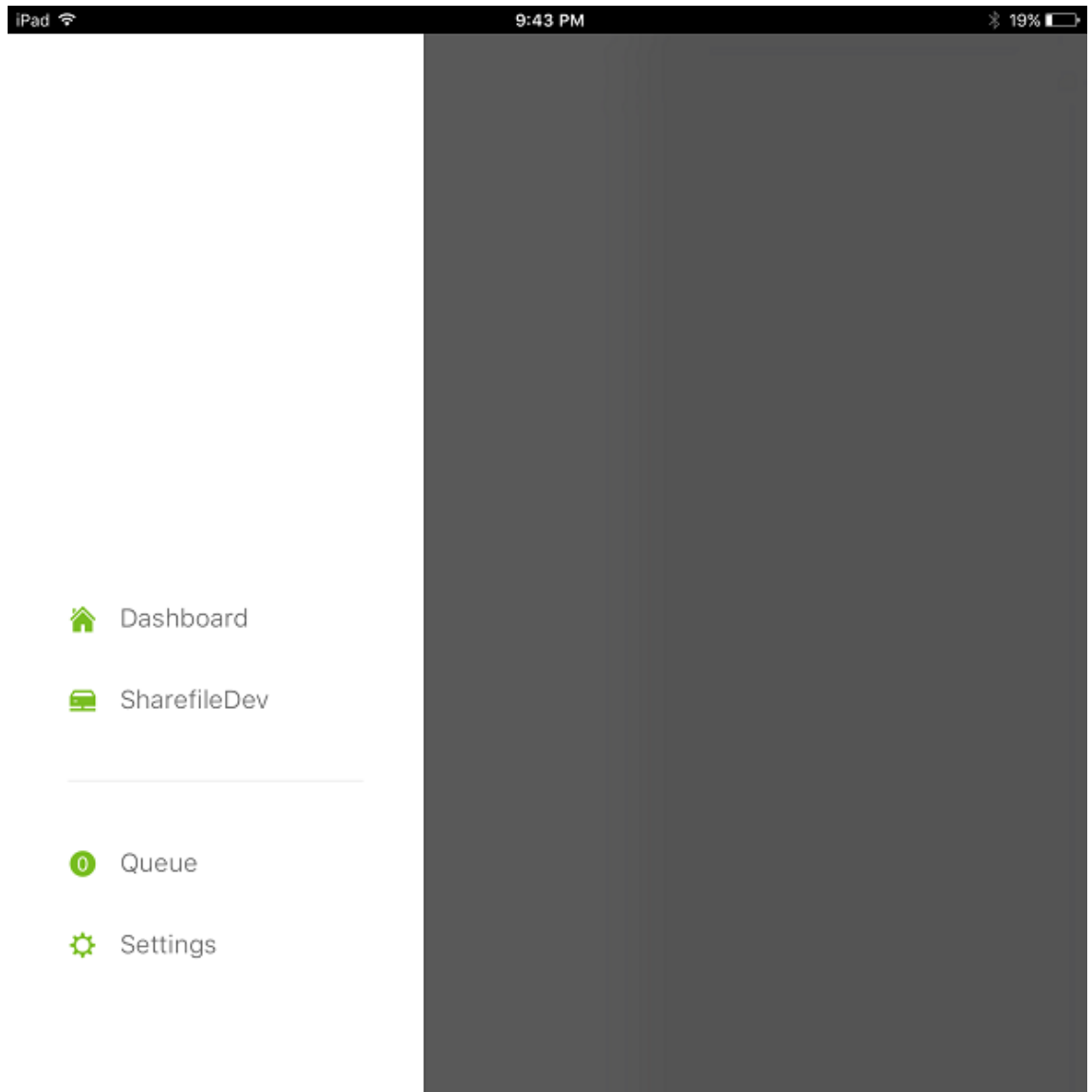
이작동모드에서는 XenMobile MDX 프레임워크가 ShareFile 클라이언트의모든네트워크트래픽을가로칩니다. 트래픽은앱전용 Micro VPN 을사용하여 NetScaler Gateway 를통해리디렉션됩니다.

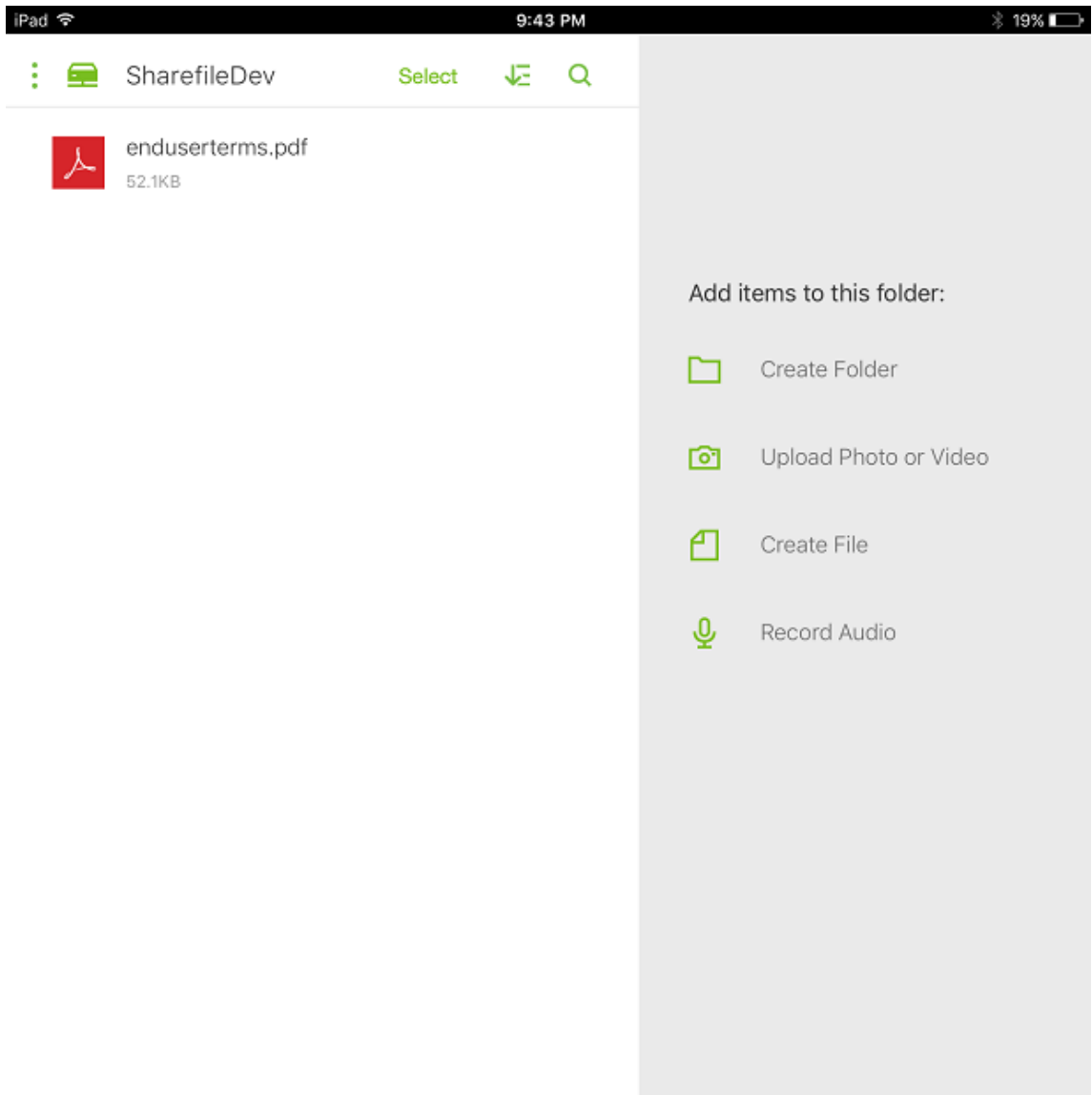
- 기본설정 VPN 모드정책을 터널링됨 - 웹 SSO 로설정합니다.

이터널링모드에서는 MDX 프레임워크가 MDX 앱의 SSL/HTTP 트래픽을종료합니다. 그런다음 MDX 가사용자 대신내부연결로의새연결을시작합니다. 이정책설정은 MDX 프레임워크가웹서버에서발행된인증챌린지를감지하고이에응답할수있게합니다.

- b) ShareFile 클라이언트를 XenMobile 에추가합니다. 자세한내용은 [Citrix Files for Endpoint Management 클라이언트통합및제공](#)에서참조하십시오.
- c) 지원되는장치에서 ShareFile 및커넥터에대한 Single Sign-On 을확인합니다.

다음샘플에서 SharefileDev 가커넥터이름입니다.

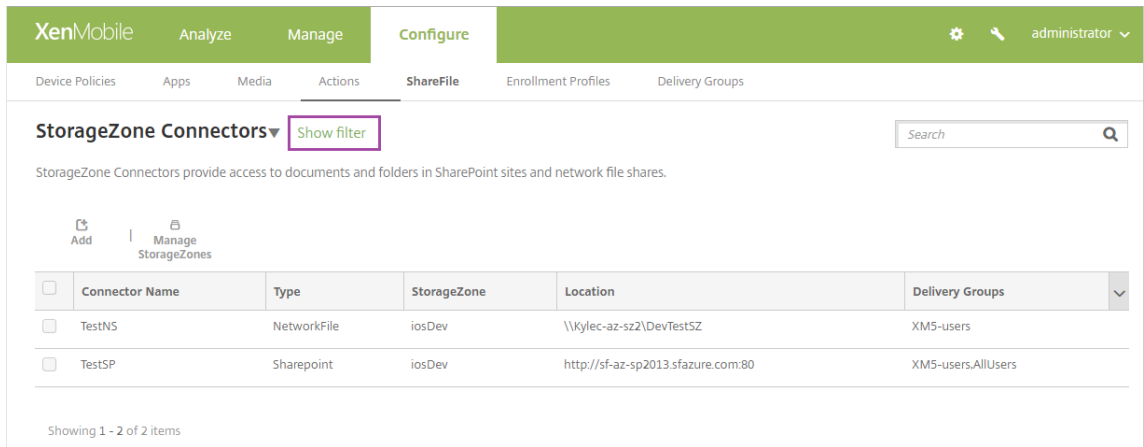




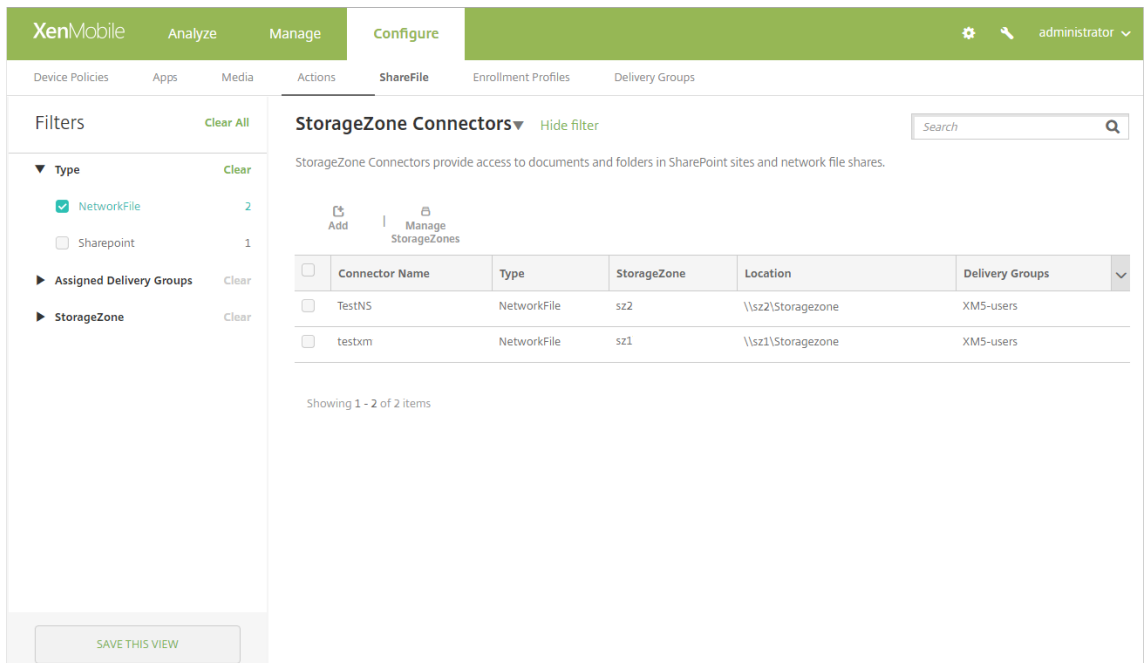
StorageZone 커넥터목록필터링

커넥터유형, 할당된배달그룹및 StorageZone 을기준으로 StorageZone 커넥터의목록을필터링할수있습니다.

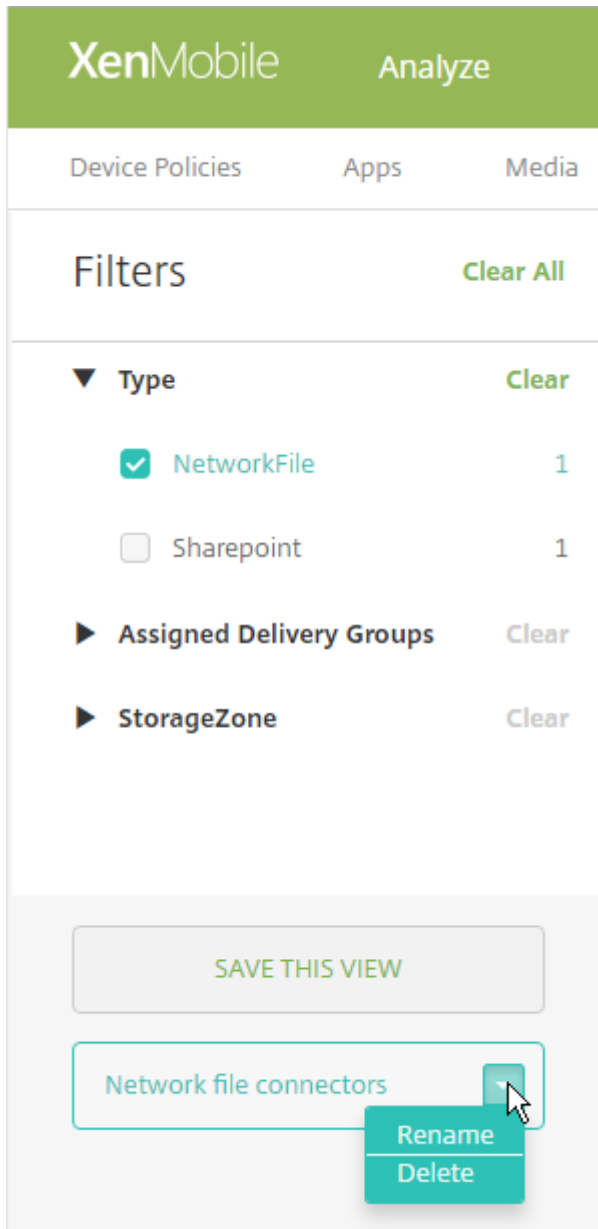
1. 구성 > **ShareFile** 로이동한다음 필터표시를클릭합니다.



2. 필터머리글을 확장하여 선택할 수 있게 만듭니다. 필터를 저장하려면 이보기저장을 클릭하고 필터 이름을 입력한 다음 저장을 클릭합니다.



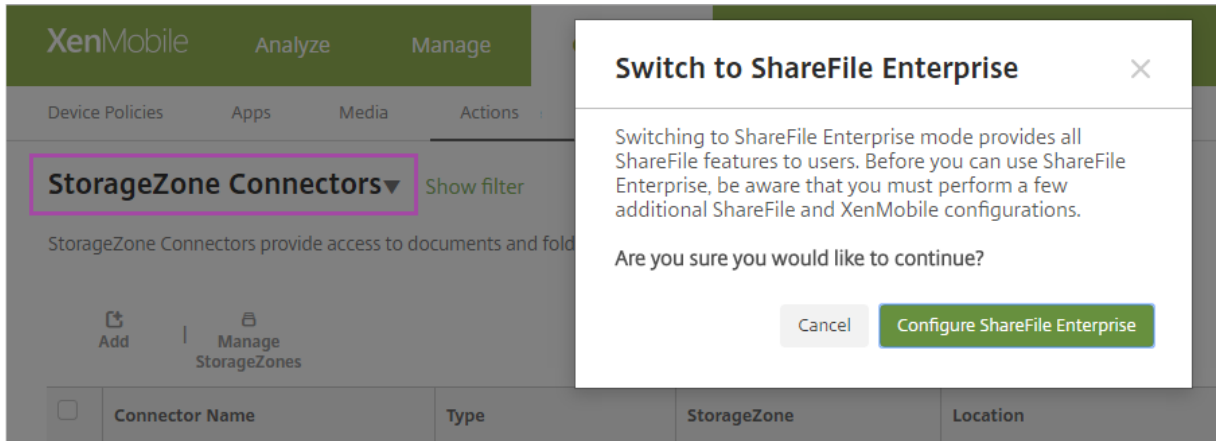
3. 필터 이름을 바꾸거나 필터를 삭제하려면 필터 이름 옆의 화살표 아이콘을 클릭합니다.



ShareFile Enterprise 로 전환

StorageZone 커넥터를 XenMobile 과 통합한 후 하나 중에 전체 ShareFile Enterprise 기능 집합으로 전환할 수 있습니다. ShareFile Enterprise 기능 집합을 사용하려면 XenMobile Enterprise Edition 이 필요합니다. XenMobile 은 기존 StorageZone 커넥터 통합 설정을 유지합니다.

구성 > **ShareFile** 로 이동하고 **StorageZone** 커넥터 드롭다운 메뉴를 클릭한 다음 **ShareFile Enterprise** 구성을 클릭합니다.



ShareFile Enterprise 구성에 자세한 내용은 [ShareFile SSO\(Single Sign-on\) 용 SAML](#)을 참조하십시오.

HDX 애플리케이션 SmartAccess

October 21, 2019

이 기능을 사용하면 장치 속성, 장치의 사용자 속성 또는 장치에 설치된 응용 프로그램을 기반으로 HDX 앱에 대한 액세스 권한을 제어할 수 있습니다. 장치를 규정위반으로 표시하여 해당 장치 액세스를 거부하는 자동화된 동작을 설정하여 이 기능을 사용합니다. 이 기능과 함께 사용되는 HDX 앱은 Virtual Apps and Desktops 에서 규정위반 장치에 대한 액세스를 거부하는 SmartAccess 정책을 사용하여 구성됩니다. XenMobile 은 서명되고 암호화된 태그를 사용하여 장치 상태를 StoreFront 에 전달합니다. 그러면 StoreFront 가 앱의 액세스 제어 정책에 따라 액세스를 허용하거나 거부합니다.

이 기능을 사용하려면 배포에 다음이 포함되어야 합니다.

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 또는 3.8
- StoreFront 서버에서 HDX 앱을 집계하도록 구성된 XenMobile Server
- 태그 서명 및 암호화에 사용되는 SAML 인증서가 구성된 XenMobile Server. 동일한 인증서가 개인 키가 없는 상태로 StoreFront 서버에 업로드됩니다.

이 기능을 사용하려면:

- StoreFront 저장소에 대한 XenMobile Server 인증서 구성
- 필요한 SmartAccess 정책을 사용하여 하나 이상의 Virtual Apps and Desktops 배달 그룹 구성
- XenMobile 에서 자동화된 작업 설정

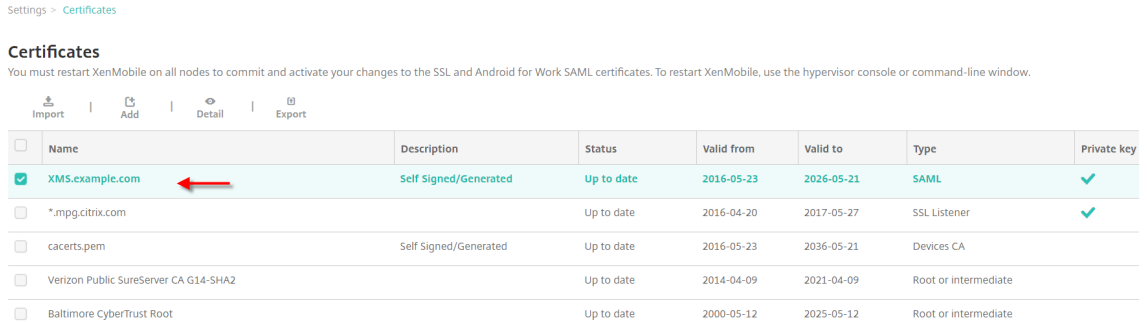
XenMobile Server 인증서를 내보내고 구성하여 StoreFront 저장소에 업로드

SmartAccess 는 서명되고 암호화된 태그를 사용하여 XenMobile 및 StoreFront 서버 간에 통신합니다. 이 통신을 사용하도록 설정하려면 XenMobile Server 인증서를 StoreFront 저장소에 추가합니다.

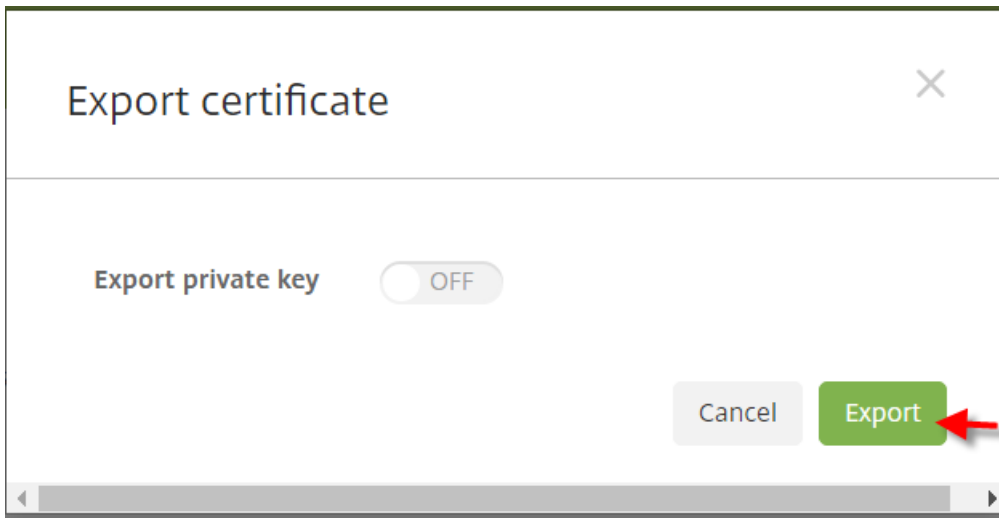
XenMobile 이도메인및인증서기반인증을사용하도록설정된경우 StoreFront 및 XenMobile 의통합에대한자세한내용은 [Support Knowledge Center](#)를참조하십시오.

XenMobile Server 에서 SAML 인증서내보내기

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다. 인증서를클릭합니다.
2. XenMobile Server 의 SAML 인증서를찾습니다.



3. 개인키내보내기가 꺼짐으로설정되어있는지확인합니다. 내보내기를클릭하여인증서를다운로드디렉터리로내보냅니다.

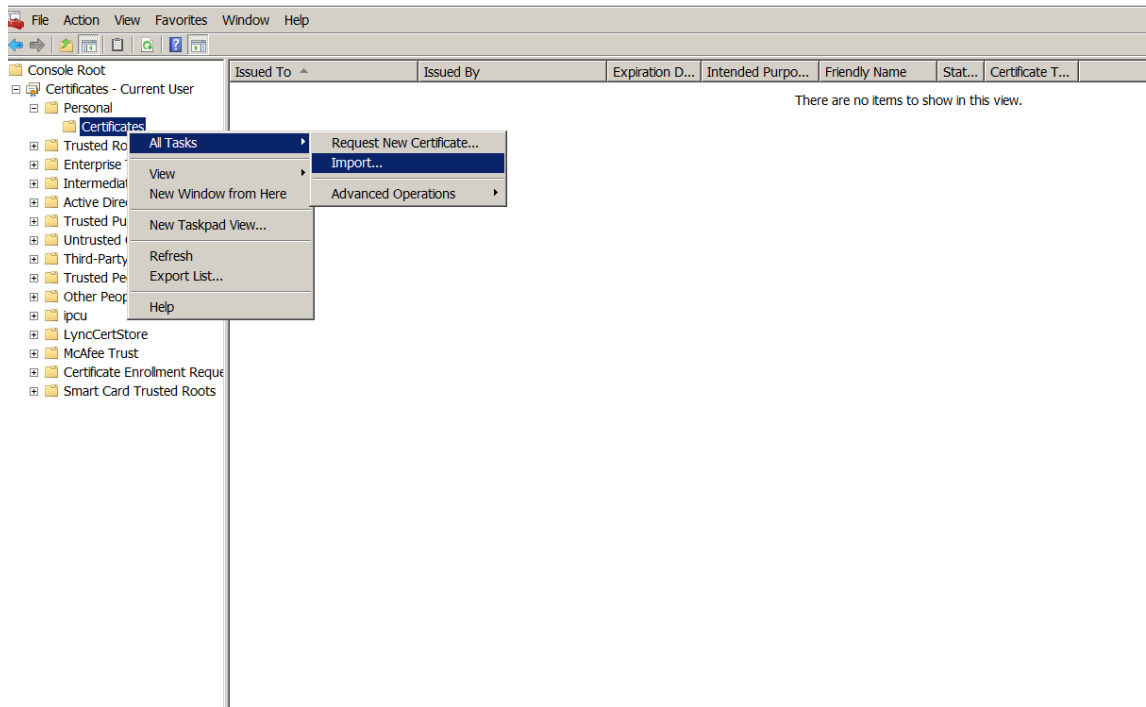


4. 다운로드디렉터리에서인증서를찾습니다. 인증서는 PEM 형식입니다.

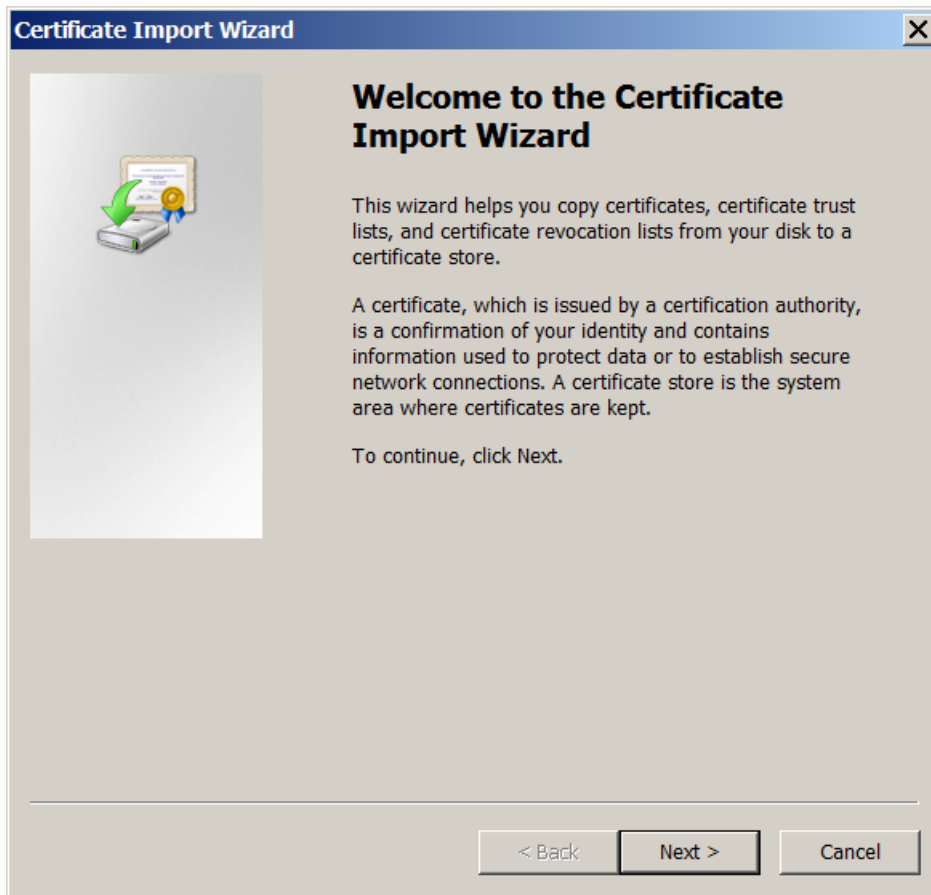


인증서를 **PEM** 에서 **CER** 로 변환

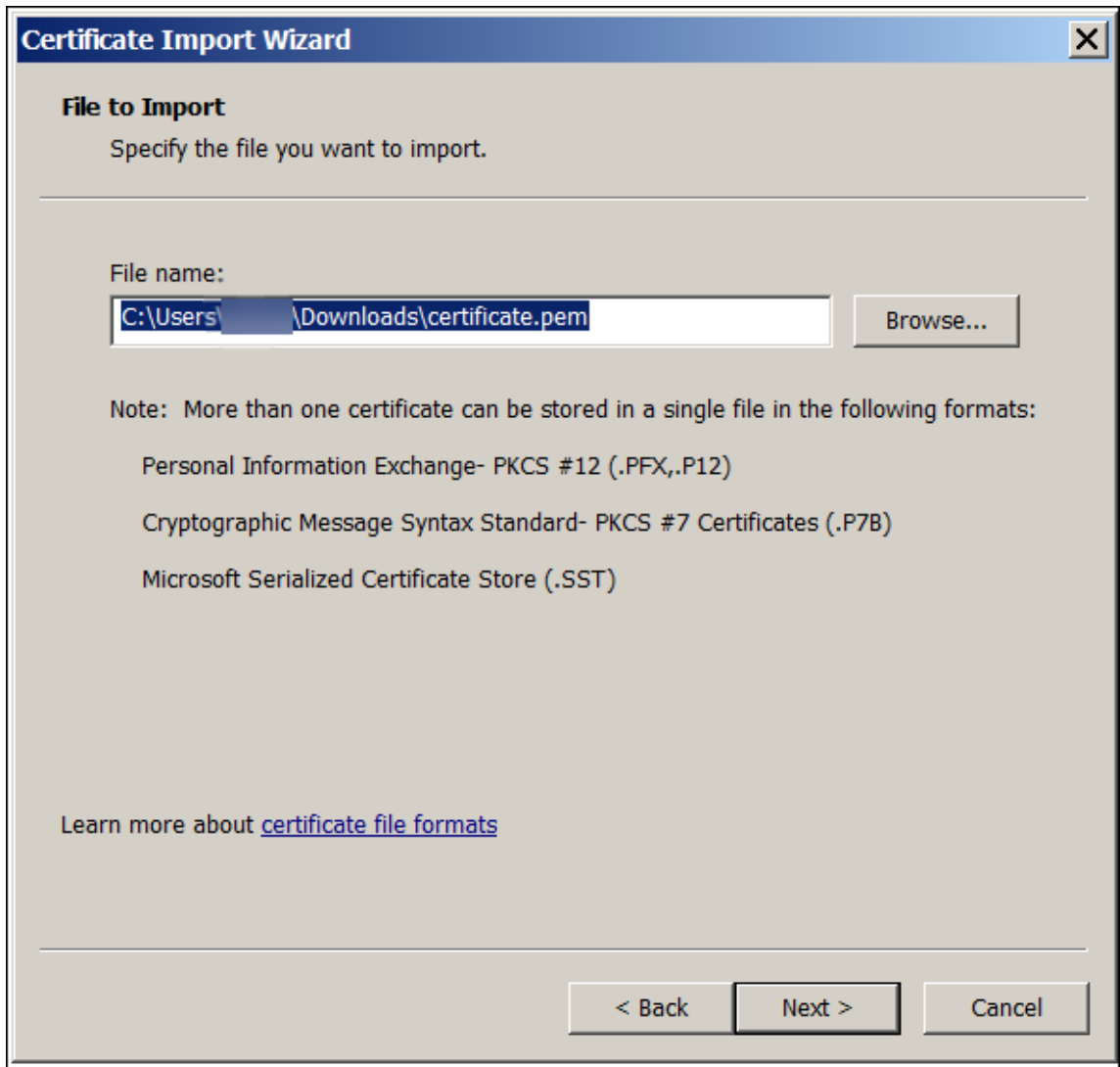
1. MMC(Microsoft Management Console) 를 열고 마우스 오른쪽 단추를 클릭하여 인증서 > 모든 작업 > 가져오기를 선택합니다.



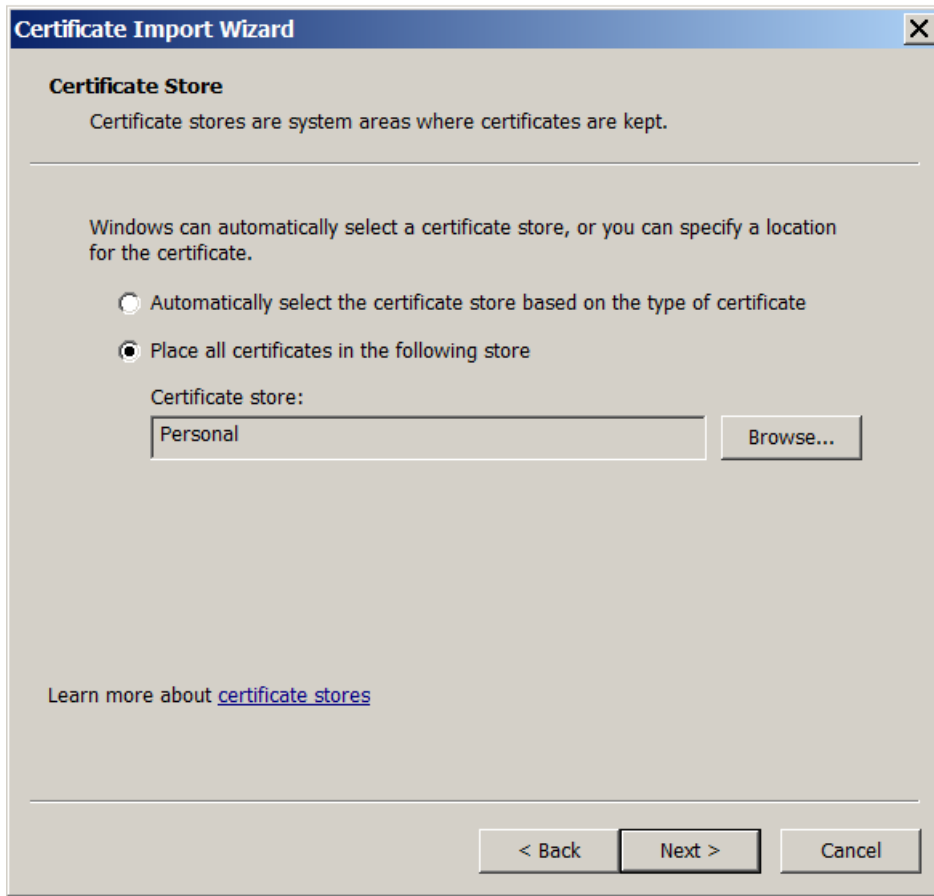
2. 인증서가 가져오기 마법사가 나타나면 다음을 클릭합니다.



3. 다운로드디렉터리에있는인증서를찾아선택합니다.

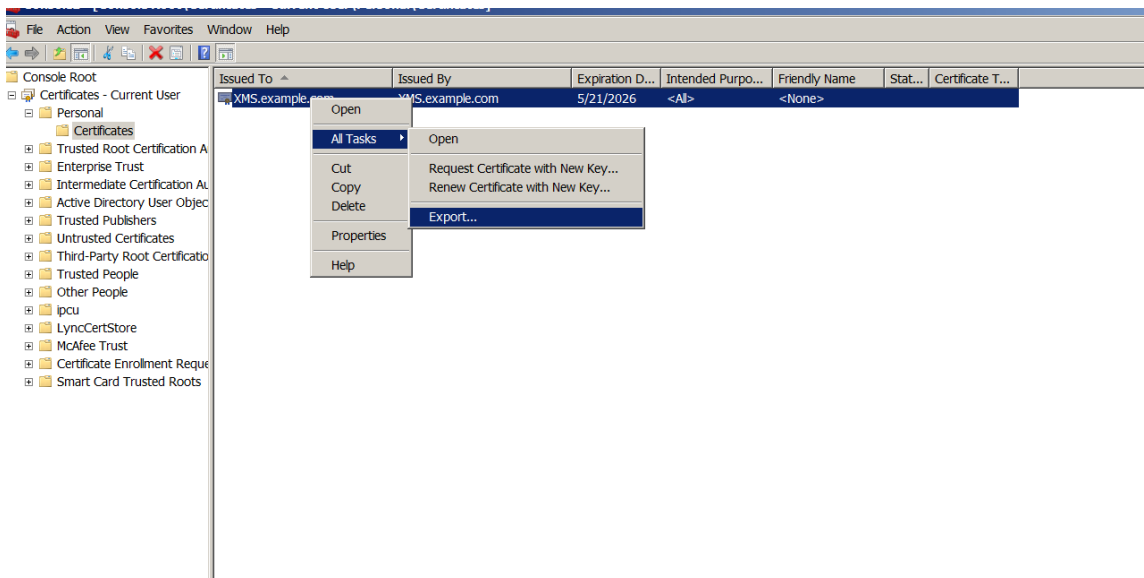


- 모든인증서를다음저장소에저장을선택하고인증서저장소로 개인을선택합니다. 다음을클릭합니다.



5. 선택내용을검토하고 마침을클릭합니다. 확인을클릭하여확인창을닫습니다.

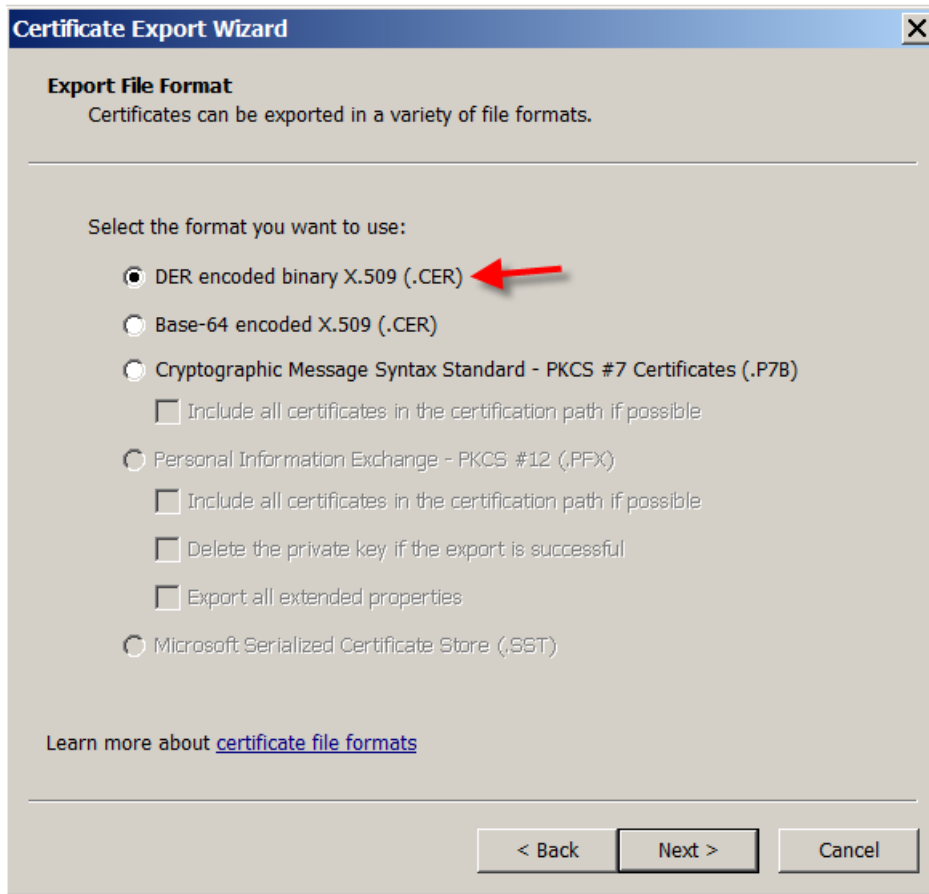
6. MMC 에서인증서를마우스오른쪽단추로클릭하고 모든작업 > 내보내기를선택합니다.



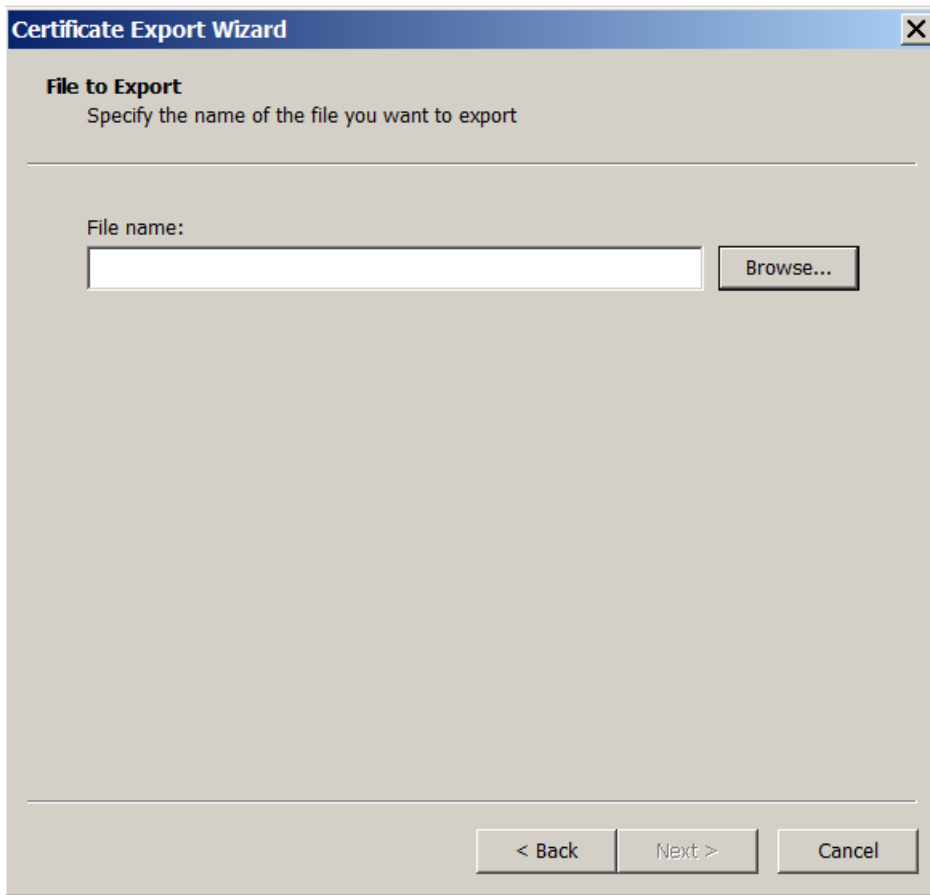
7. 인증서내보내기마법사가나타나면 다음을클릭합니다.



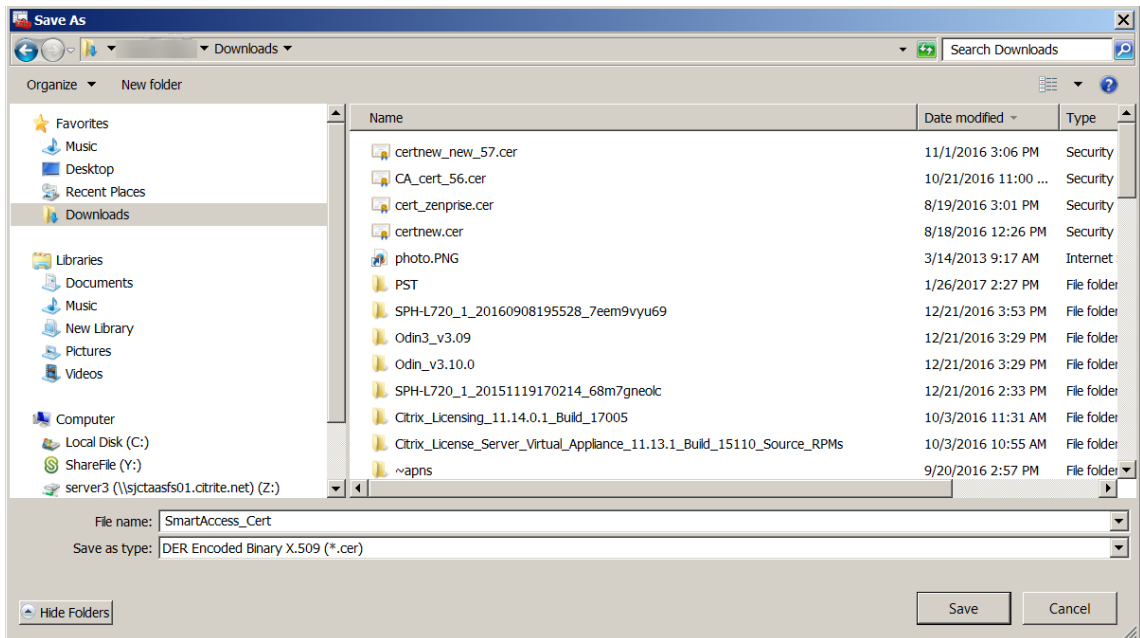
8. **DER** 로인코딩된바이너리 **X.509(.CER)** 형식을선택합니다. 다음을클릭합니다.



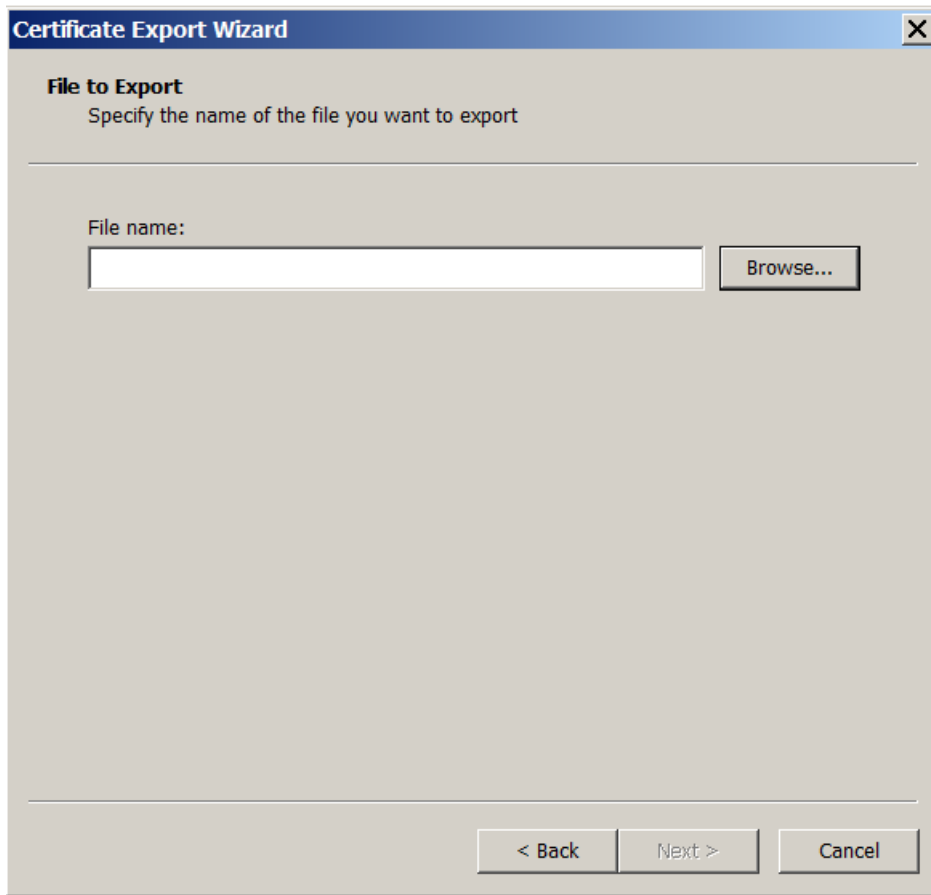
9. 인증서를 찾아봅니다. 인증서의 이름을 입력한 후 다음을 클릭합니다.



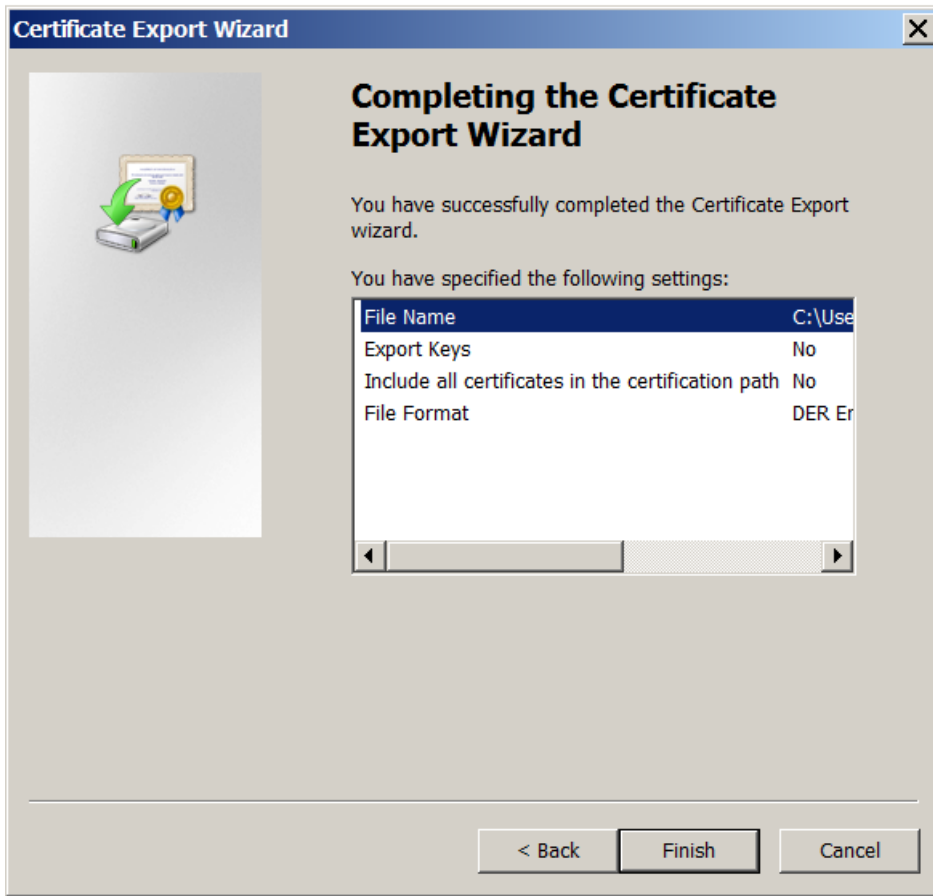
10. 인증서를저장합니다.



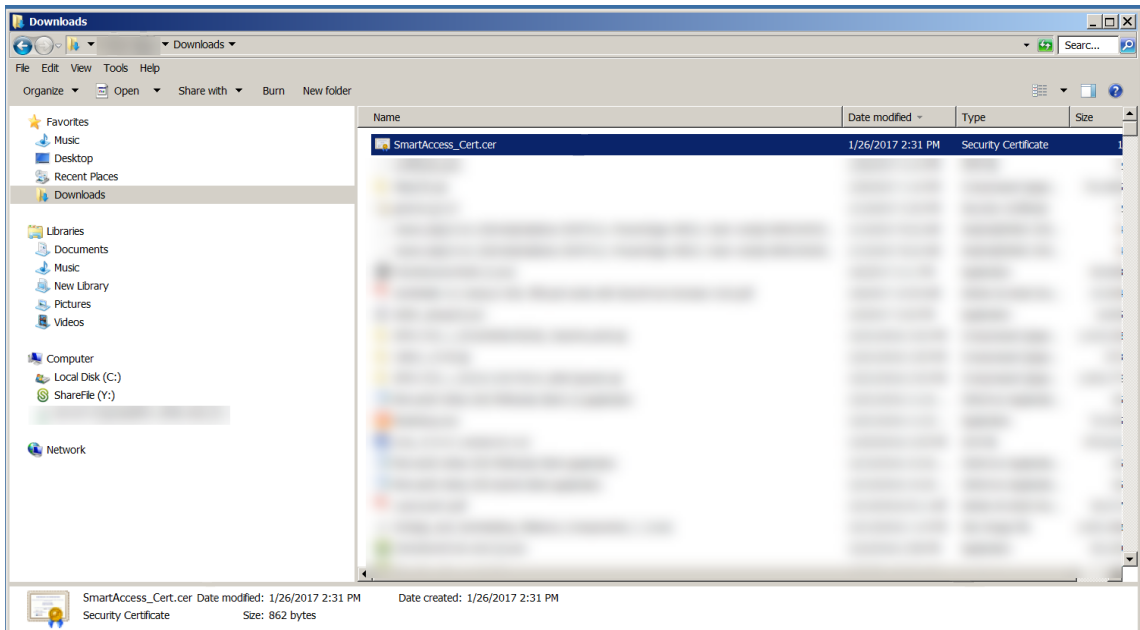
11. 인증서를찾아선택하고 다음을클릭합니다.



12. 선택내용을검토하고 마침을클릭합니다. 확인을클릭하여확인창을닫습니다.

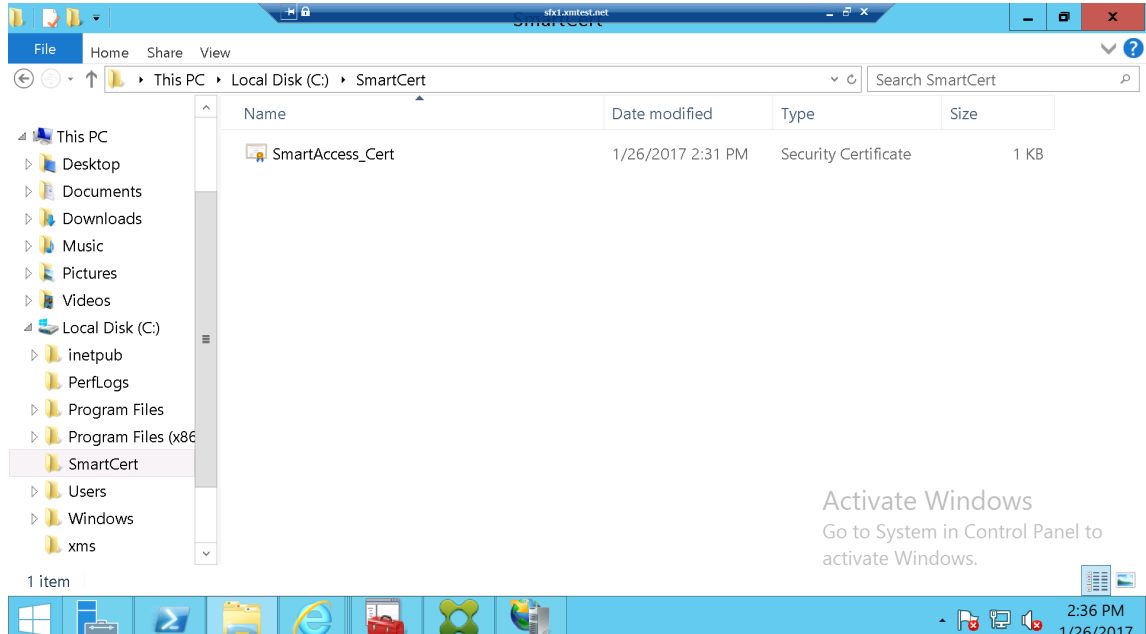


13. 다운로드디렉터리에서인증서를찾습니다. 인증서는 CER 형식입니다.



인증서를 **StoreFront** 서버에복사합니다

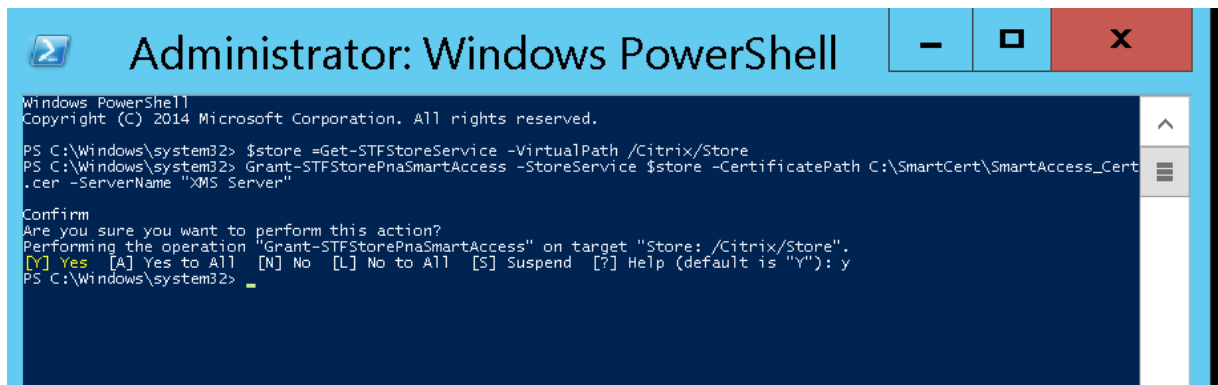
1. StoreFront 서버에서 **SmartCert** 라는폴더를만듭니다.
2. 인증서를 **SmartCert** 폴더에복사합니다.



StoreFront 저장소에서인증서구성

StoreFront 서버에서다음 PowerShell 명령을실행하여저장소에서변환된 XenMobile Server 인증서를구성합니다.

```
1 Grant-STFStorePnaSmartAccess - StoreService $store -
CertificatePath "C:\xms\xms.cer" - ServerName "XMS server"
```



StoreFront 저장소에기존인증서가있는경우다음 PowerShell 명령을실행하여인증서를해지합니다.

```
1 Revoke-STFStorePnaSmartAccess - StoreService $store - All
```

```
PS C:\Windows\system32> $store = Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Revoke-STFStorePnaSmartAccess -StoreService $store -All
Confirm
Are you sure you want to perform this action?
Performing the operation "Revoke-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32>
```

또는다음 PowerShell 명령중하나를 StoreFront 서버에서실행하여 StoreFront 저장소의기존인증서를해지할수있습니다.

- 이름으로해지:

```
1 $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "
  My XM Server"
```

- 지문으로해지:

```
1 $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess -StoreService $store -
  CertificateThumbprint "ReplaceWithThumbprint"
```

- 서버개체로해지:

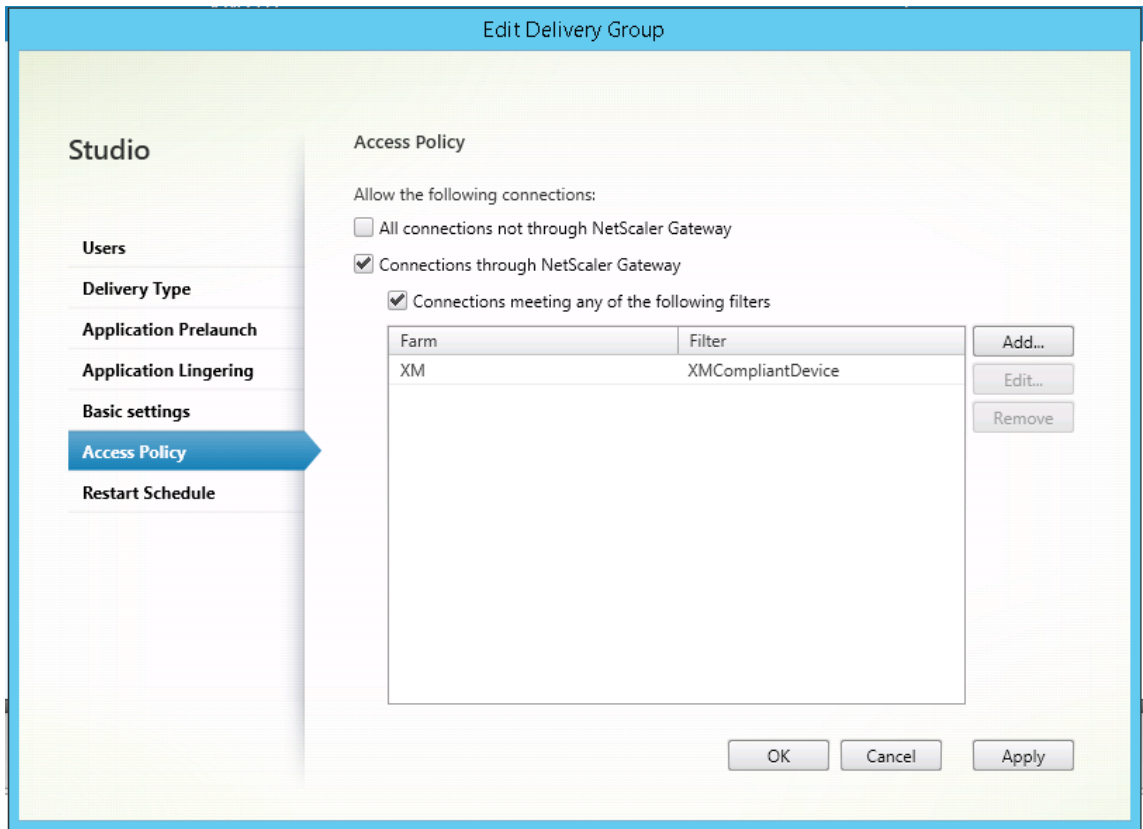
```
1 $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3 $access = Get-STFStorePnaSmartAccess -StoreService $store
4
5 Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess
  $access.AccessConditionsTrusts[0]
```

Virtual Apps and Desktops 에대한 SmartAccess 정책구성

필요한 SmartAccess 정책을 HDX 앱을전달하는배달그룹에추가하려면:

1. Virtual Apps and Desktops 서버에서 Citrix Studio 를열니다.
2. Studio 탐색창에서 **Delivery Groups(배달그룹)** 를선택합니다.
3. 액세스권한을제어하려는하나이상의앱을전달하는그룹을선택합니다. **Actions(동작)** 창에서 **Edit Delivery Group(배달그룹편집)** 을선택합니다.
4. **Access Policy(엑세스정책)** 페이지에서 **Connections through NetScaler Gateway(NetScaler Gateway 를 통한 연결)** 및 **Connection meeting any of the following(다음과일치하는연결)** 을선택합니다.
5. 추가를클릭합니다.

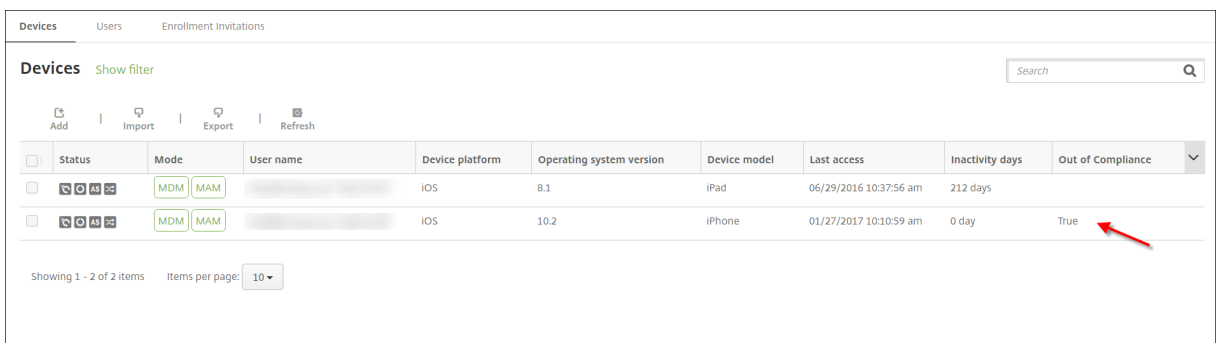
6. **Farm(팜)** 이 **XM** 이고 **Filter(필터)** 가 **XMCompliantDevice** 인액세스정책을추가합니다.



7. **Apply(적용)** 를클릭하여모든변경내용을적용하고창을열린채로두거나, **OK(확인)** 를클릭하여변경내용을적용하고창을 닫습니다.

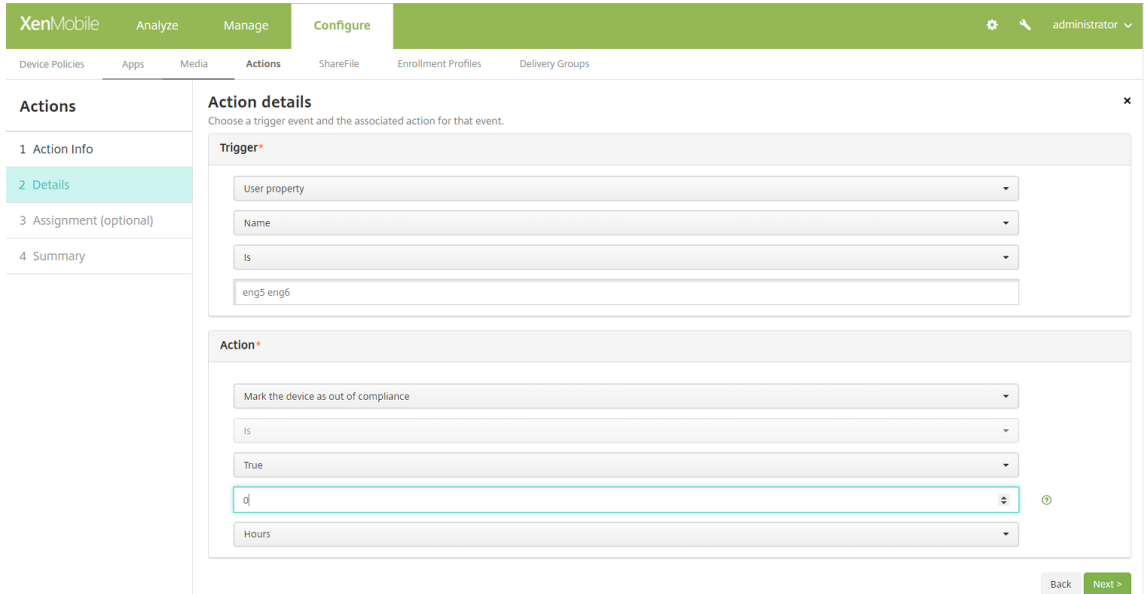
XenMobile 에서자동화된동작설정

HDX 앱에대한배달그룹에설정된 SmartAccess 정책은장치가규정을위반하면장치에대한액세스를거부합니다. 장치를규정위 반으로표시하는자동화된동작을사용합니다.



1. XenMobile 콘솔에서 구성 > 동작을클릭합니다. 동작페이지가나타납니다.
2. 추가를클릭하여동작을추가합니다. 동작정보페이지가나타납니다.

3. 동작정보페이지에서동작의이름및설명을입력합니다.
4. 다음을클릭합니다. 동작세부정보페이지가나타납니다. 다음예에서는장치에서사용자속성이름 **eng5** 또는 **eng6** 이있는경우즉시장치를규정위반으로표시하는트리거를만듭니다.

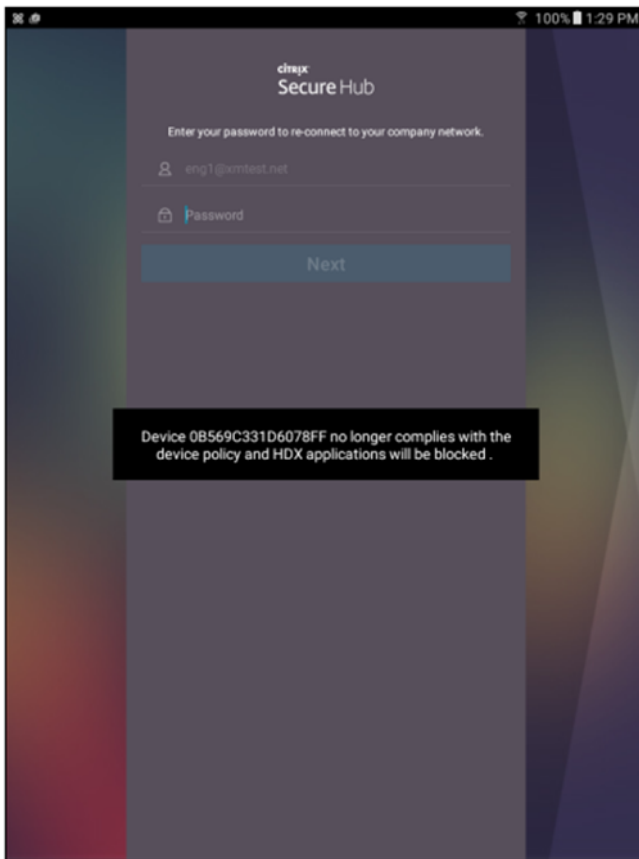


5. 트리거목록에서 장치속성, 사용자속성또는 설치된앱이름을선택합니다. SmartAccess 는이벤트트리거를지원하지않습니다.
6. 동작목록에서다음을수행합니다.
 - 장치를규정위반으로표시를선택합니다.
 - **Is** 를선택합니다.
 - **True** 를선택합니다.
 - 트리거조건이충족되면즉시장치를규정위반으로표시하도록동작을설정하려면시간프레임을 **0** 으로설정합니다.
7. 이동작을적용할 XenMobile 배달그룹을하나이상선택합니다.
8. 동작요약을검토합니다.
9. 다음을클릭한후 저장을클릭합니다.

장치가규정위반으로표시된경우 Secure Hub 저장소에더이상 HDX 앱이나타나지않습니다. 사용자는더이상앱을구독하지않습니다. 장치에알림이전송되지않으며 Secure Hub 저장소에 HDX 응용프로그램이이전에사용가능했다는내용이표시되지않습니다.

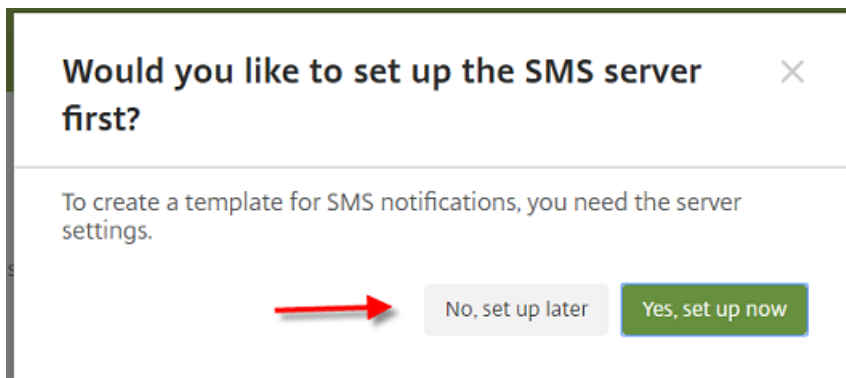
장치가규정위반으로표시될때사용자에게알리려면알림을만든다음해당알림을보내는자동화된동작을만듭니다.

이예에서는다음과같은알림을만들고장치가규정위반으로표시되는경우알림을보냅니다. “Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked.(장치일련번호또는전화번호가더이상장치정책을준수하지않으므로 HDX 응용프로그램이차단됩니다.)”



장치가 규정위반으로 표시될 때 사용자에게 표시되는 알림 만들기

1. XenMobile 콘솔에서 콘솔의 오른쪽 맨 위에 있는 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다.
2. 알림 템플릿을 클릭합니다. 알림 템플릿 페이지가 나타납니다.
3. 추가를 클릭하여 알림 템플릿 페이지에 추가합니다.
4. SMS 서버를 먼저 설정하라는 메시지가 나타나면 아니요, 나중에 설정합니다를 클릭합니다.



5. 다음 설정을 구성합니다.

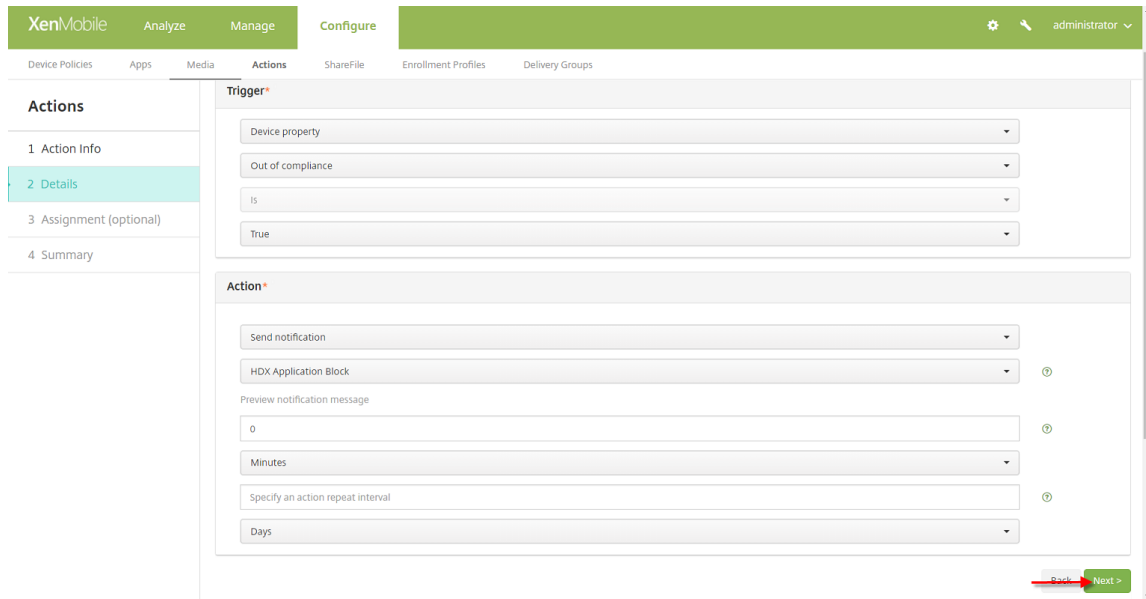
- 이름: HDX Application Block
- 설명: Agent notification when device is out of compliance
- 유형: 임시알림
- **Secure Hub:** 활성화됨
- 메시지: Device $\${firstnonnull(device.TEL_NUMBER,device.serialNumber)}$ no longer complies with the device policy and HDX applications will be blocked.

The screenshot shows a configuration form for an HDX Application Block. The 'Name' field is filled with 'HDX Application Block'. The 'Type' is set to 'Ad-Hoc Notification'. The 'SMTP' status is 'Activated'. The 'Secure Hub' status is also 'Activated'. The 'Message' field contains the text: 'Device $\${firstnonnull(device.TEL_NUMBER,device.serialNumber)}$ no longer complies with the device policy and HDX applications will be blocked.' There are 'Cancel' and 'Save' buttons at the bottom right of the form.

6. 저장을클릭합니다.

장치가규정위반으로표시되면알림을보내는동작만들기

1. XenMobile 콘솔에서 구성 > 동작을클릭합니다. 동작페이지가나타납니다.
2. 추가를클릭하여동작을추가합니다. 동작정보페이지가나타납니다.
3. 동작정보페이지에서동작의이름및설명을입력합니다.
 - 이름: HDX 차단알림
 - 설명: 장치가규정위반할경우 HDX 차단알림
4. 다음을클릭합니다. 동작세부정보페이지가나타납니다.
5. 트리거목록에서다음을수행합니다.
 - 장치속성을선택합니다.
 - 규정위반을선택합니다.
 - **Is** 를선택합니다.
 - **True** 를선택합니다.



6. 동작목록에서트리거조건이충족될때실행할동작을지정합니다.
 - 알림보내기를선택합니다.
 - 앞서만든 **HDX Application Block** 알림을선택합니다.
 - **0** 을선택합니다. 이값을 0 으로설정하면트리거조건이충족되는즉시알림이전송됩니다.
7. 이동작을적용할 XenMobile 배달그룹을하나이상선택합니다. 이예제에서는 **AllUsers** 를선택합니다.
8. 동작요약을검토합니다.
9. 다음을클릭한후 저장을클릭합니다.

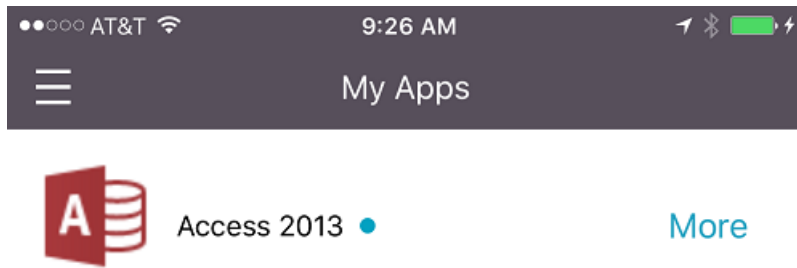
자동화된동작설정에대한자세한내용은 [자동화된동작](#) 을참조하십시오.

사용자가 **HDX** 앱에대한엑세스권한을복구하는방법

장치가다시규정을준수하게되면 HDX 앱에엑세스할수있게됩니다.

1. 장치에서 Secure Hub 저장소로이동하여저장소의앱을새로고칩니다.
2. 앱으로이동하고앱에대한 추가를누릅니다.

앱이추가되면내앱에나타나며새로설치된앱이기때문에옆에파란색점이있습니다.



미디어추가

August 23, 2019

XenMobile 에 미디어를 추가하여 사용자 장치에 미디어를 배포합니다. XenMobile 을 사용하여 Apple VPP(Volume Purchase Program) 를 통해 취득한 iBooks 를 배포할 수 있습니다.

XenMobile 에서 VPP 계정을 등록하면 구성 > 미디어에 구입한 서적 및 무료 서적이 표시됩니다. 미디어 페이지에서 배달 그룹을 선택하고 배포 규칙을 지정하여 iOS 장치에 배포할 iBooks 를 구성합니다.

사용자가 처음으로 iBooks 를 수신하고 VPP 라이선스를 수락하면 배포된 서적이 장치에 설치됩니다. 서적은 Apple iBooks 앱에 표시됩니다. 관리자는 사용자에게서 서적 라이선스를 분리하거나 장치에서 서적을 제거할 수 없습니다. XenMobile 은 iBooks 를 필수 미디어로 설치합니다. 사용자가 장치에서 설치된 서적을 삭제하는 경우 서적은 iBooks 앱에 유지되며 바로 다운로드할 수 있습니다.

사전요구사항

- iOS 장치 (최소 버전 iOS 8)
- [iOS 볼륨구입프로그램](#)에 설명된 대로 XenMobile 에서 iOS VPP 를 구성합니다.

iBooks 구성

VPP 를통해취득한 iBooks 는 구성 > 미디어페이지에표시됩니다.

<input type="checkbox"/>	Icon	Media Name	Type	Created On	Last Updated	Vpp Account
<input type="checkbox"/>		The Wonderful Wizard of Oz - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:41 PM	test
<input type="checkbox"/>		Cool Werewolf Jokes For Kids - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:28 PM	test
<input type="checkbox"/>		Science Fiction Stories - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:32 PM	test
<input type="checkbox"/>		Coming Out - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:45 AM	test
<input type="checkbox"/>		Short Stories - VPP	Apple iBooks	6/15/17 1:29 PM	6/15/17 1:29 PM	test
<input type="checkbox"/>		A Diamond in My Pocket - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:39 AM	test

Showing 1 - 6 of 6 items Items per page: 10

배포할 iBooks 를구성하려면

1. 구성 > 미디어에서 iBooks 를선택하고 편집을클릭합니다. 서적정보페이지가나타납니다.

iBook

- 1 Book Information
- 2 Platform
- iPhone
- iPad
- 3 Delivery Group Assignments (optional)

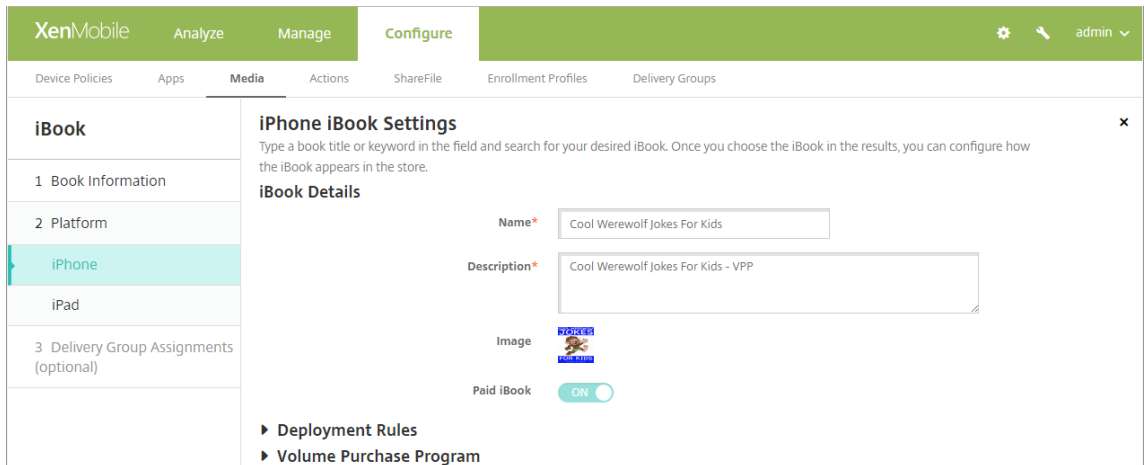
Book Information

Name*

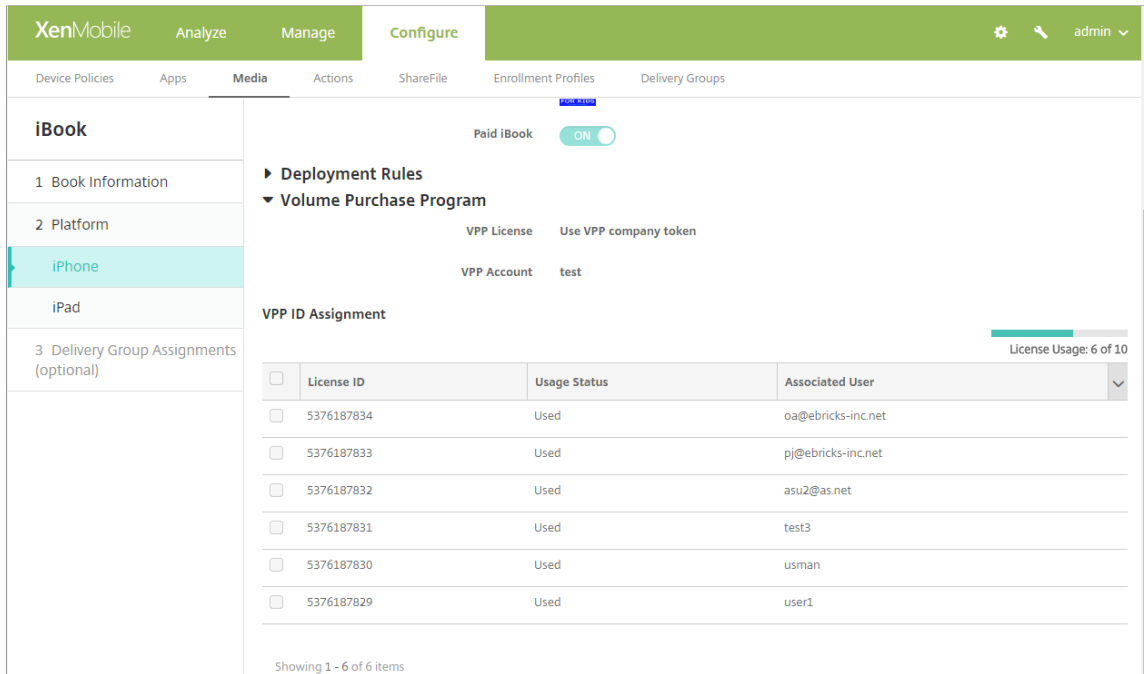
Description

이름및 설명은 XenMobile 콘솔과로그에만표시됩니다.

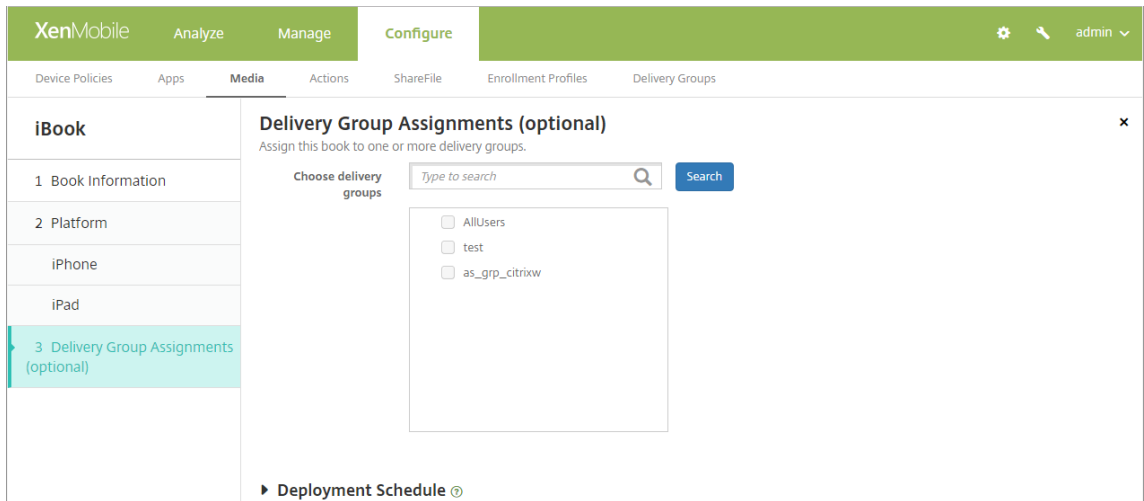
2. **iPhone iBook** 설정및 **iPad iBook** 설정페이지에서: 필요한경우 iBooks 이름과설명을변경할수있지만이러한설정을변경하지않는것이좋습니다. 이미지는정보를위한것이며편집할수없습니다. 유료 **iBook** 은 VPP 를통해구매한 iBooks 를나타냅니다.



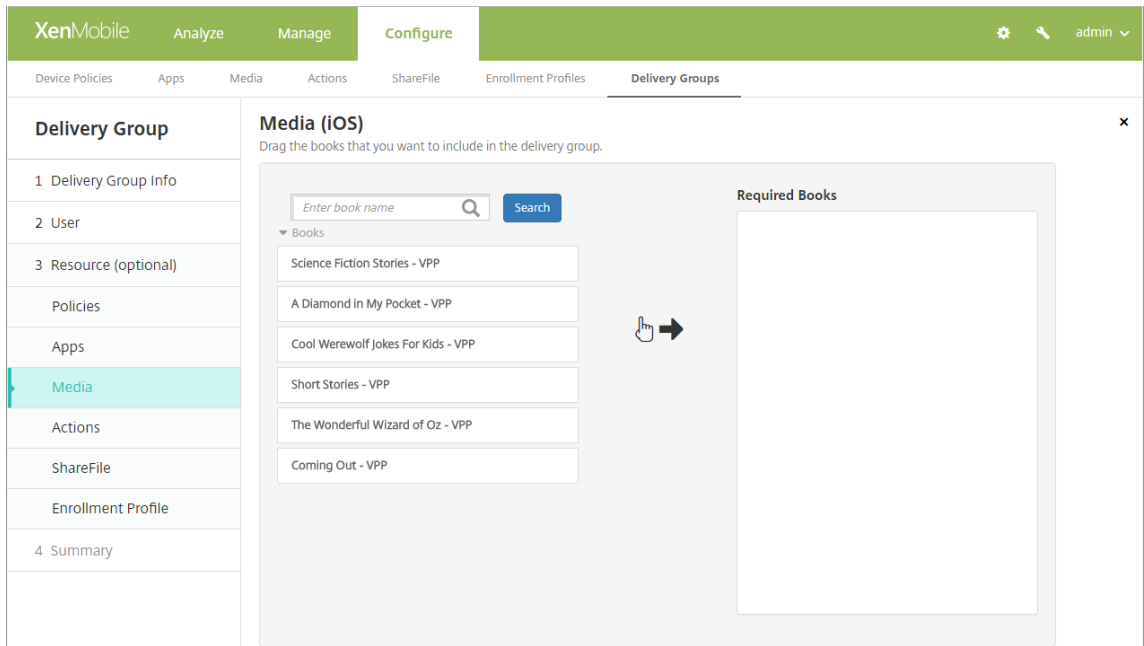
배포규칙을지정하거나 VPP 정보를볼수도있습니다.



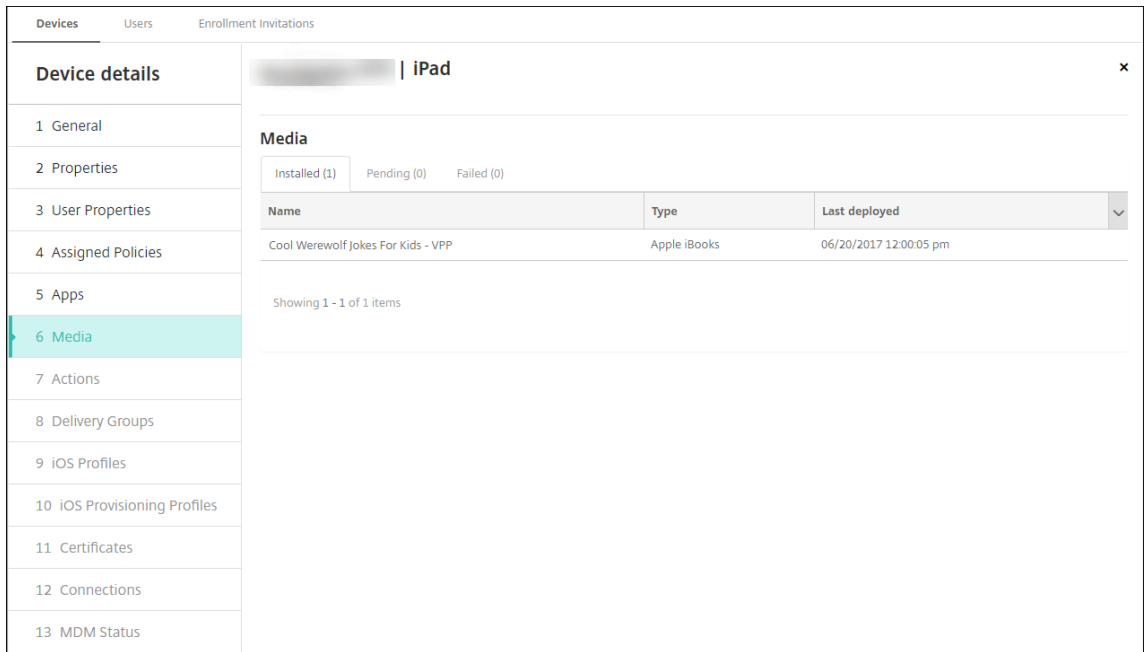
3. 필요한경우 iBooks 를배달그룹에할당하고배포일정을설정합니다.



또한 구성 > 배달그룹의 미디어탭에서도배달그룹에 iBooks 를할당할수있습니다. XenMobile 은필수서적배포만지원합니다.



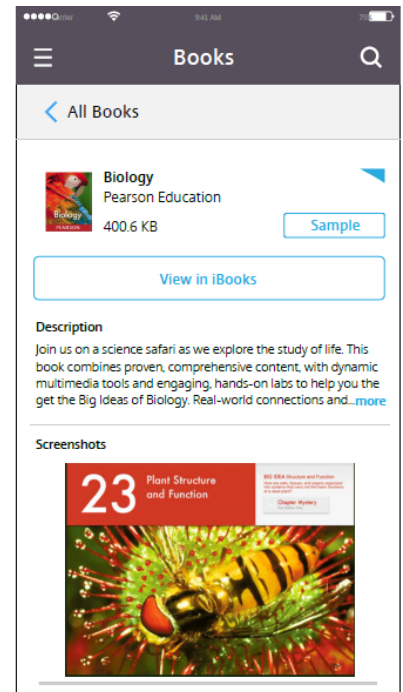
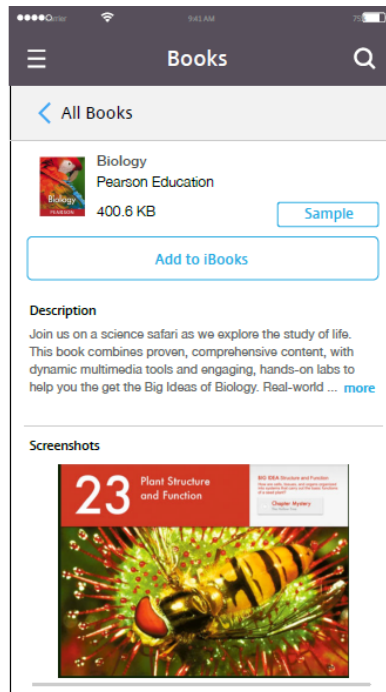
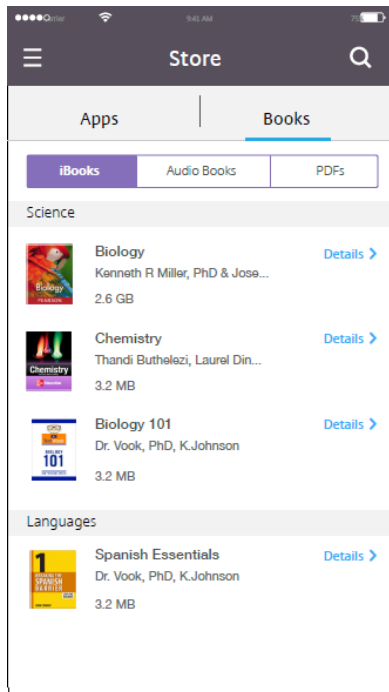
4. 배포상태를보려면 관리 > 장치의 미디어탭을사용합니다.



참고:

구성 > 미디어페이지에서서적을선택하고 삭제클릭하면 XenMobile 이목록에서해당서적을제거합니다. 그러나 VPP 에서서적을제거하지않은경우 XenMobile 이다음에 VPP 와동기화되면해당서적이목록에다시표시됩니다. 목록에서서적을제거해도장치에서서적이삭제되지는않습니다.

iBooks 는이샘플에표시된것과같이사용자장치에표시됩니다.



리소스배포

January 27, 2020

장치구성및관리에는일반적으로 XenMobile 콘솔에서리소스 (정책, 앱및미디어) 및동작을만들고배달그룹을사용하여패키징하는단계가포함됩니다. XenMobile 이배달그룹의리소스및동작을장치로푸시하는순서를 배포순서라고합니다. 이문서에서설명하는내용:

- 배달그룹추가, 관리및배포
- 배달그룹에서리소스및작업의배포순서변경
- XenMobile 은사용자가중복또는충돌하는정책이있는여러배달그룹에속한경우에배포순서를결정합니다.

배달그룹은정책, 앱, 미디어및동작조합을배포하는대상장치의사용자범주를지정합니다. 일반적으로회사, 국가, 부서, 사무실주소, 직함과같은사용자의특성에따라특정배달그룹에서사용자를포함시킵니다. 배달그룹을통해누가어떤리소스를어떤경우에이용할수있는지를보다효과적으로제어할수있습니다. 배달그룹은모든사용자에게배포하거나좀더구체적으로정의된그룹의사용자에게배포할수있습니다.

배달그룹에배포한다는것은지원되는 iOS 및 Windows 장치의모든사용자에게푸시알림을보내는것을의미합니다. 이러한사용자는배달그룹에속해있어야 XenMobile 에다시연결됩니다. 장치를재평가하고배달그룹에포함되는정책, 앱, 미디어및동작을배포할수있습니다.

Android 장치사용자: 이미연결된경우즉시리소스를받습니다. 그렇지않은경우에는예약정책에기반하여다음에연결할때리소스를받습니다.

XenMobile 을설치하고구성하면기본 AllUsers 배달그룹이만들어집니다. 여기에는모든로컬사용자와 Active Directory 사용자 포함되어있습니다. AllUsers 그룹은삭제할수없지만일부사용자에게리소스를푸시하지않으려는경우이그룹을사용하지않도록설정할수있습니다.

배포순서

배포순서는 XenMobile 이장치에리소스를푸시하는순서입니다. 배포순서는 MDM 모드에서만지원됩니다.

배포순서를결정할때 XenMobile 은정책, 앱, 미디어, 동작및배달그룹에배포규칙및배포일정과같은필터와제어조건을적용합니다. 배달그룹을추가하기전에배포목표를고려하여이섹션의내용을검토하십시오.

배포순서와관련된주요개념을요약하면다음과같습니다.

- **배포순서:** XenMobile 이장치에리소스 (정책, 앱및미디어) 및동작을푸시하는순서입니다. 약관및소프트웨어인벤토리와같은일부정책의배포순서는다른리소스에영향을주지않습니다. 동작이배포되는순서는다른리소스에영향을주지않으므로 XenMobile 이리소스를배포할때해당위치가무시됩니다.
- **배포규칙:** XenMobile 은장치속성에지정된배포규칙을사용하여정책, 앱, 미디어, 동작및배달그룹을필터링합니다. 예를들어, 도메인이름이특정값과일치하는경우배포패키지를푸시하도록배포규칙을지정할수있습니다.
- **배포일정:** XenMobile 은정책, 앱, 미디어및동작에지정된배포일정을사용하여해당항목의배포를제어합니다. 배포가특정날짜및시간에즉시이루어지거나배포조건에따라이루어지도록지정할수있습니다.

다음표에는다양한개체및리소스유형에대한필터및제어기준이나와있습니다. 배포규칙은장치속성에기반합니다.

개체/리소스	장치플랫폼	배포규칙	배포일정	사용자/그룹
장치정책	예	예	예	-
앱	예	예	예	-
미디어	예	예	예	-
동작	-	예	예	-
배달그룹	-	예	-	예

일반적인환경에서는단일사용자에게여러배달그룹이할당되어다음과같은결과가나타날가능성이큰니다.

- 배달그룹내에서중복된개체가존재합니다.
- 사용자에게할당된여러배달그룹에서특정정책이서로다르게구성됩니다.

이러한상황이발생할경우 XenMobile 은특정장치에배포하거나관련작업을수행해야하는모든개체의배포순서를계산합니다. 계산단계는장치플랫폼에독립적입니다.

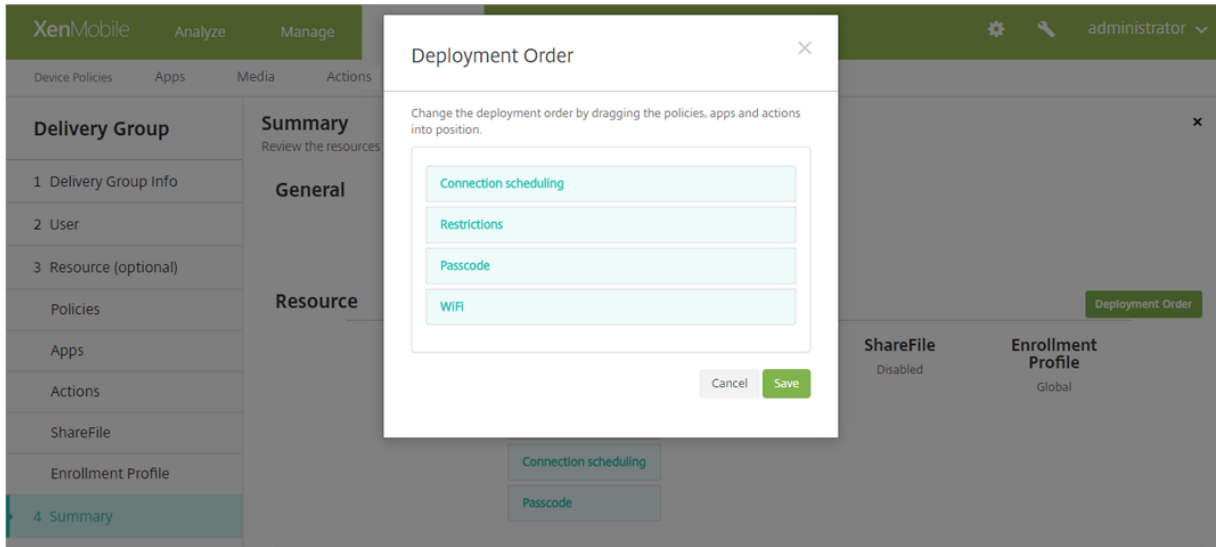
계산단계:

1. 사용자, 그룹및배포규칙의필터에기반하여특정사용자의모든배달그룹을결정합니다.
2. 선택된배달그룹내의모든리소스 (정책, 앱, 미디어및동작) 의순서지정된목록을만듭니다. 목록은장치플랫폼, 배포규칙및 배포일정의필터를기반으로합니다. 순서지정알고리즘은다음과같습니다.
 - a) 사용자정의배포순서가있는배달그룹의리소스를사용자정의배포순서가없는배달그룹의리소스보다먼저배치합니다. 이렇게배치하는이유는이러한단계다음에설명되어있습니다.
 - b) 배달그룹간에순서가동일한경우에는배달그룹이름에따라배달그룹리소스순서를지정합니다. 예를들어, 배달그룹 A 의리소스를배달그룹 B 의리소스보다먼저배치합니다.
 - c) 정렬할때는배달그룹리소스에사용자정의배포순서가지정된경우해당순서를유지합니다. 그렇지않은경우리소스이름으로배달그룹내리소스를정렬합니다.
 - d) 동일한리소스가두번이상나타나는경우중복된리소스를제거합니다.

사용자정의순서가있는리소스는사용자정의순서가없는리소스보다먼저배포됩니다. 하나의리소스가사용자에게할당된여러배달그룹에존재할수있습니다. 위의단계에나온것처럼계산알고리즘은중복된리소스를제거하고이목록에있는첫번째리소스만제공합니다. 이러한방식으로중복된리소스를제거함으로써 XenMobile 은 XenMobile 관리자정의의한순서를적용합니다.

예를들어, 다음과같은두개의배달그룹이있는경우를살펴보겠습니다.

- 배달그룹, 계정관리자 1: 리소스순서가 지정되지않습니다. 정책 **WiFi** 및 암호를포함합니다.
- 배달그룹, 계정관리자 2: 리소스순서가 지정됩니다. 정책 연결예약, 제한, 암호, **WiFi** 를포함합니다. 이상태에서 암호정책을 **WiFi** 정책보다먼저배포하려고합니다.

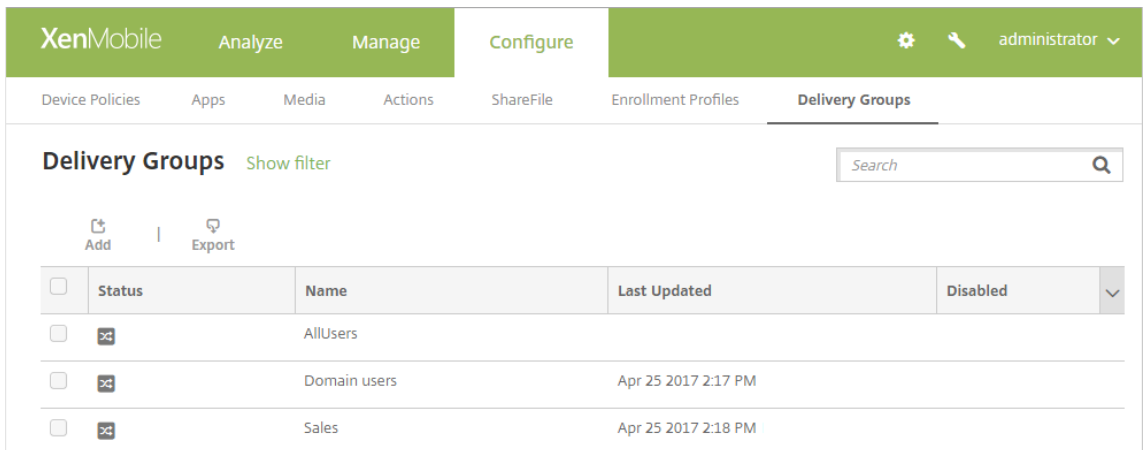


계산알고리즘이름으로만배포그룹순서를지정한경우 XenMobile 은배달그룹계정관리자 1 부터시작하여 **WiFi**, 암호, 연결예약, 제한순서로배포를수행합니다. 계정관리자 2 배달그룹의 암호및 **WiFi** 두가지는중복되므로무시됩니다.

하지만계정관리자 2 그룹에는관리자가지정한배포순서가있습니다. 따라서계산알고리즘은계정관리자 2 배달그룹의리소스를다른배달그룹의리소스보다높은순서로목록에배치합니다. 따라서 XenMobile 은 연결예약, 제한, 암호, **WiFi** 순서로정책을배포합니다. 계정관리자 1 배달그룹의 **WiFi** 및 암호정책은중복되므로무시됩니다. 이처럼계산알고리즘은 XenMobile 관리자가지정순서를따릅니다.

배달그룹을추가하려면

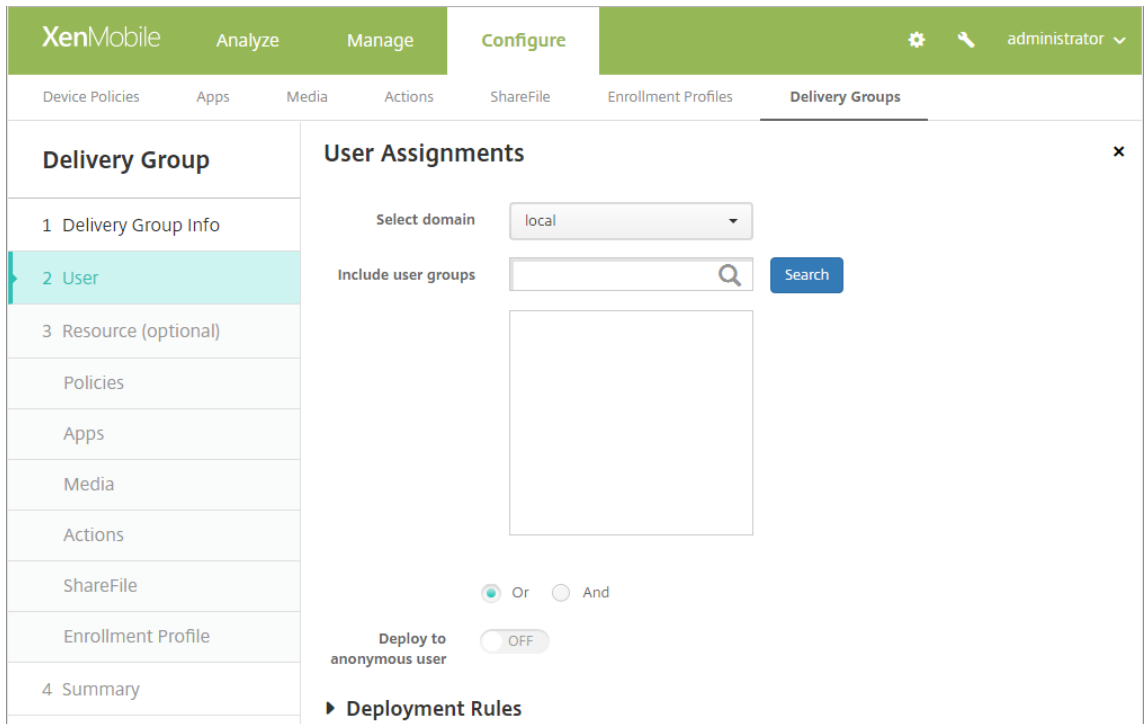
1. XenMobile 콘솔에서 구성 > 배달그룹을클릭합니다. 배달그룹페이지가나타납니다.



2. 배달그룹페이지에서 추가를클릭합니다. 배달그룹정보페이지가표시되면다음정보를입력합니다.

- 이름: 배달그룹을설명하는이름을입력합니다.
- 설명: 배달그룹에대한선택적설명을입력합니다.

3. 다음을클릭합니다. 사용자할당페이지가나타납니다. 다음설정을구성합니다.



- 도메인선택: 목록에서사용자를선택할도메인을선택합니다.
- 사용자그룹포함: 다음중하나를수행합니다.
 - 사용자그룹목록에서추가하려는그룹을클릭합니다. 선택한그룹이 선택된사용자그룹목록에나타납니다.
 - 검색을클릭하여선택된도메인의모든사용자그룹목록을봅니다.
 - 검색상자에전체또는일부그룹이름을입력한다음 검색을클릭하여사용자그룹의목록을제한합니다.

선택된사용자그룹목록에서사용자그룹을제거하려면다음중하나를수행합니다.

- 선택된사용자그룹목록에서제거할각그룹옆에있는 **X** 를클릭합니다.
- 검색을클릭하여선택된도메인의모든사용자그룹목록을봅니다. 목록을스크롤하면서제거할각그룹의확인란을 선택취소합니다.
- 검색상자에전체또는일부그룹이름을입력한다음 검색을클릭하여사용자그룹의목록을제한합니다. 목록을 스크롤하면서제거할각그룹의확인란을선택취소합니다.
- 또는/및: 리소스를배포하기위해사용자가임의의그룹에있을수있는지 (또는), 아니면모든그룹에있어야하는지 (및) 를선택합니다.
- 익명사용자에게배포: 배달그룹의인증되지않은사용자에게배포할것인지여부를선택합니다.

인증되지않은사용자는인증하지못했지만 XenMobile 에장치를연결할수있도록허용한사용자입니다.

4. 배포규칙을구성합니다.

5. 배포규칙을확장하고다음설정을구성합니다. 기본적으로 기본탭이표시됩니다.

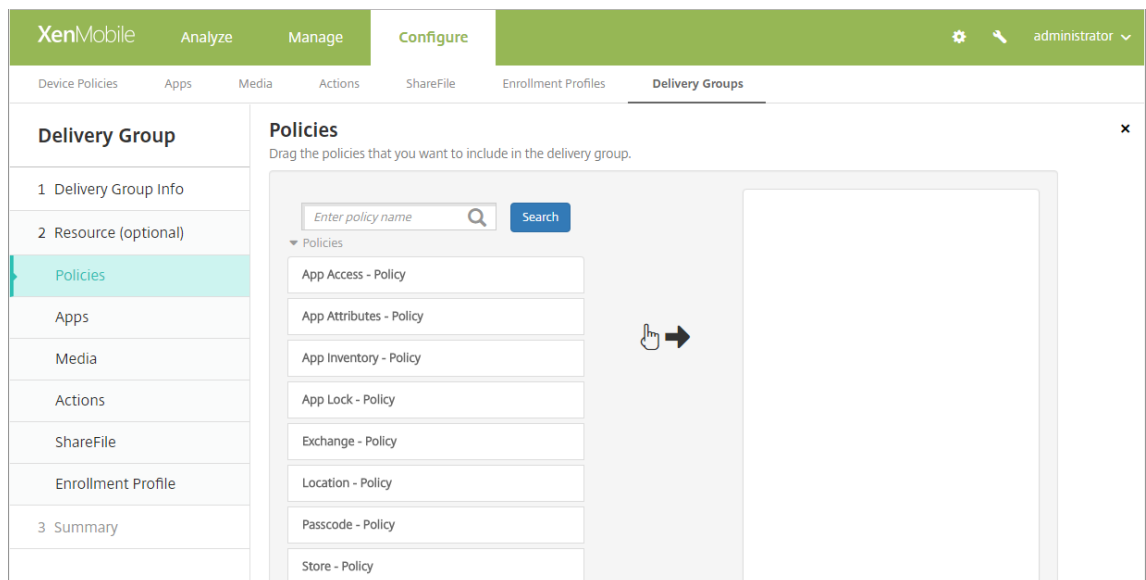
- 목록에서어떤경우에정책을배포할지정하는옵션을클릭합니다. 모든조건이충족된경우또는조건중하나라도충족 된경우정책을배포하도록선택할수있습니다. 기본옵션은 모두입니다.

- 조건을정의하려면 새규칙을클릭합니다.
 - 목록에서사용자로그온이름, 도메인이름등의조건을클릭합니다.
 - 조건을추가하려면 새규칙을다시클릭합니다.
6. 고급탭을클릭하여규칙을부울옵션과결합합니다. 기본탭에서선택한조건이표시됩니다.
7. 추가고급부울논리를사용하여규칙을결합하거나, 편집하거나, 추가할수있습니다.
- 그리고, 또는이나 아님을클릭합니다.
 - 규칙에조건을추가하려면목록에서규칙에추가할조건을선택하고오른쪽의더하기기호 (+) 를클릭합니다.
언제든지조건을클릭하여선택한다음 편집을클릭하여조건을변경하거나 삭제를클릭하여조건을제거할수있습니다.
 - 조건을추가하려면 새규칙을다시클릭합니다.
8. 다음을클릭합니다. 배달그룹리소스페이지가나타납니다. 필요한경우배달그룹에대한정책, 앱또는동작을추가할수도있습니다. 이단계를건너뛰려면 배달그룹아래에서 요약을클릭하여배달그룹구성요약을봅니다.
- 리소스를건너뛰려면 리소스 (선택사항) 아래에서추가할리소스를클릭하고해당리소스에대한단계를수행합니다.

정책을추가하려면

1. 추가하려는각정책에대해다음을수행합니다.
- 사용가능한정책목록을스크롤하면서추가할정책을찾습니다.
 - 또는검색상자에전체또는일부정책이름을입력한다음 검색을클릭하여정책목록을제한합니다.
 - 추가할정책을클릭하고오른쪽의상자로끌어옵니다.

정책을제거하려면오른쪽상자에서정책이름옆에있는 X 를클릭합니다.



2. 다음을클릭합니다. 앱페이지가나타납니다.

앱을추가하려면

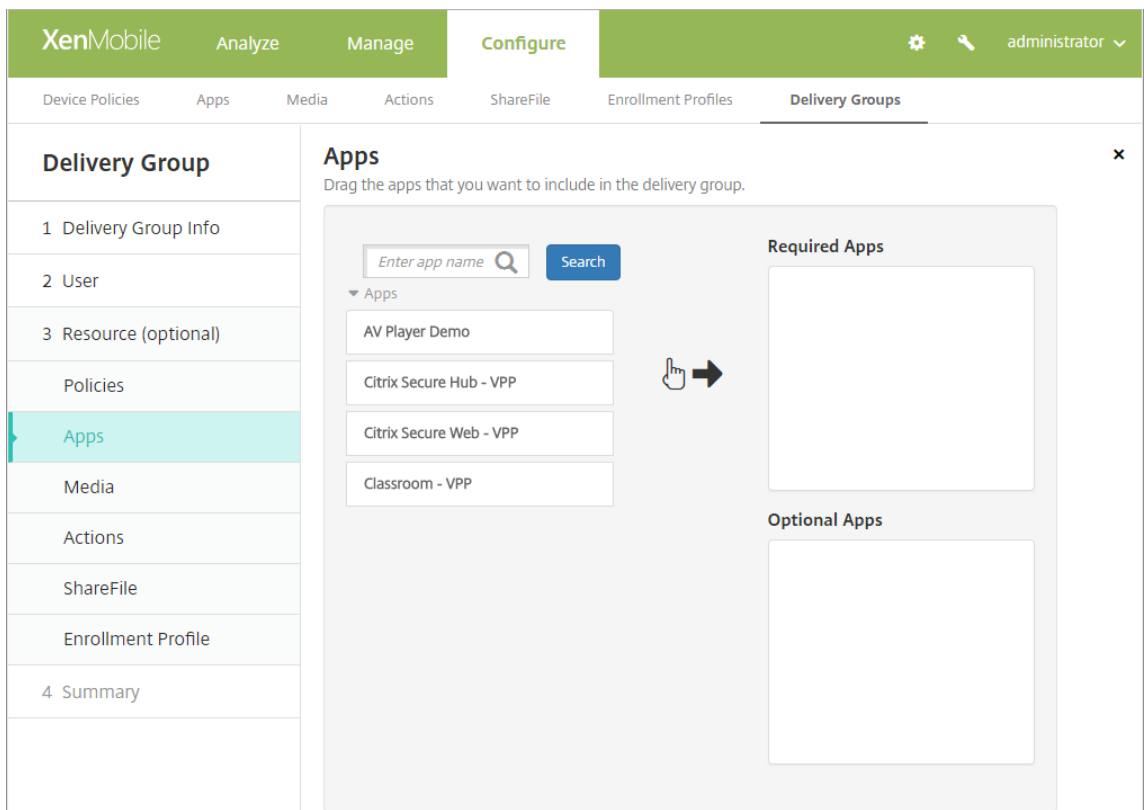
1. 추가하려는각앱에대해다음을수행합니다.

- 사용가능한앱목록을스크롤하면서추가할앱을찾습니다.
- 검색상자에전체또는일부앱이름을입력한다음 검색을클릭하여앱목록을제한합니다.
- 추가할앱을클릭하고 필수앱상자또는 선택적앱상자로킵니다.

필수로표시된앱의경우사용자는다음과같은경우에곧바로업데이트를받을수있습니다.

- 사용자가새앱을업로드하고필수앱으로표시합니다.
- 사용자가기존앱을필수앱으로표시합니다.
- 사용자가필수앱을삭제합니다.
- Secure Hub 업데이트가제공됩니다.

기능을사용하도록설정하는방법을포함하여필수앱의강제배포에대한자세한내용은 [필수앱과선택적앱정보](#)를참조하십시오.



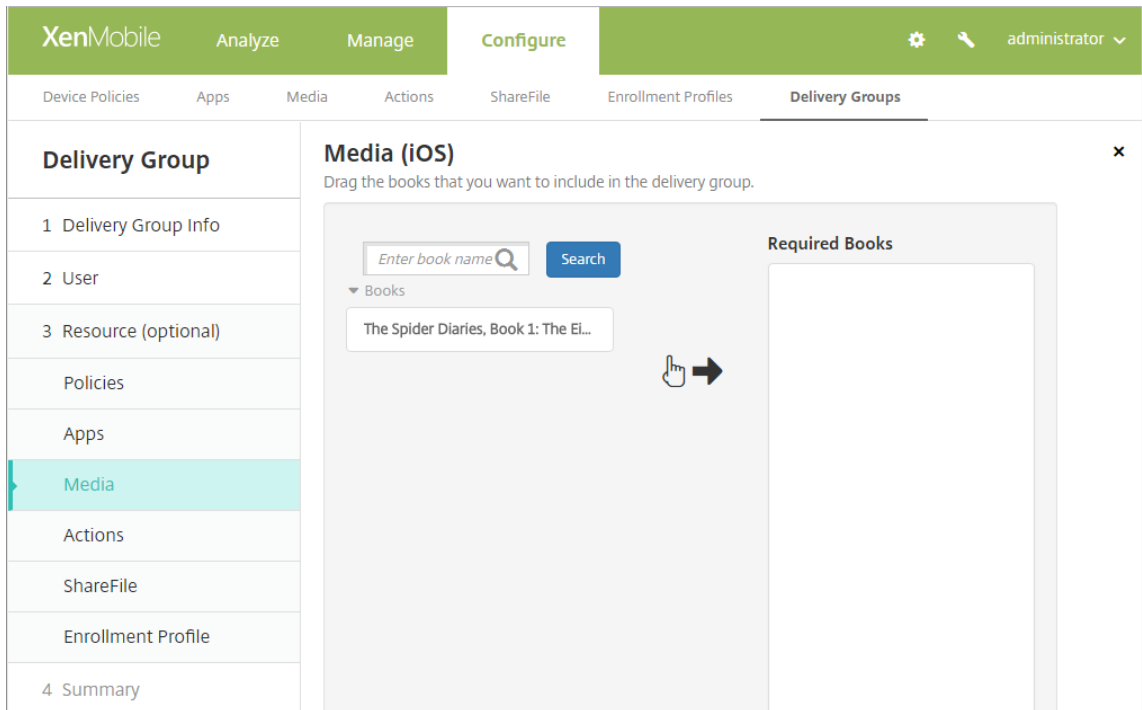
앱을제거하려면오른쪽상자에서앱이름옆에있는 X 를클릭합니다.

2. 다음을클릭합니다. 미디어페이지가나타납니다.

미디어를추가하려면

1. 추가할각서적에대해다음을수행합니다.

- 사용가능한서적목록을스크롤하면서추가할서적을찾습니다.
- 검색상자에전체또는일부서적이름을입력한다음 검색을클릭하여서적목록을제한합니다.
- 추가할서적을클릭하고 필수서적상자로끌어옵니다.



필수로표시된서적의경우사용자는다음과같은경우에곧바로업데이트를받습니다.

- 새서적을업로드하고필수앱으로표시합니다.
- 기존서적을필수서적으로표시합니다.
- 사용자가필수서적을삭제합니다.
- Secure Hub 업데이트가제공됩니다.

서적을제거하려면오른쪽상자에서서적이름옆에있는 **X** 를클릭합니다.

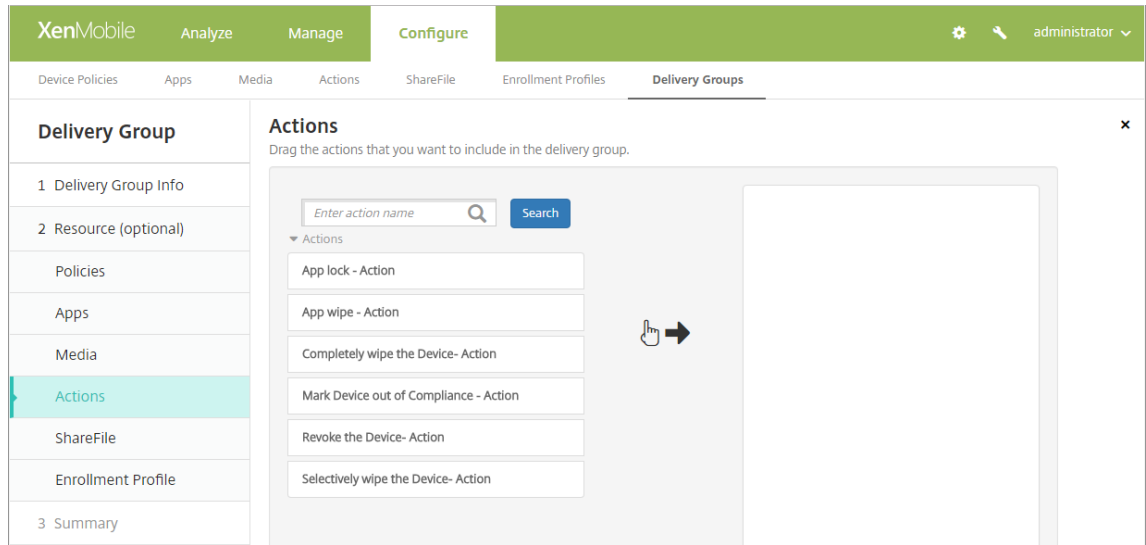
2. 다음을클릭합니다. 동작페이지가나타납니다.

동작을추가하려면

1. 추가할각동작에대해다음을수행합니다.

- 사용가능한동작목록을스크롤하면서추가할동작을찾습니다.
- 검색상자에전체또는일부동작이름을입력한다음 검색을클릭하여동작목록을제한합니다.
- 추가할동작을클릭하고오른쪽상자로끌어옵니다.

동작을 제거하려면 오른쪽 상자에서 동작 이름 옆에 있는 **X** 를 클릭합니다.

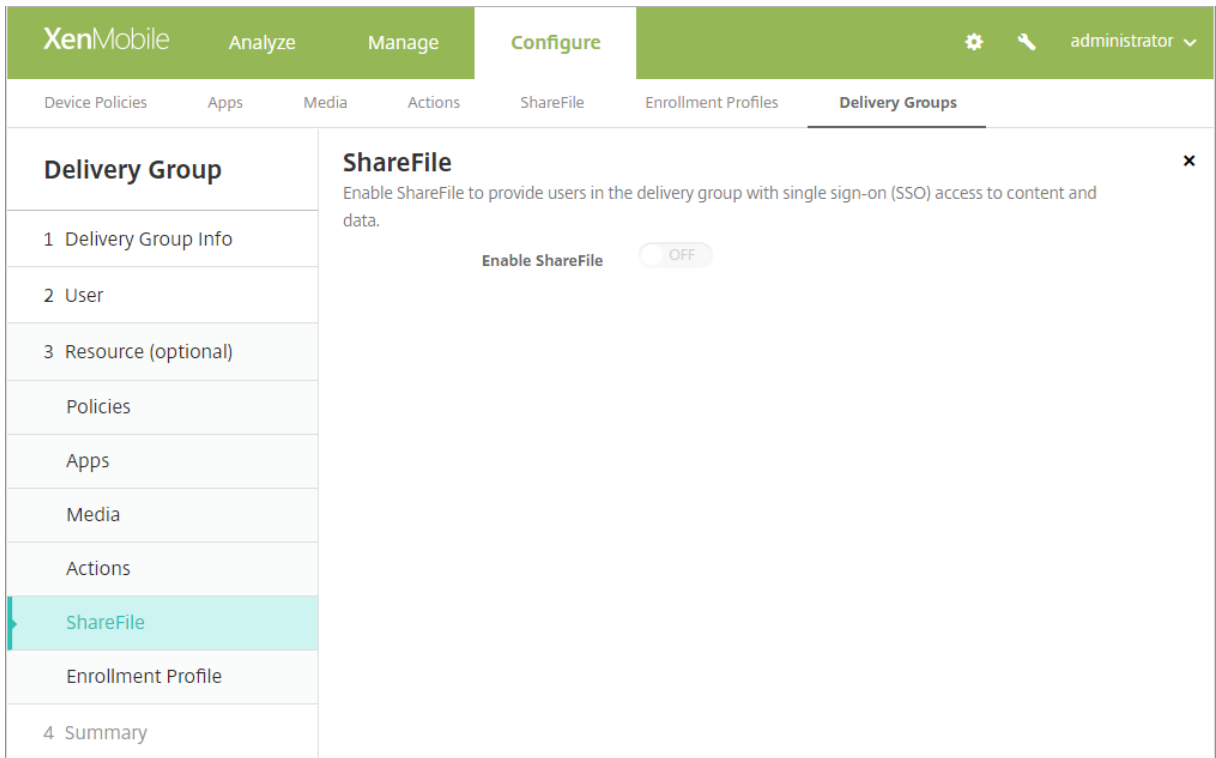


2. 다음을 클릭합니다. **ShareFile** 페이지가 나타납니다.

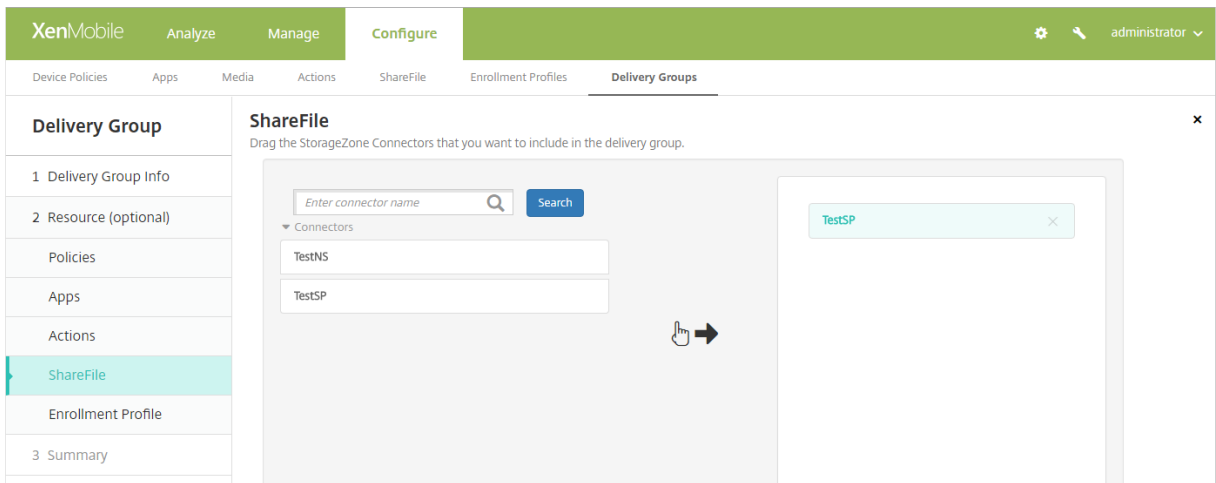
ShareFile 구성을 적용하려면

ShareFile 페이지는 XenMobile(구성 > **ShareFile**) 에 ShareFile Enterprise 를 사용하도록 구성했는지, 아니면 StorageZone 커넥터를 사용하도록 구성했는지에 따라 달라집니다.

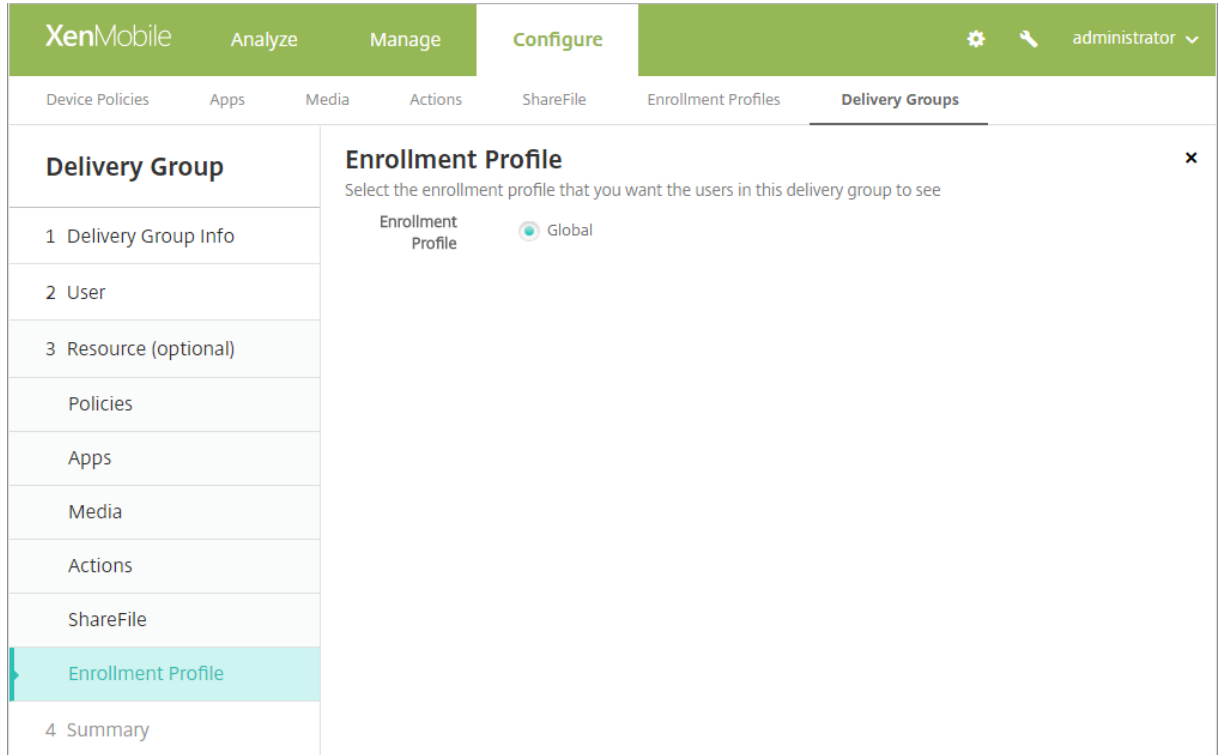
XenMobile 에 ShareFile Enterprise 를 사용하도록 구성한 경우 **ShareFile** 사용을 켜짐으로 설정하여 배달 그룹에 ShareFile 콘텐츠 및 데이터에 대한 SSO(Single Sign-On) 액세스를 제공합니다.



XenMobile 에 StorageZone 커넥터를사용하도록구성한경우배달그룹에포함할 StorageZone 커넥터를선택합니다.

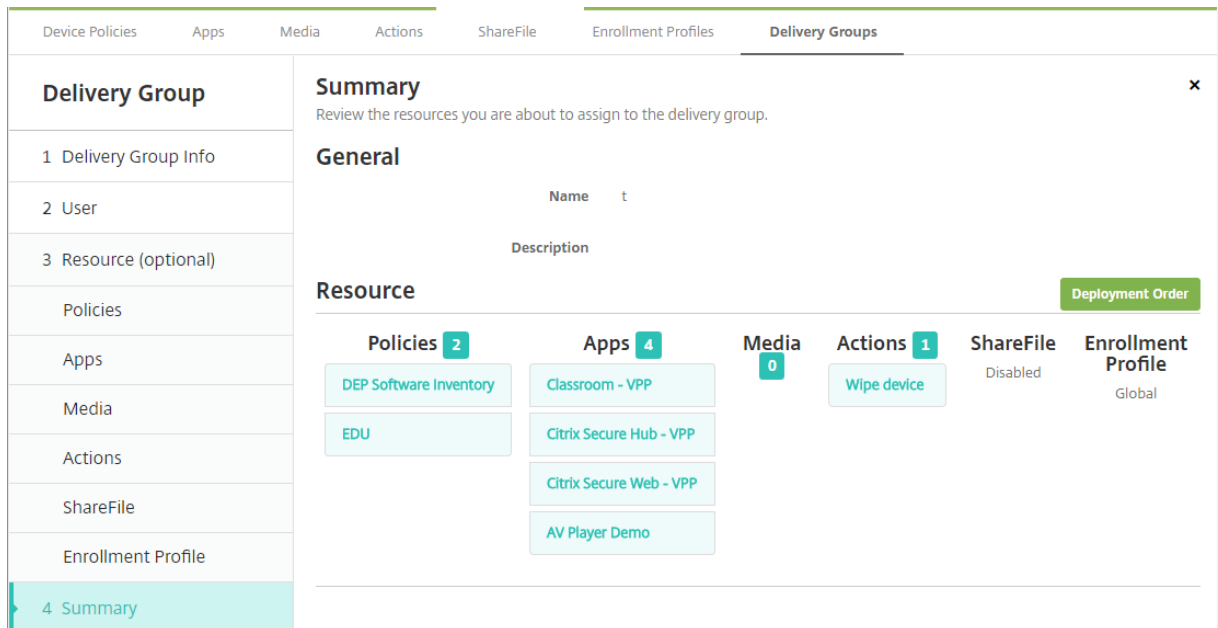


등록프로필을선택하려면



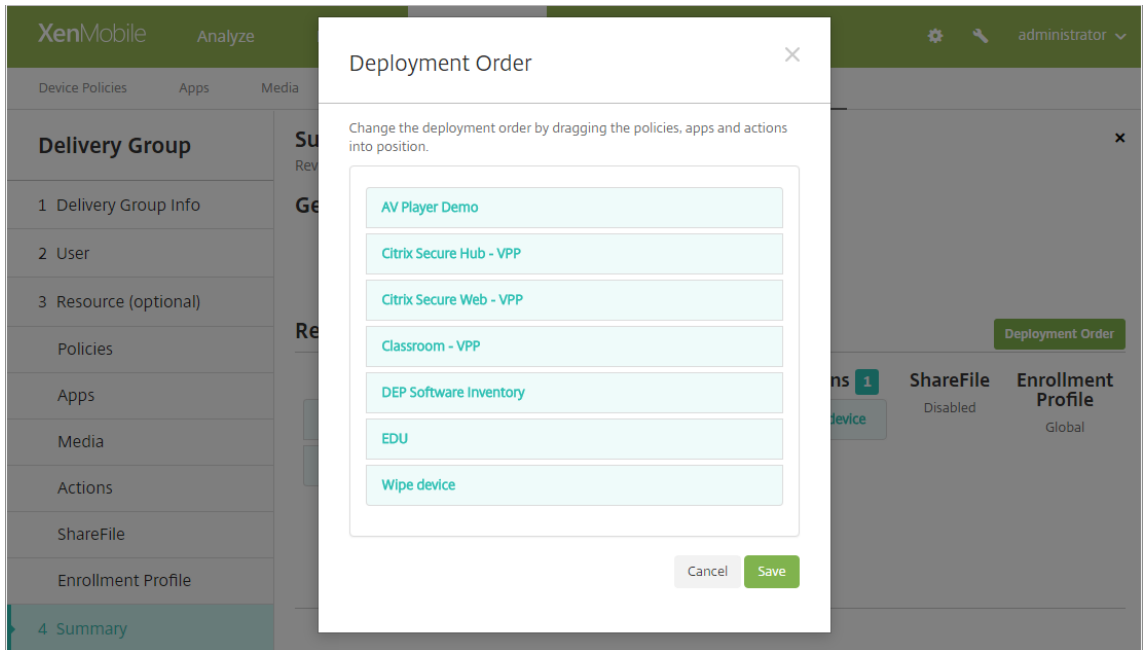
- 등록프로필: 등록프로필을선택합니다. 등록프로필을만들려면 장치등록제한을참조하십시오.
- 다음을클릭합니다. 요약페이지가나타납니다.

구성된옵션을검토하고배포순서를변경하려면



요약페이지에서배달그룹에구성한옵션을검토하고리소스의배포순서를변경할수있습니다. 요약페이지에리소스가범주별로표시됩니다. 요약페이지에는배포순서는반영되지않습니다.

1. 뒤로클릭하여이전페이지로돌아가서구성에필요한조정을수행합니다.
2. 배포순서를클릭하여배포순서를확인하거나재정렬합니다. 배포순서대화상자가나타납니다.



3. 리소스를클릭하고배포할위치로끌어옵니다. 배포순서를변경한후 XenMobile 은목록의위에서아래로리소스를배포합니다.
4. 저장클릭하여배포순서를저장합니다.
5. 저장클릭하여배달그룹을저장합니다.

배달그룹을편집하려면

기존배달그룹의이름은변경할수없습니다. 다른설정을업데이트하려면: 구성 > 배달그룹으로이동하고편집할그룹을선택한후 편집클릭합니다.

AllUsers 배달그룹을사용하거나사용하지않도록설정하려면

AllUsers 배달그룹만사용하거나사용하지않도록설정할수있습니다.

배달그룹페이지에서 **AllUsers** 옆에있는확인란을선택하고 AllUsers 가포함된줄을클릭하여 AllUsers 배달그룹을선택합니다. 다음중하나를실행합니다.

- AllUsers 배달그룹을사용하지않도록설정하려면 사용안함을클릭합니다. 이명령은 AllUsers 를사용하도록설정된(기본값) 경우에만사용할수있습니다. 배달그룹테이블의 사용안함머리글아래에 사용안함이표시됩니다.

- AllUsers 배달그룹을사용하도록설정하려면 사용을클릭합니다. 이명령은 AllUsers 를사용하지않도록설정만 경우에만 사용할수있습니다. 배달그룹테이블의 사용안함머리글아래에 사용안함이사라집니다.

배달그룹에배포하려면

배달그룹에배포한다는것은 iOS, Windows Phone 및 Windows 태블릿장치의모든사용자에게푸시알림을보내는것을의미합니다. 이러한사용자는배달그룹에속해있어야 XenMobile 에다시연결됩니다. 이방법을통해장치를재평가하고앱, 정책및작업을배포할수있습니다.

다른플랫폼장치의사용자: 해당장치가이미 XenMobile 에연결된경우즉시리소스를받습니다. 그렇지않은경우에는예약정책에기반하여다음에연결할때리소스를받습니다.

Android 장치에있는 XenMobile Store 의업데이트사용가능목록에업데이트된앱이표시되게하려면먼저앱인벤토리정책을사용자장치에배포해야합니다.

1. 배달그룹페이지에서다음중하나를수행합니다.
 - 한번에둘 이상의배달그룹에배포하려면배포하려는그룹옆에있는확인란을선택합니다.
 - 하나의배달그룹에배포하려면해당이름옆의확인란을선택하거나해당이름이포함된줄을클릭합니다.

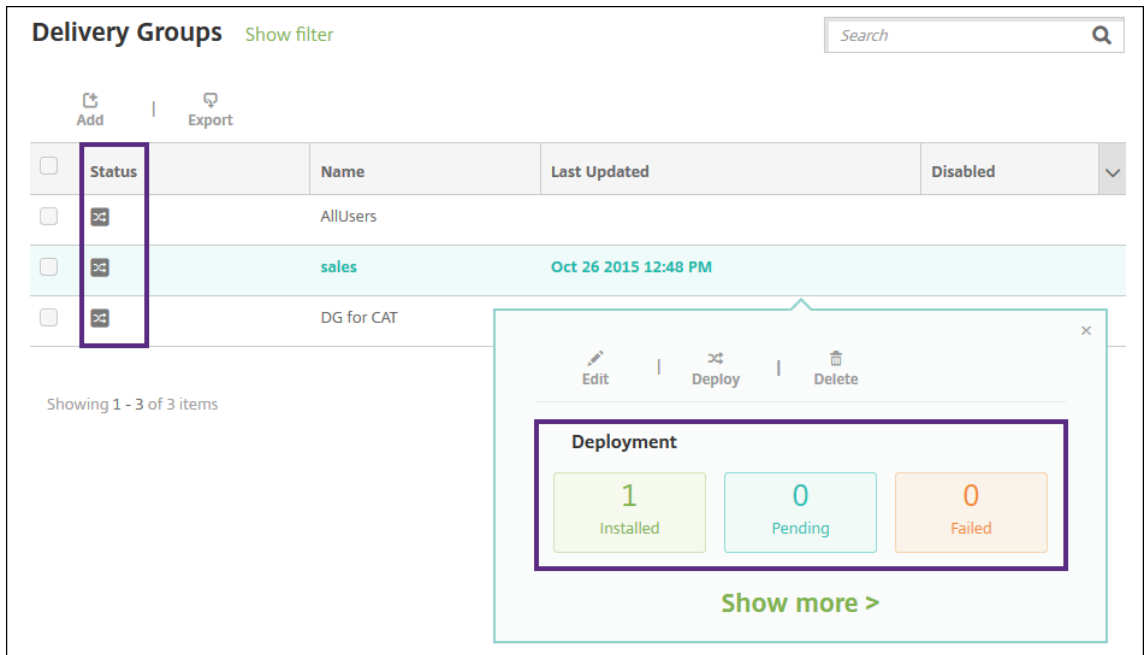
2. 배포를클릭합니다.

배달그룹을선택한방법에따라배달그룹위또는오른쪽에 배포명령이나타납니다.

앱, 정책및동작을배포할그룹이나열되어있는지확인하고 배포를클릭합니다. 장치플랫폼과예약정책에따라선택한그룹에 앱, 정책및동작이배포됩니다.

배달그룹페이지에서다음방법중하나로배포상태를확인할수있습니다.

- 배달그룹의 상태머리글아래에있는배포아이콘을확인합니다. 배포가실패한경우이아이콘에나타납니다.
- 배달그룹이포함된줄을클릭하여 설치됨, 보류중및 실패배포를나타내는오버레이를표시합니다.



배달그룹을삭제하려면

AllUsers 배달그룹은삭제할수없지만일부사용자에게게리소스를푸시하지않으려는경우이그룹을사용하지않도록설정할수있습니다.

1. 배달그룹페이지에서다음중하나를수행합니다.
 - 한번에둘이상배달그룹을삭제하려면삭제하려는그룹옆에있는확인란을선택합니다.
 - 하나의배달그룹을삭제하려면해당이름옆의확인란을선택하거나해당이름이포함된줄을클릭합니다.

2. 삭제를클릭합니다. 삭제대화상자가나타납니다.

단일배달그룹을선택하는방법에따라배달그룹위또는오른쪽에 삭제명령이나타납니다.

중요:

삭제는실행취소할수없습니다.

3. 삭제를클릭합니다.

배달그룹테이블을내보내려면

1. 배달그룹테이블위에있는 내보내기단추를클릭합니다. 배달그룹테이블에있는정보를추출하여.csv 파일로변환합니다.
2. 브라우저의일반적인단계에따라.csv 파일을열거나저장합니다. 또한작업을취소할수도있습니다.

매크로

August 23, 2019

XenMobile 은다음항목의텍스트필드내에사용자또는장치속성데이터를채우기위한방법으로매크로를제공합니다.

- 정책
- 알림
- 등록템플릿
- 자동화된동작
- 자격증명공급자인증서서명요청

XenMobile 은매크로를해당사용자또는시스템값으로바꿉니다. 예를들어사용자수천명에대해단일 Exchange 프로필을보유한 각사용자의사서함값을미리채울수있습니다.

매크로구문

매크로는다음과같은형식을사용할수있습니다.

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]] }`

달러기호 (\$) 뒤에오는모든구문은중괄호 ({}) 로묶습니다.

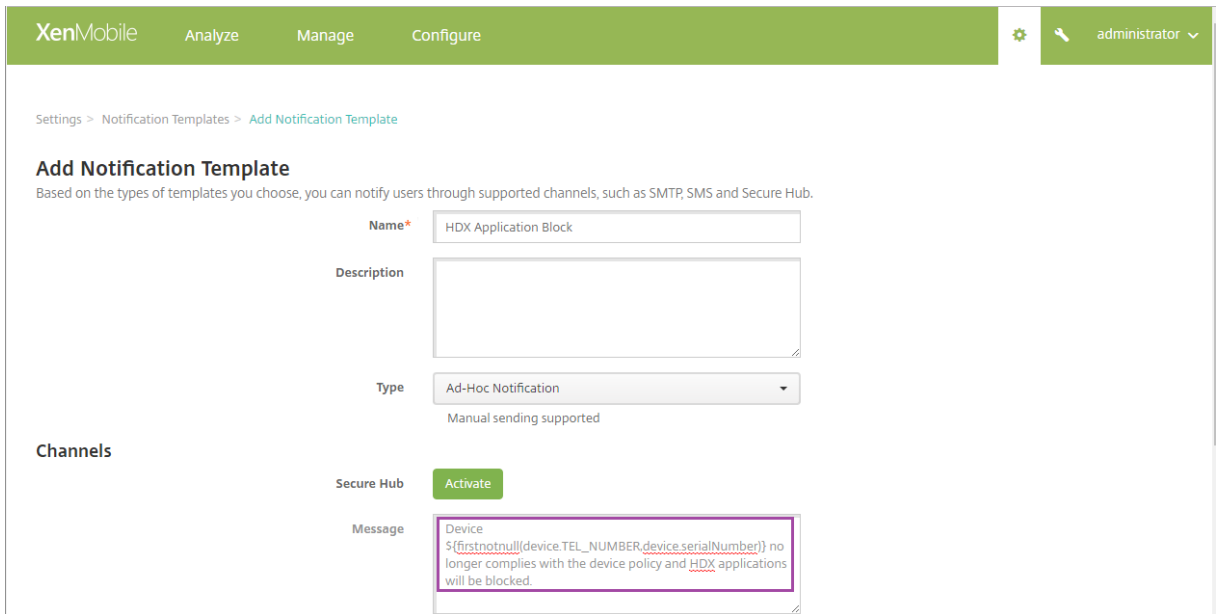
- 정규화된속성이름은사용자속성, 장치속성또는사용자지정속성을참조합니다.
- 정규화된속성이름은접두사와접두사뒤에오는실제속성이름으로구성됩니다.
- 사용자속성은 `${ user.[PROPERTYNAME] (prefix="user.") }` 형식을사용합니다.
- 장치속성은 `${ device.[PROPERTYNAME] (prefix="device.") }` 형식을사용합니다.
- 속성이름은대/소문자를구분합니다.
- 함수는제한된목록또는함수를정의하는타사참조에대한링크일수있습니다. 알림메시지를위한다음매크로에는함수 **firstnotnull** 이포함됩니다.
`${ firstnotnull(device.TEL_NUMBER,device.serialNumber) }` 장치는차단되었습니다...
- 사용자지정매크로 (사용자가정의하는속성) 의접두사는 `${ custom }` 입니다. 접두사는생략할수있습니다.

다음은정책의텍스트필드에사용자이름값을채우는널리사용되는매크로 `${ user.username }` 의예제입니다. 이매크로는다수의사용자가사용하는 Exchange ActiveSync 프로필및기타프로필을구성할때유용합니다. 다음예제에서는 Exchange 정책에서매크로를사용하는방법을보여줍니다. 사용자에대한매크로는 `${ user.username }` 입니다. 전자메일주소에대한매크로는 `${ user.mail }` 입니다.

다음예제에서는인증서서명요청에매크로를사용하는방법을보여줍니다. 주체이름에대한매크로는 **CN=\$user.username**입니다. 주체대체이름의 값에대한매크로는 **\$user.userprincipalname**입니다.

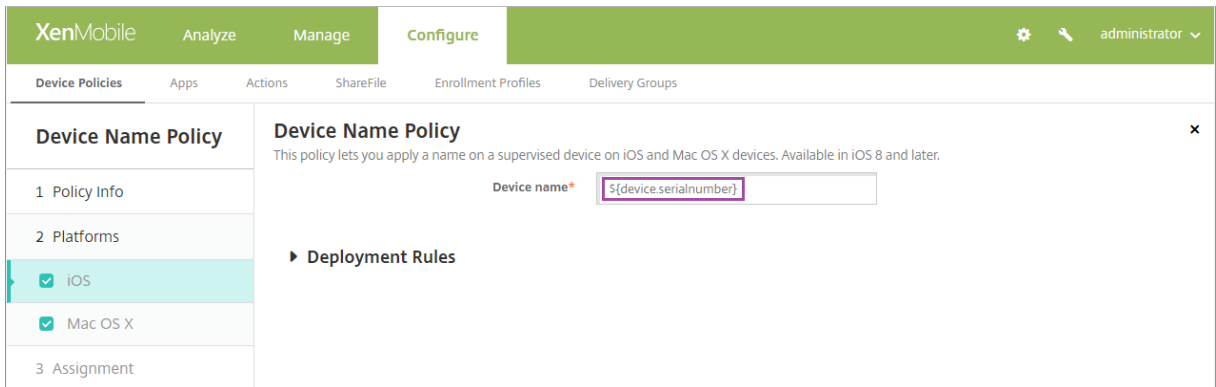
다음예제에서는알림템플릿에서매크로를사용하는방법을보여줍니다. 예제템플릿은 HDX 응용프로그램이규정을준수하지않는장치때문에차단되었을때사용자에게보내는메시지를정의합니다. 메시지에대한매크로는다음과같습니다.

Device $\{ \text{firstnotnull}(\text{device.TEL_NUMBER}, \text{device.serialNumber}) \}$ no longer complies with the device policy and HDX applications will be blocked.



알림에 사용되는 매크로에 대한 더 많은 예제를 보려면 **설정 > 알림 템플릿**으로 이동하고 사전 정의된 템플릿을 선택한 다음 **편집**을 클릭하십시오.

다음 예제에서는 장치 이름 장치 정책의 매크로를 보여줍니다. 매크로, 매크로 조합 또는 매크로와 텍스트 조합을 입력하여 각 장치에 고유한 이름을 지정할 수 있습니다. 예를 들어 `${ device.serialnumber }` 를 사용하여 장치 이름을 각 장치의 일련번호로 설정합니다. 장치 이름에 사용자 이름을 포함하려면 `${ device.serialnumber } ${ user.username }` 을 사용합니다. 장치 이름 장치 정책은 감독되는 iOS 및 macOS 장치에서 작동합니다.



기본 알림 템플릿에 대한 매크로

기본 알림 템플릿에서 사용할 수 있는 매크로는 다음과 같습니다.

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`

- `${ enrollment.url }`
- `${ enrollment.urls }`
- `${ enrollment.ios.url }`
- `${ enrollment.macos.url }`
- `${ enrollment.android.url }`
- `${ enrollment.ios.platform }`
- `${ enrollment.macos.platform }`
- `${ enrollment.android.platform }`
- `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${ firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${ outofcompliance.reason(smg_block)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

특정정책에대한매크로

장치이름장치정책 (iOS 및 macOS 용) 의경우 장치이름에다음매크로를사용할수있습니다.

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

웹클립장치정책의경우 **URL** 에다음매크로를사용할수있습니다.

- `${ webas-url }`

Samsung MDM 라이선스키장치정책의경우 **ELM** 라이선스키에다음매크로를사용할수있습니다.

- `${ elm.license.key }`

기본제공장치속성을가져오는매크로

표시이름	매크로
장치 ID	<code>\$device.id</code>

표시이름	매크로
장치 IMEI	<code>\$device.imei</code>
OS 제품군	<code>\$device.OSFamily</code>
일련번호	<code>\$device.serialNumber</code>

모든장치속성에대한매크로

다음목록에는표시이름, 웹요소및매크로가나와있습니다.

계정이일시중단되었습니까?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- `#{device.GOOGLE_AW_DIRECTORY_SUSPENDED}`

활성화잠금바이패스코드

- ACTIVATION_LOCK_BYPASS_CODE
- `#{device.ACTIVATION_LOCK_BYPASS_CODE}`

활성화잠금이사용됨

- ACTIVATION_LOCK_ENABLED
- `#{device.ACTIVATION_LOCK_ENABLED}`

활성 iTunes 계정

- ACTIVE_ITUNES
- `#{device.ACTIVE_ITUNES}`

MSP 에알려진 ActiveSync 장치

- AS_DEVICE_KNOWN_BY_ZMSP
- `#{device.AS_DEVICE_KNOWN_BY_ZMSP}`

ActiveSync ID

- EXCHANGE_ACTIVASYNC_ID
- `#{device.EXCHANGE_ACTIVASYNC_ID}`

관리자사용안함

- ADMIN_DISABLED
- `#{device.ADMIN_DISABLED}`

AIK 가있습니까?

- WINDOWS_HAS_AIK_PRESENT
- `#{device.WINDOWS_HAS_AIK_PRESENT}`

Amazon MDM API 사용가능

- AMAZON_MDM
- \${device.AMAZON_MDM}

Android Enterprise 장치 ID

- GOOGLE_AW_DEVICE_ID
- \${device.GOOGLE_AW_DEVICE_ID}

Android Enterprise 에서활성화된장치?

- GOOGLE_AW_ENABLED_DEVICE
- \${device.GOOGLE_AW_ENABLED_DEVICE}

Android Enterprise 설치유형

- GOOGLE_AW_INSTALL_TYPE
- \${device.GOOGLE_AW_INSTALL_TYPE}

스파이웨어방지프로그램서명상태

- ANTI_SPYWARE_SIGNATURE_STATUS
- \${device.ANTI_SPYWARE_SIGNATURE_STATUS}

스파이웨어방지프로그램상태

- ANTI_SPYWARE_STATUS
- \${device.ANTI_SPYWARE_STATUS}

바이러스백신서명상태

- ANTI_VIRUS_SIGNATURE_STATUS
- \${device.ANTI_VIRUS_SIGNATURE_STATUS}

바이러스백신상태

- ANTI_VIRUS_STATUS
- \${device.ANTI_VIRUS_STATUS}

ASM DEP 활성화잠금바이패스코드

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- \${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}

ASM DEP 에스크로키

- DEP_ESCROW_KEY
- \${device.DEP_ESCROW_KEY}

자산태그

- ASSET_TAG

- `#{device.ASSET_TAG}`

소프트웨어업데이트자동확인

- `AutoCheckEnabled`
- `#{device.AutoCheckEnabled}`

백그라운드에서소프트웨어업데이트자동다운로드

- `BackgroundDownloadEnabled`
- `#{device.BackgroundDownloadEnabled}`

앱업데이트자동설치

- `AutomaticAppInstallationEnabled`
- `#{device.AutomaticAppInstallationEnabled}`

OS 업데이트자동설치

- `AutomaticOSInstallationEnabled`
- `#{device.AutomaticOSInstallationEnabled}`

보안업데이트자동설치

- `AutomaticSecurityUpdatesEnabled`
- `#{device.AutomaticSecurityUpdatesEnabled}`

자동업데이트상태

- `AUTOUPDATE_STATUS`
- `#{device.AUTOUPDATE_STATUS}`

사용가능한 RAM

- `MEMORY_AVAILABLE`
- `#{device.MEMORY_AVAILABLE}`

사용가능한소프트웨어업데이트

- `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- `#{device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}`

사용가능한스토리지공간

- `FREEDISK`
- `#{device.FREEDISK}`

백업배터리

- `BACKUP_BATTERY_PERCENT`
- `#{device.BACKUP_BATTERY_PERCENT}`

기저대역펌웨어버전

- MODEM_FIRMWARE_VERSION
- \${device.MODEM_FIRMWARE_VERSION}

배터리충전

- BATTERY_CHARGING_STATUS
- \${device.BATTERY_CHARGING_STATUS}

배터리충전

- BATTERY_CHARGING
- \${device.BATTERY_CHARGING}

배터리잔량

- BATTERY_ESTIMATED_CHARGE_REMAINING
- \${device.BATTERY_ESTIMATED_CHARGE_REMAINING}

배터리런타임

- BATTERY_RUNTIME
- \${device.BATTERY_RUNTIME}

배터리상태

- BATTERY_STATUS
- \${device.BATTERY_STATUS}

MS 에알려진 BES 장치

- BES_DEVICE_KNOWN_BY_ZMSP
- \${device.BES_DEVICE_KNOWN_BY_ZMSP}

BES PIN

- BES_PIN
- \${device.BES_PIN}

BES 서버에이전트 ID

- AGENT_ID
- \${device.AGENT_ID}

BES 서버이름

- BES_SERVER
- \${device.BES_SERVER}

BES 서버버전

- BES_VERSION
- \${device.BES_VERSION}

BIOS 정보

- BIOS_INFO
- \${device.BIOS_INFO}

BitLocker 상태

- WINDOWS_HAS_BIT_LOCKER_STATUS
- \${device.WINDOWS_HAS_BIT_LOCKER_STATUS}

Bluetooth MAC 주소

- BLUETOOTH_MAC
- \${device.BLUETOOTH_MAC}

부팅디버깅이사용됩니까?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- \${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}

부팅관리자수정목록버전

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- \${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}

이동통신사업자코드

- CARRIER_CODE
- \${device.CARRIER_CODE}

이동통신사업자설정버전

- CARRIER_SETTINGS_VERSION
- \${device.CARRIER_SETTINGS_VERSION}

카탈로그 URL

- CatalogURL
- \${device.CatalogURL}

셀룰러고도

- GPS_ALTITUDE_FROM_CELLULAR
- \${device.GPS_ALTITUDE_FROM_CELLULAR}

셀룰러코스

- GPS_COURSE_FROM_CELLULAR
- \${device.GPS_COURSE_FROM_CELLULAR}

셀룰러수평정확도

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

- `device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`

셀룰러위도

- `GPS_LATITUDE_FROM_CELLULAR`
- `device.GPS_LATITUDE_FROM_CELLULAR`

셀룰러경도

- `GPS_LONGITUDE_FROM_CELLULAR`
- `device.GPS_LONGITUDE_FROM_CELLULAR`

셀룰러속도

- `GPS_SPEED_FROM_CELLULAR`
- `device.GPS_SPEED_FROM_CELLULAR`

셀룰러기술

- `CELLULAR_TECHNOLOGY`
- `device.CELLULAR_TECHNOLOGY`

셀룰러타임스탬프

- `GPS_TIMESTAMP_FROM_CELLULAR`
- `device.GPS_TIMESTAMP_FROM_CELLULAR`

셀룰러수직정확도

- `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- `device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR`

다음로그인시암호를변경하시겠습니까?

- `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- `device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`

클라이언트장치 ID

- `CLIENT_DEVICE_ID`
- `device.CLIENT_DEVICE_ID`

클라우드백업이활성화됨

- `CLOUD_BACKUP_ENABLED`
- `device.CLOUD_BACKUP_ENABLED`

코드무결성이사용됩니까?

- `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- `device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED`

코드무결성수정목록버전

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- \${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION}

색

- COLOR
- \${device.COLOR}

CPU 클럭속도

- CPU_CLOCK_SPEED
- \${device.CPU_CLOCK_SPEED}

CPU 유형

- CPU_TYPE
- \${device.CPU_TYPE}

만든시간

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- \${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}

중요소프트웨어업데이트

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- \${device.AVAILABLE_OS_UPDATE_IS_CRITICAL}

현재이동통신사업자네트워크

- 이동통신사업자
- \${device.CARRIER}

현재모바일국가코드

- CURRENT_MCC
- \${device.CURRENT_MCC}

현재모바일네트워크코드

- CURRENT_MNC
- \${device.CURRENT_MNC}

데이터로밍허용

- DATA_ROAMING_ENABLED
- \${device.DATA_ROAMING_ENABLED}

마지막 iCloud 백업날짜

- LAST_CLOUD_BACKUP_DATE
- \${device.LAST_CLOUD_BACKUP_DATE}

기본카탈로그

- IsDefaultCatalog
- \${device.IsDefaultCatalog}

DEP 계정이름

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- \${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}

DEP 정책

- WINDOWS_HAS_DEP_POLICY
- \${device.WINDOWS_HAS_DEP_POLICY}

DEP 프로필이할당됨

- PROFILE_ASSIGN_TIME
- \${device.PROFILE_ASSIGN_TIME}

DEP 프로필이푸시됨

- PROFILE_PUSH_TIME
- \${device.PROFILE_PUSH_TIME}

DEP 프로필이제거됨

- PROFILE_REMOVE_TIME
- \${device.PROFILE_REMOVE_TIME}

DEP 등록자

- DEVICE_ASSIGNED_BY
- \${device.DEVICE_ASSIGNED_BY}

DEP 등록날짜

- DEVICE_ASSIGNED_DATE
- \${device.DEVICE_ASSIGNED_DATE}

설명

- DESCRIPTION
- \${device.DESCRPTION}

장치모델

- SYSTEM_OEM
- \${device.SYSTEM_OEM}

장치이름

- DEVICE_NAME

- `device.DEVICE_NAME`

장치유형

- `DEVICE_TYPE`
- `device.DEVICE_TYPE`

방해금지가활성화됨

- `DO_NOT_DISTURB`
- `device.DO_NOT_DISTURB`

ELAM 드라이버가로드되었습니까?

- `WINDOWS_HAS_ELAM_DRIVER_LOADED`
- `device.WINDOWS_HAS_ELAM_DRIVER_LOADED`

암호화규정준수

- `ENCRYPTION_COMPLIANCE`
- `device.ENCRYPTION_COMPLIANCE`

ENROLLMENT_KEY_GENERATION_DATE

- `ENROLLMENT_KEY_GENERATION_DATE`
- `device.ENROLLMENT_KEY_GENERATION_DATE`

엔터프라이즈 ID

- `ENTERPRISEID`
- `device.ENTERPRISEID`

외부스토리지 1: 사용가능한공간

- `EXTERNAL_STORAGE1_FREE_SPACE`
- `device.EXTERNAL_STORAGE1_FREE_SPACE`

외부스토리지 1: 이름

- `EXTERNAL_STORAGE1_NAME`
- `device.EXTERNAL_STORAGE1_NAME`

외부스토리지 1: 총공간

- `EXTERNAL_STORAGE1_TOTAL_SPACE`
- `device.EXTERNAL_STORAGE1_TOTAL_SPACE`

외부스토리지 2: 사용가능한공간

- `EXTERNAL_STORAGE2_FREE_SPACE`
- `device.EXTERNAL_STORAGE2_FREE_SPACE`

외부스토리지 2: 이름

- EXTERNAL_STORAGE2_NAME
- \${device.EXTERNAL_STORAGE2_NAME}

외부스토리지 2: 총공간

- EXTERNAL_STORAGE2_TOTAL_SPACE
- \${device.EXTERNAL_STORAGE2_TOTAL_SPACE}

외부스토리지가암호화됨

- EXTERNAL_ENCRYPTION
- \${device.EXTERNAL_ENCRYPTION}

FileVault 사용

- IS_FILEVAULT_ENABLED
- \${device.IS_FILEVAULT_ENABLED}

방화벽상태

- DEVICE_FIREWALL_STATUS
- \${device.DEVICE_FIREWALL_STATUS}

방화벽상태

- FIREWALL_STATUS
- \${device.FIREWALL_STATUS}

펌웨어버전

- FIRMWARE_VERSION
- \${device.FIRMWARE_VERSION}

첫번째동기화

- ZMSP_FIRST_SYNC
- \${device.ZMSP_FIRST_SYNC}

Google Directory 별칭

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- \${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}

Google Directory 패밀리이름

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- \${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}

Google Directory 이름

- GOOGLE_AW_DIRECTORY_NAME
- \${device.GOOGLE_AW_DIRECTORY_NAME}

Google Directory 기본전자메일

- GOOGLE_AW_DIRECTORY_PRIMARY
- \${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google Directory 사용자 ID

- GOOGLE_AW_DIRECTORY_USER_ID
- \${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS 고도

- GPS_ALTITUDE_FROM_GPS
- \${device.GPS_ALTITUDE_FROM_GPS}

GPS 코스

- GPS_COURSE_FROM_GPS
- \${device.GPS_COURSE_FROM_GPS}

GPS 수평정확도

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- \${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS}

GPS 위도

- GPS_LATITUDE_FROM_GPS
- \${device.GPS_LATITUDE_FROM_GPS}

GPS 경도

- GPS_LONGITUDE_FROM_GPS
- \${device.GPS_LONGITUDE_FROM_GPS}

GPS 속도

- GPS_SPEED_FROM_GPS
- \${device.GPS_SPEED_FROM_GPS}

GPS 타임스탬프

- GPS_TIMESTAMP_FROM_GPS
- \${device.GPS_TIMESTAMP_FROM_GPS}

GPS 수직정확도

- GPS_VERTICAL_ACCURACY_FROM_GPS
- \${device.GPS_VERTICAL_ACCURACY_FROM_GPS}

하드웨어장치 ID

- HW_DEVICE_ID

- `device.HW_DEVICE_ID`

하드웨어암호화기능

- `HARDWARE_ENCRYPTION_CAPS`
- `device.HARDWARE_ENCRYPTION_CAPS`

HAS_CONTAINER

- `HAS_CONTAINER`
- `device.HAS_CONTAINER`

현재로그온되어있는 iTunes 스토어계정의해시

- `ITUNES_STORE_ACCOUNT_HASH`
- `device.ITUNES_STORE_ACCOUNT_HASH`

홈이동통신사업자네트워크

- `SIM_CARRIER_NETWORK`
- `device.SIM_CARRIER_NETWORK`

홈바일국가코드

- `SIM_MCC`
- `device.SIM_MCC`

홈바일네트워크코드

- `SIM_MNC`
- `device.SIM_MNC`

HTC API 버전

- `HTC_MDM_VERSION`
- `device.HTC_MDM_VERSION`

HTC MDM API 사용가능

- `HTC_MDM`
- `device.HTC_MDM`

ICCID

- `ICCID`
- `device.ICCID`

ID

- `AS_DEVICE_IDENTITY`
- `device.AS_DEVICE_IDENTITY`

IMEI/MEID 번호

- IMEI
- \${device.IMEI}

IMSI

- SIM_ID
- \${device.SIM_ID}

내부스토리지가암호화됨

- LOCAL_ENCRYPTION
- \${device.LOCAL_ENCRYPTION}

IP 위치

- IP_LOCATION
- \${device.IP_LOCATION}

IPV4 주소

- IP_ADDRESSV4
- \${device.IP_ADDRESSV4}

IPV6 주소

- IP_ADDRESSV6
- \${device.IP_ADDRESSV6}

실행시간

- WINDOWS_HAS_ISSUED_AT
- \${device.WINDOWS_HAS_ISSUED_AT}

탈옥/루팅

- ROOT_ACCESS
- \${device.ROOT_ACCESS}

커널디버깅이사용됩니까?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- \${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}

키오스크모드

- IS_KIOSK
- \${device.IS_KIOSK}

마지막으로알려진 IP 주소

- LAST_IP_ADDR
- \${device.LAST_IP_ADDR}

마지막정책업데이트시간

- LAST_POLICY_UPDATE_TIME
- \${device.LAST_POLICY_UPDATE_TIME}

마지막검사날짜

- PreviousScanDate
- \${device.PreviousScanDate}

마지막검사결과

- PreviousScanResult
- \${device.PreviousScanResult}

마지막으로예약된소프트웨어업데이트

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- \${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}

마지막으로예약된소프트웨어업데이트실패메시지

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- \${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}

마지막으로예약된소프트웨어업데이트상태

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- \${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}

마지막동기화

- ZMSP_LAST_SYNC
- \${device.ZMSP_LAST_SYNC}

로케이터서비스사용

- DEVICE_LOCATOR
- \${device.DEVICE_LOCATOR}

MAC 주소

- MAC_ADDRESS
- \${device.MAC_ADDRESS}

MAC 주소네트워크연결

- MAC_NETWORK_CONNECTION
- \${device.MAC_NETWORK_CONNECTION}

MAC 주소유형

- MAC_ADDRESS_TYPE

- \${device.MAC_ADDRESS_TYPE}

사서함설정

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- \${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP}

기본배터리

- MAIN_BATTERY_PERCENT
- \${device.MAIN_BATTERY_PERCENT}

MDM 분실모드활성화

- IS_MDM_LOST_MODE_ENABLED
- \${device.IS_MDM_LOST_MODE_ENABLED}

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- \${device.MDX_SHARED_ENCRYPTION_KEY}

MEID

- MEID
- \${device.MEID}

휴대폰번호

- TEL_NUMBER
- \${device.TEL_NUMBER}

모델 ID

- MODEL_ID
- \${device.MODEL_ID}

모델번호

- MODEL_NUMBER
- \${device.MODEL_NUMBER}

네트워크어댑터유형

- NETWORK_ADAPTER_TYPE
- \${device.NETWORK_ADAPTER_TYPE}

NitroDesk TouchDown 이설치됨

- TOUCHDOWN_FIND
- \${device.TOUCHDOWN_FIND}

NitroDesk TouchDown 이 MDM 을통해라이센스부여됨

- TOUCHDOWN_LICENSED_VIA_MDM
- \${device.TOUCHDOWN_LICENSED_VIA_MDM}

운영체제빌드

- SYSTEM_OS_BUILD
- \${device.SYSTEM_OS_BUILD}

운영체제버전

- OS_EDITION
- \${device.OS_EDITION}

운영체제언어 (로캘)

- SYSTEM_LANGUAGE
- \${device.SYSTEM_LANGUAGE}

운영체제버전

- SYSTEM_OS_VERSION
- \${device.SYSTEM_OS_VERSION}

조직주소

- ORGANIZATION_ADDRESS
- \${device.ORGANIZATION_ADDRESS}

조직전자메일

- ORGANIZATION_EMAIL
- \${device.ORGANIZATION_EMAIL}

조직매직

- ORGANIZATION_MAGIC
- \${device.ORGANIZATION_MAGIC}

조직이름

- ORGANIZATION_NAME
- \${device.ORGANIZATION_NAME}

조직전화번호

- ORGANIZATION_PHONE
- \${device.ORGANIZATION_PHONE}

규정위반

- OUT_OF_COMPLIANCE
- \${device.OUT_OF_COMPLIANCE}

소유자

- CORPORATE_OWNED
- \${device.CORPORATE_OWNED}

암호규정준수

- PASSCODE_IS_COMPLIANT
- \${device.PASSCODE_IS_COMPLIANT}

구성을준수하는암호

- PASSCODE_IS_COMPLIANT_WITH_CFG
- \${device.PASSCODE_IS_COMPLIANT_WITH_CFG}

현재암호

- PASSCODE_PRESENT
- \${device.PASSCODE_PRESENT}

PCRO

- WINDOWS_HAS_PCRO
- \${device.WINDOWS_HAS_PCRO}

경계위반

- GPS_PERIMETER_BREACH
- \${device.GPS_PERIMETER_BREACH}

정기적인확인

- PerformPeriodicCheck
- \${device.PerformPeriodicCheck}

개인핫스팟이활성화됨

- PERSONAL_HOTSPOT_ENABLED
- \${device.PERSONAL_HOTSPOT_ENABLED}

지오펜스의 PIN 코드

- PIN_CODE_FOR_GEO_FENCE
- \${device.PIN_CODE_FOR_GEO_FENCE}

플랫폼

- SYSTEM_PLATFORM
- \${device.SYSTEM_PLATFORM}

플랫폼 API 수준

- API_LEVEL

- \${device.API_LEVEL}

정책이름

- POLICY_NAME
- \${device.POLICY_NAME}

기본전화번호

- IDENTITY1_PHONENUMBER
- \${device.IDENTITY1_PHONENUMBER}

기본 SIM 이동통신사업자운영자

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- \${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}

기본 SIM ICCID

- IDENTITY1_ICCID
- \${device.IDENTITY1_ICCID}

기본 SIM 카드 IMEI

- IDENTITY1_IMEI
- \${device.IDENTITY1_IMEI}

기본 SIM 카드 IMSI

- IDENTITY1_IMSI
- \${device.IDENTITY1_IMSI}

기본 SIM 카드로밍

- IDENTITY1_ROAMING
- \${device.IDENTITY1_ROAMING}

기본 SIM 로밍규정준수

- IDENTITY1_ROAMING_COMPLIANCE
- \${device.IDENTITY1_ROAMING_COMPLIANCE}

제품이름

- PRODUCT_NAME
- \${device.PRODUCT_NAME}

게시자장치 ID

- PUBLISHER_DEVICE_ID
- \${device.PUBLISHER_DEVICE_ID}

재설정횟수

- WINDOWS_HAS_RESET_COUNT
- \${device.WINDOWS_HAS_RESET_COUNT}

다시시작횟수

- WINDOWS_HAS_RESTART_COUNT
- \${device.WINDOWS_HAS_RESTART_COUNT}

안전모드가사용됩니까?

- WINDOWS_HAS_SAFE_MODE
- \${device.WINDOWS_HAS_SAFE_MODE}

Samsung KNOX API 사용가능

- SAMSUNG_KNOX
- \${device.SAMSUNG_KNOX}

Samsung KNOX API 버전

- SAMSUNG_KNOX_VERSION
- \${device.SAMSUNG_KNOX_VERSION}

Samsung KNOX 증명

- SAMSUNG_KNOX_ATTESTED
- \${device.SAMSUNG_KNOX_ATTESTED}

Samsung KNOX 증명업데이트날짜

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- \${device.SAMSUNG_KNOX_ATT_UPDATED_TIME}

Samsung SAFE API 사용가능

- SAMSUNG_MDM
- \${device.SAMSUNG_MDM}

Samsung SAFE API 버전

- SAMSUNG_MDM_VERSION
- \${device.SAMSUNG_MDM_VERSION}

SBCP 해시

- WINDOWS_HAS_SBCP_HASH
- \${device.WINDOWS_HAS_SBCP_HASH}

화면: 높이

- SCREEN_HEIGHT
- \${device.SCREEN_HEIGHT}

화면: 색상수

- SCREEN_NB_COLORS
- \${device.SCREEN_NB_COLORS}

화면: 크기

- SCREEN_SIZE
- \${device.SCREEN_SIZE}

화면: 너비

- SCREEN_WIDTH
- \${device.SCREEN_WIDTH}

화면: X 축해상도

- SCREEN_XDPI
- \${device.SCREEN_XDPI}

화면: Y 축해상도

- SCREEN_YDPI
- \${device.SCREEN_YDPI}

보조전화번호

- IDENTITY2_PHONENUMBER
- \${device.IDENTITY2_PHONENUMBER}

보조 SIM 이동통신사업자운영자

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- \${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}

보조 SIM ICCID

- IDENTITY2_ICCID
- \${device.IDENTITY2_ICCID}

보조 SIM 카드 IMEI

- IDENTITY2_IMEI
- \${device.IDENTITY2_IMEI}

보조 SIM 카드 IMSI

- IDENTITY2_IMSI
- \${device.IDENTITY2_IMSI}

보조 SIM 카드로밍

- IDENTITY2_ROAMING

- `device.IDENTITY2_ROAMING`

보조 SIM 로밍규정준수

- `IDENTITY2_ROAMING_COMPLIANCE`
- `device.IDENTITY2_ROAMING_COMPLIANCE`

보안부팅이사용됩니까?

- `WINDOWS_HAS_SECURE_BOOT_ENABLED`
- `device.WINDOWS_HAS_SECURE_BOOT_ENABLED`

보안부팅상태

- `SECURE_BOOT_STATE`
- `device.SECURE_BOOT_STATE`

SecureContainer 사용

- `DLP_ACTIVE`
- `device.DLP_ACTIVE`

보안패치수준

- `SYSTEM_SECURITY_PATCH_LEVEL`
- `device.SYSTEM_SECURITY_PATCH_LEVEL`

일련번호

- `SERIAL_NUMBER`
- `device.SERIAL_NUMBER`

SMS 지원

- `IS_SMS_CAPABLE`
- `device.IS_SMS_CAPABLE`

Sony Enterprise API 사용가능

- `SONY_MDM`
- `device.SONY_MDM`

Sony Enterprise API 버전

- `SONY_MDM_VERSION`
- `device.SONY_MDM_VERSION`

감독됨

- `SUPERVISED`
- `device.SUPERVISED`

일시중단이유

- GOOGLE_AW_DIRECTORY_SUSPENSION_REASON
- \${device.GOOGLE_AW_DIRECTORY_SUSPENSION_REASON}

무단변경된상태

- TAMPERED_STATUS
- \${device.TAMPERED_STATUS}

약관

- TERMS_AND_CONDITIONS
- \${device.TERMS_AND_CONDITIONS}

약관에동의하십니까?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- \${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}

테스트서명이사용됩니까?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- \${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}

총 RAM

- MEMORY
- \${device.MEMORY}

총스토리지공간

- TOTAL_DISK_SPACE
- \${device.TOTAL_DISK_SPACE}

TPM 버전

- TPM_VERSION
- \${device.TPM_VERSION}

UDID

- UDID
- \${device.UDID}

사용자계정제어상태

- UAC_STATUS
- \${device.UAC_STATUS}

사용자에이전트

- USER_AGENT
- \${device.USER_AGENT}

사용자정의 #1

- USER_DEFINED_1
- \${device.USER_DEFINED_1}

사용자정의 #2

- USER_DEFINED_2
- \${device.USER_DEFINED_2}

사용자정의 #3

- USER_DEFINED_3
- \${device.USER_DEFINED_3}

사용자언어 (로캘)

- USER_LANGUAGE
- \${device.USER_LANGUAGE}

공급업체

- VENDOR
- \${device.VENDOR}

음성지원

- IS_VOICE_CAPABLE
- \${device.IS_VOICE_CAPABLE}

음성로밍허용

- VOICE_ROAMING_ENABLED
- \${device.VOICE_ROAMING_ENABLED}

VSM 이사용됩니까?

- WINDOWS_HAS_VSM_ENABLED
- \${device.WINDOWS_HAS_VSM_ENABLED}

WiFi MAC 주소

- WIFI_MAC
- \${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- \${device.WINDOWS_ENROLLMENT_KEY}

WinPE 가사용됩니까?

- WINDOWS_HAS_WINPE

- `device.WINDOWS_HAS_WINPE`

WNS 알림상태

- `PROPERTY_WNS_PUSH_STATUS`
- `device.PROPERTY_WNS_PUSH_STATUS`

WNS 알림 URL

- `PROPERTY_WNS_PUSH_URL`
- `device.PROPERTY_WNS_PUSH_URL`

WNS 알림 URL 만료날짜

- `PROPERTY_WNS_PUSH_URL_EXPIRY`
- `device.PROPERTY_WNS_PUSH_URL_EXPIRY`

XenMobile 에이전트 ID

- `ENROLLMENT_AGENT_ID`
- `device.ENROLLMENT_AGENT_ID`

XenMobile 에이전트수정

- `EW_REVISION`
- `device.EW_REVISION`

XenMobile 에이전트버전

- `EW_VERSION`
- `device.EW_VERSION`

Zebra API 사용가능

- `ZEBRA_MDM`
- `device.ZEBRA_MDM`

Zebra MXMF 버전

- `ZEBRA_MDM_VERSION`
- `device.ZEBRA_MDM_VERSION`

Zebra 패치버전

- `ZEBRA_PATCH_VERSION`
- `device.ZEBRA_PATCH_VERSION`

기본제공사용자속성을가져오는매크로

표시이름	매크로
domainname(도메인이름또는기본도메인)	<code>\${ user.domainname }</code>
loginname(사용자이름 + 도메인이름)	<code>\${ user.loginname }</code>
username(도메인이있는경우도메인을제외한로그인이름)	<code>\${ user.username }</code>

모든사용자속성에대한매크로

표시이름	웹요소	매크로
Active Directory 실패한로그온시도횟수	badpwdcount	<code>\${ user.badpwdcount }</code>
ActiveSync 사용자전자메일	asuseremail	<code>\${ user.asuseremail }</code>
ASM 데이터원본	asmpersonsource	<code>\${ user.asmpersonsource }</code>
ASM DEP 계정이름	asmdepaccount	<code>\${ user.asmdepaccount }</code>
ASM 관리되는 Apple ID	asmpersonmanagedappleid	<code>\${ user.asmpersonmanagedappleid }</code>
ASM 암호유형	asmpersonpasscodetype	<code>\${ user.asmpersonpasscodetype }</code>
ASM 사용자 ID	asmpersonid	<code>\${ user.asmpersonid }</code>
ASM 사용자상태	asmpersonstatus	<code>\${ user.asmpersonstatus }</code>
ASM 사용자직위	asmpersontitle	<code>\${ user.asmpersontitle }</code>
ASM 사용자고유 ID	asmpersonuniqueid	<code>\${ user.asmpersonuniqueid }</code>
ASM 소스시스템 ID	asmpersonsourcesystemid	<code>\${ user.asmpersonsourcesystemid }</code>
ASM 학생의학년	asmpersongrade	<code>\${ user.asmpersongrade }</code>

표시이름	웹요소	매크로
BES 사용자전자메일	besuseremail	<code>\${ user.besuseremail }</code>
회사	company	<code>\${ user.company }</code>
회사이름	companyname	<code>\${ user.companyname }</code>
국가	c	<code>\${ user.c }</code>
부서	department	<code>\${ user.department }</code>
설명	description	<code>\${ user.description }</code>
사용하지않는사용자	disableduser	<code>\${ user.disableduser }</code>
표시이름	displayname	<code>\${ user.displayname }</code>
고유이름	distinguishedname	<code>\${ user.distinguishedname }</code>
도메인이름	domainname	<code>\${ user.domainname }</code>
전자메일	mail	<code>\${ user.mail }</code>
이름	givenname	<code>\${ user.givenname }</code>
집주소	homestreetaddress	<code>\${ user.homestreetaddress }</code>
집구/군/시	homecity	<code>\${ user.homecity }</code>
집국가	homecountry	<code>\${ user.homecountry }</code>
집팩스	homefax	<code>\${ user.homefax }</code>
집전화	homephone	<code>\${ user.homephone }</code>
집시/도/지역	homestate	<code>\${ user.homestate }</code>
집우편번호	homezip	<code>\${ user.homezip }</code>
IP 전화	iphone	<code>\${ user.iphone }</code>
중간이니셜	middleinitial	<code>\${ user.middleinitial }</code>
중간이름	middlename	<code>\${ user.middlename }</code>
모바일	mobile	<code>\${ user.mobile }</code>
이름	cn	<code>\${ user.cn }</code>

표시이름	웹요소	매크로
사무실주소	physicaldeliveryofficename	<code>\${ user. physicaldeliveryofficename }</code>
사무실구/군/시	l	<code>\${ user.l }</code>
사무실팩스번호	facsimiletelephonenumber	<code>\${ user. facsimiletelephonenumber }</code>
사무실시/도	st	<code>\${ user.st }</code>
사무실세부주소	officestreetaddress	<code>\${ user. officestreetaddress }</code>
사무실전화번호	telephonenumber	<code>\${ user. telephonenumber }</code>
사무실우편번호	postalcode	<code>\${ user.postalcode }</code>
사서함	postofficebox	<code>\${ user.postofficebox }</code>
호출기	pager	<code>\${ user.pager }</code>
주그룹 ID	primarygroupid	<code>\${ user.primarygroupid }</code>
SAM 계정	samaccountname	<code>\${ user.samaccountname }</code>
세부주소	streetaddress	<code>\${ user.streetaddress }</code>
성	sn	<code>\${ user.sn }</code>
직위	title	<code>\${ user.title }</code>
사용자로그온이름	userprincipalname	<code>\${ user. userprincipalname }</code>

자동화된동작

January 6, 2020

XenMobile 에서이벤트, 사용자또는장치속성또는사용자장치의앱존재에대한반응을프로그래밍하는자동화된동작을만들수있습니다. 자동화된동작을만드는경우 XenMobile 에연결하는사용자장치에서수행되는동작은동작에정의된트리거에따라결정됩니다.

다. 이벤트가 트리거되면 더 심각한 동작이 수행되기 전에 문제를 수정하도록 사용자에게 알림을 보낼 수 있습니다.

예를 들어 이전에 블랙리스트에 추가한 앱 (예: “Words with Friends”) 을 검색하려고 합니다. 이 경우 장치에서 “Words with Friends” 가 검색될 때 사용자 장치를 규정 위반으로 설정하는 트리거를 지정할 수 있습니다. 이 동작은 이어서 사용자에게 앱을 제거하여 장치를 규정 준수 상태로 되돌리라는 알림을 보냅니다. 또한 사용자가 준수할 때까지 대기할 기간에 대한 시간 제한을 설정할 수 있습니다. 이 시간 제한이 지나면 정의된 동작 (예: 장치를 선택적으로 초기화) 이 수행됩니다.

사용자 장치가 규정을 위반한 후 사용자가 장치를 수정하면 관리자는 장치를 규정 준수 상태로 재설정하는 패키지를 배포하도록 정책을 구성해야 합니다.

자동으로 발생하도록 설정하는 효과의 범위는 다음과 같습니다.

- 장치를 전체적으로 또는 선택적으로 초기화
- 장치를 규정 위반으로 설정
- 장치 해지
- 더 심각한 조치가 취해지기 전에 문제를 수정하도록 사용자에게 알림 전송

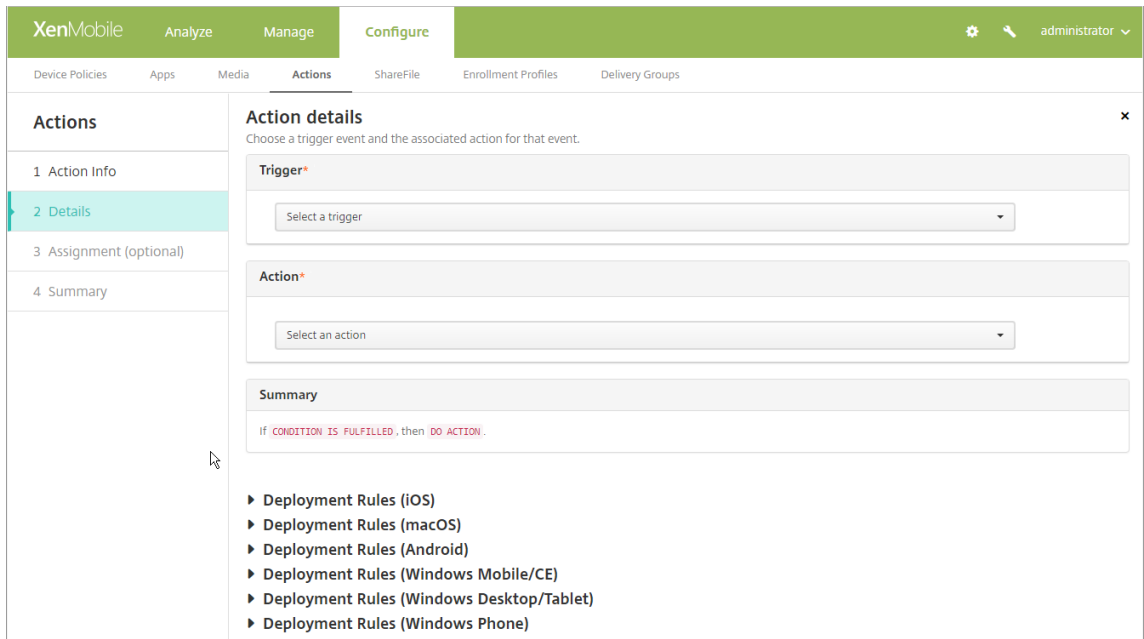
이 문서에서는 자동화 동작을 추가, 편집 및 필터링하는 방법과 MAM 전용 모드에 대한 앱 잠금 및 앱 초기화 동작을 구성하는 방법을 설명합니다.

참고:

사용자에게 알림을 보내려면 XenMobile 이 메시지를 보낼 수 있도록 먼저 SMTP 및 SMS 에 대한 XenMobile 설정에서 알림 서버를 구성해야 합니다. 자세한 내용은 [알림](#) 에서 참조하십시오. 또한 계속하기 전에 사용하려는 모든 알림 템플릿을 설정합니다. 자세한 내용은 [알림 템플릿 만들기 및 업데이트](#) 에서 참조하십시오.

1. XenMobile 콘솔에서 구성 > 동작을 클릭합니다. 동작 페이지가 나타납니다.
2. 동작 페이지에서 다음 중 하나를 수행합니다.
 - 추가를 클릭하여 동작을 추가합니다.
 - 기존 동작을 선택하여 편집하거나 삭제합니다. 사용할 옵션을 클릭합니다.
3. 동작 정보 페이지가 나타납니다.
4. 동작 정보 페이지에서 다음 정보를 입력하거나 수정합니다.
 - 이름: 동작을 고유하게 식별하는 이름을 입력합니다. 이것은 필수 필드입니다.
 - 설명: 동작의 의미를 설명합니다.
5. 다음을 클릭합니다. 동작 세부 정보 페이지가 나타납니다.

다음 예제는 이벤트 트리거를 설정하는 방법을 보여줍니다. 다른 트리거를 선택할 경우 여기에 표시된 것과 다른 옵션이 표시됩니다.



6. 동작세부정보페이지에서다음정보를입력하거나수정합니다.

트리거목록에서이동작에대한이벤트트리거유형을클릭합니다. 각트리거의의미는다음과같습니다.

- 이벤트: 미리정의된이벤트에반응합니다.
- 장치속성: MDM 모드에서수집된장치의장치특성을확인하고반응합니다. 자세한내용은 [장치속성이름맞춤](#)에서참조하십시오.
- 사용자속성: 일반적으로 Active Directory 의사용자특성에반응합니다.
- 설치된앱이름: 설치되는앱에반응합니다. MAM 전용모드에는적용되지않습니다. 장치에서앱인벤토리정책을사용하도록설정해야합니다. 앱인벤토리정책은모든플랫폼에서기본적으로사용하도록설정됩니다. 자세한내용은 [앱인벤토리장치정책](#)에서참조하십시오.

7. 다음목록에서트리거에대한응답을클릭합니다.

8. 동작목록에서트리거조건이충족될때수행할동작을클릭합니다. 알림보내기를제외하고사용자가트리거를야기한문제를해결할수있는시간을선택합니다. 해당시간내에문제가해결되지않으면선택한동작이수행됩니다. 해당작업에대한정의는 [보안동작](#)을참조하십시오.

알림보내기를선택하는경우다음단계를사용하여알림동작을보냅니다.

9. 다음목록에서알림에사용할템플릿을선택합니다. 해당알림유형에대한템플릿이없는경우를제외하고선택한이벤트와관련된알림템플릿이나타납니다. 해당하는템플릿이없는경우에는 “이이벤트유형에대한템플릿이없습니다” 라는메시지와함께템플릿구성메시지가표시됩니다. 설정에서 알림템플릿을사용하여템플릿을만듭니다.

사용자에게알림을보내려면 XenMobile 이메일지를보낼수있도록먼저 SMTP 및 SMS 에대한설정에서알림서버를구성해야합니다. [알림](#)을참조하십시오. 또한계속하기전에사용하려는모든알림템플릿을설정합니다. 알림템플릿설정에대한자세한내용은 [알림템플릿만들기및업데이트](#)를참조하십시오.

템플릿을 선택한 후 알림 메시지 미리 보기를 클릭하여 알림을 미리 볼 수 있습니다.

- 다음 필드에서 동작을 수행하기 전의 지연 시간을 일, 시간 또는 분 단위로 설정합니다. 사용자가 동작을 트리거한 문제를 해결할 때까지 동작을 반복할 간격을 설정합니다.

- 요약에서의 도한 자동화 동작이 만들어졌는지 확인합니다.

- 동작 세부 정보를 구성한 후 각 플랫폼에 대한 배포 규칙을 개별적으로 구성할 수 있습니다. 이렇게 하려면 선택한 각 플랫폼에 대한 13 단계를 완료합니다.
- 배포 규칙을 구성합니다. 배포 규칙 구성에 대한 일반 정보는 [리소스 배포](#)를 참조하십시오.

이제에서:

- 장치소유권은 **BYOD** 여야합니다.
- 장치로컬암호화는 **True** 여야합니다.
- 장치는암호규정을준수해야합니다.
- 장치 MCC(모바일국가코드) 로안도라만지정될수는없습니다.

14. 동작에대한플랫폼배포규칙을구성한후 다음을클릭합니다. 동작할당페이지가나타나면여기에서배달그룹에동작을할당합니다. 이단계는선택사항입니다.

15. 배달그룹선택액에서배달그룹을입력하여찾거나목록에서그룹을선택합니다. 선택한그룹이 애플당을받을배달그룹목록에 나타납니다.

16. 배포일정을확장하고다음설정을구성합니다.

- 배포옆에서 켜짐을클릭하여배포를예약하거나 꺼짐을클릭하여배포를차단합니다. 기본옵션은 켜짐입니다. 꺼짐을 선택하는경우다른옵션은필요하지않습니다.
- 배포일정옆에서 지금또는 나중에를클릭합니다. 기본옵션은 지금입니다.
- 나중에를클릭하는경우달력아이콘을클릭하고배포날짜와시간을선택합니다.
- 배포조건옆에서 모든연결에서를클릭하거나 이전배포가실패한경우에만을클릭합니다. 기본옵션은 모든연결에서입니다.
- 상시연결에대해배포옆에서 켜짐또는 꺼짐을클릭합니다. 기본옵션은 꺼짐입니다.

설정 > 서버속성에서백그라운드배포예약키를구성한경우에만이옵션이적용됩니다. iOS 장치에는상시연결옵션을 사용할수없습니다.

구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은모든플랫폼에적용되지만 상시연결에대해배포를선택한경우 iOS 에는적용되지않습니다.

17. 다음을클릭합니다. 요약페이지가나타나고여기서동작구성을확인할수있습니다.

18. 저장을클릭하여동작을저장합니다.

MAM 전용모드에대한앱잠금및앱초기화동작

XenMobile 콘솔에나열된모든 4 개범주의트리거 (이벤트, 장치속성, 사용자속성및설치된앱이름) 에대한응답으로장치의앱을 초기화하거나잠글수있습니다.

자동앱초기화또는앱잠금을구성하려면

1. XenMobile 콘솔에서 구성 > 동작을클릭합니다.
2. 동작페이지에서 추가를클릭합니다.
3. 동작정보페이지에서동작이름과선택적설명을입력합니다.
4. 동작세부정보페이지에서원하는트리거를선택합니다.

5. 동작에서동작을선택합니다.

이단계에서는다음조건을유의하십시오.

트리거유형이 이벤트이고값이 **Active Directory** 에서사용하지않도록설정된사용자인경우 앱초기화및 앱잠금동작이 표시되지않습니다.

트리거유형이 장치속성이고값이 **MDM** 분실모드활성화인경우다음동작이표시되지않습니다.

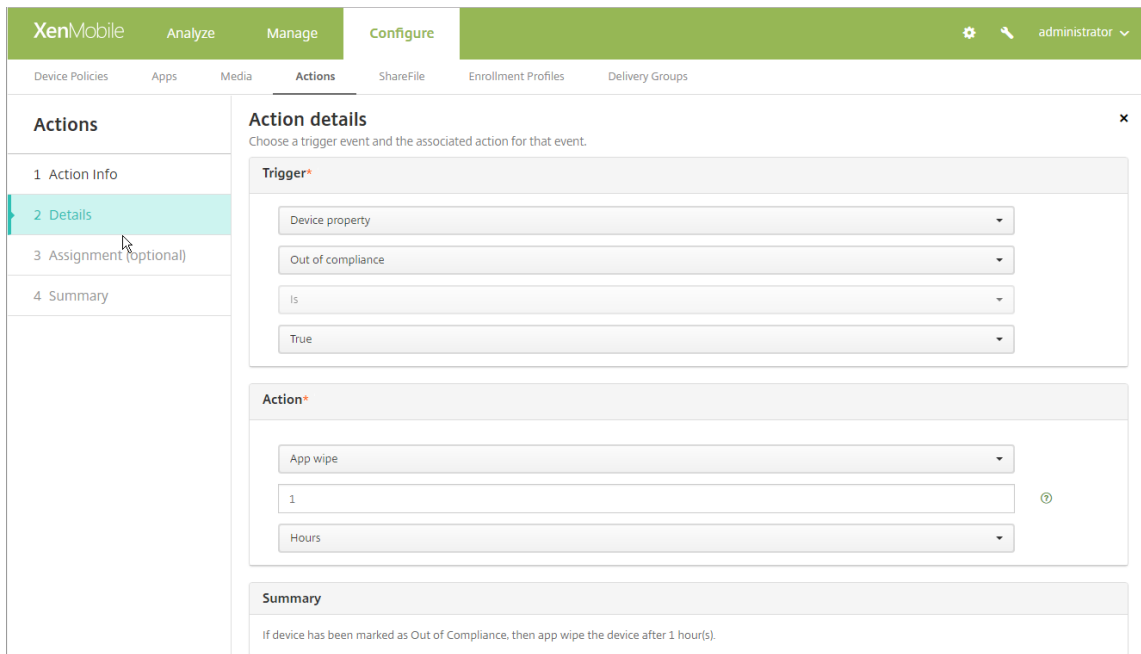
- 장치를선택적으로초기화
- 장치를완전히초기화
- 장치해지

각옵션에대해 1 시간이지연이자동으로설정되지만지연기간을분, 시간또는일단위로선택할수있습니다. 지연의목적은동작이발생하기전에사용자에게문제를수정할시간을주기위한것입니다. 앱초기화및앱잠금동작에대한자세한내용은 [보안동작](#)을참조하십시오.

참고:

트리거를 이벤트로설정하는경우반복간격은자동으로최소 1 시간으로설정됩니다. 알림을수신하려면장치에서정책 새로고침을수행하여서버와동기화해야합니다. 일반적으로장치는사용자가로그온하거나 Secure Hub 를통해수동으로정책을새로고칠때서버와동기화됩니다.

Active Directory 데이터베이스가 XenMobile 과동기화될수있도록동작이수행되기전에약 1 시간의추가지연이발생할수있습니다.



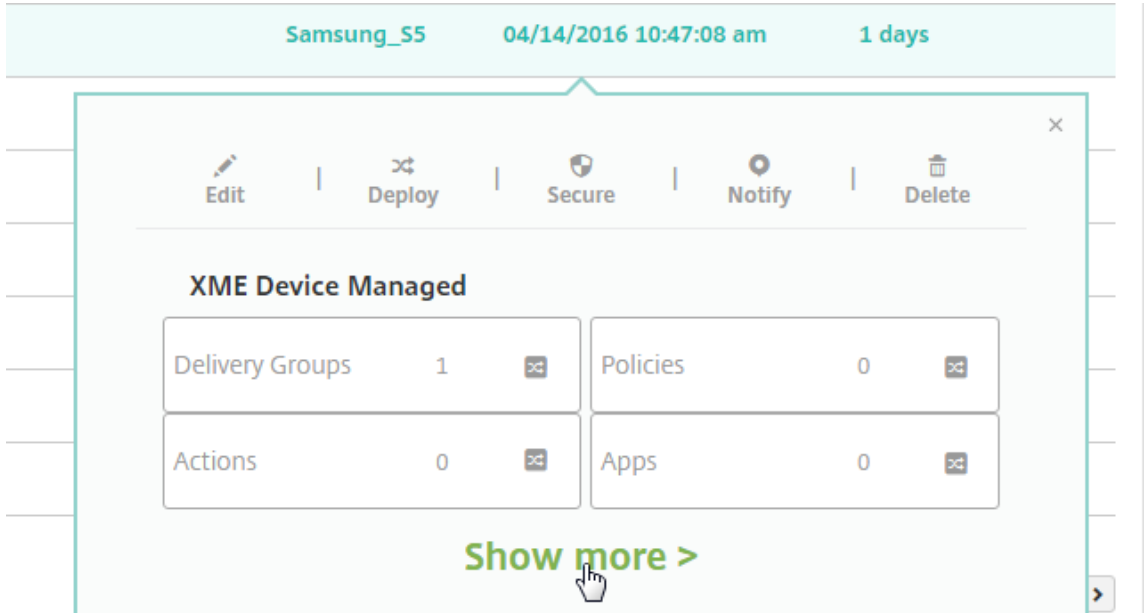
6. 배포규칙을구성하고 다음을클릭합니다.

7. 배달그룹할당및배포일정을구성하고 다음을클릭합니다.

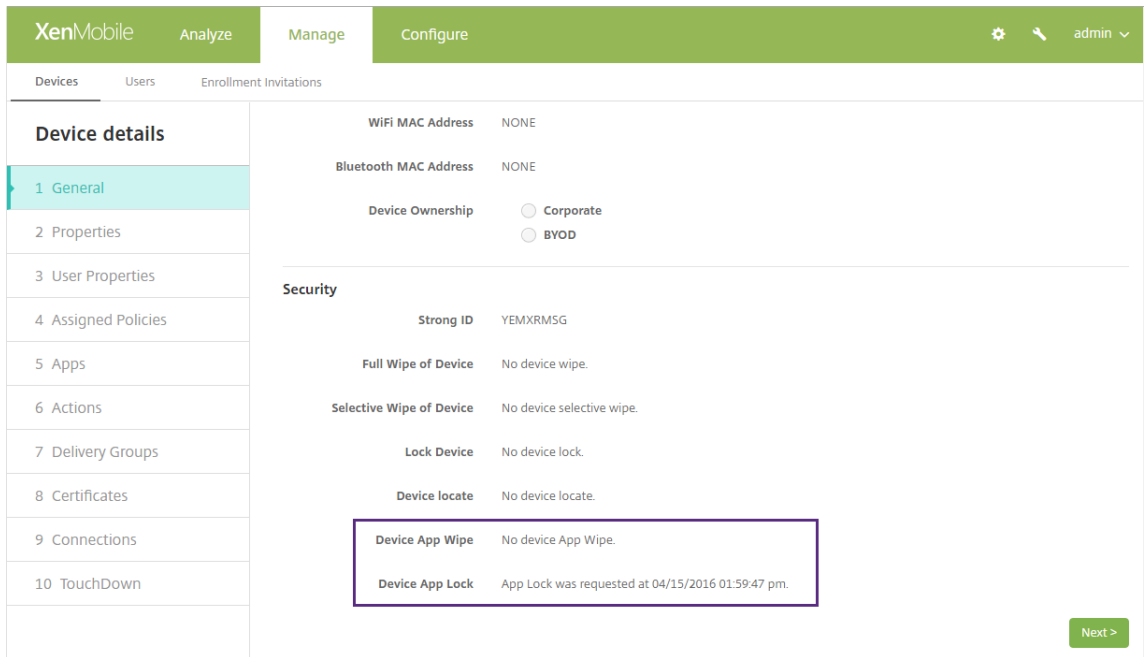
8. 저장을클릭합니다.

앱잠금또는앱초기화상태를확인하려면

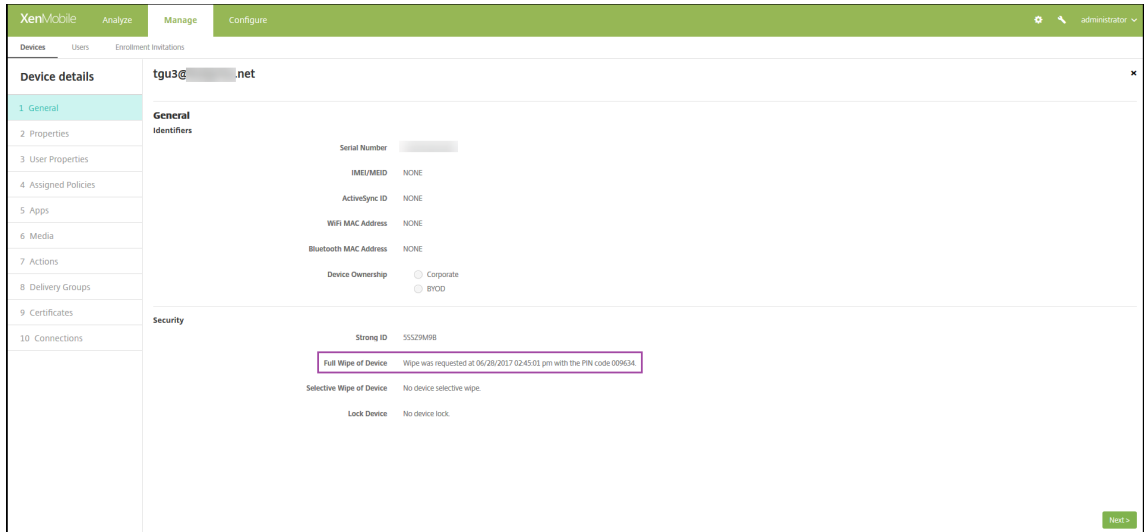
1. 관리 > 장치로이동하고장치를클릭한후 자세히표시를클릭합니다.



2. 장치앱초기화및 장치앱잠금으로스크롤합니다.



장치가초기화되면 PIN 코드를입력하라는메시지가표시됩니다. 사용자가코드를잊은경우장치세부정보에서코드를조회할 수있습니다.



모니터링및지원

January 6, 2020

XenMobile 대시보드 및 XenMobile 지원페이지를 사용하여 XenMobile Server 를 모니터링하고 문제를 해결할 수 있습니다. XenMobile 지원페이지를 사용하여 지원관련 정보 및 도구에 액세스합니다.

온-프레미스 XenMobile Server 의 경우 XenMobile CLI 에서도 동작을 수행할 수 있습니다. 자세한 내용은 [CLI\(명령줄 인터페이스\) 옵션](#)에서 참조하십시오.

XenMobile 콘솔에서 오른쪽 위 모서리의 런치 아이콘을 클릭합니다.

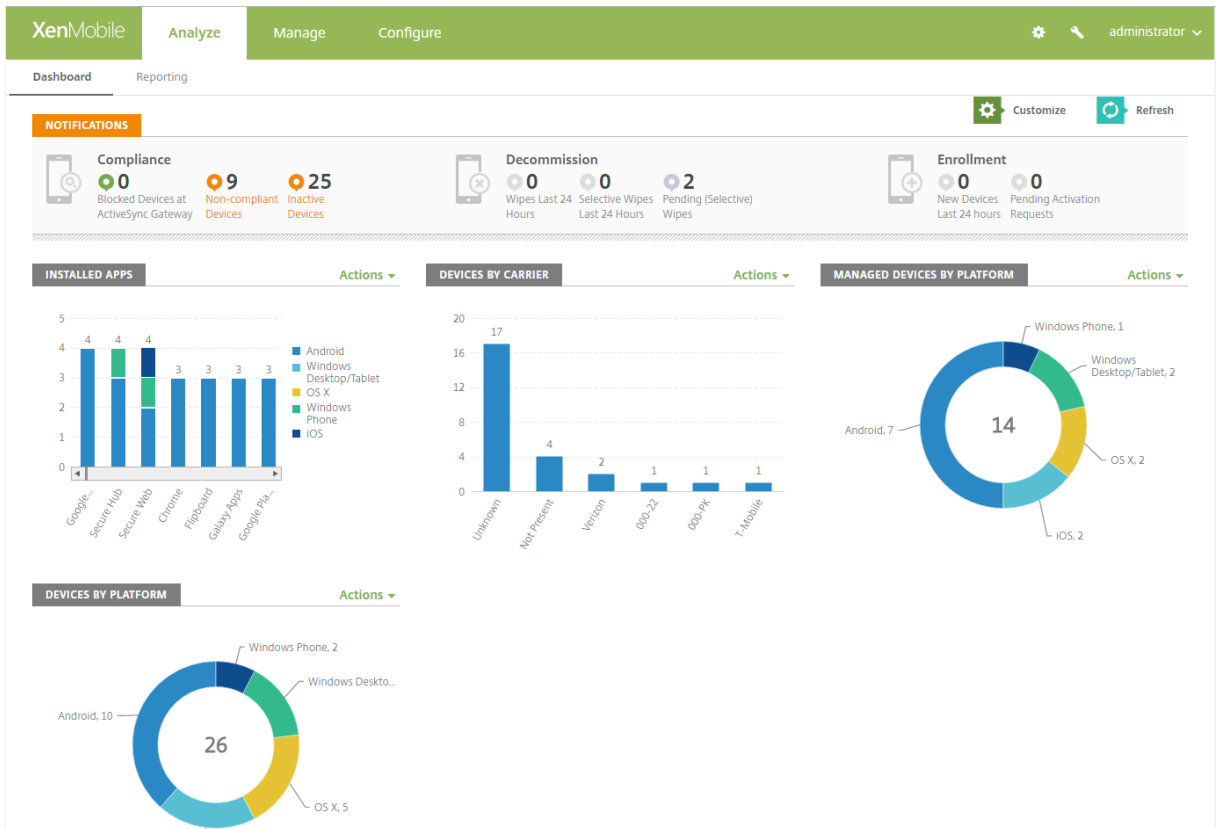


문제 해결 및 지원 페이지가 표시됩니다.

XenMobile 지원페이지를 사용하여 다음을 수행합니다.

- 진단 액세스
- 지원 번들 만들기 (온-프레미스 설치에만 해당)
- Citrix 제품 설명서 및 Knowledge Center 에 대한 링크 액세스
- 로그 작업 액세스
- 고급 구성 옵션 사용
- 도구 및 유틸리티 집합 액세스

또한 XenMobile 콘솔 대시보드에 액세스하여 정보를 한눈에 볼 수 있습니다. 이러한 정보를 사용하면 위젯을 통해 신속하게 문제점과 성공 여부를 확인할 수 있습니다.

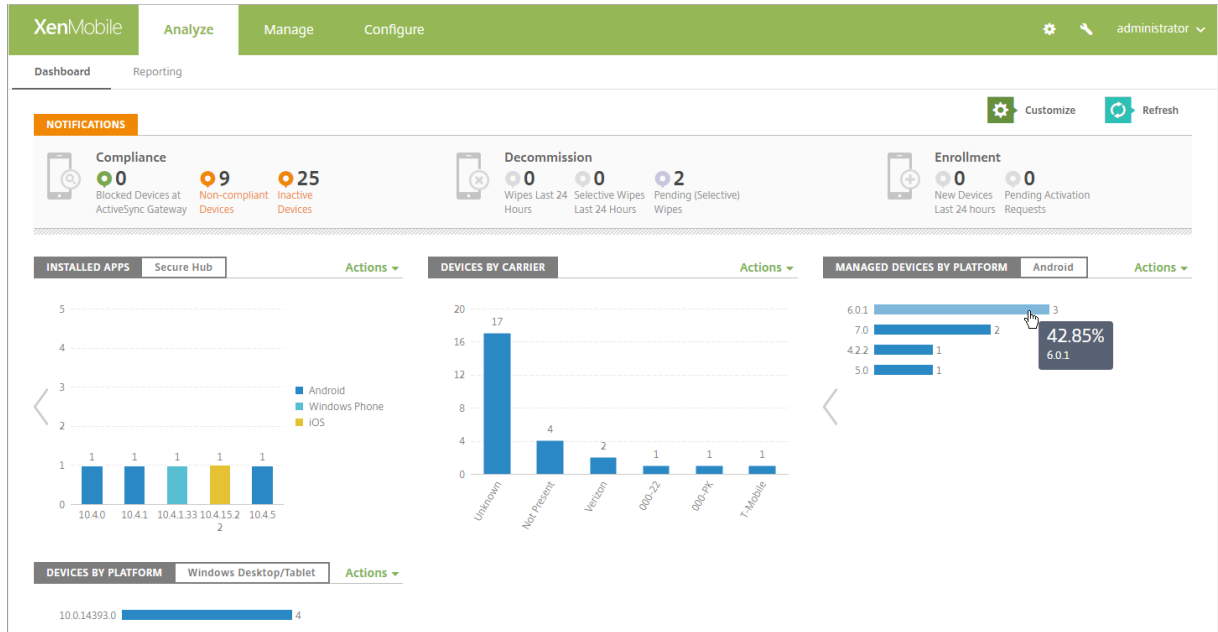


대시보드는 일반적으로 XenMobile 콘솔에 로그인할 때 처음 나타나는 페이지입니다. 콘솔의 다른 곳에서 대시보드에 액세스하려면 분석을 클릭합니다. 페이지의 레이아웃을 편집하고 나타나는 위젯을 편집하려면 대시보드에서 사용자 지정을 클릭합니다.

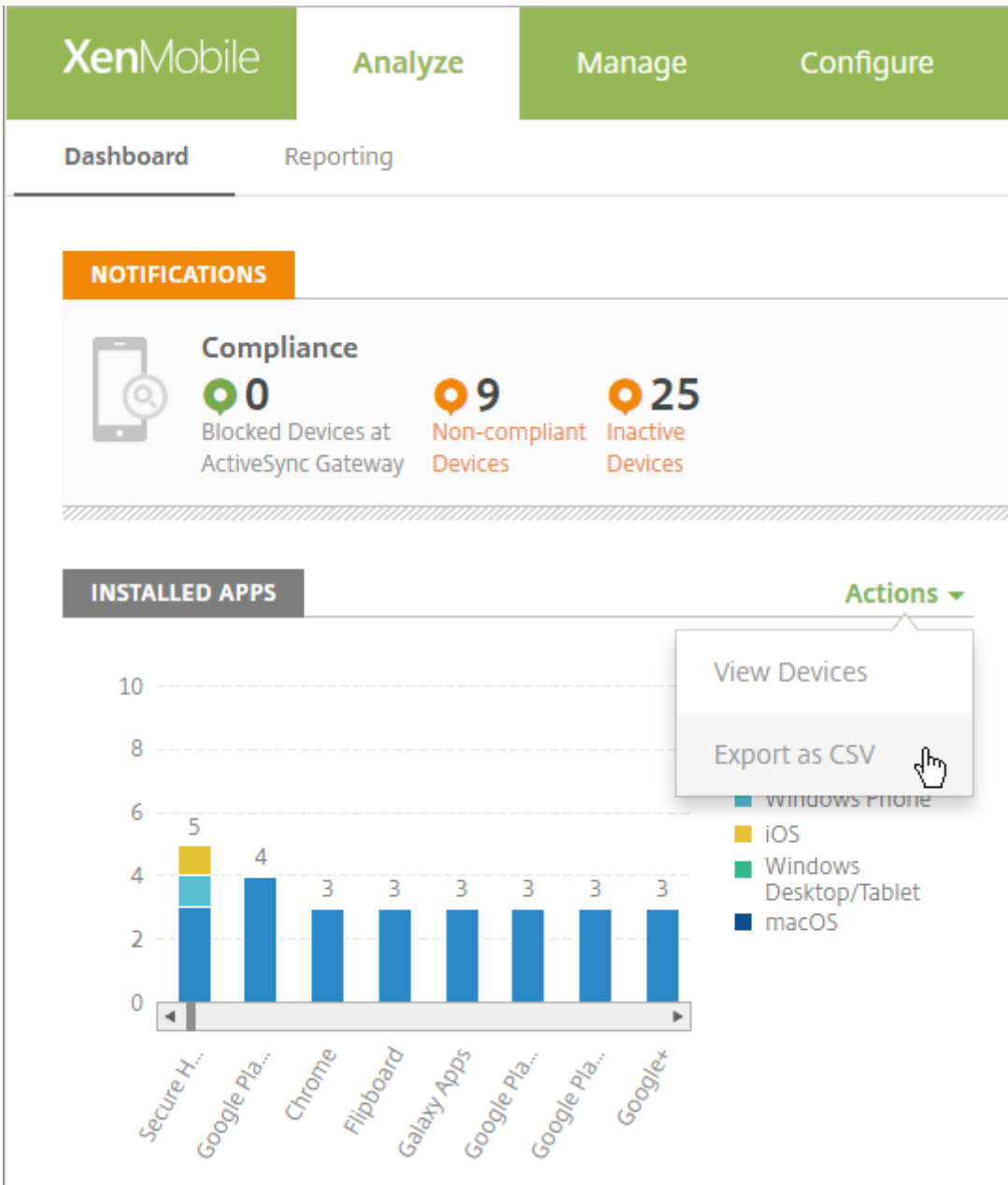
- **내 대시보드:** 최대 네 개의 대시보드를 저장할 수 있습니다. 이러한 대시보드를 개별적으로 편집하고 저장된 대시보드를 선택하여 각 대시보드를 볼 수 있습니다.
- **레이아웃 스타일:** 이 행에서는 대시보드에 표시되는 위젯 수와 위젯 배치 방법을 선택할 수 있습니다.
- **위젯 선택:** 대시보드에 표시할 정보를 선택할 수 있습니다.
 - **알림:** 왼쪽의 숫자 위에 있는 확인란을 선택하여 위젯 위에 알림 표시줄을 추가합니다. 이 표시줄에는 규격 장치, 비활성 장치 및 지난 24 시간 동안 초기화되거나 등록된 장치의 수가 표시됩니다.
 - **장치 (플랫폼 기준):** 플랫폼별로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다.
 - **장치 (이동통신사업자 기준):** 이동통신사업자별로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다. 각 표시줄을 클릭하여 플랫폼별 분석을 볼 수 있습니다.
 - **관리되는 장치 (플랫폼 기준):** 플랫폼별로 관리되는 장치의 수를 표시합니다.
 - **관리되지 않는 장치 (플랫폼 기준):** 플랫폼별로 관리되지 않는 장치의 수를 표시합니다. 이 차트에 나타나는 장치는 에이전트가 설치되어 있지만 권한이 해제되었거나 초기화되었을 수 있습니다.
 - **장치 (ActiveSync Gateway 상태 기준):** ActiveSync Gateway 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 차단됨, 허용됨 또는 알 수 없음 상태가 표시됩니다. 각 표시줄을 클릭하여 플랫폼별 데이터를 분류할 수 있습니다.
 - **장치 (소유권 기준):** 소유권 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 회사 소유, 직원 소유 또는 알 수 없는 소유권 상태가 표시됩니다.

- **Android TouchDown** 라이선스상태: TouchDown 라이선스가있는장치의수를표시합니다.
- 실패한배달그룹배포: 패키지당실패한배포의총수를표시합니다. 배포에실패한패키지만나타납니다.
- 장치 (차단된이유기준): ActiveSync 예외해차단된장치의수를표시합니다.
- 설치된앱: 앱정보의그래프에대한앱이름을입력합니다.
- **VPP** 앱라이선스사용현황: Apple Volume Purchase Program 앱에대한라이선스사용현황통계를표시합니다.

각위젯에서개별부분을클릭하여자세한정보를드릴다운할수있습니다.



또한 동작드롭다운을클릭하여정보를.csv 파일로내보낼수있습니다.



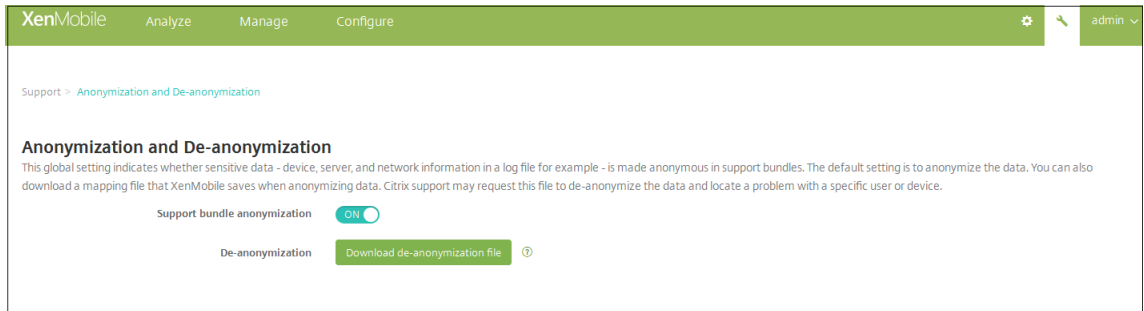
지원번들의데이터익명화

August 24, 2018

XenMobile 에서지원번들을만드는경우중요한사용자, 서버및네트워크데이터가기본적으로익명으로만들어집니다. 익명화및익명화취소페이지에서이동작을변경할수있습니다. 또한데이터를익명화할때 XenMobile 이저장하는매핑파일을다운로드할수도있습니다. Citrix 지원에서데이터의익명화를취소하고특정사용자또는장치의문제를찾기위해이파일을요청할수있습니다.

1. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다. 지원페이지가나타납니다.

2. 지원페이지에서 고급아래에있는 익명화및익명화취소를클릭합니다. 익명화및익명화취소페이지가나타납니다.



3. 지원번들익명화에서데이터를익명화할지여부를선택합니다. 기본값은 켜짐입니다.
4. 익명화취소옆에서 익명화취소파일다운로드를클릭하여문제진단을위해특정장치또는사용자정보가필요할경우 Citrix 지원에보낼매핑파일을다운로드합니다.

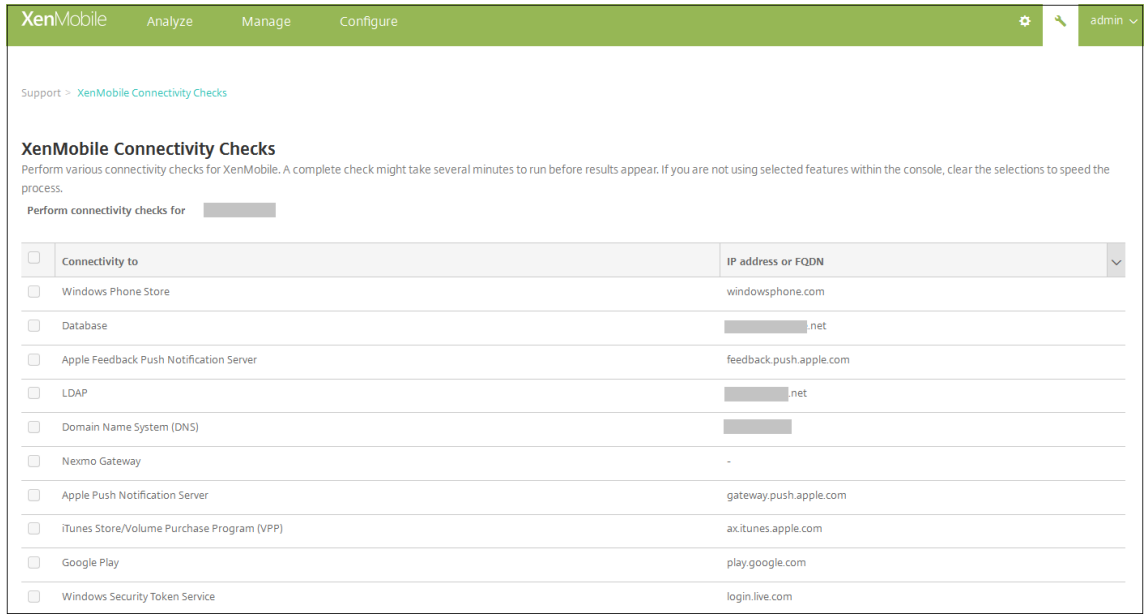
연결확인

January 6, 2020

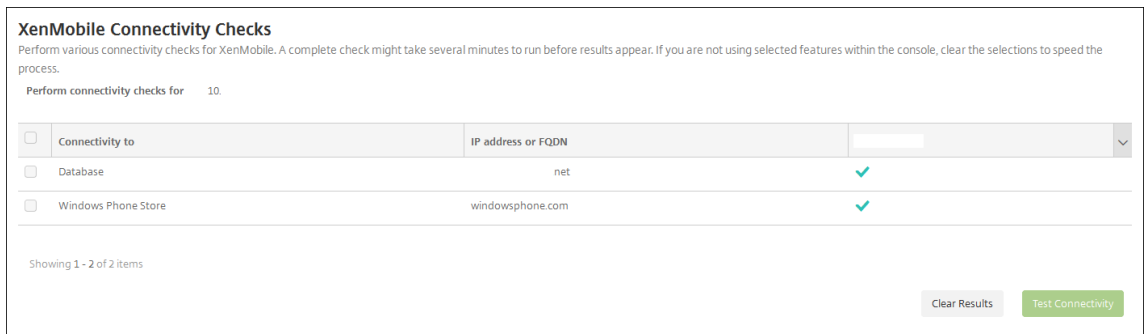
XenMobile 지원페이지에서 NetScaler Gateway 및기타서버/위치에대한 XenMobile 연결을확인할수있습니다.

XenMobile 연결확인수행

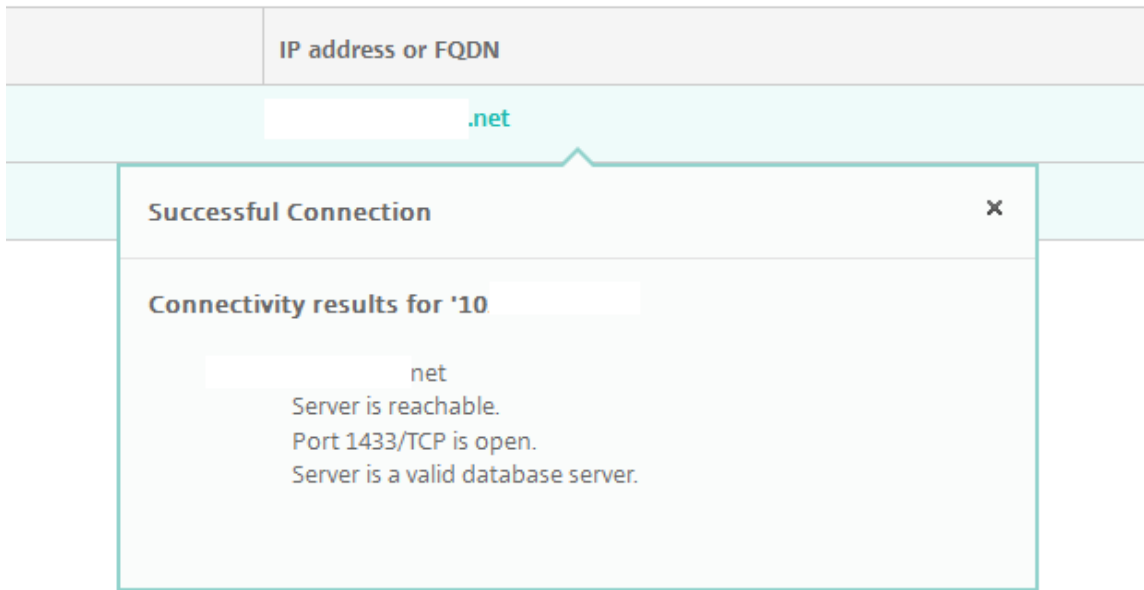
1. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다. 지원페이지가나타납니다.
2. 진단아래에서 **XenMobile** 연결확인을클릭합니다. **XenMobile** 연결확인페이지가나타납니다. XenMobile 환경에 클러스터된노드가포함되는경우모든노드가표시됩니다.



3. 연결테스트에포함할서버를선택한후 연결테스트를클릭합니다. 테스트결과페이지가나타납니다.

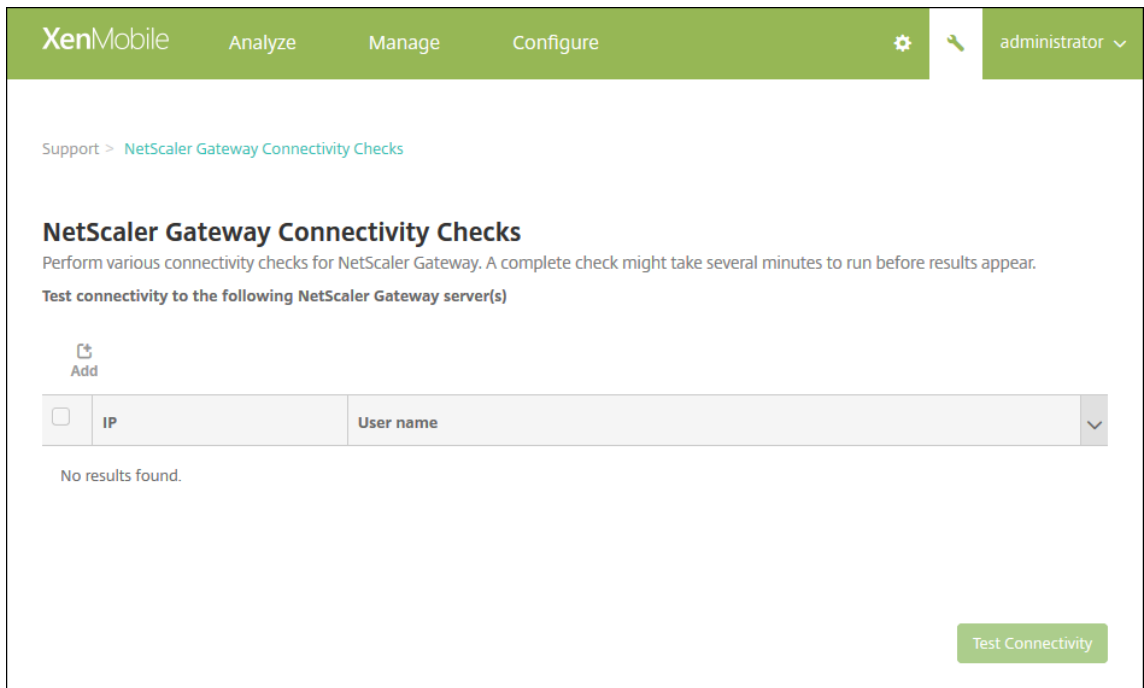


4. 테스트결과테이블에서서버를선택하여해당서버에대한자세한결과를확인합니다.

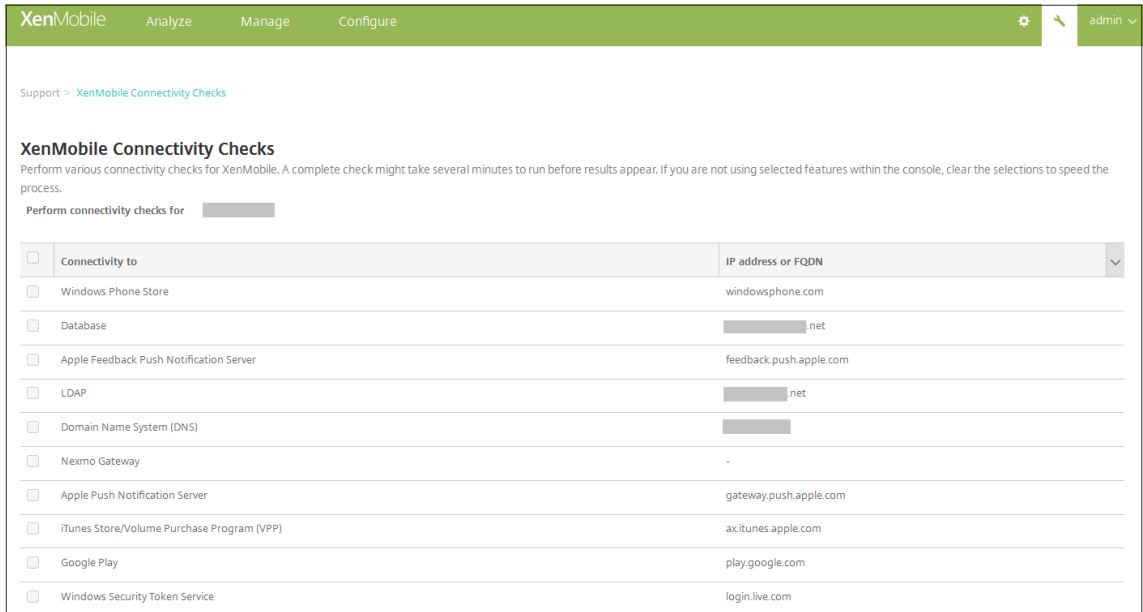


NetScaler Gateway 연결확인수행

1. 지원페이지의 진단아래에서 **NetScaler Gateway** 연결확인을클릭합니다. **NetScaler Gateway** 연결확인페이지가나타납니다. NetScaler Gateway 서버를추가하지않은경우테이블은비어있습니다.



2. 추가를클릭합니다. **NetScaler Gateway** 서버추가대화상자가나타납니다.



3. **NetScaler Gateway** 관리 IP 에서 테스트하려는 NetScaler Gateway 가 실행되는 서버의 관리 IP 주소를 입력합니다.

참고:

이전에 이미 추가된 NetScaler Gateway 서버에 대한 연결 확인을 수행하는 경우 해당 IP 주소가 제공됩니다.

4. 이 NetScaler Gateway 의 관리자 자격 증명을 입력합니다.

참고:

이전에 이미 추가된 NetScaler Gateway 서버에 대한 연결 확인을 수행하는 경우 해당 사용자 이름이 제공됩니다.

5. 추가를 클릭합니다. NetScaler Gateway 가 **NetScaler Gateway** 연결 확인 페이지의 테이블에 추가됩니다.

6. NetScaler Gateway 서버를 선택한 후에 연결 테스트를 클릭합니다. 테스트 결과 테이블에 결과가 표시됩니다.

7. 테스트 결과 테이블에서 서버를 선택하여 해당 서버에 대한 자세한 결과를 확인합니다.

사용자 환경 개선 프로그램

April 11, 2019

Citrix CEIP(사용자 환경 개선 프로그램) 는 XenMobile 에서 익명의 구성 및 사용 현황 데이터를 수집하여 Citrix 에 보냅니다. 이 데이터는 Citrix 가 XenMobile 의 품질, 안정성 및 성능을 개선하는데 도움이 됩니다. CEIP 참여는 전적으로 자발적입니다. XenMobile 을 처음 설치하거나 업데이트를 설치할 때 CEIP 참여를 선택할 수 있습니다. 참여하는 경우 일반적으로 주단위로 데이터가 수집되며 성능 및 사용 현황 데이터는 매시간 수집됩니다. 데이터는 디스크에 저장되고 HTTPS 를 통해 안전하게 Citrix 로 매주 전송됩니다. XenMobile 콘솔에서 CEIP 참여 여부를 변경할 수 있습니다. CEIP 에 대한 자세한 내용은 [Citrix CEIP\(사용자 환경 개선 프로그램\) 정보](#) 를 참조하십시오.

CEIP 참여선택

XenMobile 을 처음 설치하거나 업데이트를 수행하면 참여할지를 묻는 다음 대화상자가 표시됩니다.


Customer Experience Improvement Program ×

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

[Learn more](#)



Would you like to help make Citrix products better by joining the program?
(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)

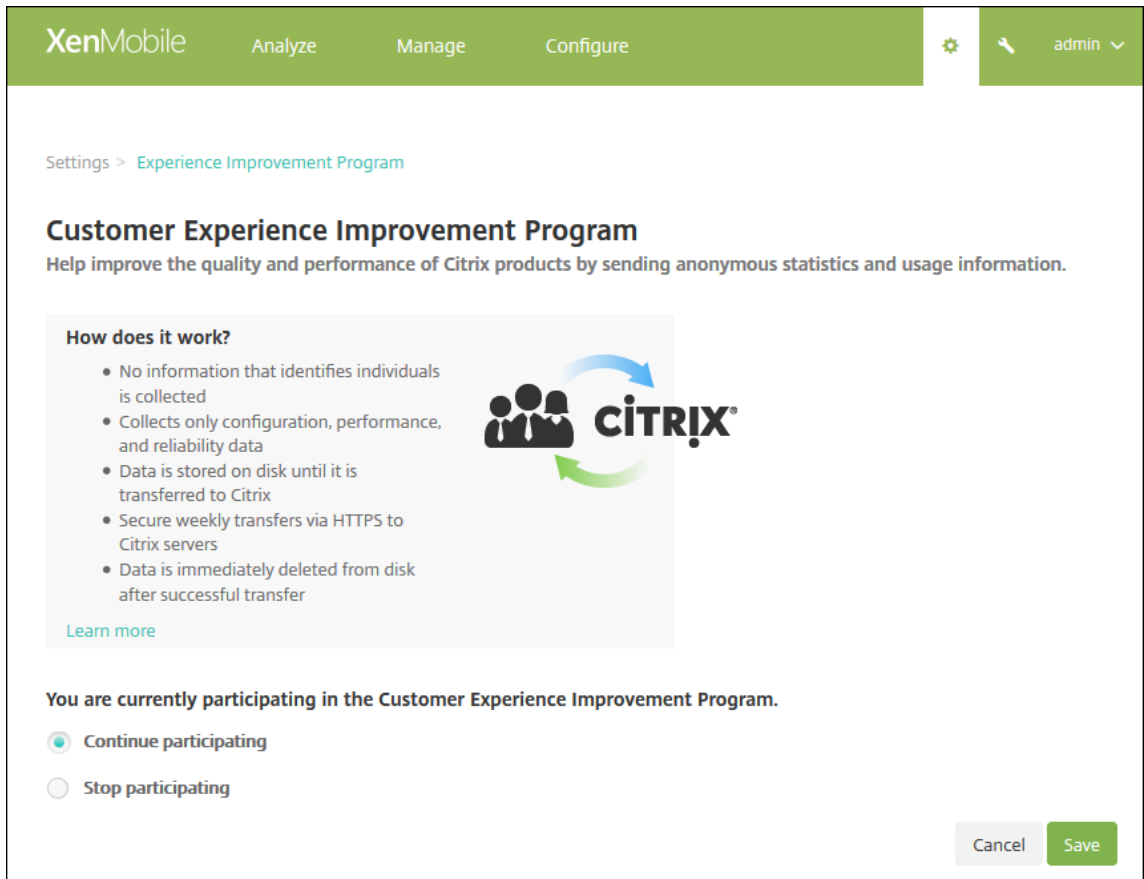
Yes, send anonymous usage and statistics information.

No

Cancel Save

CEIP 참여설정변경

1. CEIP 참여설정을 변경하려면 XenMobile 콘솔에서 오른쪽 맨 위의 기어 아이콘을 클릭하여 설정 페이지를 엽니다.
2. 서버에서 환경개선프로그램을 클릭합니다. 사용자 환경개선프로그램 페이지가 나타납니다. 표시되는 정확한 페이지는 현재 CEIP 참여여부에 따라 다릅니다.



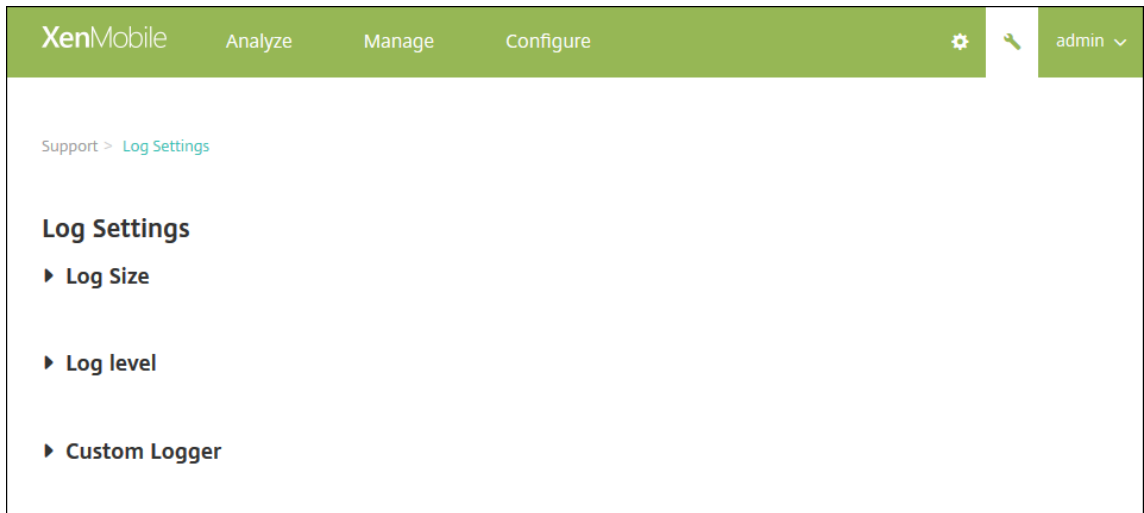
3. 현재 CEIP 에참여중이고참여를중지하려는경우 참여중지를클릭합니다.
4. 현재 CEIP 에참여하고있지않고참여를시작하려는경우 참여시작을클릭합니다.
5. 저장을클릭합니다.

로그

January 6, 2020

XenMobile 에서생성하는로그출력을사용자지정하도록로그설정을구성할수있습니다. 클러스터된 XenMobile 서버가있는경우 XenMobile 콘솔에서로그설정을구성하면해당설정이클러스터의다른모든서버와공유됩니다.

1. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다. 지원페이지가나타납니다.
2. 로그작업아래에서 로그설정을클릭합니다. 로그설정페이지가나타납니다.

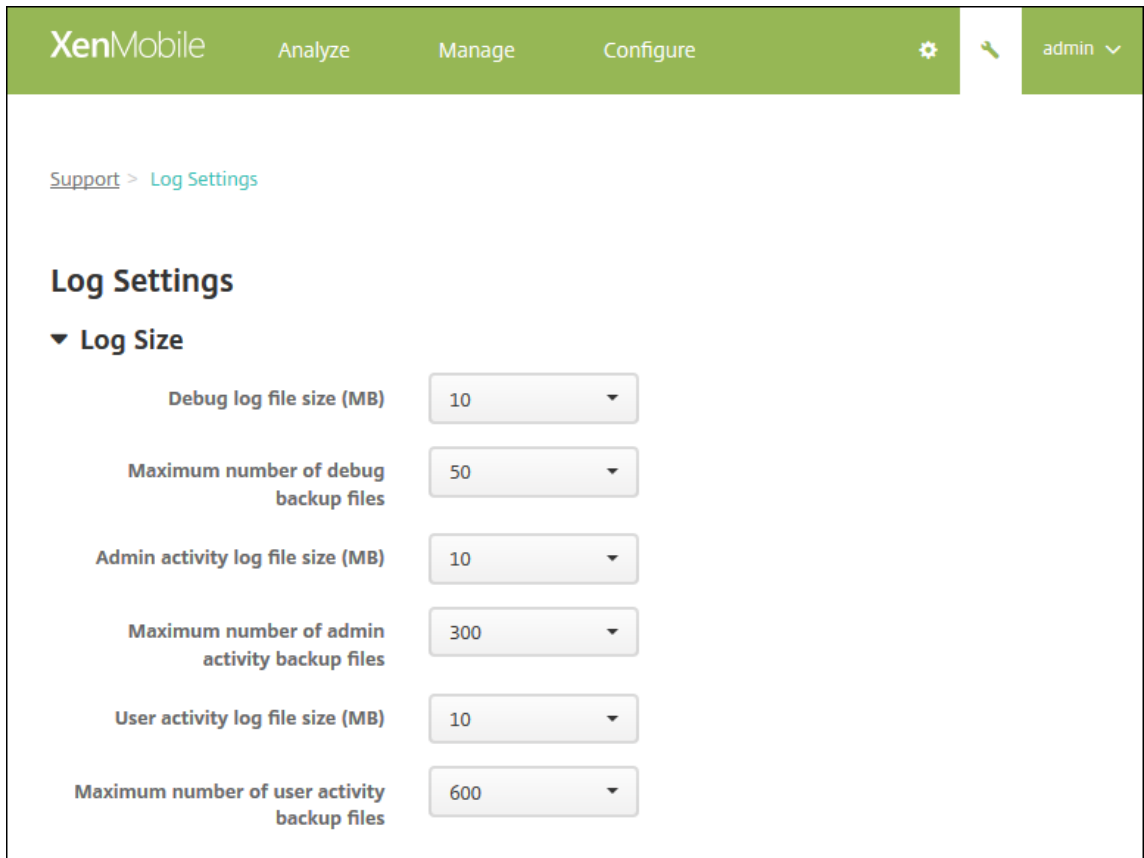


로그설정페이지에서다음과같은옵션에액세스할수있습니다.

- 로그크기. 이옵션을사용하여로그파일의크기와데이터베이스에유지되는최대로그백업파일수를제어합니다. 로그크기는 XenMobile 에서지원하는각로그 (디버그로그, 관리자작업로그및사용자작업로그) 에적용됩니다.
- 로그수준. 이옵션을사용하여로그수준을변경하거나설정을유지할수있습니다.
- 사용자지정로거. 이옵션을사용하여사용자지정로거를만듭니다. 사용자지정로그에는클래스이름과로그수준이필요합니다.

로그크기옵션을구성하려면

1. 로그설정페이지에서 로그크기를확장합니다.



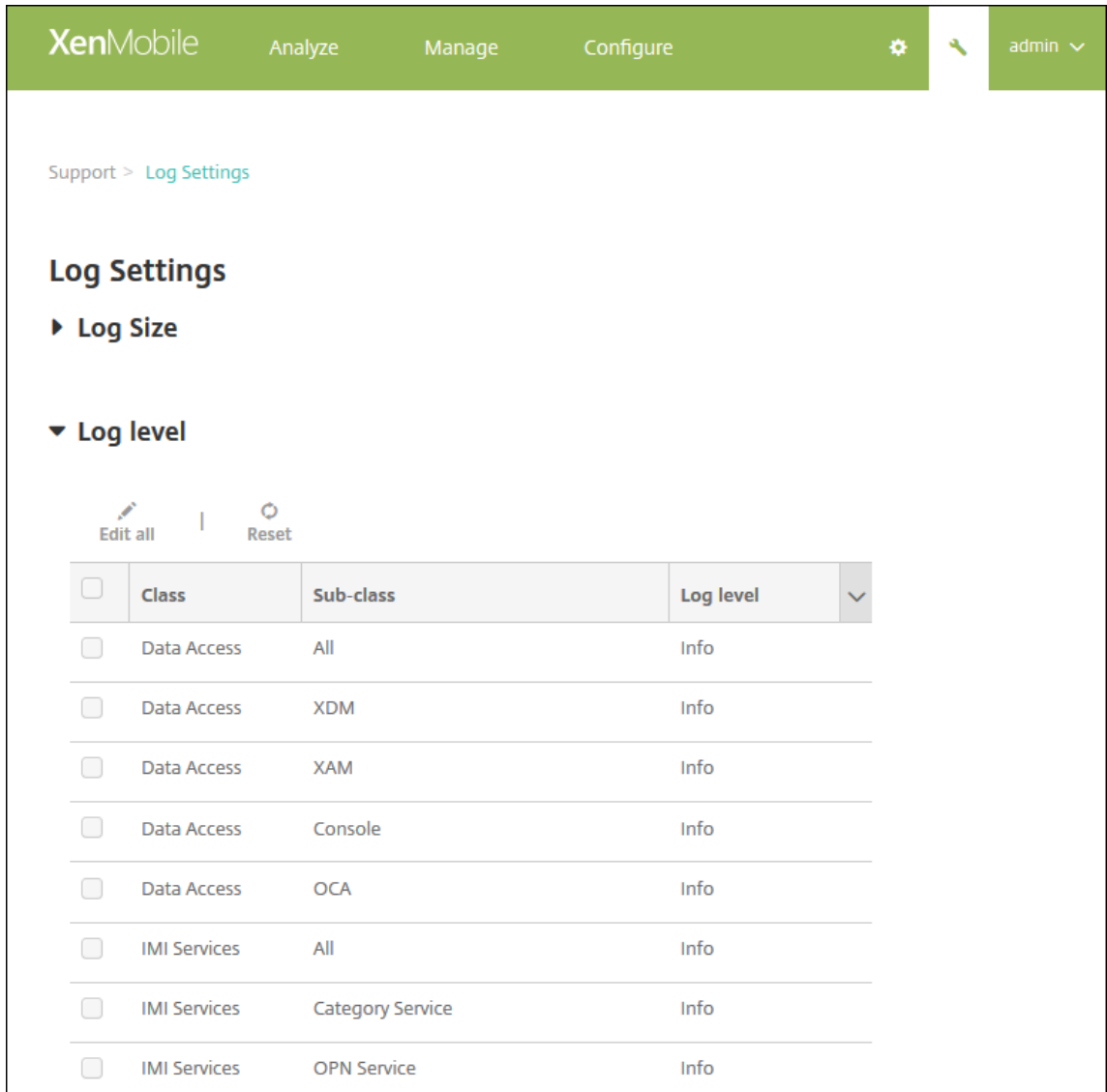
2. 다음설정을구성합니다.

- 디버그로그파일크기 **(MB)**: 목록에서 5MB 에서 20MB 사이의크기를클릭하여디버그파일의최대크기를변경합니다. 기본파일크기는 **10MB** 입니다.
- 디버그백업파일의최대수: 목록에서서버가유지하는디버그파일의최대수를클릭합니다. 기본적으로 XenMobile 은서버에 50 개의백업파일을유지합니다.
- 관리자작업로그파일크기 **(MB)**: 목록에서 5MB 에서 20MB 사이의크기를클릭하여관리자작업로그파일의최대크기를변경합니다. 기본파일크기는 **10MB** 입니다.
- 관리자작업백업파일의최대수: 목록에서서버가유지하는관리자작업파일의최대수를클릭합니다. 기본적으로 XenMobile 은서버에 300 개의백업파일을유지합니다.
- 사용자작업로그파일크기 **(MB)**: 목록에서 5MB 에서 20MB 사이의크기를클릭하여사용자작업로그파일의최대크기를변경합니다. 기본파일크기는 **10MB** 입니다.
- 사용자작업백업파일의최대수: 목록에서서버가유지하는사용자작업파일의최대수를클릭합니다. 기본적으로 XenMobile 은서버에 300 개의백업파일을유지합니다.

로그수준옵션을구성하려면

로그수준을사용하여 XenMobile 이로그에서수집하는정보의유형을지정할수있습니다. 모든사례에대해동일한수준을설정하거나개별사례를특정수준으로설정할수있습니다.

1. 로그설정페이지에서 로그수준을확장합니다. 모든로그클래스의테이블이나타납니다.



2. 다음중하나를수행합니다.

- 원하는클래스옆에있는확인란을클릭한다음 수준설정을클릭하여해당클래스의로그수준을변경합니다.
- 모두편집을클릭하여로그수준변경내용을테이블의모든클래스에적용합니다.

로그수준을설정하고 XenMobile 서버를다시부팅할때로그수준설정을유지할지여부를선택할수있는 로그수준설정대화상자가나타납니다.

Set Log Level ✕

Class name

Sub-class name

Log level

Included loggers

com.sparus.nps.ServicesManager
 com.sparus.nps.RegistryPacketBuilder
 com.sparus.nps.engine.business.impl.Engine
 eManager
 com.sparus.nps.SessionManager?

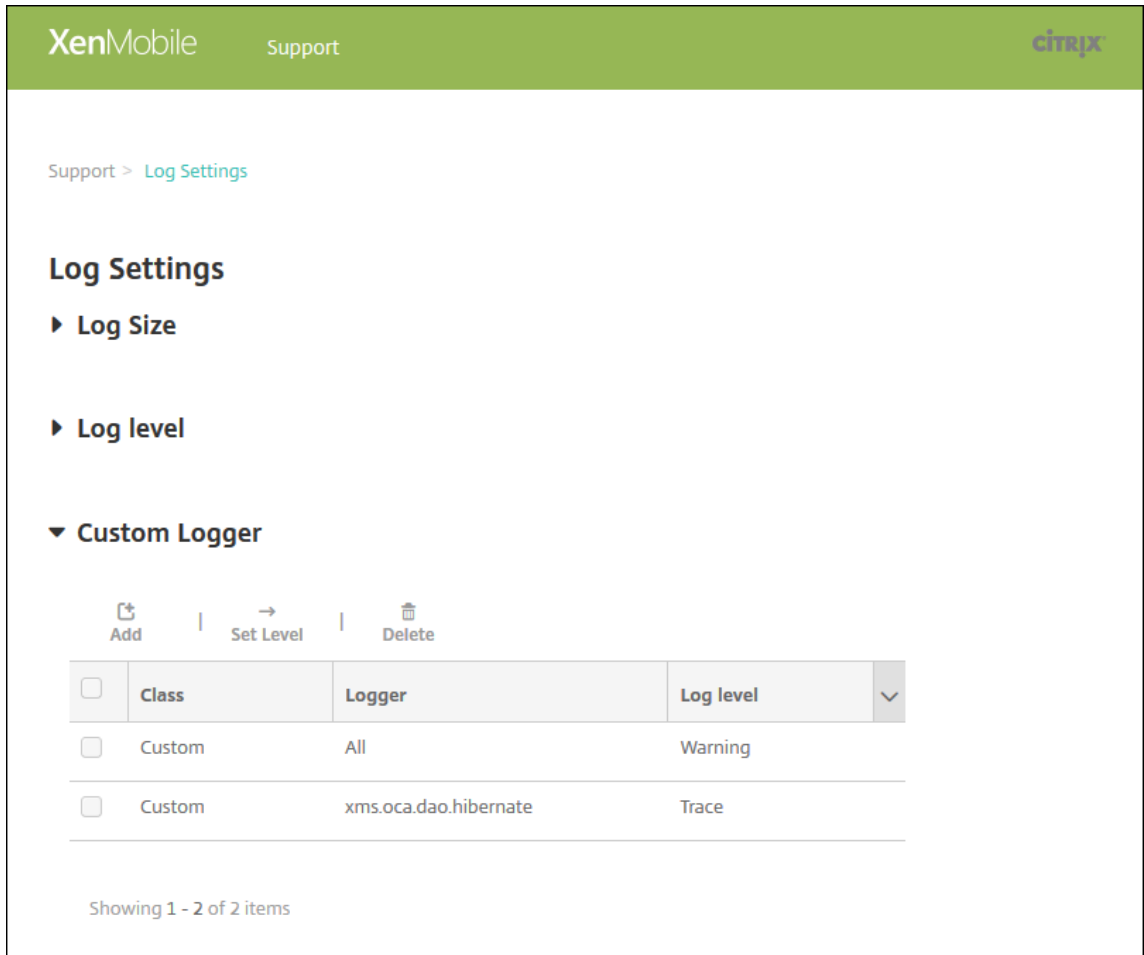
Persist settings

- 클래스이름: 모든클래스의로그수준을변경할때에는이필드에 '모두' 가표시되지만, 그렇지않은경우에는개별클래스이름이표시됩니다. 이필드는편집할수없습니다.
- 하위클래스이름: 모든클래스의로그수준을변경할때에는이필드에 '모두' 가표시되지만, 그렇지않은경우에는개별클래스의하위클래스이름이표시됩니다. 이필드는편집할수없습니다.
- 로그수준: 목록에서로그수준을클릭합니다. 지원되는로그수준은다음과같습니다.
 - 심각
 - 오류
 - 경고
 - 정보
 - 디버그
 - 추적
 - 꺼짐
- 포함된로거: 모든클래스의로그수준을변경하는경우에는이필드가비어있지만개별클래스의경우에는현재구성된로거가표시됩니다. 이필드는편집할수없습니다.
- 설정유지: 서버를다시부팅할때로그수준설정을유지하려면이확인란을선택합니다. 이확인란을선택하지않으면서버를다시부팅할때로그수준설정이기본값으로되돌아갑니다.

3. 설정을 클릭하여 변경 내용을 커밋합니다.

사용자 지정 로거를 추가하려면

1. 로그 설정 페이지에서 사용자 지정 로거를 확장합니다. 사용자 지정 로거 테이블이 나타납니다. 사용자 지정 로거를 추가하지 않은 경우에는 테이블이 비어 있습니다.



The screenshot shows the XenMobile Support interface. The breadcrumb is 'Support > Log Settings'. Under 'Log Settings', there are sections for 'Log Size', 'Log level', and 'Custom Logger'. The 'Custom Logger' section has three actions: 'Add', 'Set Level', and 'Delete'. Below these actions is a table with two columns: 'Class' and 'Logger', and a 'Log level' column with a dropdown arrow. The table contains two rows: one with 'Custom' and 'All' and 'Warning' level, and another with 'Custom' and 'xms.oca.dao.hibernate' and 'Trace' level. At the bottom, it says 'Showing 1 - 2 of 2 items'.

<input type="checkbox"/>	Class	Logger	Log level
<input type="checkbox"/>	Custom	All	Warning
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace

2. 추가를 클릭합니다. 사용자 지정 로거 추가 대화상자가 나타납니다.

Add custom logger ✕

Class name

Log level

Included loggers

3. 다음설정을구성합니다.

- 클래스이름: 이필드에는 사용자지정이표시됩니다. 이필드는편집할수없습니다.
- 로그수준: 목록에서로그수준을클릭합니다. 지원되는로그수준은다음과같습니다.
 - 심각
 - 오류
 - 경고
 - 정보
 - 디버그
 - 추적
 - 꺼짐
- 포함된로거: 사용자지정로거에포함시키려는특정로거를입력하거나모든로거를포함시키려면필드를비워둡니다.

4. 추가를클릭합니다. 사용자지정로거가 사용자지정로거테이블에추가됩니다.

▼ Custom Logger

Add
 Set Level
 Delete

	Class	Logger	Log level
<input type="checkbox"/>	Custom	All	Warning
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace

사용자지정로거를삭제하려면

1. 로그설정페이지에서 사용자지정로거를확장합니다.
2. 삭제할사용자지정로거를선택합니다.
3. 삭제를클릭합니다. 사용자지정로거를삭제할지묻는대화상자가나타납니다. 확인을클릭합니다.

중요:

이작업은실행취소할수없습니다.

모바일서비스공급자

January 6, 2020

XenMobile 에서모바일서비스공급자인터페이스를사용하여 BlackBerry 및 Exchange ActiveSync 장치를관리하고작업을실행할수있습니다.

예를들어조직에 1,000 명의사용자가있고각사용자가하나이상의장치를사용할수있습니다. 모든사용자에게관리를위해 XenMobile 에장치를등록해야한다고알린후 XenMobile 콘솔에사용자가등록한장치수가나타납니다. 이설정을구성하면 Exchange Server 에연결한장치수를확인할수있습니다. 이방법으로다음을수행할수있습니다.

- 특정사용자가장치를등록해야하는지여부를확인할수있습니다.
 - Exchange Server 에연결하는사용자장치에데이터초기화와같은명령을실행할수있습니다.
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
 2. 서버아래에서 모바일서비스공급자를클릭합니다. 모바일서비스공급자페이지가나타납니다.

The screenshot shows the 'Mobile Service Provider' configuration page in the XenMobile console. The page has a green header with 'XenMobile' and navigation tabs for 'Analyze', 'Manage', and 'Configure'. The breadcrumb is 'Settings > Mobile Service Provider'. The main heading is 'Mobile Service Provider' with a sub-heading: 'Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.' There are three input fields: 'Web service URL*' with the value 'http://XmmServer/services/zdm', 'User name*' with 'domain\admin', and 'Password*'. Below these is a toggle switch for 'Automatically update BlackBerry and ActiveSync device connections' which is currently 'OFF'. A green 'Test Connection' button is located below the toggle. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. 다음설정을구성합니다.

- 웹 서비스 **URL**: 웹 서비스의 URL 을 입력 합니다 (예: <https://<XmmServer>/services/xdmservice>).
- 사용자이름: domain\admin 형식으로 사용자이름을 입력합니다.
- 암호: 암호를 입력합니다.
- **BlackBerry** 및 **ActiveSync** 장치연결자동업데이트: 장치연결을 자동으로 업데이트할지 여부를 선택합니다. 기본값은 꺼짐입니다.
- 연결테스트를 클릭하여 연결을 확인합니다.

4. 저장을 클릭합니다.

보고서

May 21, 2019

XenMobile 은 앱 및 장치 배포를 분석하는데 사용할 수 있는 미리 정의된 보고서를 제공합니다. 각 보고서는 표와 차트로 표시됩니다. 열을 기준으로 표를 정렬하고 필터링할 수 있습니다. 차트의 특정 요소를 선택하여 더 자세한 정보를 볼 수 있습니다.

- 앱 배포 총 시도 횟수: 사용자가 자신의 장치에 설치하려고 시도한 배포된 앱을 나열합니다.
- 플랫폼별 앱: 앱과 앱 버전을 장치 플랫폼 및 버전별로 나열합니다.
- 유형별 앱: 버전, 유형 및 범주별로 앱을 나열합니다.
- 장치 등록: 등록된 모든 장치를 나열합니다.
- 장치 및 앱: 관리되는 앱을 실행 중인 장치를 나열합니다.
- 비활성 장치: XenMobile Server 속성 device.inactivity.days.threshold 로 지정된 일수 동안 활동이 없었던 장치의 목록입니다.
- 탈옥/루팅 장치: 탈옥 iOS 장치 및 루팅 Android 장치를 나열합니다.
- 약관: 약관 계약에 동의 및 거부한 사용자를 나열합니다. 차트 일부를 선택하여 더 자세히 볼 수 있습니다.
- 상위 **10** 개 앱: 배포에 실패한 앱을 10 개까지만 나열합니다.
- 장치 및 사용자의 블랙리스트 앱: 사용자의 장치에 있는 블랙리스트 앱을 나열합니다.

각 표의 데이터를 .csv 형식으로 내보낼 수 있으며 Microsoft Excel 과 같은 프로그램을 사용하여 열 수 있습니다. 각 보고서의 차트를 PDF 형식으로 내보낼 수 있습니다.

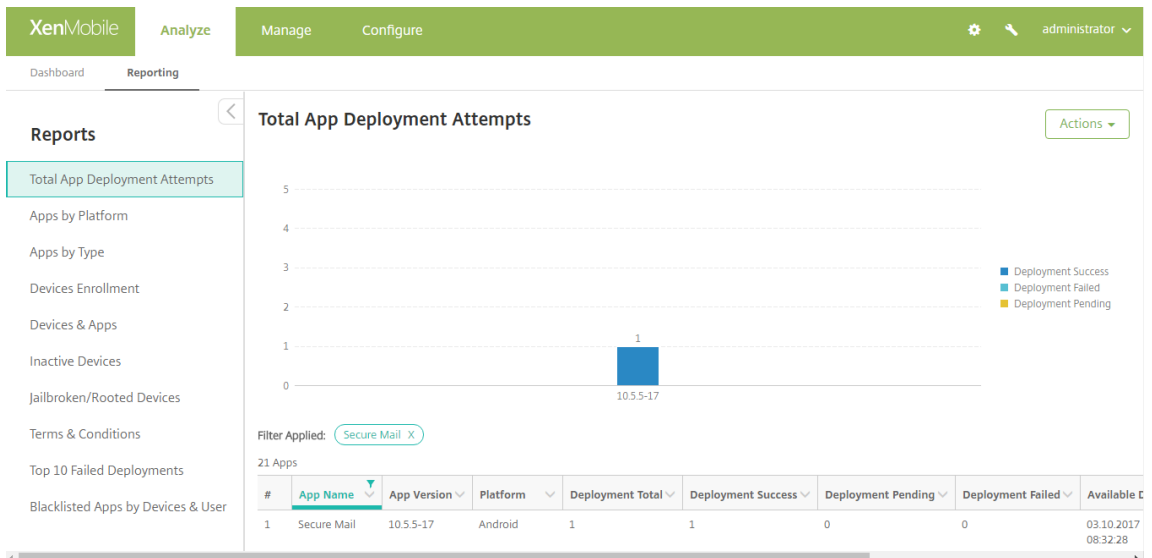
보고서를 생성하려면

1. XenMobile 콘솔에서 분석 > 보고서를 클릭합니다. 보고 페이지가 나타납니다.
2. 생성할 보고서를 클릭합니다.



보고서의더상세한정보를보려면

1. 자세히볼차트부분을클릭하면상세정보가표시됩니다.



표열을정렬, 필터링또는검색하려면열머리글을클릭합니다

The screenshot shows the 'Reporting' section of the XenMobile console. The 'Reports' sidebar on the left includes 'Total App Deployment Attempts', 'Apps by Platform', 'Apps by Type', 'Devices Enrollment', 'Devices & Apps', 'Inactive Devices', 'Jailbroken/Rooted Devices', 'Terms & Conditions', 'Top 10 Failed Deployments', and 'Blacklisted Apps by Devices & User'. The main table displays 22 apps with columns for #, App Name, App Version, Platform, Deployment Total, Deployment Success, Deployment Pending, Deployment Failed, and Available. A dropdown menu is open over the 'App Name' column, showing options for 'Sort Ascending', 'Sort Descending', 'Filter with' (containing 'secure'), and 'Secure Web'. A 'Filter' button is visible at the bottom of the dropdown.

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Enterprise1			1	1	0	0	03.10.201 09:10:10
2	SandBox_S			1	1	0	0	03.10.201 08:38:40
3	Fonts			1	0	1	0	03.10.201 09:45:07
4	SandBox_S			1	1	0	0	03.10.201 08:38:40
5	GoToMeeti			1	1	0	0	03.10.201 12:34:35
6	Secure Mail	10.5.5-17	Android	1	1	0	0	03.10.201 08:32:28
7	GreedyPenguins		Windows Mobile	1	1	0	0	03.10.201 13:01:50

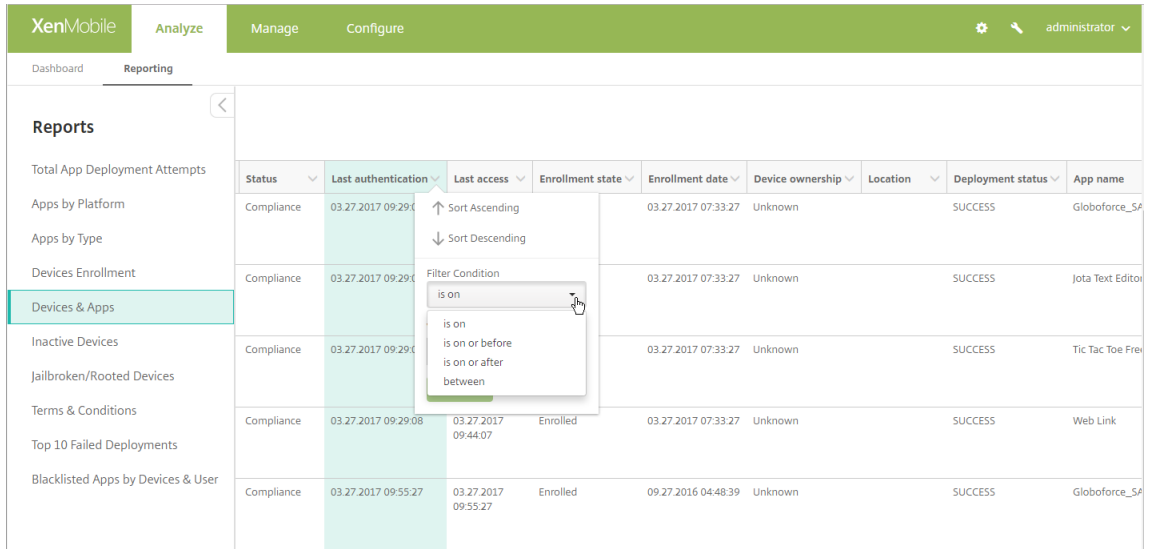
보고서를날짜로필터링하려면

1. 열머리글을클릭하면필터설정이표시됩니다.

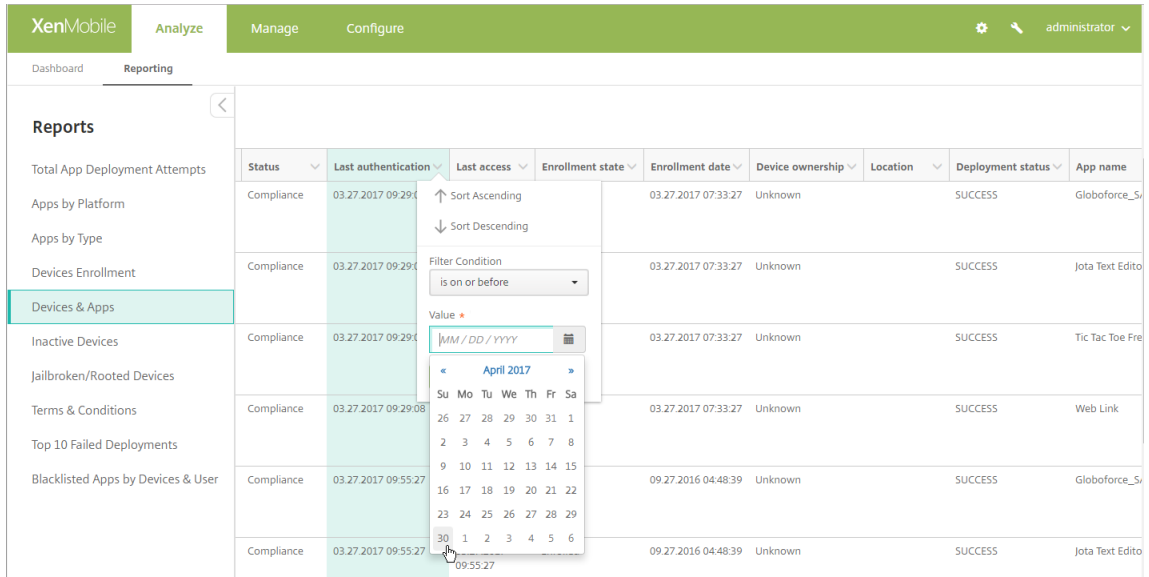
The screenshot shows the 'Reporting' section of the XenMobile console, specifically the 'Devices & Apps' report. The table displays columns for Status, Last authentication, Last access, Enrollment state, Enrollment date, Device ownership, Location, Deployment status, and App name. A dropdown menu is open over the 'Last authentication' column, showing options for 'Sort Ascending', 'Sort Descending', 'Filter Condition' (set to 'is on'), and a 'Value' field with a date picker set to 'MM/DD/YYYY'. A 'Filter' button is visible at the bottom of the dropdown.

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_SA
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_SA

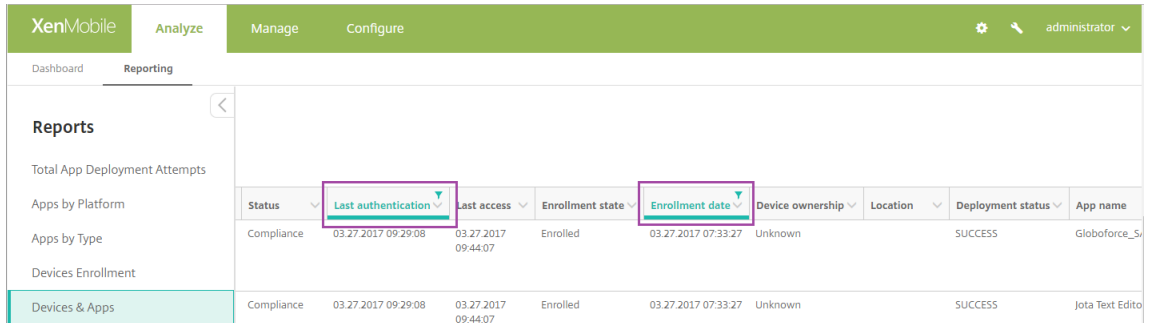
2. 필터조건에서보고되는날짜를제한할방법을선택합니다.



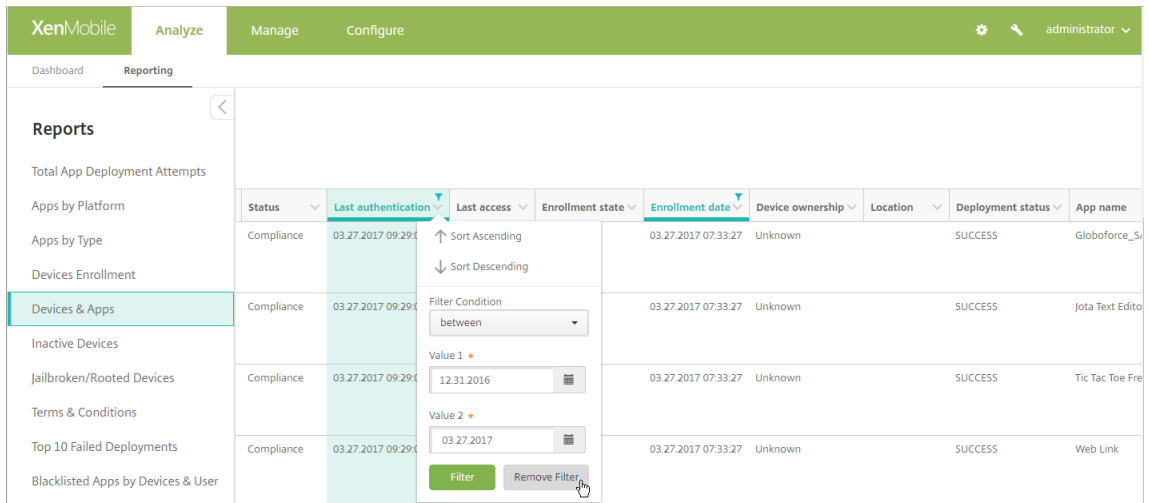
3. 날짜선택기를 사용하여 날짜를 지정합니다.



4. 날짜 필터가 있는 열이 다음 예제처럼 표시됩니다.

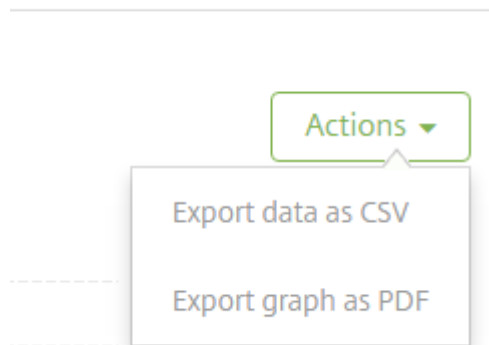


5. 필터를 제거하려면 열머리글을 클릭한다음 필터 제거를 클릭합니다.



차트또는표를내보내려면

- 차트를 PDF 형식으로내보내려면 동작, **PDF** 로그래프내보내기를차례로클릭합니다.
- 표데이터를 CSV 형식으로내보내려면 동작, **CSV** 로데이터내보내기를차례로클릭합니다.



중요:

SQL Server 를 사용하여 사용자 지정 보고서 만들 수 있지만 이 방법은 권장하지 않습니다. Citrix 는 스키마를 게시하지 않으며 알림 없이 스키마를 변경할 수 있습니다. 이 방법의 보고서를 사용하기로 결정한 경우 위기 전용 계정을 사용하여 SQL 쿼리를 실행해야 합니다. 여러 조인이 포함되어 실행에 시간이 다소 걸리는 쿼리는 그 시간 동안 XenMobile Server 성능에 영향을 미칠 수 있습니다.

SNMP 모니터링

January 6, 2020

XenMobile Server 에서 SNMP 모니터링을사용하도록설정하여모니터링시스템이 XenMobile 노드를쿼리하고노드의정보를가져오도록허용할수있습니다. 쿼리에는프로세서로드, 로드평균, 메모리사용현황및연결같은매개변수가사용됩니다. 인증및암호화사양을비롯하여 SNMP v3 에대한자세한내용은 [RFC 3414](#)에대한공식 SNMP 설명서를참조하십시오.

참고:

SNMP v3 모니터링은 XenMobile Server 10.8 이상에서지원됩니다.

SCOM 과같은 SNMP 모니터링을지원하는다양한모니터링응용프로그램을사용할수있습니다. SCOM 구성에대한자세한내용은 [Citrix Support Knowledge Center 문서](#)를참조하십시오.

사전요구사항

다음 TCP 포트를구성합니다.

- 포트 **161(UDP)**: UDP 프로토콜을사용하는 SNMP 트래픽에사용됩니다. 원본은 SNMP 관리자이고대상은 XenMobile 입니다.
- 포트 **162(UDP)**: XenMobile 의 SNMP 트랩알림을 SNMP 관리자로보내는데사용됩니다. 원본은 XenMobile 이고대상은 SNMP 관리자입니다.

XenMobile 포트구성에대한자세한내용은 [포트요구사항](#)을참조하십시오.

SNMP 를포함하는온-프레미스 XenMobile 배포의아키텍처 다이어그램은 [온-프레미스배포용참조아키텍처](#)를참조하십시오.

SNMP 를설정하는일반적인단계는다음과같습니다.

1. 사용자추가: 사용자는트랩을수신하고 XenMobile Server 를모니터링할수있는권한을상속합니다.
2. 트랩을수신할 **SNMP** 관리자추가: 트랩은 XenMobile 노드가사용자정의된최대임계값을초과할경우 XenMobile 에서생성되는알림입니다.
3. **XenMobile** 과상호작용하도록 **SNMP** 관리자구성: XenMobile Server 는특정 MIB(관리정보데이터베이스) 를사용하여작업을수행합니다. MIB 는 XenMobile 콘솔의 설정 > **SNMP** 구성페이지에서다운로드합니다. 그런다음 MIB 가져오기도구를사용하여 SNMP 관리자로 MIB 를가져옵니다.

참고:

모든 SNMP 관리자에는자체 MIB 가져오기도구가있습니다.

4. 트랩사용: XenMobile 콘솔에서트랩을사용하도록설정하고환경의요구사항에따라간격및임계값을정의합니다.
5. 타사 **SNMP** 관리자에서트랩보기: 트랩을보려면 SNMP 관리자를확인합니다. 그러나일부관리자의경우관리자외부에서도알림을사용하도록설정을구성할수있습니다. 예를들어전자메일에알림을표시하도록구성할수있습니다.

XenMobile 에서생성할수있는트랩은다음과같습니다.

트랩이름: 프로세서로드

- 모니터링 **OID(개체 ID)**: .1.3.6.1.2.1.25.3.3.1.2
- 설명: 사용자정의된간격마다시스템의 CPU 로드를모니터링합니다. 로드가사용자지정임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: 1 분동안의로드평균

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.10.1.5.1
- 설명: 사용자정의된간격마다 1 분동안평균시스템로드를모니터링합니다. 로드평균이사용자지정임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: 5 분동안의로드평균

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.10.1.5.2
- 설명: 사용자정의된간격마다 5 분동안평균시스템로드를모니터링합니다. 로드평균이사용자지정임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: 15 분동안의로드평균

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.10.1.5.3
- 설명: 사용자정의된모든간격마다 15 분동안평균시스템로드를모니터링합니다. 로드평균이사용자지정임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: 사용가능한총메모리

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.4.11
- 설명: 사용자정의된모든간격마다사용가능한메모리를모니터링합니다. 사용가능한메모리가사용자지정임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다. 참고: 사용가능한총메모리에는 RAM 과스왑메모리 (가상메모리) 가모두포함됩니다. 총스왑메모리를검색하려면 SNMP OID .1.3.6.1.4.1.2021.4.3 을사용하여쿼리할수있습니다. 사용가능한스왑메모리를검색하려면 SNMP OID .1.3.6.1.4.1.2021.4.4 를사용하여쿼리할수있습니다.

트랩이름: 사용된총디스크스토리지

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.2021.9.1.9.1
- 설명: 사용자정의된모든간격마다시스템디스크스토리지를모니터링합니다. 디스크스토리지가사용자지정임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Java 힙메모리사용현황

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.2.4.0
- 설명: 사용자정의된모든간격마다 XenMobile 의 JVM(Java Virtual Machine) 힙메모리사용현황을모니터링합니다. 사용현황이사용자지정임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Java Metaspace 사용현황

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.2.5.0
- 설명: 사용자정의된모든간격마다 XenMobile 의 Java Metaspace 사용현황을모니터링합니다. 사용현황이임계값을초과하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: LDAP 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- 설명: 사용자정의된모든간격마다 LDAP 서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: DNS 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- 설명: 사용자정의된모든간격마다 DNS 서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Google 스토어서버연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- 설명: 사용자정의된모든간격마다 Google 스토어서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Windows Phone 스토어연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.4.0
- 설명: 사용자정의된모든간격마다 Windows Phone 스토어서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Windows Tab 스토어연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- 설명: 사용자정의된모든간격마다 Windows Tab 스토어서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Windows 보안토큰서버연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- 설명: 사용자정의된모든간격마다 Windows 보안토큰서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Windows 알림서버연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- 설명: 사용자정의된모든간격마다 Windows 알림서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: APNs(Apple 푸시알림서버) 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- 설명: 사용자정의된모든간격마다 APNs 와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Apple 피드백서버연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- 설명: 사용자정의된모든간격마다 Apple 피드백서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Apple Store 서버연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.10.0

- 설명: 사용자정의된모든간격마다 Apple Store 서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: XenMobile 데이터베이스연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- 설명: 사용자정의된모든간격마다 XenMobile 데이터베이스와 XenMobile 노드사이의연결을모니터링합니다. 연결에 실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Firebase Cloud Messaging 서버연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- 설명: 사용자정의된모든간격마다 Firebase Cloud Messaging 서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: Citrix 라이선스서버연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- 설명: 사용자정의된모든간격마다 Citrix 라이선스서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: NetScaler Gateway 연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- 설명: 사용자정의된모든간격마다 NetScaler Gateway 와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: XenMobile 노드간연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- 설명: 사용자정의된모든간격마다 XenMobile 클러스터노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름: XenMobile Tomcat 노드서비스연결

- 모니터링 **OID(개체 ID):** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- 설명: 사용자정의된모든간격마다 XenMobile Tomcat 노드서비스와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

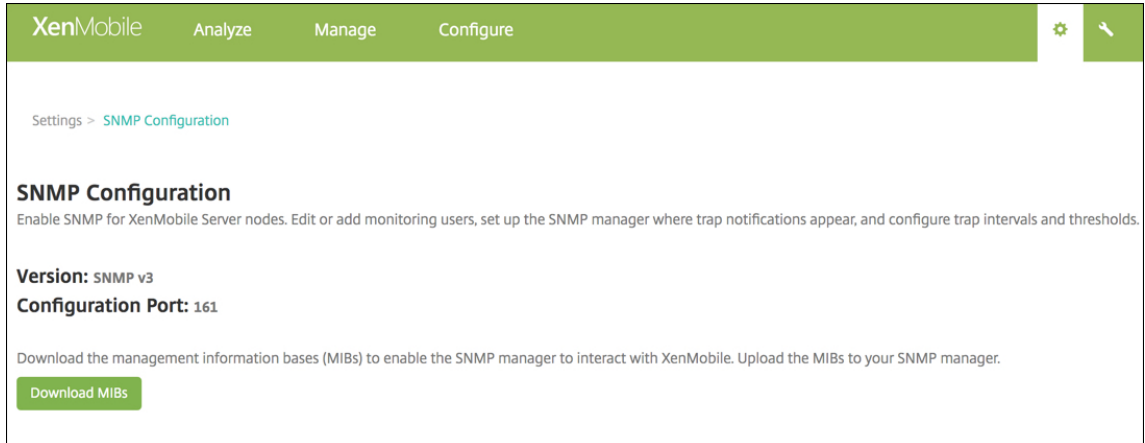
SNMP 임계값을구성할때최상의서버성능을유지하려면다음요인을고려하십시오.

- 호출빈도
- 수집할트랩데이터와임계값확인
- 노드간통신메커니즘
- 연결확인빈도
- 확인중실패에대한시간초과

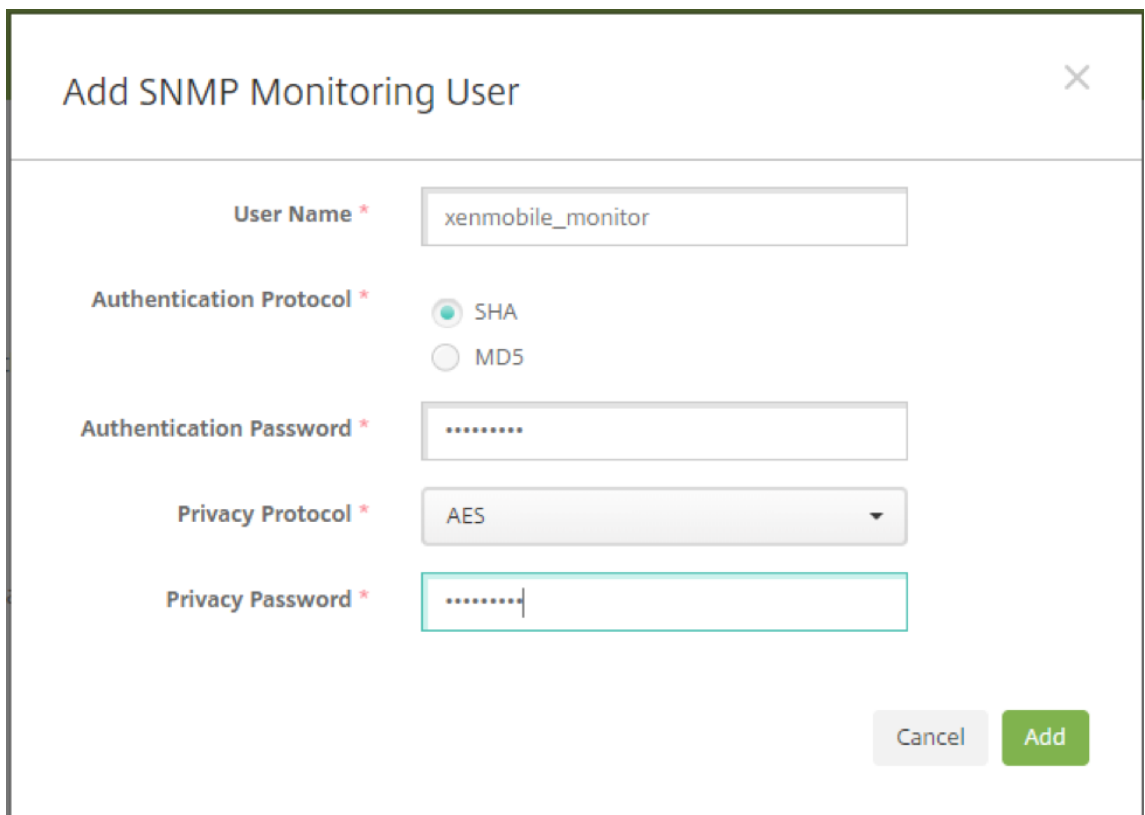
SNMP 사용자를추가하려면

SNMP 사용자는 SNMP 관리자와상호작용하고트랩을수신합니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 모니터링에서 **SNMP** 구성을클릭합니다. **SNMP** 구성페이지가나타납니다.



3. **SNMP** 모니터링사용자에서 추가를클릭합니다.
4. **SNMP** 모니터링사용자추가대화상자에서다음설정을구성합니다.



사용자이름: SNMP 관리자로로그온할때사용되는사용자이름입니다. 영숫자, 밑줄및하이픈을사용할수있지만공백과다

큰특수문자는사용자이름에서사용할수없습니다.

참고:

“xmsmonitor” 는 XenMobile 의내부사용을위해예약된이름이므로사용자이름으로추가할수없습니다.

인증프로토콜:

- **SHA**(권장)
- **MD5**

인증암호: 8~18 자의암호를입력합니다. 영숫자와특수문자를포함할수있습니다.

개인정보프로토콜:

- **DES**
- **AES 128**(권장)

개인정보암호: 8~18 자의암호를입력합니다. 영숫자와특수문자를포함할수있습니다.

SNMP 관리자를추가하려면

1. **SNMP** 관리자에서 추가를클릭합니다.
2. **SNMP** 관리자추가대화상자에서다음설정을구성합니다.

The screenshot shows a dialog box titled "Add SNMP Manager" with a close button in the top right corner. The dialog contains three input fields, each with an asterisk indicating it is required:

- Server IP Address ***: An empty text input field.
- Port ***: A text input field containing the value "162".
- SNMP User Name ***: A dropdown menu showing "xenmobile_monitor".

At the bottom right of the dialog, there are two buttons: a grey "Cancel" button and a green "Add" button.

서버 **IP** 주소: SNMP 관리자의 IP 주소를입력합니다.

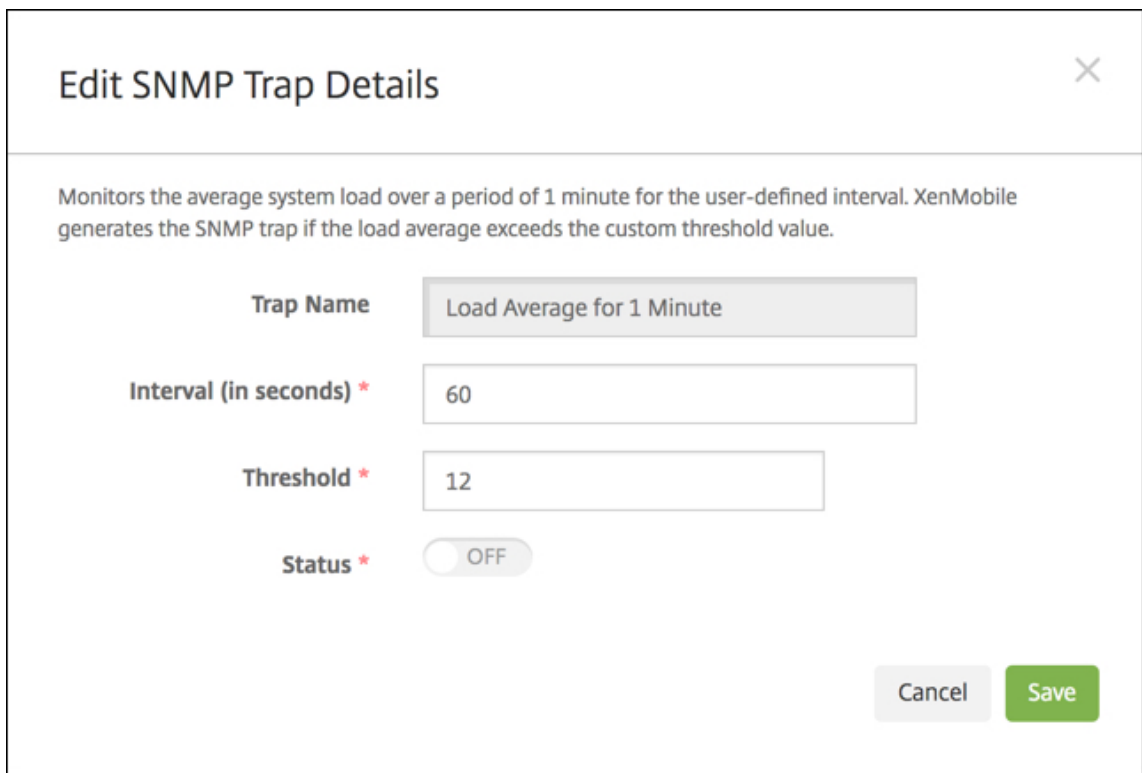
포트: 필요한경우포트번호를변경합니다. 기본값은 162 입니다.

SNMP 사용자이름: 관리자에액세스할수있는사용자이름을선택합니다.

SNMP 트랩을 사용하고 구성하려면

환경에 적합한 트랩 설정을 확인하려면 **확장성 및 성능**을 참조하십시오. 예를 들어 1 분 동안 XenMobile 로드 평균을 모니터링하려면 1 분 동안의 로드 평균을 사용하도록 설정하고 임계값을 입력합니다. XenMobile Server의 1 분 동안의 로드 평균이 지정된 임계값을 초과하면 구성된 SNMP 관리자에서 트랩을 수신합니다.

1. 개별 트랩을 사용하려면 다음 중 하나를 수행합니다.
 - 매개변수 옆의 확인란을 선택하고 **사용**을 클릭합니다.
 - 목록의 모든 트랩을 사용하려면 맨 위의 확인란을 선택하고 **사용**을 클릭합니다.
2. 트랩을 편집하려면 매개변수를 선택하고 **편집**을 클릭합니다.
3. **SNMP** 트랩 세부 정보 편집 대화 상자에서 개별 트랩의 임계값을 편집할 수 있습니다.



Edit SNMP Trap Details

Monitors the average system load over a period of 1 minute for the user-defined interval. XenMobile generates the SNMP trap if the load average exceeds the custom threshold value.

Trap Name Load Average for 1 Minute

Interval (in seconds) * 60

Threshold * 12

Status * OFF

Cancel Save

트랩 이름: 트랩의 이름입니다. 이 필드는 편집할 수 없습니다.

간격 (초): 60~86400(24 시간) 범위의 값을 사용할 수 있습니다.

임계값: 다음 트랩의 임계값만 변경할 수 있습니다.

- 프로세서 로드
- 1 분 동안의 로드 평균
- 5 분 동안의 로드 평균
- 15 분 동안의 로드 평균
- 사용 가능한 총 메모리
- 사용된 총 디스크 스토리지

- Java 힙메모리사용현황
- Java Metaspace 사용현황

상태: 트랩에 SNMP 모니터링을사용하려면 켜짐을선택합니다. 모니터링을사용하지않으려면 꺼짐을선택합니다.

SNMP 를사용한 XenMobile 모니터링에대한도움이되는정보를보려면이 [블로그게시물](#)을참조하십시오.

지원번들

January 6, 2020

Citrix 에문제를보고하거나문제를해결하려면지원번들을만듭니다. 그런다음지원번들을 CIS(Citrix Insight Services) 에업로드합니다.

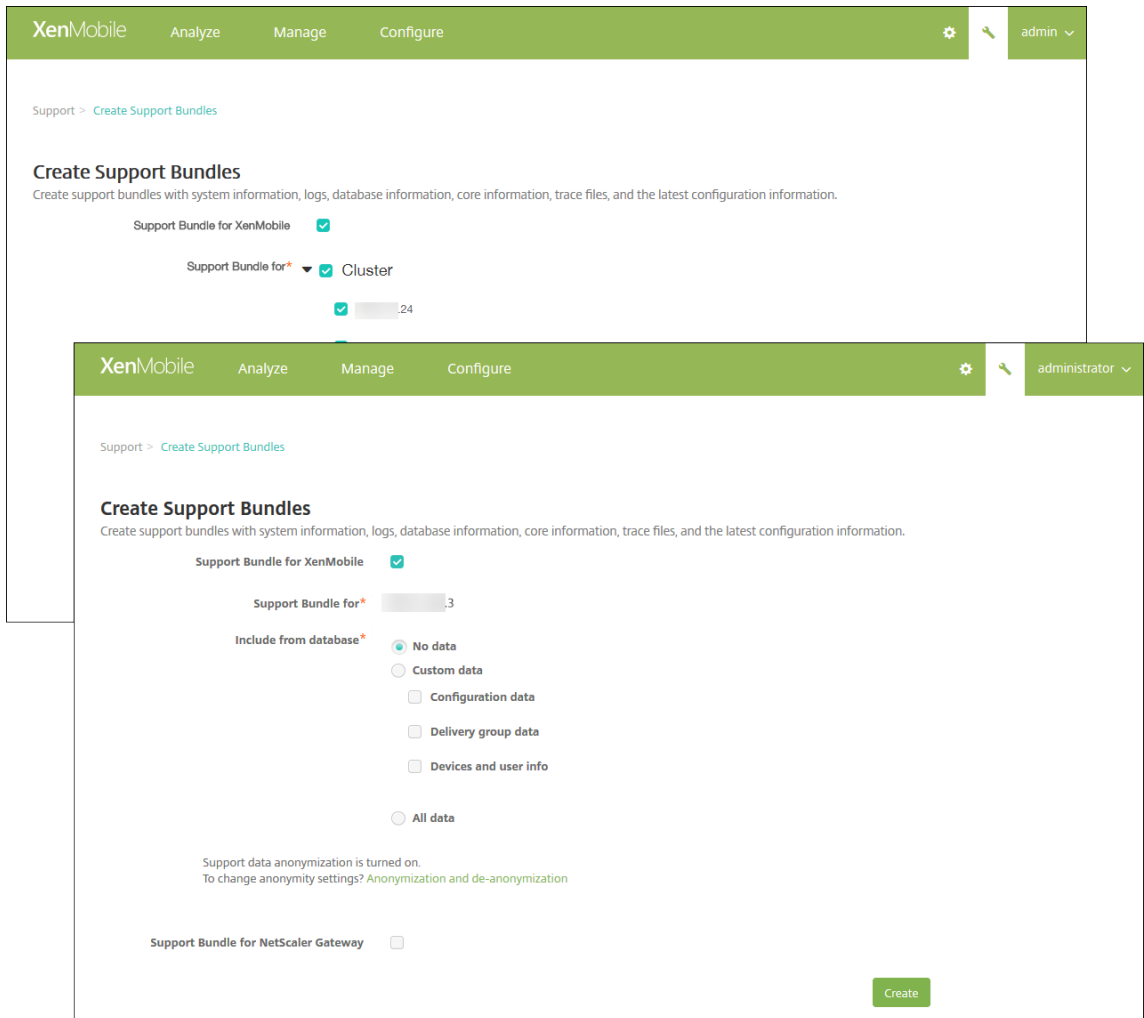
기본적으로지원번들에는다음파일에대한최대 100 개의백업아카이브가포함됩니다. 이러한파일의기본파일크기는 10MB 입니다.

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

지원번들에이러한각범주에대한 100 개의로그아카이브파일이포함되는경우로그파일이롤오버됩니다. 로그파일의최대수를이보다작게구성하면 XenMobile 이해당노드의추가로그파일을즉시삭제합니다. 로그파일수를구성하려면 문제해결및지원 > 로그설정으로이동합니다.

지원번들을만들려면:

1. XenMobile 콘솔에서오른쪽맨위의렌치아이콘을클릭합니다. 지원페이지가나타납니다.
2. 지원페이지에서 지원번들만들기를클릭합니다. 지원번들만들기페이지가나타납니다. XenMobile 환경에클러스터된노드가포함되는경우모든노드가표시됩니다.

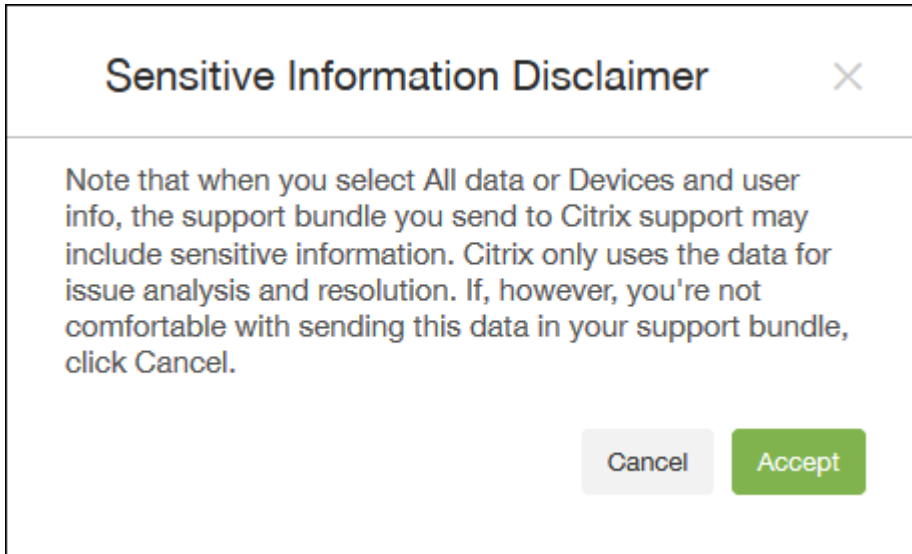


3. **XenMobile** 용지원번들확인란이선택되어있는지확인합니다.
4. XenMobile 환경에클러스터된노드가포함되는경우 다음을위한지원번들에서모든노드를선택하거나데이터를가져올노드 조합을선택할수있습니다.
5. 데이터베이스에서포함에서다음중하나를수행합니다.
 - 데이터없음을클릭합니다.
 - 사용자지정데이터를클릭합니다. 기본적으로이모든옵션이선택됩니다.
 - 구성데이터: 인증서구성및장치관리자정책이포함됩니다.
 - 배달그룹데이터: 앱유형및앱배달정책세부정보를포함한앱배달그룹정보가포함됩니다.
 - 장치및사용자정보: 장치정책, 앱, 동작및배달그룹이포함됩니다.
 - 모든데이터를클릭합니다.

참고:

장치및사용자정보또는 모든데이터를선택하고처음로지원번들을만든경우 중요한정보에대하고지사항대화상자가 나타납니다. 고지사항을읽고 동의또는 취소를클릭합니다. 취소를클릭하면지원번들을 Citrix 에업로드할수없습니

다. 동의클릭하면지원번들을 Citrix 에업로드할수있으며다음에장치또는사용자데이터가포함된지원번들을만들 때고지사항이표시되지않습니다.

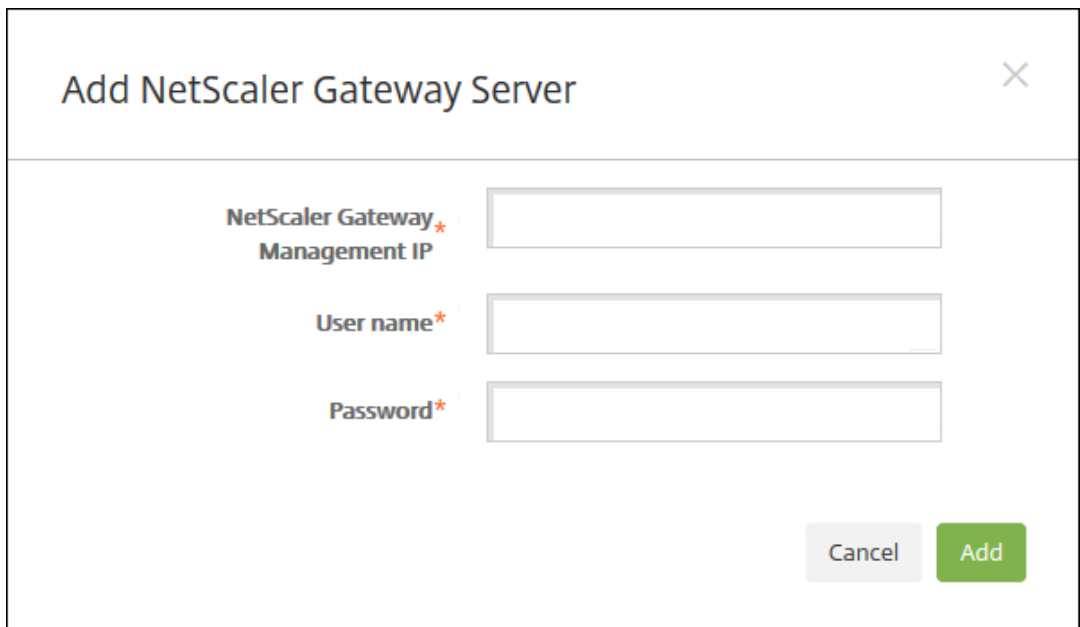


6. 지원데이터익명화가켜져있습니다다음은기본설정이데이터를익명화하는것임을나타냅니다. 데이터익명화는중요한사용자, 서버및네트워크데이터가지원번들에서익명으로표시되는것을의미합니다.

이설정을변경하려면 익명화및익명화취소를클릭합니다. 데이터익명화에대한자세한내용은 [지원번들의데이터익명화](#)를참조하십시오.

7. NetScaler Gateway 의지원번들을포함하려면: **NetScaler Gateway** 용지원번들확인란을선택하고다음을수행합니다.

a) 추가를클릭합니다. **NetScaler Gateway** 서버추가대화상자가나타납니다.



- b) **NetScaler Gateway** 관리 IP 에지원번들데이터를가져올 NetScaler Gateway 의 NetScaler 관리 IP 주소를입력합니다.

참고:

이미추가된 NetScaler Gateway 서버에서번들을만드는경우 IP 주소가입력됩니다.

- c) 사용자이름및 암호에 NetScaler Gateway 실행서버에액세스하는데필요한사용자자격증명을입력합니다.

참고:

이미추가된 NetScaler Gateway 서버에서번들을만드는경우사용자이름이입력됩니다.

8. 추가를클릭합니다. 새 NetScaler Gateway 지원번들이테이블에추가됩니다.
9. NetScaler Gateway 지원번들을추가하려면 7 단계를반복합니다.
10. **Create(만들기)** 를클릭합니다. 지원번들이만들어지고두개의새단추인 **CIS** 에업로드및 클라이언트에다운로드가나타납니다.

Citrix Insight Services 에지원번들업로드

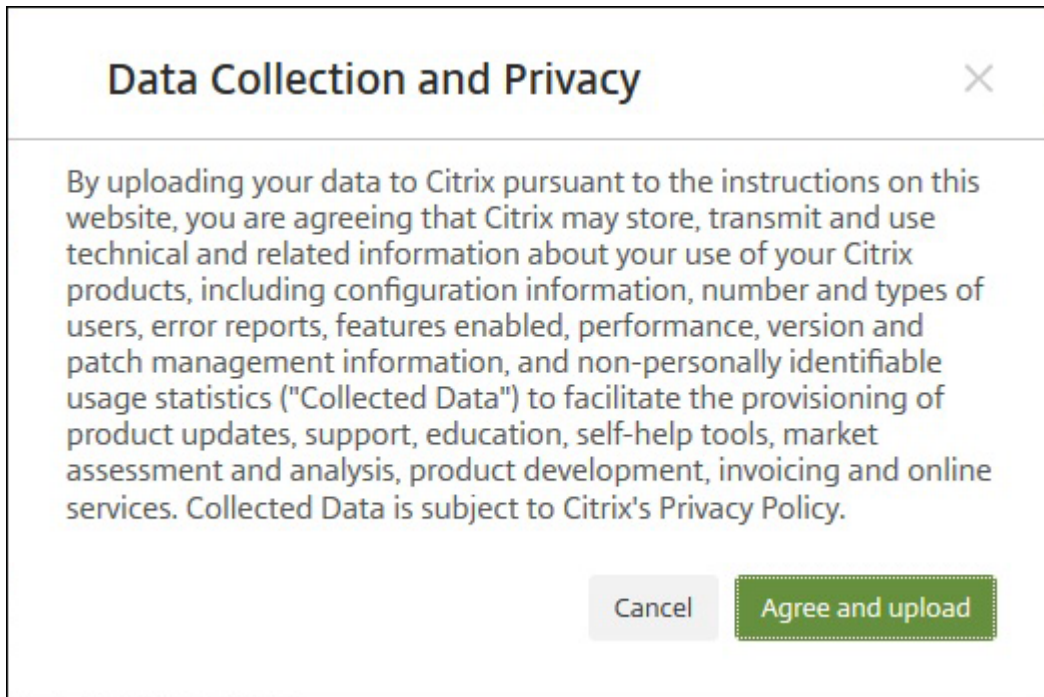
지원번들을만든후번들을 CIS(Citrix Insight Services) 에업로드하거나컴퓨터에다운로드할수있습니다.

XenMobile 에서 CIS 로의업로드에는 SSL 아웃바운드연결이사용됩니다. CIS 서버 IP 주소 (52.88.24.76, 52.88.118.220, 52.11.72.119) 에대해포트 443 을업니다. HTTPS 트래픽에대한프록시가있는경우해당프록시에서 CIS 서버 IP 주소에연결할수있는지확인하십시오.

다음단계는 CIS 에번들을업로드하는방법을보여줍니다. CIS 에업로드하려면 My Citrix ID 와암호가필요합니다.

1. 지원번들만들기페이지에서 **CIS** 에업로드를클릭합니다. **CIS(Citrix Insight Services)** 에업로드대화상자가나타납니다.
2. 사용자이름에 My Citrix ID 를입력합니다.
3. 암호에 My Citrix 암호를입력합니다.
4. 이번들을기존서비스요청번호에연결하려는경우 **SR#** 과연결확인란을선택하고표시되는두개의새로운필드에서다음을수행합니다.
 - **SR** 번호에이번들을연결할 8 자리서비스요청번호를입력합니다.
 - **SR** 설명에 SR 의설명을입력합니다.
5. 업로드를클릭합니다.

CIS 에지원번들을업로드한것이처음이고다른제품을통해 CIS 에계정을만들지않아데이터수집및개인정보계약에동의하지않은경우다음대화상자가나타납니다. 업로드를시작하려면계약에동의해야합니다. CIS 에계정이있고이전에계약에동의한경우지원번들이즉시업로드됩니다.



6. 계약을 읽고 동의및업로드를클릭합니다. 지원번들이업로드됩니다.

컴퓨터에지원번들다운로드

지원번들을만든후번들을 CIS 에업로드하거나컴퓨터에다운로드할수있습니다. 직접문제를해결하려는경우지원번들을컴퓨터에 다운로드합니다.

지원번들만들기페이지에서클라이언트에다운로드를클릭합니다. 번들이컴퓨터에다운로드됩니다.

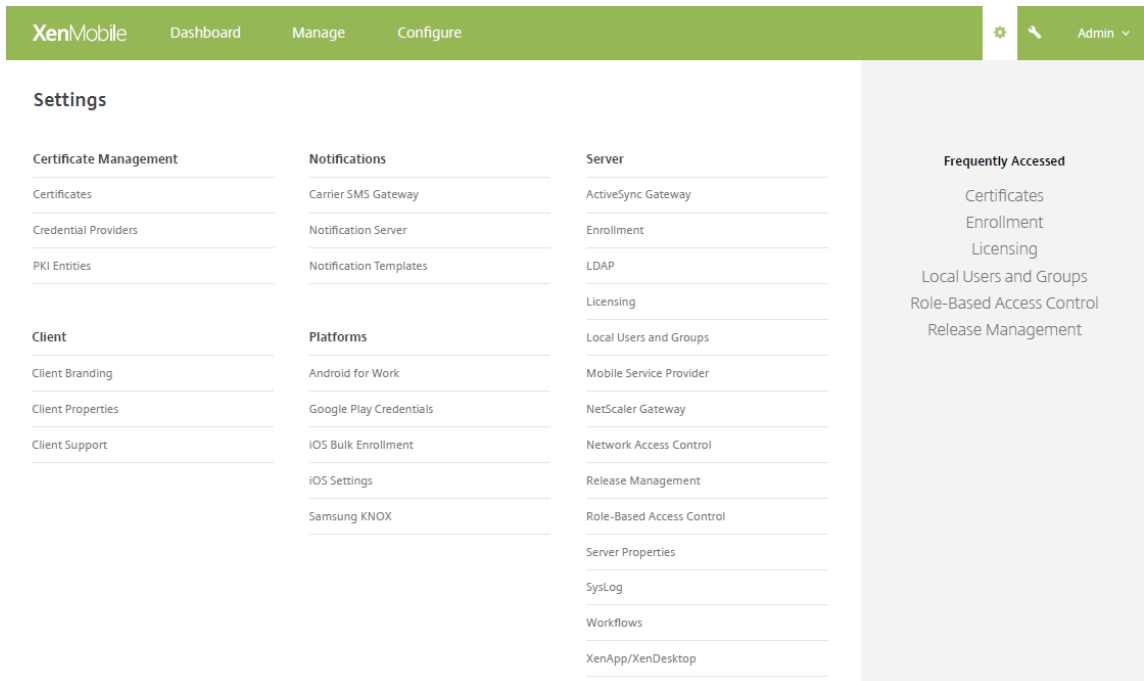
지원옵션및원격지원

January 6, 2020

사용자가지원담당자에게연락할수있도록전자메일주소를제공할수있습니다. 사용자가장치에서지원을요청하면전자메일주소가표시됩니다.

또한사용자가장치에서지원센터로로그를보내는방법도구성할수있습니다. 직접또는전자메일을사용하여로그를보내도록구성할수 있습니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.



2. 클라이언트에서 클라이언트지원을클릭합니다. 클라이언트지원페이지가나타납니다.

3. 다음설정을구성합니다.

- 지원전자메일 (**IT 지원센터**): IT 지원센터연락처의전자메일주소를입력합니다.
- 장치로그를 **IT** 지원센터에보내기: 장치로그를 직접보낼지아니면 전자메일로보낼지를선택합니다. 기본값은 전자 메일로입니다.
 - 직접을사용하면 ShareFile 에로그저장에대한설정이나타납니다. ShareFile 에로그저장을사용하는경우 ShareFile 로직접로그가전송됩니다. 그렇지않은경우 XenMobile 로전송된다음전자메일을통해지원센터 로전송됩니다. 또한기본적으로사용하도록설정되는 직접보내기가실패하면전자메일사용옵션이나타납니다. 클라이언트전자메일을사용하여서버문제에대한로그를전송하지않으려면이옵션을사용하지않을수있습니다. 그러나이옵션을사용하지않고서버문제가발생하면로그가전송되지않습니다.
 - 전자메일로를사용하면로그를전송할때클라이언트전자메일이항상사용됩니다.

4. 저장을클릭합니다.

원격지원

참고:

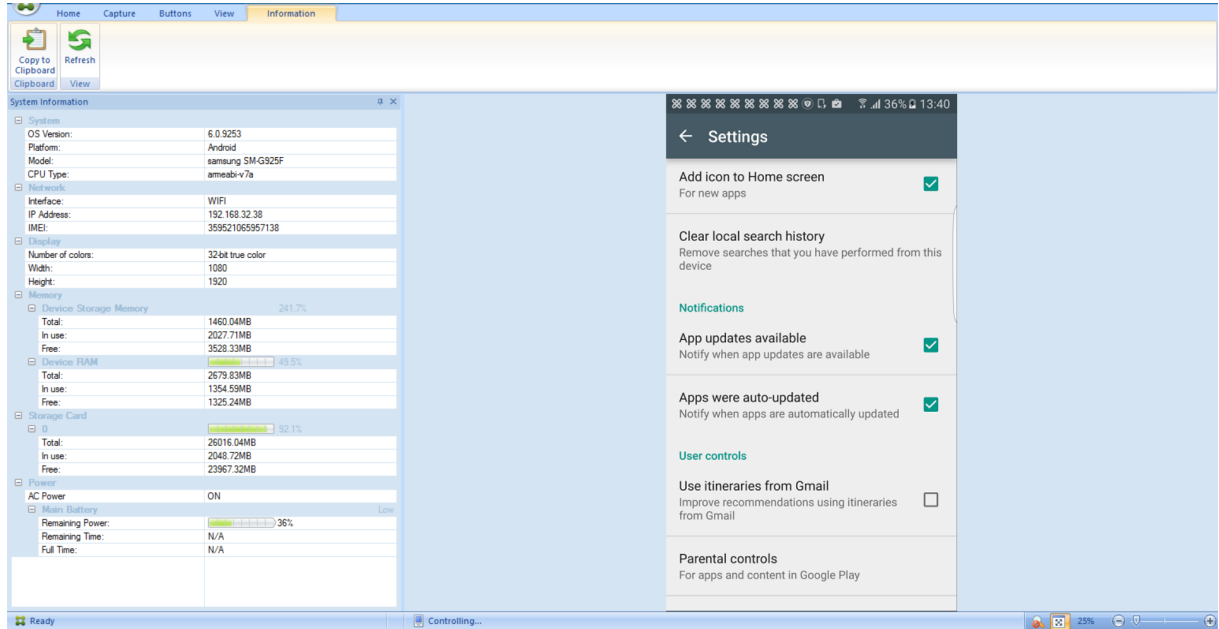
2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.

온-프레미스 XenMobile Server 배포의경우: 원격지원을사용하면지원센터담당자가관리되는 Windows CE 및 Android 모바일장치를원격으로제어할수있습니다. 스크린캐스트는 Samsung KNOX 장치에서만지원됩니다.

원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다.

원격제어세션중에:

- 사용자의 모바일 장치에 원격제어 세션이 활성화 상태임을 나타내는 아이콘이 표시됩니다.
- 원격지원 사용자는 원격지원 응용 프로그램 창과 원격제어 창에서 제어되는 장치의 렌더링을 볼 수 있습니다.



원격지원을 사용하여 다음을 수행할 수 있습니다.

- 사용자 장치에 원격으로 로그인하고 화면을 제어합니다. 사용자는 원격지원 담당자가 화면을 탐색하는 것을 지켜볼 수 있으며 이는 교육용으로 유용합니다.
- 원격 장치를 실시간으로 탐색하고 복구합니다. 구성을 변경하고, 운영체제 문제를 해결하고, 문제가 되는 앱 또는 프로세스를 사용하지 않도록 설정하거나 중지할 수 있습니다.
- 네트워크 액세스를 원격으로 사용하지 않도록 설정하고, 불법 프로세스를 중지하고, 앱 또는 맬웨어를 제거하여 위협이 다른 모바일 장치로 확산되기 전에 격리하고 억제합니다.
- 장치 벨소리를 원격으로 사용하도록 설정하고 전화를 걸어 사용자가 장치를 찾을 수 있도록 합니다. 사용자가 장치를 찾을 수 없는 경우 장치를 초기화하여 중요한 데이터가 손상되지 않도록 합니다.

또한 지원 담당자는 원격 지원을 사용하여 다음을 수행할 수 있습니다.

- 하나 이상의 XenMobile 인스턴스 내에서 연결된 모든 장치 목록을 표시합니다.
- 장치 모델, 운영체제 수준, IMEI(International Mobile Station Equipment Identity), 일련번호, 메모리 및 배터리 상태, 연결 등을 비롯한 시스템 정보를 표시합니다.
- XenMobile 의 사용자 및 그룹을 표시합니다.
- 활성 프로세스를 표시 및 종료하고 모바일 장치를 다시 시작할 수 있는 장치 작업 관리자를 실행합니다.
- 모바일 장치와 중앙 파일 서버 간의 양방향 파일 전송을 포함하는 원격 파일 전송을 실행합니다.
- 소프트웨어 프로그램을 일괄 처리로 하나 이상의 모바일 장치에 다운로드하고 설치합니다.
- 장치에서 원격 레지스트리 키 설정을 구성합니다.
- 실시간 장치 화면 원격제어를 사용하여 저대역폭 셀룰러 네트워크에서 응답 시간을 최적화합니다.
- 대부분의 모바일 장치 브랜드 및 모델에 대한 장치 스킨을 표시합니다. 스킨 편집기를 표시하여 새 장치 모델을 추가하고 물리적

를매핑합니다.

- 비디오 AVI 파일을 만드는 장치에서 일련의 상호작용을 캡처하는 기능을 통해 장치 화면 캡처, 녹화 및 재생을 사용하도록 설정합니다.
- 모바일 사용자와 지원 직원 간에 공유 화이트보드, VoIP 기반 음성 통신 및 채팅을 사용하여 라이브 모임을 수행합니다.

원격 지원 시스템 요구 사항

원격 지원 소프트웨어는 다음 요구 사항을 충족하는 Windows 기반 컴퓨터에 설치됩니다. 포트 요구 사항은 [포트 요구 사항](#)을 참조하십시오.

지원되는 플랫폼:

- Intel Xeon/Pentium 4 -1GHz 워크스테이션급 이상
- 512MB RAM 이상
- 최소 100MB 디스크 여유 공간

지원되는 운영 체제:

- Microsoft Windows 2003 Server Standard Edition 또는 Enterprise Edition SP1 이상
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 이상
- Microsoft Windows Vista SP1 이상
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

원격 지원 소프트웨어를 설치하려면

1. 원격 지원 설치 프로그램을 다운로드하려면 [XenMobile 10 다운로드 페이지](#)로 이동하고 계정에 로그인합니다.
2. **Tools(도구)**를 확장한 후 XenMobile Remote Support v9 를 다운로드합니다.
원격 지원 파일 이름은 XenMobileRemoteSupport-9.0.0.35265.exe 입니다.
3. 원격 지원 설치 프로그램을 두 번 클릭한 후 설치 마법사의 지침을 따릅니다.

명령줄에서 원격 지원을 설치하려면

다음 명령을 실행합니다.

```
1 \*RemoteSupport\*.exe /S
```

RemoteSupport 는 설치 프로그램의 이름입니다. 예를 들면 다음과 같습니다.

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

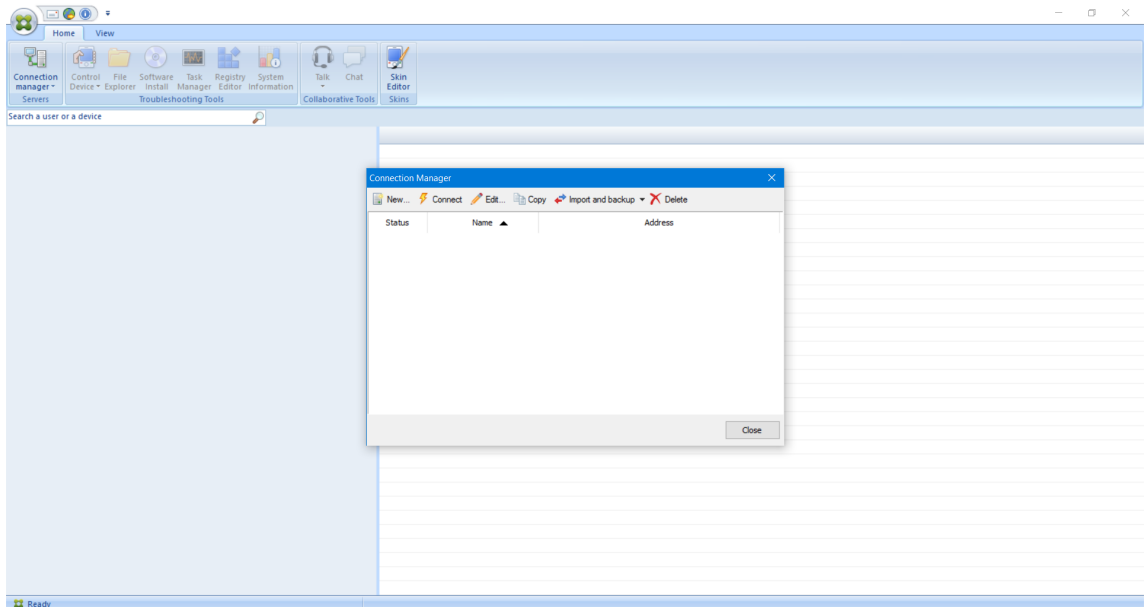
원격지원소프트웨어를설치할때다음변수를사용할수있습니다.

- /S: 기본매개변수를사용하여자동으로원격지원소프트웨어를설치합니다.
- /D=dir: 사용자지정설치디렉터리를지정합니다.

원격지원을 **XenMobile** 에연결하려면

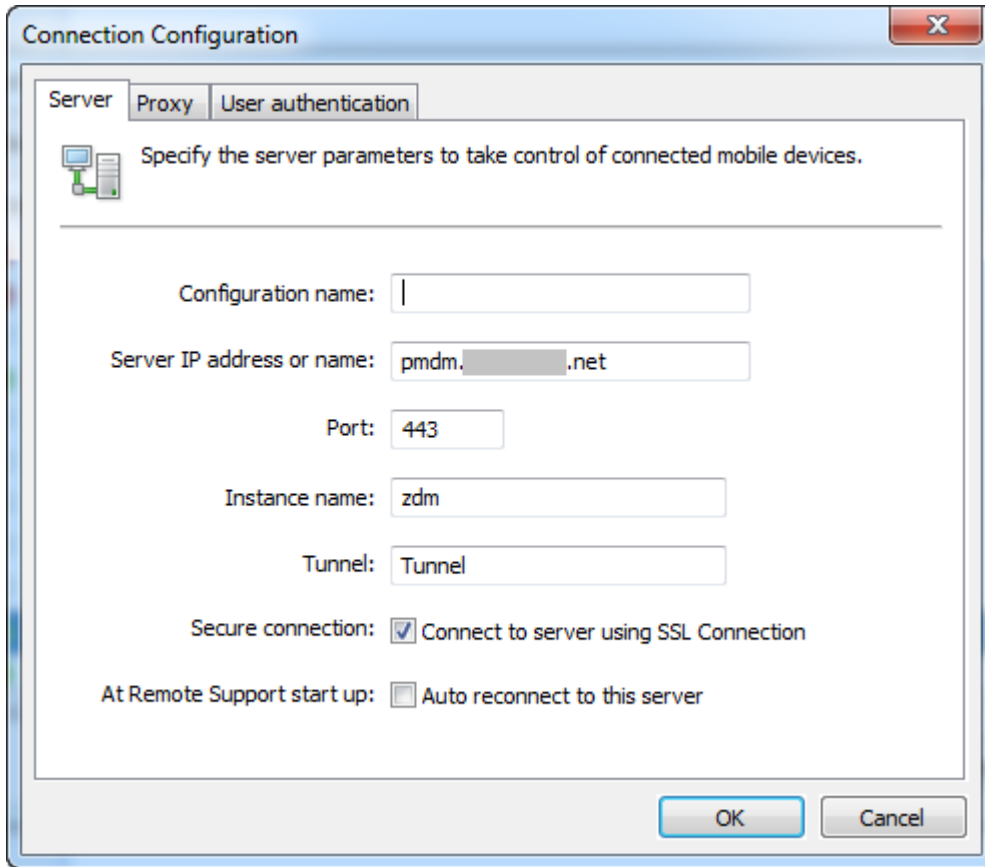
관리되는장치에대한원격지원연결을설정하려면장치를관리하는하나이상의 XenMobile Server 에원격지원의연결을추가해야 합니다. 이러한연결은 Android 및 Windows Mobile/CE 장치에대한장치정책인터널 MDM 정책에서정의한애플터널을통해 실행됩니다. 원격지원을 XenMobile 에연결하려면먼저애플터널을정의해야합니다. 자세한내용은 [애플터널링장치정책](#)에서참조하십시오.

1. 원격지원소프트웨어를시작하고 XenMobile 자격증명을사용하여로그온합니다.
2. **Connection Manager**(연결관리자) 에서 **New**(새로만들기) 를클릭합니다.

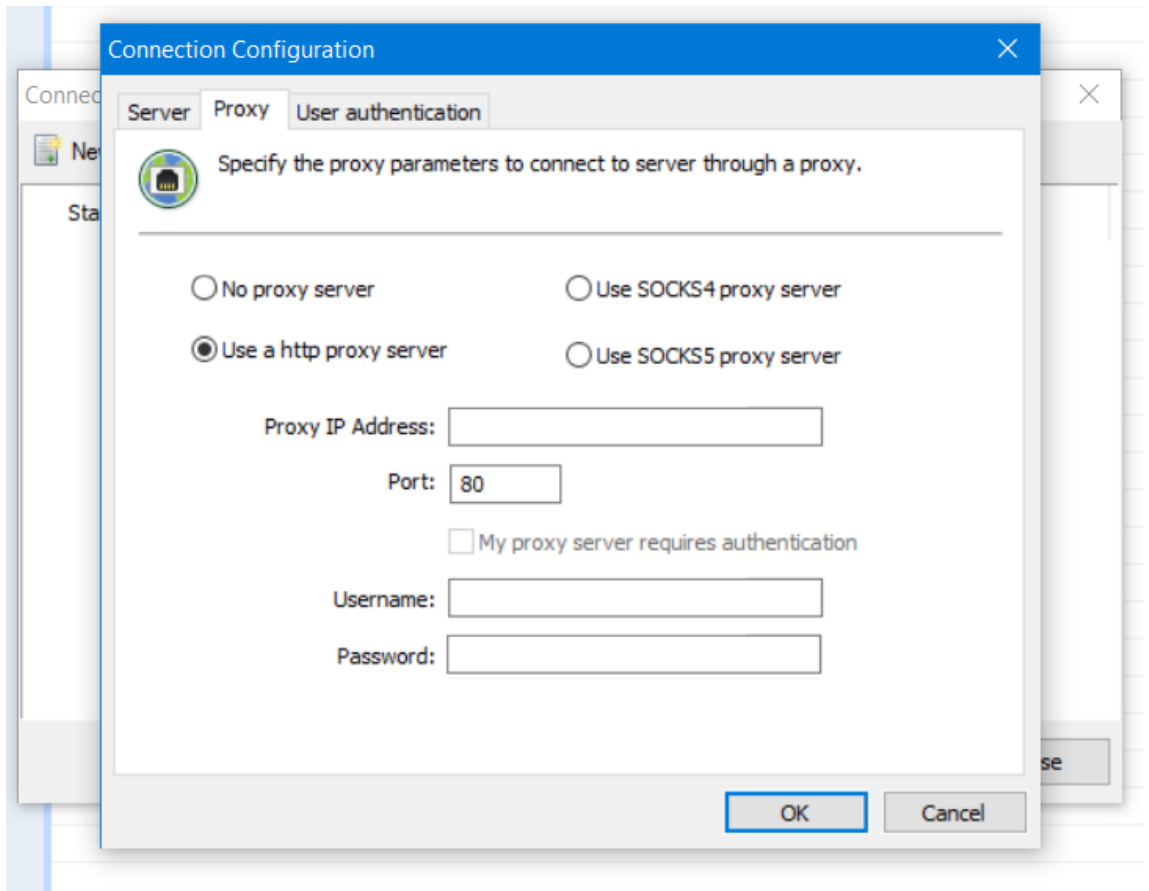


3. **Connection Configuration**(연결구성) 대화상자의 **Server**(서버) 탭에다음값을입력합니다.
 - a) **Configuration name**(구성이름) 에구성항목의이름을입력합니다.
 - b) **Server IP address or name**(서버 IP 주소또는이름) 에 XenMobile Server 의 IP 주소또는 DNS 이름을입력합니다.
 - c) **Port**(포트) 에 XenMobile Server 구성에서정의한 TCP 포트번호를입력합니다.
 - d) XenMobile 이다중테넌트배포에포함되는경우 **Instance name**(인스턴스이름) 에인스턴스이름을입력합니다.
 - e) **Tunnel**(터널) 에터널정책의이름을입력합니다.
 - f) **Connect to server using SSL Connection**(SSL 연결을사용하여서버에연결) 확인란을선택합니다.

- g) 원격지원응용프로그램을 시작할때마다 구성된 XenMobile Server 에 연결하려면 **Auto reconnect to this server(이 서버에 자동으로 다시 연결)** 확인란을 선택합니다.



4. **Proxy(프록시)** 탭에서 **Use a http proxy server(http 프록시서버사용)** 를 선택하고 다음 정보를 입력합니다.
- Proxy IP Address(프록시 IP 주소)** 에 프록시서버의 IP 주소를 입력합니다.
 - Port(포트)** 에 프록시에서 사용하는 TCP 포트번호를 입력합니다.
 - 프록시서버에 트래픽 허용을 위한 인증이 필요한 경우 **My proxy server requires authentication(내 프록시서버에 인증 필요)** 확인란을 선택합니다.
 - Username(사용자 이름)** 에 프록시서버에서 인증할 사용자 이름을 입력합니다.
 - Password(암호)** 에 프록시서버에서 인증할 암호를 입력합니다.



5. **User Authentication(사용자인증)** 탭에서 **Remember my login and password(로그인및암호저장)** 확인란을선택하고자격증명을입력합니다.

6. **OK(확인)** 를클릭합니다.

XenMobile 에연결하려면이전에만든연결을두번클릭한후연결에대해구성한사용자이름과암호를입력합니다.

Samsung KNOX 장치에대해원격지원을사용하려면

XenMobile 에서 Samsung KNOX 장치에대한원격액세스를제공하는원격지원정책을만듭니다. 두가지유형의지원을구성할수있습니다.

- **기본:** 장치에대한진단정보를볼수있습니다. 예를들어시스템정보, 실행중인프로세스, 작업관리자 (메모리및 CPU 사용량), 설치된소프트웨어폴더내용등을볼수있습니다.
- **프리미엄:** 원격으로장치화면을제어할수있습니다. 예를들어창색상을제어하고, 지원센터와사용자간의 VoIP 세션을설정하고, 지원센터와사용자간의채팅세션을설정할수있습니다.

프리미엄지원을사용하려면 XenMobile 콘솔에서 Samsung MDM 라이선스키장치정책을구성해야합니다. 이정책을구성하는경우 **Samsung KNOX** 플랫폼만선택합니다. SAFE 플랫폼의경우 Samsung 장치가 XenMobile 에등록될때 ELM 키가자동으로배포됩니다. 따라서이정책에는 Samsung SAFE 플랫폼을선택하지마십시오. 자세한내용은 [Samsung MDM 라이선스키](#)에서참조하십시오.

원격지원정책구성에대한자세한내용은 [원격지원장치정책](#)을참조하십시오.

원격지원세션을사용하려면

원격지원을시작하면원격지원응용프로그램창의왼쪽에 XenMobile 콘솔에서정의한 XenMobile 사용자그룹이표시됩니다. 기본적으로현재연결된사용자를포함하는그룹만표시됩니다. 사용자항목옆에서각사용자의장치를볼수있습니다.

1. 모든사용자를보려면왼쪽옆에서각그룹을확장합니다.
현재 XenMobile Server 에연결된사용자는녹색아이콘으로표시됩니다.
2. 현재연결되지않은사용자를포함한모든사용자를표시하려면 **View(보기)** 를클릭하고 **Non-connected devices(연결되지않은장치)** 를선택합니다.
작은녹색아이콘이없는연결되지않은사용자가표시됩니다.

XenMobile Server 에연결되었지만사용자에게할당되지않은장치는익명모드로표시됩니다. 목록에 **Anonymous(익명)** 문자열이표시됩니다. 이러한장치는로그인한사용자의장치와같은방법으로제어할수있습니다.

장치를제어하려면장치행을클릭한후 **Control Device(장치제어)** 를클릭하여장치를선택합니다. Remote Control(원격제어) 창에장치렌더링이나타납니다. 제어되는장치와다음과같은방법으로상호작용할수있습니다.

- 주창또는개별적인부동창에서색상제어를포함하여장치화면을제어합니다.
- 지원센터와사용자간의 VoIP 세션을설정합니다. VoIP 설정을구성합니다.
- 사용자와의채팅세션을설정합니다.
- 장치작업관리자에엑세스하여메모리사용량, CPU 사용량및실행중인앱과같은항목을관리합니다.
- 모바일장치의로컬디렉터리를탐색합니다. 파일을전송합니다.
- Windows 모바일장치의장치레지스트리를편집합니다.
- 장치시스템정보및설치된모든소프트웨어를표시합니다.
- 모바일장치와 XenMobile Server 의연결상태를업데이트합니다.

SysLog

January 6, 2020

시스템로그 (syslog) 서버에로그파일을보내도록 XenMobile Server(온-프레미스) 를구성할수있습니다. 서버호스트이름또는 IP 주소가필요합니다.

Syslog 는장비에서실행되는감사모듈과원격시스템에서실행될수있는서버라는두가지구성요소가있는표준로그프로토콜입니다. Syslog 프로토콜에서는데이터전송에 UDP(User Datagram Protocol) 를사용합니다. 관리자이벤트및사용자이벤트가기록됩니다.

다음과같은유형의정보를수집하도록서버를구성할수있습니다.

- XenMobile 에서수행한동작의레코드가포함된시스템로그
- XenMobile 의시스템작업을시간순으로기록한감사로그

syslog 서버가장비에서수집하는로그정보는메시지형태로로그파일에서저장됩니다. 이러한메시지에는대개다음과같은정보가포함됩니다.

- 로그메시지를생성한장비의 IP 주소
- 타임스탬프
- 메시지유형
- 이벤트와관련된로그수준 (중요, 오류, 알림, 경고, 정보, 디버그, 경보또는긴급)
- 메시지정보

XenMobile 은 log4j syslog 어펜더를사용하여 RFC5424 형식의 syslog 메시지를전송합니다. syslog 메시지의메시지데이터는특정형식이없는일반텍스트입니다.

이정보를사용하여경고출처를분석하고필요한경우교정조치를취할수있습니다.

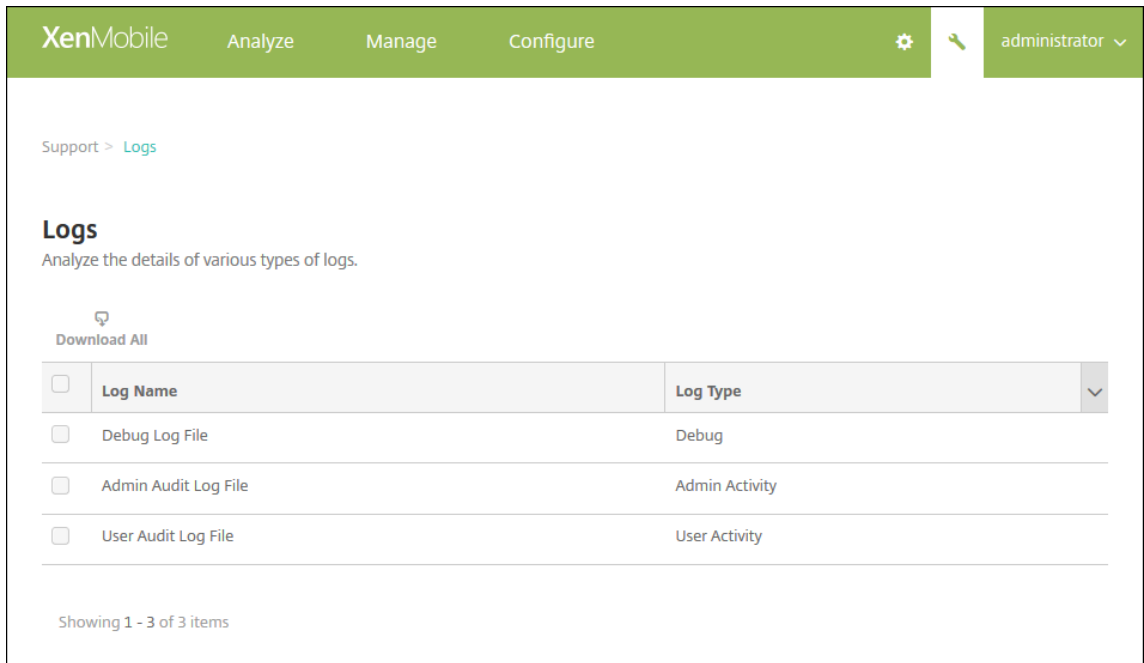
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. **Syslog** 를클릭합니다. **Syslog** 페이지가나타납니다.
3. 다음설정을구성합니다.
 - 서버: syslog 서버의 IP 주소또는 FQDN(정규화된도메인이름) 을입력합니다.
 - 포트: 포트번호를입력합니다. 기본적으로포트는 514 로설정됩니다.
 - 로깅할정보: 시스템로그및 감사를선택하거나선택취소합니다.
 - 시스템로그는 XenMobile 에서수행한동작을포함합니다.
 - 감사로그는 XenMobile 의시스템작업을시간순으로기록한레코드를포함합니다.
 - XenMobile 의디버그로그
4. 저장을클릭합니다.

XenMobile 에서로그파일보기

January 6, 2020

XenMobile 을사용한관리에도움이되는로그를보고조작하고다운로드할수있습니다.

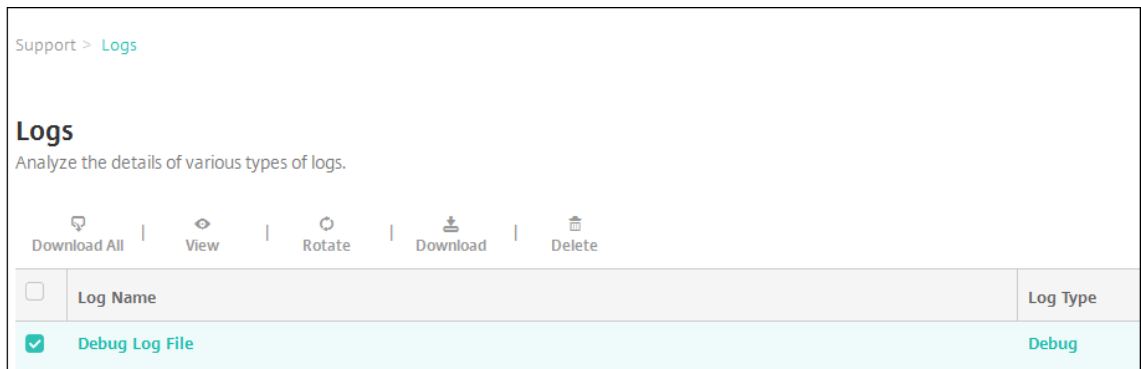
1. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다. 지원페이지가열립니다.
2. 로그작업아래에서 로그를클릭합니다. 로그페이지가나타납니다. 개별로그가테이블에표시됩니다.



3. 보려는로그를선택합니다.

- 디버그로그파일오류메시지, 서버관련동작등 Citrix 지원에대한유용한정보가들어있습니다.
- 관리자감사로그파일에는 XenMobile 콘솔작업에대한감사정보가포함되어있습니다.
- 사용자감사로그파일에는구성된사용자와관련된정보가포함되어있습니다.

4. 테이블상단에있는모두다운로드, 보기, 순환, 단일로그다운로드또는선택한로그삭제동작을수행합니다.



참고:

- 여러개의로그파일을선택하는경우 모두다운로드와 순환만사용할수있습니다.
- XenMobile 서버를클러스터링한경우연결된서버에대한로그만볼수있습니다. 다른서버에대한로그를보려면 다운로드옵션중하나를사용합니다.

5. 다음중하나를수행합니다.

- 모두다운로드: 시스템에있는모든로그 (디버그, 관리자감사, 사용자감사, 서버로그등) 가다운로드됩니다.
- 보기: 테이블아래에선택한로그내용이표시됩니다.

- **순환:** 현재로그파일이보관되고로그항목을캡처할새파일이생성됩니다. 로그파일을보관하는경우대화상자가나타납니다. 계속하려면순환을클릭합니다.
- **다운로드:** 선택한로그파일형식하나만다운로드되고동일한형식의보관된로그만다운로드됩니다.
- **삭제:** 선택한로그파일을영구적으로제거합니다.

Logs
Analyze the details of various types of logs.

Download All | View | Rotate | Download | Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```

2016-11-06T06:28:38.908-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:29:38.926-0800 | INFO | node.scheduled.executor-10 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:30:38.762-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | Begin method executeNonPrvsnTask(job: Sun Nov 06 06:45:38 PST 2016
2016-11-06T06:30:38.766-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | The number of non provision tasks Picked 2
2016-11-06T06:30:38.945-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:31:38.965-0800 | INFO | node.scheduled.executor-9 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:32:38.995-0800 | INFO | node.scheduled.executor-4 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:33:39.3-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:34:39.24-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:35:39.42-0800 | INFO | node.scheduled.executor-5 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:36:39.592-0800 | INFO | node.scheduled.executor-11 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
                
```

XenMobile Analyzer 도구

January 6, 2020

XenMobile Analyzer 는 XenMobile 의구성및타기능관련문제를진단하고해결하는데사용할수있는클라우드기반도구입니다. 이도구는 XenMobile 환경내의장치또는사용자등록및인증문제를검사합니다.

XenMobile Server 를가리키도록도구를구성하고서버배포형, 모바일플랫폼, 인증유형및사용자자격증명과같은정보를제공해야합니다. 그러면도구가서버에연결하고환경을검사하여구성문제를확인합니다. XenMobile Analyzer 에의해문제가검색되면문제해결을위한권장사항이제공됩니다.

주요기능

- 모든 XenMobile 관련문제를해결하는안전한클라우드기반의마이크로서비스입니다.
- XenMobile 구성문제를해결하는정확한권장사항입니다.
- 지원요청을줄이고 XenMobile 환경의문제해결을가속화합니다.
- XenMobile Server 릴리스에대한즉각적인지원입니다.
- 일별또는주별로상태확인을예약합니다.
- NetScaler 구성을확인합니다.
- Secure Web 테스트를통해인트라넷사이트연결가능성을확인합니다.
- Secure Mail 자동검색서비스를확인합니다.

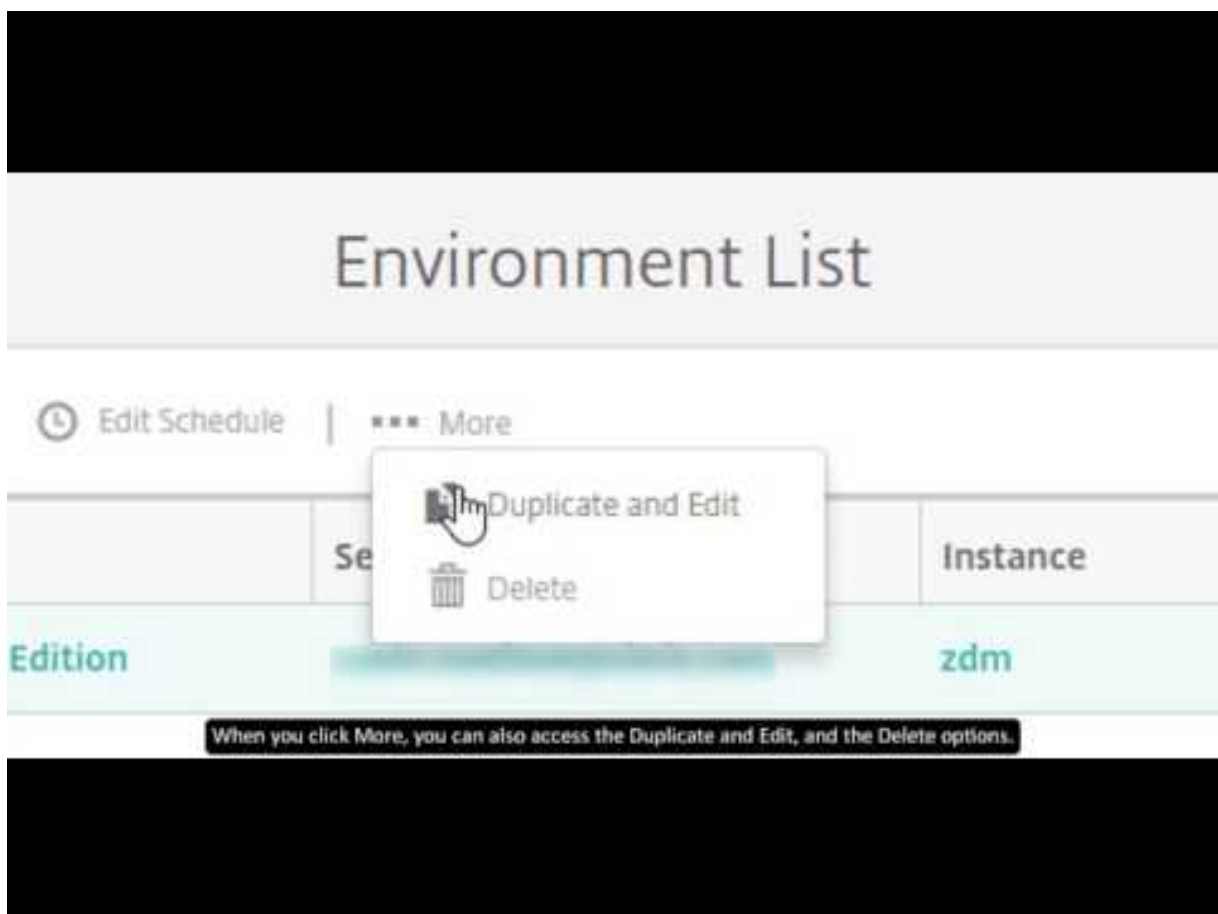
- ShareFile SSO(Single Sign-On) 를확인합니다.

새로운항목

- NetScaler 구성보고서에권장사항의수를나타내는배지알림이표시됩니다. 권장사항은특정 NetScaler Gateway 에 대한 Essential Configuration 확인을기반으로합니다.
- 테스트환경목록페이지의글로벌탐색모음내에있는아이콘이더나은사용자환경을위해재정렬되었습니다.

다음비디오는사용자인터페이스의탐색변경사항을중점적으로설명합니다.

Citrix XenMobile Analyzer: New Environment List UI(새로운환경목록 UI)



참고:

이비디오에는오디오사운드가없습니다. 전체화면모드에서가장잘보입니다.

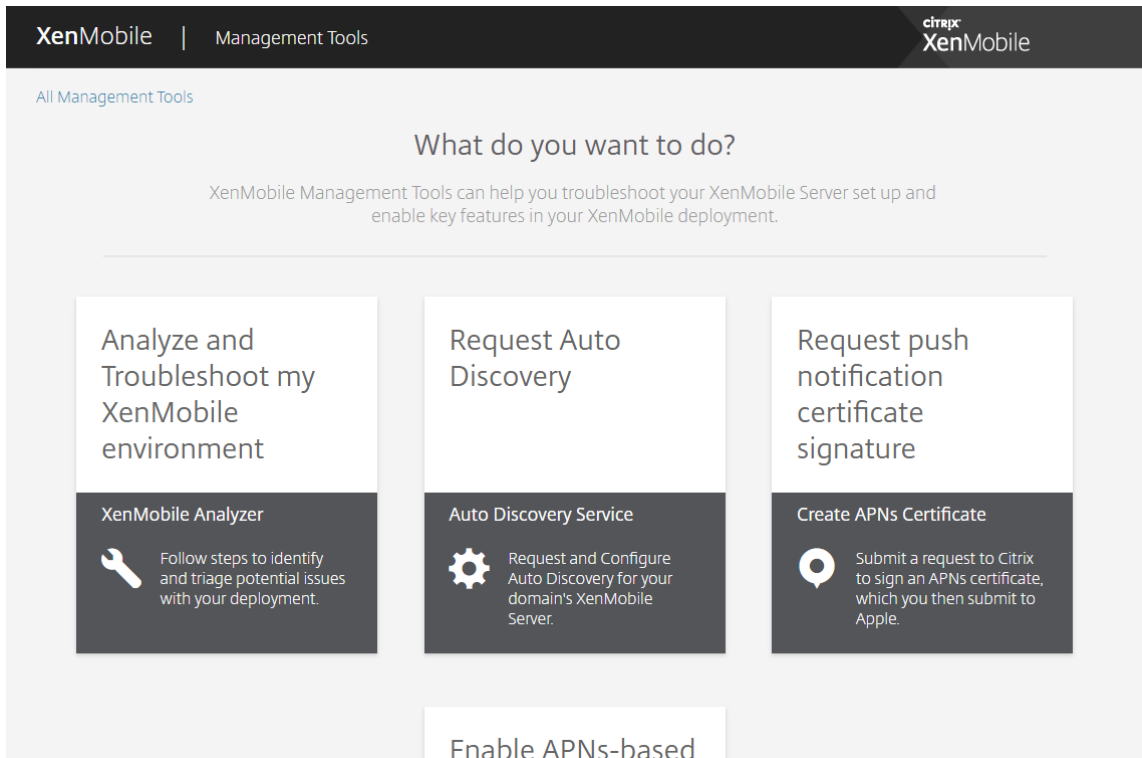
XenMobile Analyzer 액세스및시작

사전요구사항

제품	지원되는버전
XenMobile Server	10.1.0 이상
NetScaler Gateway	10.5 이상
Client Enrollment Simulation	iOS 및 Android

다음방법중하나를사용하여 XenMobile Analyzer 에액세스합니다.

- XenMobile 콘솔에서오른쪽맨위의렌치아이콘을클릭하여 문제해결및지원페이지를열니다.
- <https://xenmobiletools.citrix.com>에서 My Citrix 자격증명을 사용하여도구에액세스합니다. XenMobile Management Tools 페이지에서 XenMobile Analyzer 를 시작하려면 **Analyze and Troubleshoot my XenMobile Environment(내 XenMobile 환경분석및문제해결)** 를클릭합니다.



XenMobile Analyzer 에는분류프로세스를통해지원티켓의수를줄이도록설계된 5 개옵션이포함되어있습니다. 이옵션을사용하면모든사용자의비용을낮출수있습니다.

옵션은다음과같습니다.

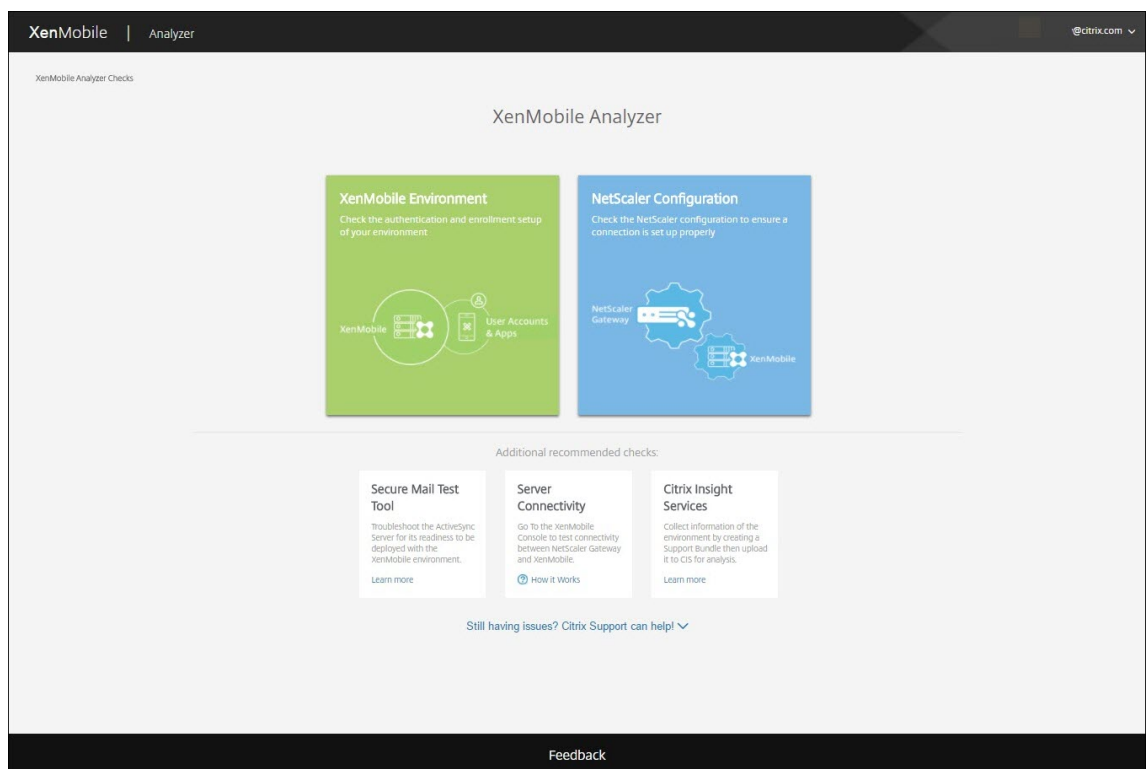
- **Environment Check(환경검사):** 이단계는설정을검사하여문제를확인하는테스트를안내합니다. 또한장치, 사용자 등록및인증문제에대한권장사항및해결방법도제공합니다.
- **NetScaler Check(NetScaler 확인):** 이단계는 NetScaler 구성의 XenMobile 배포준비상태를확인하는과정을 안내합니다.

- **Advanced Diagnostics(고급진단):** 이단계는 Citrix Insight Services 를 사용하여환경검사에서놓친추가문제를 찾는방법에대한정보를제공합니다.
- **Server Connectivity Checks(서버연결확인):** 이단계는서버연결을테스트하는데필요한지침을제공합니다.
- **Contact Citrix support(Citrix 지원문의):** 여전히문제가해결되지않는경우이단계의링크를통해 Citrix 지원사례 를만들수있는사이트로이동할수있습니다.

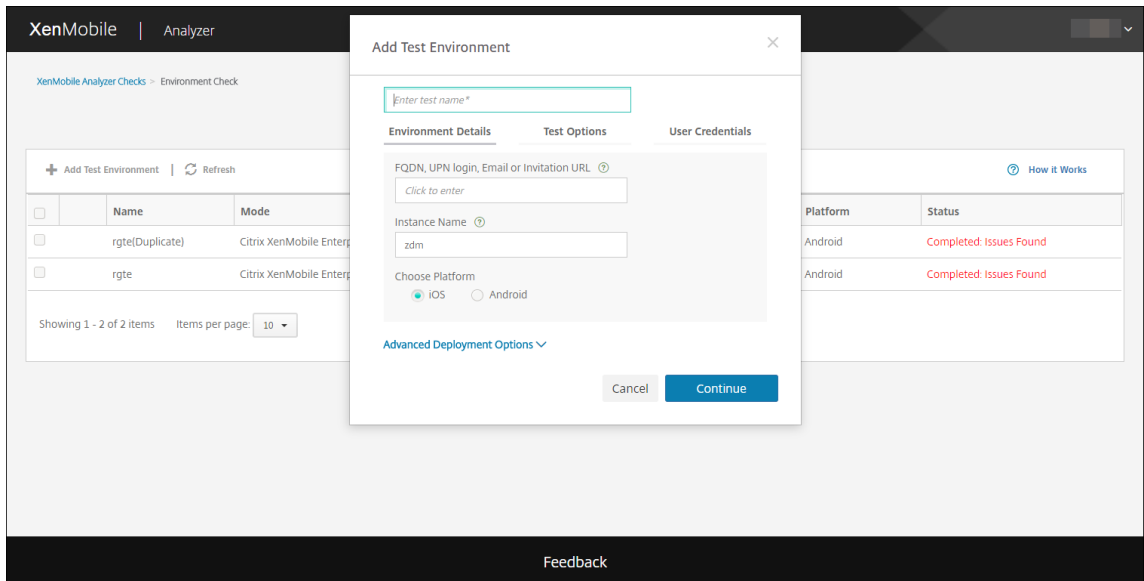
다음섹션에서는각옵션을보다자세히설명합니다.

환경검사수행

1. XenMobile Analyzer 에로그온한후 **XenMobile Environment(XenMobile 환경)** 를클릭합니다.



2. **Add Test Environment(테스트환경추가)** 를클릭합니다.
3. 새 **Add Test Environment(테스트환경추가)** 대화상자에서다음을수행합니다.



- a) 나중에테스트를식별하는데도움이되는고유한테스트이름을입력합니다.
 - b) **FQDN, UPN login(UPN 로그인), Email(전자메일) 또는 URL Invitation(URL 초대)** 에서버백세스에 사용되는정보를입력합니다.
 - c) 사용자지정인스턴스를사용하는경우 **Instance Name(인스턴스이름)** 에해당값을입력할수있습니다.
 - d) **Choose Platform(플랫폼선택)** 에서 **iOS** 또는 **Android** 를테스트플랫폼으로선택합니다.
 - e) **Advanced Deployment Options(고급배포옵션)** 을확장하면 **Deployment Mode(배포모드)** 목록에서 XenMobile 배포모드를선택할수있습니다 1. 사용가능한옵션은 **Enterprise (MDM + MAM)(엔터프라이즈 (MDM + MAM)), App Management (MAM)(앱관리 (MAM))** 또는 **Device Management (MDM)(장치관리 (MDM))** 입니다.
 - f) **Continue(계속)** 를클릭합니다.
4. **Test Options(테스트옵션)** 탭에서다음테스트중하나이상을선택하고 **Continue(계속)** 를클릭합니다.
- a) **Secure Web Connectivity(Secure Web 연결).** 인트라넷 URL 을입력합니다. URL 의연결가능성이테스트됩니다. 이테스트는 Secure Web 앱에서인트라넷 URL 에연결을시도하는동안발생할수있는잠재적연결문제를감지합니다.
 - b) **Secure Mail ADS.** 사용자전자메일 ID 를입력합니다. 이 ID 는 XenMobile 환경에서 Microsoft Exchange Server 의자동검색을테스트하는데사용됩니다. 이테스트는 Secure Mail Auto Discovery 와관련된모든문제를감지합니다.
 - c) **ShareFile SSO.** 선택할경우 XenMobile Analyzer 는 ShareFile DNS 확인이제대로수행되는지테스트합니다. 또한도구는 ShareFile SSO(Single Sign-On) 가제공된사용자자격증명과호환되는지확인합니다.

testdev02

Environment Details **Test Options** User Credentials

Apps connectivity testing (optional)

Secure Web connectivity ? ShareFile SSO ?

(https|http)://url:port

Secure Mail ADS ?

Enter your email address

Back Continue

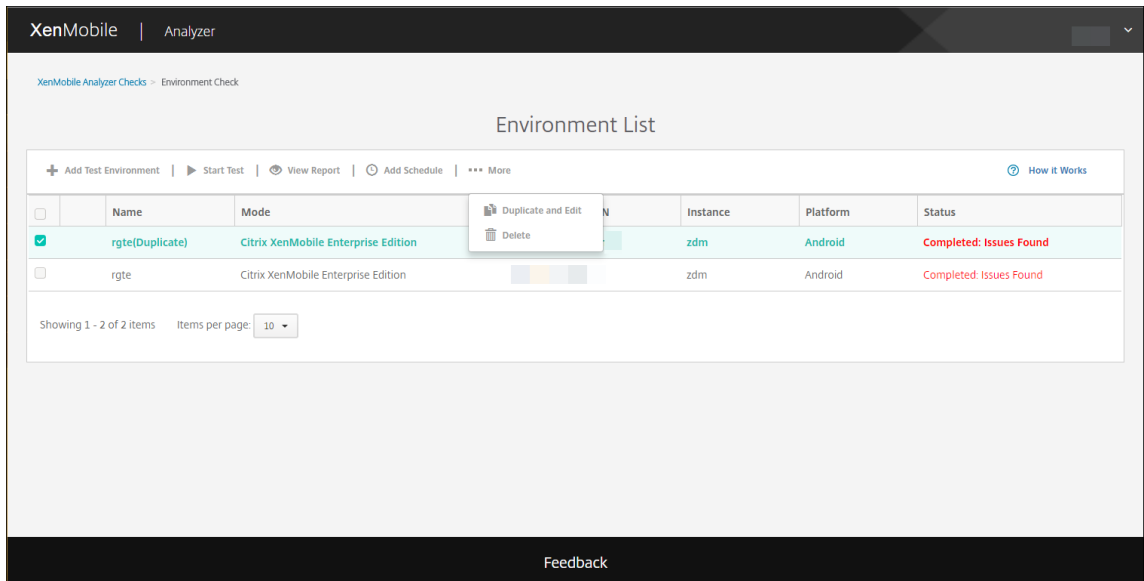
5. 서버설정에 따라 **User Credentials**(사용자자격증명) 탭에 다른 필드가 표시될 수 있습니다. 가능한 필드는 **Username**(사용자이름), **Username and Password**(사용자이름과 암호) 또는 **Username, Password**(사용자이름, 암호) 및 **Enrollment PIN**(등록 PIN)입니다.

6. **Save & Run**(저장및실행) 을클릭하여테스트를시작합니다.

진행률알림이나타납니다. 진행률대화상자를열린체로두거나대화상자를닫고테스트실행을계속할수있습니다.

통과한테스트는녹색으로표시됩니다. 실패한테스트는빨간색으로표시됩니다.

진행률대화상자를닫으면 **Environments List**(환경목록) 페이지로돌아옵니다.



Results(결과) 페이지에 Test Details(테스트세부정보), Recommendations(권장사항) 및 Results(결과) 가 표시됩니다.

7. **View Report(보고서보기)** 아이콘을 클릭하여 테스트 결과를 봅니다.

권장사항에 Citrix 기술자료문서가 연결된 경우 해당 문서가 이 페이지에 나타납니다.

8. **Results(결과)** 탭을 클릭하여 결과와 함께 도구가 수행한 개별 범주 및 테스트를 표시합니다.

- a) 보고서를 다운로드하려면 **Download Report(보고서다운로드)** 를 클릭합니다.
- b) 테스트 환경 목록으로 돌아가려면 **Environment Check(환경검사)** 를 클릭합니다.
- c) 동일한 테스트로 다시 실행하려면 **Run Again(다시실행)** 을 클릭합니다.
- d) 다른 테스트를 다시 실행하려면 **Test Environments(환경테스트)** 로 이동하고 테스트를 선택한 후 **Start Test(테스트시작)** 를 클릭합니다.
- e) 다른 XenMobile Analyzer 옵션을 선택하려면 **Go To XenMobile Analyzer Checks(XenMobile Analyzer 검사로이동)** 를 클릭합니다.

XenMobile | Analyzer

XenMobile Analyzer Checks > Environment Check > Report

Check Report

Check Complete: No Issues Found

Check Summary

Test Environment: testdoc
 Start Time: 2017-Jun-07 12:26 PM UTC
 Deployment Mode: Citrix XenMobile Enterprise Edition
 Server FQDN: navin.mathew@citrix.com
 Platform: IOS

[Edit Schedule](#) [Run Again](#)

Do you need assistance?

Citrix Support is here to help!
 For additional information, please refer to the [Support Knowledge Center](#)
 Download and share this report with your Citrix Support contact.

[Download Report](#)

Next, continue troubleshooting the XenMobile Environment using additional recommended checks:

[Troubleshoot the ActiveSync server using Secure Mail Test Tool.](#)
[Test connectivity of XenMobile Server and NetScaler Gateway.](#)
[Analyze logs and scan for known issues using Citrix Insight Services.](#)

[Go to XenMobile Analyzer Checks](#)

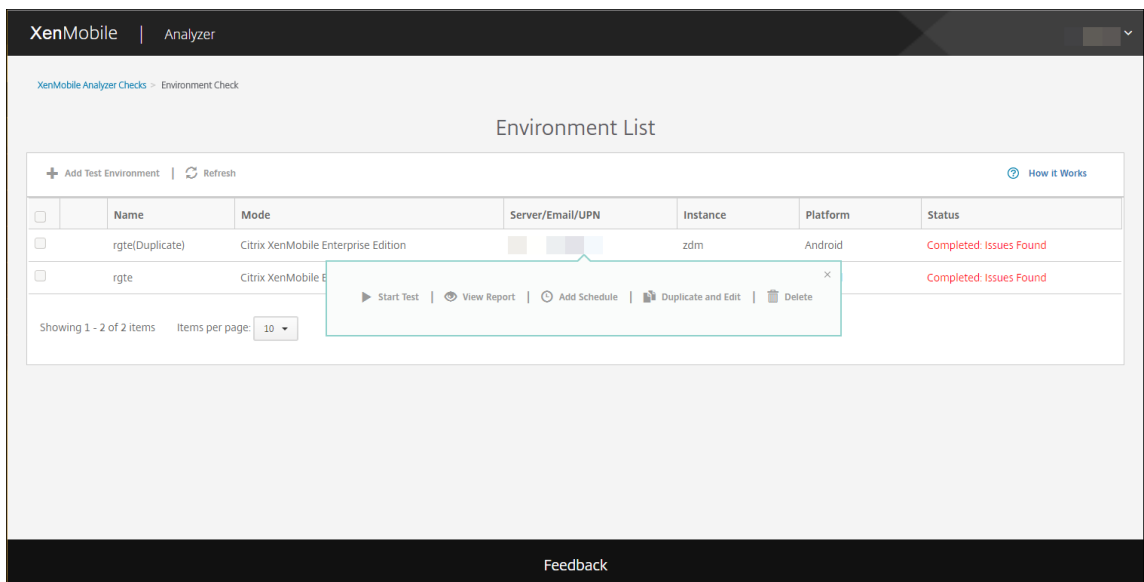
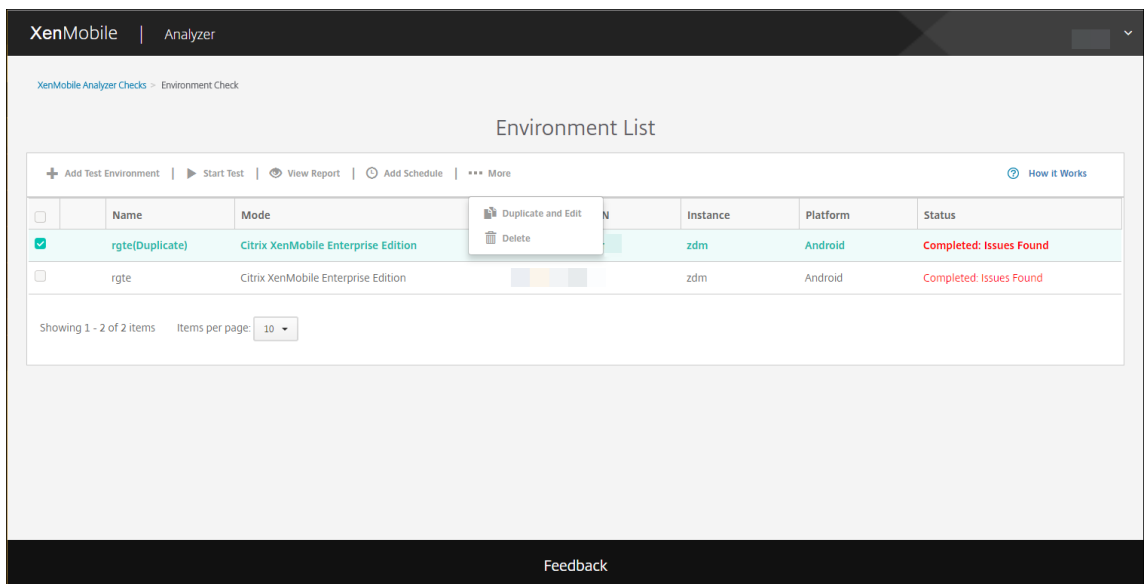
Detailed Results ✓
View all details of your test

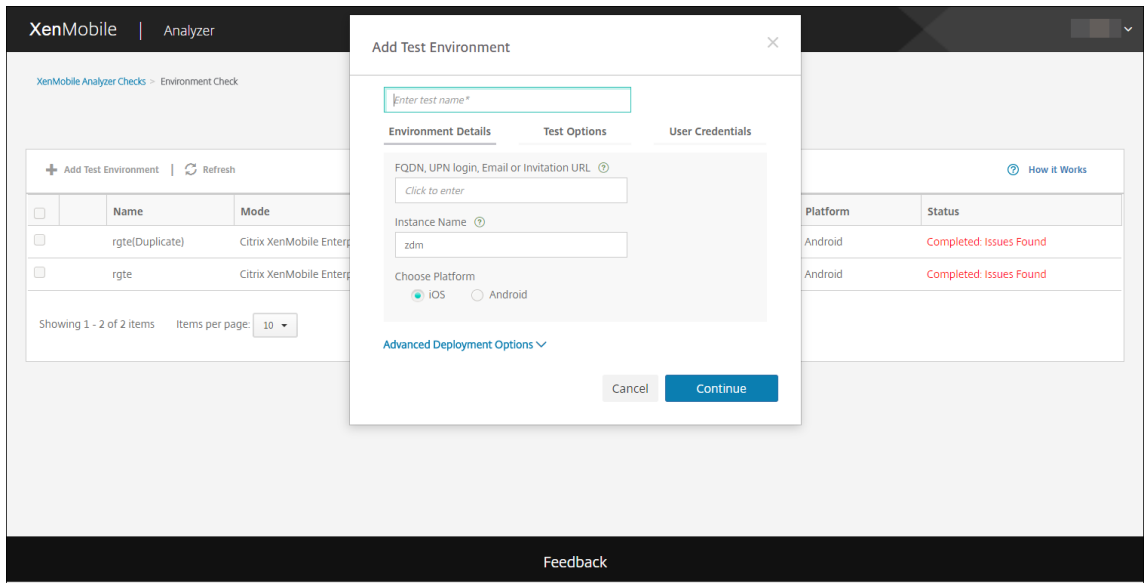
	Category	Checks	Results
✓	Initialization and Connectivity	XenMobile Server FQDN DNS Resolution	Pass
		XenMobile Server FQDN Connectivity	Pass
		XenMobile Server Certificate Validation	Pass
		XenMobile Server instance name validation	Pass
✓	Enrollment	Enrollment Authentication	Pass
		XenMobile Enrollment	Pass
✓	Authentication	Is NetScaler Gateway configured?	Yes
		NetScaler Gateway Cert Auth Enabled?	No
		NetScaler Gateway DNS Resolution	Pass
		NetScaler Gateway Connectivity	Pass
		NetScaler Gateway Certificate Validation	Pass
		NetScaler Gateway Login	Pass
		XenMobile Server connectivity through NetScaler Gateway	Pass
		XenMobile Server Authentication	Pass
✓	App Enumeration	Store Connectivity	Pass
		Device Registration	Pass
		Store App Listing	Pass
⚠	Secure Web Connectivity	NetScaler Gateway DNS Resolution	Not Tested
		NetScaler Gateway server connectivity	Not Tested
⚠	ShareFile	ShareFile Subdomain Discovery	Not Tested
		ShareFile SAML SSO	Not Tested
⚠	Secure Mail ADS	Secure Mail Auto Discovery	Not Tested
✓	Logout	XenMobile Server Logout	Pass
		NetScaler Gateway Logout	Pass

[Feedback](#)

9. Test Environments(환경테스트) 페이지에서테스트를복사하고편집할수있습니다. 그렇게하려면테스트를선택하고 **More(더보기)** 를클릭한다음 **Duplicate and Edit(복제및편집)** 를클릭합니다.

선택한테스트의복사본이만들어지고 Add Test Environment(테스트환경추가) 페이지가열리면새테스트를수정할수 있습니다.

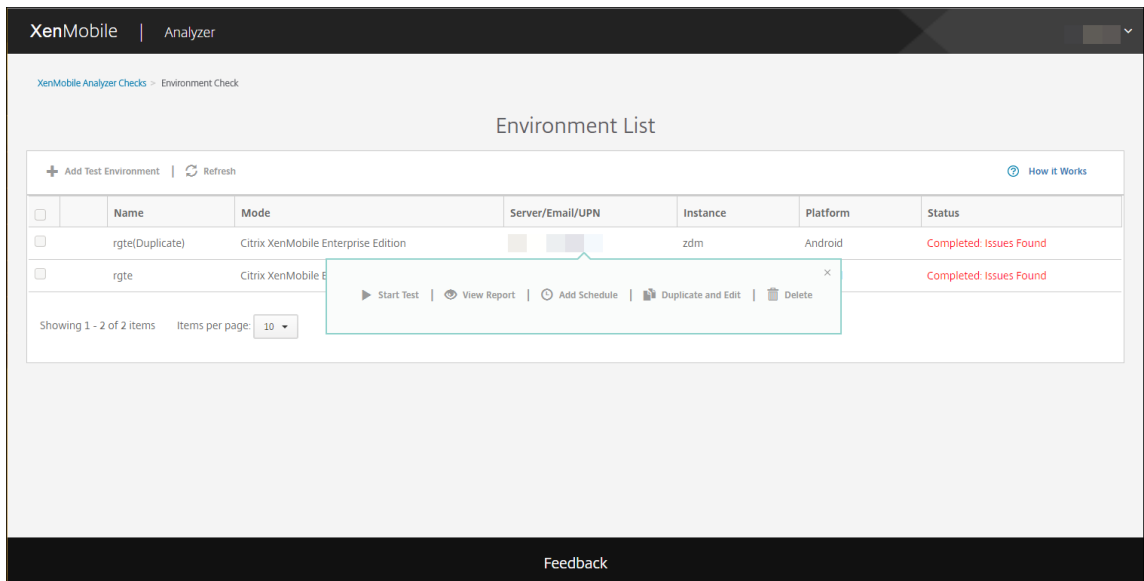




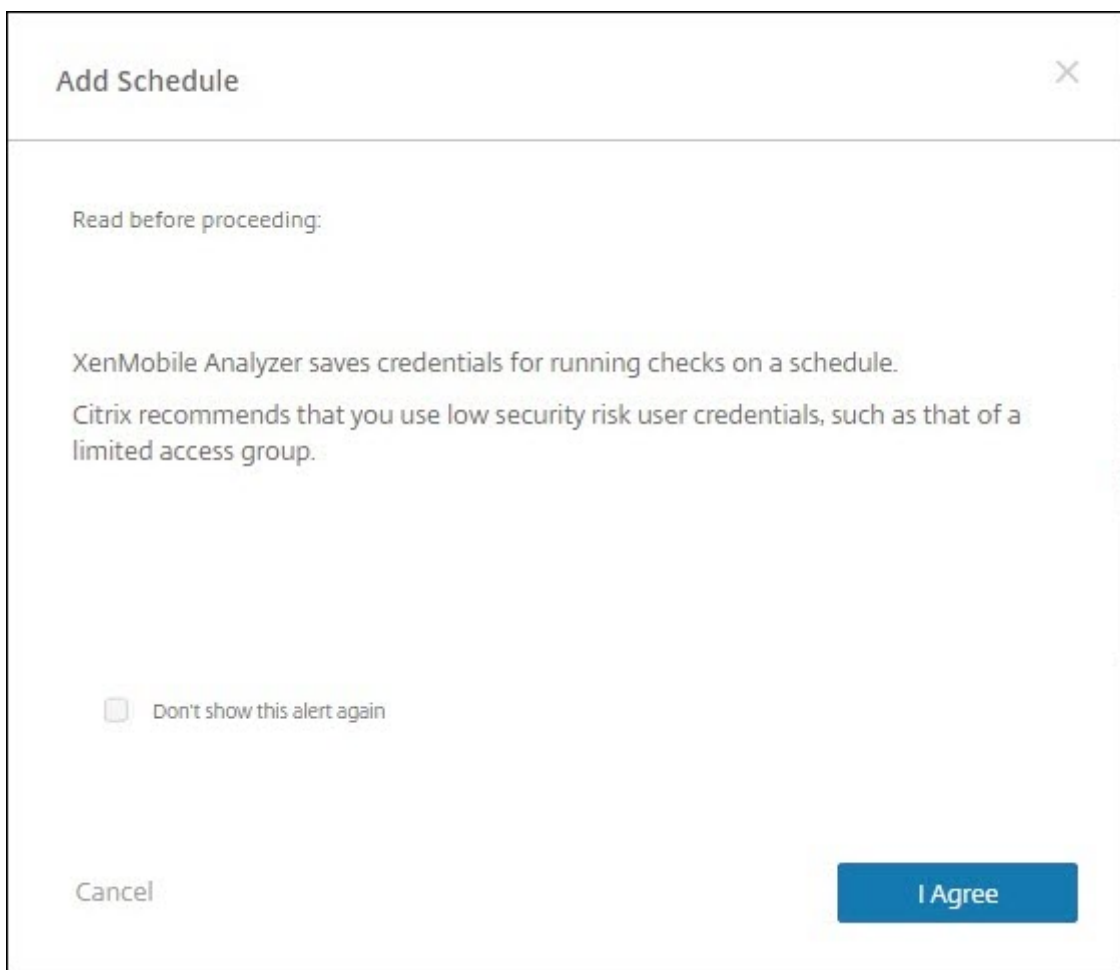
환경검사일정추가

예약된일정에자동으로테스트가실행되고결과가구성된사용자목록으로전송되도록테스트를구성할수있습니다.

1. **Environment List**(환경목록) 페이지에서일정을설정할환경을선택하고 **Add Schedule**(일정추가) 을클릭합니다.



2. **Add Schedule**(일정추가) 창에예약된테스트실행을위한자격증명이 XenMobile Analyzer 에저장된다는경고메시지가표시됩니다. 예약된테스트를실행할때는액세스권한이제한된계정을사용하는것이 좋습니다. **I Agree**(동의) 를클릭하여계속합니다.



3. 테스트실행을위한 **Username(사용자이름)** 및 **Password(암호)** 를입력합니다.

Add Schedule
✕

Enter credentials for the check

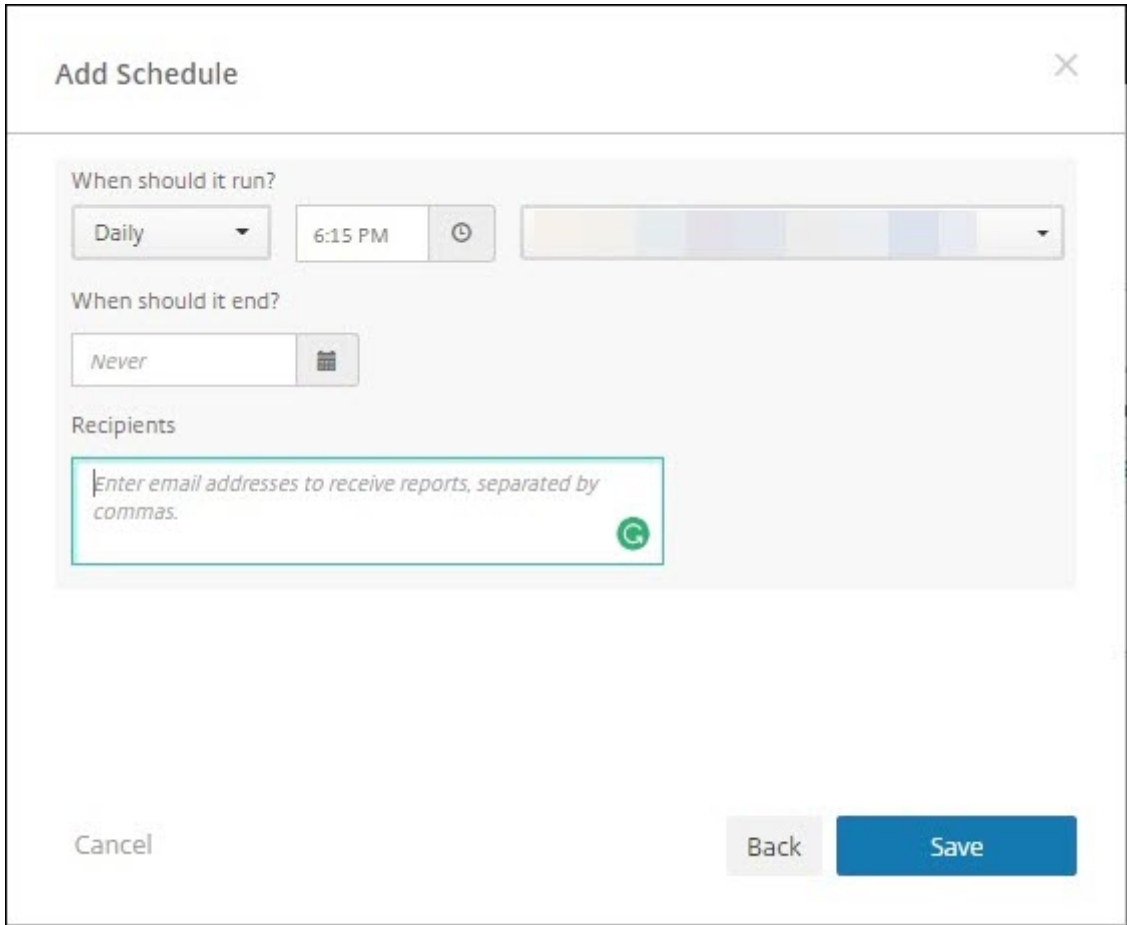
Test Name: testdoc

<p>Environment Information</p> <p>FQDN, UPN Login, Email</p> <div style="background-color: #eee; height: 15px; width: 100%;"></div> <p>Instance Name</p> <p>zdm</p> <p>Platform</p> <p>iOS</p>	<p>Secure Hub User Credentials</p> <p>Username</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;"> <i>Enter user account to test</i> </div> <p>Password</p> <div style="border: 1px solid #ccc; padding: 2px;"> <i>Enter password for user account</i> </div> <p><small>Note: Citrix stores this password securely</small></p>
---	--

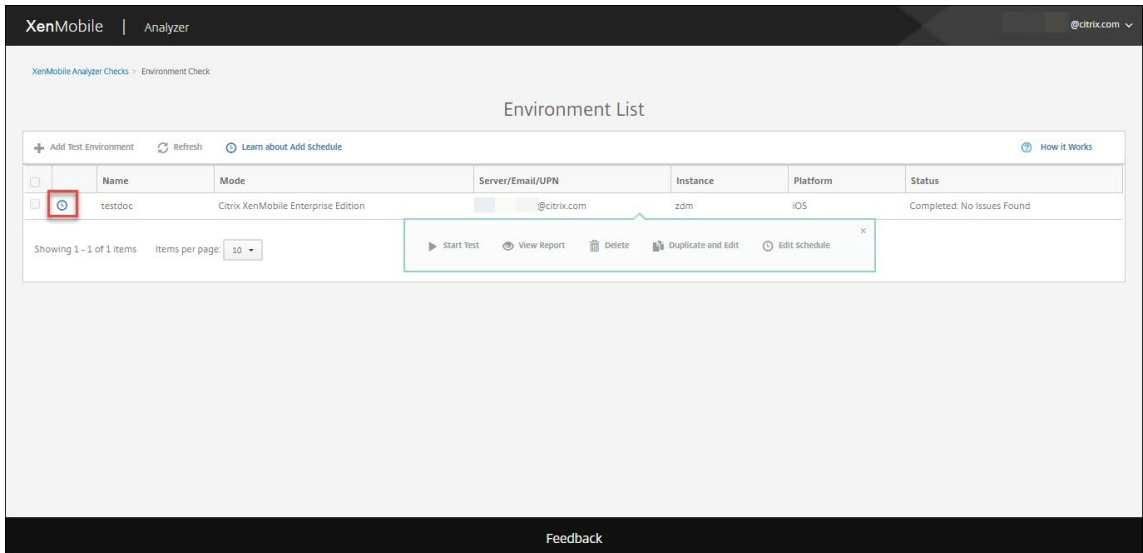
Cancel

Back
Continue

4. 테스트를 실행할 일정을 구성합니다. 드롭다운에서 **Daily(매일)** 또는 **Weekly(매주)** 를 선택할 수 있습니다. 테스트를 실행할 시간과 표준 시간대를 선택합니다. 날짜 선택기를 사용하여 예약된 테스트의 실행을 중지할 날짜를 선택하거나 테스트를 무기한 실행하도록 비워둡니다. 보고서를 받을 전자 메일 주소 목록을 심볼로 구분하여 입력합니다. 저장을 클릭합니다.



5. 테스트왼쪽의시계기호는일정이구성되었음을나타냅니다. 테스트를선택하는경우 **Edit Schedule(일정편집)** 을클릭하여테스트를실행할시기를변경할수있습니다.



6. 이창에서테스트실행시기를변경할수있습니다. 또한맨위의스위치를클릭하여사용하지않을수도있습니다. 완료되면 **Save(저장)** 를클릭합니다.

Edit Schedule ✕

Run checks automatically during this schedule ON
You can turn on/off schedule at any time.

When should it run?
Daily 6:15 PM (UTC-11:00) Midway Island, Samoa

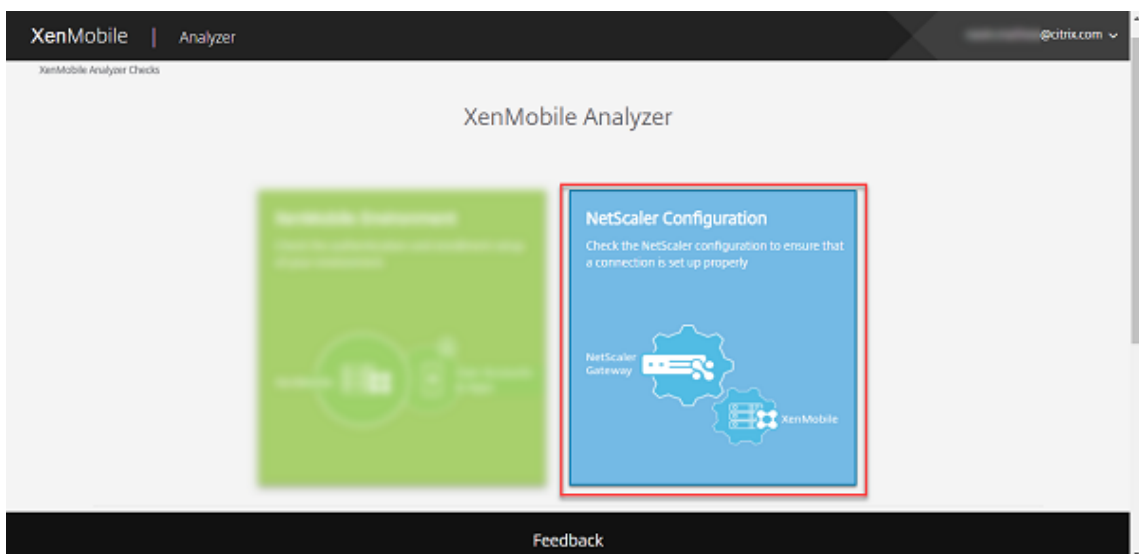
When should it end?
06/08/2017

Recipients
@citrix.com

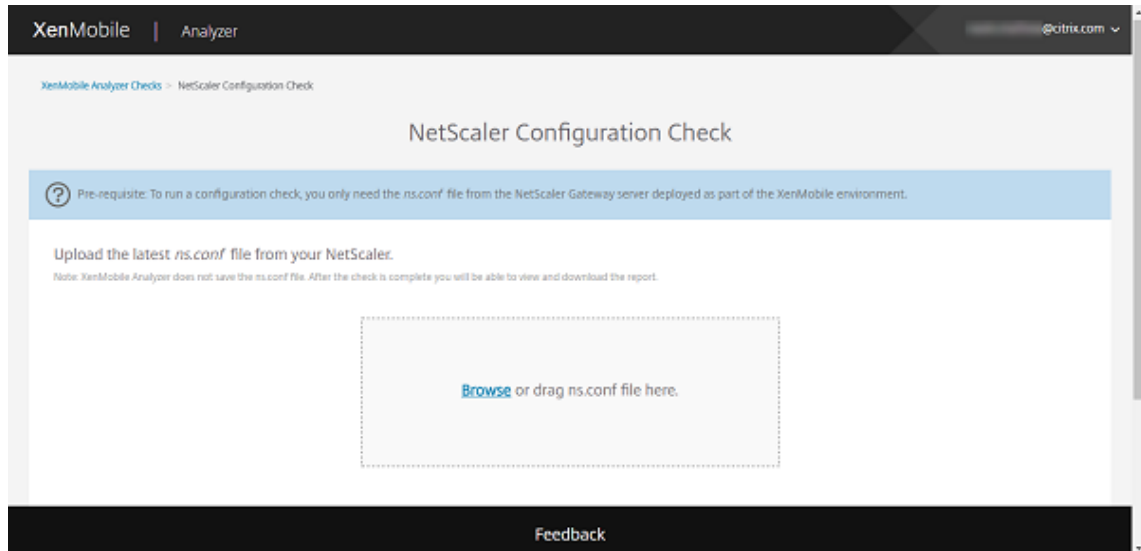
Cancel Edit Credentials Save

NetScaler 검사수행

1. XenMobile Analyzer 에로그온한후 **NetScaler Configuration(NetScaler 구성)** 을클릭합니다.



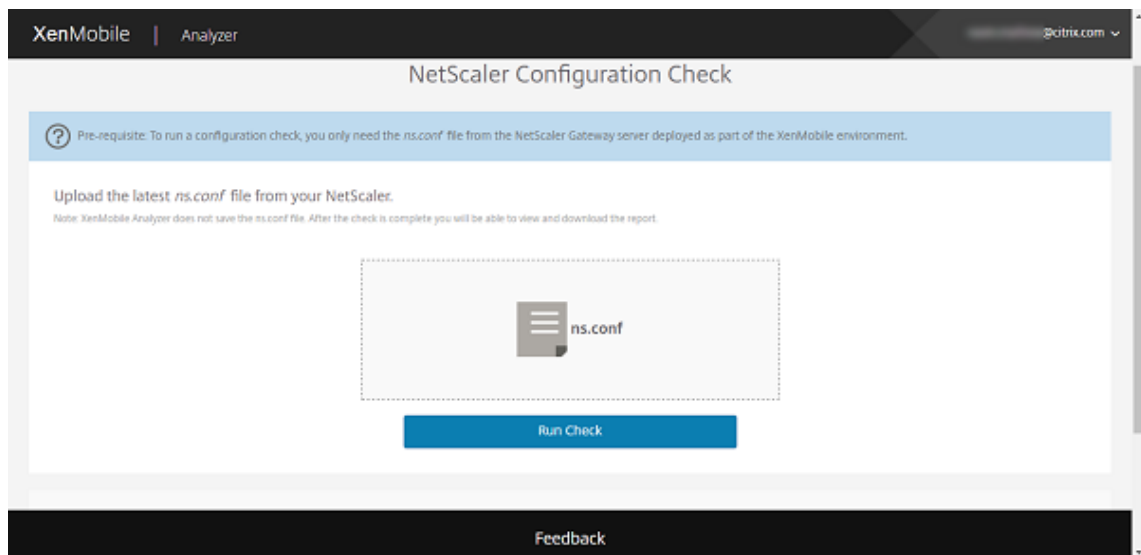
2. NetScaler 인스턴스에서 최신 ns.conf 파일을 업로드합니다. 파일을 업로드 상자에 끌어다 놓거나 **Browse**(찾아보기)를 클릭하고 ns.conf 파일을 검색하여 추가할 수 있습니다. 최신 ns.conf 파일을 다운로드하는 방법에 대한 자세한 내용은 [Support Knowledge Center](#)를 참조하십시오.



참고:

XenMobile Analyzer 는 ns.conf 파일을 저장하지 않습니다. 확인이 완료된 후 보고서를 보고 다운로드할 수 있습니다.

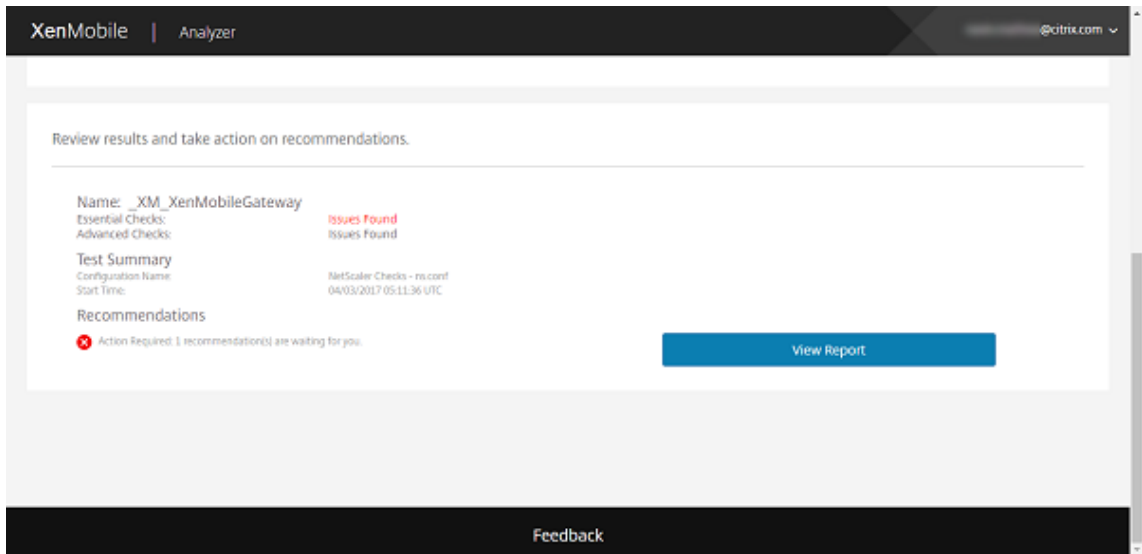
3. **Run Check**(확인실행) 를 클릭합니다.



XenMobile Analyzer 는 두 가지 유형의 구성 확인을 실행합니다.

- Essential Checks(필수사항확인) 는 성공적인 XenMobile 배포에 중요한 구성 요소를 찾습니다.
- Advanced Checks(고급확인) 는 XenMobile 배포에 중요하지 않지만 완전적인 역할을 하는 구성 요소를 찾습니다.

4. NetScaler 의필수사항및고급확인에대한권장사항을보려면 **View Report(보고서보기)** 를클릭합니다.



Configuration Report(구성보고서) 페이지가나타납니다.

XenMobile | Analyzer
@citrix.com

XenMobile Analyzer Checks > NetScaler Configuration Check > NetScaler Configuration Report

Configuration Report

Check Complete: Issues Found

< Run another test

Check Summary

Configuration Name: NetScaler Checks - ns.conf
Version: NS13.0 Build 64.34
Start Time: 2017-Jun-07 06:30 AM UTC

Note: XenMobile Analyzer does not save ns.conf file or configuration report below. Please download report and ns.conf file bundle to save to your system.

Do you need assistance?

Citrix Support is here to help!
For additional information, please refer to the Support Knowledge Center.
Download and share this report with your Citrix Support contact.

[Download report and ns.conf file bundle](#)

Next, continue troubleshooting the XenMobile Environment using additional recommended checks:

Troubleshoot the ActiveSync server using Secure Mail Test Tool.

Test connectivity of XenMobile Server and NetScaler Gateway.

Analyze logs and scan for known issues using Citrix Insight Services.

[Go to XenMobile Analyzer Checks](#)

Email report and ns.conf file bundle Send

Essential Configuration Checks

Recommendations

Policy	Details	Action
✖	LDAP	In LDAP Profile, It is recommended to set 'Server Logon Name Attribute' as 'UserPrincipalName' for client certificate authentication to work.

Showing 1 - 1 of 1 items

Detailed Results
Configuration Checklist

Policy Check	Details	Results
LDAP	_LDAP	Action Required
CERT POLICY		Pass
CLIENTLESS DOMAIN		Pass
CLIENT COOKIE		Pass
DNS		Pass
DNS SUFFIX		Pass
MAM LB		Pass
SMART ACCESS MODE	ENABLED	Pass
STA		Pass
XENMOBILE CLIENTLESS		Pass
XENMOBILE SESSION		Pass
XMS		Pass

Advanced Configuration Checks

Recommendations

Policy	Details	Action
⚠	SHAREFILE	Ensure that the ShareFile URL has been configured and bound either globally or to the virtual server.
⚠	SHAREFILE AUTH	Ensure that a valid LDAP authentication policy is bound to the sharefile authentication virtual server.
⚠	SHAREFILE AUTH	Ensure that a sharefile authentication virtual server is configured.
⚠	SHAREFILE AUTH	Ensure that LDAP Authentication policy is created and associated with a valid LDAP profile.
⚠	SHAREFILE AUTH	Primary Authentication Profile is missing.
⚠	SHAREFILE STORAGE ZONE LB	Load Balancing virtual server corresponding to Sharefile Storage Zone is not configured.
⚠	SHAREFILE STORAGE ZONE LB	No Sharefile Zone Controller configured for load balancing.
⚠	SHAREFILE STORAGE ZONE LB	Ensure that a valid CS server is configured for Sharefile Storage Zone Controller.
⚠	SPLIT TUNNEL	Ensure that a valid Intranet Application is added.
⚠	SPLIT TUNNEL	Ensure that a valid Intranet Application is bound to the virtual server.

Showing 1 - 10 of 12 items Showing 1 of 2

Detailed Results
Configuration Checklist

Policy Check	Details	Results
SHAREFILE	Not Configured	Action Recommended
SHAREFILE AUTH	Not Configured	Action Recommended
SHAREFILE STORAGE ZONE LB	Not Configured	Action Recommended
SPLIT TUNNEL	Not Configured	Action Recommended
XNC SERVER	Not Configured	Action Recommended
MDM LB		Pass
		Pass

[Feedback](#)

참고:

XenMobile Analyzer 는 NetScaler 마법사를 통해 구성된 게이트웨이 서버를 지원합니다. NetScaler Gateway 인스턴스에는 항상 ‘_XM_*name-provided-by-user-when-deploying’ 제목 규칙이 적용됩니다.

필수 구성 확인이 통과되면 종합적인 상태는 성공입니다.

필수 구성 확인이 실패하면 Recommendations(권장 사항) 표에 **Policy(정책)**, **Details(세부 정보)** 및 **Results (Action Required)(결과 (필수 조치))** 가 나열됩니다.

고급 구성 확인이 실패하면 Recommendations(권장 사항) 표에 **Policy(정책)**, **Details(세부 정보)** 및 **Results (Action Recommended)(결과 (권장 조치))** 가 나열됩니다.



구성 보고서 내의 알림 배지는 NetScaler 마법사를 통해 구성된 게이트웨이 서버와 사용자가 구성된 게이트웨이에 대한 Essential Configuration 확인의 권장 사항 수를 나타냅니다.

Configuration Report(구성 보고서) 페이지에서 다음 옵션을 사용할 수 있습니다.

- a) 세부 정보를 보려면 **Essential Configuration Checks/Advanced Configuration Checks(필수 구성 확인/고급 구성 확인)**(또는 펼침 아이콘) 를 클릭합니다.
- b) 다른 NetScaler 구성 확인을 실행하려면 **Run another test(다른 테스트 실행)** 를 클릭합니다.
- c) 다른 문제 해결 및 분석 도구 보려면 **Go to XenMobile Analyzer Checks(XenMobile Analyzer 확인)** 로 이동) 를 클릭합니다.
- d) 결과 보고서를 다운로드하려면 **Download report and ns.conf file bundle(보고서 및 ns.conf 파일 번들 다운로드)** 을 클릭하거나 **Email report and ns.conf bundle(보고서 및 ns.conf 번들 전자 메일 보내기)** 에 전자 메일 주소를 입력합니다. **Send(보내기)** 를 클릭합니다.

기타 정보 검사 수행

XenMobile Analyzer 의 환경 검사 단계와 직접 상호 작용하여 테스트를 수행할 수 있지만 다른 옵션은 정보를 제공하는 용도입니다. 이러한 각 옵션은 XenMobile 환경이 올바르게 설정되었는지 확인하는 데 사용할 수 있는 다른 지원 도구에 관한 정보를 제공합니다.

- **Advanced Diagnostics(고급 진단):** 환경의 정보를 수집한 후 Citrix Insight Services 에 업로드하는데 필요한 지침을 제공합니다. 이 도구는 데이터를 분석하고 권장 해결 방법이 포함된 맞춤형 보고서를 제공합니다.
- **Secure Mail Readiness(Secure Mail 준비):** XenMobile Exchange ActiveSync Test 응용 프로그램 다운로드를 위한 지침을 제공합니다. 이 응용 프로그램은 ActiveSync 서버 문제를 해결하여 XenMobile 환경에 배포할 수도도 록 준비합니다. 응용 프로그램이 실행되면 보고서를 보거나 다른 사용자와 공유할 수 있습니다.
- **Server Connectivity Checks(서버 연결 확인):** XenMobile 서버, 인증 서버 및 ShareFile 서버에 대한 연결을 확인하는 지침을 제공합니다.
- **Contact Citrix support(Citrix 지원 문의):** 다른 모든 방법에서 실패한 경우 Citrix 지원을 통해 지원 티켓을 만들 수 있습니다.

알려진문제

다음은 XenMobile Analyzer 의알려진문제입니다.

- Secure Web 연결검사를수행할때텍스트상자에여러 URL 을입력할수없습니다.
- Secure Hub 의공유장치인증기능이지원되지않습니다.
- Secure Web 테스트는입력된 URL 에대한연결만확인하며해당하는사이트에대한인증은확인하지않습니다.

수정된문제

다음은 XenMobile Analyzer 와관련하여해결된문제입니다.

- 등록초대를사용하여검사를수행할때테스트에통과하지만등록초대가상환되지않습니다.

REST API

January 6, 2020

참고:

이문서에서는 XenMobile Server 용 REST API 에대해다룹니다. Endpoint Management 용 REST API 에대해서는 [REST API](#)를참조하십시오.

XenMobile REST API 를사용하여 XenMobile 콘솔을통해표시되는서비스를호출할수있습니다. 모든 REST 클라이언트를 사용하여 REST 서비스를호출할수있습니다. API 를사용하면 XenMobile 콘솔에로그온하지않고서비스를호출할수있습니다.

현재사용가능한전체 API 집합을보려면 [REST 서비스에대한공용 API PDF](#) 를다운로드하십시오.

REST API 액세스에필요한권한

REST API 에액세스하려면다음권한중하나가필요합니다.

- 공용 API 액세스권한은역할기반액세스구성일부로설정됩니다. 자세한내용은 [RBAC 를사용하여역할구성](#)에서참조하십시오.
- 슈퍼사용자권한

REST API 서비스를호출하려면

REST 클라이언트또는 CURL 명령을 사용하여 REST API 서비스를호출할수있습니다. 다음예제에서는 Chrome 용 Advanced REST 클라이언트를사용합니다.

참고:

다음예제에서호스트이름및포트번호를환경에맞게변경하십시오.

로그인

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

요청: { `"login": "administrator", "password": "password"`}

메서드형식: POST

콘텐츠형식: application/json

The screenshot shows a REST client interface with the following details:

- URL:** `https://localhost:4443/xenmobile/api/v1/publicapi/login`
- Method:** POST
- Headers:** (Empty)
- Payload:**

```
{
  "login": "administrator",
  "password": "password"
}
```
- Content-Type:** application/json
- Status:** 200 OK (Loading time: 265 ms)
- Request headers:** User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36; Origin: chrome-extension://hgml0ofddffdnphfgcellkdfbfjeloo; Content-Type: application/json; Accept: */*; Accept-Encoding: gzip, deflate; Accept-Language: en-US,en;q=0.8; Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163
- Response headers:** Server: Apache-Coyote/1.1; Content-Type: text/plain; Content-Length: 53; Date: Sun, 22 Mar 2015 22:43:48 GMT
- Response body:**

```
{
  "auth_token": ""
}
```

관련정보

- [XenMobile REST API](#)

Exchange ActiveSync 용 Endpoint Management 커넥터

January 6, 2020

XenMobile Mail Manager 는이제 Exchange ActiveSync 용 Endpoint Management 커넥터입니다. Citrix 통합포트폴리오에대한자세한내용은 [Citrix 제품가이드](#)를참조하십시오.

이커넥터는다음과같이 XenMobile 의기능을확장합니다.

- EAS(Exchange Active Sync) 장치에대한동적액세스제어. EAS 장치는 Exchange 서비스에대한액세스가자동으로허용또는차단될수있습니다.
- XenMobile 이 Exchange 에서제공하는 EAS 장치파트너관계정보에액세스하는기능.
- XenMobile 이 모바일장치에대한 EAS 초기화를수행하는기능.
- XenMobile 이 Blackberry 장치에대한정보에액세스하고초기화및 ResetPassword 같은제어작업을수행하는기능.

Exchange ActiveSync 용 Endpoint Management 커넥터를다운로드하려면 [Citrix.com](#)에서 XenMobile 10 Server 아래에있는 Server Components(서버구성요소) 섹션으로이동합니다.

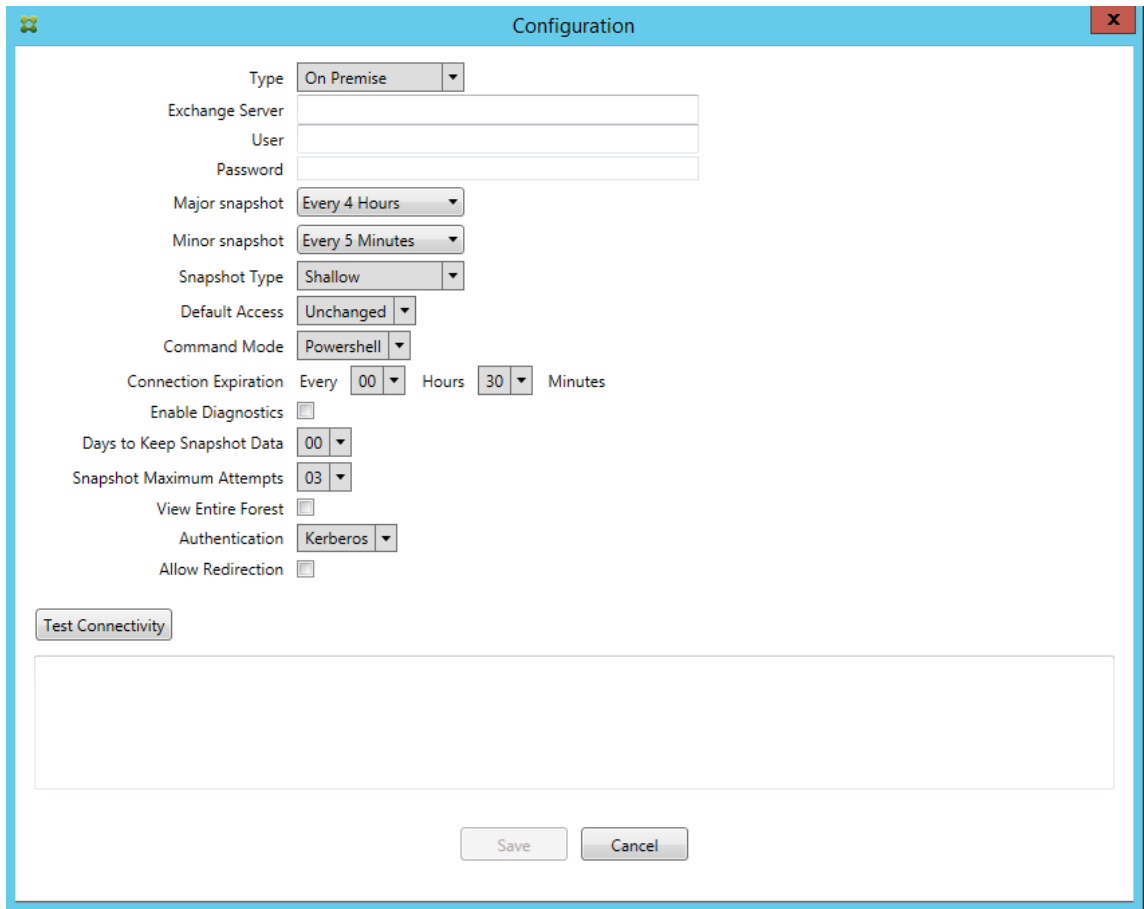
새로운항목

이후섹션에는이전의 XenMobile Mail Manager 인 Exchange ActiveSync 용 Endpoint Management 커넥터에대한새로운기능이나열됩니다.

버전 10.1.10 의새로운기능

다음문제는버전 10.1.10 에서수정되었습니다.

- 네트워크문제를자주경험하는고객은이전에제공된 3 번의시도에서스냅샷을완료하지못할수있습니다. 이릴리스에서는관리자가최대시도횟수 (1~10) 를구성할수있습니다. 이수정사항이적용됨에따라통신에서스냅샷이여러번중단되더라도스냅샷프로세스가완전히중단되지않습니다. [CXM-70837]



- 이전버전에서는스냅샷유형이 Exchange 구성목록에나타나지않았습니다. 이제스냅샷유형이나타납니다. [CXM-70846]
- PowerShell 을통해보고되는 PSRemotingTransport 예외는 Exchange 세션을더이상실행할수없음을나타냅니다. 상태는기본적으로구성파일의심각한오류목록에추가됩니다. 따라서 PSRemotingTransportException 이검색되면이후삭제를위해연결이오류상태인것으로표시됩니다. 다음번통신에는유효한연결이사용되거나새연결이만들어집니다. [XMHELP-2184, CXM-70836]
- 구성변경이저장되면새구성을로드하기전에이전에구성된내부구성요소중일부가제대로삭제되지않을수있습니다. 이문제로인해예측할수없는동작이발생할수있습니다. 이동작은특정변경사항에따라다르며변경사항이이전구성과충돌하는지여부에따라달라집니다. 이릴리스에서는새구성을로드하기전에모든내부구성요소가삭제됩니다. [XMHELP-2259, CXM-71388]

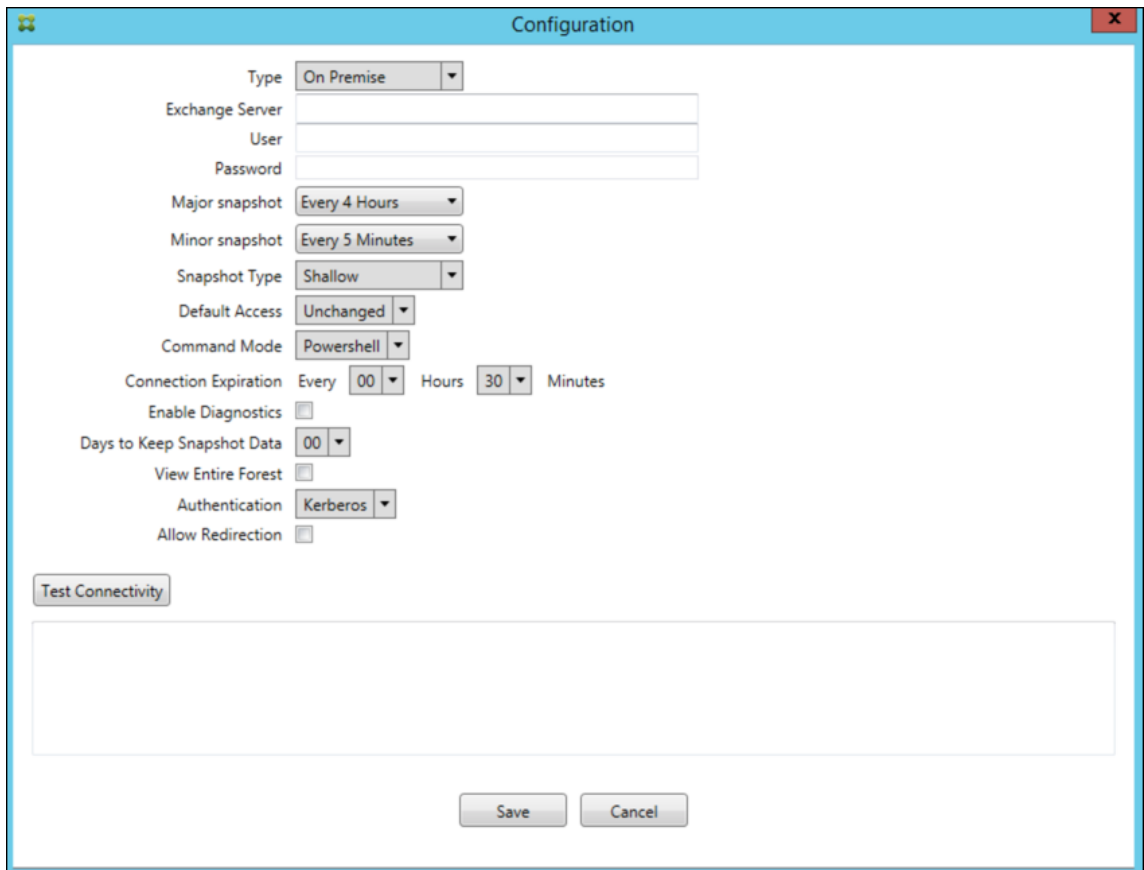
이전버전의새로운기능

다음섹션에는 Exchange ActiveSync 용 Endpoint Management 커넥터의이전버전에포함된기능과수정된문제가나와 있습니다.

버전 10.1.9 의새로운기능

다음문제는버전 10.1.9 에서수정되었습니다.

- 이제구성변경이보다일관된방식으로처리됩니다. 서비스가구성변경을감지하면각내부하위시스템이중지됩니다. 즉, 모든 활성또는예약처리가중단됩니다. 그런다음새구성이로드되고하위시스템이다시시작됩니다. 즉, 모든예약및기타내부인프라가새설정으로다시설정됩니다. 이문제는버전 10.1.8 의알려진문제를수정합니다. [CXM-47709, CXM-61330]
- 업그레이드중에기존데이터베이스구성이새구성파일에병합되지않았습니다. 이제데이터베이스구성이업그레이드된구성파일에병합됩니다. [CXM-49326]
- 스냅샷관련진단파일에서열헤더가누락되었습니다. 헤더가복원되었습니다. [CXM-62680]
- 이전버전에서업그레이드하는경우사용증인구성파일의유사한섹션이구성파일의기본값섹션을덮어씹니다. 이문제로인해 업그레이드후기본값섹선에추가또는개선사항이로드되지않습니다. 이버전부터는기본값섹선에항상최신구성이반영됩니다. [CXM-62681]
- 관리자는응용프로그램을실행할때더이상 Shift 키를눌러특정옵션에액세스할수없습니다. 이러한옵션은이전에 Citrix 사용권한으로사용할수있었습니다. 이제리디렉션허용과같은일부옵션을완벽하게사용할수있으며감지중지및개수수정같은 다른옵션은사용되지않습니다. [CXM-62767]



버전 10.1.8 의새로운기능

다음문제는버전 10.1.8 에서수정되었습니다.

- Exchange 는 Exchange ActiveSync 서비스에대한 Citrix Endpoint Management 커넥터를제한하여커넥터에서너무자주명령이실행되지않도록합니다. 이는 Office 365 에대한연결에서일반적인사항입니다. 제한이적용되면다음명령을전송하기전에서비스를지정된기간동안일시중지해야합니다. 이제구성콘솔에남은일시중지시간이표시됩니다. [CXM-48044]
- 구성파일 (config.xml) 의 “Watchdog” 또는 “SpecialistsDefaults” 섹션을수정하는경우업그레이드후구성파일에변경사항이반영되지않습니다. 이릴리스에서는수정한내용이새구성파일에올바르게병합됩니다. [CXM-52523]
- Google Analytics 로전송되는분석에특히스냅샷과관련하여더많은세부정보가추가되었습니다. [CXM-56691]
- Exchange 테스트연결기능은연결초기화를한번만시도합니다. Office 365 연결은제한될수있기때문에제한되는경우테스트연결이실패한것으로나타날수있었습니다. 이제 Exchange ActiveSync 용 Citrix Endpoint Management 커넥터가연결시작을최대세번까지시도합니다. [CXM-58180]
- Exchange 에서정책을시행하려면 Exchange ActiveSync 용 Citrix Endpoint Management 커넥터가각사서함의모든관련장치를허용목록과차단목록에포함하는 **Set-CASMailbox** 명령을컴파일해야합니다. 장치가목록에포함되지않은경우 Exchange 는기본액세스상태로폴백합니다. 이기본액세스상태가장치의원하는상태와다른경우장치는규정준수위반상태가됩니다. 따라서 Exchange 기본액세스상태가허용됨상태여야하지만차단된인 경우사용자는전자메일에액세스하지못할수있습니다. 또는전자메일에대한액세스가차단되어야하는사용자에게엑세스권한이부여될수있습니다. 이제 Exchange ActiveSync 용 Citrix Endpoint Management 커넥터가원하는상태의모든장치를각 **Set-CasMailbox** 명령에포함합니다. [CXM-61251]

다음은버전 10.1.8 에서알려진문제입니다.

스냅샷또는정책평가같은장기작업이서비스에서실행되는동안관리자가구성응용프로그램에서구성데이터를수정하는변경을수행하면서서비스가규정불가능한상태로전환될수있습니다. 이경우정책변경이처리되지않거나스냅샷이시작되지않는등의증상이나타날수있습니다. 서비스를작동상태로되돌리려면서비스를다시시작해야합니다. 서비스를시작하기전에 Windows 서비스관리자를사용하여서비스프로세스를종료해야할수있습니다. [CXM-61330]

버전 10.1.7 의새로운기능

- XenMobile Mail Manager 는이제 Exchange ActiveSync 용 Endpoint Management 커넥터입니다.
- Exchange 구성대화상자에서 **Disable Pipelining**(파이프라인처리사용안함) 옵션이더이상지원되지않습니다. config.xml 파일에서각명령에대한여러단계를구성하여동일한기능을구현할수있습니다. [CXM-54593]

다음문제는버전 10.1.7 에서수정되었습니다.

- 스냅샷기록창에서오류메시지가컨텍스트가부족한상태로표시될수있습니다. 이제오류메시지에발생위치에대한컨텍스트가접두사로추가됩니다. [CXM-49157]
- XmmGoogleAnalytics.dll 에이릴리스에해당하는파일버전이없습니다. [CXM-52518]
- 진단을개선하기위해최근에서사서함허용/차단됨상태를설정하는데사용되는장치 ID 목록에대한문자열형식을변경했습니다. 하지만너무많은장치를지정하면최대문자열크기가초과되었습니다. 이제내부배열데이터구조를사용합니다. 이구조에는크기제한이없으며데이터의형식을진단용도에적합하게지정합니다. [CXM-52610]

- Exchange 와 동기화되지 않은 장치 정책이 검색되는 경우 해당 명령에 관련 사서함에 속하지 않는 장치가 포함되어 있을 수 있습니다. 이제 Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange 에 대한 명령에 관련 사서함에 속한 장치만 나타나게 합니다. [CXM-54842]
- 일부 환경에서 Microsoft 어셈블리를 사용할 수 없습니다. 필요한 어셈블리가 이제 응용 프로그램과 함께 명시적으로 설치됩니다. [CXM-55439]
- 장치 또는 사서함의 고유 이름에서 특성이름과 등호 사이 및/또는 등호와 값 사이에 공백이 있는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터가 장치와 사서함을 올바르게 일치시키지 못할 수 있습니다. 결과적으로 스냅샷 조정 중에 일부 장치 및/또는 사서함이 거부될 수 있습니다. [CXM-56088]

참고:

이후 섹션에서는 Exchange ActiveSync 용 Endpoint Management 커넥터가 이전 이름인 XenMobile Mail Manager 로 나타납니다. 이 이름은 버전 10.1.7 에서 변경되었습니다.

버전 10.1.6.20 의 업데이트

10.1.6 에 대한 업데이트에는 버전 10.1.6.20 의 다음과 같은 수정 사항이 포함되어 있습니다.

- Exchange 와 동기화되지 않은 장치 정책이 검색되는 경우 해당 명령에 관련 사서함에 속하지 않는 장치가 포함되어 있을 수 있습니다. 이제 XenMobile Mail Manager 는 Exchange 에 대한 명령에 관련 사서함에 속한 장치만 나타나게 합니다. [CXM-54842]

버전 10.1.6 의 새로운 기능

XenMobile Mail Manager 버전 10.1.6 에는 다음과 같은 수정된 문제와 개선 사항이 포함되어 있습니다.

- 경우에 따라 스냅샷 기록창이 데이터 상 업데이트되지 않는 상태로 전환됩니다. 더욱 안정적으로 업데이트되도록 창 새로고침 메커니즘이 개선되었습니다. [CXM-47983]
- 파티셔닝된 스냅샷과 파티셔닝되지 않은 스냅샷에 두 가지 별도의 모드와 코드 경로가 사용되었습니다. 파티셔닝되지 않은 스냅샷은 단일 "*" 파티션을 사용하는 구성의 파티셔닝된 스냅샷과 동일하기 때문에 파티셔닝되지 않은 스냅샷 모드가 제거되었습니다. 이제 36 개의 파티션 (0-9, A-Z) 이 있는 파티셔닝된 스냅샷이 기본 스냅샷 모드입니다. [CXM-49093]
- 스냅샷 기록창에서 오류 메시지가 상태 메시지로 덮여 써집니다. 이제 XenMobile Mail Manager 에 두 개의 별도 필드가 표시되어 사용자가 상태와 오류를 동시에 볼 수 있습니다. [CXM-51942]
- Exchange Online (Office 365) 에 연결 할 때 스냅샷 관련 쿼리 로인해 데이터 집합이 잘릴 수 있습니다. 이 문제는 XenMobile Mail Manager 가 다중 명령 파이프라인이 있는 스크립트를 실행하는 경우에 발생할 수 있습니다. 업스트림 명령이 다운스트림 명령에 충분히 빠르게 데이터를 전달할 수 없어 작업이 조기에 완료되고 불완전한 데이터가 생깁니다. 이제 XenMobile Mail Manager 가 파이프라인 자체를 모방하고 업스트림 명령이 완료될 때까지 기다린 후 다운스트림 명령을 호출할 수 있습니다. 이 변경 사항에 따라 이제 모든 데이터가 처리되고 캡처됩니다. [CXM-52280]
- Exchange 에 대한 정책 업데이트 명령에서 해결할 수 없는 오류가 발생할 경우 동일한 명령이 오랫동안 반복적으로 작업 대기열에 반환됩니다. 이 경우 해당 명령이 Exchange 에 여러 번 전송되었습니다. 이 XenMobile Mail Manager 버전에서는 오류를 일으키는 명령이 작업 대기열에 불연속적으로만 반환됩니다. [CXM-52633]

- 특정사서함에대한정책업데이트에도모든장치허용또는차단이포함된경우 **Set-CASMailbox** 명령실행이실패합니다. 빈 목록이 **NULL** 이아닌빈문자열로변환되기때문입니다. 이제올바른데이터가전송됩니다. [CXM-53759]
- 새장치를처리할때 Exchange 에서얼마동안 (대개 15 분) “DeviceDiscovery” 로상태가반환될수있습니다. XenMobile Mail Manager 가이상태를특별히처리하지않았습니다. 이제 XenMobile Mail Manager 가이상태를처리합니다. 사용자가 UI 의모니터탭에서이상태의장치로필터링할수있습니다. [CXM-53840]
- XenMobile Mail Manager 가 XenMobile Mail Manager 데이터베이스에쓸수있는권한을확인하지않았습니다. 따라서권한이제한된경우동작을예측할수없었습니다. 이제 XenMobile Mail Manager 가데이터베이스에서필요한권한을캡처하고확인합니다. XenMobile Mail Manager 는권한이감소된것을연결테스트시 (메시지가표시됨) 또는기본구성창하단의데이터베이스표시기에 (마우스포인터를이동하면메시지가표시됨) 표시합니다. [CXM-54219]
- XenMobile Mail Manager 서비스를중지하려고할때현재작업부하에따라서비스가즉시중지되지않을수있습니다. 따라서서비스가응답하지않는상태로나타납니다. 진행중인작업이중단되어보다정상적으로종료될수있도록기능이개선되었습니다. [CXM-54282]

버전 10.1.5 의새로운기능

XenMobile Mail Manager 버전 10.1.5 에는다음과같은수정된문제가포함되어있습니다.

- Exchange 가 XenMobile Mail Manager 작업에제한을적용하는경우로그이외에는제한이적용되었다는점이표시되지않습니다. 이릴리스에서는사용자가활성스냅샷으로마우스포인터를이동하면 “제한” 상태가표시됩니다. 또한 XenMobile Mail Manager 에제한이적용되는동안에는 Exchange 에서제한이해제될때까지주소냅샷의시작이금지됩니다. [CXM-49617]
- 주소냅샷작업중 XenMobile Mail Manager 에 Exchange 의제한이적용될경우다음스냅샷을실행하기까지허용되는경과시간이부족할수있습니다. 이문제로인해제한이연장되고스냅샷이실패합니다. 이제 XenMobile Mail Manager 가 Exchange 에서지정된최소스냅샷시도대기간격동안대기합니다. [CXM-49618]
- 진단이사용되는경우명령파일에서 **Set-CasMailbox** 명령의각속성이름앞에하이픈이누락된것으로나타납니다. 이문제는진단파일의형식에서만발생하며 Exchange 에대한실제명령에서는발생하지않습니다. 하이픈누락으로인해사용자는 테스트또는유효성검사를위해명령을잘라내어 PowerShell 프롬프트에바로붙여넣지는못합니다. 하이픈이추가되었습니다. [CXM-52520]
- 사서함 ID 가 “lastname, firstname” 형식인경우 Exchange 가쿼리에서데이터를반환할때심표앞에백슬래시를추가합니다. XenMobile Mail Manager 가추가데이터쿼리를위해 ID 를사용할때이백슬래시를제거해야합니다. [CXM-52635]

알려진제한사항

참고:

다음제한사항은버전 10.1.6 에서해결되었습니다.

XenMobile Mail Manager 에는알려진제한사항이있으며, 이로인해 Exchange 에대한명령이실패할수있습니다. Exchange 에정책변경사항을적용하기위해 XenMobile Mail Manager 는 **Set_CASMailbox** 명령을실행합니다. 이명령은두가지장치목록, 즉허용목록과차단목록을사용할수있습니다. 이명령은사서함에연결된장치에적용됩니다.

이러한 목록은 Microsoft API 에 의해 각각 256 자로 제한됩니다. 이러한 목록 중 하나가 제한을 초과할 경우 명령이 완전히 실패하여 사서함의 해당 장치에 대한 모든 정책이 설정되지 않습니다. XenMobile Mail Manager 로그에 다음과 같은 오류가 보고됩니다. 차단 목록에 대한 예입니다.

“Message:’Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’ to the target. Exception setting “ActiveSyncBlockedDeviceIDs”: “The length of the property is too long. The maximum length is 256 and the length of the value provided is ...”

장치 ID 길이는 달라질 수 있지만 일반적으로 동시에 10 개 이상의 허용 또는 차단 장치가 포함될 경우 제한이 초과될 수 있습니다. 특정 사서함에 많은 장치가 연결되는 경우는 드물지만 있을 수 있습니다. XenMobile Mail Manager 가 이러한 경우를 처리하도록 개선될 때 까지 사용자와 사서함에 연결되는 장치 수를 10 개 이하로 제한하는 것이 좋습니다. [CXM-52633]

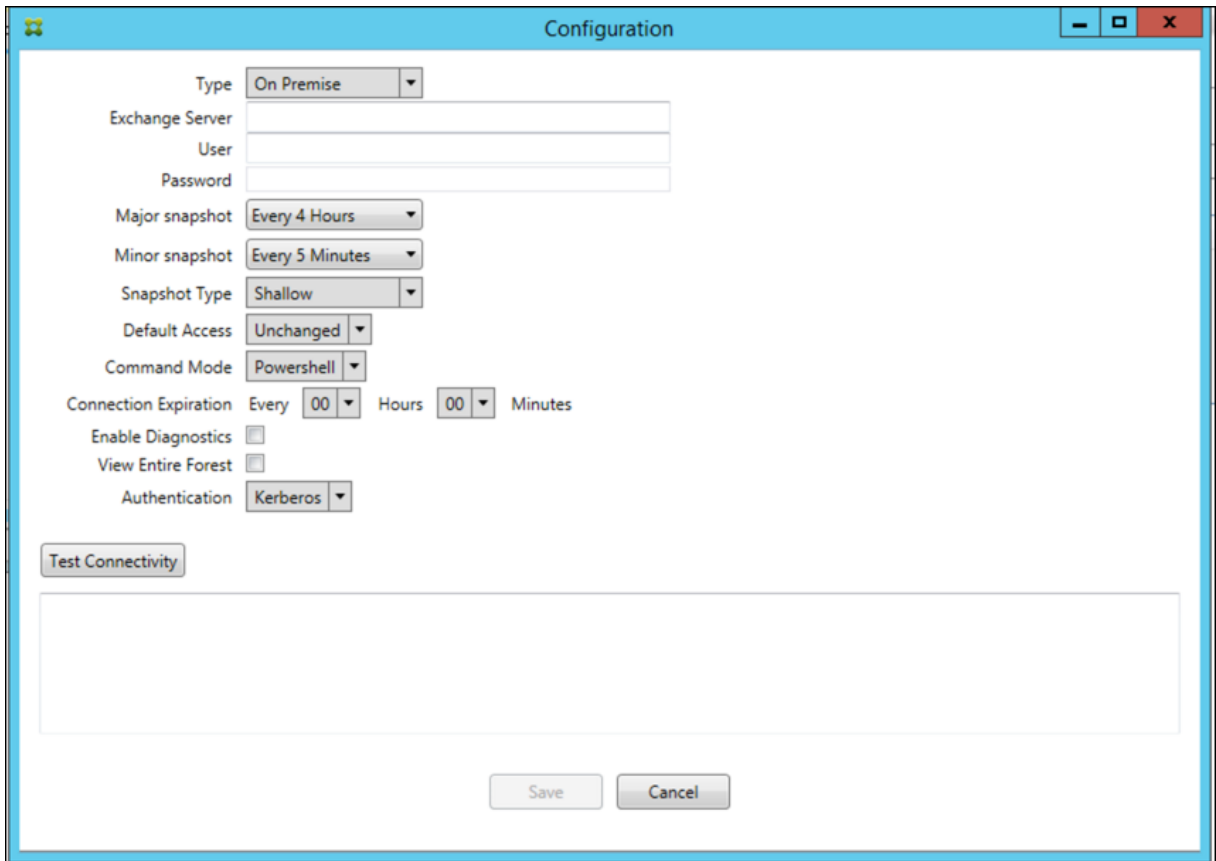
버전 10.1.4 의 새로운 기능

XenMobile Mail Manager 버전 10.1.4 에는 다음과 같은 수정된 문제가 포함되어 있습니다.

- PCI Council 에서는 보안이 취약한 TLS 1.0 의 사용을 중지하고 있습니다. XenMobile Mail Manager 에는 TLS 1.1 및 1.2 에 대한 지원이 추가되었습니다. [CXM-38573, CXM-32560]
- XenMobile Mail Manager 에는 새로운 진단 파일이 포함됩니다. Exchange 사양에서 **Enable Diagnostics**(진단 사용) 를 선택하면 새 스냅샷 기록 파일이 생성됩니다. 스냅샷을 시도할 때 마다 스냅샷의 결과로 파일에 행이 추가됩니다. [CXM-49631]
- **Set-CASMailbox** 명령에 대한 명령 진단 파일에 허용되거나 차단된 장치 목록이 나타나지 않았습니다. 대신, 파일의 관련된 인수에 내부 클래스 이름이 표시되었습니다. 이제 XenMobile Mail Manager 의 deviceID 목록이 심플로 구분된 목록으로 표시됩니다. [CXM-50693]
- 잘못된 사양으로 인해 Exchange 에 대한 연결 시도가 실패할 경우 오류 메시지가 “All connections in use(모든 연결을 사용 중임)” 라는 잘못된 메시지로 재정의되었습니다. 이제 보다 설명적인 메시지가 나타납니다. 예를 들어 “All connections are inoperable(모든 연결이 작동하지 않음)”, “Connection pool is empty(연결 풀이 비어있음)”, “All connections are throttled(모든 연결이 제한됨)” 및 “No available connections(사용 가능한 연결 없음)” 같은 메시지가 나타납니다. [CXM-50783]
- 경우에 따라 허용/차단/초기화 명령이 XenMobile Mail Manager 내부 캐시의 대기열에 여러 번 배치됩니다. 이 문제로 인해 Exchange 로 전송되는 명령이 지연됩니다. 이제 XenMobile Mail Manager 가 각 명령에 대한 단일 인스턴스만 대기열에 배치합니다. [CXM-51524]

버전 10.1.3 의 새로운 기능

- **Google Analytics** 지원: XenMobile Mail Manager 가 어떻게 사용되는지를 확인하여 제품의 개선 영역에 집중할 수 있습니다.
- 진단 사용 설정: **Configuration**(구성) 대화상자의 Configure console(콘솔 구성) 에 **Enable Diagnostic**(진단 사용) 확인란이 나타납니다.



버전 10.1.3 의수정된문제

- **Snapshot History**(스냅샷기록) 창에서스냅샷의현재상태를보여주는도구설명에실제상태가반영되지않습니다. [CXM-5570]
경우에따라 XenMobile Mail Manager 에서명령진단파일이작성되지않습니다. 이경우명령기록이하나도기록되지않습니다. [CXM-49217]
- 연결오류가발생하는경우연결이 “errored” 로표시되지않습니다. 그결과후속명령에서연결사용을시도하고다른오류가 발생할수있습니다. [CXM-49495]
- Exchange Server 에서제한이발생하면상태확인루틴에서예외가발생할수있습니다. 그결과오류가발생하거나만료된연결을삭제하지못할수있습니다. 또한 XenMobile Mail Manager 에서제한시간이만료되기전까지연결을만들지못할수 있습니다. [CXM-49794].
- Exchange 의최대세션수가초과되면 XenMobile Mail Manager 가정확한메시지가아닌 “Device Capture Failed(장치캡처실패)” 오류를보고합니다. XenMobile Mail Manager 가 Exchange 통신에정상적으로사용하는 세션두개가사용중임을나타내는메시지가보고되어야합니다. [CXM-49994]

버전 10.1.2 의새로운기능

- **Exchange** 에대한연결개선: XenMobile Mail Manager 는 PowerShell 세션을사용하여 Exchange 와통신합니다. PowerShell 세션을 Office 365 를통해처리하는경우잠시후세션이불안정해지고후속명령이성공적으로실행되

지않을수있습니다. 이제 XenMobile Mail Manager 에서연결의만료기간을설정할수있습니다. 연결이만료시간에도
달하면 XenMobile Mail Manager 가 PowerShell 세션을정상적으로종료하고세션을만들수있습니다. 이렇게하면
PowerShell 세션이불안정해질가능성이줄고스냅샷실패확률이크게감소합니다.

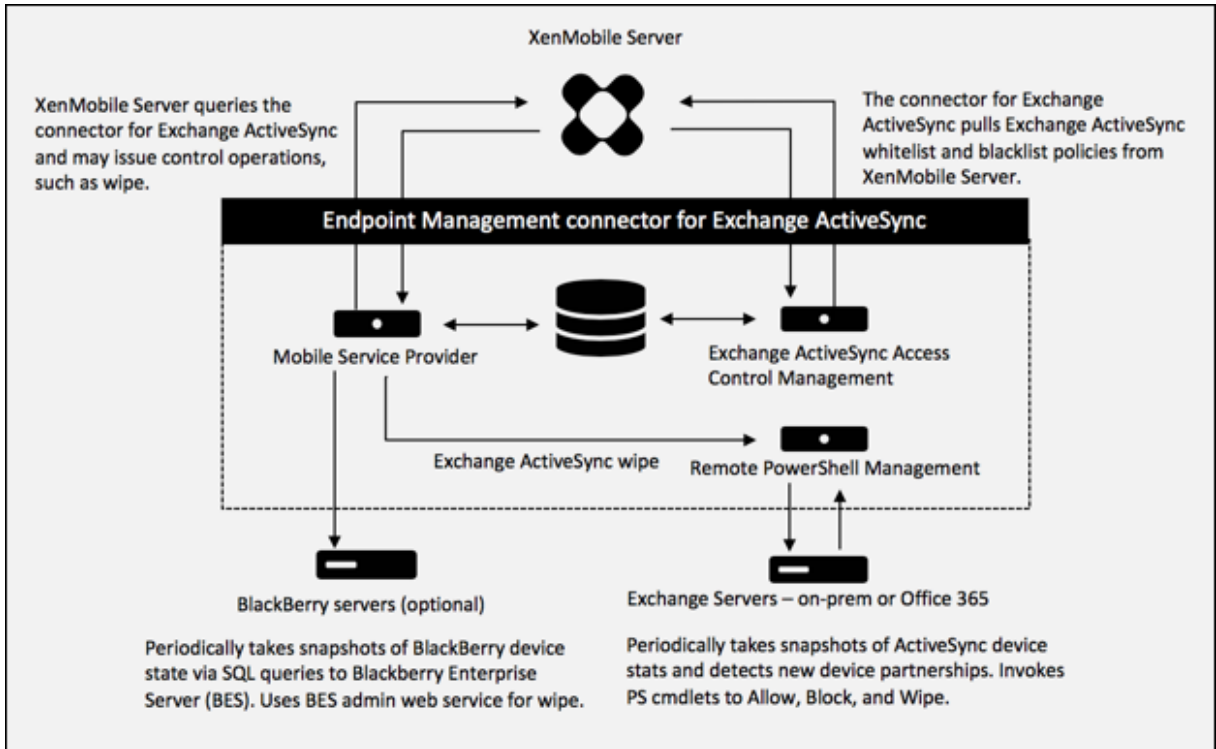
- 스냅샷워크플로개선: 주스냅샷을생성하는데시간이오래걸리고프로세스가복잡합니다. 이제스냅샷생성중에오류가발생할
경우 XenMobile Mail Manager 가여러번의시도 (최대 3 회) 를통해스냅샷을완료합니다. 후속시도는처음부터시작
되지않습니다. XenMobile Mail Manager 는중단된위치에서시도를계속합니다. 스냅샷을진행하는동안일시적인오류
를넘길수있으므로일반적으로스냅샷성공률이개선됩니다.
- 진단개선: 스냅샷중에서선택적으로생성할수있는새로운세가지진단파일을사용하여스냅샷문제를이제보다쉽게해결할수있
습니다. 이러한파일은 PowerShell 명령문제, 정보가누락된사서함및사서함에연결할수없는장치를식별하는데도움이되
니다. 관리자는이러한파일을사용하여 Exchange 에서수정할수없는데이터를식별할수있습니다.
- 메모리사용개선: 이제 XenMobile Mail Manager 가보다효율적으로메모리를사용합니다. 관리자는 XenMobile
Mail Manager 를자동으로다시시작하도록예약하여시스템에정리된슬레이트를제공할수있습니다.
- **Microsoft .NET Framework 4.6** 사전요구사항: Microsoft .NET Framework 의사전요구사항은이제버전
4.6 입니다.

수정된문제

- 자격증명오류표시: 이오류는종종 Office 365 세션불안정으로인해발생했습니다. Exchange 에대한연결개선으로이문
제가해결됩니다. (XMHELP-293, XMHELP-311, XMHELP-801)
- 정확하지않은사서함및장치수: XenMobile Mail Manager 의사서함-장치연결알고리즘이개선되었습니다. 개선된
진단기능을사용하면 XenMobile Mail Manager 가책임영역내에없다고간주하는사서함및장치를식별할수있습니다.
(XMHELP-623)
- 허용/차단/초기화명령이인식되지않음: 가끔 XenMobile Mail Manager 허용/차단/초기화명령이인식되지않는버그
가수정되었습니다. (XMHELP-489)
- 메모리관리: 메모리관리및안화가개선되었습니다. (XMHELP-419)

아키텍처

다음그림에서는 Exchange ActiveSync 용 Endpoint Management 커넥터의주요구성요소를보여줍니다. 자세한참조아
키텍처다이어그램은 [아키텍처](#)를참조하십시오.



세가지주요구성요소는다음과같습니다.

- **Exchange ActiveSync 액세스제어관리:** XenMobile 과통신하여 XenMobile 에서 Exchange ActiveSync 정책을검색하고이정책을로컬로정의된정책과병합하여 Exchange 에대한액세스가허용또는거부되어야하는 Exchange ActiveSync 장치를결정합니다. 로컬정책을통해 Active Directory 그룹, 사용자, 장치유형또는장치사용자아이전트 (일반적으로모바일플랫폼버전) 별로액세스제어를허용하도록정책규칙을확장할수있습니다.
- 원격 **PowerShell** 관리: 원격 PowerShell 명령을예약하고호출하여 Exchange ActiveSync Access Control Management 에서작성된정책을시행합니다. 주기적으로 Exchange ActiveSync 데이터베이스의스냅샷을생성하여변경되었거나새로운 Exchange ActiveSync 장치를감지합니다.
- 모바일서비스공급자: XenMobile 이 Exchange ActiveSync 및/또는 Blackberry 장치를관리하고이러한장치에 대한초기화같은제어작업을실행할수있도록웹서비스인터페이스를제공합니다.

시스템요구사항및사전요구사항

다음은 Exchange ActiveSync 용 Endpoint Management 커넥터를사용하는데필요한최소시스템요구사항입니다.

- Windows Server 2016, Windows Server 2012 R2 또는 Windows Server 2008 R2 서비스팩 1. 영어기반 서버여야합니다. Windows Server 2008 R2 서비스팩 1 에대한지원은 2020 년 1 월 14 일에종료됩니다.
- Microsoft SQL Server 2016 서비스팩 2, SQL Server 2014 서비스팩 3 또는 SQL Server 2012 서비스팩 4.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, 버전 5(선택사항).

Microsoft Exchange Server 의지원되는최소버전

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 서비스팩 3(2020 년 1 월 14 일에지원종료)

사전요구사항

- Windows Management Framework 가설치되어있어야합니다.
 - PowerShell V5, V4, V3
- PowerShell 실행정책이 Set-ExecutionPolicy RemoteSigned 를통해 RemoteSigned 로설정되어있어야합니다.
- Exchange ActiveSync 용 Endpoint Management 커넥터를실행하는컴퓨터와원격 Exchange Server 사이에 TCP 포트 80 이열려있어야합니다.
- 장치전자메일클라이언트: 일부전자메일클라이언트는한장치에대해동일한 ActiveSync ID 를일관되게반환하지않습니다. Exchange ActiveSync 용 Endpoint Management 커넥터에서는각장치에고유한 ActiveSync ID 를사용하도록요구하므로각장치에대해동일하고유 ActiveSync ID 를일관되게생성하는전자메일클라이언트만지원됩니다. 다음과같은전자메일클라이언트는 Citrix 의테스트에서오류없이실행되는것으로확인되었습니다.
 - HTC 기본전자메일클라이언트
 - Samsung 기본전자메일클라이언트
 - iOS 기본전자메일클라이언트
 - 스마트폰에대한 TouchDown
- **Exchange:** Exchange 를실행하는온-프레미스컴퓨터의요구사항은다음과같습니다.

Exchange 구성 UI 에지정된자격증명으로 Exchange Server 에연결할수있고다음 Exchange 관련 PowerShell cmdlet 을실행할수있는전체권한이이자격증명에있어야합니다.

- **Exchange Server 2010 SP2 의경우:**
 - * Get-CASMailbox
 - * Set-CASMailbox
 - * Get-Mailbox
 - * Get-ActiveSyncDevice
 - * Get-ActiveSyncDeviceStatistics
 - * Clear-ActiveSyncDevice
 - * Get-ExchangeServer
 - * Get-ManagementRole
 - * Get-ManagementRoleAssignment
- **Exchange Server 2013 및 Exchange Server 2016 의경우:**
 - * Get-CASMailbox

- * Set-CASMailbox
 - * Get-Mailbox
 - * Get-MobileDevice
 - * Get-MobileDeviceStatistics
 - * Clear-MobileDevice
 - * Get-ExchangeServer
 - * Get-ManagementRole
 - * Get-ManagementRoleAssignment
- Exchange ActiveSync 용 Endpoint Management 커넥터가 전체 포리스트를 보도록 구성된 경우 **Set-AdServerSettings -ViewEntireForest \$true** 를 실행할 수 있는 권한이 부여되어 있어야 합니다.
 - 제공된 자격 증명에 원격 셸을 통해 Exchange Server 에 연결할 수 있는 권한이 있어야 합니다. 기본적으로 Exchange 를 설치한 사용자가 이 권한을 갖습니다.
 - Microsoft TechNet 문서 [about_Remote_Requirements](#)에 따라 원격 연결을 설정하고 원격 명령을 실행하려면 원격 컴퓨터 관리자인 사용자에게 해당하는 자격 증명이어야 합니다. Set-PSSessionConfiguration 을 사용하여 관리요구사항을 제거할 수 있지만 이 명령에 대한 설명은 이 문서에 나와 있지 않습니다. 자세한 내용은 이 블로그 게시물 ([You Don't Have to Be An Administrator to Run Remote PowerShell Commands\(관리자 권한 없이 PowerShell 명령을 실행하는 방법\)](#)) 을 참조하십시오.
 - HTTP 를 통해 원격 PowerShell 요청을 지원하도록 Exchange Server 를 구성해야 합니다. 일반적으로 Exchange Server 에서 다음 PowerShell 명령을 실행하는 관리자이면 됩니다. WinRM QuickConfig.
 - Exchange 에는 많은 제한 정책이 있습니다. 정책 중 하나는 사용자당 허용되는 동시 PowerShell 연결 수를 제어합니다. Exchange 2010 의 경우 사용자당 허용되는 동시 연결 수의 기본값은 18 입니다. 연결 제한에도 달하면, Exchange ActiveSync 용 Endpoint Management 커넥터에서 Exchange Server 에 연결할 수 없습니다. PowerShell 을 통해 허용되는 최대 동시 연결 수를 변경하는 방법이 있지만 이 문서의 범위를 벗어났습니다. 관심 있는 경우 PowerShell 을 통한 원격 관리와 관련된 Exchange 제한 정책에 대해 알아보십시오.

Office 365 Exchange 에 대한 요구사항

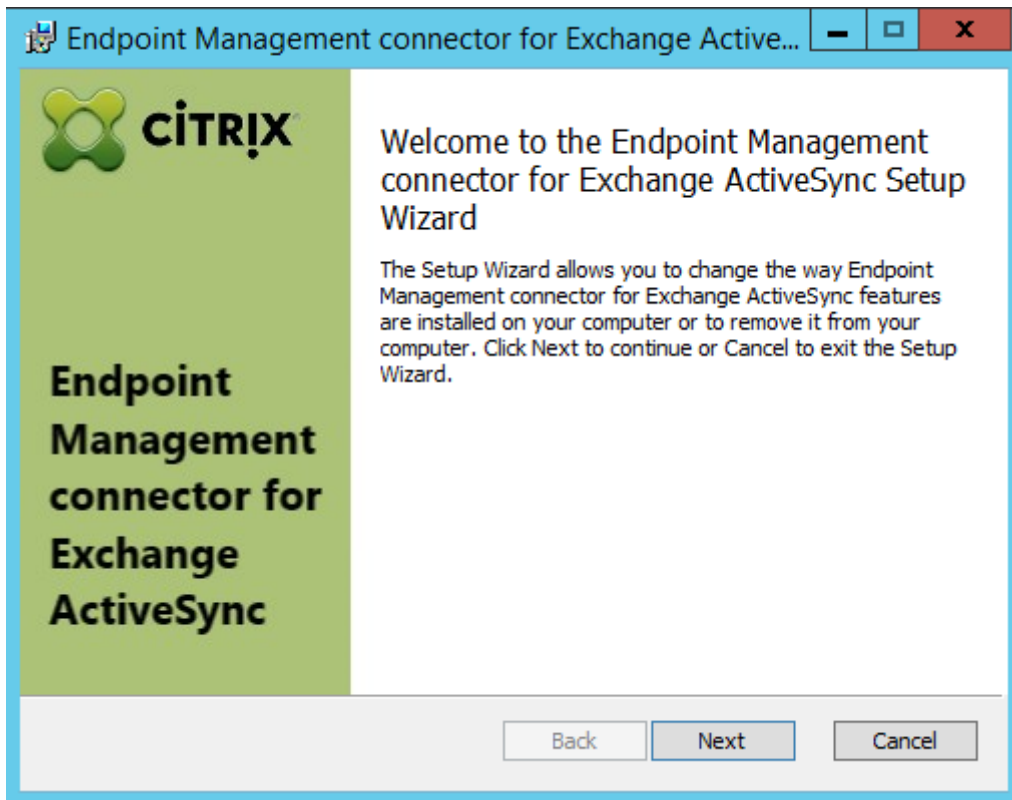
- 권한: Exchange 구성 UI 에 지정된 자격 증명으로 Office 365 에 연결할 수 있고 다음 Exchange 관련 PowerShell cmdlet 을 실행할 수 있는 전체 권한이 자격 증명에 있어야 합니다.
 - Get-CASMailbox
 - Set-CASMailbox
 - Get-Mailbox
 - Get-MobileDevice
 - Get-MobileDeviceStatistics
 - Clear-MobileDevice
 - Get-ExchangeServer
 - Get-ManagementRole
 - Get-ManagementRoleAssignment
- 권한: 제공된 자격 증명에 원격 셸을 통해 Office 365 서버에 연결할 수 있는 권한이 있어야 합니다. 기본적으로 Office 365

온라인관리자에게는필수권한이있습니다.

- **제한정책:** Exchange 에는많은제한정책이있습니다. 정책중하나사용자당허용되는동시 PowerShell 연결수를제어합니다. Office 365 의경우사용자당허용되는동시연결수의기본값은 3 입니다. 연결제한에도달하면, Exchange ActiveSync 용 Endpoint Management 커넥터에서 Exchange Server 에연결할수없습니다. PowerShell 을 통해허용되는최대동시연결수를변경하는방법이있지만문서의범위를벗어나있습니다. 관심있는경우 PowerShell 을 통한원격관리와관련된 Exchange 제한정책에대해알아보십시오.

설치및구성

1. XmmSetup.msi 파일을클릭한후설치프로그램의메시지에따라 Exchange ActiveSync 용 Endpoint Management 커넥터를설치합니다.
2. 설치방법사의마지막화면에서 **Launch the Configure utility(구성유틸리티실행)** 를선택한상태로됩니다. 또는 **Start(시작)** 메뉴에서 Exchange ActiveSync 용 Endpoint Management 커넥터를열니다.

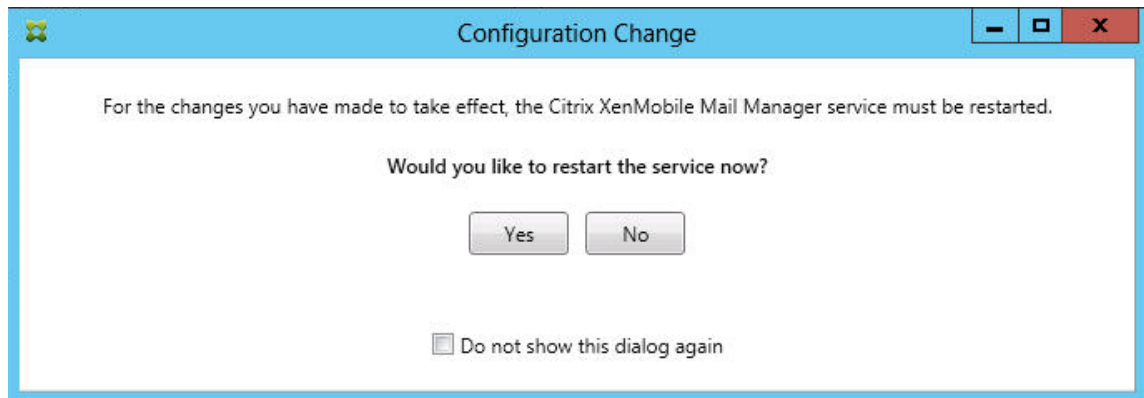


3. 다음데이터베이스속성을구성합니다.
 - **Configure(구성) > Database(데이터베이스)** 탭을선택합니다.
 - SQL Server 의이름을입력합니다 (기본값은 localhost).
 - 데이터베이스를기본값인 **CitrixXmm** 으로유지합니다.
4. SQL 에사용되는다음인증모드중하나를선택합니다.
 - **SQL:** 유효한 SQL 사용자의사용자이름과암호를입력합니다.

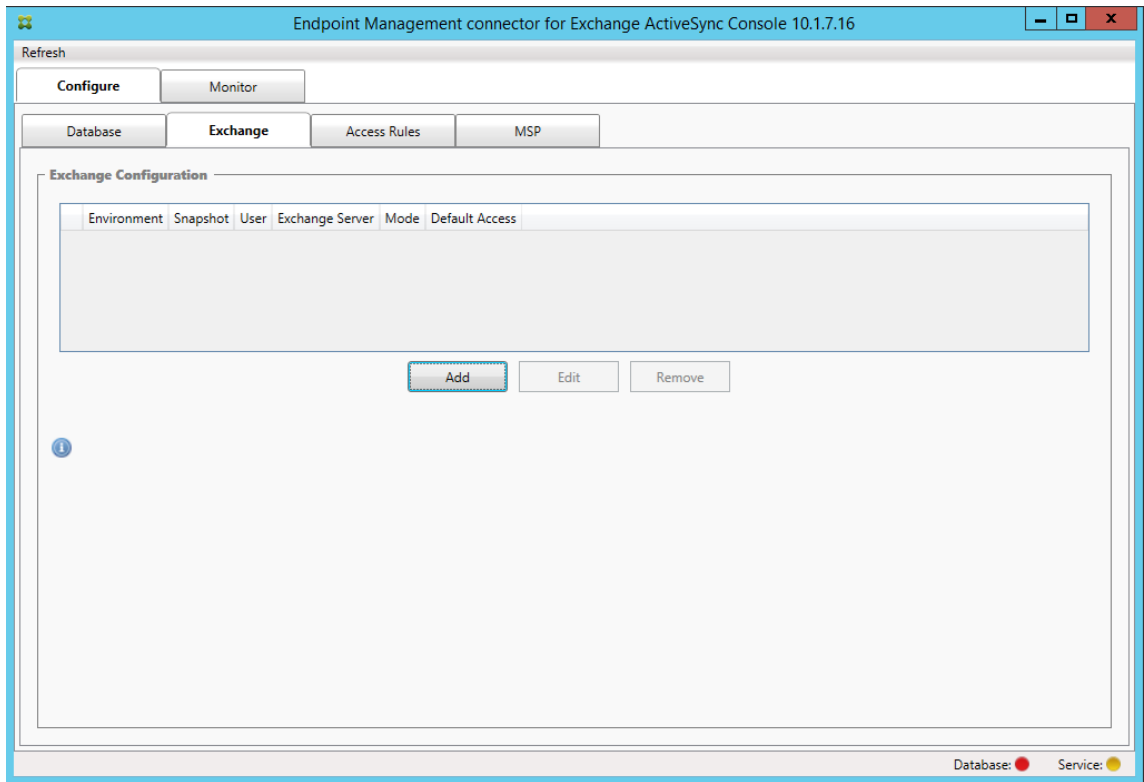
- **Windows Integrated(Windows 통합):** 이 옵션을 선택하는 경우 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스의 로그인 자격 증명을 SQL Server 액세스 권한이 있는 Windows 계정으로 변경해야 합니다. 이렇게 하려면 제어판 > 관리도구 > 서비스를 열고 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스 항목을 마우스 오른쪽 단추로 클릭한 후 로그인 탭을 클릭합니다.

BlackBerry 데이터베이스 연결에 Windows 통합을 선택하는 경우 여기서 지정하는 Windows 계정에 BlackBerry 데이터베이스 액세스 권한이 있어야 합니다.

5. **Test Connectivity(연결 테스트)** 를 클릭하여 SQL Server 에 연결되는지 확인한 후 **Save(저장)** 를 클릭합니다.
6. 서비스를 다시 시작하라는 메시지가 표시됩니다. **Yes(예)** 를 클릭합니다.



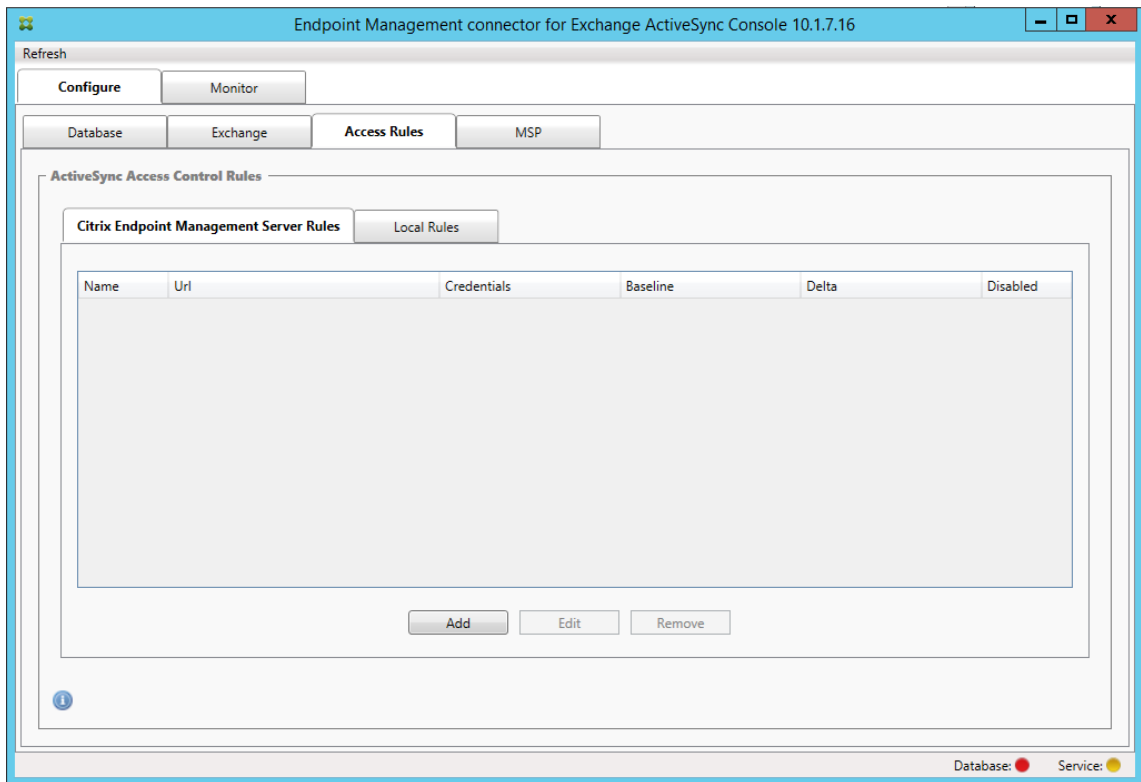
7. 하나 이상의 Exchange Server 를 구성합니다.
 - 단일 Exchange 환경을 관리하는 경우 단일 서버만 지정합니다. 여러 Exchange 환경을 관리하는 경우 각 Exchange 환경에 하나의 Exchange Server 를 지정합니다.
 - **Configure(구성) > Exchange** 탭을 클릭하고 **Add(추가)** 를 클릭합니다.



8. Exchange Server 환경유형을 **On Premise(온프레미스)** 또는 **Office 365** 중에서선택합니다.

- **On Premise(온-프레미스)** 를선택하는경우원격 PowerShell 명령에서사용할 Exchange Server 의이름을입력합니다.
- Requirements(요구사항) 섹션에명시된대로적절한 Exchange Server 권한이있는 Windows ID 의 사용자 이름을입력하고사용자에대한 암호를입력합니다.
- 주스냅샷을실행할일정을선택합니다. 주스냅샷은모든 Exchange ActiveSync 파트너관계를검색합니다.
- 부스냅샷을실행할일정을선택합니다. 부스냅샷은새로생성된 Exchange ActiveSync 파트너관계를검색합니다.
- 스냅샷유형을 **Deep(전체)** 또는 **Shallow(단순)** 중에서선택합니다. 단순스냅샷은일반적으로훨씬빠르며 Exchange ActiveSync 용 Endpoint Management 커넥터의모든 Exchange ActiveSync 액세스제어 기능을수행하기에충분합니다. 전체스냅샷은더긴시간이소요될수있으며 ActiveSync 에대해모바일서비스공급자를사용하는경우에만필요합니다. 이옵션을사용하면 XenMobile 에서관리되지않는장치를관리할수있습니다.
- **Allow(허용)**, **Block(차단)** 또는 **Unchanged(변경되지않음)** 중에서기본액세스권한을선택합니다. 이설정은 명시적인 XenMobile 또는로컬규칙에의해식별되지않은모든장치를어떻게처리할지를제어합니다. **Allow(허용)** 를선택하면이러한모든장치에대한 ActiveSync 액세스가허용됩니다. **Block(차단)** 을선택하면액세스가거부됩니다. **Unchanged(변경되지않음)** 를선택하면변경이수행되지않습니다.
- **PowerShell** 또는 **Simulation(시뮬레이션)** 중에서 ActiveSync 명령모드를선택합니다.
- **PowerShell** 모드에서 Exchange ActiveSync 용 Endpoint Management 커넥터는 PowerShell 명령을실행하여원하는액세스제어를수행합니다. 시뮬레이션모드에서 Exchange ActiveSync 용 Endpoint Management 커넥터는 PowerShell 명령을실행하지않지만의도한명령및의도한결과를데이터베이스에기록합니다. 시뮬레이션모드에서사용자는 **Monitor(모니터)** 탭을사용하여 PowerShell 모드를사용할경우일어나는결과를볼수있습니다.

- **Connection Expiration(연결만료)** 에서연결수명에대한시간및분을설정합니다. 연결이지정된수명에도달하면만료된연결로표시되고다시사용되지않습니다. 만료된연결이더이상사용되지않으면 Exchange ActiveSync 용 Endpoint Management 커넥터가연결을정상적으로종료합니다. 연결이다시필요한경우사용할수있는연결이없으면새연결이초기화됩니다. 지정되지않은경우기본값인 30 분이사용됩니다.
 - **View Entire Forest(전체포리스트보기)** 를선택하여 Exchange 환경의전체 Active Directory 포리스트를보도록 Exchange ActiveSync 용 Endpoint Management 커넥터를구성합니다.
 - **Kerberos** 또는 **Basic(기본)** 중에서인증프로토콜을선택합니다. Exchange ActiveSync 용 Endpoint Management 커넥터는온-프레미스배포에서기본인증을지원합니다. 따라서 Exchange ActiveSync 용 Endpoint Management 커넥터가 Exchange Server 가상주하는도메인의구성원이아닌경우 Exchange ActiveSync 용 Endpoint Management 커넥터를사용할수있습니다.
 - **Test Connectivity(연결테스트)** 를클릭하여 Exchange Server 에연결되는지확인한후 **Save(저장)** 를클릭합니다.
 - 서비스를다시시작하라는메시지가표시됩니다. **Yes(예)** 를클릭합니다.
9. 액세스규칙을구성합니다. **Configure(구성) > Access Rules(액세스규칙)** 탭을선택하고 **XMS Rules(XMS 규칙)** 탭을클릭한다음 **Add(추가)** 를클릭합니다.



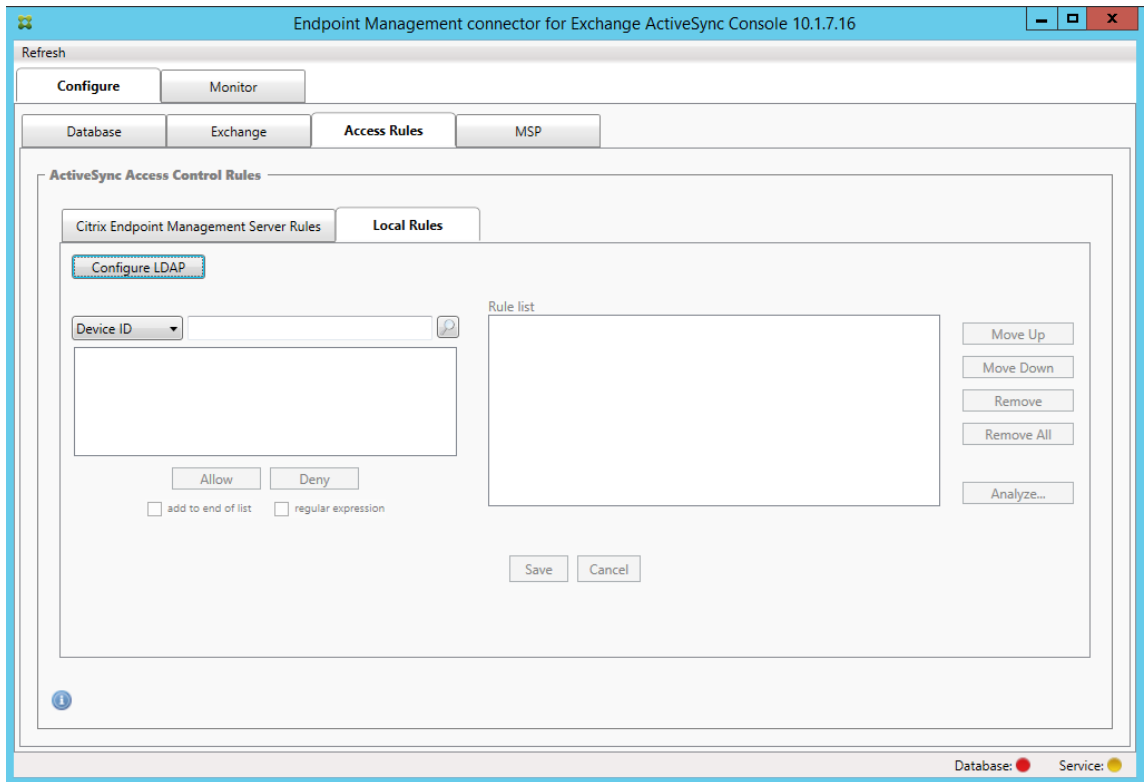
10. **XenMobile server Service Properties(XenMobile 서버서비스속성)** 페이지에서 XenMobile Server 를 가리키도록 URL 문자열을수정합니다. 예를들어인스턴스이름이 **zdm** 인경우 <https://<XdmHostName>/zdm/services/MagConfigService>를입력합니다. 이에에서는 **XdmHostName** 을 XenMobile Server 의 IP 또는 DNS 주소로바꿉니다.



- 권한이있는서버사용자를입력합니다.
- 사용자의암호를입력합니다.
- **Baseline Interval**(기준간격), **Delta Interval**(델타간격) 및 **Timeout values**(시간초과값) 를기본값으로유지합니다.
- **Test Connectivity**(연결테스트) 를클릭하여서버연결을확인한후 **OK**(확인) 를클릭합니다.

Disabled(사용안함) 확인란이선택된경우 XenMobile 메일서비스가 XenMobile 에서정책을수집하지않습니다.

11. **Local Rules**(로컬규칙) 탭을클릭합니다.

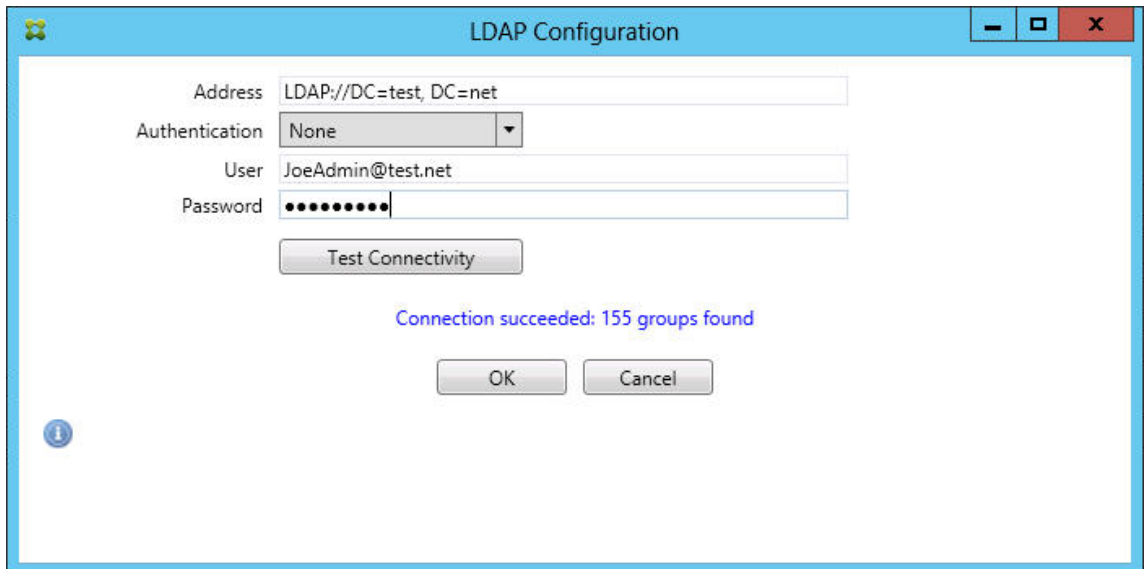


- ActiveSync 장치 ID, 장치유형, AD 그룹, 사용자또는장치 UserAgent 를기준으로로컬규칙을추가할수있습니다. 목록에서해당하는유형을선택합니다.
- 텍스트상자에텍스트또는텍스트부분을입력합니다. 필요한경우쿼리단추를클릭하여부분과일치하는엔터티를봅니다.

Group(그룹) 유형이아닌다른모든유형은스냅샷에서검색된장치에기반합니다. 따라서스냅샷을시작하고완료하지않은경우엔터티가제공되지않습니다.

- 텍스트값을선택한후 **Allow(허용)** 또는 **Deny(거부)** 를클릭하여오른쪽의 **Rule List(규칙목록)** 창에추가합니다. **Rule List(규칙목록)** 창오른쪽의단추를사용하여규칙순서를변경하거나제거할수있습니다. 규칙은지정된사용자및장치에대해규칙이표시된순서로평가되고순서가높은규칙 (최상위규칙에가까운규칙) 에대한일치항목이검색되면다음규칙이적용되지않으므로그순서가중요합니다. 예를들어모든 iPad 장치를허용하는규칙과사용자 Matt 를차단하는후속규칙이있는경우 iPad 규칙이 Matt 규칙보다적용우선순위가높으므로 Matt 의 iPad 가허용됩니다.
- 규칙목록내의규칙을분석하여잠재적재정의, 충돌또는보조구성을찾으려면 **Analyze(분석)** 를클릭하고 **Save(저장)** 를클릭합니다.

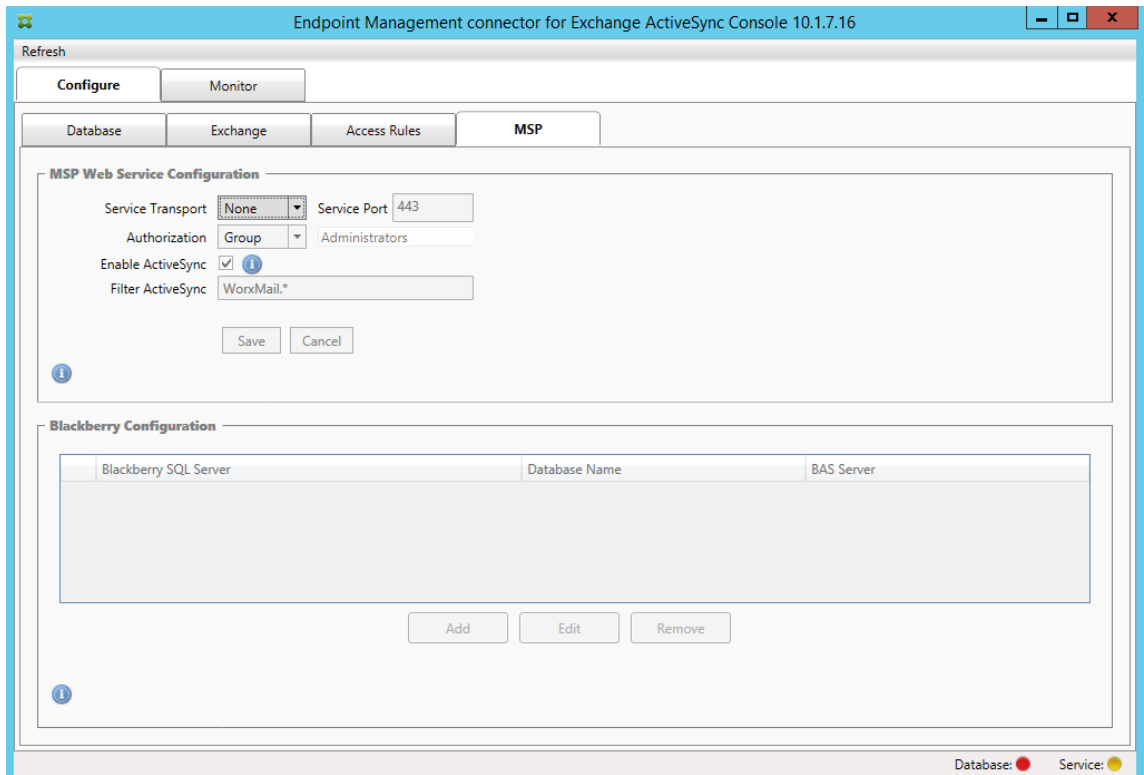
12. Active Directory 그룹에서작동하는로컬규칙을구성하려는경우 **Configure LDAP(LDAP 구성)** 를클릭한후 LDAP 연결속성을구성합니다.



13. 모바일서비스공급자를구성합니다.

모바일서비스공급자는선택사항입니다. 이설정은모바일서비스공급자인터페이스를사용하여관리되지않는장치를쿼리하도록 XenMobile 을구성한경우에만필요합니다.

- **Configure(구성) > MSP** 탭을클릭합니다.



- 모바일서비스공급자서비스에대한 Service Transport(서비스전송) 유형을 **HTTP** 또는 **HTTPS** 로설정합니다.

- 모바일서비스공급자서비스에대한 서비스포트 (일반적으로 80 또는 443) 를설정합니다. 포트 443 을사용하는경우 IIS 에서포트에바인딩된 SSL 인증서가필요합니다.
- **Authorization Group(인증그룹)** 또는 **User(사용자)** 를설정합니다. 이설정은 XenMobile 에서모바일서비스공급자서비스에연결할수있는사용자또는사용자집합을설정합니다.
- ActiveSync 쿼리를사용할지여부를설정합니다. XenMobile Server 에대해 ActiveSync 쿼리를사용하는경우하나이상의 Exchange Server 에대한스냅샷유형을 **Deep(전체)** 으로설정해야합니다. 이경우스냅샷생성시 성능이크게저하될수있습니다.
- 기본적으로정규식 WorxMail.* 와일치하는 ActiveSync 장치는 XenMobile 로전송되지않습니다. 이동작을변경하려면 **Filter ActiveSync(ActiveSync 필터링)** 필드를필요에따라변경합니다.
비워두면모든장치가 XenMobile 에전달됩니다.
- 저장을클릭합니다.

14. 필요한경우 BES(BlackBerry Enterprise Server) 를구성합니다. **Add(추가)** 를클릭하고 BES SQL Server 의서버이름을입력합니다.

- BES 관리데이터베이스의데이터베이스이름을입력합니다.
- **Authentication(인증)** 모드를선택합니다. Windows 통합인증을선택하는경우 Exchange ActiveSync 용

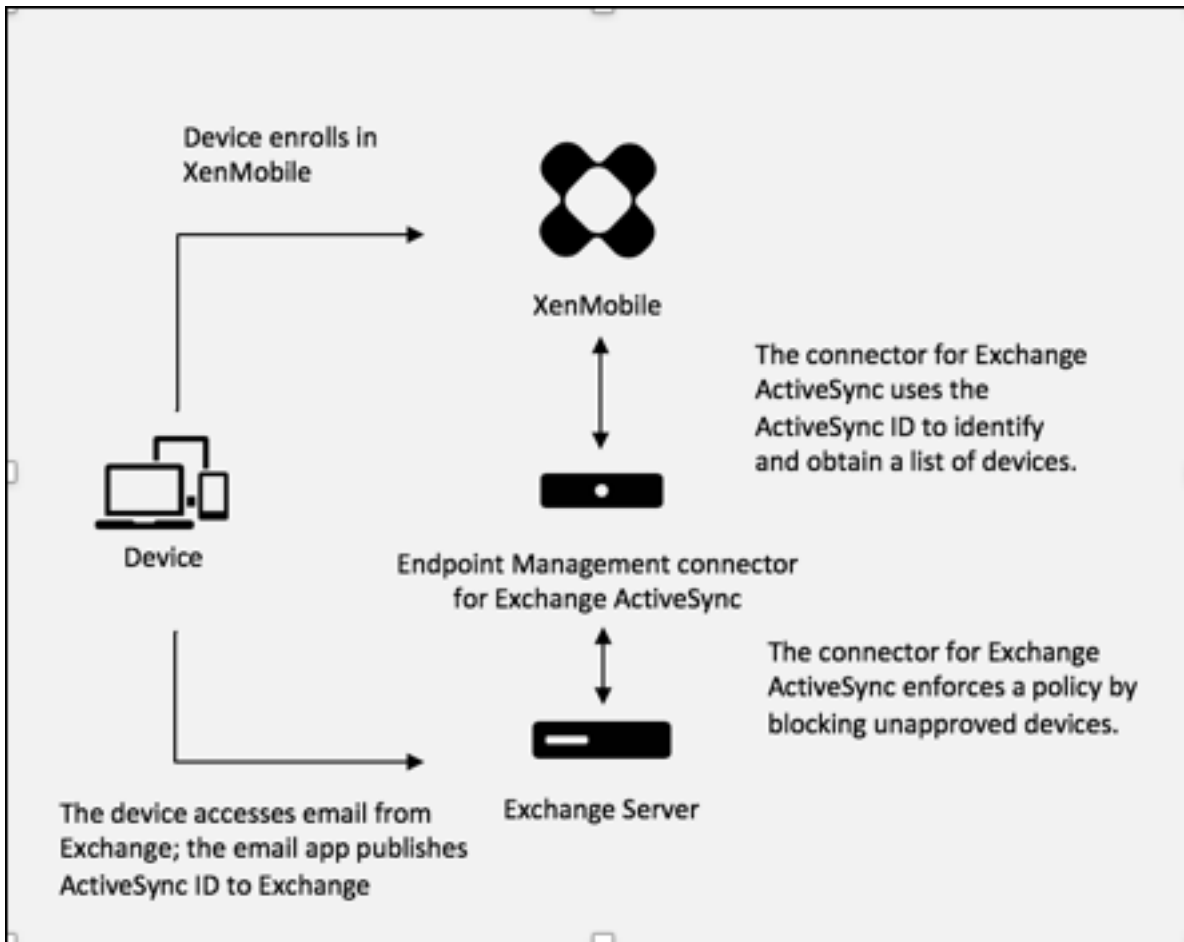
Endpoint Management 커넥터서비스의사용자계정이 BES SQL Server 에연결할때사용되는계정입니다. Exchange ActiveSync 용 Endpoint Management 커넥터데이터베이스연결에대해서도 Windows 통합 인증을선택하는경우여기서지정한 Windows 계정에 Exchange ActiveSync 용 Endpoint Management 커넥터데이터베이스에액세스할수있는권한이있어야합니다.

- **SQL authentication(SQL 인증)** 을선택하는경우사용자이름과암호를입력합니다.
- **Sync Schedule(동기화일정)** 을설정합니다. BES SQL Server 에연결할때사용되는일정이며모든장치업데이트를확인합니다.
- **Test Connectivity(연결테스트)** 를클릭하여 SQL Server 연결을확인합니다. Windows 통합을선택하는경우 Exchange ActiveSync 용 Endpoint Management 커넥터서비스사용자가아닌현재로그온한사용자를사용하여테스트가수행되므로 SQL 인증이정확히테스트되지않습니다.
- XenMobile 에서 BlackBerry 장치의원격초기화및암호재설정을지원하려면 **Enabled(사용)** 확인란을선택합니다.
- BES FQDN(정규화된도메인이름) 을입력합니다.
- 관리웹서비스에사용되는 BES 포트를입력합니다.
- BES 서비스에필요한정규화된사용자및암호를입력합니다.
- **Test Connectivity(연결테스트)** 를클릭하여 BES 연결을테스트합니다.
- 저장을클릭합니다.

ActiveSync ID 를사용하여전자메일정책적용

회사전자메일정책에따라특정장치가회사전자메일을사용하도록승인되지않을수있습니다. 이정책을준수하려면직원이그와같은 장치에서회사전자메일에액세스할수없도록해야합니다. Exchange ActiveSync 용 Endpoint Management 커넥터및 XenMobile 은함께작동하여이러한전자메일정책을적용합니다. XenMobile 은회사전자메일액세스에대한정책을설정하고승인되지않은장치가 XenMobile 에등록하면 Exchange ActiveSync 용 Endpoint Management 커넥터가정책을적용합니다.

장치의전자메일클라이언트는장치를식별하는데사용되는장치 ID(ActiveSync ID 라고도함) 를사용하여자신을 Exchange Server(또는 Office 365) 에알립니다. Secure Hub 는유사한식별자를구하고장치가등록될때 XenMobile 에해당식별자를보냅니다. 두장치 ID 를비교하여 Exchange ActiveSync 용 Endpoint Management 커넥터는특정장치에회사전자메일액세스권한이있는지여부를결정할수있습니다. 다음그림에서는이개념을보여줍니다.



XenMobile 이장치가게시하는 ID 와다른 Exchange ActiveSync 용 Endpoint Management 커넥터 ID 를 Exchange 에보내는경우 Exchange ActiveSync 용 Endpoint Management 커넥터가장치로수행할작업을 Exchange 에알릴수없 습니다.

ActiveSync ID 일치는대부분의플랫폼에서안정적으로작동합니다. 하지만일부 Android 구현환경에서장치의 ActiveSync ID 가메일클라이언트가 Exchange 에알리는 ID 와다르다는것이밝혀졌습니다. 이문제를완화하려면다음을수행할수있습니다.

- Samsung SAFE 플랫폼에서는 XenMobile 에서장치 ActiveSync 구성을푸시합니다.
- 다른모든 Android 플랫폼에서는 XenMobile 에서 TouchDown 앱과 TouchDown ActiveSync 구성을모두푸 시합니다.

하지만이렇게해도직원이 Android 장치에 TouchDown 이외의전자메일클라이언트를설치하는것은막을수없습니다. 회사전 자메일액세스정책이올바르게적용되도록하려면방어적보안입장을채택하고기본적으로거부하는정책정책을설정하여전자메일을 차단하도록 Exchange ActiveSync 용 Endpoint Management 커넥터를구성할수있습니다. 즉, 직원이 Android 장치 에서 TouchDown 이외의전자메일클라이언트를구성하는경우와 ActiveSync ID 검색이제대로작동하지않는경우해당직원의 회사전자메일액세스가거부됩니다.

액세스제어규칙

Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange ActiveSync 장치에 대한 액세스제어를동적으로 구성하는 규칙 기반 접근 방식을 제공합니다. Exchange ActiveSync 용 Endpoint Management 커넥터 액세스제어 규칙은 일치하는 식과 원하는 액세스 상태 (허용 또는 차단) 의 두 부분으로 구성됩니다. 지정된 Exchange ActiveSync 장치에 대해 규칙을 평가하여 규칙이 장치에 적용되는지 또는 장치와 일치하는지를 결정할 수 있습니다. 일치하는 식에는 여러 종류가 있습니다. 예를 들어 규칙은 지정된 장치 유형 의 모든 장치 또는 특정 Exchange ActiveSync 장치 ID 또는 특정 사용자의 모든 장치와 일치할 수 있습니다.

규칙 목록의 규칙을 추가, 제거 및 재정렬하는 동안 언제든지 **Cancel(취소)** 단추를 클릭하면 처음 규칙 목록을 열었을 때의 상태로 목록이 되돌려집니다. **Save(저장)** 를 클릭하지 않고 구성 도구를 닫으면 이 창에서 수행한 변경 내용이 손실됩니다.

Exchange ActiveSync 용 Endpoint Management 커넥터에는 로컬 규칙, XenMobile Server 규칙 (XDM 규칙이라고도 함) 및 기본 액세스 규칙의 세 가지 규칙이 있습니다.

로컬 규칙: 로컬 규칙은 우선 순위가 가장 높습니다. 로컬 규칙에 일치하는 장치가 있을 경우 규칙 평가가 중지됩니다. XenMobile Server 규칙 또는 기본 액세스 규칙은 확인되지 않습니다. 로컬 규칙은 **Configure(구성) > Access Rules(액세스 규칙) > Local Rules(로컬 규칙)** 탭을 통해 Exchange ActiveSync 용 Endpoint Management 커넥터에 로컬로 구성됩니다. 지원 일치 지정된 Active Directory 그룹 내의 사용자 구성원 자격에 기반합니다. 지원 일치는 다음 필드에 대한 정규식에 기반합니다.

- ActiveSync Device ID(ActiveSync 장치 ID)
- ActiveSync Device Type(ActiveSync 장치 유형)
- User Principal Name (UPN)(UPN(사용자 계정 이름))
- ActiveSync User Agent(ActiveSync 사용자 에이전트)(일반적으로 장치 플랫폼 또는 전자 메일 클라이언트)

주소 검색이 완료되고 장치를 찾은 경우 일반 또는 정규식 규칙을 추가할 수 있습니다. 주소 검색이 완료되지 않은 경우 정규식 규칙만 추가할 수 있습니다.

XenMobile 서버 규칙: XenMobile Server 규칙은 관리되는 장치에 대한 규칙을 제공하는 외부 XenMobile Server 에 대한 참조입니다. XenMobile Server 는 XenMobile 에 알려진 속성 (예: 장치가 탈옥 장치인지 여부 또는 장치에 금지된 앱이 포함되어 있는지 여부) 을 기반으로 장치를 허용 또는 차단된 장치로 식별하는 간략한 규칙으로 구성될 수 있습니다. XenMobile 은 이 간략한 규칙을 평가하고 허용 또는 차단된 ActiveSync 장치 ID 집합을 생성한 다음 Exchange ActiveSync 용 Endpoint Management 커넥터에 전달합니다.

기본 액세스 규칙: 기본 액세스 규칙은 잠재적으로 모든 장치와 일치할 수 있고 항상 마지막에 평가된다는 것이 특징입니다. 이 규칙은 지정된 장치가 로컬 또는 XenMobile Server 규칙과 일치하지 않을 경우 기본 액세스 규칙의 원하는 액세스 상태가 장치의 원하는 액세스 상태를 결정하는 광범위한 규칙입니다.

- **Default Access - Allow(기본 액세스 - 허용):** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치가 허용됩니다.
- **Default Access - Block(기본 액세스 - 차단):** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치가 차단됩니다.
- **Default Access - Unchanged(기본 액세스 - 변경되지 않음):** 로컬 또는 XenMobile Server 규칙과 일치하지 않는 모든 장치의 액세스 상태가 Exchange ActiveSync 용 Endpoint Management 커넥터에 의해 수정되지 않습니다.

장치가 Exchange 에의해격리모드에배치된경우아무런동작도수행되지않습니다. 예를들어장치를격리모드에서제거하는유일한방법은로컬또는 XDM 규칙으로격리를명시적으로재정의하는것입니다.

규칙평가정보

Exchange 가 Exchange ActiveSync 용 Endpoint Management 커넥터에보고하는각장치에대해다음과같이높은우선순위에서낮은우선순위로규칙이평가됩니다.

- 로컬규칙
- XenMobile Server 규칙
- 기본액세스규칙

일치가발견되면평가가중지됩니다. 예를들어로컬규칙이지정된장치와일치할경우 XenMobile Server 규칙또는기본액세스규칙으로장치가평가되지않습니다. 이는지정된규칙유형내에서도마찬가지입니다. 예를들어로컬규칙목록에지정된장치와일치하는규칙이둘이상인경우첫번째일치가발견되면평가가중지됩니다.

장치속성이변경되거나장치가추가또는제거되거나규칙자체가변경될경우 Exchange ActiveSync 용 Endpoint Management 커넥터가현재정의된규칙집합을다시평가합니다. 주스냅샷은구성가능한간격으로장치속성변경및제거를확인합니다. 부스냅샷은구성가능한간격으로새장치를확인합니다.

Exchange ActiveSync 에도액세스를제어하는규칙이있습니다. Exchange ActiveSync 용 Endpoint Management 커넥터의컨텍스트에서이러한규칙의작동방식을이해하는것이중요합니다. Exchange 는개별면제, 장치규칙및조직설정의세가지규칙수준으로구성될수있습니다. Exchange ActiveSync 용 Endpoint Management 커넥터는개별면제목록에영향을주는원격 PowerShell 요청을프로그래밍방식으로실행하여액세스제어를자동화합니다. 개별면제목록은지정된사서함에연결된허용또는차단된 Exchange ActiveSync 장치 ID 의목록입니다. Exchange ActiveSync 용 Endpoint Management 커넥터를배포하면 Exchange 내면제목록의관리가실질적으로커넥터에이전됩니다. 자세한내용은 [Microsoft article](#)를참조하십시오.

분석은동일한필드에여러규칙이정의된경우특히유용합니다. 규칙간의관계문제를해결할수있습니다. 분석은규칙필드의관점에서수행됩니다. 예를들어 ActiveSync 장치 ID, ActiveSync 장치유형, 사용자, 사용자에이전트등일치되는필드에기반한그루프로규칙이분석됩니다.

규칙용어

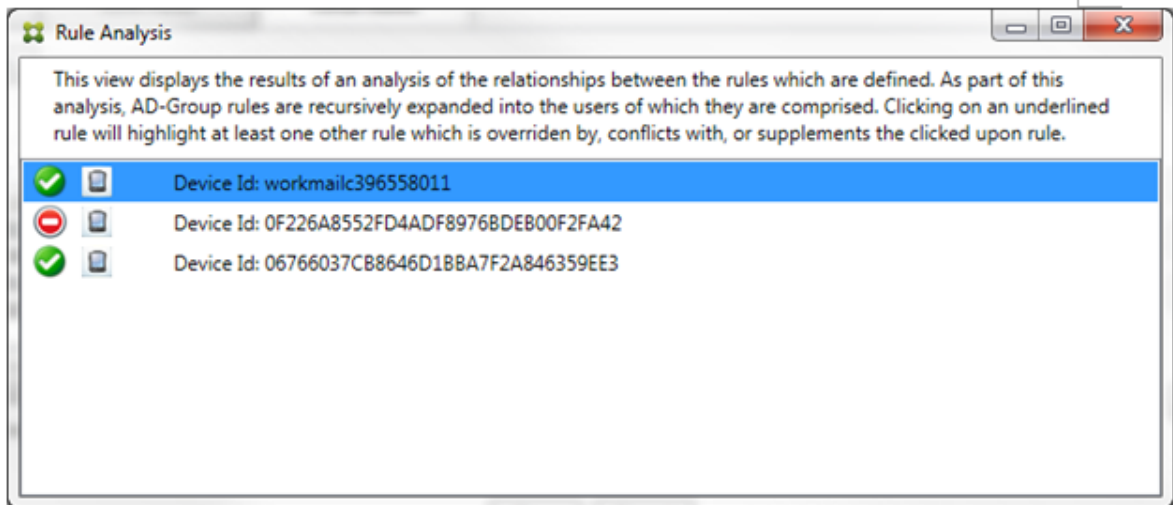
- 재정의규칙: 재정의는둘이상의규칙이동일한장치에적용될수있는경우발생합니다. 규칙은목록의우선순위에따라평가되므로적용될수있는마지막의규칙인스턴스가평가되지않을수있습니다.
- 충돌규칙: 충돌은둘이상의규칙이동일한장치에적용될수있지만액세스 (허용/차단) 가일치하지않는경우발생합니다. 충돌규칙이정규식규칙이아닌경우충돌은항상암시적으로재정의의의미합니다.
- 보완규칙: 보완은둘이상의규칙이정규식규칙이어서둘이상의정규식을하나의정규식규칙으로결합할수있는지, 또는중복되는기능이아닌지를확인해야할때발생합니다. 보완규칙은액세스 (허용/차단) 에서도충돌할수있습니다.
- 주규칙: 주규칙은대화상자안에서클릭된규칙입니다. 이규칙은실선테두리로표시됩니다. 또한위또는아래를가리키는녹색화살표가하나또는두개포함됩니다. 화살표가위를가리키는경우주규칙앞에보조규칙이있음을나타냅니다. 화살표가아래를가리키는경우주규칙뒤에보조규칙이있음을나타냅니다. 한번에하나의주규칙만활성화될수있습니다.

- 보조규칙: 보조규칙은재정의, 충돌또는추가관계를통해주규칙과관련됩니다. 이규칙은파선택두리로표시됩니다. 각주규칙에대해여러개의보조규칙이있을수있습니다. 밑줄이표시된항목을클릭하면항상주규칙의관점에서보조규칙인규칙이강조표시됩니다. 예를들어보조규칙은주규칙으로재정의되고주규칙과액세스에서충돌하며주규칙을보완합니다.

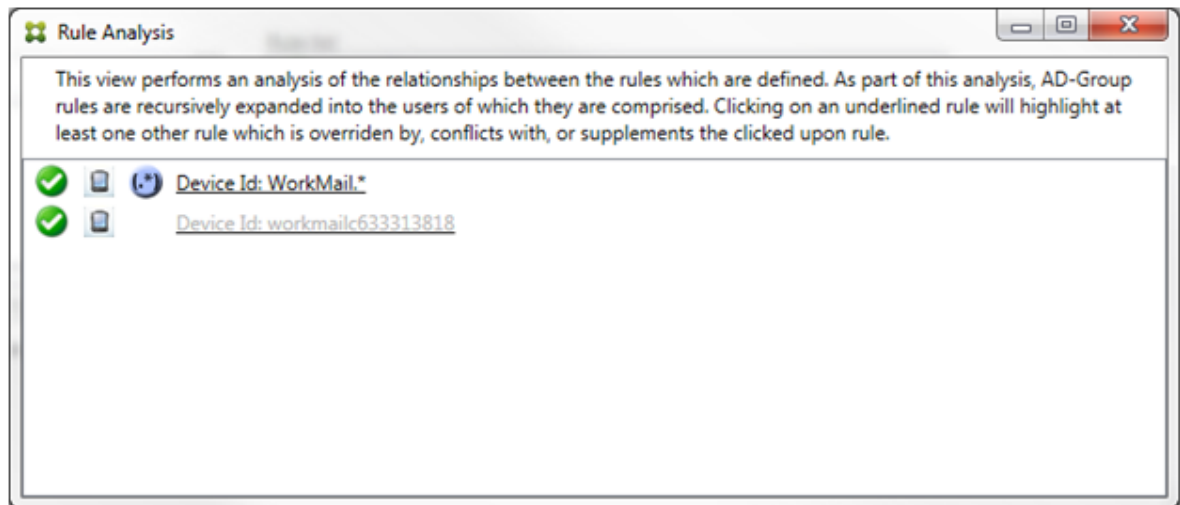
Rule Analysis(규칙분석) 대화상자에규칙유형이표시되는방법

충돌, 재정의또는보완이없는경우 Rule Analysis(규칙분석) 대화상자에밑줄이그어진항목이표시되지않습니다. 항목을클릭해도아무런영향이없습니다. 예를들어선택된항목이일반적으로모습으로표시됩니다.

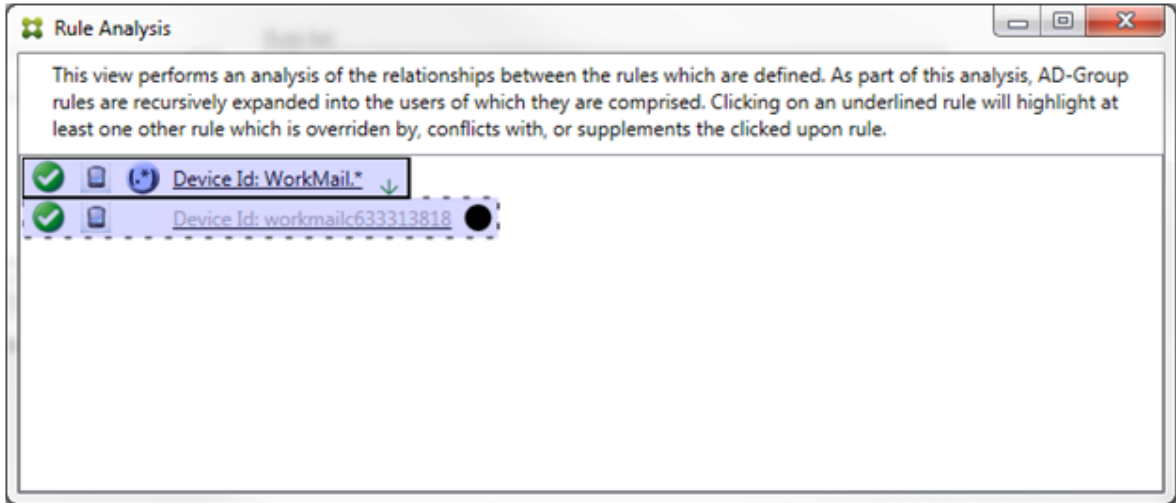
Rule Analysis(규칙분석) 창에는선택할경우충돌, 재정의, 중복또는보완규칙만표시되는확인란이있습니다.



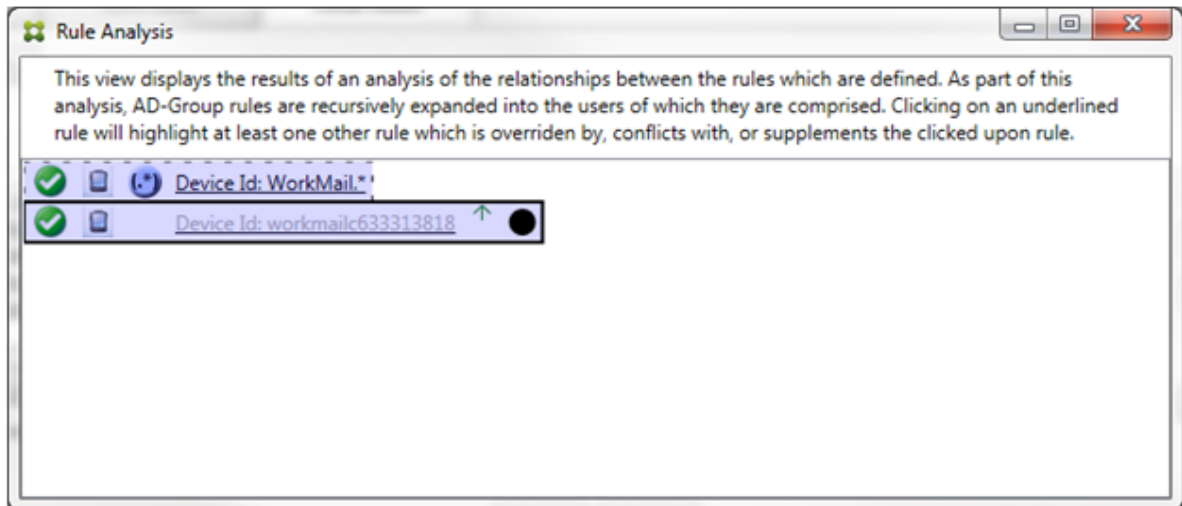
재정의가발생하는경우 2 개이상의규칙 (주규칙과보조규칙) 에밑줄이표시됩니다. 우선순위가더높은규칙으로재정의된하나이상의보조규칙은연한글꼴로표시됩니다. 재정의된규칙을클릭하면해당규칙을재정의한규칙을볼수있습니다. 규칙이주규칙이되거나보조규칙이되어재정의된규칙이강조표시되면그옆에해당규칙이비활성상태임을나타내는검정색원이표시됩니다. 예를들어규칙을클릭하기전에대화상자는다음과같이표시됩니다.



우선순위가가장높은규칙을클릭하면대화상자가다음과같이표시됩니다.

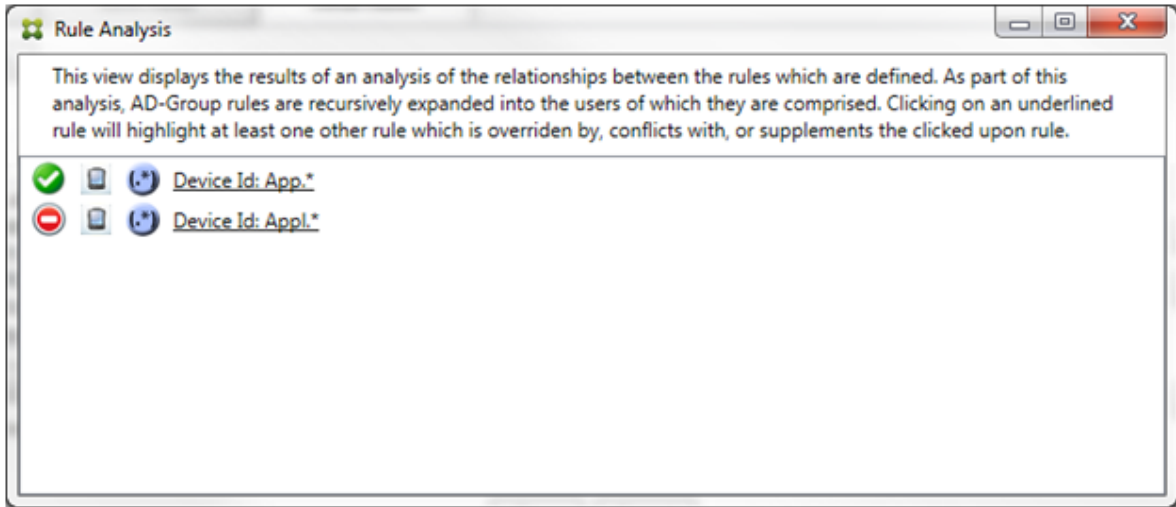


이예에서정규식규칙 `WorkMail.*`는주규칙 (실선테두리로표시됨) 이고일반규칙 `workmailc633313818`은보조규칙 (파선테두리로표시됨) 입니다. 보조규칙옆의검정색점은이규칙보다우선하는더높은우선순위의정규식규칙이있어해당규칙이비활성화 (따라서평가되지않음) 되었음을나타내는시각적표시입니다. 재정의된규칙을클릭한후대화상자는다음과같이표시됩니다.

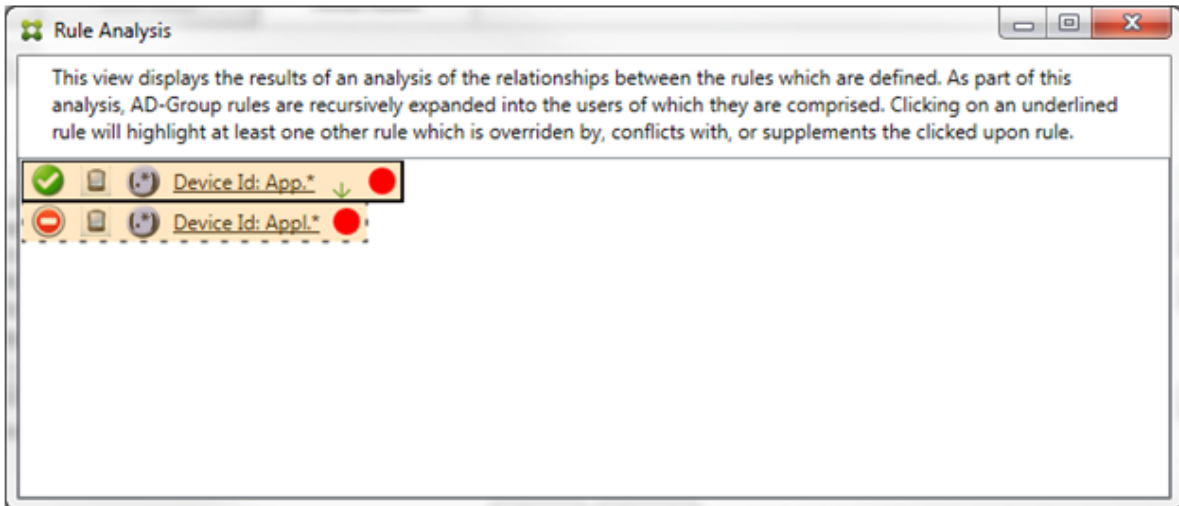


이전예에서정규식규칙 `WorkMail.*`는보조규칙 (파선테두리로표시됨) 이고일반규칙 `workmailc633313818`은주규칙 (실선테두리로표시됨) 입니다. 이단순예제에서는큰차이가없습니다. 더복잡한예제는이항목의뒷부분에나오는복합식예제를참조하십시오. 여러개의규칙이정의된시나리오에서재정의된규칙을클릭하면해당규칙을재정의한규칙을빠르게식별할수있습니다.

충돌이발생하는경우 2 개이상의규칙 (주규칙과보조규칙) 에밀줄이표시됩니다. 충돌하는규칙은빨간색점으로표시됩니다. 서로 충돌하는규칙은둘이상의정규식이정의된경우에만가능합니다. 다른모든충돌시나리오에서는충돌이발생하지않으며재정의의만발생합니다. 단순예제에서규칙중하나를클릭하기전의대화상자는다음과같이표시됩니다.

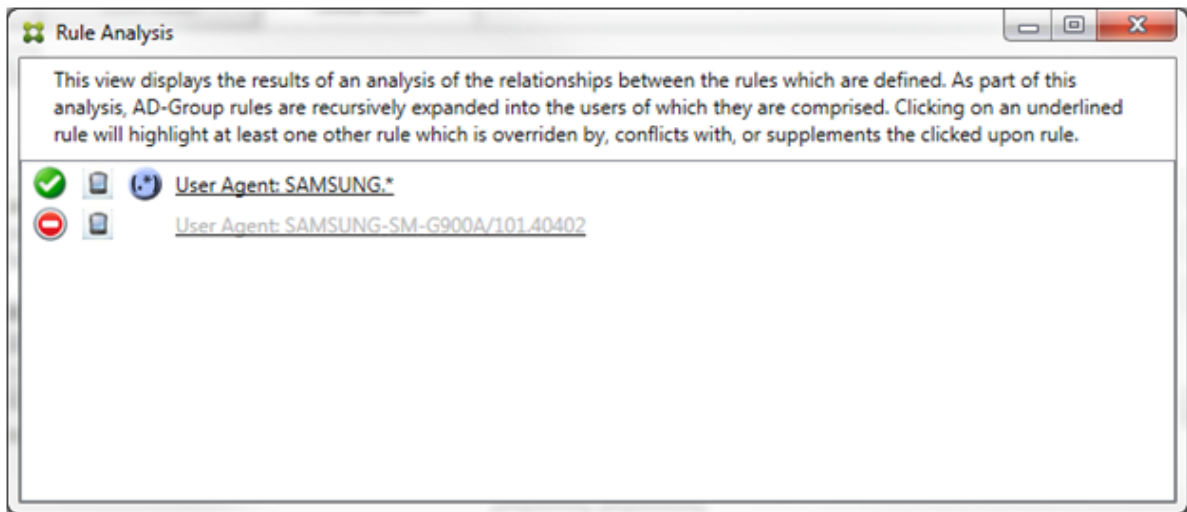


두정규식규칙을검사하면첫번째규칙은장치 ID 에 “App” 이포함된모든장치를허용하고, 두번째규칙은장치 ID 에 “Appl” 이포함된모든장치를거부하는것을알수있습니다. 또한두번째규칙이장치 ID 에 “Appl” 이포함된모든장치를거부하지만허용규칙의우선순위가더높기때문에두번째규칙의조건과일치하는장치가거부되지않습니다. 첫번째규칙을클릭한후대화상자는다음과같이표시됩니다.



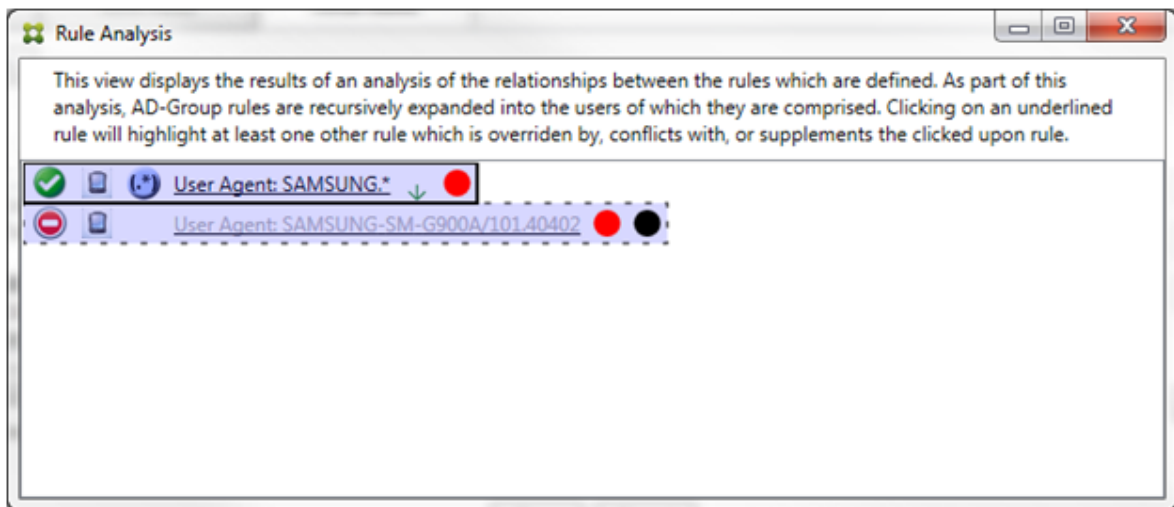
앞의시나리오에서는주규칙 (정규식규칙 App . *) 과보조규칙 (정규식규칙 Appl . *) 이모두노란색으로강조표시됩니다. 이는 둘이상의정규식규칙이단일의일치가가능한필드에적용되어중복성문제또는보다심각한문제가발생할수있음을알리는시각적경고입니다.

충돌과재정의가모두발생하는시나리오에서는주규칙 (정규식규칙 App . *) 과보조규칙 (정규식규칙 Appl . *) 이노란색으로강조표시됩니다. 이는 둘이상의정규식규칙이단일의일치가가능한필드에적용되어중복성문제또는보다심각한문제가발생할수있음을알리는시각적경고입니다.



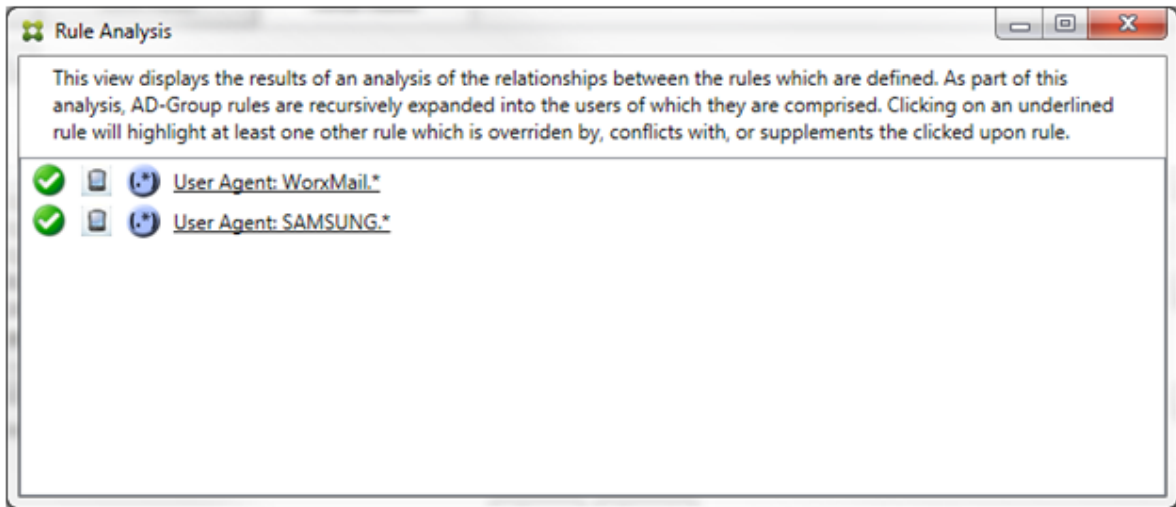
앞의예제에서첫번째규칙 (정규식규칙 SAMSUNG . *) 은다음규칙 (일반규칙 SAMSUNG-SM-G900A/101.40402) 을재정의할뿐아니라엑세스 (주규칙은허용을지정하고보조규칙은차단을지정함) 에서도다르다는것을알수있습니다. 두번째규칙 (일반규칙 SAMSUNG-SM-G900A/101.40402) 은재정의되고비활성화되었음을나타내는색이연한텍스트로표시됩니다.

정규식규칙을클릭한후대화상자는다음과같이표시됩니다.

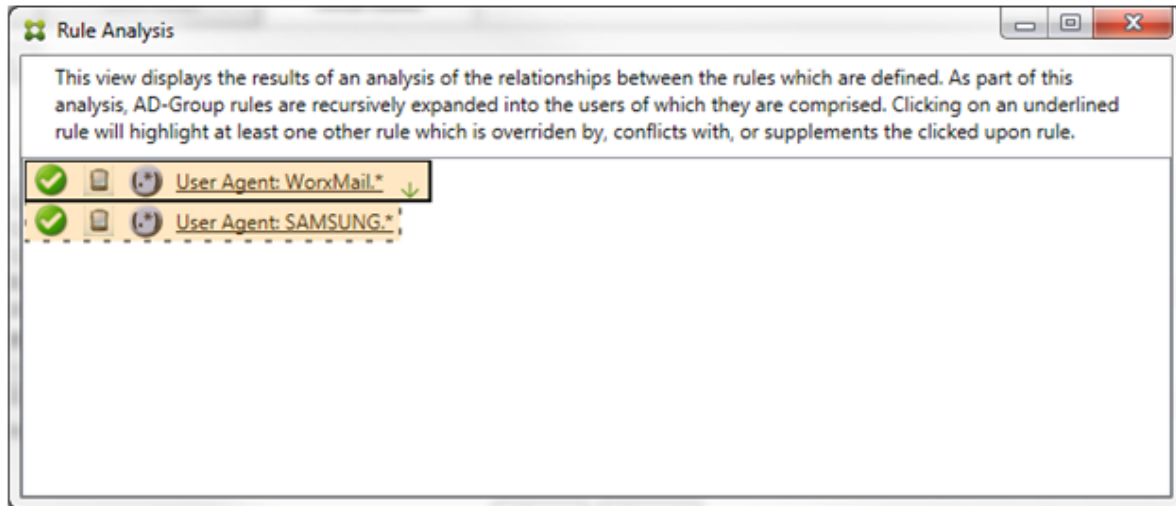


주규칙 (정규식규칙 SAMSUNG . *) 뒤에엑세스상태가하나이상의보조규칙과충돌함을나타내는빨간색점이표시됩니다. 보조규칙 (일반규칙 SAMSUNG-SM-G900A/101.40402) 뒤에엑세스상태가주규칙과충돌함을나타내는빨간색점이표시됩니다. 이규칙뒤에는규칙이재정의되었고그로인해비활성화되었음을나타내는검정색점도표시됩니다.

2 개이상의규칙 (주규칙과보조규칙) 에밀줄이표시됩니다. 다른규칙을보완하는규칙에는정규식규칙만포함됩니다. 다른규칙을보완하는규칙은노란색오버레이로표시됩니다. 단순예제에서규칙중하나를클릭하기전의대화상자는다음과같이표시됩니다.



Exchange ActiveSync 용 Endpoint Management 커넥터의 ActiveSync 장치 ID 필드에정규식규칙인두규칙이모두 적용된것을쉽게알수있습니다. 첫번째규칙을클릭한후대화상자는다음과같이표시됩니다.



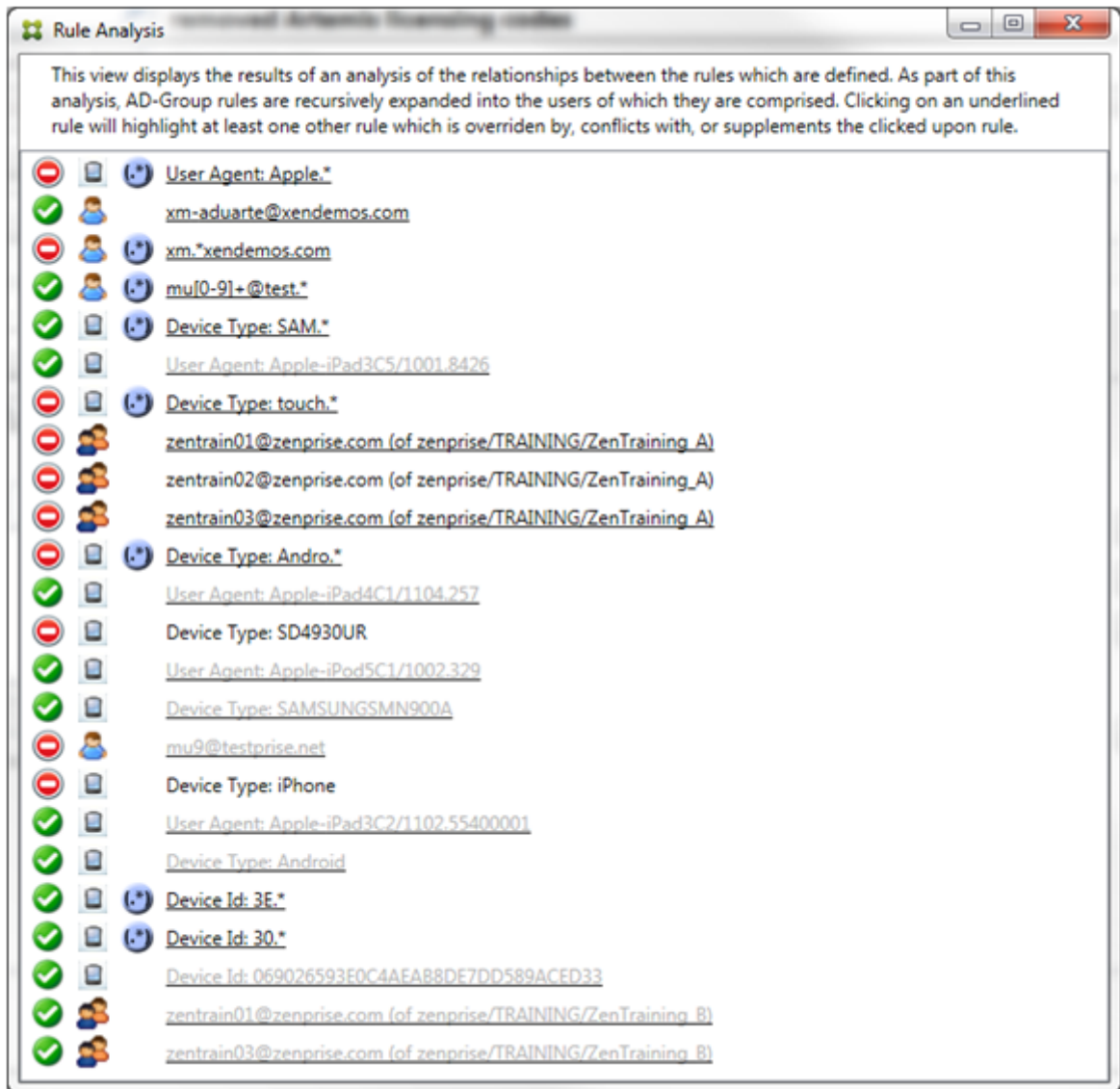
주규칙 (정규식규칙 `WorkMail.*`) 이하하나이상의추가보조규칙 (정규식규칙) 이있음을나타내는노란색오버레이로강조표시됩니다. 보조규칙 (정규식규칙 `SAMSUNG.*`) 이 Exchange ActiveSync 용 Endpoint Management 커넥터의동일한필드 (ActiveSync 장치 ID 필드) 에이규칙과주규칙 (모두정규식규칙임) 이적용되고있음을나타내는노란색오버레이로강조표시됩니다. 이경우필드는 ActiveSync 장치 ID 입니다. 정규식은겹치거나겹치지않을수있습니다. 정규식이적절하게작성되었는지여부는직접판단해야합니다.

복합식의예제

재정의, 충돌또는보완이발생할수있는상황은많습니다. 따라서가능한모든시나리오의예를제공하기란불가능합니다. 다음예제에서는하지말아야할사항을설명하고규칙분석의시각적구조가제공하는모든기능을설명합니다. 다음그림에는항목의대부분에밑줄이표시되어있습니다. 문제의규칙이우선순위가더높은규칙으로재정의되었음을나타내는연한글꼴로렌더링된항목이많습니다.



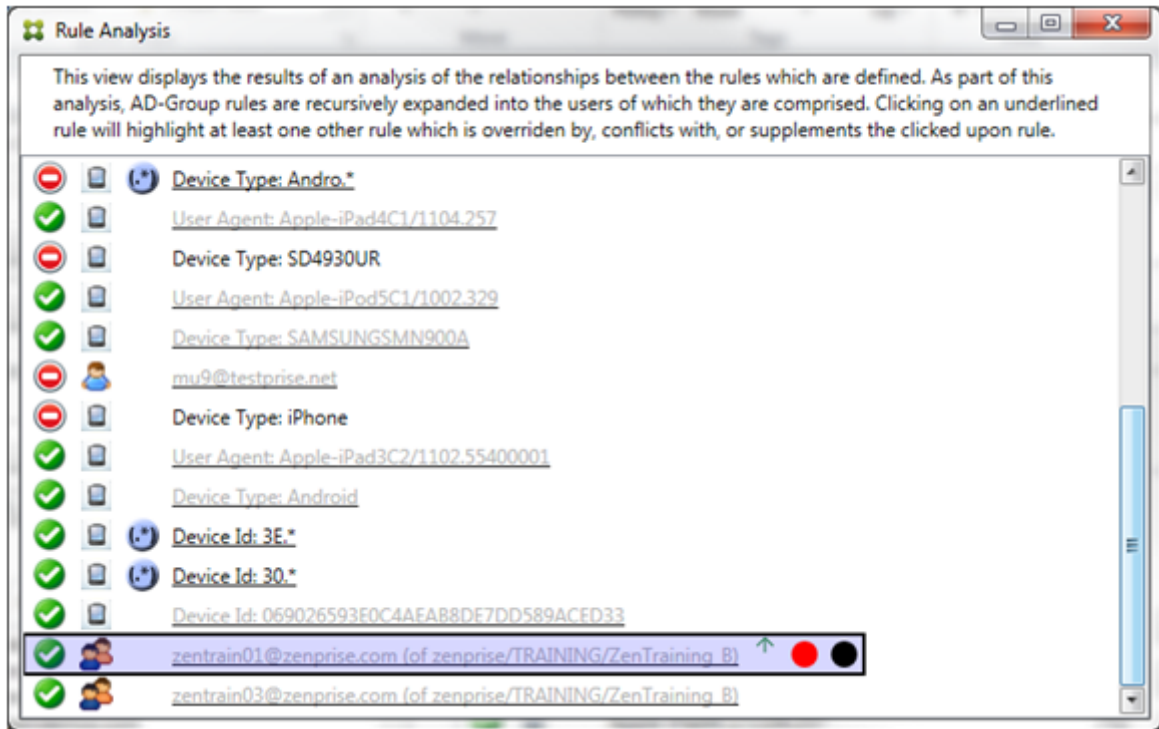
아이콘으로 표시되는 정규식 규칙의 수도 목록에 포함되어 있습니다.



재정의 분석하는 방법

특정 규칙을 재정의한 규칙을 보려면 규칙을 클릭합니다.

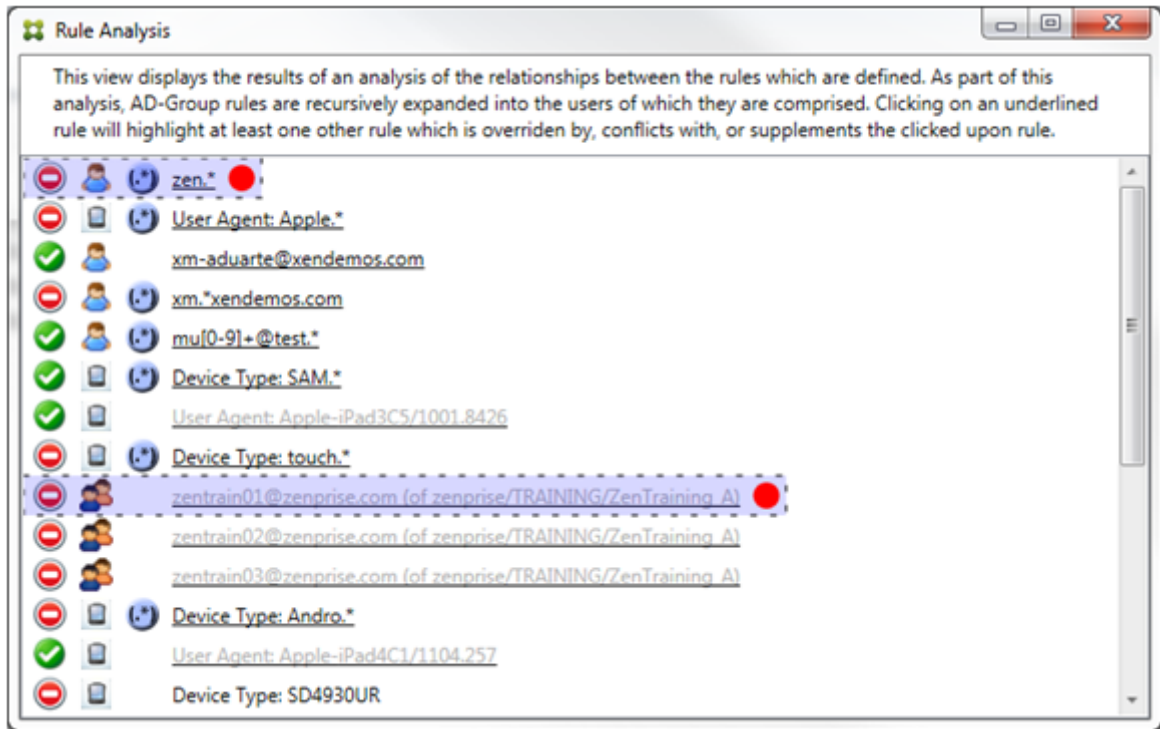
예제 1: 이 예제에서는 `zentrain01@zenprise.com`이 재정의된 이유를 검사합니다.



주규칙 (AD 그룹규칙 zenprise/TRAINING/ZenTraining B, 여기서 zentrain01@zenprise.com은 구성원임) 의특징은다음과같습니다.

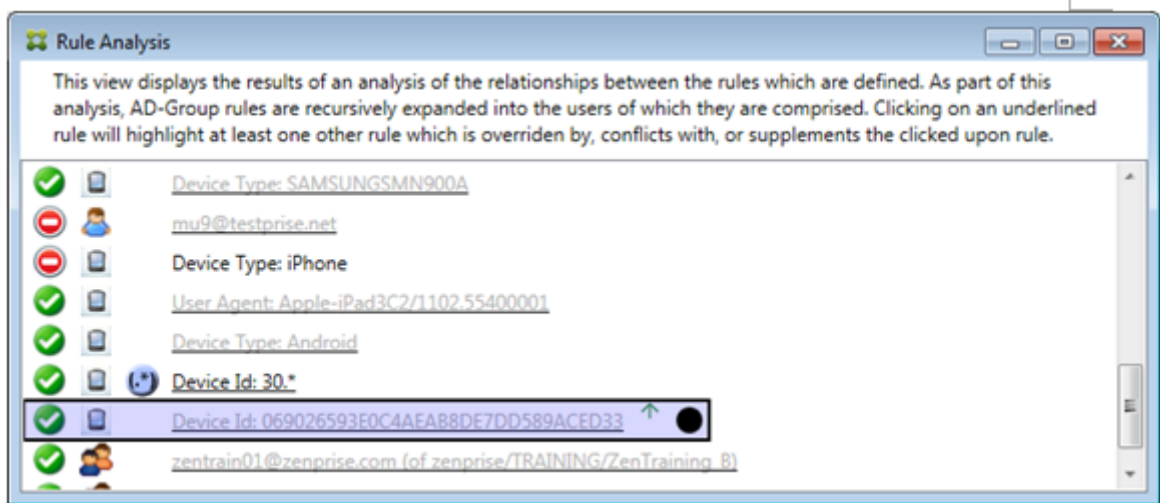
- 파란색으로강조표시되고실선테두리가포함되어있습니다.
- 위쪽을가리키는녹색화살표가있습니다 (위에보조규칙이있음을나타냄).
- 각각하나이상의보조규칙과액세스상태가충돌하고, 주규칙으로재정의되어비활성화되었음을나타내는빨간색원과검정색원이뒤에있습니다.

위로스크롤하면다음이표시됩니다.



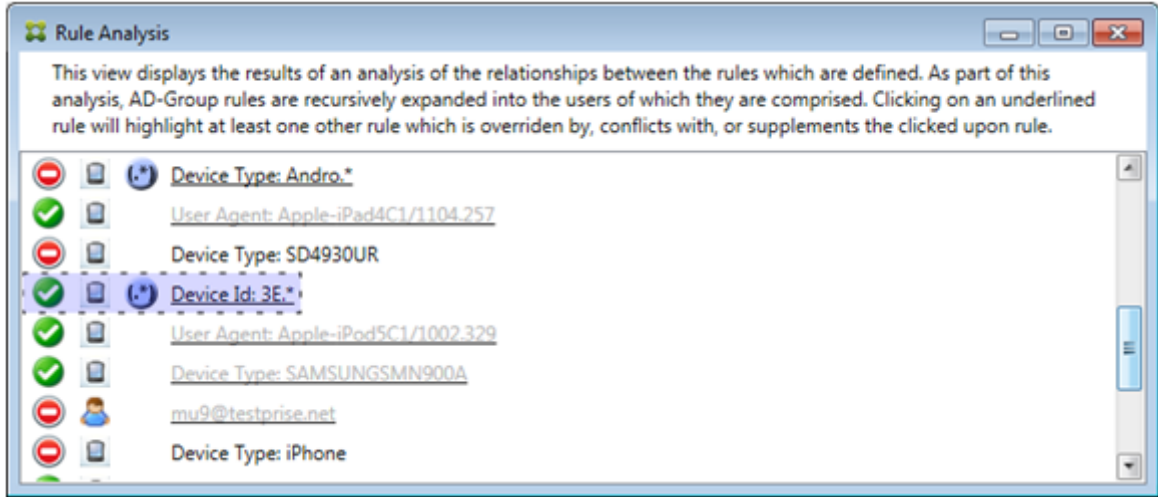
이 예에서는 정규식 규칙인 zen.*과 일반 규칙인 zentrain01@zenprise.com(zenprise/TRAINING/ZenTraining A) 의 보조 규칙 2 개가 주 규칙을 재정의합니다. 두 번째 보조 규칙에서는 Active Directory 그룹 규칙 ZenTraining A에 사용자 zentrain01@zenprise.com이 포함되고 Active Directory 그룹 규칙 ZenTraining B에도 사용자 zentrain01@zenprise.com이 포함됩니다. 그러나 보조 규칙이 주 규칙보다 우선 순위가 높기 때문에 주 규칙이 재정의되었습니다. 주 규칙의 액세스는 허용이고 두 보조 규칙의 액세스는 차단이므로 액세스가 충돌함을 나타내는 빨간색 원이 뒤에 표시됩니다.

예제 2: 이 예제에서는 ActiveSync 장치 ID 가 069026593E0C4AEAB8DE7DD589ACED33인 장치가 재정의된 이유를 보여줍니다.



주 규칙 (일반장치 ID 규칙 069026593E0C4AEAB8DE7DD589ACED33) 의 특징은 다음과 같습니다.

- 파란색으로 강조 표시되고 실선 테두리가 포함되어 있습니다.
- 위쪽을 가리키는 녹색 화살표가 있습니다 (위에 보조 규칙이 있음을 나타냄).
- 주 규칙이 보조 규칙으로 재정의되어 비활성화되었음을 나타내는 검정색 원이 뒤에 표시되어 있습니다.

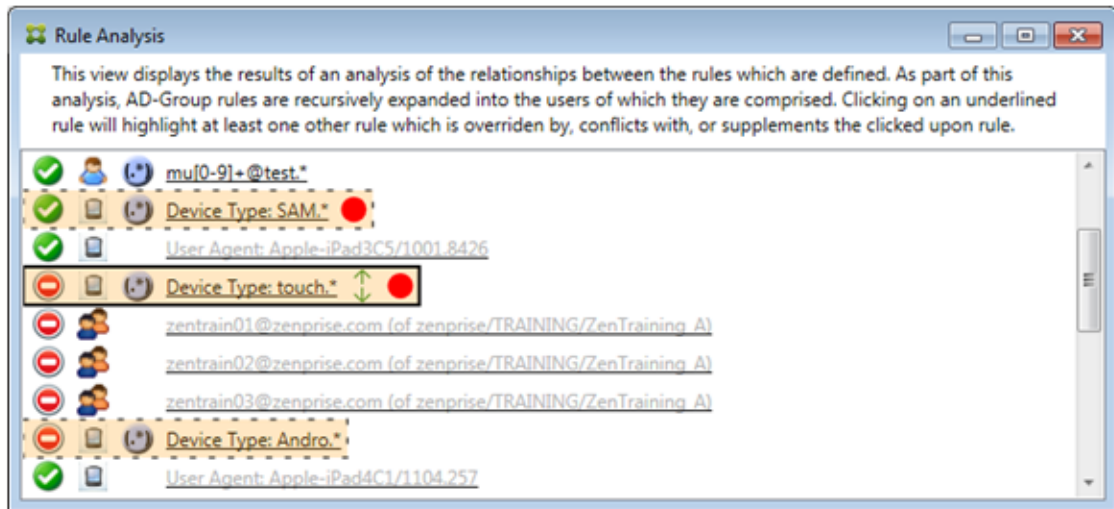


이 예에서는 단일의 보조 규칙이 주 규칙을 재정의합니다. 정규식 ActiveSync 장치 ID 규칙은 3E.*입니다. 정규식 3E.*가 069026593E0C4AEAB8DE7DD589ACED33과 일치하므로 주 규칙이 평가되지 않습니다.

보안 및 충돌을 분석하는 방법

이 예에서 기본 규칙은 정규식 ActiveSync 장치 유형 규칙인 touch.*입니다. 특징은 다음과 같습니다.

- 특정 규칙 필드 (이 예에서는 ActiveSync 장치 유형) 예외 이상의 정규식 규칙이 작동함을 나타내는 경고로 노란색 오버레이가 실선 테두리와 함께 표시되어 있습니다.
- 각각 위쪽과 아래쪽을 가리키는 두 개의 화살표가 있습니다 (우선 순위가 높은 보조 규칙과 우선 순위가 낮은 보조 규칙이 1 개 이상 있음을 나타냄).
- 액세스 상태가 허용으로 설정되어 주 규칙의 액세스 상태 인차단과 충돌하는 보조 규칙이 1 개 이상임을 나타내는 빨간색 원이 옆에 표시되어 있습니다.
- 정규식 ActiveSync 장치 유형 규칙 SAM.* 및 정규식 ActiveSync 장치 유형 규칙 Andro.*의 보조 규칙 2 개가 있습니다.
- 두 보조 규칙은 보조 규칙임을 나타내는 파선 테두리로 표시되어 있습니다.
- 두 보조 규칙에는 ActiveSync 장치 유형 규칙 필드에도 적용됨을 나타내는 노란색 오버레이가 표시되어 있습니다.
- 이러한 시나리오에서는 정규식 규칙이 중복되지 않는지 확인해야 합니다.



규칙을추가로분석하는방법

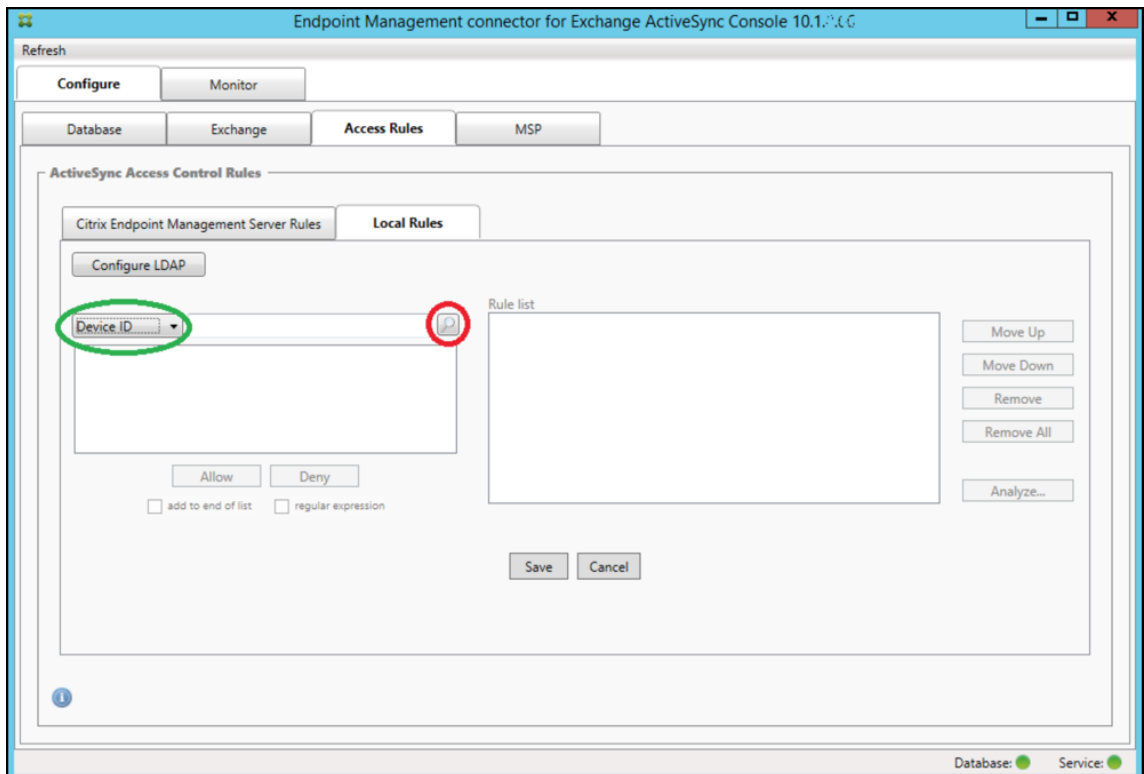
이예제에서는규칙관계가항상주규칙의관점에서파생된다는점을설명합니다. 앞의예제에서는정규식규칙클릭이값이 touch.*인장치유형의필드에적용되는방법을보여줬습니다. 보조규칙 Andro.*를클릭하면다른보조규칙집합이강조표시됩니다.



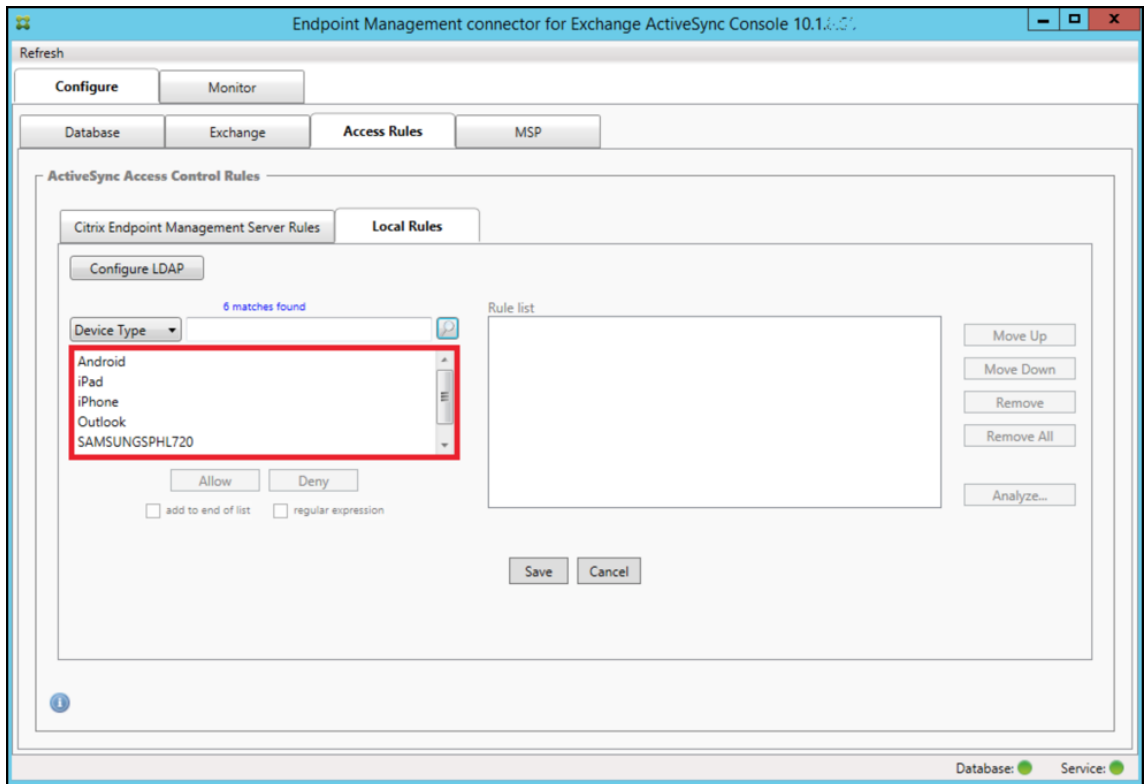
이예제는규칙관계에포함된재정의된규칙을보여줍니다. 이규칙은일반 ActiveSync 장치유형규칙인 **Android**이며재정의 (연 한글필로표시되고검정색원이표시됨) 되었으며주규칙인정규식 ActiveSync 장치유형규칙 **Andro.***와액세스상태가충돌합니다. 이규칙은클릭하기전에보조규칙이었습니다. 앞의예에서일반 ActiveSync 장치유형규칙 **Android**는보조규칙으로표시되지않았습니다. 주규칙 (정규식 ActiveSync 장치유형규칙 **touch.***) 의관점에서주규칙과관련되지않았기때문입니다.

일반식로컬규칙을구성하려면

1. **Access Rules**(액세스규칙) 탭을클릭합니다.



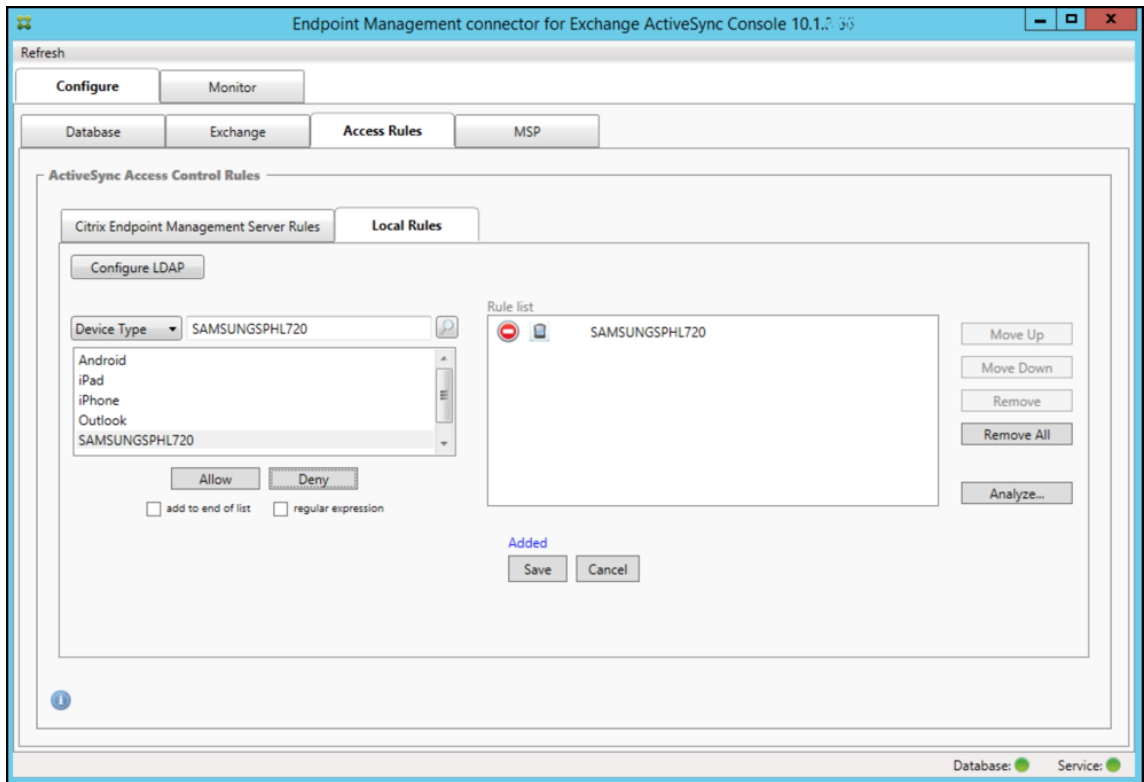
2. **Device ID**(장치 ID) 목록에서로컬규칙을만들필드를선택합니다.
3. 돋보기아이콘을클릭하여선택한필드의모든고유한일치항목을표시합니다. 이예제에서는 **Device Type**(장치유형) 필드가선택되었고목록상자아래에선택항목이표시되어있습니다.



4. 결과목록상자에서항목하나를클릭하고다음옵션중하나를클릭합니다.

- **Allow(허용)** 을클릭하면일치하는모든장치의 ActiveSync 트래픽을허용하도록 Exchange 가구성됩니다.
- **Deny(거부)** 을클릭하면일치하는모든장치의 ActiveSync 트래픽을거부하도록 Exchange 가구성됩니다.

이예에서는장치유형이 SamsungSPHL720 인모든장치의액세스가거부됩니다.



정규식을 추가하려면

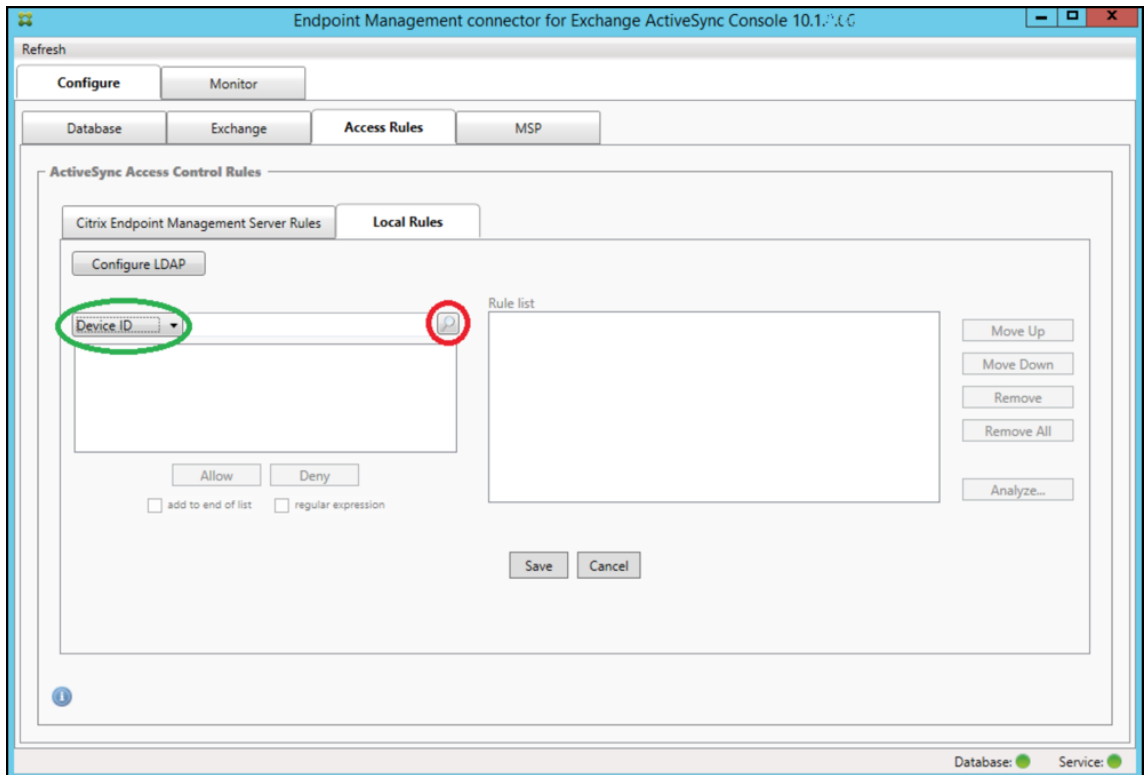


정규식로컬규칙은 옆에 표시되는 아이콘으로 구분할 수 있습니다.

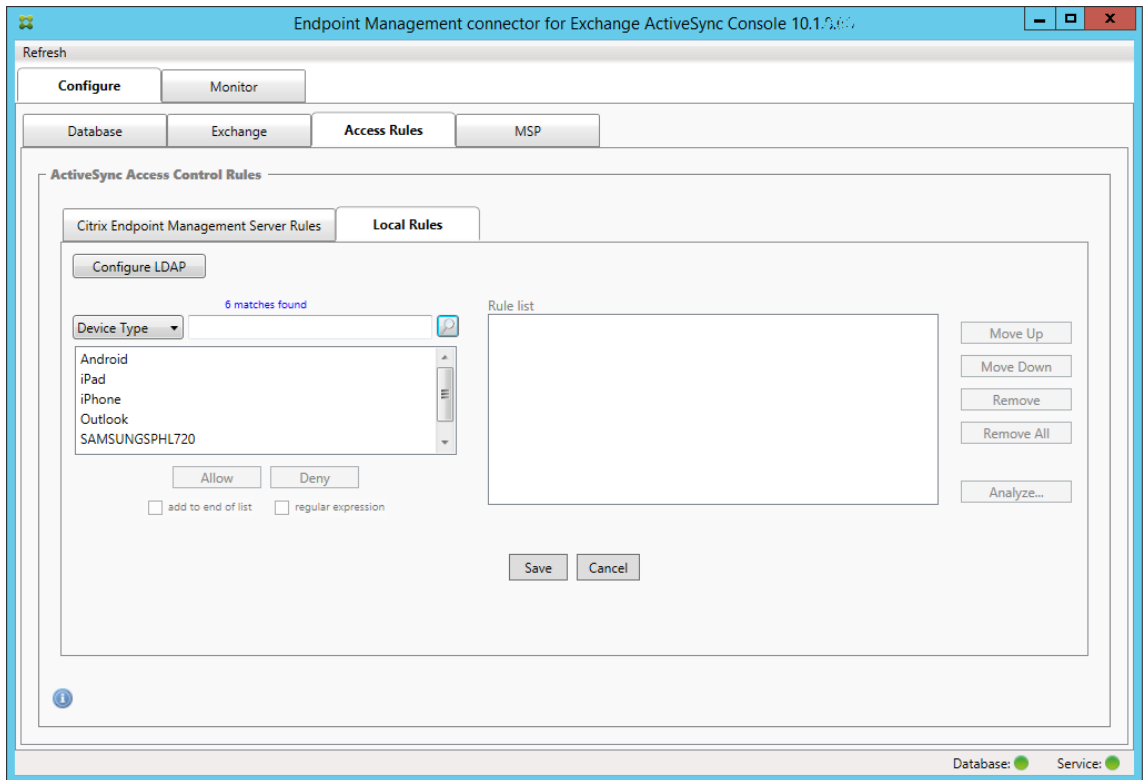
정규식규칙을 추가하려면 지정된 필드에 대한 결과 목록의 기존 값을 사용하여 정규식규칙을 작성하거나 (주스냅샷이 완료되어야 함) 원하는 정규식을 입력하면 됩니다.

기존 필드 값에서 정규식을 작성하려면

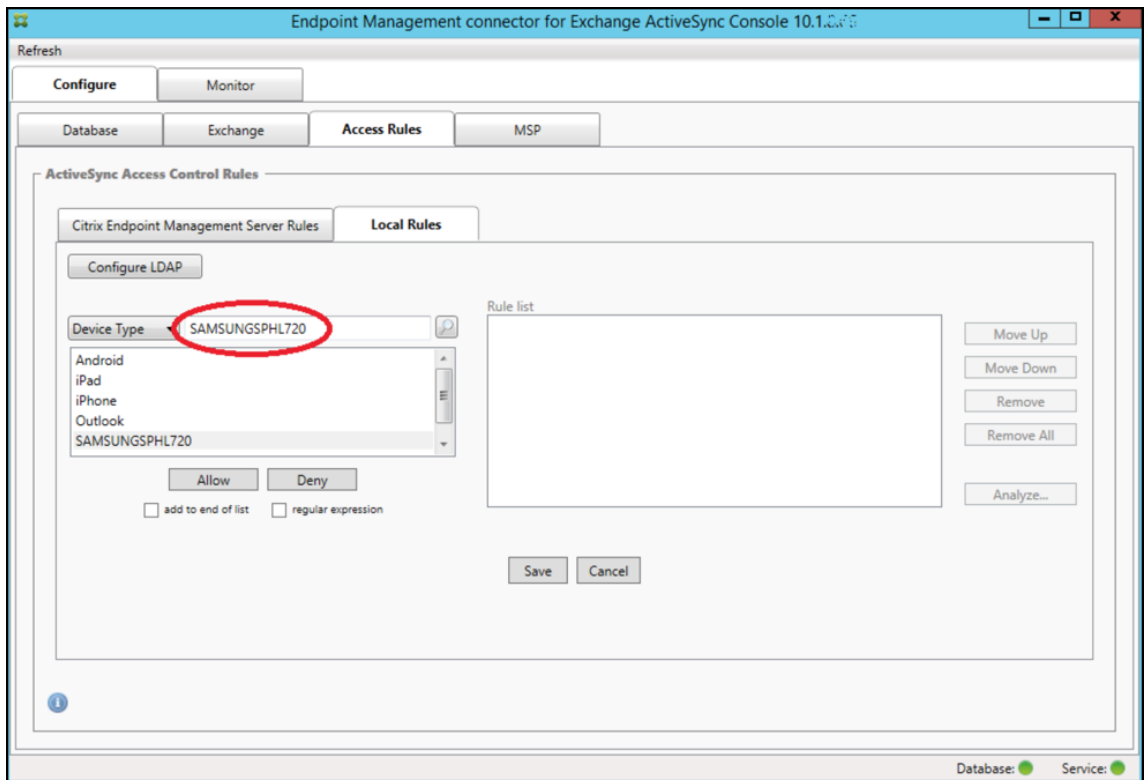
1. **Access Rules**(액세스규칙) 탭을 클릭합니다.



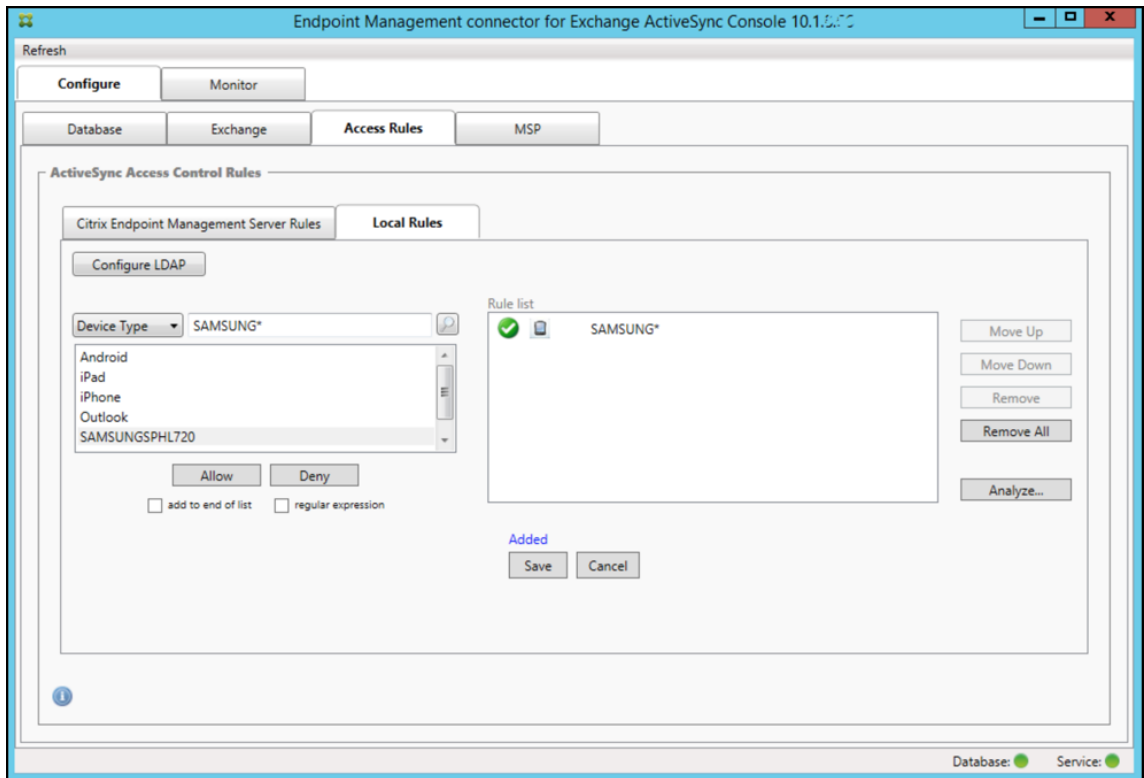
2. **Device ID(장치 ID)** 목록에서정규식로컬규칙을만들필드를선택합니다.
3. 돋보기아이콘을클릭하여선택한필드의모든고유한일치항목을표시합니다. 이예제에서는 **Device Type(장치유형)** 필드가선택되었고목록상자아래에선택항목이표시되어있습니다.



4. 결과목록에서항목중하나를클릭합니다. 이예제에서는 **SAMSUNGSPHL720** 이선택되었고 **Device Type**(장치유형) 옆의텍스트상자에표시되어있습니다.

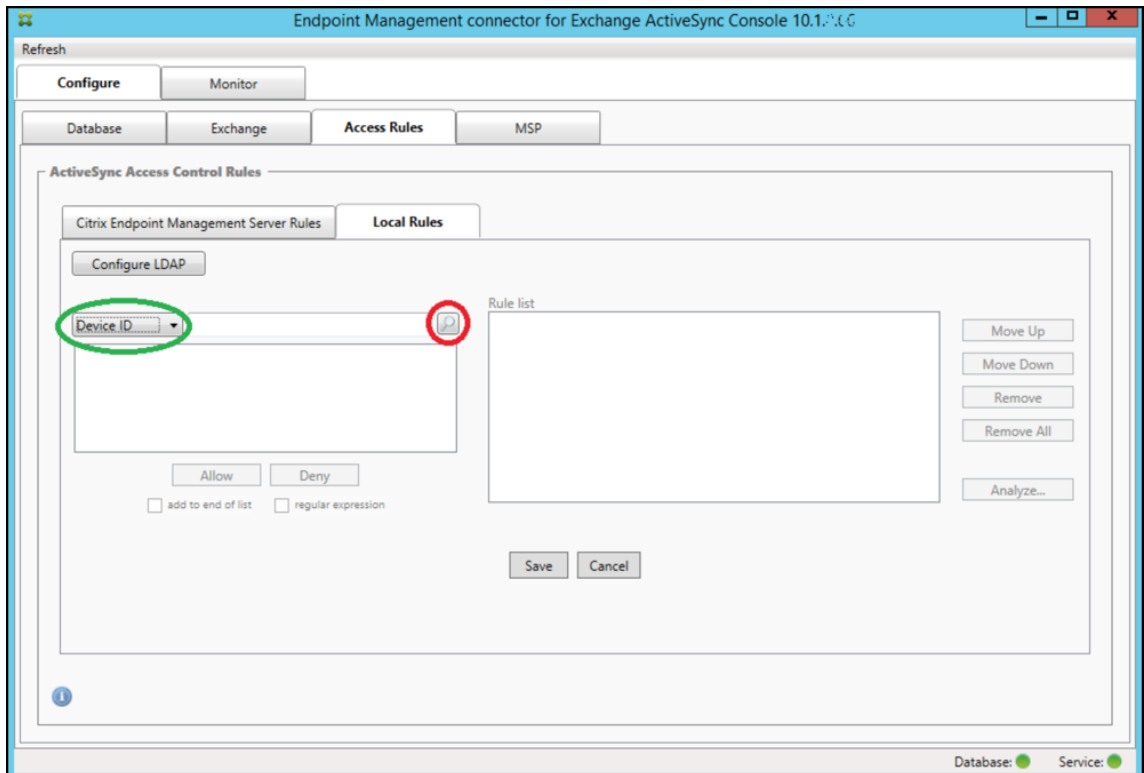


5. 장치유형값에 “Samsung” 이포함되는모든장치유형을허용하려면다음단계에따라정규식규칙을추가합니다.
 - a) 선택한항목텍스트상자안쪽을클릭합니다.
 - b) 텍스트를 **SAMUNGSPHL720** 에서다음으로변경합니다. **SAMSUNG.***.
 - c) regular expression(정규식) 확인란이선택되어있는지확인합니다.
 - d) **Allow(허용)** 를클릭합니다.

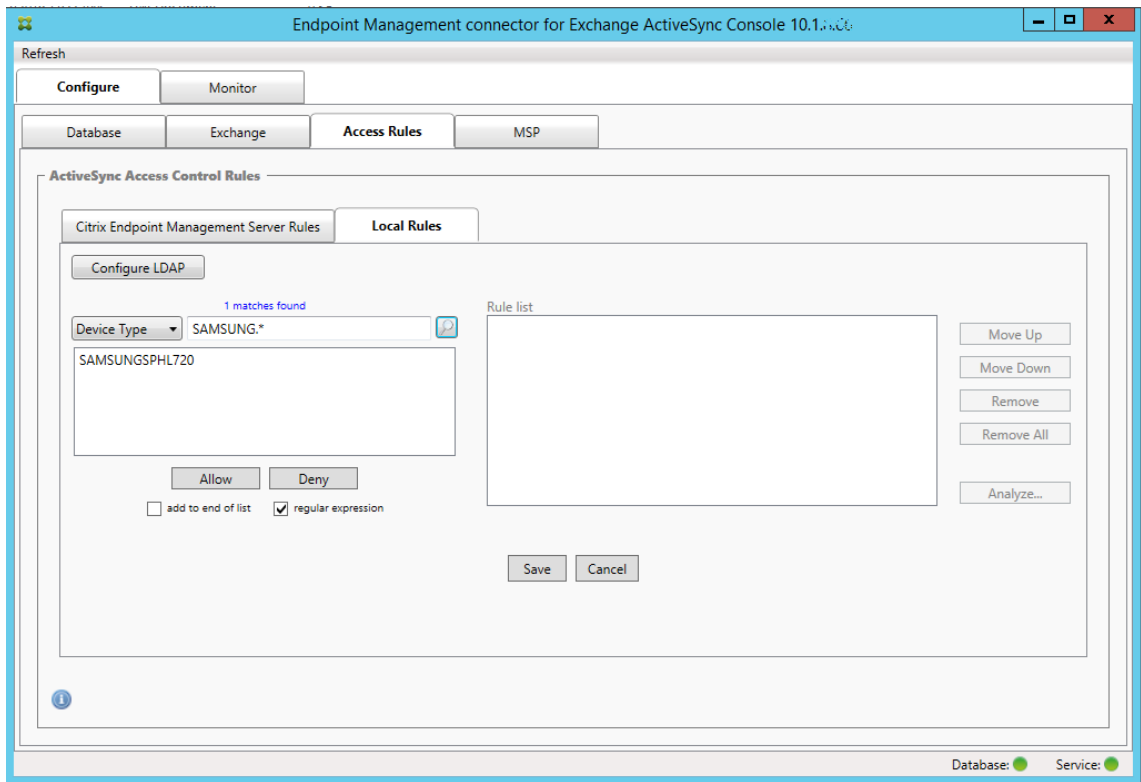


액세스규칙을작성하려면

1. **Local Rules(로컬규칙)** 탭을클릭합니다.
2. 정규식을입력하려면 Device ID(장치 ID) 목록과선택한항목텍스트상자를모두사용해야합니다.



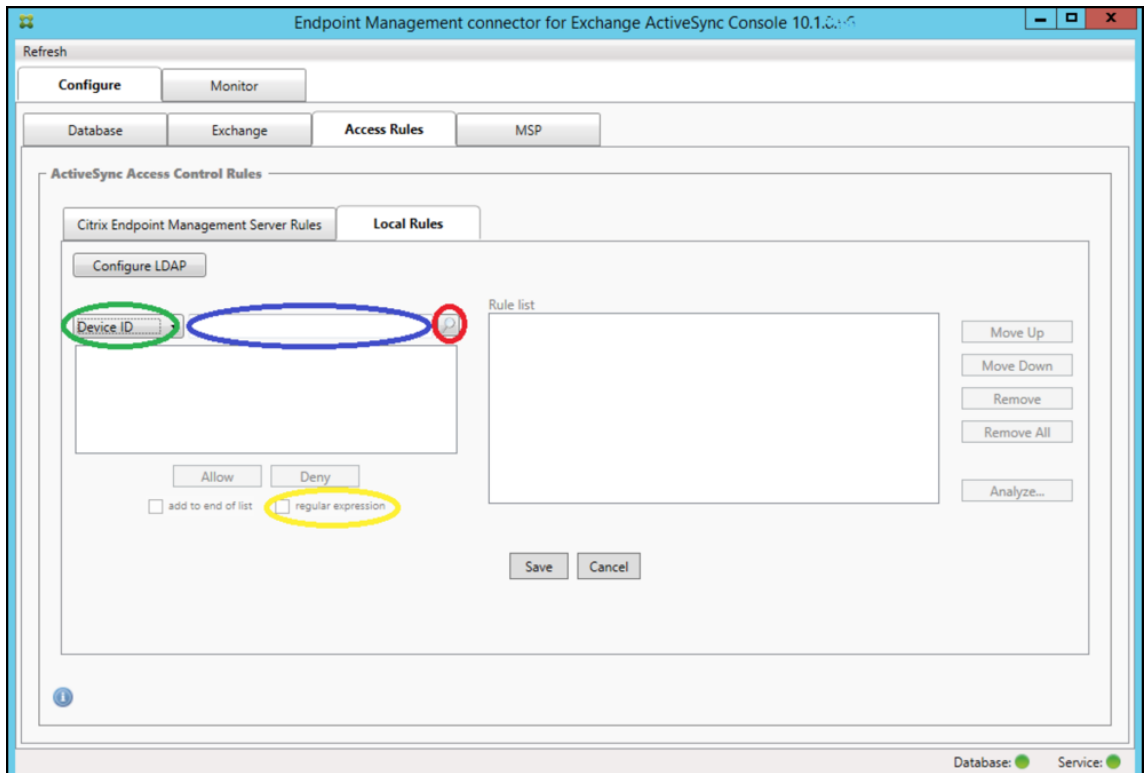
3. 일치기준으로 사용할 필드를 선택합니다. 이 예제에서는 Device Type(장치유형) 을 사용합니다.
4. 정규식을 입력합니다. 이 예에서는 다음을 사용합니다. `samsung.*`
5. regular expression(정규식) 확인란이 선택되었는지 확인한 후 **Allow**(허용) 또는 **Deny**(거부) 를 클릭합니다. 이 예에서는 **Allow**(허용) 를 선택합니다. 최종 결과는 다음과 같습니다.



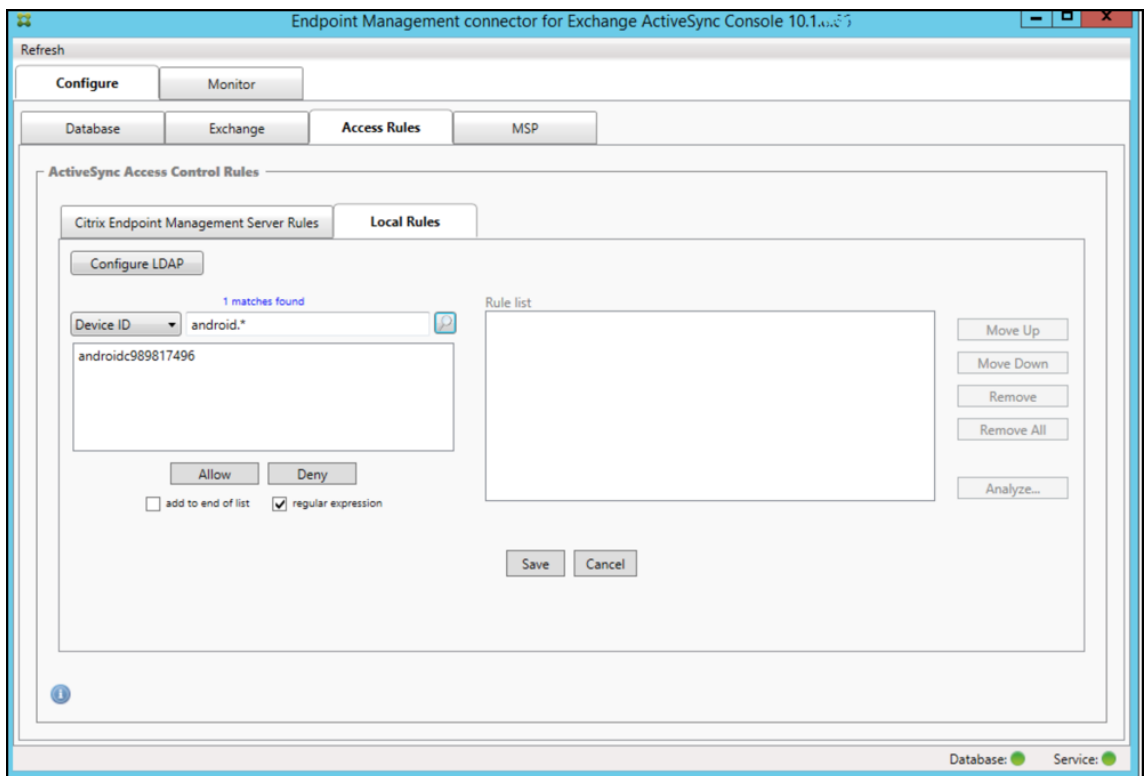
장치를 찾으려면

정규식확인란을선택하면지정된식과일치하는특정장치에대한검색을실행할수있습니다. 이기능은주소넵샷을성공적으로완료한경우에만사용할수있습니다. 정규식규칙을사용할계획이없는경우에도이기능을사용할수있습니다. 예를들어 ActiveSync 장치 ID에 “workmail” 텍스트가포함된모든장치를찾을수있습니다. 이렇게하려면다음절차를따르십시오.

1. **Access Rules(엑세스규칙)** 탭을클릭합니다.
2. 장치일치필드선택기가 Device ID(장치 ID)(기본값) 로설정되었는지확인합니다.



3. 선택한항목텍스트상자 (이전그림에서파란색으로표시됨) 안쪽을클릭한후 **workmail.***를입력합니다.
4. regular expression(정규식) 확인란이선택되었는지확인한후돋보기아이콘을클릭하여다음그림에표시된것과같이일치하는항목을표시합니다.

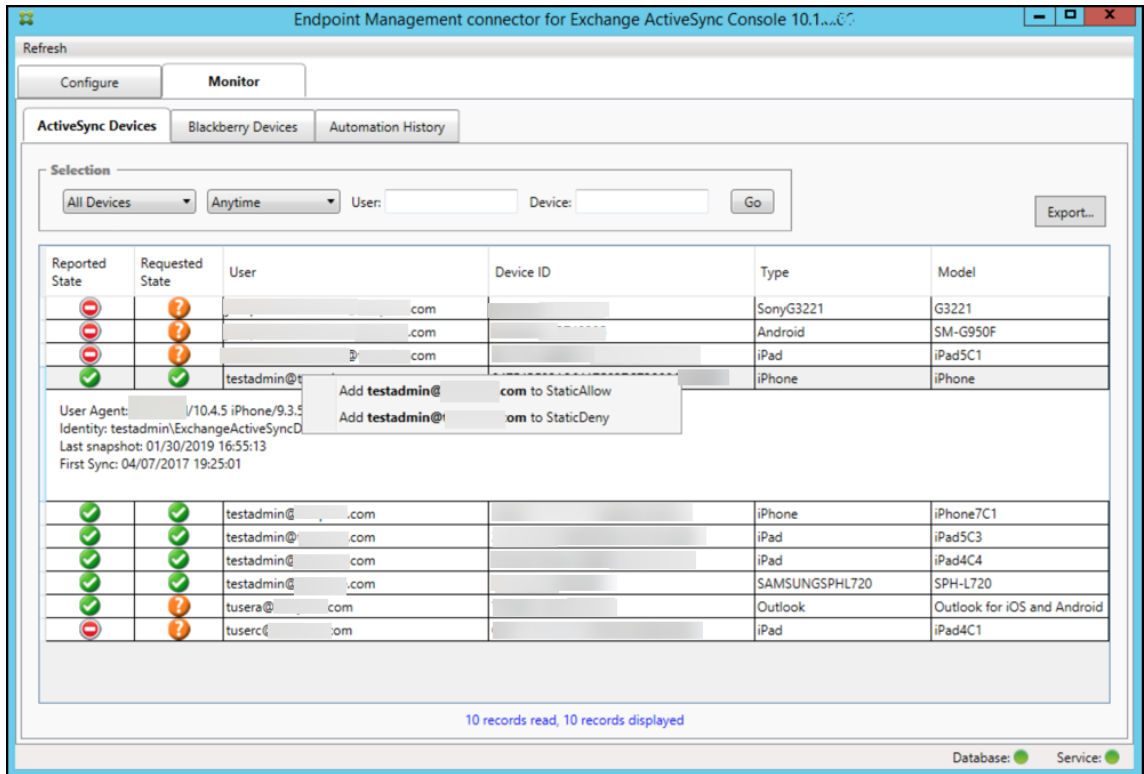


개별사용자, 장치또는장치유형을정적규칙에추가하려면

ActiveSync Devices(ActiveSync 장치) 탭에서사용자, 장치 ID 또는장치유형에기반한정책규칙을추가할수있습니다.

1. **ActiveSync Devices(ActiveSync 장치)** 탭을클릭합니다.
2. 목록에서사용자, 장치또는장치유형을마우스오른쪽단추로클릭하고선택항목을허용또는거부할지여부를선택합니다.

다음이미지는 user1 을선택한경우의 Allow/Deny(허용/거부) 옵션을보여줍니다.



장치모니터링

Exchange ActiveSync 용 Endpoint Management 커넥터의 **Monitor(모니터)** 탭을 사용하면 검색된 Exchange ActiveSync 및 BlackBerry 장치와자동화된 PowerShell 명령의실행기록을탐색할수있습니다. **Monitor(모니터)** 탭에는 다음과같은세개의탭이있습니다.

- **ActiveSync Devices(ActiveSync 장치):**
 - **Export(내보내기)** 단추를클릭하여표시된 ActiveSync 장치파트너관계를내보낼수있습니다.
 - **User(사용자), Device ID(장치 ID)** 또는 **Type(유형)** 열을마우스오른쪽단추로클릭하고적절한허용또는차단 규칙유형을선택하여로컬 (정적) 규칙을추가할수있습니다.
 - 확장된행을축소하려면 Ctrl 키를누른채로확장된행을클릭합니다.
- **Blackberry Devices(Blackberry 장치)**
- **Automation History(자동화기록)**

Configure(구성) 탭에는 모든 스냅샷 기록이 표시됩니다. 스냅샷 기록은 스냅샷 생성 시점, 스냅샷 지속 기간, 검색된 장치 수 및 발생한 모든 오류를 보여줍니다.

- **Exchange** 탭에서 원하는 Exchange Server 의 정보 아이콘을 클릭합니다.
- **MSP** 탭에서 원하는 BlackBerry Server 의 정보 아이콘을 클릭합니다.

문제 해결 및 진단

Exchange ActiveSync 용 Endpoint Management 커넥터는 오류 및 기타 작업 정보를 해당 로그 파일 (설치 폴더\log\XmmWindowsService.log) 에 기록합니다. 또한 Exchange ActiveSync 용 Endpoint Management 커넥터는 중요한 이벤트를 Windows 이벤트 로그에 기록합니다.

로그 수준을 변경하려면

Exchange ActiveSync 용 Endpoint Management 커넥터에는 오류, 정보, 경고, 디버그 및 추적 로그 수준이 포함됩니다.

참고:

뒤로 갈수록 더 많은 세부 정보 (더 많은 데이터) 가 생성됩니다. 예를 들어 오류 수준은 가장 적은 세부 정보를 제공하며 추적 수준은 가장 많은 세부 정보를 제공합니다.

로그 수준을 변경하려면 다음을 수행합니다.

1. C:\Program Files\Citrix\Citrix Endpoint Management 커넥터에서 nlog.config 파일을 엽니다.
2. <rules> 섹션에서 *minilevel* 매개변수를 원하는 로그 수준으로 변경합니다. 예를 들면 다음과 같습니다.

```
1 <rules>
2
3 <logger name="*" writeTo="file" minlevel="Debug" />
4
5 </rules>
```

3. 파일을 저장합니다.

변경 사항은 즉시 적용됩니다. Exchange ActiveSync 에 대한 커넥터를 다시 시작할 필요가 없습니다.

일반적인 오류

다음 목록에는 일반적인 오류가 포함되어 있습니다.

- Exchange ActiveSync 용 Endpoint Management 커넥터 서비스가 시작되지 않음
로그 파일 및 Windows 이벤트 로그에서 오류를 확인합니다. 일반적인 원인은 다음과 같습니다.
 - Exchange ActiveSync 용 Endpoint Management 커넥터 서비스가 SQL Server 에 액세스할 수 없습니다. 원인은 다음 문제일 수 있습니다.

- * SQL Server 서비스가 실행되고 있지 않습니다.
- * 인증에 실패했습니다.

Windows 통합인증이 구성된 경우 Exchange ActiveSync 용 Endpoint Management 커넥터 서비스의 사용자 계정이 허용된 SQL 로그온이어야 합니다. Exchange ActiveSync 용 Endpoint Management 커넥터 서비스의 계정은 기본적으로 로컬 시스템으로 설정되지만 로컬 관리자 권한이 없는 다른 계정으로 변경될 수 있습니다. SQL 인증이 구성된 경우 SQL 에서 SQL 로그온이 적절히 구성되어야 합니다.

- MSP(모바일 서비스 공급자) 에 대해 구성된 포트를 사용할 수 없습니다. 시스템의 다른 프로세스에서 사용하지 않는 수신 포트를 선택해야 합니다.

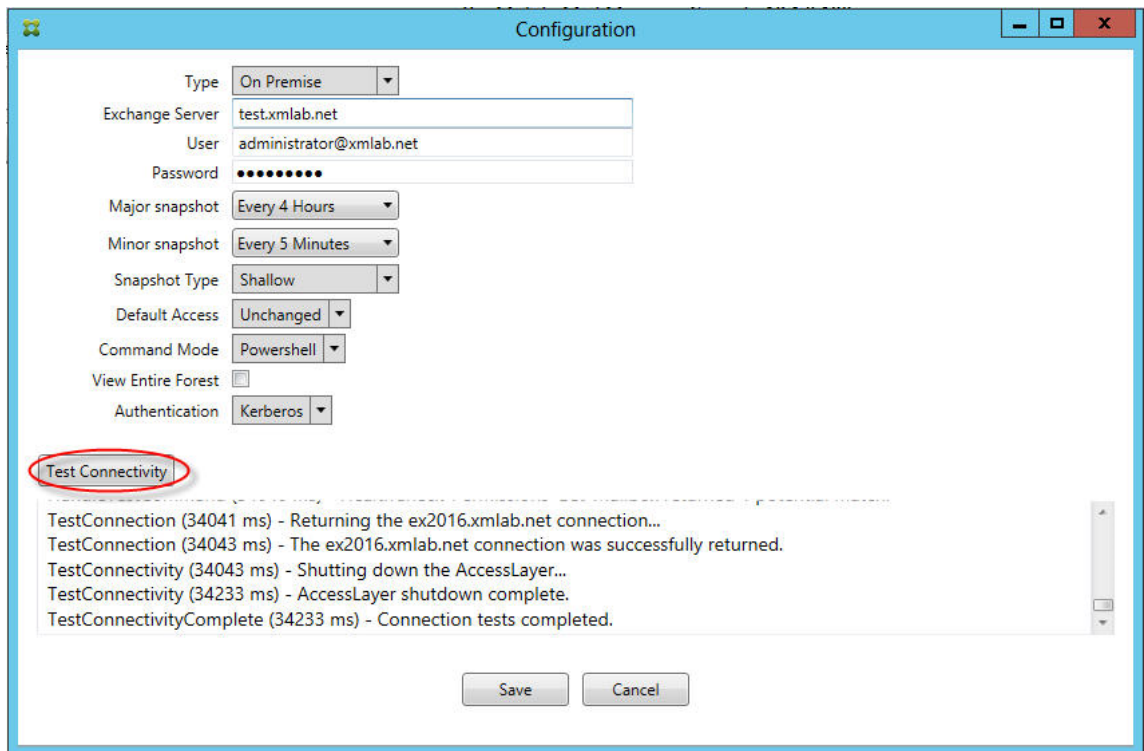
• XenMobile 에서 MSP 에 연결할 수 없음

Exchange ActiveSync 용 Endpoint Management 커넥터 콘솔의 **Configure(구성) > MSP** 탭에서 MSP 서비스 포트 및 전송이 올바르게 구성되었는지 확인합니다. 인증 그룹 또는 사용자가 올바르게 설정되었는지 확인합니다.

HTTPS 가 구성된 경우 유효한 SSL 서버 인증서가 설치되어야 합니다. IIS 가 설치된 경우 IIS Manager 를 사용하여 인증서를 설치할 수 있습니다. IIS 가 설치되지 않은 경우 [How to configure a port with an SSL certificate\(SSL 인증서로 포트를 구성하는 방법\)](#) 에서 인증서 설치에 대한 자세한 내용을 확인하십시오.

Exchange ActiveSync 용 Endpoint Management 커넥터에는 MSP 서비스 연결을 테스트하는 유틸리티 프로그램이 있습니다. `InstallFolder\MspTestServiceClient.exe` 프로그램을 실행하고 URL 및 자격 증명을 XenMobile 에서 구성할 URL 및 자격 증명으로 설정한 후 연결 테스트를 클릭합니다. XenMobile Server 에서 실행하는 웹 서비스 요청이 시뮬레이션됩니다. HTTPS 가 구성된 경우 서버의 실제 호스트 이름을 지정해야 합니다 (SSL 인증서에 지정된 이름).

연결 테스트를 사용하는 경우 하나 이상의 ActiveSyncDevice 레코드가 있어야 합니다. 그렇지 않을 경우 테스트가 실패합니다.



문제해결도구

Support\PowerShell 폴더에문제해결을위한일련의 PowerShell 유틸리티가있습니다.

문제해결도구는사용자사서함및장치를심층분석하여오류조건및잠재적오류영역을감지하고사용자에대한 RBAC 분석을수행합니다. 모든 cmdlet 의원시출력을텍스트파일에서저장할수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터

January 6, 2020

XenMobile NetScaler Connector 는이제 Exchange ActiveSync 용 Citrix Gateway 입니다. Citrix 통합포트폴리오에대한자세한내용은 [Citrix 제품가이드](#)를참조하십시오.

Exchange ActiveSync 용커넥터는 Exchange ActiveSync 프로토콜의역방향프록시역할을하는 NetScaler 에 ActiveSync 클라이언트의장치수준인증서비스를제공합니다. 인증은 XenMobile 내에서정의된정책의조합과 Exchange ActiveSync 용 Citrix Gateway 커넥터에서로컬로정의된규칙으로제어됩니다.

자세한내용은 [ActiveSync Gateway](#)에서참조하십시오.

자세한참조아키텍처다이어그램은 [아키텍처](#)를참조하십시오.

Exchange ActiveSync 용 Citrix Gateway 커넥터의현재릴리스는버전 8.5.2 입니다.

새로운항목

이후섹션에는이전의 XenMobile NetScaler Connector 인 Exchange ActiveSync 용 Citrix Gateway 커넥터의현재 및이전버전에대한새로운기능이나열됩니다.

버전 8.5.3 의새로운기능

- 이릴리스에는 ActiveSync 프로토콜 16.0 및 16.1 에대한지원이추가되었습니다.
- Google Analytics 로전송되는분석에특히스냅샷과관련하여더많은세부정보가추가되었습니다. [CXM-52261]

버전 8.5.2 의새로운기능

- XenMobile NetScaler Connector 는이제 Exchange ActiveSync 용 Citrix Gateway 입니다.

이릴리스에서는다음과같은문제가수정되었습니다.

- 둘이상의기준이정책규칙을정의하는데사용되고이러한기준중하나에서사용자 ID 가포함된경우사용자에게여러별칭이있으면규칙을적용할때별칭이확인되지않는문제가발생할수있습니다. [CXM-55355]

참고:

다음의 새로운 기능 섹션에는 Exchange ActiveSync 용 Citrix Gateway 커넥터가 이전 이름인 XenMobile NetScaler Connector 로 나타납니다. 이 이름은 버전 8.5.2 에서 변경되었습니다.

버전 **8.5.1.11** 의 새로운 기능

- 시스템 요구 사항 변경: NetScaler Connector 의 현재 버전에는 Microsoft .NET Framework 4.5 가 필요합니다.
- **Google Analytics** 지원: XenMobile NetScaler Connector 가 어떻게 사용되는지를 확인하여 제품의 개선 영역에 집중할 수 있습니다.
- **TLS 1.1** 및 **1.2** 에 대한 지원: PCI Council 에서는 보안이 취약한 TLS 1.0 의 사용을 중지하고 있습니다. XenMobile NetScaler Connector 에는 TLS 1.1 및 1.2 에 대한 지원이 추가되었습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 모니터링

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티는 Exchange Server 를 통과하면서 Secure Mobile Gateway 에 의해 허용 또는 차단된 모든 트래픽을 볼 수 있는 자세한 로깅을 제공합니다.

로그 탭을 사용하면 권한 부여를 위해 NetScaler 가 Exchange ActiveSync 용 커넥터로 전달한 ActiveSync 요청의 기록을 볼 수 있습니다.

또한 Exchange ActiveSync 용 Citrix Gateway 커넥터 웹 서비스가 실행 중인지 확인하려면 커넥터 서버의 브라우저에 URL <https://<host:port>/services/ActiveSync/Version> 을 로드합니다. URL 이 제품 버전을 문자열로 반환하면 웹 서비스가 응답하는 상태입니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터로 ActiveSync 트래픽을 시뮬레이션하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용하여 정책과 관련된 ActiveSync 트래픽을 시뮬레이션할 수 있습니다. 커넥터 구성 유틸리티에서 **Simulator**(시뮬레이터) 탭을 선택합니다. 결과에는 구성된 규칙에 따라 정책이 적용되는 방식이 표시됩니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에 대한 필터 선택

Exchange ActiveSync 용 Citrix Gateway 커넥터 필터는 장치의 정책 위반 또는 속성 설정을 분석하여 작동합니다. 장치가 조건을 충족하면 장치가 장치 목록에 배치됩니다. 이 장치 목록은 허용 목록이나 차단 목록이 아닙니다. 정의된 조건을 충족하는 장치의 목록입니다. XenMobile 내에서 커넥터에 사용 가능한 필터는 다음과 같습니다. 각 필터에는 **Allow**(허용) 또는 **Deny**(거부) 의 두 옵션이 있습니다.

- 익명 장치: XenMobile 에 등록되었지만 사용자의 ID 를 알 수 없는 장치를 허용 또는 거부합니다. 예를 들어 등록은 되었지만 사용자의 Active Directory 암호가 만료된 사용자 또는 알 수 없는 자격 증명으로 등록된 사용자일 수 있습니다.

- **Samsung KNOX 증명실패:** Samsung 장치에는보안과진단을위한기능이있습니다. 이필터는장치가 KNOX 에대해 설정되었다는확인을제공합니다. 자세한내용은 [Samsung KNOX](#)에서참조하십시오.
- **금지된앱:** 블랙리스트정책에정의된장치목록및블랙리스트앱의존재여부를기준으로장치를허용하거나거부합니다.
- **암시적허용/거부:** 다른필터규칙조건을충족하지않는모든장치의장치목록을만들고해당목록을기반으로허용또는거부합니다. 암시적허용/거부옵션을사용하면장치탭에서 Exchange ActiveSync 용 Citrix Gateway 커넥터상태가사용되고 장치의커넥터상태가표시됩니다. 또한암시적허용/거부옵션은선택되지않은다른모든커넥터필터도제어합니다. 예를들어 블랙리스트앱은커넥터에의해거부 (차단) 되지만암시적허용/거부옵션이 허용으로설정되었기때문에다른모든필터는허용됩니다.
- **비활성장치:** 지정된시간동안 XenMobile 과통신하지않은장치의장치목록을만듭니다. 이러한장치는비활성상태인것으로간주됩니다. 필터는그에따라장치를허용또는거부합니다.
- **누락된필수앱:** 사용자가등록하면설치해야하는필수앱목록을받게됩니다. 누락된필수앱필터는예를들어사용자가하나이상 의앱을삭제하여하나이상의앱이더이상없음을나타냅니다.
- **비추천앱:** 사용자가등록하면설치해야하는앱목록을받게됩니다. 비추천앱필터는해당목록에없는앱이장치에있는지확인합니다.
- **규정을준수하지않는암호:** 장치에암호가없는모든장치의장치목록을만듭니다.
- **규정위반장치:** 자체내부 IT 규정준수조건을충족하는장치를거부하거나허용할수있습니다. 규정준수는규정위반이라는이름의장치속성 (**True** 또는 **False** 인부울플래그) 으로정의되는임의의설정입니다. 이속성은수동으로만들어서값을설정하거나장치가특정조건을충족하거나충족하지않는경우자동화된동작을사용하여장치에서이속성을만들수있습니다.
 - 규정위반 = **True**. 장치가 IT 부서에서설정한규정표준및정책정의를충족하지않는경우장치는규정을위반하는것입니다.
 - 규정위반 = **False**. 장치가 IT 부서에서설정한규정표준및정책정의를충족하는경우장치는규정을준수하는것입니다.
- **해지된상태:** 모든해지된장치의장치목록을만들고해지된상태를기반으로하여허용또는거부합니다.
- **루팅된 Android/탈옥 iOS** 장치. 루팅된것으로플래그지정된모든장치의장치목록을만들고루팅된상태에따라허용또는거부합니다.
- **관리되지않는장치.** XenMobile 데이터베이스에있는모든장치의장치목록을만듭니다. 모바일응용프로그램게이트웨이는차단모드에서배포해야합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에대한연결을구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터는 Secure Web 서비스를통해 XenMobile 및다른원격구성공급자와통신합니다.

1. 커넥터구성유틸리티에서 **Config Providers**(구성공급자) 탭을클릭하고 **Add**(추가) 를클릭합니다.
2. **Config Providers**(구성공급자) 대화상자의 **Name**(이름) 에서관리권한이있는사용자이름을입력합니다. 이이름은 XenMobile Server 와의기본 HTTP 인증에서사용됩니다.
3. **Url** 에서 XenMobile GCS 의웹주소를입력합니다 (일반적으로 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 형식). *MagConfigService* 이름은대/소문자를구분합니다.
4. **Password**(암호) 에서 XenMobile Server 와의기본 HTTP 인증에서사용될암호를입력합니다.
5. **Managing Host**(호스트관리) 에서커넥터서버이름을입력합니다.

6. **Baseline Interval**(기준간격) 에서새로고침동적규칙집합을 Device Manager 에서가져올기간을지정합니다.
7. **Delta interval**(델타간격) 에서동적규칙의업데이트를가져올기간을지정합니다.
8. **Request Timeout**(요청시간초과) 에서서버요청시간초과간격을지정합니다.
9. **Config Provider**(구성공급자) 에서구성공급자서버인스턴스가정책구성을제공하는지여부를선택합니다.
10. **Events Enabled**(이벤트사용) 에서장치가차단되었을때커넥터가 XenMobile 에알리도록하려면이옵션을선택합니다. XenMobile 자동화된동작에서커넥터규칙을사용하는경우이옵션이필요합니다.
11. **Save**(저장) 를클릭한다음 **Test Connectivity**(연결테스트) 를클릭하여게이트웨이와구성공급자의연결을테스트합니다. 연결이실패하면로컬방화벽설정에서연결이허용되는지확인하거나관리자에게문의하십시오.
12. 연결이성공하면 **Disabled**(사용안함) 확인란을선택취소한다음 **Save**(저장) 를클릭합니다.

새구성공급자를추가하면 Exchange ActiveSync 용 Citrix Gateway 커넥터는공급자와연결된하나이상의정책을자동으로생성합니다. 이러한정책은 NewPolicyTemplate 섹션의 config\policyTemplates.xml 에포함된템플릿정의로정의됩니다. 이섹션내에정의된각정책요소에대해새정책이생성됩니다.

운영자는정책요소가스키마정의를준수하며표준대체문자열 (중괄호안에포함됨) 을수정하지않는범위에서정책요소를추가, 제거또는수정할수있습니다. 그런다음공급자에대한새그룹을추가하고새그룹이포함되도록정책을업데이트합니다.

XenMobile 에서정책을가져오려면

1. Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티에서 **Config Providers**(구성공급자) 탭을클릭하고 **Add**(추가) 를클릭합니다.
2. **Config Providers**(구성공급자) 대화상자의 **Name**(이름) 에서 XenMobile Server 와의기본 HTTP 인증에사용되며관리권한이있는사용자이름을입력합니다.
3. **Url** 에서 XenMobile GCS(Gateway Configuration Service) 의웹주소를입력합니다 (일반적으로 <https://<xdmHost>/xdm/services/<MagConfigService>> 형식). MagConfigService 이름은대/소문자를구분합니다.
4. **Password**(암호) 에서 XenMobile Server 와의기본 HTTP 인증에사용되는암호를입력합니다.
5. **Test Connectivity**(연결테스트) 를클릭하여게이트웨이와구성공급자의연결을테스트합니다. 연결이실패하면로컬방화벽설정에서연결이허용되는지확인하거나관리자에게문의하십시오.
6. 연결이성공하면 **Disabled**(사용안함) 확인란을선택취소한다음 **Save**(저장) 를클릭합니다.
7. **Managing Host**(호스트관리) 에서로컬호스트컴퓨터의기본 DNS 이름을그대로둡니다. 이설정는다수의 Forefront TMG(Threat Management Gateway) 서버가배열로구성된경우 XenMobile 와의통신을조정하는데사용됩니다. 설정을저장한후 GCS 를엽니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터정책모드구성

Exchange ActiveSync 용 Citrix Gateway 커넥터는다음 6 개모드에서실행될수있습니다.

- **Allow All(모두허용)**. 이 정책모드는 커넥터를 통과하는 모든 트래픽에 대한 액세스를 허용합니다. 다른 필터링 규칙은 사용되지 않습니다.
- **Deny All(모두거부)**. 이 정책모드는 커넥터를 통과하는 모든 트래픽에 대한 액세스를 거부합니다. 다른 필터링 규칙은 사용되지 않습니다.
- **Static Rules: Block Mode(정적규칙: 차단모드)**. 이 정책모드는 끝에 암시적 거부 또는 차단문이 있는 정적 규칙을 실행합니다. 커넥터는 다른 필터 규칙을 통해 허용되지 않는 장치를 차단합니다.
- **Static Rules: Permit Mode(정적규칙: 허용모드)**. 이 정책모드는 끝에 암시적 허용문이 있는 정적 규칙을 실행합니다. 다른 필터 규칙을 통해 차단 또는 거부되지 않는 장치는 커넥터를 통해 허용됩니다.
- **Static + ZDM Rules: Block Mode(정적 + ZDM 규칙: 차단모드)**. 이 정책모드는 정적 규칙을 먼저 실행한 다음, 끝에 암시적 거부 또는 차단문이 있는 XenMobile 의 동적 규칙을 실행합니다. 장치는 정의된 필터 및 Device Manager 규칙에 기반하여 허용 또는 거부됩니다. 정의된 필터 및 규칙에 일치하지 않는 모든 장치는 차단됩니다.
- **Static + ZDM Rules: Permit Mode(정적 + ZDM 규칙: 허용모드)**. 이 정책모드는 정적 규칙을 먼저 실행한 다음, 끝에 암시적 허용문이 있는 XenMobile 의 동적 규칙을 실행합니다. 장치는 정의된 필터 및 XenMobile 규칙에 기반하여 허용 또는 거부됩니다. 정의된 필터 및 규칙에 일치하지 않는 모든 장치는 허용됩니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 프로세스는 XenMobile 에서 수신된 iOS 및 Windows 기반 모바일 장치의 고유 ActiveSync ID 를 기반으로 하여 동적 규칙에 대한 허용 또는 거부를 처리합니다. Android 장치의 동작은 제조사에 따라 다르며 일부는 고유 ActiveSync ID 를 제공하지 않습니다. 이에 따라 XenMobile 은 허용 또는 차단을 결정하기 위해 Android 장치의 사용자 ID 정보를 보냅니다. 그 결과 사용자에게 Android 장치가 하나인 경우에는 허용 및 차단이 정상적으로 작동합니다. 사용자에게 Android 장치가 여러 개인 경우에는 Android 장치를 구분할 수 없기 때문에 모든 장치가 허용됩니다. 알려진 장치의 경우 ActiveSync ID 가 이러한 장치를 정적으로 차단하도록 게이트웨이를 구성할 수 있습니다. 또한 장치 유형 또는 사용자에게 이진트에 따라 차단하도록 게이트웨이를 구성할 수도 있습니다.

정책모드를 지정하려면 SMG Controller Configuration 유틸리티에서 다음을 수행합니다.

1. **Path Filters(경로 필터)** 탭을 클릭하고 **Add(추가)** 를 클릭합니다.
2. **Path Properties(경로 속성)** 대화상자의 **Policy(정책)** 목록에서 정책모드를 선택한 다음 **Save(저장)** 를 클릭합니다.

구성 유틸리티의 **Policies(정책)** 탭에서 규칙을 검토할 수 있습니다. 규칙은 Exchange ActiveSync 용 Citrix Gateway 커넥터에서 하향식으로 처리됩니다. 허용 정책에는 녹색 확인 표시가 나타납니다. 거부 정책은 선이 그려진 빨간색 원으로 표시됩니다. 화면을 새로고쳐 최근 업데이트된 규칙을 보려면 **Refresh(새로고침)** 를 클릭합니다. config.xml 파일에서 규칙 순서를 수정할 수도 있습니다.

규칙을 테스트하려면 **Simulator(시뮬레이터)** 탭을 클릭합니다. 필드에 값을 지정합니다. 로그에서 가져올 수도 있습니다. Allow(허용) 또는 Block(차단) 을 지정하는 결과 메시지가 나타납니다.

정적 규칙을 구성하려면

ActiveSync 연결 HTTP 요청의 ISAPI 필터링이 읽는 값이 포함된 정적 규칙을 입력합니다. 정적 규칙을 사용하면 Exchange ActiveSync 용 Citrix Gateway 커넥터가 다음 조건에 따라 트래픽을 허용하거나 차단할 수 있습니다.

- **User(사용자)**. Exchange ActiveSync 용 Citrix Gateway 커넥터는 장치 등록도 중 캡처된 권한 부여된 사용자 값 및 이름 구조를 사용합니다. 이러한 구조는 일반적으로 LDAP 를 통해 Active Directory 에 연결된 XenMobile 이 실행되는 서

버그참조하는도메인\사용자이름으로발견됩니다. 커넥터구성유틸리티내의 **Log(로그)** 탭에커넥터를통해전달되는값이 표시됩니다. 값구조를구분해야하거나값구조가다른경우값이전달됩니다.

- **Deviceid(ActiveSyncID)**. 연결된장치의 ActiveSyncID 라고도합니다. 이값은일반적으로 XenMobile 콘솔의 특정장치속성페이지내에서볼수있습니다. 또한이값은커넥터구성유틸리티의로그탭에서숨겨질수도있습니다.
- **DeviceType**. 커넥터는장치가 iPhone, iPad 또는기타장치유형중무엇인지판별하고이조건에따라허용또는차단할수 있습니다. 다른값과마찬가지로커넥터구성유틸리티는 ActiveSync 연결을처리중인모든연결된장치유형을표시할수있습니다.
- **UserAgent**. 사용되는 ActiveSync 클라이언트에대한정보가포함됩니다. 대개의경우지정된값은모바일장치플랫폼의 특정운영체제빌드및버전에해당합니다.

서버에서실행되는커넥터구성유틸리티는항상정적규칙을관리합니다.

1. SMG Controller 구성유틸리티에서 **Static Rules(정적규칙)** 탭을클릭한다음 **Add(추가)** 를클릭합니다.
2. **Static Rule Properties(정적규칙속성)** 대화상자에서조건으로사용할값을지정합니다. 예를들어사용자이름 (예: AllowedUser) 을입력한다음 **Disabled(사용안함)** 확인란을선택취소하여엑세스를허용할사용자를입력할수있습니다.
3. 저장을클릭합니다.

이제정적규칙이적용됩니다. 또한정규식을사용하여값을정의할수있지만 config.xml 파일에서규칙처리모드를사용하도록설정해야합니다.

동적규칙을구성하려면

XenMobile 의장치정책및속성은동적규칙을정의하며동적 Exchange ActiveSync 용 Citrix Gateway 커넥터필터를트리거할수있습니다. 이러한필터는정책위반또는속성설정의존재유무에따라트리거됩니다. 커넥터필터는장치의정책위반또는속성설정을분석하여작동합니다. 장치가조건을충족하면장치가장치목록에배치됩니다. 이장치목록은허용목록이나차단목록이아닙니다. 정의된조건을충족하는장치의목록입니다. 다음구성옵션을사용하면장치목록의장치를커넥터를사용하여허용하거나거부할지부를정의할수있습니다.

참고:

동적규칙을구성하려면 XenMobile 콘솔을사용해야합니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버아래에서 **ActiveSync Gateway** 를클릭합니다. ActiveSync Gateway 페이지가나타납니다.
3. **Activate the following rules(다음규칙활성화)** 에서활성화하려는하나이상의규칙을선택합니다.
4. Android 만의 **Android** 도메인사용자를 **ActiveSync Gateway** 로보내기에서 예를클릭하여 XenMobile 이 Android 장치정보를 Secure Mobile Gateway 로보냅니다.

이옵션을사용하도록설정하면 XenMobile 에 Android 장치사용자에대한 ActiveSync 식별자가없는경우 XenMobile 이 Android 장치정보를 Exchange ActiveSync 용 Citrix Gateway 커넥터로보냅니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 XML 파일을 편집하여 사용자 지정 정책을 구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티 **Policies(정책)** 탭의 기본 구성에서 기본 정책을 볼 수 있습니다. 사용자 지정 정책을 만들려면 Exchange ActiveSync 용 Citrix Gateway 커넥터 XML 구성 파일 (config\config.xml) 을 편집할 수 있습니다.

1. 파일에서 **PolicyList** 섹션을 찾은 다음 새 정책 요소를 추가합니다.
2. 다른 정책 그룹이나 다른 GCP 를 지원하기 위한 그룹과 같은 새 그룹도 필요한 경우 **GroupList** 섹션에서 그룹 요소를 추가합니다.
3. 필요한 경우 **GroupRef** 요소를 재정렬하여 기존 정책 내의 그룹 순서를 변경할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 XML 파일 구성

Exchange ActiveSync 용 Citrix Gateway 커넥터는 XML 구성 파일을 사용하여 커넥터 동작을 설명합니다. 이 파일은 다른 항목 중 그룹 파일과 HTTP 요청을 평가할 때 필터가 수행할 관련 동작을 지정합니다. 기본적으로 파일의 이름은 config.xml 이며, .\Program Files\Citrix\XenMobile NetScaler Connector\config 위치에서 찾을 수 있습니다.

GroupRef 노드

GroupRef 노드는 논리적 그룹 이름을 정의합니다. 기본값은 AllowGroup 및 DenyGroup 입니다.

참고:

GroupRefList 노드에서 나타나는 GroupRef 노드의 순서는 중요한 의미를 갖습니다.

GroupRef 노드의 ID 값은 특정 사용자 계정 또는 장치를 찾는 데 사용되는 구성원의 논리적 컨테이너 또는 컬렉션을 식별합니다. 작업 특성은 컬렉션의 규칙에 일치하는 구성원을 어떤 방식으로 필터링하는지를 지정합니다. 예를 들어 AllowGroup 집합의 규칙과 일치하는 사용자 계정 또는 장치는 “통과” 됩니다. 통과란 Exchange CAS 에 대한 액세스가 허용되는 것을 의미합니다. DenyGroup 집합의 규칙과 일치하는 사용자 계정 또는 장치는 “거부” 됩니다. 거부란 Exchange CAS 에 대한 액세스가 허용되지 않는 것을 의미합니다.

특정 사용자 계정/장치 또는 조합이 두 그룹 모두의 규칙을 충족할 경우에는 우선권 규칙이 사용되어 요청의 결과가 도출됩니다. 우선권은 config.xml 파일에서 위에서 아래로 GroupRef 노드의 순서를 따릅니다. GroupRef 노드는 우선순위에 따라 순위가 매겨집니다. 허용 그룹의 특정 조건에 대한 규칙은 거부 그룹의 동일 조건에 대한 규칙보다 항상 더 높은 우선순위를 가집니다.

그룹 노드

config.xml 에서는 그룹 노드도 정의합니다. 이러한 노드는 논리적 컨테이너 AllowGroup 및 DenyGroup 을 외부 XML 파일에 연결합니다. 외부 파일에서 저장된 항목이 필터 규칙의 기본을 구성합니다.

참고:

이 릴리스에서는 외부 XML 파일만 지원됩니다.

기본 설치 구성에서 두 개의 XML 파일인 allow.xml 및 deny.xml 을 구현합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터구성

속성 **Active Sync** 서비스 ID, 장치유형, 사용자에이전트 (장치운영체제), 인증된사용자및 **ActiveSync** 명령을기반으로 ActiveSync 요청을선택적으로차단또는허용하도록 Exchange ActiveSync 용 Citrix Gateway 커넥터를구성할수있습니다.

기본구성은정적및동적그룹의조합을지원합니다. SMG Controller Configuration 유틸리티를사용하여정적그룹을유지합니다. 정적그룹은지정된사용자에이전트를사용하는모든장치와같이알려진장치범주로구성될수있습니다.

동적그룹은 Gateway Configuration Provider 라고하는외부소스에의해유지됩니다. Exchange ActiveSync 용 Citrix Gateway 커넥터는주기적으로그룹을연결합니다. XenMobile 은허용및차단된장치그룹과사용자그룹을커넥터로내보낼수있습니다.

동적그룹은 Gateway Configuration Provider 라고하는외부소스에의해유지되며 Exchange ActiveSync 용 Citrix Gateway 커넥터가주기적으로수집합니다. XenMobile 은허용및차단된장치그룹과사용자그룹을커넥터로내보낼수있습니다.

정책은각그룹마다연관된작업 (허용또는차단) 과그룹구성원목록이있는순서지정된그룹목록입니다. 정책에포함될수있는그룹의수에는제한이없습니다. 일치항목이발견될때그룹의작업이수행되며이후그룹은평가되지않기때문에정책내의그룹순서는중요합니다.

구성원은요청의속성을일치시키는방법을정의합니다. 장치 ID 와같은단일속성에일치시키거나장치유형및사용자에이전트와같은여러속성에일치시킬수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에대한보안모델선택

규모에상관없이모든조직에게있어보안모델의확립은성공적모바일장치배포를위해매우중요합니다. 사용자, 컴퓨터또는장치에대한액세스를기본적으로허용하는보호또는격리된네트워크제어를사용하는경우가많습니다. 하지만이방식이항상좋은방법은아닙니다. IT 보안을관리하는조직은모두모바일장치의보안에대해조금씩다른방법이나맞춤형방법을사용할수있습니다.

모바일장치보안에는동일한논리가적용됩니다. 모바일장치의수와유형, 사용자당모바일장치의수, 사용가능한운영체제플랫폼과업의수가매우많기때문에허용모델의사용은취약한선택입니다. 대개의조직에서는제한모델이더논리적인선택입니다.

Citrix 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를 XenMobile 과통합할때허용하는구성시나리오는다음과같습니다.

허용모델 (허용모드)

허용보안모델은기본적으로모든것이허용되거나액세스권한이부여된다는전제하에작동합니다. 규칙및필터링을통해서만무언가차단되고제한이적용됩니다. 허용보안모델은모바일장치에대한보안우려가비교적느슨한조직에적합합니다. 이모델은해당하는경우 (정책규칙이실패한경우) 액세스를거부하는제한적인제어만적용합니다.

제한모델 (차단모드)

제한보안모델은 기본적으로 어떤 것도 허용되지 않거나 액세스 권한이 부여되지 않는 전제하에 작동합니다. 보안검사점을 통과하는 모든 항목이 필터링 및 검사되며 액세스를 허용하는 규칙을 통과하지 못하면 액세스가 거부됩니다. 제한보안모델은 모바일 장치에 대한 보안 기준이 비교적 엄격한 조직에 적합합니다. 이 모드에서는 액세스 허용을 위한 모든 규칙을 통과한 경우 네트워크 서비스의 기능 및 사용에 대한 액세스를 허용합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 관리

Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용하여 액세스 제어 규칙을 작성할 수 있습니다. 액세스 제어 규칙은 관리되는 장치의 ActiveSync 연결 요청에 대한 액세스를 허용하거나 차단합니다. 액세스는 장치 상태, 앱 블랙리스트 또는 화이트리스트 및 기타 규정 준수 조건에 따라 허용되거나 차단됩니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티를 사용하면 회사 전자 메일 정책을 적용하여 규정 표준을 위반하는 사용자를 차단할 수 있는 동적 및 정적 규칙을 만들 수 있습니다. 또한 전자 메일 첨부 파일 암호화를 설정하여, Exchange Server 를 통과하여 관리되는 장치로 전송되는 모든 첨부 파일을 암호화하고 권한 있는 사용자만 관리되는 장치에서 이를 볼 수 있도록 할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터를 제거하려면

1. 관리자 계정으로 XncInstaller.exe 를 실행합니다.
2. 화면 지침에 따라 제거를 완료합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터를 설치, 업그레이드 또는 제거하려면

1. 관리자 계정으로 XncInstaller.exe 를 실행하여 커넥터를 설치하거나 기존 커넥터의 업그레이드 또는 제거를 허용합니다.
2. 화면 지침에 따라 설치, 업그레이드 또는 제거를 완료합니다.

커넥터를 설치한 후에는 XenMobile 구성 서비스 및 알림 서비스를 수동으로 다시 시작해야 합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 설치

Exchange ActiveSync 용 Citrix Gateway 커넥터를 자체 Windows Server 에 설치합니다.

커넥터가 서버에 가하는 CPU 부하는 관리되는 장치 수에 따라 다릅니다. 장치 수가 많은 경우 (50,000 개 초과) 클러스터링 환경이 아니라면 둘 이상의 코어를 프로비전해야 할 수 있습니다. 커넥터의 메모리 사용량은 추가 메모리가 필요할 정도로 높지 않습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 시스템 요구 사항

Exchange ActiveSync 용 Citrix Gateway 커넥터는 NetScaler 장비에 구성된 SSL 브리지를 통해 NetScaler 와 통신합니다. 이 SSL 브리지는 장비가 모든 보안 트래픽을 XenMobile 에 직접 연결할 수 있도록 해줍니다. 커넥터에는 다음의 최소 시스템 구성이 필요합니다.

구성요소	요구사항
컴퓨터및프로세서	733MHz Pentium III 733MHz 이상프로세서. 2.0GHz Pentium III 이상프로세서 (권장)
NetScaler	소프트웨어버전 10 NetScaler 장비
메모리	1GB
하드디스크	150MB 의사용가능한하드디스크공간이있으며 NTFS 로포맷된로컬파티션
운영체제	Windows Server 2016, Windows Server 2012 R2 또는 Windows Server 2008 R2 서비스팩 1. 영어기반 서버여야합니다. Windows Server 2008 R2 서비스팩 1 에대한지원은 2020 년 1 월 14 일에종료됩니다.
기타장치	내부네트워크와통신하기위해호스트운영체제와호환되는네트워크어댑터
Microsoft .NET Framework	버전 8.5.1.11 에는 Microsoft .NET Framework 4.5 가필요합니다.
디스플레이	VGA 또는고해상도모니터

Exchange ActiveSync 용 Citrix Gateway 커넥터의호스트컴퓨터에는다음의최소사용가능한하드디스크공간이필요합니다.

- 응용프로그램: 10MB~15MB(100MB 권장)
- 로깅: 1GB(20GB 권장)

Exchange ActiveSync 용 Citrix Gateway 커넥터의플랫폼지원에대한자세한내용은 [지원되는장치운영체제](#)를참조하십시오.

장치전자메일클라이언트

일부전자메일클라이언트는한장치에대해동일한 ActiveSync ID 를일관되게반환하지않습니다. Exchange ActiveSync 용 Citrix Gateway 커넥터에서는각장치에고유한 ActiveSync ID 를사용하도록요구하므로각장치에대해동일하고유 ActiveSync ID 를일관되게생성하는전자메일클라이언트만지원됩니다. 다음과같은전자메일클라이언트는 Citrix 의테스트에 서오류없이실행되는것으로확인되었습니다.

- HTC 기본전자메일클라이언트
- Samsung 기본전자메일클라이언트
- iOS 기본전자메일클라이언트
- TouchDown

Exchange ActiveSync 용 Citrix Gateway 커넥터배포

Exchange ActiveSync 용 Citrix Gateway 커넥터를사용하면 NetScaler 를통해 XenMobile Server 와 XenMobile 관리되는장치의통신을프록시및부하분산할수있습니다. 커넥터는주기적으로 XenMobile 과통신하여정책을동기화합니다. 커넥터및 XenMobile 은함께또는독립적으로클러스터링될수있으며 NetScaler 로부하분산될수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터구성요소

- **Exchange ActiveSync 용 Citrix Gateway 커넥터서비스:** 이서비스는장치로부터의 ActiveSync 요청이인증되었는지확인하기위해 NetScaler 가호출할수있는 REST 웹서비스인터페이스를제공합니다.
- **XenMobile** 구성서비스: 이서비스는 XenMobile 과통신하여 XenMobile 정책변경내용을커넥터와동기화합니다.
- **XenMobile** 알림서비스: 이서비스는 권한이없는 장치액세스의알림을 XenMobile 에보냅니다. 이렇게하면 XenMobile 이장치가차단된이유를사용자에게알리는등의적절한조치를취할수있습니다.
- **Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티:** 관리자는이응용프로그램을사용하여커넥터를 구성하고모니터링할수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에대한수신주소를설정하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터에서 NetScaler 의 ActiveSync 트래픽승인요청을수신할수있도록하려면다음을수행합니다. 커넥터가 NetScaler 웹서비스호출을수신하는포트를지정합니다.

1. **Start(시작)** 메뉴에서 Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티를선택합니다.
2. **Web Service(웹서비스)** 탭을클릭한다음커넥터웹서비스의수신주소를입력합니다. **HTTP** 또는 **HTTPS** 또는둘다를 선택할수있습니다. 커넥터와 XenMobile 이동일한서버에함께설치된경우에는 XenMobile 과충돌하지않는포트값을 선택하십시오.
3. 값이구성되면 **Save(저장)** 를클릭한다음 **Start Service(서비스시작)** 를클릭하여웹서비스를시작합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에서장치액세스제어정책을구성하려면

관리되는장치에적용할액세스제어정책을구성하려면다음을수행하십시오.

1. Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티에서 **Path Filters(경로필터)** 탭을클릭합니다.
2. 첫번째행인 **Microsoft-Server-ActiveSync is for ActiveSync(Microsoft-Server-ActiveSync 가 ActiveSync 용)** 를선택한다음 **Edit(편집)** 를클릭합니다.
3. **Policy(정책)** 목록에서원하는정책을선택합니다. XenMobile 정책을포함하는정책의경우 **Static + ZDM: Permit Mode(정적 + ZDM: 허용모드)** 또는 **Static + ZDM: Block Mode(정적 + ZDM: 차단모드)** 를선택합니다. 이러한정책은로컬또는정적규칙을 XenMobile 의규칙과결합합니다. Permit Mode(허용모드) 는규칙에의해명시적으로 식별되지않는모든장치가 ActiveSync 에액세스할수있도록허용됨을의미합니다. Block Mode(차단모드) 는이러한장치가차단됨을의미합니다.
4. 정책을설정한후 **Save(저장)** 를클릭합니다.

XenMobile 과의통신을구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터 및 NetScaler 와 함께 사용할 XenMobile Server(구성공급자라고도 함) 의 이름과 속성을 지정합니다.

참고:

이 작업에서는 이미 XenMobile 을 설치 및 구성한 것으로 간주합니다.

1. Exchange ActiveSync 용 Citrix Gateway 커넥터 구성 유틸리티에서 **Config Providers(구성공급자)** 탭을 클릭하고 **Add(추가)** 를 클릭합니다.
2. 이 배포에서 사용 중인 XenMobile Server 의 이름과 URL 을 입력합니다. 다중 테넌트 배포에서 여러 XenMobile Server 를 배포한 경우 이름은 각 서버 인스턴스에 대해 고유해야 합니다. 예를 들어 **Name(이름)** 에 **XMS** 를 입력할 수 있습니다.
3. **Url** 에서 XenMobile GCP(GlobalConfig Provider) 의 웹 주소를 입력합니다 (일반적으로 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 형식). *MagConfigService* 이름은 대/소문자를 구분합니다.
4. **Password(암호)** 에서 XenMobile 웹 서버와의 기본 HTTP 인증에 사용될 암호를 입력합니다.
5. **Managing Host(관리호스트)** 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를 설치한 서버 이름을 입력합니다.
6. **Baseline Interval(기준간격)** 에서 새로고침 동적 규칙 집합을 XenMobile 에서 가져올 기간을 지정합니다.
7. **Request Timeout(요청시간초과)** 에서 서버 요청 시간 초과 간격을 지정합니다.
8. **Config Provider(구성공급자)** 에서 구성공급자 서버 인스턴스가 정책 구성을 제공하는지 여부를 선택합니다.
9. **Events Enabled(이벤트 사용)** 에서 장치가 차단되었을 때 Secure Mobile Gateway 가 XenMobile 에 알려도록 하려면 이 옵션을 선택합니다. Device Manager 자동화된 동작에서 Secure Mobile Gateway 규칙을 사용하는 경우 이 옵션이 필요합니다.
10. 서버를 구성한 후 **Test Connectivity(연결테스트)** 를 클릭하여 XenMobile 연결을 테스트합니다.
11. 연결이 되면 **Save(저장)** 를 클릭합니다.

중복성 및 확장성을 위한 Exchange ActiveSync 용 Citrix Gateway 커넥터 배포

Exchange ActiveSync 용 Citrix Gateway 커넥터 및 XenMobile 배포를 확장하려면 모두 동일한 XenMobile 인스턴스를 가리키는 커넥터 인스턴스를 여러 Windows 서버에 설치한 다음 NetScaler 를 사용하여 서버의 부하를 분산할 수 있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터 구성에는 두 가지 모드가 있습니다.

- 비공유 모드에서는 각 Exchange ActiveSync 용 Citrix Gateway 커넥터 인스턴스가 XenMobile Server 와 통신하며 결과 정책의 자체 사본을 유지합니다. 예를 들어 XenMobile Server 의 클러스터가 있는 경우 커넥터 인스턴스를 각 XenMobile Server 에서 실행할 수 있으며 커넥터는 로컬 XenMobile 인스턴스에서 정책을 가져옵니다.
- 공유 모드에서는 하나의 커넥터 노드가 주 노드로 지정되며 이 노드가 XenMobile 과 통신합니다. 결과 구성은 Windows 네트워킹 공유 또는 Windows(또는 타사) 복제에 의해 다른 노드 간에 공유됩니다.

전체 커넥터 구성은 하나의 폴더(몇 개의 XML 파일로 구성됨)에 있습니다. 커넥터 프로세스는 이 폴더에 있는 모든 파일의 변경 내용을 감

지하여자동으로구성을다시로드합니다. 공유모드에서는주노드에대한장애조치 (failover) 가없습니다. 하지만마지막으로알려진정상구성이커넥터프로세스에캐시되기때문에시스템은주서버중지를몇분동안 (예를들어다시시작할때까지) 허용합니다.

고급개념

May 21, 2019

참고:

이문서에서는 XenMobile Server 의고급개념에대해다룹니다. Endpoint Management 의고급정보에대해서는 [고급개념](#)을참조하십시오.

XenMobile 고급개념문서는 XenMobile 의제품설명서에대한상세한정보를제공합니다. 전문기술을통해배포시간을단축하는것이목표인이문서에는콘텐츠를작성한기술전문가의설명이인용될수있습니다.

전체 XenMobile 환경에대한의사결정사안, 권장사항, 일반적인질문및사용사례는이섹션의 XenMobile 배포안내서를참조하십시오.

XenMobile 의커뮤니티지원포럼은 [Citrix Discussions](#)를참조하십시오.

온-프레미스 XenMobile 과 Active Directory 상호작용

May 21, 2019

작성자: Siddartha Vuppala

이문서에서는 XenMobile Server 와 Active Directory 의상호작용에대해설명합니다. XenMobile Server 는인라인과백그라운드에서 Active Directory 와상호작용합니다. Active Directory 상호작용과관련된인라인및백그라운드작업에대한자세한내용은이후섹션에나와있습니다.

참고:

이문서는상호작용의개요로, 상세한내용은다루지않습니다. XenMobile 콘솔에서 Active Directory 및 LDAP 를구성하는것에대한자세한내용은 [도메인인증또는도메인및보안토큰인증](#)을참조하십시오.

인라인상호작용

XenMobile Server 는관리자가구성한 LDAP 설정을사용하여 Active Directory 와통신합니다. 이설정사용자및그룹에대한정보를검색합니다. 다음작업을수행하면 XenMobile Server 와 Active Directory 가상호작용합니다.

1. **LDAP** 구성. Active Directory 를구성하면 Active Directory 와의상호작용이발생합니다. XenMobile Server 는정보의유효성을검사하기위해 Active Directory 를통해정보를인증합니다. 서버는제공된인터넷프로토콜, 포트및서비스계정자격증명을사용하여인증을수행합니다. 바인딩에성공하면연결이올바르게구성된것입니다.

2. 그룹기반상호작용.

- a) RBAC(역할기반액세스제어) 및배달그룹정의생성시하나이상의그룹검색. XenMobile Server 관리자가 XenMobile 콘솔에서검색텍스트문자열을입력하면 XenMobile Server 가선택된도메인에서관리자가입력한하위문자열을포함하는모든그룹을검색합니다. 그런다음검색에서식별된그룹의 objectGUID, sAMAccountName 및고유이름특성을검색합니다.

참고:

이정보는 XenMobile Server 데이터베이스에서저장되지않습니다.

- b) RBAC 및배포그룹정의추가또는업데이트. XenMobile Server 관리자가이전검색결과에서해당하는 Active Directory 그룹을선택하고배포그룹정의에포함하면 XenMobile Server 가 Active Directory 에서한번에하나씩특정그룹을검색합니다. XenMobile Server 는 objectGUID 특성을검색하고구성원자격을포함하여관리자가선택한특성을검색합니다. 그룹구성원자격정보는검색된그룹의구성원자격과 XenMobile Server 데이터베이스의기존사용자또는그룹의구성원자격을확인하는데도움이됩니다. 그룹구성원자격이변경된경우영향받은사용자구성원에대한 RBAC 및배포그룹이파생되고사용자에게권한이부여됩니다.

참고:

배포그룹정의가변경된경우영향받은사용자의앱또는정책권한부여가변경될수있습니다.

- c) **OTP(일회용 PIN)** 초대. XenMobile Server 관리자가 XenMobile Server 데이터베이스에있는 Active Directory 그룹목록에서그룹을선택하면이그룹의모든직접및간접사용자가 Active Directory 에서검색됩니다. 이전단계에서식별된사용자에게 OTP 초대가전송됩니다.

참고:

이전의세가지상호작용은 XenMobile Server 구성변경에따라그룹기반상호작용이트리거되었음을나타냅니다. 구성이변경되지않은경우 Active Directory 와의상호작용이발생하지않습니다. 또한그룹측변경사항을주기적으로캡처하는백그라운드작업을수행하지않아도됩니다.

3. 사용자기반상호작용.

- a) 사용자인증. 사용자인증워크플로에서는 Active Directory 와의상호작용이두번발생합니다.
- 제공된자격증명을사용하여사용자를인증합니다.
 - objectGUID, Distinguished Name, sAMAccountName 및그룹에대한직접구성원자격을포함한선별된사용자특성을 XenMobile Server 데이터베이스에추가하거나업데이트합니다. 그룹구성원자격이변경된경우앱, 정책및액세스권한부여가재평가됩니다.
- 사용자는장치또는 XenMobile Server 콘솔에서인증을수행할수있습니다. 두시나리오에서 Active Directory 와의상호작용은동일한동작을따릅니다.
- b) App Store 액세스및새로고침. 스토어를새로고치면직접그룹구성원자격을포함한사용자특성이새로고쳐집니다. 이동작을수행하면사용자권한부여를재평가할수있습니다.
- c) 장치체크인. 관리자는 XenMobile 콘솔에서주기적장치체크인을구성할수있습니다. 장치가체크인될때마다직접그룹구성원자격을포함한해당하는사용자특성이새로고쳐집니다. 이러한체크인을통해사용자권한부여를재평가할수있습니다.

- d) 그룹별 OTP 초대. XenMobile Server 관리자가 XenMobile Server 데이터베이스에있는 Active Directory 그룹목록에서그룹을선택하면 Active Directory 에서직접및간접 (중첩) 사용자구성원이검색되고 XenMobile Server 데이터베이스에저장됩니다. 이전단계에서식별된사용자구성원에게 OTP 초대가전송됩니다.
- e) 사용자별 OTP 초대. 관리자가 XenMobile 콘솔에서검색텍스트문자열을입력하면 XenMobile Server 가 Active Directory 를쿼리하여입력텍스트문자열과일치하는사용자레코드를반환합니다. 관리자가 OTP 초대를보낼사용자를선택합니다. XenMobile Server 는 Active Directory 에서사용자세부정보를검색하고데이터베이스에이세부정보를업데이트한후사용자에게초대를전송합니다.

백그라운드상호작용

Active Directory 와의인라인통신에서는 XenMobile Server 구성이변경되면그룹기반상호작용이트리거됩니다. 구성이변경되지않은경우그룹에대해 Active Directory 와의상호작용이발생하지않습니다.

이그룹기반상호작용에는 Active Directory 와주기적으로동기화하고관심그룹에대한변경내용을업데이트하는백그라운드작업이필요합니다.

다음은 Active Directory 와상호작용하는백그라운드작업입니다.

1. 그룹동기화작업. 이작업의목적은 Active Directory 를통해관심그룹의고유이름또는 sAMAccountName 특성에대한변경내용을한번에하나씩쿼리하는것입니다. Active Directory 에검색쿼리를수행하면관심그룹의 objectGUID 를 사용하여고유이름및 sAMAccountName 특성의현재값이확인되고관심그룹의고유이름또는 sAMAccountName 값에대한변경내용이데이터베이스에업데이트됩니다.

참고:

이작업은사용자-그룹구성원자격정보를업데이트하지않습니다.

2. 중첩그룹동기화작업. 이작업은관심그룹의중첩계층에대한변경내용을업데이트합니다. XenMobile Server 에서는관심그룹의직접구성원과간접구성원에게권한을부여할수있습니다. 사용자의직접구성원자격은사용자기반인라인상호작용에서업데이트됩니다. 백그라운드에서실행되는경우이작업은간접구성원자격을추적합니다. 간접구성원자격은관심그룹의구성원인그룹에서사용자가포함되는경우를말합니다.

이작업은 XenMobile Server 데이터베이스에서 Active Directory 그룹목록을수집합니다. 이러한그룹은배포그룹 또는 RBAC 정의에포함되어있는그룹입니다. XenMobile Server 는이목록에있는각그룹의구성원을가져옵니다. 그룹의구성원은사용자및그룹을나타내는고유이름의목록으로표시됩니다. XenMobile Server 는 Active Directory 를다시쿼리하여관심그룹의사용자구성원만가져옵니다. 두목록의차이점을바탕으로관심그룹에만포함되는그룹구성원을확인한후구성원그룹의변경내용을데이터베이스에업데이트합니다. 계층의모든그룹에대해동일한프로세스가반복됩니다.

중첩그룹이변경된경우영향받은사용자에대한권한부여변경프로세스가실행됩니다.

3. 사용하지않는사용자확인. 이작업은 XenMobile 관리자가사용하지않는사용자를확인하는동작을생성한경우에만실행됩니다. 이작업은그룹동기화작업의범위내에서실행됩니다. Active Directory 를쿼리하여사용안함상태의관심사용자를한번에하나씩확인합니다.

FAQ

백그라운드 작업은 기본적으로 얼마의 빈도로 실행됩니까?

- 현지 시간으로 02:00 부터 5 시간 동안 한 번씩 그룹 동기화 작업이 실행됩니다.
- 중첩 그룹 동기화 작업은 현지 시간으로 자정부터 하루에 한 번 실행됩니다.

그룹 동기화 작업이 필요한 이유는 무엇입니까?

- Active Directory 에 있는 사용자 레코드의 memberOf 특성은 사용자가 직접 구성원인 그룹 목록이나와 있습니다. 그룹의 OU 가 변경되면 memberOf 특성에 고유 이름의 최신 값이 반영됩니다. XenMobile Server 데이터베이스도 마지막으로 새로 고쳐진 값으로 업데이트됩니다. 그룹의 고유 이름이 일치하지 않으면 사용자가 배포 그룹에 액세스할 수 없게 됩니다. 또한 해당 배포 그룹에 연결된 앱 및 정책에 액세스하지 못할 수 있습니다.
- 백그라운드 작업은 XenMobile Server 데이터베이스에 포함되는 그룹의 고유 이름 특성을 최신 상태로 유지하여 사용자가 부여받은 권한에 따라 액세스할 수 있도록 합니다.
- 동기화 작업은 Active Directory 내 그룹이 자주 변경되지 않을 것으로 가정하여 5 시간마다 실행되도록 예약됩니다.

그룹 동기화 작업을 끌 수 있습니까?

- 관심 그룹의 OU 가 변경되지 않은 것을 알고 있다면 작업은 꺼도 됩니다.

중첩된 그룹을 처리하는 백그라운드 작업이 필요한 이유는 무엇입니까?

- Active Directory 에서 그룹 중첩에 대한 변경은 일상적으로 발생하는 작업이 아닙니다. 관심 그룹의 중첩 계층이 변경되면 영항 받는 사용자의 권한 부여가 변경됩니다. 그룹이 계층에 추가되면 구성원 사용자에게 해당하는 역할이 부여됩니다. 그룹을 중첩 계층 밖으로 이동하면 그룹의 구성원 사용자가 역할 기반 권한에 액세스하지 못할 수 있습니다.
- 중첩에 대한 변경 내용은 사용자를 새로 고칠 때 캡처되지 않습니다. 중첩 변경 내용은 주문형으로 캡처할 수 없으며 백그라운드 작업을 통해 캡처됩니다.
- 중첩 변경은 자주 발생하지 않는다는 전제에 따라 변경 내용을 확인하는 백그라운드 작업은 하루에 한 번 실행됩니다.

중첩된 그룹을 처리하는 작업을 끌 수 있습니까?

- 관심 그룹의 중첩이 변경되지 않은 것을 알고 있다면 작업은 꺼도 됩니다.

XenMobile 배포

July 5, 2019

XenMobile 배포를 계획할 때는 고려할 사항이 많습니다. 선택해야 하는 장치 장치의 관리 방법 네트워크를 보호 하면서 뛰어난 사용자 환경을 제공하는 방법 필요한 하드웨어 및 하드웨어 문제 해결 방법 이 안내서에서는 이러한 질문을 비롯한 여러 질문에 대한 답을 얻을 수 있습니다. 배포 관련 항목에 대한 사용 사례 및 권장 사항과 생각하지 못했던 질문을 확인할 수 있습니다.

일부 환경 또는 사용 사례에는 지침 또는 권장 사항이 적용되지 않을 수 있습니다. XenMobile 을 실제로 배포하기 전에 테스트 환경을 설정하십시오.

이 안내서는 세 개의 주 섹션으로 구성됩니다.

- **평가:** 배포계획시 고려해야 할 일반적인 사용 사례 및 질문
- **설계 및 구성:** 환경의 설계 및 구성에 대한 권장 사항
- **작동 및 모니터링:** 실행 중인 환경이 원활하게 작동하는지 확인

평가

다른 배포와 마찬가지로 요구 사항을 평가하는 작업이 가장 먼저 수행되어야 합니다. XenMobile 을 통해 기본적으로 해결해야 하는 요구 사항은 무엇입니까? 환경의 모든 장치를 관리해야 합니까? 아니면 앱만 관리하면 됩니까? 둘 다 관리해야 합니까? XenMobile 환경에 필요한 보안 수준은 무엇입니까? 다음으로 배포 계획 시 고려해야 하는 일반적인 사용 사례 및 질문에 대해 살펴봅니다.

- [관리 모드](#)
- [장치 요구 사항](#)
- [보안 및 사용자 환경](#)
- [앱](#)
- [사용자 커뮤니티](#)
- [전자 메일 전략](#)
- [XenMobile 통합](#)
- [다중 사이트 요구 사항](#)

설계 및 구성

배포 요구 사항을 평가 한 후에는 환경의 설계 및 구성을 결정 할 수 있습니다. 계획 해야 할 몇 가지 사항:

- 서버의 하드웨어 선택
- 앱 및 장치에 대한 정책 설정
- 등록된 사용자가 저오기

이 섹션에는 이러한 각 시나리오에 대한 사용 사례 및 권장 사항이 포함되어 있습니다.

- [NetScaler 및 NetScaler Gateway 통합](#)
- [MDX 앱에 대한 SSO 및 프록시 고려 사항](#)
- [인증](#)
- [온-프레미스 배포용 참조 아키텍처](#)
- [서버 속성](#)
- [장치 및 앱 정책](#)
- [사용자 등록 옵션](#)
- [XenMobile 작업 조정](#)

작동 및 모니터링

XenMobile 을 시작하고 실행 한 후에는 모니터링을 통해 원활하게 작동하는지 확인 해야 합니다. 모니터링 섹션에서는 XenMobile 및 해당 구성 요소가 생성 하는 다양한 로그 및 메시지를 찾을 수 있는 위치와 이러한 로그를 판독 하는 방법을 설명 합니다. 또한 이 섹션에는 고

객지원피드백시간을줄일수있는일반적인문제해결단계가포함되어있습니다.

- [앱프로비전및프로비전해제](#)
- [대시보드기반작업](#)
- [역할기반액세스제어및 XenMobile 지원](#)
- [시스템모니터링](#)
- [재해복구](#)
- [Citrix 지원프로세스](#)

관리모드

January 6, 2020

각 XenMobile 인스턴스 (단일 서버또는노드클러스터) 에대해장치, 앱또는둘다를관리할지여부를선택할수있습니다. XenMobile 은장치및앱관리모드에대한다음용어를사용하며가끔배포모드라고도합니다.

- MDM 모드 (모바일기기관리모드)
- MAM 모드 (모바일앱관리모드)
- MDM+MAM 모드 (엔터프라이즈모드)

MDM 모드 (모바일기기관리모드)

중요:

MDM 모드를구성하고나중에 ENT 모드로변경하는경우동일한인증 (Active Directory) 을사용해야합니다. XenMobile 은사용자등록후의인증모드변경을지원하지않습니다. 자세한내용은 [업그레이드](#)에서참조하십시오.

MDM 을사용하는경우모바일장치를구성하고보호하고지원할수있습니다. MDM 을사용하면장치와장치의데이터를시스템수준에서보호할수있습니다. 정책, 동작및보안기능을구성할수있습니다. 예를들어장치의분실, 도난또는규정위반시장치를선택적으로초기화할수있습니다. MDM 모드에서는앱관리를사용할수없지만이모드에서공용앱스토어및엔터프라이즈앱같은모바일앱을제공할수있습니다. 다음은 MDM 모드의일반적인사용사례입니다.

- MDM 은장치수준관리정책또는제한 (예: 전체초기화, 선택적초기화또는지리적위치찾기) 이필요한회사소유장치를위한모드입니다.
- 고객이실제장치를관리해야하지만 MDX 정책 (예: 앱컨테이너화, 앱데이터공유제어또는 Micro VPN) 은필요하지않은경우.
- 사용자가모바일장치의기본전자메일클라이언트로전자메일을전송하기만하면되고이외외부액세스가가능한 Exchange ActiveSync 또는클라이언트액세스서버가있는경우. 이사용사례에서는 MDM 을사용하여전자메일전송을구성할수있습니다.
- 기본엔터프라이즈앱 (비 MDX), 공용앱스토어앱또는공용스토어에서제공되는 MDX 앱을배포하는경우. MDM 솔루션을단독으로사용하는경우장치의앱간에전송되는기밀정보의데이터유출을방지하지못할수있습니다. 데이터유출은 Office 365 앱의복사및붙여넣기또는다른이름으로저장작업에서발생할수있습니다.

MAM 모드 (모바일앱관리)

MAM 은앱데이터를보호하며앱데이터공유를제어할수있는기능을제공합니다. 또한 MAM 에서는회사데이터및리소스를개인데이터와따로관리할수있습니다. XenMobile 을 MAM 모드로구성하면 MDX 사용모바일앱을사용하여앱별컨텐츠및제어를제공할수있습니다. MAM 모드를 MAM 전용모드라고도합니다. 이용어는이모드를레거시 MAM 모드와구분합니다.

XenMobile 은 MDX 정책을활용하여네트워크액세스 (예: Micro VPN), 앱및장치상호작용, 데이터암호화및액세스를앱수준에서제어합니다.

MAM 모드는주로 BYO(Bring-Your-Own) 장치에적합합니다. 이모드에서는장치가관리되지않지만회사데이터가보호되는상태로유지되기때문입니다. MDX 에는 MDM 제어를사용하거나장치암호를암호화에사용할필요없이설정할수있는 50 개이상의 MAM 전용정책이있습니다.

또한 MAM 은모바일생산성앱을지원합니다. 이지원에는 Citrix Secure Mail 로의보안전자메일전송, 보안이적용된모바일생산성앱간의데이터공유및 ShareFile 의보안데이터스토리지가포함됩니다. 자세한내용은 [모바일생산성앱](#)에서참조하십시오.

MAM 은주로다음과같은사례에적합합니다.

- 앱수준에서관리되는모바일앱 (예: MDX 앱) 을제공합니다.
- 장치를시스템수준에서관리할필요가없습니다.

MDM+MAM(엔터프라이즈모드)

MDM+MAM 은엔터프라이즈모드라고도하는하이브리드모드로, XenMobile EMM(엔터프라이즈모빌리티관리) 솔루션에서사용가능한모든기능집합을사용하도록설정합니다. XenMobile 을 MDM+MAM 모드로구성하면 MDM 기능과 MAM 기능을모두사용할수있습니다.

XenMobile 에서는사용자로하여금장치관리의등록취소를선택할수있도록하거나장치관리의등록을의무화할지여부를지정할수있습니다. 이유연성은여러사용사례가포함되는환경에유용합니다. 이러한환경에서는 MAM 리소스에액세스할때 MDM 정책을 통한장치관리가필요하거나필요하지않을수있습니다.

MDM+MAM 은다음과같은사례에적합합니다.

- MDM 과 MAM 이모두필요한사용사례가한가지있습니다. MAM 리소스에액세스할때 MDM 이필요합니다.
- 일부사용사례에 MDM 이필요하고다른사용사례에는필요하지않습니다.
- 일부사용사례에 MAM 이필요하고다른사용사례에는필요하지않습니다.

서버모드속성을사용하여 XenMobile Server 의관리모드를지정합니다. XenMobile 콘솔에서설정을구성합니다. 모드는 MDM, MAM 또는 ENT(MDM+MAM) 일수있습니다.

사용할수있는관리모드및기능은다음표에표시된것과같이라이센스가있는 XenMobile 버전에따라결정됩니다.

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
------------------------------	-----------------------------------	-------------------------------------

MDM 기능	MDM 기능	MDM 기능
-	MAM 기능	MAM 기능
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	Secure Tasks	Secure Tasks
-	-	ShareConnect
-	-	Secure Notes
-	-	ShareFile Enterprise Edition

장치관리및 MDM 등록

XenMobile Enterprise 환경에는여러사용사례가혼재할수있으며일부사용사례에는 MAM 리소스에액세스할때 MDM 정책을통한장치관리가필요합니다. 모바일생산성업을사용자에게배포하기전에사용사례를철저히평가하고 MDM 등록이필요한지여부를결정해야합니다. MDM 등록에대한요구사항이나중요변경하려는경우사용자가장치를재등록해야합니다.

참고:

사용자에게 MDM 등록을요구할지여부를지정하려면 XenMobile 콘솔 (설정 > 서버속성) 에서 XenMobile Server 속성 등록필요를사용합니다. 이글로벌서버속성은 XenMobile 인스턴스의모든사용자및장치에적용됩니다. 이속성은 XenMobile Server 모드가 ENT 인경우에만적용됩니다.

다음은 XenMobile 엔터프라이즈모드배포에서 MDM 등록을요구할때의장점과단점 (완화옵션포함) 을요약한것입니다.

MDM 등록이선택사항인경우

장점:

- 사용자가장치를 MDM 관리에등록하지않고 MAM 리소스에액세스할수있습니다. 이옵션은사용자채택률을높입니다.
- MAM 리소스에대한액세스를보호하여엔터프라이즈데이터를보호할수있습니다.
- MDX 정책 (예: 앱암호) 을사용하여각 MDX 앱에대한앱액세스를제어할수있습니다.
- Citrix PIN 과함께 NetScaler, XenMobile Server 및응용프로그램별시간초과를구성하여추가계층의보호를제공할수있습니다.

- MDM 동작은 장치에 적용되지 않지만 일부 MDX 정책을 사용하여 MAM 액세스를 거부할 수 있습니다. 거부는 시스템 설정 (예: 탈옥 또는 루팅 장치) 에 따라 수행됩니다.
- 사용자가 첫 사용시 장치를 MDM 에 등록할지 여부를 선택할 수 있습니다.

단점:

- MDM 에 등록되지 않은 장치에서 MAM 리소스를 사용할 수 있습니다.
- MDM 정책 및 동작을 MDM 등록 장치에서만 사용할 수 있습니다.

완화 옵션:

- 사용자가 규정 위반을 선택하는 경우 책임을 져야 한다는 회사 약관에 동의하도록 합니다. 관리자에게 관리되지 않는 장치를 모니터링하도록 합니다.
- 응용 프로그램 타이머를 사용하여 응용 프로그램 액세스 및 보안을 관리합니다. 시간 초과 값을 줄이면 보안이 개선되지만 사용자 경험에 영향을 미칠 수 있습니다.
- 필요한 경우 두 번째 XenMobile 환경에서 MDM 등록을 요구할 수 있습니다. 이 옵션을 고려할 때는 두 환경을 관리하는 것으로 인해 추가 오버헤드가 발생하고 리소스가 추가로 필요하다는 점을 염두에 두십시오.

MDM 등록이 필수인 경우

장점:

- MAM 리소스에 대한 액세스를 MDM 관리 장치로만 제한할 수 있습니다.
- 원하는 경우 MDM 정책 및 동작을 환경의 모든 장치에 적용할 수 있습니다.
- 사용자가 장치 등록을 취소할 수 없습니다.

단점:

- 모든 사용자가 필수적으로 MDM 에 등록해야 합니다.
- 회사에서 개인 장치를 관리하는 것을 반대하는 사용자의 채택이 감소할 수 있습니다.

완화 옵션:

- XenMobile 이 실제로 장치에서 관리하는 항목과 관리자가 액세스할 수 있는 정보를 사용자에게 알려줍니다.
- MDM 관리가 필요하지 않은 장치에 대해 MAM 서버 모드 (MAM 전용 모드) 의 두 번째 XenMobile 환경을 사용할 수 있습니다. 이 옵션을 고려할 때는 두 환경을 관리하는 것으로 인해 추가 오버헤드가 발생하고 리소스가 추가로 필요하다는 점을 염두에 두십시오.

MAM 모드와 레거시 MAM 모드 정보

XenMobile 10.3.5 에는 새로운 MAM 전용 서버 모드가 도입되었습니다. 이전 MAM 모드와 새 MAM 모드를 구분하기 위해 설명서에는 다음과 같은 용어가 사용됩니다. 새 모드는 MAM 전용 또는 MA 라고 하며 이전 MAM 모드는 레거시 MAM 모드라고 합니다.

MAM 전용 모드는 XenMobile 의 서버 모드 속성이 MAM 일 때 적용됩니다. 장치는 MAM 모드에서 등록됩니다.

레거시 MAM 기능은 XenMobile 의 서버 모드 속성이 ENT 이고 사용자가 장치 등록을 선택하지 않는 경우 적용됩니다. 이 경우 장치는 MAM 모드에서 등록됩니다. MDM 관리를 등록 취소하는 사용자에게는 계속해서 레거시 MAM 기능이 제공됩니다.

참고:

이전에는 서버모드속성을 MAM 으로설정해도 ENT 로설정할때와동일한효과가있었습니다. MDM 관리를선택하지않은사
용자에게레거시 MAM 기능이제공되었습니다.

다음표에는특정라이선스유형및원하는장치모드에서사용되는서버모드설정이요약되어있습니다.

라이선스버전	장치등록에사용할모드	설정된서버모드속성
Enterprise/Advanced/MDM	MDM 모드	MDM
Enterprise/Advanced	MAM 모드 (MAM 전용모드)	MAM
Enterprise/Advanced	MDM+MAM 모드	ENT(레거시 MAM 모드에서작동하는 장치관리에등록하지않는사용자)

MAM 전용모드는이전에 ENT 모드에서만사용할수있었던다음기능을지원합니다. Windows Phone 에서는이러한기능을사
용할수없습니다.

- **인증서기반인증:** MAM 전용모드는인증서기반인증을지원합니다. 사용자는 Active Directory 암호가만료된경우에도
계속해서앱에엑세스할수있습니다. MAM 장치에서인증서기반인증을사용하는경우 NetScaler Gateway 를구성해야
합니다. 기본적으로 **XenMobile** 설정 > **NetScaler Gateway** 에서인증을위한사용자인증서제공은 꺼짐으로설정
되어있습니다. 이는사용자이름과암호인증이사용됨을의미합니다. 이설정을 켜짐으로설정하면인증서인증이사용됩니다.
- **자가지원포털:** 사용자가직접앱잠금및앱초기화를수행할수있습니다. 이러한동작은장치의모든앱에적용됩니다. 구성 > 동
작에서앱잠금및앱초기화동작을구성할수있습니다.
- **모든등록모드:** 관리 > 등록초대에서구성된높은수준의보안, 초대 URL 및 2 단계가포함됩니다.
- **Android** 및 **iOS** 장치에대한장치등록제한: 사용자당장치수서버속성이 구성 > 등록프로필로이동했고이제모든서버모
드에적용됩니다.
- **MAM 전용 API:** MAM 전용장치에서 REST 서비스를호출할수있습니다. REST 클라이언트와 XenMobile REST
API 를사용하여 XenMobile 콘솔에표시되는서비스를호출할수있습니다.
- MAM 전용 API 를사용하여다음을수행할수있습니다.
 - 초대 URL 과일회용 PIN 을전송합니다.
 - 장치에서앱잠금초기화를실행합니다.

다음표에는레거시 MAM 기능과 MAM 전용기능의차이점이요약되어있습니다.

등록시나리오및기타기능	레거시 MAM(ENT 서버모드)	MAM 전용모드 (MAM 서버모드)
인증서인증	지원되지않음.	지원됨. 인증서인증을사용하려면 NetScaler Gateway 가필요합니 다.

배포요구사항	장치에서직접 XenMobile Server 에액세스하지않아도됩니다.	장치에서직접 XenMobile Server 에액세스하지않아도됩니다.
등록옵션	NetScaler Gateway FQDN 을사용하거나 MDM FQDN 을사용하는경우등록하지않도록선택합니다.	XenMobile Server FQDN 을사용합니다.
등록방법 *	사용자이름 + 암호	사용자이름 + 암호, 높은수준의보안, 초대 URL + PIN, 초대 URL + 암호, 2 단계, 사용자이름 + PIN
앱잠금및초기화	지원됨.	지원됨.
앱잠금및초기화에대한자가지원포털옵션	지원되지않음.	지원됨.
앱초기화동작	앱이장치에유지되지만사용할수없습니다. XenMobile 은클라이언트의계정만삭제합니다.	앱이장치에유지되지만사용할수없습니다. XenMobile 은클라이언트의계정만삭제합니다.
MAM 전용사용에대한자동화동작.	이벤트, 장치속성, 사용자속성동작이 지원됩니다. 설치된앱기반자동화동작은지원되지않습니다.	이벤트, 장치속성, 사용자속성및일부 앱기반동작 (예: 앱초기화및앱잠금) 이 지원됩니다.
Active Directory 사용자가삭제될때의기본제공동작	앱초기화가지원됩니다.	앱초기화가지원됩니다.
등록제한	지원됨. 등록프로필을통해구성됩니다.	지원됨. 등록프로필을통해구성됩니다.
소프트웨어인벤토리	지원됨. XenMobile 이장치에설치된 앱을나열합니다.	지원되지않음.

* 알림관련: 등록초대를보낼때는 SMTP 방법만지원됩니다.

중요:

MAM 전용모드에서이전에등록한사용자는장치를재등록해야합니다. 사용자등록에필요한 XenMobile Server FQDN 을사용자에게알려줘야합니다. MAM 전용모드에서는 ENT 모드와마찬가지로 XenMobile Server FQDN 을사용하여 장치를등록합니다. 레거시 MAM 모드의경우 NetScaler Gateway FQDN 을사용하여장치를등록합니다.

장치요구사항

April 19, 2019

모든배포에서가장중요한고려사항중하나를아웃할장치입니다. iOS, Android 및 Windows 플랫폼에서옵션은많습니다. XenMobile 이지원하는장치목록은 [지원되는장치플랫폼](#)을참조하십시오.

BYOD(Bring Your Own Device) 환경에서는여러유형의지원되는플랫폼이사용될수있습니다. 그러나등록할수있는장치를사용자에게알릴때에는지원되는장치플랫폼문서의제한사항을고려하십시오. 환경에서 1~2 개의장치만허용한다하더라도 XenMobile 은 iOS, Android 및 Windows 장치에서조금씩다르게작동합니다. 각플랫폼에서사용할수있는기능집합이다른니다.

또한모든앱이태블릿폼팩터와휴대폰폼팩터모두에서사용할수있도록설계되는것은아닙니다. 대대적인변경을수행하기전에앱을테스트하여롤아웃하려는장치화면에앱이맞는지확인하십시오.

다음과같은등록요소도고려할수있습니다. Apple 및 Google 은엔터프라이즈등록프로그램을제공합니다. [Apple DEP\(장치등록프로그램\)](#) 및 [Google Android Enterprise](#)를통해직원이바로사용할수있도록미리구성된장치를구입할수있습니다. 이러한 프로그램을사용하지않는경우에도사용자에게 SMS 를통해초대링크를보낼지여부를고려해야합니다. 태블릿에서는 SMS 를사용할수없습니다.

등록에대한자세한내용은 [사용자등록옵션](#)을참조하십시오.

보안및사용자환경

January 6, 2020

보안은모든조직에서중요하지만보안과사용자환경사이의균형을맞춰야합니다. 아주안전하지만사용하기가매우어려운환경을구축할수있는가하면, 액세스제어가엄격하지않은 사용자친화적인환경을구축할수도있습니다. 이가상안내서의다른섹션에서는보안기능에대한자세한내용을다루지만이문서의목적은사용가능한보안옵션의일반적인개요를제공하고, XenMobile 의일반적인보안문제에대해고찰하는시간을가질수있도록하는것입니다.

다음은각사용사례에서주로고려해야할사항입니다.

- 특정앱, 전체장치또는둘다를보호해야합니까?
- 사용자 ID 를인증할때어떤방법을사용하고싶습니까? LDAP 인증, 인증서기반인증또는두인증의조합을사용할계획입니까?
- 사용자세션은얼마후에시간초과됩니까? 백그라운드서비스, NetScaler 및오프라인중앱액세스에대한시간초과값이서로 다르다는점에유의하십시오.
- 사용자가장치수준암호및/또는앱수준암호를설정해야합니까? 사용자가시도할수있는로그온횟수는몇번입니까? MAM 을통해구현될수있는추가앱별인증요구사항과이러한요구사항이사용자경험에미치는영향을고려하십시오.
- 사용자에게적용하려는다른제한사항은무엇입니까? 사용자가 Siri 같은클라우드서비스에액세스할수있어야합니까? 사용자는제공된각앱을사용하여무엇을할수있고무엇을할수없습니까? 사무실공간안에있는동안셀룰러데이터요금소비가되지 않도록회사 WiFi 정책을배포해야합니까?

앱과장치

가장먼저고려해야할사항중하나는다른특정앱만보호 (모바일앱관리또는 MAM) 해야하는지, 전체장치를보호 (모바일기기관리또는 MDM) 해야하는지에대한것입니다. 일반적으로, 장치수준제어가필요하지않은경우, 특히조직에서 BYOD(Bring Your Own Device) 를지원하는경우에는모바일앱만관리하면됩니다.

MAM 전용환경에서사용자는사용자에게제공되는리소스에액세스할수있습니다. MAM 정책은앱자체를보호하고관리합니다.

MDM 은전체장치를보호하는데사용되며장치의모든소프트웨어에대한인벤토리를만들고탈옥또는루팅된장치또는안전하지않은소프트웨어가설치된장치의등록을차단하는기능이포함됩니다. 그러나이수준의제어를사용하면사용자가개인장치에이렇게많은권한을허용하는것을주저하고등록비용이감소할수있습니다.

일부장치에 MDM 을요구하고다른장치에는요구하지않을수있지만이렇게하려면두개의전용환경을설정해야하므로추가리소스및유지관리가필요합니다.

인증

인증은사용자환경과많은관련이있는영역입니다. 이미 Active Directory 를실행중인조직에서는 Active Directory 를사용하여시스템에대한사용자액세스를제공하는것이가장간단한방법입니다.

인증사용자환경에서중요한또다른요소는시간초과입니다. 보안수준이높은환경에서는사용자가시스템에액세스할때마다로그온해야하지만일부조직에서는이옵션이적합하지않을수있습니다. 예를들어전자메일에액세스할때마다자격증명을입력하도록하면사용자불만이증가할수있을뿐아니라불필요한것일수도있습니다.

사용자엔트로피

보안을추가하려면 사용자엔트로피라고하는기능을사용할수있습니다. Citrix Secure Hub 와일부다른앱은암호, PIN 및인증서같은공동데이터를공유하여모든기능이올바르게작동되도록합니다. 이정보는 Secure Hub 의일반저장소에저장됩니다. **Encrypt Secrets(암호암호화)** 옵션을통해사용자엔트로피를사용하면 XenMobile 이 UserEntropy 라는이름의새저장소를만들고일반저장소의정보를새저장소로이동합니다. Secure Hub 또는다른앱에서데이터에액세스하려면사용자가암호또는 PIN 을입력해야합니다.

사용자엔트로피를사용하면여러위치에서인증계층이추가됩니다. 즉, 앱에서암호, PIN 및인증서가포함된 UserEntropy 저장소의공유데이터에액세스할때마다사용자가암호또는 PIN 을입력해야합니다.

사용자엔트로피에대한자세한내용은 XenMobile 설명서에서 [MDX Toolkit 정보](#)를참조하십시오. 사용자엔트로피를켜려면 [클라이언트속성](#)에서관련설정을찾을수있습니다.

정책

MDX 정책과 MDM 정책은조직에많은유연성을제공하지만사용자를제한할수도있습니다. 일부상황에서는이러한정책이필요할수있지만정책으로인해시스템을사용하지못할수도있습니다. 예를들어 Siri 또는 iCloud 같이원치않는중요한데이터를보낼가능성이있는클라우드응용프로그램에대한액세스를차단하려는경우이러한서비스에대한액세스를차단하는정책을설정할수있지만이러

한정책으로 인해의도치않은결과가발생할수있다는점을고려해야합니다. iOS 키보드마이크에도클라우드액세스가사용되며이기능에대한액세스도차단할수있습니다.

앱

EMM(엔터프라이즈모빌리티관리) 은 MDM(모바일기기관리) 과 MAM(모바일응용프로그램관리) 으로나뉩니다. MDM 은모바일장치외보안및제어에사용되고 MAM 은응용프로그램의제공및관리를용이하게합니다. BYOD 채택이증가하면 XenMobile 같은 MAM 솔루션을구현하여응용프로그램제공, 소프트웨어라이선스, 구성및응용프로그램수명주기관리를지원할수있습니다.

XenMobile 을사용하면특정 MAM 정책및 VPN 설정을구성하여데이터유출및기타보안위협을방지함으로써이러한앱을추가로 보호할수있습니다. XenMobile 은 MAM 전용또는 MDM 전용환경으로솔루션을배포하거나동일한플랫폼에서 MDM 과 MAM 기능을모두제공하는통합 XenMobile 엔터프라이즈환경으로구현할수있는유연성을제공합니다.

모바일장치에앱을제공하는것에더해 XenMobile 은 MDX 기술을통해앱을컨테이너화할수있는기능을제공합니다. MDX 는장치수준암호화와구분된암호화를통해앱을보호합니다. 앱을초기화하거나잠금수있으며세분화된정책기반제어가앱에적용됩니다. ISV(독립소프트웨어공급업체) 는 Worx App SDK 를사용하여이러한제어를적용할수있습니다.

기업환경에서사용자는다양한모바일앱을사용하여업무를지원합니다. 공용앱스토어의앱, 사내에서개발한앱또는일부경우기본앱이여기에포함될수있습니다. XenMobile 은이러한앱을다음과같이범주화합니다.

공용앱: iTunes 또는 Google Play 와같은공용앱스토어에서무료또는유료로제공되는앱이포함됩니다. 조직외부의공급업체는주로공용앱스토어를통해앱을제공합니다. 이옵션을사용하는경우공급업체의고객이인터넷에서직접앱을다운로드할수있습니다. 조직의사용자는사용자요구사항에따라수많은공용앱을사용할수있습니다. 예를들어 GoToMeeting, Salesforce 및 EpicCare 앱이이러한앱에포함됩니다.

Citrix 는공용앱스토어에서직접앱이진을다운로드한다음 MDX Toolkit 을사용하여엔터프라이즈배포용으로래핑하는것을지원하지않습니다. 타사용용프로그램을래핑해야하는경우앱공급업체를통해 MDX Toolkit 을사용하여래핑할수있는앱이진을받아야합니다.

사내앱: 많은조직이사내개발자를통해특정기능을제공하는앱을만듭니다. 사내개발자는조직내에서이러한앱을독립적으로개발하고배포합니다. 경우에따라일부조직에서는 ISV 가제공하는앱을사용하기도합니다. 이러한앱을기본앱으로배포하거나 XenMobile 같은 MAM 솔루션을사용하여앱을컨테이너화할수있습니다. 예를들어의료조직에서는의사가모바일장치에서환자정보를볼수있도록하는사내앱을만들수있습니다. 그러다음 MDX Toolkit 으로앱을래핑하여환자정보를보호하고백엔드환자데이터베이스서버에대한 VPN 액세스를지원할수있습니다.

웹및 SaaS 앱: 내부네트워크에서액세스되는앱 (웹앱) 또는공용네트워크를통해액세스되는앱 (SaaS) 이포함됩니다. XenMobile 에서는앱커넥터목록을사용하여사용자지정웹및 SaaS 앱을만들수도있습니다. 이러한앱커넥터를사용하면기존웹앱에대한 SSO(Single Sign-on) 를쉽게구현할수있습니다. 자세한내용은 [앱커넥터유형](#)에서참조하십시오. 예를들어 Google Apps 에대한 SAML(Security Assertion Markup Language) 기반 SSO 에는 Google Apps SAML 을사용할수있습니다.

모바일생산성앱: Citrix 에서개발한앱으로, XenMobile 라이선스에포함됩니다. 자세한내용은 [모바일생산성앱정보](#)에서참조하십시오. 또한 Citrix 는다른 ISV 에서 Worx App SDK 를사용하여개발하는다른 [비즈니스용앱](#)을제공합니다.

HDX 앱: Windows 에서호스트되는앱으로, StoreFront 를사용하여게시합니다. Citrix Virtual Apps and Desktops 환경이있는경우이러한앱을 XenMobile 과통합하여등록된사용자에게앱을제공할수있습니다.

XenMobile 을 사용하여 배포하고 관리하려는 모바일 앱의 유형에 따라 기본 구성과 아키텍처가 달라집니다. 예를 들어 권한 수준이 서로 다른 여러 사용자 그룹이 단일 앱을 사용하려는 경우 개별 배달 그룹을 만들어 동일한 앱의 두 가지 개별 버전을 배포할 수 있습니다. 또한 사용자 장치에서 정책 불일치가 발생하지 않도록 사용자 그룹 구성원 자격이 상호 배타적인지 확인해야 합니다.

또한 Apple iOS VPP (Volume Purchase Program) 를 사용하여 iOS 응용 프로그램 라이선스를 관리해야 할 수 있습니다. 이 옵션을 사용하려면 VPP 프로그램에 등록하고 XenMobile 콘솔에서 VPP 라이선스를 사용하여 앱을 배포하도록 XenMobile VPP 설정을 구성해야 합니다. 이와 같은 다양한 활용 사례에서는 XenMobile 환경을 구현하기 전에 MAM 전략을 평가하고 계획하는 것이 중요합니다. MAM 전략을 계획하려면 먼저 다음을 정의합니다.

앱 유형: 지원하려는 서로 다른 유형의 앱을 나열하고 공용, 기본, 모바일 생산성 앱, 웹, 사내, ISV 앱 및 기타 등으로 앱을 범주화합니다. 또한 서로 다른 장치 플랫폼 (예: iOS 및 Android) 에 대한 앱을 범주화합니다. 범주화는 각 앱 유형에 필요한 서로 다른 XenMobile 설정을 조정하는 데 유용합니다. 예를 들어 특정 앱에는 래핑을 사용할 수 없으며 일부 앱의 경우 Worx App SDK 를 사용하여 다른 앱과의 상호 작용을 위한 특수 API 를 사용하도록 설정해야 할 수 있습니다.

네트워크 요구 사항: 특정 네트워크 액세스 요구 사항 및 적절한 설정으로 앱을 구성해야 합니다. 예를 들어 특정 앱은 VPN 을 통해 내부 네트워크에 액세스해야 하고 다른 앱은 DMZ 를 통해 액세스를 라우팅하기 위해 인터넷 액세스가 필요할 수 있습니다. 이러한 앱이 필요한 네트워크에 연결하려면 다양한 설정을 적절히 구성해야 합니다. 앱별 네트워크 요구 사항을 정의하면 아키텍처의 사결정이 조기에 확정되므로 전체 구현 프로세스가 간소화됩니다.

보안 요구 사항: XenMobile 서버를 설치할 때 올바른 구성을 만들려면 개별 앱 또는 모든 앱에 적용되는 보안 요구 사항을 정의하는 것이 중요합니다. MDX 정책 같은 설정은 개별 앱에 적용되지만 세션 및 인증 설정은 모든 앱에 적용되며 일부 앱에는 특정 암호화, 컨테이너화, 래핑, 암호화, 인증, 지오펜스, 암호 또는 데이터 공유 요구 사항이 포함될 수 있습니다. 이러한 요구 사항을 사전에 간략히 정의하면 배포가 간소화됩니다.

배포 요구 사항: 정책 기반 배포를 사용하면 규정을 준수하는 사용자만 게시된 앱을 다운로드하도록 허용할 수 있습니다. 예를 들어 장치 암호화를 사용하거나, 관리되는 장치이거나, 최소 운영 체제 버전을 충족하는 장치에서만 특정 앱을 다운로드할 수 있도록 설정할 수 있습니다. 또한 특정 앱을 회사 사용자에게만 제공할 수 있습니다. 이러한 요구 사항을 사전에 간략히 정의해야 적절한 배포 규칙 또는 동작을 구성할 수 있습니다.

라이선스 요구 사항: 앱 관련 라이선스 요구 사항을 기록해야 합니다. 이러한 메모는 라이선스 사용 현황을 효과적으로 관리하고, XenMobile 에서 라이선스를 용이하게 하는 특정 기능을 구성해야 할지 여부를 결정하는데 도움이 됩니다. 예를 들어 iOS 앱을 배포하는 경우 사용자는 앱이 무료인지, 유료인지에 관계없이 Apple 의 앱 라이선스 요구 사항에 따라 iTunes 계정으로 로그인해야 합니다. Apple VPP 에 등록하면 이러한 앱을 XenMobile 을 통해 배포하고 관리할 수 있습니다. VPP 를 사용하면 사용자가 iTunes 계정으로 로그인하지 않고 앱을 다운로드할 수 있습니다. 또한 Samsung SAFE 및 Samsung KNOX 같은 도구에는 기능을 배포하기 전에 완료해야 하는 특수한 라이선스 요구 사항이 있습니다.

블랙리스트/화이트리스트 요구 사항: 특정 앱의 경우 사용자의 설치 또는 사용을 전혀 허용하지 않을 수 있습니다. 블랙리스트를 만들면 규정 위반 이벤트가 정의됩니다. 관리자는 이러한 규정 위반이 발생할 경우 트리거할 정책을 설정할 수 있습니다. 또한 사용은 허용되지만 하나 이상의 이유로 블랙리스트에 포함되는 앱이 존재할 수 있습니다. 이 경우 관리자는 화이트리스트에 앱을 추가하고, 앱을 사용할 수 있지만 필수 앱은 아님을 표시할 수 있습니다. 또한 새 장치에 미리 설치된 앱에는 운영 체제의 일부는 아니지만 자주 사용되는 앱이 포함될 수 있습니다. 이러한 앱은 블랙리스트 전략과 상충할 수 있습니다.

앱사용사례

한의료조직에서 XenMobile 을배포하여모바일앱의 MAM 솔루션으로사용하려고합니다. 모바일앱은회사및 BYOD 사용자에게제공됩니다. IT 부서에서는다음앱을제공하고관리하기로결정합니다.

- **모바일생산성앱:** Citrix 가제공하는 iOS 및 Android 앱입니다.
- **Secure Mail:** 전자메일, 일정및연락처앱입니다.
- **Secure Web:** 인터넷및인트라넷사이트에대한액세스를제공하는보안웹브라우저입니다.
- **Secure Notes:** 전자메일및일정통합기능이포함된보안메모앱입니다.
- **ShareFile:** 공유데이터에액세스하고파일공유, 동기화및편집을수행하는앱입니다.

공용앱스토어

- **Secure Hub:** XenMobile 과통신하는모든모바일장치에사용되는클라이언트입니다. IT 부서에서는 Secure Hub 클라이언트를통해보안설정, 구성및모바일앱을모바일장치에푸시합니다. Android 및 iOS 장치는 Secure Hub 를통해 XenMobile 에등록됩니다.
- **Citrix Receiver:** 사용자가모바일장치에서 Citrix Virtual Apps and Desktops 로호스트된응용프로그램을열때 사용하는모바일앱입니다.
- **GoToMeeting:** 사용자가다른컴퓨터사용자, 고객, 클라이언트또는동료와인터넷을통해실시간으로만날수있도록하는 온라인모임, 데스크톱공유및비디오컨퍼런스클라이언트입니다.
- **SalesForce1:** Salesforce1 을사용하면사용자가모바일장치에서 Salesforce 에액세스하고모든 Salesforce 사용자에대한통합환경에서모든 Chatter, CRM, 사용자지정앱및비즈니스프로세스를확인할수있습니다.
- **RSA SecurID:** 2 단계인증을위한소프트웨어기반토큰입니다.
- **EpicCare** 앱: 환자차트, 환자목록, 일정및메시징에대한액세스를보호하고이동중에액세스할수있도록하는의료기관종사자용앱입니다.
 - **Haiku:** iPhone 및 Android 폰용모바일앱입니다.
 - **Canto:** iPad 용모바일앱입니다.
 - **Rover:** iPhone 및 iPad 용모바일앱입니다.

HDX: Citrix Virtual Apps and Desktops 를통해제공되는앱입니다.

- **Epic Hyperspace:** 전자의료기록관리를위한 Epic 클라이언트응용프로그램입니다.

ISV

- **Vocera:** HIPAA 준수 VoIP(Voice-over IP) 및메시징모바일앱으로, iPhone 및 Android 스마트폰을통해시간과 장소에관계없이 Vocera 음성기술의이점을활용할수있도록합니다.

사내앱

- **HCMail:** 암호화된메시지를작성하고, 내부메일서버의주소록을검색하고, 암호화된메시지를전자메일클라이언트를사용하여연락처로보내는데유용한앱입니다.

사내웹앱

- **PatientRounding:** 여러부서에서환자건강정보를기록하는데사용되는웹응용프로그램입니다.
- **Outlook Web Access:** 웹브라우저를통해전자메일에액세스할수있습니다.
- **SharePoint:** 조직전체의파일및데이터공유에사용됩니다.

다음표에는 MAM 구성에필요한기본정보가나와있습니다.

앱이름	앱유형	MDX 래핑	iOS	Android
Secure Mail	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
Secure Web	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
Secure Notes	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
ShareFile	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
Secure Hub	공용앱	해당없음	예	예
Citrix Receiver	공용앱	해당없음	예	예
GoToMeeting	공용앱	해당없음	예	예
SalesForce1	공용앱	해당없음	예	예
RSA SecurID	공용앱	해당없음	예	예
Epic Haiku	공용앱	해당없음	예	예
Epic Canto	공용앱	해당없음	예	아니요
Epic Rover	공용앱	해당없음	예	아니요
Epic Hyperspace	HDX 앱	해당없음	예	예
Vocera	ISV 앱	예	예	예
HCMail	사내앱	예	예	예
PatientRounding	웹앱	해당없음	예	예
Outlook Web Access	웹앱	해당없음	예	예
SharePoint	웹앱	해당없음	예	예

다음표에는 XenMobile 에서 MAM 정책을구성할때참조할수있는특정요구사항이나와있습니다.

앱이름	프록시필터링	라이선스	지오펠스	Worx App SDK	최소운영체제버전
Epic Canto	필요없음	VPP	필요없음	해당없음	적용되지않음
Epic Rover	필요없음	VPP	필요없음	해당없음	적용되지않음
Epic Hyperspace	필요없음	해당없음	필요없음	해당없음	적용되지않음
Vocera	필수	해당없음	필수	필수	적용
HCMail	필수	해당없음	필수	필수	적용
PatientRound- ing	필수	해당없음	필요없음	해당없음	적용되지않음
Outlook Web Access	필수	해당없음	필요없음	해당없음	적용되지않음
SharePoint	필수	해당없음	필요없음	해당없음	적용되지않음

사용자커뮤니티

모든조직은서로다른기능적역할로운영되는다양한사용자커뮤니티로구성됩니다. 이러한사용자커뮤니티는사용자의모바일장치를 통해제공되는다양한리소스를사용하여서로다른작업및사무기능을수행합니다. 사용자는관리자가제공하는모바일장치를사용하거나개인모바일장치를사용하여자택또는원격사무실에서근무할수있으며이러한장치에서특정보안규정준수규칙이적용되는도구에 액세스할수있습니다.

업무를간소화하거나지원할목적으로모바일장치를사용하는사용자커뮤니티가많아지면 EMM(엔터프라이즈모빌리티관리) 을통해데이터유출을방지하고조직의보안제한을시행하는것이중요합니다. 관리자는효율적이고정교한모바일기기관리를위해사용자커뮤니티를범주화할수있습니다. 이렇게하면사용자리소스에매핑하는작업이간소화되고올바른보안정책을해당하는사용자에게적용할수있습니다.

다음에는의료조직의사용자커뮤니티를 EMM 용으로분류하는방법을설명합니다.

사용자커뮤니티사용사례

이예의의료조직은기술리소스및액세스권한을다수의사용자 (예: 네트워크및계열사직원및자원봉사자) 에게제공합니다. 조직은 EMM 솔루션을일반사용자에게만롤아웃하기로선택했습니다.

이조직의사용자역할및기능은임상, 비임상및계약업체를포함하는하위그룹으로분류될수있습니다. 선택한사용자집합에는회사모바일장치가제공되고다른사용자집합은개인장치에서제한된회사리소스에액세스할수있습니다. 적절한수준의보안제한을적용하고데이터유출을방지하기위해조직은회사 IT 부서를통해등록된각장치, 회사장치및 BYOD(Bring Your Own Device) 를관리하기로결정했습니다. 또한사용자는단일장치만등록할수있습니다.

다음섹션에는각하위그룹의역할및기능에대한개요가나와있습니다.

임상

- 간호사
- 의사 (진료의, 외과의등)
- 전문가 (영양사, 임상병리사, 마취의, 방사선사, 심장전문의, 종양전문의등)
- 외부의사 (직원이아닌의사및원격사무실에서근무하는근로자)
- 가정건강서비스 (환자의집을방문하여의사서비스를수행하는사무실및모바일근로자)
- 연구전문가 (6 개연구기관에서약물문제에대한답을찾는임상연구를수행하는지식근로자및고급사용자)
- 교육및훈련 (교육및훈련중인간호사, 의사및전문가)

비임상

- 공유서비스 (HR, 급여, 미지급금, 공급망서비스등다양한경영지원기능을수행하는사무실근로자)
- 의사서비스 (관리서비스, 분석및비즈니스인텔리전스, 비즈니스시스템, 클라이언트서비스, 재무, 관리되는치료관리, 환자 액세스솔루션, 매출주기솔루션등다양한건강관리, 관리서비스및비즈니스프로세스공급자솔루션을수행하는사무실근로자)
- 지원서비스 (복리후생관리, 임상통합, 커뮤니케이션, 보상및실적관리, 설비및부동산서비스, HR 기술시스템, 정보서비스, 내부감사및프로세스개선등다양한비임상기능을수행하는사무실근로자)
- 자선프로그램 (자선프로그램지원과관련된다양한기능을수행하는사무실및모바일근로자)

계약업체

- 제조업체및공급업체파트너 (내부에서근무하거나사이트간 VPN 을통해원격으로연결하여다양한비임상지원기능을제공)

이조직에서는위의정보를바탕으로다음과같은엔터티를만들었습니다. XenMobile 의배달그룹에대한자세한내용은 [리소스배 포](#)를참조하십시오.

Active Directory OU(조직구성단위) 및그룹

OU = XenMobile 리소스인 경우:

- OU = 임상, 그룹 =
 - XM 간호사
 - XM 의사
 - XM 전문가
 - XM 외부의사
 - XM 가정건강서비스
 - XM 연구전문가
 - XM 교육및훈련
- OU = 비임상, 그룹 =
 - XM 공유서비스
 - XM 의사서비스

- XM 지원서비스
- XM 자선프로그램

XenMobile 로컬사용자및그룹

그룹 = 계약업체인경우, 사용자 =

- 공급업체 1
- 공급업체 2
- 공급업체 3
- ... 공급업체 10

XenMobile 배달그룹

- 임상간호사
- 임상 의사
- 임상전문가
- 임상외부의사
- 임상가정건강서비스
- 임상연구전문가
- 임상교육및훈련
- 비임상공유서비스
- 비임상의사서비스
- 비임상지원서비스
- 비임상자선프로그램

배달그룹과사용자그룹매핑

Active Directory 그룹	XenMobile 배달그룹
XM 간호사	임상간호사
XM 의사	임상 의사
XM 전문가	임상전문가
XM 외부의사	임상외부의사
XM 가정건강서비스	임상가정건강서비스
XM 연구전문가	임상연구전문가
XM 교육및훈련	임상교육및훈련

XM 공유서비스	비임상공유서비스
XM 의사서비스	비임상의사서비스
XM 지원서비스	비임상지원서비스
XM 자선프로그램	비임상자선프로그램

배달그룹과리소스매핑

다음표에는이사용사례의각배달그룹에할당되는리소스가설명되어있습니다. 첫번째표는모바일앱할당을보여주고두번째표는공용 앱, HDX 앱및장치관리리소스를보여줍니다.

XenMobile 배달그룹	Citrix 모바일앱	공용모바일앱	HDX 모바일앱
임상간호사	X		
임상의사			
임상전문가			
임상외부의사	X		
임상가정건강서비스	X		
임상연구전문가	X		
임상교육및훈련		X	X
비임상공유서비스		X	X
비임상의사서비스		X	X
비임상지원서비스	X	X	X
비임상자선프로그램	X	X	X
계약업체	X	X	X

XenMobile 배달그룹	공용앱: RSA SecurID	공용앱: EpicCare Haiku	HDX 앱: Epic Hy-perspace	암호정책	장치제한	자동화된동작	WiFi 정책
임상간호사							X

임상의사		X
임상전문가		
임상외부의사		
임상가정건강서비스		
임상연구전문가		
임상교육및훈련	X	X
비임상공유서비스	X	X
비임상의사서비스	X	X
비임상지원서비스	X	X

참고및사전요구사항

- XenMobile 을초기구성하는동안모든사용자라는이름의기본배달그룹이만들어집니다. 이배달그룹을사용하는경우모든 Active Directory 사용자가 XenMobile 에등록할수있습니다.
- XenMobile 은요청이있을경우 LDAP 서버에대한동적연결을사용하여 Active Directory 사용자및그룹을동기화합니다.
- 사용자가 XenMobile 에서매핑되지않은그룹에포함되는경우해당사용자는등록할수없습니다. 마찬가지로사용자가여러그룹의구성원인경우 XenMobile 은해당사용자를 XenMobile 에매핑된그룹의구성원으로만범주화합니다.
- MDM 등록을필수로규정하려면 XenMobile 콘솔의서버속성에서등록필요옵션을 True 로설정해야합니다. 자세한내용은 [서버속성](#)에서참조하십시오.
- SQL Server 데이터베이스의 dbo.userlistgrps 아래에서항목을삭제하여 XenMobile 배달그룹에서사용자그룹을삭제할수있습니다.
주의: 이동작을수행하기전에 XenMobile 및데이터베이스의백업을만드십시오.

XenMobile 의장치소유권정보

사용자장치의소유자에따라사용자그룹화할수있습니다. 장치소유권에는회사소유장치와 BYOD(Bring Your Own Device)라고하는사용자소유장치가포함됩니다. XenMobile 콘솔의설정페이지에서배포규칙과 XenMobile 서버속성을사용하여

BYOD 장치의네트워크연결방법을제어할수있습니다. 배포규칙에대한자세한내용은 XenMobile 설명서에서 [배포규칙구성](#) 문서를참조하십시오. 서버속성에대한자세한내용은 [서버속성](#)을참조하십시오.

앱에액세스하려는모든 BYOD 사용자에게회사의장치관리에대한동의를요구하도록서버속성을설정하거나장치관리없이회사앱에대한사용자액세스를제공할수있습니다.

서버설정 **wsapi.mdm.required.flag** 를 **true** 로설정하면 XenMobile 이모든 BYOD 장치를관리하며등록을거부하는사용자는앱액세스가거부됩니다. 엔터프라이즈 IT 팀이보안을강화하는동시에사용자에게개선된등록경험을제공해야한다면 XenMobile 에서사용자장치를등록할때 **wsapi.mdm.required.flag** 를 **true** 로설정하는것이 좋습니다.

wsapi.mdm.required.flag 를기본설정인 **false** 로유지하면사용자가등록을거부할수있지만사용자는장치에서 XenMobile Store 를통해앱에액세스할수있습니다. 장치관리없이엔터프라이즈앱관리만으로개인정보보호, 법적또는규제제한을준수할수있는환경에서는 **wsapi.mdm.required.flag** 를 **false** 로설정하는것이 좋습니다.

XenMobile 을통해관리되지않는장치의사용자는 XenMobile Store 를통해앱을설치할수있습니다. 선택적초기화또는전체초기화같은장치수준제어대신앱정책을사용하여앱액세스를제어할수있습니다. 설정한값에따라정책은장치에서주기적으로 XenMobile 서버에연결하여앱실행이허용되는지여부를확인해야 합니다.

보안요구사항

XenMobile 환경을배포할때의보안고려사항은그양이급속도로많아질수있습니다. 서로맞물린항목과설정이많기때문에허용가능한수준의보호를제공하기위해먼저설정해야하는항목또는선택해야하는항목을파악하기가어려울수있습니다. 다음표에간략히설명된높은수준의보안, 더높은수준의보안및가장높은수준의보안에대한권장사항을참조하면이러한항목및설정을보다간단하게선택할수 있습니다.

참고로배포모드선택은보안고려사항만으로설명되지않는다는점에유의하십시오. 또한배포모드를선택하기전에사용사례의요구사항을검토하고보안고려사항을완화할수있는지여부를결정해야 합니다.

높음: 이러한설정을사용하면최적의사용자환경을제공하면서대부분의조직에허용되는기본적인수준의보안을유지할수 있습니다.

더높음: 이러한설정은보안과사용편의성간에더적절한균형을유지합니다.

가장높음: 이러한권장사항을따르면사용편의성및사용자채택을포기하고매우높은수준의보안을제공할수 있습니다.

배포모드보안고려사항

다음표에는각보안수준에대한배포모드가명시되어 있습니다.

높은수준의보안	더높은수준의보안	최고수준의보안
MAM 및/또는 MDM	MDM+MAM	MDM+MAM 및 FIPS

참고:

- 사용사례에 따라 MDM 전용 또는 MAM 전용 배포로 보안 요구사항을 충족하고 우수한 사용자 환경을 제공할 수 있습니다.
- 앱 컨테이너화, Micro VPN 또는 앱별 정책이 필요하지 않은 경우 MDM 을 사용하여 충분히 장치치를 관리하고 보호할 수 있습니다.
- 앱 컨테이너화를 통해 모든 비즈니스 및 보안 요구사항을 충족할 수 있는 BYOD 같은 사용 사례의 경우 MAM 전용 모드를 사용하는 것이 좋습니다.
- 보안 수준이 높은 환경 (및 회사에서 발행한 장치) 에서는 MDM+MAM 모드를 사용하여 제공되는 모든 보안 기능을 활용하는 것이 좋습니다. MDM 등록은 XenMobile 콘솔의 서버 속성을 통해 적용해야 합니다.
- FIPS 옵션은 정부 기관처럼 가장 높은 보안 수준이 요구되는 환경을 위한 옵션입니다.

FIPS 모드를 사용하는 경우 SQL 트래픽을 암호화하도록 SQL Server 를 구성해야 합니다.

NetScaler 및 NetScaler Gateway 보안 고려 사항

다음 표에는 각 보안 수준에 대한 NetScaler 및 NetScaler Gateway 권장 사항이 명시되어 있습니다.

높은 수준의 보안	더 높은 수준의 보안	최고 수준의 보안
NetScaler 가 권장됩니다. MAM 및 ENT 의 경우 NetScaler Gateway 가 필요하며 MDM 의 경우 권장됩니다.	XenMobile 이 DMZ 에 있는 경우 XenMobile 용 표준 NetScaler 마법사 구성과 SSL 브리지를 사용합니다. 또는 XenMobile 서버가 내부 네트워크에 있는 경우 보안 표준을 충족하는데 필요하다면 SSL 오프로드를 사용합니다.	SSL 오프로드 및 종단간 암호화

참고:

- MDM 모드에서는 SSL 트래픽을 XenMobile 서버에서 종료하는 것을 조건으로 NAT 또는 기존 타사 프록시/부하 분산 장치를 통해 XenMobile 서버를 인터넷에 공개할 수 있지만 여기에는 잠재적 보안 위험이 있습니다.
- 보안 수준이 높은 환경에서는 기본 XenMobile 구성의 NetScaler 로 지정된 수준 이상의 보안 요구사항을 충족할 수 있어야 합니다.
- 보안 요구사항이 가장 높은 MDM 환경에서는 SSL 을 NetScaler 에서 종료하여 경계에서 트래픽을 검사하는 동시에 종단간 SSL 암호화를 유지할 수 있습니다.
- 필요한 경우 SSL/TLS 암호화를 정의할 수 있습니다.
- SSL FIPS NetScaler 하드웨어도 사용할 수 있습니다.
- 자세한 내용은 [NetScaler Gateway 및 NetScaler 통합](#)에서 참조하십시오.

등록 보안 고려 사항

다음 표에는 각 보안 수준에 대한 NetScaler 및 NetScaler Gateway 권장 사항이 명시되어 있습니다.

높은 수준의 보안	더 높은 수준의 보안	최고 수준의 보안
Active Directory 그룹 구성원 자격만 사용됩니다. 모든 사용자 배달 그룹은 사용되지 않습니다.	초대 전용 등록 모드를 사용합니다. Active Directory 그룹 구성원 자격만 사용됩니다. 모든 사용자 배달 그룹은 사용되지 않습니다.	장치 ID에 연결된 등록 모드를 사용합니다. Active Directory 그룹 구성원 자격만 사용됩니다. 모든 사용자 배달 그룹은 사용되지 않습니다.

참고:

- 일반적으로, 미리 정의된 Active Directory 그룹의 사용자만 등록을 제한하는 것이 좋습니다. 그렇게 하려면 기본 제공되는 모든 사용자 배달 그룹을 사용하지 않도록 설정해야 합니다.
- 등록 초대를 사용하여 초대받은 사용자로 등록을 제한할 수 있습니다.
- OTP(일회용 PIN) 등록 초대를 2 단계 솔루션으로 사용하고 사용자가 등록할 수 있는 장치 수를 제어할 수 있습니다.
- 보안 수준이 가장 높은 환경의 경우 등록 초대를 SN/UDID/IMEI 로 장치에 연결할 수 있습니다. 2 단계 옵션을 사용하여 Active Directory 암호 및 OTP 를 요구할 수도 있습니다. (OTP 는 Windows 장치에서 지원되는 옵션이 아닙니다.)

장치 PIN 보안 고려 사항

다음 표에는 각 보안 수준에 대한 장치 PIN 권장 사항이 명시되어 있습니다.

높은 수준의 보안	더 높은 수준의 보안	최고 수준의 보안
권장. 장치 수 준 암호화에는 높은 수준의 보안이 필요합니다. MDM 을 통해 적용할 수 있습니다. MAM 전용 모드에서 MDX 정책을 사용하여 필수로 설정할 수 있습니다.	MDM 및/또는 MDX 정책을 사용하여 적용됩니다.	MDM 및 MDX 정책을 사용하여 적용됩니다. MDM 복잡한 암호 정책.

참고:

- Citrix 는 장치 PIN 의 사용을 권장합니다.
- 장치 PIN 은 MDM 정책을 통해 적용할 수 있습니다.
- 예를 들어 BYOD 사용 사례에서 MDX 정책을 사용하여 장치 PIN 을 관리되는 앱 사용을 위한 요구 사항 중 하나로 만들 수 있습니다.
- MDM 과 MDX 정책 옵션을 결합하여 MDM+MAM 환경의 보안을 강화하는 것이 좋습니다.
- 보안 요구 사항이 가장 높은 환경에서는 복잡한 암호 정책을 구성하고 MDM 을 통해 적용할 수 있습니다. 장치가 암호 정책을 준수하지 않는 경우 관리자에게 알리거나 선택적/전체 장치 초기화를 실행하는 자동화된 동작을 구성할 수 있습니다.

앱

January 6, 2020

EMM(엔터프라이즈모빌리티관리) 은 MDM(모바일기기관리) 과 MAM(모바일응용프로그램관리) 으로 나뉩니다. MDM 은 모바일 장치의 보안 및 제어에 사용되고 MAM 은 응용프로그램의 제공 및 관리를 용이하게 합니다. BYOD 채택이 증가하면 XenMobile 같은 MAM 솔루션을 구현하여 응용프로그램 제공, 소프트웨어 라이선스, 구성 및 응용 프로그램 수명 주기 관리를 지원할 수 있습니다.

XenMobile 을 사용하면 특정 MAM 정책 및 VPN 설정을 구성하여 데이터 유출 및 기타 보안 위협을 방지함으로써 이러한 앱을 추가로 보호할 수 있습니다. XenMobile 은 MAM 전용 또는 MDM 전용 환경으로 솔루션을 배포하거나 동일한 플랫폼에서 MDM 과 MAM 기능을 모두 제공하는 통합 XenMobile 엔터프라이즈 환경으로 구현할 수 있는 유연성을 제공합니다.

모바일 장치에 앱을 제공하는 것 외에도 XenMobile 은 MDX 기술을 통해 앱을 컨테이너화할 수 있는 기능을 제공합니다. MDX 는 장치 수준 암호화와 구분된 암호화를 통해 앱을 보호합니다. 앱을 초기화하거나 잠글 수 있으며 세분화된 정책 기반 제어가 앱에 적용됩니다. ISV(독립 소프트웨어 공급업체) 는 Worx App SDK 를 사용하여 이러한 제어를 적용할 수 있습니다.

기업 환경에서 사용자는 다양한 모바일 앱을 사용하여 업무를 지원합니다. 공용 앱스토어의 앱, 사내에서 개발한 앱 또는 일부 경우 기본 앱이 여기에 포함될 수 있습니다. XenMobile 은 이러한 앱을 다음과 같이 범주화합니다.

- **공용 앱:** iTunes 또는 Google Play 와 같은 공용 앱스토어에서 무료 또는 유료로 제공되는 앱이 포함됩니다. 조직 외부의 공급업체는 주로 공용 앱스토어를 통해 앱을 제공합니다. 이 옵션을 사용하는 경우 공급업체의 고객이 인터넷에서 직접 앱을 다운로드할 수 있습니다. 조직의 사용자는 사용자 요구 사항에 따라 수많은 공용 앱을 사용할 수 있습니다. 예를 들어 GoToMeeting, Salesforce 및 EpicCare 앱이 이러한 앱에 포함됩니다.

Citrix 는 공용 앱스토어에서 직접 앱을 다운로드한 다음 MDX Toolkit 을 사용하여 엔터프라이즈 배포용으로 래핑하는 것을 지원하지 않습니다. 타사 응용 프로그램을 래핑해야 하는 경우 앱 공급업체를 통해 MDX Toolkit 을 사용하여 래핑할 수 있는 앱을 받을 수 있습니다.

- **사내 앱:** 많은 조직이 사내 개발자를 통해 특정 기능을 제공하는 앱을 만듭니다. 사내 개발자는 조직 내에서 이러한 앱을 독립적으로 개발하고 배포합니다. 경우에 따라 일부 조직에서는 ISV 가 제공하는 앱을 사용하기도 합니다. 이러한 앱을 기본 앱으로 배포하거나 XenMobile 같은 MAM 솔루션을 사용하여 앱을 컨테이너화할 수 있습니다. 예를 들어 의료 조직에서는 의사가 모바일 장치에서 환자 정보를 볼 수 있도록 하는 사내 앱을 만들 수 있습니다. 그런 다음 MDX Toolkit 으로 앱을 래핑하여 환자 정보를 보호하고 백엔드 환자 데이터베이스 서버에 대한 VPN 액세스를 지원할 수 있습니다.
- **웹 및 SaaS 앱:** 내부 네트워크에서 액세스되는 앱 (웹 앱) 또는 공용 네트워크를 통해 액세스되는 앱 (SaaS) 이 포함됩니다. XenMobile 에서는 앱 커넥터 목록을 사용하여 사용자 지정 웹 및 SaaS 앱을 만들 수도 있습니다. 이러한 앱 커넥터를 사용하면 기존 웹 앱에 대한 SSO(Single Sign-on) 를 쉽게 구현할 수 있습니다. 자세한 내용은 [앱 커넥터 유형](#) 에서 참조하십시오. 예를 들어 Google Apps 에 대한 SAML(Security Assertion Markup Language) 기반 SSO 에는 Google Apps SAML 을 사용할 수 있습니다.
- **Citrix 모바일 생산성 앱:** Citrix 에서 개발한 앱으로, XenMobile 라이선스에 포함됩니다. 자세한 내용은 [모바일 생산성 앱 정보](#) 에서 참조하십시오. 또한 Citrix 는 다른 ISV 에서 Worx App SDK 를 사용하여 개발하는 다른 [비즈니스용 앱](#) 을 제공합니다.

- **HDX 앱:** Windows 에서호스트되는앱으로, StoreFront 를사용하여게시합니다. Citrix Virtual Apps and Desktops 환경이있는경우이러한앱을 XenMobile 과통합하여등록된사용자에게앱을제공할수있습니다.

XenMobile 을사용하여배포하고관리하려는모바일앱의유형에따라기본구성과아키텍처가달라집니다. 예를들어권한수준이서로 다른여러사용자그룹이단일앱을사용하려는경우개별배달그룹을만들어동일한앱의두가지개별버전을배포할수있습니다. 또한사용자장치에서정책불일치가발생하지않도록사용자그룹구성원자격이상호배타적인지확인해야합니다.

또한 Apple iOS VPP(Volume Purchase Program) 를사용하여 iOS 응용프로그램라이센스를관리해야할수있습니다. 이 옵션을사용하려면 VPP 프로그램에등록하고 XenMobile 콘솔에서 VPP 라이선스를사용하여앱을배포하도록 XenMobile VPP 설정을구성해야합니다. 이와같은다양한활용사례에서는 XenMobile 환경을구현하기전에 MAM 전략을평가하고계획하는 것이중요합니다. MAM 전략을계획하려면먼저다음을정의합니다.

- 앱유형 - 지원하려는서로다른유형의앱을나열하고공용, 기본, Worx, 웹, 사내, ISV 앱및기타등으로앱을범주화합니다. 또한서로다른장치플랫폼 (예: iOS 및 Android) 에대한앱을범주화합니다. 범주화는각앱유형에필요한서로다른 XenMobile 설정을조정하는데유용합니다. 예를들어특정앱에는래핑을사용할수없으며일부앱의경우 Worx App SDK 를사용하여다른앱과의상호작용을위한특수 API 를사용하도록설정해야할수있습니다.
- 네트워크요구사항 - 특정네트워크액세스요구사항및적절한설정으로앱을구성해야합니다. 예를들어특정앱은 VPN 을통해 내부네트워크에액세스해야하고다른앱은 DMZ 를통해액세스를라우팅하기위해인터넷액세스가필요할수있습니다. 이러한앱이필요한네트워크에연결하려면다양한설정을적절히구성해야합니다. 앱별네트워크요구사항을정의하면아키텍처의사결정이조기에확정되므로전체구현프로세스가간소화됩니다.
- 보안요구사항 - XenMobile Server 를설치할때올바른구성을만들려면개별앱또는모든앱에적용되는보안요구사항을정의하는것이중요합니다. MDX 정책같은설정개별앱에적용되지만세션및인증설정은모든앱에적용되며일부앱에는특정암호화, 컨테이너화, 래핑, 암호화, 인증, 지오펀스, 암호또는데이터공유요구사항이포함될수있습니다. 이러한요구사항을사전에간략히정의하면배포가간소화됩니다. XenMobile 의보안에대한자세한내용은 [보안및사용자환경](#)을참조하십시오.
- 배포요구사항 - 정책기반배포를사용하면규정을준수하는사용자만게시된앱을다운로드하도록허용할수있습니다. 예를들어장치암호화를사용하거나, 관리되는장치이거나, 최소운영체제버전을충족하는장치에서만특정앱을다운로드할수있도록설정할수있습니다. 또한특정앱을회사사용자에게만제공할수있습니다. 이러한요구사항을사전에간략히정의해야적절한배포규칙또는동작을구성할수있습니다.
- 라이선스요구사항 - 앱관련라이선스요구사항을기록해야합니다. 이러한메모는라이선스사용현황을효과적으로관리하고, XenMobile 에서라이선스를용이하게하는특정기능을구성해야할지여부를결정하는데도움이됩니다. 예를들어 iOS 앱을배포하는경우사용자는앱이무료인지, 유료인지에관계없이 Apple 의앱라이선스요구사항에따라 iTunes 계정으로그인해야합니다. Apple VPP 에등록하면이러한앱을 XenMobile 을통해배포하고관리할수있습니다. VPP 를사용하면사용자가 iTunes 계정으로그인하지않고앱을다운로드할수있습니다. 또한 Samsung SAFE 및 Samsung KNOX 같은도구에는기능을배포하기전에완료해야하는특수한라이선스요구사항이있습니다.
- 블랙리스트/화이트리스트요구사항 - 특정앱의경우사용자의설치또는사용을전혀허용하지않을수있습니다. 블랙리스트를만들면규정위반이벤트가정의됩니다. 관리자는이러한규정위반이발생할경우트리거할정책을설정할수있습니다. 또한사용은허용되지만하나이상의이유로블랙리스트에포함되는앱이존재할수있습니다. 이경우관리자는화이트리스트에앱을추가하고, 앱을사용할수있지만필수앱은아님을표시할수있습니다. 또한새장치에미리설치된앱에는운영체제의일부는아니지만 자주사용되는앱이포함될수있습니다. 이러한앱은블랙리스트전략과상충할수있습니다.

사용사례

한의료조직에서 XenMobile 을배포하여모바일앱의 MAM 솔루션으로사용하려고합니다. 모바일앱은회사및 BYOD 사용자에게제공됩니다. IT 부서에서는다음앱을제공하고관리하기로결정합니다.

모바일생산성앱: Citrix 가제공하는 iOS 및 Android 앱입니다. 자세한내용은 [모바일생산성앱](#)에서참조하십시오.

Citrix Secure Hub: XenMobile 과통신하는모든모바일장치에사용되는클라이언트입니다. IT 부서에서는 Secure Hub 를통해보안설정, 구성및모바일앱을모바일장치에푸시합니다. Android 및 iOS 장치는 Secure Hub 를통해 XenMobile 에 등록됩니다.

Citrix Receiver: 모바일장치사용자가 Citrix Virtual Apps 로호스트된응용프로그램을열때사용하는모바일앱입니다.

GoToMeeting: 사용자가다른컴퓨터사용자, 고객, 클라이언트또는동료와인터넷을통해실시간으로만날수있도록하는온라인모임, 데스크톱공유및비디오컨퍼런스클라이언트입니다.

SalesForce1: Salesforce1 을사용하면사용자가모바일장치에서 Salesforce 에액세스하고모든 Salesforce 사용자에게대한통합환경에서모든 Chatter, CRM, 사용자지정앱및비즈니스프로세스를확인할수있습니다.

RSA SecurID: 2 단계인증을위한소프트웨어기반토큰입니다.

EpicCare 앱: 환자차트, 환자목록, 일정및메시징에대한액세스를보호하고이동중에액세스할수있도록하는의료기관종사자용앱입니다.

Haiku: iPhone 및 Android 폰용모바일앱입니다.

Canto: iPad 용모바일앱입니다.

Rover: iPhone 및 iPad 용모바일앱입니다.

HDX: Citrix Virtual Apps 를통해제공되는앱입니다.

- **Epic Hyperspace:** 전자의료기록관리를위한 Epic 클라이언트응용프로그램입니다.

ISV:

- **Vocera:** HIPAA 준수 VoIP(Voice-over IP) 및메시징모바일앱으로, iPhone 및 Android 스마트폰을통해시간과 장소에관계없이 Vocera 음성기술의이점을활용할수있도록합니다.

사내앱:

- **HCMail:** 암호화된메시지를작성하고, 내부메일서버의주소록을검색하고, 암호화된메시지를전자메일클라이언트를사용하여연락처로보내는데유용한앱입니다.

사내웹앱:

- **PatientRounding:** 여러부서에서환자건강정보를기록하는데사용되는웹응용프로그램입니다.
- **Outlook Web Access:** 웹브라우저를통해전자메일에액세스할수있습니다.
- **SharePoint:** 조직전체의파일및데이터공유에사용됩니다.

다음표에는 MAM 구성에필요한기본정보가나와있습니다.

앱이름	앱유형	MDX 래핑	iOS	Android
Secure Mail	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
Secure Web	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
Secure Notes	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
ShareFile	XenMobile App	아니요 (버전 10.4.1 이상의경우)	예	예
Secure Hub	공용앱	해당없음	예	예
Citrix Receiver	공용앱	해당없음	예	예
GoToMeeting	공용앱	해당없음	예	예
SalesForce1	공용앱	해당없음	예	예
RSA SecurID	공용앱	해당없음	예	예
Epic Haiku	공용앱	해당없음	예	예
Epic Canto	공용앱	해당없음	예	아니요
Epic Rover	공용앱	해당없음	예	아니요
Epic Hyperspace	HDX 앱	해당없음	예	예
Vocera	ISV 앱	예	예	예
HCMail	사내앱	예	예	예
PatientRounding	웹앱	해당없음	예	예
Outlook Web Access	웹앱	해당없음	예	예
SharePoint	웹앱	해당없음	예	예

다음표에는 XenMobile 에서 MAM 정책을구성할때참조할수있는특정요구사항이나와있습니다.

앱 이름	VPN 필요	상호작용 (컨텐츠)	상호작용 (컨텐츠)	장치암호화	프록시 필터링	라이센스	지오편스	Worx App SDK	최소 운영체제 버전
Secure Mail	예	선택적으로 허용	허용	필요없음	필수	해당없음	선택적으로 필요	해당없음	적용
Secure Web	예	허용	허용	필요없음	필수	해당없음	필요없음	해당없음	적용
Secure Notes	예	허용	허용	필요없음	필수	해당없음	필요없음	해당없음	적용
ShareFile	예	허용	허용	필요없음	필수	해당없음	필요없음	해당없음	적용
Secure Hub	예	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
Citrix Receiver	예	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
GoToMeeting	아니요	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
SalesForce	아니요	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
RSA SecurID	아니요	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
Epic Haiku	예	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
Epic Canto	예	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
Epic Rover	예	해당없음	해당없음	해당없음	필요없음	VPP	필요없음	해당없음	적용되지 않음
Epic Hyper-space	예	해당없음	해당없음	해당없음	필요없음	해당없음	필요없음	해당없음	적용되지 않음

앱이름	VPN 필요	상호작용 (컨텐츠)	상호작용 (컨텐츠)	장치암호화	프록시 필터링	라이센스	지오펀스	Worx App SDK	최소 운영체제 버전
Vocera	예	허용되지 않음	허용되지 않음	필요없음	필수	해당없음	필수	필수	적용
HCMail	예	허용되지 않음	허용되지 않음	필수	필수	해당없음	필수	필수	적용
PatientRound- ing	예	해당없음	해당없음	필수	필수	해당없음	필요없음	해당없음	적용되지 않음
Outlook Web Access	예	해당없음	해당없음	필요없음	필수	해당없음	필요없음	해당없음	적용되지 않음
SharePoint	예	해당없음	해당없음	필요없음	필수	해당없음	필요없음	해당없음	적용되지 않음

사용자커뮤니티

January 6, 2020

모든 조직은 서로 다른 기능적 역할로 운영되는 다양한 사용자 커뮤니티로 구성됩니다. 이러한 사용자 커뮤니티는 사용자 모바일 장치를 통해 제공되는 다양한 리소스를 사용하여 서로 다른 작업 및 사무 기능을 수행합니다. 사용자는 관리자가 제공한 모바일 장치를 사용하여 재택 근무를 하거나 원격 사무실에서 근무할 수 있습니다. 또는 개인 모바일 장치를 사용하여 특정 보안 규정 준수 규칙이 적용되는 도구에 액세스할 수 있습니다.

모바일 장치를 사용하는 사용자 커뮤니티가 많아지면 EMM(엔터프라이즈 모바일리티 관리) 유통해 데이터 유출을 방지하고 조직의 보안 제한을 시행해야 합니다. 관리자는 효율적이고 정교한 모바일 기기 관리를 위해 사용자 커뮤니티를 범주화할 수 있습니다. 이렇게 하면 사용자 리소스에 매핑하는 작업이 간소화되고 올바른 보안 정책을 해당하는 사용자에게 적용할 수 있습니다.

사용자 커뮤니티를 범주화하는 작업에는 다음과 같은 구성 요소가 사용됩니다.

- Active Directory OU(조직 구성 단위) 및 그룹

특정 Active Directory 보안 그룹에 추가된 사용자는 정책 및 리소스 (예: 앱) 를 받을 수 있습니다. Active Directory 보안 그룹에서 사용자를 제거하면 이전에 허용되었던 XenMobile 리소스에 대한 액세스 권한이 제거됩니다.

- XenMobile 로컬 사용자 및 그룹

Active Directory 에계정이없는사용자는로컬 XenMobile 사용자로만들수있습니다. 관리자는로컬사용자를 Active Directory 사용자와동일한방식으로배달그룹에추가하고리소스를프로비전할수있습니다.

- XenMobile 배달그룹

권한수준이서로다른여러사용자그룹이단일앱을사용하려는경우개별배달그룹을만들어야할수있습니다. 개별배달그룹을 사용하면동일한앱의두가지개별버전을배포할수있습니다.

- 배달그룹과사용자그룹매핑

Active Directory 그룹에대한배달그룹매핑은일대일또는일대다방식일수있습니다. 기본정책및앱을일대다배달그룹매핑에할당합니다. 기능별정책및앱을일대일배달그룹매핑에할당합니다.

- 배달그룹과애플리소스매핑

특정앱을각배달그룹에할당합니다.

- 배달그룹과 MDM 리소스매핑

앱및특정장치관리리소스를각배달그룹에할당합니다. 예를들어앱유형 (공용, HDX 및기타), 앱유형별특정앱리소스 (예: 장치정책및자동화동작) 를혼합하여배달그룹을구성합니다.

다음에는의료조직의사용자커뮤니티를 EMM 용으로분류하는방법을설명합니다.

사용사례

이예의의료조직은기술리소스및액세스권한을다수의사용자 (예: 네트워크및계열사직원및자원봉사자) 에게제공합니다. 조직은 EMM 솔루션을일반사용자에게만출하하기로선택했습니다.

이조직의사용자역할및기능은임상, 비밀상및계약업체를포함하는하위그룹으로나눌수있습니다. 선택한사용자집합에는회사모바일장치가제공되고다른사용자집합은개인장치 (BYOD) 에서제한된회사리소스에액세스할수있습니다. 적절한수준의보안제한을 적용하고데이터유출을방지하기위해조직은회사 IT 부서를통해등록된장치를관리하기로결정했습니다. 또한사용자는단일장치만등록할수있습니다.

다음섹션에는각하위그룹의역할및기능에대한개요가나와있습니다.

임상

- 간호사
- 의사 (진료의, 외과의등)
- 전문가 (영양사, 임상병리사, 마취의, 방사선사, 심장전문의, 종양전문의등)
- 외부의사 (직원이나닌의사및원격사무실에서근무하는근로자)
- 가정건강서비스 (환자의집을방문하여의사서비스를수행하는사무실및모바일근로자)
- 연구전문가 (6 개연구기관에서약물문제에대한답을찾는임상연구를수행하는지식근로자및고급사용자)
- 교육및훈련 (교육및훈련중인간호사, 의사및전문가)

비임상

- 공유서비스 (HR, 급여, 미지급금, 공급망서비스등다양한경영지원기능을수행하는사무실근로자)
- 의사서비스 (관리서비스, 분석및비즈니스인텔리전스, 비즈니스시스템, 클라이언트서비스, 재무, 관리되는치료관리, 환자 액세스솔루션, 매출주기솔루션등다양한건강관리, 관리서비스및비즈니스프로세스공급자솔루션을수행하는사무실근로자)
- 지원서비스 (복리후생관리, 임상통합, 커뮤니케이션, 보상및실적관리, 설비및부동산서비스, HR 기술시스템, 정보서비스, 내부감사및프로세스개선등다양한비임상기능을수행하는사무실근로자)
- 자선프로그램 (자선프로그램지원과관련된다양한기능을수행하는사무실및모바일근로자)

계약업체

- 제조업체및공급업체파트너 (내부에서근무하거나사이트간 VPN 을통해원격으로연결하여다양한비임상지원기능을제공)

이 조직에서는 위의 정보를 바탕으로 다음과 같은 엔터티를 만들었습니다. XenMobile 의 배달 그룹에 대한 자세한 내용은 XenMobile 제품설명서에서 [리소스배포](#)를 참조하십시오.

Active Directory OU(조직구성단위) 및 그룹

OU = XenMobile 리소스인 경우

- OU = 임상, 그룹 =
 - XM 간호사
 - XM 의사
 - XM 전문가
 - XM 외부의사
 - XM 가정건강서비스
 - XM 연구전문가
 - XM 교육및훈련
- OU = 비임상, 그룹 =
 - XM 공유서비스
 - XM 의사서비스
 - XM 지원서비스
 - XM 자선프로그램

XenMobile 로컬사용자및 그룹

그룹 = 계약업체인 경우, 사용자 =

- 공급업체 1
- 공급업체 2

- 공급업체 3
- ... 공급업체 10

XenMobile 배달그룹

- 임상간호사
- 임상 의사
- 임상전문가
- 임상외부의사
- 임상가정건강서비스
- 임상연구전문가
- 임상교육및훈련
- 비임상공유서비스
- 비임상의사서비스
- 비임상지원서비스
- 비임상자선프로그램

배달그룹과사용자그룹매핑

Active Directory 그룹	XenMobile 배달그룹
XM 간호사	임상간호사
XM 의사	임상 의사
XM 전문가	임상전문가
XM 외부의사	임상외부의사
XM 가정건강서비스	임상가정건강서비스
XM 연구전문가	임상연구전문가
XM 교육및훈련	임상교육및훈련
XM 공유서비스	비임상공유서비스
XM 의사서비스	비임상의사서비스
XM 지원서비스	비임상지원서비스
XM 자선프로그램	비임상자선프로그램

배달그룹과앱리소스매핑

	Secure Mail	Secure Web	Secure Notes	ShareFile	Receive	SalesFo	RSA Se-curlD	EpicCar Haiku	Epic Hy-per-space
임상간 호사	X	X	X	X					
임상의 사									
임상전 문가									
임상외 부의사	X		X	X					
임상가 정건강 서비스	X		X	X					
임상연 구전문 가	X		X	X					
임상교 육맞훈 련								X	X
비임상 공유서 비스								X	X
비임상 의사서 비스								X	X
비임상 지원서 비스	X		X	X				X	X
비임상 자선프 로그램	X		X	X				X	X

계약업체	X	X	X	X	X	X	X
------	---	---	---	---	---	---	---

배달그룹과 MDM 리소스매핑

	MDM: 암호정책	MDM: 장치제한	MDM: 자동화된동작	MDM: WiFi 정책
임상간호사				X
임상의사		X		
임상전문가				
임상외부의사				
임상가정건강서비스				
임상연구전문가				
임상교육및훈련				
비임상공유서비스				
비임상의사서비스				
비임상지원서비스				
비임상자선프로그램				
계약업체				X

참고및사전요구사항

- XenMobile 을초기구성하는동안모든사용자라는이름의기본배달그룹이만들어집니다. 이배달그룹을사용하는경우모든 Active Directory 사용자가 XenMobile 에등록할수있습니다.
- XenMobile 은요청이있을경우 LDAP 서버에대한동적연결을사용하여 Active Directory 사용자및그룹을동기화합니다.
- 사용자가 XenMobile 에서매핑되지않은그룹에포함되는경우해당사용자는등록할수없습니다. 마찬가지로사용자가여러 그룹의구성원인경우 XenMobile 은해당사용자를 XenMobile 에매핑된그룹의구성원으로범주화합니다.
- MDM 등록을필수로규정하려면 XenMobile 콘솔의 서버속성에서 등록필요옵션을 **True** 로설정합니다. 자세한내용은 [서버속성](#)에서참조하십시오.

- XenMobile 배달그룹에서 사용자그룹을 삭제하려면 SQL Server 데이터베이스의 `dbo.userlistgrps` 아래에서 항목을 삭제합니다.

주의:

이 동작을 수행하기 전에 XenMobile 및 데이터베이스의 백업을 만드십시오.

XenMobile 의 장치 소유권 정보

사용자 장치의 소유자에 따라 사용자를 그룹화할 수 있습니다. 장치 소유권에는 회사 소유 장치와 BYOD(Bring Your Own Device)라고 하는 사용자 소유 장치가 포함됩니다. XenMobile 콘솔의 설정 페이지에서 배포 규칙과 XenMobile 서버 속성을 사용하여 BYOD 장치의 네트워크 연결 방법을 제어할 수 있습니다. 배포 규칙에 대한 자세한 내용은 XenMobile 설명서에서 [리소스 배포](#) 문서를 참조하십시오. 서버 속성에 대한 자세한 내용은 이 안내서에서 [서버 속성](#)을 참조하십시오.

앱 액세스하려는 모든 BYOD 사용자에게 회사의 장치 관리에 대한 동의를 요구하도록 서버 속성을 설정할 수 있습니다. 또는 장치 관리를 요구하지 않고 회사 앱에 대한 액세스 권한을 제공할 수 있습니다.

서버 속성 **`wsapi.mdm.required.flag`** 를 **`true`** 로 설정하면 XenMobile 이 모든 BYOD 장치를 관리하며 등록을 거부하는 사용자는 앱 액세스가 거부됩니다. 엔터프라이즈 IT 팀이 보안을 강화하는 동시에 사용자에게 개선된 등록 경험을 제공해야 한다면 **`wsapi.mdm.required.flag`** 를 **`true`** 로 설정하는 것이 좋습니다.

`wsapi.mdm.required.flag` 를 기본 설정인 **`false`** 로 유지하면 사용자가 등록을 거부할 수 있습니다. 그러나 사용자는 장치에서 XenMobile Store 를 통해 앱 액세스할 수 있습니다. 장치 관리 없이 엔터프라이즈 앱 관리만으로도 개인 정보 보호, 법적 또는 규제 제한을 준수할 수 있는 환경에서는 **`wsapi.mdm.required.flag`** 를 **`false`** 로 설정하는 것이 좋습니다.

XenMobile 을 통해 관리되지 않는 장치의 사용자는 XenMobile Store 를 통해 앱을 설치할 수 있습니다. 선택적 초기화 또는 전체 초기화 같은 장치 수준 제어 대신 앱 정책을 사용하여 앱 액세스를 제어할 수 있습니다. 일부 정책 설정을 사용하려면 장치에서 주기적으로 XenMobile 서버에 연결하여 앱 실행이 허용되는지 여부를 확인해야 합니다.

전자 메일 전략

April 19, 2019

조직에서 모바일리티 관리 이니셔티브를 시행하는 주된 이유는 모바일 장치에서 전자 메일에 안전하게 액세스할 수 있도록 하기 위해서입니다. XenMobile 설계의 주요 구성 요소 중 하나는 올바른 전자 메일 전략을 결정하는 것입니다. XenMobile 은 보안, 사용자 환경 및 통합 요구 사항에 따라 다양한 사용 사례를 수용하는 다수의 옵션을 제공합니다. 이 문서에서는 클라이언트 선택부터 메일 트래픽 흐름에 이르는 올바른 솔루션을 선택하기 위한 일반적인 설계의 사결정 프로세스와 고려 사항에 대해 다룹니다.

전자 메일 클라이언트 선택

전체 전자 메일 전략을 설계할 때는 일반적으로 클라이언트를 가장 먼저 선택합니다. Citrix Secure Mail, 특정 모바일 플랫폼 운영 체제에 포함되는 기본 메일 또는 공용 앱 스토어를 통해 제공되는 타사 클라이언트를 포함하는 여러 클라이언트 중에서 선택할 수 있습니다. 요

구사항에 따라 단일 (표준) 클라이언트를 사용하여 사용자 커뮤니티를 지원하거나 클라이언트 조합을 사용해야 할 수 있습니다.

다음 표에는 사용 가능한 여러 클라이언트 옵션에 대한 간략한 설계 고려 사항이 나와 있습니다.

항목	Secure Mail	기본 (예: iOS Mail)	타사 메일 (예: TouchDown)
최소 XenMobile 버전	고급	MDM	MDM
구성	MDX 정책을 통해 구성된 Exchange 계정 프로필.	MDM 정책을 통해 구성된 Exchange 계정 프로필. Android 지원은 SAFE/KNOX, HTC 및 Android Enterprise 로 제한됩니다. 다른 모든 클라이언트는 타사 클라이언트로 간주됩니다.	일반적으로 사용자가 수동으로 구성해야 합니다. TouchDown 전용 MDM 정책을 통한 Exchange 계정 프로필 구성.
보안	설계 시부터 보안이 적용되어 가장 높은 수준의 보안을 제공합니다. 데이터 암호화 수준이 추가된 MDX 정책을 사용합니다. Secure Mail 은 MDX 정책을 통해 완벽하게 관리되는 앱입니다. Citrix PIN 을 사용하여 인증 계층을 추가합니다.	공급업체/앱 기능 집합에 따릅니다. 더 높은 수준의 보안을 제공합니다. 장치 암호화 설정을 사용합니다 (MDX 정책을 통한 보안 없음). 앱 액세스에 대해 장치 수준 인증을 사용합니다.	공급업체/앱 기능 집합에 따릅니다. 높은 수준의 보안을 제공합니다.
통합	기본적으로 관리되는 앱 (MDX) 과의 상호 작용을 허용합니다. Citrix Secure Web 을 사용하여 웹 URL 을 엽니다. 파일 저장 및 첨부 시 ShareFile 을 사용합니다. GoToMeeting 에 직접 참여하고 전화 접속합니다.	기본적으로 관리되지 않는 다른 앱 (비 MDX) 과의 상호 작용만 가능합니다.	기본적으로 관리되지 않는 다른 앱 (비 MDX) 과의 상호 작용만 가능합니다.
배포/라이선스	공용 앱 스토어에서 MDM 을 통해 직접 Secure Mail 을 푸시할 수 있습니다. XenMobile Advanced 및 Enterprise 라이선스에 포함됩니다.	플랫폼 운영 체제에 포함된 클라이언트 앱입니다. 추가 라이선스 요구 사항이 없습니다.	MDM 을 통해 엔터프라이즈 앱으로 푸시하거나 공용 앱 스토어에서 직접 푸시할 수 있습니다. 앱 공급업체에 따라 연결된 라이선스 모델/비용이 적용됩니다.

지원	클라이언트 및 EMM 솔루션 을 단일 공급업체 (Citrix) 가 지원합니다. Secure Hub/앱 디버그로깅 기능에 지원 연락처가 포함되어 있습 니다. 하나의 클라이언트만 지원하면 됩니다.	공급업체 (Apple/Google) 가정의 한 지원을 사용할 수 있습니다. 장치 플랫폼에 따라 여러 클라 이언트를 지원해야 할 수 있습 니다.	공급업체가 정의한 지원을 사 용할 수 있습니다. 모든 관리 되는 장치 플랫폼에서 타사 클 라이언트가 지원된다고 가정 하면 하나의 클라이언트만 지 원하면 됩니다.
----	---	--	--

메일 트래픽 흐름 및 필터링 고려 사항

이 섹션에서는 XenMobile 의 컨텍스트에서 메일 (ActiveSync) 트래픽의 흐름과 관련된 세 가지 주요 시나리오 및 설계 고려 사항에 대해 설명합니다.

시나리오 1: 공개된 Exchange

일반적으로 Exchange ActiveSync 서비스를 인터넷에 공개하는 외부 클라이언트를 지원하는 환경입니다. 모바일 ActiveSync 클라이언트는 이 외부 대상 경로를 통해 역방향 프록시 (예: NetScaler) 또는 에지 서버를 사용하여 연결합니다. 이 옵션은 기본 또는 타사 메일 클라이언트를 사용하려는 경우 필요하며 이 시나리오에서 이러한 클라이언트가 주로 사용될 수도 있습니다. 일반적인 사례는 아니지만 이 시나리오에서 Secure Mail 클라이언트를 사용할 수도 있습니다. 이 경우 앱의 MDX 정책 및 관리를 통해 제공되는 보안 기능을 활용할 수 있습니다.

시나리오 2: NetScaler 를 통해 터널링됨 (Micro VPN 및 STA)

Secure Mail 클라이언트를 사용하는 경우 Micro VPN 기능을 사용하려면 이 시나리오가 기본적으로 적용됩니다. 이 경우 Secure Mail 클라이언트는 NetScaler Gateway 를 통해 ActiveSync 에 대한 보안 연결을 설정합니다. 기본적으로, Secure Mail 은 내부 네트워크에서 ActiveSync 에 직접 연결하는 클라이언트로 간주될 수 있습니다. Citrix 고객은 Secure Mail 을 모바일 ActiveSync 클라이언트로 표준화하는 경우가 많습니다. 이러한 표준화는 첫 번째 시나리오에 설명된 것과 같이 공개된 Exchange Server 에서 ActiveSync 서비스가 인터넷에 공개되는 것을 방지하기 위해 수행됩니다.

관리되는 앱 (MDX 래핑 앱) 만 Micro VPN 기능을 사용할 수 있습니다. 따라서 기본 클라이언트에는 이 시나리오가 적용되지 않습니다. 타사 클라이언트를 MDX Toolkit 으로 래핑할 수도 있지만 일반적인 사례는 아닙니다. 장치 수준 VPN 클라이언트를 사용하여 기본 또는 타사 클라이언트에 대한 터널링된 액세스를 허용하려는 솔루션은 과정이 복잡하고 실행 가능하지 않은 것으로 검증되었습니다.

시나리오 3: 클라우드에서 호스팅되는 Exchange 서비스

클라우드에서 호스팅되는 Exchange 서비스 (예: Microsoft Office 365) 의 인기가 높아지고 있습니다. XenMobile 의 컨텍스트에서 이 시나리오는 첫 번째 시나리오와 동일하게 다루어질 수 있습니다. ActiveSync 서비스가 인터넷에 공개되기 때문입니다. 이

경우클라우드서비스공급자요구사항에따라클라이언트를선택해야합니다. 일반적으로대부분의 ActiveSync 클라이언트 (예: Secure Mail) 및다른기본또는타사클라이언트를선택할수있습니다.

XenMobile 은이시나리오의세가지영역에서더많은가치를제공합니다.

- Secure Mail 의 MDX 정책및앱관리를통한클라이언트래핑
- MDM 정책및지원되는클라이언트 (TouchDown 같은기본클라이언트) 를사용하여클라이언트구성
- Exchange ActiveSync 용 Endpoint Management 커넥터를사용한 ActiveSync 필터링업선

메일트래픽필터링고려사항

인터넷에공개되는대부분의서비스와 마찬가지로, 경로를보호하고허가된액세스에대한필터링을제공해야합니다. XenMobile 솔루션에는기본및타사클라이언트를위한 ActiveSync 필터링기능을제공하도록설계된두가지구성요소가포함되어있습니다. Exchange ActiveSync 용 Citrix Gateway 커넥터와 Exchange ActiveSync 용 Endpoint Management 커넥터입니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터

Exchange ActiveSync 용 Citrix Gateway 커넥터를사용하면 NetScaler 를 ActiveSync 트래픽의프록시로사용하여경계에서 ActiveSync 필터링을제공할수있습니다. 필터링구성요소가메일트래픽흐름의경로에배치되므로메일이환경에들어오거나환경에서나갈때트래픽을가로칩니다. Exchange ActiveSync 용 Citrix Gateway 커넥터는 NetScaler 와 XenMobile Server 의중간자역할을합니다. 장치가 NetScaler 의 ActiveSync 가상서버를통해 Exchange 와통신하면 NetScaler 가 Exchange ActiveSync 용커넥터서비스에대한 HTTP 콜아웃을수행합니다. 그러면이서비스가 XenMobile 을통해장치상태를확인합니다. 장치상태에따라 Exchange ActiveSync 용커넥터는연결허용또는거부에대한회신을 NetScaler 을보냅니다. 사용자, 에이전트및장치유형또는 ID 에따라액세스를필터링하는정적규칙을구성할수도있습니다.

이설정을사용하면추가보안계층을통해 Exchange ActiveSync 서비스를인터넷에공개하여허가되지않은액세스를방지할수있습니다. 설계고려사항은다음과같습니다.

- Windows Server: Exchange ActiveSync 용커넥터구성요소를사용하려면 Windows Server 가필요합니다.
- 필터링규칙설정: Exchange ActiveSync 용커넥터는사용자정보가아닌장치상태및정보를바탕으로필터링하도록설계되었습니다. 사용자 ID 로필터링하는정적규칙을구성할수있지만예를들어 Active Directory 그룹구성원자격으로필터링하는옵션은없습니다. Active Directory 그룹필터링에대한요구사항이있는경우 Exchange ActiveSync 용 Endpoint Management 커넥터를대신사용할수있습니다.
- NetScaler 확장성: NetScaler 를통한 ActiveSync 트래픽프록시에대한요구사항이있는경우 NetScaler 인스턴스 크기를올바르게조정하여모든 ActiveSync SSL 연결의추가된작업부하를지원하는것이중요합니다.
- NetScaler 통합캐싱: NetScaler 의 Exchange ActiveSync 용커넥터구성은통합캐싱기능을사용하여 Exchange ActiveSync 용커넥터의응답을캐싱합니다. 이구성으로인해 NetScaler 는지정된세션의모든 ActiveSync 트랜잭션에대한요청을 Exchange ActiveSync 용 Citrix Gateway 커넥터에전송하지않아도됩니다. 이구성은충분한성능및확장성에대해서도중요한역할을합니다. 통합캐싱은 NetScaler Platinum Edition 을통해사용하거나 Enterprise Edition 의기능에대한라이센스를개별적으로취득할수있습니다.

- 사용자지정필터링정책: 사용자지정 NetScaler 정책을만들어표준의기본모바일클라이언트외의특정 ActiveSync 클라이언트를제한해야할수있습니다. 이구성을사용하려면 ActiveSync HTTP 요청및 NetScaler 응답자정책만들기에대한지식이있어야합니다.
- Secure Mail 클라이언트: Secure Mail 에는 Micro VPN 기능이있습니다. 이기능을사용하면경계에서필터링을수행하지않아도됩니다. Secure Mail 클라이언트는 NetScaler Gateway 를통해연결되는경우일반적으로내부 (신뢰할수있는) ActiveSync 클라이언트로서여겨집니다. 기본및타사 (Exchange ActiveSync 용커넥터포함) 클라이언트와 Secure Mail 클라이언트를모두지원해야합니다. Secure Mail 트래픽은 Exchange ActiveSync 용커넥터에서사용된 NetScaler 가상서버를통하지않는것이 좋습니다. 이트래픽이 DNS 를통해흐르도록하고 Exchange ActiveSync 용커넥터정책이 Secure Mail 클라이언트에영향을미치지않도록할수있습니다.

XenMobile 배포의 Exchange ActiveSync 용 Citrix Gateway 커넥터 다이어그램은 [온-프레미스배포용참조아키텍처](#)를 참조하십시오.

Exchange ActiveSync 용 Endpoint Management 커넥터

Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange 서비스수준에서 ActiveSync 필터링을제공하는 XenMobile 구성요소입니다. 따라서메일이 XenMobile 환경에들어올때가아니라 Exchange 서비스에도달할때만필터링이한번수행됩니다. Mail Manager 은 PowerShell 을사용하여 Exchange ActiveSync 에장치파트너관계정보를쿼리하고장치격리동작을통해액세스를제어합니다. 이러한동작은 Exchange ActiveSync 용 Endpoint Management 커넥터규칙기준에따라장치를격리하거나격리해제합니다. Exchange ActiveSync 용 Citrix Gateway 커넥터와 마찬가지로 Exchange ActiveSync 용 Endpoint Management 커넥터는 XenMobile 을통해장치상태를확인하여장치규정준수에따라액세스를필터링합니다. 장치유형또는 ID, 에이전트버전및 Active Directory 그룹구성원자격에따라액세스를필터링하는정적규칙을구생할수도있습니다.

이솔루션에는 NetScaler 의사용이필요하지않습니다. 기존 ActiveSync 트래픽의라우팅을변경하지않고 Exchange ActiveSync 용 Endpoint Management 커넥터를배포할수있습니다. 설계고려사항은다음과같습니다.

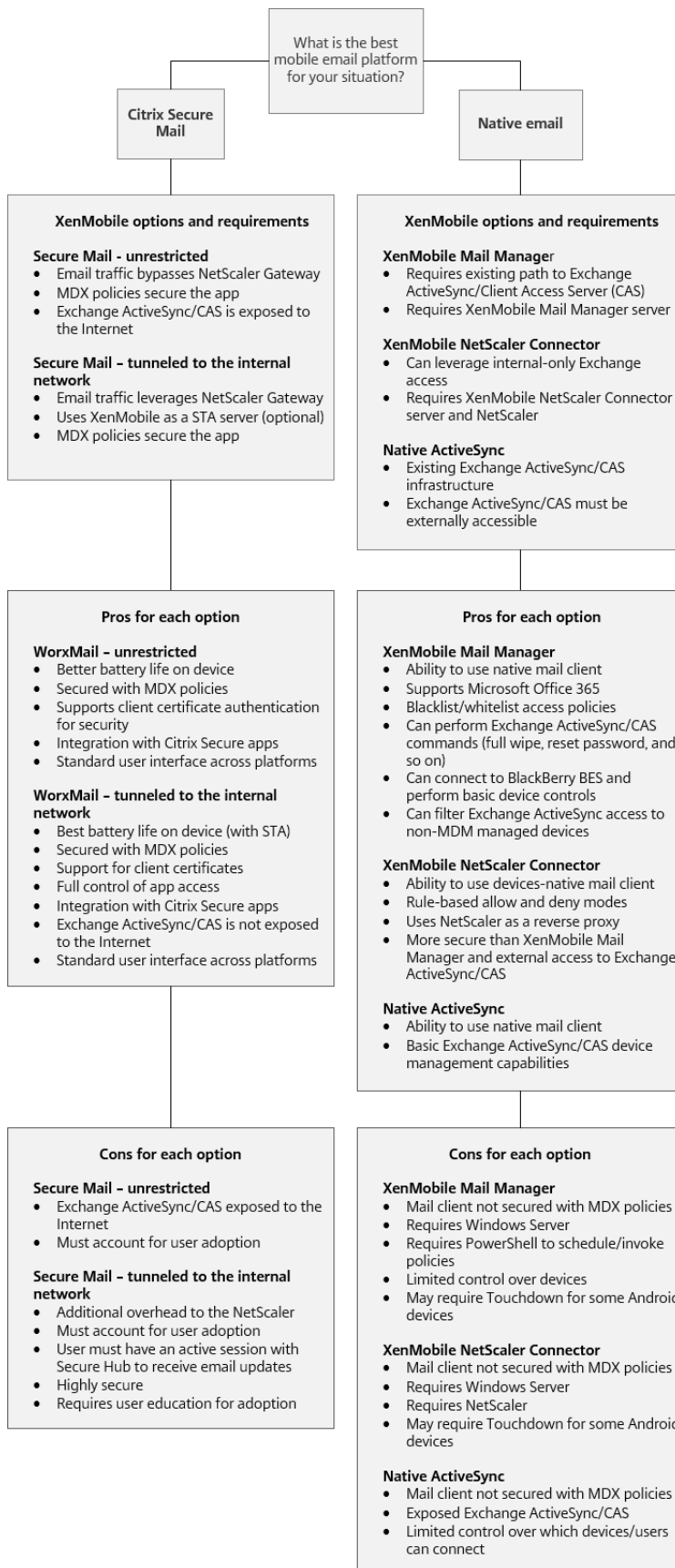
- Windows Server: Exchange ActiveSync 용 Endpoint Management 커넥터구성요소를사용하려면 Windows Server 를배포해야합니다.
- 필터링규칙설정: Exchange ActiveSync 용 Citrix Gateway 커넥터와 마찬가지로 Exchange ActiveSync 용 Endpoint Management 커넥터에는장치상태를평가하는필터링규칙이포함됩니다. 또한 Exchange ActiveSync 용 Endpoint Management 커넥터는 Active Directory 그룹구성원자격을기준으로필터링하는정적규칙을지원합니다.
- Exchange 통합: Exchange ActiveSync 용 Endpoint Management 커넥터는 ActiveSync 역할을호스팅하는 Exchange CAS(클라이언트액세스서버) 에직접액세스하고장치격리동작을제어할수있어야합니다. 이요구사항은환경아키텍처및보안상태에따라문제가될수있습니다. 따라서이기술요구사항을사전에평가하는것이중요합니다.
- 다른 ActiveSync 클라이언트: Exchange ActiveSync 용 Endpoint Management 커넥터는 ActiveSync 서비스수준에서필터링을수행하므로 XenMobile 환경외의다른 ActiveSync 클라이언트를고려해야합니다. Exchange ActiveSync 용 Endpoint Management 커넥터정적규칙을구성하면다른 ActiveSync 클라이언트에의도하지않은영향이발생하는것을방지할수있습니다.
- 확장된 Exchange 기능: Exchange ActiveSync 와 Exchange ActiveSync 용 Endpoint Management 커

넥터를 직접 통합하면 XenMobile 이모바일장치에서 Exchange ActiveSync 초기화를 수행할 수 있습니다. 또한 XenMobile 은 Exchange ActiveSync 용 Endpoint Management 커넥터를 통해 Blackberry 장치에 대한 정보에 액세스하고 다른 제어 작업을 수행할 수 있습니다.

XenMobile 배포의 Exchange ActiveSync 용 Endpoint Management 커넥터 다이어그램은 [온-프레미스 배포용 참조아키텍처](#)를 참조하십시오.

전자메일 플랫폼의 사결정 트리

다음 그림은 XenMobile 배포에서 기본 전자메일과 Secure Mail 솔루션을 사용할 때의 장점과 단점을 이해하는데 도움이 됩니다. 연결된 XenMobile 옵션과 서버, 네트워크 및 데이터베이스 액세스 지원을 위한 요구사항을 고려하여 솔루션을 선택할 수 있습니다. 장점 및 단점에는 보안, 정책 및 사용자 인터페이스 고려사항에 대한 세부 정보가 포함됩니다.



XenMobile 통합

January 6, 2020

이 문서에서는 XenMobile 과 기존 네트워크 및 솔루션의 통합을 계획할 때 고려해야 할 사항에 대해 다룹니다. 예를 들어 Virtual Apps and Desktops 에 NetScaler 를 사용 중인 경우 다음을 고려해야 할 수 있습니다.

- 기존 NetScaler 인스턴스를 사용해야 하나? 새로운 전용 인스턴스를 사용해야 하나?
- StoreFront 를 사용하여 게시된 HDX 앱을 XenMobile 과 통합하려고 하나?
- XenMobile 에서 ShareFile 을 사용할 계획입니까?
- XenMobile 에 통합하려는 네트워크 액세스 제어 솔루션이 있습니까?
- 네트워크의 모든 아웃바운드 트래픽에 대한 웹 프록시를 배포 하나?

NetScaler 및 NetScaler Gateway

XenMobile ENT 및 MAM 모드에는 NetScaler Gateway 가 필요합니다. NetScaler Gateway 는 모든 회사 리소스에 액세스할 수 있는 Micro VPN 경로를 제공하며 강력한 다중 단계 인증을 지원합니다. 다음의 경우 모든 XenMobile Server 장치 모드에 NetScaler 부하 분산이 필요합니다.

- 다수의 XenMobile Server 가 있는 경우.
- XenMobile Server 가 DMZ 또는 내부 네트워크에 있는 경우 (트래픽이 장치에서 NetScaler 를 거쳐 XenMobile 로 흐르는 경우).

기존 NetScaler 인스턴스를 사용하거나 XenMobile 전용의 새 인스턴스를 설정할 수 있습니다. 다음 섹션에서는 기존 NetScaler 인스턴스 또는 새로운 전용 NetScaler 인스턴스를 사용할 때의 장점과 단점을 살펴봅니다.

XenMobile 용으로 만든 NetScaler Gateway VIP 를 통해 NetScaler MPX 공유

장점:

- 모든 Citrix 원격 연결 (Citrix Virtual Apps and Desktops, 전체 VPN 및 클라이언트 없는 VPN) 에 공통된 NetScaler 인스턴스를 사용합니다.
- 인증서 인증 및 DNS, LDAP 및 NTP 같은 서비스 액세스 시 기존 NetScaler 구성을 사용합니다.
- 단일 NetScaler 플랫폼 라이선스를 사용합니다.

단점:

- 동일한 NetScaler 에서 두 개의 아주 다른 사용 사례를 처리하는 경우 확장을 계획하기가 더 어렵습니다.
- 가끔, Citrix Virtual Apps and Desktops 사용 사례에 대한 특정 NetScaler 버전이 필요할 수 있습니다. 이러한 버전에는 XenMobile 의 알려진 문제가 포함될 수 있습니다. 또는 XenMobile 에 NetScaler 버전의 알려진 문제가 포함될 수 있습니다.
- NetScaler Gateway 가 있는 경우 XenMobile 에 대한 NetScaler 구성을 만들 때 XenMobile 용 NetScaler 마법사를 두 번 실행할 수 없습니다.

- NetScaler Gateway 11.1 이상에서 Platinum 라이선스를 사용하는 경우를 제외하고 NetScaler 에 설치되고 VPN 연결에 필요한 사용자 액세스 라이선스가 풀링됩니다. 모든 NetScaler 가상 서버에서 이러한 라이선스를 사용할 수 있으므로 XenMobile 외의 다른 서비스에 의해 라이선스가 소비될 수 있습니다.

전용 NetScaler VPX/MPX 인스턴스

장점:

Citrix 는 전용 NetScaler 인스턴스를 사용할 것을 권장합니다.

- 확장을 계획하기가 쉽고 XenMobile 트래픽이 이미 리소스 제약이 있을 수 있는 NetScaler 인스턴스와 분리됩니다.
- XenMobile 과 Citrix Virtual Apps and Desktops 에서 서로 다른 NetScaler 소프트웨어 버전을 사용해야 하는 경우 문제가 방지됩니다. XenMobile 과 호환되는 최신 NetScaler 버전 및 빌드를 사용하는 것이 일반적으로 권장됩니다.
- 기본 제공되는 XenMobile 용 NetScaler 마법사를 통해 XenMobile 에 사용할 NetScaler 를 구성할 수 있습니다.
- 가상 서비스와 물리적 서비스가 분리됩니다.
- NetScaler Gateway 11.1 이상에서 Platinum 라이선스를 사용하는 경우를 제외하고 XenMobile 에 필요한 사용자 라이선스가 NetScaler 의 XenMobile 서비스에만 제공됩니다.

단점:

- NetScaler 에서 XenMobile 구성을 지원하는 추가 서비스를 설정해야 합니다.
- 다른 NetScaler 플랫폼 라이선스가 필요합니다. 각 NetScaler 인스턴스에 NetScaler Gateway 라이선스가 필요합니다.

NetScaler 및 NetScaler Gateway 를 XenMobile 서버 모드와 통합할 때의 고려 사항에 대한 자세한 내용은 [NetScaler 및 NetScaler Gateway 통합](#)을 참조하십시오.

StoreFront

Citrix Virtual Apps and Desktops 환경이 있는 경우 StoreFront 를 사용하여 HDX 응용 프로그램을 XenMobile 과 통합할 수 있습니다. HDX 앱을 XenMobile 과 통합하는 경우:

- XenMobile 에 등록된 사용자가 앱을 사용할 수 있습니다.
- XenMobile Store 에 다른 모바일 앱과 함께 앱이 표시됩니다.
- XenMobile 이 StoreFront 의 레거시 PNAgent(서비스) 사이트를 사용합니다.
- Citrix Receiver 가 장치에 설치된 경우 HDX 앱이 Citrix Receiver 사용을 시작합니다.

StoreFront 에는 StoreFront 인스턴스 당 하나의 서비스 사이트를 사용해야 하는 제한이 있습니다. 여러 저장소가 있고 이러한 저장소를 다른 프로젝트 사용과 구분해야 하는 경우 XenMobile 에 사용할 새 StoreFront 인스턴스 및 서비스 사이트를 만드는 것이 좋습니다.

고려 사항은 다음과 같습니다.

- StoreFront 에대한특정인증요구사항이있습니까? StoreFront 서비스사이트에로그온하려면 Active Directory 자격증명이필요합니다. 인증서기반인증만사용하는고객은동일한 NetScaler Gateway 를사용하는 XenMobile 을통해 응용프로그램을열거할수없습니다.
- 동일한저장소를사용합니까? 새저장소를만듭니까?
- 동일한 StoreFront 서버를사용합니까? 새 StoreFront 서버를사용합니까?

다음섹션에서는 Receiver 및모바일생산성앱에대해개별 StoreFront 또는결합된 StoreFront 를사용할때의장점과단점을살펴봅니다.

기존 **StoreFront** 인스턴스를 **XenMobile** 서버와통합

장점:

- 동일한저장소: 동일한 NetScaler VIP 를 HDX 액세스에사용하는것으로가정할경우 XenMobile 용 StoreFront 를 추가로구성할필요가없습니다. 동일한저장소를사용하고 Receiver 액세스를새 NetScaler VIP 로연결한다고가정하면 적절한 NetScaler Gateway 구성을 StoreFront 에추가해야합니다.
- 동일한 StoreFront 서버: 기존 StoreFront 설치및구성을사용합니다.

단점:

- 동일한저장소: Virtual Apps and Desktops 작업부하를지원하기위해 StoreFront 를재구성할경우 XenMobile 에도부정적인영향이발생할수있습니다.
- 동일한 StoreFront 서버: 대규모환경의경우 XenMobile 에서앱을열거하고시작할때 PNAgent 를사용하므로추가부하가발생할수있습니다.

XenMobile 서버통합에새로운전용 **StoreFront** 인스턴스사용

장점:

- 새저장소: XenMobile 의 StoreFront 저장소에대한구성변경이 기존 Virtual Apps and Desktops 작업부하에영향을미치지않습니다.
- 새 StoreFront 서버: 서버구성변경이 Virtual Apps and Desktops 워크플로에영향을미치지않습니다. 또한 XenMobile 에서 PNAgent 를사용하여앱을열거하고시작할때발생하는부하외의부하가확장성에영향을미치지않습니다.

단점:

- 새저장소: StoreFront 저장소구성.
- 새 StoreFront 서버: 새 StoreFront 설치및구성이필요합니다.

자세한내용은 XenMobile 설명서에서 [Citrix Secure Hub](#) 를 통한 [Virtual Apps and Desktops](#) 을 참조하십시오.

ShareFile

사용자는 ShareFile 을 사용하여 모든 장치의 모든 데이터에 액세스하고 동기화할 수 있습니다. ShareFile 을 사용하면 조직 내부 및 외부 사용자와 안전하게 데이터를 공유할 수 있습니다. ShareFile 을 XenMobile Advanced Edition 또는 Enterprise Edition 과 통합하면 XenMobile 을 통해 ShareFile 에 다음을 제공할 수 있습니다.

- XenMobile App 사용자의 SSO(Single Sign-on) 인증.
- Active Directory 기반 사용자 계정 프로비전.
- 포괄적인 액세스 제어 정책.

모바일 사용자는 모든 ShareFile Enterprise 기능 집합을 사용할 수 있습니다.

또는 StorageZone 커넥터만 통합하도록 XenMobile 을 구성할 수 있습니다. StorageZone 커넥터를 사용하면 ShareFile 에서 다음에 액세스할 수 있습니다.

- 문서 및 폴더
- 네트워크 파일 공유
- SharePoint 사이트: 사이트 모음 및 문서 라이브러리.

연결된 파일 공유에는 Citrix Virtual Apps and Desktops 환경에 사용된 것과 동일한 네트워크 드라이브가 포함될 수 있습니다. XenMobile 콘솔을 사용하여 ShareFile Enterprise 또는 StorageZones 커넥터와의 통합을 구성할 수 있습니다. 자세한 내용은 [XenMobile](#) 에서 [ShareFile 사용](#) 에서 참조하십시오.

다음 섹션에서는 ShareFile 에 대한 설계의사 결정을 내릴 때 고려할 수 있는 질문을 살펴봅니다.

ShareFile Enterprise 통합 또는 StorageZone 커넥터만 통합

질문:

- Citrix 에서 관리하는 StorageZones 에 데이터를 저장해야 하나요?
- 사용자에게 파일 공유 및 동기화 기능을 제공하려고 하나요?
- 사용자가 ShareFile 웹사이트의 파일에 액세스할 수 있어야 하나요? 또는 모바일 장치에서 Office 365 콘텐츠 및 개인용 클라우드 커넥터에 액세스해야 하나요?

설계의사 결정:

- 위 질문 중 하나 이상에 대한 답이 “예” 인 경우 ShareFile Enterprise 와 통합합니다.
- StorageZone 커넥터만 통합하는 경우 SharePoint 사이트 및 네트워크 파일 공유 등의 기존 온-프레미스 스토리지 저장소에 대한 보안 모바일 액세스를 iOS 사용자에게 제공할 수 있습니다. 이 구성에서는 ShareFile 하위 도메인을 설정하거나 사용자를 ShareFile 에 프로비전하거나 ShareFile 데이터를 호스팅하지 않습니다. StorageZones 커넥터를 XenMobile 과 함께 사용하면 사용자 정보가 회사 네트워크 밖으로 유출되지 않도록 하는 보안 제한 사항을 준수할 수 있습니다.

ShareFile StorageZones Controller 서버 위치

질문:

- 온-프레미스스토리지또는기능 (예: StorageZone 커넥터) 이필요합니까?
- ShareFile 의온-프레미스기능을사용하는경우 ShareFile StorageZones Controller 는네트워크의어디에위치합니까?

설계의사결정:

- StorageZones Controller 서버의위치 (ShareFile 클라우드, 온-프레미스단일테넌트스토리지시스템또는지원되는 타사클라우드스토리지) 를결정합니다.
- StorageZones Controller 를사용하려면인터넷엑세스를통해 Citrix ShareFile 제어부와통신해야합니다. 직접엑세스, NAT/PAT 구성또는프록시구성등다양한방법으로연결할수있습니다.

StorageZone 커넥터

질문:

- CIFS 공유경로는무엇입니까?
- SharePoint URL 은무엇입니까?

설계의사결정:

- 온-프레미스 StorageZones Controller 에서이러한위치에엑세스해야하는지여부를결정합니다.
- StorageZone 커넥터에서파일저장소, CIFS 공유및 SharePoint 같은내부리소스와통신해야하므로 StorageZones Controller 를내부네트워크의 DMZ 방화벽뒤와 NetScaler 앞에배치하는것이 좋습니다.

SAML 과 XenMobile Enterprise 통합

질문:

- ShareFile 에 Active Directory 인증이필요합니까?
- XenMobile 용 ShareFile 앱을처음으로사용할때 SSO 가필요합니까?
- 현재환경에표준 IdP 가있습니까?
- SAML 을사용해야하는도메인은몇개입니까?
- Active Directory 사용자에대한전자메일별칭이여러개입니까?
- Active Directory 도메인마이그레이션이진행중이거나곧예약되어있습니까?

설계의사결정:

XenMobile Enterprise 환경에서는 SAML 을 ShareFile 의인증메커니즘으로사용할수있습니다. 인증옵션은다음과같습니다.

- XenMobile 서버를 SAML 의 IdP(ID 공급자) 로사용합니다.

이옵션을사용하면사용자환경을향상하고 ShareFile 계정생성을자동화하는동시에모바일앱 SSO 기능을지원할수있습니다.

- XenMobile 서버에서이프로세스가향상되며 Active Directory 동기화가필요하지않습니다.
- ShareFile 사용자관리도구를사용자프로비전에서사용합니다.

- 지원되는타사공급업체를 SAML 의 IdP 로사용합니다.

기존의지원되는 IdP 가있고모바일앱 SSO 기능이필요하지않은경우이옵션이가장적합할수있습니다. 이옵션을사용하려면계정 프로비전에 ShareFile 사용자관리도구를사용해야합니다.

타사 IdP 솔루션 (예: ADFS) 을사용하는경우 Windows 클라이언트측에서 SSO 기능을사용할수도있습니다. ShareFile SAML IdP 를선택하기전에사용사례를평가하십시오.

또한두사용사례를모두충족하기위해 [ADFS 및 XenMobile 을이중 IDP 로구성](#)할수있습니다.

모바일앱

질문:

- 사용하려는 ShareFile Mobile 앱은무엇입니까 (공용, MDM, MDX)?

설계의사결정:

- Apple App Store 및 Google Play Store 로부터모바일생산성앱을배포할수있습니다. 공용앱스토어배포를사용하는경우 Citrix 다운로드페이지에서래핑된앱을받을수있습니다.
- 보안수준이낮고컨테이너화가필요하지않은경우공용 ShareFile 응용프로그램은적합하지않을수있습니다. MDM 전용 환경에서는 XenMobile 을 MDM 모드에서사용하여 ShareFile 앱의 MDM 버전을제공할수있습니다.
- 자세한내용은 [앱](#) 및 [Citrix ShareFile for XenMobile](#) 항목을참조하십시오.

보안, 정책및액세스제어

질문:

- 데스크톱, 웹및모바일사용자에게적용해야하는제한은무엇입니까?
- 사용자에게적용하려는표준액세스제어설정은무엇입니까?
- 사용하려는파일보존정책은무엇입니까?

설계의사결정:

- ShareFile 을사용하여직원권한및장치보안을관리할수있습니다. 자세한내용은 [직원권한](#) 및 [장치및앱관리](#)를참조하십시오.
- 일부 ShareFile 장치보안설정및 MDX 정책은동일한기능을제어합니다. 이러한경우 XenMobile 정책이우선하며 ShareFile 장치보안설정이그다음으로적용됩니다. 예: ShareFile 에서외부앱을사용하지않도록설정하고 XenMobile 에서사용하도록설정하면외부앱이 ShareFile 에서사용되지않습니다. XenMobile 에서는 PIN/암호를 사용하지않고 ShareFile 앱에서 PIN/암호를사용하도록앱을구성할수있습니다.

표준및제한된 **StorageZone**

질문:

- 제한된 StorageZone 이필요합니까?

설계의사결정:

- 표준 StorageZone 은중요하지않은데이터에서사용되며이를통해직원들은직원이외의사람들과데이터를공유할수있습니다. 이옵션은도메인외부의데이터공유와관련된위크플로를지원합니다.
- 제한된 StorageZone 은중요한데이터를보호합니다. 인증된도메인사용자만해당영역에서저장된데이터에액세스할수있습니다.

웹프록시

HTTP(S)/SOCKS 프록시를통해 XenMobile 트래픽을라우팅하는가장일반적인시나리오는 XenMobile 서버가상주하는서브넷에서아웃바운드인터넷엑세스를통해필요한 Apple, Google 또는 Microsoft IP 주소에엑세스할수없는경우입니다. XenMobile 에서모든인터넷트래픽을프록시서버로라우팅하도록프록시서버설정을지정할수있습니다. 자세한내용은 [프록시서버사용](#)에서참조하십시오.

다음표에서는 XenMobile 에서사용되는가장일반적인프록시의장점및단점에대해설명합니다.

옵션	장점	단점
XenMobile 서버에서 HTTP(S)/SOCKS 프록시를사용합니다.	정책이 XenMobile 서버서브넷의아웃바운드인터넷연결을허용하지않는경우 HTTP(S) 또는 SOCKS 프록시를구성하여인터넷연결을제공할수있습니다.	프록시서버가실패하면 APNs(iOS) 또는 Firebase Cloud Messaging(Android) 연결이끊깁니다. 그결과모든 iOS 및 Android 장치에대한장치알림이실패합니다.
Secure Web 에서 HTTP(S) 프록시를사용합니다.	HTTP/HTTPS 트래픽을모니터링하여인터넷활동이조직의표준을준수하는지확인할수있습니다.	이구성에서는모든 Secure Web 인터넷트래픽을회사네트워크로다시터널링한다음인터넷으로전송해야합니다. 회사의인터넷연결이브라우저를제한하는경우이구성이인터넷브라우저성능에영향을미칠수있습니다.

분할터널링에대한 NetScaler 세션프로필구성은트래픽에다음과같은영향을미칩니다.

NetScaler 분할터널링이 꺼짐인경우:

- MDX 네트워크엑세스정책이 내부네트워크로터널링된경우: 모든트래픽에 NetScaler Gateway 로다시터널링되는 Micro VPN 또는 cVPN(클라이언트없는 VPN) 터널이사용됩니다.
- 프록시서버에대한 NetScaler 트래픽정책/프로필을구성하고 NetScaler Gateway VIP 에정책을바인딩합니다.

중요:

Secure Hub cVPN 트래픽을프록시에서제외하십시오.

- 자세한내용은 [XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode\(Secure Browse 모드에서프록시서버를통한 XenMobile Secure Hub 트래픽\)](#)에서참조하십시오.

NetScaler 분할터널링이 켜짐인경우:

- MDX 네트워크 액세스정책이 내부네트워크로터널링됨으로구성된앱의경우: 앱이웹리소스에직접액세스를시도합니다. 웹 리소스가공개적으로제공되지않는경우이러한앱은 NetScaler Gateway 로폴백합니다.
- 프록시서버에대한 NetScaler 트래픽정책및프로필을구성합니다. 그런다음이러한정책및프로필을 NetScaler Gateway VIP 에바인딩합니다.

중요:

Secure Hub cVPN 트래픽을프록시에서제외하십시오.

Split DNS(DNS 분할)(Client experience(클라이언트환경) 아래) 에대한 NetScaler 세션프로필구성은분할터널링과 유사하게작동합니다.

Split DNS(DNS 분할) 를사용하고 둘다로설정환경우:

- 클라이언트가 FQDN 을로컬로확인한다음실패시 NetScaler 로폴백하여 DNS 를확인합니다.

Split DNS(DNS 분할) 를 원격으로설정환경우:

- DNS 확인이 NetScaler 에서만수행됩니다.

Split DNS(DNS 분할) 를 로컬로설정환경우:

- 클라이언트가 FQDN 을로컬로확인합니다. NetScaler 는 DNS 확인에사용되지않습니다.

Access Control(액세스제어)

이제회사에서네트워크내부및외부의모바일장치를관리할수있습니다. XenMobile 같은엔터프라이즈모빌리티관리솔루션은모바일장치의위치에관계없이보안및제어를제공할수있습니다. 뿐만아니라 NAC(네트워크액세스제어) 솔루션과함께사용할경우 QoS 를추가하고네트워크내부의장치를보다세부적으로제어할수있습니다. 이러한결합을사용할경우 XenMobile 장치의보안평가를 NAC 솔루션을통해확장할수있습니다. 그런다음 NAC 솔루션에서 XenMobile 보안평가를사용하여인증의사결정을지원하고처리할수있습니다. Citrix 는 Cisco Identity Services Engine(ISE) 또는 ForeScout 에대해 NAC 와 XenMobile 의통합을검증했습니다. Citrix 는다른 NAC 솔루션에대한통합을보장하지않습니다.

NAC 솔루션과 XenMobile 의통합은다음과같은장점을제공합니다.

- 엔터프라이즈네트워크의모든끝점에대한보안, 규정준수및제어가개선됩니다.
- NAC 솔루션은다음과같은기능을제공합니다.
 - 회사네트워크에연결하는장치를즉시감지합니다.
 - XenMobile 에장치특성을쿼리합니다.

- 그런다음해당정보를사용하여이러한장치를허용, 차단, 제한또는리디렉션할지결정합니다. 이러한결정은회사에서 선택하는보안정책에따라다릅니다.

- IT 관리자는 NAC 솔루션을사용하여관리되지않는장치와규정을준수하지않는장치를확인할수있습니다.

XenMobile 에서지원되는 NAC 규정준수필터에대한설명은 [네트워크액세스제어](#)를참조하십시오.

다중사이트요구사항

August 23, 2019

고가용성및재해복구를위한여러사이트를포함하는 XenMobile 배포를설계하고구성할수있습니다. 이문서에서는 XenMobile 배포에사용되는고가용성및재해복구모델의개요를제공합니다.

고가용성

- XenMobile 클러스터노드의경우 NetScaler 가부하분산을처리합니다. 자세한내용은 [클러스터링구성](#)
- XenMobile 서버노드는활성/활성구성으로작동합니다.
- 용량이필요하면추가 XenMobile 서버노드가고가용성클러스터에추가됩니다. 단일노드는최대약 8,500 개의사용자장치를처리할수있습니다 (자세한내용은 [확장성및성능](#) 참조).
- 8,500 개사용자장치를처리하는서버하나와중복성을위한추가서버하나를나타내는 “n+1” 로 XenMobile 서버를구성하는것이 좋습니다.
- 가능한경우모든 NetScaler 인스턴스에대해고가용성을구성하여두번째 NetScaler 와구성을동기화하는것이 좋습니다.
- 표준 NetScaler 고가용성쌍은활성/비활성구성으로작동합니다.

일반적인고가용성 XenMobile 배포에는다음이포함됩니다.

- NetScaler 인스턴스 (VPX 또는 MPX) 2 개. NetScaler SDX 플랫폼을사용하는경우에도고가용성을고려해야합니다.
- 동일한데이터베이스설정으로구성된둘이상의 XenMobile 서버.

재해복구

활성데이터센터 1 개와비활성데이터센터 1 개로구성된데이터센터 2 개를사용하여 XenMobile 의재해복구를구성할수있습니다. 활성/활성설정의사용자환경을제공하기위해활성/활성데이터센터경로를만들려면 NetScaler 와 GSLB(Global Server Load Balancing) 를사용합니다.

재해복구를위한 XenMobile 배포에는다음이포함됩니다.

- 하나이상의 NetScaler 인스턴스, XenMobile 서버및 SQL Server 데이터베이스가포함된데이터센터 2 개.
- 트래픽을데이터센터로전달하는 GSLB 서버. 사이트에대한트래픽을처리하는 XenMobile 등록 URL 과 NetScaler Gateway URL 모두에대해 GSLB 서버를구성합니다.

- XenMobile 용 NetScaler 마법사를 사용하여 NetScaler Gateway 를 구성하는 경우 기본적으로 GSLB 가 XenMobile 등록 서버에 대한 트래픽과 NetScaler Gateway 에 대한 트래픽을 MAM 부하 분산 서버로 이동하는 중에 확인하도록 설정되지 않으므로 추가 단계를 수행해야 합니다. 이러한 단계의 준비 및 구현에 대한 자세한 내용은 [재해 복구](#) 를 참조하십시오.
- Always On 가용성 그룹의 클러스터링된 SQL Server.
- XenMobile 서버와 SQL Server 간 대기 시간은 5 밀리초 미만이어야 합니다.

참고:

이 안내서에 설명된 재해 복구 방법은 액세스 계층에 대한 자동 재해 복구만 제공합니다. 장치에서 XenMobile 서버에 연결하려 면 장애 조치 (failover) 사이트에서 모든 XenMobile 서버 노드와 SQL Server 데이터베이스를 수동으로 시작해야 합니다.

NetScaler Gateway 및 NetScaler 통합

January 6, 2020

NetScaler Gateway 를 XenMobile 과 통합하면 내부 네트워크로 원격 액세스하는 MAM 장치에 대한 인증 메커니즘을 사용할 수 있습니다. 이 통합을 사용하면 모바일 장치의 앱에서 NetScaler Gateway 로 연결되는 Micro VPN 을 만들어 모바일 생산성 앱에 서 인터넷의 회사 서버에 연결할 수 있습니다.

XenMobile 서버가 여러 개이거나 XenMobile 서버가 DMZ 또는 내부 네트워크에 있는 경우 (트래픽이 장치에서 NetScaler 를 거쳐 XenMobile 로 흐르는 경우) 모든 XenMobile 서버 장치 모드에서 NetScaler 부하 분산을 사용해야 합니다.

XenMobile Server 모드에 대한 통합 요구 사항

NetScaler Gateway 및 NetScaler 의 통합 요구 사항은 XenMobile Server 모드 (MAM, MDM 및 ENT) 에 따라 다릅니다.

MAM

XenMobile Server 를 MAM 모드에서 사용:

- **NetScaler Gateway** 가 필요합니다. NetScaler Gateway 는 모든 회사 리소스에 액세스할 수 있는 Micro VPN 경로를 제공하며 강력한 다중 단계 인증을 지원합니다.
- 부하 분산에는 **NetScaler** 가 권장됩니다.

XenMobile 앞에 부하 분산 장치를 배치하는 고가용성 구성으로 XenMobile 을 배포하는 것이 좋습니다. 자세한 내용은 [MAM 모드와 레거시 MAM 모드 정보](#) 에서 참조하십시오.

MDM

XenMobile Server 를 MDM 모드에서사용:

- NetScaler Gateway 가필요하지않습니다. MDM 배포의경우 NetScaler Gateway 는모바일장치 VPN 에권장됩니다.
- 보안및부하분산에는 NetScaler 가권장됩니다.

보안및부하분산을위해 NetScaler 장비를 XenMobile 서버앞에배포하는것이 좋습니다. XenMobile 서버를 DMZ 에배포하는표준배포의경우 XenMobile 용 NetScaler 마법사와함께 XenMobile 서버부하분산을 SSL 브리지모드에서사용하는것이 좋습니다. XenMobile 서버가 DMZ 대신내부네트워크에상주하고보안상의이유로이러한구성이필요한경우배포에 SSL 오프로드를고려할수도있습니다.

SSL 트래픽이 XenMobile 서버에서종료되는경우 (SSL 브리지) NAT 또는기존타사프록시나 MDM 용부하분산장치를 통해 XenMobile 서버를인터넷에공개할수있지만이접근방식은잠재적보안위험으로인해권장되지않습니다.

보안수준이높은환경에서는기본 XenMobile 구성의 NetScaler 로지정된수준이상의보안요구사항을충족할수있어야 합니다.

보안요구사항이가장높은 MDM 환경에서는 SSL 을 NetScaler 에서종료하여경계에서트래픽을검사하는동시에중단간 SSL 암호화를유지할수있습니다. 자세한내용은 [보안요구사항](#)에서참조하십시오. NetScaler 는 SSL/TLS 암호화및 SSL FIPS NetScaler 하드웨어를정의하는옵션을제공합니다.

ENT(MAM+MDM)

XenMobile Server 를 ENT 모드에서사용:

- NetScaler Gateway 가필요합니다. NetScaler Gateway 는모든회사리소스에액세스할수있는 Micro VPN 경로를제공하며강력한다중단계인증을지원합니다.

XenMobile 서버모드가 ENT 이고사용자가 MDM 등록을선택하는경우장치는레거시 MAM 모드에서작동합니다. 레거시 MAM 모드에서는 NetScaler Gateway FQDN 을사용하여장치를등록합니다. 자세한내용은 [MAM 모드와레거시 MAM 모드정보](#)에서참조하십시오.

- 부하분산에는 NetScaler 가권장됩니다. 자세한내용은위의 “MDM” 아래 NetScaler 요점을참조하십시오.

중요:

초기등록의경우사용자장치의트래픽은 SSL 오프로드또는 SSL 브리지에대한부하분산가상서버의구성여부와관계없이 XenMobile 서버에서인증됩니다.

설계의사결정

다음섹션에는 NetScaler Gateway 와 XenMobile 의통합을계획할때고려해야하는다수의설계의사결정이요약되어있습니다.

라이선스및버전

의사결정세부정보:

- 사용할 NetScaler 의버전은무엇입니까?
- NetScaler 에플랫폼라이선스를적용했습니까?
- MAM 기능이필요한경우 NetScaler Universal Access 라이선스를적용했습니까?

설계지침:

NetScaler Gateway 에올바른라이선스를적용하십시오. Exchange ActiveSync 용 Citrix Gateway 커넥터를사용하는 경우통합캐싱이필요할수있으므로적절한 NetScaler 버전이있어야합니다.

NetScaler 기능을사용하기위한라이선스요구사항은다음과같습니다.

- XenMobile MDM 부하분산을사용하려면 NetScaler Standard 이상의플랫폼라이선스가필요합니다.
- StorageZones Controller 를통한 ShareFile 부하분산을사용하려면 NetScaler Standard 이상의플랫폼라이선스가필요합니다.
- XenMobile Enterprise Edition 에는 MAM 에필요한 NetScaler Gateway Universal 라이선스가포함되어있습니다.
- Exchange 부하분산을사용하려면 NetScaler Platinum 플랫폼라이선스또는 NetScaler Enterprise 플랫폼라이선스 (통합캐싱라이선스포함) 가필요합니다.

XenMobile 에대한 NetScaler 버전

의사결정세부정보:

- XenMobile 환경에서실행되는 NetScaler 버전은무엇입니까?
- 개별인스턴스가필요합니까?

설계지침:

NetScaler Gateway 가상서버를위한전용 NetScaler 인스턴스를사용하는것이 좋습니다. XenMobile 환경에서필요한최소버전의 NetScaler 와빌드가사용되고있는지확인하십시오. XenMobile 과호환되는최신 NetScaler 버전및빌드를사용하는것이 가장 좋습니다. NetScaler Gateway 업그레이드가 기존환경에영향을미칠수있는경우 XenMobile 을위한두번째전용인스턴스를만드는것이적절할수 있습니다.

XenMobile 의 NetScaler 인스턴스를 VPN 연결을사용하는다른앱과공유하려는경우두앱에서사용하기에충분한 VPN 라이선스가있는지확인하십시오. XenMobile 테스트및프로덕션환경에서는 NetScaler 인스턴스를공유할수 없습니다.

인증서

의사결정세부정보:

- XenMobile 환경을등록하고액세스할때더높은수준의보안이필요합니까?
- LDAP 를사용할수없습니까?

설계지침:

XenMobile 에대한기본구성은사용자이름및암호인증입니다. XenMobile 환경에대한등록및액세스시추가보안계층을추가하려면인증서기반인증을사용하는것이 좋습니다. 인증서를 LDAP 와함께 2 단계인증에사용하여 RSA 서버없이더높은수준의보안을제공할수있습니다.

LDAP 를허용하지않고스마트카드또는유사한방법을사용하는경우인증서를구성하면 XenMobile 에스마트카드를나타낼수 있습니다. 그런다음사용자는 XenMobile 에서생성된고유한 PIN 을사용하여등록합니다. 사용자가액세스권한을획득하면 XenMobile 이이후에 XenMobile 환경에인증하는데사용될인증서를만들어배포합니다.

XenMobile 은타사인증기관에대해서만 CRL(인증서해지목록) 을지원합니다. Microsoft CA 가구성된경우 XenMobile 은 NetScaler 를사용하여해지를관리합니다. 클라이언트인증서기반인증을구성하는경우 NetScaler CRL(인증서해지목록) 설정인 **Enable CRL Auto Refresh(CRL 자동새로고침사용)** 을구성해야하는지여부를고려합니다. 이렇게하면 MAM 전용모드의장치사용자가장치의기존인증서를사용하여인증할수없습니다. 이경우 XenMobile 은새인증서를다시발급합니다. 사용자인증서가해지된경우사용자의인증서생성을제한하지않기때문입니다. 이설정을사용하면 CRL 이만료된 PKI 엔터티를확인하는경우 PKI 엔터티의보안이강화됩니다.

네트워크토폴로지

의사결정세부정보:

- 필요한 NetScaler 토폴로지는무엇입니까?

설계지침:

XenMobile 에는 NetScaler 인스턴스를사용하는것이 좋습니다. 그러나네트워크내부의트래픽이 DMZ 외부로이동하는것을원하지않는다면 NetScaler 의추가인스턴스를설정하여한 NetScaler 인스턴스를내부사용자에게제공하고다른인스턴스를외부사용자에게제공할수있습니다. 사용자가내부네트워크와외부네트워크를전환하는경우 DNS 레코드캐싱으로인해 Secure Hub 에서로그온시도가증가할수있습니다.

XenMobile 은 NetScaler Gateway 이중홉을지원하지않습니다.

전용또는공유 **NetScaler Gateway VIP**

의사결정세부정보:

- 현재 Virtual Apps and Desktops 에 NetScaler Gateway 를사용하고있습니까?
- XenMobile 에서 Virtual Apps and Desktops 와동일한 NetScaler Gateway 를활용할계획입니까?
- 두트래픽흐름에대한인증요구사항은무엇입니까?

설계지침:

Citrix 환경에 XenMobile 에더해 Virtual Apps and Desktops 가포함되는경우동일한 NetScaler 인스턴스와 NetScaler Gateway 가상서버를동시에사용할수있습니다. 버전관리충돌및환경격리가발생할수있으므로각 XenMobile 환경에서전용 NetScaler 인스턴스및 NetScaler Gateway 를사용하는것이 좋습니다. 그러나전용 NetScaler 인스턴

스를 사용할 수 없는 경우에는 XenMobile 과 Virtual Apps and Desktops 에 공유되는 NetScaler Gateway vServer 대신 전용 vServer 를 사용하여 Secure Hub 에 대한 트래픽 흐름을 분리하는 것이 좋습니다.

LDAP 인증을 사용하는 경우 Receiver 및 Secure Hub 에서 동일한 NetScaler Gateway 에 문제없이 인증할 수 있습니다. 인증서 기반 인증을 사용하는 경우 XenMobile 은 인증서를 MDX 컨테이너에 푸시하고 Secure Hub 는 이 인증서를 사용하여 NetScaler Gateway 에 인증합니다. Receiver 는 Secure Hub 와 분리되며 Secure Hub 와 동일한 인증서를 사용하여 동일한 NetScaler Gateway 에 인증할 수 없습니다.

이 경우 두 개의 NetScaler Gateway VIP 에 동일한 FQDN 을 사용하여 문제를 해결할 수 있습니다. 동일한 IP 주소를 사용하여 두 개의 NetScaler Gateway VIP 를 만들고, Secure Hub 에 사용할 VIP 에는 표준 443 포트를 사용하고 Virtual Apps and Desktops(Receiver 배포) 에 사용할 VIP 에는 포트 444 를 사용합니다. 그러면 하나의 FQDN 이 동일한 IP 주소로 확인됩니다. 이해결방범을 사용하는 경우 기본값이 포트 443 이 아닌 포트 444 에 대해 ICA 파일을 반환하도록 StoreFront 를 구성해야 할 수 있습니다. 이해결방범을 사용하는 경우 사용자가 포트 번호를 입력할 필요가 없습니다.

NetScaler Gateway 시간초과

의사결정세부정보:

- XenMobile 트래픽에 대한 NetScaler Gateway 시간초과를 어떻게 구성할 것입니까?

설계지침:

NetScaler Gateway 에는 Session time-out(세션시간초과) 및 Forced time-out(강제시간초과) 라는 설정이 포함됩니다. 자세한 내용은 **권장되는 구성**에서 참조하십시오. 백그라운드 서비스, NetScaler 및 오프라인 응용 프로그램 액세스에 대한 시간초과 값이 서로 다르다는 점에 유의하십시오.

MAM 에 대한 XenMobile 부하 분산 장치 IP 주소

의사결정세부정보:

- VIP 에 내부 또는 외부 IP 주소를 사용합니까?

설계지침:

공용 IP 주소를 NetScaler Gateway VIP 에 사용할 수 있는 환경에서 XenMobile 부하 분산 VIP 및 주소를 이 방식으로 할당하면 등록 실패가 발생할 수 있습니다.

이 시나리오에서 등록 실패를 방지하려면 부하 분산 VIP 에 내부 IP 가 사용되어야 합니다. 가상 IP 주소는 사실 IP 주소의 RFC 1918 표준을 준수해야 합니다. 가상 IP 주소를 가상 서버에서 사용하는 경우 NetScaler 가 인증 프로세스 중에 XenMobile 서버에 연결할 수 없습니다. 자세한 내용은 <https://support.citrix.com/article/CTX200430>에서 참조하십시오.

MDM 부하 분산 메커니즘

의사결정세부정보:

- NetScaler Gateway 를 사용하여 XenMobile 서버부하를 어떻게 분산하려고 합니까?

설계지침:

XenMobile 이 DMZ 에있는 경우 SSL 브리지를 사용합니다. XenMobile 서버가 내부 네트워크에 있는 경우 보안 표준을 충족해야 한다면 SSL 오프로드를 사용합니다.

- SSL 브리지 모드에서 NetScaler VIP 를 사용하여 XenMobile 서버부하를 분산하는 경우 인터넷 트래픽이 XenMobile 서버로 직접 흐르고 여기서 연결이 종료됩니다. SSL 브리지 모드는 설정 및 문제 해결이 가장 간단한 모드입니다.
- SSL 오프로드 모드에서 NetScaler VIP 를 사용하여 XenMobile 서버부하를 분산하는 경우 인터넷 트래픽이 NetScaler 로 직접 흐르고 여기서 연결이 종료됩니다. NetScaler 는 NetScaler 을 XenMobile 서버에 연결하는 새 세션을 설정합니다. SSL 오프로드 모드는 설정 및 문제 해결이 좀 더 복잡합니다.

SSL 오프로드를 통한 MDM 부하 분산의 서비스 포트

의사 결정 세부 정보:

- 부하 분산에 SSL 오프로드 모드를 사용하려는 경우 백엔드 서비스에 사용할 포트는 무엇입니까?

설계지침:

SSL 오프로드의 경우 다음과 같이 포트 80 또는 8443 을 선택합니다.

- 포트 80 을 활용하여 XenMobile 서버에 다시 연결함으로써 완벽한 오프로드를 수행합니다.
- 종단간 암호화, 즉 트래픽 재암호화는 지원되지 않습니다. 자세한 내용은 Citrix 지원 문서 [Supported Architectures Between NetScaler and XenMobile Server](#) (NetScaler 와 XenMobile Server 간에 지원되는 아키텍처) 를 참조하십시오.

등록 FQDN

의사 결정 세부 정보:

- 등록 및 XenMobile 인스턴스/부하 분산 VIP 에 사용할 FQDN 은 무엇입니까?

설계지침:

클러스터의 첫 번째 XenMobile 서버를 처음으로 구성할 때는 XenMobile 서버 FQDN 을 입력해야 합니다. 이 FQDN 은 MDM VIP URL 및 내부 MAM LB VIP URL 과 일치해야 합니다. 내부 NetScaler 주소 레코드는 MAM LB VIP 를 확인합니다. 자세한 내용은 이 문서의 나중에 나오는 “배포 유형별 등록 FQDN” 을 참조하십시오.

또한 XenMobile SSL 수신기 인증서, 내부 MAM LB VIP 인증서 및 MDM VIP 인증서 (MDM VIP 에서 SSL 오프로드를 사용하는 경우) 와 동일한 인증서를 사용해야 합니다.

중요:

등록 FQDN 을 구성한 후에는 변경할 수 없습니다. 새 등록 FQDN 을 사용하려면 새 SQL Server 데이터베이스와 XenMobile 서버를 다시 구축해야 합니다.

Secure Web 트래픽

의사결정세부정보:

- Secure Web 을내부웹브라우저로만제한할계획입니까?
- 내부및외부웹브라우저에서 Secure Web 을사용할계획입니까?

설계지침:

내부웹브라우저에서만 Secure Web 을사용하려는경우 Secure Web 에서기본적으로모든내부사이트에연결할수있다고가정하면 NetScaler Gateway 구성은간단하며, 방화벽과프록시서버를구성해야할수있습니다.

내부와외부브라우저에도모두 Secure Web 을사용하려는경우 SNIP 에서아웃바운드인터넷액세스가가능해야합니다. 일반적으로 IT 부서에서는등록된장치 (MDX 컨테이너사용) 를회사네트워크의연장으로보기때문에 Secure Web 연결을 NetScaler 로다시보내고프록시서버를통과한다음인터넷으로나가는방식으로구성하려고합니다. 기본적으로 Secure Web 액세스는내부네트워크로터널링됩니다. 즉, Secure Web 은모든네트워크액세스에대해내부네트워크로다시터널링되는응용프로그램별 VPN 터널을사용하고 NetScaler 는분할터널링설정을사용합니다.

Secure Web 연결에대한설명은 [사용자연결구성](#)을참조하십시오.

Secure Mail 에대한푸시알림

의사결정세부정보:

- 푸시알림을사용할계획입니까?

iOS 용설계지침:

NetScaler Gateway 구성이 STA(Secure Ticket Authority) 를포함하고분할터널링이꺼져있으면 NetScaler Gateway 는 Secure Mail 에서 iOS 용 Secure Mail 의푸시알림에지정된 Citrix 수신기서비스 URL 로의트래픽을허용해야합니다.

Android 용설계지침:

활성폴링기간이라는 MDX 정책대신 FCM(Firebase Cloud Messaging) 을사용하여 Android 장치에서 XenMobile 에 연결하는방법과시기를제어할수있습니다. FCM 을구성하면모든보안동작또는배포명령이실행될때사용자에게 XenMobile 서버에다시연결하라는메시지를표시하는 Secure Hub 푸시알림이트리거됩니다.

HDX STA

의사결정세부정보:

- HDX 응용프로그램엑세스를통합할경우사용할 STA 는무엇입니까?

설계지침:

HDX STA 는 StoreFront 의 STA 와일치해야하며 Virtual Apps and Desktops 팜에서유효해야합니다.

ShareFile

의사결정세부정보:

- 환경에서 ShareFile StorageZone Controller 를 사용할 계획입니까?
- 사용할 ShareFile VIP URL 은 무엇입니까?

설계지침:

환경에 ShareFile StorageZone Controller 를 포함하려는 경우 ShareFile 콘텐츠스위칭 VIP(ShareFile 제어부에서 StorageZone 컨트롤러 서버와 통신할 때 사용됨), ShareFile 부하분산 VIP 와 필요한 모든 정책 및 프로필을 올바르게 구성해야 합니다. 자세한 내용은 Citrix ShareFile StorageZones Controller 설명서를 참조하십시오.

SAML IdP

의사결정세부정보:

- ShareFile 에 SAML 이 필요한 경우 XenMobile 을 SAML IdP 로 사용할 것입니까?

설계지침:

권장되는 모범 사례는 ShareFile 을 XenMobile Advanced Edition 또는 XenMobile Enterprise Edition 과 통합하는 것입니다. 이 방법은 SAML 기반 페더레이션 구성하는 것보다 간단합니다. 이러한 XenMobile 버전과 함께 ShareFile 을 사용하면 모바일 생산성 앱 사용자가 SSO(Single Sign-on) 를 사용하여 ShareFile 에 인증하고, Active Directory 에 따라 사용자 계정을 프로비전할 수 있으며, 포괄적인 액세스 제어 정책을 활용할 수 있습니다. XenMobile 콘솔을 사용하여 ShareFile 구성을 수행하고 서비스 수준 및 라이선스 사용 현황을 모니터링할 수 있습니다.

ShareFile 클라이언트에는 XenMobile 용 ShareFile 클라이언트 (래핑된 ShareFile) 와 ShareFile Mobile 클라이언트 (래핑되지 않은 ShareFile) 의 두 가지가 있습니다. 차이점을 이해하려면 [ShareFile for XenMobile 클라이언트와 ShareFile Mobile 클라이언트의 차이점](#) 을 참조하십시오.

MDX Toolkit 으로 래핑된 ShareFile Mobile 앱과 래핑되지 않은 ShareFile 클라이언트 (예: 웹사이트, Outlook 플러그인 또는 동기화 클라이언트) 에 대한 SSO 액세스를 SAML 을 사용하여 제공하도록 XenMobile 과 ShareFile 을 구성할 수 있습니다.

XenMobile 을 ShareFile 의 SAML IdP 로 사용하려는 경우 구성이 올바른지 확인하십시오. 자세한 내용은 [ShareFile 을 사용하는 SSO 를 위한 SAML](#) 에서 참조하십시오.

ShareConnect 직접연결

의사결정세부정보:

- ShareConnect 를 실행하는 컴퓨터 또는 모바일 장치에서 사용자가 호스트 컴퓨터에 액세스할 때 직접연결을 사용할 것입니까?

설계지침:

ShareConnect 를 사용할 경우 사용자는 iPad, Android 태블릿 및 Android 휴대폰을 통해 컴퓨터에 안전하게 연결하여 파일 및 응용 프로그램에 액세스할 수 있습니다. 직접 연결의 경우, XenMobile 은 NetScaler Gateway 를 사용하여 로컬 네트워크 외부의 리소스에 대한 보안 액세스를 제공합니다. 구성에 대한 자세한 내용은 [ShareConnect](#) 를 참조하십시오.

배포 유형별 등록 FQDN

배포 유형	등록 FQDN
엔터프라이즈 (MDM+MAM) 및 MDM 등록 필수	XenMobile 서버 FQDN
엔터프라이즈 (MDM+MAM) 및 MDM 등록 선택	XenMobile 서버 FQDN 또는 NetScaler Gateway FQDN
MDM 전용	XenMobile 서버 FQDN
MAM 전용 (레거시)	NetScaler Gateway FQDN
MAM 전용	XenMobile 서버 FQDN

배포 요약

올바른 구성을 위해 XenMobile 용 NetScaler 마법사를 사용하는 것이 좋습니다. 마법사는 한번만 사용할 수 있습니다. 테스트, 개발 및 프로덕션 환경을 위한 다수의 XenMobile 인스턴스가 있는 경우 추가 환경에 대한 NetScaler 를 수동으로 구성해야 합니다. 작동 중인 환경에서는 XenMobile 에서 사용할 NetScaler 를 수동으로 구성하기 전에 설정을 기록해 두십시오.

마법사를 사용하는 경우 결정해야 하는 중요한 사항은 XenMobile 서버에 대한 통신에 HTTPS 를 사용할지, 아니면 HTTP 를 사용할지입니다. HTTPS 는 NetScaler 와 XenMobile 간의 트래픽을 암호화하는 보안 백엔드 통신을 제공하며 재암호화 시 XenMobile 서버 성능이 저하될 수 있습니다. HTTP 는 더 높은 XenMobile 서버 성능을 제공하지만 NetScaler 와 XenMobile 간의 트래픽이 암호화되지 않습니다. 다음 표에 XenMobile 서버용 NetScaler 의 HTTP 및 HTTPS 포트 요구 사항이 나와 있습니다.

HTTPS

일반적으로, NetScaler MDM 가상 서버 구성에는 SSL 브리지가 권장됩니다. MDM 가상 서버에서 사용되는 NetScaler SSL 오프로드의 경우 XenMobile 은 포트 80 만 백엔드 서비스로 지원합니다.

배포 유형	NetScaler 부하 분산 방법	SSL 재암호화	XenMobile 서버 포트
MDM	SSL 브리지	해당 없음	443, 8443

MAM	SSL 오프로드	사용	8443
Enterprise	MDM: SSL 브리지	해당없음	443, 8443
Enterprise	MAM: SSL 오프로드	사용	8443

HTTP

배포유형	NetScaler 부하분산방법	SSL 재암호화	XenMobile 서버포트
MDM	SSL 오프로드	지원되지않음	80
MAM	SSL 오프로드	사용	8443
Enterprise	MDM: SSL 오프로드	지원되지않음	80
Enterprise	MAM: SSL 오프로드	사용	8443

XenMobile 배포의 NetScaler Gateway 다이어그램은 [온-프레미스배포용참조아키텍처](#)를 참조하십시오.

MDX 앱에 대한 SSO 및 프록시 고려 사항

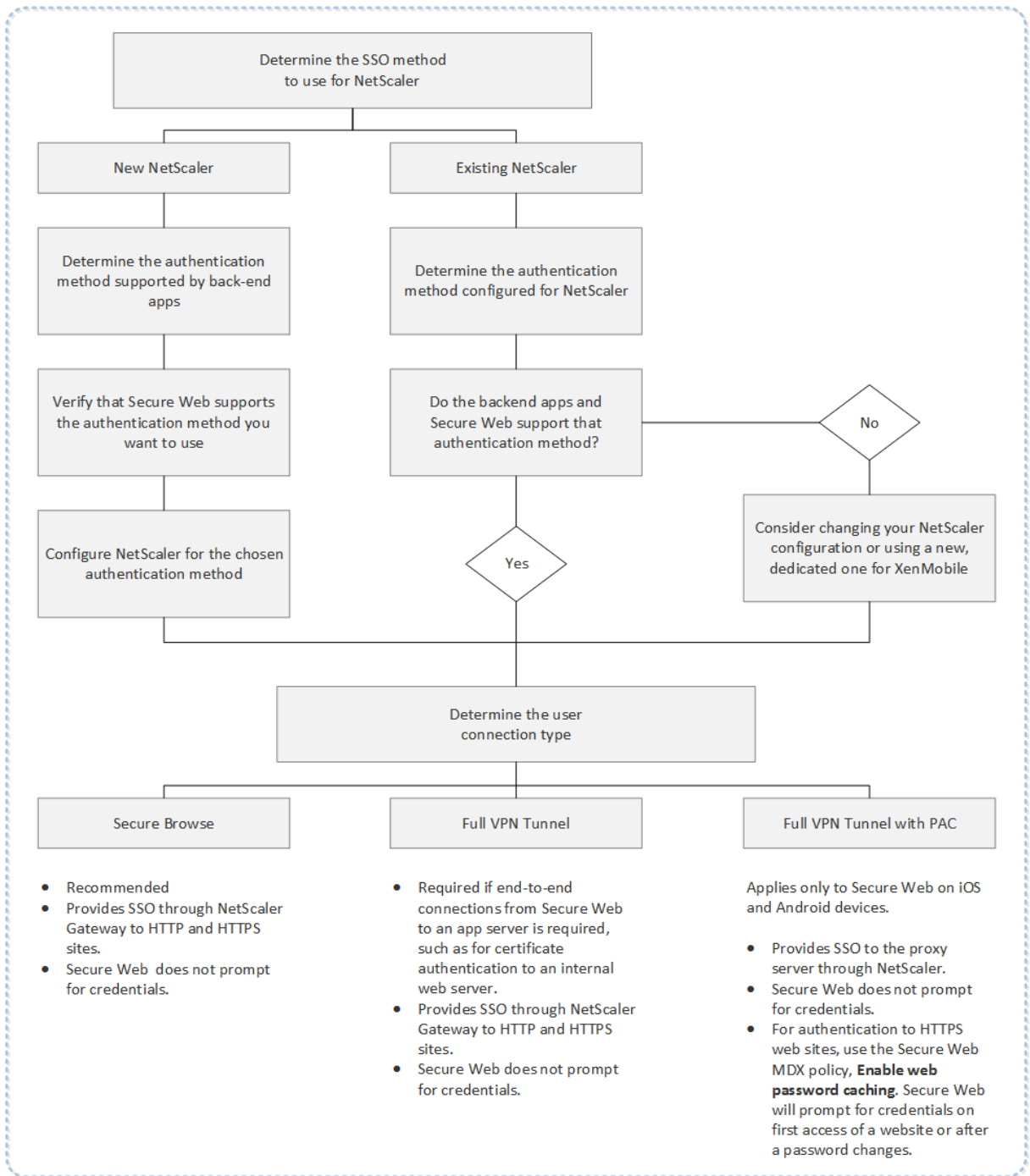
April 11, 2019

XenMobile 을 NetScaler 와 통합하면 모든 백엔드 HTTP/HTTPS 리소스에 대한 SSO(Single Sign-on) 를 사용자에게 제공할 수 있습니다. SSO 인증요구 사항에 따라 다음 옵션 중 하나를 사용하도록 MDX 앱에 대한 사용자 연결을 구성할 수 있습니다.

- 클라이언트 없는 VPN 유형인 Secure Browse
- 전체 VPN 터널

환경에서 SSO 를 제공하기에 NetScaler 가 적합하지 않은 경우 정책 기반 로컬 암호 캐싱을 통해 MDX 앱을 구성할 수 있습니다. 이 문서에서는 Secure Web 을 중심으로 다양한 SSO 및 프록시 옵션에 대해 알아봅니다. 개념은 다른 MDX 앱에도 적용됩니다.

다음 순서도는 SSO 및 사용자 연결에 대한 의사결정 흐름을 요약한 것입니다.



NetScaler 인증방법

이 섹션에서는 NetScaler 가 지원 하는 인증 방법에 대한 일반 정보를 제공합니다.

SAML 인증

SAML(Security Assertion Markup Language) 을사용하도록 NetScaler 를구성하는경우사용자는 SSO(Single Sign-on) 에 SAML 프로토콜을지원하는웹앱에연결할수있습니다. NetScaler Gateway 는 SAML 웹앱에대해 IdP(ID 공급자) SSO(Single Sign-on) 를지원합니다.

필요한구성:

- NetScaler 트래픽프로필에서 SAML SSO 를구성합니다.
- 요청한서비스에대한 SAML iDP 를구성합니다.

NTLM 인증

세션프로필에서웹앱에대한 SSO 를사용하도록설정하면 NetScaler 가자동으로 NTLM 인증을수행합니다.

필요한구성:

- NetScaler 세션또는트래픽프로필에서 SSO 를사용하도록설정합니다.

Kerberos 가장

XenMobile 은 Secure Web 에대해서만 Kerberos 를지원합니다. Kerberos SSO 를사용하도록 NetScaler 를구성하는경우사용자암호가 NetScaler 에제공되면 NetScaler 가가장을사용합니다. 가장은 NetScaler 가 Secure Web 같은서비스에액세스하는데필요한티켓을사용자자격증명을사용하여가져온다는것을의미합니다.

필요한구성:

- 연결에서 Kerberos 영역을식별할수있도록 NetScaler “Worx” 세션정책을구성합니다.
- NetScaler 에서 KCD(Kerberos 제한위임) 계정을구성합니다. 이계정을암호없이구성하고 XenMobile 게이트웨이의트래픽정책에바인딩합니다.
- 이러한 구성 및 다른 구성에 대한 세부 정보는 Citrix 블로그 [WorxWeb and Kerberos Impersonation SSO\(WorxWeb 및 Kerberos 가장 SSO\)](#)를참조하십시오.

Kerberos 제한위임

XenMobile 은 Secure Web 에대해서만 Kerberos 를지원합니다. Kerberos SSO 를사용하도록 NetScaler 를구성하는경우사용자암호가 NetScaler 에제공되지않으면 NetScaler 가제한위임을사용합니다.

제한위임을사용하는경우 NetScaler 는사용자및서비스에대한티켓을가져올때지정된관리자계정을사용합니다.

필요한구성:

- NetScaler 의필요한권한및 KDC 계정을사용하여 Active Directory 에서 KCD 계정을구성합니다.
- NetScaler 트래픽프로필에서 SSO 를사용하도록설정합니다.
- Kerberos 인증에대한백엔드웹사이트를구성합니다.

- 이러한 구성 및 다른 구성에 대한 세부 정보는 Citrix 블로그 [Configuring Kerberos Single Sign-on for WorxWeb\(WorxWeb 에대한 Kerberos Single Sign-on 구성\)](#)을 참조하십시오.

양식입력인증

양식기반 SSO(Single Sign-on) 를 사용하도록 NetScaler 를 구성하는 경우 사용자는 단 한번의 로그인으로 네트워크의 모든 보호되는 앱에 액세스할 수 있습니다. 이 인증 방법은 Secure Browse 또는 전체 VPN 모드를 사용하는 앱에 적용됩니다.

필요한 구성:

- NetScaler 트래픽 프로필에서 양식기반 SSO 를 구성합니다.

다이제스트 HTTP 인증

세션 프로필에서 웹 앱에 대한 SSO 를 사용하도록 설정하면 NetScaler 가 자동으로 다이제스트 HTTP 인증을 수행합니다. 이 인증 방법은 Secure Browse 또는 전체 VPN 모드를 사용하는 앱에 적용됩니다.

필요한 구성:

- NetScaler 세션 또는 트래픽 프로필에서 SSO 를 사용하도록 설정합니다.

기본 HTTP 인증

세션 프로필에서 웹 앱에 대한 SSO 를 사용하도록 설정하면 NetScaler 가 자동으로 기본 HTTP 인증을 수행합니다. 이 인증 방법은 Secure Browse 또는 전체 VPN 모드를 사용하는 앱에 적용됩니다.

필요한 구성:

- NetScaler 세션 또는 트래픽 프로필에서 SSO 를 사용하도록 설정합니다.

Secure Browse, 전체 VPN 터널 또는 PAC 포함 전체 VPN 터널

다음 섹션에서는 Secure Web 에 대한 사용자 연결 유형에 대해 설명합니다. 자세한 내용은 Citrix 설명서에서 [Secure Web 문서 사용자 연결 구성](#)을 참조하십시오.

전체 VPN 터널

내부 네트워크로 터널링되는 연결은 전체 VPN 터널을 사용할 수 있습니다. Secure Web 의 기본 설정 VPN 모드 정책을 사용하여 전체 VPN 터널을 구성할 수 있습니다. 클라이언트 인증서 또는 종단간 SSL 을 사용하여 내부 네트워크의 리소스로 연결되는 경우 전체 VPN 터널을 사용하는 것이 좋습니다. 전체 VPN 터널은 모든 프로토콜을 TCP 를 통해 처리합니다. 전체 VPN 터널을 Windows, Mac, iOS 및 Android 장치에서 사용할 수 있습니다.

전체 VPN 터널 모드에서 NetScaler 는 HTTPS 세션 내부를 볼 수 없습니다.

Secure Browse

내부네트워크에터널링되는연결은 Secure Browse 라고하는클라이언트없는 VPN 의변형을사용할수있습니다. Secure Browse 는 Secure Web 의 기본설정 VPN 모드정책에대해지정된기본구성입니다. SSO(Single Sign-On) 가필요한연결에는 Secure Browse 를사용하는것이 좋습니다.

Secure Browse 모드에서 NetScaler 는 HTTPS 세션을두부분으로분리합니다.

- 클라이언트에서 NetScaler 로
- NetScaler 에서백엔드리소스서버로

NetScaler 는이와같은분리를통해클라이언트와서버간의모든트랜잭션을파악하고 SSO 를제공합니다.

Secure Browse 모드에서사용될때 Secure Web 에대해프록시서버를구성할수도있습니다. 자세한내용은블로그 [XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode\(Secure Browse 모드에서프록시서버를 통한 XenMobile WorxWeb 트래픽\)](#)를참조하십시오.

PAC 포함전체 VPN 터널

iOS 및 Android 장치의 Secure Web 에대해전체 VPN 터널배포와함께 PAC(Proxy Automatic Configuration) 파일을사용할수있습니다. XenMobile 은 NetScaler 에의해제공되는프록시인증을지원합니다. PAC 파일에는웹브라우저에서 해당 URL 에액세스하기위해프록시를선택하는방식을정의하는규칙이포함됩니다. PAC 파일규칙은내부및외부사이트에대한처리방식을지정할수있습니다. Secure Web 은 PAC 파일규칙을구문분석하고프록시서버정보를 NetScaler Gateway 로보냅니다. NetScaler Gateway 는 PAC 파일또는프록시서버를인지하지못합니다.

HTTPS 웹사이트인증의경우 Secure Web MDX 정책인 웹암호캐싱사용을통해 Secure Web 을인증하고 MDX 를통해프록시서버에 SSO 를제공할수있습니다.

NetScaler 분할터널링

SSO 및프록시구성을계획할때는 NetScaler 분할터널링을사용하지여부또한결정해야합니다. NetScaler 분할터널링은필요한경우에만사용하는것이 좋습니다. 이섹션에서는분할터널링의작동방식을간략히설명합니다. NetScaler 는라우팅테이블에따라트래픽경로를결정합니다. NetScaler 분할터널링이켜져있는경우 Secure Hub 는인터넷트래픽에서내부 (보호되는) 네트워크트래픽을구분합니다. Secure Hub 는 DNS 접미사및인트라넷응용프로그램을사용하여트래픽을구분합니다. 그런다음 Secure Hub 는내부네트워크트래픽만 VPN 터널을통해터널링합니다. NetScaler 분할터널링이꺼져있는경우모든트래픽이 VPN 터널을통과합니다.

- 보안상의이유로모든트래픽을모니터링해야하는경우 NetScaler 분할터널링을끄십시오. 그러면모든트래픽이 VPN 터널을통과합니다.
- PAC 포함전체 VPN 터널을사용하는경우 NetScaler Gateway 분할터널링을사용하지않아야합니다. 분할터널링이켜져있고 PAC 파일이구성된경우 PAC 파일규칙이 NetScaler 분할터널링규칙보다우선합니다. 트래픽정책에구성된프록시서버는 NetScaler 분할터널링규칙을재정의하지않습니다.

기본적으로 네트워크 액세스 정책은 Secure Web 에 대해 내부 네트워크로 터널링됨으로 설정됩니다. 이 구성에서 MDX 앱은 NetScaler 분할터널링 설정을 사용합니다. 일부 다른 모바일 생성 애플리케이션의 경우 네트워크 액세스 정책의 기본값이 다릅니다.

NetScaler Gateway 에는 Micro VPN 역분할터널링 모드도 있습니다. 이 구성에서는 NetScaler 로터널링되지 않는 IP 주소로 구성된 제외 목록을 사용할 수 있습니다. 이러한 주소는 장치의 인터넷 연결을 사용하여 전송됩니다. 역분할터널링에 대한 자세한 내용은 NetScaler Gateway 설명서를 참조하십시오.

XenMobile 에는 역분할터널링 제외 목록이 포함됩니다. 특정 웹사이트를 NetScaler Gateway 를 통해 터널링하지 않으려는 경우 LAN(Local Area Network) 를 사용하여 연결하는 FQDN(정규화된 도메인 이름) 또는 DNS 접미사의 침표로 구분된 목록을 추가할 수 있습니다. 이 목록은 역분할터널링이 구성된 NetScaler Gateway 의 Secure Browse 모드에서만 적용됩니다.

인증

January 6, 2020

XenMobile 배포에서 인증을 구성하는 방법을 결정할 때는 여러 요소를 고려해야 합니다. 이 섹션에서는 다음을 설명하여 인증에 영향을 미치는 다양한 요소를 쉽게 이해할 수 있도록 합니다.

- 인증과 관련된 기본 MDX 정책, XenMobile 클라이언트 속성 및 NetScaler Gateway 설정.
- 이러한 정책, 클라이언트 속성 및 설정의 상호 작용 방식.
- 각 선택의 득실.

이 문서에는 보안 수준을 높이려는 경우 권장되는 구성에 대한 세 가지 예제도 포함되어 있습니다.

광범위하게 말해 보안이 강력하면 사용자가 더 자주 인증해야 하므로 사용자 환경이 덜 최적화됩니다. 이러한 요소의 균형을 맞추는 방식은 조직의 요구 사항 및 우선순위에 따라 다릅니다. 권장되는 세 가지 구성을 검토하여 사용 가능한 인증 방법의 상호 작용과 XenMobile 환경의 배포를 최적화하는 방법을 파악하십시오.

인증 모드

온라인 인증: 사용자가 XenMobile 네트워크에 들어갈 수 있습니다. 인터넷 연결이 필요합니다.

오프라인 인증: 인증이 장치에서 수행됩니다. 사용자가 보안 저장소의 잠금을 해제하고, 다운로드된 메일, 캐시된 웹사이트 및 메모 같은 항목에 오프라인으로 액세스합니다.

인증 방법

1 단계

LDAP: XenMobile 에서 LDAP(Lightweight Directory Access Protocol) 와 호환되는 하나 이상의 디렉터리 (예: Active Directory) 에 대한 연결을 구성할 수 있습니다. 회사 환경에 대한 SSO(Single Sign-on) 를 제공할 때 주로 사용되는 방법

입니다. Active Directory 암호캐싱을 통해 Citrix PIN 을 사용하도록 선택하면 LDAP 로 사용자 환경을 개선하는 동시에 등록, 암호 관리 및 계정 잠금 시 복잡한 암호를 사용하는 보안을 제공할 수 있습니다.

자세한 내용은 [도메인 또는 도메인과 STA](#) 문서를 참조하십시오.

클라이언트 인증서: XenMobile 을 업계 표준 인증 기관과 통합하여 인증서를 온라인 인증의 유일한 방법으로 사용할 수 있습니다. XenMobile 은 일회용 암호, 초대 URL 또는 LDAP 자격 증명이 필요한 사용자 등록 후 이 인증서를 제공합니다. 클라이언트 인증서를 기본적인 인증 방법으로 사용하는 경우 Citrix PIN 을 사용하여 클라이언트 인증서 전용 환경에서 장치의 인증서를 보호해야 합니다.

XenMobile 은 타사 인증 기관에 대해서만 CRL (인증서 해지 목록) 을 지원합니다. Microsoft CA 가 구성된 경우 XenMobile 은 NetScaler 를 사용하여 해지를 관리합니다. 클라이언트 인증서 기반 인증을 구성하는 경우 NetScaler CRL (인증서 해지 목록) 설정인 Enable CRL Auto Refresh (CRL 자동 새로고침 사용) 을 구성해야 하는 지 여부를 고려합니다. 이렇게 하면 MAM 전용 모드의 장치 사용자가 장치의 기존 인증서를 사용하여 인증할 수 없습니다. 이 경우 XenMobile 은 새 인증서를 다시 발급합니다. 사용자 인증서가 해지된 경우 사용자의 인증서 생성을 제한하지 않기 때문입니다. 이 설정을 사용하면 CRL 이 만료된 PKI 엔터티를 확인하는 경우 PKI 엔터티의 보안이 강화됩니다.

인증서 기반 인증을 사용하여 사용자를 인증하거나 엔터프라이즈 CA (인증 기관) 를 사용하여 장치 인증서를 발급하려는 경우 필요한 배포를 보여주는 다이어그램은 [온-프레미스 배포 참조 아키텍처](#) 를 참조하십시오.

2 단계

LDAP + 클라이언트 인증서: XenMobile 환경에서 이 구성은 NetScaler 의 2 단계 인증을 통한 보안과 최상의 SSO 기능으로 보안과 사용자 환경을 최적화합니다. LDAP 와 클라이언트 인증서를 모두 사용하면 사용자가 알고 있는 것 (Active Directory 암호) 과 사용자가 가지고 있는 것 (장치의 클라이언트 인증서) 을 사용하여 보안을 제공할 수 있습니다. Secure Mail (및 다른 모바일 생산성 앱) 은 올바르게 구성된 Exchange 클라이언트 액세스 서버 환경에서 클라이언트 인증서 인증을 통해 처음 사용하는 사용자를 위한 원활한 환경을 자동으로 구성하고 제공할 수 있습니다. 사용 편의성을 최적화하기 위해 이 옵션을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다.

LDAP + 토큰: 이 구성에서는 전형적인 LDAP 자격 증명 구성에 더해 RADIUS 프로토콜을 사용하는 일회용 암호를 사용할 수 있습니다. 사용 편의성을 최적화하기 위해 이 옵션을 Citrix PIN 및 Active Directory 암호 캐싱과 결합할 수 있습니다.

인증과 관련된 중요 정책, 설정 및 클라이언트 속성

다음은 권장되는 세 가지 구성에서 중요한 역할을 하는 정책, 설정 및 클라이언트 속성입니다.

MDX 정책

앱 암호: 커짐인 경우, 앱을 시작하거나 비활성화된 후 다시 시작할 때 앱 잠금을 해제하려면 Citrix PIN 또는 암호가 필요합니다. 기본값은 커짐입니다.

모든 앱에 대해 비활성화 타이머를 구성하려면 XenMobile 콘솔에서 설정 탭의 클라이언트 속성에서 INACTIVITY_TIMER 값을 분으로 설정합니다. 기본값은 15 분입니다. 비활성화 타이머를 사용하지 않고 앱을 시작할 때만 PIN 또는 암호 입력 메시지가 표시되도록 하려면 값을 0 으로 설정합니다.

참고:

암호화키정책에 대해 보안 오프라인을 선택하는 경우 이 정책이 자동으로 사용됩니다.

온라인 세션 필요: 꺼짐인 경우, 사용자가 엔터프라이즈 네트워크에 연결되어 있고 세션이 활성 상태여야 장치의 앱에 액세스할 수 있습니다. 꺼짐인 경우 활성 세션이 없어도 장치의 앱에 액세스할 수 있습니다. 기본값은 꺼짐입니다.

최대 오프라인 기간 (시간): XenMobile 에서 앱 권한 부여 재확인 및 정책 새로고침 없이 앱을 실행할 수 있는 최대 기간을 정의합니다. 최대 오프라인 기간을 설정하는 경우 iOS 용 Secure Hub 에 유효한 NetScaler Gateway 토큰이 있으면 앱이 사용자 작업 중단 없이 XenMobile 에서 MDX 앱에 대한 새 정책을 검색합니다. Secure Hub 에 유효한 NetScaler 토큰이 없는 경우 앱 정책을 업데이트하려면 사용자가 Secure Hub 를 통해 인증해야 합니다. NetScaler Gateway 세션이 비활성화되거나 세션 시간 초과 정책이 적용되는 경우 NetScaler 토큰이 무효화될 수 있습니다. 사용자가 Secure Hub 에 다시 로그인하면 앱을 계속 실행할 수 있습니다.

이 기간이 만료되기 30 분, 15 분 및 5 분 전에 사용자에게 로그인하라는 메시지가 표시되며 이 기간이 만료되면 사용자가 로그인할 때까지 앱은 잠금 상태를 유지합니다. 기본값은 **72 시간 (3 일)**입니다. 최소 기간은 1 시간입니다.

참고:

사용자가 이동이 잦고 해외 로밍을 사용해야 할 수 있는 시나리오의 경우 72 시간 (3 일) 의 기본값이 너무 짧을 수 있습니다.

백그라운드 서비스 티켓 만료: 백그라운드 네트워크 서비스 티켓이 유효한 기간입니다. Secure Mail 이 NetScaler Gateway 를 통해 ActiveSync 를 실행하는 Exchange Server 에 연결하는 경우 XenMobile 에서 Secure Mail 이 내부 Exchange Server 에 연결하는데 사용할 토큰을 발급합니다. 이 속성 설정에 따라 Secure Mail 이 인증 및 Exchange Server 에 대한 연결에 사용할 새 토큰을 요구하지 않고 토큰을 사용할 수 있는 기간이 결정됩니다. 시간 제한이 만료되면 사용자가 다시 로그인해야 새 토큰이 생성됩니다. 기본값은 **168 시간 (7 일)**입니다. 이 시간 제한이 만료되면 메일 알림이 중단됩니다.

온라인 세션에 필요한 유효 기간 (분): 온라인 세션 필요 정책에 따라 앱을 더 이상 사용하지 못하게 될 때까지 온라인 세션의 유효성이 검사되지 않고도 사용자가 앱을 오프라인으로 사용할 수 있는 시간 (분) 을 결정합니다. 기본값은 0(유효 기간 없음)입니다.

MDX Toolkit 인증 정책에 대한 자세한 내용은 [iOS 용 XenMobile MDX 정책](#) 및 [Android 용 XenMobile MDX 정책](#) 을 참조하십시오.

XenMobile 클라이언트 속성

참고:

클라이언트 속성은 XenMobile 에 연결하는 모든 장치에 적용되는 글로벌 설정입니다.

Citrix PIN: 단순한 로그인 환경을 제공하려면 Citrix PIN 을 사용하도록 선택할 수 있습니다. PIN 을 사용하면 사용자가 Active Directory 사용자 이름 및 암호 같은 다른 자격 증명을 반복적으로 입력하지 않아도 됩니다. Citrix PIN 을 독립 실행형 오프라인 인증으로만 구성하거나 PIN 을 Active Directory 암호 캐시와 결합하여 인증을 간소화함으로써 사용 편의성을 최적화할 수 있습니다. XenMobile 콘솔의 설정 > 클라이언트 > 클라이언트 속성에서 Citrix PIN 을 구성할 수 있습니다.

다음은 몇 가지 속성을 요약한 것입니다. 자세한 내용은 [클라이언트 속성](#) 에서 참조하십시오.

ENABLE_PASSCODE_AUTH

표시 이름: Enable Citrix PIN Authentication(Citrix PIN 인증 사용)

이키를 사용하여 Citrix PIN 기능을 활성화할 수 있습니다. Citrix PIN 또는 암호를 사용하는 경우 Active Directory 암호 대신 사용할 PIN 을 정의하라는 메시지가 나타납니다. **ENABLE_PASSWORD_CACHING** 을 사용하도록 설정했거나 XenMobile 에서 인증서 인증을 사용하는 경우 이 설정을 사용하도록 설정해야 합니다.

가능한 값: **true** 또는 **false**

기본 값: **false**

ENABLE_PASSWORD_CACHING

** 표시 이름: **Enable User Password Caching(사용자 암호 캐싱 사용)

이키를 사용하면 사용자의 Active Directory 암호가 모바일 장치에 로컬로 캐싱됩니다. 이키를 true 로 설정하면 Citrix PIN 또는 암호를 설정하라는 메시지가 사용자에게 표시됩니다. 이키를 **true** 로 설정하는 경우 **ENABLE_PASSCODE_AUTH** 키를 true 로 설정해야 합니다.

가능한 값: **true** 또는 **false**

기본 값: **false**

PASSCODE_STRENGTH

표시 이름: PIN Strength Requirement(PIN 강도 요구 사항)

이키는 Citrix PIN 또는 암호의 강도를 정의합니다. 이 설정을 변경하면 사용자가 다음 번에 인증을 수행할 때 Citrix PIN 또는 암호를 설정하라는 메시지가 나타납니다.

가능한 값: **Low**(낮음), **Medium**(중간) 또는 **Strong**(강함)

기본 값: **Medium**(중간)

INACTIVITY_TIMER

표시 이름: Inactivity Timer(비활성 타이머)

이키는 사용자가 장치를 비활성 상태로 둔 후에 Citrix PIN 또는 암호를 입력하라는 메시지가 없이는 앱에 액세스할 수 있는 시간 (분 단위) 을 정의합니다. MDX 앱에 대해 이 설정을 사용하도록 설정하려면 앱 암호 설정을 꺼짐으로 설정해야 합니다. 앱 암호 설정이 꺼짐으로 설정된 경우, 사용자는 전체 인증을 수행하기 위해 Secure Hub 로 리디렉션됩니다. 이 설정을 변경하면 다음에 사용자에게 인증하라는 메시지가 표시될 때 값이 적용됩니다. 기본 값은 15 분입니다.

ENABLE_TOUCH_ID_AUTH

표시 이름: Enable Touch ID Authentication(Touch ID 인증 사용)

오프라인 인증에서 지문 판독기 (iOS 만 해당) 를 사용할 수 있습니다. 온라인 인증에서는 기본 인증 방법을 사용해야 합니다.

ENCRYPT_SECRETS_USING_PASSCODE

표시 이름: Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)

이키를 사용하면 민감한 데이터를 iOS 키 집합과 같은 플랫폼 기반 기본 저장소가 아닌 모바일 장치의 기밀 저장소에 저장할 수 있습니다. 이 구성 키는 주요 애플 팩트의 강력한 암호화를 활성화하지만 사용자 엔트로피 (사용자만 알고 있는 사용자 생성 임의의 PIN 코드) 도 증가합니다.

가능한값: **true** 또는 **false**

기본값: **false**

NetScaler 설정

Session time-out(세션시간초과): 이설정을 사용하면 NetScaler 에서 지정된 간격 동안 네트워크 활동이 감지되지 않을 경우 NetScaler Gateway 가 세션 연결을 끊습니다. 이 설정은 NetScaler Gateway 플러그인, Citrix Receiver, Secure Hub 또는 웹 브라우저를 통해 연결하는 사용자에게 적용됩니다. 기본값은 **1440** 분입니다. 이 값을 0 으로 설정하면 설정이 사용되지 않습니다.

Forced time-out(시간초과 강제 적용): 이 설정을 사용하면 NetScaler Gateway 가 시간초과 간격이 지난 후 사용자의 활동이 부와 관계없이 세션 연결을 끊습니다. 시간초과 간격이 경과하면 사용자는 어떠한 작업으로도 연결 종단을 방지할 수 없습니다. 이 설정은 NetScaler Gateway 플러그인, Citrix Receiver, Secure Hub 또는 웹 브라우저를 통해 연결하는 사용자에게 적용됩니다. Secure Mail 에서 특수 NetScaler 모드인 STA 를 사용하는 경우 Secure Mail 세션에는 시간초과 강제 적용 설정이 적용되지 않습니다. 기본값은 **1440** 분입니다. 이 값을 비워두면 설정이 사용되지 않습니다.

NetScaler Gateway 의 시간초과 설정에 대한 자세한 내용은 NetScaler 설명서를 참조하십시오.

장치에서 자격 증명을 입력하여 XenMobile 을 통해 인증 하라는 메시지를 사용자에게 표시하는 시나리오에 대한 자세한 내용은 [인증 프롬프트 시나리오](#) 를 참조하십시오.

기본 구성 설정

다음 설정은 XenMobile 용 NetScaler 마법사, MDX Toolkit 및 XenMobile 콘솔에서 제공되는 기본값입니다.

설정	설정을 찾는 위치	기본 설정
세션 시간 초과	NetScaler Gateway	1440 분
Force time-out(강제 시간 초과)	NetScaler Gateway	1440 분
최대 오프라인 기간	MDX 정책	72 시간
백그라운드 서비스 티켓 만료	MDX 정책	168 시간 (7 일)
온라인 세션 필요	MDX 정책	꺼짐
온라인 세션에 필요한 유효 기간	MDX 정책	0
앱 암호	MDX 정책	켜짐
Encrypt secrets using Passcode(암호를 사용하여 암호 암호화)	XenMobile 클라이언트 속성	False

설정	설정을찾는위치	기본설정
Enable Citrix PIN Authentication(Citrix PIN 인증 사용)	XenMobile 클라이언트속성	False
PIN Strength Requirement(PIN 강도요구사항)	XenMobile 클라이언트속성	중간
PIN Type(PIN 유형)	XenMobile 클라이언트속성	숫자
Enable User Password Caching(사용자암호캐싱사용)	XenMobile 클라이언트속성	False
Inactivity Timer(비활성화타이머)	XenMobile 클라이언트속성	15
Enable Touch ID Authentication(Touch ID 인증 사용)	XenMobile 클라이언트속성	False

권장되는구성

이 섹션에서는 가장 낮은 수준의 보안과 최적의 사용자 환경부터 가장 높은 수준의 보안과 좀 더 불편한 사용자 환경에 이르는 세 가지 XenMobile 구성예제를 제공합니다. 이러한 예제는 자체 구성을 적용할 위치를 결정할 때 유용한 참조로 사용될 수 있습니다. 이러한 설정을 수정하려면 다른 설정도 함께 변경해야 합니다. 예를 들어 최대 오프라인 기간은 세션 시간 초과보다 작아야 합니다.

최고 수준의 보안

이 구성은 가장 높은 수준의 보안을 제공하지만 사용 편의성이 크게 떨어지는 단점이 있습니다.

설정	설정을찾는위치	권장되는설정	동작의영향
세션시간초과	NetScaler Gateway	1440	사용자는 온라인 인증이 요구되는 경우에만 24 시간마다 Secure Hub 자격 증명을 입력합니다.
Force time-out(강제시간초과)	NetScaler Gateway	1440	온라인 인증이 24 시간마다 엄격히 요구됩니다. 활동이 있다고 해서 세션 수명이 연장되지는 않습니다.

최대오프라인기간	MDX 정책	23	매일정책을새로고쳐야합니다.
백그라운드서비스티켓만료	MDX 정책	72 시간	STA 에대한시간제한으로, NetScaler Gateway 세션토큰없이세션수명을연장할수있습니다. Secure Mail 의경우 STA 시간초과를세션시간초과보다길게설정하면사용자가세션이만료되기전에앱을열지않은경우사용자에게메시지를표시하지않고메일알림이중지되는상황을방지할수있습니다.
온라인세션필요	MDX 정책	꺼짐	유효한네트워크연결및 NetScaler Gateway 세션에서앱을사용할수있습니다.
온라인세션에필요한유예기간	MDX 정책	0	유예기간이없습니다 (온라인세션필요를사용하는경우).
앱암호	MDX 정책	켜짐	응용프로그램에대한암호가필요합니다.
Encrypt secrets using Passcode(암호를사용하여암호암호화)	XenMobile 클라이언트속성	true	사용자엔트로피에서파생된키로저장소를보호합니다.
Enable Citrix PIN Authentication(Citrix PIN 인증사용)	XenMobile 클라이언트속성	true	Citrix PIN 을사용하여사용자인증환경을간소화합니다.
PIN Strength Requirement(PIN 강도 요구사항)	XenMobile 클라이언트속성	Strong(강함)	높은수준의암호복잡성을요구합니다.
PIN Type(PIN 유형)	XenMobile 클라이언트속성	영숫자	영숫자시퀀스의 PIN 을사용합니다.

Enable Password Caching(암호캐싱사용)	XenMobile 클라이언트속성	False	Active Directory 암호는 캐싱되지 않으며오프라인인증의 경우 Citrix PIN 이사용됩니다.
Inactivity Timer(비활성화타이머)	XenMobile 클라이언트속성	15	사용자가이기간에 MDX 앱 또는 Secure Hub 를사용하지 않으면오프라인인증에 대한메시지가표시됩니다.
Enable Touch ID Authentication(Touch ID 인증사용)	XenMobile 클라이언트속성	False	iOS 에서오프라인인증에 대해 Touch ID 를사용하지 않도록설정합니다.

더높은수준의보안

중도에가까운접근방식인이구성은 7 일대신최대 3 일에한번씩사용자인증을요구하고보안을강화합니다. 인증횟수가증가하여컨테이너가더자주잠기므로장치를사용하지않을때의데이터보안이강화됩니다.

설정	설정을찾는위치	권장되는설정	동작의영향
세션시간초과	NetScaler Gateway	4320	사용자는온라인인증이요구되는경우에만 3 일마다 Secure Hub 자격증명을입력합니다.
Force time-out(강제시간초과)	NetScaler Gateway	값을지정하지않음	활동이있는경우세션이연장됩니다.
최대오프라인기간	MDX 정책	71	정책을 3 일마다새로고쳐야합니다. 시간차이를두면세션시간초과전에정책을새로고칠수있습니다.

백그라운드서비스티켓만료	MDX 정책	168 시간	STA 에대한시간제한으로, NetScaler Gateway 세션토큰없이세션수명을연장할수있습니다. Secure Mail 의경우 STA 시간초과를세션시간초과보다길게설정하면사용자가세션이만료되기전에앱을열지않은경우 사용자에게메시지를표시하지않고메일알림이중지되는상황을방지할수있습니다.
온라인세션필요	MDX 정책	꺼짐	유효한네트워크연결및 NetScaler Gateway 세션에서앱을사용할수있습니다.
온라인세션에필요한유예기간	MDX 정책	0	유예기간이없습니다 (온라인세션필요를사용하는경우).
앱암호	MDX 정책	켜짐	응용프로그램에대한암호가필요합니다.
Encrypt secrets using Passcode(암호를사용하여암호암호화)	XenMobile 클라이언트속성	False	사용자엔트로피없이저장소를암호화할수있습니다.
Enable Citrix PIN Authentication(Citrix PIN 인증사용)	XenMobile 클라이언트속성	true	Citrix PIN 을사용하여사용자인증환경을간소화합니다.
PIN Strength Requirement(PIN 강도 요구사항)	XenMobile 클라이언트속성	중간	중간수준의암호복잡성규칙을적용합니다.
PIN Type(PIN 유형)	XenMobile 클라이언트속성	숫자	숫자시퀀스의 PIN 을사용합니다.
Enable Password Caching(암호캐싱사용)	XenMobile 클라이언트속성	true	사용자 PIN 이캐싱되고 Active Directory 암호를보호하는데사용됩니다.

Inactivity Timer(비활성화 타이머)	XenMobile 클라이언트 속성	30	사용자가 이 기간에 MDX 앱 또는 Secure Hub 를 사용하지 않으면 오프라인 인증에 대한 메시지가 표시됩니다.
Enable Touch ID Authentication(Touch ID 인증 사용)	XenMobile 클라이언트 속성	true	iOS 에서 오프라인 인증에 대해 Touch ID 를 사용하도록 설정합니다.

높은 수준의 보안

이 구성은 사용자에게 가장 편리한 환경과 기본 수준의 보안을 제공합니다.

설정	설정을 찾는 위치	권장되는 설정	동작의 영향
세션 시간 초과	NetScaler Gateway	10080	사용자는 온라인 인증이 요구되는 경우에만 7 일마다 Secure Hub 자격 증명을 입력합니다.
Force time-out(강제 시간 초과)	NetScaler Gateway	값을 지정하지 않음	활동이 있는 경우 세션이 연장됩니다.
최대 오프라인 기간	MDX 정책	167	정책을 매주 (7 일마다) 새로 고쳐야 합니다. 시간 차이를 두면 세션 시간 초과 전에 정책을 새로 고칠 수 있습니다.
백그라운드 서비스 티켓 만료	MDX 정책	240	STA 에 대한 시간 제한으로, NetScaler Gateway 세션 토큰 없이 세션 수명을 연장할 수 있습니다. Secure Mail 의 경우 STA 시간 초과를 세션 시간 초과보다 길게 설정하면 사용자가 세션 만료되기 전에 앱을 열지 않은 경우 사용자에게 메시지를 표시하지 않고 메일 알림이 중지되는 상황을 방지할 수 있습니다.

온라인세션필요	MDX 정책	꺼짐	유효한네트워크연결및 NetScaler Gateway 세션에서앱을사용할수있습니다.
온라인세션에필요한유예기간	MDX 정책	0	유예기간이없습니다 (온라인세션필요를사용하는경우).
앱암호	MDX 정책	켜짐	응용프로그램에대한암호가 필요합니다.
Encrypt secrets using Passcode(암호를사용하여암호암호화)	XenMobile 클라이언트속성	False	사용자엔트로피없이저장소를암호화할수있습니다.
Enable Citrix PIN Authentication(Citrix PIN 인증사용)	XenMobile 클라이언트속성	true	Citrix PIN 을사용하여사용자인증환경을간소화합니다.
PIN Strength Requirement(PIN 강도 요구사항)	XenMobile 클라이언트속성	Low(낮음)	암호복잡성을요구하지않습니다.
PIN Type(PIN 유형)	XenMobile 클라이언트속성	숫자	숫자시퀀스의 PIN 을사용합니다.
Enable Password Caching(암호캐싱사용)	XenMobile 클라이언트속성	true	사용자 PIN 이캐싱되고 Active Directory 암호를 보호하는데사용됩니다.
Inactivity Timer(비활성화타이머)	XenMobile 클라이언트속성	90	사용자가이기간에 MDX 앱 또는 Secure Hub 를사용하지않으면오프라인인증에 대한메시지가표시됩니다.
Enable Touch ID Authentication(Touch ID 인증사용)	XenMobile 클라이언트속성	true	iOS 에서오프라인인증에 대해 Touch ID 를사용하도록 설정합니다.

상위단계인증사용

일부앱에는항상된인증 (예: 토큰또는적극적세션시간초과같은보조인증요소) 이필요할수있습니다. 이인증방법을 MDX 정책을통해제어할수있습니다. 또한이방법을사용하려면별개의가상서버를사용하여동일하거나다른 NetScaler 장비에서인증방법을제어

해야합니다.

설정	설정을찾는위치	권장되는설정	동작의영향
대체 NetScaler Gateway	MDX 정책	보조 NetScaler 장비의 FQDN 및포트가필요합니다.	보조 NetScaler 장비인증 및세션정책을사용하여향상된인증을제어할수있습니다.

사용자가대체 NetScaler Gateway 인스턴스로그온하는앱을열면다른모든앱이이 NetScaler Gateway 인스턴스를사용하여내부네트워크와통신합니다. 세션은향상된보안을사용하는 NetScaler Gateway 인스턴스에서세션이시간초과되는경우에만하위수준의보안을사용하는 NetScaler Gateway 인스턴스로전환됩니다.

온라인세션필요사용

Secure Web 같은특정응용프로그램의경우사용자세션이인증되고장치가인터넷에연결된동안에만사용자의앱실행을허용해야할수있습니다. 이정책을사용하면이옵션이적용되고유예기간동안사용자가작업을마칠수있습니다.

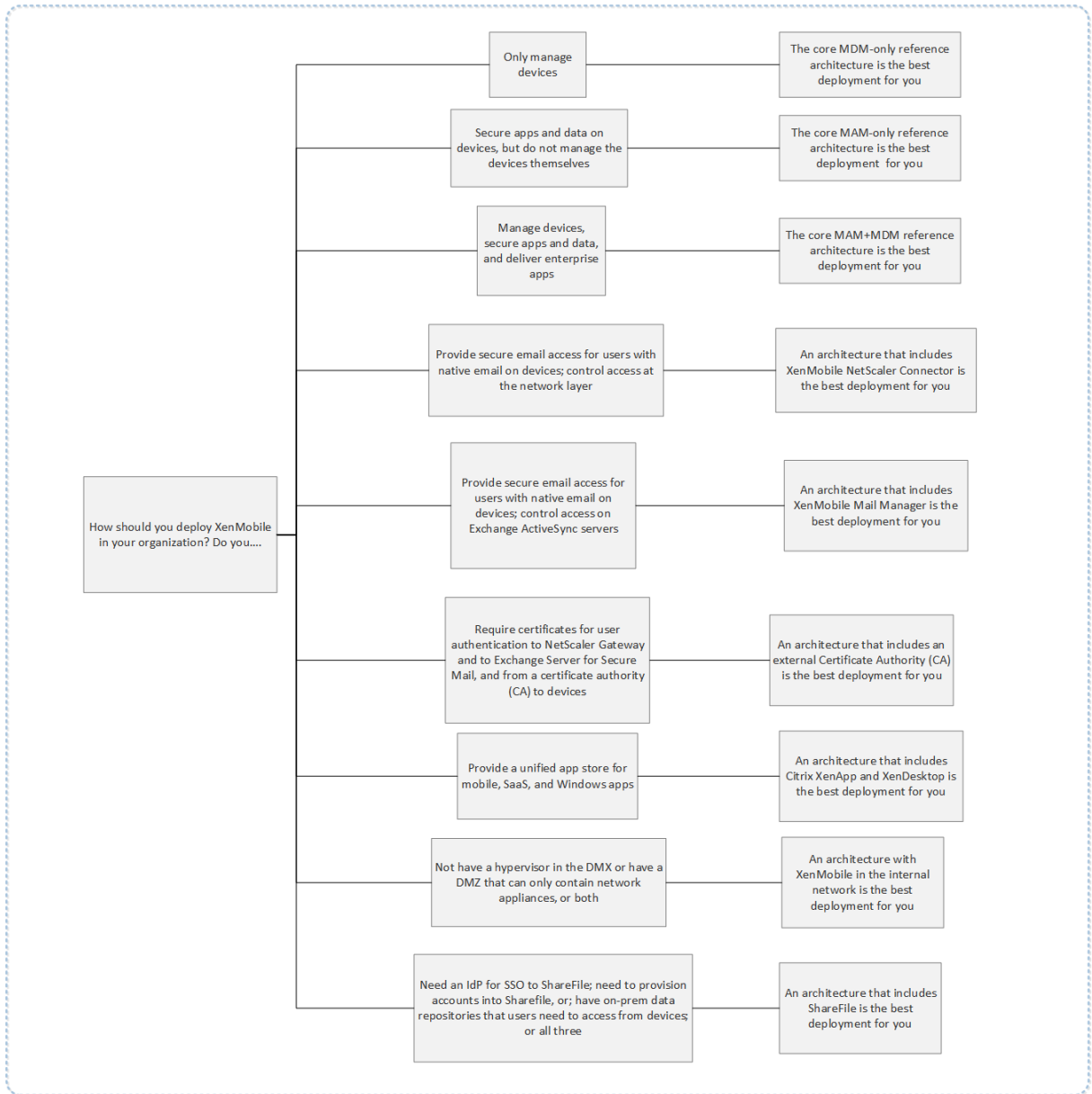
설정	설정을찾는위치	권장되는설정	동작의영향
온라인세션필요	MDX 정책	켜짐	장치가온라인상태이고유효한인증토큰이있는지확인합니다.
온라인세션에필요한유예기간	MDX 정책	15	사용자의앱사용을중지하기전에 15 분의유예기간을허용합니다.

온-프리미스배포용참조아키텍처

January 6, 2020

이문서의그림은 XenMobile 의온-프리미스배포에대한참조아키텍처를설명합니다. 배포시나리오에는 MDM 전용, MAM 전용 및 MDM+MAM 을핵심아키텍처로배포하는시나리오와 SNMP Manager, Exchange ActiveSync 용 Citrix Gateway 커넥터, Exchange ActiveSync 용 Endpoint Management 커넥터및 Virtual Apps and Desktops 같은구성요소를포함하는배포시나리오가포함됩니다. 그림에는 XenMobile 에필요한최소구성요소가나와있습니다.

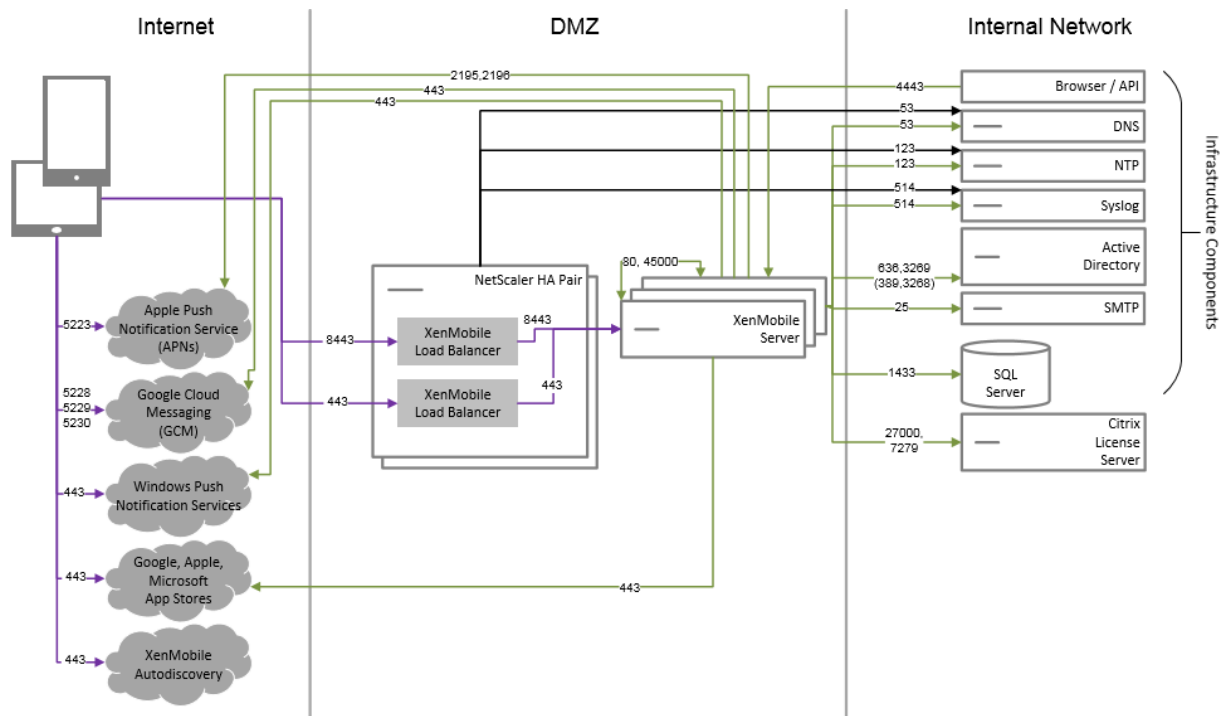
이차트를배포의사결정의일반지침으로사용하십시오.



그림에서 커넥터 위쪽의 숫자는 구성요소 간 연결을 허용하기 위해 열어야 하는 포트를 나타냅니다. 전체 포트 목록은 XenMobile 설명서에서 [포트요구사항](#)을 참조하십시오.

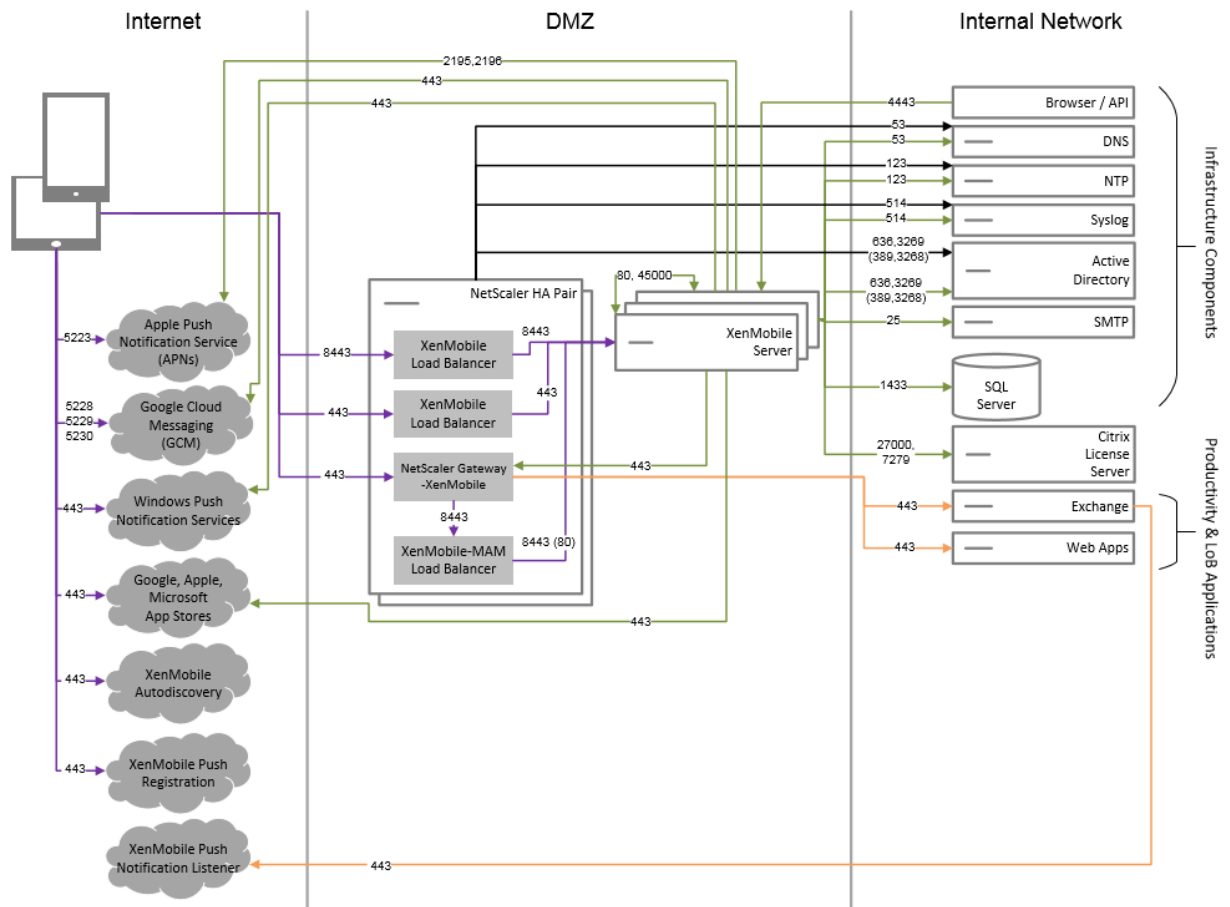
핵심 MDM 전용 참조 아키텍처

XenMobile의 MDM 기능만 사용하려는 경우 이 아키텍처를 배포합니다. 예를 들어 회사에서 발급한 장치를 MDM을 통해 관리하여 장치 정책 및 앱을 배포하고, 자산 인벤토리를 검색하고, 장치 초기화 같은 동작을 장치에 수행해야 하는 경우 이 아키텍처를 배포합니다.



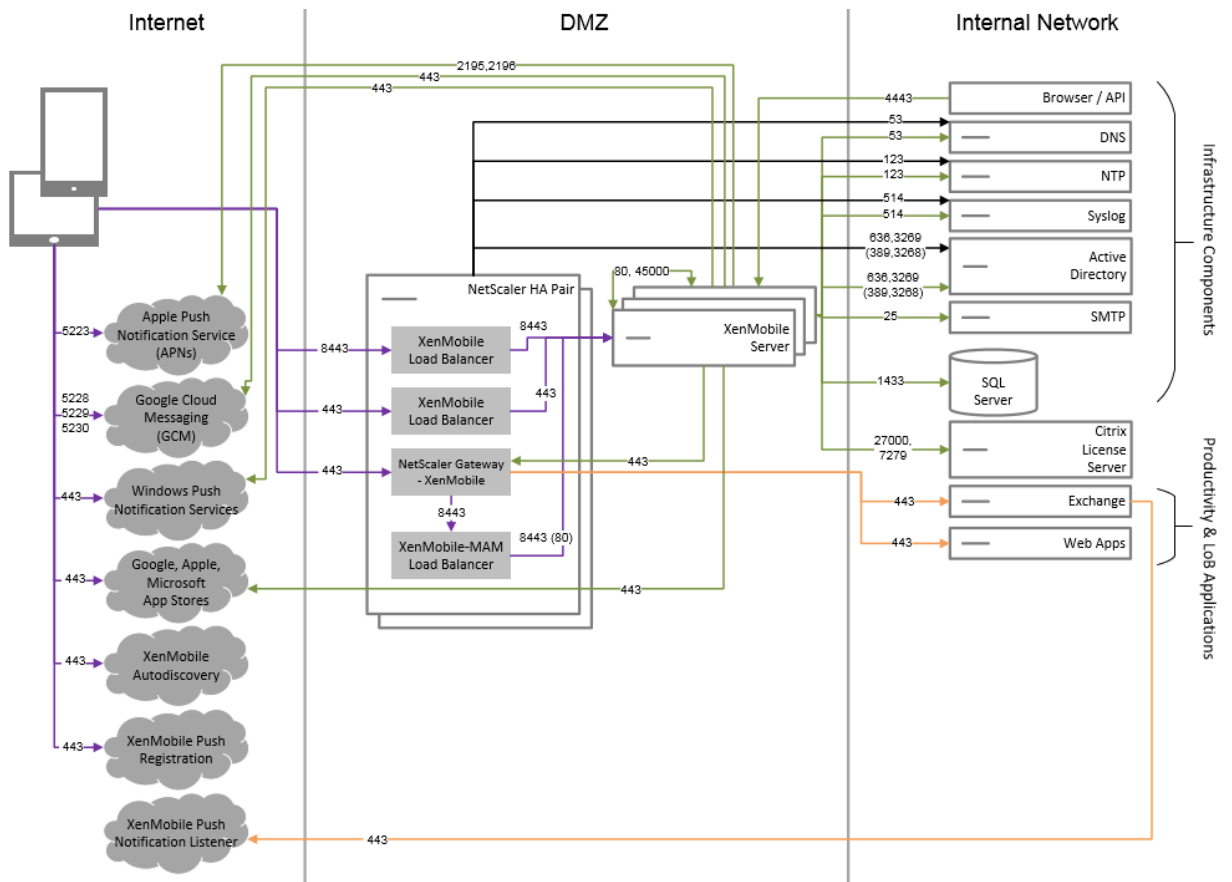
핵심 **MAM** 전용참조아키텍처

MDM 에대한장치등록없이 XenMobile 의 MAM 기능만사용하려는경우이아키텍처를배포합니다. 예를들어 BYO 모바일장치 의앱및데이터를보호하려는경우와엔터프라이즈모바일앱을제공하고앱잠금및데이터초기화기능을사용하려는경우이아키텍처를 배포할수있습니다. 장치를 MDM 에등록할수없습니다.



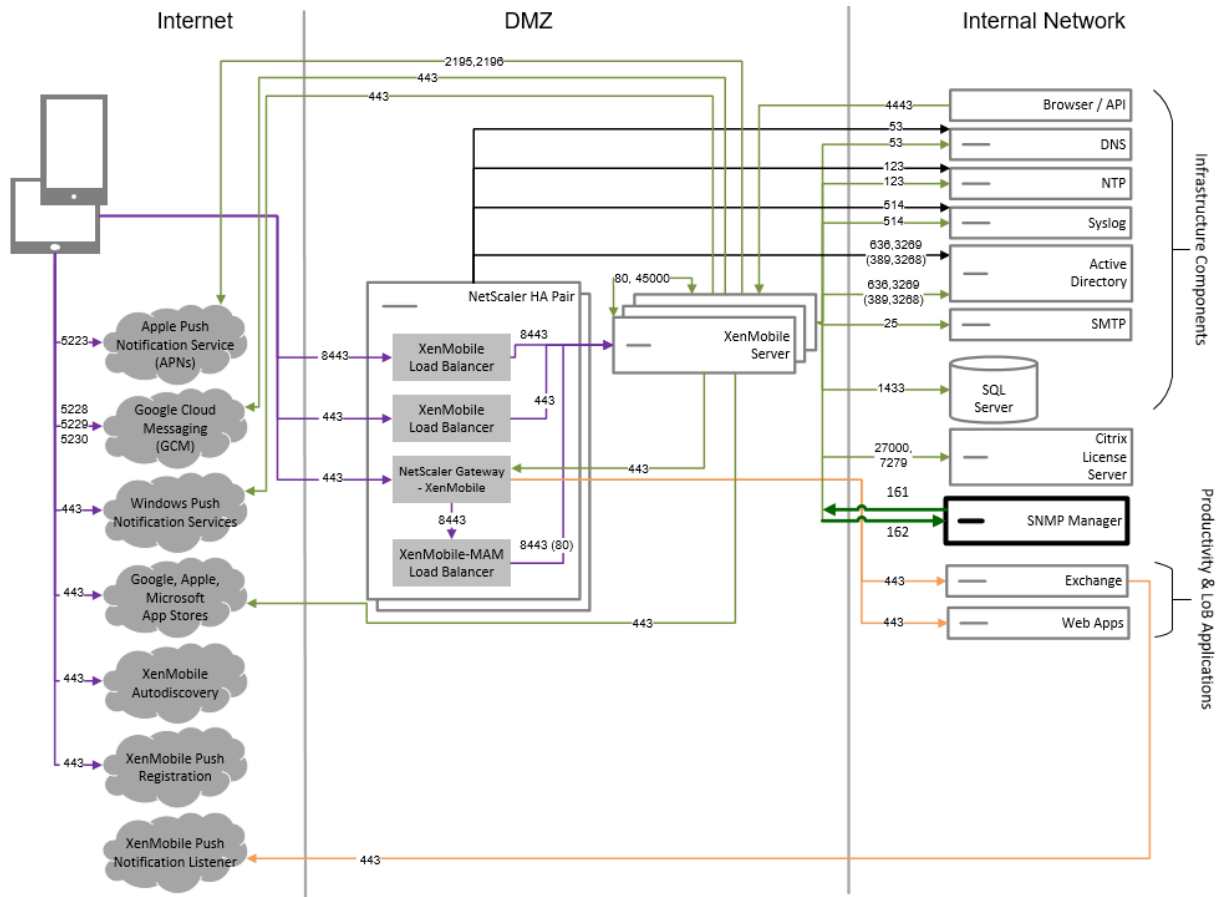
핵심 **MAM+MDM** 참조아키텍처

XenMobile의 MDM+MAM 기능을 사용하려는 경우 이 아키텍처를 배포합니다. 예를 들어 회사가 발급한 장치를 MDM을 통해 관리하려는 경우, 장치 정책 및 앱을 배포하려는 경우, 자산 인벤토리를 검색하고 장치를 초기화하는 기능을 사용하려는 경우 이 아키텍처를 배포합니다. 또한 엔터프라이즈 모바일 앱을 제공하고 앱 잠금 및 장치의 데이터 초기화 기능을 사용하려는 경우에도 이 아키텍처를 배포할 수 있습니다.



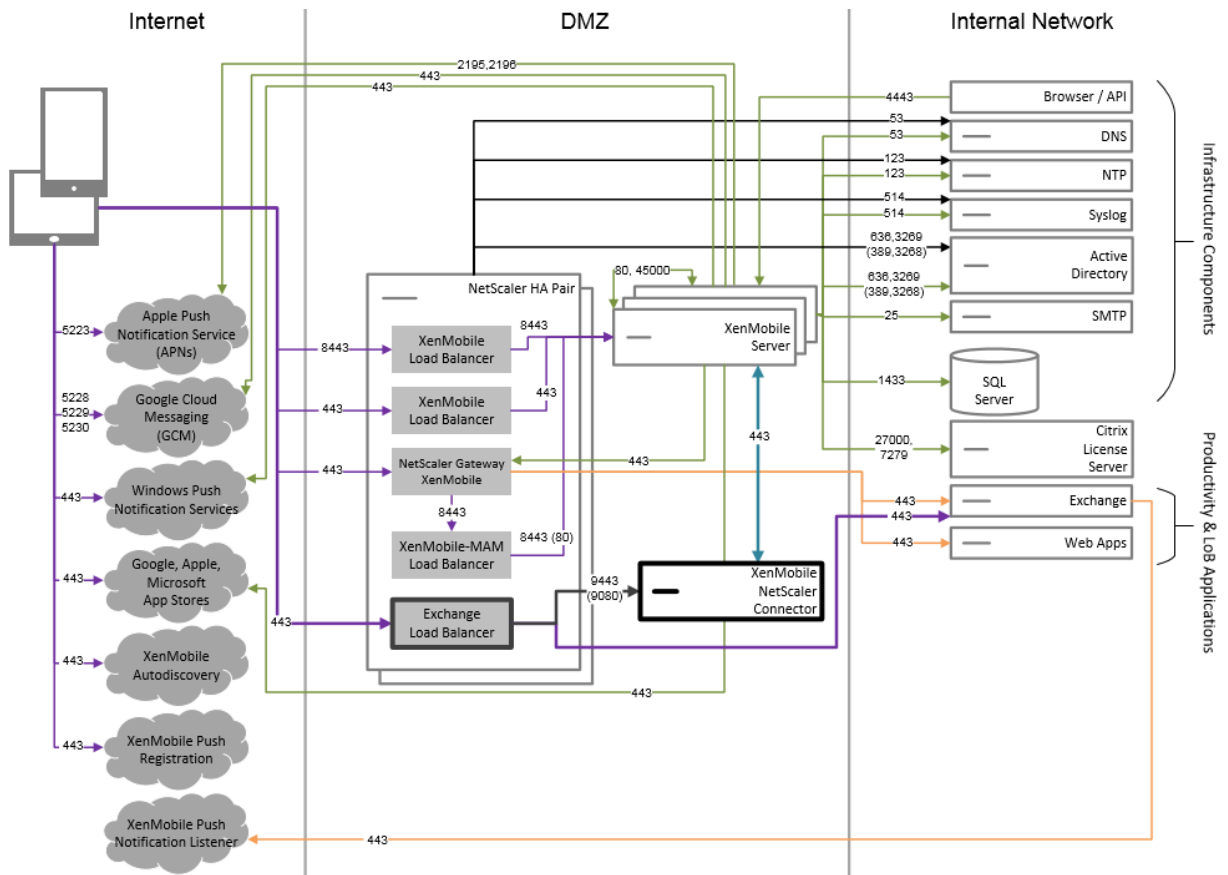
SNMP 를사용하는참조아키텍처

XenMobile 과함께 SNMP 모니터링을사용하려는경우이아키텍처를배포합니다. 예를들어모니터링시스템이 XenMobile 노드를쿼리하고노드의정보를가져오도록허용하려는경우이아키텍처를배포할수있습니다. 자세한내용은 [SNMP 모니터링](#)에서참조하십시오.



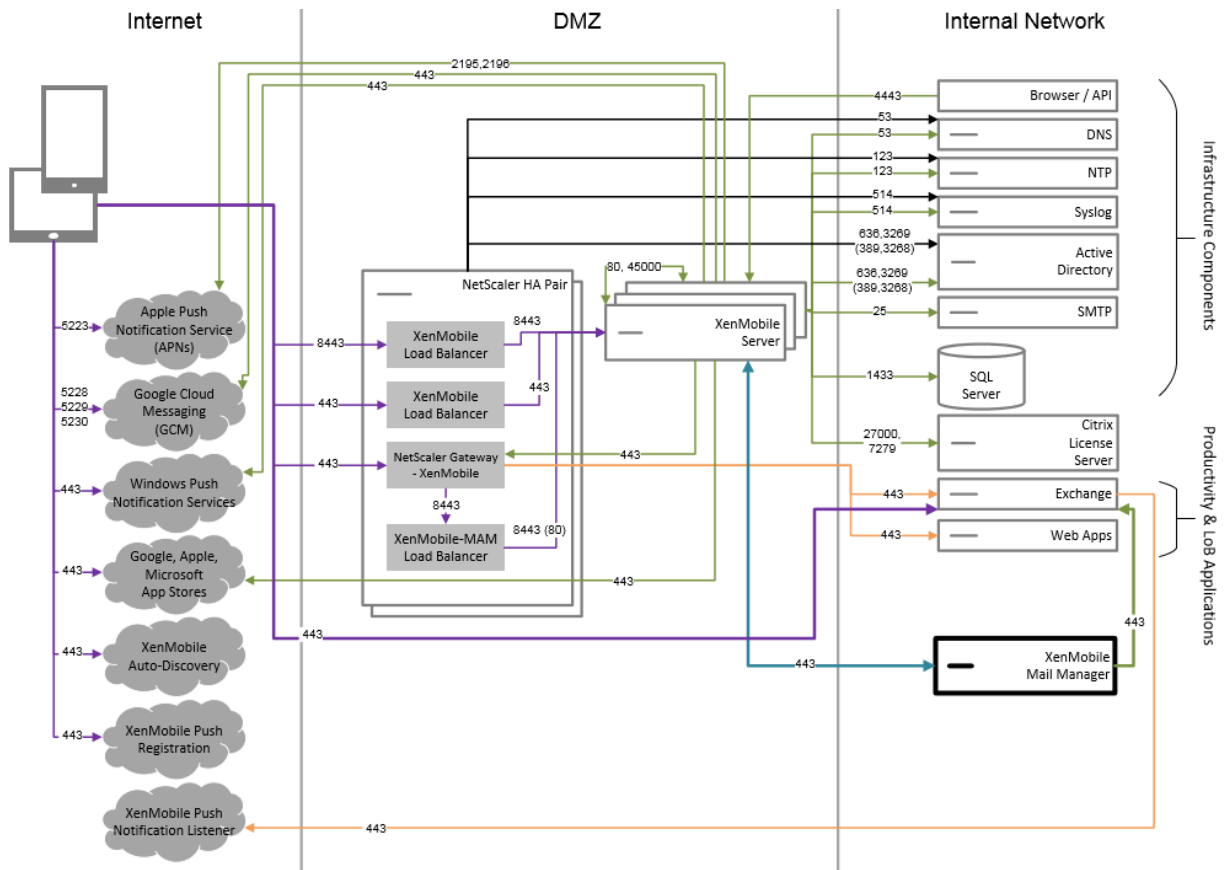
Exchange ActiveSync 용 Citrix Gateway 커넥터가 포함된 참조 아키텍처

XenMobile 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어 기본 모바일 전자메일 앱을 사용하는 사용자에게 보안 전자메일 액세스를 제공해야 하는 경우 이 아키텍처를 배포할 수 있습니다. 이러한 사용자는 계속해서 기본 앱을 통해 전자메일에 액세스하거나 시간이 지남에 따라 Citrix Secure Mail 로 전환할 수 있습니다. 액세스 제어는 트래픽이 Exchange Active Sync 서버에 도달하기 전에 네트워크 계층에서 수행되어야 합니다. 다이어그램에는 Exchange ActiveSync 용 커넥터가 MDM 과 MAM 아키텍처에 배포된 것으로 표시되었지만 Exchange ActiveSync 용 커넥터를 동일한 방식으로 MDM 전용 아키텍처의 일부로 배포할 수도 있습니다.



Exchange ActiveSync 용 Endpoint Management 커넥터가 포함된 참조 아키텍처

XenMobile 에서 Exchange ActiveSync 용 Endpoint Management 커넥터를 사용할 계획이라면 이 아키텍처를 배포하십시오. 예를 들어 기본 모바일 전자메일 앱을 사용하는 사용자에게 보안 전자메일 액세스를 제공해야 하는 경우 이 아키텍처를 배포할 수 있습니다. 이러한 사용자는 계속해서 기본 앱을 통해 전자메일에 액세스하거나 시간이 지남에 따라 Secure Mail 로 전환할 수 있습니다. 액세스 제어는 Exchange ActiveSync 서버에서 수행할 수 있습니다. 다이어그램에는 MDM 및 MAM 아키텍처에 배포된 Exchange ActiveSync 용 Endpoint Management 커넥터가 표시되어 있지만 동일한 방식으로 MDM 전용 아키텍처의 일부로 Exchange ActiveSync 용 Endpoint Management 커넥터를 배포할 수도 있습니다.

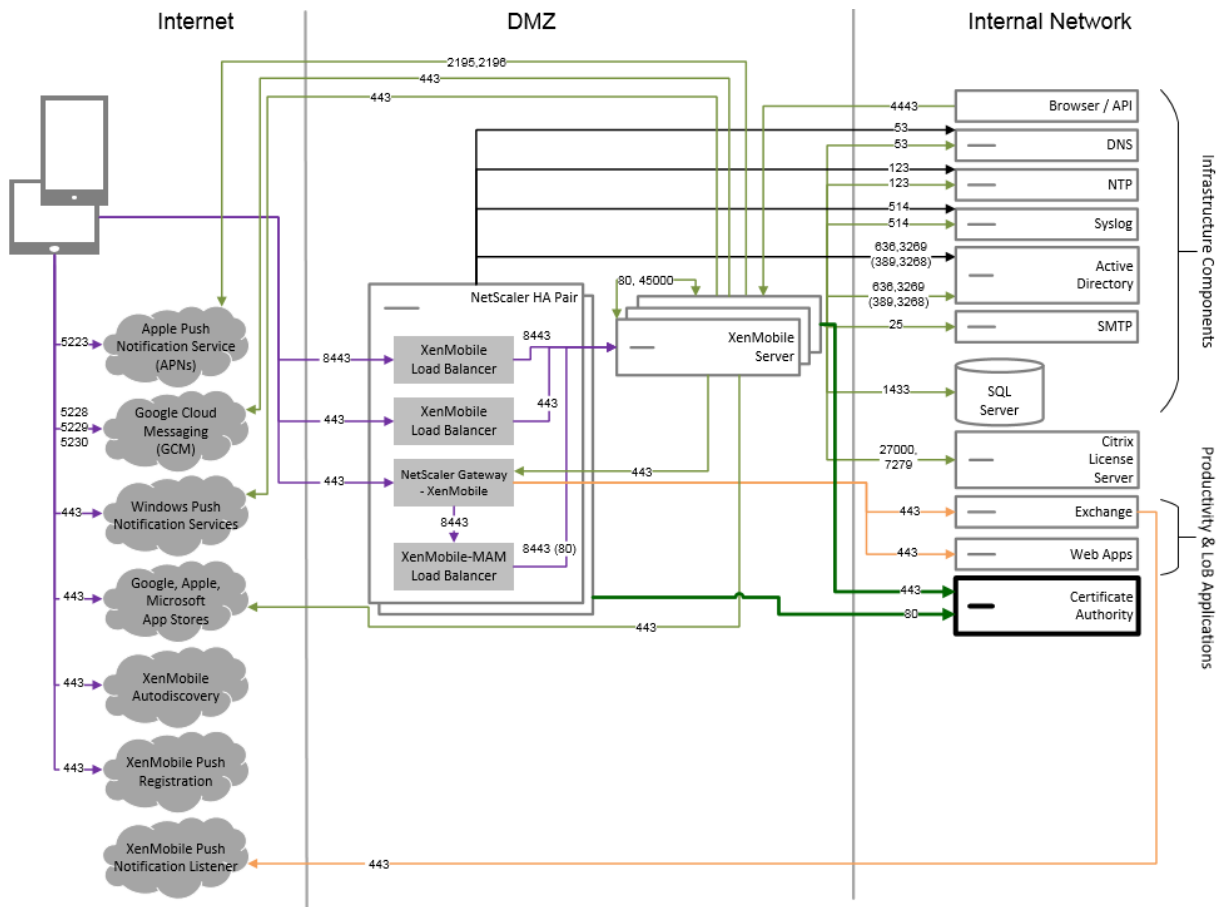


외부인증기관을사용하는참조아키텍처

외부인증기관을포함하는배포는다음요구사항을하나이상충족해야하는경우권장됩니다.

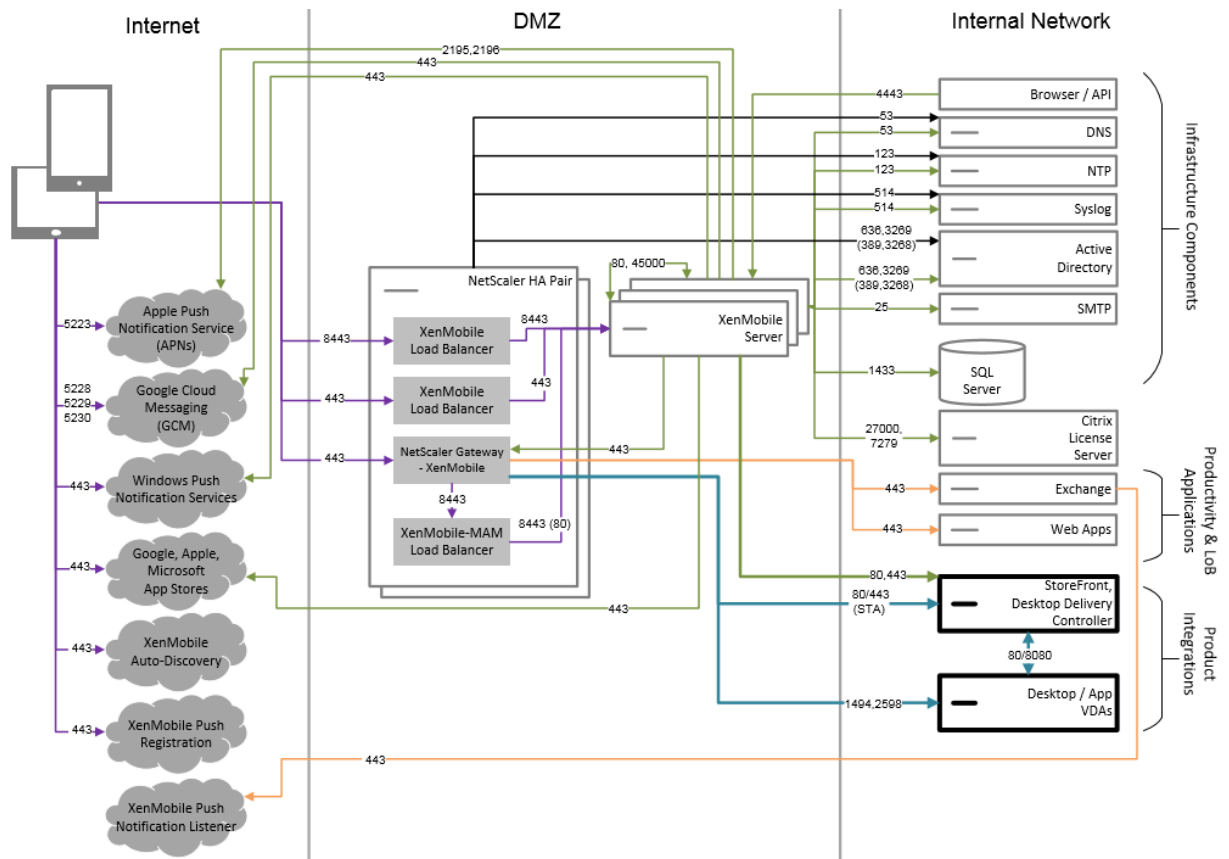
- NetScaler Gateway 에대한사용자인증 (인트라넷액세스) 에사용자인증서를사용해야합니다.
- Secure Mail 사용자에게사용자인증서를사용하여 Exchange Server 에인증하도록해야합니다.
- 회사인증기관에서발급한인증서를모바일장치 (예: WiFi 액세스시) 에푸시해야합니다.

다이어그램에는 MDM+MAM 아키텍처로배포된외부인증기관이표시되어있지만외부인증기관을동일한방식으로 MDM 전용또는 MAM 전용아키텍처의일부로배포할수도있습니다.



Virtual Apps and Desktops 를 사용하는 참조 아키텍처

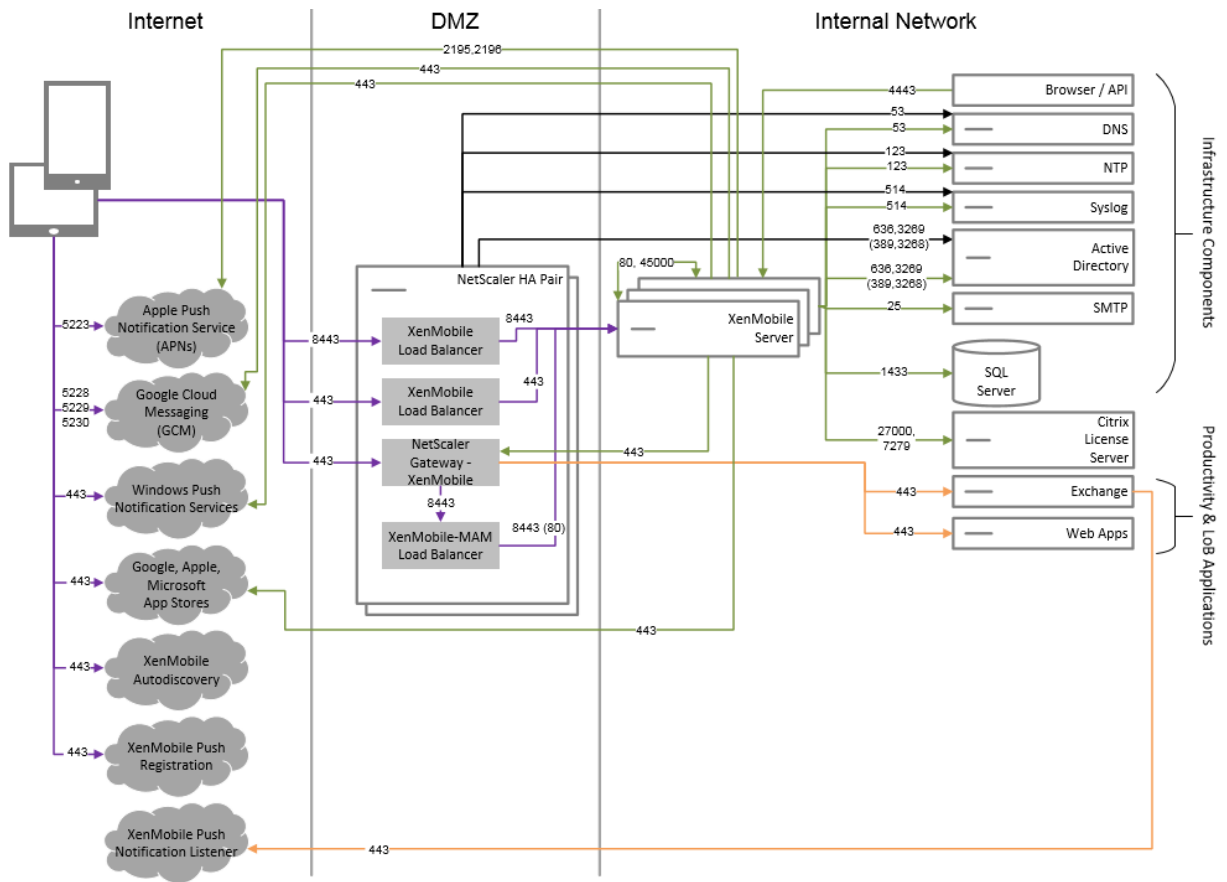
Virtual Apps and Desktops 를 XenMobile 과 통합하려는 경우 이 아키텍처를 배포합니다. 예를 들어 모바일 사용자에게 모든 유형의 응용 프로그램 (모바일, SaaS 및 Windows) 에 대한 통합 앱스토어를 제공해야 하는 경우 이 아키텍처를 배포할 수 있습니다. 다이어그램에는 Virtula Desktops 가 MDM+MAM 아키텍처로 배포된 것으로 표시되었지만 이러한 데스크톱을 동일한 방식으로 MAM 전용 아키텍처의 일부로 배포할 수도 있습니다.



XenMobile 이 내부네트워크에 있는 참조아키텍처

다음요구사항중하나이상을 충족해야하는경우 내부네트워크의 XenMobile 을 사용하는 아키텍처를 배포할 수 있습니다.

- DMZ 에 하이퍼바이저가 없거나 배치할 수 없습니다.
- DMZ 에는 네트워크 장비만 포함되어야 합니다.
- 보안요구사항에 따라 SSL 오프로드를 사용해야 합니다.



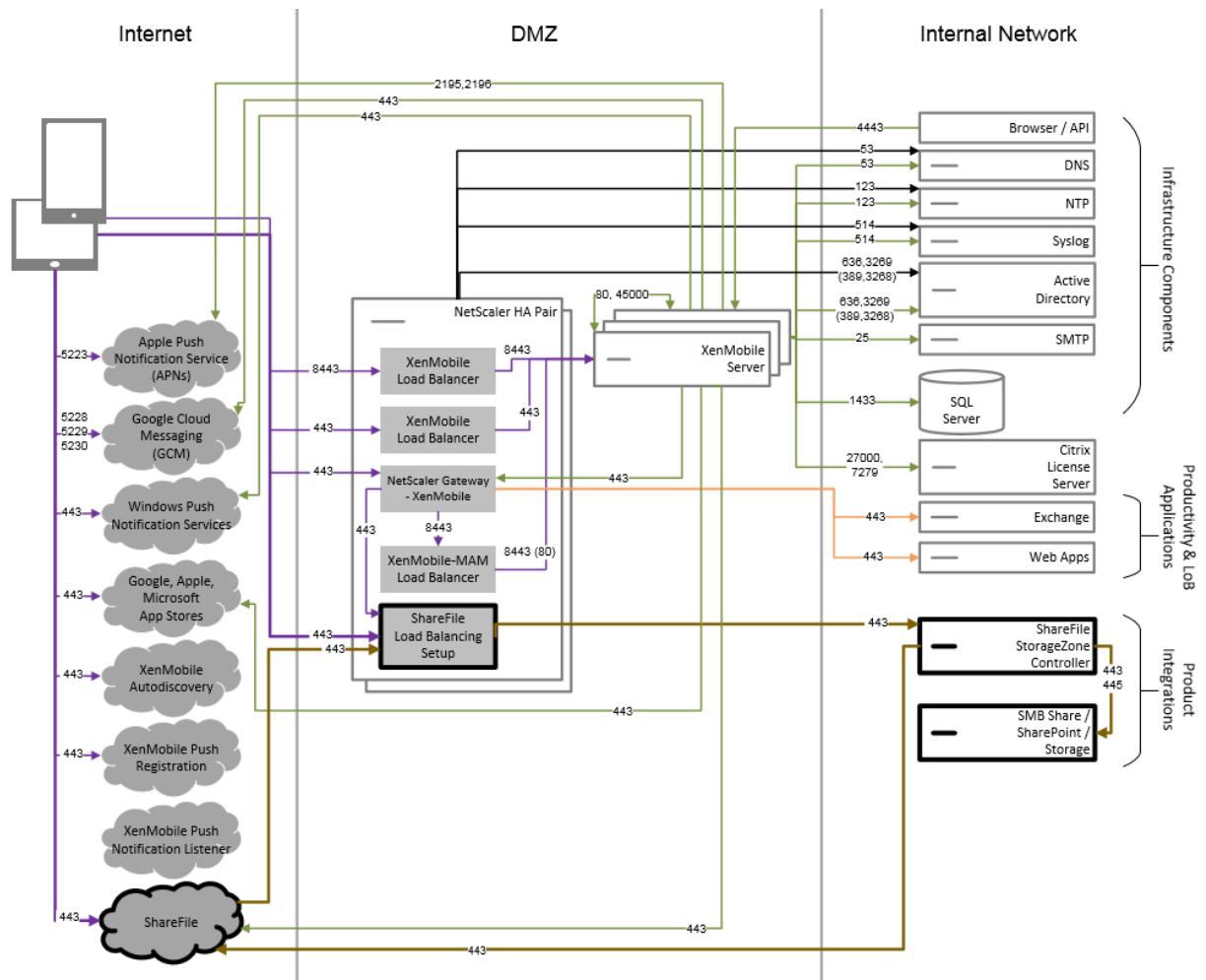
ShareFile 을 사용하는 참조 아키텍처

ShareFile Enterprise 또는 StorageZone 커넥터만 XenMobile 과 통합하려는 경우 이 아키텍처를 배포합니다. ShareFile Enterprise 를 통합하면 다음 요구 사항 중 하나 이상을 충족할 수 있습니다.

- IDP 를 통해 ShareFile.com 에 대한 SSO(Single Sign-on) 를 사용자에게 제공해야 합니다.
- ShareFile.com 에 계정을 프로비전할 수 있어야 합니다.
- 모바일 장치에서 액세스해야 하는 온-프레미스 데이터 저장소가 있습니다.

StorageZone 커넥터만 통합하는 경우 SharePoint 사이트 및 네트워크 파일 공유 등의 기존 온-프레미스 스토리지 저장소에 대한 보안 모바일 액세스를 사용자에게 제공할 수 있습니다. 이 구성에서는 ShareFile 하위 도메인을 설정하거나 사용자를 ShareFile 에 프로비전하거나 ShareFile 데이터를 호스팅할 필요가 없습니다.

다이어그램에는 ShareFile 이 MDM+MAM 아키텍처로 배포된 것으로 표시되었지만 ShareFile 을 동일한 방식으로 MAM 전용 아키텍처의 일부로 배포할 수도 있습니다.



서버속성

January 6, 2020

서버속성은 전체 XenMobile 인스턴스의 작업, 사용자 및 장치에 적용되는 글로벌 속성입니다. 이 문서에서 다루는 서버속성이 현재 환경에 해당하는지 여부를 평가하는 것이 좋습니다. 다른 서버속성을 변경하기 전에 Citrix 에 문의하십시오.

일부 서버속성을 변경하려면 각 XenMobile 서버 노드를 다시 시작해야 합니다. 다시 시작이 필요한 경우 XenMobile 이 알림을 제공합니다.

일부 서버속성은 성능 및 안정성을 개선하는데 도움이 됩니다. 자세한 내용은 [XenMobile 작업 조정](#)에서 참조하십시오.

관리되는 **Google Play Store** 의 모든 앱에 액세스. **true** 인 경우 XenMobile 은 관리되는 Google Play Store 에서 공용 Google Play Store 의 모든 앱에 액세스할 수 있게 합니다. 이 속성을 **true** 로 설정하면 모든 Android Enterprise 사용자에 대한 공용 Google Play Store 앱이 화이트리스트에 추가됩니다. 이후 관리자는 [제한장치 정책](#)을 사용하여 이러한 앱에 대한 액세스를 제어할 수 있습니다. 기본값은 **false** 입니다.

루팅된 **Android** 및 탈옥 **iOS** 장치의 등록 차단: 이 속성이 **True** 인 경우 XenMobile 은 루팅된 Android 장치와 탈옥 iOS 장치에 대한 등록을 차단합니다. 기본값은 **True** 입니다. 권장되는 설정은 모든 보안 수준에 대해 **True** 입니다.

등록 필요: 이 속성은 XenMobile Server 모드가 ENT 인 경우에만 적용되며 사용자의 MDM 등록을 필수로 규정할지 여부를 지정합니다. 이 속성은 XenMobile 인스턴스의 모든 사용자 및 장치에 적용됩니다. 등록을 필수로 규정하면 보안 수준이 높아지지만 필수로 규정할지 여부는 MDM 이 필요한지 여부에 따라 결정합니다. 기본적으로 등록은 필수가 아닙니다.

이 속성이 **False** 인 경우 사용자는 등록을 거부할 수 있으며 장치에서 XenMobile Store 를 통해 앱에 액세스할 수 있습니다. 이 속성이 **True** 인 경우 등록을 거부하는 모든 사용자는 앱 액세스가 거부됩니다.

사용자 등록 후 이 속성을 변경하면 사용자가 재등록해야 합니다.

MDM 등록의 필수 여부에 대한 설명은 [장치 관리 및 MDM 등록](#) 을 참조하십시오.

XenMobile MDM 자가 지원 포털 콘솔의 최대 비활성 시간격입니다 (분): 이 속성이름에는 이전 XenMobile 버전이 반영됩니다. 이 속성은 XenMobile 콘솔의 최대 비활성 시간격을 제어합니다. 시간격은 XenMobile 콘솔에서 비활성 사용자가 로그아웃되기까지의 시간 (분) 입니다. 시간제한이 0 인 경우 비활성 사용자가 로그인 상태로 유지됩니다. 기본값은 **30** 입니다.

비활성 시간제한 (분): XenMobile 서버의 공용 API 를 사용하여 XenMobile 콘솔 또는 타사 앱에 액세스한 비활성 사용자가 XenMobile 에서 로그아웃되기까지의 시간 (분) 입니다. 시간제한 값이 0 이면 비활성 사용자가 로그인된 상태로 유지됩니다. API 에 액세스하는 타사 앱의 경우 일반적으로 로그인 유지가 필요합니다. 기본값은 **5** 입니다.

iOS 장치 관리 등록 루트 **CA** 설치 필요: Apple 의 최신 등록 워크플로에서 사용자는 MDM 프로필을 수동으로 설치해야 합니다. Apple Business Manager 또는 Apple School Manager 에서 할당된 서버에 대한 MDM 등록에는 이 워크플로가 적용되지 않습니다. 그러나 MDM 수동 등록 중에 iOS 장치 사용자에게는 등록 중에 MDM 장치 인증서를 묻는 메시지만 표시됩니다.

수동 등록 중에 더 나은 사용자 환경을 제공할 수 있도록 `ios.mdm.enrollment.installRootCaIfRequired` 서버 속성을 **false** 로 변경하는 것이 좋습니다. 기본값은 **true** 입니다. 이 변경이 적용되면 MDM 등록 중에 사용자가 간편하게 프로필을 설치할 수 있는 Safari 창이 열립니다.

VPP 기준 간격: **VPP** 기준 간격은 XenMobile 이 Apple 에서 VPP 라이선스를 다시 가져오는 최소 간격을 설정합니다. 라이선스 정보를 새로고치면 VPP 에서 가져온 앱을 수동으로 삭제하는 것과 같은 모든 변경 내용을 XenMobile 에 반영할 수 있습니다. 기본적으로 XenMobile 은 VPP 라이선스 기준을 최소 **720** 분마다 새로고칩니다.

설치된 VPP 라이선스가 많은 경우 (예: 50,000 개 초과) 기준 간격을 늘려 라이선스가 가져오기의 빈도 및 오버헤드를 줄이는 것이 좋습니다. Apple 에서 VPP 라이선스가 자주 변경될 것으로 예상되는 경우 값을 낮춰 XenMobile 에 변경 내용이 업데이트 되도록 하는 것이 좋습니다. 두 기준 사이의 최소 간격은 60 분입니다. cron 작업은 60 분마다 백그라운드에서 실행되므로 VPP 기준 간격이 60 분 인 경우 기준 사이의 간격이 최대 119 분까지 지연될 수 있습니다.

장치 및 앱 정책

January 6, 2020

XenMobile 장치 및 앱 정책을 사용하면 다음과 같은 요소 간의 균형을 최적화할 수 있습니다.

- 엔터프라이즈 보안

- 회사데이터및자산보호
- 사용자개인정보보호
- 사용자환경의생산성및품질개선

이러한요소간의최적화된균형은상황에따라다를수있습니다. 예를들어규제가많은조직 (예: 금융) 의경우기본적으로사용자생산성이고려되는교육, 소매등의다른업종보다엄격한보안제어가필요합니다.

사용자 ID, 장치, 위치및연결유형에따라정책을중앙에서제어하고구성하여회사콘텐츠의악의적사용을제한할수있습니다. 장치의분실또는도난이발생하는경우비즈니스응용프로그램및데이터를원격으로사용하지않도록설정하거나, 잠그거나, 초기화할수있습니다. 전체적인결과는직원만족도및생산성을개선하는동시에보안및관리제어를보장하는솔루션을구현하는것입니다.

이문서에서는보안과관련된다수의장치및앱정책을중점적으로다룹니다.

보안위험을해결하는정책

XenMobile 의장치및앱정책은보안위험을나타낼수있는다수의상황을해결합니다. 예를들면다음과같습니다.

- 사용자가신뢰할수없는장치와예측할수없는위치에서앱및데이터에엑세스를시도하는경우
- 사용자가장치간에데이터를이동하는경우
- 권한이없는사용자가데이터에엑세스를시도하는경우
- 회사에서자신의장치 (BYOD) 를사용한사용자가퇴사한경우
- 사용자가장치를부적절한장소에두는경우
- 사용자가항상안전하게네트워크에엑세스해야하는경우
- 사용자가직접장치를관리하고, 관리자가업무용데이터와개인용데이터를분리해야하는경우
- 유효상태의장치에서사용자자격증명을다시확인해야하는경우
- 사용자가중요한콘텐츠를복사하여보호되지않는전자메일시스템에붙여넣는경우
- 사용자가중요한데이터가포함된전자메일첨부파일또는웹링크를개인계정과회사계정이모두저장된장치에서수신하는경우

이러한상황은다음과같은회사데이터를보호할때두가지영역과관련하여고려되어야합니다.

- 유희데이터
- 전송중데이터

XenMobile 이유희데이터를보호하는방법

모바일장치에저장된데이터를유희데이터라고합니다. XenMobile 의 MAM(모바일응용프로그램관리) 기능을사용하면모바일생산성엔, MDX 사용앱및연결된데이터를완벽하게관리하고, 보호하고, 제어할수있습니다. XenMobile 배포용앱을지원하는 Worx App SDK 는 Citrix MDX 앱컨테이너기술을활용하여사용자의모바일장치에서회사앱및데이터와개인용앱및데이터를분리합니다. 이렇게하면포괄적인정책기반제어를통해사용자지정개발, 타사또는 BYO 모바일앱을보호할수있습니다.

XenMobile 에는광범위한 MDX 정책라이브러리에더해앱수준암호화도포함되어있습니다. XenMobile 은모든 MDX 사용앱안에서저장된데이터를개별적으로암호화하며장치 PIN 코드가필요하지않고정책을적용하기위해장치를관리할필요가없습니다.

정책및 Worx App SDK 를사용하면다음을수행할수있습니다.

- 비즈니스앱및데이터와개인용앱및데이터를안전한모바일컨테이너로분리합니다.
- 암호화및기타모바일 DLP(데이터손실방지) 기술을사용하여앱을보호합니다.

MDX 정책은다수의작업제어기능을제공하므로 MDX 래핑앱을원활하게통합하는동시에모든통신을제어할수있습니다. 이렇게하면 MDX 사용앱에서만데이터에액세스할수있도록하는등의정책을적용할수있습니다.

장치및앱정책제어외에유휴데이터를보호하는가장좋은방법은암호화입니다. XenMobile 은 MDX 사용앱에저장된모든데이터에암호화계층을추가하여공개파일암호화, 개인파일암호화및암호화제외같은기능을정책을통해제어할수있도록합니다. Worx App SDK 는 FIPS 140-2 호환 AES 256 비트암호화와함께보호되는 Citrix Secret Vault 에저장된키를사용합니다.

XenMobile 이전송중데이터를보호하는방법

사용자의모바일장치와회사의내부네트워크를이동하는데이터를전송중데이터라고합니다. MDX 앱컨테이너기술은 NetScaler Gateway 를통해내부네트워크에대한응용프로그램별 VPN 액세스를제공합니다.

직원이모바일장치에서보안엔터프라이즈네트워크에상주하는회사전자메일서버, 회사인트라넷에서호스트되는 SSL 사용웹응용 프로그램및파일서버또는 Microsoft SharePoint 에저장된문서등의리소스에액세스하려는경우를생각해보십시오. MDX 를사용하면모바일장치에서응용프로그램별 Micro VPN 을통해이모든엔터프라이즈리소스에액세스할수있습니다. 각장치에는전용 Micro VPN 터널이생성됩니다.

Micro VPN 기능은신뢰할수없는모바일장치의보안을침해할수있는장치전체 VPN 을사용하지않습니다. 따라서내부네트워크가전체회사시스템을감염시킬수있는맬웨어또는공격에노출되지않습니다. 회사모바일앱과개인용모바일앱이한장치에서공존할수있습니다.

더강력한수준의보안을제공하려면 MDX 사용앱을앱인증및 Micro VPN 세션에서사용되는대체 NetScaler Gateway 정책으로구성할수있습니다. 대체 NetScaler Gateway 를정책이필요한온라인세션에서사용하여앱에서특정게이트웨이에대한인증을강제할수있습니다. 이러한게이트웨이는보통다른 (높은수준의보장) 인증요구사항및트래픽관리정책을가지게됩니다.

Micro VPN 은보안기능에더해압축알고리즘같은데이터최적화기술을제공합니다. 압축알고리즘은최소한의데이터만가장빠른시간내에전송될수있도록하여모바일프로젝트의성공의핵심요소인개선된사용자환경을제공합니다.

장치정책은주기적으로재평가되어야합니다. 예를들어다음과같은상황에서는정책을다시평가해야합니다.

- XenMobile 의새버전에장치운영체제업데이트릴리스로인한새정책또는업데이트된정책이포함되는경우.
- 새장치유형을추가하는경우. 많은정책이모든장치에공통적으로적용되지만각장치에해당운영체제와관련된일련의정책이있습니다. 따라서 iOS, Android 및 Windows 장치간에는물론 Android 를실행하는장치제조업체사이에서도차이가있을수있습니다.
- XenMobile 작업을엔터프라이즈또는산업변경 (예: 새로운회사보안정책또는규정준수규제) 과동기화해야하는경우.
- MDX Toolkit 의새버전에새로운정책또는업데이트된정책이포함되는경우.
- 앱을추가하거나업데이트하는경우.
- 새앱또는새요구사항의결과로새로운사용자워크플로를통합해야하는경우.

앱정책및사용사례시나리오

Secure Hub 를통해제공할앱을선택할수있지만이러한앱이 XenMobile 과상호작용하는방식을정의해야할수도있습니다. 특정시간이경과한후사용자에게인증을요구하거나정보에대한오프라인엑세스를제공하고싶다면앱정책을통해그렇게할수있습니다. 다음목록에는일부정책과정책을사용하는방법이포함되어있습니다. 각플랫폼에대한모든 MDX 앱정책의목록은 [MDX 정책요약](#)을 참조하십시오.

인증정책

- 장치암호

이정책의용도: 사용자가장치 PIN 을사용하는장치에서만 MDX 앱에엑세스할수있도록하려면장치암호정책을사용하도록 설정합니다. iOS 9 장치를위한이기능은장치수준에서 MDX 컨테이너에 iOS 암호화가사용되도록합니다.

사용자예: 이정책을사용하면사용자가 iOS 장치에서 PIN 코드를설정해야 MDX 앱에엑세스할수있습니다.

- 앱암호

이정책의용도: 사용자가앱을열고데이터에엑세스하기전에관리되는앱에인증하라는 Secure Hub 메시지를표시하려면 앱암호정책을사용하도록설정합니다. 사용자는관리자가 XenMobile Server 설정의클라이언트속성에서구성한설정예 따라 Active Directory 암호, Citrix PIN 또는 iOS TouchID 를사용하여인증할수있습니다. 클라이언트속성에서비활성타이머를설정하면사용이중지되는동안타이머가다시만료되기전까지 Secure Hub 가관리되는앱에대한사용자인증 메시지를표시하지않습니다.

앱암호는장치암호와다릅니다. 장치암호정책이장치에푸시된경우 Secure Hub 는암호또는 PIN 을구성하라는메시지를 표시합니다. 장치를켜거나비활성타이머가만료되는경우사용자는구성한암호또는 PIN 을사용하여장치잠금을해제해야장치에엑세스할수있습니다. 자세한내용은 [XenMobile 의인증](#)에서참조하십시오.

사용자예: 장치에서 Citrix Secure Web 응용프로그램을열때비활성기간이만료된경우사용자가웹사이트를탐색하려면 Citrix PIN 을입력해야합니다.

- 온라인세션필요

이정책의용도: 응용프로그램의실행에웹앱 (웹서비스) 액세스가필요한경우이정책을사용하면 XenMobile 이앱을사용하기전에엔터프라이즈네트워크에연결하거나활성세션이있어야한다는내용의메시지를표시합니다.

사용자예: 사용자가온라인세션필요정책을사용하는 MDX 앱을열려는경우셀룰러또는 Wi-Fi 서비스를사용하여네트워크에연결하기전까지앱을사용할수없습니다.

- 최대오프라인기간

이정책의용도: 사용자가오랜시간동안앱을오프라인으로실행하는경우 XenMobile 에서앱권한부여를재확인하거나정책을새로고치도록하려면이정책을추가보안옵션으로사용합니다.

사용자예: 최대오프라인기간을사용하여 MDX 앱을구성하면사용자가오프라인타이머기간이만료되기전까지앱을오프라인으로열고사용할수있습니다. 이시점에서메시지가표시되면사용자가셀룰러또는 Wi-Fi 서비스를통해네트워크에다시연결하고재인증해야합니다.

기타액세스정책

- 앱업데이트유예기간 (시간)

이정책의용도: XenMobile Store 에최신버전이출시된앱의경우사용자는앱업데이트유예기간내에앱을업데이트해야합니다. 기간이만료되면사용자가앱을업데이트해야앱의데이터에액세스할수있습니다. 이값을설정할때는특히해외출장으로인해장시간오프라인상태로유지될수있는모바일작업자의요구사항을고려하십시오.

사용자예: Secure Mail 의새버전을 XenMobile Store 에로드한다음앱업데이트유예기간을 6 시간으로설정합니다. 6 시간이만료되기전에 Secure Mail 앱을업데이트하라는메시지가모든 Secure Mail 사용자에게표시됩니다. 6 시간이만료되면 Secure Hub 가사용자를 XenMobile Store 로라우팅합니다.

- 활성폴링기간 (분)

이정책의용도: 활성폴링기간은앱잠금, 앱초기화등의보안동작을수행하기위해 XenMobile 이앱을확인하는간격입니다.

사용자예: 활성폴링기간정책을 60 분으로설정할경우앱잠금명령을 XenMobile 에서장치로전송하면마지막폴링시간으로부터 60 분내에잠금이수행됩니다.

암호화정책

이정책의용도: XenMobile 에는 Secure Hub 및다른모바일생산성앱이중요한데이터 (예: 암호및암호화키) 를장치에유지할때사용하는기밀저장소가포함되어있습니다. 플랫폼의기본키저장소대신사용되는이기밀저장소에는강력한암호화계층이사용됩니다. 장치가손상된경우에도회사데이터는 MDX 컨테이너에암호화된상태로유지되며 XenMobile 은컨테이너외부데이터를전송하기전에해당데이터를난독처리합니다.

사용자예: 장치소유자가장치 PIN 을설정하지않았거나장치 PIN 이손상된경우 Secure Hub 컨테이너내부의회사데이터는안전하게유지됩니다.

앱상호작용정책

이정책의용도: MDX 앱에서장치의다른앱으로이동하는문서및데이터의흐름을제어하려면앱상호작용정책을사용합니다. 예를들어사용자는컨테이너외부의개인용앱으로데이터를이동하거나컨테이너외부의데이터를컨테이너화된앱에붙여넣을수없습니다.

사용자예: 앱상호작용정책을제한됨으로설정하면사용자가 Secure Mail 의텍스트를 Secure Web 에복사할수있지만데이터를컨테이너외부의개인용 Safari 또는 Chrome 브라우저에복사할수없습니다. 또한사용자는 Secure Mail 의첨부문서를 ShareFile 또는 Quick Edit 에서열수있지만컨테이너외부의개인용파일보기앱에서는이첨부문서를열수없습니다.

앱제한정책

이정책의용도: MDX 앱이열려있는동안사용자가액세스할수있는기능을제어하려면앱제한정책을사용합니다. 이정책을사용하면앱이실행되는동안악의적인활동을수행할수없습니다. 앱제한정책은 iOS 와 Android 에서조금다릅니다. 예를들어 iOS 에서는 MDX 앱이실행되는동안 iCloud 에대한엑세스를차단할수있습니다. Android 에서는 MDX 앱이실행되는동안 NFC 사용을중지할수있습니다.

사용자예: 앱제한정책을 사용하여 iOS 의 MDX 앱에서받아쓰기를차단하는경우사용자는 MDX 앱이실행되는동안 iOS 키보드에서받아쓰기기능을사용할수없습니다. 따라서사용자가받아쓰는데이터가보안되지않은타사클라우드받아쓰기서비스로전달되지않습니다. 사용자가컨테이너외부의개인용앱을열때는개인커뮤니케이션용으로받아쓰기옵션을사용할수있습니다.

앱네트워크액세스정책

이정책의용도: 장치의컨테이너에있는 MDX 앱에서회사네트워크안의데이터에액세스할수있도록하려면앱네트워크액세스정책을사용합니다. 네트워크액세스정책에서 내부네트워크로터널링됨옵션을설정하면 MDX 앱에서 NetScaler 를통한백엔드웹서비스또는데이터저장소로의 Micro VPN 이자동화됩니다.

사용자예: 사용자가터널링을사용하는 MDX 앱 (예: Secure Web) 을열면사용자가 VPN 을시작하지않아도브라우저가열리고인트라넷사이트가시작됩니다. Secure Web 앱이 Micro VPN 기술을사용하여내부사이트에자동으로액세스합니다.

앱지오로케이션및지오펠스정책

이정책의용도: 앱지오로케이션및지오펠스를제어하는정책에는중심점경도, 중심점위도및반경이포함됩니다. 이러한정책은 MDX 앱의데이터에대한액세스를특정지리적영역으로제한합니다. 정책은위도및경도좌표의반경을사용하여지리적영역을정의합니다. 사용자가정의된반경밖에서앱을사용하려고하면앱이잠긴상태로유지되고사용자가앱데이터에액세스할수없습니다.

사용자예: 사용자는사무실위치에있는동안합병및인수데이터에액세스할수있습니다. 사무실위치밖으로이동하면이중요한데이터에액세스할수없게됩니다.

Secure Mail 앱정책

- 백그라운드네트워크서비스

이정책의용도: Secure Mail 의백그라운드네트워크서비스는실질적으로 SOCKS5 프록시인 STA(Secure Ticket Authority) 를활용하여 NetScaler Gateway 를통해연결합니다. STA 는오래유지되는연결을지원하며 Micro VPN 에비해개선된배터리수명을제공합니다. 따라서 STA 는지속적으로연결되는메일에적합합니다. Secure Mail 을사용하는경우이러한설정을구성하는것이 좋습니다. XenMobile 용 NetScaler 마법사는 Secure Mail 에대해자동으로 STA 를설정합니다.

사용자예: STA 가사용되지않는경우 Android 사용자가 Secure Mail 을열면 VPN 을열라는메시지가표시됩니다. VPN 은장치에서열린상태로유지됩니다. STA 가사용되는경우 Android 사용자가 Secure Mail 을열면 Secure Mail 이 VPN 없이원활하게연결됩니다.

- 기본동기화간격

이정책의용도: 이설정사용자가 Secure Mail 에처음으로액세스할때 Secure Mail 과동기화되는전자메일의기본일수를지정합니다. 참고로 2 주간의전자메일은 3 일보다동기화가오래걸리며사용자설정프로세스가길어집니다.

사용자예: 사용자가 Secure Mail 을처음설정할때기본동기화간격을 3 일로설정하면현재부터지난 3 일까지받은전자메일이받은편지함에표시됩니다. 사용자가 3 일전의전자메일을보려는경우검색을수행할수있습니다. 그러면 Secure Mail

이 서버에 저장된 이전 전자 메일을 표시합니다. Secure Mail 을 설치한 후 각 사용자는 요구 사항에 적합하게 이 설정을 변경할 수 있습니다.

장치 정책 및 사용 사례 동작

장치 정책은 MDM 정책이라고도 하며 XenMobile 이 장치에서 작동하는 방식을 결정합니다. 많은 정책이 모든 장치에 공통적으로 적용되지만 각 장치에 해당 운영 체제와 관련된 일련의 정책이 있습니다. 다음 목록에는 일부 장치 정책과 정책을 사용하는 방법이 포함되어 있습니다. 모든 장치 정책의 목록은 [장치 정책](#) 아래 문서를 참조하십시오.

- 앱 인벤토리 정책

이 정책의 용도: 사용자에 의해 설치된 앱을 확인해야 하는 경우 장치에 앱 인벤토리 정책을 배포합니다. 앱 인벤토리 정책을 배포하지 않은 경우 사용자가 XenMobile Store 에서 설치한 앱만 표시되며 개인적으로 설치한 응용 프로그램은 표시되지 않습니다. 회사 장치에서 실행할 수 없는 특정 앱을 블랙리스트에 추가하려는 경우 이 정책을 사용해야 합니다.

사용자 예: MDM 으로 관리되는 장치의 사용자는 이 기능을 사용하지 않도록 설정할 수 없습니다. 사용자가 개인적으로 설치한 응용 프로그램이 XenMobile 관리자에게 표시됩니다.

- 앱 잠금 정책

이 정책의 용도: Android 용 앱 잠금 정책을 사용하면 앱을 블랙리스트 또는 화이트리스트에 추가할 수 있습니다. 예를 들어 앱을 화이트리스트에 추가하여 키오스크 장치를 구성할 수 있습니다. 일반적으로 앱 잠금 정책은 사용자가 설치할 수 있는 앱을 제한하므로 회사 소유 장치에만 배포됩니다. 재정의 암호를 설정하여 차단된 앱에 대한 사용자 액세스를 제공할 수 있습니다.

사용자 예: Angry Birds 앱을 차단하는 앱 잠금 정책을 배포한다고 가정할 경우 사용자는 Angry Birds 앱을 Google Play 에서 설치할 수 있지만 앱을 열면 관리자가 앱을 차단했다는 내용의 메시지가 표시됩니다.

- 연결 예약 정책

이 정책의 용도: Windows Mobile 장치에서 MDM 관리, 앱 푸시 및 정책 배포를 위해 XenMobile Server 에 다시 연결할 수 있도록 하려면 연결 예약 정책을 사용해야 합니다. Android, Android Enterprise 및 Chrome OS 장치의 경우 이 정책 대신 Google FCM(Firebase Cloud Messaging) 을 사용하여 XenMobile Server 에 대한 연결을 제어합니다. 예약 옵션은 다음과 같습니다.

- **항상:** 연결을 영구적으로 활성 상태로 유지합니다. 보안을 최적화하려면 이 옵션을 사용하는 것이 좋습니다. 항상을 선택하는 경우 연결로 인해 배터리가 소진되지 않도록 연결 타이머 정책도 사용하십시오. 연결을 활성 상태로 유지하면 초기화 또는 잠금과 같은 보안 명령을 주문형으로 장치에 푸시할 수 있습니다. 또한 장치에 배포하는 각 정책에서 배포 일정을 상시 연결에 대해 배포를 선택해야 합니다.
- **안함:** 수동으로 연결합니다. 안함 옵션을 사용하면 보안 정책을 장치에 배포할 수 없어 사용자가 새 앱 또는 정책을 받을 수 없으므로 프로덕션 배포에 사용하지 않는 것이 좋습니다.
- **매:** 지정된 간격으로 연결합니다. 이 옵션이 적용될 때 잠금 또는 초기화와 같은 보안 정책을 전송하면 다음에 장치가 연결할 때 정책이 처리됩니다.
- **일정 정의:** 사용하면 네트워크 연결이 끊긴 후 XenMobile 이 사용자 장치를 XenMobile Server 에 다시 연결하고 제어 패킷을 정의된 시간 내에 정기적으로 전송하여 연결을 모니터링합니다.

사용자예: 등록된장치에암호정책을배포하려고합니다. 예약정책을사용하면장치가정기적인간격으로서버에다시연결하여 새정책을수집합니다.

- 자격증명정책

이정책의용도: 주로 WiFi 정책과함께사용됩니다. 자격증명정책을사용하면인증서인증이필요한내부리소스에대한인증에 사용할인증서를배포할수있습니다.

사용자예: 장치의무선네트워크를구성하는 WiFi 정책을배포합니다. WiFi 네트워크를사용하려면인증서로인증해야합니 다. 자격증명정책은인증서를배포하고배포된인증서는운영체제키저장소에저장됩니다. 그러면사용자가내부리소스에연결 할때인증서를선택할수있습니다.

- **Exchange** 정책

이정책의용도: XenMobile 에서는두가지옵션을사용하여 Microsoft Exchange ActiveSync 전자메일을전송할수 있습니다.

- **Secure Mail** 앱: 공용앱스토어또는 XenMobile Store 에서배포하는 Secure Mail 앱을사용하여전자메일 을전송합니다.

- **기본전자메일 앱:** 장치의기본전자메일클라이언트에서 ActiveSync 전자메일을사용하도록설정하려면 Exchange 정책을사용합니다. 기본전자메일에대한 Exchange 정책을사용하는경우 Active Directory 특성 에서사용자데이터를채우는매크로를사용할수있습니다. 예를들어예: \${user.username} 을사용하여사용자이 름을채우고 \${user.domain} 을사용하여사용자도메인을채울수있습니다.

사용자예: Exchange 정책을푸시할때 Exchange Server 세부정보를장치에전송합니다. 그러면 Secure Hub 가인 증메시지를표시하고전자메일동기화가시작됩니다.

- 위치정책

이정책의용도: 위치정책을사용하면장치가 Secure Hub 에대한 GPS 를사용하는경우지도에서장치의위치를찾을수있 습니다. 이정책을배포한후 XenMobile Server 에서위치명령을보내면장치가위치좌표를사용하여응답합니다.

사용자예: 위치정책이배포되고 GPS 가장치에서사용되는경우장치를찾지못하는사용자는 XenMobile 자가지원포털에 로그인하고찾기옵션을선택하여지도에서장치의위치를확인할수있습니다. 사용자는 Secure Hub 에서위치서비스를사 용할수있도록선택해야합니다. 사용자가직접장치를등록하는경우관리자는위치서비스사용을적용할수없습니다. 이정책을 사용할때는배터리수명에미치는영향도고려해야합니다.

- 암호정책

이정책의용도: 암호정책을사용하면관리되는장치에 PIN 코드또는암호를적용할수있습니다. 이암호정책을사용하면장치 에암호에대한복잡성및시간초과를설정할수있습니다.

사용자예: 관리되는장치에암호정책을배포하면 Secure Hub 가암호또는 PIN 을구성하라는메시지를표시합니다. 장치 를켜거나비활성타이머가만료되는경우사용자는구성한암호또는 PIN 을사용하여장치잠금을해제해야장치에엑세스할수 있습니다.

- 프로필제거정책

이정책의용도: 사용자그룹에정책을배포하고나중에일부사용자에게서정책을제거해야하는경우프로필제거정책을만들고프로필제거정책을지정된사용자이름에만배포하는배포규칙을사용하여선택한사용자에대한정책을제거할수있습니다.

사용자에: 프로필제거정책을사용자장치에배포하는경우사용자는변경내용을알지못할수있습니다. 예를들어프로필제거정책이장치카메라를사용할수없도록하는제한을제거하는경우사용자는카메라사용이허용된것을알지못합니다. 사용자경험에영향을미치는변경이발생하는경우해당사항을사용자에게알려주는것이 좋습니다.

- **제한정책**

이정책의용도: 제한정책은관리되는장치의기능을잠그고제어할수있다는수의옵션을제공합니다. 지원되는장치에대한수백가지제한옵션을사용할수있으며여기에는장치의카메라또는마이크사용을제한하는옵션부터앱스토어같은타사서비스에대한로밍규칙및액세스를적용하는옵션이포함됩니다.

사용자에: iOS 장치에제한을배포하는경우사용자는 iCloud 또는 iTunes 스토어에액세스하지못할수있습니다.

- **약관정책**

이정책의용도: 관리자는장치관리와관련된법적영향을사용자에게알려야할수있습니다. 또한회사데이터를장치에푸시할때의보안위험을사용자가숙지할수있도록해야합니다. 사용자가등록하기전에관리자는사용자지정약관문서를사용하여규칙및고지사항을게시할수있습니다.

사용자에: 사용자등록프로세스중에약관정보가표시됩니다. 사용자가명시된조건에동의하지않으면등록프로세스가종료되고사용자는회사데이터에액세스할수없게됩니다. 약관에동의하거나거부한사용자를보여주는보고서를생성하여 HR/법무/규정준수팀에제공할수있습니다.

- **VPN 정책**

이정책의용도: 이전 VPN Gateway 기술을사용하여백엔드시스템에대한액세스를제공하려면 VPN 정책을사용합니다. 이정책은 Cisco AnyConnect, Juniper 및 Citrix VPN 을포함하는다수의 VPN 공급자를지원합니다. VPN 게이트웨이가이옵션을지원하는경우이정책을 CA 에연결하고주문형 VPN 을사용하도록설정할수도있습니다.

사용자에: VPN 정책을사용하면사용자가내부도메인에액세스할때사용자장치에서 VPN 연결이열립니다.

- **웹클립정책**

이정책의용도: 웹사이트를직접여는아이콘을장치에푸시하려면웹클립정책을사용합니다. 웹클립에는웹사이트링크가포함되며사용자지정아이콘을포함할수있습니다. 장치에서웹클립은앱아이콘처럼표시됩니다.

사용자에: 사용자는웹클립아이콘을클릭하여액세스가필요한서비스를제공하는인터넷사이트를열수있습니다. 웹링크를사용하면브라우저앱을열고링크주소를입력하는것보다편리합니다.

- **WiFi 정책**

이정책의용도: WiFi 정책을사용하면 SSID, 인증데이터및구성데이터같은 WiFi 네트워크세부정보를관리되는장치에배포할수있습니다.

사용자에: WiFi 정책을배포하면장치가자동으로 WiFi 네트워크에연결되고사용자를인증합니다. 인증된사용자는네트워크에액세스할수있습니다.

- **Windows Information Protection 정책**

이정책의용도: 엔터프라이즈데이터의잠재적유출을방지하려면 WIP(Windows Information Protection) 정책을 사용합니다. 설정한적용수준에서 Windows Information Protection 이필요한앱을지정할수있습니다. 예를들어부적절한데이터공유를차단하거나부적절한데이터공유에대해경고를표시하고사용자의정책재정의를허용할수있습니다. 부적절한데이터공유를로깅하고허용하는동안 WIP 를자동으로실행할수있습니다.

사용자예: 부적절한데이터공유를차단하는 WIP 정책을구성하는경우사용자가보호되는파일을보호되지않는위치로복사하거나저장하면보호되는콘텐츠가포함된작업을이위치에배치할수없다는내용의메시지가표시됩니다.

• **XenMobile Store** 정책

이정책의용도: XenMobile Store 는관리자가사용자에게필요한모든회사앱및데이터리소스를게시할수있는통합앱스토어입니다. 관리자는웹앱, SaaS 앱, MDX 래핑앱, Citrix 생산성앱, 기본모바일앱 (예: .ipa 또는.apk 파일), iTunes 및 Google play 앱, 웹링크및 Citrix StoreFront 를사용하여게시된 Virtual Apps and Desktops 앱을추가할수있습니다.

사용자예: XenMobile 에장치를등록한후사용자는 Citrix Secure Hub 앱을통해 XenMobile Store 에액세스합니다. 여기서사용자는제공되는모든회사앱및서비스를확인할수있습니다. 사용자는 XenMobile Store 에서앱을클릭하여설치하고, 데이터에엑세스하고, 앱을평가하고후기를작성하고, 앱업데이트를다운로드할수있습니다.

사용자등록옵션

January 6, 2020

사용자장치를 XenMobile 에등록하도록하는방법은여러가지입니다. 구체적인내용을고려하기전에환경의장치를등록할모드즉, 엔터프라이즈모드 (MDM+MAM), MDM 모드또는 MAM 모드 (MAM 전용모드) 로등록할지여부를결정해야합니다. 관리모드에대한자세한내용은 [관리모드](#)를참조하십시오.

개괄적으로등록옵션에는네가지가있습니다.

- **등록초대:** 사용자에게등록초대또는초대링크를전송합니다.
- **자가지원포털:** 사용자가방문하여 Secure Hub 를다운로드하고장치를등록하거나등록초대를직접전송할수있는포털을설정합니다.
- **수동등록:** 사용자에게시스템이실행중이며등록할수있음을알리는전자메일, 안내서또는기타커뮤니케이션을전송합니다. 그러면사용자가 Secure Hub 를다운로드하고수동으로장치를등록합니다.
- **엔터프라이즈:** 장치등록의다른옵션은 Apple DEP(장치등록프로그램) 및 Google Android Enterprise 를사용하는것입니다. 이러한프로그램을통해미리구성되고직원이사용할수있도록준비된장치를구입할수있습니다. 자세한내용은 [Apple DEP\(장치등록프로그램\)](#) 및 [Google Android Enterprise](#) 항목을참조하십시오.

등록초대

iOS, macOS 및 Android 장치사용자에게전자메일로등록초대를보낼수있습니다. 또한 iOS, macOS, Android 또는 Windows 장치사용자에게 SMTP 또는 SMS 를통해설치링크를보낼수있습니다. 자세한내용은 [장치등록](#)에서참조하십시오.

등록초대방법을사용하기로선택하는경우: 플랫폼에따라 7 개등록모드중에서선택할수있으며모드를조합하여사용할수있습니다. XenMobile 설정페이지에서모드를사용하거나사용하지않도록설정할수있으며사용자이름 + 암호, 2 단계및사용자이름 + PIN 중에서기본값을선택할수있습니다. 각등록모드에대한자세한내용은 [등록모드를구성하려면](#)을참조하십시오.

인증서기반을선택하는경우사용자이름 + 암호의기존인증을허용되는옵션에서제외하는것이 좋습니다. 이모드를사용할경우환경의 등록절차가취약해지고규정된보안품질이무효화될수있습니다.

초대는많은용도로사용됩니다. 초대이가장일반적인용도는사용자에게시스템을사용할수있고등록할수있음을알리는것입니다. 초대 URL 은고유합니다. 한사용자가사용한초대 URL 은다시사용될수없습니다. 이속성을사용하여시스템에등록하는사용자또는 장치를제한할수있습니다.

iOS 사용자가등록중에다음방법중하나를사용하여자격증명을제공하도록 XenMobile 을설정할수있습니다.

- 사용자가등록중에자격증명을입력합니다.
- 사용자가파생된자격증명공급자의스마트카드를데스크톱에연결된판독기에삽입합니다. 파생된자격증명에대한자세한내용은 [파생된자격증명](#)을참조하십시오.

XenMobile 콘솔에서등록프로필에대한옵션을선택하고특정사용자가등록할수있는장치수를 Active Directory 그룹에따라제어할수있습니다. 예를들어회계부서에서사용자당하나의장치만등록할수있도록하려면등록프로필을통해이러한시나리오를구성할수있습니다.

특정등록옵션을사용할경우추가비용및문제가발생할수있다는점에주의하십시오. SMS 를 사용하여초대를보내려는경우추가인프라를설정해야합니다. 이옵션에대한자세한내용은 [알림](#)을참조하십시오.

또한전자메일로초대를보내려는경우사용자가 Secure Hub 외부에서전자메일에액세스할수있는지확인하십시오. MDM 등록의 경우 OTP(일회용암호) 등록모드를 Active Directory 암호대신사용할수있습니다.

자가지원포털

사용자는자가지원포털을통해등록초대를요청할수있습니다. 기본모드는사용자이름 + 암호이지만이요구사항을 2 단계또는사용자이름 + PIN 으로변경할수도있습니다. 자가지원포털설정에대한자세한내용은 [등록모드를구성하려면](#)을참조하십시오.

수동등록

수동등록에서는사용자가자동검색을사용하거나서버정보를입력하여 XenMobile 에연결합니다. 자동검색을사용하는경우사용자는전자메일주소또는 Active Directory 자격증명만사용자계정이름형식으로입력하여서버에로그온합니다. 자동검색을사용하지않는경우사용자는서버주소와 Active Directory 자격증명을입력해야합니다. 자동검색설정에대한자세한내용은 [XenMobile Autodiscovery Service](#)를참조하십시오.

수동등록은여러가지방법으로간편하게완료할수있습니다. 가이드를생성하고가이드를사용자에게배포한다음직접등록하도록합니다. IT 부서를통해특정시간슬롯의사용자그룹을수동으로등록할수있습니다. 사용자가자격증명및/또는서버정보를입력해야하는유사한방법을사용할수있습니다.

사용자등록

환경을설정후에는사용자를환경에등록하는방법을결정해야합니다. 사용자등록모드에대한구체적인내용은이문서의이전섹션에 설명되어있습니다. 이섹션에서는사용자에게연락하는방법을설명합니다.

공개등록과선택적초대

사용자를등록할때는두가지기본적인방법을통해등록을허용할수있습니다. 기본적으로 LDAP 자격증명과 XenMobile 환경정보를가지고있는모든사용자가등록할수있는공개등록을허용할수있습니다. 또는등록초대를받은사용자만허용하여사용자수를제한할수있습니다. Active Directory 그룹을기준으로공개등록을제한할수도있습니다.

초대방법을사용하는경우사용자가등록할수있는장치수를제한할수도있습니다. 공개등록은대부분의경우허용되지만몇가지고려해야할사항이있습니다.

- MAM 환경을롤아웃하는경우 Active Directory 그룹구성원자격을통해간편하게등록을제한할수있습니다.
- MDM 환경에서등록을제한할수있는유일한방법은 Active Directory 그룹구성원자격에따라등록할수있는장치를제한하는것입니다. 환경에서회사장치만허용하려는경우이방법은문제가되지않습니다. 그러나 BYOD 작업공간에서환경의장치수를제한하려는경우이방법을고려해야할수있습니다.
- 또한사용자라이센스가있는지장치라이센스가있는지여부도고려해야합니다. 사용자라이센스를사용하는경우각사용자가다수의장치를사용할수있고라이센스는하나만소비됩니다. 장치라이센스를사용하는경우등록된각장치에라이센스하나가소비됩니다.

선택적초대는공개등록보다필요한작업이약간더많기때문에예일반적으로덜 자주수행됩니다. 사용자가환경에서장치를등록하려면관리자가각사용자에게고유한초대를보내야합니다. 등록초대를보내는방법에대한자세한내용은 [등록초대보내기](#)를참조하십시오.

환경에등록하려는각사용자또는그룹에대한초대를보내야하며조직의규모에따라시간이오래걸릴수있습니다. Active Directory 그룹을사용하여초대를일괄적으로생성할수있지만이접근방식은연속적으로수행해야합니다.

먼저사용자에게연락

공개등록을사용할지선택적초대를사용할지를결정하고이러한환경을설정후에는사용자에게등록옵션을알려주어야합니다.

선택적초대방법을사용하는경우전자메일및 SMS 메시지가프로세스에포함됩니다. 공개등록의경우에도 XenMobile 콘솔을통해전자메일을보낼수있습니다. 자세한내용은 [등록초대보내기](#)에서참조하십시오.

두경우모두전자메일을사용하려면 SMTP 서버가필요합니다. 문자메시지의경우 SMS 서버가필요합니다. 따라서의사결정을내릴때추가비용을고려해야할수있습니다. 또한방법을선택하기전에새사용자가정보 (예: 전자메일) 에 액세스하는방법을고려해야합니다. 모든사용자로하여금 XenMobile 을통해전자메일에액세스하도록하려는경우초대전자메일을보내는것이문제가될수있습니다.

공개등록환경의경우 XenMobile 외의다른방법으로커뮤니케이션을보낼수도있습니다. 사용자가 Secure Hub 앱을다운로드할수있는위치와등록시사용해야하는방법등모든관련정보를포함하기만하면됩니다. 자동검색을끈경우에는사용자에게 XenMobile 서버주소도알려줘야합니다. 자동검색에대한자세한내용은 [XenMobile Autodiscovery Service](#)를참조하십시오.

XenMobile 작업조정

September 27, 2019

XenMobile 작업의 성능 및 안정성은 XenMobile 의 많은 설정과 관련되며 NetScaler 및 SQL Server 데이터베이스 구성에 따라 달라집니다. 이 문서에서는 XenMobile 의 조정 및 최적화와 관련하여 관리자가 가장 자주 구성하는 설정을 중점적으로 설명합니다. XenMobile 을 배포하기 전에 이 문서의 각 설정을 평가하는 것이 좋습니다.

중요:

다음 지침은 XenMobile 서버 CPU 및 RAM 이 장치수에 적합하다고 가정합니다. 확장성에 대한 자세한 내용은 [확장성 및 성능](#) 을 참조하십시오.

다음 서버 속성은 전체 XenMobile 인스턴스의 작업, 사용자 및 장치에 글로벌로 적용됩니다. 일부 서버 속성을 변경하려면 각 XenMobile 서버 노드를 다시 시작해야 합니다. 다시 시작이 필요한 경우 XenMobile 이 알림을 제공합니다.

다음 조정 지침은 클러스터된 환경과 클러스터되지 않은 환경에 모두 적용됩니다.

hibernate.c3p0.idle_test_period

XenMobile Server 속성인 사용자 지정 키는 연결 유효성이 자동으로 검사되기까지의 유휴 시간 (초) 을 결정합니다. 다음과 같이 키를 구성합니다. 기본값은 **30** 입니다.

- 키: 사용자 지정 키
- 키: **hibernate.c3p0.idle_test_period**
- 값: **120**
- 표시 이름: **hibernate.c3p0.idle_test_period**
- 설명: **Hibernate** 유휴 테스트 기간

hibernate.c3p0.max_size

이 사용자 지정 키는 XenMobile 에서 SQL Server 데이터베이스에 대해 열 수 있는 최대 연결 수를 결정합니다. XenMobile 은 이 사용자 지정 키에 지정된 값을 상한으로 사용합니다. 필요한 경우에만 연결이 열립니다. 데이터베이스 서버의 용량에 따라 설정을 결정합니다.

클러스터된 구성에서는 다음 수식을 참고하십시오. c3p0 연결에 노드 수를 곱한 값은 XenMobile 이 SQL Server 데이터베이스에 실제로 열 수 있는 최대 연결 수와 동일합니다.

클러스터된 구성 및 클러스터되지 않은 구성에서 SQL Server 규모를 작게 하여 이 값을 너무 높게 설정하면 최고 부하 중에 SQL 측에서 리소스 문제가 발생할 수 있습니다. 이 값을 너무 낮게 설정하면 사용 가능한 SQL 리소스를 활용하지 못할 수 있습니다.

다음과 같이 키를 구성합니다. 기본값은 **1000** 입니다.

- 키: **hibernate.c3p0.max_size**

- 값: **1000**
- 표시이름: **hibernate.c3p0.max_size**
- 설명: SQL 에대한 DB 연결

hibernate.c3p0.min_size

이사용자지정키는 XenMobile 에서 SQL Server 데이터베이스에대해여는최소연결수를결정합니다. 다음과같이키를구성합니다. 기본값은 **100** 입니다.

- 키: **hibernate.c3p0.min_size**
- 값: **100**
- 표시이름: **hibernate.c3p0.min_size**
- 설명: SQL 에대한 DB 연결

hibernate.c3p0.timeout

이사용자지정키는유휴시간초과를결정합니다. 데이터베이스클러스터장애조치 (failover) 를사용하는경우이사용자지정키를추가하고, 유휴시간초과를낮추도록설정하는것이 좋습니다. 기본값은 **120** 입니다.

- 키: 사용자지정키
- 키: **hibernate.c3p0.timeout**
- 값: **120**
- 표시이름: **hibernate.c3p0.timeout**
- 설명: 데이터베이스유휴시간초과

푸시서비스하트비트간격

이설정은 iOS 장치에서중간에 APNs 알림이전송되지않았는지를확인하는빈도를결정합니다. APNs 하트비트빈도를늘리면데이터베이스통신을최적화할수있습니다. 값이너무크면불필요한부하가추가될수있습니다. 이설정은 iOS 에만적용됩니다. 기본값은 **20** 시간입니다.

환경에 iOS 장치가많은경우하트비트간격으로인해필요이상의부하가발생할수있습니다. 선택적초기화, 잠금및전체초기화같은보안동작은이하트비트를사용하지않습니다. 이러한동작이실행될때는 APNs 알림이장치로전송되기때문입니다. 이값은 Active Directory 그룹구성원자격이변경후정책을업데이트하는속도를제어합니다. 그러므로부하를줄이려면이값을 12~20 시간사이의값으로늘리는것이적절합니다.

iOS MDM APNS 연결풀크기

장치수가 100 대이상인경우 APNs 연결풀이너무작으면 APNs 작업성능에부정적인영향을미칠수있습니다. 애플정책이장치에느리게배포되고장치등록이느려지는등의성능문제가발생할수있습니다. 기본값은 **1** 입니다. 약 400 개의장치마다이값을 1 씩늘리는것이 좋습니다 (최대값 **15**).

auth.ldap.connect.timeout

느린 LDAP 응답을 보완하려면 다음 사용자 지정 키의 서버 속성을 추가하는 것이 좋습니다.

- 키: 사용자 지정 키
- 키: **auth.ldap.connect.timeout**
- 값: **60000**
- 표시 이름: **auth.ldap.connect.timeout**
- 설명: **LDAP** 연결 시간 초과

auth.ldap.read.timeout

느린 LDAP 응답을 보완하려면 다음 사용자 지정 키의 서버 속성을 추가하는 것이 좋습니다.

- 키: 사용자 지정 키
- 키: **auth.ldap.read.timeout**
- 값: **60000**
- 표시 이름: **auth.ldap.read.timeout**
- 설명: **LDAP** 읽기 시간 제한

기타 서버 최적화

서버 속성	기본 설정	이 설정을 변경하는 이유
백그라운드 배포	1,440 분	백그라운드 정책 배포 빈도 (분)입니다. Android 장치의 상시 연결에만 적용됩니다. 정책 배포 빈도를 늘리면 서버 부하가 감소합니다. 권장되는 설정은 1440 (24 시간)입니다.
백그라운드 하드웨어 인벤토리	1,440 분	백그라운드 하드웨어 인벤토리 빈도 (분)입니다. Android 장치의 상시 연결에만 적용됩니다. 하드웨어 인벤토리 빈도를 늘리면 서버 부하가 감소합니다. 권장되는 설정은 1440 (24 시간)입니다.

삭제된 Active Directory 사용자 를확인하는간격	15 분	Active Directory 의표준동기화시 간은 15 분입니다. 값이 0 인경우 XenMobile 이삭제된 Active Directory 사용자를확인하지않습니 다. 권장되는설정은 15 분입니다.
MaxNumberOfWorker	3	많은수의 VPP 라이선스를가져올때사 용되는스레드수입니다. 기본값은 3 입 니다. 추가최적화가필요한경우스레드 수를늘릴수있습니다. 그러나예를들어 6 과같이스레드수가커지면 VPP 를가 져올때 CPU 사용량이높아진다는점에 유의하십시오.

Android 장치의배포예약최적화

Google FCM(Firebase Cloud Messaging) 을사용하여 Android 장치에대한배포를예약할수있습니다.

XenMobile 환경에서 FCM 을사용하면 iOS 장치의 APNs 와유사하게 Android 장치에서실시간에가까운알림을사용할수
있습니다. FCM 을구성하면 XenMobile 이정책업데이트, 선택적초기화등의작업을수행하기위해장치에연결해야하는경우
XenMobile 서버가 FCM 서버로알림메시지를보내요청을클라이언트장치로전달합니다. 장치에 FCM 의알림이수신되면장치가
추가지침을위해다시 XenMobile 에연결합니다. 이방법에는타사서버 (Google) 가사용되므로회사의 IT 부서또는 Citrix 지원
에서제어할수없는서비스중단이발생할수있습니다.

FCM 서비스등록방법에대한자세한내용은 [XenMobile and Firebase Cloud Messaging \(FCM\) Configura-
tion\(XenMobile 및 FCM\(Firebase Cloud Messaging\) 구성\)](#)을참조하십시오.

Android 에서 FCM 을사용하는경우다음 XenMobile 서버속성에유의하십시오.

- **FCM API Key(FCM API 키):** Google Developers Console 에서만들어진키입니다.
- **FCM Sender ID(FCM 보낸사람 ID):** Google Developers Console 의프로젝트번호입니다.
- **FCM Registration ID TTL(FCM 등록 ID TTL):** 장치 FCM 등록 ID 를갱신하기전의지연기간 (일) 입니다. 기본값
은 **10** 입니다.
- **FCM Heartbeat Interval(FCM 하트비트간격):** 기본값은 **20** 시간입니다.

SQL DB 에서교착상태를확인하고기록데이터를삭제하는방법

교착상태가발견되면다음쿼리를실행하여교착상태를확인하십시오. 그런다음데이터베이스관리자또는 Microsoft SQL 팀을통
해정보를확인할수있습니다.

SQL 쿼리

```
1 SELECT
2
3 db.name DB_Service,
4
5 tl.request_session_id,
6
7 wt.blocking_session_id,
8
9 OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,
10
11 tl.resource_type,
12
13 h1.TEXT AS RequestingText,
14
15 h2.TEXT AS BlockingText,
16
17 tl.request_mode
18
19 FROM sys.dm_tran_locks AS tl
20
21 INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id
22
23 INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
    resource_address
24
25 INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
    resource_associated_entity_id
26
27 INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
    request_session_id
28
29 INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
    blocking_session_id
30
31 CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1
32
33 CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2
34
35 GO
```

데이터베이스정리

중요:

테이블을 변경하기 전에 데이터베이스를 백업합니다.

1. 다음 쿼리를 실행하여 기록 데이터를 확인합니다.

```
1 select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;  
2 select COUNT(\*) as total_record from dbo.EWSESS;  
3 select COUNT(*) as total_record from dbo.EWAUDIT;
```

2. 이전의 3 개 테이블에서 데이터를 삭제합니다.

참고:

기록 데이터가 테이블에 표시되지 않을 수 있습니다. 이 경우 실행을 건너뛰고 특정 테이블에 대한 쿼리를 잘라냅니다.

```
1 truncate TABLE dbo.EWDEPLOY_HISTO;  
2 truncate TABLE dbo.EWSESS;  
3 truncate TABLE dbo.EWAUDIT;
```

3. 교착상태로 인해 차단되었던 SELECT 쿼리를 차단 해제합니다. 이 단계에서 추가 교착상태가 처리됩니다.

```
1 ALTER DATABASE <database_name> SET          READ_COMMITTED_SNAPSHOT  
   ON WITH ROLLBACK IMMEDIATE
```

4. 기본적으로 데이터베이스 정리는 세션 보존 및 감사 보존 데이터 유지를 위해 7 일로 설정되며 사용자 수가 많은 경우 값이 증가합니다. 정리 값을 1 일 또는 2 일로 변경합니다. 서버 속성에서 다음 변경을 수행합니다.

```
1 zdm.dbcleanup.sessionRetentionTimeInDays = 1 day  
2 zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day  
3 zdm.dbcleanup.auditRetentionTimeInDays=1 day
```

KEYSTORE 테이블에서 분리된 항목 정리

XenMobile 노드의 성능이 좋지 않으면 KEYSTORE 테이블이 너무 크지 않은지 확인합니다. XenMobile 은 등록 인증서를 ENROLLMENT_CERTIFICATE 및 KEYSTORE 테이블에 저장합니다. 장치를 삭제하거나 재등록하면 ENROLLMENT_CERTIFICATE 테이블의 인증서가 삭제됩니다. KEYSTORE 테이블의 항목은 그대로 유지되며, 이로 인해 성능 문제가 발생할 수 있습니다. KEYSTORE 테이블에서 분리된 항목을 정리하려면 다음 절차를 수행하십시오.

중요:

테이블을 변경하기 전에 데이터베이스를 백업합니다.

1. 다음 쿼리를 실행하여 기록 데이터를 확인합니다.

```
1 select COUNT(*) from KEYSTORE
```

2. 다음쿼리를사용하여 KEYSTORE 테이블에서분리된항목이있는지확인합니다.

```
1 WITH cte(KEYSTORE_ID)
2 AS (SELECT KEYSTORE_ID
3     FROM ENROLLMENT_CERTIFICATE
4     UNION
5     SELECT CA_KEYSTORE_ID
6     FROM LDAP_CONFIG
7     UNION
8     SELECT CLIENT_KEYSTORE_ID
9     FROM LDAP_CONFIG
10    UNION
11    SELECT KEYSTORE_ID
12    FROM SAML_SERVICE_PROVIDER
13    UNION
14    SELECT KEYSTORE_ID
15    FROM SERVER_CERTIFICATE)
16 SELECT keystore.id
17 FROM keystore
18     LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
19 WHERE KEYSTORE_ID IS NULL;
```

3. 다음쿼리를사용하여분리된항목을지웁니다.

```
1 WITH cte(KEYSTORE_ID)
2 AS (SELECT KEYSTORE_ID
3     FROM ENROLLMENT_CERTIFICATE
4     UNION
5     SELECT CA_KEYSTORE_ID
6     FROM LDAP_CONFIG
7     UNION
8     SELECT CLIENT_KEYSTORE_ID
9     FROM LDAP_CONFIG
10    UNION
11    SELECT KEYSTORE_ID
12    FROM SAML_SERVICE_PROVIDER
13    UNION
14    SELECT KEYSTORE_ID
15    FROM SERVER_CERTIFICATE)
16 DELETE FROM keystore
17 WHERE id IN
18 (
19     SELECT keystore.id
20     FROM keystore
21     LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
```

```
22 WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
23 );
```

4. KEYSTORE 테이블에 인덱스를 추가하여 검색 효율성을 높입니다.

```
1 DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
2 ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
3 CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
    ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
    DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
```

앱 프로비전 및 프로비전 해제

May 21, 2019

응용 프로그램 프로비전은 주로 XenMobile 환경 내 모바일 앱의 래핑, 구성, 제공 및 관리로 구성되는 모바일 앱 수명 주기를 중심으로 수행됩니다. 일부 경우에는 응용 프로그램 코드의 배포나 수정도 프로비전 프로세스에 포함될 수 있습니다. XenMobile에는 앱 프로비전에서 사용할 수 있는 다양한 도구와 프로세스가 포함되어 있습니다.

앱 프로비전에 관한 문서를 읽기 전에 [앱](#) 및 [사용자 커뮤니티](#)에 대한 문서를 읽는 것이 좋습니다. 조직에서 사용자에게 제공할 앱의 유형을 확정 한 후에 앱의 수명 주기 관리 프로세스에 대한 개요를 작성할 수 있습니다.

앱 프로비전 프로세스를 정의 할 때는 다음 요점을 고려하십시오.

- **앱 프로파일링:** 처음에는 제한된 수의 앱을 사용하여 시작할 수 있지만 사용자 채택률이 증가하고 환경의 규모가 확장됨에 따라 관리하는 앱의 수가 빠른 속도로 증가할 수 있습니다. 앱 프로비전을 쉽게 관리하려면 처음부터 구체적인 앱 프로필을 정의해야 합니다. 앱 프로파일링은 앱을 기술적 관점의 논리적 그룹으로 범주화하는데 도움이 됩니다. 예를 들어 다음과 같은 요소를 기준으로 앱 프로필을 생성할 수 있습니다.
 - 버전: 추적에 사용할 앱 버전
 - 인스턴스: 서로 다른 사용자 집합 (예: 서로 다른 액세스 수준)에 배포되는 다수의 인스턴스
 - 플랫폼: iOS, Android 또는 Windows
 - 대상: 표준 사용자, 부서, 최고 수준 경영진
 - 소유권: 앱을 소유하는 부서
 - 유형: MDX, 공용, 웹 및 SaaS 또는 웹 링크
 - 업그레이드 주기: 앱을 업그레이드 하는 빈도
 - 라이선스: 라이선스 요구 사항 및 소유권
 - MDX 정책: MDX 보안 정책으로 래핑하거나 래핑하지 않음
 - 네트워크 액세스: 액세스 유형 (예: Secure Browse 또는 전체 VPN)

참고:

터널링됨 - 웹 SSO는 MDX 설정에서 Secure Browse 의미입니다. 동작은 동일합니다.

예:

요소	Secure Mail	메일	사내	Epic Rover
버전	10.1	10.1	X.x	X.x
인스턴스	중요발신인	의사	임상	임상
플랫폼	iOS	iOS	iOS	iOS
대상사용자	VIP 사용자	의사	임상사용자	임상사용자
소유권	IT	IT	IT	IT
유형	MDX	MDX	기본	공개
업그레이드주기	분기별	분기별	매년	해당없음
라이선스	해당없음	해당없음	해당없음	VPP
MDX 정책	예	예	예	아니요
네트워크엑세스	VPN	VPN	VPN	공개

- **앱버전관리:** 앱버전을유지관리하고추적하는작업은프로비전프로세스의중요한부분입니다. 버전관리는일반적으로사용자에게미치는영향없이수행됩니다. 앱의새버전을다운로드할수있을때만사용자에게알림이제공됩니다. 관리자의관점에서프로덕션환경에미치는영향을방지하려면비프로덕션용량에서각앱버전을검토하고테스트해야합니다.

이러한검토및테스트는특정업그레이드가실제로필요한지여부를평가할때에도중요합니다. 앱업그레이드에는일반적으로두가지유형이있습니다. 하나는특정버그에대한수정과같은부분업그레이드이고, 다른하나는앱에중요한변경및개선사항을도입하는주릴리스입니다. 두경우모두앱의릴리스정보를주의깊게검토하여업그레이드가필요한지여부를평가해야합니다.

- **앱서명및래핑:** XenMobile 에서는 MDX 정책을관리되는앱에서사용하여앱래핑을통해회사데이터를보호할수있습니다. MDX Toolkit 의앱래핑에대한자세한내용은 XenMobile 설명서에서 [MDX Toolkit](#)을참조하십시오. 래핑된앱의앱프로비전프로세스는래핑되지않은표준앱의프로비전프로세스와크게다릅니다.
- **앱보안:** 프로비전프로세스의일부로개별앱또는앱프로필의보안요구사항을정의합니다. 앱을배포하기전에특정 MDM 또는 MAM 정책에보안요구사항을매핑하여앱배포를간소화하고가속화할수있습니다. 특정앱을다르게배포하거나앱에서준수해야하는보안규정유형에따라 XenMobile 환경의아키텍처를변경해야할수있습니다. 예를들어중요한비즈니스인텔리전스앱을사용할수있도록장치를암호화해야거나종단간 SSL 암호화또는지오픈스가필요한특정앱을사용해야할수있습니다.
- **앱제공:** XenMobile 에서는앱을 MDM 앱또는 MAM 앱으로제공할수있습니다. MDM 앱은 XenMobile Store 에표시됩니다. 이스토어를사용하면장치수준제한을시행하는것외에도로앱을제어할필요가없으므로공용앱또는기본앱을사용자에게편리하게제공할수있습니다. 이와반대로 MAM 모드에서앱을제공하면앱제공과앱자체를완벽하게제어할수있습니다. 온-프레미스 XenMobile 배포에서 MDM 과함께앱관리요구사항을시행하는대부분의환경에서는 MAM 모드에서앱을제공하는것이더적합합니다. MAM 모드에서앱을제공하는경우모바일장치를 XME(MDM+MAM) 또는 MAM 전용 모드에등록해야합니다.
- **응용프로그램유지관리:**

- 초기감사수행: 프로덕션환경에있는앱버전과마지막업그레이드주기를지속적으로추적해야합니다. 업그레이드가필요한특정기능또는버그수정을기록하십시오.
- 기준설정: 각앱의안정적인최신릴리스목록을유지해야합니다. 업그레이드후에기치않은문제가발생할경우이앱버전으로폴백해야합니다. 또한롤백계획을개발해야합니다. 앱업그레이드를프로덕션환경에배포하기전에테스트환경에서테스트해야합니다. 가능한경우일부프로덕션사용자에게업그레이드를먼저배포한후전체사용자기반에배포합니다.
- Citrix 소프트웨어업데이트알림및타사소프트웨어공급업체알림구독: 앱의최신릴리스를유지하려면알림을구독하는것이중요합니다. 경우에따라테스트를위한 EAR(Early Access Release) 빌드가사전에제공될수도있습니다.
- 사용자알림을위한전략고안: 앱업그레이드가제공될때사용자에게알림을전송하는전략을정의해야합니다. 배포전에교육을제공하여사용자가준비할수있도록합니다. 앱업데이트전에여러번알림을전송할수있습니다. 앱에따라전자메일알림또는웹사이트가가장좋은알림방법이될수있습니다.

앱수명주기관리는앱의초기배포부터사용중지까지의전체수명주기를나타냅니다. 앱의수명주기는다음과같은 5 개단계로분류될수 있습니다.

1. 사양요구사항: 비즈니스사례및사용자요구사항에서시작됩니다.
2. 개발: 앱이비즈니스요구사항을충족하는지검증합니다.
3. 테스트: 테스트사용자, 문제및버그를식별합니다.
4. 배포: 앱을프로덕션사용자에게배포합니다.
5. 유지관리: 앱버전을업데이트합니다. 프로덕션환경에서앱을업데이트하기전에테스트환경에서앱을배포하십시오.

Secure Mail 을사용한응용프로그램수명주기에

1. 사양요구사항: 보안요구사항에따라, 컨테이너화되고 MDX 보안정책을지원하는메일앱이필요합니다.
2. 개발: 앱이비즈니스요구사항을충족하는지검증합니다. MDX 정책제어를앱에적용할수있어야합니다.
3. 테스트: Secure Mail 을테스트사용자그룹에할당하고 XenMobile Server 에서해당하는 MDX 파일을배포합니다. 테스트사용자가전자메일을성공적으로보내고받을수있으며일정및연락처에액세스할수있음을검증합니다. 또한테스트사용자는문제를보고하고버그를식별합니다. 테스트사용자의피드백에따라 Secure Mail 구성을프로덕션사용에맞게최적화합니다.
4. 배포: 테스트단계가완료되면 Secure Mail 을프로덕션사용자에게할당하고 XenMobile Server 에서해당하는 MDX 파일을배포합니다.
5. 유지관리: Secure Mail 의새로운업데이트가제공됩니다. Citrix 다운로드에서새 MDX 파일을다운로드하고 XenMobile Server 의기존 MDX 파일을대체합니다. 사용자에게업데이트를수행하도록알립니다. 참고: 앱을 XenMobile 프로덕션환경에업로드하고사용자에게배포하기전에테스트환경에서이프로세스를완료하고테스트하는것이 좋습니다.

자세한내용은 [iOS 모바일애플래핑](#) 및 [Android 모바일애플래핑](#) 항목을참조하십시오.

대시보드기반작업

January 6, 2020

XenMobile 콘솔대시보드에 액세스하여 정보를 한눈에 볼 수 있습니다. 이러한 정보를 사용하면 위젯을 통해 신속하게 문제점과 성공 여부를 확인할 수 있습니다.

대시보드는 일반적으로 XenMobile 콘솔에서 처음 로그인할 때 나타나거나 화면입니다. 콘솔의 다른 곳에서 대시보드에 액세스하려면 분석을 클릭합니다. 페이지의 레이아웃을 편집하고 나타나거나 위젯을 편집하려면 대시보드에서 사용자 지정 을 클릭합니다.

- **내 대시보드:** 최대 네 개의 대시보드를 저장할 수 있습니다. 이러한 대시보드를 개별적으로 편집하고 저장된 대시보드를 선택하여 각 대시보드를 볼 수 있습니다.
- **레이아웃 스타일:** 이 행에서는 대시보드에 표시되는 위젯 수와 위젯 배치 방법을 선택할 수 있습니다.
- **위젯 선택:** 대시보드에 표시할 정보를 선택할 수 있습니다.
 - **알림:** 왼쪽의 숫자 위에 있는 확인란을 선택하여 위젯 위에 알림 표시줄을 추가합니다. 이 표시줄에는 규격 장치, 비활성 장치 및 지난 24 시간 동안 초기화되거나 등록된 장치의 수가 표시됩니다.
 - **장치 (플랫폼 기준):** 플랫폼별로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다.
 - **장치 (이동통신사업자 기준):** 이동통신사업자별로 관리되는 장치와 관리되지 않는 장치의 수를 표시합니다. 각 표시줄을 클릭하여 플랫폼별 분석을 볼 수 있습니다.
 - **관리되는 장치 (플랫폼 기준):** 플랫폼별로 관리되는 장치의 수를 표시합니다.
 - **관리되지 않는 장치 (플랫폼 기준):** 플랫폼별로 관리되지 않는 장치의 수를 표시합니다. 이 차트에 나타나는 장치는 에이전트가 설치되어 있지만 권한이 해제되었거나 초기화되었을 수 있습니다.
 - **장치 (ActiveSync Gateway 상태 기준):** ActiveSync Gateway 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 차단됨, 허용됨 또는 알 수 없음 상태가 표시됩니다. 각 표시줄을 클릭하여 플랫폼별 로 데이터를 분류할 수 있습니다.
 - **장치 (소유권 기준):** 소유권 상태별로 그룹화된 장치 수를 표시합니다. 정보에는 회사 소유, 직원 소유 또는 알 수 없는 소유권 상태가 표시됩니다.
 - **Android TouchDown** 라이선스 상태: TouchDown 라이선스가 있는 장치의 수를 표시합니다.
 - **실패한 배달 그룹 배포:** 패키지당 실패한 배포의 총 수를 표시합니다. 배포에 실패한 패키지만 나타납니다.
 - **장치 (차단된 이유 기준):** ActiveSync 에이전트 차단된 장치의 수를 표시합니다.
 - **설치된 앱:** 이 위젯을 사용하면 앱 이름을 입력하여 그래프에 해당 앱에 대한 정보를 표시할 수 있습니다.
 - **VPP** 앱 라이선스 사용 현황: Apple Volume Purchase Program 앱에 대한 라이선스 사용 현황 통계를 표시합니다.

사용 사례

대시보드 위젯을 사용하여 환경을 모니터링하는 다수의 방법에 대한 몇 가지 예제는 다음과 같습니다.

- 모바일 생산성 앱을 배포한 후 모바일 생산성 앱이 장치에 설치되지 않는다는 내용의 지원 티켓을 받았습니다. 규정 위반 장치 및 설치된 앱 위젯을 사용하여 모바일 생산성 앱이 설치되지 않은 장치를 확인합니다.

- 비활성장치를 환경에서 제거하고 라이선스를 재확보하기 위해 비활성장치를 모니터링하려고 합니다. 비활성장치 위젯을 사용하여 통계를 추적합니다.
- 데이터가 올바르게 동기화되지 않는다는 내용의 지원 티켓을 받았습니다. 장치 (**ActiveSync Gateway** 상태 기준) 및 장치 (차단된 이유 기준) 위젯을 사용하여 문제가 ActiveSync 와 관련된 것인지 여부를 확인할 수 있습니다.

보고

환경 설정 및 사용자 등록이 완료된 후 보고서를 실행하여 배포에 관한 내용을 확인할 수 있습니다. XenMobile 은 환경에서 실행되는 장치를 파악하는데 도움이 되는 다수의 보고서를 기본적으로 제공합니다. 자세한 내용은 [보고서](#)에서 참조하십시오.

중요:

SQL Server 를 사용하여 사용자 지정 보고서를 만들 수 있지만 이 방법은 권장하지 않습니다. SQL Server 데이터베이스를 방법으로 사용하면 XenMobile 배포에 예기치 않은 결과가 발생할 수 있습니다. 이 방법의 보고서를 사용하기로 결정한 경우 읽기 전용 계정을 사용하여 SQL 쿼리를 실행해야 합니다.

역할 기반 액세스 제어 및 **XenMobile** 지원

July 5, 2019

XenMobile 은 RBAC(역할 기반 액세스 제어) 를 사용하여 XenMobile 시스템 기능 (예: XenMobile 콘솔, 자가 지원 포털, 원격 지원 및 공용 API) 에 대한 사용자 및 그룹의 액세스를 제한합니다. 이 문서에서는 XenMobile 에 기본 제공되는 역할과 XenMobile 에서 RBAC 를 활용하는 지원 모델을 결정할 때의 고려 사항에 대해 설명합니다.

참고:

2019 년 1 월 1 일부터 신규 고객에게는 더 이상 원격 지원이 제공되지 않습니다. 기존 고객은 제품을 계속 사용할 수 있지만 Citrix 는 개선 사항이나 수정 사항을 제공하지 않습니다.

기본 제공 역할

다음과 같은 기본 제공 역할에 부여되는 액세스 권한을 변경하고 역할을 추가할 수 있습니다. 각 역할에 연결된 액세스 및 기능 권한과 역할의 기본 설정을 모두 보려면 XenMobile 설명서에서 [Role-Based Access Control Defaults\(역할 기반 액세스 제어 기본값\)](#) 를 다운로드하십시오. 각 기능에 대한 정의는 XenMobile 설명서에서 [RBAC 를 사용하여 역할 구성](#) 을 참조하십시오.

관리 역할

부여되는 기본 액세스 권한:

- 자가 지원 포털 및 원격 지원 을 제외한 전체 시스템 액세스 권한.
- 기본적으로 관리자는 일부 지원 작업 (예: 연결 확인 및 지원 번들 만들기) 을 수행할 수 있습니다.

고려사항:

- 일부관리자또는전체관리자가자가지원포털또는원격지원에액세스해야합니까? 그렇다면관리역할을편집하거나고나리역할을추가할수있습니다.
- 일부관리자또는관리자그룹에대한엑세스를추가로제한하려면관리템플릿에따라역할을추가하고권한을편집합니다.

장치프로비전

부여되는기본액세스권한:

- XenMobile 콘솔에액세스하여 Windows CE 장치에대한기본적인관리작업 (장치추가, 변경및제거, 설정페이지사용)을수행할수있는권한.

고려사항:

- Windows CE 장치에만적용됩니다.

지원

부여되는기본액세스권한:

- 원격지원에대한액세스권한.

고려사항:

- 온-프레미스 XenMobile Server 배포의경우: 원격지원을사용하면지원센터담당자가관리되는 Windows CE 및 Android 모바일장치를원격으로제어할수있습니다. 스크린캐스트는 Samsung KNOX 장치에서만지원됩니다.
- 원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다.

사용자

부여되는기본액세스권한:

- 인증된사용자가등록링크를생성할수있는자가지원포털에대한액세스권한. 사용자는등록링크를사용하여장치를등록하거나등록초대를보낼수있습니다.
- XenMobile 콘솔에대한제한된액세스권한: 장치기능 (예: 장치초기화, 잠금/잠금해제, 컨테이너잠금/잠금해제, 위치확인및지리적제한설정, 장치벨울림, 컨테이너암호재설정), 등록초대추가, 제거및보내기.

고려사항:

- 사용자역할을할당하면사용자가직접지원리소스를찾을수있습니다.
- 공유장치를지원하려면공유장치등록에대한사용자역할을만듭니다.

XenMobile 지원모델에대한고려사항

채택할수있는지원모델은매우방대하며, 수준 1 및 2 지원을처리하는타사와수준 3 및 4 지원을처리하는직원이포함될수있습니다. 지원부하를분산하는방식에관계없이 XenMobile 배포및사용자기반에관한이섹션의고려사항을속지하십시오.

사용자가회사소유의장치를사용합니까? BYO 장치를사용합니까?

지원에영향을미치는기본적인질문은 XenMobile 환경의사용자장치를누가소유하는지에대한것입니다. 사용자가회사소유의장치를사용하는경우관리자는장치를잡그는방법으로하위수준을지원을제공할수있습니다. 이경우관리자는지원센터를통해장치문제에대한지원및장치사용방법에대한지원을사용자에게제공할수있습니다. 지원해야하는장치의유형에따라지원센터에대한 RBAC 장치프로비전및지원역할을어떻게사용할지고려하십시오.

사용자가 BYO 장치를사용하는경우사용자는장치지원에대한자료를직접찾아야할수있습니다. 이경우조직이제공하는지원은 XenMobile 관련문제에중점을둔관리역할에더가깝습니다.

데스크톱의지원모델은무엇입니까?

데스크톱의지원모델이다른회사소유장치에적절한지여부를고려하십시오. 동일한지원조직을사용할수있습니까? 추가로필요한교육은무엇입니까?

XenMobile 자가지원포털에대한액세스권한을사용자에게제공할계획입니까?

일부조직은 XenMobile 에대한액세스권한을사용자에게부여하는것을선호하지않지만사용자에게일부자가지원기능기능을제공하면지원조직의부하를줄일수있습니다. RBAC 의기본사용자역할에원하지않는권한이포함된다면원하는권한만포함된새역할을만들어보십시오. 요구사항을충족하는데필요한수의역할을만들수있습니다.

시스템모니터링

October 21, 2019

앱액세스및연결을위한작동시간을최적화하려면 XenMobile 환경에서다음과같은핵심구성요소를모니터링해야합니다.

XenMobile 서버

XenMobile 서버는로그를생성하여로컬스토리지에저장합니다. 이로그를시스템로그 (syslog) 서버로내보낼수있습니다. 로그설정을구성하여크기제한또는로그수준을지정하거나특정이벤트를필터링하는사용자지정로그를생성할수있습니다. 언제든지 XenMobile 콘솔에서 XenMobile 서버로그를확인할수있습니다. 또한 syslog 서버를통해로그의정보를프로덕션 Splunk 로깅서버로내보낼수있습니다.

다음목록에는 XenMobile 에서사용할수있는서로다른로그파일유형이설명되어있습니다.

디버그로그파일: XenMobile 의핵심웹서비스에대한디버그수준정보 (오류메시지및서버관련동작포함) 가포함됩니다.

메시지형식:

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>
```

- 여기서 <id>는고유식별자 (예: sessionID) 입니다.
- 여기서 <log message>는응용프로그램이제공하는메시지입니다.

관리자감사로그파일: XenMobile 콘솔작업에대한감사정보가포함됩니다.

참고:

관리자감사로그와사용자감사로그에는동일한형식이사용됩니다.

메시지형식:

필수적인날짜및타임스탬프값을제외한다른모든특성은선택사항입니다. 선택적필드는메시지에서 “ ”로표시됩니다.

```
<date> <timestamp> "<username/id>"<sessionid>"<deviceid>"<clientip>"
"<action>"<status>"<application name>"<app user id>"<user agent>"<
details>"
```

다음표에는사용가능한관리자감사로그이벤트가나열되어있습니다.

이벤트용관리자감사로그메시지	상태
로그인	성공/실패
로그아웃	성공/실패
관리자가져오기	성공/실패
관리자업데이트	성공/실패
응용프로그램가져오기	성공/실패
응용프로그램추가	성공/실패
응용프로그램업데이트	성공/실패
응용프로그램삭제	성공/실패
응용프로그램바인딩	성공/실패
응용프로그램바인딩해제	성공/실패
응용프로그램사용안함	성공/실패
응용프로그램사용	성공/실패
범주가져오기	성공/실패
범주추가	성공/실패
범주업데이트	성공/실패
그룹삭제	성공/실패
인증서추가	성공/실패
인증서삭제	성공/실패

이벤트용관리자감사로그메시지	상태
활성인증서	성공/실패
CSR 인증서	성공/실패
인증서내보내기	성공/실패
인증서체인삭제	성공/실패
인증서체인추가	성공/실패
커넥터가져오기	성공/실패
커넥터추가	성공/실패
커넥터삭제	성공/실패
커넥터업데이트	성공/실패
장치가져오기	성공/실패
장치잠금	성공/실패
장치잠금해제	성공/실패
장치초기화	성공/실패
장치초기화취소	성공/실패
장치삭제	성공/실패
역할가져오기	성공/실패
역할추가	성공/실패
역할업데이트	성공/실패
역할삭제	성공/실패
역할바인딩	성공/실패
역할바인딩해제	성공/실패
구성설정업데이트	성공/실패
워크플로전자메일업데이트	성공/실패
워크플로추가	성공/실패
워크플로삭제	성공/실패
Active Directory 추가	성공/실패
Active Directory 업데이트	성공/실패
masteruserlist 추가	성공/실패
masteruserlist 업데이트	성공/실패

이벤트용관리자감사로그메시지	상태
DNS 업데이트	성공/실패
네트워크업데이트	성공/실패
로그서버업데이트	성공/실패
로그서버의로그전송	성공/실패
syslog 업데이트	성공/실패
Receiver 업데이트관련업데이트	성공/실패
시간서버업데이트	성공/실패
신뢰업데이트	성공/실패
서비스레코드추가	성공/실패
서비스레코드업데이트	성공/실패
Receiver 전자메일업데이트	성공/실패
패치업로드	성공/실패
스냅샷가져오기	성공/실패
앱스토어앱세부정보가져오기	성공/실패
MDM 업데이트	성공/실패
MDM 삭제	성공/실패
HDX 추가	성공/실패
HDX 업데이트	성공/실패
HDX 삭제	성공/실패
브랜딩추가	성공/실패
브랜딩삭제	성공/실패
SSL 오프로드업데이트	성공/실패
계정속성추가	성공/실패
계정속성삭제	성공/실패
계정속성업데이트	성공/실패
알림추가	성공/실패

사용자감사로그파일: 등록된장치의사용자활동과관련된정보가포함됩니다.

참고:

사용자감사로그와관리자감사로그에는동일한형식이사용됩니다.

메시지형식:

필수적인날짜및타임스탬프값을제외한다면다른모든특성은선택사항입니다. 선택적필드는메시지에서 “ ”로표시됩니다. 예를들면다음과같습니다.

```
<date> <timestamp> "<username/id>"<sessionid>"<deviceid>"<clientip>"
"<action>"<status>"<application name>"<app user id>"<user agent>"<
details>"
```

다음표에는사용가능한사용자감사로그이벤트가나열되어있습니다.

이벤트용사용자감사로그메시지	상태
로그인	성공/실패
세션시간초과	성공/실패
구독	성공/실패
등록취소	성공/실패
사전시작	성공/실패
AGEE SSO	성공/실패
ShareFile 용 SAML 토큰	성공/실패
장치등록	성공/실패
장치확인	잠금/초기화
장치업데이트	성공/실패
토큰새로고침	성공/실패
암호저장됨	성공/실패
암호검색됨	성공/실패
사용자가암호변경을시작함	성공/실패
모바일클라이언트다운로드	성공/실패
로그아웃	성공/실패
검색서비스	성공/실패
끝점서비스	성공/실패

MDM 기능	상태
REGHIVE	성공/실패
Cab 인벤토리	성공/실패
Cab	성공/실패
Cab 자동설치	성공/실패
Cab 셸설치	성공/실패
Cab 폴더만들기	성공/실패
Cab 파일가져오기	성공/실패
파일폴더만들기	성공/실패
파일가져오기	성공/실패
파일전송됨	성공/실패
스크립트폴더만들기	성공/실패
스크립트가져오기	성공/실패
스크립트전송됨	성공/실패
스크립트셸실행	성공/실패
스크립트자동실행	성공/실패
APK 인벤토리	성공/실패
APK	성공/실패
APK 셸설치	성공/실패
APK 자동설치	성공/실패
APK 폴더만들기	성공/실패
APK 파일가져오기	성공/실패
APK 앱	성공/실패
EXT 앱	성공/실패
목록가져오기	성공/실패
목록전송됨	성공/실패
장치찾기	성공/실패
CFG	성공/실패
잠금해제	성공/실패
SharePoint 초기화	성공/실패

MDM 기능	상태
SharePoint 구성	성공/실패
프로필제거	성공/실패
응용프로그램제거	성공/실패
관리되지않는응용프로그램제거	성공/실패
관리되지않는프로필제거	성공/실패
IPA 앱	성공/실패
EXT 앱	성공/실패
상환코드적용	성공/실패
설정적용	성공/실패
장치추적사용	성공/실패
앱관리정책	성공/실패
SD 카드초기화	성공/실패
암호화된전자메일첨부파일	성공/실패
브랜딩	성공/실패
보안브라우저	성공/실패
컨테이너브라우저	성공/실패
컨테이너잠금해제	성공/실패
컨테이너암호재설정	성공/실패
AG 클라이언트인증자격증명	성공/실패

NetScaler 는 각 XenMobile 서버클러스터노드에대한 HTTP 요청을 시뮬레이션하는 지능형모니터링프로브로 구성된 XenMobile 웹서비스상태도모니터링합니다. 이프로브는서비스가온라인상태인지확인한후수신된응답에따라응답합니다. 노드 가예상대로응답하지않는경우 NetScaler 는서버를중단상태로표시합니다. 또한 NetScaler 는노드를부하분산폴에서제거하 고, NetScaler 모니터링솔루션을통해알림을생성하는데사용할이벤트를기록합니다.

관리자는표준하이퍼바이저모니터링도구를사용하여 XenMobile 가상컴퓨터를모니터링하고 CPU, 메모리, 스토리지사용률메 트릭에관한알림을제공할수도있습니다.

SQL Server 및데이터베이스

SQL Server 및데이터베이스성능은 XenMobile Service 에직접적인영향을미칩니다. XenMobile 인스턴스는항상데이 터베이스에액세스할수있어야하며 SQL 인프라가중단될경우오프라인으로전환됩니다 (예: 응답하지않음). XenMobile 콘

솔은 SQL Server 에서디스크공간문제가발생한후잠시동안작동을계속할수있습니다. 데이터베이스가동시간을최대화하고 XenMobile 작업부하를처리하기에충분한수준의성능을유지하려면 [Microsoft 권장사항](#)에따라 SQL Server 의상태를사전에 모니터링해야합니다. 또한 XenMobile 환경이확장됨에따라 CPU, 메모리및스토리지에대한리소스할당을조정하여서비스수준 계약을보장해야합니다.

NetScaler

NetScaler 는내부스토리지에메트릭을기록하거나외부로그서버로로그를보낼수있는기능을제공합니다. NetScaler 로그를프로덕션 Splunk 로그서버로내보내도록 syslog 서버를구성할수있습니다. NetScaler 에서사용할수있는로그수준은다음과같습니다.

- 긴급
- 알림
- 중요
- 오류
- 경고
- 정보

로그파일은 NetScaler 스토리지의 /var/log/ns.log 디렉터리에 newnslog 라는이름으로도저장됩니다. NetScaler 는 GZIP 알고리즘을사용하여파일을오버하고압축합니다. 로그파일이름은 newnslog.xx.gz 형식을사용하며여기서 xx 는실행 번호를나타냅니다.

NetScaler 는모니터링옵션으로 SNMP 트랩및알림도지원합니다. SNMP 트랩목록은 [SNMP 모니터링](#)을참조하십시오.

재해복구

May 21, 2019

재해복구를위해활성/수동장애조치 (failover) 전략을사용하여여러사이트가포함된 XenMobile 배포를설계하고구성할수있습니다.

이문서에서설명하는권장재해복구전략은다음으로구성됩니다.

- 모든엔터프라이즈사용자에게글로벌서비스를제공하는첫번째지리적위치의데이터센터에있는단일의 XenMobile 활성사이트 (기본사이트).
- 두번째지리적위치의데이터센터에있는두번째 XenMobile 사이트 (재해복구사이트). 이재해복구사이트는기본사이트에서사이트전체데이터센터장애가발생하는경우활성-비활성사이트장애조치 (failover) 를제공합니다. 기본사이트에는장애조치 (failover) 를용이하게하는 XenMobile, SQL 데이터베이스, NetScaler 인프라가포함되며기본사이트에대한 연결실때이벤트를통해사용자에게 XenMobile 에대한액세스를제공합니다.

재해복구사이트의 XenMobile 서버는 정상작동중에도 오프라인으로 유지되며 기본사이트의 전체사이트를 재해복구사이트로 장애 조치 (failover) 해야 하는 재해복구시나리오에서만 온라인으로 전환됩니다. 재해복구사이트의 SQL Server 는 재해복구사이트에서 XenMobile 서버를 시작하기 전에 활성상태이고 연결을 제공할 준비가 되어 있어야 합니다.

이재해복구전략은 중단시 MDM 및 MAM 연결을 재해복구사이트로 라우팅하도록 DNS 를 변경함으로써 NetScaler 액세스 계층을 수동으로 장애 조치 (failover) 합니다.

참고:

이 아키텍처를 사용하려면 비동기식 데이터베이스 백업에 대한 프로세스와 SQL 인프라의고가용성을 보장할 방법이 있어야 합니다.

재해복구 장애 조치 (failover) 프로세스

1. 재해복구 장애 조치 (failover) 프로세스를 테스트하려면 기본사이트에서 XenMobile 서버를 종료하여 사이트 장애를 시뮬레이션합니다.
2. XenMobile 서버의 공용 DNS 레코드를 재해복구사이트의 외부 IP 주소를 가리키도록 변경합니다.
3. SQL Server 의 내부 DNS 레코드를 재해복구사이트의 SQL Server IP 주소를 가리키도록 변경합니다.
4. 재해복구사이트에서 XenMobile SQL 데이터베이스를 온라인으로 전환합니다. SQL Server 및 데이터베이스가 활성상태이고 로컬 XenMobile 서버에서 사이트로의 연결을 제공할 준비가 되었는지 확인합니다.
5. 재해복구사이트에서 XenMobile 서버를 켭니다.

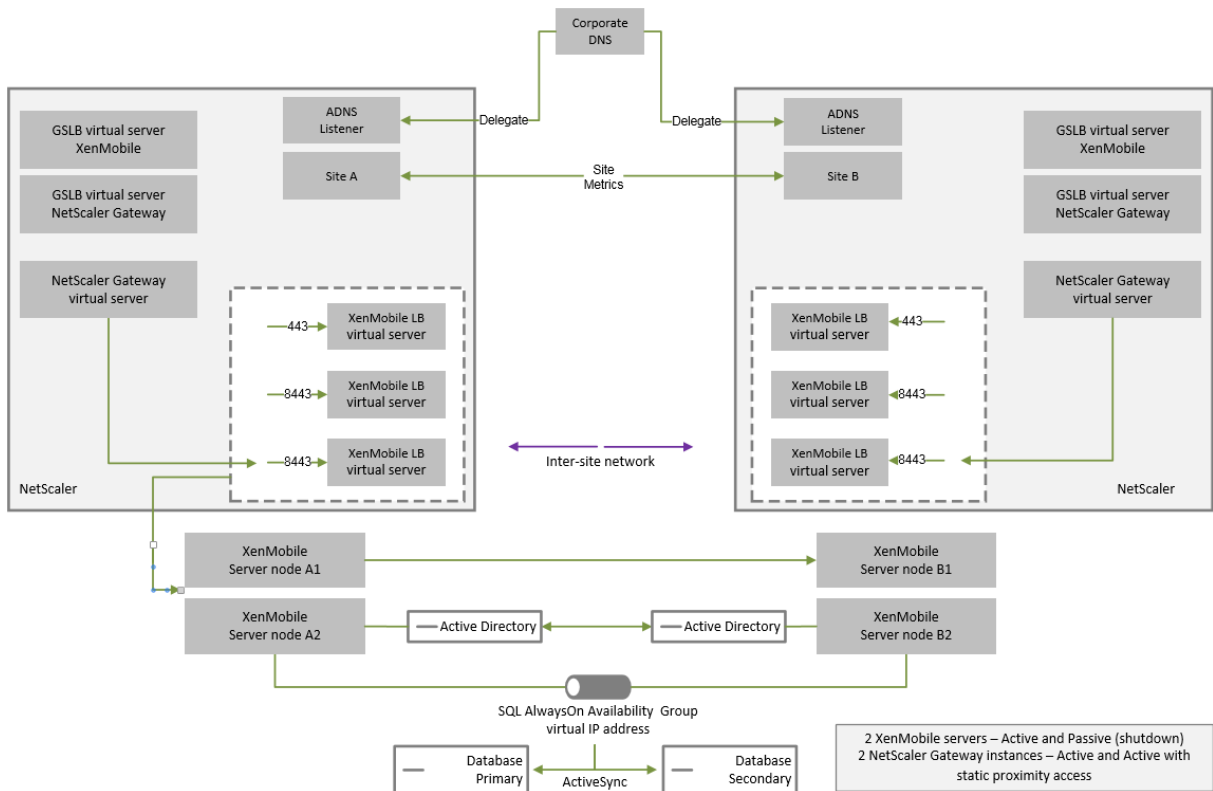
XenMobile 서버 업데이트 프로세스

패치 및 릴리스로 XenMobile 을 업데이트 할 때는 다음 단계에 따라 기본 서버와 재해복구 서버의 코드를 동일하게 유지하십시오.

1. 기본사이트의 XenMobile 서버에 패치가 적용되었거나 업그레이드되었는지 확인합니다.
2. SQL Server 의 DNS 레코드가 기본사이트의 활성 SQL Server 데이터베이스로 확인되는지 확인합니다.
3. 재해복구사이트의 XenMobile 서버를 온라인으로 전환합니다. 이 서버는 업그레이드 프로세스 중에만 WAN 의 기본사이트 데이터베이스에 연결합니다.
4. 필요한 패치 및 업데이트를 모든 재해복구사이트의 XenMobile 서버에 적용합니다.
5. XenMobile Server 를 다시 시작하고 패치 또는 업그레이드가 성공했는지 확인합니다.

재해복구 참조 아키텍처 다이어그램

다음 다이어그램은 XenMobile 의 재해복구 배포에 대한 아키텍처 개요를 보여줍니다.



재해복구용 GSLB

이아키텍처의주요요소는 GSLB(Global Server Load Balancing) 를 사용하여트래픽을올바른데이터센터로전달하는것입
니다.

기본적으로 XenMobile 용 NetScaler 마법사에서는재해복구에 GSLB 를사용하지않는방식으로 NetScaler Gateway 가
구성됩니다. 따라서추가단계를수행해야합니다.

GSLB 의작동방식

GSLB 는 DNS 형태로존재합니다. 참여 NetScaler 장비는신뢰할수있는 DNS 서버역할을하며 DNS 레코드를올바른 IP 주소
(일반적으로트래픽을수신할수있는 VIP) 로확인합니다. NetScaler 장비는트래픽을해당시스템으로전달하는 DNS 쿼리에응답
하기전에시스템상태를확인합니다.

레코드가확인되면트래픽을확인하는 GSLB 의역할이완료됩니다. 클라이언트는대상 VIP(가상 IP) 주소와직접통신합니다. DNS
클라이언트동작은레코드의만료방식과시기를제어하는데있어서중요한역할을합니다. 이는주로 NetScaler 시스템의경계외부에
서수행됩니다. 따라서 GSLB 에는 DNS 이름확인과동일한제한이적용됩니다. 클라이언트가응답을캐시하므로이방식의부하분
산은기존의부하분산과달리실시간으로수행되지않습니다.

NetScaler 의 GSLB 구성 (사이트, 서비스및모니터포함) 은올바른 DNS 이름확인을제공하는데사용됩니다.

서버게시를위한실제구성 (이시나리오에서는 XenMobile 용 NetScaler 마법사에서생성되는구성) 은 GSLB 의영향을받지않습니다. GSLB 는 NetScaler 에있는개별서비스입니다.

XenMobile 에서 **GSLB** 를사용하는경우의도메인위임문제

XenMobile 용 NetScaler Gateway 는 XenMobile 용 NetScaler 마법사에서구성됩니다. 이마법사는부하분산가상서버세개와 NetScaler Gateway 가상서버한개를생성합니다.

부하분산가상서버두개는포트 443 및 8443 에서 MDM 트래픽을처리합니다. NetScaler Gateway 는포트 8443 에서 MAM 트래픽을수신한후세번째서버인 MAM 부하분산가상서버에전달합니다. MAM 부하분산가상서버로이동하는모든트래픽인 NetScaler Gateway 를통과합니다.

MAM 부하분산가상서버에는 XenMobile 서버와동일한 SSL 인증서가필요하며장치등록시사용된 FQDN 과동일한 FQDN 이사용됩니다. 또한또 MAM 부하분산서버는 MDM 부하분산서버중하나와동일한포트 (8443) 를사용합니다. 트래픽을확인하기위해 XenMobile 용 NetScaler 마법사는 NetScaler Gateway 에로컬 DNS 레코드를생성합니다. DNS 레코드는장치등록시사용된 FQDN 과일치합니다.

이구성은 XenMobile 서버 URL 이 GSLB 도메인 URL 이아닌경우적용됩니다. GSLB 도메인 URL 이재해복구를이유로 XenMobile 서버 URL 로사용된경우로컬 DNS 레코드로인해 NetScaler Gateway 가 MDM 부하분산서버로의트래픽을확인할수없게됩니다.

GSLB 재해복구의 **CNAME** 방법

XenMobile 용 NetScaler 마법사의기본구성으로인해발생하는문제를해결하려면상위도메인 (`company.com`) 에 XenMobile 서버 FQDN 에대한 CNAME 레코드를생성하고신뢰할수있는 NetScaler 의위임된하위영역 (`gslb.company.com`) 에있는레코드를가리키면됩니다. 이렇게하면트래픽을확인하는데필요한 MAM 부하분산 VIP 주소에대한정적 DNS A 레코드를생성할수있습니다.

1. 외부 DNS 에서 NetScaler GSLB 의 GSLB 도메인 FQDN 을가리키는 XenMobile 서버 FQDN 에대한 CNAME 를생성합니다. 두개의 GSLB 도메인이필요합니다. 하나는 MDM 트래픽을위한것이고다른한나는 MAM(NetScaler Gateway) 트래픽을위한것입니다.

예:

```
CNAME = xms.company.com IN CNAME xms.gslb.comany.com
```

2. 각사이트의 NetScaler Gateway 인스턴스에서 CNAME 레코드가가리키는 FQDN 으로 GSLB 가상서버를생성합니다.

예:

```
bind gslb vserver xms-gslb -domainName xms.gslb.company.com
```

XenMobile 용 NetScaler 마법사를사용하여 NetScaler Gateway 를배포하는경우 MAM 부하분산서버를구성할때 XenMobile 서버 URL 을사용하십시오. 그러면 XenMobile 서버 URL 에대한정적 DNS A 레코드가생성됩니다.

3. XenMobile 서버 URL([xms.company.com](#)) 을 사용하여 Secure Hub 에등록하는클라이언트를테스트합니다.

이예에서는다음 FQDN 을사용합니다.

- [xms.company.com](#) - MDM 트래픽과장치등록에 사용되는 URL 이며이예에서는 XenMobile 용 NetScaler 마법사를사용하여구성되었습니다.
- [xms.gslb.company.com](#) - XenMobile 서버의 GSLB 도메인 FQDN 입니다.

Citrix 지원프로세스

September 27, 2019

Citrix 기술지원서비스를켜면 Citrix 제품관련문제에대한지원을받을수있습니다. 이그룹은해결방법및해결책을제공하며개발팀과협력하여솔루션을제공합니다.

Citrix Consulting Services 또는 Citrix Education Services 는제품교육과관련된지원과함께제품사용, 구성, 설치또는환경설계및아키텍처에관한조언을제공합니다.

Citrix Consulting 은 POC, 경제적영향평가, 인프라상태확인, 설계요구사항분석, 아키텍처설계확인, 통합및운영프로세스개발등 Citrix 제품관련프로젝트를지원합니다.

Citrix Education 은 Citrix 가상화, 클라우드및네트워킹기술에대한업계최고의 IT 교육및인증을제공합니다.

지원사례를작성하기전에자가지원리소스및권장사항을완벽하게검토하는것이 좋습니다. 예를들어 Citrix 기술전문가가작성한문서와공지에엑세스하거나, Citrix 솔루션및기술에대한제품설명서를보거나, Citrix 경영진, 제품팀및기술전문가의직설을읽어볼수있는다수의위치가있습니다. 각각 [Knowledge Center](#), [제품설명서](#) 및 [블로그](#) 페이지를참조하십시오.

추가적인대화형지원이필요하다면토론포럼에참여하여다른고객으로부터질문에대한실시간답변을얻거나, 사용자그룹및관심그룹내에서아이디어, 의견, 기술정보및모범사례를공유하거나, Citrix 지원의소셜네트워킹사이트를모니터링하는 Citrix 지원엔지니어와상호작용할수있습니다. 각각 [지원포럼](#), [Citrix Community](#) 및 [Twitter](#) 의 [Citrix 지원](#) 페이지를참조하십시오.

교육및인증과정에엑세스하여기술을강화할수도있습니다. [Citrix Education](#)에서자세한내용을참조하십시오.

Citrix Insight Services 는단순한온라인문제해결플랫폼과 Citrix 환경을위한상태감사기를제공합니다. XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor 및 Citrix Gateway 에서사용할수있습니다. [분석도구](#)에서자세한내용을참조하십시오.

기술지원을받으려면전화또는웹을통해지원사례를만들어야합니다. 중요도가낮거나중간인문제에대해서는웹을사용하고, 중요도가높은문제에대해서는전화옵션을사용할수있습니다. XenMobile 문제와관련하여지원을문의하는방법에대한자세한내용은 [지원부서에문의하는방법](#)을참조하십시오.

Citrix 솔루션제공에대한방대한경험을갖춘, 고도로숙련된단일의담당자를원한다면 Citrix 서비스의 Technical Relationship Manager 에게문의할수있습니다. Citrix 서비스제공및이점에대한자세한내용은 [Citrix Worldwide Services](#)를참조하십시오.

XenMobile 에서그룹등록초대보내기

May 21, 2019

작성자: John Bartel III

XenMobile 에서그룹에등록초대를보낼수있습니다. 중첩그룹에도초대를보낼수있습니다. 그룹초대를설정할때하나이상의장치 플랫폼을지정할수있습니다. 또한장치에태그를지정하여회사소유의장치를직원소유의장치와구분하는등의작업을수행할수있습니다. 그런다음사용자장치에대한인증유형을설정합니다.

참고:

사용자지정알림플릿을사용하려는경우등록모드를구성하기전에플릿을설정해야합니다. 알림플릿에대한자세한내용은 [알림플릿만들기및업데이트](#) 문서를참조하십시오.

사용자계정, 역할및등록모드와초대의기본구성에대한자세한내용은 [사용자계정, 역할및등록](#)을참조하십시오.

일반단계

1. XenMobile 콘솔에서 관리 > 등록초대로이동합니다.
2. 화면왼쪽위의 추가를클릭하고 초대추가를클릭합니다.
3. 받는사람메뉴에서 그룹을클릭합니다.

이단계에서하나이상의플랫폼을선택할수있습니다. 회사내에서로다른운영체제플랫폼조합이있는경우모든플랫폼을선택합니다. 확실히사용되지않는플랫폼만선택을취소합니다.

4. 초대프로세스중에장치태그를지정하도록선택할수있습니다. 회사또는 직원을선택합니다.

태그를지정하면회사소유의장치와직원소유의장치를쉽게구분할수있습니다.

5. 도메인목록에서그룹이있는도메인을선택합니다.
6. 그룹목록에서초대를보낼 Active Directory 그룹을선택합니다.
7. 등록모드를사용하여사용자에게원하는인증유형을설정할수있습니다.

- 사용자이름 + 암호
- 높은수준의보안
- 초대 URL
- 초대 URL + PIN
- 초대 URL + 암호
- 2 단계
- 사용자이름 + PIN

8. 에이전트다운로드, 등록 **URL**, 등록 **PIN** 및 등록확인플릿에대해이전에만든사용자지정알림플릿을선택합니다. 또는나열된기본값을선택합니다.

사용자 지정 알림 템플릿을 사용하려는 경우 등록 모드를 구성하기 전에 템플릿을 설정해야 합니다. 알림 템플릿에 대한 자세한 내용은 [알림](#) 문서를 참조하십시오.

이러한 알림 템플릿에는 XenMobile 내에서 구성된 SMTP 서버 설정을 사용합니다. 계속하기 전에 SMTP 정보를 먼저 설정합니다.

참고:

다음 이후에 만료 및 최대 시도 횟수 옵션은 선택한 등록 모드 옵션에 따라 변경됩니다. 이러한 옵션은 변경할 수 없습니다.

9. 초대 보내기 대해 쉼을 선택한 다음 저장 및 보내기를 클릭하여 프로세스를 완료합니다.

중첩 그룹 지원

중첩 그룹을 사용하여 초대 보내 수 있습니다. 일반적으로 중첩 그룹은 유사한 권한을 가진 그룹이 서로 바인딩되어 있는 대규모 환경에서 사용됩니다.

설정 > **LDAP** 로 이동하고 중첩 그룹 지원 옵션을 사용하도록 설정합니다.

문제 해결 및 알려진 제한

문제: Active Directory 그룹에서 제거된 사용자에게도 초대가 전송됩니다.

해결 방법: Active Directory 환경의 규모에 따라 변경 내용이 모든 서버로 전파되는데 최대 6 시간이 소요될 수 있습니다. 최근에서 사용자 또는 중첩 그룹을 제거한 경우 XenMobile 에서 이러한 사용자가 그룹의 일부로 간주될 수 있습니다.

그러므로 그룹에 다른 그룹 초대를 보내기 전에 최대 6 시간을 기다리는 것이 가장 좋습니다.

온-프레미스 장치 상태 증명 서버 구성

January 6, 2020

작성자: Sanket Mishra

Windows 10 모바일 장치에 대한 DHA(장치 상태 증명) 를 온-프레미스 Windows 서버를 통해 사용할 수 있습니다. DHA 온-프레미스를 사용하려면 먼저 DHA 서버를 구성해야 합니다.

DHA 서버를 구성한 후 온-프레미스 DHA 서비스를 사용하도록 설정하는 XenMobile Server 정책을 만듭니다. 이 정책 생성에 대한 자세한 내용은 [장치 상태 증명 장치 정책](#) 을 참조하십시오.

DHA 서버의 사전 요구 사항

- 데스크톱 환경 설치 옵션을 사용하여 설치된 Windows Server Technical Preview 5 이상을 실행하는 서버.

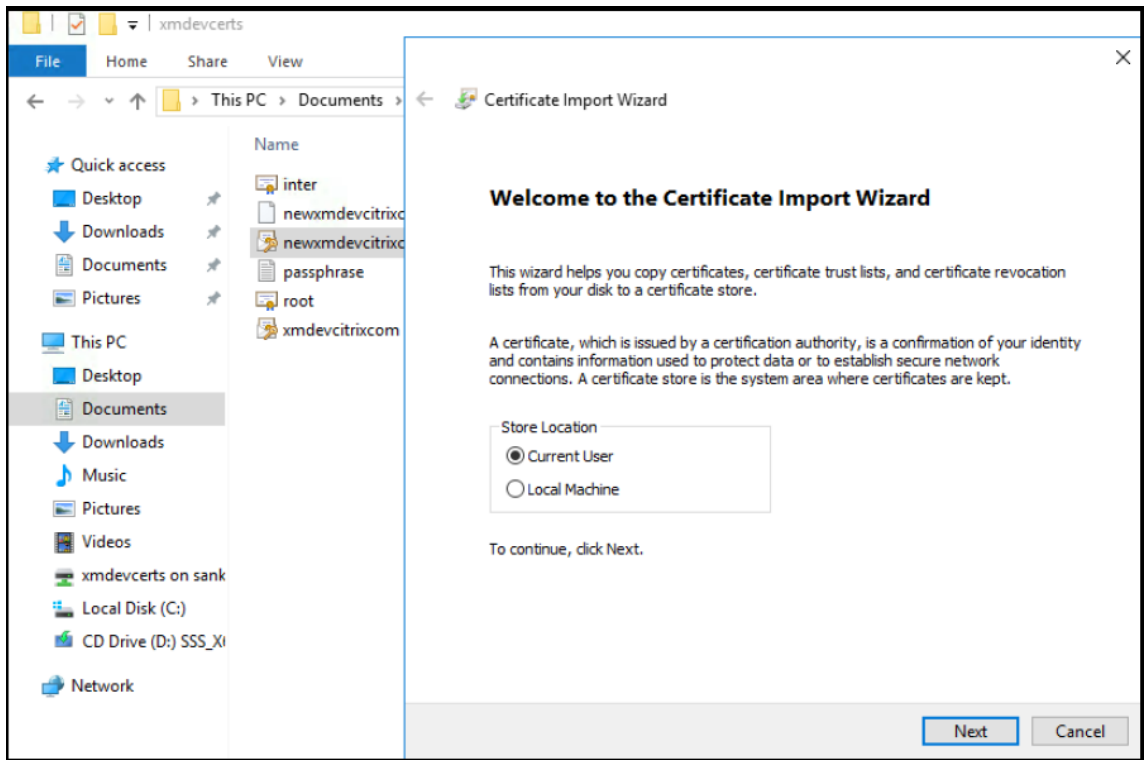
- 하나 이상의 Windows 10 클라이언트 장치. 이러한 장치에는 최신 버전의 Windows 를 실행하는 TPM 1.2 또는 2.0 이 있어야 합니다.
- 인증서:
 - **DHA SSL** 인증서. 내보내기 가능한 개인 키를 사용하여 엔터프라이즈의 신뢰할 수 있는 루트 체인으로 연결되는 x.509 SSL 인증서. 이 인증서는 서버-서버 (DHA 서비스와 MDM 서버) 및 서버-클라이언트 (DHA 서비스와 Windows 10 장치) 커뮤니케이션을 포함하여 전송 중인 DHA 데이터 통신을 보호합니다.
 - **DHA 서명** 인증서. 내보내기 가능한 개인 키를 사용하여 엔터프라이즈의 신뢰할 수 있는 루트 체인으로 연결되는 x.509 인증서. DHA 서비스는 이 인증서를 디지털 서명에 사용합니다.
 - **DHA 암호화** 인증서. 내보내기 가능한 개인 키를 사용하여 엔터프라이즈의 신뢰할 수 있는 루트 체인으로 연결되는 x.509 인증서. DHA 서비스는 이 인증서를 암호화에도 사용합니다.
- 다음과 같은 인증서 유효성 검사 모드 중에서 하나를 선택합니다.
 - **EKCert.** EKCert 유효성 검사 모드는 인터넷에 연결되지 않은 조직의 장치에 최적화되었습니다. EKCert 유효성 검사 모드에서 실행되는 DHA 서비스에 연결하는 장치는 인터넷에 직접 연결할 수 없습니다.
 - **AIKCert.** AIKCert 유효성 검사 모드는 인터넷에 액세스할 수 있는 작동 환경에 최적화되었습니다. AIKCert 유효성 검사 모드에서 실행되는 DHA 서비스에 연결하는 장치는 인터넷에 직접 연결할 수 있고 Microsoft 에서 AIK 인증서를 가져올 수 있어야 합니다.

Windows 서버에 DHA 서버 역할 추가

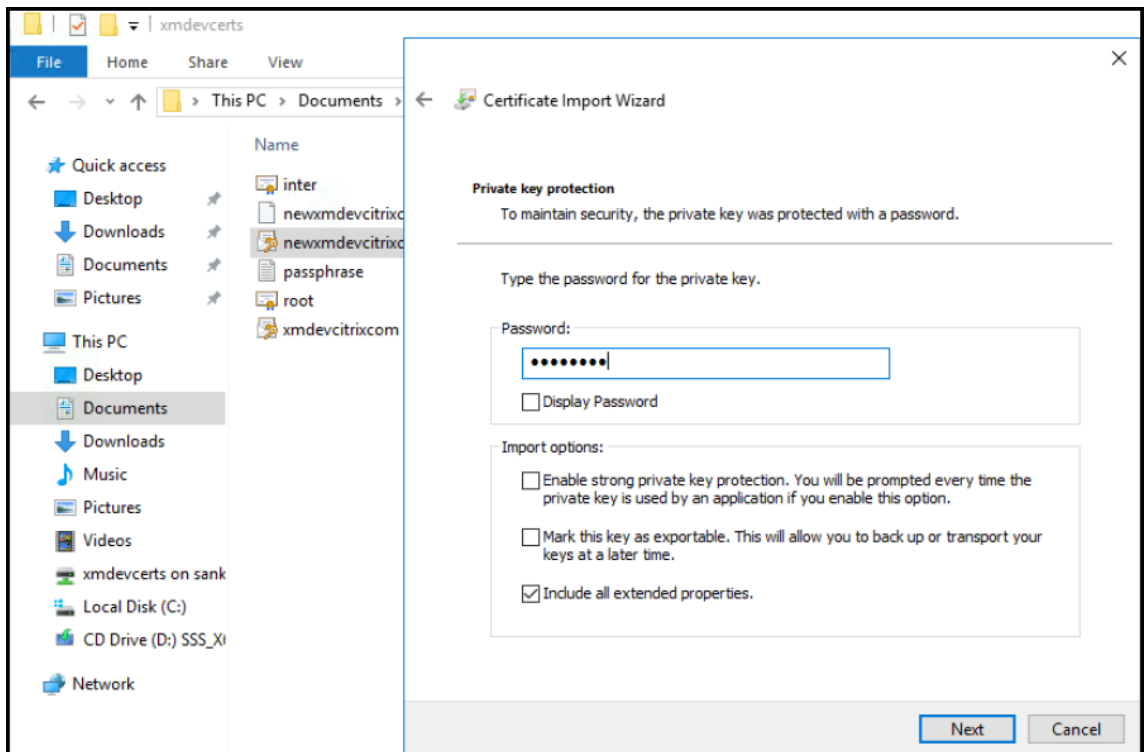
1. Windows 서버에서 서버 관리자가 이미 열려 있지 않은 경우 시작을 클릭하고 서버 관리자를 클릭합니다.
2. 역할 및 기능 추가를 클릭합니다.
3. 시작하기 전에 페이지에서 다음을 클릭합니다.
4. 설치 유형 선택 페이지에서 역할 기반 또는 기능 기반 설치를 클릭하고 다음을 클릭합니다.
5. 대상 서버 선택 페이지에서 서버 풀에서 서버 선택을 클릭하고 서버를 선택한 후 다음을 클릭합니다.
6. 서버 역할 선택 페이지에서 장치 상태 증명서 인란을 선택합니다.
7. 선택 사항: 기능 추가를 클릭하여 필요한 다른 역할 서비스 및 기능을 설치합니다.
8. 다음을 클릭합니다.
9. 기능 선택 페이지에서 다음을 클릭합니다.
10. 웹 서버 역할 (IIS) 페이지에서 다음을 클릭합니다.
11. 역할 서비스 선택 페이지에서 다음을 클릭합니다.
12. 장치 상태 증명서 서비스 페이지에서 다음을 클릭합니다.
13. 설치 선택 확인 페이지에서 설치를 클릭합니다.
14. 설치가 완료되면 닫기를 클릭합니다.

서버의 인증서 저장소에 SSL 인증서 추가

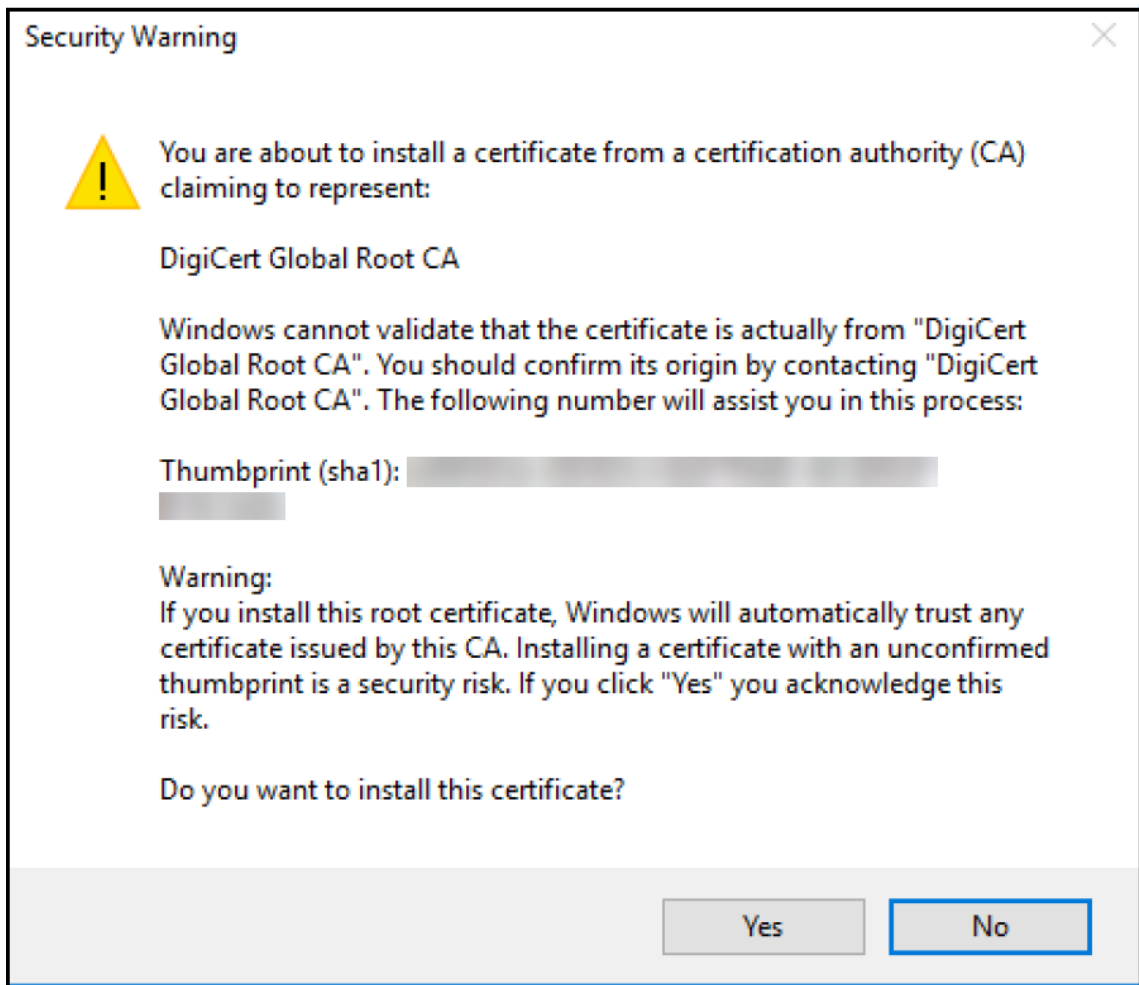
1. SSL 인증서 파일을 이동하고 파일을 선택합니다.
2. 현재 사용자를 저장소 위치로 선택하고 다음을 클릭합니다.



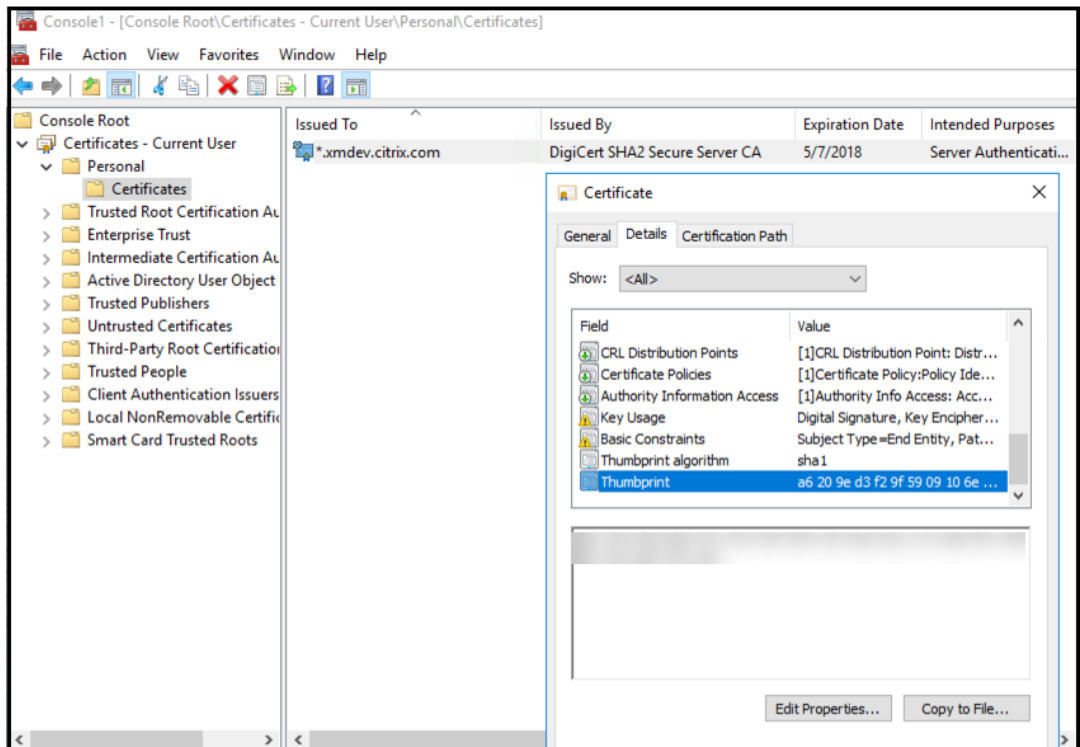
3. 개인키에대한암호를입력합니다.
4. 확장속성모두포함가져오기옵션이선택되었는지확인합니다. 다음을클릭합니다.



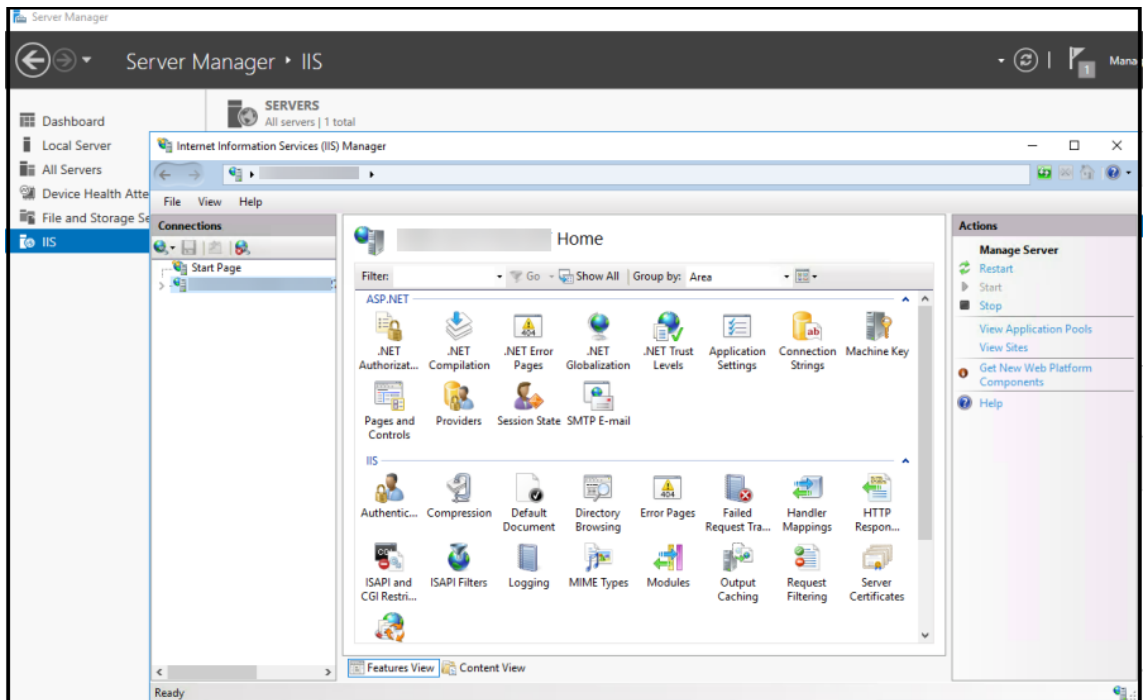
5. 이창이나타나면 예를클릭합니다.



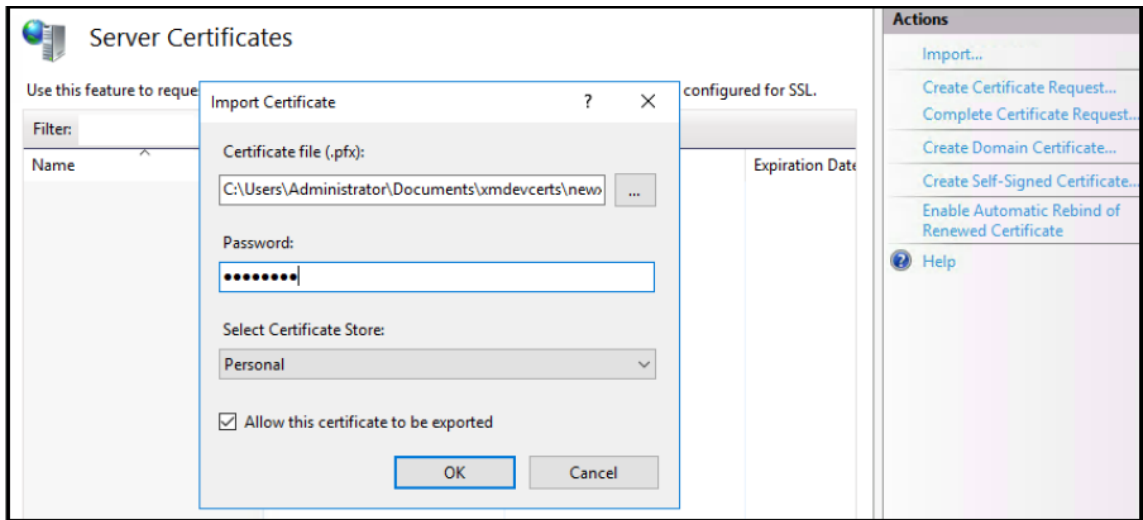
6. 인증서가설치되었는지확인합니다.
 - a) 명령프롬프트창을열니다.
 - b) **mmc** 를입력하고 Enter 키를누릅니다. 로컬컴퓨터저장소의인증서를보려면관리자역할이있어야합니다.
 - c) 파일메뉴에서 스냅인추가/제거를클릭합니다.
 - d) 추가를클릭합니다.
 - e) 독립실행형스냅인추가대화상자에서 인증서를선택합니다.
 - f) 추가를클릭합니다.
 - g) 인증서스냅인대화상자에서 내사용자계정을선택합니다. 서비스계정소유자로로그인한경우 서비스계정을선택합니다.
 - h) 컴퓨터선택대화상자에서 마침을클릭합니다.



7. 서버관리자 > IIS 로이동하고아이콘목록에서 서버인증서를선택합니다.

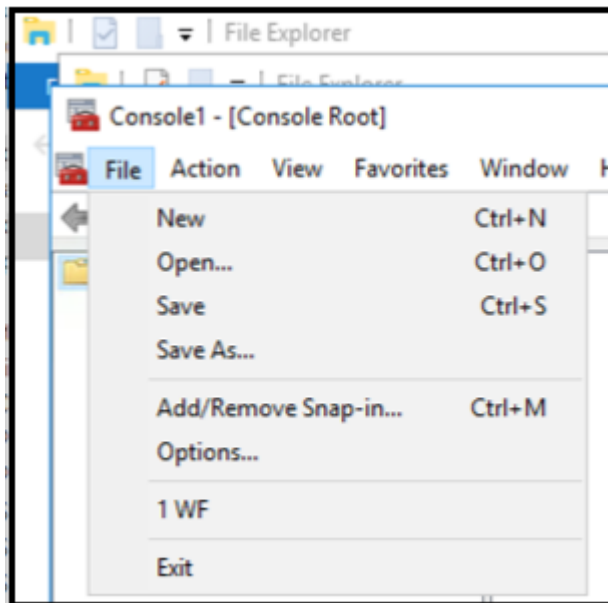


8. 작업메뉴에서 가져오기...를선택하여 SSL 인증서를가져옵니다.

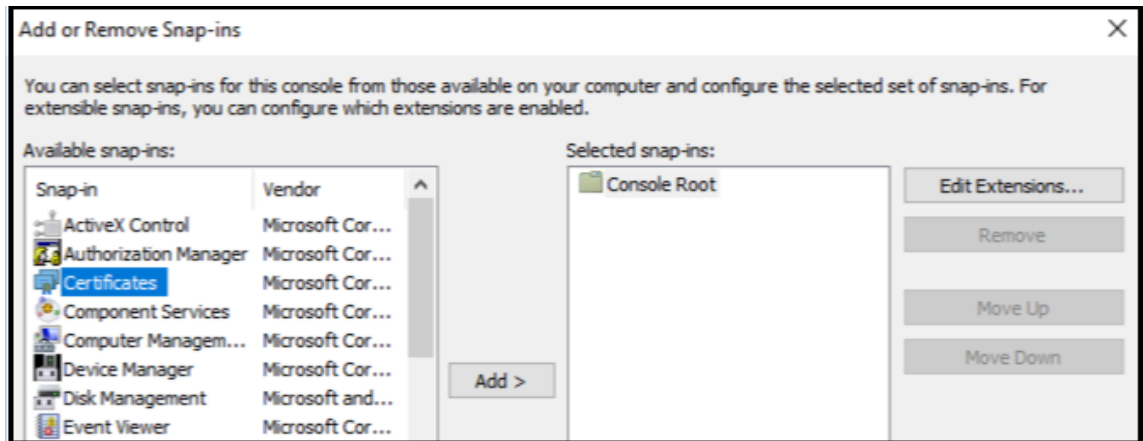


인증서지문검색및저장

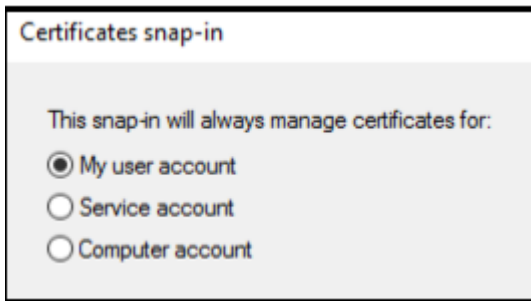
1. 파일탐색기검색표시줄에 **mmc** 를입력합니다.
2. 콘솔루트창에서 파일 > 스냅인추가/제거...를클릭합니다.



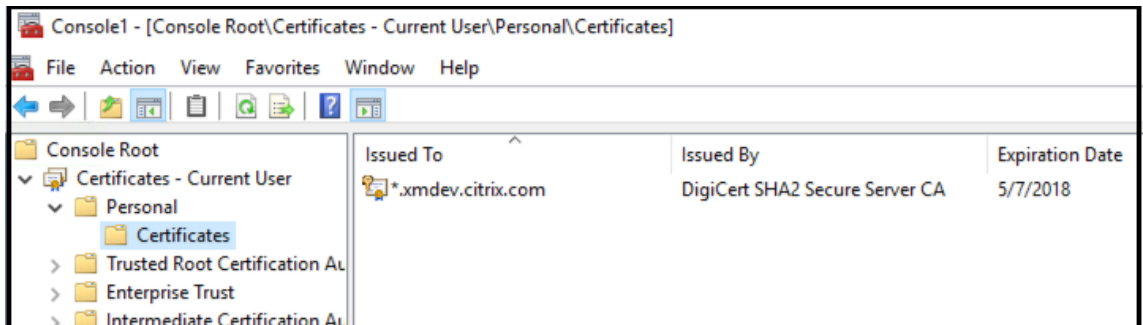
3. 사용가능한스냅인에서인증서를선택하고선택한스냅인에추가합니다.



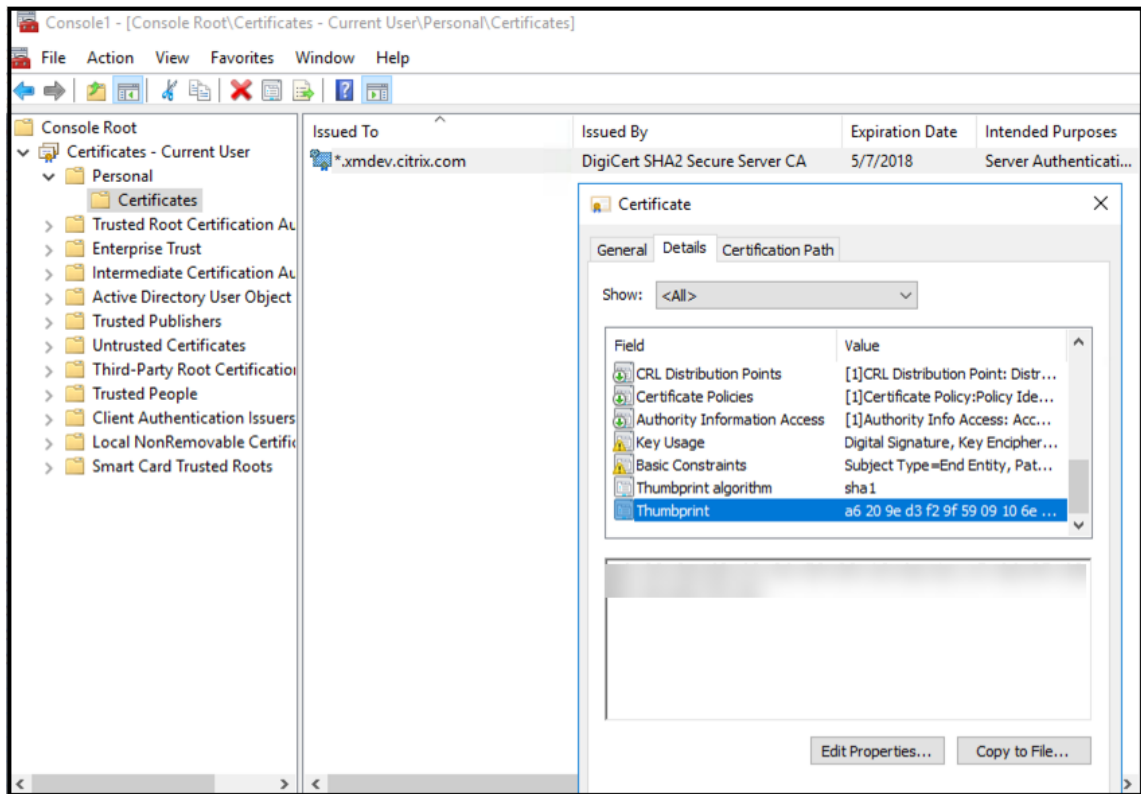
4. 내사용자계정을선택합니다.



5. 인증서를선택하고 확인을클릭합니다.



6. 인증서를두번클릭하고 세부정보탭을선택합니다. 아래로스크롤하여인증서지문을표시합니다.



7. 지문을파일에복사합니다. PowerShell 명령에서지문을사용하는경우공백을제거합니다.

서명및암호화인증서설치

Windows 서버에서다음 PowerShell 명령을실행하여서명및암호화인증서를설치합니다.

표시된것과같이 ReplaceWithThumbprint 자리표시자를바꾸고큰따옴표로묶습니다.

```

1 $key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
2   $_.Thumbprint -like "ReplaceWithThumbprint" }
3
4
5 $keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
6
7 $keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
   $keyname iccls $keypath /grant IIS_IUSRS':R

```

TPM 루트인증서추출및신뢰할수있는인증서패키지설치

Windows 서버에서다음명령을실행합니다.

```

1 mkdir .\TrustedTpm

```

```
2
3 expand -F:* .\TrustedTpm.cab .\TrustedTpm
4
5 cd .\TrustedTpm
6
7 .\setup.cmd
```

DHA 서비스구성

Windows 서버에서다음명령을실행하여 DHA 서비스를구성합니다.

ReplaceWithThumbprint 자리표시자를바꿉니다.

```
1 Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
   ReplaceWithThumbprint
2
3 -SigningCertificateThumbprint ReplaceWithThumbprint
4
5 -SslCertificateStoreName My -SslCertificateThumbprint
   ReplaceWithThumbprint
6
7 -SupportedAuthenticationSchema "AikCertificate"
```

Windows 서버에서다음명령을실행하여 DHA 서비스에대한인증서체인정책을설정합니다.

```
1 $policy = Get-DHASCertificateChainPolicy
2
3 $policy.RevocationMode = "NoCheck"
4
5 Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

다음프롬프트에다음과같이응답합니다.

```
1 Confirm
2
3 Are you sure you want to perform this action?
4
5 Performing the operation "Install-DeviceHealthAttestation" on
   target "WIN-N27D1FKCEBT".
6
7 [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?]
   Help (default is "Y"): A
8
9 Adding SSL binding to website 'Default Web Site'.
```

```
10
11   Add SSL binding?
12
13   [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15   Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17   Add application pool?
18
19   [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21   Adding web application 'DeviceHealthAttestation' to website '
22     Default Web Site'.
23
24   Add web application?
25
26   [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
27
28   Adding firewall rule 'Device Health Attestation Service' to allow
29     inbound connections on port(s) '443'.
30
31   Add firewall rule?
32
33   [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
34
35   Setting initial configuration for Device Health Attestation Service
36     .
37
38   Set initial configuration?
39
40   [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
41
42   Registering User Access Logging.
43
44   Register User Access Logging?
45
46   [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

구성확인

DHASActiveSigningCertificate 가활성상태인지확인하려면서버에서다음명령을실행합니다.

```
Get-DHASActiveSigningCertificate
```

인증서가활성상태인경우인증서유형 (서명) 과지문이표시됩니다.

DHSAActiveSigningCertificate 가활성상태인지확인하려면서버에서다음명령을실행합니다.

표시된것과같이 ReplaceWithThumbprint 자리표시자를바꾸고큰따옴표로묶습니다.

```
1 Set-DHSAActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
   -Force
2
3 Get-DHSAActiveEncryptionCertificate
```

인증서가활성상태인경우지문이나타납니다.

최종검사를수행하려면다음 URL 로이동합니다.

<https://<dha.myserver.com>/DeviceHealthAttestation/ValidateHealthCertificate/v1>

DHA 서비스가실행중인경우 “메서드를사용할수없음” 이나타납니다.



Secure Mail 푸시알림을통한 EWS 의인증서기반인증구성

May 21, 2019

작성자: Vijay Kumar Kunchakuri

Secure Mail 푸시알림이작동하려면인증서기반인증을사용하도록 Exchange Server 를구성해야합니다. 특히 Secure Hub 를인증서기반인증을사용하여 XenMobile 에등록한경우이요구사항을충족해야합니다.

인증서기반인증을사용하여 Exchange 메일서버에 Active Sync 및 EWS(Exchange 웹서비스) 가상디렉터리를구성해야합니다.

이러한구성을완료하지않으면 Secure Mail 푸시알림에대한구독이실패하고 Secure Mail 에서배지업데이트가수행되지않습니다.

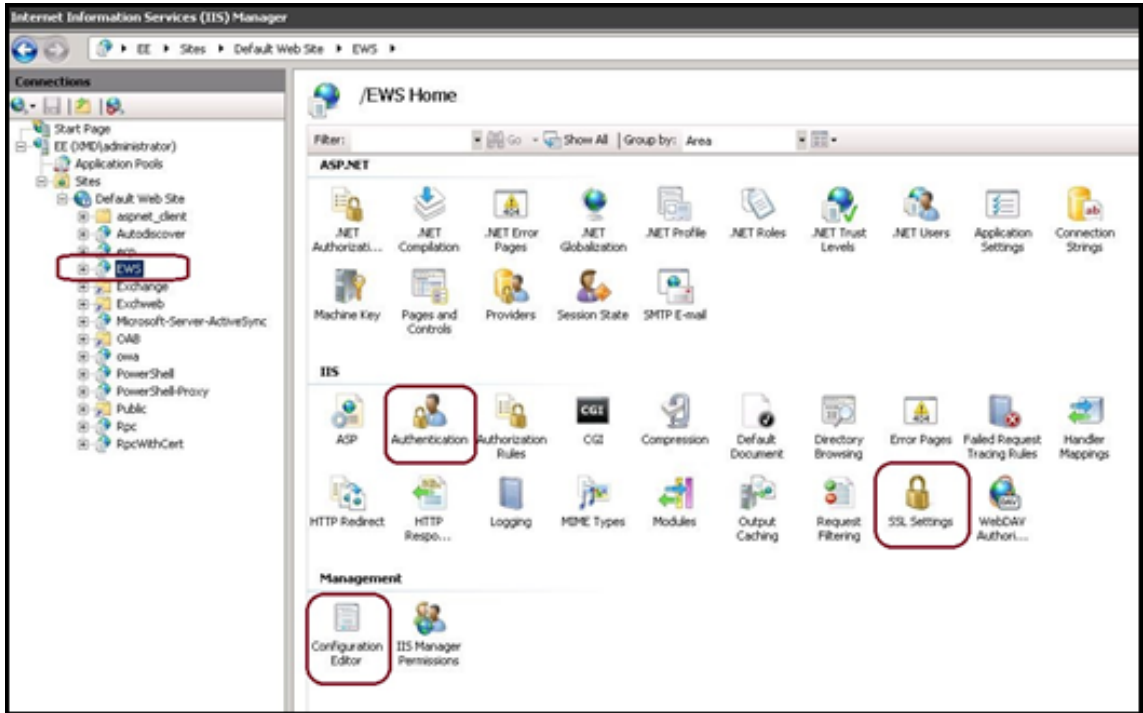
이문서에서는인증서기반인증을구성하는단계를설명합니다. 구성은 Exchange Server 의 EWS 가상디렉터리에대한것입니다.

구성을시작하려면다음을수행하십시오.

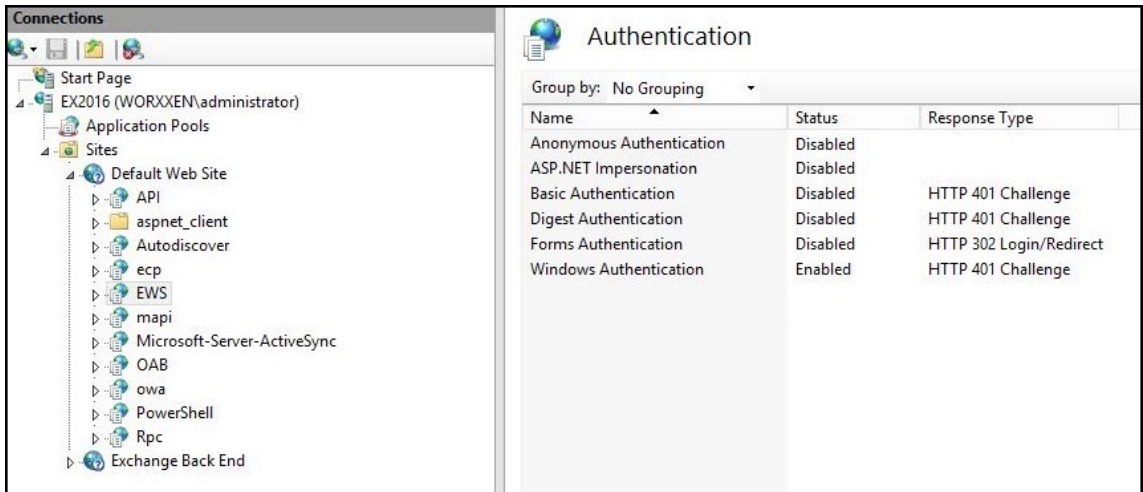
1. EWS 가상디렉터리가설치된하나이상의서버에로그온합니다.

2. IIS 관리자콘솔을열입니다.
3. 기본웹사이트에서 EWS 가상디렉터리를클릭합니다.

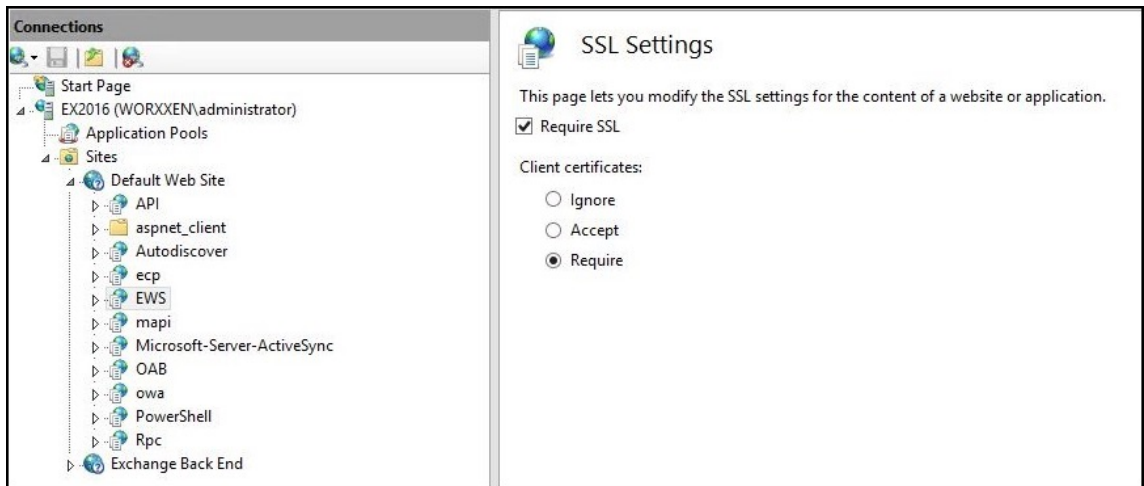
인증, SSL, 구성편집기스냅인은 IIS 관리자콘솔의오른쪽에표시됩니다.



4. EWS 에대한 인증설정이다음그림과같이구성되었는지확인합니다.



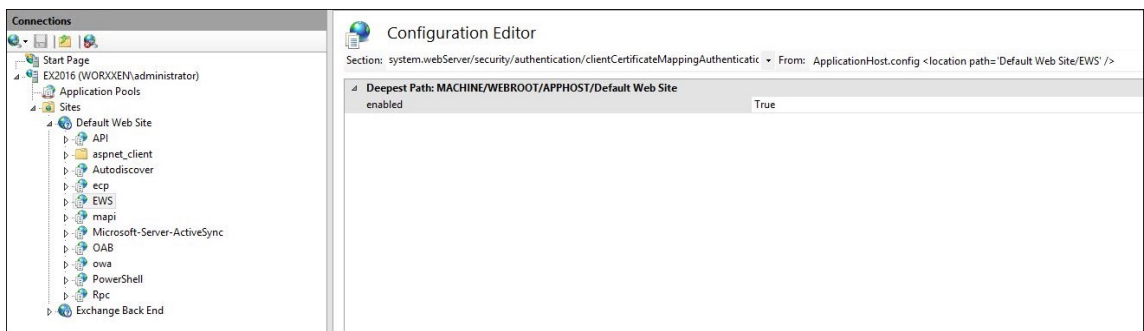
5. EWS 가상디렉터리에대한 **SSL** 설정을구성합니다.
 - a) **SSL** 필요확인란을선택합니다.
 - b) 클라이언트인증서에서 필요를클릭합니다. 다른 EWS 메일클라이언트가사용자이름과암호를자격증명으로사용하여 Exchange Server 에인증하고연결하는경우이옵션을 수락으로설정할수있습니다.



6. 구성편집기를 클릭하고 섹션드롭다운목록에서다음섹션으로이동합니다.

- **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. **enabled** 값을 **True** 로설정합니다.



8. 구성편집기를 클릭하고 섹션드롭다운목록에서다음섹션으로이동합니다.

- **system.webServer/serverRuntime**

9. **uploadReadAheadSize** 값을 **10485760**(10MB) 또는 **20971520**(20MB) 으로설정하거나조직에필요한값으로설정합니다.

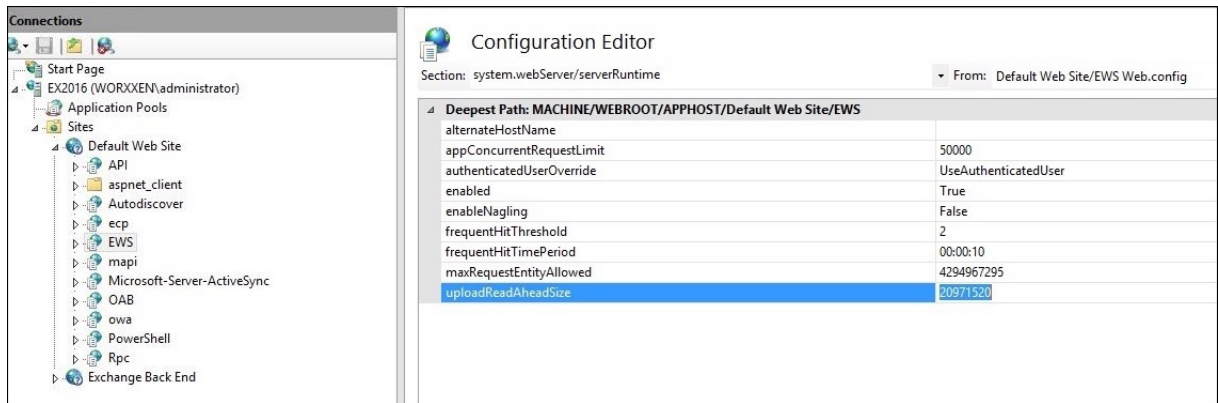
중요:

이값을올바르게설정하지않으면인증서기반인증이 EWS 푸시알림을구독하는동안실패하고오류코드 413 이표시됩니다.

이값을 **0** 으로설정하지마십시오.

자세한내용은다음타사리소스를참조하십시오.

- [Microsoft IIS Server Runtime\(Microsoft IIS 서버런타임\)](#)
- [Butsch Client Management Blog\(Butsch 클라이언트관리블로그\)](#)



iOS 푸시알림과 관련된 Secure Mail 문제를 해결하는 방법에 대한 자세한 내용은 [Citrix Support Knowledge Center](#) 문서를 참조하십시오.

관련정보

[iOS 용 Secure Mail 의푸시알림](#)

XenMobile MDM(모바일기기관리) 을 Cisco ISE(ID 서비스엔진) 와통합

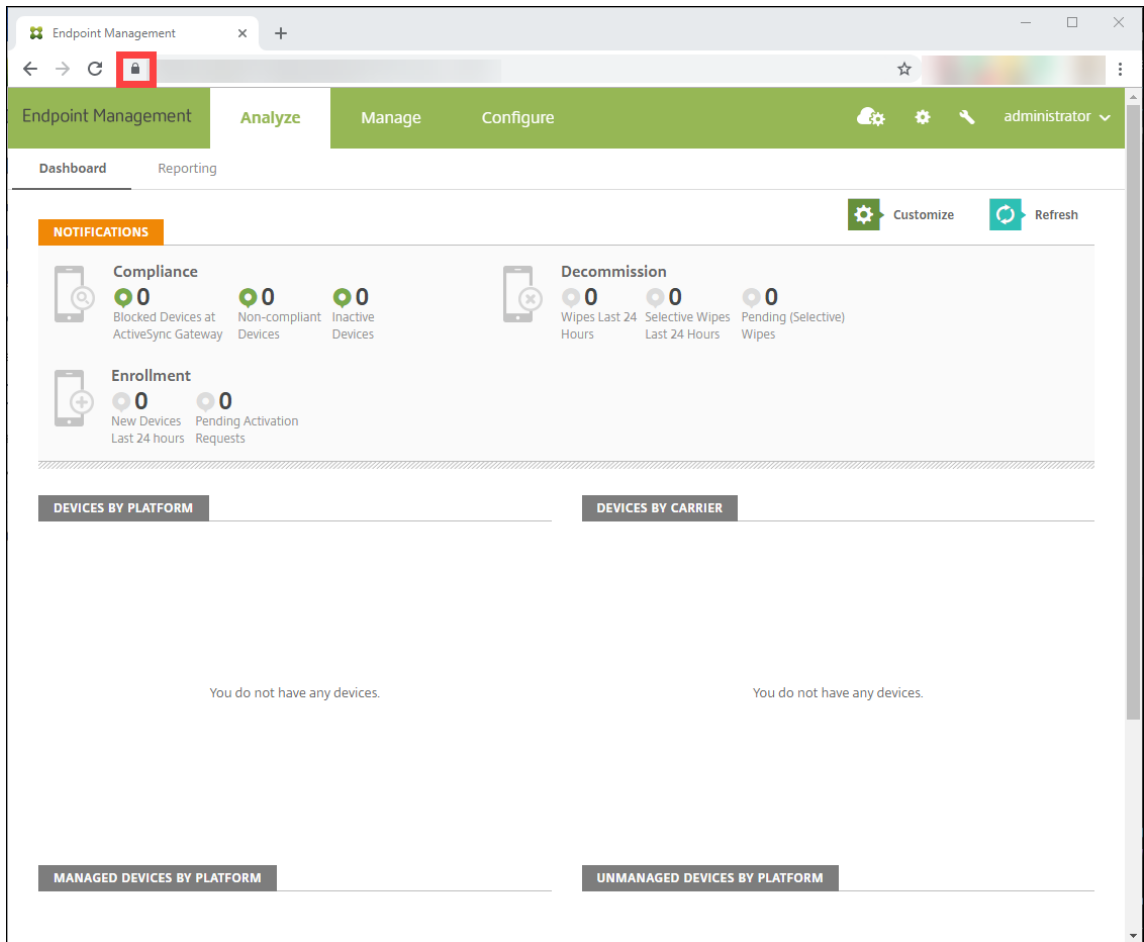
January 6, 2020

작성자: John Bartel III

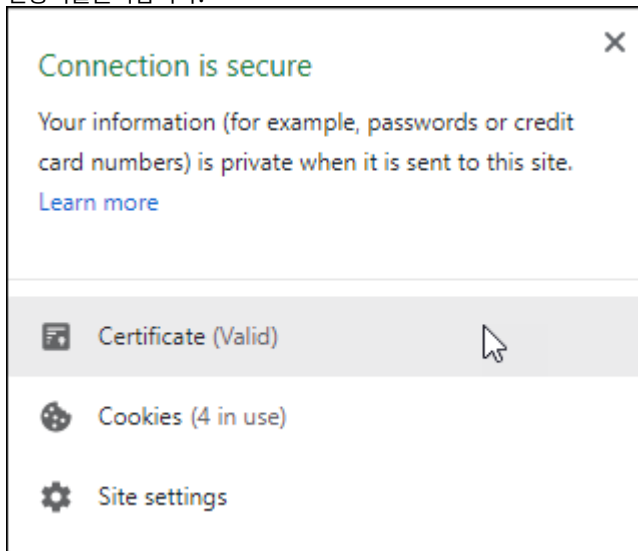
Cisco ISE 는작업공간에서모바일장치를배포, 보안, 모니터링, 통합및관리하는데사용됩니다. 모바일장치에다운로드된소프트웨어를통해응용프로그램및패치의배포를제어하고엔드포인트의데이터및구성을제어할수있습니다. XenMobile 을 Cisco ISE 와 통합하면 Cisco ISE 콘솔에서비호환장치및관리되지않는장치를관리할수있습니다. 또한 XenMobile 을사용하면회사서비스에 대한액세스를선택적으로허용, 거부또는격리할수있습니다.

XenMobile 과의통합을설정하려면 XenMobile Server 에서관리자 RBAC 역할이할당된로컬서비스계정을만듭니다. Cisco ISE 는이역할을사용하여 XenMobile API 에액세스할수있습니다. ISE 는 XenMobile 인증서를신뢰해야합니다. 이인증서를 다운로드하려면웹 브라우저를열고서버 URL 로이동하여로그인합니다.

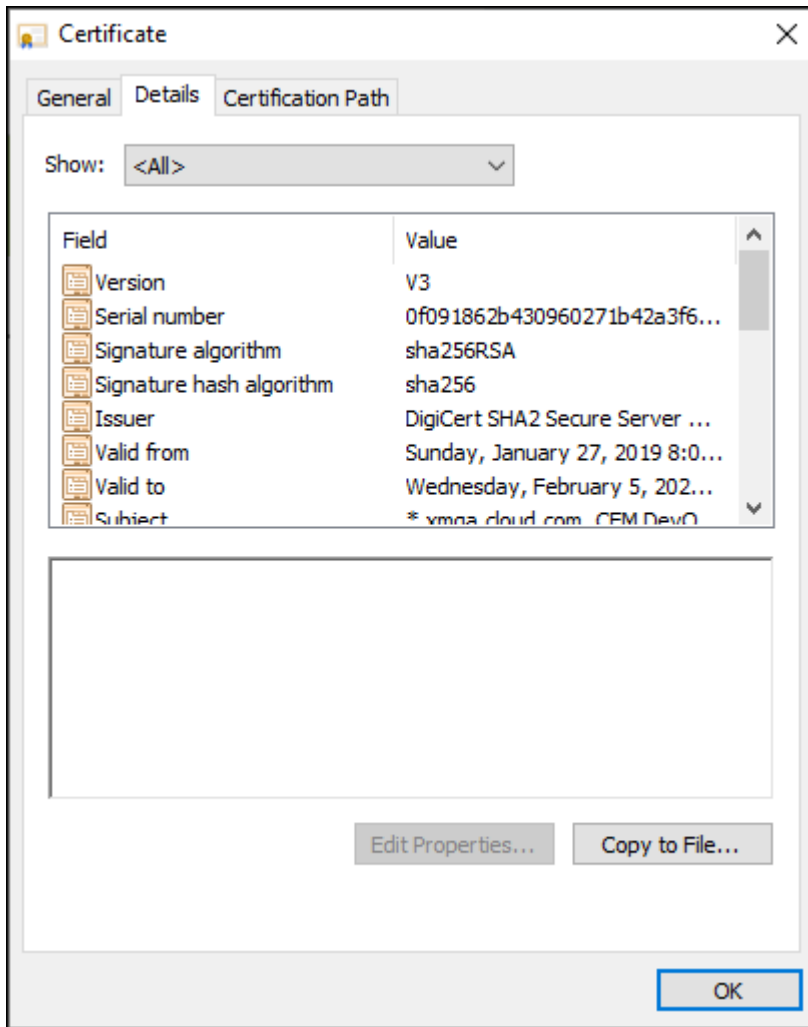
1. 로그인한후주소표시줄의 URL 옆에있는잠금표시를클릭합니다.



2. 인증서를 클릭합니다.



3. 세부정보탭을 선택하고 파일로복사를 클릭합니다.



4. 마법사에 따라 인증서를 로컬로 저장합니다.
5. Cisco ISE 콘솔에 로그인하고 이전에 다운로드한 XenMobile 인증서를 가져옵니다. 인증서를 Cisco ISE 의 신뢰할 수 있는 인증서 저장소로 가져옵니다. 이 가져오기는 Cisco ISE 가 XenMobile Server 와의 통신을 신뢰하는 데 필요합니다.
 - a) **Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > Trusted Certificates(신뢰할 수 있는 인증서)** 로 이동합니다. 가져오기를 클릭합니다.
 - b) 인증서 이름을 지정하고 **Trust for authentication within ISE(ISE 내의 인증 신뢰)** 및 **Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰)** 확인란을 선택합니다.
6. XenMobile 을 Cisco ISE 내부의 외부 MDM 으로 추가합니다.
 - a) **Administration(관리) > Network Resource(네트워크 리소스) > External MDM(외부 MDM)** 으로 이동합니다. **Add(추가)** 를 클릭하고 다음을 입력합니다.
 - **Server Host(서버 호스트):** XenMobile FQDN
 - **Port(포트):** 443
 - **Instance name(인스턴스 이름):** XenMobile Server 의 인스턴스 이름입니다. 대부분의 배포에서 인스턴스 이름은 기본적으로 "zdm" 입니다.
 - **User Name(사용자 이름):** 이 작업에 대해 만든 사용자 이름을 입력합니다. 사용자는 원래 관리자 RBAC 그룹

의로컬관리자계정이어야합니다.

- **Password(암호):** 방금추가한사용자의암호입니다.
- **Enable(사용)** 확인란을선택합니다.

7. 테스트에성공하면 **Submit(제출)** 을클릭합니다.

Cisco ISE 에대한자세한내용은 [Cisco 설명서](#)를참조하십시오.

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).