citrix

XenMobile Server 현재릴리스

Contents

롤링패치에대한릴리스정보

August 24, 2022

이섹션에는최신 XenMobile Server 롤링패치에대한릴리스정보가포함되어있습니다. 아래링크를클릭하여해결된문제및알려진문제, 기능변경사항, 필요한작업을확인하십시오.

최신롤링패치에는동일한릴리스에대한이전롤링패치의모든수정사항이포함되어있습니다.

현재릴리스의패치에대한릴리스정보	게시날짜	지원문서
10.14 롤링패치 7	Aug 18, 2022	CTX463691
10.14 롤링패치 6	May 23, 2022	CTX459871
10.14 롤링패치 5	Mar 30, 2022	CTX399411
10.14 롤링패치 4	Jan 26, 2022	CTX339069
10.14 롤링패치 3	Dec 22, 2021	CTX335897
10.14 롤링패치 2	Dec 15, 2021	CTX335763
10.14 롤링패치 1	Nov 19, 2021	CTX335342

이전릴리스의패치에대한릴리스정보	게시날짜	지원문서
10.13 롤링패치 9	Jun 14, 2022	CTX460128
10.13 롤링패치 8	Apr 12, 2022	CTX447596
10.13 롤링패치 7	Mar 1, 2022	CTX341602
10.13 롤링패치 6	Dec 21, 2021	CTX335875
10.13 롤링패치 5	Dec 15, 2021	CTX335753
10.13 롤링패치 4	Aug 11, 2021	CTX324159
10.13 롤링패치 3	May 13, 2021	CTX315034
10.13 롤링패치 2	Feb 25, 2021	CTX296934
10.13 롤링패치 1	Jan 8, 2021	CTX289495
10.12 롤링패치 11	Dec 21, 2021	CTX335861
10.12 롤링패치 10	Dec 16, 2021	CTX335785
10.12 롤링패치 9	Oct 8, 2021	CTX331040
10.12 롤링패치 8	Jun 2, 2021	CTX316910

이전릴리스의패치에대한릴리스정보	게시날짜	지원문서
10.12 롤링패치 7	Mar 29, 2021	CTX309096
10.12 롤링패치 6	Jan 26, 2021	CTX292680
10.11 롤링패치 7	Nov 18, 2020	CTX286435
10.10 롤링패치 6	Jul 22, 2020	CTX279101

XenMobile Server 10.14 롤링패치 7 릴리스에대한릴리스정보

August 24, 2022

이릴리스노트에서는 XenMobile Server 10.14 롤링패치 7 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

- **OS** 업데이트
  - **iOS 16** 지원**.** XenMobile Server 및 Citrix 모바일생산성앱은 iOS 16 과호환되지만현재는새로운 iOS 16 기능을지원하지않습니다.
  - **Android 13** 지원. 이제 XenMobile Server 에서 Android 13 에대한 Android Enterprise 장치업데이트를지원합니다. 보안및개인정보보호혜택에대한요약은 Android 문서를참조하십시오.
- 사용되지않는기능**.** 이제다음기능이지원되지않습니다.
  - RBAC 역할 - 공유및 COSU 장치등록자 [CXM-104826]
  - Android - Sony 및 HTC [CXM-104827]
  - 높은보안등록모드 [CXM-104828]
  - 파생된자격증명 [CXM-104829]
  - SEAMS [CXM-104833]
  - Windows Phone 장치 [CXM-104834], [CXM-104835]
  - 일반, DigiCert 관리형및 Entrust 어댑터 PKI 엔터티. [CXM-104990]

  자세한내용은 지원중단을참조하십시오.
- 모바일서비스공급자 **(MSP)** 인터페이스에대한지원이중단되었습니다**.** 콘솔에서 MSP 인터페이스를제거하는새로운서버속성 (`deprecate.mobile.service.provider`) 을추가하고 MSP 에대한지원은중단했으며, 이속성은기본적으로 **True** 로설정되어있습니다. 자세한내용은 서버속성을참조하십시오. [CXM-104836]
- **Windows 10** 장치에대한 ***Wi-Fi*** 감지핫스팟자동연결제한허용지원을제거합니다**.** 자세한내용은 Windows 데스크톱/태블릿설정을참조하십시오. [CXM-104839]

- **Nexmo SMS** 게이트웨이에대한지원이중단되었습니다. 새로운서버속성 (`deprecate.carrier.sms.gateway`) 을추가하고 Nexmo SMS 에대한지원은중단했으며, 이속성은기본적으로 **True** 로설정되어있습니다. Nexmo SMS 는자가지원포털에서도더이상사용되지않습니다. 자세한내용은 알림을참조하십시오. [CXM-104840]
- **Google** 의 **API** 지원중단. Google 은 XenMobile Server 에서앱카테고리및라이선스에사용되는여러 API 를더이상지원하지않습니다. 다음과같은변경사항이적용됩니다.
  - 이제승인하지않고추가할앱을선택합니다. 관리되는앱스토어앱을참조하십시오.
  - 이제앱을카테고리가아닌컬렉션으로구성할수있습니다. 앱구성을참조하십시오.
  - 더이상사용자로부터앱라이선스를분리할수없습니다. 앱추가를참조하십시오. [CXM-105835]
- **Android Enterprise** 관리형앱을자동으로업데이트하도록우선순위를구성합니다. Android Enterprise 관리형앱을낮은우선순위로자동업데이트할지아니면높은우선순위로업데이트할지를지정합니다. 자동업데이트를연기할수도있습니다. 자세한내용은 관리되는앱자동업데이트장치정책을참조하십시오. [CXM-105837]

XenMobile Server 10.14.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

- Google Play 에서일부공용앱을사용할수없는경우 Android 를실행하는일부기기에서는 Secure Hub 에액세스할수없습니다. [CXM-105492]
- SSL 인증서갱신후특정 macOS 장치에서는설치된프로필및인증서가자동으로제거됩니다. [CXM-105759]
- XenMobile Server 콘솔에서는이름에 **/** 기호가있는제한장치정책을편집할수없습니다. [CXM-105828]
- 출시된 DEP 장치는 XenMobile Server 콘솔에계속표시됩니다. [CXM-105905]
- Secure Hub 스토어에액세스할수없습니다. 다음오류가발생합니다. 로그인이만료되었습니다. 계속하려면다시로그인하십시오. [CXM-106054]

XenMobile Server 10.14 롤링패치 6 릴리스에대한릴리스정보

May 26, 2022

이릴리스노트에서는 XenMobile Server 10.14 롤링패치 6 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

새제한정책이추가되었습니다. 작업프로필에서복사및붙여넣기허용및 개인프로필에서데이터공유허용을제한정책에추가했습니다. 개인프로필에서작업프로필로복사, 붙여넣기및가져오기를제한하려면이러한정책을 꺼짐으로설정합니다. 자세한내용은 제한장치정책을참조하십시오. [CXM-104599]

XenMobile Server 10.14.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

- XenMobile Server 에서일부 VPP 앱의올바른버전이자동으로업데이트되지않습니다. [CXM-104329]
- XenMobile Server 버전 10.14 에서는특정 Active Directory 사용자를삭제할수없습니다. [CXM-105176]
- iOS 15 를실행하는장치를새로등록할때연결유형이 **AlwaysOn IKEv2** 이중구성으로설정된경우 VPN 정책배포가실패합니다. [CXM-105181]

XenMobile Server 10.14 롤링패치 **5** 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.14 롤링패치 5 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

- **Google Analytics** 를 활 성 화 합 니 다. XenMobile Server 에 서 Google Analytics 를 활 성 화 하 려 면 **xms.ga.enabled** 서버속성의값을 **True** 로설정합니다. 기본값은 **True** 입니다. [CXM-104006]
- **Secure Hub APN** 인증서갱신**.** XenMobile Server 10.14 에대한 Secure Hub Apple 푸시알림서비스 (APN) 인증서가 2022 년 5 월 7 일에만료됩니다. 이업데이트는 Secure Hub APN 인증서를갱신하며, 이인증서는 2023 년 4 월 8 일에만료됩니다. [CXM-104194]

XenMobile Server 10.14.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

- 장치의 CA 갱신이후 XenMobile Server 에서장치인증서발급자 CA 가업데이트되지않습니다. [CXM-104234]
- 일부장치의 SQL 데이터베이스에는두개의인증서항목이있어오류가발생합니다. [CXM-104296]
- XenMobile Server 버전 10.14 에서는프로필장치프로비저닝정책을편집할수없습니다. [CXM-104461]
- XenMobile Server 에서 ShareFile Enterprise 를커넥터로변경할때배달그룹아래에서 GUI 가업데이트되지않습니다. [CXM-104470]

XenMobile Server 10.14 롤링패치 **4** 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.14 롤링패치 4 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

WSDL 서비스를사용하도록설정합니다. XenMobile 서버에서 WSDL 서비스를사용하도록설정하려면서버속성값 `wsdl.service.enabled`을 **True** 로설정합니다. ActiveSync 게이트웨이커넥터를사용할때필요합니다. 기본값은 **False** 입니다. [CXM-103017]

XenMobile Server 10.14.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

- 일부 Android Enterprise 장치에서는배달그룹및할당된정책또는앱이간헐적으로적용되지않습니다. [CXM-102044]
- XenMobile Server 버전 10.13 에서는 StorageZone 커넥터만사용하여 StorageZone 컨트롤러를연결하고구성할수없습니다. [CXM-102661]
- MDM 전용모드로등록된 iOS 장치에서는 Secure Hub 가 App Store 에서연브라우저를통해앱을추가할수없습니다. 다음오류가발생합니다. 로그인이만료되었습니다. 계속하려면다시로그인하십시오. [CXM-102664]
- XenMobile Server 버전 10.13 RP1 이상에서는 SNMP 모니터링의 XenMobile 노드간연결트랩이작동하지않습니다. [CXM-102753]
- XenMobile Server 에서잘못된시간이 W-SU 시간대에표시됩니다. [CXM-102856]

XenMobile Server 10.14 롤링패치 3 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.14 롤링패치 3 의향상된기능및해결된문제와알려진문제에대해설명합니다.

이릴리스에는버그수정이포함되어있습니다.

XenMobile Server 10.14.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

XenMobile Server 10.14 롤링패치 2 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.14 롤링패치 2 의향상된기능및해결된문제와알려진문제에대해설명합니다.

XenMobile Server 10.14.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

해결된문제

XenMobile Server 에서는사용량이많은시간에서버노드의높은 CPU 사용률을확인할수있습니다. [CXM-102568]

XenMobile Server 10.14 롤링패치 1 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.14 롤링패치 1 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

- **Windows 10** 장치를지원합니다**.** 이제 XenMobile 을사용하여 Windows 11 장치를관리할수있습니다. 자세한내용은 운영체제지원목록을참조하십시오. [CXM-99999]
- **macOS** 의연결모드및네트워크우선순위를구성합니다**.** Wi-Fi 장치정책에서 macOS 장치에대한 연결모드설정을활성화하여사용자가네트워크에참여하는방법을선택합니다. 장치는로그인창에입력한시스템자격증명또는자격증명을통해사용자를인증할수있습니다. 네트워크가여러개인경우 우선순위필드에숫자를입력하여네트워크연결의우선순위를설정합니다. 장치는번호가가장낮은네트워크를선택합니다. 자세한내용은 Wi-Fi 장치정책의 macOS 설정을참조하십시오. [CXM-100879]
- Google 의 Android Enterprise 장치에서그룹라이선스에대한지원이중단되므로 XenMobile Server 에서그룹라이선스를 Google 에동기화할수없습니다. 자세한내용은 이문서를참조하십시오. [CXM-101209]

알려진문제

등록된장치중 macOS 11 이전버전에서 macOS 12 로업그레이드된장치또는 macOS 12 에새로등록된장치는장치의 시스템환경설정 **>** 프로필에 “확인되지않음” 으로표시될수있습니다. 자세한내용과해결방법은이 지원문서를참조하십시오.[CXM-101843]

수정된문제

- iOS 15 또는 macOS 12 장치를등록한후 MDM 구성프로필에 확인되지않음으로표시됩니다. [CXM-99379]
- XenMobile Server 콘솔에서앱의설정을수정하여모든플랫폼의선택을취소하고저장하면해당앱이 구성 **>** 앱에나열되지않습니다. [CXM-99851]
- Android Enterprise 플랫폼에서 Citrix Launcher 를종료할수없습니다. 다음오류가발생합니다. 암호가잘못되었습니다. [CXM-100975]
- XenMobile Server 버전 10.14 에서는 iOS 및 macOS 프로필가져오기정책을편집할수없습니다. [CXM-102393]

XenMobile Server 10.13 롤링패치 9 릴리스에대한릴리스정보

June 17, 2022

이릴리스노트에서는 XenMobile Server 10.13 롤링패치 9 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

- 새제한정책이추가되었습니다**.** 작업프로필에서복사및붙여넣기허용및 개인프로필에서데이터공유허용을제한정책에추가했습니다. 개인프로필에서작업프로필로복사, 붙여넣기및가져오기를제한하려면이러한정책을 꺼짐으로설정합니다. 자세한내용은 제한장치정책을참조하십시오. [CXM-104600]

XenMobile Server 10.13.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

- XenMobile Server 에서 ShareFile Enterprise 를커넥터로변경할때배달그룹아래에서 GUI 가업데이트되지않습니다. [CXM-104476]
- 장치의 CA 갱신이후 XenMobile Server 에서장치인증서발급자 CA 가업데이트되지않습니다. [CXM-104545]
- XenMobile Server 버전 10.13 에서는특정 Active Directory 사용자를삭제할수없습니다. [CXM-105177]
- iOS 15 를실행하는장치를새로등록할때연결유형이 **AlwaysOn IKEv2** 이중구성으로설정된경우 VPN 정책배포가실패합니다. [CXM-105195]

XenMobile Server 10.13 롤링패치 8 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.13 롤링패치 8 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

- 로컬사용자가약한암호를사용하지못하도록암호유효성검사를활성화합니다. `enable.password.strength.validation`을 **`true`**로설정하면약한암호를사용하는로컬사용자를추가할수없습니다. **`false`**로설정하면약한암호로로컬사용자를만들수있습니다. 기본값은 **`true`**입니다. [CXM-104085]
- **Secure Hub APN** 인증서갱신**.** XenMobile Server 10.13 에대한 Secure Hub Apple 푸시알림서비스 (APN) 인증서가 2022 년 5 월 7 일에만료됩니다. 이업데이트는 Secure Hub APN 인증서를갱신하며, 이인증서는 2023 년 4 월 8 일에만료됩니다. [CXM-104195]

XenMobile Server 10.13.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

- 일부장치의 SQL 데이터베이스에는두개의인증서항목이있어오류가발생합니다. [CXM-104297]
- XenMobile Server 에서일부 VPP 앱의올바른버전이자동으로업데이트되지않습니다. [CXM-104330]
- XenMobile Server 버전 10.13 에서는프로필장치프로비저닝정책을편집할수없습니다. [CXM-104464]

XenMobile Server 10.13 롤링패치 7 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.13 롤링패치 7 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

- **WSDL** 서비스를사용하도록설정합니다**.** XenMobile 서버에서 WSDL 서비스를사용하도록설정하려면서버속성값 `wsdl.service.enabled`을 **True** 로설정합니다. ActiveSync 게이트웨이커넥터를사용할때필요합니다. 기본값은 **False** 입니다. [CXM-103131]
- **Google Analytics** 를 활 성 화 합 니 다. XenMobile Server 에 서 Google Analytics 를 활 성 화 하 려 면 **xms.ga.enabled** 서버속성의값을 **True** 로설정합니다. 기본값은 **True** 입니다. [CXM-103823]

XenMobile Server 10.13.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

XenMobile Server 에서잘못된시간이 W-SU 시간대에표시됩니다. [CXM-102922]

XenMobile Server 10.13 롤링패치 6 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.13 롤링패치 6 의향상된기능및해결된문제와알려진문제에대해설명합니다.

이릴리스에는버그수정이포함되어있습니다.

XenMobile Server 10.13.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

XenMobile Server 10.13 롤링패치 4 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.13 롤링패치 4 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

Android 12 를지원합니다. 이제 XenMobile Server 에서 Android 12 에대한 Android Enterprise 장치업데이트를지원합니다. 보안및개인정보보호혜택에대한요약은 Android 문서를참조하십시오.

XenMobile Server 10.13.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

수정된문제

- APN 용 HTTP/2 기반 API 로전환하면 `ios.mdm.apns.connectionPoolSize` 서버속성이숨겨집니다. [CXM-95479]
- XenMobile Server 버전 10.12 에서는특정앱의 VPP 속성을수정할수없습니다. [CXM-96854]
- 필요한웹앱이 MDM 전용장치에자동으로설치되지않습니다. [CXM-97477]
- XenMobile Server 버전 10.13 에서는 **CLI** 아래에서프록시서버를구성할때 iOS 장치에서실행중인 Secure Hub 로알림을보낼수없습니다. [CXM-97807]
- XenMobile Server 버전 10.13 에서 장치세부정보에액세스하는동안오류가발생합니다. 이오류는장치속성에 **”“**의값이있는경우발생합니다. [CXM-97951]

XenMobile Server 10.13 롤링패치 **3** 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.13 롤링패치 3 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

Secure Hub APN 인증서갱신**.** XenMobile Server 10.13 에대한 Secure Hub APNs(Apple 푸시알림서비스) 인증서가 2021 년 6 월 17 일에만료됩니다. 이업데이트는 Secure Hub APN 인증서를갱신하며, 이인증서는 2022 년 5 월 7 일에만료됩니다. [CXM-94070]

APN 알림에대한대체포트**.** 이제 XenMobile Server 포트 443 의대안으로포트 2197 을사용할수있도록지원합니다. 포트 2197 을사용하여 `api.push.apple.com`에 APN 알림을보내고이로부터피드백을받을수있습니다. 포트는 HTTP/2 기반 APN 공급자 API 를사용합니다. 서버속성 `apns.http2.alternate.port.enabled`의기본값은 **`false`**입니다. 대체포트를사용하려면서버속성을업데이트한다음서버를다시시작하십시오. [CXM-93911]

수정된문제

macOS 10.14 이상을실행하는장치를등록한직후 XenMobile Server 콘솔에장치속성이항상채워지는것은아닙니다. 장치를다시시작하고나면장치속성이예상대로나타납니다. [CXM-94150]

제한정책에서동일한앱에대해 시스템앱활성화및 애플리케이션비활성화설정을모두활성화하면앱이작업프로필에나타납니다. [CXM-94097]

XenMobile Server 콘솔에 SNMP 사용자를추가하면 **SNMP** 모니터링사용자목록에사용자가나타나지않거나 SNMP 에이전트가비활성화됩니다. [CXM-93199]

XenMobile Server 에서 NetScaler Gateway 연결확인에결과가표시되지않습니다. [CXM-93134]

XenMobile Server 콘솔에올바른루트인증서만료날짜가표시되지않습니다. [CXM-93133]

XenMobile Server 10.12 롤링패치 11 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.12 롤링패치 11 의향상된기능및해결된문제와알려진문제에대해설명합니다.

이릴리스에는버그수정이포함되어있습니다.

XenMobile Server 10.12.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

XenMobile Server 10.12 롤링패치 10 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.12 롤링패치 10 의향상된기능및해결된문제와알려진문제에대해설명합니다.

이릴리스에는버그수정이포함되어있습니다.

XenMobile Server 10.12.0 의이전롤링패치에대한자세한내용은 롤링패치에대한릴리스정보를참조하십시오.

XenMobile Server 10.12 롤링패치 9 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.12 롤링패치 9 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

Android 12 를지원합니다. XenMobile Server 는 Android Enterprise 장치에서 Android 12 를지원합니다. 보안및개인정보보호혜택에대한요약은 Android에대한 Google 설명서를참조하십시오. [CXM-97765]

Windows 10 장치를지원합니다**.** 이제 XenMobile Server 를사용하여 Windows 11 장치를관리할수있습니다. 자세한내용은 운영체제지원목록을참조하십시오. [CXM-99995]

수정된문제

앱자동업데이트설정이비활성화되면기기에설치된 Apple 볼륨구매앱이최신버전으로자동업데이트됩니다. [CXM-95985]

XenMobile Server 버전 10.12 에서 장치세부정보에액세스하는동안오류가발생합니다. 이오류는장치속성에 ”“의값이있는경우발생합니다. [CXM-97953]

XenMobile Server 콘솔에서앱의설정을수정하여모든플랫폼의선택을취소하고저장하면해당앱이 구성 **>** 앱에나열되지않습니다. [CXM-99708]

XenMobile Server 10.12 롤링패치 **8** 릴리스에대한릴리스정보

May 6, 2022

이릴리스노트에서는 XenMobile Server 10.12 롤링패치 8 의향상된기능및해결된문제와알려진문제에대해설명합니다.

새로운항목

Secure Hub APN 인증서갱신**.** XenMobile Server 10.12 에대한 Secure Hub APNs(Apple 푸시알림서비스) 인증서가 2021 년 6 월 17 일에만료됩니다. 이업데이트는 Secure Hub APN 인증서를갱신하며, 이인증서는 2022 년 5 월 7 일에만료됩니다. [CXM-94513]

수정된문제

- macOS 10.14 이상을실행하는장치를등록한직후 XenMobile Server 콘솔에장치속성이항상채워지는것은아닙니다. 장치를다시시작하고나면장치속성이예상대로나타납니다. [CXM-94221]
- XenMobile Server 10.12 에서 ShareFile 가간헐적으로연결을설정하는데실패합니다. [CXM-95419]

XenMobile Server 10.14 의새로운기능

February 2, 2022

Citrix ADC 에서지원중단되는클래식정책에대한지속적인지원

Citrix 는최근 Citrix ADC 12.0 빌드 56.20 부터클래식정책기반기능의일부를지원중단한다고발표했습니다. Citrix ADC 지원중단고지는 Citrix Gateway 와의기존 XenMobile Server 통합에는영향을주지않습니다. XenMobile Server 는클래식정책을계속지원하므로별도의작업이필요하지않습니다.

XenMobile 마이그레이션서비스

XenMobile Server 를온-프레미스에서사용하는경우무료 XenMobile 마이그레이션서비스를사용하여 Endpoint Management 를시작할수있습니다. XenMobile Server 에서 Citrix Endpoint Management 로마이그레이션할때장치를재등록할필요는없습니다.

마이그레이션을시작하려면해당지역의 Citrix 영업사원또는 Citrix 파트너에게문의하십시오. XenMobile 마이그레이션서비스를참조하십시오.

사용중단발표

단계적으로중단되는 Citrix XenMobile 기능에대한고급알림은 사용중단을참조하십시오.

엔드포인트를 **iOS 14.5** 로업그레이드하기전에

Citrix 는엔드포인트를 iOS 14.5 로업그레이드하기전에다음작업을수행하여앱충돌을완화할것을권장합니다.

- Citrix Secure Mail 및 Secure Web 을 21.2.X 이상으로업그레이드합니다. MDX 또는엔터프라이즈앱업그레이드를참조하십시오.
- MDX Toolkit 을사용하는경우 MDX Toolkit 21.3.X 이상으로모든타사 iOS 애플리케이션을래핑합니다. 최신버전은 MDX Toolkit 다운로드페이지를확인하십시오.

온-프레미스 **Citrix ADC** 를업그레이드하기전에

온-프레미스 Citrix ADC 를특정버전으로업그레이드하면 Single Sign-on 오류가발생할수있습니다. 회사직원로그인옵션이있는브라우저에서 Citrix Files 또는 ShareFile 도메인 URL 에 Single Sign-on 으로인해오류가발생합니다. 사용자가로그인할수없습니다.

이문제의해결방법: Citrix Gateway 의 ADC CLI 에서다음명령을아직실행하지않은경우명령을실행하여전역 SSO 를사용하도록설정합니다.

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

자세한내용은다음을참조하십시오.

- Citrix ADC 릴리스 (Feature Phase) 13.0 빌드 67.39/67.43
- 영향을받는 SSO 구성

문제해결을완료한후사용자는회사직원로그인옵션이제공되는브라우저에서 SSO 를사용하여 Citrix Files 또는 ShareFile 도메인 URL 에인증할수있습니다. [CXM-88400]

XenMobile 10.14 로업그레이드하기전에 (온-프레미스)

일부시스템요구사항이변경되었습니다. 자세한내용은 시스템요구사항및호환성과 XenMobile 호환성을참조하십시오.

1. 업그레이드할 XenMobile Server 를실행하는가상컴퓨터의 RAM 이 8GB 미만인경우 8GB 이상으로 RAM 을늘리는것이좋습니다.
2. 최신버전의 XenMobile Server 10.14 로업데이트하기전에 Citrix License Server 를 11.16 이상으로업데이트하십시오.

   최신버전의 XenMobile 에는 Citrix License Server 11.16(최소버전) 이필요합니다.

   > 참고:
   >
   > XenMobile 10.14 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2021 년 9 월 15 일입니다. Citrix 라이센스의 Customer Success Services 날짜는이날짜보다이후여야합니다.
   >
   > 날짜는라이센스서버의라이센스옆에서볼수있습니다. 최신버전의 XenMobile 을이전버전의라이센스서버환경에연결하면연결확인이실패하고라이센스서버를구성할수없게됩니다.

   라이센스의날짜를갱신하려면 Citrix 포털에서최신라이센스파일을다운로드하고라이센스서버에파일을업로드하십시오. Customer Success Services를참조하십시오.
3. 클러스터된환경의경우: iOS 11 이상을실행하는장치에 iOS 정책및앱을배포하려면다음과같은요구사항이충족되어야합니다. Citrix Gateway 에 SSL 지속성이구성되어있으면모든 XenMobile Server 노드에서포트 80 을열어야합니다.
4. XenMobile 업데이트를설치하기전에 VM 의기능을사용하여시스템스냅샷을생성합니다. 또한시스템구성데이터베이스를백업합니다. 업그레이드도중문제가발생하는경우전체백업을사용하여복구할수있습니다.

업그레이드하려면

이번릴리스에서 XenMobile 은 VMware ESXi 7.0 을지원합니다. ESXi 7.0 를설치하거나업그레이드하기전에 10.14 로업그레이드해야합니다.

XenMobile 10.13.x 또는 10.12.x 에서직접 XenMobile 10.14 로업그레이드할수있습니다. 업그레이드를수행하려면사용가능한최신이진파일을다운로드합니다. https://www.citrix.com/downloads로이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server >** 제품소프트웨어 **> XenMobile Server 10** 으로이동합니다. 해당하는하이퍼바이저에대한 XenMobile Server 소프트웨어타일에서 파일다운로드를클릭합니다.

업그레이드를업로드하려면 XenMobile 콘솔의 릴리스관리페이지를사용합니다. 릴리스관리페이지를사용하여업그레이드하려면을참조하십시오.

업그레이드후

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

- 이인증서유효성검사오류는 XenMobile Server 에서호스트이름유효성검사를비활성화해야함을나타냅니다.
- 기본적으로호스트이름유효성검사는 Microsoft PKI 서버를제외한발신연결에대해활성화됩니다.
- 호스트이름유효성검사로인해배포가중단되는경우서버속성 `disable.hostname.verification`을 **`true`**로 변경하십시오. 이속성의기본값은 **`false`**입니다.

플랫폼지원업데이트

- **iOS 15:** XenMobile Server 및 Citrix 모바일생산성앱은 iOS 15 와호환되지만현재는새로운 iOS 15 기능을지원하지않습니다.
- **Android 12:** XenMobile Server 는 Android 12 를지원합니다. Google Device Administration API 의지원중단이 Android 10 이상을실행하는장치에미치는영향에대해서는 장치관리에서 Android Enterprise 로마이그레이션을참조하십시오. 이 Citrix 블로그도참조하십시오.

장치정책

- Google 설정과더욱가깝게일치하고구성을단순화하도록모든 Android Enterprise 등록모드에두가지설정을추가했습니다.
  - **Bluetooth** 공유허용**:** 선택을취소할경우사용자가장치에서나가는 Bluetooth 공유를설정할수없습니다.
  - 앱제거허용**:** 사용자가관리되는 Google Play 스토어내에서앱을제거하도록허용합니다.

  또한 무선업그레이드허용설정을제한정책에서 OS 업데이트정책으로이동했습니다.

  이러한변경사항에대한자세한내용은 제한장치정책 및 OS 업데이트장치정책을참조하십시오.
- Android Enterprise 에대한제한설정이명확하게재구성되었습니다. 때로는설정이름이약간변경되는경우가있습니다. 재구성에대한자세한내용은 Android Enterprise 설정을참조하십시오.
- 이제 Android Enterprise 장치에서관리되는앱을자동으로업데이트할수있습니다. 자세한내용은 관리되는앱자동업데이트장치정책을참조하십시오.
- Files 장치정책을사용하여업로드가능한파일형식목록을구성할수있습니다. 다음파일유형은이허용목록에추가해도업로드할수없습니다.
  - .cab
  - .appx
  - .ipa
  - .apk
  - .xap
  - .mdx
  - .exe

  자세한내용은 서버속성을참조하십시오.

장치등록

- 이제 iOS 및 Android 장치에대해서로다른등록프로필을만들수있습니다. XenMobile Server 는등록유형이서로다른여러등록프로필을지원합니다. 자세한내용은 등록프로필을참조하십시오.
- 완전관리형 Android 11 이상장치는회사소유장치모드로작업프로필에등록됩니다. 새로운모드는장치에서개인프로필과직장프로필을추가로구분합니다. 이변경사항을통해조직은관리되는프로필을보다효과적으로제어할수있으며사용자에게개인프로필에대한더효과적인개인정보보호를제공할수있습니다. 자세한내용은 Android Enterprise 및 서버속성을참조하십시오.
- 이제사용자가 iOS 또는 macOS 장치를설정할때건너뛸설정화면을추가로지정할수있습니다.
  - iOS
    - 복원완료**:** 설치중에복원이완료되었는지여부가사용자에게표시되지않습니다. iOS 14.0 에해당합니다.
    - 업데이트완료**:** 설치중에소프트웨어업데이트가완료되었는지여부가사용자에게표시되지않습니다. iOS 14.0 에해당합니다.
  - macOS
    - 접근성**:** 사용자가 Voice Over 를자동으로들을수없습니다. 장치가이더넷에연결된경우에만사용할수있습니다. macOS 11 이상에해당합니다.
    - 생체인식**:** 사용자가 Touch ID 및 Face ID 를설정할수없습니다. macOS 10.12.4 이상에해당합니다.
    - **True Tone:** 사용자가 4 채널센서를설정해디스플레이의화이트밸런스를동적으로조정할수없습니다. macOS 10.13.6 이상에해당합니다.
    - **Apple Pay:** 사용자가 Apple Pay 를설정할수없습니다. 이설정을선택취소하면사용자는 Touch ID 및 Apple ID 를설정해야합니다. **Apple ID** 및 생체인식설정이선택취소되었는지확인합니다. macOS 10.12.4 이상에해당합니다.
    - 스크린타임**:** 사용자가스크린타임을활성화할수없습니다. macOS 10.15 이상에해당합니다.

  설정옵션구성에대한자세한내용은 Apple 배포프로그램을통한장치배포를참조하십시오.

업데이트로그파일표시

업데이트로그파일표시라는새옵션은 문제해결메뉴의 로그명령줄인터페이스에서사용할수있습니다. 이옵션을사용하면업데이트로그목록의내용을볼수있으며문제해결의효율성을높일수있습니다. 명령줄인터페이스도구에대한자세한내용은 명령줄인터페이스옵션을참조하십시오.

오류로그파일

문제해결및지원 **>** 로그에서로그를확인할때이제디버그로그에서필터링된오류가표시된로그를확인할수있습니다. 자세한내용은 XenMobile 에서로그파일보기를참조하십시오.

서버속성

- `afw.allow.legacy.apps` 서버속성을구성하여레거시 Android 앱을 Android Enterprise 앱에제공할지여부를결정할수있습니다. 자세한내용은 서버속성을참조하십시오.
- 이제 XenMobile Server 포트 443 의대안으로포트 2197 을사용할수있도록지원합니다. 포트 2197 을사용하여 `api.push.apple.com`에서 APN 알림을보내고받을수있습니다. 포트는 HTTP/2 기반 APN 공급자 API 를사용합니다. 서버속성 `apns.http2.alternate.port.enabled`의기본값은 **`false`**입니다. 포트 2197 을사용하려면서버속성을업데이트한다음서버를다시시작하십시오.
- 암호유효성검사는사용자가약한암호를사용하지못하도록합니다. `enable.password.strength.validation` 속성을 **`true`**로설정하면약한암호를사용하는로컬사용자를만들수없습니다.

VPN 가상서버목록개선

VPN 서버이름에 `_XM_XenMobileGetway`가포함되어있지않으면 XenMobile Server 는목록에서사용가능한첫번째 VPN 가상서버를선택합니다.

Citrix Launcher 지원

XenMobile Server 는 Android Enterprise 장치에서 Citrix Launcher 를지원합니다. 자세한내용은 Launcher 구성 장치정책을참조하십시오.

XenMobile Server 색상개편

XenMobile Server 는 Citrix 브랜드색상업데이트를준수합니다.

XenMobile Server 10.13 의새로운기능

May 6, 2022

XenMobile Server 10.13(PDF 다운로드)

Citrix ADC 에서지원중단되는클래식정책에대한지속적인지원

Citrix 는최근 Citrix ADC 12.0 빌드 56.20 부터클래식정책기반기능의일부를지원중단한다고발표했습니다. Citrix ADC 지원중단고지는 Citrix Gateway 와의기존 XenMobile Server 통합에는영향을주지않습니다. XenMobile Server 는클래식정책을계속지원하므로별도의작업이필요하지않습니다.

XenMobile 마이그레이션서비스

XenMobile Server 를온-프레미스에서사용하는경우무료 XenMobile 마이그레이션서비스를사용하여 Endpoint Management 를시작할수있습니다. XenMobile Server 에서 Citrix Endpoint Management 로마이그레이션할때장치를재등록할필요는없습니다.

마이그레이션을시작하려면해당지역의 Citrix 영업사원또는 Citrix 파트너에게문의하십시오. XenMobile 마이그레이션서비스를참조하십시오.

사용중단발표

단계적으로중단되는 Citrix XenMobile 기능에대한고급알림은 사용중단을참조하십시오.

엔드포인트를 **iOS 14.5** 로업그레이드하기전에

Citrix 는엔드포인트를 iOS 14.5 로업그레이드하기전에다음작업을수행하여앱충돌을완화할것을권장합니다.

- Citrix Secure Mail 및 Secure Web 을 21.2.X 이상으로업그레이드합니다. MDX 또는엔터프라이즈앱업그레이드를참조하십시오.
- MDX Toolkit 을사용하는경우 MDX Toolkit 21.3.X 이상으로모든타사 iOS 애플리케이션을래핑합니다. 최신버전은 MDX Toolkit 다운로드페이지를확인하십시오.

온-프레미스 **Citrix ADC** 를업그레이드하기전에

온-프레미스 Citrix ADC 를특정버전으로업그레이드하면 Single Sign-on 오류가발생할수있습니다. 회사직원로그인옵션이있는브라우저에서 Citrix Files 또는 ShareFile 도메인 URL 에 Single Sign-on 으로인해오류가발생합니다. 사용자가로그인할수없습니다.

이문제의해결방법: Citrix Gateway 의 ADC CLI 에서다음명령을아직실행하지않은경우명령을실행하여전역 SSO 를사용하도록설정합니다.

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

자세한내용은다음을참조하십시오.

- Citrix ADC 릴리스 (Feature Phase) 13.0 빌드 67.39/67.43
- 영향을받는 SSO 구성

문제해결을완료한후사용자는회사직원로그인옵션이제공되는브라우저에서 SSO 를사용하여 Citrix Files 또는 ShareFile 도메인 URL 에인증할수있습니다. [CXM-88400]

XenMobile 10.13 로업그레이드하기전에 (온-프레미스)

일부시스템요구사항이변경되었습니다. 자세한내용은 시스템요구사항및호환성과 XenMobile 호환성을참조하십시오.

1. 업그레이드할 XenMobile Server 를실행하는가상컴퓨터의 RAM 이 8GB 미만인경우 8GB 이상으로 RAM 을늘리는것이좋습니다.
2. 최신버전의 XenMobile Server 10.13 으로업데이트하기전에 Citrix License Server 를 11.16 이상으로업데이트하십시오.

   최신버전의 XenMobile 에는 Citrix License Server 11.16(최소버전) 이필요합니다.

   > 참고:
   >
   > XenMobile 10.13 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2020 년 9 월 29 일입니다. Citrix 라이센스의 Customer Success Services 날짜는이날짜보다이후여야합니다.
   >
   > 날짜는라이센스서버의라이센스옆에서볼수있습니다. 최신버전의 XenMobile 을이전버전의라이센스서버환경에연결하면연결확인이실패하고라이센스서버를구성할수없게됩니다.

   라이센스의날짜를갱신하려면 Citrix 포털에서최신라이센스파일을다운로드하고라이센스서버에파일을업로드하십시오. Customer Success Services를참조하십시오.
3. 클러스터된환경의경우: iOS 11 이상을실행하는장치에 iOS 정책및앱을배포하려면다음과같은요구사항이충족되어야합니다. Citrix Gateway 에 SSL 지속성이구성되어있으면모든 XenMobile Server 노드에서포트 80 을열어야합니다.
4. XenMobile 업데이트를설치하기전에 VM 의기능을사용하여시스템스냅샷을생성합니다. 또한시스템구성데이터베이스를백업합니다. 업그레이드도중문제가발생하는경우전체백업을사용하여복구할수있습니다.

업그레이드하려면

이번릴리스에서 XenMobile 은 VMware ESXi 7.0 을지원합니다. ESXi 7.0 를설치하거나업그레이드하기전에 10.13 으로업그레이드해야합니다.

XenMobile 10.12.x 또는 10.11.x 에서직접 XenMobile 10.13 으로업그레이드할수있습니다. 업그레이드를수행하려면사용가능한최신이진파일을다운로드합니다. https://www.citrix.com/downloads로이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server >** 제품소프트웨어 **> XenMobile Server 10** 으로이동합니다. 해당하는하이퍼바이저에대한 XenMobile Server 소프트웨어타일에서 파일다운로드를클릭합니다.

업그레이드를업로드하려면 XenMobile 콘솔의 릴리스관리페이지를사용합니다. 릴리스관리페이지를사용하여업그레이드하려면을참조하십시오.

업그레이드후

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

- 이인증서유효성검사오류는 XenMobile Server 에서호스트이름유효성검사를비활성화해야함을나타냅니다.
- 기본적으로호스트이름유효성검사는 Microsoft PKI 서버를제외한발신연결에대해활성화됩니다.
- 호스트이름유효성검사로인해배포가중단되는경우서버속성 `disable.hostname.verification`을 **`true`**로 변경하십시오. 이속성의기본값은 **`false`**입니다.

플랫폼지원업데이트

- **iOS 14:** XenMobile Server 및 Citrix 모바일생산성앱은 iOS 14 와호환되지만현재는새로운 iOS 14 기능을지원하지않습니다. MDX Toolkit 20.8.5 이상을사용하거나 MAM SDK 를사용하여앱을준비합니다.
- **Android 11:** XenMobile Server 는 Android 11 을지원합니다. Google Device Administration API 의지원중단이 Android 10 이상을실행하는장치에미치는영향에대해서는 장치관리에서 Android Enterprise 로마이그레이션을참조하십시오. 이 Citrix 블로그도참조하십시오.

단일환경에서여러장치및앱관리모드구성

이제하나의 XenMobile 사이트를구성하여여러등록구성을지원할수있습니다. 등록프로필의역할이장치및앱관리를위한등록설정을포함하도록확장되었습니다.

등록프로필은단일 XenMobile 콘솔내에서여러사용사례와장치마이그레이션경로를지원합니다. 사용사례에는다음이포함됩니다.

- Mobile Device Management(MDM 전용)
- MDM+MAM(Mobile Application Management)
- MAM 전용
- 회사소유등록
- BYOD 등록 (MDM 등록취소기능)
- Android Enterprise 등록으로 Android 장치관리자등록마이그레이션 (완전관리됨, 작업프로필, 전용장치)

등록프로필은이제지원중단된 `xms.server.mode` 서버속성을대체합니다. 이러한변경은기존배달그룹과등록된장치에영향을미치지않습니다.

전용장치를등록하지않아도된다면 `enable.multimode.xms`을 **`false`**로설정하여이기능을비활성화하면됩니다. 서버속성을참조하십시오.

다음표는기존서버모드에서새등록프로필기능으로자동화된마이그레이션경로를보여줍니다.

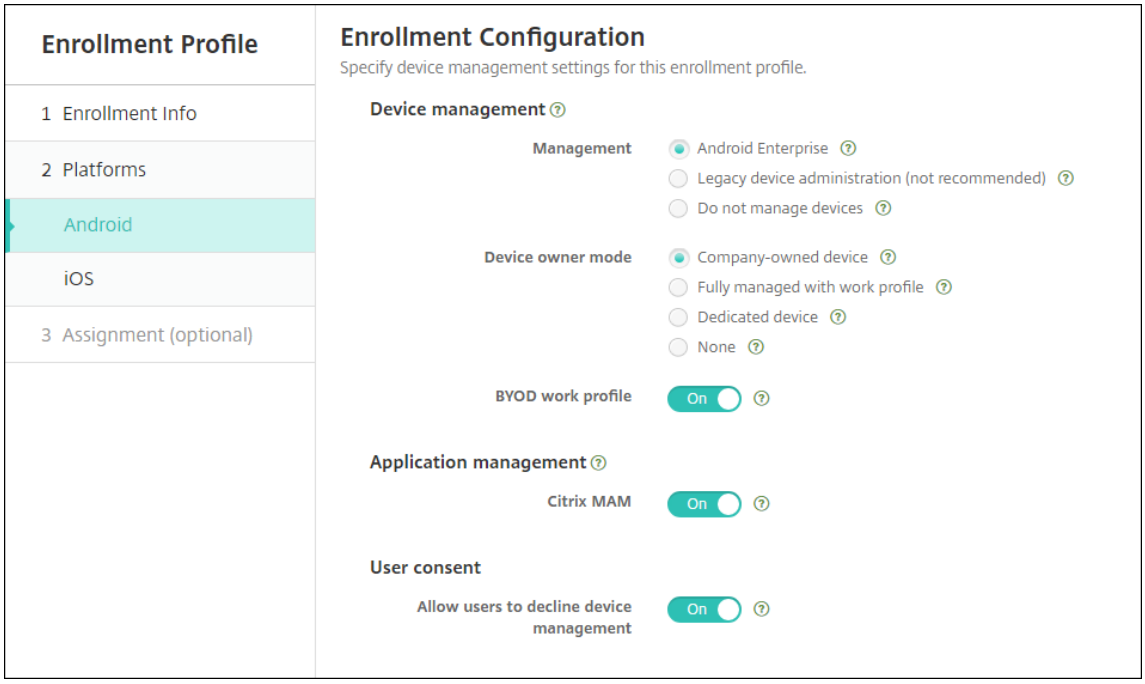
기존서버속성	새관리모드
ENT 모드 (iOS)	Citrix MAM 을활용하는 Apple 장치등록
ENT 모드 (Android)	Citrix MAM 을활용하는레거시장치관리자
ENT 모드 (Android Enterprise)	Citrix MAM 을활용하는완전관리형장치 (이전의 COPE) 의작업프로필

기존서버속성	새관리모드
MAM 모드 (iOS 및 Android)	Citrix MAM
MDM 모드 (iOS)	Apple 장치등록
MDM 모드 (Android)	레거시장치관리자
MDM 모드 (Android Enterprise)	완전관리형장치의작업프로필

배달그룹을만들면해당그룹에등록프로필을첨부할수있습니다. 등록프로필을첨부하지않으면 XenMobile 이전역등록프로필을첨부합니다.

등록프로필은다음장치관리기능을제공합니다.

- **Android** 장치관리자 **(DA)** 모드를 **Android Enterprise** 로더쉽게마이그레이션할수있습니다**.** Android Enterprise 장치의경우설정에완전관리형장치, 완전관리형장치의작업프로필, 전용장치와같은장치소유자모드가포함됩니다. Android Enterprise를참조하십시오.



이업그레이드의경우서버모드에대한현재 XenMobile 구성과 설정 **> Android Enterprise** 가다음과같이새로운등록프로필설정에매핑됩니다.

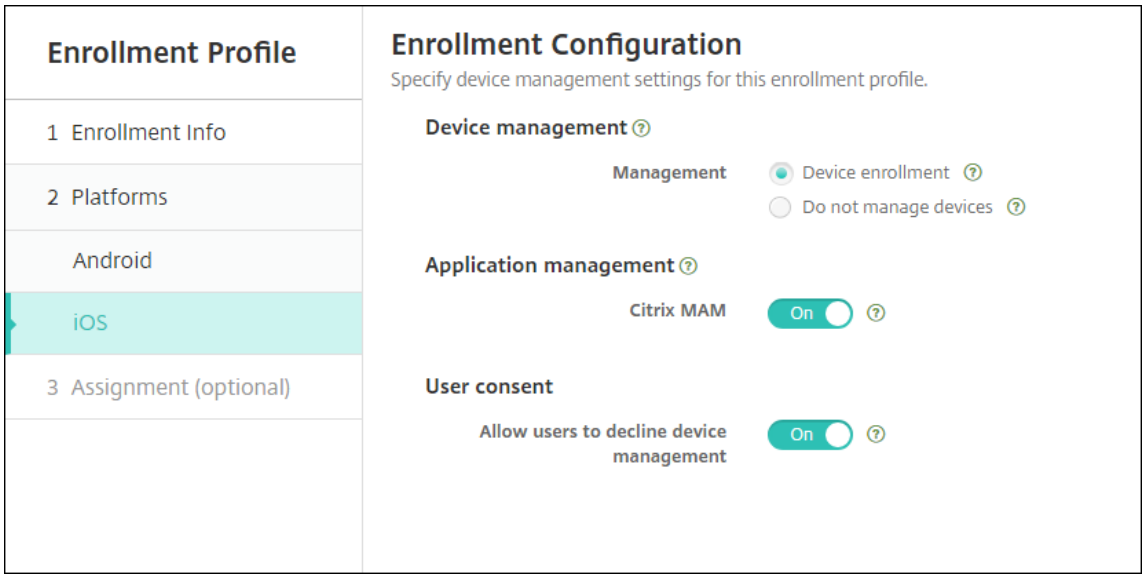
현재구성	관리설정	장치소유자모드설정	Citrix MAM 설정
MDM. 관리되는 Google Play(Android Enterprise)	Android Enterprise	완전관리형장치의작업프로필	꺼짐

현재구성	관리설정	장치소유자모드설정	Citrix MAM 설정
MDM, G Suite(레거시 DA)	레거시 DA	해당없음	꺼짐
MAM	장치관리안함	해당없음	켜짐
MDM+MAM. 관리되는 Google Play(Android Enterprise)	Android Enterprise*	완전관리형장치의작업프로필	켜짐
MDM+MAM, G Suite(레거시 DA)	레거시 DA*	해당없음	켜짐

* 등록이필요한경우 사용자의장치관리거부를허용을 꺼짐으로설정합니다.

업그레이드하고나면현재등록프로필에이러한매핑이반영됩니다. 신규사용사례를레거시 DA 로부터의전환으로처리하려면다른등록프로필생성여부를고려해보십시오.

- 더간편해진 **iOS** 관리**.** iOS 장치의경우설정에서장치를관리되는장치또는관리되지않는장치로등록할지를선택할수있습니다.



이업그레이드의경우이전구성이새등록프로필에다음과같이매핑됩니다.

서버모드	관리설정	Citrix MAM 설정
MDM	장치등록	꺼짐
MAM	장치관리안함	켜짐
MDM+MAM	장치등록	켜짐

등록이필요한경우 사용자의장치관리거부를허용을 꺼짐으로설정합니다.

강화된등록프로필에다음과같은제한이존재합니다.

- 일회용 PIN 또는 2 단계인증등록초대에는강화된등록프로필기능을사용할수없습니다.

등록프로필을참조하십시오.

최신 **HTTP/2** 기반 **APN** 제공업체 **API** 지원

Apple 의 Apple 푸시알림서비스레거시바이너리프로토콜지원이 2021 년 3 월 31 일에종료됩니다. Apple 에서는 HTTP/2 기반 APN 제공업체 API 를대신사용하도록권장합니다. XenMobile Server 에서는이제 HTTP/2 기반 API 를지원합니다. 자세한정보는 https://developer.apple.com/에서뉴스업데이트 “Apple 푸시알림서비스업데이트” 를참고하십시오. APN 연결확인과관련된지원은 연결확인을참조하십시오.

다음 XenMobile Server 버전에서기본적으로 HTTP/2 기반 API 를지원합니다.

- XenMobile Server 10.13
- XenMobile Server 10.12 롤링패치 5 이상

다음 XenMobile Server 버전을사용하는경우지원을이용하려면 **apple.apns.http2** 서버속성을추가해야합니다.

- XenMobile Server 10.12 롤링패치 2-4 이상
- XenMobile Server 10.11 롤링패치 5 이상

XenMobile Server 10.11 은더이상지원되지않으므로최신릴리스로업그레이드하는것이좋습니다.

여러 **iOS** 장치에장치인증서기반 **IPsec VPN** 사용

장치인증서기반 IPsec VPN 이필요한 iOS 장치마다 VPN 장치정책과자격증명장치정책을구성하는대신프로세스를자동화해보십시오.

1. 연결유형이 **IKEv2** 항상켜짐인상태로 iOS VPN 장치정책을구성합니다.
2. 장치 **ID** 기반장치인증서를장치인증방법으로선택합니다.
3. 사용할 장치 **ID** 유형을선택합니다.
4. REST API 를사용하여장치인증서를일괄적으로가져옵니다.

VPN 장치정책구성에대한자세한내용은 VPN 장치정책을참조하십시오. 인증서일괄가져오기에대한자세한내용은 REST API 로 인증서일괄업로드를참조하십시오.

Apple 볼륨구매앱자동업데이트

볼륨구매계정을추가하면 (설정 **> iOS** 설정) 이제모든 iOS 앱을자동으로업데이트할수있습니다. Apple 볼륨구매에서 앱자동업데이트설정을참고하십시오.

로컬사용자계정의암호요구사항

XenMobile 콘솔에서로컬사용자계정을추가하거나편집할경우최신암호요구사항을따라야합니다.

자세한내용은 로컬사용자계정을추가하려면을참조하십시오.

- 암호요구사항**:** XenMobile Server 콘솔에서로컬사용자계정을추가하거나편집할경우최신암호요구사항을따르십시오. 로컬사용자계정을추가하려면을참조하십시오.
- 로컬사용자계정잠금**:** 사용자가유효하지않은로그인시도를연속으로할수있는최대횟수에도달한경우로컬사용자계정이 30 분간잠깁니다. 잠금기간이만료될때까지시스템에서는모든인증시도를거부합니다. XenMobile Server 콘솔에서계정의잠금을해제하려면 관리 **>** 사용자로이동한다음사용자계정을선택하고 로컬사용자잠금해제를클릭합니다. 로컬사용자계정을잠금해제하려면을참조하십시오.

장치정책

Android Enterprise 장치의신규장치정책및장치정책설정이추가되었습니다.

Android Enterprise 장치에서트레이도구모음아이콘숨기기

이제 Android Enterprise 장치에서트레이도구모음아이콘을숨기거나표시할지여부를선택할수있습니다. XenMobile 옵션 장치정책을참조하십시오.

작업프로필모드또는완전관리형장치모드의 **Android Enterprise** 장치에대한추가인증서관리기능

관리되는키저장소에서인증기관을설치할뿐아니라이제다음기능도관리할수있습니다.

- 특정관리되는앱을사용하는인증서를구성합니다**.** Android Enterprise 의인증서장치정책에이제 인증서를사용할앱설정이포함됩니다. 이정책에서선택한자격증명공급자가발행한사용자인증서를사용할앱을지정할수있습니다. 런타임중에인증서에대한액세스권한이자동으로앱에부여됩니다. 모든앱에인증서를사용하려면앱목록을비워두십시오. 자격증명장치정책을참조하십시오.
- 관리되는키저장소에서인증서를자동으로삭제하거나비시스템 **CA** 인증서를제거하십시오**.** 자격증명장치정책을참조하십시오.
- 사용자가관리되는키저장소에저장된자격증명을수정할수없게합니다**.** Android Enterprise 의제한장치정책에이제 사용자가사용자자격증명을구성하도록허용설정이포함됩니다. 기본적으로이설정은 켜짐입니다. 제한장치정책을참조하십시오.

관리되는구성에서더간편하게사용하는인증서별칭

관리되는구성장치설정이포함된 자격증명장치정책에서새 인증서별칭설정을사용합니다. 이렇게하면사용자작업없이도앱이 VPN 에서인증할수있습니다. 앱로그에서자격증명별칭을찾는대신자격증명별칭을만듭니다. 관리되는구성장치정책의 인증서별칭필드에입력하여별칭을만듭니다. 자격증명장치정책의 인증서별칭설정에동일한인증서별칭을입력합니다. 관리되는구성정책 및 자격증명장치정책을참조하십시오.

Android Enterprise 장치의 **"**한번잠금사용**"** 설정제어

암호장치정책의새로운 통합암호사용설정을사용하면장치에별도의암호와작업프로필이필요한지여부를제어할수있습니다. 이설정전에는사용자가장치의 한번잠금사용설정으로이동작을제어했습니다. 통합암호사용이 켜짐이면사용자는장치에작업프로필과동일한암호를사용할수있습니다. 통합암호사용이 꺼짐이면사용자는장치에작업프로필과동일한암호를사용할수없습니다. 기본값은 꺼짐입니다. Android 9.0 이상을실행하는 Android Enterprise 장치에 통합잠금사용설정을사용할수있습니다. 암호장치정책을참조하십시오.

규정을준수하지않는 **Android Enterprise** 장치의앱과바로가기표시

Android Enterprise 의암호장치정책에는새로운설정인 암호가규정을준수하지않는경우앱및바로가기표시가있습니다. 이설정을사용하여장치암호가더이상규정을준수하지않을경우앱과바로가기를계속표시할수있습니다. Citrix 에서는암호가규정을준수하지않는경우규정을준수하지않는장치로표시하도록자동화된작업을만드는것을권장합니다. 암호장치정책을참조하십시오.

Android Enterprise 작업프로필장치또는완전히관리되는장치에서인쇄하는기능비활성화

제한장치정책에서 인쇄허용안함설정을사용하면사용자가 Android Enterprise 장치에서액세스할수있는프린터로인쇄할수있는지여부를지정할수있습니다. Android Enterprise 설정을참조하십시오.

키오스크정책에서패키지이름을추가하여전용장치의앱허용

이제 Android Enterprise 플랫폼에서허용할패키지이름을입력할수있습니다. Android Enterprise 설정을참조하십시오.

Android Enterprise 작업프로필및완전히관리되는장치에대한 **Keyguard** 관리

Android Keyguard 는장치및 Work Challenge 잠금화면을관리합니다. 다음과같은 Keyguard 관리장치정책을사용하여 제어합니다.

- 작업프로필장치의 Keyguard 관리. 사용자가장치 Keyguard 와 Work Challenge Keyguard 의잠금을해제하기 전에사용할수있는기능을지정할수있습니다. 예를들어, 기본적으로사용자는지문잠금해제를사용하고잠금화면에서수정되지않은알림을확인할수있습니다. Keyguard 관리정책을사용하여 Android 9.0 이상을실행하는장치에대해모든생체 인증을비활성화할수도있습니다.
- 완전관리형전용장치의 Keyguard 관리. Keyguard 화면의잠금을해제하기전에신뢰할수있는에이전트, 보안카메라와 같이사용할수있는기능을지정할수있습니다. 또는모든 Keyguard 기능을사용하지않도록선택할수있습니다.

Keyguard 관리장치정책을참조하십시오.

XenMobile 콘솔에서 **Android Enterprise** 의엔터프라이즈앱게시

Android Enterprise 개인앱을추가할때더이상 Google Play 개발자계정을등록하지않아도됩니다. XenMobile 콘솔에서 APK 파일을업로드하고게시할수있도록관리되는 Google Play 스토어 UI 가열립니다. 자세한내용은 엔터프라이즈앱추가를참조하십시오.

XenMobile 콘솔에서 **Android Enterprise** 의웹앱게시

이제관리되는 Google Play 또는 Google 개발자포털로이동하지않고도 XenMobile 용 Android Enterprise 웹앱을게시할수있습니다. 구성 **>** 앱 **>** 웹링크에서 업로드를클릭하면파일을업로드하고저장할수있도록관리되는 Google Play 스토어 UI 가열립니다. 약 10 분안에앱을승인하고게시할수있습니다. 자세한내용은 웹링크추가를참조하십시오.

XenMobile Server REST API 로 **iOS** 장치에인증서일괄업로드

한번에인증서하나를업로드하는것이실용적이지않다면 XenMobile Server REST API 를사용하여 iOS 장치에인증서를일괄업로드할수있습니다.

1. 연결유형이 **IKEv2** 항상켜짐인상태로 iOS VPN 장치정책을구성합니다.
2. 장치 **ID** 기반장치인증서를장치인증방법으로선택합니다.
3. 사용할 장치 **ID** 유형을선택합니다.
4. REST API 를사용하여장치인증서를일괄적으로가져옵니다.

VPN 장치정책구성에대한자세한내용은 VPN 장치정책을참조하십시오. 인증서일괄가져오기에대한자세한내용은 REST API 로 iOS 장치에인증서일괄업로드를참조하십시오.

암호화키새로고침

XenMobile CLI 의고급설정에서 암호화키새로고침옵션이추가됩니다. 이옵션을사용하여암호화키를한번에한노드씩새로고칠수있습니다. 시스템옵션을참조하십시오.

ESXi 7.0 지원

이번릴리스에서 XenMobile 은 VMware ESXi 7.0 을지원합니다. ESXi 7.0 를설치하거나업그레이드하기전에 10.13 으로업그레이드해야합니다.

새서버속성

이제다음서버속성이제공됩니다.

- **iOS App Store** 링크에호스트이름허용**:** 콘솔이아닌공개 API 를사용하여 iOS 용공개앱스토어앱을추가하려면원할경우허용된호스트이름목록을구성합니다.
- 로컬사용자계정잠금한도**:** 계정이잠기기전에로컬사용자에게허용되는로그인시도횟수를구성합니다.
- 로컬사용자계정잠금시간**:** 로그인시도가너무많이실패한경우로컬사용자가잠기는시간의길이를구성합니다.
- 설정된파일업로드최대크기제한**:** 업로드한파일에대한최대파일크기를제한할수있습니다.
- 허용되는파일업로드최대크기**:** 업로드된파일의최대파일크기를설정합니다.

이러한속성에대한자세한내용은 서버속성을참조하십시오.

셀프서비스디스크정리수행

디스크사용량이라는새명령줄인터페이스를 문제해결메뉴에서사용할수있습니다. 이옵션을사용하면코어덤프파일과지원번들파일목록을볼수있습니다. 목록을확인한후명령줄을통해이러한파일을모두삭제하도록선택할수있습니다. 명령줄인터페이스도구에 대한자세한내용은 명령줄인터페이스옵션을참조하십시오.

XenMobile Server 10.12 의새로운기능

January 5, 2022

XenMobile Server 10.12(PDF 다운로드)

XenMobile 마이그레이션서비스

XenMobile Server 를온-프레미스에서사용하는경우무료 XenMobile 마이그레이션서비스를사용하여 Endpoint Management 를시작할수있습니다. XenMobile Server 에서 Citrix Endpoint Management 로마이그레이션할때장치를재등록할필요는없습니다.

마이그레이션을시작하려면해당지역의 Citrix 영업사원또는 Citrix 파트너에게문의하십시오. 자세한내용은 XenMobile 마이그레이션서비스를참조하십시오.

사용중단발표

단계적으로중단되는 Citrix XenMobile 기능에대한고급알림은 사용중단을참조하십시오.

예정된변경사항에대한 **Android** 장치준비

이전에발표된사용중단은 Android 및 Android Enterprise 장치에영향을미칩니다.

- Android 10 에대한 DA(장치관리) 등록:
  - **2020** 년 **7** 월 **31** 일**:** 레거시 Android 장치관리모드에대한신규등록이중단됩니다.
  - **2020** 년 **11** 월 **1** 일**:** Google 의레거시장치관리 API 사용이중단됩니다. 레거시장치관리모드에서실행되는 Android 10 장치는더이상작동하지않습니다.
- MDX 암호화:
  - **2020** 년 **8** 월 **1** 일**:** Citrix 모바일생산성및타사 MDX 앱에대한 MDX 암호화가플랫폼암호화로마이그레이션됩니다.
  - **2020** 년 **9** 월 **1** 일**:** MDX 암호화가수명종료에도달합니다.

레거시 **DA** 에서등록된장치의경우

- MDX 암호화를사용하지않는경우별도의조치가필요하지않습니다.

- MDX 암호화를사용하는경우 2020 년 7 월 31 일이전에 Android 장치를 Android Enterprise 로마이그레이션하십시오. Android 10 을실행하는장치는 Android Enterprise 를사용하여등록하거나재등록해야합니다. 이요구사항에는 MAM 전용모드의 Android 장치가포함됩니다. 장치관리에서 Android Enterprise 로마이그레이션을참조하십시오.

7 월 **31** 일을기준으로 **Android Enterprise** 에이미등록된장치의경우

- Android Enterprise 플랫폼을사용하여앱을게시한경우 Android Enterprise 를통해암호화가이미처리되었습니다. 작업이필요하지않습니다.
- 레거시 Android 플랫폼을사용하여앱을게시한경우 2020 년 7 월 31 일이전에 Android Enterprise 를사용하여앱을다시게시합니다.

XenMobile 10.12 로업그레이드하기전에 (온-프레미스)

일부시스템요구사항이변경되었습니다. 자세한내용은 시스템요구사항및호환성과 XenMobile 호환성을참조하십시오.

1. 최신버전의 XenMobile Server 10.12 로업데이트하기전에 Citrix License Server 를 11.16 이상으로업데이트하십시오.

   최신버전의 XenMobile 에는 Citrix License Server 11.16(최소버전) 이필요합니다.

   > 참고:
   >
   > 미리보기에자체라이센스를사용하려는경우 XenMobile 10.12 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2020 년 1 월 20 일이라는점을숙지하십시오. Citrix 라이센스의 Customer Success Services 날짜는이날짜보다이후여야합니다.
   >
   > 날짜는라이센스서버의라이센스옆에서볼수있습니다. 최신버전의 XenMobile 을이전버전의라이센스서버환경에연결하면연결확인이실패하고라이센스서버를구성할수없게됩니다.

   라이센스의날짜를갱신하려면 Citrix 포털에서최신라이센스파일을다운로드하고라이센스서버에파일을업로드하십시오. 자세한내용은 Customer Success Services를참조하십시오.

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

업그레이드하려면

XenMobile 10.11.x 또는 10.10.x 에서직접 XenMobile 10.12 로업그레이드할수있습니다. 업그레이드를수행하려면사용가능한최신이진파일을다운로드합니다. https://www.citrix.com/downloads로이동하십시오. **Citrix Endpoint**

Management(XenMobile) > XenMobile Server > 제품소프트웨어 **> XenMobile Server 10** 으로이동합니다. 해당하는하이퍼바이저에대한 XenMobile Server 소프트웨어타일에서 파일다운로드를클릭합니다.

업그레이드를업로드하려면 XenMobile 콘솔의 릴리스관리페이지를사용합니다. 자세한내용은 릴리스관리페이지를사용하여업그레이드하려면을참조하십시오.

업그레이드후

XenMobile 10.12 로업그레이드한후 (온-프레미스):

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

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

iOS 13 에대한추가지원

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(**장치등록프로그램**)** 페이지에포함되어있습니다. 이러한화면을건너뛰도록 XenMobile Server 를구성할수없습니다. 이러한페이지는 iOS 13 장치사용자에게나타납니다.
- iOS 13 이상에서는이전버전의 iOS 에대한감독또는감독되지않은장치에서사용할수있었던일부제한장치정책설정을감독되는장치에서만사용할수있습니다. 현재 XenMobile Server 콘솔의도구설명에는이러한설정이 iOS 13 이상에서감독되는장치전용이라는설명이표시되지않습니다.
  - 하드웨어제어허용:
    - FaceTime
    - 앱설치
  - 앱허용:
    - iTunes 스토어
    - Safari
    - Safari > 자동채우기
  - 네트워크 - iCloud 동작허용:
    - iCloud 문서및데이터
  - 감독되는경우에만해당되는설정 - 허용:
    - 게임센터 > 친구추가
    - 게임센터 > 멀티플레이게임
  - 미디어콘텐츠 - 허용:

* 음악, 팟캐스트및 iTunes U 의성인등급자료

이러한제한은다음과같이적용됩니다.

- iOS 12 이하장치가이미 XenMobile Server 에등록되어있는상태에서 iOS 13 으로업그레이드하는경우위의제한사항은감독되지않는장치및감독되는장치에적용됩니다.
- 감독되지않는 iOS 13 이상장치를 XenMobile Server 에등록하는경우위의제한사항은감독되는장치에만적용됩니다.
- 감독되는 iOS 13 이상장치를 XenMobile Server 에등록하는경우위의제한사항은감독되는장치에만적용됩니다.

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 지원문서를참조하십시오.

조직또는학교에서 VPP(Volume Purchase Program) 만사용하는경우 ABM/ASM 에등록한다음기존 VPP 구매자를새 ABM/ASM 계정으로초대할수있습니다. ASM 의경우 https://school.apple.com으로이동합니다. ABM 의경우 https://business.apple.com으로이동합니다.

XenMobile 에서 VPP 계정을업데이트하려면:

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. **iOS** 설정을클릭합니다. **Volume Purchase Program** 구성페이지가나타납니다.
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.

자세한내용은다음을참조하십시오.

- Apple 배포프로그램
- Apple 장치의대량등록

Android Enterprise COPE 장치에대한지원

XenMobile Server 는작업프로필이있는완전관리형 Android Enterprise 장치 (이전의 COPE(회사소유의개인사용) 장치)를지원합니다. 이러한장치는완전관리형 Android Enterprise 장치의한유형으로, 작업프로필이있는장치를말합니다. 장치와작업프로필에개별정책설정을적용할수있습니다. 이릴리스의경우:

- 자격증명, 암호및제한장치정책을사용하여장치와작업프로필에개별설정을적용할수있습니다.
- 위치장치정책의위치모드설정을 COPE 장치자체에적용할수있지만 COPE 장치의작업프로필에는적용할수없습니다. 위치장치정책의다른설정은 COPE 에서사용할수없습니다.
- 장치또는작업프로필에잠금보안동작을개별적으로적용할수있습니다.

장치정책

작업프로필이있는완전관리형 Android Enterprise 장치 (COPE 장치) 의경우일부장치정책의개별설정을전체장치와작업프로필에적용할수있습니다. XenMobile Server 콘솔에서일부장치정책의개별설정을적용할수있습니다. 다른장치정책을사용하여전체장치에만설정을적용하거나작업프로필로완전히관리되는장치의작업프로필에만설정을적용할수있습니다.

보안동작

작업프로필이있는완전관리형 Android Enterprise 장치 (COPE devices) 의경우다음을적용할수있습니다.

- 잠금보안동작을장치또는작업프로필에개별적으로적용.
- 다른모든보안동작을장치에적용.

등록프로필을사용하여 **Android** 장치의등록옵션제어

XenMobile 배포에서 Android Enterprise 를사용하도록설정한경우이제등록프로필을사용하여 Android 장치의등록방법을제어할수있습니다. 등록프로필은 Android 장치를기본 Android Enterprise 모드 (완전관리형또는작업프로필) 로등록할지, 아니면레거시 (장치관리자) 모드로등록할지를결정합니다.

기본적으로글로벌등록프로필은신규및공장기본값으로재설정된 Android Enterprise 장치를완전관리형장치로등록하고, BYOD Android Enterprise 장치를작업프로필장치로등록합니다. 자세한내용은 Android Enterprise를참조하십시오.

Android Enterprise 를기본등록으로사용하도록레거시 **Android** 장치준비

Google 은장치관리의장치관리자모드사용을중단하고장치소유자모드또는프로필소유자모드에서모든 Android 장치를관리할것을권장하고있습니다. Google Android Enterprise 개발자가이드의 장치관리자사용중단을참조하십시오. 이변경사항을지원하기위해이제 Android 장치의기본등록옵션이 Android Enterprise 로변경되었습니다.

따라서 XenMobile 배포에서 Android Enterprise 를사용하도록설정한경우새로등록되거나다시등록되는모든 Android 장치는 Android Enterprise 장치로등록됩니다.

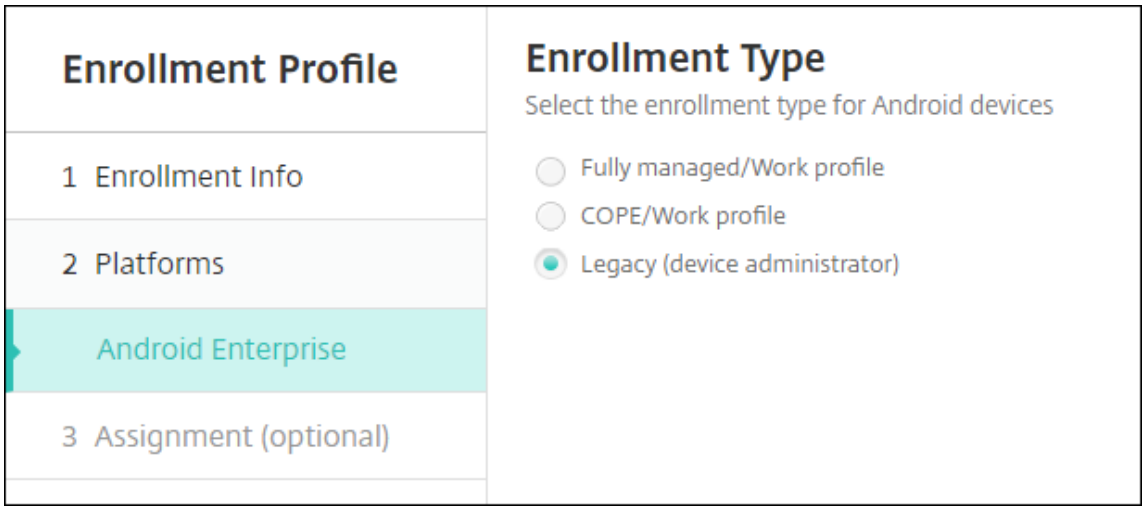
이변경사항을준비하기위해이제 XenMobile 에서 Android 장치의등록방법을제어하는등록프로필을생성할수있습니다.

조직이레거시 Android 장치를장치소유자모드또는프로필소유자모드에서관리할준비가되지않았을수있습니다. 이러한장치를장치관리자모드에서계속해서관리할수있습니다. 레거시장치에대한등록프로필을만들고등록된모든레거시장치를재등록하십시오.

레거시장치에대한등록프로필을만들려면:

1. XenMobile 콘솔에서 구성 **>** 등록프로필로이동합니다.

2. 등록프로필을추가하려면 추가를클릭합니다. 등록정보페이지에서등록프로필의이름을입력합니다.
3. 다음을클릭하거나 플랫폼에서 **Android Enterprise** 를선택합니다. 등록구성페이지가나타납니다.
4. 관리를 레거시 **(**장치관리**)** 로설정합니다. 다음을클릭하거나 할당 **(**옵션**)** 을선택합니다. 배달그룹할당화면이나타납니다.



5. 전용장치를등록하는관리자가포함된배달그룹을선택합니다. 그런다음 저장을클릭합니다.

장치관리자모드에서레거시장치관리를계속하려면이프로필을사용하여등록하거나재등록합니다. 사용자로하여금 Secure Hub 를다운로드하고등록서버 URL 을제공하도록하면작업프로필장치와유사하게장치관리자장치를등록할수있습니다.

Android Enterprise 로의전환에대한 Endpoint Management 지원에대한자세한내용은블로그 Android Enterprise 를기본 Citrix Endpoint Management 서비스로설정을참조하십시오.

Android Enterprise 의간소화된앱관리

이제관리되는 Google Play 또는 Google 개발자포털로이동하지않고도 XenMobile Server 용앱을승인하거나게시할수있습니다. 따라서몇시간이아닌약 10 분안에앱을승인하고게시할수있습니다.

XenMobile Server 콘솔에서공용앱스토어용 **Android Enterprise** 앱승인**.** 이제 XenMobile Server 콘솔을종료하지않고도관리되는 Google Play Store 앱을승인할수있습니다. 검색필드에앱이름을입력하면관리되는 Google Play Store UI 가열리고앱승인및저장에대한지침이표시됩니다. 결과에앱이표시되면앱세부정보를구성할수있습니다. 공용앱스토어앱추가를참조하십시오.

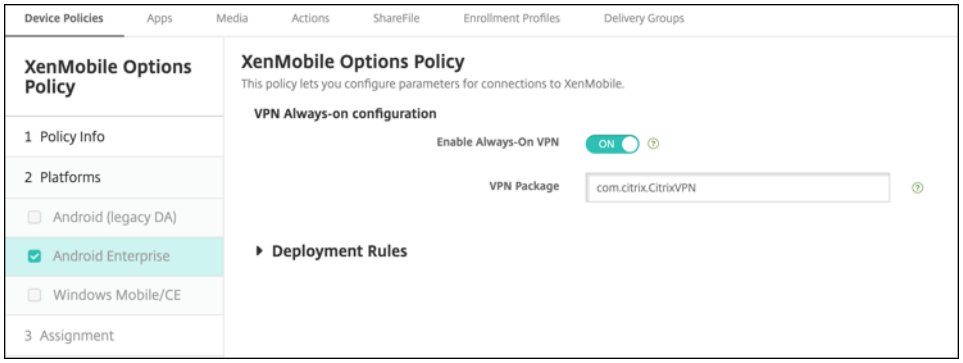
Android Enterprise 용 **MDX** 앱추가**.** 이제 XenMobile Server 콘솔에서 Android Enterprise 가 MDX 앱배포플랫폼으로지원됩니다. MDX 앱추가를참조하십시오.

XenMobile Server 콘솔에서 **Android Enterprise** 용 **MDX** 앱승인**.** 이제 XenMobile Server 콘솔을종료하지않고도 Android Enterprise 용관리되는 Google Play Store 앱을승인할수있습니다. MDX 파일을업로드하면관리되는 Google Play Store UI 가열리고앱승인및저장에대한지침이표시됩니다. MDX 앱추가를참조하십시오.

Android Enterprise 에대한항상 **VPN** 연결지원

이제 XenMobile Server 옵션장치정책에서 Android Enterprise 에대해항상 VPN 연결을사용하도록설정할수있습니다.

Android Enterprise ㅇ에대한 VPN 프로필을구성할때 기본 **VPN** 프로필에 VPN 프로필의이름을입력합니다. XenMobile 은사용자가특정프로필을누르지않고 Citrix SSO 앱의사용자인터페이스에서연결스위치를누를때이프로필을사용합니다. 이필드를비워두면기본프로필이연결에사용됩니다. 하나의프로필만구성된경우기본프로필로표시됩니다. 항상 VPN 연결의경우항상 VPN 연결을설정하는데사용할 VPN 프로필의이름으로이필드를설정해야합니다.



Android Enterprise 앱에대한제품트랙구성

Android Enterprise 에대한공용앱스토어앱또는 MDX 앱을추가할때사용자장치에푸시할제품트랙을구성할수있습니다. 예를들어테스트용으로설계된추적이있는경우해당추적을선택하여특정배달그룹에할당할수있습니다. 릴리스롤아웃에대한자세한내용은 Google Play 도움말센터를참조하십시오. 제품트랙구성에대한자세한내용은 MDX 앱추가 또는 공용앱스토어앱추가를참조하십시오.

macOS 사용자에대한암호재설정강제

macOS 장치에암호정책이포함된구성프로필이수신되는경우사용자는정책설정을충족하는암호를제공해야합니다. 이제사용자의다음인증시에암호재설정을강제할수있습니다. macOS(10.13 이상) 에대한암호장치정책에서새로운설정인 **Force passcode reset(**암호재설정강제적용**)** 을사용하도록설정합니다. 암호정책에대한자세한내용은 암호장치정책을참조하십시오.

XenMobile Server 10.11 의새로운기능

May 6, 2022

XenMobile Server 10.11(PDF 다운로드)

XenMobile 마이그레이션서비스

XenMobile Server 를온-프레미스에서사용하는경우무료 XenMobile 마이그레이션서비스를사용하여 Endpoint Management 를시작할수있습니다. XenMobile Server 에서 Citrix Endpoint Management 로마이그레이션할때장치를재등록할필요는없습니다.

마이그레이션을시작하려면해당지역의 Citrix 영업사원또는 Citrix 파트너에게문의하십시오. 자세한내용은 XenMobile 마이그레이션서비스를참조하십시오.

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 지원문서를참조하십시오.

조직또는학교에서 VPP(Volume Purchase Program) 만사용하는경우 ABM/ASM 에등록한다음기존 VPP 구매자를새 ABM/ASM 계정으로초대할수있습니다. ASM 의경우 https://school.apple.com으로이동합니다. ABM 의경우 https://business.apple.com으로이동합니다.

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 에대한추가지원

> 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(**장치등록프로그램**)** 페이지에포함되지않습니다. 따라서이러한화면을건너뛰도록 XenMobile Server 를구성할수없습니다. 이러한페이지는 iOS 13 장치사용자에게나타납니다.
- iOS 13 이상에서는이전버전의 iOS 에대한감독또는감독되지않은장치에서사용할수있었던일부제한장치정책설정을감독되는장치에서만사용할수있습니다. 현재 XenMobile Server 콘솔의도구설명에는이러한설정이 iOS 13 이상에서감독되는장치전용이라는설명이표시되지않습니다.
  - 하드웨어제어허용:
    - FaceTime
    - 앱설치
  - 앱허용:
    - iTunes 스토어
    - Safari
    - Safari > 자동채우기
  - 네트워크 - iCloud 동작허용:
    - iCloud 문서및데이터
  - 감독되는경우에만해당되는설정 - 허용:
    - 게임센터 > 친구추가
    - 게임센터 > 멀티플레이게임
  - 미디어콘텐츠 - 허용:
    - 음악, 팟캐스트및 iTunes U 의성인등급자료

이러한제한은다음과같이적용됩니다.

- iOS 12 이하장치가이미 XenMobile Server 에등록되어있는상태에서 iOS 13 으로업그레이드하는경우위의제한사항은감독되지않는장치및감독되는장치에적용됩니다.
- 감독되지않는 iOS 13 이상장치를 XenMobile Server 에등록하는경우위의제한사항은감독되는장치에만적용됩니다.
- 감독되는 iOS 13 이상장치를 XenMobile Server 에등록하는경우위의제한사항은감독되는장치에만적용됩니다.

iOS 13 및 **macOS 15** 의신뢰할수있는인증서에대한요구사항

Apple 은 TLS 서버인증서에대한새로운요구사항을도입했습니다. 모든인증서가새로운 Apple 요구사항을따르는지확인하십시오. Apple 게시물 https://support.apple.com/en-us/HT210176를참조하십시오. 인증서관리에대한도움말은 XenMobile 에서인증서업로드를참조하십시오.

GCM 에서 **FCM** 으로업그레이드

2018 년 4 월 10 일을기준으로 Google 은 GCM(Google Cloud Messaging) 을더이상사용하지않습니다. Google 은 2019 년 5 월 29 일에 GCM 서버및클라이언트 API 를제거했습니다.

> 중요요구사항:
>
> - 최신버전의 XenMobile Server 로업그레이드하십시오.
> - 최신버전의 Secure Hub 로업그레이드하십시오.

Google 에서는 FCM 의새로운기능을활용할수있도록즉시 FCM(Firebase Cloud Messaging) 으로업그레이드할것을권장합니다. Google 의자세한내용은 https://developers.google.com/cloud-messaging/faq 및 https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html을참조하십시오.

Android 장치로의푸시알림에대한지원을계속하려면: XenMobile Server 에서 GCM 을사용하는경우 FCM 으로마이그레이션합니다. 그런다음 Firebase Cloud Messaging 콘솔에서제공되는새 FCM 키를사용하여 XenMobile Server 를업데이트합니다.

다음단계는신뢰할수있는인증서를사용할때의등록워크플로에대한것입니다.

업그레이드단계:

1. Google 의정보에따라 GCM 에서 FCM 으로업그레이드합니다.
2. Firebase Cloud Messaging 콘솔에서새 FCM 키를복사합니다. 이키는다음단계를수행하는데필요합니다.
3. XenMobile Server 콘솔에서 설정 **> Firebase Cloud Messaging** 으로이동하고설정을구성합니다.

다음에 XenMobile Server 로체크인하고정책새로고침을수행하면장치가 FCM 으로전환됩니다. Secure Hub 에서장치를새로고치려면: Secure Hub 에서 기본설정 **>** 장치정보로이동하고 정책새로고침을누릅니다.
FCM 구성에대한자세한내용은 Firebase Cloud Messaging을참조하십시오.

XenMobile 마이그레이션서비스

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

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 (온-프레미스)

일부시스템요구사항이변경되었습니다. 자세한내용은 시스템요구사항및호환성과 XenMobile 호환성을참조하십시오.

1. 최신버전의 XenMobile Server 10.11 로업데이트하기전에 Citrix License Server 를 11.15 이상으로업데이트하십시오.

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

> 참고:
>
> 미리보기에자체라이센스를사용하려는경우 XenMobile 10.11 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2019 년 4 월 9 일이라는점을숙지하십시오. Citrix 라이센스의 Customer Success Services 날짜는이날짜보다이후여야합니다.
>
> 날짜는라이센스서버의라이센스옆에서볼수있습니다. 최신버전의 XenMobile 을이전버전의라이센스서버환경에연결하면연결확인이실패하고라이센스서버를구성할수없게됩니다.

라이센스의날짜를갱신하려면 Citrix 포털에서최신라이센스파일을다운로드하고라이센스서버에파일을업로드하십시오. 자세한내용은 Customer Success Services를참조하십시오.

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

업그레이드하려면

XenMobile 10.10.x 또는 10.9.x 에서 XenMobile 10.11 로직접업그레이드할수있습니다. 업그레이드를수행하려면사용가능한최신이진파일을다운로드합니다. https://www.citrix.com/downloads로이동하십시오. **Citrix Endpoint Management(**및 **Citrix XenMobile Server) > XenMobile Server(**온-프레미스**) >** 제품소프트웨어 **> XenMobile Server 10** 으로이동합니다. 해당하는하이퍼바이저에대한 XenMobile Server 소프트웨어타일에서 파일다운로드를클릭합니다.

업그레이드를업로드하려면 XenMobile 콘솔의 릴리스관리페이지를사용합니다. 자세한내용은 릴리스관리페이지를사용하여업그레이드하려면을참조하십시오.

업그레이드후

XenMobile 10.11 으로업그레이드한후 (온-프레미스):

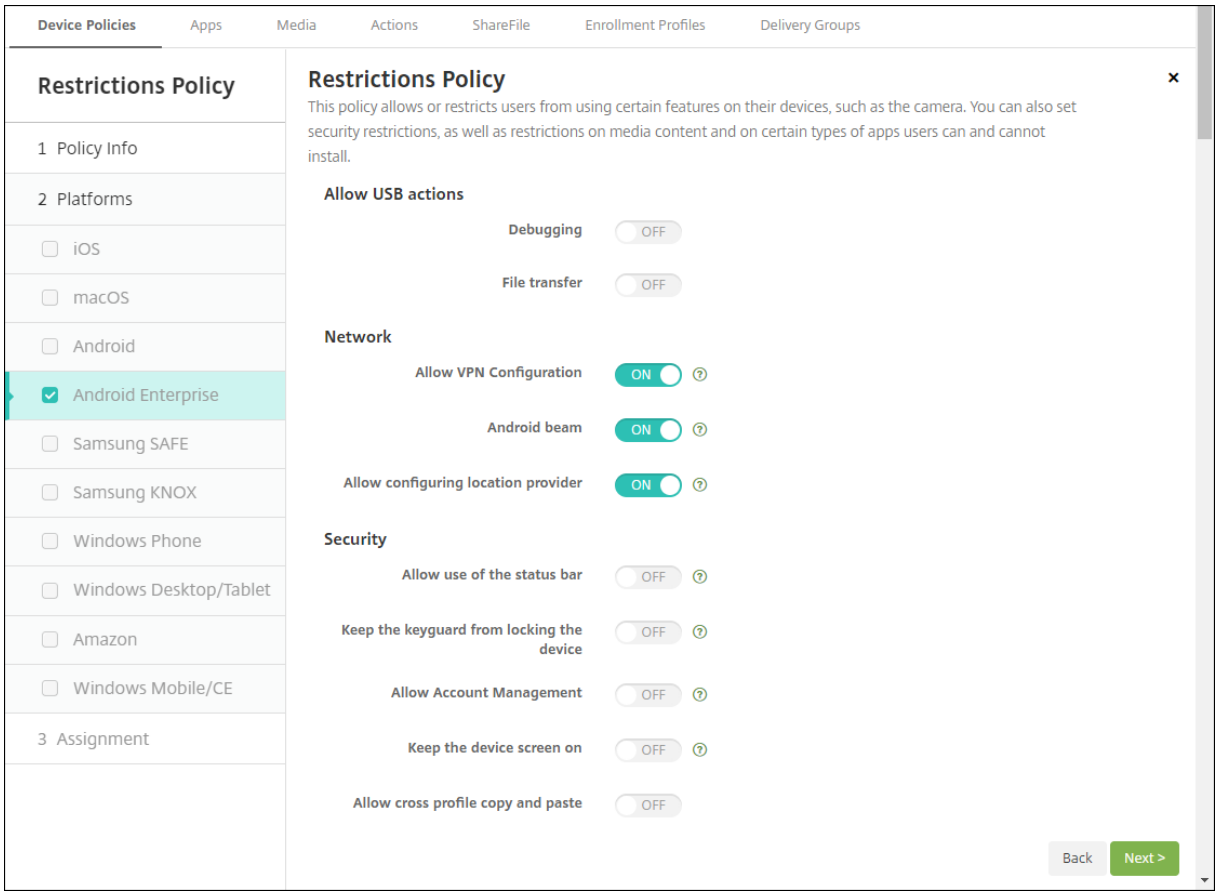
연결구성을변경하지않았는데도발신연결이관련된기능이작동을중지하는경우 XenMobile Server 로그에다음과같은오류가있는지확인하십시오. “VPP Server 에연결할수없습니다. 호스트이름 ‘192.0.2.0’ 이피어가제공한인증서제목과일치하지않습니다.”

이인증서유효성검사오류는 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 라이센스키를구성합니다.
- 제한장치정책설정**.**

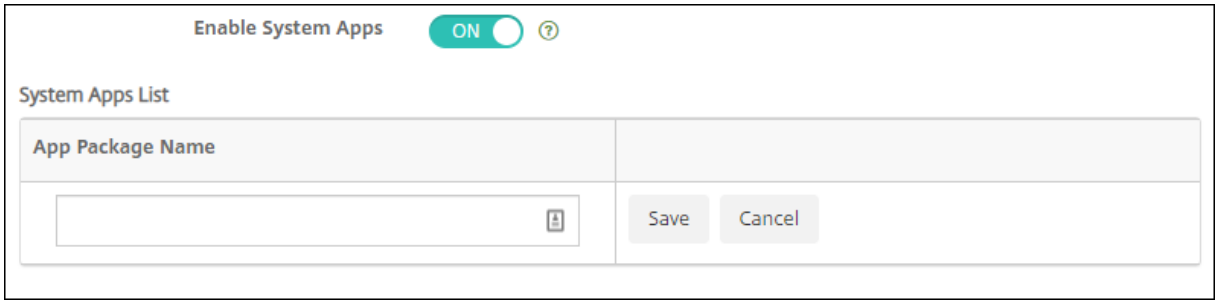


Android Enterprise 의앱인벤토리장치정책**.** 이제관리되는장치에서 Android Enterprise 앱의인벤토리를수집할수있습니다. 앱인벤토리장치정책을참조하십시오.

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 앱이허용됩니다. 이후관리자는 제한장치정책을사용하여이러한앱에대한액세스를제어할수있습니다.

Android Enterprise 장치에서시스템앱사용**.** Android Enterprise 작업프로필모드또는완전관리형모드에서사용자가앱에미리설치된시스템앱을실행할수있도록하려면 제한장치정책을구성합니다. 이구성은카메라, 갤러리및기타기본장치앱에대한액세스권한을사용자에게부여합니다. 특정앱에대한액세스를제한하려면 Android Enterprise 앱권한장치정책을사용하여앱권한

을설정합니다.



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

전용 Android Enterprise 장치는단일사용사례를이행하는데전용으로사용되는완전관리형장치입니다. 이러한장치는이사용사례에필요한작업을수행하는데필요한단일앱또는소수의앱으로제한되어야합니다. 또한사용자가장치에서다른앱을사용하도록설정하거나다른작업을수행하지못하도록차단해야합니다.

Android Enterprise 장치프로비저닝에대한자세한내용은 전용 Android Enterprise 장치프로비저닝을참조하십시오.

정책이름변경**.** Google 용어에맞추기위해 Android Enterprise 앱제한장치정책의이름이이제관리되는구성장치정책으로변경되었습니다. 관리되는구성장치정책의내용을참조하십시오.

Android Enterprise 의잠금및암호재설정

XenMobile 은이제 Android Enterprise 장치에대한잠금및암호재설정보안동작을지원합니다. 이러한장치는 Android 8.0 이상을실행하는작업프로필모드에등록되어야합니다.

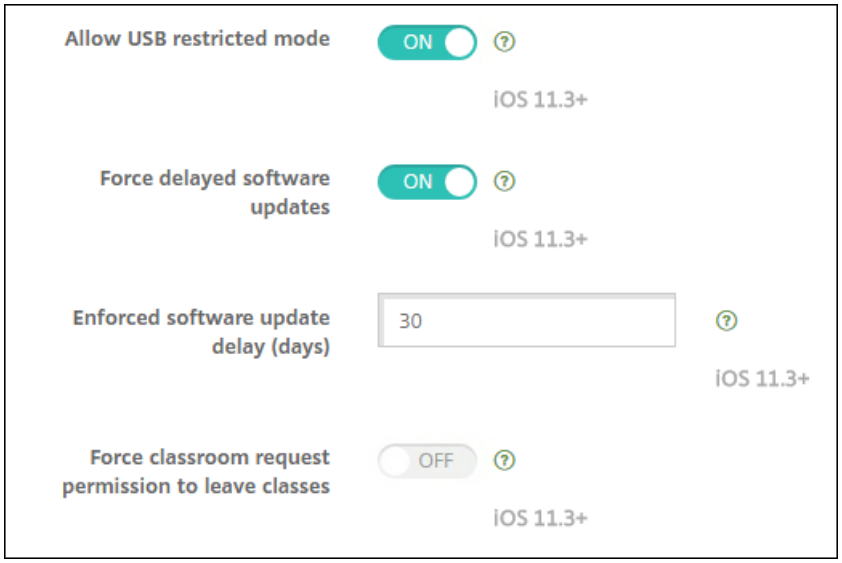
- 전송된암호로작업프로필이잠깁니다. 장치는잠기지않습니다.
- 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않는경우:
  - 작업프로필에암호가이미설정되어있지않으면장치가잠깁니다.
  - 작업프로필에암호가이미설정되어있으면작업프로필은잠기지만장치는잠기지않습니다.

잠금및암호재설정보안동작에대한자세한내용은 보안동작을참조하십시오.

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.



제한장치정책을참조하십시오.

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**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 서명을켜거나끌수있습니다. 기본값은 꺼짐입니다.
- **S/MIME** 서명인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서사용할서명자격증명을선택할수있습니다. 기본값은 꺼짐입니다.

S/MIME 암호화의경우:

- 암호화 **ID** 자격증명**:** 사용할암호화자격증명을선택합니다.
- 메시지별 **S/MIME** 전환사용**:** 켜짐으로설정하면작성하는각메시지에대해 S/MIME 암호화를켜거나끌수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
- 기본적으로 **S/MIME** 암호화사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 를기본적으로켤지여부를선택할수있습니다. 기본값은 꺼짐입니다.
- **S/MIME** 암호화인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나끌수있습니다. 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 장치정책을참조하십시오.

iOS 용메일장치정책업데이트

iOS 12 이상의추가 **S/MIME Exchange** 서명및암호화설정**.** 메일장치정책에 S/MIME 서명및암호화를구성하는추가설정이포함됩니다.

S/MIME 서명의경우:

- **S/MIME** 서명사용**:** 이계정이 S/MIME 서명을지원하는지여부를선택합니다. 기본값은 켜짐입니다. 켜짐으로설정하면다음필드가나타납니다.
  - **S/MIME** 서명사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 서명을켜거나끌수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
  - **S/MIME** 서명인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서사용할서명자격증명을선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.

S/MIME 암호화의경우:

- **S/MIME** 암호화사용**:** 이계정이 S/MIME 암호화를지원하는지여부를선택합니다. 기본값은 꺼짐입니다. 켜짐으로설정하면다음필드가나타납니다.
  - 메시지별 **S/MIME** 전환사용**:** 켜짐으로설정하면작성하는각메시지에대해 S/MIME 암호화를켜거나끌수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
  - 기본적으로 **S/MIME** 암호화사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 를기본적으로켤지여부를선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
  - **S/MIME** 암호화인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나끌수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.

메일장치정책을참조하십시오.

iOS 용앱알림장치정책업데이트

다음앱알림설정은 iOS 12 부터사용할수있습니다.

- **CarPlay** 로표시**:** 켜짐인경우 Apple CarPlay 에알림이표시됩니다. 기본값은 켜짐입니다.
- 중요알림사용**:** 켜짐인경우앱이방해금지및벨소리설정을무시하는중요알림으로알림을표시할수있습니다. 기본값은 꺼짐입니다.

앱알림장치정책을참조하십시오.

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 구성을참조하십시오.

RBAC(역할기반액세스제어) 권한변경

로컬사용자추가/삭제 RBAC 권한이로컬사용자추가와로컬사용자삭제의두가지권한으로분할되었습니다.

자세한내용은 RBAC 를사용하여역할구성을참조하십시오.

타사고지사항

January 5, 2022

XenMobile 의이릴리스에는다음문서에정의된약관에따라사용이허가된타사소프트웨어가포함될수있습니다.

XenMobile 타사고지사항

사용중단

August 24, 2022

이문서의발표내용은단계적으로중단되는 XenMobile Server 기능에대한사전알림을제공하기위한것입니다. 회사에서적시에의사결정을내릴수있도록돕기위해이정보를제공합니다. Citrix 는고객의사용및피드백을모니터링하여이러한중단시기를결정합니다. 발표내용은후속릴리스에서변경될수있으며사용되지않는모든기능이발표에포함되지않을수있습니다. 제품수명주기지원에대한자세한내용은 제품수명주기지원정책 문서를참조하십시오.

지원중단및제거

다음목록에는사용되지않거나제거된 XenMobile Server 기능이나와있습니다.

사용되지않는항목은즉시제거되지않습니다. Citrix 는사용되지않는항목이향후릴리스에서제거되기전까지이러한항목에대한지원을계속합니다.

제거된항목은 XenMobile Server 에서제거되거나더이상지원되지않습니다.

수명종료에도달한모바일생산성앱에대한자세한내용은 EOL 및사용되지않는앱을참조하십시오.

항목	설명	사용중단발표	제거됨	대체
Windows Information Protection(WIP)	Microsoft 의발표 (여기) 에따라 Windows Information Protection 은더이상지원되지않습니다.	August 2022	목표: 2022 년 10 월	대체없음
PKI ID: 일반, Symantec PKI, DigiCert, Entrust 어댑터	일반, DigiCert 관리형및 Entrust 어댑터 PKI 엔터티는더이상지원되지않습니다.	June 2021	January 2022	대체없음
등록초대설정	장치 IMEI, 일련번호및 UDID 를사용하여등록초대를만드는지원은더이상사용되지않습니다.	January 2022	May 2022	등록초대를만들때 XenMobile 콘솔의 관리 > 등록초대에서사용가능한설정을구성합니다.
이동통신사업자 SMS 게이트웨이	Nexmo SMS 게이트웨이알림에대한지원이중단됨	January 2022	April 2022	SMTP 서버알림 사용

항목	설명	사용중단발표	제거됨	대체
모바일서비스공급자 (MSP)	BlackBerry 및기타 Exchange ActiveSync 장치를 쿼리하고작업을실행하는 MSP 인터페이스에대한지원이중단됨	January 2022	April 2022	대체없음
Samsung 키오스크 모드	장치관리자 (DA) 모드에기반한레거시 Samsung 키오스크 모드의지원을중단합니다.	January 2022	March 2022	Android Enterprise(AE) 키오스크모드를사용합니다.
Windows 장치에대한 Wi-Fi 감지핫스팟 자동연결제한을허용합니다.	Windows 10 장치에대한 Wi-Fi 감지핫스팟자동연결제한허용지원을제거합니다. Windows 10 은더이상이기능을지원하지않습니다. 자세한내용은 Microsoft 설명서를참조하십시오.	October 2021	February 2022	대체없음
Samsung SAFE/Samsung Knox 플랫폼	SAFE 및 Knox API 의지원을중단합니다.	January 2022	March 2022	Android Enterprise 로 Knox 정책을설정하려면관리형앱구성정책을통해 Knox 서비스플러그인을사용합니다.
높은보안등록모드	높은보안등록보안모드를사용한등록초대생성은더이상지원되지않습니다.	July 2021	February 2022	지원되는등록보안모드목록은 장치등록을 참조하십시오.

항목	설명	사용중단발표	제거됨	대체
RBAC 역할 - 공유장치등록자및 COSU 장치등록자	공유장치등록자와 COSU 장치등록자모두에미리정의된역할기반액세스제어설정의지원을중단합니다.	July 2021	December 2021	지원되는등록방법을 통해 iOS 장치를구성합니다. 등록프로필을통해 Android COSU (전용) 장치를구성합니다.
Knox Mobile Enrollment(레거시 DA)	모든 Android 버전에서레거시장치관리자모드인 KME(Knox Mobile Enrollment) 에대한지원이사용되지않습니다.	May 2021	June 2021	KME 를사용하여 Android Enterprise 모드로등록합니다. Android 9, 10, 11 은 Android Enterprise 를지원합니다.
Android 7.x 및 iOS 12.x 용 Citrix 모바일앱및 Workspace 앱	Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱의 Android 7.x 및 iOS 12.x 버전에대한지원이중단되었습니다.	2021 년 4 월	June 2021	최소한각주요운영체제플랫폼의현재및이전버전을사용합니다. 이전장치는등록된상태로유지됩니다. 그러나 Citrix 는레거시장치를테스트하거나지원하지않습니다.
파생된자격증명	파생된자격증명및 Citrix Derived Credential Manager 앱에대한지원이중단되었습니다.	March 2021	December 2021	iOS 에서지원되는인증유형목록은 iOS를 참조하십시오.
Internet Explorer 11	XenMobile Server 콘솔에서는 Internet Explorer 사용이더이상지원되지않습니다.	January 2021	January 2021	Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari 중하나의최신버전을사용하십시오.

항목	설명	사용중단발표	제거됨	대체
Android 용 RSA 소프트웨어토큰지원	Android 용 Secure Hub 에 RSA 소프트웨어토큰 직접가져오기는더이상지원되지않습니다.	January 2021	February 2021	Google Play 에서 제공되는 RSA 보안 ID 앱내부에서 RSA 소프트웨어토큰을가져올수있습니다. 그런다음 Citrix Gateway 인증에토큰을사용할수있습니다.
Android - Sony	Android Sony 장치및 Sony 관련정책에대한지원은중단되었습니다.	January 2021	February 2022	Android Enterprise 사용
Android - HTC	Android HTC 장치및 HTC 관련정책에 대한지원은중단되었습니다.	January 2021	February 2022	Android Enterprise 사용
XenMobile 대시보드의타사구성요소	XenMobile 대시보드의일부로사용되는타사구성요소는사용중단될예정입니다.	December 2020	January 2021	대시보드를계속사용하려면 XenMobile 10.12 이상으로업그레이드하십시오.
Android Enterprise 장치에서레거시장치관리자모드에대해게시된앱	Android Enterprise 에등록된장치에레거시 DA 플랫폼용으로게시된앱은더이상제공되지않습니다.	October 2020	November 2020	Android Enterprise 장치의 경우 Android Enterprise 플랫폼용으로앱을게시합니다. DA 모드인장치에레거시 DA 앱을계속게시하려면이러한앱에대해별도의배달그룹을만듭니다.

항목	설명	사용중단발표	제거됨	대체
APNs 송신포트	APN 레거시바이너리 프로토콜에대한 Apple 의지원은 2021 년 3 월 31 일부로종료됩니다. Apple 에서는 HTTP/2 기반 APN 제공업체 API 를대신 사용하도록권장합니다. 이변경의일환으로 APN 알림을 `*.push.apple.com`에보내는데사용되는포트 2195 및 2196 이더이상지원되지않습니다.	October 2020	March 2021	대신포트 443 또는 2197 을사용하십시오. 장치관리를위한 XenMobile 포트열기를참조하십시오.
Samsung SEAMS 컨테이너	Samsung SEAMS 컨테이너에대한지원이중단되었습니다.	June 2020	August 2020	Android Enterprise 용 Samsung Knox 서비스플러그인 (KSP) 앱을사용합니다. Knox 서비스플러그인앱추가를참조하십시오.
자체서명된 SSL(Secure Sockets Layer) 인증서	모든장치플랫폼에서 자체서명된 SSL 인증서지원이사용중단되었습니다.	May 2020		이 SSL 인증서를잘알려진 CA(인증기관) 의신뢰할수있는 SSL 인증서로교체합니다.

항목	설명	사용중단발표	제거됨	대체
인증서기반인증서명 알고리즘 (비 FIPS 및약한암호화)	다음서명알고리즘에 대한지원이사용중단 되었습니다. SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA SHA1withDSA, RIPEMD160withRS RIPEMD128withRS RIPEMD256withRS	May 2020	June 2021	XenMobile 콘솔에서 자격증명공급자의 CSR 을만들때 (설정 **>** 자격증명공급자 **>** 인증서서명요청 **(CSR)**) 더강력한암호화를선택합니다.
데이터베이스서버	Microsoft SQL Server 2014 이하에대한지원이중단됩니다.	October 2021	August 2022	지원되는다음버전중하나로시스템을업데이트하십시오. Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 또는 Microsoft SQL Server 2019 CTP 3.2. 시스템요구사항및호환성에서 지원되는서버목록을 참조하십시오.

항목	설명	사용중단발표	제거됨	대체
하이퍼바이저	Citrix XenServer 6.5.x 이전버전과 VMware ESXi 5.5 업데이트 3 이전버전, Hyper-V 2012 에대한지원이중단되었습니다.	May 2020	August 2020	지원되는다음버전중하나로시스템을업데이트하십시오. Citrix Hypervisor 8.0 이상, Citrix XenServer 7.0 이상, VMware (ESXi 6.0, ESXi 6.5.0 업데이트 3, ESXi 6.7 업데이트 2 패치 10 또는 ESXi 7.0) 또는 Hyper-V (Windows Server 2016 또는 Windows Server 2019).
Citrix Launcher	Citrix Launcher 앱에대한지원이중단되었습니다.	May 2020	August 2020 (앱스토어에서제거)	장치를키오스크 (전용장치) 로프로비저닝합니다. 자세한내용은 Citrix Launcher 대체를참조하십시오.
Android 6.x 및 iOS 11.x 용 Citrix 모바일앱및 Workspace 앱	Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱의 Android 6.x 및 iOS 11.x 버전에대한지원이중단되었습니다.	April 2020	June 2020	최소한각주요운영체제플랫폼의현재및이전버전을사용합니다.

항목	설명	사용중단발표	제거됨	대체
MDX Toolkit 및 MDX Service	MAM(모바일애플리케이션관리) SDK 를 위해 MDX Toolkit 및 MDX Service 에 대한지원이중단되었습니다. 전환기간동안 MDX 래핑앱과 MAM SDK 개발앱을 모두사용할수있습니다.	March 2020	Target: July 2022	엔터프라이즈응용프로그램을계속관리하려면 MAM SDK 를 사용합니다.
MDX: 대체게이트웨이서버	iOS 및 Android 장치에대한상위단계인증이사용되지않습니다.	March 2020	September 2021	대체없음
MDX: Micro VPN(전체터널모드)	iOS 및 Android 장치에대한전체 VPN(가상사설망) 터널이사용되지않습니다.	March 2020	September 2021	MAM SDK 웹 SSO 모드를사용하거나 Citrix SSO 연결유형을사용하여앱별 VPN 정책을만듭니다.
MDX: PAC 파일지원	iOS 및 Android 장치에대한전체 VPN 터널배포에사용되는 PAC(Proxy Automatic Configuration) 파일이더이상지원되지않습니다.	March 2020	September 2021	프록시서버연결을통해내부네트워크에액세스하려면 Citrix Gateway 를사용합니다.

항목	설명	사용중단발표	제거됨	대체
MDX 공유장치지원	MDX 앱에대한공유장치지원이중단되었습니다.	March 2020	September 2021	Android Enterprise 의경우 MDM 에대한공유장치지원을사용합니다. iOS 의경우 Apple School Manager 또는 GroundControl 을사용합니다.
Android 10 의신규장치관리자등록	Android 10 장치에서레거시장치관리자모드에대한신규등록또는재등록지원이중단되었습니다. 이미등록된장치는계속작동합니다.	February 2020	September 2020	Android 10 이상인신규장치를 Android Enterprise 에등록합니다.
Android 10 장치의레거시장치관리자모드	Google 에서일부 Device Administrator API 의사용을중단했습니다. Citrix 는 Citrix Secure Hub 를대상 Android API 수준 29 로업그레이드한이후로장치관리자모드에등록된 Android 10 장치를지원하지않습니다.	February 2020	November 2020	Android 10 장치를 Android Enterprise 로마이그레이션합니다.

항목	설명	사용중단발표	제거됨	대체
MDX 암호화	XenMobile 콘솔에서 MDX 암호화및 MDX 암호화기능이 사용되지않습니다.	October 2019	September 2020	규정준수확인이추가된암호화관리기능을 사용하여 iOS 또는 Android 플랫폼암호화를사용하도록설정합니다. 2020 년 7 월까지 MDX 암호화마이그레이션을테스트하고계획해야합니다.
암호장치정책: Android Enterprise 에대한 제한없음설정	Android 7 이상을 실행하는 Android Enterprise 장치에서문자제한이있는암호생성만지원됩니다. 이전에 필수문자를 제한없음으로설정한경우이번업데이트이후 해당값은 숫자만으로 변경됩니다.	February 2019	April 2019	이변경사항은현재사용자로그인환경에영향을주지않습니다.
원격지원	클러스터링된온-프레미스 XenMobile Server 배포에대한 원격지원클라이언트가더이상지원되지않습니다.	January 2019	August 2020	대체없음
iOS 용 Secure Hub 네트워크확장	Secure Hub release 20.3.0 이후로 iOS 장치의네트워킹기능사용자지정을허용하는네트워크확장프레임워크가사용되지않습니다.	October 2018	March 2020	대체없음

항목	설명	사용중단발표	제거됨	대체
TLS 버전 1.0 및 1.1	XenMobile 의보안을개선하기위해 Citrix 는이제 TLS(전송계층보안) 1.0 및 1.1 을통한모든통신을차단합니다. PCI 보안표준위원회에서는보안약화를이유로 TLS 1.0 및 TLS 1.1 의사용을중단하고있습니다.	June 2018	March 2019	TLS 1.2 로업그레이드합니다.
Windows Mobile/CE	Windows Mobile/CE 장치가더이상지원되지않습니다.	April 2018	September 2020	Windows 10 데스크톱및랩톱을사용합니다.
Android TouchDown	DigiCert 는 Android TouchDown 지원을중단했습니다. Citrix 는 Exchange 장치정책에서 Android TouchDown 플랫폼페이지를삭제할예정입니다.	2018 년 7 월	2021	권장사항: Citrix Secure Mail 을사용하십시오.

수정된문제

May 6, 2022

XenMobile 10.14 에서는다음과같은문제가수정되었습니다.

- XMS 10.12 로업그레이드하면 XenMobile Server 콘솔의대시보드보기에문제가발생합니다. [CXM-88918]
- 일반 PKI 가구성된경우 Apple 장치에서 Apple 배포프로그램 (이전의 DEP) 등록이실패합니다. [CXM-89978]
- RBAC(역할기반액세스제어) 를사용하여로그인할때등록프로필을편집하려면추가권한이필요합니다. [CXM-89985]

- XenMobile Server 콘솔에서는 Chrome 앱에대한 관리되는구성정책을편집할수없습니다. [CXM-89986]
- iOS 플랫폼에서연결유형이 **AlwaysOn IKEv2** 이중구성인 VPN 정책을편집하면오류가발생합니다. [CXM-90010]
- **SamAccountName** 으로 Android Enterprise 장치를등록하는데실패하고 "작업프로필이삭제되었으며프로필을초기화합니다" 라는오류메시지가표시됩니다. [CXM-90049]
- 데이터베이스는소문자 "u" 로시작하는사용자이름을허용하지않습니다. [CXM-90722]
- XenMobile Server 콘솔에 SIM 카드가삽입되지않은장치의 ICCID(집적회로카드 ID) 가표시됩니다. [CXM-90845]
- iOS 14 를실행하는장치에서 Apple DEP(장치등록프로그램) 등록이실패합니다. [CXM-91697]
- XenMobile Server 콘솔에올바른루트인증서만료날짜가표시되지않습니다. [CXM-91961]
- XenMobile Server 에서 NetScaler Gateway 연결확인에결과가표시되지않습니다. [CXM-93129]
- XenMobile Server 콘솔에 SNMP 사용자를추가하면 *SNMP* 모니터링사용자목록에사용자가나타나지않거나 SNMP 에이전트가비활성화됩니다. [CXM-93197]
- 제한장치정책에서동일한앱에대해 시스템앱활성화및 애플리케이션비활성화설정을모두활성화하면앱이여전히작업프로필에나타납니다. [CXM-93671]
- APN 용 HTTP/2 기반 API 로전환하면 `ios.mdm.apns.connectionPoolSize` 서버속성이숨겨집니다. [CXM-95478]
- XenMobile Server 버전 10.12 에서는특정앱의 VPP 속성을수정할수없습니다. [CXM-96796]
- 앱자동업데이트설정이비활성화되면기기에설치된 Apple 볼륨구매앱이최신버전으로자동업데이트됩니다. [CXM-96855]
- XenMobile Server 버전 10.13 에서는 **CLI** 아래에서프록시서버를구성할때 iOS 장치에서실행중인 Secure Hub 로알림을보낼수없습니다. [CXM-97609]
- XenMobile Server 버전 10.13 에서 장치세부정보에액세스하는동안오류가발생합니다. 이오류는장치속성에 **"**"의값이있는경우발생합니다. [CXM-97952]
- 버전 10.13.0 롤링패치릴리스의수정된문제는다음을참조하십시오.
  - XenMobile Server 10.13 롤링패치 8 에대한릴리스정보
  - XenMobile Server 10.13 롤링패치 7 에대한릴리스정보
  - XenMobile Server 10.13 롤링패치 6 에대한릴리스정보

관련정보

XenMobile Support Knowledge Center

알려진문제

May 6, 2022

XenMobile 10.14 에는다음과같은알려진문제가있습니다.

- XenMobile Server 10.8 또는 10.9 이미지를 VMware ESXi 6.7 또는 6.5 업데이트 2 로가져온후: VM 을다시시작하면구성앱이시작되지않고 XenMobile Server 가복구모드로전환되고 IP 설정이지워집니다. 이문제를해결하려면새 VM 을 VMXNET3 NIC 로작성한다음해당 VM 을복구모드로전환된 VM 의데이터베이스에통합하십시오. [CXM-54581]
- iOS 15 또는 macOS 12 장치를등록한후 MDM 구성프로필에 '확인되지않음' 으로표시됩니다. [CXM-98525]
- Android 12 로업그레이드하면작업프로필모드로재등록된장치가장치관리테이블에두번나타납니다. [CXM-99712]
- Android 12 를실행하는 MDM 등록장치에 locate 명령을전송하면 Secure Hub 를시작할때영구적으로로드되는흰색화면이나타납니다. [CXM-99878]
- 모바일생산성앱과관련된알려진문제에대해서는 Secure Hub, Secure Mail 및 Secure Web을참조하십시오.
- 최신버전 10.13.0 롤링패치릴리스의알려진문제는다음을참조하십시오.
  - XenMobile Server 10.13 롤링패치 8 에대한릴리스정보

관련정보

XenMobile Support Knowledge Center

아키텍처

January 5, 2022

조직의장치및앱관리요구사항에따라 XenMobile 아키텍처의 XenMobile 구성요소가결정됩니다. XenMobile 의구성요소는모듈식이며상호기반하여구축됩니다. 예를들어, 배포에는 Citrix Gateway 가포함됩니다.

- Citrix Gateway 를통해사용자는모바일앱에원격으로액세스하고사용자장치유형을추적할수있습니다.
- XenMobile 에서는이러한앱과장치를관리할수있습니다.

XenMobile 구성요소배포: XenMobile 을배포하여사용자가다음과같은방법으로내부네트워크의리소스에연결하도록할수있습니다.

- 내부네트워크로의연결. 원격사용자의경우 Citrix Gateway 를통해 VPN 또는 Micro VPN 연결을사용하여연결할수있습니다. 이연결은내부네트워크의앱및데스크톱에대한액세스를제공합니다.
- 장치등록. 사용자가 XenMobile 에서모바일장치를등록할수있으므로네트워크리소스에연결하는장치를 XenMobile 콘솔에서관리할수있습니다.

- 웹, SaaS 및모바일앱. 사용자는 XenMobile 에서 Secure Hub 를통해웹, SaaS 및모바일앱에액세스할수있습니다.
- Windows 기반앱및가상데스크톱. 사용자는 Citrix Receiver 또는웹브라우저에연결하여 StoreFront 또는 Web Interface 에서 Windows 기반앱및가상데스크톱에액세스할수있습니다.

온-프레미스 XenMobile Server 에대해이러한기능을수행하려면 XenMobile 구성요소를다음순서로배포하는것이좋습니다.

- Citrix Gateway. Quick Configuration(빠른구성) 마법사를통해 Citrix Gateway 의설정을구성하여 XenMobile, StoreFront 또는 Web Interface 와의통신을설정할수있습니다. Citrix Gateway 에서 Quick Configuration(빠른구성) 마법사를사용하기전에 XenMobile, StoreFront 또는 Web Interface 중하나를설치하여통신을설정해야합니다.
- XenMobile. XenMobile 을설치한후 XenMobile 콘솔에서사용자의모바일장치등록을허용하는정책및설정을구성할수있습니다. 또한모바일, 웹및 SaaS 앱을구성할수있습니다. 모바일앱에는 Apple App Store 또는 Google Play 앱이포함될수있습니다. 또한사용자는 MDX Toolkit 을사용하여래핑되고콘솔에업로드된모바일앱에연결할수있습니다.
- MAM SDK 또는 MDX Toolkit. MDX 래핑기술은 2022 년 3 월에 EOL(수명종료) 에도달할예정입니다. 엔터프라이즈애플리케이션을계속관리하면 MAM SDK 를통합해야합니다.

  MAM(모바일응용프로그램관리) SDK 는 iOS 및 Android 플랫폼에서제공되지않는 MDX 기능을제공합니다. iOS 또는 Android 앱을보호하고 MDX 를사용설정할수있습니다. 내부스토어또는공개앱스토어를통해이러한앱을제공합니다. MDX 앱 SDK를참조하십시오.
- StoreFront(선택사항). Receiver 연결을통해 StoreFront 의 Windows 기반앱및가상데스크톱에대한액세스를제공할수있습니다.
- Citrix Files(선택사항). Citrix Files 를배포하는경우 XenMobile 을통해엔터프라이즈디렉터리를통합하여 SAML(Security Assertion Markup Language) ID 공급자로사용할수있습니다. Citrix Content Collaboration 의 ID 공급자구성에대한자세한내용은 Content Collaboration 지원사이트를참조하십시오.

XenMobile 은 XenMobile 콘솔을통해장치관리및앱관리를제공합니다. 이섹션에서는 XenMobile 배포의참조아키텍처를설명합니다.

프로덕션환경에서는확장성및서버중복성을위해 XenMobile 솔루션을클러스터구성으로배포하는것이좋습니다. 또한 Citrix ADC SSL 오프로드기능을사용하면 XenMobile Server 의부하가줄고처리량이늘어납니다. Citrix ADC 에부하분산을위한가상 IP 주소 2 개를구성하여 XenMobile 클러스터를설정하는방법에대한자세한내용은 클러스터링을참조하십시오.

재해복구배포용으로 XenMobile 을구성하는방법에대한자세한내용은배포안내서의 재해복구 문서를참조하십시오. 이문서에는아키텍처다이어그램이포함되어있습니다.

다음섹션에서는 XenMobile 배포의다양한참조아키텍처를설명합니다. 참조아키텍처다이어그램은 XenMobile 배포안내서문서인 온-프레미스배포용참조아키텍처 및 아키텍처를참조하십시오. 전체포트목록은 포트요구사항(온-프레미스) 및 포트요구사항(클라우드) 을참조하십시오.

MDM(모바일기기관리) 모드

> 중요:
>
> MDM 모드를구성하고나중에 ENT 모드로변경하는경우동일한인증 (Active Directory) 을사용해야합니다. XenMobile 은사용자등록후의인증모드변경을지원하지않습니다. 자세한내용은 XenMobile MDM Edition 에서 Enterprise Edition 으로업그레이드를참조하십시오.

XenMobile MDM Edition 은모바일기기관리를제공합니다. 플랫폼지원은 지원되는장치운영체제를참조하십시오. XenMobile 의 MDM 기능만사용하려는경우 XenMobile 을 MDM 모드로배포합니다. 예를들어다음을수행할수있습니다.

- 장치정책및앱배포
- 자산인벤토리검색
- 장치에서장치초기화와같은동작수행

권장모델에서 XenMobile Server 는 DMZ 에배치되며 XenMobile 의보호를개선하는 Citrix ADC 를선택적으로그앞에배포할수있습니다.

MAM(모바일앱관리) 모드

MAM 또는 MAM 전용모드는모바일앱관리를제공합니다. 플랫폼지원은 지원되는장치운영체제를참조하십시오. XenMobile 의 MAM 기능만사용하고 MDM 에장치를등록하지않으려는경우 XenMobile 을 MAM 모드로배포합니다. 예를들어다음을수행할수있습니다.

- BYO 모바일장치의앱및데이터보안
- 엔터프라이즈모바일앱제공
- 앱잠금및데이터초기화

장치를 MDM 에등록할수없습니다.

이배포모델에서 XenMobile Server 는 XenMobile 의보호를개선하는 Citrix Gateway 다음에배치됩니다.

MDM+MAM 모드

MDM 과 MAM 모드를함께사용하면모바일앱및데이터관리기능과모바일기기관리기능을사용할수있습니다. 플랫폼지원은 지원되는장치운영체제를참조하십시오. 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 Citrix 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

June 17, 2022

> 참고:
>
> 이문서에서는 XenMobile Server 10.14 의시스템요구사항및호환성에대해다룹니다. Endpoint Management 의 시스템요구사항에대해서는 시스템요구사항을참조하십시오.

추가요구사항및호환성정보는다음문서를참조하십시오.

- XenMobile 호환성
- 지원되는장치운영체제
- 포트요구사항
- 확장성
- 라이센싱
- FIPS 140-2 준수
- 언어지원

XenMobile 10.14 를실행하려면다음과같은최소시스템요구사항이필요합니다.

- 다음중하나:
  - Citrix Hypervisor 8.1 또는 8.0 또는 Citrix XenServer(지원되는버전: 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2), 자세한내용은 XenServer를참조하십시오. Citrix Hypervisor 버전 8.2 CU1 이상은지원되지않습니다.
  - VMware(지원되는버전: ESXi 6.0, ESXi 6.5.0 Update 3 또는 ESXi 6.7 Update 2 패치 10, ESXi 7.0 Update 2a), 자세한내용은ESXi 6.7 해결방법 및 VMware를참조하십시오.
  - Hyper-V(지원되는버전: Windows Server 2016 및 Windows Server 2019), 자세한내용은 Hyper-V를 참조하십시오.
- Exchange ActiveSync 10.1.10 용 Endpoint Management 커넥터또는 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 11.16.

  XenMobile Server 를업그레이드하기전에라이센스서버를업데이트하십시오.

ESXi 6.7 해결방법

ESXi 6.7 이작동하려면다음해결방법을수행해야합니다.

1. VMware 에서제공하는 OVF 도구를사용하여 citrix.com 에서다운로드한 OVA 파일을추출합니다. VMware 페이지 (https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491) 에서 OVF 도구를얻습니다.
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. 저장을클릭합니다.
9. VM 의전원을켭니다.

Citrix Gateway 시스템요구사항

XenMobile 10.14 와함께 Citrix Gateway 를실행하려면다음과같은최소시스템요구사항이필요합니다.

- Citrix Gateway(온프레미스). 지원되는버전: 12.1 이상
- 또한 Active Directory 와통신하기위한서비스계정이있어야합니다. 쿼리및읽기권한만있으면됩니다.

XenMobile 10.14 데이터베이스요구사항

XenMobile 에는다음데이터베이스중하나가필요합니다.

- Microsoft SQL Server

  XenMobile 은지원되는다음버전중하나를실행하는 Microsoft SQL Server 데이터베이스를지원합니다. SQL Server 데이터베이스및해당하드웨어요구사항에대한자세한내용은 Microsoft 설명서를참조하십시오.

  - Microsoft SQL Server 2014 SP3
  - Microsoft SQL Server 2016 SP2
  - Microsoft SQL Server 2017 CU 25
  - Microsoft SQL Server 2019 CU 12

  Microsoft SQL Server 데이터베이스요구사항은배포크기에따라다릅니다. 배포규모에따른 Microsoft SQL Server 데이터베이스요구사항에대한자세한내용은 확장성을참조하십시오.

  XenMobile 은데이터베이스고가용성을위한 SQL Basic 가용성그룹 (Always On 가용성그룹) 및 SQL 클러스터링을지원합니다.

  Microsoft SQL 은원격으로사용하는것이좋습니다.

  Microsoft SQL 업그레이드에대한자세한내용은 Microsoft 문서 SQL Server 업그레이드를참조하십시오.

- PostgreSQL(테스트환경전용). PostgreSQL 은 XenMobile 에포함되어있으며테스트환경에서로컬또는원격으로사용할수있습니다. 데이터베이스마이그레이션은지원되지않습니다. 테스트환경에서만든데이터베이스를프로덕션환경으로이동할수없습니다.

  모든 XenMobile 버전은 Windows 용원격 PostgreSQL 9.5.1 및 9.5.11 을지원할때다음과같은제한사항이있으므로프로덕션환경에는권장되지않습니다. 최대 300 개장치지원장치개수가 300 개가넘을경우온-프레미스 SQL Server 사용클러스터링지원안함

SQL Server 서비스계정요구사항

XenMobile 에사용할 SQL Server 서비스계정에 `DBcreator` 역할권한이있는지확인합니다. XenMobile Server 설치중에지정하는 SQL Server 계정암호를기록합니다. XenMobile Server 복구중에 XenMobile 데이터베이스를복제해야하는경우이암호가필요합니다.

TDE(Transparent Data Encryption) 를사용하여 SQL Server 데이터베이스를보호합니다. 온-프레미스배포용참조아키텍처의참조아키텍처에표시된대로 SQL Server 포트에대한외부액세스를허용하지마십시오.

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

- 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
- Virtual Apps and Desktops 7 1909
- Virtual Apps and Desktops 7 2006

StoreFront 호환성

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

기타호환성

- Exchange ActiveSync 10.1.10 용 Endpoint Management 커넥터
  - 이전버전은테스트되지않았습니다.
- Exchange ActiveSync 8.5.3.19 용 Citrix Gateway 커넥터
  - 이전버전은테스트되지않았습니다.

XenMobile 호환성

March 24, 2022

> 참고**:**
>
> 이문서에서는 XenMobile Server 의호환성에대해다룹니다. Endpoint Management 에서테스트된구성요소에대해서는 Endpoint Management 호환성을참조하십시오.

새로운기능, 수정사항및정책업데이트를사용하려면 Citrix 권장사항에따라다음의최신버전을설치하는것이좋습니다.

- Citrix 에서는 Mobile Application Management(MAM) SDK 를엔터프라이즈 iOS 및 Android 앱과통합하여 MDX 기능을앱에적용하도록권장합니다.

  MDX Toolkit 은 2022 년 7 월에 EOL(수명종료) 에도달할예정입니다. 엔터프라이즈앱을계속관리하면 MAM SDK 를통합해야합니다.

이문서에서는통합이가능한지원되는 XenMobile 구성요소의버전을요약하여보여줍니다.

호환성및업그레이드경로

Secure Hub, MDX Toolkit 및모바일생산성앱의최신버전은 XenMobile Server 의현재및이전버전과호환됩니다.

최신버전의모바일생산성앱에는최신버전의 Secure Hub 가필요합니다. 이전두버전의앱은최신 Secure Hub 와호환됩니다. 자세한내용은 Citrix Product Matrix(Citrix 제품매트릭스)를참조하십시오.

Citrix 는공용앱스토어에서만 XenMobile 생산성앱의배포를지원합니다.

XenMobile Server(온-프레미스)

- 이전두버전의 XenMobile Server 에서업그레이드할수있습니다.
- 최신버전의 XenMobile Server: XenMobile Server 10.14
- 업그레이드원본:
  - XenMobile Server 10.13.x
  - XenMobile Server 10.12.x

모바일생산성앱

사용자는공용앱스토어에서모바일생산성앱에액세스할수있습니다. 최신버전의모바일생산성앱에는최신버전의 Secure Hub 가필요합니다. 이전두버전의앱은최신 Secure Hub 와호환됩니다.

릴리스케이던스가 2 주인모바일생산성앱에대한자세한정보는 릴리스타임라인을참조하십시오. 지원에대한자세한내용은 모바일생산성앱지원을참조하십시오.

MAM SDK

MAM SDK 는 iOS 및 Android 플랫폼에서제공되지않는 MDX 기능을제공합니다. 내부스토어또는공개앱스토어를통해이러한앱을제공합니다. MDX 앱 SDK를참조하십시오.

MDX Toolkit

MDX 래핑기술은 2022 년 7 월에 EOL(수명종료) 에도달할예정입니다. 엔터프라이즈응용프로그램을계속관리하려면 MAM SDK 를포함해야합니다.

Citrix 는 MDX Toolkit 의최신릴리스 3 개 (n.n.n) 를지원합니다. MDX Toolkit 의새로운기능을참조하십시오.

브라우저지원

XenMobile Server 콘솔에는지원되는다음웹브라우저중하나가필요합니다.

- Google Chrome 최신버전
- Mozilla Firefox 최신버전
- Microsoft Edge 최신버전
- Apple Safari 최신버전

지원되는장치운영체제

August 12, 2022

> 참고:
>
> 이문서에서는 XenMobile Server 10.13 에서지원되는장치운영체제에대해다룹니다. Endpoint Management 에 지원되는운영체제는 지원되는장치운영체제를참조하십시오.

XenMobile 은앱, 장치관리등엔터프라이즈모바일관리를위한다음플랫폼및운영체제를실행하는장치를지원합니다. 플랫폼제한 및보안기능으로인해 XenMobile 에서일부플랫폼의일부기능이지원되지않을수있습니다.

이문서에포함된지원되는장치플랫폼정보는 Exchange ActiveSync 용 Citrix Gateway 커넥터및 Exchange ActiveSync 용 XenMobile 커넥터에도적용됩니다.

모바일생산성앱의최신버전과 MDX 암호화가지원되는장치는 모바일생산성앱지원을참조하십시오.

> 참고:
>
> Citrix 는최소한각주요운영체제플랫폼의현재및이전버전을지원합니다. 최신 Endpoint Management 버전의일부기능은이전플랫폼릴리스에서작동하지않을수있습니다.
>
> 지원중단발표는 사용중지를참조하십시오.

운영체제지원목록

Citrix XenMobile 은다음운영체제를지원합니다.

- **Android:** 9.x, 10.x, 11.x, 12.x

  Android 10 이상에대해서는 Android 고려사항을참조하십시오.

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

  XenMobile 및 Citrix 모바일앱은 iOS 14.x 와호환되지만현재는모든새로운 iOS 14.x 기능을지원하지않습니다. iOS 14.x 용사내엔터프라이즈앱을래핑하려면 MDX Toolkit 21.8.5 이상을사용하거나 MAM SDK 를사용하여앱을준비합니다.

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

  XenMobile 및 Citrix 모바일앱은 iPadOS 14.x 와호환되지만현재는모든새로운 iPadOS 14.x 기능을지원하지않습니다.

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

  XenMobile 및 Citrix 모바일앱은 macOS 11 과호환되지만현재는모든새로운 macOS 11 기능을지원하지않습니다.

- **Windows** 데스크톱및태블릿**:** (MDM 에만해당). Windows 10 및 Windows 11

- **Samsung SAFE** 및 **Knox:** 호환되는 Samsung 장치에서 XenMobile 은 SAFE(Samsung for Enterprise) 및 Samsung Knox 정책을지원하고확장합니다. XenMobile 에서 SAFE 정책및제한을배포하려면먼저 SAFE API 를

사용하도록설정해야합니다. 이작업을수행하려면기본제공 Samsung ELM(Enterprise License Management) 키를장치에배포합니다. Samsung MDM 라이센스키장치정책을참조하십시오.

Android 고려사항

Android 10 이상으로업그레이드하기전에: Google Device Administration API 의지원중단이 Android 10 을실행하는 장치에미치는영향에대해서는 장치관리에서 Android Enterprise 로마이그레이션을참조하십시오.

- Citrix 에서는 Android 10 장치를레거시장치관리모드에서등록하지않을것을권장합니다. Google 에서는 Device Administration API 의지원을중단할예정이며, 이는 Android 10 이상을실행하는장치에영향을미칩니다. API 가지원중단되고나면레거시장치관리모드에서는 Android 10 이상인장치를등록할수없습니다. Citrix 는장치관리모드에서 Android 11 장치등록을지원하지않습니다.
- Citrix 에서는 Android 10 장치에 Android Enterprise 를사용할것을권장합니다. 자세한내용은 장치관리에서 Android Enterprise 로마이그레이션을참조하십시오.
- Google API 변경은 MAM 전용모드에서등록된장치에는영향을주지않습니다.

업그레이드전에:

- 서버인프라가 subjectAltName(SAN) 확장에일치하는호스트이름을가진보안인증서와호환되는지확인하십시오.
- 호스트이름을확인하려면서버가일치하는 SAN 이포함된인증서를제공해야합니다. Citrix 는호스트이름과일치하는 SAN 이포함된인증서만신뢰합니다.

포트요구사항

August 12, 2022

장치및앱에서 XenMobile 과통신할수있도록하려면방화벽에서특정포트를열어야합니다. 열어야하는포트가다음표에나열되어 있습니다.

Citrix Gateway 및 **XenMobile** 의앱관리를위한포트열기

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

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

Citrix ADC 에서 Launch Darkly 로의트래픽을활성화하려면이 Support Knowledge Center 문서에나와있는 IP 주소를사용할수있습니다.

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

TCP 포트	설명	원본	대상
21 또는 22	FTP 또는 SCP 서버로지원번들을보내는데사용됩니다.	XenMobile	FTP 또는 SCP 서버
53(TCP 및 UDP)	DNS 연결에사용됩니다.	Citrix Gateway, XenMobile	DNS 서버
80	Citrix Gateway 가두번째방화벽을통해 VPN 연결을내부네트워크리소스에전달합니다. 이상황은일반적으로사용자가 Citrix Gateway 플러그인으로로그온한경우발생합니다.	Citrix Gateway	인트라넷웹사이트
80 또는 8080, 443	열거, 티켓생성및인증에사용되는 XML 및 STA(Secure Ticket Authority) 포트입니다. 포트 443 을사용할것을권장합니다.	StoreFront 및 Web Interface XML 네트워크트래픽, Citrix Gateway STA	Virtual Apps 또는 Desktops
123(TCP 및 UDP)	NTP(Network Time Protocol) 서비스에사용됩니다.	Citrix Gateway, XenMobile	NTP 서버
389	보안되지않은 LDAP 연결에사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증서버또는 Microsoft Active Directory
443	Citrix Receiver 의 StoreFront 연결또는 Receiver for Web 의 Virtual Apps and Desktops 연결에사용됩니다.	인터넷	Citrix Gateway
443	웹, 모바일및 SaaS 앱제공을위해 XenMobile 에연결할때사용됩니다.	인터넷	Citrix Gateway

TCP 포트	설명	원본	대상
443	일반장치와 XenMobile Server 의통신에사용됩니다.	XenMobile	XenMobile
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	인증서인증을사용하지않는배포의콜백 URL 에사용됩니다.	XenMobile	Citrix Gateway
514	XenMobile 과 syslog 서버간의연결에사용됩니다.	XenMobile	Syslog 서버
636	보안 LDAP 연결에사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증서버또는 Active Directory
1494	내부네트워크의 Windows 기반응용프로그램에대한 ICA 연결에사용됩니다. 이포트는열어두는것이좋습니다.	Citrix Gateway	Virtual Apps 또는 Desktops
1812	RADIUS 연결에사용됩니다.	Citrix Gateway	RADIUS 인증서버
2598	세션안정성을사용한내부네트워크의 Windows 기반응용프로그램에대한연결에사용됩니다. 이포트는열어두는것이좋습니다.	Citrix Gateway	Virtual Apps 또는 Desktops

TCP 포트	설명	원본	대상
3268	Microsoft 글로벌카탈로그의보안되지않은 LDAP 연결에사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증서버또는 Active Directory
3269	Microsoft 글로벌카탈로그의보안 LDAP 연결에사용됩니다.	Citrix Gateway, XenMobile	LDAP 인증서버또는 Active Directory
9080	Citrix ADC 와 Exchange ActiveSync 용 Citrix Gateway 커넥터간의 HTTP 트래픽에사용됩니다.	Citrix ADC	Exchange ActiveSync 용 Citrix Gateway 커넥터
30001	HTTPS 서비스의초기스테이징을위한관리 API	내부 LAN	XenMobile Server
9443	Citrix ADC 와 Exchange ActiveSync 용 Citrix Gateway 커넥터간의 HTTPS 트래픽에사용됩니다.	Citrix ADC	Exchange ActiveSync 용 Citrix Gateway 커넥터
45000; 80	클러스터에배포된두 XenMobile VM 간의통신에사용됩니다. 포트 80 은노드간통신및 SSL 오프로드에사용됩니다.	XenMobile	XenMobile
8443	등록, XenMobile Store 및 MAM(모바일앱관리) 에사용됩니다.	XenMobile, Citrix Gateway, 장치, 인터넷	XenMobile
4443	관리자가브라우저를통해 XenMobile 콘솔에액세스할때사용됩니다. 또한모든 XenMobile 클러스터노드의로그및지원번들을한노드에서다운로드하는데사용됩니다.	액세스지점 (브라우저), XenMobile	XenMobile
27000	외부 Citrix License Server 에액세스할때사용되는기본포트입니다.	XenMobile	Citrix License Server

TCP 포트	설명	원본	대상
7279	들어오고나가는 Citrix 라이센스를확인할때사용되는기본포트입니다.	XenMobile	Citrix 공급업체데몬
161	UDP 프로토콜을사용하는 SNMP 트래픽에사용됩니다.	SNMP 관리자	XenMobile
162	XenMobile 의 SNMP 트랩알림을 SNMP 관리자로 보내는데사용됩니다. 원본은 XenMobile 이고대상은 SNMP 관리자입니다.	XenMobile	SNMP 관리자

장치관리를위한 **XenMobile** 포트열기

XenMobile 이네트워크에서통신할수있도록하려면다음포트를엽니다.

TCP 포트	설명	원본	대상
25	XenMobile 알림서비스의 기본 SMTP 포트입니다. SMTP 서버가다른포트를사용하는경우방화벽이해당포트를차단하지않는지확인하십시오.	XenMobile	SMTP 서버
80 및 443	Apple iTunes App Store 또는 Google Play(80 을사용해야함) 에대한엔터프라이즈앱스토어연결입니다. Apple 볼륨구매에사용됩니다. iOS 또는 Android 용 Secure Hub 에서앱스토어의앱을게시하는데사용됩니다.	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 알림릴레이간의아웃바운드연결에사용됩니다.	XenMobile	Nexmo SMS 릴레이서버
389	보안되지않은 LDAP 연결에사용됩니다.	XenMobile	LDAP 인증서버또는 Active Directory
443	Android 의등록및상담원설정에사용됩니다.	인터넷	XenMobile
443	Android 및 Windows 장치및 MDM 원격지원클라이언트의등록및에이전트설정에사용됩니다.	인터넷 LAN 및 Wi-Fi	XenMobile
1433	원격데이터베이스서버에대한연결에기본적으로사용됩니다 (선택사항).	XenMobile	SQL Server
443 또는 2197	APNs 알림을 `*.push.apple.com`으로전송하는데사용됩니다.	XenMobile	인터넷 (공용 IP 주소 17.0.0.0/8 을사용하는 APNs 호스트)
5223	iOS 장치에서 `*.push.apple.com`으로의 APNs 아웃바운드연결에사용됩니다.	iOS 장치	인터넷 (공용 IP 주소 17.0.0.0/8 을사용하는 APNs 호스트)
8081	선택적 MDM 원격지원클라이언트의앱터널에사용됩니다. 기본값은 8081 입니다.	원격지원클라이언트	XenMobile
8443	iOS 장치등록에사용됩니다.	인터넷, LAN 및 Wi-Fi	XenMobile

자동검색서비스연결을위한포트요구사항

이포트구성은 Android 용 Secure Hub 로부터연결되는 Android 장치가내부네트워크내에서 Citrix ADS(자동검색서비스)에액세스할수있도록합니다. ADS 를통해제공되는보안업데이트를다운로드하려면 ADS 에액세스해야합니다.

> 참고:
>
> ADS 연결에서프록시서버가지원되지않을수있습니다. 이시나리오에서는 ADS 연결이프록시서버를우회할수있게허용합니다.

인증서고정을사용하려는경우다음사전요구사항을수행합니다.

- **XenMobile Server** 및 **Citrix ADC** 인증서를수집합니다**.** 인증서는 PEM 형식이어야하고공용인증서여야하며개인 키가아니어야합니다.
- **Citrix** 지원팀에연락하여인증서고정을사용하기위한요청을제출하십시오**.** 이과정에서인증서를요구받게됩니다.

인증서고정을사용하려면장치등록전에장치가 ADS 에연결되어야합니다. 그렇게해야최신보안정보가 Secure Hub 에제공됩니다. Secure Hub 에서장치를등록하려면장치가 ADS 에연결되어야합니다. 그러므로내부네트워크내에서 ADS 액세스를열어야 장치를등록할수있습니다.

Android 또는 iOS 용 Secure Hub 에대해 ADS 액세스를허용하려면다음 FQDN 으로포트 443 을엽니다.

FQDN	포트	IP 및포트사용
discovery.cem.cloud.us	443	Secure Hub - CloudFront 를통한 ADS 통신

지원되는 IP 주소에대한정보는 AWS 의클라우드기반 Storage Center를참고하십시오.

Android Enterprise 네트워크요구사항

Android Enterprise 를위한네트워크환경을설정할때고려해야할아웃바운드연결에대한자세한내용은 Google 지원문서 Android Enterprise 네트워크요구사항을참조하십시오.

XenMobile 의포트요구사항

관리형 Google Play Enterprise 를만들고 관리형 Google Play iFrame에액세스하려면네트워크에서다음대상호스트에연결할수있어야합니다.. Google 은앱검색및승인을간소화하기위해 EMM 개발자가관리형 Play iFrame 을사용할수있도록했습니다. 관리형 Play iFrame 을사용하려면 XenMobile 콘솔에액세스하는브라우저에 Google Play 에대한액세스권한이있어야합니다.

대상호스트	포트	설명
play.google.com	TCP/443	Google Play 스토어, Play Enterprise 가입에사용
*.googleapis.com	TCP/443	Google Mobile Management, Google API, Google Play 스토어 API 에사용
accounts.youtube.com, accounts.google.com	TCP/443	계정인증에사용
apis.google.com	TCP/443	GCM 및기타 Google 웹서비스에사용

대상호스트	포트	설명
ogs.google.com	TCP/443	iFrame UI 요소에사용
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

January 5, 2022

XenMobile 인프라의규모를이해하는것은 XenMobile 을어떻게배포하고구성할지결정하는데있어중요합니다. 이문서에는확장성테스트데이터와소규모에서대규모에이르는온-프레미스 XenMobile 엔터프라이즈배포의성능과확장성을위한인프라요구사항을결정하는지침이포함되어있습니다.

여기서확장성은배포에이미등록된장치가해당배포에동시에다시연결되는능력의관점에서정의됩니다.

- 확장성은배포에등록된최대장치수로정의됩니다.
- 로그인속도는기존장치가배포에다시연결될수있는최대속도로정의됩니다.

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

XenMobile Enterprise Edition 에서모든테스트를수행했습니다.

테스트는 Citrix Gateway 8200 을사용하여수행되었습니다. 비슷하거나더큰용량의 Citrix ADC 장비에서는비슷한수준또는더뛰어난확장성과성능이나타날수있습니다.

확장성테스트결과의요약은다음과같습니다.

최대 **75,000** 개장치의배포에대한확장성테스트결과요약

로그인속도 (기존사용자의다시연결속도) - 시간당최대 9,375 개장치

사용된구성:

- Citrix 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
시간당기존장치의다시연결속도	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 외부데이터베이스	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

XenMobile Server 구성	합계	사용자당
MDX	50	30
웹및 SaaS	20	20
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-프레미스배포용참조아키텍처의 “핵심 MAM + MDM 참조아키텍처” 를참조하십시오.

주의사항및제한사항

이문서에나온확장성테스트결과를고려할때다음사항에유의하십시오.

- Windows 플랫폼은테스트되지않았습니다.

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

라이센싱

March 24, 2022

> 중요:
>
> Citrix 라이센스반환및수정프로세스가 2020 년 11 월 4 일부터변경되었습니다. 자세한내용은다음문서를참조하십시오.
>
> - 내계정을사용하여라이센스를반환하는방법
> - 라이센스파일재할당방법

XenMobile 은 Citrix Licensing 을사용하여라이센스를관리합니다. XenMobile Server 및 Citrix Gateway 를사용하려면라이센스가필요합니다.

Citrix Gateway 라이센스에대한자세한내용은 Citrix Gateway 설명서를참조하십시오. Citrix Licensing 에대한자세한내용은 The Citrix Licensing System(Citrix Licensing 시스템)을참조하십시오.

XenMobile Server 를구입하면라이센스활성화지침이포함된주문확인전자메일메시지가전송됩니다. 신규고객은주문을제출하기전에라이센스프로그램에등록해야합니다. XenMobile 라이센스모델및프로그램에대한자세한내용은 XenMobile licensing(XenMobile 라이센스)을참조하십시오.

요구사항

- 최신버전의 XenMobile Server 로업데이트하기전에 Citrix License Server 를 11.16.x 이상으로업데이트하십시오. 이전라이센스서버버전은최신버전의 XenMobile 을지원하지않습니다.
- XenMobile 라이센스를다운로드하기전에 Citrix Licensing 을설치해야합니다. 라이센스파일을생성하려면 Citrix Licensing 을설치한서버의이름이필요합니다. XenMobile 을설치하면 Citrix Licensing 이기본적으로이서버에설치됩니다. 또는기존 Citrix Licensing 배포를사용하여 XenMobile 라이센스를관리할수있습니다. Citrix Licensing 설치, 배포및관리에대한자세한내용은 제품라이센스를참조하십시오.
- XenMobile 의노드또는인스턴스를클러스터하려는경우원격서버에서 Citrix Licensing 을사용해야합니다.
- 받은모든라이센스파일의로컬복사본을유지하는것이좋습니다. 구성파일의백업복사본을저장하면모든라이센스파일이백업에포함됩니다. 그러나구성파일을먼저백업하지않고 XenMobile 을다시설치하는경우원래라이센스파일이필요합니다.

XenMobile 라이센스고려사항

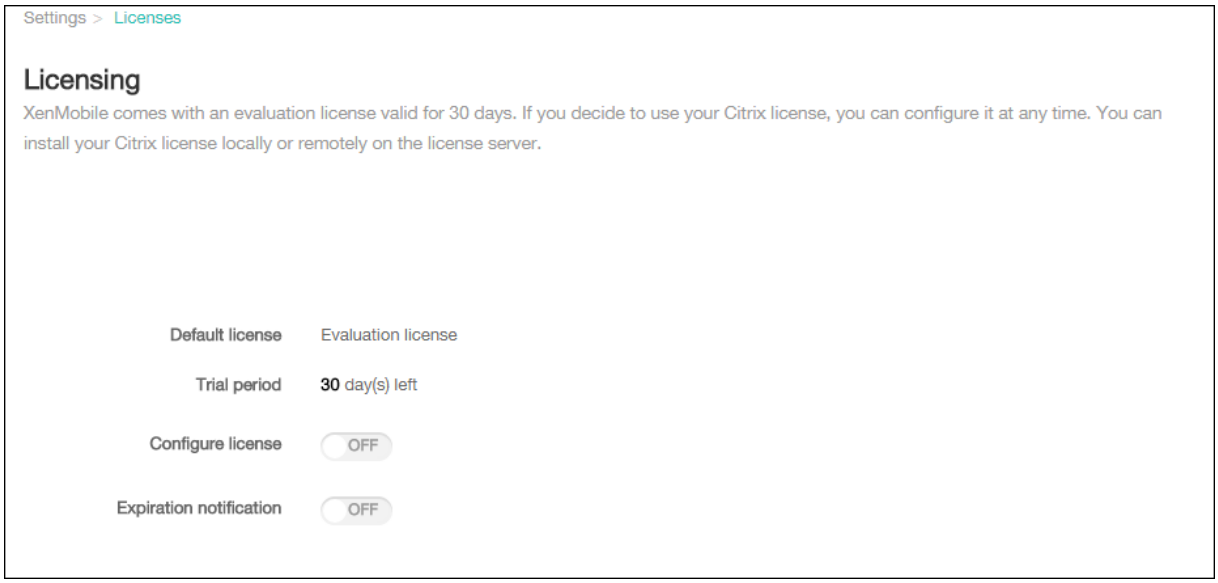
라이센스가없는경우평가모드에서 30 일의유예기간동안 XenMobile 의모든기능을사용할수있습니다. 이평가모드는한번만사용할수있으며 XenMobile 을설치한날부터 30 일간유효합니다. 유효한 XenMobile 라이센스가있는지여부와관계없이 XenMobile 웹콘솔에대한액세스는차단되지않습니다. XenMobile 콘솔에서평가기간이얼마나남았는지를확인할수있습니다.

XenMobile 에서다수의라이센스를업로드할수있지만한번에하나의라이센스만활성화할수있습니다.

XenMobile 라이센스가만료되면더이상장치관리기능을수행할수없습니다. 예를들어새사용자또는장치를등록할수없고등록된장치에배포한앱및구성을업데이트할수없습니다. XenMobile 라이센스모델및프로그램에대한자세한내용은 XenMobile licensing(XenMobile 라이센스)을참조하십시오.

XenMobile 콘솔에서라이센스페이지를찾으려면

XenMobile 을설치한후 라이센스페이지가처음으로나타날때라이센스는기본 30 일평가모드로설정되고아직구성되지않은상태로표시됩니다. 이페이지에서라이센스를추가하고구성할수있습니다.



1. XenMobile 콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 라이센스를클릭합니다. 라이센스페이지가나타납니다.

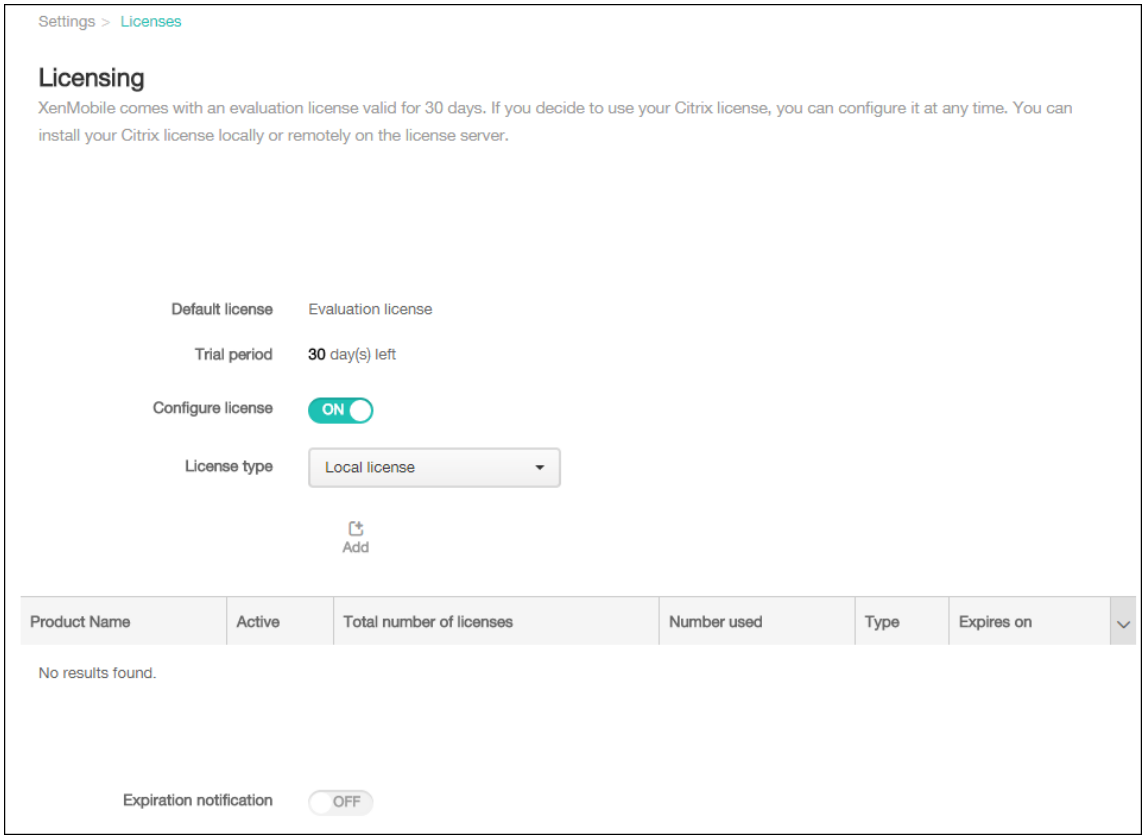
로컬라이센스를추가하려면

새라이센스를추가하면테이블에새라이센스가나타납니다. 추가한첫번째라이센스가자동으로활성화됩니다. 동일한범주 (예: Enterprise) 와유형의여러라이센스를추가하는경우이러한라이센스가테이블의한행에나타납니다. 이경우공통라이센스의결합된양이 총라이센스수및 사용된수에반영됩니다. 만료날짜에는공통라이센스중에서가장빠른만료날짜가표시됩니다.

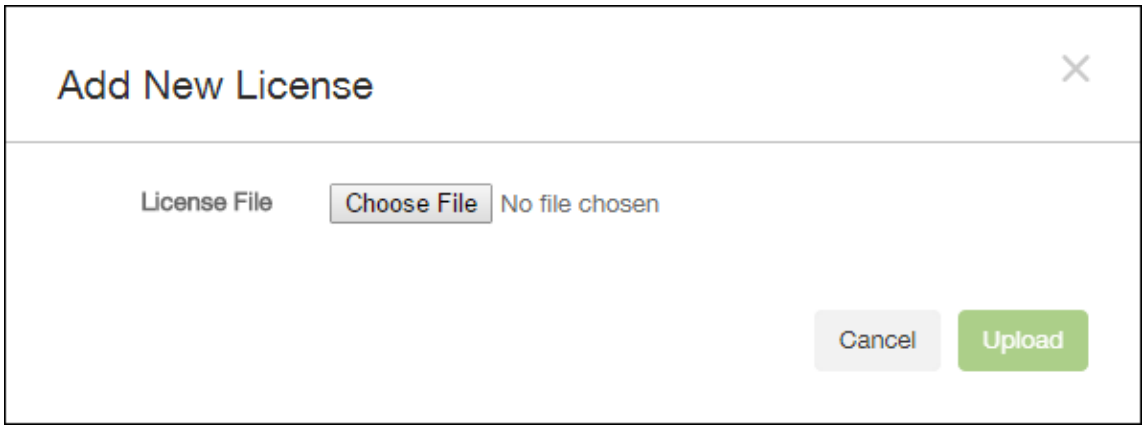
모든로컬라이센스는 XenMobile 콘솔을통해관리합니다.

1. Simple License Service 에서 License Administration Console 을통해라이센스파일을가져오거나 Citrix.com 계정에서직접가져옵니다. 자세한내용은 Citrix Licensing 설명서를참조하십시오.
2. XenMobile 콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
3. 라이센스를클릭합니다. 라이센스페이지가나타납니다.

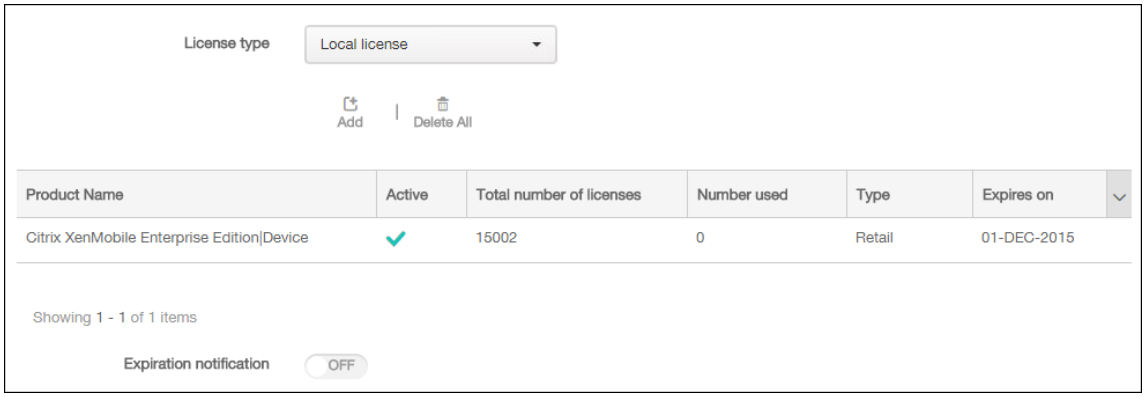
4. 라이센스구성을 켜짐으로설정합니다. 라이센스유형목록, 추가단추및 라이센스테이블이표시됩니다. 라이센스테이블에는 XenMobile 에서사용한라이센스가포함됩니다. Citrix 라이센스를추가하지않은경우테이블이비어있습니다.



5. 라이센스유형이 로컬라이센스로설정되어있는지확인하고 추가를클릭합니다. 새라이센스추가대화상자가나타납니다.



6. 새라이센스추가대화상자에서 파일선택을클릭하고라이센스파일의위치를찾습니다.
7. 업로드를클릭합니다. 라이센스가로컬로업로드되고테이블에나타납니다.



8. 라이센스페이지의테이블에나타난라이센스를활성화합니다. 테이블의첫번째라이센스인경우해당라이센스가자동으로활성화됩니다.

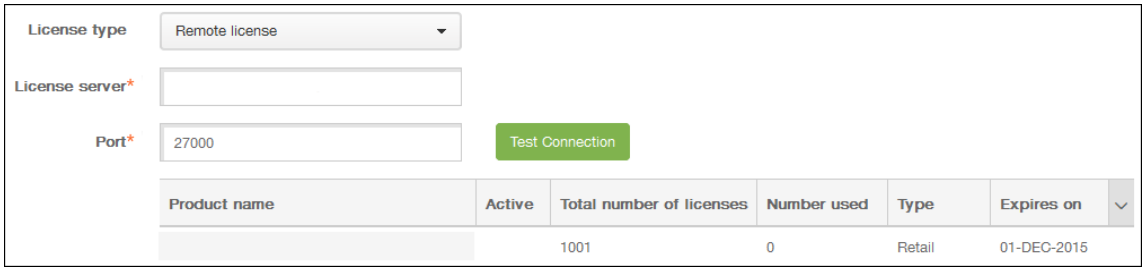
원격라이센스를추가하려면

원격 Citrix Licensing 서버를사용하는경우 Citrix Licensing 서버를사용하여 모든라이센스작업을관리합니다. 자세한내용은 제품라이센스를참조하십시오.

1. 라이센스서버인증서를 XenMobile Server 로가져옵니다 (설정 **>** 인증서).
2. 기본적으로호스트이름유효성검사는 Microsoft PKI 서버를제외한발신연결에대해활성화됩니다. 호스트이름유효성검사로인해배포가중단되는경우서버속성 **disable.hostname.verification** 을 **true** 로변경하십시오. 이속성의기본값은 **false** 입니다.

   호스트이름유효성검사가실패하면서버로그에다음과같은오류가포함됩니다. “볼륨구매서버에연결할수없습니다. 호스트이름 ‘192.0.2.0’ 은피어가제공한인증서주체와일치하지않습니다.”

3. 라이센스페이지에서 라이센스구성을 켜짐으로설정합니다. 라이센스유형목록, 추가단추및 라이센스테이블이표시됩니다. 라이센스테이블에는 XenMobile 에서사용한라이센스가포함됩니다. Citrix 라이센스를추가하지않은경우테이블이비어있습니다.
4. 라이센스유형을 원격라이센스로설정합니다. 추가단추가 라이센스서버및 포트필드와 연결테스트단추로바뀝니다.



5. 다음설정을구성합니다.

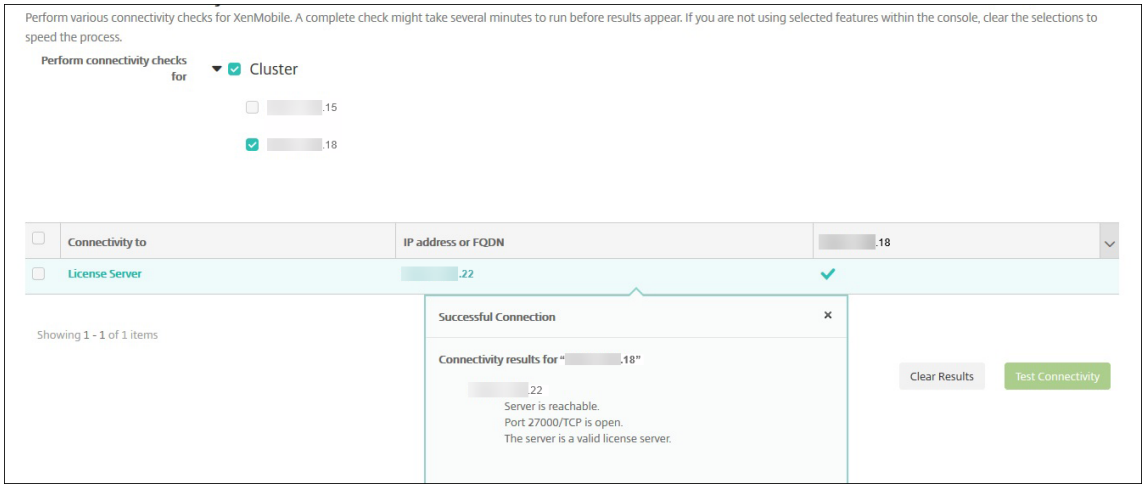
   - 라이센스서버: 원격라이센스서버의 IP 주소또는 FQDN(정규화된도메인이름) 을입력합니다.
   - 포트: 기본포트를사용하거나라이센스서버와의통신에사용할포트번호를입력합니다.

6. 연결테스트를클릭합니다. 연결이성공적인경우 XenMobile 이라이센스서버에연결하고라이센스테이블이사용가능한라이센스로채워집니다. 테이블에라이센스가하나만있는경우자동으로활성화됩니다.

   연결테스트를클릭하면 XenMobile 이다음을확인합니다.

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

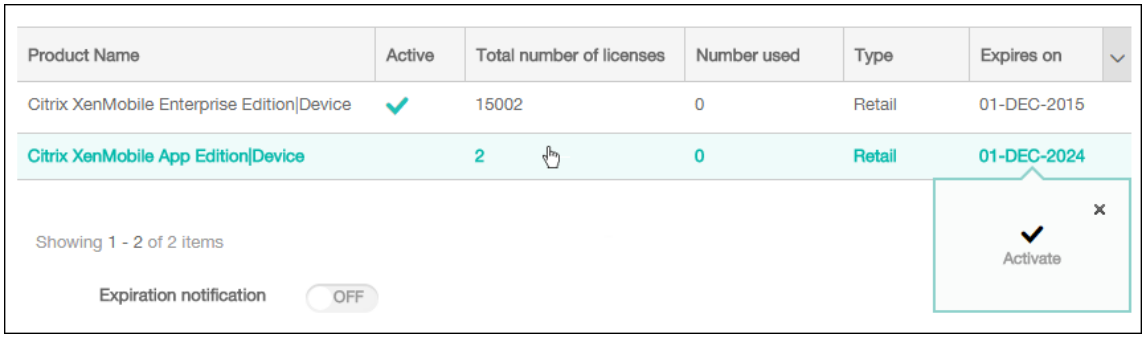
   연결이실패한경우표시된오류메시지를검토하고필요한사항을수정한후 연결테스트를클릭합니다.



서로다른라이센스를활성화하려면

라이센스가여러개인경우활성화할라이센스를선택할수있습니다. 그러나한번에하나의라이센스만활성화할수있습니다.

1. 라이센스페이지의 라이센스테이블에서활성화할라이센스의행을클릭합니다. 활성화확인대화상자가행옆에나타납니다.



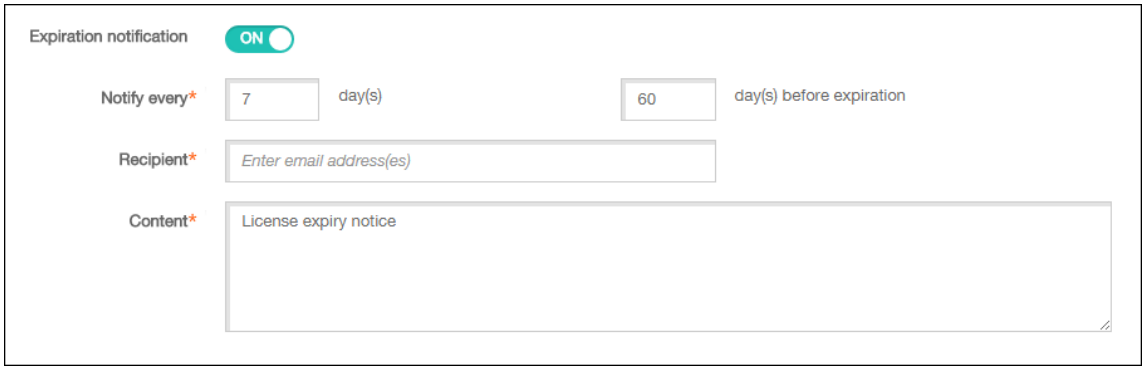
2. 활성화를클릭합니다. 활성화대화상자가나타납니다.
3. 활성화를클릭합니다. 선택한라이센스가활성화됩니다.

   > 중요:
   >
   > 선택한라이센스를활성화하면현재라이센스가비활성화됩니다.

만료알림을자동화하려면

원격또는로컬라이센스를활성화한후라이센스만료날짜가가까워질때알림을보내도록 XenMobile 을구성할수있습니다.

1. 라이센스페이지에서 만료알림을 켜짐으로설정합니다. 새알림관련필드가나타납니다.



2. 다음설정을구성합니다.
   - 알림간격: 유형:
   - 알림을보낼빈도 (예: **7** 일마다) 입니다.
   - 알림전송을시작할시기 (예: 라이센스만료 60 일전) 입니다.
   - 받는사람: 자신의전자메일주소또는라이센스담당자의전자메일주소를입력합니다.
   - 내용: 받는사람이알림에서볼만료알림메시지를입력합니다.
3. 저장을클릭합니다. 설정을기반으로 XenMobile 이 내용에입력된텍스트가포함된전자메일메시지를 받는사람에입력된 받는사람에게보내기시작합니다. 알림은설정한빈도로전송됩니다.

FIPS 140-2 준수

January 5, 2022

미국 NIST(표준기술연구소) 에서발행한 FIPS(Federal Information Processing Standard) 는보안시스템에사용되는 암호화모듈의보안요구사항을지정합니다. FIPS 140-2 는이표준의두번째버전입니다. NIST 가검증한 FIPS 140 모듈에대한자세한내용은 NIST Computer Security Resource Center를참조하십시오.

> 중요:
>
> - XenMobile FIPS 모드는초기설치중에만설정할수있습니다.
> - XenMobile 모바일기기관리전용, XenMobile 모바일앱관리전용및 XenMobile MDM+MAM 은모두 HDX 앱을사용하지않는한 FIPS 를준수합니다.

iOS 의모든저장데이터및전송중데이터암호화작업에는 Citrix 및 Apple 에서제공하는 FIPS 검증암호화모듈이사용됩니다. Android 의모든저장데이터암호화작업에는 FIPS 검증암호화모듈또는장치제조업체에서제공하는플랫폼암호화모듈이사용됩니다. 장치제조업체의모듈에대한자세한정보는 Citrix 담당자에게문의하십시오.

지원되는 Windows 장치의 MDM(모바일기기관리) 에대한모든저장데이터및전송중데이터암호화작업에는 FIPS 검증암호화모듈이사용됩니다.

XenMobile MDM 의모든저장데이터및전송중데이터암호화작업에는 FIPS 검증암호화모듈이사용됩니다. MDM 흐름의모든저장된데이터와전송중데이터에는 FIPS 준수암호화모듈이사용됩니다. 이보안에는위에서설명한모바일장치에대한암호화작업에더해모바일장치와 Citrix Gateway 간의암호화작업이포함됩니다.

MDX Vault 는 iOS 및 Android 장치의 MDX 래핑된앱및연관된저장데이터를 FIPS 인증암호화모듈을사용하여암호화합니다.

언어지원

December 1, 2020

모바일생산성앱및 XenMobile 콘솔은영어이외의언어로사용하기적합합니다. 앱이사용자의기본설정언어로현지화되지않은경우에도영어이외의문자및키보드입력이지원됩니다. 모든 Citrix 제품의국제화지원에대한자세한내용은 https://support.citrix.com/article/CTX119253을참조하십시오.

이문서에서는 XenMobile 의최신릴리스에서지원되는언어를나열합니다.

XenMobile 콘솔및자가지원포털

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

모바일생산성앱

X 는해당언어로앱을사용할수있음을나타냅니다.

iOS 및 Android

언어	Secure Hub	Secure Mail	Secure Web	QuickEdit
일본어	X	X	X	X
중국어 (간체)	X	X	X	X
중국어 (번체)	X	X	X	X

언어	Secure Hub	Secure Mail	Secure Web	QuickEdit
프랑스어	X	X	X	X
독일어	X	X	X	X
스페인어	X	X	X	X
한국어	X	X	X	X
포르투갈어	X	X	X	X
네덜란드어	X	X	X	X
이탈리아어	X	X	X	X
덴마크어	X	X	X	X
스웨덴어	X	X	X	X
히브리어	X	X	X	iOS 만해당
아랍어	X	X	X	X
러시아어	X	X	X	X
터키어	X	X	Android 전용	-
폴란드어	X	X	X	-

Windows

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

설치및구성

June 30, 2022

시작하기전에

다음사전설치체크리스트를사용하여온-프레미스에 XenMobile 을설치하기위한사전요구사항과설정을확인할수있습니다. 각작업또는메모에는요구사항이적용되는구성요소또는기능을나타내는열이포함되어있습니다.

XenMobile 배포를계획할때는많은요소를고려해야합니다. 전체 XenMobile 환경에대한권장사항, 일반적인질문및사용사례는 XenMobile 배포안내서를참조하십시오.

설치단계는이문서뒷부분의 XenMobile 설치 섹션을참조하십시오.

사전설치체크리스트

기본네트워크연결

다음은 XenMobile 솔루션에필요한네트워크설정입니다.

사전요구사항또는설정	구성요소또는기능	설정메모
원격사용자가연결하는 FQDN(정규화된 도메인이름) 을적어둡니다.	XenMobile 및 Citrix Gateway	
공용및로컬 IP 주소를적어둡니다.		

사전요구사항또는설정	구성요소또는기능	설정메모	
방화벽을구성하여 NAT(Network Address Translation) 를설정하려면이러한 IP 주소가필요합니다.	XenMobile 및 Citrix Gateway		
서브넷마스크를적어둡니다.	XenMobile 및 Citrix Gateway		
DNS IP 주소를적어둡니다.	XenMobile 및 Citrix Gateway		
WINS 서버 IP 주소 (해당하는경우) 를적어둡니다.	Citrix Gateway		
Citrix Gateway 호스트이름을식별하고적어둡니다.	Citrix Gateway	이항목은 FQDN 이아닙니다. FQDN 은가상서버에바인딩되어있고사용자가연결하는서명된서버인증서에포함되어있습니다. Citrix Gateway 에서설치마법사를사용하여호스트이름을구성할수있습니다.	Citrix Gateway
XenMobile 의 IP 주소를적어둡니다. XenMobile 의인스턴스하나를설치하는경우 IP 주소하나를예약합니다. 클러스터를구성하는경우필요한모든 IP 주소를적어둡니다.	XenMobile		
Citrix Gateway 에구성된공용 IP 주소 1 개	Citrix Gateway		

사전요구사항또는설정	구성요소또는기능	설정메모	
Citrix Gateway 에 대한외부 DNS 항목 1 개	Citrix Gateway		
웹프록시서버 IP 주소, 포트, 프록시호스트목록및관리자사용자이름/암호를적어둡니다. 회사네트워크(해당하는경우) 에프록시서버를배포하는경우이러한설정은선택사항입니다.	Citrix Gateway	웹프록시에대한사용자이름을구성할때 sAMAccount-Name 또는 UPN(사용자계정이름) 을사용할수있습니다.	XenMobile 및 Citrix Gateway
기본게이트웨이 IP 주소를적어둡니다.	XenMobile 및 Citrix Gateway		
시스템 IP(NSIP) 주소및서브넷마스크를적어둡니다.	Citrix Gateway		
서브넷 IP(SNIP) 주소및서브넷마스크를적어둡니다.	Citrix Gateway		
인증서에서 Citrix Gateway 가상서버 IP 주소및 FQDN 을적어둡니다. 다수의가상서버를구성하려면인증서의모든가상 IP 주소및 FQDN 을적어둡니다.	Citrix Gateway		

사전요구사항또는설정	구성요소또는기능	설정메모
사용자가 Citrix Gateway 를통해액세스할수있는내부네트워크를적어둡니다. 예: 10.10.0.0/24. 분할터널링이켜짐으로설정된경우사용자가 Secure Hub 또는 Citrix Gateway 플러그인에연결할때액세스해야하는모든내부네트워크및네트워크세그먼트를입력합니다.	Citrix Gateway	
XenMobile Server, Citrix Gateway, 외부 Microsoft SQL Server 및 DNS 서버간의네트워크연결이접속가능한지확인합니다.	XenMobile 및 Citrix Gateway	

라이센스

XenMobile 을사용하려면 Citrix Gateway 및 XenMobile 에대한라이센스옵션을구입해야합니다. Citrix Licensing 에대한자세한내용은 The Citrix Licensing System(Citrix Licensing 시스템)을참조하십시오.

사전요구사항	구성요소	위치메모
Citrix 웹사이트에서범용라이센스를구입합니다. 자세한내용은 Citrix Gateway 설명서에서 Licensing(라이센스) 을참조하십시오.	Citrix Gateway, XenMobile 및 Citrix License Server	

인증서

XenMobile 및 Citrix Gateway 를사용자장치의다른 Citrix 제품및앱과연결하려면인증서가필요합니다. 자세한내용은 XenMobile 설명서의 인증서및인증 섹션을참조하십시오.

사전요구사항	구성요소	참고
필요한인증서를받아서설치합니다.	XenMobile 및 Citrix Gateway	

포트

XenMobile 구성요소와통신할수있도록포트를엽니다.

사전요구사항	구성요소	참고
XenMobile 포트를엽니다.	XenMobile 및 Citrix Gateway	

데이터베이스

XenMobile 에데이터베이스연결을구성해야합니다. XenMobile 저장소에는 시스템요구사항및호환성에명시된지원되는버전 중하나에서실행되는 Microsoft SQL Server 데이터베이스가필요합니다. Microsoft SQL 은원격으로사용하는것이좋습니다. PostgreSQL 은 XenMobile 에포함되어있으며 테스트환경에서만로컬또는원격으로사용할수있습니다.

기본적으로 XenMobile 은 jTDS 데이터베이스드라이버를사용합니다. XenMobile Server 의온-프레미스설치에 Microsoft JDBC 드라이버를사용하려면 SQL Server 드라이버를참조하십시오.

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 Citrix Gateway	
Active Directory 도메인이름을적어둡니다.	XenMobile 및 Citrix Gateway	
Active Directory 서비스계정을사용자 ID, 암호및도메인별칭을포함하여적어둡니다.		
Active Directory 서비스계정은 XenMobile 이 Active Directory 에쿼리할때사용하는계정입니다.	XenMobile 및 Citrix Gateway	
사용자가위치한디렉터리수준을나타내는사용자기본 DN 을적어둡니다. 예: `cn=users,dc=ace,dc=com`. Citrix Gateway 및 XenMobile 은 사용자기본 DN 을사용하여 Active Directory 에쿼리합니다.	XenMobile 및 Citrix Gateway	
그룹이위치한디렉터리수준을나타내는그룹기본 DN 을적어둡니다. Citrix Gateway 및 XenMobile 은이 DN 을사용하여 Active Directory 에쿼리합니다.	XenMobile 및 Citrix Gateway	

XenMobile 과 **Citrix Gateway** 간연결

사전요구사항	구성요소	설정메모
XenMobile 호스트이름을적어둡니다.	XenMobile	
XenMobile 의 FQDN 또는 IP 주소를적어둡니다.	XenMobile	
사용자가액세스할수있는앱을파악합니다.	Citrix Gateway	

사전요구사항	구성요소	설정메모
콜백 URL 을적어둡니다.	XenMobile	

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

Citrix ADC 의 Quick Configuration(빠른구성) 마법사를사용하여 XenMobile 과 Citrix Gateway 간의연결설정및 XenMobile 과 Secure Hub 간의연결설정을구성하는것이좋습니다. 두번째가상서버를생성하여 Citrix Receiver 와웹브라우저에서사용자연결을사용하도록설정합니다. 이러한연결은 Virtual Apps and Desktops 에있는 Windows 기반응용프로그램과가상데스크톱에대한연결입니다. 이러한설정도 Citrix ADC 의 Quick Configuration(빠른구성) 마법사를사용하여구성하는것이좋습니다.

사전요구사항	구성요소	설정메모
Citrix Gateway 호스트이름및외부 URL 을적어둡니다. 외부 URL 은사용자가연결하는웹주소입니다.	XenMobile	
Citrix Gateway 콜백 URL 을적어둡니다.	XenMobile	
가상서버의 IP 주소와서브넷마스크를적어둡니다.	Citrix Gateway	
Program Neighborhood Agent 또는 Virtual Apps and Desktops 사이트의경로를적어둡니다.	Citrix Gateway 및 XenMobile	
STA(Secure Ticket Authority) 를실행하는 Virtual Apps and Desktops 서버의 FQDN 또는 IP 주소를적어둡니다 (ICA 연결에만해당).	Citrix Gateway	
XenMobile 의공용 FQDN 을적어둡니다.	Citrix Gateway	
Secure Hub 의공용 FQDN 을적어둡니다.	Citrix 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 에서실행됩니다. XenCenter 또는 vSphere 관리콘솔을사용하여 XenMobile 을설치할수있습니다.

> 참고:
>
> NTP 서버또는수동구성을사용하여하이퍼바이저에정확한시간이구성되어있는지확인합니다. XenMobile 에서해당시간을사용합니다. XenMobile 시간을하이퍼바이저와동기화할때표준시간대관련문제가나타나는경우 XenMobile 이 NTP 서버를가리키도록하면이문제를방지할수있습니다. 이렇게하려면 CLI 옵션에나온대로 XenMobile CLI 를사용합니다.

XenServer 또는 **VMware ESXi** 사전요구사항. XenServer 또는 VMware ESXi 에 XenMobile 를설치하기전에다음을수행해야합니다. 자세한내용은 XenServer 또는 VMware 설명서를참조하십시오.

- 적절한하드웨어리소스가있는컴퓨터에 XenServer 또는 VMware ESXi 를설치합니다.
- XenCenter 또는 vSphere 를별도의컴퓨터에설치합니다. XenCenter 또는 vSphere 를호스트하는컴퓨터는네트워크를통해 XenServer 또는 VMware ESXi 호스트에연결합니다.

Hyper-V 관련사전요구사항. Hyper-V 에 XenMobile 을설치하기전에다음을수행해야합니다. 자세한내용은 Hyper-V 설명서를참조하십시오.

- 적절한시스템리소스가있는컴퓨터에 Windows Server 2008 R2, Windows Server 2012 또는 Windows Server 2012 R2 를설치하고 Hyper-V 와역할을사용하도록설정합니다. Hyper-V 역할을설치할때 Hyper-V 에서가상네트워크를만드는데사용할서버에서 NIC 를지정해야합니다. 일부 NIC 는호스트용으로남겨둘수있습니다.
- Virtual Machines/<*build-specific UUID*>.xml 파일을삭제합니다.
- Legacy/<*build-specific UUID*>.exp 파일을 Virtual Machines 로이동합니다.

Windows Server 2008 R2 또는 Windows Server 2012 를설치하는경우다음을수행합니다.

VM 구성을나타내는 Hyper-V 매니페스트파일에두가지버전 (.exp 및.xml) 이있기때문에이러한단계가필요합니다. Windows Server 2008 R2 및 Windows Server 2012 릴리스는.exp 만지원합니다. 이러한릴리스의경우설치전에.exp 매니페스트파일만있어야합니다.

Windows Server 2012 R2 에서는이러한추가단계가필요없습니다.

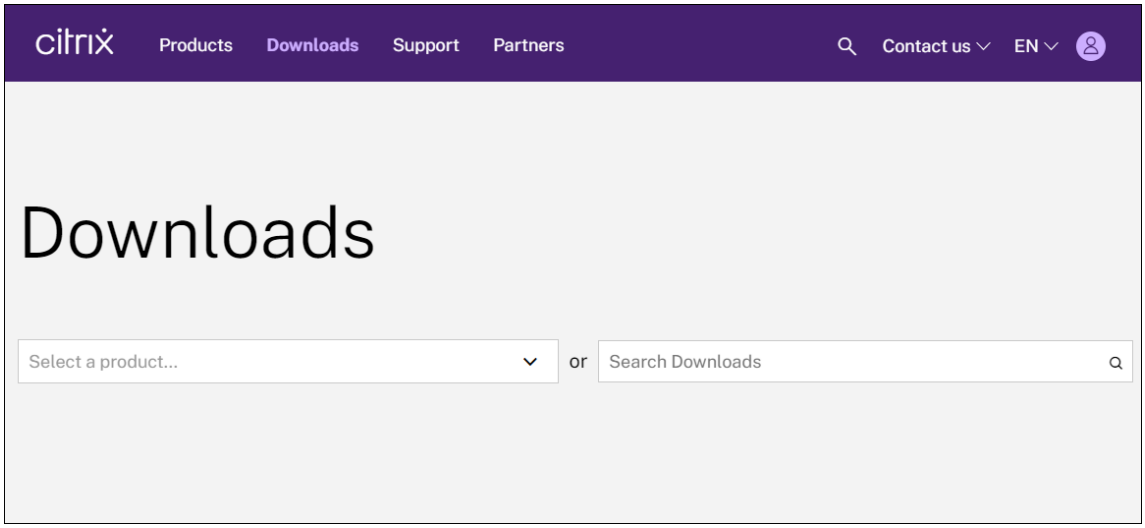
FIPS 140-2 모드. XenMobile Server 를 FIPS 모드로설치하려는경우 XenMobile 을사용하여 FIPS 구성에나온일련의사전요구사항을완료합니다.

XenMobile 제품소프트웨어다운로드

Citrix 웹사이트에서제품소프트웨어를다운로드할수있습니다. 사이트에로그온한후 Download(다운로드) 링크를사용하여다운로드할소프트웨어가있는페이지로이동합니다.

XenMobile 소프트웨어를다운로드하려면

1. Citrix 웹사이트로이동합니다.
2. Search(검색) 상자옆에있는 **Log On(**로그온**)** 을클릭하여계정에로그온합니다.
3. **Downloads(**다운로드**)** 탭을클릭합니다.
4. 다운로드페이지의 제품선택목록에서 **Citrix Endpoint Management(**및 **Citrix XenMobile Server)** 를선택합니다. Citrix Endpoint Management(및 Citrix XenMobile Server) 페이지가자동으로나타납니다.



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

Citrix Gateway 소프트웨어를다운로드하려면

Citrix Gateway 가상장비또는소프트웨어업그레이드를기존 Citrix Gateway 장비에다운로드하려면다음절차를사용합니다.

1. Citrix 웹사이트로이동합니다.
2. Citrix 웹사이트에아직로그온하지않은경우 Search(검색) 상자옆에있는 **Log On(**로그온**)** 을클릭하여계정에로그온합니다.

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

   > 참고**:**
   >
   > **Virtual Appliances(**가상장비**)** 를클릭하여 Citrix ADC VPX 를다운로드할수도있습니다. 이옵션을선택하면각하이퍼바이저에대한가상컴퓨터용소프트웨어목록이나타납니다.

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 템플릿을배포할때네트워킹속성을구성하지않는것이좋습니다. 이렇게하면고가용성구성에서복제후두번째 XenMobile 가상컴퓨터를다시시작할때발생하는 IP 주소관련문제를방지할수있습니다.

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

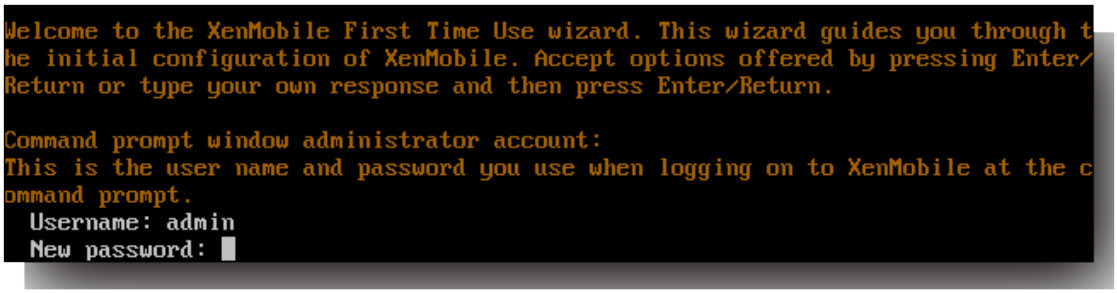
명령프롬프트창에서 **XenMobile** 구성

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.

   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: ! ## $ %)



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)

> 참고:
>
> 이이미지와다음이미지에표시된주소는작동하지않는주소이며예를위해서만제공되었습니다.

5. 무작위암호화암호를생성하여보안을강화하려면 **y** 를입력하고고유한암호를제공하려면 **n** 을입력합니다. **y** 를입력하여무작위암호를생성하는것이좋습니다.

   암호는중요한데이터를보호하는데사용되는암호화키의보호차원에서사용됩니다. 데이터의암호화및암호해독시서버파일시스템에저장된암호해시를사용하여키가검색됩니다. 암호는볼수없습니다.

> 참고:
>
> 환경을확장하고추가서버를구성하려는경우고유한암호를제공합니다. 무작위암호를선택하는경우암호를볼수없습니다.


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

6. 필요한경우 FIPS(Federal Information Processing Standard) 를사용하도록설정합니다. FIPS 에대한자세한내용은 FIPS를참조하십시오. 또한 XenMobile 을사용하여 FIPS 구성에설명된대로일련의사전요구사항을충족해야합니다.

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

7. 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 은원격으로사용하는것이좋습니다. PostgreSQL 은 XenMobile 에포함되어있으며 테스트환경에서만로컬또는원격으로사용할수있습니다.
  - 데이터베이스마이그레이션은지원되지않습니다. 테스트환경에서만든데이터베이스를프로덕션환경으로이동할수없습니다.

- 필요한경우 **y** 를입력하여데이터베이스에대한 SSL 인증을사용합니다.
- XenMobile 을호스트하는서버의 FQDN(정규화된도메인이름) 을입력합니다. 이하나의호스트서버에서장치관리와앱관리서비스를모두제공합니다.
- 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.

10. **Enter** 키를눌러설정을적용합니다.

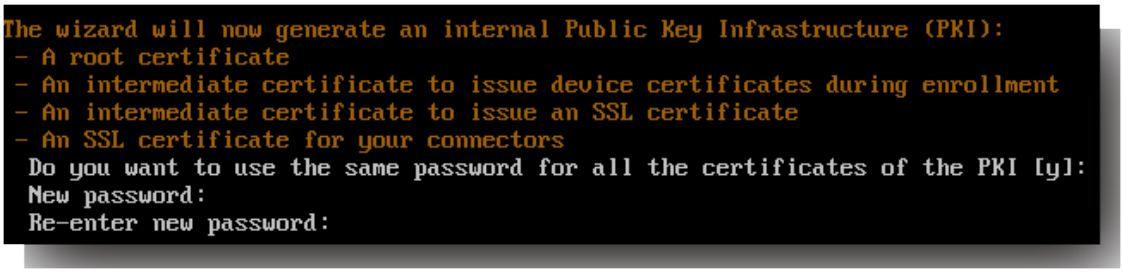
11. 통신포트를확인합니다. 포트와용도에대한자세한내용은 포트요구사항을참조하십시오.

    > 참고:
    >
    > **Enter**(Mac 의경우 Return) 키를눌러기본포트를적용합니다.

12. XenMobile 을처음으로설치하는것이므로이전 XenMobile 릴리스에서의업그레이드에대한다음질문은건너뜁니다.

13. 각 PKI(공개키인프라) 인증서에동일한암호를사용하려면 **y** 를입력합니다. XenMobile PKI 기능에대한자세한내용은 인증서업로드를참조하십시오.

    > 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 cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

> 참고:
>
> 새암호를입력할때별표와같은문자는표시되지않습니다.

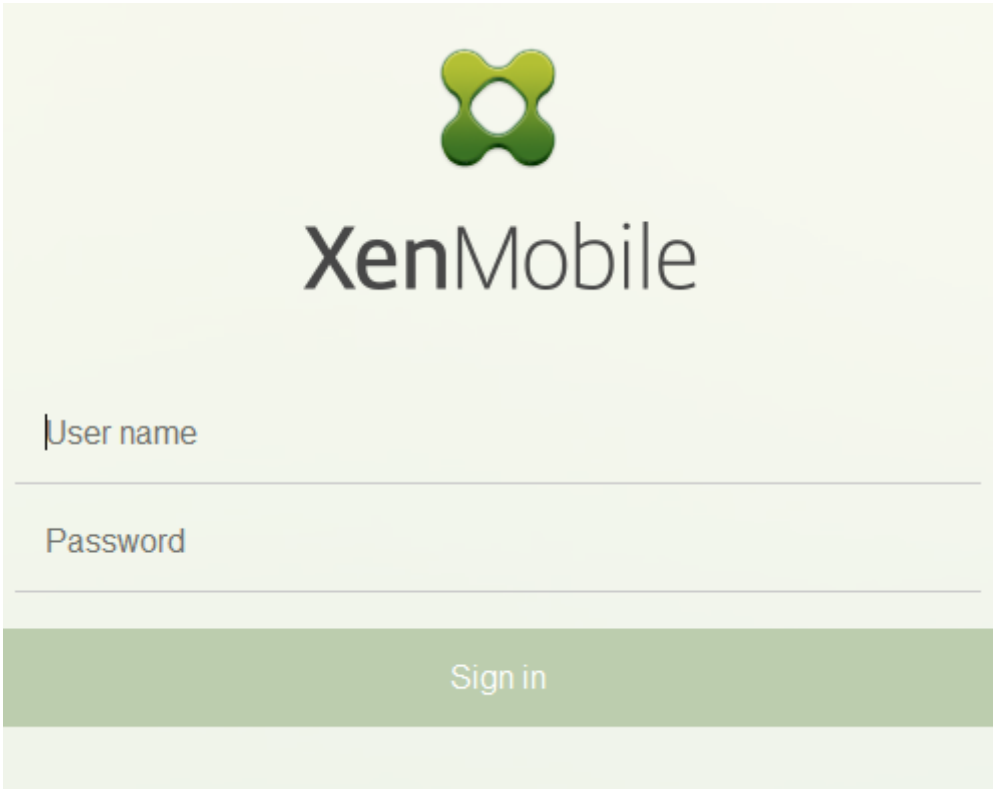
17. **Enter** 키를눌러설정을적용합니다. 초기시스템구성이저장됩니다.
18. 새로운설치이므로업그레이드중인지묻는메시지가나타나면 **n** 을입력합니다.
19. 화면에나타나는전체 URL 을복사하고웹브라우저에서이초기 XenMobile 구성을계속합니다.

```
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. 라이센스페이지가나타납니다.
4. 라이센스를구성합니다. 라이센스를업로드하지않는경우 30 일동안유효한평가라이센스를사용합니다. 라이센스를추가및 구성하고만료알림을구성하는방법에대한자세한내용은 라이센스를참조하십시오.

   > 중요:
   >
   > XenMobile 의클러스터노드또는인스턴스를추가하여 XenMobile 클러스터링을사용하려는경우원격서버에서 Citrix Licensing 을사용해야합니다.

5. 인증서페이지에서 가져오기를클릭합니다. 가져오기대화상자가나타납니다.
6. APNs 및 SSL 수신기인증서를가져옵니다. iOS 장치를관리하려면 APNs 인증서가필요합니다. 인증서사용방법에대한 자세한내용은 인증서를참조하십시오.

   > 참고:
   >
   > 이단계를수행하려면서버를다시시작해야합니다.

7. 환경에해당되는경우 Citrix Gateway 를구성합니다. Citrix Gateway 를구성하는방법에대한자세한내용은 Citrix Gateway 및 XenMobile과 XenMobile 환경에대한설정구성을참조하십시오.

   > 참고:
   >
   > - 내부네트워크경계 (또는인트라넷) 에 Citrix Gateway 를배포할수있습니다. 이배포는내부네트워크에잇는 서버, 앱및기타네트워크리소스에대한안전한단일지점액세스를제공합니다. 이배포에서는모든원격사용자가 내부네트워크의리소스에액세스하기위해먼저 Citrix Gateway 에연결해야합니다.

> • Citrix Gateway 는선택적인설정이지만이페이지에서데이터를입력한후에페이지에서나가려면모든필수필드를지우거나작성해야합니다.

8. Active Directory 에서사용자및그룹에액세스하려면 LDAP 구성을완료합니다. LDAP 연결을구성하는방법에대한자세한내용은 LDAP 구성을참조하십시오.
9. 사용자에게메시지를보낼수있도록알림서버를구성합니다. 알림서버구성에대한자세한내용은 알림을참조하십시오.

사후요구사항. XenMobile Server 를다시시작하여인증서를활성화합니다.

XenMobile 을사용하여 FIPS 구성

January 5, 2022

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 데이터베이스에외부 SQL Server 2014 를사용합니다. 또한보안 SSL 통신을사용하도록 SQL Server 를구성해야합니다. SQL Server 에대한보안 SSL 통신을구성하는방법에대한자세한내용은 데이터베이스엔진에대한암호화된연결사용 (SQL Server Configuration Manager)을참조하십시오.
- 보안 SSL 통신을사용하려면 SQL Server 에잘알려진 CA(인증기관) 의신뢰할수있는 SSL 인증서를설치해야합니다. SQL Server 2014 에는와일드카드인증서를사용할수없습니다. 따라서 SQL Server FQDN 을사용하여 SSL 인증서를요청하는것이좋습니다.

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. 이옵션은비프로덕션및진단용도로제공되며프로덕션 XenMobile Server 에서지원되지않습니다.

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

> 참고:
>
> SQL 로그온또는 Active Directory 계정을사용하여 SQL Server 에액세스할수있지만사용하는로그온계정이 DBcreator 역할을보유해야합니다.

4. Active Directory 계정을사용하려면도메인\사용자이름형식으로자격증명을입력합니다.
5. 이러한단계를완료한후에는 XenMobile 초기설정을진행합니다.

FIPS 모드가성공적으로구성되었는지확인하려면 XenMobile 명령줄인터페이스에로그온합니다. 로그온배너에 **In FIPS Compliant Mode(FIPS** 준수모드**)** 가표시됩니다.

인증서가져오기

다음절차는인증서를가져와 XenMobile 에서 FIPS 를구성하는방법을설명합니다. 이는 VMware 하이퍼바이저를사용하는데 필요합니다.

SQL 사전요구사항

1. XenMobile 에서 SQL 인스턴스로의연결은보안되어야하며 SQL Server 2012 또는 SQL Server 2014 버전이어야 합니다. 연결보안에대한자세한내용은 Microsoft Management Console 을사용하여 SQL Server 인스턴스에대해 SSL 암호화를활성화하는방법을참조하십시오.
2. 서비스가제대로다시시작되지않으면다음을확인합니다. **Services.msc** 를엽니다.
   a) SQL Server 서비스에사용되는로그온계정정보를복사합니다.
   b) SQL Server 에서 MMC.exe 를엽니다.
   c) 파일 **>** 스냅인추가**/**제거로이동한후해당인증서항목을두번클릭하여인증서스냅인을추가합니다. 마법사의두페이지에서컴퓨터계정과로컬컴퓨터를선택합니다.
   d) 확인을클릭합니다.
   e) 인증서 **(**로컬컴퓨터**) >** 개인 **>** 인증서를확장하여가져온 SSL 인증서를찾습니다.
   f) 가져온인증서를마우스오른쪽단추로클릭한후 (SQL Server 구성관리자에서선택) 모든작업 **>** 개인키관리를클릭합니다.
   g) 그룹또는사용자이름아래에서 추가를클릭합니다.
   h) 앞단계에서복사한 SQL 서비스계정이름을입력합니다.
   i) 모든권한허용옵션을선택취소합니다. 기본적으로서비스계정은모든권한과읽기권한을둘다갖지만개인키를읽는권한만필요합니다.
   j) **MMC** 를닫고 SQL 서비스를시작합니다.
3. SQL 서비스가제대로시작되는지확인합니다.

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. 로컬서버의웹브라우저에서.cer 위치로이동합니다 (`https://localhost/certname.cer`). 루트인증서텍스트가브라우저에나타납니다.
8. 사용중인웹브라우저에루트인증서가표시되지않을경우다음과같이 IIS 서버에서 ASP 를사용하도록설정되어있는지확인합니다.
   a) 서버관리자를엽니다.
   b) 관리 **>** 역할및기능추가에서마법사로이동합니다.
   c) 서버역할에서 웹서버 **(IIS)**, 웹서버, 응용프로그램개발을차례로확장한후 **ASP** 를선택합니다.
   d) 설치가완료될때까지 다음을클릭합니다.
9. `https://localhost/cert.cer`로이동합니다.

   자세한내용은 웹서버 (IIS)를참조하십시오.

   > 참고**:**
   >
   > 이절차에 CA 의 IIS 인스턴스를사용할수있습니다.

초기 **FIPS** 구성시루트인증서가져오기

명령줄콘솔에서처음으로 XenMobile 구성단계를완료하는경우다음설정을완료하여루트인증서를가져와야합니다. 설치단계에대한자세한내용은 XenMobile 설치를참조하십시오.

- 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 클라이언트속성을참조하십시오.

클러스터링구성

March 19, 2021

클러스터링을구성하려면 Citrix ADC 에다음두부하분산가상 IP 주소를구성합니다.

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

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

사전요구사항

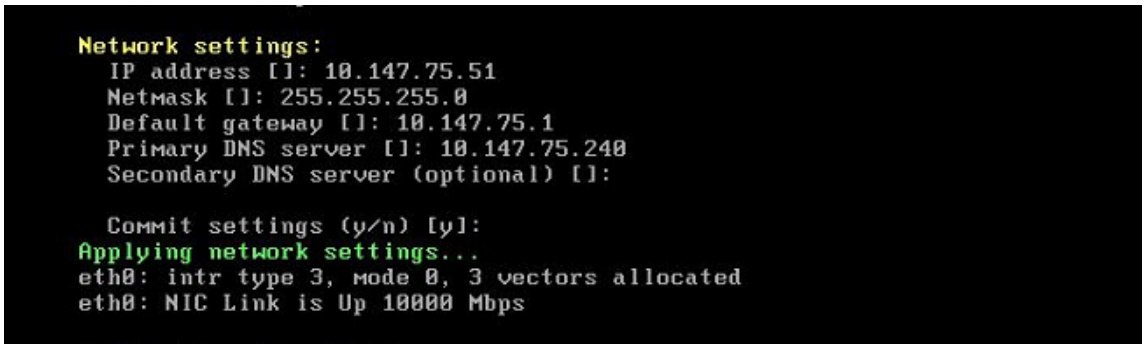
- 필요한 XenMobile 노드가완전히구성되어있어야합니다.
- 모든클러스터노드와 XenMobile 데이터베이스에 NTP 를구성합니다. 클러스터링이올바르게작동하려면이러한모든서버의시간이동일해야합니다.
- MDM 부하분산장치용공용 IP 주소하나와 MAM 용사설 IP 주소하나
- 서버인증서
- Citrix Gateway 가상 IP 주소에사용할가용 IP 주소하나
- 클러스터설치및 MDM 전용또는엔터프라이즈모드 (MDM+MAM) 에서 XenMobile 을배포한경우: 모든 Citrix ADC MDM 부하분산장치, 즉포트 8443 및 443 에대해설정된가상서버에 **Source IP persistence(**소스 **IP** 지속성**)** 를사용하도록 Citrix ADC 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 아키텍처를참조하십시오.

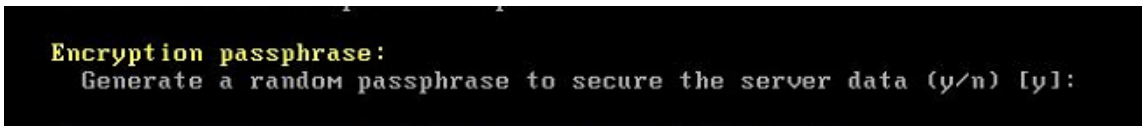
XenMobile 클러스터노드설치

필요한노드수에따라 XenMobile VM 을만듭니다. 새 VM 이동일한데이터베이스를가리키도록하고동일한 PKI 인증서암호를제공합니다.

1. 새 VM 의명령줄콘솔을열고관리자계정에대한새암호를입력합니다.
2. 다음그림에표시된것과같이네트워크구성세부정보를제공합니다.

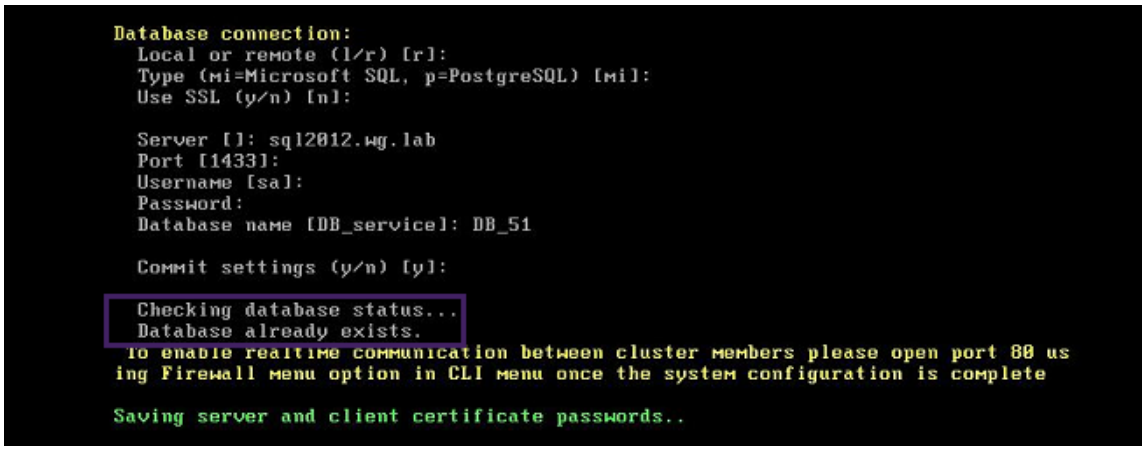


3. 데이터보호를위해기본암호를사용하려면 **y** 를입력합니다. 또는 **n** 을입력한후새암호를입력합니다.

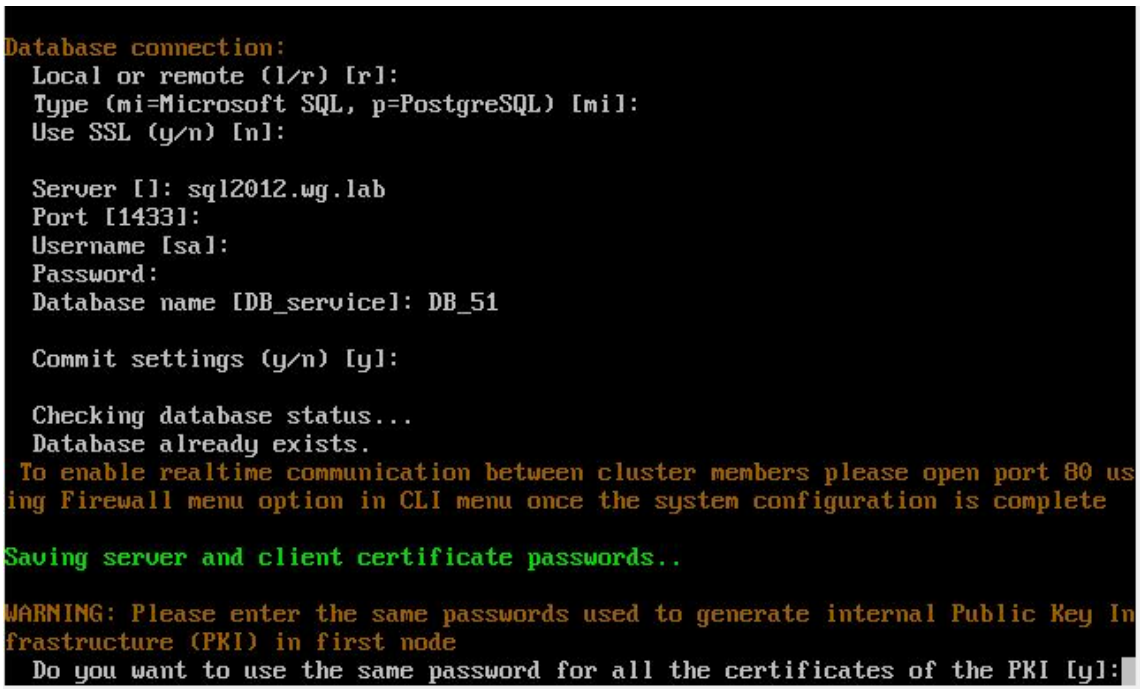


4. FIPS 를사용하려면 **y** 를입력하고그렇지않으면 **n** 을입력합니다.

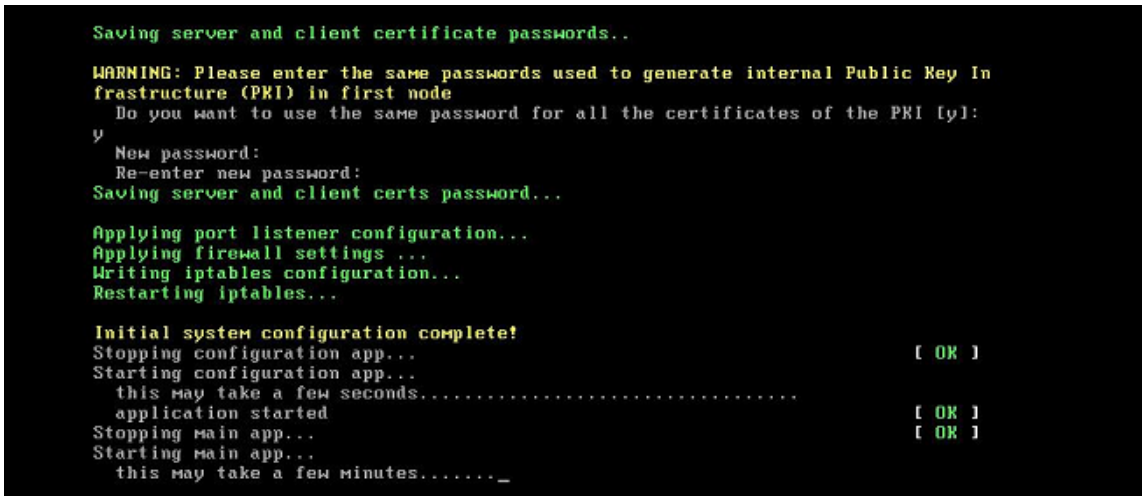
5. 이전에완벽하게구성된 VM 이가리키는동일한데이터베이스를가리키도록데이터베이스를구성합니다. “Database already exists(데이터베이스가이미있습니다)” 라는메시지가표시됩니다.



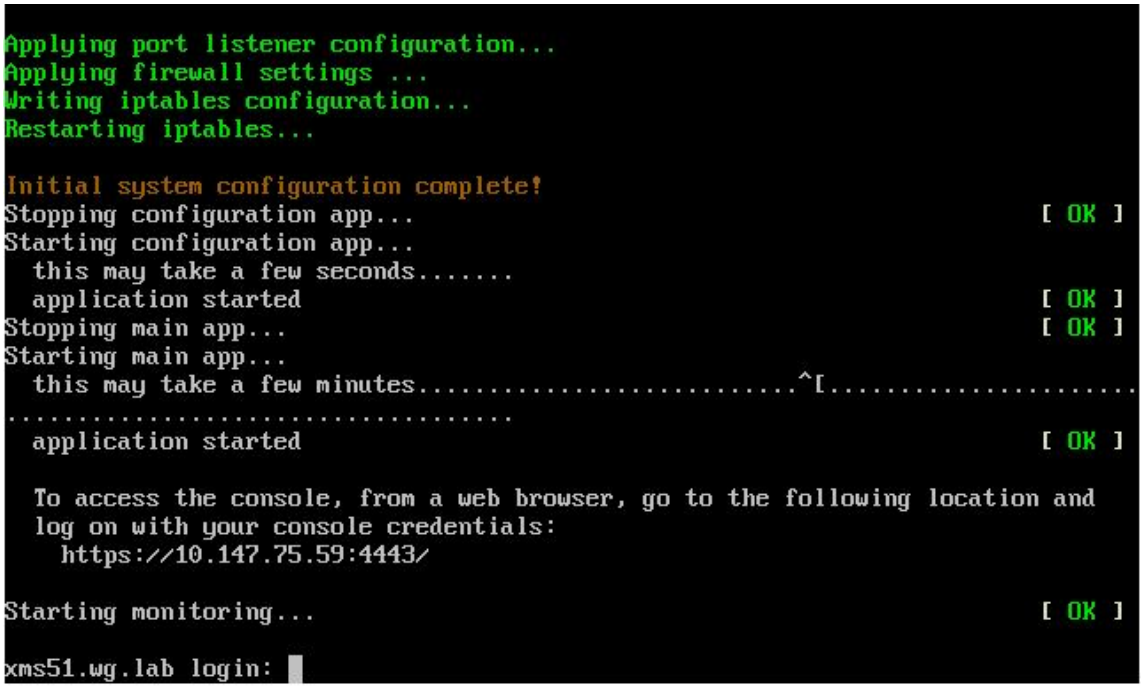
6. 첫번째 VM 에대해제공한것과동일한인증서암호를입력합니다.



암호를입력하면두번째노드에대한초기구성이완료됩니다.



7. 구성이완료되면서버가다시시작되고로그온대화상자가나타납니다.

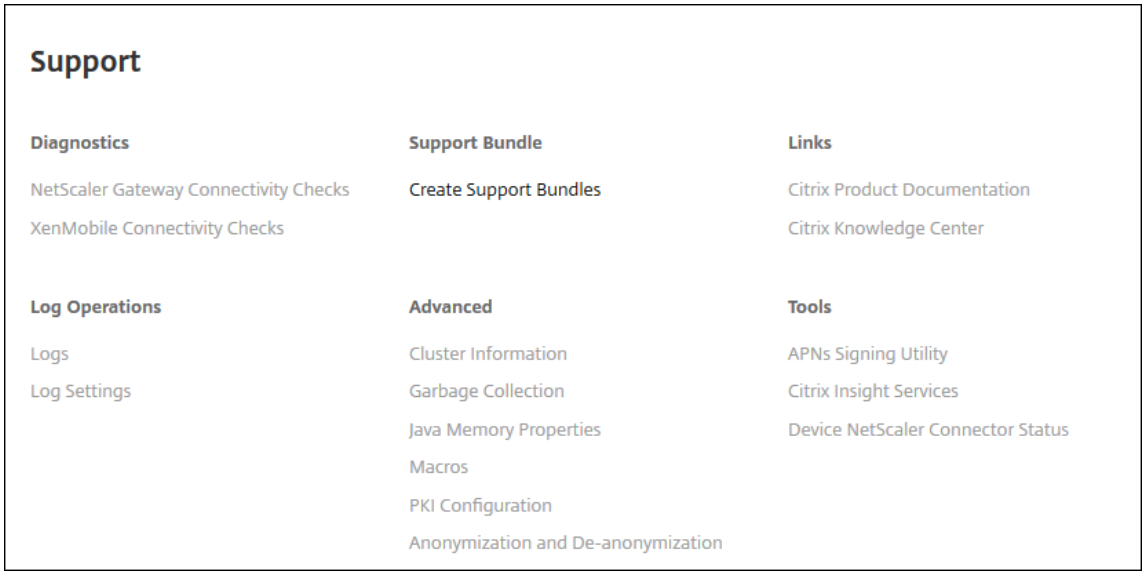


> 참고:
>
> 로그온대화상자는첫번째 VM 의로그온대화상자와동일합니다. 두대화상자가일치하는것을통해두 VM 이동일한데이터베이스서버를사용한다는것을확인할수있습니다.

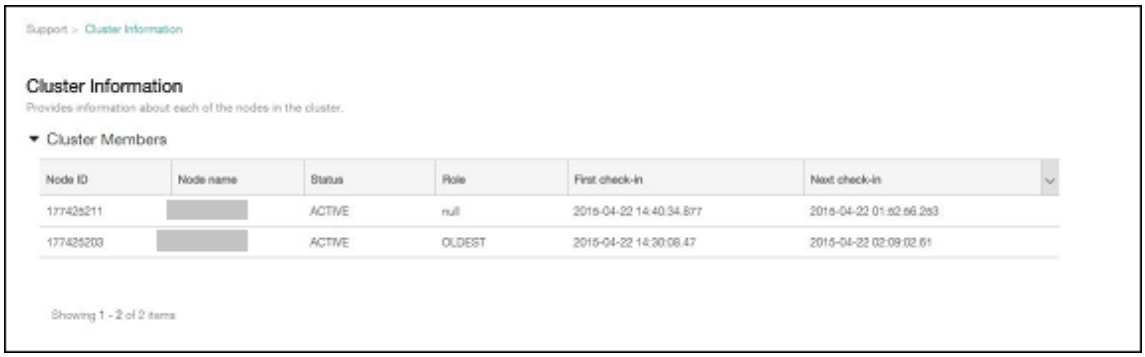
8. XenMobile 의 FQDN(정규화된도메인이름) 을사용하여웹브라우저에서 XenMobile 콘솔을엽니다.
9. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다.

지원페이지가열립니다.

10. 고급아래에서 클러스터정보를클릭합니다.



클러스터구성원, 장치연결정보, 작업등을포함하여클러스터에대한모든정보가나타납니다. 이제새노드가클러스터의구성원이됩니다.

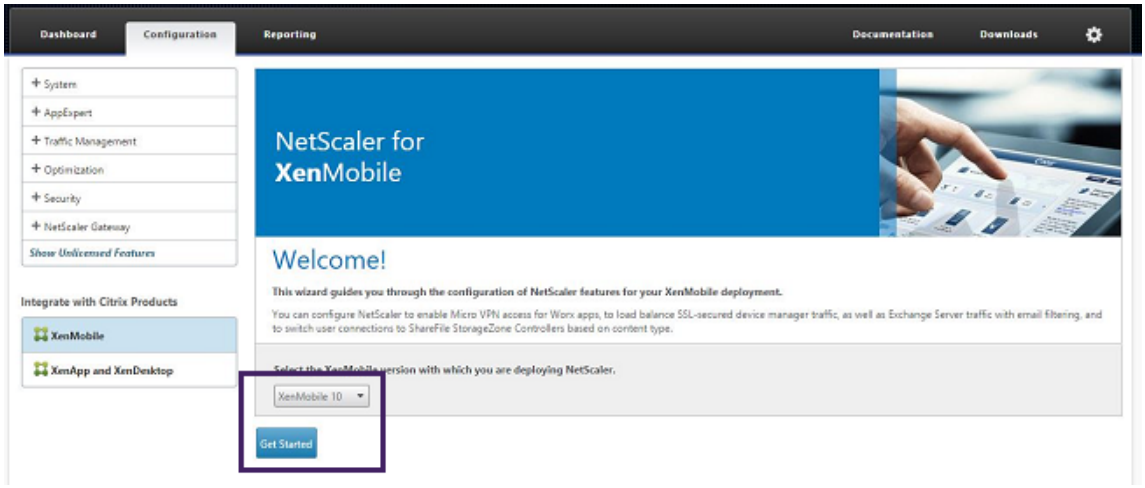


동일한단계를수행하여다른노드를추가할수있습니다. 클러스터에추가된첫번째노드는 **OLDEST** 역할을갖습니다. 그후에추가된노드에는 **NONE** 또는 **null** 역할이표시됩니다.

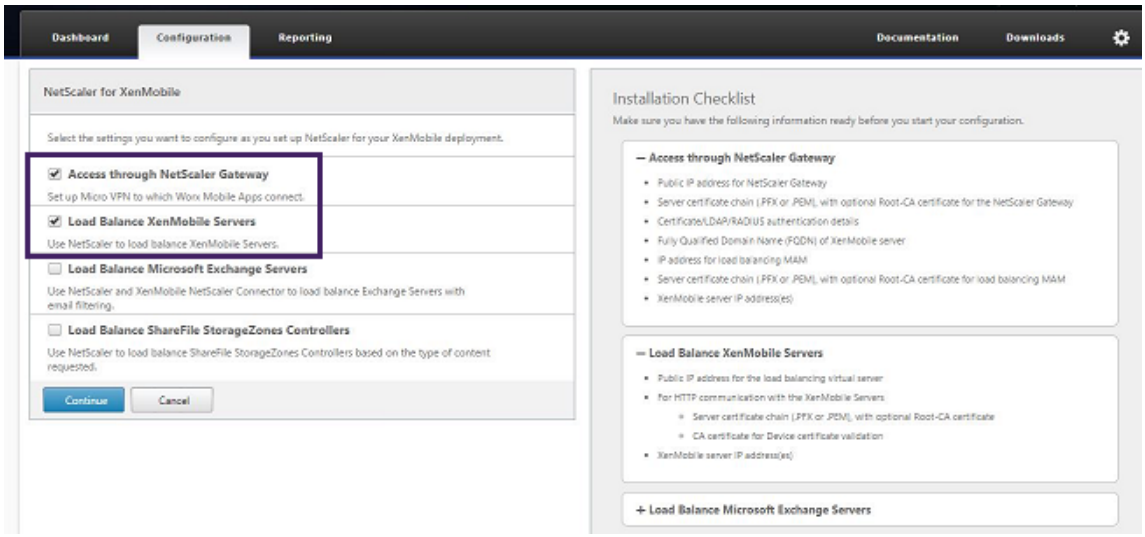
Citrix ADC 에서 **XenMobile** 클러스터에대한부하분산을구성하려면

필요한노드를 XenMobile 클러스터의구성원으로추가한후에는노드가클러스터에액세스할수있도록부하를분산합니다. 부하분산을수행하려면 Citrix ADC 에서사용할수있는 XenMobile 마법사를실행합니다. 다음단계는마법사를실행하여 XenMobile 의부하를분산하는방법을설명합니다.

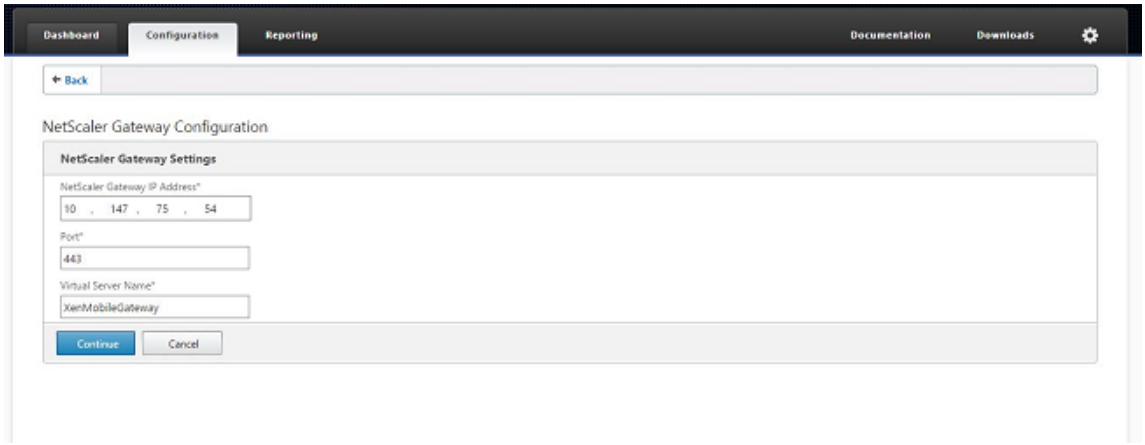
1. Citrix ADC 에로그온합니다.
2. Configuration(구성) 탭에서 **XenMobile** 을클릭하고 **Get Started(**시작**)** 를클릭합니다.



3. **Citrix Gateway** 를통해액세스확인란과 **XenMobile Server** 부하분산확인란을선택한후 계속을클릭합니다.

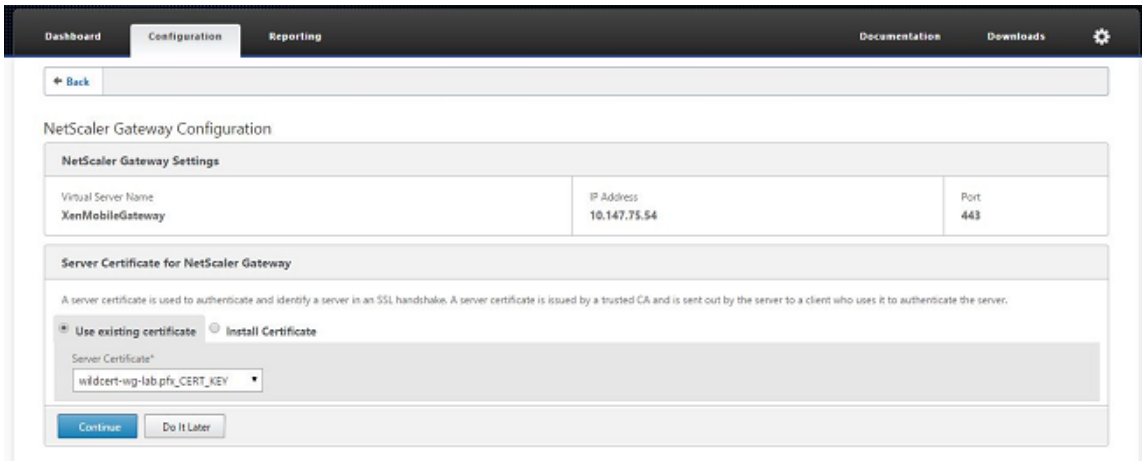


4. Citrix Gateway 의 IP 주소를입력하고 **Continue(**계속**)** 를클릭합니다.

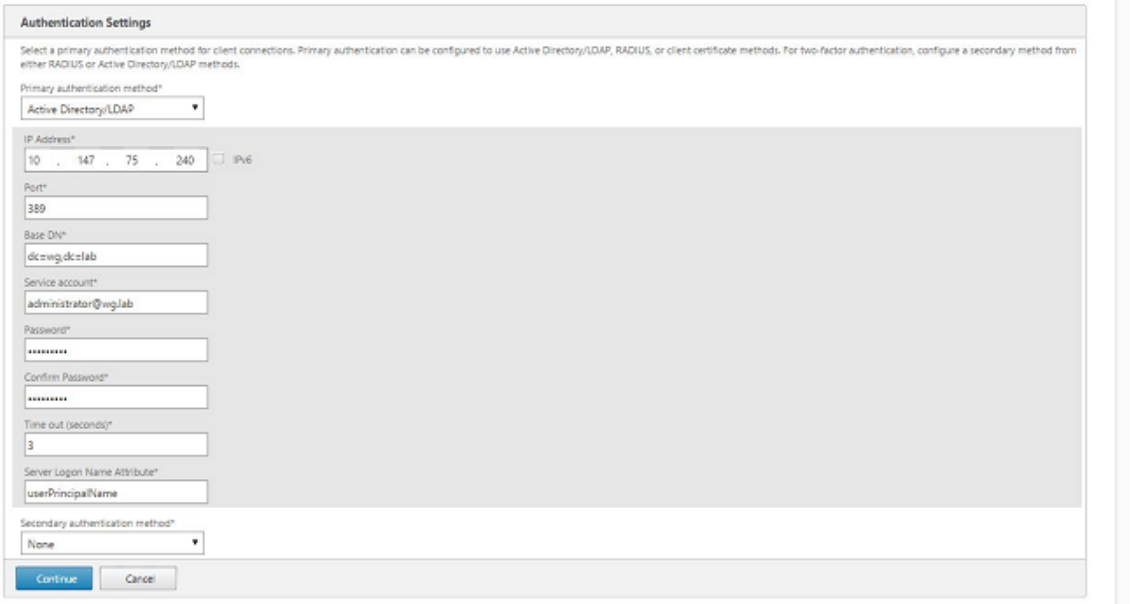


5. 다음중하나를수행하여서버인증서를 Citrix Gateway 가상 IP 주소에바인딩한후 **Continue(**계속**)** 를클릭합니다.
   - **Use existing certificate(**기존인증서사용**)** 에서, 목록에서해당서버인증서를선택합니다.

- **Install Certificate(**인증서설치**)** 탭을클릭하여새서버인증서를업로드합니다.

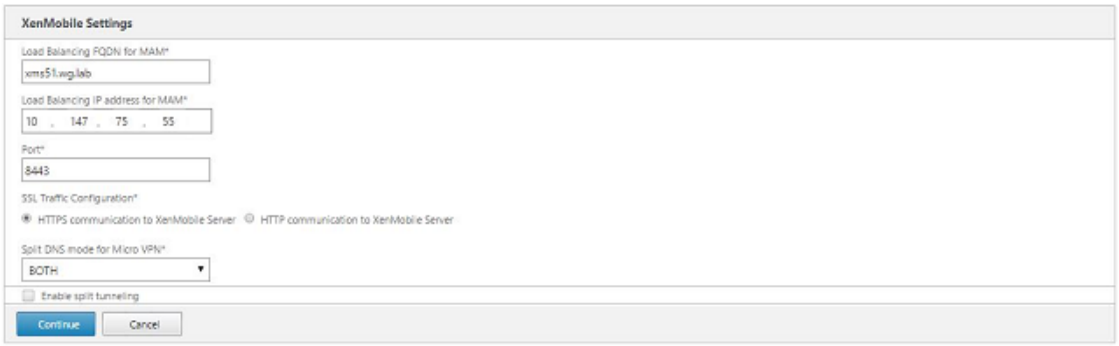


6. 인증서버세부정보를입력하고 **Continue(**계속**)** 를클릭합니다.



> 참고:
>
> Server Logon Name Attribute(서버로그온이름특성) 가 XenMobile LDAP 구성에서지정한것과동일해야합니다.

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

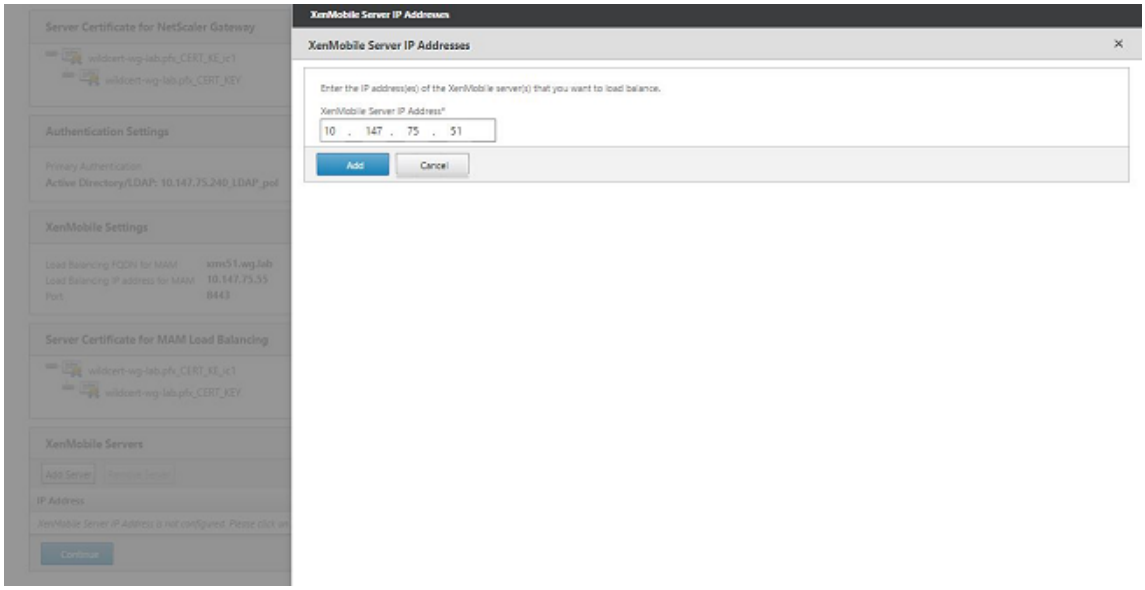


> 참고:
>
> MAM 부하분산가상 IP 주소의 FQDN 과 XenMobile 의 FQDN 이동일해야합니다.

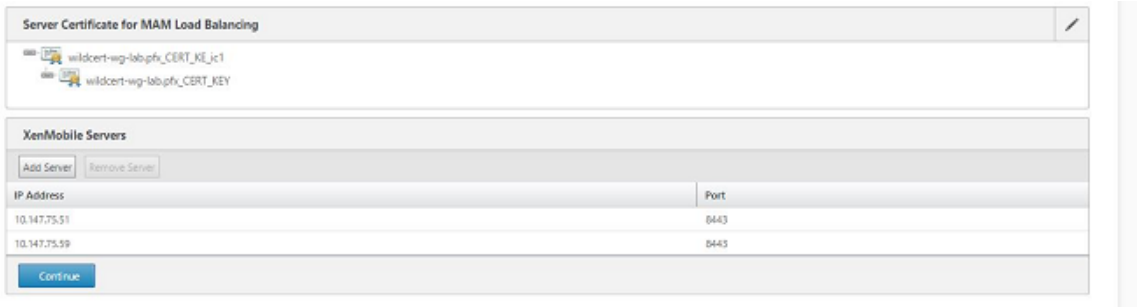
8. SSL 브리지모드 (HTTPS) 를사용하려는경우 **HTTPS communication to XenMobile Server(XenMobile** 서버에대한 **HTTPS** 통신**)** 를선택합니다. 그러나 SSL 오프로드를사용하려는경우앞의그림에나온것처럼 **HTTP communication to XenMobile Server(XenMobile Server** 에대한 **HTTP** 통신**)** 를선택합니다. 이문서에서는 SSL 브리지모드 (HTTPS) 를선택했습니다.
9. MAM 부하분산가상 IP 주소에대한서버인증서를바인딩하고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

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

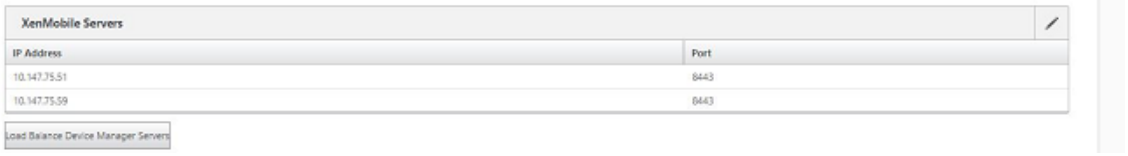
11. XenMobile 노드의 IP 주소를입력하고 Add(추가) 를클릭합니다.



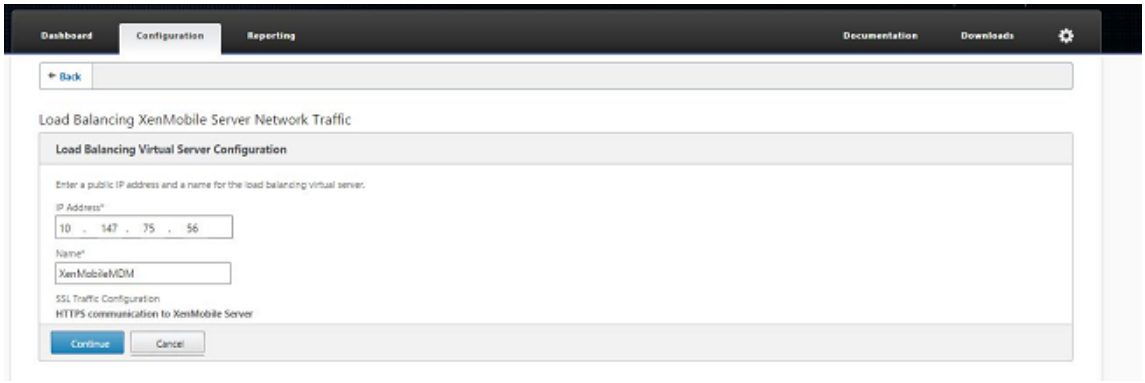
12. 10-11 단계를반복하여 XenMobile 클러스터의일부인 XenMobile 노드를추가합니다. 추가한모든 XenMobile 노드가표시됩니다. Continue(계속) 을클릭합니다.



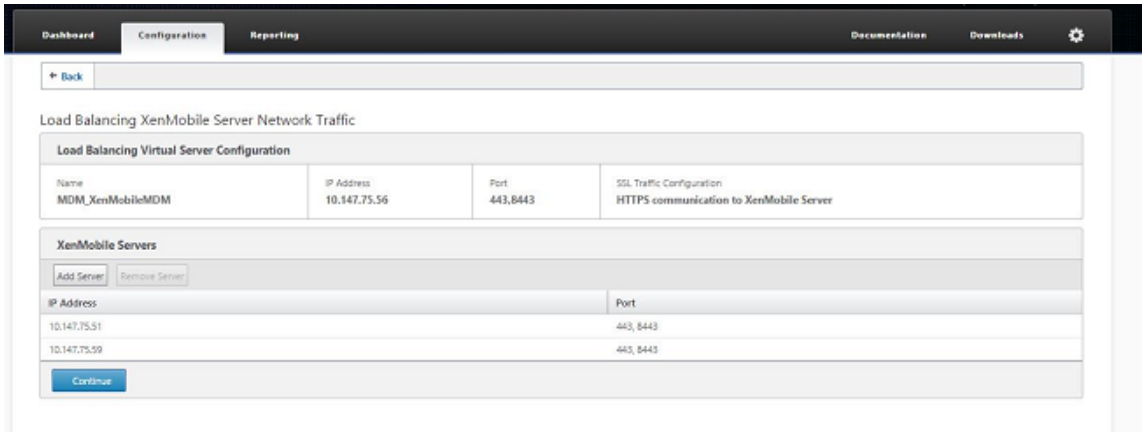
13. **Load Balance Device Manager Servers(**부하분산장치관리자서버**)** 를클릭하여 MDM 부하분산구성을계속합니다.



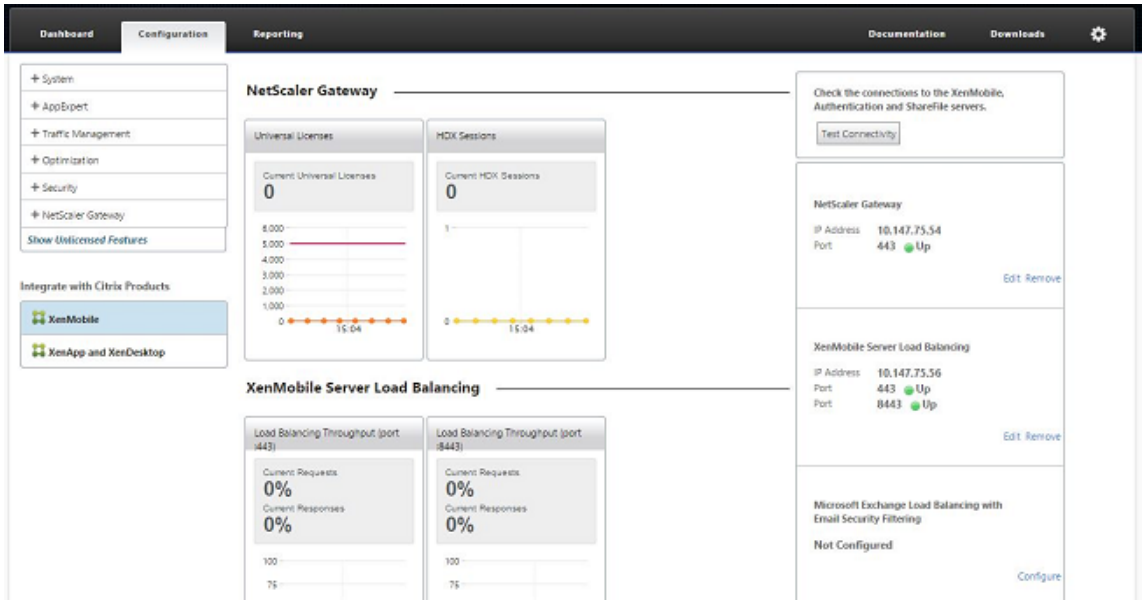
14. MDM 부하분산 IP 주소에사용할 IP 주소를입력하고 **Continue(**계속**)** 를클릭합니다.



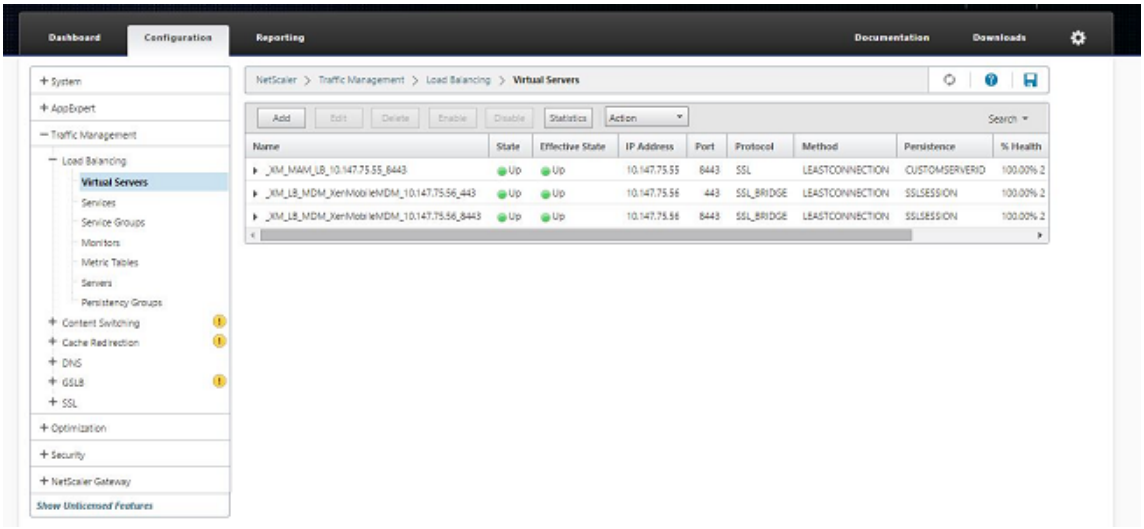
15. XenMobile 노드가목록에표시되면 **Continue(**계속**)** 를누른다음 Done(완료) 을클릭하여프로세스를마칩니다.



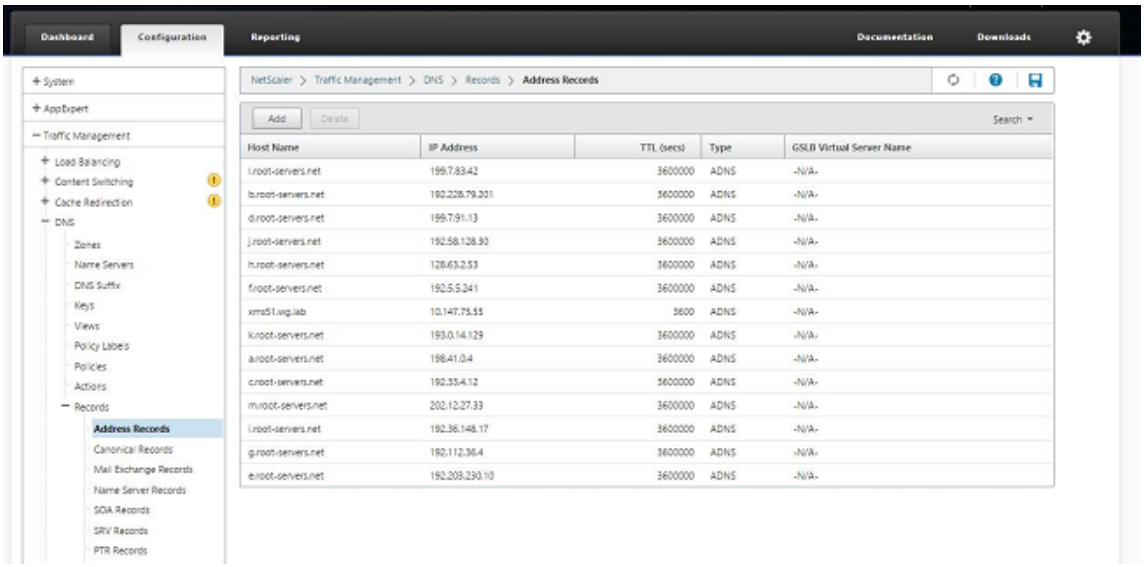
XenMobile 페이지에가상 IP 주소상태가표시됩니다.



16. 가상 IP 주소가제대로작동하는지확인하기위해 Configuration(구성) 탭을클릭하고 **Traffic Management(**트래픽관리**) > Load Balancing(**부하분산**) > Virtual Servers(**가상서버**)** 로이동합니다.



Citrix ADC 의 DNS 항목이 MAM 부하분산가상 IP 주소를가리키는것을볼수있습니다.



재해복구가이드

January 5, 2022

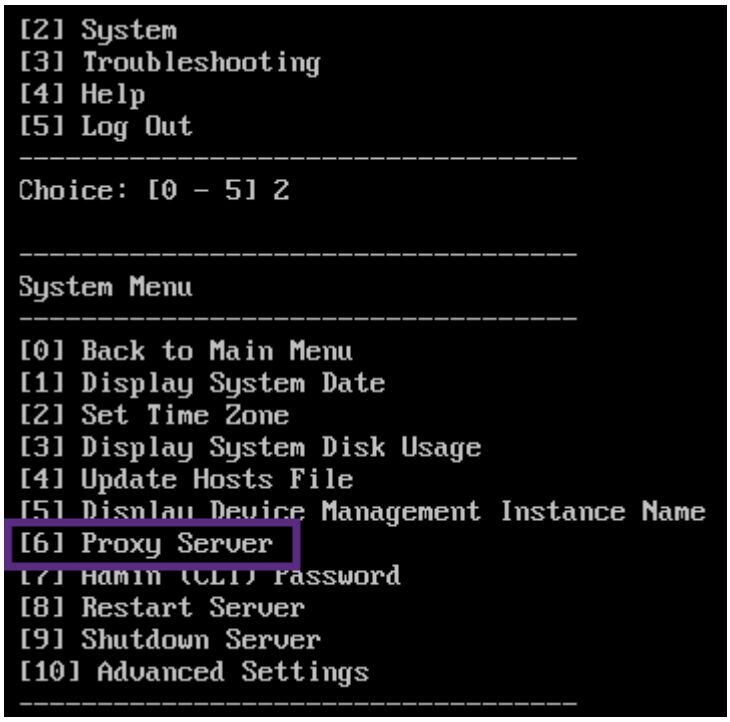
재해복구를위해활성/수동장애조치 (failover) 전략을사용하여여러사이트가포함된 XenMobile 배포를설계하고구성할수있습니다. 자세한내용은 XenMobile 배포안내서 재해복구 문서를참조하십시오.

프록시서버사용

January 5, 2022

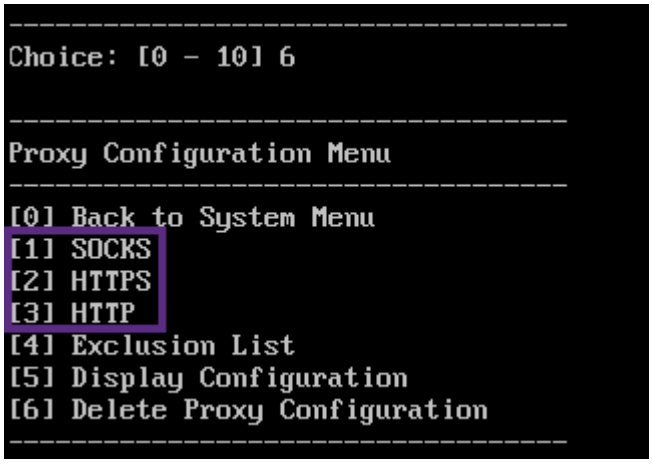
아웃바운드인터넷트래픽을제어하려면 XenMobile 에서해당트래픽을처리할프록시서버를설정하면됩니다. 프록시서버는 CLI(명령줄인터페이스) 를통해설정합니다. 프록시서버를설정하려면시스템을다시시작해야합니다.

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



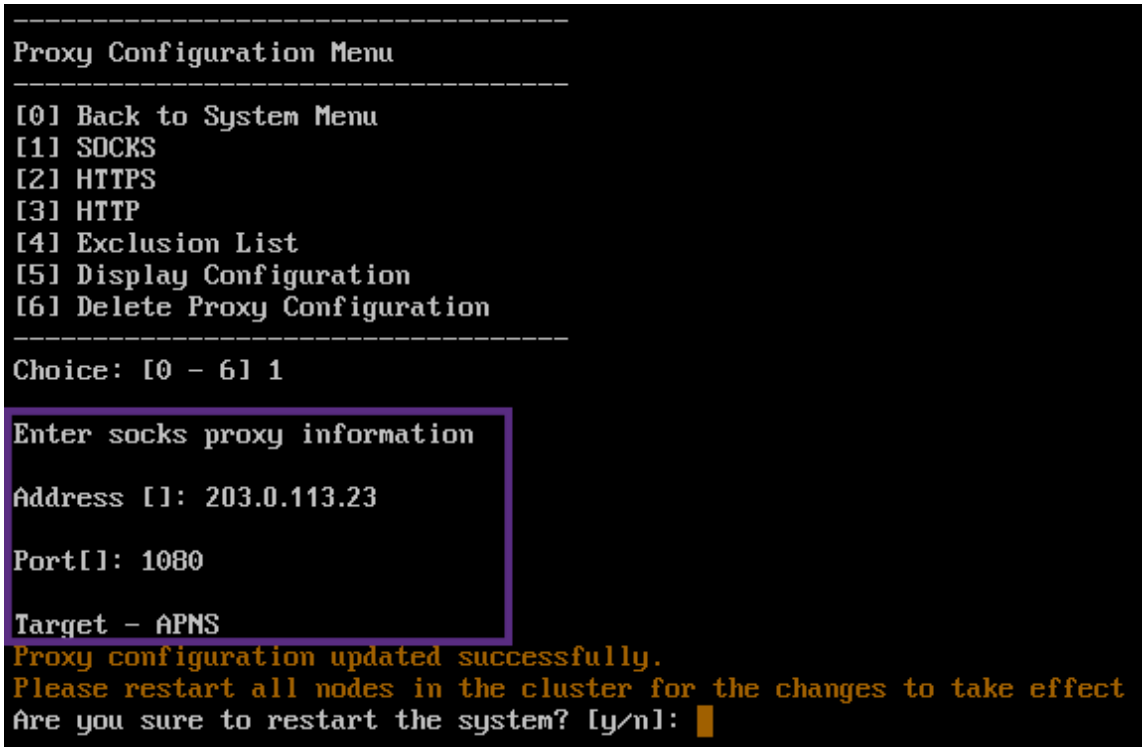
3. 프록시구성메뉴에서 **1** 을입력하여 SOCKS 를선택합니다.

   이설정을저장하기전에 HTTPS 도구성해야합니다. 동일한구성에서 SOCKS 및 HTTPS 설정을저장하지않으면프록시가작동하지않습니다.

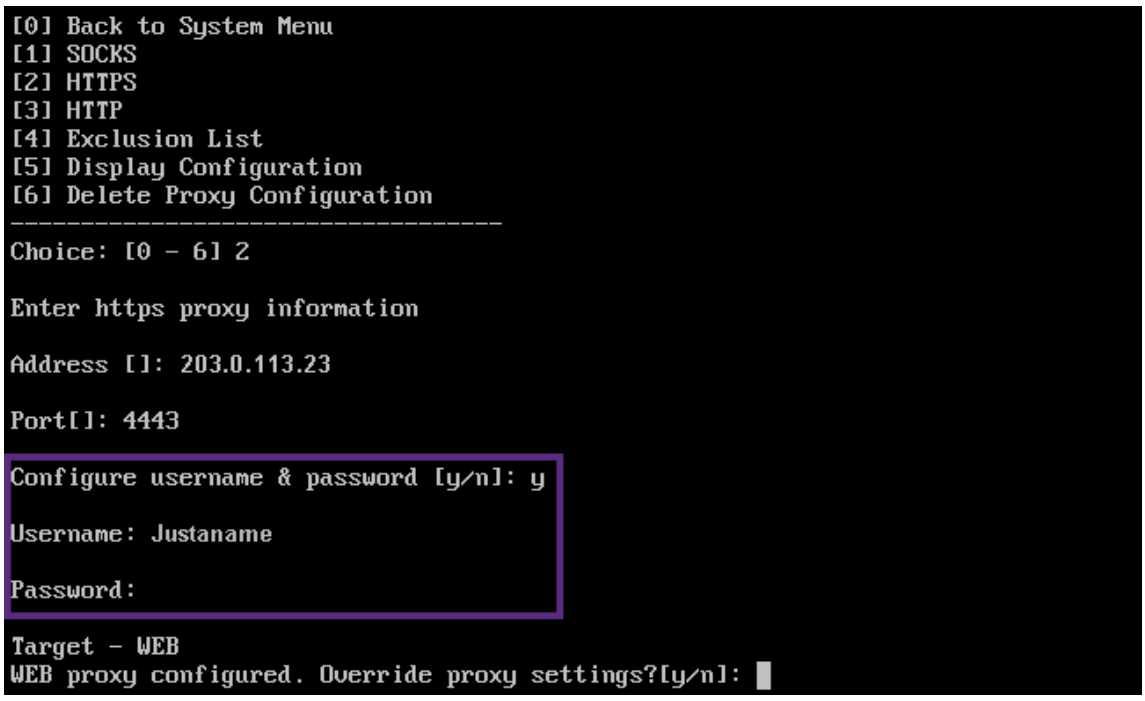


4. 프록시서버 IP 주소, 포트번호및대상을입력합니다. 각프록시서버유형에대해지원되는대상유형은다음표를참조하십시오.

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



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



7. **y** 를입력하여설정을저장합니다.

SQL Server 구성

January 5, 2022

온-프레미스 XenMobile Server 에서 SQL Server 에연결하는경우다음드라이버중하나를사용할수있습니다.

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

다음의경우 jTDS 드라이버가기본드라이버입니다.

- XenMobile Server 를온-프레미스로설치합니다.
- jTDS 드라이버를사용하도록구성된 XenMobile Server 에서업그레이드합니다.

XenMobile 은두드라이버에대해 SQL Server 인증또는 Windows 인증을지원합니다. 이러한인증및드라이버조합에대해 SSL 을켜거나끌수있습니다.

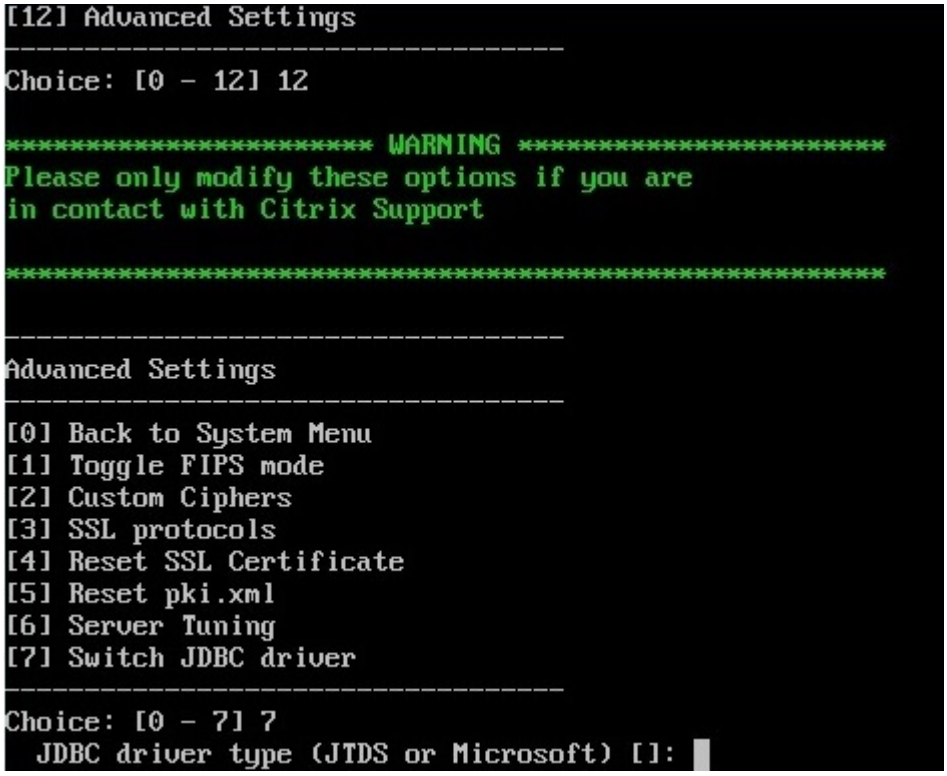
Windows 인증과함께 Microsoft JDBC 드라이버를사용하는경우드라이버에 Kerberos 통합인증이사용됩니다. XenMobile 은 Kerberos 에접속하여 Kerberos KDC(키배포센터) 세부정보를가져옵니다. 필요한세부정보가제공되지않는경우 XenMobile CLI 에 Active Directory 서버의 IP 주소를입력하라는메시지가표시됩니다.

jTDS 드라이버를 JDBC 드라이버로전환하려면모든 XenMobile Server 노드에 SSH 로연결한후 XenMobile CLI 를사용하여구성합니다. 단계는다음과같이현재 jTDS 드라이버구성에따라다릅니다.

Microsoft JDBC 로전환 (SQL Server 인증)

이러한단계를완료하려면 SQL Server 사용자이름과암호가필요합니다.

1. 모든 XenMobile Server 노드에 SSH 로연결합니다.
2. XenMobile CLI 메인메뉴에서 **2** 를입력하여 시스템메뉴를선택합니다.
3. **12** 를입력하여고급설정을선택합니다.
4. **7** 을입력하여 JDBC 드라이버전환을선택한후 **m** 을입력하여 Microsoft 를선택합니다.



5. 메시지가표시되면 **y** 를입력하여 SQL 인증을선택하고 SQL Server 사용자이름과암호를입력합니다.
6. 각 XenMobile Server 노드에대해단계를반복합니다.
7. 각 XenMobile Server 노드를다시시작합니다.

Microsoft JDBC 로전환 (SSL 꺼짐, Windows 인증)

이러한단계를완료하려면 Active Directory 사용자이름및암호 Kerberos KDC 영역및 KDC 사용자이름이필요합니다.

1. 모든 XenMobile Server 노드에 SSH 로연결합니다.
2. XenMobile CLI 메인메뉴에서 **2** 를입력하여 시스템메뉴를선택합니다.
3. **12** 를입력하여고급설정을선택합니다.
4. **7** 을입력하여 JDBC 드라이버전환을선택한후 **m** 을입력합니다.
5. SQL Server 인증의사용여부를묻는메시지가표시되면 **n** 을입력합니다.
6. 메시지가표시되면 SQL Server 에구성된 Active Directory 사용자이름과암호를입력합니다.
7. XenMobile 에서 Kerberos KDC 영역이자동으로검색되지않으면 SQL Server FQDN 을비롯한 KDC 세부정보를묻는메시지가표시됩니다.
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.

SQL Server 에서 Windows 인증을사용하는경우 Windows Active Directory 에서데이터베이스암호를변경해야합니다. 그런다음데이터베이스서버의데이터베이스관리자계정을새로고쳐암호변경을동기화합니다. 그러면다음과같이 XenMobile 에서암호를변경할수있습니다.

> 중요:
>
> - XenMobile 의데이터베이스암호변경을위해예약된유지관리기간을계획합니다. 암호는시스템중단시간에변경해야합니다.
> - 암호를변경할때는모든 XenMobile 노드가네트워크에연결되어있는지확인하십시오. 암호를변경한후 XenMobile 을다시시작합니다.
>
>   If you don't restart XenMobile after a password change, XenMobile goes into recovery mode. In that case, revert to the old password in SQL server, restart XenMobile, and change the password again.

1. 모든 XenMobile Server 노드가실행중인지확인합니다. 클러스터링된환경의경우모든노드를가동합니다.
2. Citrix ADC 부하분산장치에서가상서버를사용하지않도록설정하여 XenMobile 에대한수신장치트래픽을차단합니다.
3. SQL Server 에서데이터베이스암호를변경하려면: XenMobile CLI 에로그인하고 **Configuration > Database** 로이동한다음메시지가표시되면변경된암호를입력합니다.

```
Server []: <ipAddress>
Port [1433]: 1433
Username [sa]: <userName>
Password: <****>
<!--NeedCopy-->
```

4. **Y** 를입력하여서버를다시시작합니다.
5. 클러스터의다른모든노드에대해 3 단계와 4 단계를반복합니다.
6. Citrix ADC 부하분산장치에서가상서버를사용하도록설정하여수신장치트래픽의차단을해제합니다.

서버속성

August 12, 2022

XenMobile 에는서버전체작업에적용되는다수의속성이있습니다. 이문서에서는여러서버속성을설명하고서버속성을추가, 편집 또는삭제하는방법을자세히설명합니다.

일부속성은사용자지정키입니다. 사용자지정키를추가하려면 추가를클릭한다음 키에서 사용자지정키를선택합니다.

일반적으로구성되는속성에대한자세한내용은 XenMobile 가상안내서에서 서버속성을참조하십시오.

서버속성정의

Add Device Always(항상장치추가**)**

- **true** 인경우 XenMobile 이등록에실패한장치도 XenMobile 콘솔에추가합니다. 따라서등록을시도한장치를볼수있습니다. 기본값은 **false** 입니다.

AG Client Cert Issuing Throttling Interval(AG 클라이언트인증서발급제한간격**)**

- 인증서생성사이의유예기간입니다. 이간격은 XenMobile 이짧은기간에장치용인증서를여러개생성하는것을방지합니다. 이값은변경하지않는것이좋습니다. 기본값은 **30** 분입니다.

Audit Log Cleanup Execution Time(감사로그정리실행시간**)**

- 감사로그정리를시작하는시간이며 HH:MM AM/PM 형식을사용합니다. 예: 04:00 AM. 기본값은 **02:00 AM** 입니다.

Audit Log Cleanup Interval (in Days)(감사로그정리간격 **(**일**))**

- XenMobile 에감사로그가유지되는일수입니다. 기본값은 **1** 입니다.

Audit Logger(감사로거**)**

- **False** 인경우 UI(사용자인터페이스) 이벤트를기록하지않습니다. 기본값은 **False** 입니다.

Audit Log Retention (in Days)(감사로그유지 **(**일**))**

- XenMobile 에감사로그가유지되는일수입니다. 기본값은 **7** 입니다.

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

- 느린 LDAP 응답을보완하려면다음사용자지정키의서버속성을추가하는것이좋습니다.
  - 키: 사용자지정키
  - 키: **auth.ldap.connect.timeout**
  - 값: **60000**

- 표시이름: **auth.ldap.connect.timeout**
- 설명: **LDAP** 연결시간초과
- 키: 사용자지정키
- 키: **auth.ldap.read.timeout**
- 값: **60000**
- 표시이름: **auth.ldap.read.timeout**
- 설명: **LDAP** 읽기시간제한

인증서갱신 **(**초**)**

- XenMobile 이인증서갱신을시작하는인증서가만료되기전의시간 (초) 입니다. 예를들어인증서가 12 월 30 일에만료될예정이고이속성이 30 일로설정된경우장치가 12 월 1 일에서 12 월 30 일사이에연결하면 XenMobile 이인증서갱신을시작합니다. 기본값은 **2592000** 초 (30 일) 입니다.

연결시간제한

- XenMobile 이장치에대한 TCP 연결을종료하기전까지의세션비활성시간제한 (분) 입니다. 세션은열린상태로유지됩니다. Android 장치및원격지원에적용됩니다. 기본값은 **5** 분입니다.

Microsoft 인증서버에대한연결시간제한

- XenMobile 이인증서서버의응답을대기하는시간 (초) 입니다. 인증서서버가느리고트래픽이많은경우이값을 60 초이상으로늘립니다. 120 초후에응답하지않는인증서서버는유지관리가필요합니다. 기본값은 **15000** 밀리초 (15 초) 입니다.

기본배포채널

- XenMobile 이리소스를장치에배포하는방법을사용자수준 (**DEFAULT_TO_USER**) 또는장치수준에서결정합니다. 기본값은 **DEFAULT_TO_DEVICE** 입니다.

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

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

호스트이름확인사용안함

- 기본적으로호스트이름유효성검사는 Microsoft PKI 서버를제외한발신연결에대해활성화됩니다. 호스트이름유효성검사가실패하면서버로그에다음과같은오류가포함됩니다. “볼륨구매서버에연결할수없습니다. 호스트이름 ‘192.0.2.0’ 은 피어가제공한인증서주체와일치하지않습니다.” 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 OTAE(macOS OTAE 사용**)**

- **false** 인경우 macOS 장치에대한등록링크의사용을차단합니다. 즉, macOS 사용자는등록초대를통해서만등록할수있습니다. 기본값은 **true** 입니다.

Enable Notification Trigger(알림트리거사용**)**

- Secure Hub 클라이언트알림을사용하거나사용하지않도록설정합니다. **true** 값은알림을사용합니다. 기본값은 **true** 입니다.

force.server.push.required.apps

- 다음과같은경우에 Android 및 iOS 장치에서필수앱의강제배포를사용하도록설정합니다.
  - 사용자가새앱을업로드하고필수앱으로표시합니다.
  - 사용자가기존앱을필수앱으로표시합니다.
  - 사용자가필수앱을삭제합니다.

  - Secure Hub 업데이트가제공됩니다.

필수앱의강제배포는기본적으로 **false** 로설정됩니다. 강제배포를사용하도록설정하려면사용자지정키를만들고 값을 **true** 로설정하십시오. 강제배포중에는엔터프라이즈앱및공용앱스토어앱을포함한 MDX 지원필수앱이즉시업그레이드됩니다. 관리자가앱업데이트유예기간에대한 MDX 정책을구성하고사용자가앱을나중에업그레이드하도록선택하는경우에도업그레이드가수행됩니다.

- 키: 사용자지정키
- 키: **force.server.push.required.apps**
- 값: **false**
- 표시이름: **force.server.push.required.apps**
- 설명: 필수앱을강제로배포

ActiveSync 가허용및거부된사용자전체목록끌어오기

- XenMobile 이 ActiveSync 가허용및거부한사용자의전체목록 (기준) 을가져오는간격 (초) 입니다. 기본값은 **28800** 초입니다.

hibernate.c3p0.idle_test_period

- XenMobile Server 속성인사용자지정키는연결유효성이자동으로검사되기까지의유휴시간 (초) 을결정합니다. 다음과같이키를구성합니다. 기본값은 **30** 입니다.
- 키: 사용자지정키
- 키: **hibernate.c3p0. idle_test_period**
- 값: **30**
- 표시이름: **hibernate.c3p0. idle_test_period =*nnn***
- 설명: **Hibernate** 유휴테스트기간

hibernate.c3p0.max_size

- 이사용자지정키는 XenMobile 에서 SQL Server 데이터베이스에대해열수있는최대연결수를결정합니다. XenMobile 은이사용자지정키에지정한값을상한으로사용합니다. 필요한경우에만연결이열립니다. 데이터베이스서버의용량에따라설정을결정합니다. 자세한내용은 XenMobile 작업조정을참조하십시오. 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. 다음과같이키를구성합니다. 기본값은 **100** 입니다.
- 키: **hibernate.c3p0.min_size**
- 값: **100**
- 표시이름: **hibernate.c3p0.min_size**
- 설명: **SQL** 에대한 **DB** 연결

hibernate.c3p0.timeout

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

원격분석의사용여부를식별합니다

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

Inactivity Timeout in Minutes(비활성시간제한 **(**분**))**

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

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** 프로필설치**)** 을클릭해야합니다.

iOS Device Management Enrollment First Step Delayed(iOS 장치관리등록의첫번째단계지연**)**

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

iOS Device Management Enrollment First Step Delayed(iOS 장치관리등록의마지막단계지연**)**

- 이속성값은장치등록중에 MDM 프로필이설치된후장치의에이전트가시작되기까지대기해야하는시간을지정합니다. 이속성은네트워크대기시간또는속도문제가있는경우에만편집하는것이좋습니다. 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 프로필서비스및 XenMobile iOS 에이전트 ID 에대한개인키의크기를정의합니다. 기본값은 **1024** 입니다.

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

- XenMobile 이인증서갱신을시작하는인증서가만료되기전의시간 (일) 을지정합니다. 예를들어인증서가 10 일후에만료되고이속성이 **10** 일인경우장치가만료 9 일전에연결하면 XenMobile 이새인증서를발급합니다. 기본값은 **30** 일입니다.

iOS MDM APNS Private Key Password(iOS MDM APNS 개인키암호**)**

- 이속성에는 XenMobile 에서 Apple 서버로알림을푸시할때필요한 APNs 암호가포함됩니다.

Length of Inactivity Before Device Is Disconnected(장치연결을해제하기전비활성시간**)**

- XenMobile 이연결을해제하기전에장치가마지막인증부터비활성상태로있을수있는시간을지정합니다. 기본값은 **7** 일입니다.

MAM Only Device Max

- 이사용자지정키는각사용자가등록할수있는 MAM 전용장치의수를제한합니다. 다음과같이키를구성합니다. 값이 **0** 이면장치를무제한등록할수있습니다.

- 키 = **number.of.mam.devices.per.user**
- 값 = **5**
- 표시이름 = **MAM Only Device Max**
- 설명 = 각사용자가등록할수있는 **MAM** 장치수를제한합니다**.**

MaxNumberOfWorker

- 많은수의볼륨구매라이센스를가져올때사용되는스레드수입니다. 기본값은 **3** 입니다. 추가최적화가필요한경우스레드수를늘릴수있습니다. 그러나예를들어 6 과같이스레드수가커지면볼륨구매를가져올때 CPU 사용량이높아집니다.

Citrix ADC Single Sign-On

- **False** 인경우 Citrix ADC 에서 XenMobile 로의 SSO 중에 XenMobile 콜백기능이사용되지않습니다. Citrix Gateway 구성에콜백 URL 이포함되는경우 XenMobile 이콜백기능을사용하여 Citrix Gateway 세션 ID 를확인합니다. 기본값은 **False** 입니다.

Number of consecutive failed uploads(연속업로드실패수**)**

- CEIP(사용자환경개선프로그램) 업로드중에연속적으로실패한횟수를표시합니다. 업로드가실패하면값이증가합니다. 업로드가 15 회실패하면 XenMobile 이원격분석이라고도하는 CEIP 를사용하지않도록설정합니다. 자세한내용은 원격분석의사용여부를식별합니다서버속성을참조하십시오. 업로드가성공하면값이 **0** 으로재설정됩니다.

Number of Users Per Device(장치당사용자수**)**

- 동일한장치를 MDM 에등록할수있는사용자의최대수입니다. **0** 값은무제한의사용자가동일한장치를등록할수있음을의미합니다. 기본값은 **0** 입니다.

Pull of Incremental Change of Allowed and Denied Users(허용및거부된사용자의증분변경끌어오기**)**

- XenMobile 이 PowerShell 명령을실행하여 ActiveSync 장치의델타를가져올때도메인의응답을대기하는시간 (초) 입니다. 기본값은 **60** 초입니다.

Read Timeout to Microsoft Certification Server(Microsoft 인증서버에대한읽기시간제한**)**

- XenMobile 이읽기를수행할때인증서서버의응답을대기하는시간 (초) 입니다. 인증서서버가느리고트래픽이많은경우이 값을 60 초이상으로늘릴수있습니다. 120 초후에응답하지않는인증서서버는유지관리가필요합니다. 기본값은 **15000** 밀리초 (15 초) 입니다.

REST Web Services(REST 웹서비스)

- REST 웹서비스를사용합니다. 기본값은 **true** 입니다.

지정된크기의청크로장치정보를검색합니다

- 이값은장치내보내기중내부적으로다중스레드처리에사용됩니다. 값이클수록단일스레드가더많은장치를구문분석합니다. 값이작을수록더많은스레드가장치를가져옵니다. 값을줄이면내보내기및장치목록가져오기성능이향상되지만사용가능한메모리가줄어들수있습니다. 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. 서버모드의기본값은라이센스유형에관계없이 **ENT** 입니다.

XenMobile MDM Edition 라이센스가있는경우유효한서버모드는서버속성에서설정한서버모드와관계없이항상 MDM 입니다. MDM Edition 라이센스가있는경우서버모드를 MAM 또는 ENT 로설정하여앱관리를사용할수없습니다.

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

유효한서버모드는라이센스유형과서버모드의조합입니다. MDM 라이센스에유효한서버모드는서버모드설정과관계없이항상 MDM 입니다. Enterprise 및 Advanced 라이센스의경우유효한서버모드는서버모드가 **ENT** 또는 **MDM** 인경우서버모드와일치합니다. 서버모드가 **MAM** 인경우유효한서버모드는 ENT 입니다.

XenMobile 은라이센스활성화, 라이센스삭제및서버속성에서서버모드변경작업에대한서버로그에서버모드를추가합니다. 로그파일만들기및보기에대한자세한내용은 로그와 XenMobile 의로그파일보기및분석을참조하십시오.

Content Collaboration 구성유형

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

Static Timeout in Minutes(정적시간제한 **(**분**))**

- 웹서비스시간제한유형서버속성이 **STATIC_TIMEOUT** 인경우: 이속성은 XenMobile 이다음을사용한후관리자를로그아웃하기전의시간 (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** 인경우자체호스트된앱을 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** 장치초기화수행**)**

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

Exchange 의사용자만

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

VP 기준간격

- XenMobile 이 Apple 에서볼륨구매라이센스를다시가져오는최소간격입니다. 라이센스정보를새로고치면볼륨구매에서가져온앱을수동으로삭제하는것과같은모든변경내용을 XenMobile 에반영할수있습니다. 기본적으로 XenMobile 에서볼륨구매라이센스기준은최소 **720** 분마다새로고쳐집니다.

설치된볼륨구매라이센스가많은경우 (예: 50,000 개초과) Citrix 에서는라이센스가져오기의빈도및오버헤드가줄도록값을늘릴것을권장합니다. Apple 에서볼륨구매라이센스가자주변경될것으로예상되는경우 Citrix 에서는 XenMobile 에변경내용이업데이트되도록값을낮출것을권장합니다. 두기준사이의최소간격은 60 분입니다. 또한 XenMobile 은 60 분마다델타가져오기를수행하여마지막가져오기이후의변경내용을캡처합니다. 그러므로볼륨구매기준간격이 60 분인경우기준사이의간격이최대 119 분까지지연될수있습니다.

웹서비스시간제한유형

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

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

Windows WNS 채널 **-** 갱신전일수

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

Windows WNS 하트비트간격

- XenMobile 이 3 분마다 5 번장치에연결한후장치에연결하기전까지기다릴시간입니다. 기본값은 **6** 시간입니다.

XAM 일회용티켓

- OTT(일회용인증토큰) 로앱을다운로드할수있는시간 (밀리초) 입니다. 이속성은 **Android** 장치의인증되지않은앱다운로드및 **Windows** 장치의인증되지않은앱다운로드속성과함께사용됩니다. 이러한속성은인증되지않은앱다운로드를허용할지여부를지정합니다. 기본값은 **3600000** 입니다.

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

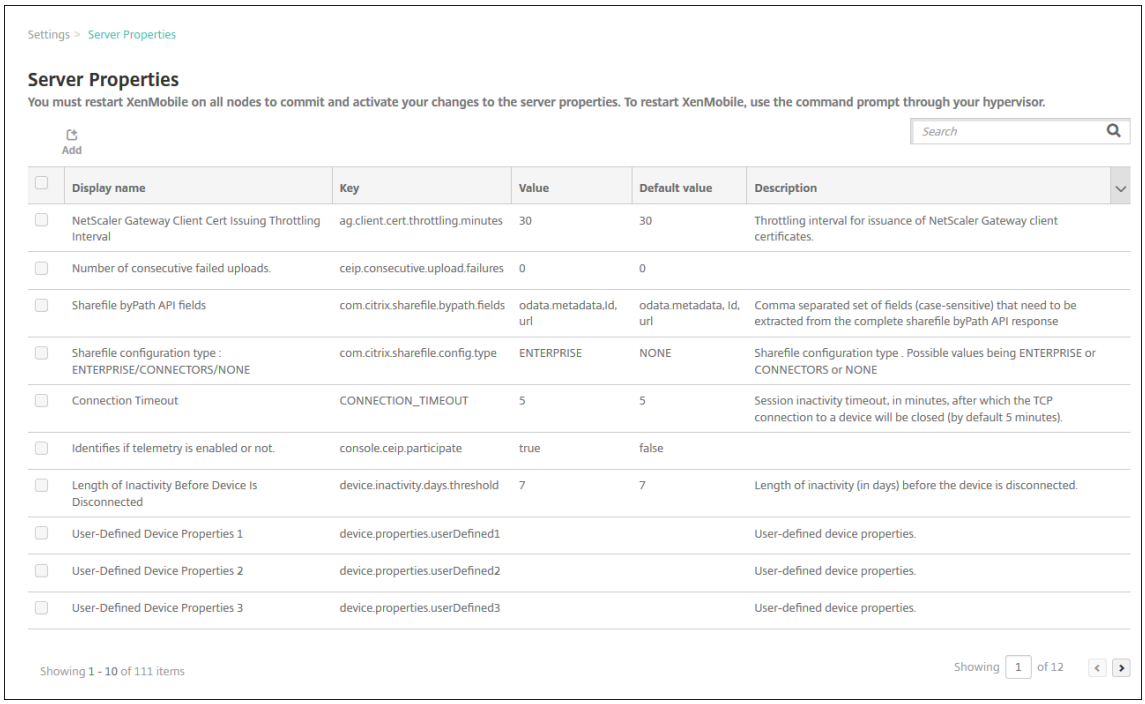
- XenMobile 자가지원포털에서비활성사용자가로그아웃되기까지의시간 (분) 입니다. 시간제한이 **0** 인경우비활성사용자가로그인상태로유지됩니다. 기본값은 **30** 입니다.

서버속성추가**,** 편집또는삭제

XenMobile 에서서버에속성을적용할수있습니다. 변경한후에는모든노드에서 XenMobile 을다시시작하여변경내용을커밋하고활성화해야합니다.

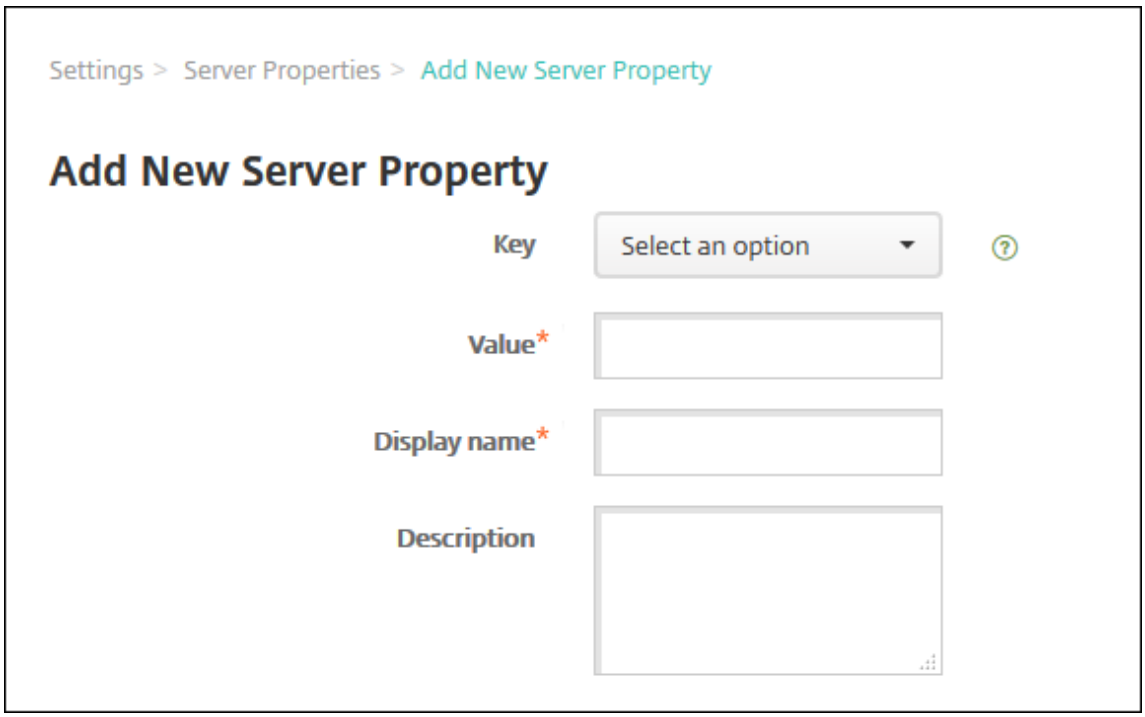
> 참고**:**
>
> XenMobile 을다시시작하려면하이퍼바이저를통해명령프롬프트를사용합니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버아래에서 서버속성을클릭합니다. 서버속성페이지가나타납니다. 이페이지에서서버속성을추가, 편집또는삭제할수있습니다.



서버속성을추가하려면

1. 추가를클릭합니다. 새서버속성추가페이지가나타납니다.



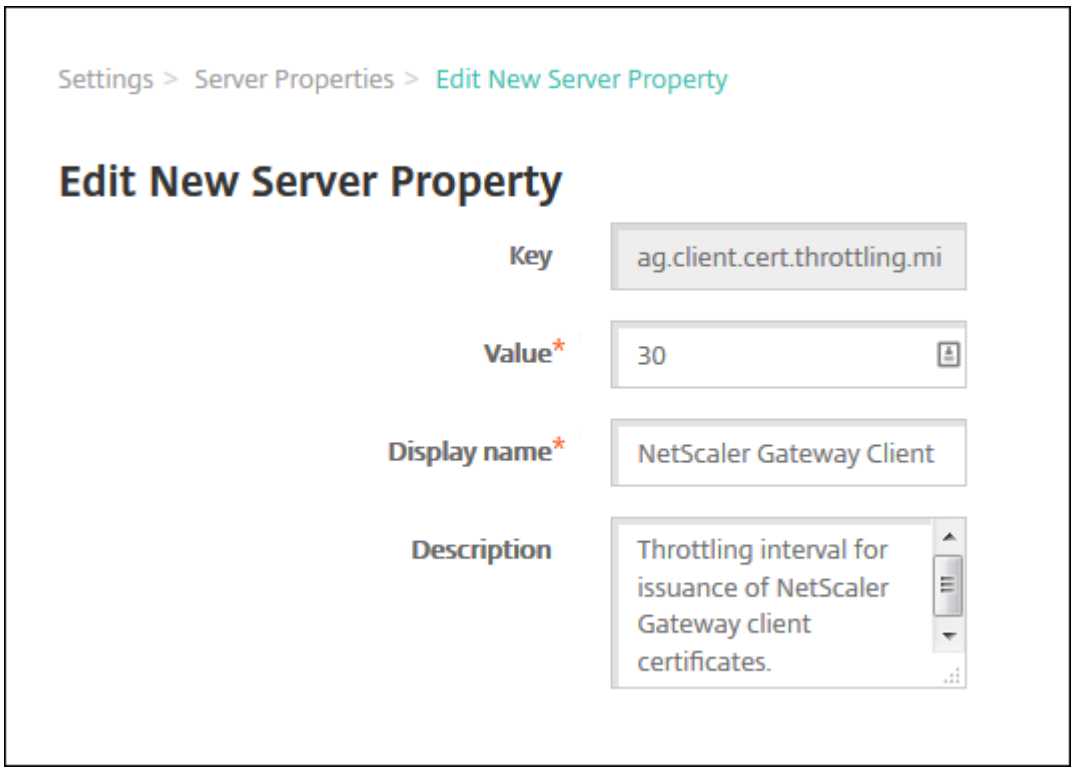
2. 다음설정을구성합니다.
   - 키: 목록에서해당하는키를선택합니다. 키는대/소문자를구분합니다. 속성값을편집하기전또는특수키를요청하려는경우 Citrix 지원에문의하십시오.
   - 값: 선택한키에따른값을입력합니다.
   - 표시이름: 서버속성테이블에표시되는새속성값의이름을입력합니다.
   - 설명: 필요한경우새서버속성의설명을입력합니다.
3. 저장을클릭합니다.

서버속성을편집하려면

1. 서버속성테이블에서편집할서버속성을선택합니다.

   서버속성옆의확인란을선택하면서버속성목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하여목록오른쪽의옵션메뉴를엽니다.

2. 편집을클릭합니다. 새서버속성편집페이지가나타납니다.



3. 다음정보를적절하게변경합니다.
   - 키: 이필드는변경할수없습니다.
   - 값: 속성값입니다.
   - 표시이름: 속성이름입니다.
   - 설명: 속성설명입니다.
4. 저장을클릭하여변경내용을저장하거나 취소를클릭하여속성을변경하지않고그대로유지합니다.

서버속성을삭제하려면

1. 서버속성테이블에서삭제할서버속성을선택합니다.

   각속성옆에있는확인란을선택하여삭제할속성을둘이상선택할수있습니다.
2. 삭제를클릭합니다. 확인대화상자가나타납니다. 삭제를다시클릭합니다.

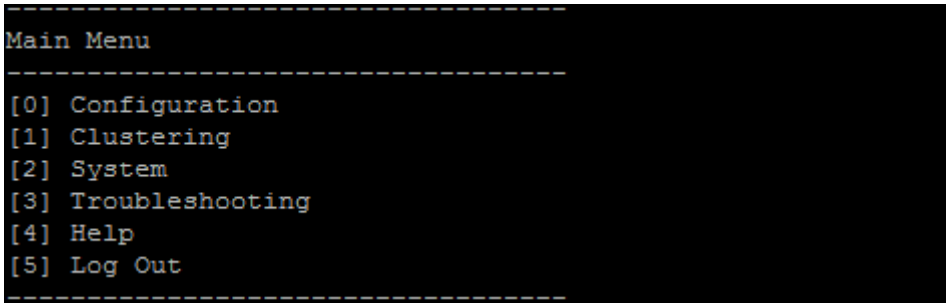
CLI(명령줄인터페이스) 옵션

January 5, 2022

XenMobile Server 온-프레미스설치의경우다음과같은방법으로 CLI 옵션에액세스할수있습니다.

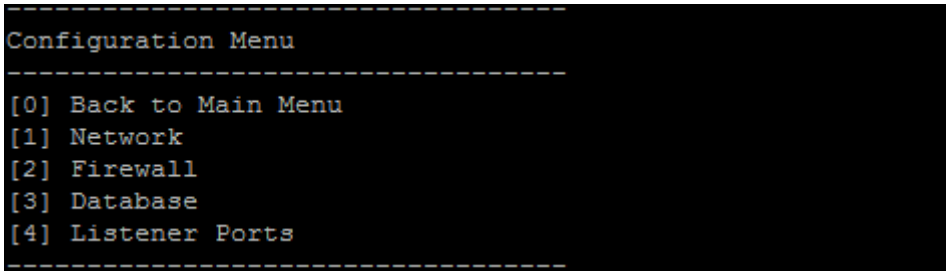
- **XenMobile** 이설치된하이퍼바이저사용: 하이퍼바이저에서, 가져온 XenMobile 가상컴퓨터를선택하고명령프롬프트보기를시작한후 XenMobile 의관리자계정에로그온합니다. 자세한내용은해당하이퍼바이저의설명서를참조하십시오.
- 방화벽에 **SSH** 가사용되는경우 **SSH** 사용**:** XenMobile 에대한관리자계정에로그온합니다.

CLI 를사용하여다양한구성및문제해결작업을수행할수있습니다. 다음그림은 CLI 의최상위메뉴를보여줍니다.

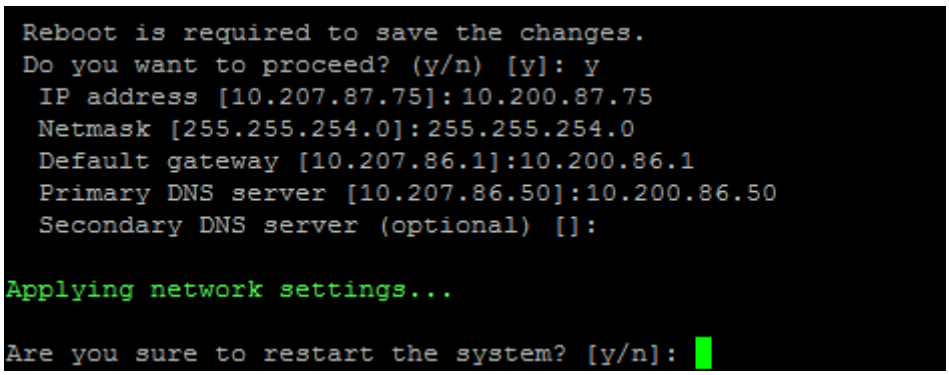


구성옵션

다음은 **Configuration Menu** 의샘플과각옵션에대해표시되는설정입니다.



[1] Network



[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]:
```

클러스터링옵션

다음은 **Clustering Menu** 의샘플과각옵션에대해표시되는설정입니다.

```
-----------------------------------
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

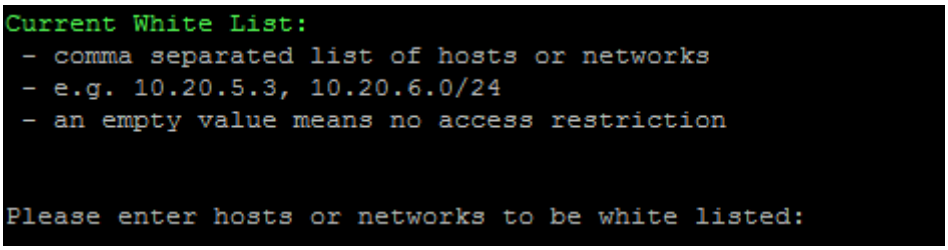
클러스터링을사용하도록선택할경우다음과같은메시지가나타납니다.

```
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



[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.

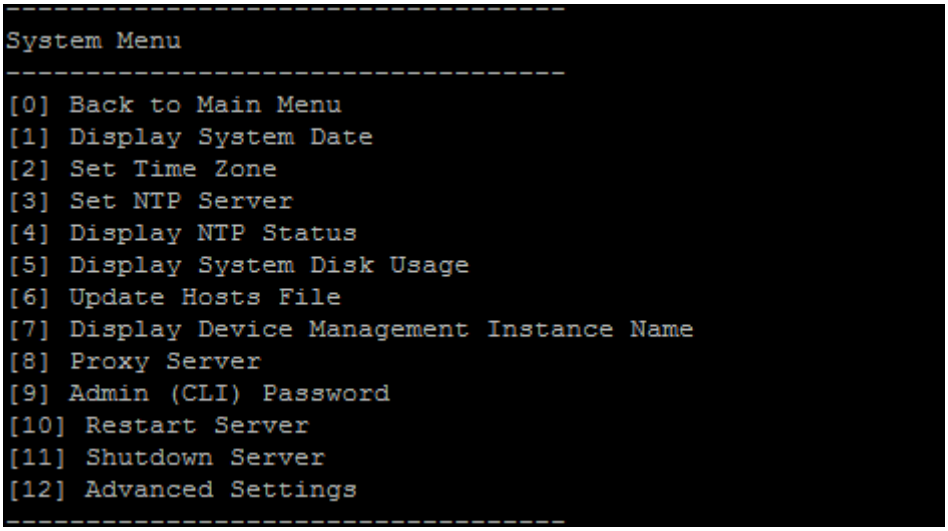
Hazelcast Cluster Members:

[IP 주소나열됨**]**

> 참고**:**
>
> 구성된노드가클러스터의일부가아닌경우해당노드를다시시작합니다.

시스템옵션

System Menu 에서는시스템수준정보를표시또는설정하거나, 서버를다시시작또는종료하거나, **Advanced Settings** 에액세스할수있습니다.



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

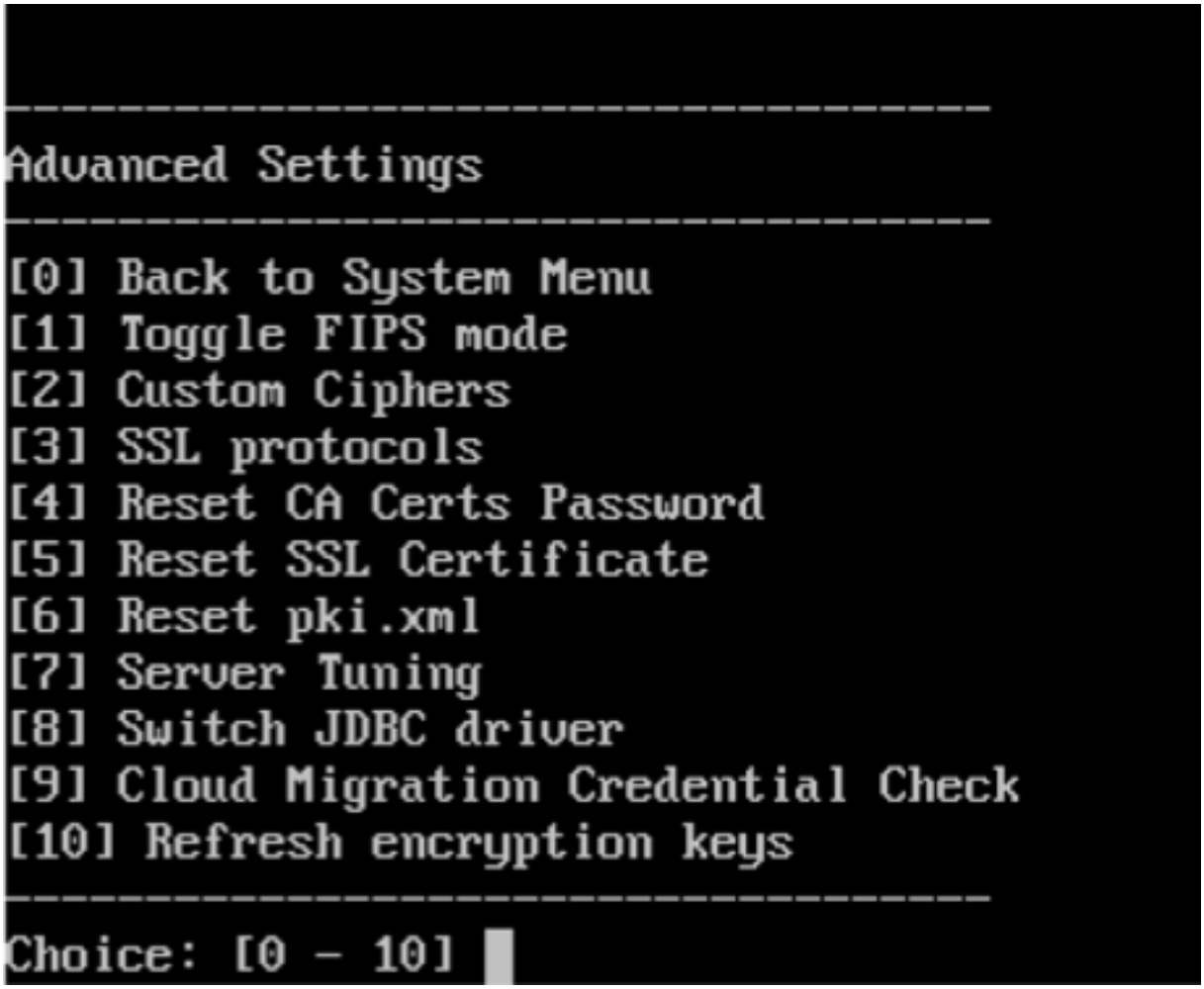
[5]Display System Disk Usage 메뉴항목에서디스크공간을확인할수도있습니다.

서버노드종료정보

클러스터에서단일서버노드를종료하는경우일반적으로 확장성및성능에설명된요구사항을충족하는다른노드에서작업부하를처리할수있습니다. 영향은동시에종료된노드수, 총사용자수및노드가종료된시간에따라다를수있습니다.

- 사용자는여전히 Secure Hub 및스토어에액세스할수있습니다.
- 사용가능한노드에서사용자수를처리할수있는경우사용자는배포된관리되는앱에액세스하고이러한앱을시작할수있습니다. 연결이느려져장치체크인속도가느려질수있습니다.
- 장치정책은모든노드가종료되지않는한계속해서작동합니다. 리소스와장치수에따라정책배포속도가더느려질수있습니다.

[12] Advanced Settings



SSL protocols 옵션은기본적으로허용된모든프로토콜로설정됩니다. **New SSL protocols to enable** 프롬프트가표시되면사용할프로토콜을입력합니다. XenMobile 은응답에포함되지않은모든프로토콜을사용하지않습니다. 예를들어 TLSv1 을사용하지않으려면 `TLSv1.2,TLSv1.1`을입력한다음 **y** 를입력하여 XenMobile Server 를다시시작합니다.

Server Tuning 옵션에는서버연결시간초과, 최대연결수 (포트별) 및최대스레드수 (포트별) 가포함됩니다.

Switch JDBC driver 옵션은 **jTDS** 와 **Microsoft** JDBC 입니다. 기본드라이버는 jTDS 입니다. Microsoft JDBC 드라이버전환에대한자세한내용은 SQL Server 드라이버를참조하십시오.

문제해결옵션

다음은 **Troubleshooting Menu** 의샘플과각옵션에대해표시되는설정입니다.


```
------------------------------------
Troubleshooting Menu
------------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
------------------------------------
Choice: [0 - 4] 4
```

[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 debug log file
 [2] Display update 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
---------------------------------
```

[4] 디스크사용량

```
---------------------------------------
Troubleshooting Menu
---------------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
---------------------------------------
Choice: [0 - 4] 4
```

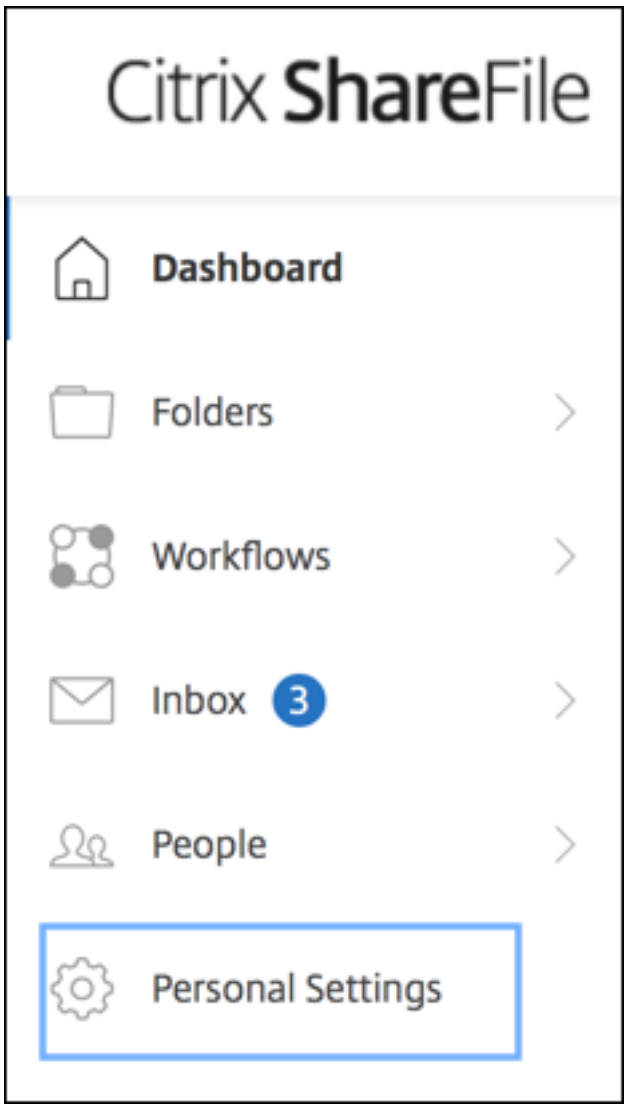
Citrix Files 를 **FTP** 사이트로사용하여지원번들을업로드하려면

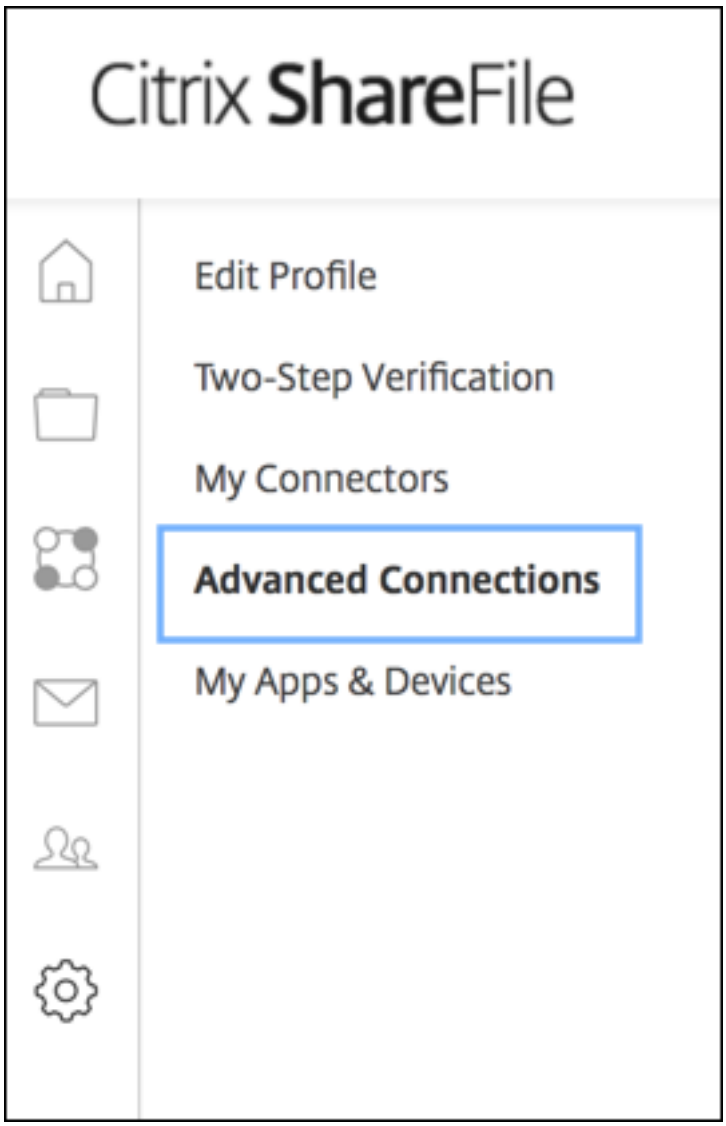
지원번들업로드를시작하기전에 Citrix Files 에서다음필수구성요소를구성합니다.

1. FTP 로그온세부정보를확인합니다.

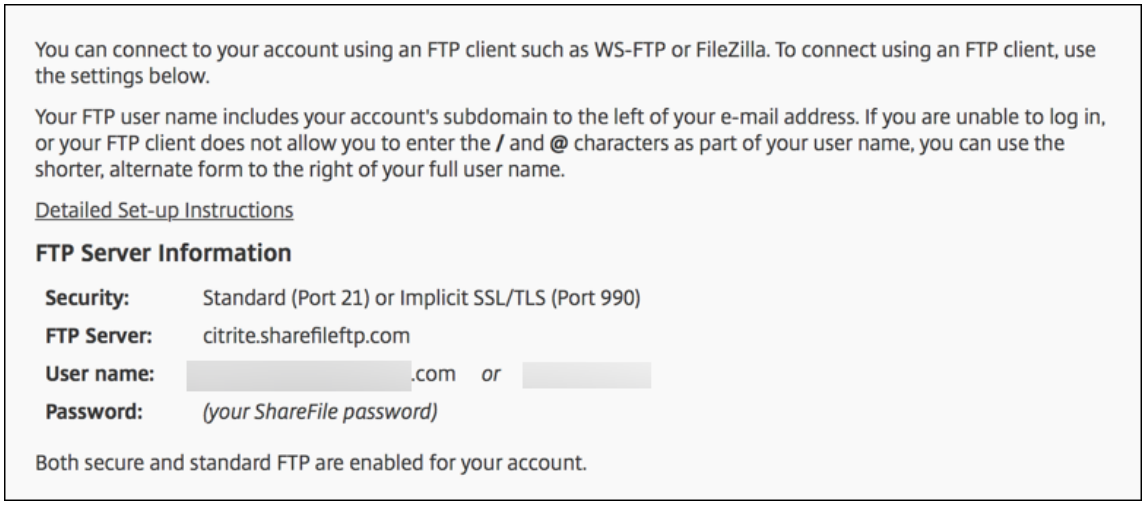
   a. 웹브라우저에서 https://citrix.sharefile.com을엽니다.

   b. **Personal Settings(**개인설정**)** 를클릭한후 **Advanced connections(**고급연결**)** 를클릭합니다.





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

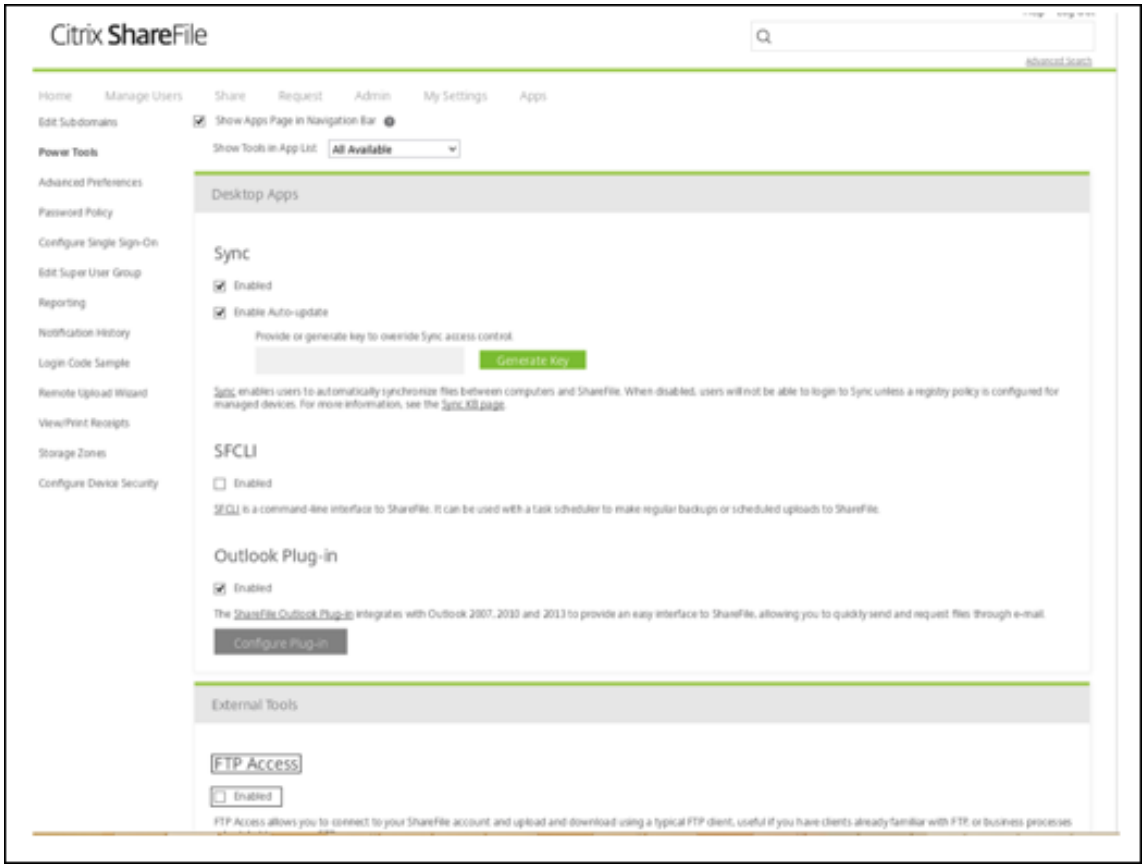
Security:	Standard (Port 21) or Implicit SSL/TLS (Port 990)
FTP Server:	citrite.sharefileftp.com
User name:	.com *or*
Password:	*(your ShareFile password)*

Both secure and standard FTP are enabled for your account.

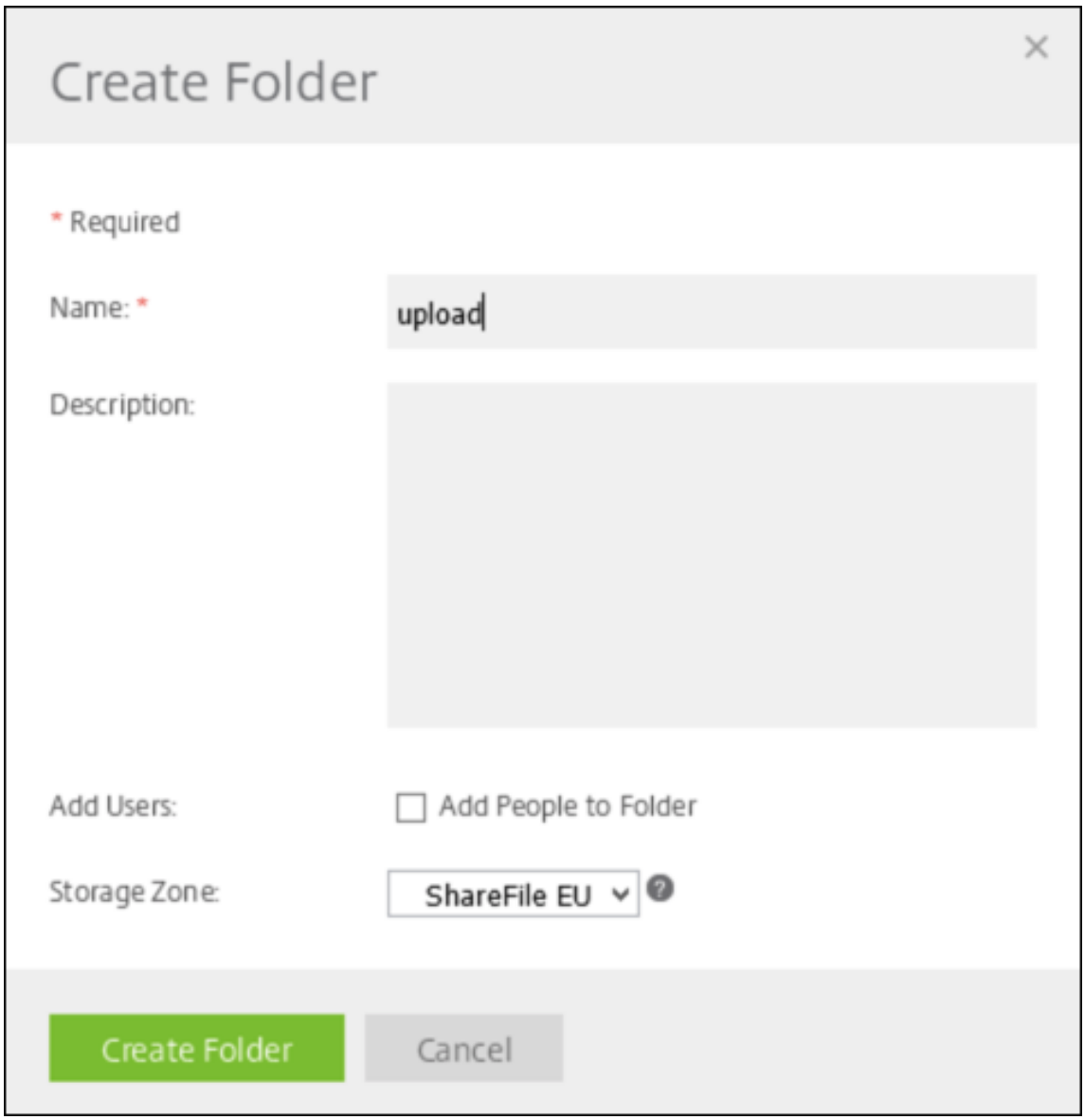
> 참고:
>
> - XenMobile 에서업로드하는파일은 Linux CLI 기반 FTP 클라이언트입니다. 따라서사용자이름의일부로 백슬래시 (\) 및기호 (@) 문자를입력할수없습니다.
> - 영숫자사용자 ID 가보이지않으면 Content Collaboration 관리자또는 Content Collaboration 지원으로부터이사용자 ID 를요청할수있습니다.

2. Citrix Files 서버에서 FTP 통신및 FTPS 를사용할수있는지확인합니다. 이상적으로는 Content Collaboration 관리자가 FTP 통신에서사용자계정을여는것을허용합니다. 그러나가끔은 FTPS 통신만허용됩니다.

   관리자권한이있는사용자는 설정, 관리설정, 고급기본설정을클릭한후 **ShareFile** 도구사용을클릭하여이설정을확인하고사용하도록설정할수있습니다. 외부앱, **FTP** 액세스에서 사용확인란을선택해야합니다.



3. FTP 클라이언트에서파일업로드에대한디렉터리로사용할공유폴더를만듭니다. 홈, 폴더를차례로클릭한후 개인폴더를클릭합니다.
4. 맨오른쪽에서더하기 (+) 아이콘을클릭하고 **Create Folder(**폴더만들기**)** 를클릭한다음폴더이름을입력합니다.



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

> 참고**:**
>
> 지원번들이있는경우메시지가표시되면 **y** 를입력하여번들을재정의합니다.

6. 지원번들을 FTP 서버에업로드합니다.

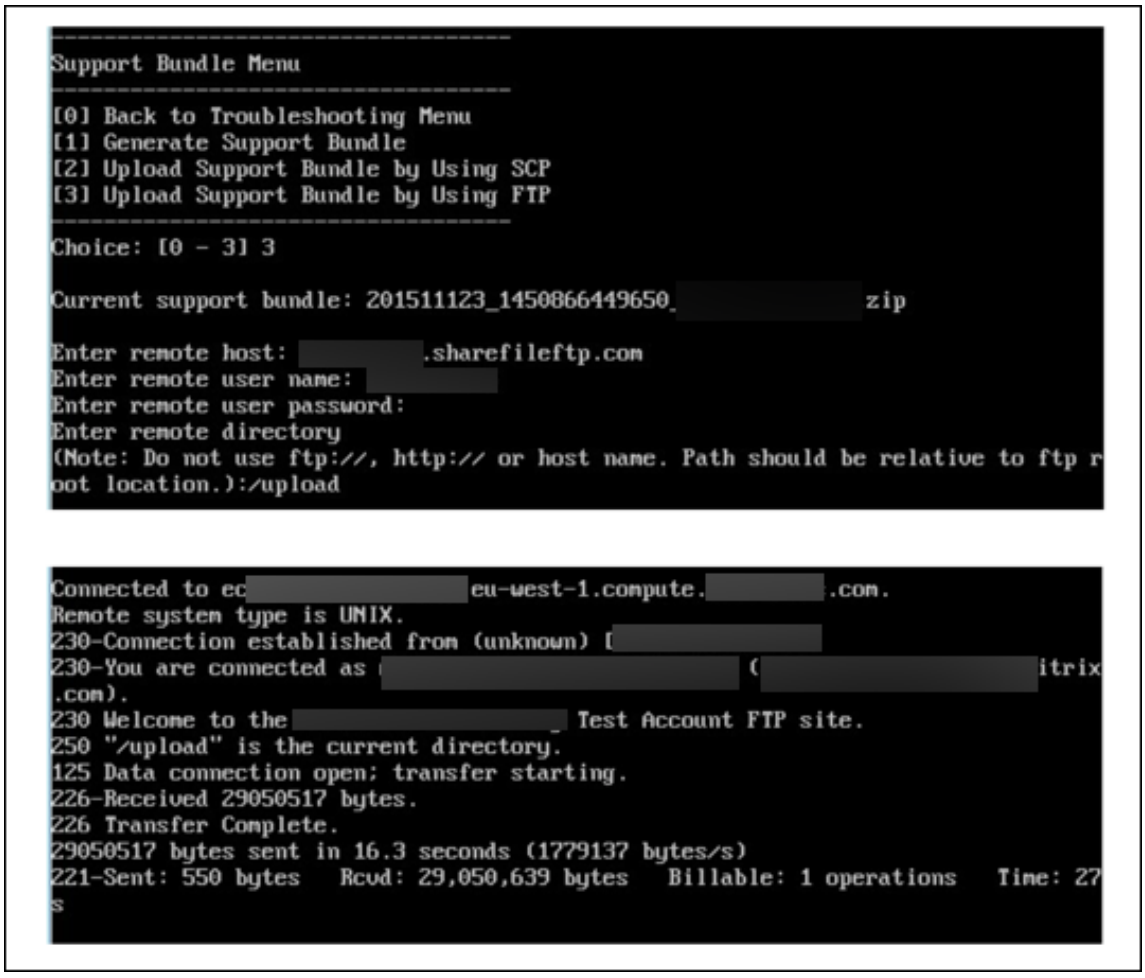
   a. **Upload Support Bundle by using FTP(FTP** 를사용하여지원번들업로드**)** 를선택합니다.

   b. **Enter remote host(**원격호스트입력**):** 메시지가표시되면 FTP 서버이름을입력합니다. Citrix Files 가 FTP 서버로사용되는경우회사이름다음에 Citrix Files FTP 사이트이름을입력합니다. 예: citrix.sharefileftp.com

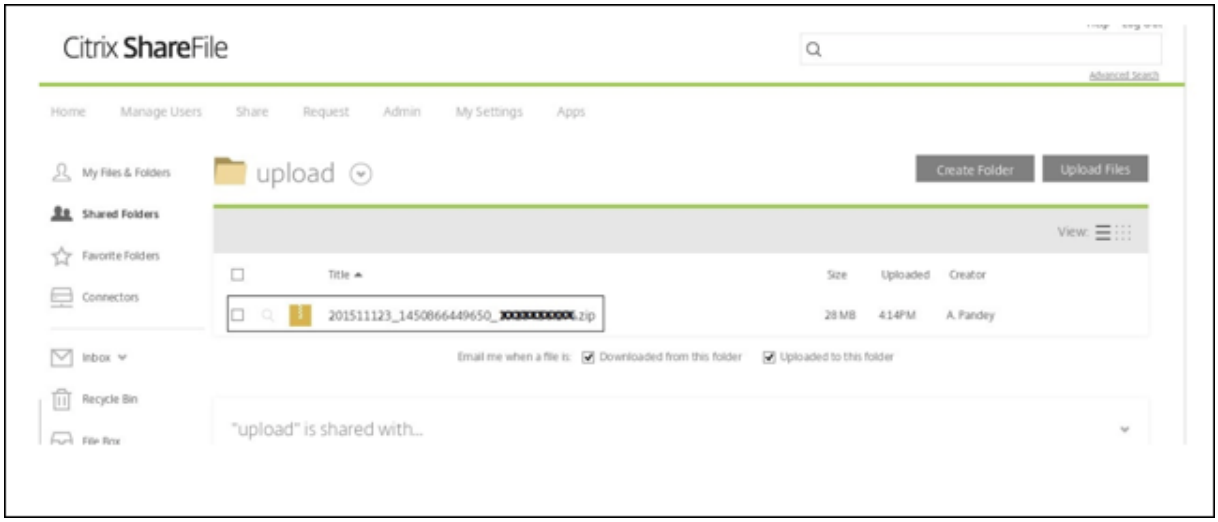
   c. **Enter remote user name(**원격사용자이름입력**):** 메시지가표시되면영숫자사용자 ID 를입력합니다.

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

e. **Enter remote directory(**원격디렉터리입력**):** 메시지가표시되면 Citrix Files 에서만든공유폴더이름을입력한 후 **Enter** 키를누릅니다.



업로드한지원번들을 Citrix Files 에서만든공유폴더에서볼수있습니다.



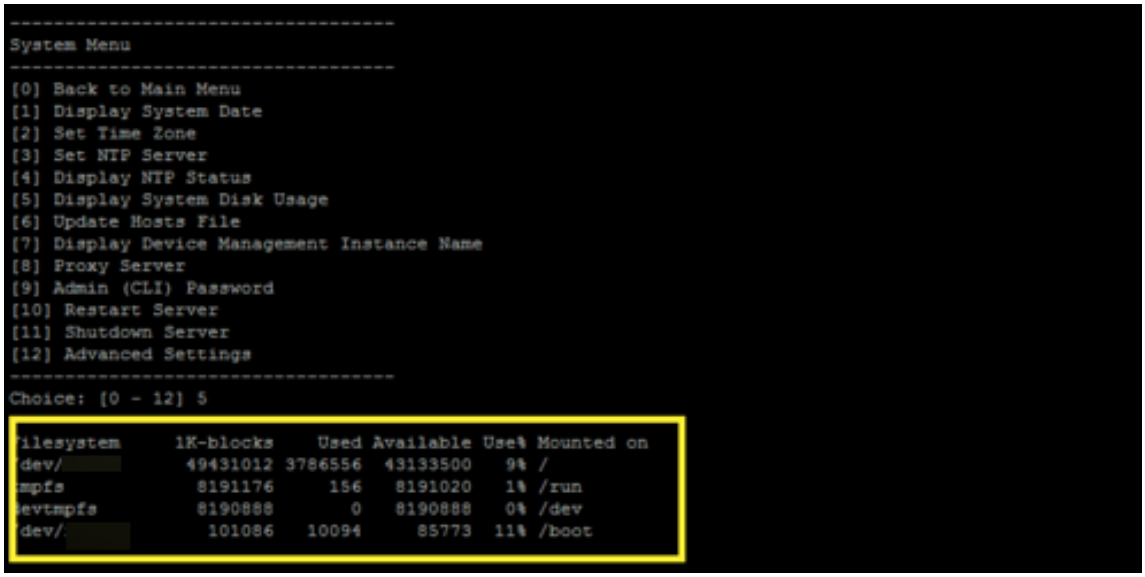
Citrix Files FTP 에대한자세한내용은이 Citrix Support Knowledge Center 문서를참조하십시오.

디스크공간을확인하려면

CLI 에서다음과같이시스템디스크공간을확인할수있습니다.

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

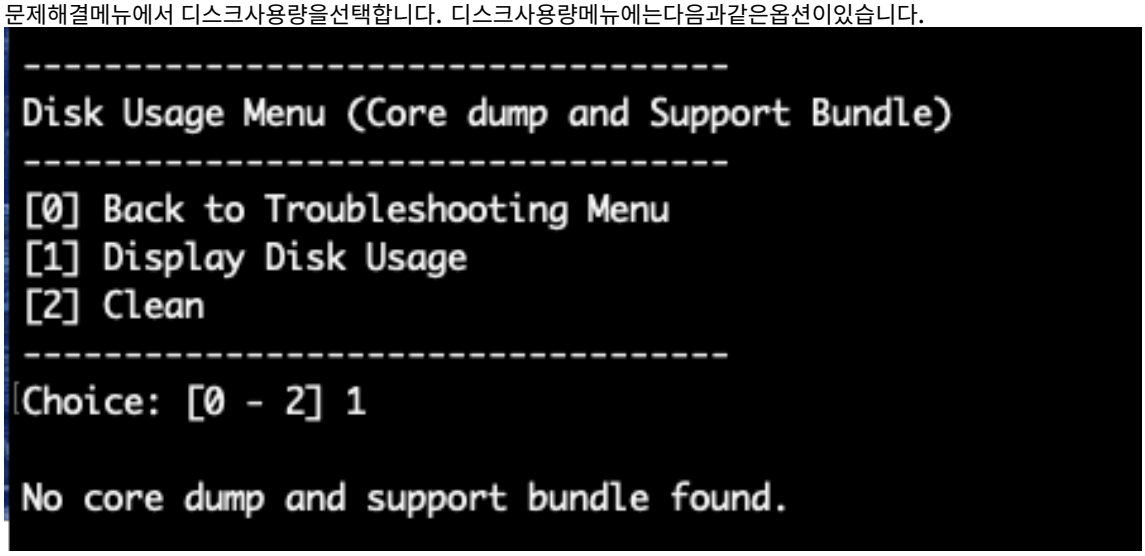
   파일시스템정보가나타납니다.



셀프서비스디스크정리수행

다음과같이 CLI 에서디스크를정리할수있습니다.

1. 문제해결메뉴에서 디스크사용량을선택합니다. 디스크사용량메뉴에는다음과같은옵션이있습니다.



2. 유형 1 은코어덤프파일과지원번들파일유형을나열합니다. 파일이존재하지않으면다음메시지가표시됩니다. 코어덤프및지원번들이없습니다.
3. 유형 2 는검사된코어덤프파일과지원번들파일을정리합니다.

XenMobile 콘솔에대한워크플로시작하기

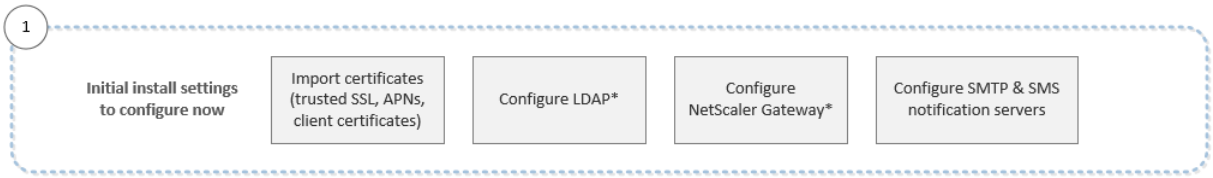
August 12, 2022

XenMobile 콘솔은 XenMobile 의통합된관리도구입니다. 이문서에서는 XenMobile 를설치했고콘솔에서작업할수있는상태인것으로가정합니다. XenMobile 을아직설치하지않은경우 XenMobile 설치를참조하십시오. XenMobile 콘솔의브라우저지원에대한자세한내용은 XenMobile 호환성문서를참조하십시오.

초기설정워크플로

명령줄콘솔과 XenMobile 콘솔에서차례로 XenMobile 을구성하고나면대시보드가열립니다. 초기구성화면으로돌아갈수없습니다. 일부설치구성을건너뛴경우콘솔에서다음설정을구성할수있습니다. 사용자, 앱및장치를추가하기전에다음설치설정을완료해야합니다. 먼저콘솔의오른쪽맨위에있는기어아이콘을클릭합니다.

> 참고:
>
> 별표가있는항목은선택적요소입니다.



각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

- 인증
- Citrix Gateway 및 XenMobile
- 알림

Android, iOS 및 Windows 플랫폼을지원하려면다음과같은계정관련설정을완료해야합니다.

Android

- Google Play 자격증명을만듭니다. 자세한내용은 Google Play Launch(시작)를참조하십시오.
- Android Enterprise 관리자계정을만듭니다. 자세한내용은 Android Enterprise를참조하십시오.
- Google 의도메인이름을확인합니다. 자세한내용은 Google Workspace 도메인확인을참조하십시오.
- API 를사용하도록설정하고 Android Enterprise 의서비스계정을만듭니다. 자세한내용은 Android Enterprise 도움말을참조하십시오.

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 Portal을참조하십시오. XenMobile 및 APNs 에대한자세한내용은 APNs 인증서 및 iOS 용 Secure Mail 의푸시알림을참조하십시오.
- 볼륨구매회사토큰을만듭니다. 자세한내용은 Apple Volume Purchasing Program을참조하십시오.

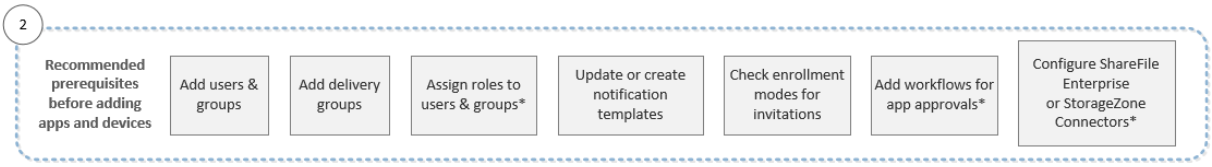
Windows

- Microsoft Windows 스토어개발자계정을만듭니다. 자세한내용은 계정유형, 위치및수수료를참조하십시오.
- Microsoft Windows 스토어게시자 ID 를가져옵니다. 자세한내용은 계정설정및프로필정보관리를참조하십시오.
- Windows 장치등록에 XenMobile 자동검색을사용하려는경우공용 SSL 인증서를사용할수있는지확인합니다. 자세한내용은 XenMobile 자동검색서비스를참조하십시오.

콘솔사전요구사항워크플로

이워크플로에서는앱및장치를추가하기전에구성해야할사전요구사항을보여줍니다.

> 참고:
>
> 별표가있는항목은선택적요소입니다.



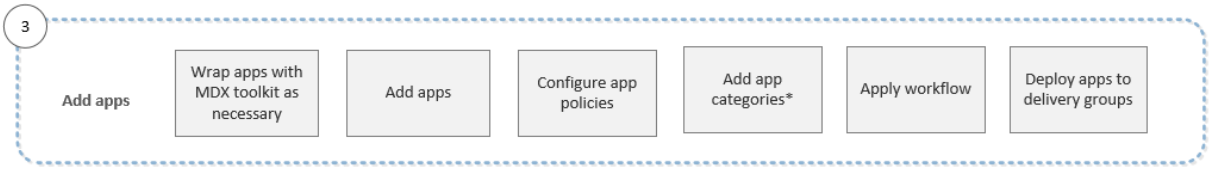
각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

- 사용자계정, 역할및등록
- 리소스배포
- RBAC 를사용하여역할구성
- 알림
- 워크플로적용
- XenMobile 에서 Citrix Content Collaboration 사용

앱워크플로추가

이워크플로는 XenMobile 에앱을추가하는경우따라야할권장순서를보여줍니다.

> 참고:
>
> 별표가있는항목은선택적요소입니다.



각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

- MDX Toolkit 정보
- 앱추가
- MDX 정책요약
- 워크플로적용
- 리소스배포

장치워크플로추가

이워크플로는 XenMobile 에서장치를추가하고등록하는경우따라야할권장순서를보여줍니다.

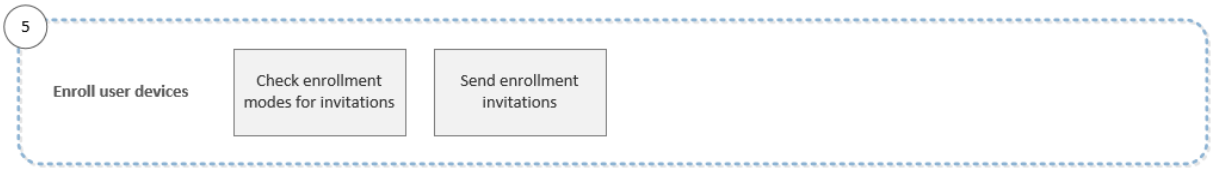
> 참고:
>
> 별표가있는항목은선택적요소입니다.

각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서및섹션을참조하십시오.

- 장치
- 지원되는장치운영체제
- 리소스배포
- 모니터링및지원
- 자동화된동작

사용자장치워크플로등록

이워크플로는 XenMobile 에서사용자장치를등록하는경우따라야할권장순서를보여줍니다.



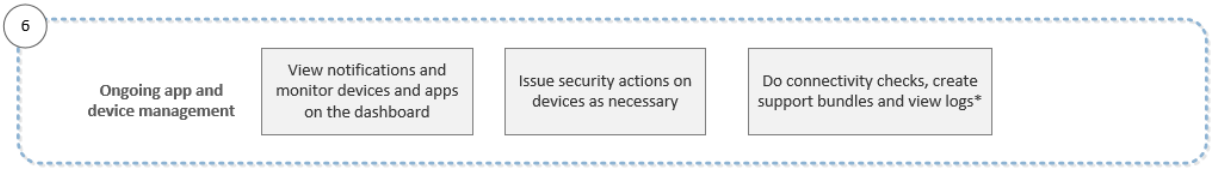
각설정에대한자세한내용과단계별절차는다음 Citrix 제품설명서문서를참조하십시오.

- 사용자계정, 역할및등록
- 알림

진행중인앱및장치관리워크플로

이워크플로는콘솔에서수행할수있는앱및장치관리작업을보여줍니다.

> 참고:
>
> 별표가있는항목은선택적요소입니다.



콘솔의오른쪽위모서리에있는렌치아이콘을클릭하면표시되는지원옵션에대한자세한내용은 모니터링및지원을참조하십시오.

인증서및인증

August 12, 2022

XenMobile 작동중에다음과같은다양한구성요소가인증에관여합니다.

- **XenMobile Server:** XenMobile Server 는등록보안및등록환경을정의하는위치입니다. 사용자등록에대한옵션은다음과같습니다.
  - 등록을모두에게공개할지초대전용으로할지여부.
  - 2 단계인증을요구할지 3 단계인증을요구할지여부. XenMobile 의클라이언트속성을통해 Citrix PIN 인증을사용하도록설정하고 PIN 의복잡성과만료시간을구성합니다.
- **Citrix ADC:** Citrix ADC 는 Micro VPN SSL 세션을종료할수있는기능을제공합니다. 또한 Citrix ADC 는네트워크전송중보안기능을제공하며사용자가앱에액세스할때마다사용되는인증환경을정의할수있게해줍니다.
- **Secure Hub:** 등록작업에서 Secure Hub 와 XenMobile Server 가함께작동합니다. Secure Hub 는장치에서 Citrix ADC 와통신하는엔터티입니다. 세션이만료되면 Secure Hub 가 Citrix ADC 로부터인증티켓을받아 MDX 앱에해당티켓을전달합니다. Citrix 는인증서고정을권장하며, 이방식은메시지가로채기 (man-in-the-middle) 공격을방지해줍니다. 자세한내용은 Secure Hub 문서에서 인증서고정 섹션을참조하십시오.

  또한 Secure Hub 를통해 MDX 보안컨테이너를쉽게사용할수있습니다. Secure Hub 는정책을푸시하고앱이시간초과되면 Citrix ADC 를통해세션을만들며 MDX 시간초과및인증환경을정의합니다. 또한 Secure Hub 는탈옥감지, 지오로케이션확인및사용자가적용한모든정책을관리합니다.

- **MDX** 정책**:** MDX 정책은장치에서데이터저장소를만듭니다. MDX 정책은 Micro VPN 연결을다시 Citrix ADC 로리디렉션하고오프라인모드제한과시간초과같은클라이언트정책을적용합니다.

1 단계인증및 2 단계인증방법의개요를비롯한인증구성에대한자세한내용은배포안내서에서 인증 문서를참조하십시오.

XenMobile 의인증서를사용하여보안연결을만들고사용자를인증할수있습니다. 이문서의나머지부분에서인증서에대해설명합니다. 다른구성세부정보에대해서는다음과같은문서를참조하십시오.

- 도메인인증또는도메인및보안토큰인증
- 클라이언트인증서인증또는인증서와도메인인증
- PKI 엔터티
- 자격증명공급자
- APNs 인증서
- Citrix Files 의 SSO(Single Sign-on) 용 SAML
- Microsoft Azure Active Directory 서버설정
- Wi-Fi 서버인증을위한인증서를장치로보내려면: Wi-Fi 장치정책
- 내부루트인증기관 (CA) 인증서와같이인증에사용되지않는독특한인증서또는특정정책을푸시하려면 자격증명장치정책을수행합니다.

인증서

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

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

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

XenMobile 에서 iOS 장치를등록하고관리하려면 Apple 에서 APNs(Apple 푸시알림서비스) 인증서를설정하고만드십시오. 단계에대해서는 APNs 인증서를참조하십시오.

다음표에서는각 XenMobile 구성요소에대한인증서형식및유형을보여줍니다.

XenMobile 구성요소	인증서형식	필요한인증서유형
Citrix Gateway	PEM(BASE64), PFX(PKCS #12)	SSL, 루트 (Citrix Gateway 가 PFX 를자동으로 PEM 으로변환함)

XenMobile 구성요소	인증서형식	필요한인증서유형
XenMobile Server	.p12(Windows 기반컴퓨터의경우.pfx)	SSL, SAML, APNs(XenMobile 이설치프로세스중에전체 PKI 도생성함) 중요: XenMobile Server 는.pem 확장의인증서를지원하지않습니다. .pem 인증서를사용하려면.pem 파일을인증서와키로분할하고각각을 XenMobile Server 로가져옵니다.
StoreFront	PFX(PKCS #12)	SSL, 루트

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

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

> 중요**: iOS, iPadOS** 및 **macOS** 의신뢰할수있는인증서에대한요구사항
>
> Apple 은 TLS 서버인증서에대한새로운요구사항을도입했습니다. 모든인증서가새로운 Apple 요구사항을따르는지확인하십시오. Apple 게시물 https://support.apple.com/en-us/HT210176를참조하십시오.
>
> Apple 은 TLS 서버인증서의최대허용수명을줄이는중입니다. 이변경사항은 2020 년 9 월이후에발급된서버인증서에만영향을줍니다. Apple 게시물 https://support.apple.com/en-us/HT211025를참조하십시오.

XenMobile 에서인증서업로드

업로드하는인증서에는인증서콘텐츠를포함하여인증서테이블의항목이포함됩니다. 인증서가필요한 PKI 통합구성요소를구성할때컨텍스트에종속적인조건을충족하는서버인증서를선택하십시오. 예를들어 Microsoft 인증기관 (CA) 과통합되도록 XenMobile 을구성한다고가정합니다. Microsoft CA 에대한연결은클라이언트인증서를사용하여인증되어야합니다.

이섹션에서는인증서를업로드하는일반적인절차를제공합니다. 클라이언트인증서만들기, 업로드및구성에대한자세한내용은 클라이언트인증서인증또는인증서와도메인인증을참조하십시오.

개인키요구사항

XenMobile 은지정된인증서에대한개인키를소유하거나소유하지않을수있습니다. 마찬가지로 XenMobile 에서사용자가업로드한인증서에개인키를요구하거나요구하지않을수있습니다.

인증서업로드

다음과같은두가지옵션으로인증서를업로드할수있습니다.

- 인증서를콘솔에개별적으로업로드합니다.
- REST API 로 iOS 장치에인증서를일괄업로드합니다.

콘솔에인증서를업로드할때주요옵션두가지가있습니다.

- 키저장소가져오기를클릭합니다. PKCS #12 형식을업로드하려는경우가아니라면계속해서설치하려는키저장소의항목을식별합니다.
- 클릭하여인증서를가져옵니다.

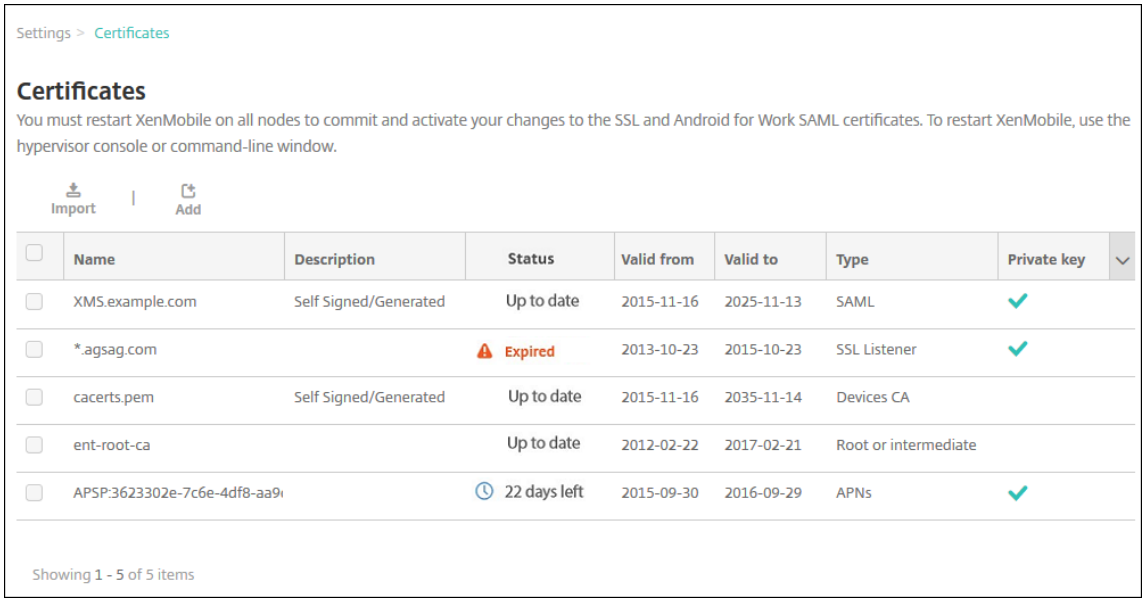
CA 가요청에서명하기위해사용하는 CA 인증서 (개인키포함안함) 를업로드할수있습니다. 또한클라이언트인증을위해 SSL 클라이언트인증서 (개인키포함) 를업로드할수있습니다.

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

키저장소를가져오려면

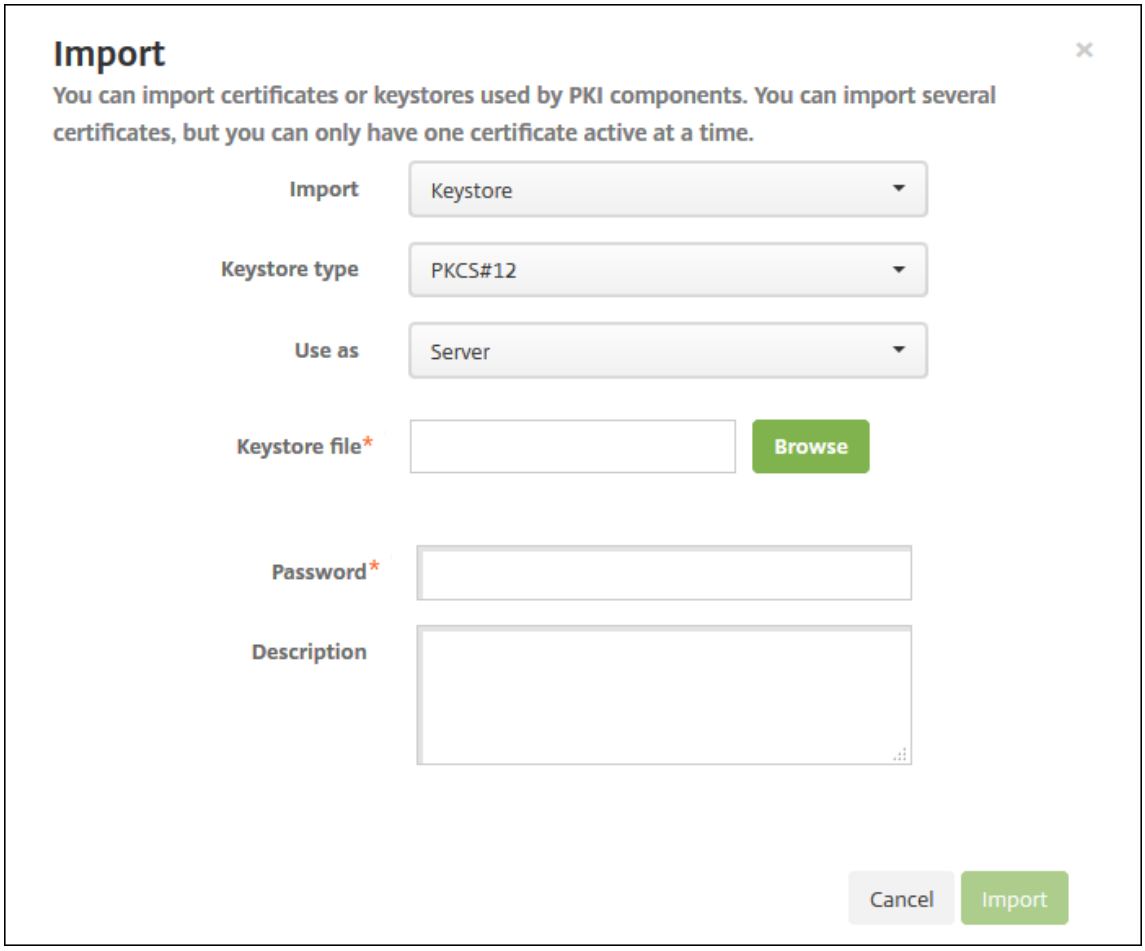
보안인증서저장소인키저장소는여러항목을포함할수있도록설계되어있습니다. 따라서키저장소에서로드할경우로드할항목을식별하는항목별칭을지정하라는메시지가나타납니다. 별칭을지정하지않으면저장소의첫번째항목이로드됩니다. PKCS #12 파일은대개항목하나만포함하기때문에 PKCS #12 를키저장소유형으로선택하면별칭필드가나타나지않습니다.

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



3. 가져오기를클릭합니다. 가져오기대화상자가나타납니다.
4. 다음설정을구성합니다.

- 가져오기**:** 목록에서 키저장소를클릭합니다. 가져오기대화상자가변경되어사용가능한키저장소옵션이나타납니다.



- 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.

인증서를가져오려면

파일또는키저장소항목에서인증서를가져오면 XenMobile 이입력에서인증서체인을구성합니다. XenMobile 은해당체인의모든인증서를가져와각인증서에대한서버인증서항목을만듭니다. 이작업은파일또는키저장소항목의인증서가체인을형성하는경우에만작동합니다. 예를들어체인의각후속인증서가이전인증서의발급자여야합니다.

필요한경우가져온인증서에대한설명을추가할수있습니다. 설명은체인의첫번째인증서에만첨부됩니다. 나중에나머지인증서의설명을업데이트할수있습니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭한다음 인증서를클릭합니다.
2. 인증서페이지에서 가져오기를클릭합니다. 가져오기대화상자가나타납니다.
3. 가져오기대화상자의 가져오기에서인증서가선택되어있지않은경우 인증서를클릭합니다.
4. 가져오기대화상자가변경되어사용가능한인증서옵션이나타납니다. 용도에서키저장소를사용할방법을선택합니다. 사용가능한옵션은다음과같습니다.
   - 서버. 서버인증서는 XenMobile 웹콘솔에업로드되어 XenMobile Server 에서기능적으로사용되는인증서입니다. 여기에는 CA 인증서, RA 인증서및클라이언트인증용인증서와인프라의다른구성요소가포함됩니다. 또한서버인증서를장치에배포할인증서의저장소로사용할수있습니다. 이옵션은특히장치에서신뢰를형성하는데사용되는 CA 에적용됩니다.
   - **SAML**. SAML(Security Assertion Markup Language) 인증을사용하면서버, 웹사이트및앱에대한 SSO(Single Sign-On) 액세스를제공할수있습니다.
   - **SSL** 수신기. SSL(Secure Sockets Layer) 수신기는 XenMobile 에 SSL 암호화활동을알립니다.
5. 찾아보기로가져올.p12(또는 Windows 기반컴퓨터의경우.pfx) 파일형식의키저장소를찾습니다.
6. 찾아보기로인증서에대한선택적인개인키파일을찾습니다. 개인키는인증서의암호화및암호해독에사용됩니다.
7. 필요한경우서로다른인증서를구분할때도움이되도록인증서에대한설명을입력합니다.
8. 가져오기를클릭합니다. 인증서가인증서테이블에추가됩니다.

REST API 로 **iOS** 장치에인증서를일괄업로드합니다

한번에인증서하나를업로드하는것이실용적이지않다면 REST API 를사용하여 iOS 장치에일괄업로드할수있습니다. 이방식은.p12 형식의인증서를지원합니다. REST API 에대한자세한정보는 REST API를참조하십시오.

1. `device_identity_value.p12` 형식으로각인증서파일의이름을변경합니다. `device_identity_value` 는각장치의 IMEI, 일련번호또는 MEID 일수있습니다.

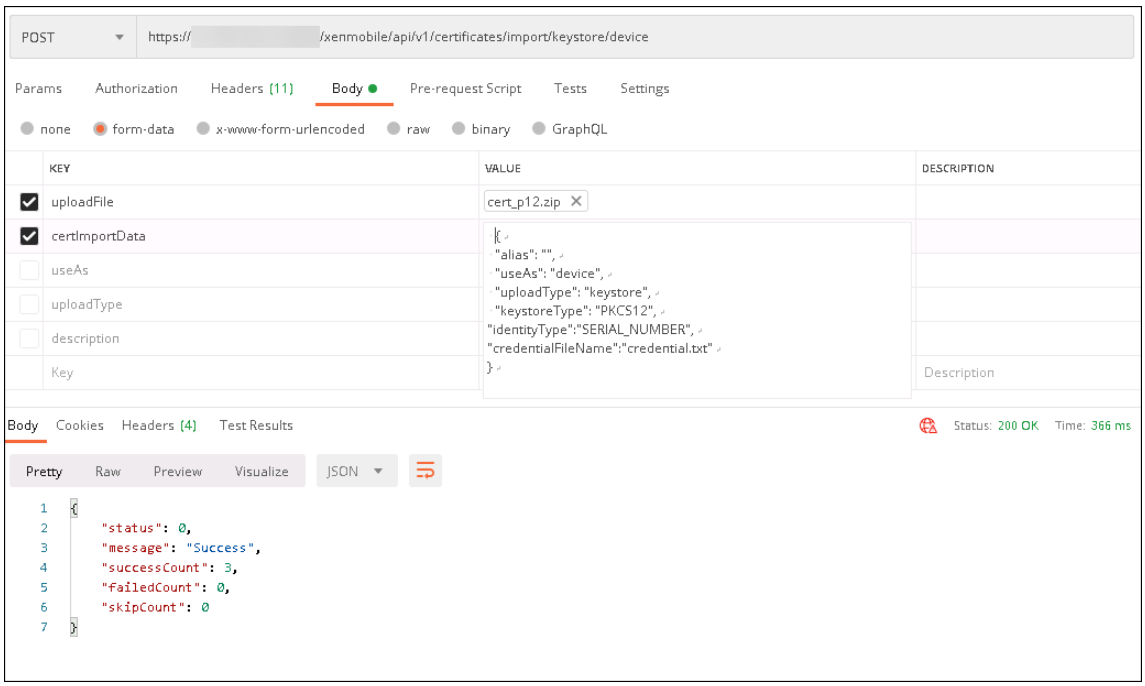
   일례로, 일련번호를인증방식으로사용하기로선택합니다. 한장치의일련번호가 `A12BC3D4EFGH`이므로해당장치에설치될것으로예상되는인증서파일에 `A12BC3D4EFGH.p12`라는이름을지정합니다.

2. .p12 인증서의암호를저장할텍스트파일을만듭니다. 해당파일의새줄에각장치의장치식별자와암호를입력합니다. `device_identity_value=password` 형식을사용합니다. 다음을참조하십시오.

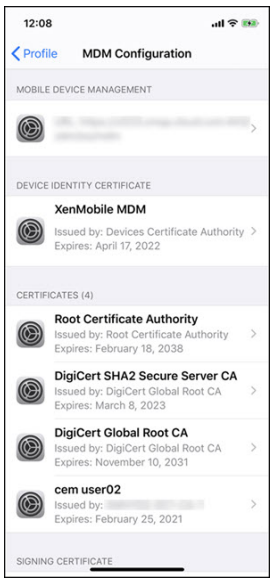

```
A12BC3D4EFGH.p12=password1!
A12BC3D4EFIJ.p12=password2@
A12BC3D4EFKL.p12=password3#
<!--NeedCopy-->
```

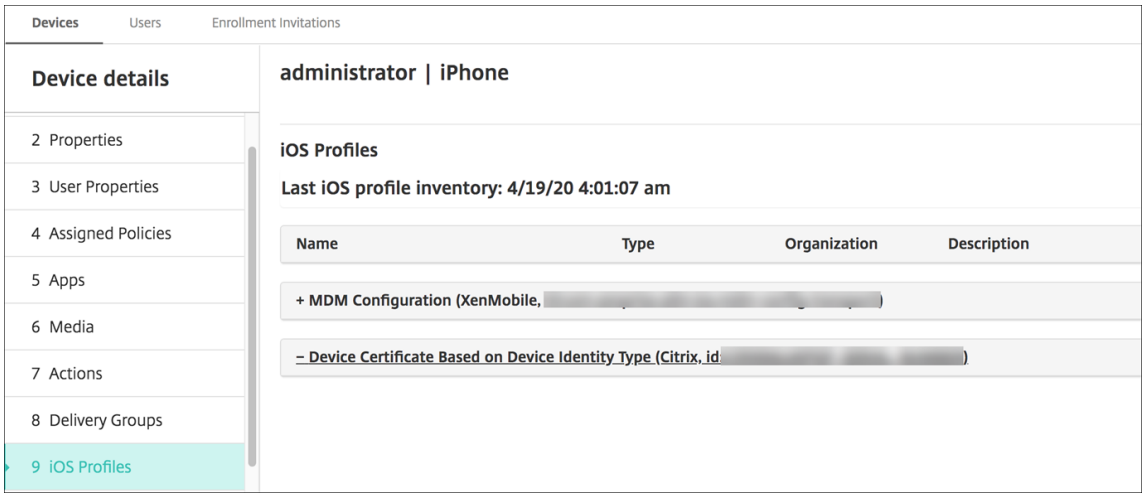
3. 생성한모든인증서와텍스트파일을.zip 파일에담습니다.
4. REST API 클라이언트를실행하고 XenMobile 에로그인한다음인증토큰을가져옵니다.
5. 인증서를가져와서다음내용을본문에입력합니다.

```
{

    ”alias”: ””,
    ”useAs”: ”device”,
    ”uploadType”: ”keystore”,
    ”keystoreType”: ”PKCS12”,
    ”identityType”:”SERIAL_NUMBER”,        # identity type can be ”SERIAL_NUMBER”,”IMEI”,”MEID”
    ”credentialFileName”:”credential.txt”   # The credential file name in .zip
 }

<!--NeedCopy-->
```



6. 인증서유형이 **IKEv2** 항상켜짐이고장치인증방식이 장치 **ID** 기반장치인증서인 VPN 정책을만듭니다. 인증서파일이름에사용한 장치 **ID** 유형을선택합니다. VPN 장치정책을참조하십시오.
7. iOS 장치를등록하고 VPN 정책이배포되기를기다립니다. 장치의 MDM 구성을확인하여인증서설치를확인합니다. XenMobile 콘솔에서도장치세부정보를확인할수있습니다.



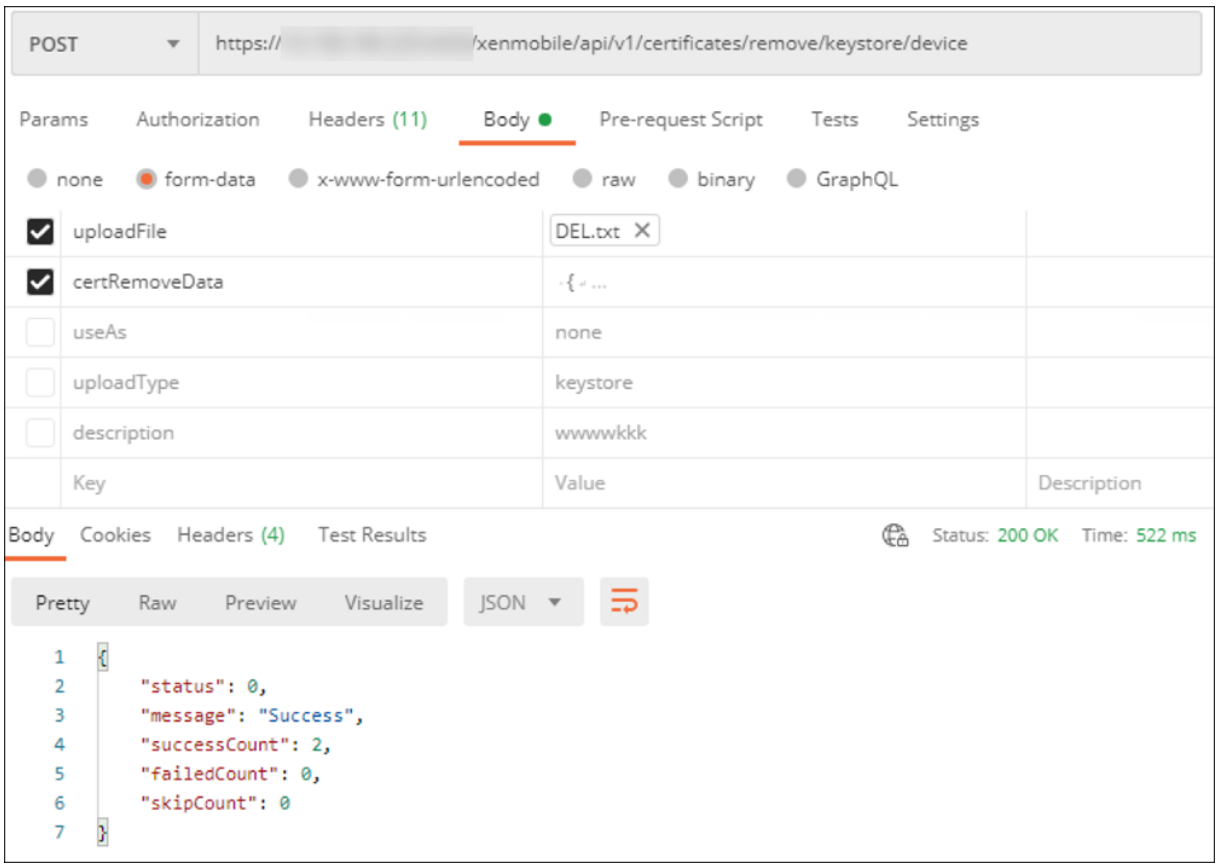


삭제할각인증서에나열된 device_identity_value로텍스트파일을만들어서인증서를일괄삭제할수도있습니다. REST API 에서삭제 API 를호출하고다음요청을사용하여 device_identity_value를적절한식별자로대체합니다.

```
```
{

    ”identityType”=”device_identity_value”
 }

<!--NeedCopy--> ```
```

 
```



인증서업데이트

XenMobile 은특정시점에공개키당하나의인증서만시스템에존재하도록허용합니다. 이미가져온인증서와동일한키쌍의인증서를가져오려고하면기존항목을바꾸거나항목을삭제할수있습니다.

인증서를가장효과적으로업데이트하려면 XenMobile 콘솔에서다음을수행하십시오. 콘솔의오른쪽맨위에있는기어아이콘을클릭하여 설정페이지를연다음 인증서를클릭합니다. 가져오기대화상자에서새인증서를가져옵니다.

서버인증서를업데이트할경우이전인증서를사용하는구성요소가자동으로새인증서를사용하도록전환됩니다. 마찬가지로, 장치에서버인증서를배포한경우인증서가다음번배포에서자동으로업데이트됩니다.

인증서갱신

XenMobile Server 는 PKI: 루트 CA, 장치 CA 및서버 CA 에대해내부적으로다음과같은인증기관을사용합니다. 이러한 CA 는논리적그룹으로분류되며그룹이름이제공됩니다. 새 XenMobile Server 인스턴스를프로비저닝하면세개의 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 를갱신하거나다시생성하고이러한인증기관에서발급한장치인증서를갱신하는데다음과 같은 API 를사용할수있습니다.

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

자세한내용은 Public API for REST Services(REST 서비스에대한공용 API) PDF 에서다음섹션을참조하십시오.

- 섹션 3.16.58, Renew Device Certificate(장치인증서갱신)
- 섹션 3.23, Internal PKI CA Groups(내부 PKI CA 그룹)

장치관리콘솔에는장치에서등록인증서를갱신하는데사용된보안조치인 인증서갱신이포함됩니다.

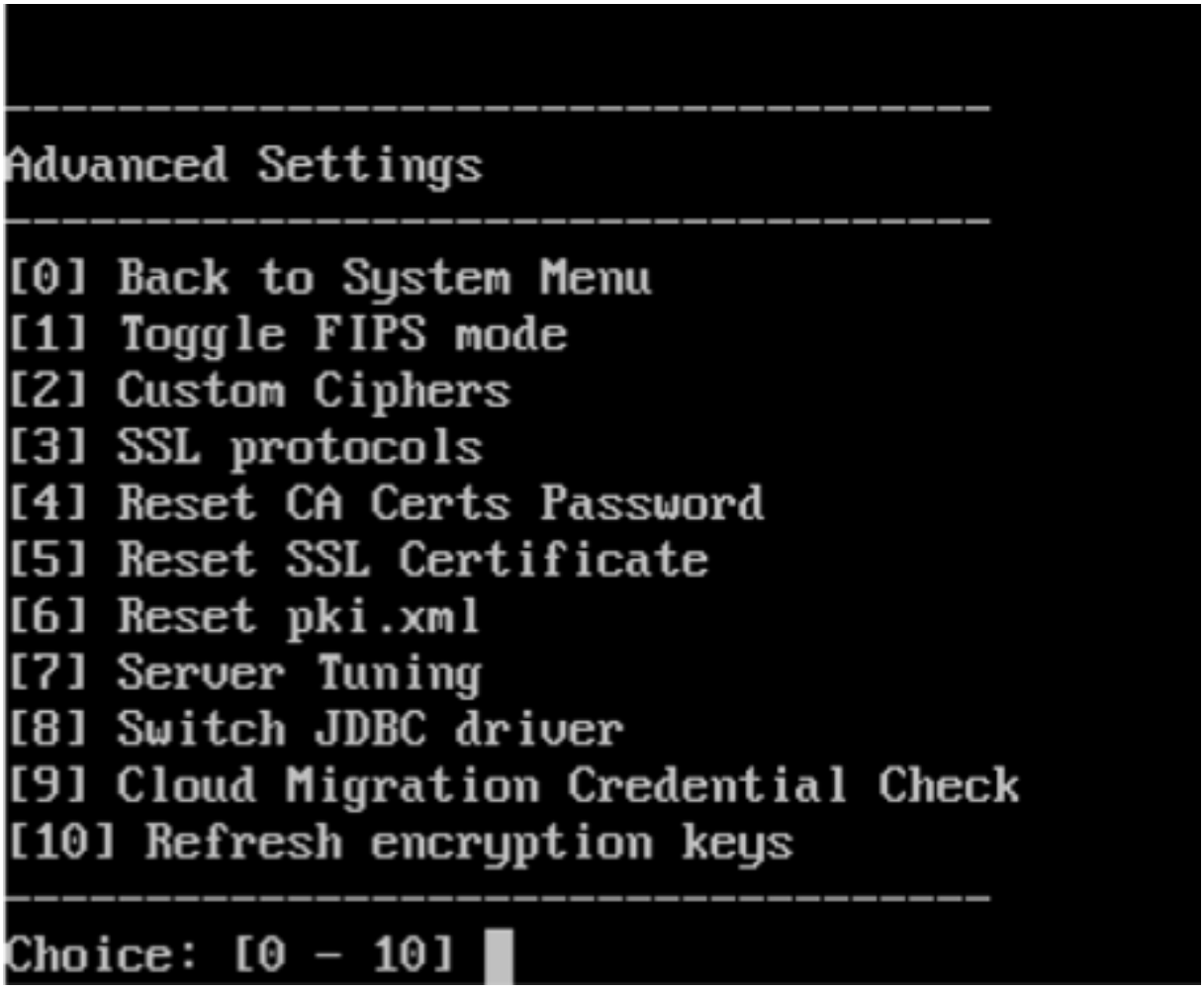
사전요구사항

- 기본적으로이인증서새로고침기능은사용되지않도록설정됩니다. 인증서새로고침기능을활성화하려면 **refresh.internal.ca** 서버속성값을 **True** 로설정하십시오.

> 중요**:**
>
> Citrix ADC 에 SSL 오프로드가설정된경우새인증서를생성할때새 cacert.perm 으로부하분산장치를업데이트해야합니다. Citrix Gateway 설정에대한자세한내용은 To use SSL Offload mode for Citrix ADC IPs(NCitrix ADC VIP 에대해 SSL 오프로드모드사용)를참조하십시오.

클러스터노드에대한서버 **CA** 인증서암호를재설정하는 **CLI** 옵션

한 XenMobile Server 노드에서서버 CA 인증서를생성한후 XenMobile CLI 를사용하여다른클러스터노드의인증서암호를재설정합니다. CLI 기본메뉴에서 시스템 **>** 고급설정 **> CA** 인증서암호재설정을선택합니다. 새 CA 인증서가없는경우암호를재설정하면 XenMobile 이암호를재설정하지않습니다.



XenMobile 인증서관리

특히만료날짜와관련암호에대해, XenMobile 배포에서사용하는인증서를기록해두는것이좋습니다. 이섹션에서는 XenMobile 에서인증서를보다쉽게관리할수있도록도와줍니다.

환경에다음과같은인증서중일부또는전체가포함될수있습니다.

- XenMobile Server
  - MDM FQDN 에대한 SSL 인증서
  - SAML 인증서 (Citrix Files 용)
  - 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

  MAM SDK 는앱을래핑하지않으므로인증서가필요하지않습니다.

- Citrix ADC
  - 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. 또한더이상앱에대한푸시알림을보낼수없습니다.

iOS 장치관리용 **APNs** 인증서

XenMobile 에서 iOS 장치를등록하고관리하려면 Apple 에서 APNs 인증서를설정하고만드십시오. 인증서가만료되면사용자가 XenMobile 에등록할수없으며사용자의 iOS 장치를관리할수없게됩니다. 자세한내용은 APNs 인증서를참조하십시오.

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
8 <!--NeedCopy-->
```

MDX Toolkit(iOS 배포인증서)

물리적 iOS 장치에서실행되는앱 (Apple App Store 의앱제외) 은다음과같은서명요구사항을충족해야합니다.

- 프로비전프로필로앱을서명합니다.
- 해당하는배포인증서로앱을서명합니다.

유효한 iOS 배포인증서가있는지확인하려면다음을수행하십시오.

1. Apple Enterprise Developer 포털에서 MDX Toolkit 으로래핑할각앱에대한명시적앱 ID 를만듭니다. 사용할수있는앱 ID 의예는다음과같습니다. `com.CompanyName.ProductName`.
2. Apple Enterprise Developer 포털에서 **Provisioning Profiles(**프로비전프로필**) > Distribution(**배포**)** 으로이동하고사내프로비전프로필을만듭니다. 이전단계에서만든각앱 ID 에대해이단계를반복합니다.
3. 모든프로비전프로필을다운로드합니다. 자세한내용은 iOS 모바일앱래핑을참조하십시오.

모든 XenMobile Server 인증서가유효한지확인하려면다음을수행하십시오.

1. XenMobile 콘솔에서 설정 **>** 인증서를클릭합니다.
2. APNs, SSL 수신기, 루트및중간인증서를비롯한모든인증서가유효한지확인합니다.

Android 키저장소

키저장소는 Android 앱에서명하는데사용된인증서가들어있는파일입니다. 키유효기간이만료되면사용자가더이상새버전의앱으로원활하게업그레이드할수없습니다.

Citrix ADC

Citrix ADC 에서인증서만료를처리하는방법에대한자세한내용은 Citrix Support Knowledge Center 에서 How to handle certificate expiry on NetScaler(NetScaler 에서인증서만료를처리하는방법)를참조하십시오.

만료된 Citrix ADC 인증서를통해서는사용자가스토어에등록및액세스할수없습니다. 또한만료된인증서로인해 Secure Mail 사용시 Exchange Server 에연결할수없습니다. 또한사용자가 HDX 앱을나열하고열수없습니다 (만료된인증서에따라다름).

Expiry Monitor 및 Command Center 를사용하면 Citrix ADC 인증서를추적할수있습니다. 인증서만료시 Center 로부터알림을받게됩니다. 이러한도구를사용하여다음과같은 Citrix ADC 인증서를모니터링할수있습니다.

- 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

Citrix Gateway 및 XenMobile

July 18, 2022

XenMobile 을사용하여 Citrix Gateway 를구성할때내부네트워크에대한원격장치액세스를위한인증메커니즘을설정합니다. 이기능을사용하면모바일장치의앱이인트라넷의회사서버에액세스할수있습니다. XenMobile 은장치의앱에서 Citrix Gateway 로 Micro VPN 을만들수있습니다.

Citrix Gateway 에서실행되는 XenMobile 에서스크립트를내보내어 XenMobile 과함께사용할 Citrix Gateway 를구성합니다.

Citrix Gateway 구성스크립트사용을위한필수구성요소

Citrix ADC 요구사항:

- Citrix ADC(최소버전 11.0, 빌드 70.12).
- LDAP 가부하분산되는경우이외에는 Citrix ADC IP 주소가구성되고 LDAP 서버에연결됩니다.
- Citrix ADC 서브넷 (SNIP) IP 주소가구성되어있고필요한백엔드서버에연결되며포트 8443/TCP 를통해공용네트워크액세스가가능합니다.
- DNS 가공용도메인을확인할수있습니다.
- Citrix ADC 가플랫폼/범용또는평가판라이센스로라이센스허가되었습니다. 자세한내용은 https://support.citrix.com/article/CTX126049에서참조하십시오.
- Citrix Gateway SSL 인증서가 Citrix ADC 에업로드되고설치되었습니다. 자세한내용은 https://support.citrix.com/article/CTX136023에서참조하십시오.

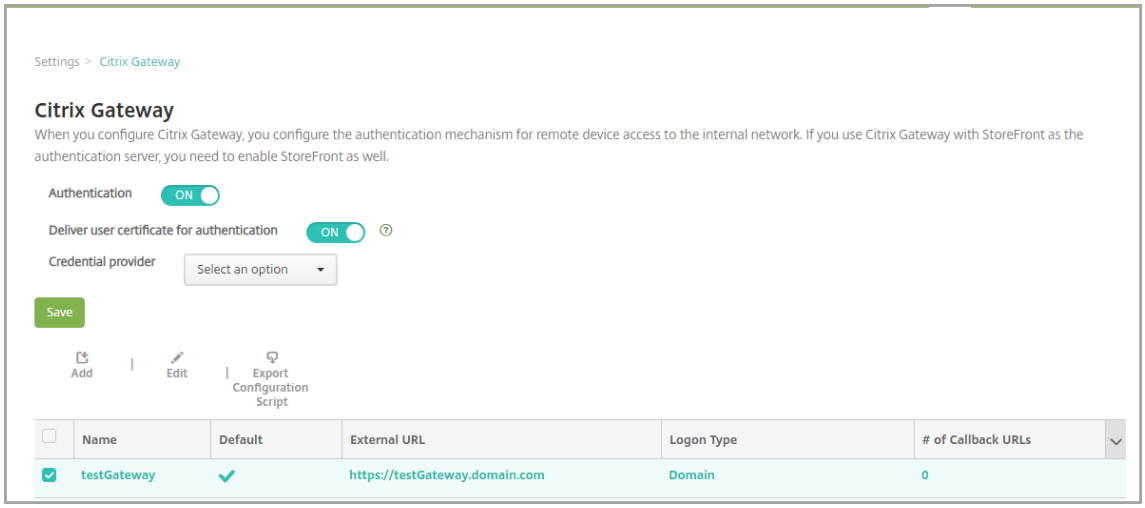
XenMobile 요구사항:

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

내부네트워크에대한원격장치액세스를위한인증구성

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.

2. 서버아래에서 **Citrix Gateway** 를클릭합니다. **Citrix Gateway** 페이지가나타납니다. 다음예제에서는 Citrix Gateway 인스턴스가존재합니다.



3. 다음설정을구성합니다.

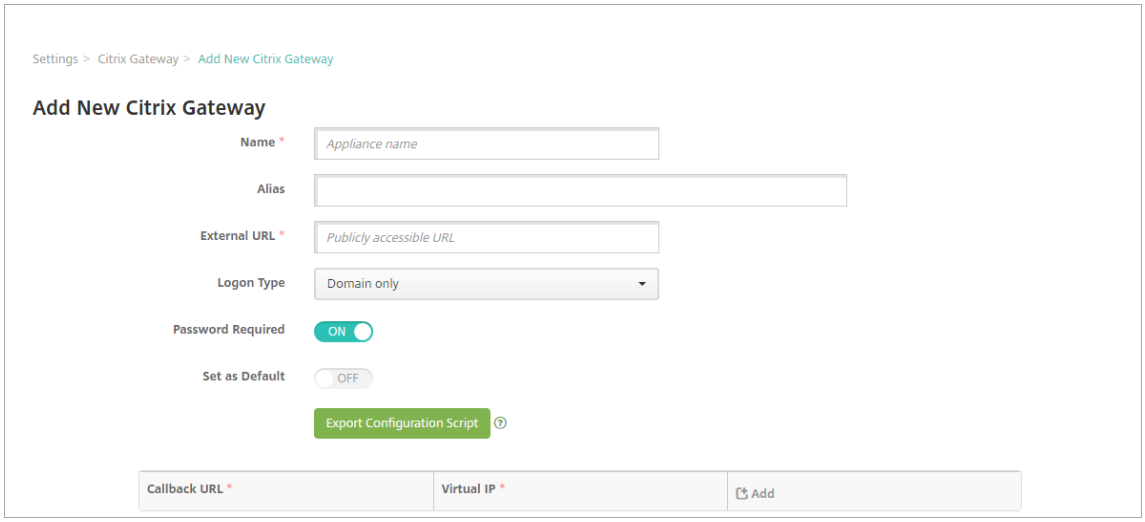
   - 인증**:** 인증을사용하도록설정하지여부를선택합니다. 기본값은 켜짐입니다.
   - 인증을위한사용자인증서제공**:** Citrix Gateway 에서클라이언트인증서인증을처리할수있도록 XenMobile 에서 Secure Hub 와인증인증서를공유하기를원하는지여부를선택합니다. 기본값은 꺼짐입니다.
   - 자격증명공급자**:** 목록에서사용할자격증명공급자를클릭합니다. 자세한내용은 자격증명공급자를참조하십시오.

4. 저장을클릭합니다.

Citrix Gateway 인스턴스추가

인증설정을저장한후 Citrix Gateway 인스턴스를 XenMobile 에추가합니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가열립니다.
2. 서버아래에서 **Citrix Gateway** 를클릭합니다. **Citrix Gateway** 페이지가나타납니다.
3. 추가를클릭합니다. 새 **Citrix Gateway** 추가페이지가나타납니다.



4. 다음설정을구성합니다.

   - 이름**:** Citrix Gateway 인스턴스의이름을입력합니다.
   - 별칭**:** 원하는경우 Citrix Gateway 의별칭이름을포함합니다.
   - 외부 **URL:** Citrix Gateway 의공개적으로액세스가능한 URL 을입력합니다. 예를들어, `https://receiver.com`입니다.
   - 로그온유형**:** 로그온유형을선택합니다. 유형에는 도메인만, 보안토큰만, 도메인및보안토큰, 인증서, 인증서및도메인, 인증서및보안토큰이포함됩니다. 암호필요필드의기본설정은선택한 로그온유형에따라달라집니다. 기본값은 도메인만입니다.

   여러개의도메인이있는경우 인증서및도메인을사용합니다. XenMobile 및 Citrix Gateway 를통한여러도메인인증구성에대한자세한내용은여러도메인에대한인증구성을참조하십시오.

   인증서및보안토큰을사용하는경우 Secure Hub 를지원하기위해 Citrix Gateway 에서몇가지추가구성이필요합니다. 자세한내용은 Configuring XenMobile for Certificate and Security Token Authentication(인증서및보안토큰인증을사용하기위한 XenMobile 구성)을참조하십시오.

   자세한내용은배포안내서의 인증을참조하십시오.

   - 암호필요**:** 암호인증을요구할지여부를선택합니다. 기본값은선택한 로그온유형에따라달라집니다.
   - 기본값으로설정**:** 이 Citrix Gateway 를기본값으로사용할지여부를선택합니다. 기본값은 꺼짐입니다.
   - 구성스크립트내보내기**:** 단추를클릭하면 Citrix Gateway 에업로드하는구성번들을내보내서 XenMobile 설정으로구성할수있습니다. 자세한내용은이단계뒤의 “XenMobile Server 와함께사용할온-프레미스 Citrix Gateway 구성” 을참조하십시오.
   - 콜백 **URL** 및 가상 **IP:** 이러한필드를추가하기전에설정을저장하십시오. 자세한내용은이문서의콜백 URL 및 Citrix Gateway VPN 가상 IP 추가를참조하십시오.

5. 저장을클릭합니다.

   새 Citrix Gateway 가추가되고테이블에나타납니다. 인스턴스를편집하거나삭제하려면목록에서이름을클릭합니다.

XenMobile Server 와함께사용할 **Citrix Gateway** 구성

XenMobile 과함께사용할온-프레미스 Citrix Gateway 를구성하려면이문서에서자세히설명하는다음일반단계를수행하십시오.

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

이스크립트로 XenMobile 에필요한 Citrix Gateway 설정을구성합니다.

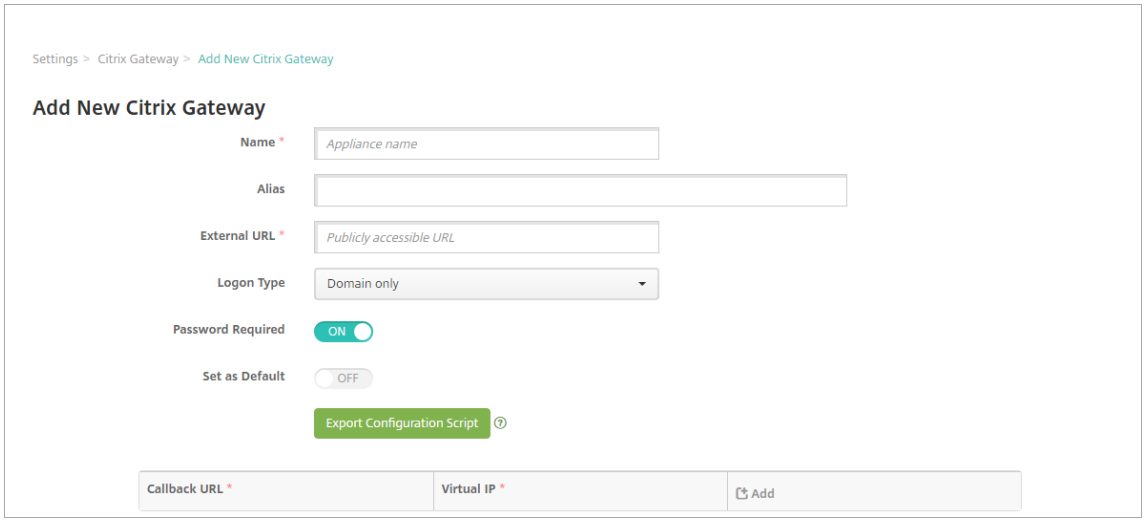
- MDM 및 MAM 에필요한 Citrix Gateway 가상서버
- Citrix Gateway 가상서버의세션정책
- XenMobile Server 세부정보
- Citrix Gateway 가상서버의인증정책및동작
  스크립트에 LDAP 구성설정이설명됩니다.
- 프록시서버의트래픽동작및정책
- 클라이언트없는액세스프로필
- Citrix ADC 의정적로컬 DNS 레코드
- 기타바인딩: 서비스정책, CA 인증서

다음구성은스크립트에서처리되지않습니다.

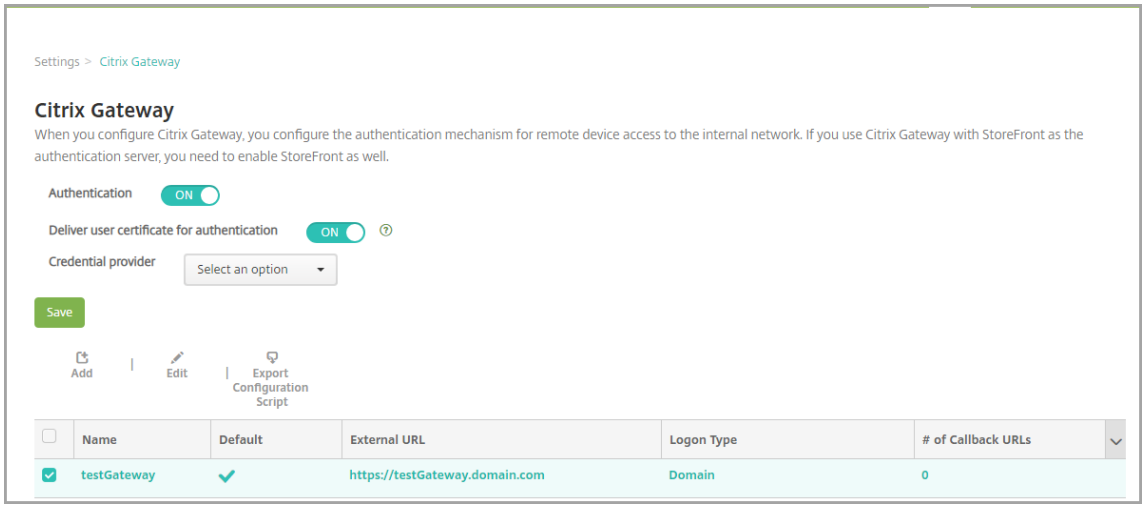
- Exchange 부하분산
- Citrix Files 부하분산
- ICA 프록시구성
- SSL 오프로드

스크립트를다운로드**,** 업데이트및실행하려면

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



또는 Citrix Gateway 인스턴스를추가하고스크립트를내보내기전에 저장을클릭하는경우: 설정 **> Citrix Gateway** 로돌아가서 Citrix ADC 를선택한다음 구성스크립트내보내기와 다운로드를차례로클릭합니다.



구성스크립트내보내기를클릭하면 XenMobile 에서.tar.gz 스크립트번들이만들어집니다. 스크립트번들에는다음이포함됩니다.

- 상세지침이포함된추가정보파일
- Citrix ADC 에서필요한구성요소를구성하는데사용되는 Citrix ADC CLI 명령이포함된스크립트
- 공용루트 CA 인증서와 XenMobile Server 의중간 CA 인증서 (현재릴리스에서는 SSL 오프로드에대해이러한 인증서가필요하지않음)
- Citrix ADC 구성을제거하는데사용되는 Citrix ADC 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 o
f private IP addresses.
# <MDM_LB_IP> -- Virtual IP Address to be assigned for MDM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <NSG_VIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reacha
ble from your devices either directly or via a NAT.
```

3. 스크립트번들에포함된추가정보파일의설명에따라, 편집된스크립트를 Citrix ADC 배시셸 (shell) 에서실행합니다. 예:

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

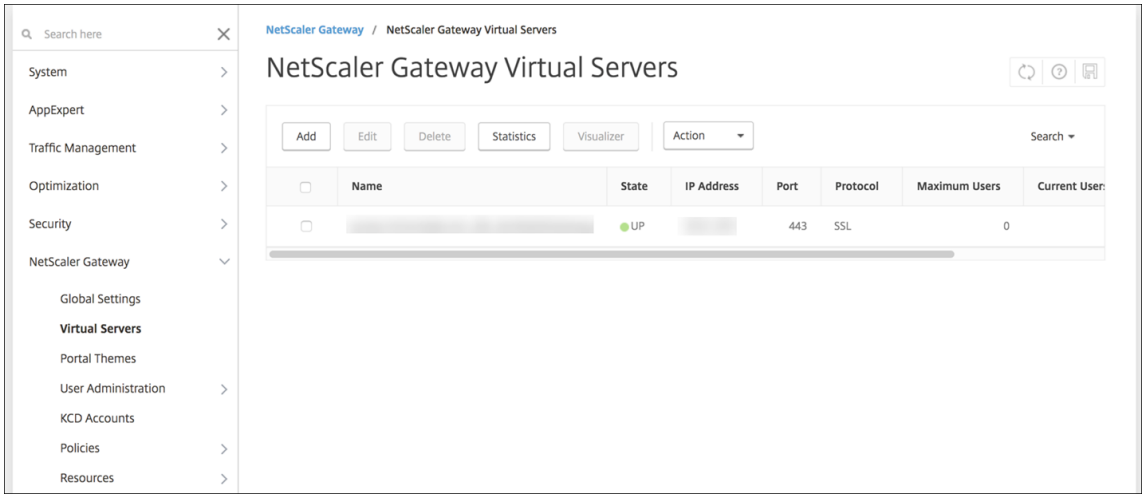
   ```
   login as: nsroot
   ##############################################################################
   #                                                                            #
   #        WARNING: Access to this system is for authorized users only         #
   #         Disconnect IMMEDIATELY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

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

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

   스크립트가완료되면다음줄이나타납니다.

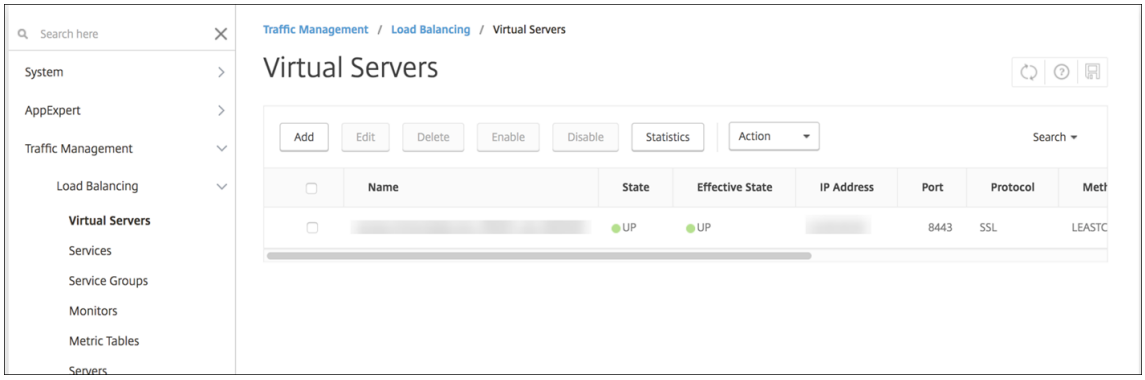
   ```
   exec: save ns config
    Done
    Done
   root@ns#
   ```

구성테스트

1. Citrix Gateway 가상서버의상태가 작동인지확인합니다.



2. 프록시부하분산가상서버의상태가 작동인지확인합니다.



3. 웹브라우저를열고 Citrix Gateway URL 에연결하여인증을시도합니다. 인증이실패하면 HTTP 상태 404 - 찾을수없음메시지가나타납니다.
4. 장치를등록하고 MDM 및 MAM 모두에등록되었는지확인합니다.

콜백 **URL** 및 **Citrix Gateway VPN** 가상 **IP** 추가

Citrix Gateway 인스턴스를추가한후콜백 URL 을추가하고 Citrix Gateway 가상 IP 주소를지정할수있습니다. 이설정은선택사항이지만특히 XenMobile Server 가 DMZ 에있는경우보안을강화하기위해구성할수있습니다.

1. 설정 **> Citrix Gateway** 에서 Citrix Gateway 를선택하고 편집을클릭합니다.
2. 테이블에서 추가를클릭합니다.
3. 콜백 **URL** 로 FQDN(정규화된도메인이름) 을입력합니다. 콜백 URL 은요청이 Citrix Gateway 에서온요청인지확인합니다.

   콜백 URL 이 XenMobile Server 에서연결가능한 IP 주소로확인되는지확인합니다. 콜백 URL 은외부 Citrix Gateway URL 또는다른 URL 일수있습니다.
4. Citrix Gateway 가상 **IP** 주소를입력한다음 저장을클릭합니다.

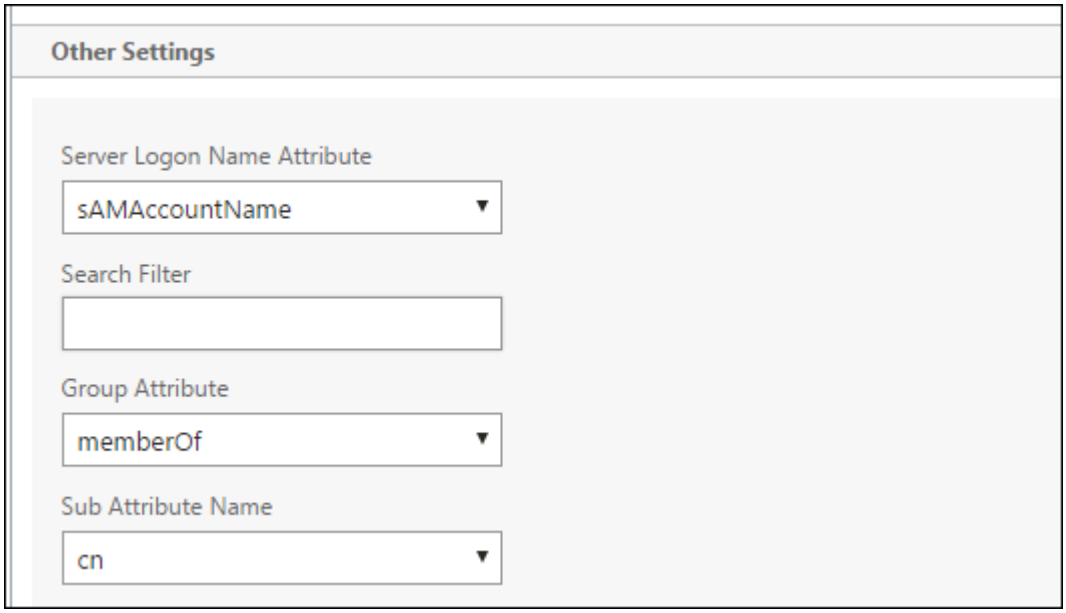
여러도메인에대한인증구성

테스트, 개발및프로덕션환경을위한다수의 XenMobile Server 인스턴스가있는경우추가환경에대한 Citrix Gateway 를수동으로구성합니다. XenMobile 용 Citrix ADC 마법사는한번만사용할수있습니다.

Citrix Gateway 구성

여러도메인환경에대한 Citrix Gateway 인증정책및세션정책을구성하려면:

1. Citrix Gateway 구성유틸리티의 구성탭에서 **Citrix Gateway >** 정책 **>** 인증을확장합니다.
2. 탐색창에서 **LDAP** 를클릭합니다.
3. LDAP 프로필을클릭하여편집합니다. 서버로그온이름특성을 **userPrincipalName** 또는검색에사용하려는특성으로변경합니다. XenMobile 콘솔에서 LDAP 설정구성시사용할수있도록지정한특성을메모해둡니다.

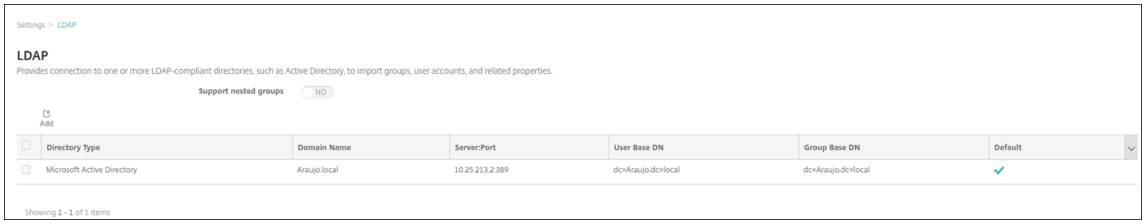


4. 각 LDAP 정책에대해이러한단계를반복합니다. 각도메인에는개별 LDAP 정책이필요합니다.
5. Citrix Gateway 가상서버에바인딩된세션정책에서 **Edit session profile(**세션프로필편집**) > Published Applications(**게시된응용프로그램**)** 로이동합니다. **Single Sign-On Domain(Single Sign-On** 도메인**)** 이비어있는지확인합니다.

XenMobile Server 구성

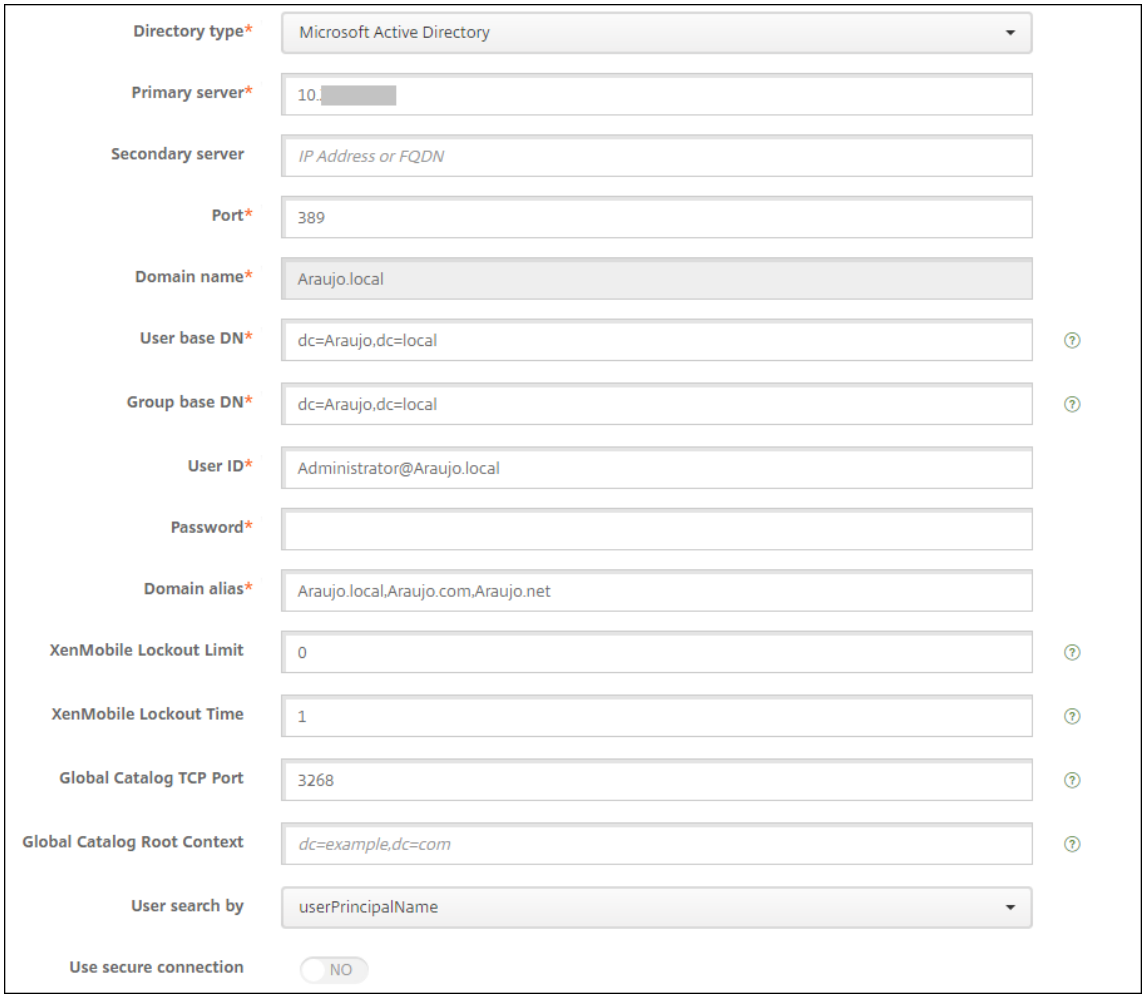
여러도메인의 XenMobile 환경에대한 LDAP 를구성하려면:

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



2. 다음정보를제공합니다.

   - 도메인별칭에서사용자인증에사용할각도메인을지정합니다. 도메인을쉼표로구분하십시오. 도메인사이에공백을사용하지마십시오. 예: `domain1.com,domain2.com,domain3.com`
   - 사용자검색기준필드가 Citrix 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 부하분산장치가상서버 (포트 443 용및포트 8443 용) 를구성합니다. 설정시다음정보를템플릿으로활용합니다.

> 중요:
>
> 다음업데이트는 SSL 오프로드가구성된 Citrix Gateway 에만적용됩니다.

1. XMS_DropURLs라는이름의패턴집합을만듭니다.

```
add policy patset XMS_DropURLs
<!--NeedCopy-->
```

2. 이새로운패턴집합에다음 URL 을추가합니다. 필요에따라이목록을사용자지정합니다.

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6

bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5

bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4

bind policy patset XMS_DropURLs /zdm/log.jsp -index 3

bind policy patset XMS_DropURLs /zdm/login.jsp -index 2

bind policy patset XMS_DropURLs /zdm/console -index 1
<!--NeedCopy-->
```

3. 연결요청이지정된서브넷에서시작되지않는한이러한 URL 에대한모든트래픽을삭제하는정책을만듭니다.

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

4. 새정책을두 MDM 부하분산장치가상서버 (포트 443 및 8443) 에바인딩합니다.

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST
```



```
2
3 bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
     XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
     REQUEST
4 <!--NeedCopy-->
```

5. 브라우저를통한 MAM URL 액세스차단

   브라우저를통해 MAM URL 에직접액세스하면사용자에게 Active Directory 자격증명을입력하라는메시지가표시됩니다. 이는사용자가자격증명의유효성을검사하는도구역할을하지만일부사용자는이를보안위반으로간주할수있습니다. 다음섹션은 NetScaler 의응답자정책기능을사용하여 MAM URL(NetScaler Gateway VIP) 에대한브라우저액세스를제한하는데도움이됩니다.

   다음응답자정책중하나를만들어 NetScaler Gateway 가상서버에바인딩합니다.

   - `add responder policy Resp_Brow_Pol "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"Mozilla\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")"DROP`
   - `add responder policy Resp_Brow_Pol_CR "!HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")"DROP`
   - `add responder policy Resp_Brow_Pol_CR "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")"DROP`

   `bind vpn vserver _XM_XenMobileGateway -policy Resp_Brow_Pol_CR -priority 100 -gotoPriorityExpression END -type REQUEST`를사용하여 NetScaler Gateway 가상서버에바인딩

   > 참고:
   >
   > `_XM_XenMobileGateway`는 NetScaler Gateway 가상서버의예제이름입니다.

도메인인증또는도메인및보안토큰인증

January 5, 2022

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

LDAP 는 IP(인터넷프로토콜) 네트워크를통한분산디렉터리정보서비스액세스및유지관리를지원하는공급업체중립적인오픈소스응용프로그램프로토콜입니다. 디렉터리정보서비스는네트워크에서사용가능한사용자, 시스템, 네트워크, 서비스및응용프로그램

에대한정보를공유하는데사용됩니다.

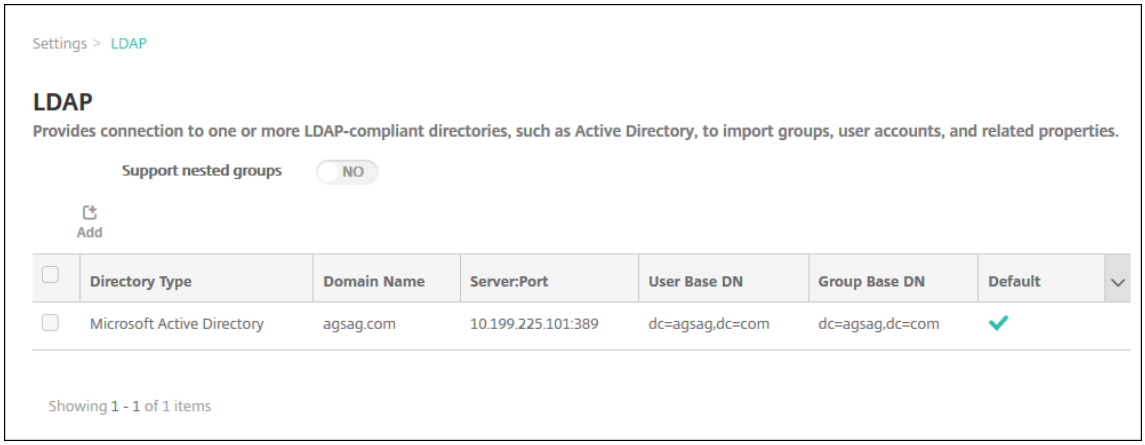
LDAP 는일반적으로다수의서비스에서하나의암호 (사용자당) 를공유하는 SSO(Single Sign-on) 를사용자에게제공할때사용됩니다. SSO(Single Sign-on) 를사용하면사용자가회사웹사이트에한번로그온하여회사인트라넷에대한액세스를인증할수있습니다.

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

> 중요:
>
> XenMobile 은사용자가 XenMobile 에서장치를등록한후도메인인증에서다른인증모드로의인증모드변경을지원하지않습니다.

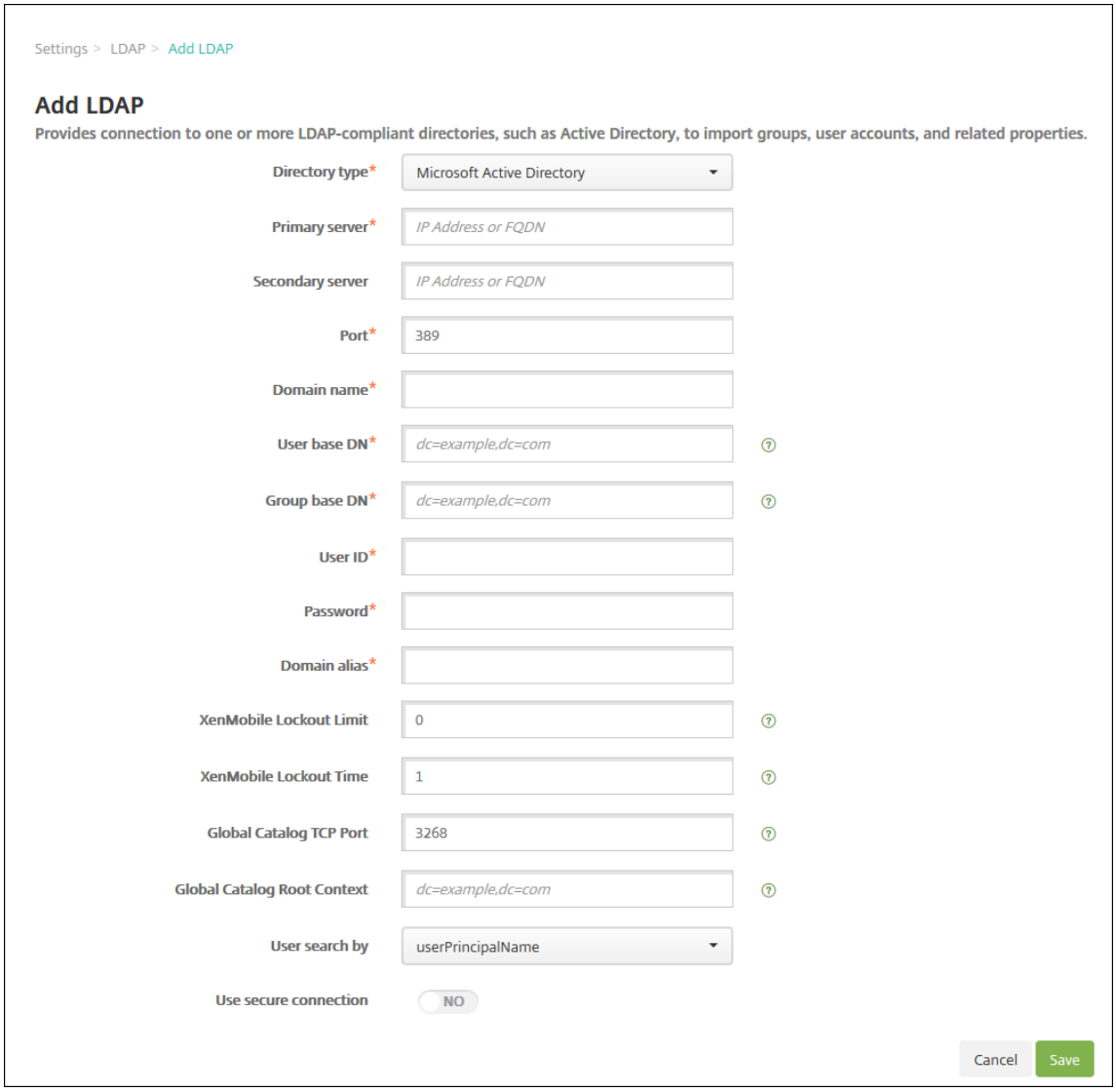
XenMobile 에서 LDAP 연결을추가하려면

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



LDAP 호환디렉터리를추가하려면

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



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. 등록후 도메인별칭설정을변경하는경우사용자가다시등록해야합니다.
- **XenMobile** 잠금제한**:** 실패한로그온시도횟수를 **0** 에서 **999** 사이의숫자로입력합니다. **0** 값은 XenMobile 이실패한로그온시도를기준으로사용자를잠그지않음을의미합니다.
- **XenMobile** 잠금시간**:** 잠금제한을초과한후사용자가대기해야하는시간 (분) 을나타내는 **0** 에서 **99999** 사이의숫자를입력합니다. **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. 기본값은 **userPrincipalName** 입니다. 등록후 사용자검색기준설정을변경하는경우사용자가다시등록해야합니다.
- 보안연결사용**:** 보안연결을사용할지여부를선택합니다. 기본값은 아니요입니다.

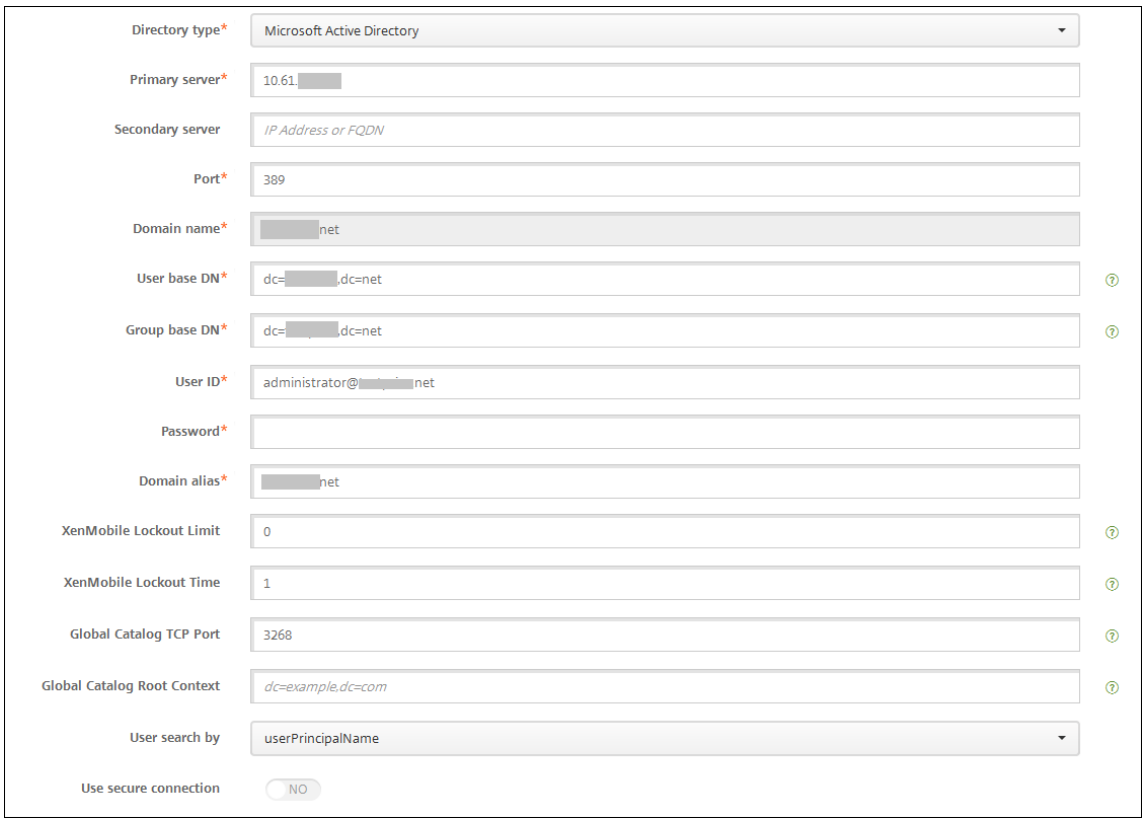
3. 저장을클릭합니다.

LDAP 호환디렉터리를편집하려면

1. **LDAP** 테이블에서편집하려는디렉터리를선택합니다.

   디렉터리옆에있는확인란을선택하면 LDAP 목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.

2. 편집을클릭합니다. **LDAP** 편집페이지가나타납니다.



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. 예를들어 `cn=users` 가그룹이름인경우 `cn=users`, `dc=servername`, `dc=net`입니다. `DN` 및 `servername`은 Active Directory 를실행하는서버의이름을나타냅니다.
   - 사용자 **ID:** Active Directory 계정과연관된사용자 ID 를입력합니다.
   - 암호**:** 사용자와연관된암호를입력합니다.
   - 도메인별칭**:** 도메인이름의별칭을입력합니다. 등록후 도메인별칭설정을변경하는경우사용자가다시등록해야합니다.
   - **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. 등록후 사용자검색기준설정을변경하는경우사용자가다시등록해야합니다.
- 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 여러도메인에대한인증구성의절차를참조하십시오. 이러한단계는온-프레미스버전의 XenMobile Server 와 Endpoint Management 클라우드릴리스에서동일합니다.

도메인과보안토큰인증구성

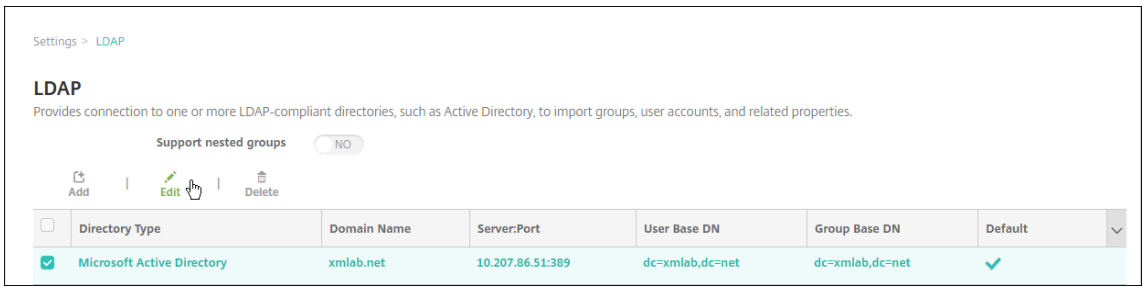
RADIUS 프로토콜을사용하여사용자가 LDAP 자격증명과일회용암호를사용하여인증하도록 XenMobile 을구성할수있습니다.

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

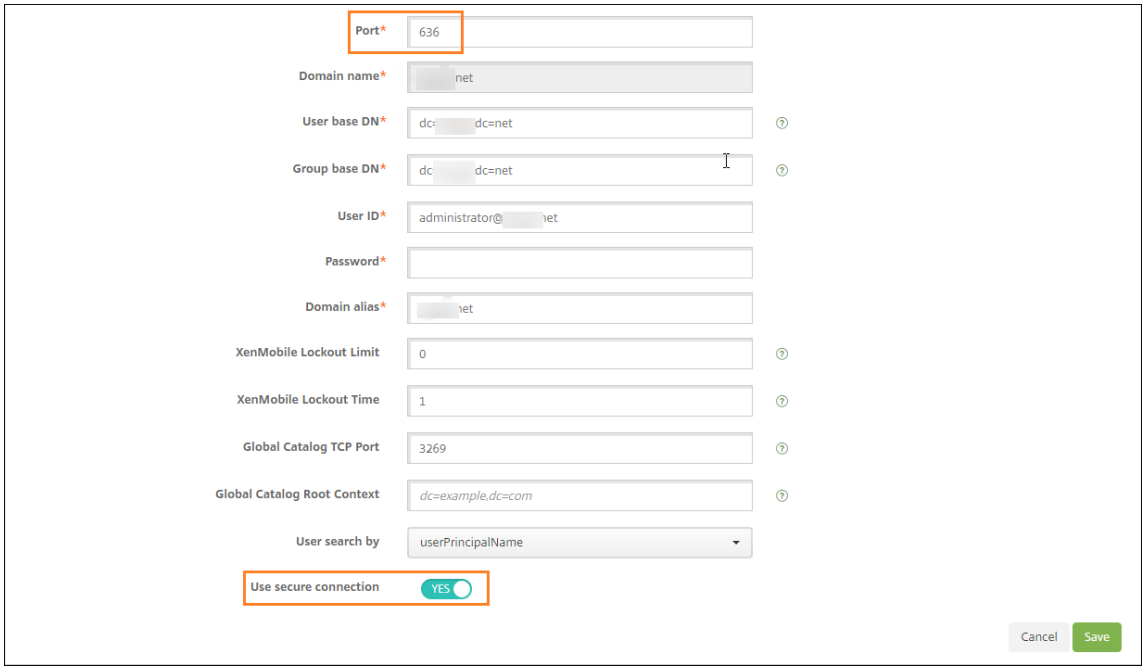
LDAP 설정구성

인증에 LDAP 를사용하려면 XenMobile 에인증기관에서발급한 SSL 인증서를설치해야합니다. 자세한내용은 XenMobile 에서인증서업로드를참조하십시오.

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



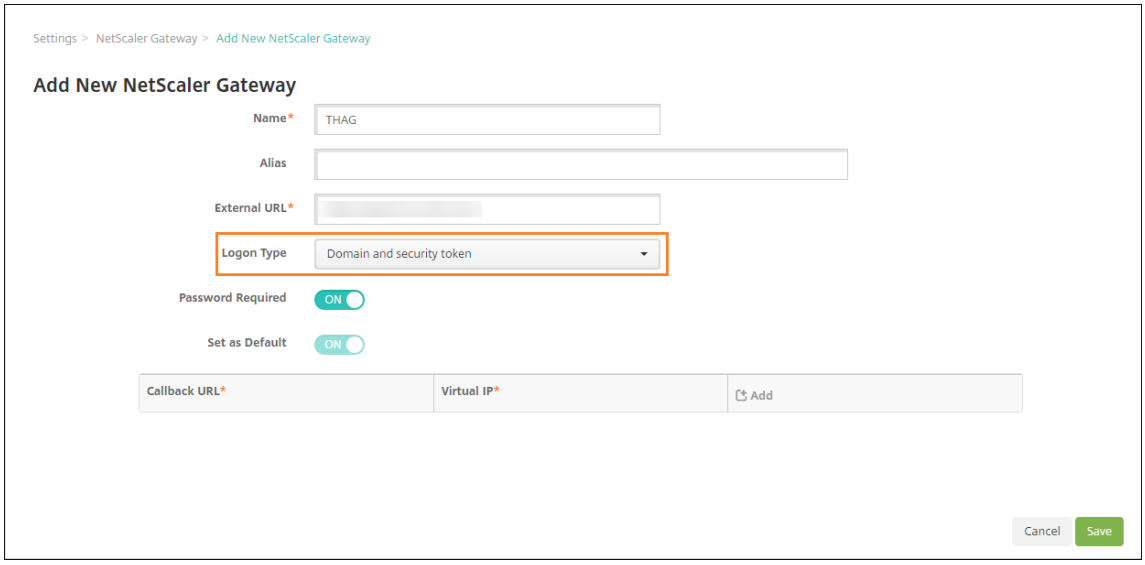
3. 포트가 **636**(보안 LDAP 연결의경우) 또는 **3269**(Microsoft 보안 LDAP 연결의경우) 인지확인합니다.
4. 보안연결사용을 예로변경합니다.



Citrix Gateway 설정구성

다음단계에서는이미 Citrix Gateway 인스턴스를 XenMobile 에추가했다고가정합니다. Citrix Gateway 인스턴스를추가하려면 Citrix Gateway 인스턴스추가를참조하십시오.

1. 설정에서 **Citrix Gateway** 를클릭합니다.
2. **Citrix Gateway** 를선택하고 편집을클릭합니다.
3. 로그온유형에서 도메인및보안토큰을선택합니다.



Citrix PIN 및사용자암호캐싱사용

Citrix PIN 및사용자암호캐싱을사용하도록설정하려면 설정 **>** 클라이언트속성으로이동하여 **Enable Citrix PIN Authentication(Citrix PIN** 인증사용**)** 및 **Enable User Password Caching(**사용자암호캐싱사용**)** 확인란을선택합니다. 자세한내용은 클라이언트속성을참조하십시오.

도메인및보안토큰인증을위해 **Citrix Gateway** 구성

XenMobile 과함께사용되는가상서버에대한 Citrix Gateway 세션프로필및정책을구성합니다. 자세한내용은 Citrix Gateway 설명서를참조하십시오.

클라이언트인증서인증또는인증서와도메인인증

August 12, 2022

XenMobile 에대한기본구성은사용자이름및암호인증입니다. XenMobile 환경에대한등록및액세스시추가보안계층을추가하려면인증서기반인증을사용하는것이좋습니다. XenMobile 환경에서이구성은보안과사용자환경을모두고려한최고의조합입니다. 인증서인증과도메인인증을함께사용하면 SSO 를사용하는동시에 Citrix ADC 의 2 단계인증을통해강화된보안이적용됩니다.

사용편의성을최적화하기위해인증서및도메인인증을 Citrix PIN 및 Active Directory 암호캐싱과결합할수있습니다. 그러면사용자가 LDAP 사용자이름과암호를반복적으로입력하지않아도됩니다. 등록, 암호만료및계정잠금의경우사용자가사용자이름과암호를입력합니다.

> 중요:
>
> XenMobile 은사용자가 XenMobile 에서장치를등록한후도메인인증에서다른인증모드로의인증모드변경을지원하지않습니다.

LDAP 를허용하지않고스마트카드또는유사한방법을사용하는경우인증서를구성하면 XenMobile 에스마트카드를나타낼수있습니다. 그런다음사용자는 XenMobile 에서생성된고유한 PIN 을사용하여등록합니다. 사용자가액세스권한을획득하면 XenMobile 이 XenMobile 환경에인증하는데사용될인증서를만들어배포합니다.

Citrix ADC 인증서전용인증또는인증서및도메인인증을사용하는경우 XenMobile 용 Citrix ADC 마법사를통해 XenMobile 에필요한구성을수행할수있습니다. XenMobile 용 Citrix ADC 마법사는한번만실행할수있습니다.

보안이매주중요한환경에서는조직외부의공용네트워크또는보안되지않은네트워크에서 LDAP 자격증명을사용하는것이조직에큰 보안위협으로간주됩니다. 이러한환경에서는클라이언트인증서와보안토큰을사용하는 2 단계인증을선택할수있습니다. 자세한내용은 Configuring XenMobile for Certificate and Security Token Authentication(인증서및보안토큰인증을사용하기위한 XenMobile 구성)을참조하십시오.

클라이언트인증서인증은 XenMobile MAM 모드 (MAM 단독) 및 ENT 모드 (사용자가 MDM 으로등록시) 에사용할수있습니다. 하지만사용자가레거시 MAM 모드로등록하는경우클라이언트인증서인증을 XenMobile ENT 모드에사용할수없습니다. XenMobile ENT 및 MAM 모드로클라이언트인증서인증을사용하려면 Microsoft 서버와 XenMobile Server 를구성한후 Citrix Gateway 를구성해야합니다. 이문서에설명된대로다음의일반적인단계를따릅니다.

Microsoft 서버:

1. Microsoft Management Console 에인증서스냅인을추가합니다.
2. CA(인증기관) 에템플릿을추가합니다.
3. CA 서버에서 PFX 인증서를만듭니다.

XenMobile Server:

1. XenMobile 에인증서를업로드합니다.
2. 인증서기반인증을위한 PKI 엔터티를만듭니다.
3. 자격증명공급자를구성합니다.
4. 인증을위한사용자인증서를제공하도록 Citrix Gateway 를구성합니다.

Citrix Gateway 구성에대한자세한내용은 Citrix ADC 설명서의다음문서를참조하십시오.

- Client authentication(클라이언트인증)
- SSL profile infrastructure(SSL 프로필인프라)
- Configuring and Binding a Client Certificate Authentication Policy(클라이언트인증서인증구성및바인딩)

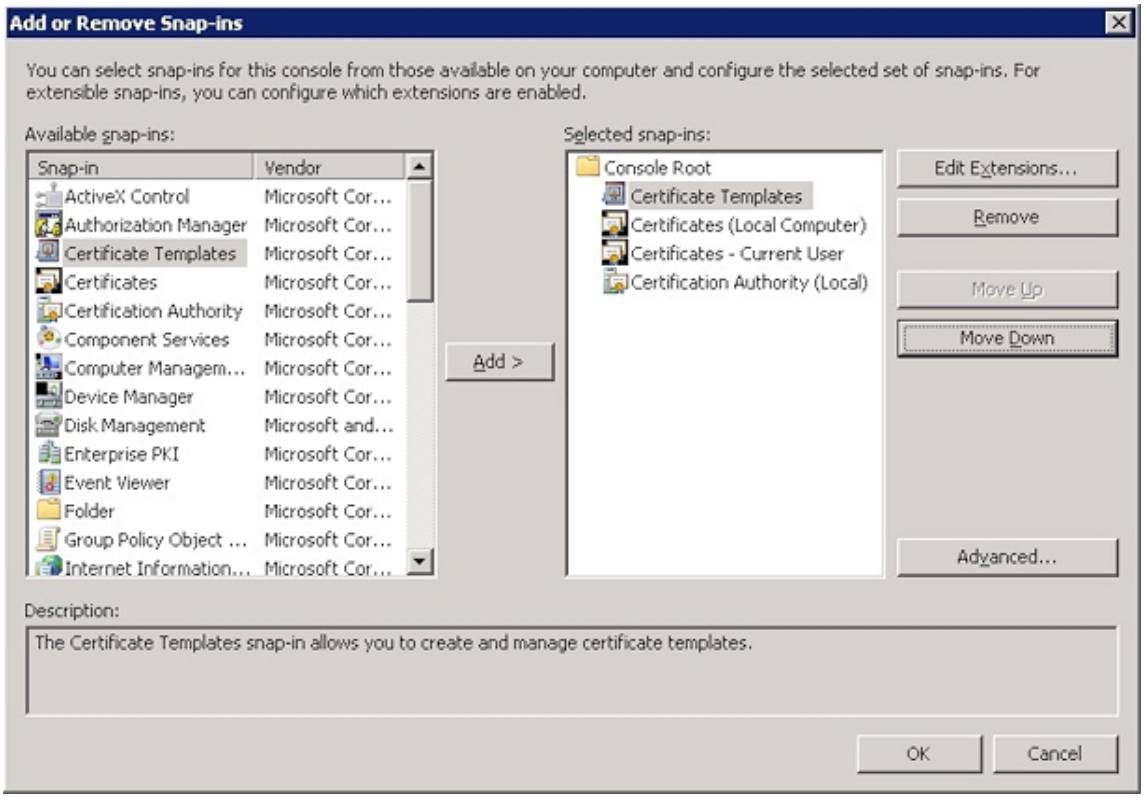
사전요구사항

- Microsoft 인증서서비스엔터티템플릿을생성할때는특수문자를제외하여등록된장치와관련된인증문제를방지하십시오. 예를들어템플릿이름에다음문자를사용하지마십시오. : ! $ ()## % + * ~ ? | { } []

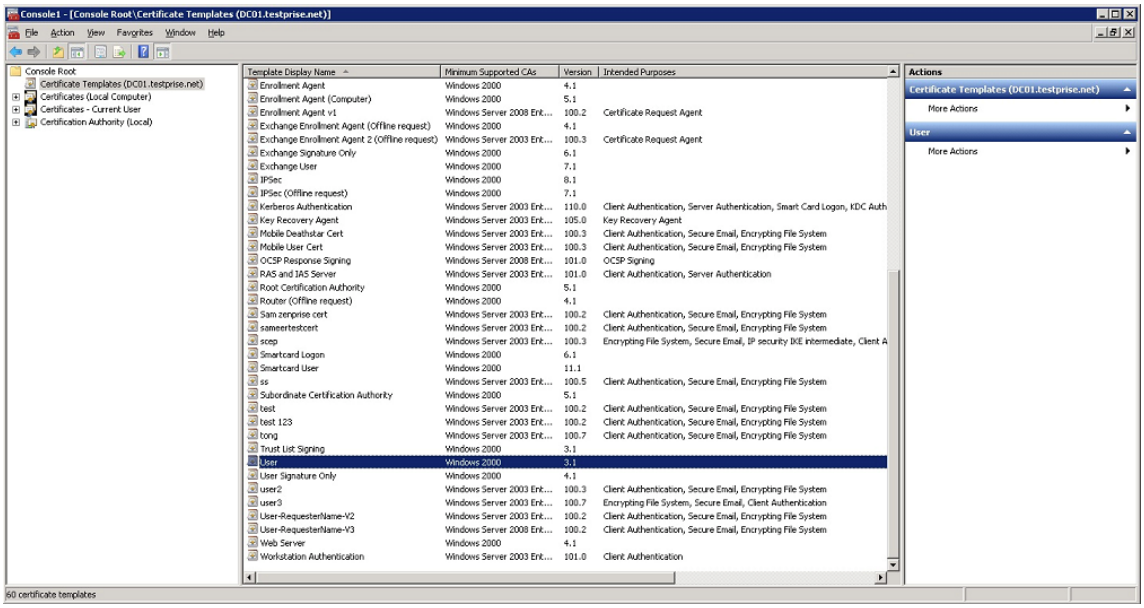
- Exchange ActiveSync 에대한인증서기반인증을구성하려면이 Microsoft 블로그를참조하십시오. 클라이언트인증서를요구하도록 Exchange ActiceSync 의인증기관 (CA) 서버사이트를구성합니다..
- Exchange Server 로의 ActiveSync 트래픽을보안하기위해개인서버인증서를사용하는경우, 필요한모든루트및중간인증서가모바일장치에있어야합니다. 그렇지않으면 Secure Mail 에서사서함을설정하는동안인증서기반인증이실패합니다. Exchange IIS 콘솔에서다음작업을수행해야합니다.
  - Exchange 와함께 XenMobile 을사용하기위한웹사이트를추가하고웹서버인증서를바인딩합니다.
  - 포트 9443 을사용합니다.
  - 해당웹사이트에대해 “Microsoft Server ActiveSync” 용하나와 “EWS” 용하나의두가지응용프로그램을추가해야합니다. 이러한응용프로그램모두에대해 **SSL** 설정아래에서 **SSL** 필요를선택합니다.

Microsoft Management Console 에인증서스냅인을추가합니다

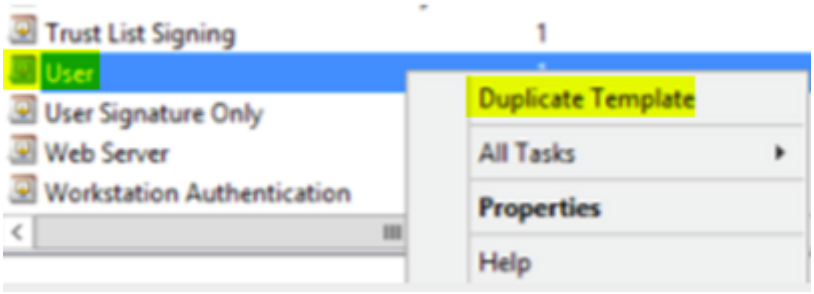
1. 콘솔을열고 스냅인추가/제거를클릭합니다.
2. 다음과같은스냅인을추가합니다.
   - 인증서템플릿
   - 인증서 (로컬컴퓨터)
   - 인증서 - 현재사용자
   - 인증기관 (로컬)



3. 인증서템플릿을확장합니다.



4. 사용자템플릿과 템플릿복제를선택합니다.

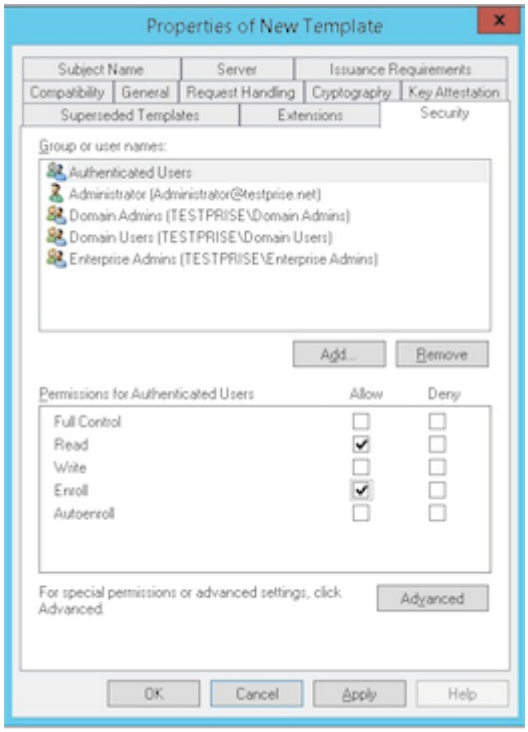


5. 템플릿표시이름을제공합니다.

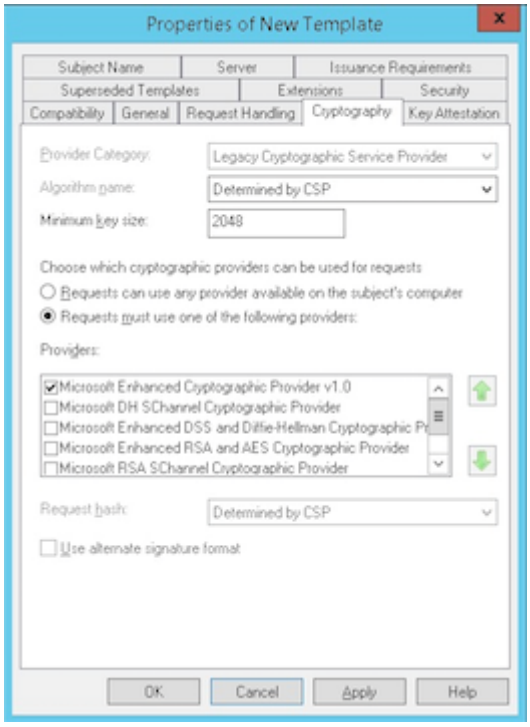
> 중요:
>
> 필요한경우에만 **Active Directory** 에인증서게시확인란을선택합니다. 이옵션을선택하면모든사용자클라이언트인증서가 Active Directory 에서생성되어 Active Directory 데이터베이스가복잡해질수있습니다.

6. 템플릿유형으로 **Windows 2003 Server** 를선택합니다. Windows 2012 R2 서버에서 호환성아래에있는 인증기관을선택하고받는사람을 **Windows 2003** 으로설정합니다.

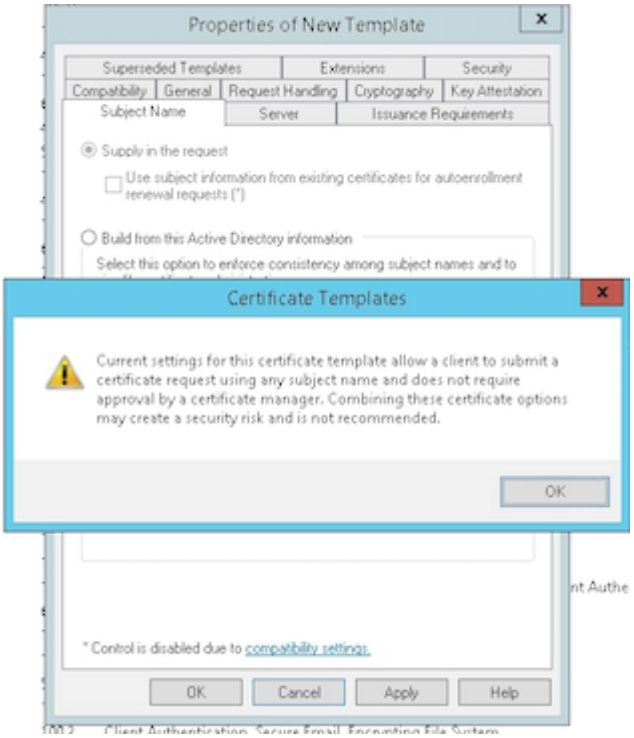
7. 보안아래에서인증된사용자에대해 허용열의 등록옵션을선택합니다.



8. 암호화아래에서키크기를제공하는지확인합니다. 키크기는나중에 XenMobile 을구성할때입력합니다.

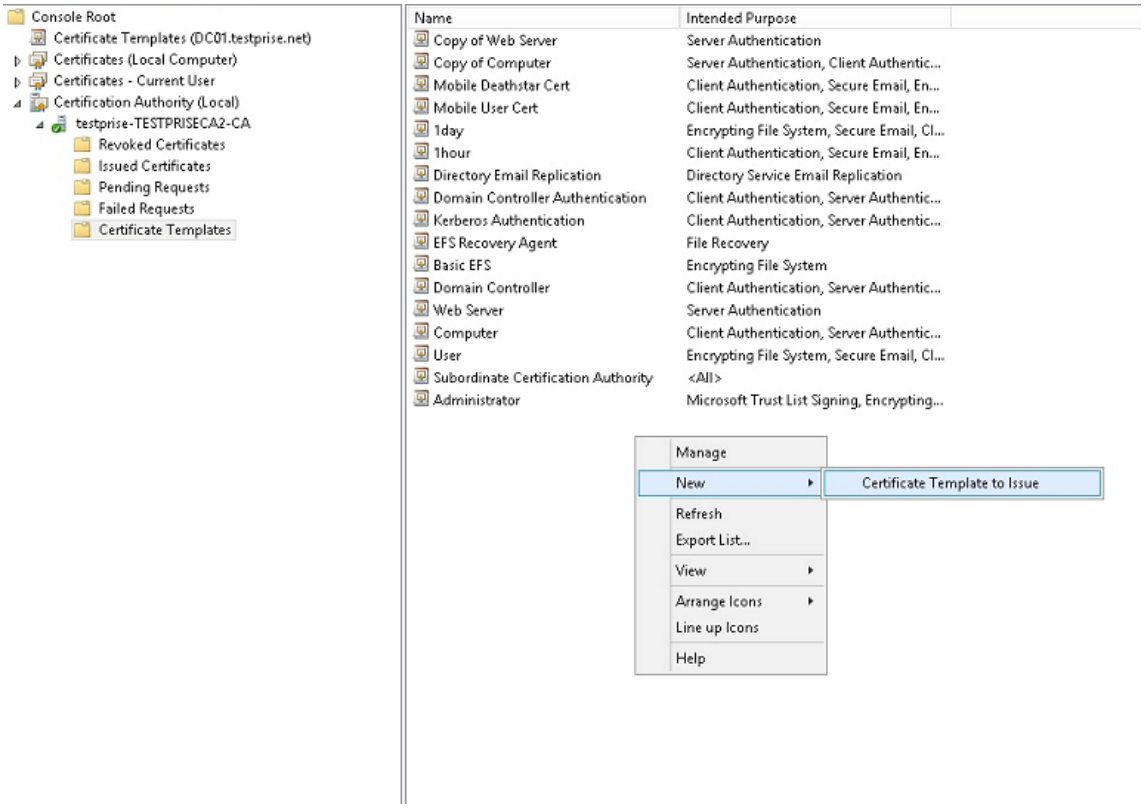


9. 주체이름아래에서 요청에서제공을선택합니다. 변경내용을적용한후저장합니다.

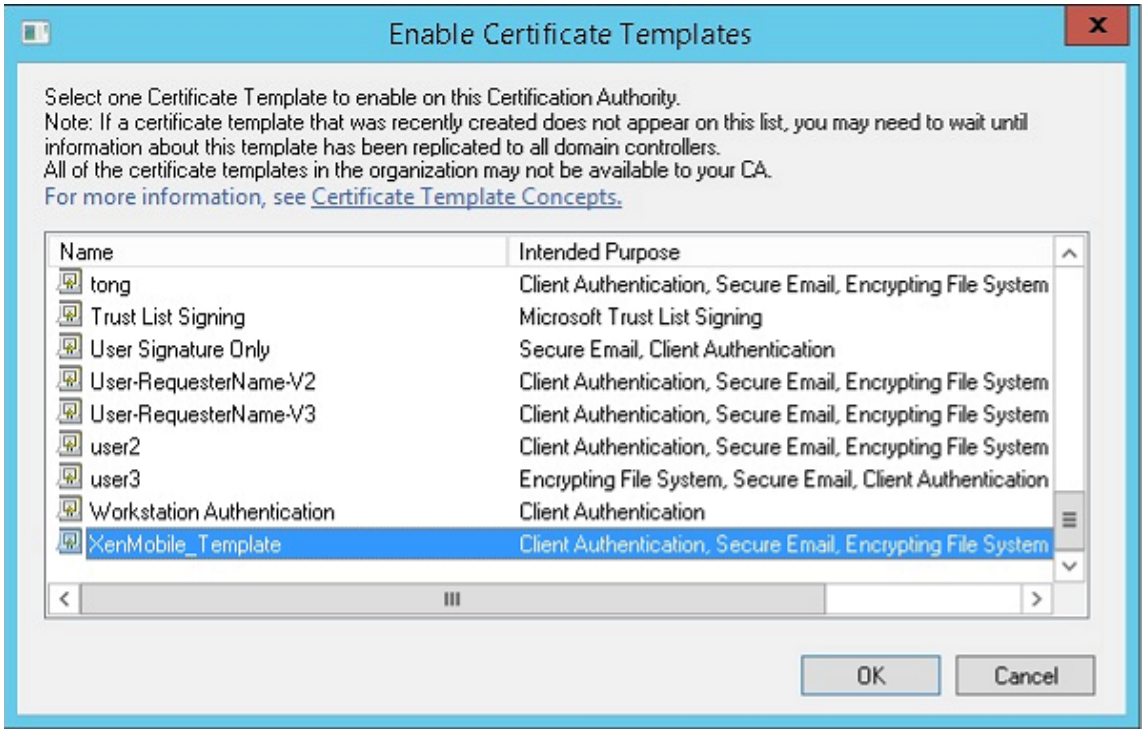


인증기관에템플릿추가

1. 인증기관으로이동하여 인증서템플릿을선택합니다.
2. 오른쪽창에서마우스오른쪽단추를클릭한후 새로만들기 **>** 발급할인증서템플릿을선택합니다.

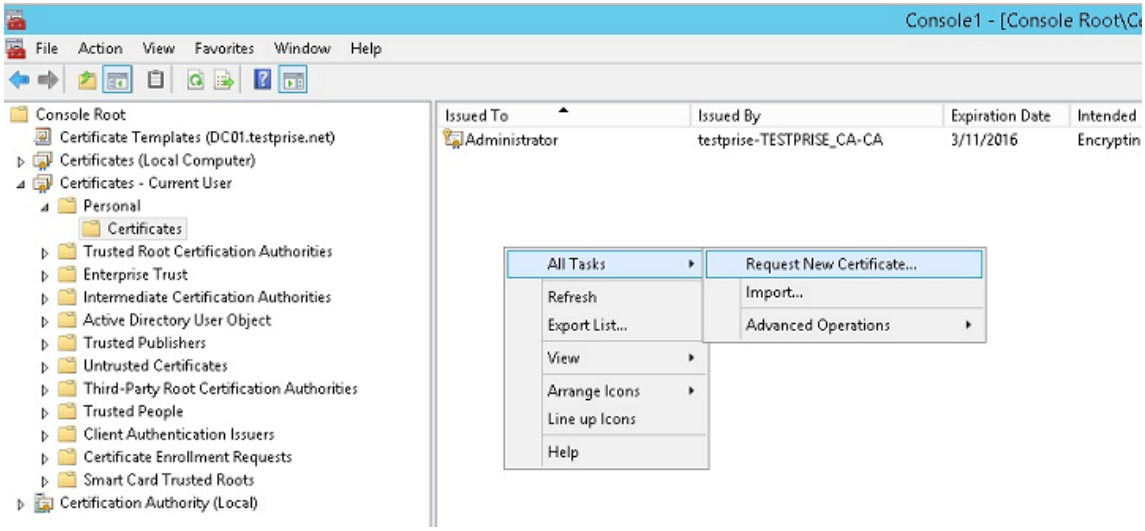


3. 이전단계에서만든템플릿을선택한다음 확인을클릭하여 인증기관에추가합니다.

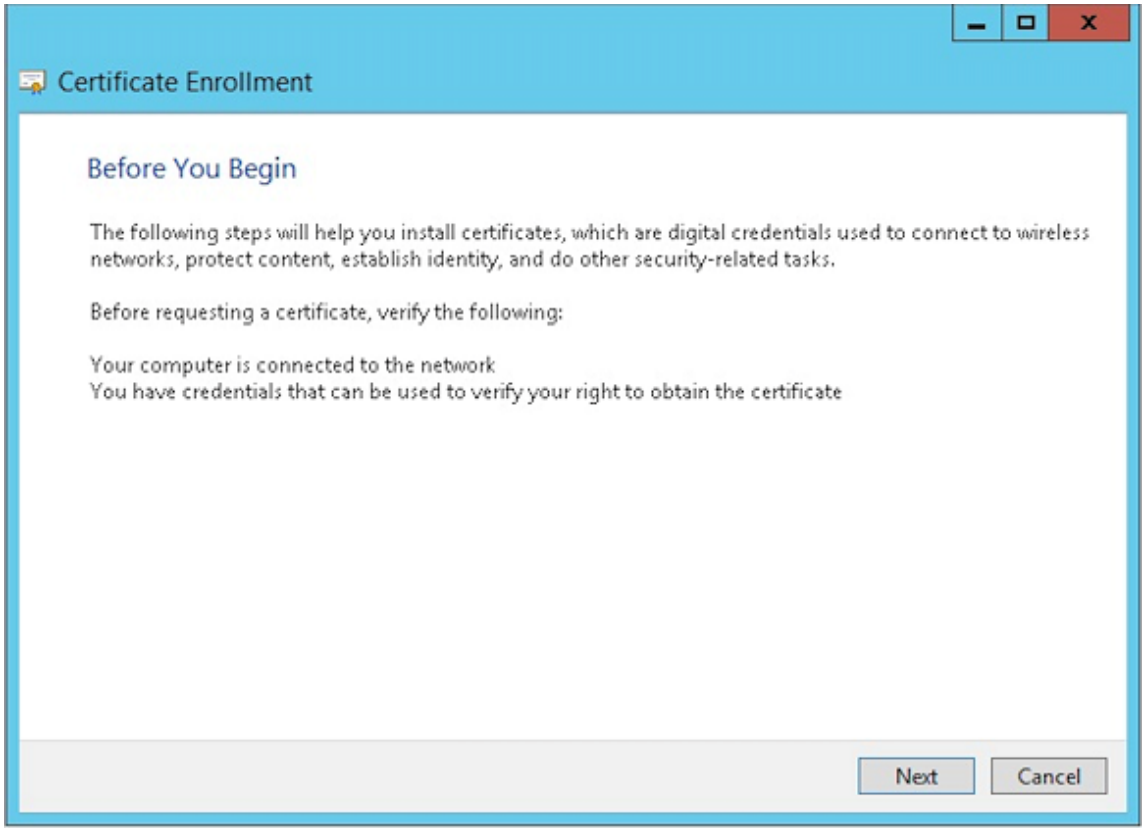


CA 서버에서 **PFX** 인증서만들기

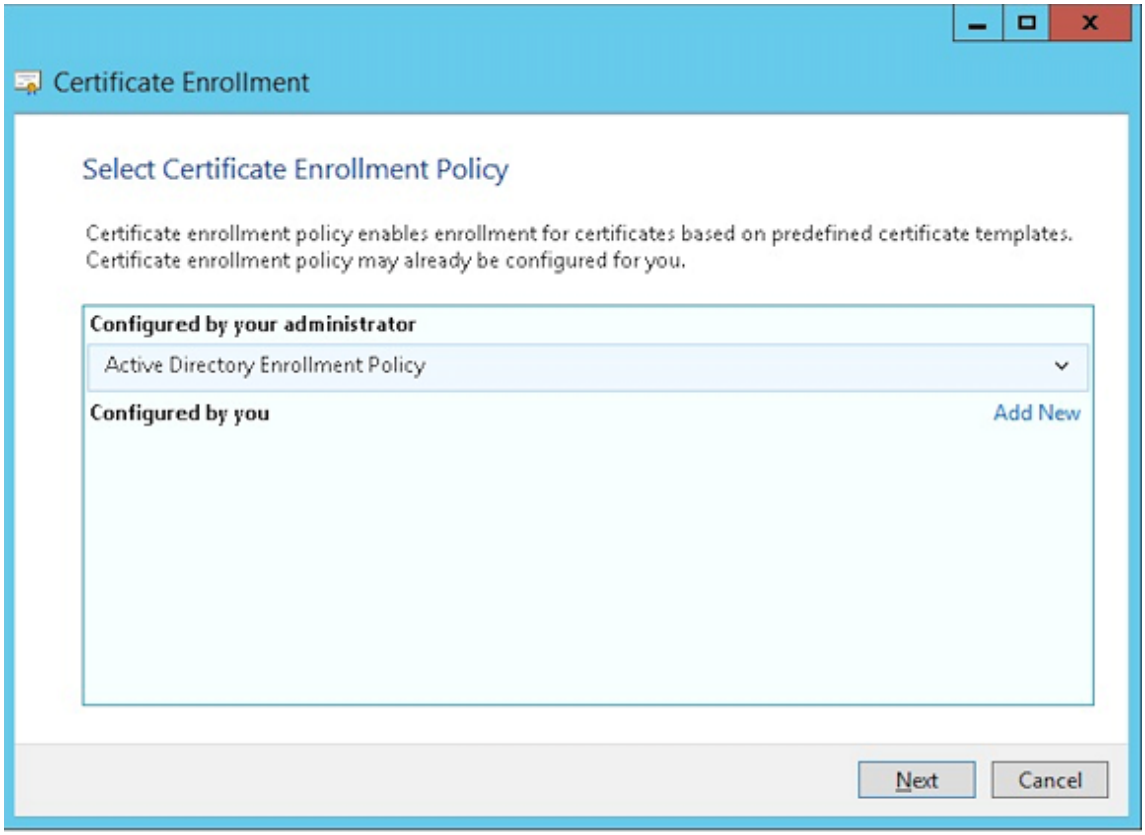
1. 로그인한서비스계정을사용하여사용자.pfx 인증서를만듭니다. .pfx 를 XenMobile 에업로드하면 XenMobile 이장치를등록하는사용자에대해사용자인증서를요구하게됩니다.
2. 현재사용자아래에서 인증서를확장합니다.
3. 오른쪽창을마우스오른쪽단추로클릭하고 새인증서요청을클릭합니다.



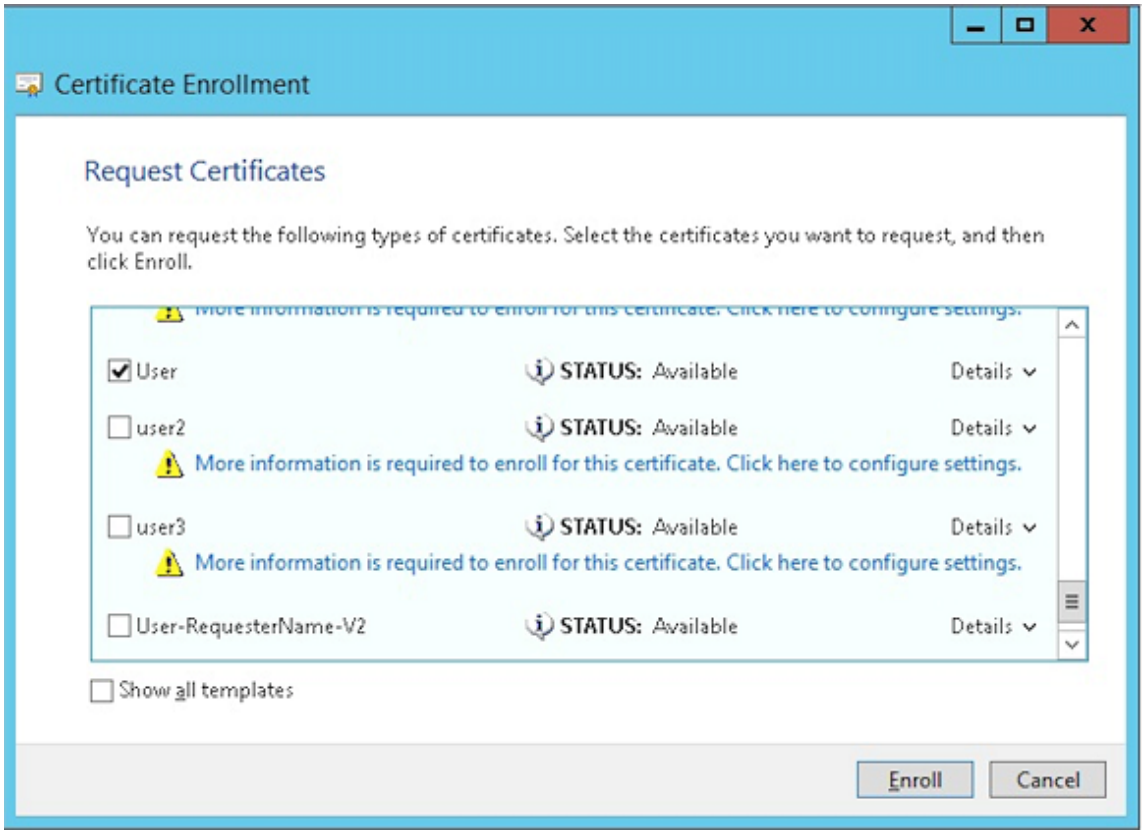
4. 인증서등록화면이나타납니다. 다음을클릭합니다.



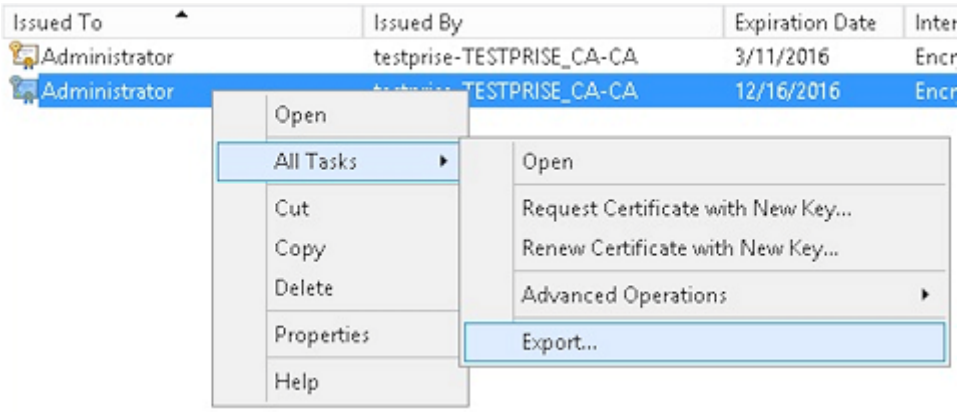
5. **Active Directory** 등록정책을선택하고 다음을클릭합니다.



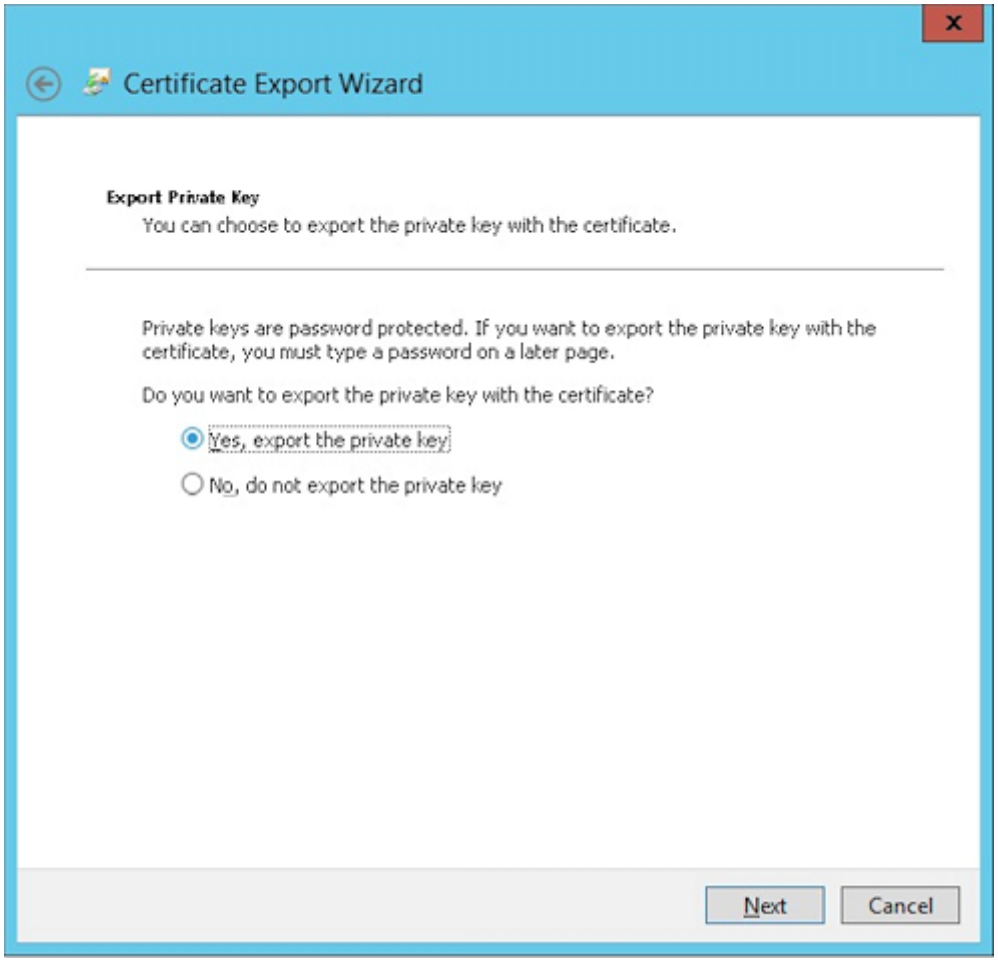
6. 사용자템플릿을선택한후 등록을클릭합니다.



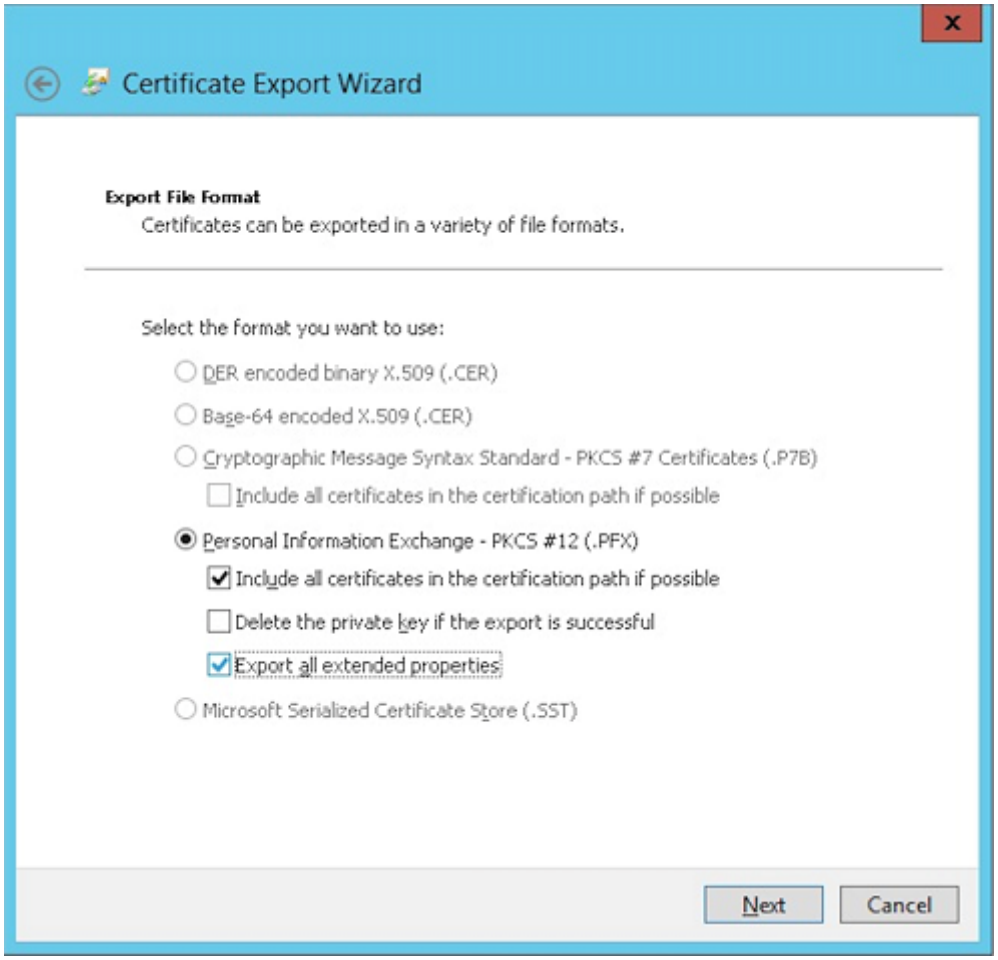
7. 이전단계에서만든.pfx 파일을내보냅니다.



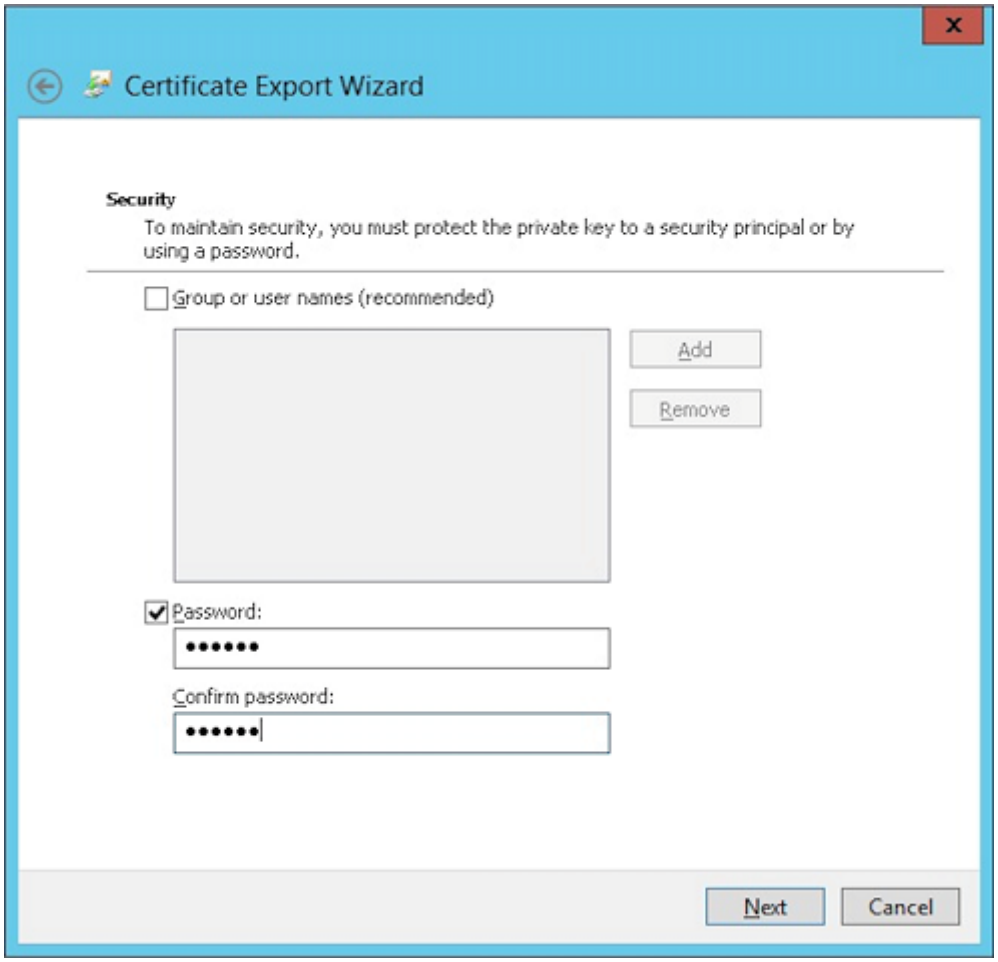
8. 예, 개인키를내보냅니다를클릭합니다.



9. 가능하면인증경로에있는인증서모두포함및 확장속성모두내보내기확인란을선택합니다.



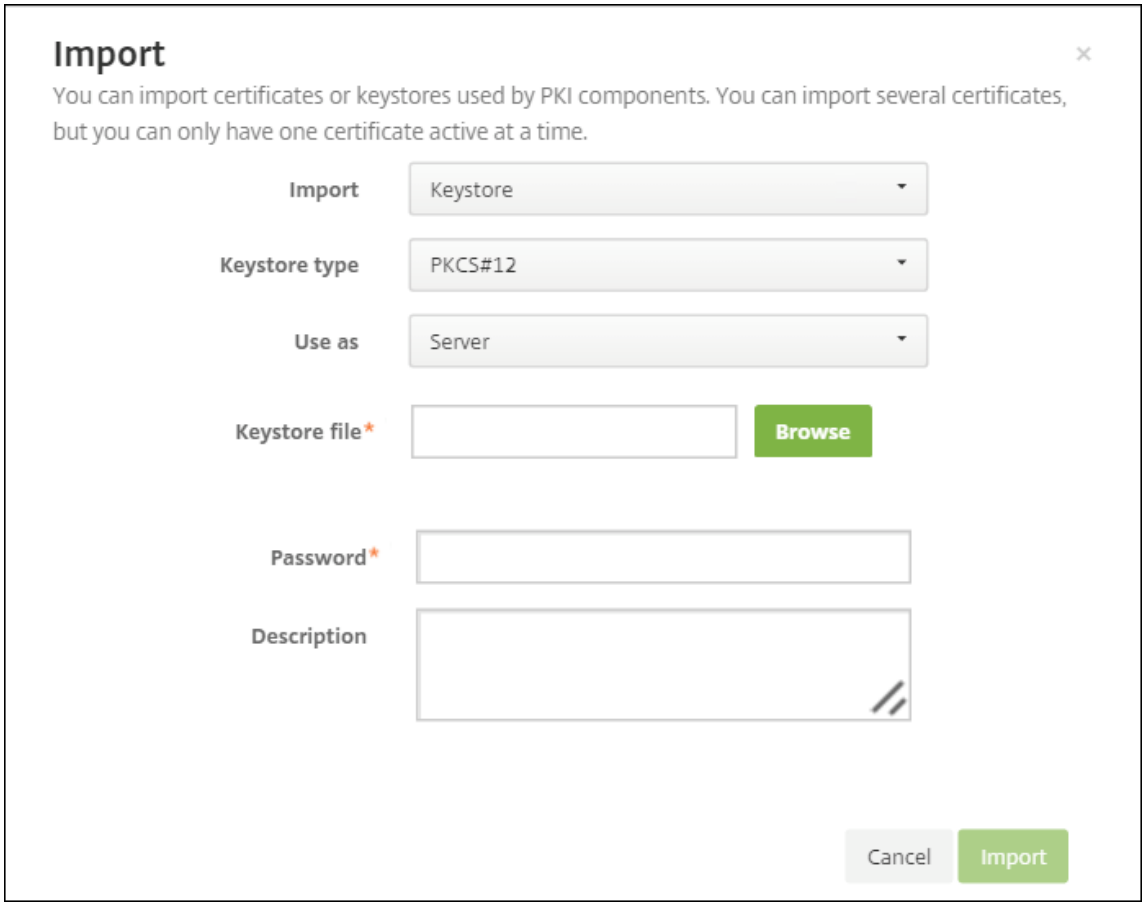
10. XenMobile 에이인증서를업로드할때사용할암호를설정합니다.



11. 하드드라이브에인증서를저장합니다.

XenMobile 에인증서업로드

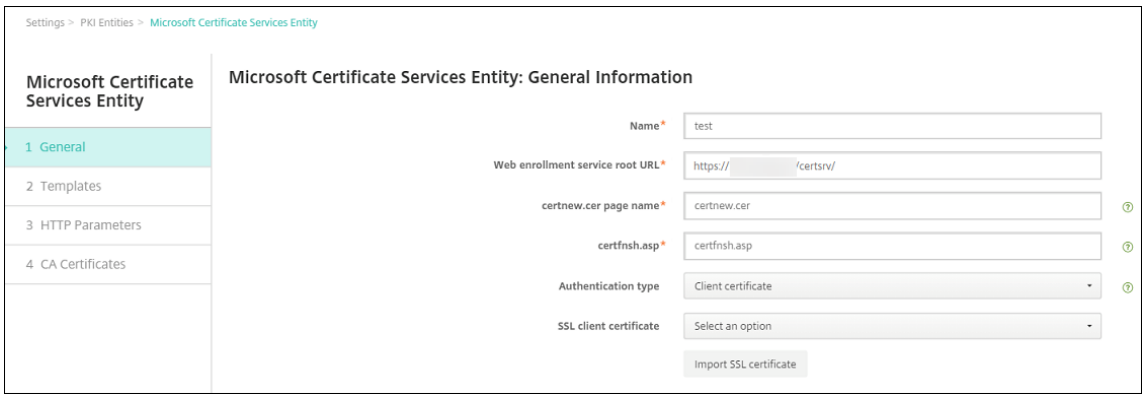
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정화면이나타납니다.
2. 인증서를클릭한후 가져오기를클릭합니다.
3. 다음매개변수를입력합니다.
   - 가져오기**:** 키저장소
   - 키저장소유형**:** PKCS #12
   - 용도**:** 서버
   - 키저장소파일**:** 찾아보기를클릭하여만들어둔 `.pfx` 인증서를선택합니다.
   - 암호**:** 이인증서에대해만든암호를입력합니다.



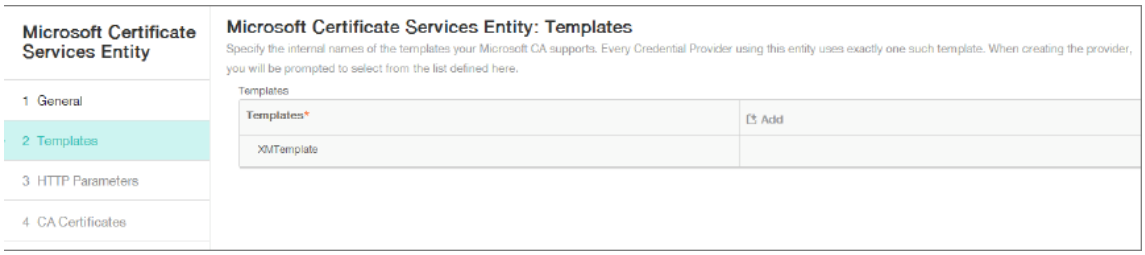
4. 가져오기를클릭합니다.
5. 인증서가올바르게설치되었는지확인합니다. 올바르게설치된인증서가사용자인증서로표시됩니다.

인증서기반인증을위한 **PKI** 엔터티만들기

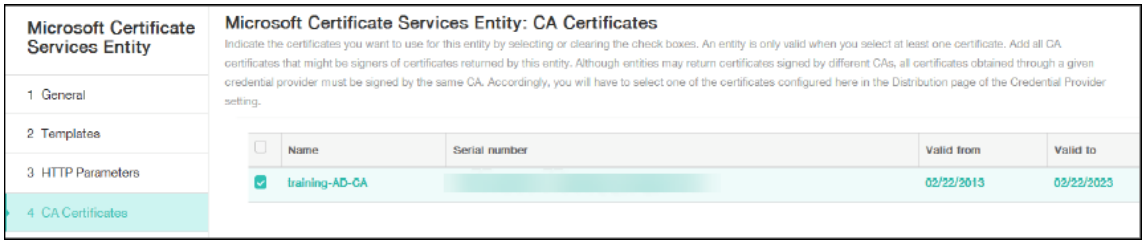
1. 설정에서 자세히 **>** 인증서관리 **> PKI** 엔터티로이동합니다.
2. 추가를클릭한후 **Microsoft** 인증서서비스엔터티를클릭합니다. **Microsoft** 인증서서비스엔터티**:** 일반정보화면이나타납니다.
3. 다음매개변수를입력합니다.
   - 이름**:** 원하는이름을입력합니다.
   - 웹등록서비스루트 **URL:** `https://RootCA-URL/certsrv/` URL 경로에서마지막슬래시 (/) 를반드시추가해야합니다.
   - **certnew.cer** 페이지이름**:** certnew.cer(기본값)
   - **certfnsh.asp:** certfnsh.asp(기본값)
   - 인증유형**:** 클라이언트인증서
   - **SSL** 클라이언트인증서**:** XenMobile 클라이언트인증서를발급하는데사용할사용자인증서를선택합니다.



4. 템플릿아래에서 Microsoft 인증서를구성할때만든템플릿을추가합니다. 공백을추가하지마십시오.



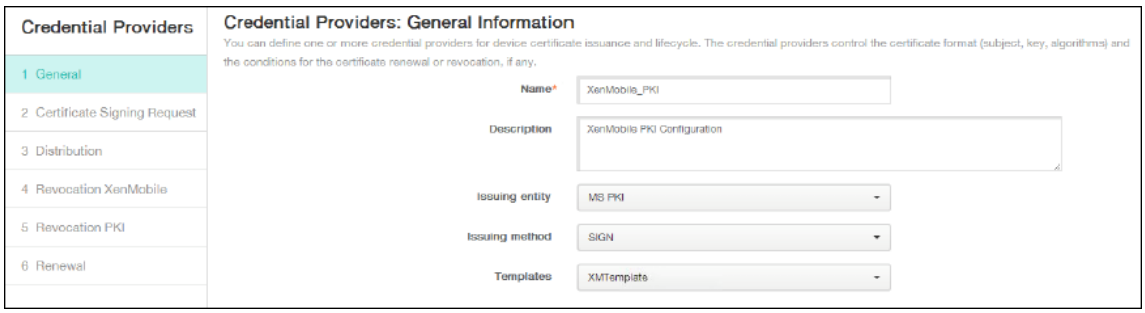
5. HTTP 매개변수를생략하고 **CA** 인증서를클릭합니다.
6. 사용자환경에해당하는루트 CA 이름을선택합니다. 이루트 CA 는 XenMobile 클라이언트인증서에서가져온체인의일부입니다.



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.



4. **CSR** 을클릭한후다음매개변수를입력합니다.

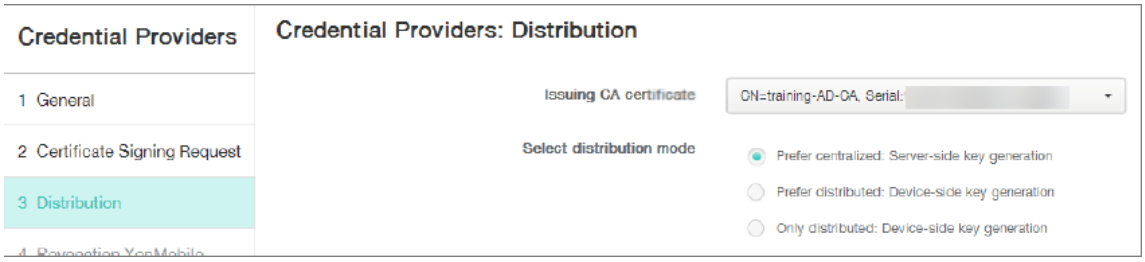
   - 키알고리즘**:** RSA
   - 키크기**:** 2048
   - 서명알고리즘**:** SHA256withRSA
   - 주체이름 `cn=$user.username`

   주체대체이름에대해 추가를클릭한후다음매개변수를입력합니다.

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

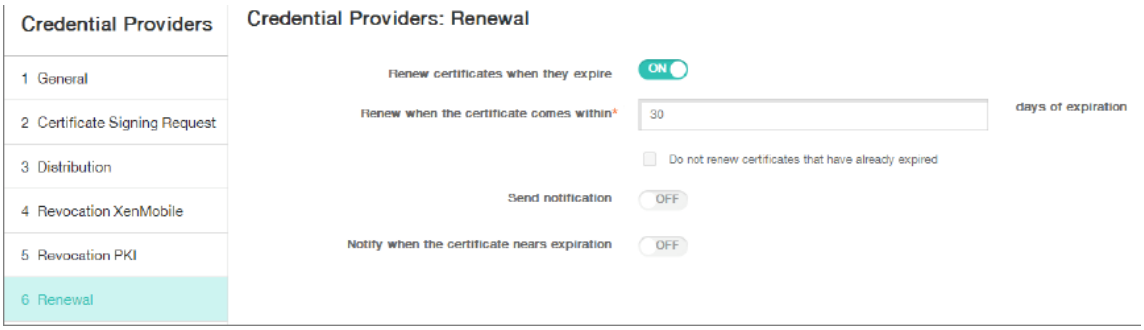
5. 배포를클릭한후다음매개변수를입력합니다.

   - **CA** 인증서발급**:** XenMobile 클라이언트인증서에서명한발급 CA 를선택합니다.
   - 배포모드선택**:** 중앙집중식선호**:** 서버측키생성을선택합니다.



6. 그다음의두섹션, 즉 해지 **XenMobile** 및 해지 **PKI** 에대해필요에따라매개변수를설정합니다. 이예에서는두옵션을모두건너뜁니다.
7. 갱신을클릭합니다.

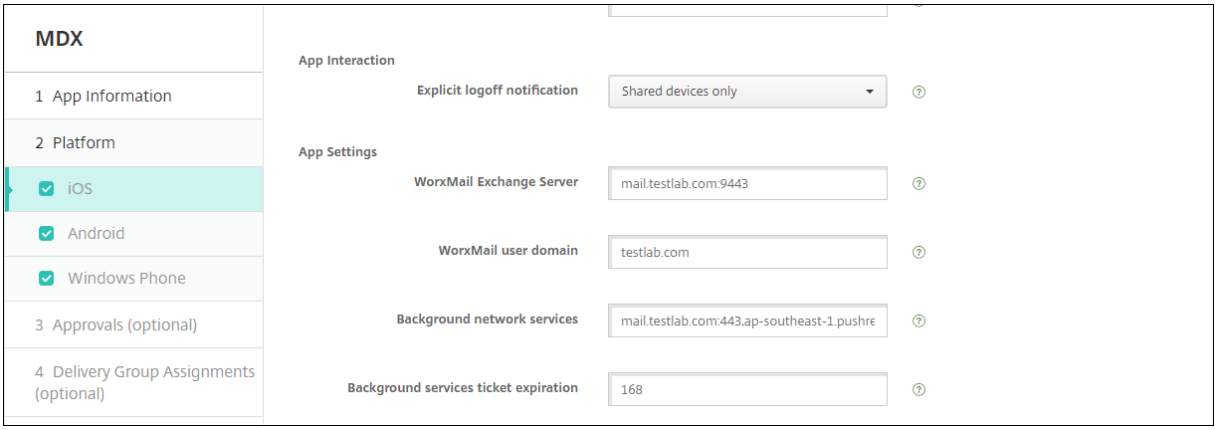
8. 인증서가만료될때갱신에대해 켜짐을선택합니다.
9. 다른모든설정을기본값으로그대로두거나필요에따라변경합니다.



10. 저장을클릭합니다.

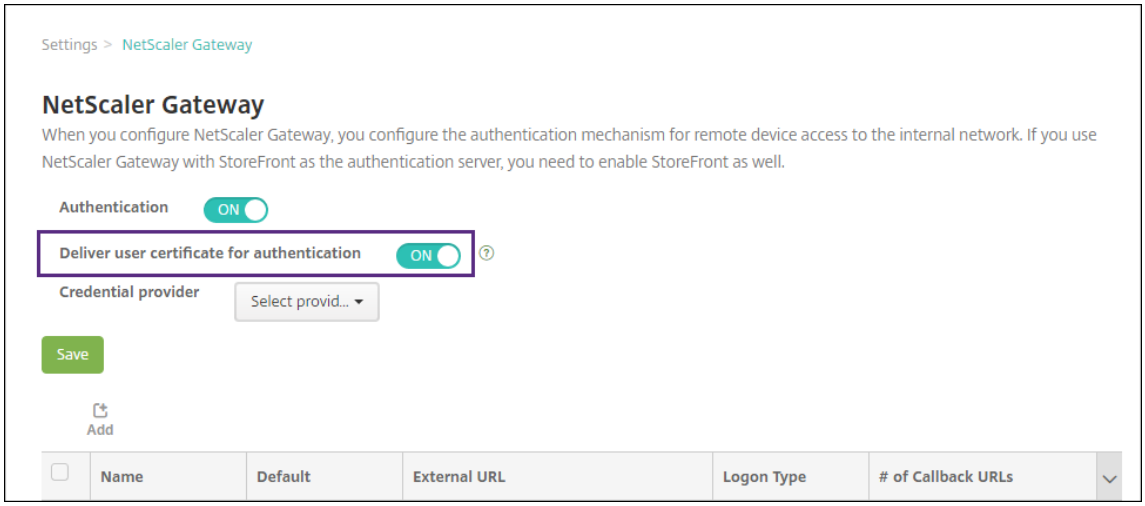
인증서기반인증을사용하도록 **Secure Mail** 구성

Secure Mail 을 XenMobile 에추가할경우, 앱설정아래에서 Exchange 설정을구성해야합니다.

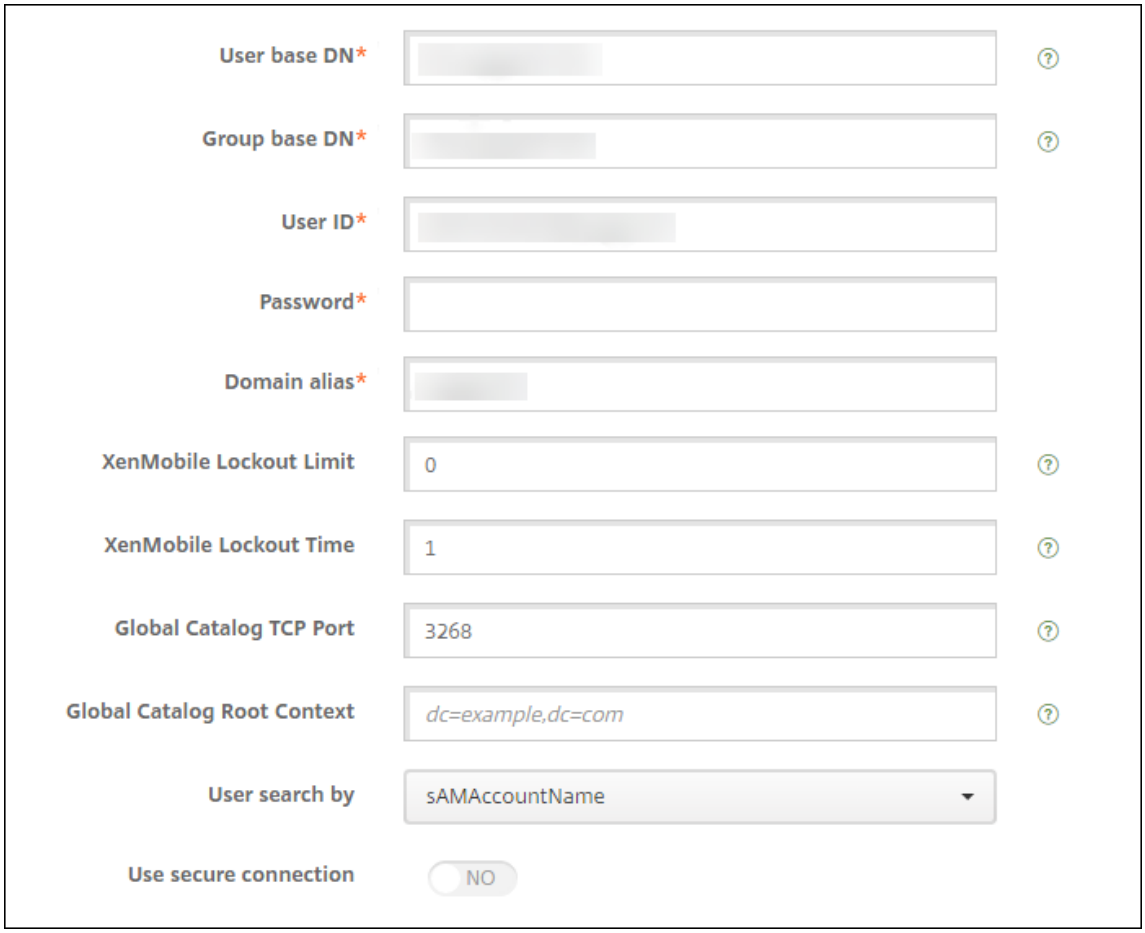


XenMobile 에서 **Citrix ADC** 인증서제공구성

1. XenMobile 콘솔에로그온하고오른쪽위모서리의기어아이콘을클릭합니다. 설정화면이나타납니다.
2. 서버아래에서 **Citrix Gateway** 를클릭합니다.
3. Citrix Gateway 가아직추가되지않은경우 추가를클릭하고설정을지정합니다.
   - 외부 **URL:** `https://YourCitrixGatewayURL`
   - 로그온유형**:** 인증서및도메인
   - 암호필요**:** 꺼짐
   - 기본값으로설정**:** 켜짐
4. 인증을위한사용자인증서제공에서 켜짐을선택합니다.



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



Citrix PIN 및사용자암호캐싱사용

Citrix PIN 및사용자암호캐싱을사용하도록설정하려면 설정 **>** 클라이언트속성으로이동하여 **Enable Citrix PIN Authentication(Citrix PIN** 인증사용**)** 및 **Enable User Password Caching(**사용자암호캐싱사용**)** 확인란을선택합니다. 자세한내용은 클라이언트속성을참조하십시오.

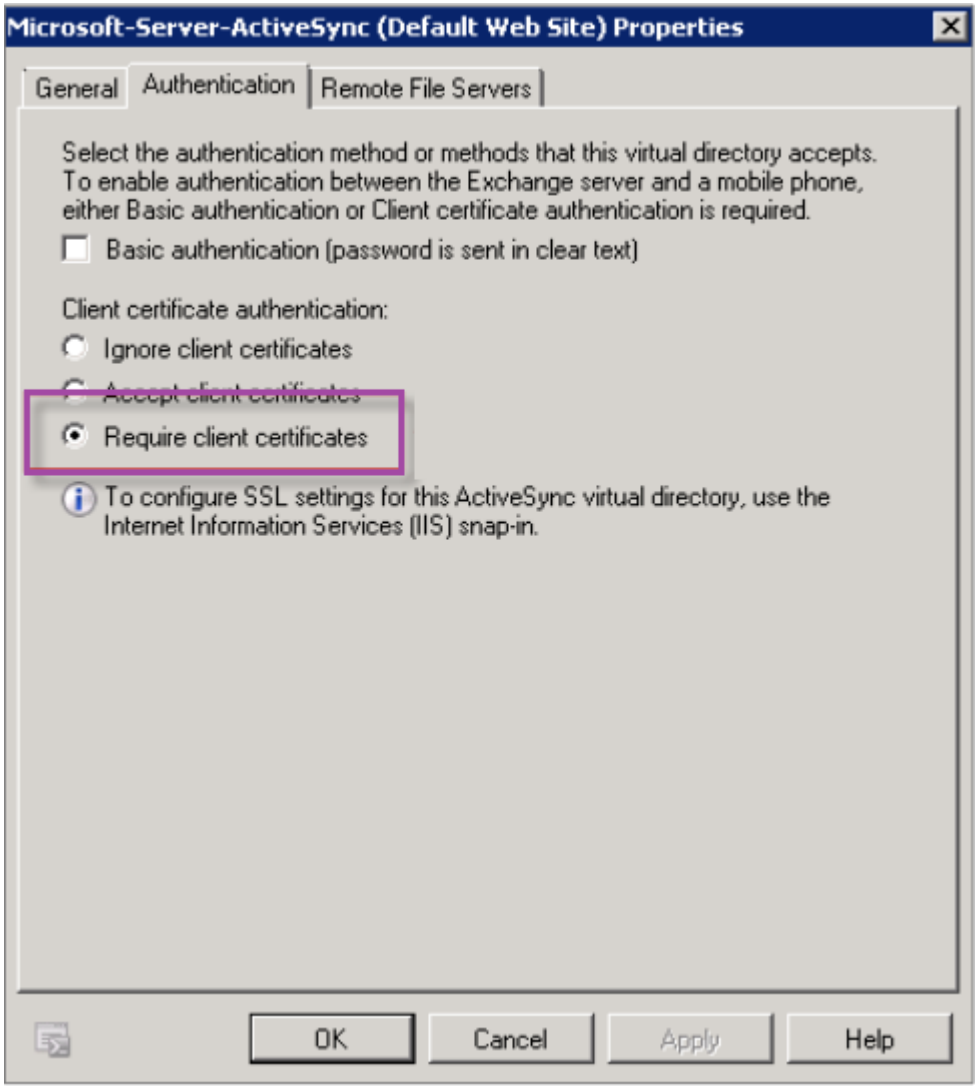
클라이언트인증서구성문제해결

위의구성과 Citrix Gateway 구성을성공적으로완료한후사용자워크플로는다음과같습니다.

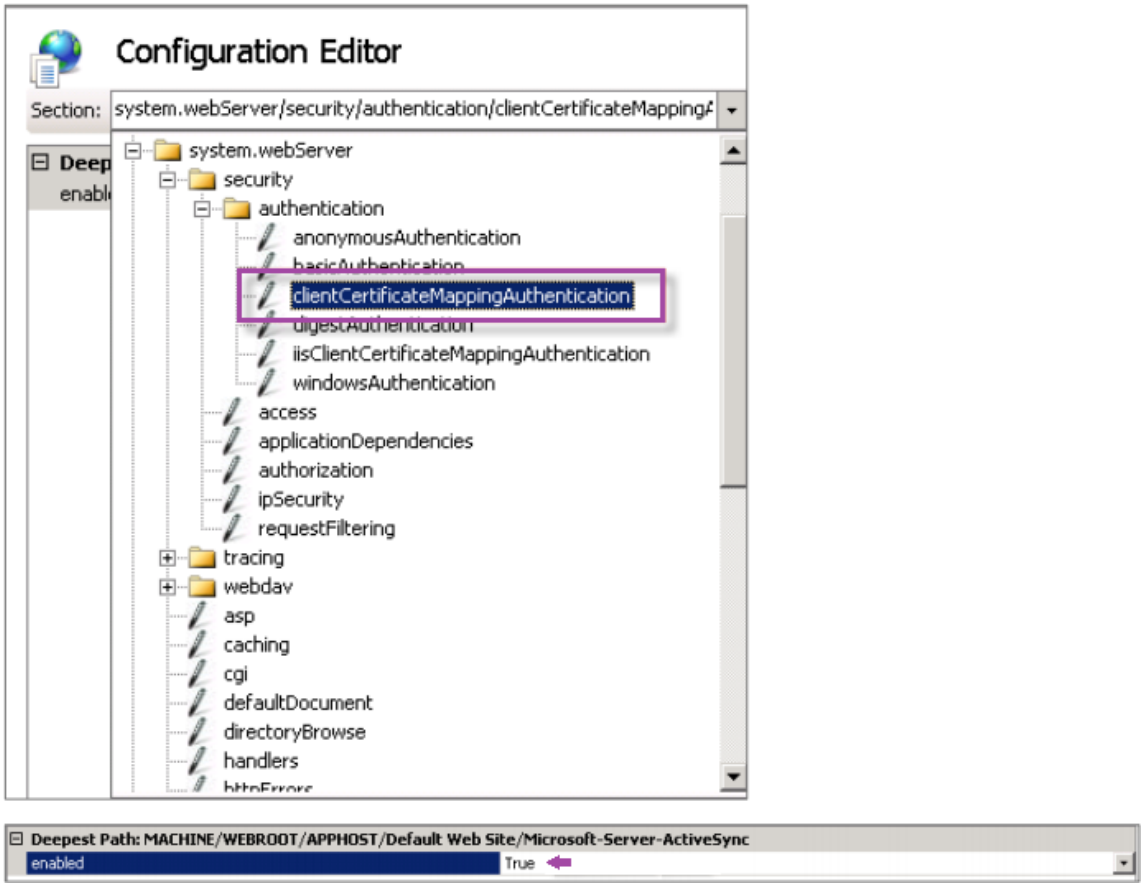
1. 사용자가모바일장치를등록합니다.
2. XenMobile 에서 Citrix PIN 을만들라는메시지를사용자에게표시합니다.
3. 그런다음사용자가 XenMobile Store 로리디렉션됩니다.
4. 사용자가 Secure Mail 을시작할때는 XenMobile 이사서함구성을위한사용자자격증명을입력하라는메시지를표시하지않습니다. 대신 Secure Mail 이 Secure Hub 에서클라이언트인증서를요청하고인증을위해 Microsoft Exchange Server 에제출합니다. 사용자가 Secure Mail 을시작할때자격증명을입력하라는메시지가 XenMobile 에표시될경우구성을확인하십시오.

사용자가 Secure Mail 을다운로드하고설치할수있지만사서함구성중에 Secure Mail 이구성을완료하지못할경우:

1. Microsoft Exchange Server ActiveSync 에서트래픽을보안하기위해개인 SSL 서버인증서를사용하는경우, 모든루트및중간인증서가모바일장치에설치되어있는지확인합니다.
2. ActiveSync 에대해선택한인증유형이 클라이언트인증서필요인지확인합니다.



3. Microsoft Exchange Server 에서 **Microsoft-Server-ActiveSync** 사이트를확인하여클라이언트인증서매핑인증이사용하도록설정되어있는지검토합니다. 기본적으로클라이언트인증서매핑은사용되지않습니다. 이옵션은 구성편집기 **>** 보안 **>** 인증아래에있습니다.



True 를선택한후에 적용을클릭해야변경내용이적용됩니다.

4. XenMobile 콘솔에서 Citrix Gateway 설정을확인합니다. 인증을위한사용자인증서제공이 켜짐이고 자격증명공급자에올바른프로필이선택되어있는지확인합니다.

클라이언트인증서가모바일장치에제공되었는지확인하려면

1. XenMobile 콘솔에서 관리 **>** 장치로이동하여장치를선택합니다.
2. 편집또는 자세히표시를클릭합니다.
3. 배달그룹섹션으로이동하여다음항목을검색합니다.

   Citrix Gateway Credentials: Requested credential, CertId=

클라이언트인증서협상을사용하도록설정했는지확인하려면

1. 다음 `netsh` 명령을실행하여 IIS 웹사이트에바인딩된 SSL 인증서구성을표시합니다.

   ```
   netsh http show sslcert
   ```

2. 클라이언트인증서협상의값이 사용안함인경우다음명령을실행하여사용하도록설정합니다.


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

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

예:

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

PKI 엔터티

May 17, 2022

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

XenMobile 은다음과같은 PKI 엔터티유형을지원합니다.

- Microsoft 인증서서비스
- 임의의 CA(인증기관)

XenMobile 은다음과같은 CA 서버를지원합니다.

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

일반적인 **PKI** 개념

유형에관계없이모든 PKI 엔터티는다음과같은하위집합의기능을갖습니다.

- 서명**:** CSR(인증서서명요청) 을기반으로새인증서발급
- 가져오기**:** 기존인증서및키쌍복구
- 해지**:** 클라이언트인증서해지

CA 인증서정보

PKI 엔터티를구성하는경우해당엔터티에의해발급 (또는복구) 되는인증서의서명자가어느 CA 인증서인지를 XenMobile 에알립니다. 이 PKI 엔터티는개수에제한없이서로다른 CA 가서명한 (가져오거나새로서명된) 인증서를반환할수도있습니다.

PKI 엔터티구성의일환으로이러한각 CA 의인증서를제공합니다. 이를위해인증서를 XenMobile 에업로드한후 PKI 엔터티에서참조해야합니다. 임의 discretionary CA 의경우인증서는묵시적으로서명 CA 인증서이지만외부엔터티의경우인증서를수동으로지정해야합니다.

> 중요**:**
>
> Microsoft 인증서서비스엔터티템플릿을생성할때등록된장치와관련된인증문제를방지하려면특수문자를템플릿이름에사용하지마십시오. 예를들어다음을사용하지마십시오. `! : $ ( )## % + * ~ ? | { } [ ]`

Microsoft 인증서서비스

XenMobile 은웹등록인터페이스를통해 Microsoft 인증서서비스와상호작용합니다. XenMobile 은그인터페이스를통해새인증서발급만지원합니다. Microsoft CA 에서 Citrix Gateway 사용자인증서를생성하면 Citrix 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 인증서에명시된인증서형식을제외하고배포하는인증서에대한요구사항이없습니다.
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. 이페이지에서는시스템이이엔터티를통해얻는인증서의서명자를 XenMobile 에알려야합니다. CA 인증서가갱신되면 XenMobile 에서인증서를업데이트합니다. XenMobile 이변경내용을투명하게엔터티에적용합니다.
10. **Microsoft** 인증서서비스엔터티**: CA** 인증서페이지에서엔터티에사용할인증서를선택합니다.
11. 저장을클릭합니다.

    PKI 엔터티테이블에해당엔터티가나타납니다.

Citrix ADC CRL(인증서해지목록)

XenMobile 은타사인증기관에대해서만 CRL(인증서해지목록) 을지원합니다. Microsoft CA 가구성된경우 XenMobile 은 Citrix ADC 를사용하여인증서해지를관리합니다.

클라이언트인증서기반인증을구성하는경우 Citrix ADC CRL(인증서해지목록) 설정인 **Enable CRL Auto Refresh(CRL** 자동새로고침사용**)** 를구성할지여부를고려합니다. 이단계는 MAM 전용모드의장치사용자가장치의기존인증서를사용하여인증할수없도록합니다.

XenMobile 에서는인증서가해지된경우사용자가사용자인증서를생성할수있으므로새인증서가다시발급됩니다. 이설정을사용하면 CRL 이만료된 PKI 엔터티를확인하는경우 PKI 엔터티의보안이강화됩니다.

임의의 **CA**

임의의 CA 는 CA 인증서와연결된개인키를 XenMobile 에제공하는경우만들어집니다. XenMobile 은지정된매개변수에따라인증서발급, 해지및상태정보를내부적으로처리합니다.

임의의 CA 를구성하는경우해당 CA 에대한 OCSP(온라인인증서상태프로토콜) 지원을활성화할수있습니다. OCSP 지원을사용하도록설정한경우에한해 CA 는 `id-pe-authorityInfoAccess` 확장을 CA 가발급한인증서에추가합니다. 이확장은다음위치의 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. 중앙집중식옵션을사용하는것이좋습니다. 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** 지원사용을 켜짐으로설정합니다. 이확장은 CA OCSP Responder(https://<server>/<instance>/ocsp) 를가리킵니다.
   - OCSP 지원을사용하도록설정한경우 OSCP 서명 CA 인증서를선택합니다. XenMobile 에업로드한 CA 인증서에서인증서목록이생성됩니다.

10. 저장을클릭합니다.

    PKI 엔터티테이블에임의의 CA 가나타납니다.

자격증명공급자

August 12, 2022

자격증명공급자는 XenMobile 시스템의다양한부분에서사용하는실제인증서구성입니다. 자격증명공급자는인증서의원본, 매개변수및수명주기를정의합니다. 이러한작업은인증서가장치구성의일부인지독립실행형 (즉, 있는그대로장치에푸시됨) 인지에따라발생합니다.

장치등록은인증서수명주기를제한합니다. 즉, XenMobile 은등록과정에서일부인증서를발급할수있지만등록전에는인증서를발급하지않습니다. 또한등록이해지되면하나의등록컨텍스트내에서내부 PKI 에의해발급된인증서가해지됩니다. 관리관계가종료된

후에는유효한인증서가남아있지않습니다.

단일구성이동시에여러개의인증서를관리할수있도록여러곳에서단일자격증명공급자구성을사용할수있습니다. 통일성은배포리소스및배포에기반합니다. 예를들어자격증명공급자 P 가구성 C 의일부로장치 D 에배포된경우 P 에대한발급설정은 D 에배포된인증서를결정합니다. 마찬가지로 D 에대한갱신설정은 C 가업데이트될때적용됩니다. D 에대한해지설정도 C 가삭제되거나 D 가해지될때적용됩니다.

이규칙에따라 XenMobile 의자격증명공급자구성은다음을결정합니다.

- 인증서의원본.
- 인증서를얻는방법: 새인증서에서명하거나기존인증서및키쌍을가져옵니다 (복구).
- 발급또는복구를위한매개변수. 예: 키크기, 키알고리즘및인증서확장같은 CSR(인증서서명요청) 매개변수.
- 인증서가장치로전달되는방식.
- 해지조건. XenMobile 에서관리관계가끊어지면모든인증서가해지되지만구성에서만료이전에해지되도록지정할수있습니다. 예를들어연결된장치구성이삭제된경우인증서가해지되도록구성할수있습니다. 또한특정조건에서는 XenMobile 에서관련인증서의해지가백엔드 PKI(공개키인프라) 로전송될수있습니다. 즉, XenMobile 에서인증서가해지되면 PKI 에서인증서가해지될수있습니다.
- 갱신설정. 지정된자격증명공급자를통해받은인증서는만료날짜가가까워질때자동으로갱신될수있습니다. 또는이러한상황과별개로만료날짜가다가올때알림을실행할수있습니다.

사용가능한구성옵션은주로자격증명공급자에대해선택한 PKI 엔터티및발급방법의유형에따라다릅니다.

인증서발급방법

서명을통해발급방법이라고하는인증서를얻을수있습니다.

이방법을사용할경우발급에새개인키를만들고, CSR 을만들고, 서명을위해 CSR 을 CA(인증기관) 에제출하는과정이포함됩니다. XenMobile 은 MS 인증서서비스엔터티와임의의 CA 엔터티모두에대한서명방법을지원합니다.

자격증명공급자는서명발급방법을사용합니다.

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 은클라이언트에게인증기관의역할을수행할권한이있음을입증해야합니다. 이권한은앞서언급한인증서를 XenMobile 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. 중앙집중식모드를선호하거나, 분산모드를선호하거나또는분산모드를요구하도록각자격증명공급자를구성할수있습니다. 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 태블릿등록	아니요	아니요
Windows 태블릿구성	아니요 (Windows 10 및 Windows 11 릴리스에서지원되는 WiFi 장치정책제외)	아니요

인증서해지

해지에는세가지유형이있습니다.

- 내부적해지**:** 내부적해지는 XenMobile 에서유지관리하는인증서상태에영향을줍니다. XenMobile 은제시된인증서를평가하거나인증서에대한 OCSP 상태정보를제공할때이상태를고려합니다. 자격증명공급자구성에따라다양한조건에서이러한상태가영향을받는방식이결정됩니다. 예를들어자격증명공급자는인증서가장치에서삭제된경우인증서에해지플래그를지정하도록지정할수있습니다.
- 외부에서전파된해지**:** 해지 XenMobile 이라고알려진이해지유형은외부 PKI 에서취득한인증서에적용됩니다. 자격증명공급자구성에정의된조건에따라 XenMobile 에서내부적으로인증서가해지되는경우 PKI 에서인증서가해지됩니다.
- 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. 장치가연결되면서버는인증서 `NotAfter` 날짜가현재날짜에서지정된기간을뺀날짜보다이후인지여부를확인합니다. 인증서가조건을충족하면 XenMobile 이인증서갱신을시도합니다.

자격증명공급자생성

자격증명공급자구성은주로자격증명공급자에대해선택한발급엔터티및발급방법의요인에따라달라집니다. 내부엔터티또는외부엔터티를사용하는자격증명공급자를구분할수있습니다.

- XenMobile 에대해내부인임의의엔터티는내부엔터티입니다. 임의의엔터티에대한발급방법은항상서명입니다. 서명은발급작업을수행할때마다 XenMobile 이엔터티에대해선택된 CA 인증서로새키쌍을서명한다는것을의미합니다. 키쌍이장치에서생성되는지, 아니면서버에서생성되는지는선택한배포방법에따라다릅니다.
- 회사인프라의일부인외부엔터티에는 Microsoft CA 가포함됩니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭하고 설정 **>** 자격증명공급자를클릭합니다.
2. 자격증명공급자페이지에서 추가를클릭합니다.

   자격증명공급자**:** 일반정보페이지가나타납니다.
3. 자격증명공급자**:** 일반정보페이지에서다음을수행합니다.
   - 이름**:** 새공급자구성의고유한이름을입력합니다. 이이름은나중에 XenMobile 콘솔의다른부분에서구성을식별할때사용됩니다.
   - 설명**:** 자격증명공급자를설명합니다. 이필드는선택사항이지만설명을사용하면이자격증명공급자에대한유용한세부정보를제공할수있습니다.
   - 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. 기본하드웨어및소프트웨어에따라달라질수있는거짓음성반응을방지하기위해 XenMobile 은키크기를강제하지않습니다. 자격증명공급자구성을프로덕션환경에서활성화하기전에항상테스트환경에서테스트해야합니다.

- 서명알고리즘**:** 새인증서에대한값을클릭합니다. 값은키알고리즘에따라달라집니다.

- 주체이름**:** 필수항목입니다. 새인증서주체의 DN(고유이름) 을입력합니다. 예: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

  예를들어클라이언트인증서인증의경우다음설정을사용합니다.

  - 키알고리즘**:** RSA
  - 키크기**:** 2048
  - 서명알고리즘**:** SHA256withRSA
  - 주체이름 `cn=$user.username`

- 주체대체이름테이블에항목을추가하려면 추가를클릭합니다. 대체이름의유형을선택하고두번째열에값을입력합니다.

  클라이언트인증서인증의경우다음을지정합니다.

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

    주체이름과마찬가지로값필드에 XenMobile 매크로를사용할수있습니다.

6. 다음을클릭합니다.

   자격증명공급자**:** 배포페이지가나타납니다.

7. 자격증명공급자**:** 배포페이지에서다음을수행합니다.

   - **CA** 인증서발급목록에서제공된 CA 인증서를클릭합니다. 자격증명공급자가임의의 CA 엔터티를사용하기때문에자격증명공급자에대한 CA 인증서는항상엔터티자체에서구성된 CA 인증서입니다. 여기에나온 CA 인증서는외부엔터티를사용하는구성과의일관성을위한것입니다.
   - 배포모드선택에서다음과같은키생성및배포방법중하나를클릭합니다.
     - 중앙집중식선호**:** 서버측키생성**:** 이중앙집중식옵션을사용하는것이좋습니다. 이옵션은 XenMobile 에서지원하는모든플랫폼을지원하며 Citrix Gateway 인증을사용할때필요합니다. 개인키가생성되어서버에저장되고사용자장치에배포됩니다.
     - 분산식선호**:** 장치측키생성**:** 개인키가생성되고사용자장치에저장됩니다. 이분산모드에서는 SCEP 를사용하며 keyUsage keyEncryption 이포함된 RA 암호화인증서와 KeyUsage digitalSignature 가포함된 RA 서명인증서가필요합니다. 암호화와서명에모두동일한인증서를사용할수있습니다.
     - 분산전용**:** 장치측키생성**:** 이옵션은 “선호” 가아닌 “전용” 이기때문에장치측키생성이실패하거나사용할수없는경우사용할수있는옵션이없다는것을제외하면분산식선호: 장치측키생성과동일하게작동합니다.

분산식선호**:** 장치측키생성또는 분산전용**:** 장치측키생성을선택한경우 RA 서명인증서및 RA 암호화인증서를클릭합니다. 둘모두에동일한인증서를사용할수있습니다. 인증서에대한새필드가나타납니다.

8. 다음을클릭합니다.

   자격증명공급자**:** 해지 **XenMobile** 페이지가나타납니다. 이페이지에서 XenMobile 이이공급자구성을통해발급된인증서를어떤조건일때내부적으로해지된것으로플래그지정해야하는지를구성합니다.

9. 자격증명공급자**:** 해지 **XenMobile** 페이지에서다음을수행합니다.

   - 발급된인증서해지에서인증서를해지할시기를나타내는옵션중하나를선택합니다.
   - 인증서가해지될때 XenMobile 의알림을받으려면 알림보내기의값을 켜짐으로설정하고알림템플릿을선택합니다.
   - XenMobile 에서인증서가해지될때 PKI 에서인증서를해지하려면 **PKI** 에대한인증서해지를 켜짐으로설정하고 엔터티목록에서템플릿을클릭합니다. 엔터티목록에해지기능이있는모든사용가능한엔터티가표시됩니다. XenMobile 에서인증서가해지되면해지요청이엔터티목록에서선택된 PKI 로전송됩니다.

10. 다음을클릭합니다.

    자격증명공급자**:** 해지 **PKI** 페이지가나타납니다. 이페이지에서인증서가해지된경우 PKI 에서수행할동작을식별합니다. 알림메시지를생성하는옵션도사용할수있습니다.

11. PKI 에서인증서를해지하려면 자격증명공급자**:** 해지 **PKI** 페이지에서다음을수행합니다.

    - 외부해지확인사용설정을 켜짐으로변경합니다. 해지 PKI 와관련된추가필드가나타납니다.
    - **OCSP** 응답자 **CA** 인증서목록에서인증서주체의 DN(고유이름) 을클릭합니다.

      DN 필드값에 XenMobile 매크로를사용할수있습니다. 예: `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

May 11, 2022

> 중요**:**
>
> APN 레거시바이너리프로토콜에대한 Apple 의지원은 2021 년 3 월 31 일부터종료됩니다. Apple 에서는 HTTP/2 기반 APN 제공업체 API 를대신사용하도록권장합니다. 릴리스 10.13.0 부터 XenMobile Server 에서는 HTTP/2 기반 API 를지원합니다. 자세한정보는 https://developer.apple.com/에서뉴스업데이트 “Apple 푸시알림서비스업데이트” 를참고하십시오. APN 연결확인과관련된지원은 연결확인을참조하십시오.

XenMobile 에서 iOS 및 macOS 장치를등록하고관리하려면 Apple 의 APNs(Apple 푸시알림서비스) 인증서를설정합니다.

워크플로요약:

- **1** 단계**:** 다음방법중하나를통해CSR(인증서서명요청) 만들기
  - macOS 에서키체인접근을사용하여 CSR 만들기(Citrix 에서권장)

  - Microsoft IIS 를사용하여 CSR 만들기
  - OpenSSL 을사용하여 CSR 만들기
- **2** 단계**:** XenMobile Tools 에서CSR 에서명
- **3** 단계**:** 서명된 CSR 을 Apple 에제출하고 APNs 인증서얻기
- **4** 단계**:** 1 단계에서사용한것과동일한컴퓨터를사용하여CSR 을완료하고 PKCS #12 파일내보내기
  - macOS 에서키체인접근을사용하여 PKCS #12 파일만들기
  - Microsoft IIS 를사용하여 PKCS #12 파일만들기
  - OpenSSL 을사용하여 PKCS #12 파일만들기
- **5** 단계**:** XenMobile 로 APNs 인증서가져오기
- **6** 단계**:** APN 인증서갱신

CSR 만들기

macOS 에서는키체인접근을사용하여 CSR 을만드는것이좋습니다. Microsoft IIS 또는 OpenSSL 을사용하여 CSR 을만들수도있습니다.

> 중요**:**
>
> - 인증서를만드는데사용된 Apple ID 의경우:
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.
>   - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device reenrollment.
> - 실수로또는의도적으로인증서를해지하면장치를관리할수없게됩니다.
> - iOS 개발자기업프로그램을사용하여 Mobile Device Manager 푸시인증서를만든경우 Apple Push Certificates Portal 에서마이그레이션인증서에대한작업을처리해야합니다.

macOS 에서키체인접근을사용하여 **CSR** 만들기

1. macOS 를실행하는컴퓨터의 응용프로그램 **>** 유틸리티에서키체인접근앱을시작합니다.
2. 키체인접근메뉴를열고 인증지원 **>** 인증기관에서인증서요청을클릭합니다.
3. 다음과같은정보를입력하라는메시지가나타납니다.
   - 전자메일주소**:** 인증서관리를담당하는개인또는역할계정의전자메일주소입니다.
   - 일반이름**:** 인증서관리를담당하는개인또는역할계정의일반이름입니다.
   - **CA** 전자메일주소**:** 인증기관의전자메일주소입니다.
4. 디스크에저장됨및 본인이키쌍정보지정옵션을선택하고 계속을클릭합니다.
5. CSR 파일의이름을입력하고컴퓨터에파일을저장한다음 저장을클릭합니다.

6. 키쌍정보를지정합니다. 2048 비트의 키크기와 **RSA** 알고리즘을선택한다음 계속을클릭합니다. APNs 인증서프로세스의일부로 CSR 파일을업로드할준비가되었습니다.
7. 인증지원의 CSR 프로세스가완료되면 완료를클릭합니다.
8. 계속하려면CSR 에서명합니다.

Microsoft IIS 를사용하여 **CSR** 만들기

APNs 인증서요청을생성하기위한첫번째단계는 CSR(증서서명요청) 을만드는것입니다. Windows 의경우 Microsoft IIS 를사용하여 CSR 을만듭니다.

1. Microsoft IIS 를엽니다.
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.
7. 계속하려면CSR 에서명합니다.

OpenSSL 을사용하여 **CSR** 만들기

macOS 장치또는 Microsoft IIS 를사용하여 CSR 을생성할수없는경우 OpenSSL 을사용합니다. OpenSSL 웹사이트에서 OpenSSL 을다운로드하여설치할수있습니다.

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
```



```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    Customer
Organizational Unit Name (eg, section) [:Marketing
Common Name (eg, YOUR name) []:John Doe
Email Address []:john.doe@customer.com
<!--NeedCopy-->
```

3. 다음메시지가나타나면 CSR 개인키의암호를입력합니다.

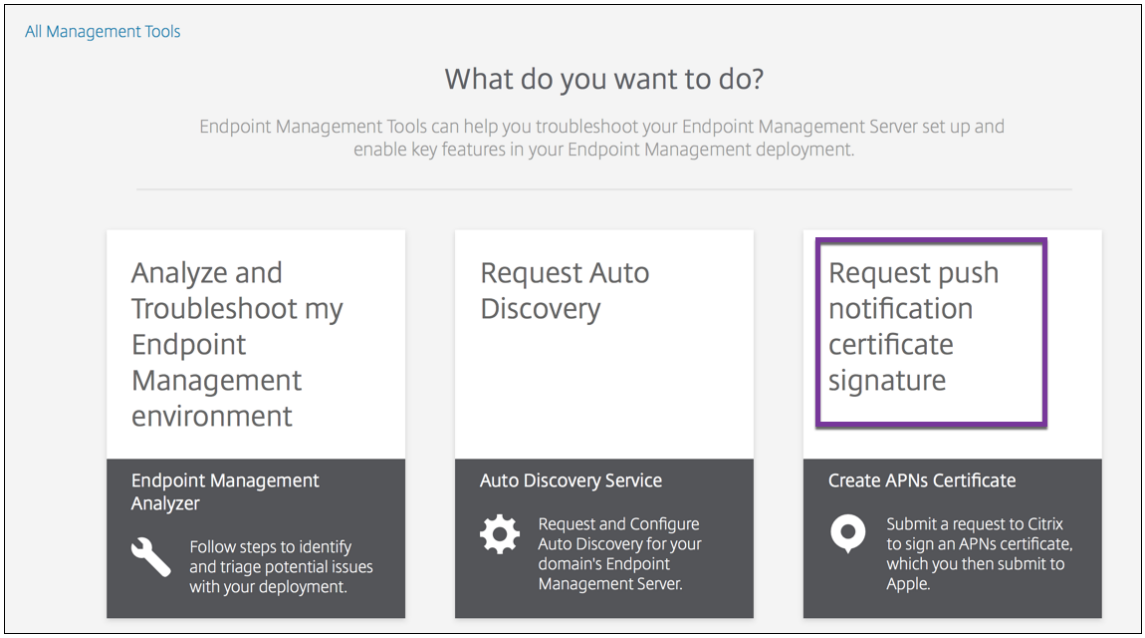
```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
<!--NeedCopy-->
```

4. 계속하려면다음섹션에설명된대로 CSR 에서명합니다.

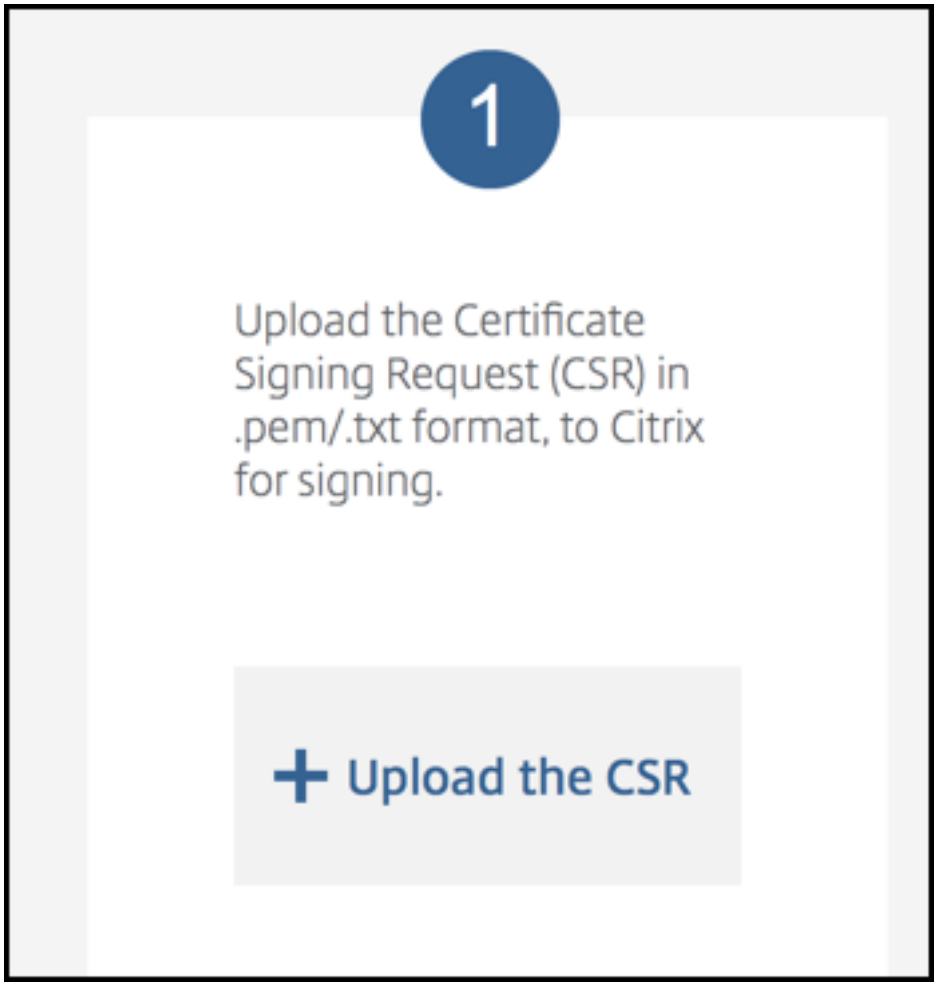
CSR 서명

XenMobile 에서인증서를사용하려면서명을위해 Citrix 에인증서를제출합니다. Citrix 는모바일기기관리서명인증서로 CSR 에서명하고서명된파일을 `.plist` 형식으로반환합니다.

1. 브라우저에서 Endpoint Management Tools 웹사이트로이동한다음 **Request push notification certificate signature(**푸시알림인증서서명요청**)** 을클릭합니다.



2. 새인증서만들기페이지에서 **CSR** 업로드를클릭합니다.



3. 인증서를찾아선택합니다.

   인증서는.pem/txt 형식이어야합니다.

4. **Endpoint Management APNs CSR** 서명페이지에서 서명을클릭합니다. CSR 이서명되고구성된다운로드폴더에 자동으로저장됩니다.

5. 계속하려면다음섹션에설명된대로서명된 CSR 을제출합니다.

Apple 에서명된 **CSR** 을제출하여 **APNs** 인증서받기

Citrix 에서서명된 CSR(증서서명요청) 을받았으면 Apple 에 CSR 을제출하여 XenMobile 로가져오는데필요한 APNs 인증서를받습니다.

> 참고**:**
>
> 일부사용자가 Apple Push Portal 로그인과관련된문제를보고했습니다. 또는 Apple 개발자포털에로그인한후다음단계를따르십시오.

1. 브라우저에서 Apple Push Certificates Portal로이동합니다.

2. **Create a Certificate(**인증서생성**)** 를클릭합니다.
3. Apple 에서인증서를만드는것이처음이라면 **I have read and agree to these terms and conditions(**이용약관을읽었고이에동의합니다**.)** 확인란을선택하고 **Accept(**동의**)** 를클릭합니다.
4. **Choose File(**파일선택**)** 을클릭하고컴퓨터에서서명된 CSR 을찾아선택한다음 **Upload(**업로드**)** 를클릭합니다. 업로드가성공했다는확인메시지가나타납니다.
5. **Download(**다운로드**)** 를클릭하여.pem 인증서를검색합니다.
6. 계속하려면 CSR 을완료하고다음섹션에설명된대로 PKCS #12 파일을내보냅니다.

CSR 을완료하고 **PKCS #12** 파일내보내기

Apple 에서 APNs 인증서를받은후키체인접근, Microsoft IIS 또는 OpenSSL 로돌아가서인증서를 PCKS #12 파일로내보냅니다.

PKCS #12 파일에는 APNS 인증서파일과개인키가들어있습니다. PFX 파일의확장자는일반적으로.pfx 또는.p12 입니다. .pfx 및.p12 파일을서로바꿔서사용할수있습니다.

> 중요**:**
>
> 로컬시스템에서개인및공개키를저장하거나내보내는것이좋습니다. 재사용을위해 APNs 인증서에액세스하려면키가필요합니다. 동일한키가없으면인증서가유효하지않으므로전체 CSR 및 APNs 프로세스를반복해야합니다.

macOS 에서키체인접근을사용하여 **PKCS #12** 파일만들기

> 중요**:**
>
> 이작업에는 CSR 을생성할때사용한것과동일한 macOS 장치를사용합니다.

1. 장치에서 Apple 에서받은프로덕션 ID(.pem) 인증서를찾습니다.
2. 키체인접근응용프로그램을시작하고 **Login(**로그인**) > My Certificates(**내인증서**)** 탭으로이동합니다. 제품 ID 인증서를열려있는창으로끌어다놓습니다.
3. 인증서를클릭하고왼쪽화살표를확장하여인증서에연결된개인키가포함되어있는지확인합니다.
4. 인증서를 PCKS #12(.pfx) 인증서로내보내려면인증서와개인키를선택하고마우스오른쪽단추로클릭한다음 **Export 2 items(2** 개항목내보내기**)** 를선택합니다.
5. 인증서파일에 XenMobile 에서사용할고유이름을지정합니다. 이름에공백문자를사용하지마십시오. 저장된인증서의폴더위치를선택하고.pfx 파일형식을선택한후 저장을클릭합니다.
6. 인증서를내보낼암호를입력합니다. 고유하고강력한암호를사용하는것이좋습니다. 또한나중에사용하고참조할수있도록인증서와암호를안전하게보관하십시오.
7. 키체인접근앱에로그인암호또는선택한키체인을묻는메시지가나타납니다. 암호를입력한다음 **OK(**확인**)** 를클릭합니다. 이제저장된인증서를 XenMobile 서버에서사용할수있습니다.
8. 계속하려면XenMobile 로 APN 인증서가져오기를참조하십시오.

Microsoft IIS 를사용하여 **PKCS #12** 파일만들기

> 중요**:**
>
> 이작업에는 CSR 을생성하는데사용한 IIS 서버와동일한서버를사용합니다.

1. Microsoft IIS 를엽니다.
2. 서버인증서아이콘을클릭합니다.
3. 서버인증서창에서 인증서요청완료를클릭합니다.
4. Apple 의 Certificate.pem 파일을찾아선택합니다. 그런다음친숙한이름이나인증서이름을입력하고 확인을클릭합니다. 이름에공백문자를사용하지마십시오.
5. 4 단계에서식별한인증서를선택하고 내보내기를클릭합니다.
6. .pfx 인증서의위치및파일이름과암호를지정한다음 확인을클릭합니다.

   인증서를 XenMobile 로가져오려면해당인증서의암호가필요합니다.
7. XenMobile 을설치할서버에.pfx 인증서를복사합니다.
8. 계속하려면XenMobile 로 APN 인증서가져오기를참조하십시오.

OpenSSL 을사용하여 **PKCS #12** 파일만들기

OpenSSL 을사용하여 CSR 을만드는경우 OpenSSL 을사용하여.pfx APNs 인증서도만들수있습니다.

1. 명령프롬프트또는셸에서다음명령을실행합니다. `Customer.privatekey.pem`은 CSR 의개인키이고 `APNs_Certificate.pem`은방금 Apple 에서받은인증서입니다.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey
   .pem -out apns_identity.pfx
   ```
2. .pfx 인증서파일의암호를입력합니다. XenMobile 에인증서를업로드할때암호를다시사용하므로이암호를기억하고있어야합니다.
3. .pfx 인증서파일의위치를기록합니다. 콘솔을사용하여파일을업로드할수있도록파일을 XenMobile 서버에복사합니다.
4. 계속하려면다음섹션에설명된대로 APNs 인증서를 XenMobile 로가져옵니다.

XenMobile 로 **APNs** 인증서가져오기

새 APNs 인증서를받은후 APNs 인증서를 XenMobile 로가져와인증서를처음으로추가하거나인증서를바꿉니다.

1. XenMobile 콘솔에서 설정 **>** 인증서로이동합니다.
2. 가져오기 **>** 키저장소를클릭합니다.
3. 용도에서 **APNs** 를선택합니다.
4. 컴퓨터에서.pfx 또는.p12 파일을찾습니다.

5. 암호를입력하고 가져오기를클릭합니다.

XenMobile 의인증서에대한자세한내용은 인증서및인증을참조하십시오.

APNs 인증서갱신

> 중요:
>
> 갱신프로세스에다른 Apple ID 를사용하는경우사용자장치를다시등록해야합니다.

APNs 인증서를갱신하려면인증서를만드는단계를수행한다음 Apple Push Certificates Portal로이동합니다. 포털을사용하여새인증서를업로드합니다. 로그온하면기존인증서또는이전 Apple Developers 계정에서가져온인증서가표시됩니다.

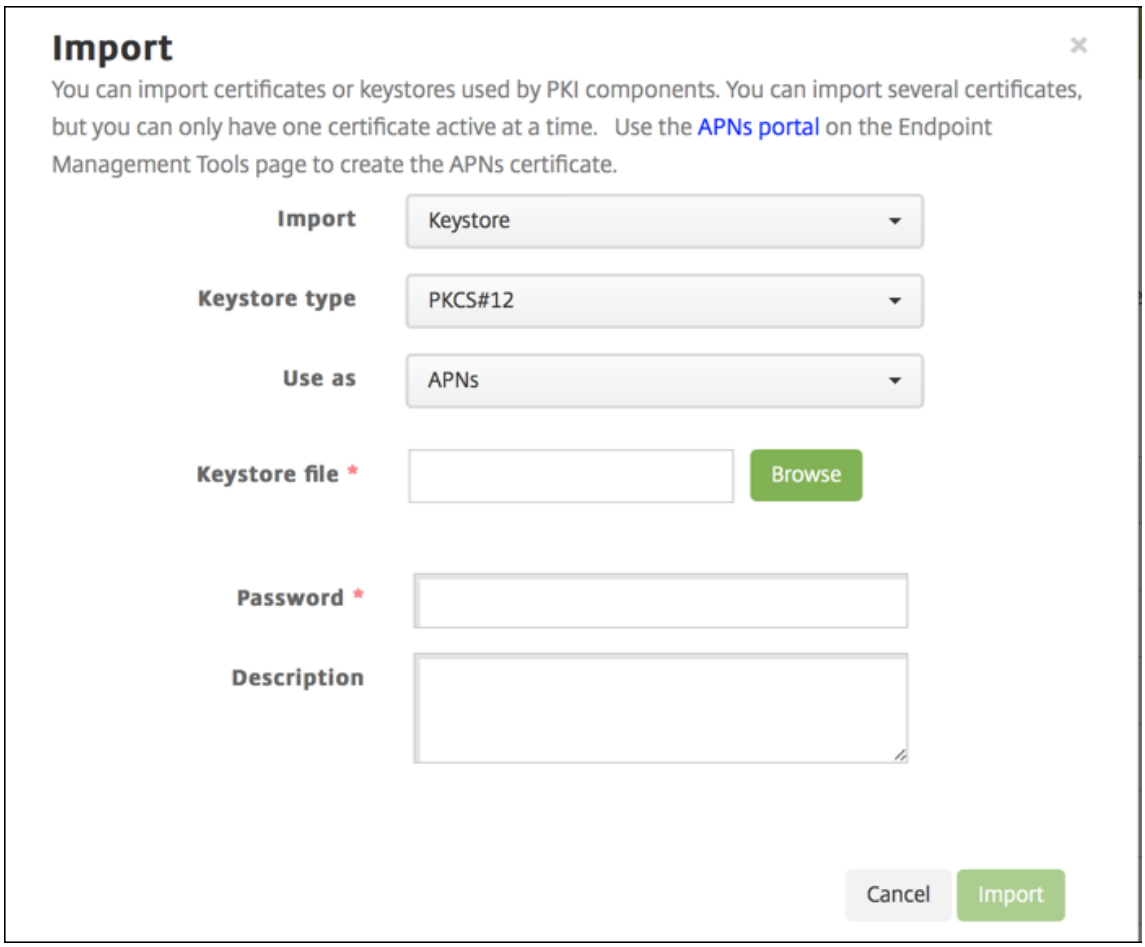
Certificates Portal 에서인증서를갱신할때유일한차이점은 **Renew(**갱신**)** 를클릭한다는것입니다. 사이트에액세스하려면 Certificates Portal 에개발자계정이있어야합니다. 인증서를갱신하려면동일한조직이름과 Apple ID 를사용합니다.

APNs 인증서만료시기를확인하려면 XenMobile 콘솔에서 설정 **>** 인증서로이동합니다. 인증서가만료된경우해지하지마십시오.

1. Microsoft IIS, 키체인접근 (macOS) 또는 OpenSSL 을사용하여 CSR 을생성합니다. CSR 생성에대한자세한내용은인증서서명요청만들기를참조하십시오.
2. 브라우저에서 Endpoint Management 도구로이동합니다. 그런다음 **Request push notification certificate signature(**푸시알림인증서서명요청**)** 를클릭합니다.
3. **+ Upload the CSR(+ CSR** 업로드**)** 을클릭합니다.
4. 대화상자에서 CSR 로이동한후 **Open(**열기**)** 을클릭하고 **Sign(**서명**)** 을클릭합니다.
5. `.plist` 파일이표시되면저장합니다.
6. 3 단계제목에서 **Apple Push Certificates Portal** 을클릭하고로그온합니다.
7. 갱신할인증서를선택하고 **Renew(**갱신**)** 를클릭합니다.
8. `.plist` 파일을업로드합니다. .pem 파일이출력으로표시됩니다. .pem 파일을저장합니다.
9. 이.pem 파일을사용하여 CSR 을완료합니다 (1 단계에서 CSR 을생성할때사용한방법에따라).
10. 인증서를.pfx 파일로내보냅니다.

XenMobile 콘솔에서.pfx 파일을가져오고다음과같이구성을완료합니다.

1. 설정 **>** 인증서 **>** 가져오기로이동합니다.
2. 가져오기메뉴에서 키저장소를선택합니다.
3. 키저장소유형메뉴에서 **PKCS#12** 를선택합니다.
4. 용도에서 **APNs** 를선택합니다.



5. 키저장소파일에대해 찾아보기를클릭하고해당파일로이동합니다.
6. 암호에인증서암호를입력합니다.
7. 필요한경우 설명을입력합니다.
8. 가져오기를클릭합니다.

XenMobile 의 인증서페이지로리디렉션됩니다. 이름, 상태, 유효기간시작일및 유효기간종료일필드가업데이트됩니다.

Citrix Files 의 SSO(Single Sign-on) 용 SAML

January 5, 2022

SAML(Security Assertion Markup Language) 을사용하여 Citrix Files 모바일앱에대한 SSO(Single Sign-On) 액세스를제공하도록 XenMobile 및 Citrix Content Collaboration 을구성할수있습니다. 이기능에는다음이포함됩니다.

- MDX Toolkit 을통해 MAM SDK 를사용하거나래핑된 Citrix Files 앱
- 웹사이트, Outlook 플러그인또는동기화클라이언트와같이래핑되지않은 Citrix Files 클라이언트

- 래핑된 **Citrix Files** 앱의경우. Citrix Files 모바일앱을통해 Citrix Files 에로그온하는사용자는사용자인증과 SAML 토큰획득을위해 Secure Hub 로리디렉션됩니다. 인증이성공하면 Citrix Files 모바일앱이 SAML 토큰을 Content Collaboration 으로전송합니다. 초기로그온후사용자는 SSO 를통해 Citrix Files 모바일앱에액세스할수있습니다. 또한매번로그온하지않고도 Content Collaboration 의문서를 Secure Mail 메일에첨부할수있습니다.
- 래핑되지않은 **Citrix Files** 클라이언트의경우. 웹브라우저또는다른 Citrix Files 클라이언트를사용하여 Citrix Files 에로그온하는사용자가 XenMobile 로리디렉션됩니다. XenMobile 이사용자를인증하면인증된사용자가받은 SAML 토큰이 Content Collaboration 으로전송됩니다. 초기로그온후사용자는매번로그온하지않고 SSO 를통해 Citrix Files 클라이언트에액세스할수있습니다.

XenMobile 을 Content Collaboration 에대한 SAML IdP(ID 공급자) 로사용하려면이문서에설명된대로 Enterprise 계정을사용하도록 XenMobile 을구성해야합니다. 또한 StorageZone 커넥터에서만작동하도록 XenMobile 을구성할수있습니다. 자세한내용은 XenMobile 에서 Citrix Content Collaboration 사용을참조하십시오.

자세한참조아키텍처다이어그램은 아키텍처를참조하십시오.

사전요구사항

XenMobile 및 Citrix Files 앱에서 SSO 를구성하려면먼저다음과같은사전요구사항을충족해야합니다.

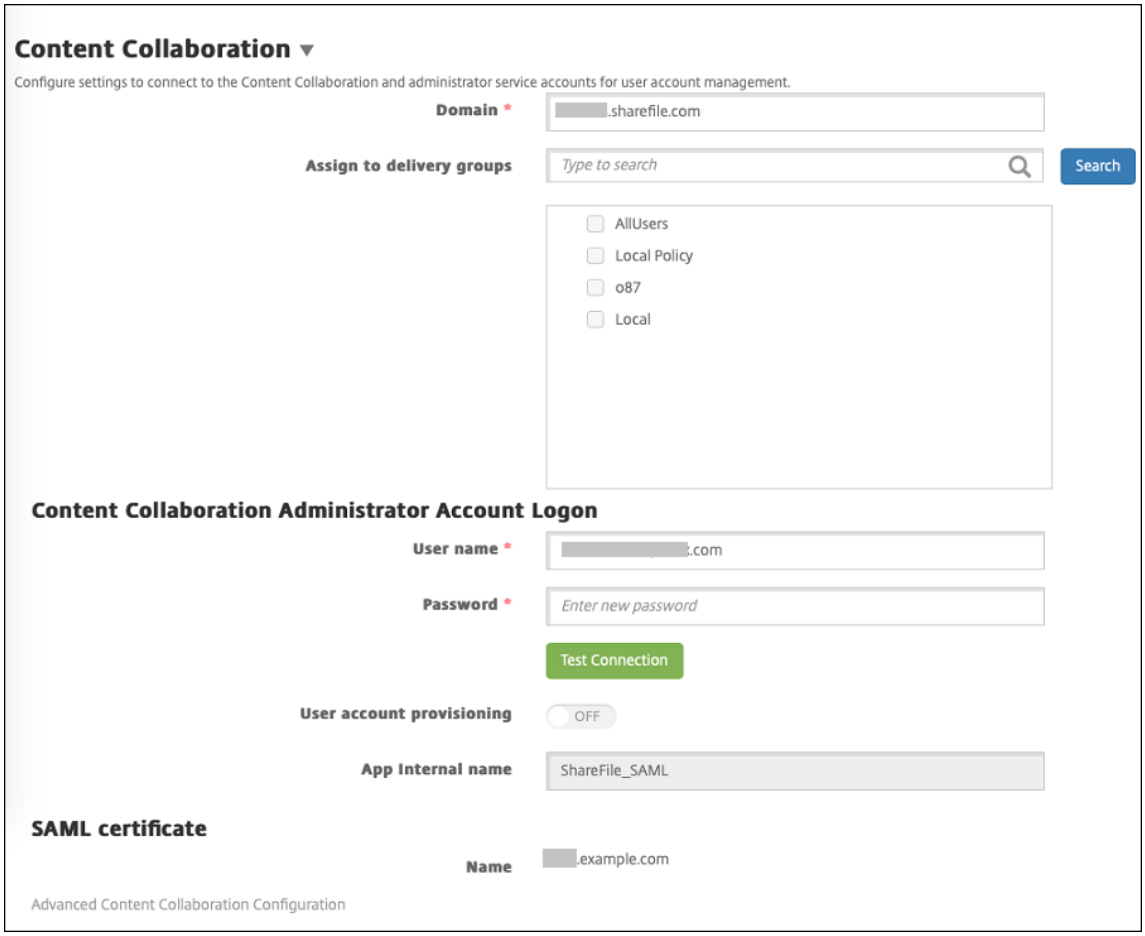
- MAM SDK 또는호환되는버전의 MDX Toolkit(Citrix Files 모바일앱용)

  자세한내용은 XenMobile 호환성을참조하십시오.
- 호환되는버전의 Citrix Files 모바일앱및 Secure Hub
- Content Collaboration 관리자계정
- XenMobile 과 Content Collaboration 간의연결이확인됨

Content Collaboration 액세스구성

Content Collaboration 에대한 SAML 을설정하기전에다음과같이 Content Collaboration 액세스정보를제공합니다.

1. XenMobile 웹콘솔에서 구성 **> ShareFile** 을클릭합니다. **ShareFile** 구성페이지가나타납니다. 콘솔에 ShareFile 대신 Content Collaboration 이라는용어가표시될수있습니다.



2. 다음설정을구성합니다.

   - 도메인**:** Content Collaboration 하위도메인이름을입력합니다. 예: `example.sharefile.com`.
   - 배달그룹에할당**:** Content Collaboration 에서 SSO 를사용할수있게하려는배달그룹을선택하거나검색합니다.
   - **ShareFile** 관리자계정로그온
   - 사용자이름**:** Content Collaboration 관리자사용자이름을입력합니다. 이사용자는관리자권한을가지고있어야합니다.
   - 암호**:** Content Collaboration 관리자암호를입력합니다.
   - 사용자계정프로비저닝**:** 이설정을사용하지않도록설정합니다. 사용자프로비저닝에 Content Collaboration 사용자관리도구를사용합니다. 사용자계정및메일그룹프로비전을참조하십시오.

3. 연결테스트를클릭하여 Content Collaboration 관리자계정이지정된 Content Collaboration 계정으로인증하는사용자이름과암호를확인합니다.

4. 저장을클릭합니다.

   - XenMobile 이 Content Collaboration 과동기화되고 Content Collaboration 설정인 **ShareFile** 발급자/엔터티 **ID** 및 로그인 **URL** 이업데이트됩니다.
   - 구성 **> ShareFile** 페이지에 앱내부이름이표시됩니다. Citrix Files.com SSO 설정수정의뒷부분에설명된단

계를완료하려면이이름이필요합니다.

래핑된 **Citrix Files MDX** 앱을위한 **SAML** 설정

래핑된 Citrix Files MDX 앱의 Single Sign-on 구성에 Citrix Gateway 를사용하지않아도됩니다. 웹사이트, Outlook 플러그인또는동기화클라이언트와같이래핑되지않은 Citrix Files 클라이언트에대한액세스를구성하려면 다른 Citrix Files 클라이언트에대한 Citrix Gateway 구성을참조하십시오.

다음단계는 iOS 및 Android 앱및장치에적용됩니다. 래핑된 Citrix Files MDX 앱에대해 SAML 을구성하려면다음을수행합니다.

1. MDX Toolkit 을사용하여 Citrix Files 모바일앱을래핑합니다. MDX Toolkit 으로앱을래핑하는것에대한자세한내용은 Wrapping Apps with the MDX Toolkit(MDX Toolkit 으로앱래핑)을참조하십시오.
2. XenMobile 콘솔에서래핑된 Citrix Files 모바일앱을업로드합니다. MDX 앱업로드에대한자세한내용은 XenMobile 에 MDX 앱을추가하려면을참조하십시오.
3. SAML 설정을확인합니다. 앞서구성한관리자사용자이름과암호로 Content Collaboration 에로그온합니다.
4. Content Collaboration 및 XenMobile 이동일한표준시간대로구성되어있는지확인합니다. XenMobile 이구성된표준시간대를기준으로정확한시간을표시하는지확인합니다. 그렇지않은경우 SSO 가실패할수있습니다.

Citrix Files 모바일앱의유효성검사

1. 사용자장치에서 Secure Hub 를설치하고구성합니다.
2. XenMobile Store 에서 Citrix Files 모바일앱을다운로드하고설치합니다.
3. Citrix Files 모바일앱을시작합니다. Citrix Files 는사용자이름이나암호를묻지않고시작됩니다.

Secure Mail 로유효성검사

1. 아직완료하지않은경우사용자장치에서 Secure Hub 를설치하고구성합니다.
2. XenMobile Store 에서 Secure Mail 을다운로드하여설치하고설정합니다.
3. 새전자메일양식을열고 **Citrix Files** 에서첨부를누릅니다. 사용자이름이나암호를묻지않고전자메일에첨부할수있는파일이표시됩니다.

다른 **Citrix Files** 클라이언트에대한 **Citrix Gateway** 구성

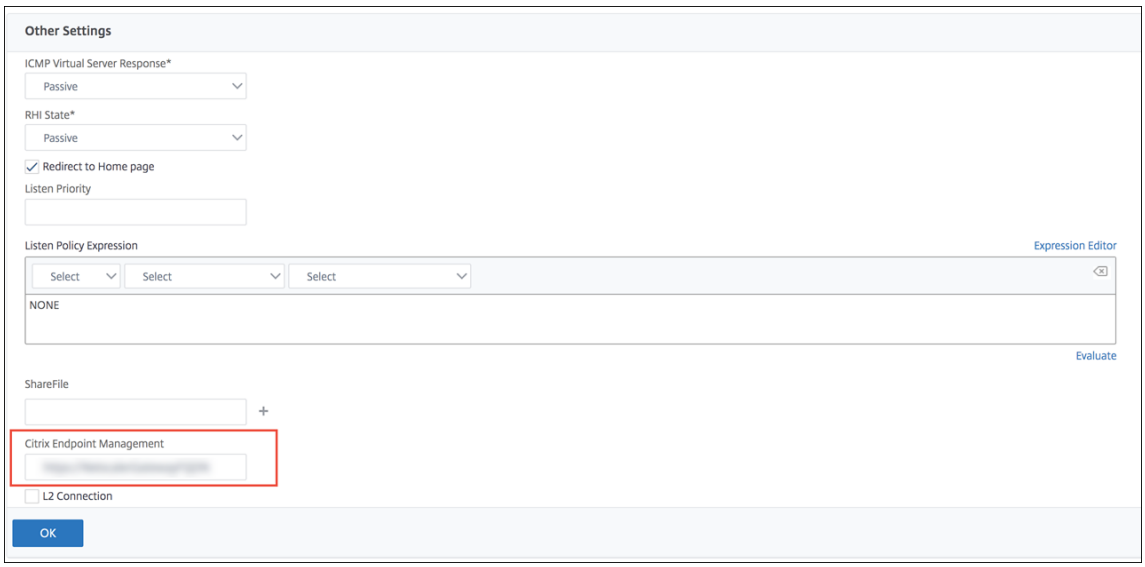
웹사이트, Outlook 플러그인또는동기화클라이언트와같이래핑되지않은 Citrix Files 클라이언트에대한액세스권한을구성하려면다음과같이 XenMobile 을 SAML ID 공급자로사용하는것을지원하도록 Citrix Gateway 를구성합니다.

- 홈페이지리디렉션을사용하지않도록설정합니다.
- Citrix Files 세션정책및프로필을만듭니다.
- Citrix Gateway 가상서버에서정책을구성합니다.

홈페이지리디렉션사용안함

/cginfra 경로를통해수신되는요청의기본동작을사용하지않도록설정합니다. 이렇게하면사용자가구성된홈페이지대신원래요청된내부 URL 을볼수있습니다.

1. XenMobile 로그온에사용되는 Citrix Gateway 가상서버의설정을편집합니다. Citrix ADC 에서 **Other Settings(**기타설정**)** 로이동한다음 **Redirect to Home Page(**홈페이지로리디렉션**)** 확인란을선택취소합니다.



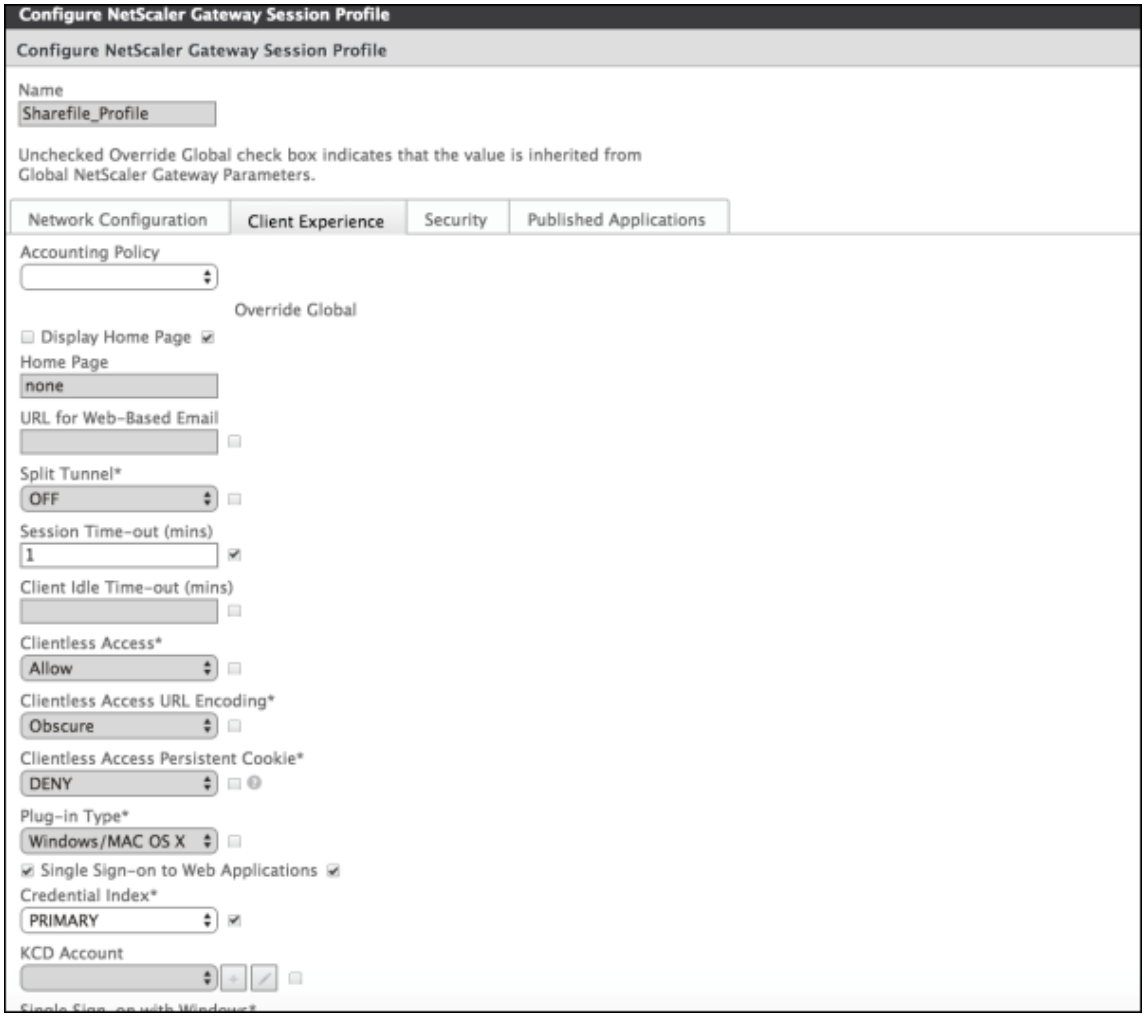
2. **ShareFile**(현재의 Content Collaboration) 에서 XenMobile 내부서버의이름과포트번호를입력합니다.
3. **Citrix Endpoint Management** 아래에 XenMobile URL 을입력합니다. 사용중인 Citrix Gateway 버전에이전제품이름인 **AppController** 가표시될수있습니다.

   이구성은 /cginfra 경로를통해입력된 URL 에대한요청을인증합니다.

Citrix Files 세션정책및요청프로필만들기

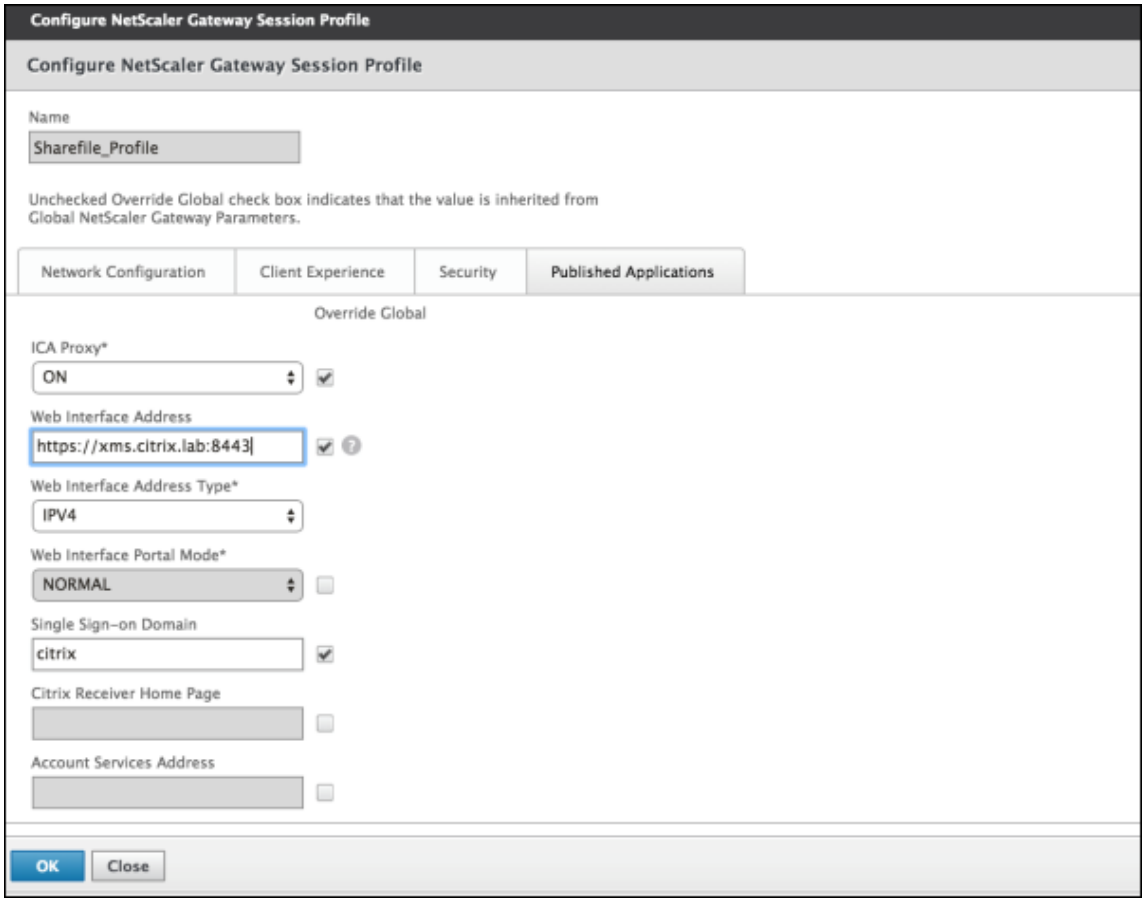
다음과같은설정을구성하여 Citrix Files 세션정책및요청된프로필을만듭니다.

1. Citrix Gateway 구성유틸리티의왼쪽탐색창에서 **Citrix Gateway >** 정책 **>** 세션을클릭합니다.
2. 세션정책을만듭니다. 정책탭에서 추가를클릭합니다.
3. 이름필드에 **ShareFile_Policy** 를입력합니다.
4. **+** 단추를클릭하여동작을만듭니다. 세션프로필만들기페이지가나타납니다.



다음설정을구성합니다.

- **Name(**이름**): ShareFile_Profile** 을입력합니다.
- **Client Experience(**클라이언트환경**)** 탭을클릭하고다음과같은설정을구성합니다.
  - **Home Page(**홈페이지**): none** 을입력합니다.
  - **Session Time-out (mins)(**세션시간제한 **(**분**)**: **1** 을입력합니다.
  - **Single Sign-on to Web Applications(**웹응용프로그램에대한 **SSO):** 이설정을선택합니다.
  - **Credential Index(**자격증명색인**):** 목록에서 **PRIMARY** 를클릭합니다.
- **Published Applications(**게시된응용프로그램**)** 탭을클릭합니다.

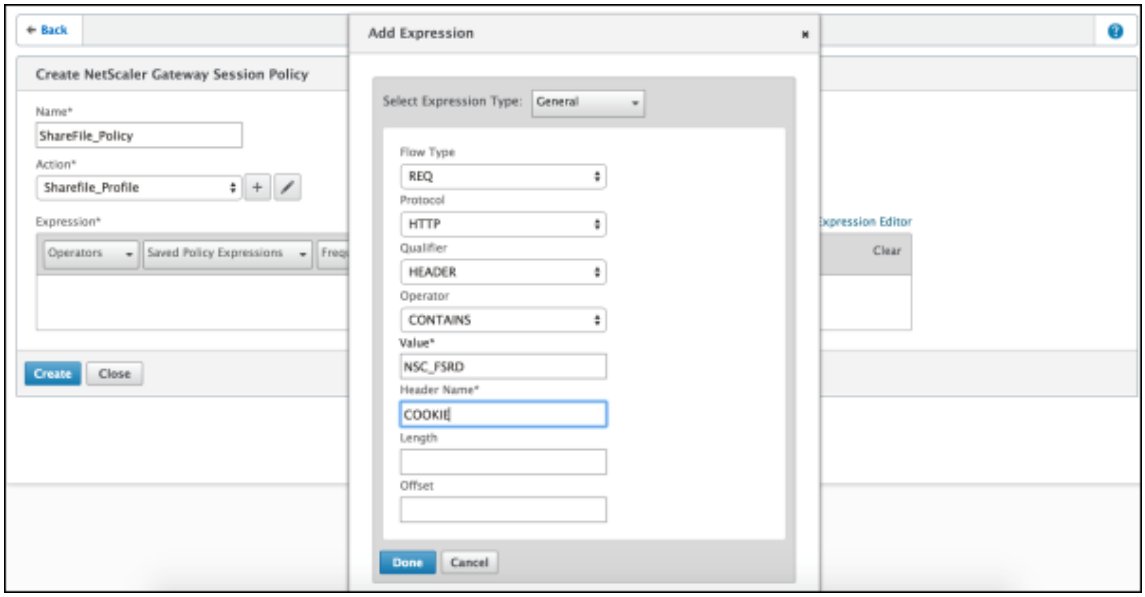


다음설정을구성합니다.

- **ICA Proxy(ICA** 프록시**): ON(**켜짐**)** 을클릭합니다.
- **Web Interface Address(**웹인터페이스주소**):** XenMobile Server URL 을입력합니다.
- **Single Sign-on Domain(SSO** 도메인**):** Active Directory 도메인이름을입력합니다.

  Citrix 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.

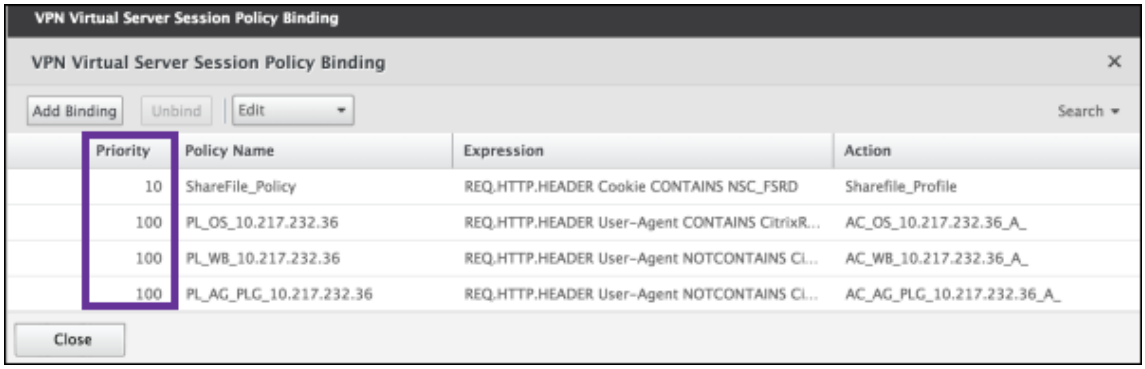
7. **Create(만들기)** 를클릭한다음 **Close(닫기)** 를클릭합니다.

Citrix Gateway 가상서버에서정책구성

Citrix Gateway 가상서버에서다음과같은설정을구성합니다.

1. Citrix Gateway 구성유틸리티의왼쪽탐색창에서 **Citrix Gateway >** 가상서버를클릭합니다.
2. **Details(세부정보)** 창에서 Citrix 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 (가장작은숫자) 를갖도록설정합니다. 예:



7. **Done(**완료**)** 을클릭한다음실행중인 Citrix ADC 구성을저장합니다.

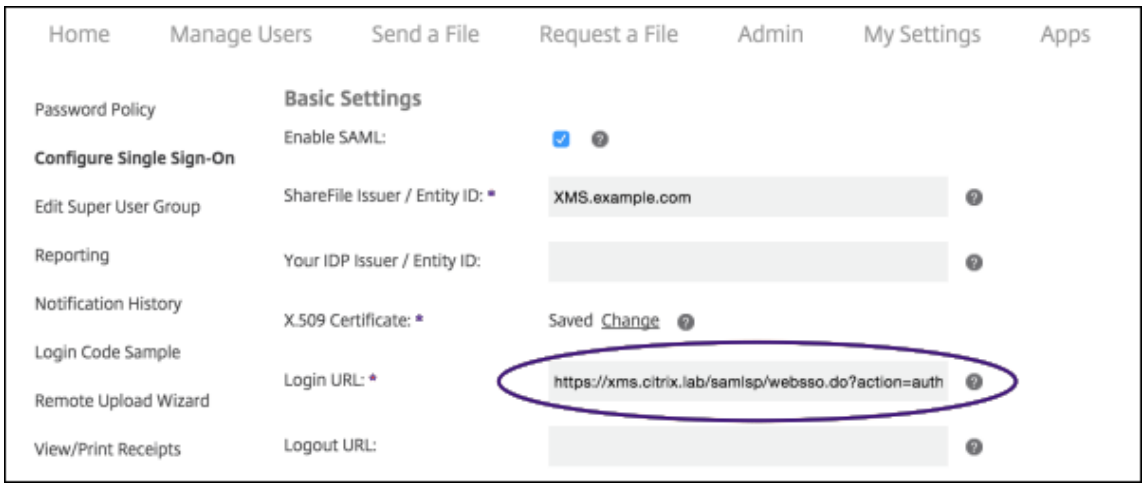
Citrix Files.com SSO 설정수정

MDX 및비 MDX Citrix Files 앱을다음과같이변경합니다.

> 중요**:**
>
> 다음과같은경우내부응용프로그램이름에새번호가추가됩니다.
>
> - Citrix Files 앱을수정또는재생성할때마다
> - XenMobile 에서 Content Collaboration 설정을변경할때마다
>
> 그러므로 Citrix Files 웹사이트에서로그인 URL 을업데이트하여업데이트된앱이름을반영해야합니다.

1. Content Collaboration 계정 (`https://<subdomain>.sharefile.com`) 에 Content Collaboration 관리자로로그온합니다.
2. Content Collaboration 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 Citrix Gateway 가상서버외부 FQDN 과 **/cginfra/https/**를삽입한다음 XenMobile FQDN 뒤에 **8443** 을추가합니다.

  다음은편집된 URL 의샘플입니다. `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

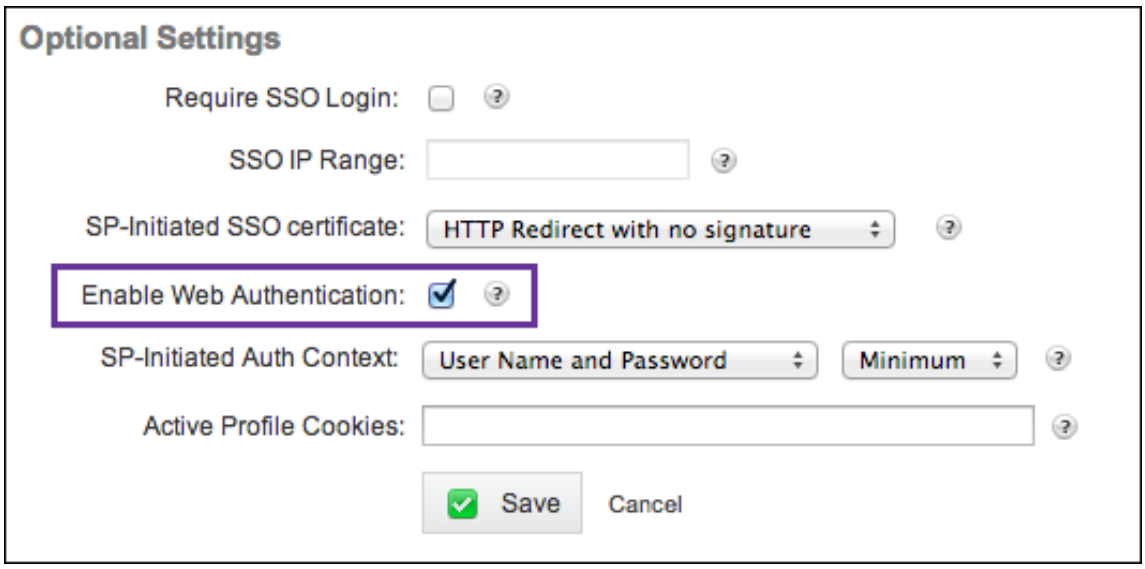
- &app=ShareFile_SAML_SP 매개변수를내부 Citrix Files 응용프로그램이름으로변경합니다. 내부이름은기본적으로 ShareFile_SAML입니다. 그러나구성을변경할때마다내부이름에번호가추가됩니다(ShareFile_SAML_2, ShareFile_SAML_3 등). 구성 **> ShareFile** 페이지에서 앱내부이름을찾을수있습니다.

  다음은편집된 URL 의샘플입니다. `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- URL 끝에 &nssso=**true**를추가합니다.

  다음은최종 URL 의샘플입니다. `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. 옵션설정에서 웹인증사용확인란을선택합니다.



구성유효성검사

다음을수행하여구성의유효성을검사합니다.

1. 브라우저를 `https://<subdomain>sharefile.com/saml/login`으로가리킵니다.

   Citrix Gateway 로그온양식으로리디렉션됩니다. 리디렉션되지않으면이전구성설정을확인하십시오.

2. 구성한 Citrix Gateway 및 XenMobile 환경의사용자이름과암호를입력합니다.

   `<subdomain>.sharefile.com`의 Citrix Files 폴더가나타납니다. Citrix Files 폴더가보이지않으면적절한 로그온자격증명을입력했는지확인하십시오.

IdP 역할을하는 Azure Active Directory

May 6, 2022

Azure Active Directory(ADD) 를 IdP(ID 공급자) 로구성하면사용자가 Azure 자격증명을사용하여 XenMobile 에등록할 수있습니다.

iOS, Android, Windows 10, Windows 11 장치가지원됩니다. iOS 및 Android 장치는 Secure Hub 를통해등록됩니다. 이인증방법은 Citrix Secure Hub 를통해 MDM 에등록하는사용자만사용할수있습니다. MAM 에등록하는장치는 AAD 자격증명을사용하여인증할수없습니다. MDM+MAM 을통해 Secure Hub 를사용하려면 MAM 등록에 Citrix Gateway 를 사용하도록 XenMobile 을구성합니다. 자세한내용은 Citrix Gateway 및 XenMobile을참조하십시오.

설정 **>** 인증 **> IDP** 에서 Azure 를 IdP 로구성합니다. **IDP** 페이지는이버전의 XenMobile 에새롭게추가된페이지입니다. 이전버전의 XenMobile 에서는 설정 **> Microsoft Azure** 에서 Azure 를추가했습니다.

요구사항

- 버전및라이센스
  - iOS 또는 Android 장치를등록하려면 Secure Hub 10.5.5 가필요합니다.
  - Windows 10 및 Windows 11 장치를등록하려면 Microsoft Azure Premium 라이센스가필요합니다.
- 디렉터리서비스및인증
  - XenMobile Server 가인증서기반인증을사용하도록구성해야합니다.
  - Citrix ADC 를인증에사용중인경우인증서기반인증을사용하도록 Citrix ADC 를구성해야합니다.
  - 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 로그인화면에 Azure Active Directory 사용자이름과암호를입력합니다.
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 에사용자지정도메인이름추가를참조하십시오.
2. 디렉터리통합도구를사용하여온-프레미스디렉터리를 Azure Active Directory 로확장합니다. 자세한내용은 디렉터리통합을참조하십시오.

Azure AD 를사용하여 Windows 10 및 Windows 11 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 단계에서만든온-프레미스 MDM 응용프로그램을선택합니다. 이사용자의장치관리옵션을선택하여모든사용자또는특정사용자그룹에대한 MDM 관리를사용하도록설정합니다.

   Windows 10 및 Windows 11 장치에 Azure AD 를사용하는방법에대한자세한내용은 Microsoft 문서 Azure Active Directory 와 MDM 통합을참조하십시오.

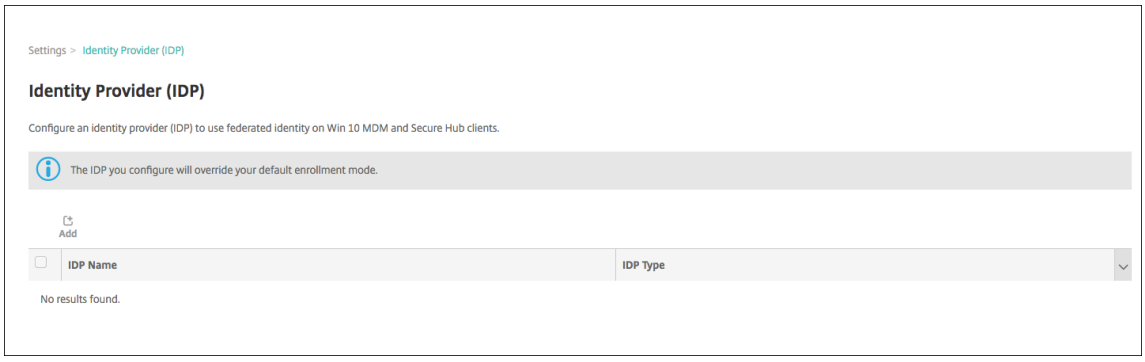
Azure AD 를 IdP 로구성

1. Azure 계정에서필요한다음정보를찾거나메모합니다.

   - Azure 응용프로그램설정페이지의테넌트 ID.
   - Azure AD 를사용하여 Windows 10 및 Windows 11 장치를등록하려는경우다음도필요합니다.
     - 앱 **ID URI:** XenMobile 을실행하는서버의 URL 입니다.
     - 클라이언트 **ID:** Azure 구성페이지에서앱의고유식별자입니다.
     - 키**:** Azure 응용프로그램설정페이지에서확인할수있습니다.

2. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.

3. 인증아래에서 **IDP(ID** 공급자**)** 를클릭합니다. **ID** 공급자페이지가나타납니다.

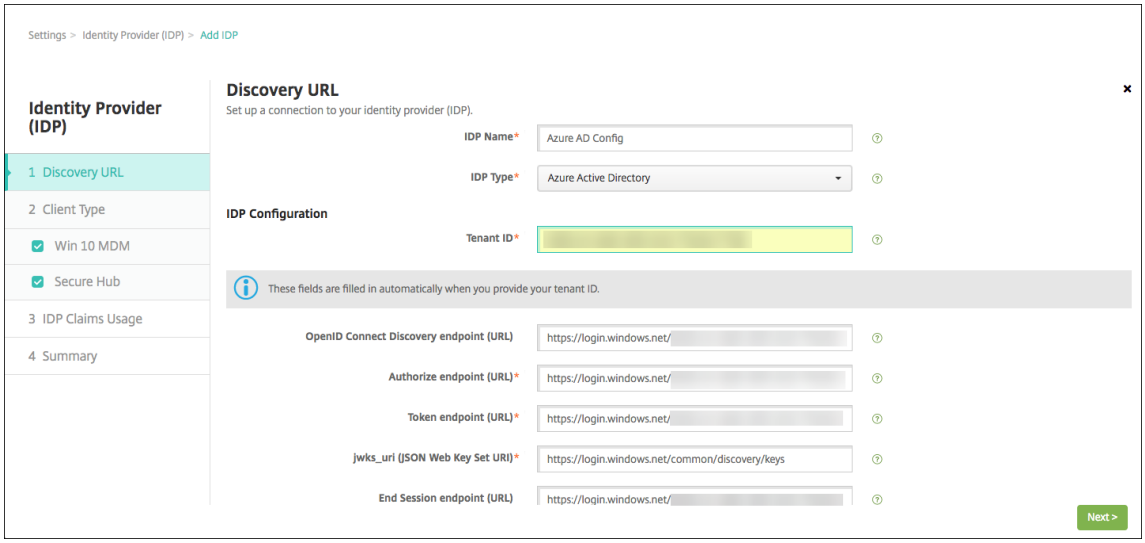


4. 추가를클릭합니다. **IDP** 구성페이지가나타납니다.

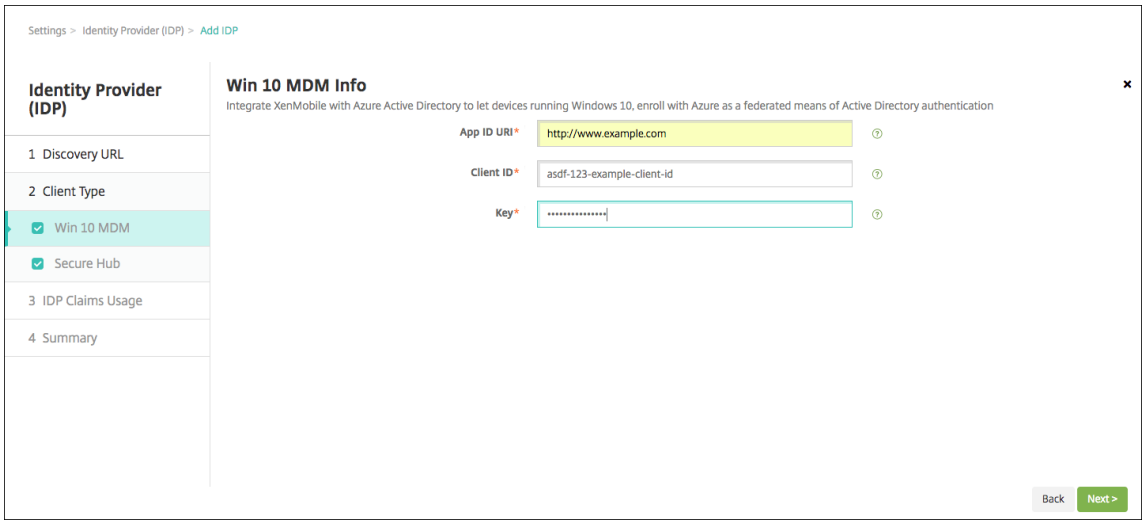
5. IdP 에대한다음정보를구성합니다.

   - **IDP** 이름**:** 만들려는 IdP 연결의이름을입력합니다.
   - **IDP** 유형**:** Azure Active Directory 를 IdP 유형으로선택합니다.
   - 테넌트 **ID:** Azure 응용프로그램설정페이지에서이값을복사합니다. 브라우저주소표시줄에서숫자와문자로구성된섹션을복사합니다.

   예를들어 `https://manage.windowszaure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...`에서테넌트 ID 는 `abc123-abc123-abc123`입니다.



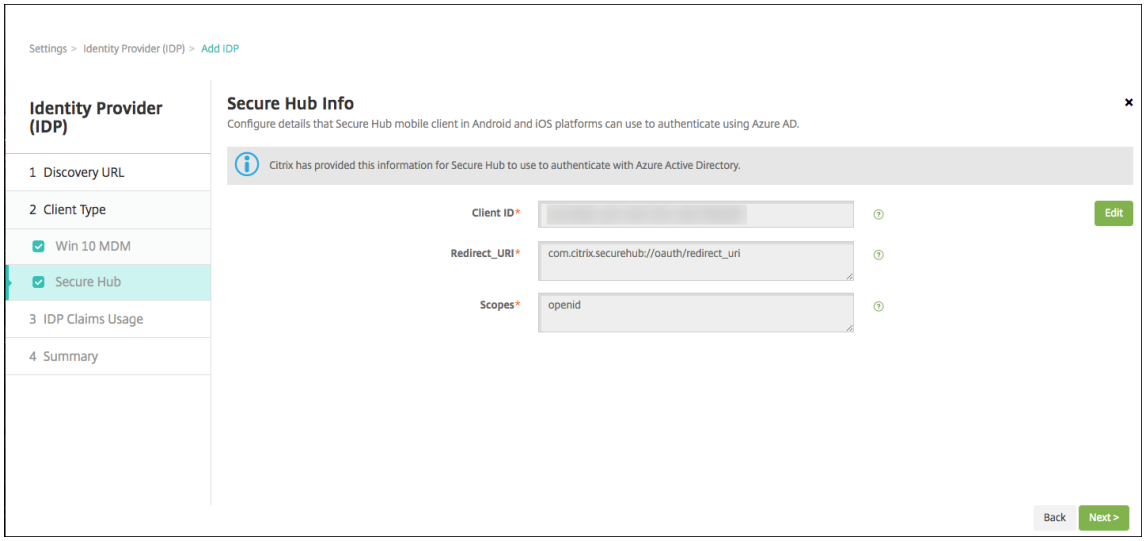
6. 나머지필드는자동으로입력됩니다. 입력되면 다음을클릭합니다.
7. MDM 등록에대해 Azure AD 를사용하여 Windows 10 및 Windows 11 장치를등록하도록 XenMobile 을구성하려면다음설정을구성하십시오. 이선택적단계를건너뛰려면 **Windows MDM** 을선택취소합니다.
   - 앱 **ID URI:** Azure 설정을구성할때입력한 XenMobile Server 의 URL 을입력합니다.
   - 클라이언트 **ID:** Azure 구성페이지에서이값을복사하여붙여넣습니다. 클라이언트 ID 는앱의고유식별자입니다.
   - 키**:** Azure 응용프로그램설정페이지에서이값을복사합니다. 키아래에있는목록에서기간을선택하고설정을저장합니다. 그런다음키를복사하여이필드에붙여넣을수있습니다. 앱이 Microsoft Azure AD 에서데이터를읽거나쓸때키가필요합니다.



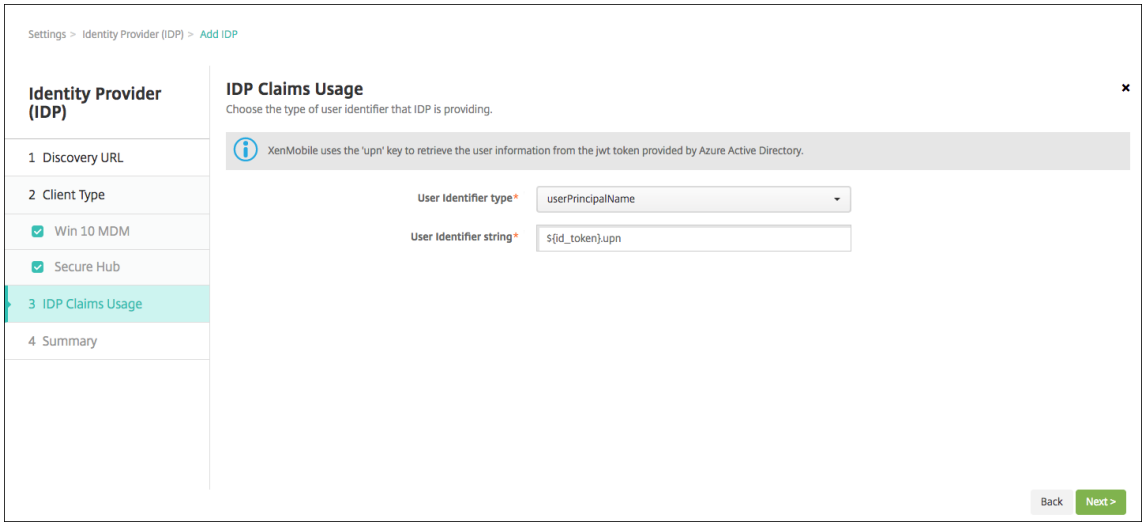
8. 다음을클릭합니다.

   Citrix 는 Secure Hub 를 Microsoft Azure 에등록했으며정보를유지합니다. 이화면에는 Secure Hub 가 Azure Active Directory 와통신하는데사용하는세부정보가표시됩니다. 이페이지는향후이러한정보를변경해야할때사용됩니다. Citrix 에서편집하도록안내하는경우에만이페이지를편집하십시오.

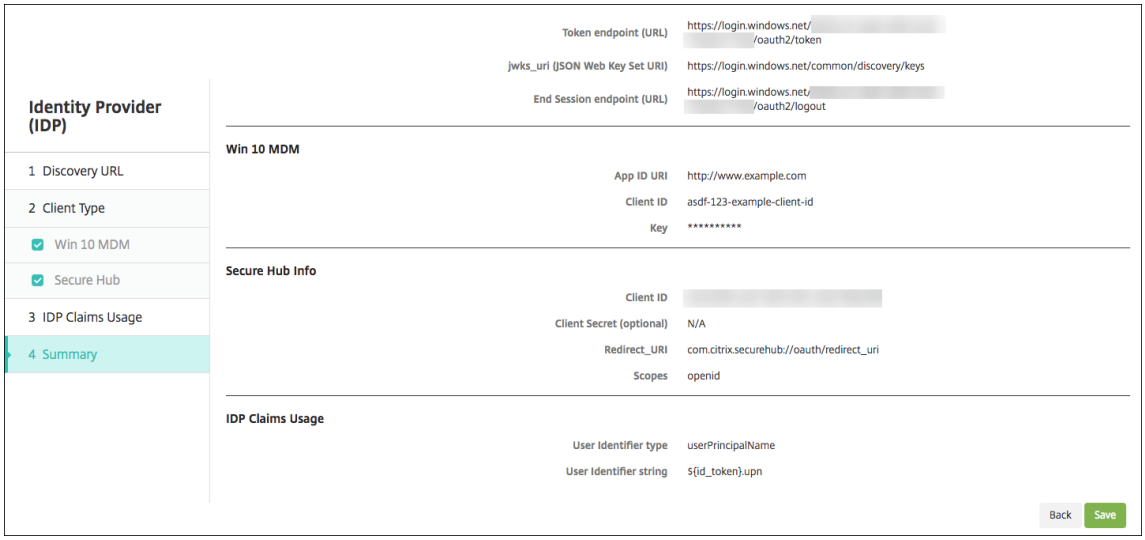
9. 다음을클릭합니다.



10. IdP 가제공하는사용자식별자유형을구성합니다.
    - 사용자식별자유형**:** 드롭다운목록에서 **userPrincipalName** 을선택합니다.
    - 사용자식별자문자열**:** 이필드는자동으로입력됩니다.
11. 다음을클릭합니다.

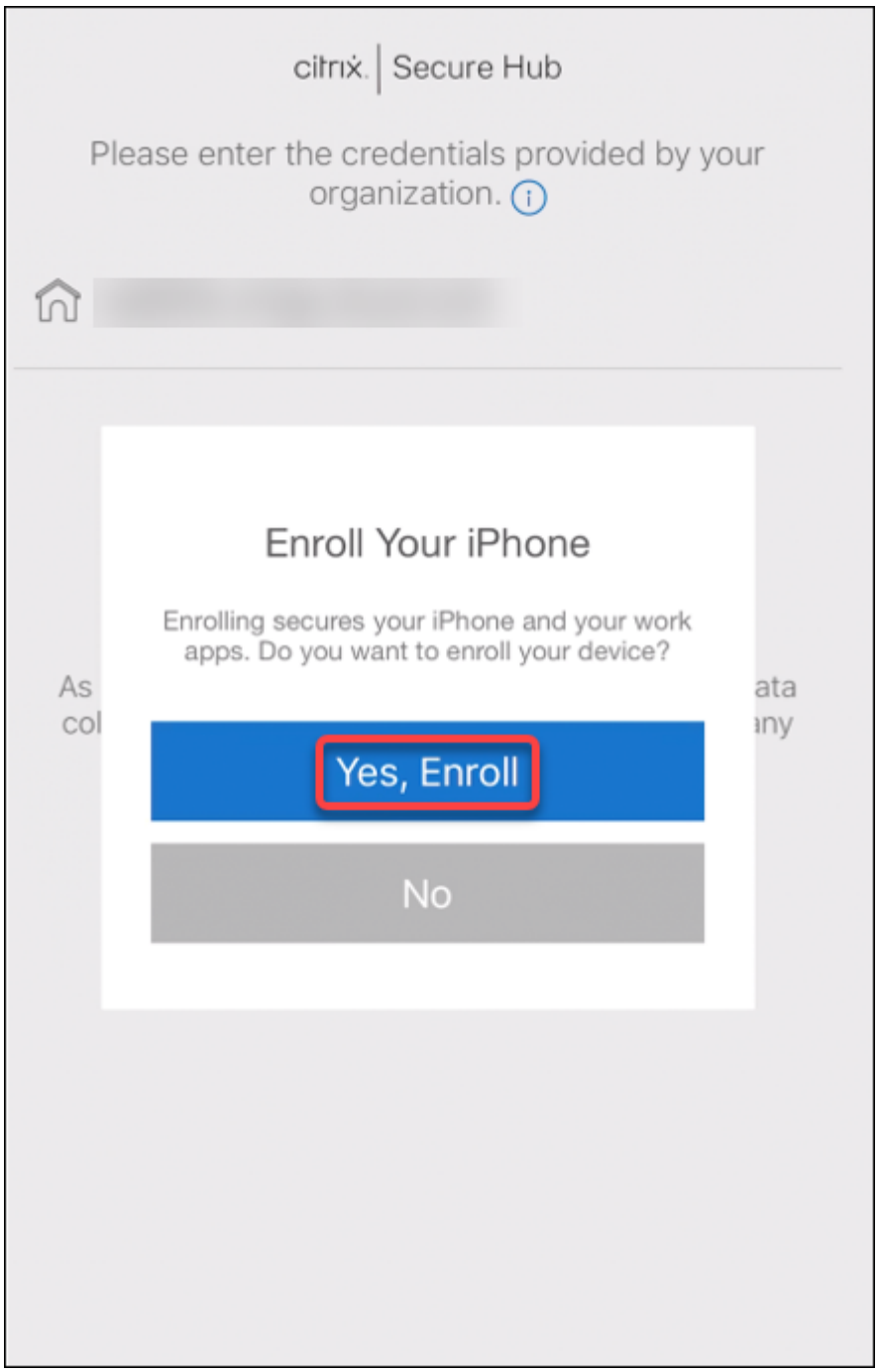


12. 요약페이지를검토하고 저장을클릭합니다.

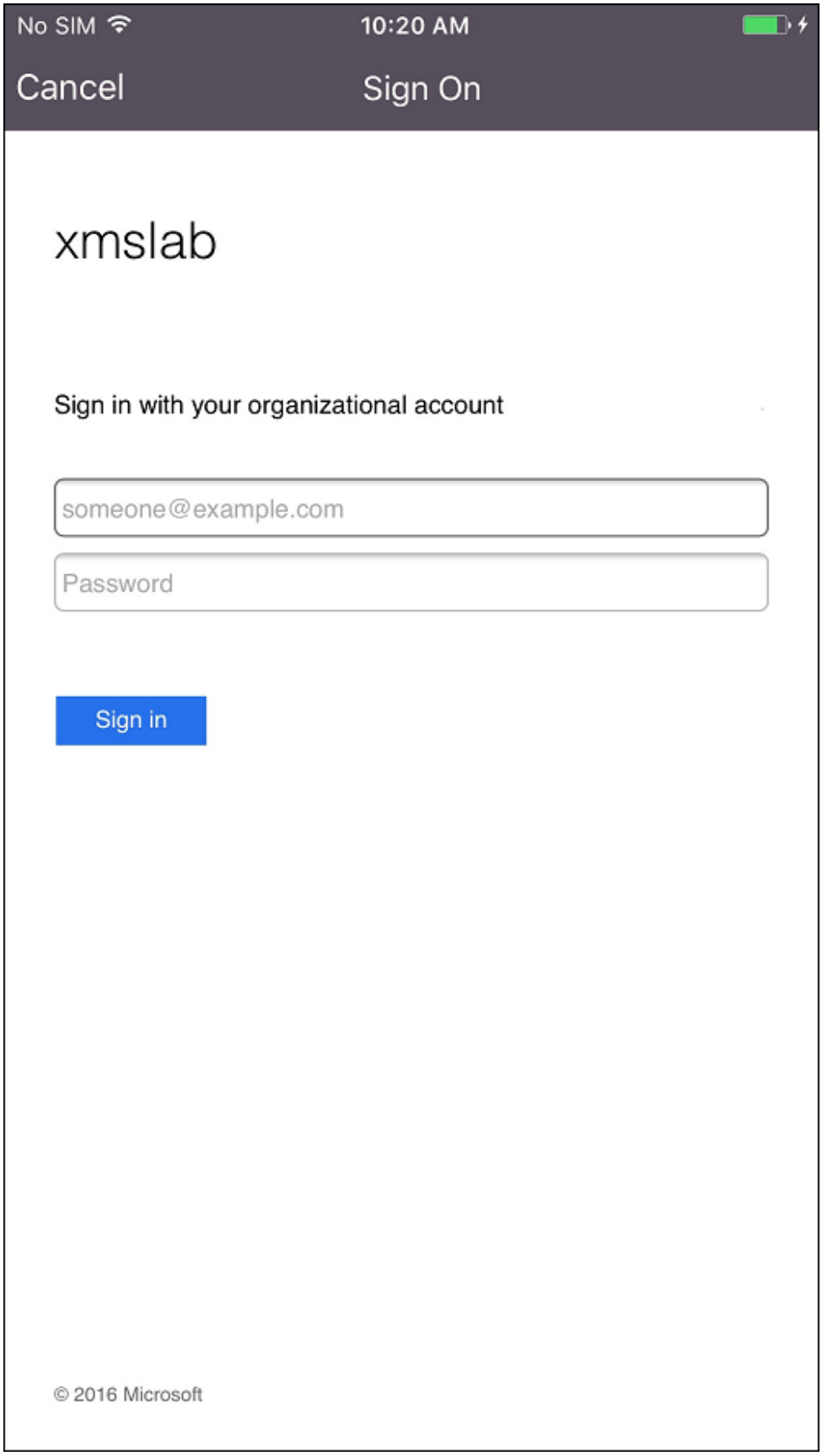


사용자가경험하는환경

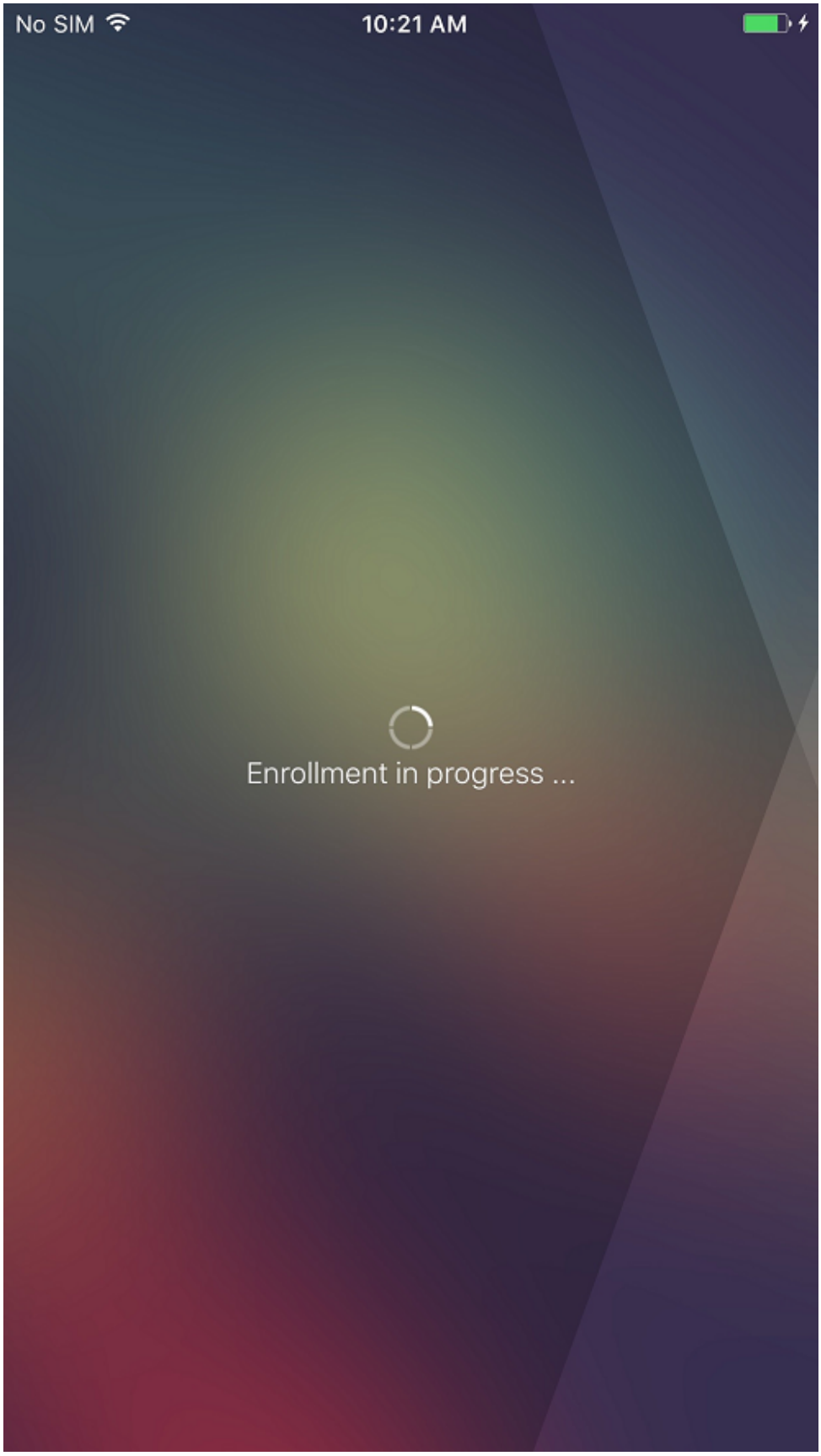
1. 사용자가 Secure Hub 를시작합니다. 그런다음사용자는 XenMobile Server 의 FQDN(정규화된도메인이름), UPN(사용자계정이름) 또는전자메일주소를입력합니다.

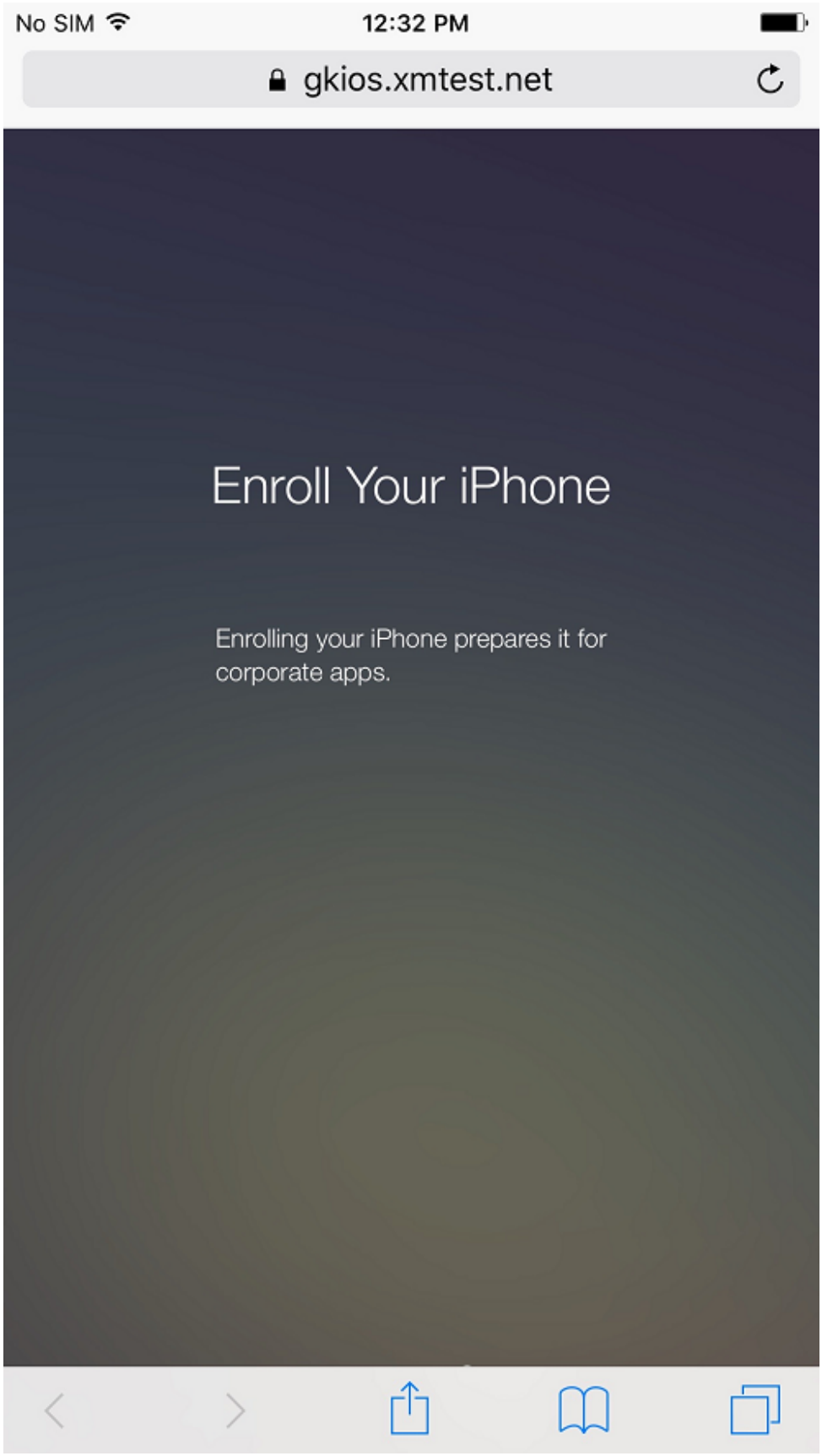


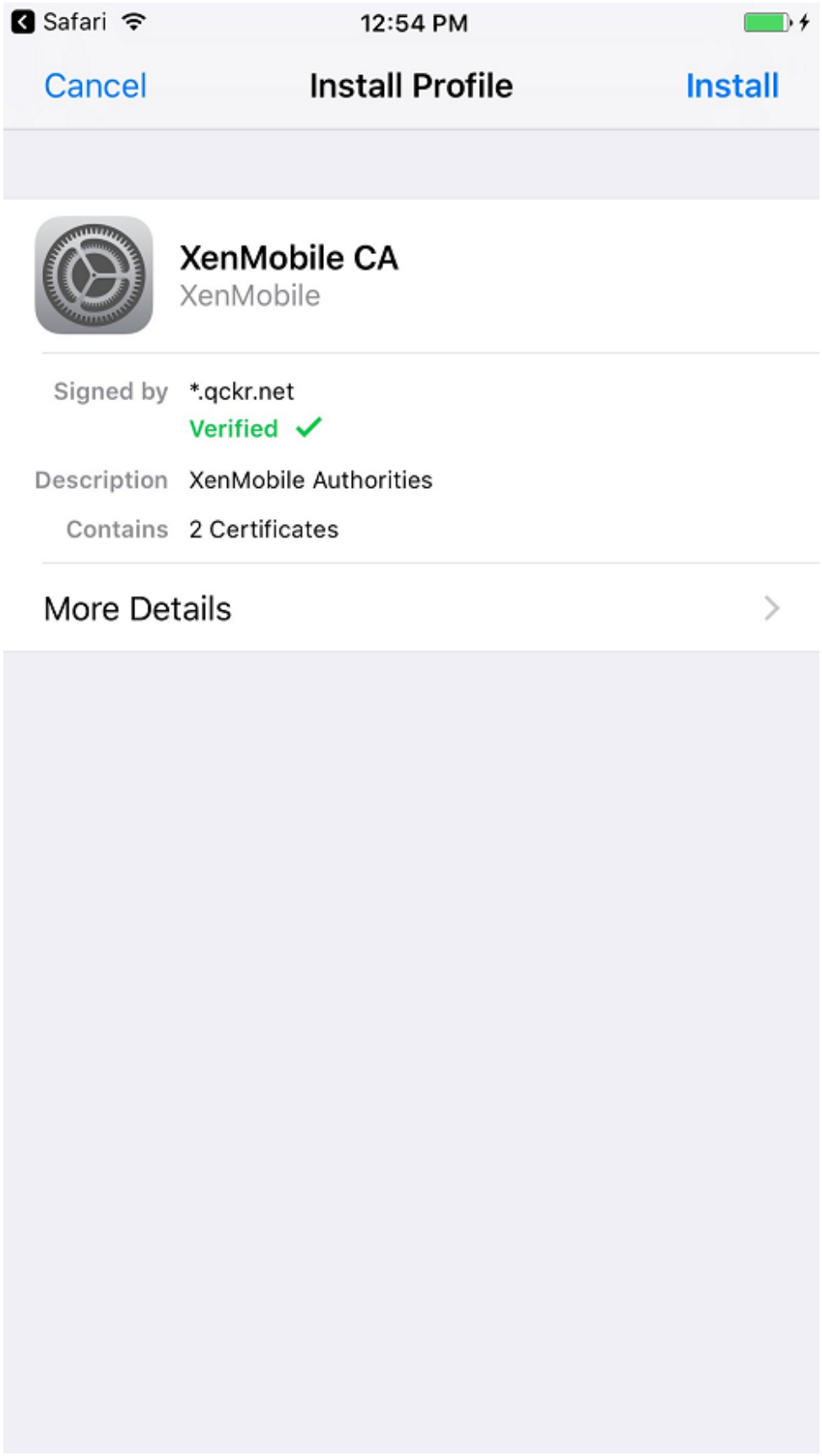
2. 그리고 예**.** 등록하겠습니다를클릭합니다.



3. 사용자는자신의 Azure AD 자격증명을사용하여로그온합니다.







4. 사용자는 Secure Hub 를통한다른등록과동일한방법으로등록단계를완료합니다.

> 참고:
>
> XenMobile 은등록초대에대해 Azure AD 를통한인증을지원하지않습니다. 사용자에게등록 URL 이포함된등록초대를보내는경우사용자는 Azure AD 대신 LDAP 를통해인증합니다.

파생된자격증명

April 5, 2021

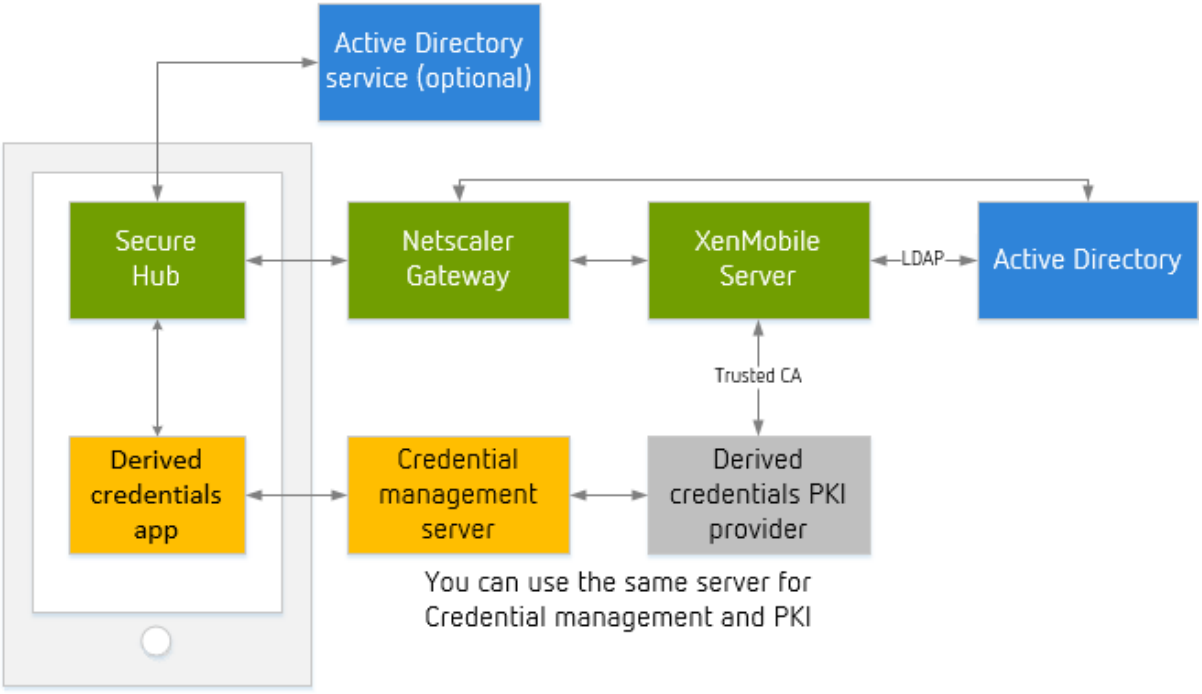
파생된자격증명은모바일장치를위한강력한인증을제공합니다. 스마트카드는자격증명을제공하며, 카드가아닌모바일장치에상주합니다. 스마트카드는 PIV(Personal Identity Verification) 카드입니다.

파생된자격증명은 UPN 같은사용자식별자가포함된등록인증서입니다. XenMobile 은자격증명공급자로부터받은자격증명을장치의보안저장소에저장합니다.

XenMobile 은파생된자격증명을장치등록및인증에사용할수있습니다. 파생된자격증명을사용하도록구성하면 XenMobile 이등록초대또는기타등록보안모드를지원하지않습니다. iOS 를등록하는동안파생된자격증명앱을사용할수있습니다.

아키텍처

등록을위해 XenMobile Server 는다음다이어그램에서와같이구성요소에연결합니다.

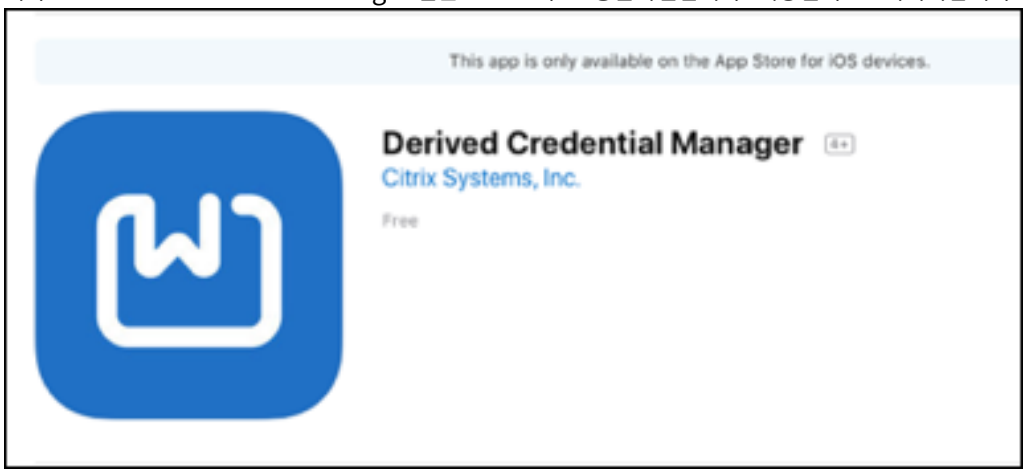


- 장치등록도중 Secure Hub 는파생된자격증명앱에서인증서를가져옵니다.

- 파생된자격증명앱은등록도중자격증명관리서버와통신합니다.
- 자격증명관리서버와타사 PKI 공급자에같거나다른서버를사용할수있습니다.
- 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.



    - Citrix Derived Credential Manager 앱은신규등록만지원합니다. 장치사용자는재등록해야합니다.
      - XenMobile Server 버전 10.8 이상.
      - MDM+MAM 으로장치를등록해야합니다.
  - 기타파생된자격증명공급자**:** 다른자격증명솔루션대부분은 XenMobile 과호환될가능성이높지만운영환경에배포하기전에통합을테스트하십시오.
- 자격증명공급자서버에인증서를발급하는기관의루트인증서가있어야합니다. 이렇게설정하면 XenMobile 이등록도중디지털서명된인증서를수락할수있습니다. 인증서추가에대한자세한내용은 인증서및인증을참조하십시오.
  - 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 확장의 otherName, rfc822Name 또는 dNSName 필드로형식지정되어야합니다. 다른필드는지원되지않습니다. 주체대체이름에대한자세한내용은 RFC(https://www.ietf.org/rfc/rfc5280.txt) 를참조하십시오.
  - 전자메일또는 CN 에서주체필드의사용자 ID 는지원되지않습니다.

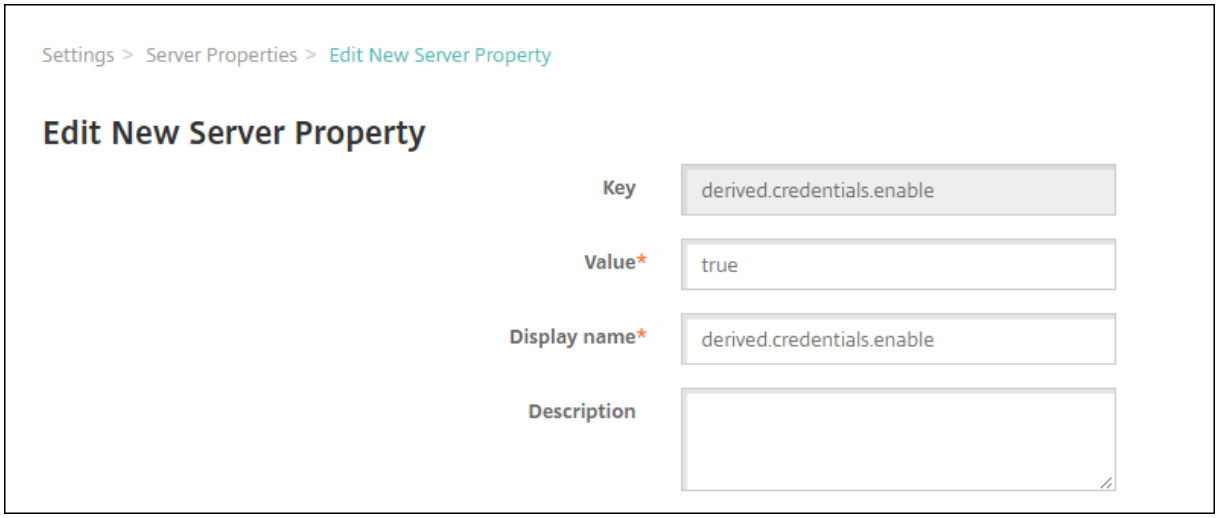
- 인증서인증또는인증서와보안토큰인증에대해구성된 Citrix Gateway

파생된자격증명을사용하도록설정

기본적으로 XenMobile 콘솔에는 설정 **>** 파생된자격증명페이지가포함되지않습니다.

파생된자격증명에대한인터페이스를사용하려면:

- 설정 **>** 서버속성에서 **derived.credentials.enable** 을서버속성으로추가하고속성값을 **true** 로설정합니다.

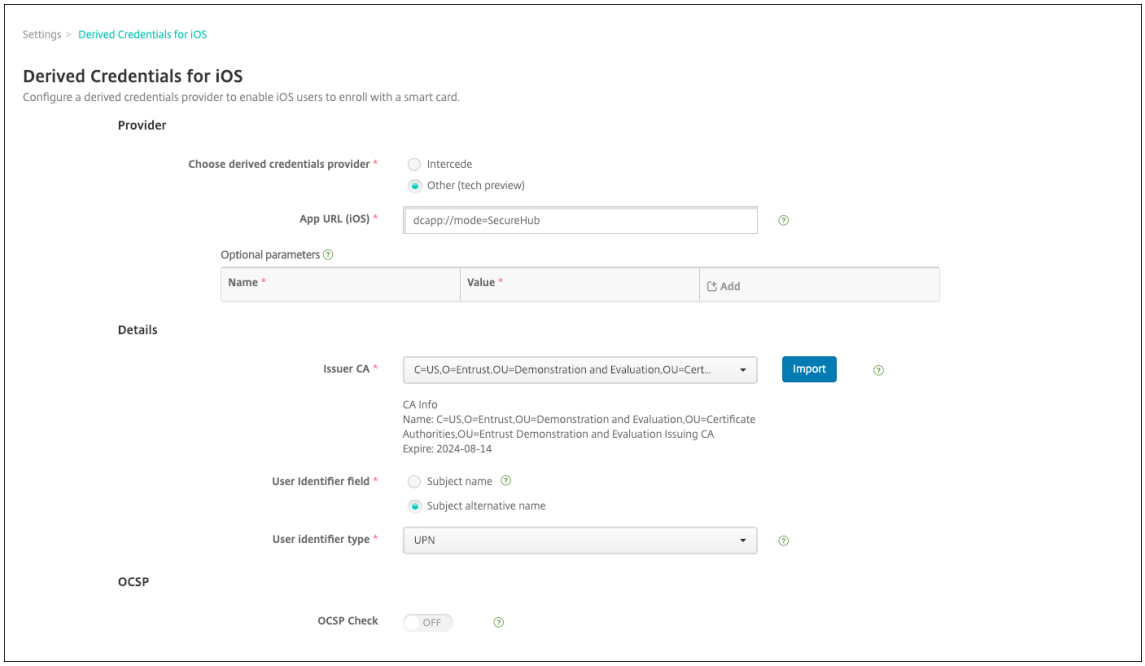


파생된자격증명구성

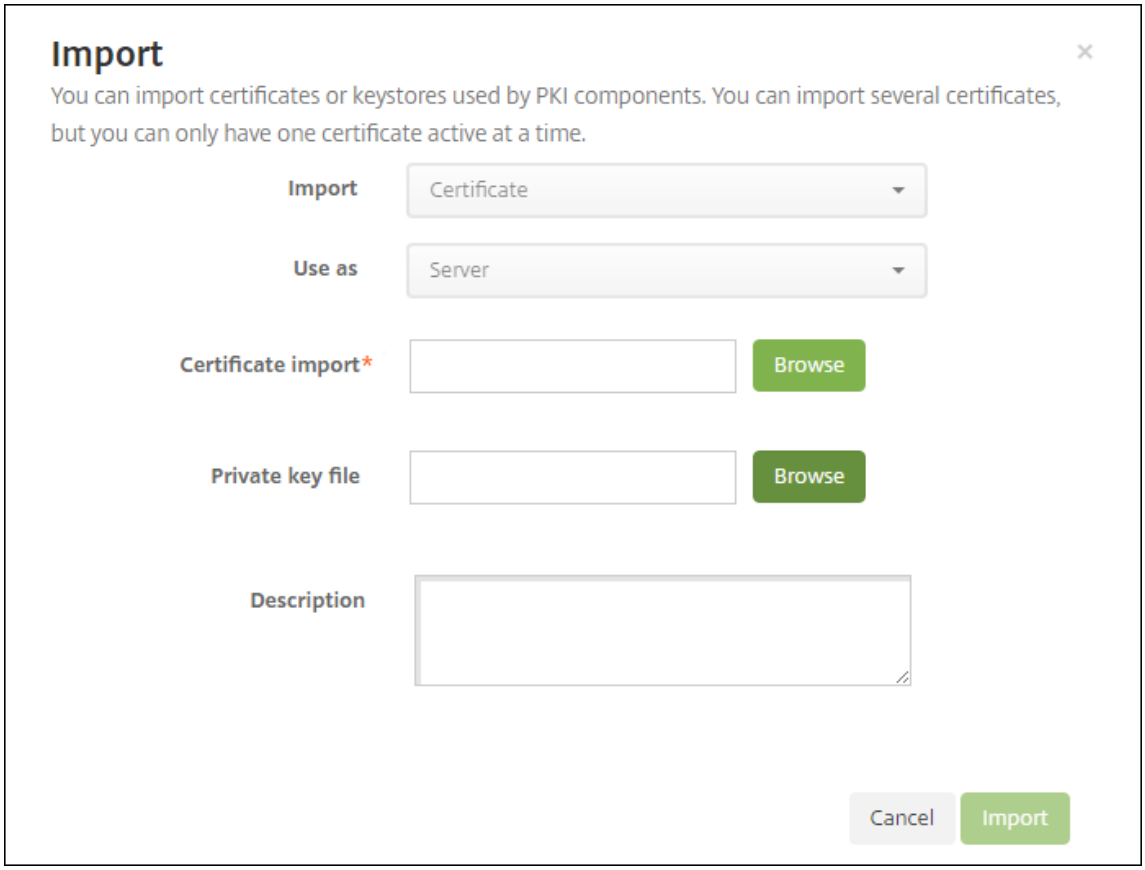
여기서는 XenMobile 과통합할계획인파생된자격증명공급자에대한작동하는구성이있는것으로가정합니다. 그러면해당서버와통신하도록 XenMobile 을구성할수있습니다. 이미 XenMobile 에추가된파생된자격증명 CA 인증서를선택하거나인증서를가져올수도있습니다.

해당 CA 인증서에대한 OCSP(Online Certificate Status Protocol) 지원을활성화할수있습니다. OCSP 에대한자세한내용은 PKI 엔터티의 “임의의 CA” 를참조하십시오.

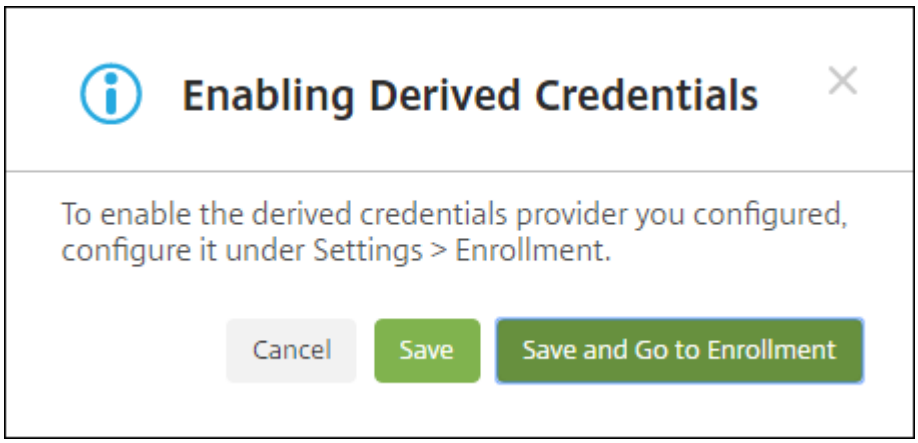
1. XenMobile 콘솔에서 설정 **> iOS** 용파생된자격증명으로이동하십시오.
2. Entrust Datacard 의경우 파생된자격증명공급자선택에서 기타를선택합니다. 앱 **URL(iOS)** 에 `dcapp://mode=SecureHub`를입력합니다.



3. 선택적매개변수**:** 일부파생된자격증명공급자의경우연결을위한매개변수를제공해야할수있습니다. 예를들어공급업체에서 백엔드서버의 URL 을지정하도록요구할수있습니다. 추가를클릭하여매개변수를제공합니다.
4. 파생된자격증명의인증서지정: 인증서가이미 XenMobile 에업로드된경우 발급자 **CA** 에서해당인증서를선택합니다. 그렇지않은경우에는 가져오기를클릭하여인증서를추가합니다. 인증서가져오기대화상자가나타납니다.
5. 인증서가져오기대화상자에서 찾아보기를클릭하여인증서로이동합니다. 그런다음 찾아보기를클릭하여개인키파일로이동합니다.

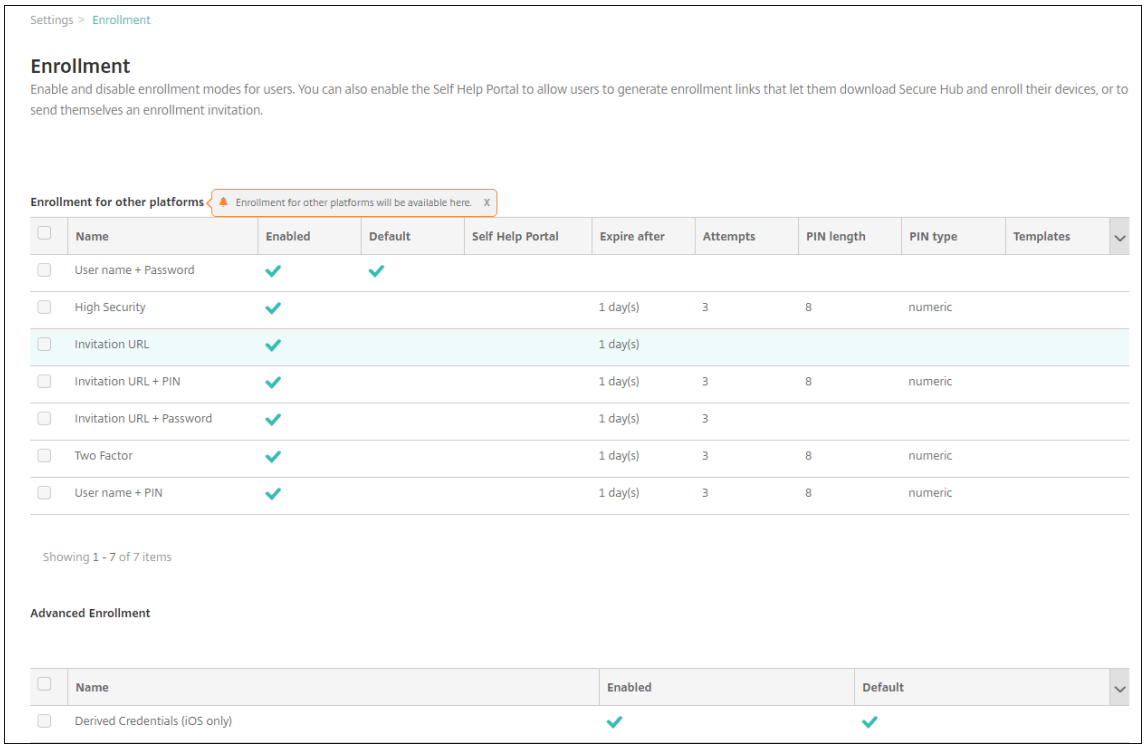


6. 설정을구성합니다.
   - Citrix Derived Credential Manager 앱의경우 사용자식별자필드는 주체대체이름이고 사용자식별자유형은 **userPrincipalName** 입니다.
   - 다른파생된자격증명공급자의경우해당공급자에정보를요청하십시오.
7. 원하는경우 OCSP 응답자를사용하여인증서해제를확인할수있습니다. 보안을위해 OCSP 응답자를사용하는것이좋습니다. 기본적으로 OSP 확인은 꺼짐입니다.
   - CA 인증서에대한 OCSP 지원을활성화하는경우 사용자지정 **OCSP URL** 사용에대한옵션을선택합니다. 기본적으로 XenMobile 은인증서에서 OCSP URL 을추출합니다 (해지를위해인증서정의사용옵션). 응답자 URL 을지정하려면 사용자지정사용을클릭하고 URL 을입력합니다.
   - 응답자 **CA:** 응답자 **CA** 에서인증서를선택합니다. 또는 가져오기를클릭한다음 인증서가져오기대화상자를사용하여인증서를찾습니다.
8. 저장을클릭합니다. 파생된자격증명사용대화상자가나타납니다.

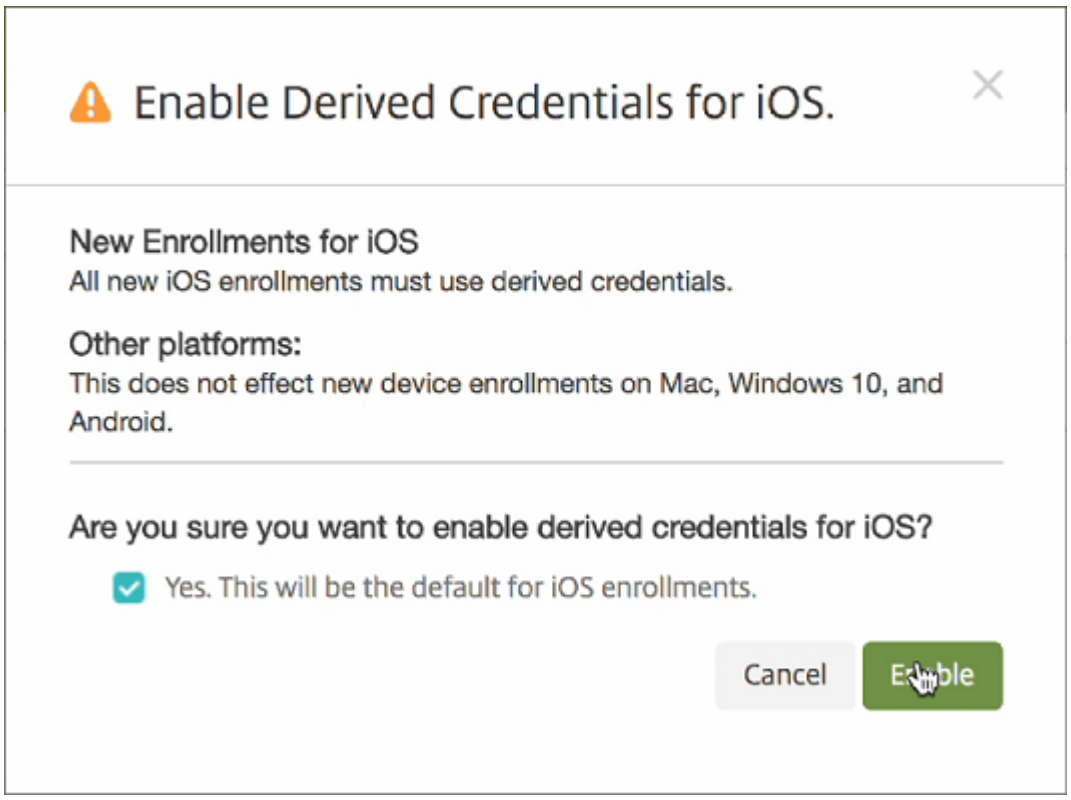


- 파생된자격증명구성을사용하도록설정하려면 저장을클릭합니다. 파생된자격증명을사용하려면등록설정도구성해야합니다.
- 파생된자격증명구성을사용하도록설정한다음곧바로 설정 **>** 등록으로이동하려면 저장하고등록으로이동을클릭하십시오.

9. 등록에파생된자격증명을사용하도록설정하려면: 설정 **>** 등록페이지의 고급등록아래에서 파생된자격증명 **(iOS** 전용**)** 을선택하고 사용을클릭합니다.



10. 확인대화상자가나타납니다. 파생된자격증명을사용하도록설정하려면확인란을선택하고 사용을클릭합니다.



11. 파생된자격증명등록에대한옵션을편집하려면 설정 **>** 등록으로이동하고 파생된자격증명 **(iOS** 전용**)** 을선택한다음 편집을클릭합니다.

파생된자격증명을사용하도록설정한후: 장치등록보고서의 등록모드열에 **derived_credentials** 가표시됩니다.

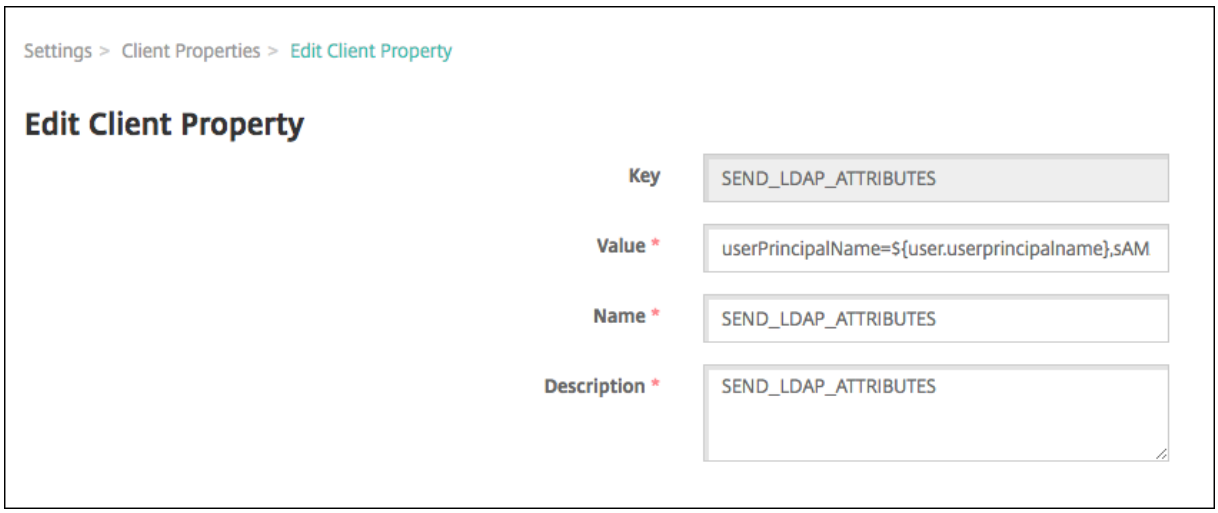
> 중요**:**
>
> 파생된자격증명공급자를추가한후 XenMobile Server 를다시시작합니다.

XenMobile Server 에서 **Secure Mail** 구성

Secure Mail 에서파생된자격증명을지원하려면 `SEND_LDAP_ATTRIBUTES` 클라이언트속성을추가합니다. 클라이언트속성추가에대한자세한내용은 클라이언트속성을참조하십시오.

클라이언트속성에대한다음정보를사용합니다.

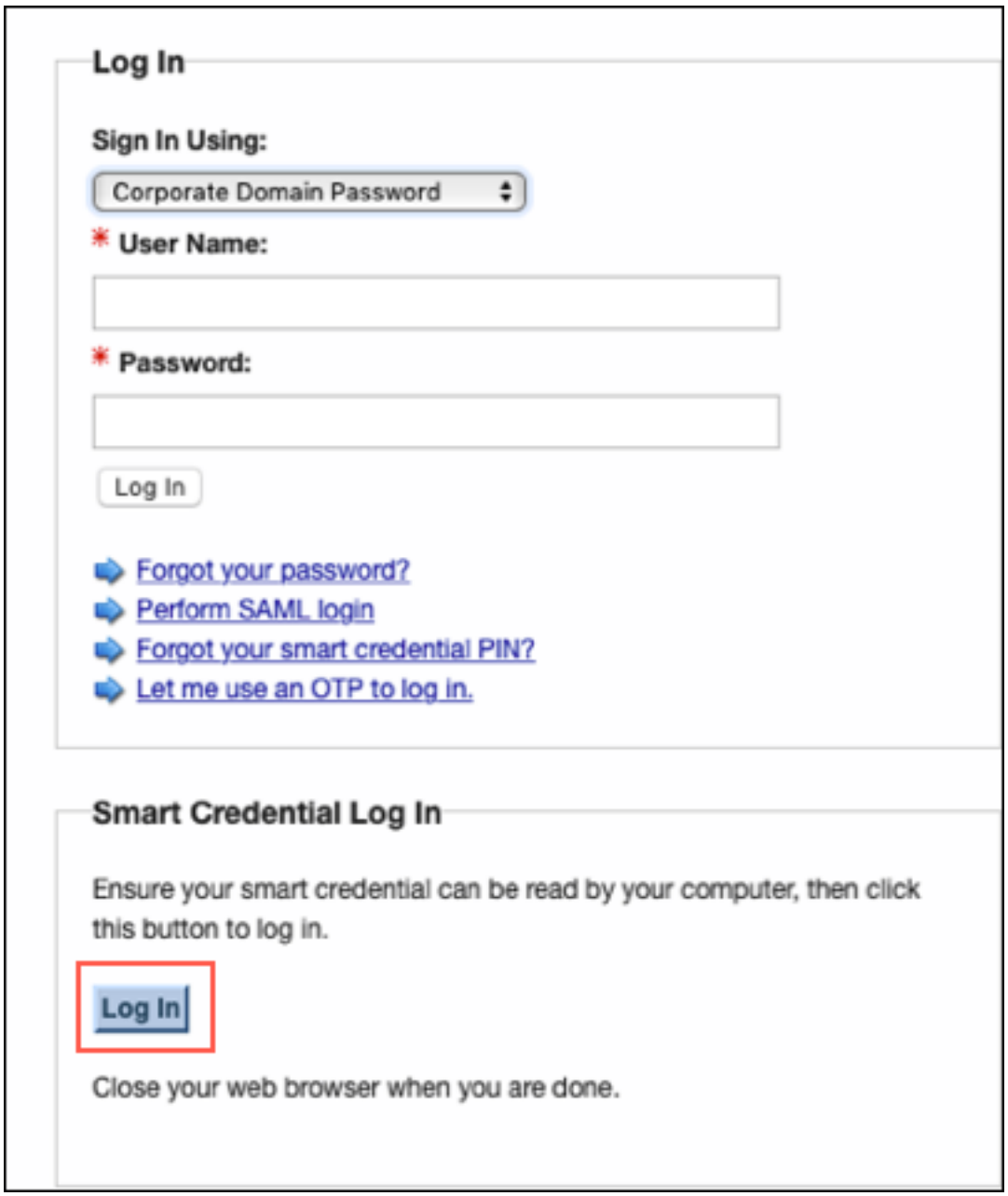
- 키**:** `SEND_LDAP_ATTRIBUTES`
- 값**:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



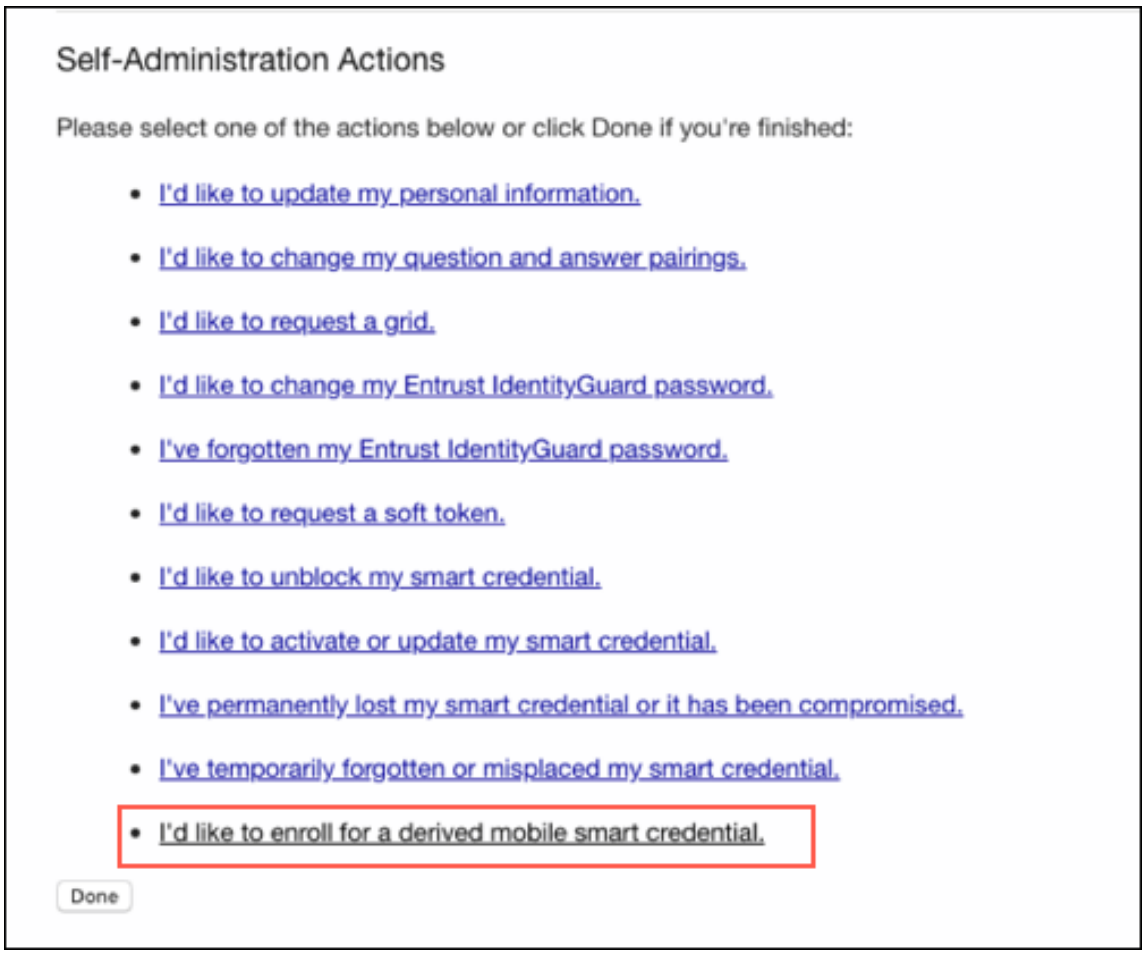
iOS 장치에서 Entrust Datacard 의파생된자격증명활성화

> 참고:
>
> Entrust 웹사이트를사용하는상태로 PIV 카드를변경할때브라우저캐시를지웁니다.

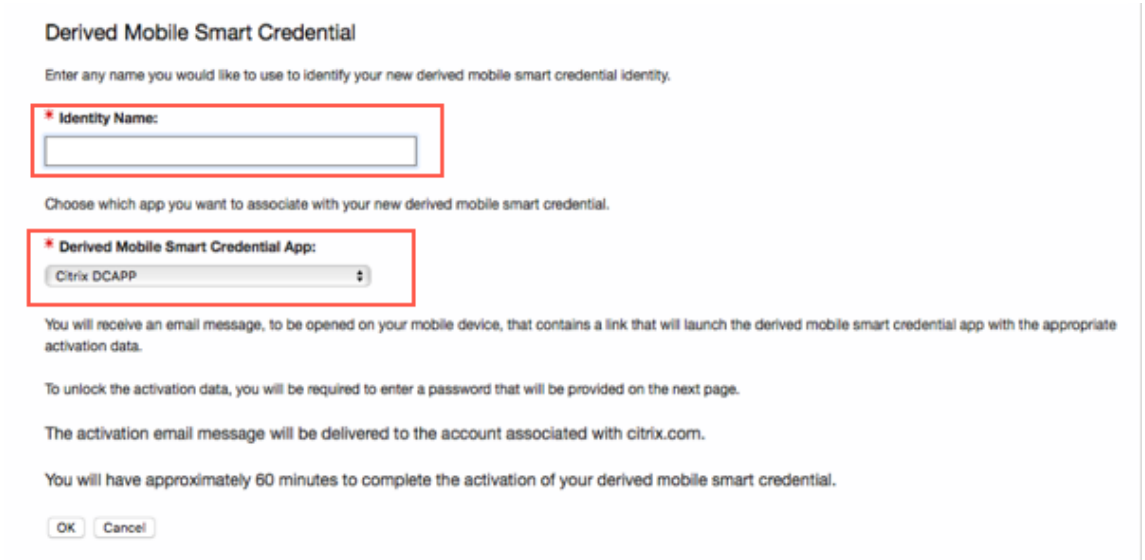
1. 새로운스마트자격증명을요청하려면데스크톱또는장치를사용하여 Entrust 사이트에로그인합니다. 페이지하단의 **Smart Credential Log In(**스마트자격증명로그인**)** 버튼을사용하여로그인할수있습니다. 사용자데스크톱에부착된판독기에스마트카드를삽입해야합니다.



2. **Self-Administration Actions**(자체관리작업) 에서 **I'd like to enroll for a derived mobile smart credential**(파생된모바일스마트자격증명등록) 을선택하고 **Done**(완료) 을클릭합니다.



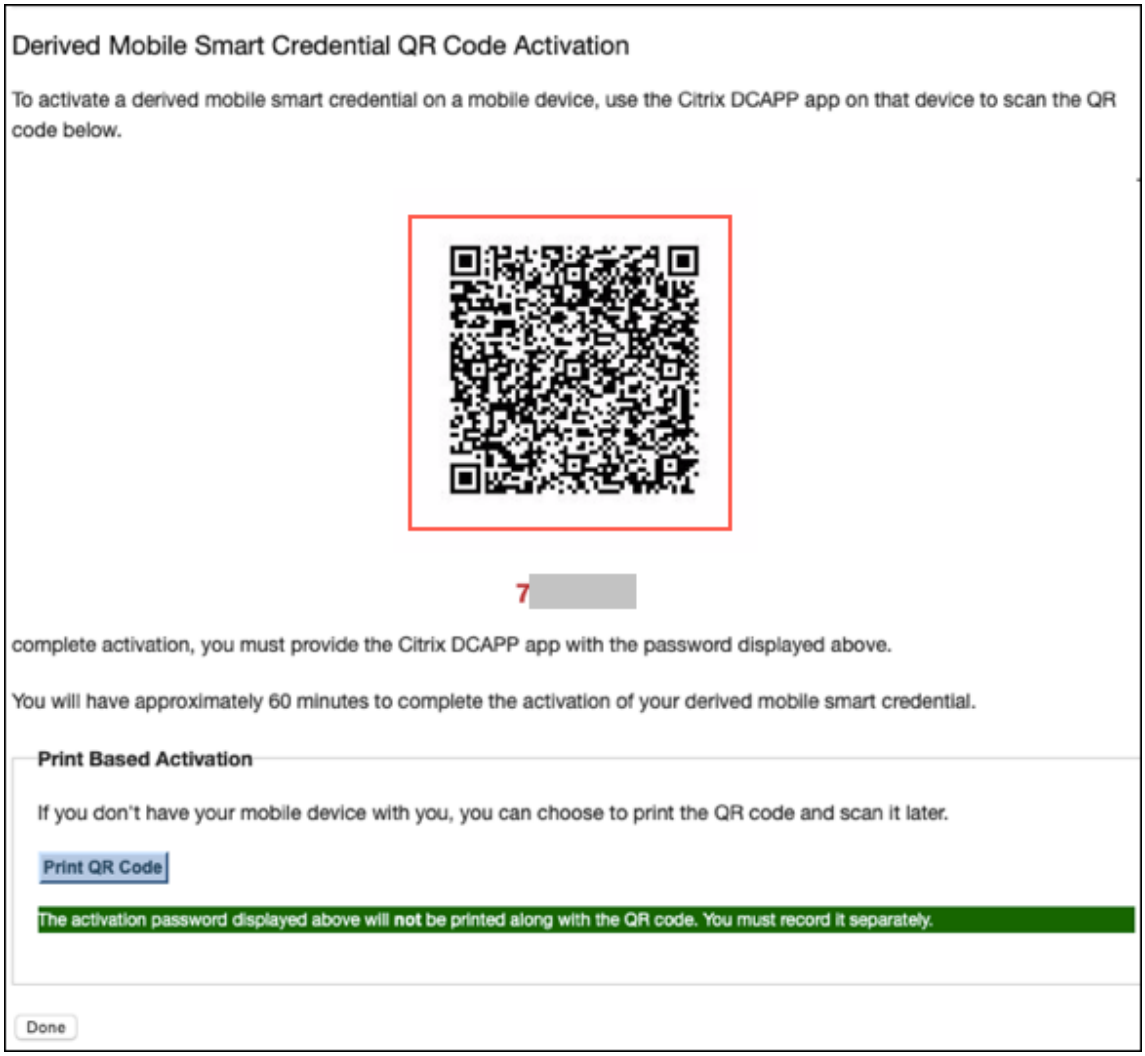
3. **Derived Mobile Smart Credential(**파생된모바일스마트자격증명**)** 화면에서 **Identity Name(ID** 이름**)** 을제공합니다. 사용자는사용자이름또는 ID 번호와같은고유이름을선택할수있습니다.
4. Derived credential app(파생된자격증명앱) 메뉴에서 **Citrix DCAPP** 를선택하고 **Ok(**확인**)** 를클릭합니다.



QR 코드활성화화면이나타나고모바일장치로코드를스캔하라는메시지가표시됩니다.

> 참고:
>
> 기본적으로파생된자격증명 QR 코드는 3 분후에만료됩니다.

5. 장치에서 **Derived Credential Manager** 앱을사용하여 QR 코드를스캔하고활성화를완료합니다.

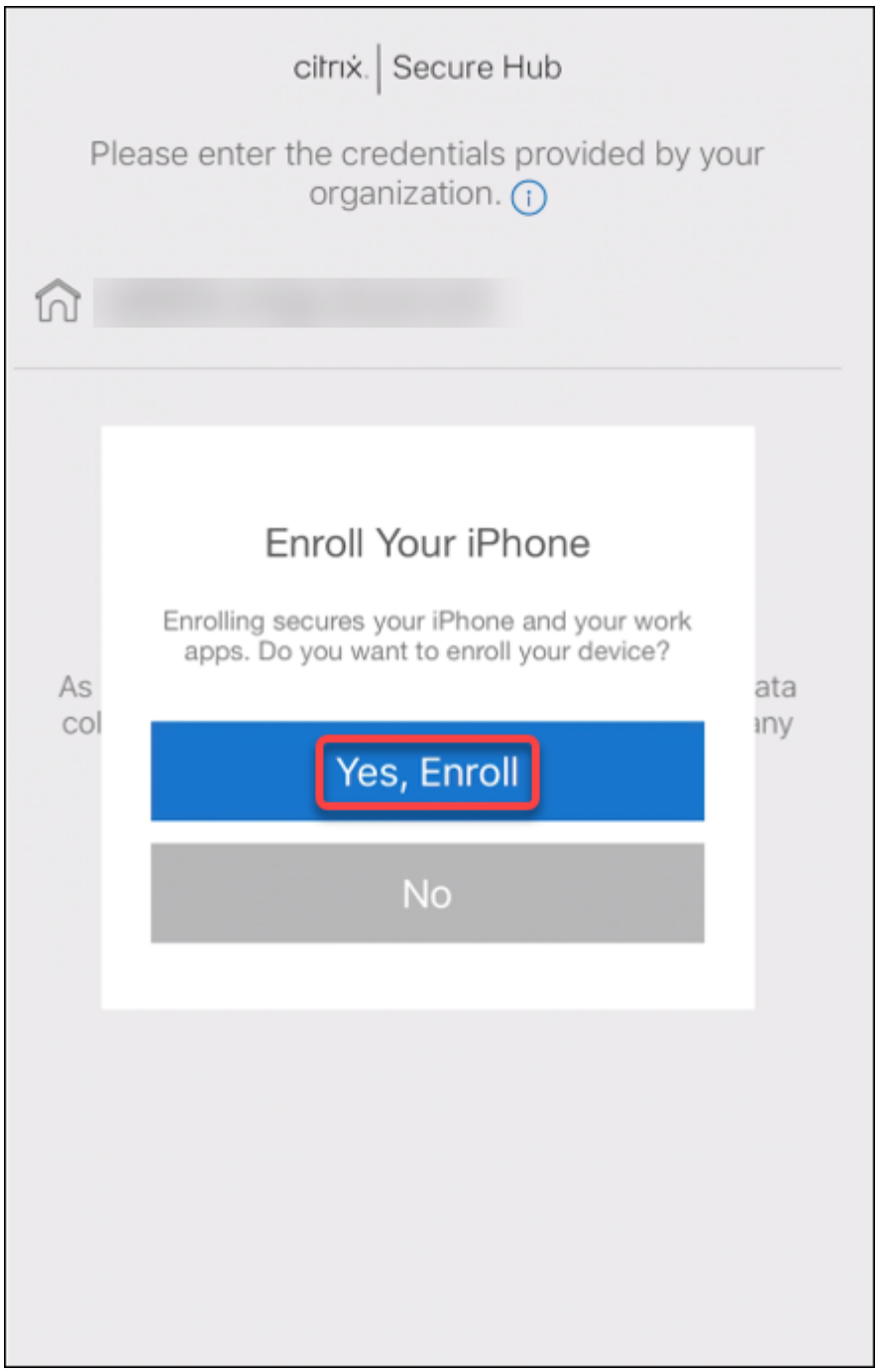


장치등록

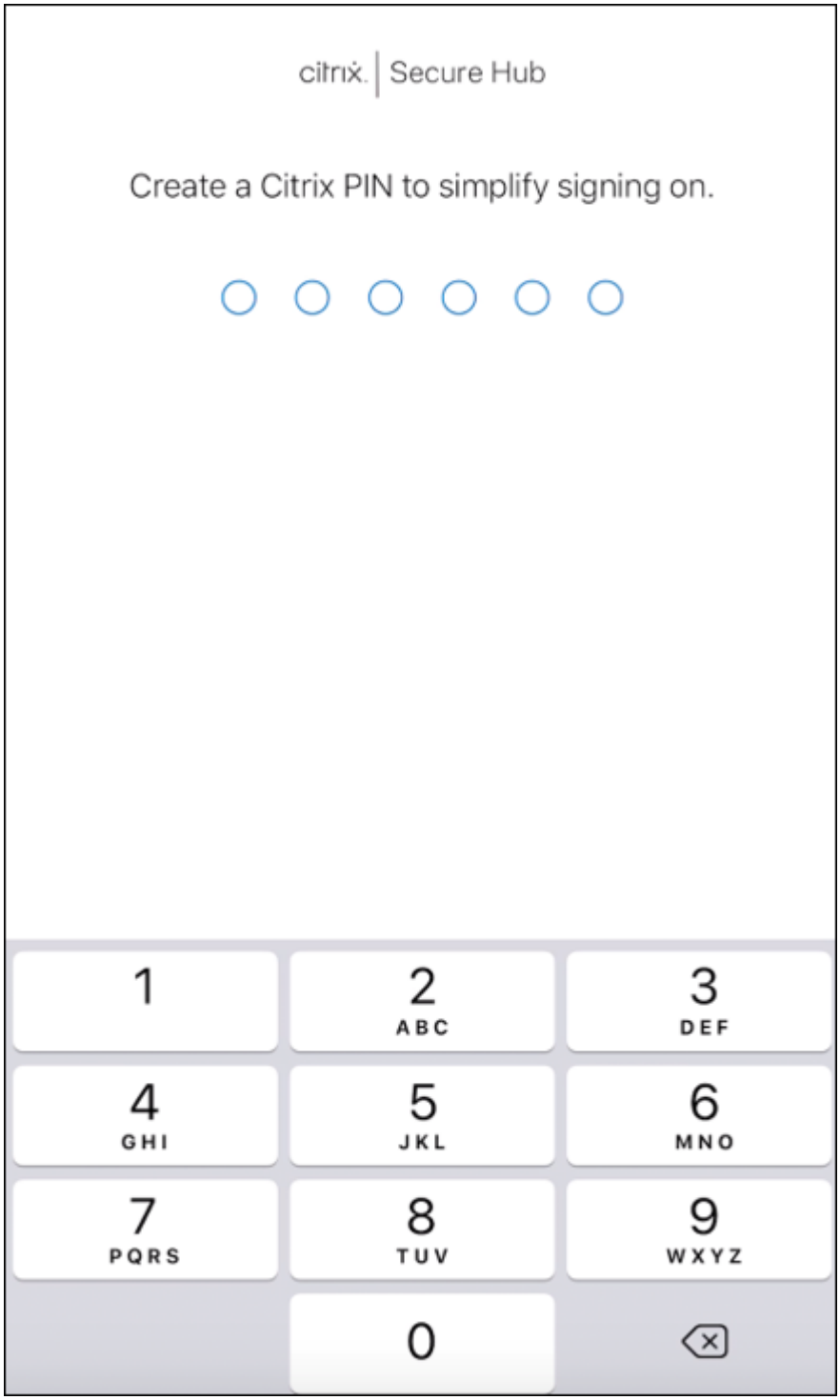
이문서의앞부분에설명된설정을완료하면사용자가파생된자격증명을사용하여장치를등록할수있습니다.

> 참고:
>
> 이섹션의스크린샷에는 Entrust Datacard 가예로사용되었습니다.

1. **Secure Hub** 를눌러서엽니다. 메시지가나타나면 XenMobile Server FQDN(정규화된도메인이름) 을입력하고 **Next(**다음**)** 를클릭합니다.
2. **Yes, Enroll(**예**.** 등록하겠습니다**)** 를클릭합니다. Secure Hub 에서장치등록이시작됩니다.

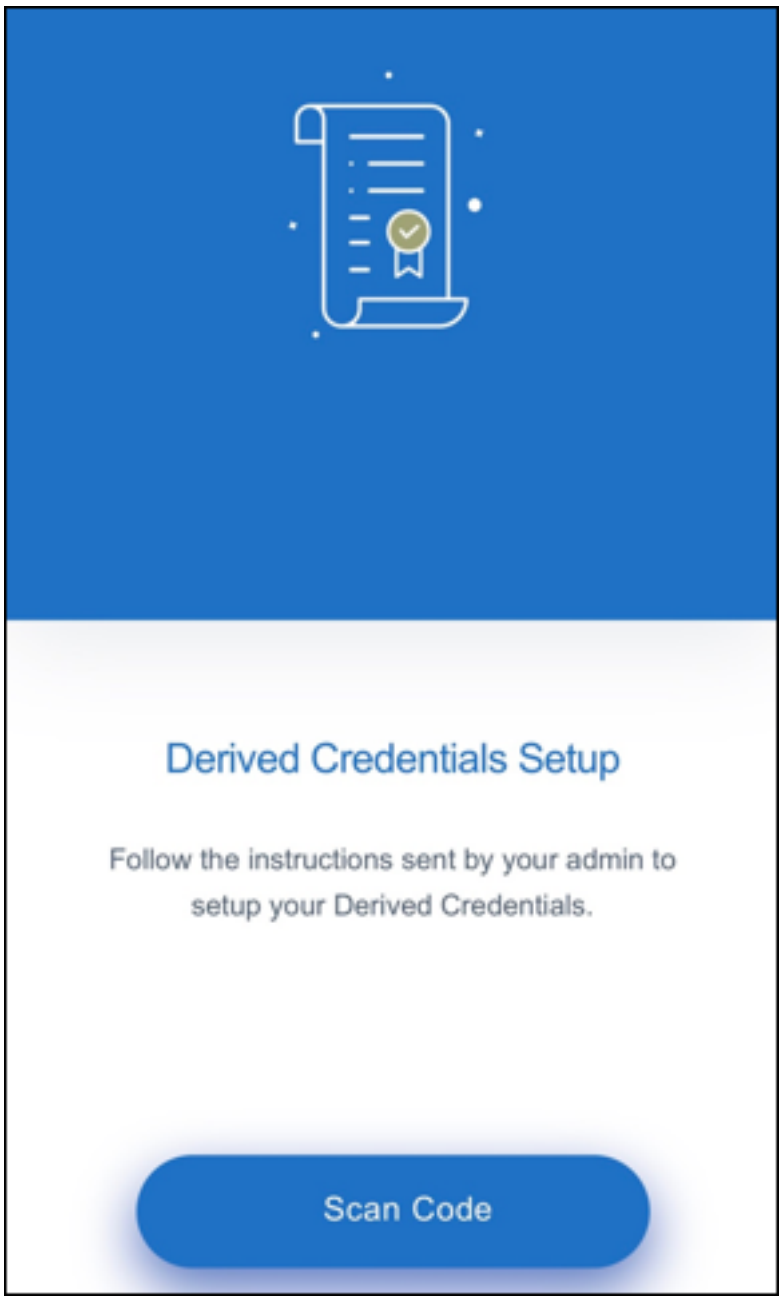


XenMobile Server 에서파생된자격증명을지원하는경우 Secure Hub 에사용자가 Citrix PIN 을생성하고확인하도록요청하는메시지가표시됩니다.



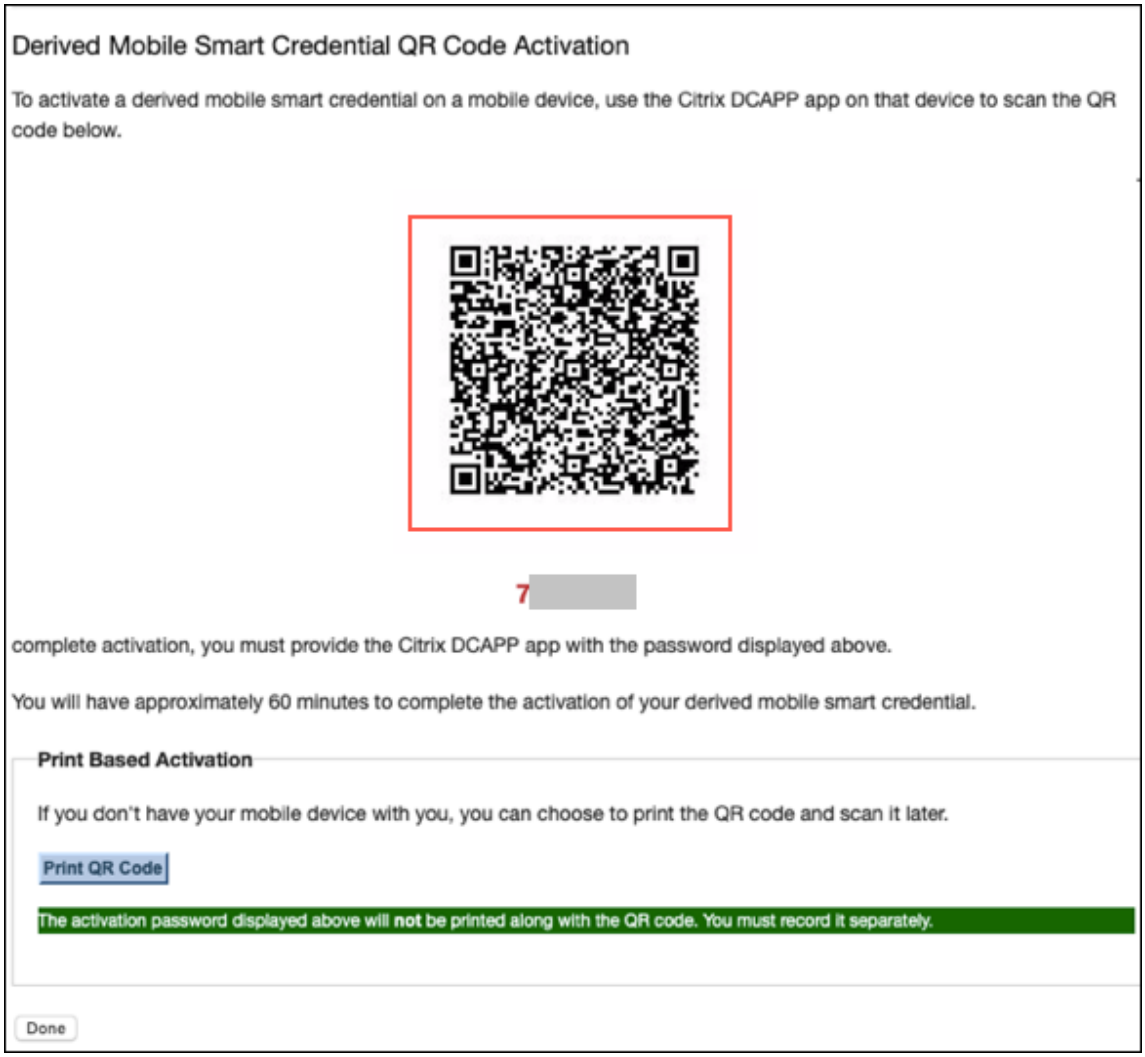
Citrix PIN 을확인하면파생된자격증명설정시작화면이나타납니다. 지침에따라스마트자격증명을활성화합니다.

3. **Scan code(**코드스캔**)** 를누릅니다. 휴대폰카메라가활성화됩니다.

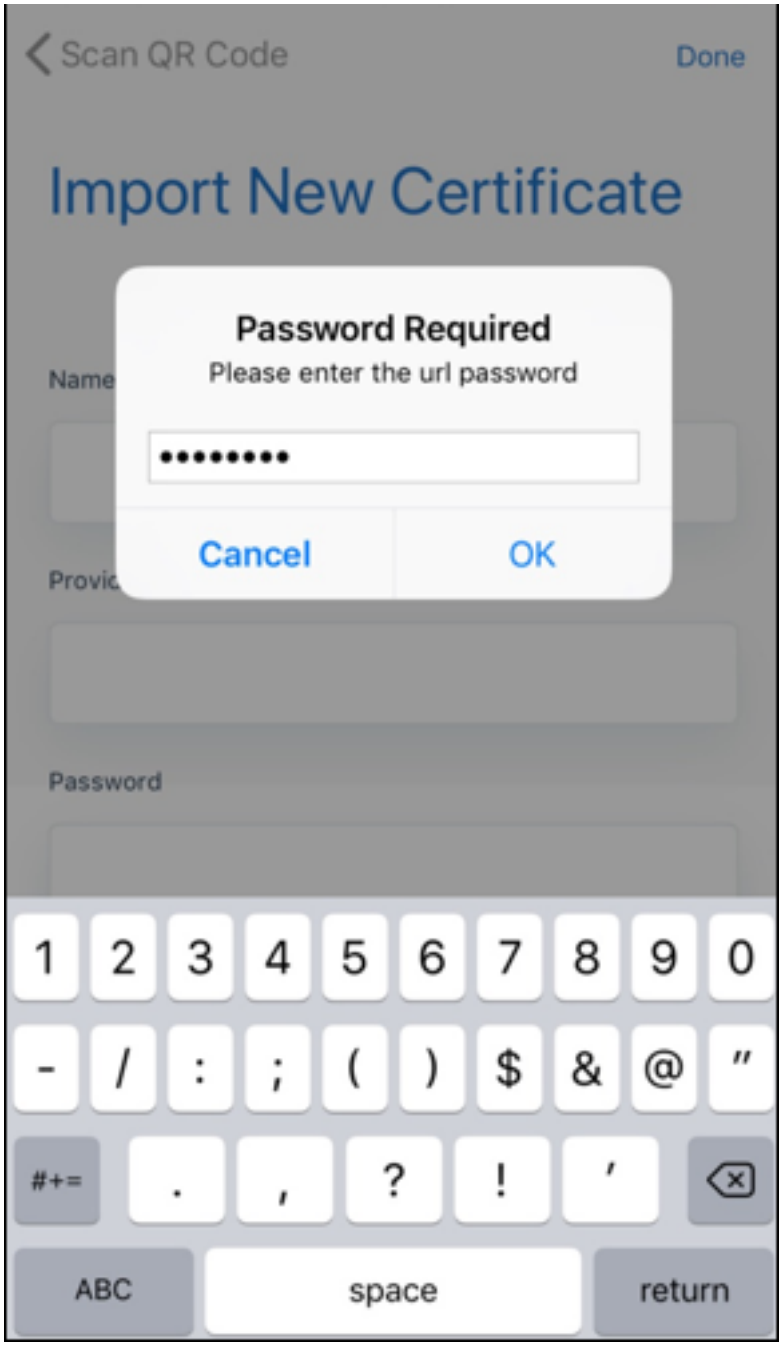


> 참고:
>
> QR 코드를스캔하려면카메라와마이크가사용되도록설정되었고필요한액세스권한이있는지확인하십시오.

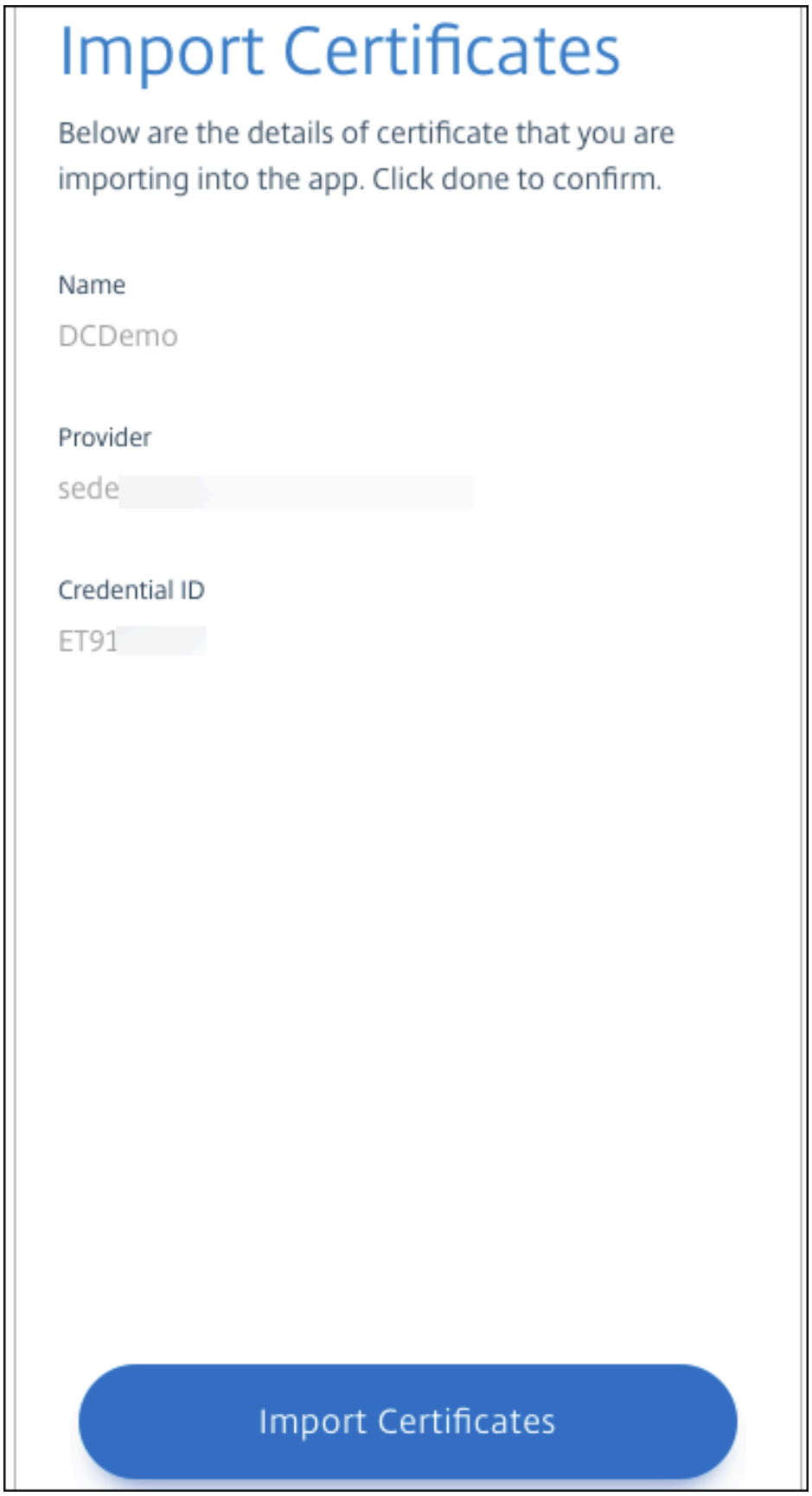
4. 파생자격증명앱에서이전단계에서만든 QR 코드를스캔합니다.



5. QR 코드를스캔한후 **Import New Certificate(**새인증서가져오기**)** 화면에서암호대화상자가나타나면암호를입력하고 **OK(**확인**)** 를클릭합니다.



Import New Certificate(새인증서가져오기**)** 화면이나타나고필드가자동으로채워집니다.



6. 인증서가성공적으로추가되면 **Derived Credentials(**파생된자격증명**)** 화면에서 **Continue to Secure Hub(Secure Hub** 로계속**)** 를클릭합니다.

7. Secure Hub 에서메시지가표시되면새 PIN 을입력합니다.

   PIN 인증후 Secure Hub 가인증서를다운로드합니다. 메시지에따라등록을완료합니다.

XenMobile 콘솔에서장치정보를보려면:

- 관리 > 장치로이동한다음명령상자를표시할장치를선택합니다. 자세히표시를클릭합니다.
- 분석 > 대시보드로이동합니다.

업그레이드

September 29, 2021

> 팁: **XenMobile Migration Service**
>
> XenMobile Server 를온-프레미스에서사용하는경우무료 XenMobile 마이그레이션서비스를사용하여 Endpoint Management 를시작할수있습니다. XenMobile Server 에서 Citrix Endpoint Management 로마이그레이션할때장치를재등록할필요는없습니다.
>
> 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 10.14 로업그레이드하기전에

1. 최신버전의 XenMobile Server 10.14 로업데이트하기전에 Citrix License Server 를 11.16 이상으로업데이트하십시오.

   최신버전의 XenMobile 에는 Citrix License Server 11.16(최소버전) 이필요합니다.

   XenMobile 10.14 의 Customer Success Services 날짜 (이전의 Subscription Advantage 날짜) 는 2021 년 9 월 15 일입니다. Citrix 라이센스의 Customer Success Services 날짜는이날짜보다이후여야합니다. 날짜는라이센스서버의라이센스옆에서볼수있습니다. 최신버전의 XenMobile 을이전버전의라이센스서버환경에연결하면연결확인이실패하고라이센스서버를구성할수없게됩니다.

   라이센스의날짜를갱신하려면 Citrix 포털에서최신라이센스파일을다운로드하고라이센스서버에파일을업로드하십시오. 자세한내용은 Customer Success Services를참조하십시오.

2. 클러스터된환경의경우: iOS 11 이상을실행하는장치에 iOS 정책및앱을배포하려면다음과같은요구사항이충족되어야합니다. Citrix Gateway 에 SSL 지속성이구성되어있으면모든 XenMobile Server 노드에서포트 80 을열어야합니다.

3. 업그레이드할 XenMobile Server 를실행하는가상컴퓨터의 RAM 이 8GB 미만인경우 8GB 이상으로 RAM 을늘리는것이좋습니다.

4. XenMobile 업데이트를설치하기전에 VM 의기능을사용하여시스템스냅샷을생성합니다. 또한시스템구성데이터베이스를백업합니다. 업그레이드도중문제가발생하는경우전체백업을사용하여복구할수있습니다.

업그레이드하려면

XenMobile 10.13.x 또는 10.12.x 에서직접 XenMobile 10.14 로업그레이드할수있습니다. 업그레이드를수행하려면사용가능한최신이진파일을다운로드합니다. https://www.citrix.com/downloads로이동하십시오. **Citrix Endpoint Management(XenMobile) > XenMobile Server >** 제품소프트웨어 **> XenMobile Server 10** 으로이동합니다. 해당하는하이퍼바이저에대한 XenMobile Server 소프트웨어타일에서 파일다운로드를클릭합니다. 업그레이드를업로드하려면 XenMobile 콘솔의 릴리스관리페이지를사용합니다.

릴리스관리페이지를사용하여업그레이드하려면

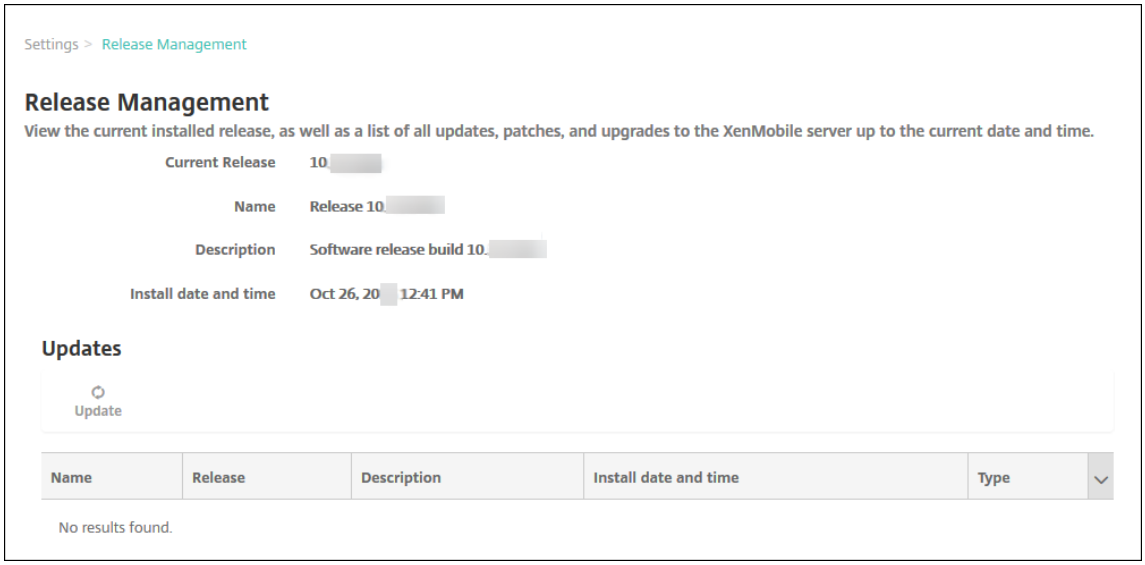
릴리스관리페이지를사용하여최신버전의 XenMobile Server 로업그레이드합니다.

사전요구사항:

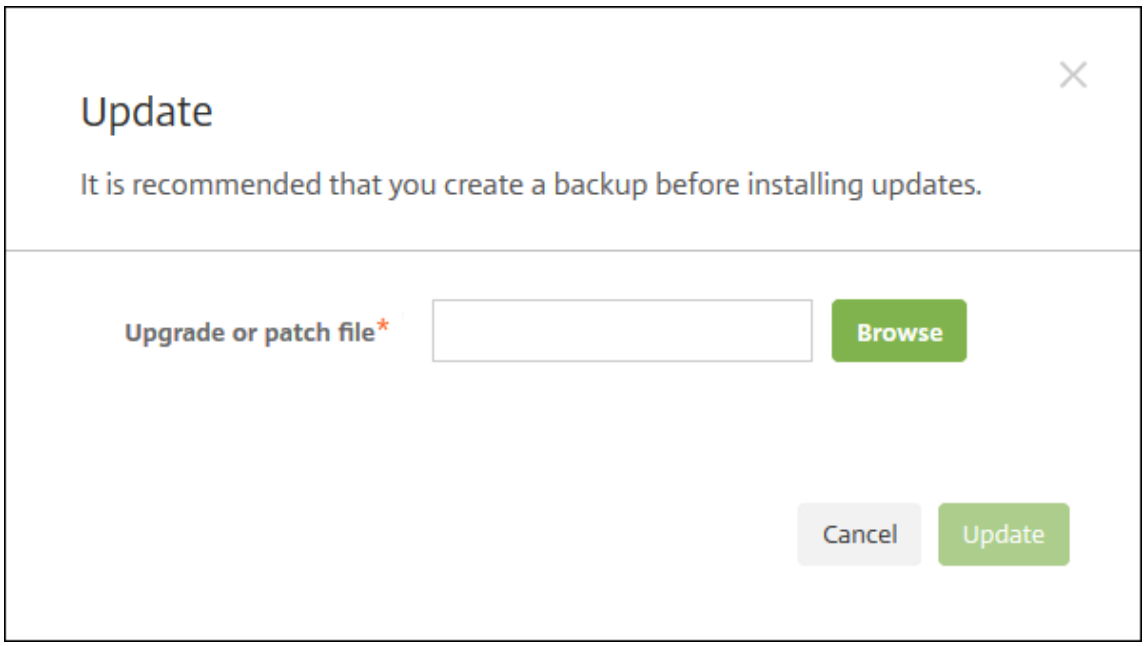
- 시스템요구사항을검토합니다.

클러스터링된배포의경우이문서의끝부분에나오는지침을참조하십시오.

1. 최신이진파일을다운로드합니다. https://www.citrix.com/downloads로이동하십시오. **Citrix Endpoint Management(및 Citrix XenMobile Server) > XenMobile Server(온-프레미스) >** 제품소프트웨어 **> XenMobile Server 10** 으로이동합니다. 해당하는하이퍼바이저에대한 XenMobile Server 소프트웨어타일에서 파일다운로드를클릭합니다.
2. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
3. 릴리스관리를클릭합니다. 릴리스관리페이지가나타납니다.



4. 업데이트아래에서 업데이트를클릭합니다. 업데이트대화상자가나타납니다.



5. 찾아보기를클릭하고파일위치로이동하여 Citrix.com 에서다운로드한 XenMobile 업그레이드파일을선택합니다.
6. 업데이트를클릭한후메시지가표시되면 XenMobile 을다시시작합니다.

   몇가지이유로업데이트를성공적으로완료할수없는경우문제를나타내는오류메시지가표시됩니다. 그런다음업데이트시도이전의상태로시스템이되돌려집니다.

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. 호스트이름유효성검사로인해배포가중단되는경우서버속성 **disable.hostname.verification** 을 **true** 로변경하십시오. 이속성의기본값은 **false** 입니다.

Citrix 는 XenMobile 의최신버전또는중요업데이트를 Citrix.com 에게시합니다. 또한각고객의기록된연락처로알림을전송합니다.

클러스터된 **XenMobile** 배포를업그레이드하려면

> 중요:
>
> XenMobile 업데이트를설치하기전에 VM(가상컴퓨터) 의기능을사용하여시스템스냅샷을생성합니다. 또한시스템구성데

> 이터베이스를백업합니다. 업그레이드도중문제가발생하는경우전체백업을사용하여복구할수있습니다.

시스템이클러스터모드로구성된경우다음단계에따라 XenMobile 10 릴리스의각노드를업데이트합니다.

1. 설정 **>** 릴리스관리에서모든노드에.bin 파일을업로드합니다.
2. CLI 의 시스템메뉴에서모든노드를종료합니다.
3. CLI 의 시스템메뉴에서노드하나를시작하고서비스가실행되는지확인합니다.
4. 다른노드를하나씩시작합니다.

   XenMobile 에서업데이트를성공적으로완료할수없는경우문제를나타내는오류메시지가표시됩니다. 그런다음 XenMobile 이업데이트시도이전의상태로시스템을되돌립니다.

XenMobile MDM Edition 에서 **Enterprise Edition** 으로업그레이드

XenMobile MDM Edition 을 iOS 및 Android 장치용 XenMobile Enterprise Edition 으로업그레이드할수있습니다.

사전요구사항

- 올바른 Enterprise 라이센스.
- Citrix Gateway 가구성되어있습니다.

업그레이드하려면

1. 설정 **>** 라이센스로이동하고올바른 Enterprise Edition 라이센스유형이업로드되었는지확인합니다.
2. 설정 **>** 서버속성으로이동하고 서버모드속성을 **MDM** 에서 **ENT** 로변경합니다.
3. 설정 **> Citrix Gateway** 로이동하고 Citrix Gateway 세부정보를구성합니다. 인증모드를 MDM Edition 과동일한모드, 즉도메인인증 (Active Directory) 으로설정합니다. XenMobile 은사용자등록후의인증모드변경을지원하지않습니다.
4. 선택사항: 설정 **>** 클라이언트속성으로이동하고 Citrix PIN 인증을사용하도록설정합니다.

이단계를완료한후에는사용자가다음단계를수행하여장치를엔터프라이즈모드로전환해야합니다.

iOS 사용자

1. Secure Hub 닫기: 장치홈단추를빠르게두번누르고 Secure Hub 앱을위로밉니다.
2. Secure Hub 를엽니다.

Android 사용자

1. Secure Hub 를엽니다.
2. 기본설정 **>** 장치정보로이동합니다.
3. 정책새로고침을클릭합니다.

Citrix PIN 인증을사용하도록설정한경우 Secure Hub 가 PIN 을만들라는메시지를사용자에게표시합니다. 사용자가 PIN 을생성하면 XenMobile 이장치를엔터프라이즈모드로구성합니다. 그러면 XenMobile 콘솔의 관리 **>** 장치페이지에 MDM 과 MAM 이장치의활성모드로표시됩니다.

사용자계정, 역할및등록

September 29, 2021

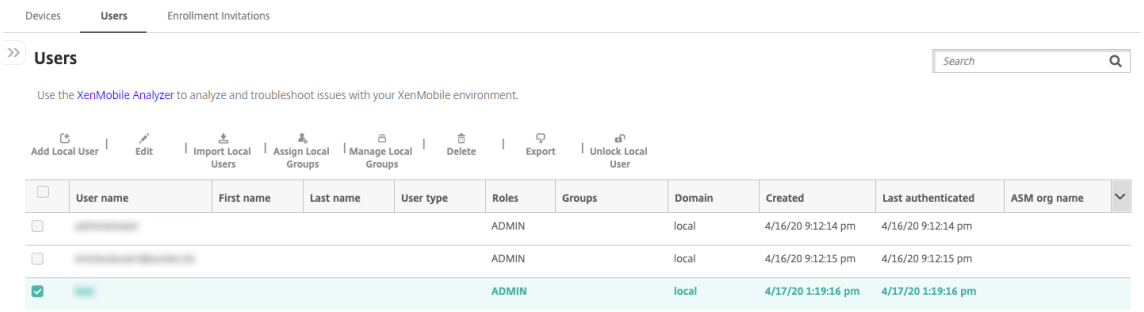
XenMobile 콘솔의 관리탭및 설정페이지에서사용자계정, 역할및등록을구성합니다. 별도로지정되지않는한, 다음작업에대한단계는이문서에서제공됩니다.

- 사용자계정및그룹:
  - 관리 **>** 사용자에서수동으로사용자계정을추가하거나.csv 프로비저닝파일을사용하여계정을가져오고로컬그룹을관리합니다.
  - 설정 **>** 워크플로에서워크플로를사용하여사용자계정의생성및제거를관리합니다.
- 사용자계정및그룹의역할
  - 설정 **>** 역할기반액세스제어에서미리정의된역할또는권한집합을사용자및그룹에할당합니다. 이러한권한은시스템기능에대한사용자액세스수준을제어합니다. 자세한내용은 RBAC 를사용하여역할구성을참조하십시오.
  - 설정 **>** 알림템플릿에서자동화동작, 등록및사용자에게보내는표준알림메시지에사용할알림템플릿을만들거나업데이트합니다. 세가지채널 (Secure Hub, SMTP 또는 SMS) 을통해메시지를보내는알림템플릿을구성합니다. 자세한내용은 알림템플릿만들기및업데이트를참조하십시오.
- 등록보안모드및초대
  - 설정 **>** 등록에서최대 7 개등록보안모드를구성하고등록초대를보냅니다. 각등록보안모드별로사용자가장치를등록할때수행해야하는보안수준과단계가다릅니다.
  - XenMobile 에서사용자등록에 AutoDiscovery 사용

로컬사용자계정을추가, 편집, 잠금해제또는삭제하려면

로컬사용자계정을 XenMobile 에수동으로추가하거나프로비저닝파일을사용하여계정을가져올수있습니다. 프로비저닝파일에서사용자계정을가져오는단계는사용자계정가져오기를참조하십시오.

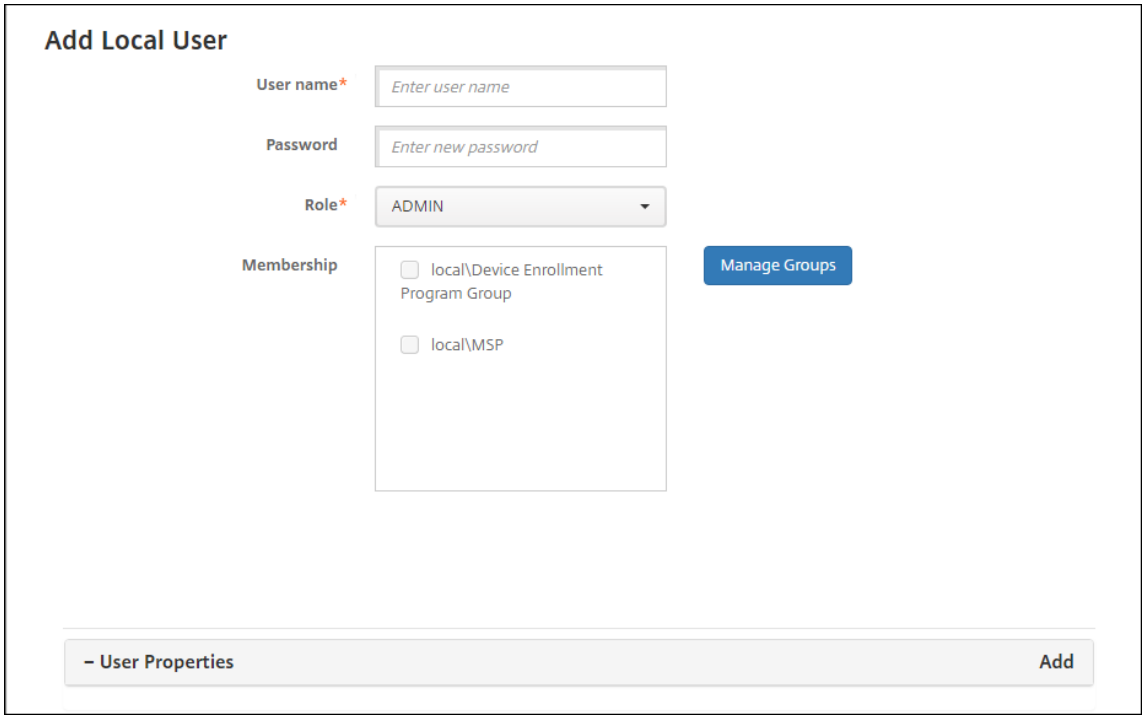
1. XenMobile 콘솔에서 관리 **>** 사용자를클릭합니다. 사용자페이지가나타납니다.



2. 필터표시를클릭하여목록을필터링합니다.

로컬사용자계정을추가하려면

1. 사용자페이지에서 로컬사용자추가를클릭합니다. 로컬사용자추가페이지가나타납니다.



2. 다음설정을구성합니다.

- 사용자이름**:** 이름을입력합니다. 필수필드입니다. 이름에공백과대/소문자를포함할수있습니다.
- 암호**:** 선택적사용자암호를입력합니다. 암호는 14 자이상이어야하며다음기준을모두충족해야합니다.
  - 숫자 2 개이상포함
  - 대문자와소문자각각 1 개이상포함
  - 특수문자 1 개이상포함
  - 사전에등재된단어나, Citrix 사용자이름또는전자메일주소와같이제한된단어를포함하지마십시오.
  - 1111, 1234, asdf 와같이 3 개이상이어지거나반복되는문자또는키보드패턴을포함하지마십시오.
- 역할**:** 목록에서사용자역할을클릭합니다. 역할에대한자세한내용은 RBAC 를사용하여역할구성을참조하십시오. 사용가능한옵션은다음과같습니다.
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- 구성원자격**:** 목록에서사용자를추가할그룹을클릭합니다.
- 사용자속성**:** 선택적사용자속성을추가합니다. 추가할각사용자속성에대해 추가를클릭하고다음을수행합니다.
  - 사용자속성**:** 목록에서속성을클릭하고속성옆의필드에사용자속성특성을입력합니다.

- 완료를클릭하여사용자속성을저장하거나 취소를클릭합니다.

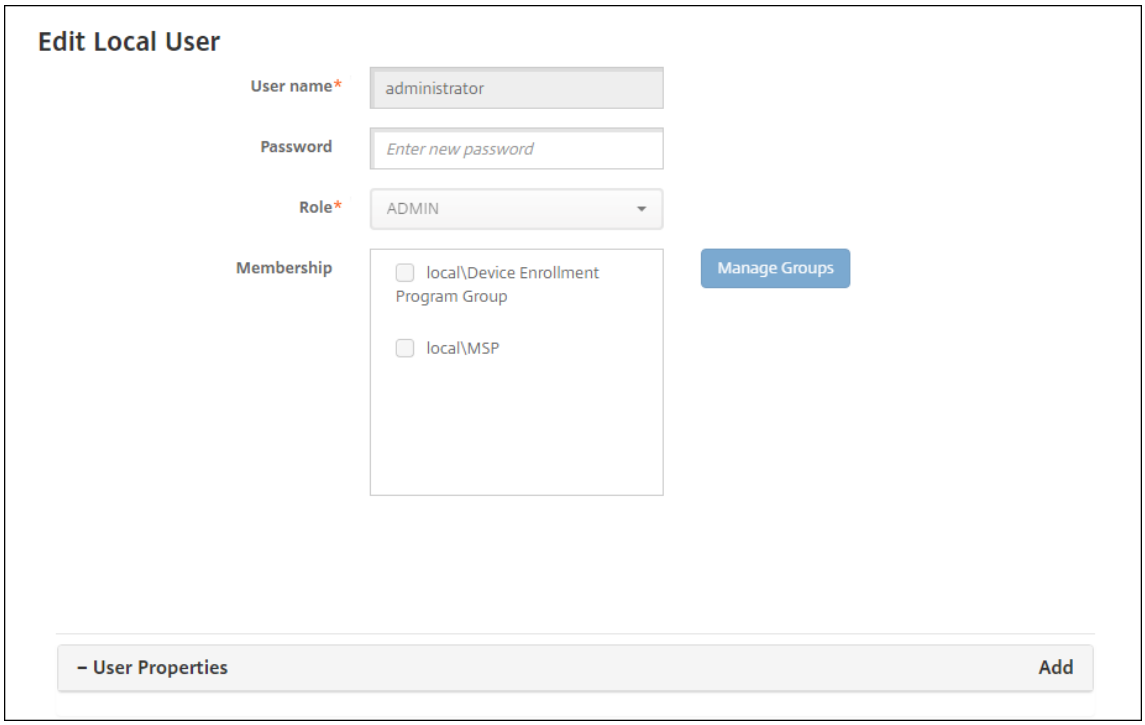
기존사용자속성을삭제하려면속성이포함된줄위로마우스포인터를이동하고오른쪽의 X 아이콘을클릭합니다. 속성이즉시 삭제됩니다.

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.

로컬사용자계정을잠금해제하려면

1. 사용자페이지의사용자목록에서사용자계정을클릭하여선택합니다.
2. 로컬사용자잠금해제를클릭합니다. 확인대화상자가나타납니다.
3. 잠금해제를클릭하여사용자계정을잠금해제하거나 취소를클릭하여사용자를변경하지않은상태로둡니다.

로컬사용자계정을삭제하려면

1. 사용자페이지의사용자목록에서사용자계정을클릭하여선택합니다.

각사용자계정옆의확인란을선택하여둘이상의사용자계정을선택하고삭제할수있습니다.

1. 삭제를클릭합니다. 확인대화상자가나타납니다.
2. 삭제를클릭하여사용자계정을삭제하거나 취소를클릭합니다.

Active Directory 사용자삭제

한번에한명이상의 Active Directory 사용자를삭제하려면사용자를선택하고 삭제를클릭합니다.

장치가등록되어있는사용자를삭제한후해당장치를재등록하려면재등록하기전에해당장치를삭제하십시오. 장치를삭제하려면 관리 **>** 장치에서장치를선택한다음 삭제를클릭합니다.

사용자계정가져오기

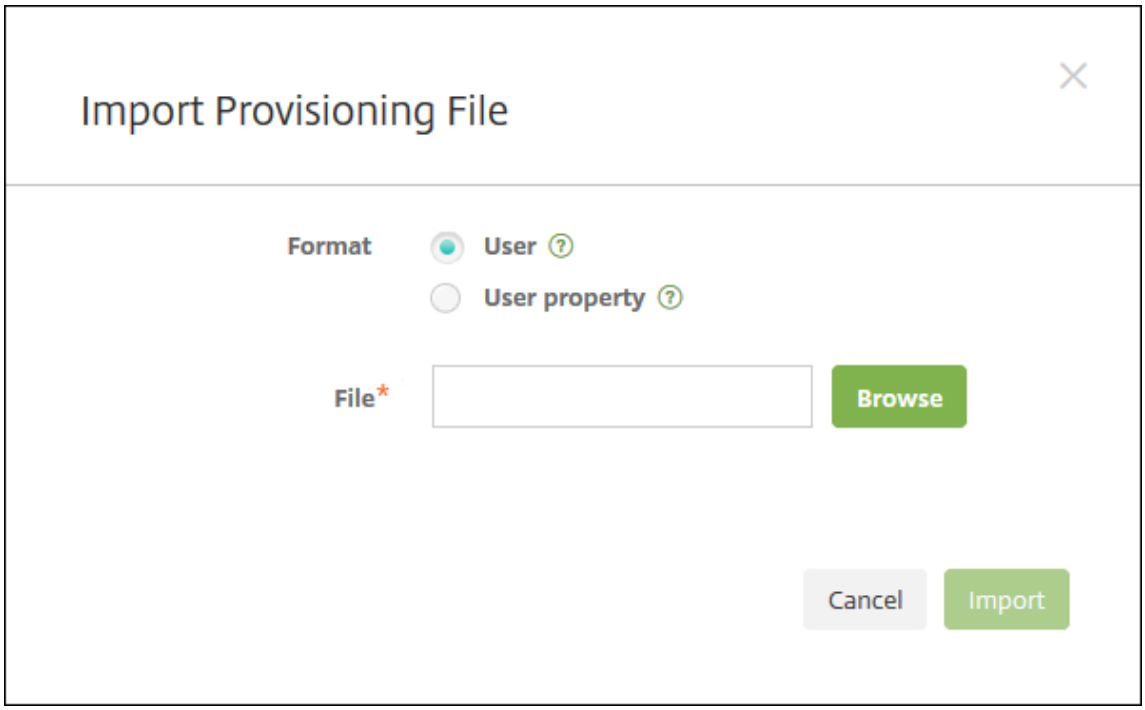
프로비저닝파일이라고하는.csv 파일을수동으로만들어로컬사용자계정및속성을가져올수있습니다. 프로비저닝파일형식에대한자세한내용은프로비저닝파일형식을참조하십시오.

> 참고**:**
>
> - 로컬사용자의경우가져오기파일에사용자이름과함께도메인이름을사용합니다. 예를들어 username@domain 을지정합니다. 만들거나가져오는로컬사용자가 XenMobile 에서관리되는도메인에대한사용자인경우해당사용자는해당하는 LDAP 자격증명을사용하여등록할수없습니다.
> - XenMobile 내부사용자디렉터리로사용자계정을가져오는경우기본도메인을사용하지않으면가져오기프로세스속도가빨라집니다. 도메인을사용하지않도록설정하면등록에영향을미치므로내부사용자가져오기가완료된후기본도메인을다시사용하도록설정합니다.
> - 로컬사용자는 UPN(사용자계정이름) 형식을사용할수있습니다. 그러나관리되는도메인은사용하지않는것이좋습니다. 예를들어 example.com 이관리되는경우이 UPN 형식 (user@example.com) 으로로컬사용자를만들지

> 마십시오.

프로비저닝파일을준비한후다음단계에따라 XenMobile 로파일을가져옵니다.

1. XenMobile 콘솔에서 관리 **>** 사용자를클릭합니다. 사용자페이지가나타납니다.
2. 로컬사용자가져오기를클릭합니다. 프로비저닝파일가져오기대화상자가나타납니다.



3. 가져오는프로비저닝파일의형식으로 사용자또는 속성을선택합니다.
4. 찾아보기를클릭하고파일위치로이동하여사용할프로비저닝파일을선택합니다.
5. 가져오기를클릭합니다.

프로비저닝파일형식

프로비저닝파일을수동으로만들어서사용자계정과속성을 XenMobile 로가져올수있습니다. 유효한형식은다음과같습니다.

- 사용자프로비저닝파일필드**:** `user;password;role;group1;group2`
- 사용자특성프로비저닝파일필드**:** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> 참고**:**
>
> - 프로비저닝파일내의필드는세미콜론 (;) 으로구분합니다. 필드자체에세미콜론이포함되는경우백슬래시문자 (\) 로이스케이프처리합니다. 예를들어 `propertyV;test;1;2` 속성을프로비저닝파일에 `propertyV\\;test\\;1\\;2`로입력합니다.
> - 역할의유효한값은미리정의된 USER, ADMIN, SUPPORT 및 DEVICE_PROVISIONING 과정의된다른역할입니다.

> - 그룹계층을만들때는마침표문자 (.) 를구분기호로사용합니다. 그룹이름에는마침표를사용하지마십시오.
> - 특성프로비저닝파일의속성특성에는소문자를사용합니다. 데이터베이스는대/소문자를구분합니다.

사용자프로비저닝콘텐츠의예

`user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` 항목은다음을의미합니다.

- 사용자**:** `user01`
- 암호**:** `pwd;01`
- 역할**:** `USER`
- 그룹**:**
  - `myGroup.users01`
  - `myGroup.users02`
  - `myGroup.users.users01`

또다른예로 `AUser0;1.password;USER;ActiveDirectory.test.net`은다음을의미합니다.

- 사용자**:** `AUser0`
- 암호**:** `1.password`
- 역할**:** `USER`
- 그룹**:** `ActiveDirectory.test.net`

사용자특성프로비저닝콘텐츠의예

`user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` 항목은다음을의미합니다.

- 사용자**:** `user01`
- 속성 **1**
  - 이름**:** `propertyN`
  - 값**:** `propertyV;test;1;2`
- 속성 **2:**
  - 이름**:** `prop 2`
  - 값**:** `prop2 value`

등록보안모드구성

XenMobile 에서장치등록보안모드를구성하여장치등록을위한보안수준과알림템플릿을지정합니다.

XenMobile 은사용자가장치를등록할때수행해야하는보안수준과단계가다른 7 가지등록보안모드를제공합니다. XenMobile Server 콘솔의 설정 **>** 등록페이지에서등록보안모드를구성할수있습니다.

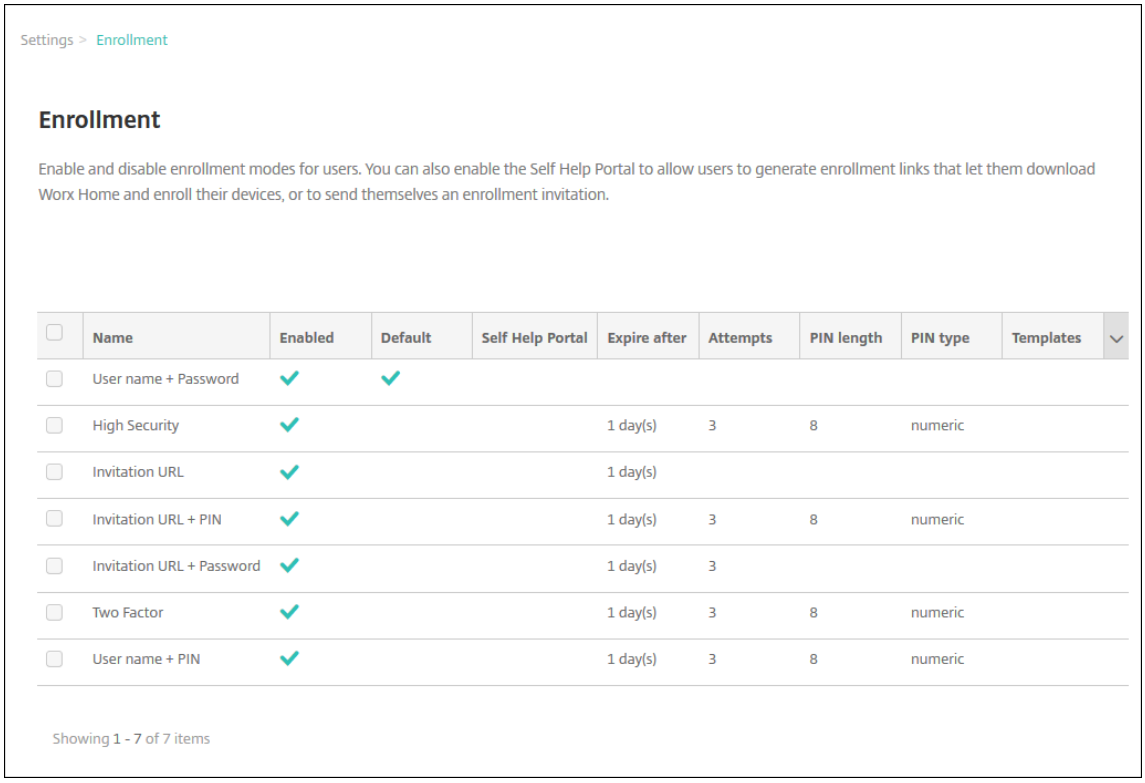
일부모드는자가지원포털에서사용할수있도록제공할수있습니다. 사용자는포털에서장치를등록하는데사용하는등록링크를생성합니다. iOS, iPadOS, macOS, Android Enterprise 및레거시 Android 사용자는포털에서본인에게등록초대를보내도록선택할수있습니다. Windows 장치에서는등록초대를사용할수없습니다.

등록초대는 관리 > 등록초대페이지에서보낼수있습니다. 자세한내용은 등록초대보내기를참조하십시오.

> 참고:
>
> 사용자지정알림템플릿을사용하려는경우등록모드를구성하기전에템플릿을설정해야합니다. 알림템플릿에대한자세한내용은 알림템플릿만들기또는업데이트를참조하십시오.

1. XenMobile 콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 등록을클릭합니다. 사용가능한모든등록보안모드테이블이포함된 등록페이지가나타납니다. 기본적으로모든등록보안모드가사용됩니다.
3. 목록에서등록보안모드를선택하여편집합니다. 그런다음모드를기본값으로설정하거나모드를사용하지않도록설정하거나자가지원포털을통한사용자액세스를허용합니다.

   > 참고:
   >
   > 등록보안모드옆의확인란을선택하면등록보안모드목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.



   다음등록보안모드중에서선택합니다.

   - 사용자이름 + 암호
   - 높은수준의보안
   - 초대 URL
   - 초대 URL + PIN
   - 초대 URL + 암호

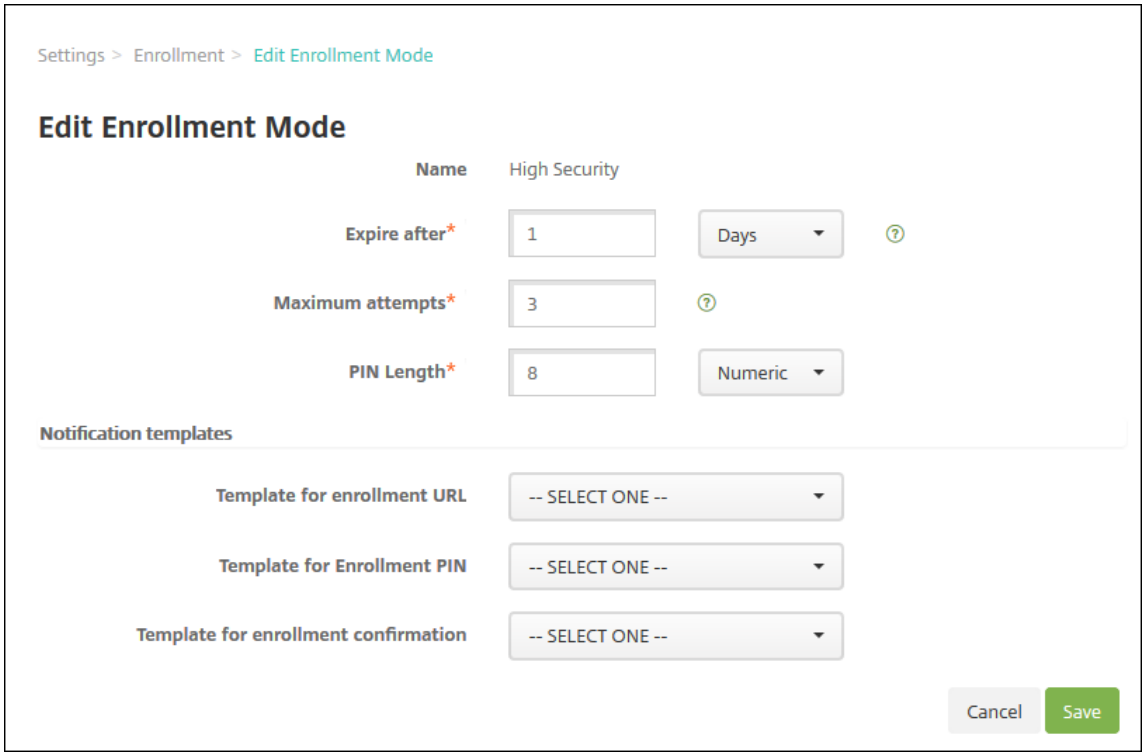
- 2 단계인증
- 사용자이름 + PIN

등록초대를사용하여초대를받은사용자로등록을제한할수있습니다. 등록초대를보내기위해서는 초대 **URL**, 초대 **URL + PIN** 또는 초대 **URL +** 암호등록보안모드만사용할수있습니다. 사용자이름 **+** 암호, **2** 단계인증또는 사용자이름 **+ PIN** 으로등록하는장치의경우사용자는 Secure Hub 에서자격증명을수동으로입력해야합니다.

OTP(일회용 PIN) 등록초대를 2 단계인증솔루션으로사용할수있습니다. OTP 등록초대는사용자가등록할수있는장치의 수를제어합니다. Windows 장치에서는 OTP 초대를사용할수없습니다.

등록보안모드를편집하려면

1. 등록목록에서등록보안모드를선택한후 편집을클릭합니다. 등록모드편집페이지가나타납니다. 선택한모드에따라표시되는옵션이결정됩니다.



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 에사용할템플릿을클릭합니다. 예를들어등록초대템플릿은사용자에게전자메일또는 SMS 를보냅니다. 방법은사용자가 XenMobile 에장치를등록할때사용할수있는템플릿의구성방법에따라다릅니다. 알림템플릿에대한자세한내용은 알림템플릿만들기또는업데이트를참조하십시오.
  - 등록 **PIN** 용템플릿**:** 목록에서등록 PIN 에사용할템플릿을클릭합니다.
  - 등록확인용템플릿**:** 목록에서사용자가성공적으로등록되었음을알릴때사용할템플릿을클릭합니다.

3. 저장을클릭합니다.

등록보안모드를기본값으로설정하려면

등록보안모드를기본값으로설정하면다른등록보안모드를선택하지않는한모든장치등록요청에해당모드가사용됩니다. 기본값으로설정된등록보안모드가없는경우장치를등록할때마다등록요청을만들어야합니다.

> 참고**:**
>
> 사용자이름 **+** 암호**, 2** 단계또는 사용자이름 **+ PIN** 등록보안모드만기본값으로사용할수있습니다.

1. 사용자이름 **+** 암호**, 2** 단계또는 사용자이름 **+ PIN** 중에서기본등록보안모드를선택합니다.

   모드를기본값으로사용하려면먼저사용하도록설정해야합니다.

2. 기본값을클릭합니다. 이제선택한모드가기본값입니다. 이전에기본값으로설정된다른등록보안모드는더이상기본값이아닙니다.

등록보안모드를사용하지않도록설정하려면

등록보안모드를사용하지않도록설정하면그룹등록초대와자가지원포털에서등록모드를사용할수없게됩니다. 한등록보안모드를사용하지않도록설정하고다른등록보안모드를사용하도록설정하여사용자가장치를등록하는방법을변경할수있습니다.

1. 등록보안모드를선택합니다.

   기본등록보안모드는사용하지않도록설정할수없습니다. 기본등록보안모드를사용하지않도록설정하려면먼저기본값상태를제거해야합니다.

2. **Disable** 을클릭합니다. 등록보안모드가더이상사용되지않습니다.

자가지원포털에서등록보안모드를사용하도록설정하려면

자가지원포털에서등록보안모드를사용하도록설정하면사용자가개별적으로 XenMobile 에장치를등록할수있습니다.

> 참고:
>
> - 등록보안모드를자가지원포털에서사용할수있으려면등록모드를사용하도록설정하고알림템플릿에연결해야합니다.
> - 자가지원포털에는한번에하나의등록보안모드만사용하도록설정할수있습니다.

1. 등록보안모드를선택합니다.
2. 자가지원포털을클릭합니다. 이제사용자가자가지원포털에서선택한등록보안모드를사용할수있습니다. 자가지원포털에사용하도록설정된다른모드는더이상사용자에게제공되지않습니다.

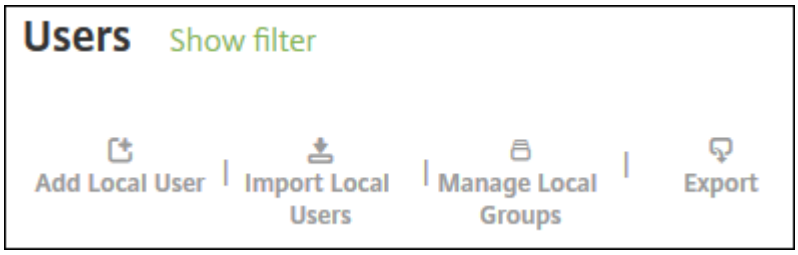
그룹추가또는제거

XenMobile 콘솔에서 사용자, 로컬사용자추가, 로컬사용자편집페이지의 그룹관리대화상자에서그룹을관리할수있습니다. 그룹편집명령은없습니다.

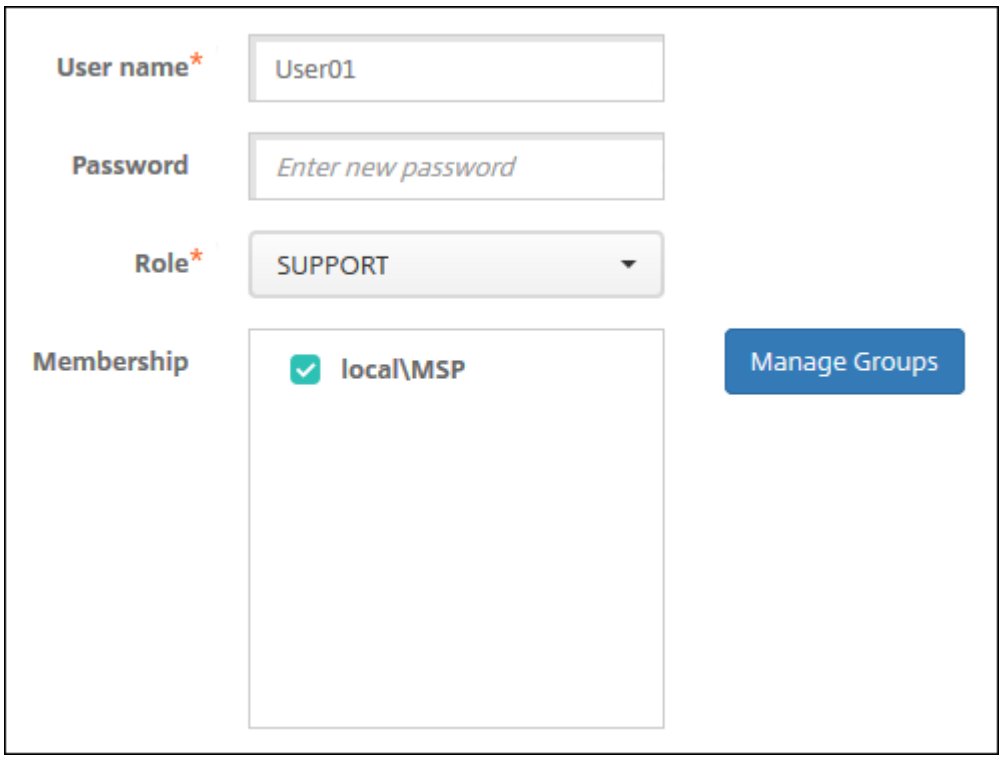
그룹을제거하는경우그룹제거가사용자계정에영향을주지않는다는점을기억하십시오. 그룹을제거하면해당그룹에대한사용자연결만제거됩니다. 또한사용자가해당그룹에연결된배달그룹에서제공하는앱또는프로필에액세스할수없게됩니다. 그러나다른모든그룹연결은그대로유지됩니다. 다른로컬그룹에연결되지않은사용자는상위수준에연결됩니다.

로컬그룹을추가하려면

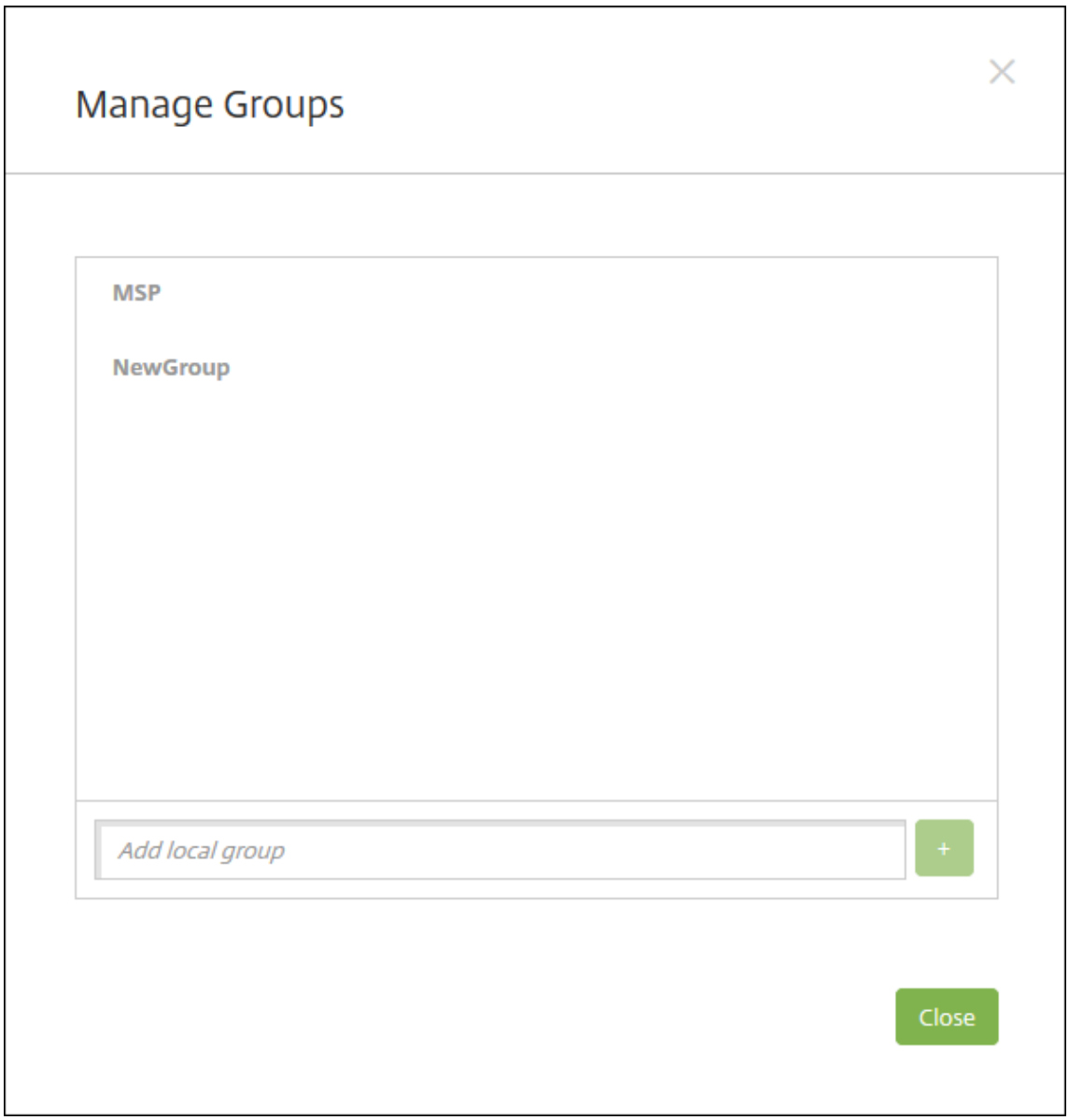
1. 다음중하나를수행합니다.
   - 사용자페이지에서 로컬그룹관리를클릭합니다.



   - 로컬사용자추가페이지또는 로컬사용자편집페이지에서 그룹관리를클릭합니다.



그룹관리대화상자가나타납니다.



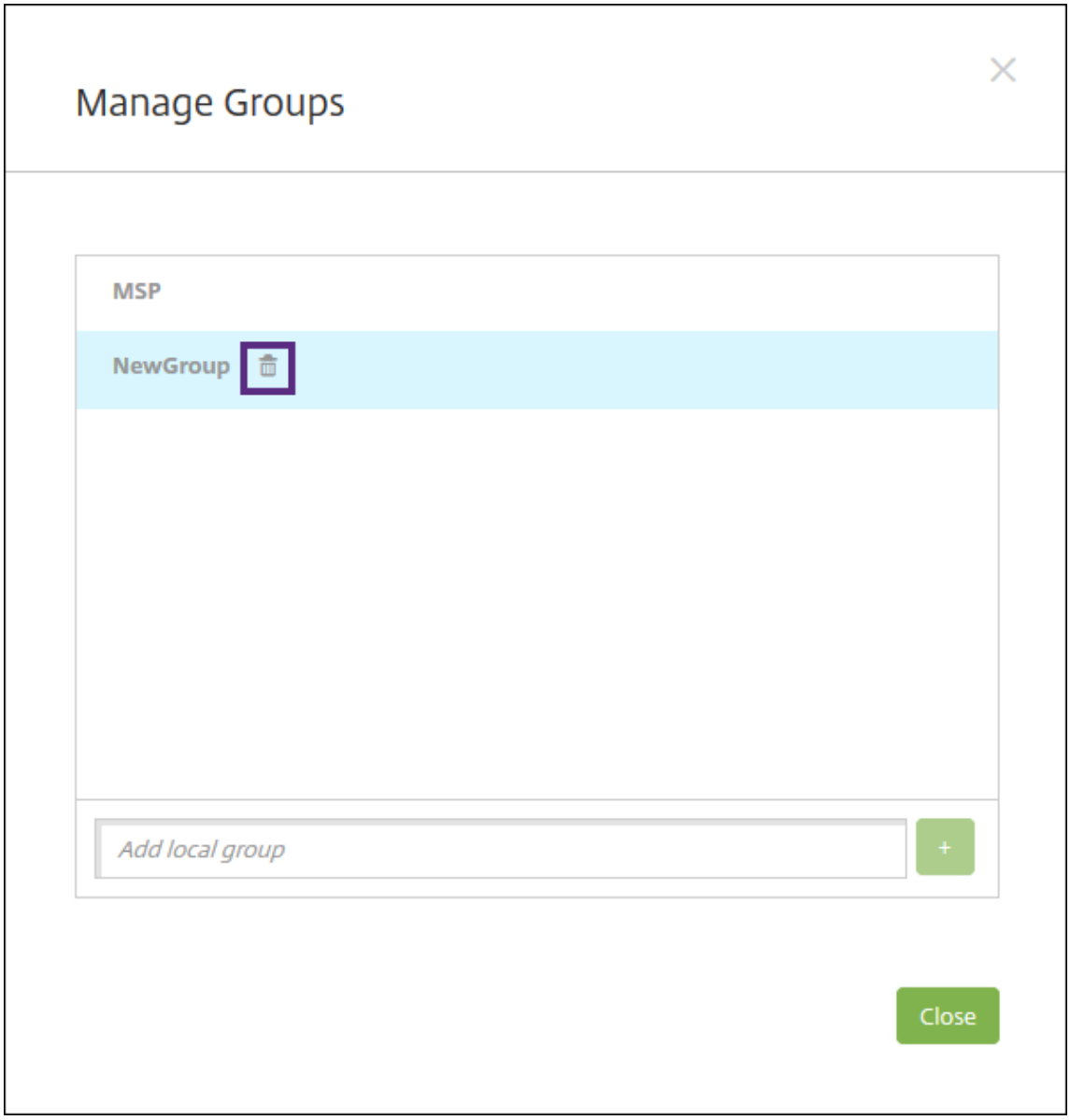
2. 그룹목록아래에새그룹이름을입력한후더하기기호 (**+**) 를클릭합니다. 사용자그룹이목록에추가됩니다.
3. **Close(**닫기**)** 를클릭합니다.

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. 워크플로를사용하려면먼저조직에서사용자계정요청을승인할권한이있는담당자를식별합니다. 그런다음워크플로템플릿을사용하여사용자계정요청을만들고승인할수있습니다.

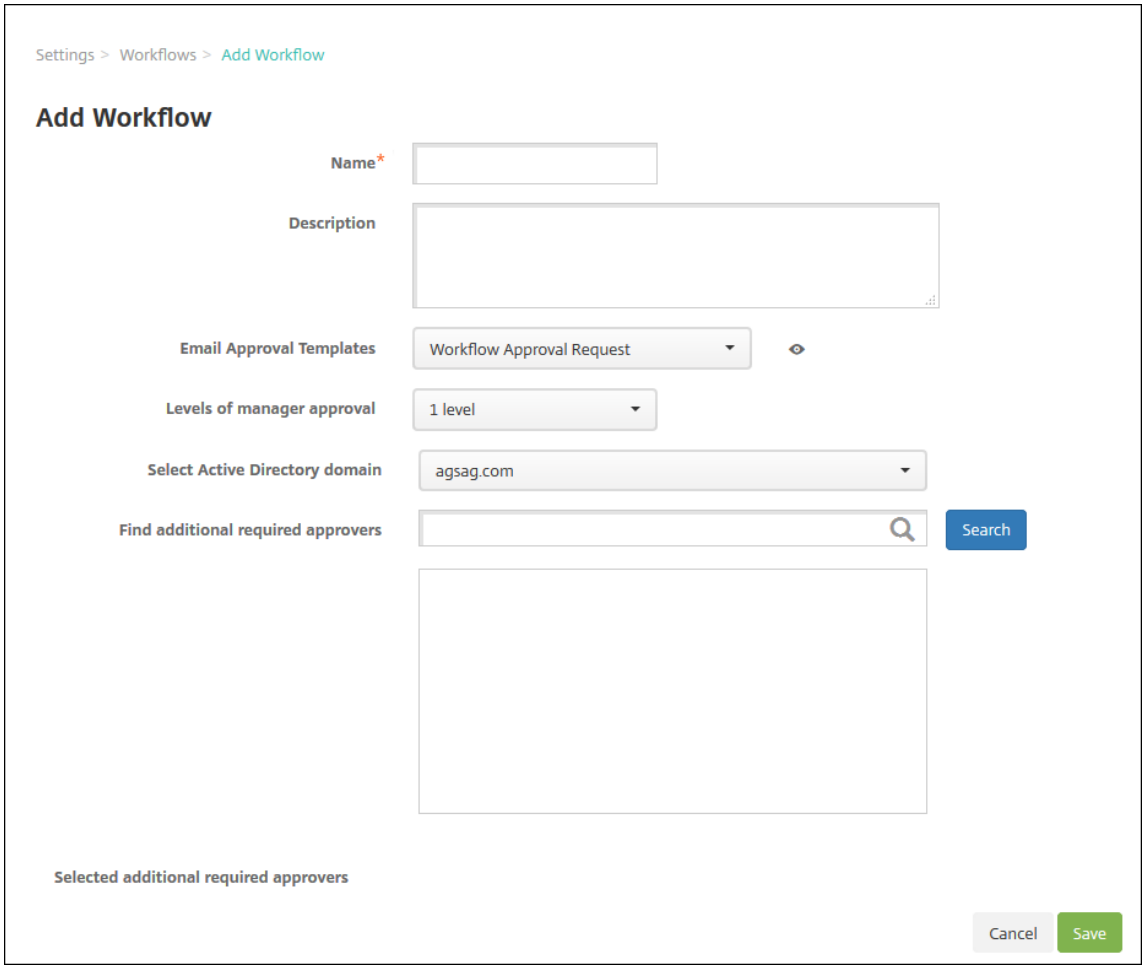
XenMobile 을처음으로설정하는경우워크플로를사용하기전에먼저워크플로전자메일설정을구성해야합니다. 워크플로전자메일설정은언제든지변경할수있습니다. 이러한설정에는전자메일서버, 포트, 전자메일주소및사용자계정생성요청에승인이필요한지여부가포함됩니다.

XenMobile 의두위치에서워크플로를구성할수있습니다.

- XenMobile 콘솔의 워크플로페이지와 워크플로페이지에서앱구성에사용할여러워크플로를구성할수있습니다. 워크플로페이지에서워크플로를구성하는경우앱을구성할때워크플로를선택할수있습니다.
- 앱의응용프로그램커넥터를구성할때워크플로이름을입력한다음사용자계정요청을승인할수있는사용자를구성합니다. XenMobile 에앱추가를참조하십시오.

사용자계정에대한관리자승인을최대 3 개수준까지할당할수있습니다. 사용자계정을승인할다른사용자가필요한경우해당사용자의이름또는전자메일주소를사용하여검색하고선택할수있습니다. XenMobile 에서해당사용자가검색되면워크플로에추가하면됩니다. 새사용자계정에대한승인또는거부를위한전자메일이워크플로의모든사용자에게전송됩니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 워크플로를클릭합니다. 워크플로페이지가나타납니다.
3. 추가를클릭합니다. 워크플로추가페이지가나타납니다.



4. 다음설정을구성합니다.

   - 이름**:** 워크플로의고유한이름을입력합니다.
   - 설명**:** 필요한경우워크플로의설명을입력합니다.
   - 전자메일승인템플릿**:** 목록에서할당할전자메일승인템플릿을선택합니다. XenMobile 콘솔의 설정아래에있는 알림템플릿섹션에서전자메일템플릿을만듭니다. 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 에서가져옵니다.
   - 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.

등록프로필

January 5, 2022

등록프로필은다음을지정합니다.

- Android 및 iOS 장치에대한장치관리등록옵션. Android 의경우 MDM+MAM(ENT) 서버모드에제공되는등록옵션은 MDM 모드의옵션과다릅니다.
- Android 및 iOS 장치에대한앱관리등록옵션.
- 기타등록옵션:
  - 사용자가등록할수있는장치수를제한할지여부.
    장치제한에도달하면사용자에게장치등록제한이초과되었음을설명하는오류메시지가표시됩니다.
  - 사용자가장치관리를거부할수있는지여부.

등록프로필을사용하여단일 XenMobile Server 콘솔내에서여러사용사례와장치마이그레이션경로를결합할수있습니다. 일부 사용사례에는다음이포함됩니다.

- Mobile Device Management(MDM 전용)
- MDM+MAM(Mobile Application Management)
- MAM 전용
- 회사소유등록

- BYOD 등록 (MDM 등록취소기능)
- Android Enterprise 등록으로 Android 장치관리자등록마이그레이션 (완전관리됨, 작업프로필, 전용장치)

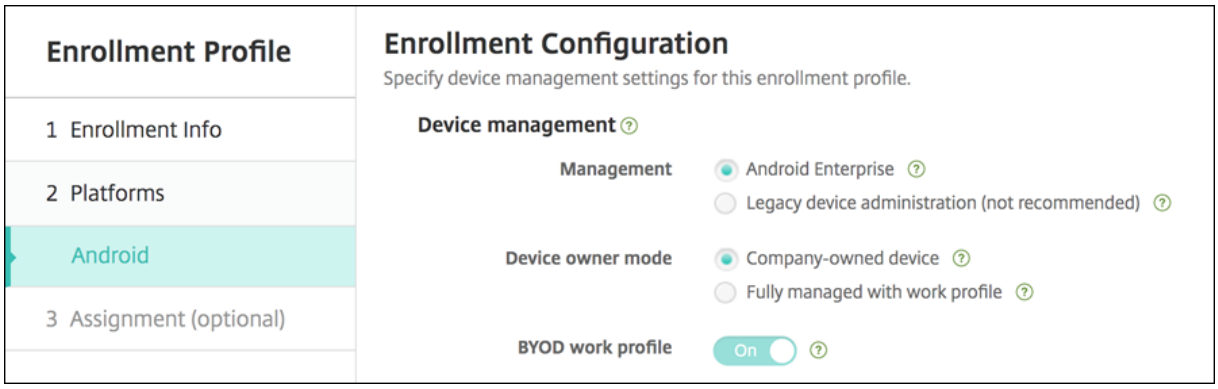
배달그룹을만들때 Global 이라는기본등록프로필을사용하거나다른등록프로필을지정할수있습니다.

플랫폼별등록프로필기능에는다음이포함됩니다.

- **Android** 장치**:** 장치소유자모드를지정합니다. 완전히관리, 작업프로필로완전히관리, BYOD 업무프로필을예로들수있습니다. 전용장치옵션은 XenMobile 용엔터프라이즈또는고급라이선스가있는경우에만나타납니다. 기본적으로 Android Enterprise 및앱관리에서새장치를등록합니다. 등록보안모드 사용자이름 **+ PIN**, 초대 **URL**, 초대 **URL + PIN**, 초대 **URL +** 암호는 Android Enterprise 에사용할수없습니다.
- **iOS** 장치**:** 장치등록유형: 장치등록을지정하거나장치를관리하지않습니다. iOS 설정은 XenMobile 엔터프라이즈또는고급라이센스가있는경우에만표시됩니다. 기본적으로 Apple 장치관리및앱관리에서새장치를등록합니다.

Android 장치에대한전용장치등록이나 Android 또는 iOS 장치에대한 MAM 전용등록이필요하지않은경우 `enable.multimode.xms` 서버속성을비활성화해도됩니다. 그러나이속성을계속활성화해두면모든유형의등록프로필을처리하는데 XenMobile Server 하나만있으면됩니다. 서버속성을참조하십시오.

`enable.multimode.xms`를비활성화할경우아래스크린샷에있는설정만사용할수있습니다.

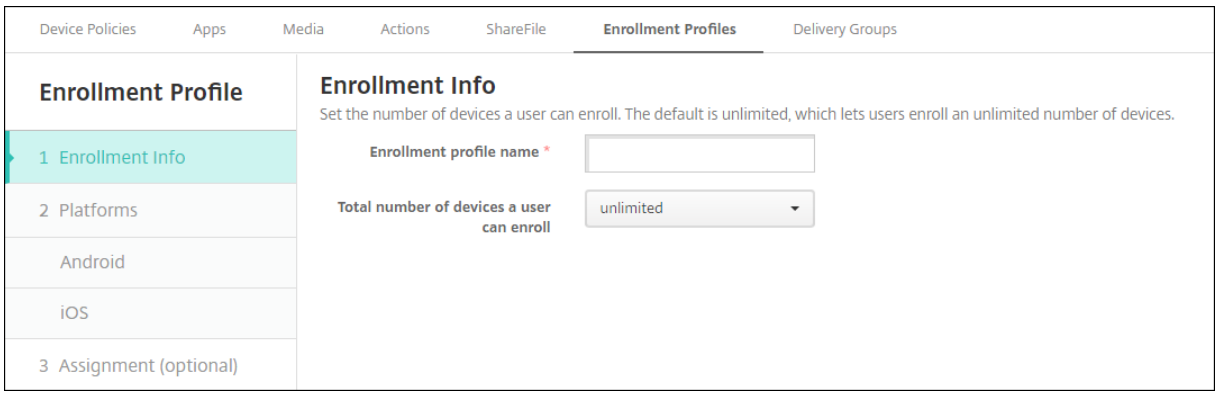


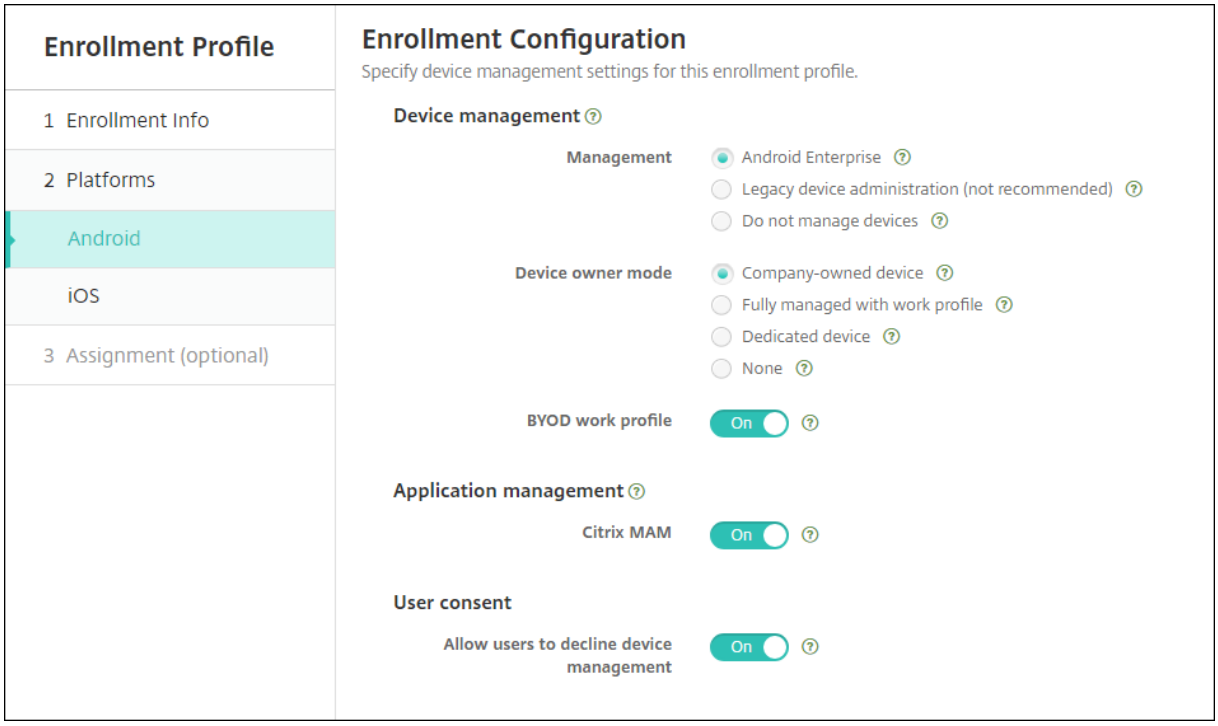
이러한설정에대한자세한내용은 Android Enterprise를참조하십시오.

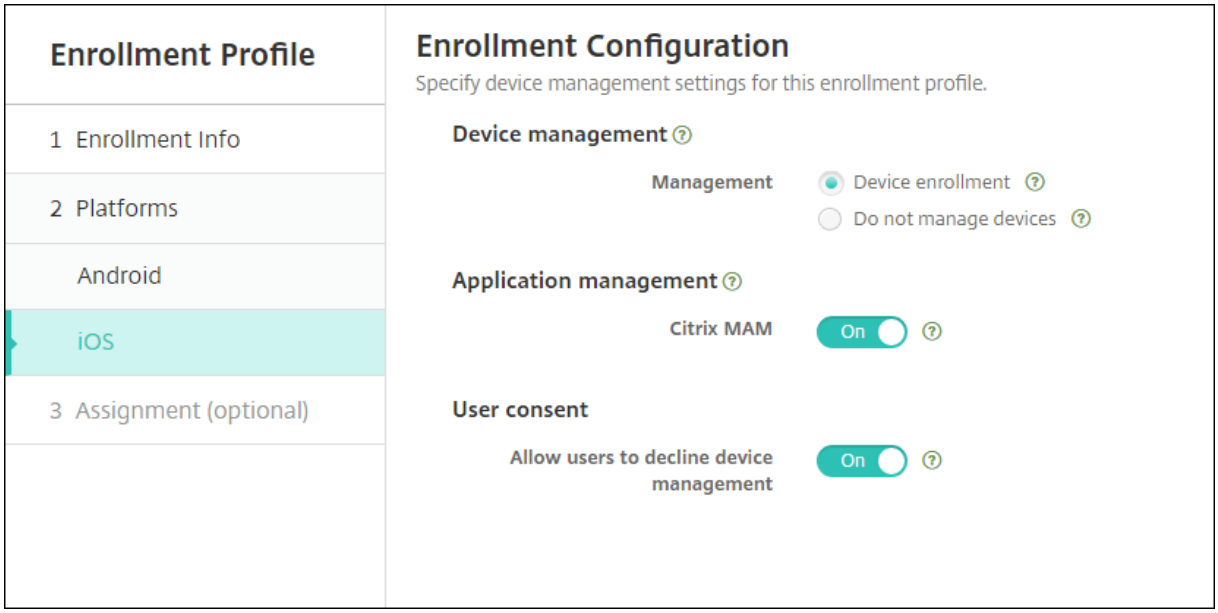
Global 등록프로필

기본등록프로필의이름은 Global 입니다. Global 프로필은등록프로필을만들기회가생길때까지테스트하는데유용합니다.

다음스크린샷은 Global 등록프로필의기본설정을보여줍니다.







등록프로필, 배달그룹및등록

등록프로필과배달그룹은다음과같이상호작용합니다.

- 하나이상의배달그룹에등록프로필을연결할수있습니다.
- 사용자가등록프로필이다른여러배달그룹에속하는경우사용되는등록프로필은배달그룹의이름에따라결정됩니다. XenMobile Server 는사전순으로표시된배달그룹목록의마지막에나타나는배달그룹을선택합니다. 예를들어다음과같은항목이있다고가정합니다.
  - “EP1” 과 “EP2” 라는등록프로필 2 개
  - “DG1” 과 “DG2” 라는배달그룹 2 개
  - “DG1” 은 “EP1” 에연결되어있습니다.
  - “DG2” 는 “EP2” 에연결되어있습니다.

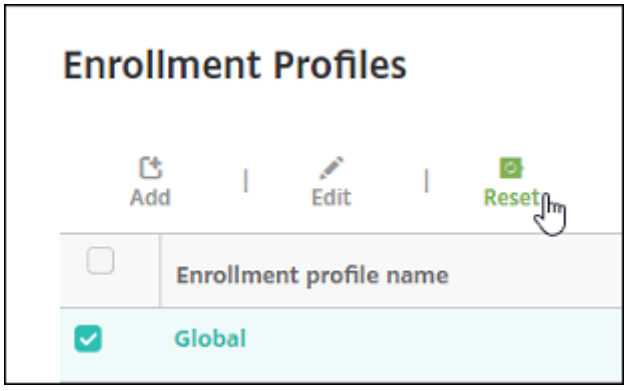
  등록사용자가 “DG1” 및 “DG2” 배달그룹에모두있는경우 XenMobile Server 는 “EP2” 등록프로필을사용하여사용자의등록유형을결정합니다.
- 배포순서는 MDM(장치관리) 에대해구성된등록프로필이있는배달그룹의장치에만적용됩니다.
- 장치가등록된후등록프로필을일부변경하려면다시등록해야합니다.
  - MDM 에대해구성된등록프로필에 MAM 추가.
  - MDM 에등록된장치를 MDM+MAM 에대해구성된배달그룹으로이동. 이러한변경사항은새장치등록에만영향을미칩니다. 기존장치등록은영향을받지않습니다.
  - MAM 에대해구성된등록프로필에 MDM 추가.
- 다른등록프로필로전환해도기존의등록된장치에는영향을주지않습니다. 그러나변경내용을적용하려면사용자가해당장치를등록취소했다가다시등록해야합니다.

등록프로필을만들려면

1. XenMobile Server 콘솔에서 구성 **>** 등록프로필로이동합니다.
2. 등록정보페이지에서프로필을설명하는이름을입력합니다. 기본적으로사용자는무제한장치를등록할수있습니다. 사용자당장치수를제한하는값을선택합니다. 이제한은사용자가등록하는 MAM 또는 MDM 관리형 Android 및 iOS 장치의합계에적용됩니다.
3. 플랫폼페이지를작성합니다. 플랫폼별등록설정에대한정보는다음에서확인하십시오.
   - Android Enterprise
   - iOS: 지원되는등록방법
4. 할당페이지에서하나이상의배달그룹을등록프로필에연결합니다.

   사용자는서로다른등록프로필이있는여러배달그룹에속할수있습니다. 이경우사용되는등록프로필은배달그룹의이름에따라결정됩니다. XenMobile 은사전순으로표시된배달그룹목록의마지막에나타나는배달그룹을선택합니다. 배달그룹을만들려면 구성 **>** 배달그룹으로이동합니다.

등록프로필목록이 구성 **>** 등록프로필페이지에나타납니다. Global 프로필을편집하거나원래기본설정으로재설정하려면 Global 프로필의열을선택하고 재설정을클릭합니다. Global 프로필은삭제할수없습니다.



RBAC 를사용하여역할구성

August 12, 2022

사전정의된각 RBAC(역할기반액세스제어) 역할에는특정액세스및기능권한이연결되어있습니다. 이문서에서는각사용권한이수행하는작업에대해설명합니다. 각기본제공역할에대한기본사용권한의전체목록을보려면 Role-Based Access Control Defaults(역할기반액세스제어기본값)를다운로드하십시오.

사용권한을적용할때 RBAC 역할에관리권한이있는사용자그룹을정의합니다. 기본관리자는적용된사용권한설정을변경할수없습니다. 기본적으로, 적용된사용권한은모든사용자그룹에적용됩니다.

할당을수행할때 RBAC 역할을그룹에할당하면사용자그룹이 RBAC 관리자권한을소유하게됩니다.

> 중요:
>
> 설정권한에서 RBAC 권한은관리자사용자에게자신의권한을할당할수있는기능을포함하여모든권한을부여합니다. Endpoint Management 시스템의모든항목을조작할수있는기능을제공하려는사용자에게만이액세스권한을부여하시기바랍니다.

이문서의섹션은다음과같습니다.

- 관리역할
- 지원역할
- 사용자역할
- RBAC 를사용하여역할구성

관리역할

미리정의된관리자역할을가진사용자는 XenMobile 에서다음기능에액세스하거나액세스할수없습니다. 기본적으로, 허가된액세스 (자가지원포털제외), 콘솔기능및 권한적용을사용할수있습니다.

허가된액세스

관리자콘솔액세스	관리자는 XenMobile 콘솔의모든기능에액세스할수있습니다.
자가지원포털액세스	관리자에게는자가지원포털액세스권한이없습니다.
공유장치등록자	관리자에게는공유장치등록자액세스권한이없습니다. 이기능은공유장치를등록해야하는사용자를위한것입니다.
원격지원액세스	관리자는원격지원액세스를소유합니다.*
공용 API 액세스	관리자는공용 API 에액세스하여 XenMobile 콘솔에서사용할수있는동작을프로그래밍방식으로수행할수있습니다. 이러한동작에는인증서, 앱, 장치, 배달그룹및로컬사용자관리가포함됩니다.
COSU 장치등록자	이기능이등록프로필로구성되지않은경우관리자가전용 Android Enterprise 장치 (COSU 장치라고도함) 를등록하는방법을제공합니다.

* 원격지원을사용하면지원센터담당자가관리되는 Android 모바일장치를원격으로제어할수있습니다. 스크린캐스트는 Samsung Knox 장치에서만지원됩니다. 원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다. 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix

는개선사항이나수정사항을제공하지않습니다.

콘솔기능

관리자는 XenMobile 콘솔에대한무제한액세스권한을갖습니다.

———————-	——-
대시보드	대시보드는관리자가 XenMobile 콘솔에로그온한후표시되는첫번째페이지입니다. 대시보드에는알림및장치에대한기본정보가표시됩니다.
보고	분석 **>** 보고페이지에는앱및장치배포를분석할수있는미리정의된보고서가제공됩니다.
장치	관리 **>** 장치페이지에서는사용자장치를관리할수있습니다. 관리자는페이지에서개별장치를추가하거나장치프로비저닝파일을가져와한번에여러장치를추가할수있습니다.
로컬사용자및그룹	관리 **>** 사용자페이지에서는로컬사용자및로컬사용자그룹을추가, 편집또는삭제할수있습니다.
등록	관리 **>** 등록초대페이지는 XenMobile 에장치를등록할사용자를초대하는방법을관리하는곳입니다.
정책	구성 **>** 장치정책페이지는 VPN 및 Wi-Fi 와같은장치정책을관리하는위치입니다.
앱	구성 **>** 앱페이지는관리자가사용자가장치에설치할수있는다양한앱을관리하는곳입니다.
미디어	구성 **>** 미디어페이지는관리자가사용자가장치에설치할수있는다양한미디어를관리하는곳입니다.
동작	구성 **>** 동작페이지는이벤트를트리거하는응답을관리하는곳입니다.
등록프로필	구성 **>** 등록프로필페이지에서관리자는사용자가장치를등록할때사용할등록프로필 (모드) 을구성할수있습니다.
배달그룹	구성 **>** 배달그룹페이지는관리자가배달그룹및배달그룹과관련된리소스를관리하는곳입니다.
설정	설정페이지에서는클라이언트및서버속성, 인증서및자격증명공급자같은시스템설정을관리할수있습니다. 중요**:** 이러한설정에는 RBAC 권한이포함됩니다. RBAC 권한은사용자에게자신의권한을할당할수있는기능을포함하여모든권한을부여합니다. Endpoint Management 시스템의모든항목을조작할수있는기능을제공하려는사용자에게만이액세스권한을부여하시기바랍니다.	
지원	문제해결및지원페이지에서진단실행, 로그생성같은문제해결활동을수행할수있습니다.

장치

관리자는장치제한사항을설정하고, 장치에대한알림을설정및전송하고, 장치의앱을관리하는등콘솔을통해장치기능에액세스합니다.

장치전체초기화	장치에서모든데이터와앱을초기화하며, 장치에메모리카드가있는경우메모리카드도초기화합니다.
제한사항지우기	하나이상의장치제한사항을제거합니다.
장치선택적초기화	개인데이터및앱은그대로유지하고장치에서모든회사데이터및앱을초기화합니다.

위치보기	장치의위치를확인하고지리적제한사항을설정합니다. 포함사항: 장치찾기, 장치의위치보기, 장치추적, 시간대별장치위치추적
장치잠금	사용자가장치를사용할수없도록원격으로장치를잠급니다.
장치잠금해제	사용자가장치를사용할수있도록원격으로장치의잠금을해제합니다.
컨테이너잠금	장치에서회사컨테이너를원격으로잠급니다.
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	장치의모든앱에대한액세스를거부합니다. Android 에서는사용자가 XenMobile 에로그인할수없습니다. iOS 에서는사용자가로그인할수는있지만앱에액세스할수는없습니다.
앱초기화	Android 에서는이작업으로사용자의 XenMobile 계정이삭제됩니다. iOS 에서는이작업으로 XenMobile 기능에액세스하는데필요한암호화키가삭제됩니다.
소프트웨어인벤토리보기	어떤소프트웨어가장치에설치되어있는지확인합니다.
AirPlay 미러링요청	AirPlay 스트리밍을시작하도록요청합니다.
AirPlay 미러링중지	AirPlay 스트리밍을중지합니다.

분실모드활성화	관리 **>** 장치에서감독되는장치를분실모드로설정하여잠금화면에서감독되는장치를차단할수있습니다. 분실모드를사용하면장치가분실또는도난당했을때장치를찾을수도있습니다.
분실모드비활성화	관리 **>** 장치에서분실모드로설정된장치의분실모드를비활성화할수있습니다.
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
로컬사용자잠금 ID 받기
로컬사용자잠금삭제

등록

관리자는등록초대를추가및삭제하고, 사용자에게알림을보내고, 등록테이블을.csv 파일로내보낼수있습니다.

등록추가/삭제	사용자또는사용자그룹에대한등록초대를추가하거나제거합니다.
사용자알림	사용자또는사용자그룹에대한등록초대를보냅니다.

등록초대테이블내보내기	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	공용앱스토어앱또는엔터프라이즈앱 (MDX 지원아님) 을추가하거나제거합니다.
앱스토어또는엔터프라이즈앱편집	공용앱스토어앱또는엔터프라이즈앱 (MDX 지원아님) 을변경합니다.
MDX, 웹, SaaS 앱추가/삭제	MDX 지원앱, 내부네트워크의앱 (웹앱) 또는공용네트워크 (SaaS) 의앱을 XenMobile 에추가하거나제거합니다.
MDX, 웹및 SaaS 앱편집	MDX 지원앱, 내부네트워크의앱 (웹앱) 또는공용네트워크 (SaaS) 의앱을 XenMobile 에서변경합니다.
범주추가/삭제	XenMobile Store 에서앱을표시할수있는범주를추가하거나삭제합니다.
공용/엔터프라이즈앱을배달그룹에할당	배포를위해공용앱스토어앱또는 MDX 지원앱을배달그룹에할당합니다.

MDX/WebLink/SaaS 앱을배달그룹에할당	Single Sign-on(WebLink) 이필요하지않거나공용네트워크 (SaaS) 에있는 MDX 지원앱을배달그룹에할당합니다.
앱테이블내보내기	앱페이지에서앱정보를수집하여.csv 파일로내보냅니다.

미디어

공용앱스토어또는볼륨구매라이센스를통해취득한미디어를관리합니다.

앱스토어또는엔터프라이즈서적추가/삭제
공용/엔터프라이즈서적을배달그룹에할당
앱스토어또는엔터프라이즈서적편집

동작

작업추가/삭제	트리거 (이벤트, 장치/사용자속성또는설치된앱이름) 및관련응답에의해정의된동작을추가하거나제거합니다.
작업편집	트리거 (이벤트, 장치/사용자속성또는설치된앱이름) 및관련응답에의해정의된동작을변경합니다.
작업을배달그룹에할당	사용자장치에배포하기위해배달그룹에동작을할당합니다.
작업내보내기	동작페이지에서동작정보를수집하여.csv 파일로내보냅니다.

배달그룹

관리자는 구성 **>** 배달그룹페이지에서배달그룹을관리합니다.

배달그룹추가/삭제	지정된사용자및선택적인정책, 앱및동작을추가하는배달그룹을만들거나제거합니다.
배달그룹편집	기존배달그룹을변경하여, 사용자및선택적인정책, 앱및동작을수정합니다.

배달그룹배포	배달그룹을사용할수있게만듭니다.
배달그룹내보내기	배달그룹페이지에서배달그룹정보를수집하고이를.csv 파일로내보냅니다.

등록프로필

등록프로필을관리합니다.

등록프로필추가/삭제
등록프로필편집
배달그룹에등록프로필할당

설정

관리자는 설정페이지에서다양한설정을구성합니다.

RBAC	RBAC 할당, 역할을할당합니다. 중요**:** 이권한은사용자에게자신의권한을할당할수있는기능을포함하여모든권한을부여합니다. Endpoint Management 시스템의모든항목을조작할수있는기능을제공하려는사용자에게만이액세스권한을부여하시기바랍니다.
LDAP	그룹, 사용자계정및관련속성을가져올수있도록하나이상의 LDAP 호환디렉터리 (예: Active Directory) 를관리합니다.
라이센스	온-프레미스 XenMobile Server 에해당합니다. Citrix 라이센스를관리합니다.
등록	사용자및자가지원포털에대해등록보안모드를사용하도록설정합니다.
릴리스관리	현재설치된릴리스를확인합니다. 포함사항: 릴리스관리업데이트
인증서	APNS 인증서편집, 인증서 SSL 수신기

알림템플릿	자동화동작이나등록에서, 아니면사용자에게표준알림메시지를제공할때사용할알림템플릿을만듭니다.
워크플로	앱구성에사용할수있도록사용자계정의만들기, 승인및제거를관리합니다.
자격증명공급자	장치인증서를발급하도록승인된하나이상의자격증명공급자를추가합니다. 자격증명공급자는인증서형식과인증서를갱신하거나해지하기위한조건을제어합니다.
PKI 엔터티	공개키인프라엔터티 (일반, Microsoft 인증서서비스또는 임의의 CA) 를관리합니다.
PKI 연결테스트	설정 **> PKI** 엔터티페이지의연결테스트단추를사용하여서버에액세스할수있는지확인합니다.
클라이언트속성	암호유형, 강도또는만료와같은사용자장치의다양한속성을관리합니다.
클라이언트지원	사용자가지원서비스에연락할수있는방법 (전자메일, 전화또는지원티켓전자메일) 을설정합니다.
클라이언트브랜딩	XenMobile Store 의사용자지정스토어이름과기본스토어보기를생성합니다. XenMobile Store 또는 Secure Hub 에표시되는사용자지정로고를추가합니다.
이동통신사업자 SMS 게이트웨이	이동통신사업자의 SMS 게이트웨이를설정하여이동통신사업자의 SMS 게이트웨이를통해 XenMobile 이전송하는알림을구성합니다.
알림서버	사용자에게전자메일을보내도록 SMTP 게이트웨이서버를설정합니다.
ActiveSync Gateway	규칙및속성을통해사용자및장치에대한사용자액세스를관리합니다.
Apple 배포프로그램	XenMobile 에 Apple 배포프로그램계정을추가합니다.
Apple Configurator 장치등록	XenMobile 에서 Apple Configurator 설정을구성합니다.
iOS/볼륨구매설정	Apple 볼륨구매계정을추가합니다.
모바일서비스공급자	모바일서비스공급자인터페이스를사용하여 BlackBerry 및기타 Exchange ActiveSync 장치를쿼리하고작업을실행합니다.

Citrix Gateway	온-프레미스 XenMobile Server 에해당합니다. Citrix Gateway 를추가합니다. 인증을사용할지여부와인증시사용자인증서를푸시할지여부를선택합니다. 자격증명공급자를선택합니다.
네트워크액세스제어	장치가규정을준수하지않는지확인하고네트워크에대한액세스를거부하는조건을설정합니다.
Samsung Knox	XenMobile 이 Samsung Knox 증명서버 REST API 를쿼리하거나쿼리하지않도록설정합니다.
서버속성	서버속성을추가하거나수정합니다. 모든노드에서 XenMobile 을다시시작해야합니다.
Syslog	온-프레미스 XenMobile Server 에해당합니다. 서버호스트이름또는 IP 주소를사용하여시스템로그 (syslog) 서버로로그파일을보냅니다.
XenApp 및 XenDesktop	사용자가 Citrix Secure Hub 를통해 Virtual Apps and Desktops 를추가할수있습니다.
Citrix Files	XenMobile 에서 Enterprise 계정을사용할경우: Content Collaboration 계정및관리자서비스계정에연결하여사용자계정을관리하는설정을구성합니다. 기존 Citrix Files 도메인및관리자자격증명이필요합니다. XenMobile 과함께 StorageZone 커넥터를사용하는경우: StorageZone 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.
XenMobile Tools	XenMobile Tools 페이지에액세스합니다.

SNMP 구성	XenMobile Server 노드에대해 SNMP 를사용하도록설정합니다. 모니터링사용자를편집또는추가하고, 트랩알림이나타나는 SNMP 관리자를설정하고, 트랩간격과임계값을구성합니다.

지원

관리자는다양한지원작업을수행할수있습니다.

Citrix Gateway 연결확인	IP 주소로 Citrix Gateway 에대한다양한연결확인을수행합니다. 사용자이름및암호가필요합니다.
XenMobile 연결확인	선택한 XenMobile 기능 (예: 데이터베이스, DNS 또는 Google Plan) 에대한연결확인을수행합니다.
지원번들만들기	온-프레미스 XenMobile Server 에해당합니다. 문제해결을위해 Citrix 지원에보낼파일을생성합니다. XenMobile 또는 Citrix Gateway 에대한시스템정보, 로그, 데이터베이스정보, 핵심정보, 추적파일및최신구성정보가포함됩니다.
Citrix 제품설명서	공개 Citrix XenMobile 설명서사이트에액세스합니다.
Citrix Knowledge Center	Citrix 지원사이트에액세스하여기술자료문서를검색합니다.
로그	디버그, 관리자감사및사용자감사에대한로그파일세부정보에액세스하고분석합니다.
클러스터정보	온-프레미스 XenMobile Server 에해당합니다. 클러스터된환경의각노드에대한정보에액세스합니다.
가비지수집	온-프레미스 XenMobile Server 에해당합니다. 더이상사용하지않는메모리개체에대한정보에액세스합니다.
Java 메모리속성	온-프레미스 XenMobile Server 에해당합니다. Java 메모리사용현황, 메모리세부정보및메모리풀세부정보의스냅샷에액세스합니다.
매크로	프로필, 정책, 알림또는등록템플릿의텍스트필드에사용자또는장치속성데이터를채웁니다. 단일정책을구성하여대규모사용자기반에정책을배포하고각대상사용자에게사용자관련값이표시되게합니다.
PKI 구성	PKI 구성정보를가져오고내보냅니다.

APNS 서명유틸리티	APNs(Apple Push Network signing) 인증서에대한요청을제출하거나 iOS 용 Secure Mail APNs 인증서를업로드합니다.
Citrix Insight Services	다양한문제에대한도움을받으려면 CIS(Citrix Insight Services) 에로그를업로드하십시오.
Exchange ActiveSync 용 Citrix Gateway 커넥터장치상태	장치 ActiveSync ID 를기반으로 Exchange ActiveSync 용 Citrix Gateway 커넥터로전송된장치의상태를 XenMobile 에쿼리합니다.
익명화및익명화취소	온-프레미스 XenMobile Server 에해당합니다. XenMobile 에서지원번들을만드는경우중요한사용자, 서버및네트워크데이터가기본적으로익명으로만들어집니다. 고급아래의 지원 **>** 익명화및익명화취소에서이동작을변경할수있습니다.
로그설정	로그수준을사용자지정하거나사용자지정로거를추가합니다.

그룹액세스제한

관리사용자는모든사용자그룹에권한을적용할수있습니다.

지원역할

지원역할이있는사용자는원격지원에액세스할수있습니다. 이권한은기본적으로모든사용자에게적용되며이설정을편집할수없습니다.

사용자역할

사용자역할을가진사용자는다음과같이 XenMobile 에제한적으로액세스할수있습니다.

허가된액세스

자가지원포털	사용자는 XenMobile 에서자가지원포털에만액세스할수있습니다.

콘솔기능

사용자는 XenMobile 콘솔에대해다음과같은제한적인액세스권한을갖습니다.

장치

장치전체초기화	장치에서모든데이터와앱을초기화하며, 장치에메모리카드가있는경우메모리카드도초기화합니다.
장치선택적초기화	개인데이터및앱은그대로유지하고장치에서모든회사데이터및앱을초기화합니다.
위치보기	장치의위치를확인하고지리적제한사항을설정합니다. 포함사항: 장치찾기, 장치의위치보기, 장치추적, 시간대별장치위치추적
장치잠금	장치를원격으로잠가사용할수없게만듭니다.
장치잠금해제	장치를원격으로잠금해제하여사용할수있게만듭니다.
컨테이너잠금	장치에서회사컨테이너를원격으로잠급니다.
컨테이너잠금해제	장치에서회사컨테이너를원격으로잠금해제합니다.
컨테이너암호재설정	회사컨테이너암호를재설정합니다.
ASM DEP 사용/활성화잠금바이패스	활성화잠금을사용하면감독되는 iOS 장치에바이패스코드가저장됩니다. 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.
- 지원**:** 원격지원에대한액세스권한을부여합니다.
- 사용자**:** 장치를등록할수있고자가지원포털에액세스할수있는사용자가사용합니다.

사용자역할을만들기위해사용자지정하는템플릿으로기본역할을사용할수도있습니다. 기본역할에정의된기능이외의특정시스템기능에액세스할수있는권한이있는새로운사용자역할을만들수있습니다.

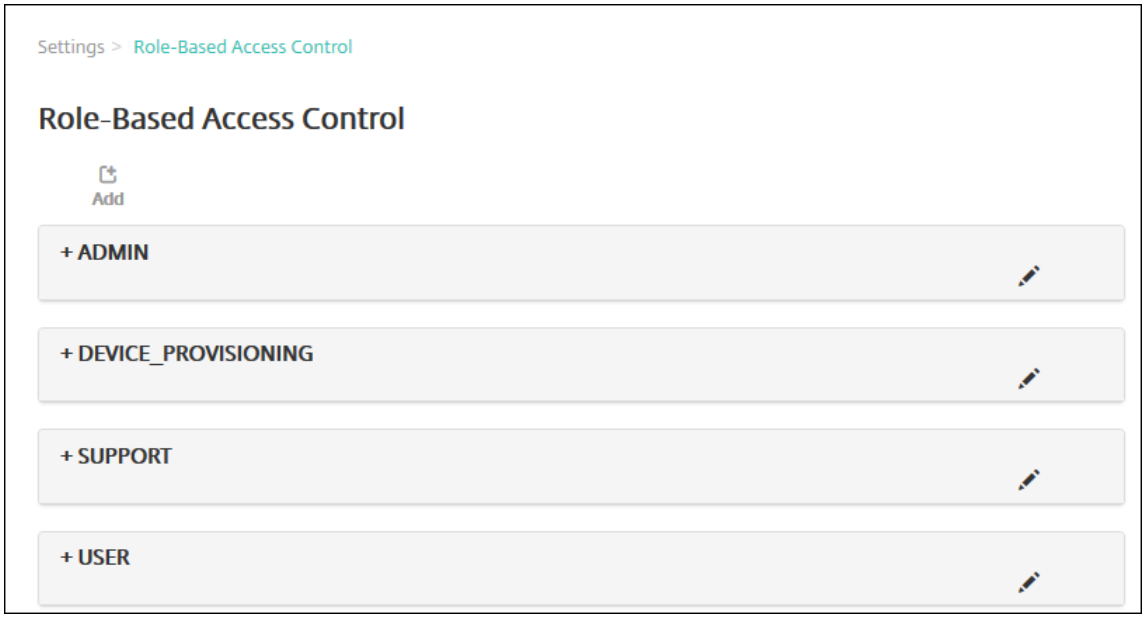
역할은로컬사용자 (사용자수준) 또는 Active Directory 그룹 (해당그룹의모든사용자가동일한권한을가짐) 에할당할수있습니다. 사용자가여러 Active Directory 그룹에속하는경우모든권한이병합되어해당사용자의권한을정의합니다. 예를들어 ADGroupA 사용자는관리자장치를찾을수있고 ADGroupB 사용자는직원장치를초기화할수있습니다. 이경우, 두그룹모두에속하는사용자는관리자와직원의장치를찾고초기화할수있습니다.

> 참고**:**
>
> 로컬사용자에게는하나의역할만할당될수있습니다.

XenMobile 의 RBAC 기능을사용하여다음을수행할수있습니다.

- 역할을만듭니다.
- 역할에그룹을추가합니다.
- 로컬사용자를역할에연결합니다.

1. XenMobile 콘솔에서 설정 **>** 역할기반액세스제어로이동합니다. 역할기반액세스제어페이지가나타납니다. 이페이지에는네개의기본사용자역할과앞서추가한모든역할이표시됩니다.



역할옆에있는더하기기호 (+) 를클릭하면다음그림과같이역할이확장되어해당역할에대한모든권한이표시됩니다.

2. 새사용자역할을추가하려면 추가를클릭합니다. 역할을편집하려면기존역할오른쪽에있는펜아이콘을클릭합니다. 역할을삭제하려면역할오른쪽에있는휴지통아이콘을클릭합니다. 기본사용자역할은삭제할수없습니다.

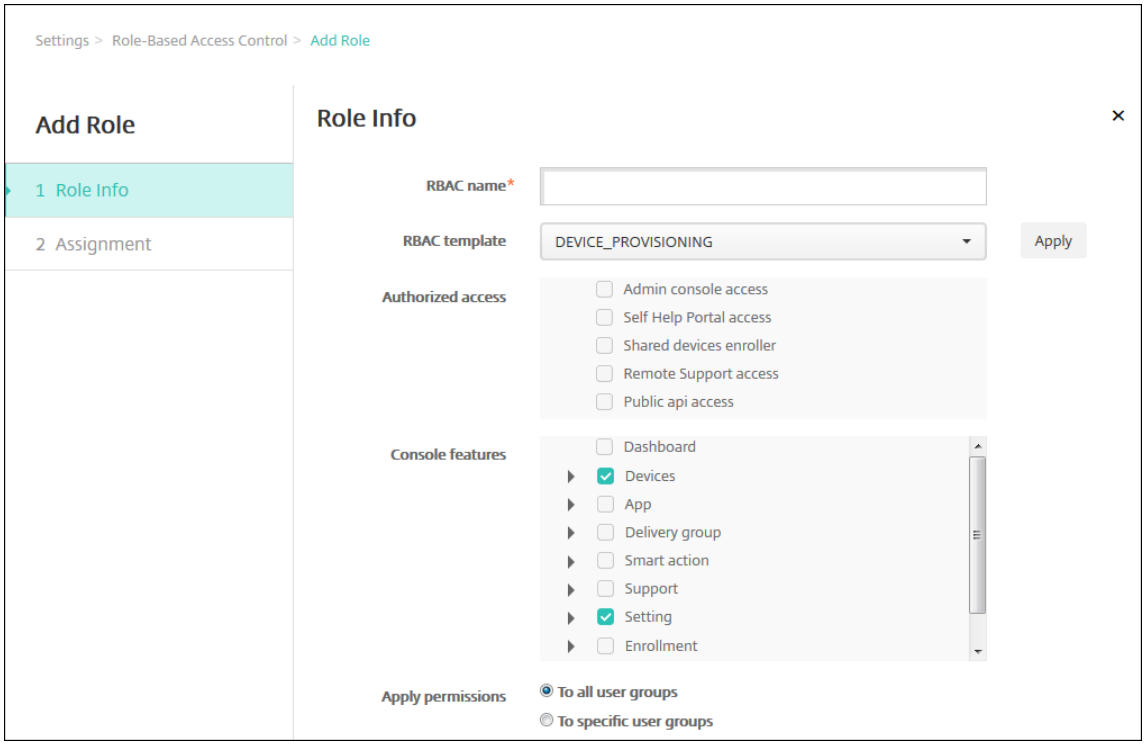
    - 추가또는연필아이콘을클릭하면 역할추가또는 역할편집페이지가나타납니다.
    - 휴지통아이콘을클릭하면확인대화상자가나타납니다. 선택한역할을제거하려면 삭제를클릭합니다.

3. 다음정보를입력하여사용자역할을만들거나편집합니다.

    - **RBAC** 이름**:** 새사용자역할을설명하는이름을입력합니다. 기존역할의이름은변경할수없습니다.
    - **RBAC** 템플릿**:** 선택적으로, 새역할의시작점으로사용할템플릿을클릭합니다. 기존역할을편집하는경우템플릿을선택할수없습니다.

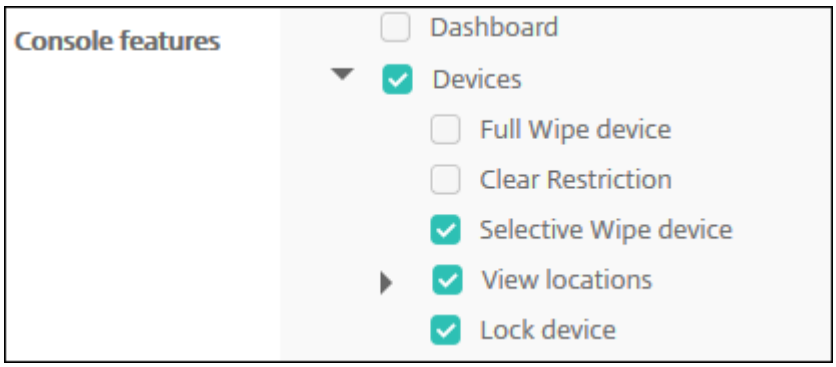
    RBAC 템플릿은기본사용자역할입니다. 이러한템플릿은해당역할과연결된사용자가갖는시스템기능에대한액세스권한을정의합니다. RBAC 템플릿을선택한후 허가된액세스및 콘솔기능필드에서해당역할과연결된모든권한을확인할수있습니다. 템플릿사용은선택사항입니다. 허가된액세스및 콘솔기능필드에서역할에할당할옵션을직접선택할수있습니다.

4. **RBAC** 템플릿필드가까이에있는 적용을클릭하여 허가된액세스및 콘솔기능을미리정의된액세스권한과기능권한으로채웁니다.



5. 허가된액세스및 콘솔기능의확인란을선택하고선택취소하여역할을사용자지정합니다.

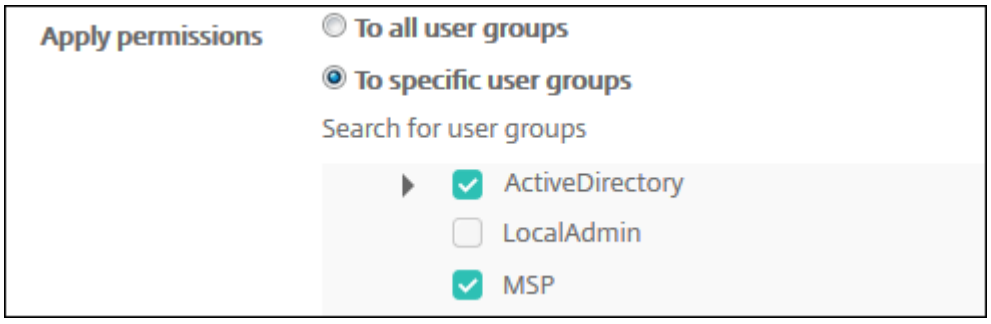
   콘솔기능옆에있는삼각형을클릭하면해당기능과관련된권한이선택하거나선택취소할수있도록나타납니다. 최상위확인란을클릭하면해당콘솔영역에대한액세스가금지됩니다. 이러한옵션을활성화하려면최상위아래에있는개별옵션을선택합니다. 예를들어다음그림에서역할에할당된사용자에게 장치전체초기화및 제한사항지우기옵션은나타나지않습니다. 선택된옵션이나타납니다.



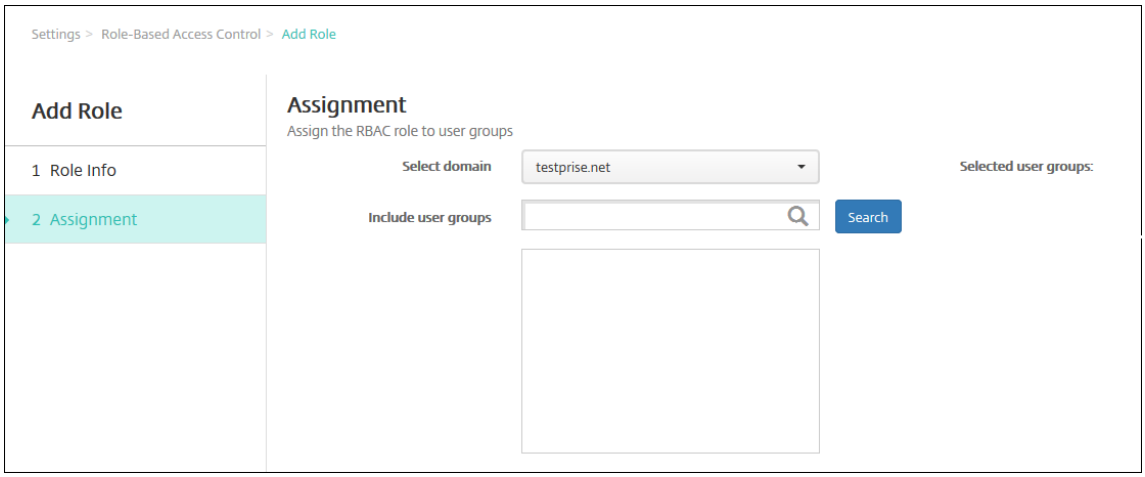
6. 권한적용**:** 하나이상의사용자그룹을선택하여관리자가관리할수있는그룹을제한합니다. 특정사용자그룹을클릭하면하나이상의그룹을선택할수있는그룹목록이나타납니다.

   예를들어 RBAC 관리자에게 ActiveDirectory 및 MSP 사용자그룹에대한권한이있는경우:

   - 관리자는 ActiveDirectory 그룹, MSP 그룹또는두그룹모두에있는사용자에대한정보에만액세스할수있습니다.
   - 관리자는다른로컬또는 AD 사용자를볼수없습니다. 관리자는이러한그룹중하나의하위그룹에속하는사용자를볼수있습니다.
   - 관리자는다음으로초대장을보낼수있습니다.
     - 권한그룹및해당하위그룹
     - 권한그룹및하위그룹의구성원인사용자

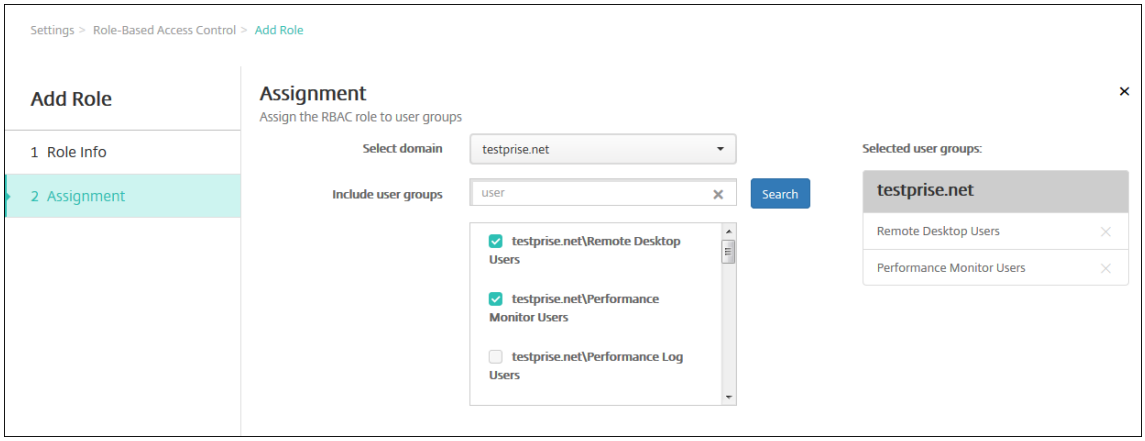


7. 다음을클릭합니다. 할당페이지가나타납니다.



8. 다음정보를입력하여사용자그룹에역할을할당합니다.

- 도메인선택**:** 목록에서도메인을클릭합니다.
- 사용자그룹포함**:** 검색을클릭하여사용가능한모든그룹의목록을보거나, 그룹이름전체또는일부를입력하여해당이름을포함하는그룹으로만목록을제한합니다.
- 나타나는목록에서역할을할당할사용자그룹을선택합니다. 사용자그룹을선택하면해당그룹이 선택된사용자그룹목록에나타납니다.



> 참고**:**
>
> 선택된사용자그룹목록에서사용자그룹을제거하려면사용자그룹이름옆에있는 X 를클릭합니다.

9. 저장을클릭합니다.

알림

June 10, 2022

XenMobile 에서다음과같은용도로알림을사용할수있습니다.

- 선택적인사용자그룹에게여러가지시스템관련기능을전달합니다. 특정사용자를대상으로이러한알림을보낼수도있습니다. 예를들어모든 iOS 장치사용자, 장치가규정위반상태인사용자, 직원소유의장치사용자등을대상으로할수있습니다.
- 사용자및장치를등록합니다.
- 특정조건이충족될때사용자에게자동으로알림을보냅니다 (자동화동작사용). 예:
  - 규정문제로인해기업도메인에서사용자장치를차단할예정인경우
  - 장치가탈옥또는루팅된경우

자동화동작에대한자세한내용은 자동화된동작을참조하십시오.

XenMobile 에서알림을보내려면게이트웨이및알림서버를구성해야합니다. XenMobile 에서알림서버를설정하고 SMTP(Simple Mail Transfer Protocol) 및 SMS(Short Message Service) 게이트웨이서버를구성하여사용자에게전자메일및텍스트 (SMS) 알림을보낼수있습니다. 알림을사용하여 SMTP 또는 SMS 의두개채널로메시지를보낼수있습니다.

- SMTP 는연결지향적인텍스트기반프로토콜로, 일반적으로 TCP(Transmission Control Protocol) 연결을통해명령문자열을실행하고필요한데이터를제공하는방식으로메일을보낸사람과메일을받는사람이통신합니다. SMTP 세션은

SMTP 클라이언트 (메시지를보내는사람) 에서시작된명령과이에대한 SMTP 서버의응답으로구성됩니다.

- SMS 는전화, 웹또는모바일통신시스템의문자메시지서비스구성요소입니다. SMS 는표준화된통신프로토콜을사용하여유선전화또는휴대폰장치에서 SMS 를교환할수있도록합니다.

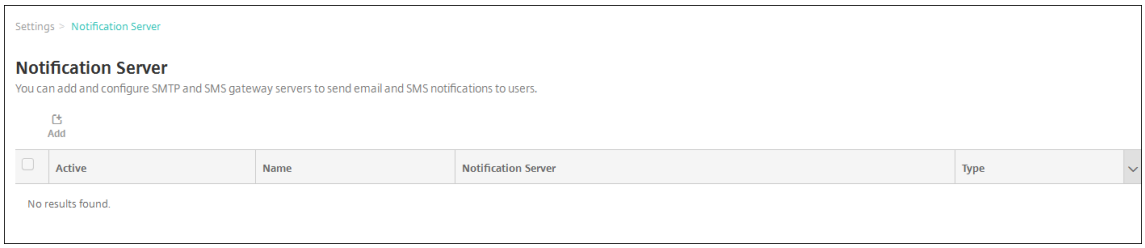
또한 XenMobile 에서이동통신사업자 SMS 게이트웨이를설정하여이동통신사업자의 SMS 게이트웨이를통해전송되는알림을구성할수있습니다. 이동통신사업자는통신네트워크를통한 SMS 전송의송수신에 SMS 게이트웨이를사용합니다. 이러한텍스트기반메시지는표준화된통신프로토콜을사용하여유선전화또는휴대폰장치에서 SMS 를교환할수있도록합니다.

사전요구사항

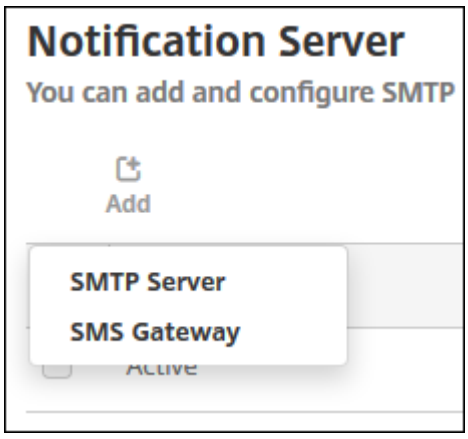
- SMS 게이트웨이를구성하기전에시스템관리자에게문의하여서버정보를확인하십시오. SMS 서버가내부회사서버에서호스트되는지, 호스트되는전자메일서비스의일부인지를확인해야합니다. 후자의경우서비스공급자의웹사이트에서정보를얻어야합니다.
- 사용자에게메시지를보내도록 SMTP 알림서버를구성합니다. 서버가내부서버에서호스트되는경우시스템관리자에게구성정보를문의하십시오. 서버가호스트되는전자메일서비스인경우서비스공급자의웹사이트에서해당하는구성정보를찾으십시오.
- 하나의활성 SMTP 서버와하나의활성 SMS 서버를동시에사용할수있습니다. 두통신채널모두하나의활성구성을허용합니다.
- 네트워크 DMZ 에위치한 XenMobile 에서포트 25 를열어내부네트워크의 SMTP 서버를다시가리키도록합니다. 이렇게하면 XenMobile 에서성공적으로알림을보낼수있습니다.

SMTP 서버및 **SMS** 게이트웨이구성

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 알림에서 알림서버를클릭합니다. 알림서버페이지가나타납니다.

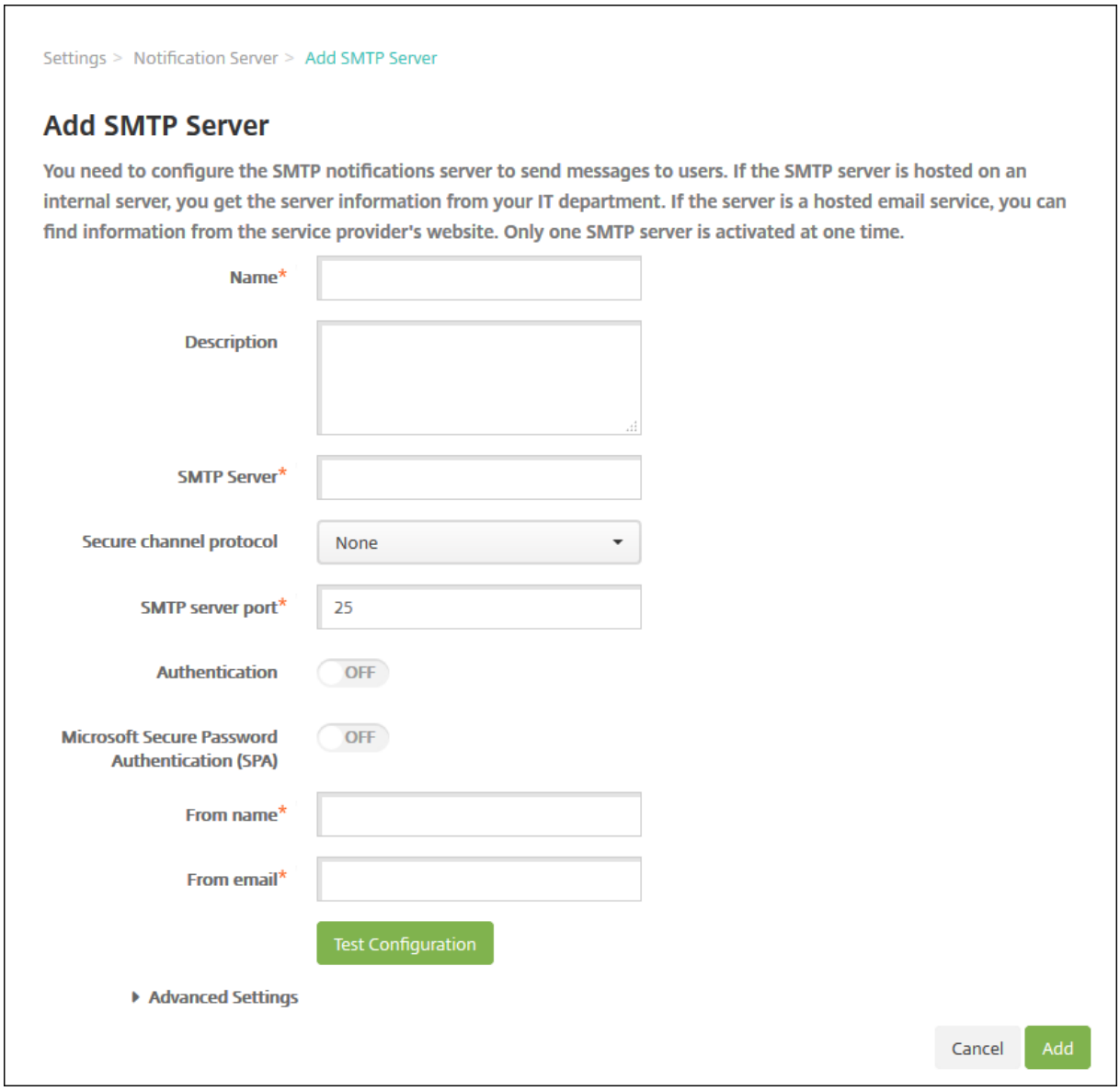


3. 추가를클릭합니다. SMTP 서버또는 SMS 게이트웨이를구성하는옵션이포함된메뉴가나타납니다.



- SMTP 서버를추가하려면 **SMTP** 서버를클릭하고 SMTP 서버를추가하려면의단계에따라이설정을구성합니다.
- SMS 게이트웨이를추가하려면 **SMS** 게이트웨이를클릭하고 SMS 게이트웨이를추가하려면의단계에따라이설정을구성합니다.

SMTP 서버추가



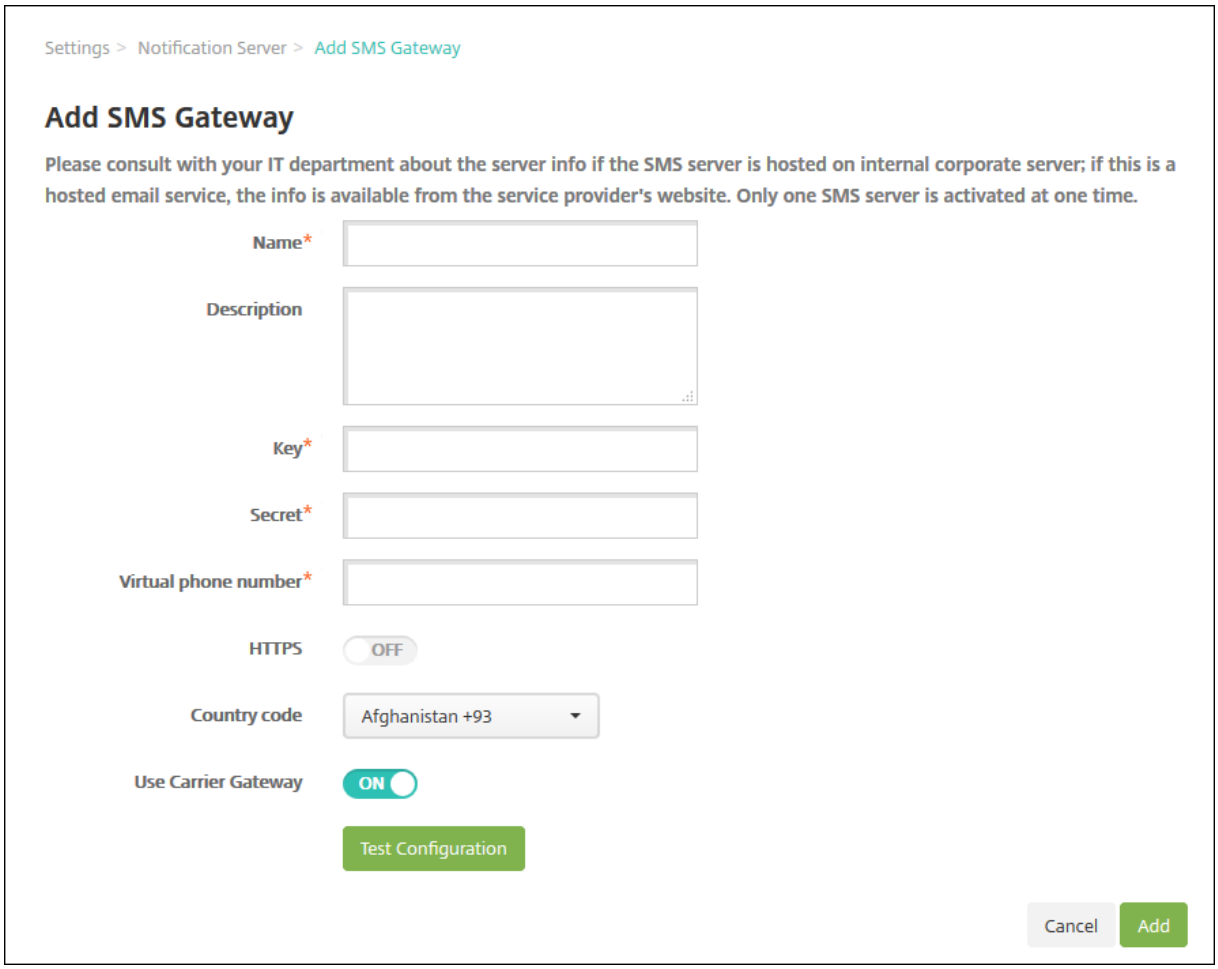
1. 다음설정을구성합니다.

   - 이름**:** SMTP 서버계정에연결된이름을입력합니다.
   - 설명**:** 필요한경우서버의설명을입력합니다.
   - **SMTP** 서버**:** 서버의호스트이름을입력합니다. 호스트이름은 FQDN(정규화된도메인이름) 또는 IP 주소일수있습니다.
   - 보안채널프로토콜**:** 목록에서서버가사용하는보안채널프로토콜에대해 **SSL**, **TLS** 또는 없음을클릭합니다 (보안인증을사용하도록서버가구성된경우). 기본값은 없음입니다.
   - **SMTP** 서버포트**:** SMTP 서버에서사용하는포트를입력합니다. 기본적으로포트는 25 로설정됩니다. SMTP 연결에 SSL 보안채널프로토콜이사용되는경우포트는 465 로설정됩니다.
   - 인증**:** 켜짐또는 꺼짐을선택합니다. 기본값은 꺼짐입니다.

- 인증을사용하는경우다음설정을구성합니다.
  - 사용자이름**:** 인증에사용할사용자이름을입력합니다.
  - 암호**:** 인증사용자의암호를입력합니다.
- **Microsoft SPA(**보안암호인증**):** SMTP 서버에서 SPA 를사용하는경우 켜짐을클릭합니다. 기본값은 꺼짐입니다.
- 발신자이름**:** 클라이언트에서이서버의알림전자메일을수신할때 보낸사람상자에표시되는이름을입력합니다. 예를들어, 회사 IT 를입력합니다.
- 발신자전자메일**:** 전자메일받는사람이 SMTP 서버에서보낸알림에회신할때사용하는전자메일주소를입력합니다.

2. 구성테스트를클릭하여테스트전자메일알림을보냅니다.
3. 고급설정을확장하고다음설정을구성합니다.
   - **SMTP** 재시도횟수**:** SMTP 서버에서보낸실패한메시지를재시도할횟수를입력합니다. 기본값은 5 입니다.
   - **SMTP** 시간제한**:** SMTP 요청을보낼때대기할기간 (초) 을입력합니다. 시간제한으로인해메시지전송이지속적으로실패하는경우이값을늘립니다. 이값을줄일때는주의하십시오. 시간초과로인해배달되지않은메시지의수가늘어날수있습니다. 기본값은 30 초입니다.
   - 최대 **SMTP** 받는사람수**:** SMTP 서버에서보내는전자메일메시지당최대받는사람수를입력합니다. 기본값은 100 입니다.
4. 추가를클릭합니다.

SMS 게이트웨이추가



> 메모**:**
>
> XenMobile 은 Nexmo SMS 메시지만지원합니다. Nexmo 메시지사용을위한계정이없는경우 웹사이트를방문하여계정을만드십시오.

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.

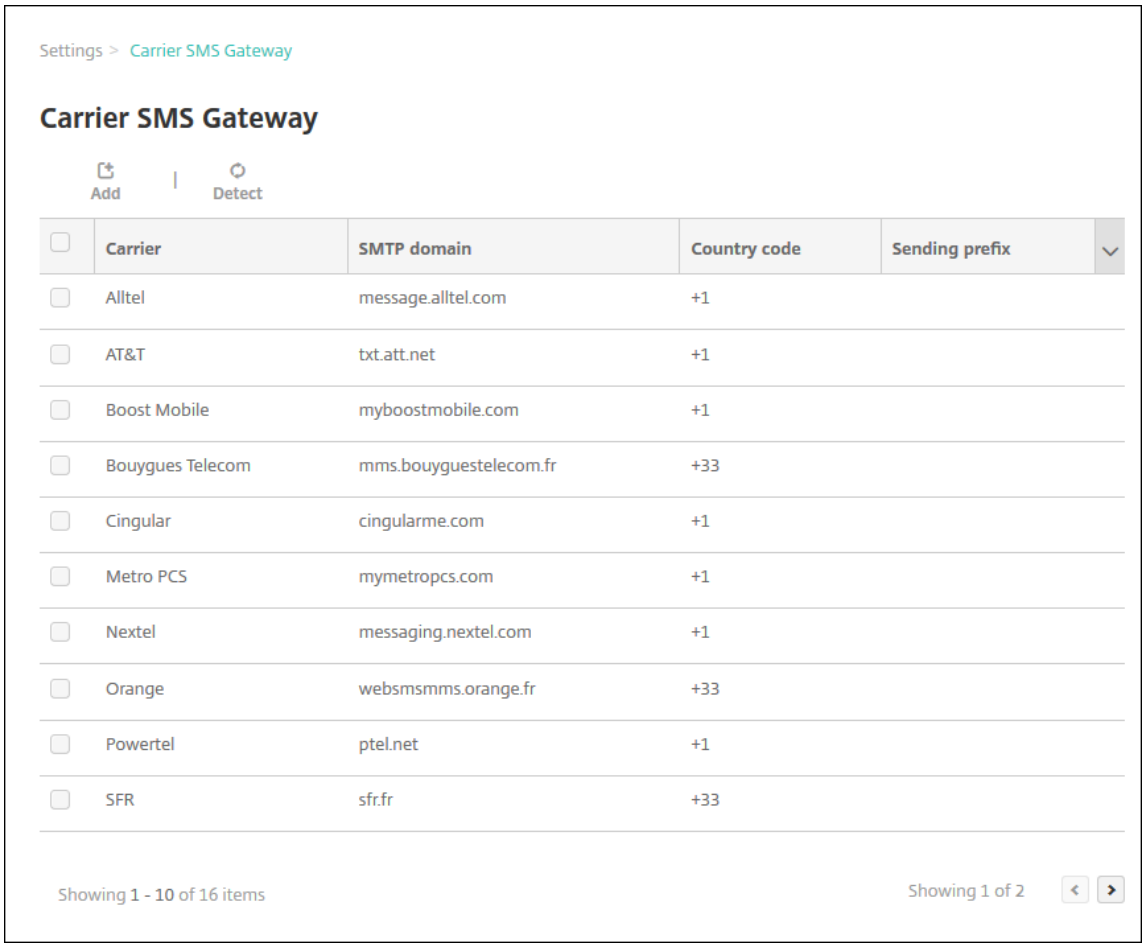
- 국가코드: 목록에서조직의받는사람에대한기본 SMS 국가코드접두사를클릭합니다. 이필드는항상 + 기호로시작됩니다. 기본값은 아프가니스탄 **+93** 입니다.

2. 구성테스트를클릭하여현재구성으로테스트메시지를보냅니다. 인증, 가상전화번호오류등과같은연결오류는즉시감지되고표시됩니다. 휴대폰간에전송된메시지와같은시간내에메시지가수신됩니다.
3. 추가를클릭합니다.

이동통신사업자 **SMS** 게이트웨이추가

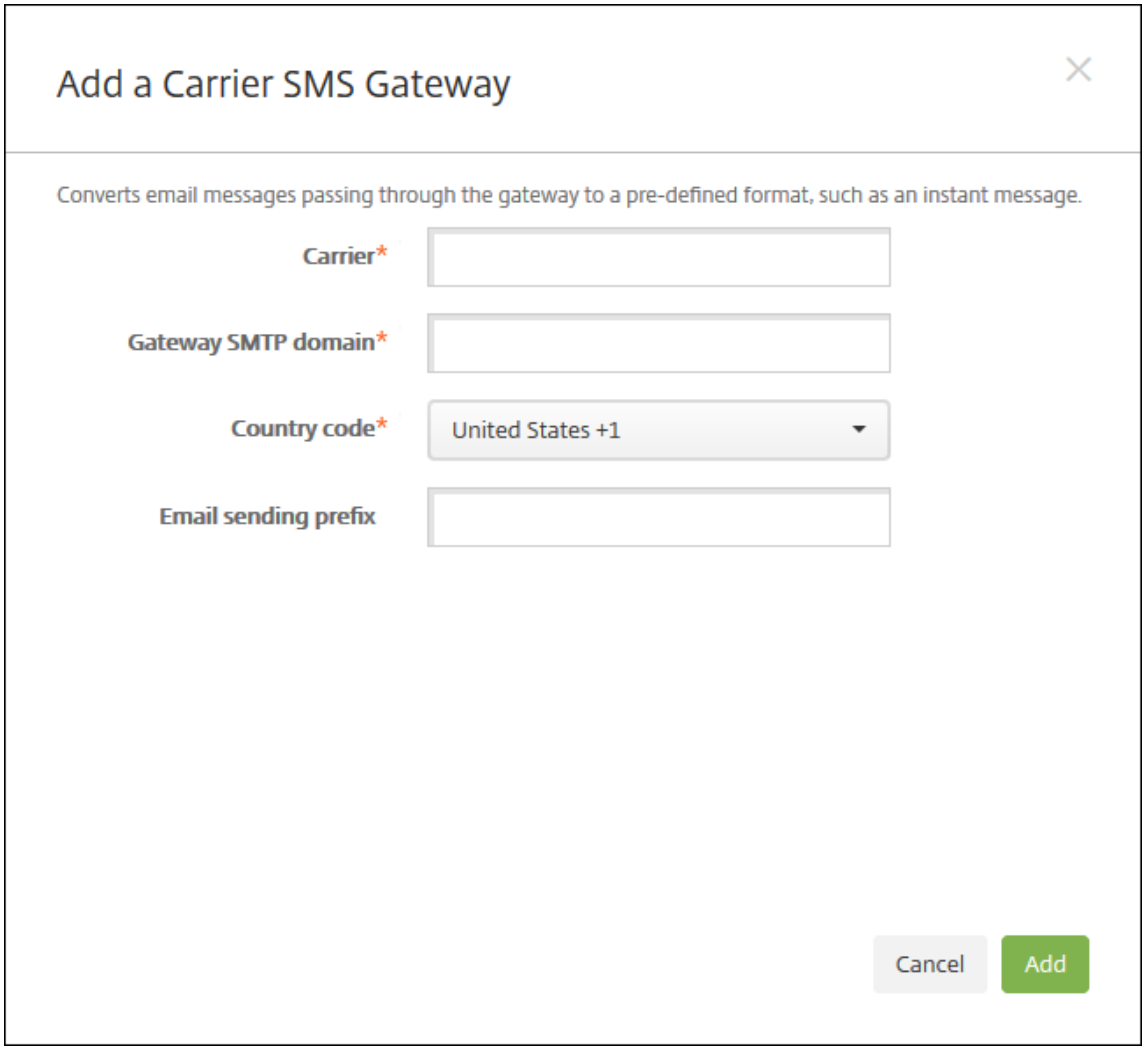
XenMobile 에서이동통신사업자의 SMS 게이트웨이를설정하여이동통신사업자의 SMS 게이트웨이를통해전송되는알림을구성할수있습니다. 이동통신사업자는 SMS(Short Message Service) 게이트웨이를사용하여통신네트워크에서 SMS 전송을보내거나받습니다. 이러한텍스트기반메시지는표준화된통신프로토콜을사용하여유선전화또는휴대폰장치에서 SMS 를교환할수있도록합니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 알림에서 이동통신사업자 **SMS** 게이트웨이를클릭합니다. 이동통신사업자 **SMS** 게이트웨이페이지가열립니다.



3. 다음중하나를수행합니다.

   - 검색을클릭하여자동으로게이트웨이를검색합니다. 새로운이동통신사업자가검색되지않았음을나타내거나등록된장치중에서검색된새이동통신사업자를나열하는대화상자가나타납니다.
   - 추가를클릭합니다. 이동통신사업자 **SMS** 게이트웨이추가대화상자가나타납니다.



> 메모:
>
> XenMobile 은 Nexmo SMS 메시지만지원합니다. Nexmo 메시지사용을위한계정이없는경우 웹사이트를방문하여계정을만드십시오.

4. 다음설정을구성합니다.

   - 이동통신사업자: 이동통신사업자의이름을입력합니다.
   - 게이트웨이 **SMTP** 도메인: SMTP 게이트웨이에연결된도메인을입력합니다.
   - 국가코드: 목록에서이동통신사업자의국가코드를클릭합니다.
   - 전자메일전송접두사: 필요한경우전자메일전송접두사를지정합니다.

5. 추가를클릭하여새이동통신사업자를추가하거나 취소를클릭하여새이동통신사업자를추가하지않습니다.

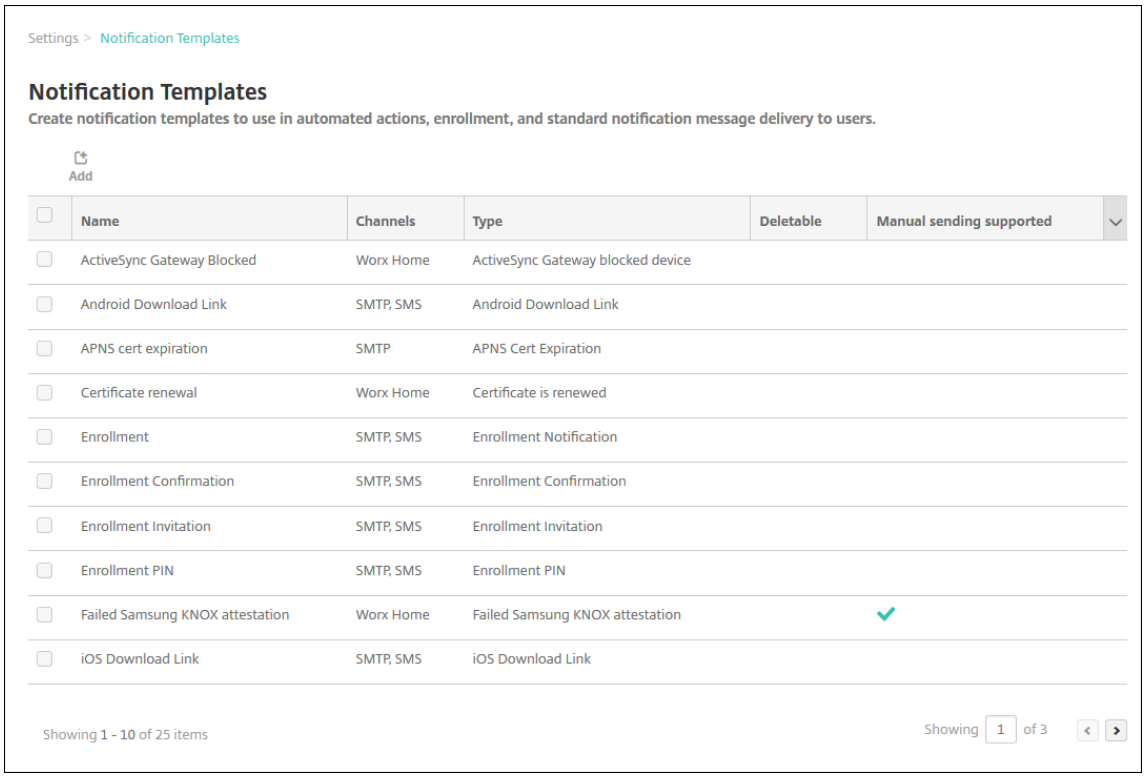
알림템플릿만들기및업데이트

XenMobile 에서자동화동작, 등록및사용자에게보내는표준알림메시지에사용할알림템플릿을만들거나업데이트할수있습니다. 세가지채널 (Secure Hub, SMTP 또는 SMS) 을통해메시지를보내는알림템플릿을구성합니다.

XenMobile 에는시스템의모든장치에자동으로응답하는서로다른이벤트유형을반영하는다수의미리정의된알림템플릿이있습니다.

> 메모:
>
> SMTP 또는 SMS 채널을사용하여사용자에게알림을보내려는경우채널을설정한후활성화해야합니다. 채널이설정되지않은경우알림템플릿을추가할때채널을설정하라는메시지가표시됩니다.

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 알림템플릿을클릭합니다. 알림템플릿페이지가나타납니다.



알림템플릿추가

1. 추가를클릭합니다. SMS 게이트웨이또는 SMTP 서버가설정되지않은경우 SMS 및 SMTP 알림의사용에관한메시지가표시됩니다. SMTP 서버또는 SMS 게이트웨이를지금설정하거나나중에설정하도록선택할수있습니다.

   SMS 또는 SMTP 서버설정을지금설정하도록선택하는경우 설정페이지의 알림서버페이지로리디렉션됩니다. 사용할채널을설정한후 알림템플릿페이지로돌아가서알림템플릿추가또는수정을계속할수있습니다.

> 중요:
>
> SMS 또는 SMTP 서버설정을나중에설정하도록선택하는경우알림템플릿을추가하거나편집할때이러한채널을활성화할수없으므로사용자알림을보낼때이러한채널을사용할수없게됩니다.

2. 다음설정을구성합니다.

   - 이름: 템플릿에대한설명적이름을입력합니다.
   - 설명: 템플릿에대한설명을입력합니다.
   - 유형: 목록에서알림유형을클릭합니다. 선택한유형에대해지원되는채널만표시됩니다. 미리정의된템플릿인 APNS 인증서만료템플릿만허용됩니다. 즉, 이유형의새템플릿을추가할수없습니다.

   > 메모:
   >
   > 일부템플릿유형의경우유형아래에 '수동보내기지원' 이라는구가표시됩니다. 이구는 대시보드및 장치페이지의 알림목록에있는템플릿을사용하여사용자에게수동으로알림을보낼수있음을의미합니다. 모든채널에서제목또는메시지필드에다음매크로를사용하는템플릿에는수동보내기를사용할수없습니다.

   - ${outofcompliance.reason(allowlist_blocklist_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 서버를설정한후에만 SMTP 알림을활성화할수있습니다.

   - 보낸사람: 알림을보낸사람을선택적으로입력합니다. 이름, 전자메일주소또는둘다를입력할수있습니다.
   - 받는사람: 이필드에는올바른 SMTP 받는사람주소로알림이전송되도록임시알림을제외한모든알림에대해미리작성된매크로가포함됩니다. 템플릿의매크로는수정하지않는것이좋습니다. 세미콜론 (;) 으로주소를구분하여사용자외에받는사람을추가할수있습니다 (예: 회사관리자). 임시알림을보내려면이페이지에서특정받는사람을입력하거나 관리 > 장치페이지에서장치를선택하고거기에서알림을보낼수있습니다. 자세한내용은 장치를참조하십시오.
   - 제목: 알림에대한설명적인제목을입력합니다. 이것은필수필드입니다.

- 메시지**:** 사용자에게보낼메시지를입력합니다. 메시지에서매크로를사용하는방법에대한자세한내용은 매크로를참조하십시오.

SMS:

- 활성화**:** 알림채널을사용하려면클릭합니다.

  SMTP 서버를설정한후에만 SMTP 알림을활성화할수있습니다.

- 받는사람**:** 이필드에는올바른 SMS 받는사람주소로알림이전송되도록임시알림을제외한모든알림에대해미리작성된매크로가포함됩니다. 템플릿의매크로는수정하지않는것이좋습니다. 임시알림을보내려면특정받는사람을입력하거나 관리 **>** 장치페이지에서장치를선택할수있습니다.

- 메시지**:** 사용자에게보낼메시지를입력합니다. 이것은필수필드입니다. 메시지에서매크로를사용하는방법에대한자세한내용은 매크로를참조하십시오.

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. 확인대화상자가나타납니다.
3. 삭제를클릭하여알림템플릿을삭제하거나 취소를클릭하여알림템플릿삭제를취소합니다.

장치

January 5, 2022

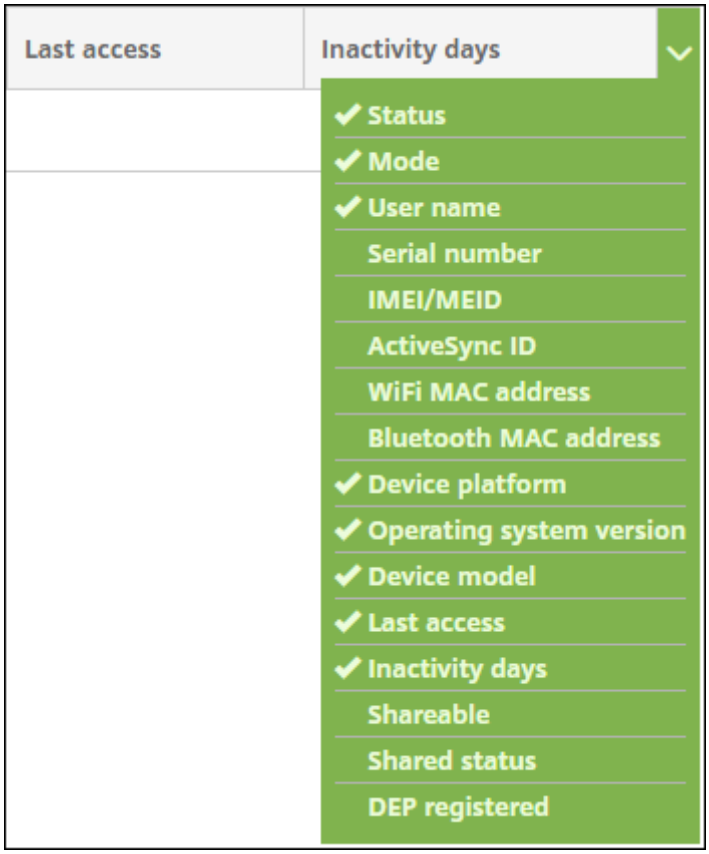
Citrix XenMobile 은단일관리콘솔에서다양한유형의장치를프로비저닝, 관리, 보안및인벤토리를수행할수있습니다.

XenMobile 서버데이터베이스는모바일장치목록을저장합니다. 고유일련번호또는 IMEI(International Mobile Station Equipment Identity)/MEID(Mobile Equipment Identifier) 가각모바일장치를고유하게정의합니다. XenMobile 콘솔에장치를채우려면수동으로장치를추가하거나파일에서장치목록을가져올수있습니다. 장치프로비저닝파일형식에대한자세한내용은이문서뒷부분에서장치프로비저닝파일형식을참조하십시오.

XenMobile 콘솔의 장치페이지에는각장치와다음과같은정보가나열됩니다.

- 상태**:** 장치의탈옥상태, 관리되는상태, Active Sync Gateway 를사용할수있는지여부및배포상태가아이콘으로나타납니다.
- 모드**:** 장치모드가 MDM 또는 MAM 인지, 아니면둘모두인지.
- 사용자이름, 장치플랫폼, 운영체제버전, 장치모델, 마지막액세스및 비활성일수같은장치에대한기타정보. 이러한머리글은기본적으로표시됩니다.

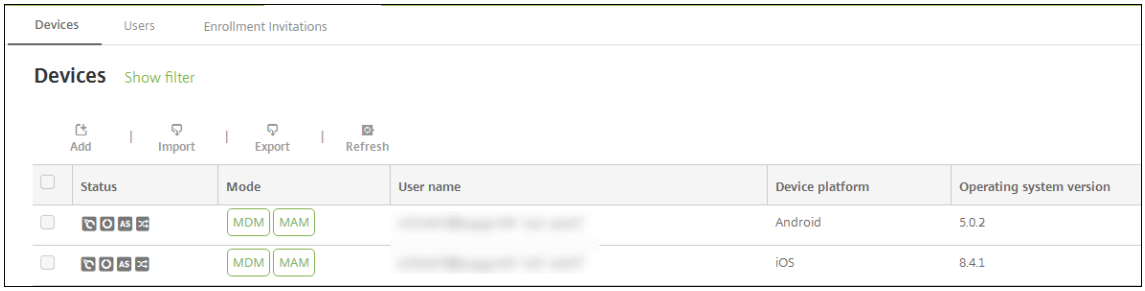
장치테이블을사용자지정하려면마지막머리글의아래쪽화살표를클릭하십시오. 그런다음테이블에표시할추가머리글을선택하거나제거할머리글을선택취소합니다.



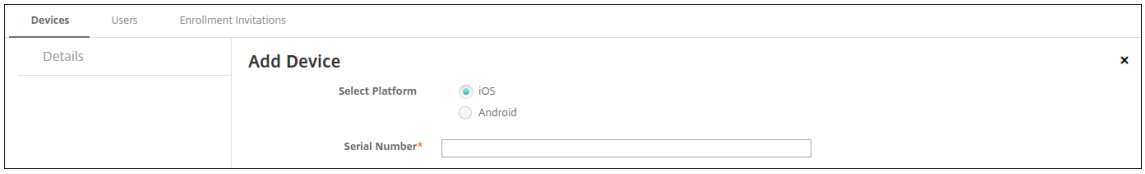
수동으로장치를추가하고, 장치프로비저닝파일에서장치를가져오고, 장치세부정보를편집하고, 보안작업을수행하고, 장치에알림을보낼수있습니다. 모든장치테이블데이터를.csv 파일로내보내사용자지정보고서를만들수도있습니다. 서버는모든장치특성을내보냅니다. 필터를적용한경우.csv 파일을만들때 XenMobile 이필터를사용합니다.

수동으로장치추가

1. XenMobile 콘솔에서 관리 **>** 장치를클릭합니다. 장치페이지가나타납니다.



2. 추가를클릭합니다. 장치추가페이지가나타납니다.



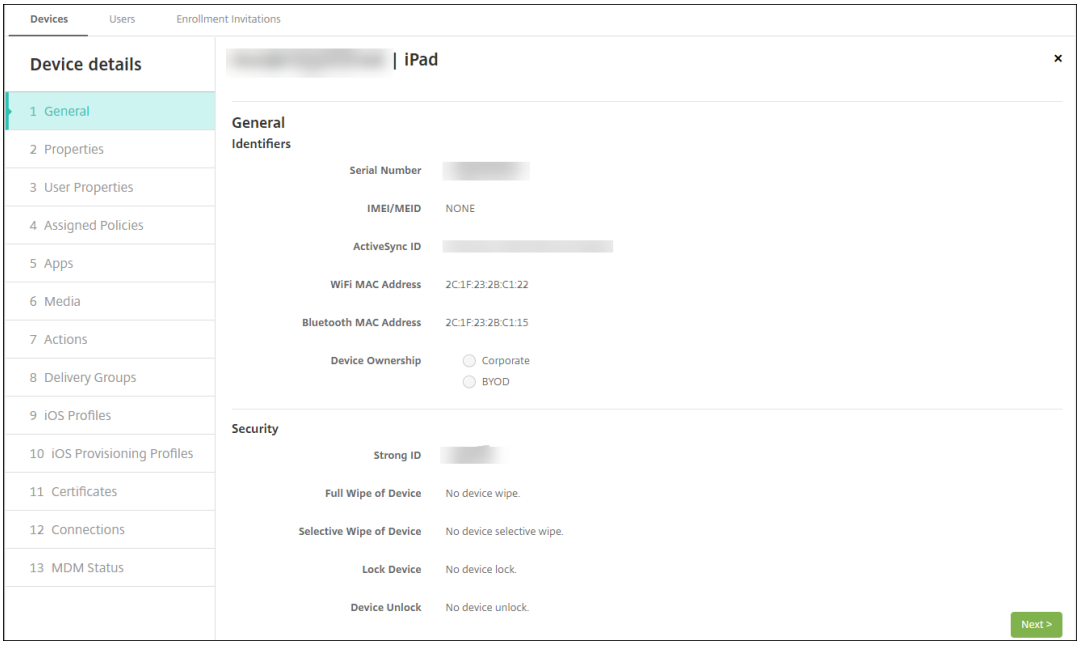
3. 다음설정을구성합니다.

   - 플랫폼선택**: iOS** 또는 **Android** 를클릭합니다.
   - 일련번호**:** 장치일련번호를입력합니다.
   - **IMEI/MEID:** Android 장치에만해당하며, 필요한경우장치 IMEI/MEID 정보를입력합니다.

4. 추가를클릭합니다. 장치테이블이나타나고목록맨아래에장치가추가되어있습니다. 추가한장치를선택한다음나타나는메뉴에서 편집을클릭하여장치세부정보를보고확인합니다.

   > 참고**:**
   >
   > 장치옆에있는확인란을선택하면장치목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.

   - 엔터프라이즈 (XME) 또는 MDM 모드로구성된 XenMobile Server
   - 구성된 LDAP
   - 로컬그룹및로컬사용자를사용중인경우:
     - 하나이상의로컬그룹.
     - 로컬그룹에할당된로컬사용자.
     - 배달그룹은로컬그룹과연결됩니다.
   - Active Directory 를사용중인경우:
     - 배달그룹은 Active Directory 그룹과연결됩니다.



5. 일반페이지에는일련번호, ActiveSync ID 및플랫폼유형에대한기타정보같은장치 식별자가나열됩니다. 장치소유권의경우 회사또는 **BYOD** 를선택합니다.

   일반페이지에는강력한 ID, 장치잠금, 활성화잠금바이패스및플랫폼유형에대한기타정보같은장치 보안속성도나열됩니다. 장치전체초기화필드에는사용자 PIN 코드가포함됩니다. 장치가초기화된후사용자는이코드를입력해야합니다. 사용자가코드를잊은경우여기서코드를조회할수있습니다.

6. 속성페이지에는 XenMobile 이프로비저닝할장치속성이나열됩니다. 이목록에는장치를추가하는데사용된프로비저닝파일에포함된모든장치속성이표시됩니다. 속성을추가하려면 추가를클릭한다음목록에서속성을선택합니다. 각속성에유효한값에대해서는 장치속성이름및값 PDF 를참조하십시오.

   속성을추가하면처음에는속성을추가한범주아래에나타납니다. 다음을클릭한후 속성페이지로돌아가면속성이해당목록에나타납니다.

   속성을삭제하려면목록위에마우스포인터를이동하고오른쪽에있는 **X** 를클릭합니다. 항목이즉시삭제됩니다.

7. 나머지 장치세부정보섹션에는장치에대한요약정보가포함되어있습니다.

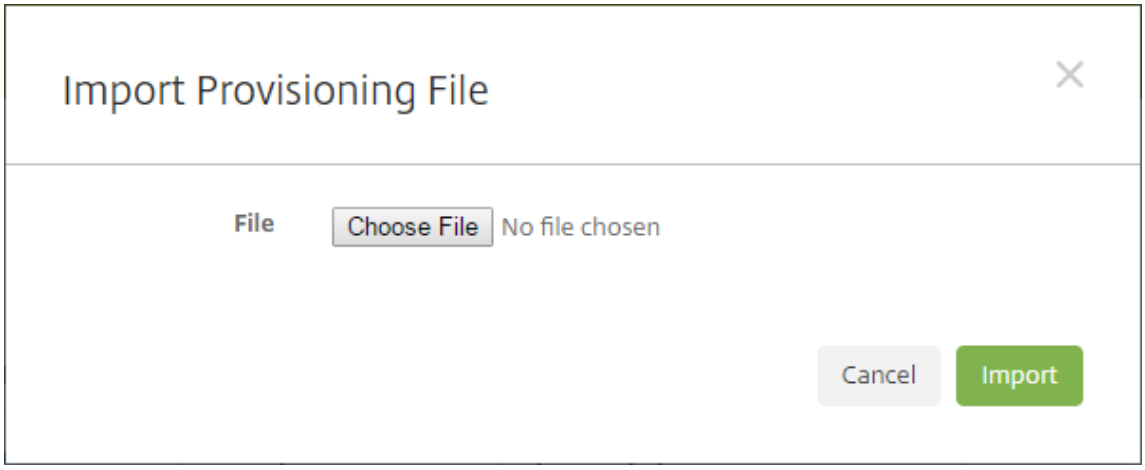
   - 사용자속성**:** RBAC 역할, 그룹구성원자격, 볼륨구매계정및사용자속성을표시합니다. 이페이지에서볼륨구매계정을사용중지할수있습니다.
   - 할당된정책**:** 배포된정책, 보류중인정책및실패한정책의수를포함하여할당된정책의수를표시합니다. 각정책에대해정책이름, 유형및마지막배포정보를제공합니다.
   - 앱**:** 마지막인벤토리에대한설치된앱배포, 보류중인앱배포및실패한앱배포의수를표시합니다. 앱이름, 식별자, 유형및기타정보를제공합니다.
   - 미디어**:** 마지막인벤토리에대해배포된미디어배포, 보류중인미디어배포및실패한미디어배포의수를표시합니다.
   - 동작**:** 배포된동작, 보류중인동작및실패한동작의수를표시합니다. 마지막배포의동작이름및시간을제공합니다.
   - 배달그룹**:** 성공한배달그룹, 보류중인배달그룹및실패한배달그룹의수를표시합니다. 각배포에대해배달그룹이름및배포시간을제공합니다. 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.

프로비저닝파일에서장치가져오기

이동통신사업자또는장치제조업체가제공한파일을가져오거나고유한장치프로비저닝파일을만들수있습니다. 자세한내용은이문서뒷부분에서장치프로비저닝파일형식을참조하십시오.

1. 관리 **>** 장치로이동하여 가져오기를클릭합니다. 프로비저닝파일가져오기대화상자가나타납니다.

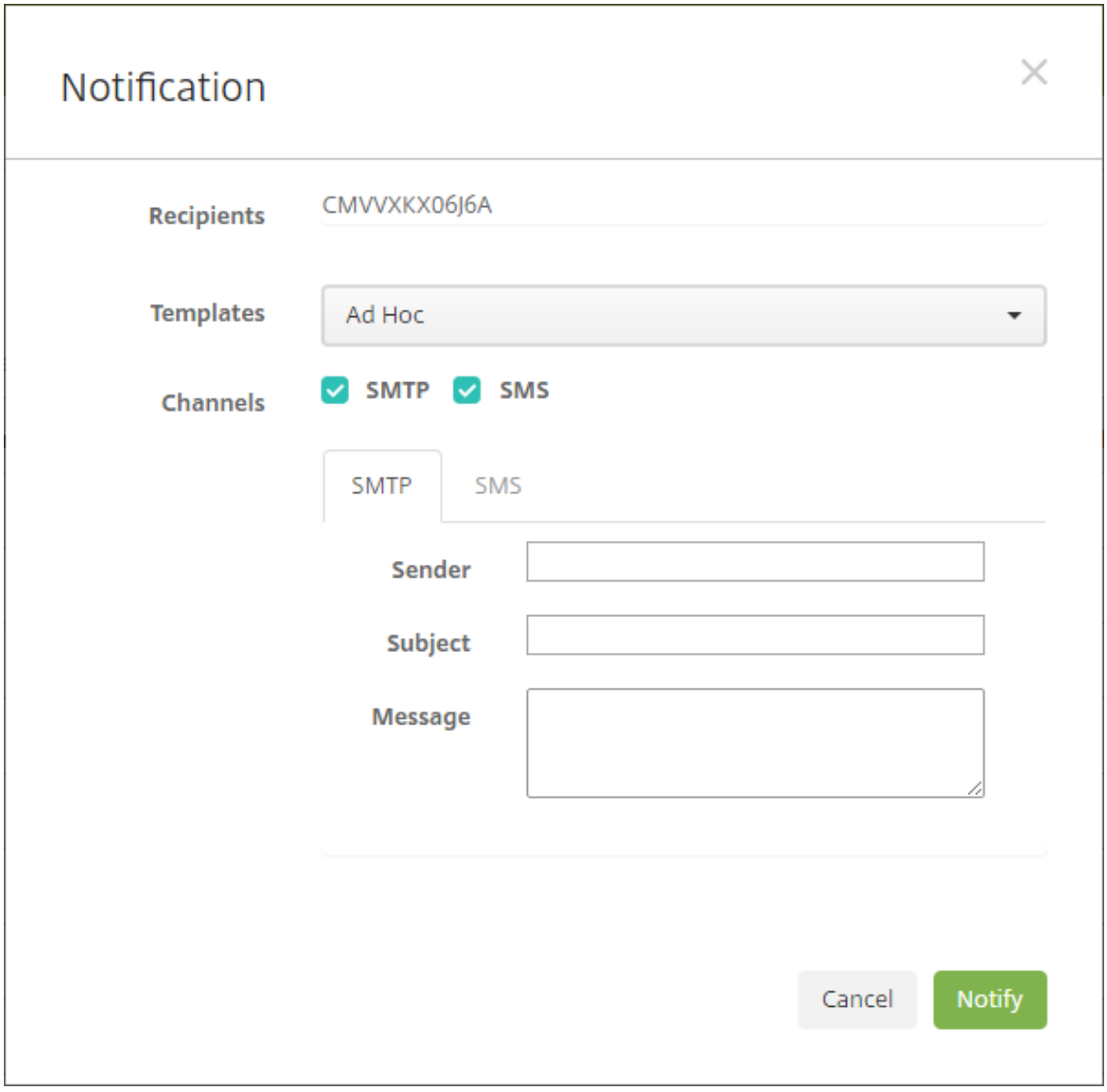


2. 파일선택을클릭한다음가져오려는파일을찾습니다.
3. 가져오기를클릭합니다. 장치테이블에가져온파일이나열됩니다.
4. 장치정보를편집하려면장치를선택한다음 편집을클릭합니다. 장치세부정보페이지에대한자세한내용은수동으로장치추가를참조하십시오.

장치에알림보내기

장치페이지에서장치에알림을보낼수있습니다. 알림에대한자세한내용은 알림을참조하십시오.

1. 관리 **>** 장치페이지에서알림을보낼하나이상의장치를선택합니다.
2. 알림을클릭합니다. 알림대화상자가나타납니다. 받는사람필드에알림을받을모든장치가나열됩니다.



3. 다음설정을구성합니다.
   - 템플릿**:** 목록에서보내려는알림을유형을클릭합니다. 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.

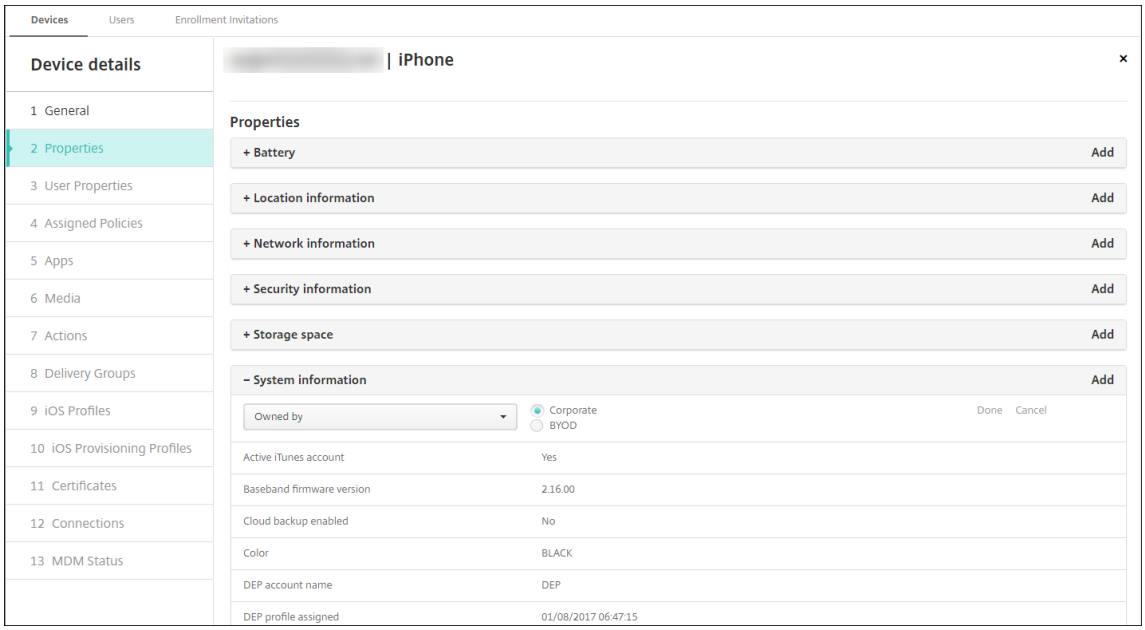
사용자장치에수동으로태그지정

다음과같은방법으로 XenMobile 에서장치에수동으로태그를지정할수있습니다.

- 초대기반등록프로세스도중
- 자가지원포털등록프로세스도중
- 장치소유권을장치속성으로추가

장치에회사소유또는직원소유태그를지정하는옵션도있습니다. 자가지원포털을사용하여장치를자가등록할때장치에회사소유또는직원소유태그를지정할수있습니다. 다음과같이장치에수동으로태그를지정할수도있습니다.

1. XenMobile 콘솔의 장치탭에서장치에속성을추가합니다.
2. 이름이 소유자인속성을추가하고 회사또는 **BYOD**(직원소유) 중에서선택합니다.



장치프로비저닝파일형식

여러모바일운영자또는장치제조업체에서인증된모바일장치의목록을제공합니다. 이러한목록을사용하면긴모바일장치목록을수동으로입력할필요가없습니다. XenMobile 은지원되는세가지장치유형 (Android, iOS 및 Windows) 모두에공통되는가져오기파일형식을지원합니다.

수동으로만들며장치를 XenMobile 로가져오기위해사용하는프로비저닝파일은다음과같은형식이어야합니다.

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:

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;
4050BF3F5173010816100655105903 93;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

파일의각줄은장치하나를기술합니다. 위샘플에서첫번째항목은다음과같은의미입니다.

- SerialNumber: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- PropertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

ActiveSync Gateway

December 1, 2020

ActiveSync 는 Microsoft 에서개발한모바일데이터동기화프로토콜입니다. ActiveSync 는핸드헬드장치및데스크톱 (또는랩톱) 컴퓨터와데이터를동기화합니다.

XenMobile 에서 ActiveSync Gateway 규칙을구성할수있습니다. 이러한규칙에따라장치에서 ActiveSync 데이터에대한액세스를허용하거나거부할수있습니다. 예를들어누락된필수앱규칙을활성화하면 XenMobile 은필수앱에대해앱액세스정책을확인하고필수앱이누락된경우 ActiveSync 데이터에대한액세스를거부합니다. 각규칙에대해 허용또는 거부중하나를선택할수있습니다. 기본설정은 허용입니다.

앱액세스장치정책에대한자세한내용은 앱액세스장치정책을참조하십시오.

XenMobile 은다음규칙을지원합니다.

익명장치**:** 장치가익명모드인지확인합니다. 이확인은장치가다시연결할때 XenMobile 이사용자를다시인증할수없는경우사용할수있습니다.

Samsung KNOX 증명실패**:** 장치가 Samsung KNOX 증명서버의쿼리에실패했는지확인합니다.

금지된앱**:** 장치에앱액세스정책에정의된금지된앱이있는지확인합니다.

암시적허용및거부**:** 이동작이 ActiveSync Gateway 의기본값입니다. 게이트웨이는다른필터규칙기준을충족시키지않는모든장치의장치목록을만들고해당목록을기반으로연결을허용하거나거부합니다. 일치하는규칙이없으면기본값은암시적허용입니다.

비활성장치**:** 서버속성의장치비활성일수임계값설정에정의된대로장치가비활성상태인지확인합니다.

누락된필수앱**:** 앱액세스정책에정의된대로, 장치에필수앱이누락되었는지확인합니다.

비추천앱**:** 앱액세스정책에정의된대로, 장치에비추천앱이있는지확인합니다.

규정을준수하지않는암호**:** 사용자암호가규정을준수하는지확인합니다. iOS 및 Android 장치에서 XenMobile 은현재장치에있는암호가장치로보낸암호정책을준수하는지여부를확인할수있습니다. 예를들어 iOS 에서는 XenMobile 이암호정책을장치에보내는경우 60 분내에암호를설정해야합니다. 사용자가암호를설정하기전에암호가규정을준수하지않을수있습니다.

규정위반장치**:** 규정위반장치속성에따라장치가규정을위반하는지여부를확인합니다. 이속성은대개자동화된동작이나 XenMobile API 를활용하는제 3 자에의해변경됩니다.

해지된상태**:** 장치인증서가해지되었는지여부를확인합니다. 해지된장치는다시권한이부여될때까지다시등록할수없습니다.

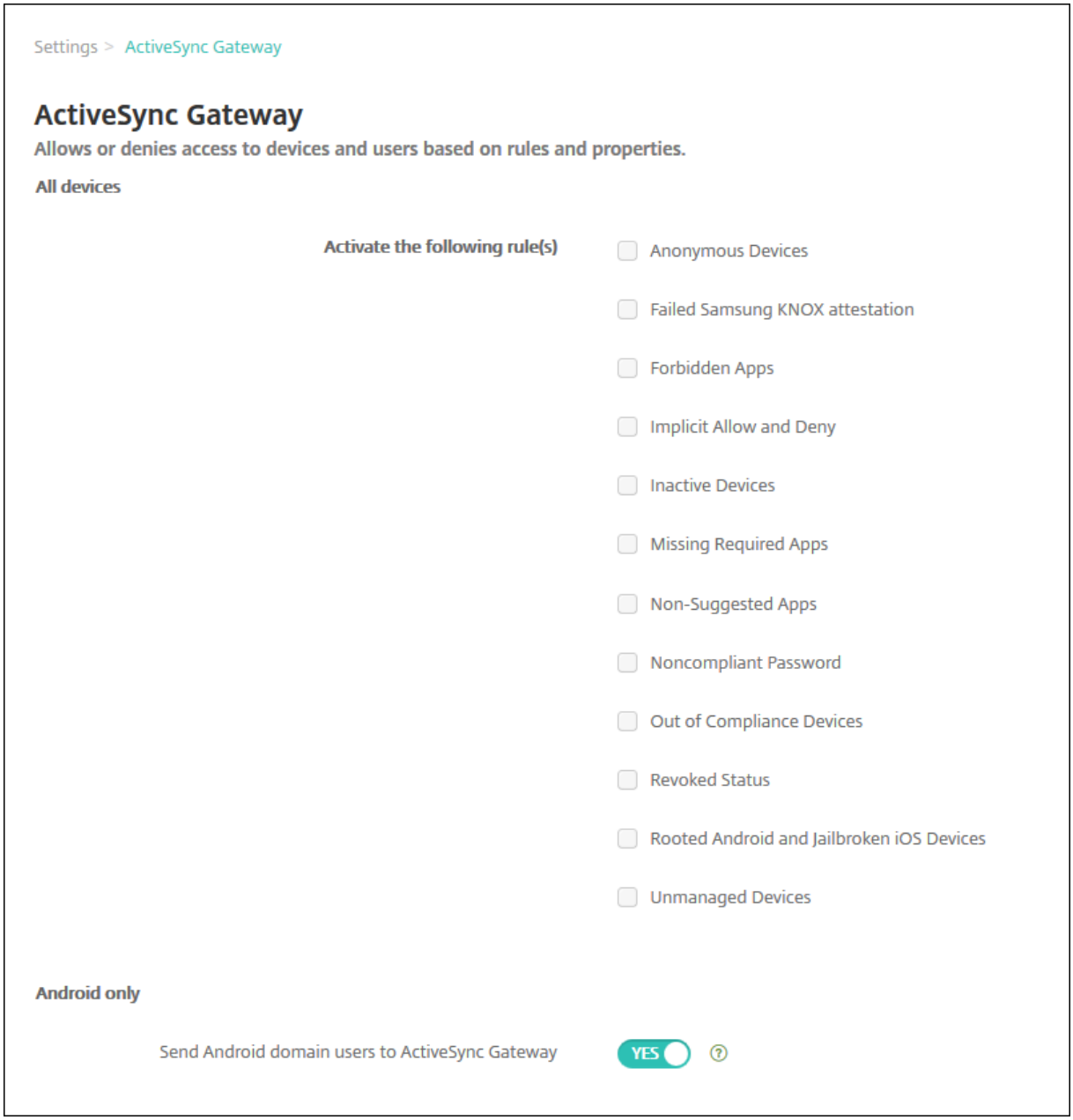
루팅된 **Android** 및탈옥 **iOS** 장치**:** Android 또는 iOS 장치가탈옥되어있는지확인합니다.

관리되지않는장치**:** 장치가여전히 XenMobile 제어하에관리되는상태에있는지확인합니다. 예를들어 MAM 로등록된장치나등록되지않은장치는관리되지않습니다.

Android 도메인사용자를 **ActiveSync Gateway** 로보내기**:** XenMobile 이 Android 장치정보를 ActiveSync Gateway 로보내도록하려면 예를클릭합니다.

ActiveSync Gateway 설정을구성하려면

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버아래에서 **ActiveSync Gateway** 를클릭합니다. **ActiveSync Gateway** 페이지가나타납니다.



1. **Activate the following rules(**다음규칙활성화**)** 에서활성화하려는하나이상의규칙을선택합니다.
2. **Android** 만의 **Android** 도메인사용자를 **ActiveSync Gateway** 로보내기에서 예를클릭하여 XenMobile 이 Android 장치정보를 ActiveSync Gateway 로보내도록합니다.
3. 저장을클릭합니다.

장치관리에서 **Android Enterprise** 로마이그레이션

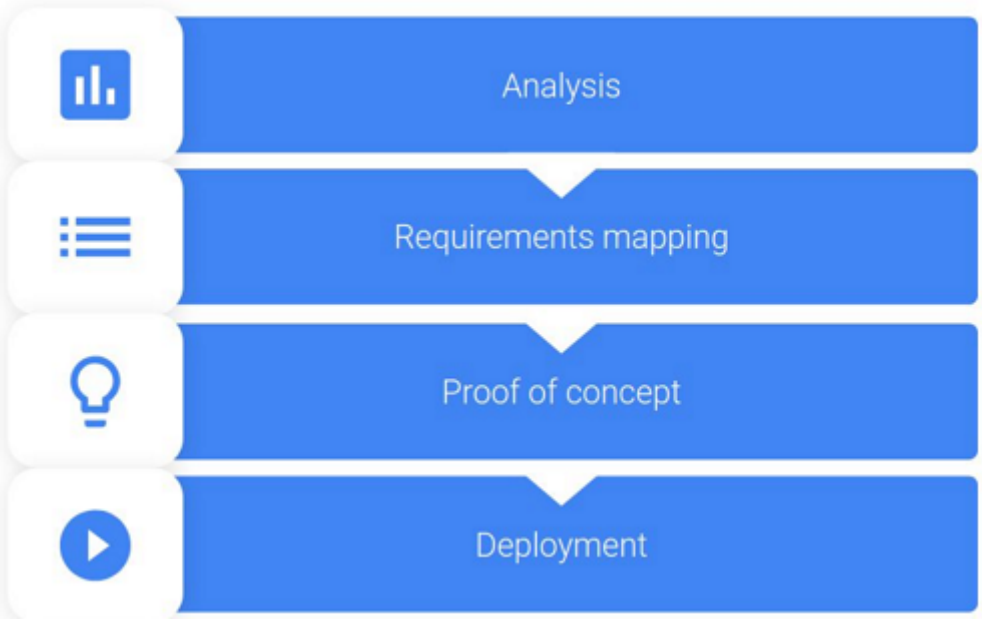
January 5, 2022

이문서에서는레거시 Android 장치관리에서 Android Enterprise 로마이그레이션할때의고려사항및권장사항에대해설명합니다. 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 마이그레이션지침서에레거시장치관리와 Android Enterprise 의차이점이자세히설명되어있습니다. Google 에서마이그레이션정보를읽어보시기바랍니다.

또한이게시물은장치관리마이그레이션의 4 단계에대해설명하며다음다이어그램을포함하고있습니다. 이문서에는마이그레이션단계에서 XenMobile 과관련된권장사항이포함되어있습니다.



> Android Enterprise 마이그레이션 지침서의다이어그램.
> Google 의허가하에다시게시되었습니다.

장치관리사용중단의영향

Google 은다음장치관리 API 의사용을중단할예정입니다. Android Q API 수준을대상으로 Secure Hub 를업그레이드한후에는 Android Q 를실행하는장치에서이러한 API 가작동하지않습니다.

- 카메라사용안함: 장치카메라에대한액세스를제어합니다.
- 암호만료: 구성가능한기간이지난후사용자에게암호를변경하도록강제합니다.
- 암호제한: 제한적인암호요구사항을설정합니다.

API 사용중단은 Citrix MAM 전용모드에등록된장치에는영향을주지않습니다.

권장사항

다음은 Android 레거시장치관리모드에이미등록된장치, 등록되지않은장치및 Citrix MAM 전용모드에등록된장치에대한권장사항입니다.

장치등록상태	권장작업
기존장치가장치관리모드에등록되었으며 Android Q 로업그레이드할수있습니다.	장치를 Android Q 로업그레이드하기전에장치관리모드에서 Android Enterprise 로마이그레이션하십시오.
기존장치가장치관리모드로등록되어있습니다. 장치를 Android Q 로업그레이드할수없습니다.	장치를장치관리모드로유지할수있습니다. 그러나장치새로고침시 Android Enterprise 로장치를이동할계획을세우십시오.
기존장치가장치관리모드에등록되었으며 Android Q 로업그레이드되었습니다.	Google 이 API 의사용을중단하기전에장치관리모드에서 Android Enterprise 로마이그레이션하십시오. XenMobile 콘솔에이러한장치에대한경고메시지가나타납니다.
새로운장치가 Android Q 와함께제공되었고장치관리모드에등록되었습니다.	Google 이 API 의사용을중단하기전에장치관리모드에서 Android Enterprise 로마이그레이션하십시오. XenMobile 콘솔에이러한장치에대한경고메시지가나타납니다.
Android Q 와함께제공되거나업그레이드할수있는새장치입니다. 장치는등록되지않았습니다.	모든새로운장치에대해 Android Enterprise 를사용하십시오.
Android Q 의새장치또는기존장치는 Google 이 API 의사용을중단한후장치관리모드에등록됩니다.	Google API 사용중단의영향을방지하려면 Google 에서 API 사용을중단하기전에 Android Enterprise 로마이그레이션하는것이좋습니다. 이날짜이후에는이러한장치의등록이실패합니다.
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: 공장기본값으로재설정해야합니다. QR 코드, NFC(근거리통신) 범프, DPC(장치정책컨트롤러) 식별자, 제로터치를사용하여장치를등록합니다.

2. 앱마이그레이션전략을만듭니다.
3. 사용사례요구사항을 Android Enterprise 기능에매핑합니다. 요구사항및해당 Android 버전과가장일치하는각장치요구사항에대한기능을문서화합니다.
4. 기능요구사항에따라최소 Android OS(7.0, 8.0, 9.0) 를결정합니다.
5. ID 모델을선택합니다.
   - 권장: 관리되는 Google Play 계정
   - Google Cloud Identity 고객인경우에만 Google G-Suite 계정사용
6. 장치전략만들기:
   - 작업없음: 장치가최소 OS 수준을충족하는경우
   - 업그레이드: 장치가지원되고지원되는 OS 로업데이트할수있는경우
   - 교체: 장치를지원되는 OS 수준으로업데이트할수없는경우

권장되는앱마이그레이션전략

요구사항매핑을완료한후 Android 플랫폼에서 Android Enterprise 플랫폼으로앱을이동합니다. 앱게시에대한자세한내용은 앱추가를참조하십시오.

- 공용스토어앱
  1. 마이그레이션할앱을선택한다음앱을편집하여 Google Play 설정을지우고 **Android Enterprise** 를플랫폼으로선택합니다.
  2. 배달그룹을선택합니다. 앱이필수인경우앱을배달그룹의 필수앱목록으로이동합니다.

  앱을저장하면 Google Play Store 에나타납니다. 작업프로필이있는경우 Google Play Store 의작업프로필에앱이표시됩니다.
- 비공개 (엔터프라이즈) 앱

  비공개앱은사내에서개발하거나타사개발자가개발합니다. Google Play 를사용하여비공개앱을게시하는것이좋습니다.
  1. 마이그레이션할앱을선택한다음앱을편집하여 **Android Enterprise** 를플랫폼으로선택합니다.
  2. APK 파일을업로드한다음앱설정을구성합니다.
  3. 앱을필수배달그룹에게시합니다.
- MDX 앱
  1. 마이그레이션할앱을선택한다음앱을편집하여 **Android Enterprise** 를플랫폼으로선택합니다.
  2. MDX 파일을업로드합니다. 앱승인프로세스를진행합니다.

3. MDX 정책을선택합니다.

Enterprise MDX 앱의경우 MDX SDK 모드래핑된앱으로변경하는것이좋습니다.

- 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.

- 이시나리오에서사용자는현재구성으로계속해서레거시장치를사용합니다. 관리자는 Android Enterprise 관리를위한새장치를설정합니다.
- 기존장치는업그레이드또는교체가필요한경우에만마이그레이션합니다.
- 일반적인수명주기가끝나면기존장치를 Android Enterprise 관리로마이그레이션합니다. 또는손실이나파손으로인해교체가필요한경우이러한장치를마이그레이션할수있습니다.

Android Enterprise

May 6, 2022

Android Enterprise 는 Google 이 Android 장치를위한엔터프라이즈관리솔루션으로제공하는도구및서비스집합입니다. Android Enterprise 에서:

- XenMobile 을사용하여회사소유의 Android 장치와 BYOD(bring your own device) Android 장치를관리합니다.
- 전체장치를관리하거나장치의개별프로필을관리할수있습니다. 개별프로필은개인계정, 앱및데이터로부터비즈니스계정, 앱및데이터를분리합니다.
- 또한인벤토리관리와같은일회성전용장치를관리할수도있습니다. Google 의 Android Enterprise 기능에대한개요는 Android Enterprise 관리를참조하십시오.

리소스:

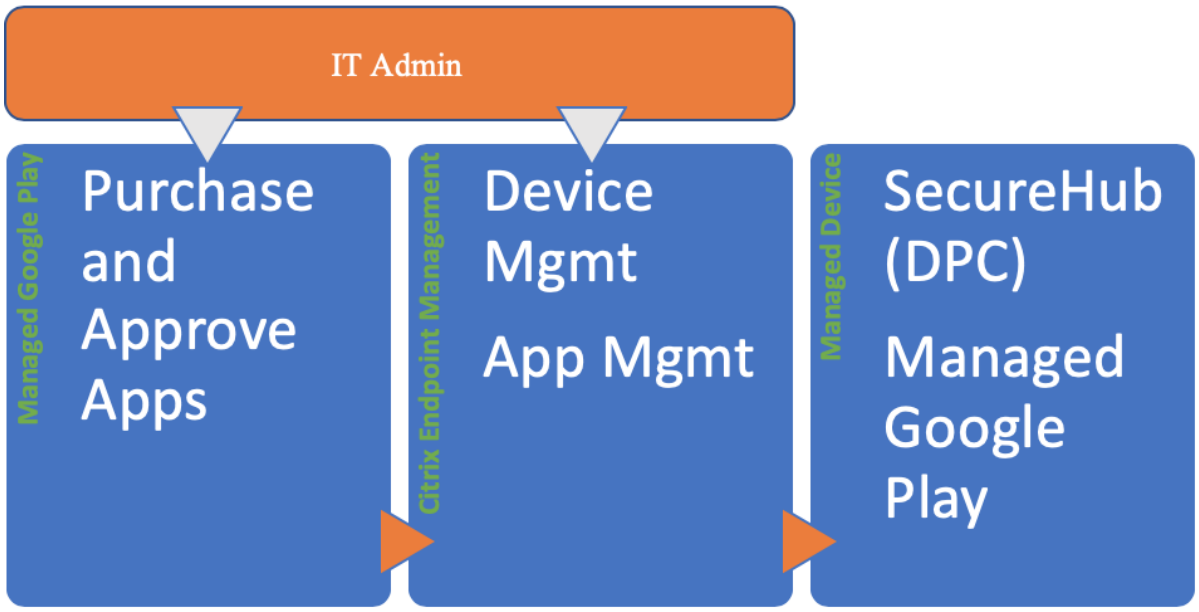
- Android Enterprise 와관련된용어및정의목록은 Google Android Enterprise 개발자가이드에서 Android Enterprise 용어를참조하십시오. Google 은이러한용어를자주업데이트합니다.
- XenMobile 에대해지원되는 Android 운영체제는 지원되는기기운영체제를참조하십시오.
- Android Enterprise 를위한네트워크환경을설정할때고려해야할아웃바운드연결에대한자세한내용은 Google 지원문서 Android Enterprise 네트워크요구사항을참조하십시오.

XenMobile 을관리되는 Google Play 와통합하여 Android Enterprise 를사용하는경우엔터프라이즈를만들게됩니다. Google 에서는엔터프라이즈를조직과 EMM(엔터프라이즈모바일관리) 솔루션간의바인딩으로정의합니다. 조직에서솔루션을통해관리하는모든사용자및장치는해당엔터프라이즈에속합니다.

Android Enterprise 의엔터프라이즈에는 EMM 솔루션, DPC(장치정책컨트롤러) 앱및 Google 엔터프라이즈앱플랫폼의세가지구성요소가있습니다. XenMobile 을 Android Enterprise 와통합하는경우전체솔루션에는다음과같은구성요소가포함됩니다.

- **XenMobile:** Citrix EMM 입니다. XenMobile 은안전한디지털작업공간을위한통합 XenMobile 솔루션입니다. 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 엔터프라이즈앱플랫폼입니다. Google Play EMM API 는앱정책을설정하고앱을배포합니다.

다음그림은관리자가이러한구성요소와상호작용하는방식과구성요소가서로상호작용하는방식을보여줍니다.



XenMobile 에서관리되는 **Google Play** 사용

> 참고:
>
> 관리형 Google Play 또는 Google Workspace 를사용하여 Citrix 를 EMM 공급자로등록할수있습니다. 이문서에서는관리되는 Google Play 와함께 Android Enterprise 를사용하는방법에대해설명합니다. 조직에서 Google Workspace 를사용하여앱에대한액세스를제공하는경우 Android Enterprise 를함께사용할수있습니다. Google Workspace 고객을위한레거시 Android Enterprise(이전명칭 G Suite)를참조하십시오.

관리되는 Google Play 를사용하는경우장치와최종사용자에게관리형 Google Play 계정을프로비전합니다. 관리되는 Google Play 계정을통해사용자가관리되는 Google Play 에액세스하여제공되는앱을설치하고사용할수있습니다. 조직에서타사 ID 서비스를사용하는경우관리형 Google Play 계정을기존 ID 계정과연결할수있습니다.

이유형의엔터프라이즈는도메인에연결되지않으므로단일조직에대해둘이상의엔터프라이즈를만들수있습니다. 예를들어조직내의각부서또는리전을서로다른엔터프라이즈로등록하여별도의장치및앱집합을관리할수있습니다.

관리되는 Google Play 는 XenMobile 관리자에게 Google Play 의사용자환경및앱스토어기능과함께기업을위해설계된관리기능을제공합니다. 관리형 Google Play 를사용하여장치의 Android Enterprise 작업공간에배포할앱을추가, 구매및승인합니다. Google Play 를사용하여공용앱, 개인앱및타사앱을배포할수있습니다.

관리되는장치의사용자에게있어서관리되는 Google Play 는엔터프라이즈앱스토어입니다. 사용자는앱을탐색하고, 앱세부정보를보고, 앱을설치할수있습니다. 공개버전의 Google Play 와달리관리형 Google Play 에서는사용자에게별도로제공되는앱만설치할수있습니다.

장치배포시나리오및작동모드

장치배포시나리오는배포한장치의소유자와장치의관리방법을나타냅니다. 장치프로필은 DPC 가장치에서정책을관리하고실행하는방식을나타냅니다.

작업프로필은개인계정, 앱및데이터로부터비즈니스계정, 앱및데이터를분리합니다. 작업프로필에대한자세한내용은 Google Android Enterprise 도움말항목 작업프로필이란무엇인가요를참조하십시오.

> 중요:
>
> Android 11 으로 Android Enterprise 장치를업데이트할경우 Google 은 "작업프로필로완전히관리" 로관리되는장치를보안이강화된신규작업프로필환경으로마이그레이션합니다. 자세한내용은 Android Enterprise 의작업프로필로완전히관리에예정된변경사항을참조하십시오.

장치관리	사용사례	작업프로필	개인프로필	참고
기업소유장치 (완전관리형)	작업전용인기업소유장치	아니요	예. DPC 는장치전체연결구성, 글로벌설정구성및공장기본값으로재설정과같은장치전체작업을수행할수있습니다.	신규또는공장기본값재설정장치전용입니다.
작업프로필로완전히관리	작업및개인용기업소유장치	예	예. 이러한장치에서는 DPC 의복사본 2 개가실행됩니다. 하나는장치소유자모드에서장치를관리하고다른하나는프로필소유자모드에서작업프로필을관리합니다. 장치와작업프로필에개별정책을적용할수있습니다.	이전에는 COPE(회사소유의개인사용) 장치라고했습니다.
전용장치 *	디지털사이니지또는티켓인쇄와같이단일사용사례를위해구성된회사소유장치	아니요	예. 필수앱만제공하고사용자가다른앱을추가하지못하도록합니다.	이전에는 COSU(회사소유일회사용) 장치라고했습니다.

장치관리	사용사례	작업프로필	개인프로필	참고
BYOD 작업프로필 **	작업프로필모드로등록된개인장치 (이전에는프로필소유자모드라고도함)	예	예. DPC 는전체장치가아닌작업프로필만관리합니다.	이러한장치가새장치이거나공장기본값으로재설정될필요는없습니다.

* 사용자는전용장치를공유할수있습니다. 사용자가전용장치에서앱에로그인하면작업상태는장치가아닌앱에대한상태가됩니다.

** XenMobile 은 BYOD 작업프로필모드에서와같이 Zebra 장치를지원하지않습니다. XenMobile 은 Zebra 장치를완전관리형장치및장치레거시모드 (장치관리모드라고도함) 로지원합니다.

레거시모드에서장치소유자또는프로필소유자모드로마이그레이션하는방법에대한자세한내용은 기기관리에서 Android Enterprise 로마이그레이션을참조하십시오.

인증방법

등록프로필은사용자가 MDM 을취소할수있는옵션과함께 Android 장치가 MAM, MDM 또는 MDM+MAM 으로등록되는지여부를결정합니다.

보안수준및필요한등록단계에대한정보는 등록보안모드구성을참조하십시오.

XenMobile 은 MDM+MAM 으로등록된 Android 장치에대해다음과같은인증방법을지원합니다. 자세한내용은 인증서및인증에있는문서를참조하십시오.

- 도메인
- 도메인및보안토큰
- 클라이언트인증서
- 클라이언트인증서와도메인
- ID 공급자:
  - Azure Active Directory
  - Citrix ID 공급자

거의사용되지않는또다른인증방법은클라이언트인증서와보안토큰입니다. 자세한내용은 https://support.citrix.com/article/CTX215200에서참조하십시오.

요구사항

Android Enterprise 사용을시작하기전에다음이필요합니다.

- 계정및자격증명:
  - 관리되는 Google Play 로 Android Enterprise 를설정하려면회사의 Google 계정
  - 최신 MDX 파일을다운로드하려면 Citrix 고객계정

  - 개인앱을배포하려면 (선택사항) Google 개발자계정

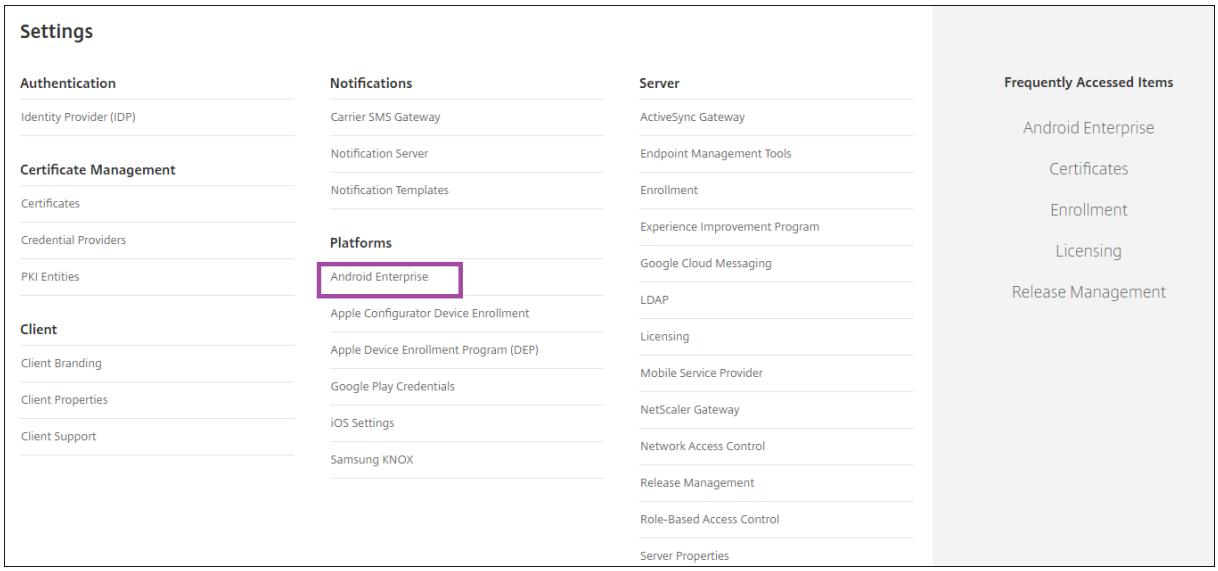
- XenMobile 에대해구성된 Firebase Cloud Messaging(FCM) 지침은 Firebase Cloud Messaging을참조하십시오.
- Samsung Knox 모바일등록 (선택사항) 의경우 Knox 프리미엄라이센스

Google Play 에 **XenMobile** 연결

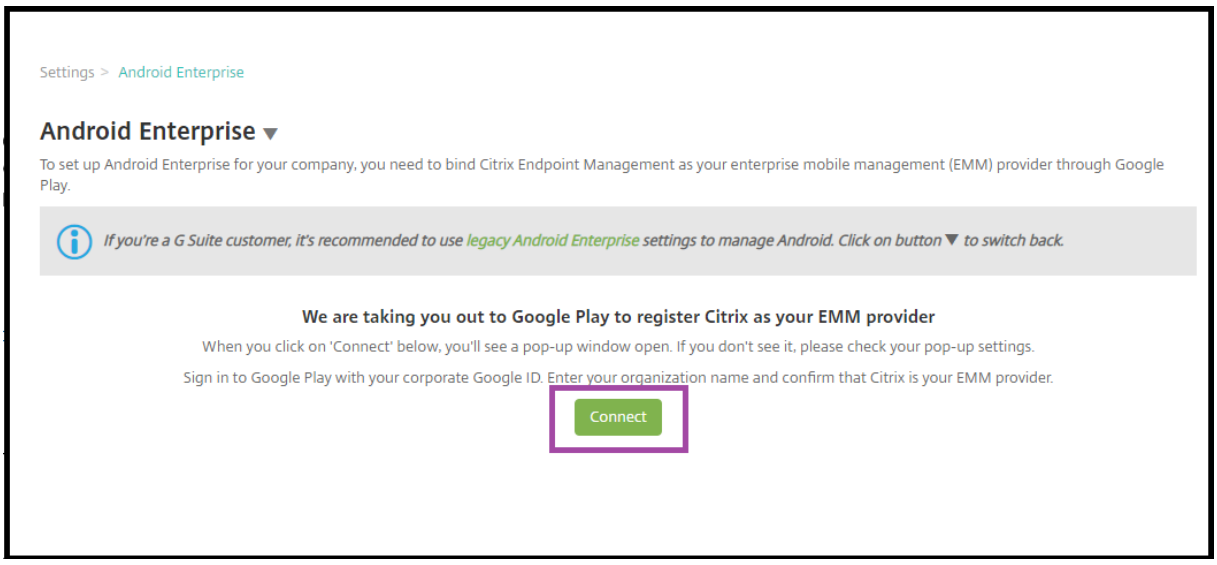
조직에대한 Android Enterprise 를설정하려면관리되는 Google Play 를통해 Citrix 를 EMM 공급자로등록합니다. 이설정은관리되는 Google Play 를 XenMobile 에연결하고 XenMobile 에 Android Enterprise 의엔터프라이즈를만듭니다.

Google Play 에로그인하려면회사 Google 계정이필요합니다.

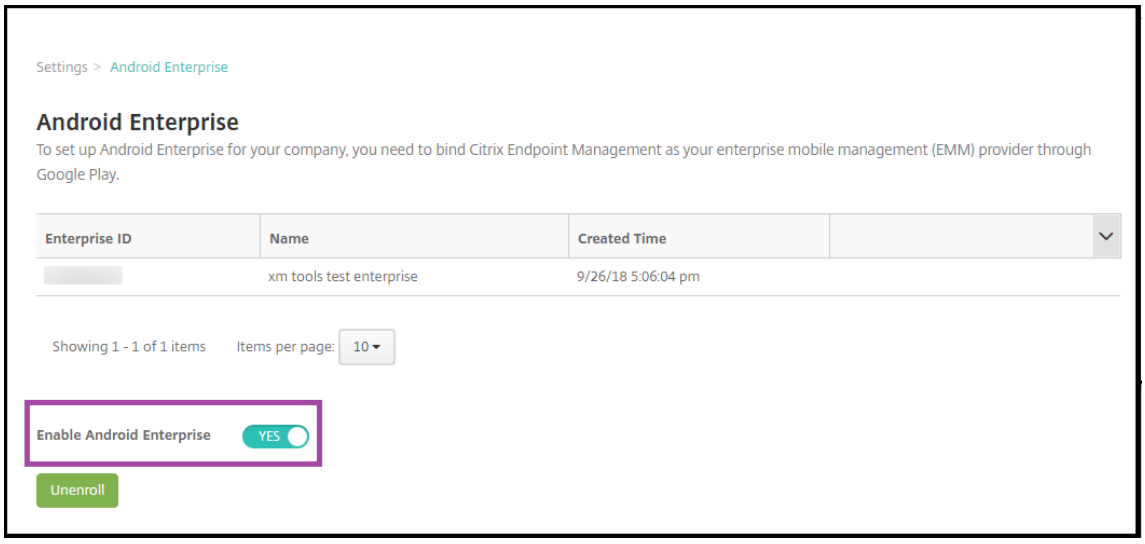
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 설정 **> Android Enterprise** 로이동합니다.



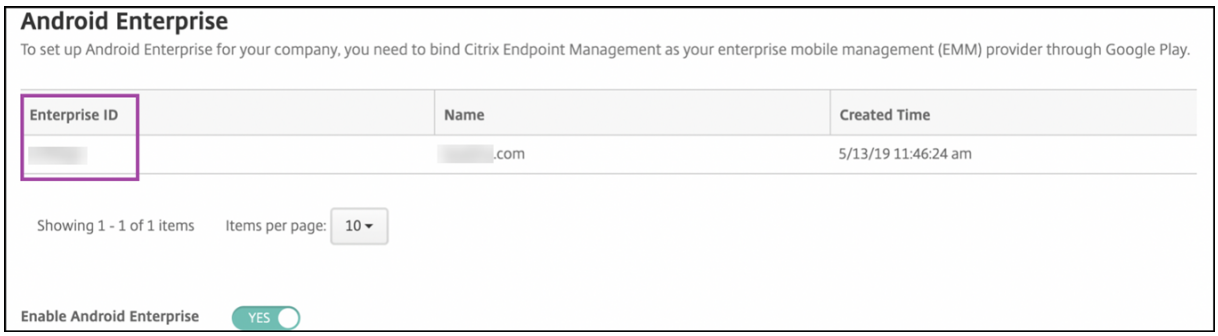
1. 연결을클릭합니다. Google Play 가열립니다.



1. 회사 Google 계정자격증명을사용하여 Google Play 에로그인합니다. 조직이름을입력하고 Citrix 가 EMM 공급자인지확인합니다.
2. Android Enterprise 에대한엔터프라이즈 ID 가추가되었습니다. Android Enterprise 를사용하려면 **Android Enterprise** 사용을 예로밉니다.



엔터프라이즈 ID 가 XenMobile 콘솔에나타납니다.



환경이 Google 에연결되었고장치를관리할준비가되었습니다. 이제사용자를위한앱을제공할수있습니다.

XenMobile 을사용하여사용자에게 Citrix 모바일생산성앱, MDX 앱, 공용앱스토어앱, 웹및 SaaS 앱, 엔터프라이즈앱및웹링크를제공할수있습니다. 이러한유형의앱및사용자에게제공하는방법에대한자세한내용은 앱추가를참조하십시오.

다음섹션에서는모바일생산성앱을제공하는방법을보여줍니다.

Android Enterprise 사용자에게 **Citrix** 모바일생산성앱제공

Android Enterprise 사용자에게 Citrix 모바일생산성앱을제공하려면다음단계가필요합니다.

1. 앱을 MDX 앱으로게시합니다. 앱을 MDX 앱으로구성을참조하십시오.
2. 사용자가장치의작업프로필에액세스할때사용할보안챌린지에대한규칙을구성합니다. 보안챌린지정책구성을참조하십시오.

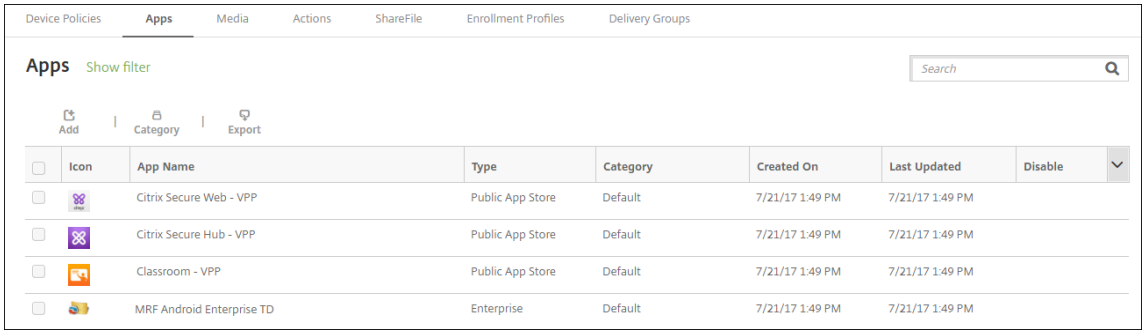
게시한앱은 Android Enterprise 엔터프라이즈에등록된장치에제공됩니다.

> 참고**:**
>
> Android Enterprise 공용앱스토어앱을 Android 사용자에게배포할경우해당사용자는 Android Enterprise 에자동으로등록됩니다.

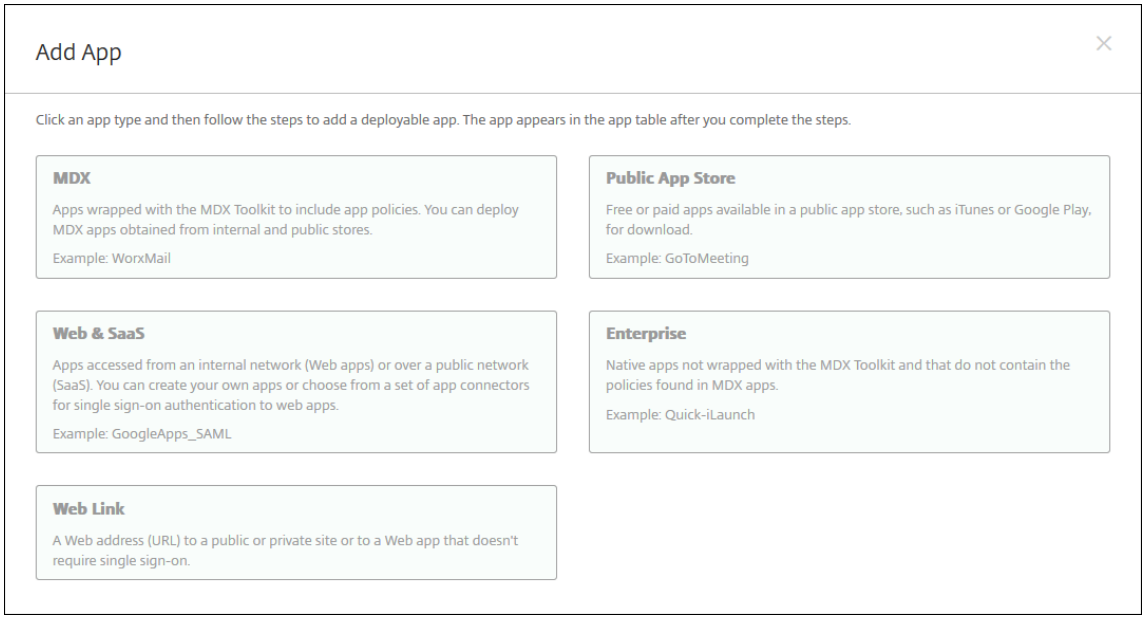
앱을 **MDX** 앱으로구성

Citrix 생산성앱을 Android Enterprise 용 MDX 앱으로구성하려면:

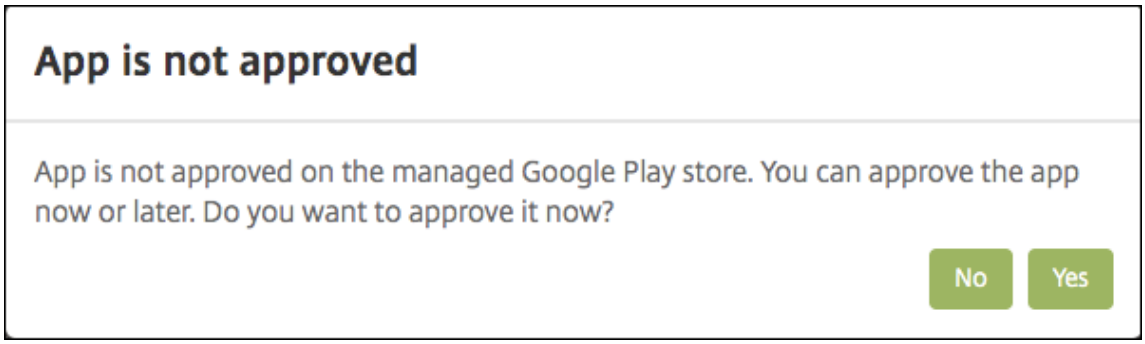
1. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 앱페이지가나타납니다.



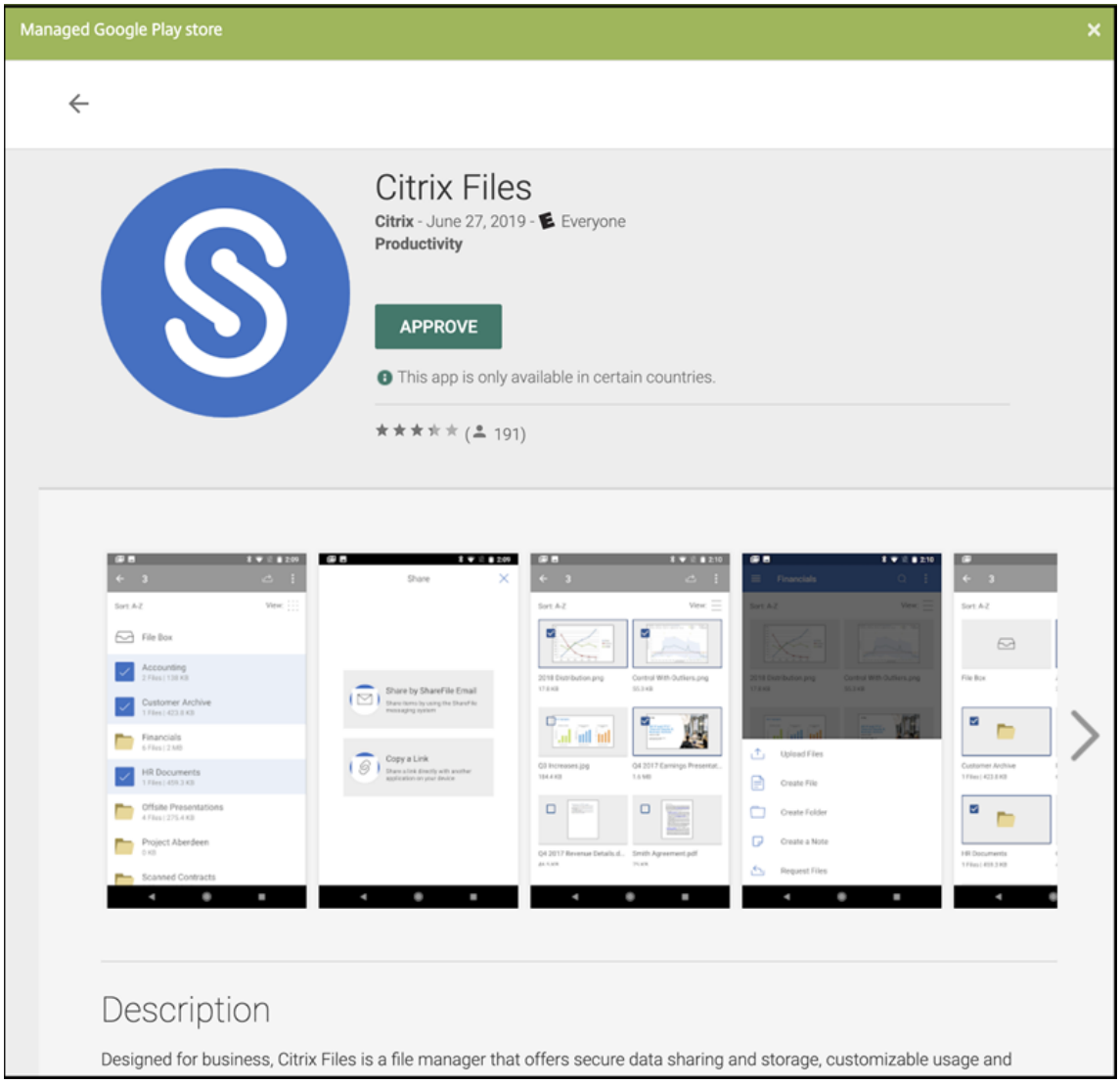
2. 추가를클릭합니다. 앱추가대화상자가나타납니다.



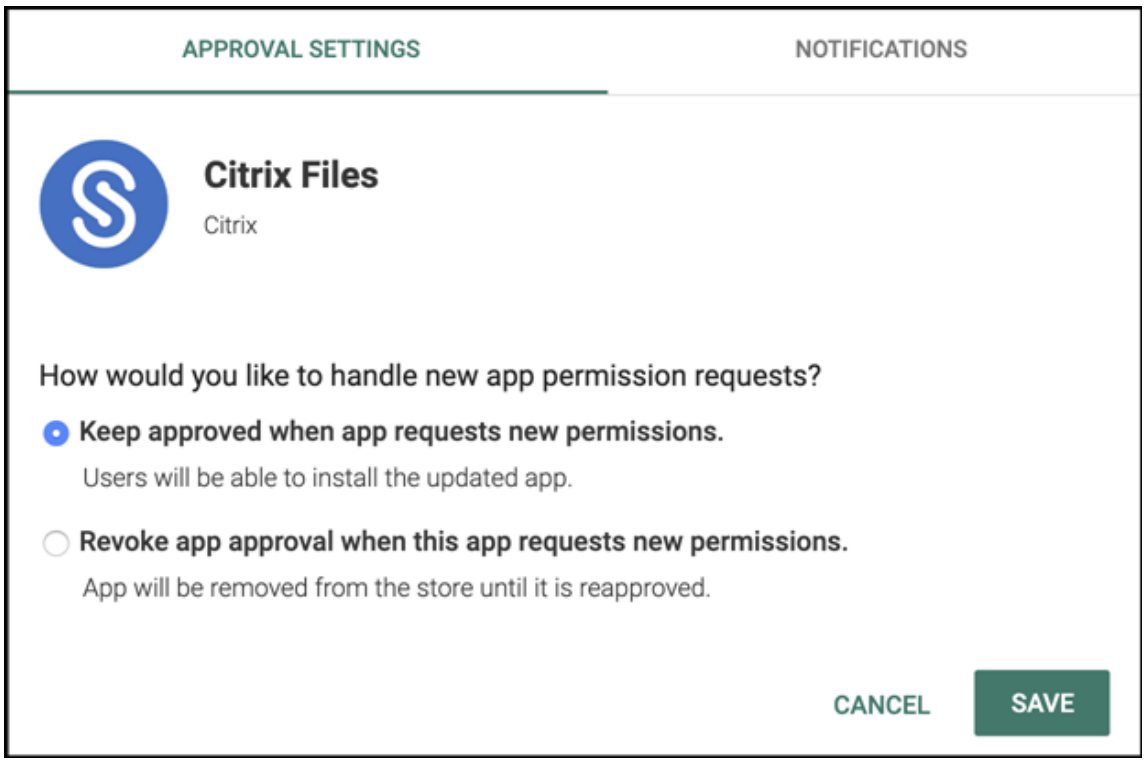
3. **MDX** 를클릭합니다. 앱정보페이지가나타납니다.
4. 페이지왼쪽에서 **Android Enterprise** 를플랫폼으로선택합니다.
5. 앱정보페이지에서다음정보를입력합니다.
   - 이름**:** 앱의설명적이름을입력합니다. 이이름은 앱테이블의 앱이름아래에표시됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은 앱범주정보를참조하십시오.
6. 다음을클릭합니다. **Android Enterprise MDX** 앱페이지가나타납니다.
7. 업로드를클릭하고앱의.mdx 파일이있는파일위치로이동합니다. 파일을선택하고 열기를클릭합니다.
8. 연결된응용프로그램에관리되는 Google Play Store 의승인이필요한경우 UI 에알림이표시됩니다. XenMobile 콘솔을종료하지않고응용프로그램을승인하려면 예를클릭합니다.



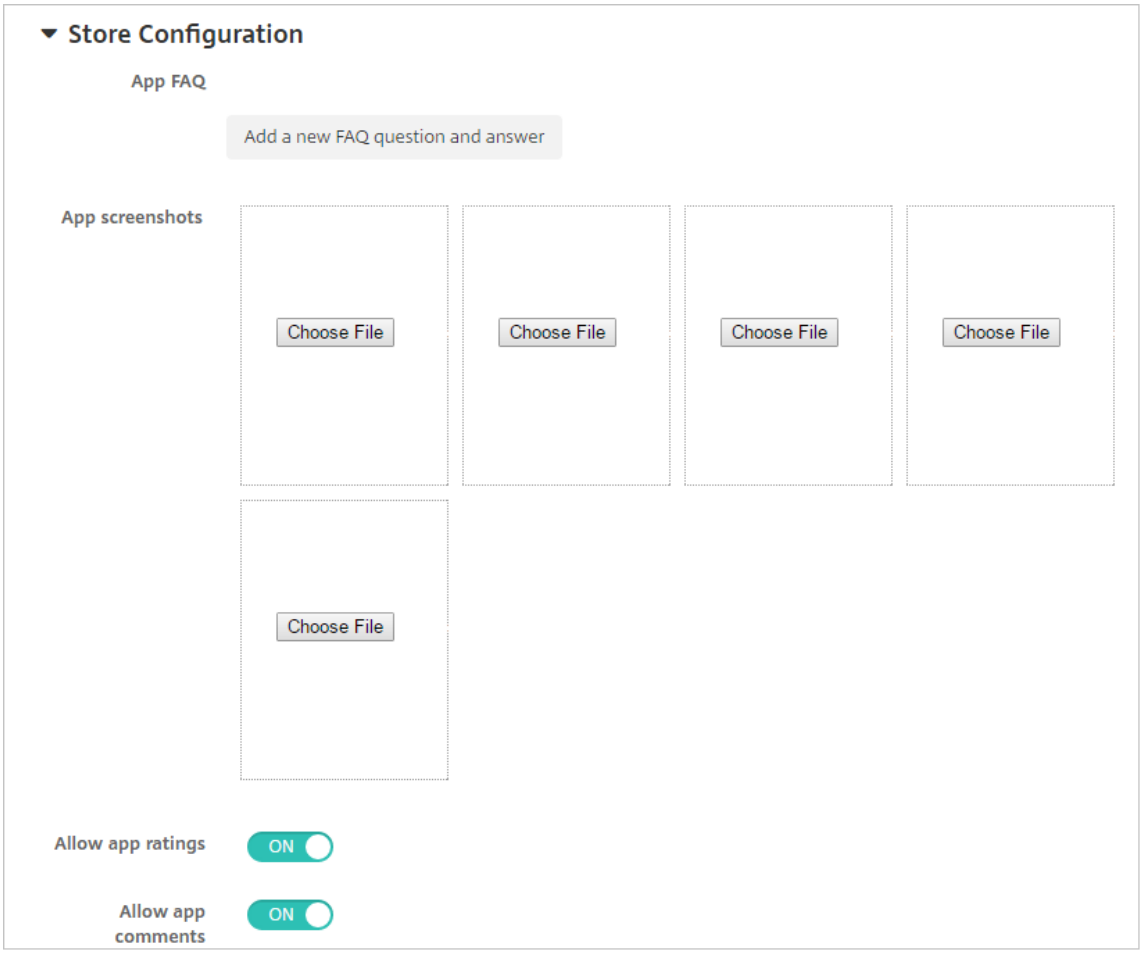
9. 관리되는 Google Play Store 페이지가열리면 승인을클릭합니다.



10. **Approve(**승인**)** 를다시클릭합니다.
11. **Keep approved when app requests new permissions(**앱이새권한을요청할때승인된상태로유지**)** 를선택합니다. 저장을클릭합니다.



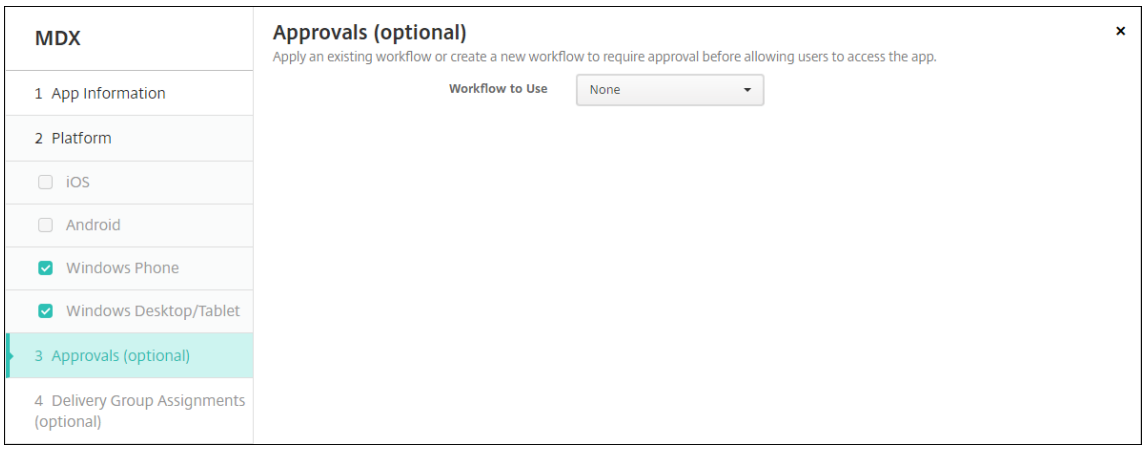
12. 앱이승인되고저장되면페이지에더많은설정이나타납니다. 다음설정을구성합니다.
    - 파일이름**:** 앱에연결된파일이름을입력합니다.
    - 앱설명**:** 앱에대한설명을입력합니다.
    - 제품트랙**:** 사용자장치로푸시할제품트랙을지정합니다. 테스트용으로설계된추적이있는경우해당추적을선택하여사용자에게할당할수있습니다. 기본값은프로덕션입니다.
    - 앱버전**:** 필요한경우앱버전번호를입력합니다.
    - 패키지 **ID:** Google Play Store 에있는앱의 URL 입니다.
    - 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
    - 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
    - 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.
13. **MDX** 정책을구성합니다. MDX 앱의앱정책에대한자세한내용은 MDX 정책요약 및 MAM SDK 개요를참조하십시오.
14. 배포규칙을구성합니다. 자세한내용은 리소스배포를참조하십시오.
15. 스토어구성을확장합니다. 이설정은 Android Enterprise 앱에적용되지않으며, 이러한앱은관리되는 Google Play 에만나타납니다.



필요한경우앱스토어에나타나는앱또는화면캡처에대한 FAQ 를추가할수있습니다. 또한사용자의앱평가또는설명추가를허용할지여부를설정할수있습니다.

- 다음설정을구성합니다.
  - 앱 **FAQ:** 앱에대한 FAQ(질문과답변) 를추가합니다.
  - 앱스크린샷**:** 앱스토어의앱을분류하는데도움이되는화면캡처를추가합니다. 업로드하는그래픽은 PNG 여야합니다. GIF 또는 JPEG 이미지는업로드할수없습니다.
  - 앱등급허용**:** 사용자의앱평가를허용할지여부를선택합니다. 기본값은 켜짐입니다.
    앱설명허용**:** 선택한앱에대한사용자의설명을허용할지여부를선택합니다. 기본값은 켜짐입니다.

16. 다음을클릭합니다. 승인페이지가나타납니다.

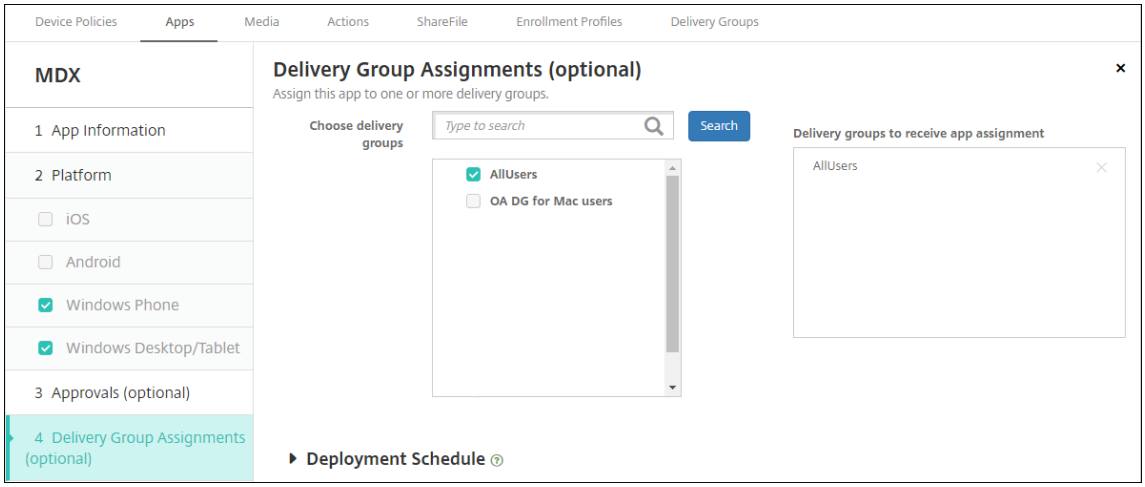


사용자계정을만들때승인이필요한경우워크플로를사용합니다. 승인워크플로를설정하지않으려는경우 15 단계로건너뛸수있습니다.

다음설정을구성하여워크플로를할당하거나만듭니다.

- 사용할워크플로**:** 목록에서기존워크플로를클릭하거나 새워크플로만들기를클릭합니다. 기본값은 없음입니다.
- 새워크플로만들기를선택하는경우다음설정을구성합니다. 자세한내용은 워크플로적용을참조하십시오.
- 이름**:** 워크플로의고유한이름을입력합니다.
- 설명**:** 필요한경우워크플로의설명을입력합니다.
- 전자메일승인템플릿**:** 목록에서할당할전자메일승인템플릿을선택합니다. 이필드오른쪽에있는눈모양아이콘을클릭하면템플릿을미리볼수있는대화상자가나타납니다.
- 관리자승인수준**:** 목록에서이워크플로에필요한관리자승인수준의번호를선택합니다. 기본값은 1 수준입니다. 사용가능한옵션은다음과같습니다.
  - 필요없음
  - 1 수준
  - 2 수준
  - 3 수준
- **Active Directory** 도메인선택**:** 목록에서워크플로에사용할적절한 Active Directory 도메인을선택합니다.
- 추가로필요한승인자찾기**:** 검색필드에추가로필요한사람의이름을입력하고 검색을클릭합니다. 이름은 Active Directory 에서가져옵니다.
- 필드에이름이나타나면해당하는이름옆의확인란을선택합니다. 이름과전자메일주소가 추가로필요한승인자선택됨목록에나타납니다.
  - 추가로필요한승인자선택됨목록에서사용자를제거하려면다음중하나를수행합니다.
    - 선택한도메인에있는모든사용자의목록을표시하려면 검색을클릭합니다.
    - 검색결과를제한하려면검색상자에이름전체또는일부를입력한다음 검색을클릭합니다.
    - 추가로필요한승인자선택됨목록에있는사용자는검색결과목록에서해당이름옆에확인표시가있습니다. 목록을스크롤하고제거하려는각이름옆에있는확인란의선택을취소합니다.

17. 다음을클릭합니다. 배달그룹할당페이지가나타납니다.



18. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.
19. 배포일정을확장하고다음설정을구성합니다.
    - 배포옆에서 켜짐을클릭하여배포를예약하거나 꺼짐을클릭하여배포를차단합니다. 기본옵션은 켜짐입니다.
    - 배포일정옆에서 지금또는 나중에를클릭합니다. 기본옵션은 지금입니다.
    - 나중에를클릭하는경우달력아이콘을클릭하고배포날짜와시간을선택합니다.
    - 배포조건옆에서 모든연결에서를클릭하거나 이전배포가실패한경우에만을클릭합니다. 기본옵션은 모든연결에서입니다.
    - 상시연결에대해배포옆에 꺼짐이선택되어있는지확인합니다. 기본옵션은 꺼짐입니다. 버전이 10.18.19 이상인 XenMobile 을사용하여시작한경우 Android Enterprise 에서는상시연결을사용할수없습니다. 버전 10.18.19 이하인 XenMobile 을사용하여시작한고객에게는연결을권장하지않습니다.

      설정 **>** 서버속성에서백그라운드배포예약키를구성한경우에만이옵션이적용됩니다.

      구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은 상시연결에대해배포를제외하고모든플랫폼에적용됩니다.
20. 저장을클릭합니다.

단계를반복하여각모바일생산성앱에대해 MDX 앱을구성합니다.

보안챌린지정책구성

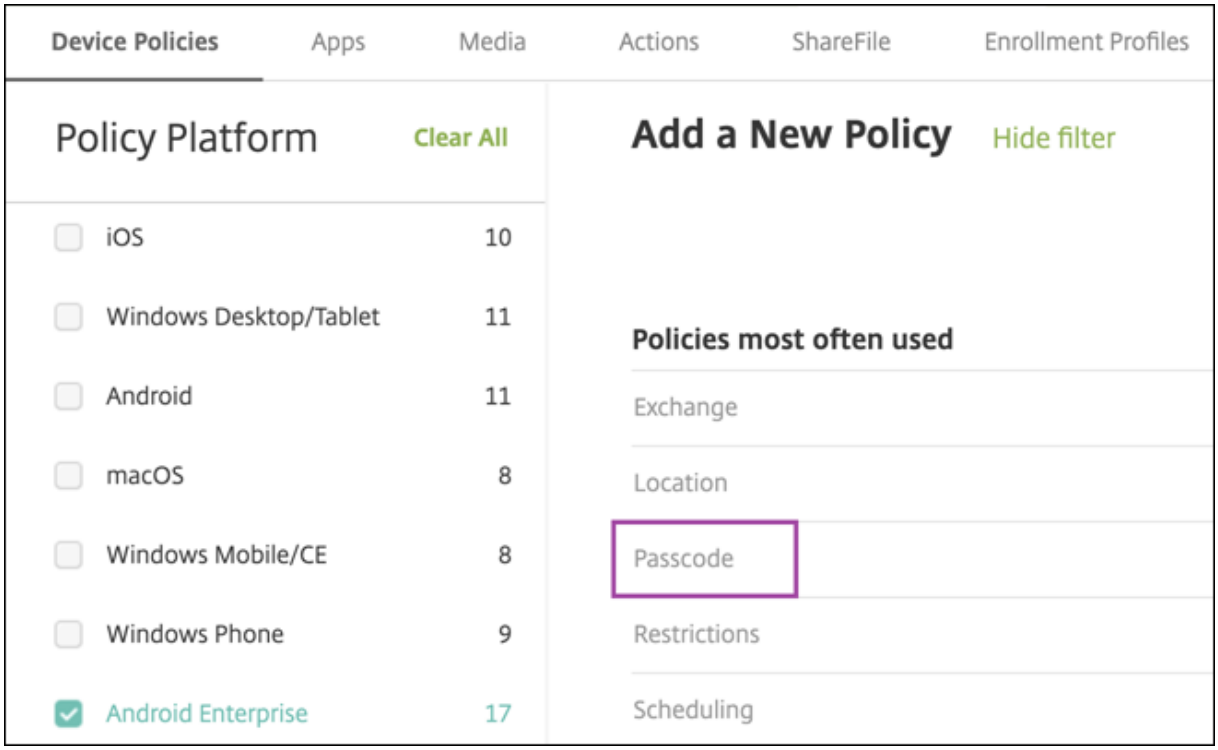
XenMobile 암호장치정책은사용자가자신의장치또는장치의 Android Enterprise 작업프로필에액세스하도록하는보안챌린지에대한규칙집합을구성합니다. 보안챌린지는암호또는생체인식일수있습니다. 암호정책에대한자세한내용은 암호장치정책을참조하십시오.

- Android Enterprise 배포에 BYOD 장치가포함되는경우작업프로필에대한암호정책을구성합니다.
- 배포에회사소유의완전관리형장치가포함되는경우장치자체에대한암호정책을구성합니다.

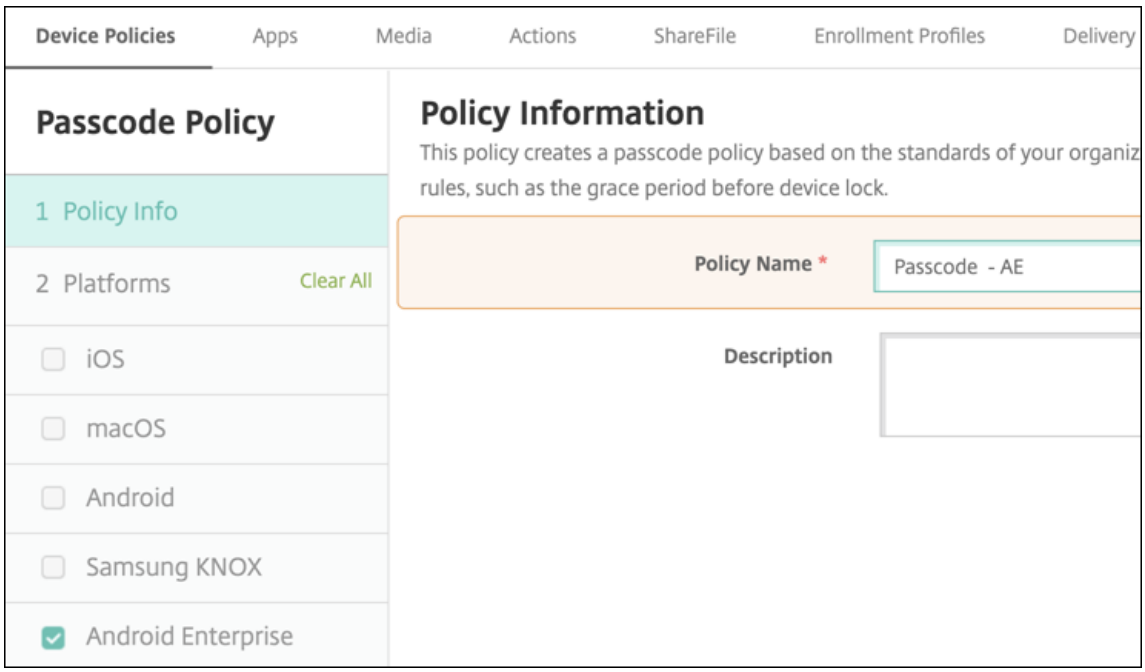
- 배포에두가지유형의장치가모두포함되는경우두유형의암호정책을모두구성합니다.

암호정책을구성하려면:

1. XenMobile 콘솔에서 구성 **>** 장치정책으로이동합니다.
2. 추가를클릭합니다.
3. 필터표시를클릭하여 정책플랫폼창을표시합니다. 정책플랫폼창에서 **Android Enterprise** 를선택합니다.
4. 오른쪽창에서 암호를클릭합니다.



1. 정책이름을입력합니다. 다음을클릭합니다.



2. 암호정책설정을구성합니다.
   - 장치자체의보안챌린지에사용할수있는설정을보려면 장치암호필요를 켜짐으로설정합니다.
   - 작업프로필보안챌린지에사용할수있는설정을보려면 작업프로필보안챌린지를 켜짐으로설정합니다.
3. 다음을클릭합니다.
4. 정책을하나이상의배달그룹에할당합니다.
5. 저장을클릭합니다.

등록프로필만들기

XenMobile 배포에서 Android Enterprise 를사용하도록설정한경우등록프로필을사용하여 Android 장치의등록방법을제어할수있습니다. 등록프로필을만들어서 Android Enterprise 장치를등록할경우등록프로필을구성하여새장치와공장기본값으로재설정된장치를다음으로등록할수있습니다.

- 완전히관리되는장치
- 전용장치 (COSU 장치)
- 작업프로필로완전히관리되는장치 (COPE 장치)

이러한 Android Enterprise 등록프로필을각각구성하여 BYOD Android 장치를작업프로필장치로등록할수도있습니다.

XenMobile 배포에서 Android Enterprise 를사용하도록설정한경우새로등록되거나다시등록되는모든 Android 장치는 Android Enterprise 장치로등록됩니다. 기본적으로글로벌등록프로필은신규및공장기본값으로재설정된 Android 장치를완전관리형장치로등록하고, BYOD Android 장치를작업프로필장치로등록합니다.

등록프로필을만들경우배달그룹을할당합니다. 사용자가등록프로필이다른여러배달그룹에속하는경우사용되는등록프로필은배달그룹의이름에따라결정됩니다. XenMobile 은사전순으로표시된배달그룹목록의마지막에나타나는배달그룹을선택합니다. 자세

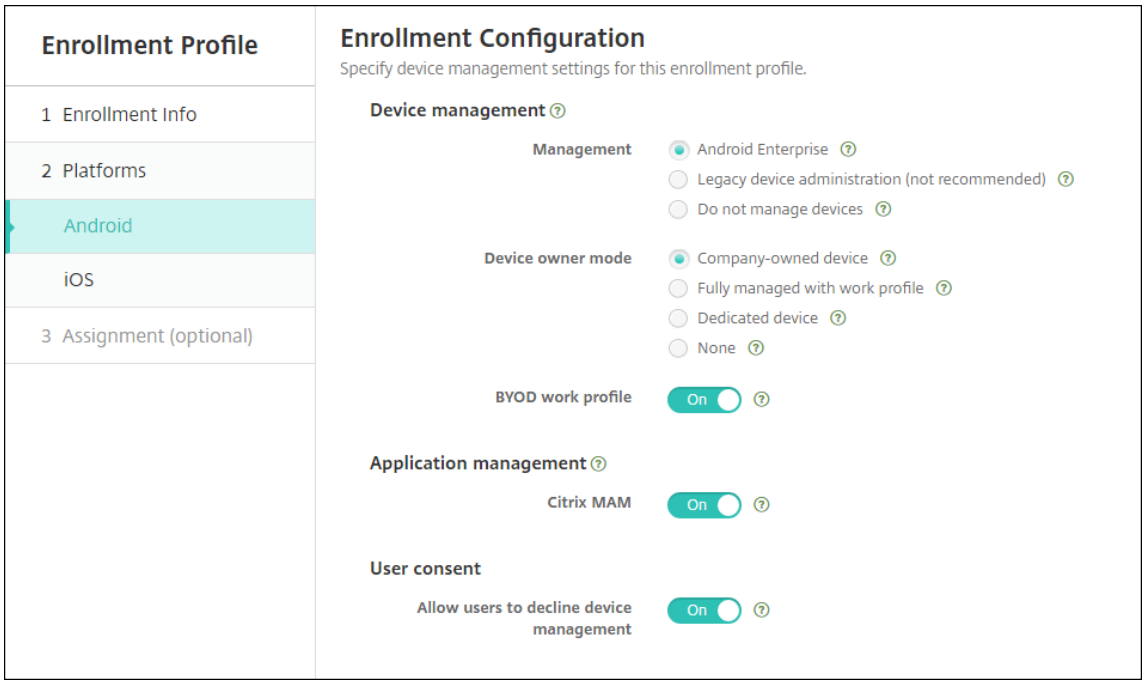
한내용은 등록프로필을참조하십시오.

등록프로필을사용하여 MDM 전용, MDM+MAM, MAM 전용과같이여러사용사례를결합할수있습니다. 서버속성 `xms.server.mode`에반영된 XenMobile Server 라이센스유형에따라 구성 **>** 등록프로필에서제공되는설정이결정됩니다.

완전히관리되는장치에대한등록프로필추가

글로벌등록프로필은기본적으로완전히관리되는장치를등록하지만완전히관리되는장치를등록할추가등록프로필을만들수있습니다.

1. XenMobile 콘솔에서 구성 **>** 등록프로필로이동합니다.
2. 등록프로필을추가하려면 추가를클릭합니다. 등록정보페이지에서등록프로필의이름을입력합니다.
3. 이프로필을가진구성원이등록할수있는장치수를설정합니다.
4. 플랫폼에서 **Android** 를선택하거나 다음을클릭합니다. 등록구성페이지가나타납니다.
5. 관리를 **Android Enterprise** 로설정합니다.
6. 장치소유자모드를 기업소유장치로설정합니다.

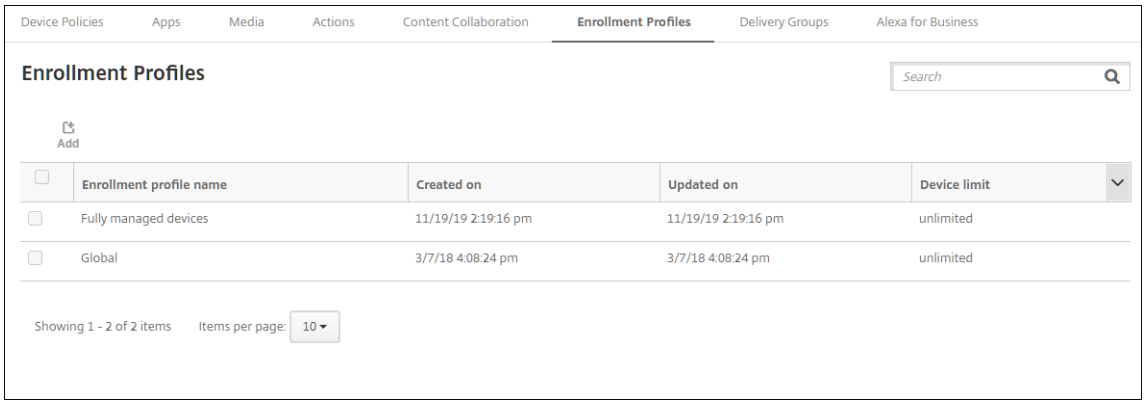


7. **BYOD** 작업프로필을사용하면 BYOD 장치를작업프로필장치로구성하기위한등록프로필을구성할수있습니다. 신규및공장기본값으로재설정된장치를완전히관리되는장치로등록합니다.
   - BYOD 장치를작업프로필장치로등록하도록허용하려면 **BYOD** 작업프로필을 켜짐으로설정합니다. 기본값은 켜짐입니다.
   - 완전히관리되는장치에대한등록을제한하려면 **BYOD** 작업프로필을 꺼짐으로설정합니다.

8. Citrix MAM 에서장치등록여부를선택합니다.
9. **BYOD** 작업프로필을 켜짐으로설정할경우사용자동의를구성합니다. BYOD 작업프로필장치사용자가장치등록시장치관리를거부할수있도록허용하려면 사용자의장치관리거부를허용을 켜짐으로설정합니다.

   BYOD 작업프로필이 켜짐으로설정되면 사용자의장치관리거부를허용의기본값은 켜짐입니다. **BYOD** 작업프로필이 꺼짐으로설정되면 사용자의장치관리거부를허용이비활성화됩니다.
10. 할당 **(**옵션**)** 을선택합니다. 배달그룹할당화면이나타납니다.
11. 완전히관리되는장치를등록하는관리자가포함된배달그룹을선택합니다. 그런다음 저장을클릭합니다.

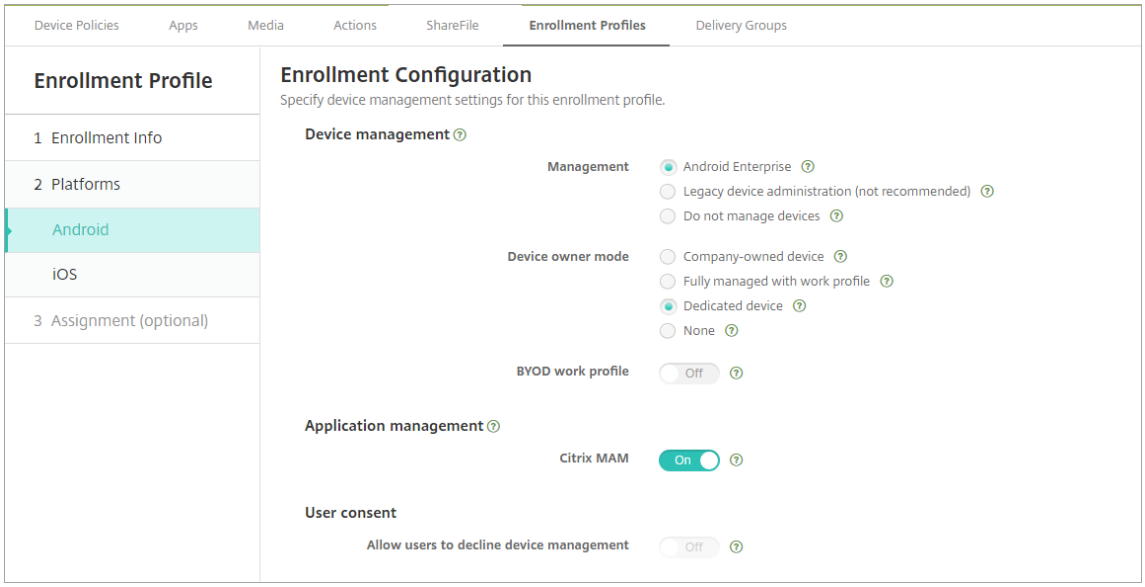
    추가한프로필과함께등록프로필페이지가나타납니다.



전용장치등록프로필추가

XenMobile 배포에전용장치가포함되는경우단일 XenMobile 관리자또는소규모관리자그룹이다수의전용장치를등록합니다. 이러한관리자가필요한모든장치를등록할수있도록하려면사용자당무제한의장치가허용되는관리자용등록프로필을만듭니다.

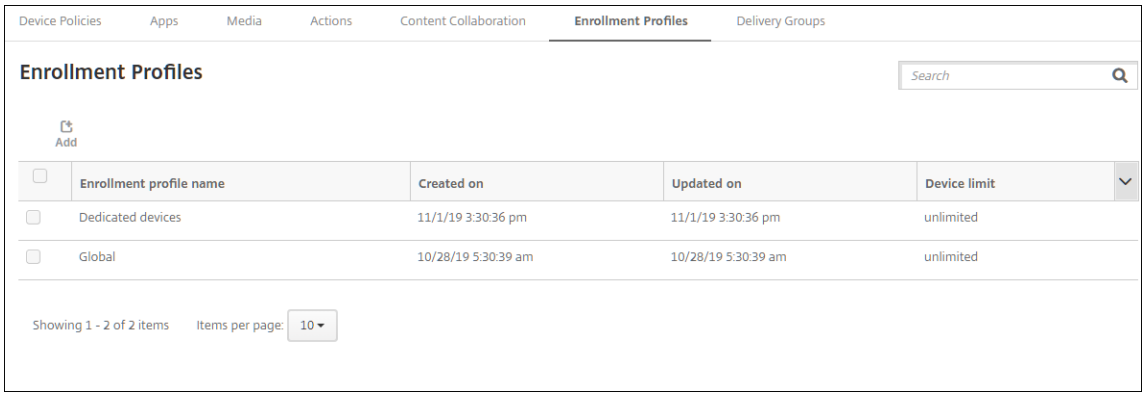
1. XenMobile 콘솔에서 구성 **>** 등록프로필로이동합니다.
2. 등록프로필을추가하려면 추가를클릭합니다. 등록정보페이지에서등록프로필의이름을입력합니다. 이프로필을가진구성원이등록할수있는장치수가무제한으로설정되어있는지확인합니다.
3. 플랫폼에서 **Android** 를선택하거나 다음을클릭합니다. 등록구성페이지가나타납니다.
4. 관리를 **Android Enterprise** 로설정합니다.
5. 장치소유자모드를 전용장치로설정합니다.



6. **BYOD** 작업프로필을사용하면 BYOD 장치를작업프로필장치로구성하기위한등록프로필을구성할수있습니다. 신규및공장기본값으로재설정된장치를전용장치로등록합니다. BYOD 장치를작업프로필장치로등록하도록허용하려면 **BYOD** 작업프로필을 켜짐으로설정합니다. 기업소유장치에대한등록을제한하려면 **BYOD** 작업프로필을 꺼짐으로설정합니다. 기본값은 켜짐입니다.
7. Citrix MAM 에서장치등록여부를선택합니다.
8. **BYOD** 작업프로필을 켜짐으로설정할경우사용자동의를구성합니다. BYOD 작업프로필장치사용자가장치등록시장치관리를거부할수있도록허용하려면 사용자의장치관리거부를허용을 켜짐으로설정합니다.

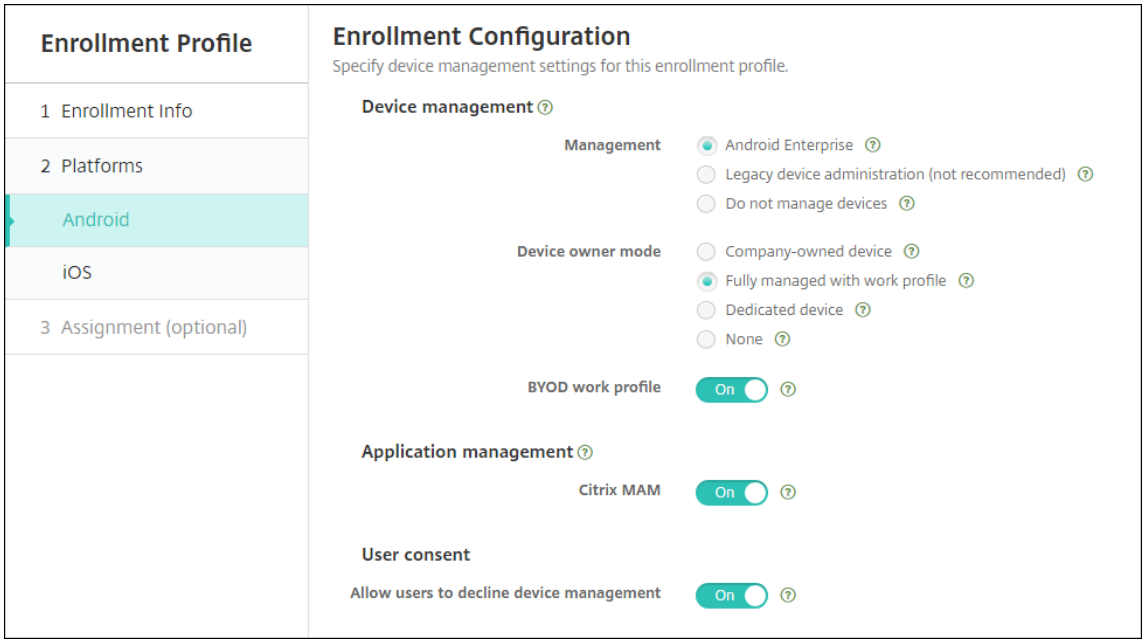
   BYOD 작업프로필이 켜짐으로설정되면 사용자의장치관리거부를허용의기본값은 켜짐입니다. **BYOD** 작업프로필이 꺼짐으로설정되면 사용자의장치관리거부를허용이비활성화됩니다.
9. 할당 **(**옵션**)** 을선택합니다. 배달그룹할당화면이나타납니다.
10. 전용장치를등록하는관리자가포함된배달그룹을선택합니다. 그런다음 저장을클릭합니다.

    추가한프로필과함께등록프로필페이지가나타납니다.



작업프로필로완전히관리되는장치에대한등록프로필추가

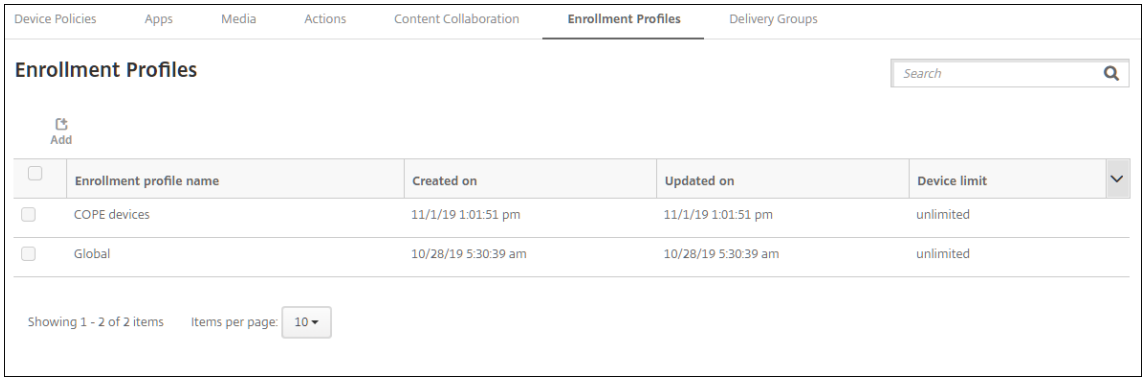
1. XenMobile 콘솔에서 구성 **>** 등록프로필로이동합니다.
2. 등록프로필을추가하려면 추가를클릭합니다. 등록정보페이지에서등록프로필의이름을입력합니다.
3. 이프로필을가진구성원이등록할수있는장치수를설정합니다.
4. 플랫폼에서 **Android** 를선택하거나 다음을클릭합니다. 등록구성페이지가나타납니다.
5. 관리를 **Android Enterprise** 로설정합니다. 장치소유자모드를 작업프로필로완전히관리로설정합니다.



6. **BYOD** 작업프로필을사용하면 BYOD 장치를작업프로필장치로구성하기위한등록프로필을구성할수있습니다. 신규및공장기본값으로재설정된장치를작업프로필로완전히관리되는장치로등록합니다. BYOD 장치를작업프로필장치로등록하도록허용하려면 **BYOD** 작업프로필을 켜짐으로설정합니다. 전용장치에대한등록을제한하려면 **BYOD** 작업프로필을 꺼짐으로설정합니다. 기본값은 꺼짐입니다.
7. Citrix MAM 에서장치등록여부를선택합니다.
8. **BYOD** 작업프로필을 켜짐으로설정할경우사용자동의를구성합니다. BYOD 작업프로필장치사용자가장치등록시장치관리를거부할수있도록허용하려면 사용자의장치관리거부를허용을 켜짐으로설정합니다.

   BYOD 작업프로필이 켜짐으로설정되면 사용자의장치관리거부를허용의기본값은 켜짐입니다. **BYOD** 작업프로필이 꺼짐으로설정되면 사용자의장치관리거부를허용이비활성화됩니다.
9. 할당 **(**옵션**)** 을선택합니다. 배달그룹할당화면이나타납니다.
10. 배달그룹또는작업프로필로완전히관리되는장치를등록하는관리자가포함된배달그룹을선택합니다. 그런다음 저장을클릭합니다.

    추가한프로필과함께등록프로필페이지가나타납니다.



레거시장치에대한등록프로필추가

Google 은장치관리의장치관리자모드를지원중단할예정입니다. Google 은장치소유자모드또는프로필소유자모드에서모든 Android 장치를관리할것을권장하고있습니다. (Google Android Enterprise 개발자가이드의 장치관리사용중단 참고)

이변경사항을지원하려면:

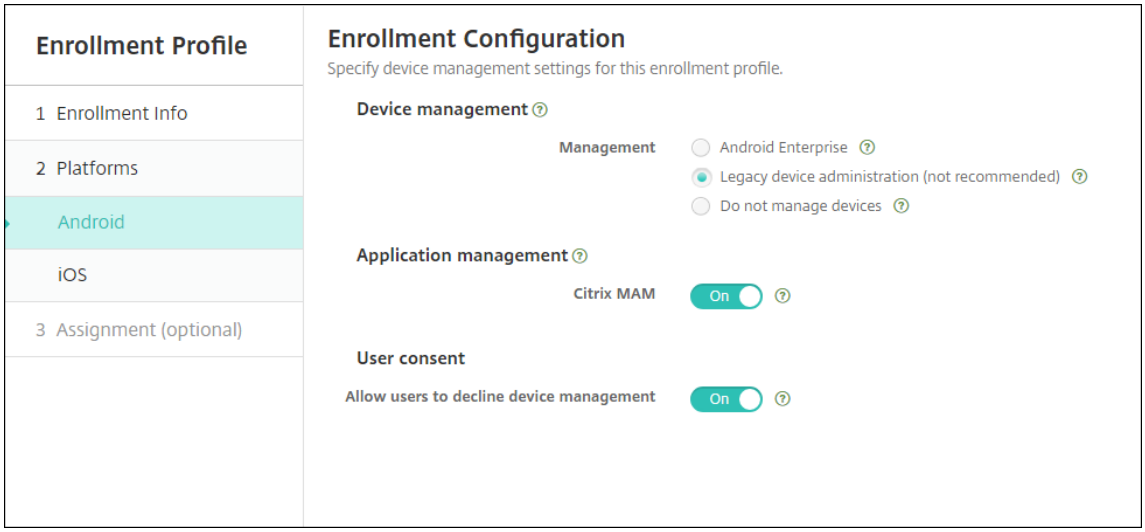
- Citrix 에서는 Android 장치에대한기본등록옵션으로 Android Enterprise 를사용합니다.
- XenMobile 배포에서 Android Enterprise 를사용하도록설정한경우새로등록되거나다시등록되는모든 Android 장치는 Android Enterprise 장치로등록됩니다.

조직이 Android Enterprise 를사용하여레거시 Android 장치를관리할준비가되지않았을수있습니다. 이러한장치를장치관리자모드에서계속해서관리할수있습니다. 장치관리자모드로이미등록된장치의경우 XenMobile 에서장치관리자모드로계속관리합니다.

신규 Android 장치등록에장치관리자모드를사용하도록허용하려면레거시장치에대한등록프로필을만듭니다.

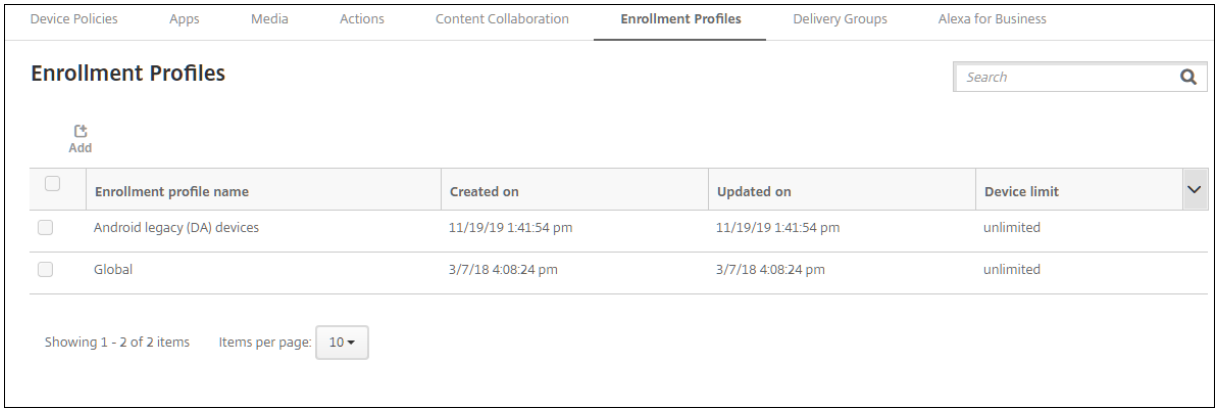
레거시장치에대한등록프로필을만들려면:

1. XenMobile 콘솔에서 구성 **>** 등록프로필로이동합니다.
2. 등록프로필을추가하려면 추가를클릭합니다. 등록정보페이지에서등록프로필의이름을입력합니다.
3. 이프로필을가진구성원이등록할수있는장치수를설정합니다.
4. 플랫폼에서 **Android** 를선택하거나 다음을클릭합니다. 등록구성페이지가나타납니다.
5. 관리를 레거시장치관리 **(**권장되지않음**)** 로설정합니다. 다음을클릭합니다.



6. Citrix MAM 에서장치등록여부를선택합니다.
7. 사용자가장치등록시장치관리를거부할수있도록허용하려면 사용자의장치관리거부를허용을 켜짐으로설정합니다. 기본값은 켜짐입니다.
8. 할당 (옵션) 을선택합니다. 배달그룹할당화면이나타납니다.
9. 전용장치를등록하는관리자가포함된배달그룹을선택합니다. 그런다음 저장을클릭합니다.

추가한프로필과함께등록프로필페이지가나타납니다.



장치관리자모드에서레거시장치관리를계속하려면이프로필을사용하여등록하거나재등록합니다. 사용자로하여금 Secure Hub 를다운로드하고등록서버 URL 을제공하도록하면작업프로필장치와유사하게장치관리자장치를등록할수있습니다.

Android Enterprise 작업프로필장치프로비전

Android Enterprise 작업프로필장치는프로필소유자모드에서등록됩니다. 이러한장치가새장치이거나공장기본값으로재설정될필요는없습니다. BYOD 장치는작업프로필장치로등록됩니다. 등록환경은 XenMobile 의 Android 등록과비슷합니다. 사용자가 Google Play 에서 Secure Hub 를다운로드하고장치를등록합니다.

Android Enterprise 에서작업프로필장치로장치를등록하는경우 **USB** 디버깅및알수없는소스설정은장치에서기본적으로비활성화됩니다.

Android Enterprise 에서작업프로필장치로장치를등록하는경우항상 Google Play 로이동하십시오. 거기서사용자의개인프로필에 Secure Hub 가표시되도록설정합니다.

Android Enterprise 완전관리형장치프로비전

이전섹션에서설정한배포에서완전관리형장치를등록할수있습니다. 완전관리형장치는회사소유의장치이며장치소유자모드에서등록됩니다. 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 식별자토큰을사용하여장치등록을참조하십시오.
- **NFC(**근거리통신**)** 범프**:** NFC 범프등록방법은근거리통신을사용하여두장치간데이터를전송합니다. 새장치또는공장기본값으로재설정된장치에서는 Bluetooth, Wi-Fi 및기타통신모드를사용할수없습니다. NFC 는이상태에서장치가사용할수있는유일한통신프로토콜입니다. NFC 범프를사용하여장치등록을참조하십시오.
- **QR** 코드**:** QR 코드등록은태블릿과같이 NFC 를지원하지않는분산된제품군의장치를등록할때사용될수있습니다. QR 코드등록방법은설치마법사에서 QR 코드를스캔하여장치프로필모드를설정하고구성합니다. QR 코드를사용하여장치등록을참조하십시오.
- 제로터치**:** 제로터치등록을사용하면장치전원을처음켤때자동으로등록하도록장치를구성할수있습니다. 제로터치등록은 Android 9.0 이상을실행하는일부 Android 장치에서지원됩니다. 제로터치등록을참조하십시오.
- **Google** 계정**:** 사용자가 Google 계정자격증명을입력하여프로비저닝프로세스를시작합니다. 이옵션은 Google Workspace 를사용하는엔터프라이즈용입니다.

Citrix DPC 식별자토큰을사용하여장치등록

새장치또는공장기본값으로재설정된장치의초기설정을위해전원을켠후 Google 계정을입력하라는메시지가표시되면 `afw##xenmobile`을입력합니다. 이동작을수행하면 Secure Hub 가다운로드되고설치됩니다. 그런다음사용자는 Secure Hub 설정메시지에따라등록을완료합니다.

최신버전의 Secure Hub 가 Google Play Store 에서다운로드되므로이등록방법이대부분의고객에게권장됩니다. 다른등록방법과달리, XenMobile Server 에서다운로드하기위해 Secure Hub 를제공하지않습니다.

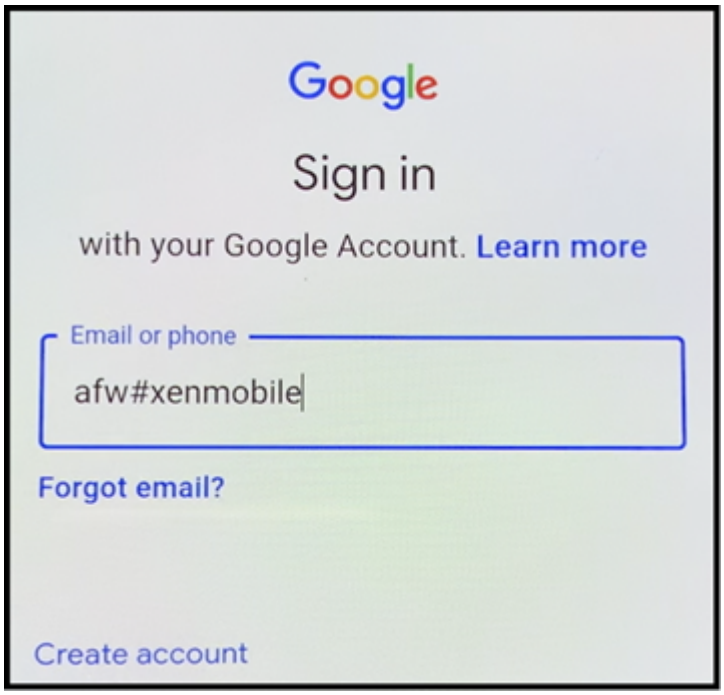
시스템요구사항

- Android OS 를실행하는모든 Android 장치에서지원됩니다.

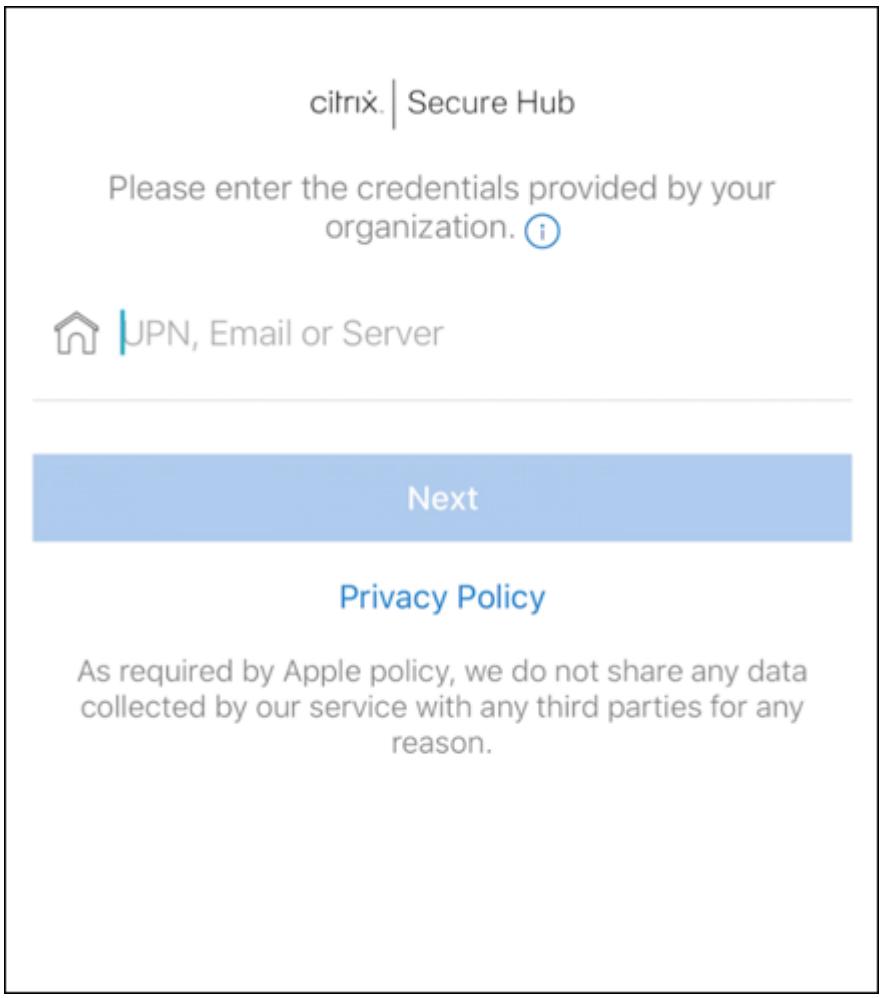
장치를등록하려면

1. 새장치또는공장기본값으로재설정된장치의전원을켭니다.

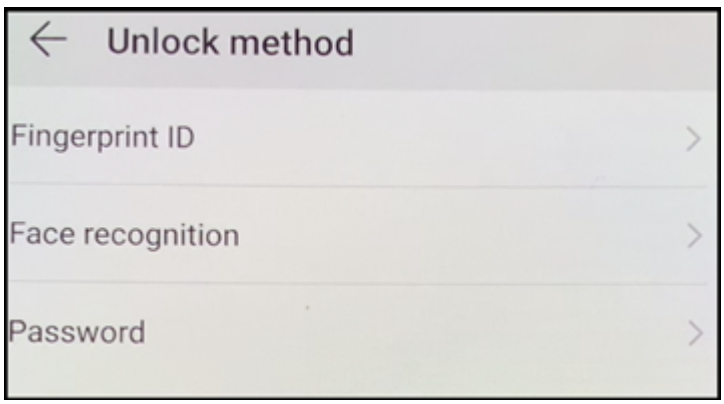
2. 초기장치설정이로드되고 Google 계정을입력하라는메시지가표시됩니다. 장치에장치의홈화면이로드되는경우알림표시줄에서 설정완료알림을확인합니다.
3. 전자메일또는전화필드에 `afw##xenmobile`을입력합니다.



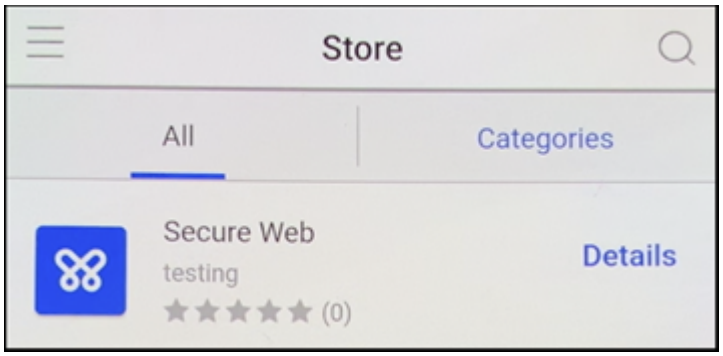
4. Android Enterprise 화면에서 Secure Hub 를설치하라는메시지가표시되면 설치를누릅니다.
5. Secure Hub 설치관리자화면에서 **Install(**설치**)** 을누릅니다.
6. 모든앱권한요청에대해 **Allow(**허용**)** 를누릅니다.
7. **Accept & Continue(**동의및계속**)** 를눌러 Secure Hub 를설치하고장치관리를허용합니다.
8. 이제 Secure Hub 가설치되었고기본등록화면에표시됩니다. 이예에서는 AutoDiscovery 을설정하지않았습니다. 자동검색을설정했다면사용자가사용자이름/전자메일을입력하고서버를찾을수있습니다. 대신환경에대한등록 URL 을입력하고 다음을누릅니다.



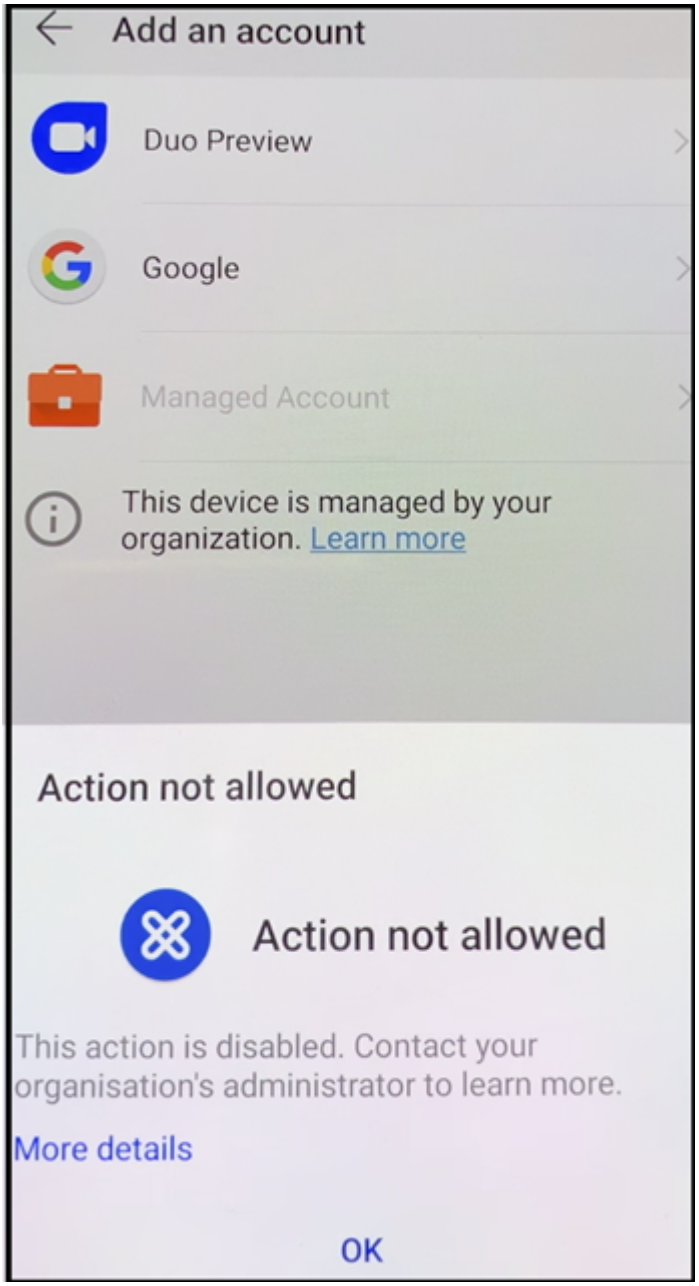
9. XenMobile 의기본구성에서는사용자가 MAM 을사용할지아니면 MDM+MAM 을사용할지를선택할수있습니다. 이와 같은메시지가표시되면 예**.** 등록을눌러 MDM+MAM 을선택합니다.
10. 사용자이름과암호를입력하고 다음을누릅니다.
11. 장치암호를구성하라는메시지가표시됩니다. 설정을누르고암호를입력합니다.
12. 작업프로필잠금해제방법을구성하라는메시지가표시됩니다. 이예에서는 암호를누르고 **PIN** 을누른다음 PIN 을입력합니다.



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. 화면공유또는원격디버깅을위한개발자옵션도차단됩니다.



NFC 범프를사용하여장치등록

NFC 범프를사용하여완전하게관리되는장치로장치를등록하려면두장치, 즉출고기본값으로재설정된장치와 XenMobile Provisioning Tool 을실행하는장치가필요합니다.

시스템요구사항및사전요구사항

- 지원되는 Android 장치.

- 완전하게관리되는장치로서 Android Enterprise 용으로프로비전된새장치또는출고기본값으로재설정된장치. 이사전요구사항을완료하는단계는이문서의뒷부분에서찾을수있습니다.
- NFC 호환성이있으며구성된 Provisioning Tool 이실행되고있는또다른장치. Provisioning Tool 은 Secure Hub 또는 Citrix 다운로드페이지에서사용할수있습니다.

각장치에는하나의 Android Enterprise 프로필인관리되는 Secure Hub 만있어야합니다. 각장치에는하나의프로필만허용됩니다. 두번째 DPC 앱을추가하려고하면설치된 Secure Hub 가제거됩니다.

NFC 범프를통해전송된데이터

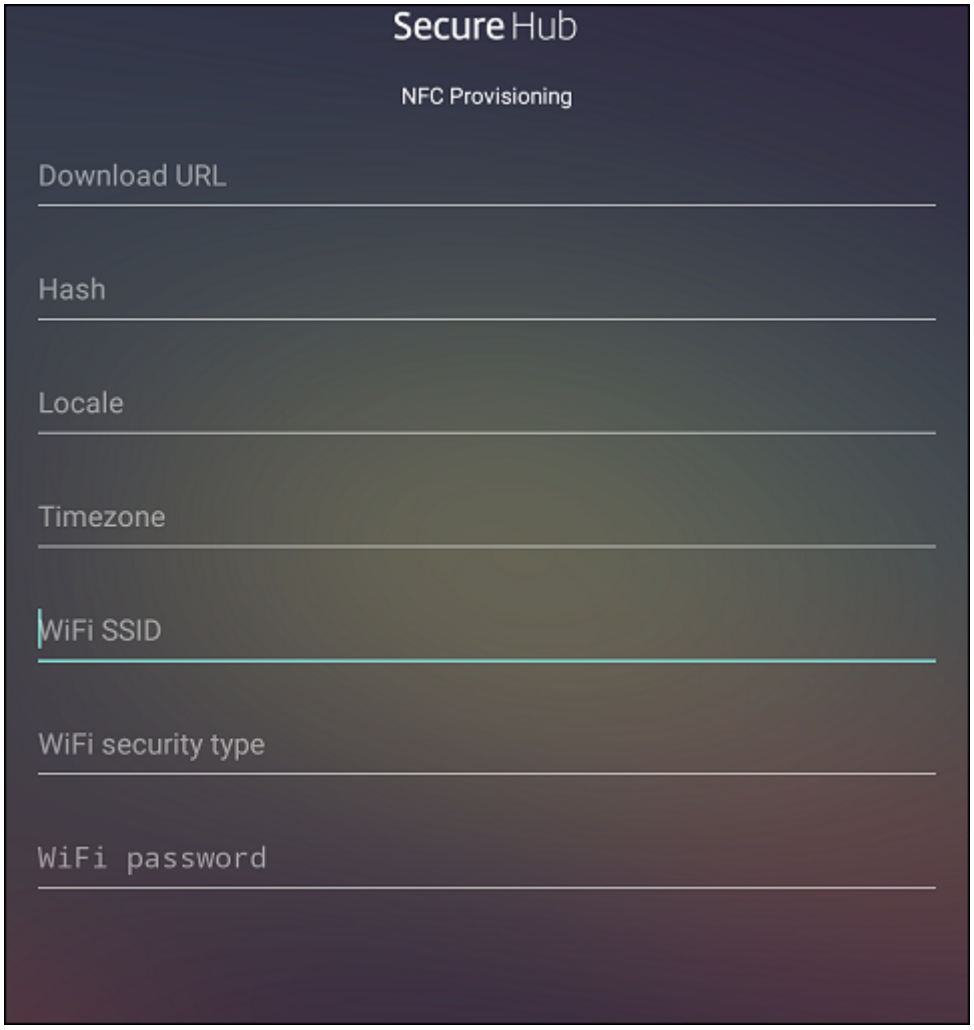
출고기본값으로재설정된장치를프로비저닝하려면 NFC 범프를통해다음데이터를전송하여 Android Enterprise 를초기화해야합니다.

- 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.



필요한필드에데이터를입력하거나텍스트파일을사용해데이터를채울수있습니다. 다음절차의단계에서는텍스트파일을구성하고각 필드에대한설명을포함시키는방법에대해설명합니다. 입력한정보가앱에저장되지않으므로나중에사용할수있도록정보를유지하려면텍스트파일을만들수있습니다.

텍스트파일을사용하여 **Provisioning Tool** 을구성하려면

파일의이름을 nfcprovisioning.txt 로지정하고장치의 SD 카드에있는 /sdcard/ 폴더에파일을저장합니다. 그러면앱에서 텍스트파일을읽고값을채울수있습니다.

텍스트파일에는다음과같은데이터가포함되어야합니다.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>

이줄은 EMM 공급자앱의인트라넷/인터넷위치입니다. NFC 범프후에출고기본값으로재설정된장치가 Wi-Fi 에연결되면장치가 이위치에액세스하여다운로드할수있어야합니다. URL 은특수한형식이필요하지않은일반 URL 입니다.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>

이줄은 EMM 공급자앱의체크섬입니다. 이체크섬은다운로드가성공했는지확인하는데사용됩니다. 체크섬을얻는단계에대해서는이문서뒷부분에서설명합니다.

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

이줄은 Provisioning Tool 이실행되고있는장치의연결된 Wi-Fi SSID 입니다.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

지원되는값은 WEP 및 WPA2 입니다. Wi-Fi 가보호되지않는경우이필드는비어있어야합니다.

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Wi-Fi 가보호되지않는경우이필드는비어있어야합니다.

android.app.extra.PROVISIONING_LOCALE=<locale>

언어및국가코드를입력합니다. 언어코드는 ISO 639-1에정의된대로소문자두자로구성된 ISO 언어코드입니다 (예: en). 국가코드는 ISO 3166-1에정의된대로대문자두자로구성된 ISO 국가코드입니다 (예: US). 예를들어, 미국에서사용하는영어의경우 en_US 를입력합니다. 코드를입력하지않으면국가및언어가자동으로입력됩니다.

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

장치가실행되는표준시간대입니다. 지역/위치형식의 Olson 이름을입력합니다. 예를들어태평양표준시의경우 America/Los_Angeles 를입력합니다. 이름을입력하지않으면표준시간대가자동으로입력됩니다.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

값이앱에 Secure Hub 로하드코딩되어있기때문에이데이터는필요하지않습니다. 여기서는완결성을위해언급되었습니다.

예를들어 WPA2 를사용하여보호되는 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=ga50TwdCmfdJ72LGRFkke4Crb
\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=ga50TwdCmfdJ72LGRFkke4Crb
\u003d
```


android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Citrix Secure Hub 체크섬을얻으려면

Secure Hub 체크섬은상수값 (qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM) 입니다. Secure Hub 의 APK 파일을다운로드하려면다음 Google Play 스토어링크를사용하십시오. https://play.google.com/managed/downloadManagingApp?identifier=xenmobile

앱체크섬을얻으려면

사전요구사항:

- Android SDK Build Tools 의 **apksigner** 도구
- OpenSSL 명령줄

모든앱의체크섬을얻으려면다음단계를따르십시오.

1. Google Play 스토어에서앱의 APK 파일을다운로드합니다.
2. OpenSSL 명령줄에서 **apksigner** 도구: android-sdk/build-tools/<version>/apksigner로 이동하고다음내용을입력합니다.

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

명령이유효한체크섬을반환합니다.

3. QR 코드를생성하려면 PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM 필드에체크섬을입력합니다. 예:

```
{

  ”android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME”: ”com.zenprise/com.zenprise.configuration.AdminFunction”,
  ”android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM”:”qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM”,
```



```
5    "android.app.extra.
        PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
        play.google.com/managed/downloadManagingApp?identifier=xenmobile",
6    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
7
8        "serverURL": "https://supportablility.xm.cloud.com"
9      }
10
11   }
12
13 <!--NeedCopy-->
```

사용된라이브러리

Provisioning Tool 의소스코드에는다음과같은라이브러리가사용되었습니다.

- Apache 라이센스 2.0 에따라 Google 이제작한 v7 appcompat 라이브러리, 디자인지원라이브러리및 v7 `appcompat` 라이브러리

  자세한내용은 지원라이브러리기능가이드를참조하십시오.

- Apache 라이센스 2.0 에따라 Jake Wharton 이제작한 Butter Knife

QR 코드를사용하여장치등록

QR 코드를사용하여완전하게관리되는장치를등록하려면 JSON 을생성하고 JSON 을 QR 코드로변환하여 QR 코드를생성합니다. QR 코드가장치카메라로스캔되어장치가등록됩니다.

시스템요구사항

- Android 9.0 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: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

키: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

값: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

다음필드는선택사항입니다.

- **android.app.extra.PROVISIONING_LOCALE:** 언어및국가코드를입력합니다.

  언어코드는 ISO 639-1에정의된대로소문자두자로구성된 ISO 언어코드입니다 (예: en). 국가코드는 ISO 3166-1에정의된대로대문자두자로구성된 ISO 국가코드입니다 (예: US). 예를들어, 미국에서사용하는영어의경우 en_US 를입력합니다.

- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가실행되고있는표준시간대입니다.

  지역/위치형식의 Olson 이름을입력합니다. 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) 이후경과한시간이며, 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": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

JSON 유효성검사도구 (예: https://jsonlint.com) 를사용하여생성된 JSON 의유효성을검사하고온라인 QR 코드생성기 (예: https://www.qr-code-generator.com) 를사용하여해당 JSON 문자열을 QR 코드로변환합니다.

이 QR 코드는공장기본값으로재설정된장치에서스캔되어해당장치를완전관리형장치로등록하는데사용됩니다.

장치를등록하려면

새장치또는공장기본값으로재설정된장치의전원을켠후:

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.

제로터치등록

제로터치등록을사용하면장치전원을처음켤때완전관리형장치로프로비전하도록설정할수있습니다.

장치에구성을적용할때사용할수있는온라인도구인 Android 제로터치포털에서장치리셀러를통해계정을만들수있습니다. 그런다음 Android 제로터치포털에서하나이상의제로터치등록구성을만들고계정에할당된장치에구성을적용합니다. 사용자가이러한장치의전원을켜면장치가자동으로 XenMobile 에등록됩니다. 장치에할당된구성에따라자동등록프로세스가정의됩니다.

시스템요구사항

- 제로터치등록에대한지원은 Android 9.0 부터시작됩니다.

리셀러의장치및계정정보

- 제로터치등록이가능한장치는엔터프라이즈리셀러또는 Google 파트너로부터구입할수있습니다. Android Enterprise 제로터치파트너목록은 Android 웹사이트를참조하십시오.
- 리셀러를통해만든 Android Enterprise 제로터치포털계정.
- 리셀러가제공하는 Android Enterprise 제로터치포털계정로그인정보.

제로터치구성만들기

제로터치구성을만들때는구성세부정보를지정하는사용자지정 JSON 을포함합니다.

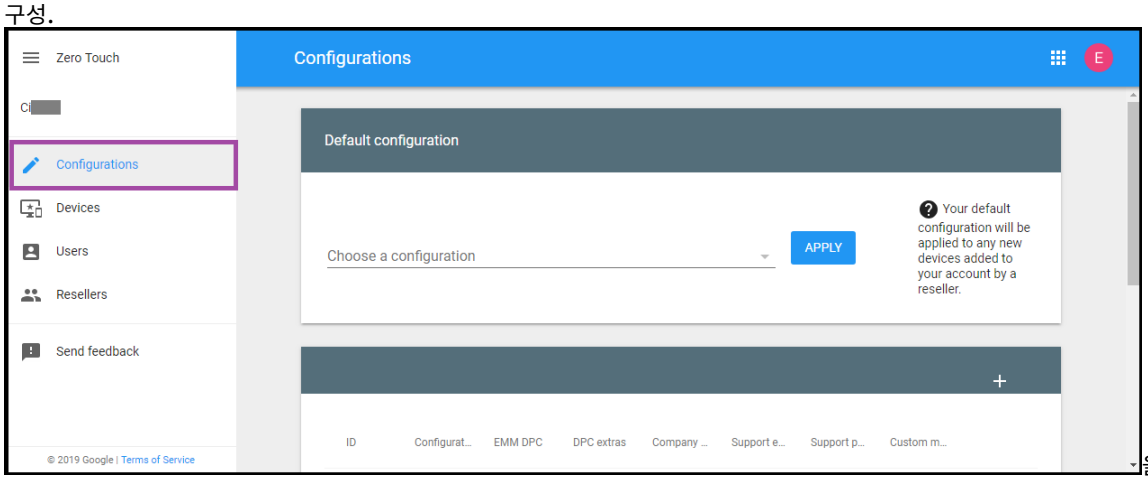
이 JSON 을사용하여지정한 XenMobile Server 에등록할장치를구성합니다. 이예에서는 'URL' 을서버의 URL 로대체하십시오.

```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL",
7            }
8
9         }
10
11 <!--NeedCopy-->
```


매개변수가더많은선택적 JSON 을사용하여구성을추가로사용자지정할수있습니다. 이예에서는 XenMobile Server 와이구성을사용하는장치가서버에로그온할때사용하는사용자이름과암호를지정합니다.

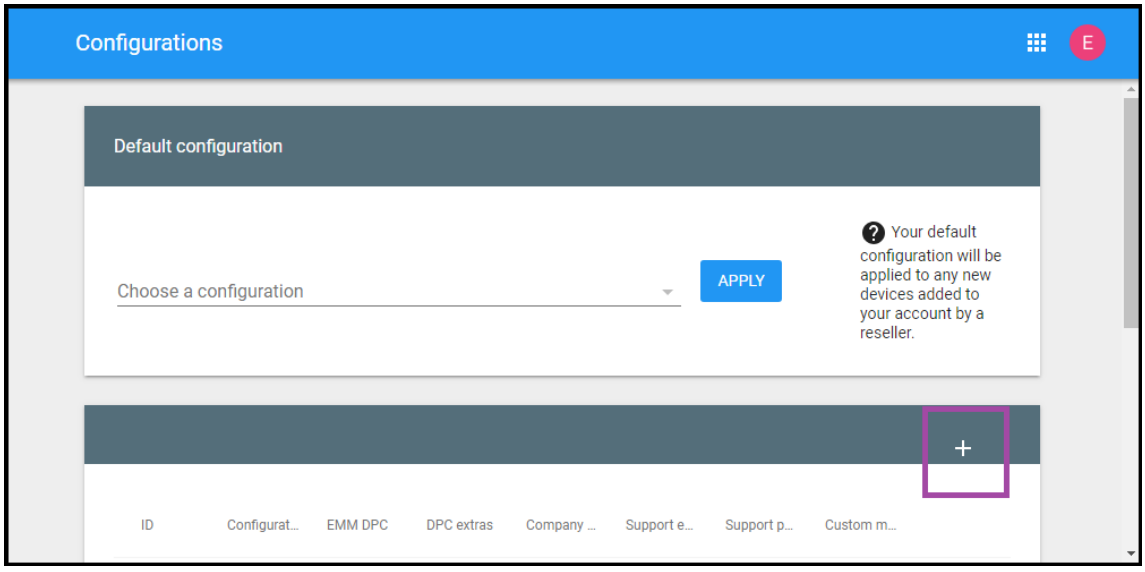
```
{

   ”android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE”:
     {

         ”serverURL”:”URL”,
         ”xm_username”:”username”,
         ”xm_password”:”password”
      }

        }

<!--NeedCopy-->
```

1. https://partner.android.com/zerotouch에서 Android 제로터치포털로이동합니다. 제로터치장치리셀러의계정정보를사용하여로그인합니다.
2. 구성.

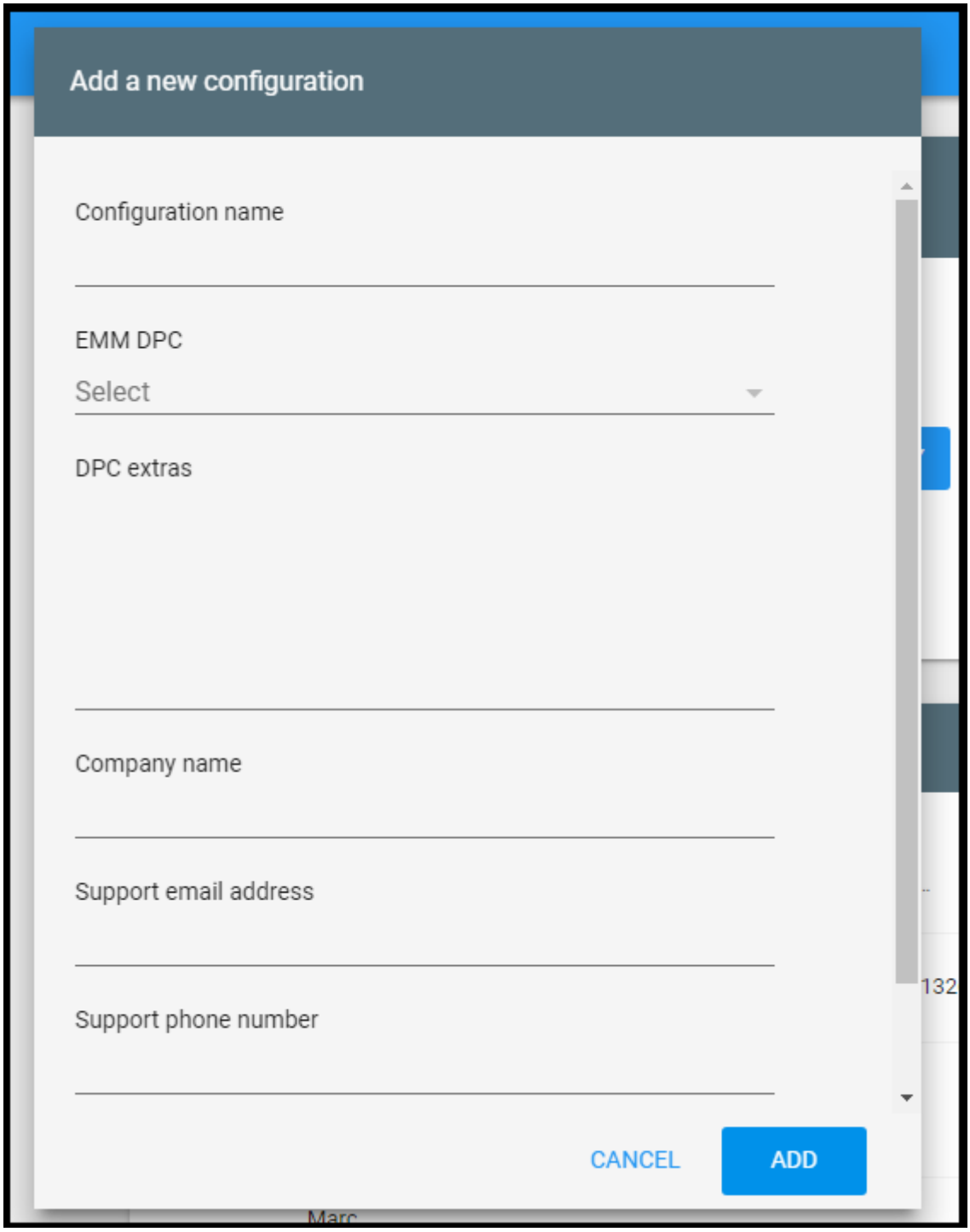


을 클릭합니다.

3. 구성테이블위에서 **+** 를클릭합니다.



4. 구성창이표시되면구성정보를입력합니다.



- **Configuration name(구성이름):** 이구성에대해선택한이름을입력합니다.
- **EMM DPC: Citrix Secure Hub** 를선택합니다.
- **DPC extras(DPC 추가항목):** 이필드에사용자지정 JSON 텍스트를붙여넣습니다.
- **Company name(회사이름):** 장치프로비전중에 Android Enterprise 제로터치장치에표시할이름을입력합니다.
- **Support email address(지원전자메일주소):** 사용자가지원을문의할수있는전자메일주소를입력합니다. 이

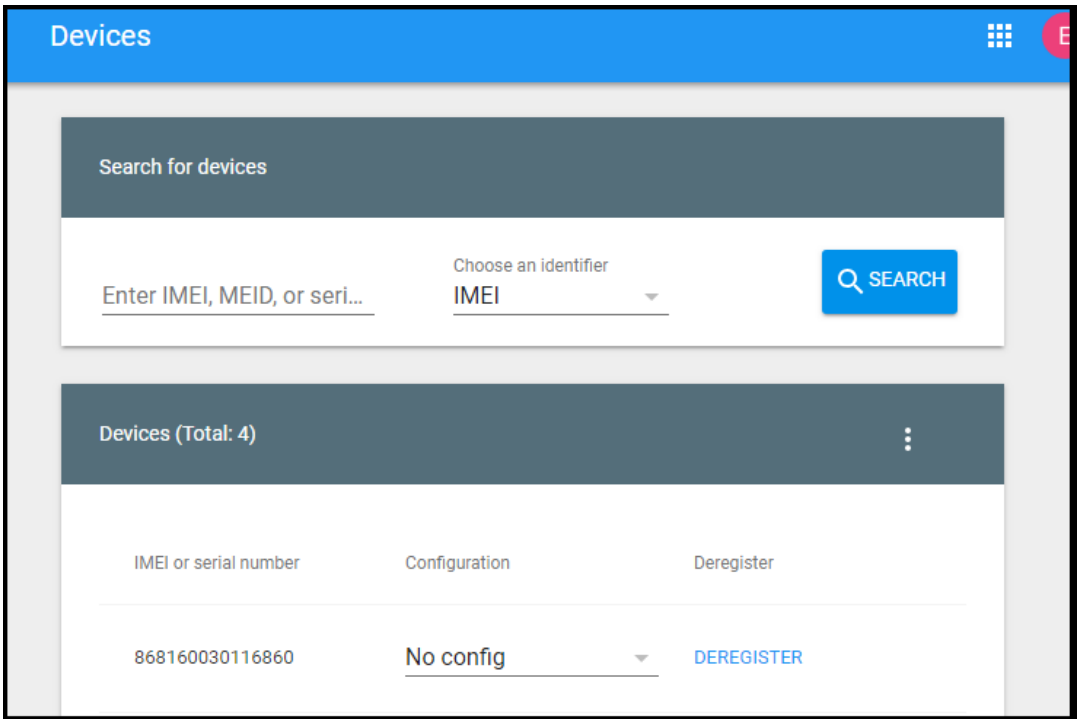
주소는장치프로비전전에 Android Enterprise 제로터치장치에나타납니다.

- **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 관리자를위한제로터치등록을참조하십시오. 이 Android Enterprise 도움말항목에는구성을관리하고장치에구성을적용하는방법에대한자세한정보가나와있습니다.

전용 **Android Enterprise** 장치프로비전

전용 Android Enterprise 장치는단일사용사례를이행하는데전용으로사용되는완전관리형장치입니다. 전용장치를 COSU(회사소유일회사용) 장치라고도합니다. 이러한장치는이사용사례에필요한작업을수행하는데필요한단일앱또는소수의앱으로제한되

어야합니다. 또한사용자가장치에서다른앱을사용하도록설정하거나다른작업을수행하지못하도록차단해야합니다.

Android Enterprise 로완전히관리되는장치프로비저닝에설명된대로완전관리되는다른장치에사용되는등록방법중하나를사용하여전용장치를등록합니다. 전용장치를프로비전하려면등록하기전에추가설정이필요합니다.

전용장치를프로비전하려면:

- XenMobile 배포에전용장치를등록할수있도록허용하는 XenMobile 관리자용등록프로필을추가합니다. 등록프로필만들기를참조하십시오.
- 전용장치에서액세스할앱을허용합니다.
- 필요한경우작업잠금모드를허용하도록허용된앱을설정합니다. 앱이작업잠금모드에있으면사용자가앱을열때앱이장치화면에고정됩니다. 홈단추가나타나지않고뒤로단추가비활성화됩니다. 사용자는로그아웃과같이앱에프로그래밍된작업을사용하여앱을종료할수있습니다.
- 추가한등록프로필로각장치를등록합니다.

시스템요구사항

- 전용장치등록지원은 Android 6.0 부터시작됩니다.

앱허용및작업잠금모드설정

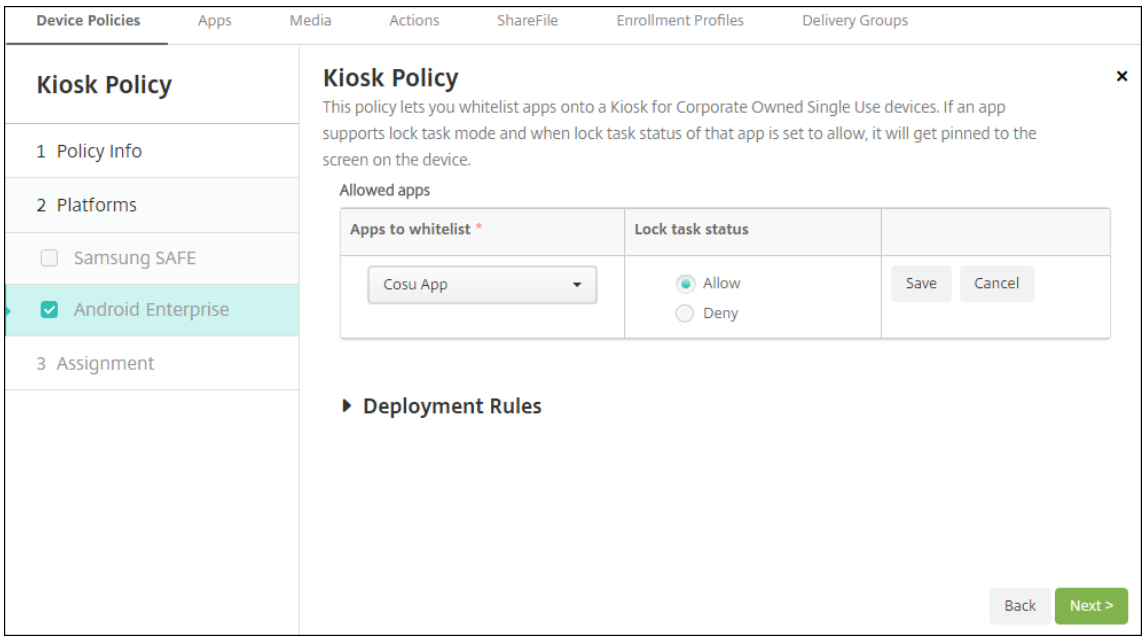
키오스크장치정책을사용하면앱을허용하고작업잠금모드를설정할수있습니다. 기본적으로 Secure Hub 와 Google Play 서비스는허용됩니다.

키오스크정책을추가하려면:

1. XenMobile 콘솔에서 구성 **>** 장치정책을클릭합니다. 장치정책페이지가나타납니다.
2. 추가를클릭합니다. 새정책추가대화상자가나타납니다.
3. 자세히를확장한후보안아래에서 키오스크를클릭합니다. 키오스크정책페이지가나타납니다.
4. 플랫폼에서 **Android Enterprise** 를선택합니다. 다른플랫폼을지웁니다.
5. 정책정보창에서 정책이름과필요한경우 설명을입력합니다.
6. 다음을클릭한후 추가를클릭합니다.
7. 앱을허용하고해당앱에대한작업잠금모드를허용또는거부하려면:

   목록에서허용할앱을선택합니다.

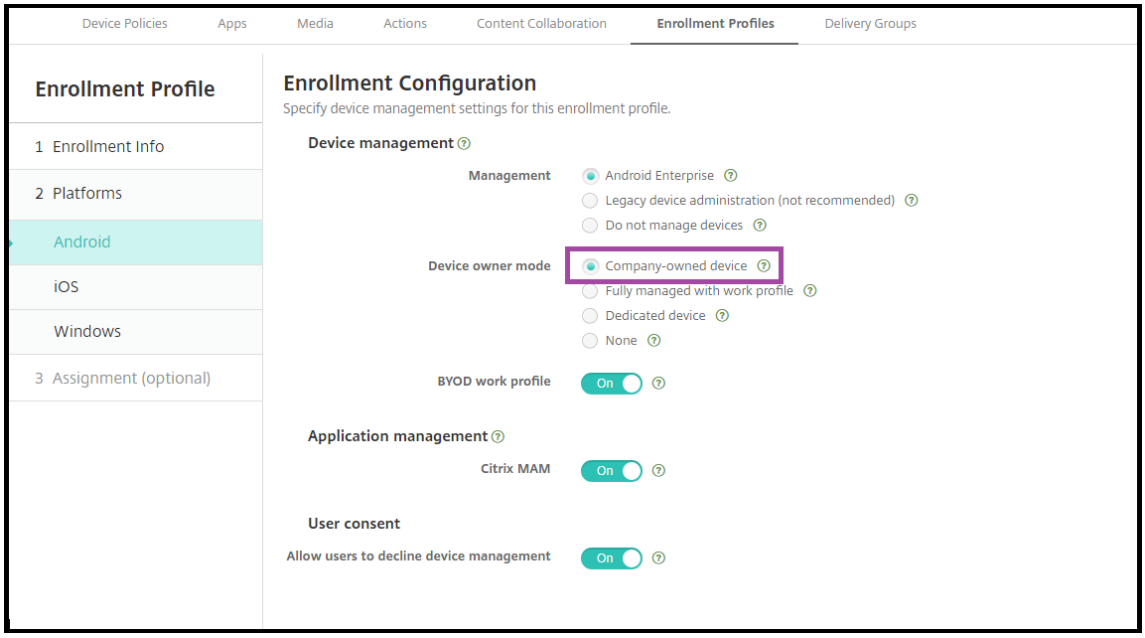
   사용자가앱을시작할때장치화면에앱이고정되도록설정하려면 허용을선택합니다. 앱이고정되지않도록설정하려면 거부를선택합니다. 기본값은 허용입니다.



8. 저장을클릭합니다.
9. 다른앱을허용하고해당앱에대한작업잠금모드를허용또는거부하려면 추가를클릭합니다.
10. 배포규칙을구성하고배달그룹을선택합니다. 자세한내용은 장치정책을참조하십시오.

장치를등록하려면

1. 다음을클릭하거나 플랫폼에서 **Android** 를선택합니다. 등록구성페이지가나타납니다.
2. 관리를 **Android Enterprise** 로설정합니다.
3. 장치소유자모드를 기업소유장치로설정합니다.



4. 할당 **(**옵션**)** 을선택합니다. 배달그룹할당화면이나타납니다.
5. 전용장치를등록하는관리자가포함된배달그룹을선택합니다. 그런다음 저장을클릭합니다.

등록프로필에서 **BYOD** 작업프로필을설정하면신규장치가아니거나공장기본값으로재설정되지않은장치가작업프로필장치로등록됩니다. Android Enterprise 작업프로필장치프로비전을참조하십시오.

작업프로필이있는완전관리형 **Android Enterprise** 장치 **(COPE** 장치**)** 프로비전

작업프로필로완전히관리되는장치 (이전의 COPE 장치) 는업무용및개인용으로사용되는회사소유의장치입니다. 전체장치는조직에서관리합니다. 하나의정책집합을장치에적용하고개별정책집합을작업프로필에적용할수있습니다.

XenMobile 콘솔에서작업프로필로완전히관리되는장치는다음과같은용어로표시됩니다.

- 장치소유권은 “회사” 입니다.
- 장치 Android Enterprise 설치유형은 “회사소유개인사용” 입니다.

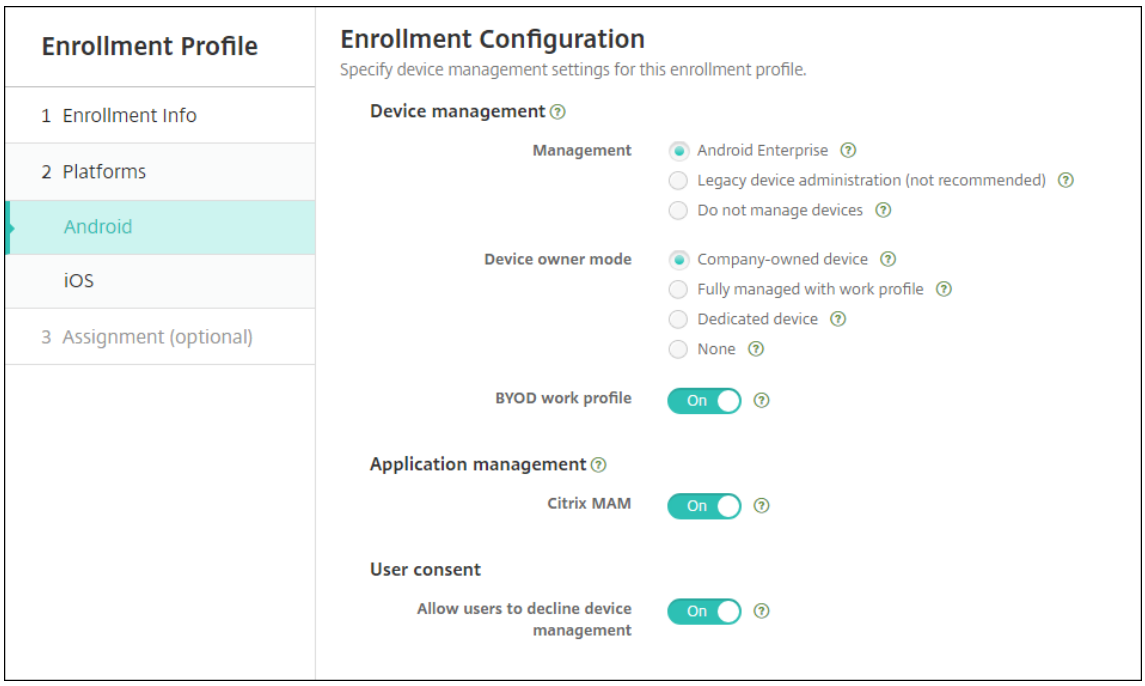
시스템요구사항

- 작업프로필로완전히관리되는장치의등록은 Android 9.0 부터 Android 10.x 까지지원됩니다.

작업프로필로완전히관리되는장치에대한등록프로필추가

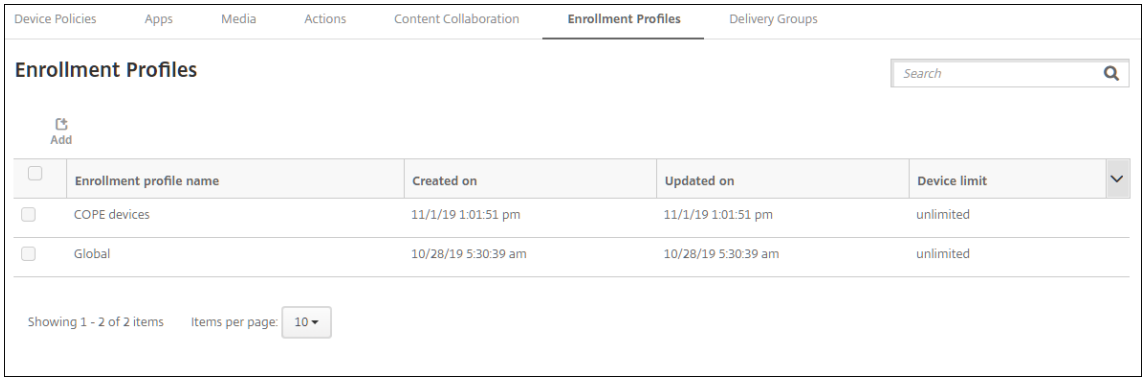
작업프로필로완전히관리되는장치의등록을위한등록프로필을만듭니다. 이등록프로필에할당된배달그룹의관리자는완전관리형장치를작업프로필에등록할수있습니다. 이러한관리자가필요한모든장치를등록할수있도록하려면사용자당무제한의장치가허용되는관리자용등록프로필을만듭니다. 작업프로필로완전히관리되는장치를등록하는관리자가포함된배달그룹에이프로필을할당합니다.

1. XenMobile 콘솔에서 구성 **>** 등록프로필로이동합니다.
2. 등록프로필을추가하려면 추가를클릭합니다. 등록정보페이지에서등록프로필의이름을입력합니다. 이프로필을가진구성원이등록할수있는장치수가무제한으로설정되어있는지확인합니다.
3. 다음을클릭하거나 플랫폼에서 **Android Enterprise** 를선택합니다. 등록구성페이지가나타납니다.
4. 등록유형을다음중하나로설정합니다.
    - 완전관리형프로필**/**작업프로필**:** 새장치또는공장기본값으로재설정된장치가완전관리형장치로등록됩니다. BYOD 장치는사용자가관리하는작업프로필을통해서만등록됩니다.
    - **COPE/**작업프로필**:** 새장치또는공장기본값으로재설정된장치가작업프로필을사용하여완전관리형장치로등록됩니다. BYOD 장치는사용자가관리하는작업프로필을통해서만등록됩니다.



5. 할당 (선택사항) 을선택하거나 다음을클릭합니다. 배달그룹할당화면이나타납니다.
6. 전용장치를등록하는관리자가포함된배달그룹을선택합니다. 그런다음 저장을클릭합니다.

   추가한프로필과함께등록프로필페이지가나타납니다.



사용자가등록프로필이다른여러배달그룹에속하는경우사용되는등록프로필은배달그룹의이름에따라결정됩니다. XenMobile 은사전순으로표시된배달그룹목록의마지막에나타나는배달그룹을선택합니다.

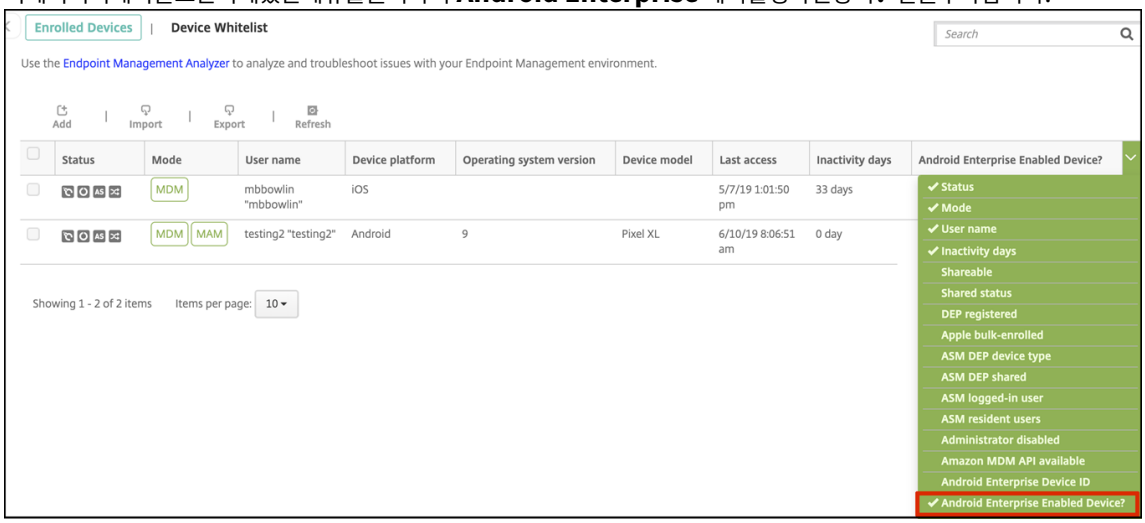
장치를등록하려면

새장치또는공장기본값으로재설정된장치는 DPC 식별자토큰, NFC(근거리통신) 범프또는 QC 코드방법을사용하여작업프로필로완전히관리되는장치로등록됩니다. Citrix DPC 식별자토큰을사용하여장치등록, NFC 범프를사용하여장치등록 또는QR 코드를사용하여장치등록을참조하십시오.

새장치또는공장기본값으로재설정된장치는 Android Enterprise 작업프로필장치프로비저닝에설명된대로작업프로필장치로등록됩니다.

XenMobile 콘솔에서 **Android Enterprise** 장치보기

1. XenMobile 콘솔에서 관리 **>** 장치로이동합니다.
2. 이페이지의테이블오른쪽에있는메뉴를클릭하여 **Android Enterprise** 에서활성화된장치**?** 열을추가합니다.



3. 사용가능한보안동작을보려면완전관리형장치를선택하고 보안을클릭합니다. 장치가완전관리형경우 전체초기화작업을사용할수있지만 선택적초기화는사용할수없습니다. 이차이는장치가관리되는 Google Play Store 의앱만허용하기때문입니다. 사용자가공용스토어에서응용프로그램을설치할수있는옵션은없습니다. 장치의모든콘텐츠는조직에서관리합니다.

Android Enterprise 장치및앱정책구성

기기및앱수준모두에서제어되는정책에대한개요는 Android Enterprise 에서지원되는기기정책및 MDX 정책을참조하십시오.

정책에대해알아야할사항:

- 데이터손실방지**:** XenMobile MAM 컨테이너기술은암호화및기타모바일 DLP(데이터손실방지) 기술로앱을보호합니다. MDX 지원앱에대해 Citrix MAM SDK 또는 MDX Toolkit 을사용합니다.
- 기기제한**:** 수십가지기기제한을통해다음과같은기능을제어할수있습니다.
  - 장치카메라의사용
  - 업무및개인프로필간복사및붙여넣기사용
- 앱별 **VPN:** 관리되는구성장치정책을사용하여 Android Enterprise 용 VPN 프로필을구성합니다.
- 전자메일정책**:** 관리되는구성장치정책을사용하여앱을구성하는것이좋습니다.

다음표에는 Android Enterprise 장치에사용할수있는모든장치정책이나열되어있습니다.

> 중요**:**
>
> Android Enterprise 에등록하고 MDX 앱을사용하는장치의경우: MDX 및 Android Enterprise 를통해일부설정을제어할수있습니다. MDX 에대해제한이최소한인정책설정을사용하고 Android Enterprise 를통해정책을제어합니다.

Android Enterprise 앱권한	관리되는구성	앱인벤토리
앱제거	관리되는앱자동업데이트	OS 업데이트제어
자격증명	사용자지정 XML	Exchange
Files	Keyguard 관리	키오스크
위치	암호	제한사항
Samsung MDM 라이센스키	예약	Wi-Fi
XenMobile 옵션		

작업프로필로완전히관리되는장치의장치정책 **(COPE** 장치**)**

작업프로필로완전히관리되는장치 (COPE 장치) 의경우일부장치정책을사용하여전체장치와작업프로필에개별설정을적용할수있습니다. 다른장치정책을사용하여전체장치에만설정을적용하거나작업프로필로완전히관리되는장치의작업프로필에만설정을적용할수있습니다.

정책	적용대상
Android Enterprise 앱권한	작업프로필
관리되는구성	작업프로필
앱인벤토리	작업프로필
앱제거	작업프로필

정책	적용대상
관리되는앱자동업데이트	작업프로필
OS 업데이트제어	해당없음
자격증명	작업프로필
사용자지정 XML	해당없음
Exchange	해당없음
Files	작업프로필
Keyguard 관리	장치및작업프로필
키오스크	해당없음
위치	장치 (위치모드만해당)
암호	장치및작업프로필
제한사항	장치및작업프로필 (장치및작업프로필에대한개별정책만들기)
Samsung MDM 라이센스키	해당없음
예약	작업프로필
Wi-Fi	장치
XenMobile 옵션	작업프로필

Android Enterprise 의지원되는장치정책및 MDX 정책 및 MAM SDK 개요도참조하십시오.

보안동작

Android Enterprise 는다음과같은보안동작을지원합니다. 각보안동작에대한설명은 보안동작을참조하십시오.

보안동작	작업프로필	완전관리형
인증서갱신	예	예
전체초기화	아니요	예
찾기	예	예
잠금	예	예
Lock and Reset Password(잠금및암호재설정)	아니요	예
Notify (Ring)(알림 (벨울림))	예	예

보안동작	작업프로필	완전관리형
해지	예	예
선택적초기화	예	아니요

보안동작참고사항

- 위치장치정책에서장치에대한위치모드를 높은정확도또는 배터리절약으로설정하지않으면찾기보안동작이실패합니다. 위치장치정책을참조하십시오.
- Android 9.0 이전버전의 Android 를실행하는작업프로필장치:
  - 잠금및암호재설정작업이지원되지않습니다.
- Android 9.0 이상인작업프로필장치:
  - 전송된암호로작업프로필이잠깁니다. 장치자체는잠기지않습니다.
  - 작업프로필에암호가설정되지않은경우:
    * 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않는경우: 장치가잠깁니다.
  - 작업프로필에암호가설정된경우:
    * 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않는경우: 작업프로필은잠기지만장치자체는잠기지않습니다.
- 작업프로필로완전히관리되는장치 (COPE 장치):
  - 장치또는작업프로필에잠금보안동작을개별적으로적용할수있습니다.

Android Enterprise 엔터프라이즈등록취소

Android Enterprise 엔터프라이즈를더이상사용하지않으려면엔터프라이즈등록을취소하면됩니다.

> 경고**:**
>
> 엔터프라이즈등록이취소되면엔터프라이즈를통해이미등록된장치의 Android Enterprise 앱이기본상태로재설정됩니다. Google 은더이상장치를관리하지않습니다. 새로운 Android Enterprise 에등록하는경우관리되는 Google Play 에서새조직의앱을승인해야합니다. 그런다음에야 XenMobile 콘솔에서앱을업데이트할수있습니다.

Android Enterprise 엔터프라이즈등록취소후:

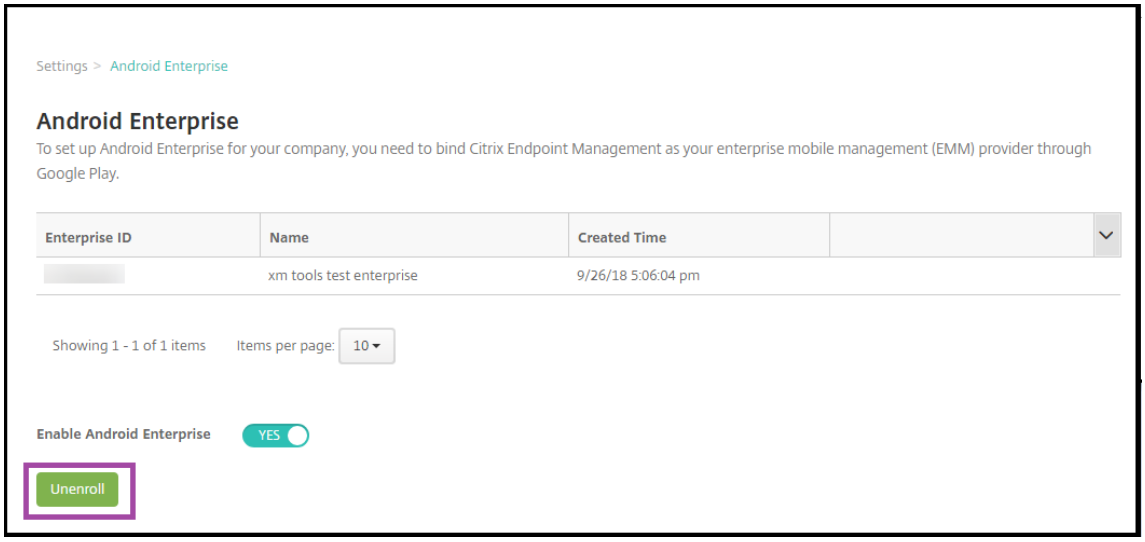
- 엔터프라이즈를통해등록된장치및사용자의 Android Enterprise 앱이기본상태로재설정됩니다. 이전에적용된관리되는구성정책은더이상작업에영향을미치지않습니다.
- XenMobile 은엔터프라이즈를통해등록된장치를관리합니다. Google 의관점에서이러한장치는관리되지않는장치입니다. 새로운 Android Enterprise 앱을추가할수없습니다. 관리되는구성정책을적용할수없습니다. 예약, 암호및제한같은다른정책을이러한장치에적용할수있습니다.
- Android Enterprise 에장치를등록하려고하면 Android Enterprise 장치가아닌 Android 장치로등록됩니다.

XenMobile Server 콘솔및 XenMobile Tools 를사용하여 Android Enterprise 엔터프라이즈를등록취소합니다.

이작업을수행하면 XenMobile 에서 XenMobile Tools 에대한팝업창이열립니다. 시작하기전에사용하는브라우저에서팝업창을여는데필요한권한이 XenMobile 에있는지확인하십시오. Google Chrome 같은일부브라우저의경우팝업차단을사용하지않도록설정하고 XenMobile 사이트주소를팝업차단허용목록에추가해야합니다.

Android Enterprise 엔터프라이즈를등록취소하려면:

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 설정페이지에서 **Android Enterprise** 를클릭합니다.
3. 등록취소를클릭합니다.



Android Enterprise 앱배포

January 6, 2022

XenMobile 은장치에배포되는앱을관리합니다. 다음유형의 Android Enterprise 앱을구성하고배포할수있습니다.

- 관리되는앱스토어앱**:** 이러한앱으로는관리되는 Google Play 스토어에서이용할수있는무료또는유료앱이있습니다. 예를들어 GoToMeeting 이포함됩니다.
- **MDX:** MAM SDK 로준비되거나 MDX Toolkit 으로래핑되는앱입니다. 이러한앱에는 MDX 정책이포함됩니다. 내부및공용스토어에서 MDX 앱을얻을수있습니다. Citrix 모바일생산성앱을 MDX 앱으로배포합니다.
- **Enterprise:** 직접개발하거나다른출처에서획득한개인앱입니다. 이러한앱은관리되는 Google Play 스토어를통해사용자에게제공합니다. 관리되는 Google Play 스토어는 Google 엔터프라이즈앱스토어입니다.
- **MDX** 지원개인앱**:** MAM SDK 로준비되거나 MDX Toolkit 으로래핑된엔터프라이즈앱입니다.

엔터프라이즈앱과 MDX 지원개인앱을두가지방식으로추가할수있습니다.

- 이문서의엔터프라이즈앱 및MDX 지원개인앱 섹션에설명된대로 XenMobile 콘솔에앱을엔터프라이즈앱으로추가합니다.

- Google 개발자계정을사용하여관리되는 Google Play 스토어에앱을직접게시합니다. 그런다음 XenMobile 콘솔에앱을관리되는앱스토어앱으로추가합니다. 관리되는앱스토어앱을참조하십시오.

Google 개발자계정을사용하여앱을게시한다음 XenMobile 콘솔사용으로전환할경우앱의소유권이달라집니다. 이경우두위치모두에서앱을관리합니다. Citrix 에서는한가지방법으로앱을추가하는것을권장합니다.

관리되는 Google Play 스토어에서자체관리앱을제거해야하는경우 Google 에티켓을개시합니다. 개발자가관리되는 Google Play 스토어에서앱을비활성화할수는있지만삭제할수는없습니다.

다음섹션에서는 Android Enterprise 앱구성에관해더자세히알아봅니다. 앱배포에관한자세한내용은 앱추가를참조하십시오. 이문서에는다음이포함됩니다.

- 웹및 SaaS 앱또는웹링크를추가하는일반적인워크플로
- 엔터프라이즈및공용스토어앱을위한필수앱워크플로
- 엔터프라이즈앱용 Citrix CDN(콘텐츠배달네트워크) 에서엔터프라이즈앱을제공하는방법

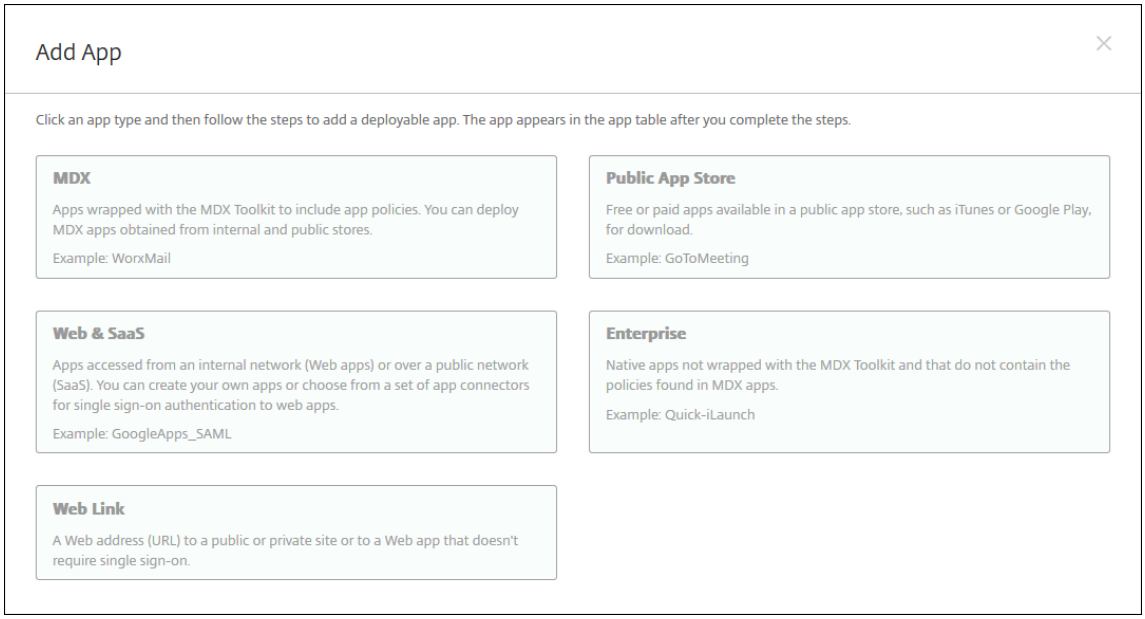
관리되는앱스토어앱

관리되는 Google Play 스토어에서유료또는무료로제공되는앱을 XenMobile 에추가할수있습니다.

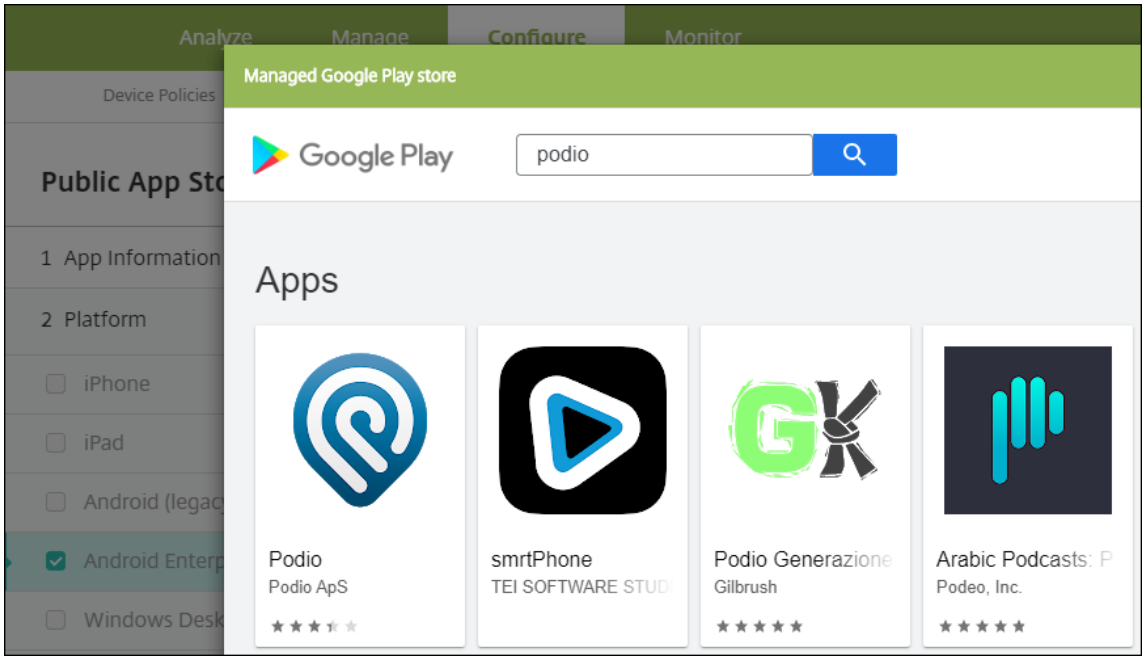
> 참고**:**
>
> 관리되는 Google Play 에서도 Google Play 스토어의모든앱에액세스할수있게만들려면 관리되는 **Google Play** 스토어의모든앱에액세스서버속성을사용합니다. 서버속성을참조하십시오. 이속성을 **true** 로설정하면모든 Android Enterprise 사용자가공용 Google Play 스토어앱에액세스할수있습니다. 이후 제한장치정책을사용하여이러한앱에대한액세스를제어할수있습니다.

1 단계**:** 앱추가및구성

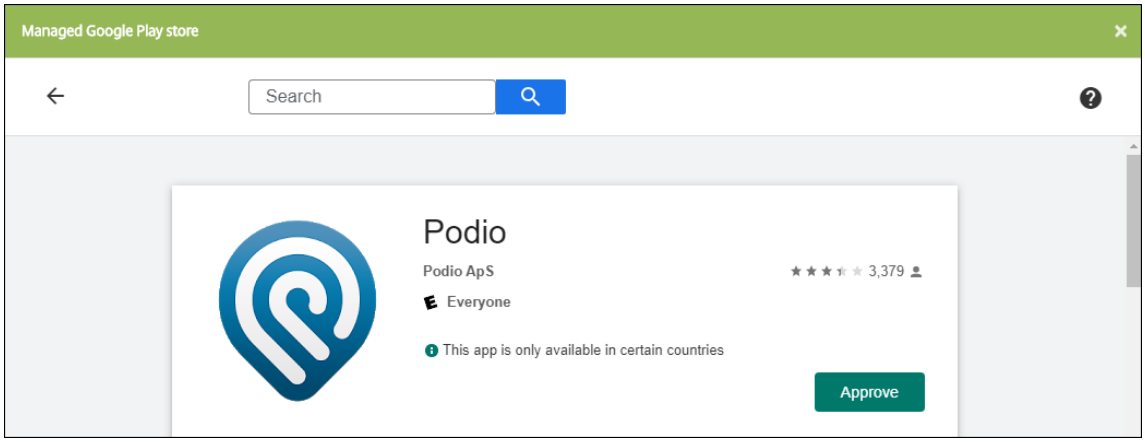
1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 추가를클릭합니다.
2. 공용앱스토어를클릭합니다.



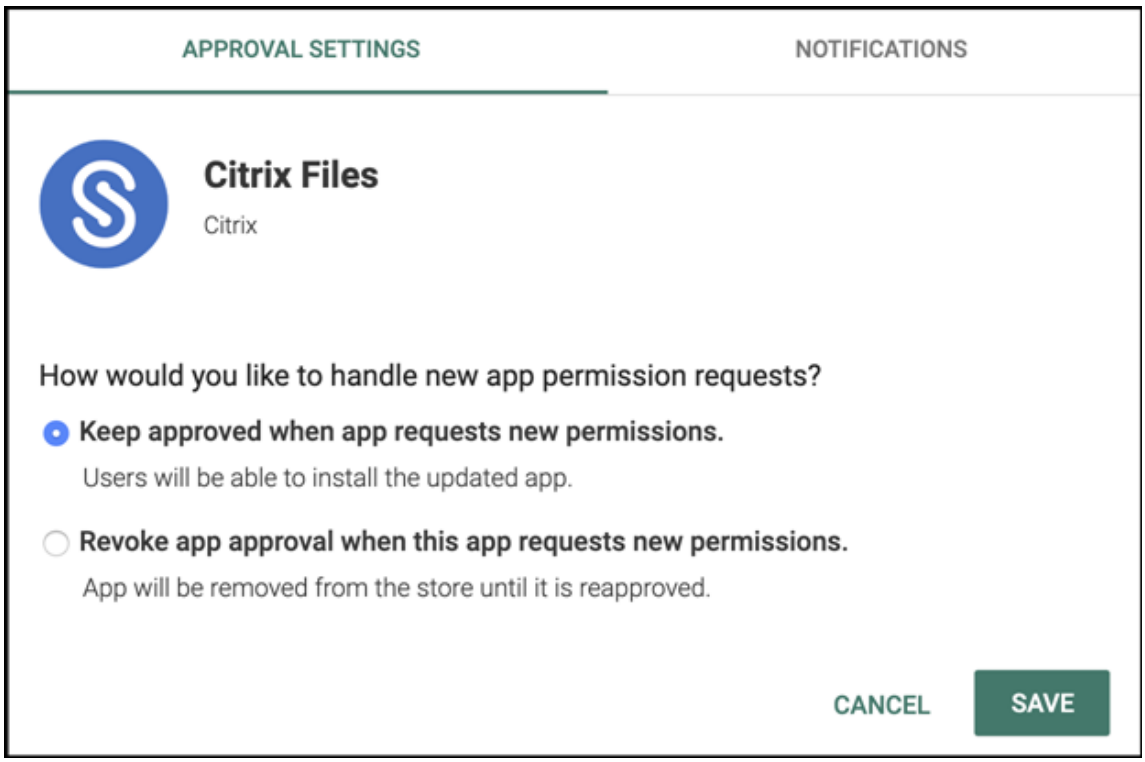
3. 앱정보창에서다음정보를입력합니다.
   - 이름**:** 앱을설명하는이름을입력합니다. 이이름은 앱테이블의 앱이름아래에표시됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은 앱범주정보를참조하십시오.
4. 플랫폼으로 **Android Enterprise** 를선택합니다.
5. 검색상자에앱이름또는패키지 ID 를입력하고 검색을클릭합니다. Google Play Store 에서패키지 ID 를찾을수있습니다. ID 는앱의 URL 에있습니다. 예를들어 `com.Slack`은 `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`의패키지 ID 입니다.



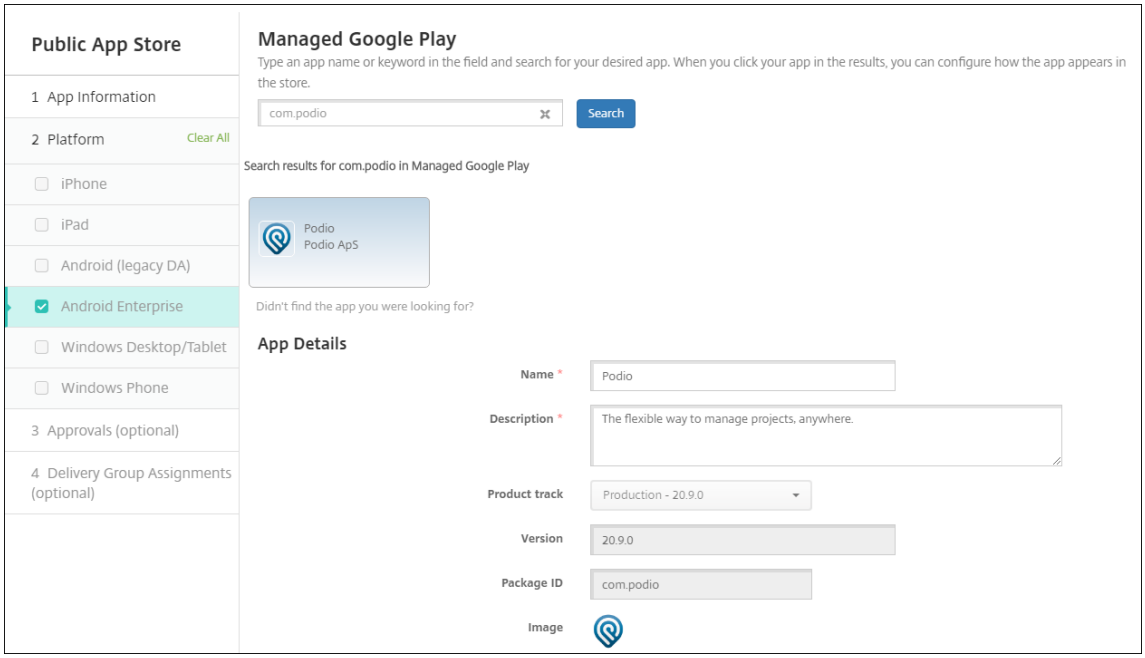
6. 검색기준과일치하는앱이표시됩니다. 원하는앱을클릭한다음 승인을클릭합니다.



7. **Approve(**승인**)** 를다시클릭합니다.
8. **Keep approved when app requests new permissions(**앱이새권한을요청할때승인된상태로유지**)** 를선택합니다. 저장을클릭합니다.



9. 앱아이콘을클릭하고앱 이름및 설명을구성합니다.

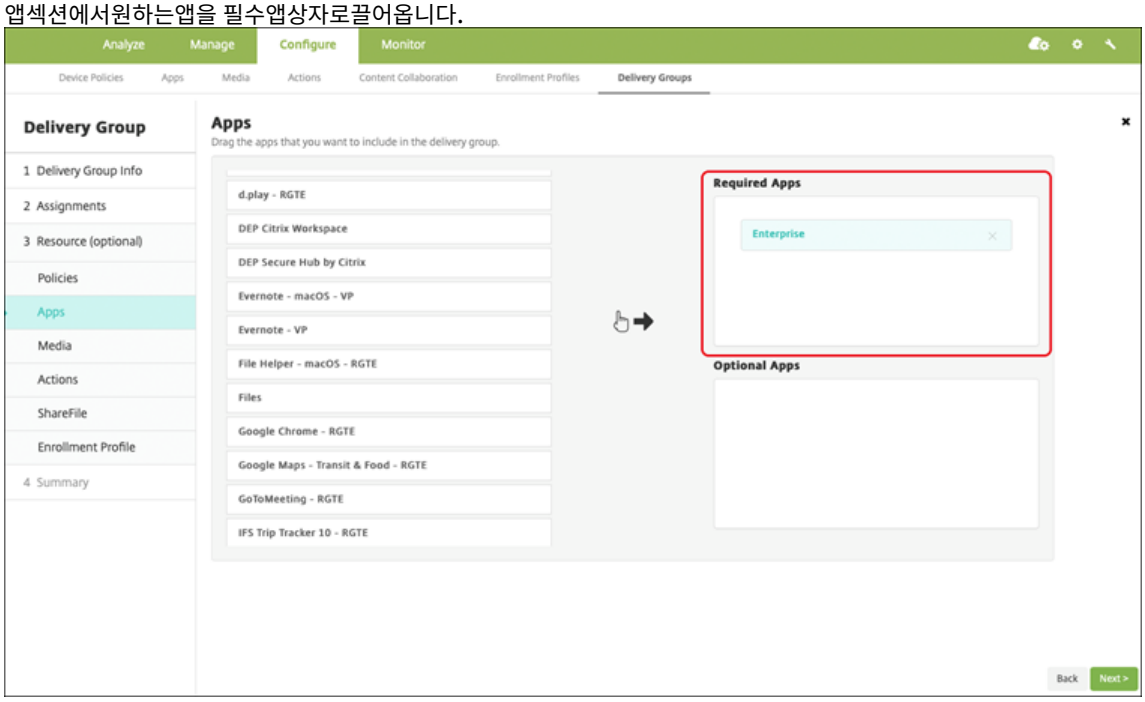


10. 앱에배달그룹을할당하고 저장을클릭합니다. 자세한내용은 리소스배포를참조하십시오.

2 단계**:** 앱배포구성

1. 구성 **>** 배달그룹으로이동한다음구성한배달그룹을선택합니다. 편집을클릭합니다.

2. 앱섹션에서원하는앱을 필수앱상자로끌어옵니다.



3. 요약페이지에서 저장을클릭합니다.
4. 배달그룹페이지에서배달그룹을선택하고 배포를클릭합니다.

MDX 앱

XenMobile 에 MDX 파일을추가하고앱세부정보와정책설정을구성합니다. Android Enterprise 에대해 Citrix 모바일생산성앱을구성하려면 MDX 앱으로추가합니다. 각장치플랫폼유형에사용할수있는앱정책에대한자세한내용은다음을참조하십시오.

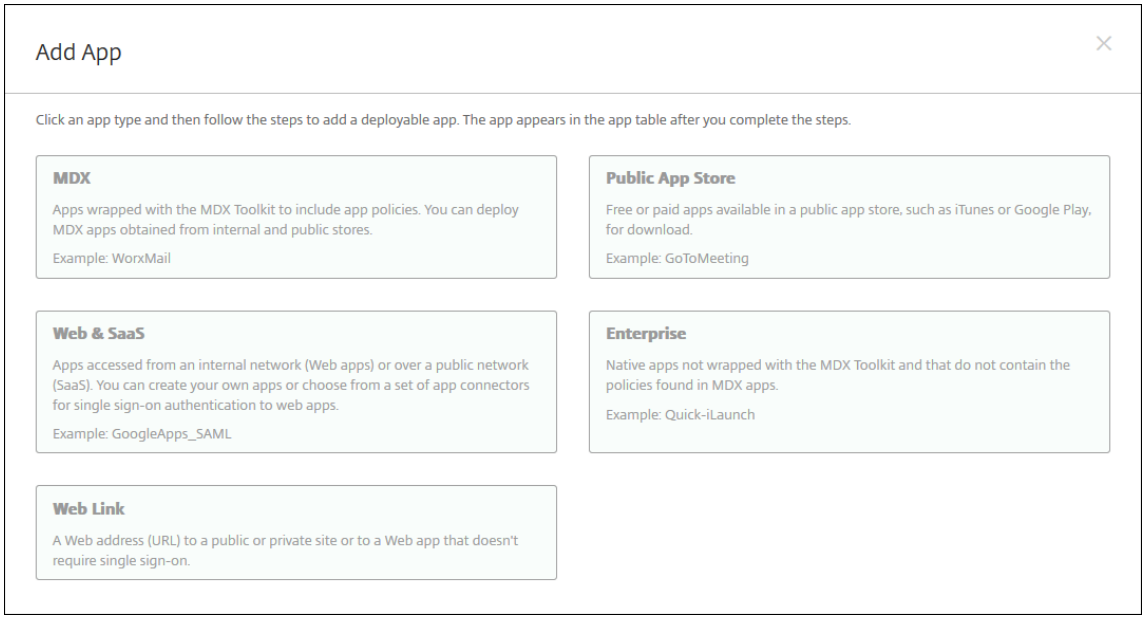
- MAM SDK Overview(MAM SDK 개요)
- MDX 정책요약

1 단계**:** 앱추가및구성

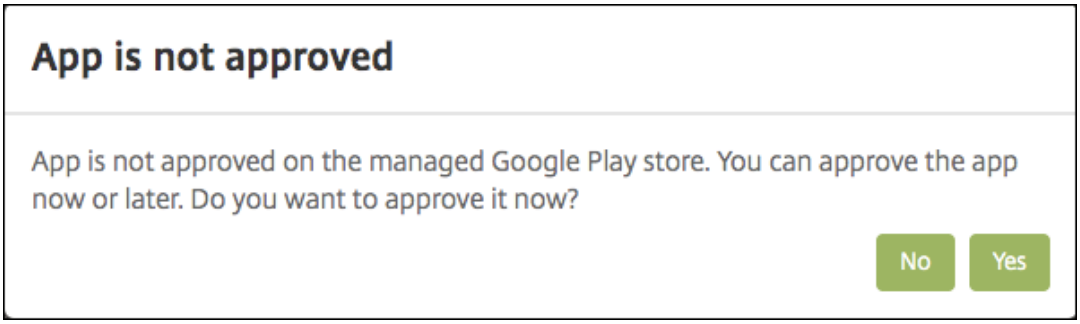
1. Citrix 모바일생산성앱의경우공용스토어 MDX 파일을다운로드하고 https://www.citrix.com/downloads로이동합니다. **Citrix Endpoint Management(XenMobile) > Citrix Endpoint Management** 생산성앱으로이동합니다.

   다른 MDX 앱유형의경우 MDX 파일을가져옵니다.

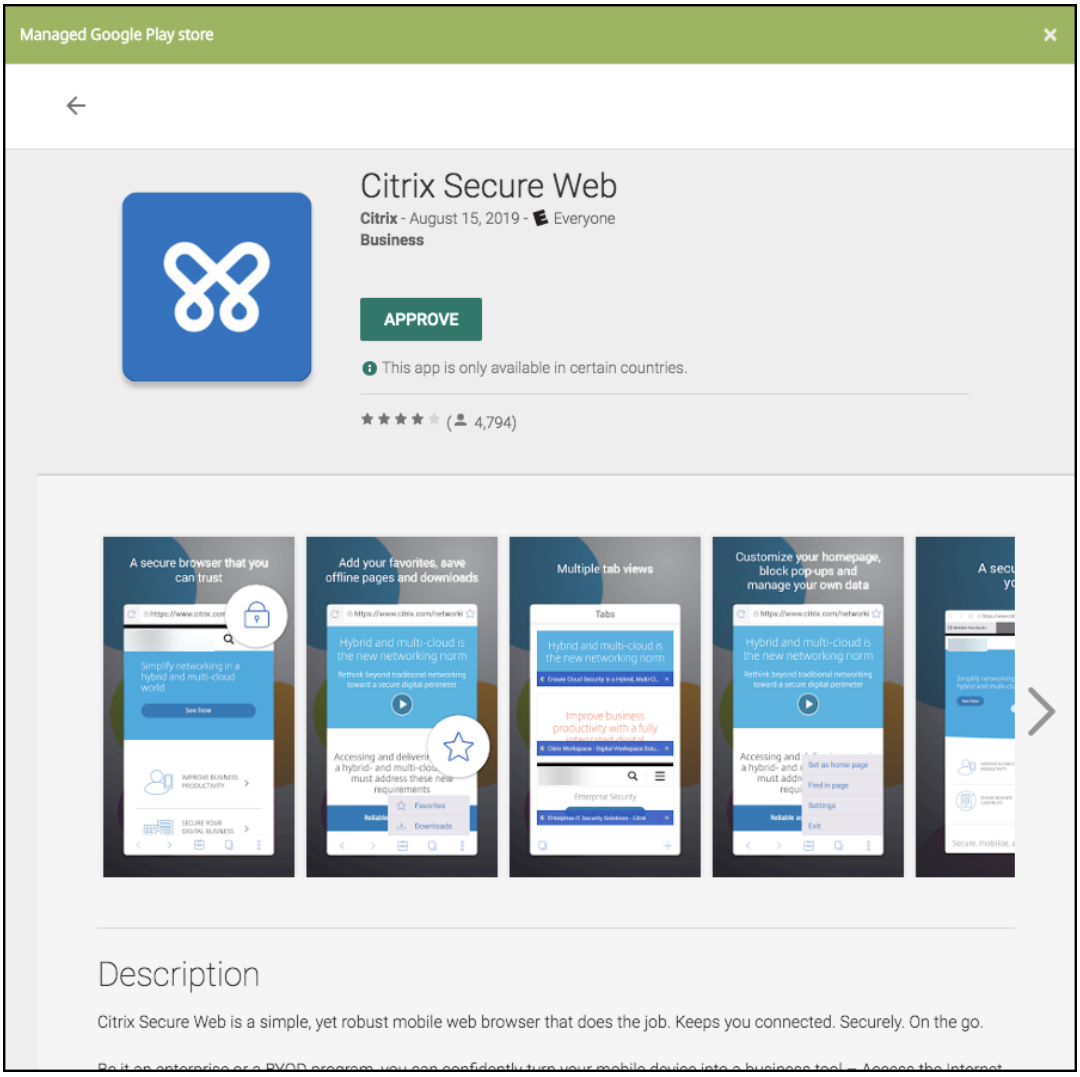
2. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 추가를클릭합니다. 앱추가대화상자가나타납니다.



3. **MDX** 를클릭합니다. **MDX** 앱정보페이지가나타납니다. 앱정보창에서다음정보를입력합니다.
   - 이름**:** 앱을설명하는이름을입력합니다. 이이름은 앱테이블의 앱이름아래에표시됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은 앱범주정보를참조하십시오.
4. 플랫폼으로 **Android Enterprise** 를선택합니다.
5. 업로드를클릭하고 MDX 파일로이동합니다. Android Enterprise 는 MAM SDK 또는 MDX Toolkit 으로준비한앱만지원합니다.
   - 연결된응용프로그램에관리되는 Google Play Store 의승인이필요한경우 UI 에알림이표시됩니다. XenMobile 콘솔을종료하지않고응용프로그램을승인하려면 예를클릭합니다.

     관리되는 Google Play Store 가열리면지침에따라앱을승인하고저장합니다.



앱이성공적으로추가되면 앱세부정보페이지가나타납니다.

6. 다음설정을구성합니다.

   - 파일이름**:** 앱에연결된파일이름을입력합니다.
   - 앱설명**:** 앱에대한설명을입력합니다.
   - 앱버전**:** 필요한경우앱버전번호를입력합니다.
   - 패키지 **ID:** 관리되는 Google Play 스토어에서가져온앱의패키지 ID 를입력합니다.
   - 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
   - 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
   - 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.

7. **MDX** 정책을구성합니다. MDX 정책은플랫폼별로다르며인증, 장치보안, 앱제한과같은정책영역에대한옵션이포함됩니다. 콘솔에서각정책에는정책을설명하는도구설명이포함됩니다. 각장치플랫폼유형에사용할수있는앱정책에대한자세한내용은다음을참조하십시오.

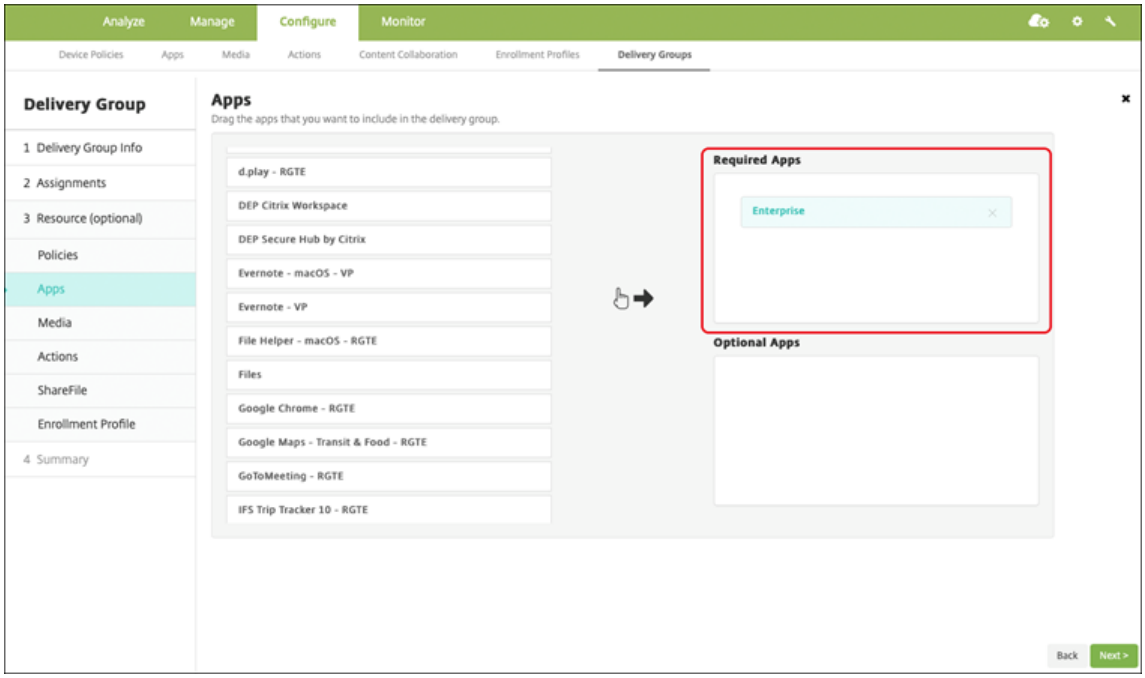
   - MAM SDK Overview(MAM SDK 개요)

- MDX 정책요약

8. 배포규칙및저장소구성을구성합니다.
9. 앱에배달그룹을할당하고 저장을클릭합니다. 자세한내용은 리소스배포를참조하십시오.

2 단계**:** 앱배포구성

1. 구성 **>** 배달그룹으로이동한다음구성한배달그룹을선택합니다. 편집을클릭합니다.
2. 앱섹션에서원하는앱을 필수앱상자로끌어옵니다.



3. 요약페이지에서 저장을클릭합니다.
4. 배달그룹페이지에서배달그룹을선택하고 배포를클릭합니다.

엔터프라이즈앱

엔터프라이즈앱은 MAM SDK 또는 MDX Toolkit 으로준비되지않은개인앱을나타냅니다. 이러한앱을직접개발하거나다른출처에서직접획득할수있습니다. 엔터프라이즈앱을추가하려면앱과연결된 APK 파일이필요합니다.Google 개인앱모범사례를따르십시오.

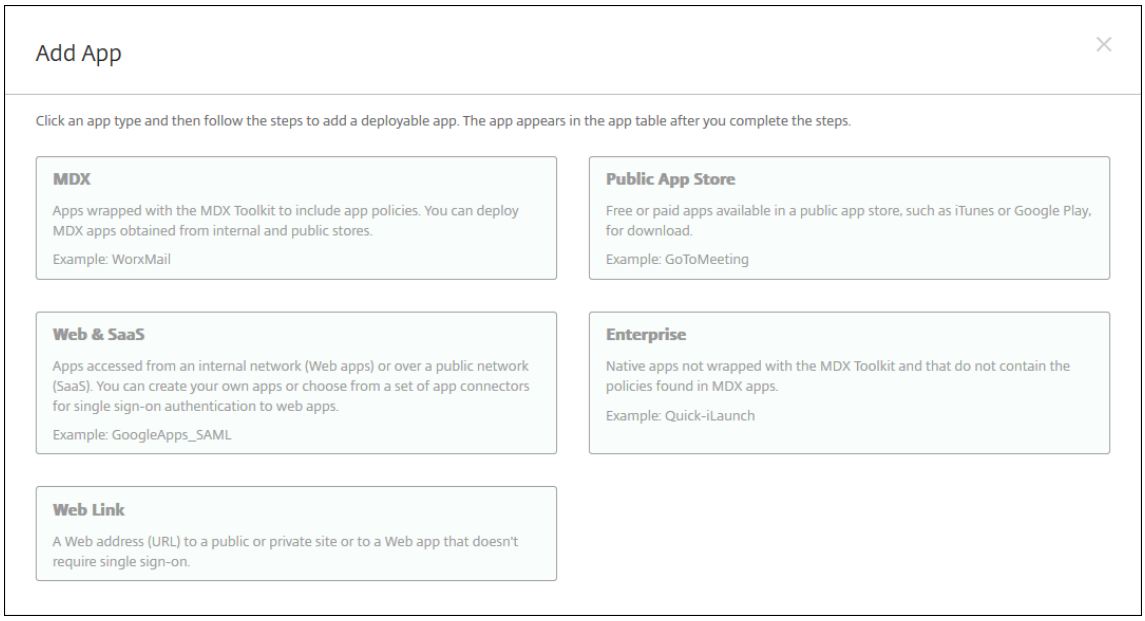
1 단계**:** 앱추가및구성

다음의두가지방식중하나로앱을추가합니다.

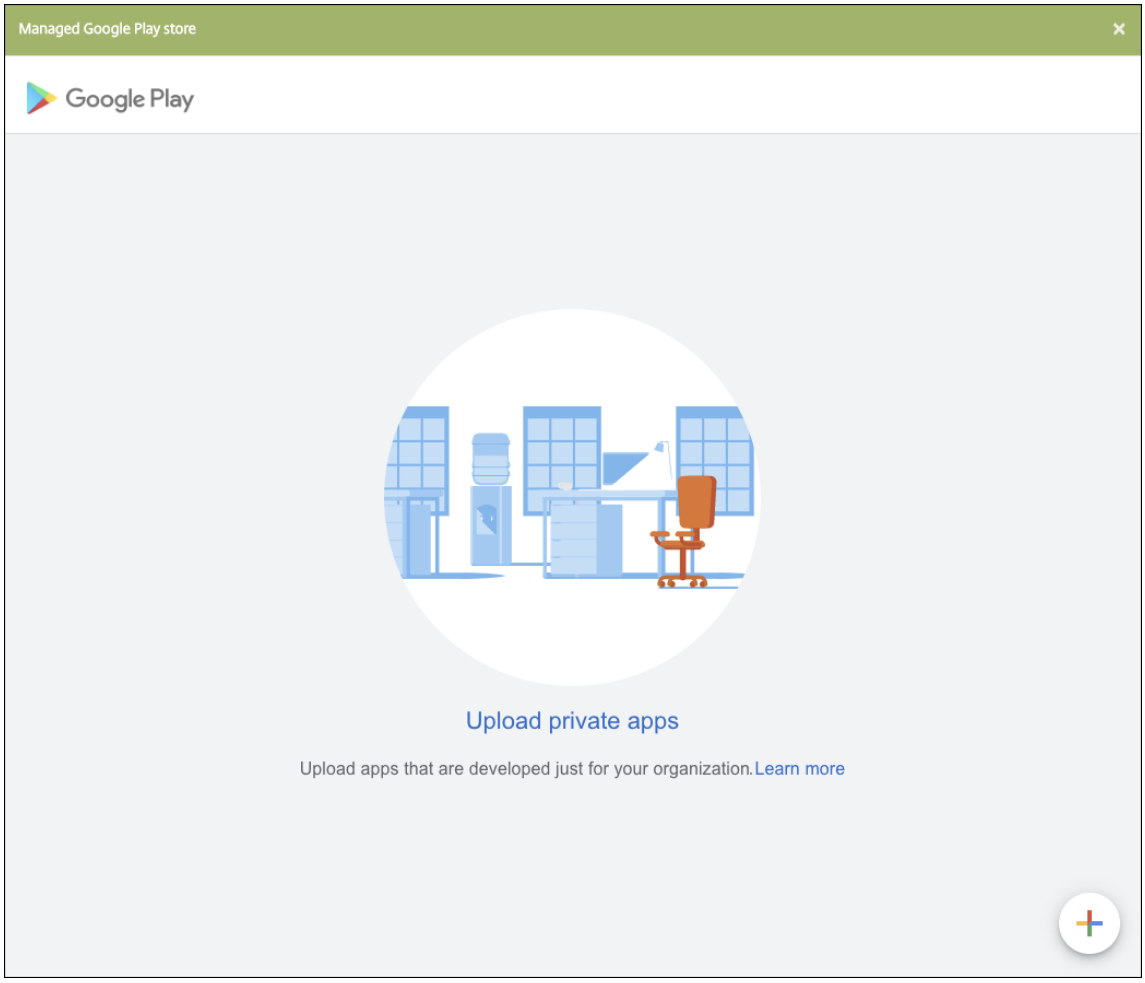
- 관리되는 Google Play 스토어에직접앱을게시하고 XenMobile 콘솔에관리되는 Play 스토어앱으로추가합니다. 개인앱게시 방법에관한 Google 문서를따르고관리되는앱스토어앱 섹션의단계를따르십시오.

- 앱을 XenMobile 콘솔에엔터프라이즈앱으로추가합니다. 다음단계를수행합니다.

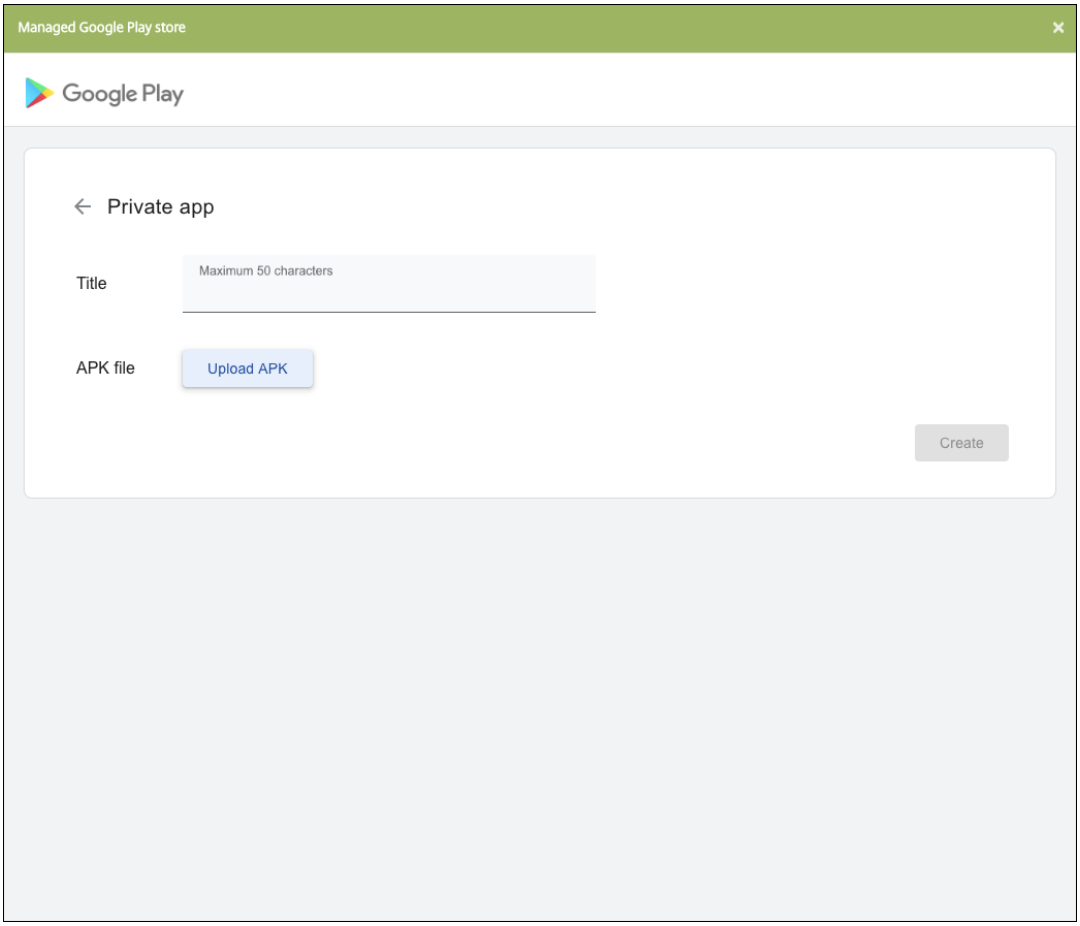
1. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 추가를클릭합니다. 앱추가대화상자가나타납니다.



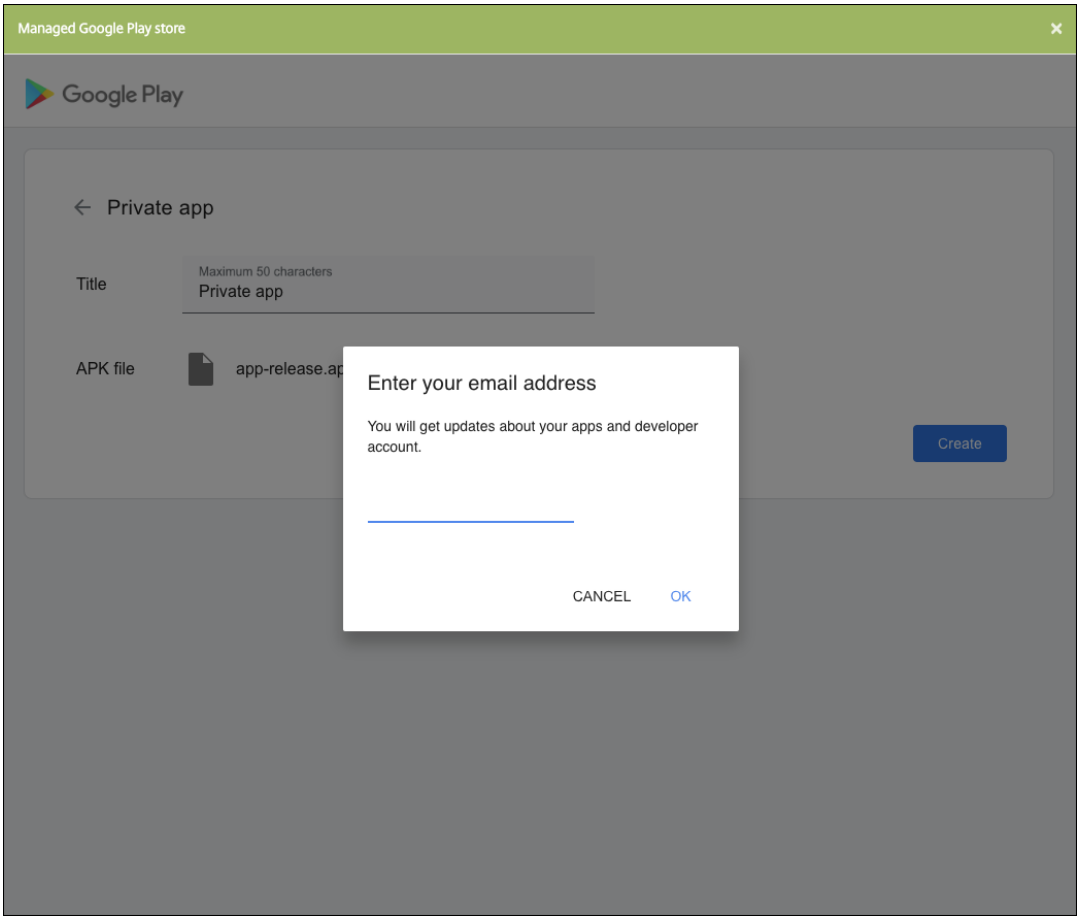
2. 엔터프라이즈를클릭합니다. 앱정보창에서다음정보를입력합니다.
   - 이름**:** 앱의설명적이름을입력합니다. 이이름은앱테이블의앱이름아래에나열됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은 앱범주정보를참조하십시오.
3. 플랫폼으로 **Android Enterprise** 를선택합니다.
4. 업로드버튼을클릭하면관리되는 Google Play Store 가열립니다. 개발자계정을등록하지않고도개인앱을게시할수있습니다. 계속하려면오른쪽아래의 **+** 아이콘을클릭합니다.



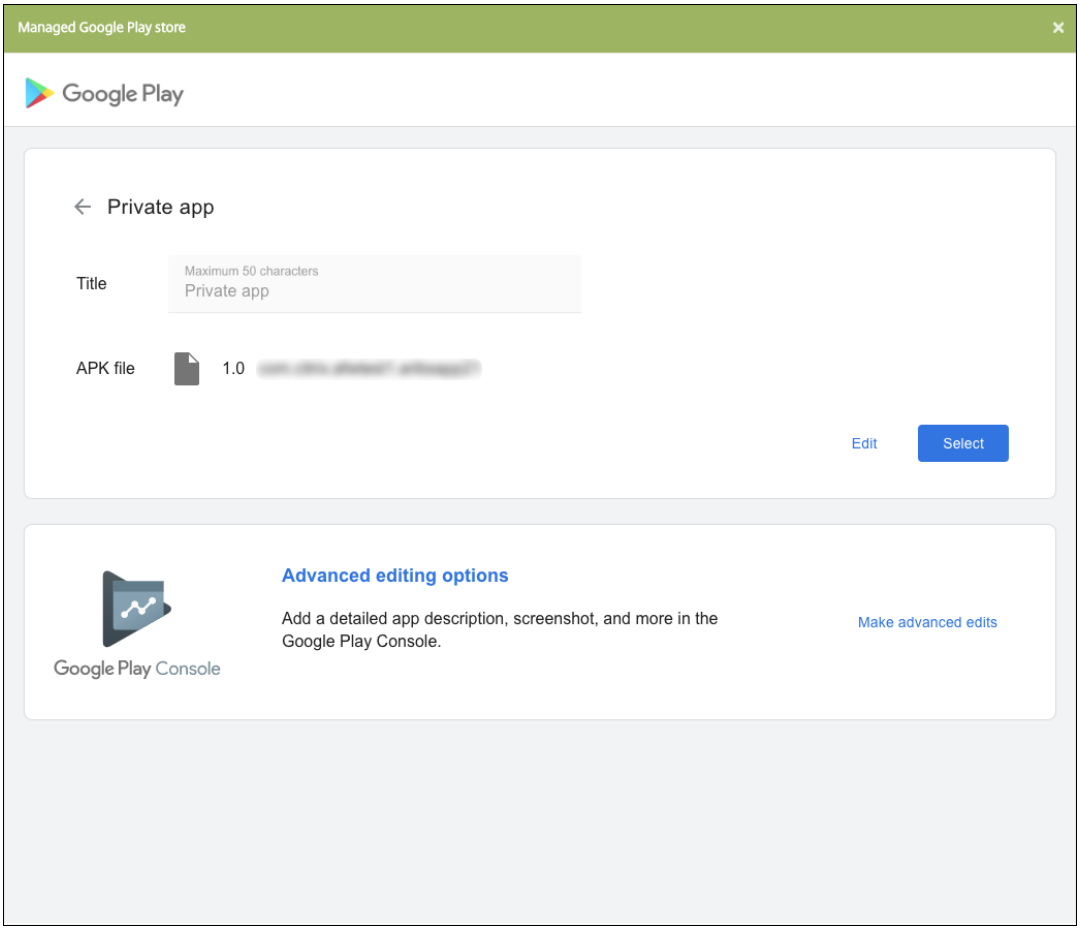
a) 앱이름을입력하고.apk 파일을업로드합니다. 작업을마치면 **Create(**만들기**)** 를클릭합니다. 개인앱을게시하는데최대 10 분이걸릴수있습니다.



b) 앱에대한업데이트를받으려면이메일주소를입력합니다.



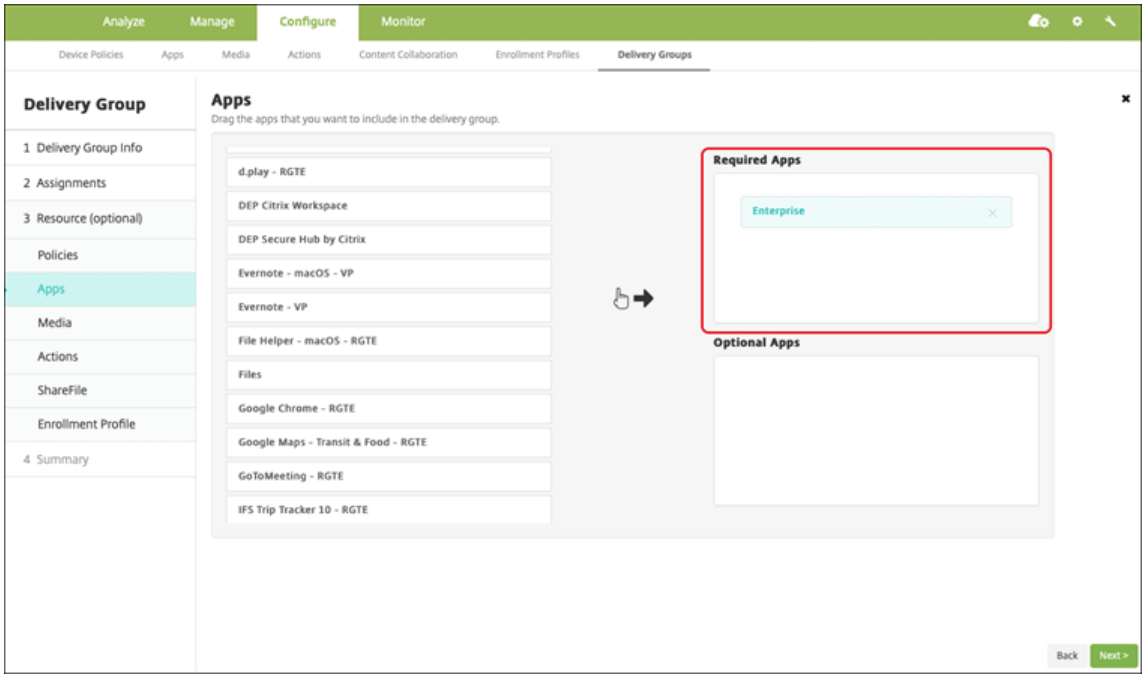
c) 애플리케이션이게시되고난후개인앱의아이콘을클릭합니다. 앱설명을추가하거나앱아이콘을변경하는등다른작업을수행하려면 고급편집을클릭합니다. 아니면 선택을클릭하여앱정보페이지를엽니다.



5. 다음을클릭합니다. 플랫폼에대한앱정보페이지가나타납니다.
6. 다음과같은플랫폼유형에대한설정을구성합니다.
   - 파일이름**:** 필요한경우앱의새이름을입력합니다.
   - 앱설명**:** 필요한경우앱에대한새설명을입력합니다.
   - 앱버전**:** 이필드는변경할수없습니다.
   - 패키지 **ID:** 앱의고유식별자입니다.
   - 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
   - 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
   - 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.
7. 배포규칙및저장소구성을구성합니다.
8. 앱에배달그룹을할당하고 저장을클릭합니다. 자세한내용은 리소스배포를참조하십시오.

2 단계**:** 앱배포구성

1. 구성 **>** 배달그룹으로이동한다음구성한배달그룹을선택합니다. 편집을클릭합니다.
2. 앱섹션에서원하는앱을 필수앱상자로끌어옵니다.



3. 요약페이지에서 저장을클릭합니다.
4. 배달그룹페이지에서배달그룹을선택하고 배포를클릭합니다.

MDX 지원개인앱

Android Enterprise 앱을 MDX 지원엔터프라이즈앱으로추가하려면다음단계를따르십시오.

1. 개인 Android Enterprise 앱과 MDX 지원앱을만듭니다.
2. XenMobile 콘솔에앱을추가합니다.
   - 관리되는 Google Play 스토어에서앱을호스팅하고게시합니다.
   - 앱을 XenMobile 콘솔에 Enterprise 앱으로추가합니다.
3. MDX 파일을 XenMobile 에추가합니다.

Google Play Store 를통해앱을호스트하고게시하기로했다면 Google 인증서서명을선택하지마십시오. 앱을 MDX 로지원하는데사용한것과동일한인증서로앱에서명합니다. 앱게시에관한자세한정보는 앱게시 및 앱서명에관한 Google 문서를참고하십시오. MAM SDK 는앱을래핑하지않으므로앱개발에사용한인증서이외의인증서가필요하지않습니다.

Google Play Console 을통한비공개앱게시에관한자세한정보는 Play Console 에서개인앱게시 방법에관한 Google 문서를참조하십시오.

XenMobile 을통해앱을게시하려면다음섹션을참조하십시오.

비공개 **Android Enterprise** 앱준비

비공개 Android Enterprise 앱을만들경우 Google 개인앱모범사례를따라야합니다.

개인 Android Enterprise 앱을만든후앱과 MAM SDK 를통합하거나 MDX Toolkit 을사용하여앱을래핑합니다. 그런다음 결과파일을 XenMobile 에추가합니다.

업데이트된.apk 파일을업로드하여앱을업데이트할수있습니다. 다음단계는 MDX Toolkit 을통한앱래핑에적용됩니다.

1. 비공개 Android Enterprise 앱을만들고서명된.apk 파일을생성합니다.
2. 다음예제파일에는알려진모든정책이포함되어있으며그중일부는사용자환경에적용되지않을수있습니다. 사용할수없는설정은무시됩니다. 다음매개변수로 XML 파일을만듭니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
            NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
        <ActivePollPeriod>60</ActivePollPeriod>
        <PublicFileAccessLimitsList/>
        <CutAndCopy>Unrestricted</CutAndCopy>
        <Paste>Unrestricted</Paste>
        <DocumentExchange>Unrestricted</DocumentExchange>
        <OpenInExclusionList/>
        <InboundDocumentExchange>Unrestricted</
            InboundDocumentExchange>
        <InboundDocumentExchangeWhitelist/>
        <connectionSecurityLevel>TLS</connectionSecurityLevel>
        <DisableCamera>false</DisableCamera>
        <DisableGallery>false</DisableGallery>
        <DisableMicrophone>false</DisableMicrophone>
```



```
34          <DisableLocation>false</DisableLocation>
35          <DisableSms>false</DisableSms>
36          <DisableScreenCapture>false</DisableScreenCapture>
37          <DisableSensor>false</DisableSensor>
38          <DisableNFC>false</DisableNFC>
39          <BlockLogs>false</BlockLogs>
40          <DisablePrinting>false</DisablePrinting>
41          <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
               MvpnNetworkAccess>
42          <MvpnSessionRequired>False</MvpnSessionRequired>
43          <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44          <DisableLocalhostConnections>false</
               DisableLocalhostConnections>
45          <CertificateLabel/>
46          <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47          <DefaultLoggerLevel>15</DefaultLoggerLevel>
48          <MaxLogFiles>2</MaxLogFiles>
49          <MaxLogFileSize>2</MaxLogFileSize>
50          <RedirectSystemLogs>false</RedirectSystemLogs>
51          <EncryptLogs>false</EncryptLogs>
52          <GeofenceLongitude>0</GeofenceLongitude>
53          <GeofenceLatitude>0</GeofenceLatitude>
54          <GeofenceRadius>0</GeofenceRadius>
55          <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56          <Authentication>OfflineAccessOnly</Authentication>
57          <ReauthenticationPeriod>480</ReauthenticationPeriod>
58          <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59      </Policies>
60  </MobileAppPolicies>
61  <!--NeedCopy-->
```

3. MDX Toolkit 을사용하여앱을래핑합니다. MDX Toolkit 사용에대한자세한내용은 Android 모바일앱래핑을참조하십시오.

   apptype 매개변수를 프리미엄으로설정합니다. 다음에설명된명령에서이전단계의 XML 파일을사용합니다.

   앱의스토어 URL 을알고있다면 **storeURL** 매개변수를스토어 URL 로설정합니다. 앱이게시된후사용자는스토어 URL 에서앱을다운로드합니다.

   다음은 SampleAEapp 이라는앱을래핑하는데사용되는 MDX Toolkit 명령의예입니다.

```
1  ```
2   java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
       Duser.variant
3   -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
```



```
4   -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
5   -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
6   -MinPlatform 5.0
7   -keystore /MyKeystore
8   -storepass mystorepwd123
9   -keyalias key0
10  -keypass mykeypwd123
11  -storeURL ”https://play.google.com/store/apps/details?id=
        SampleAEappPackage”
12  -appType Premium
13  -premiumMdxPolicies <Path to Premium policy XML>
14 <!--NeedCopy--> ```
```

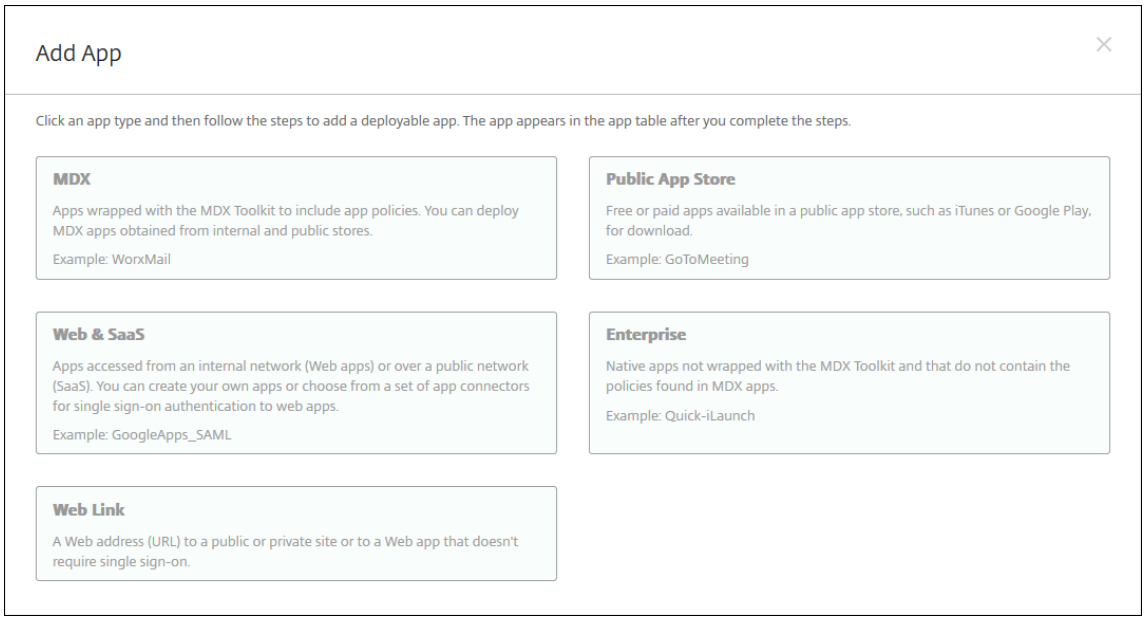
앱을래핑하면래핑된.apk 파일과.mdx 파일이생성됩니다.

래핑된**.apk** 파일추가

다음의두가지방식중하나로앱을추가합니다.

- 관리되는 Google Play 스토어에직접앱을게시하고 XenMobile 콘솔에관리되는 Play 스토어앱으로추가합니다. 개인 앱게시 방법에관한 Google 문서를따르고관리되는앱스토어앱 섹션의단계를따르십시오.
- 앱을 XenMobile 콘솔에엔터프라이즈앱으로추가합니다. 다음단계를수행합니다.

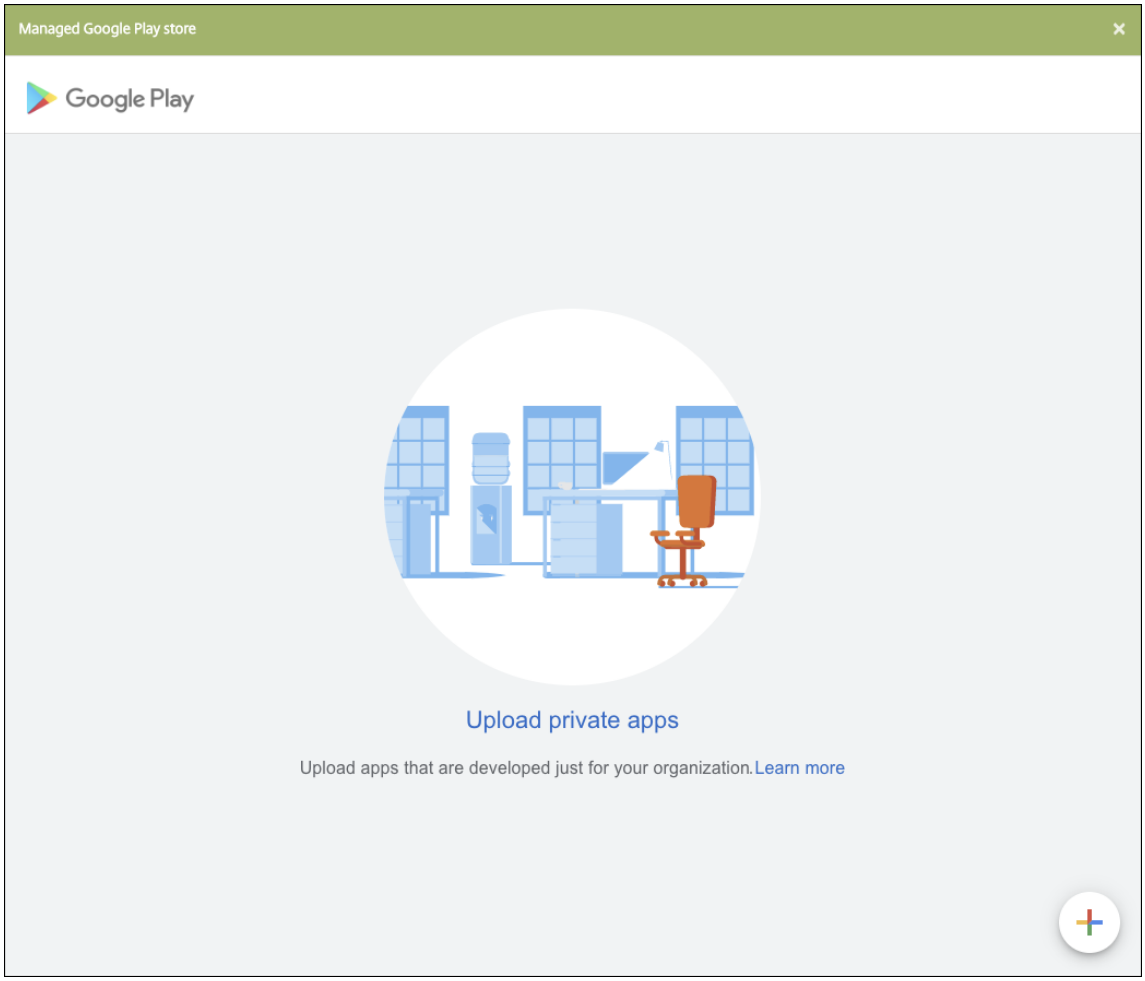
1. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 앱페이지가열립니다.
2. 추가를클릭합니다. 앱추가대화상자가나타납니다.



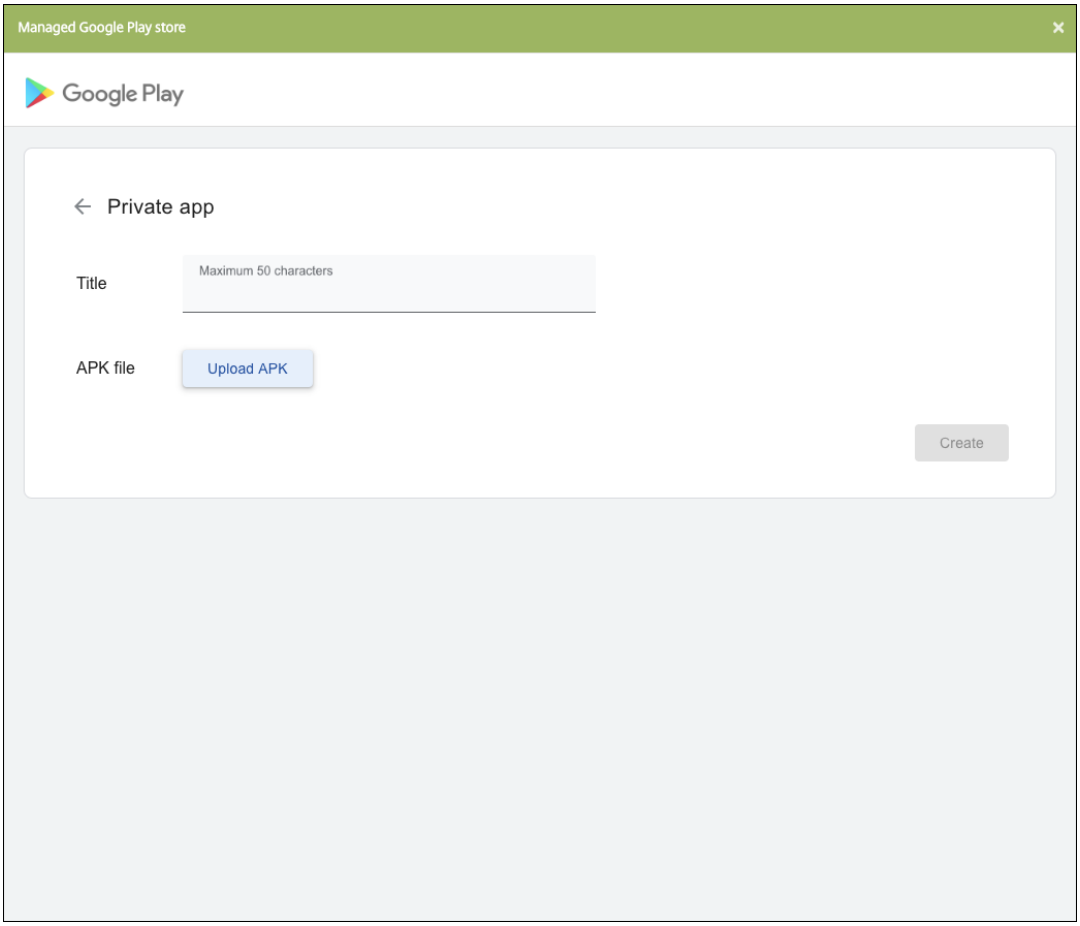
3. 엔터프라이즈를클릭합니다. 앱정보창에서다음정보를입력합니다.
    - 이름**:** 앱의설명적이름을입력합니다. 이이름은앱테이블의앱이름아래에나열됩니다.

- 설명**:** 앱의선택적설명을입력합니다.
- 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은 앱범주정보를참조하십시오.

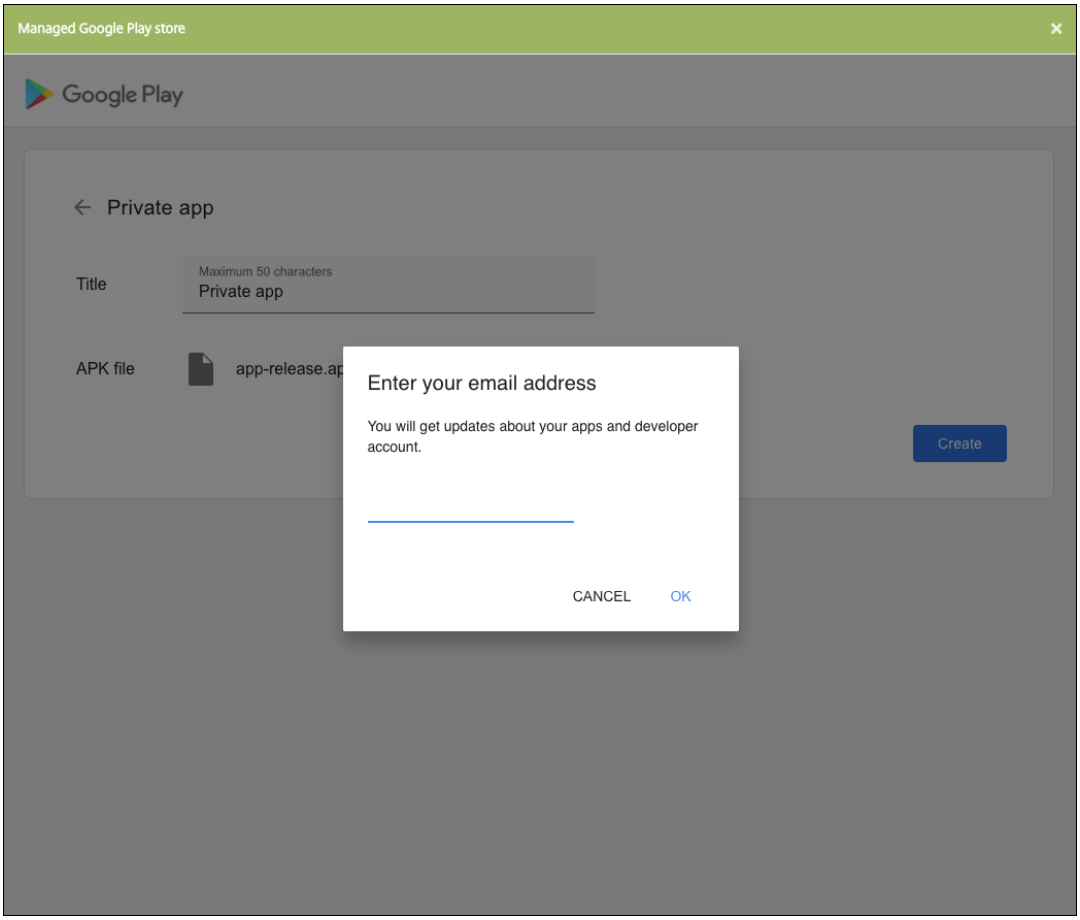
4. 플랫폼으로 **Android Enterprise** 를선택합니다.
5. 업로드버튼을클릭하면관리되는 Google Play Store 가열립니다. 개발자계정을등록하지않고도개인앱을게시할수있습니다. 계속하려면오른쪽아래의 **+** 아이콘을클릭합니다.



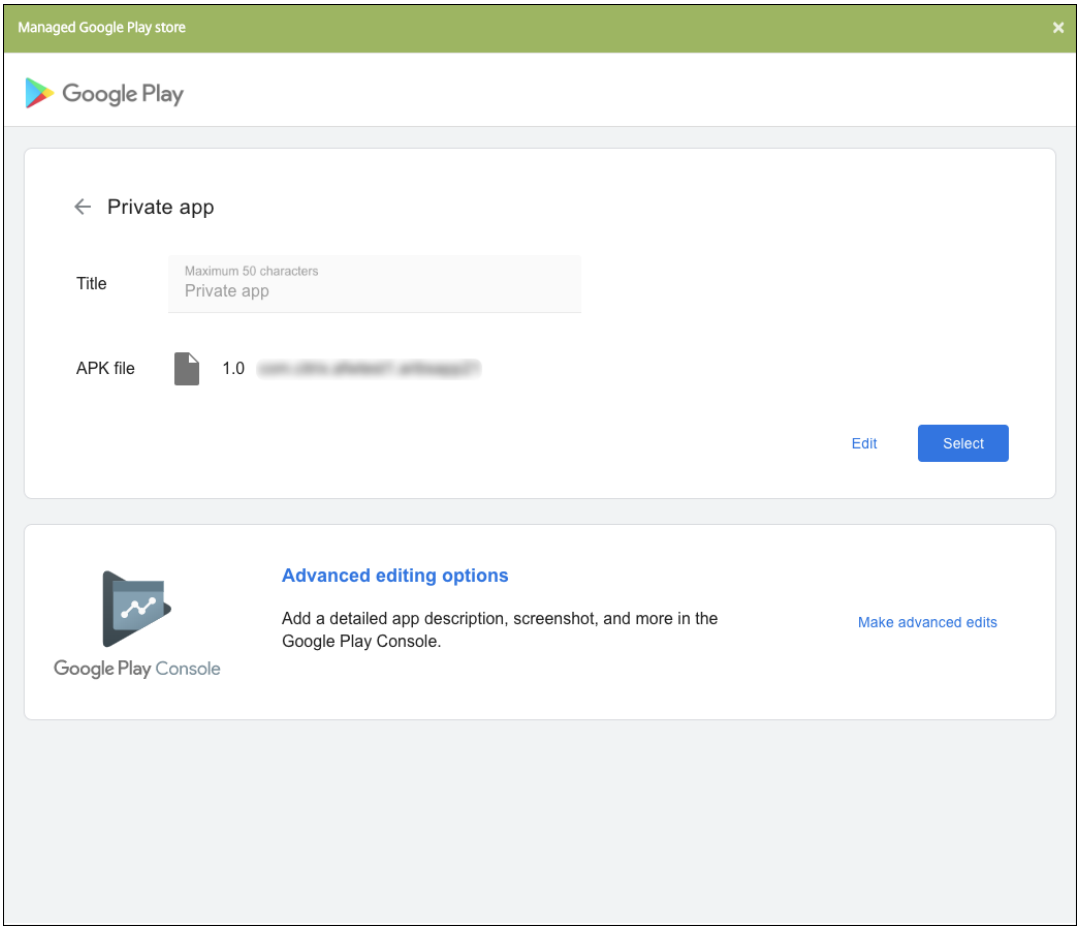
a) 앱이름을입력하고.apk 파일을업로드합니다. 작업을마치면 **Create(**만들기**)** 를클릭합니다. 개인앱을게시하는데최대 10 분이걸릴수있습니다.



b) 앱에대한업데이트를받으려면이메일주소를입력합니다.



c) 응용프로그램이게시된후개인앱의아이콘을클릭하고 선택을클릭하여앱정보페이지를엽니다.



6. 다음을클릭합니다. 플랫폼에대한앱정보페이지가나타납니다.
7. 다음과같은플랫폼유형에대한설정을구성합니다.
   - 파일이름**:** 필요한경우앱의새이름을입력합니다.
   - 앱설명**:** 필요한경우앱에대한새설명을입력합니다.
   - 앱버전**:** 이필드는변경할수없습니다.
   - 패키지 **ID:** 앱의고유식별자입니다.
   - 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
   - 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
   - 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.
8. 배포규칙및저장소구성을구성합니다.
9. **Android Enterprise** 엔터프라이즈앱페이지에서 다음을엽니다. 승인페이지가나타납니다.

   워크플로를사용하여사용자의앱액세스를허용하기전에승인을요구하려면 워크플로적용을참조하십시오. 승인워크플로가필요하지않은경우 13 단계로건너뛰어도됩니다.
10. 다음을클릭합니다.
11. 배달그룹할당페이지가나타납니다. 이페이지에서는아무조치도필요하지않습니다. .mdx 파일을추가할경우이앱의배달그

룹과배포일정을구성합니다. 저장을클릭합니다.

선택사항**:** 스토어 **URL** 을추가하거나변경합니다

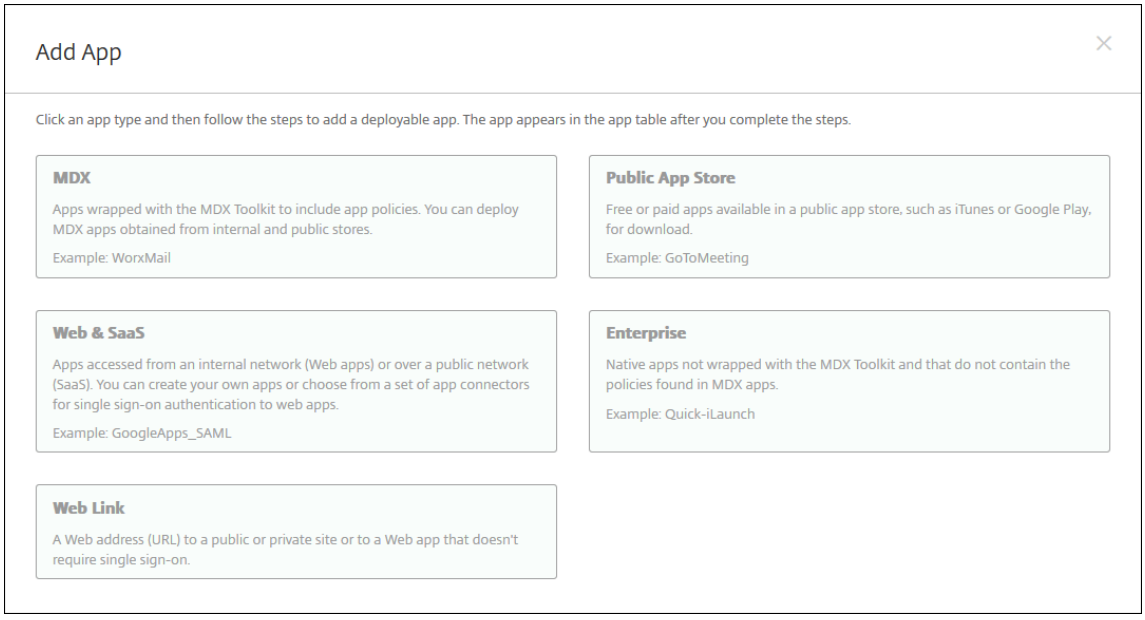
앱을래핑했을때스토어 URL 을몰랐다면지금스토어 URL 을추가합니다.

1. 관리되는 Google Play Store 에서앱을확인합니다. 앱을선택하면스토어 URL 이브라우저의주소표시줄에표시됩니다. URL 형식에서앱의패키지이름을복사합니다. 예: `https://play.google.com/store/apps/details?id=SampleAEappPackage`. 복사한 URL 이 `https://play.google.com/work/`으로시작할수있습니다. `work`를 `store`로변경했는지확인합니다.
2. MDX Toolkit 을사용하여스토어 URL 을.mdx 파일에추가합니다.

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL ”https://play.google.com/store/apps/details?id=
   SampleAEappPackage”
<!--NeedCopy-->
```

.mdx 파일추가

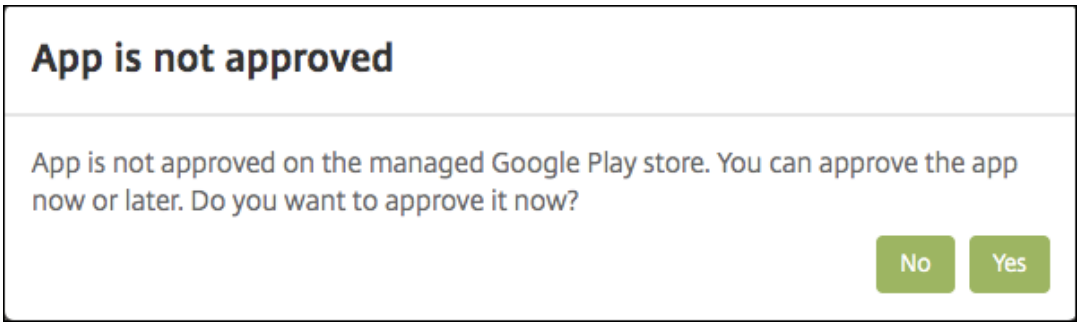
1. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 추가를클릭합니다. 앱추가대화상자가나타납니다.



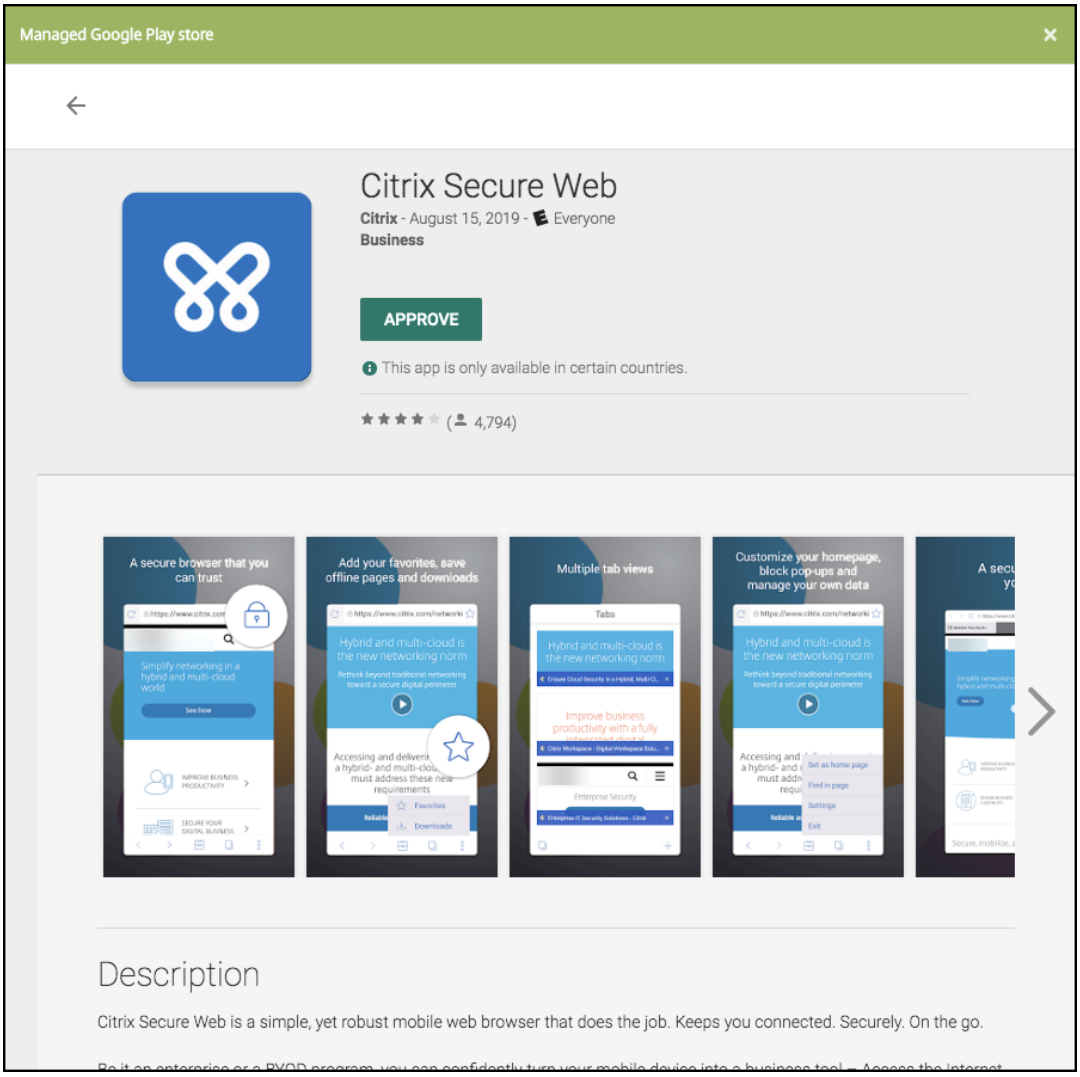
2. **MDX** 를클릭합니다. **MDX** 앱정보페이지가나타납니다. 앱정보창에서다음정보를입력합니다.

- 이름**:** 앱을설명하는이름을입력합니다. 이이름은 앱테이블의 앱이름아래에표시됩니다.
- 설명**:** 앱의선택적설명을입력합니다.
- 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은 앱범주정보를참조하십시오.

3. 플랫폼으로 **Android Enterprise** 를선택합니다.
4. 업로드를클릭하고 MDX 파일로이동합니다. Android Enterprise 는 MDX Toolkit 으로래핑된앱만지원합니다.
   - 연결된응용프로그램에관리되는 Google Play Store 의승인이필요한경우 UI 에알림이표시됩니다. XenMobile 콘솔을종료하지않고응용프로그램을승인하려면 예를클릭합니다.



   관리되는 Google Play Store 가열리면지침에따라앱을승인하고저장합니다.



앱이성공적으로추가되면 앱세부정보페이지가나타납니다.

5. 다음설정을구성합니다.

   - 파일이름**:** 앱에연결된파일이름을입력합니다.
   - 앱설명**:** 앱에대한설명을입력합니다.
   - 앱버전**:** 필요한경우앱버전번호를입력합니다.
   - 패키지 **ID:** 관리되는 Google Play 스토어에서가져온앱의패키지 ID 를입력합니다.
   - 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
   - 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
   - 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.

6. **MDX** 정책을구성합니다. MDX 정책은플랫폼별로다르며인증, 장치보안및앱제한등정책영역에대한옵션이포함됩니다. 콘솔에서각정책에는정책을설명하는도구설명이포함됩니다. 각장치플랫폼유형에사용할수있는앱정책에대한자세한내용은다음을참조하십시오.

   - MAM SDK Overview(MAM SDK 개요)

- MDX 타사앱정책요약

7. 배포규칙및저장소구성을구성합니다.

   설정 **>** 서버속성에서백그라운드배포예약키를구성한경우 상시연결에대해배포가적용됩니다.

   상시연결옵션:

   - 버전 10.18.19 이상으로 Endpoint Management 를사용하기시작한 Android Enterprise 고객은사용할 수없습니다.
   - 버전 10.18.19 이전으로 Endpoint Management 를사용하기시작한 Android Enterprise 고객에게는권장되지않습니다.

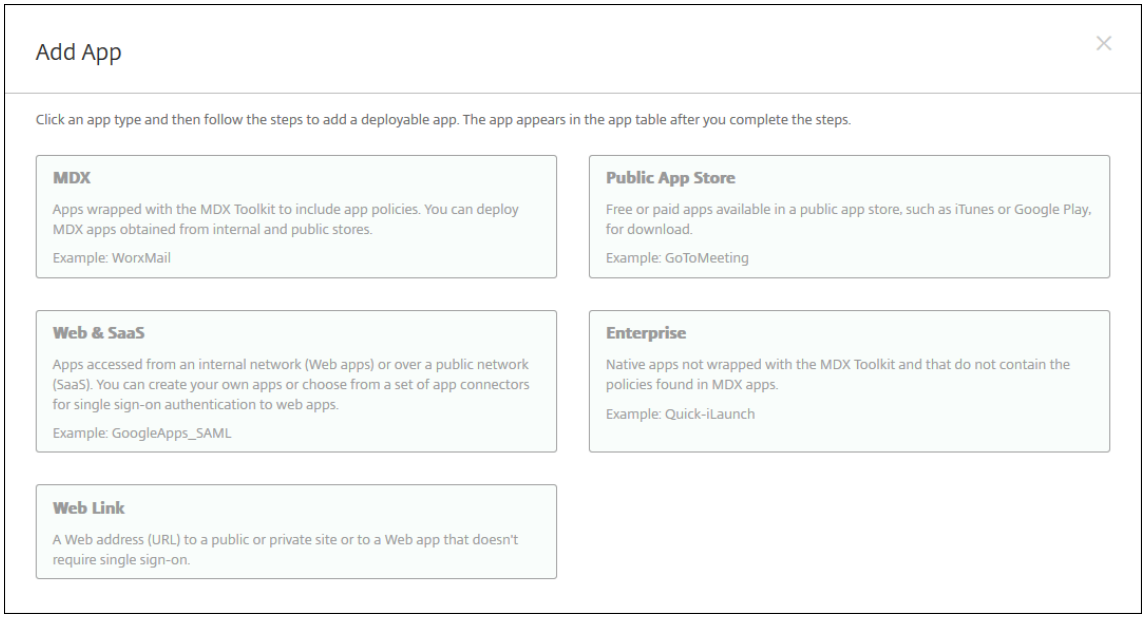
   구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은 상시연결에대해배포를제외하고모든플랫폼에적용됩니다.

8. 앱에배달그룹을할당하고 저장을클릭합니다. 자세한내용은 리소스배포를참조하십시오.

앱업데이트

Android Enterprise 앱을업데이트하려면업데이트된.apk 파일을래핑하고업로드합니다.

1. MAM SDK 또는 MDX Toolkit 을사용하여업데이트된앱의.apk 파일을래핑합니다.
2. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 앱페이지가열립니다.

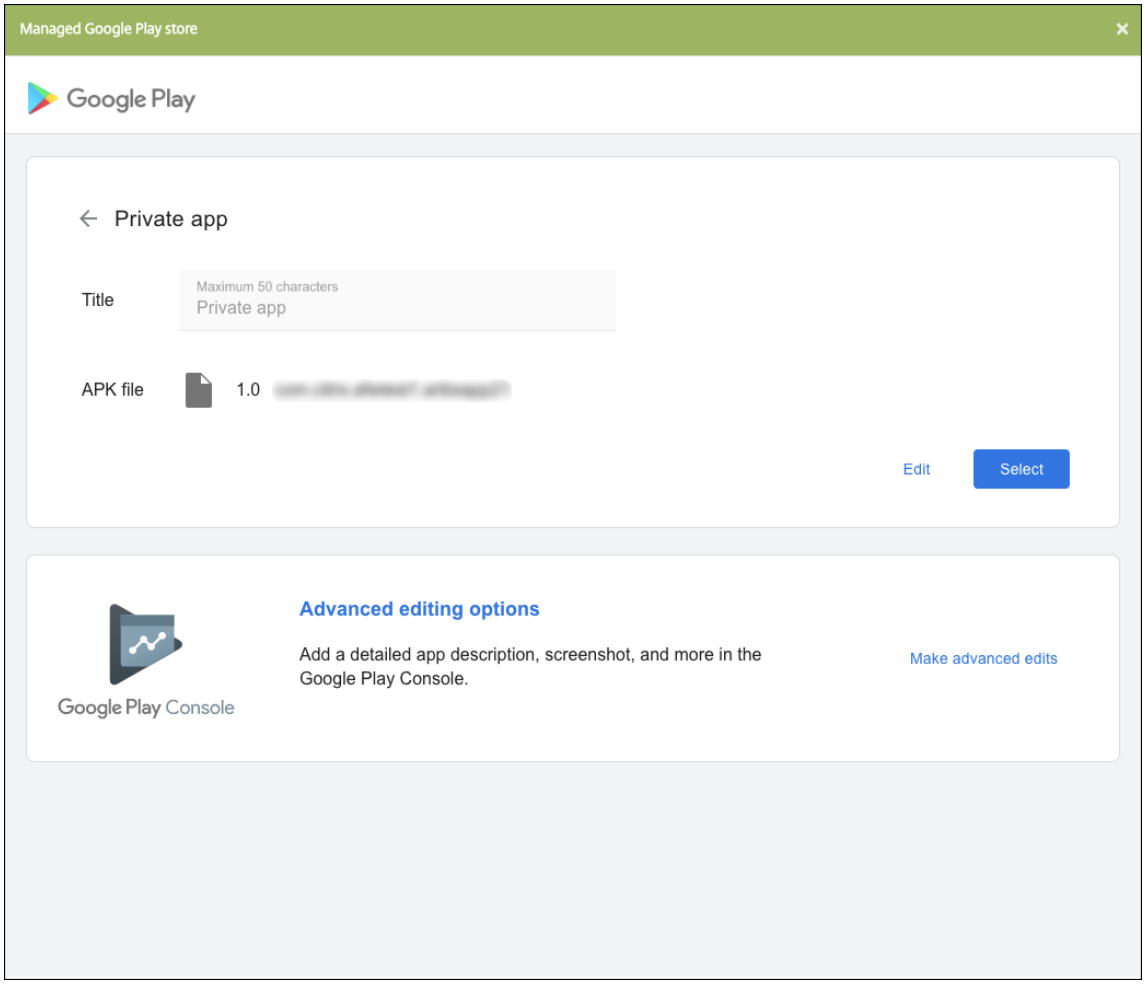


3. 추가를클릭합니다. 앱추가대화상자가나타납니다.
4. 엔터프라이즈를클릭합니다. 앱정보창에서다음정보를입력합니다.

   - 이름**:** 앱의설명적이름을입력합니다. 이이름은앱테이블의앱이름아래에나열됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.

- 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은 앱범주정보를참조하십시오.

5. 플랫폼으로 **Android Enterprise** 를선택합니다.
6. 다음을클릭합니다. **Android Enterprise** 엔터프라이즈앱페이지가나타납니다.
7. 업로드를클릭합니다.
8. 관리되는 Google Play 스토어페이지에서업데이트할앱을선택합니다.
9. 앱정보페이지에서.apk 파일이름옆에있는 편집을클릭합니다.



10. 새.apk 파일로이동한다음업로드합니다.
11. 관리되는 Google Play 스토어페이지에서 저장을클릭합니다.

Google Workspace 고객을위한레거시 Android Enterprise(이전명칭 G Suite)

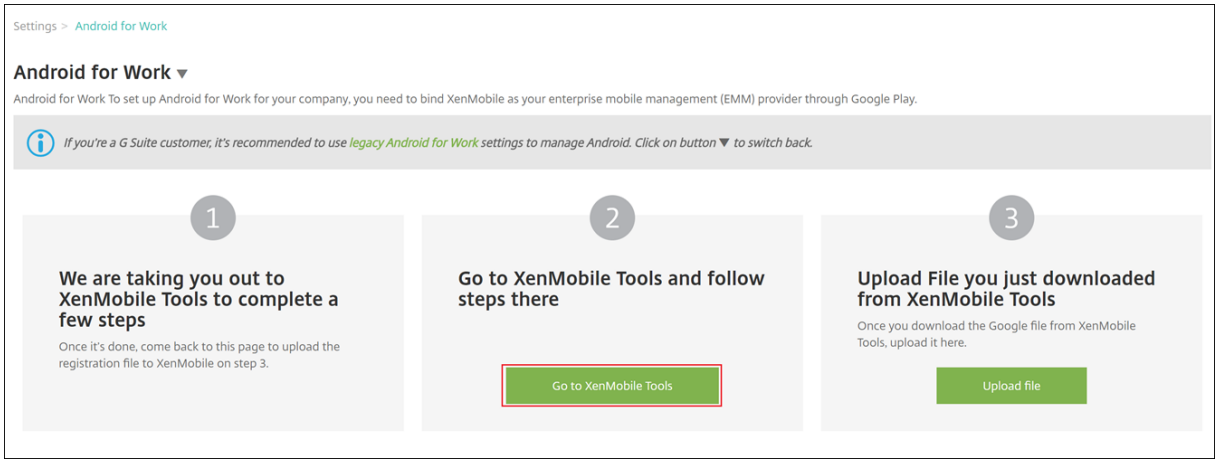
February 2, 2022

Google Workspace(이전명칭 G Suite) 고객은레거시 Android Enterprise 설정을사용하여레거시 Android Enterprise 를구성해야합니다.

레거시 Android Enterprise 요구사항:

- 공개적으로액세스할수있는도메인
- Google 관리자계정
- 관리되는프로필을지원하고 Android 5.0 Lollipop 이상을실행중인장치
- Google Play 가설치된 Google 계정
- 장치에설정된작업프로필

레거시 Android Enterprise 를구성하려면 XenMobile 설정의 **Android Enterprise** 페이지에서 레거시 **Android Enterprise** 를클릭합니다.



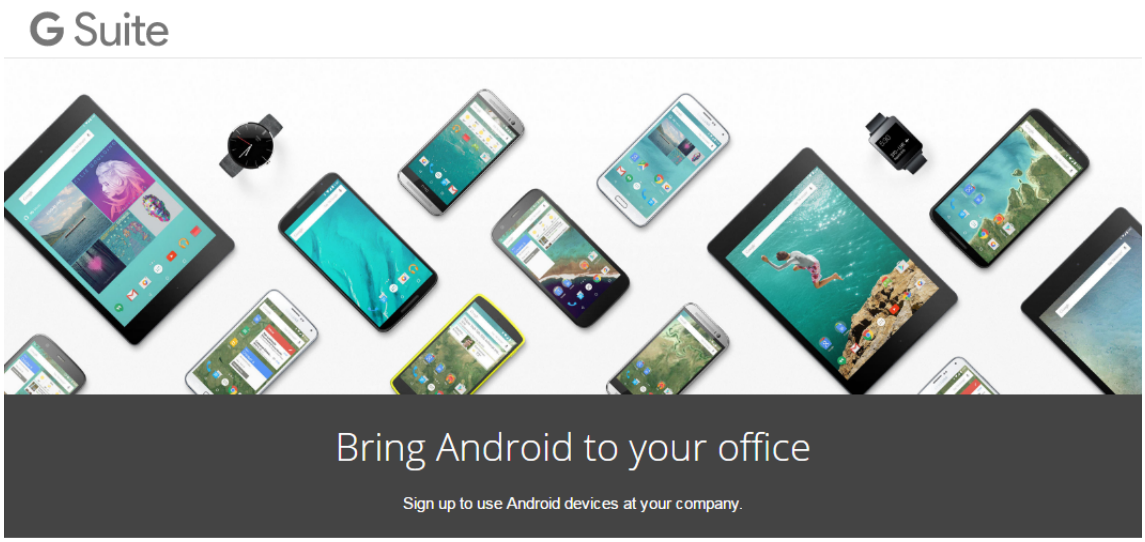
Android Enterprise 계정만들기

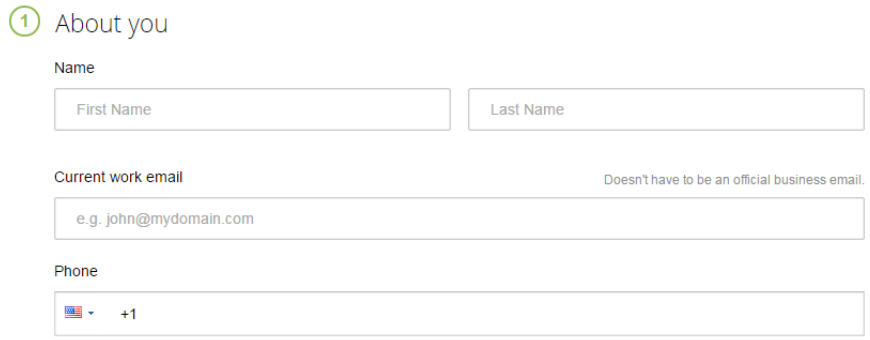
Android Enterprise 계정을설정하려면먼저 Google 에서도메인이름을확인해야합니다.

Google 에서이미도메인이름을확인한경우Android Enterprise 서비스계정설정및 Android Enterprise 인증서다운로드단계로건너뛸수있습니다.

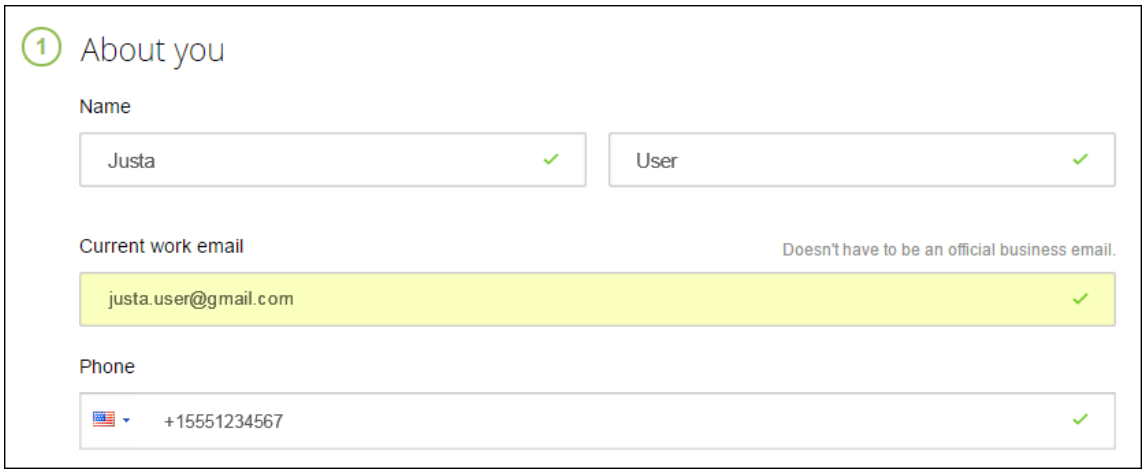
1. https://gsuite.google.com/signup/basic/welcome로이동합니다.

   관리자및회사정보를입력하는다음과같은페이지가표시됩니다.

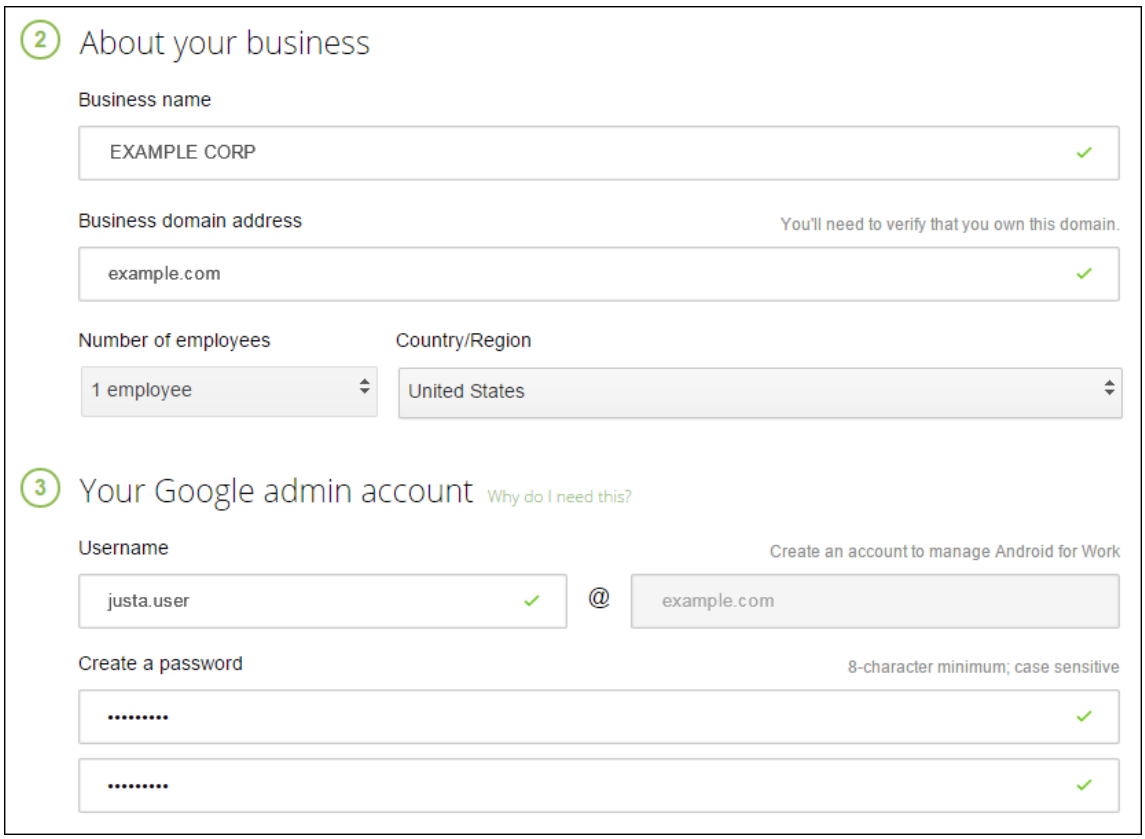




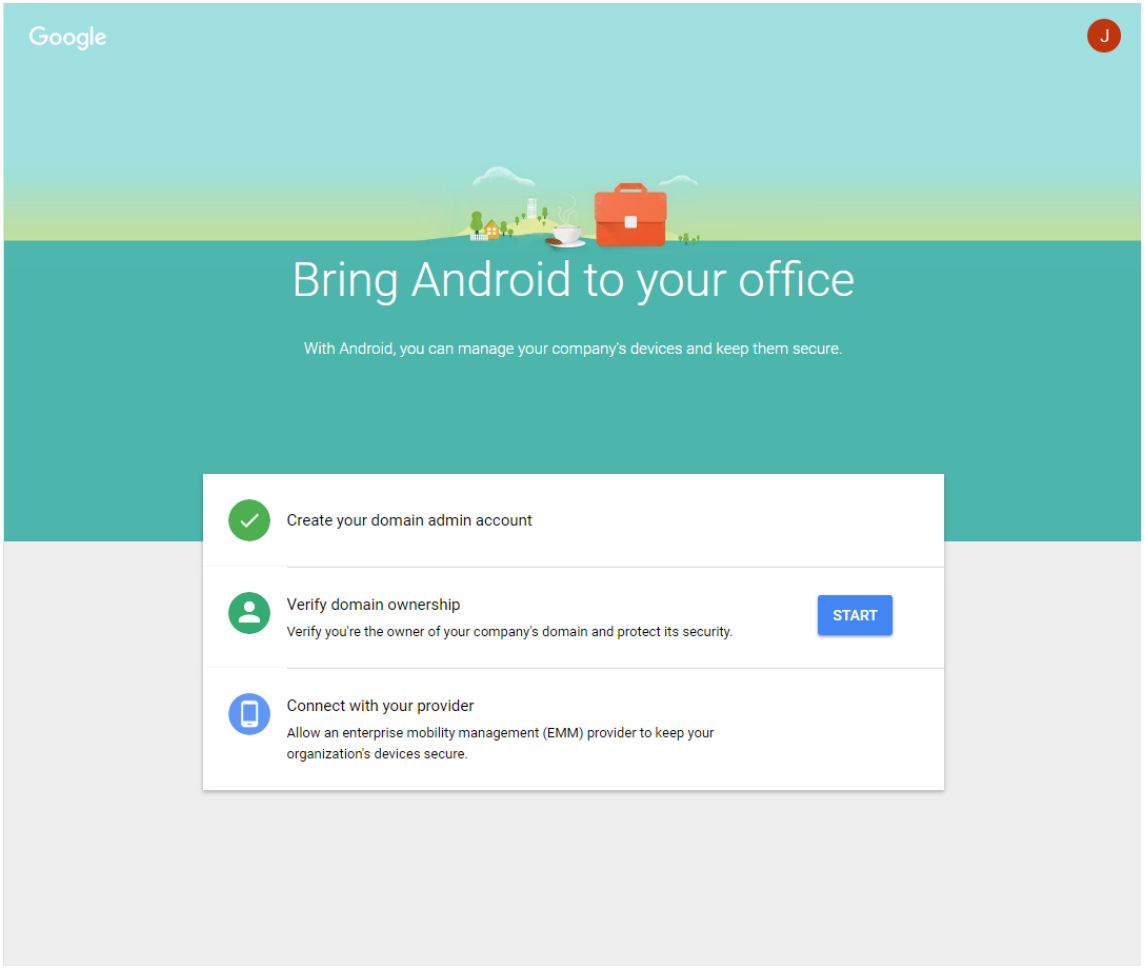
2. 관리자사용자정보를입력합니다.



3. 관리자계정정보와더불어회사정보를입력합니다.



프로세스의첫번째단계가완료되면다음페이지가표시됩니다.



도메인소유권확인

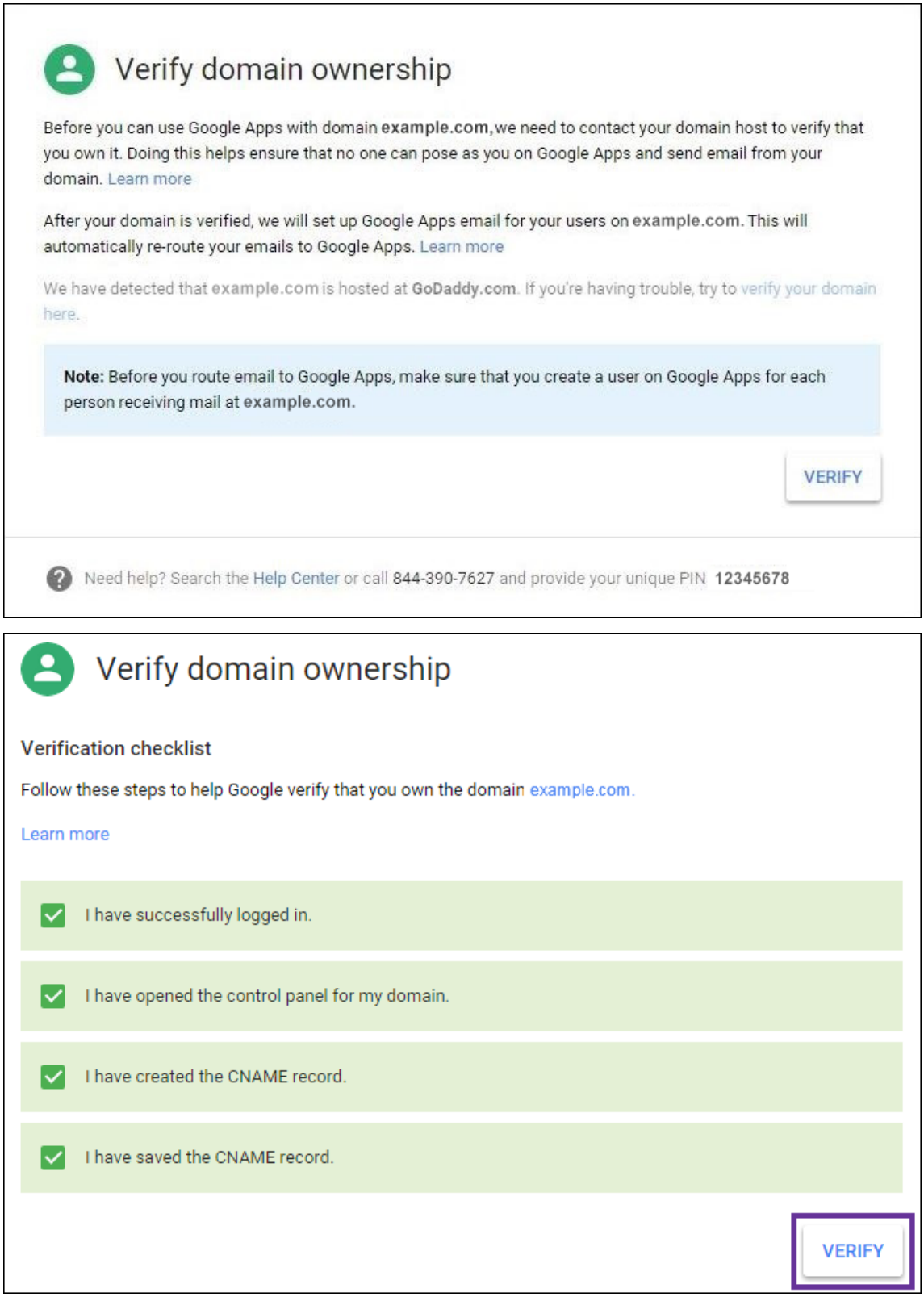
다음방법중하나를사용하여 Google 이도메인을확인할수있게만듭니다.

- TXT 또는 CNAME 레코드를도메인호스트의웹사이트에추가합니다.
- 도메인의웹서버에 HTML 파일을업로드합니다.
- 홈페이지에 <meta> 태그를추가합니다. 첫번째방법을사용하는것이좋습니다. 이문서에서는도메인소유권을확인하는단계를다루지않습니다. 필요한정보는 https://support.google.com/a/answer/6248925에서찾을수있습니다.

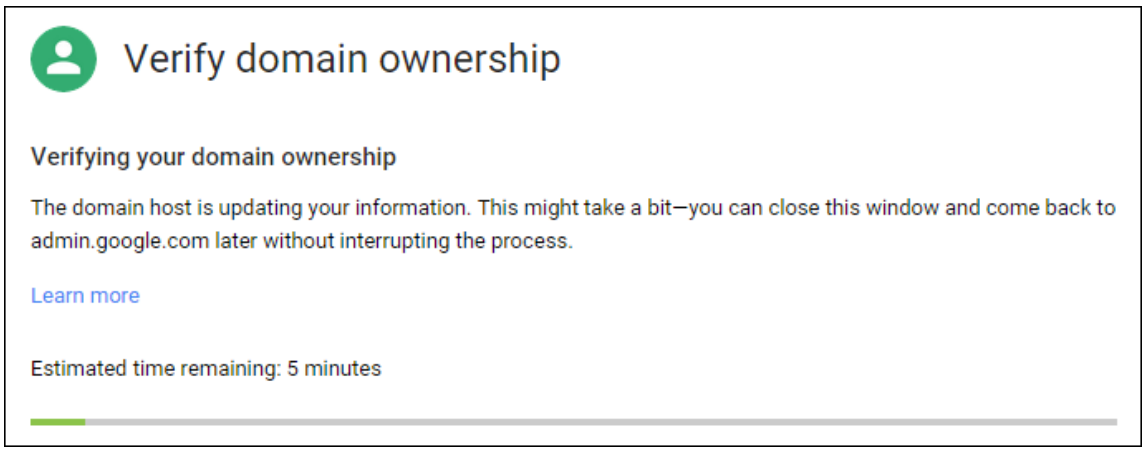
1. **Start(**시작**)** 를클릭하여도메인확인을시작합니다.

   Verify domain ownership(도메인소유권확인**)** 페이지가나타납니다. 페이지의지침에따라도메인을확인합니다.

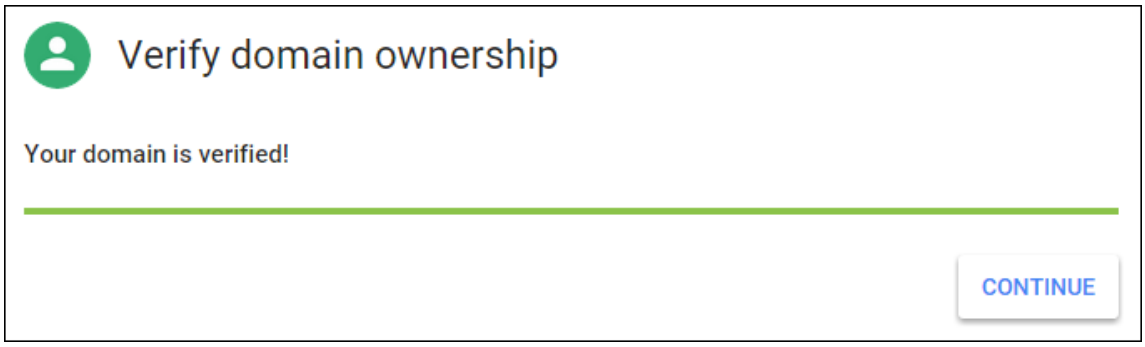
2. **Verify(**확인**)** 를클릭합니다.



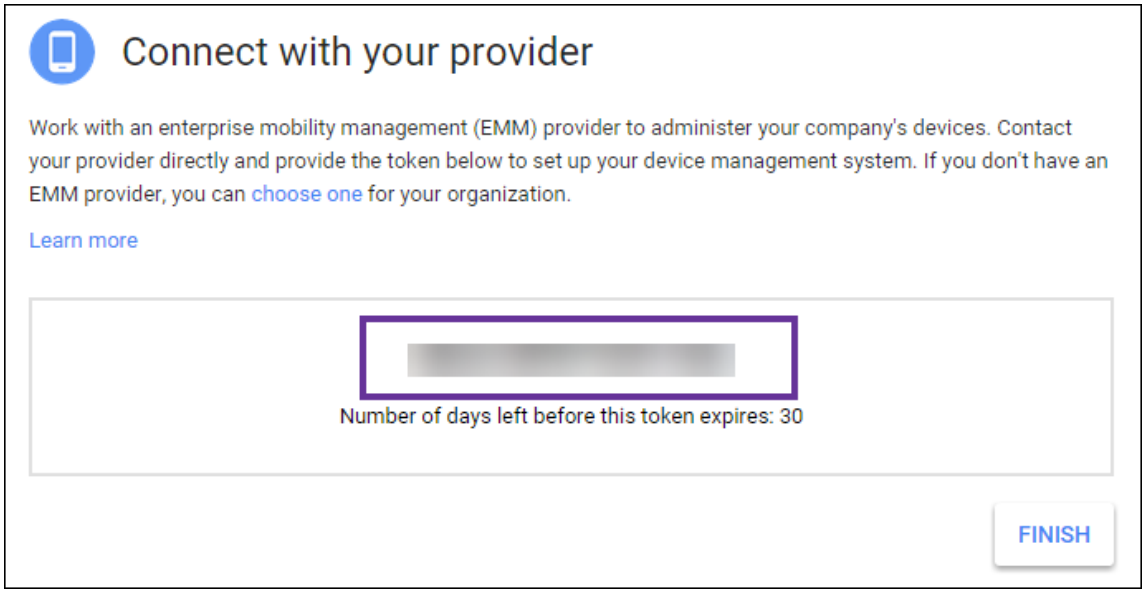
3. Google 이도메인소유권을확인합니다.



4. 확인이성공하면다음페이지가나타납니다. **Continue(**계속**)** 을클릭합니다.



5. Citrix 에제공하고 Android Enterprise 설정을구성할때사용하는 EMM 바인딩토큰이만들어집니다. 토큰을복사하여저장합니다. 나중에서설정절차에서이토큰이필요합니다.



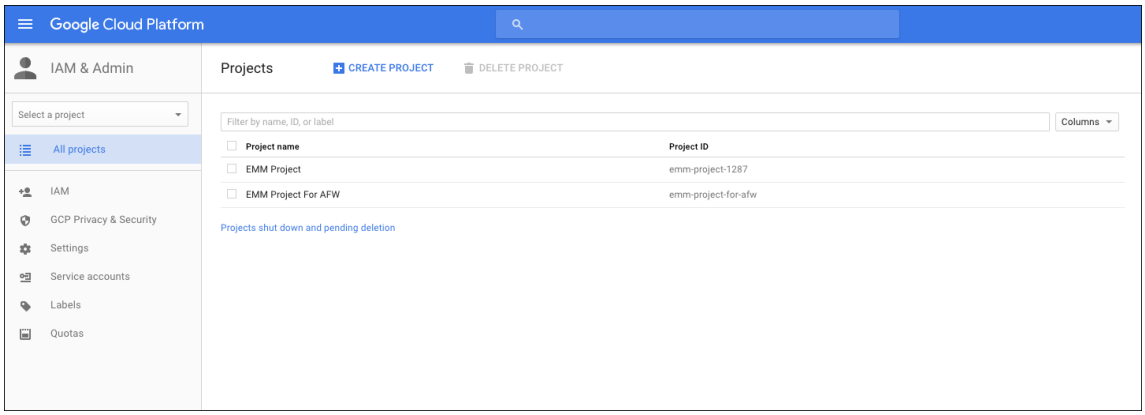
6. **Finish(**마침**)** 를클릭하여 Android Enterprise 설정을완료합니다. 도메인을확인했음을나타내는페이지가나타납니다.

Android Enterprise 서비스계정을만든후 Google 관리콘솔에로그인하여모바일관리설정을관리할수있습니다.

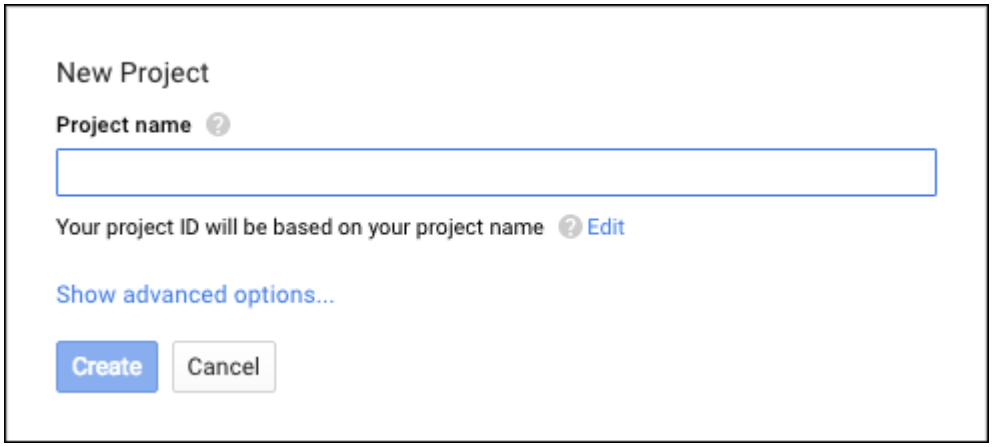
Android Enterprise 서비스계정설정및 **Android Enterprise** 인증서다운로드

XenMobile 이 Google Play 및디렉터리서비스에액세스할수있게하려면개발자를위한 Google 프로젝트포털을사용하여서비스계정을만들어야합니다. 이서비스계정은 XenMobile 과 Android 용 Google 서비스사이의서버간통신에사용됩니다. 사용되는인증프로토콜에대한자세한내용은 https://developers.google.com/identity/protocols/OAuth2ServiceAccount를참조하십시오.

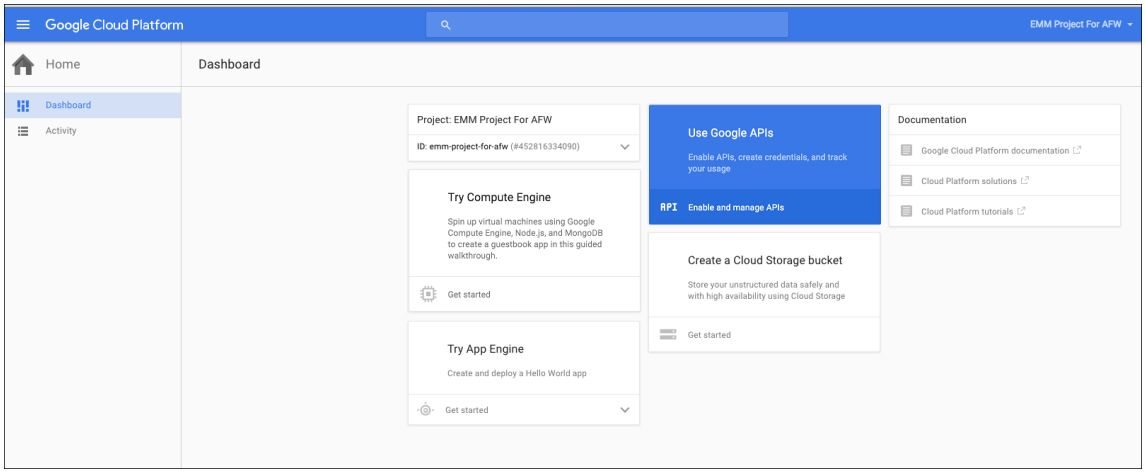
1. 웹브라우저에서 https://console.cloud.google.com/project로이동하여 Google 관리자자격증명으로로그인합니다.
2. **Projects(**프로젝트**)** 목록에서 **Create Project(**프로젝트만들기**)** 를클릭합니다.



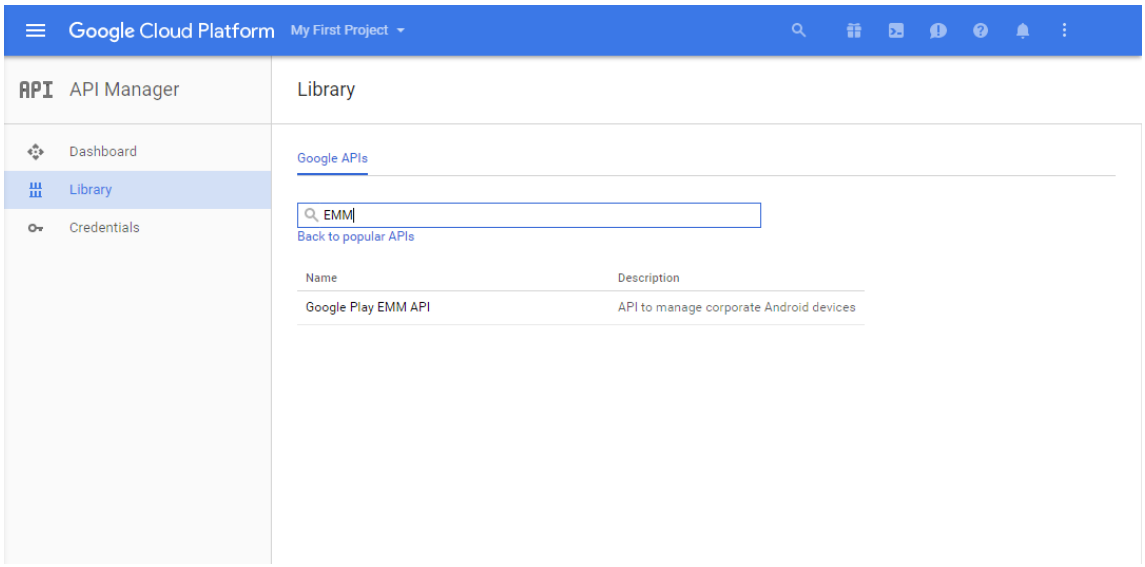
3. **Project name(**프로젝트이름**)** 에프로젝트이름을입력합니다.



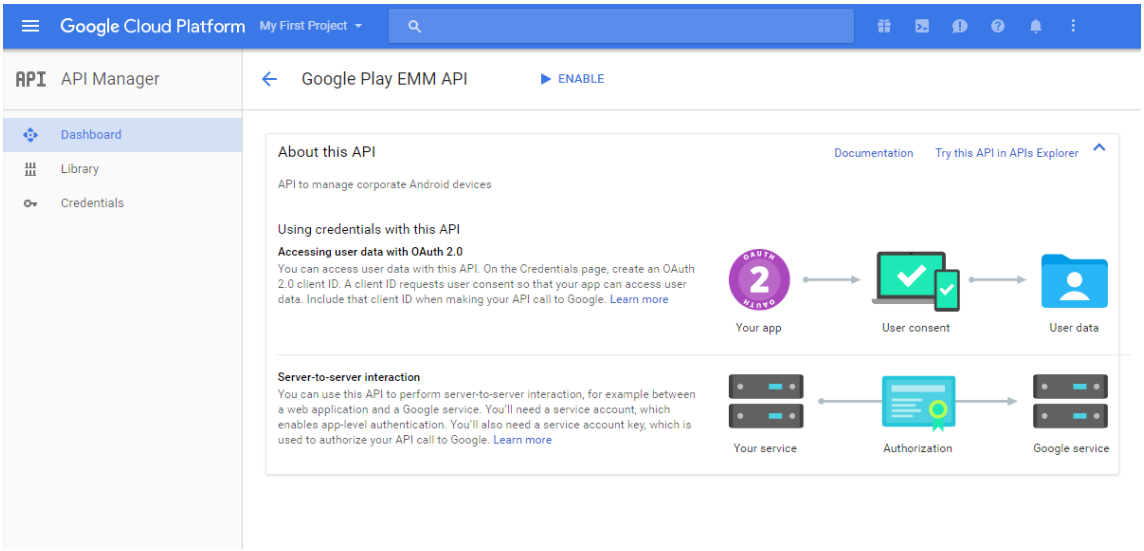
4. 대시보드에서 **Use Google APIs(Google API** 사용**)** 를클릭합니다.



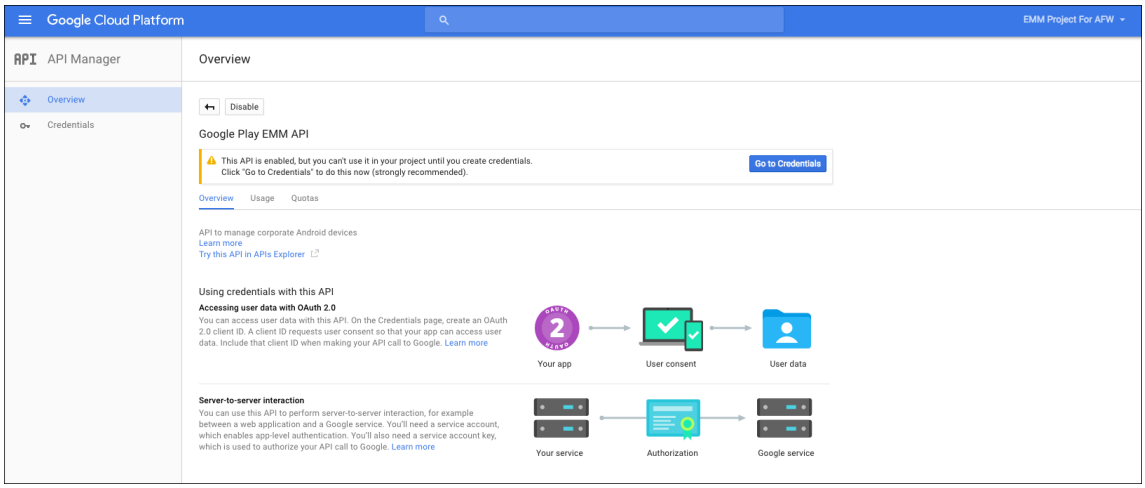
5. **Library(**라이브러리**)** 를클릭하고 **Search(**검색**)** 에 **EMM** 을입력한다음검색결과를클릭합니다.



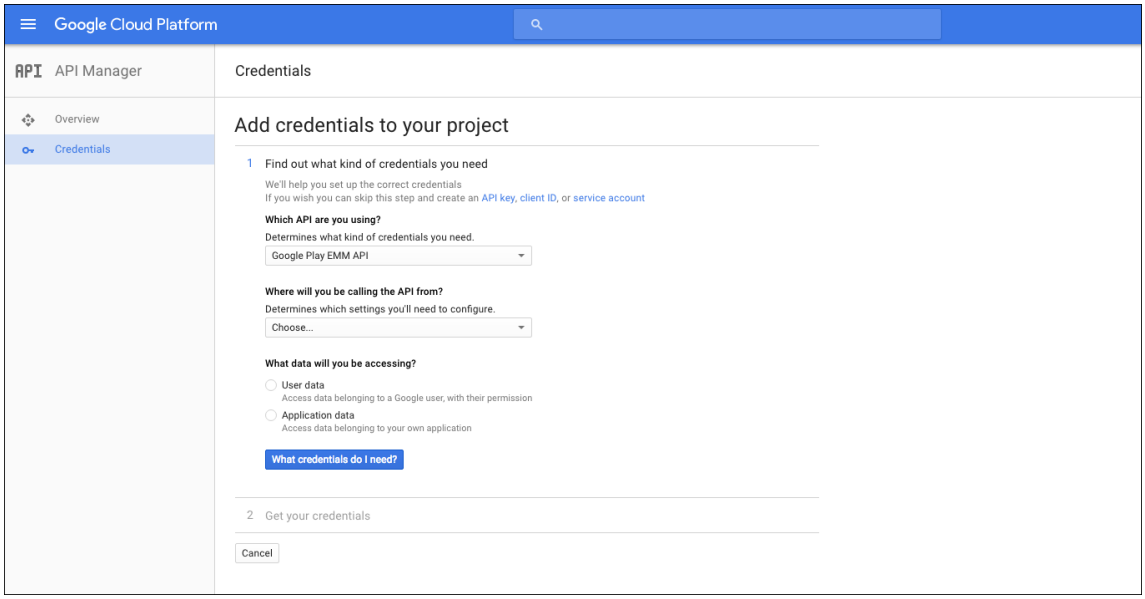
6. **Overview(**개요**)** 페이지에서 **Enable(**사용**)** 을클릭합니다.



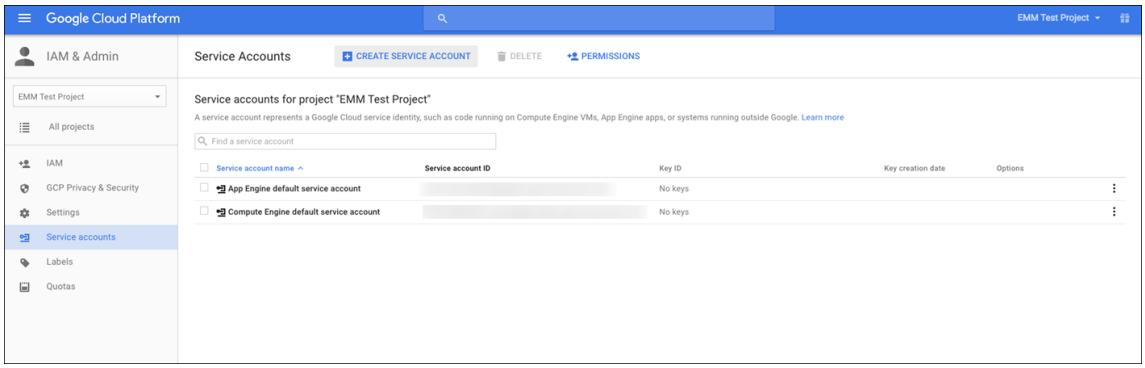
7. **Google Play EMM API** 옆에서 **Go to Credentials(**자격증명으로이동**)** 를클릭합니다.



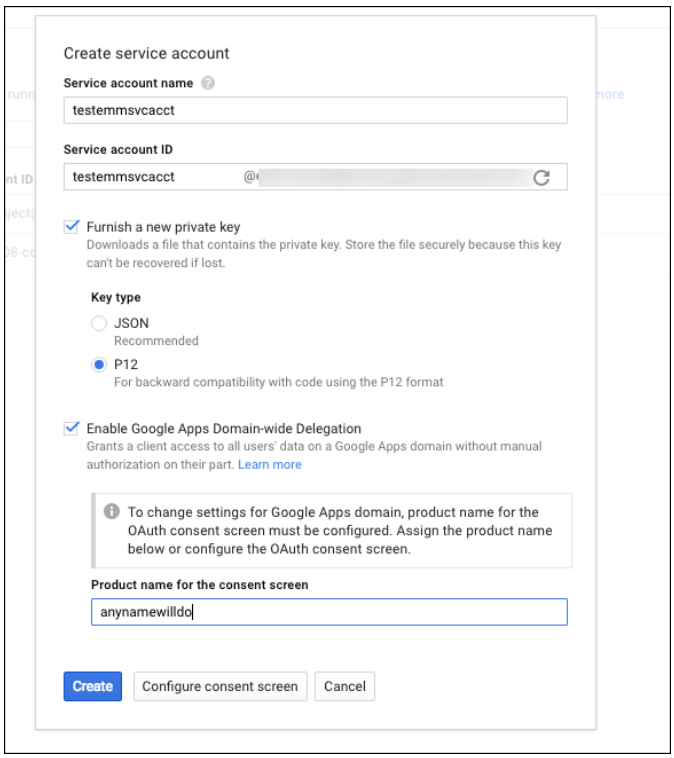
8. **Add credentials to our project(**프로젝트에자격증명추가**)** 목록의 1 단계에서 **service account(**서비스계정**)** 를클릭합니다.



9. **Service Accounts(**서비스계정**)** 페이지에서 **Create Service Account(**서비스계정만들기**)** 를클릭합니다.

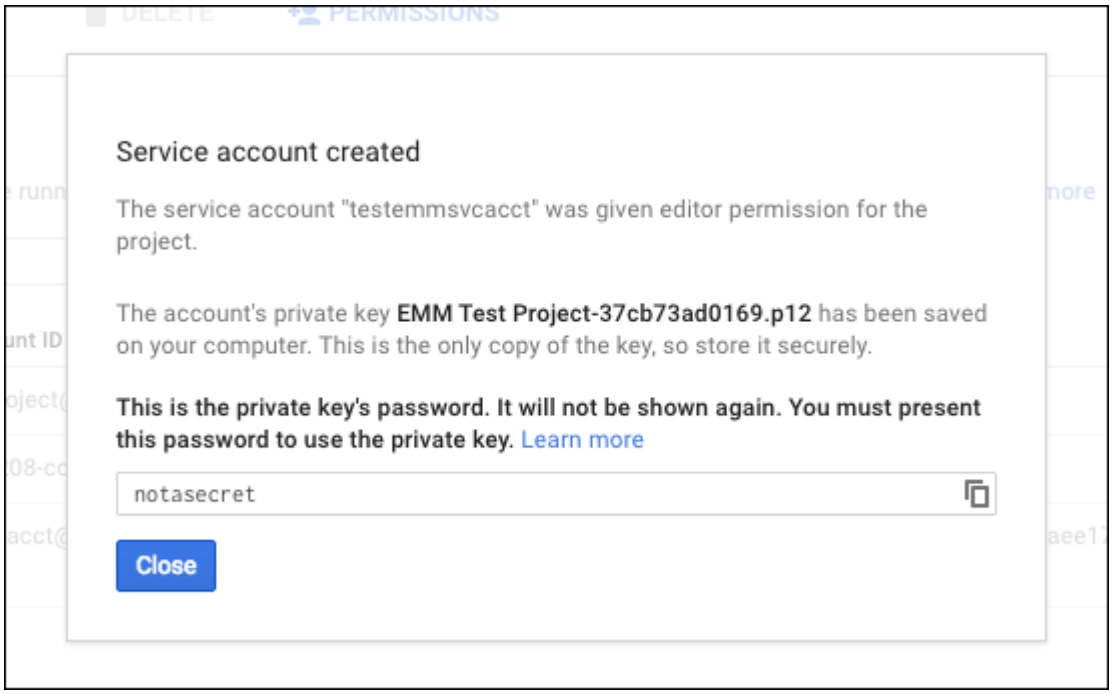


10. **Create service account(**서비스계정만들기**)** 에서계정이름을지정하고 **Furnish a new private key(**새개인키준비**)** 확인란을선택합니다. **P12** 를클릭하고 **Enable Google Apps Domain-wide Delegation(Google Apps** 도메인전체위임사용**)** 확인란을선택한후 **Create(**만들기**)** 를클릭합니다.

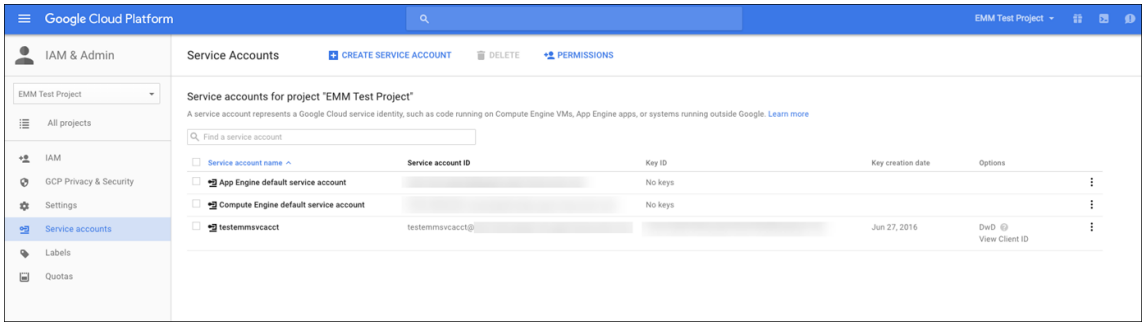


인증서 (P12 파일) 가컴퓨터에다운로드됩니다. 인증서를안전한위치에저장합니다.

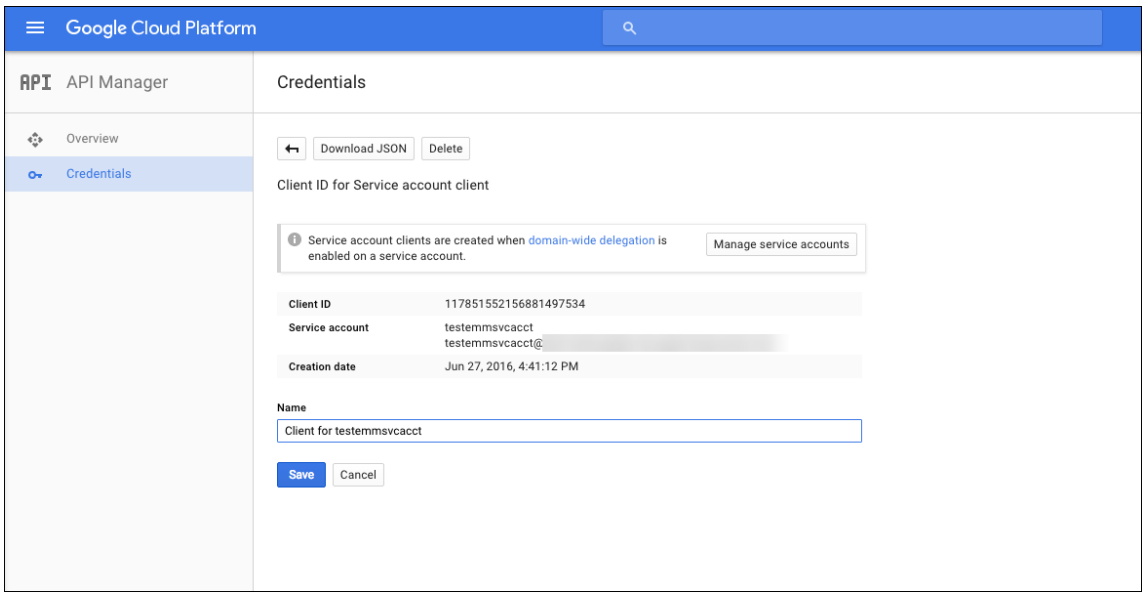
11. **Service account created**(서비스계정만들어짐) 확인페이지에서 **Close**(닫기) 를클릭합니다.



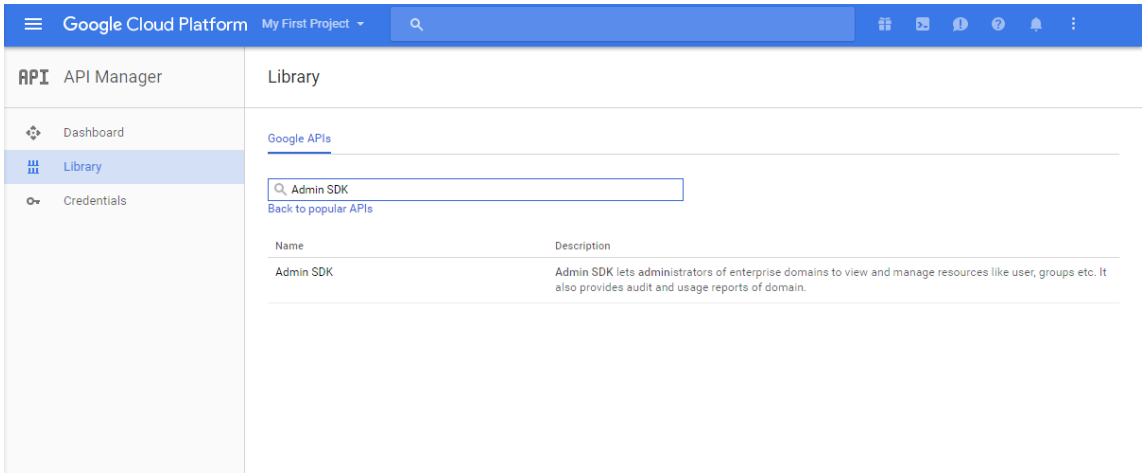
12. **Permissions**(권한) 에서 **Service accounts**(서비스계정) 를클릭한다음서비스계정의 **Options**(옵션) 에서 **View Client ID**(클라이언트 **ID** 보기) 를클릭합니다.



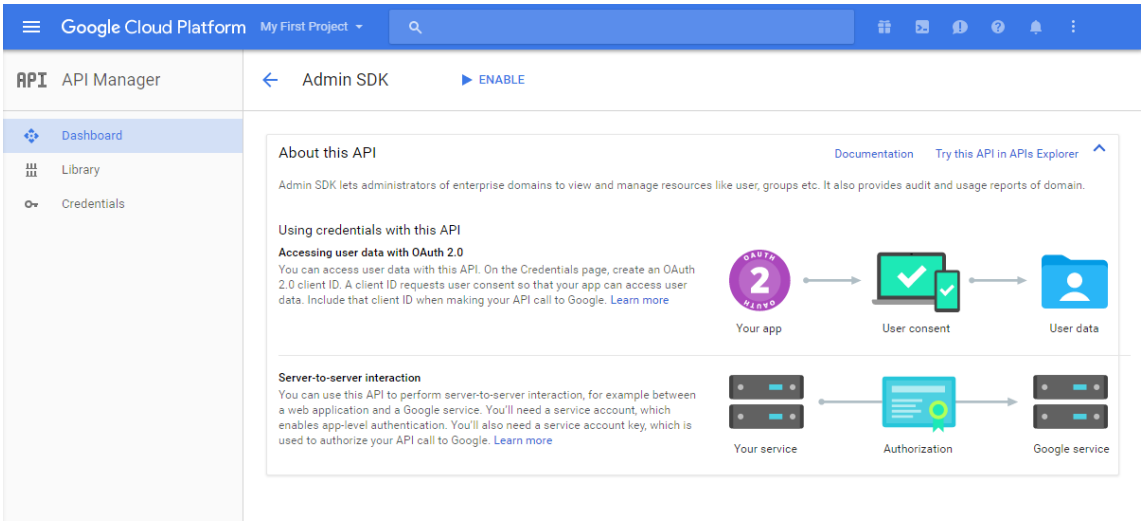
13. Google 관리콘솔의계정승인에필요한세부정보가표시됩니다. **Client ID(**클라이언트 **ID)** 및 **Service account ID(**서비스계정 **ID)** 를나중에정보를검색할수있는위치에복사합니다. 허용하기위해 Citrix 지원에도메인이름을보낼때이 정보가필요합니다.



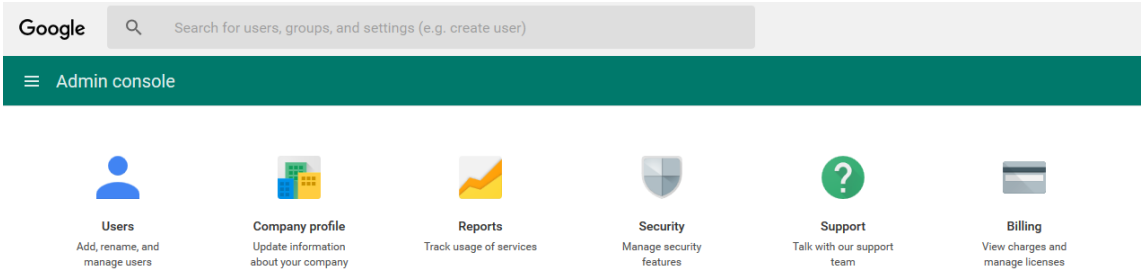
14. **Library(**라이브러리**)** 페이지에서 **Admin SDK** 를검색한다음검색결과를클릭합니다.



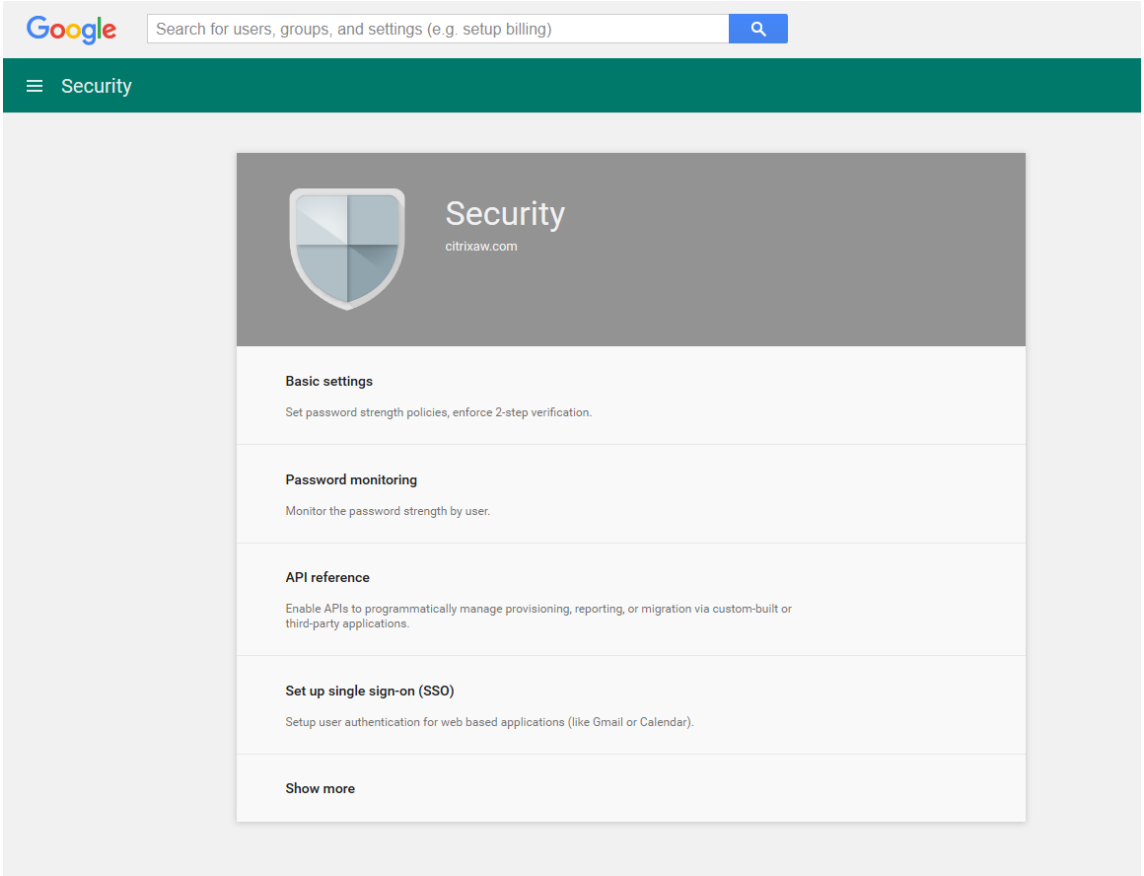
15. **Overview(**개요**)** 페이지에서 **Enable(**사용**)** 을클릭합니다.

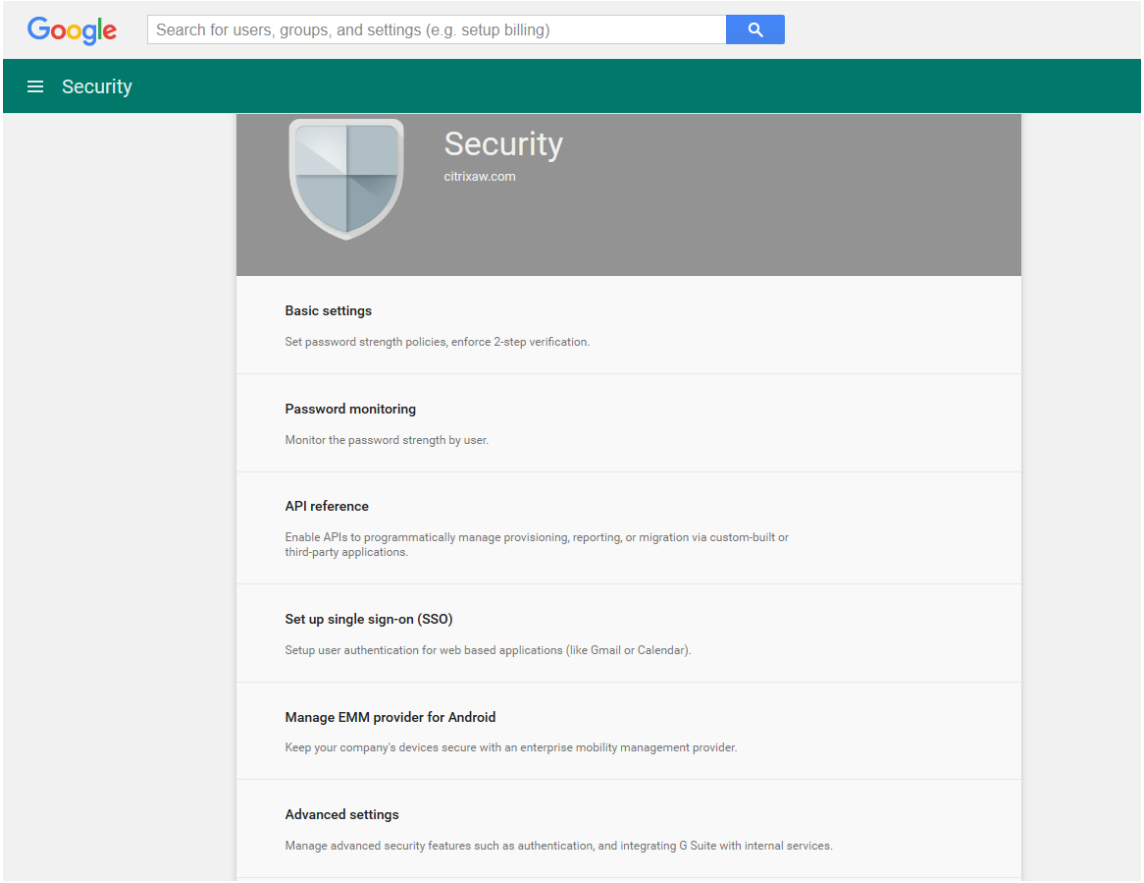


16. 도메인에대한 Google 관리콘솔을연다음 **Security(**보안**)** 를클릭합니다.

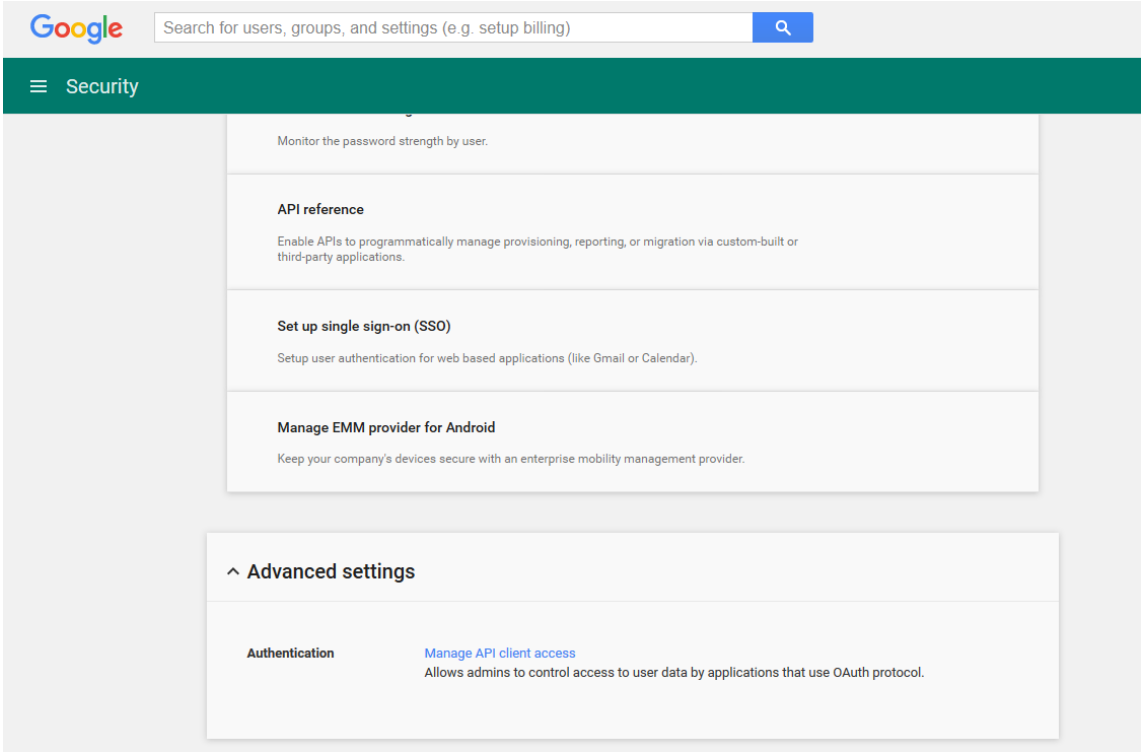


17. **Settings(**설정**)** 페이지에서 **Show more(**자세히표시**)** 를클릭한다음 **Advanced settings(**고급설정**)** 를클릭합니다.

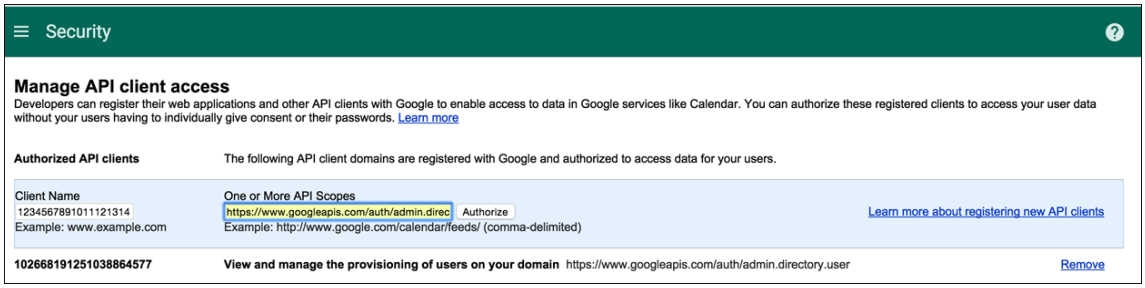




18. **Manage API client access(API** 클라이언트액세스관리**)** 를클릭합니다.



19. **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.



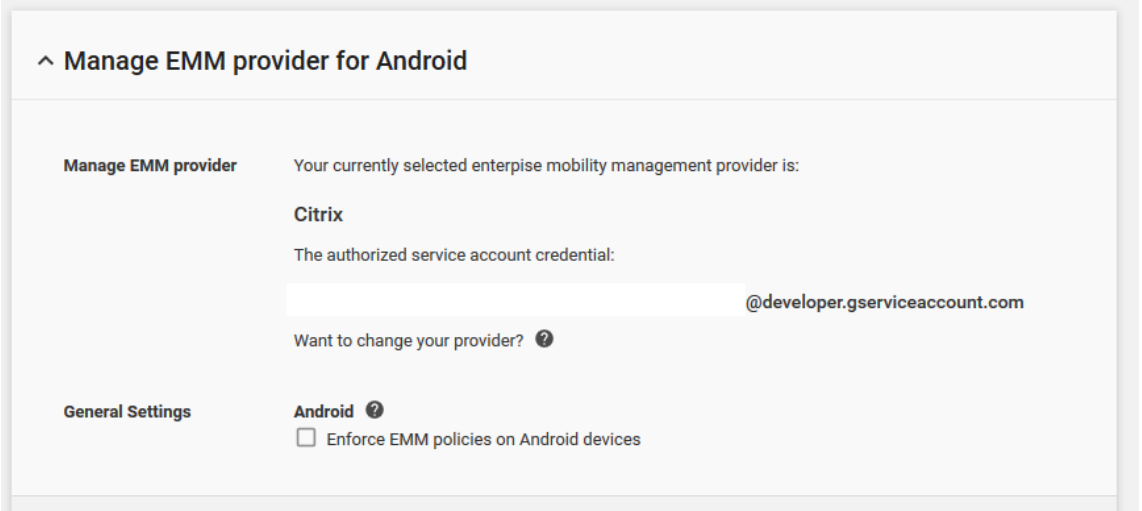
EMM 바인딩

XenMobile 을사용하여 Android 장치를관리하려면먼저 Citrix 기술지원팀에연락하여도메인이름, 서비스계정및바인딩토큰을제공해야합니다. Citrix 는해당토큰을사용자의 EMM(엔터프라이즈모빌리티관리) 공급자로 XenMobile 에바인딩합니다. Citrix 기술지원의연락처정보는 Citrix Technical Support(Citrix 기술지원)를참조하십시오.

1. 바인딩을확인하려면 Google Admin 포털에로그인한다음 **Security(**보안**)** 를클릭합니다.
2. **Manage EMM provider for Android(Android** 용 **EMM** 공급자관리**)** 를클릭합니다.

   Google Android Enterprise 계정이 EMM 공급자로 Citrix 에바인딩되었음을확인할수있습니다.

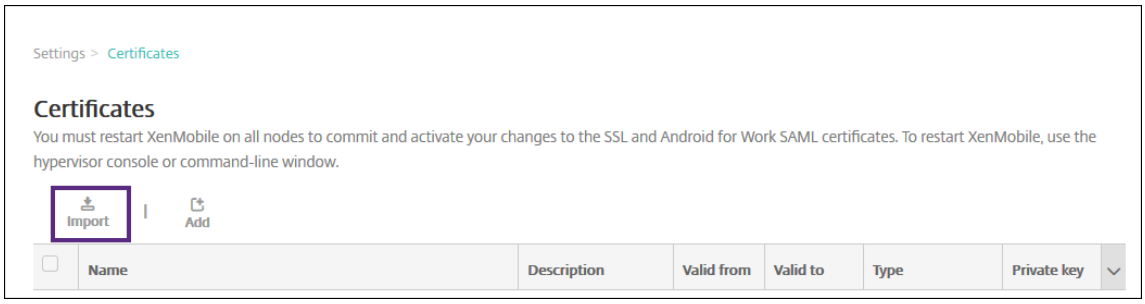
   토큰바인딩을확인한후 XenMobile 콘솔을사용하여 Android 장치를관리할수있습니다. 14 단계에서생성한 P12 인증서를가져옵니다. Android Enterprise 서버설정을지정하고, SAML 기반 SSO(Single Sign On) 를사용하도록설정하고, Android Enterprise 장치정책을하나이상정의합니다.



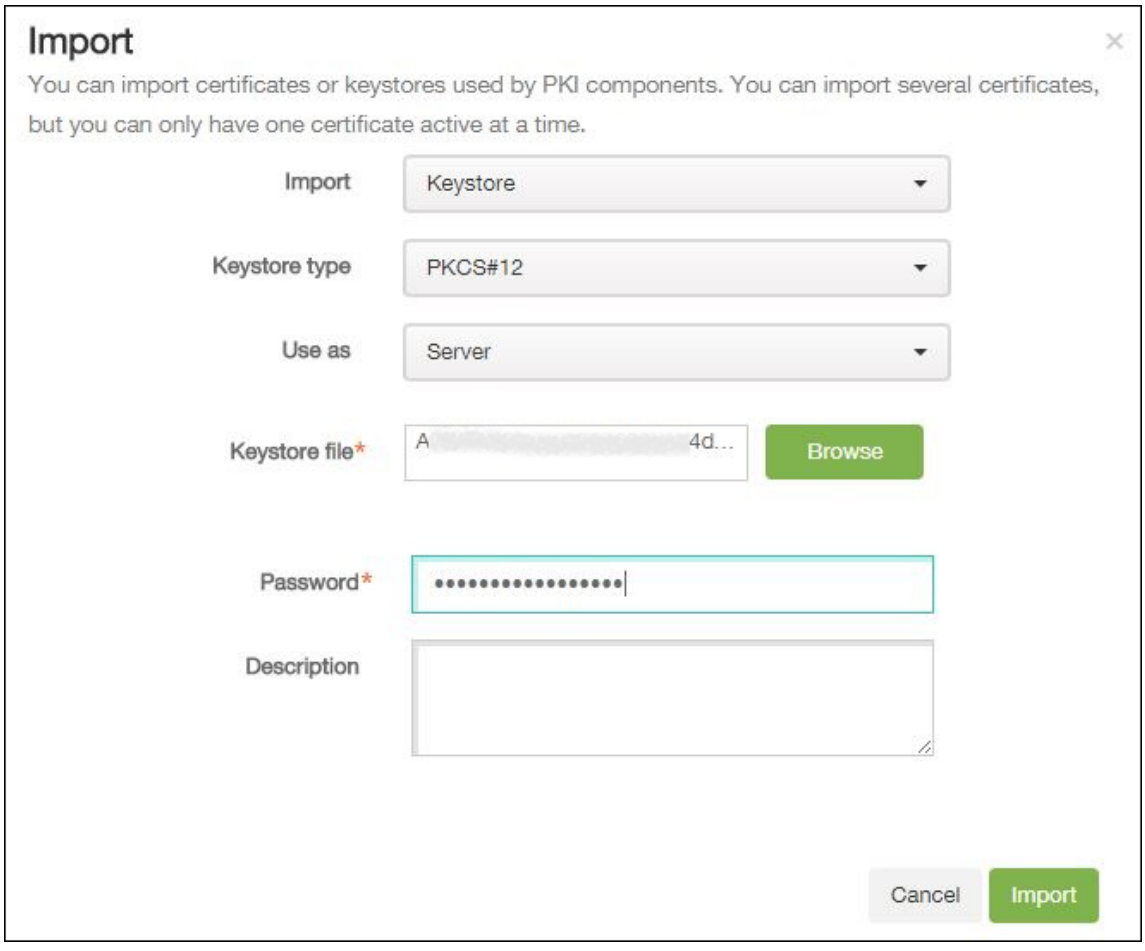
P12 인증서가져오기

Android Enterprise P12 인증서를가져오려면다음단계를따르십시오.

1. XenMobile 콘솔에로그인합니다.
2. 콘솔의오른쪽맨위에있는기어아이콘을클릭하여 설정페이지를연다음 인증서를클릭합니다. 인증서페이지가나타납니다.



3. 가져오기를클릭합니다. 가져오기대화상자가나타납니다.



다음설정을구성합니다.

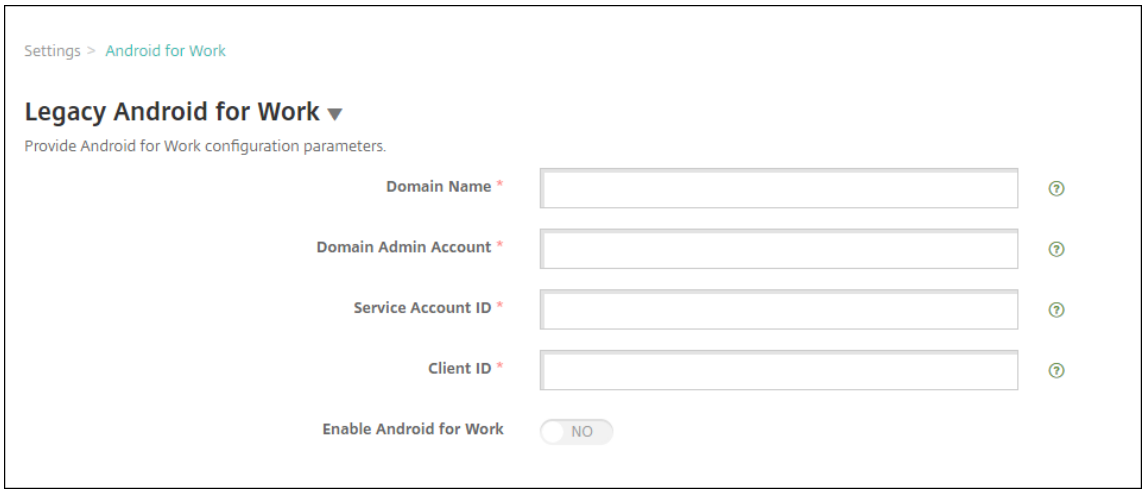
- 가져오기**:** 목록에서 키저장소를클릭합니다.
- 키저장소유형**:** 목록에서 **PKCS#12** 를클릭합니다.
- 용도**:** 목록에서 서버를클릭합니다.
- 키저장소파일**:** 찾아보기를클릭하고 P12 인증서를찾아선택합니다.
- 암호**:** 키저장소암호를입력합니다.

- 설명**:** 인증서에대한선택적설명을입력합니다.

4. 가져오기를클릭합니다.

Android Enterprise 서버설정

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버아래에서 **Android Enterprise** 를클릭합니다. **Android Enterprise** 페이지가나타납니다.

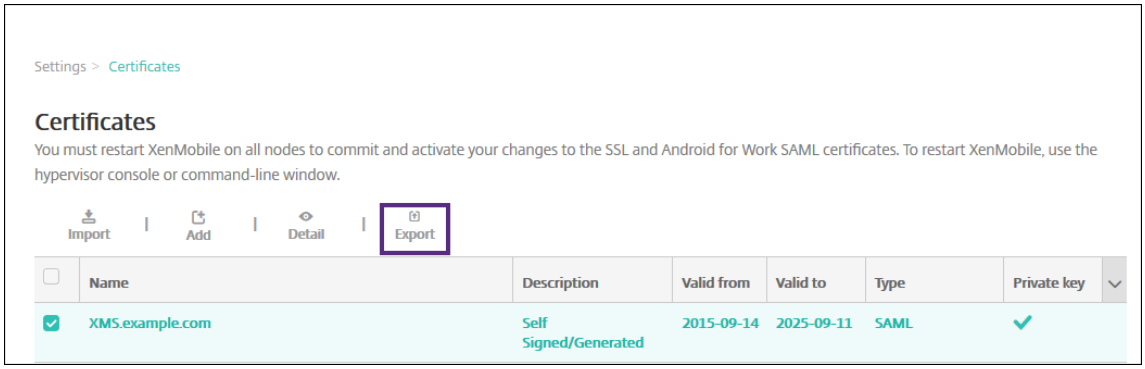


다음설정을구성한후 저장을클릭합니다.

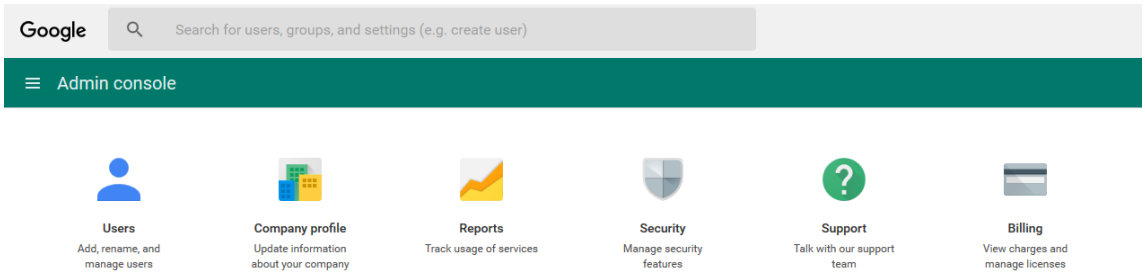
- 도메인이름**:** Android Enterprise 도메인이름을입력합니다 (예: domain.com).
- 도메인관리자계정**:** 도메인관리자사용자이름을입력합니다 (예: Google 개발자포털에사용되는전자메일계정).
- 서비스계정 **ID:** 서비스계정 ID 를입력합니다. 예를들어 Google 서비스계정에연결된전자메일 (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com) 을입력합니다.
- 클라이언트 **ID:** Google 서비스계정의클라이언트 ID(숫자) 를입력합니다.
- **Android Enterprise** 사용**:** Android Enterprise 를사용하거나사용하지않도록선택합니다.

SAML 기반 **SSO(Single Sign On)** 사용

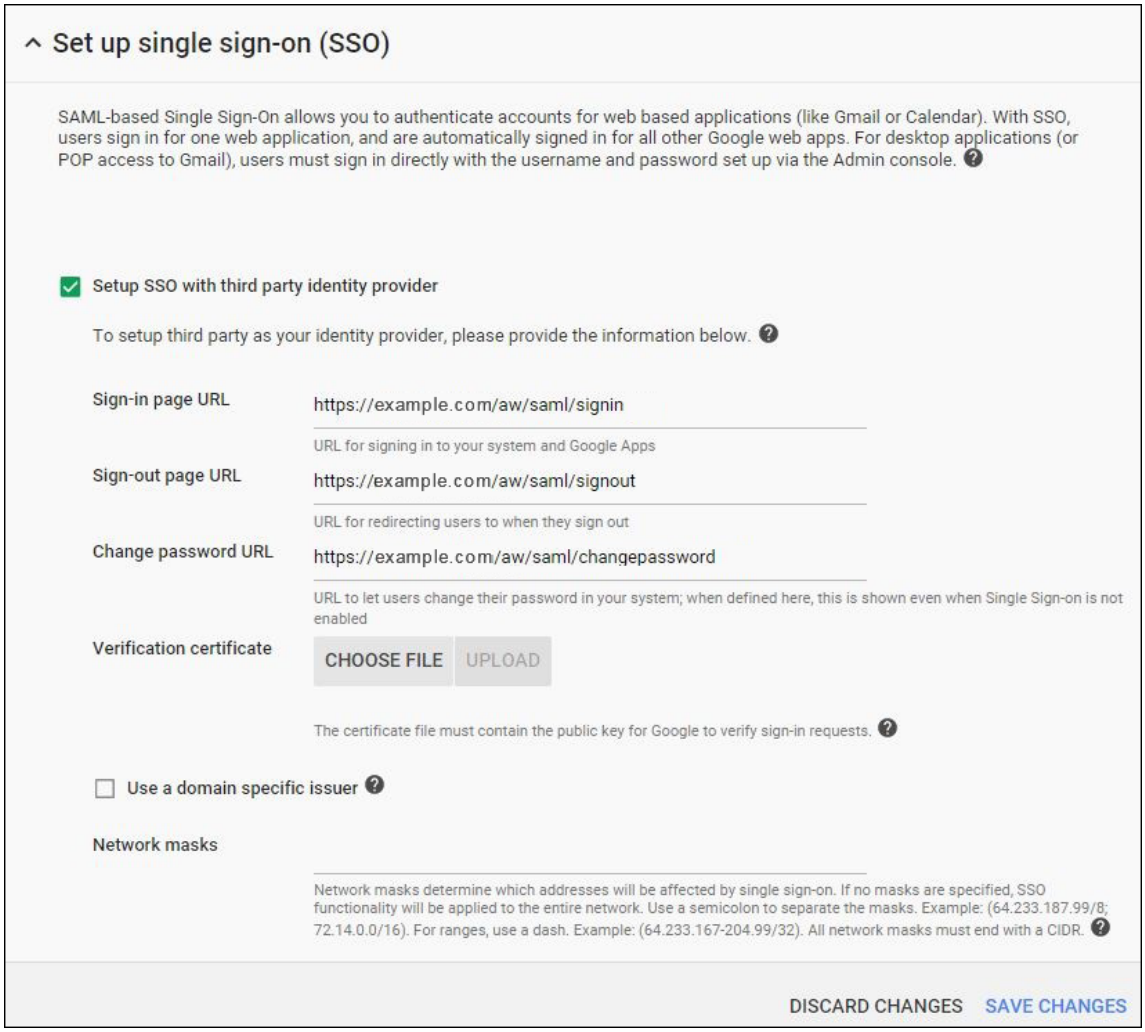
1. XenMobile 콘솔에로그인합니다.
2. 콘솔오른쪽위모서리에서기어아이콘을클릭합니다. 설정페이지가나타납니다.
3. 인증서를클릭합니다. 인증서페이지가나타납니다.



4. 인증서목록에서 SAML 인증서를클릭합니다.
5. 내보내기를클릭하고인증서를컴퓨터에저장합니다.
6. Android Enterprise 관리자자격증명을사용하여 Google Admin 포털에로그인합니다. 포털액세스에대한자세한내용은 Google Admin 포털을참조하십시오.
7. **Security(**보안**)** 를클릭합니다.



8. **Security(**보안**)** 아래에서 **Set up single sign-on (SSO)(SSO(Single Sign-On)** 설정**)** 을클릭한후다음과같은설정을구성합니다.

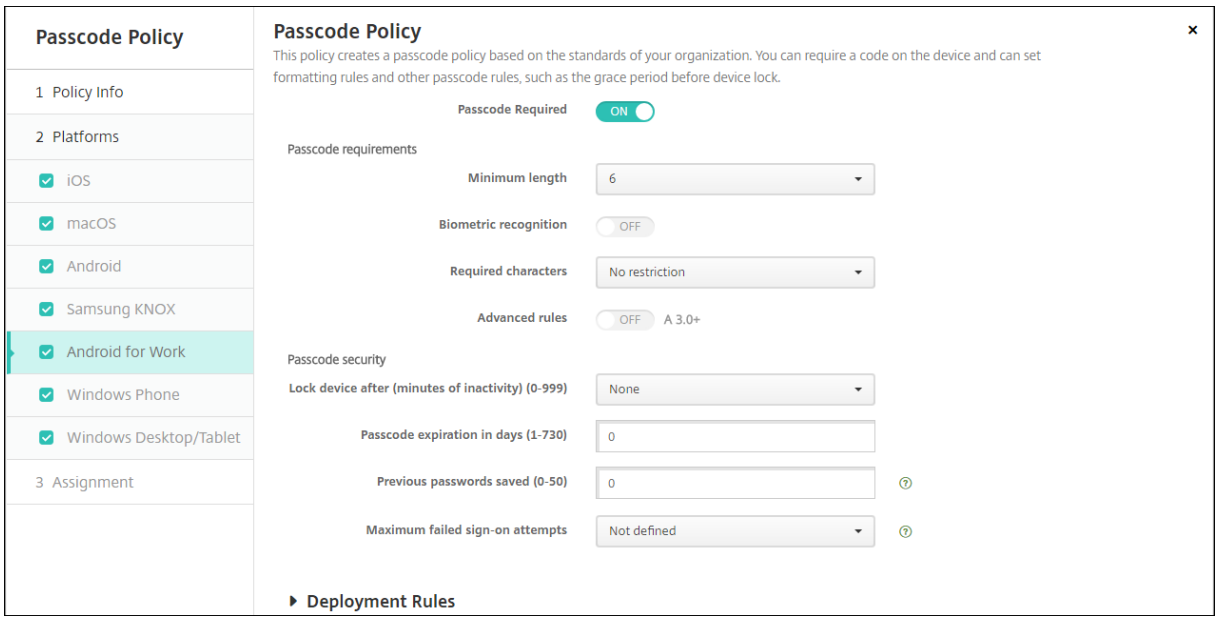


- **Sign-in page URL(**로그인페이지 **URL):** 사용자가시스템및 Google Apps 에로그인할수있는 URL 을입력합니다. 예: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **Sign out page URL(**로그아웃페이지 **URL):** 사용자가로그아웃한경우리디렉션되는 URL 을입력합니다. 예: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **Change password URL(**암호변경 **URL):** 사용자가시스템의암호를변경할수있는 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.



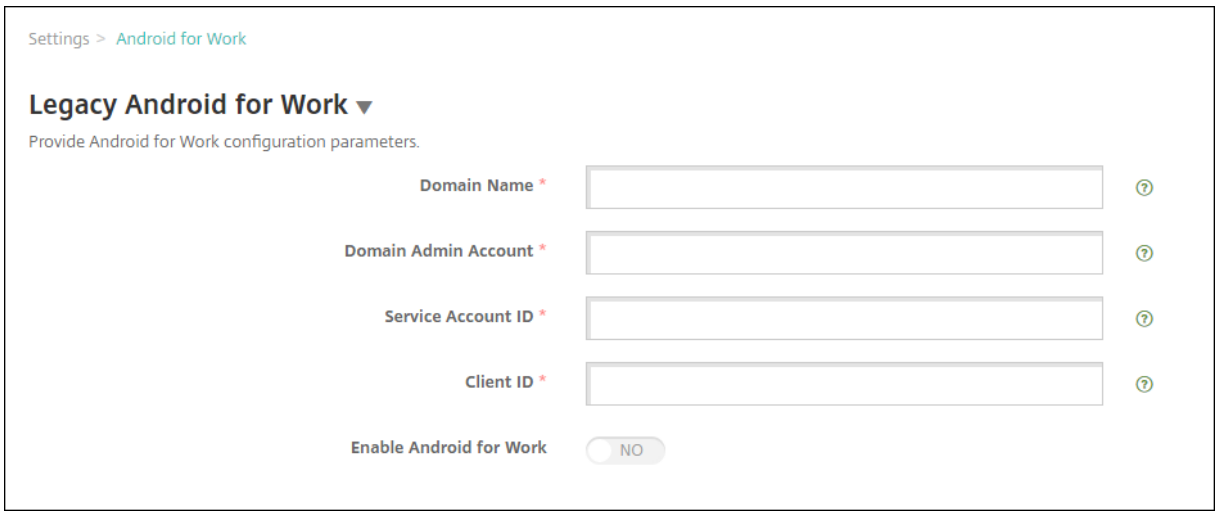
모든장치정책을설정하는기본단계는다음과같습니다.

1. XenMobile 콘솔에로그온합니다.
2. 구성을클릭한다음 장치정책을클릭합니다.
3. 추가를클릭한다음 새정책추가대화상자에서추가하려는정책을선택합니다. 이예제에서는 암호를클릭합니다.
4. 정책정보페이지를완성합니다.
5. **Android Enterprise** 를클릭한다음정책에대한설정을구성합니다.
6. 배달그룹에정책을할당합니다.

Android Enterprise 계정설정구성

장치에서 Android 앱및정책관리를시작하려면먼저 XenMobile 에서 Android Enterprise 도메인및계정정보를설정해야합니다. 먼저 Google 에서 Android Enterprise 설정작업을완료하여도메인관리자를설정하고서비스계정 ID 및바인딩토큰을얻습니다.

1. XenMobile 웹콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 서버아래에서 **Android Enterprise** 를클릭합니다. **Android Enterprise** 구성페이지가나타납니다.



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 **Google Workspace** 파트너액세스설정

일부 Chrome 용엔드포인트관리기능은 Google 파트너 API 를사용하여 XenMobile 과 Google Workspace 도메인간에통신합니다. 예를들어 XenMobile 에는시크릿모드와게스트모드같은 Chrome 기능을관리하기위한장치정책용 API 가필요합니다.

파트너 API 를사용하려면 XenMobile 콘솔에서 Google Workspace 도메인을설정한다음 Google Workspace 계정을구성합니다.

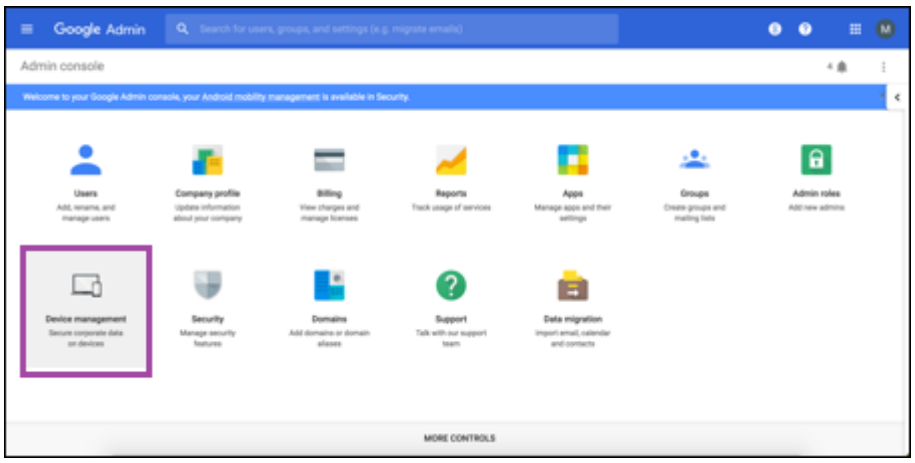
XenMobile 에서 **Google Workspace(**이전명칭 **G Suite)** 도메인설정

XenMobile 이 Google Workspace 도메인의 API 와통신하도록설정하려면 설정 **> Google Chrome** 구성으로이동하여설정을구성합니다.

- **G Suite** 도메인**:** XenMobile 에필요한 API 를호스팅하는 Google Workspace 도메인입니다.
- **G Suite** 관리도메인**:** G Suite 도메인의관리자계정입니다.
- **G Suite** 클라이언트 **ID:** Citrix 의클라이언트 ID 입니다. Google Workspace 도메인에대한파트너액세스를구성하려면이값을사용합니다.
- **G Suite** 엔터프라이즈 **ID:** 계정의엔터프라이즈 ID 로, Google Enterprise 계정에서채워집니다.

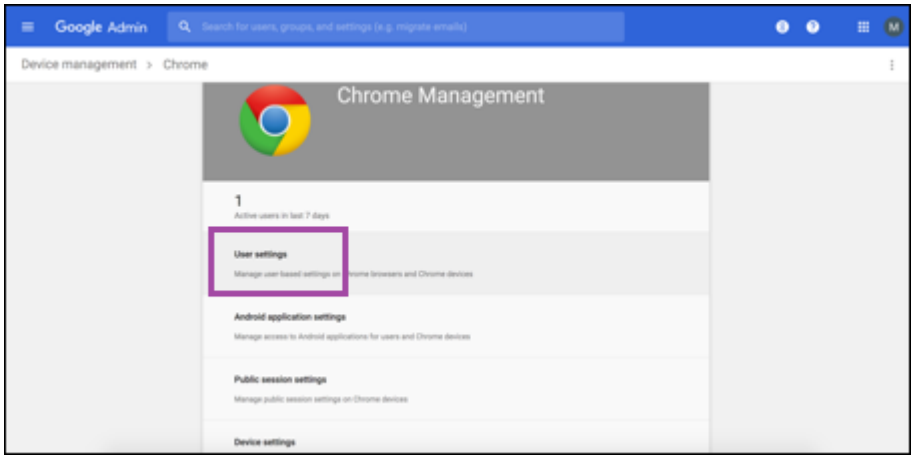
Google Workspace 도메인의장치와사용자에대한파트너액세스설정

1. Google 관리자콘솔에로그인합니다. https://admin.google.com
2. **Device Management(**장치관리**)** 를클릭합니다.



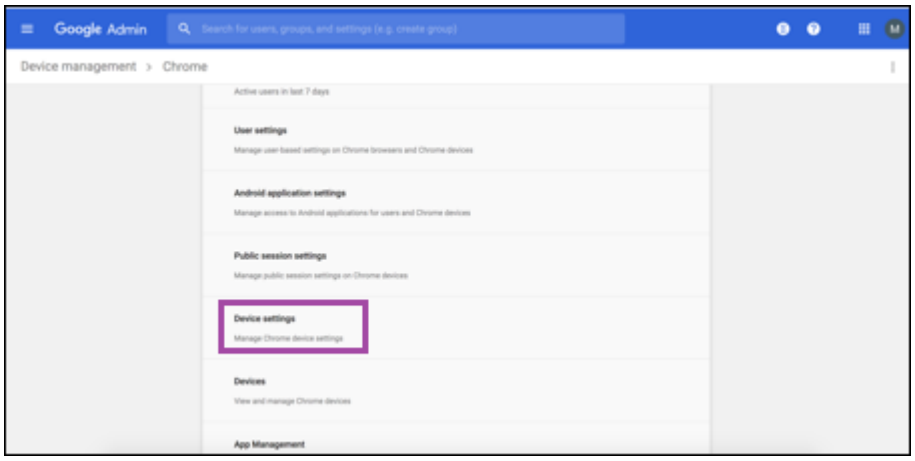
3. **Chrome management(Chrome** 관리**)** 를클릭합니다.

4. **User settings(**사용자설정**)** 를클릭합니다.

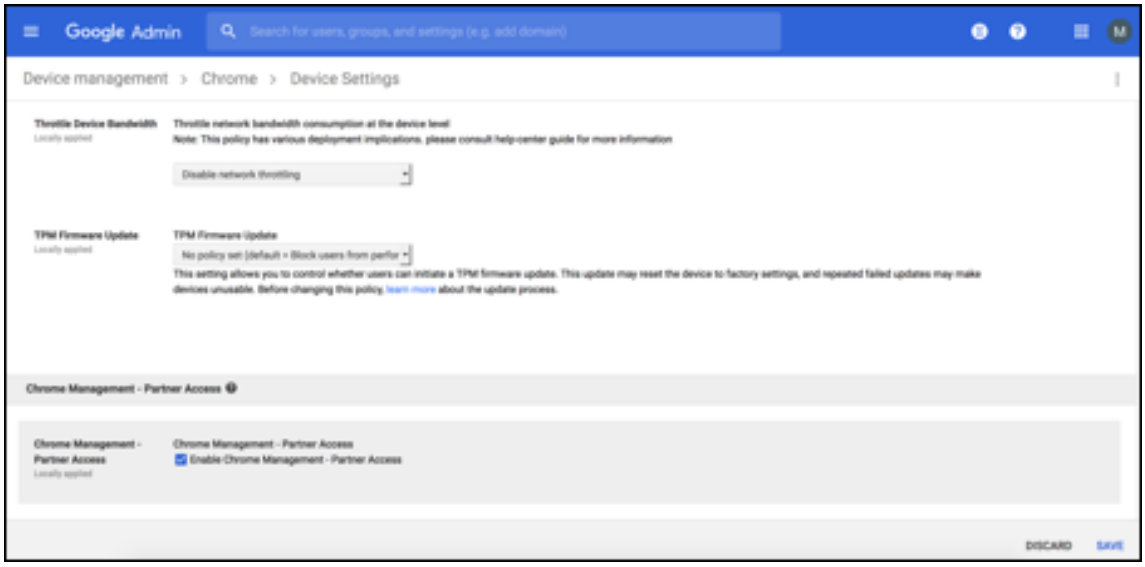


5. **Chrome Management - Partner Access(Chrome** 관리 **-** 파트너액세스**)** 를검색합니다.

6. **Enable Chrome Management - Partner Access(Chrome** 관리 **-** 파트너액세스사용**)** 확인란을선택합니다.
7. 파트너액세스를이해하고사용하길원한다는데동의합니다. 저장을클릭합니다.
8. Chrome 관리페이지에서 **Device Settings(**장치설정**)** 를클릭합니다.



9. **Chrome Management - Partner Access(Chrome** 관리 **-** 파트너액세스**)** 를검색합니다.

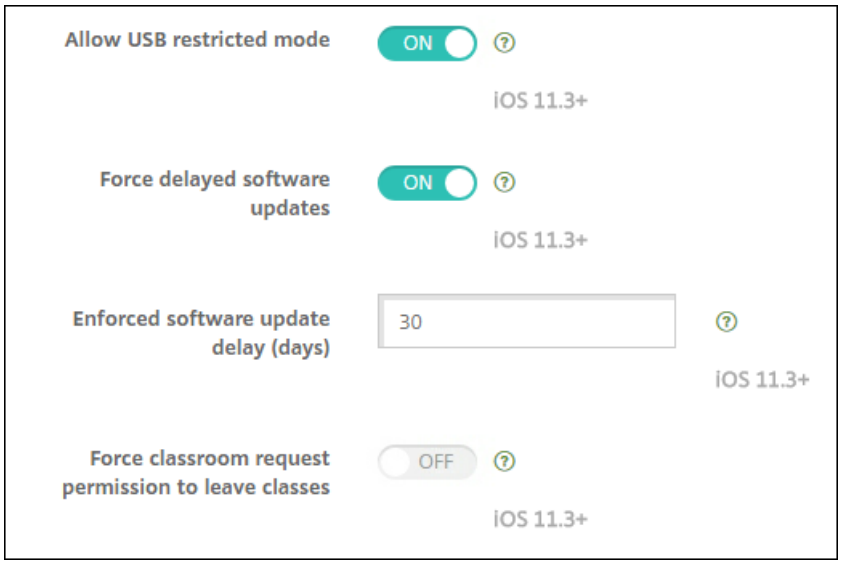


10. **Enable Chrome Management - Partner Access(Chrome** 관리 **-** 파트너액세스사용**)** 확인란을선택합니다.
11. 파트너액세스를이해하고사용하길원한다는데동의합니다. 저장을클릭합니다.
12. **Security(**보안**)** 페이지로이동한다음 **Advanced Settings(**고급설정**)** 를클릭합니다.

13. **Manage API client access(API** 클라이언트액세스관리**)** 를클릭합니다.
14. XenMobile 콘솔에서 설정 **> Google Chrome** 구성으로이동하여 Google Workspace 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 사이트주소를팝업차단허용목록에추가해야합니다.

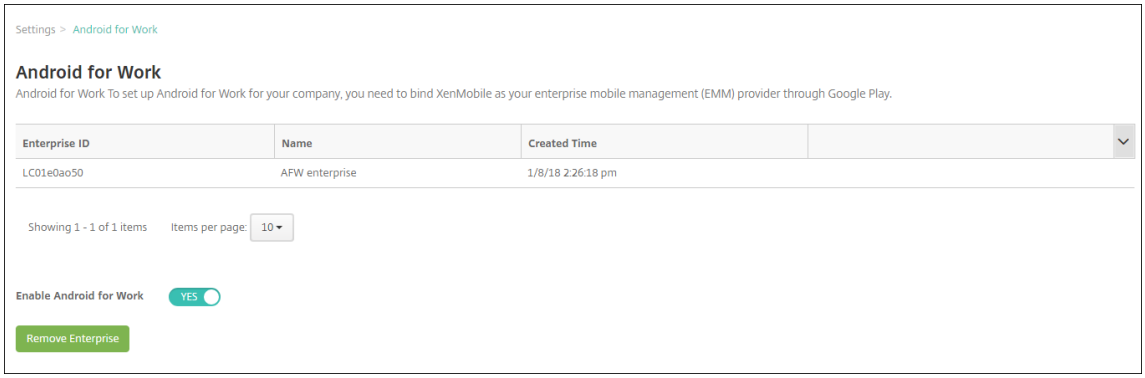
> 경고**:**
>
> 엔터프라이즈등록이취소되면엔터프라이즈를통해이미등록된장치의 Android Enterprise 앱이기본상태로재설정됩니다. 장치가더이상 Google 을통해관리되지않습니다. Android Enterprise 엔터프라이즈에다시등록하는경우추가구성을수행하지않으면이전기능이복원되지않을수있습니다.

Android Enterprise 엔터프라이즈등록취소후:

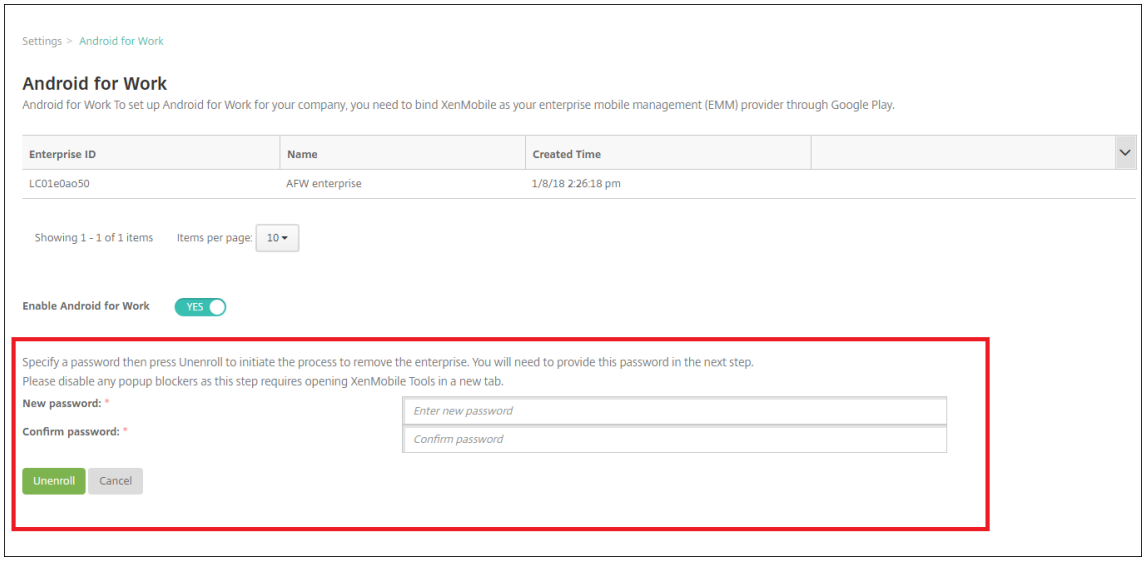
- 엔터프라이즈를통해등록된장치및사용자의 Android Enterprise 앱이기본상태로재설정됩니다. 이전에적용된 Android Enterprise 앱권한및 Android Enterprise 앱제한정책이더이상유효하지않습니다.
- 엔터프라이즈를통해등록된장치는 XenMobile 을통해관리되지만 Google 측면에서는관리되지않습니다. 새로운 Android Enterprise 앱을추가할수없습니다. 새로운 Android Enterprise 앱권한또는 Android Enterprise 앱제한정책을적용할수없습니다. 예약, 암호및제한같은다른정책은계속해서이러한장치에적용할수있습니다.
- Android Enterprise 에장치를등록하려고하면 Android Enterprise 장치가아닌 Android 장치로등록됩니다.

Android Enterprise 엔터프라이즈를등록취소하려면:

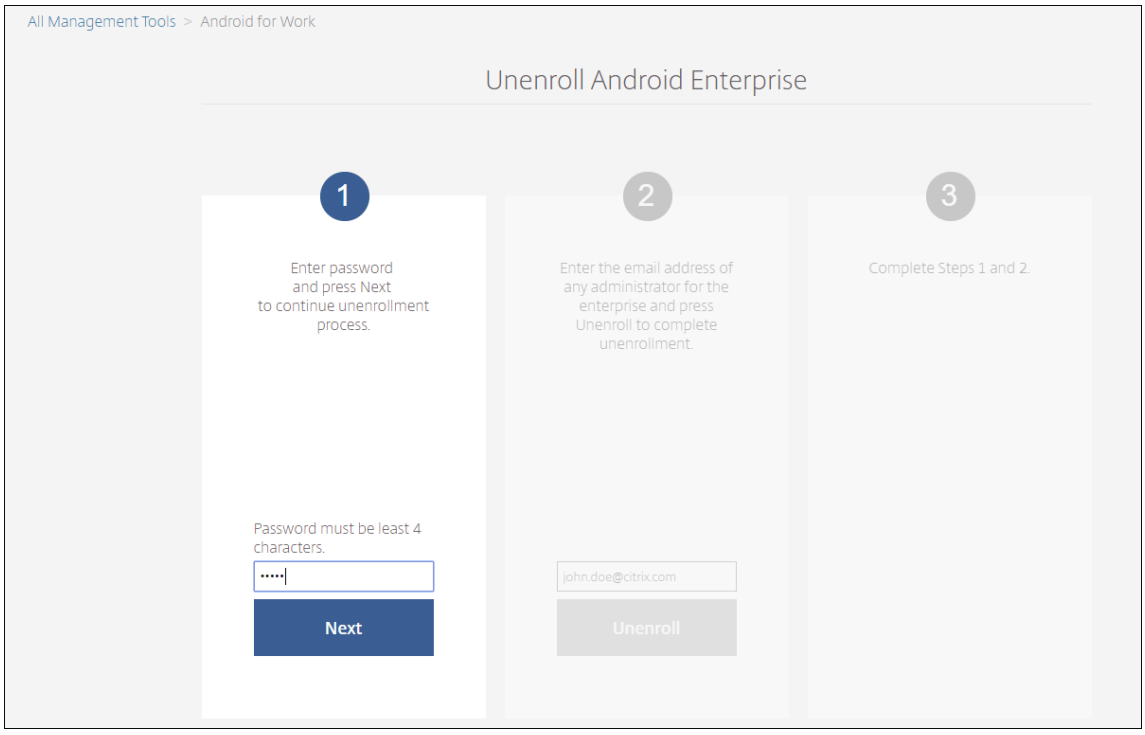
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 설정페이지에서 **Android Enterprise** 를클릭합니다.
3. 엔터프라이즈제거를클릭합니다.



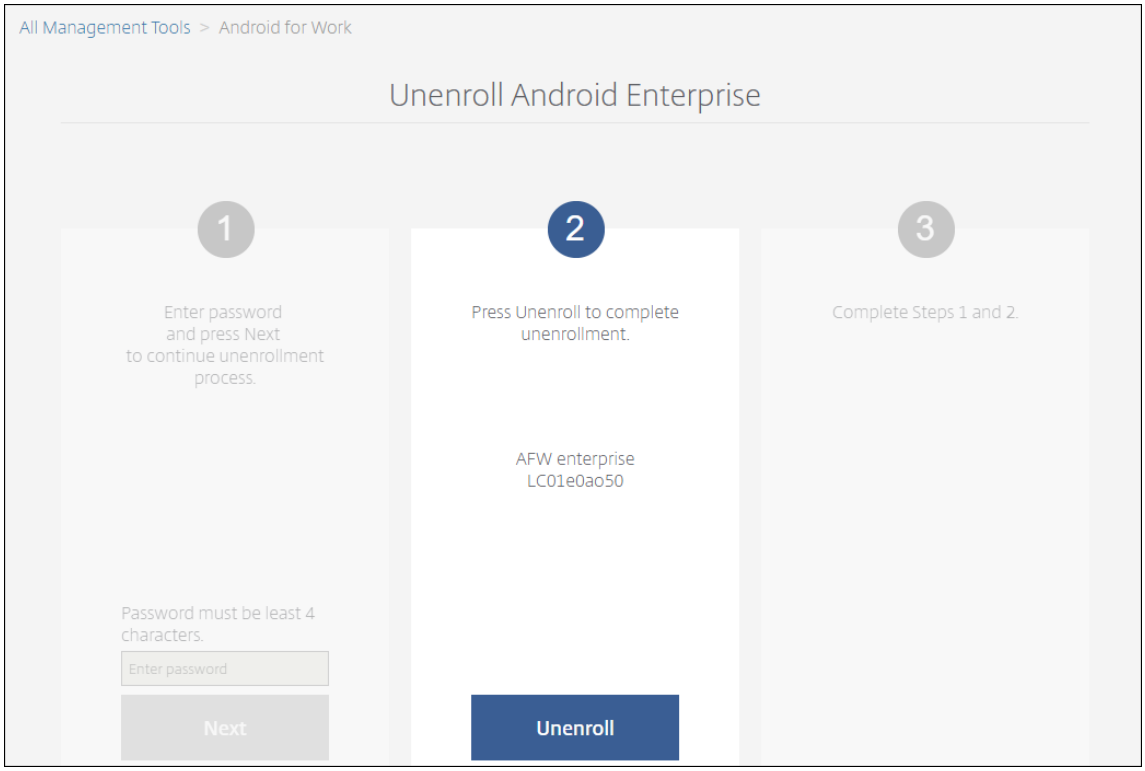
4. 암호를지정합니다. 그다음단계에서등록취소를완료하려면암호가필요합니다. 그런다음 등록취소를클릭합니다.



5. XenMobile Tools 페이지가열리면이전단계에서만든암호를입력합니다.



6. 등록취소를클릭합니다.



Android Enterprise 에서완전하게관리되는장치프로비전

회사소유장치만 Android Enterprise 에서완전하게관리되는장치가될수있습니다. 완전하게관리되는장치에서는작업프로필뿐만아니라전체장치가회사또는조직에의해제어됩니다. 완전하게관리되는장치를작업관리장치라고도합니다.

XenMobile 은완전하게관리되는장치에대해다음과같은등록방법을지원합니다.

- **afw#xenmobile:** 이등록방법을사용하는경우사용자가장치를설정할때 “afw#xenmobile” 문자를입력합니다. 이토큰은 XenMobile 이관리하는장치로장치를식별하고 Secure Hub 를다운로드합니다.
- **QR** 코드**:** QR 코드프로비저닝을통해태블릿과같이 NFC 를지원하지않는분산된제품군의장치를간편하게프로비저닝할수있습니다. QR 코드등록방법은출고기본값으로재설정된제품군장치에사용할수있습니다. QR 코드등록방법은설치마법사에서 QR 코드를스캔하여완전하게관리되는장치를설정하고구성합니다.
- **NFC(**근거리통신**)** 범프**:** NFC 범프등록방법은출고기본값으로재설정된제품군장치에사용할수있습니다. NFC 범프는근거리통신을사용하여두장치간데이터를전송합니다. 출고기본값으로재설정된장치에서는 Bluetooth, Wi-Fi 및기타통신모드를사용할수없습니다. NFC 는이상태에서장치가사용할수있는유일한통신프로토콜입니다.

afw#xenmobile

이등록방법은새장치또는출고기본값으로재설정된장치의전원을켠후초기설정시사용됩니다. 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: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-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.apk`에서다운로드할수있습니다. Secure Hub APK 의경로는프로비저닝시장치가연결되는 Wi-Fi 연결을통해액세스할수있어야합니다.

다음필드는선택사항입니다.

- **android.app.extra.PROVISIONING_LOCALE:** 언어및국가코드를입력합니다.

  언어코드는 ISO 639-1에정의된대로소문자두자로구성된 ISO 언어코드입니다 (예: en). 국가코드는 ISO 3166-1에정의된대로대문자두자로구성된 ISO 국가코드입니다 (예: US). 예를들어, 미국에서사용하는영어의경우 en_US 를입력합니다.

- **android.app.extra.PROVISIONING_TIME_ZONE:** 장치가실행되고있는표준시간대입니다.

  지역/위치형식의 Olson 이름을입력합니다. 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": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

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 를사용하도록설정한 XenMobile Server 버전 10.4

- 완전하게관리되는장치로서 Android Enterprise 용으로프로비전된새장치또는출고기본값으로재설정된장치. 이사전요구사항을완료하는단계는이문서의뒷부분에서찾을수있습니다.
- NFC 호환성이있으며구성된 Provisioning Tool 이실행되고있는또다른장치. Provisioning Tool 은 Secure Hub 10.4 또는 Citrix 다운로드페이지에서사용할수있습니다.

각장치에는 EMM(엔터프라이즈모빌리티관리) 앱으로관리되는 Android Enterprise 프로필이하나만있을수있습니다. XenMobile 에서 Secure Hub 는 EMM 앱입니다. 각장치에는하나의프로필만허용됩니다. 두번째 EMM 앱을추가하면첫번째 EMM 앱이제거됩니다.

NFC 범프를통해전송된데이터

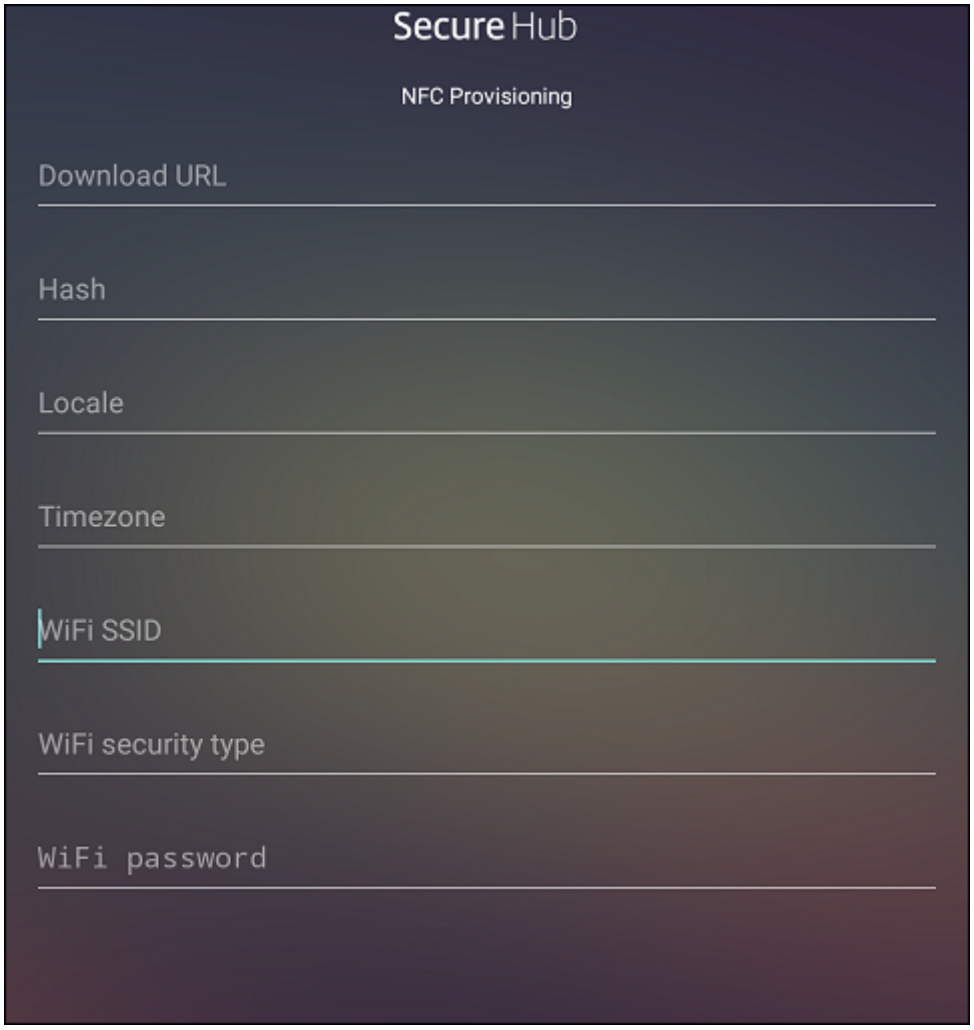
출고기본값으로재설정된장치를프로비저닝하려면 NFC 범프를통해다음데이터를전송하여 Android Enterprise 를초기화해야합니다.

- 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. 입력한정보가앱에저장되지않으므로나중에사용할수있도록정보를유지하려면텍스트파일을만들수있습니다.

텍스트파일을사용하여 **Provisioning Tool** 을구성하려면

파일의이름을 nfcprovisioning.txt 로지정하고장치의 SD 카드에있는 /sdcard/ 폴더에파일을저장합니다. 그러면앱에서텍스트파일을읽고값을채울수있습니다.

텍스트파일에는다음과같은데이터가포함되어야합니다.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

이줄은 EMM 공급자앱의인트라넷/인터넷위치입니다. NFC 범프후에출고기본값으로재설정된장치가 Wi-Fi 에연결되면장치가이위치에액세스하여다운로드할수있어야합니다. URL 은특수한형식이필요하지않은일반 URL 입니다.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>`

이줄은 EMM 공급자앱의체크섬입니다. 이체크섬은다운로드가성공했는지확인하는데사용됩니다. 체크섬을얻는단계에대해서는이문서뒷부분에서설명합니다.

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

이줄은 Provisioning Tool 이실행되고있는장치의연결된 Wi-Fi SSID 입니다.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

지원되는값은 WEP 및 WPA2 입니다. Wi-Fi 가보호되지않는경우이필드는비어있어야합니다.

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Wi-Fi 가보호되지않는경우이필드는비어있어야합니다.

android.app.extra.PROVISIONING_LOCALE=<locale>

언어및국가코드를입력합니다. 언어코드는 ISO 639-1에정의된대로소문자두자로구성된 ISO 언어코드입니다 (예: en). 국가코드는 ISO 3166-1에정의된대로대문자두자로구성된 ISO 국가코드입니다 (예: US). 예를들어, 미국에서사용하는영어의경우 en_US 를입력합니다. 코드를입력하지않으면국가및언어가자동으로입력됩니다.

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

장치가실행되는표준시간대입니다. 지역/위치형식의 Olson 이름을입력합니다. 예를들어태평양표준시의경우 America/Los_Angeles 를입력합니다. 이름을입력하지않으면표준시간대가자동으로입력됩니다.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

값이앱에 Secure Hub 로하드코딩되어있기때문에이데이터는필요하지않습니다. 여기서는완결성을위해언급되었습니다.

예를들어 WPA2 를사용하여보호되는 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=ga50TwdCmfdJ72LGRFkke4Crb
\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=ga50TwdCmfdJ72LGRFkke4Crb
\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.

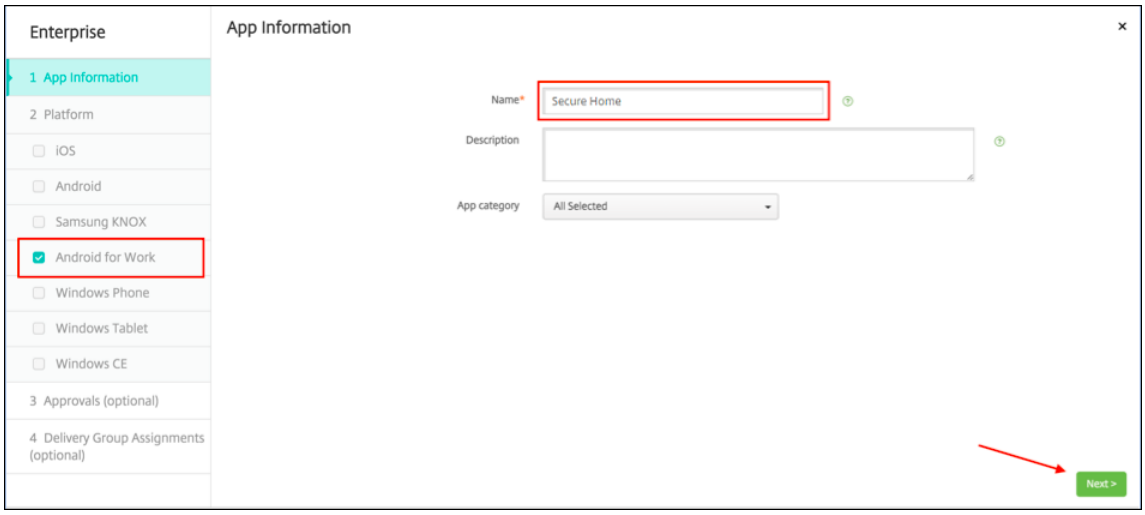
   앱추가창이나타납니다.

2. 엔터프라이즈를클릭합니다.

   앱정보페이지가나타납니다.

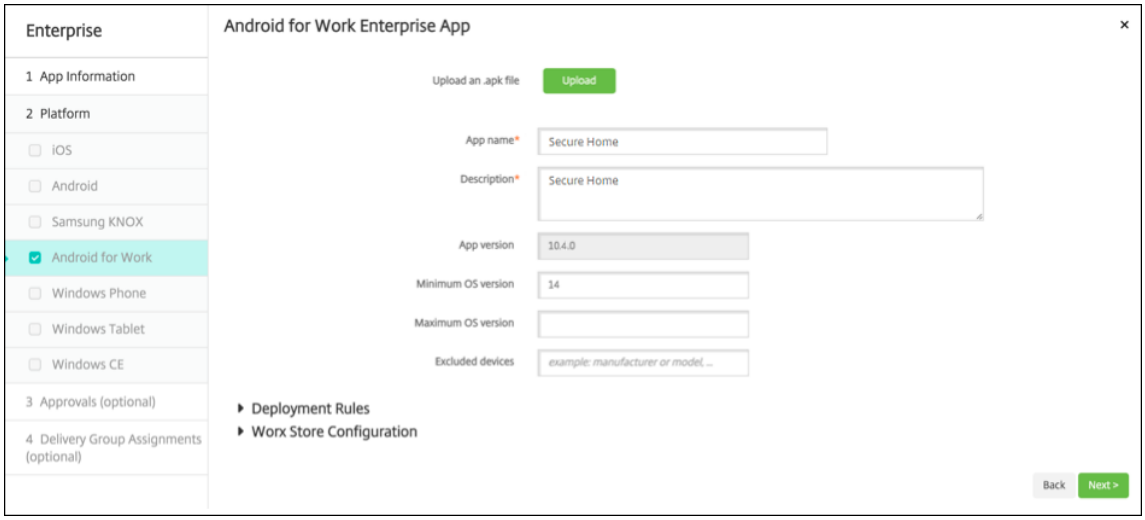
3. 다음과같은구성을선택한후 다음을클릭합니다.

   Android Enterprise 엔터프라이즈앱페이지가나타납니다.



4. .apk 에대한경로를제공한후 다음을클릭하고파일을업로드합니다.

   업로드가완료되면업로드된패키지의세부정보가나타납니다.



5. 다음을클릭하여 JSON 파일을다운로드하는페이지를엽니다. 이파일을사용하여 Google Play 에업로드할수있습니다. Secure Hub 의경우 Google Play 에업로드할필요가없지만 SHA1 값을읽으려면 JSON 파일이필요합니다.

   일반적인 JSON 파일은다음과같은형식입니다.

6. **file_sha1_base64** 값을복사한후 Provisioning Tool 의 해시필드에이값을사용합니다.

   > 참고:
   >
   > 해시는 URL 로사용할수있는형식이어야합니다.

   - 모든 **+** 기호를 **-**로변환합니다.
   - 모든 **/** 기호를 **_** 로변환합니다.
   - 끝에있는 **\u003d** 를 **=** 로바꿉니다.

   장치의 SD 카드에있는 nfcprovisioning.txt 파일에해시를저장하면앱에서안전을위한변환을수행합니다. 하지만수동으로해시를입력하는경우 URL 안전성을보장하는것은사용자의책임입니다.

사용된라이브러리

Provisioning Tool 의소스코드에는다음과같은라이브러리가사용되었습니다.

- Apache 라이센스 2.0 에따라 Google 이제작한 v7 appcompat 라이브러리, 디자인지원라이브러리및 v7 Palette 라이브러리

  자세한내용은 지원라이브러리기능가이드를참조하십시오.

- Apache 라이센스 2.0 에따라 Jake Wharton 이제작한 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 디버깅및알수없는소스설정은장치에서기본적으로비활성화됩니다.

> 팁:
>
> Android Enterprise 에서작업프로필장치로장치를등록하는경우항상 Google Play 로이동하십시오. 거기서사용자의 개인프로필에 Secure Hub 가표시되도록설정합니다.

iOS

January 5, 2022

XenMobile Server 에서 iOS 장치를관리하려면 Apple 의 APNs(Apple 푸시알림서비스) 인증서를설정합니다. 자세한내용은 APN 인증서를참조하십시오.

등록프로필은사용자가 MDM 을취소할수있는옵션과함께 iOS 장치가 MDM+MAM 으로등록되는지여부를결정합니다. XenMobile Server 는 MDM+MAM 에서 iOS 장치에대해다음과같은인증유형을지원합니다. 자세한내용은 인증서및인증에 있는문서를참조하십시오.

- 도메인
- 도메인및보안토큰
- 클라이언트인증서
- 클라이언트인증서와도메인

> **iOS 13** 의신뢰할수있는인증서에대한요구사항:
>
> Apple 은 TLS 서버인증서에대한새로운요구사항을도입했습니다. 모든인증서가새로운 Apple 요구사항을따르는지확인하십시오. Apple 게시물 https://support.apple.com/en-us/HT210176를참조하십시오. 인증서관리에대한도움말은 XenMobile Server 에서인증서업로드를참조하십시오.

지원되는운영체제에대해서는 지원되는장치운영체제를참조하십시오.

iOS 14 호환기능

XenMobile Server 및 Citrix 모바일앱은 iOS 14 와호환되지만현재는새로운 iOS 14 기능을지원하지않습니다.

감독되는 iOS 기기의경우소프트웨어업그레이드를최대 90 일까지지연시킬수있습니다. iOS 에대한제한장치정책에서다음설정을사용합니다.

- 소프트웨어업데이트강제지연
- 소프트웨어업데이트시행지연

iOS 설정을참조하십시오. 사용자등록모드또는감독되지않은 (전체 MDM) 모드의장치에는이러한설정을사용할수없습니다.

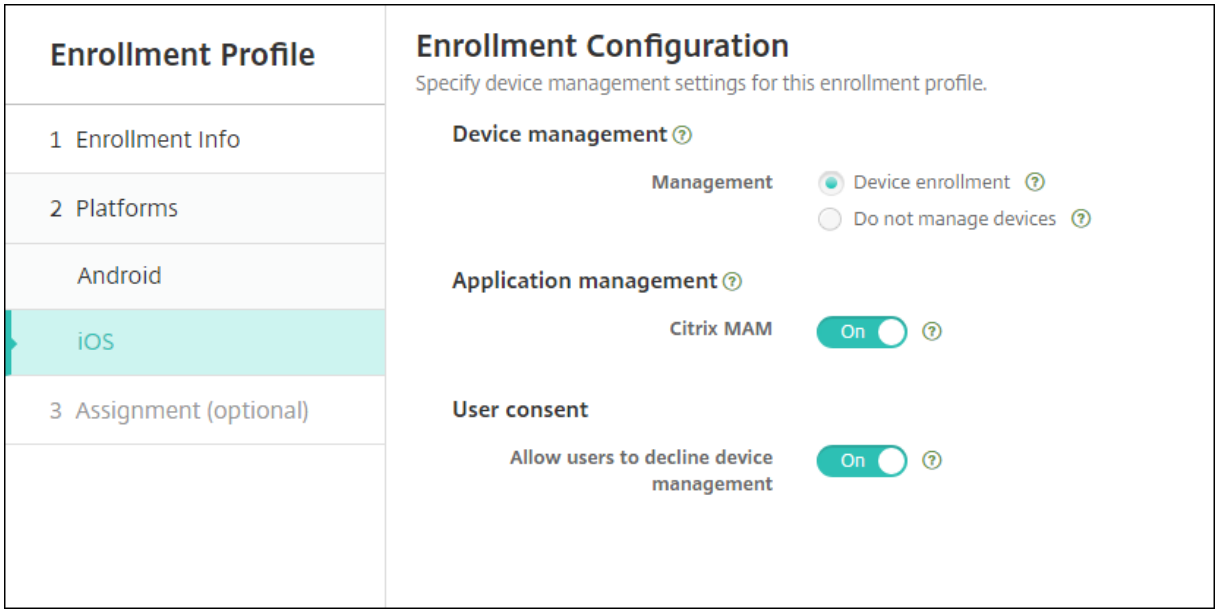
열린상태로유지되어야하는 **Apple** 호스트이름

일부 Apple 호스트이름은 iOS, macOS 및 Apple App Store 의올바른작동을보장하기위해열린상태로유지되어야합니다. 이러한호스트이름을차단하면 iOS, iOS 앱, MDM 작업, 장치및앱등록등의설치, 업데이트및적절한작동에영향을줄수있습니다. 자세한내용은 https://support.apple.com/en-us/HT201999 항목을참조하십시오.

지원되는등록방법

등록프로필의 iOS 장치관리방법을지정합니다. 장치등록또는 MDM 등록안함을선택할수있습니다.

iOS 장치의등록설정을구성하려면 구성 **>** 등록프로필 **> iOS** 로이동합니다.



다음표에는 XenMobile Server 가 iOS 장치에대해지원하는등록방법이나와있습니다.

방법	지원됨
Apple 배포프로그램	예
Apple School Manager	예
Apple Configurator	예
수동등록	예
등록초대	예

Apple 에는비즈니스및교육계정을위한장치등록프로그램이있습니다. 비즈니스계정의경우 XenMobile Server 에서 Apple 배포프로그램을사용하여장치를등록하고관리하려면 Apple 배포프로그램에등록해야합니다. 이프로그램은 iOS 및 macOS 장치를위한것입니다. Apple 배포프로그램을통한장치배포를참조하십시오.

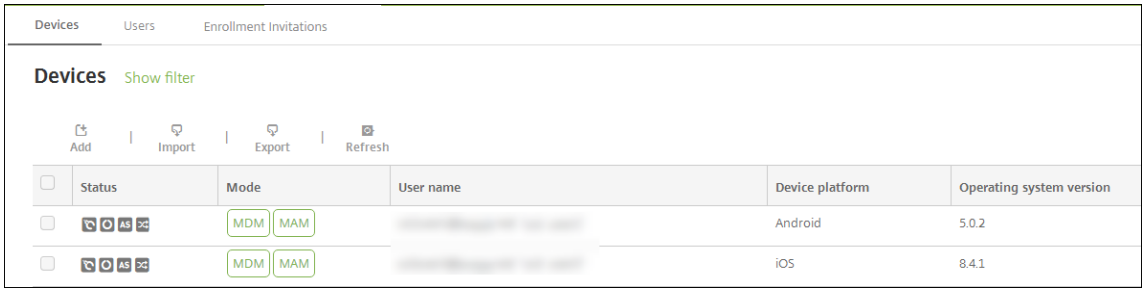
교육계정의경우 Apple School Manager 계정을생성합니다. Apple School Manager 는배포프로그램과볼륨구매를통합합니다. Apple School Manager 는교육용 Apple 배포프로그램의한유형입니다. Apple 교육기능과통합을참조하십시오.

Apple 배포프로그램을사용하여 iOS 및 macOS 장치를대량등록할수있습니다. 이러한장치는 Apple, 참여 Apple 공인리셀러또는이동통신사업자에서직접구입할수있습니다. iOS 장치를 Apple 에서직접구매하든구매하지않든 Apple Configurator 를사용하여이러한장치를등록할수있습니다. Apple 장치의대량등록을참조하십시오.

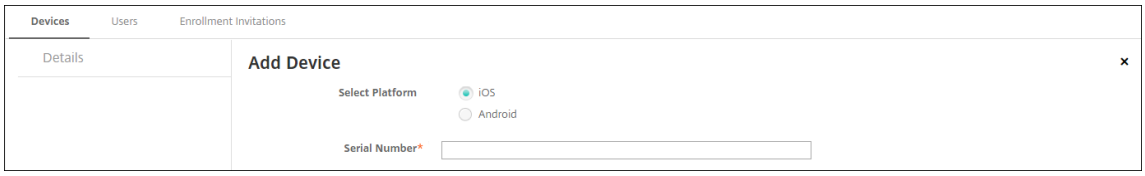
수동으로 **iOS** 장치추가

테스트목적등으로 iOS 장치를수동으로추가하려면다음단계를수행하십시오.

1. XenMobile Server 콘솔에서 관리 **>** 장치를클릭합니다. 장치페이지가나타납니다.



2. 추가를클릭합니다. 장치추가페이지가나타납니다.



3. 다음설정을구성합니다.

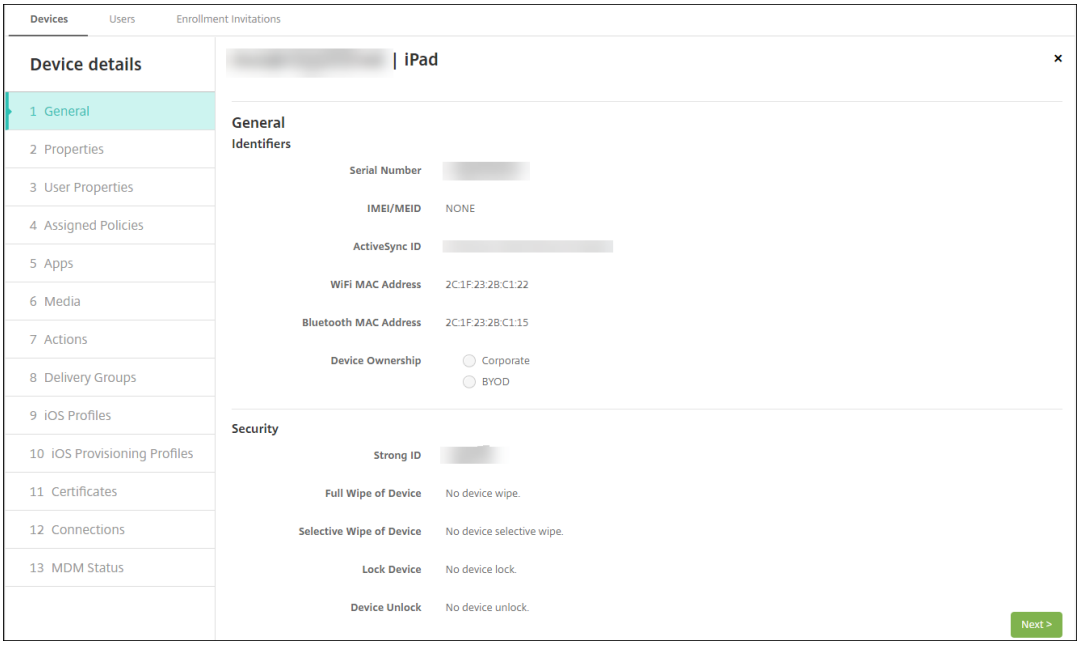
   - 플랫폼선택**: iOS** 를클릭합니다.
   - 일련번호**:** 장치일련번호를입력합니다.

4. 추가를클릭합니다. 장치테이블이나타나고목록맨아래에장치가추가되어있습니다. 장치세부정보를보고확인하려면: 추가한장치를선택한다음나타나는메뉴에서 편집을클릭합니다.

   > 참고**:**
   >
   > 장치옆에있는확인란을선택하면장치목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.

   - 구성된 LDAP
   - 로컬그룹및로컬사용자를사용중인경우:
     - 하나이상의로컬그룹.
     - 로컬그룹에할당된로컬사용자.
     - 배달그룹은로컬그룹과연결됩니다.

- Active Directory 를사용중인경우:
  - 배달그룹은 Active Directory 그룹과연결됩니다.



5. 일반페이지에는일련번호및플랫폼유형에대한기타정보같은장치 식별자가나열됩니다. 장치소유권의경우 회사또는 **BYOD** 를선택합니다.

   일반페이지에는강력한 ID, 장치잠금, 활성화잠금바이패스및플랫폼유형에대한기타정보같은장치 보안속성도나열됩니다. 장치전체초기화필드에는사용자 PIN 코드가포함됩니다. 장치가초기화된후사용자는이코드를입력해야합니다. 사용자가 코드를잊은경우여기서코드를조회할수있습니다.

6. 속성페이지에는 XenMobile Server 가프로비전할장치속성이나열됩니다. 이목록에는장치를추가하는데사용된프로비저닝파일에포함된모든장치속성이표시됩니다. 속성을추가하려면 추가를클릭한다음목록에서속성을선택합니다. 각속성에유효한값에대해서는 장치속성이름및값 PDF 를참조하십시오.

   속성을추가하면처음에는속성을추가한범주아래에나타납니다. 다음을클릭한후 속성페이지로돌아가면속성이해당목록에 나타납니다.

   속성을삭제하려면목록위에마우스포인터를이동하고오른쪽에있는 **X** 를클릭합니다. XenMobile Server 에서항목이즉시삭제됩니다.

7. 나머지 장치세부정보섹션에는장치에대한요약정보가포함되어있습니다.

   - 사용자속성**:** RBAC 역할, 그룹구성원자격, 볼륨구매계정및사용자속성을표시합니다. 이페이지에서볼륨구매계정을사용중지할수있습니다.
   - 할당된정책**:** 배포된정책, 보류중인정책및실패한정책의수를포함하여할당된정책의수를표시합니다. 각정책에대해 정책이름, 유형및마지막배포정보를제공합니다.
   - 앱**:** 마지막인벤토리에대한설치된앱배포, 보류중인앱배포및실패한앱배포의수를표시합니다. 앱이름, 식별자, 유형 및기타정보를제공합니다. iOS 및 macOS 인벤토리키 (예: **HasUpdateAvailable**) 에대한설명은 모바일기기관리 (MDM) 프로토콜을참조하십시오.

- 미디어**:** 마지막인벤토리에대해배포된미디어배포, 보류중인미디어배포및실패한미디어배포의수를표시합니다.
- 동작**:** 배포된동작, 보류중인동작및실패한동작의수를표시합니다. 마지막배포의동작이름및시간을제공합니다.
- 배달그룹**:** 성공한배달그룹, 보류중인배달그룹및실패한배달그룹의수를표시합니다. 각배포에대해배달그룹이름및배포시간을제공합니다. 배달그룹을선택하여상태, 동작및채널또는사용자를비롯한자세한정보를확인합니다.
- **iOS** 프로필**:** 이름, 유형, 조직및설명을비롯한마지막 iOS 프로필인벤토리를표시합니다.
- **iOS** 프로비전프로필**:** UUID, 만료날짜및관리상태와같은엔터프라이즈배포프로비전프로필정보를표시합니다.
- 인증서**:** 유효하거나, 만료되거나, 해지된인증서에대해유형, 공급자, 발급자, 일련번호및만료전까지남은날짜와같은정보를표시합니다.
- 연결**:** 첫번째연결상태및마지막연결상태를표시합니다. 각연결에대해사용자이름, 마지막두번째 (끝에서두번째) 인증시간및마지막인증시간을제공합니다.
- **MDM** 상태**:** MDM 상태, 마지막푸시시간및마지막장치회신시간같은정보를표시합니다.

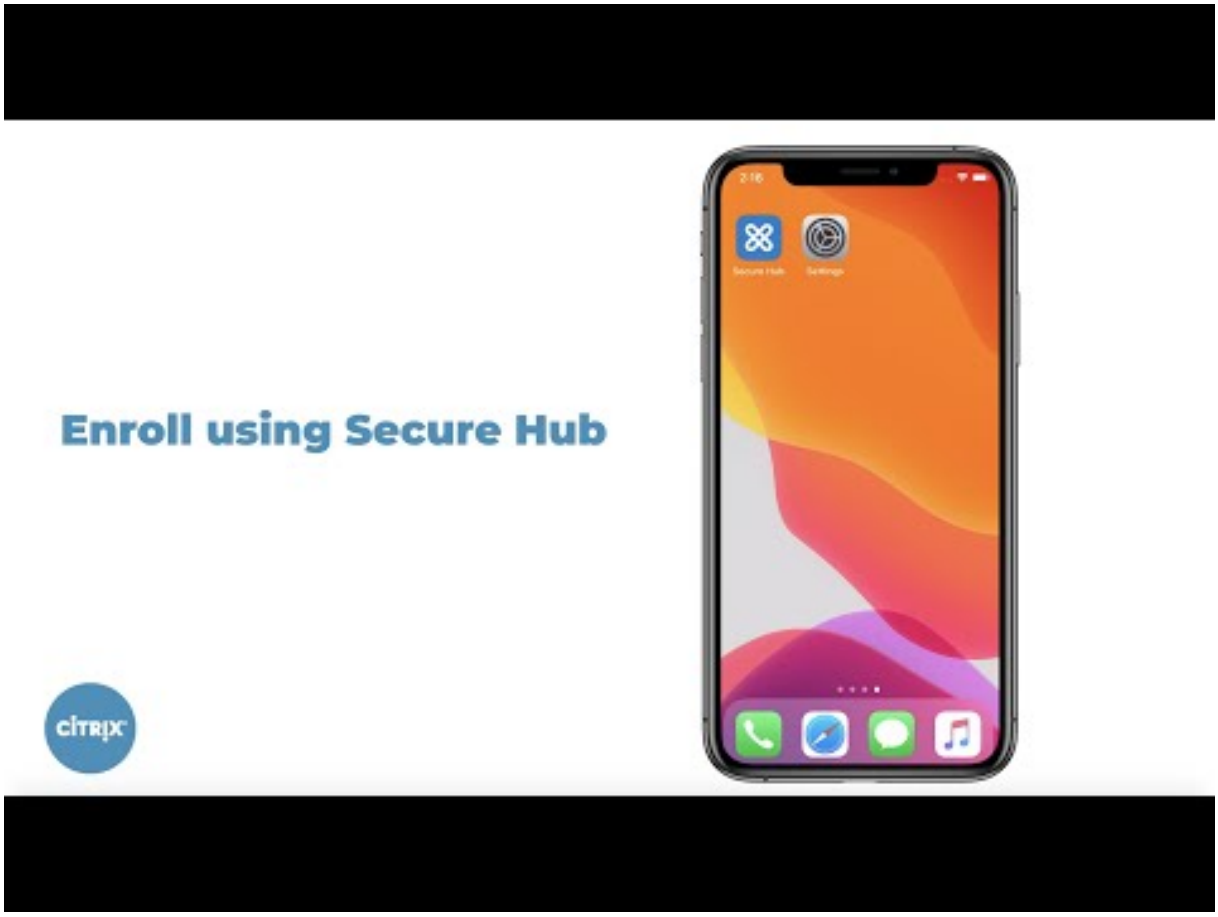
iOS 장치정책구성

이러한정책을사용하여 XenMobile Server 가 iOS 를실행하는장치와상호작용하는방식을구성할수있습니다. 다음표에는 iOS 장치에사용할수있는모든장치정책이나열되어있습니다.

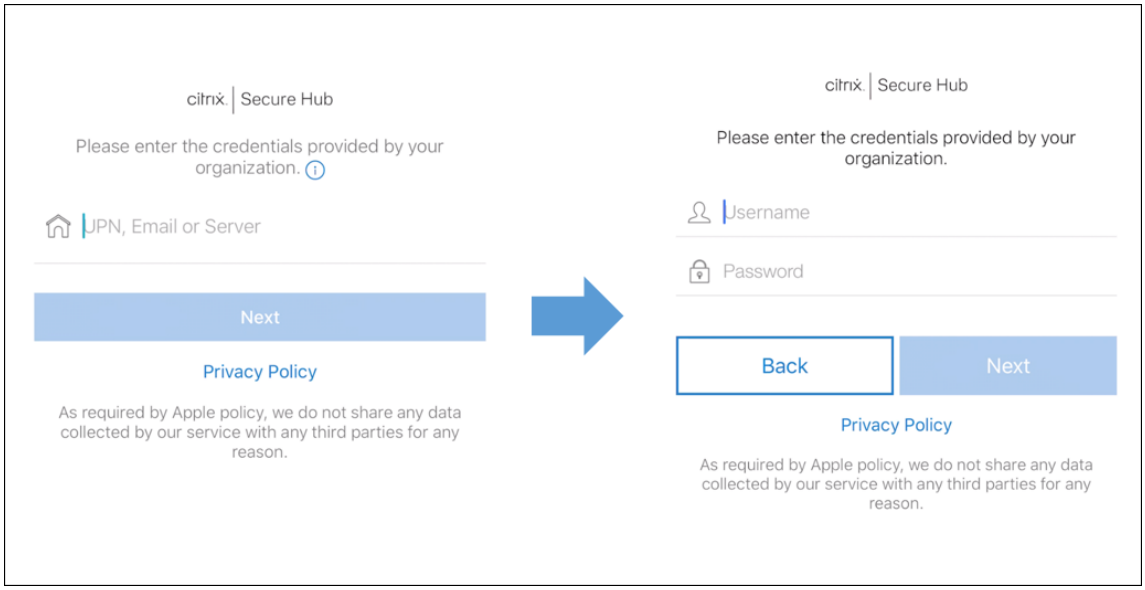
AirPlay 미러링	AirPrint	APN
앱액세스	앱특성	앱구성
앱인벤토리	앱잠금	앱네트워크사용
앱제거	앱알림	일정 (CalDAV)
셀룰러	연락처 (CardDAV)	OS 업데이트제어
자격증명	장치이름	교육구성
Exchange	글꼴	홈화면레이아웃
iOS 및 macOS 프로필가져오기	LDAP	위치
메일	관리되는도메인	MDM 옵션
조직정보	암호	개인핫스폿
프로필제거	프로비전프로필	프로비전프로필제거
프록시	제한사항	로밍
SCEP	공유 iPad - 최대상주사용자수	공유 iPad - 암호잠금유예기간
SSO 계정	스토어	구독중인일정
약관	VPN	배경화면
웹콘텐츠필터	웹클립	WiFi

iOS 장치등록

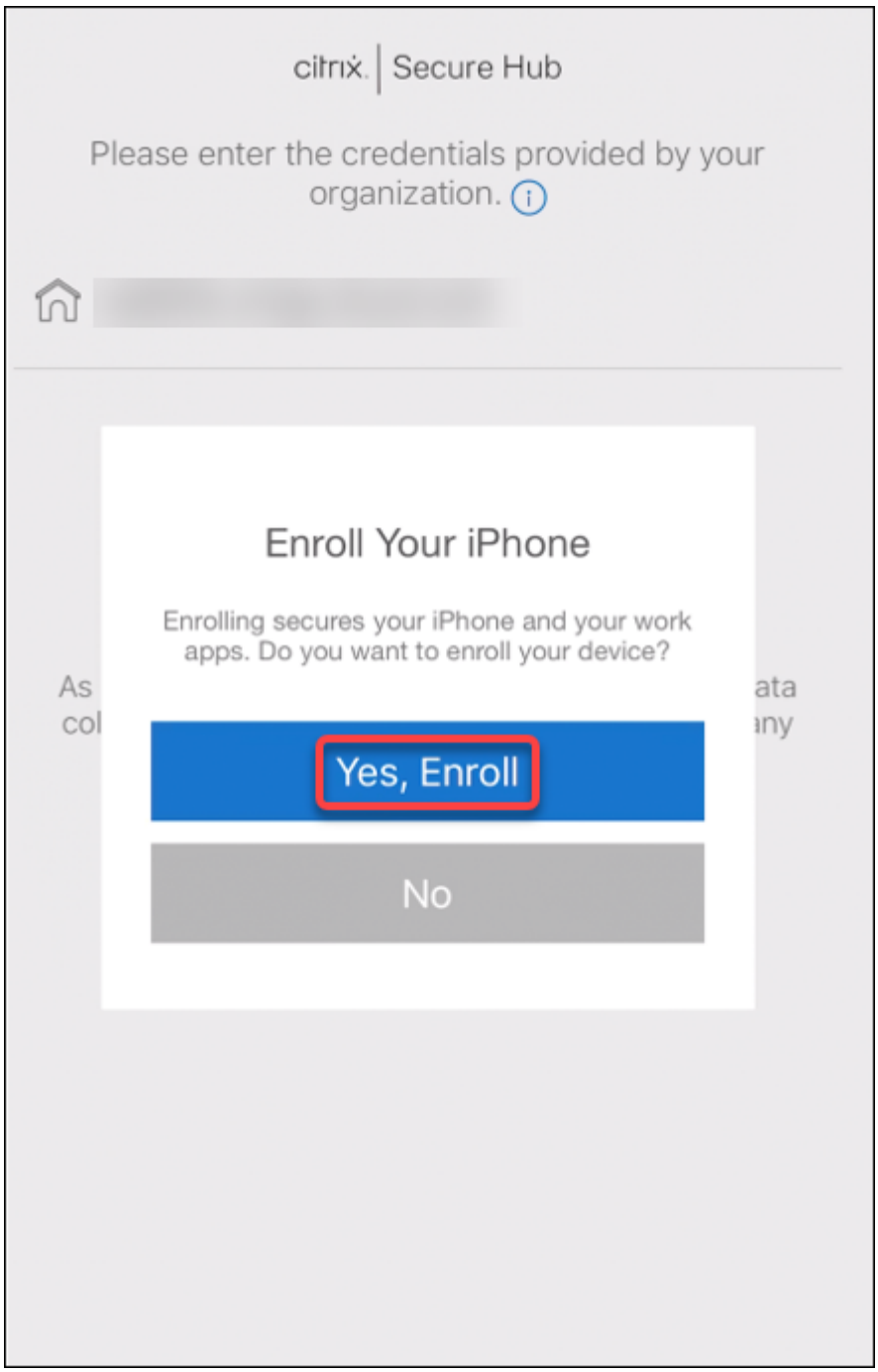
이섹션에서는사용자가 iOS 장치 (12.2 이상) 를 XenMobile Server 에등록하는방법을보여줍니다. iOS 등록에대한자세한내용을보려면다음비디오를여십시오.



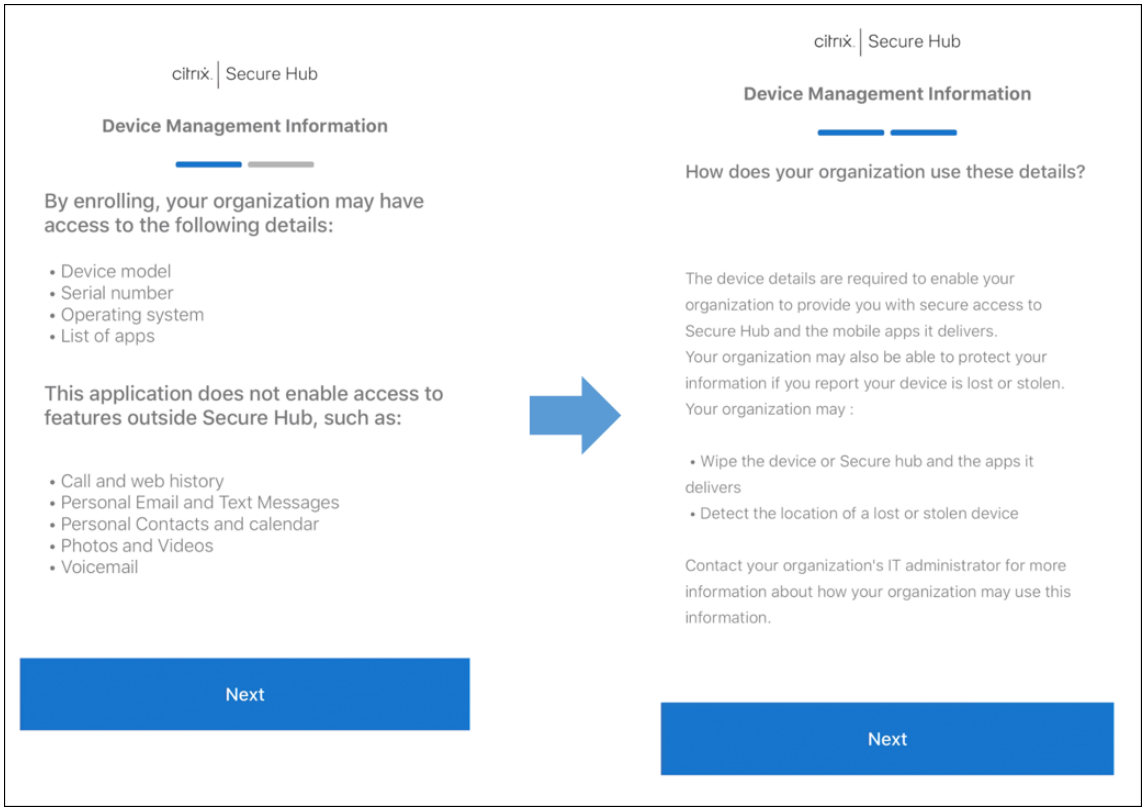
1. iOS 장치의 Apple Store 로이동하여 Citrix Secure Hub 앱을다운로드한후이앱을누릅니다.
2. 앱을설치하라는메시지가표시되면 다음을누른후 설치를누릅니다.
3. Secure Hub 가설치된후에 **Open(**열기**)** 을누릅니다.
4. XenMobile Server 서버이름, UPN(사용자계정이름) 또는전자메일주소와같은회사자격증명을입력합니다. 그리고 **Next(**다음**)** 를클릭합니다.



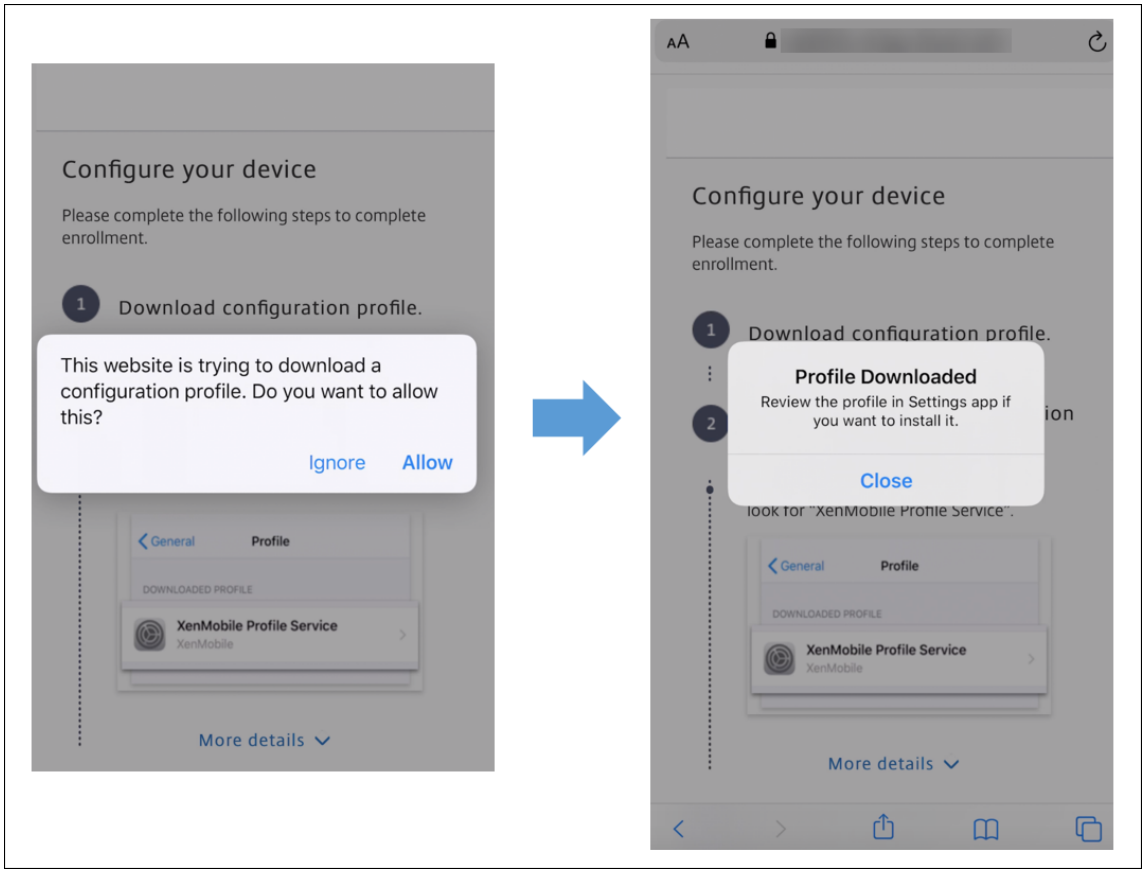
5. 예, 등록을눌러 iOS 장치를등록합니다.



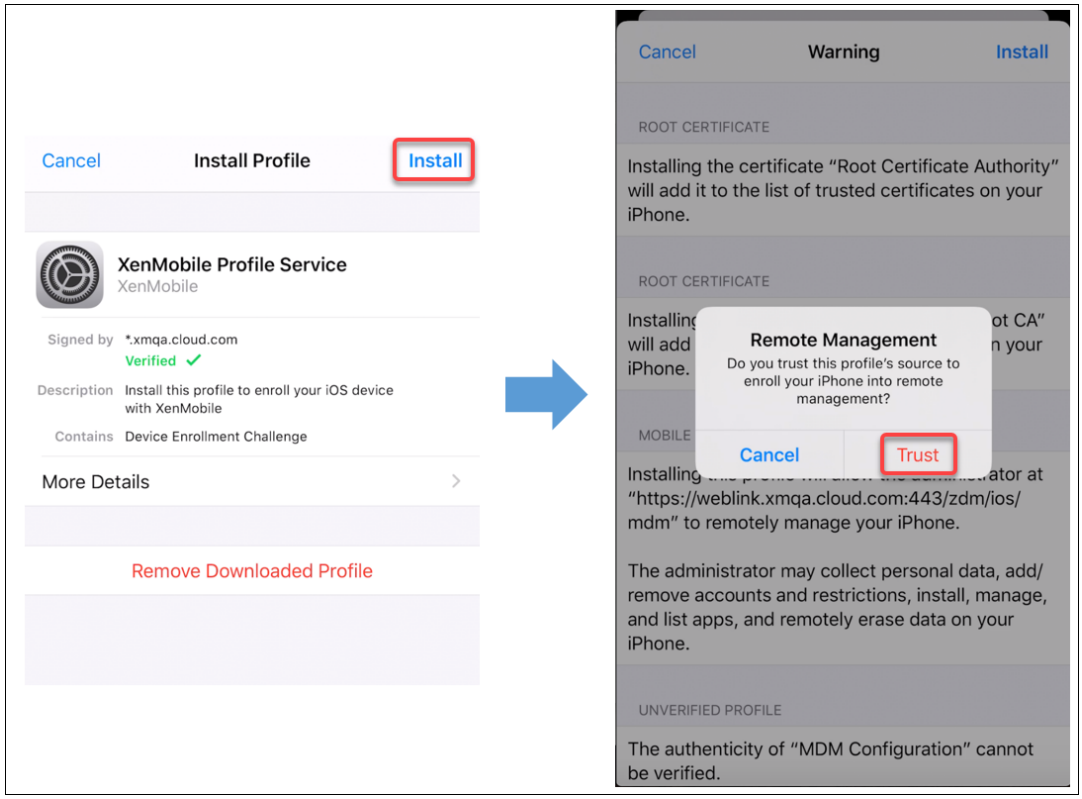
6. XenMobile Server 가수집하는데이터목록이나타납니다. 다음을클릭합니다. 조직에서해당데이터를사용하는방법에 대한설명이표시됩니다. 다음을클릭합니다.



7. 자격증명을입력한후메시지가표시되면 허용을눌러구성프로필을다운로드합니다. 구성프로필을다운로드한후 닫기를누릅니다.



8. 장치설정에서 iOS 인증서를설치하고장치를신뢰할수있는목록에추가합니다.
   - 설정 **>** 일반 **>** 프로필 **> XenMobile** 프로필서비스로이동하고 설치를눌러프로필을추가합니다.
   - 알림창에서 신뢰를눌러장치를원격관리에등록합니다.



9. 등록이성공하면 Secure Hub 를엽니다. MDM+MAM 에등록하는경우: 자격증명의유효성이확인된후메시지가표시되면 Citrix PIN 을만들고확인합니다.
10. 워크플로가완료되면장치가등록됩니다. 이제 App Store 에액세스하여 iOS 장치에설치할수있는앱을볼수있습니다.

보안동작

iOS 는다음과같은보안동작을지원합니다. 각보안동작에대한설명은 보안동작을참조하십시오.

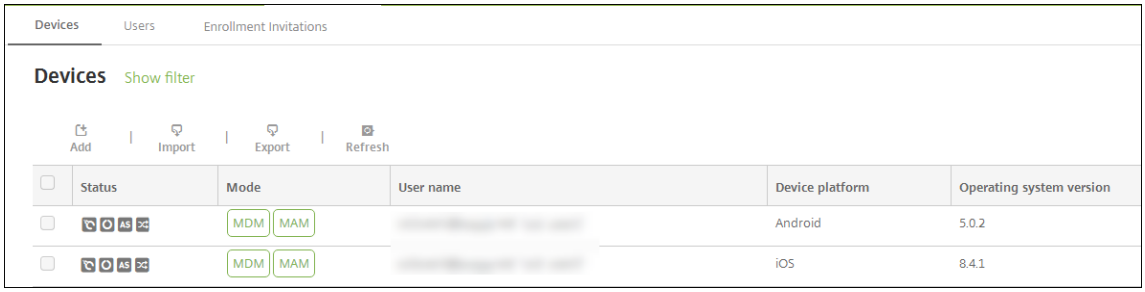
활성화잠금바이패스	앱잠금	앱초기화
ASM 활성화잠금	인증서갱신	제한사항지우기
분실모드활성화/비활성화	추적활성화/비활성화	전체초기화
찾기	잠금	벨울림
AirPlay 미러링요청/중지	다시시작/종료	Revoke/Authorize(해지/권한부여)
선택적초기화	잠금해제	

iOS 장치잠금

분실된 iOS 장치를잠그고장치잠금화면에메시지와전화번호를표시할수있습니다.

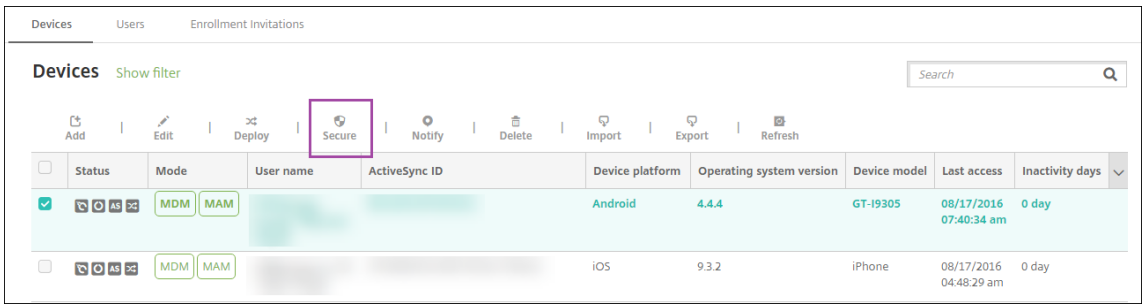
잠겨있는장치에메시지와전화번호를표시하려면 XenMobile Server 콘솔에서 암호 정책을 **true** 로설정합니다. 또는사용자가수동으로장치에서암호를사용하도록설정할수있습니다.

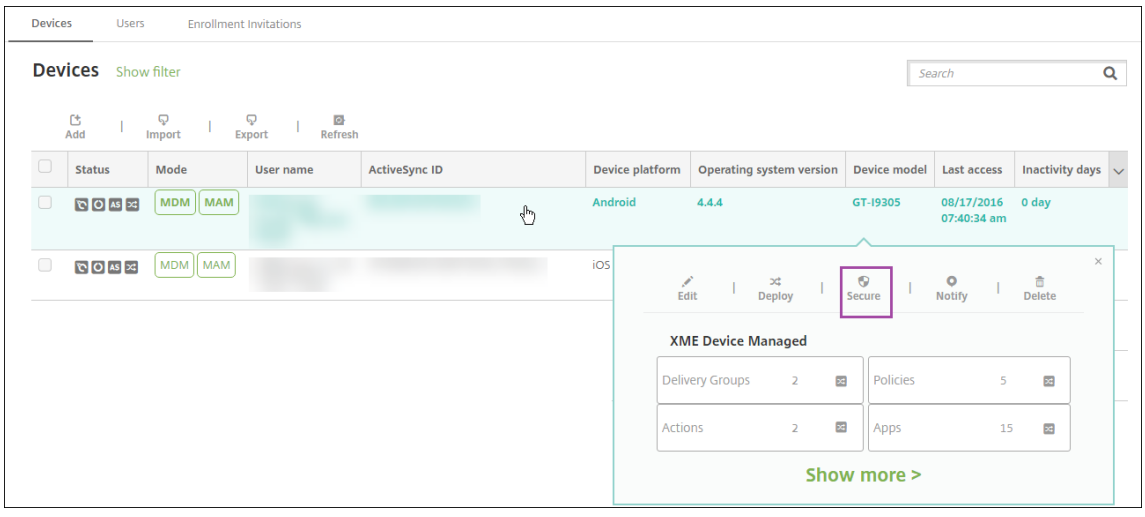
1. 관리 **>** 장치를클릭합니다. 장치페이지가나타납니다.



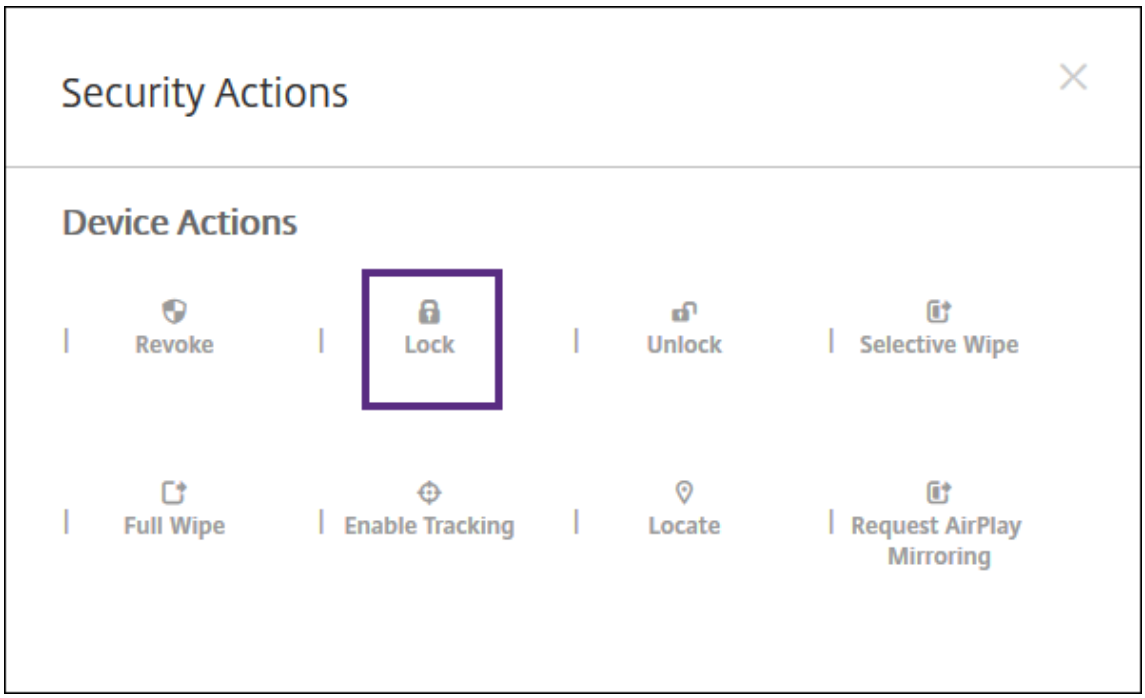
2. 잠글 iOS 장치를선택합니다.

   장치옆에있는확인란을선택하여장치목록위의옵션메뉴를표시합니다. 목록에서아무위치를클릭하여목록오른쪽의옵션메뉴를표시합니다.

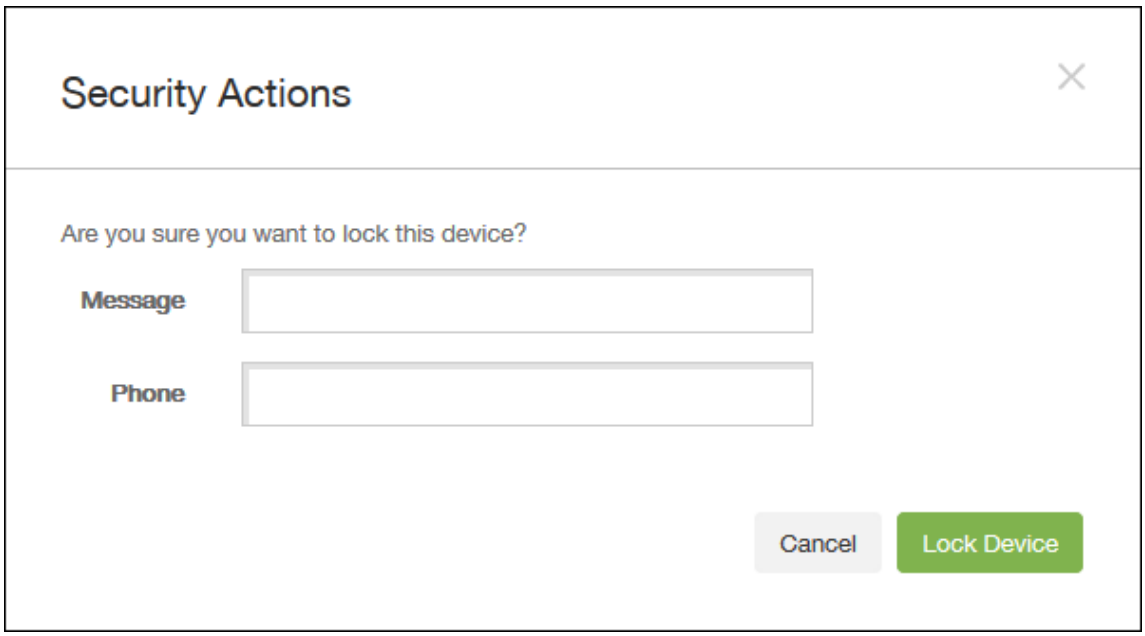




3. 옵션메뉴에서 보안을클릭합니다. 보안동작대화상자가나타납니다.



4. 잠금을클릭합니다. 보안동작확인대화상자가표시됩니다.



5. 필요에따라장치잠금화면에표시되는메시지와전화번호를입력합니다.

   메시지필드에입력하는내용에 “iPad 분실” 이라는단어가추가됩니다.

   메시지필드를비워두고전화번호를입력할경우장치잠금화면에 “소유자에게통화” 라는메시지가표시됩니다.

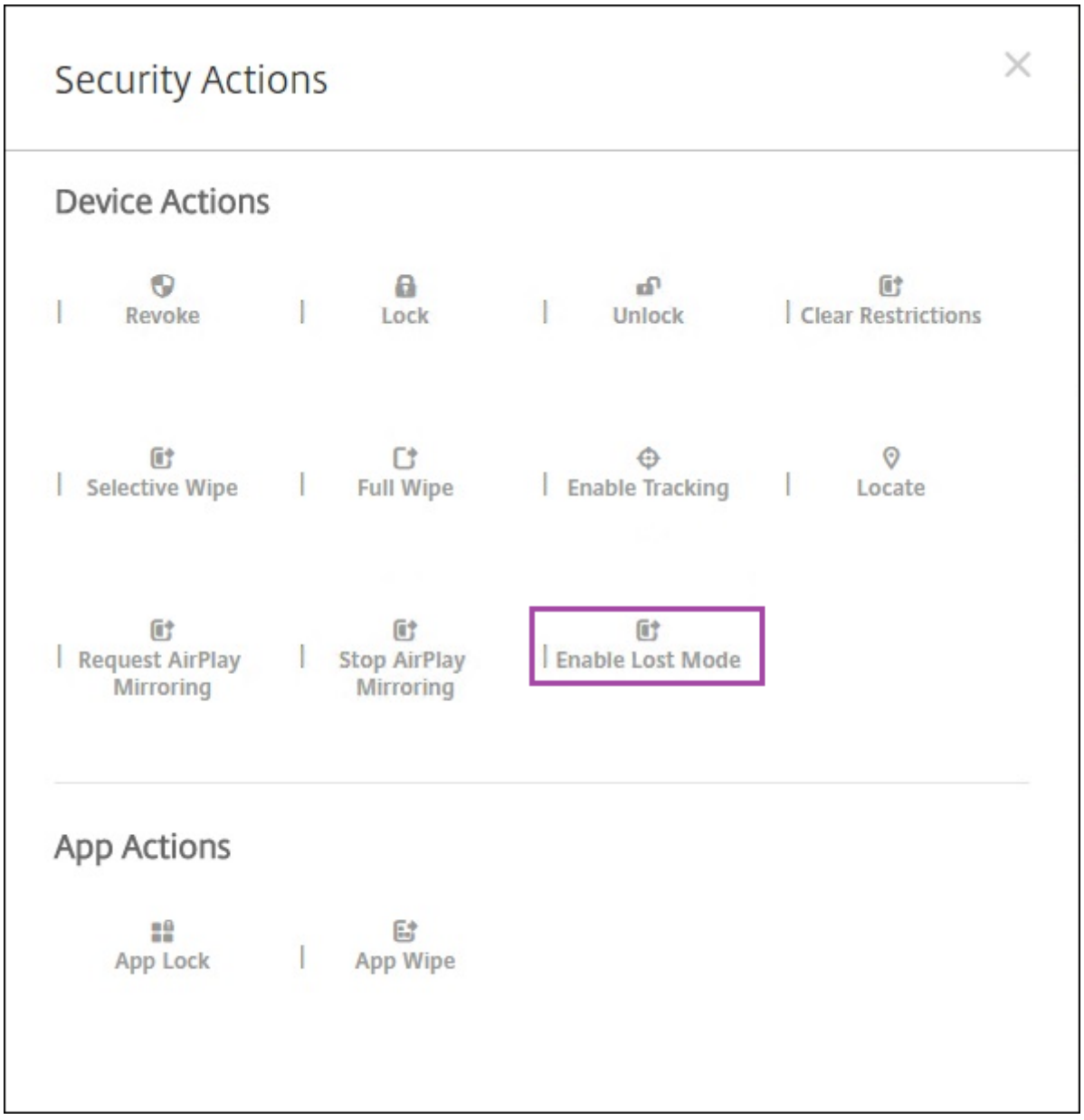
6. 장치잠금을클릭합니다.

iOS 장치를분실모드로전환

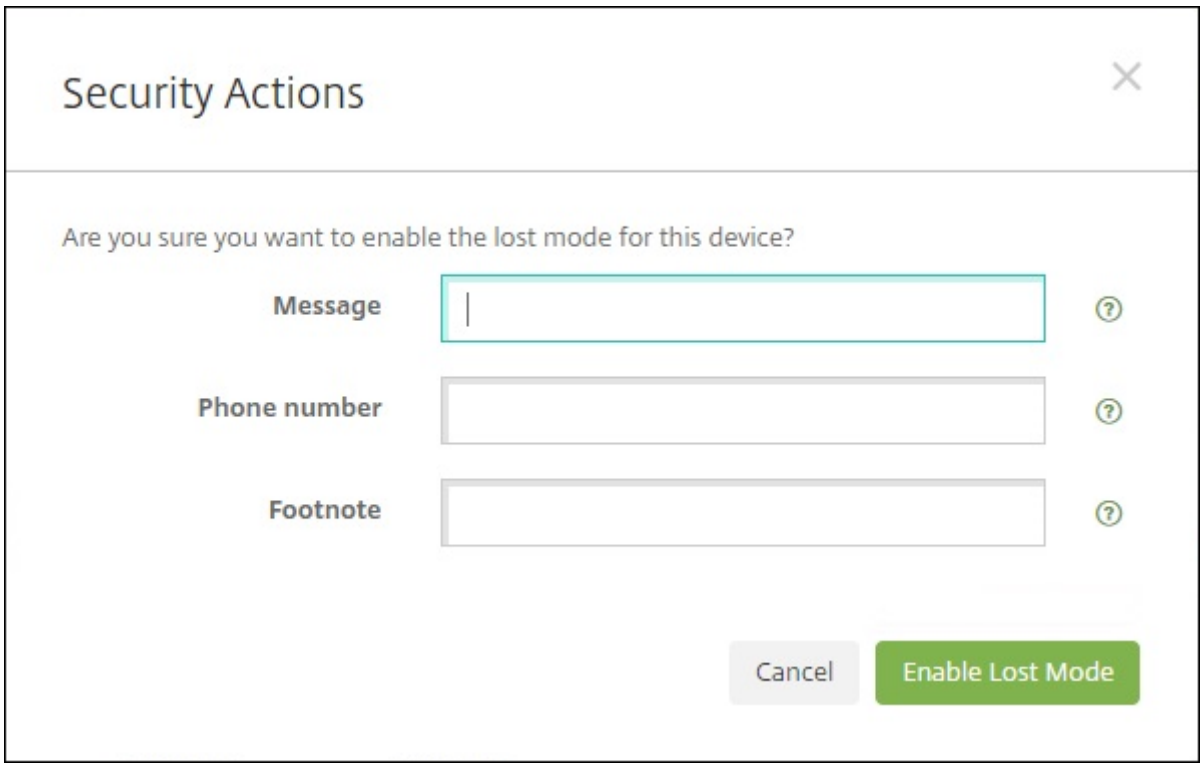
XenMobile Server 분실모드장치속성은 iOS 장치를분실모드로전환합니다. Apple 의관리되는분실모드와달리 XenMobile Server 의분실모드에서는다음동작중하나를수행하여사용자가 나의 **iPhone/iPad** 찾기설정을구성하거나 Citrix Secure Hub 의위치서비스를사용하지않아도장치위치를찾을수있습니다.

XenMobile Server 분실모드에서는 XenMobile Server 만장치잠금을해제할수있습니다. 이와반대로 XenMobile Server 장치잠금기능을사용하는경우에는사용자가제공된 PIN 코드를사용하여장치를직접잠금해제할수있습니다.

분실모드를사용하거나사용하지않으려면: 관리 **>** 장치로이동하고감독되는 iOS 장치를선택한후 보안을클릭합니다. 분실모드활성화또는 분실모드비활성화를클릭합니다.

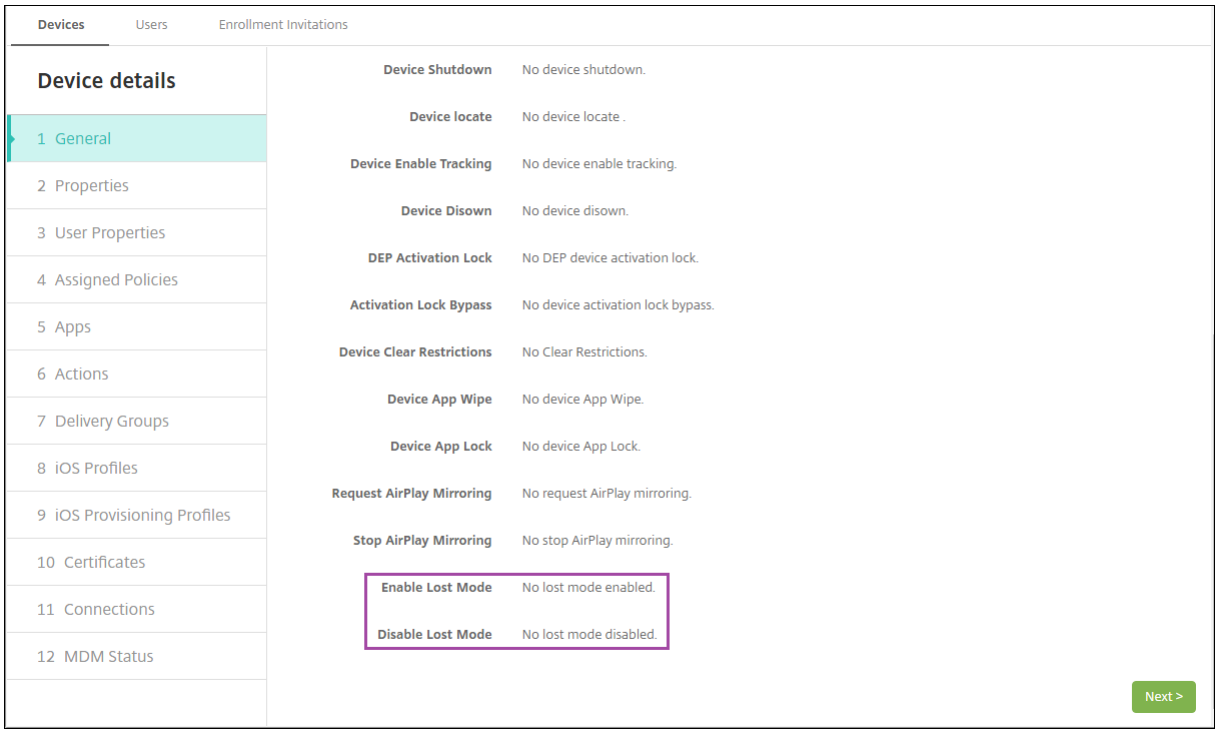


분실모드활성화를클릭하고장치가분실모드가될때장치에표시할정보를입력합니다.

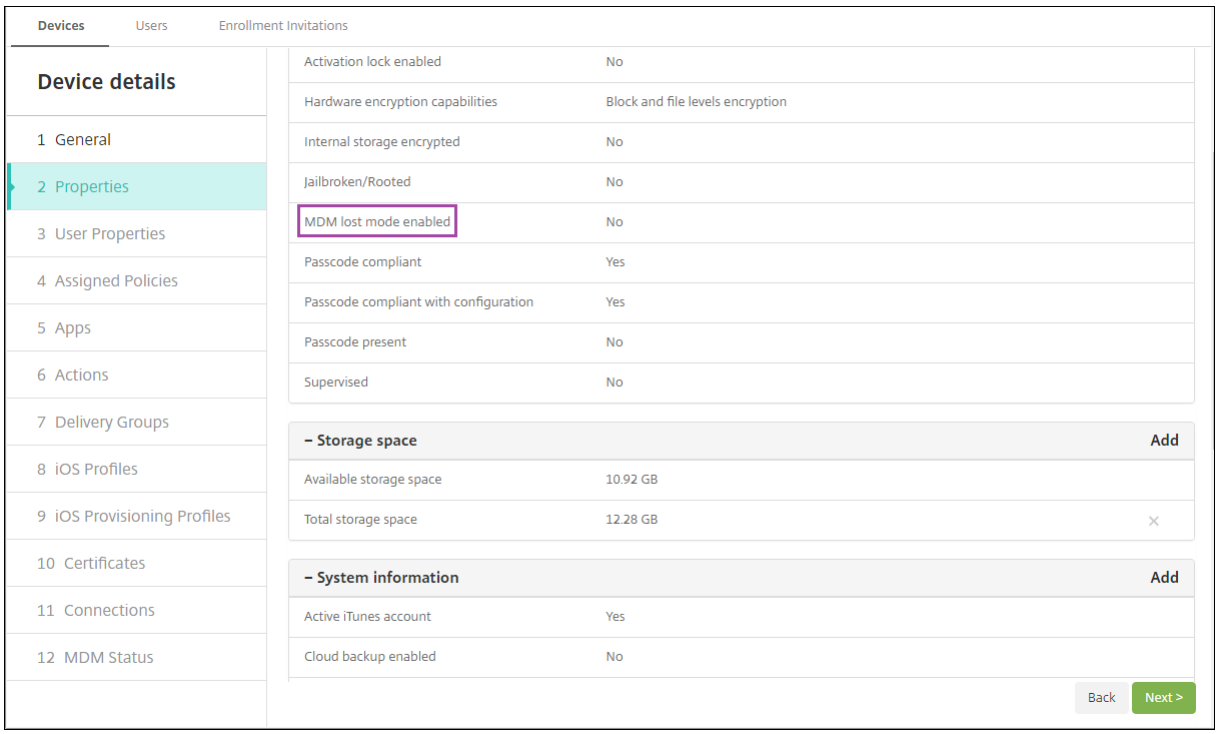


다음방법중하나를사용하여분실모드상태를확인합니다.

- 보안동작창에서단추가 분실모드비활성화인지확인합니다.
- 관리 **>** 장치에서 일반탭의 보안아래에서마지막분실모드활성화또는분실모드비활성화동작을확인합니다.



- 관리 **>** 장치의 속성탭에서 **MDM** 분실모드활성화설정의값이올바른지확인합니다.



iOS 장치에서 XenMobile Server 분실모드를사용하는경우 XenMobile Server 콘솔이다음과같이변경됩니다.

- 구성 **>** 동작에서 동작목록에 장치해지, 장치를선택적으로초기화및 장치를완전히초기화자동화동작이포함되지않습니다.
- 관리 **>** 장치에서 보안동작목록에 해지및 장치선택적초기화동작이더이상포함되지않습니다. 필요한경우보안동작을사용하여 전체초기화를수행할수있습니다.

보안동작화면의 메시지에무엇을입력하든지관계없이끝에 “iPad 분실” 이라는단어가추가됩니다.

메시지를비워두고전화번호를입력할경우장치잠금화면에 “소유자에게통화” 라는메시지가표시됩니다.

iOS 활성화잠금바이패스

활성화잠금은분실되거나도난당한장치의재활성화를방지하는내 iPhone/iPad 찾기기능입니다. 활성화잠금은누군가가내 iPhone/iPad 찾기를끄고장치를지우거나장치를재활성화하여사용하려고할경우사용자의 Apple ID 와암호를요구합니다. 조직이소유한장치의경우예를들어장치를재설정하거나재할당하기위해활성화잠금을바이패스해야합니다.

활성화잠금을사용하도록설정하려면 XenMobile Server MDM 옵션장치정책을구성하고배포합니다. 그러면사용자의 Apple 자격증명이없이도 XenMobile Server 콘솔에서장치를관리할수있습니다. 활성화잠금의 Apple 자격증명요구사항을바이패스하려면 XenMobile Server 콘솔에서활성화잠금바이패스보안동작을실행합니다.

예를들어사용자가분실된휴대폰을반환하거나전체초기화전후에장치를설정하는경우 Apple App Store 계정자격증명을묻는메시지가표시될때 XenMobile Server 콘솔에서활성화잠금바이패스보안동작을실행하여이단계를바이패스할수있습니다.

활성화잠금바이패스를위한장치요구사항

- Apple Configurator 또는 Apple 배포프로그램을통해감독됨

- iCloud 계정을사용하여구성됨
- 내 iPhone/iPad 찾기를사용하도록설정됨
- XenMobile Server 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.

- 사용자에게내 iPhone/iPad 찾기를끄지말라고일러두십시오. 장치에서전체초기화를수행하지마십시오. 두경우모두사용자에게 iCloud 계정암호를입력하라는메시지가표시됩니다. 계정유효성검사후모든콘텐츠와설정을지운다음사용자에게 iPhone/iPad 활성화화면이표시되지않습니다.
- 활성화잠금바이패스코드가생성되고활성화잠금을사용하도록설정한장치의경우전체초기화후 iPhone/iPad 활성화페이지를바이패스할수없으면 XenMobile Server 에서장치를삭제할필요가없습니다. 관리자또는사용자가 Apple 지원팀에연락하여직접장치의차단을해제할수있습니다.
- 하드웨어인벤토리중에 XenMobile Server 는장치에서활성화잠금바이패스코드를쿼리합니다. 바이패스코드를사용할수있는경우장치가해당코드를 XenMobile Server 에전송합니다. 그런다음장치에서바이패스코드를제거하려면 XenMobile Server 콘솔에서활성화잠금바이패스보안동작을전송합니다. 이때장치의차단을해제하려면 XenMobile Server 와 Apple 에바이패스코드가있어야합니다.
- 활성화잠금바이패스보안동작은 Apple 서비스의이용가용성에따라달라집니다. 이동작이작동하지않는경우다음과같이장치의차단을해제할수있습니다. 장치에서수동으로 iCloud 계정의자격증명을입력합니다. 또는사용자이름필드를비워두고암호필드에바이패스코드를입력합니다. 바이패스코드를조회하려면 관리 **>** 장치로이동하여장치를선택하고 편집, 속성을차례로클릭합니다. 활성화잠금바이패스코드는 보안정보아래에있습니다.

macOS

January 5, 2022

XenMobile 에서 macOS 장치를관리하려면 Apple 의 APNs(Apple 푸시알림서비스) 인증서를설정합니다. 자세한내용은 APN 인증서를참조하십시오.

XenMobile 이 macOS 장치를 MDM 으로등록합니다. XenMobile 은 MDM 에서 macOS 장치에대해다음과같은등록유형을지원합니다.

- 도메인

- 도메인과일회용암호
- 초대 URL 과일회용암호

> **macOS 15** 의신뢰할수있는인증서요구사항**:**
>
> Apple 은 TLS 서버인증서에대한새로운요구사항을도입했습니다. 모든인증서가새로운 Apple 요구사항을따르는지확인하십시오. Apple 게시물 https://support.apple.com/en-us/HT210176를참조하십시오. 인증서관리에대한도움말은 XenMobile 에서인증서업로드를참조하십시오.

macOS 장치관리를시작하는일반적인워크플로는다음과같습니다.

1. macOS 장치정책관리.
2. macOS 장치등록.
3. 장치및앱보안작업을설정합니다. 보안동작을참조하십시오.

지원되는운영체제에대해서는 지원되는장치운영체제를참조하십시오.

열린상태로유지되어야하는 **Apple** 호스트이름

일부 Apple 호스트이름은 iOS, macOS 및 Apple App Store 의올바른작동을보장하기위해열린상태로유지되어야합니다. 이러한호스트이름을차단하면 iOS, iOS 앱, MDM 작업, 장치및앱등록등의설치, 업데이트및적절한작동에영향을줄수있습니다. 자세한내용은 https://support.apple.com/en-us/HT201999 항목을참조하십시오.

지원되는등록방법

다음표에는 XenMobile 에서 macOS 장치에지원하는등록방법이나와있습니다.

방법	지원됨
Apple 배포프로그램	예
Apple School Manager	예
Apple Configurator	아니요
수동등록	예
등록초대	예

Apple 에는비즈니스및교육계정을위한장치등록프로그램이있습니다. 비즈니스계정의경우 XenMobile 에서 Apple 배포프로그램을사용하여장치를등록하고관리하려면 Apple 배포프로그램에등록해야합니다. 이프로그램은 iOS 및 macOS 장치를위한것입니다. Apple 배포프로그램을통한장치배포를참조하십시오.

교육계정의경우 Apple School Manager 계정을생성합니다. Apple School Manager 는배포프로그램과볼륨구매를통합합니다. Apple School Manager 는교육용 Apple 배포프로그램의한유형입니다. Apple 교육기능과통합을참조하십시오.

Apple 배포프로그램을사용하여 iOS 및 macOS 장치를대량등록할수있습니다. 이러한장치는 Apple, 참여 Apple 공인리셀러또는이동통신사업자에서직접구입할수있습니다.

macOS 장치정책관리

이러한정책을사용하여 XenMobile 이 macOS 를실행하는장치와상호작용하는방식을구성할수있습니다. 다음표에는 macOS 장치에사용할수있는모든장치정책이나열되어있습니다.

AirPlay 미러링	앱인벤토리	일정 (CalDAV)
연락처 (CardDAV)	OS 업데이트제어	자격증명
장치이름	Exchange	FileVault
방화벽	글꼴	iOS 및 macOS 프로필가져오기
LDAP	메일	암호
프로필제거	제한사항	SCEP
VPN	웹클립	Wi-Fi

macOS 장치등록

XenMobile 에서는 macOS 를실행하는장치를등록하는두가지방법을제공합니다. 두방법모두 macOS 사용자가장치에서직접온라인으로등록할수있습니다.

- 사용자에게등록초대보내기**:** 이등록방법을이용하면 macOS 장치에대해다음등록모드를설정할수있습니다.
  - 사용자이름 + 암호
  - 사용자이름 + PIN
  - 2 단계인증

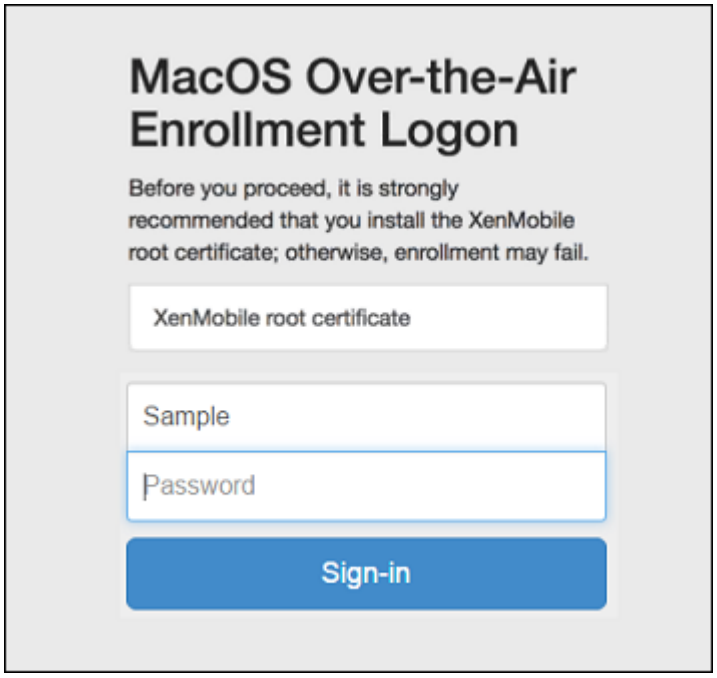
  사용자가등록초대의지침을따르면사용자이름이입력된로그온화면이표시됩니다.
- 사용자에게등록링크보내기**:** macOS 장치를등록하는이방법은사용자에게등록링크를보냅니다. 사용자는이링크를 Safari 또는 Chrome 브라우저에서열수있습니다. 그런다음사용자이름과암호를제공하여등록합니다.

  서버속성인 **Enable macOS OTAE** 를 **false** 로설정하여 macOS 장치에대한등록링크를사용하지못하도록할수있습니다. 이렇게하면 macOS 사용자가등록초대만사용하여등록할수있습니다.

macOS 사용자에게등록초대보내기

1. macOS 사용자등록을위한초대를추가합니다. 등록초대만들기를참조하십시오.

2. 사용자가초대를수신하고링크를클릭하면다음화면이 Safari 브라우저에표시됩니다. XenMobile 이사용자이름을채웁니다. 등록보안모드를 **2** 단계로선택한경우다른필드가나타납니다.



3. 사용자는필요에따라인증서를설치합니다. 사용자에게인증서를설치할것인지묻는메시지가표시되는지여부는 macOS 에대해공개적으로신뢰할수있는 SSL 인증서와공개적으로신뢰할수있는디지털서명인증서를구성했는지여부에따라달라집니다. 인증서에대한자세한내용은 인증서및인증을참조하십시오.

4. 사용자가요청된자격증명을제공합니다.

   Mac 장치정책이설치됩니다. 이제모바일장치를관리하듯이 XenMobile 로 macOS 장치를관리할수있습니다.

macOS 사용자에게설치링크보내기

1. 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.

   설치링크를전송하는방법에대한자세한내용은 등록초대보내기를참조하십시오.

2. 사용자는필요에따라인증서를설치합니다. iOS 와 macOS 에대해공개적으로신뢰할수있는 SSL 인증서및디지털서명인증서를구성한경우사용자에게인증서를설치하라는메시지가표시됩니다. 인증서에대한자세한내용은 인증서및인증을참조하십시오.

3. 사용자가자신의 Mac 에로그온합니다.

   Mac 장치정책이설치됩니다. 이제모바일장치를관리하듯이 XenMobile 로 macOS 장치를관리할수있습니다.

보안동작

macOS 는다음과같은보안동작을지원합니다. 각보안동작에대한설명은 보안동작을참조하십시오.

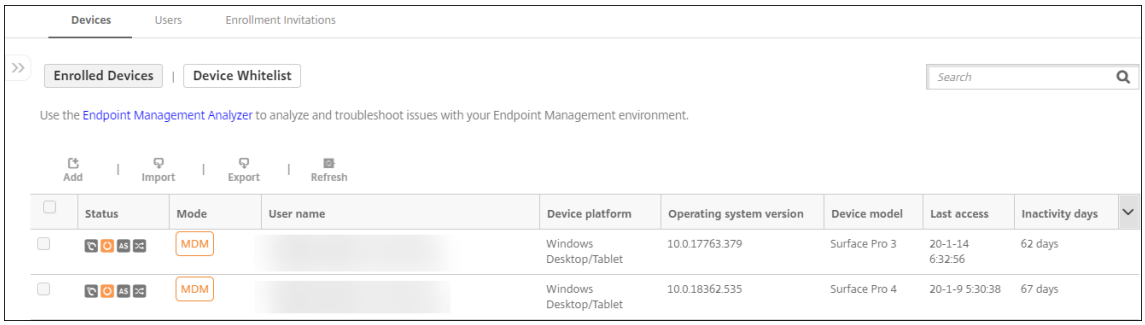
해지	잠금	선택적초기화
전체초기화	인증서갱신	

macOS 장치잠금

분실한 macOS 장치를원격으로잠글수있습니다. XenMobile 이장치를잠급니다. 그런다음 PIN 코드를생성하여장치에이코드를설정합니다. 장치에액세스하려면사용자는 PIN 코드를입력해야합니다. 잠금을제거하려면 XenMobile 콘솔에서 잠금취소를사용합니다.

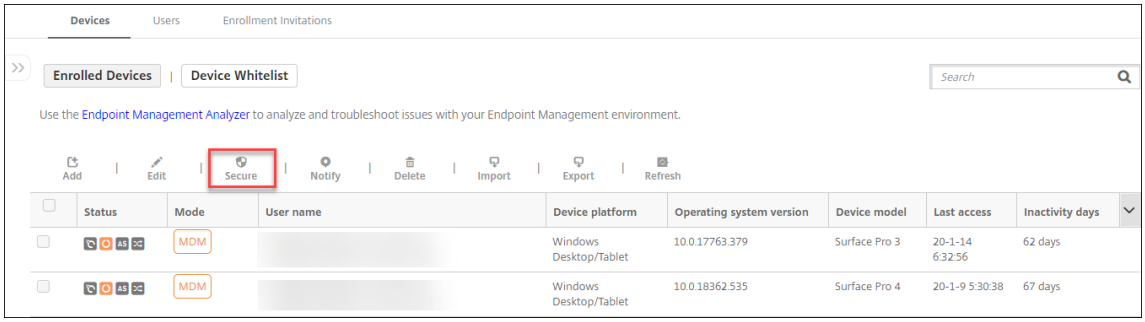
암호 장치정책을사용하여 PIN 코드로연결된추가설정을구성할수있습니다. 자세한내용은 macOS 설정을참조하십시오.

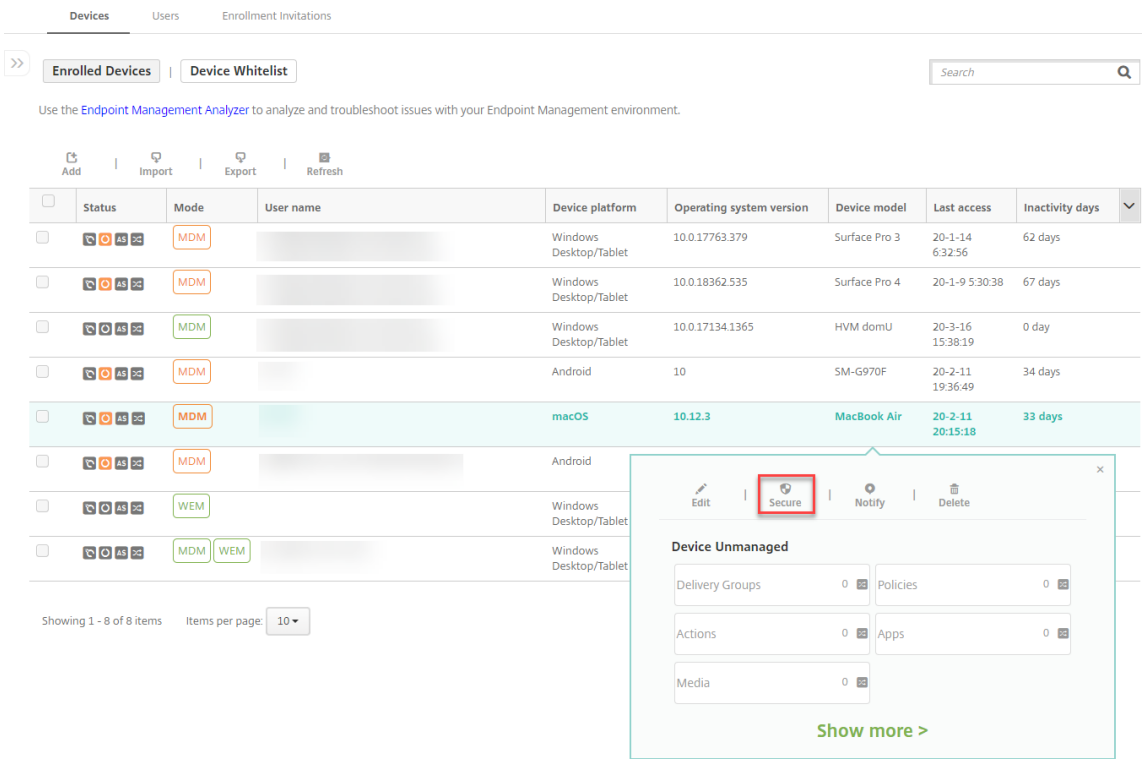
1. 관리 **>** 장치를클릭합니다. 장치페이지가나타납니다.



2. 잠글 macOS 장치를선택합니다.

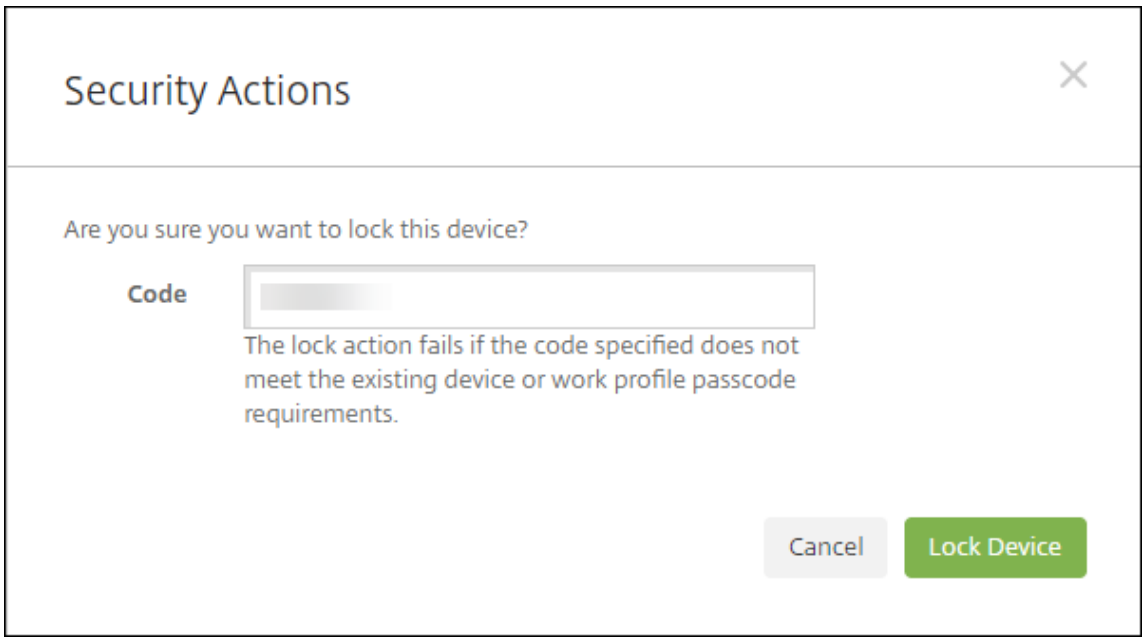
   장치옆에있는확인란을선택하여장치목록위의옵션메뉴를표시합니다. 목록에나열된항목중아무위치나클릭하면목록오른쪽에옵션메뉴를표시할수도있습니다.





3. 옵션메뉴에서 보안을클릭합니다. 보안동작대화상자가나타납니다.

4. 잠금을클릭합니다. 보안동작확인대화상자가표시됩니다.



5. 장치잠금을클릭합니다.

> 중요:
>
> XenMobile 이생성한코드를새용하는대신암호를지정할수도있습니다. 지정한코드가장치또는기존작업프로필의코드요구사항을충족하지않으면잠금동작이실패합니다.

Apple 장치의대량등록

January 5, 2022

XenMobile 에서는두가지방법을사용하여많은수의 iOS, iPadOS 및 macOS 장치를등록할수있습니다.

- Apple 배포프로그램을사용하여 Apple, 참여 Apple 공인리셀러또는이동통신사업자로부터직접구입한 iOS, iPadOS 및 macOS 장치를등록합니다. 이러한지원에는공유 iPad 도포함됩니다. XenMobile 은 Apple Business Manager(ABM) 용 Apple 배포프로그램과교육용 Apple School Manager(ASM) 를지원합니다. 이문서에서는여러장치를 ABM 계정과통합하는방법에대해설명합니다. ABM 에등록하고 ABM 계정을 XenMobile 과연결하는방법에대한자세한내용은 Apple 배포프로그램을통한장치배포를참조하십시오. Apple School Manager 계정에대한자세한내용은 Apple 교육기능과통합을참조하십시오.

  macOS 장치를등록하려면 XenMobile 에서해당장치가 macOS 10.10 이상을실행해야합니다.

- Apple Configurator 2 를사용하여 Apple 에서직접구입했는지여부와관계없이 iOS 장치를등록할수도있습니다.

ABM 사용시:

- 장치를터치하거나준비할필요가없습니다. 대신, ABM 을통해장치일련번호또는구매주문번호를제출하여장치를구성하고등록할수있습니다.

- XenMobile 에장치가등록된후에는장치를사용자에게제공하여바로사용하도록할수있습니다. ABM 을사용하여장치를설정하면장치를처음시작할때완료해야하는설정도우미의몇몇단계를제거할수있습니다.
- ABM 설정에대한자세한정보는 Apple Business Manager의설명서를참고하십시오.

Apple Configurator 2 를사용하는경우:

- iOS 장치를 macOS 10.7.2 이상을실행하는 Apple 컴퓨터와 Apple Configurator 2 앱에연결합니다. Apple Configurator 2 를통해 iOS 장치를준비하고정책을구성할수있습니다.
- 필요한정책으로장치를프로비전한후장치에서처음으로 XenMobile 에연결하면 XenMobile 의정책이장치에수신됩니다. 그런다음장치관리를시작할수있습니다.
- Apple Configurator 사용에대한자세한내용은 Apple Configurator 도움말을참조하십시오.

사전요구사항

XenMobile 과 Apple 간의연결에필요한포트를엽니다. 자세한내용은 포트요구사항을참조하십시오.

XenMobile 와 Apple Business Manager 계정통합

ABM 계정을 XenMobile 로설정하지않은경우 Apple 배포프로그램을통한장치배포의다음단계를완료하십시오.

- Apple Business Manager 에등록합니다.
- Apple Business Manager 계정을 XenMobile 과연결합니다.
- 배포프로그램지원장치를주문합니다.
- 배포프로그램지원장치를관리합니다.

일괄등록을위한기본서버설정

iOS, iPadOS, macOS 장치의대량주문을 MDM 서버에할당하기위해 XenMobile 을기본서버로설정할수있습니다.

1. 관리자또는장치등록관리자계정을사용하여 Apple Business Manager에로그인합니다.
2. 사이드바에서 설정 **>** 장치관리설정을클릭합니다.
3. 기존 MDM 서버를선택합니다. 기본장치할당에서 변경을클릭합니다. 각장치유형에대해기본 XenMobile Server 를선택합니다. 완료를클릭합니다.

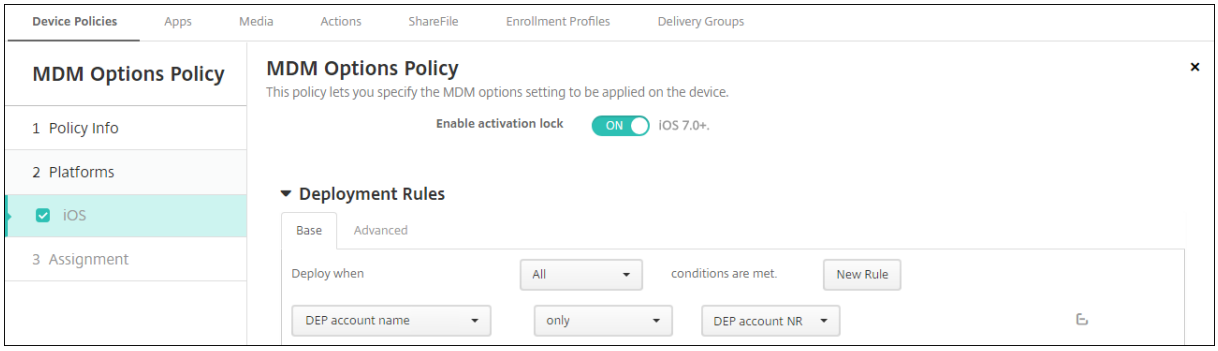
ABM 계정에대한장치정책및앱의배포규칙구성

구성 **>** 장치정책및 구성 **>** 앱아래의 배포규칙섹션을사용하여서로다른장치정책및앱에 ABM 계정을연결할수있습니다. 다음과같은정책또는앱을지정할수있습니다.

- 특정 ABM 계정에만배포합니다.
- 선택한계정을제외한모든 ABM 계정에배포합니다.

ABM 계정목록에상태가사용또는사용안함상태인계정만포함됩니다. 사용되지않는 ABM 계정에는 ABM 장치가속하지않습니다. 따라서 XenMobile 에서는해당장치에앱또는정책을배포하지않습니다.

다음예에서장치정책은 ABM 계정이름이 “ABM Account NR” 인장치에만배포됩니다.

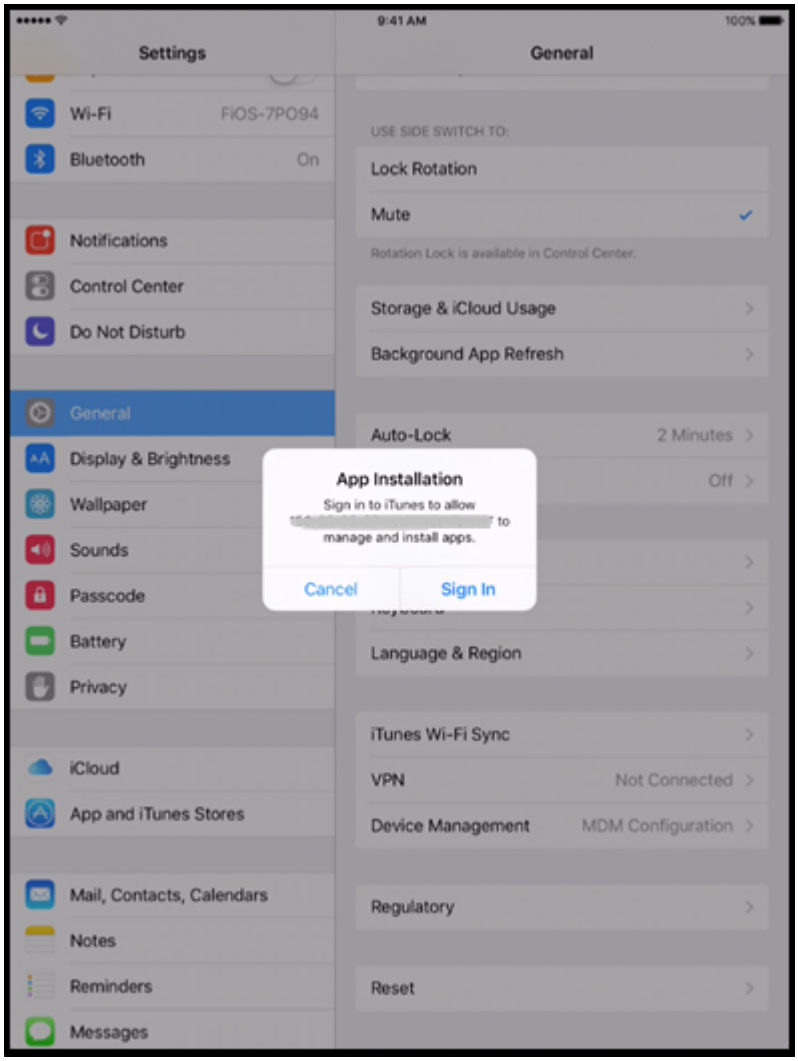


Apple 배포프로그램지원장치등록시사용자환경

Apple 배포프로그램지원장치를등록할때의사용자환경은다음과같습니다.

1. 사용자가 Apple 배포프로그램지원장치를시작합니다.
2. XenMobile 은 XenMobile 콘솔에서구성한 Apple 배포프로그램구성을 Apple 배포프로그램지원장치에제공합니다.
3. 사용자가장치에서초기설정을구성합니다.
4. 장치에서 XenMobile 장치등록프로세스가자동으로시작됩니다.
5. 사용자가장치에서다른초기설정을계속구성합니다.
6. 홈화면에 Citrix Secure Hub 를다운로드할수있도록 Apple App Store 에로그인하라는메시지가나타날수있습니다.

> 참고:
>
> 장치기반볼륨구매앱할당을사용하여 Secure Hub 앱을배포하도록 XenMobile 을구성할경우이단계는선택사항입니다. 이경우 Apple App Store 계정을만들거나기존계정을사용할필요가없습니다.



7. Secure Hub 를열고자격증명을입력합니다. 정책에의해요구되는경우 Citrix PIN 을생성하고확인하라는메시지가표시될수있습니다.

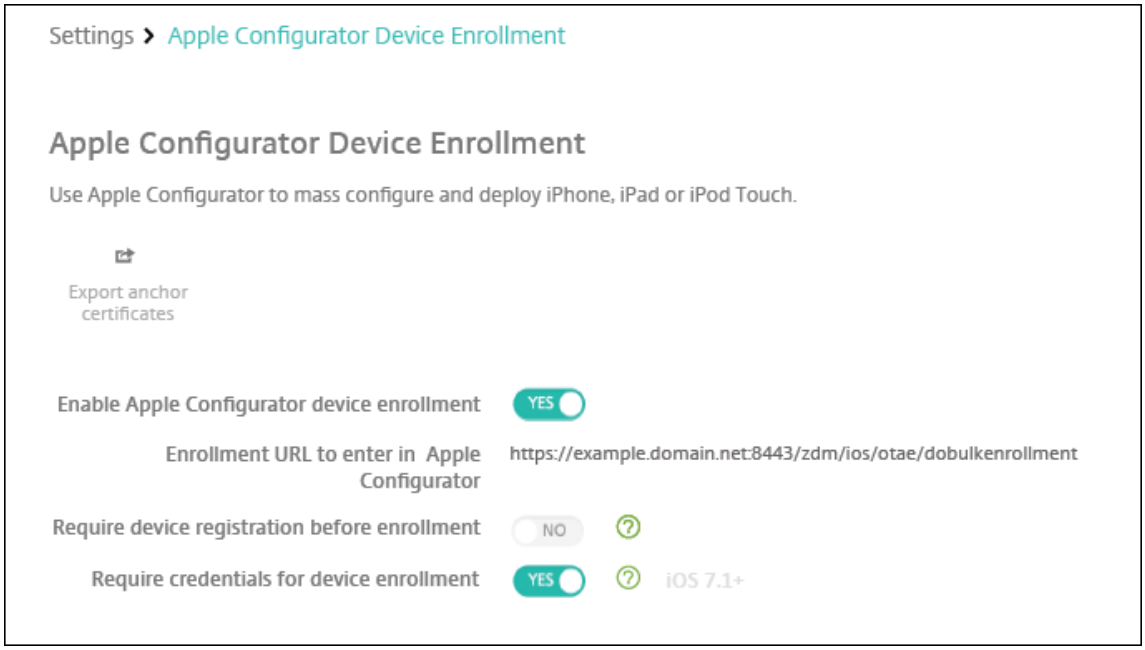
   XenMobile 에서나머지필수앱을장치에배포합니다.

Apple Configurator 2 설정구성

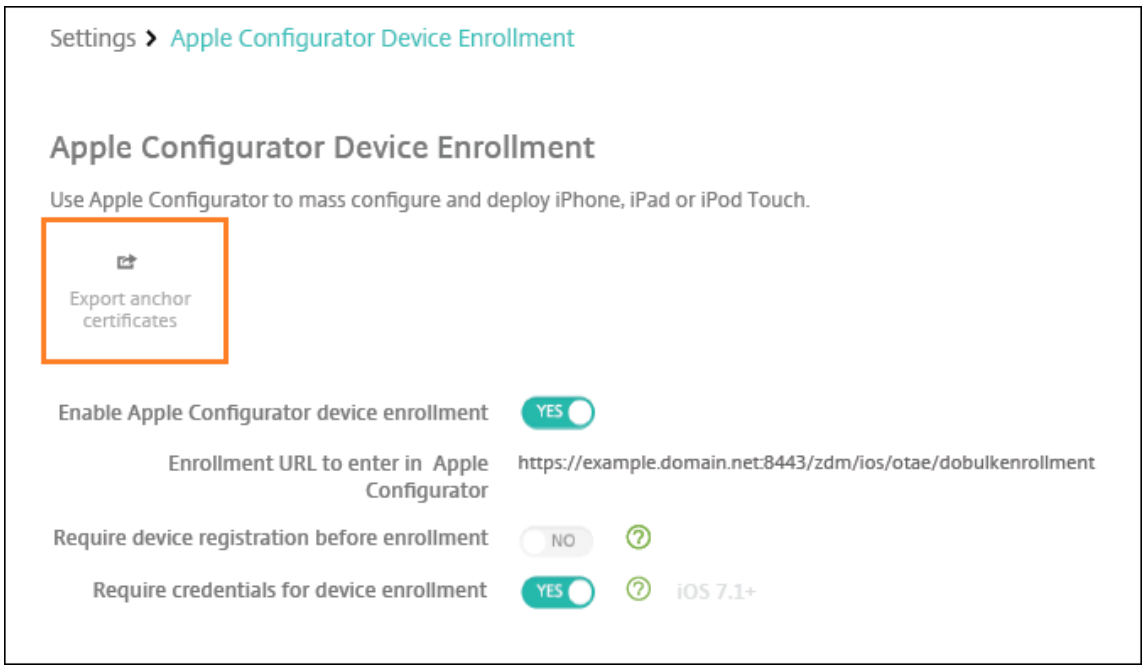
Apple Business Manager 대신 Apple Configurator 2 를사용하여 iPhone 및 iPad 장치를일괄구성하고배포할수있습니다.

1 단계**: XenMobile** 에서설정구성

1. XenMobile 콘솔에서 설정 **> Apple Configurator** 장치등록으로이동합니다.



2. **Apple Configurator** 장치등록허용을 예로설정합니다.
3. **Apple Configurator** 에입력할등록 **URL** 은읽기전용필드입니다. 이설정은 Apple 과통신하는 XenMobile Server 의 URL 을제공합니다. Apple Configurator 2 에서설정을구성할때이 URL 을복사하여붙여넣습니다. 등록 URL 은 XenMobile Server 의 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. 기본값은등록에자격증명을요구하지않는것입니다.
6. 참고: XenMobile 서버에서신뢰할수있는 SSL 인증서를사용하는경우이단계를건너뜁니다. 앵커인증서내보내기를클릭하고 certchain.pem 파일을 macOS 키집합 (로그인또는시스템) 에저장합니다.



2 단계**: Apple Configurator 2** 에서설정구성

1. App Store 에서 Apple Configurator 2 를설치합니다.
2. 도킹커넥터-USB 케이블을사용하여 Apple Configurator 2 를실행하는 Mac 에장치를연결합니다. 연결된장치는최대 30 개까지동시에구성할수있습니다. Dock 커넥터가없는경우전원이연결된하나이상의 USB 2.0 고속허브를사용하여장치에연결합니다.
3. Apple Configurator 2 를시작합니다. Configurator 에는감독을위해준비할수있는모든장치가표시됩니다.
4. 감독할장치를준비하려면:
   - 구성을정기적으로다시적용하여장치의제어를유지하려면 장치감독을선택합니다. 다음을클릭합니다.

     > 중요**:**
     >
     > 감독모드로장치를설정하면선택한버전의 iOS 가장치에설치되어이전에저장된사용자데이터또는앱이장치에서완전히초기화됩니다.

   - iOS 에서 **Latest(**최신**)** 를클릭하여설치할최신버전의 iOS 를검색합니다.
5. **MDM** 서버에서등록에서 MDM 서버를선택합니다. 새서버를추가하려면 다음을클릭합니다.
6. **MDM** 서버정의에서서버이름을제공하고 XenMobile 콘솔에서 MDM 서버 URL 을붙여넣습니다.
7. 조직에할당에서장치를감독할조직을선택합니다.

   Apple Configurator 2 로장치를준비하는방법에대한자세한내용은 Apple Configurator 도움말페이지 장치준비를 참조하십시오.
8. 각장치를준비할때장치를켜서 iOS 설정도우미를시작하면장치를처음으로사용할수있도록준비됩니다.

Apple Configurator 2 에서 **Apple Business Manager** 에장치를할당하려면

Apple Configurator 2 에서 iPhone 및 iPad 장치를 Apple Business Manager 계정과연결할수있습니다. 장치를추가하면 장치섹션에표시됩니다. 이러한장치에는 Apple Configurator 2 를통해할당된등록설정이더이상포함되지않습니다. 자세한내용은 Apple Configurator 2 에서 Apple Business Manager 에추가된장치할당을참조하십시오.

Apple 배포프로그램사용시인증서갱신또는업데이트

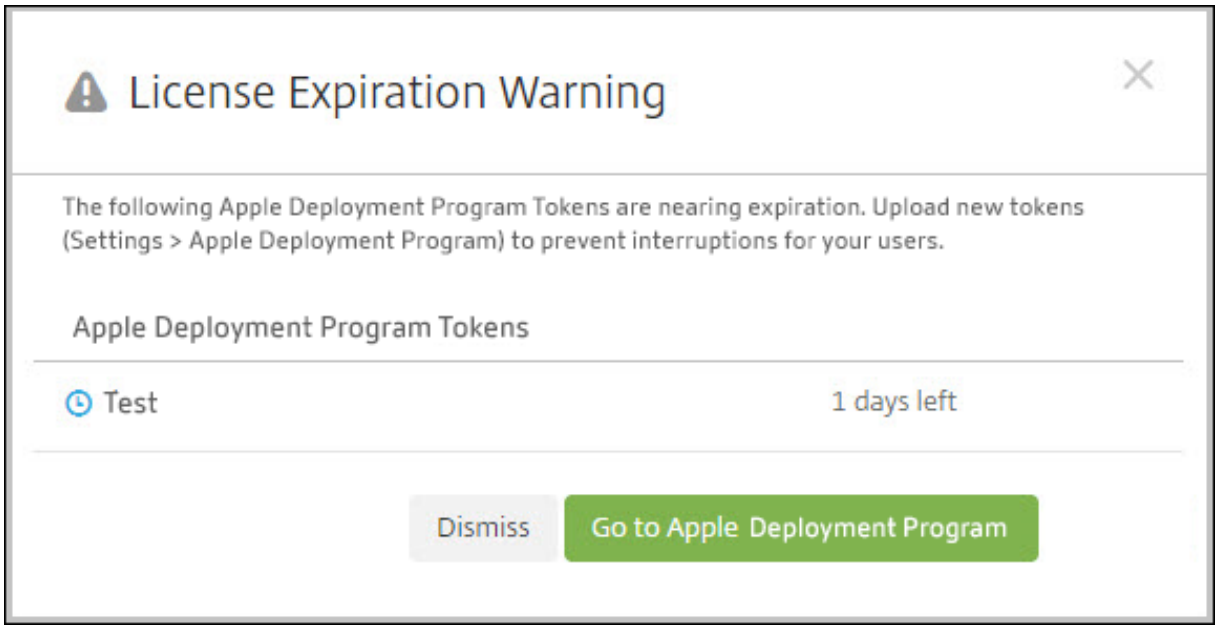
XenMobile SSL(Secure Sockets Layer) 인증서가갱신되면 XenMobile 콘솔의 설정 **>** 인증서에서새인증서를업로드합니다. 가져오기대화상자의 용도에서인증서가 SSL 에사용되도록 **SSL** 수신기를클릭합니다. 서버를다시시작하면 XenMobile 이새 SSL 인증서를사용합니다. XenMobile 의인증서에대한자세한내용은 XenMobile 의인증서업로드를참조하십시오.

SSL 인증서를갱신하거나업데이트할때 Apple 배포프로그램과 XenMobile 간의트러스트관계를다시설정할필요는없습니다. 그러나이문서의이전단계에따라언제든지 **Apple** 배포프로그램설정을다시구성할수있습니다.

Apple 배포프로그램에대한자세한정보는 Apple 설명서에서확인하십시오.

Apple 배포프로그램과 **XenMobile** 사이의연결갱신

XenMobile 은자동화된장치등록서버토큰이만료되면라이센스만료경고를표시합니다.



Apple School Manager/Apple Business Manager 의토큰을교체합니다.

1 단계**: XenMobile** 서버에서공개키다운로드

1. XenMobile 콘솔에서 설정 **> Apple** 배포프로그램으로이동하여새공개키를다운로드합니다.

2 단계**: Apple** 계정에서서버토큰파일생성및다운로드

1. Apple Business Manager 에로그인하여토큰을다운로드합니다.
2. 설정을열고토큰이필요한서버를선택합니다. 편집을클릭합니다.
3. **MDM** 서버설정에서 XenMobile 에서다운로드한새로운공개키를업로드하고변경사항을저장합니다.
4. 토큰다운로드를클릭하여새토큰을다운로드합니다.

3 단계**: XenMobile** 에서서버토큰파일업로드

1. Citrix XenMobile 에서 설정 **> Apple** 배포프로그램으로이동합니다.
2. 배포프로그램계정을선택하고 편집을클릭한다음서버토큰파일을업로드합니다.
3. 다음을클릭하고변경사항을저장합니다.

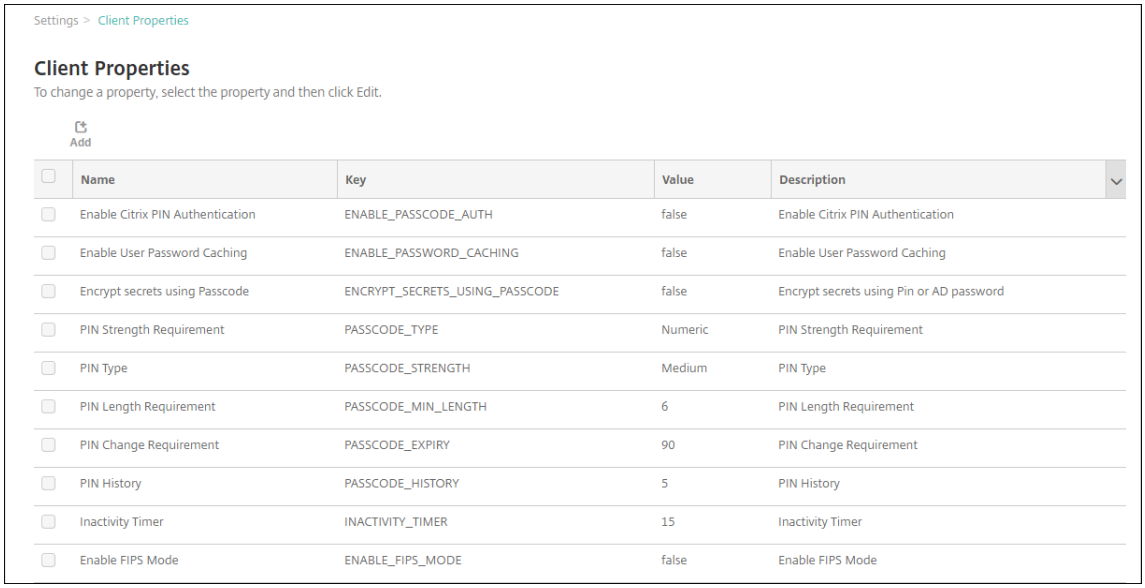
클라이언트속성

March 14, 2022

클라이언트속성은사용자장치에서 Secure Hub 에직접제공되는정보를포함합니다. 이러한속성을사용하여 Citrix PIN 같은고급설정을구성할수있습니다. Citrix 지원에서클라이언트속성을가져옵니다.

클라이언트속성은 Secure Hub 가릴리스될때마다변경될수있으며클라이언트앱의경우가끔변경될수있습니다. 보다일반적으로구성된클라이언트속성에대한자세한내용은이문서뒷부분에서클라이언트속성참조를참조하십시오.

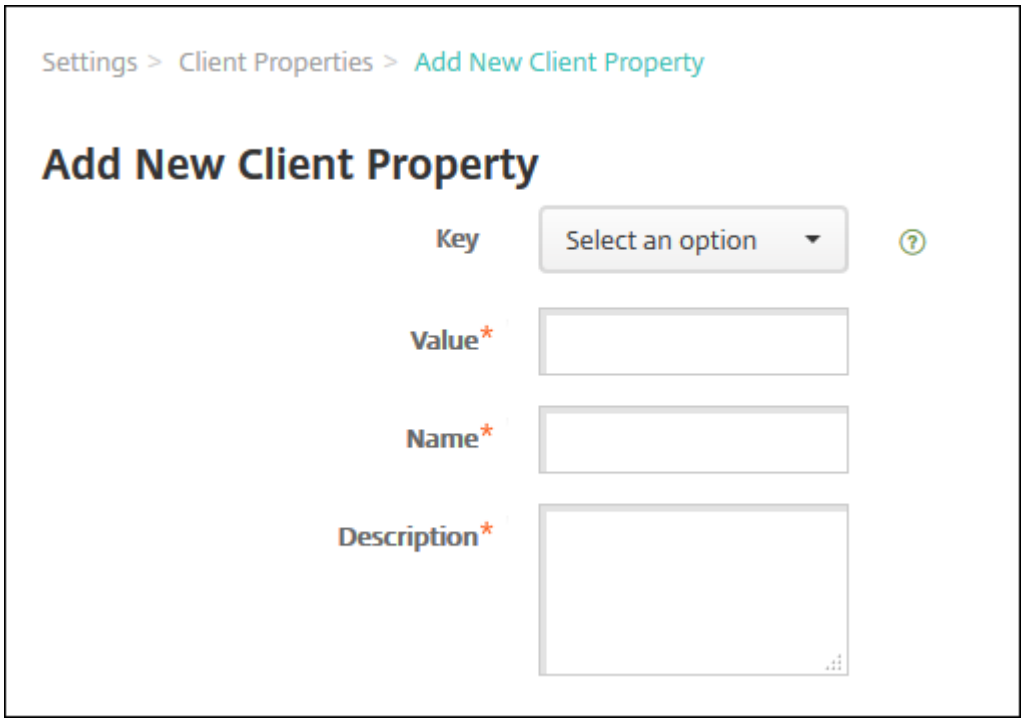
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 클라이언트에서 클라이언트속성을클릭합니다. 클라이언트속성페이지가나타납니다. 이페이지에서클라이언트속성을추가, 편집또는삭제할수있습니다.



Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

클라이언트속성을추가하려면

1. 추가를클릭합니다. 새클라이언트속성추가페이지가나타납니다.



2. 다음설정을구성합니다.

   - **키:** 목록에서추가하려는속성을클릭합니다. 중요: 이설정을업데이트하기전에 Citrix 지원에문의하십시오. 특수키를요청할수있습니다.
   - **값:** 선택한속성값입니다.

- 이름**:** 속성의이름입니다.
- 설명**:** 속성의설명입니다.

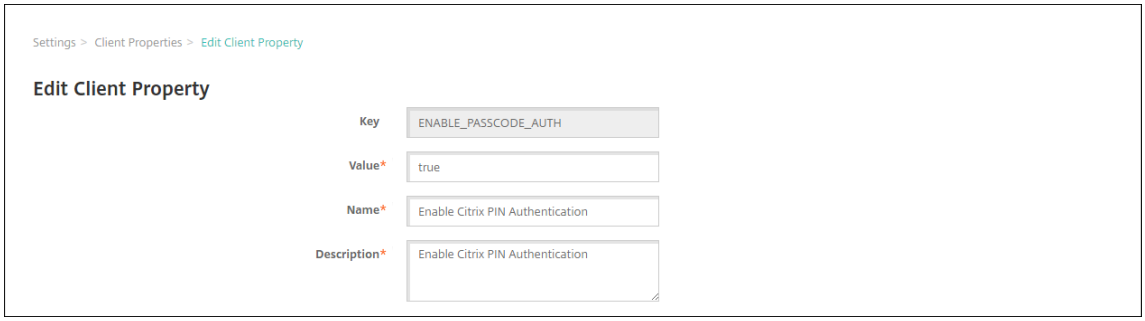
3. 저장을클릭합니다.

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. 시간제한후에는앱을더이상사용할수없습니다. 데이터초기화에는설치된각앱의앱데이터 (앱캐시및사용자데이터등) 를지우는작업이포함됩니다.

  비활성화시간은서버가특정시간동안사용자검증을위한인증요청을수신하지않는기간을의미합니다. 예를들어이속성이 30 일인경우사용자가앱을 30 일넘게사용하지않으면정책이적용됩니다.

  이글로벌보안정책은 iOS 및 Android 플랫폼에적용되며기존의앱잠금및초기화정책의향상된버전입니다.

- 이 글 로 벌 정 책 을 구 성 하 려 면 설 정 **>** 클 라 이 언 트 속 성 으 로 이 동 한 다 음 사 용 자 지 정 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)
  - 자격증명저장소를사용하면 Android 또는 iOS 사용자가모바일생산성앱에액세스할때암호를한번만입력하면됩니다. Citrix PIN 사용여부와상관없이자격증명저장소를사용할수있습니다. Citrix PIN 을사용하지않는경우사

용자는 Active Directory 암호를입력합니다. XenMobile 은 Secure Hub 및공용스토어앱에대해서만자격증명저장소와함께 Active Directory 암호를사용하도록지원합니다. 자격증명저장소와함께 Active Directory 암호를사용하는경우 XenMobile 에서 PKI 인증을지원하지않습니다.

- Secure Mail 에자동등록하려면이속성을 **true** 로설정해야합니다.
- 이사용자지정클라이언트정책을구성하려면 설정 **>** 클라이언트속성으로이동한다음사용자지정키 **ENABLE_CREDENTIAL_STORE** 를추가하고 값을 **true** 로설정합니다.

- **ENABLE_FIPS_MODE**
  - 표시이름: Enable FIPS Mode(FIPS 모드사용)
  - 이속성은모바일장치에서 FIPS 모드의사용여부를설정합니다. 값을변경하면 Secure Hub 가다음번온라인인증을수행할때새값을장치로전달합니다.
  - 가능한값: **true** 또는 **false**
  - 기본값: **false**
- **ENABLE_PASSCODE_AUTH**
  - 표시이름: Enable Citrix PIN Authentication(Citrix PIN 인증사용)
  - 이속성을사용하여 Citrix PIN 기능을활성화할수있습니다. Citrix PIN 또는암호를사용하는경우 Active Directory 암호대신사용할 PIN 을정의하라는메시지가나타납니다. 이설정은 ENABLE_PASSWORD_CACHING 이활성화되거나 XenMobile 이인증서인증을사용하는경우자동으로활성화됩니다.

    오프라인인증의경우로컬에서 Citrix PIN 의유효성이검사되고사용자가요청한앱이나콘텐츠에액세스하도록허용됩니다. 온라인인증의경우 Citrix PIN 또는암호를사용하여 Active Directory 암호또는인증서를잠금해제한다음이를 XenMobile 로전송하여인증을수행합니다.

    ENABLE_PASSCODE_AUTH 가 true 이고 ENABLE_PASSWORD_CACHING 이 false 인경우 Secure Hub 에암호가저장되지않으므로온라인인증시항상암호입력메시지가표시됩니다.
  - 가능한값: **true** 또는 **false**
  - 기본값: **false**
- **ENABLE_PASSWORD_CACHING**
  - 표시이름: Enable User Password Caching(사용자암호캐싱사용)
  - 이속성을사용하면 Active Directory 암호가모바일장치에로컬로캐싱됩니다. 이속성을 **true** 로설정하는경우 **ENABLE_PASSCODE_AUTH** 속성도 **true** 로설정해야합니다. 사용자암호캐싱을사용하도록설정한경우 Citrix PIN 또는암호를설정하라는메시지가나타납니다.
  - 가능한값: **true** 또는 **false**
  - 기본값: **false**
- **ENABLE_TOUCH_ID_AUTH**
  - 표시이름: Enable Touch ID Authentication(Touch ID 인증사용)
  - Touch ID 인증을지원하는장치의경우이속성은장치에서 Touch ID 인증의사용여부를설정합니다요구사항:

사용자장치가 Citrix PIN 또는 LDAP 를사용하도록설정되어있어야합니다. LDAP 인증이해제된경우(예: 인증서기반인증만사용되는경우) 사용자가 Citrix PIN 을설정해야합니다. 이경우클라이언트속성 **ENABLE_PASSCODE_AUTH** 가 **false** 인경우에도 XenMobile 에 Citrix PIN 이필요합니다.

사용자가앱을시작할때 Touch ID 를사용하라는메시지에응답해야하도록 **ENABLE_PASSCODE_AUTH** 를 **false** 로설정합니다.

- 가능한값: **true** 또는 **false**
- 기본값: **false**

- **ENABLE_WORXHOME_CEIP**
  - 표시이름: Enable Worx Home CEIP(Worx Home CEIP 사용)
  - 이속성은 CEIP(사용자환경개선프로그램) 를활성화합니다. 이기능은익명의구성및사용현황데이터를 Citrix 에정기적으로전송합니다. 이데이터는 Citrix 가 XenMobile 의품질, 안정성및성능을개선하는데도움이됩니다.
  - 값: **true** 또는 **false**
  - 기본값: **false**
- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 표시이름: Encrypt secrets using Passcode(암호를사용하여암호암호화)
  - 이속성은민감한데이터를 iOS 키집합과같은플랫폼기반기본저장소가아닌장치의기밀저장소에저장합니다. 이속성을사용하면키아티팩트의암호화가강화되고사용자엔트로피가추가됩니다. 사용자엔트로피는사용자가생성한임의의 PIN 코드로, 이 PIN 코드는사용자만알고있습니다.

    사용자장치에서높은수준을보안을제공하려면이속성을활성화하는것이좋습니다. 이경우사용자에게 Citrix PIN 에대한인증프롬프트가더많이나타납니다.
  - 가능한값: **true** 또는 **false**
  - 기본값: **false**
- **INACTIVITY_TIMER**
  - 표시이름: Inactivity Timer(비활성타이머)
  - 이속성은사용자가장치를비활성상태로둔후에 Citrix PIN 또는암호를입력하라는메시지없이앱에액세스할수있는시간을정의합니다. MDX 앱에대해이설정을사용되도록설정하려면앱암호설정을켜짐으로설정합니다. 앱암호설정이꺼짐으로설정된경우사용자는전체인증을수행하기위해 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(장애시전자메일을사용하여장치로그를 IT 지원센터에보내기)
  - 이속성은전자메일을사용하여 IT 에장치로그를보내는기능의사용여부를설정합니다.
  - 가능한값: **true** 또는 **false**
  - 기본값: **true**

- **PASSCODE_EXPIRY**
  - 표시이름: PIN Change Requirement(PIN 변경요구사항)
  - 이속성은 Citrix PIN 또는암호가유효한기간을정의합니다. 이기간이지나면사용자가 Citrix PIN 또는암호를변경하도록강제합니다. 이설정을변경하면현재 Citrix PIN 또는암호가만료된경우에만새값이설정됩니다.
  - 가능한값: **1** ~ **99**(권장) 입니다. PIN 재설정을제거하려면값을매우높은숫자로설정합니다 (예: 100,000,000,000). 원래만료기간을 1 일에서 99 일사이로설정한경우해당기간동안이기간을큰수로변경하면 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: 약함, 중간, 다소강함또는 강함
  - 기본값: 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
높음	인접한숫자는같을수없습니다.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Strong(강함)	같은숫자를세번이상사용하지마십시오. 세개이상의숫자를연속으로사용하지마십시오. 세개이상의연속된숫자를역순으로사용하지마십시오.	102983, 085085, 824673, 132312	132132, 131313, 902030

영숫자암호에대한규칙:

암호강도	영숫자암호유형에대한규칙	허용	허용안함
Low(낮음)	하나이상의숫자와하나의문자가있어야합니다.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
Medium(중간)(기본설정)	낮음암호강도에대한규칙에더해문자와모든숫자가동일해서는안됩니다. 문자가연속해서는안되며숫자가연속해서는안됩니다.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, or cba123
높음	최소한대문자하나와소문자하나를포함해야합니다.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Strong(강함)	최소한숫자하나, 특수기호하나, 대문자하나및소문자하나를포함해야합니다.	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**)** 를선택하면사용자가문자와숫자조합 (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. 새로고침간격을변경하려면 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. 이렇게하면사용자가추가정보를제공하거나추가단계를수행하지않고 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 정책과유사하게매크로로지정됩니다.
  - 다음은이속성의샘플계정서비스응답입니다.

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName=
    eng1,displayName=user\,test1,email=user@site.com\,user@site.com"
    name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - 이속성의경우 XenMobile 은쉼표문자를문자열종결자로취급합니다. 그러므로특성값에쉼표가포함되는경우그앞에백슬래시를추가해야합니다. 백슬래시를추가하면클라이언트가포함된쉼표를특성값의끝으로해석하지않습니다. 백슬래시문자는 "\\"로표현합니다.
- **HIDE_THREE_FINGER_TAP_MENU**

  - 이속성이설정되지않거나 **false** 로설정된경우사용자가장치에서세손가락누르기를수행하여숨겨진기능메뉴에액세스할수있습니다. 숨겨진기능메뉴를사용하면사용자가응용프로그램데이터를재설정할수있습니다. 이속성을 **true** 로설정하면사용자가숨겨진기능메뉴에액세스할수없습니다.
  - 이 글 로 벌 클 라 이 언 트 정 책 을 구 성 하 려 면 설 정 **>** 클 라 이 언 트 속 성 으 로 이 동 하 고 사 용 자 지 정 키 **HIDE_THREE_FINGER_TAP_MENU** 를추가한다음 값을설정합니다.

- **TUNNEL_EXCLUDE_DOMAINS**
  - 표시이름: Tunnel Exclude Domains
  - 기본적으로 MDX 는 Micro VPN 터널링에서 XenMobile SDK 및앱이여러기능에사용하는일부서비스끝점을제외합니다. 예를들어이러한끝점에는 Google Analytics, Citrix Cloud Services, Active Directory 서비스등엔터프라이즈네트워크를통한라우팅이필요하지않은서비스가포함됩니다. 제외되는도메인의기본목록을재정의하려면이클라이언트속성을사용합니다.
  - 이 글 로 벌 클 라 이 언 트 정 책 을 구 성 하 려 면 설 정 **>** 클 라 이 언 트 속 성 으 로 이 동 한 다 음 사 용 자 지 정 키 **TUNNEL_EXCLUDE_DOMAINS** 를추가하고 값을설정합니다.
  - 값: 터널링에서제외할도메인으로기본목록을바꾸려면쉼표로구분된도메인접미사목록을입력합니다. 터널링에모든도메인을포함하려면 **none** 을입력합니다. 기본값은다음과같습니다.

    ```
    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.xm.citrix.com,rttf.citrix.com,rttf
    -staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,
    stream.launchdarkly.com
    ```

Apple 배포프로그램을통한장치배포

August 12, 2022

Apple 에는비즈니스및교육계정을위한장치등록프로그램이있습니다. 비즈니스계정의경우 XenMobile 에서 Apple Business Manager(ABM) 또는 Apple School Manager(ASM) 를사용하여장치를등록하고관리하려면 Apple 배포프로그램에등록해야합니다. 이프로그램은 iOS, iPadOS 및 macOS 장치를위한것입니다.

Apple 배포프로그램은조직을위한프로그램이며개인사용자는사용할수없습니다. Apple Deployment Program 계정을만들려면상당한양의회사세부정보를제공해야합니다. 따라서계정을요청하고승인을받는데시간이걸릴수있습니다.

교육계정의경우 Apple School Manager 계정을생성합니다. ASM 는 Apple 배포프로그램과 Apple 볼륨구매를통합합니다. Apple School Manager 계정을생성하려면 Apple School 사이트로이동합니다.

Apple 배포프로그램등록

Apple Business Manager 에등록하려면 business.apple.com으로이동합니다. 지금등록을클릭하여새계정을신청합니다. 조직의전자메일주소 (예: deployment@company.com) 를사용하는것이가장좋습니다. 등록절차에는며칠이걸릴수있습니다. 로그온자격증명을받은후 Apple Business Manager 에제공된단계에따라계정을만듭니다.

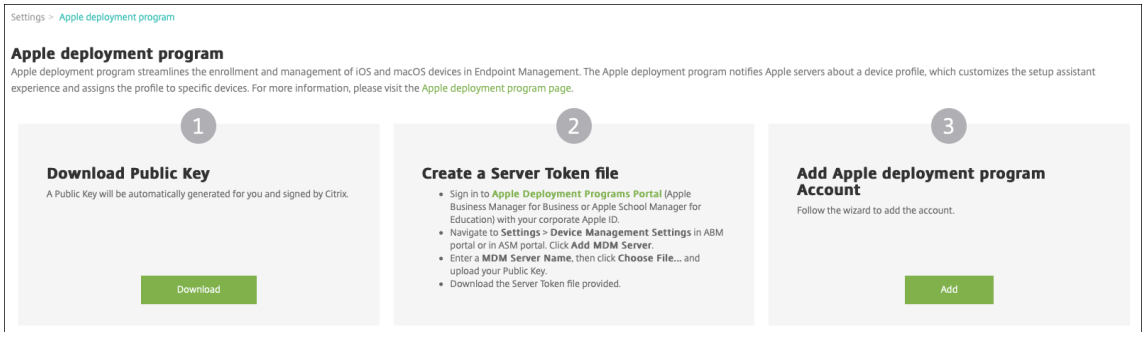
> 참고**:**
>
> 교육계정의경우 Apple 교육기능과통합을참조하십시오.

XenMobile 와 **Apple Business Manager** 계정연결

Apple Business Manager 계정을 XenMobile 배포와연결하려면 XenMobile 콘솔과 Apple Business Manager 에정보를입력합니다. 다음단계를따르십시오.

1 단계**: XenMobile** 서버에서공개키다운로드

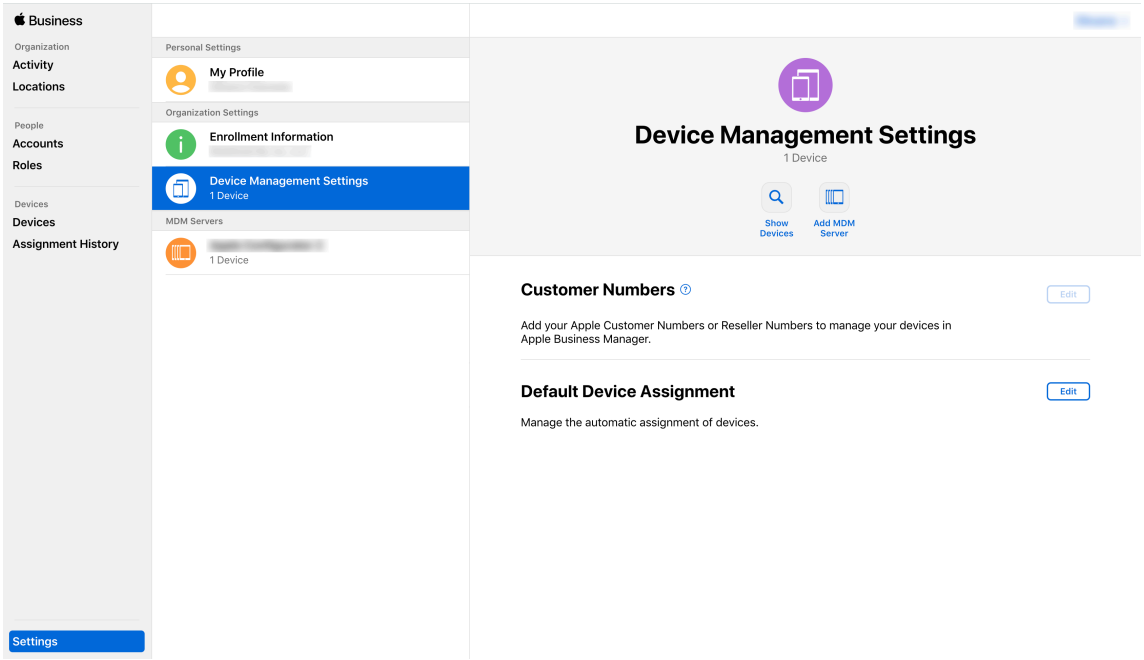
1. XenMobile 콘솔에서 설정 **> Apple** 배포프로그램으로이동합니다.



2. 공개키다운로드에서 다운로드를클릭합니다.

2 단계**: Apple** 계정에서서버토큰파일생성및다운로드

1. 관리자또는장치등록관리자계정을사용하여 Apple Business Manager에로그인합니다.
2. 사이드바하단에서 설정을클릭한다음 장치관리설정 **> MDM** 서버설정을클릭합니다.



3. **MDM** 서버이름설정에서 XenMobile Server 의이름을입력합니다. 입력하는서버이름은참조용입니다. 서버 URL 또는이름이아닙니다.
4. 공개키업로드에서 파일선택을클릭합니다. XenMobile 에서다운로드한공개키를업로드한다음변경내용을저장합니다.
5. 토큰다운로드를클릭하여서버토큰파일을컴퓨터에다운로드합니다.

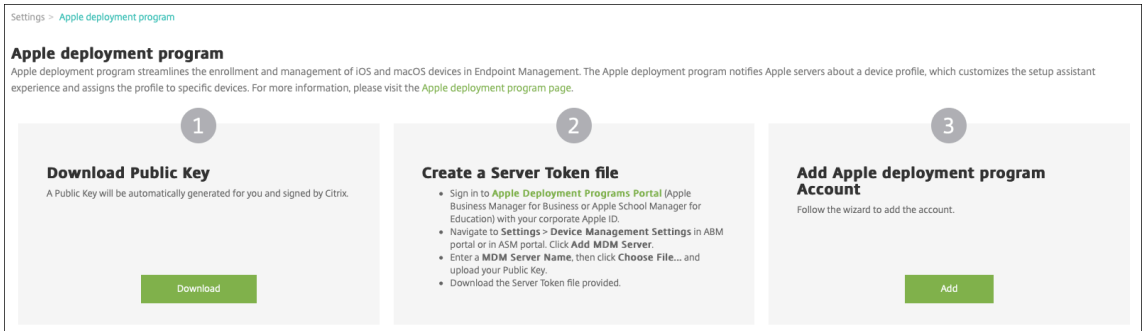
   서버토큰파일은 ABM 계정을 XenMobile 에추가할때업로드해야합니다. 토큰파일을가져오면 ABM 토큰정보가 XenMobile 콘솔에표시됩니다.
6. 기본장치할당에서 변경을클릭합니다. 장치할당방법을선택한후요청된정보를제공합니다. 자세한내용은 ABM 사용자가이드를참조하십시오.

3 단계**: XenMobile** 에 **ABM** 계정추가

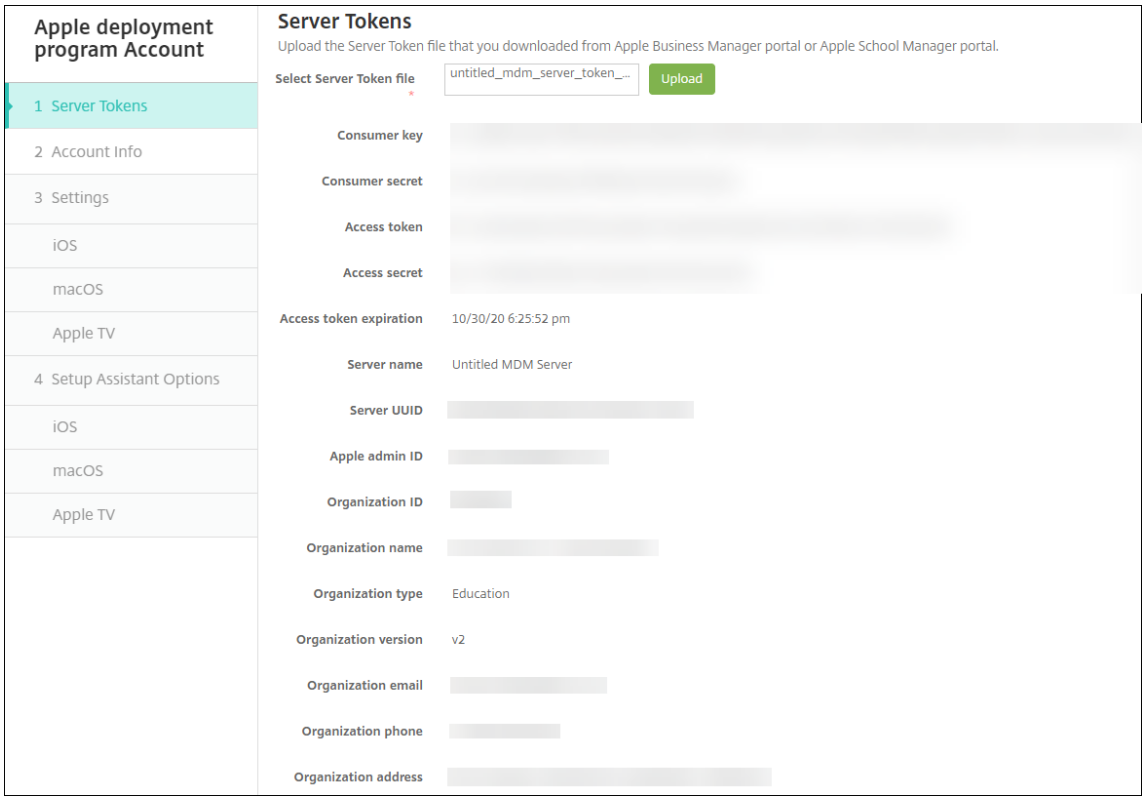
여러개의 ABM 계정을 XenMobile 에추가할수있습니다. 이기능을사용하면서로다른등록설정및설정도우미옵션을국가, 부서별로사용할수있습니다. 그런다음 ABM 계정을여러장치정책에연결할수있습니다.

예를들어여러국가에있는동일한 XenMobile 서버의모든 ABM 계정을중앙집중화하여모든 ABM 장치를가져오고감독할수있습니다. 등록설정및설정도우미옵션을부서, 조직계층또는다른구조별로사용자지정하면정책을통해조직전체에적절한기능을제공하고사용자가적절한지원을받을수있습니다.

1. XenMobile 콘솔에서 설정 **> Apple** 배포프로그램으로이동한다음 **Apple** 배포프로그램계정추가에서 추가를클릭합니다.

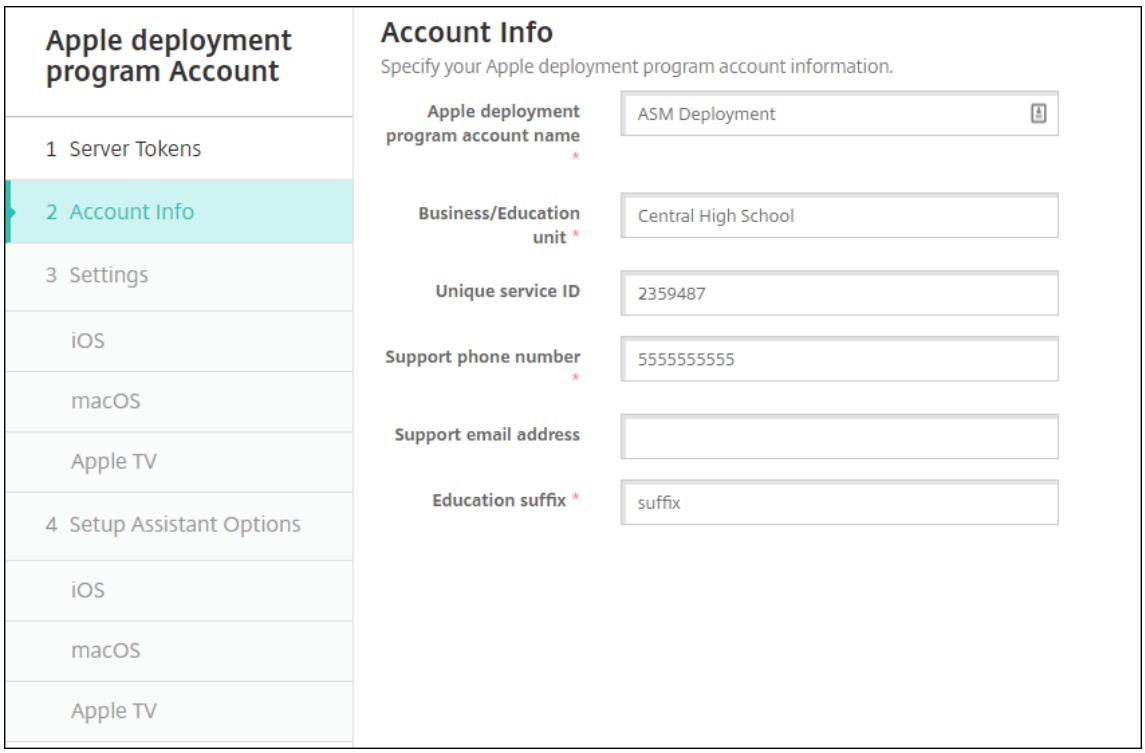


2. 서버토큰페이지에서서버토큰파일을지정하고 업로드를클릭합니다.



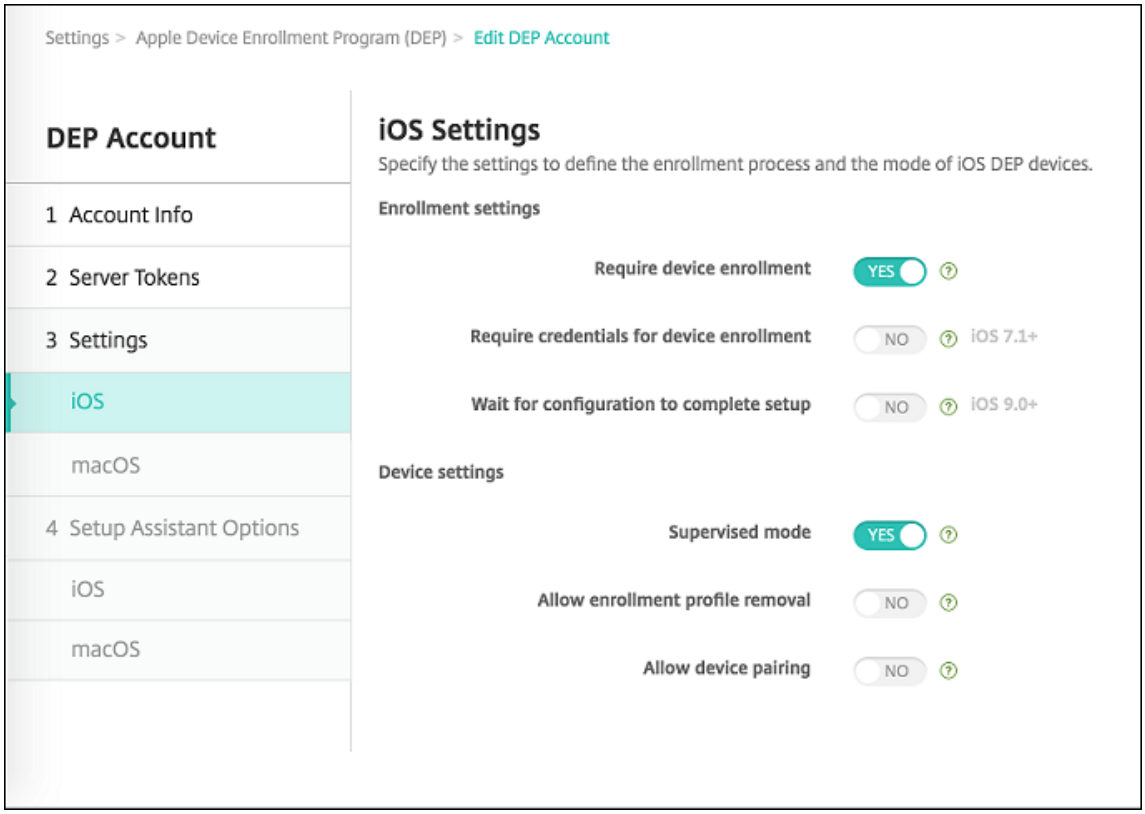
서버토큰정보가표시됩니다.

3. 계정정보페이지에서다음설정을지정합니다.



- **Apple** 배포프로그램계정이름**:** 이 Apple 배포프로그램계정의고유한이름입니다. 국가또는조직계층구조별과같이 Apple 배포프로그램계정을구성하는방식을반영하는이름을사용합니다.
- **Business/Education unit(**비즈니스**/**교육단위**):** 장치를할당할비즈니스단위또는부서입니다. 이것은필수필드입니다.
- 고유서비스 **ID:** 계정을식별하는데도움이되는선택적고유 ID 입니다.
- 지원전화번호**:** 사용자가설정중에전화할수있는지원전화번호입니다. 이것은필수필드입니다.
- 지원전자메일주소**:** 최종사용자에게제공되는선택적지원전자메일주소입니다.

4. **iOS** 설정에서다음설정을지정합니다.



등록설정:

- 장치등록필요**:** 사용자가장치를등록해야하는지여부를설정합니다. 기본값은 예입니다.
- 장치등록에자격증명필요**:** ABM 설정중에사용자가자격증명을입력해야하는지여부를설정합니다. 모든사용자에게장치등록중에자격증명을입력하도록요구하는것이좋습니다. 즉, 권한이있는사용자만장치를등록할수있도록허용합니다. 기본값은 예입니다.

  처음설정하기전에 ABM 을사용설정하고이옵션을선택하지않으면 XenMobile 이 ABM 구성요소를만듭니다. 이렇게만들어지는구성요소로는 ABM 사용자, Secure Hub, 소프트웨어인벤토리, ABM 배포그룹이있습니다. 이옵션을선택하면 XenMobile 이구성요소를만들지않습니다. 그결과나중에이옵션을삭제할경우자격증명을입력하지않은사용자는 ABM 구성요소가존재하지않으므로 ABM 으로등록할수없습니다. ABM 구성요소를추가하려면 ABM 계정을사용하지않도록설정한다음사용하도록설정해야합니다.
- 구성에서설정을완료할때까지대기**:** 모든 MDM 리소스가장치에배포될때까지사용자가설정도우미모드에있어야하는지여부를설정합니다. 이옵션은감독모드인장치에서사용할수있습니다. 기본값은 아니요입니다.
- Apple 설명서에따르면장치가설정도우미모드에있는동안에는다음명령이작동하지않을수있습니다.
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring

- DeviceLock

장치설정:

- 감독모드**:** Apple Configurator 를사용하여 ABM 등록장치를관리하거나 구성에서설정을완료할때까지대기를사용하는경우 예로설정해야합니다. 기본값은 예입니다. iOS 장치를감독모드로전환하는방법에대한자세한내용은 Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.
- 등록프로필제거허용**:** 원격으로제거할수있는프로필을장치에서사용하도록할지여부를설정합니다. 기본값은 아니요입니다.
- 장치페어링허용**:** ABM 을통해등록한장치를 Apple Music 및 Apple Configurator 를통해관리할지여부를설정합니다. 기본값은 아니요입니다.

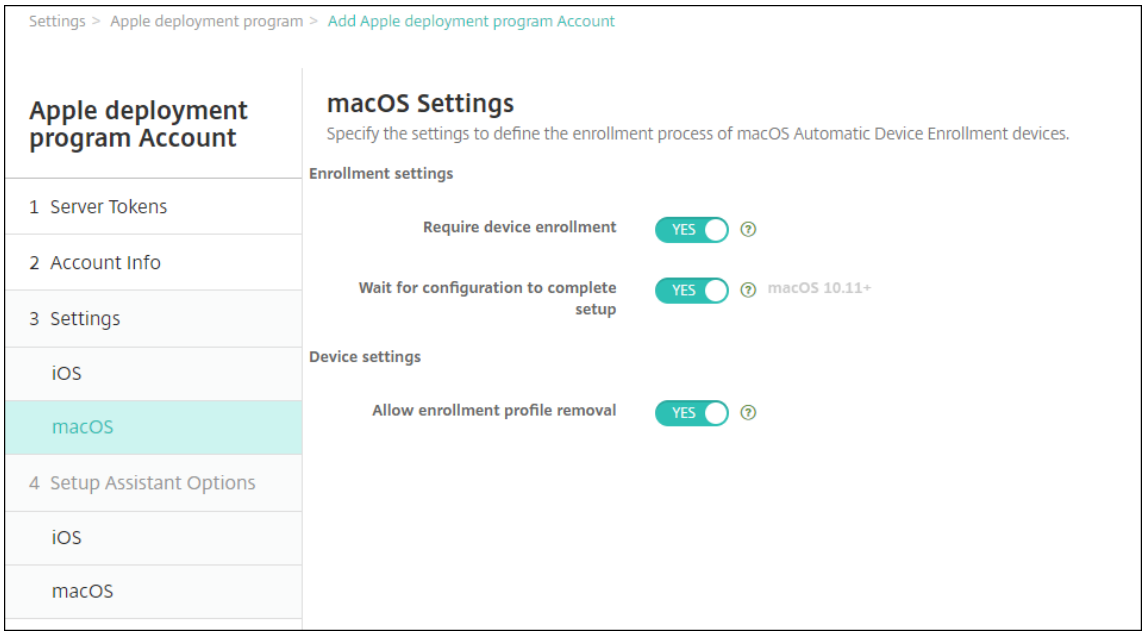
감독 ID

GroundControl 도구를사용하는경우인증서를추가하여다음을수행할수있습니다.

- 페어링제한을재정의하여 "이호스트신뢰" 메시지를방지합니다.
- USB 로관리되는장치동작을에스컬레이션하여사용자상호작용없는프로필설치와같은활동을수행합니다. 이렇게하면 GroundControl 로체크아웃에단일앱모드와장치잠금을사용할수있습니다.
- 백업을 ABM 장치에복원합니다.

GroundControl 에대한자세한정보는 roundControl 웹사이트를참조하십시오.

5. **macOS** 설정에서다음설정을지정합니다.



등록설정:

- 장치등록필요**:** 사용자가장치를등록해야하는지여부를설정합니다. 기본값은 예입니다.
- 구성에서설정을완료할때까지대기**:** 예인경우 MDM 리소스암호가장치에배포되기전까지설정도우미에서 macOS 장치가계속되지않습니다. 해당배포는로컬계정이만들어지기전에발생합니다. 이설정은 macOS 10.11 이상장치에서사용할수있습니다. 기본값은 아니요입니다.

장치설정:

- 등록프로필제거허용**:** 원격으로제거할수있는프로필을장치에서사용하도록할지여부를설정합니다. 기본값은 아니요입니다.

6. **iOS** 설정도우미옵션에서사용자가장치를처음으로시작할때 iOS 설정도우미가건너뛸단계를선택합니다. 화면을건너뛰면관련기능에는기본설정이사용됩니다. 건너뛴기능에대한액세스를완전히제한하지않는한사용자는설정이완료된후해당기능을구성할수있습니다. 기능액세스제한에대한자세한내용은 제한장치정책을참조하십시오. 모든항목에대한기본값은선택되어있지않습니다. 다음설명에서는설정선택시발생하는결과에대해설명합니다.

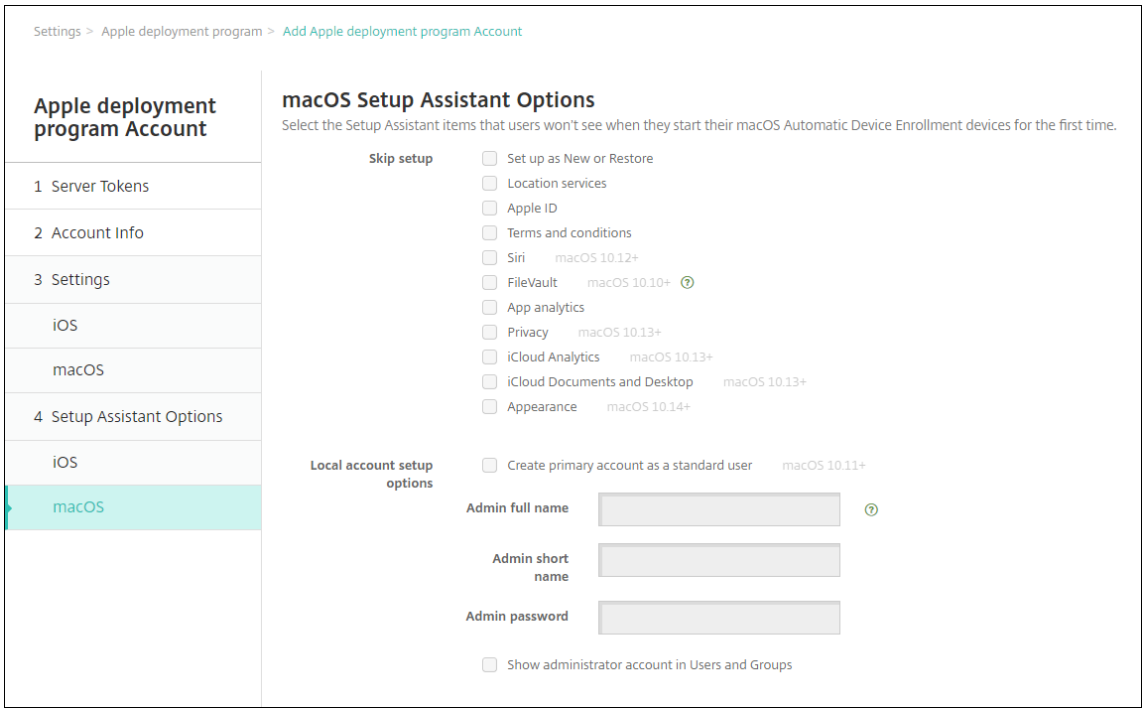
- 위치서비스**:** 사용자가장치에서위치서비스를설정할수없습니다.
- **Touch ID:** 사용자가 iOS 장치에서 Touch ID 또는 Face ID 를설정할수없습니다.
- 암호잠금**:** 사용자가장치에대한암호를설정할수없습니다. 암호가없으면사용자는 Touch ID 또는 Apple Pay 를사용할수없습니다.
- 새로설정또는복원**:** 사용자가장치를새로설정하거나 iCloud 또는 Apple App Store 백업에서설정할수없습니다.
- **Android** 에서이동**:** 사용자가 Android 장치의데이터를 iOS 장치로전송할수없습니다. 이옵션은 새로설정또는복원을선택한경우에만사용할수있습니다 (즉, 단계가생략됨).
- **Apple ID:** 사용자가장치에대한관리형 Apple ID 계정을설정할수없습니다.
- 이용약관**:** 사용자가장치사용약관을읽고수락할수없습니다.
- **Apple Pay:** 사용자가 Apple Pay 를설정할수없습니다. 이설정을선택취소하면사용자는 Touch ID 및 Apple ID 를설정해야합니다. 이러한설정이선택취소되었는지확인하시기바랍니다.
- **Siri:** 사용자가 Siri 를구성할수없습니다.
- 앱분석**:** 사용자가충돌데이터및사용현황통계를 Apple 과공유할지여부를설정할수없습니다.
- 표시확대/축소**:** 사용자가 iOS 장치에서디스플레이해상도 (표준또는확대) 를설정할수없습니다.
- **True Tone:** 사용자가 4 채널센서를설정해디스플레이의화이트밸런스를동적으로조정할수없습니다.
- 홈버튼**:** 사용자가홈버튼스타일의피드백을설정할수없습니다.
- 새로운기능하이라이트**:** 사용자에게 Apple 소프트웨어의새로운기능에대한정보를보여주는화면이표시되지않습

니다.

- 개인정보보호**:** 사용자에게데이터및개인정보보호패널이표시되지않습니다. iOS 11.3 이상에해당합니다.
- 소프트웨어업데이트**:** 사용자가 iOS 를최신버전으로업데이트할수없습니다. iOS 12.0 이상에해당합니다.
- 스크린타임**:** 사용자가스크린타임을활성화할수없습니다. iOS 12.0 이상에해당합니다.
- **SIM** 설정**:** 사용자가셀룰러요금제를설정하지못하도록합니다. iOS 12.0 이상에해당합니다.
- **iMessage** 및 **FaceTime:** 사용자가 iMessage 와 FaceTime 사용설정하지못하도록합니다. iOS 12.0 이상에해당합니다.
- 모양**:** 사용자가모양모드를선택할수없습니다. iOS 13.0 이상에해당합니다.
- 시작**:** 사용자에게 시작화면이표시되지않습니다. iOS 13.0 이상에해당합니다.
- 복원완료**:** 설치중에복원이완료되었는지여부가사용자에게표시되지않습니다. iOS 14.0 에해당합니다.
- 업데이트완료**:** 설치중에소프트웨어업데이트가완료되었는지여부가사용자에게표시되지않습니다. iOS 14.0 에해당합니다.

ABM 계정이 설정 **> Apple** 배포프로그램에표시됩니다.

7. **macOS** 설정도우미옵션에서사용자가장치를처음으로시작할때 macOS 설정도우미가건너뛸단계를선택합니다. 화면을건너뛰면관련기능에는기본설정이사용됩니다. 건너뛴기능에대한액세스를완전히제한하지않는한사용자는설정이완료된후해당기능을구성할수있습니다. 기능액세스제한에대한자세한내용은 제한장치정책을참조하십시오. 모든항목에대한기본값은선택되어있지않습니다. 다음설명에서는설정선택시발생하는결과에대해설명합니다.



- 새장치로설정또는복원**:** 사용자가장치를새장치로또는 Time Machine 백업에서장치를설정하거나시스템마이그레이션을수행할수없습니다.
- 위치서비스**:** 사용자가장치에서위치서비스를설정할수없습니다. macOS 10.11 이상에해당합니다.
- **Apple ID:** 사용자가장치에대한관리형 Apple ID 계정을설정할수없습니다.

- 이용약관**:** 사용자가장치사용약관을읽고수락할수없습니다.
- **Siri:** 사용자가 Siri 를구성할수없습니다. macOS 10.12 이상에해당합니다.
- **FileVault:** FileVault 를사용하여시동디스크를암호화합니다. XenMobile 은 iCloud 에로그인한로컬사용자계정이하나인경우에만 FileVault 설정을적용합니다.

  macOS FileVault 디스크암호화기능으로시스템볼륨콘텐츠를암호화하여시스템볼륨을보호할수있습니다(https://support.apple.com/en-us/HT204837). FileVault 가꺼져있는최신휴대용 Mac 에서설정도우미를실행하면이기능을켜라는메시지가표시될수있습니다. 새시스템과 OS X 10.10 또는 10.11 로업그레이드한시스템에메시지가표시되지만시스템에로컬관리자계정이하나이고이계정으로 iCloud 에로그인한경우에만표시됩니다.
- 앱분석**:** 사용자가충돌데이터및사용현황통계를 Apple 과공유할지여부를설정할수없습니다.
- 개인정보보호**:** 사용자에게데이터및개인정보보호패널이표시되지않습니다. macOS 10.13 이상에해당합니다.
- **iCloud** 분석**:** 사용자가진단 iCloud 데이터를 Apple 에전송할지여부를선택할수없습니다. macOS 10.13 이상에해당합니다.
- **iCloud** 문서및데스크톱**:** 사용자가 iCloud 데스크톱및문서를설정할수없습니다. macOS 10.13 이상에해당합니다.
- 모양**:** 사용자가모양모드를선택할수없습니다. macOS 10.14 이상에해당합니다.
- 접근성**:** 사용자가 Voice Over 를자동으로들을수없습니다. 장치가이더넷에연결된경우에만사용할수있습니다. macOS 11 이상에해당합니다.
- 생체인식**:** 사용자가 Touch ID 및 Face ID 를설정할수없습니다. macOS 10.12.4 이상에해당합니다.
- **True Tone:** 사용자가 4 채널센서를설정해디스플레이의화이트밸런스를동적으로조정할수없습니다. macOS 10.13.6 이상에해당합니다.
- **Apple Pay:** 사용자가 Apple Pay 를설정할수없습니다. 이설정을선택취소하면사용자는 Touch ID 및 Apple ID 를설정해야합니다. **Apple ID** 및 생체인식설정이선택취소되었는지확인합니다. macOS 10.12.4 이상에해당합니다.
- 스크린타임**:** 사용자가스크린타임을활성화할수없습니다. macOS 10.15 이상에해당합니다.
- 로컬계정설정옵션**:** 장치에서관리자계정을만들때사용할설정을지정합니다. 사용자는이정보로 macOS 장치에로그인합니다. XenMobile 이지정된정보를사용하여계정을만듭니다.
  - 표준사용자로기본계정생성**:** 이사용자에게장치의관리자권한을부여하는대신 XenMobile 에서는표준권한이있는사용자를생성합니다. macOS 에는관리자계정이필요하므로 XenMobile 은관리자계정을먼저만든다음새표준계정을만들고기본으로설정합니다.
  - 관리자전체이름**:** 시스템에서관리자계정에대해표시할이름을입력합니다.
  - 관리자짧은이름**:** 장치에서홈폴더에간략하게표시할이름을입력합니다.
  - 관리자암호**:** 관리자계정의보안암호를입력합니다.

- 사용자및그룹의관리자계정표시**:** 지워질경우관리자계정은 macOS 설정의 관리자및그룹에나타나지않습니다. 기본계정을표준사용자로생성할경우이설정을사용하여 XenMobile 에서만든관리자계정을먼저숨깁니다.

배포프로그램사용장치주문

Apple 또는배포프로그램지원공인리셀러또는통신사에서직접배포프로그램지원장치를주문할수있습니다. Apple 에서주문하려면 Apple 배포프로그램포털에서 Apple 고객 ID 를제공합니다. 고객 ID 를통해구입한장치가 Apple 배포프로그램계정과연결될수있습니다.

리셀러또는이동통신사업자에서주문하려면 Apple 리셀러또는이동통신사업자에연락하여 Apple 배포프로그램에참여하는지여부를문의해야합니다. 장치를구입할때리셀러의 Apple 배포프로그램 ID 를요청하십시오. Apple 배포프로그램리셀러를 Apple 배포프로그램계정에추가할때이정보가필요합니다. 리셀러의 Apple 배포프로그램 ID 를추가한후배포프로그램고객 ID 를받게됩니다. 배포프로그램고객 ID 를리셀러에제공하면리셀러에서이 ID 를사용하여장치구매정보를 Apple 에제출합니다. 자세한내용은 Apple 사용장치등록사이트를참조하십시오.

배포프로그램지원장치관리

주문이배송되면 iOS, iPadOS 및 macOS 장치를 XenMobile Server 에연결할수있습니다.

1. 관리자또는장치등록관리자계정을사용하여 Apple Business Manager에로그인합니다.
2. 사이드바에서 장치를클릭합니다. Apple 에서직접구입한장치는자동으로표시됩니다. Apple Configurator 2 에서 Apple Business Manager 로장치를할당하려면 Apple Business Manager 사용자가이드를참조하십시오.
3. 목록에서장치또는총장치수를선택하고 장치관리편집을클릭합니다. 다음두가지옵션이있습니다.
   - MDM 서버에장치를할당하려면 서버에할당에서 XenMobile Server 의이름을선택합니다. **Continue(**계속**)** 을클릭합니다.
     새장치를 Apple Business Manager 에일괄할당하려면할당할기본 XenMobile Server 를설정합니다. 자세한내용은 일괄등록을위한기본서버설정을참조하십시오.
   - XenMobile Server 에서장치할당을취소하려면 할당취소를선택합니다.

이제 Apple 배포프로그램장치가선택한 XenMobile Server 에연결됩니다.

서비스를받기위해 iOS, iPadOS 또는 macOS 장치를보낼경우 Apple Business Manager 에서장치를제거해야합니다. 서비스를받은장치를다시받으면장치를 XenMobile Server 에다시할당해야합니다. 장치를교체할때주문번호를사용하여 XenMobile Server 에새장치를할당할수있습니다.

할당된장치의기록을검토하려면다음단계를따르십시오.

1. 관리자또는장치등록관리자계정을사용하여 Apple Business Manager에로그인합니다.
2. 사이드바에서 할당내역을클릭합니다. 그런다음할당을선택하여자세한정보를확인합니다.
3. 다운로드를클릭하여할당된장치와할당되지않은장치모두의일련번호가포함된 CSV 파일을다운로드합니다.

장치를판매했거나도난당했거나수리할수없는경우 Apple Business Manager 에서 iOS, iPadOS, macOS 장치를제거할수있습니다.

1. 관리자또는장치등록관리자계정을사용하여 Apple Business Manager에로그인합니다.
2. 사이드바에서 장치를클릭하고장치를검색합니다.
3. 장치를선택하고 장치해제를클릭합니다. 대화상자에서변경사항을확인하여프로그램에서장치를제거합니다. iOS 및 iPadOS 장치를다시추가하려면 Apple Configurator 2 를사용합니다. Apple Configurator 2 를사용하여 macOS 장치를다시추가할수없습니다.

장치등록

August 24, 2022

사용자장치를원격으로안전하게관리하기위해사용자장치를 XenMobile 에등록합니다. XenMobile 클라이언트소프트웨어가사용자장치에설치되며사용자의 ID 가인증됩니다. 그런다음 XenMobile 과사용자프로필이설치됩니다. 다음으로, XenMobile 콘솔에서장치관리작업을수행할수있습니다. 정책을적용하고, 앱을배포하고, 장치에데이터를푸시하고, 분실또는도난된장치를잠그고초기화하고찾을수있습니다.

iOS, Android, Windows 10 및 Windows 11 장치에서 Azure Active Directory 등록이지원됩니다. Azure 를 IDP(ID 공급자) 로구성하는방법에대한자세한내용은 Azure Active Directory 를 IDP 로 XenMobile 과통합을참조하십시오.

> 참고:
>
> iOS 장치사용자를등록하려면 APNs 인증서를요청해야합니다. 자세한내용은 인증서및인증을참조하십시오.

사용자및장치에대한구성옵션을업데이트하려면 관리 **>** 등록초대페이지로이동합니다. 자세한내용은이문서의등록초대보내기를 참조하십시오.

Android 장치

> 참고:
>
> Android Enterprise 장치등록에대한자세한내용은 Android Enterprise를참조하십시오.

1. Android 장치의 Google Play 스토어로이동하여 Citrix Secure Hub 앱을다운로드한후이앱을누릅니다.
2. 앱을설치할것인지묻는메시지가나타나면 다음을클릭한후 설치를클릭합니다.
3. Secure Hub 가설치된후에 **Open(**열기**)** 을누릅니다.
4. XenMobile Server 이름, UPN(사용자계정이름) 또는전자메일주소와같은회사자격증명을입력합니다. 그리고 **Next(**다음**)** 를클릭합니다.
5. **Activate device administrator(**장치관리자활성화**)** 화면에서 **Activate(**활성화**)** 를누릅니다.
6. 회사암호를입력한다음 **Sign On(**로그온**)** 을누릅니다.
7. XenMobile 이구성된방식에따라 Citrix PIN 을생성하라는메시지가나타날수있습니다. PIN 을사용하여 Secure Hub 및 Secure Mail 과 Citrix Files 등의다른 XenMobile 사용앱에로그온할수있습니다. Citrix PIN 을두번입력합니다. **Create Citrix PIN(Citrix PIN** 만들기**)** 화면에서 PIN 을입력합니다.
8. PIN 을다시입력합니다. Secure Hub 가열립니다. 이제 XenMobile Store 에액세스하여 Android 장치에설치할수있는앱을볼수있습니다.

9. 등록후앱을장치에자동으로푸시하도록 XenMobile 을구성한경우사용자에게앱을설치하라는메시지가나타납니다. 또한 XenMobile 에서구성한정책이장치에배포됩니다. 설치를눌러앱을설치합니다.

Android 장치를등록취소하고다시등록하려면

사용자가 Secure Hub 내에서등록을취소할수있습니다. 사용자가다음절차를사용하여등록을취소하는경우 XenMobile 콘솔의장치인벤토리에장치가계속나타납니다. 하지만장치에대한작업을수행할수없습니다. 장치를추적하고장치규정준수여부를모니터링할수없습니다.

1. Secure Hub 앱을눌러서엽니다.
2. 휴대폰인지태블릿인지에따라다음절차를수행합니다.

   휴대폰에서:

   - 화면왼쪽에서살짝밀어설정창을엽니다.
   - **Preferences(**기본설정**)**, **Accounts(**계정**)**, **Delete Account(**계정삭제**)** 를차례로누릅니다.

   태블릿에서:

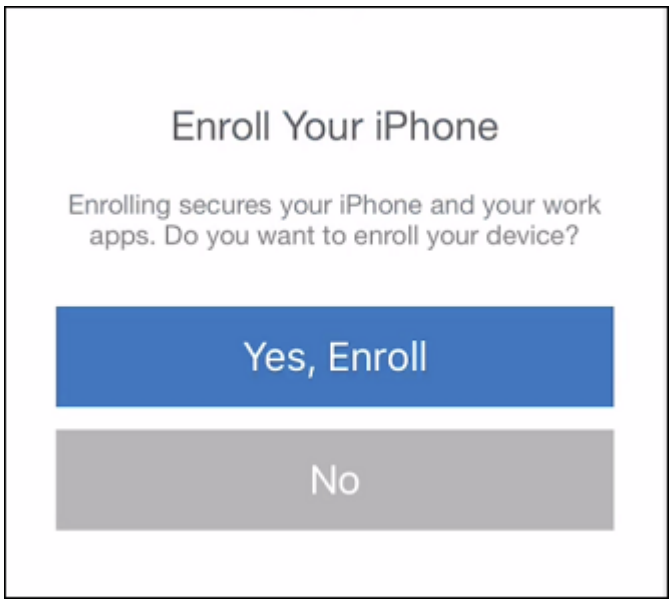
   - 오른쪽맨위의전자메일주소옆에있는화살표를누릅니다.
   - **Preferences(**기본설정**)**, **Accounts(**계정**)**, **Delete Account(**계정삭제**)** 를차례로누릅니다.
3. **Re-Enroll(**재등록**)** 을누릅니다. 장치를재등록할것인지확인하는메시지가표시됩니다.
4. 확인을누릅니다.

   장치가등록취소됩니다.
5. 화면의지침에따라장치를다시등록합니다.

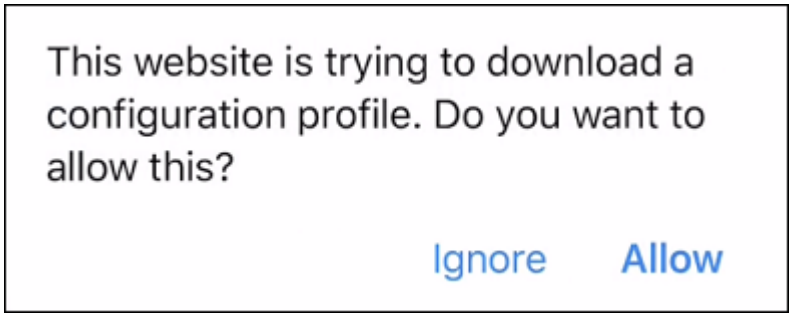
iOS 장치등록

이섹션에서는사용자가 iOS 장치 (12.2 이상) 를 XenMobile Server 에등록하는방법을보여줍니다. iOS 등록에대한자세한내용을보려면다음비디오를여십시오.

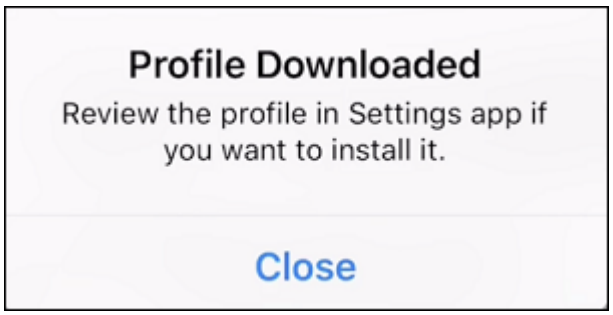
1. iOS 장치의 Apple Store 로이동하여 Citrix Secure Hub 앱을다운로드한후이앱을누릅니다.
2. 앱을설치하라는메시지가표시되면 다음을누른후 설치를누릅니다.
3. Secure Hub 가설치된후에 **Open(**열기**)** 을누릅니다.
4. XenMobile Server 이름, UPN(사용자계정이름) 또는전자메일주소와같은회사자격증명을입력합니다. 그리고 **Next(**다음**)** 를클릭합니다.
5. 예**,** 등록을눌러 iOS 장치를등록합니다.



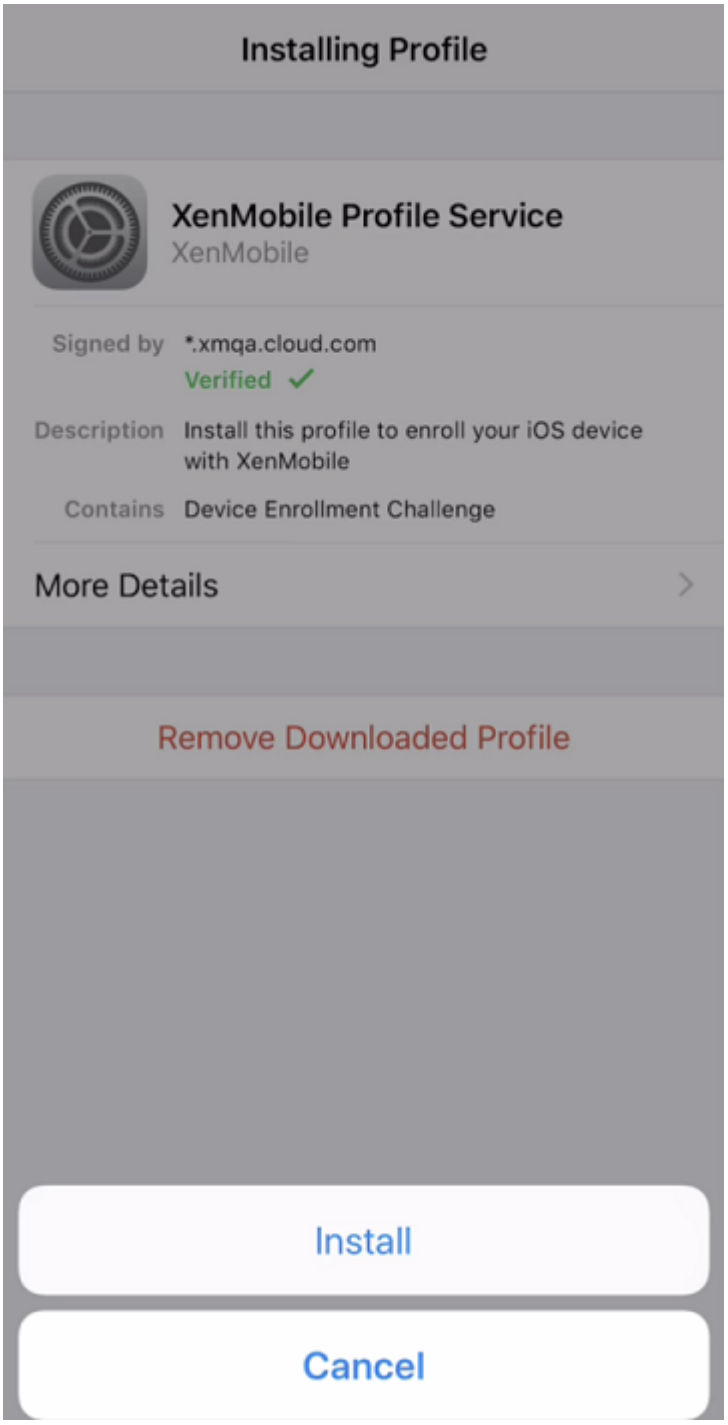
6. 자격증명을입력한후메시지가표시되면 허용을눌러구성프로필을다운로드합니다.



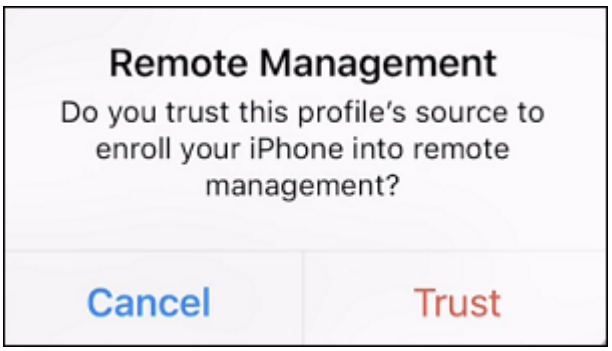
7. 구성프로필을다운로드한후 닫기를누릅니다.



8. 장치설정에서 iOS 인증서를설치하고장치를신뢰할수있는목록에추가합니다.
   - 설정 **>** 일반 **>** 프로필 **>** **XenMobile** 프로필서비스로이동하고 설치를눌러프로필을추가합니다.



- 알림창에서 신뢰를눌러장치를원격관리에등록합니다.



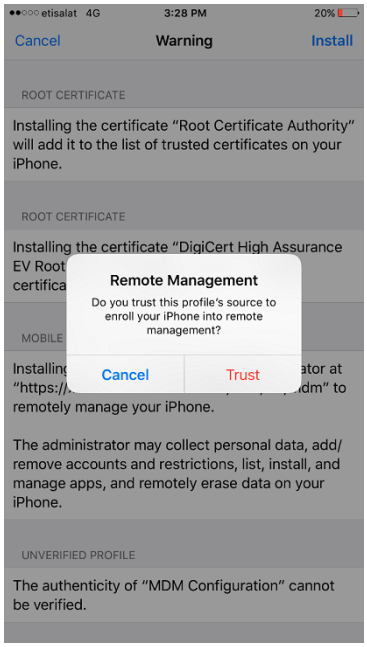
9. Secure Hub 에로그인합니다. MDM+MAM 에등록하는경우: 자격증명의유효성이확인된후메시지가표시되면 Citrix PIN 을만들고확인합니다.
10. 워크플로가완료되면장치가등록됩니다. 이제 App Store 에액세스하여 iOS 장치에설치할수있는앱을볼수있습니다.

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. 메시지가표시되면사용자이름과암호또는 PIN 을입력합니다. 다음을클릭합니다.
5. 등록하라는메시지가표시되면 **Yes, Enroll(**예**,** 등록**)** 을클릭하고메시지가표시되면자격증명을입력합니다.
6. 설치를눌러 Citrix Profile Services 를설치합니다.

7. 신뢰를누릅니다.



8. 열기를누르고자격증명을입력합니다.

macOS 장치

XenMobile 에서는 macOS 를실행하는장치를등록하는두가지방법을제공합니다. 두방법모두 macOS 사용자가장치에서직접온라인으로등록할수있습니다.

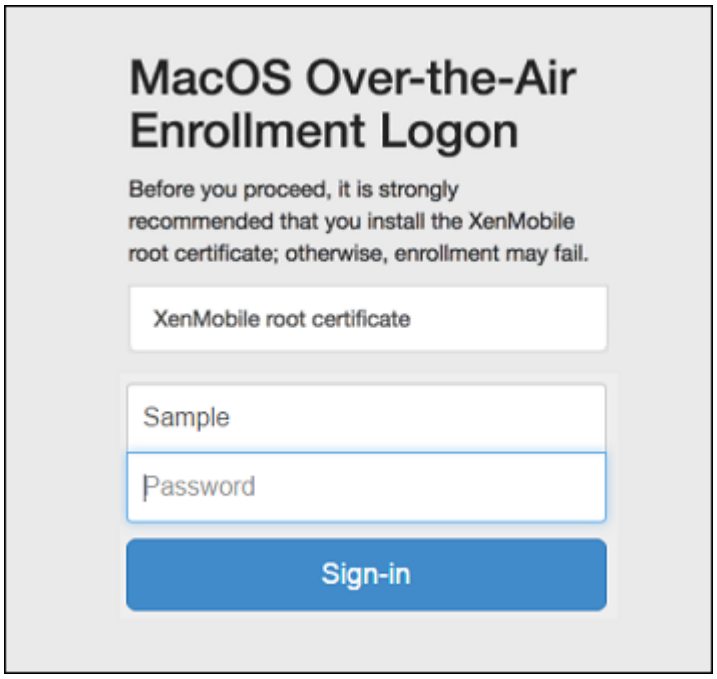
- 사용자에게등록초대보내기**:** 이등록방법을이용하면 macOS 장치에대해다음등록모드를설정할수있습니다.
  - 사용자이름 + 암호
  - 사용자이름 + PIN
  - 2 단계

  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 장치정책을참조하십시오.
2. macOS 사용자등록을위한초대를추가합니다. 자세한내용은이문서에서사용자에게등록초대보내기를참조하십시오.
3. 사용자가초대를수신하고링크를클릭하면다음화면이 Safari 브라우저에표시됩니다. XenMobile 이사용자이름을채웁니다. 등록보안모드를 **2** 단계로선택한경우다른필드가나타납니다.



4. 사용자는필요에따라인증서를설치합니다. 사용자에게인증서를설치할것인지묻는메시지가표시되는지여부는 macOS 에대해공개적으로신뢰할수있는 SSL 인증서와공개적으로신뢰할수있는디지털서명인증서를구성했는지여부에따라달라집니다. 인증서에대한자세한내용은 인증서및인증을참조하십시오.
5. 사용자가요청된자격증명을제공합니다.

   Mac 장치정책이설치됩니다. 이제모바일장치를관리하듯이 XenMobile 로 Mac 을관리할수있습니다.

사용자에게설치링크보내기

1. 필요에따라 XenMobile 콘솔에서 macOS 장치정책을설정합니다. 장치정책에대한자세한내용은 장치정책을참조하십시오.
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 인증서및인증을참조하십시오.
4. 사용자가자신의 Mac 에로그온합니다.

   Mac 장치정책이설치됩니다. 이제모바일장치를관리하듯이 XenMobile 로 Mac 을관리할수있습니다.

Windows 장치

Windows 10 및 Windows 11 장치는페더레이션된 Active Directory 인증수단으로 Azure 를사용하여등록됩니다. 다음방법중하나로 Windows 10 및 Windows 11 장치를 Microsoft Azure AD 에가입시킬수있습니다.

- 장치의전원을처음켤때 Azure AD 기본가입의일환으로 MDM 에등록합니다.
- 장치를구성한다음 Windows 설정페이지에서 Azure AD 가입의일환으로 MDM 에등록합니다.

XenMobile 에는다음 Windows 운영체제를실행하는장치를등록할수있습니다.

- Windows 10
- Windows 11

사용자가자신의장치를통해직접등록할수있습니다.

> 참고:
>
> Windows 10 RS2 휴대폰및태블릿의경우재등록시사용자에게서버 URL 을입력하라는메시지가표시되지않습니다. 이문제를해결하려면장치를다시시작하십시오. 또는전자메일주소화면에서 서비스에연결하는중맞은편에있는 X 를눌러서버

> URL 페이지로이동합니다. 이것은타사문제입니다.

관리자는지원되는 Windows 장치를관리할수있도록사용자등록에대한 Windows 검색서비스및자동검색을구성해야합니다.

Windows 장치사용자가 Azure 를사용하여등록할수있게하려면먼저 XenMobile 에서 Microsoft Azure 서버설정을구성해야합니다. 자세한내용은 Microsoft Azure Active Directory 서버설정을참조하십시오.

자체검색을사용하여 **Windows** 장치를등록하려면

Windows 장치관리를사용하려면자동검색서비스및 Windows 검색서비스를구성하는것이좋습니다. 자세한내용은 XenMobile 자동검색서비스를참조하십시오.

1. 장치에서사용가능한모든 Windows 업데이트를확인하고설치합니다.
2. 참메뉴에서 설정을누른후에 계정 **>** 회사또는학교액세스 **>** 회사또는학교에연결을누릅니다.
3. Windows 10 및 Windows 11 의경우: 회사이메일주소를입력한다음 계속을탭합니다. Windows 8.1 의경우: 장치관리사용을탭합니다. 로컬사용자로등록하려면올바른도메인이름을사용하여존재하지않는전자메일주소를입력합니다(예: `foo@mydomain.com`). 이를통해 Windows 의기본제공장치관리를통해등록이수행되는알려진 Microsoft 제한사항을바이패스할수있습니다. 서비스에연결중대화상자에서로컬사용자와연결된사용자이름및암호를입력합니다. 장치에서 XenMobile Server 가자동으로검색되고등록프로세스가시작됩니다.
4. 암호를입력합니다. XenMobile 의사용자그룹에속하는계정과연결된암호를사용합니다.
5. Windows 10 및 Windows 11 의경우: 사용약관대화상자에서장치가관리되는것에동의함을나타내고 동의를누릅니다. Windows 8.1 의경우: **IT** 관리자의앱및서비스허용대화상자에서장치가관리되는것에동의함을나타내고 켜기를누릅니다.

자체검색을사용하지않고 **Windows** 장치를등록하려면

자동검색을사용하지않고 Windows 장치를등록할수있습니다. 그러나자동검색을구성하는것이좋습니다. 자동검색을사용하지않고등록하면원하는 URL 에연결하기전에포트 80 이호출됩니다. 따라서이는프로덕션배포를위한최선의방법으로간주되지않습니다. 이프로세스는테스트환경과 POC 배포에서만사용하는것이좋습니다.

1. 장치에서사용가능한모든 Windows 업데이트를확인하고설치합니다.
2. Windows 10 및 Windows 11 의경우: 참메뉴에서 설정을누른후에 계정 **>** 회사또는학교액세스 **>** 회사또는학교에연결을누릅니다. Windows 8.1 의경우: **PC** 설정 **>** 네트워크 **>** 회사를누릅니다.
3. 회사전자메일주소를입력합니다.
4. Windows 10 및 Windows 11 의경우: 자동검색이구성되지않은경우 5 단계에설명된대로서버세부정보를입력할수있는옵션이표시됩니다. Windows 8.1 의경우: 자동으로서버주소검색이 켜짐으로설정된경우 꺼짐옵션을눌러서설정합니다.
5. Windows 10 및 Windows 11 의경우: 서버주소입력필드에 `https://serverfqdn:8443/serverInstance/wpe` 주소를입력합니다.

8443 이외의포트가인증되지않은 SSL 연결에사용된경우이주소에서 8443 대신해당포트번호를사용합니다.

Windows 8.1 의경우: `https://serverfqdn:8443/serverInstance/Discovery.svc` 형식으로서버주소를입력합니다.

8443 이외의포트가인증되지않은 SSL 연결에사용된경우이주소에서 8443 대신해당포트번호를사용합니다.

6. 암호를입력합니다.
7. Windows 10 및 Windows 11 의경우: 사용약관대화상자에서장치가관리되는것에동의함을나타내고 동의를누릅니다. Windows 8.1 의경우: **IT** 관리자의앱및서비스허용대화상자에서장치가관리되는것에동의함을나타내고 켜기를누릅니다.

등록초대보내기

XenMobile 콘솔에서 iOS, macOS, Android Enterprise 및레거시 Android 장치사용자에게등록초대를보낼수있습니다. 또한 iOS, Android Enterprise 또는레거시 Android 장치사용자에게설치링크도보낼수있습니다.

등록초대는다음과같이보냅니다.

- 한명의로컬사용자또는 Active Directory 사용자에게등록초대를보내는경우: 지정한휴대폰번호및통신회사이름의 SMS 를통해사용자에게초대가발송됩니다.
- 그룹에대한등록초대인경우: 사용자에게 SMS 로초대가발송됩니다. Active Directory 사용자에게 Active Directory 의전자메일주소및휴대폰번호가있는경우해당사용자는초대를받습니다. 로컬사용자는사용자속성에지정된전자메일및전화번호로초대를받습니다.

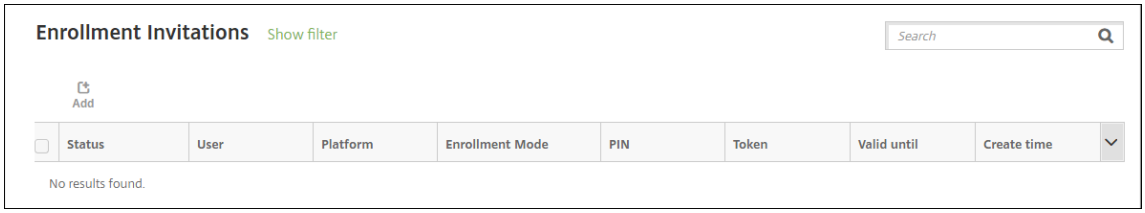
사용자가등록하면해당사용자의장치는 관리 **>** 장치에관리되는장치로표시됩니다. 초대 URL 의상태는 상환됨으로표시됩니다.

사전요구사항

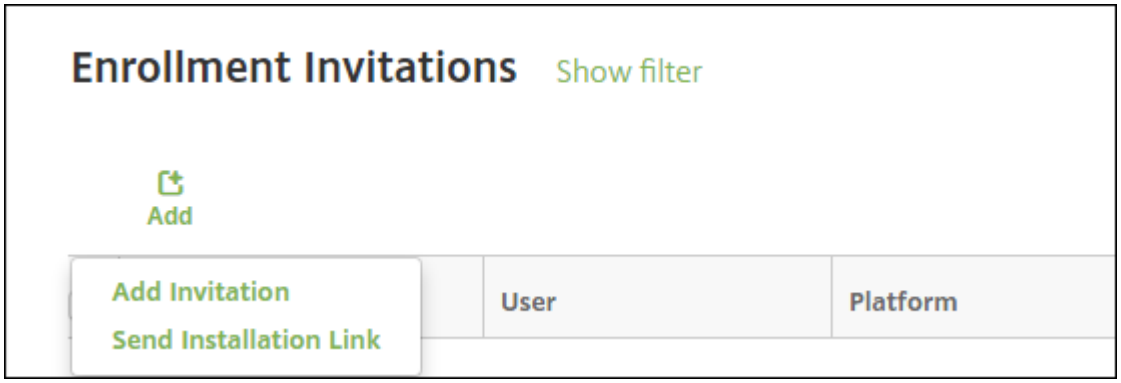
- 엔터프라이즈 (XME) 또는 MDM 모드로구성된 XenMobile Server
- 구성된 LDAP
- 로컬그룹및로컬사용자를사용중인경우:
  - 하나이상의로컬그룹.
  - 로컬그룹에할당된로컬사용자.
  - 배달그룹은로컬그룹과연결됩니다.
- Active Directory 를사용중인경우:
  - 배달그룹은 Active Directory 그룹과연결됩니다.

등록초대만들기

1. XenMobile 콘솔에서 관리 **>** 등록초대를클릭합니다. 등록초대페이지가나타납니다.



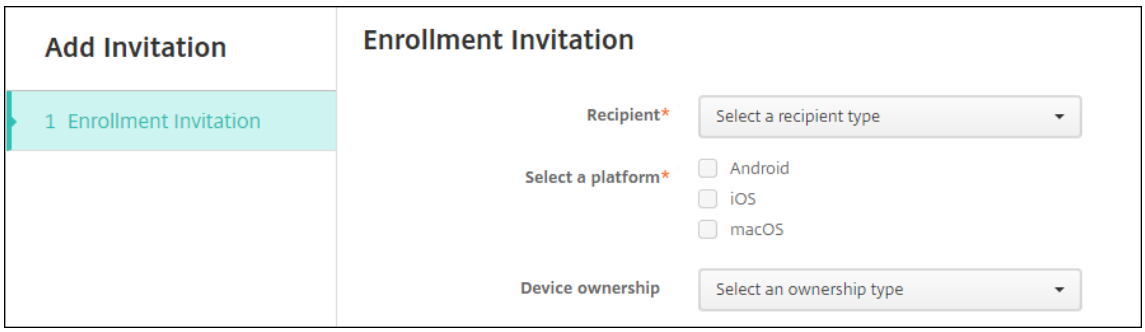
2. 추가를클릭합니다. 등록옵션메뉴가나타납니다.



- 사용자또는그룹에등록초대를보내려면 초대추가를클릭합니다.
- SMTP 또는 SMS 를통해받는사람목록에등록설치링크를보내려면 설치링크보내기를클릭합니다.

이후단계에서는등록초대및설치링크보내기에대해설명합니다.

3. 초대추가를클릭합니다. 등록초대화면이나타납니다.



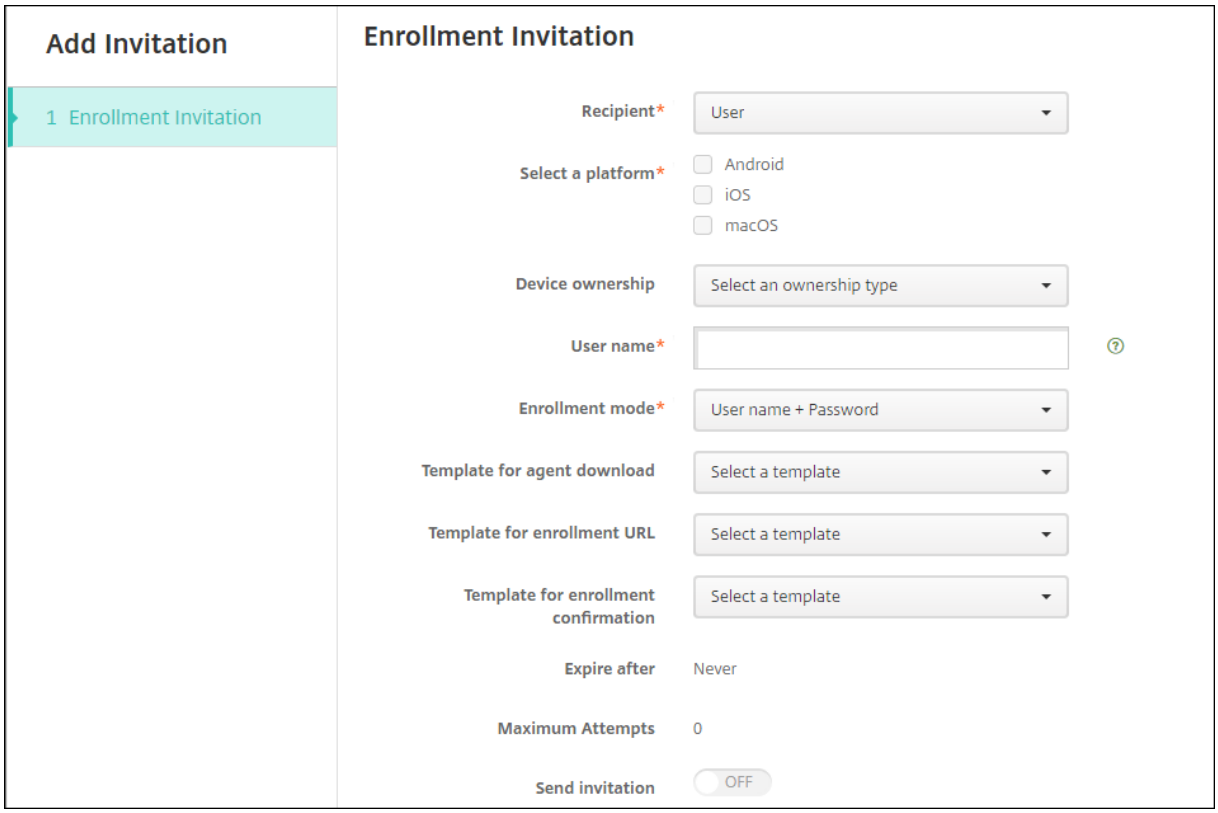
4. 다음설정을구성합니다.

- 받는사람**:** 그룹또는 사용자를선택합니다.
- 플랫폼선택**:** 받는사람이 그룹인경우모든플랫폼이선택됩니다. 플랫폼선택은변경할수있습니다. 받는사람이 사용자인경우플랫폼이선택되지않습니다. 플랫폼을선택합니다.

  Android Enterprise 장치에대한등록초대를만들려면 **Android > Android Enterprise** 를선택합니다.
- 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. 필요에따라사용자의전화번호를입력합니다.
   - 통신회사**:** 여러플랫폼을선택하거나 macOS 만선택한경우에는이설정이나타나지않습니다. 사용자의전화번호에연결할통신회사를선택합니다.
   - 등록모드**:** 사용자의등록보안모드를선택합니다. 기본값은 사용자이름 **+** 암호입니다. 일부플랫폼에서는다음옵션중일부를사용할수없습니다.
     - 사용자이름 + 암호
     - 높은수준의보안
     - 초대 URL
     - 초대 URL + PIN
     - 초대 URL + 암호
     - 2 단계
     - 사용자이름 + PIN

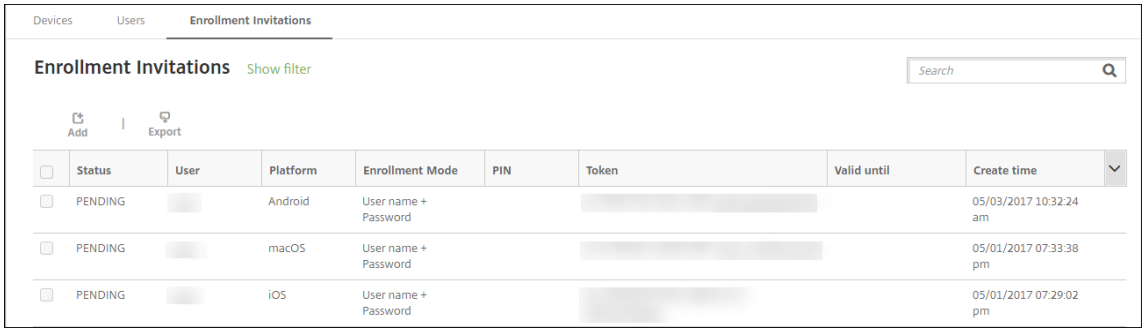
등록초대를보내기위해서는 초대 **URL**, 초대 **URL + PIN** 또는 초대 **URL +** 암호등록보안모드만사용할수있습니다. 사용자이름 **+** 암호, **2** 단계또는 사용자이름 **+ PIN** 으로등록하는장치의경우사용자는 Secure Hub 에서자격증명을수동으로입력해야합니다.

등록용 PIN 을일회용 PIN 이라고도합니다. 이러한 PIN 은사용자가등록할때만유효합니다.

> 참고**:**
>
> PIN 이포함된등록보안모드를선택하면 등록 **PIN** 용템플릿필드가나타납니다. 여기서 등록 **PIN** 을클릭합니다.

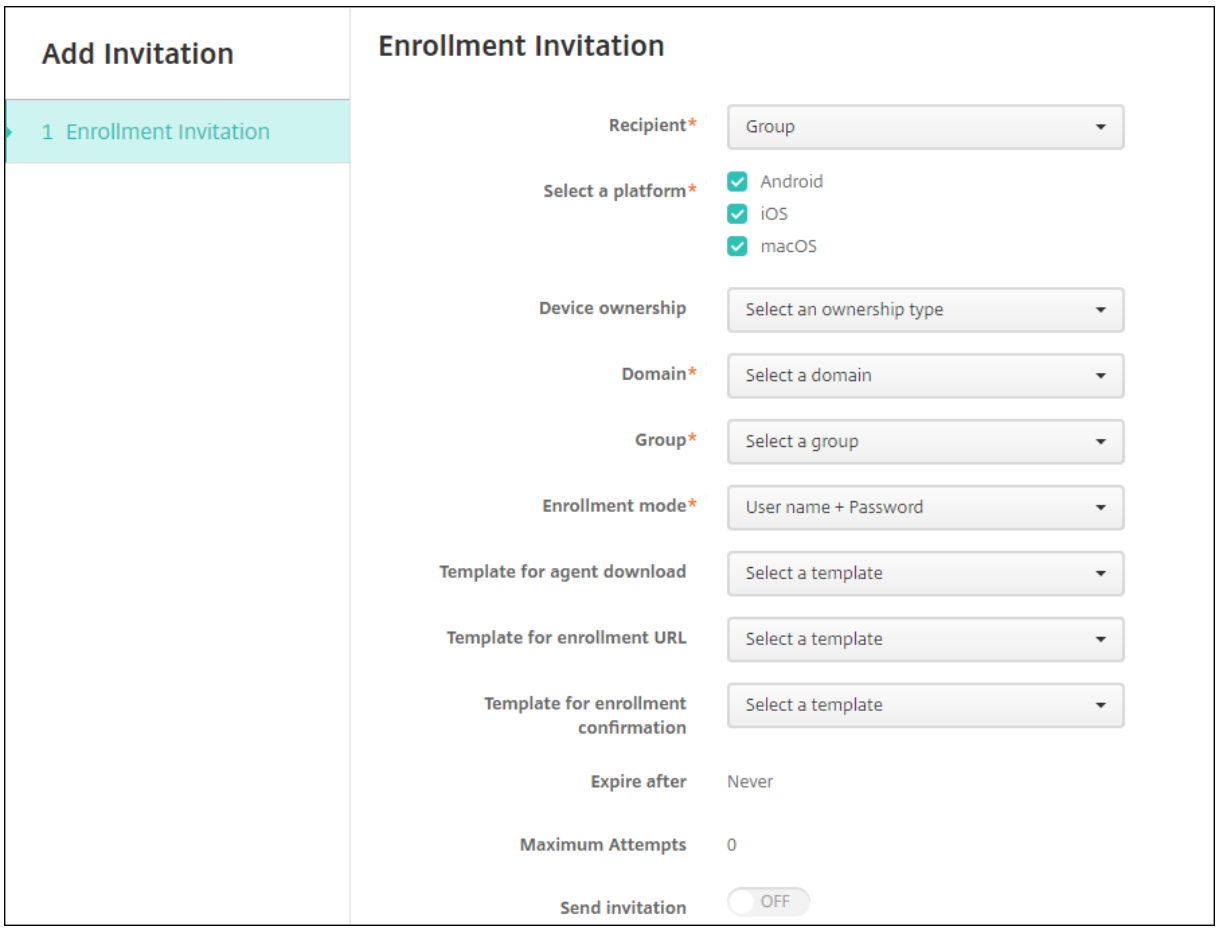
- 에이전트다운로드용템플릿**:** 다운로드링크라는이름의다운로드링크템플릿을선택합니다. 이템플릿은지원되는모든플랫폼용템플릿입니다.
- 등록 **URL** 용템플릿**:** 등록초대를선택합니다.
- 등록확인용템플릿**:** 등록확인을선택합니다.
- 다음이후에만료**:** 이필드는등록모드를구성한경우설정되며등록이만료되는시기를나타냅니다. 등록보안모드구성에대한자세한내용은 등록보안모드구성을참조하십시오.
- 최대시도횟수**:** 이필드는 등록모드를구성할때설정되며등록프로세스가진행되는최대횟수를나타냅니다. 등록보안모드구성에대한자세한내용은 등록보안모드구성을참조하십시오.
- 초대보내기**:** 초대를즉시보내려면 켜짐을선택합니다. 초대를 등록초대페이지의테이블에추가하되보내지않으려면 꺼짐을선택합니다.

2. 초대보내기를사용하도록설정한경우 저장및보내기를클릭합니다. 그렇지않은경우 저장을클릭합니다. 등록초대페이지의테이블에초대가표시됩니다.



그룹에등록초대를보내려면

다음그림에서는그룹에대한등록초대를구성하기위한설정을보여줍니다.



1. 다음설정을구성합니다.

   - 도메인**:** 초대를받을그룹의도메인을선택합니다.
   - 그룹**:** 초대를받을그룹을선택합니다.
   - 등록모드**:** 그룹의사용자를등록할방식을선택합니다. 기본값은 사용자이름 **+** 암호입니다. 일부플랫폼에서는다음옵션중일부를사용할수없습니다.
     - 사용자이름 + 암호
     - 높은수준의보안
     - 초대 URL
     - 초대 URL + PIN
     - 초대 URL + 암호
     - 2 단계
     - 사용자이름 + PIN

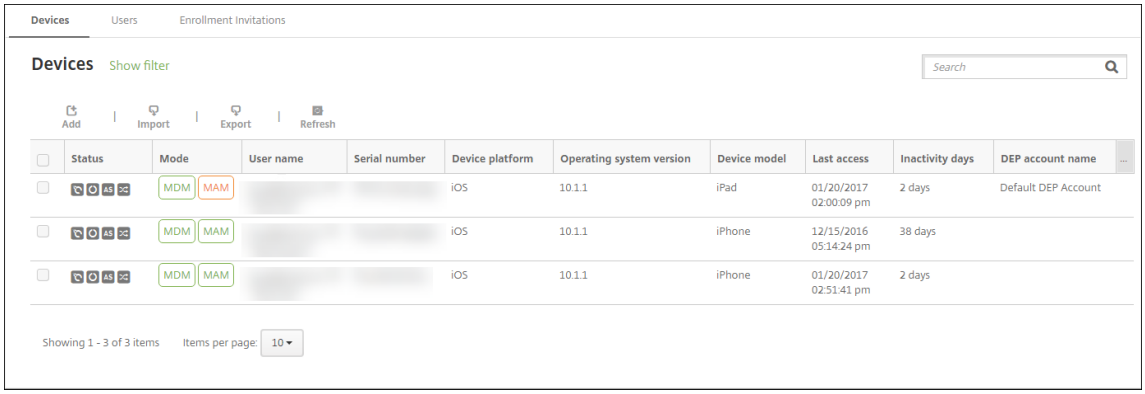
   등록초대를보내기위해서는 초대 **URL**, 초대 **URL + PIN** 또는 초대 **URL +** 암호등록보안모드만사용할수있습니다. 사용자이름 **+** 암호, **2** 단계또는 사용자이름 **+ PIN** 으로등록하는장치의경우사용자는 Secure Hub 에서자격증명을수동으로입력해야합니다.

   선택한각플랫폼에유효한등록보안모드만표시됩니다.

> 참고:
>
> PIN 이포함된등록보안모드를선택하면 등록 **PIN** 용템플릿필드가나타납니다. 여기서 등록 **PIN** 을클릭합니다.

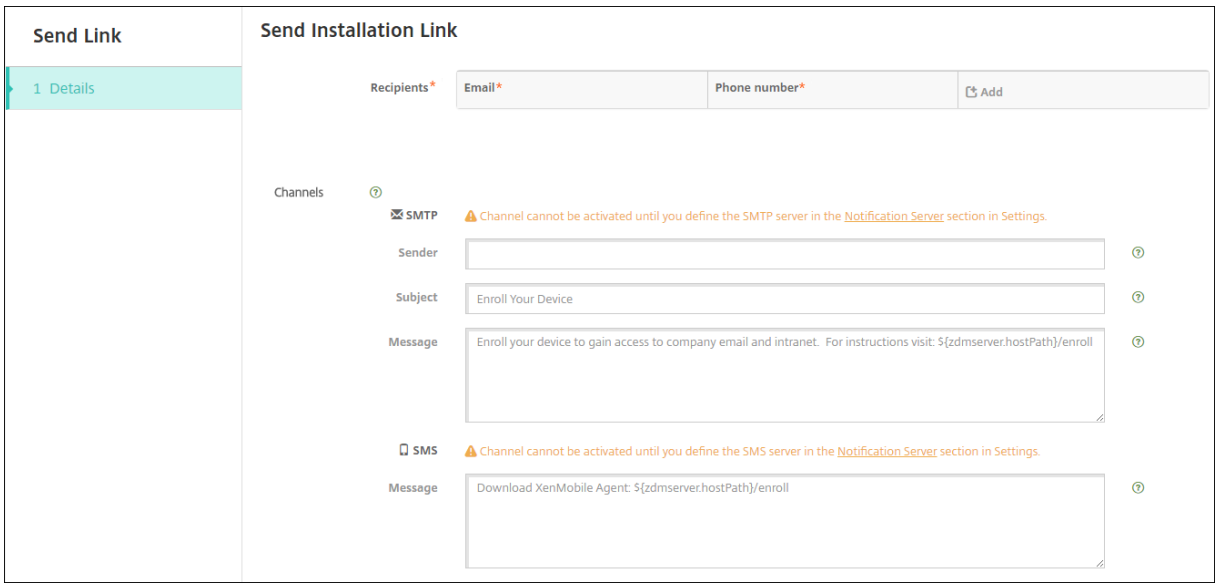
- 에이전트다운로드용템플릿: 다운로드링크: 라는이름의다운로드링크템플릿을선택합니다. 이템플릿은지원되는모든플랫폼용템플릿입니다.
- 등록 **URL** 용템플릿: 등록초대를선택합니다.
- 등록확인용템플릿: 등록확인을선택합니다.
- 다음이후에만료: 이필드는등록모드를구성한경우설정되며등록이만료되는시기를나타냅니다. 등록보안모드구성에대한자세한내용은 등록보안모드구성을참조하십시오.
- 최대시도횟수: 이필드는등록모드를구성할때설정되며등록프로세스가진행되는최대횟수를나타냅니다. 등록보안모드구성에대한자세한내용은 등록보안모드구성을참조하십시오.
- 초대보내기: 초대를즉시보내려면 켜짐을선택합니다. 초대를 등록초대페이지의테이블에추가하되보내지않으려면 꺼짐을선택합니다.

2. 초대보내기를사용하도록설정한경우 저장및보내기를클릭합니다. 그렇지않은경우 저장을클릭합니다. 등록초대페이지의테이블에초대가표시됩니다.



설치링크를보내려면

등록설치링크를보내기전에 설정페이지에서알림서버의채널 (SMTP 또는 SMS) 을구성해야합니다. 자세한내용은 알림을참조하십시오.



1. 다음설정을구성한후 저장을클릭합니다.

   - 받는사람**:** 추가하려는각받는사람에대해 추가를클릭한후다음작업을수행합니다.
     - 전자메일**:** 받는사람의전자메일주소를입력합니다. 이것은필수필드입니다.
     - 전화번호**:** 받는사람의전화번호를입력합니다. 이것은필수필드입니다.

     > 참고**:**
     >
     > 기존의받는사람을삭제하려면목록이포함된줄위로마우스포인터를이동한후오른쪽의휴지통아이콘을클릭합니다. 확인대화상자가나타납니다. 삭제를클릭하여목록을삭제하거나 취소를클릭하여목록을유지합니다.
     >
     > 기존의받는사람을편집하려면목록이포함된줄위로마우스포인터를이동한후오른쪽의펜아이콘을클릭합니다. 목록을업데이트한후 저장을클릭하여변경된목록을저장하거나 취소를클릭하여목록을변경되지않은상태로유지합니다.

   - 채널**:** 등록설치링크를보내는데사용할채널을선택합니다. **SMTP** 또는 **SMS** 를통해알림을보낼수있습니다. 설정 페이지의 알림서버에서서버설정을구성할때까지이러한채널을활성화할수없습니다. 자세한내용은 알림을참조하십시오.
   - **SMTP:** 다음과같은선택적설정을구성합니다. 이러한필드에아무것도입력하지않으면선택한플랫폼에구성된알림템플릿에지정되어있는기본값이사용됩니다.
     - 보낸사람**:** 선택적보낸사람을입력합니다.
     - 제목**:** 선택적메시지제목을입력합니다. 예를들어, “장치를등록하십시오.” 를사용할수있습니다.
     - 메시지**:** 받는사람에게보낼선택적인메시지를입력합니다. 예를들어 “조직의앱과전자메일에대한액세스권한을얻으려면장치를등록하십시오.” 를사용할수있습니다.
   - **SMS:** 다음설정을구성합니다. 이필드에아무것도입력하지않으면선택한플랫폼에구성된알림템플릿에지정되어있는기본값이사용됩니다.
     - 메시지**:** 받는사람에게보낼메시지를입력합니다. 이필드는 SMS 기반알림에필요합니다.

> 참고: 북미지역의경우 160 자를초과하는 SMS 메시지는여러메시지로배달됩니다.

2. **Send(**보내기**)** 를클릭합니다.

> 참고:
>
> 해당환경에서 sAMAccountName 을사용하는경우초대를받고링크를클릭한사용자가사용자이름을편집해야인증이완료됩니다. 사용자이름은 sAMAccountName@domainname.com 의형식으로표시됩니다. 사용자는 @domainname.com 부분을제거해야합니다.

플랫폼별등록보안모드

다음표에는사용자장치를등록하는데사용할수있는보안모드가나와있습니다. 표에서 예는등록프로필이다른특정등록및관리모드를지원하는장치플랫폼을나타냅니다.

MDM 등록보안모드	Citrix Gateway 의 MAM 등록보안모드	관리모드	다양한 등록프로필지원	Android(레거시)	Android Enterprise	iOS(사용자등록모드)	iOS	macOS	Windows
Citrix Cloud 를통한 ID 공급자로서의 Azure AD 및 Okta	클라이언트인증서	MDM+MA 또는 MDM	예	예	예	예	예	아니요	아니요

MDM 등록보안모드	Citrix Gateway 의 MAM 등록보안모드	관리모드	다양한 등록프로필지원	Android(레거시)	Android Enterprise	iOS(사용자등록모드)	iOS	macOS	Windows
사용자 이름 + 암호	LDAP, LDAP+ 클라이언트인증서및 클라이언트인증서만	MDM+MAM, MDM 또는 MAM(MAM 전용모드는 Citrix Gateway 에서클라이언트인증서를지원하지않음)	예	예	예	예	예	예	예
초대 URL	클라이언트인증서	MDM+MAM 또는 MDM	예	예	예	아니요	예	아니요	아니요
초대 URL + PIN	클라이언트인증서	MDM+MAM 또는 MDM	예	예	예	아니요	예	아니요	아니요
초대 URL + 암호	LDAP, LDAP+ 클라이언트인증서및 클라이언트인증서만	MDM+MAM 또는 MDM	예	예	예	아니요	예	아니요	아니요

MDM 등록보안모드	Citrix Gateway 의 MAM 등록보안모드	관리모드	다양한 등록프로필지원	Android(레거시)	Android Enterprise	iOS(사용자등록모드)	iOS	macOS	Windows
2 단계인증 (사용자이름 + 암호 + PIN)	LDAP, LDAP+클라이언트인증서및클라이언트인증서만	MDM+MAM 또는 MDM	예	예	예	아니요	예	예	아니요
사용자이름 + PIN	클라이언트인증서	MDM+MAM 또는 MDM	예	예	예	아니요	예	예	아니요

다음은 iOS, Android 및 Android Enterprise 장치에서등록보안모드가작동하는방식에대해설명합니다.

- **User name +** 암호 (기본값)
  - 사용자에게등록 URL 이포함된단일알림을보냅니다. 사용자가 URL 을클릭하면 Secure Hub 가열립니다. 그런다음사용자가사용자이름과암호를입력하여 XenMobile 에장치를등록합니다.
- 초대 **URL**
  - 사용자에게등록 URL 이포함된단일알림을보냅니다. 사용자가 URL 을클릭하면 Secure Hub 가열립니다. XenMobile 서버이름및 예**,** 등록하겠습니다단추가나타납니다. 사용자가 예**,** 등록하겠습니다를탭하여 XenMobile 에장치를등록합니다.
- 초대 **URL + PIN**
  - 사용자에게다음전자메일을보냅니다.
    - 등록 URL 이포함된전자메일로, 여기에서사용자는 Secure Hub 를통해 XenMobile 에장치를등록할수있습니다.
    - 전자메일에는장치를등록할때사용자가입력해야하는일회용 PIN 과사용자의 Active Directory(또는로컬)암호가포함되어있습니다.
  - 이모드에서는사용자가알림에있는등록 URL 을사용해야만등록할수있습니다. 사용자가알림초대를분실하면등록할수없습니다. 하지만다른초대장을보낼수있습니다.
- 초대 **URL +** 암호
  - 사용자에게등록 URL 이포함된단일알림을보냅니다. 사용자가 URL 을클릭하면 Secure Hub 가열립니다. 사용자가암호를입력할수있는필드와함께 XenMobile 서버이름이나타납니다.
- **2** 단계

  - 사용자에게등록 URL 과일회용 PIN 이포함된단일알림을보냅니다. 사용자가 URL 을클릭하면 Secure Hub 가열립니다. 사용자가암호및 PIN 번호를입력할수있는두개의필드와함께 XenMobile 서버이름이나타납니다.
- 사용자이름 **+ PIN**
  - 사용자에게다음전자메일을보냅니다.
    * 등록 URL 이포함된전자메일로, 여기에서사용자는 Secure Hub 를다운로드하여설치할수있습니다. Secure Hub 가열리면사용자이름과암호를입력하여 XenMobile 에장치를등록하라는메시지가표시됩니다.
    * 전자메일에는장치를등록할때사용자가입력해야하는일회용 PIN 과사용자의 Active Directory(또는로컬) 암호가포함되어있습니다.
  - 사용자가알림초대를분실하면등록할수없습니다. 하지만다른초대장을보낼수있습니다.

다음은 macOS 장치에서등록보안모드가작동하는방식에대해설명합니다.

- 사용자이름 **+** 암호
  - 사용자에게등록 URL 이포함된단일알림을보냅니다. 사용자가 URL 을클릭하면 Safari 브라우저가열립니다. 로그인페이지가나타나고 XenMobile 에장치를등록하려면사용자이름과암호를입력하라는메시지가표시됩니다.
- **2** 단계
  - 사용자에게등록 URL 과일회용 PIN 이포함된단일알림을보냅니다. 사용자가 URL 을클릭하면 Safari 브라우저가열립니다. 사용자가암호와 PIN 번호를입력할수있는두개의필드가표시된로그인페이지가나타납니다.
- 사용자이름 **+ PIN**
  - 사용자에게다음전자메일을보냅니다.
    * 등록 URL 이포함된전자메일입니다. 사용자가 URL 을클릭하면 Safari 브라우저가열립니다. 로그인페이지가나타나고 XenMobile 에장치를등록하려면사용자이름과암호를입력하라는메시지가표시됩니다.
    * 전자메일에는장치를등록할때사용자가입력해야하는일회용 PIN 과사용자의 Active Directory(또는로컬) 암호가포함되어있습니다.
  - 사용자가알림초대를분실하면등록할수없습니다. 하지만다른초대장을보낼수있습니다.

Windows 장치에는등록초대를보낼수없습니다. Windows 사용자는장치를통해직접등록할수있습니다.

Firebase Cloud Messaging

January 5, 2022

> 참고**:**
>
> FCM(Firebase Cloud Messaging) 은이전의 GCM(Google Cloud Messaging) 입니다. 일부 XenMobile 콘솔레이블및메시지에는 GCM 용어가사용됩니다.

FCM(Firebase Cloud Messaging) 을사용하여 Android 장치의 XenMobile 연결방법및시기를제어하는것이좋습니다. FCM 에구성된 XenMobile 은 FCM 을사용하도록설정된 Android 장치에연결알림을전송합니다. 모든보안동작또는배포명령이실행되면사용자에게 XenMobile 서버에다시연결하라는메시지를표시하는푸시알림이트리거됩니다.

이문서의구성단계를완료하고장치를체크인하면장치가 XenMobile Server 의 FCM 서비스에등록됩니다. 이연결은 FCM 을사용하여 XenMobile Service 에서장치로거의실시간통신을가능하게합니다. FCM 등록은새로운장치등록및이전에등록된장치에서작동합니다.

장치에대한연결을시작해야하는 XenMobile 이 FCM 서비스에연결하면 FCM 서비스가연결알림을장치에제공합니다. 이유형의연결은 Apple 이푸시알림서비스에사용하는연결과유사합니다.

사전요구사항

- 최신 Secure Hub 클라이언트
- Google 개발자계정자격증명
- FCM 지원 Android 장치에설치된 Google Play 서비스

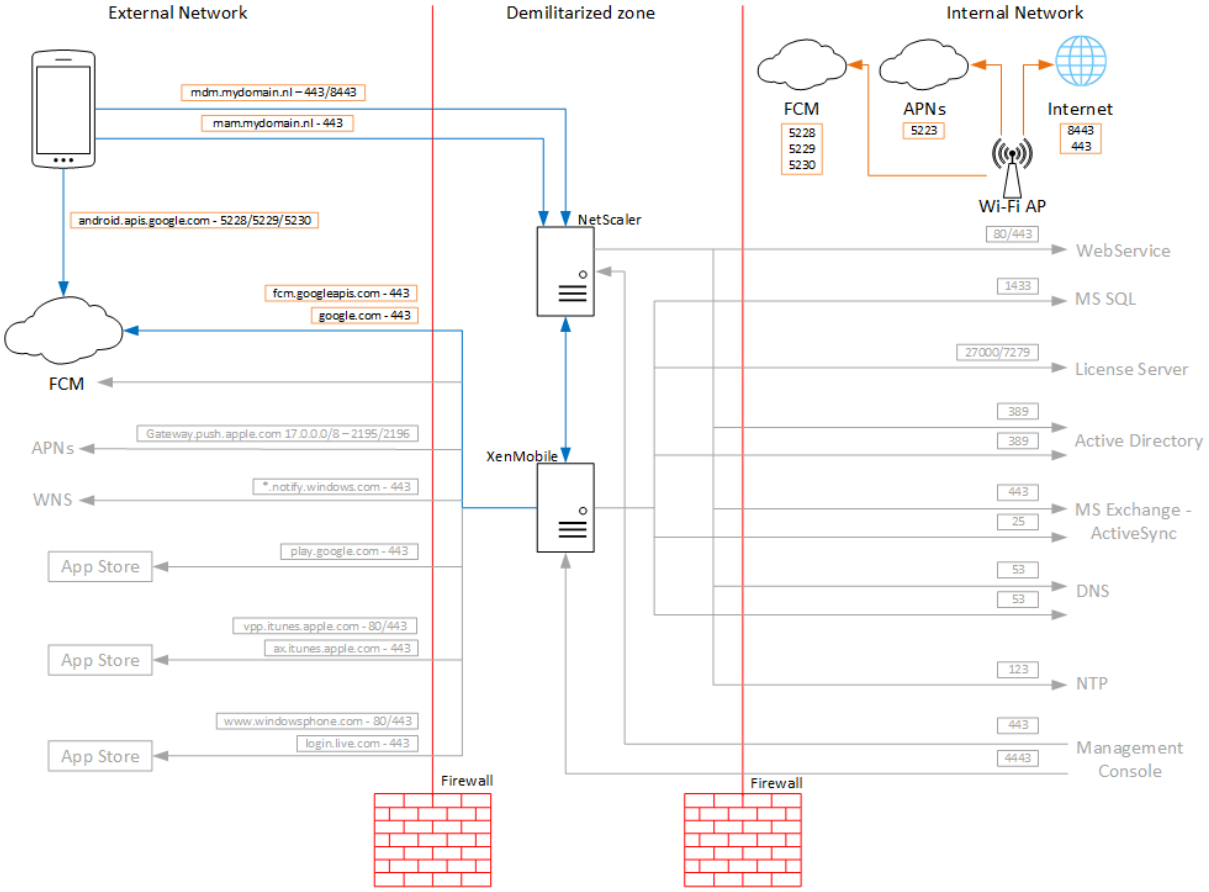
방화벽포트

- XenMobile 에서 `fcm.googleapis.com` 및 `Google.com`에대해포트 443 을엽니다.
- 장치 Wi-Fi 에서나가는인터넷통신을위해포트 5228, 5229 및 5230 을엽니다.
- 나가는연결을허용하려면 IP 제한없이포트 5228~5230 을허용하는것이좋습니다. IP 제한이필요한경우에는 IPv4 및 IPv6 블록의모든 IP 주소를허용하는것이좋습니다. 이러한블록은 Google ASN of 15169에나와있습니다. 해당목록을매월업데이트하십시오.

자세한내용은 포트요구사항을참조하십시오.

아키텍처

이다이어그램은외부및내부네트워크의 FCM 에대한통신흐름을보여줍니다.

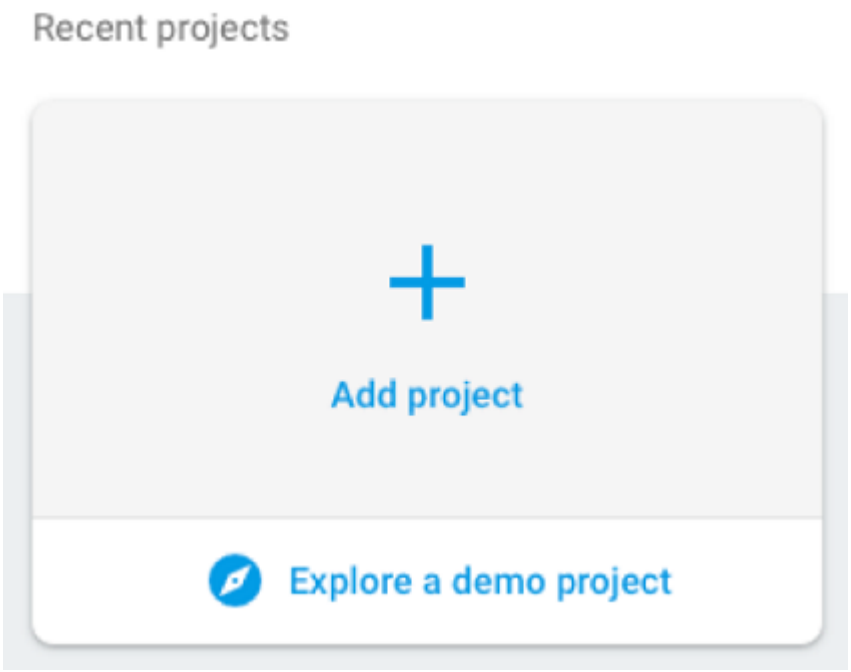


FCM 에대해 **Google** 계정을구성하려면

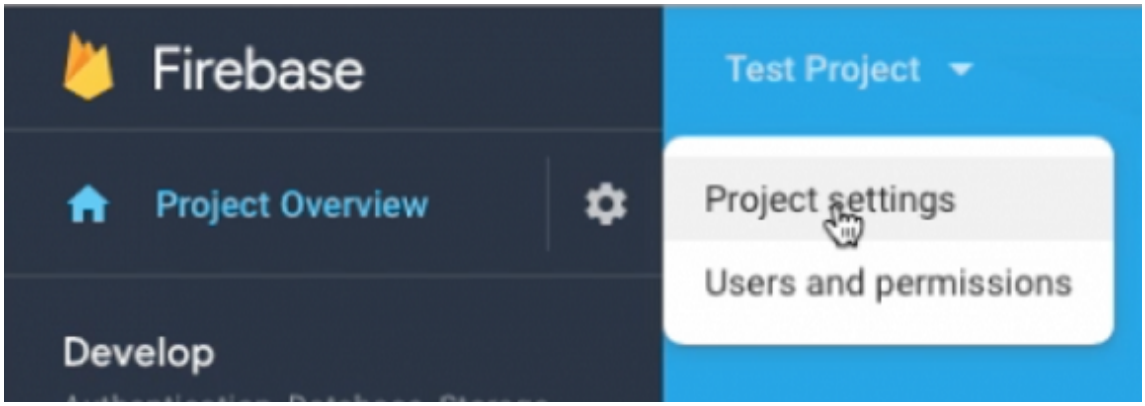
1. Google 개발자계정자격증명을사용하여다음 URL 에로그인합니다.

   https://console.firebase.google.com/

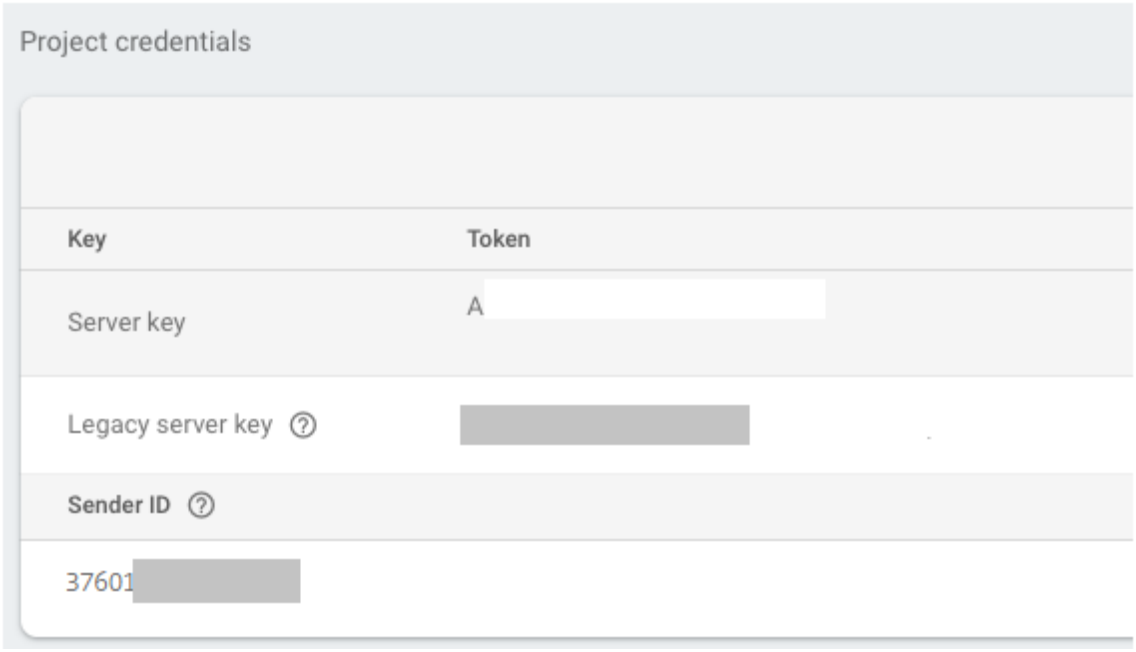
2. **Add project(**프로젝트추가**)** 를클릭합니다.



3. 프로젝트를만든후 **Project settings(**프로젝트설정**)** 를클릭합니다.



4. **Cloud Messaging(**클라우드메시징**)** 탭을클릭합니다. **Server key(**서버키**)** 와 **Sender ID(**보낸사람 **ID)** 값을복사합니다. 다음절차에서 XenMobile 콘솔에이러한값을붙여넣습니다. 2016 년 10 월부터는 Firebase 콘솔에서서버키를만들어야합니다.

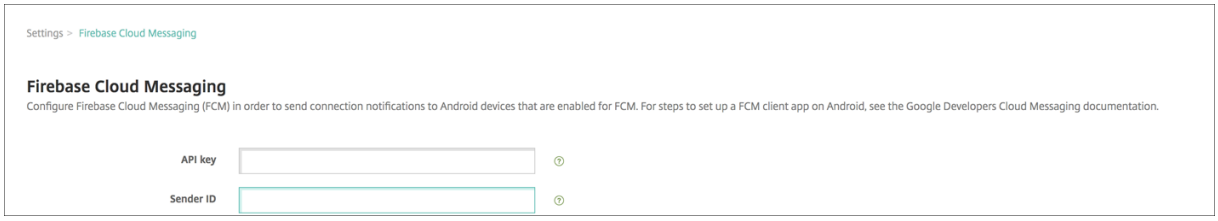


Android 에서 FCM 클라이언트앱을설정하는단계는이 Google Developers Cloud Messaging 문서 (https://firebase.google.com/docs/cloud-messaging/android/client) 를참조하십시오.

XenMobile 을 FCM 에대해구성하려면

XenMobile 콘솔에서 설정 **> Firebase Cloud Messaging** 으로이동합니다.

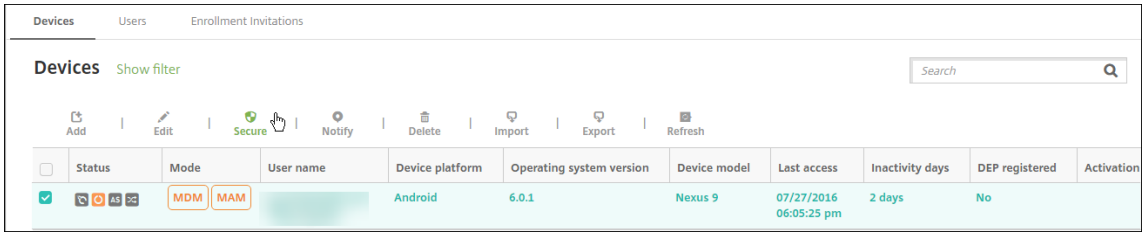
- **API** 키를편집하고 Firebase Cloud Messaging 구성마지막단계에서복사한 Firebase Cloud Messaging 서버 키를입력합니다.
- 보낸사람 **ID** 를편집하고이전절차에서복사한 보낸사람 **ID** 값을입력합니다.



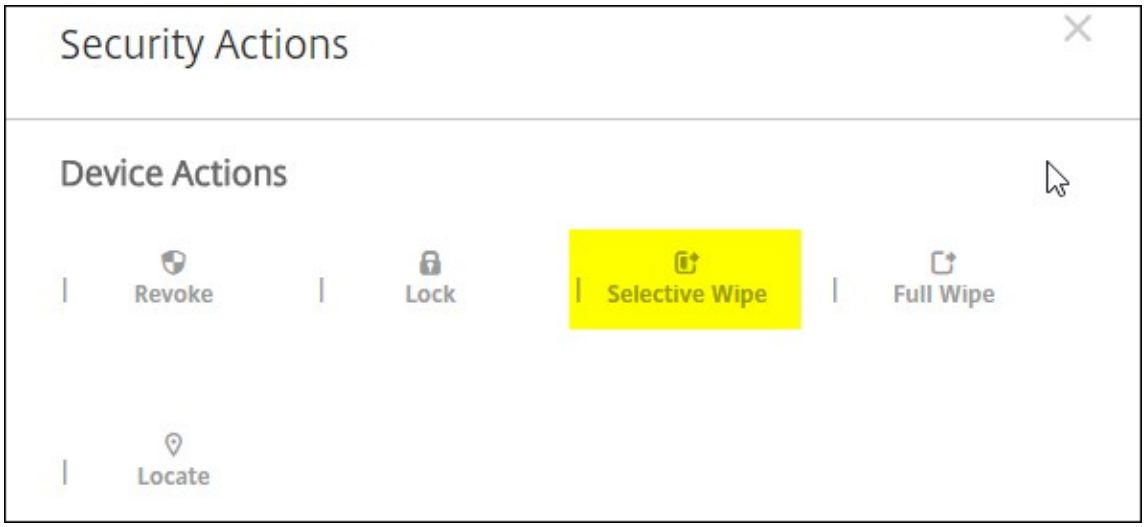
설정을완료한후예약장치정책을제거하거나해당정책을변경하여연결빈도를줄일수있습니다.

구성을테스트하려면

1. Android 장치를등록합니다.
2. XenMobile 에서연결이끊기도록장치를유휴상태로잠시둡니다.
3. XenMobile 콘솔에로그인하고 관리를클릭하고 Android 장치를선택한후 보안을클릭합니다.



4. 장치동작에서 선택적초기화를클릭합니다.



구성이성공적인경우장치에서선택적초기화가수행됩니다.

Apple 교육기능과통합

January 5, 2022

Apple 교육을사용하는환경에서 XenMobile 을 MDM(모바일기기관리) 솔루션으로사용할수있습니다. XenMobile 지원에는 Apple School Manager(ASM) 및 iPad 용 Classroom 앱이포함됩니다. XenMobile 교육구성장치정책은 Apple 교육을사용할강사및학생장치를구성합니다.

사전구성을마친감독되는 iPad 를강사와학생에게제공하십시오. 이구성에는 XenMobile 의 ASM 등록, 새암호로구성된관리되는 Apple ID 계정과필수볼륨구매앱및 iBooks 가포함됩니다.

다음은 Apple 교육기능에대한 XenMobile 의주요지원입니다.

Apple School Manager

ASM 은교육기관에서사용되는 iOS(iPadOS) 장치와 macOS 노트북을설정, 배포및관리할수있도록하는서비스입니다. ASM 에는 IT 관리자가다음을수행할수있는웹기반포털이포함되어있습니다.

- Apple 배포프로그램장치를여러 MDM 서버에할당합니다.

- 앱및 iBooks 를위한볼륨구매라이센스를구매합니다.
- 관리되는 **Apple ID** 를대량으로생성합니다. 이사용자지정된 Apple ID 를사용하면 Apple 서비스에액세스하여 iCloud Drive 에문서를저장하고 Apple App Store 교육과정에등록하는등의작업을수행할수있습니다.

여러개의 ASM 계정을 XenMobile 에추가할수있습니다. 예를들어이기능을사용하면서로다른등록설정및설정도우미옵션을교육단위또는부서별로사용할수있습니다. 그런다음 ASM 계정을여러장치정책에연결할수있습니다.

ASM 계정을 XenMobile 콘솔에추가하면 XenMobile 이클래스및명단정보를검색합니다. 장치설정시 XenMobile 은다음을수행합니다.

- 장치를등록합니다.
- 배포에구성된리소스를설치합니다 (예: 장치정책, 교육구성, 홈화면레이아웃등).
- 볼륨구매를통해구매한앱과 iBooks 를설치합니다.

사전구성을마친장치를강사와학생에게제공합니다. 분실또는도난장치의경우 MDM 분실모드기능을사용하여장치를잠그고찾을수있습니다.

iPad 용 Classroom 앱

iPad 용 Classroom 앱은강사가학생장치에연결하여관리할수있도록합니다. 장치화면을보고, iPad 에서앱을열고, 웹링크를공유하고열수있습니다.

Classroomp 은 App Store 에서무료로사용할수있습니다. XenMobile 콘솔에앱을업로드한다음교육구성장치정책을사용하여강사장치에배포할 Classroom 앱을구성합니다.

Apple 교육기능에대한자세한내용은 Apple 교육 사이트와같은사이트의 Apple 교육배포가이드를참고하십시오.

사전요구사항

- Citrix Gateway
- MDM+MAM 에대해구성된교육프로필
- Apple iPad 3 세대 (최소버전) 또는 iPad Mini(iOS 9.3 이상)

> 참고:
>
> XenMobile 은 LDAP 또는 Active Directory 에대해 ASM 사용자계정을검사하지않습니다. 그러나 XenMobile 을 LDAP 또는 Active Directory 에연결하여 ASM 강사나학생과관련되지않는사용자및장치를관리할수있습니다. 예를들어 Active Directory 를사용하여 Secure Mail 및 Secure Web 을다른 ASM 구성원 (예: IT 관리자) 에게제공할수있습니다.
>
> ASM 강사및학생은로컬사용자이므로 Citrix Secure Hub 를강사및학생의장치에배포할필요가없습니다.
>
> Citrix Gateway 인증이포함되는 MAM 등록은로컬사용자를지원하지않습니다 (Active Directory 사용자만지원). 따라서 XenMobile 은필수볼륨구매앱과 iBooks 만강사와학생의장치에배포합니다.

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** 구성

Apple 또는 Apple 공인리셀러/통신사를통해 iPad 를구입한후이섹션의워크플로에따라 ASM 계정및장치를설정하십시오. 이 워크플로에는 ASM 포털과 XenMobile 콘솔에서수행하는단계가포함되어있습니다.

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, 교육기관을 ASM 으로업그레이드를참조하십시오. ASM 계정을생성하려면 https://school.apple.com/으로이동하고지침에따라등록합니다. ASM 에처음로그인하면설정도우미가열립니다.

- Apple School Manager 사전요구사항, 설정도우미및관리작업에대한자세한내용은 Apple School Manager 사용자가이드를참조하십시오.
- ASM 을설정할때는 Active Directory 도메인이름과다른도메인이름을사용합니다. 예를들어 ASM 도메인이름에 `appleid` 같은접두사를추가합니다.
- ASM 을명단데이터에연결하면 ASM 이강사및학생이사용할, 관리되는 Apple ID 를생성합니다. 명단데이터에는강사, 학생및클래스가포함됩니다. ASM 에명단데이터추가에대한자세한정보는앞서참고했던 ASM 사용자가이드에서확인하십시오.
- 앞서참고했던 ASM 사용자가이드의설명에따라관리되는 Apple ID 형식을해당교육기관에맞게사용자지정할수있습니다.

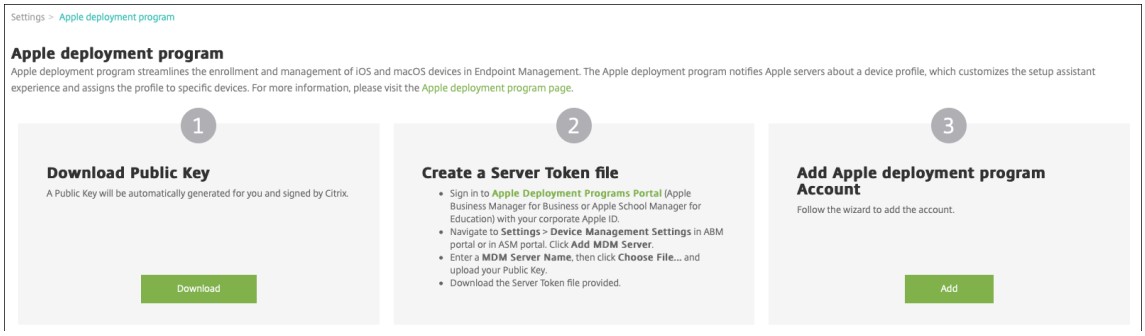
  > 중요**:**
  >
  > ASM 정보를 XenMobile 로가져온후에는관리되는 Apple ID 를변경하지마십시오.

- 리셀러또는통신사를통해장치를구매한경우이러한장치를 ASM 에연결합니다. 자세한정보는앞서참고했던 ASM 사용자가이드에서확인하십시오.

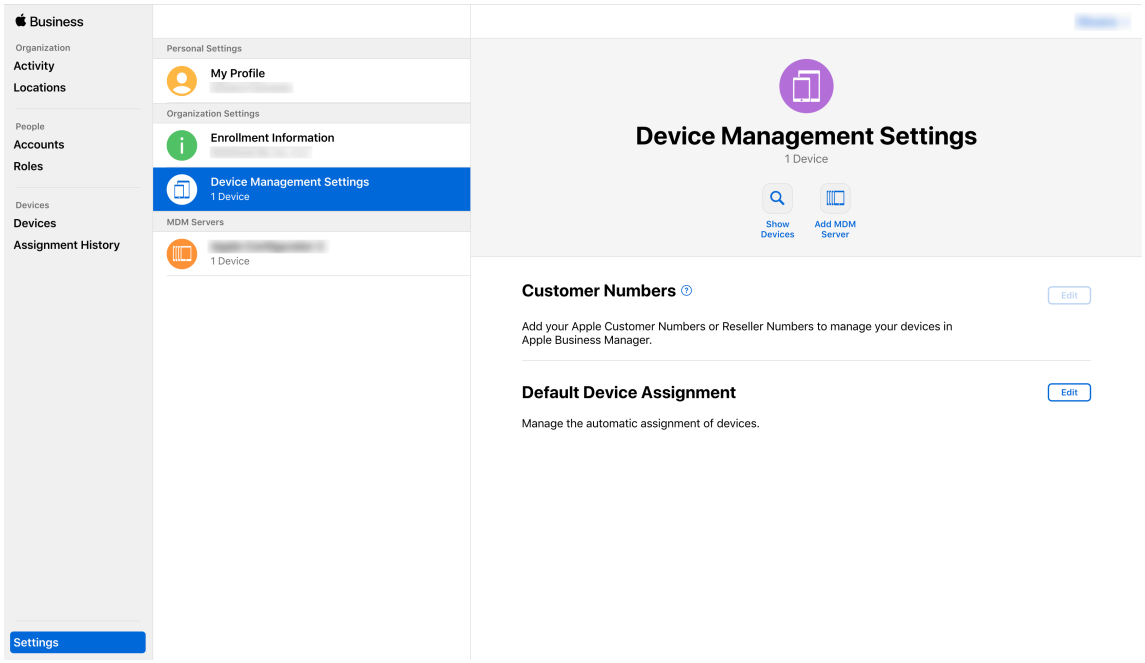
2 단계**: XenMobile** 을 **Apple School Manager** 의 **MDM** 서버로구성하고장치할당구성

ASM 포털에는 **MDM** 서버탭이있습니다. 이설정을완료하려면 XenMobile 의공개키파일이필요합니다.

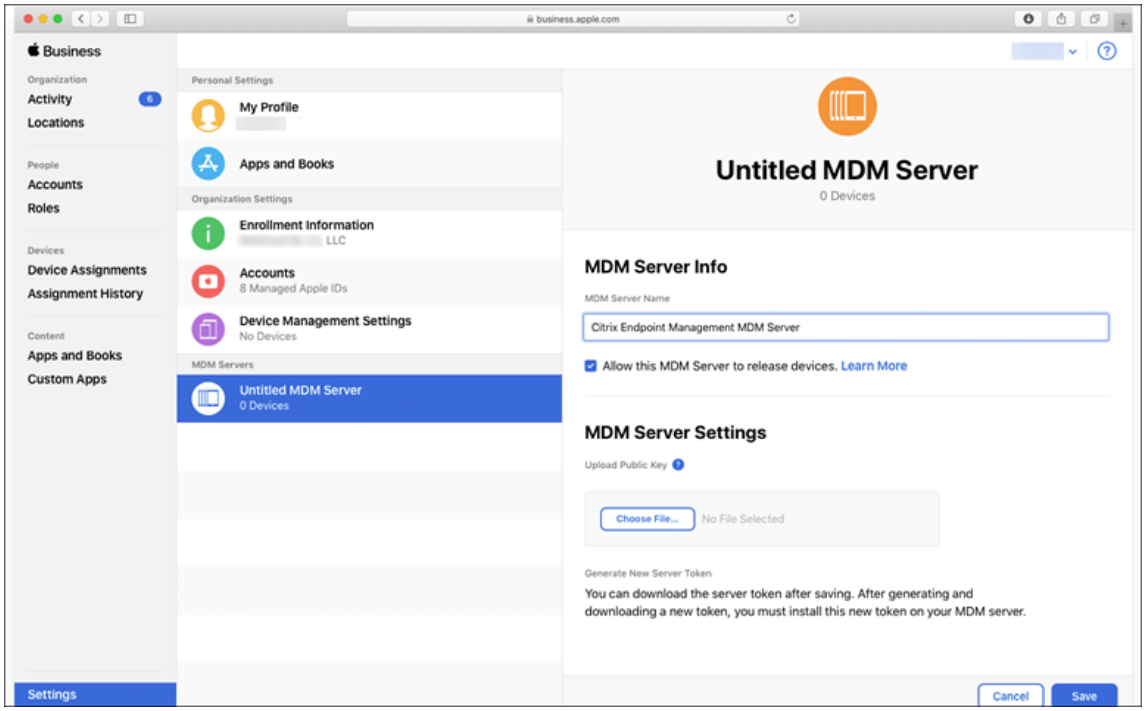
1. XenMobile 의공개키를로컬컴퓨터에다운로드합니다. XenMobile 콘솔에서 설정 **> Apple** 배포프로그램으로이동합니다.



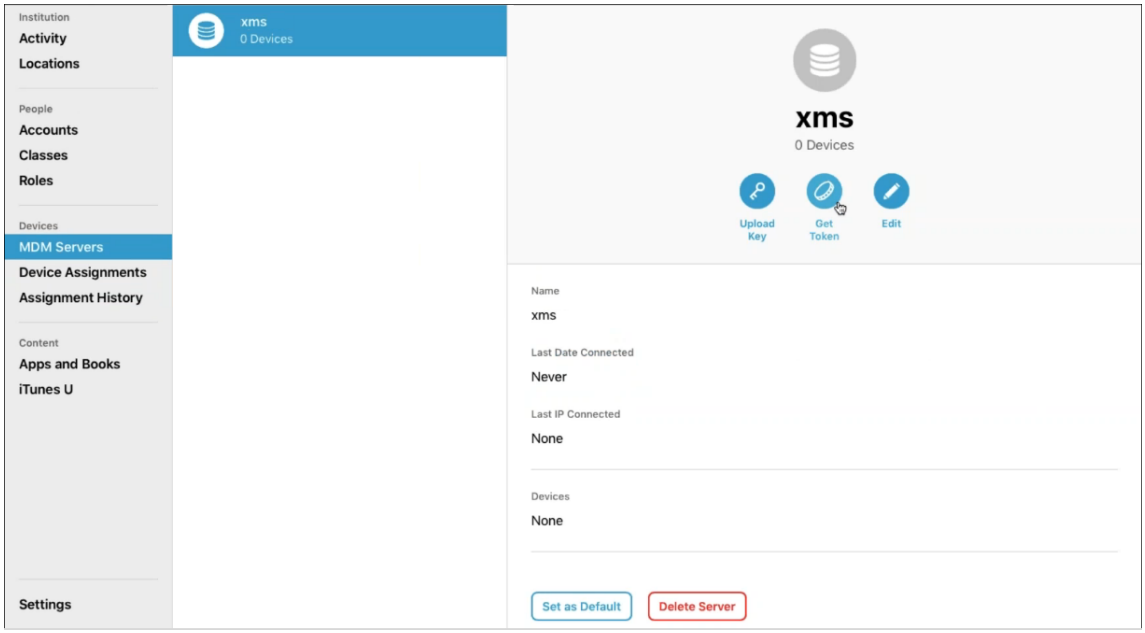
2. 공개키다운로드에서 다운로드를클릭하고 PEM 파일을저장합니다.
3. **Apple School Manager** 포털에서 설정을클릭한다음 장치관리설정을클릭합니다. **MDM** 서버추가를클릭합니다.



4. XenMobile 이름을입력합니다. 입력하는서버이름은참조용이며서버의 URL 또는이름이아닙니다. 공개키업로드에서 파일선택을클릭합니다.



5. XenMobile 에서다운로드한공개키를업로드하고 저장을클릭합니다.
6. 서버토큰을생성합니다. 토큰다운로드를클릭하여서버토큰파일을컴퓨터에다운로드합니다.

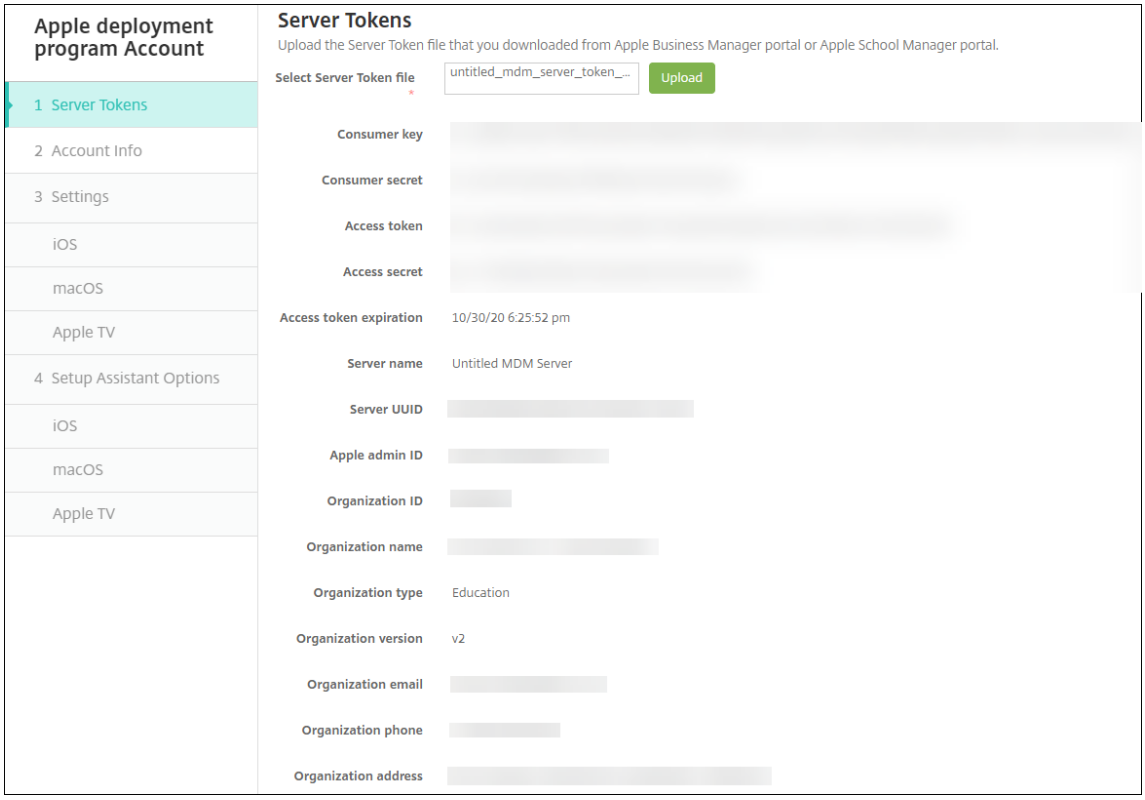


7. 기본장치할당에서 변경을클릭합니다. 장치할당방법을선택한후요청된정보를제공합니다. 자세한내용은 ABM 사용자가이드를참조하십시오.

3 단계: XenMobile 에 Apple School Manager 계정추가

1. XenMobile 콘솔에서 설정 > **Apple** 배포프로그램으로이동한다음 **Apple** 배포프로그램계정추가에서 추가를클릭합니다.

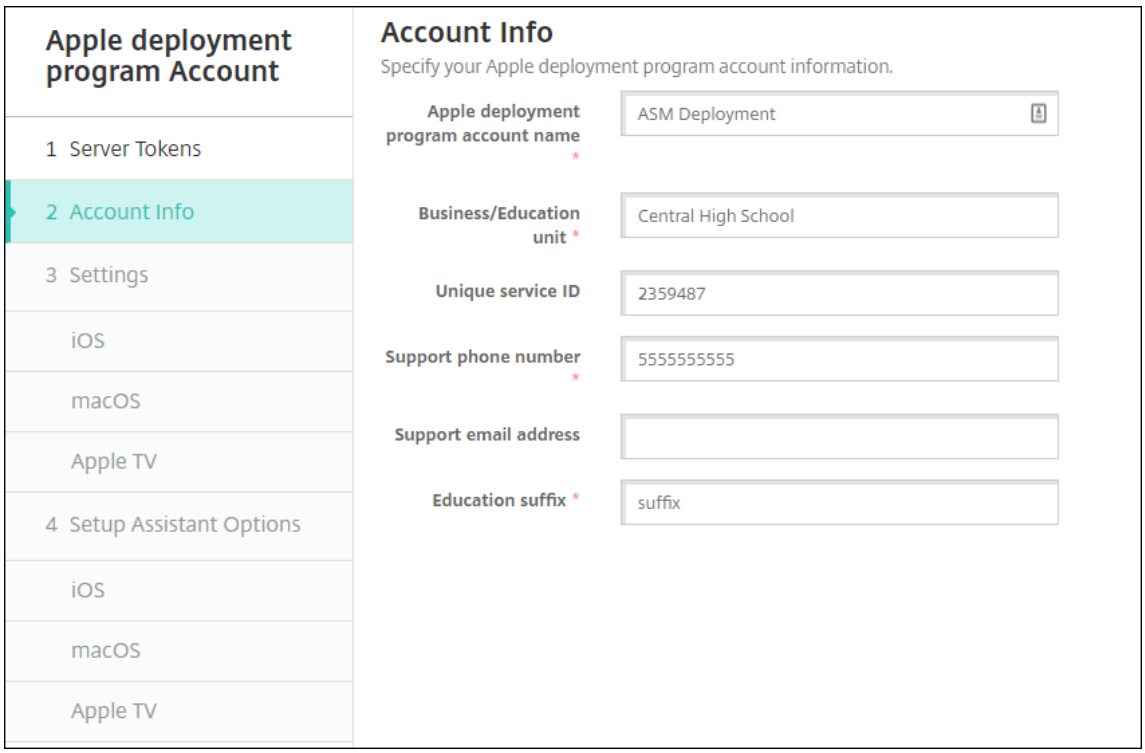
2. 서버토큰페이지에서 업로드를클릭하고 ASM 포털에서다운로드한서버토큰파일 (P7M 파일) 을선택합니다. 토큰정보페이지가나타납니다.



   참고:

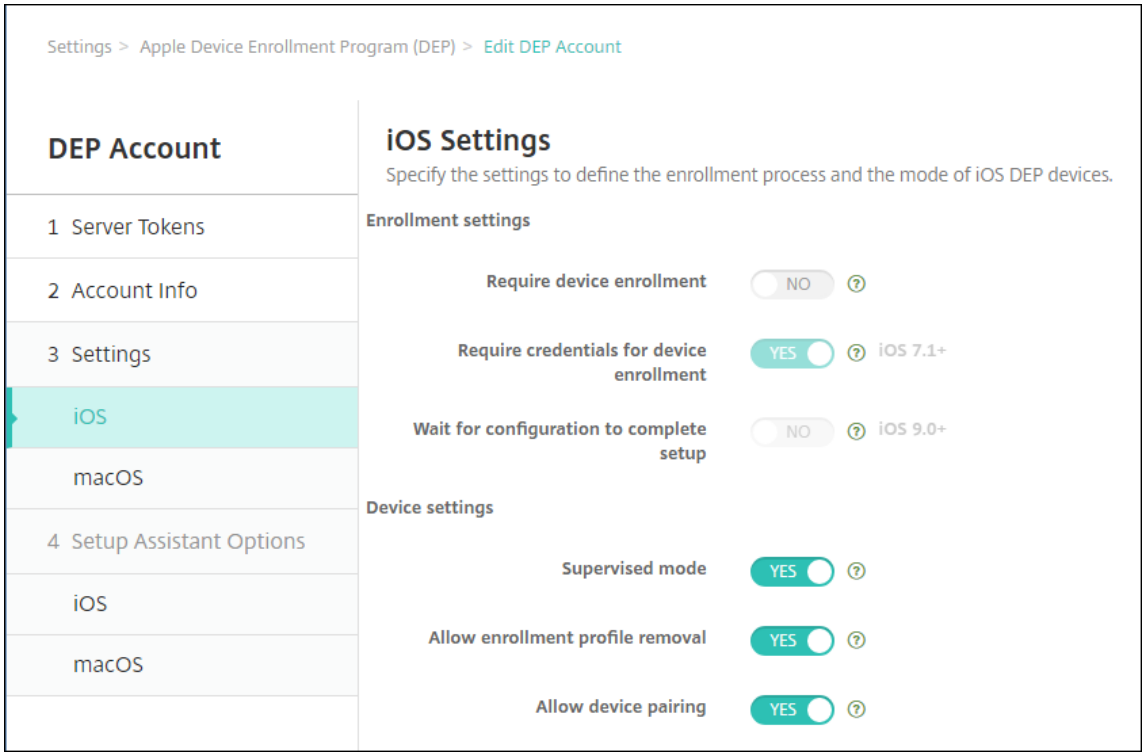
   - 조직 **ID** 는 Apple 배포프로그램의고객 ID 입니다.
   - ASM 계정의 조직유형은 교육이고 조직버전은 **v2** 입니다.

3. 계정정보페이지에서다음설정을지정합니다.



- **Apple** 배포프로그램계정이름**:** 이 Apple 배포프로그램계정의고유한이름입니다. 국가또는조직계층구조별과같이 Apple 배포프로그램계정을구성하는방식을반영하는이름을사용합니다.
- **Business/Education unit(**비즈니스**/**교육단위**):** 장치를할당할교육단위또는부서입니다. 이것은필수필드입니다.
- 고유서비스 **ID:** 계정을식별하는데도움이되는선택적고유 ID 입니다.
- 지원전화번호**:** 사용자가설정중에전화할수있는지원전화번호입니다. 이것은필수필드입니다.
- 지원전자메일주소**:** 최종사용자에게제공되는선택적지원전자메일주소입니다.
- 교육접미사**:** 지정된 ASM 배포프로그램계정의클래스에플래그를지정합니다. (볼륨구매접미사는지정된볼륨구매계정의앱과 iBooks 에플래그를지정합니다.) ASM 배포프로그램과 ASM 볼륨구매계정모두에동일한접미사를사용하는것이좋습니다.

4. 다음을클릭합니다. **iOS** 설정에서다음설정을지정합니다.

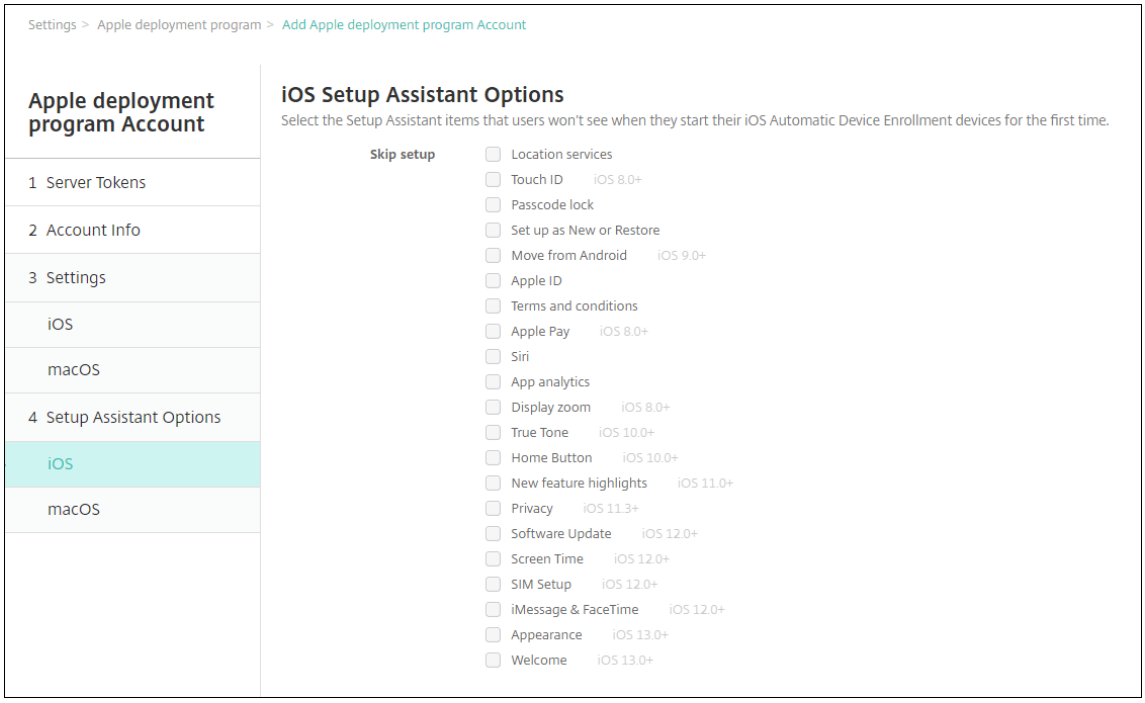


- 등록설정
  - 장치등록필요**:** 사용자가장치를등록해야합니다. 이설정을 아니요로변경합니다.
  - 장치등록에자격증명필요**:** Apple 배포프로그램설정중에사용자가자격증명을입력해야합니다. XenMobile 과 ASM 의통합의경우이설정은기본적으로 예이며변경할수없습니다. Apple 배포프로그램에는장치등록을위한자격증명이필요합니다.
  - 구성에서설정을완료할때까지대기**:** 모든 MDM 리소스가장치에배포될때까지사용자가설정도우미모드에있어야하는지여부를설정합니다. XenMobile 과 ASM 통합의경우이설정은기본적으로 아니요입니다. Apple 설명서에따르면장치가설정도우미모드에있는동안에는다음명령이작동하지않을수있습니다.
    - InviteToProgram
    - InstallApplication
    - InstallMedia
    - ApplyRedemptionCode
- 장치설정
  - 감독모드**:** iOS 장치를감독모드로전환합니다. 기본값인 예를변경하지마십시오. iOS 장치를감독모드로전환하는방법에대한자세한내용은 Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.
  - 공유모두**:** iPad 에서공유모드를설정합니다. 최소요구사항을충족하지않는장치는공유할수없습니다.
  - 등록프로필제거허용**:** ASM 통합의경우사용자가장치에서등록프로필을제거할수있도록합니다. 이설정을 예로변경합니다.

- 장치페어링허용**:** ASM 통합의경우 App Store 및 Apple Configurator 를통해관리할수있도록장치페어링을허용합니다. 이설정을 예로변경합니다.

5. **iOS** 설정도우미옵션에서사용자가장치를처음으로시작할때건너뛸 iOS 설정도우미단계를선택합니다. 기본적으로설정도우미에는모든단계가포함됩니다. 설정도우미에서단계를제거하면사용자환경이간소화됩니다.

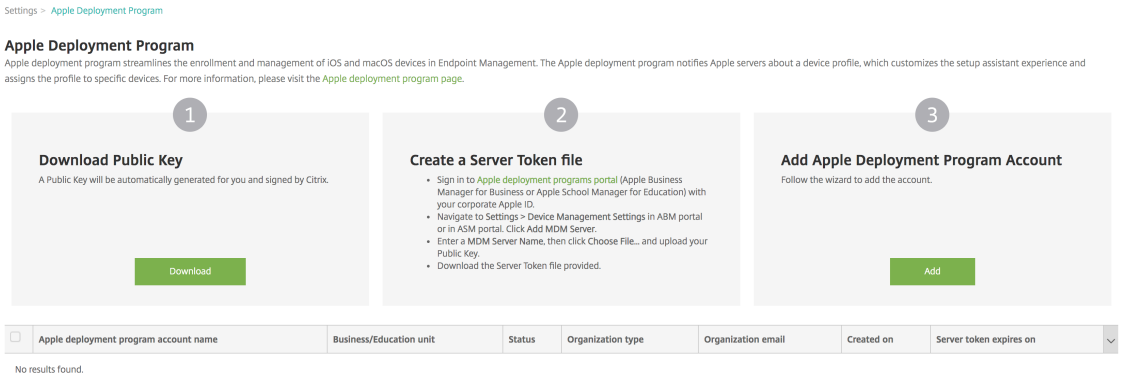
> 중요**:**
>
> **Apple ID** 및 약관단계는포함하는것이좋습니다. 이단계는강사와학생이관리되는 Apple ID 의새암호를입력하고필수약관에동의하는데사용됩니다.



- 위치서비스**:** 장치에위치서비스를설정합니다.
- **Touch ID:** iOS 장치에서 Touch ID 를설정합니다.
- 암호잠금**:** 장치에대한암호를만듭니다.
- 새로설정또는복원**:** 장치를새로설정하거나 iCloud 또는 Apple App Store 백업에서복원합니다.
- **Android** 에서이동**:** Android 장치의데이터를 iOS 장치로전송할수있도록합니다. 이옵션은 새로설정또는복원을선택한경우에만사용할수있습니다 (즉, 단계가생략됨).
- **Apple ID:** 장치에대한 Apple ID 계정을설정합니다. 확인란을선택하여이단계를포함하는것이좋습니다.
- 약관**:** 사용자가장치사용에대한약관에동의해야합니다. 확인란을선택하여이단계를포함하는것이좋습니다.
- **Apple Pay:** iOS 장치에 Apple Pay 를설정합니다.
- **Siri:** 장치에서 Siri 를사용하거나사용하지않습니다.
- 앱분석**:** 충돌데이터및사용현황통계를 Apple 과공유할지여부를설정합니다.
- 표시확대/축소**:** iOS 장치에서디스플레이해상도 (표준또는확대) 를설정합니다.
- **True Tone:** iOS 장치에서 True Tone 디스플레이를설정합니다.
- 홈버튼**:** 홈버튼화면민감도를설정합니다.

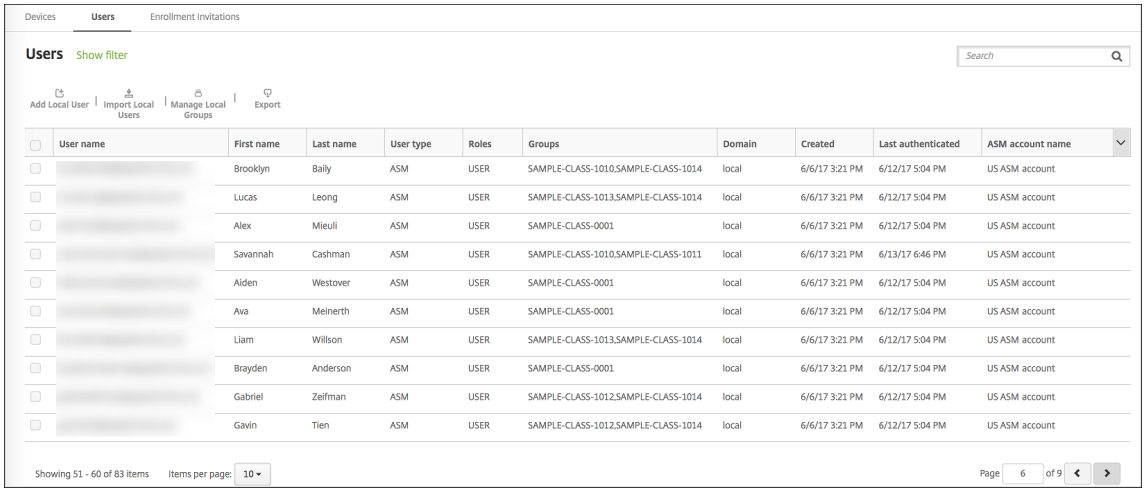
- 새로운기능하이라이트**:** iOS 11.0 장치 (최소버전) 에서어디서든 Dock 에접근하기와최근앱간전환이라는온보딩 정보제공용화면을설정합니다.
- 개인정보보호**:** Apple 배포프로그램장치를설정하는동안사용자에게데이터및개인정보보호창을표시하지않습니다. iOS 11.3 이상에해당합니다.
- **SoftwareUpdate:** Apple 배포프로그램장치를설정하는동안사용자에게필수소프트웨어업데이트화면을표시하지않습니다. iOS 12.0 이상에해당합니다.
- **ScreenTime:** Apple 배포프로그램장치를설정하는동안사용자에게 Screen Time(화면시간) 화면을표시하지않습니다. iOS 12.0 이상에해당합니다.
- **SIM Setup(SIM** 설정**):** Apple 배포프로그램장치를설정하는동안사용자에게 Add Cellular Plan(데이터요금제추가) 화면을표시하지않습니다. iOS 12.0 이상에해당합니다.
- **iMessage & FaceTime:** Apple 배포프로그램장치를설정하는동안사용자에게 iMessage 및 FaceTime 화면을표시하지않습니다. iOS 12.0 이상에해당합니다.

6. 계정이 설정 **> Apple** 배포프로그램에표시됩니다. XenMobile 과 ASM 계정간의연결을테스트하려면계정을선택하고 연결테스트를클릭합니다.



상태메시지가나타납니다.

몇분후 ASM 의사용자계정이 관리 **>** 사용자페이지에나타납니다. XenMobile 은각사용자에대해가져온, 관리되는 Apple ID 를바탕으로로컬사용자계정을생성합니다. 다음예에서사용자계정에대해사용자지정된 Apple ID 도메인이름 접두사는 `appleid`입니다.

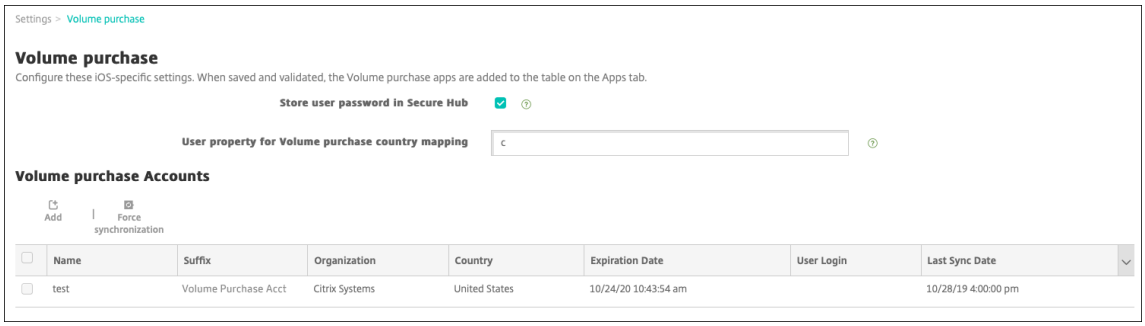


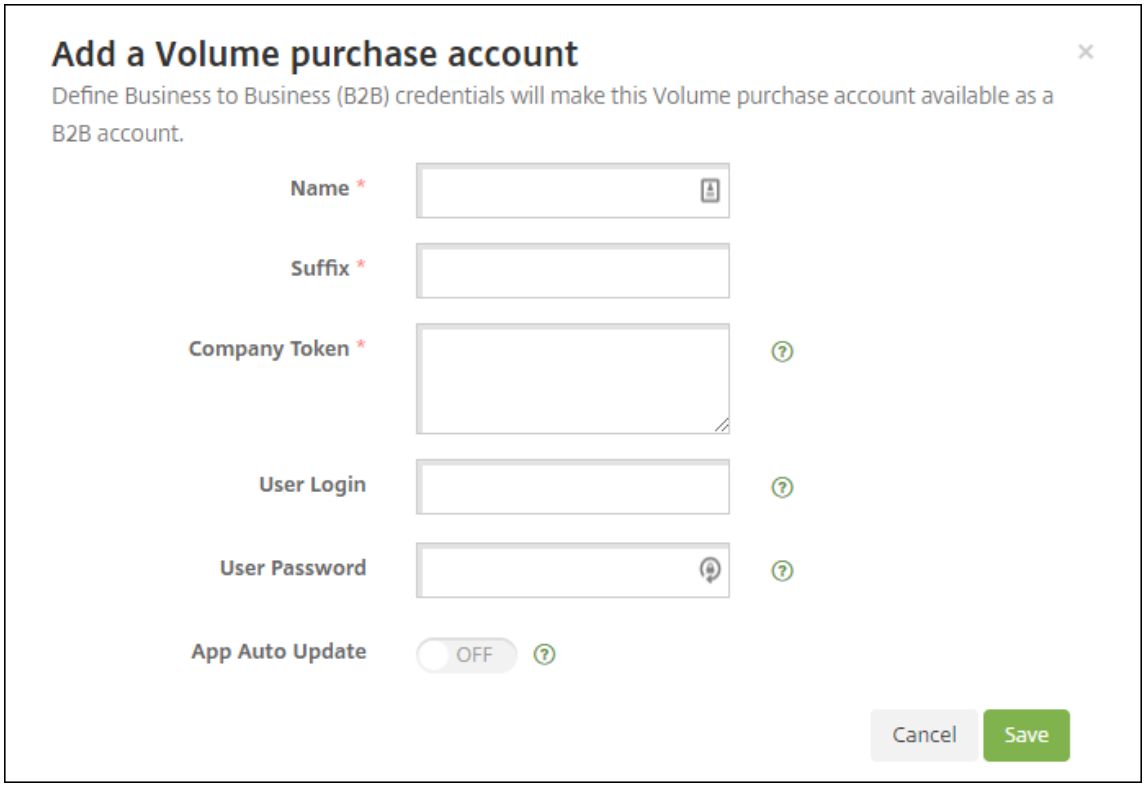
지정된 ASM 계정에대한모든사용자를찾으려면사용자검색필터에계정이름을입력합니다.

4 단계: Apple School Manager 의교육볼륨구매계정구성

이섹션에서는앱및 iBooks 용볼륨구매라이센스를구매할때사용한볼륨구매계정을 XenMobile 에지정합니다.

1. ASM 에대한교육볼륨구매계정을구성하려면 Apple 볼륨구매의지침을따르십시오. 볼륨구매계정추가화면에서회사토큰을입력해야합니다. 교육볼륨구매계정에서직접토큰을다운로드하고 볼륨구매계정추가화면에붙여넣습니다.





2. 볼륨구매라이센스를 XenMobile 로가져오는동안몇분정도기다리십시오.

5 단계: Apple School Manager 사용자의암호추가

ASM 계정을추가한후 XenMobile 이 ASM 에서클래스와사용자를가져옵니다. XenMobile 에서클래스는로컬그룹으로처리되며콘솔에서 "그룹" 이라는용어가사용됩니다. ASM 에그룹이름이있는클래스의경우 XenMobile 이해당그룹이름을클래스에할당합니다. 그렇지않은경우 XenMobile 은소스시스템 ID 를그룹이름으로사용합니다. 과정이름은 ASM 에서고유하지않으므로 XenMobile 은교육과정이름을클래스이름으로사용하지않습니다.

XenMobile 은관리되는 Apple ID 를사용하여사용자유형이 **ASM** 인로컬사용자를생성합니다. 사용자가로컬인이유는 ASM 이모든외부데이터원본과별개로자격증명을생성하기때문입니다. 따라서 XenMobile 은이러한사용자를인증할때디렉터리서버를사용하지않습니다.

ASM 은 XenMobile 에임시사용자암호를보내지않습니다. CSV 파일로가져오거나수동으로추가해야합니다. 임시사용자암호를가져오려면:

1. 관리되는 Apple ID 의임시암호를생성할때 ASM 에서생성된 CSV 파일을가져옵니다.
2. CSV 파일을편집하여사용자가 XenMobile 에임시암호를등록할때제공한새암호로바꿉니다. 이목적으로사용하는암호유형에는제약이없습니다.

   CSV 파일의입력형식은다음과같습니다. `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

   여기서:

사용자: `user@appleid.citrix.com`

이름: `Firstname`

중간이름: `Middle`

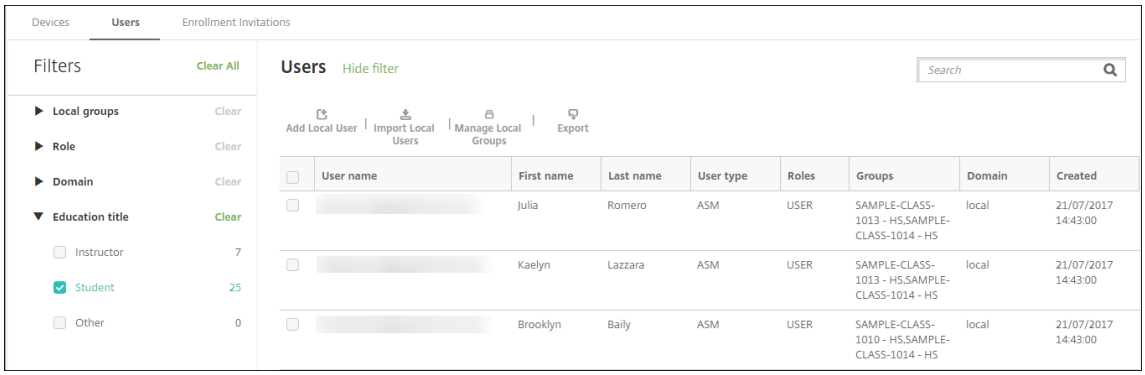
성: `Lastname`

암호: `Password123!`

3. XenMobile 콘솔에서 관리 **>** 사용자를클릭합니다. 사용자페이지가나타납니다.

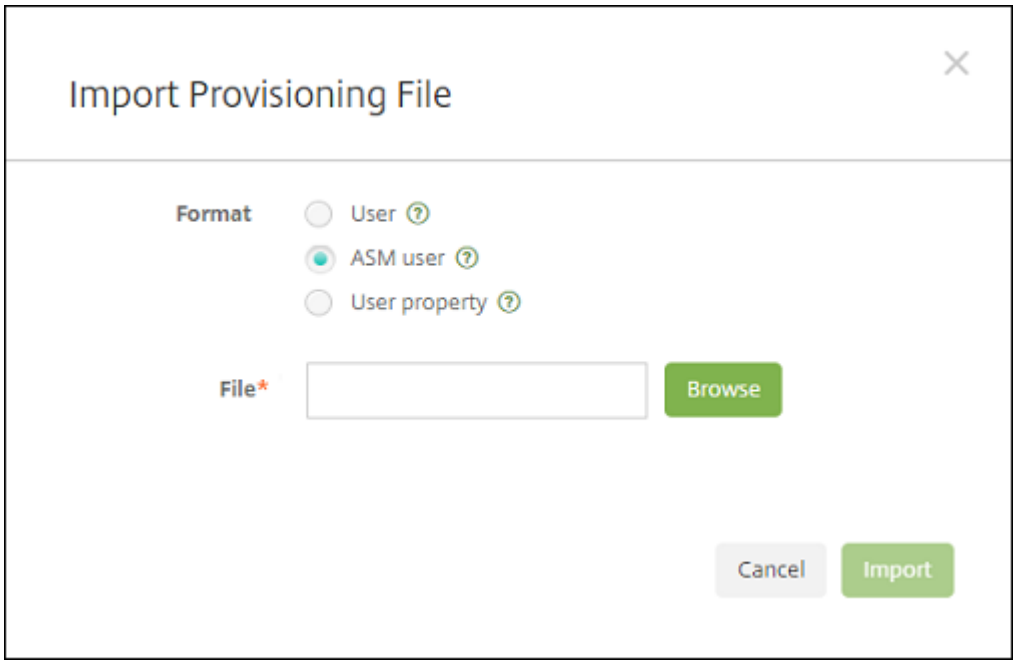
   다음 관리 **>** 사용자화면샘플에는 ASM 에서가져온사용자목록이나와있습니다. 사용자목록에서:

   - 사용자이름에는관리되는 Apple ID 가표시됩니다.
   - 사용자유형은 **ASM** 이고 ASM 에서생성된계정임을나타냅니다.
   - 그룹에는클래스가표시됩니다.

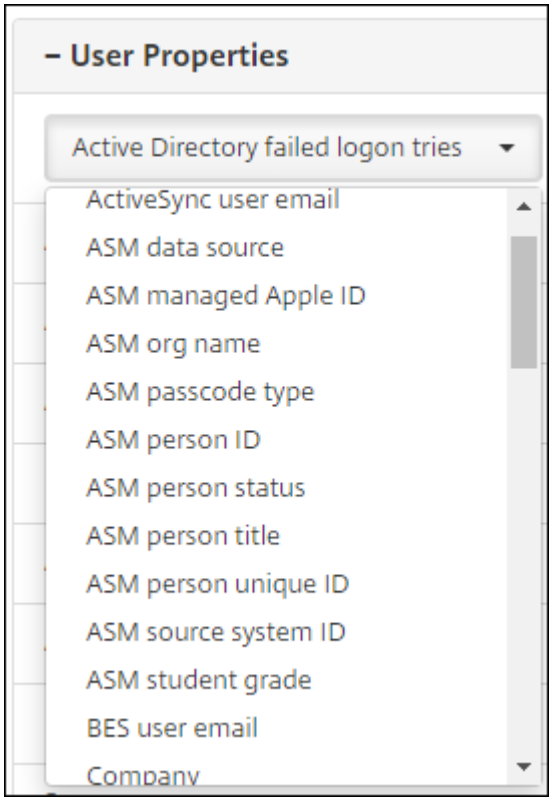


4. 로컬사용자가져오기를클릭합니다. 프로비저닝파일가져오기대화상자가나타납니다.

5. 형식으로 **ASM** 사용자를선택하고, 2 단계에서준비한 CSV 파일로이동한후 가져오기를클릭합니다.



6. 로컬사용자의속성을보려면사용자를선택하고 편집을클릭합니다.



이름속성외에도다음과같은 ASM 속성을사용할수있습니다.

- **ASM** 데이터원본**:** 클래스의데이터원본입니다 (예: **CSV** 또는 **SFTP**).
- **ASM** 관리되는 **Apple ID:** 관리되는 Apple ID 에는교육기관이름과 `appleid`가포함될수있습니다. 예를들어 ID 는 johnappleseed@appleid.myschool.edu 와유사할수있습니다. XenMobile 는인증에관리되는 Apple ID 를사용합니다.
- **ASM** 조직이름**:** XenMobile 에서계정에지정한이름입니다.
- **ASM** 암호유형**:** 사용자의암호정책으로, 복합형식 (학생암호가아닌암호로, 8 자이상의숫자및문자로구성됨), **4**(자리) 또는 **6**(자리) 입니다.
- **ASM** 사용자고유 **ID:** 사용자의식별자입니다.
- **ASM** 사용자상태**:** 관리되는 Apple ID 가 활성또는 비활성인지여부를지정합니다. 사용자가관리되는 Apple ID 계정에대한새암호를제공하면이상태가활성으로전환됩니다.
- **ASM** 사용자직위**:** 강사, 학생또는기타입니다.
- **ASM** 사용자고유 **ID:** 사용자의고유식별자입니다.
- **ASM** 소스시스템 **ID:** 시스템소스의식별자입니다.
- **ASM** 학생학년**:** 학생의학년정보입니다 (강사에게는사용되지않음).

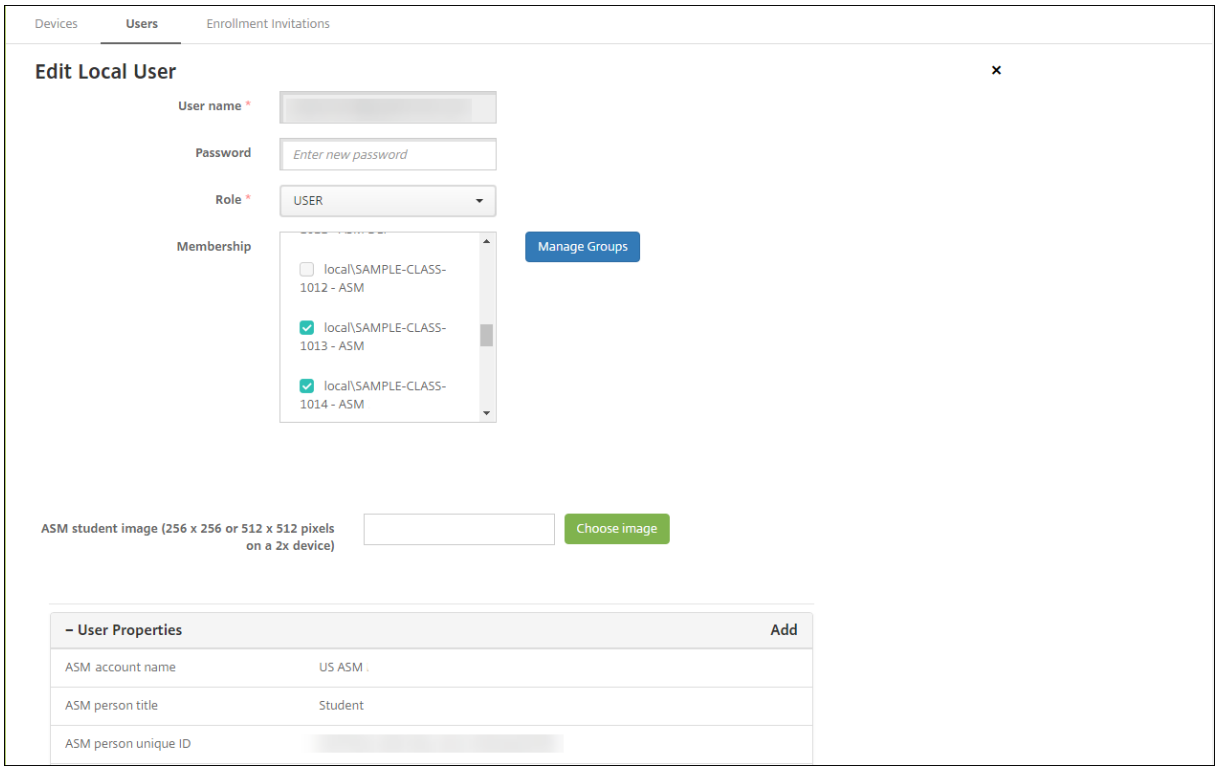
6 단계**:** 학생의사진추가 **(**선택사항**)**

각학생의사진을추가할수있습니다. 강사가 Apple Classroom 앱을사용하는경우이앱에사진이나타납니다.

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** 에추가

배달그룹은사용자범주에배포할리소스를정의합니다. 예를들어강사와학생에대한배달그룹하나를생성하거나여러배달그룹을생성하여여러강사또는학생에게전송되는앱, 미디어및정책을사용자지정할수있습니다. 클래스당하나이상의배달그룹을생성할수있습니다. 또한관리자 (교육기관의다른직원) 를위한하나이상의배달그룹을생성할수있습니다.

사용자장치에배포하는리소스에는장치정책, 볼륨구매앱및 iBooks 가포함됩니다.

- 장치정책:

  강사가 Classroom 앱을사용하는경우교육구성장치정책이필요합니다. 다른장치정책을검토하여강사및학생의 iPad 를구성하고제한하는방법을결정하십시오.

- 볼륨구매앱:

  XenMobile 을사용하려면볼륨구매앱을교육사용자의필수앱으로배포해야합니다. XenMobile 은볼륨구매앱의선택적배포를지원하지않습니다.

  Apple Classroom 앱을사용하는경우강사장치에만앱을배포하십시오.

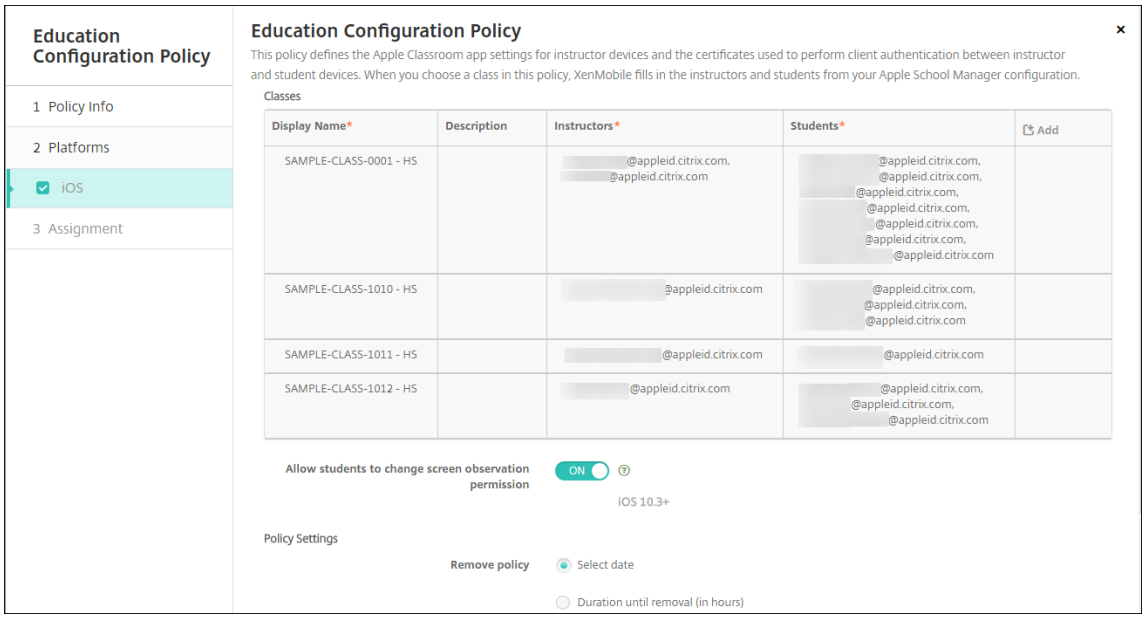
강사또는학생에게제공하려는다른앱을배포합니다. 이솔루션은 Citrix Secure Hub 앱을사용하지않으므로강사또는학생에게이앱을배포하지않아도됩니다.

- 볼륨구매 iBooks:

  XenMobile 이 ASM 계정에연결하면구매한 iBooks 가 XenMobile 콘솔의 구성 **>** 미디어에나타납니다. 이페이지에나열되는 iBooks 는배달그룹에추가할수있습니다. XenMobile 은 iBooks 를필수미디어로만지원합니다.

강사및학생을위한리소스및배달그룹을계획한후에는이러한항목을 XenMobile 콘솔에서생성할수있습니다.

1. 강사또는학생장치에배포할장치정책을생성합니다. 교육구성장치정책에대한자세한내용은 교육구성장치정책을참조하십시오.

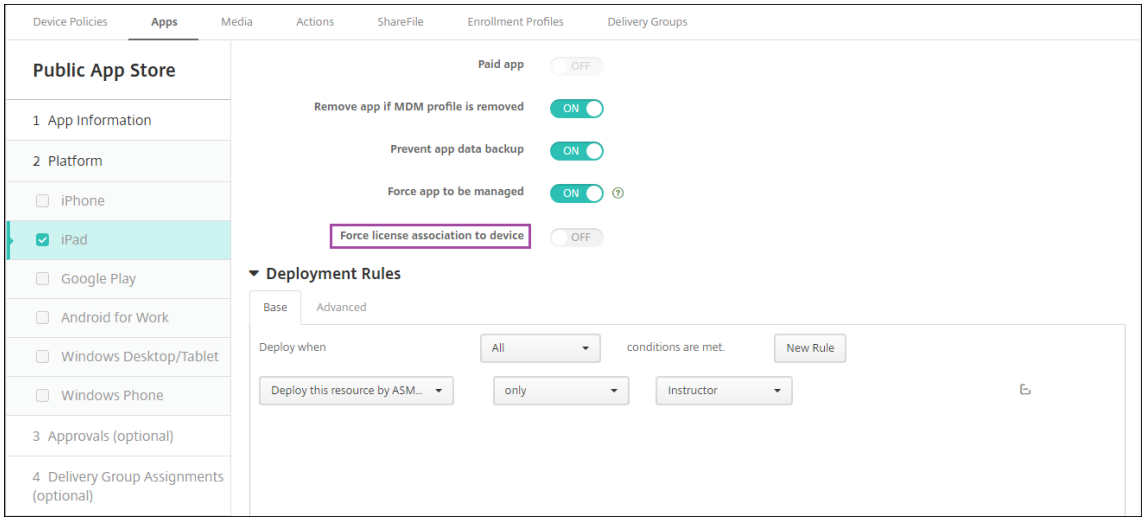


장치정책에대한자세한내용은 장치정책과개별정책문서를참조하십시오.

2. 앱 (구성 **>** 앱) 과 iBooks(구성 **>** 미디어) 를구성합니다.

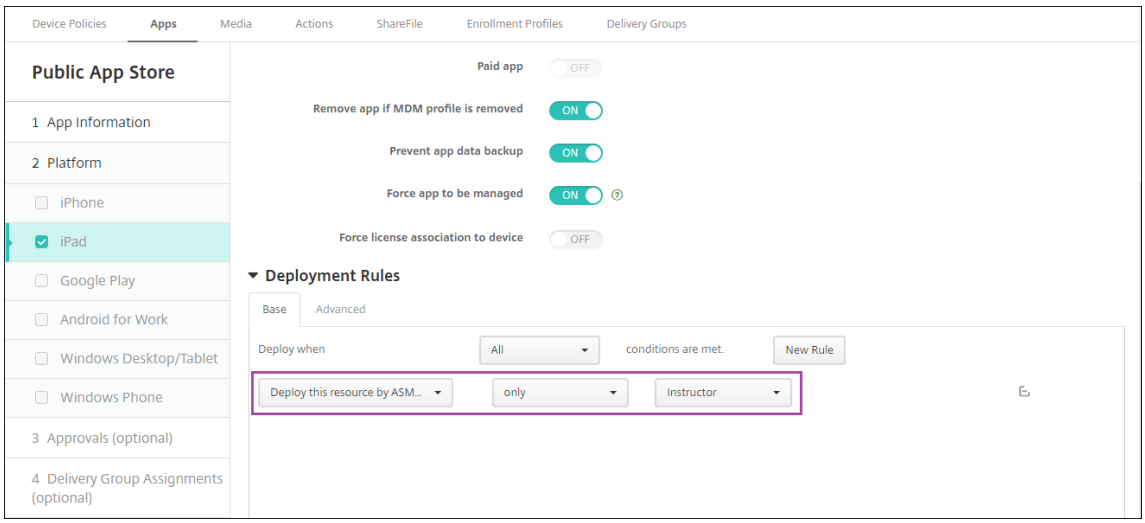
   - 기본적으로 XenMobile 은앱및 iBooks 를사용자수준에서할당합니다. 첫배포시강사및학생에게는 ASM 등록메시지가표시됩니다. 사용자가초대를수락하면다음배포 (6 시간이내) 시 ASM 앱과 iBooks 가전송됩니다. Citrix 에서는새 ASM 사용자에게앱및 iBooks 의배포를강제하도록권장합니다. 그러려면배달그룹을선택하고 배포를클릭합니다.

     장치수준에서앱 (iBooks 제외) 을할당하도록선택할수있습니다. 그러려면 장치에강제로라이센스연결설정을 켜짐으로변경합니다. 장치수준에서앱을할당하면사용자에게 Apple 볼륨구매가입을위한초대가전송되지않습니다.



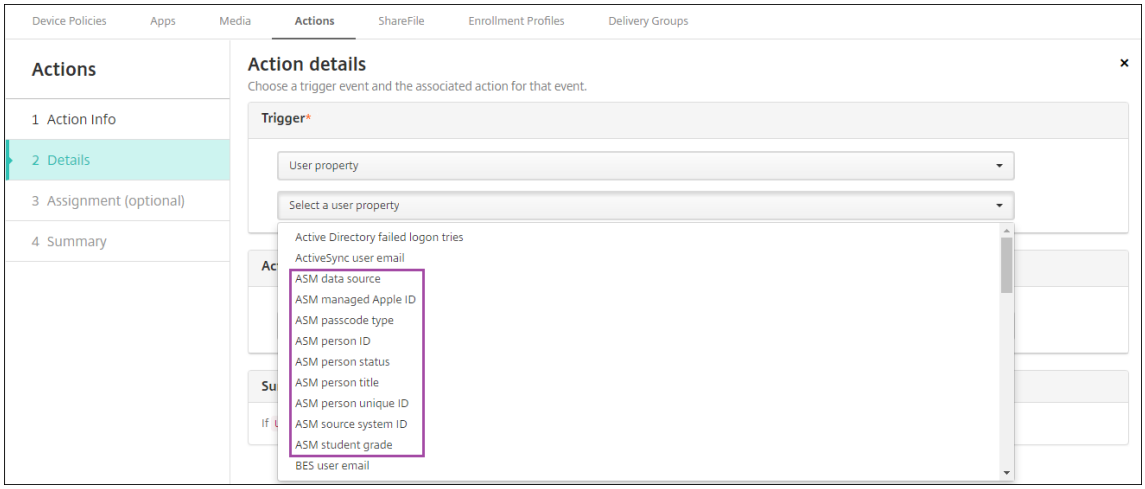
- 강사에게만앱을배포하려면강사만포함된배달그룹을선택하거나다음배포규칙을사용합니다.

```
Deploy this resource by ASM device type
only
Instructor
<!--NeedCopy-->
```



- 볼륨구매앱추가와관련된도움말은 공용앱스토어앱추가를참조하십시오.

3. 선택사항입니다. ASM 사용자속성을기반으로동작을생성합니다. 예를들어새앱이설치될때학생장치에알림을보내는동작을생성할수있습니다. 또는다음예제에표시된것과같이사용자속성이트리거하는동작을생성할수있습니다.

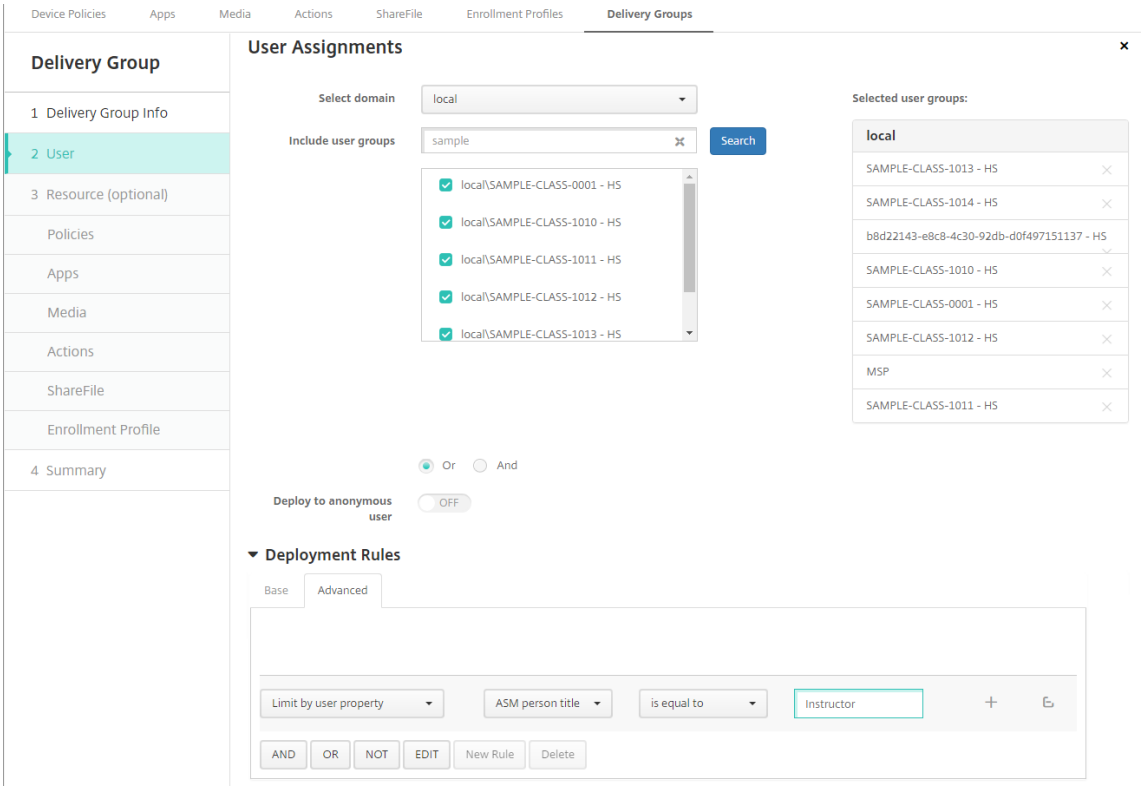


동작을생성하려면 구성 **>** 동작으로이동합니다. 동작구성에대한자세한내용은 자동화된동작을참조하십시오.

4. 구성 **>** 배달그룹에서강사및학생을위한배달그룹을생성합니다. ASM 에서가져온클래스를선택합니다. 또한강사및학생에대한배포규칙을생성합니다.

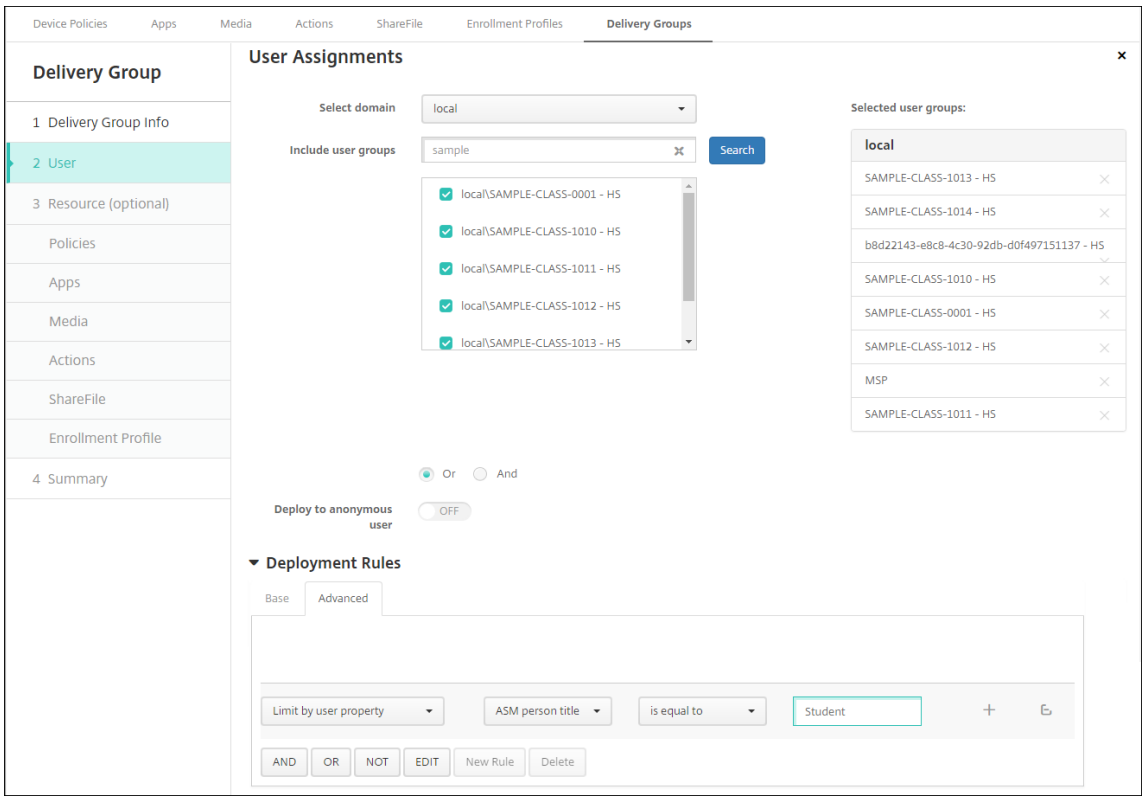
   예를들어다음은강사에대한사용자할당입니다. 배포규칙은다음과같습니다.

```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

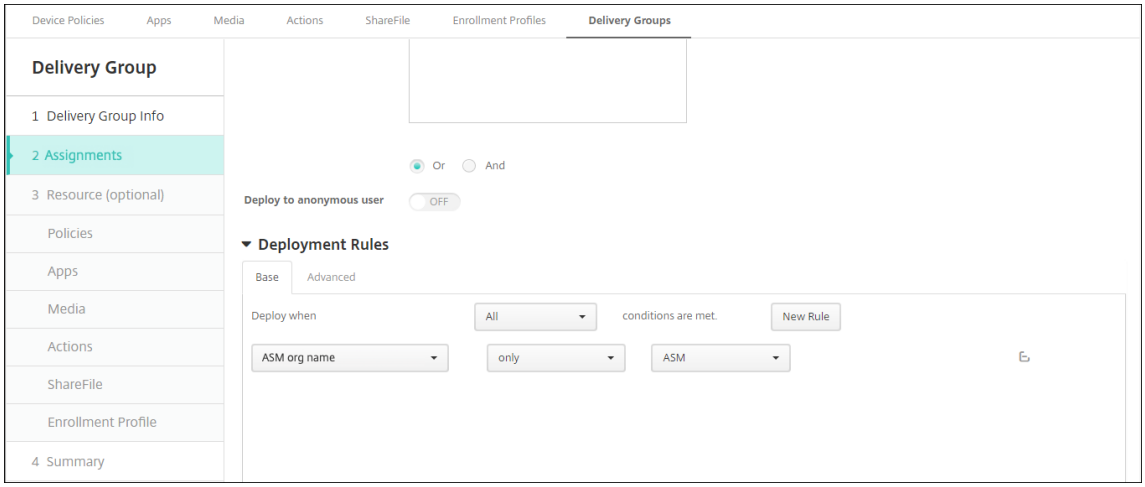



다음은학생에대한사용자할당입니다. 배포규칙은다음과같습니다.

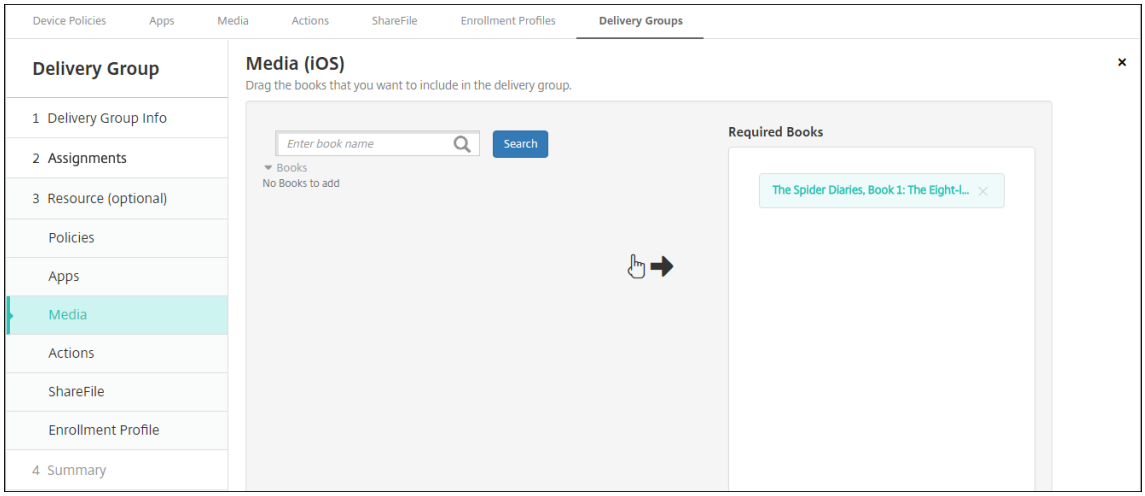
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

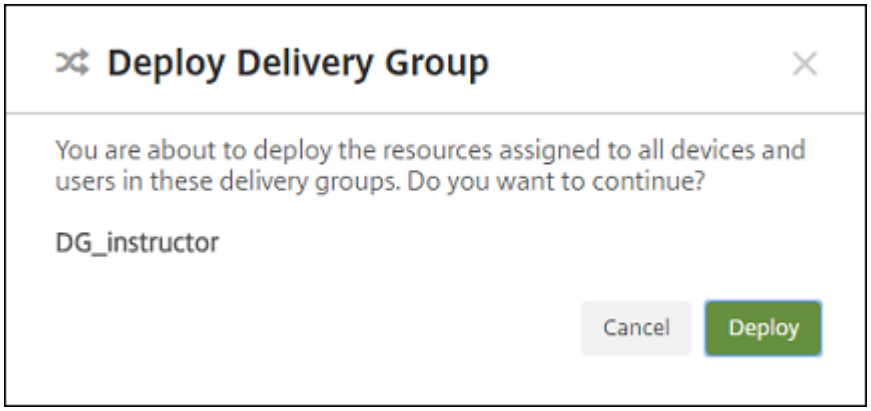
ASM 조직이름에기반한배포규칙을사용하여배달그룹을필터링할수도있습니다.



5. 배달그룹에리소스를할당합니다. 다음예제는배달그룹에포함된 iBooks 를보여줍니다.



다음예제는배달그룹을선택하고 배포를클릭할때표시되는확인대화상자를보여줍니다.



자세한내용은 리소스배포의 “배달그룹을편집하려면” 과 “배달그룹을배포하려면” 을참조하십시오.

8 단계**:** 강사및학생장치등록테스트

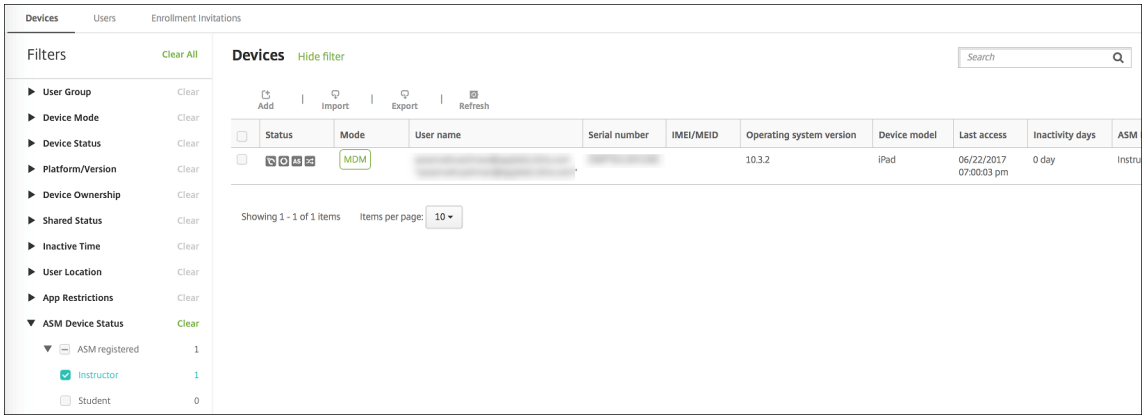
다음방법중하나를사용하여장치를등록할수있습니다.

- 학교관리자는 XenMobile 콘솔에서설정할수있는사용자암호를사용하여강사및학생장치를등록할수있습니다. 따라서앱과미디어가이미설정된장치를사용자에게제공할수있습니다.
- 사용자는장치를받은후관리자가제공한사용자암호를사용하여등록합니다. 등록이완료되면 XenMobile 이장치정책, 앱및미디어를장치에전송합니다.

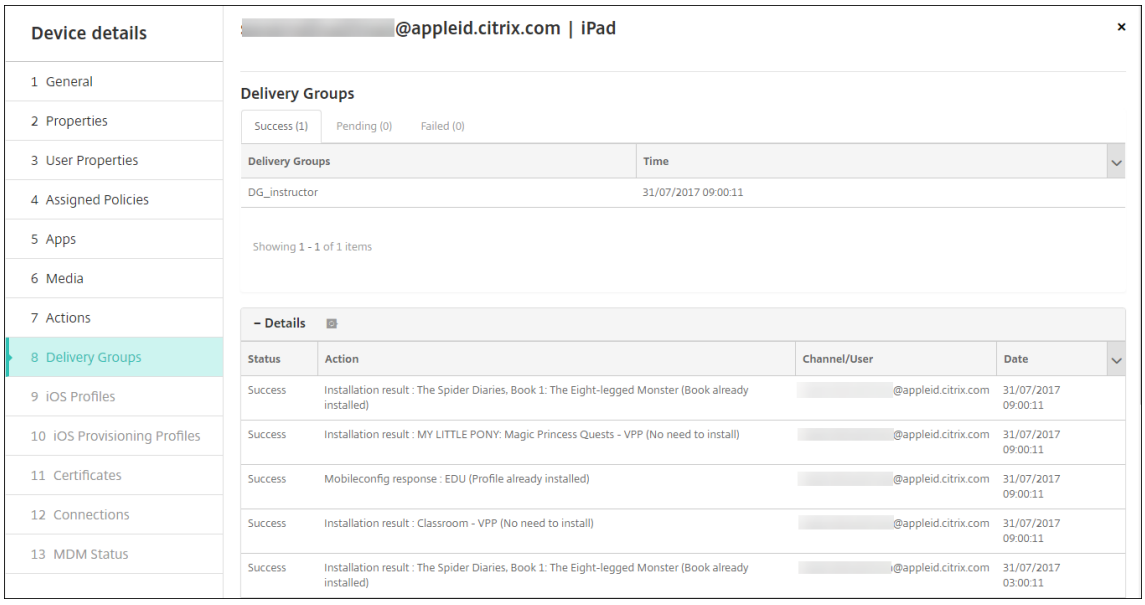
등록을테스트하려면 ASM 에연결된 Apple 배포프로그램장치를사용합니다.

1. 장치가 ASM 에연결되지않은경우하드리셋을수행하여장치콘텐츠및설정을지웁니다.
2. 강사용 ASM 장치를등록합니다. 그런다음학생용 ASM 장치를등록합니다.
3. 관리 **>** 장치페이지에서두 ASM 장치가 MDM 전용으로등록되었는지확인합니다.

   ASM 등록됨, **ASM** 공유됨, 강사, 학생등의장치상태에따라 장치페이지를필터링할수있습니다.



4. 각장치에대한 MDM 리소스가올바르게배포되었는지확인하려면: 장치를선택하고 편집을클릭한후여러페이지를확인합니다.



9 단계**:** 장치배포

강사와학생에게장치를배포할수있도록이벤트를호스트하는것이좋습니다.

사전등록된장치를배포하지않는경우에는사용자에게다음항목도제공하십시오.

- 등록용 XenMobile 암호
- 관리되는 Apple ID 에대한 ASM 임시암호

첫번째사용자환경은다음과같습니다.

1. 하드리셋후사용자가처음으로장치를시작하면 XenMobile 이장치등록을위한등록화면을표시합니다.
2. 사용자는관리되는 Apple ID 와인증에사용되는 XenMobile 암호를 XenMobile 에제공합니다.

3. Apple ID 설정단계에서관리되는 Apple ID 와 ASM 임시암호를제공하라는메시지가사용자에게표시됩니다. 이러한항목은 Apple 서비스에대해사용자를인증하는데사용됩니다.
4. 관리되는 Apple ID 의암호 (iCloud 의데이터를보호하는데사용됨) 를생성하라는메시지가표시됩니다.
5. 설정도우미를마치면 XenMobile 이장치에정책, 앱및미디어를설치하기시작합니다. 사용자수준에서할당된앱및 iBooks 의경우강사및학생에게볼륨구매등록메시지가표시됩니다. 사용자가초대를수락하면다음배포 (6 시간이내) 시볼륨구매앱과 iBooks 가전송됩니다.

공유 **iPad** 구성

한교실에있는여러학생이한명또는여러명의강사가가르치는다양한과목에서 iPad 를공유할수있습니다.

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

XenMobile 은공유 iPad 에서두가지통신채널을사용합니다. 장치소유자 (강사) 에게는시스템채널을사용하고현재상주사용자 (학생) 에게는사용자채널을사용합니다. XenMobile 은이러한채널을사용하여 Apple 이지원하는리소스에적절한 MDM 명령을보냅니다.

시스템채널을통해배포되는리소스는다음과같습니다.

- 교육구성, 잠금화면메시지, 최대상주사용자수및암호잠금유예기간과같은장치정책
- 장치기반볼륨구매앱

  Apple 은공유 iPad 에서엔터프라이즈앱또는사용자기반볼륨구매앱을지원하지않습니다. 공유 iPad 에설치된앱은사용자별로적용되는것이아니라장치에글로벌로적용됩니다.

- 사용자기반볼륨구매 iBooks

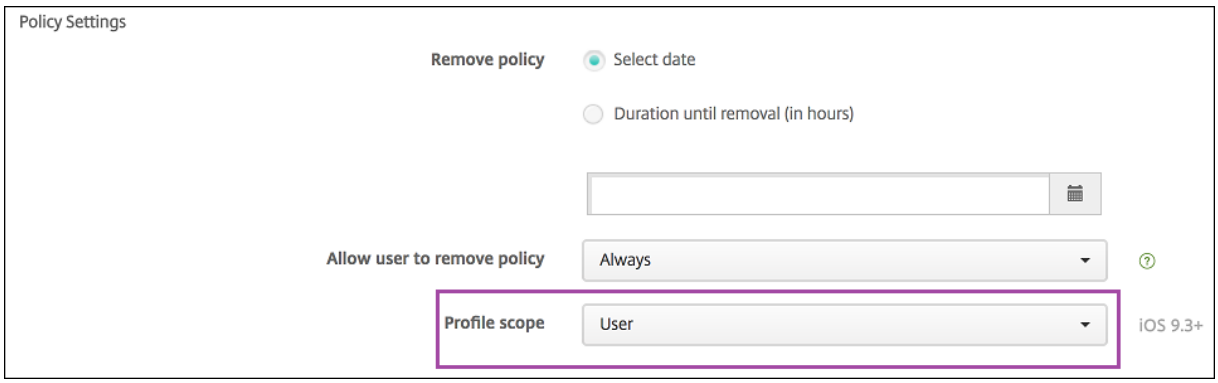
  Apple 은공유 iPad 의사용자기반볼륨구매 iBooks 할당을지원합니다.

사용자채널을통해배포되는리소스는다음과같습니다.

- 장치정책: 앱알림, 홈화면레이아웃및제한사항

  XenMobile 은사용자채널을통해이러한장치정책만지원합니다.

장치정책을구성할때정책설정 프로필범위에서배포채널을지정합니다.



사용자채널을통해배포한장치정책을제거하려면프로필제거정책에대해 배포범위를 사용자로선택해야합니다.

일반적인워크플로

일반적으로사전구성을마친감독되는공유 iPad 를강사에게제공합니다. 그런다음강사가학생에게장치를배포합니다. 강사에게사전등록된공유 iPad 를배포하지않는경우: 강사에게 XenMobile 서버암호를제공하여장치를등록할수있도록해야합니다.

공유 iPad 를구성하고등록하는일반적인워크플로는다음과같습니다.

1. XenMobile 서버콘솔을사용하여 ASM 계정을추가하고 (설정 **> Apple** 배포프로그램) 공유모드를사용하도록설정합니다. 자세한내용은다음의 “공유 iPad 에대한 ASM 계정관리” 를참조하십시오.
2. 이섹션에설명된대로 XenMobile 에필요한장치정책, 앱및미디어를추가합니다. 이러한리소스를배달그룹에할당합니다.
3. 강사로하여금공유 iPad 에대해하드리셋을수행하도록합니다. 등록에대한원격관리화면이나타납니다.
4. 강사가공유 iPad 를등록합니다.
   XenMobile 이등록된각공유 iPad 에구성된리소스를배포합니다. 자동으로다시시작된후강사는학생과장치를공유할수있습니다. iPad 에로그인페이지가나타납니다.
5. 학생이클래스를선택한다음관리되는 Apple ID 와임시 ASM 암호를입력합니다.
   공유 iPad 가 ASM 에인증하고학생에게 ASM 암호를생성하라는메시지를표시합니다. 학생은다음번에공유 iPad 에로그인할때새 ASM 암호를제공합니다.
6. iPad 를공유하는다른학생은이전단계를반복하여로그인할수있습니다.

공유 **iPad** 에대한 **ASM** 계정관리

Apple Education 에서 XenMobile 을이미사용하는경우: 강사가사용하는장치와같이공유되지않는장치에대한기존 ASM 계정이 XenMobile 에구성되어있습니다. 공유장치와비공유장치모두에동일한 ASM 및동일한 XenMobile 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 의각그룹에대한장치그룹을클래스별또는강사별로만듭니다.

- 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** 계정추가

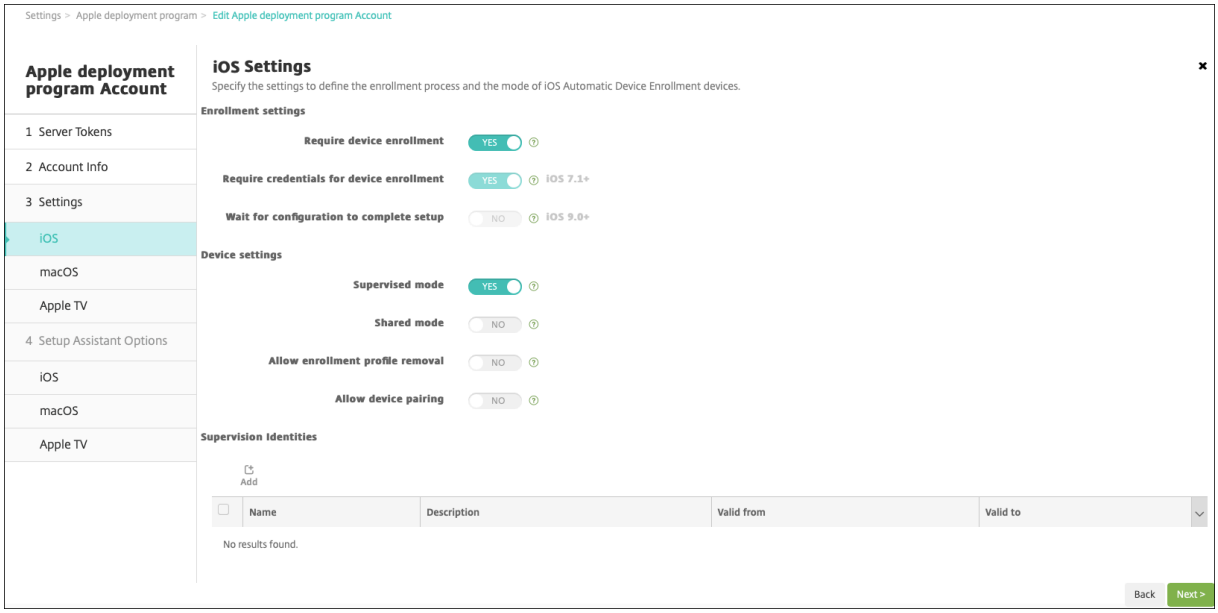
XenMobile 서버콘솔에서여러 ASM 계정을생성하는경우공유 iPad 그룹을자동으로가져옵니다 (각클래스또는강사당 1 대).

- 장치그룹 1 MDM 서버 > 장치그룹 1 계정
- 장치그룹 2 MDM 서버 > 장치그룹 2 계정
- 장치그룹 N MDM 서버 > 장치그룹 N 계정

공유 iPad 와관련된요구사항은다음과같습니다.

- 다음설정이사용되는각장치그룹에대해 ASM 계정 1 개:
  - 장치등록필요
  - 감독모드
  - 공유모드
- 지정된교육조직의경우모든 ASM 계정에동일한 교육접미사를사용해야합니다.

계정을추가하려면 설정 **> Apple** 배포프로그램으로이동합니다.

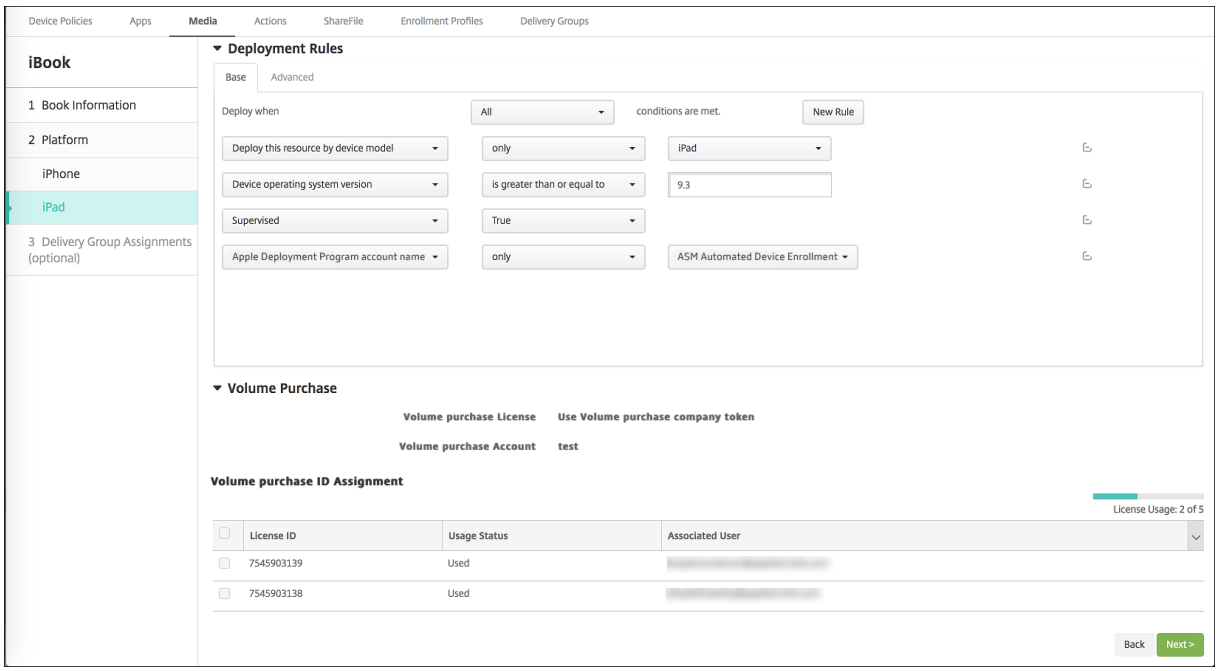


공유 **iPad** 의앱

공유 iPad 는장치기반볼륨구매앱할당을지원합니다. 공유 iPad 에앱을배포하기전에 XenMobile 은장치에볼륨구매라이센스를할당하라는요청을 Apple 볼륨구매서버에보냅니다. 볼륨구매할당을확인하려면 구성 **>** 앱 **> iPad** 로이동하고 볼륨구매를확장합니다.

공유 **iPad** 의미디어

공유 iPad 는사용자기반볼륨구매 iBooks 할당을지원합니다. 공유 iPad 에 iBooks 를배포하기전에 XenMobile 은학생에게볼륨구매라이센스를할당하라는요청을 Apple 볼륨구매서버에보냅니다. 볼륨구매할당을확인하려면 구성 **>** 미디어 **> iPad** 로이동하고 볼륨구매를확장합니다.



공유 **iPad** 에대한배포규칙

공유 iPad 배포의경우배달그룹수준의규칙은사용자속성과관련이있으므로적용되지않습니다. 각장치그룹에대한정책, 앱및미디어를필터링하려면계정이름을기준으로리소스에대한배포규칙을추가합니다. 예:

- 장치그룹 1 계정의경우다음배포규칙을설정합니다.

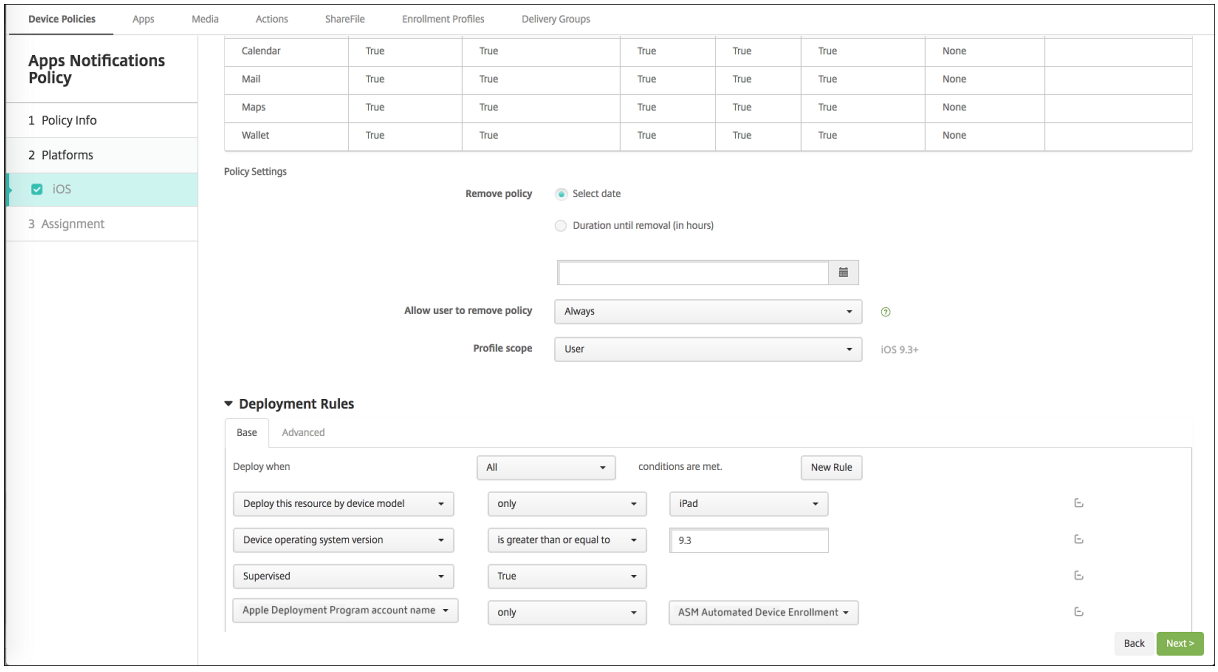
```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```


- 장치그룹 2 계정의경우다음배포규칙을설정합니다.

```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- 장치그룹 N 계정의경우다음배포규칙을설정합니다.

```
Apple Deployment Program account name
Only
Device Group N account

<!--NeedCopy-->
```



Apple 교실앱을강사에게만배포하려면 (공유되지않는 iPad 사용) 다음배포규칙을사용하여 'ASM 에공유됨' 상태로리소스를필터링합니다.

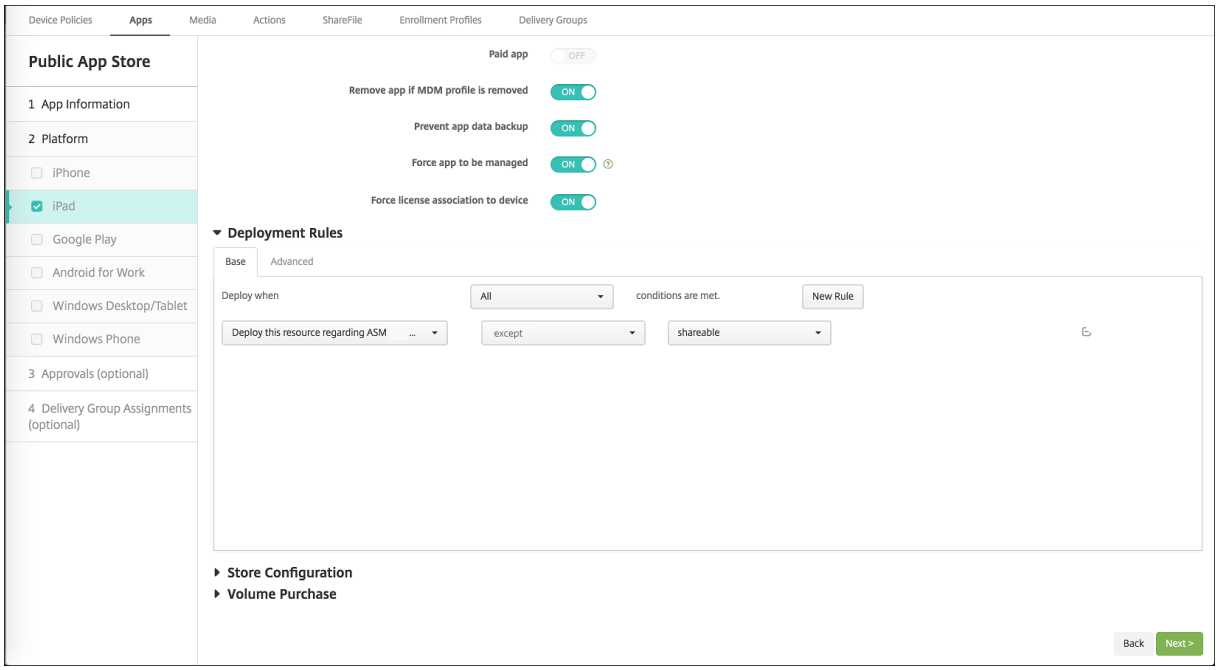
```
Deploy this resource regarding ASM shared mode
only
unshared

```



```
<!--NeedCopy-->
```

또는:

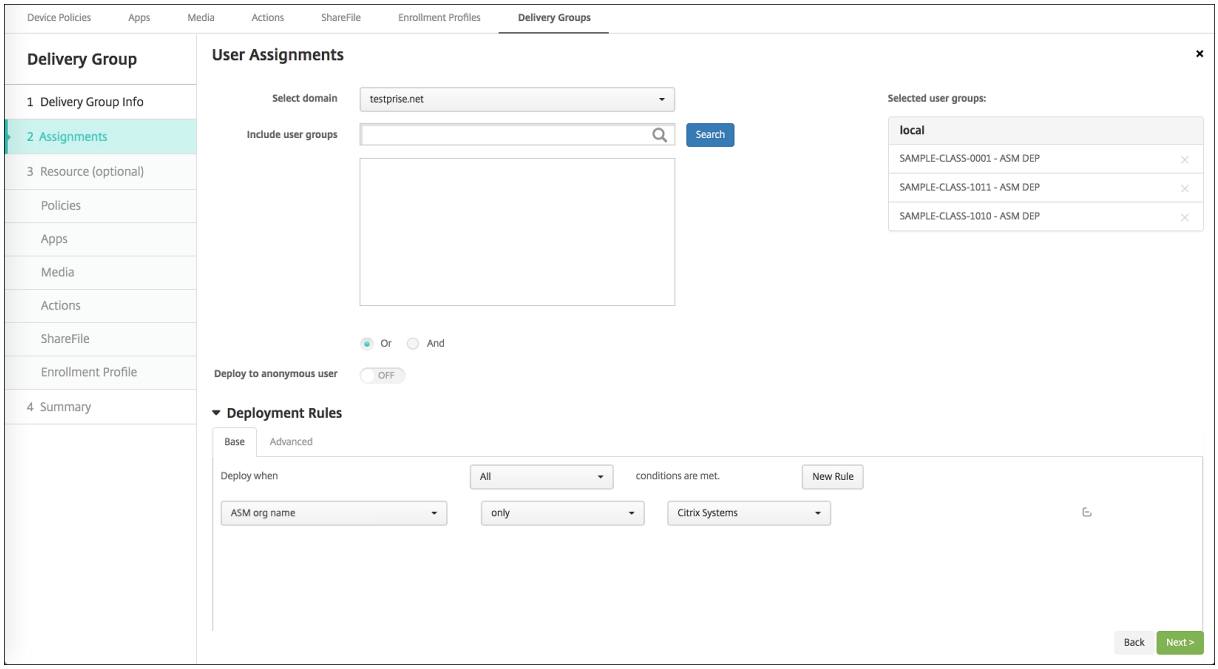
```
Deploy this resource regarding ASM shared mode
except
shareable

<!--NeedCopy-->
```



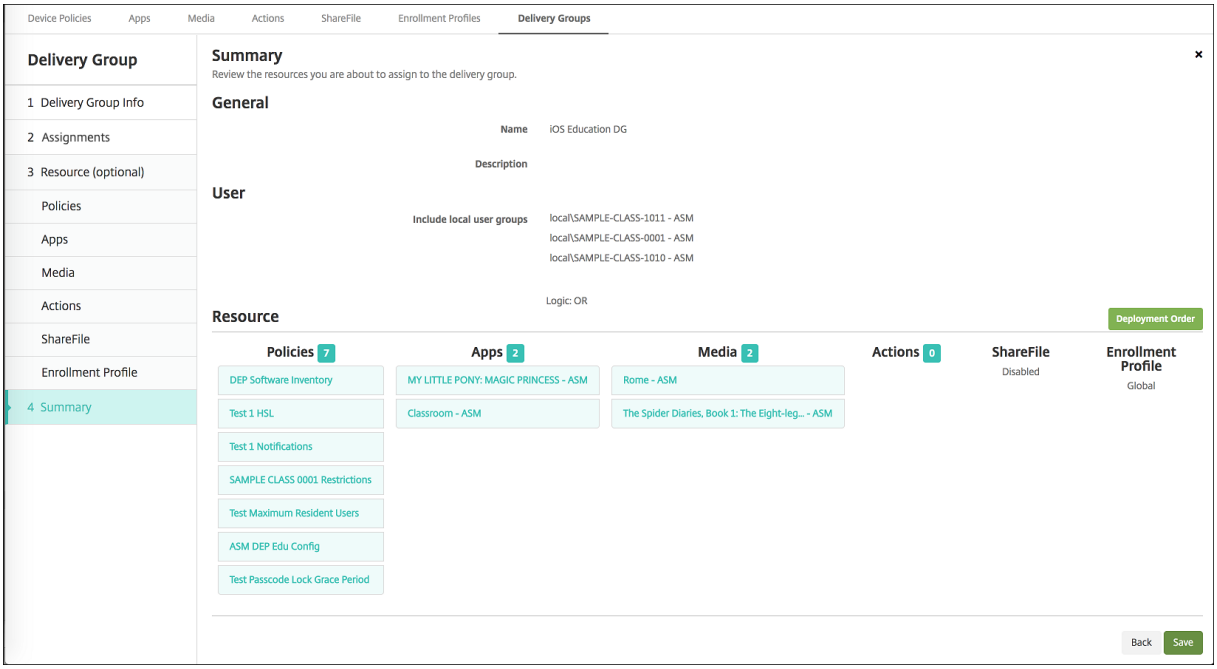
공유 **iPad** 의배달그룹

각강사의장치그룹에대해

- 하나의배달그룹을구성합니다. 강사의경우교육구성정책에서정의하는모든클래스를할당합니다.



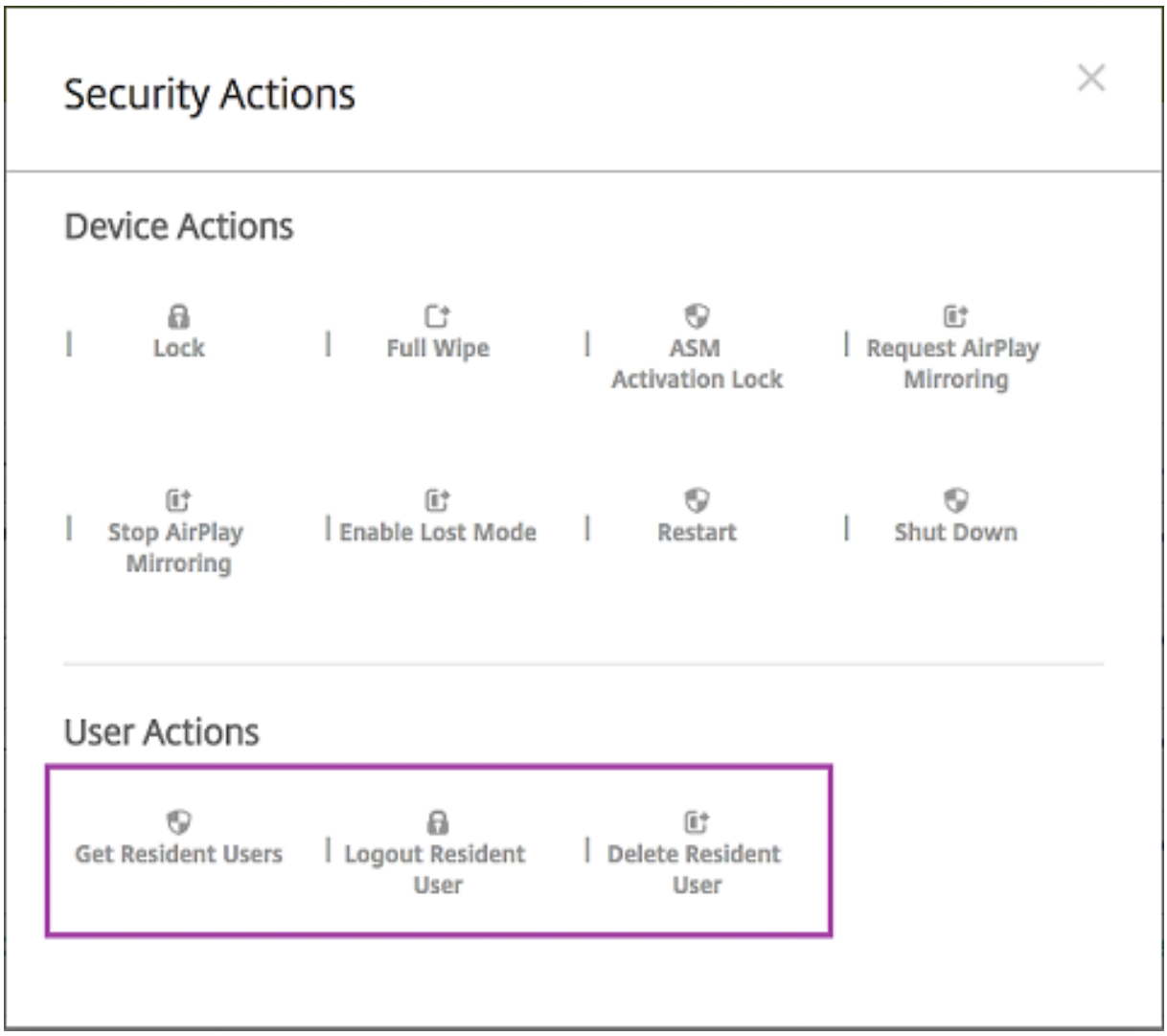
- 해당배달그룹에는다음과같은 MDM 리소스가포함되어야합니다.
  - 장치정책:
    - 교육구성
    - 잠금화면메시지
    - 앱알림
    - 홈화면레이아웃
    - 제한사항
    - 최대상주사용자수
    - 암호잠금유예기간
  - 필수볼륨구매앱
  - 필수볼륨구매 iBooks



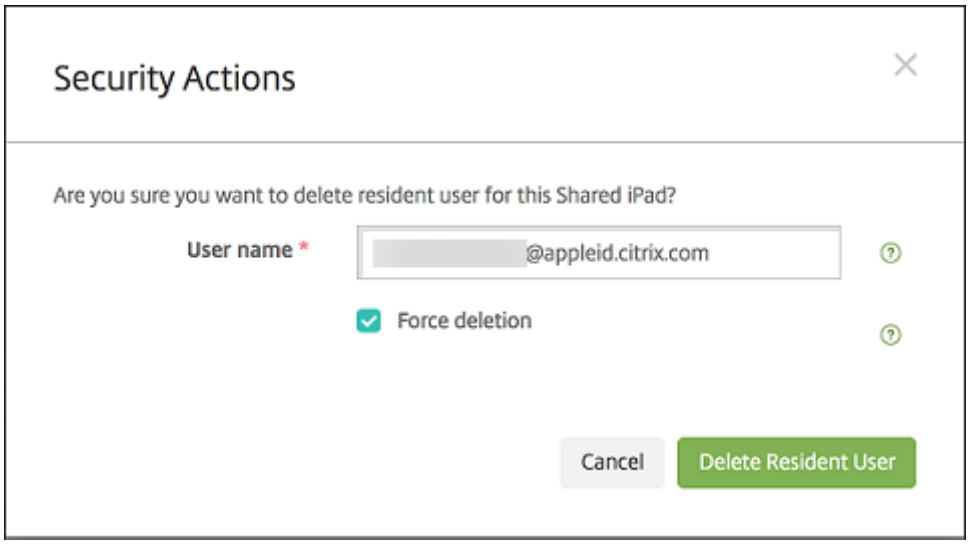
공유 **iPad** 의보안동작

기존보안동작외에공유 iPad 에대해다음보안동작을사용할수있습니다.

- 상주사용자가져오기**:** 현재장치에활성계정이있는사용자를나열합니다. 이동작은장치와 XenMobile 콘솔간에강제로동기화됩니다.
- 상주사용자로그아웃**:** 현재사용자의로그아웃을강제수행합니다.
- 상주사용자삭제**:** 특정사용자에대한현재세션을삭제합니다. 사용자는다시로그인할수있습니다.



상주사용자삭제를클릭한후사용자이름을지정할수있습니다.

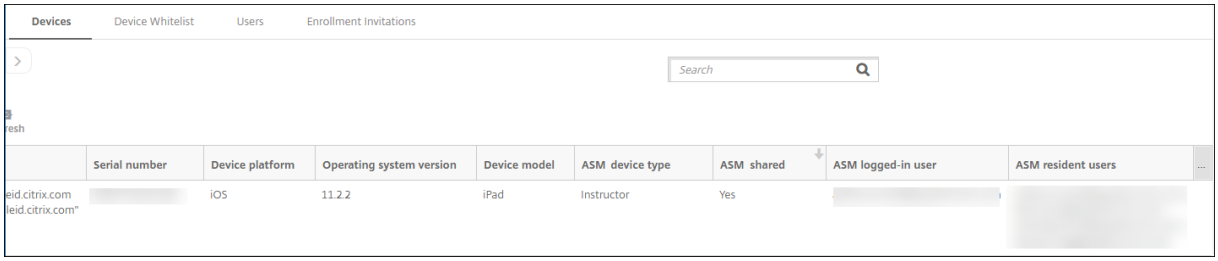


보안동작결과는 관리 **>** 장치 **>** 일반및 관리 **>** 장치 **>** 배달그룹페이지에나타납니다.

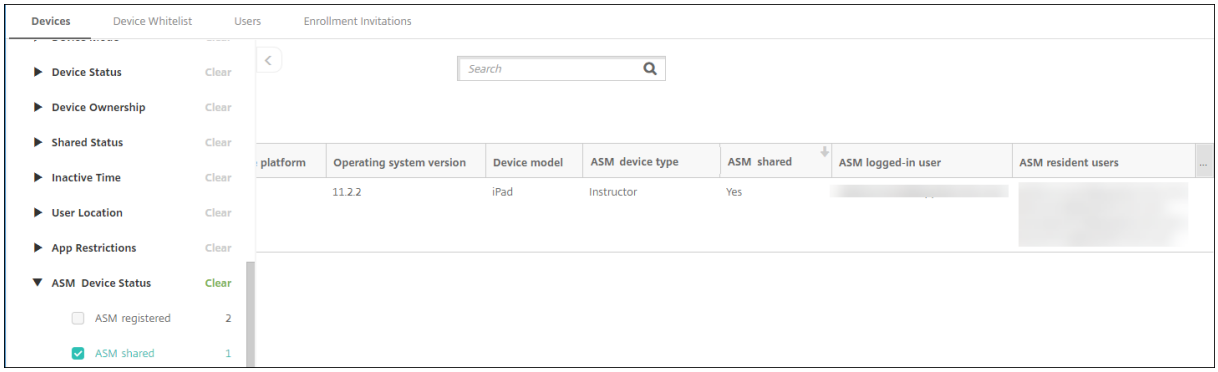
공유 **iPad** 에대한정보얻기

관리 **>** 장치페이지에서공유 iPad 와관련된정보를찾습니다.

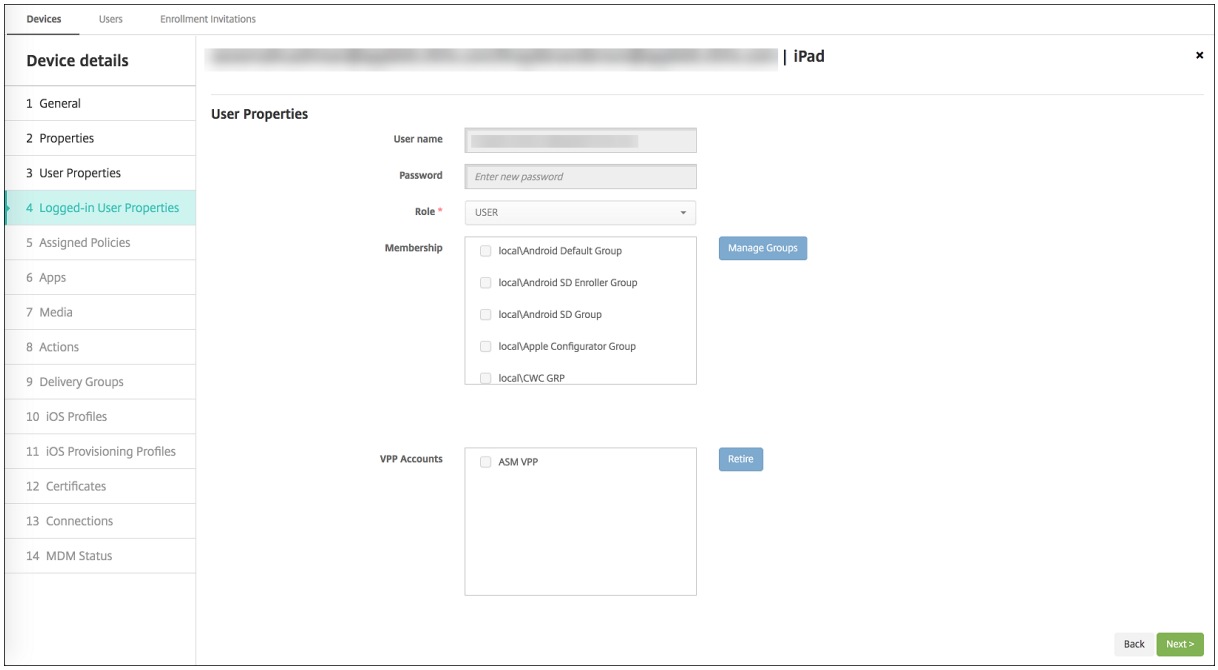
- 다음을조회할수있습니다.
  - 장치의공유여부 (**ASM** 에공유됨)
  - 공유장치에로그인한사용자 (**ASM** 에로그인한사용자)
  - 공유장치에할당된모든사용자 (**ASM** 상주사용자)

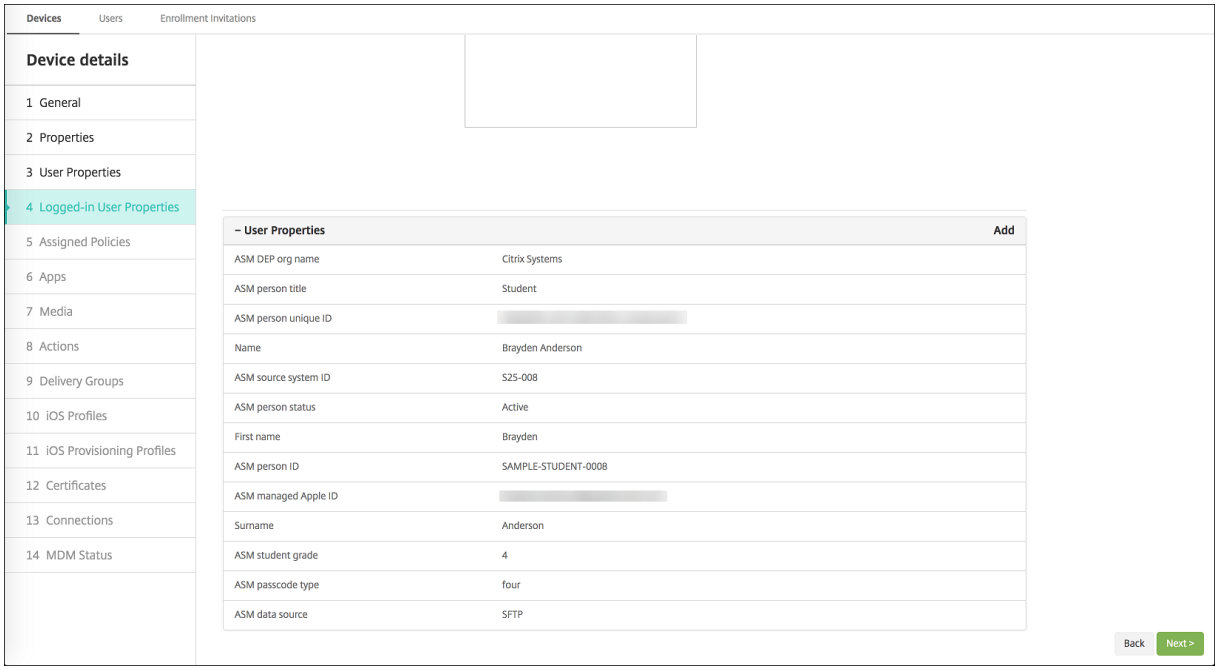


- **ASM** 장치상태로장치목록을필터링합니다.

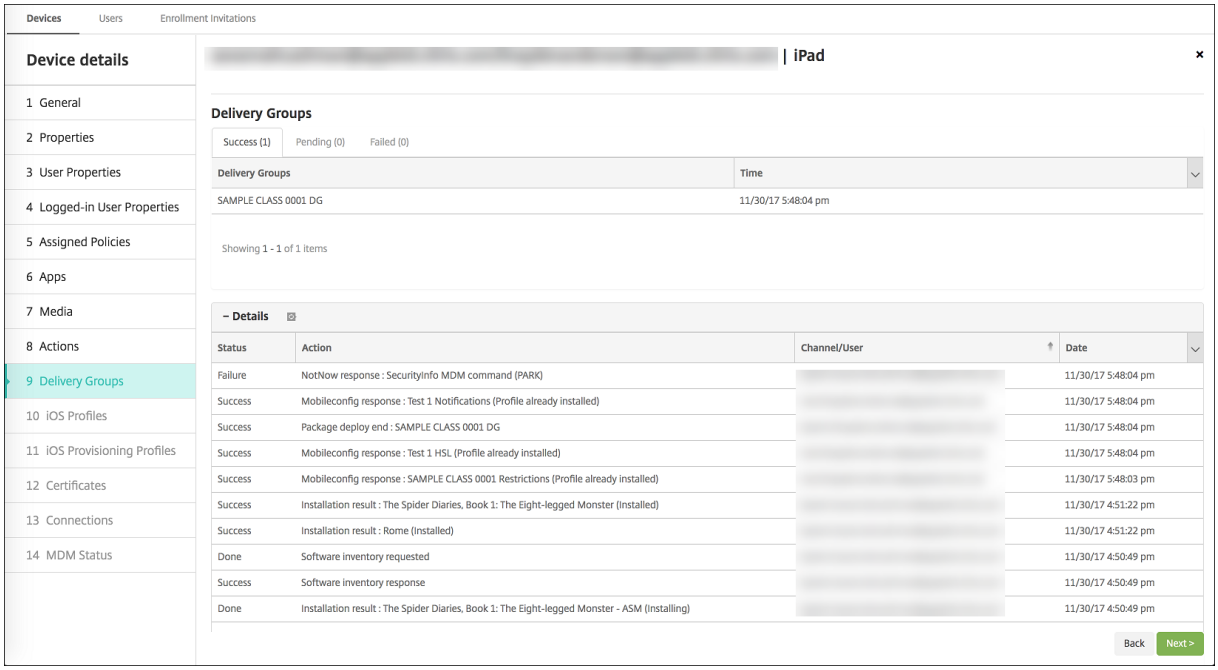


- 관리 **>** 장치 **>** 로그인한사용자속성페이지에서공유 iPad 에로그인한사용자에대한세부정보를봅니다.

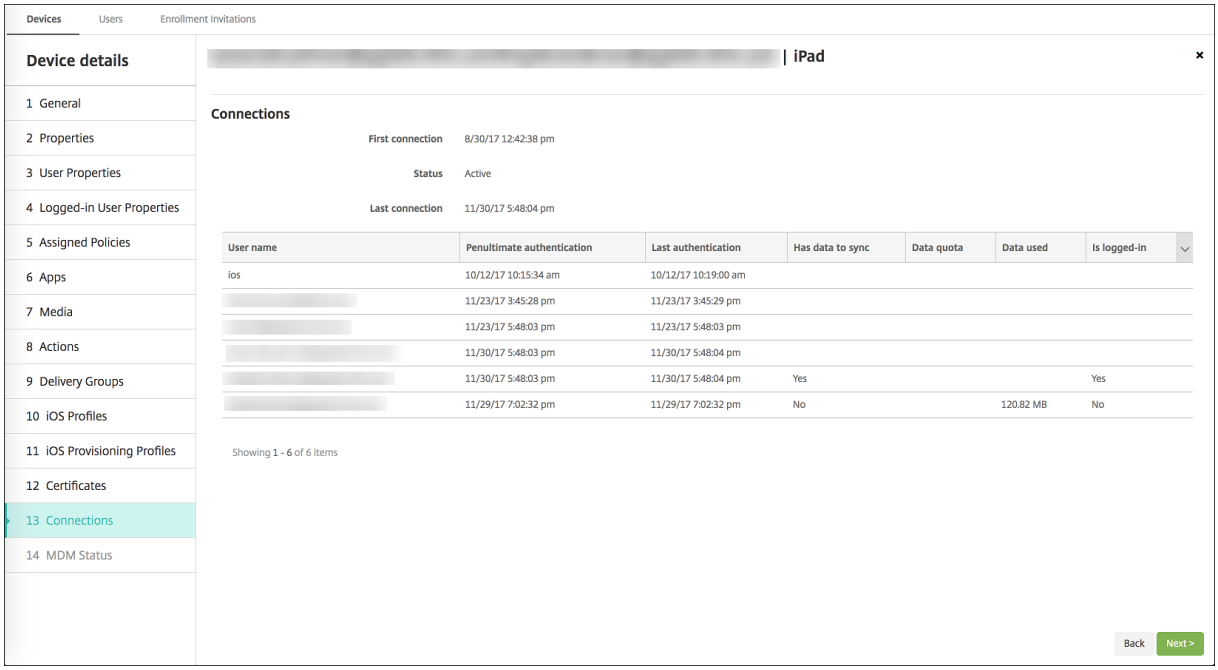




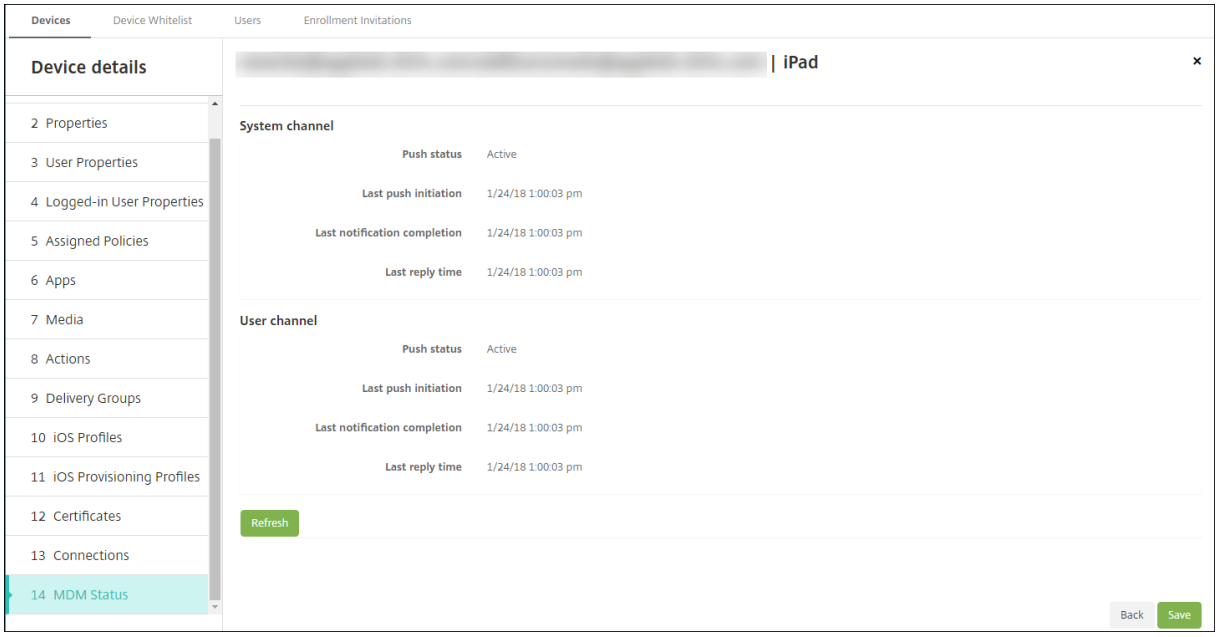
- 관리 **>** 장치 **>** 배달그룹페이지에서배달그룹의강사및사용자에게리소스를배포할때사용되는채널을확인합니다. 채널/사용자열에는유형 (시스템또는 사용자) 과받는사람 (강사또는학생) 이표시됩니다.



- 상주사용자에대한정보를확인합니다.
  - 동기화할데이터있음**:** 사용자에게클라우드에동기화할데이터가있는지여부를나타냅니다.
  - 데이터할당량**:** 사용자에게설정된데이터할당량 (바이트) 입니다. 사용자할당량이일시적으로꺼져있거나사용자에게적용되지않는경우할당량이표시되지않을수있습니다.
  - 사용한데이터**:** 사용자가사용한데이터의양 (바이트) 입니다. 시스템에서정보를수집할때오류가발생하면값이나타나지않을수있습니다.
  - 로그인되어있음**:** 사용자가장치에로그온했는지여부를나타냅니다.



- 두채널의푸시상태를확인합니다.



강사, 학생및클래스데이터관리

강사, 학생및클래스데이터를관리하는경우다음을참고하십시오.

- ASM 정보를 XenMobile 로가져온후에는관리되는 Apple ID 를변경하지마십시오. XenMobile 은 ASM 사용자식별자를사용하여사용자를식별합니다.
- 하나이상의교육구성장치정책을생성한후 ASM 의클래스데이터를추가하거나변경하는경우: 정책을편집하고다시배포합니다.
- 교육구성장치정책을배포한후클래스의강사가변경되는경우: 정책을검토하여 XenMobile 콘솔에서업데이트되는지확인한후정책을다시배포합니다.
- ASM 포털에서사용자속성을업데이트하면 XenMobile 이이러한속성을콘솔에도업데이트합니다. 그러나 ASM 사용자직위속성 (강사, 학생또는기타) 은다른속성과같은방법으로 XenMobile 에전송되지않습니다. 그러므로 ASM 에서 ASM 사용자직위를변경하는경우다음단계를수행하여 XenMobile 에변경내용이반영될수있도록하십시오.

데이터를관리하려면:

1. ASM 포털에서학생학년을업데이트하고강사학년을지웁니다.
2. 학생계정을강사계정으로변경한경우클래스의학생목록에서해당사용자를제거합니다. 그런다음동일한클래스또는다른클래스의강사목록에사용자를추가합니다.

   강사계정을학생계정으로변경한경우클래스에서해당사용자를제거합니다. 그런다음동일한클래스또는다른클래스의학생목록에사용자를추가합니다. 다음동기화 (기본적으로 5 분마다) 또는가져오기 (기본적으로 24 시간마다) 중에업데이트내용이 XenMobile 콘솔에표시됩니다.
3. 변경내용을적용하도록교육구성장치정책을편집하고다시배포합니다.

- ASM 포털에서사용자를삭제하면 XenMobile 이가져오기후 XenMobile 콘솔에서도해당사용자를삭제합니다.

  다음서버속성값을변경하여두기준사이의간격을줄일수있습니다. **bulk.enrollment.fetchRosterInfoDelay**(기본값은 **1440** 분)

- 리소스배포후: 학생이클래스에참여하면해당학생만포함된배달그룹을생성하고리소스를학생에게배포합니다.
- 학생또는강사가임시암호를잊은경우 ASM 관리자에게문의하도록하십시오. 관리자는임시암호를제공하거나새암호를생성할수있습니다.

Apple School Manager Apple 배포프로그램에등록된분실또는도난장치관리

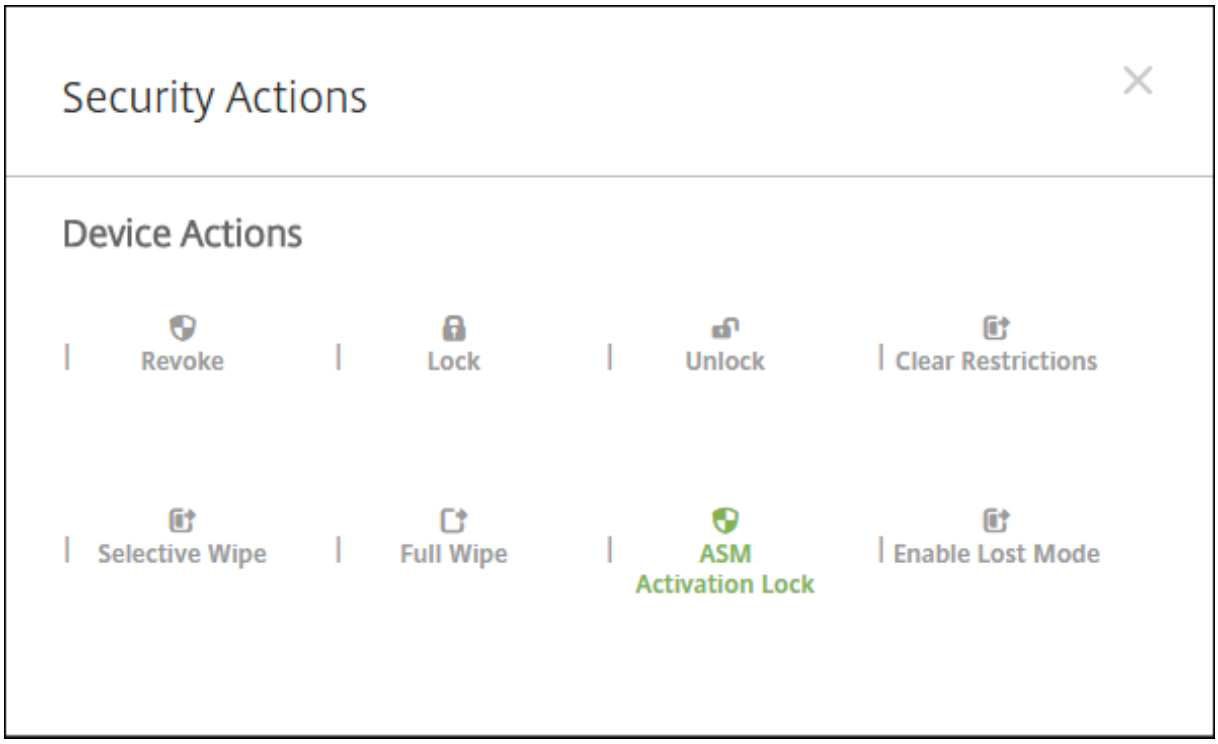
Apple 의내 iPhone/iPad 찾기서비스에는활성화잠금기능이포함되어있습니다. 활성화잠금기능은권한이없는사용자가 Apple 배포프로그램에등록된분실또는도난장치를사용하거나재판매할수없도록합니다.

XenMobile 에포함된 **ASM** 활성화잠금보안동작을사용하면 ASM Apple 배포프로그램등록장치에잠금코드를전송할수있습니다.

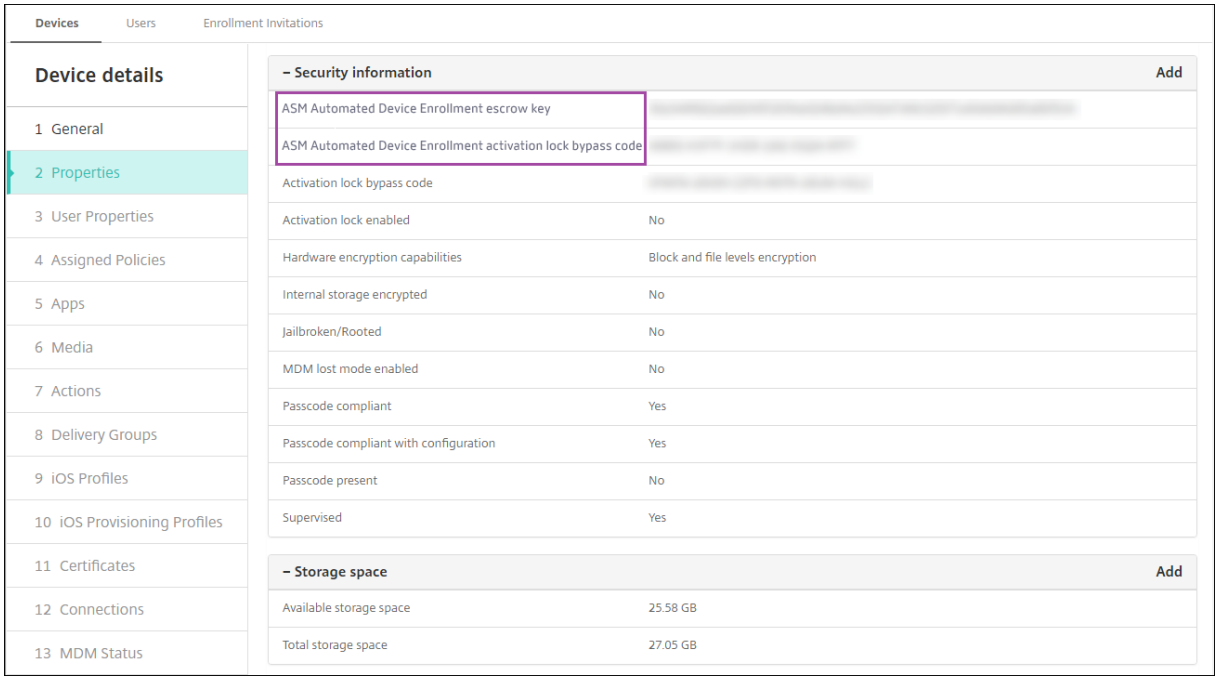
ASM 활성화잠금보안동작을사용하면사용자가내 iPhone/iPad 찾기서비스를사용하지않고 XenMobile 을통해장치를찾을수있습니다. ASM 장치가하드리셋되거나전체초기화된경우사용자는관리되는 Apple ID 와암호를제공하여장치잠금을해제할수있습니다.

콘솔에서잠금을해제하려면 활성화잠금바이패스보안동작을클릭합니다. 활성화잠금바이패스에대한자세한내용은 iOS 활성화잠금바이패스를참조하십시오. 또한로그인을비워두고 **ASM** 활성화잠금바이패스코드를암호로입력할수도있습니다. 이정보는 장치세부정보의 속성탭에나와있습니다.

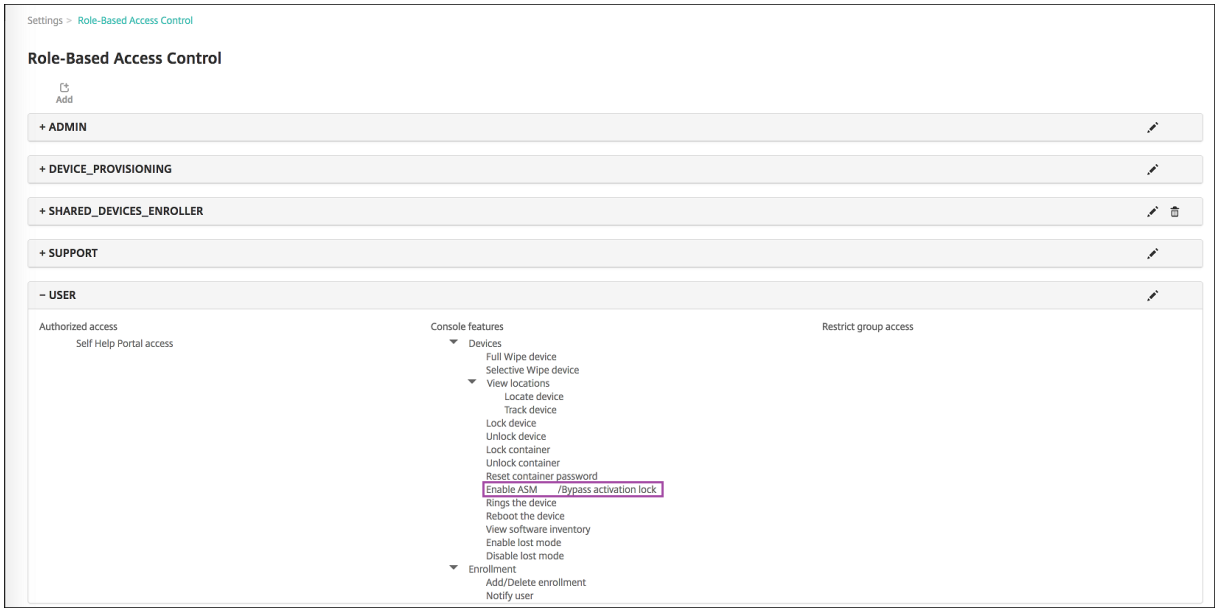
활성화잠금을설정하려면 관리 **>** 장치에서장치를선택하고 보안을클릭한후 **ASM** 활성화잠금을클릭합니다.



ASM 에스크로키와 **ASM** 활성화잠금바이패스코드속성은 장치세부정보에표시됩니다.



ASM 활성화잠금에대한 RBAC 권한은 장치 **>ASM** 활성화잠금바이패스입니다.



Apple 앱배포

August 12, 2022

XenMobile 은장치에배포되는앱을관리합니다. 다음유형의 iOS/iPadOS 및 macOS 앱을구성하고배포할수있습니다.

- 공용앱스토어 **(iOS/iPadOS** 전용**):** Apple App Store 또는 Google Play 와같은공용앱스토어에서무료또는유료로제공되는앱이포함됩니다. 예를들어 GoToMeeting 이포함됩니다.
- **Enterprise(iOS/iPadOS/macOS):** MDX 가지원되지않으며 MDX 앱과연결된정책이포함되지않는기본앱입니다.
- **MDX(iOS/iPadOS** 전용**):** MAM SDK 로준비되거나 MDX Toolkit 으로래핑된앱입니다. 이러한앱에는 MDX 정책이포함됩니다. 내부및공용스토어에서 MDX 앱을얻을수있습니다.
- 볼륨구매 **(iOS/iPadOS/macOS):** Apple 볼륨구매프로그램을통해관리되는라이센스가적용된앱입니다.
- **iOS** 사용자지정앱 **(iOS/iPadOS** 전용**):** 사내에서또는타사에서개발한독점 B2B 앱입니다.

다양한앱유형에관한정보는 앱추가에서확인하십시오.

배포중에는 Apple Business Management(ABM) 또는 Apple School Management(ASM) 계정이필요한배포가있습니다. 자세한내용은다음섹션을참조하십시오.

Citrix 에서는앱및배포방식의각유형에대해구성집합을사용하기를권장합니다. 기타플랫폼의앱배포에관한정보는 앱추가에서확인하십시오. 다음섹션에서는 iOS 앱구성에관해더자세히알아봅니다.

앱배포의일반적인단계

시나리오	1 단계: 계정연결	2 단계: 앱추가및구성	3 단계: 배달그룹구성및앱배포
공용앱스토어앱, Citrix 이동성앱포함	해당없음	**XenMobile** 에서**:** 구성 **>** 앱으로이동하여 iPhone 또는 iPad 용 공용앱스토어앱을추가합니다. 앱을구성하고배달그룹에할당합니다.	**XenMobile** 에서**:** 배달그룹을사용하여앱을구성하고배포합니다.
Apple 볼륨구매를통해제공되는공용앱스토어앱, Citrix 이동성앱포함	Apple 배포프로그램에등록합니다. **XenMobile** 에서**:** 설정 **>** 볼륨구매로이동하여볼륨구매계정을추가합니다.	**ABM** 또는 **ASM** 에서**:** Apps 및 Books 에서앱을구매하고추가합니다. **XenMobile** 에서**:** 구성 **>** 앱으로이동한다음앱을구성하고배달그룹에할당합니다.	**XenMobile** 에서**:** 배달그룹을사용하여앱을구성하고배포합니다.
엔터프라이즈앱	해당없음	**XenMobile** 에서**:** 구성 **>** 앱으로이동합니다. 추가를클릭한다음 엔터프라이즈를클릭합니다. IPA 파일을업로드합니다. 앱을구성하고배달그룹에할당합니다.	**XenMobile** 에서**:** 배달그룹을사용하여앱을구성하고배포합니다.

시나리오	1 단계: 계정연결	2 단계: 앱추가및구성	3 단계: 배달그룹구성및앱배포
MDX 앱	해당없음	**XenMobile** 에서**:** 구성 **>** 앱으로이동합니다. 추가를 클릭한다음 **MDX** 를클릭합니다. 플랫폼에대해 **iPad**/**iPhone** 을선택해야합니다. MDX 파일을업로드합니다. 앱을구성하고배달그룹에할당합니다.	**XenMobile** 에서**:** 배달그룹을사용하여앱을구성하고배포합니다.
Apple 볼륨구매로배포된 MDX 앱	Apple 배포프로그램에등록합니다. **XenMobile** 에서**:** 설정 **>** 볼륨구매로이동하여볼륨구매계정을추가합니다.	**ABM** 에서**:** Apps 및 Books 에서앱을구매하고추가합니다. ABM 계정에앱을연결합니다. **XenMobile** 에서**:** 구성 **>** 앱으로이동한다음앱을구성하고배달그룹에할당합니다.	**XenMobile** 에서**:** 배달그룹을사용하여앱을구성하고배포합니다.
사용자지정앱	Apple 배포프로그램에등록합니다. **XenMobile** 에서**:** 설정 **>** 볼륨구매로이동하여볼륨구매계정을추가합니다.	**ABM** 에서**:** 앱을 App Store 에비공개앱으로추가합니다. 앱을 ABM 계정에연결합니다. **XenMobile** 에서**:** 구성 **>** 앱으로이동한다음앱을구성하고배달그룹에할당합니다.	**XenMobile** 에서**:** 배달그룹을사용하여앱을구성하고배포합니다.
MDX 지원사용자지정앱	Apple 배포프로그램에등록합니다. **XenMobile** 에서**:** 설정 **>** 볼륨구매로이동하여볼륨구매계정을추가합니다.	**ABM** 에서**:** 앱을 App Store 에비공개앱으로추가합니다. 앱을 ABM 계정에연결합니다. **XenMobile** 에서**:** 구성 **>** 앱으로이동한다음 MDX 파일을업로드합니다. 앱을구성하고배달그룹에할당합니다.	**XenMobile** 에서**:** 배달그룹을사용하여앱을구성하고배포합니다.

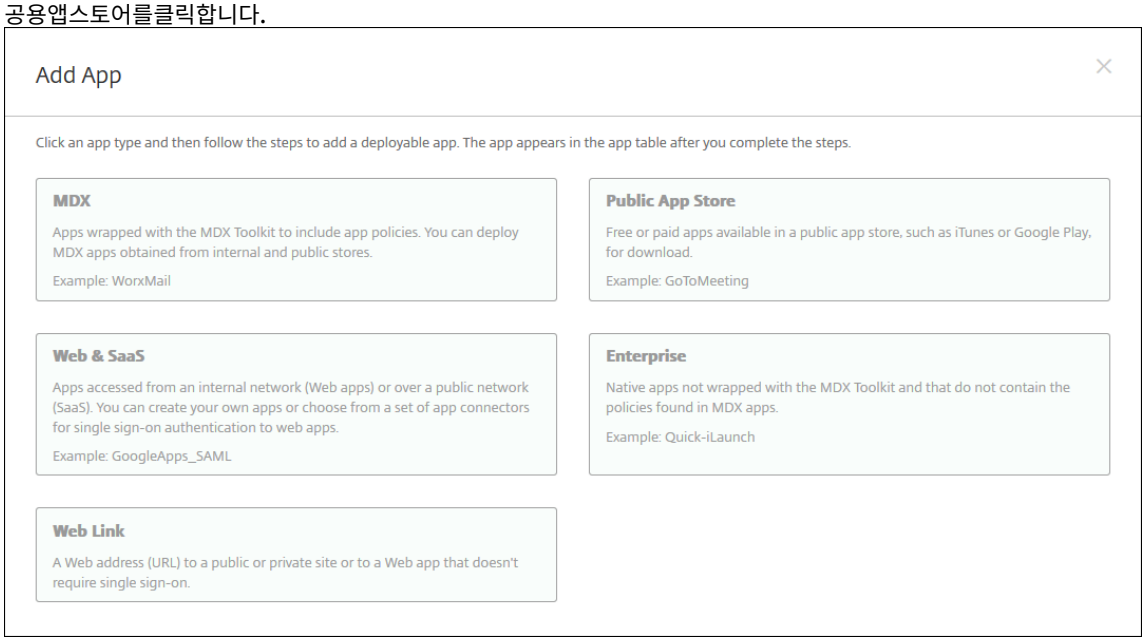
공용앱스토어앱

App Store 에서제공되는유료및무료앱을 XenMobile 에추가할수있습니다.

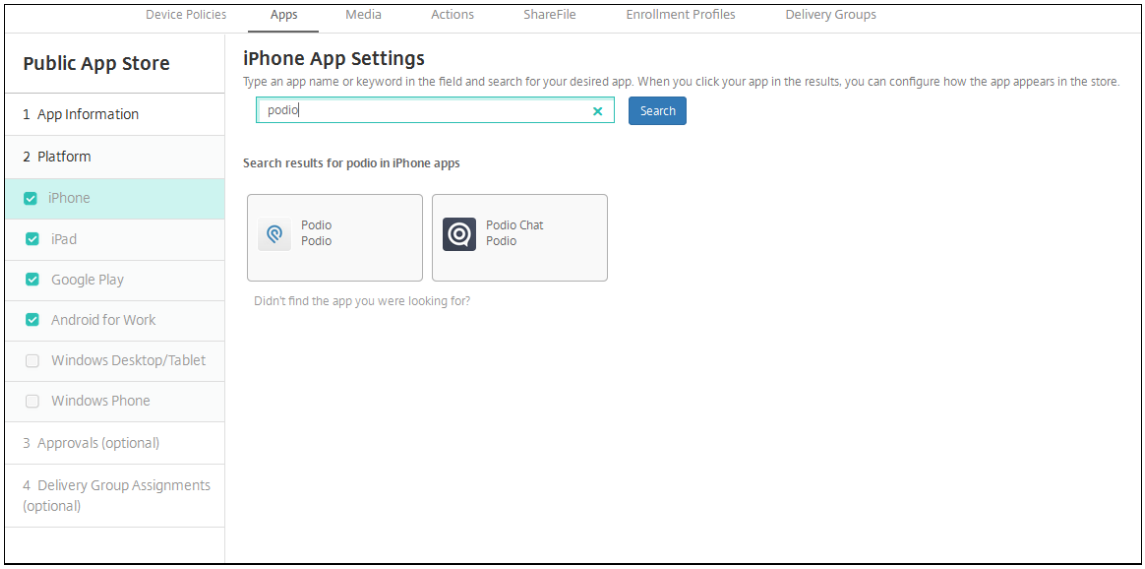
기능가용성	
장치감독필요	아니요
사용자등록모드제공	아니요
사용가능한플랫폼	iOS/iPadOS

1 단계**:** 앱추가및구성

1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 추가를클릭합니다.
2. 공용앱스토어를클릭합니다.



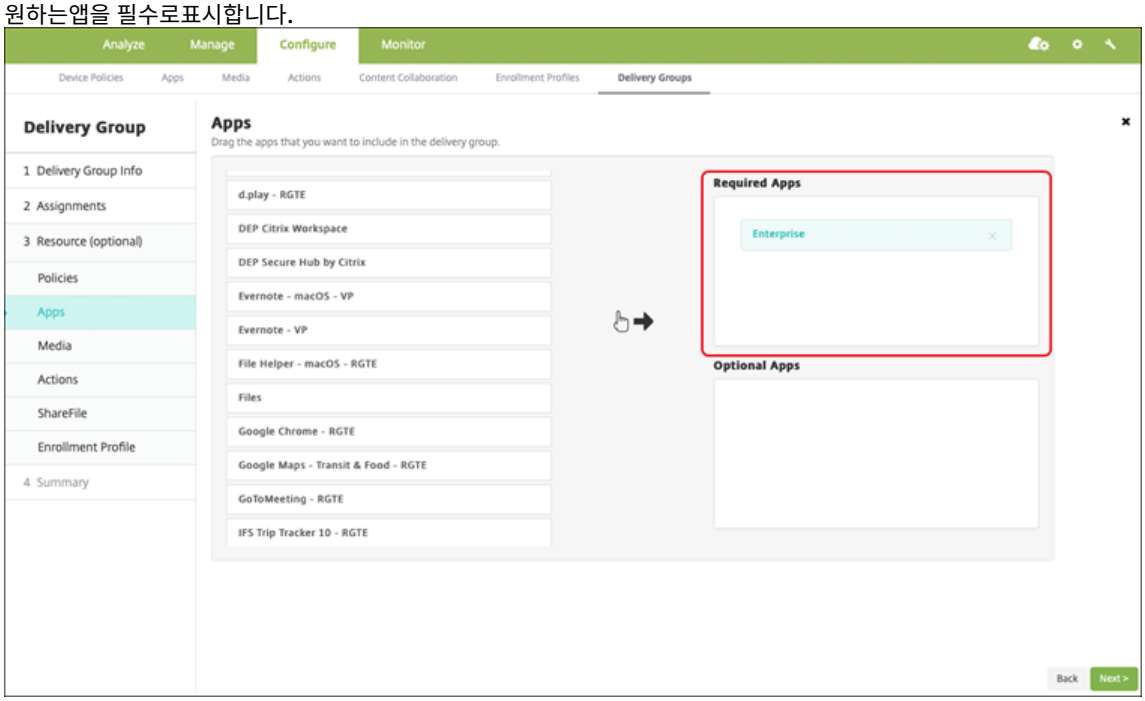
3. 플랫폼에대해 **iPhone** 또는 **iPad** 를선택합니다.
4. 검색상자에앱이름을입력하고 검색을클릭합니다.



5. 검색기준과일치하는앱이표시됩니다. 원하는앱을클릭합니다.
6. 배달그룹을앱에할당하고 저장을클릭합니다.

2 단계**:** 앱배포구성

1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다.
2. 구성할앱을선택하고 편집을클릭합니다.
3. Citrix 에서는 강제로앱관리기능을사용하기를권장합니다.
4. 배달그룹을할당하고 저장을클릭합니다.
5. 구성 **>** 배달그룹 **>** 앱으로이동합니다.
6. 원하는앱을 필수로표시합니다.



7. 구성 **>** 배달그룹으로다시돌아갑니다.
8. 배달그룹을선택하고 배포를클릭합니다.
9. 사용자는앱을설치하라는요청을받고수락후앱이백그라운드에서설치됩니다.

Apple 볼륨구매를통해제공되는공용앱스토어앱

Apple 볼륨구매프로그램을통해 iOS/iPadOS 앱라이센스를관리할수있습니다. XenMobile 에볼륨구매앱을추가하려면이러한단계를따릅니다.

기능가용성	
장치감독필요	아니요
사용자등록모드제공	예
사용가능한플랫폼	iOS/iPadOS/macOS

1 단계**:** 계정연결

1. Apple Business Manager(ABM) 또는 Apple School Manager(ASM) 에서설정하고등록합니다. 이러한프로그램에대한자세한내용은 Apple 설명서를참조하십시오.
2. XenMobile 로 ABM/ASM 계정을연결합니다. 볼륨구매계정연결에대한자세한내용은 Apple 볼륨구매를참조하십시

오.

3. 볼륨구매계정을추가할경우 앱자동업데이트를활성화합니다. 이설정을사용하면 Apple 앱스토어에업데이트가나타날경우사용자기기의앱이자동으로업데이트됩니다.

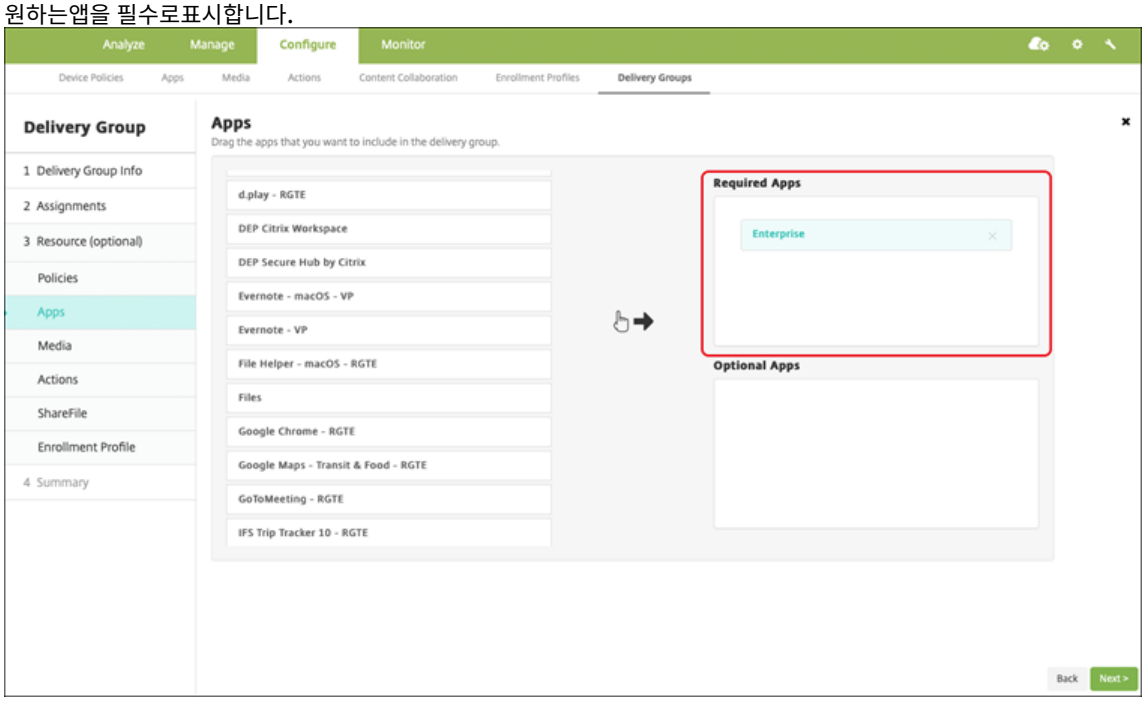
2 단계**: Apple** 에서앱과라이센스받기

ABM/ASM 계정에서앱을추가합니다. Apple App Store 또는 Apple Books(iOS/iPadOS 전용) 에서구매한항목을추가할수있습니다. 무료앱이라도모두구매해야합니다.

앱을비즈니스에서사용할수있도록하는방법은 Apple 설명서에서참고하십시오.

3 단계**:** 앱배포구성

1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다.
2. 구성할볼륨구매앱을선택하고 편집을클릭합니다.
3. **iPhone**, **iPad** 또는 **macOS** 중에서플랫폼을선택합니다.
4. Citrix 에서는 강제로앱관리기능 (iOS/iPadOS 전용) 을사용하기를권장합니다.
5. 배달그룹을할당하고 저장을클릭합니다.
6. 구성 **>** 배달그룹 **>** 앱으로이동합니다.
7. 원하는앱을 필수로표시합니다.



8. 구성 **>** 배달그룹으로다시돌아갑니다.
9. 배달그룹을선택하고 배포를클릭합니다.
10. 사용자는앱을설치하라는요청을받고수락후앱이백그라운드에서설치됩니다.

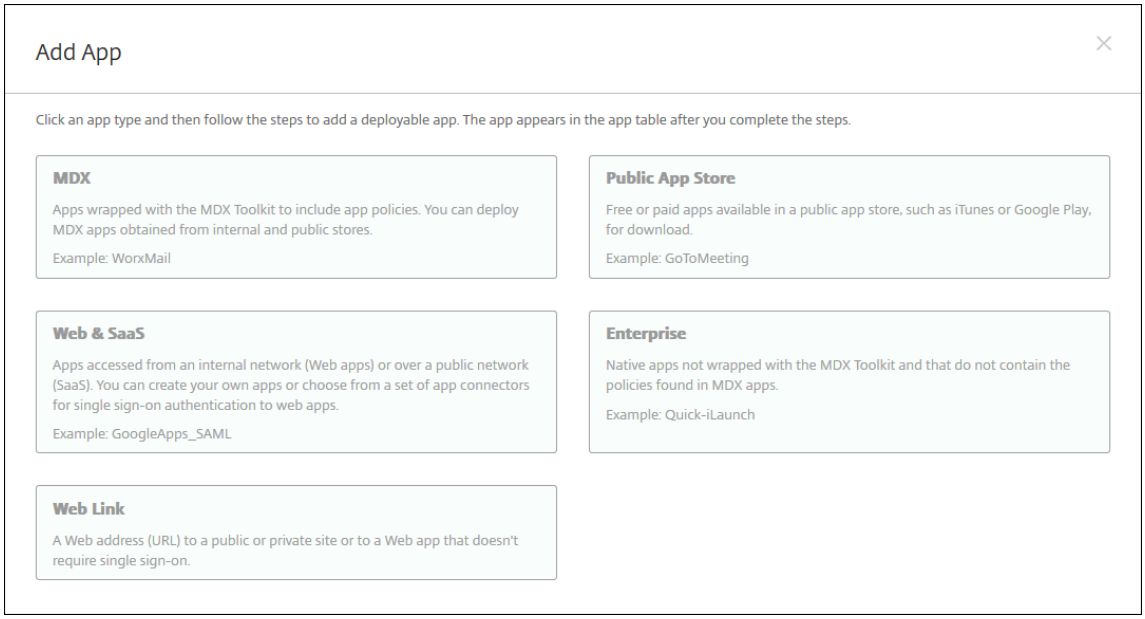
엔터프라이즈앱

MDX 정책이연결되어있지않은기본앱도추가할수있습니다. App Store 에없는앱을추가하려면이러한단계를따릅니다.

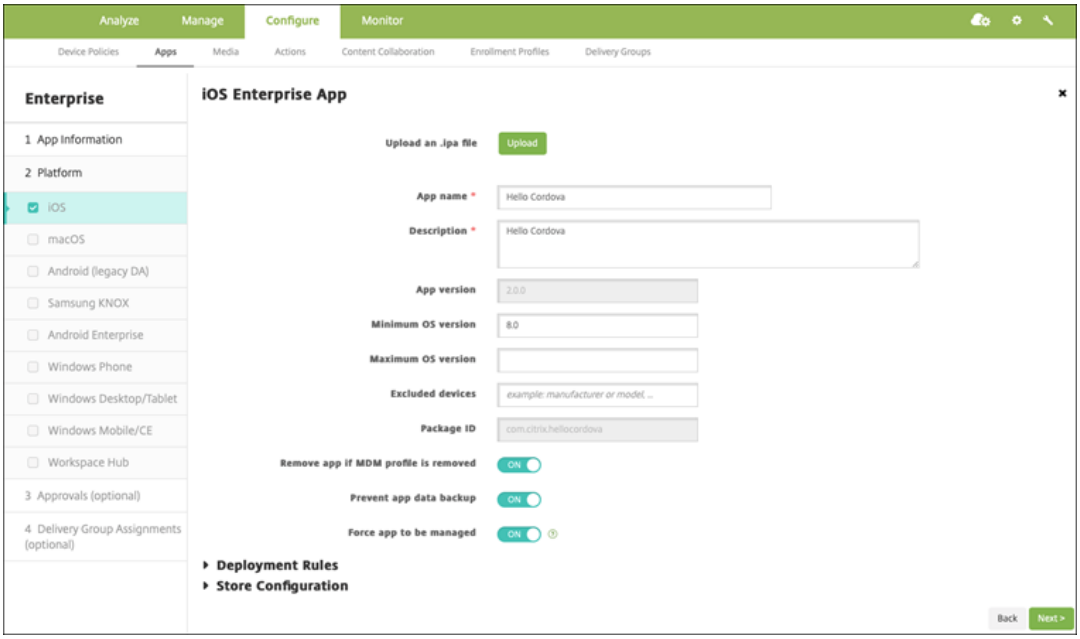
기능가용성	
장치감독필요	아니요
사용자등록모드제공	예
OS	iOS/iPadOS/macOS

1 단계**:** 앱추가및구성

1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 추가를클릭합니다.
2. 엔터프라이즈를클릭합니다.



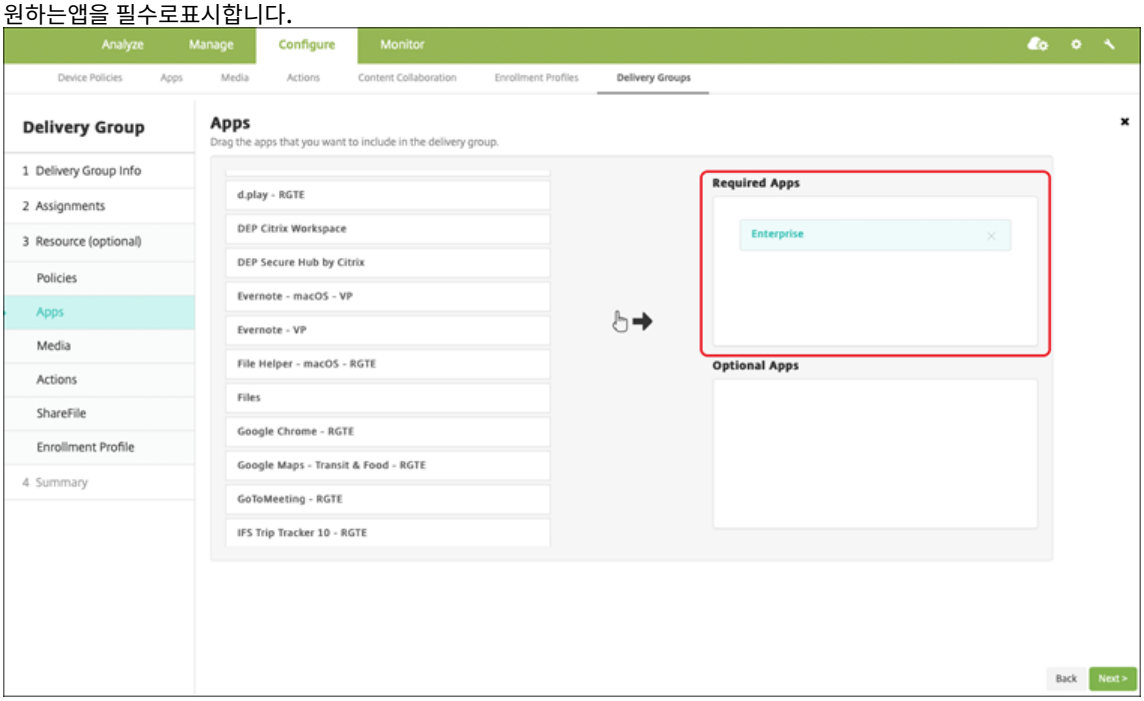
3. 앱정보페이지에서다음을구성합니다.
   - 이름**:** 앱을설명하는이름을입력합니다. 이이름은앱테이블의앱이름아래에표시됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다.
4. 다음을클릭합니다. 앱플랫폼페이지가나타납니다.
5. **iPhone**, **iPad** 또는 **macOS** 중에서플랫폼을선택합니다.
6. IPA 파일업로드 (iOS/iPadOS) 또는 PKG 파일업로드 (macOS)
7. 다음을클릭합니다. 앱세부정보페이지가나타납니다.
8. 다음설정을구성합니다.
   - 파일이름**:** 필요한경우앱의새이름을입력합니다.
   - 앱설명**:** 필요한경우앱에대한새설명을입력합니다.
   - 앱버전**:** 이필드는변경할수없습니다.
   - 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
   - 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
   - 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.
   - **MDM** 프로필이제거된경우앱제거**:** MDM 프로필이제거된경우장치에서앱을제거할지여부를선택합니다. 기본값은켜짐입니다.(iOS/iPadOS 전용)
   - 앱데이터백업방지**:** 앱이데이터를백업하는것을방지할지여부를선택합니다. 기본값은켜짐입니다.(iOS/iPadOS 전용)
   - 강제로앱관리**:** 관리되지않는앱을설치하는경우감독되지않는장치의사용자에게앱관리를허용하라는메시지를표시하려면 켜짐을선택합니다. 사용자가메시지를수락하면앱이관리됩니다.(iOS/iPadOS 전용)



9. 배달그룹을앱에할당하고 저장을클릭합니다.

2 단계**:** 앱배포구성

1. XenMobile 콘솔에서 구성 **>** 배달그룹으로이동합니다. 구성할배달그룹을선택하고 앱페이지를클릭합니다.
2. 원하는앱을 필수로표시합니다.



3. 구성 **>** 배달그룹으로이동합니다.
4. 배달그룹을선택하고 배포를클릭합니다.
5. 사용자는앱을설치하라는요청을받고수락후앱이백그라운드에서설치됩니다.

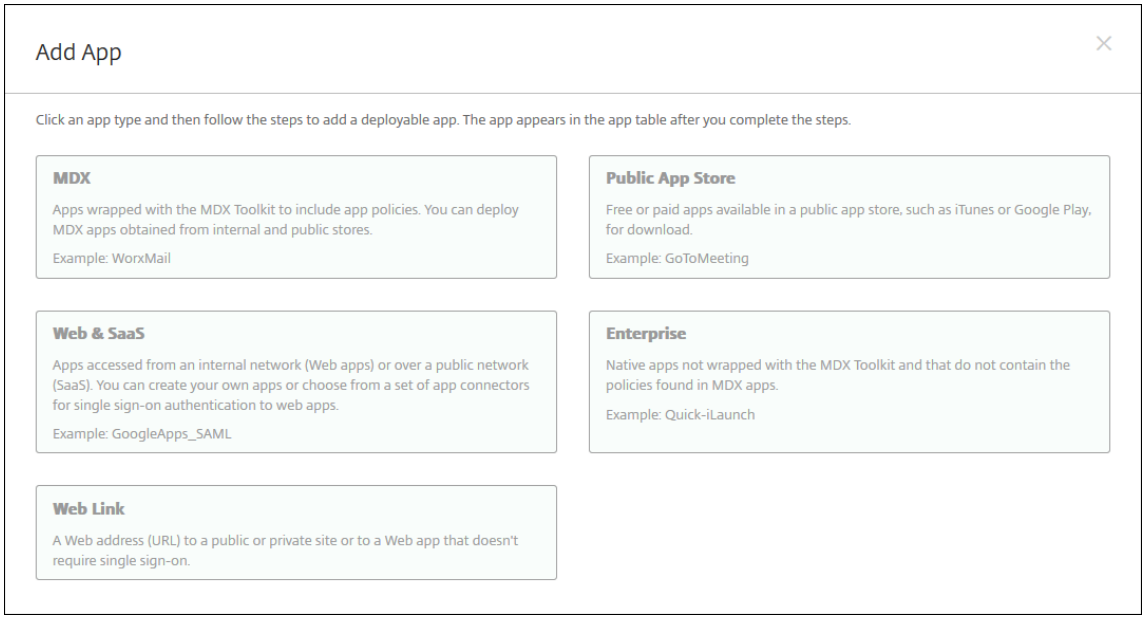
MDX 앱

MDX 정책과보안기능을사용하려면 MAM SDK 지원또는 MDX 래핑앱을추가하십시오. 볼륨구매를사용하거나볼륨구매없이도 MDX 앱을배포할수있습니다.

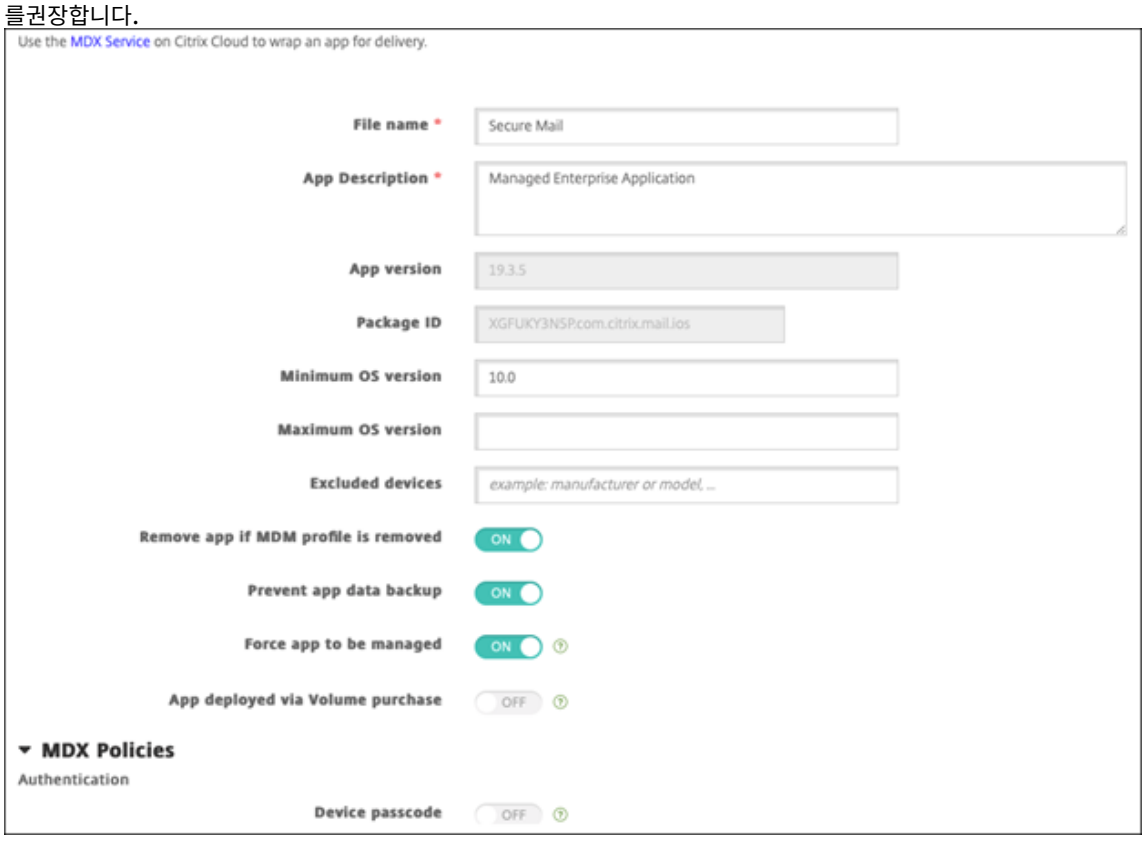
기능가용성	
장치감독필요	아니요
사용자등록모드제공	예
사용가능한플랫폼	iOS/iPadOS

1 단계**:** 앱추가및구성

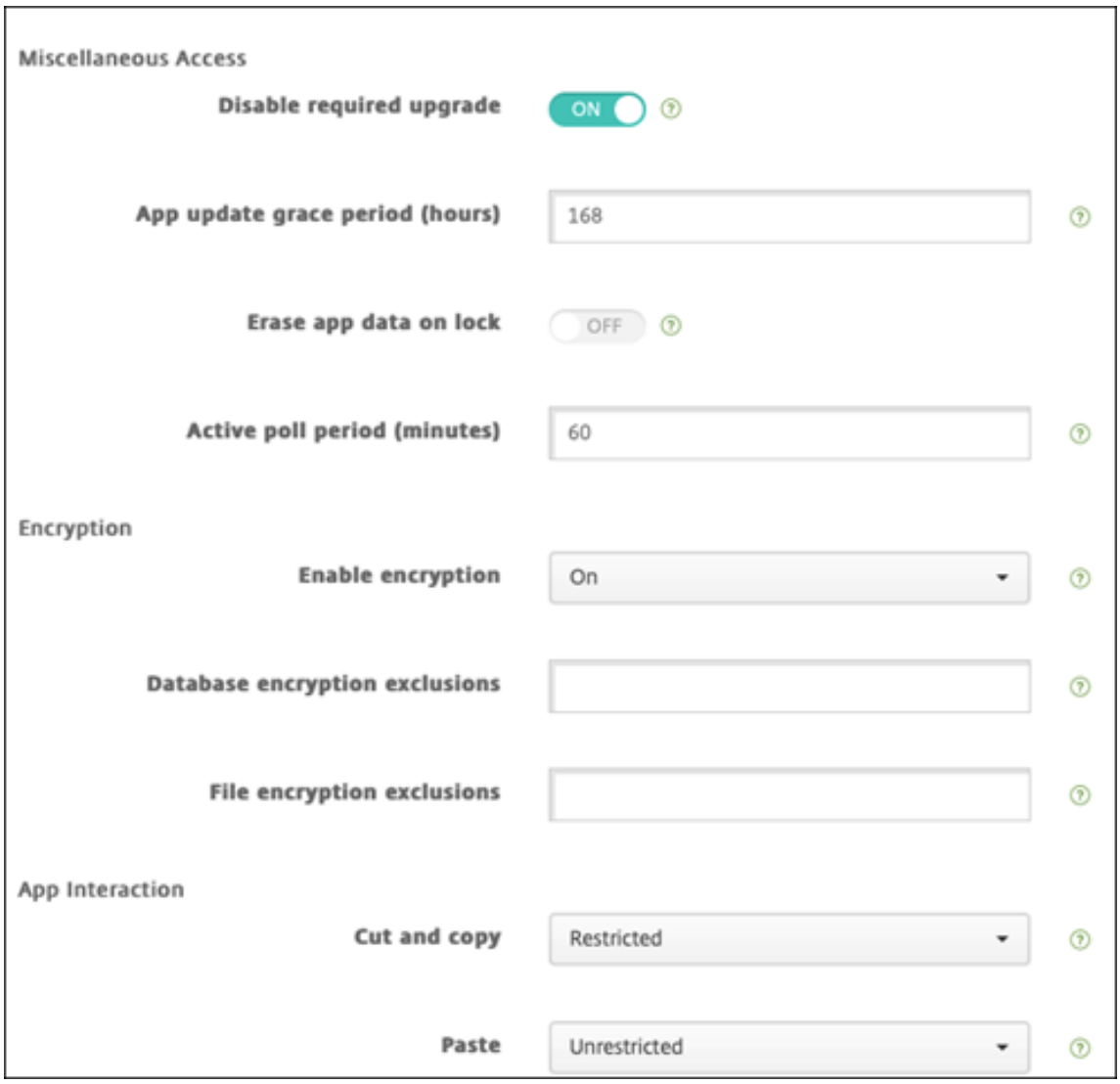
1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 추가를클릭합니다.
2. **MDX** 를클릭합니다.



3. 플랫폼에대해 **iPhone** 또는 **iPad** 를선택합니다.
4. MDX 파일을업로드합니다.
5. 앱세부정보를구성합니다. 볼륨구매를통해배포된앱을 꺼짐으로설정합니다. Citrix 에서는 강제로앱관리기능도사용하기를권장합니다.



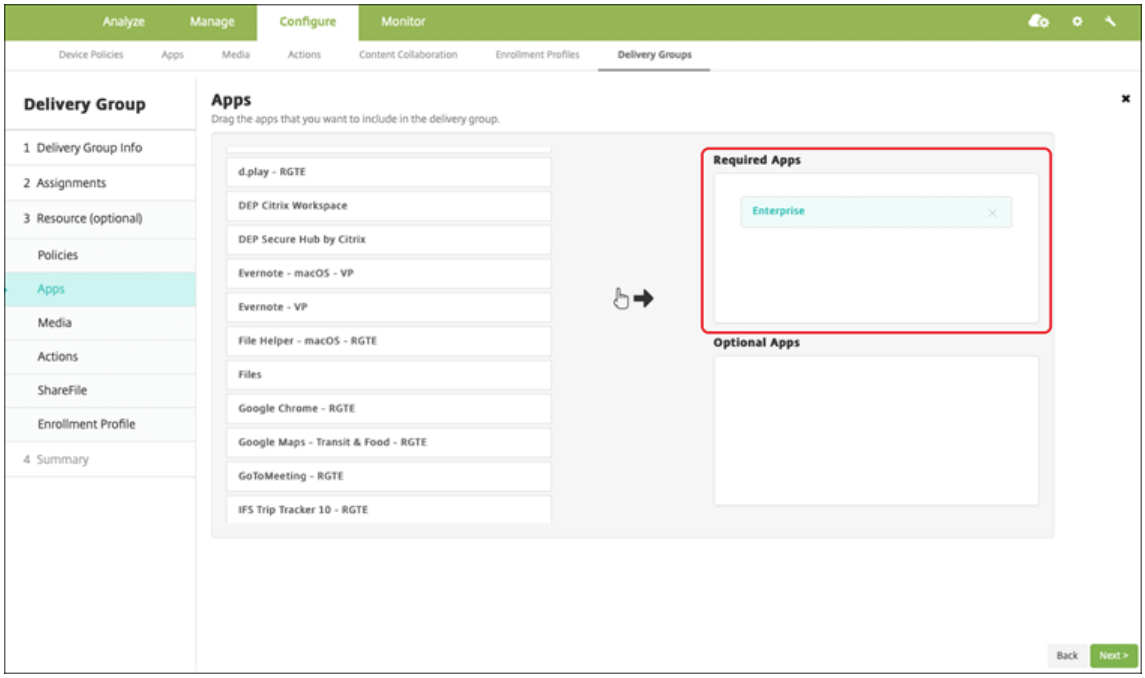
6. MDX 정책을구성합니다. 필수업그레이드사용안함을 켜짐으로설정합니다.



7. 배달그룹을앱에할당하고 저장을클릭합니다.

2 단계**:** 앱배포구성

1. XenMobile 콘솔에서 구성 **>** 배달그룹 **>** 앱으로이동합니다.
2. 원하는앱을 필수로표시합니다.



3. 구성 **>** 배달그룹으로이동합니다.
4. 배달그룹을선택하고 배포를클릭합니다.
5. 사용자는앱을설치하라는요청을받고수락후앱이백그라운드에서설치됩니다.

Apple 볼륨구매로배포된 MDX 앱

MDX 정책과보안기능을사용하려면 MAM SDK 지원또는 MDX 래핑앱을추가하십시오. 볼륨구매를사용하여앱을배포하려면앱이앱스토어에있어야합니다.

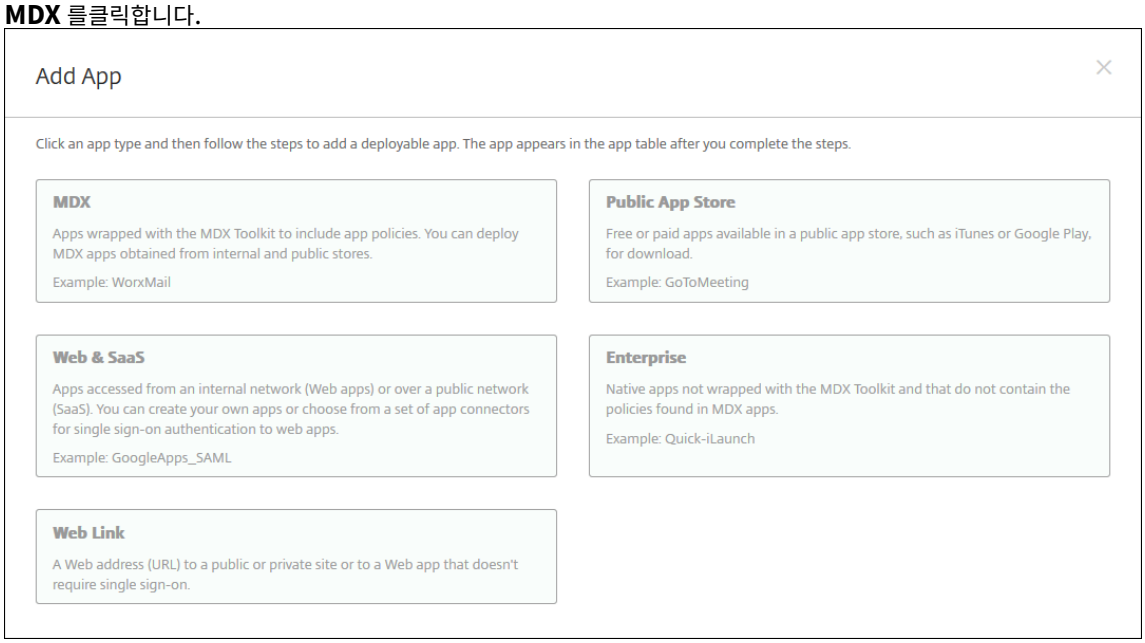
기능가용성	
장치감독필요	아니요
사용자등록모드제공	예
사용가능한플랫폼	iOS/iPadOS

1 단계**:** 계정연결

1. Apple Business Manager(ABM) 또는 Apple School Manager(ASM) 에서설정하고등록합니다. 이러한프로그램에대한자세한내용은 Apple 설명서를참조하십시오.
2. XenMobile 로 ABM/ASM 계정을연결합니다. 볼륨구매계정연결에대한자세한내용은 Apple 볼륨구매를참조하십시오.
3. 볼륨구매계정을추가할경우 앱자동업데이트를활성화합니다. 이설정을사용하면 Apple 앱스토어에업데이트가나타날경우사용자기기의앱이자동으로업데이트됩니다.

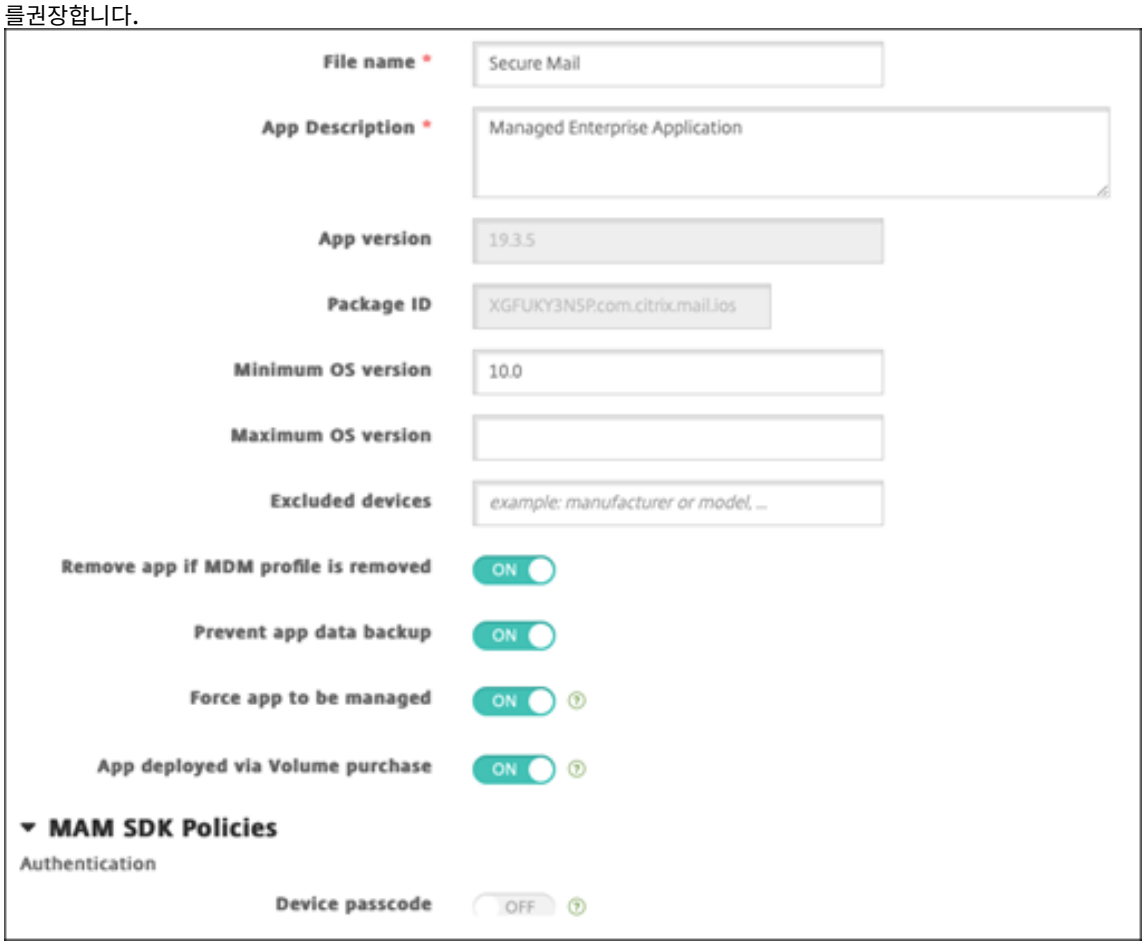
2 단계**:** 앱추가및구성

1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 추가를클릭합니다.
2. **MDX** 를클릭합니다.

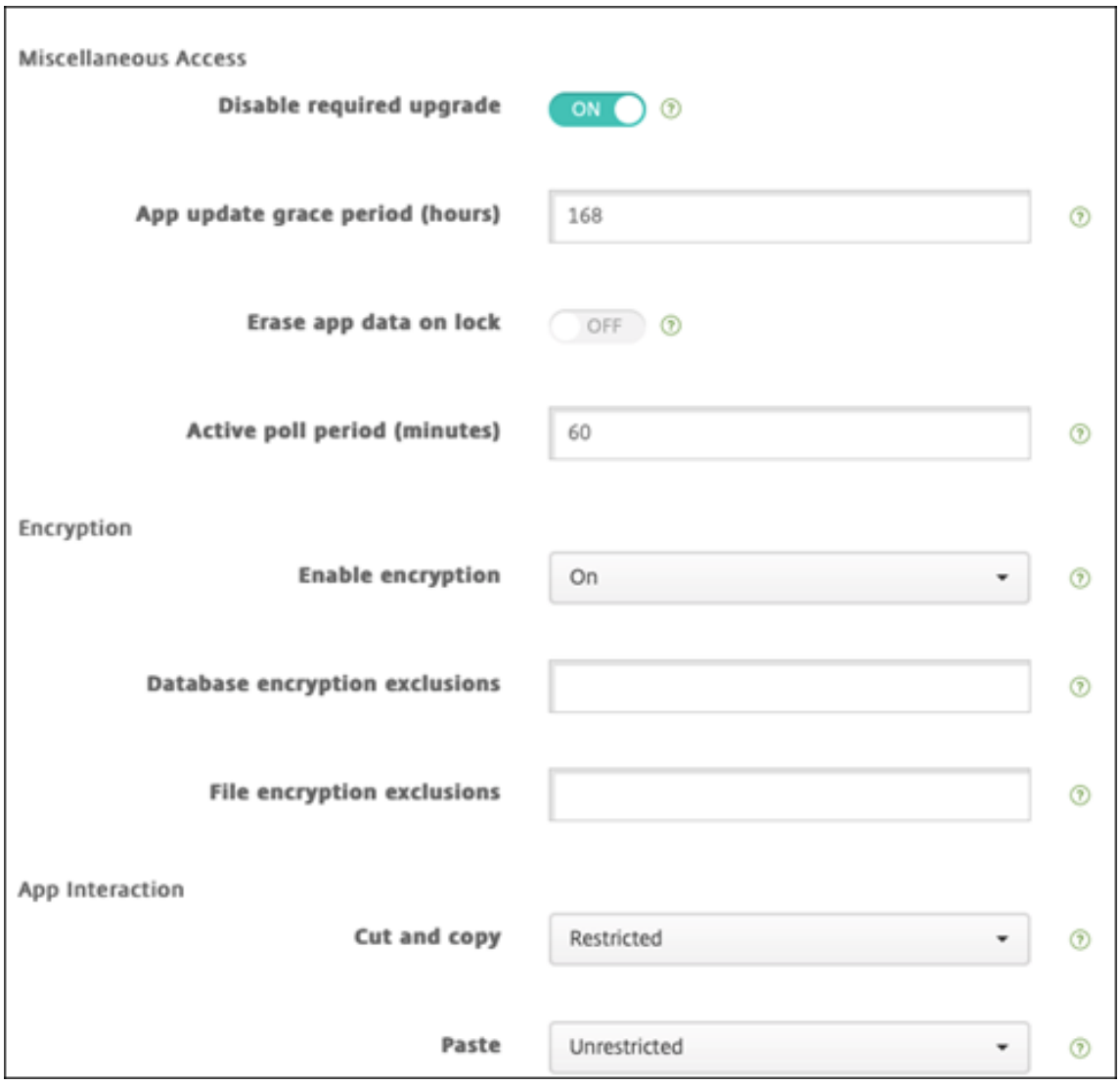


3. 플랫폼에대해 **iPhone** 또는 **iPad** 를선택합니다.

4. MDX 파일을업로드합니다.
5. 앱세부정보를구성합니다. 볼륨구매를통해배포된앱을 켜짐으로설정합니다. Citrix 에서는 강제로앱관리기능도사용하기를권장합니다.



6. MDX 정책을구성합니다. 필수업그레이드사용안함을 켜짐으로설정합니다.

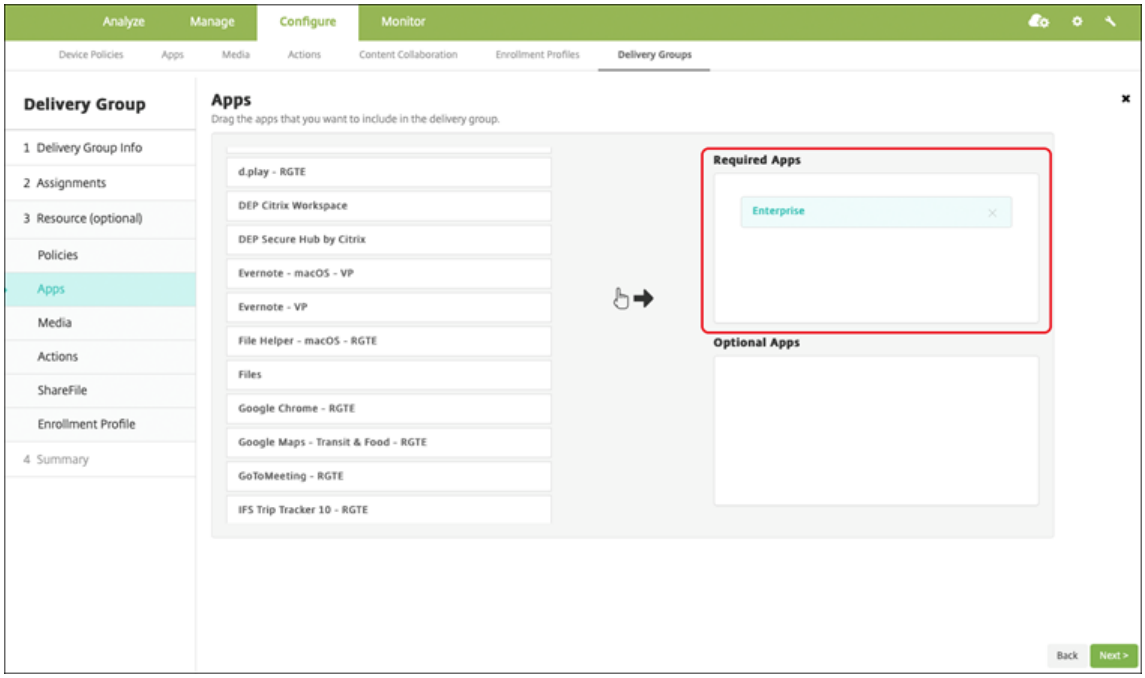


7. 각플랫폼마다배달그룹을앱에할당하고 저장을클릭합니다.

이구성으로인해이앱에대한항목 2 개가앱목록에나열됩니다. 구성할앱을선택할경우 유형이 **MDX** 인앱을선택합니다.

3 단계**:** 앱배포구성

1. XenMobile 콘솔에서 구성 **>** 배달그룹 **>** 앱으로이동합니다.
2. 원하는볼륨구매앱을 필수로표시합니다.



3. 구성 **>** 배달그룹으로이동합니다.
4. 배달그룹을선택하고 배포를클릭합니다.
5. 사용자는앱을설치하라는요청을받고수락후앱이백그라운드에서설치됩니다.

사용자지정앱

사용자지정앱은독점적 B2B 앱입니다. XenMobile 및 Apple 볼륨구매를사용하여비공개로안전하게독점앱을배포할수있습니다. 이러한앱은특정파트너, 클라이언트, 프랜차이즈, 내부직원에게배포할수있습니다.

기능가용성	
장치감독필요	아니요
사용자등록모드제공	예
사용가능한플랫폼	iOS/iPadOS

사용자지정앱에대한요구사항

- Apple Business Manager 또는 Apple School Manager 계정
- Apple 볼륨구매계정 (iOS 7 이상인장치필요)
- 다음 Apple 등록모드중하나를사용하여 XenMobile 에서장치를등록합니다.
  - 자동화된장치등록
  - 장치등록
  - 사용자등록

1 단계**:** 계정연결

볼륨구매를사용하여사용자지정앱을배포하려면볼륨구매계정을 XenMobile 에연결합니다.

1. Apple Business Manager(ABM) 에서설정하고등록합니다. 이러한프로그램에대한자세한내용은 Apple 설명서를 참조하십시오.
2. XenMobile 로 ABM 계정을연결합니다. 볼륨구매계정연결에대한자세한내용은 Apple 볼륨구매를참조하십시오.
3. 볼륨구매계정을추가할경우 앱자동업데이트를활성화합니다. 이설정을사용하면 Apple 앱스토어에업데이트가나타날경우사용자기기의앱이자동으로업데이트됩니다.

2 단계**: ABM** 에서앱구성

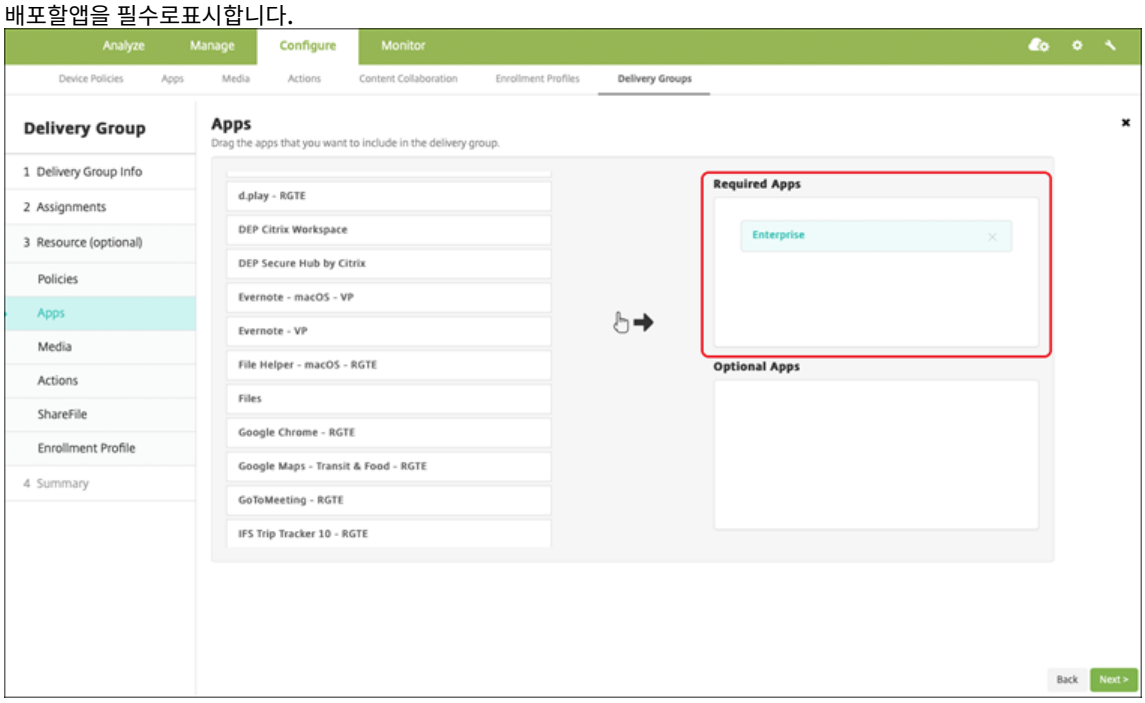
ABM 계정에서앱을추가합니다. 자체사용자지정앱을업로드하고배포하거나다른조직의사용자지정앱에대한라이센스를구매할수 있습니다. ABM 의사용자지정앱추가및사용에대한자세한정보는 Apple 설명서에서확인하십시오.

3 단계**: XenMobile** 에서앱추가및구성

1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 앱목록에볼륨구매앱이표시됩니다.
2. 구성할앱을선택합니다. 편집을클릭합니다.
3. **iPhone**, **iPad** 또는 **macOS** 중에서플랫폼을선택합니다.
4. 앱을배포할배달그룹을선택합니다. 저장을클릭합니다.

4 단계**:** 앱배포구성

1. XenMobile 콘솔에서 구성 **>** 배달그룹 **>** 앱으로이동합니다.
2. 배포할앱을 필수로표시합니다.



3. 구성 **>** 배달그룹으로다시돌아갑니다.
4. 배포할배달그룹을선택하고 배포를클릭합니다.
5. 사용자가앱배포요청을받습니다. 사용자가요청을수락하면앱이백그라운드에서설치됩니다.

MDX 지원사용자지정앱

MDX 정책과보안기능을사용하려면 MAM SDK 지원또는 MDX 래핑사용자지정앱을추가하십시오.

기능가용성	
장치감독필요	아니요
사용자등록모드제공	예
사용가능한플랫폼	iOS/iPadOS

1 단계**:** 계정연결

볼륨구매를사용하여사용자지정앱을배포하려면볼륨구매계정을 XenMobile 에연결합니다.

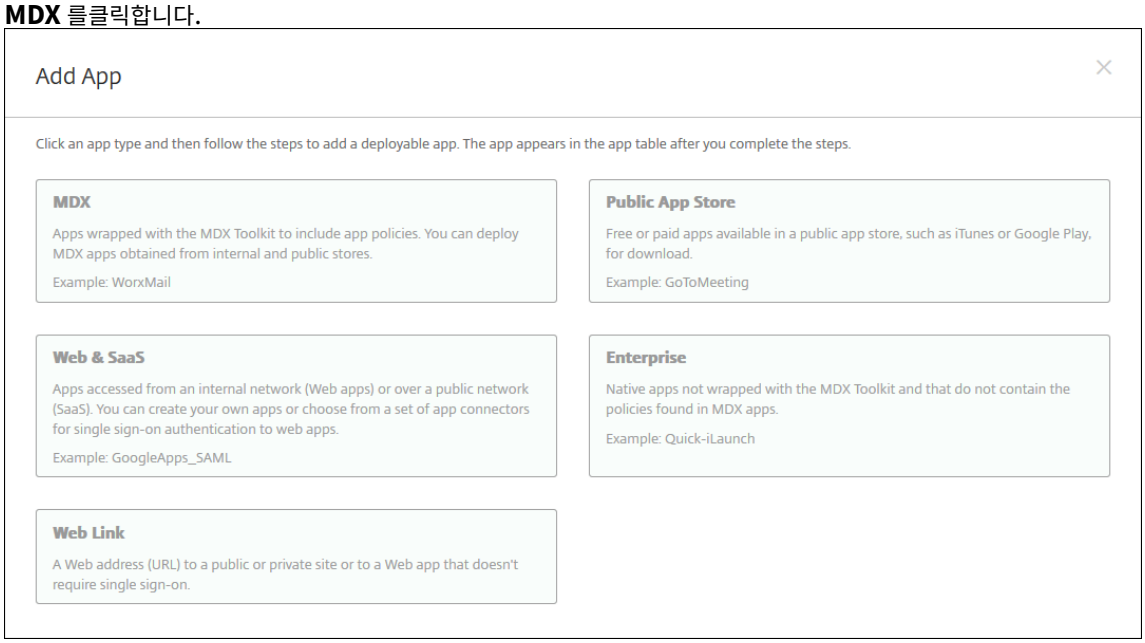
1. Apple Business Manager(ABM) 에서설정하고등록합니다. 이러한프로그램에대한자세한내용은 Apple 설명서를 참조하십시오.
2. XenMobile 로 ABM 계정을연결합니다. 볼륨구매계정연결에대한자세한내용은 Apple 볼륨구매를참조하십시오.
3. 볼륨구매계정을추가할경우 앱자동업데이트를활성화합니다. 이설정을사용하면 Apple 앱스토어에업데이트가나타날경우사용자기기의앱이자동으로업데이트됩니다.

2 단계**: ABM** 에서앱구성

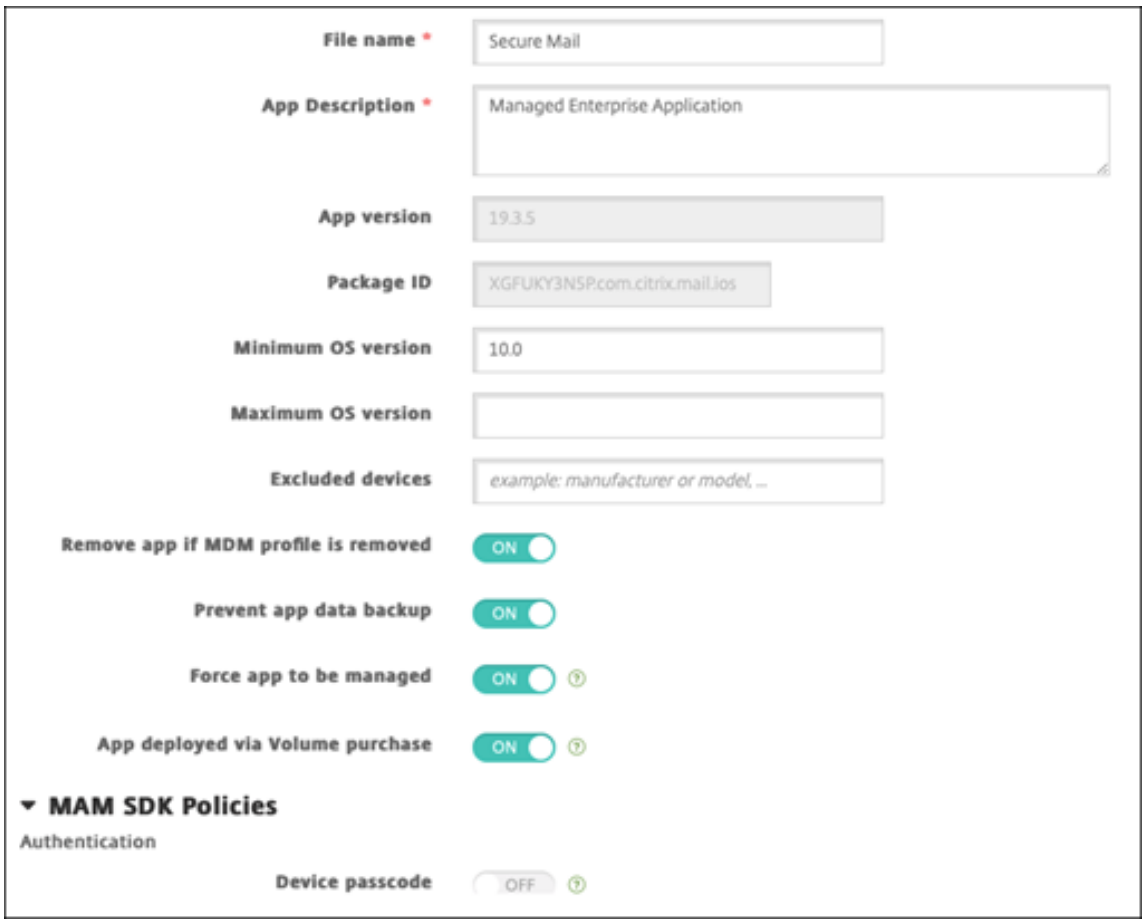
ABM 계정에서앱을추가합니다. 자체사용자지정앱을업로드하고배포하거나다른조직의사용자지정앱에대한라이센스를구매할수 있습니다. ABM 의사용자지정앱추가및사용에대한자세한정보는 Apple 설명서에서확인하십시오.

3 단계**: XenMobile** 에서앱추가및구성

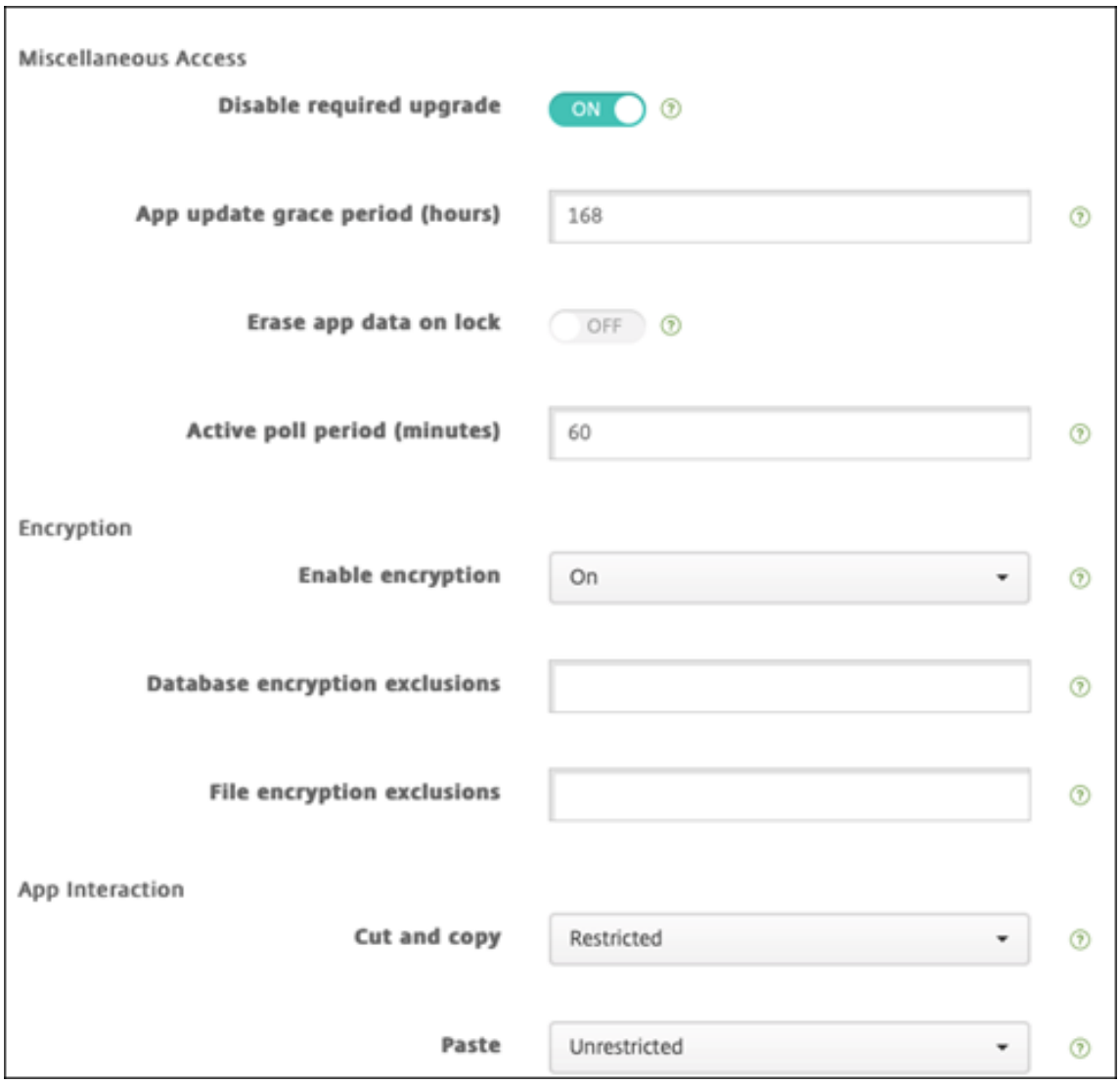
1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 추가를클릭합니다.
2. **MDX** 를클릭합니다.



3. **iPhone** 또는 **iPad** 플랫폼을선택합니다.
4. 추가할앱의 MDX 파일을업로드합니다.
5. 앱세부정보를구성합니다. 볼륨구매를통해배포된앱을 켜짐으로설정합니다. Citrix 에서는 강제로앱관리기능도사용하기를권장합니다.



6. MDX 정책을구성합니다. 필수업그레이드사용안함을 켜짐으로설정합니다.

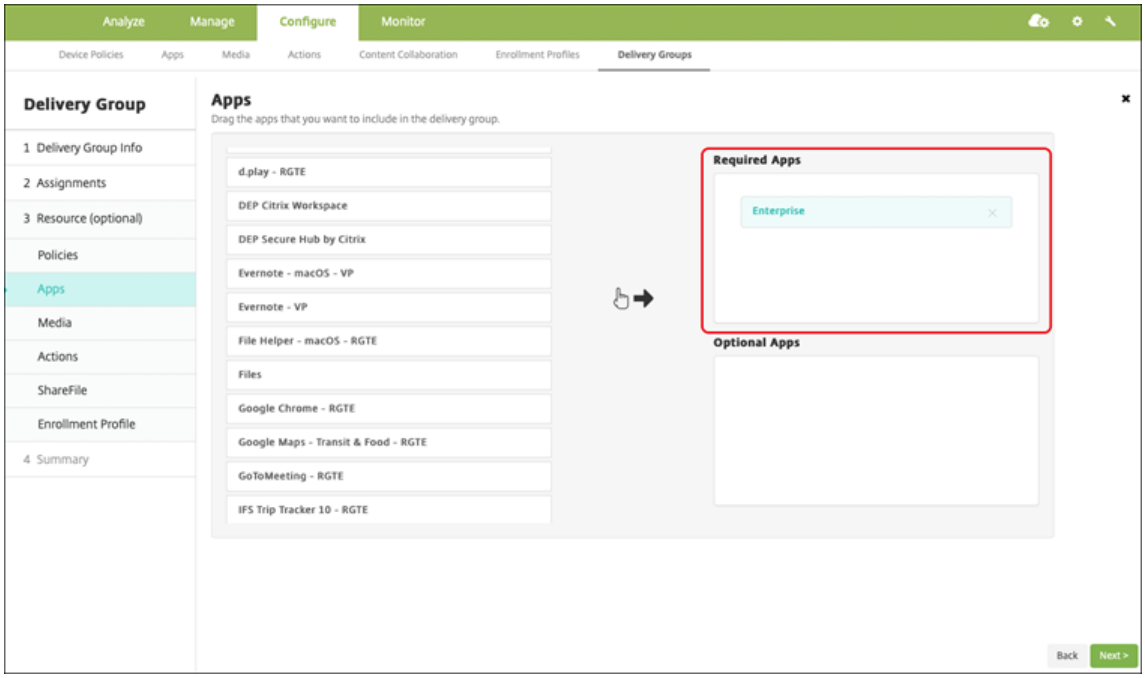


7. 배달그룹을앱에할당하고 저장을클릭합니다.

이구성으로인해이앱에대한항목 2 개가앱목록에나열됩니다. 구성할앱을선택할경우 유형이 **MDX** 인앱을선택합니다.

4 단계**:** 앱배포구성

1. XenMobile 콘솔에서 구성 **>** 앱으로이동합니다. 앱목록에볼륨구매앱이표시됩니다.
2. 구성할앱을선택합니다. 편집을클릭합니다.
3. 각플랫폼에앱을배포할배달그룹을선택합니다. 저장을클릭합니다.
4. 구성 **>** 배달그룹 **>** 앱으로다시돌아갑니다.
5. 배포할앱을 필수로표시합니다.



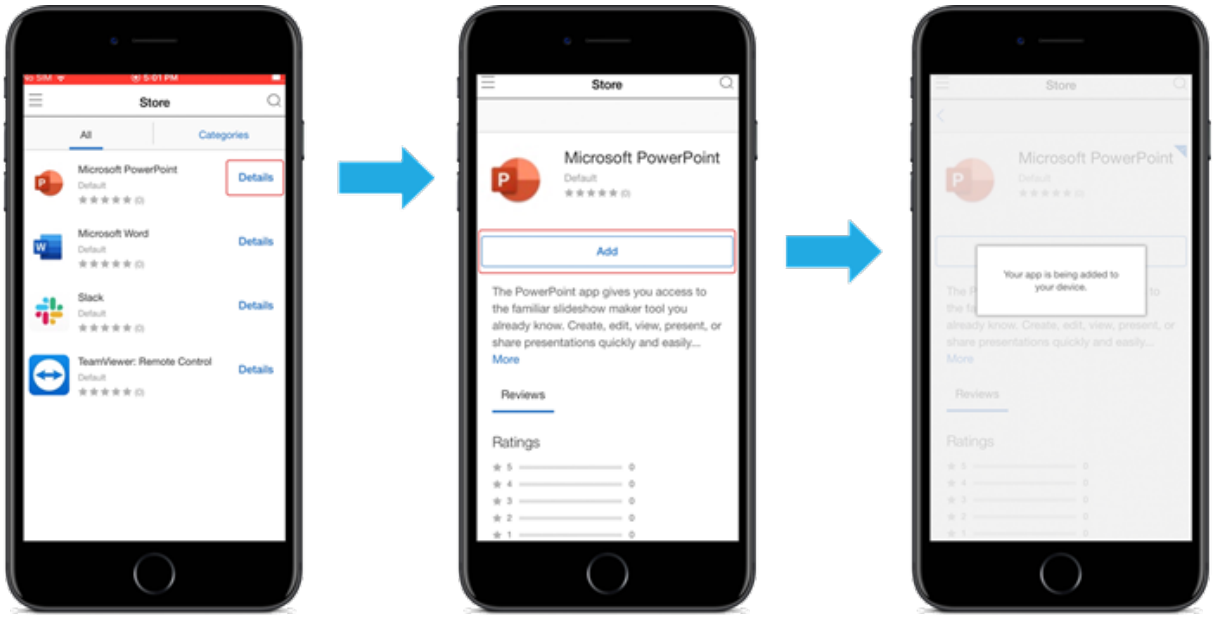
6. 구성 **>** 배달그룹으로다시돌아갑니다.
7. 배포할배달그룹을선택하고 배포를클릭합니다.
8. 사용자가앱배포요청을받습니다. 수락하면앱이백그라운드에서설치됩니다.

옵션앱 **(iOS/iPadOS** 전용**)**

Citrix 에서는앱을 필수로배포하기를권장합니다. 필수앱은사용자장치에자동으로설치되므로상호작용이최소화됩니다. 이러한기능을사용하면앱을자동으로업데이트할수도있습니다.

옵션앱을통해사용자는설치할앱을선택할수있지만사용자는 Secure Hub 를통해수동으로설치를개시해야합니다.

옵션앱을설치하려면 Secure Hub 를실행하고 스토어로이동한다음원하는앱의 세부정보를선택하고 추가를클릭합니다.



네트워크액세스제어

May 6, 2022

NAC(네트워크액세스제어) 솔루션을사용하여 Android 및 Apple 장치에대한 Endpoint Management 장치보안평가를확장할수있습니다. NAC 솔루션에서 XenMobile 보안평가를사용하여인증의사결정을지원하고처리할수있습니다. NAC 장비를구성한후 XenMobile 에서구성한장치정책및 NAC 필터가적용됩니다.

NAC 솔루션과함께 XenMobile 을사용하면 QoS 를추가하고네트워크내부에있는장치를보다세밀하게제어할수있습니다. NAC 를 XenMobile 과통합하여얻을수있는장점에대한요약은 액세스제어에서확인하십시오.

다음은 XenMobile 통합이지원되는솔루션입니다.

- Citrix Gateway
- Cisco Identity Services Engine(ISE)
- ForeScout

다른 NAC 솔루션에대한통합은보장되지않습니다.

네트워크의 NAC 장비사용:

- XenMobile 은 iOS, Android Enterprise 및 Android 장치의엔드포인트보안기능으로 NAC 를지원합니다.
- XenMobile 에서필터를사용하여규칙또는속성에따라장치를 NAC 준수또는비준수장치로설정할수있습니다. 예:
  - XenMobile 의관리되는장치가지정된기준을충족하지않으면 XenMobile 이해당장치를비준수장치로표시합니다. 네트워크에서규정을준수하지않는장치는 NAC 장비에의해차단됩니다.
  - XenMobile 의관리되는장치에비준수앱이설치되어있는경우 NAC 필터에의해 VPN 연결이차단될수있습니다. 따라서비준수사용자장치는 VPN 을통해앱이나웹사이트에액세스할수없습니다.
  - Citrix Gateway 를 NAC 에사용하는경우분할터널링을사용하도록설정하여 Citrix Gateway 플러그인에서불필요한네트워크트래픽을 Citrix Gateway 로보내는것을방지할수있습니다. 분할터널링에대한자세한내용은 분할터널링구성을참조하십시오.

지원되는 **NAC** 준수필터

XenMobile Server 는다음과같은 NAC 준수필터를지원합니다.

익명장치**:** 장치가익명모드인지확인합니다. 이확인은장치가다시연결할때 XenMobile 이사용자를다시인증할수없는경우사용할수있습니다.

Samsung Knox 증명실패**:** 장치가 Samsung Knox 증명서버의쿼리에실패했는지확인합니다.

금지된앱**:** 장치에앱액세스장치정책에정의된금지된앱이있는지확인합니다. 해당정책에대한자세한내용은 앱액세스장치정책을참조하십시오.

비활성장치**:** 서버속성의 장치비활성일수임계값설정에정의된대로장치가비활성상태인지확인합니다. 자세한내용은 서버속성을참조하십시오.

누락된필수앱**:** 앱액세스정책에정의된대로, 장치에필수앱이누락되었는지확인합니다.

비추천앱**:** 앱액세스정책에정의된대로, 장치에비추천앱이있는지확인합니다.

규정을준수하지않는암호**:** 사용자암호가규정을준수하는지확인합니다. iOS 및 Android 장치에서 XenMobile 은현재장치에있는암호가장치로보낸암호정책을준수하는지여부를확인할수있습니다. 예를들어 iOS 에서는 XenMobile 이암호정책을장치에보내는경우 60 분내에암호를설정해야합니다. 사용자가암호를설정하기전에암호가규정을준수하지않을수있습니다.

규정위반장치**:** 규정위반장치속성에따라장치가규정을위반하는지여부를확인합니다. 일반적으로 XenMobile API 를사용하는자동화된작업또는타사에서는이장치속성을변경합니다.

해지된상태**:** 장치인증서가해지되었는지여부를확인합니다. 해지된장치는다시권한이부여될때까지다시등록할수없습니다.

루팅된 **Android** 및탈옥 **iOS** 장치**:** Android 또는 iOS 장치가탈옥되어있는지확인합니다.

관리되지않는장치**:** 장치가여전히 XenMobile 제어하에관리되는상태에있는지확인합니다. 예를들어 MAM 로등록된장치나등록되지않은장치는관리되지않습니다.

> 참고**:**

> 묵시적준수/비준수필터는 XenMobile 로관리되는장치에만기본값을설정합니다. 예를들어차단된앱이설치된장치또는등록되지않은장치는비준수로표시됩니다. 이러한장치는 NAC 장비에의해네트워크에서차단됩니다.

구성개요

NAC 구성요소를나열된순서대로구성하는것이좋습니다.

1. NAC 를지원하도록장치정책구성:

   iOS 장치의경우**:**NAC 를지원하도록 VPN 장치정책구성을참조하십시오.

   Android Enterprise 장치의경우**:**Citrix SSO 에대한 Android Enterprise 관리되는구성만들기를참조하십시오.

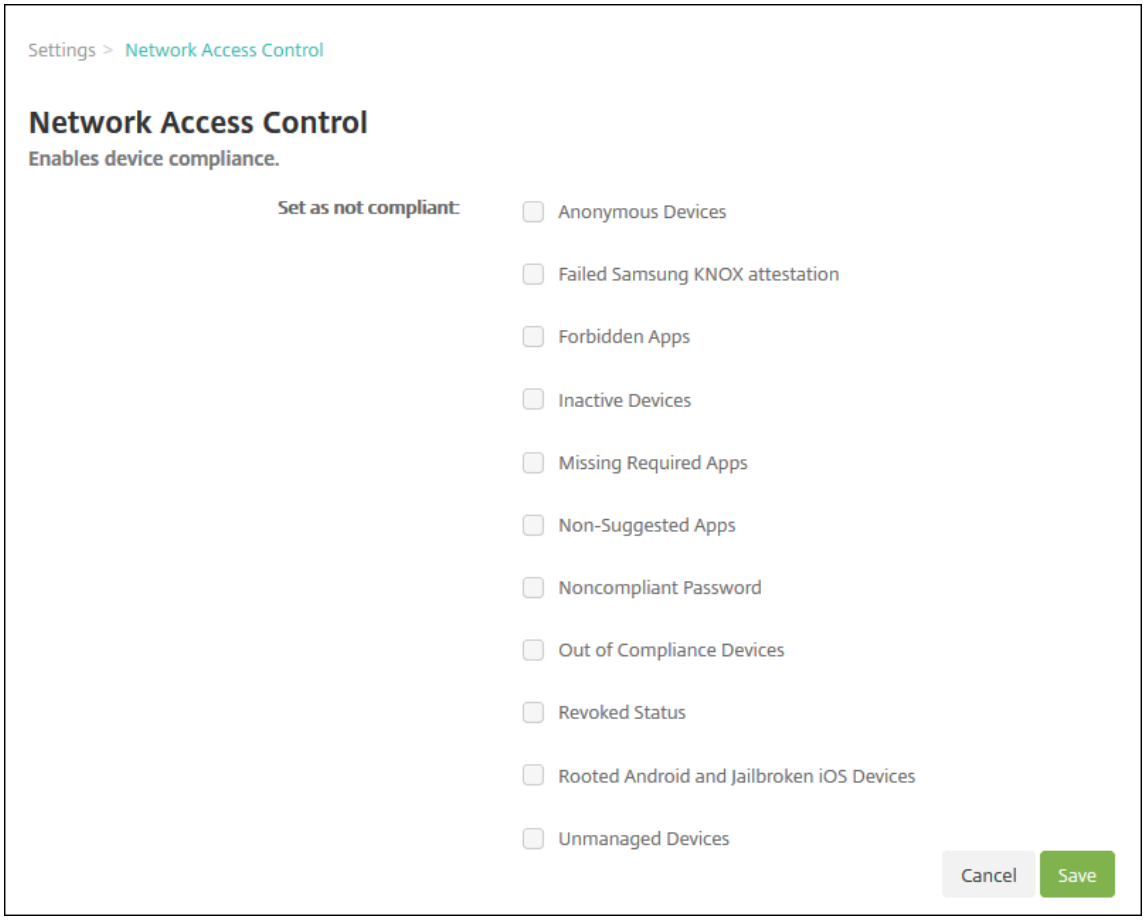
   Android 장치의경우**:**Android 용 Citrix SSO 프로토콜구성을참조하십시오.

2. XenMobile 에서 NAC 필터사용.
3. NAC 솔루션구성:
   - Citrix Gateway, NAC 를지원하도록 Citrix Gateway 정책업데이트에자세히설명되어있습니다.

     장치에 Citrix SSO 를설치해야합니다. Citrix Gateway 클라이언트를참조하십시오.
   - Cisco ISE: Cisco 설명서를참조하십시오.
   - ForeScout: ForeScout 설명서를참조하십시오.

XenMobile 에서 **NAC** 필터사용

1. XenMobile 콘솔에서 설정 **>** 네트워크액세스제어로이동합니다.



2. 사용하려는 규정비준수상태로설정필터에대한확인란을선택합니다.
3. 저장을클릭합니다.

NAC 를지원하도록 Citrix Gateway 정책업데이트

VPN 가상서버에서고급 (클래식아님) 인증및 VPN 세션정책을구성해야합니다.

아래의단계는다음과같은특성의 Citrix Gateway 를업데이트합니다.

- XenMobile Server 환경과통합됩니다.
- 또는 XenMobile Server 환경의일부가아닌 VPN 용으로설정되었고 XenMobile 에연결할수있습니다.

가상 VPN 서버의콘솔창에서다음을수행합니다. 명령및예제의 IP 주소는가상의주소입니다.

1. VPN 가상서버에서클래식정책을사용하는경우모든클래식정책을제거하고바인딩해제합니다. 확인하려면다음을입력합니다.

   ```
   show vpn vserver <VPN_VServer>
   ```

   클래식이라는단어가포함된모든결과를제거합니다. 예: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

정책을제거하려면다음을입력합니다.

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. 다음을입력하여해당하는고급세션정책을만듭니다.

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   예: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. 다음을입력하여정책을 VPN 가상서버에바인딩합니다.

   ```
   bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
   ```

4. 다음을입력하여인증가상서버를만듭니다.

   ```
   add authentication vserver <authentication vserver name> <service type>
    <ip address>
   ```

   예: `add authentication vserver authvs SSL 0.0.0.0`
   예제에서 `0.0.0.0`은인증가상서버가공개되지않음을의미합니다.

5. 다음을입력하여 SSL 인증서를가상서버에바인딩합니다.

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver
   certificate>
   ```

   예: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. VPN 가상서버의인증가상서버에인증프로필을연결합니다. 먼저다음을입력하여인증프로필을만듭니다.

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication
    vserver name>
   ```

   예:

   ```
   add authentication authnProfile xm_nac_prof -authnVsName authvs
   ```

7. 다음을입력하여인증프로필을 VPN 가상서버에연결합니다.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   예:

   ```
   set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. 다음을입력하여 Citrix Gateway 에서장치로의연결을확인합니다.

   ```
   curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --
   header ”X-Citrix-VPN-Device-ID: deviceid_<device_id>”
   ```

   예를들어다음쿼리는환경에등록된첫번째장치 (`deviceid_1`) 의규정준수상태를확인하여연결을확인합니다.

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header ”X-
   Citrix-VPN-Device-ID: deviceid_1”
   ```


성공적인결과는다음예제와유사합니다.

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. 이전단계가성공하면 XenMobile 에대한웹인증작업을만듭니다. 먼저 iOS VPN 플러그인에서장치 ID 를추출하는정책식을만듭니다. 다음을입력합니다.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
   TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. 다음을입력하여요청을 XenMobile 에보냅니다. 이예에서 XenMobile Server IP 는 `10.207.87.82`, FQDN 은 `example.em.server.com:4443`입니다.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
     4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "
    Host: example.em.server.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+
    xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.
    RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ
    (\"Compliant\")"
    ```

    XenMobile NAC 의성공적인출력은 `HTTP status 200 OK`입니다. `X-Citrix-Device-State` 헤더의값은 `Compliant`여야합니다.

11. 다음을입력하여작업을연결할인증정책을만듭니다.

    ```
    add authentication Policy <policy name> -rule <rule> -action <web
    authentication action>
    ```

    예: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER (\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. 다음을입력하여기존 LDAP 정책을고급정책으로변환합니다.

    ```
    add authentication Policy <policy_name> -rule <rule> -action <LDAP
    action name>
    ```

    예: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 다음을입력하여 LDAP 정책을연결할정책레이블을추가합니다.

    ```
    add authentication policylabel <policy_label_name>
    ```

    예: `add authentication policylabel ldap_pol_label`

14. 다음을입력하여 LDAP 정책을정책레이블에연결합니다.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol
 -priority 100 -gotoPriorityExpression NEXT
```

15. 준수장치를연결하여 NAC 테스트를수행하고 LDAP 인증에성공하는지확인합니다. 다음을입력합니다.

```
bind authentication vserver <authentication vserver> -policy <web
authentication policy> -priority 100 -nextFactor <ldap policy label> -
gotoPriorityExpression END
```

16. 인증가상서버에연결할 UI 를추가합니다. 다음명령을입력하여장치 ID 를검색합니다.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -
action lschema_single_factor_deviceid
```

17. 다음을입력하여인증가상서버를바인딩합니다.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority
 100 -gotoPriorityExpression END
```

18. LDAP 고급인증정책을만들어 Secure Hub 연결을사용하도록설정합니다. 다음을입력합니다.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP

bind authentication vserver authvs -policy ldap_xm_test_pol -priority
110 -gotoPriorityExpression NEXT
```

Samsung Knox

July 18, 2022

Samsung 은 XenMobile Server 와호환되는여러솔루션을제공합니다.

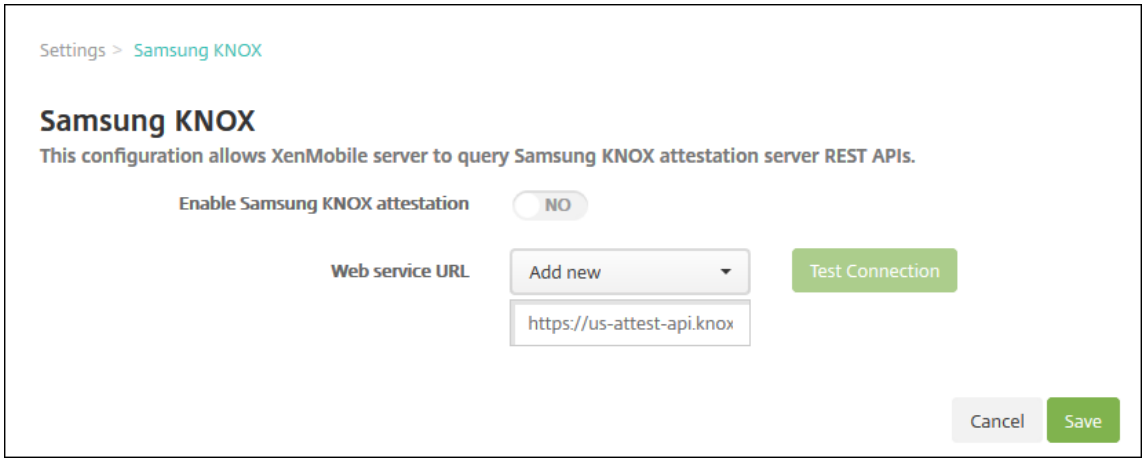
- XenMobile 은호환되는 Samsung 장치에서 Samsung Knox 정책을지원하고확장합니다.
- Knox Service 플로그인 (KSP) 은 Knox Platform for Enterprise (KPE) 기능의하위집합을지원하는앱입니다. KPE 에대한 Samsung 의정보는 엔터프라이즈용 Knox 플랫폼구성 및 개요를참조하십시오.

XenMobile 에서 Samsung Knox 증명서버 REST API 를쿼리하도록구성할수있습니다.

Samsung Knox 는하드웨어보안기능을사용하여운영체제및응용프로그램에대한여러수준의보호를제공합니다. 이중한수준의보안기능이증명을통해플랫폼에서제공됩니다. 증명서버는모바일장치핵심시스템소프트웨어 (예: 부팅로더및커널) 에대한확인을수행합니다. 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. 그런다음목록에서다음중하나를수행합니다.
   - 적절한증명서버를클릭합니다.
   - 새로추가를클릭하고웹서비스 URL 을입력합니다.
5. 연결테스트를클릭하여연결을확인합니다. 성공또는실패메시지가나타납니다.
6. 저장을클릭합니다.

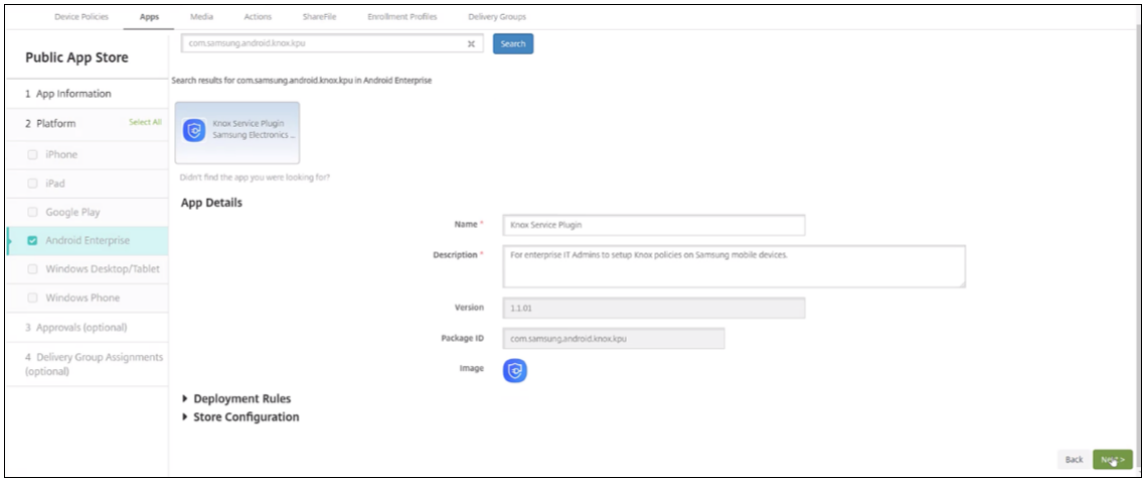
> 참고:
>
> Samsung Knox Mobile Enrollment 를사용하여여러 Samsung Knox 장치를각장치에대한수동구성없이 XenMobile 또는원하는모바일장치관리자에등록할수있습니다. 자세한내용은 Samsung KNOX 대량등록을참조하십시오.

Knox 서비스플러그인앱추가

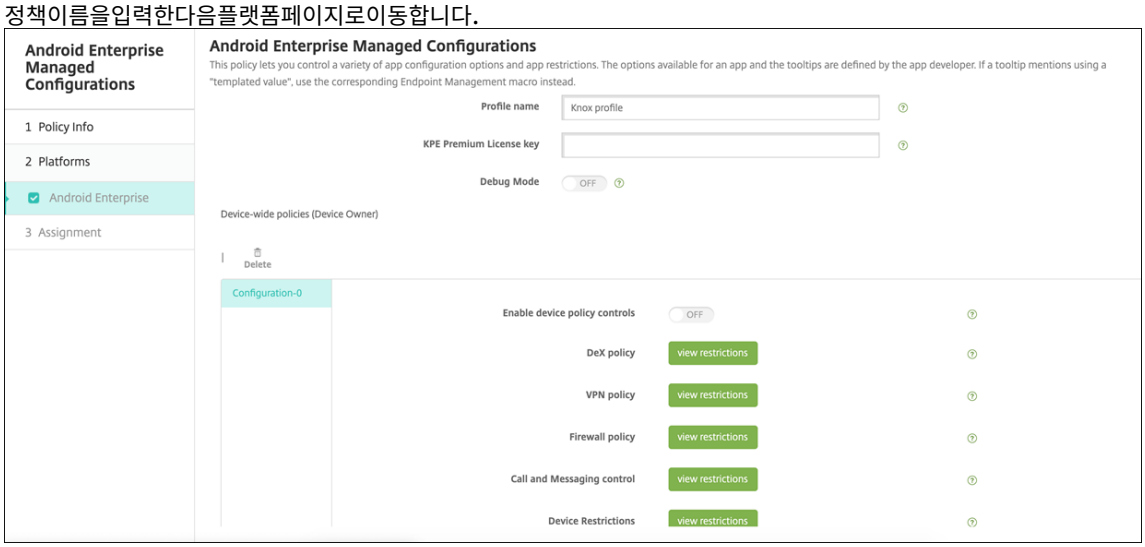
Knox 와함께 Android Enterprise 를사용하려는경우 KSP(Knox 서비스플러그인) 를 XenMobile 에추가합니다. KSP 앱은 AndroidOEMConfig 를사용하여보안정책, 유연한 VPN 구성및생체인증제어와같은기능을지원합니다. AndroidOEMConfig 를사용하면 OEM 및 EMM(엔드포인트모빌리티관리자) 에서맞춤형 OEM API 를지원할수있습니다. 이러한 API 는 Android Enterprise 를통해지원되지않는사용사례에적용됩니다.

KSP 에대한자세한내용은 Knox 서비스플러그인가이드를참조하십시오.

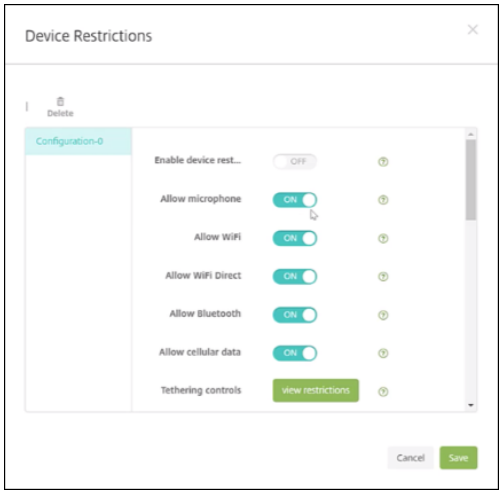
1. Google 계정에로그인하고 `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`로이동합니다. Knox 서비스플러그인앱을승인합니다.
2. XenMobile 콘솔에로그인하고 Knox 서비스플러그인을공용앱스토어앱으로추가합니다. 공용앱스토어앱추가에대한자세한내용은 공용앱스토어앱추가에서확인하십시오.



3. XenMobile 콘솔에서 구성 **>** 장치정책으로이동합니다. 추가를클릭합니다.
4. 관리되는구성을클릭합니다. 대화상자가나타나면메뉴에서 **Knox** 서비스플러그인을선택합니다. 관리되는구성정책에대한자세한내용은 관리되는구성정책을참조하십시오.
5. 정책이름을입력한다음플랫폼페이지로이동합니다.



6. 플랫폼페이지에서 Knox 프로필의 프로필이름을입력하고 Samsung 의 **KPE Premium** 라이센스키를입력합니다. 이러한필드아래에표시되는정책은 Knox 배포에서가져온것입니다. Knox 정책에대한자세한내용은이섹션의앞부분에참조된 Knox Service Admin Plug-in Guide(Knox 서비스관리플러그인가이드) 를참조하십시오.



7. 다음을클릭하고정책에대한배포규칙을구성합니다.
8. 저장을클릭합니다.

Samsung Knox 대량등록

January 5, 2022

여러 Samsung Knox 장치를각장치에대한수동구성없이 XenMobile 또는 Mobile Device Manager 에등록하려면 Knox Mobile Enrollment 를사용합니다. 이등록은최초사용시에또는공장기본값으로재설정이후에발생합니다. 또한관리자가장치에직접사용자이름과암호를전달할수있으므로사용자가등록시정보를입력할필요가없습니다.

> 참고:
>
> Knox Mobile Enrollment 설정은 XenMobile Knox 컨테이너와관련없습니다. Knox Mobile Enrollment 에대한자세한내용은 Knox Mobile Enrollment 관리가이드를참조하십시오.

Knox Mobile Enrollment 사전요구사항

- XenMobile 이구성되고 (라이센스및인증서포함) 실행중이어야합니다.
- Secure Hub APK 파일. Knox Mobile Enrollment 를설정할때이파일을업로드합니다.
- KME 요구사항목록은 Knox Mobile Enrollment 소개를참조하십시오.
- Samsung Knox Platform for Enterprise(PKE) 라이센스는장치정책을적용하는데필요합니다. XenMobile 장치정책인 Knox Platform for Enterprise 에서라이센스키를제공합니다.

Secure Hub APK 파일을다운로드하려면

Google Play 스토어로이동하여 Android 용 Citrix Secure Hub 파일을다운로드합니다.

방화벽예외구성

KNOX Mobile Enrollment 에액세스하려면다음방화벽예외를구성합니다. 이러한방화벽예외중일부는모든장치에필요하고 일부는장치의특정지리적지역에만필요합니다.

장치지역	URL	포트	대상
모두	https://gslb.secb2b.com	443	KNOX Mobile Enrollment 초기화를위한글로벌부하분산장치
모두	https://gslb.secb2b.com	80	일부제한된레거시장치에서 KNOX Mobile Enrollment 초기화를위한글로벌부하분산장치
모두	umc-cdn.secb2b.com	443	Samsung 에이전트업데이트서버
모두	bulkenrollment.s3.amazonaws.com	80	KNOX Mobile Enrollment 고객 EULA
모두	eula.secb2b.com	443	KNOX Mobile Enrollment 고객 EULA
모두	us-be-api-mssl.samsungknox.com	443	IMEI 확인을위한 Samsung 서버
미국	https://us-segd-api.secb2b.com	443	미국지역용 Samsung 엔터프라이즈게이트웨이
유럽	https://eu-segd-api.secb2b.com	443	유럽지역용 Samsung 엔터프라이즈게이트웨이
중국	https://china-segd-api.secb2b.com	443	중국지역용 Samsung 엔터프라이즈게이트웨이

> 참고:
>
> Knox Mobile Enrollment 관리가이드에서방화벽예외의전체목록을확인할수있습니다.

Knox Mobile Enrollment 액세스권한얻기

Knox Mobile Enrollment 액세스권한을얻으려면 KME 로시작에서 Samsung 설명서를따르십시오.

Knox Mobile Enrollment 설정

Knox Mobile Enrollment 액세스권한을얻은후 Knox 포털에로그인합니다.

등록프로세스는일반적인단계를따릅니다.

1. MDM 콘솔정보및설정으로 MDM 프로필을생성합니다.

   MDM 프로필은 MDM 에연결하는방법을장치에알려줍니다.

2. 장치를 MDM 프로필에추가합니다.

   장치정보를포함하는 CSV 파일을업로드하거나 Google Play 에서 Knox 배포앱을설치해서사용할수있습니다.

3. 장치소유권이확인되면 Samsung 에서알려줍니다.

4. 사용자에게 MDM 자격증명을제공합니다. Wi-Fi 를사용하여인터넷에연결하고메시지에따라장치를등록할것을사용자에게지시합니다.

MDM 프로필을생성하려면

Samsung 설명서에설명된프로필구성에대한단계를따릅니다.

다음필드또는단계가나타나면설명에따라다음과같이구성하십시오.

- **MDM** 선택**:** 메뉴에서 **Citrix** 를선택합니다. 장치소유자프로필에만해당합니다.
- **MDM** 에이전트 **APK:** 장치소유자프로필에만해당합니다. Secure Hub APK 다운로드 URL(`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`) 을입력합니다.

  APK 파일은등록중에장치가액세스할수있는서버에있을수있습니다. 등록중장치에서는다음작업을수행합니다.

  - APK 다운로드 URL 에서 Secure Hub 를다운로드합니다.
  - Secure Hub 를설치합니다.
  - 다음에설명된사용자지정 JSON 데이터로 Secure Hub 를엽니다.

  .apk 파일이름의대문자표시는입력한 URL 과일치해야합니다. 예를들어파일이름이모두소문자이면 URL 에서도모두소문자여야합니다.

- **MDM** 서버 **URI:** MDM 서버 URI 를지정하지마십시오. XenMobile 은 Samsung MDM 프로토콜을사용하지않습니다.
- 사용자지정 **JSON** 데이터**:** Secure Hub 에서등록하려면 XenMobile 서버주소, 사용자이름및암호가있어야합니다. Secure Hub 에서사용자에게메시지를표시하지않도록 JSON 에서해당데이터를제공할수있습니다. Secure Hub 는 JSON 에서이러한필드가누락된경우에만사용자에게서버주소, 사용자또는암호를요청하는메시지를표시합니다.

  사용자지정 JSON 데이터의형식은입니다.

  ```
  { "serverURL": "URL", "xm_username":"Username", "xm_password":"Password"}
  ```


일괄등록에일반적인이예에서 Secure Hub 는등록하는중에사용자에게서버주소또는자격증명을요청하는메시지를표시하지않습니다.

```
{ "serverURL":"https://example.com/zdm", "xm_username":"userN", "
xm_password":"password1234"}
{ "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2"
, "xm_password":"password7890"}
```

키오스크기반장치에일반적인이예에서는 Secure Hub 가사용자에게다음과같이자격증명을요청하는메시지를표시합니다.

```
{ "serverURL":"https://example.com/zdm"}
```

Android Enterprise 의제로터치등록에대한사용자지정 JSON 을입력할수도있습니다.

```
1       {
2
3           "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4           {
5
6               "serverURL":"URL","xm_username":"username","
                    xm_password":"password"
7            }
8
9        }
10
11  <!--NeedCopy-->
```

장치에서등록을시작할때지정된 URL 에서 Secure Hub 를다운로드하고 Secure Hub 를설치한다음엽니다.

추가구성

구성에대한자세한정보는다음 Samsung 설명서페이지에서확인하십시오.

- 장치구성: 장치를대량으로추가합니다.
- Samsung Knox 배포앱: Bluetooth, NFC 또는 Wi-Fi Direct 등록을통해디바이스를등록합니다.
- Knox Mobile Enrollment: Samsung Knox 에대한자세한내용은 Samsung 설명서를참조하십시오.

버전 **2.4** 이전의 **Knox API** 를실행하는장치를등록하려면

Knox API 가버전 2.4 이전인장치에서는초기장치설정중일괄등록이시작되지않습니다. 대신사용자가등록을시작해야합니다. 이렇게하려면사용자는 Samsung 사이트로이동하여새로운 Mobile Enrollment 클라이언트를다운로드하고등록을시작합니다.

다운로드한등록클라이언트는 Knox 2.4/2.4.1 장치용으로 Knox 대량등록포털에구성된것과동일한 MDM 프로필및 APK 를사용합니다.

일반적으로사용자는다음단계를따릅니다.

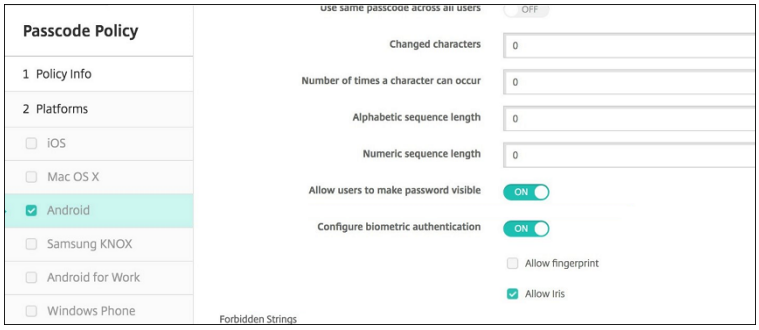
1. 장치를켜고 Wi-Fi 에연결합니다. Mobile Enrollment 가시작되지않거나 Wi-Fi 를사용할수없으면다음을수행합니다.
   a) Samsung Knox Mobile Enrollment로이동합니다.
   b) 다음버튼을눌러모바일데이터로장치를등록합니다.
2. **Knox** 로등록메시지가나타나면 계속을누릅니다.
3. EULA(제공되는경우) 를읽습니다. 다음을누릅니다.
4. 메시지가나타나면 IT 관리자가제공한 사용자 **ID** 및 암호를입력합니다.

이시점에서사용자자격증명의유효성이검사되고장치가조직의엔터프라이즈 IT 환경에등록됩니다.

Samsung 장치에생체인증을사용/사용안함으로설정

XenMobile 는생체인증으로도알려진지문및홍채인식인증을지원합니다. 사용자작업이없어도 Samsung 장치에대한생체인증을활성화하고비활성화할수있습니다. 관리자가 XenMobile 에서생체인증을사용하지않도록설정하면사용자와타사앱이이기능을사용하도록설정할수없습니다.

1. XenMobile 콘솔에서 구성 > 장치정책을클릭합니다. 장치정책페이지가나타납니다.
2. 추가를클릭합니다. 새정책추가페이지가나타납니다.
3. 암호를클릭합니다. 암호정책정보페이지가나타납니다.
4. 정책정보창에서다음정보를입력합니다.
   - 정책이름**:** 정책을설명하는이름을입력합니다.
   - 설명**:** 필요한경우정책의설명을입력합니다.
5. 다음을클릭합니다. 플랫폼페이지가나타납니다.
6. 플랫폼에서 **Android** 또는 **Samsung Knox** 를선택합니다.
7. 생체인증구성을 켜짐으로설정합니다.
8. **Android** 를선택한경우 **Samsung SAFE** 에서 지문허용또는 홍채허용또는둘다를선택합니다.



보안동작

August 12, 2022

관리 **>** 장치페이지에서장치및앱보안동작을수행합니다. 장치동작에는해지, 잠금, 잠금해제및초기화가포함됩니다. 앱보안동작에는앱잠금및앱초기화가포함됩니다.

- 활성화잠금바이패스**:** 장치활성화전에감독되는 iOS 장치에서활성화잠금을제거합니다. 이명령은개인 Apple ID 또는암호가없어도사용할수있습니다.
- 앱잠금**:** 장치의모든앱에대한액세스를거부합니다. Android 에서는앱이잠기면사용자가 XenMobile 에로그인할수없습니다. iOS 에서는사용자가로그인할수있지만앱에액세스할수는없습니다.
- 앱초기화**:** Secure Hub 에서사용자계정을제거하고장치를등록취소합니다. 사용자는 앱초기화취소작업을수행할때까지다시등록할수없습니다.
- **ASM** 배포프로그램활성화잠금**:** Apple School Manager DEP 에등록된 iOS 장치에대한활성화잠금바이패스코드를생성합니다.
- 제한사항지우기**:** 감독되는 iOS 장치에서이명령을사용하면사용자가구성한제한암호및제한설정을 XenMobile 이지울수있습니다.
- 분실모드활성화/비활성화**:** 감독되는 iOS 장치를분실모드로전환하고장치에표시할메시지, 전화번호및각주를보냅니다. 이명령을두번째로보내면장치가분실모드에서해제됩니다.
- 추적활성화**:** Android 또는 iOS 장치에서이명령을사용하면 XenMobile 에서특정장치의위치를정의된빈도로폴링할수있습니다. 지도에서장치의좌표및위치를보려면 관리 **>** 장치로이동하고장치를선택한다음 편집을클릭합니다. 장치정보는 일반탭의 보안아래에있습니다. 추적사용설정을사용하여장치를지속적으로추적합니다. Secure Hub 는장치가실행중일때주기적으로위치를보고합니다.
- 전체초기화**:** 모든메모리카드를포함하여장치에서모든데이터와앱을즉시지웁니다.
  - Android 장치의경우이요청에메모리카드를초기화하는옵션도포함될수있습니다.
  - 작업프로필로완전히관리되는 Android Enterprise 장치 (COPE 장치) 의경우선택적초기화로작업프로필을제거한후전체초기화를수행할수있습니다.
  - iOS 및 macOS 장치의경우장치가잠겨있더라도초기화가수행됩니다. iOS 11 장치 (최소버전) 의경우: 전체초기화를확인할때장치의셀룰러데이터요금제가보존되도록선택할수있습니다.
  - 메모리카드콘텐츠가삭제되기전에장치사용자가장치전원을끄면사용자의장치데이터액세스가가능할수있습니다.
  - 요청이장치로전송되기전까지는초기화요청을취소할수있습니다.
- 위치**:** 관리 **>** 장치페이지의 장치세부정보 **>** 일반에서장치를찾고지도를포함한장치위치를보고할수있습니다. 찾기는일회성작업입니다. 찾기작업을사용하면작업을수행할때현재장치위치가표시됩니다. 일정기간동안장치를지속적으로추적하려면 추적사용설정을사용합니다.
  - Android(Android Enterprise 제외) 장치또는 Android Enterprise(회사소유또는 BYOD) 장치에이작업을적용하는경우다음동작을숙지하십시오.

        * 위치찾기를사용하려면사용자가등록중에위치권한을부여해야합니다. 사용자는위치권한을부여하지않도록선택할수있습니다. 사용자가등록도중권한을부여하지않으면 XenMobile 은위치명령을전송할때다시 위치권한을요청합니다.
    - iOS 또는 Android Enterprise 장치에이기능을적용할경우다음제한사항에유의하십시오.
        * Android Enterprise 장치의경우 위치장치정책에서장치에대한위치모드를 높은정확도또는 배터리절약으로설정하지않으면이요청이실패합니다.
        * iOS 장치의경우이명령은장치가 MDM 분실모드에있는경우에만성공합니다.

- 잠금**:** 원격으로장치를잠급니다. 이작업은장치를분실한경우그리고장치를도난당했는지여부가불확실한경우에유용합니다. 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.
        * 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않고작업프로필에암호가이미설정되지않은경우장치가잠깁니다.
        * 암호가전송되지않았거나전송된암호가암호요구사항을충족하지않지만작업프로필에암호가이미설정되어있는경우에는작업프로필이잠기지만장치는잠기지않습니다.
- **Notify (Ring)(**알림 **(**벨울림**)):** Android 장치에서사운드를울립니다.
- 다시부팅**:** Windows 10 및 Windows 11 장치를다시시작합니다. Windows 태블릿및 PC 의경우 “System will reboot soon(시스템이곧다시부팅됩니다.)” 라는메시지가표시되고 5 분안에다시부팅됩니다.
- **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.
    - Android 장치를선택적으로초기화하면장치도철회됩니다. 콘솔에서재인증하거나삭제한후에만장치를다시등록할수있습니다.

  - 작업프로필로완전히관리되는 Android Enterprise 장치 (COPE 장치) 의경우선택적초기화로작업프로필을제거한후전체초기화를수행할수있습니다. 아니면동일한사용자이름으로장치를다시등록할수있습니다. 장치를다시등록하면작업프로필이다시생성됩니다.
  - Samsung Knox API 를사용하도록설정한경우장치를선택적으로초기화하면 Samsung Knox 컨테이너도제거됩니다.
  - iOS 및 macOS 장치의경우이명령은 MDM 을통해설치된모든프로필을제거합니다.
  - Windows 장치에서의선택적초기화는현재로그온된모든사용자의프로필폴더내용도제거합니다. 선택적초기화는구성을통해사용자에게배달하는웹클립은제거하지않습니다. 웹클립을제거하려면사용자가자신의장치를수동으로등록취소해야합니다. 선택적으로초기화된장치를다시등록할수없습니다.

- 잠금해제**:** 잠겨있을때장치로전송된암호를지웁니다. 이명령은장치를잠금해제하지않습니다.

관리 **>** 장치의 장치세부정보페이지에도장치보안속성이나열됩니다. 이러한속성에는강력한 ID, 장치잠금, 활성화잠금바이패스및플랫폼유형에대한기타정보등이포함됩니다. 장치전체초기화필드에는사용자 PIN 코드가포함됩니다. 장치가초기화된후사용자는이코드를입력해야합니다. 사용자가코드를잊은경우여기서코드를조회할수있습니다.

Android 장치에대한보안동작

보안동작	Android(Android Enterprise 장치제외)	Android Enterprise(BYOD)	Android Enterprise(회사소유)
앱잠금	예	아니요	아니요
앱초기화	예	아니요	아니요
전체초기화	예	아니요	예
찾기	예: Android 6.0 이상을실행하는장치의경우위치를사용하려면사용자가등록도중위치권한을부여해야합니다. 사용자는위치권한을부여하지않도록선택할수있습니다. 사용자가등록도중권한을부여하지않으면 XenMobile 은위치명령을전송할때다시위치권한을요청합니다.	예: Android 6.0 이상을실행하는장치의경우위치를사용하려면사용자가등록도중위치권한을부여해야합니다. 사용자는위치권한을부여하지않도록선택할수있습니다. 사용자가등록도중권한을부여하지않으면 XenMobile 은위치명령을전송할때다시위치권한을요청합니다.	예: Android 6.0 이상을실행하는장치의경우위치를사용하려면사용자가등록도중위치권한을부여해야합니다. 사용자는위치권한을부여하지않도록선택할수있습니다. 사용자가등록도중권한을부여하지않으면 XenMobile 은위치명령을전송할때다시위치권한을요청합니다.
잠금	예	예	예
Lock and Reset Password(잠금및암호재설정)	예	아니요	예
Notify (Ring)(알림 (벨울림))	예	예	예

보안동작	Android(Android Enterprise 장치제외)	Android Enterprise(BYOD)	Android Enterprise(회사소유)
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 배포프로그램활성화잠금	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** 태블릿 **10**
찾기	예
잠금	예

보안동작	**Windows** 태블릿 **10**
Lock and Reset Password(잠금및암호재설정)	아니요
다시부팅	예
해지	예
벨울림	아니요
선택적초기화	예
초기화	예

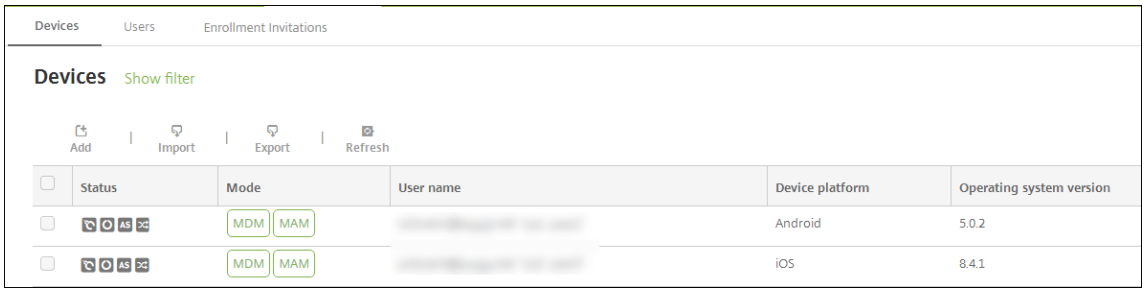
이문서의나머지부분에서는다양한보안동작을수행하는단계를설명합니다. 일부동작은자동화할수도있습니다. 자세한내용은 자동화된동작을참조하십시오.

iOS 장치잠금

분실된 iOS 장치를잠그고장치잠금화면에메시지와전화번호를표시할수있습니다. 이기능은 iOS 7 이상을실행하는장치에서지원됩니다.

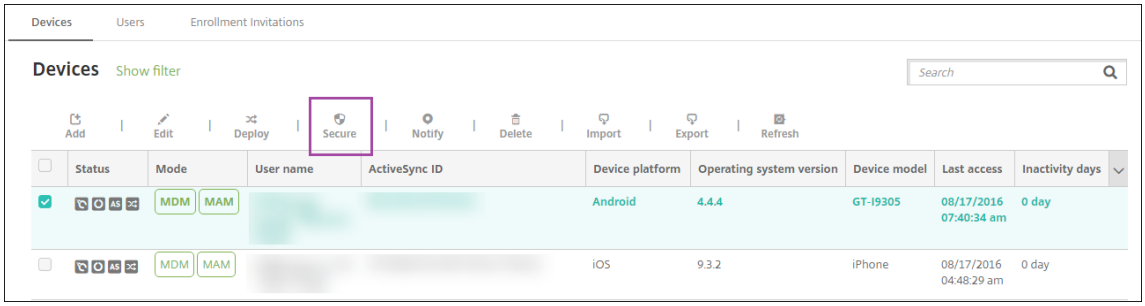
잠겨있는장치에메시지와전화번호를표시하려면 XenMobile 콘솔에서 암호 정책을 **true** 로설정합니다. 또는사용자가수동으로장치에서암호를사용하도록설정할수있습니다.

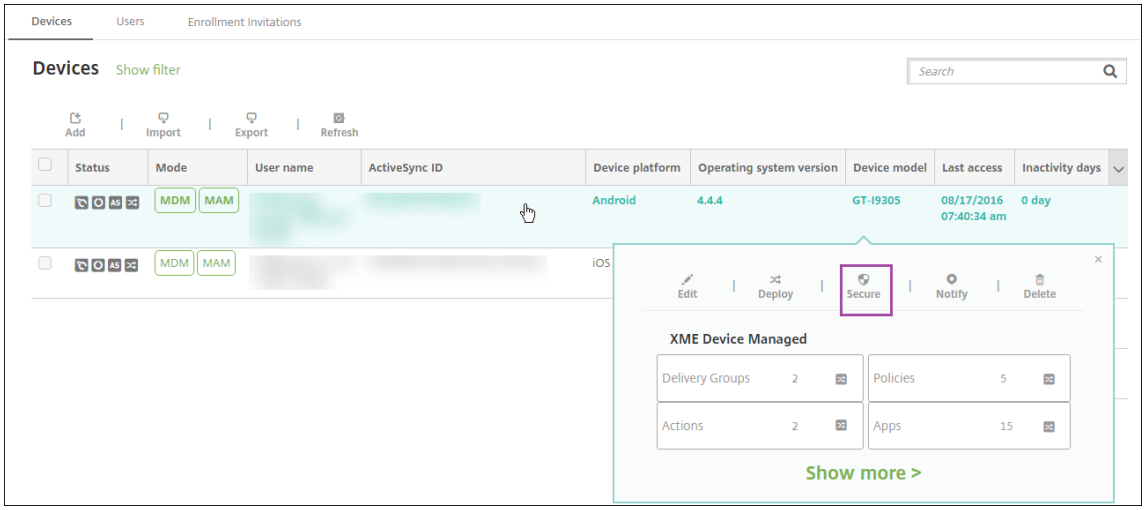
1. 관리 **>** 장치를클릭합니다. 장치페이지가나타납니다.



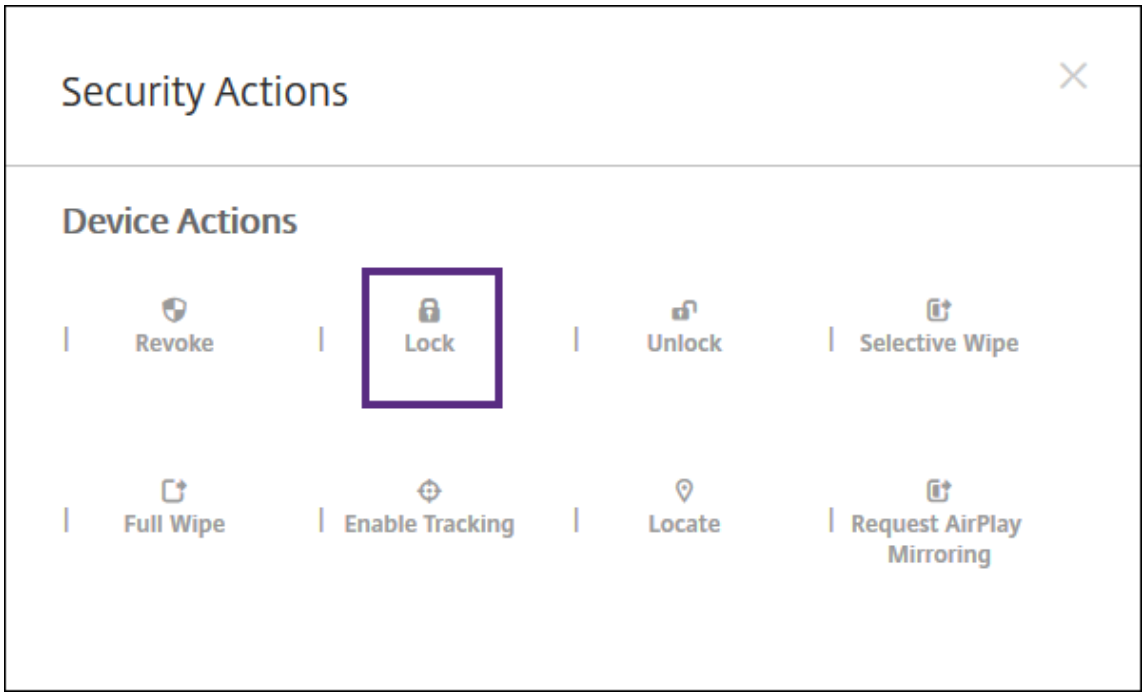
2. 잠글 iOS 장치를선택합니다.

   장치옆에있는확인란을선택하면장치목록위에옵션메뉴가표시됩니다. 목록에서아무위치를클릭하면목록의오른쪽에옵션메뉴가나타납니다.

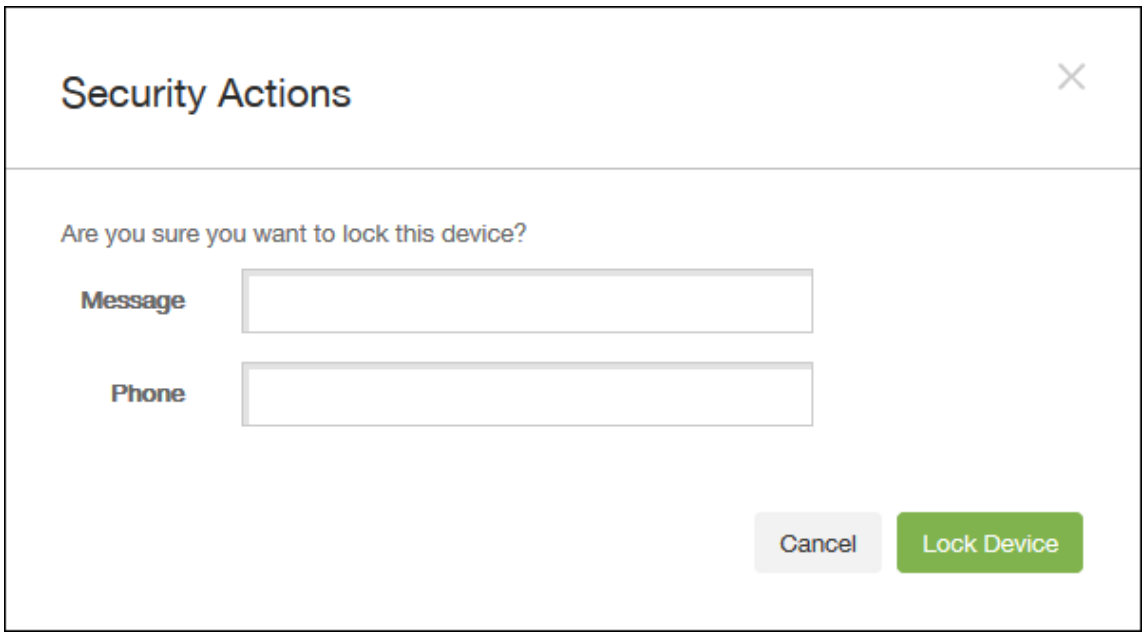




3. 옵션메뉴에서 보안을클릭합니다. 보안동작대화상자가나타납니다.



4. 잠금을클릭합니다. 보안동작확인대화상자가표시됩니다.



5. 필요에따라장치잠금화면에표시되는메시지와전화번호를입력합니다.

   iOS 7 이상을실행하는 iPad 의경우: 메시지필드에입력하는내용에 “iPad 분실” 이라는단어가추가됩니다.

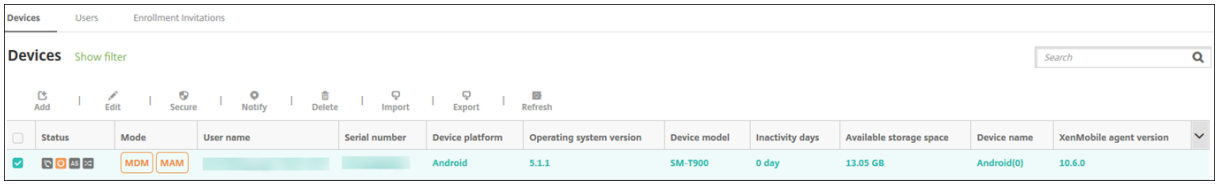
   iOS 7 이상을실행하는 iPhone 의경우: 메시지필드를비워두고전화번호를입력할경우장치잠금화면에 “소유자에게통화” 라는메시지가표시됩니다.

6. 장치잠금을클릭합니다.

XenMobile 콘솔에서장치제거

> 중요**:**
>
> XenMobile 콘솔에서장치를제거하는경우관리되는앱및데이터는장치에남습니다. 관리되는앱및데이터를장치에서제거하려면이문서뒷부분의 “장치삭제” 를참조하십시오.

XenMobile 콘솔에서장치를제거하려면 관리 **>** 장치로이동하여관리되는장치를선택한다음 삭제를클릭합니다.



장치를선택적으로초기화

1. 관리 **>** 장치로이동하고관리되는장치를선택한다음 보안을클릭합니다.
2. 보안동작에서 선택적초기화를클릭합니다.

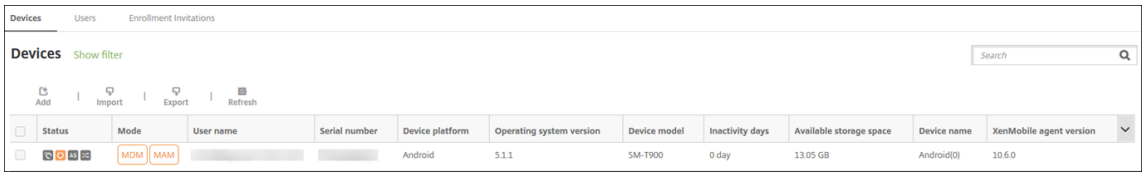
3. Android 장치의경우에만회사네트워크에서장치를분리합니다. 이렇게하려면장치가초기화된후 보안동작에서 해지를클릭하십시오.

   초기화가수행되기전에선택적초기화요청을철회하려면 보안동작에서 선택적초기화취소를클릭합니다.

장치삭제

이절차는관리되는앱및데이터를장치에서제거하고 XenMobile 콘솔의장치목록에서장치를삭제합니다. Endpoint Management Public REST API 를사용하여장치를대량으로삭제할수있습니다.

1. 관리 **>** 장치로이동하고관리되는장치를선택한다음 보안을클릭합니다.
2. 선택적초기화를클릭합니다. 메시지가나타나면 선택적초기화수행을클릭합니다.
3. 초기화명령이성공했는지확인하려면 관리 **>** 장치를새로고치십시오. 모드열에서 MDM 및 MAM 의색이황색이면초기화명령이성공한것입니다.



4. 관리 **>** 장치에서장치를선택한다음 삭제를클릭합니다. 메시지가나타나면 삭제를다시클릭합니다.

앱잠금, 잠금해제, 초기화또는초기화취소

1. 관리 **>** 장치로이동하고관리되는장치를선택한다음 보안을클릭합니다.
2. 보안동작에서앱동작을클릭합니다.

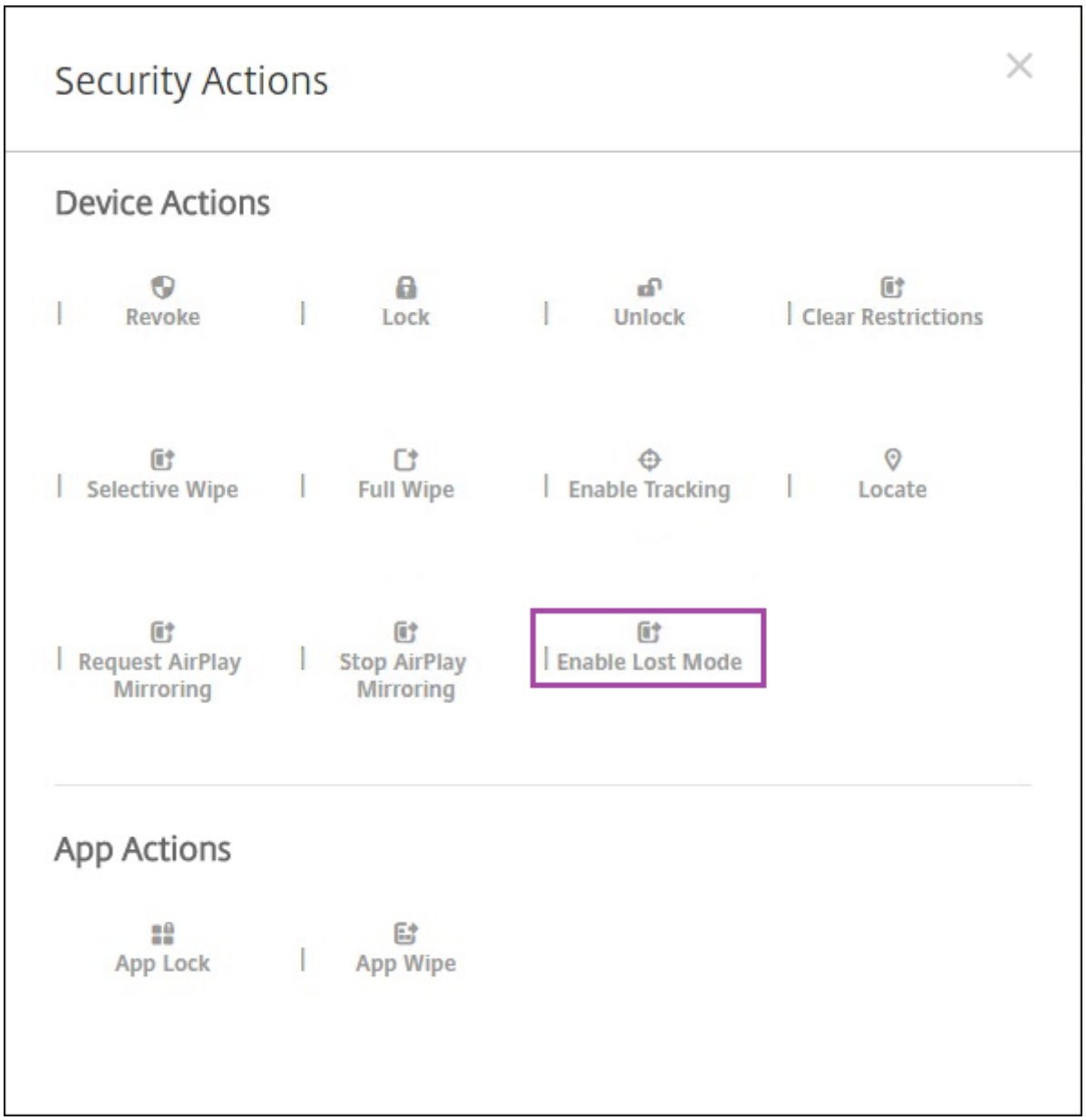
   보안동작상자를사용하여 Active Directory 에서계정이사용하지않도록설정되었거나삭제된사용자의장치상태를확인할수있습니다. 앱잠금해제또는앱초기화취소동작이나타나면앱이잠겼거나초기화되었음을나타냅니다.

iOS 장치를분실모드로전환

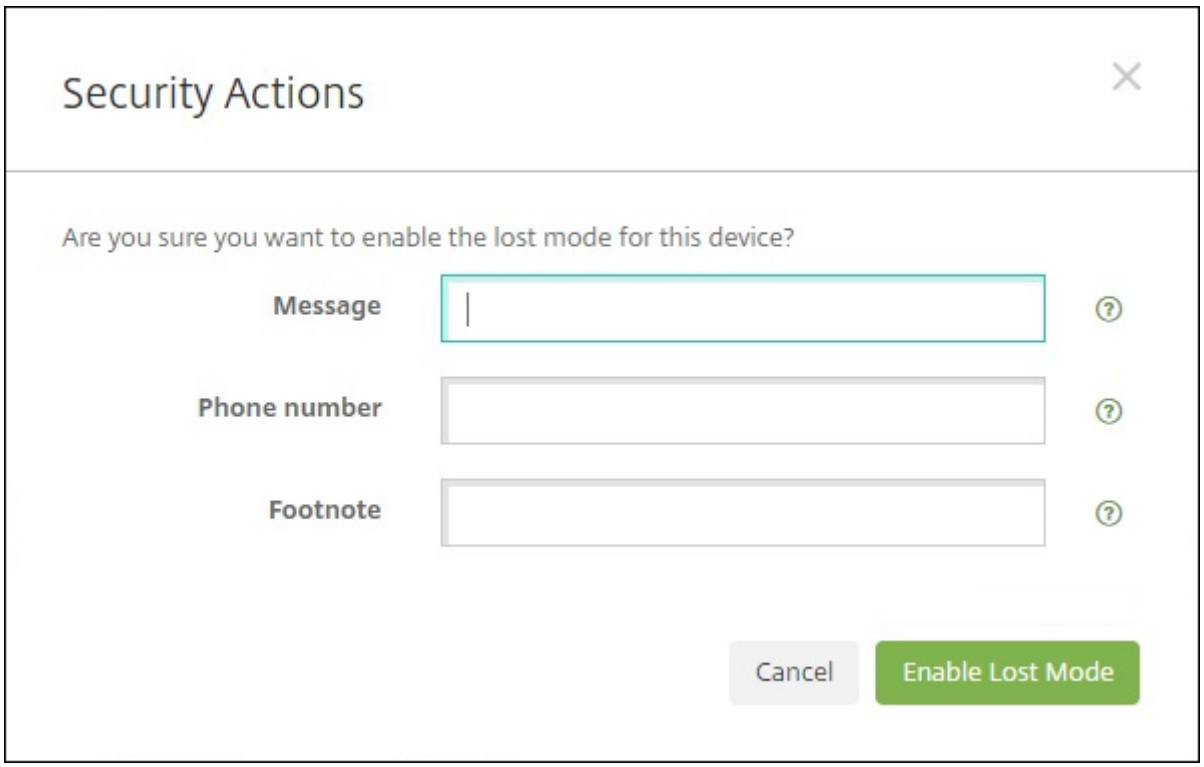
XenMobile 분실모드장치속성은 iOS 장치를분실모드로전환합니다. Apple 의관리되는분실모드와달리 XenMobile 의분실모드에서는다음동작중하나를수행하여사용자가 나의 **iPhone/iPad** 찾기설정을구성하거나 Citrix Secure Hub 의위치서비스를사용하지않아도장치위치를찾을수있습니다.

XenMobile 분실모드에서는 XenMobile Server 만장치잠금을해제할수있습니다. 이와반대로 XenMobile 장치잠금기능을사용하는경우에는사용자가제공된 PIN 코드를사용하여장치를직접잠금해제할수있습니다.

분실모드를사용하거나사용하지않으려면: 관리 **>** 장치로이동하고감독되는 iOS 장치를선택한후 보안을클릭합니다. 분실모드활성화또는 분실모드비활성화를클릭합니다.

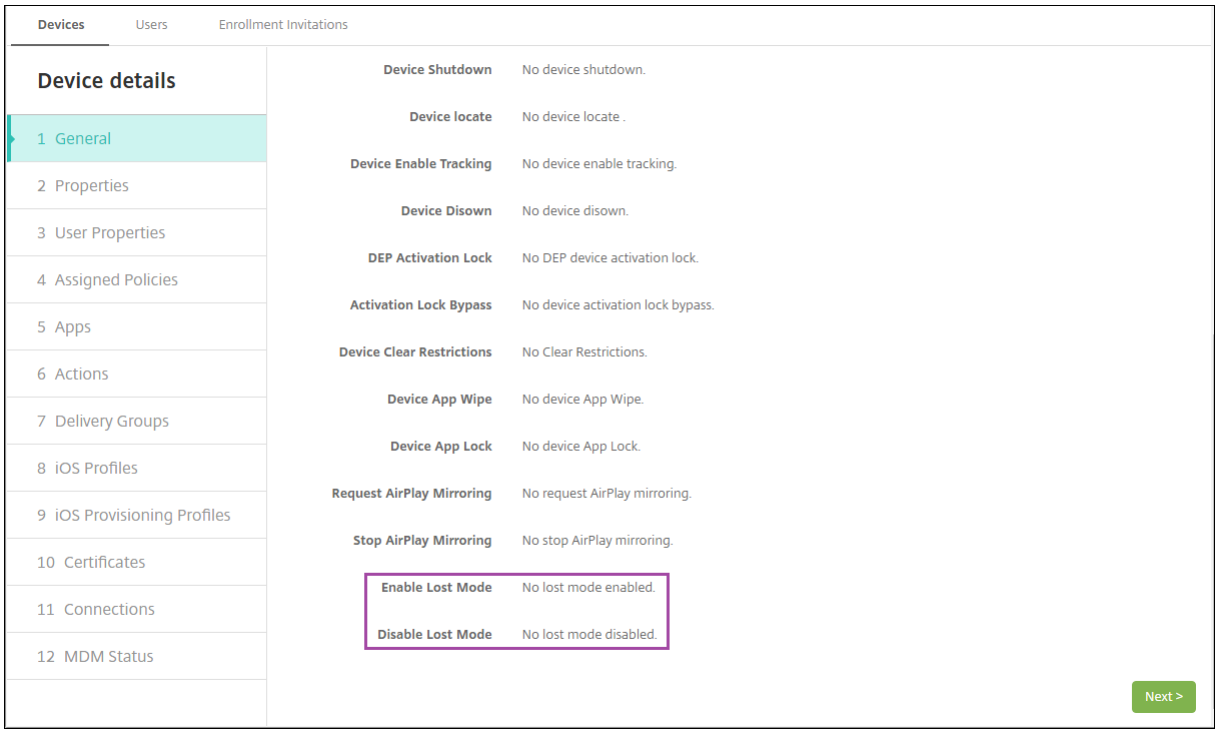


분실모드활성화를클릭하고장치가분실모드가될때장치에표시할정보를입력합니다.

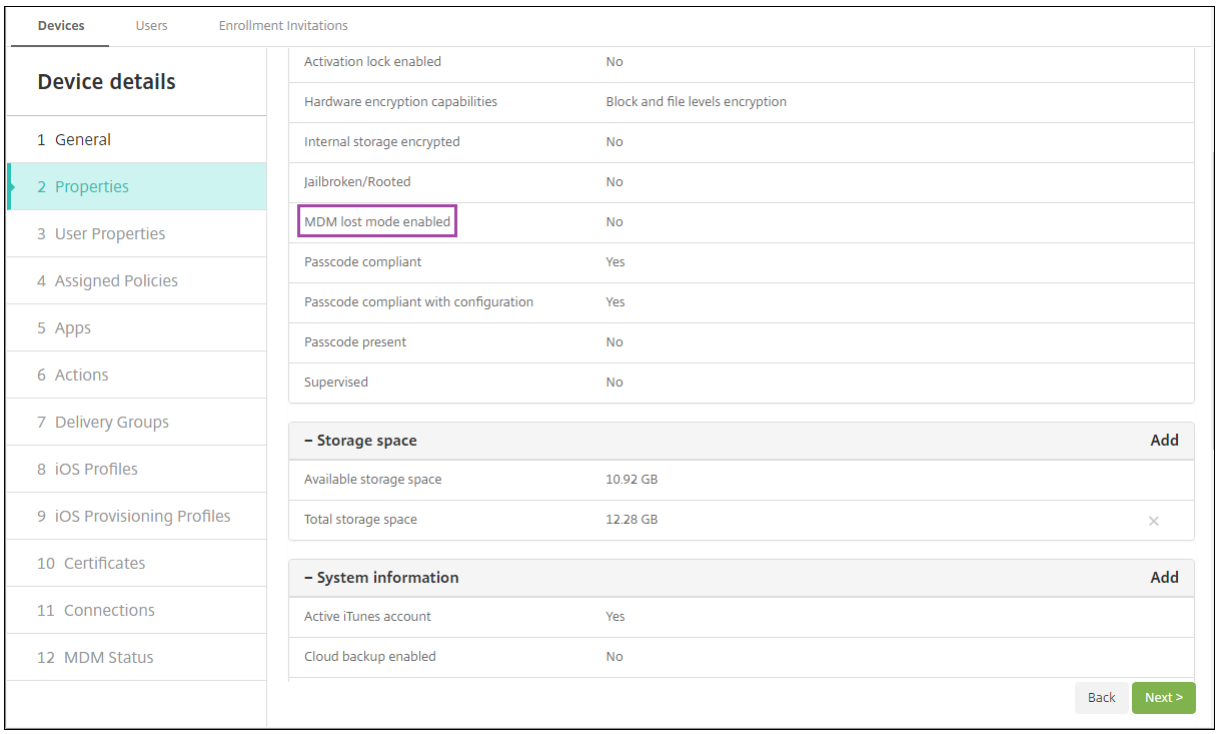


다음방법중하나를사용하여분실모드상태를확인합니다.

- 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 찾기를비활성화하고장치를지우거나장치를재활성화하여사용하려고할경우사용자의 Apple ID 와암호를요구합니다. 조직이소유한장치의경우예를들어장치를재설정하거나재할당하기위해활성화잠금을바이패스해야합니다.

활성화잠금을사용하도록설정하려면 XenMobile MDM 옵션장치정책을구성하고배포합니다. 그러면사용자의 Apple 자격증명이없이도 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.

- 사용자에게내 iPhone/iPad 찾기를비활성화하지말라고안내하십시오. 장치에서전체초기화를수행하지마십시오. 두경우모두사용자에게 iCloud 계정암호를입력하라는메시지가표시됩니다. 계정유효성검사후모든콘텐츠와설정을지운다음 사용자에게 iPhone/iPad 활성화화면이표시되지않습니다.
- 활성화잠금바이패스코드가생성되고활성화잠금을사용하도록설정한장치의경우전체초기화후 iPhone/iPad 활성화페이지를바이패스할수없으면 XenMobile 에서장치를삭제할필요가없습니다. 관리자또는사용자가 Apple 지원팀에연락하여직접장치의차단을해제할수있습니다.
- 하드웨어인벤토리중에 XenMobile 은장치에서활성화잠금바이패스코드를쿼리합니다. 바이패스코드를사용할수있는경우장치가해당코드를 XenMobile 에전송합니다. 그런다음장치에서바이패스코드를제거하려면 XenMobile 콘솔에서 활성화잠금바이패스보안동작을전송합니다. 이때장치의차단을해제하려면 XenMobile Server 와 Apple 에바이패스코드가있어야합니다.
- 활성화잠금바이패스보안동작은 Apple 서비스의이용가용성에따라달라집니다. 이동작이작동하지않는경우다음과같이장치의차단을해제할수있습니다. 장치에서수동으로 iCloud 계정의자격증명을입력합니다. 또는사용자이름필드를비워두고암호필드에바이패스코드를입력합니다. 바이패스코드를조회하려면 관리 **>** 장치로이동하여장치를선택하고 편집, 속성을차례로클릭합니다. 활성화잠금바이패스코드는 보안정보아래에있습니다.

공유장치

January 5, 2022

XenMobile 을통해여러사용자가공유할수있는장치를구성할수있습니다. 공유장치기능을사용하면, 예를들어병원의임상의사가특정장치를가지고다닐필요없이주변에있는장치를사용하여앱과데이터에액세스할수있습니다. 법집행, 소매및제조와같은분야의

교대근무자가장치를공유하여장비비용을절감할수도있습니다.

공유장치에대한주요사항

지원되는모든 iOS 및 Android 장치를공유장치로사용할수있습니다. 지원되는장치목록은 지원되는장치운영체제를참조하십시오.

MDM 등록

- iOS 및 Android 태블릿과스마트폰에서모두사용할수있습니다. XenMobile Enterprise 공유장치에대한 Apple 배포프로그램등록은지원하지않습니다. 승인된 Apple 배포프로그램을사용하여이모드의공유장치를등록합니다.
- 클라이언트인증서인증, Citrix PIN, Touch ID, 사용자엔트로피및 2 단계인증은지원하지않습니다.

MDM+MAM 등록

- iOS 및 Android 장치에서만사용할수있습니다.
- Active Directory 사용자이름및암호인증만지원됩니다.
- 클라이언트인증서인증, Secure Hub 암호, Touch ID, 사용자엔트로피및 2 단계인증은지원하지않습니다.
- MAM 전용등록은지원하지않습니다. MDM 에서장치를등록해야합니다.
- Secure Mail, Secure Web, ShareFile 모바일앱만지원합니다. HDX 앱은지원하지않습니다.
- Active Directory 사용자만지원합니다. 로컬사용자와그룹은지원하지않습니다.
- MDM+MAM 로업데이트하려면기존 MDM 전용공유장치의재등록이필요합니다.
- 사용자는장치의기본앱을공유할수없습니다.
- 처음등록할때다운로드된후에는사용자로그인중에모바일생산성앱이다시다운로드되지않습니다.
- Android 에서보안을위해각사용자의데이터를격리하려면 XenMobile 콘솔의 루팅된장치허용안함정책을 켜짐으로설정합니다.

공유장치등록을위한사전요구사항

공유장치를등록하려면먼저다음을수행해야합니다.

- 공유장치등록사용자역할을만듭니다. RBAC 를사용하여역할구성을참조하십시오.
- 공유장치사용자를만듭니다. 로컬사용자계정을추가, 편집, 잠금해제또는삭제하려면을참조하십시오.
- 공유장치사용자에게적용할기본정책, 앱및동작을포함하는배달그룹을만듭니다. 리소스배포를참조하십시오.

MDM+MAM 등록사전요구사항

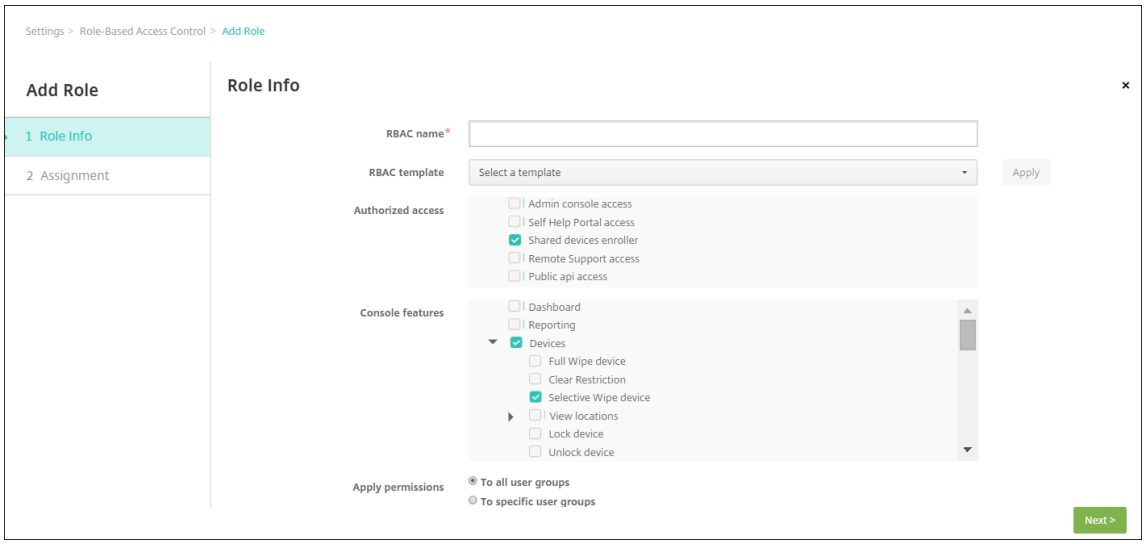
1. Active Directory 그룹을만듭니다. **Shared Device Enrollers** 와같이설명하는이름을부여합니다.
2. 공유장치를등록할 Active Directory 사용자를이그룹에추가합니다. 이용도로새계정을사용하려면새 Active Directory 사용자 (예: **sdenroll**) 를만들고해당사용자를 Active Directory 그룹에추가합니다.

공유장치구성

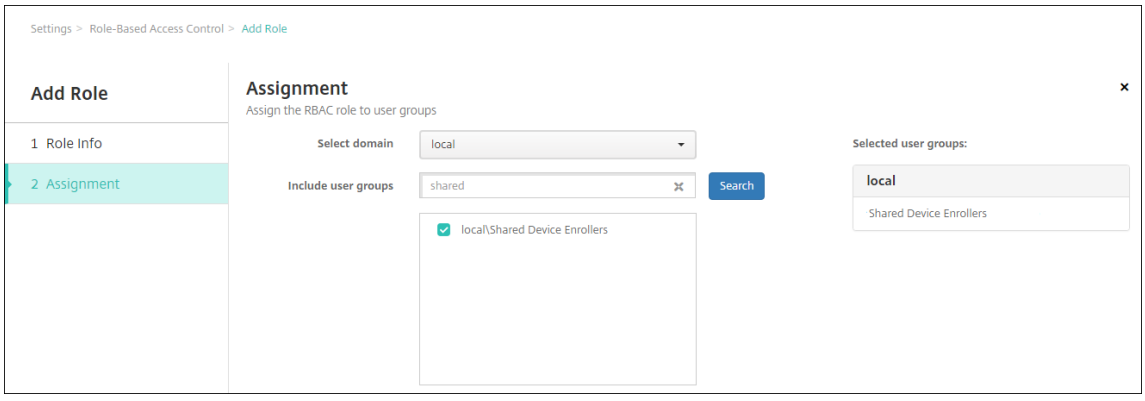
다음단계에따라공유장치를구성합니다.

1. XenMobile 콘솔에서오른쪽위모서리의기어를클릭합니다. 설정페이지가나타납니다.
2. 역할기반액세스제어를클릭한다음 추가를클릭합니다. 역할추가화면이나타납니다.
3. 허가된액세스아래에서 공유장치등록자권한이있는 **Shared Device Enrollment User** 라는공유장치등록사용자역할을만듭니다. 콘솔기능에서 장치를확장한다음 장치선택적초기화를선택하십시오. 이설정을사용하면장치가등록취소될때공유장치등록자계정을통해프로비저닝된앱및정책이 Secure Hub 를통해삭제됩니다.

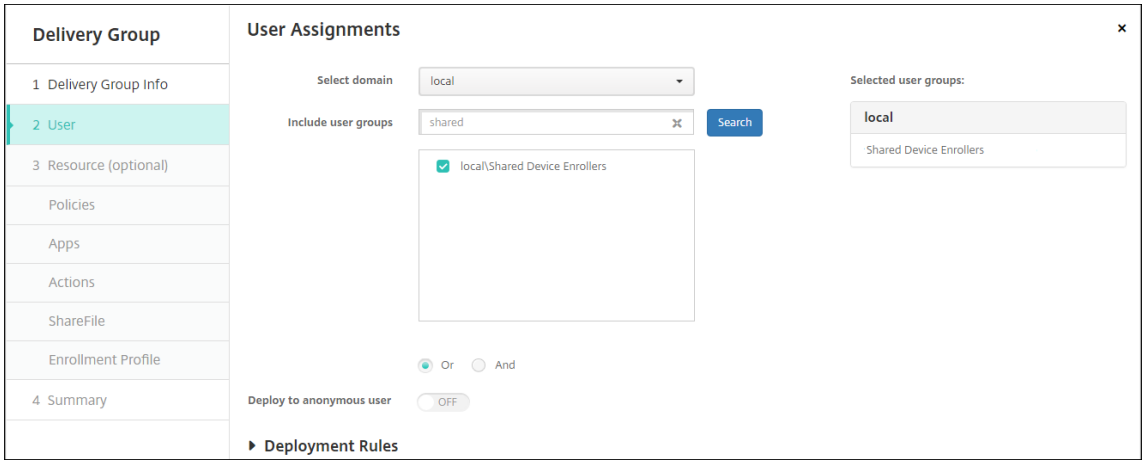
   권한적용은기본설정인 모든사용자그룹으로유지하거나, 특정사용자그룹을사용하여특정 Active Directory 사용자그룹에권한을할당합니다.



   다음을클릭하여 할당화면으로이동합니다. 1 단계에서사전요구사항에따라만든공유장치등록역할을공유장치등록사용자의 Active Directory 그룹에할당합니다. 다음이미지에서 **citrix.lab** 은 Active Directory 도메인이고 **Shared Device Enrollers** 는 Active Directory 그룹입니다.



4. 사용자가로그인되어있지않을때장치에적용할기본정책, 앱및동작을포함하는배달그룹을만듭니다. 그런다음공유장치등록사용자의 Active Directory 그룹과배달그룹을연결합니다.



5. 공유장치에 Secure Hub 를설치하고공유장치등록사용자계정을사용하여 XenMobile 에장치를등록합니다. 이제 XenMobile 콘솔을통해장치를보고관리할수있습니다. 자세한내용은 장치등록을참조하십시오.
6. 서로다른정책을적용하거나인증된사용자를위한추가앱을제공하려면해당사용자와연결되고공유장치에만배포된배달그룹을만들어야합니다. 그룹을만들때배포규칙을구성하여패키지가공유장치에배포되도록합니다. 자세한내용은 리소스배포를참조하십시오.
7. 장치공유를중지하려면선택적초기화를수행하여장치에서공유장치등록사용자계정을제거합니다. 장치에배포된앱과정책을모두제거합니다.

공유장치사용자환경

MDM 등록

사용자는자신이사용할수있는리소스만보며모든공유장치에서동일한환경을사용합니다. 공유장치등록정책및앱이항상장치에유지됩니다. 공유장치에등록되어있지않은사용자가 Secure Hub 에로그온하면해당사용자의정책및앱이장치에배포됩니다. 해당사용자가로그오프하면공유장치등록의일부가아닌모든정책과앱은제거됩니다. 공유장치등록리소스는그대로유지됩니다.

MDM+MAM 등록

공유장치등록사용자가등록할때장치에 Secure Mail 및 Secure Web 이배포됩니다. 사용자데이터는장치에서안전하게유지관리됩니다. Secure Mail 또는 Secure Web 에로그온하는다른사용자에게데이터가노출되지않습니다.

한번에한사용자만 Secure Hub 에로그온할수있습니다. 다음사용자가로그온하려면이전사용자가로그오프해야합니다. 보안상의이유로 Secure Hub 는공유장치에사용자자격증명을저장하지않으므로사용자는로그온할때마다자격증명을입력해야합니다. Secure Hub 은이전사용자와연결된정책, 앱, 데이터가제거될때까지새로운로그온을차단합니다.

공유장치등록은앱을업그레이드하는프로세스를변경하지않습니다. 이전과마찬가지로, 공유장치사용자에게업그레이드를푸시할수있으며공유장치사용자가장치에서바로앱을업그레이드할수있습니다.

권장 **Secure Mail** 정책

- 최상의 Secure Mail 성능을얻으려면장치를공유할사용자의수를기반으로 최대동기화기간을설정합니다. 무제한동기화를허용하는것은권장하지않습니다.

장치를공유하는사용자수	권장최대동기화기간
21–25	1 주이하
6–20	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

January 5, 2022

자동검색서비스는전자메일기반 URL 검색을통해사용자의등록프로세스를간소화합니다. 또한자동검색서비스는등록확인, 인증서고정같은기능과 Citrix Workspace 고객을위한기타이점을제공합니다. Citrix Cloud 에서호스팅되는이서비스는여러 XenMobile 배포의중요한부분입니다.

자동검색서비스를사용하면다음과같은이점이있습니다.

- 회사네트워크자격증명을사용하여장치를등록할수있습니다.
- XenMobile Server 주소에대한세부정보를입력할필요가없습니다.
- 사용자이름을 UPN(사용자계정이름) 형식으로입력합니다. 예를들어, `user@mycompany.com`입니다.

보안수준이높은환경에서는자동검색서비스를사용하는것이좋습니다. 자동검색서비스는중간자공격을방지하는공개키인증서고정을지원합니다. 인증서고정을사용하면 Citrix 클라이언트가 XenMobile 과통신할때회사에서서명한인증서가사용됩니다. XenMobile 사이트에대한인증서고정을구성하려면 Citrix 지원서비스에문의하십시오. 인증서고정에대한자세한내용은 인증서고정을참조하십시오.

자동검색서비스에액세스하려면 https://adsui.cloud.com(상업용) 또는 https://adsui.cem.cloud.us(정부) 로이동합니다.

사전요구사항

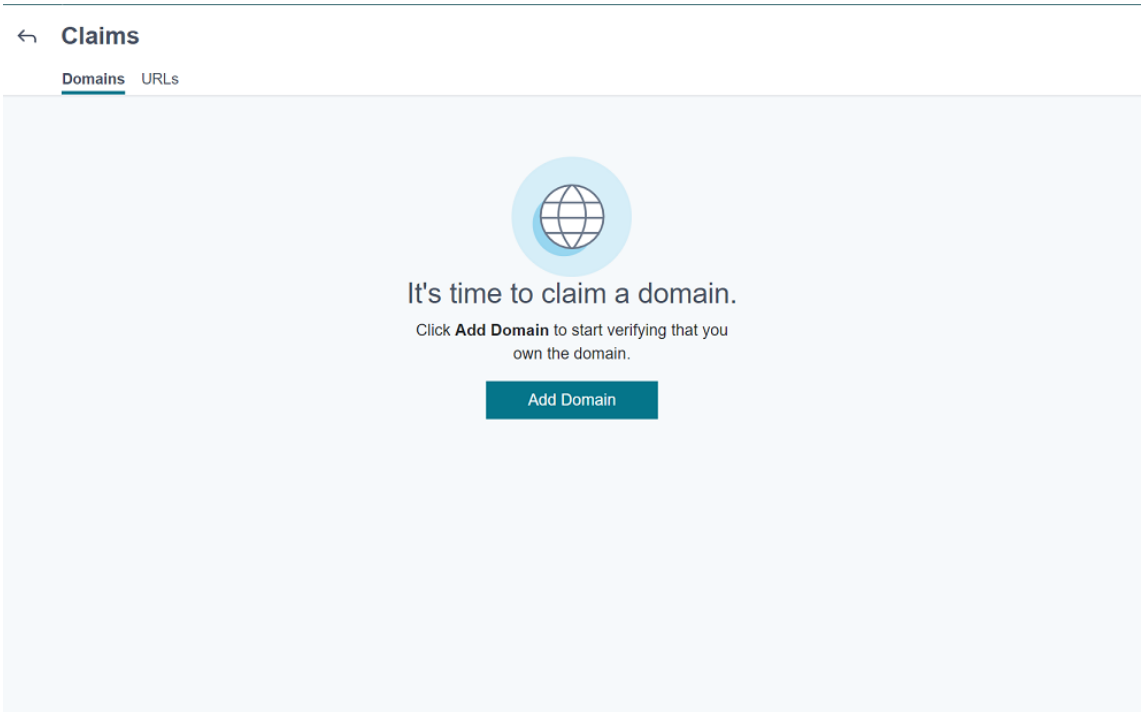
- Citrix Cloud 의새로운자동검색서비스를사용하려면다음과같은 Secure Hub 최신버전이필요합니다.
  - iOS 의경우 Secure Hub 버전 21.6.0 이상
  - Android 경우 Secure Hub 버전 21.8.5 이상

    이전버전의 Secure Hub 을실행하는장치에서서비스중단이발생할수있습니다.
- 새자동검색서비스에액세스하려면전체액세스권한이있는 Citrix Cloud 관리자계정이있어야합니다. 자동검색서비스는사용자지정액세스권한이있는관리자계정을지원하지않습니다. 계정이없는경우 Citrix Cloud 가입을참조하십시오.

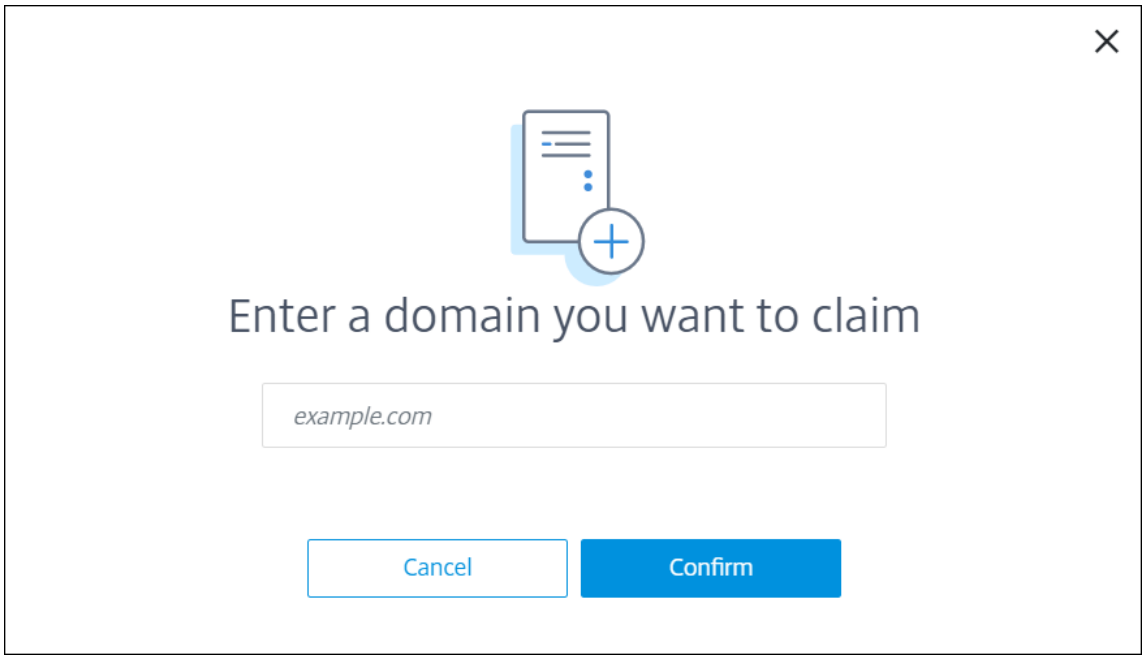
  Citrix 는서비스중단없이기존의모든자동검색레코드를 Citrix Cloud 로마이그레이션했습니다. 마이그레이션된레코드는새콘솔에자동으로나타나지않습니다. 소유권을증명하려면새자동검색서비스에서도메인을회수해야합니다. 자세한내용은 CTX312339를참조하십시오.
- Endpoint Management 배포에대해자동검색서비스를사용하기전에도메인을확인하고요청합니다. 최대 10 개의도메인을요청할수있습니다. 요청은확인된도메인과자동검색서비스를연결합니다. 11 개이상의도메인을요청하려면 SRE 티켓을열거나 Citrix 기술지원에문의하십시오.
- Citrix Gateway FQDN 대신 MAM 포트설정을사용하여 MAM 트래픽을데이터센터로보낼수있습니다. Citrix Gateway 의포트와함께정규화된도메인이름을입력하면클라이언트장치는 **MAM** 포트설정의구성을사용합니다.
- 광고차단으로인해사이트가열리지않는경우전체웹사이트에대한광고차단기를비활성화해야합니다.

도메인요청

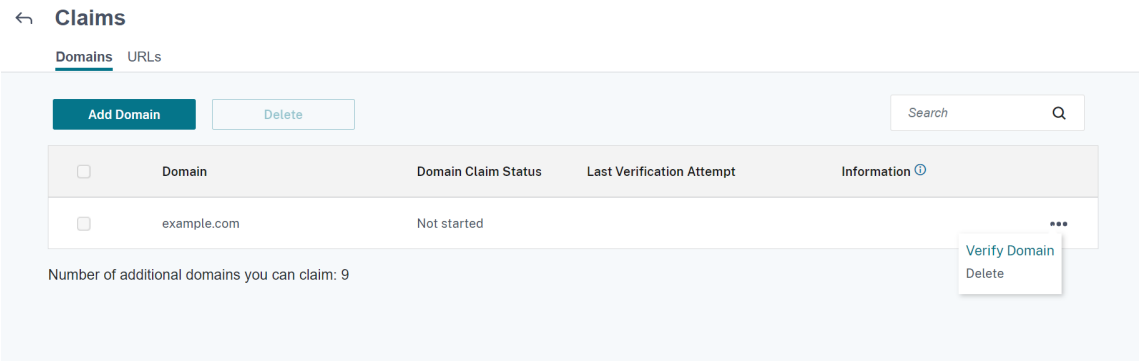
1. 요청 **>** 도메인탭에서 도메인추가를클릭합니다.



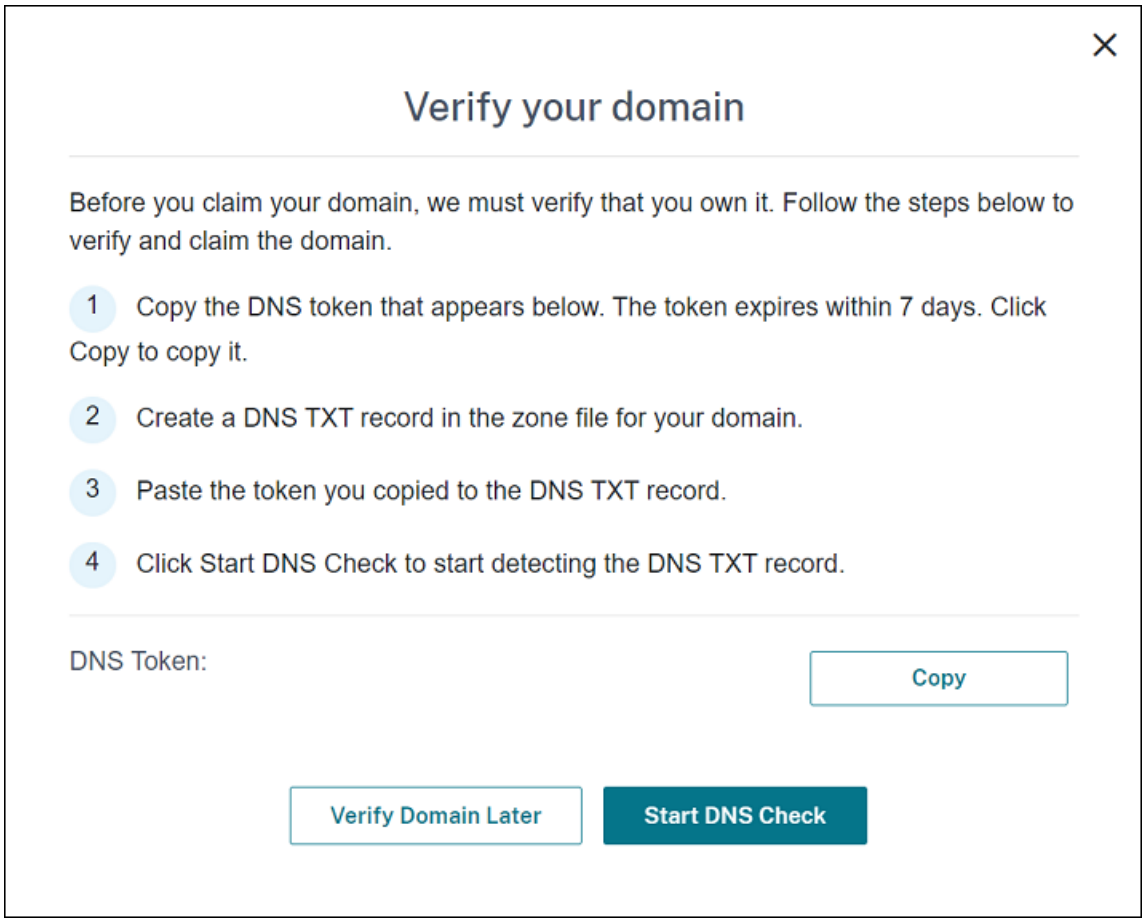
2. 대화상자가나타나면 XenMobile 환경의도메인이름을입력하고 확인을클릭합니다. 도메인이 요청 **>** 도메인에나타납니다.



3. 추가한도메인에서줄임표메뉴를클릭하고 도메인확인을선택하여확인프로세스를시작합니다. 도메인확인페이지가나타납니다.



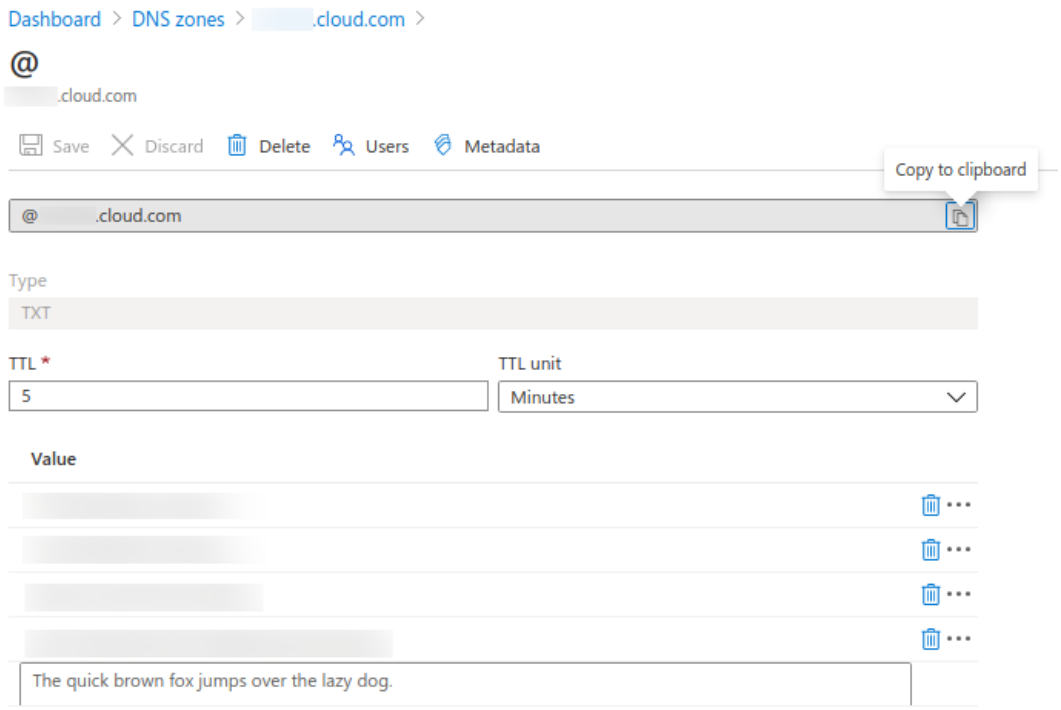
4. 도메인확인페이지에서지침에따라도메인을소유하고있는지확인합니다.



a) 복사를클릭하여 DNS 토큰을클립보드에복사합니다.

b) 도메인의영역파일에서 DNS TXT 레코드를만듭니다. 이렇게하려면도메인호스팅공급자포털로이동하여복사한 DNS 토큰을추가합니다.

다음스크린샷은도메인호스팅공급자포털을보여줍니다. 실제포털은다르게보일수있습니다.



c) Citrix Cloud 의 도메인확인페이지에서 **DNS** 확인시작을클릭하여 DNS TXT 레코드검색을시작합니다. 나중에 도메인을확인하려면 나중에도메인확인을클릭합니다.

확인프로세스에는보통약 1 시간정도가소요됩니다. 그러나응답을반환하는데최대 2 일까지걸릴수있습니다. 상태확인중에로그아웃했다가다시로그인해도괜찮습니다.

구성이완료되면도메인상태가 보류중에서 확인됨으로변경됩니다.

5. 도메인을요청한후자동검색서비스에대한정보를제공합니다. 추가한도메인의말줄임표메뉴를클릭한다음 **Endpoint Management** 정보추가를클릭합니다. 자동검색서비스정보페이지가나타납니다.
6. 다음정보를입력한다음 저장을클릭합니다.
   - **Endpoint Management** 서버 **FQDN:** XenMobile Server 의정규화된도메인이름을입력합니다. 예: `example.xm.cloud.com`. 이설정은 MDM 및 MAM 제어트래픽에사용됩니다.
   - **Citrix Gateway FQDN:** Citrix Gateway 의정규화된도메인이름을 FQDN 또는 FQDN: 포트형식으로입력합니다. 예: `example.com`. 이설정은 MAM 트래픽을데이터센터로보내는데사용됩니다. MDM 전용배포의 경우이필드를비워둡니다.

     > 참고:
     >
     > Citrix 는 MAM 트래픽을제어하기위해 **Citrix Gateway FQDN** 대신 **MAM** 포트를사용하기를권장합니다. Citrix Gateway 의포트와함께정규화된도메인이름을입력하면클라이언트장치는 **MAM** 포트설정의 구성을사용합니다.

- 인스턴스이름**:** 위에서구성한 XenMobile Server 의인스턴스이름을입력합니다. 인스턴스이름을잘모르는경우기본값인 **zdm** 을그대로둡니다.
- **MDM** 포트**:** MDM 제어트래픽및 MDM 등록에사용되는포트를입력합니다. 클라우드기반서비스의경우기본값은 443 입니다.
- **MAM** 포트**:** MAM 제어트래픽, MAM 등록, iOS 등록및앱열거에사용되는포트를입력합니다. 클라우드기반서비스의경우기본값은 8443 입니다.

Windows 장치에대한자동검색요청

Windows 장치를등록하려는경우다음을수행합니다.

1. Citrix 지원서비스에문의하여 Windows 자동검색을사용하도록설정하는지원요청을만듭니다.
2. `enterpriseenrollment.mycompany.com`에대해공개적으로서명된와일드카드가아닌 SSL 인증서를얻습니다. 이 `mycompany.com` 부분은사용자가등록하는데사용하는계정이포함된도메인입니다. .pfx 형식의 SSL 인증서와암호를이전단계에서만든지원요청에연결합니다.

   두개이상의도메인을사용하여 Windows 장치를등록하려면다음과같은구조의다중도메인인증서를사용할수도있습니다.

   - SubjectDN 과기본도메인을지정하는 CN(예: enterpriseenrollment.mycompany1.com)
   - 나머지도메인에해당하는 SAN(예: enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com 등)
3. DNS 에 CNAME(정식이름) 레코드를만들고 SSL 인증서주소 (enterpriseenrollment.mycompany.com) 를 autodisc.xm.cloud.com 에매핑합니다.

   Windows 장치사용자가 UPN 을사용하여등록하면 Citrix 등록서버는다음을수행합니다.

   - XenMobile Server 에대한세부정보를제공합니다.
   - XenMobile 에서유효한인증서를요청하도록장치에지시합니다.

이시점에서지원되는모든장치를등록할수있습니다. 다음섹션으로이동하여장치에리소스를제공할준비를합니다.

장치정책

August 12, 2022

정책을만들어 XenMobile 이장치와상호작용하는방식을구성할수있습니다. 많은정책이모든장치에공통적으로적용되지만각장치에해당운영체제와관련된일련의정책이있습니다. 따라서플랫폼간에는물론 Android 장치제조업체사이에서도차이가있을수있습니다.

각장치정책에대한요약설명은이문서의장치정책요약을참조하십시오.

> 참고:
>
> 환경에 GPO(그룹정책개체) 가구성되어있는경우:
>
> Windows 10 및 Windows 11 용 XenMobile 장치정책을구성할때다음규칙을고려하십시오. 하나이상의등록된장치에서정책이충돌하는경우 GPO 와일치하는정책이우선합니다.

Android Enterprise 컨테이너가지원하는정책은 Android Enterprise를참조하십시오.

사전요구사항

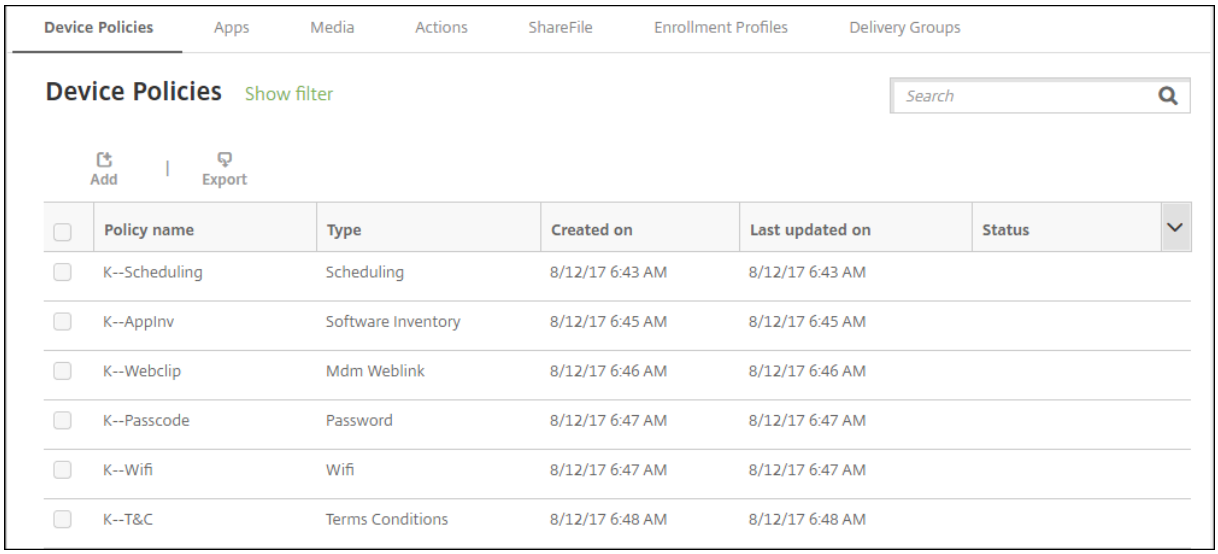
- 사용하려는배달그룹을만듭니다.
- 필요한모든 CA 인증서를설치합니다.

장치정책추가

장치정책을만드는기본단계는다음과같습니다.

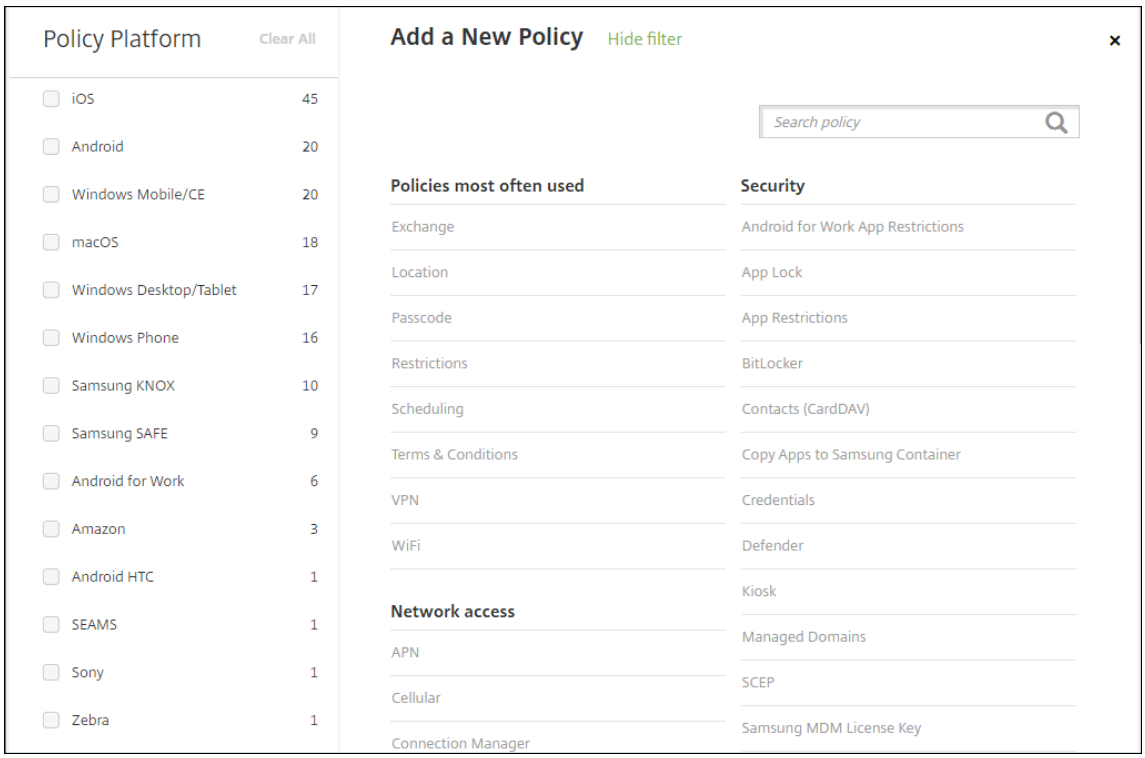
1. 정책의이름을지정하고관련설명을입력합니다.
2. 하나이상의플랫폼에대한정책을구성합니다.
3. 배포규칙을만듭니다 (선택사항).
4. 배달그룹에정책을할당합니다.
5. 배포일정을구성합니다 (선택사항).

장치정책을만들고관리하려면 구성 **>** 장치정책으로이동합니다.

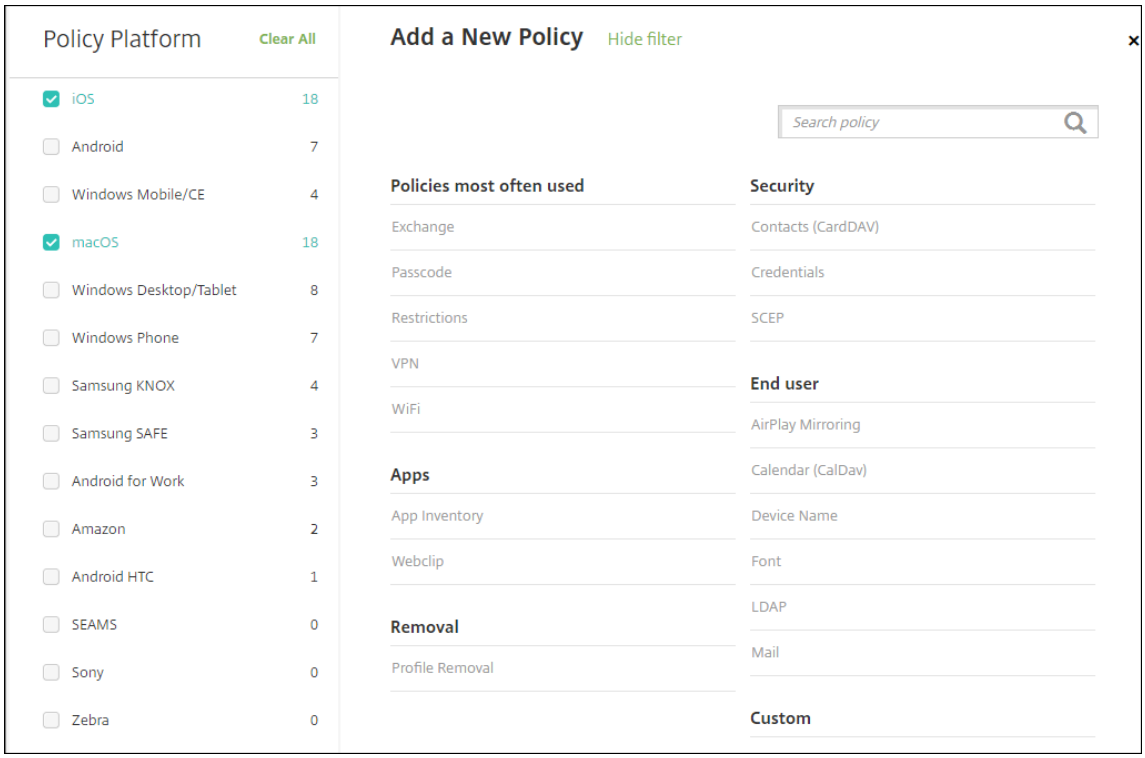


정책을추가하려면:

1. 장치정책페이지에서 추가를클릭합니다. 새정책추가페이지가나타납니다.



2. 하나이상의플랫폼을클릭하여선택한플랫폼에대한장치정책목록을봅니다. 정책추가를계속하려면정책이름을클릭합니다.



검색상자에정책이름을입력할수도있습니다. 입력할때잠재적검색결과가나타납니다. 목록에해당정책이있으면정책을클릭합니다. 선택한정책만결과에유지됩니다. 해당정책을클릭하여정책에대한 정책정보페이지를엽니다.

3. 정책에포함할플랫폼을선택합니다. 5 단계에서선택한플랫폼에대한구성페이지가나타납니다.
4. 정책정보페이지를작성한후 다음을클릭합니다. 정책정보페이지에서는정책을식별하고추적하는데도움이되는정책이름과 같은정보를수집합니다. 이페이지는모든정책에대해유사합니다.
5. 플랫폼페이지를작성합니다. 3 단계에서선택한각플랫폼에대해플랫폼페이지에나타납니다. 이러한페이지는각정책에따라 다릅니다. 정책은플랫폼마다차이가있을수있습니다. 모든정책이모든플랫폼에적용되는것은아닙니다.

   일부페이지에는항목표가포함되어있습니다. 기존의항목을삭제하려면목록이포함된줄위로마우스포인터를이동한후오른쪽의휴지통아이콘을클릭합니다. 확인대화상자에서 삭제를클릭합니다.

   기존의항목을편집하려면목록이포함된줄위로마우스포인터를이동한후오른쪽의펜아이콘을클릭합니다.

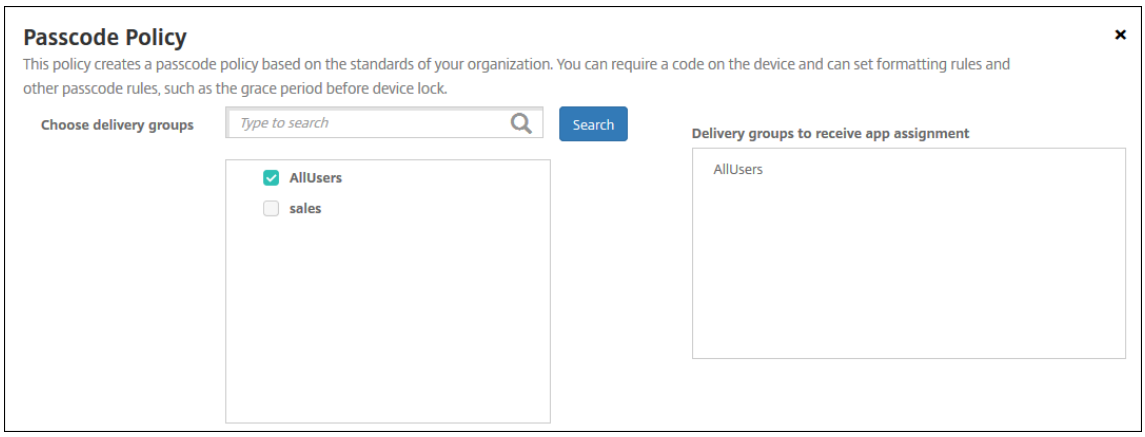
배포규칙, 할당및일정을구성하려면

배포규칙을구성하는방법에대한자세한내용은 리소스배포를참조하십시오.

1. 플랫폼페이지에서 배포규칙을확장하고다음설정을구성합니다. 기본적으로 기본탭이표시됩니다.
   - 목록에서어떤경우에정책을배포할지지정하는옵션을클릭합니다. 모든조건이충족된경우또는조건중하나라도충족된경우정책을배포하도록선택할수있습니다. 기본옵션은 모두입니다.
   - 조건을정의하려면 새규칙을클릭합니다.
   - 목록에서 장치소유권및 **BYOD** 와같은조건을클릭합니다.
   - 조건을더추가하려면 새규칙을다시클릭합니다. 원하는만큼많은조건을추가할수있습니다.
2. 고급탭을클릭하여규칙을부울옵션과결합합니다. 기본탭에서선택한조건이표시됩니다.
3. 추가고급부울논리를사용하여규칙을결합하거나, 편집하거나, 추가할수있습니다.
   - 그리고, 또는이나 아님을클릭합니다.
   - 목록에서규칙에추가할조건을선택합니다. 그런다음오른쪽의더하기기호 (**+**) 를클릭하여규칙에조건을추가합니다.

     언제든지조건을클릭하여선택한다음 편집을클릭하여조건을변경하거나 삭제를클릭하여조건을제거할수있습니다.
   - 새규칙을클릭하여다른조건을추가합니다.
4. 다음을클릭하여다음플랫폼페이지로이동하거나, 모든플랫폼페이지가완료된경우 할당페이지로이동합니다.
5. 할당페이지에서정책을적용할배달그룹을선택합니다. 배달그룹을클릭하면 앱할당을받을배달그룹상자에해당그룹이표시됩니다.

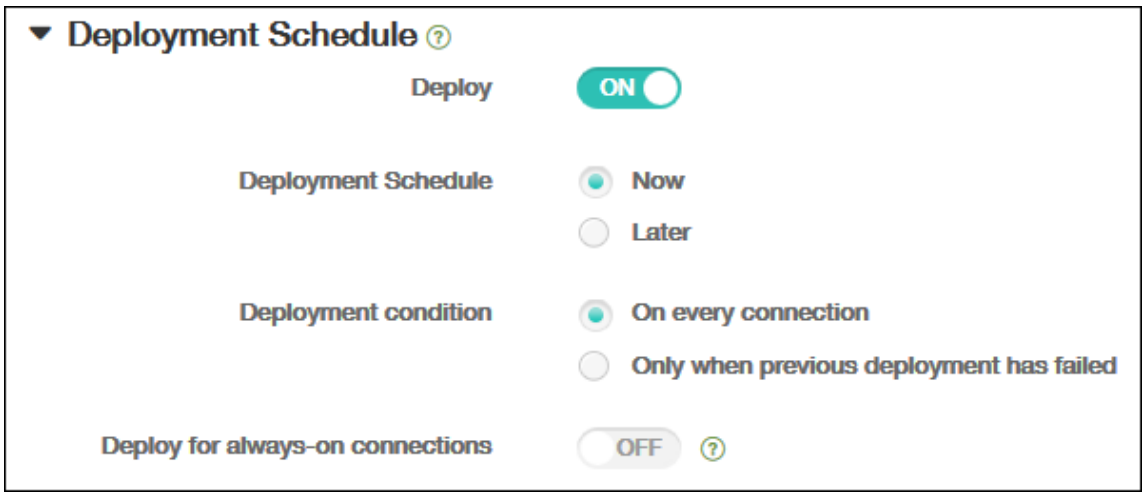
   앱할당을받을배달그룹은배달그룹을선택하기전까지표시되지않습니다.



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 장치에는상시연결옵션을사용할수없습니다.
     >
     > 구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은모든플랫폼에적용되지만 상시연결에대해배포를선택한경우 iOS 에는적용되지않습니다.



7. 저장을클릭합니다.

   장치정책테이블에정책이표시됩니다.

장치에서장치정책제거

장치에서장치정책을제거하는단계는플랫폼에따라다릅니다.

- Android

  Android 장치에서장치정책을제거하려면 XenMobile 제거장치정책을사용합니다. 자세한내용은 XenMobile 제거장치정책을참조하십시오.

- iOS 및 macOS

  iOS 또는 macOS 장치에서장치정책을제거하려면프로필제거장치정책을사용합니다. iOS 및 macOS 장치에서모든정책은 MDM 프로필의일부입니다. 따라서제거할정책에대해서만프로필제거장치정책을만들수있습니다. 나머지정책과프로필은장치에유지됩니다. 자세한내용은 프로필제거장치정책을참조하십시오.

- Windows 10 및 Windows 11

  Windows 데스크톱또는태블릿장치에서장치정책을직접제거할수는없습니다. 그러나다음방법중하나를사용할수있습니다.

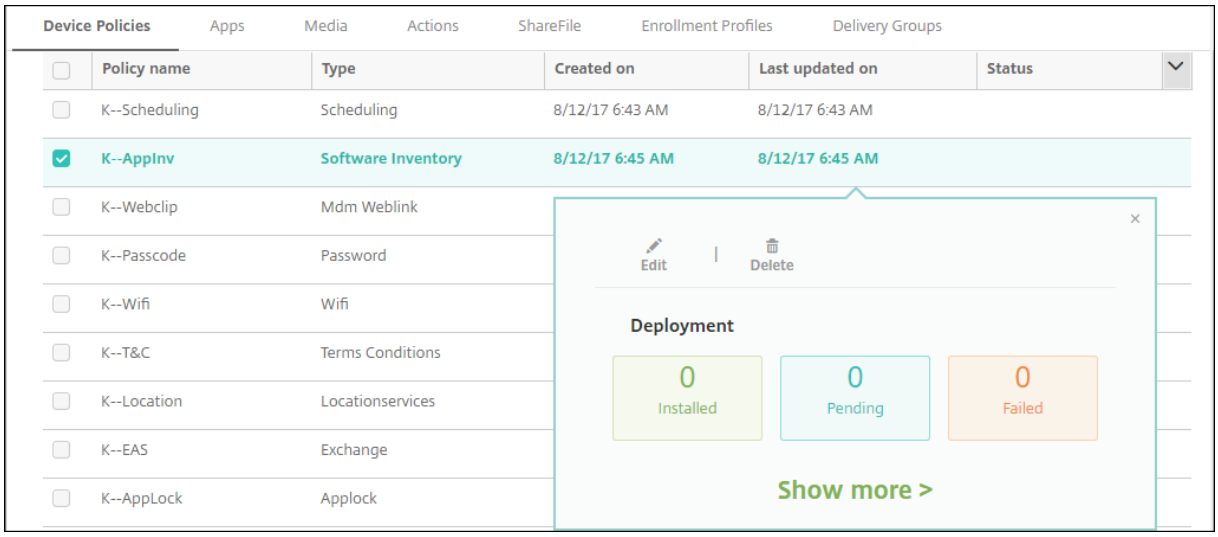
  - 장치의등록을취소한다음새정책집합을장치에푸시합니다. 그런다음사용자가재등록하여계속합니다.
  - 보안작업을푸시하여특정장치를선택적으로초기화합니다. 이렇게하면장치에서모든회사앱및데이터가제거됩니다. 그러면해당장치만포함하는배달그룹에서장치정책을제거하고배달그룹을장치로푸시할수있습니다. 그런다음사용자가재등록하여계속합니다.

- Chrome OS

  Chrome OS 장치에서장치정책을제거하려면해당장치만포함하는배달그룹에서장치정책을제거하면됩니다. 그런다음배달그룹을장치에푸시합니다.

장치정책편집

정책을편집하려면정책옆에있는확인란을선택하여정책목록위에옵션메뉴를표시합니다. 또는목록에서정책을클릭하여목록오른쪽에옵션메뉴를표시합니다.



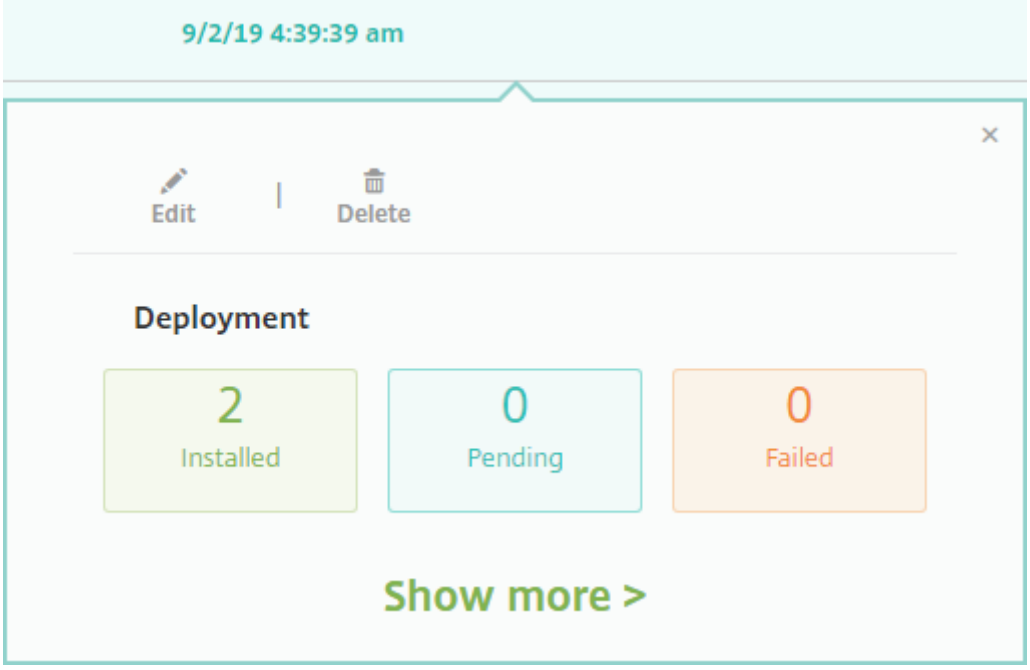
정책세부정보를보려면 자세히표시를클릭합니다.

장치정책에대한모든설정을편집하려면 편집을클릭합니다.

삭제를클릭하면확인대화상자가나타납니다. 삭제를다시클릭하여정책을삭제합니다.

정책배포상태확인

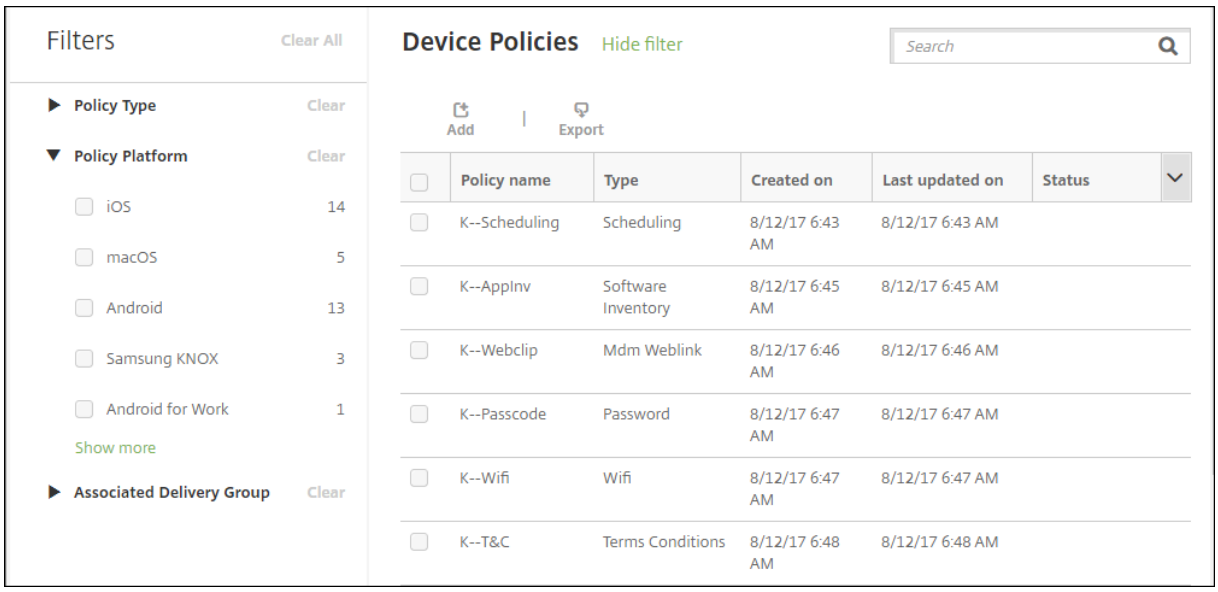
구성 **>** 장치정책페이지에서정책행을클릭하여배포상태를확인합니다.



정책배포가보류중인경우사용자는 기본설정 **>** 장치정보 **>** 정책새로고침을눌러 Secure Hub 에서정책을새로고칠수있습니다.

추가된장치정책목록필터링

추가된정책목록을정책유형, 플랫폼및관련배달그룹으로필터링할수있습니다. 구성 **>** 장치정책페이지에서 필터표시를클릭합니다. 목록에서보려는항목의확인란을선택합니다.



필터를저장하려면 이보기저장을클릭합니다. 그러면해당필터이름이 이보기저장단추아래의단추에표시됩니다.

장치정책요약

장치정책이름	장치정책설명
AirPlay 미러링	특정 AirPlay 장치 (예: 다른 Mac 컴퓨터) 를 iOS 장치에 추가합니다. 감독되는장치의허용목록에장치를추가하는옵션도있습니다. 이옵션은사용자를허용목록의 AirPlay 장치로 만제한합니다.
AirPrint	iOS 장치의 AirPrint 프린터목록에 AirPrint 프린터를추가합니다. 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. 이설정은대부분의최신휴대폰에이미정의되어있습니다. 조직이모바일장치에서인터넷에연결하는데소비자 APN 을사용하지않는경우이정책을사용합니다.

장치정책이름	장치정책설명
앱액세스	장치의필수앱, 선택적앱또는차단앱목록을정의합니다. 그런 다음자동화된동작을만들어장치가앱목록을따르는데대응할 수있습니다.
앱특성	iOS 장치에대한관리되는앱번들 ID 또는앱별 VPN 식별자와같은특성을지정합니다.
앱구성	관리되는구성을지원하는앱의다양한설정및동작을원격으로 구성합니다. 이렇게하려면 iOS 장치에 XML 구성파일 (속성 목록또는 plist) 을배포합니다. 또는 Windows 10 휴대전화, Windows 10 또는 Windows 11 을실행하는데스크톱, 태블릿장치에키/값쌍을배포합니다.
앱인벤토리	관리되는장치에서앱의인벤토리를수집합니다. 그러면 XenMobile 이해당장치에배포된앱액세스정책과인벤토리를비교합니다. 이런방식으로앱액세스허용또는차단목록에있는앱을감지하고적절한조치를수행할수있습니다.
앱잠금	사용자가 iOS 또는특정 Android 장치에서실행할수있거나 실행할수없는앱의목록을정의합니다.
앱네트워크사용	iOS 장치에서관리되는앱이셀룰러데이터네트워크와같은네트워크를사용하는방식을지정하는네트워크사용규칙을설정합니다. 이러한규칙은관리되는앱에만적용됩니다. 관리되는앱은 XenMobile 을통해사용자장치에배포되는앱입니다.
앱제한	사용자가 Samsung KNOX 장치에설치할수없도록방지할 앱에대한차단목록을만듭니다. 또한사용자가설치할수있는앱에대한허용목록을만들수있습니다.
앱제거	사용자장치에서앱을제거합니다.
앱제거제한	사용자가제거할수있는앱과제거할수없는앱을지정합니다.
앱알림	iOS 사용자가지정된앱의알림을수신하는방법을제어합니다.
관리되는앱자동업데이트	Android Enterprise 장치에서설치되어있는관리되는앱이업데이트되는방식을제어합니다.
BitLocker	Windows 10 및 Windows 11 장치의 BitLocker 인터페이스에서사용할수있는설정을구성합니다.
브라우저	사용자장치가브라우저를사용할수있는지여부또는장치가사용할수있는브라우저기능을정의합니다.

장치정책이름	장치정책설명
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 KNOX 컨테이너로복사합니다. KNOX 컨테이너에복사된앱은사용자가 KNOX 컨테이너에로그인하는경우에만사용할수있습니다.
자격증명	XenMobile 의 PKI 구성에대한통합된인증을수행할수있습니다. 예를들어 PKI 엔터티, 키저장소, 자격증명공급자또는서버인증서에대한인증이가능합니다.
사용자지정 XML	장치프로비전, 장치기능사용, 장치구성및장애관리같은기능을최적화합니다.
Defender	Windows 10 및 Windows 11 데스크톱과태블릿의 Windows Defender 설정을구성합니다.
장치상태증명	Windows 10 및 Windows 11 장치가해당상태를보고하도록합니다. 이를위해장치에서특정데이터및런타임정보를분석을위해 HAS(상태증명서비스) 로전송합니다. HAS 에서상태증명인증서를생성하고반환하면장치가이를 XenMobile 에보냅니다. XenMobile 은상태증명인증서를받은후인증서의내용에따라이전에구성된자동동작을배포할수있습니다.
장치이름	장치를식별할수있도록 iOS 와 macOS 장치에이름을설정합니다. 매크로, 텍스트또는둘의조합을사용하여장치이름을정의할수있습니다.
교육구성	Apple 교육을사용할강사및학생장치를구성합니다. 강사가 Classroom 앱을사용하는경우교육구성장치정책이필요합니다.

장치정책이름	장치정책설명
Exchange	장치의기본전자메일클라이언트에서 ActiveSync 전자메일을사용하도록설정합니다.
Files	사용자에대한특정기능을수행하는스크립트파일을 XenMobile 에추가합니다. 또는 Android 장치사용자가장치에서액세스할수있는문서파일을추가할수있습니다. 파일을추가하는경우장치에서파일이저장될디렉터리를지정할수도있습니다.
FileVault	이정책을사용하면등록된 macOS 장치에서 FileVault 장치암호화를사용하도록설정할수있습니다. 사용자가로그인할 때 FileVault 설정을건너뛸수있는횟수를제어할수도있습니다. macOS 10.7 이상에서사용할수있습니다.
방화벽	방화벽설정을구성합니다. 장치에서허용하거나차단할 IP 주소, 포트및호스트이름을지정합니다. 또한프록시및프록시경로조정설정을구성할수있습니다.
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.
Keyguard 관리	장치 Keyguard 와 Work Challenge Keyguard 의잠금을해제하기전에사용자에게제공되는기능을제어합니다. 완전관리형전용장치에대한장치 Keyguard 기능도제어할수있습니다. 예를들어지문잠금해제, 신뢰할수있는에이전트, 알림과같은잠금화면기능을비활성화할수있습니다.
키오스크	Samsung SAFE 장치에서앱사용을제한합니다. 사용가능한앱을하나이상의특정앱으로제한할수있습니다. 이정책은특정유형또는클래스의앱만실행하도록마련된회사장치에유용합니다. 또한이정책을사용하면키오스크모드의장치홈화면및잠금화면배경에대한사용자지정이미지를선택할수있습니다.

장치정책이름	장치정책설명
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 가설정된경우지도에서장치의위치를찾을수있습니다. 장치에이정책을배포한후 XenMobile Server 에서찾기명령을보낼수있습니다. 그러면장치가해당위치좌표를사용하여응답합니다. 또한 XenMobile 은지오펜스및추적정책을지원합니다.
메일	iOS 또는 macOS 장치에대한전자메일계정을구성합니다.
관리되는도메인	전자메일및 Safari 브라우저에적용되는관리되는도메인을정의합니다. 관리되는도메인을사용하면 Safari 를사용하여도메인에서다운로드한문서를열수있는앱을제어함으로써회사데이터를보호할수있습니다. iOS 8 이상의감독되는장치의경우 URL 또는하위도메인을지정하여사용자가브라우저에서문서, 첨부파일및다운로드를열수있는방법을제어할수있습니다.
MDM 옵션	감독되는 iOS 7.0 이상의전화장치에서내전화찾기및 iPad 활성화잠금을관리합니다.
조직정보	XenMobile 이 iOS 장치에배포하는알림메시지에대한조직정보를지정합니다.
암호	관리되는장치에 PIN 코드또는암호를적용합니다. 장치서암호복잡성과시간초과를설정할수있습니다.
개인핫스폿	사용자가 WiFi 네트워크범위내에없는경우인터넷에연결할 수있습니다. 사용자는개인핫스폿기능을사용하여 iOS 장치에서셀룰러데이터연결을통해연결합니다.
프로필제거	사용자의 iOS 또는 macOS 장치에서앱프로필을제거합니다.

장치정책이름	장치정책설명
프로비전프로필	장치에보낼엔터프라이즈배포프로비전프로필을지정합니다. iOS 엔터프라이즈앱을개발하고코드서명하는경우일반적으로프로비전프로필을포함합니다. Apple iOS 장치에서앱을실행하려면이프로필이필요합니다. 프로비전프로필이누락되었거나만료된경우사용자가앱을눌러서열때앱의작동이중단됩니다.
프로비전프로필제거	iOS 프로비전프로필을제거합니다.
프록시	iOS 를실행하는장치에대한글로벌 HTTP 프록시설정을지정합니다. 장치당하나의글로벌 HTTP 프록시정책만배포할수있습니다.
원격지원	Samsung KNOX 장치에원격으로액세스할수있습니다. 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.
제한사항	관리되는장치의기능을잠그고제어하기위한수백개의옵션을제공합니다. 제한옵션의예로는카메라또는마이크를사용하지않도록설정, 로밍규칙적용, 앱스토어를비롯한타사서비스에대한액세스적용등이있습니다.
로밍	iOS 장치에서음성및데이터로밍을허용할것인지여부를구성합니다. 음성로밍을사용하지않도록설정하면데이터로밍이자동으로비활성화됩니다.
Samsung MDM 라이센스키	SAFE 정책및제한사항을배포하기전에장치에배포해야하는기본제공 Samsung ELM(엔터프라이즈라이센스관리) 키를지정합니다. XenMobile 은 Samsung E-FOTA(Enterprise Firmware-Over-The-Air) 서비스도지원합니다. XenMobile 은 SAFE(Samsung for Enterprise) 와 Samsung KNOX 정책을모두지원하고확장합니다.
예약	MDM 관리, 앱푸시및정책배포를위해 Android 장치에서 XenMobile Server 에다시연결하는데필요합니다. 이정책을장치에보내지않고 Google FCM 을사용하도록설정하지않을경우장치에서서버에다시연결할수없습니다.
SCEP	외부 SCEP 서버에서인증서를검색하도록 iOS 및 macOS 장치를구성합니다. 또한 XenMobile 에연결되어있는 PKI 의 SCEP 를사용하여장치에인증서를제공할수있습니다. 이를위해분산모드에서 PKI 엔터티와 PKI 공급자를만듭니다.

장치정책이름	장치정책설명
SSO 계정	사용자가 XenMobile 과회사내부리소스에액세스하기위해 한번만로그온하도록 SSO(Single Sign-On) 계정을만듭니다. 사용자가장치에자격증명을저장할필요가없습니다. XenMobile 은 App Store 의앱을포함한앱전반의 SSO 계정에엔터프라이즈사용자자격증명을사용합니다. 이정책은 Kerberos 인증과호환됩니다. iOS 에서사용할수있습니다.
스토리지암호화	내부및외부스토리지를암호화합니다. 일부장치의경우이정책으로인해사용자가해당장치에서스토리지카드를사용하지못하게됩니다.
구독중인일정	iOS 장치의캘린더목록에구독일정을추가합니다. 사용자장치의구독일정목록에추가하기전에일정을구독해야합니다.
약관	사용자가회사네트워크에대한연결을제어하는특정회사정책에동의하도록요구합니다. 사용자가 XenMobile 에장치를등록할때약관에동의해야만장치를등록할수있습니다. 약관에동의하지않으면등록프로세스가취소됩니다.
터널	원격지원에만사용됩니다. 원격지원을사용하면지원센터담당자가관리되는 Windows CE 및 Android 모바일장치를원격으로제어할수있습니다. 원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다. 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.
VPN	레거시 VPN 게이트웨이기술을사용하는백엔드시스템에대한액세스를제공합니다. 이정책은장치에배포할수있는 VPN 게이트웨이연결세부정보를제공합니다. XenMobile 은 Cisco AnyConnect, Juniper, Citrix VPN 을비롯한여러 VPN 공급자를지원합니다. VPN 게이트웨이가이옵션을지원하는경우이정책을 CA 에연결하고주문형 VPN 을사용하도록설정할수있습니다.
배경화면	iOS 장치잠금화면, 홈화면또는둘다에배경화면을설정하기위해.png 또는.jpg 파일을추가합니다. iPad 및 iPhone 에서서로다른배경화면을사용하려면서로다른배경화면정책을만들어해당사용자에게배포합니다.
웹콘텐츠필터	iOS 장치에서웹콘텐츠를필터링합니다. XenMobile 은 Apple 자동필터기능과허용및차단목록에추가된사이트를사용합니다. 감독되는 iOS 장치에서만사용할수있습니다.

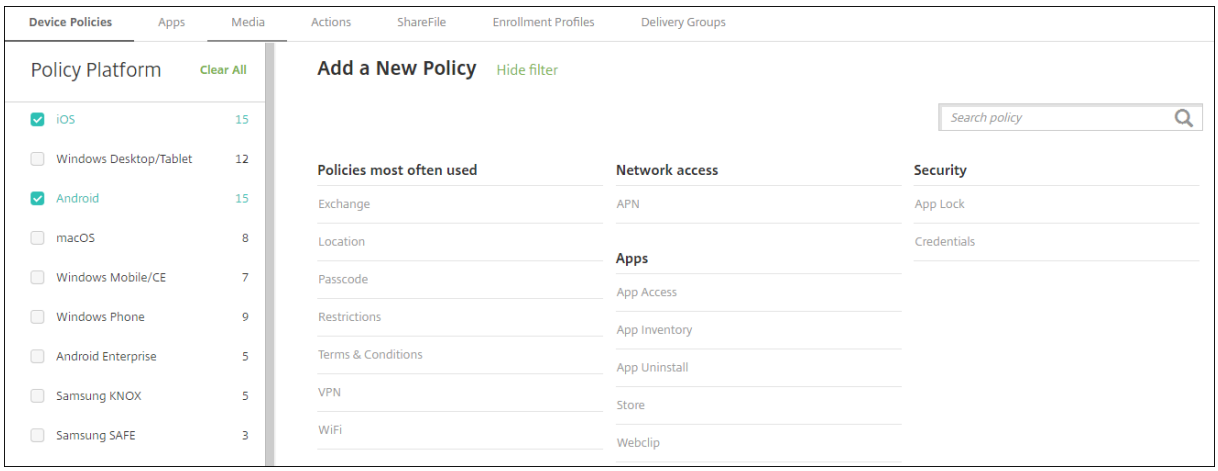
장치정책이름	장치정책설명
웹클립	웹사이트에대한바로가기또는웹클립을배치하여앱과나란히사용자장치에표시합니다. iOS, macOS X 및 Android 장치의웹클립을나타내는사용자지정아이콘을지정할수있습니다. Windows 태블릿에는레이블과 URL 만필요합니다.
WiFi	관리자가관리되는장치에 WiFi 라우터세부정보를배포할수있습니다. 라우터세부정보에는 SSID, 인증데이터및구성데이터가포함됩니다.
Windows Information Protection	정책에대해설정한적용수준에서 Windows Information Protection 이필요한앱을지정합니다. 이정책은감독되는 Windows 10 및 Windows 11 장치에대한것입니다.
XenMobile Store	XenMobile Store 웹클립을사용자장치의홈화면에표시할지여부를지정합니다.
XenMobile 옵션	Android 장치에서 XenMobile 에연결할때 Secure Hub 동작을구성합니다.
XenMobile 제거	Android 및 Windows Mobile/CE 장치에서 XenMobile 을제거합니다. 이정책을배포하면배포그룹에있는모든장치에서 XenMobile 이제거됩니다.

플랫폼별장치정책

August 12, 2022

플랫폼별로사용가능한정책을보려면:

1. XenMobile 콘솔에서 구성 **>** 장치정책으로이동합니다.
2. 추가를클릭합니다.
3. 정책플랫폼창의목록에각장치플랫폼이나타납니다. 해당창이열리지않으면 필터표시를클릭합니다.
4. 단일플랫폼에사용할수있는모든정책목록을보려면해당플랫폼을선택합니다. 여러플랫폼에사용할수있는정책목록을보려면각플랫폼을선택합니다. 정책은선택한각플랫폼에적용되는경우에만목록에나타납니다.



XenMobile 의최신릴리스는다음과같은플랫폼에대한장치정책을지원합니다.

- Amazon
- Android
- Android Enterprise
- Android Zebra
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Windows 10 및 Windows 11 데스크탑/태블릿

XenMobile 의최신릴리스에서지원되는장치에대한자세한내용은 지원되는장치플랫폼을참조하십시오.

> 참고:
>
> 환경에 GPO(그룹정책개체) 가구성되어있는경우:
>
> Windows 10 및 Windows 11 용 XenMobile 장치정책을구성할때다음규칙을고려하십시오. 하나이상의등록된장치에서정책이충돌하는경우 GPO 와일치하는정책이우선합니다.

AirPlay 미러링장치정책

January 5, 2022

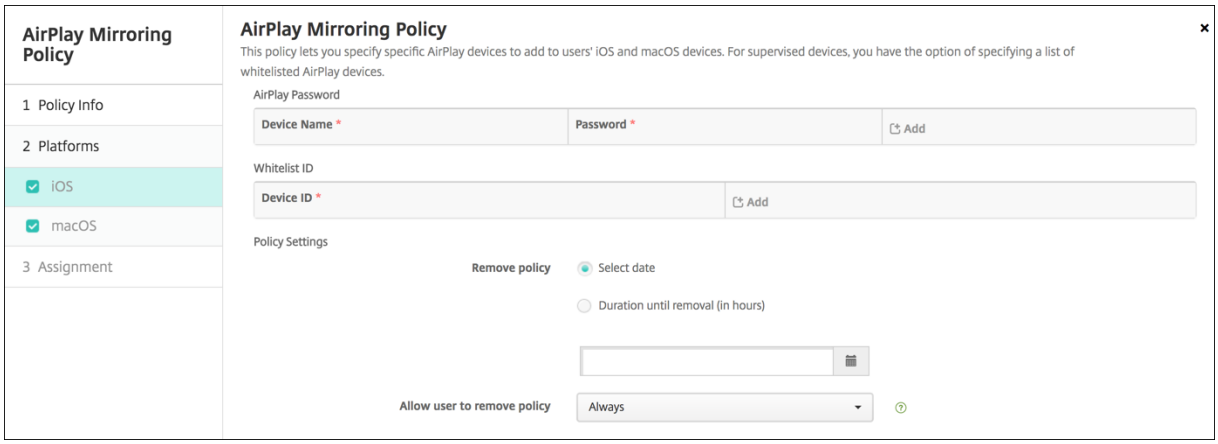
Apple AirPlay 기능을사용하면장치디스플레이의내용을다른 Mac 컴퓨터로정확하게미러링할수있습니다.

XenMobile 에서특정 AirPlay 장치 (예: 다른 Mac 컴퓨터) 를 iOS 장치에추가하는장치정책을추가할수있습니다. 또한감독되는장치의경우허용목록에장치를추가할수있습니다. 그러면허용목록에있는 AirPlay 장치로만사용자가제한됩니다. 장치를감독모드로전환하는방법에대한자세한내용은 Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.

> 참고:
>
> 계속하기전에추가할모든장치에대한장치 ID 와암호가있는지확인하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

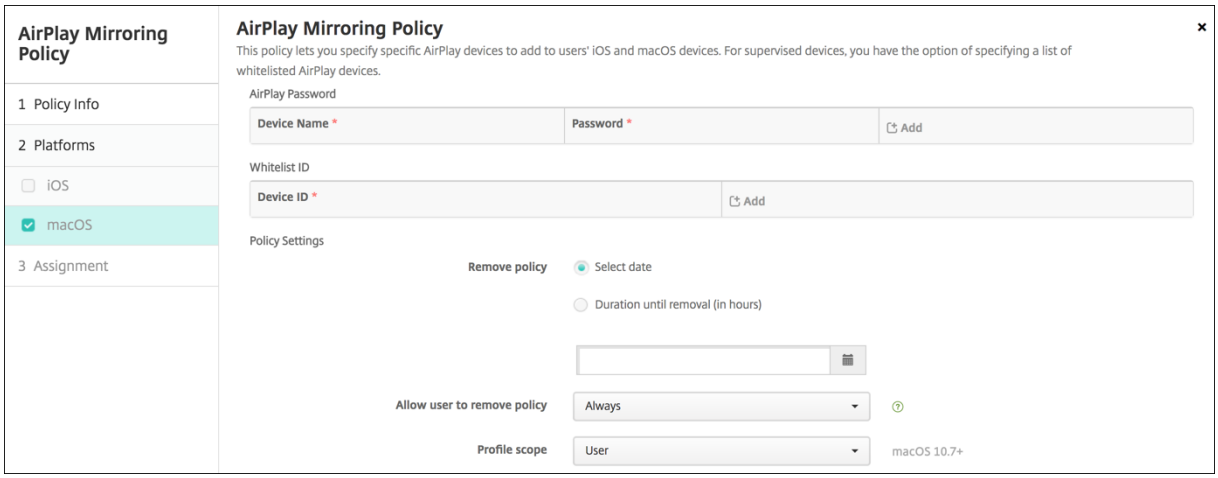


- **AirPlay** 암호**:** 추가할각장치에대해 추가를클릭하고다음을수행합니다.
  - 장치 **ID:** 하드웨어주소 (Mac 주소) 를 xx:xx:xx:xx:xx:xx 형식으로입력합니다. 이필드는대/소문자를구분하지않습니다.
  - 암호**:** 장치에대한선택적암호를입력합니다.
  - 추가를클릭하여장치를추가하거나 취소를클릭하여장치추가를취소합니다.
- 화이트리스트 **ID:** 감독되지않는장치의경우이목록이무시됩니다. 이목록의장치 ID 는사용자장치에제공되는유일한 AirPlay 장치입니다. 목록에추가할각 AirPlay 장치에대해 추가를클릭하고다음을수행합니다.

  > 참고**:**
  >
  > XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는용어가포함됩니다. 향후릴리스에서이러한용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.

  - 장치 **ID:** 장치 ID 를 xx:xx:xx:xx:xx:xx 형식으로입력합니다. 이필드는대/소문자를구분하지않습니다.
  - 추가를클릭하여장치를추가하거나 취소를클릭하여장치추가를취소합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.

macOS 설정



- **AirPlay** 암호**:** 추가할각장치에대해 추가를클릭하고다음을수행합니다.
  - 장치 **ID:** 하드웨어주소 (Mac 주소) 를 xx:xx:xx:xx:xx:xx 형식으로입력합니다. 이필드는대/소문자를구분하지않습니다.
  - 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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

AirPrint 장치정책

January 5, 2022

XenMobile 에서장치정책을추가하여 AirPrint 프린터를 iOS 장치에있는 AirPrint 프린터목록에추가할수있습니다. 이정책을사용하면프린터와장치가서로다른서브넷에있는환경을보다쉽게지원할수있습니다.

이정책은 iOS 7.0 이상에적용됩니다.

> 참고:
>
> 각프린터의 IP 주소와리소스경로를알고있는지확인하십시오.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- **AirPrint** 대상: 추가하려는각 AirPrint 대상에대해 추가를클릭한후다음을수행합니다.
  - **IP** 주소: AirPrint 프린터 IP 주소를입력합니다.
  - 리소스경로: 프린터와연결된리소스경로를입력합니다. 이값은 _ipps.tcp Bonjour 레코드의매개변수에해당합니다. 예를들어 printers/Canon_MG5300_series 또는 printers/Xerox_Phaser_7600 과같습니다.
  - 저장을클릭하여프린터를추가하거나 취소를클릭하여프린터추가를취소합니다.
- 정책설정
  - 정책제거: 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 (시간) 입니다.
    - 날짜선택: 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 (시간): 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

Android Enterprise 앱권한

January 5, 2022

작업프로필내의 Android Enterprise 앱에대한요청에서 Google 이 "위험한" 권한이라고하는권한을처리하는방법을구성할수있습니다. 앱의권한요청에대한부여또는거부를확인하는메시지를사용자에게표시할지여부를제어할수있습니다. 이기능은 Android 7.0 이상을실행하는장치에적용됩니다.

Google 에서위험한권한이란사용자의개인정보와관련되거나사용자의저장된데이터또는다른앱의작동에영향을미칠수있는데이터또는리소스에대한액세스권한을앱에제공하는권한을뜻합니다. 예를들어사용자의연락처를읽을수있는권한은위험한권한입니다.

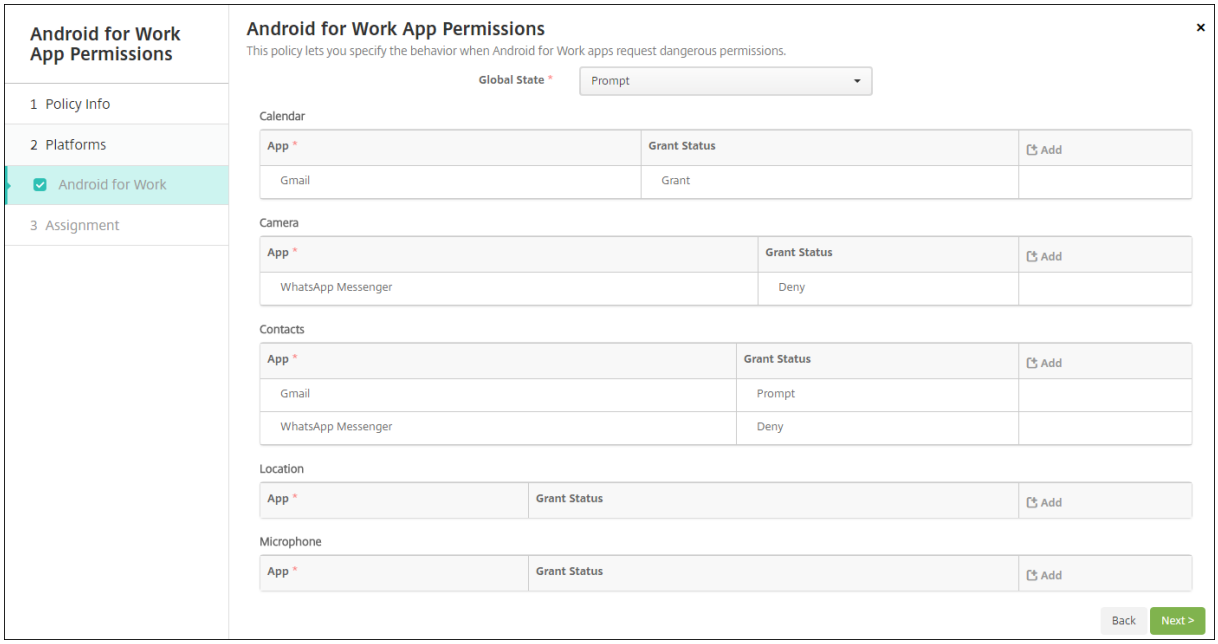
작업프로필안에있는 Android Enterprise 앱에대한모든위험한권한요청의동작을제어하는글로벌상태를구성할수있습니다. 또한 Google 이정의한대로개별권한그룹에대한위험한권한요청의동작을각앱에대해제어할수있습니다. 이러한개별설정은글로벌상태를재정의합니다.

Google 이권한그룹을정의하는방법에대한자세한내용은이 Android 개발자가이드에서 "권한그룹" 을참조하십시오.

기본적으로위험한권한요청을부여하거나거부하라는메시지가사용자에게표시됩니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Android Enterprise 설정



- 글로벌상태**:** 모든위험한권한요청의동작을제어합니다. 목록에서 프롬프트, 부여또는 거부를클릭합니다.
  - 프롬프트**:** 위험한권한요청을부여하거나거부하라는메시지가사용자에게표시됩니다.
  - 부여**:** 모든위험한권한요청이부여됩니다. 사용자에게메시지가표시되지않습니다.
  - 거부**:** 모든위험한권한요청이거부됩니다. 사용자에게메시지가표시되지않습니다.

  기본값은 프롬프트입니다.
- 각앱의각권한그룹에대한개별동작을설정합니다. 권한그룹의동작을구성하려면: 추가를클릭하고 앱에서목록의앱을선택합니다. Android Enterprise 시스템앱을구성하는경우 새로추가를클릭하고제한장치정책에서사용하도록설정한응용프로그램패키지이름을입력합니다. 부여상태에서 프롬프트, 부여또는 거부를선택합니다. 이부여상태는글로벌상태를재정의합니다.
  - 프롬프트**:** 이앱의이권한그룹에서위험한권한요청을부여하거나거부하라는메시지가사용자에게표시됩니다.
  - 부여**:** 이앱의이권한그룹에서위험한권한요청이부여됩니다. 사용자에게메시지가표시되지않습니다.
  - 거부**:** 이앱의이권한그룹에서위험한권한요청이거부됩니다. 사용자에게메시지가표시되지않습니다.

  기본값은 프롬프트입니다.
- 앱및부여상태옆의 저장을클릭합니다.
- 권한그룹의앱을추가하려면 추가를다시클릭하고이단계를반복합니다.
- 모든권한그룹에대한부여상태설정이완료되면 다음을클릭합니다.

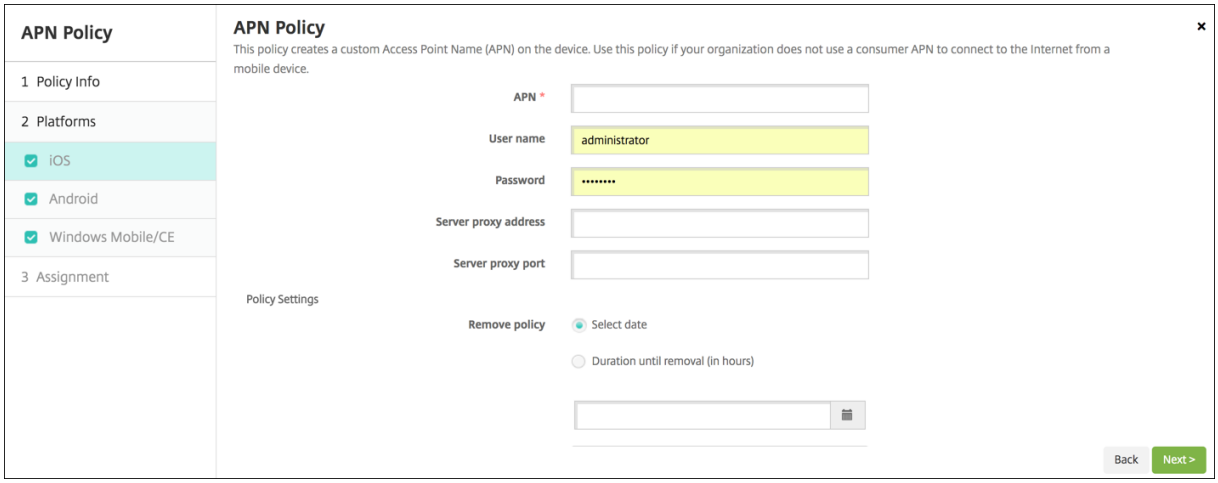
APN 장치정책

August 12, 2022

iOS 및 Android 장치에대한사용자지정 APN(액세스포인트이름) 장치정책을추가할수있습니다. 조직에서모바일장치로부터인터넷에연결하는데소비자 APN 을사용하지않을경우이정책을사용하십시오. APN 정책은특정이동통신사업자의 GPRS(General Packet Radio Service) 에장치를연결하는데사용되는설정을결정합니다. 이설정은대부분의최신휴대폰에이미정의되어있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

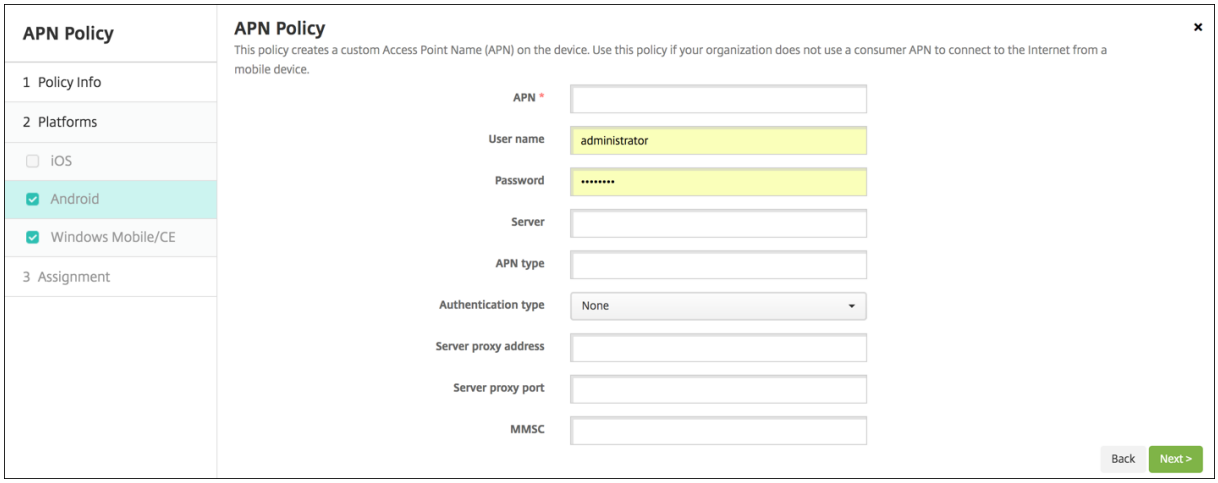
iOS 설정



- **APN:** 액세스지점의이름을입력합니다. 이이름은허용된 iOS APN 과일치해야합니다. 그렇지않으면정책이실패합니다.
- 사용자이름**:** 이문자열은이 APN 의사용자이름을지정합니다. 사용자이름이누락된경우프로필설치중에문자열을입력하라는메시지가표시됩니다.
- 암호**:** 이 APN 에대한사용자의암호입니다. 쉽게알수없도록암호는암호화됩니다. 암호가페이로드에서누락된경우프로필설치중에암호를묻는메시지가표시됩니다.
- 서버프록시주소**:** APN 프록시의 IP 주소또는 URL 입니다.
- 서버프록시포트**:** APN 프록시의포트번호입니다. 서버프록시주소를입력한경우포트가필수입니다.
- 정책설정의 정책제거옆에서 날짜선택또는 제거할때까지의기간 **(**시간**)** 을클릭합니다.
  - 날짜선택을클릭하는경우달력을클릭하여제거할날짜를선택합니다.
  - 사용자가정책을제거하도록허용목록에서 항상, 암호필요또는 안함을클릭합니다.
  - 암호필요를클릭하는경우 제거암호옆에필요한암호를입력합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.

* 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

Android 설정



- **APN:** 액세스지점의이름을입력합니다. 이이름은허용된 Android APN 과일치해야합니다. 그렇지않으면정책이실패합니다.
- 사용자이름**:** 이문자열은이 APN 의사용자이름을지정합니다. 사용자이름이누락된경우프로필설치중에문자열을입력하라는메시지가표시됩니다.
- 암호**:** 이 APN 에대한사용자의암호입니다. 쉽게알수없도록암호는암호화됩니다. 암호가페이로드에서누락된경우프로필설치중에암호를묻는메시지가표시됩니다.
- 서버**:** 스마트폰을대상으로하는이설정은대개비어있습니다. 표준웹사이트에액세스하거나렌더링수없는휴대폰의경우 WAP(Wireless Application Protocol) 게이트웨이서버를참조합니다.
- **APN** 유형**:** 이설정은액세스지점에대한이동통신사업자의의도된용도와일치해야합니다. 이것은쉼표로구분된 APN 서비스지정자문자열이며이동통신사업자의공표된정의와일치해야합니다. 다음예를참조하십시오.
  - *. 모든트래픽은이액세스지점을통과합니다.
  - mms. 멀티미디어트래픽은이액세스지점을통과합니다.
  - default. 멀티미디어를비롯한모든트래픽은이액세스지점을통과합니다.
  - supl. SUPL(Secure User Plane Location) 은보조 GPS(A-GPS) 와연결됩니다.
  - dun. 전화접속네트워킹은시대에뒤떨어져거의사용되지않습니다.
  - hipri. 우선순위가높은네트워킹입니다.
  - fota. FOTA(Firmware Over The Air) 는펌웨어업데이트를수신하는데사용됩니다.
- 인증유형**:** 목록에서사용할인증유형을클릭합니다. 기본값은없음입니다.
- 서버프록시주소**:** 이동통신사업자 APN HTTP 프록시의 IP 주소또는 URL 입니다.
- 서버프록시포트**:** APN 프록시의포트번호입니다. 서버프록시주소를입력한경우포트가필수입니다.
- **MMSC:** 이동통신사업자가제공한 MMS 게이트웨이서버주소입니다.
- **MMS(**멀티미디어메시징서버**)** 프록시주소**:** MMS 트래픽을위한멀티미디어메시징서비스서버입니다. MMS 는 SMS 의후신으로, 사진이나비디오와같은멀티미디어콘텐츠가포함된더큰메시지를보낼수있습니다. 이러한서버에는특정프로토콜

(예: MM1, … MM11).

- **MMS** 포트**:** MMS 프록시에사용되는포트입니다.

앱액세스장치정책

August 12, 2022

XenMobile 의앱액세스장치정책을사용하면장치에설치해야하거나, 장치에설치할수있거나, 장치에설치해서는안되는앱의목록을정의할수있습니다. 그런다음자동화된동작을만들어장치가앱목록을따르는데대응할수있습니다. iOS 및 Android 장치에대한앱액세스정책을만들수있습니다.

한번에한가지유형의액세스정책만구성할수있습니다. 필수앱, 추천앱또는금지된앱목록중하나에대한정책을추가할수있지만동일한앱액세스정책내에서목록을혼합할수는없습니다. 각유형의목록에대한정책을만드는경우 XenMobile 의정책이어떤앱목록에적용되는지알수있도록각정책의이름을신중하게지정하는것이좋습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

플랫폼설정

- 액세스정책**:** 필수, 추천또는 금지를클릭합니다. 기본값은 필수입니다.
- 하나이상의앱을목록에추가하려면 추가를클릭한후다음을수행합니다.
  - 앱이름**:** 앱이름을입력합니다.
  - 앱식별자**:** 선택적인앱식별자를입력합니다.
  - 저장또는 취소를클릭합니다.
  - 추가할각앱에대해이단계를반복합니다.

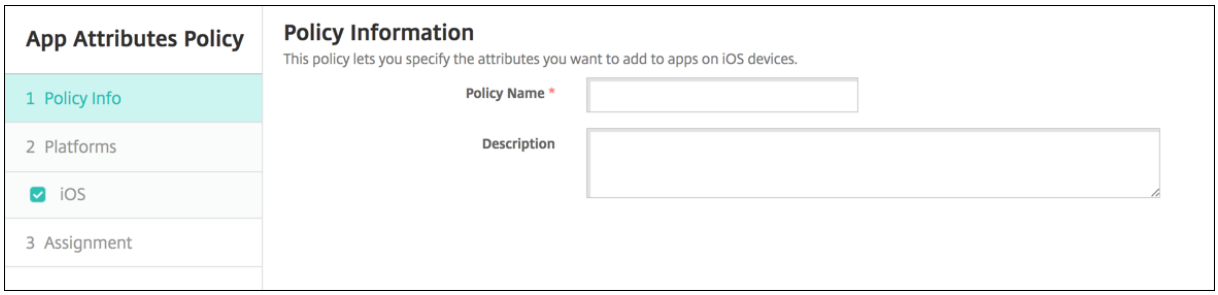
앱특성장치정책

January 5, 2022

앱특성장치정책을사용하면 iOS 장치에대한관리되는앱번들 ID 또는앱별 VPN 식별자와같은특성을지정할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



- 관리되는앱번들 **ID:** 목록에서앱번들 ID 또는 새로추가를클릭합니다.
  - 새로추가를클릭하는경우표시되는필드에앱번들 ID 를입력합니다.
- 앱별 **VPN** 식별자**:** 목록에서앱별 VPN 식별자를클릭합니다.

앱구성장치정책

August 12, 2022

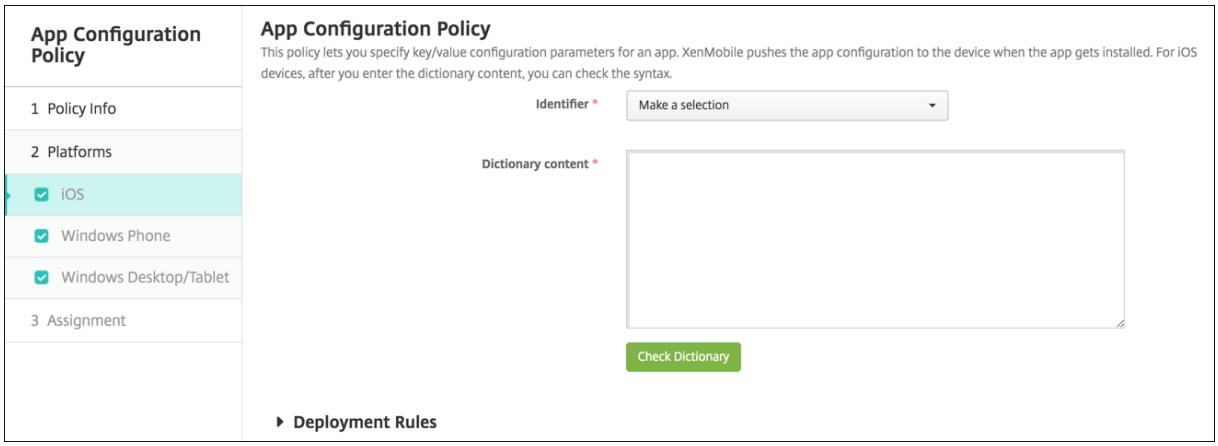
다음을배포하여관리되는구성을지원하는앱을원격으로구성할수있습니다.

- iOS 장치에 XML 구성파일 (속성목록또는 plist 라고함) 을배포합니다.
- 또는 Windows 10 전화, Windows 10 또는 Windows 11 를실행하는태블릿또는데스크톱장치에대한키/값쌍을배포합니다.

구성은앱의다양한설정및동작을지정합니다. 사용자가앱을설치하면 XenMobile 이장치로구성을푸시합니다. 구성할수있는실제설정및동작은앱에따라다르며이문서에서다루지않습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

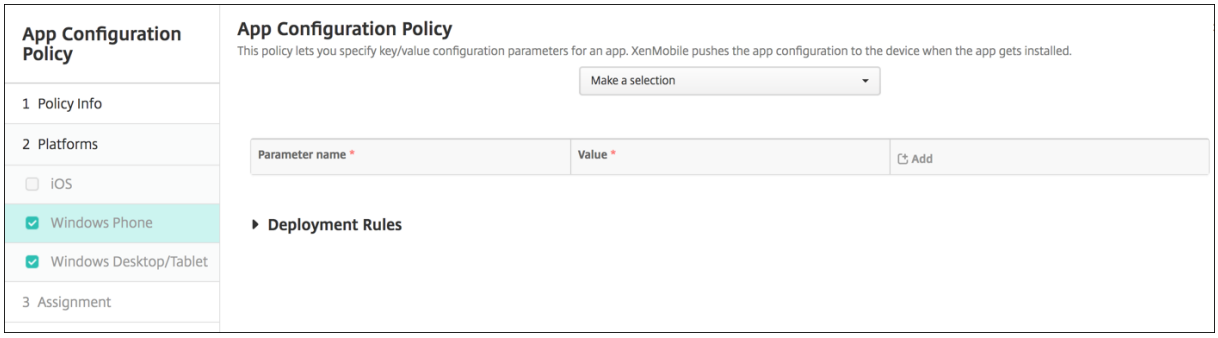
iOS 설정

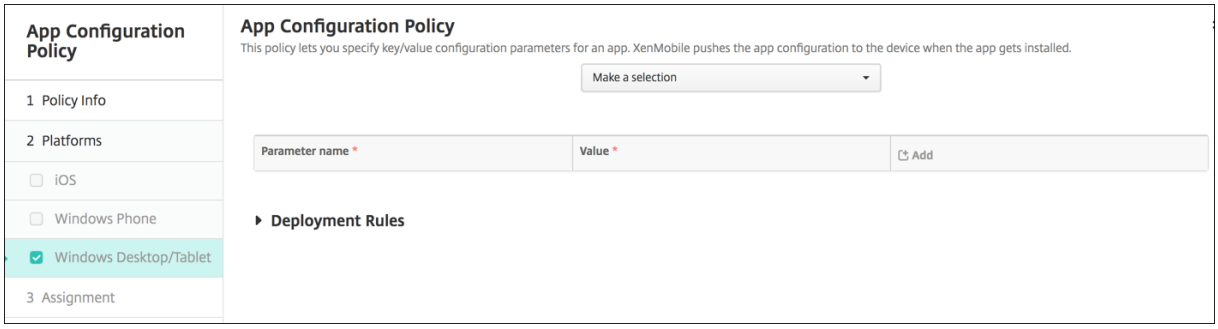


- 식별자**:** 목록에서구성할앱을클릭하거나 새로추가를클릭하여새앱을목록에추가합니다.

  - 새로추가를클릭하는경우표시되는필드에앱식별자를입력합니다.
- 사전내용**:** XML 속성목록 (plist) 구성정보를입력하거나복사하여붙여넣습니다.
- 사전확인을클릭합니다. XenMobile 이 XML 을확인합니다. 오류가없으면콘텐츠상자아래에 올바른 **XML** 이표시됩니다. 콘텐츠상자아래에구문오류가표시되면계속하기전에해당오류를수정해야합니다.

Windows 데스크톱/태블릿설정





- 선택목록에서구성할앱을클릭하거나 새로추가를클릭하여새앱을목록에추가합니다.
  - 새로추가를클릭하는경우표시되는필드에패키지제품군이름을입력합니다.
- 추가할각구성매개변수에대해 추가를클릭하고다음을수행합니다.
  - 매개변수이름**:** Windows 장치에대한응용프로그램설정의키이름을입력합니다. Windows 앱설정에대한자세한 내용은 Microsoft 설명서를참조하십시오.
  - 값**:** 지정된매개변수의값을입력합니다.
  - 추가를클릭하여매개변수를추가하거나 취소를클릭하여매개변수추가를취소합니다.

앱인벤토리장치정책

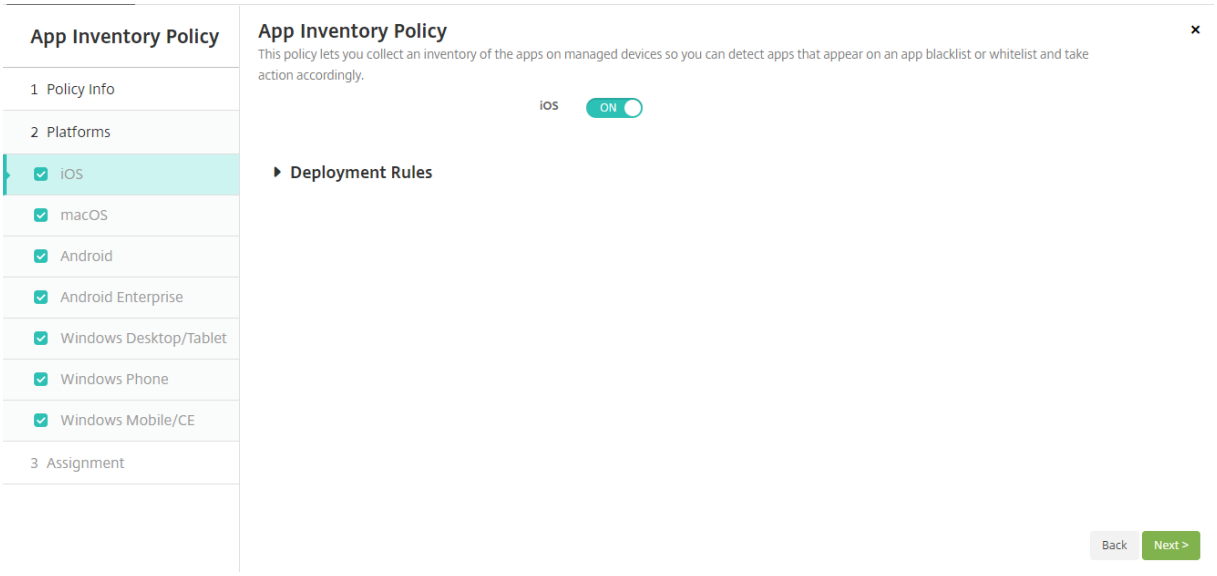
August 12, 2022

앱인벤토리정책을사용하면관리되는장치에서앱의인벤토리를수집할수있습니다. 그러면 XenMobile 이해당장치에배포된앱액세스정책과인벤토리를비교합니다. 이런방식으로앱허용또는차단목록에표시되는앱을감지하고적절한조치를수행할수있습니다.

iOS, macOS, Android, Android Enterprise 또는 Windows Desktop/Tablet 장치에대한앱액세스정책을만들수있습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

플랫폼설정



- 선택한각플랫폼에대해기본설정을그대로사용하거나설정을 꺼짐으로변경합니다. 기본값은 켜짐입니다.

앱잠금장치정책

January 5, 2022

앱잠금장치정책은장치에서실행될수있는앱목록또는장치에서실행을차단할앱목록을정의합니다. iOS 및 Android 장치에대해이정책을구성할수있지만정책이작동하는정확한방식은각플랫폼마다다릅니다. 예를들어 iOS 장치에서는여러앱을차단할수없습니다.

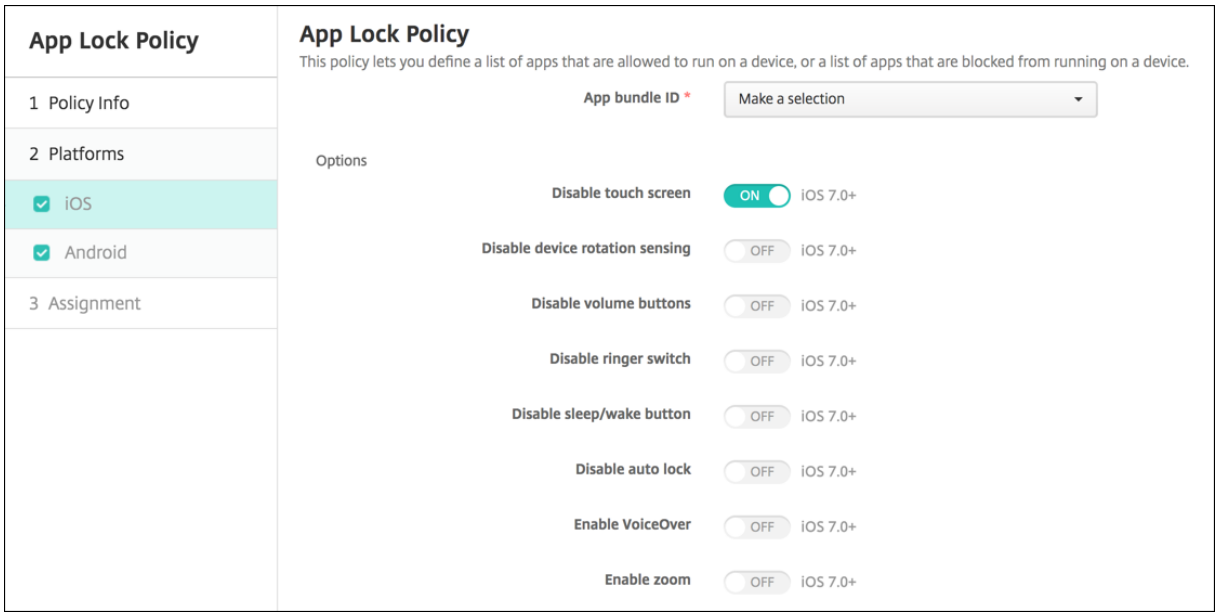
마찬가지로, iOS 장치에서는정책당하나의 iOS 앱만선택할수있습니다. 즉, 사용자는장치를사용하여하나의앱만실행할수있습니다. 앱잠금정책이시행될때관리자가구체적으로허용한옵션외의다른어떤작업도장치에서수행할수없습니다.

또한 iOS 장치에서앱잠금정책을푸시하려면장치가감독되어야합니다.

장치정책은대부분의 Android L 및 M 장치에서작동하지만앱잠금의경우필요한 API 를 Google 이더이상제공하지않기때문에 Android N 이상장치에서작동하지않습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



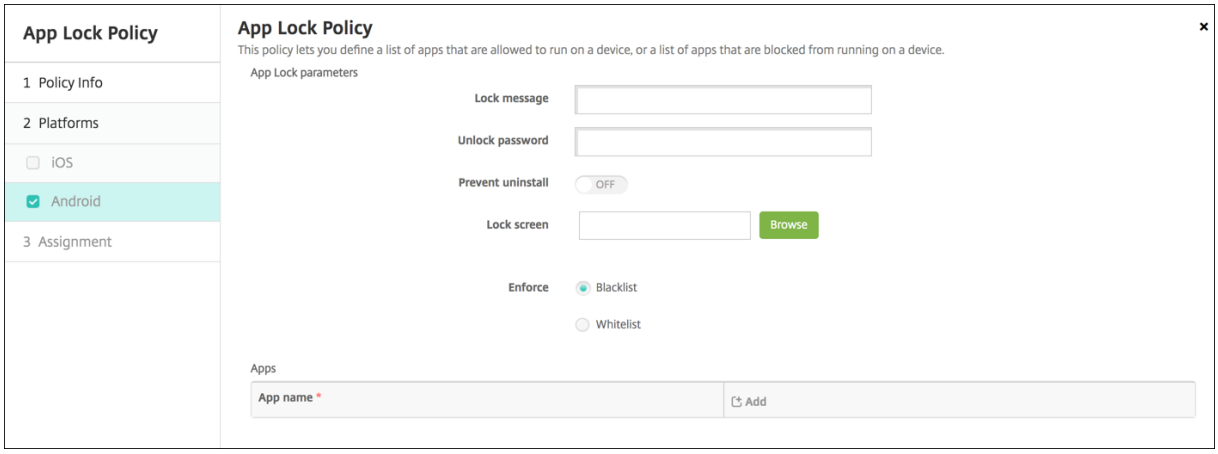
- 앱번들 **ID:** 목록에서이정책을적용할앱을클릭하거나 새로추가를클릭하여새앱을목록에추가합니다. 새로추가를선택하는 경우표시되는필드에앱이름을입력합니다.
- 옵션**:** 다음각옵션은 iOS 7.0 이상에만적용됩니다. 각옵션의기본값은 꺼짐이며터치스크린사용안함은예외적으로기본값이 켜짐입니다.
  - 터치스크린사용안함
  - 장치회전감지사용안함
  - 볼륨단추사용안함
  - 벨소리전환사용안함

    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
- 정책설정

- 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
  - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
  - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

Android 설정

> 참고**:**
>
> 앱잠금장치정책을사용하여 Android 설정앱을차단할수없습니다.



- 앱잠금매개변수
  - 잠금메시지**:** 사용자가잠긴앱을열려고할때표시할메시지를입력합니다.
  - 잠금해제암호**:** 앱잠금을해제하는암호를입력합니다.
  - 제거금지**:** 사용자가앱을제거하도록허용할지여부를선택합니다. 기본값은 꺼짐입니다.
  - 잠금화면**:** 찾아보기를클릭하고파일의위치로이동하여장치의잠금화면에표시할이미지를선택합니다.
  - 적용**:** 블랙리스트를클릭하여장치에서실행될수없는앱목록을만들거나 화이트리스트를클릭하여장치에서실행될수있는앱목록을만듭니다.

    > 참고**:**
    >
    > XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는용어가포함됩니다. 향후릴리스에서 이러한용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.
- 앱**:** 추가를클릭하고다음을수행합니다.
  - 앱이름**:** 목록에서앱이름을클릭하여허용또는차단목록에추가하거나 새로추가를클릭하여사용가능한앱목록에새앱을추가합니다.
  - 새로추가를선택하는경우표시되는필드에앱이름을입력합니다.
  - 저장또는 취소를클릭합니다.
  - 허용또는차단목록에추가할각앱에이러한단계를반복합니다.

앱네트워크사용장치정책

January 5, 2022

iOS 장치에서관리되는앱이셀룰러데이터네트워크와같은네트워크를사용하는방식을지정하는네트워크사용규칙을설정할 수있습니다. 이러한규칙은관리되는앱에만적용됩니다. 관리되는앱은 XenMobile 을통해사용자장치에배포되는앱입니다. XenMobile 을통해배포되지않고사용자가장치에직접다운로드한앱이나장치를 XenMobile 에등록할때장치에이미설치되어있던앱은여기에해당되지않습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 로밍셀룰러데이터허용**:** 지정된앱이로밍중에셀룰러데이터연결을사용할수있는지여부를선택합니다. 기본값은 꺼짐입니다.
- 셀룰러데이터허용**:** 지정된앱이셀룰러데이터연결을사용할수있는지여부를선택합니다. 기본값은 꺼짐입니다.
- 앱식별자일치**:** 목록에추가할각앱에대해 추가를클릭한후다음을수행합니다.
  - 앱식별자**:** 앱식별자를입력합니다.
  - 목록에앱을저장하려면 저장을클릭하고저장하지않으려면 취소를클릭합니다.

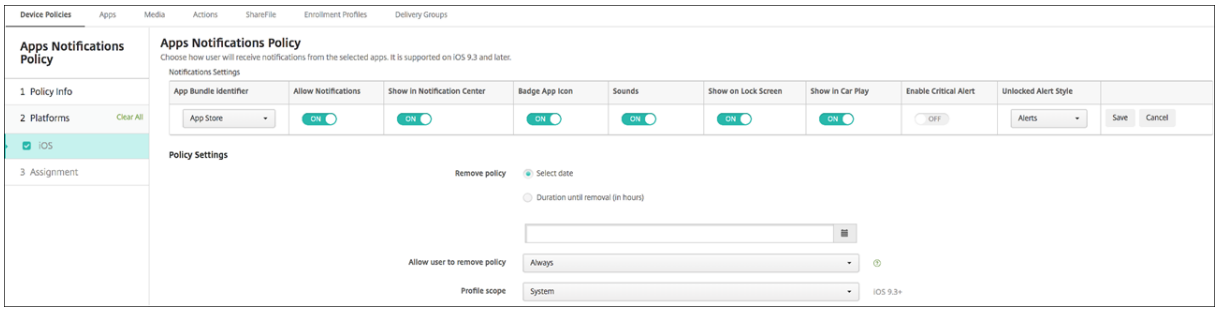
앱알림장치정책

January 5, 2022

앱알림정책을사용하여 iOS 사용자가지정된앱의알림을수신하는방법을제어할수있습니다. 이정책은 iOS 9.3 이상을실행하는장치에서지원됩니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



- 앱번들 **ID:** 이정책을적용할앱을지정합니다.

- 알림허용**:** 알림을허용하려면 켜짐을선택합니다.
- 알림센터에표시**:** 사용자장치의알림센터에알림을표시하려면 켜짐을선택합니다.
- 배지앱아이콘**:** 알림과함께배치앱아이콘을표시하려면 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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 iOS 9.3 이상에서만사용할수있습니다.

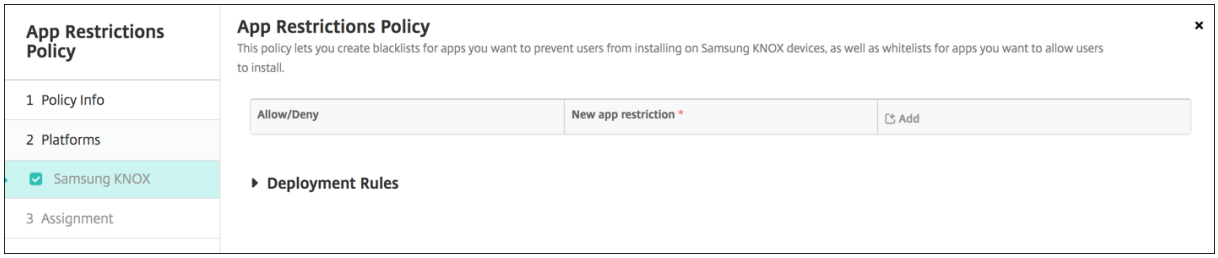
앱제한장치정책

January 5, 2022

사용자가 Samsung KNOX 장치에설치할수없도록방지할앱에대한차단목록을만들수있습니다. 또한사용자가설치할수있도록할앱에대한허용목록을만들수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Samsung KNOX 설정



허용/거부목록에추가할각앱에대해 추가를클릭하고다음을수행합니다.

- 허용/거부**:** 사용자가앱을설치하도록허용할지여부를선택합니다.
- 새앱제한**:** 앱패키지 ID 를입력합니다 (예: com.kmdm.af.crackle).
- 저장을클릭하여허용/거부목록에앱을저장하거나 취소를클릭하여허용/거부목록에앱을저장하지않습니다.

앱터널링장치정책

August 12, 2022

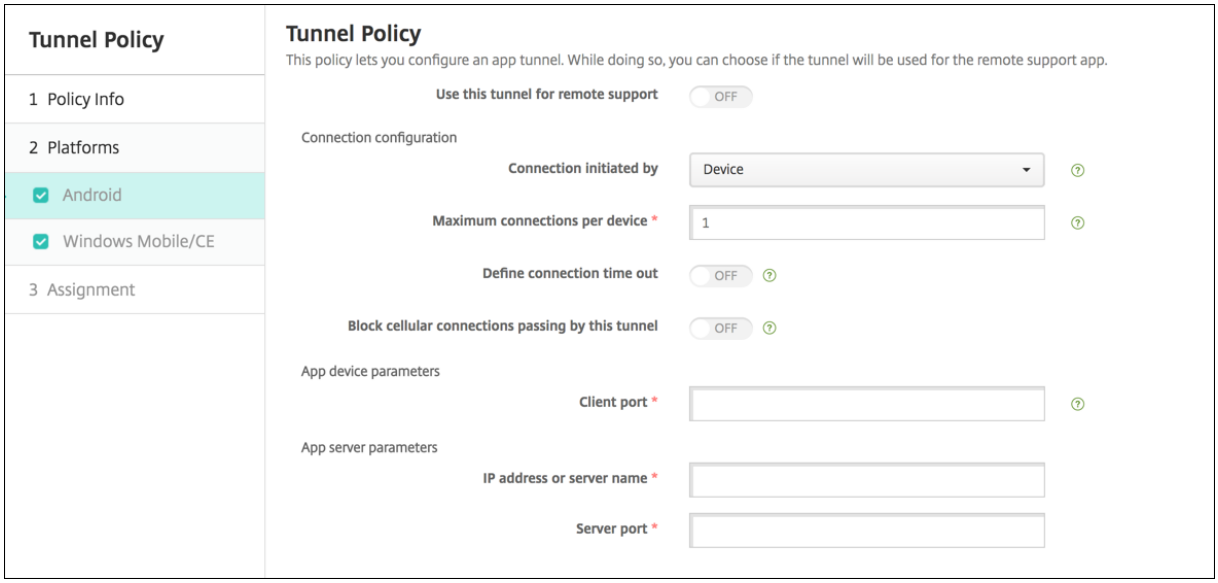
> 중요**:**
>
> 앱터널링장치정책은원격지원에만사용됩니다. 원격지원에대한자세한내용은 지원옵션및원격지원을참조하십시오. 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.

응용프로그램터널 (앱터널) 은모바일앱의무중단서비스및데이터전송안정성을개선하도록설계되었습니다. 앱터널은모든모바일장치앱의클라이언트구성요소와앱서버구성요소간의프록시매개변수를정의합니다. 또한관리지원을위해앱터널을사용하여장치에대한원격지원터널을만들수있습니다. Android 장치에대한앱터널링정책을구성할수있습니다.

이정책에서정의한터널을통해전송되는모든앱트래픽은앱을실행하는서버로리디렉션되기전에 XenMobile 을통과합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Android 설정



- 이터널을원격지원에사용**:** 원격지원에터널을사용할지여부를선택합니다.

  구성단계는원격지원을선택하는지여부에따라다릅니다.

- 원격지원을선택하지않은경우다음을수행합니다.
  - 연결을시작한원본**:** 장치또는 서버를클릭하여연결을시작하는원본을지정합니다.
  - 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.

앱제거장치정책

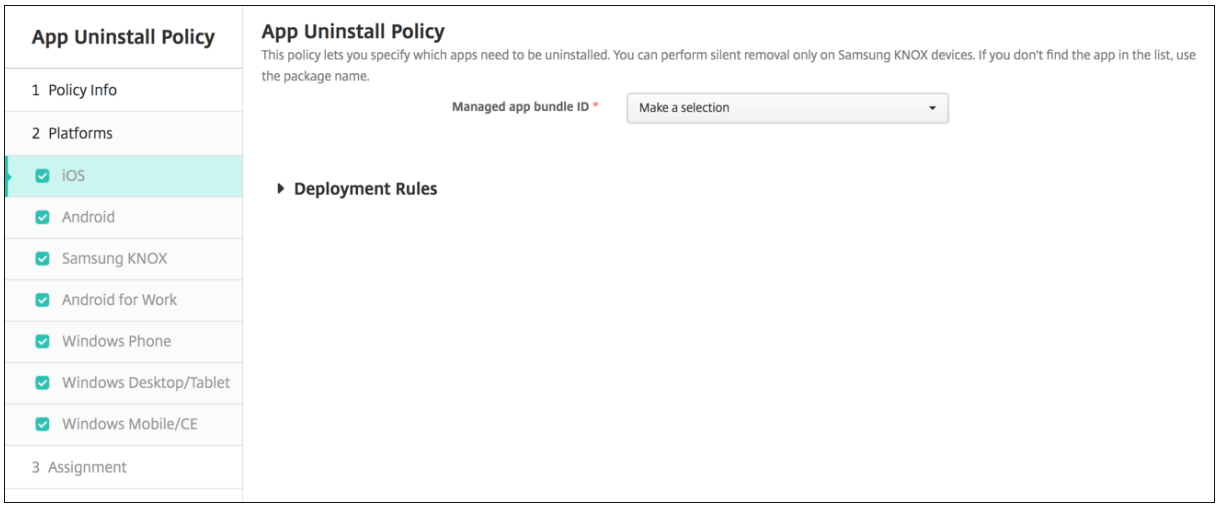
August 12, 2022

iOS, Android, Samsung KNOX, Android Enterprise 및 Windows Desktop/Tablet 플랫폼에대한앱제거정책을만들수있습니다. 앱제거정책을사용하면여러가지이유로사용자장치에서앱을제거할수있습니다. 예를들어특정앱을더이상지원하지않으려하거나회사가기존앱을다른공급업체의유사한앱으로교체하려고할수있습니다.

이정책이사용자장치에배포되면해당앱이제거됩니다. Samsung KNOX 장치를제외하고사용자에게앱을제거할것인지묻는메시지가표시됩니다. Samsung KNOX 장치사용자에게는앱을제거할것인지묻는메시지가나타나지않습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



- 관리되는앱번들 **ID:** 목록에서기존앱을클릭하거나 새로추가를클릭합니다. 이플랫폼에구성된앱이없는경우목록은비어있을것이므로새앱을추가해야합니다.
  - 추가를클릭하면앱이름을입력할수있는필드가나타납니다.

다른모든플랫폼설정

- 제거할앱**:** 추가하려는각앱에대해 추가를클릭한후다음을수행합니다.
  - 앱이름**:** 목록에서기존앱을클릭하거나 새로추가를클릭하여새앱이름을입력합니다. 이플랫폼에구성된앱이없는경우목록은비어있을것이므로새앱을추가해야합니다.
  - 추가를클릭하여앱을추가하거나 취소를클릭하여앱추가를취소합니다.

해당공용앱스토어앱을설치한후자동으로엔터프라이즈앱을제거합니다

공용앱스토어버전이설치될때 Citrix 앱의엔터프라이즈버전을제거하도록 XenMobile 을구성할수있습니다. 이기능을사용하면 공용앱스토어버전이설치된후사용자장치에두개의동일한앱아이콘이나타나는것이방지됩니다.

앱제거장치정책의배포조건은새버전설치시이전앱을사용자장치에서제거하도록 XenMobile 을트리거합니다. 이기능은 XenMobile Server 에엔터프라이즈모드 (XME) 로연결되어관리되는 iOS 장치에서만사용할수있습니다.

설치된앱이름조건을사용하여배포규칙을구성하려면:

- 엔터프라이즈앱에대한 관리되는앱번들 **ID** 를지정합니다.
- 규칙추가: 새규칙을클릭한다음샘플에표시된것과같이 설치된앱이름및 같음을선택합니다. 공용앱스토어앱의앱번들 ID 를입력합니다.

예제에서공용앱스토어앱 (com.citrix.mail.ios) 이지정된배달그룹의장치에설치될때 XenMobile 이엔터프라이즈버전 (com.citrix.mail) 을제거합니다.

앱제거제한장치정책

January 5, 2022

Samsung SAFE 또는 Amazon 장치에서사용자가제거할수있거나제거할수없는앱을지정할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Samsung SAFE 또는 **Amazon** 설정

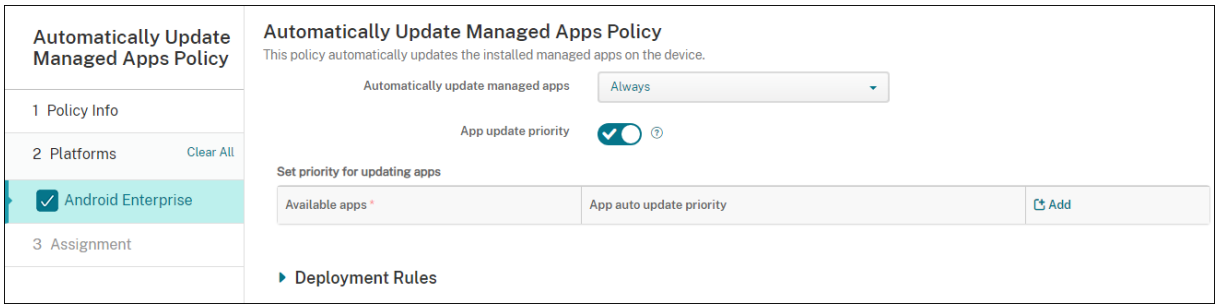
- 앱제거제한설정**:** 추가하려는각앱규칙에대해 추가를클릭한후다음을수행합니다.
  - 앱이름**:** 목록에서앱을클릭하거나 새로추가를클릭하여새앱을추가합니다.
  - 규칙**:** 사용자가앱을제거할수있는지여부를선택합니다. 기본값은설치제거를허용하는것입니다.
  - 저장또는 취소를클릭합니다.

관리되는앱자동업데이트장치정책

August 24, 2022

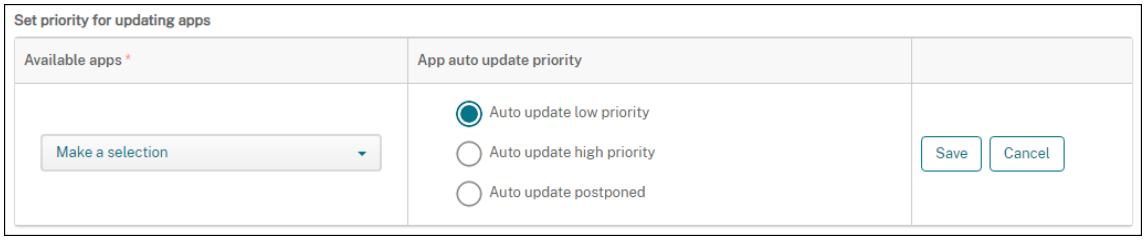
이정책은 Android Enterprise 장치에서설치되어있는관리되는앱이업데이트되는방식을제어합니다. 사용자가장치에서앱을자동업데이트하는기능을제한할수있습니다. 사용자가기기에서앱에대한자동업데이트를제어할수있도록허용할경우관리되는 Google Play 스토어에서자동앱업데이트정책을설정합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.



- 관리되는앱자동업데이트
  - 항상**:** 자동앱업데이트를활성화합니다. 항상이기본값입니다.
  - 사용자가정책을구성하도록허용**:** 사용자가관리되는 Google Play 스토어에서기기에대한자동앱업데이트정책을구성하도록허용합니다.
  - 사용안함**:** 자동앱업데이트를비활성화합니다.
  - 장치가 **Wi-Fi** 에연결된경우에만**:** 장치가 Wi-Fi 에연결된경우에만자동앱업데이트를허용합니다.
- 앱업데이트우선순위**:** 켜짐인경우각관리되는앱의업데이트우선순위수준을구성할수있습니다.

- 앱업데이트우선순위설정**:** 추가를클릭하여앱의업데이트우선순위를구성합니다.



- 사용가능한앱**:** 메뉴에서앱을선택하여업데이트우선순위를구성합니다.
- 앱자동업데이트우선순위**:** 다음에서업데이트우선순위를선택합니다.
  - 낮은우선순위자동업데이트**:** 기기가충전중이고, 활발하게사용되고있지않으며, 무제한네트워크에연결되면앱이업데이트됩니다.
  - 높은우선순위자동업데이트**:** 제한없이최대한빨리앱을업데이트합니다.
  - 자동업데이트연기됨**:** 새버전을사용할수있게된후최대 90 일동안앱이자동으로업데이트되지않습니다. 90 일이지나면앱이낮은우선순위로자동업데이트됩니다. 앱이업데이트된후 90 일동안앱이자동으로업데이트되지않습니다. 사용자는언제든지앱을수동으로업데이트할수있습니다.
- 완료되면 저장을클릭합니다. 연필아이콘을클릭하여구성을편집할수있습니다. 휴지통을클릭하여구성을삭제합니다.

BitLocker 장치정책

August 12, 2022

Windows 10 및 Windows 11 에는 BitLocker 라는디스크암호화기능이포함되어있습니다. BitLocker 는분실또는도난장치의파일및시스템에대한무단액세스를추가로보호합니다. BitLocker 를 TPM(신뢰할수있는플랫폼모듈) 칩버전 1.2 이상과함께사용하면추가보호를적용할수있습니다. TPM 칩은암호화작업을처리하고암호화키를생성및저장하고키사용을제한합니다.

Windows 10 빌드 1703 부터 MDM 정책을통해 BitLocker 를제어할수있습니다. XenMobile 에서 BitLocker 장치정책을사용하여 Windows 10 및 Windows 11 장치의 BitLocker 마법사에서제공되는설정을구성할수있습니다. 예를들어 BitLocker 가활성화된장치에서는시작시드라이브잠금을해제하는방법, 복구키를백업하는방법및고정드라이브의잠금을해제하는방법에대한메시지를사용자에게표시할수있습니다. BitLocker 장치정책설정을통해다음을구성할수도있습니다.

- TPM 칩이없는장치에서 BitLocker 를활성화할지여부
- BitLocker 인터페이스에복구옵션을표시할지여부
- BitLocker 가활성화되지않은경우고정또는이동식드라이브에대한쓰기액세스를거부할지여부

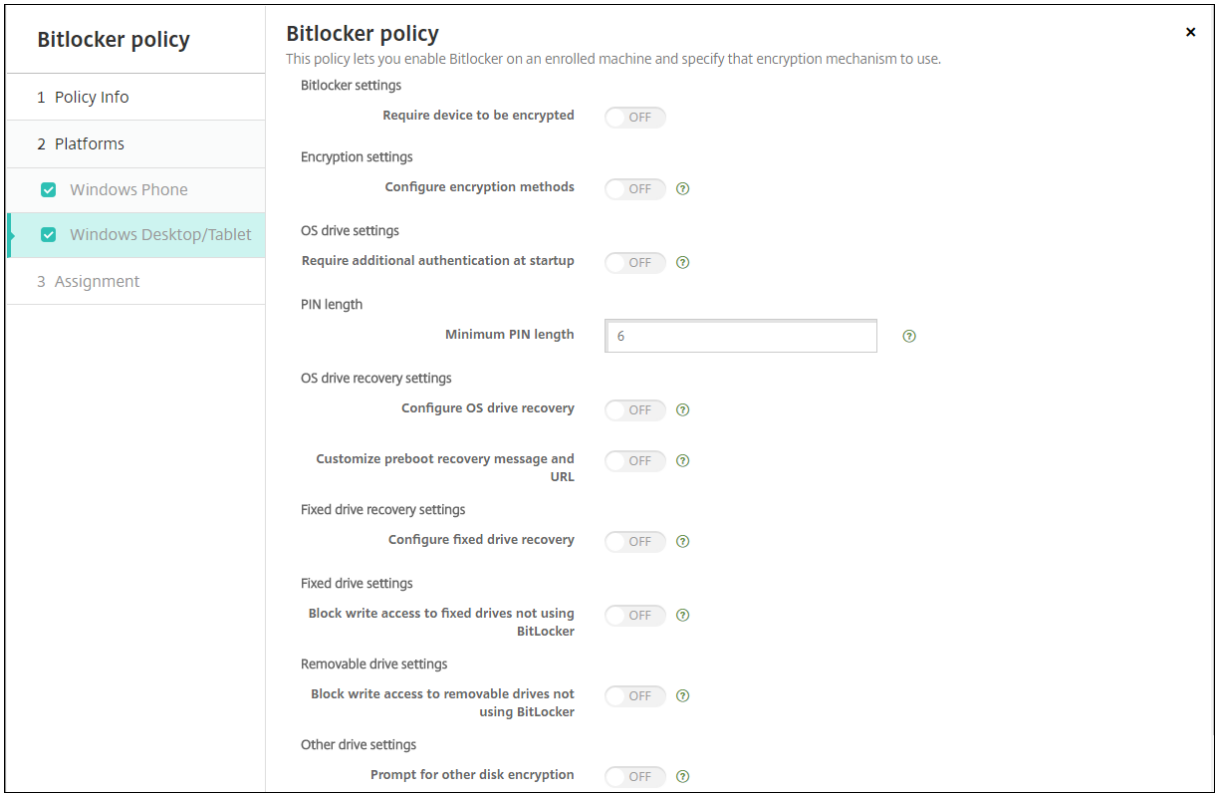
> 참고**:**
>
> 장치에서 BitLocker 암호화가시작된후에는장치에업데이트된 BitLocker 장치정책을배포하여 BitLocker 설정을변경할수없습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

요구사항

- BitLocker 장치정책을사용하려면 Windows 10 또는 Windows 11 Enterprise 버전이필요합니다.
- BitLocker 장치정책을배포하기전에 BitLocker 를사용할수있도록환경을준비하십시오. BitLocker 시스템요구사항 및설정을포함한 Microsoft 의자세한정보는 BitLocker 및해당노드아래의문서를참조하십시오.

Windows Desktop 및태블릿설정



- 장치암호화필요**:** Windows 데스크톱또는태블릿의 BitLocker 암호화사용설정에대한메시지를사용자에게표시할지여부를결정합니다. 켜짐인경우등록이완료되면장치암호화가필요함을나타내는메시지가표시됩니다. 꺼짐인경우사용자에게 메시지가표시되지않으며 BitLocker 에는정책설정이사용됩니다. 기본값은 꺼짐입니다.
- 암호화방법구성**:** 특정드라이브유형에사용할암호화방법을결정합니다. 꺼짐인경우 BitLocker 마법사에드라이브유형에사용할암호화방법을선택하라는메시지가표시됩니다. 모든드라이브의암호화방법은기본적으로 XTS-AES 128 비트입니다. 이동식드라이브의암호화방법은기본적으로 AES-CBC 128 비트입니다. 켜짐인경우정책에지정된암호화방법이 BitLocker 에사용됩니다. 켜짐인경우 운영체제드라이브, 고정드라이브및 이동식드라이브의추가설정이나타납니다. 각 드라이브유형에대해기본암호화방법을선택합니다. 기본값은 꺼짐입니다.
- 시작시추가인증필요**:** 장치시작시추가로필요한인증을지정합니다. TPM 칩이없는장치에서 BitLocker 를허용할지여부도지정합니다. 꺼짐인경우 TPM 이없는장치에서 BitLocker 암호화를사용할수없습니다. TPM 에대한자세한내용은 Microsoft 문서 TPM(신뢰할수있는플랫폼모듈) 기술개요를참조하십시오. 켜짐인경우다음추가설정이나타납니다. 기본값은 꺼짐입니다.

- **TPM** 칩이없는장치에서 **BitLocker** 차단**:** TPM 칩이없는장치에서 BitLocker 를사용하려면잠금해제암호또는시작키를생성해야합니다. 시작키는 USB 드라이브에저장되며사용자는시작전에 USB 드라이브를장치에연결해야합니다. 잠금해제암호는 8 자이상입니다. 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 Group Policy settings(BitLocker 그룹정책설정)를참조하십시오. 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.

- 사전부팅복구메시지및 **URL** 사용자지정**:** 복구화면에 BitLocker 의사용자지정된메시지및 URL 을표시할지여부를지정합니다. 켜짐인경우 기본복구메시지및 **URL** 사용, 빈복구메시지및 **URL** 사용, 사용자지정복구메시지사용및 사용자지정복구 **URL** 사용의추가설정이나타납니다. 꺼짐인경우기본복구메시지및 URL 이표시됩니다. 기본값은 꺼짐입니다.
- 고정드라이브복구구성**:** BitLocker 로암호화된고정드라이브에대한사용자복구옵션을구성합니다. BitLocker 는고정드라이브암호화에대한메시지를사용자에게표시하지않습니다. 시작시드라이브잠금을해제하려면사용자가암호또는스마트카드를제공해야합니다. 사용자가고정드라이브의 BitLocker 암호화를사용하도록설정한경우이정책에포함되지않은시작잠금해제설정이 BitLocker 인터페이스에표시됩니다. 관련설정에대한자세한내용은이목록의앞부분에있는 **OS** 드라이브복구구성을참조하십시오. 기본값은 꺼짐입니다.
- **BitLocker** 를사용하지않는고정드라이브에대한쓰기액세스차단**:** 켜짐인경우 BitLocker 로암호화된고정드라이브에만쓰기작업을수행할수있습니다. 기본값은 꺼짐입니다.
- **BitLocker** 를사용하지않는이동식드라이브에대한쓰기액세스차단**:** 켜짐인경우 BitLocker 로암호화된이동식드라이브에만쓰기작업을수행할수있습니다. 이설정은조직에서다른이동식드라이브에대한쓰기액세스를허용하는지여부에따라구성하십시오. 기본값은 꺼짐입니다.
- 다른디스크암호화인경우메시지표시**:** 장치의다른디스크암호화에대한경고메시지를표시하지않도록설정할수있습니다. 기본값은 꺼짐입니다.

브라우저장치정책

January 5, 2022

Samsung SAFE 또는 Samsung KNOX 장치에대한브라우저장치정책을만들어사용자장치에서브라우저를사용할수있는지여부를정의하거나장치에서사용할수있는브라우저기능을제한할수있습니다.

Samsung 장치에서브라우저를완전히사용하지않도록설정하거나팝업, JavaScript, 쿠키, 자동채우기및부정행위경고시행을사용하거나사용하지않도록설정할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Samsung SAFE 및 **Samsung KNOX** 설정

- 브라우저사용안함**:** 사용자의장치에서 Samsung 브라우저를완전히사용하지않을지여부를선택합니다. 기본값은 꺼짐이고사용자가브라우저를사용할수있습니다. 브라우저를사용하지않도록설정하면다음옵션이사라집니다.
- 팝업사용안함**:** 브라우저에서팝업메시지를허용할지여부를선택합니다.
- **Javascript** 사용안함**:** 브라우저에서 JavaScript 실행을허용할지여부를선택합니다.
- 쿠키사용안함**:** 쿠키를허용할지여부를선택합니다.

- 자동채우기사용안함**:** 사용자가브라우저의자동채우기기능을켜는것을허용할지여부를선택합니다.
- 부정행위경고시행**:** 사용자가사기를목적으로하는웹사이트또는손상된웹사이트를방문할때경고를표시할지여부를선택합니다.

캘린더 **(CalDav)** 장치정책

January 5, 2022

XenMobile 에서사용자의 iOS 또는 macOS 장치에캘린더 (CalDAV) 계정을추가하는장치정책을추가할수있습니다. 이정책을사용하면해당사용자가 CalDAV 를지원하는모든서버와일정데이터를동기화할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

셀룰러장치정책

January 5, 2022

이정책을사용하면 iOS 장치에대한셀룰러네트워크설정을구성할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

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(액세스포인트이름) 구성의이름입니다.
  - 인증유형**:** 목록에서 **CHAP** 또는 **PAP** 를클릭합니다. 기본값은 **PAP** 입니다.
  - 사용자이름및 암호**:** 인증에사용할사용자이름과암호입니다.
  - 프록시서버**:** 프록시서버네트워크주소입니다.
  - 프록시서버포트**:** 프록시서버포트입니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.

* 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

연결예약장치정책

February 2, 2022

> 중요**:**
>
> FCM(Firebase Cloud Messaging) 을사용하여 Android, Android Enterprise 및 Chrome OS 장치의 XenMobile Server 연결을제어하는것이좋습니다. FCM 사용에대한자세한내용은 Firebase Cloud Messaging을참조하십시오.

FCM 을사용하지않도록선택한경우연결예약정책을만들어사용자장치에서 XenMobile Server 에연결하는방법과시기를제어할수있습니다.

사용자가수동으로장치에연결하거나장치가정의된시간내에연결하도록지정할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

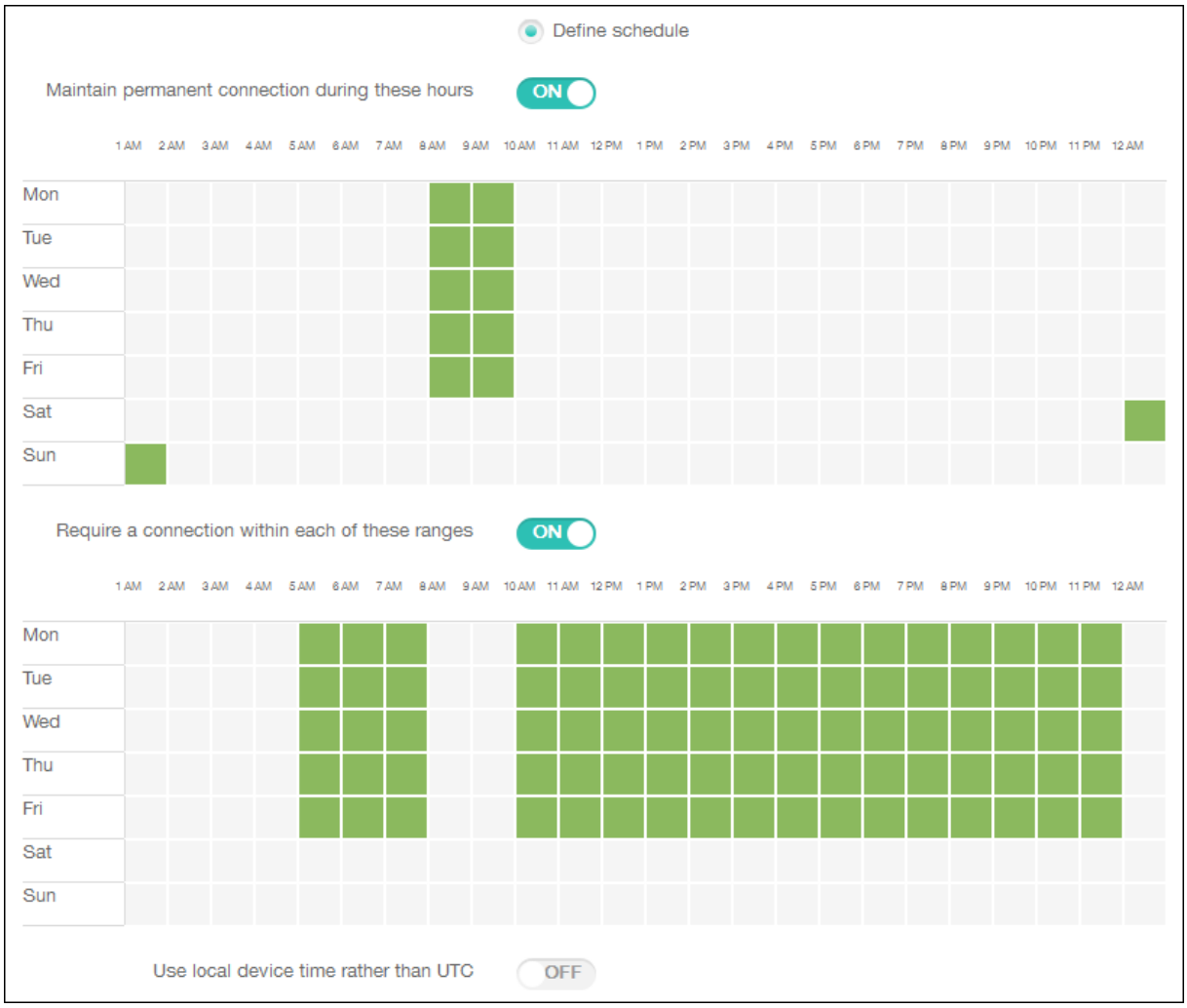
플랫폼설정

- 장치에서연결하도록요구**:** 이일정에대해설정할옵션을클릭합니다.
  - 항상**:** 연결을영구적으로활성상태로유지합니다. 네트워크연결이끊긴후사용자장치의 XenMobile 이 XenMobile 서버에다시연결을시도하고제어패킷을정기적으로전송하여연결을모니터링합니다. 보안을최적화하려면이옵션을사용하는것이좋습니다. 항상을선택하는경우장치 터널정책인 연결시간제한정의설정을사용하여연결로인해배터리가소진되지않도록하십시오. 연결을활성상태로유지하면초기화또는잠금과같은보안명령을주문형으로장치에푸시할수있습니다. 또한장치에배포하는각정책에서 배포일정옵션 상시연결에대해배포를선택해야합니다.
  - 안함**:** 수동으로연결합니다. 사용자가장치의 XenMobile 에서연결을시작해야합니다. 이옵션을사용하면보안정책을장치에배포할수없어사용자가새앱또는정책을받을수없으므로프로덕션배포에사용하지않는것이좋습니다.
  - 간격**:** 지정된간격으로연결합니다. 이옵션이적용될때잠금또는초기화와같은보안정책을전송하면다음에장치가연결할때동작이처리됩니다. 이옵션을선택하면 **N** 분마다연결필드가나타납니다. 이필드에장치를다시연결하기전까지의시간 (분) 을입력해야합니다. 기본값은 **20** 입니다.
  - 일정정의**:** 사용하면네트워크연결이끊긴후사용자장치의 XenMobile 이 XenMobile 서버에다시연결을시도하고제어패킷을정의된시간내에정기적으로전송하여연결을모니터링합니다. 연결시간을정의하는방법은다음에나오는연결시간정의를참조하십시오.
    * 다음시간동안고정된연결유지**:** 사용자장치가정의된시간동안연결되어야합니다.
    * 다음각범위내에서연결하도록요구**:** 사용자장치가정의된시간동안한번이상연결되어야합니다.
    * **UTC** 가아닌로컬장치시간사용**:** 정의된시간을 UTC(협정세계시) 가아닌로컬장치시간과동기화합니다.

연결시간정의

다음옵션을사용하면원하는시간을정의할수있는시간표시줄이나타납니다. 특정시간동안영구적으로연결하도록하거나특정시간내에연결하도록하는옵션중에서하나를선택하거나둘다를선택할수있습니다. 시간표시줄의각사각형은 30 분입니다. 주중오전 8 시부터오전 9 시사이에연결하도록하려면주중오전 8 시와오전 9 시사이의시간표시줄사각형두개를클릭합니다.

예를들어다음그림에서시간표시줄 2 개는주중오전 8 시부터오전 9 시까지영구적으로연결해야하고토요일오전 12 시부터일요일오전 1 시까지영구적으로연결해야하며주중매일오전 5 시부터오전 8 시또는오전 10 시부터오후 11 시사이에한번이상연결해야함을나타냅니다.



연락처 **(CardDAV)** 장치정책

January 5, 2022

XenMobile 에서장치정책을추가하여 iOS 연락처 (CardDAV) 계정을사용자의 iOS 또는 macOS 장치에추가하고이러한장치의연락처데이터를 CardDAV 를지원하는모든서버와동기화할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.

- 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

OS 업데이트제어장치정책

September 29, 2021

OS 업데이트제어장치정책을사용하여다음을배포할수있습니다.

- 감독되는 iOS 장치에최신 OS 업데이트를배포할수있습니다.

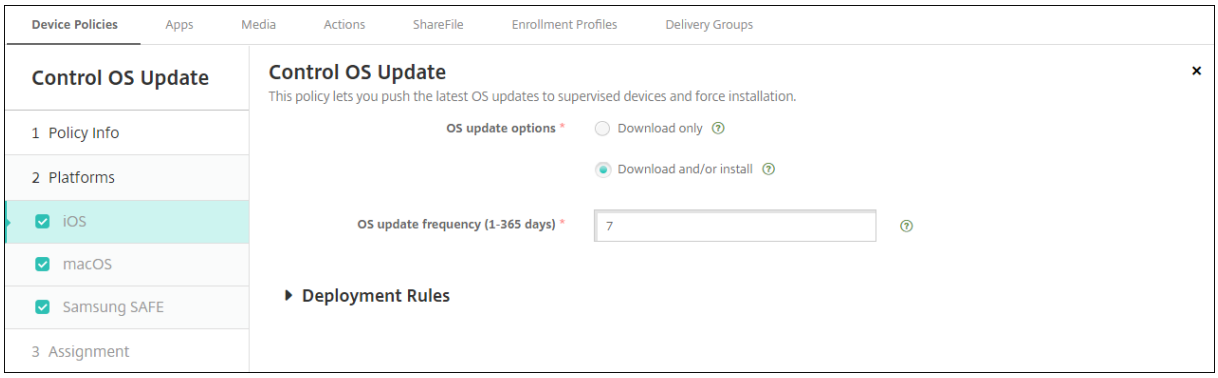
  OS 업데이트장치정책은 Apple 배포프로그램에등록된감독되는장치에대해서만작동합니다.

- 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.

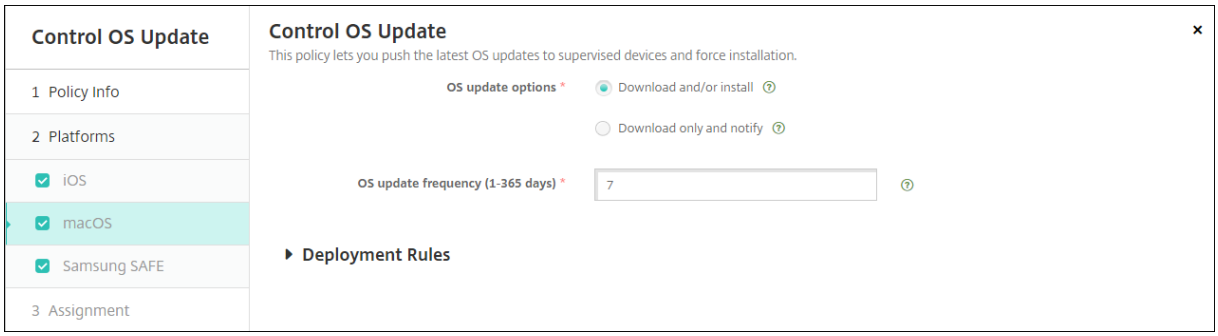
이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



- **OS** 업데이트옵션**:** 두옵션모두 **OS** 업데이트빈도에따라최신 OS 업데이트를감독되는장치에다운로드합니다. 장치에업데이트를설치하라는메시지가표시됩니다. 이메시지는사용자가장치를잠금해제한후표시됩니다.
- **OS** 업데이트빈도**:** XenMobile 이장치 OS 를확인하고업데이트할빈도를결정합니다. 기본값은 **7** 일입니다.

macOS 설정



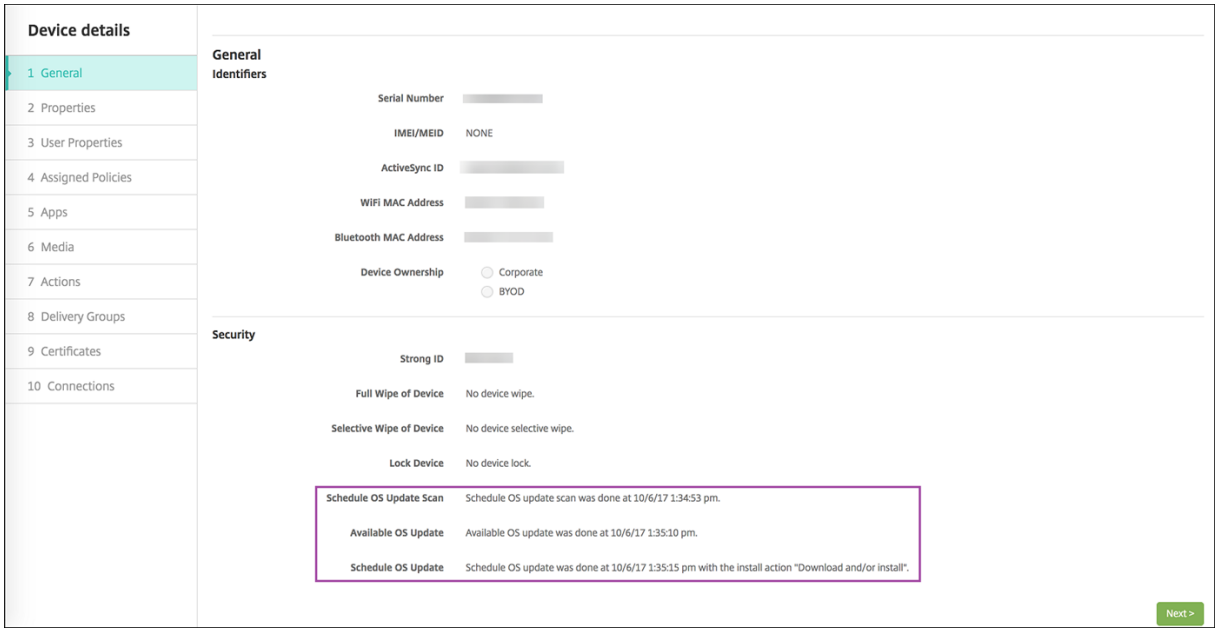
- **OS** 업데이트옵션**:** 두옵션모두 **OS** 업데이트빈도에따라최신 macOS 업데이트를다운로드합니다. 선택에따라, 업데이트를설치하거나 App Store 를통해업데이트를사용할수있음을사용자에게알릴수있습니다.
- **OS** 업데이트빈도**:** XenMobile 이장치 OS 를확인하고업데이트할빈도를결정합니다. 기본값은 **7** 일입니다.

iOS 및 macOS 업데이트작업의상태확인

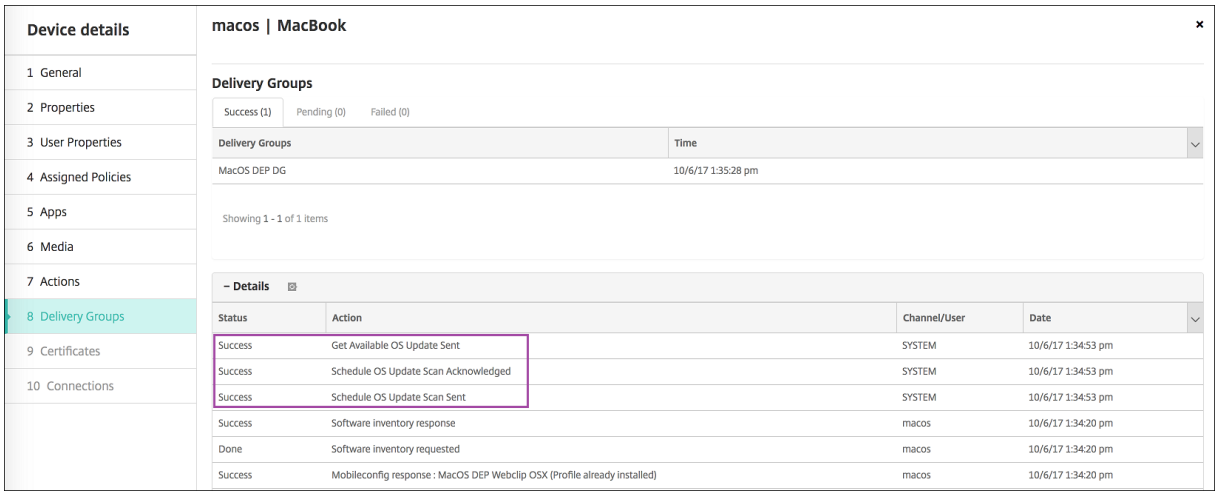
iOS 및 macOS 의경우 XenMobile 이 OS 업데이트제어정책을장치에배포하지않습니다. 대신 XenMobile 은정책을사용하여다음과같은 MDM 명령을장치에전송합니다.

- OS 업데이트검사예약: OS 업데이트에대한백그라운드검사를수행하도록장치에요청합니다 (iOS 의경우선택사항).
- 사용가능한 OS 업데이트: 장치를쿼리하여사용가능한 OS 업데이트목록을확인합니다.
- OS 업데이트예약: macOS 업데이트, 앱업데이트또는둘다를수행하도록장치에요청합니다. OS 및앱업데이트를다운로드하거나설치하는시기는장치 OS 에따라결정됩니다.

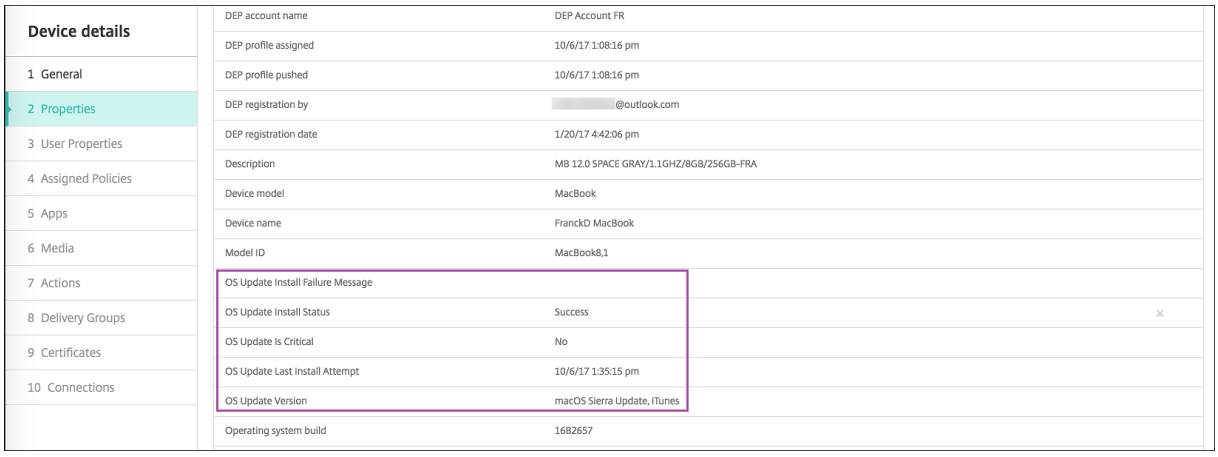
관리 **>** 장치 **>** 장치세부정보 **(**일반**)** 페이지에예약된 OS 업데이트검사와사용가능한 OS 업데이트검사, 예약된 macOS 및앱업데이트의상태가표시됩니다.

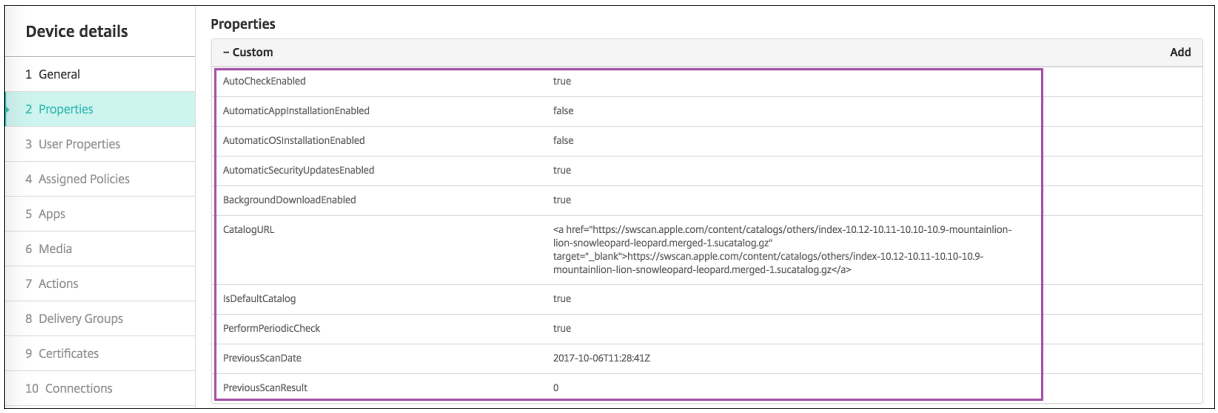


업데이트작업의상태에대한자세한내용을보려면 관리 **>** 장치 **>** 장치세부정보 **(**배달그룹**)** 페이지로이동합니다.



사용가능한 OS 업데이트및마지막설치시도등의세부정보를보려면 관리 **>** 장치 **>** 장치세부정보 **(**속성**)** 페이지로이동합니다.

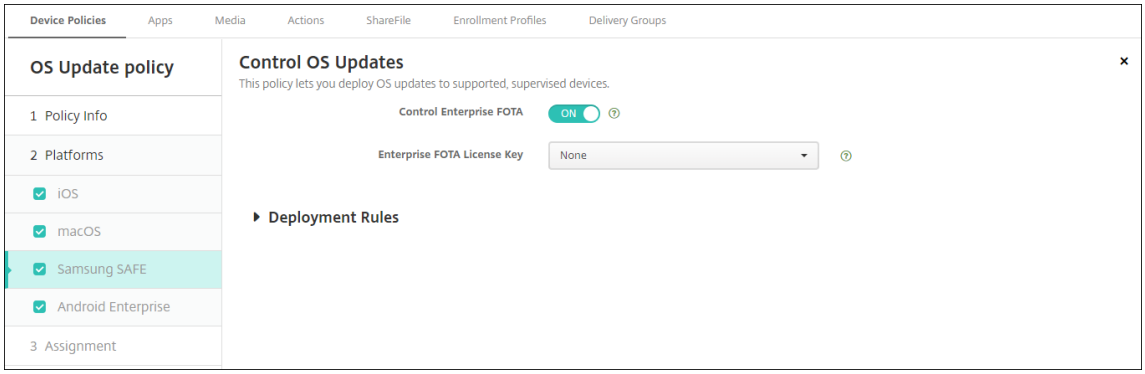




Samsung SAFE 설정

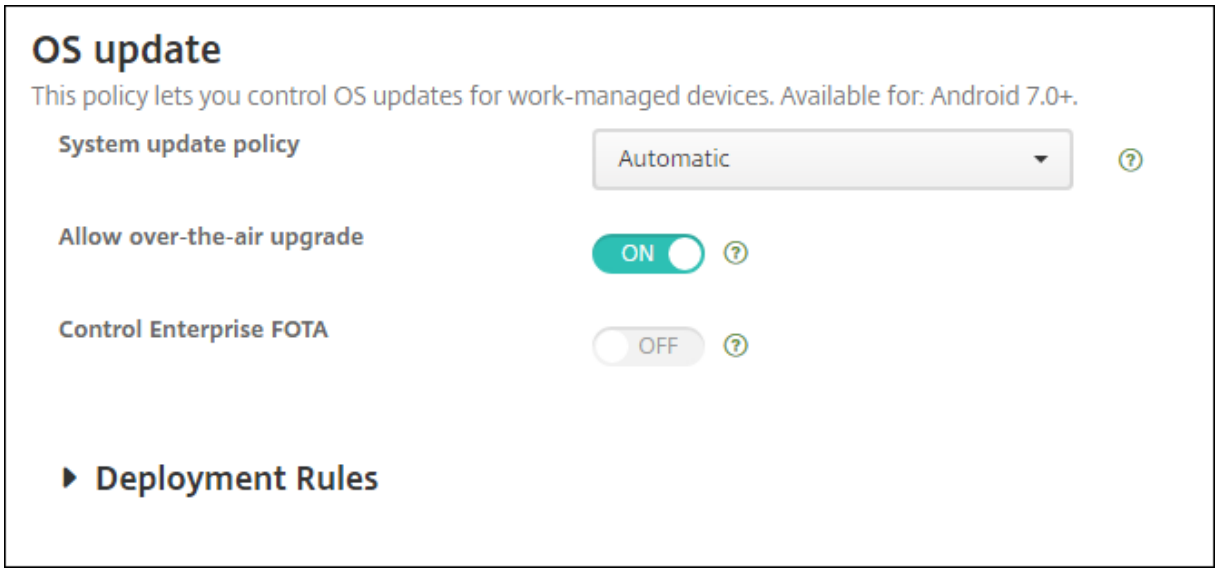
Samsung E-FOTA(Enterprise FOTA) 는장치의업데이트시기및사용할펌웨어버전을알려줍니다. E-FOTA 를사용하려면:

1. Samsung 에서받은키및라이센스정보를사용하여 Samsung MDM 라이센스키장치정책을만듭니다. 자세한내용은 Samsung MDM 라이센스키장치정책을참조하십시오.
2. Enterprise FOTA 를사용하려면 OS 업데이트제어장치정책을만듭니다.



- **Enable Enterprise FOTA(Enterprise FOTA 사용):** 켜짐으로설정합니다.
- **Enterprise FOTA** 라이센스키**:** Samsung MDM 라이센스키장치정책이름을선택합니다.

Android Enterprise 설정



- 시스템업데이트정책**:** 시스템업데이트시기를결정합니다. 엔터프라이즈 **FOTA** 제어설정을사용하도록설정하면이설정의구성에관계없이업데이트가자동으로수행됩니다.
  - 자동**:** 업데이트가제공되면설치합니다.
  - 기간내**:** 시작시간과 종료시간에지정된일일유지관리기간내에업데이트를자동으로설치합니다.
    * 시작시간**:** 유지관리기간의시작시간으로, 장치의로컬시간을기준으로자정이후의분수 (**0~1440**) 로측정됩니다. 기본값은 **0** 입니다.
    * 종료시간**:** 유지관리기간의종료시간으로, 장치의로컬시간을기준으로자정이후의분수 (**0~1440**) 로측정됩니다. 기본값은 **120** 입니다.

  - 연기**:** 사용자가최대 30 일까지업데이트를연기할수있습니다.
- 무선업그레이드허용**:** 사용하지않도록설정하면사용자장치에서소프트웨어업데이트를무선으로수신할수없습니다. 기본값은 켜짐입니다.
- 엔터프라이즈 **FOTA** 제어**:** 사용하도록설정하면 Samsung 장치가최신업데이트를확인하고자동으로설치합니다. 사용하지않도록설정하면사용자가직접업데이트를확인하고수동으로설치할수있습니다. Samsung Knox 3.0 이상을실행하는 Android Enterprise 장치를위한설정입니다. 기본값은 꺼짐입니다.
  - 엔터프라이즈 **FOTA** 라이센스키**:** 업데이트를확인할때사용할라이센스키를선택합니다. Samsung MDM 라이선스키정책에서이설정을구성할수있습니다. Samsung Knox 3.0 이상을실행하는 Android Enterprise 장치를위한설정입니다. 기본값은 없음입니다. **Samsung MDM** 라이센스키장치정책을사용하여키를설정할수있습니다. Samsung MDM 라이센스키장치정책을참조하십시오.

Samsung 컨테이너에앱복사장치정책

January 5, 2022

장치에이미설치된앱의경우해당앱을지원되는 Samsung 장치에서 KNOX 컨테이너로복사하도록지정할수있습니다. 지원되는장치에대한자세한내용은 Samsung 문서 Knox 에서구축한디바이스를참조하십시오.

KNOX 컨테이너에복사된앱은사용자가 KNOX 컨테이너에로그인하는경우에만사용할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

사전요구사항

- XenMobile 에장치를등록합니다.
- Samsung MDM 키 (ELM 및 KLM) 를배포합니다. 수행방법에대해서는 Samsung MDM 라이센스키장치정책을참조하십시오.
- 장치에앱을설치합니다.
- 장치에서 KNOX 를초기화하여앱을 KNOX 컨테이너에복사합니다.

플랫폼설정

- 새앱**:** 목록에추가하려는각앱에대해 추가를클릭한후다음을수행합니다.
  - 패키지 ID 를입력합니다 (예: LacingArt 앱의경우 com.mobiwolf.lacingart).
  - 저장또는 취소를클릭합니다.

자격증명장치정책

August 12, 2022

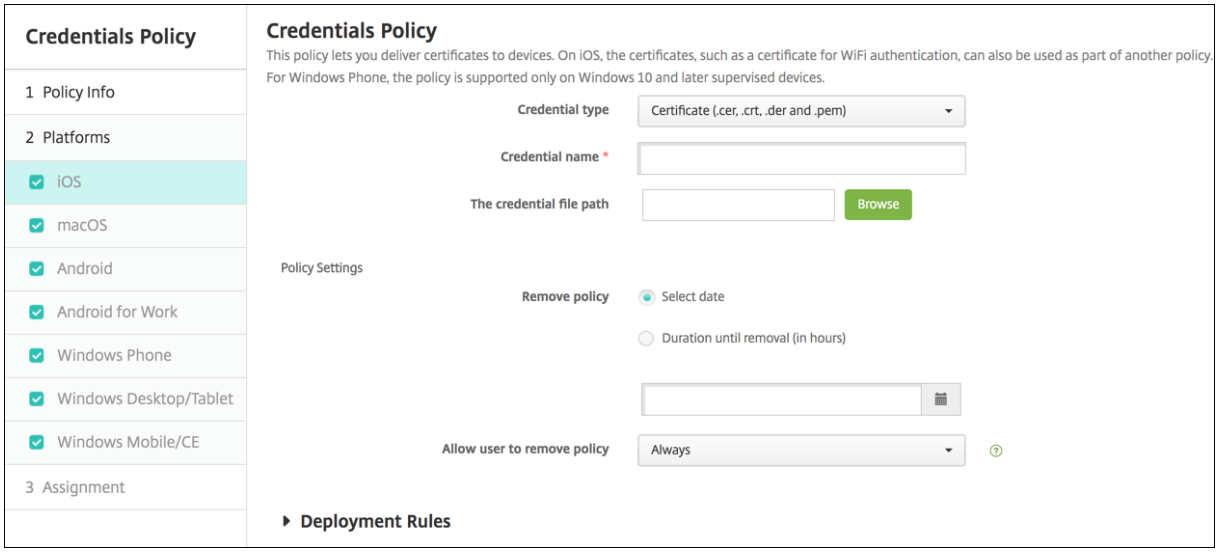
자격증명장치정책은 XenMobile 에서구성된 PKI 를가리킵니다. 예를들어, PKI 구성에는 PKI 엔터티, 키저장소, 자격증명공급자또는서버인증서가포함될수있습니다. 자격증명에대한자세한내용은 인증서및인증을참조하십시오.

지원되는각플랫폼마다이문서에서설명되어있는서로다른값집합이필요합니다.

> 참고:
>
> 이정책을만들기전에각플랫폼에사용할자격증명정보와모든인증서및암호가필요합니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

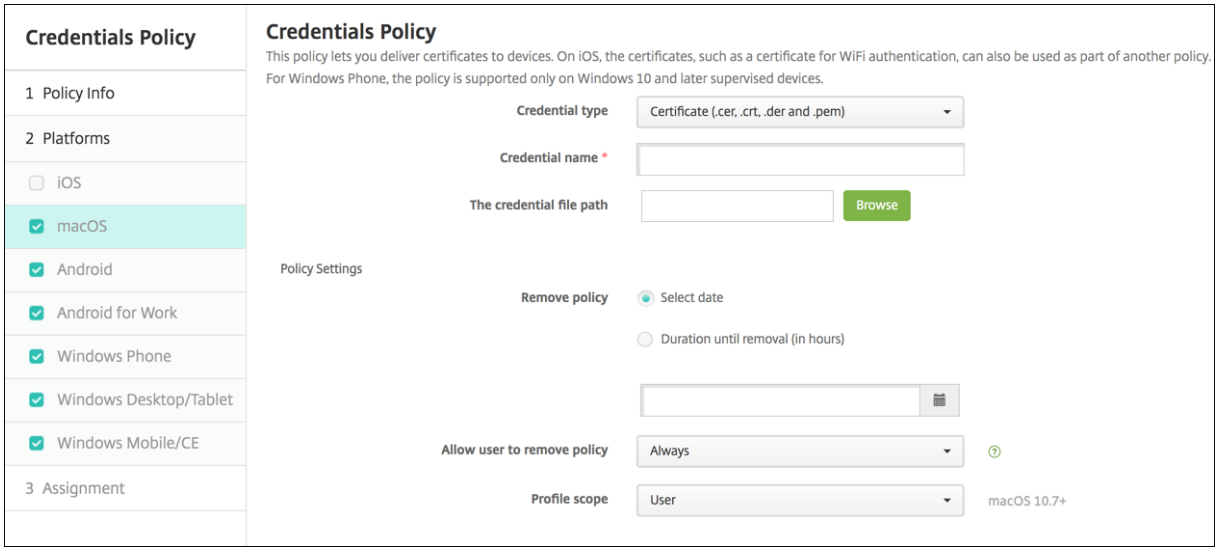


다음설정을구성합니다.

- 자격증명유형: 목록에서이정책에사용할자격증명유형을클릭하고선택한자격증명에대해다음정보를입력합니다.
  - 인증서
    - 자격증명이름: 자격증명의고유한이름을입력합니다.
    - 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
  - 키저장소
    - 자격증명이름: 자격증명의고유한이름을입력합니다.
    - 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
    - 암호: 자격증명에대한키저장소암호를입력합니다.
  - 서버인증서
    - 서버인증서: 목록에서사용할인증서를클릭합니다.
  - 자격증명공급자
    - 자격증명공급자: 목록에서자격증명공급자의이름을클릭합니다.
- 정책설정
  - 정책제거: 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 (시간) 입니다.

* 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
* 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

macOS 설정

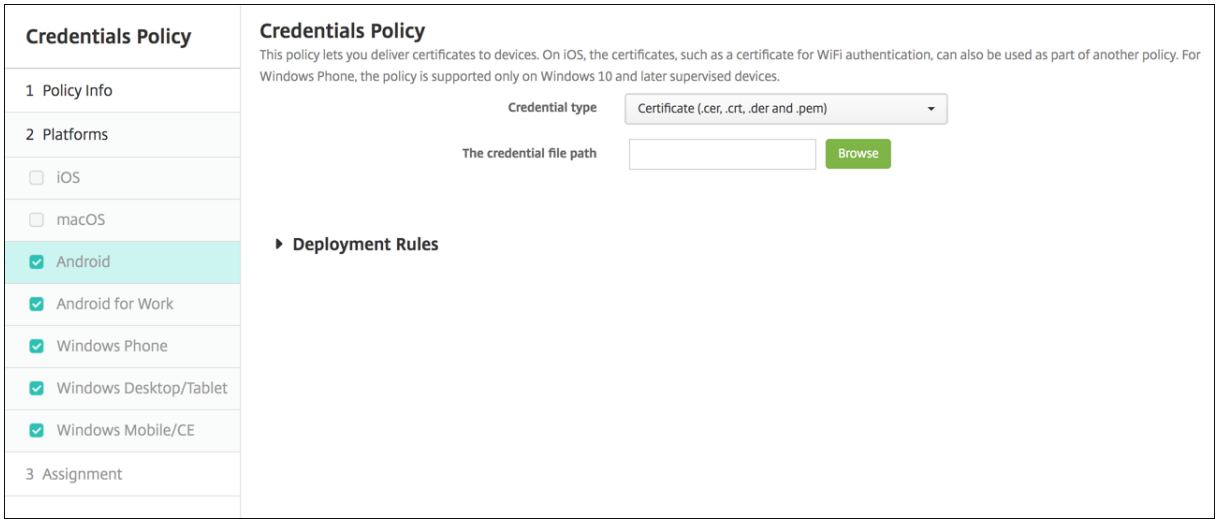


다음설정을구성합니다.

- 자격증명유형**:** 목록에서이정책에사용할자격증명유형을클릭하고선택한자격증명에대해다음정보를입력합니다.
  - 인증서
    * 자격증명이름**:** 자격증명의고유한이름을입력합니다.
    * 자격증명파일경로**:** 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
  - 키저장소
    * 자격증명이름**:** 자격증명의고유한이름을입력합니다.
    * 자격증명파일경로**:** 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
    * 암호**:** 자격증명에대한키저장소암호를입력합니다.
  - 서버인증서
    * 서버인증서**:** 목록에서사용할인증서를클릭합니다.
  - 자격증명공급자
    * 자격증명공급자**:** 목록에서자격증명공급자의이름을클릭합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    * 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    * 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.

- 프로필범위: 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

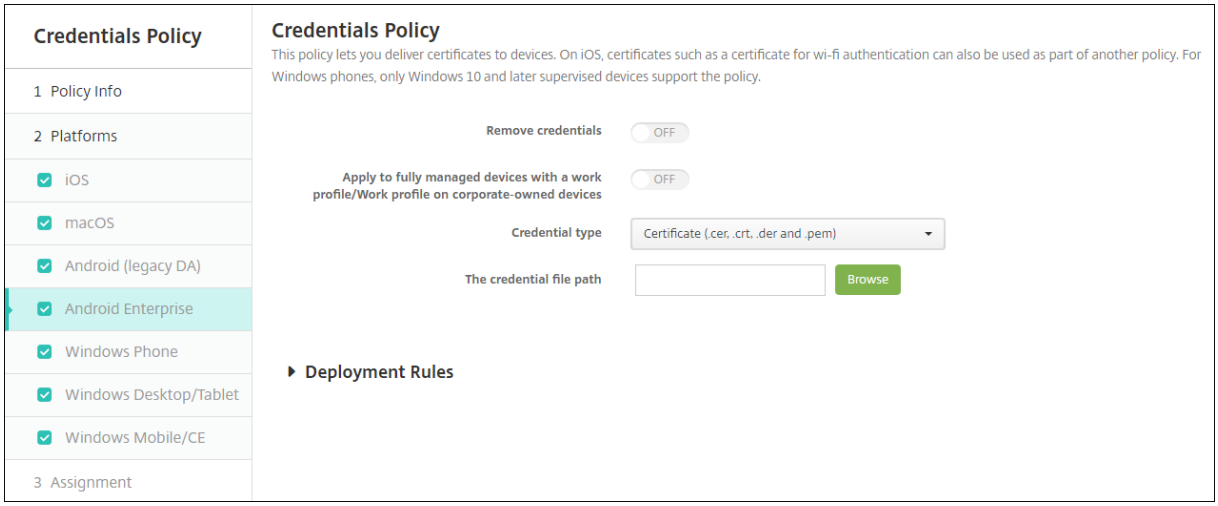
Android 설정



다음설정을구성합니다.

- 자격증명유형: 목록에서이정책에사용할자격증명유형을클릭하고선택한자격증명에대해다음정보를입력합니다.
  - 인증서
    - 자격증명이름: 자격증명의고유한이름을입력합니다.
    - 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
  - 키저장소
    - 자격증명이름: 자격증명의고유한이름을입력합니다.
    - 자격증명파일경로: 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
    - 암호: 자격증명에대한키저장소암호를입력합니다.
  - 서버인증서
    - 서버인증서: 목록에서사용할인증서를클릭합니다.
  - 자격증명공급자
    - 자격증명공급자: 목록에서자격증명공급자의이름을클릭합니다.

Android Enterprise 설정



XenMobile 이자격증명설정을적용하는방식을결정하려면다음설정을구성합니다.

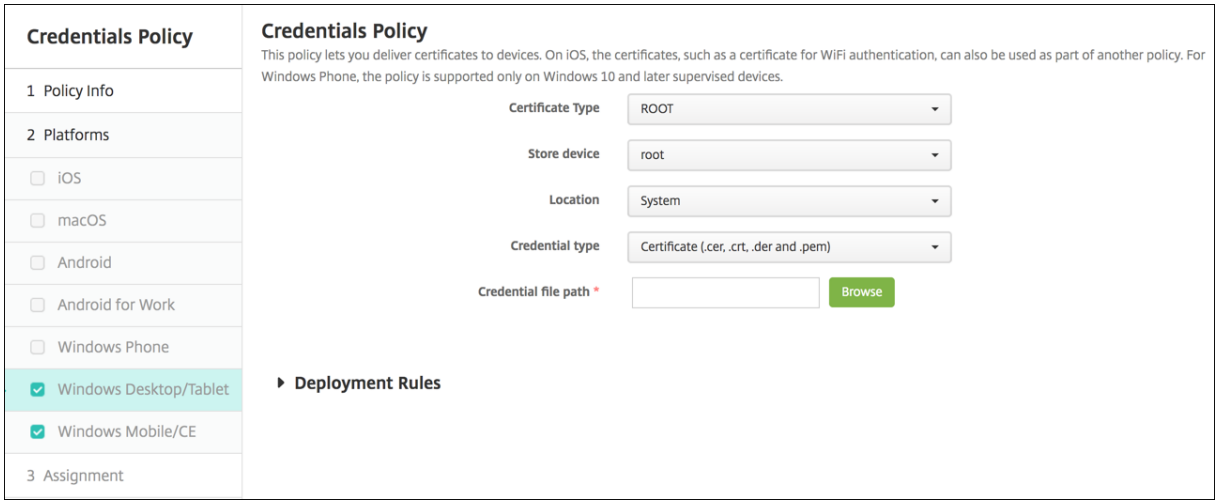
- 자격증명제거**:** 켜짐으로설정하면다음설정이구성됩니다. 기본값은 꺼짐입니다.
  - 사용자자격증명제거**:** 관리되는키저장소에서인증서를삭제합니다. 기본값은 꺼짐입니다.
  - 신뢰할수있는루트인증서제거**:** 비시스템 CA 인증서를모두제거합니다. 기본값은 꺼짐입니다.
- 작업프로필/회사소유장치의작업프로필을사용하는완전관리형장치에적용**:** 작업프로필로완전히관리되는장치에대해자격증명정책설정을구성할수있도록허용합니다. 이설정이 켜짐인경우구성한자격증명설정이작업프로필에만적용됩니다. 이설정이 꺼짐인경우구성하는자격증명설정이장치에만적용됩니다. 기본값은 꺼짐입니다.

자격증명설정을구성합니다.

- 자격증명유형**:** 목록에서이정책에사용할자격증명유형을클릭하고선택한자격증명에대해다음정보를입력합니다.
  - 인증서
    - 자격증명파일경로**:** 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
  - 키저장소
    - 자격증명파일경로**:** 찾아보기를클릭하고파일위치로이동하여자격증명파일을선택합니다.
    - 인증서별칭**:** 인증서별칭으로앱에서인증서에액세스하기가더간편해집니다. 관리되는구성장치정책에서인증서별칭을구성합니다. 그런다음자격증명장치정책의 인증서별칭필드에별칭을입력합니다. 앱에서사용자작업없이도인증서를검색하고 VPN 을인증합니다.
    - 암호**:** 자격증명에대한키저장소암호를입력합니다.
  - 서버인증서
    - 서버인증서**:** 목록에서사용할인증서를클릭합니다.
  - 자격증명공급자
    - 인증서별칭**:** 인증서별칭으로앱에서인증서에액세스하기가더간편해집니다. 관리되는구성장치정책에서인증서별칭을구성합니다. 그런다음자격증명장치정책의 인증서별칭필드에별칭을입력합니다. 앱에서사용자작업없이도인증서를검색하고 VPN 을인증합니다.
    - 자격증명공급자**:** 목록에서자격증명공급자의이름을클릭합니다.
    - 인증서를사용할앱**:** 이공급자의자격증명에자동으로액세스하는앱을지정하려면 추가를클릭하고앱을선택한

다음 저장을클릭합니다.

Windows 데스크톱/태블릿설정



- 인증서유형**:** 목록에서 루트또는 클라이언트를클릭합니다.
- 루트를클릭하는경우다음설정을구성합니다.
  - 스토어장치**:** 목록에서자격증명의인증서저장소위치로 루트, 내또는 **CA** 를클릭합니다. 내의경우사용자의인증서저장소에인증서가저장됩니다.
  - 위치**:** Windows 10 또는 Windows 11 태블릿의경우 시스템이유일한위치입니다.
  - 자격증명유형**:** Windows 10 및 Windows 11 태블릿의경우 인증서가유일한자격증명유형입니다.
  - 자격증명파일경로**:** 찾아보기를클릭하고파일위치로이동하여인증서파일을선택합니다.
- 클라이언트를클릭하는경우다음설정을구성합니다.
- 위치**:** Windows 10 또는 Windows 11 태블릿의경우 시스템이유일한위치입니다.
- 자격증명유형**:** Windows 10 및 Windows 11 태블릿의경우 키저장소가유일한자격증명유형입니다.
- 자격증명이름**:** 자격증명의이름을입력합니다. 이것은필수필드입니다.
- 자격증명파일경로**:** 찾아보기를클릭하고파일위치로이동하여인증서파일을선택합니다.
- 암호**:** 자격증명과연관된암호를입력합니다. 이것은필수필드입니다.

사용자지정 **XML** 장치정책

August 12, 2022

XenMobile 에서사용자지정 XML 정책을만들어지원되는 Windows 및 Zebra Android 와 Android Enterprise 장치에서다음기능을사용자지정할수있습니다.

- 장치구성을비롯한프로비저닝, 기능을사용하거나사용하지않도록설정
- 사용자가설정및장치매개변수를변경하도록허용하는것을비롯한장치구성

- 앱및시스템소프트웨어를비롯하여장치에로드할새소프트웨어또는버그수정을제공하는것을포함하는소프트웨어업그레이드
- 장치에서오류및상태보고서를받는것을비롯한오류관리

> 참고:
>
> XML 콘텐츠를만들때는% 문자를주의해서사용하십시오. % 문자는 XML 예약문자로, XML 특수문자를이스케이프하는데만사용됩니다. 이름에% 를사용하려면%25 로인코딩합니다.

Windows 장치의경우: OMA DM(Open Mobile Alliance Device Management) API 를사용하여사용자지정 XML 구성을만듭니다. OMA DM API 로사용자지정 XML 을만드는것은이항목의범위를벗어납니다. OMA DM API 를사용하는방법에대한자세한내용은 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 정책또는제한정책을휴대폰에배포한후브라우저가사용되는상태로유지됩니다. 이문제를해결하려면휴대폰을다시시작하십시오. 이것은타사문제입니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Windows Desktop/Tablet, Zebra Android 및 **Android Enterprise** 설정

- **XML** 콘텐츠**:** 정책에추가할사용자지정 XML 코드를입력하거나잘라내붙여넣습니다.

  다음을클릭하면 XenMobile 이 XML 콘텐츠구문을확인합니다. 모든구문오류가콘텐츠상자아래에나타납니다. 계속하려면먼저모든오류를해결합니다.

  구문오류가없으면 사용자지정 **XML** 정책할당페이지가나타납니다.

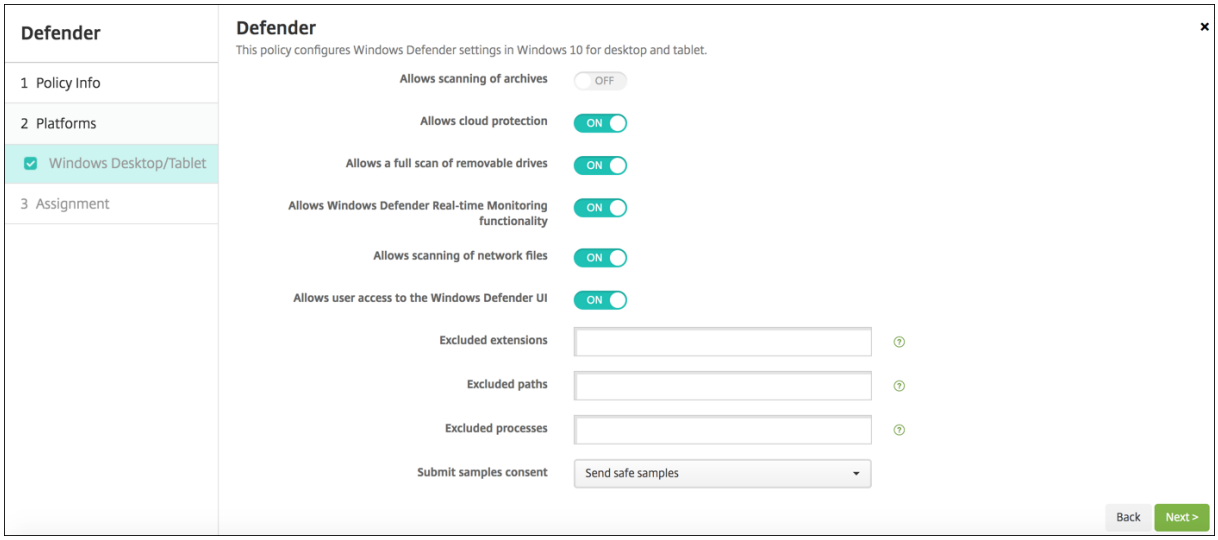
Defender 장치정책

January 5, 2022

Windows Defender 는 Windows 10 및 Windows 11 에포함된맬웨어방지프로그램입니다. XenMobile 장치정책인 Defender 를사용하여 Windows 10 및 Windows 11 데스크톱및태블릿에대한 Microsoft Defender 정책을구성할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Windows Desktop 및태블릿설정



- 보관파일에대한검사허용**:** Defender 가보관파일을검사하는것을허용하거나허용하지않습니다. 기본값은 꺼짐입니다.
- 클라우드보호허용**:** Defender 가 Microsoft 로맬웨어활동과관련된정보를보내는것을허용하거나허용하지않습니다. 기본값은 켜짐입니다.
- 이동식드라이브에대한전체검사허용**:** Defender 가 USB 스틱같은이동식드라이브를검사하는것을허용하거나허용하지않습니다. 기본값은 켜짐입니다.
- **Windows Defender** 실시간모니터링기능허용**:** 기본값은 켜짐입니다.
- 네트워크파일에대한검사허용**:** Defender 가네트워크파일을검사하는것을허용하거나허용하지않습니다. 기본값은 켜짐입니다.
- **Windows Defender UI** 에대한사용자액세스허용**:** 사용자가 Windows Defender 사용자인터페이스에액세스할수있는지여부를지정합니다. 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.

장치상태증명장치정책

January 5, 2022

XenMobile 에서 Windows 10 및 Windows 11 장치가분석을위해특정데이터및런타임정보를 HAS(상태증명서비스) 에전송하여해당상태를보고하도록할수있습니다. HAS 에서상태증명인증서를생성하고반환하면장치가이를 XenMobile 에보냅니다. XenMobile 은상태증명인증서를받은후상태증명인증서의내용에따라이전에설정된자동동작을배포할수있습니다.

HAS 에의해확인되는데이터는다음과같습니다.

- AIK 존재
- Bit Locker 상태
- 부팅디버깅사용
- 부팅관리자수정목록버전
- 코드무결성사용
- 코드무결성수정목록버전
- Apple 배포프로그램정책
- ELAM 드라이버로드
- 실행시간
- 커널디버깅사용
- PCR
- 재설정횟수
- 다시시작횟수
- 안전모드사용
- SBCP 해시
- 보안부팅사용
- 테스트서명사용
- VSM 사용
- WinPE 사용

자세한내용은 Microsoft 장치 HealthAttestation CSP 페이지를참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Microsoft Cloud 를사용하여 **DHA** 를구성하려면

장치상태증명정책을추가하고선택한각플랫폼에대해다음설정을구성합니다.

- 장치상태증명사용**:** 장치상태증명을요구할것인지를선택합니다. 기본값은 꺼짐입니다.

온프레미스 **Windows DHA** 서버를사용하여 **DHA** 를구성하려면

DHA 온-프레미스를사용하려면먼저 DHA 서버를구성해야합니다. 그런다음온-프레미스 DHA 서비스를활성화하는 XenMobile Server 정책을생성합니다.

1. DHA 를구성하려면 Windows Server 2016 Technical Preview 5 이상을실행하는컴퓨터에 DHA 서버역할을설치해야합니다. 자세한내용은 온프레미스장치상태증명서버구성을참조하십시오.

2. 장치상태증명정책을추가하고다음설정을구성합니다.
    - 장치상태증명사용**:** 켜짐으로설정합니다.
    - 온프레미스 **Health Attestation Service** 구성**:** 켜짐으로설정합니다.
    - **On-prem DHA Service FQDN(**온**-**프레미스 **DHA** 서비스 **FQDN):** 설정하는 DHA 서버의정규화된도메인이름을입력합니다.
    - **On-prem DHA API version(**온**-**프레미스 **DHA API** 버전**):** DHA 서버에설치된 DHA 서비스의버전을선택합니다.

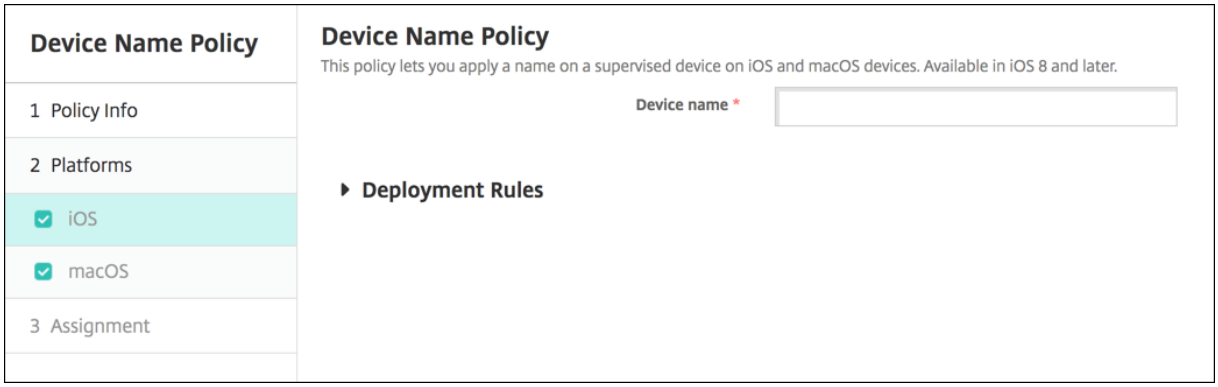
장치이름장치정책

January 5, 2022

감독되는 iOS 및 macOS 장치에장치를쉽게식별할수있도록하는이름을설정할수있습니다. 매크로, 텍스트또는둘다를사용하여장치이름을정의할수있습니다. 예를들어장치일련번호로장치이름을설정하려는경우 ${device.serialnumber} 를사용할수있습니다. 사용자이름과도메인의조합으로장치이름을설정하려면 ${user.username}@example.com 을사용할수있습니다. 매크로에대한자세한내용은 XenMobile 의매크로를참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 및 **macOS** 설정



- 장치이름**:** 매크로, 매크로조합또는매크로와텍스트조합을입력하여각장치에고유한이름을지정합니다. 예를들어 ${device.serialnumber} 를사용하여장치이름을각장치의일련번호로설정하거나 ${device.serialnumber} ${user.username} 을사용하여장치이름에사용자이름을포함합니다.

교육구성장치정책

January 5, 2022

교육구성장치정책은다음을정의합니다.

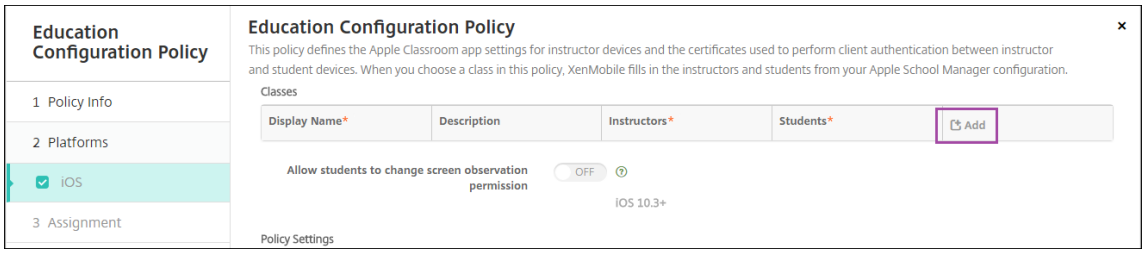
- 강사장치의 Apple Classroom 앱설정
- 강사장치와학생장치간의클라이언트인증을수행하는데사용되는인증서

이정책에서클래스를선택하면 XenMobile 콘솔에 Apple School Manager 구성의강사및학생이입력됩니다. 이정책의 Apple Classroom 앱설정이모든클래스에대해동일한경우하나의정책을생성합니다.

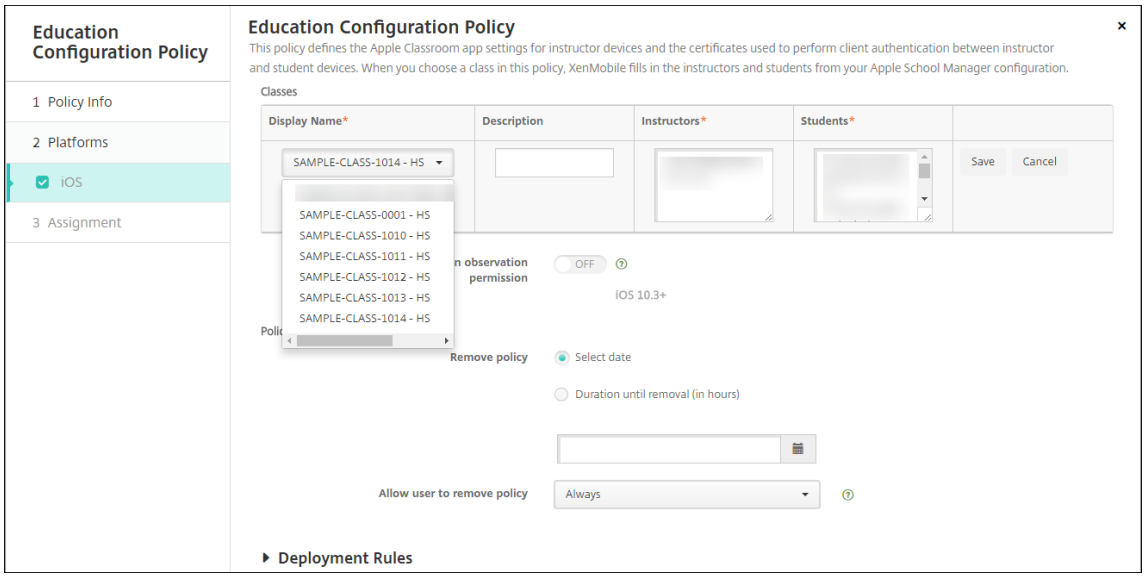
이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

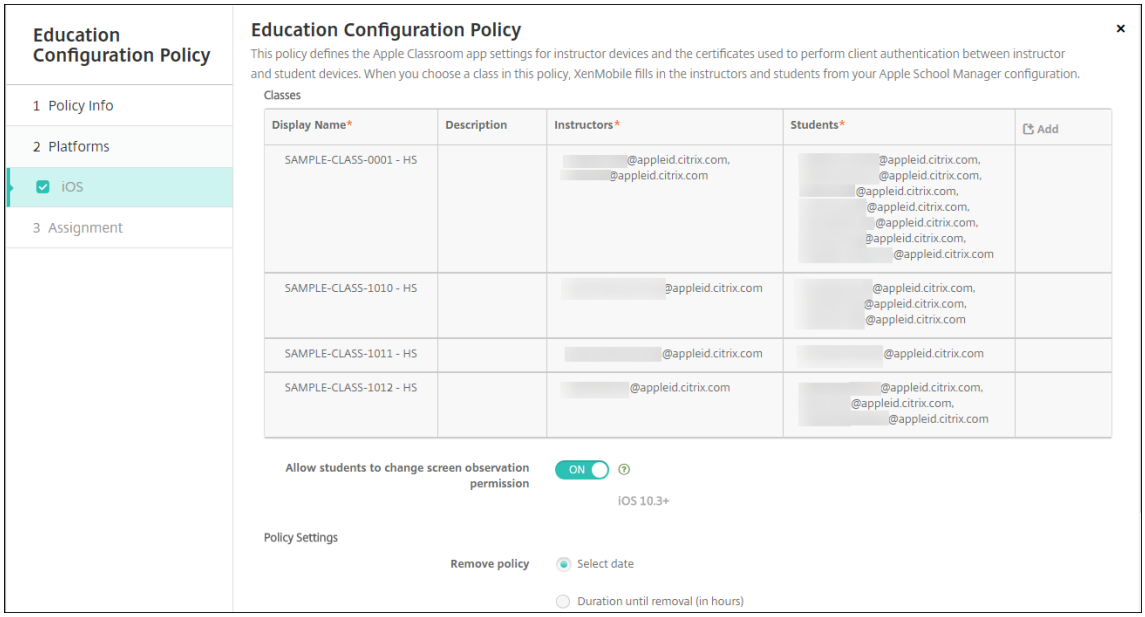
- 클래스**:** 클래스를추가하려면 추가를클릭합니다.



그런다음 표시이름목록을클릭합니다. 연결된 Apple School Manager 계정에서가져온클래스목록이나타납니다.



표시이름에서클래스를선택하면 XenMobile 이강사와학생을입력합니다. 클래스추가를계속합니다.

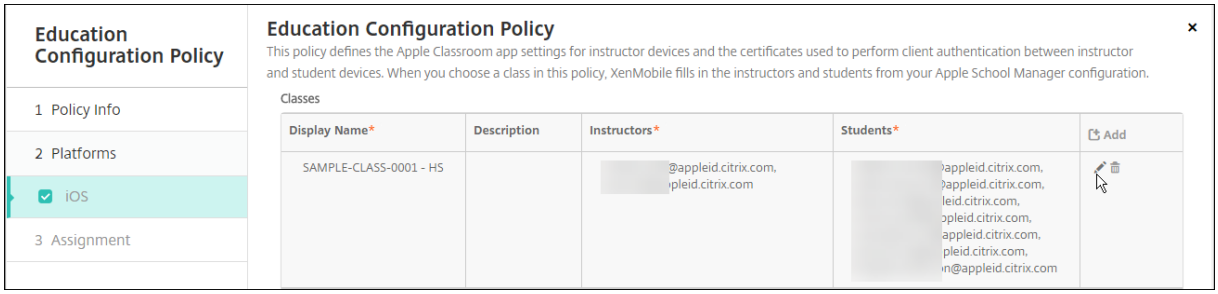


- 학생들이화면관찰허가를변경할수있도록허용**:** 켜짐인경우관리되는클래스에등록한학생은강사가자신의장치화면을볼수있도록허용할지여부를선택할수있습니다. 기본값은 꺼짐입니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.

정책의클래스정보를편집하려면

클래스에설명을추가할수있습니다 (Classroom 앱의 “표시이름”). 또한강사와학생을추가하거나제거할수있습니다. XenMobile 은이러한변경내용을 Apple School Manager 계정에저장하지않습니다. 자세한내용은 Apple 교육기능과통합의 “강사, 학생및클래스데이터관리” 를참조하십시오.

편집할클래스의 추가열위로마우스를이동하고연필아이콘을클릭합니다.



정책에서클래스를삭제하려면삭제할클래스의 추가열위로마우스를이동하고휴지통아이콘을클릭합니다.

Exchange 장치정책

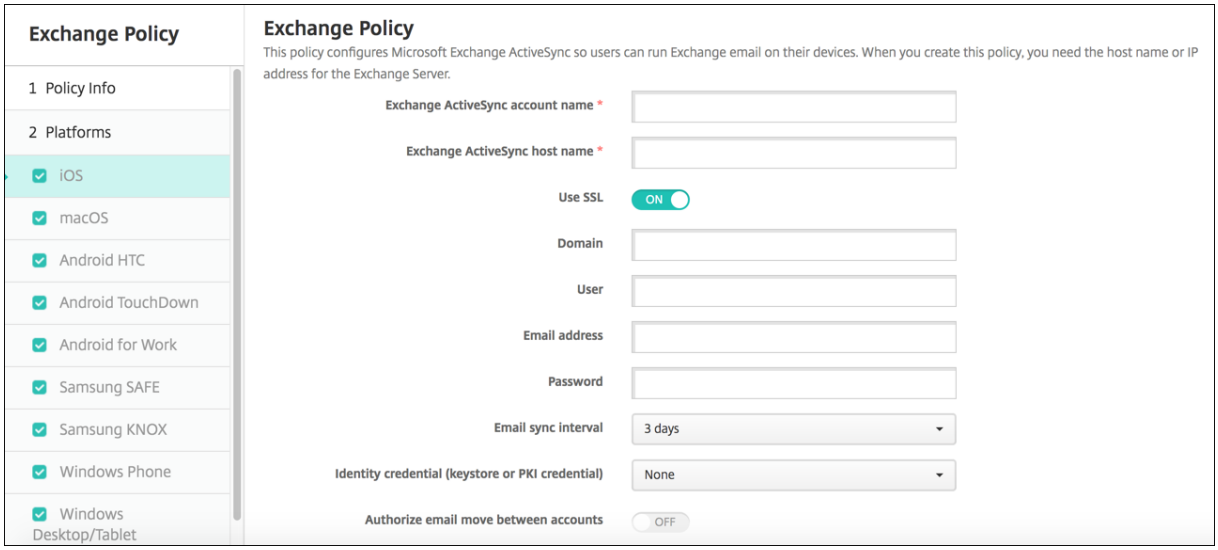
August 12, 2022

Exchange ActiveSync 장치정책을사용하여 Exchange 에서호스팅되는회사전자메일에액세스할수있도록사용자장치의전자메일클라이언트를구성할수있습니다. iOS, macOS, Android Enterprise, Samsung SAFE, Samsung KNOX 및 Windows 태블릿에대한정책을만들수있습니다. 각플랫폼마다다른값집합이필요합니다. 값집합에대해서는이후섹션에서자세히설명합니다.

이정책을만들려면 Exchange Server 의호스트이름또는 IP 주소가필요합니다. ActiveSync 설정에대한자세한내용은 Microsoft 문서 ActiveSync CSP를참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

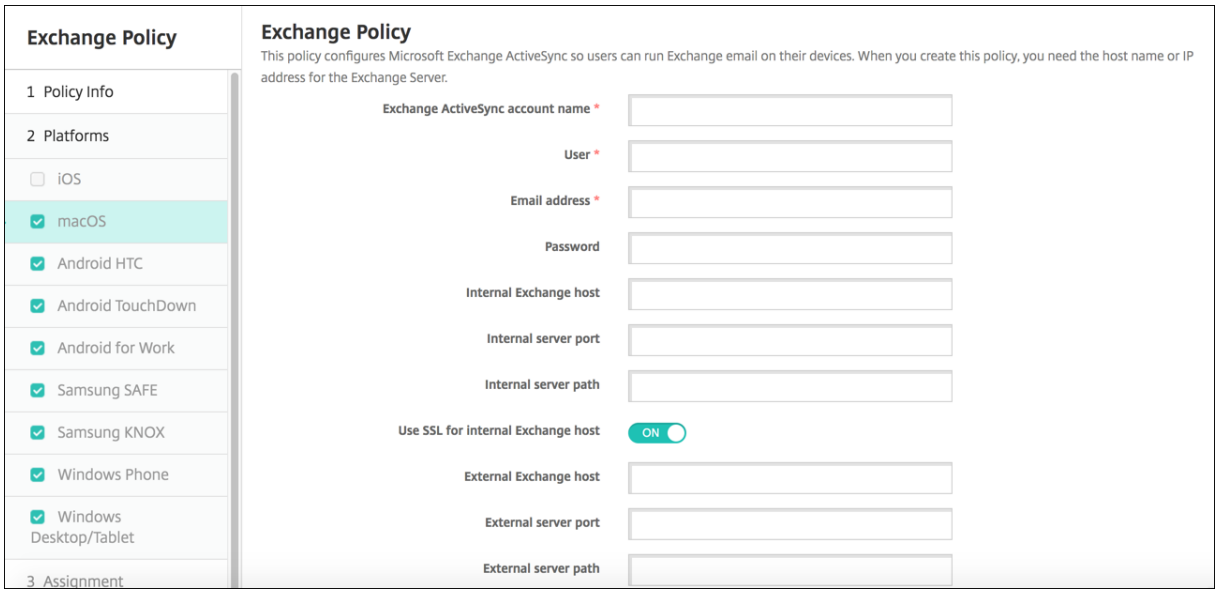
iOS 설정



- **Exchange ActiveSync** 계정이름**:** 사용자장치에표시되는전자메일계정에대한설명을입력합니다.
- **Exchange ActiveSync** 호스트이름**:** 전자메일서버의주소를입력합니다.
- **SSL** 사용**:** 사용자의장치와 Exchange Server 간의연결을보호할지여부를선택합니다. 기본값은 켜짐입니다.
- 도메인**:** Exchange Server 가상주하는도메인을입력합니다. 이필드에서 $user.domainname 시스템매크로를사용하여사용자도메인이름을자동으로조회할수있습니다.
- 사용자**:** Exchange 사용자계정의사용자이름을지정합니다. 이필드에서 $user.username 시스템매크로를사용하여사용자이름을자동으로조회할수있습니다.
- 전자메일주소**:** 전체전자메일주소를지정합니다. 이필드에서 $user.mail 시스템매크로를사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **OAuth** 사용**:** 켜짐으로설정된경우연결인증에 OAuth 가사용됩니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
- 암호**:** Exchange 사용자계정에대한선택적암호를입력합니다. **OAuth** 사용이 켜짐인경우이설정이나타나지않습니다.

- 전자메일동기화간격**:** 목록에서전자메일이 Exchange Server 와동기화되는빈도를선택합니다. 기본값은 **3** 일입니다.
- **ID** 자격증명 **(**키저장소또는 **PKI):** XenMobile 에대한 ID 공급자를구성한경우목록에서선택적인 ID 자격증명을클릭합니다. 이필드는 Exchange 가클라이언트인증서인증을요구하는경우에만필요합니다. 기본값은 없음입니다.
- 계정간전자메일이동승인**:** 사용자가이계정에서다른계정으로전자메일을이동하고다른계정에서전자메일을전달하고회신할수있도록허용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 전자메일앱에서만전자메일보내기**:** 전자메일을보낼사용자를 iOS 메일앱으로제한할지여부를선택합니다. 기본값은 꺼짐입니다.
- 최근전자메일동기화사용안함**:** 사용자가최근주소를동기화하지못하도록할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션은 iOS 6.0 이상에만적용됩니다.
- **S/MIME** 서명사용**:** 이계정이 S/MIME 서명을지원하는지여부를선택합니다. 기본값은 켜짐입니다. 켜짐으로설정하면다음필드가나타납니다.
  - 서명 **ID** 자격증명**:** 사용할서명자격증명을선택합니다.
  - **S/MIME** 서명사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 서명을켜거나끌수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
  - **S/MIME** 서명인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서사용할서명자격증명을선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 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 암호화를켜거나끌수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
  - 기본적으로 **S/MIME** 암호화사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 를기본적으로켤지여부를선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
  - **S/MIME** 암호화인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나끌수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

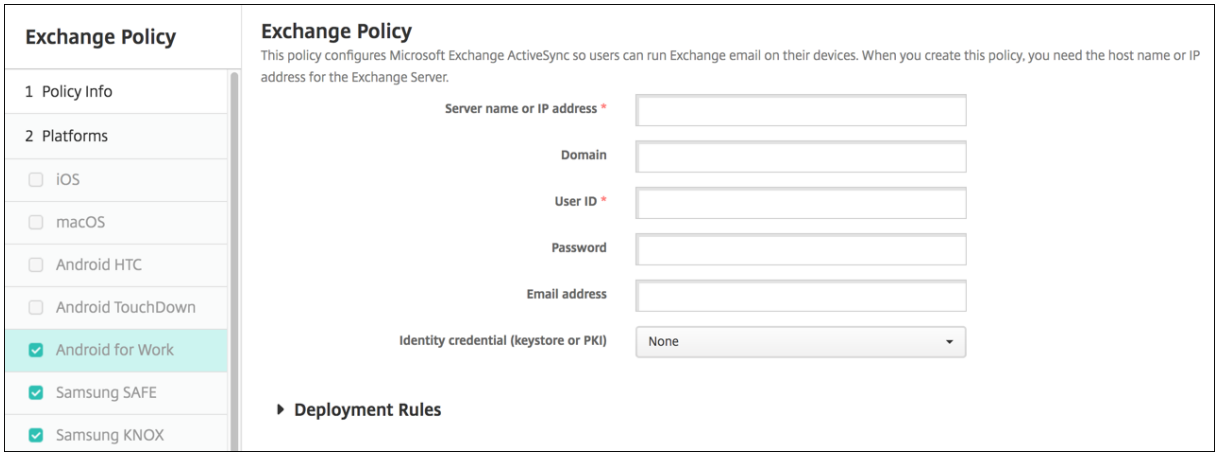
macOS 설정



- **Exchange ActiveSync** 계정이름**:** 사용자장치에표시되는전자메일계정에대한설명을입력합니다.
- 사용자**:** Exchange 사용자계정의사용자이름을지정합니다. 이필드에서 $user.username 시스템매크로를사용하여사용자이름을자동으로조회할수있습니다.
- 전자메일주소**:** 전체전자메일주소를지정합니다. 이필드에서 $user.mail 시스템매크로를사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **OAuth** 사용**:** 켜짐으로설정된경우연결인증에 OAuth 가사용됩니다. 기본값은 꺼짐입니다. 이옵션은 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 호스트이름을입력합니다.
- 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 호스트이름을입력합니다.

- 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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

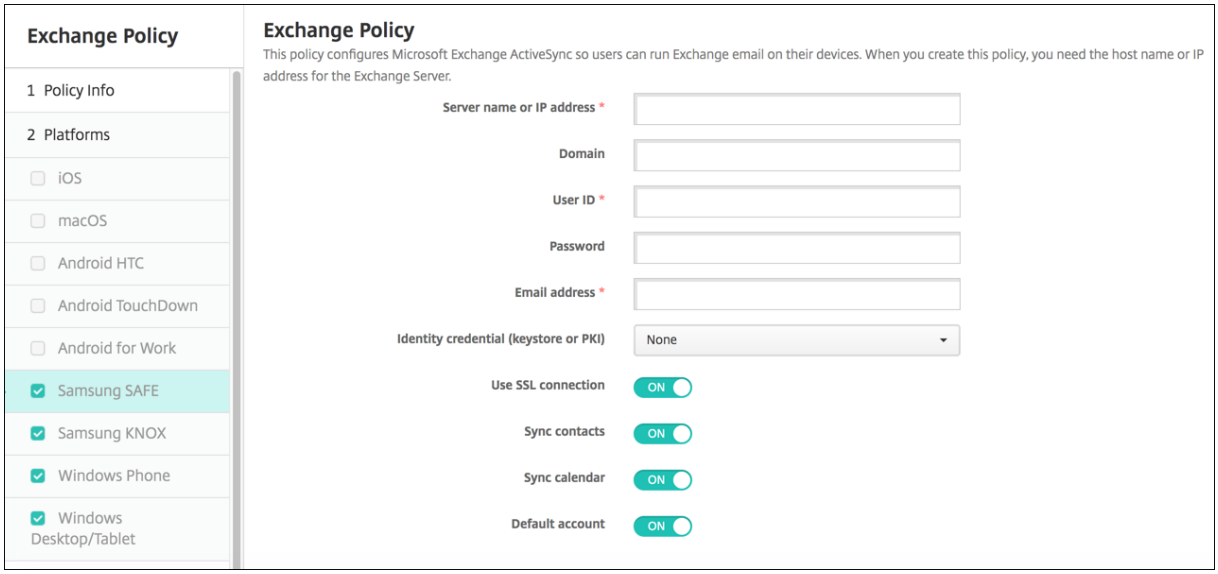
Android Enterprise



- 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.

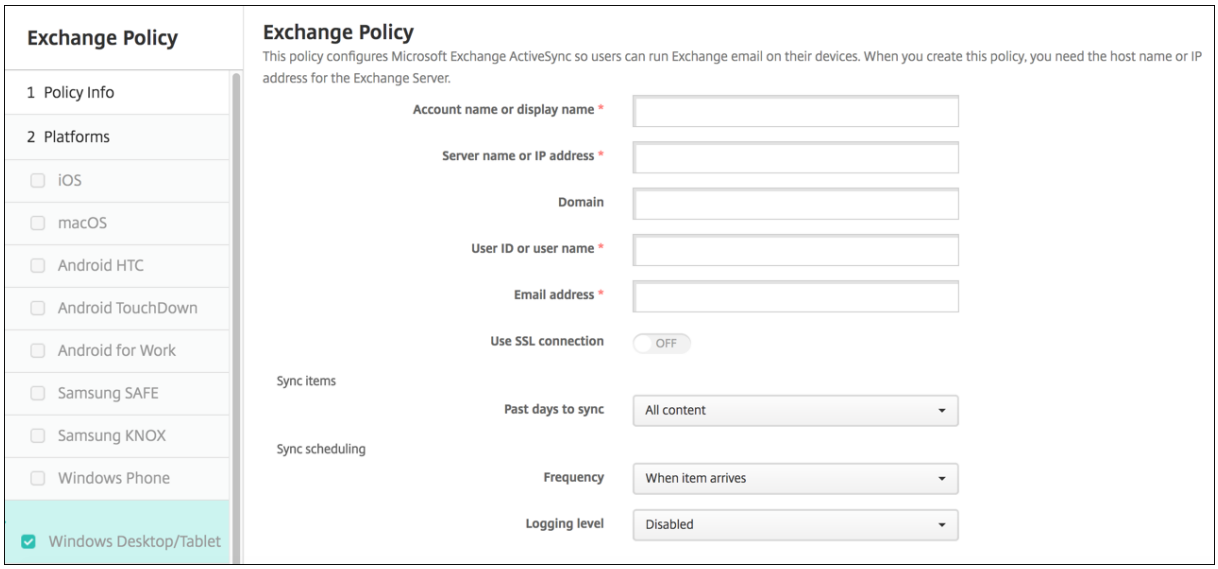
- 전자메일주소**:** 전체전자메일주소를지정합니다. 이필드에서 $user.mail 시스템매크로를사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **ID** 자격증명 **(**키저장소또는 **PKI):** XenMobile 에대한 ID 공급자를구성한경우목록에서선택적인 ID 자격증명을클릭합니다. 이필드는 Exchange 가클라이언트인증서인증을요구하는경우에만필요합니다. 기본값은 없음입니다.

Samsung SAFE 및 **Samsung KNOX** 설정



- 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.
- **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 데스크톱/태블릿설정



> 참고**:**
>
> 이정책에서는사용자암호를설정하도록허용하지않습니다. 사용자는정책이푸시된후장치에서해당매개변수를설정해야합니다.

- 계정이름또는표시이름**:** Exchange ActiveSync 계정이름을입력합니다.
- 서버이름또는 **IP** 주소**:** Exchange Server 의호스트이름또는 IP 주소를입력합니다.
- 도메인**:** Exchange Server 가상주하는도메인을입력합니다. 이필드에서 $user.domainname 시스템매크로를사용하여사용자도메인이름을자동으로조회할수있습니다.
- 사용자 **ID** 또는사용자이름**:** Exchange 사용자계정의사용자이름을지정합니다. 이필드에서 $user.username 시스템매크로를사용하여사용자이름을자동으로조회할수있습니다.
- 전자메일주소**:** 전체전자메일주소를지정합니다. 이필드에서 $user.mail 시스템매크로를사용하여사용자전자메일계정을자동으로조회할수있습니다.
- **SSL** 연결사용**:** 사용자장치와 Exchange Server 간의연결을보호할지여부를선택합니다. 기본값은 꺼짐입니다.
- 동기화할과거일수**:** 목록에서장치의모든콘텐츠를 Exchange Server 와동기화할과거일수를클릭합니다. 기본값은 모든콘텐츠입니다.
- 빈도**:** 목록에서 Exchange Server 에서장치로보낸데이터를동기화할때사용할일정을클릭합니다. 기본값은 항목이도착할때입니다.
- 로깅수준**:** 목록에서 사용안함, 기본또는 고급을클릭하여 Exchange 활동을로깅할때사용할세부정보수준을지정합니다. 기본값은 사용안함입니다.

파일장치정책

August 12, 2022

사용자가 Android 및 Android Enterprise 장치에서액세스할수있도록파일을추가하고배포할수있습니다. 장치에파일을저장할디렉토리를지정합니다. 예를들어사용자가회사문서또는.pdf 파일을받게하려고합니다. 장치에파일을배포하고파일의위치를사용자에게알립니다.

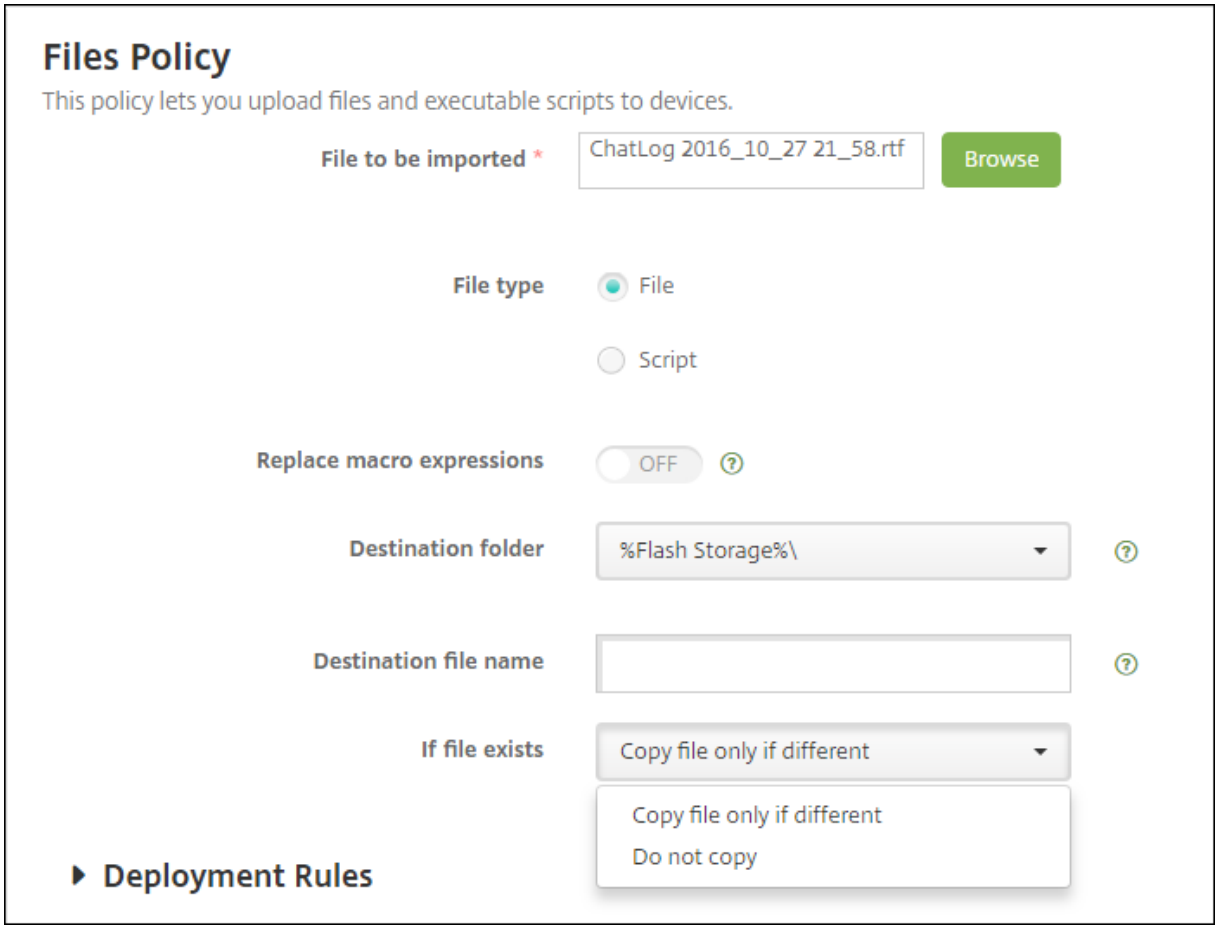
Android 장치는기본적으로스크립트실행을지원하지않습니다. 스크립트를실행하려면타사소프트웨어가필요합니다.

이정책에는다음과같은파일형식을추가할수있습니다.

- 텍스트기반파일 (.xml, .html, .py 등)
- 문서, 그림, 스프레드시트또는프레젠테이션등의기타파일

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Android Enterprise 설정



- 가져올파일**:** 가져올파일을선택하려면 찾아보기를클릭하고파일의위치로이동합니다.
- 파일형식**:** 파일또는 스크립트를선택합니다.
- 즉시실행**:** 스크립트를선택하면 즉시실행옵션이나타납니다. 이설정을활성화해도동작이실행되지않습니다. 사용자가스크립트를수동으로실행해야합니다. 매크로식바꾸기**:** 스크립트의매크로토큰이름을장치또는사용자속성으로바꿀지여부를선택합니다. 매크로구문은매크로를참조하십시오. 기본값은 꺼짐입니다.

- 대상폴더**:** 목록에서업로드된파일을저장할위치를선택하거나 새로추가를클릭하여나열되지않은파일위치를선택합니다. %XenMobile Folder%\ 또는%Flash Storage%\ 매크로를경로식별자의시작부분으로사용할수있습니다.
- 대상파일이름**:** 선택사항입니다. 장치에배포하기전에파일이름을변경해야하는경우파일이름을입력합니다.
- 파일이있는경우**:** 목록에서기존파일을복사할지여부를선택합니다. 기본값은 파일이다른경우에만복사입니다.

Android 설정

- 가져올파일**:** 찾아보기를클릭하고파일의위치로이동하여가져올파일을선택합니다.
- 파일형식**:** 파일또는 스크립트를선택합니다.
- 즉시실행**:** 스크립트를선택하면 즉시실행옵션이나타납니다. 이설정을활성화해도동작이실행되지않습니다. 사용자가스크립트를수동으로실행해야합니다. 매크로식바꾸기**:** 스크립트의매크로토큰이름을장치또는사용자속성으로바꿀지여부를선택합니다. 기본값은 꺼짐입니다.
- 대상폴더**:** 목록에서업로드된파일을저장할위치를선택하거나 새로추가를클릭하여나열되지않은파일위치를선택합니다. 또는%XenMobile Folder%\ 또는%Flash Storage%\ 매크로를경로식별자의시작부분으로사용할수있습니다.
- 대상파일이름**:** 필요에따라장치에배포하기전에이름을변경해야할경우파일에다른이름을입력합니다.
- 파일이다른경우에만복사**:** 목록에서기존파일과다른경우파일을복사할것인지여부를선택합니다. 기본값은다른경우에파일을복사하는것입니다.

FileVault 장치정책

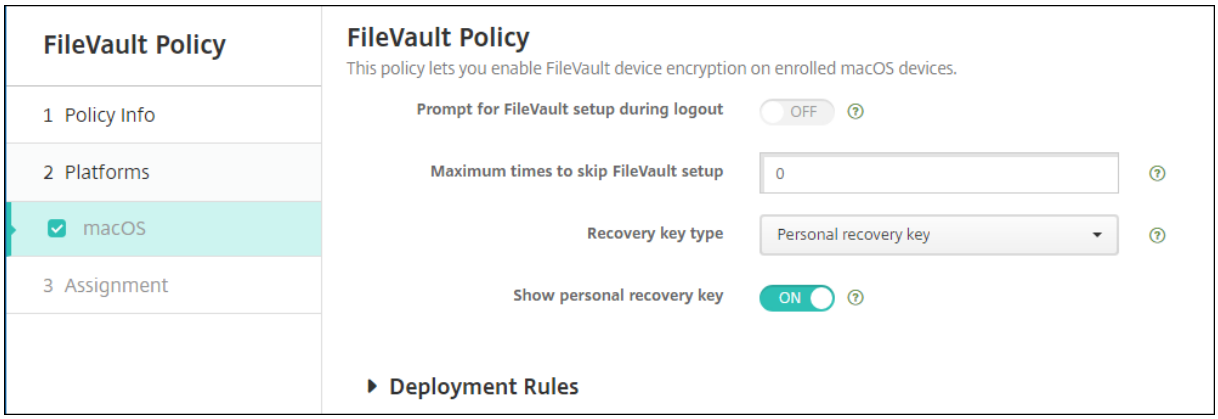
August 24, 2018

macOS FileVault 디스크암호화기능은시스템볼륨콘텐츠를암호화하여시스템볼륨을보호합니다. macOS 장치에서 FileVault 를사용하도록설정하면장치를시작할때마다사용자가계정암호를사용하여로그인해야합니다. 사용자가암호를잊은경우 복구키를사용하여디스크잠금을해제하고암호를재설정할수있습니다.

XenMobile 장치정책인 FileVault 는 FileVault 사용자설치화면을사용하도록설정하고복구키같은설정을구성합니다. FileVault 에대한자세한내용은 Apple 지원사이트 (https://support.apple.com) 를참조하십시오.

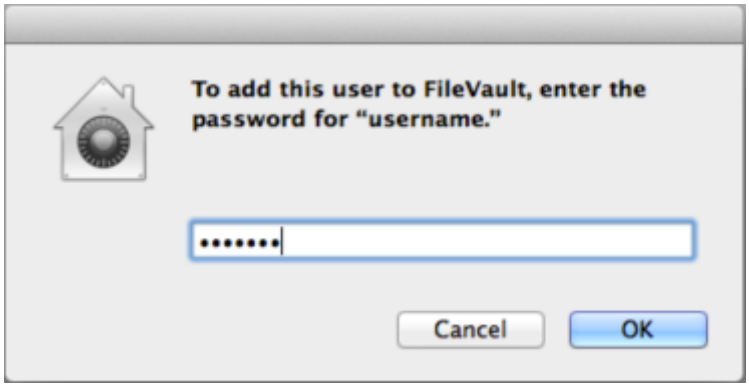
FileVault 정책을추가하려면 구성 **>** 장치정책으로이동합니다.

macOS 설정

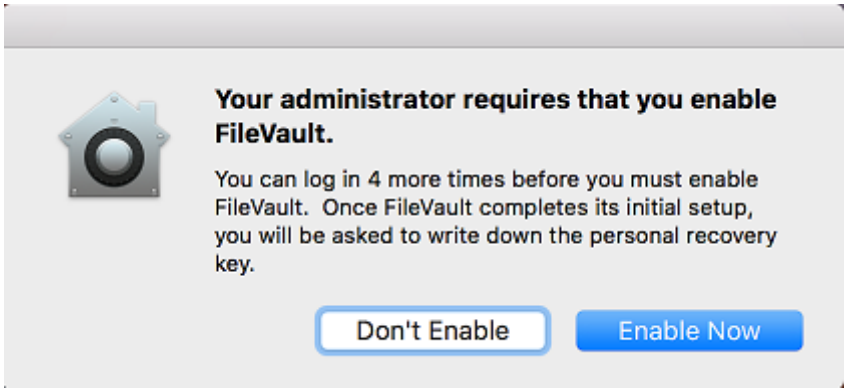


- 로그아웃도중 **FileVault** 설정에대해묻기**:** 켜짐인경우 **FileVault** 설정을건너뛸최대횟수옵션에지정된대로다음 N 번째로그아웃시 FileVault 를사용할지여부를묻는메시지를표시합니다. 꺼짐인경우 FileVault 암호확인메시지가표시되지않습니다.

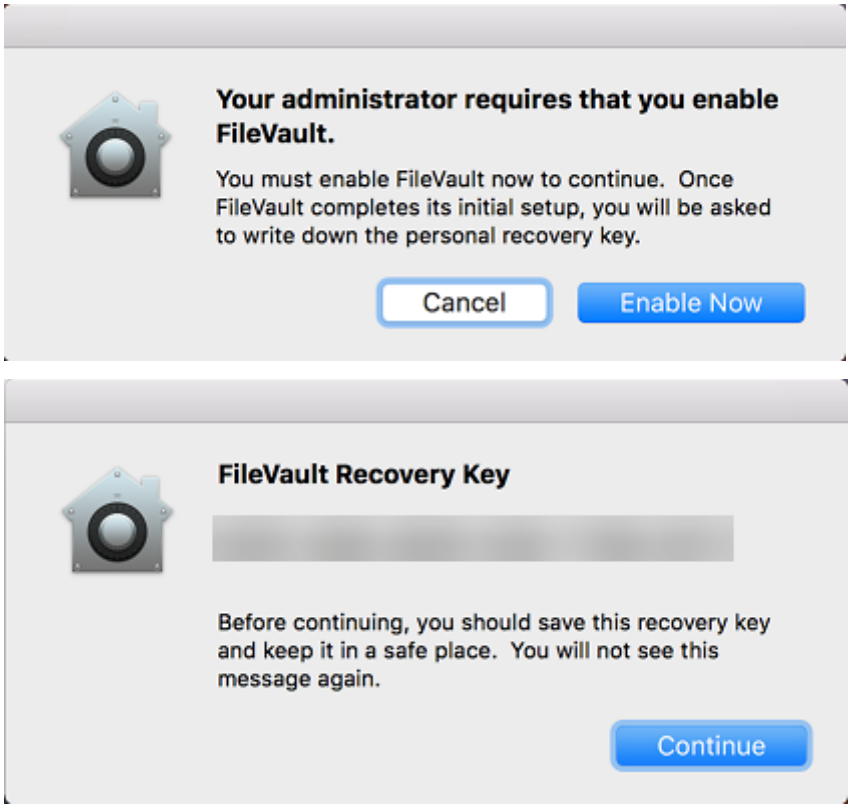
이설정을켜고 FileVault 정책을배포하면사용자가장치에서로그아웃할때다음화면이나타납니다. 이화면에는사용자가로그오프전에 FileVault 를사용하도록설정할수있는옵션이표시됩니다.



FileVault 설정을건너뛸최대횟수값이 0 이아닌경우: 이설정을끄고 FileVault 정책을배포하면사용자가로그온할때다음화면이나타납니다.



FileVault 설정을건너뛸최대횟수값이 0 이거나사용자가최대횟수로설정을건너뛴경우다음화면이나타납니다.



글꼴장치정책

January 5, 2022

iOS 및 macOS 장치에글꼴을더추가하는장치정책을 XenMobile 에서추가할수있습니다. 글꼴은트루타입 (.ttf) 또는오픈타입 (.oft) 형식이어야합니다. 글꼴모음 (.ttc 또는.otc) 은지원되지않습니다.

iOS 의경우, 이정책은 iOS 7.0 이상의버전에만적용됩니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 사용자에게표시되는이름**:** 글꼴목록에서사용자에게표시되는이름을입력합니다.
- 글꼴파일**:** 찾아보기를클릭하고파일의위치로이동하여사용자장치에추가할글꼴파일을선택합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.

    * 제거할때까지의기간 (시간): 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

macOS 설정

- 사용자에게표시되는이름: 글꼴목록에서사용자에게표시되는이름을입력합니다.
- 글꼴파일: 찾아보기를클릭하고파일의위치로이동하여사용자장치에추가할글꼴파일을선택합니다.
- 정책설정
  - 정책제거: 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 (시간) 입니다.
    * 날짜선택: 달력을클릭하여제거할특정날짜를선택합니다.
    * 제거할때까지의기간 (시간): 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용: 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위: 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

홈화면레이아웃장치정책

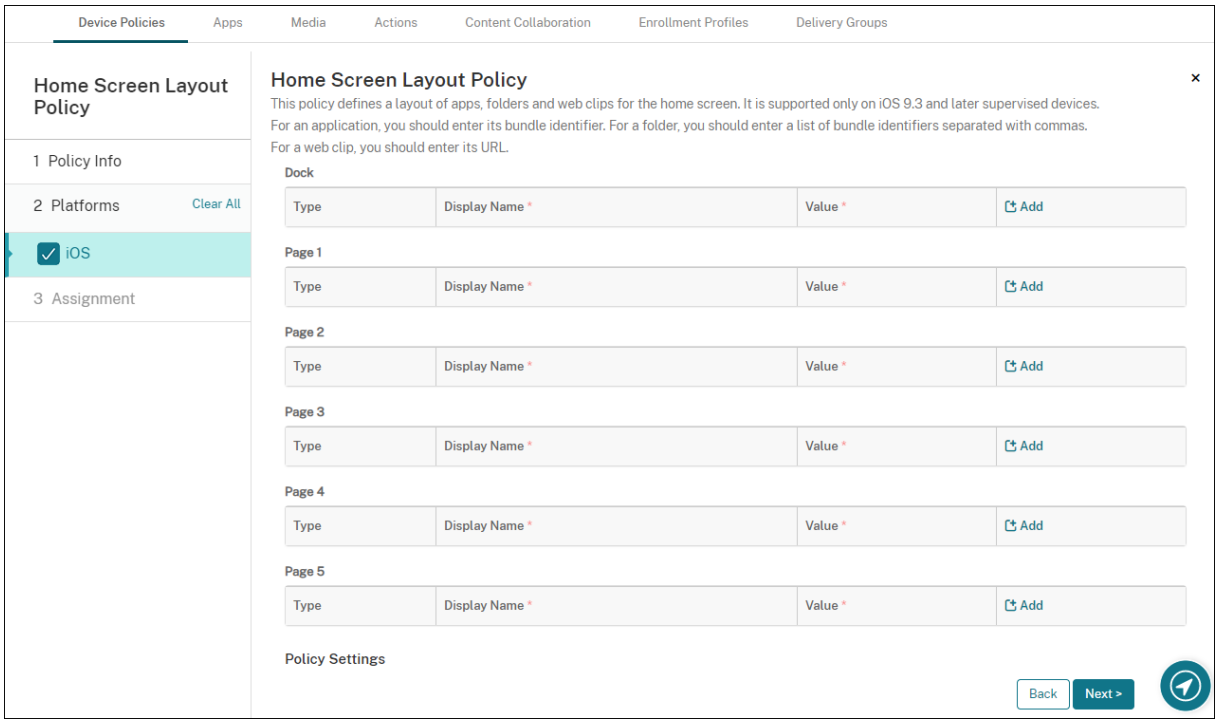
January 5, 2022

iOS 홈화면의앱및폴더레이아웃을지정할수있습니다. 홈화면레이아웃장치정책은 iOS 9.3 이상의감독되는장치에적용됩니다.

> 중요:
>
> 한장치에여러개의홈화면레이아웃정책을배포하면장치에서 iOS 오류가발생합니다. 이제한은이 XenMobile 정책또는 Apple Configurator 를통해홈화면을정의할때적용됩니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

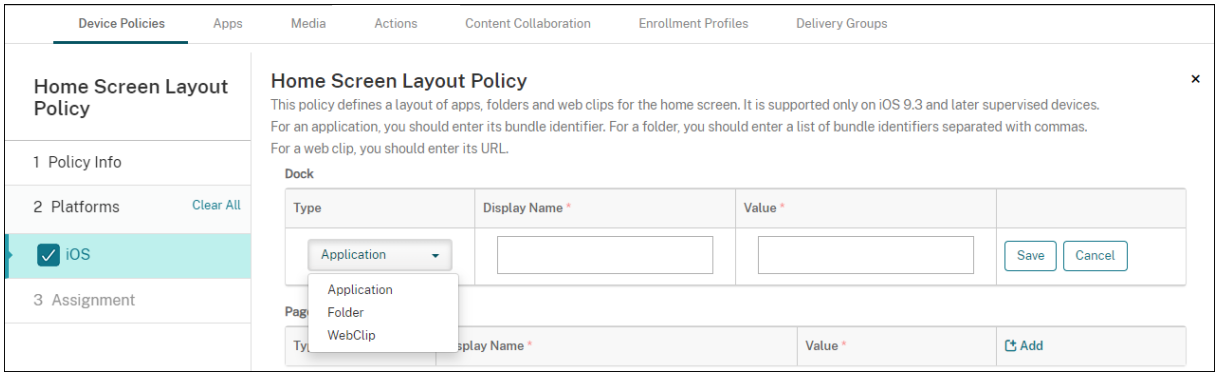
iOS 설정



- 구성할각화면영역 (예: **Dock** 또는 **1** 페이지) 에대해 추가를클릭합니다.
- 유형**:** 응용프로그램, 폴더또는 웹클립을선택합니다.

  제한장치정책의 제한된앱사용 **>** 일부앱만허용설정을사용하면웹클립이홈화면에올바르게표시되지않을수있습니다. 웹클립이올바르게표시되지않을경우다음중하나를수행합니다.

  - 제한된앱사용을 모든앱허용또는 일부앱허용안함으로설정합니다.
  - 제한된앱사용을 일부앱만허용으로설정한상태에서번들 ID `com.apple.webapp`로앱을추가하여웹클립을허용합니다.



- 표시이름**:** 홈화면에표시되는앱또는폴더의이름입니다.
- 값**:** 앱의경우번들식별자입니다. 폴더의경우쉼표로구분된번들식별자목록을입력합니다. 웹클립의경우번들 ID(`com.apple.webClip.managed`) 를입력하고웹클립정책에서웹클립 URL 을구성합니다. URL 이동일한웹클립값이둘이상인경우 iOS 11.3 이상인장치에서동작이정의되지않습니다.

- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 iOS 9.3 이상에서만사용할수있습니다.

iOS 및 macOS 프로필장치정책가져오기

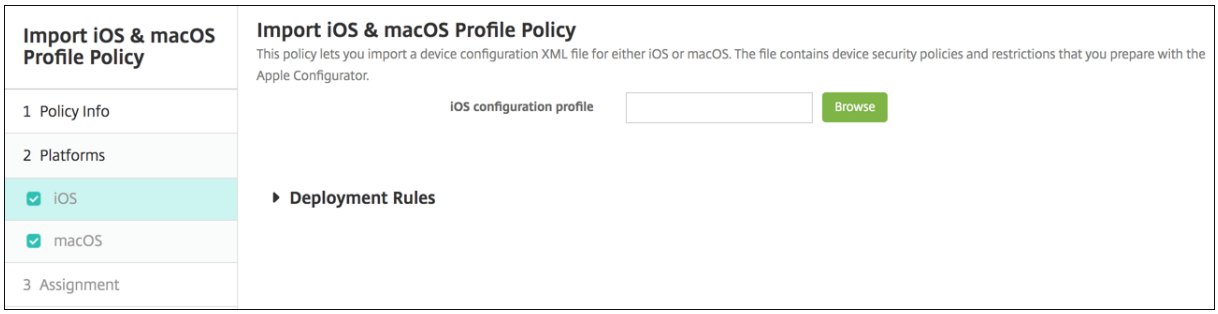
January 5, 2022

XenMobile 로 iOS 와 macOS 장치를위한장치구성 XML 파일을가져올수있습니다. 이파일에는 Apple Configurator 로작성한장치보안정책및제한사항이포함되어있습니다.

이문서의뒷부분에설명된대로 Apple Configurator 를사용하여 iOS 장치를감독모드로설정할수있습니다. Apple Configurator 를사용하여구성파일을만드는방법에대한자세한내용은 Apple Configurator 지원을참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 및 macOS 설정



- **iOS** 구성프로필또는 **macOS** 구성프로필**:** 가져올구성파일을선택하려면 찾아보기를클릭하고해당파일위치로이동합니다.

Apple Configurator 를사용하여 iOS 장치를감독모드로설정

Apple Configurator 를사용하려면 macOS 10.7.2 이상을실행하는 Apple 컴퓨터가필요합니다.

> 중요**:**
>
> 감독모드로장치를설정하면선택한버전의 iOS 가장치에설치되어이전에저장된사용자데이터또는앱이장치에서완전히초기

> 화됩니다.

1. iTunes 에서 Apple Configurator 를설치합니다.
2. Apple 컴퓨터에 iOS 장치를연결합니다.
3. Apple Configurator 를시작합니다. 감독을위해준비할장치가있다고표시됩니다.
4. 감독할장치를준비하려면:
    a) 감독컨트롤을 켜짐으로전환합니다. 정기적으로구성을다시적용하여장치에대한제어를지속적으로유지하려는경우 이설정을선택하는것이좋습니다.
    b) 필요에따라장치에이름을지정합니다.
    c) iOS 에서 최신을클릭하여설치할최신버전의 iOS 를검색합니다.
5. 장치를감독하도록준비할수있는상태가되면 **Prepare(**준비**)** 를클릭합니다.

Keyguard 관리장치정책

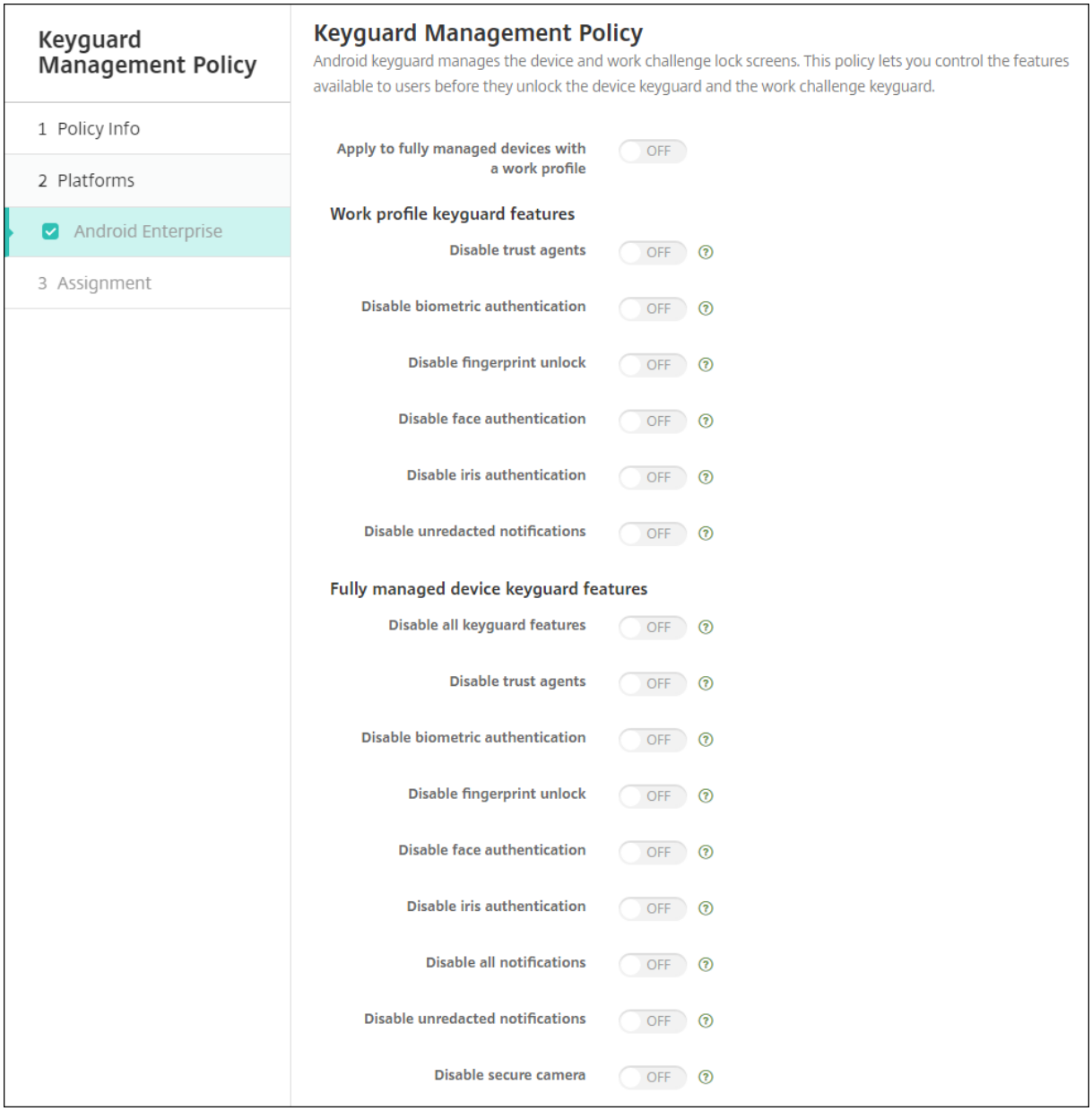
January 5, 2022

Android Keyguard 는장치및 Work Challenge 잠금화면을관리합니다. 이정책을통해 Android Enterprise 작업프로필 Keyguard 및고급장치 Keyguard 기능을관리할수있습니다. 다음을제어할수있습니다.

- 작업프로필장치의 Keyguard 관리. 사용자가장치 Keyguard 와 Work Challenge Keyguard 의잠금을해제하기 전에사용할수있는기능을지정할수있습니다. 예를들어, 기본적으로사용자는지문잠금해제를사용하고잠금화면에서수정되지않은알림을확인할수있습니다.
- 완전관리형전용장치의 Keyguard 관리. Keyguard 화면의잠금을해제하기전에신뢰할수있는에이전트, 보안카메라와 같이사용할수있는기능을지정할수있습니다. 또는모든 Keyguard 기능을사용하지않도록선택할수있습니다.
- 작업프로필로완전히관리되는장치의 Keyguard 관리. 하나의 Keyguard Management 정책을사용하여장치와작업 프로필에개별설정을적용할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Android Enterprise 설정



- 작업프로필로완전히관리되는장치에적용**:** 작업프로필로완전히관리되는장치에대해 Keyguard Management 장치정책설정을구성할수있도록허용합니다.

  이설정이 켜짐인경우별도의설정을장치와작업프로필로완전히관리되는장치의작업프로필에적용할수있습니다.

  이설정이 꺼짐인경우작업프로필장치와완전관리형장치에설정을적용할수있습니다. 작업프로필에구성한설정은작업프로필장치에만적용됩니다. 완전관리형장치에구성한설정은완전관리형장치에만적용됩니다.

  기본값은 꺼짐입니다.

- 작업프로필 **Keyguard** 기능**:** 사용자가작업프로필 Keyguard(잠금화면) 의잠금을해제하기전에다음기능을사용할수있는지를제어합니다.

  - 신뢰할수있는에이전트비활성화**:** 꺼짐인경우작업프로필에 Challenge 가설정되어있으면신뢰할수있는에이전트는보안 Keyguard 화면에서작동할수있습니다. 켜짐으로설정하면작업프로필의신뢰할수있는에이전트가모두비활성화됩니다. 기본값은 꺼짐입니다.
  - 생체인증비활성화**:** 꺼짐인경우작업프로필에 Challenge 가설정되어있으면보안 Keyguard 화면에서생체인증을사용할수있습니다. 켜짐으로설정하면작업프로필의생체인증이비활성화됩니다. 이설정은지문잠금해제, 안면인증, 홍채인증을비활성화합니다. 기본값은 꺼짐입니다. Android 9.0 이상에적용됩니다.
  - 지문잠금해제비활성화**:** 켜짐인경우작업프로필에 Challenge 가설정되어있으면보안 Keyguard 화면에서지문잠금해제를사용할수없습니다. 작업프로필에서지문잠금해제를사용하려면 꺼짐으로설정합니다. 기본값은 꺼짐입니다.
  - 안면인증비활성화**:** 꺼짐인경우작업프로필에 Challenge 가설정되어있으면보안 Keyguard 화면에서안면인증을사용할수있습니다. 켜짐으로설정하면작업프로필의안면인증이비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에적용됩니다.
  - 홍채인증비활성화**:** 꺼짐인경우작업프로필에 Challenge 가설정되어있으면보안 Keyguard 화면에서홍채인증을사용할수있습니다. 켜짐으로설정하면작업프로필의홍채인증이비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에적용됩니다.
  - 수정되지않은알림비활성화**:** 꺼짐인경우수정된알림과수정되지않은알림이모두보안 Keyguard 화면에표시됩니다. 켜짐으로설정하면수정되지않은알림이비활성화되고수정된알림만표시됩니다. 기본값은 꺼짐입니다.

- 완전관리형장치 **Keyguard** 기능**:** 사용자가장치 Keyguard(잠금화면) 의잠금을해제하기전에다음기능을사용할수있는지를제어합니다. 이러한기능은완전관리형장치나전용장치에적용됩니다.

  - 모든 **Keyguard** 기능비활성화**:** 꺼짐인경우현재및향후의모든 Keyguard 맞춤화를보안 Keyguard 화면에서사용할수있습니다. 켜짐으로설정하면모든 Keyguard 맞춤화가비활성화됩니다. 기본값은 꺼짐입니다.
  - 신뢰할수있는에이전트비활성화**:** 꺼짐인경우신뢰할수있는에이전트는보안 Keyguard 화면에서작동할수있습니다. 켜짐으로설정하면신뢰할수있는에이전트가비활성화됩니다. 기본값은 꺼짐입니다.
  - 생체인증비활성화**:** 꺼짐인경우장치에 Challenge 가설정되어있으면보안 Keyguard 화면에서생체인증을사용할수있습니다. 켜짐으로설정하면장치에서생체인증이비활성화됩니다. 이설정은지문잠금해제, 안면인증, 홍체인증을비활성화합니다. 기본값은 꺼짐입니다. Android 9.0 이상에적용됩니다.
  - 지문잠금해제비활성화**:** 꺼짐인경우장치에 Challenge 가설정되어있으면보안 Keyguard 화면에서지문잠금해제를사용할수있습니다. 켜짐으로설정하면장치에서지문잠금해제가비활성화됩니다. 기본값은 꺼짐입니다.
  - 안면인증비활성화**:** 꺼짐인경우장치에 Challenge 가설정되어있으면보안 Keyguard 화면에서안면인증을사용할수있습니다. 켜짐으로설정하면장치에서안면인증이비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에적용됩니다.
  - 홍채인증비활성화**:** 꺼짐인경우장치에 Challenge 가설정되어있으면보안 Keyguard 화면에서홍채인증을사용할수있습니다. 켜짐으로설정하면장치에서홍채인증이비활성화됩니다. 기본값은 꺼짐입니다. Android 9.0 이상에적용됩니다.
  - 모든알림비활성화**:** 꺼짐인경우모든알림이보안 Keyguard 화면에표시됩니다. 켜짐으로설정하면모든알림이표시됩니다. 기본값은 꺼짐입니다.
  - 수정되지않은알림비활성화**:** 꺼짐인경우수정된알림과수정되지않은알림이모두보안 Keyguard 화면에표시됩니다. 켜짐으로설정하면수정되지않은알림이비활성화되고수정된알림만표시됩니다. 기본값은 꺼짐입니다.
  - 보안카메라비활성화**:** 꺼짐인경우보안 Keyguard 화면에서보안카메라를사용할수있습니다. 켜짐으로설정하면보

안카메라가비활성화됩니다. 기본값은 꺼짐입니다.

키오스크장치정책

February 2, 2022

키오스크정책을사용하면실행할수있는앱을제한하여장치를키오스크모드로제한할수있습니다. 키오스크모드에서잠기는장치의부분은 XenMobile 을통해제어되지않습니다. 정책을배포한후장치에서키오스크모드설정을관리할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Samsung SAFE 장치를키오스크모드로만들려면

1. Samsung MDM 라이센스키장치정책에설명된대로모바일장치에서 Samsung SAFE API 키를사용하도록설정합니다. 이단계를통해 Samsung SAFE 장치에서정책을사용하도록설정할수있습니다.
2. Firebase Cloud Messaging에설명된대로 Android 장치에서 Firebase Cloud Messaging 을사용하도록설정합니다. 이단계를통해 Android 장치가다시 XenMobile 에연결될수있습니다.
3. 다음섹션에설명된대로키오스크장치정책을추가합니다.
4. 이세가지장치정책을적절한배달그룹에할당합니다. 배달그룹에앱인벤토리와같은다른정책을포함할지여부를고려합니다.

   키오스크모드에서장치를제거하려면 키오스크모드가 사용안함으로설정된키오스크장치정책을만듭니다. 배달그룹을업데이트하여키오스크모드를사용하도록설정한키오스크정책을제거하고키오스크모드를사용하지않도록설정한키오스크정책을추가합니다.

키오스크장치정책을추가하려면

키오스크모드에서지정하는모든앱은사용자의장치에이미설치되어있어야합니다.

일부옵션은 Samsung MDM(모바일기기관리) API 4.0 이상에만적용됩니다.

Samsung SAFE 설정

특정앱만사용할수있도록지정할수있습니다. 이정책은특정유형또는클래스의앱만실행하도록마련된회사장치에유용합니다. 또한이정책을사용하면장치가키오스크모드상태일때장치홈화면및잠금화면배경에대한사용자지정이미지를선택할수있습니다.

- 키오스크모드**:** 사용또는 사용안함을클릭합니다. 기본값은 사용입니다. 사용안함을클릭하면다음옵션이모두사라집니다.
- **Launcher** 패키지**:** 사용자가하나이상의키오스크앱을열수있는사내 Launcher 를개발하지않는경우이필드를비워두는것이좋습니다. 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 꺼짐으로설정하면공통 SAFE 암호필드를변경할수없습니다. 기본값은 꺼짐입니다.
- 공통 **SAFE** 암호**:** 모든 Samsung SAFE 장치에대해일반암호정책을설정한경우이필드에해당암호를입력합니다.
- 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

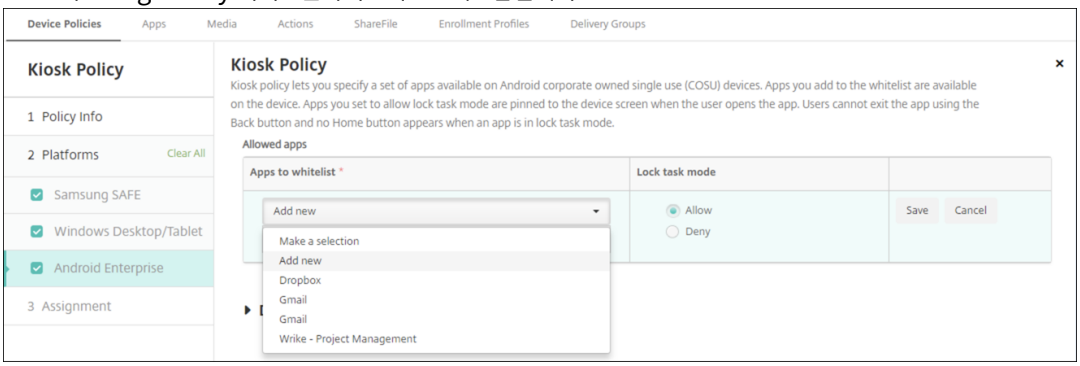
COSU(회사소유일회사용) 장치라고도하는전용 Android Enterprise 장치의경우앱을허용하고작업잠금모드를설정할수있습니다. 기본적으로 Secure Hub 와 Google Play 서비스는허용목록에포함됩니다.

앱을허용하려면 추가를클릭합니다. 여러앱을허용할수있습니다. 자세한내용은 Android Enterprise를참조하십시오.

> 참고**:**
>
> XenMobile Server 콘솔에는 “블랙리스트” 와 “화이트리스트” 라는용어가포함되어있습니다. 향후릴리스에서이러한용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.

- 화이트리스트에추가할앱**:** 화이트리스트에추가할앱의패키지이름을입력하거나목록에서앱을선택합니다.
  - 새로추가를클릭하여목록에표시할승인된앱의패키지이름을입력합니다.
  - 목록에서기존앱을선택합니다. 목록에는 XenMobile Server 에업로드된앱이표시됩니다. 기본적으로 Secure

Hub 와 Google Play 서비스는화이트리스트에포함됩니다.



- 작업잠금모드**:** 사용자가앱을시작할때장치화면에앱이고정되도록설정하려면 허용을선택합니다. 앱이고정되지않도록설정하려면 거부를선택합니다. 기본적으로 Secure Hub 와 Google Play 서비스는허용됩니다. 기본값은 허용입니다.

앱이작업잠금모드에있으면사용자가앱을열때앱이장치화면에고정됩니다. 홈단추가나타나지않고뒤로단추가비활성화됩니다. 사용자는로그아웃과같이앱에프로그래밍된작업을사용하여앱을종료할수있습니다.

Launcher 구성장치정책

September 29, 2021

Citrix Launcher 를사용하면 XenMobile 에의해배포되는 Android 장치의사용자환경을사용자지정할수있습니다. Citrix Launcher 및 Launcher 구성장치정책은 Android Enterprise 와호환되지않습니다.

Launcher 구성정책을추가하여이러한 Citrix Launcher 기능을제어할수있습니다.

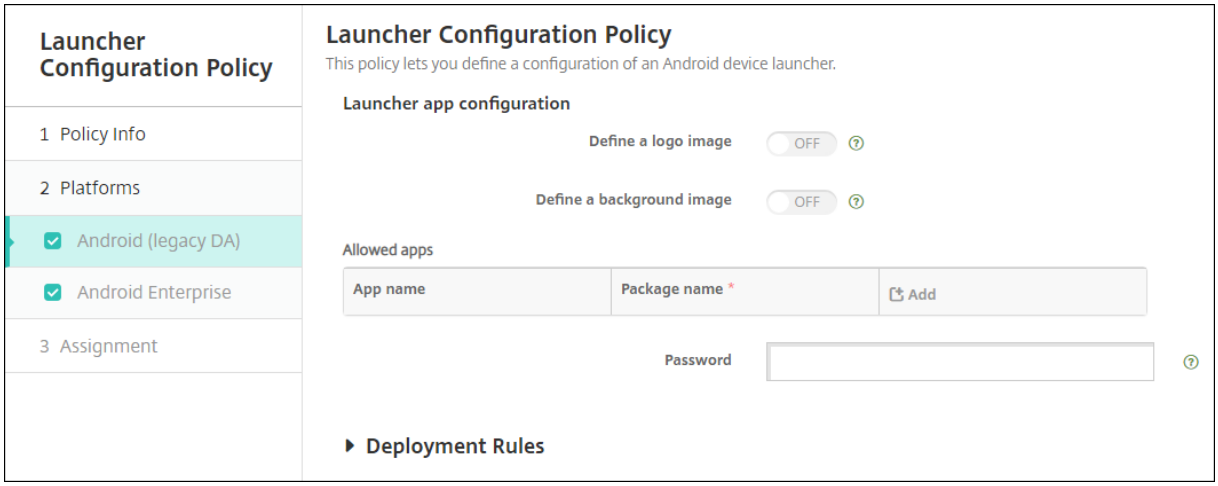
- 사용자가지정된앱에만액세스할수있도록 Android 장치를관리합니다.
- 필요에따라 Citrix Launcher 아이콘의사용자지정로고이미지와 Citrix Launcher 의사용자지정배경이미지를지정합니다.
- 사용자가 Launcher 를종료할때입력해야하는암호를지정합니다.

Citrix Launcher 를사용하면이러한장치수준제한을적용하는동시에사용자가 WiFi 설정, Bluetooth 설정및장치암호설정과같은장치설정에기본적으로액세스하여유연하게운영할수있습니다. Citrix Launcher 는장치플랫폼이이미제공하는보안에추가적인보안계층을더하기위한것이아닙니다.

Citrix Launcher 를배포하면 XenMobile 이 Launcher 를설치하고기본 Android Launcher 를대체합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Android(레거시 DA) 및 Android Enterprise 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.
  - 추가할새앱**:** 추가할앱의전체이름을입력합니다. 예를들어 Android 일정앱의경우 com.android.calendar 를입력합니다.
  - 저장을클릭하여앱을추가하거나 취소를클릭하여앱추가를취소합니다.
- 암호**:** Citrix Launcher 를종료할때사용자가입력해야하는암호입니다.

LDAP 장치정책

January 5, 2022

XenMobile 에서 iOS 장치에대한 LDAP 정책을만들어사용할 LDAP 서버에대한정보 (예: 필요한계정정보등) 를제공할수있습니다. 또한 LDAP 서버를쿼리할때사용할 LDAP 검색정책집합을제공합니다.

이정책을구성하려면 LDAP 호스트이름이필요합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 계정설명**:** 선택적계정설명을입력합니다.

- 계정사용자이름**:** 선택적사용자이름을입력합니다.
- 계정암호**:** 선택적암호를입력합니다. 이필드는암호화된프로필에만사용합니다.
- **LDAP** 호스트이름**:** LDAP 서버호스트이름을입력합니다. 이것은필수필드입니다.
- **SSL** 사용**:** LDAP 서버에대한 Secure Socket Layer 연결을사용할지여부를선택합니다. 기본값은 켜짐입니다.
- 검색설정**:** LDAP 서버에쿼리할때사용할검색설정을추가합니다. 원하는수의검색설정을추가할수있지만계정을유용하게사용하려면적어도하나이상의검색설정을추가해야합니다. 추가를클릭하고다음을수행합니다.
  - 설명**:** 검색설정의설명을입력합니다. 이것은필수필드입니다.
  - 범위**:** 기준, 한수준또는 하위트리를선택하여검색할 LDAP 트리의깊이를정의합니다. 기본값은 기준입니다.
    - 기준은검색기준이가리키는노드를검색합니다.
    - 한수준은기준노드와한수준아래노드를검색합니다.
    - 하위트리는기준노드와모든하위노드를깊이에관계없이검색합니다.
  - 검색기준**:** 검색을시작할노드에대한경로를입력합니다. 예를들어 ou=people 또는 0=example corp 을입력합니다. 이것은필수필드입니다.
  - 저장을클릭하여검색설정을추가하거나 취소를클릭하여검색설정추가를취소합니다.
  - 추가할각검색설정에대해이단계를반복합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

macOS 설정

- 계정설명**:** 선택적계정설명을입력합니다.
- 계정사용자이름**:** 선택적사용자이름을입력합니다.
- 계정암호**:** 선택적암호를입력합니다. 이필드는암호화된프로필에만사용합니다.
- **LDAP** 호스트이름**:** LDAP 서버호스트이름을입력합니다. 이것은필수필드입니다.
- **SSL** 사용**:** LDAP 서버에대한 Secure Socket Layer 연결을사용할지여부를선택합니다. 기본값은 켜짐입니다.
- 검색설정**:** LDAP 서버에쿼리할때사용할검색설정을추가합니다. 원하는수의검색설정을추가할수있지만계정을유용하게사용하려면적어도하나이상의검색설정을추가해야합니다. 추가를클릭하고다음을수행합니다.
  - 설명**:** 검색설정의설명을입력합니다. 이것은필수필드입니다.
  - 범위**:** 기준, 한수준또는 하위트리를선택하여검색할 LDAP 트리의깊이를정의합니다. 기본값은 기준입니다.
    - 기준은검색기준이가리키는노드를검색합니다.
    - 한수준은기준노드와한수준아래노드를검색합니다.
    - 하위트리는기준노드와모든하위노드를깊이에관계없이검색합니다.
  - 검색기준**:** 검색을시작할노드에대한경로를입력합니다. 예를들어 ou=people 또는 0=example corp 을입력합니다. 이것은필수필드입니다.
  - 저장을클릭하여검색설정을추가하거나 취소를클릭하여검색설정추가를취소합니다.
  - 추가할각검색설정에대해이단계를반복합니다.

- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

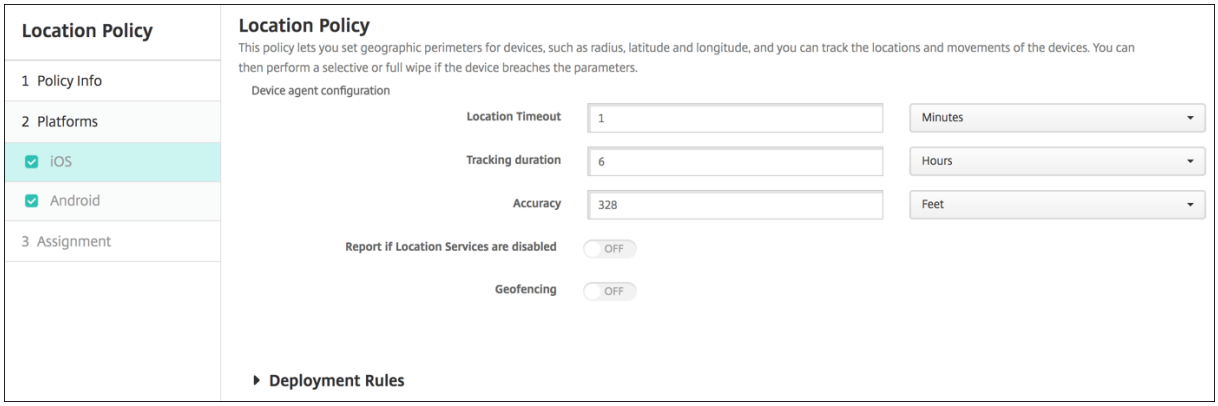
위치장치정책

January 5, 2022

XenMobile 에서위치장치정책을만들어지리적경계를적용할수있습니다. 사용자가정의된경계 (지오펜스라고도함) 를위반하면 XenMobile 이특정동작을수행할수있습니다. 예를들어사용자가정의된경계를위반할경우사용자에게경고메시지를보내도록정책을구성할수있습니다. 사용자가경계를위반할경우즉시또는지연후에사용자의회사데이터를초기화하는정책을구성할수있습니다. 장치추적및찾기사용여부와같은보안조치에대한자세한내용은 보안동작을참조하십시오.

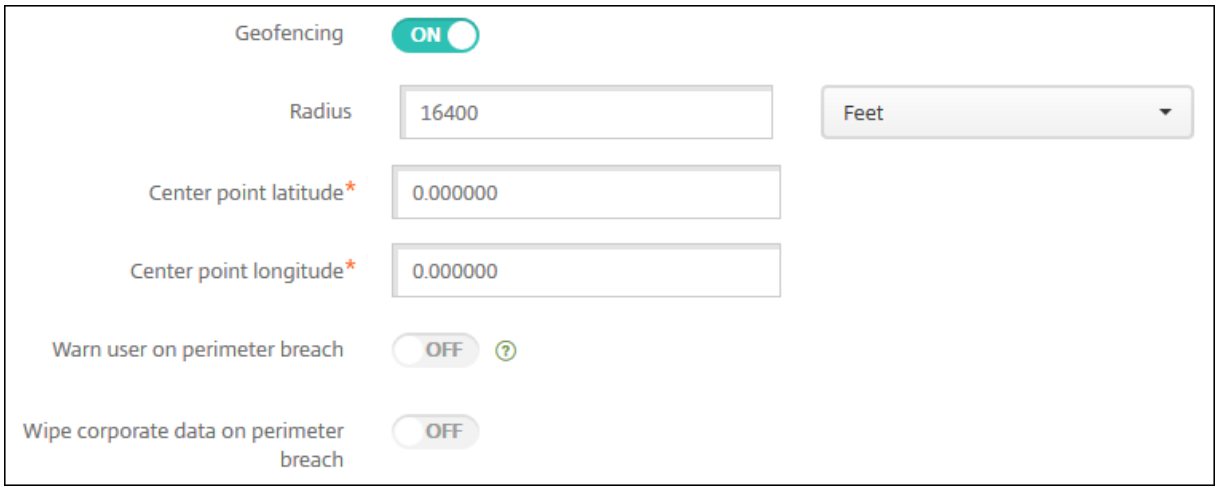
이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



- 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.

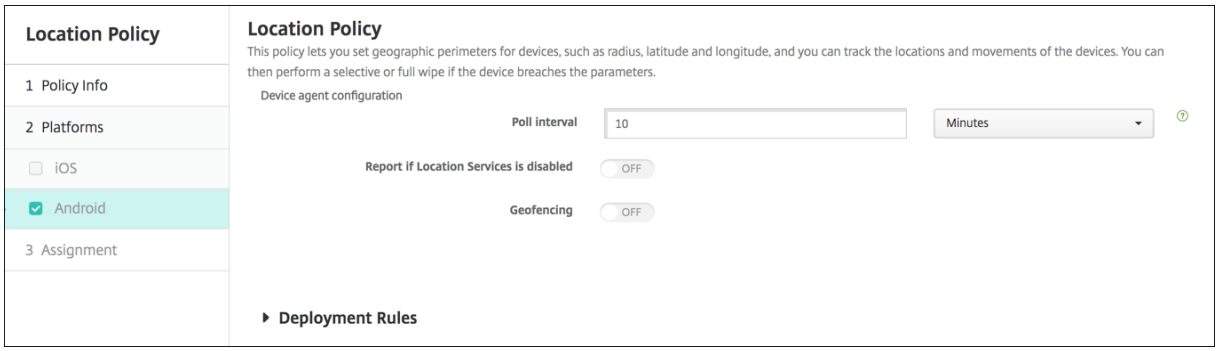
- 위치서비스가사용하지않도록설정될경우보고**:** GPS 를사용하지않을때장치가 XenMobile 에보고서를보낼지여부를선택합니다. 기본값은 꺼짐입니다.
- 지오펜스



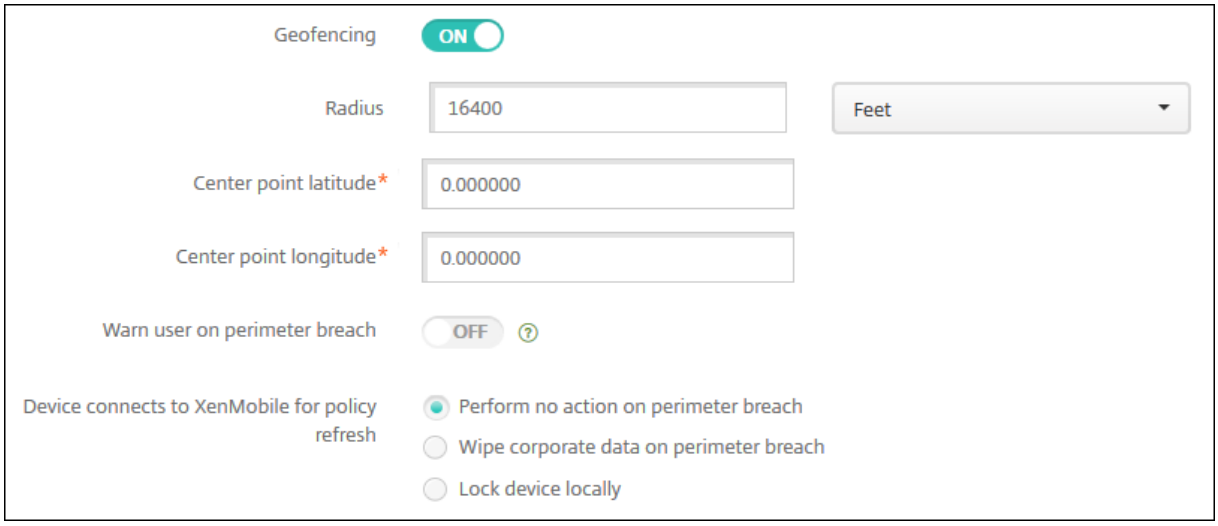
지오펜스를사용하도록설정한경우다음설정을구성합니다.

- 반경**:** 숫자를입력한다음목록에서반경을측정하는데사용할단위를클릭합니다. 기본값은 16,400 피트입니다. 유효한반경은다음과같습니다.
  - 164~164,000 피트
  - 50~50,000 미터
  - 54~54,680 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. 이설정은 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.
- 지오펜스



지오펜스를사용하도록설정한경우다음설정을구성합니다.

- 반경**:** 숫자를입력한다음목록에서반경을측정하는데사용할단위를클릭합니다. 기본값은 16,400 피트입니다. 유효한반경은다음과같습니다.
  - 164~164,000 피트
  - 1~50 킬로미터
  - 50~50,000 미터
  - 54~54,680 야드
  - 1~31 마일
- 중심점위도**:** 위도 (예: 37.787454) 를입력하여지오펜스중심점의위도를정의합니다.
- 중심점경도**:** 경도 (예: 122.402952) 를입력하여지오펜스중심점의경도를정의합니다.
- 경계위반시사용자에게경고표시**:** 사용자가정의된경계를위반할경우경고메시지를발행할지여부를선택합니다. 기본값은

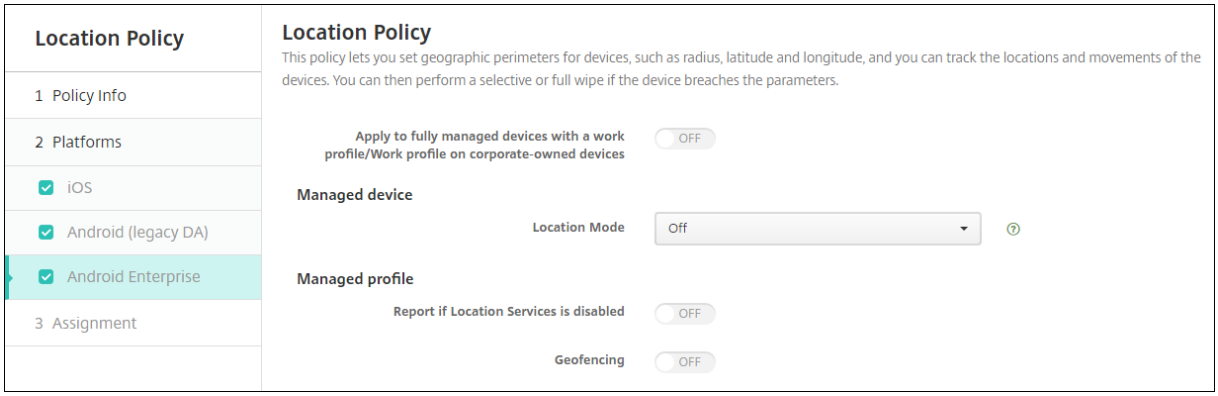
꺼짐입니다. 경고메시지를표시하는데에는 XenMobile 연결이필요하지않습니다.

- 정책새로고침을위해장치가 **XenMobile** 에연결**:** 사용자가경계를위반한경우에대해다음옵션중하나를선택합니다.
  - 경계위반시아무런동작을수행하지않음**:** 아무작업도하지않습니다. 이설정은기본값입니다.
  - 경계위반시회사데이터초기화**:** 지정된시간이지난후회사데이터를초기화합니다. 이옵션을사용하도록설정하면 로컬초기화시지연필드가나타납니다.
    * 숫자를입력한다음목록에서초또는분을클릭하여사용자의장치에서회사데이터를초기화하기전에대기할기간을설정합니다. 이설정은 XenMobile 이사용자의장치를선택적으로초기화하기전에사용자가허용된위치로돌아갈수있는기회를제공합니다. 기본값은 0 초입니다.
  - 잠금시지연**:** 지정된시간이지난후사용자의장치를잠급니다. 이옵션을사용하도록설정하면 잠금시지연필드가나타납니다.
    * 숫자를입력한다음목록에서초또는분을클릭하여사용자의장치를잠그기전에대기할기간을설정합니다. 이설정은 XenMobile 이사용자의장치를잠그기전에사용자가허용된위치로돌아갈수있는기회를제공합니다. 기본값은 0 초입니다.

Android Enterprise 설정

Android 위치추적이작동하려면다음요구사항을충족해야합니다.

- Android 8.5 이상
- Android Enterprise 의제한장치정책에서위치공유허용설정사용설정됨
- 연결예약 (Firebase Cloud Messaging 권장)



작업프로필로완전히관리되는장치에적용

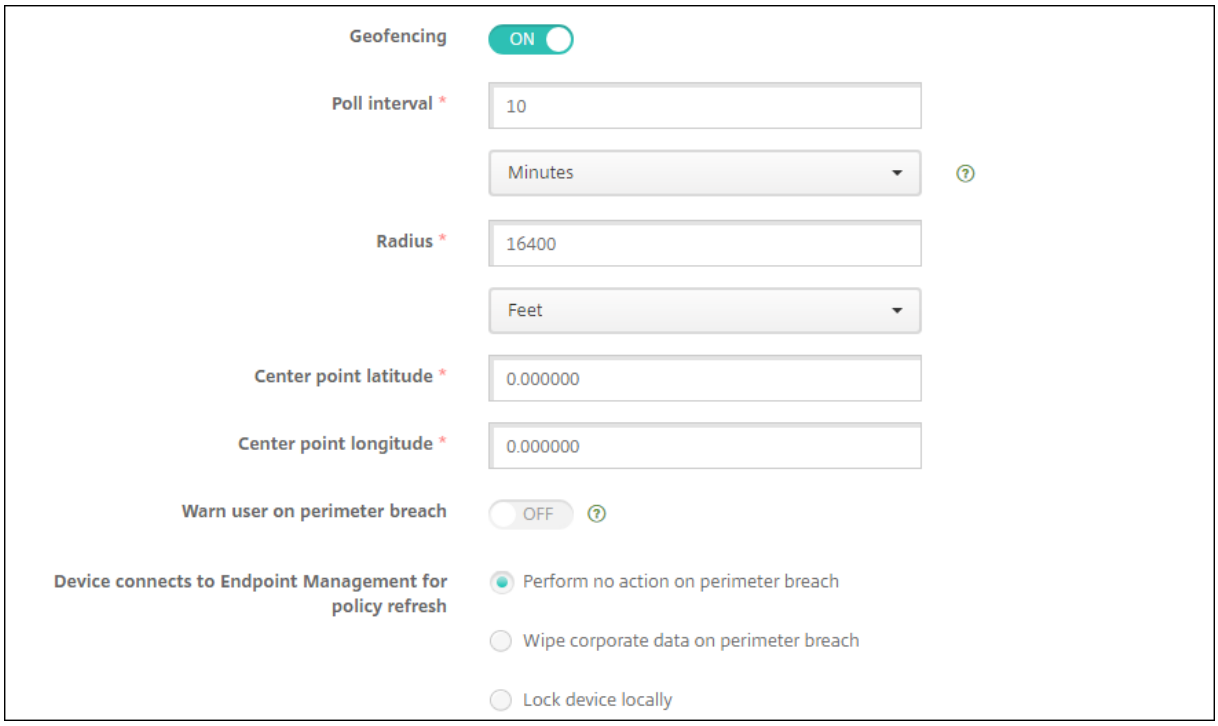
작업프로필로완전히관리되는장치의경우위치모드설정을사용할수있습니다.

- 작업프로필/회사소유장치의작업프로필을사용하는완전관리형장치에적용**:** 작업프로필로완전히관리되는장치에대해위치모드를구성할수있도록허용합니다. 이설정이켜져있으면작업프로필에대한위치모드설정을구성합니다.
  - 위치서비스가사용하지않도록설정될경우보고**:** 사용자가 GPS 를끈경우장치에서 XenMobile Server 에보고서를보낼지여부를선택합니다. 기본값은 꺼짐입니다.
  - 지오펜스**:** 관리되는장치에서이문서의설정을참조하십시오.

작업프로필/회사소유장치의작업프로필을사용하는완전관리형장치에적용이꺼짐이면다음섹션에표시된것과같이관리되는장치와작업프로필에설정이적용됩니다. 기본값은 꺼짐입니다.

관리되는장치

- 위치모드**:** 사용할위치검색의수준을지정합니다. 위치모드가높은정확도또는배터리절약으로설정된경우에만찾기보안동작을사용할수있습니다. 기본값은높은정확도입니다.
  - 높은정확도**:** GPS, 네트워크및기타센서를포함한모든위치검색방법을사용하도록설정합니다.
  - 센서만**:** GPS 및기타센서만사용하도록설정합니다.
  - 배터리절약**:** 네트워크위치공급자만사용하도록설정합니다.
  - 꺼짐**:** 위치검색을사용하지않습니다.
- 지오펜스**:**



지오펜스를사용하도록설정한경우다음설정을구성합니다.

- 폴링간격**:** 숫자를입력한다음 분, 시간또는 일을클릭하여 XenMobile Server 가장치의위치를수정하려고시도하는빈도를설정합니다. 유효한값은 1~1440 분, 1~24 시간또는일수입니다. 기본값은 **10** 분입니다. 이값을 10 분미만으로설정하면장치의배터리수명이저하될수있습니다.
- 반경**:** 숫자를입력한다음반경을측정하는데사용할단위를클릭합니다. 기본값은 **5,000** 미터 (**16,400** 피트) 입니다. 유효한반경은다음과같습니다.
  - 164~164,000 피트
  - 1~50 킬로미터
  - 50~50,000 미터

  - 54~54,680 야드
  - 1~31 마일

- 중심점위도**:** 위도 (예: 37.787454) 를입력하여지오펜스중심점의위도를정의합니다. 값을조회하려면 관리 **>** 장치에서장치를선택하고 보안을클릭한다음 찾기를클릭합니다. 장치를찾은후 XenMobile Server 는 보안아래의장치 세부정보 **>** 일반페이지에장치위치를보고합니다.
- 중심점경도**:** 경도 (예: 122.402952) 를입력하여지오펜스중심점의경도를정의합니다.
- 경계위반시사용자에게경고표시**:** 사용자가정의된경계를위반할경우경고메시지를발행할지여부를선택합니다. 기본값은 꺼짐입니다. 경고메시지를표시하는데에는 XenMobile Server 연결이필요하지않습니다.
- 정책새로고침을위해장치가 **XenMobile Server** 에연결**:** 사용자가경계를위반한경우에대해다음옵션중하나를선택합니다.
  - 경계위반시아무런동작을수행하지않음**:** 아무작업도하지않습니다. 이설정은기본값입니다.
  - 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 를끈경우장치에서 XenMobile Server 에보고서를보낼지여부를선택합니다. 기본값은 꺼짐입니다.
- 지오펜스**:** 관리되는장치에서이문서의설정을참조하십시오.

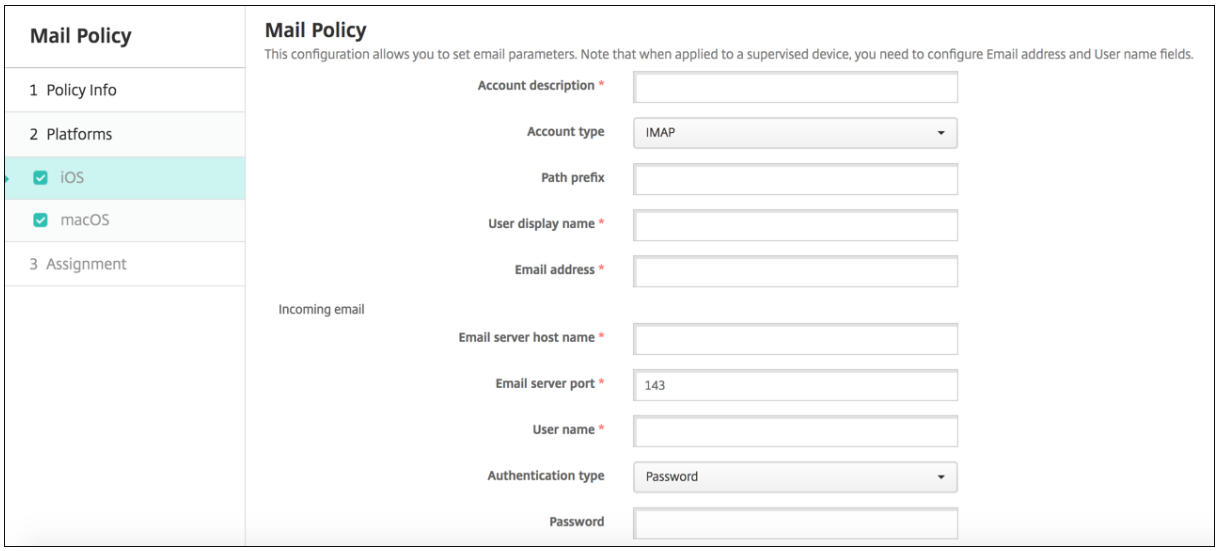
메일장치정책

January 5, 2022

XenMobile 에서메일장치정책을추가하여 iOS 또는 macOS 장치에서전자메일계정을구성할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 및 macOS 설정



- 계정설명**:** 메일및설정앱에나타나는계정설명을입력합니다. 이것은필수필드입니다.
- 계정유형**: IMAP** 또는 **POP** 를선택하여사용자계정에사용할프로토콜을선택합니다. 기본값은 **IMAP** 입니다. **POP** 를선택하면다음 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. 기본값은꺼짐입니다.
- 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. 이옵션은 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 서명을켜거나끌수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
    * **S/MIME** 서명인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서사용할서명자격증명을선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 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 암호화를켜거나끌수있는옵션이표시됩니다. 기본값은 꺼짐입니다.
    * 기본적으로 **S/MIME** 암호화사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 를기본적으로켤지여부를선택할수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.
    * **S/MIME** 암호화인증서 **UUID** 사용자재정의가능**:** 켜짐으로설정하면사용자가장치설정에서 S/MIME 암호화 ID 및암호화를켜거나끌수있습니다. 기본값은 꺼짐입니다. 이옵션은 iOS 12.0 이상에적용됩니다.

- 정책설정
  - 정책제거**:** 나중에정책을제거하려면 날짜선택또는 제거할때까지의기간 **(**시간**)** 에서정책을제거하도록이설정을구성하면됩니다.
  - 사용자가정책을제거하도록허용**:** 사용자가메일정책을제거하는것을 항상허용하거나, 암호필요로만허용하거나 안함으로설정합니다.
  - 프로필범위**:** macOS 에한해정책을 사용자수준별로적용할지전체 시스템에적용할지를선택합니다.

관리되는구성정책

May 6, 2022

관리되는구성장치정책은다양한앱구성옵션과앱제한을제어합니다. 앱개발자는앱에서사용할수있는옵션과도구설명을정의합니다. 도구설명에 "템플릿값" 사용이언급되는경우해당하는 XenMobile 매크로를대신사용합니다. 자세한내용은 원격구성개

요(Android 개발자사이트) 및 매크로를참조하십시오.

앱구성설정에는다음과같은항목이포함될수있습니다.

- 앱전자메일설정
- 웹브라우저의 URL 허용또는차단
- 셀룰러연결을통해또는 Wi-Fi 연결을통해서만앱콘텐츠동기화를제어하는옵션

앱에대해표시되는설정에대한자세한내용은앱개발자에게문의하십시오.

사전요구사항

- Google 에서 Android Enterprise 설정작업을완료하고 Android Enterprise 를관리되는 Google Play 에연결합니다. 자세한내용은 Android Enterprise를참조하십시오.
- XenMobile 에 Android Enterprise 앱을추가합니다. 자세한내용은 XenMobile 에앱추가를참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

앱별 **VPN** 에대한요구사항

AE 에대한앱별 VPN 을만들려면관리되는구성정책을구성하는것외에도추가단계를수행해야합니다. 또한다음사전요구사항도충족하는지확인해야합니다.

- 온프레미스 Citrix Gateway
- 다음응용프로그램이장치에설치됩니다.
  - Citrix SSO
  - Citrix Secure Hub

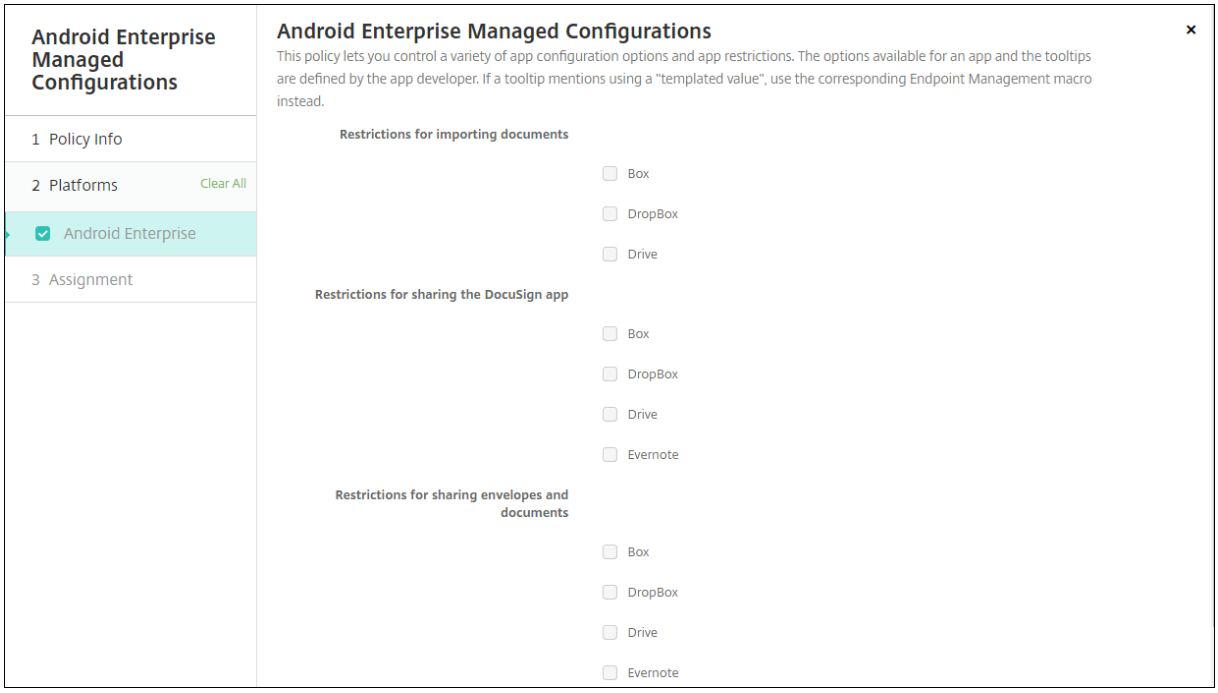
AE 장치에대한앱별 VPN 을구성하는일반적인워크플로는다음과같습니다.

1. 이문서에설명된대로 VPN 프로필을구성합니다.
2. 앱별 VPN 에서트래픽을허용하도록 Citrix ADC 를구성합니다. 자세한내용은 Citrix Gateway 에서전체 VPN 설정을참조하십시오.

Android Enterprise 설정

관리되는구성장치정책을추가하도록선택하면앱을선택하라는메시지가나타납니다. XenMobile 에추가된 Android Enterprise 앱이없는경우계속진행할수없습니다.

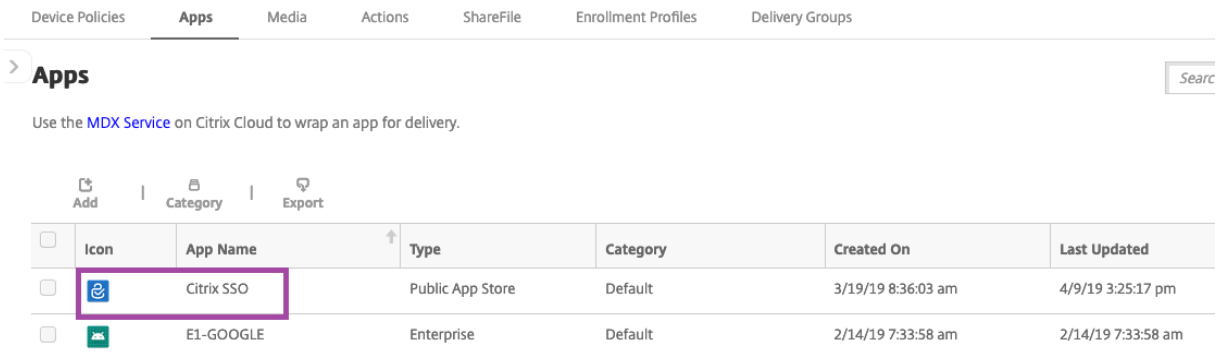
앱을선택한후정책설정을구성합니다. 설정은각앱마다다릅니다.



Android Enterprise 에대한 **VPN** 프로필구성

Citrix SSO 앱과관리되는구성장치정책을사용하여 Android Enterprise 장치에서사용할수있는 VPN 프로필을제공합니다.

먼저 Citrix SSO 를 Google Play Store 앱으로 XenMobile 콘솔에추가합니다. 공개앱스토어앱추가를참조하십시오.



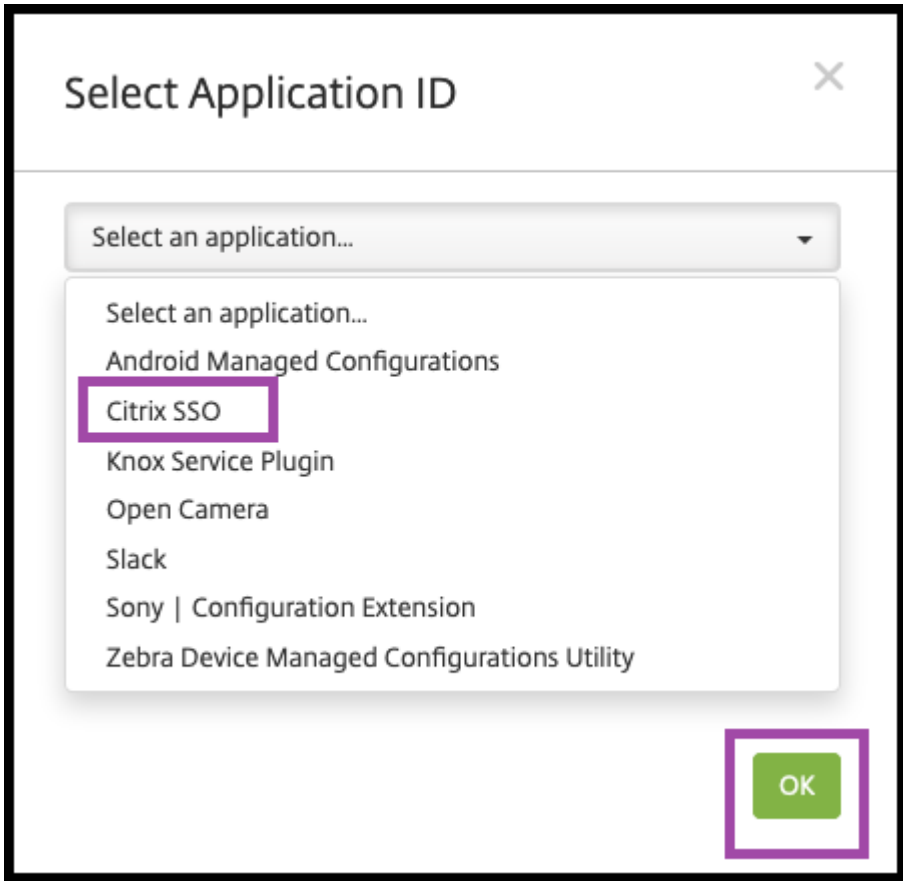
Citrix SSO 에대한 **Android Enterprise** 관리되는구성만들기

Citrix SSO 에대한관리되는구성장치정책을구성하여 VPN 프로필을만듭니다. 만든 VPN 프로필에는 Citrix SSO 앱이설치되고정책이배포된장치에서액세스할수있습니다.

Citrix Gateway FQDN 및포트가필요합니다.

1. XenMobile 콘솔에서 구성 **>** 장치정책을클릭합니다. 추가를클릭합니다.
2. **Android Enterprise** 를선택합니다. 관리되는구성을클릭합니다.

3. 응용프로그램 **ID** 선택창이나타나면목록에서 **Citrix SSO** 를선택하고 확인을클릭합니다.



4. Citrix SSO VPN 구성에대한이름과설명을입력합니다. 다음을클릭합니다.

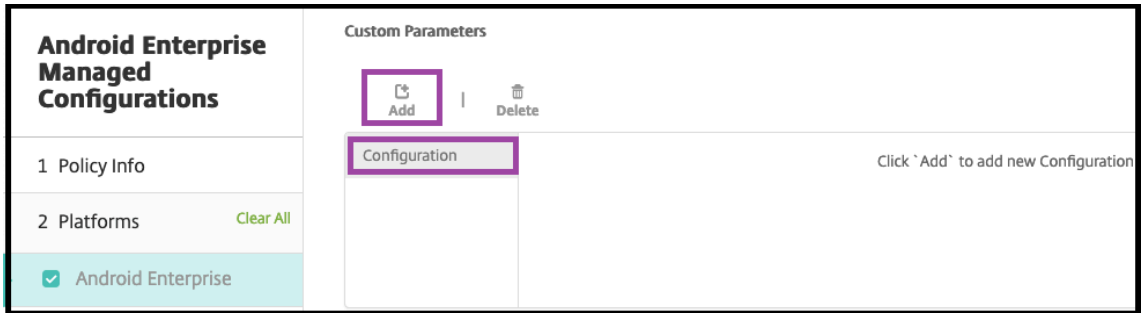
5. VPN 프로필매개변수를구성합니다.

   - **VPN** 프로필이름**.** VPN 프로필의이름을입력합니다. 둘이상의 VPN 프로필을만드는경우각각에대해고유한이름

을사용합니다. 이름을제공하지않으면 서버주소필드에입력한주소가 VPN 프로필이름으로사용됩니다.

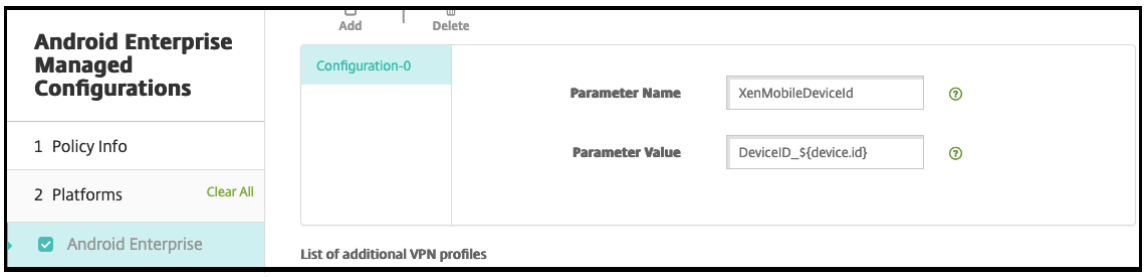
- 서버주소 **(*).** Citrix Gateway FQDN 을입력합니다. Citrix Gateway 포트가 443 이아닌경우해당포트를입력합니다. URL 형식을사용합니다. 예:`https://gateway.mycompany.com:8443`.
- 사용자이름 **(**선택사항**).** 최종사용자가 Citrix Gateway 에인증할때사용하는사용자이름을제공합니다. 이필드에 XenMobile 매크로 {user.username} 을사용할수있습니다. 매크로를참조하십시오. 사용자이름을제공하지않으면사용자가 Citrix Gateway 에연결할때사용자이름을제공하라는메시지가표시됩니다.
- 암호 **(**선택사항**).** 최종사용자가 Citrix Gateway 에인증할때사용하는암호를제공합니다. 암호를제공하지않으면사용자가 Citrix Gateway 에연결할때암호를제공하라는메시지가표시됩니다.
- 인증서별칭 **(**선택사항**).** 인증서별칭을입력합니다. 인증서별칭으로앱에서인증서에액세스하기가더간편해집니다. 동일한인증서별칭을자격증명장치정책에사용할경우앱에서사용자작업없이인증서를검색하고 VPN 을인증합니다.
- 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 에서트래픽이허용되거나차단되는앱의목록입니다. 쉼표또는세미콜론으로구분하여앱패키지이름을나열합니다. 앱패키지이름은대소문자를구분하며이목록에나타나는이름은 Google Play Store 에나타나는것과정확히일치해야합니다. 이목록은선택사항입니다. 장치전체 VPN 을프로비전하려면이목록을비워두십시오.
- 기본 **VPN** 프로필**.** 사용자가특정프로필을누르지않고 Citrix SSO 앱의사용자인터페이스에서연결스위치를누를때사용할 VPN 프로필의이름을입력합니다. 이필드를비워두면기본프로필이연결에사용됩니다. 하나의프로필만구성된경우기본프로필로표시됩니다. 항상 VPN 연결의경우항상 VPN 연결을설정하는데사용할 VPN 프로필의이름으로이필드를설정해야합니다.
- 사용자프로필사용안함**.** 이설정이켜짐인경우사용자는장치에서자체 VPN 을만들수없습니다. 이설정이꺼짐인경우사용자는장치에서자체 VPN 을만들수있습니다. 기본값은꺼짐입니다.
- 신뢰할수없는서버차단**.** Citrix Gateway 에대해자체서명된인증서를사용하는경우또는 Citrix Gateway 인증서를발급하는 CA 의루트인증서가시스템 CA 목록에없는경우이설정은꺼짐입니다. 이설정이켜짐인경우 Android 운영체제에서는 Citrix Gateway 인증서의유효성이검사됩니다. 유효성검사에실패하면연결이허용되지않습니다. 기본값은켜짐입니다.

6. 필요한경우사용자지정매개변수를만듭니다. 사용자지정매개변수 **XenMobileDeviceId** 와 **UserAgent** 가지원됩니다. 현재 VPN 구성을선택하고 추가를클릭합니다.



a) 사용자지정매개변수를만듭니다.

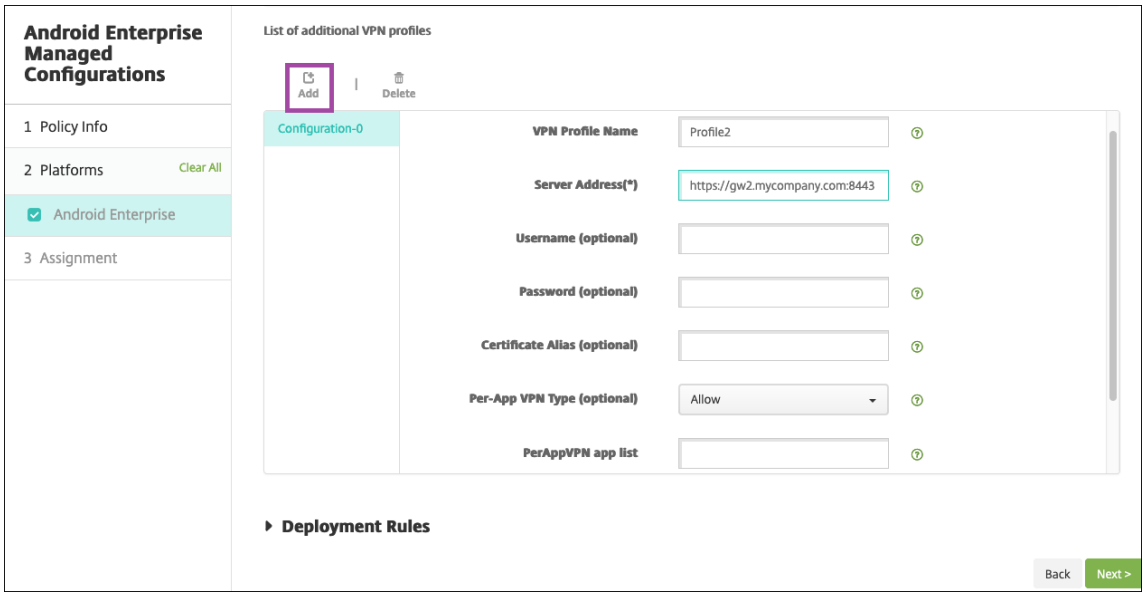
- 매개변수이름**. XenMobileDeviceId** 를입력합니다. 이필드는 XenMobile 의장치등록을기준으로네트워크액세스검사에사용할장치 ID 입니다. XenMobile 에서장치를등록하고관리하는경우 VPN 연결이허용됩니다. 그렇지않으면 VPN 설정시인증이거부됩니다.
- 매개변수값 XenMobile 에서장치의등록및관리상태를결정하려면 XenMobileDeviceID 의값을 `DeviceID_${ device.id }`로설정합니다.



a) 다른사용자지정매개변수를만들려면 추가를다시클릭합니다. 이사용자지정매개변수를만듭니다.

- 매개변수이름**. UserAgent** 를입력합니다. 이텍스트는 Citrix Gateway 에서추가검사를수행하기위해사용자에이전트 HTTP 헤더에추가됩니다. 이텍스트의값은 Citrix 게이트웨이와통신하는동안 Citrix SSO 앱을통해사용자에이전트 HTTP 헤더에추가됩니다.
- 매개변수값**.** 사용자에이전트 HTTP 헤더에추가할텍스트를입력합니다. 이텍스트는 HTTP 사용자에이전트 사양을준수해야합니다.

7. 필요한경우 VPN 프로필구성을추가로만듭니다. 구성목록에서 추가를클릭합니다. 새구성이목록에나타납니다. 새구성을 선택하고 5 단계와 6 단계를반복합니다 (선택사항).



8. 원하는 VPN 프로필을모두만들었으면 다음을클릭합니다.
9. Citrix SSO 의이관리되는구성에대한배포규칙을구성합니다.
10. 저장을클릭합니다.

이제 Citrix SSO 에대한이러한관리되는구성이구성된장치정책목록에나타납니다.

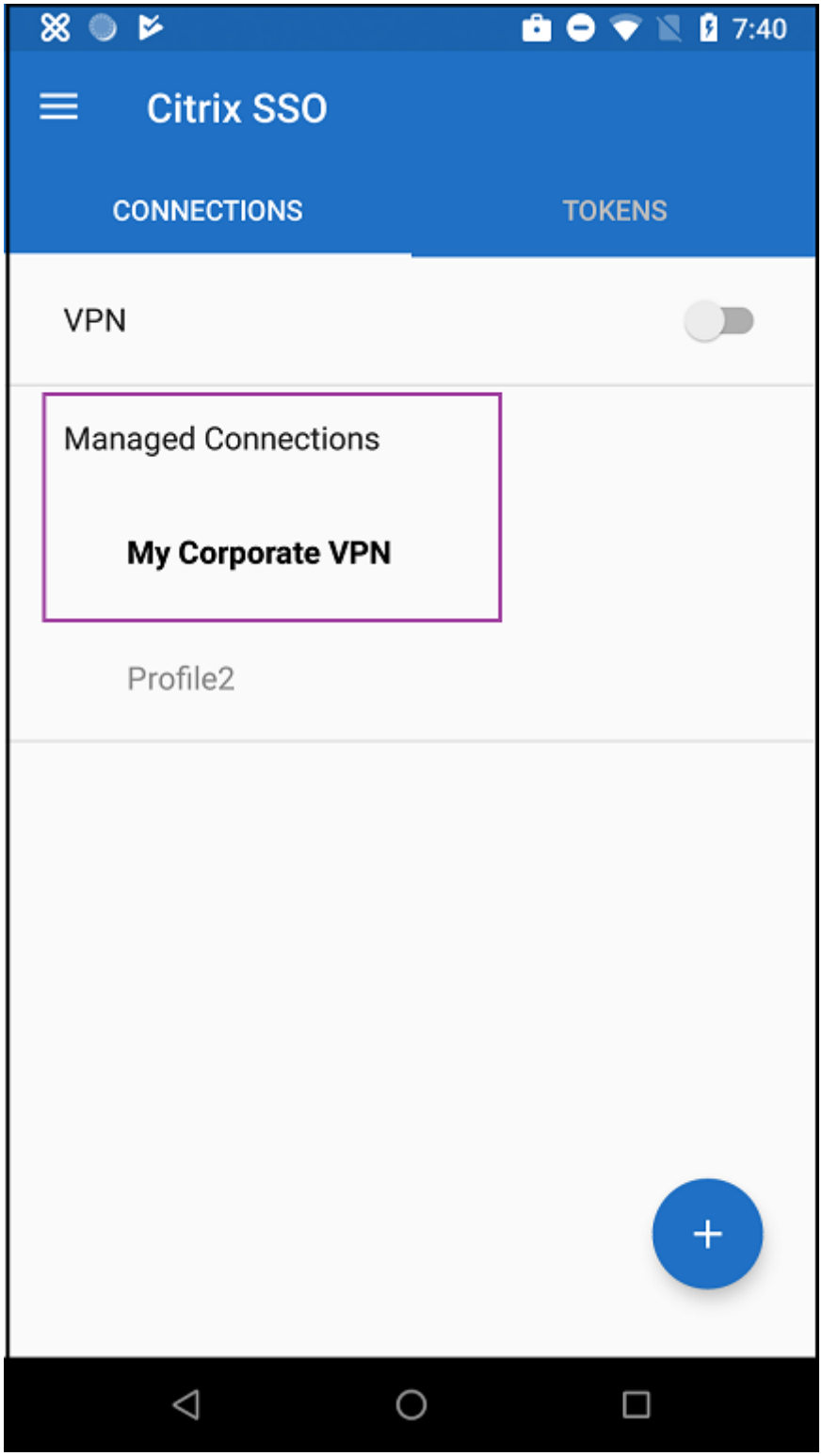
구성한 VPN 프로필에대해항상켜기를사용하려면 XenMobile 옵션장치정책을설정합니다.

> 참고**:**
> Android Enterprise 의항상 VPN 연결에는 Citrix Secure Hub 19.5.5 이상이필요합니다.

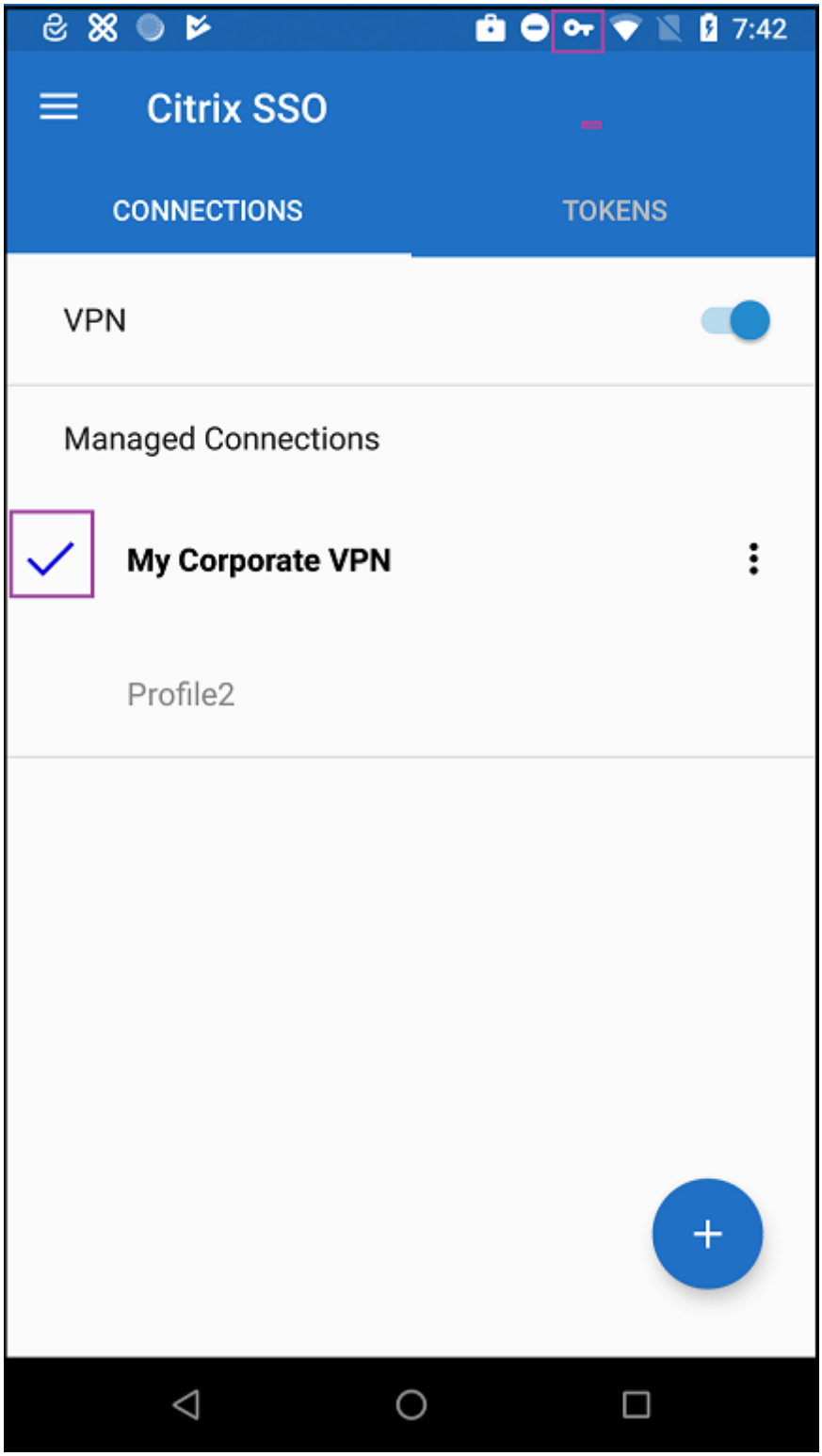
장치에서 **VPN** 프로필에액세스

만든 VPN 프로필에액세스하려면 Android Enterprise 사용자가 Google Play Store 에서 Citrix SSO 를설치해야합니다.

구성한 VPN 프로필은앱의 **Managed Connections(**관리되는연결**)** 영역에나타납니다. 사용자는 VPN 프로필을사용하여 연결하려는 VPN 프로필을누릅니다.



사용자가인증되고연결되면 VPN 프로필옆에확인표시가나타납니다. 열쇠아이콘은 VPN 이연결되어있음을나타냅니다.



Zebra OEMConfig 를사용하여 Zebra Android 장치관리

Zebra Technologies OEMConfig 관리도구를사용하여 Zebra Android 장치를관리할수있습니다. Zebra OEMConfig 앱에대한자세한내용은 Zebra Technologies 웹사이트를참조하십시오.

XenMobile 은 Zebra OEMConfig 버전 9.2 이상을지원합니다. 장치에 Zebra OEMConfig 를설치하기위한시스템요구사항에대한자세한내용은 Zebra Technologies 웹사이트에서 OEMConfig 설정을참조하십시오.

먼저 Zebra OEMConfig 앱을 Google Play Store 앱으로 XenMobile 콘솔에추가합니다. 공개앱스토어앱추가를참조하십시오.

Zebra OEMConfig 앱에대한 Android Enterprise 관리되는구성만들기

Zebra OEMConfig 앱에대한관리되는구성장치정책을구성합니다. 이정책은 Zebra OEMConfig 앱이설치되고정책이배포된 Zebra 장치에적용됩니다.

1. XenMobile 콘솔에서 구성 **>** 장치정책을클릭합니다. 추가를클릭합니다.
2. **Android Enterprise** 를선택합니다. 관리되는구성을클릭합니다.
3. 응용프로그램 **ID** 선택창이나타나면목록에서 **ZebraOEMConfig powered by MX(MX** 기반 **ZebraOEMConfig)** 를선택하고 확인을클릭합니다.
4. Zebra OEMConfig 구성의이름과설명을입력합니다. 다음을클릭합니다.
5. Zebra OEMConfig 구성의이름을입력합니다.
6. 사용가능한매개변수를구성합니다. 예:
   - 장치전면의카메라를사용하지않으려면 **Camera Configuration(**카메라구성**)** 을선택하고 **Use of Front Camera(**전면카메라사용**)** 를 **Off(**꺼짐**)** 로설정합니다.
   - 장치시간형식을변경하려면 **Clock Configuration(**시계구성**)** 을선택하고 **Time Format(**시간형식**)** 을 **12**(12 시간형식) 또는 **24**(24 시간형식) 로설정합니다.

사용가능한모든구성의목록및설명은 Zebra Technologies 웹사이트에서 Zebra 관리구성을참조하십시오.

1. 필요한경우 Zebra OEMConfig 구성을추가로만들수있습니다. 구성목록에서 추가를클릭합니다. 새구성이목록에나타납니다. 새구성을선택하고매개변수를구성합니다.
2. 원하는 Zebra OEMConfig 구성을모두만들었으면 다음을클릭합니다.
3. Zebra OEMConfig 의이관리되는구성에대한배포규칙을구성합니다.
4. 저장을클릭합니다.

관리되는도메인장치정책

January 5, 2022

전자메일및 Safari 브라우저에적용되는관리되는도메인을정의할수있습니다. 관리되는도메인을사용하면 Safari 를사용하여도메인에서다운로드한문서를열수있는앱을제어함으로써회사데이터를보호할수있습니다.

iOS 8 이상의감독되는장치의경우 URL 또는하위도메인을지정하여사용자가브라우저에서문서, 첨부파일및다운로드를열수있는방법을제어할수있습니다. iOS 9.3 이상의감독되는장치의경우사용자가 Safari 에서암호를저장할수있는 URL 을지정할수있습니다.

iOS 장치를감독모드로설정하는단계는 Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.

사용자가관리되는전자메일도메인목록에없는도메인의받는사람에게전자메일을보낼경우사용자장치에서회사도메인외부의사람에게메시지를보낸다는경고가표시됩니다.

문서, 첨부파일또는다운로드등의항목: 사용자가관리되는웹도메인목록에있는웹도메인에서 Safari 를사용하여항목을열면관련회사앱에서항목이열립니다. 해당항목이관리되는웹도메인목록의웹도메인에없는경우사용자가회사앱으로항목을열수없고관리되지않는개인앱을사용해야합니다.

감독되는장치의경우 Safari 암호자동채우기도메인을지정하지않더라도장치가임시다중사용자로구성된경우사용자가암호를저장할수없습니다. 그러나임시다중사용자로구성되지않은장치에서는사용자가모든암호를저장할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

도메인을지정하려면:

형식	설명
`example.com`	`site.example.com/`을제외하고, `example.com` 아래의모든경로를관리되는경로로처리합니다.
`foo.example.com`	`example.com/` 또는 `bar.example.com/`을제외하고, `foo.example.com` 아래의모든경로를관리되는경로로처리합니다.
`\*.example.com`	`example.com/`을제외하고, `foo.example.com` 또는 `bar.example.com` 아래의모든경로를관리되는경로로처리합니다.
`example.com/sub`	`example.com/`을제외하고, `example.com/sub`와그아래모든경로를관리되는경로로처리합니다.
`foo.example.com/sub`	`example.com`, `example.com/sub`, `foo.example.com/` 또는 `bar.example.com/sub`를제외하고, `foo.example.com/sub` 아래의모든경로를관리되는경로로처리합니다.

형식	설명
*.example.com/sub	example.com 또는 foo.example.com/을제외하고, foo.example.com/sub 또는 bar.example.com/sub 아래의모든경로를관리되는경로로처리합니다.

규칙:

- 도메인비교시 URL 의선행 “www” 와후행슬래시는무시됩니다.
- 포트번호가포함된항목의경우해당포트번호를지정하는주소만관리되는주소로간주됩니다. 그외항목의경우표준포트 (http 의경우포트 80, https 의경우포트 443) 만관리되는것으로간주됩니다. 예를들어 *.example.com:8080 패턴은 https://site.example.com:8080/page.html과일치하지만 https://site.example.com/page.html과는일치하지않는한편, *.example.com 패턴은 https://site.example.com/page.html 및 https://site.example.com/page.html과일치하지만 https://site.example.com:8080/page.html과는일치하지않습니다.
- 관리되는 Safari 웹도메인정의는누적됩니다. 관리되는 Safari 웹도메인페이로드에의해정의되는패턴은모두 URL 요청과일치시키는데사용됩니다.

설정:

- 관리되는도메인
  - 표시되지않은전자메일도메인**:** 목록에포함하려는각전자메일도메인에대해 추가를클릭한후다음을수행합니다.
    - 관리되는전자메일도메인**:** 전자메일도메인을입력합니다.
    - 전자메일도메인을저장하려면 저장을클릭하고저장하지않으려면 취소를클릭합니다.
  - 관리되는 **Safari** 웹도메인**:** 목록에포함하려는각웹도메인에대해 추가를클릭한후다음을수행합니다.
    - 관리되는웹도메인**:** 웹도메인을입력합니다.
    - 웹도메인을저장하려면 저장을클릭하고저장하지않으려면 취소를클릭합니다.
  - **Safari** 암호자동채우기도메인**:** 목록에포함하려는각자동채우기도메인에대해 추가를클릭한후다음을수행합니다.
    - **Safari** 암호자동채우기도메인**:** 자동채우기도메인을입력합니다.
    - 자동채우기도메인을저장하려면 저장을클릭하고저장하지않으려면 취소를클릭합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

MDM 옵션장치정책

January 5, 2022

감독되는 iOS 7.0 이상의전화장치에서내전화찾기및 iPad 활성화잠금을관리하는장치정책을 XenMobile 에서만들수있습니다. iOS 장치를감독모드로설정하는단계는 Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.

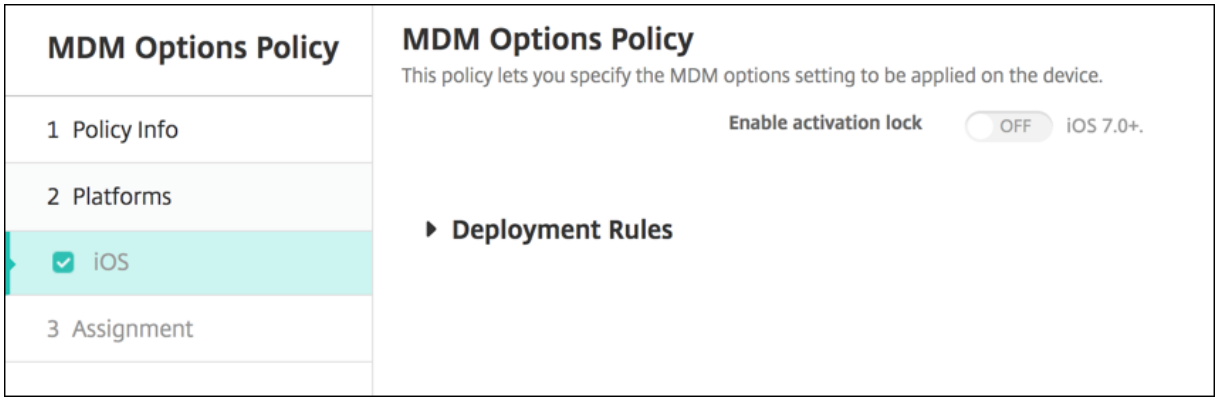
활성화잠금은분실되거나도난당한장치의재활성화를방지하는내 iPhone/iPad 찾기기능입니다. 활성화잠금은누군가가내 iPhone/iPad 찾기를끄고장치를지우거나장치를재활성화하여사용하려고할경우사용자의 Apple ID 와암호를요구합니다. 조직이소유한장치의경우예를들어장치를재설정하거나재할당하기위해활성화잠금을바이패스해야합니다.

활성화잠금을사용하도록설정하려면 XenMobile MDM 옵션장치정책을구성하고배포합니다. 그러면사용자의 Apple 자격증명이없이도 XenMobile 콘솔에서장치를관리할수있습니다. 활성화잠금의 Apple 자격증명요구사항을바이패스하려면 XenMobile 콘솔에서활성화잠금바이패스보안동작을실행합니다.

예를들어사용자가분실된휴대폰을반환하거나전체초기화전후에장치를설정하는경우 iTunes 계정자격증명을묻는메시지가표시될때 XenMobile 콘솔에서활성화잠금바이패스보안동작을실행하여이단계를바이패스할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



- 활성화잠금사용**:** 이정책을배포할장치에서활성화잠금을사용것인지를선택합니다. 기본값은 꺼짐입니다.

MDM 옵션장치정책을배포하여활성화잠금을사용하도록설정하면 관리 **>** 장치페이지에서해당장치를선택하고 보안을클릭할때보안동작 활성화잠금바이패스가표시됩니다. 활성화잠금바이패스를사용하면장치사용자의 Apple ID 및암호를몰라도장치활성화전에감독되는장치에서활성화잠금을해제할수있습니다. 전체초기화전후에활성화잠금바이패스를장치에전송할수있습니다. 자세한내용은보안동작문서에서 iOS 활성화잠금바이패스를참조하십시오.

조직정보장치정책

January 5, 2022

XenMobile 에서 iOS 장치에푸시되는알림메시지에대한조직정보를지정하는장치정책을 XenMobile 에서추가할수있습니다. iOS 7 이상의장치에서이정책을사용할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 이름**:** XenMobile 을실행하는조직의이름을입력합니다.
- 주소**:** 조직의주소를입력합니다.
- 전화**:** 조직의지원전화번호를입력합니다.
- 전자메일**:** 지원전자메일주소를입력합니다.
- 매직**:** 조직에서관리하는서비스를설명하는단어나구절을입력합니다.

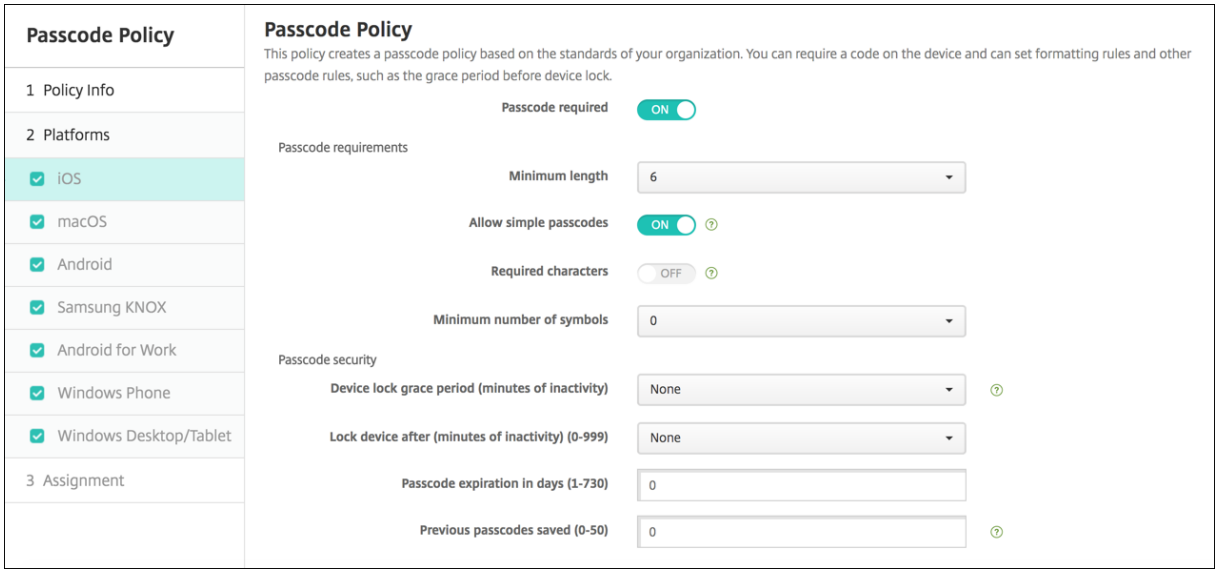
암호장치정책

August 12, 2022

조직의표준에따라 XenMobile 에서암호정책을만듭니다. 사용자의장치에암호를요구할수있으며다양한형식및암호규칙을설정할수있습니다. iOS, macOS, Android, Samsung KNOX, Android Enterprise 및 Windows Desktop/Tablet 에대한정책을만들수있습니다. 각플랫폼마다이문서에서설명되어있는서로다른값집합이필요합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

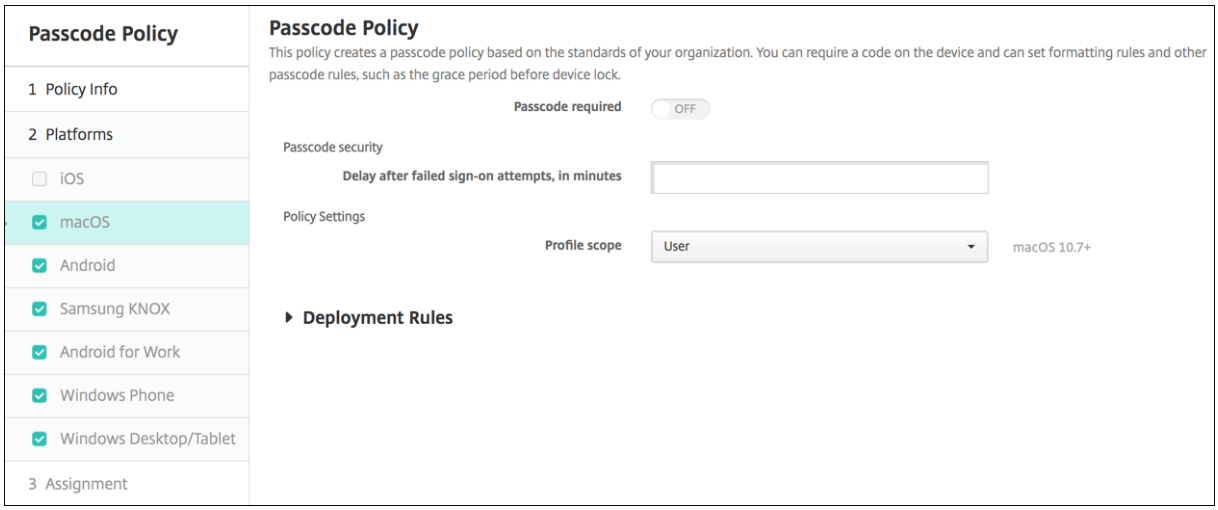
iOS 설정



- 암호필요**:** 암호를요구하고 iOS 암호장치정책의구성옵션을표시하려면이옵션을선택합니다. 페이지가확장되어암호요구사항, 암호보안및정책설정에대한설정을구성할수있게됩니다.

- 암호요구사항
  - 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.
  - 다음의비활성시간 **(**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.

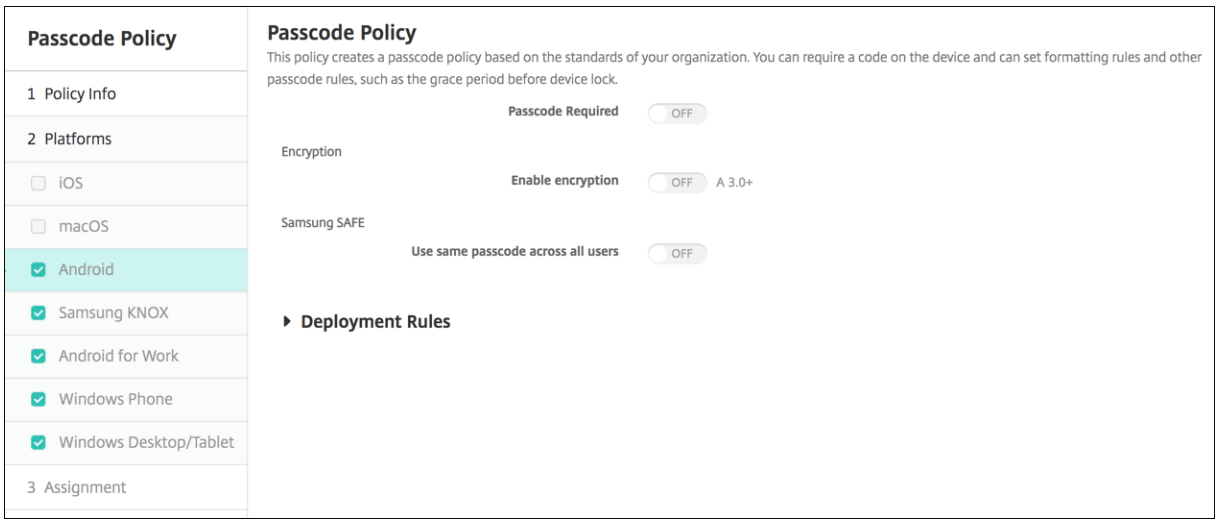
macOS 설정



- 암호필요**:** 암호를요구하고 iOS 암호장치정책의구성옵션을표시하려면이옵션을선택합니다. 페이지가확장되어암호요구사항, 암호보안및정책설정에대한설정을구성할수있게됩니다.
- 암호필요를사용하지않으려면 로그온시도에실패한후지연시간 **(**분**)** 옆에사용자가암호를다시입력할수있게될때까지대기하는시간 (분) 을입력합니다.
- 암호필요를사용하도록설정한경우다음설정을구성합니다.
- 암호요구사항
  - 최소길이**:** 목록에서최소암호길이를클릭합니다. 기본값은 **6** 입니다.
  - 단순암호허용**:** 단순암호를허용할지여부를선택합니다. 단순암호는반복적또는순차적문자집합입니다. 기본값은 켜

짐입니다.
  - 필수문자**:** 암호에적어도문자가하나있어야하는지여부를선택합니다. 기본값은 꺼짐입니다.
  - 최소기호개수**:** 목록에서암호에포함되어야하는기호의수를클릭합니다. 기본값은 **0** 입니다.
- 암호보안
  - 장치잠금유예기간 **(**비활성시간 **(**분**)):** 목록에서잠긴장치의잠금을해제하려는사용자가암호를입력해야하는기간을클릭합니다. 기본값은 없음입니다.
  - 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. 이횟수를넘으면장치가잠깁니다. 기본값은 정의되지않음입니다.
  - 로그온시도에실패한후지연시간 **(**분**):** 사용자가암호를다시입력할수있게될때까지대기하는시간 (분) 을입력합니다.
  - **Force passcode reset(**암호재설정강제적용**):** 사용자는다음에인증할때암호를재설정해야합니다.
- 정책설정
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

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.
  - 고급규칙을사용하도록설정한경우다음과같은목록각각에서암호에포함되어야하는각문자유형의최소수를클릭합니다.
    * 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.

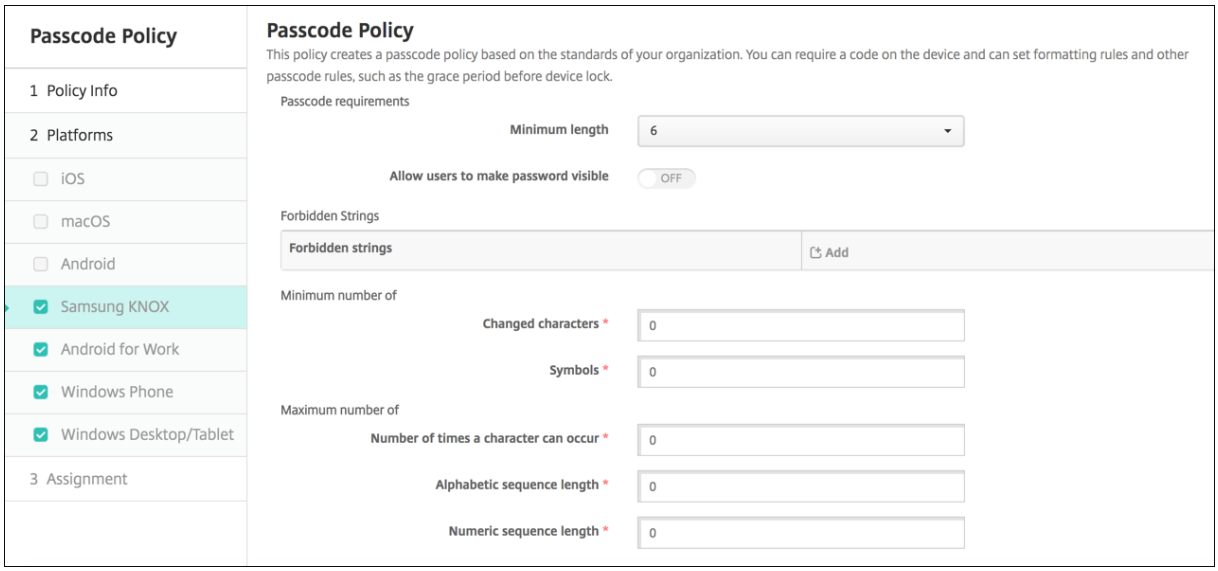
    장치를암호화하려면충전된배터리로시작하고암호화가실행되는수시간동안장치를꽂힌상태로유지해야합니다. 암호화프로세스가중단되면장치의데이터중일부또는전부가손실될수있습니다. 장치를암호화한후에는프로세스를되돌릴수없으며, 암호화를취소하는유일한방법은장치의모든데이터를지우고공장기본값으로재설정하는것입니다.
- **Samsung SAFE**

  > 참고**:**
  >
  > Samsung SAFE 장치에서얼굴또는홍채인식을사용하지않도록설정한경우해결방법: Samsung SAFE 용제한장치정책을만듭니다. 제한정책에서 응용프로그램사용안함을켜고테이블에 `com.samsung.android.bio.face.service` 또는 `com.samsung.android.server.iris`를추가합니다. 그런다음제한정책

> 을배포합니다.

- 모든사용자가동일한암호사용**:** 모든사용자에게동일한암호를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이 설정은 Samsung SAFE 장치에만적용되며 암호필요설정과관계없이사용할수있습니다.
- 모든사용자가동일한암호사용을사용하도록설정한경우 암호필드에모든사용자가사용할암호를입력합니다.
- 암호필요를사용하도록설정한경우다음과같은 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. 생체인증을사용하도록설정할지여부를선택합니다. 기본값은 꺼짐입니다. 켜짐으로설정하는 경우다음과같은옵션을설정할수있습니다.
    - 지문허용. 사용자가지문을사용하여인증할수있도록하려면이옵션을선택합니다.
    - 홍채허용. 사용자가홍채를사용하여인증할수있도록하려면이옵션을선택합니다.
  - 금지된문자열**:** 금지된문자열을만들어사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등과같이쉽게추측할수있는안전하지않은문자열을사용하지못하게합니다. 거부하려는각문자열에 대해 추가를클릭한후다음을수행합니다.
    - 금지된문자열**:** 사용자가사용할수없는문자열을입력합니다.
    - 저장을클릭하여문자열을추가하거나 취소를클릭하여문자열추가를취소합니다.

Samsung KNOX 설정



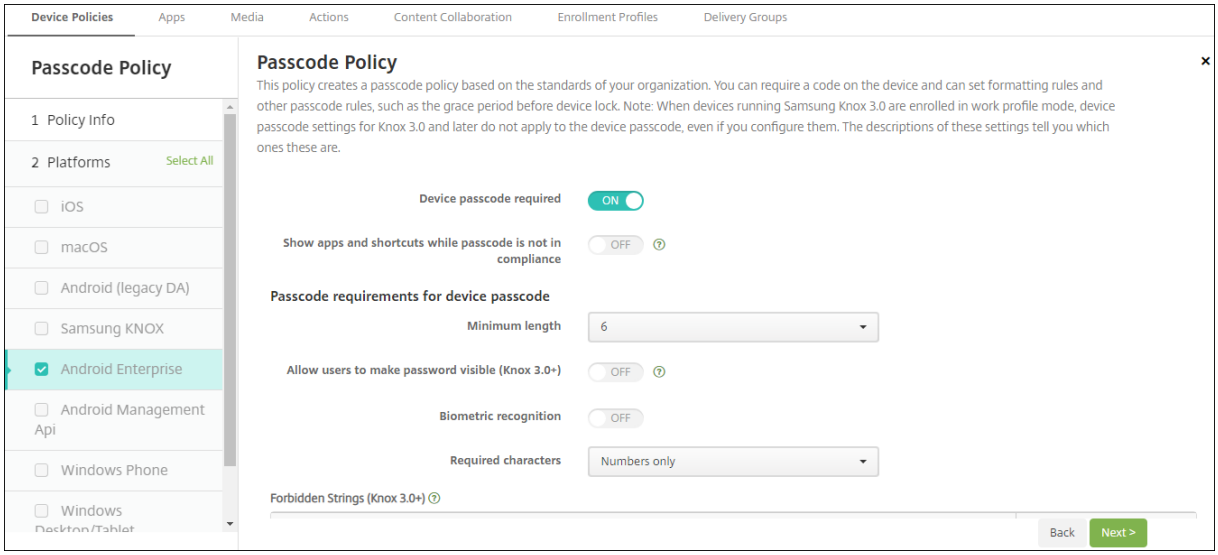
- 암호요구사항
  - 최소길이**:** 목록에서최소암호길이를클릭합니다. 기본값은 **6** 입니다.
  - 사용자에게암호표시허용**:** 사용자가암호를볼수있는지여부를선택합니다.
  - 금지된문자열**:** 금지된문자열을만들어사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등

과같이쉽게추측할수있는안전하지않은문자열을사용하지못하게합니다. 거부하려는각문자열에대해추가를클릭한후다음을수행합니다.

* 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. 유효한값은 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



Android Enterprise 장치의경우장치의암호또는 Android Enterprise 작업프로필의보안챌린지를요구하거나둘다를요구

할수있습니다.

Android 9.0 이상및 Samsung Knox 3.0 이상을실행하는장치의경우 **Android Enterprise** 페이지에서 Samsung Knox 에대한설정을구성합니다. 이전버전의 Android 또는 Samsung Knox 를실행하는장치의경우 **Samsung Knox** 페이지를사용합니다.

> 참고**:**
>
> Samsung Knox 3.0 을실행하는장치를작업프로필장치로등록한경우 Knox 3.0 이상에대한장치암호설정은구성된경우라하더라도장치암호에적용되지않습니다.

- 장치암호필요**:** 장치에암호가필요합니다. 이설정이 켜짐인경우 장치암호의암호요구사항및 장치암호의암호보안에서설정을구성합니다. 기본값은 꺼짐입니다.
- 암호가규정을준수하지않는경우앱및바로가기표시**:** 이설정이 켜짐이면암호가규정을준수하지않더라도장치의앱과바로가기가숨겨지지않습니다. 이설정이 꺼짐이면암호가규정을준수하지않는경우앱과바로가기가숨겨집니다. 이설정을사용하면 Citrix 에서는암호가규정을준수하지않는경우규정을준수하지않는장치로표시하도록자동화된작업을만드는것을권장합니다. 기본값은 꺼짐입니다.
- 장치암호의암호요구사항**:**
  - 최소길이**:** 최소암호길이를지정합니다. 기본값은 6 입니다.
  - 사용자에게암호표시허용**:** 올바른 Knox 라이센스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전관리형장치에만해당됩니다. 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 제한없음설정을따르지않습니다. 기본값은 숫자와문자모두입니다.
  - 금지된문자열**:** 올바른 Knox 라이센스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전관리형장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다. 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 라이센스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전관리형장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다. 사용자가이전암호에서변경해야하는문자수를지정합니다. 기본값은 **0** 입니다.
    - 최대개수**:** 올바른 Knox 라이센스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전관리형장치에만해당됩니다. 이설정은작업프로필장치로등록된장치에는적용되지않습니다.
        * 한문자의최대사용횟수**:** 한문자가암호에서발생할수있는최대횟수를지정합니다. 기본값은 **0** 이며최대제한이없음을의미합니다.
        * 연속영문자길이**:** 암호에서연속될수있는영문자의최대길이를지정합니다. 기본값은 **0** 이며최대제한이없음을의미합니다.
        * 연속숫자길이**:** 암호에서연속될수있는숫자의최대길이를지정합니다. 기본값은 **0** 이며최대제한이없음을의미합니다.
- 장치암호의암호보안**:**
    - 다음로그온시도실패후장치초기화**:** 사용자가로그인에실패할수있는횟수를지정합니다. 이횟수를넘으면장치가전체초기화됩니다. 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 라이센스키가구성된 Samsung Knox 3.0 이상을실행하는장치를위한설정입니다. 완전관리형장치에만해당됩니다. 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 라이센스키가구성된 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 라이센스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다. 사용자가암호로사용할수없는문자열을지정합니다. 금지된문자열을만들어사용자가 “password”, “pwd”, “welcome”, “123456”, “111111” 등과같이쉽게추측할수있는안전하지않은문자열을사용하지못하게합니다. 거부할각문자열

에대해 추가를클릭하고사용금지하려는문자열을입력한다음 저장을클릭하여문자열을추가하거나 취소를클릭하여문자열추가를취소합니다.

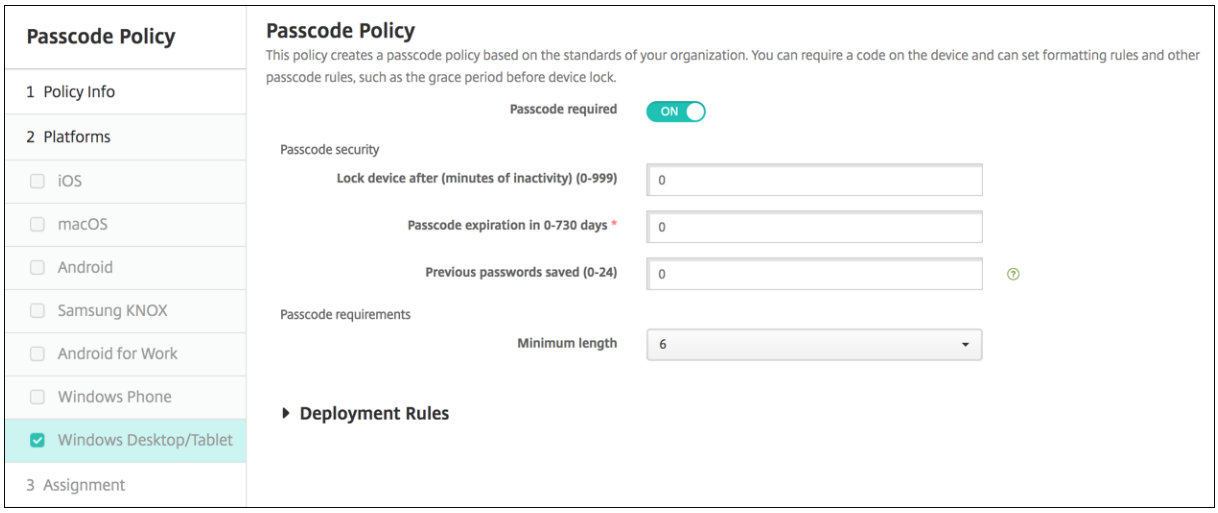
- 고급규칙**:** 암호에서발생할수있는문자유형에대해고급규칙을적용합니다. 이설정이 켜짐인경우 최소개수및 최대개수에서설정을구성합니다. Android 5.0 이전의 Android 장치에서는이설정을사용할수없습니다. 기본값은 꺼짐입니다.
- 최소개수**:**
  - 기호**:** 기호의최소수를지정합니다. 기본값은 **0** 입니다.
  - 문자**:** 문자의최소수를지정합니다. 기본값은 **0** 입니다.
  - 소문자**:** 소문자의최소수를지정합니다. 기본값은 **0** 입니다.
  - 대문자**:** 대문자의최소수를지정합니다. 기본값은 **0** 입니다.
  - 숫자또는기호**:** 숫자또는기호의최소수를지정합니다. 기본값은 **0** 입니다.
  - 숫자**:** 숫자의최소수를지정합니다. 기본값은 **0** 입니다.
  - 변경된문자**:** 올바른 Knox 라이센스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다. 사용자가이전암호에서변경해야하는문자수를지정합니다. 기본값은 **0** 입니다.
- 최대개수**:** 올바른 Knox 라이센스키가구성된 Knox 3.0 이상을실행하는장치를위한설정입니다.
  - 한문자의최대사용횟수**:** 한문자가암호에서발생할수있는최대횟수를지정합니다. 기본값은 **0** 이며최대제한이없음을의미합니다.
  - 연속영문자길이**:** 암호에서연속될수있는영문자의최대길이를지정합니다. 기본값은 **0** 이며최대제한이없음을의미합니다.
  - 연속숫자길이**:** 암호에서연속될수있는숫자의최대길이를지정합니다. 기본값은 **0** 이며최대제한이없음을의미합니다.
- 통합암호사용**:** 켜짐인경우사용자는장치와작업프로필에하나의암호를사용합니다. 꺼짐인경우:
  - 사용자는장치와작업프로필에다른암호를사용해야합니다.
  - 사용자가장치와작업프로필에하나의암호를사용하려고설정한장치의 한번잠금사용설정이비활성화됩니다. 사용자가활성화할수없습니다.
  - 작업프로필보안인증질문에대한암호요건이장치암호보다복잡한경우: 한번잠금사용설정을활성화한사용자에게작업프로필암호를변경하라는메시지가표시됩니다.

  기본값은 꺼짐입니다. Android 9.0 부터사용할수있습니다.

- 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 라이센스키가구성된 Knox 3.0 이상을실행하는장치를위한설

정입니다. 사용자가로그온에실패할수있는횟수를지정합니다. 그후장치가잠깁니다. 기본값은 정의되지않음입니다.

Windows 데스크톱/태블릿설정



- 간편로그온허용안함**:** 사용자가사진암호또는생체인식로그온을사용하여장치에액세스할수있도록허용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 최소암호길이**:** 목록에서최소암호길이를클릭합니다. 기본값은 **6** 입니다.
- 초기화하기전까지의최대암호시도횟수**:** 목록에서사용자가로그인에실패할수있는횟수를클릭합니다. 이횟수를넘으면장치에서데이터가초기화됩니다. 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.

개인핫스폿장치정책

January 5, 2022

사용자가 WiFi 네트워크범위외부에있을때 iOS 장치의개인핫스폿기능을통해셀룰러데이터연결을사용하여인터넷에연결하도록허용할수있습니다. iOS 7.0 이상에서사용가능합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 개인핫스폿사용안함**:** 사용자의장치에서개인핫스폿기능을사용하지않도록설정할지여부를선택합니다. 기본값은사용자의장치에서개인핫스폿을끄는 꺼짐입니다. 이정책은기능을사용하지않도록설정하지않습니다. 사용자는여전히자신의장치에서개인핫스폿을사용할수있지만정책이배포될때개인핫스폿이해제되어기본적으로켜져있지않습니다.

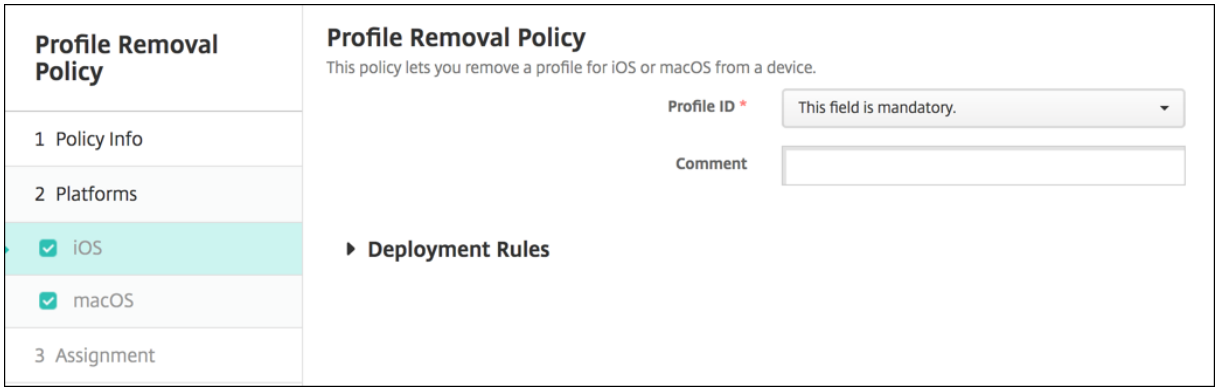
프로필제거장치정책

January 5, 2022

XenMobile 에서앱프로필제거장치정책을만들수있습니다. 정책을배포하면사용자의 iOS 또는 macOS 장치에서앱프로필이제거됩니다.

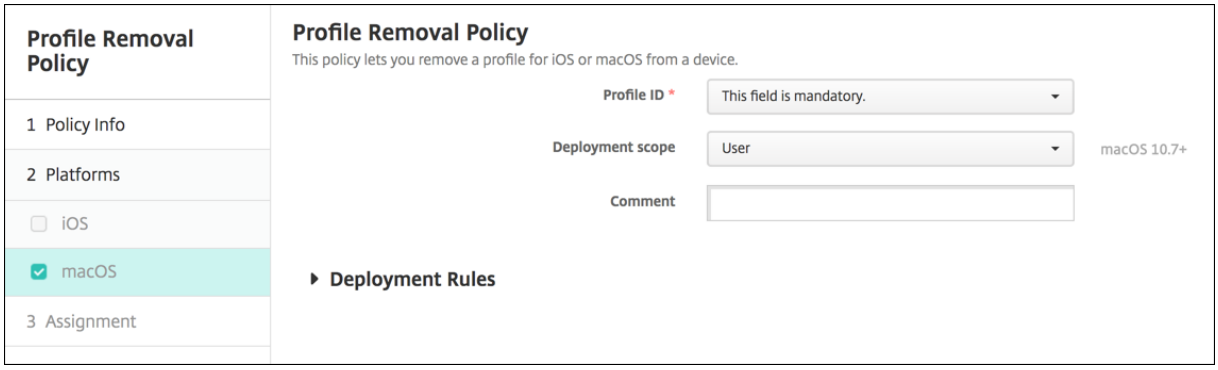
이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



- 프로필 **ID:** 목록에서앱프로필 ID 를클릭합니다. 이것은필수필드입니다.
- 설명**:** 선택적설명을입력합니다.

macOS 설정



- 프로필 **ID:** 목록에서앱프로필 ID 를클릭합니다. 이것은필수필드입니다.
- 배포범위**:** 목록에서 사용자또는 시스템을클릭합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.
- 설명**:** 선택적설명을입력합니다.

프로비전프로필장치정책

January 5, 2022

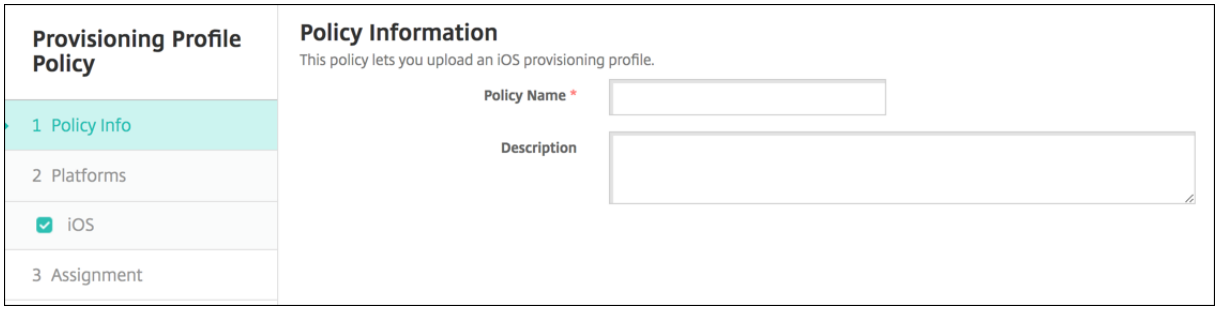
iOS 엔터프라이즈앱을개발하고코드서명하는경우일반적으로엔터프라이즈배포프로비전프로필을포함합니다. Apple iOS 장치에서앱을실행하려면이프로필이필요합니다. 프로비전프로필이누락되었거나만료된경우사용자가앱을눌러서열때앱의작동이중단됩니다.

프로비전프로필의주요문제는 Apple Developer Portal 에서생성된후 1 년지나면만료된다는것입니다. 따라서사용자에의해등록된모든 iOS 장치에서모든프로비전프로필의만료날짜를추적해야합니다. 만료날짜를추적하는작업에는실제만료날짜뿐아니라어떤사용자가어떤앱버전을사용하는지를지속적으로파악하는것도포함됩니다. 두가지해결방법은프로비전프로필을사용자에게전자메일로보내거나웹포털에게시해다운로드하여설치하도록하는것입니다. 이러한해결방법은효과가있지만오류가발생하기쉽습니다. 사용자가전자메일의지침에대응하거나웹포털에서올바른프로필을다운로드하여설치해야하기때문입니다.

이프로세스를사용자에게투명하게진행하려면 XenMobile 에서장치정책을사용하여프로비전프로필을설치하거나제거할수있습니다. 누락되었거나만료된프로필은필요에따라제거되고최신프로필이사용자의장치에설치되므로앱을누르기만하면열어서사용할수있습니다.

프로비전프로필정책을만들려면먼저프로비전프로필파일을만들어야합니다. 자세한내용은 Apple Developer 사이트에서개발프로비전프로필을만드는방법에대한 Apple 설명서를참조하십시오.

iOS 설정



- **iOS** 프로비전프로필**:** 찾아보기를클릭하고파일위치로이동하여가져올프로비전프로필파일을선택합니다.

프로비전프로필제거장치정책

January 5, 2022

장치정책을사용하여 iOS 프로비전프로필을제거할수있습니다. 프로비전프로필에대한자세한내용은 프로비전프로필장치정책을 참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- **iOS** 프로비전프로필**:** 목록에서제거할프로비전프로필을클릭합니다.
- 설명**:** 필요한경우설명을추가합니다.

프록시장치정책

August 12, 2022

XenMobile 에서장치정책을추가하여 iOS 6.0 이상을실행하는장치에대한글로벌 HTTP 프록시설정을지정할수있습니다. 장치당하나의글로벌 HTTP 프록시정책만배포할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

사전요구사항

이정책을배포하기전에글로벌 HTTP 프록시를설정할모든 iOS 장치를감독모드로설정해야합니다. 자세한내용은 Apple Configurator 를사용하여 iOS 장치를감독모드로전환 또는 Apple 배포프로그램을통해장치배포를참조하십시오.

장치로프록시정책을보내기전에장치를등록하기위한배포규칙을설정합니다.

iOS 설정

- 프록시구성**:** 사용자의장치에서프록시를구성하는방법에대해 수동또는 자동을클릭합니다.
  - 수동을클릭하는경우다음설정을구성합니다.
    - 프록시서버의호스트이름또는 **IP** 주소**:** 프록시서버의호스트이름또는 IP 주소를입력합니다. 이것은필수필드입니다.
    - 프록시서버용포트**:** 프록시서버포트번호를입력합니다. 이것은필수필드입니다.
    - 사용자이름**:** 프록시서버인증에사용할선택적사용자이름을입력합니다.
    - 암호**:** 프록시서버인증에사용할선택적암호를입력합니다.
  - 자동을클릭하는경우다음설정을구성합니다.

    * 프록시 **PAC URL:** 프록시구성을정의하는 PAC 파일의 URL 을입력합니다.
    * **PAC** 에연결할수없는경우직접연결허용**:** PAC 파일에연결할수없는경우대상에직접연결할수있도록할지여부를선택합니다. 기본값은 켜짐입니다. 이옵션은 iOS 7.0 이상에서만사용할수있습니다.

- 종속네트워크에액세스하기위한프록시바이패스허용**:** 종속네트워크에액세스하기위한프록시바이패스를허용할것인지여부를선택합니다. 기본값은 꺼짐입니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    * 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    * 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

원격지원장치정책

August 12, 2022

> 참고**:**
>
> 온-프레미스 XenMobile Server 배포의경우: 원격지원을사용하면지원센터담당자가관리되는 Android 모바일장치를원격으로제어할수있습니다. 스크린캐스트는 Samsung KNOX 장치에서만지원됩니다.
>
> 원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다.
>
> 자세한내용은 지원옵션및원격지원을참조하십시오.

XenMobile 에서지원되는 Windows 및 Android 장치에대한원격액세스를제공하는원격지원정책을만듭니다. 두가지유형의지원을구성할수있습니다.

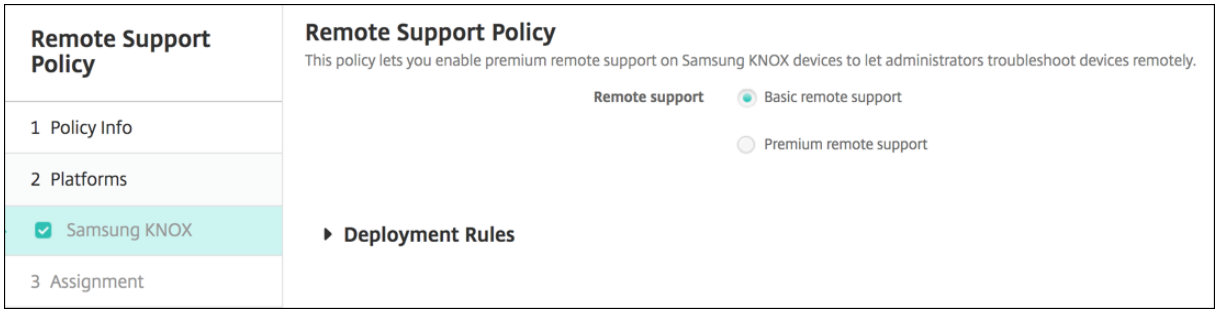
- 기본 - 시스템정보, 실행중인프로세스, 작업관리자 (메모리및 CPU 사용량), 설치된소프트웨어폴더내용등과같은장치에대한진단정보를볼수있습니다.
- 프리미엄 - 원격으로장치화면을제어할수있습니다.
  - 색상제어 (주창또는개별적인부동창에서)
  - 지원센터와사용자간의 VoIP(Voice-over-IP) 세션설정
  - 설정구성
  - 지원센터와사용자간의채팅세션설정

이정책을구현하려면다음을수행해야합니다.

- 사용자환경에서 XenMobile Remote Support 앱을설치합니다.
- Remote Support 앱터널을구성합니다. 자세한내용은 앱터널링장치정책을참조하십시오.
- 이항목에설명된대로 Samsung KNOX 원격지원장치정책을구성합니다.
- 앱터널원격지원정책과 Samsung KNOX 원격지원정책을모두사용자장치에배포합니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Android 설정



- 원격지원: 기본원격지원또는 프리미엄원격지원을선택합니다. 기본값은 기본원격지원입니다.

제한장치정책

August 12, 2022

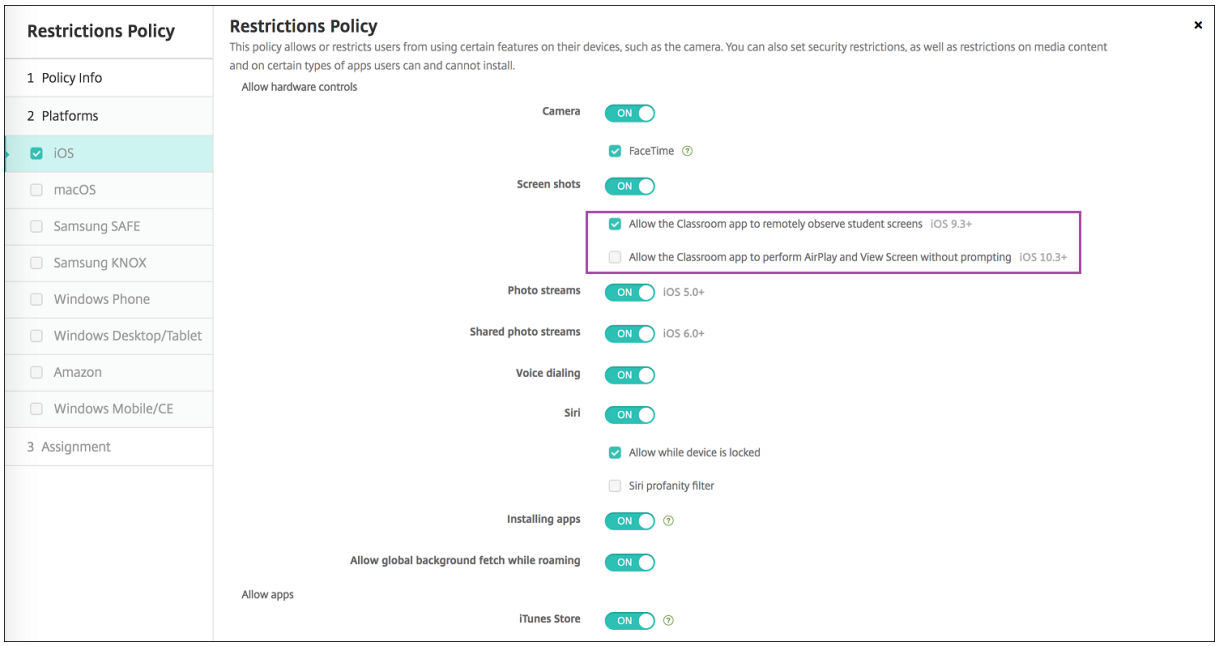
제한장치정책은사용자장치에서카메라와같은특정기능을허용하거나제한합니다. 또한보안제한을설정하고미디어콘텐츠에대한제한과사용자가설치할수있는앱유형및설치할수없는앱유형에대한제한을설정할수있습니다. 대부분의제한설정은기본적으로 켜짐 또는 허용입니다. 주요예외사항은 iOS 보안 - 시행기능및모든 Windows 태블릿기능입니다. 이러한기능은기본적으로 꺼짐 또는 제한으로설정됩니다.

Windows 10 RS2 휴대폰: Internet Explorer 를사용하지않는사용자지정 XML 정책또는제한정책을휴대폰에배포한후브라우저가사용되는상태로유지됩니다. 이문제를해결하려면휴대폰을다시시작하십시오. 이것은타사문제입니다.

> 팁:
>
> 켜짐을선택한모든옵션은사용자가해당작업을수행하거나기능을사용할수있다는의미입니다. 예:
>
> 카메라. 켜짐이면사용자가장치에서카메라를사용할수있습니다. 꺼짐이면사용자가장치에서카메라를사용할수없습니다.
>
> 스크린샷. 켜짐이면사용자가장치에서스크린샷을만들수있습니다. 꺼짐이면사용자가장치에서스크린샷을만들수없습니다.

이정책을추가하거나구성하려면 구성 > 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정



일부 iOS 제한정책설정은여기와 XenMobile 콘솔제한정책페이지에설명된대로특정버전의 iOS 에만적용됩니다.

iOS 제한정책설정은장치가사용자등록모드, 감독되지않는모드 (전체 MDM) 또는감독모드에서등록된경우적용됩니다. 다음표에는 iOS 13 이상에대한각제한정책설정에사용할수있는등록모드가나와있습니다.

표에나와있듯이 iOS 13 부터는이전에감독되지않은모드및감독모드에서사용할수있었던일부설정을감독모드에서만사용할수있습니다. 다음규칙이적용됩니다.

- 감독되는 iOS 13 이상장치를 XenMobile 에등록하는경우설정이장치에적용됩니다.
- 감독되지않는 iOS 13 이상장치를 XenMobile 에등록하는경우설정이장치에적용되지않습니다.
- iOS 12 이하장치가이미 XenMobile 에등록되었고 iOS 13 으로업그레이드된경우변경사항은없습니다. 이설정은업그레이드전과마찬가지로장치에적용됩니다.

iOS 장치를감독모드로설정하는방법에관한정보는 Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.

설정	사용자등록	감독되지않음	감독됨
하드웨어제어허용			
카메라	아니요	예	예
FaceTime	아니요	아니요 (iOS 13 의새로운기능)	예
스크린샷	예	아니요	예
교실앱이학생화면을원격으로관찰할수있도록허용	아니요	아니요	예

설정	사용자등록	감독되지않음	감독됨
메시지를표시하지않고교실 앱이 AirPlay 및화면보기를수행할수있도록허용	아니요	아니요	예
사진스트림	아니요	예	예
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

설정	사용자등록	감독되지않음	감독됨
iCloud 사진키집합	아니요	예	예
iCloud 사진라이브러리	아니요	예	예
보안 - 시행			
암호화된백업	예	예	예
제한된 AD 추적	아니요	예	예
첫번째 AirPlay 페어링의 암호	예	예	예
Wrist Detect 를사용하기 위해페어링된 Apple Watch	예	예	예
AirDrop 을사용하여관리되는문서공유	예	예	예
보안 - 허용			
신뢰할수없는 SSL 인증서 수락	아니요	예	예
인증서신뢰설정에대한자동 업데이트	아니요	예	예
관리되지않는앱에있는관리되는앱의문서	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

설정	사용자등록	감독되지않음	감독됨
엔터프라이즈북에대한백업	예	예	예
엔터프라이즈북동기화에대한메모및하이라이트	예	예	예
Spotlight 에대한인터넷결과	아니요	예	예
엔터프라이즈앱신뢰	아니요	예	예
감독되는경우에만해당되는설정 - 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 의새로운기능)	예
친구추가	아니요	아니요	예
멀티플레이게임	아니요	아니요 (iOS 13 의새로운기능)	예

설정	사용자등록	감독되지않음	감독됨
계정설정수정	아니요	아니요	예
앱셀룰러데이터설정수정	아니요	아니요	예
앱셀룰러데이터설정수정	아니요	아니요	예
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
진단제출수정	아니요	아니요	예
Bluetooth 수정	아니요	아니요	예
받아쓰기허용	아니요	아니요	예
Wi-Fi 정책에따라설치된 Wi-Fi 네트워크에만참가	아니요	아니요	예
메시지를표시하지않고교실 앱이 AirPlay 및화면보기 를수행할수있도록허용	아니요	아니요	예
메시지를표시하지않고교실 앱이앱및장치를잠글수있도 록허용	아니요	아니요	예
메시지를표시하지않고교실 앱클래스에자동참가	아니요	아니요	예
AirPrint 허용	아니요	아니요	예

설정	사용자등록	감독되지않음	감독됨
키집합에 AirPrint 자격증명저장허용	아니요	아니요	예
iBeacon 을사용하여 AirPrint 프린터검색허용	아니요	아니요	예
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
소프트웨어업데이트강제지연	아니요	아니요	예
소프트웨어업데이트시행지연	아니요	아니요	예
교실에서클래스를나갈때허가요청시행	아니요	아니요	예
자동날짜및시간적용	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 의새로운기능)	예
iBooks 의성관련성인등급콘텐츠	아니요	예	예
평가지역	아니요	예	예

설정	사용자등록	감독되지않음	감독됨
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** 및화면보기를수행할수있도록허용설정에따라강사에게권한을제공할지여부를묻는메시지가학생에게표시됩니다. 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 및받아쓰기정책을참조하십시오.
  - 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**:** 이설정을사용하는경우사용자가의심스러운피싱웹사이트를방문하면 Safari 경고가나타납니다. 기본값은이기능을제한하는것이며, 경고가실행되지않습니다.
        * **JavaScript** 사용**:** Safari 에서 JavaScript 를실행하도록허용합니다.
        * 팝업차단**:** 웹사이트를보는동안팝업을차단합니다. 기본값은이기능을제한하는것이며, 팝업을차단하지않습니다.
    - 쿠키적용**:** 쿠키가허용되는범위를설정합니다. 목록에서쿠키를허용하거나제한하는옵션을선택합니다. 기본옵션은항상이며, Safari 에서모든웹사이트가쿠키를저장하도록허용합니다. 다른옵션은 현재웹사이트만, 안함및 방문한웹사이트에서만입니다.

- 네트워크 **- iCloud** 동작허용
    - **iCloud** 문서및데이터**:** 사용자가문서및데이터를 iCloud 에동기화하도록허용합니다. 감독되는 iOS 장치를위한설정입니다.
    - **iCloud** 백업**:** 사용자가장치를 iCloud 에백업하도록허용합니다.
    - **iCloud** 키집합**:** 사용자가암호, Wi-Fi 네트워크, 신용카드및기타정보를 iCloud 키집합에저장하도록허용합니다.
    - 클라우드사진라이브러리**:** 사용자가 iCloud 사진라이브러리에액세스할수있도록허용합니다.

- 보안 **-** 시행

  기본값은다음과같은기능을제한하는것이며, 보안기능이사용되지않습니다.

    - 암호화된백업**:** iCloud 에대한백업을암호화합니다.
    - 제한된 **AD** 추적**:** 표적광고추적을차단합니다.
    - 첫번째 **Airplay** 페어링의암호**:** AirPlay 지원장치는 AirPlay 를사용하기전에화면상의일회용코드로확인을받아야합니다.
    - **Wrist Detect** 를사용하기위해페어링된 **Apple Watch:** 손목인식을사용하려면페어링된 Apple Watch 가있어야합니다.
    - **AirDrop** 을사용하여관리되는문서공유**:** 이옵션을 켜짐으로설정하면 AirDrop 이관리되지않는드롭대상으로나타납니다.

- 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.
  - 엔터프라이즈앱신뢰**:** 엔터프라이즈응용프로그램을신뢰할수있도록허용합니다. 엔터프라이즈앱은조직에따라맞춤제작된앱입니다. 이러한앱은내부적으로만들거나외부공급업체를통해개발및구매할수있습니다. 자세한내용은 iOS 에사용자지정엔터프라이즈앱설치를참조하십시오.
  - **Spotlight** 에대한인터넷결과**:** Spotlight 가인터넷뿐만아니라장치의검색결과를표시하도록허용합니다.
  - 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 장치를감독모드로전환을참조하십시오.

  - 모든내용및설정지우기**:** 사용자가장치에서모든콘텐츠및설정을지울수있도록허용합니다.
  - 제한구성**:** 사용자가장치에서자녀보호기능을구성하도록허용합니다.
  - 팟캐스트**:** 사용자가팟캐스트를다운로드하고동기화하도록허용합니다.
  - 구성프로필설치**:** 사용자가배포된구성프로필과다른구성프로필을설치하도록허용합니다.
  - 지문수정**:** 사용자가 Touch ID 지문을변경하거나삭제하도록허용합니다.
  - 장치에서앱설치**:** 사용자가앱을설치하도록허용합니다. 이설정을비활성화하면최종사용자가새앱을설치하지못하게됩니다. App Store 가비활성화되고아이콘이홈화면에서제거됩니다.
  - 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. 전통적인저널리스트가아닌소비자가사용자생성콘텐츠를제작합니다. 예를들어 Twitter 또는 Facebook 에서찾은콘텐츠가사용자가생성한콘텐츠입니다.

- **iBooks:** 사용자가 iBooks 앱을사용할수있도록허용합니다.
- 앱제거**:** 사용자가장치에서앱을삭제하도록허용합니다.
- 게임센터**:** 사용자가장치에서 Game Center 를통해온라인게임을플레이할수있도록허용합니다.
  * 친구추가**:** 사용자가게임을할친구에게알림을보낼수있도록허용합니다.
  * 멀티플레이게임**:** 사용자가장치에서멀티플레이게임을시작할수있도록허용합니다.
- 계정설정수정**:** 사용자가장치계정설정을수정할수있도록허용합니다.
- 앱셀룰러데이터설정수정**:** 앱이셀룰러데이터를사용하는방식을사용자가수정할수있도록허용합니다.
- 내친구찾기설정수정**:** 사용자가내친구찾기설정을변경할수있도록허용합니다.
- 비 **Configurator** 호스트와페어링**:** 관리자가사용자장치가페어링할수있는장치를제어할수있도록허용합니다. 이설정을사용하지않도록설정하면 Apple Configurator 를실행하는감독되는호스트이외에는페어링할수없습니다. 감독호스트인증서가구성되어있지않으면모든페어링을사용할수없습니다.
- 키보드자동완성**:** 사용자장치가키보드자동완성기능을사용하여입력하는단어를제안할수있도록허용합니다. 사용자가추천단어에액세스하지못하도록하는표준화된테스트관리와같은상황에서는이옵션을비활성화하십시오.
- 키보드자동수정**:** 사용자장치가키보드자동수정을사용할수있도록허용합니다. 사용자가자동수정에액세스하지못하도록하는표준화된테스트관리와같은상황에서는이옵션을비활성화하십시오.
- 키보드맞춤법검사**:** 입력하는동안사용자장치가맞춤법검사를사용할수있도록허용합니다. 사용자가맞춤법검사에액세스하지못하도록하는표준화된테스트관리와같은상황에서는이옵션을비활성화하십시오.
- 정의조회**:** 입력하는동안사용자장치가정의조회를사용할수있도록허용합니다. 사용자가입력하는동안정의를조회하지못하도록하는표준화된테스트관리와같은상황에서는이옵션을비활성화하십시오.
- 단일앱번들 **ID:** 장치에대한제어권한을유지하고다른앱또는기능과의상호작용을방지하도록허용된앱목록을만듭니다.
  앱을추가하려면 추가를클릭하고 앱이름을입력한후 저장을클릭합니다. 추가할각앱에대해이프로세스를반복합니다.
- 뉴스**:** 사용자가뉴스앱을사용할수있도록허용합니다.
- **Apple Music** 서비스**:** 사용자가 Apple Music 서비스를사용할수있도록허용합니다. Apple Music 서비스를허용하지않는경우 Music 앱이클래식모드에서실행됩니다.
- **iTunes Radio:** 사용자가 iTunes Radio 를사용할수있도록허용합니다.
- 알림수정**:** 사용자가알림설정을수정할수있도록허용합니다.
- 제한된앱사용**:** 사용자가제공된번들 ID 를기반으로모든앱을사용하거나일부앱을사용하거나사용하지않도록허용합니다. 감독되는장치에만적용됩니다. 일부앱만허용을선택할경우번들 ID 가 `com.apple.webapp`인앱을추가하여웹클립을허용합니다.

> 참고**:**
>
> iOS 11 부터앱제한에서사용할수있는 Apple 정책이변경되었습니다. Apple 의경우더이상적절한 iOS 응용프로그램번들을제한하여설정앱과전화앱에대한액세스를제거할수없습니다.

일부앱을차단하는제한장치정책을구성한후정책배포: 나중에해당앱중일부또는전부를허용하려는경우제한장치정책을변경하고배포해도제한이변경되지않습니다. 이경우 iOS 가변경내용을 iOS 프로필에적용하지않습니다. 계속하려면프로필제거정책을사용하여 iOS 프로필을제거한후업데이트된제한장치정책을배포해야합니다.

이설정을 **Only allow some apps(**일부앱만허용**)** 로변경하는경우: 이정책을배포하기전에 Apple 배포프로그램을사용하여등록된장치의사용자가설정도우미에서 Apple 계정에로그인할수있도록해당사용자에게알려줘야합니다. 그렇지않으면사용자가장치에서 2 단계인증을사용하지않도록설정해야 Apple 계정에로그인하고허용된앱에액세스할수있습니다.

- 진단제출수정**:** 사용자가 설정 **>** 진단및사용현황창의설정에서진단제출및앱분석설정을변경할수있도록허용합니다.
- **Bluetooth** 수정**:** 사용자가 Bluetooth 설정을수정할수있도록허용합니다.
- 받아쓰기허용**:** 감독되는경우에만해당. 이제한을 꺼짐으로설정하면음성텍스트변환을포함한받아쓰기입력이허용되지않습니다. 기본설정은 켜짐입니다.
- **WiFi** 정책에따라설치된 **WiFi** 네트워크에만참가**:** 선택사항입니다. 감독되는경우에만해당. 이제한을 켜짐으로설정하면구성프로필을통해설정된장치만 Wi-Fi 네트워크에참여할수있습니다. 기본설정은 꺼짐입니다.
- 메시지를표시하지않고교실앱이 **AirPlay** 및화면보기를수행할수있도록허용**:** 이제한을선택하면권한에대한메시지표시없이강사가학생장치에서 AirPlay 및화면보기를수행할수있습니다. 기본설정은선택취소되어있습니다. 감독되는 iOS 장치를위한설정입니다.
- 메시지를표시하지않고교실앱이앱및장치를잠글수있도록허용**:** 이제한을 켜짐으로설정하면교실앱이사용자에게메시지를표시하지않고자동으로사용자장치와앱을잠급니다. 기본설정은 꺼짐입니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
- 메시지를표시하지않고교실앱클래스에자동참가**:** 이제한을 켜짐으로설정하면교실앱이사용자에게메시지를표시하지않고사용자를자동으로클래스에참가시킵니다. 기본설정은 꺼짐입니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
- **AirPrint** 허용**:** 이제한을 꺼짐으로설정하면사용자가 AirPrint 를사용하여인쇄할수없습니다. 기본설정은 켜짐입니다. 이제한이 켜짐인경우다음과같은추가제한이표시됩니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
  - 키집합에 **AirPrint** 자격증명저장허용**:** 이제한을선택취소하면 AirPrint 사용자이름과암호가키집합에저장되지않습니다. 기본설정은선택되어있습니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
  - **iBeacon** 을사용하여 **AirPrint** 프린터검색허용**:** 이제한을선택취소하면 AirPrint 프린터에대한 iBeacon 검색이사용되지않습니다. 이렇게하면위장한 AirPrint Bluetooth 알림의네트워크트래픽피싱

이방지됩니다. 기본설정은선택되어있습니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.

* 신뢰할수있는인증서가있는대상에만 **AirPrint** 허용**:** 이제한을선택하면사용자가 AirPrint 를사용하여신뢰할수있는인증서가있는대상에만인쇄할수있습니다. 기본설정은선택취소되어있습니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.

- **VPN** 구성추가**:** 이제한을 꺼짐으로설정하면사용자가 VPN 구성을만들수없습니다. 기본설정은 켜짐입니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
- 셀룰러요금제설정수정**:** 이제한을 꺼짐으로설정하면사용자가셀룰러요금제설정을수정할수없습니다. 기본설정은 켜짐입니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
- 시스템앱제거**:** 이제한을 꺼짐으로설정하면사용자가시스템앱을장치에서제거할수없습니다. 기본설정은 켜짐입니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
- 새로운주변장치설정**:** 이제한을꺼짐으로설정하면사용자가새로운주변장치를설정할수없습니다. 기본설정은켜짐입니다. iOS 11(최소버전) 을실행하는감독되는장치에서사용할수있습니다.
- **USB** 제한모드허용**:** 꺼짐인경우장치가잠겨있는동안항상 USB 액세서리에연결할수있습니다. 기본값은 켜짐입니다. iOS 11.3 이상의감독되는장치에서만사용할수있습니다.
- 소프트웨어업데이트강제지연**:** 켜짐인경우사용자에게소프트웨어업데이트표시가지연됩니다. 이제한을적용하면소프트웨어업데이트릴리스날짜로부터지정된기간 (일) 까지소프트웨어업데이트가표시되지않습니다. 기본값은 꺼짐입니다. iOS 11.3 이상의감독되는장치에서만사용할수있습니다.
- 소프트웨어업데이트시행지연 **(**일**):** 장치에서소프트웨어업데이트를지연할일수를지정할수있습니다. 최대지연은 **90** 일입니다. 기본값은 **30** 일입니다. iOS 11.3 이상의감독되는장치에서만사용할수있습니다.
- 교실에서클래스를나갈때허가요청시행**:** 켜짐인경우교실앱을통해관리되지않는과정에등록한학생이과정을나가려면교사의허가를요청해야합니다. 기본값은 꺼짐입니다. iOS 11.3 이상의감독되는장치에서만사용할수있습니다.
- 자동날짜및시간적용**:** 감독되는장치에서날짜와시간을자동으로설정할수있습니다. 켜짐인경우장치사용자는 일반 **>** 날짜및시간에서 자동으로설정을끌수없습니다. 장치의표준시간대는장치가해당위치를확인할수있는경우에만업데이트됩니다. 즉, 장치에위치서비스가활성화된셀룰러연결또는 Wi-Fi 연결이있는경우입니다. 기본값은 꺼짐입니다. iOS 12 이상의감독되는장치에서만사용할수있습니다.
- 암호자동채우기**:** 선택사항입니다. 사용하지않는경우사용자는암호자동채우기또는강력한자동암호기능을사용할수없습니다. 기본값은 켜짐입니다. iOS 12 부터사용할수있습니다.
- 암호근접요청**:** 선택사항입니다. 사용하지않는경우사용자의장치는주변장치에서암호를요청하지않습니다. 기본값은 켜짐입니다. iOS 12 부터사용할수있습니다.
- 암호공유**:** 선택사항입니다. 사용하지않는경우사용자는 AirDrop 암호기능을사용하여암호를공유할수없습니다. 기본값은 켜짐입니다. iOS 12 부터사용할수있습니다.

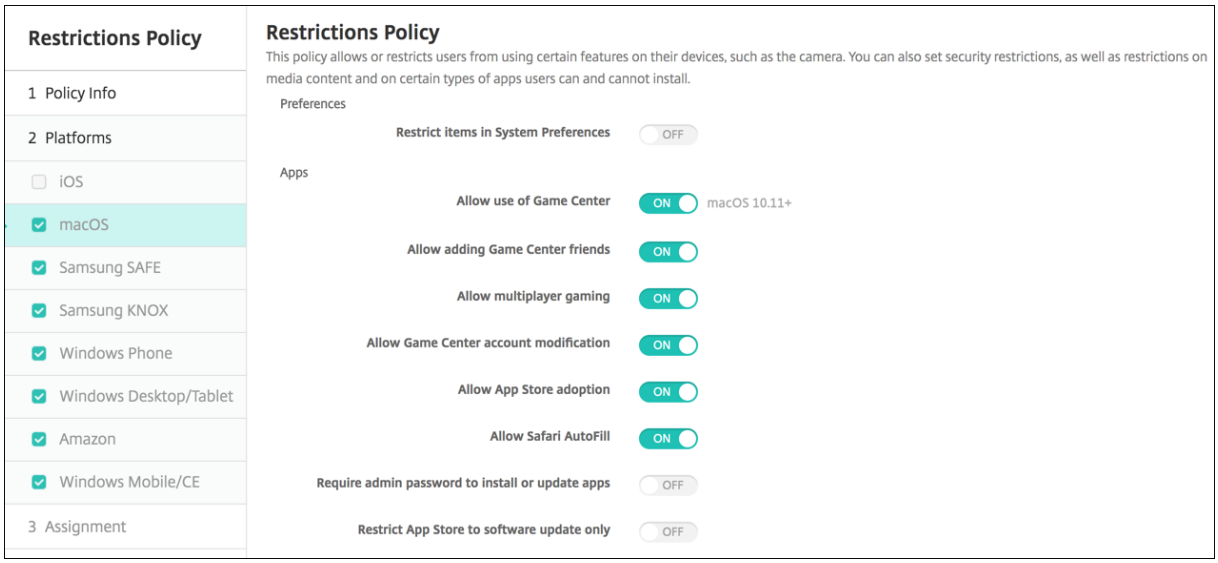
- 보안 **-** 잠금화면에표시
  - 제어센터**:** 잠금화면에서제어센터에액세스할수있습니다. 사용자는제어센터에서비행기모드, Wi-Fi, Bluetooth, 방해금지모드및회전잠금설정을쉽게수정할수있습니다.

  - 알림**:** 잠금화면에서알림을허용합니다.
  - 오늘의보기**:** 날씨및오늘날짜의일정항목과같은정보를잠금화면에집계하는 [오늘의보기] 를허용합니다.

- 미디어콘텐츠 **-** 허용
  - 음악**,** 팟캐스트및 **iTunes U** 의성인등급자료**:** 사용자의장치에무삭제판자료를허용합니다.
  - **iBooks** 의성관련성인등급콘텐츠**:** iBooks 에서무삭제판자료를다운로드하도록허용합니다.
  - 평가지역**:** 유해콘텐츠차단등급을얻는지역을설정합니다. 목록에서평가지역을설정할국가를클릭합니다. 기본값은미국입니다.
  - 영화**:** 사용자장치에서영화를허용할지여부를설정합니다. 영화가허용된경우선택적으로영화등급을설정합니다. 목록에서장치에영화를허용하거나제한하는옵션을선택합니다. 기본값은모든영화허용입니다.
  - **TV** 쇼**:** 사용자장치에서 TV 쇼를허용할지여부를설정합니다. TV 쇼가허용된경우선택적으로 TV 쇼등급을설정합니다. 목록에서장치에 TV 쇼를허용하거나제한하는옵션을선택합니다. 기본값은모든 TV 쇼허용입니다.
  - 앱**:** 사용자장치에서앱을허용할지여부를설정합니다. 앱이허용된경우선택적으로앱등급을설정합니다. 목록에서장치에앱을허용하거나제한하는옵션을선택합니다. 기본값은모든앱허용입니다.

- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    * 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    * 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 iOS 9.3 이상에서만사용할수있습니다.

macOS 설정



- 기본설정

- 시스템기본설정에서항목제한**:** 시스템기본설정에대한사용자액세스를허용하거나제한합니다. 기본값은시스템기본설정에대한사용자의전체액세스를허용하는 꺼짐입니다. 사용하는경우다음설정을구성합니다.
  - 시스템기본설정창**:** 선택한설정을사용할지여부를선택합니다. 기본값은모든설정을사용하도록설정하는것이며, 기본적으로 켜짐입니다.
    - 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**:** 추가를클릭하고사용자액세스를제한할폴더의파일경로 (예: /Applications/Utilities) 를입력한다음 저장을클릭합니다. 사용자가액세스할수없게하려는모든폴더에대해이단계를반복합니다.
    * 허용되는폴더**:** 추가를클릭하고사용자에게액세스하도록허가할폴더의파일경로를입력한다음 저장을클릭합니다. 사용자가액세스할수있게하려는모든폴더에대해이단계를반복합니다.
- 위젯
  - 다음대시보드위젯만실행되도록허용**:** 세계시계또는계산기와같이사용자에게실행하도록허용된대시보드위젯을허용하거나제한합니다. 기본값은사용자가모든위젯을실행하도록허용하는 꺼짐입니다. 사용하는경우다음설정을구성합니다.
    * 허용되는위젯**:** 추가를클릭하고실행하도록허용된위젯의이름및 ID 를입력한다음 저장을클릭합니다. 대시보드에서실행하려는각위젯에대해이단계를반복합니다.
- 미디어
  - **AirDrop** 허용**:** 사용자가인접한 iOS 장치와사진, 비디오, 웹사이트, 위치등을공유할수있도록허용합니다.
- 공유
  - 새공유서비스를자동으로사용**:** 공유서비스를자동으로사용할지여부를선택합니다.
  - 메일**:** 공유사서함을허용할지여부를선택합니다.
  - **Facebook:** 공유 Facebook 계정을허용할지여부를선택합니다.
  - 비디오서비스 **- Flickr, Vimeo, Tudou** 및 **Youku:** 공유비디오서비스를허용할지여부를선택합니다.
  - **Aperture** 에추가**:** Aperture 에공유기능을추가하도록허용할지여부를선택합니다.
  - **Sina Weibo:** 공유 Sina Weibo 마이크로블로그계정을허용할지여부를선택합니다.
  - **Twitter:** 공유 Twitter 계정을허용할지여부를선택합니다.
  - 메시지**:** 메시지에대한공유액세스를허용할지여부를선택합니다.
  - **iPhoto** 에추가**:** iPhoto 에공유기능을추가하도록허용할지여부를선택합니다.

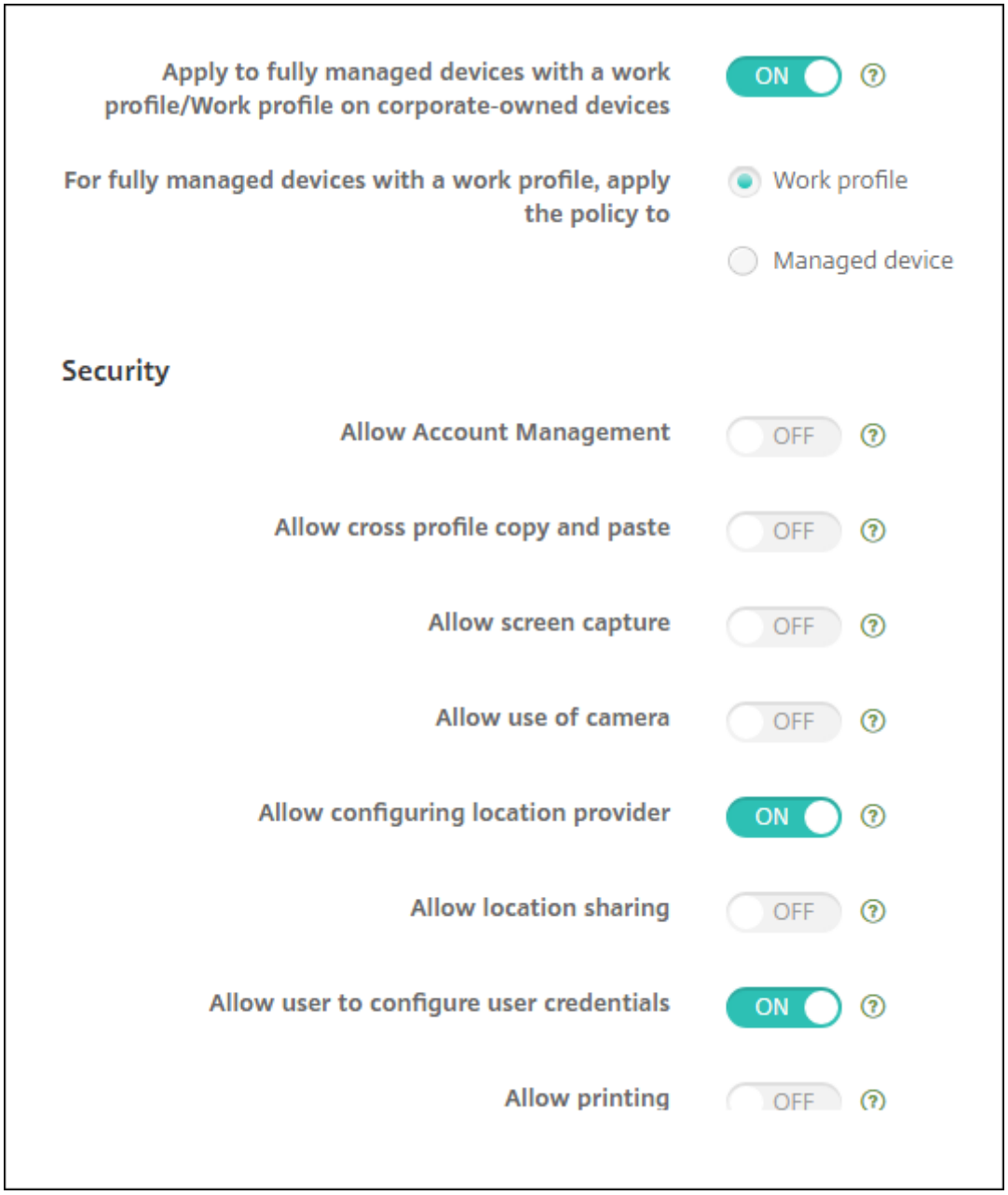
  - 읽기목록에추가**:** 읽기목록에공유기능을추가하도록허용할지여부를선택합니다.
  - **AirDrop:** 공유 AirDrop 계정을허용할지여부를선택합니다.
- 기능
  - 데스크톱바탕화면잠금**:** 사용자가바탕화면사진을변경할수있는지여부를선택합니다. 기본값은사용자가바탕화면사진을변경할수있는 꺼짐입니다.
  - 카메라사용허용**:** 사용자가 Mac 에서카메라를사용할수있는지여부를선택합니다. 기본값은사용자가카메라를사용할수없는 꺼짐입니다.
  - **Apple Music** 허용**:** 사용자가 Apple Music 서비스를사용할수있도록허용합니다 (macOS 10.12 이상). Apple Music 서비스를허용하지않는경우 Music 앱이클래식모드에서실행됩니다. 감독되는장치에만적용됩니다. 기본값은 켜짐입니다.
  - **Spotlight** 제안허용**:** 사용자가 Spotlight 제안을사용하여 Mac 을검색하고인터넷, iTunes 및 App Store 의 Spotlight 제안을제공할수있는지여부를선택합니다. 기본값은사용자가 Spotlight 제안을사용하지못하게하는 꺼짐입니다.
  - 조회허용**:** 사용자가상황에맞는메뉴또는 Spotlight 검색메뉴를사용하여단어의정의를조회할수있는지여부를선택합니다. 기본값은사용자가 Mac 에서조회를사용하지못하게하는꺼짐입니다.
  - 로컬계정에 **iCloud** 암호사용허용**:** 사용자가 Apple ID 및 iCloud 암호를사용하여 Mac 에로그온할수있는지여부를선택합니다. 이정책을사용하도록설정하면사용자가 Mac 의 모든로그인화면에서하나의 ID 와암호만사용하게됩니다. 기본값은사용자가 Apple ID 및 iCloud 암호를사용하여 Mac 에액세스할수있도록허용하는 켜짐입니다.
  - **iCloud** 문서및데이터허용**:** 사용자가 Mac 에서 iCloud 에저장된문서및데이터에액세스할수있도록허용할지여부를선택합니다. 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**:** 이옵션및 Apple Watch 에대한자세한내용은 https://www.imore.com/auto-unlock을참조하십시오 (macOS 10.12 이상). 기본값은 켜짐입니다.

- **Touch ID** 를통한 **Mac** 잠금해제허용**:** (macOS 10.12.4 이상). 기본값은 켜짐입니다.
- 소프트웨어업데이트강제지연**:** 켜짐인경우사용자에게소프트웨어업데이트표시가지연됩니다. 소프트웨어업데이트릴리스날짜로부터지정된기간 (일) 까지소프트웨어업데이트가표시되지않습니다. 기본값은 꺼짐입니다. macOS 10.13.4 이상을실행하는감독되는장치에만사용할수있습니다.
- 소프트웨어업데이트시행지연 **(**일**):** 장치에서소프트웨어업데이트를지연할일수를지정합니다. 최대값은 90 일입니다. 기본값은 **30** 입니다. macOS 10.13.4 이상을실행하는감독되는장치에만사용할수있습니다.
- 암호자동채우기**:** 선택사항입니다. 사용하지않는경우사용자는암호자동채우기또는강력한자동암호기능을사용할수없습니다. 기본값은 켜짐입니다. macOS 10.14 부터사용할수있습니다.
- 암호근접요청**:** 선택사항입니다. 사용하지않는경우사용자의장치는주변장치에서암호를요청하지않습니다. 기본값은 켜짐입니다. macOS 10.14 부터사용할수있습니다.
- 암호공유**:** 선택사항입니다. 사용하지않는경우사용자는 Airdrop 암호기능을사용하여암호를공유할수없습니다. 기본값은 켜짐입니다. macOS 10.14 부터사용할수있습니다.

Android 설정

- 카메라**:** 사용자가장치에서카메라를사용할수있도록허용합니다. 꺼짐인경우카메라가사용되지않습니다. 기본값은 켜짐입니다.

Android Enterprise 설정



새 Android 장치또는공장기본값으로재설정된 Android 장치가작업프로필모드로등록되면 Android 9.0-10.x 를실행하는장치는작업프로필이있는완전관리형장치로등록됩니다. Android 11 이상을실행하는장치는회사소유장치에서작업프로필로등록됩니다. 제한정책은장치또는관리되는장치의작업프로필에적용할수있습니다.

회사소유장치모드로작업프로필에등록된장치에서는다음제한을작업프로필에만사용할수있습니다.

- 백업서비스허용
- 시스템앱사용
- Keyguard 가장치를잠그지않도록방지

- 상태표시줄의사용허용
- 장치화면을켜진상태로유지
- 응용프로그램설정의사용자제어허용
- 사용자가사용자자격증명을구성하도록허용
- VPN 구성허용
- USB 대용량스토리지허용
- 공장기본값으로재설정허용
- 앱제거허용
- Google Play 이외의앱허용
- 상호프로필복사및붙여넣기허용
- 앱확인사용
- 계정관리허용
- 인쇄허용
- NFC 허용
- 사용자추가허용

Android Enterprise 의작업프로필모드에서장치를등록하는경우 **USB** 디버깅및알수없는소스설정은기본적으로사용되지않도록설정됩니다.

Android 9.0-10.x 및 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.

회사소유장치모드로작업프로필에등록된장치에는 Samsung 제한이적용되지않습니다. Knox 서비스플러그인 (KSP) 을사용하여이러한장치에 Samsung 제한을적용합니다. 자세한내용은 Samsung 설명서를참조하십시오.

최신 Samsung Knox 관리기능에 Samsung Knox 3.4 이상을사용할것을권장합니다.

- 작업프로필/회사소유장치의작업프로필을사용하는완전관리형장치에적용**:** 작업프로필로완전히관리되는장치에대해제한정책설정이구성될수있도록허용합니다. 이설정이 켜짐인경우다음설정중하나를선택합니다.
  - 작업프로필**:** 구성하는제한설정이장치의작업프로필에만적용됩니다.
  - 장치관리**:** 구성하는제한설정이장치에만적용됩니다.

  이설정이 꺼짐인경우구성하는자격증명설정은작업프로필에명시적으로적용되는설정을제외하고장치에적용됩니다. 기본값은 꺼짐입니다.

작업프로필/회사소유장치의작업프로필을사용하는완전관리형장치에적용이꺼짐인경우다음설정을구성합니다.

- 보안
  - 계정관리허용**:** 작업프로필및관리되는장치에계정을추가할수있습니다. 기본값은 꺼짐입니다.
  - 상호프로필복사및붙여넣기허용**:** 켜짐일경우사용자는 Android Enterprise 프로필의앱과개인영역의앱사이에복사해서붙여넣을수있습니다. 기본값은 꺼짐입니다.
  - 화면캡처허용**:** 사용자가장치화면의화면캡처를기록하거나생성할수있습니다. 기본값은 꺼짐입니다.

- 카메라사용허용**:** 사용자가장치카메라로사진을찍고비디오를만들수있습니다. 기본값은 꺼짐입니다.
- **VPN** 구성허용**:** 사용자가 VPN 구성을만들수있습니다. Android 6 이상을실행하는작업프로필장치와완전관리형장치를위한설정입니다. 기본값은 켜짐입니다.
- 백업서비스허용**:** 사용자가장치에서응용프로그램및시스템데이터를백업할수있습니다. 기본값은 켜짐입니다.
- **NFC** 허용**:** 사용자가 NFC(근거리통신) 를사용하여장치의웹페이지, 사진, 비디오또는기타콘텐츠를다른장치로보낼수있도록허용합니다. MDM 4.0 이상에해당합니다. 기본값은 켜짐입니다.
- 위치공급자구성허용**:** 사용자가자신의장치에서 GPS 를켤수있습니다. Android API 28 이상을위한설정입니다. 기본값은 켜짐입니다.
- 위치공유허용**:** 관리되는프로필의경우장치소유자가이설정을재정의할수있습니다. 기본값은 꺼짐입니다.

  > 팁**:**
  >
  > XenMobile 에서위치장치정책을만들어지리적경계를적용할수있습니다. 위치장치정책을참조하십시오.

- 사용자가사용자자격증명을구성하도록허용**:** 사용자가관리형키저장소의자격증명을구성할수있는지여부를지정합니다. 기본값은 켜짐입니다.
- 인쇄허용**:** 켜짐인경우이설정은사용자가사용자장치에서액세스할수있는모든프린터로인쇄할수있도록허용합니다. 기본값은 꺼짐입니다. Android 9 이상에서사용할수있습니다.
- **USB** 디버깅허용**:** 기본값은 꺼짐입니다.

- 앱
  - 시스템앱사용**:** 사용자가사전설치된장치앱을실행할수있도록허용합니다. 기본값은 꺼짐입니다. 특정앱을사용하려면 시스템앱목록테이블에서 추가를클릭합니다.
    - 시스템앱목록**:** 장치에서사용할시스템앱목록입니다. 시스템앱사용을 켜짐으로설정하고앱패키지이름을추가합니다. 시스템앱의패키지이름을조회하려면 Android Debug Bridge(adb) 를사용하여 Android 패키지관리자 (pm) 명령을호출하면됩니다. 예: `adb shell "pm list packages -f name"`. 여기서 "name" 은패키지이름의일부입니다. 자세한내용은 https://developer.android.com/studio/command-line/adb 항목을참조하십시오. Android Enterprise 기기의경우 Android Enterprise 앱권한 정책을사용하여앱권한을제한할수있습니다.
  - 응용프로그램사용안함**:** 장치에서지정된목록의앱이실행되지않도록차단합니다. 기본값은 꺼짐입니다. 설치된앱을사용하지않도록설정하려면설정을 켜짐으로변경한다음 응용프로그램목록테이블에서 추가를클릭합니다.
    - 응용프로그램목록**:** 차단하려는앱의목록입니다. 응용프로그램사용안함을 켜짐으로설정하고앱을추가합니다. 앱패키지이름을입력합니다. 앱목록을변경하고배포하면이전앱목록을덮어씁니다. 예: com.example1 및 com.example2 를사용하지않도록설정하고나중에 com.example1 및 com.example3 으로목록을변경하는경우 XenMobile 은 com.example.2 를사용하도록설정합니다.
  - 앱확인사용**:** OS 에서앱을검사하여악성동작을검색할수있도록합니다. 기본값은 켜짐입니다.
  - **Google** 앱사용**:** 사용자가 Google 모바일서비스에서컨테이너로앱을다운로드할수있습니다. 기본값은 켜짐입니다.
  - **Google Play** 이외의앱허용**:** Google Play 이외의스토어에서앱을설치할수있습니다. 기본값은 꺼짐입니다.

- 응용프로그램설정의사용자제어허용**:** 사용자가앱을제거하고, 앱을사용하지않도록설정하고, 캐시및데이터를지우고, 앱을강제로중지하고, 기본값을지울수있습니다. 사용자는설정앱에서이러한작업을수행합니다. 기본값은 꺼짐입니다.
- 앱제거허용**:** 사용자가관리되는 Google Play 스토어내에서앱을제거하도록허용합니다. 기본값은 꺼짐입니다. 이설정을표시하려면서버속성 (`afw.restriction.policy.v2`) 을활성화합니다. 서버속성에대한자세한내용은 서버속성을참조하십시오.

- **BYOD** 작업프로필
  - 홈화면에작업프로필앱위젯허용**:** 이설정이 켜짐인경우사용자가작업프로필앱위젯을장치홈화면에배치할수있습니다. 이설정이 꺼짐인경우사용자가작업프로필앱위젯을장치홈화면에배치할수없습니다. 기본값은 꺼짐입니다.
    - 위젯이허용되는앱**:** 홈화면에서허용할앱목록입니다. 홈화면에작업프로필앱위젯허용을 켜짐으로설정하고앱을추가합니다. 추가를클릭하고목록에서홈화면에허용할위젯의앱을선택합니다. 저장을클릭합니다. 더많은앱위젯을허용하려면이프로세스를반복합니다.
  - 장치연락처에작업프로필연락처허용**:** 수신전화에대해관리되는 Android Enterprise 프로필에있는연락처가상위프로필에표시됩니다 (Android 7.0 이상). 기본값은 꺼짐입니다.

- 완전관리형장치만
  - 사용자추가허용**:** 사용자가장치에새사용자를추가할수있도록허용합니다. 기본값은 켜짐입니다.
  - 데이터로밍허용**:** 로밍하는동안사용자가셀룰러데이터를사용할수있도록허용합니다. 기본값은꺼짐이며, 사용자의장치에서로밍이비활성화됩니다. 기본값은 꺼짐입니다.
  - **SMS** 허용**:** 사용자가 SMS 메시지를보내고받을수있습니다. 기본값은 꺼짐입니다.
  - 상태표시줄의사용허용**:** 켜짐인경우관리되는장치및전용장치 (COSU 장치라고도함) 에서상태표시줄이사용됩니다. 이렇게설정하면알림, 빠른설정및전체화면모드에서벗어날수있는기타화면오버레이가사용되지않습니다. 사용자는시스템설정으로이동하여알림을볼수있습니다. Android 6.0 이상을위한설정입니다. 기본값은 꺼짐입니다.
  - **Bluetooth** 허용**:** 사용자가 Bluetooth 를사용할수있습니다. 기본값은 켜짐입니다.
    - **Bluetooth** 공유허용**:** 선택을취소할경우사용자가장치에서나가는 Bluetooth 공유를설정할수없습니다. 기본값은선택되어있습니다. 이설정을표시하려면서버속성 (`afw.restriction.policy.v2`) 을활성화합니다. 서버속성에대한자세한내용은 서버속성을참조하십시오.
  - 날짜및시간구성허용**:** 사용자가장치에서날짜및시간을변경할수있습니다. 기본값은 켜짐입니다.
  - 공장기본값으로재설정허용**:** 사용자가장치에서공장기본값으로재설정을수행할수있습니다. 기본값은 켜짐입니다.
  - 장치화면을켜진상태로유지**:** 이설정을 켜짐으로설정하면장치를연결할때장치화면이켜진상태로유지됩니다. 기본값은 꺼짐입니다.
  - **USB** 대용량스토리지허용**:** USB 연결을통해사용자의장치와컴퓨터간에서대용량데이터파일을전송할수있습니다. 기본값은 켜짐입니다.
  - 마이크허용**:** 사용자가장치에서마이크를사용할수있습니다. 기본값은 켜짐입니다.
  - 테더링허용**:** 사용자가휴대용핫스폿을구성하고데이터를테더링할수있습니다. 기본값은 꺼짐입니다.
  - **Keyguard** 가장치를잠그지않도록방지**:** 켜짐일경우관리되는장치및전용장치 (COSU 장치라고도함) 의잠금화면에서 Keyguard 가사용되지않습니다. 기본값은 꺼짐입니다.
  - **Wi-Fi** 변경허용**:** 켜짐인경우사용자가 Wi-Fi 를켜거나끄고 Wi-Fi 네트워크에연결할수있습니다. 기본값은 켜짐입니다.

- 파일전송허용**:** USB 를통한파일전송을허용합니다. 기본값은 꺼짐입니다.

- **Samsung**
  - **TIMA** 키저장소사용**:** TIMA 키저장소는대칭키에대한 TrustZone 기반의보안키저장소를제공합니다. RSA 키쌍및인증서는저장을위해기본키저장소공급자로라우팅됩니다. 기본값은 꺼짐입니다.
  - 공유목록허용**:** 사용자가공유방법목록의앱간에서콘텐츠를공유할수있습니다. 기본값은 켜짐입니다.
  - 감사로그사용**:** 장치의법의학분석을위한이벤트감사로그만들기를사용하도록설정합니다. 기본값은 꺼짐입니다.

- **Samsung:** 완전관리형장치만
  - **ODE** 신뢰할수있는부팅확인사용**:** ODE 신뢰할수있는부팅확인을사용하여 bootloader 에서시스템이미지까지신뢰체인을설정합니다. 기본값은 켜짐입니다.
  - 긴급호출만허용**:** 사용자가장치에서긴급통화전용모드를사용할수있습니다. 기본값은 꺼짐입니다.
  - 펌웨어복구허용**:** 사용자가장치에서펌웨어를복구할수있습니다. 기본값은 켜짐입니다.
  - 빠른암호화허용**:** 사용된메모리공간의암호화만허용합니다. 이암호화는모든데이터를암호화하는전체디스크암호화와대조됩니다. 이데이터에는설정, 응용프로그램데이터, 다운로드한파일및응용프로그램, 미디어및기타파일이포함됩니다. 기본값은 켜짐입니다.
  - **Common Criteria** 모드사용**:** 장치를 Common Criteria 모드로전환합니다. Common Criteria 구성은엄격한보안프로세스를적용합니다. 기본값은 켜짐입니다.
  - 재부팅배너사용**:** 사용자의장치가다시시작되면 DoD 에서승인시스템사용알림메시지또는배너를표시합니다. 기본값은 꺼짐입니다.
  - 설정변경허용**:** 사용자가완전관리형장치에서설정을변경할수있습니다. 기본값은 켜짐입니다.
  - 백그라운드데이터사용활성화**:** 완전히관리되는장치의경우앱이백그라운드에서데이터를동기화할수있습니다. 기본값은 켜짐입니다.
  - 클립보드허용**:** 사용자가장치의클립보드에데이터를복사할수있도록허용합니다.
    * 클립보드공유허용**:** 사용자가장치와컴퓨터간에서클립보드콘텐츠를공유할수있도록허용합니다 (MDM 4.0 이상).
  - 홈키허용**:** 사용자가완전관리형장치에서 홈키를사용할수있습니다. 기본값은 켜짐입니다.
  - 모의위치허용**:** 사용자가 GPS 위치를조작할수있습니다. 완전관리형장치에사용할수있습니다. 기본값은 꺼짐입니다.
  - **NFC:** 사용자가완전관리형장치에서 NFC 를사용할수있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
  - 전원끄기허용**:** 사용자가완전관리형장치를끌수있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
  - **Wi-Fi Direct** 허용**:** 사용자가 Wi-Fi 연결을통해다른장치에직접연결할수있습니다. 기본값은 켜짐입니다. 켜짐인경우 **Wi-Fi** 변경허용설정을사용하도록설정해야합니다.
  - **SD** 카드허용**:** 가능한경우사용자가장치에서 SD 카드를사용할수있습니다. 기본값은 켜짐입니다.
  - **USB** 호스트스토리지허용**:** USB 장치가연결될때사용자의장치가 USB 호스트로작동할수있도록허용합니다. 그러면사용자의장치가 USB 장치에전원을공급합니다. 기본값은 켜짐입니다.
  - 음성다이얼허용**:** 사용자가장치에서음성다이얼을사용할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
  - **S Beam** 허용**:** 사용자가 NFC 및 Wi-Fi Direct 를사용하여다른사용자와콘텐츠를공유할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
  - **S Voice** 허용**:** 사용자가장치에서지능형개인비서및지식탐색기를사용할수있습니다 (MDM 4.0 이상). 기본값은

켜짐입니다.

- **USB** 테더링허용**:** 사용자가 USB 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 테더링허용설정도 켜짐이어야합니다.
- **Bluetooth** 테더링허용**:** 사용자가 Bluetooth 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 테더링허용설정도 켜짐이어야합니다.
  - **Bluetooth** 공유허용**:** 선택을취소할경우사용자가장치에서나가는 Bluetooth 공유를설정할수없습니다. 기본값은선택되어있습니다. 이설정을표시하려면서버속성 (`afw.restriction.policy.v2`) 을활성화합니다. 서버속성에대한자세한내용은 서버속성을참조하십시오.
- **Wi-Fi** 테더링허용**:** 사용자가 Wi-Fi 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 테더링허용설정도 켜짐이어야합니다.
- 들어오는 **MMS** 허용**:** 사용자가 MMS 메시지를받을수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 나가는 **MMS** 허용**:** 사용자가 MMS 메시지를보낼수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 들어오는 **SMS** 허용**:** 사용자가 SMS 메시지를받을수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 나가는 **SMS** 허용**:** 사용자가 SMS 메시지를보낼수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 모바일네트워크구성**:** 사용자가셀룰러데이터연결을사용할수있도록허용합니다. 기본값은 꺼짐입니다.
- 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).
- 보안 **VPN** 통신만허용**:** 사용자가보안연결만사용할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- 오디오녹음허용**:** 사용자가장치에서오디오를녹음할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다. 켜짐인경우 마이크허용설정을켜야합니다.
- 비디오녹화허용**:** 사용자가장치에서비디오를녹화할수있습니다 (MDM 4.0 이상). 기본값은 꺼짐입니다. 켜짐인경우 카메라사용허용설정을켜야합니다.
- 로밍시푸시메시지허용**:** 사용자가푸시에셀룰러데이터를사용할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 데이터로밍허용설정을사용하도록설정해야합니다.
- 로밍시자동동기화허용**:** 사용자가동기화에셀룰러데이터를사용할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 데이터로밍허용설정을사용하도록설정해야합니다.
- 로밍시음성통화허용**:** 사용자가음성통화에셀룰러데이터를사용할수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 데이터로밍허용설정을사용하도록설정해야합니다.

- **Samsung: Knox** 컨테이너**/**완전관리형장치
  - 해지확인사용**:** 해지된인증서를확인할수있습니다. 기본값은 꺼짐입니다.
- **Samsung: Knox** 컨테이너만

- 앱을컨테이너로이동**:** 사용자가 Knox 컨테이너와장치의개인영역간에앱을이동할수있습니다. 기본값은 켜짐입니다.
- 다단계인증적용**:** 사용자는지문과함께암호또는 PIN 과같은다른인증방법을사용하여장치를열어야합니다. 기본값은 켜짐입니다.
- 컨테이너에대한인증적용**:** 장치의잠금을해제하는데사용되는방법과다른인증방법을사용하여 KNOX 컨테이너를여십시오. 기본값은 켜짐입니다.
- 보안키패드사용**:** 사용자가 Knox 컨테이너내부의보안키보드를사용하도록강제합니다. 기본값은 켜짐입니다.

- **Samsung: DeX**
  - **Samsung DeX** 사용**:** 지원되는 Knox 지원장치가 Samsung DeX 모드에서실행되도록합니다. Samsung Knox 3.1(최소버전) 이필요합니다. 기본값은 켜짐입니다. Samsung DeX 장치요구사항및 Samsung DeX 설정방법에대한자세한내용은 Samsung 개발자문서를참조하십시오.
    * **DeX** 모드에서만이더넷허용**:** Samsung DeX 모드에서이더넷을사용하도록설정합니다 DeX 모드에서는 셀룰러데이터, Wi-Fi, 테더링 (Wi-Fi, Bluetooth 및 USB) 이제한됩니다. 기본값은선택되어있지않습니다.
    * **DeX** 로고이미지업로드**:** Samsung DeX 아이콘으로사용할.png 이미지를지정하려면이설정을선택합니다.
    * **DeX** 화면시간초과 **(**초**):** DeX 화면이꺼질때까지의유휴시간 (초) 을지정합니다. 시간초과를비활성화하려면 **0** 을입력합니다. 기본값은 **1200** 초 (20 분) 입니다.
    * **Samsung DeX** 앱에서앱바로가기추가**:** 앱패키지이름을지정하여앱바로가기를 DeX 파일에추가합니다. 앱패키지이름을조회하려면 Google Play 로이동하여앱을선택합니다. URL 에는패키지이름 (`https://play.google.com/store/apps/details?id=<package.name><!--NeedCopy-->`) 이포함됩니다.
    * **Samsung DeX** 앱에서앱바로가기제거**:** 앱패키지이름을지정하여 DeX 에서바로가기를제거합니다. 앱패키지이름을조회하려면 Google Play 로이동합니다.
    * **Samsung DeX** 모드에서비활성화할앱패키지**:** Samsung DeX 모드에서차단할앱패키지의쉼표로구분된목록을지정합니다. 예: `"com.android.chrome", "com.google.android.gm"` `<!--NeedCopy-->`.

작업프로필로완전히관리되는장치에적용이켜짐이고 작업프로필이있는완전히관리되는장치의경우정책을다음항목에적용이 작업프로필로설정된경우다음설정을구성합니다.

- 보안
  - 계정관리허용**:** 작업프로필및관리되는장치에계정을추가할수있습니다. 기본값은 꺼짐입니다.
  - 상호프로필복사및붙여넣기허용**:** 켜짐일경우사용자는 Android Enterprise 프로필의앱과개인영역의앱사이에복사해서붙여넣을수있습니다. 기본값은 꺼짐입니다.
  - 화면캡처허용**:** 사용자가장치화면의화면캡처를기록하거나생성할수있습니다. 기본값은 꺼짐입니다.
  - 카메라사용허용**:** 사용자가장치카메라로사진을찍고비디오를만들수있습니다. 기본값은 꺼짐입니다.
  - 위치공급자구성허용**:** 사용자가자신의장치에서 GPS 를켤수있습니다. Android API 28 이상을위한설정입니다. 기본값은 켜짐입니다.

- 위치공유허용**:** 관리되는프로필의경우장치소유자가이설정을재정의할수있습니다. 기본값은 꺼짐입니다.

  > 팁**:**
  >
  > XenMobile 에서위치장치정책을만들어지리적경계를적용할수있습니다. 위치장치정책을참조하십시오.

- 사용자가사용자자격증명을구성하도록허용**:** 사용자가관리형키저장소의자격증명을구성할수있는지여부를지정합니다. 기본값은 켜짐입니다.
- 인쇄허용**:** 켜짐인경우이설정은사용자가사용자장치에서액세스할수있는모든프린터로인쇄할수있도록허용합니다. 기본값은 꺼짐입니다. Android 9 이상에서사용할수있습니다.

- 앱
  - 시스템앱사용**:** 사용자가사전설치된장치앱을실행할수있도록허용합니다. 기본값은 꺼짐입니다. 특정앱을사용하려면 시스템앱목록테이블에서 추가를클릭합니다.
    - 시스템앱목록**:** 장치에서사용할시스템앱목록입니다. 시스템앱사용을 켜짐으로설정하고앱패키지이름을추가합니다. 시스템앱의패키지이름을조회하려면 Android Debug Bridge(`adb`) 를사용하여 Android 패키지관리자 (`pm`) 명령을호출하면됩니다. 예: `adb shell "pm list packages -f name "`. 여기서 "name" 은패키지이름의일부입니다. 자세한내용은 https://developer.android.com/studio/command-line/adb 항목을참조하십시오. Android Enterprise 기기의경우 Android Enterprise 앱권한 정책을사용하여앱권한을제한할수있습니다.
  - 응용프로그램사용안함**:** 장치에서지정된목록의앱이실행되지않도록차단합니다. 기본값은 꺼짐입니다. 설치된앱을사용하지않도록설정하려면설정을 켜짐으로변경한다음 응용프로그램목록테이블에서 추가를클릭합니다.
    - 응용프로그램목록**:** 차단하려는앱의목록입니다. 응용프로그램사용안함을 켜짐으로설정하고앱을추가합니다. 앱패키지이름을입력합니다. 앱목록을변경하고배포하면이전앱목록을덮어씁니다. 예: com.example1 및 com.example2 를사용하지않도록설정하고나중에 com.example1 및 com.example3 으로목록을변경하는경우 XenMobile 은 com.example.2 를사용하도록설정합니다.
  - 앱확인사용**:** OS 에서앱을검사하여악성동작을검색할수있도록합니다. 기본값은 켜짐입니다.
  - **Google** 앱사용**:** 사용자가 Google 모바일서비스에서컨테이너로앱을다운로드할수있습니다. 기본값은 켜짐입니다.
  - **Google Play** 이외의앱허용**:** Google Play 이외의스토어에서앱을설치할수있습니다. 기본값은 꺼짐입니다.
  - 응용프로그램설정의사용자제어허용**:** 사용자가앱을제거하고, 앱을사용하지않도록설정하고, 캐시및데이터를지우고, 앱을강제로중지하고, 기본값을지울수있습니다. 사용자는설정앱에서이러한작업을수행합니다. 기본값은 꺼짐입니다.
  - 앱제거허용**:** 사용자가관리되는 Google Play 스토어내에서앱을제거하도록허용합니다. 기본값은 꺼짐입니다. 이설정을표시하려면서버속성 (`afw.restriction.policy.v2`) 을활성화합니다. 서버속성에대한자세한내용은 서버속성을참조하십시오.

- **BYOD** 작업프로필
  - 홈화면에작업프로필앱위젯허용**:** 이설정이 켜짐인경우사용자가작업프로필앱위젯을장치홈화면에배치할수있습니다. 이설정이 꺼짐인경우사용자가작업프로필앱위젯을장치홈화면에배치할수없습니다. 기본값은 꺼짐입니다.
    - 위젯이허용되는앱**:** 홈화면에서허용할앱목록입니다. 홈화면에작업프로필앱위젯허용을 켜짐으로설정하고앱을추가합니다. 추가를클릭하고목록에서홈화면에허용할위젯의앱을선택합니다. 저장을클릭합니다. 더많은

앱위젯을허용하려면이프로세스를반복합니다.

- 장치연락처에작업프로필연락처허용**:** 수신전화에대해관리되는 Android Enterprise 프로필에있는연락처가상위프로필에표시됩니다 (Android 7.0 이상). 기본값은 꺼짐입니다.

- **Samsung**
  - **TIMA** 키저장소사용**:** TIMA 키저장소는대칭키에대한 TrustZone 기반의보안키저장소를제공합니다. RSA 키쌍및인증서는저장을위해기본키저장소공급자로라우팅됩니다. 기본값은 꺼짐입니다.
  - 공유목록허용**:** 사용자가공유방법목록의앱간에서콘텐츠를공유할수있습니다. 기본값은 켜짐입니다.
  - 감사로그사용**:** 장치의법의학분석을위한이벤트감사로그만들기를사용하도록설정합니다. 기본값은 꺼짐입니다.
- **Samsung: Knox** 컨테이너**/**완전관리형장치
  - 해지확인사용**:** 해지된인증서를확인할수있습니다. 기본값은 꺼짐입니다.
- **Samsung: Knox** 컨테이너만
  - 앱을컨테이너로이동**:** 사용자가 Knox 컨테이너와장치의개인영역간에서앱을이동할수있습니다. 기본값은 켜짐입니다.
  - 다단계인증적용**:** 사용자는지문과함께암호또는 PIN 과같은다른인증방법을사용하여장치를열어야합니다. 기본값은 켜짐입니다.
  - 컨테이너에대한인증적용**:** 장치의잠금을해제하는데사용되는방법과다른인증방법을사용하여 KNOX 컨테이너를여십시오. 기본값은 켜짐입니다.
  - 보안키패드사용**:** 사용자가 Knox 컨테이너내부의보안키보드를사용하도록강제합니다. 기본값은 켜짐입니다.

작업프로필로완전히관리되는장치에적용이켜짐이고 작업프로필이있는완전히관리되는장치의경우정책을다음항목에적용이 관리되는장치로설정된경우다음설정을구성합니다.

- 보안
  - 계정관리허용**:** 작업프로필및관리되는장치에계정을추가할수있습니다. 기본값은 꺼짐입니다.
  - 상호프로필복사및붙여넣기허용**:** 켜짐일경우사용자는 Android Enterprise 프로필의앱과개인영역의앱사이에복사해서붙여넣을수있습니다. 기본값은 꺼짐입니다.
  - 화면캡처허용**:** 사용자가장치화면의화면캡처를기록하거나생성할수있습니다. 기본값은 꺼짐입니다.
  - 카메라사용허용**:** 사용자가장치카메라로사진을찍고비디오를만들수있습니다. 기본값은 꺼짐입니다.
  - **VPN** 구성허용**:** 사용자가 VPN 구성을만들수있습니다. Android 6 이상을실행하는작업프로필장치와완전관리형장치를위한설정입니다. 기본값은 켜짐입니다.
  - 백업서비스허용**:** 사용자가장치에서응용프로그램및시스템데이터를백업할수있습니다. 기본값은 켜짐입니다.
  - **NFC** 허용**:** 사용자가 NFC(근거리통신) 를사용하여장치의웹페이지, 사진, 비디오또는기타콘텐츠를다른장치로보낼수있도록허용합니다. MDM 4.0 이상에해당합니다. 기본값은 켜짐입니다.
  - 위치공급자구성허용**:** 사용자가자신의장치에서 GPS 를켤수있습니다. Android API 28 이상을위한설정입니다. 기본값은 켜짐입니다.
  - 위치공유허용**:** 관리되는프로필의경우장치소유자가이설정을재정의할수있습니다. 기본값은 꺼짐입니다.

> 팁:
>
> XenMobile 에서위치장치정책을만들어지리적경계를적용할수있습니다. 위치장치정책을참조하십시오.

  - 사용자가사용자자격증명을구성하도록허용: 사용자가관리형키저장소의자격증명을구성할수있는지여부를지정합니다. 기본값은 켜짐입니다.
  - 인쇄허용: 켜짐인경우이설정은사용자가사용자장치에서액세스할수있는모든프린터로인쇄할수있도록허용합니다. 기본값은 꺼짐입니다. Android 9 이상에서사용할수있습니다.
  - **USB** 디버깅허용: 기본값은 꺼짐입니다.

- 앱
  - 시스템앱사용: 사용자가사전설치된장치앱을실행할수있도록허용합니다. 기본값은 꺼짐입니다. 특정앱을사용하려면 시스템앱목록테이블에서 추가를클릭합니다.
    * 시스템앱목록: 장치에서사용할시스템앱목록입니다. 시스템앱사용을 켜짐으로설정하고앱패키지이름을추가합니다. 시스템앱의패키지이름을조회하려면 Android Debug Bridge(`adb`) 를사용하여 Android 패키지관리자 (`pm`) 명령을호출하면됩니다. 예: `adb shell "pm list packages -f name "`. 여기서 "name" 은패키지이름의일부입니다. 자세한내용은 https://developer.android.com/studio/command-line/adb 항목을참조하십시오. Android Enterprise 기기의경우 Android Enterprise 앱권한 정책을사용하여앱권한을제한할수있습니다.
  - 응용프로그램사용안함: 장치에서지정된목록의앱이실행되지않도록차단합니다. 기본값은 꺼짐입니다. 설치된앱을사용하지않도록설정하려면설정을 켜짐으로변경한다음 응용프로그램목록테이블에서 추가를클릭합니다.
    * 응용프로그램목록: 차단하려는앱의목록입니다. 응용프로그램사용안함을 켜짐으로설정하고앱을추가합니다. 앱패키지이름을입력합니다. 앱목록을변경하고배포하면이전앱목록을덮어씁니다. 예: com.example1 및 com.example2 를사용하지않도록설정하고나중에 com.example1 및 com.example3 으로목록을변경하는경우 XenMobile 은 com.example.2 를사용하도록설정합니다.
  - 앱확인사용: OS 에서앱을검사하여악성동작을검색할수있도록합니다. 기본값은 켜짐입니다.
  - **Google** 앱사용: 사용자가 Google 모바일서비스에서컨테이너로앱을다운로드할수있습니다. 기본값은 켜짐입니다.
  - **Google Play** 이외의앱허용: Google Play 이외의스토어에서앱을설치할수있습니다. 기본값은 꺼짐입니다.
  - 응용프로그램설정의사용자제어허용: 사용자가앱을제거하고, 앱을사용하지않도록설정하고, 캐시및데이터를지우고, 앱을강제로중지하고, 기본값을지울수있습니다. 사용자는설정앱에서이러한작업을수행합니다. 기본값은 꺼짐입니다.
  - 앱제거허용: 사용자가관리되는 Google Play 스토어내에서앱을제거하도록허용합니다. 기본값은 꺼짐입니다. 이설정을표시하려면서버속성 (`afw.restriction.policy.v2`) 을활성화합니다. 서버속성에대한자세한내용은 서버속성을참조하십시오.

- 완전관리형장치만
  - 사용자추가허용: 사용자가장치에새사용자를추가할수있도록허용합니다. 기본값은 켜짐입니다.
  - 데이터로밍허용: 로밍하는동안사용자가셀룰러데이터를사용할수있도록허용합니다. 기본값은꺼짐이며, 사용자의장치에서로밍이비활성화됩니다. 기본값은 꺼짐입니다.
  - **SMS** 허용: 사용자가 SMS 메시지를보내고받을수있습니다. 기본값은 꺼짐입니다.

- 상태표시줄의사용허용**:** 켜짐인경우관리되는장치및전용장치 (COSU 장치라고도함) 에서상태표시줄이사용됩니다. 이렇게설정하면알림, 빠른설정및전체화면모드에서벗어날수있는기타화면오버레이가사용되지않습니다. 사용자는시스템설정으로이동하여알림을볼수있습니다. Android 6.0 이상을위한설정입니다. 기본값은 꺼짐입니다.
- **Bluetooth** 허용**:** 사용자가 Bluetooth 를사용할수있습니다. 기본값은 켜짐입니다.
  - **Bluetooth** 공유허용**:** 선택을취소할경우사용자가장치에서나가는 Bluetooth 공유를설정할수없습니다. 기본값은선택되어있습니다. 이설정을표시하려면서버속성 (`afw.restriction.policy.v2`) 을활성화합니다. 서버속성에대한자세한내용은 서버속성을참조하십시오.
- 날짜및시간구성허용**:** 사용자가장치에서날짜및시간을변경할수있습니다. 기본값은 켜짐입니다.
- 공장기본값으로재설정허용**:** 사용자가장치에서공장기본값으로재설정을수행할수있습니다. 기본값은 켜짐입니다.
- 장치화면을켜진상태로유지**:** 이설정을 켜짐으로설정하면장치를연결할때장치화면이켜진상태로유지됩니다. 기본값은 꺼짐입니다.
- **USB** 대용량스토리지허용**:** USB 연결을통해사용자의장치와컴퓨터간에서대용량데이터파일을전송할수있습니다. 기본값은 켜짐입니다.
- 마이크허용**:** 사용자가장치에서마이크를사용할수있습니다. 기본값은 켜짐입니다.
- 테더링허용**:** 사용자가휴대용핫스폿을구성하고데이터를테더링할수있습니다. 기본값은 꺼짐입니다. 이설정이켜져있으면 Samsung 장치에서다음설정을사용할수있습니다.
- **Keyguard** 가장치를잠그지않도록방지**:** 켜짐일경우관리되는장치및전용장치 (COSU 장치라고도함) 의잠금화면에서 Keyguard 가사용되지않습니다. 기본값은 꺼짐입니다.
- **Wi-Fi** 변경허용**:** 켜짐인경우사용자가 Wi-Fi 를켜거나끄고 Wi-Fi 네트워크에연결할수있습니다. 기본값은 켜짐입니다.
- 파일전송허용**:** USB 를통한파일전송을허용합니다. 기본값은 꺼짐입니다.

- **Samsung**
  - **TIMA** 키저장소사용**:** TIMA 키저장소는대칭키에대한 TrustZone 기반의보안키저장소를제공합니다. RSA 키쌍및인증서는저장을위해기본키저장소공급자로라우팅됩니다. 기본값은 꺼짐입니다.
  - 공유목록허용**:** 사용자가공유방법목록의앱간에서콘텐츠를공유할수있습니다. 기본값은 켜짐입니다.
  - 감사로그사용**:** 장치의법의학분석을위한이벤트감사로그만들기를사용하도록설정합니다. 기본값은 꺼짐입니다.

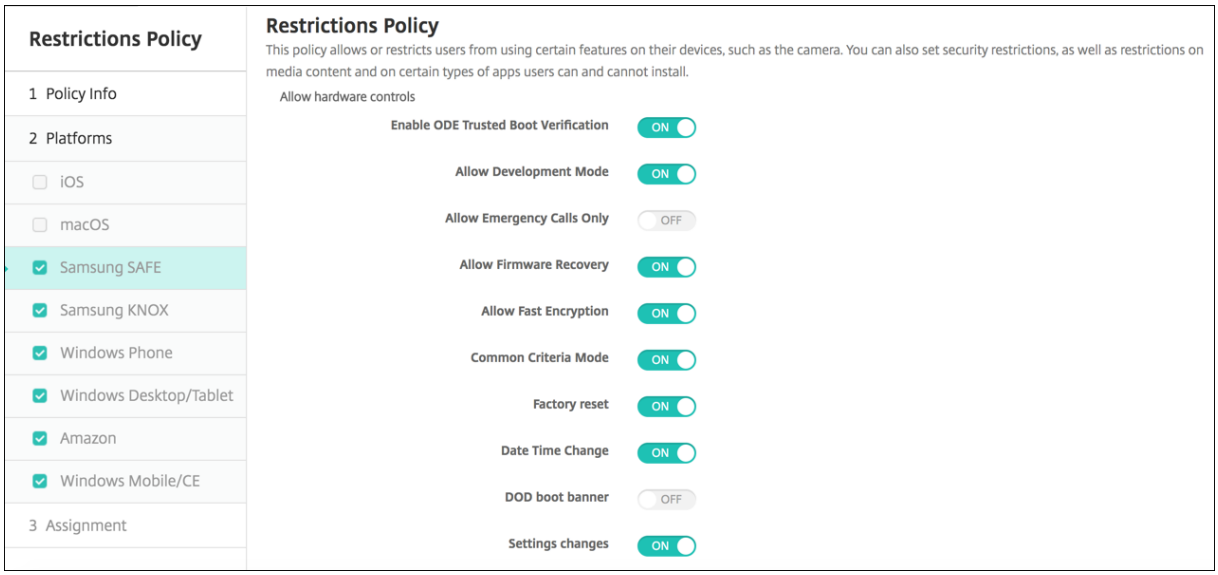
- **Samsung:** 완전관리형장치만
  - **ODE** 신뢰할수있는부팅확인사용**:** ODE 신뢰할수있는부팅확인을사용하여 bootloader 에서시스템이미지까지신뢰체인을설정합니다. 기본값은 켜짐입니다.
  - 긴급호출만허용**:** 사용자가장치에서긴급통화전용모드를사용할수있습니다. 기본값은 꺼짐입니다.
  - 펌웨어복구허용**:** 사용자가장치에서펌웨어를복구할수있습니다. 기본값은 켜짐입니다.
  - 빠른암호화허용**:** 사용된메모리공간의암호화만허용합니다. 이암호화는모든데이터를암호화하는전체디스크암호화와대조됩니다. 이데이터에는설정, 응용프로그램데이터, 다운로드한파일및응용프로그램, 미디어및기타파일이포함됩니다. 기본값은 켜짐입니다.
  - **Common Criteria** 모드사용**:** 장치를 Common Criteria 모드로전환합니다. Common Criteria 구성은엄격한보안프로세스를적용합니다. 기본값은 켜짐입니다.
  - 재부팅배너사용**:** 사용자의장치가다시시작되면 DoD 에서승인시스템사용알림메시지또는배너를표시합니다. 기본값은 꺼짐입니다.

- 설정변경허용**:** 사용자가완전관리형장치에서설정을변경할수있습니다. 기본값은 켜짐입니다.
- 백그라운드데이터사용활성화**:** 완전히관리되는장치의경우앱이백그라운드에서데이터를동기화할수있습니다. 기본값은 켜짐입니다.
- 클립보드허용**:** 사용자가장치의클립보드에데이터를복사할수있도록허용합니다. 기본값은 켜짐입니다.
  - 클립보드공유허용**:** 사용자가장치와컴퓨터간에서클립보드콘텐츠를공유할수있도록허용합니다 (MDM 4.0 이상).
- 홈키허용**:** 사용자가완전관리형장치에서 홈키를사용할수있습니다. 기본값은 켜짐입니다.
- 모의위치허용**:** 사용자가 GPS 위치를조작할수있습니다. 완전관리형장치에사용할수있습니다. 기본값은 꺼짐입니다.
- **NFC:** 사용자가완전관리형장치에서 NFC 를사용할수있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- 전원끄기허용**:** 사용자가완전관리형장치를끌수있습니다 (MDM 3.0 이상). 기본값은 켜짐입니다.
- **Wi-Fi Direct** 허용**:** 사용자가 Wi-Fi 연결을통해다른장치에직접연결할수있습니다. 기본값은 켜짐입니다. 켜짐인경우 **Wi-Fi** 변경허용설정을사용하도록설정해야합니다.
- **SD** 카드허용**:** 가능한경우사용자가장치에서 SD 카드를사용할수있습니다. 기본값은 켜짐입니다.
- **USB** 호스트스토리지허용**:** USB 장치가연결될때사용자의장치가 USB 호스트로작동할수있도록허용합니다. 그러면사용자의장치가 USB 장치에전원을공급합니다. 기본값은 켜짐입니다.
- 음성다이얼허용**:** 사용자가장치에서음성다이얼을사용할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **S Beam** 허용**:** 사용자가 NFC 및 Wi-Fi Direct 를사용하여다른사용자와콘텐츠를공유할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **S Voice** 허용**:** 사용자가장치에서지능형개인비서및지식탐색기를사용할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- **USB** 테더링허용**:** 사용자가 USB 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 테더링허용설정도 켜짐이어야합니다.
- **Bluetooth** 테더링허용**:** 사용자가 Bluetooth 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 테더링허용설정도 켜짐이어야합니다.
- **Wi-Fi** 테더링허용**:** 사용자가 Wi-Fi 연결을사용하여다른장치와모바일데이터연결을공유할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 테더링허용설정도 켜짐이어야합니다.
- 들어오는 **MMS** 허용**:** 사용자가 MMS 메시지를받을수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 나가는 **MMS** 허용**:** 사용자가 MMS 메시지를보낼수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 들어오는 **SMS** 허용**:** 사용자가 SMS 메시지를받을수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 나가는 **SMS** 허용**:** 사용자가 SMS 메시지를보낼수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 **SMS** 허용설정을켜야합니다.
- 모바일네트워크구성**:** 사용자가셀룰러데이터연결을사용할수있도록허용합니다. 기본값은 꺼짐입니다.
- 일별제한 **(MB):** 사용자가하루에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
- 주별제한 **(MB):** 사용자가한주에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성

화하는 0 입니다 (MDM 4.0 이상).
- 월별제한 **(MB):** 사용자가한달에사용할수있는모바일데이터의양 (MB) 을입력합니다. 기본값은이기능은비활성화하는 0 입니다 (MDM 4.0 이상).
- 보안 **VPN** 통신만허용**:** 사용자가보안연결만사용할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다.
- 오디오녹음허용**:** 사용자가장치에서오디오를녹음할수있습니다 (MDM 4.0 이상). 기본값은 켜짐입니다. 켜짐인경우 마이크허용설정을켜야합니다.
- 비디오녹화허용**:** 사용자가장치에서비디오를녹화할수있습니다 (MDM 4.0 이상). 기본값은 꺼짐입니다. 켜짐인경우 카메라사용허용설정을켜야합니다.
- 로밍시푸시메시지허용**:** 사용자가푸시에셀룰러데이터를사용할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 데이터로밍허용설정을사용하도록설정해야합니다.
- 로밍시자동동기화허용**:** 사용자가동기화에셀룰러데이터를사용할수있도록허용합니다. 기본값은 꺼짐입니다. 켜짐인경우 데이터로밍허용설정을사용하도록설정해야합니다.
- 로밍시음성통화허용**:** 사용자가음성통화에셀룰러데이터를사용할수있습니다. 기본값은 꺼짐입니다. 켜짐인경우 데이터로밍허용설정을사용하도록설정해야합니다.

- **Samsung: Knox** 컨테이너**/**완전관리형장치
  - 해지확인사용**:** 해지된인증서를확인할수있습니다. 기본값은 꺼짐입니다.
- **Samsung: Knox** 컨테이너만
  - 앱을컨테이너로이동**:** 사용자가 Knox 컨테이너와장치의개인영역간에서앱을이동할수있습니다. 기본값은 켜짐입니다.
  - 다단계인증적용**:** 사용자는지문과함께암호또는 PIN 과같은다른인증방법을사용하여장치를열어야합니다. 기본값은 켜짐입니다.
  - 컨테이너에대한인증적용**:** 장치의잠금을해제하는데사용되는방법과다른인증방법을사용하여 KNOX 컨테이너를여십시오. 기본값은 켜짐입니다.
  - 보안키패드사용**:** 사용자가 Knox 컨테이너내부의보안키보드를사용하도록강제합니다. 기본값은 켜짐입니다.

Samsung SAFE 설정



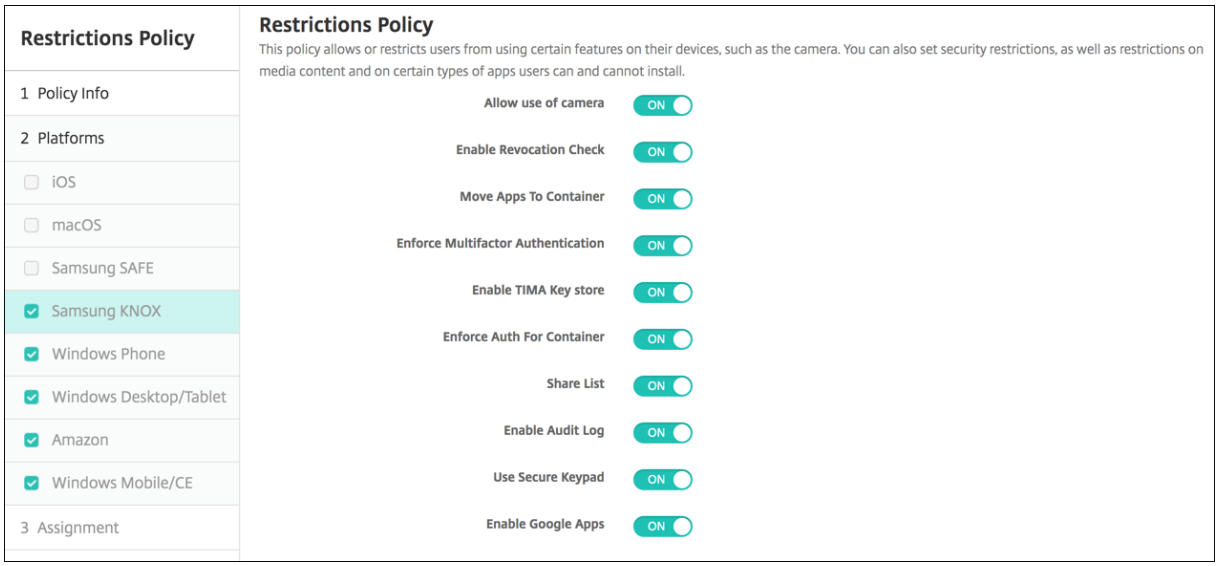
일부옵션은특정 Samsung 모바일기기관리 API 에서만사용할수있습니다. 이러한옵션에는관련버전정보가표시되어있습니다.

- 하드웨어제어허용
  - **ODE** 신뢰할수있는부팅확인사용**:** ODE 신뢰할수있는부팅확인을사용하여 bootloader 에서시스템이미지까지 신뢰체인을설정합니다.
  - 개발모드허용**:** 사용자가장치에서개발자설정을사용할수있도록허용합니다.
  - 긴급호출만허용**:** 사용자가장치에서긴급통화전용모드를사용할수있도록허용합니다.
  - 펌웨어복구허용**:** 사용자가장치에서펌웨어를복구할수있도록허용합니다.
  - 빠른암호화허용**:** 사용된메모리공간의암호화만허용합니다. 반대로, 전체디스크암호화는설정, 응용프로그램데이터, 다운로드한파일및응용프로그램, 미디어및기타파일을비롯한모든데이터를암호화합니다.
  - **Common Criteria** 모드**:** 장치를 Common Criteria 모드로만듭니다. Common Criteria 구성은엄격한 보안프로세스를적용합니다.
  - 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 위치를조작할수있도록용합니다.
  - **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, 비디오또는기타콘텐츠를다른장치로보낼수 있도록허용합니다 (MDM 4.0 이상).
  - 오디오녹음**:** 사용자가장치에서오디오를녹음할수있도록허용합니다 (MDM 4.0 이상).
  - 비디오녹음**:** 사용자가장치에서비디오를녹음할수있도록허용합니다 (MDM 4.0 이상).
  - 위치서비스**:** 사용자가장치에서 GPS 를켤수있도록허용합니다.
  - 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 도구를사용하여장치와컴퓨터간에서파일을동기화할수있도록 허용합니다.
  - 테더링**:** 사용자가 USB 연결을통해다른장치와모바일데이터연결을공유할수있도록허용합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

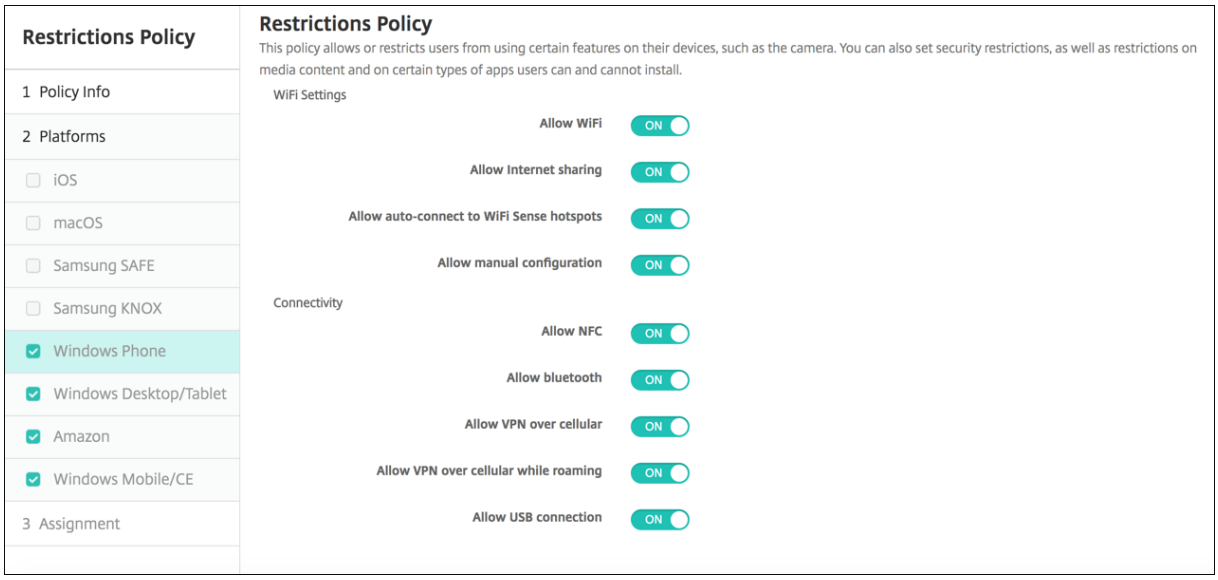
Samsung KNOX 설정



이러한옵션은 Samsung KNOX Premium(KNOX 2.0) 에서만사용할수있습니다.

- 카메라사용허용**:** 사용자가장치에서카메라를사용할수있도록허용합니다.
- 해지확인허용**:** 해지된인증서를확인하도록설정합니다.
- 앱을컨테이너로이동**:** 사용자가 KNOX 컨테이너와장치의개인영역간에서앱을이동할수있도록허용합니다.
- 다중단계인증적용**:** 사용자는지문과함께암호또는 PIN 과같은다른인증방법을사용하여장치를열어야합니다.
- **TIMA** 키저장소사용**:** TIMA 키저장소는대칭키에대한 TrustZone 기반의보안키저장소를제공합니다. RSA 키쌍및인증서는저장을위해기본키저장소공급자로라우팅됩니다.
- 컨테이너에대한인증적용**:** 장치의잠금을해제할때사용한 KNOX 컨테이너를열려면별도의다른인증을사용하십시오.
- 공유목록**:** 사용자가공유방법목록의앱간에서콘텐츠를공유할수있도록허용합니다.
- 감사로그사용**:** 장치의법의학분석을위한이벤트감사로그만들기를사용하도록설정합니다.
- 보안키패드사용**:** 사용자가 KNOX 컨테이너내부의보안키보드를사용하도록강제합니다.
- **Google** 앱사용**:** 사용자가 Google 모바일서비스에서 KNOX 컨테이너로앱을다운로드할수있도록허용합니다.
- 인증스마트카드브라우저**:** 스마트카드판독기가탑재된장치에서브라우저인증을사용하도록설정합니다.

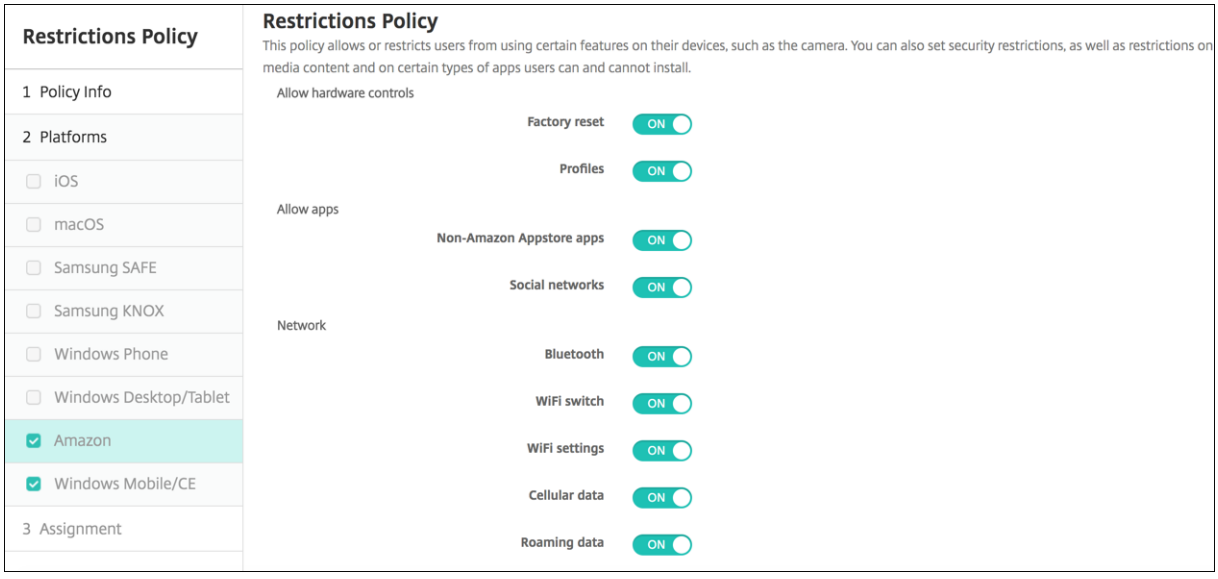
Windows 데스크톱/태블릿설정



- **WiFi** 설정
  - 인터넷공유허용**:** 장치가 WiFi 핫스폿으로전환되어다른장치와인터넷연결을공유할수있도록허용합니다.
  - **WiFi** 감지핫스폿에자동연결허용**:** 장치가 WiFi Sense 핫스폿에자동으로연결할수있도록허용합니다. 이옵션이작동하려면위치서비스를사용하도록설정해야합니다.
- 연결
  - 셀룰러를통한 **VPN** 허용**:** 장치가 VPN 을통해셀룰러네트워크에연결할수있도록허용합니다.
  - 로밍하는동안셀룰러를통한 **VPN** 허용**:** 장치가셀룰러네트워크를통해로밍할때장치가 VPN 을통해연결할수있도록허용합니다.
  - 셀룰러데이터로밍허용**:** 로밍하는동안사용자가셀룰러데이터를사용할수있도록허용합니다.
- 계정
  - **Microsoft** 계정연결허용**:** 장치가전자메일과관련이없는연결인증및서비스에대해 Microsoft 계정을사용할수있도록허용합니다.
  - **Microsoft** 이외의전자메일허용**:** 사용자가 Microsoft 이외의전자메일계정을추가할수있도록허용합니다.
- 시스템
  - 스토리지카드허용**:** 장치가스토리지카드를사용할수있도록허용합니다.
  - 원격분석**:** 목록에서옵션을클릭하여장치가원격분석정보를보내는것을허용하거나제한합니다. 기본값은 허용입니다. 다른옵션은 허용안함및 허용**,** 보조데이터요청제외입니다.
  - 위치서비스허용**:** 위치서비스를허용합니다.
  - 내부빌드에대한미리보기허용**:** 사용자가 Microsoft 내부빌드를미리볼수있도록허용합니다.
- 카메라**:**
  - 카메라사용허용**:** 사용자가장치의카메라를사용할수있도록허용합니다.
- **Bluetooth:**
  - 검색가능모드허용**:** Bluetooth 장치가로컬장치를찾을수있도록허용합니다.
  - 로컬장치이름**:** 로컬장치의이름입니다.

- 경험**:**
  - **Cortana** 허용**:** 사용자가지능형개인비서및지식탐색기인 Cortana 에액세스할수있도록허용합니다.
  - 장치검색허용**:** 네트워크를통한장치검색을허용합니다.
  - **MDM** 수동등록해제허용**:** 사용자가수동으로 XenMobile MDM 에서장치의등록을해제할수있도록허용합니다.
  - 장치설정동기화허용**:** 로밍중에사용자가 Windows 10 및 Windows 11 장치간에서설정을동기화할수있도록허용합니다.
- 위쪽잠금**:**
  - 알림허용**:** 잠금화면에알림메시지를허용합니다.
- 앱
  - 앱스토어자동업데이트허용**:** 앱스토어에서앱이자동으로업데이트되도록허용합니다.
- 개인정보**:**
  - 개인설정입력허용**:** 입력개인설정서비스가실행되어사용자의입력내용에따라펜및터치키보드등의예측입력을개선할수있도록허용합니다.
- 설정**:**
  - 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.

로밍장치정책

August 12, 2022

사용자의 iOS 장치에서음성및데이터로밍을허용할것인지여부를구성하는장치정책을 XenMobile 에서추가할수있습니다. 음성로밍을사용하지않도록설정하면데이터로밍이자동으로비활성화됩니다. iOS 의경우 iOS 5.0 이상의장치에서만이정책을사용할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 음성로밍사용안함**:** 음성로밍을사용하지않을것인지여부를선택합니다. 이옵션을사용하도록설정하면데이터로밍이자동으로비활성화됩니다. 기본값은 꺼짐, 즉음성로밍을사용하는것입니다.
- 데이터로밍사용안함**:** 데이터로밍을사용하지않을것인지여부를선택합니다. 이옵션은음성로밍이활성화된경우에만사용할수있습니다. 기본값은 꺼짐, 즉데이터로밍을사용하는것입니다.

Samsung MDM 라이센스키장치정책

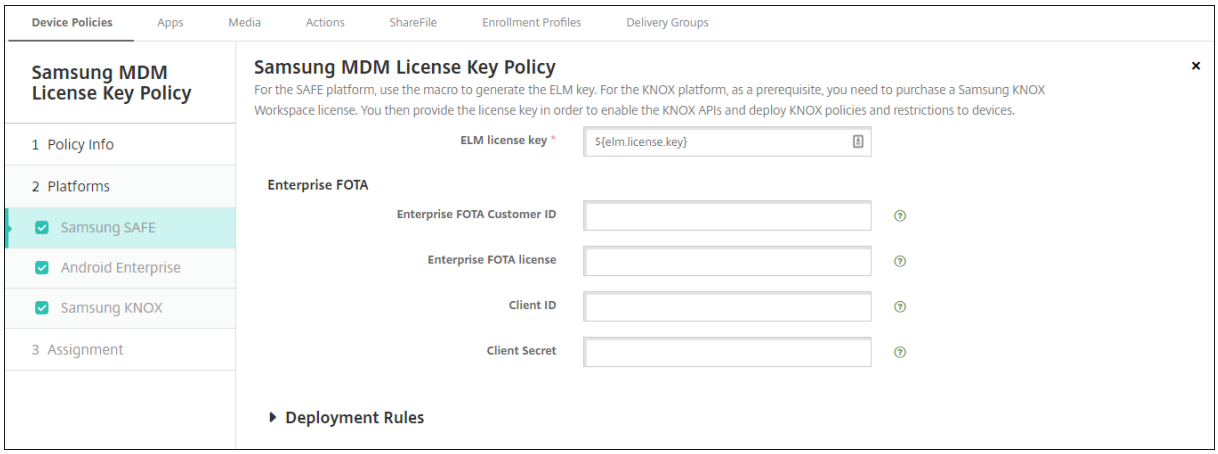
January 5, 2022

SAFE 정책및제한사항을배포하기전에장치에배포해야하는기본제공 Samsung ELM(엔터프라이즈라이센스관리) 키를지정

합니다. XenMobile 은 Samsung E-FOTA(Enterprise Firmware-Over-The-Air) 서비스도지원합니다. XenMobile 은 SAFE(Samsung for Enterprise) 와 Samsung KNOX 정책을모두지원하고확장합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Samsung SAFE 설정



- **ELM** 라이센스키**:** XenMobile 은 ELM 라이센스키를생성하는매크로로이필드를미리채웁니다. 필드가비어있는경우매크로 ${elm.license.key} 를입력합니다.

Samsung E-FOTA 설정구성

Samsung E-FOTA(Enterprise FOTA) 는장치의업데이트시기및사용할펌웨어버전을알려줍니다. E-FOTA 를사용하면업데이트를배포하기전에테스트하여업데이트가앱과호환되는지확인할수있습니다. 사용자개입없이제공되는최신펌웨어버전으로업데이트하도록장치를강제할수있습니다.

Samsung 은인증된펌웨어를실행하는 Samsung Knox 2.7.1 장치 (최소버전) 에대해 E-FOTA 를지원합니다.

XenMobile 은 XenMobile 콘솔에서 Knox E-FOTA One 에장치를추가하는작업을지원합니다. XenMobile 에서장치목록을내보내는방법에대한자세한내용은 장치테이블내보내기를참조하십시오. Knox E-FOTA One 에장치를추가하는방법에대한자세한내용은 Samsung 문서를참조하십시오.

XenMobile 은 MDM 솔루션에서 Knox E-FOTA 를지원하지않습니다.

E-FOTA 정책을구성하려면:

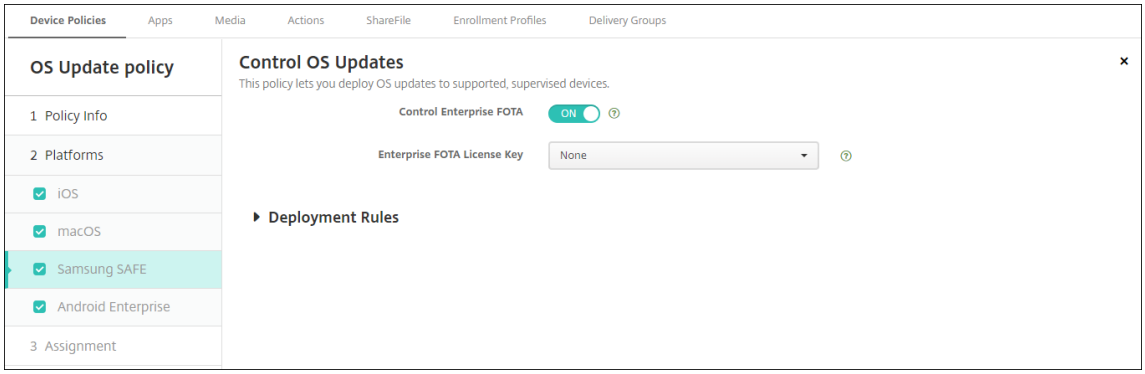
1. Samsung 에서받은키및라이센스정보를사용하여 Samsung MDM 라이센스키장치정책을만듭니다. 그러면 XenMobile Server 가정보의유효성을확인하고정보를등록합니다. XenMobile 에서 E-FOTA 문제를감지한경우문제를나타내는오류메시지가나타납니다. 문제를해결하기위해제공된코드를사용합니다. 자세한내용은 개발자안내서를참조하십시오.

   ELM 라이센스키를입력합니다. XenMobile 은 ELM 라이센스키를생성하는매크로로이필드를미리채웁니다. 필드가비어있는경우매크로 ${elm.license.key} 를입력합니다.

E-FOTA 패키지를구입할때 Samsung 에서제공한다음정보를입력합니다.

- **Enterprise FOTA** 고객 **ID**
- **Enterprise FOTA** 라이센스
- 클라이언트 **ID**
- 클라이언트암호

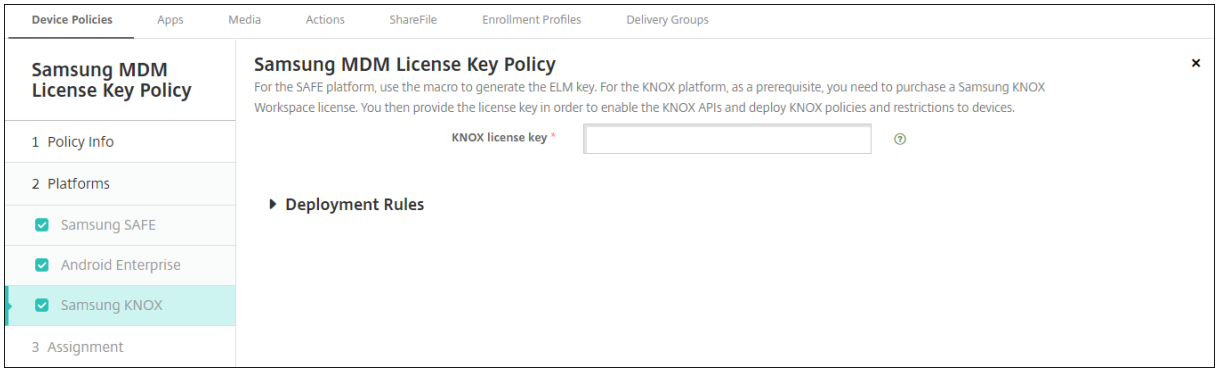
2. 필요한경우 OS 업데이트제어장치정책을만듭니다.



- **Enable Enterprise FOTA(Enterprise FOTA** 사용**):** 켜짐으로설정합니다.
- **Enterprise FOTA** 라이센스키**:** 1 단계에서만든 Samsung MDM 라이센스키정책이름을선택합니다.

3. OS 업데이트제어정책을 Secure Hub 에배포합니다.

Android Enterprise 및 **Samsung KNOX** 설정



- **KNOX** 라이센스키**:** Samsung 에서받은 KNOX 라이센스키를입력합니다.

Samsung SAFE 방화벽장치정책

January 5, 2022

이정책을사용하면 Samsung 장치에대한방화벽설정을구성할수있습니다. 허용하거나차단할 IP 주소, 포트및호스트이름을입력합니다. 프록시및프록시경로조정설정도구성할수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Samsung SAFE 설정

- 호스트허용/거부**:** 액세스를허용하거나거부할각호스트에대해 추가를클릭하고다음을구성합니다.
  - 호스트이름/**IP** 범위**:** 영향을줄사이트의호스트이름또는 IP 주소범위입니다.
  - 포트/포트범위**:** 포트또는포트범위입니다.
  - 허용/거부규칙필터**:** 화이트리스트를클릭하여사이트액세스를허용하거나 블랙리스트를클릭하여사이트액세스를거부합니다.

    > 참고**:**
    > XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는용어가포함됩니다. 향후릴리스에서 이러한용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.
- 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.

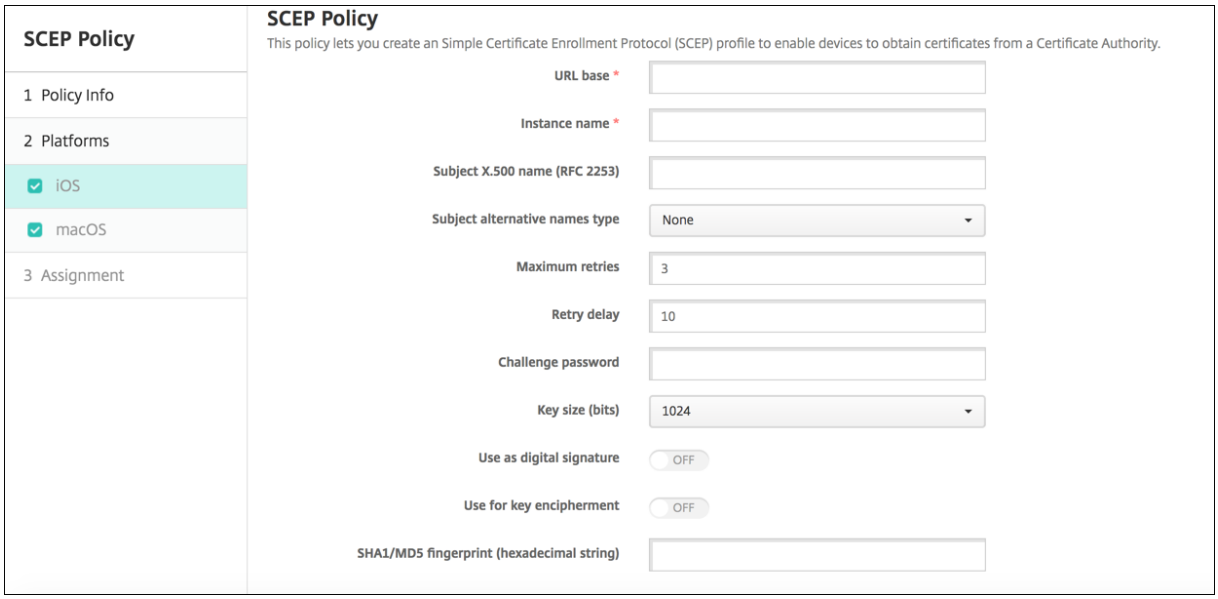
SCEP 장치정책

January 5, 2022

이정책을사용하면 SCEP(단순인증서등록프로토콜) 를사용하여외부 SCEP 서버에서인증서를검색하도록 iOS 및 macOS 장치를구성할수있습니다. XenMobile 에연결된 PKI 에서 SCEP 를사용하여장치에인증서를제공하려면분산모드에서 PKI 엔터티및 PKI 공급자를만들어야합니다. 자세한내용은 PKI 엔터티를참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

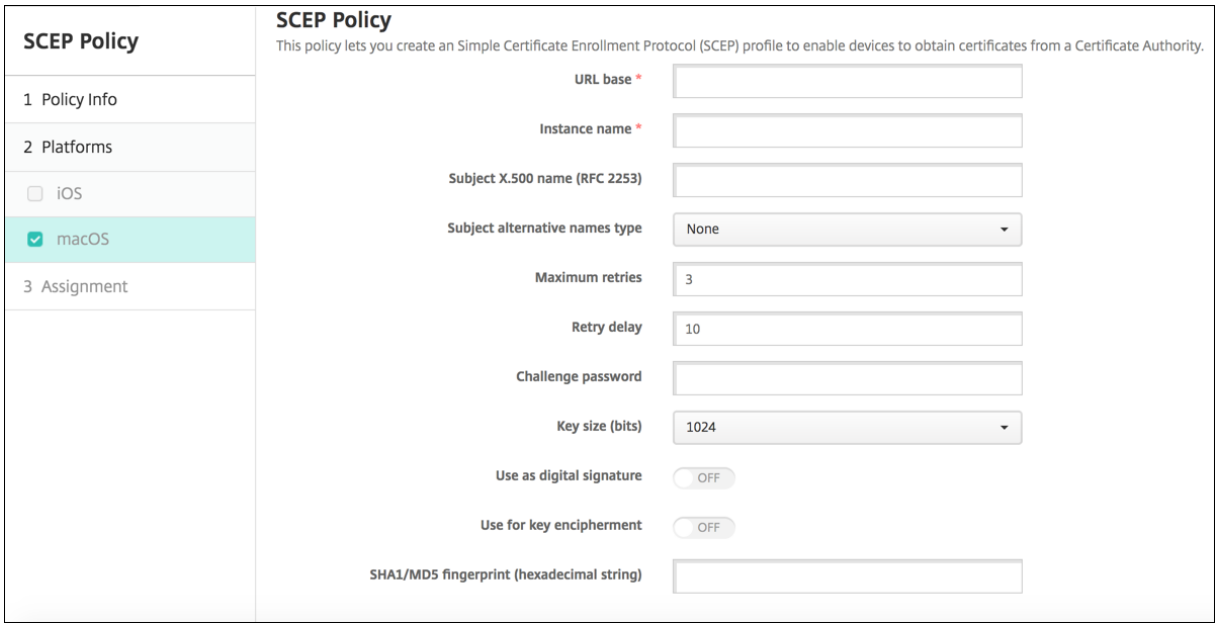
iOS 설정



- **URL** 기준**:** HTTP 또는 HTTPS 를통해 SCEP 요청을전송할 SCEP 서버주소를입력합니다. 개인키는 CSR(인증서명요청) 로전송되지않으므로요청을암호화되지않은상태로보내도안전할수있습니다. 그러나일회용암호를재사용하는것이허용되므로 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”]]] 로변환될수있습니다. 국가 (C), 지역 (L), 시/도 (ST), 조직 (O), 조직구성단위 (OU) 및일반이름 (CN) 에대한바로가기가포함된점형식숫자로 OID 를표현할수있습니다.
- 주체대체이름유형**:** 목록에서대체이름유형을클릭합니다. SCEP 정책은 CA 의인증서발급에필요한값을제공하는선택적대체이름유형을지정할수있습니다. 없음, **RFC 822** 이름, **DNS** 이름또는 **URI** 를지정할수있습니다.
- 최대재시도횟수**:** SCEP 서버가 PENDING 응답을보내는경우장치에서재시도할횟수를입력합니다. 기본값은 **3** 입니다.
- 재시도지연**:** 다음재시도전에대기할시간을초로입력합니다. 첫번째재시도는지연없이시도됩니다. 기본값은 **10** 입니다.
- 챌린지암호**:** 미리공유한암호를입력합니다.
- 키크기 **(**비트**): 2048** 이상을키크기 (비트단위) 로선택합니다.
- 디지털서명으로사용**:** 인증서를디지털서명으로사용할지여부를지정합니다. 인증서를사용하여디지털서명을확인하는경우, 예를들어 CA 에서발급된인증서인지여부를확인하는경우 SCEP 서버가공개키를사용하여해시를해독하기전에이방식으로인증서를사용할수있는지여부를확인합니다.
- 키암호화에사용**:** 인증서를키암호화에사용할지여부를지정합니다. 서버에서클라이언트가제공한인증서의공개키를사용하여데이터가개인키를사용하여암호화되었는지확인하는경우인증서를키암호화에사용할수있는지여부를먼저확인할수있습니다. 그렇지않은경우작업에실패합니다.

- **SHA1/MD5** 지문 **(16** 진수문자열**):** CA 에서 HTTP 를사용하는경우이필드를사용하여 CA 인증서지문을제공합니다. 이지문은등록시장치에서 CA 응답의진위를확인하는데사용됩니다. SHA1 또는 MD5 지문을입력하거나서명을가져올인증서를선택할수있습니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    * 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    * 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

macOS 설정



- **URL** 기준**:** HTTP 또는 HTTPS 를통해 SCEP 요청을전송할 SCEP 서버주소를입력합니다. 개인키는 CSR(인증서서명요청) 로전송되지않으므로요청을암호화되지않은상태로보내도안전할수있습니다. 그러나일회용암호를재사용하는것이허용되므로 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”]]] 로변환될수있습니다. 국가 (C), 지역 (L), 시/도 (ST), 조직 (O), 조직구성단위 (OU) 및일반이름 (CN) 에대한바로가기가포함된점형식숫자로 OID 를표현할수있습니다.
- 주체대체이름유형**:** 목록에서대체이름유형을클릭합니다. SCEP 정책은 CA 의인증서발급에필요한값을제공하는선택적대체이름유형을지정할수있습니다. 없음, **RFC 822** 이름, **DNS** 이름또는 **URI** 를지정할수있습니다.

- 최대재시도횟수**:** SCEP 서버가 PENDING 응답을보내는경우장치에서재시도할횟수를입력합니다. 기본값은 **3** 입니다.
- 재시도지연**:** 다음재시도전에대기할시간을초로입력합니다. 첫번째재시도는지연없이시도됩니다. 기본값은 **10** 입니다.
- 챌린지암호**:** 미리공유한암호를입력합니다.
- 키크기 **(**비트**): 2048** 이상을키크기 (비트단위) 로선택합니다.
- 디지털서명으로사용**:** 인증서를디지털서명으로사용할지여부를지정합니다. 인증서를사용하여디지털서명을확인하는경우, 예를들어 CA 에서발급된인증서인지여부를확인하는경우 SCEP 서버가공개키를사용하여해시를해독하기전에이방식으로인증서를사용할수있는지여부를확인합니다.
- 키암호화에사용**:** 인증서를키암호화에사용할지여부를지정합니다. 서버에서클라이언트가제공한인증서의공개키를사용하여데이터가개인키를사용하여암호화되었는지확인하는경우인증서를키암호화에사용할수있는지여부를먼저확인할수있습니다. 그렇지않은경우작업에실패합니다.
- **SHA1/MD5** 지문 **(16** 진수문자열**):** CA 에서 HTTP 를사용하는경우이필드를사용하여 CA 인증서지문을제공합니다. 이지문은등록시장치에서 CA 응답의진위를확인하는데사용됩니다. SHA1 또는 MD5 지문을입력하거나서명을가져올인증서를선택할수있습니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

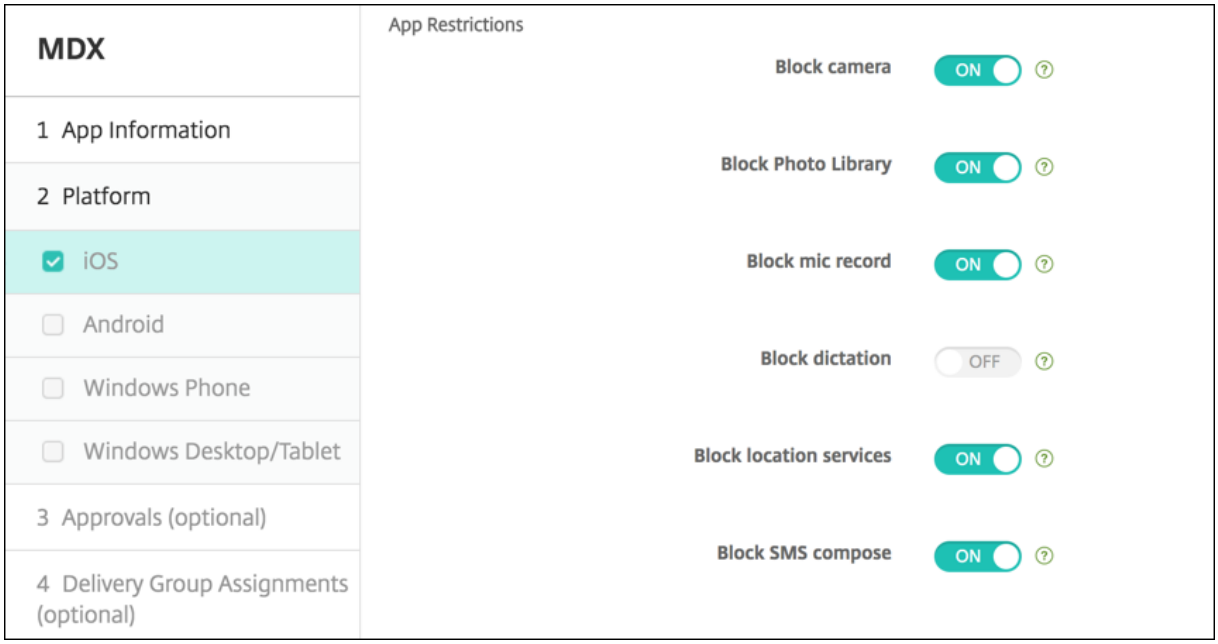
Siri 및받아쓰기정책

January 5, 2022

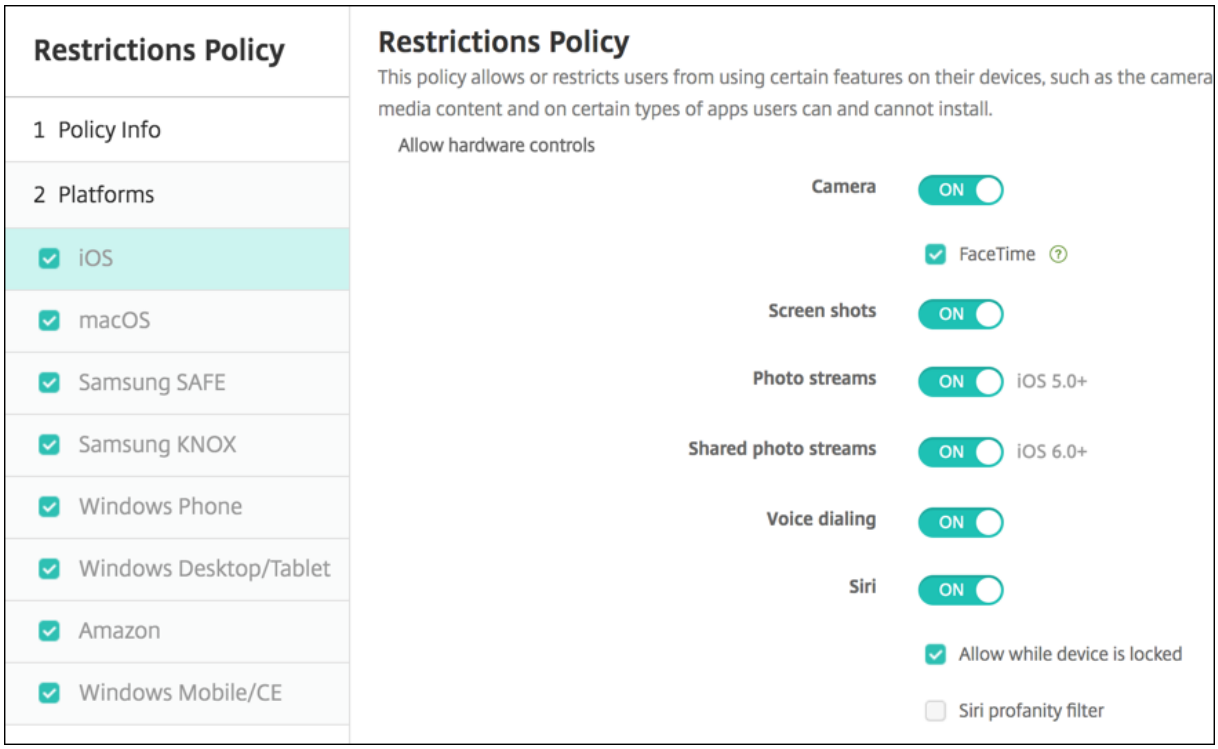
사용자가 Siri 에무언가를요청하거나관리되는 iOS 장치에서텍스트를받아쓰면 Apple 이 Siri 를개선하기위해음성데이터를수집합니다. 이음성데이터는 Apple 의클라우드기반서비스를통과하므로보안 XenMobile 컨테이너외부에있게됩니다. 그러나받아쓰기결과인텍스트는컨테이너내에서그대로유지됩니다.

보안요구에따라 XenMobile 에서 Siri 및받아쓰기서비스를차단할수있습니다.

MAM 배포에서각앱에대한 받아쓰기차단정책은기본적으로 켜짐입니다. 즉, 장치의마이크가사용되지않습니다. 받아쓰기를허용하려면이정책을 꺼짐으로설정합니다. 이정책은 XenMobile 콘솔의 구성 **>** 앱에서찾을수있습니다. 앱을선택하고 편집을클릭한 후 **iOS** 를클릭합니다.



또한 MDM 배포에서 구성 **>** 장치정책의 Siri 정책을통해 Siri 를사용하지않도록설정할수있습니다. Siri 사용은기본적으로허용됩니다.



Siri 와받아쓰기를허용할지여부를결정할때주의해야할몇가지사항은다음과같습니다.

- Apple 이공개한정보에따르면 Apple 은 Siri 및받아쓰기음성클립데이터를최대 2 년간유지합니다. 이데이터에는사용자를나타내는무작위값이할당되며이무작위번호에음성파일이연결되어있습니다. 자세한내용은 Wired 문서 Apple reveals how long Siri keeps your data(Apple, Siri 에사용자데이터를유지하는기간공개)를참조하십시오.

- iOS 장치에서 설정 **>** 일반 **>** 키보드로이동하고 받아쓰기활성화아래의링크를눌러 Apple 의개인정보보호정책을검토할 수있습니다.

SSO 계정장치정책

January 5, 2022

사용자가다양한앱에서 XenMobile 과회사내부리소스에액세스하기위해한번만로그온하도록 XenMobile 에서 SSO(Single Sign-On) 계정을만듭니다. 사용자가장치에자격증명을저장할필요가없습니다. App Store 의앱을포함하여앱전반에걸쳐 SSO 계정엔터프라이즈사용자자격증명이사용됩니다. 이정책은 Kerberos 인증백엔드와함께작동하도록설계되었습니다.

이정책은 iOS 7.0 이상에만적용됩니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

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 로그온에서장치에캐시되었을수있는 Kerberos 토큰을제공하며 SSO 를시도하지않습니다. 일치항목은 URL 의호스트부분에서정확히일치해야합니다. 예를들어 `https://shopping.apple.com`은유효하지만 `https://*.apple.com`은유효하지않습니다.
    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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.

* 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
* 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

스토리지암호화장치정책

August 12, 2022

XenMobile 에서스토리지암호화장치정책을만들어내부및외부스토리지를암호화하고장치에따라사용자로하여금장치에서스토리지카드를사용하지못하도록합니다.

Samsung SAFE 장치에대한정책을만들수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

사전요구사항

Samsung SAFE 장치의경우이정책을구성하기전에다음요구사항을충족해야합니다.

- 사용자의장치에서화면잠금옵션을설정합니다.
- 사용자의장치를연결하고 80% 이상충전합니다.
- 장치에서숫자및문자또는기호를모두포함하는암호를요구하는지확인합니다.

Samsung SAFE 설정구성

- 내부스토리지암호화**:** 사용자장치의내부스토리지를암호화할것인지를선택합니다. 내부스토리지에는장치메모리와내부스토리지가포함됩니다. 기본값은 켜짐입니다.
- 외부스토리지암호화**:** 사용자장치의외부스토리지를암호화할것인지를선택합니다. 기본값은 켜짐입니다.

스토어장치정책

January 5, 2022

iOS, Android 또는 Windows 태블릿장치의홈화면에 XenMobile Store 웹클립을표시할지여부를지정하는정책을 XenMobile 에서만들수있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

플랫폼설정

구성하는각플랫폼에대해 XenMobile Store 웹클립을사용자장치에표시할지여부를선택합니다. 기본값은 켜짐입니다.

구독캘린더장치정책

January 5, 2022

XenMobile 에장치정책을추가하여 iOS 장치에있는캘린더목록에구독캘린더를추가할수있습니다. 구독할수있는공개캘린더목록이 www.apple.com/downloads/macosx/calendars에나와있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

약관장치정책

August 12, 2022

사용자가회사네트워크에대한연결을통제하는회사의특정정책에동의하도록하려면 XenMobile 에서약관장치정책을만듭니다. 사용자가 XenMobile 에장치를등록할때약관이표시되며약관에동의해야만장치를등록할수있습니다. 약관에동의하지않으면등록프로세스가취소됩니다.

회사에다양한국가의사용자가있고사용자의모국어로약관에동의하게하려면약관에대한정책을여러언어로만들수있습니다. 배포하려는각플랫폼및언어조합에대한파일을제공해야합니다. Android 및 iOS 장치의경우 PDF 파일을제공해야합니다. Windows 장치의경우텍스트 (.txt) 파일및동반이미지파일을제공해야합니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 및 **Android** 설정

- 가져올파일**:** 찾아보기를클릭하고파일의위치로이동하여가져올약관파일을선택합니다.
- 기본약관**:** 이파일이서로다른약관을사용하는여러그룹의구성원인사용자의기본문서인지여부를선택합니다. 기본값은 꺼짐입니다.

Windows 태블릿설정

- 가져올파일**:** 찾아보기를클릭하고파일의위치로이동하여가져올약관파일을선택합니다.
- 이미지**:** 찾아보기를클릭하고파일위치로이동하여가져올이미지파일을선택합니다.
- 기본약관**:** 이파일이서로다른약관을사용하는여러그룹의구성원인사용자의기본문서인지여부를선택합니다. 기본값은 꺼짐입니다.

VPN 장치정책

August 12, 2022

VPN 장치정책은사용자장치에서회사리소스에안전하게연결할수있게하는 VPN(가상사설망) 설정을구성합니다. 다음플랫폼에대한 VPN 장치정책을구성할수있습니다. 플랫폼마다서로다른값이필요합니다. 이에대해서는이문서에자세히설명되어있습니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

앱별 **VPN** 에대한요구사항

VPN 정책을통해다음플랫폼에대해앱별 VPN 기능을구성합니다.

- iOS
- macOS
- Android(레거시 DA)
- Samsung SAFE
- Samsung Knox

Android Enterprise 장치에대한 VPN 을구성하려면 Citrix SSO 앱에대한관리되는구성장치정책을만듭니다. Android Enterprise 에대한 VPN 프로필구성을참조하십시오.

특정연결유형에대해앱별 VPN 옵션을사용할수있습니다. 다음표는앱별 VPN 옵션이제공되는경우를보여줍니다.

플랫폼	**Connection type(**연결유형**)**	비고
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO 또는사용자 지정 SSL.	
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA 또는 사용자지정 SSL.	
Android(레거시 DA)	Citrix SSO	
Samsung SAFE	IPSEC, SSL	VPN 유형이 일반으로설정됨
Samsung Knox	IPSEC, SSL	VPN 유형이 일반으로설정됨

Citrix SSO 앱을사용하여 iOS 및 Android(레거시 DA) 장치에대한앱별 VPN 을만들려면 VPN 정책구성외에추가단계를수행해야합니다. 또한다음사전요구사항도충족하는지확인해야합니다.

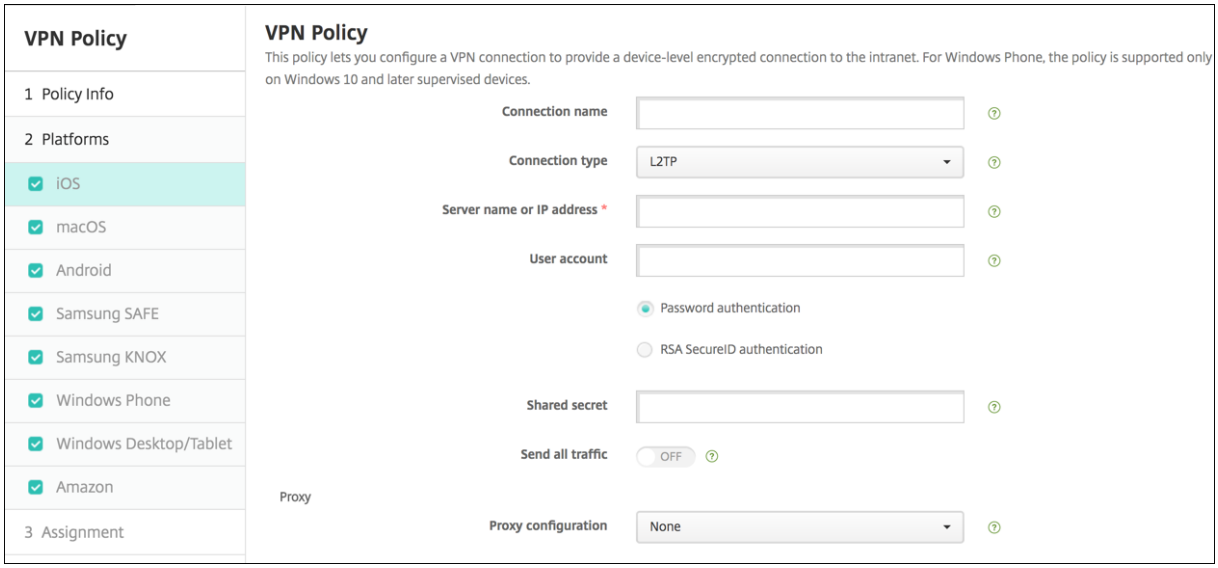
- 온프레미스 Citrix Gateway
- 다음응용프로그램이장치에설치됩니다.
  - Citrix SSO
  - Citrix Secure Hub

Citrix SSO 앱을사용하여 iOS 및 Android 장치에대한앱별 VPN 을구성하는일반적인워크플로는다음과같습니다.

1. 이문서에설명된대로 VPN 장치정책을구성합니다.
   - *iOS* 의경우 iOS 용 Citrix SSO 프로토콜구성을참조하십시오. VPN 장치정책을통해 iOS 용 Citrix SSO 프로토콜을구성한후에는앱을앱별 VPN 정책에연결하는앱특성정책도만들어야합니다. 자세한내용은 앱별 VPN 구성을참조하십시오.
     - 연결을위한인증유형필드에대해 인증서를선택할경우인증서기반 Endpoint Management 인증을먼저구성해야합니다. 클라이언트인증서인증또는인증서와도메인인증을참조하십시오.
   - *Android(*레거시 *DA)* 에대해서는 Android 용 Citrix SSO 프로토콜구성을참조하십시오.
     - 연결을위한인증유형필드에대해 인증서또는 암호및인증서를선택할경우인증서기반 Endpoint Management 인증을먼저구성해야합니다. 클라이언트인증서인증또는인증서와도메인인증을참조하십시오.
2. 앱별 VPN 에서트래픽을허용하도록 Citrix ADC 를구성합니다. 자세한내용은 Citrix Gateway 에서전체 VPN 설정을 참조하십시오.

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:
>   - **Connection type** = **Citrix SSO**
>   - **Enable per-app VPN** = **On**
>   - **Provider type** = **Packet tunnel**
> 3. iOS 에대한앱특성장치정책을추가합니다. 앱별 **VPN** 식별자의경우 **iOS_VPN** 을선택합니다.



- 연결이름**:** 연결이름을입력합니다.
- 연결유형**:** 목록에서이연결에사용할프로토콜을선택합니다. 기본값은 **L2TP** 입니다.
  - **L2TP:** 미리공유한키인증을사용하는계층 2 터널링프로토콜입니다.
  - **PPTP:** 지점간터널링입니다.
  - **IPSec:** 회사 VPN 연결입니다.
  - **Cisco Legacy AnyConnect:** 이연결유형을사용하려면 Cisco Legacy AnyConnect VPN 클라이언트가사용자장치에설치되어있어야합니다. 이제는사용되지않는 VPN 프레임워크에기반하는 Cisco Legacy AnyConnect 클라이언트는단계적으로중단됩니다. 자세한내용은지원문서 https://support.citrix.com/article/CTX227708에서참조하십시오.
    현재 Cisco AnyConnect 클라이언트를사용하려면 연결유형에서 사용자지정 **SSL** 을선택합니다. 필요한설정은이섹션에서 “사용자지정 SSL 프로토콜구성” 을참조하십시오.
  - **Juniper SSL:** Juniper Networks SSL VPN 클라이언트입니다.
  - **F5 SSL:** F5 Networks SSL VPN 클라이언트입니다.
  - **SonicWALL Mobile Connect:** iOS 용 Dell 통합 VPN 클라이언트입니다.
  - **Ariba VIA:** Ariba Networks Virtual Internet Access 클라이언트입니다.

  - **IKEv2(iOS** 에만해당**):** iOS 전용 Internet Key Exchange 버전 2 입니다.
  - **AlwaysOn IKEv2:** IKEv2 를사용하여상시액세스를제공합니다.
  - **AlwaysOn IKEv2** 이중구성**:** IKEv2 이중구성을사용하여상시액세스를제공합니다.
  - **Citrix SSO:** iOS 12 이상을위한 Citrix SSO 클라이언트입니다.
  - 사용자지정 **SSL:** 사용자지정 Secure Socket Layer 입니다. 이연결유형은번들 ID 가 **com.cisco.anyconnect** 인 Cisco AnyConnect 클라이언트에필요합니다. 연결이름을 **Cisco AnyConnect** 로지정합니다. VPN 정책을배포하고 iOS 장치에대해 NAC(네트워크액세스제어) 필터를사용하도록설정할수도있습니다. 이필터는호환되지않는앱이설치된장치에대한 VPN 연결을차단합니다. 이구성에는다음 iOS 섹션에설명된대로 iOS VPN 정책에대한특정설정이필요합니다. NAC 필터를사용하는데필요한기타설정에대한자세한내용은 네트워크액세스제어를참조하십시오.

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 켜짐인경우설정구성에대한자세한내용은 iOS 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 켜짐인경우설정구성에대한자세한내용은 iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용**:** 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을사용하는경우다음설정을구성합니다.
  - 주문형일치앱사용**:** 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다. 기본값은 꺼짐입니다.
  - 공급자유형**:** 앱별 VPN 을 앱프록시로제공할지, 아니면 패킷터널로제공할지를선택합니다. 기본값은 앱프록시입니다.
  - **Safari** 도메인**:** 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수

행합니다.

* 도메인**:** 추가할도메인을입력합니다.
* 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

iOS 용 **Juniper SSL** 프로토콜구성

- 공급자번들식별자**:** 앱별 VPN 프로필에앱의번들식별자와동일한유형의여러 VPN 공급자가포함되는경우여기서사용할공급자를지정합니다.
- 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. 기본값은꺼짐입니다.
    * 주문형 **VPN** 사용**:** 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은 iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용**:** 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을사용하는경우다음설정을구성합니다.
  - 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 **F5 SSL** 프로토콜구성

- 공급자번들식별자**:** 앱별 VPN 프로필에앱의번들식별자와동일한유형의여러 VPN 공급자가포함되는경우여기서사용할공급자를지정합니다.
- 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 켜짐인경우설정구성에대한자세한내용은 iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용**:** 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을사용하는경우다음설정을구성합니다.
  - 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

- 공급자번들식별자**:** 앱별 VPN 프로필에앱의번들식별자와동일한유형의여러 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 켜짐인경우설정구성에대한자세한내용은 iOS 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.

  - **Safari** 도메인**:** 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
    * 도메인**:** 추가할도메인을입력합니다.
    * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

iOS 용 **Ariba VIA** 프로토콜구성

- 공급자번들식별자**:** 앱별 VPN 프로필에앱의번들식별자와동일한유형의여러 VPN 공급자가포함되는경우여기서사용할공급자를지정합니다.
- 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 켜짐인경우설정구성에대한자세한내용은 iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용**:** 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을사용하는경우다음설정을구성합니다.
  - 주문형일치앱사용**:** 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다.
  - **Safari** 도메인**:** 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
    * 도메인**:** 추가할도메인을입력합니다.
    * 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

iOS 용 **IKEv2** 프로토콜구성

이섹션에는 IKEv2, AlwaysOn IKEv2 및 AlwaysOn IKEv2 이중구성프로토콜에사용되는설정이포함되어있습니다. AlwaysOn IKEv2 이중구성프로토콜의경우셀룰러및 Wi-Fi 네트워크에대해이러한모든설정을구성합니다.

- 사용자가자동연결을비활성화하도록허용**:** AlwaysOn 프로토콜용입니다. 사용자가자신의장치에서네트워크자동연결을끌수있게허용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 서버의호스트이름또는 **IP** 주소**:** VPN 서버의서버이름또는 IP 주소를입력합니다.
- 로컬식별자**:** IKEv2 클라이언트의 FQDN 또는 IP 주소입니다. 이것은필수필드입니다.
- 원격식별자**:** VPN 서버의 FQDN 또는 IP 주소입니다. 이것은필수필드입니다.

- 장치인증**:** 이연결에대한인증유형으로 공유암호, 인증서또는 장치 **ID** 에기반한장치인증서를선택합니다. 기본값은 공유암호입니다.
  - 공유암호를선택하는경우선택적공유암호키를입력합니다.
  - 인증서를선택하는경우사용할 **ID** 자격증명을선택합니다. 기본값은 없음입니다.
  - 장치 **ID** 에기반한장치인증서를선택할경우사용할 장치 **ID** 유형을선택합니다. 기본값은 **IMEI** 입니다. 이옵션을사용하려면 REST API 를사용하여인증서를일괄적으로가져옵니다. REST API 로 iOS 장치에인증서일괄업로드를 참조하십시오. **IKEv2** 항상켜짐을선택한경우에만사용할수있습니다.
- 확장인증사용**:** EAP(확장인증프로토콜) 를사용할지여부를선택합니다. 켜짐을선택하는경우 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. 보조일치도메인목록을확인자의검색도메인목록에추가할지여부를결정합니다. 기본값은 켜짐입니다.
- 보조일치도메인**:** 선택사항입니다. DNS 서버주소에포함된 DNS 확인자설정을사용할 DNS 쿼리를결정하는데사용되는 도메인문자열목록입니다. 이키는특정도메인의호스트만터널의 DNS 확인자를사용하여확인되는분할 DNS 구성을생성합니다. 이목록의도메인중하나에포함되지않은호스트는시스템의기본확인자를사용하여확인됩니다.

이매개변수에빈문자열이포함된경우해당문자열이기본도메인입니다. 분할터널구성은이방법으로먼저모든 DNS 쿼리를직접 VPN DNS 서버로전달한후기본 DNS 서버로전달할수있습니다. VPN 터널이네트워크의기본경로인경우나열된 DNS 서버가기본확인자가됩니다. 이경우보조일치도메인목록이무시됩니다.

- **IKE SA** 매개변수및하위 **SA** 매개변수. 각 SA(보안연결) 매개변수옵션에대해다음설정을구성합니다.
  - 암호화알고리즘**:** 목록에서사용할 IKE 암호화알고리즘을선택합니다. 기본값은 **3DES** 입니다.
  - 무결성알고리즘**:** 목록에서사용할무결성알고리즘을선택합니다. 기본값은 **SHA1-96** 입니다.
  - **Diffie Hellman** 그룹**:** 목록에서 Diffie Hellman 그룹번호를선택합니다. 기본값은 **2** 입니다.
  - **IKE** 수명 **(**분**):** SA 수명 (키다시지정간격) 을나타내는 10 에서 1440 사이의정수를입력합니다. 기본값은 **1440** 분입니다.
- 서비스예외**:** AlwaysOn 프로토콜용입니다. 서비스예외는 AlwaysOn VPN 에서제외되는시스템서비스입니다. 다음서비스예외설정을구성합니다.
  - 음성사서함**:** 목록에서음성사서함예외의처리방법을선택합니다. 기본값은 트래픽이터널을통해전달되도록허용입니다.
  - **AirPrint:** 목록에서 AirPrint 예외의처리방법을선택합니다. 기본값은 트래픽이터널을통해전달되도록허용입니다.
  - 종속웹시트의트래픽이 **VPN** 터널외부로전달되도록허용**:** 사용자가 VPN 터널외부의공용핫스폿에연결할수있게허용할지여부를선택합니다. 기본값은 꺼짐입니다.
  - 모든종속네트워킹앱의트래픽이 **VPN** 터널외부로전달되도록허용**:** VPN 터널외부에있는모든핫스폿네트워킹앱을허용할지여부를선택합니다. 기본값은 꺼짐입니다.
  - 종속네트워킹앱번들식별자**:** 사용자액세스가허용되는각핫스폿네트워킹앱번들식별자에대해 추가를클릭하고핫스폿네트워킹앱 번들식별자를입력합니다. 저장을클릭하여앱번들식별자를저장합니다.
- 앱별 **VPN**. IKEv2 연결유형에대한설정을구성합니다.
  - 앱별 **VPN** 사용**:** 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다.
  - 주문형일치앱사용**:** 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다. 기본값은 꺼짐입니다.
  - **Safari** 도메인**:** 추가를클릭하여 Safari 도메인이름을추가합니다.
- 프록시구성**:** 프록시서버를통해 VPN 연결을라우팅하는방법을선택합니다. 기본값은 없음입니다.

iOS 용 **Citrix SSO** 프로토콜구성

Citrix SSO 클라이언트는 Apple Store(https://apps.apple.com/us/app/citrix-sso/id1333396910) 에서제공됩니다.

- 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 켜짐인경우설정구성에대한자세한내용은 iOS 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/id1135064690에서 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**:** 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
    - 연결할때 **PIN** 확인**:** 사용자가네트워크에연결할때 PIN 확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
    - 주문형 **VPN** 사용**:** 사용자가네트워크에연결할때 VPN 연결트리거를사용할지여부를선택합니다. 기본값은 꺼짐입니다. 주문형 **VPN** 사용이 켜짐인경우설정구성에대한자세한내용은 iOS 용주문형 VPN 사용설정구성을참조하십시오.
- 앱별 **VPN** 사용**:** 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을켜짐으로설정하는경우다음설정을구성합니다.
  - 주문형일치앱사용**:** 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다.
  - 공급자유형**:** 공급자가 VPN 서비스인지프록시서비스인지를나타내는공급자유형입니다. VPN 서비스의경우 패킷터널을선택합니다. 프록시서비스의경우 앱프록시를선택합니다. Cisco AnyConnect 클라이언트의경우 패킷터널을선택합니다.
  - **Safari** 도메인**:** 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
    - 도메인**:** 추가할도메인을입력합니다.
    - 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.
- 사용자지정 **XML:** 추가할각사용자지정 XML 매개변수에대해 추가를클릭하고다음을수행합니다.
  - 매개변수이름**:** 추가할매개변수의이름을입력합니다.
  - 값**:** 매개변수이름에연결된값을입력합니다.
  - 저장을클릭하여매개변수를저장하거나 취소를클릭하여매개변수를저장하지않습니다.

NAC 를지원하도록 **VPN** 장치정책구성

1. NAC 필터를구성하려면 연결유형이 사용자지정 **SSL** 이어야합니다.
2. **VPN** 의 연결이름을지정합니다.
3. 사용자지정 **SSL** 식별자에는 **com.citrix.NetScalerGateway.ios.app** 를입력합니다.
4. 공급자번들식별자에는 **com.citrix.NetScalerGateway.ios.app.vpnplugin** 을입력합니다.

3 단계와 4 단계의값은 NAC 필터링에필요한 Citrix SSO 설치에서가져옵니다. 인증암호는구성하지않습니다. NAC 기능사용에대한자세한내용은 네트워크액세스제어를참조하십시오.

iOS 용주문형 **VPN** 사용옵션구성

- 주문형도메인**:** 각도메인과사용자가연결할때수행할관련작업에대해 추가를클릭하고다음을수행합니다.

- 도메인**:** 추가할도메인을입력합니다.
- 동작**:** 목록에서가능한동작중하나를선택합니다.
  - 항상설정**:** 도메인에서항상 VPN 연결이트리거됩니다.
  - 설정안함**:** 도메인에서 VPN 연결이트리거되지않습니다.
  - 필요한경우설정**:** 도메인이름확인에실패하는경우도메인이 VPN 연결시도를트리거합니다. 실패는 DNS 서버에서도메인을확인할수없거나다른서버로리디렉션되거나시간초과되는경우발생합니다.
  - 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.
- 주문형규칙
  - 동작**:** 목록에서수행할동작을선택합니다. 기본값은 **EvaluateConnection** 입니다. 가능한동작은다음과같습니다.
    - 허용**:** 트리거시주문형 VPN 연결을허용합니다.
    - 연결**:** VPN 연결을무조건시작합니다.
    - 연결끊기**:** VPN 연결을제거하고규칙이일치하지않는한주문형 VPN 에다시연결하지않습니다.
    - **EvaluateConnection:** 각연결에대한 ActionParameters 배열을평가합니다.
    - 무시**:** 기존 VPN 연결을유지하지만규칙이일치하지않는한주문형 VPN 에다시연결하지않습니다.
  - **DNSDomainMatch:** 장치의검색도메인목록과일치할수있는추가할각도메인에대해 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:** 목록에서사용하는기본네트워크인터페이스하드웨어유형을선택합니다. 기본값은 지정되지않음입니다. 가능한값은다음과같습니다.
    - 지정되지않음**:** 모든네트워크인터페이스하드웨어와일치합니다. 이옵션은기본값입니다.
    - 이더넷**:** 이더넷네트워크인터페이스하드웨어만일치합니다.
    - **WiFi:** Wi-Fi 네트워크인터페이스하드웨어만일치합니다.
    - 셀룰러**:** 셀룰러네트워크인터페이스하드웨어만일치합니다.
  - **SSIDMatch:** 현재네트워크와일치할추가할각 SSID 에대해 추가를클릭하고다음을수행합니다.
    - **SSID:** 추가할 SSID 를입력합니다. 네트워크가 Wi-Fi 네트워크가아닌경우또는 SSID 가표시되지않는경우일치가실패합니다. 모든 SSID 와일치하려면이목록을비워둡니다.
    - 저장을클릭하여 SSID 를저장하거나 취소를클릭하여 SSID 를저장하지않습니다.
  - **URLStringProbe:** 가져올 URL 을입력합니다. 이 URL 을리디렉션없이성공적으로가져온경우이규칙이일치합니다.
  - **ActionParameters : Domains:** EvaluateConnection 이검사하는추가할각도메인에대해 추가를클릭

하고다음을수행합니다.

* 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** 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** 콘텐츠텍스트상자아래에 올바른 XML 이녹색텍스트로표시됩니다. 올바르지않은경우오류를설명하는오류메시지가주황색텍스트로표시됩니다.

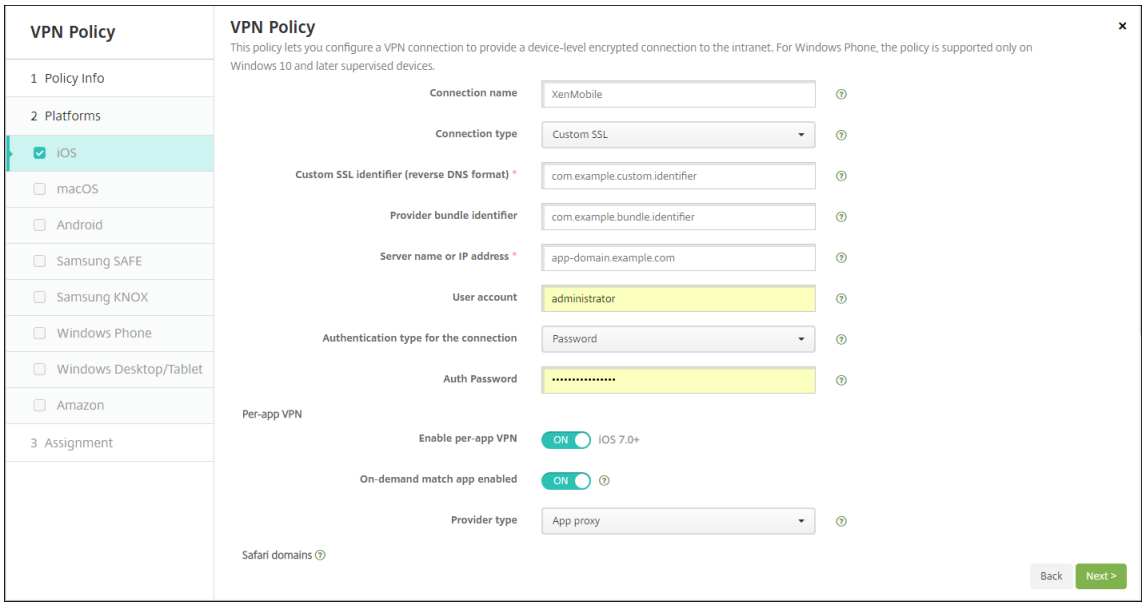
- 프록시
  – 프록시구성**:** 목록에서프록시서버를통해 VPN 연결을라우팅하는방법을선택합니다. 기본값은 없음입니다.
    * 수동을사용하는경우다음설정을구성합니다.
      · 프록시서버의호스트이름또는 **IP** 주소**:** 프록시서버의호스트이름또는 IP 주소를입력합니다. 이것은필수필드입니다.
      · 프록시서버용포트**:** 프록시서버포트번호를입력합니다. 이것은필수필드입니다.
      · 사용자이름**:** 선택적프록시서버사용자이름을입력합니다.
      · 암호**:** 선택적프록시서버암호를입력합니다.
    * 자동을구성하는경우다음설정을구성합니다.
      · 프록시서버 **URL:** 프록시서버의 URL 을입력합니다. 이것은필수필드입니다.
- 정책설정
  – 정책설정의 정책제거옆에서 날짜선택또는 제거할때까지의기간 **(**시간**)** 을선택합니다.
  – 날짜선택을선택하는경우달력을클릭하여제거할특정날짜를선택합니다.
  – 사용자가정책을제거하도록허용목록에서 항상, 암호필요또는 안함을선택합니다.
  – 암호필요를선택하는경우 제거암호옆에필요한암호를입력합니다.

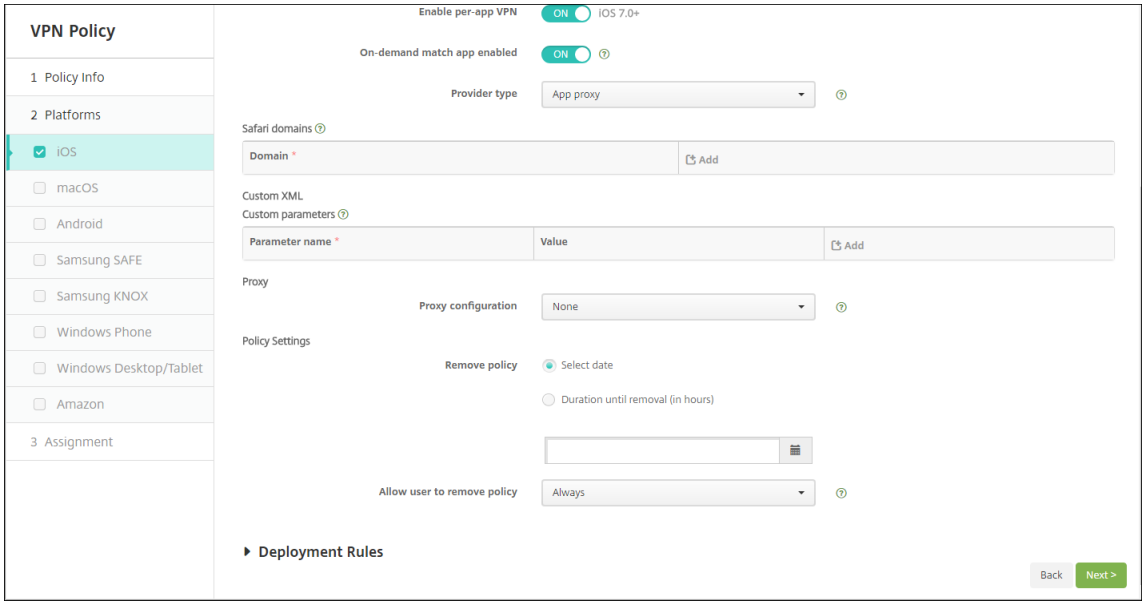
앱별 **VPN** 구성

iOS 에대한앱별 VPN 옵션은 Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO 및사용자지정 SSL 연결유형에사용할수있습니다.

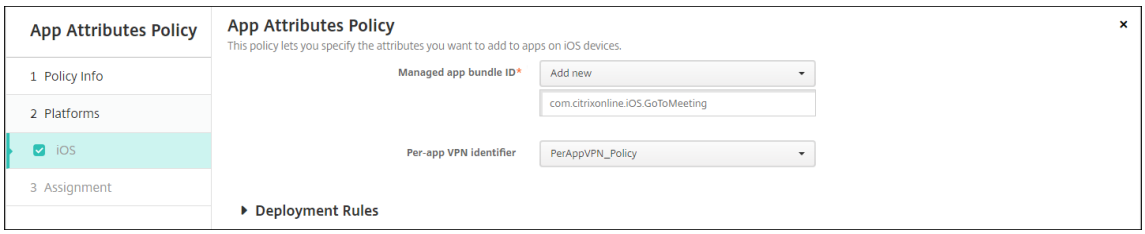
앱별 VPN 을구성하려면:

1. 구성 **>** 장치정책에서 VPN 정책을생성합니다. 예:



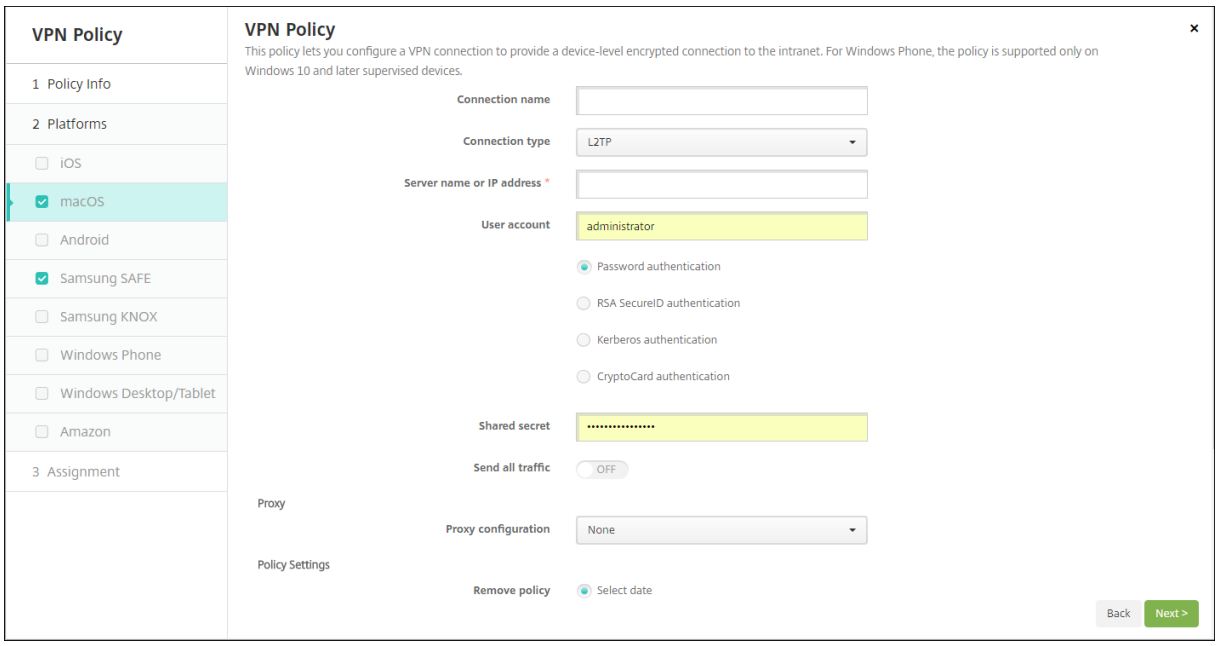


2. 구성 **>** 장치정책에서앱을앱별 VPN 정책에연결하는앱특성정책을생성합니다. 앱별 **VPN** 식별자에대해 1 단계에서생성한 VPN 정책의이름을선택합니다. 관리되는앱번들 **ID** 에대해앱목록에서선택하거나앱번들 ID 를입력합니다. (iOS 앱인벤토리정책을배포하는경우앱목록에앱이포함됩니다.)



- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

macOS 설정



- 연결이름**:** 연결이름을입력합니다.
- 연결유형**:** 목록에서이연결에사용할프로토콜을선택합니다. 기본값은 L2TP 입니다.
  - **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.

다음섹션에는이전에설명한각연결유형에대한구성옵션이나열되어있습니다.

macOS 용 **L2TP** 프로토콜구성

- 서버이름또는 **IP** 주소**:** VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정**:** 선택적사용자계정을입력합니다.
- 암호인증, **RSA SecurID** 인증, **Kerberos** 인증또는 **CryptoCard** 인증을선택합니다. 기본값은 암호인증입니다.
- 공유암호**:** IPsec 공유암호키를입력합니다.
- 모든트래픽보내기**:** VPN 을통해모든트래픽을보낼지여부를선택합니다. 기본값은 꺼짐입니다.

macOS 용 **PPTP** 프로토콜구성

- 서버이름또는 **IP** 주소**:** VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정**:** 선택적사용자계정을입력합니다.
- 암호인증, **RSA SecurID** 인증, **Kerberos** 인증또는 **CryptoCard** 인증을선택합니다. 기본값은 암호인증입니다.
- 암호화수준**:** 원하는암호화수준을선택합니다. 기본값은 없음입니다.
  - 없음**:** 암호화를사용하지않습니다.
  - 자동**:** 서버에서지원하는가장강력한암호화수준을사용합니다.
  - 최대 (128 비트): 항상 128 비트암호화를사용합니다.
- 모든트래픽보내기**:** VPN 을통해모든트래픽을보낼지여부를선택합니다. 기본값은 꺼짐입니다.

macOS 용 **IPsec** 프로토콜구성

- 서버이름또는 **IP** 주소**:** VPN 서버의서버이름또는 IP 주소를입력합니다.
- 사용자계정**:** 선택적사용자계정을입력합니다.
- 연결에대한인증유형**:** 목록에서이연결에대한인증유형으로 공유암호또는 인증서를선택합니다. 기본값은 공유암호입니다.
  - 공유암호인증을사용하는경우다음설정을구성합니다.
    - 그룹이름**:** 선택적그룹이름을입력합니다.
    - 공유암호**:** 선택적공유암호키를입력합니다.
    - 하이브리드인증사용**:** 하이브리드인증을사용할지여부를선택합니다. 하이브리드인증을사용하면서버가먼저클라이언트에서자체인증된후클라이언트가서버에서자체인증됩니다. 기본값은 꺼짐입니다.
    - 암호확인**:** 사용자가네트워크에연결할때암호확인메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다.
  - 인증서인증을사용하는경우다음설정을구성합니다.
    - **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 켜짐인경우설정구성에대한자세한내용은주문형 VPN 사용옵션구성을참조하십시오.

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 켜짐인경우설정구성에대한자세한내용은주문형 VPN 사용옵션구성을참조하십시오.
  - 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 사용설정구성을참조하십시오.
- 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 **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 사용설정구성을참조하십시오.
- 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 **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 사용설정구성을참조하십시오.
- 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 **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 사용설정구성을참조하십시오.
- 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 용사용자지정 **SSL** 프로토콜구성

- 사용자지정 **SSL** 식별자 **(**역방향 **DNS** 형식**):** SSL 식별자를역방향 DNS 형식으로입력합니다. 이것은필수필드입니다.
- 서버이름또는 **IP** 주소**:** VPN 서버의서버이름또는 IP 주소를입력합니다. 이것은필수필드입니다.
- 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 사용설정구성을참조하십시오.
  - 앱별 **VPN:** 앱별 VPN 을사용할지여부를선택합니다. 기본값은 꺼짐입니다. 이옵션을사용하는경우다음설정을구성합니다.
    - 주문형일치앱사용**:** 앱별 VPN 서비스에연결된앱이네트워크통신을시작할때앱별 VPN 연결을자동으로트리거할지여부를선택합니다.
    - **Safari** 도메인**:** 포함하려는앱별 VPN 연결을트리거할수있는각 Safari 도메인에대해 추가를클릭하고다음을수행합니다.
      - 도메인**:** 추가할도메인을입력합니다.
      - 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.
- 사용자지정 **XML:** 추가할각사용자지정 XML 매개변수에대해 추가를클릭하고다음을수행합니다.
  - 매개변수이름**:** 추가할매개변수의이름을입력합니다.
  - 값**:** 매개변수이름에연결된값을입력합니다.
  - 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.

주문형 **VPN** 사용옵션구성

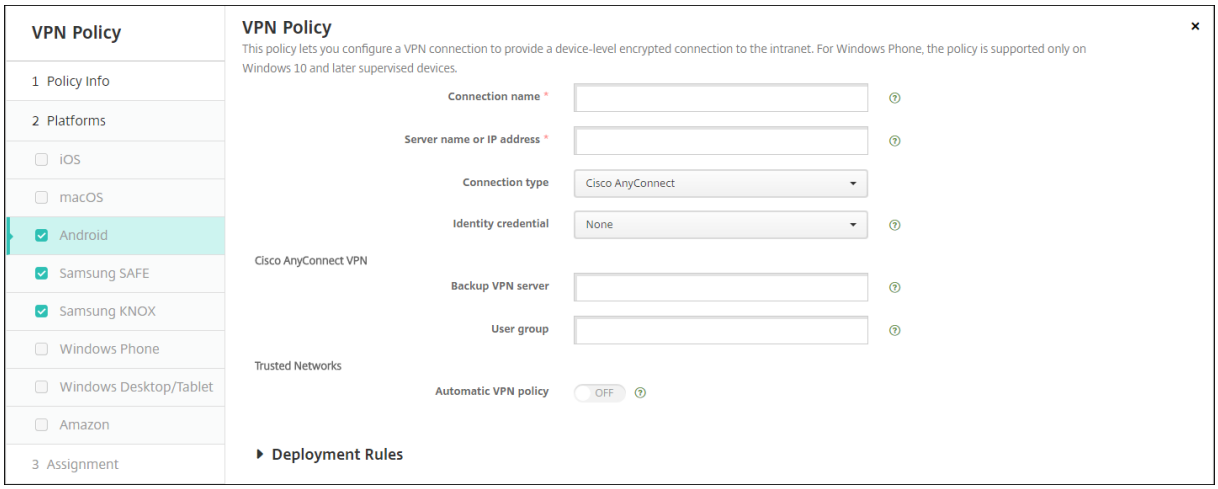
- 주문형도메인**:** 추가할각도메인및사용자가도메인에연결할때수행할동작에대해 추가를클릭하고다음을수행합니다.
  - 도메인**:** 추가할도메인을입력합니다.
  - 동작**:** 목록에서가능한동작중하나를선택합니다.
    - 항상설정**:** 도메인에서항상 VPN 연결이트리거됩니다.
    - 설정안함**:** 도메인에서 VPN 연결이트리거되지않습니다.
    - 필요한경우설정**:** 도메인이름확인에실패하는경우도메인이 VPN 연결시도를트리거합니다. 실패는 DNS 서버에서도메인을확인할수없거나다른서버로리디렉션되거나시간초과되는경우발생합니다.
  - 저장을클릭하여도메인을저장하거나 취소를클릭하여도메인을저장하지않습니다.
- 주문형규칙
  - 동작**:** 목록에서수행할동작을선택합니다. 기본값은 **EvaluateConnection** 입니다. 가능한동작은다음과같습니다.

    * 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. 이옵션은기본값입니다.
    * 이더넷**:** 이더넷네트워크인터페이스하드웨어만일치합니다.
    * **WiFi:** Wi-Fi 네트워크인터페이스하드웨어만일치합니다.
    * 셀룰러**:** 셀룰러네트워크인터페이스하드웨어만일치합니다.
- **SSIDMatch:** 현재네트워크와일치할추가할각 SSID 에대해 추가를클릭하고다음을수행합니다.
    * **SSID:** 추가할 SSID 를입력합니다. 네트워크가 Wi-Fi 네트워크가아닌경우또는 SSID 가표시되지않는경우일치가실패합니다. 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** 도메인에대한 **VPN** 동작을선택합니다. 기본값은 **ConnectIfNeeded** 입니다. 가능한동작은다음과같습니다.
    * **ConnectIfNeeded:** 도메인이름확인에실패하는경우도메인이 VPN 연결시도를트리거합니다. 실패는 DNS 서버에서도메인을확인할수없거나다른서버로리디렉션되거나시간초과되는경우발생합니다.
    * **NeverConnect:** 도메인에서 VPN 연결이트리거되지않습니다.
- **ActionParameters : RequiredDNSServers:** 지정된도메인을확인할때사용할각 DNS 서버 IP 주소에대해 추가를클릭하고다음을수행합니다.

        * **DNS** 서버**: ActionParameters** : **DomainAction** = **ConnectIfNeeded** 인경우에만유효합니다. 추가할 DNS 서버를입력합니다. 이서버는장치의현재네트워크구성에포함된서버가아니어도됩니다. DNS 서버에연결할수없는경우 VPN 연결이대신설정됩니다. 이 DNS 서버는내부 DNS 서버또는신뢰할수있는외부 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.

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**:** 이옵션을사용하거나사용하지않도록설정하여 VPN 이신뢰할수있는네트워크및신뢰할수없는네트워크에반응하는방법을설정합니다. 사용하는경우다음설정을구성합니다.
    - 신뢰할수있는네트워크정책**:** 목록에서원하는정책을선택합니다. 기본값은 연결끊기입니다. 사용가능한옵션은다음과같습니다.
      - 연결끊기**:** 클라이언트가신뢰할수있는네트워크에서 VPN 연결을종료합니다. 이설정은기본값입니다.
      - 연결**:** 클라이언트가신뢰할수있는네트워크에서 VPN 연결을시작합니다.
      - 아무작업도하지않음**:** 클라이언트가아무런동작을수행하지않습니다.
      - 일시중지**:** 사용자가신뢰할수있는네트워크외부에서 VPN 세션을설정한후신뢰할수있는네트워크로구성된네트워크로들어가면 VPN 세션이일시중지됩니다. 사용자가신뢰할수있는네트워크에서다시나가면세션이다시시작됩니다. 이설정을사용하면신뢰할수있는네트워크에서나간후새 VPN 세션을설정할필요가없습니다.
    - 신뢰할수없는네트워크정책**:** 목록에서원하는정책을선택합니다. 기본값은 연결입니다. 사용가능한옵션은다음과같습니다.
      - 연결**:** 클라이언트가신뢰할수없는네트워크에서 VPN 연결을시작합니다.
      - 아무작업도하지않음**:** 클라이언트가신뢰할수없는네트워크에서 VPN 연결을시작합니다. 이옵션을사용하면항상 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.
  - 사용자이름및 암호**:** 암호또는 암호및인증서의 인증유형에대한 VPN 자격증명을입력합니다. 선택사항입니다.

VPN 자격증명을입력하지않으면 Citrix VPN 앱에사용자이름과암호를입력하라는메시지가표시됩니다.

- **ID** 자격증명**:** 인증유형이 인증서또는 암호및인증서인경우표시됩니다. 목록에서 ID 자격증명을선택합니다.

- 앱별 **VPN** 사용**:** 앱별 VPN 을사용할지여부를선택합니다. 앱별 VPN 을사용하지않는경우모든트래픽이 Citrix VPN 터널을통과합니다. 앱별 VPN 을사용하는경우다음설정을지정합니다. 기본값은 꺼짐입니다.
  - 화이트리스트또는 블랙리스트**:** 화이트리스트인경우허용된모든앱이이 VPN 터널을통과합니다. 블랙리스트인경우차단목록의앱을제외한모든앱이이 VPN 터널을통과합니다.

    > 참고**:**
    >
    > XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는용어가포함됩니다. 향후릴리스에서 이러한용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.

  - 응용프로그램목록**:** 허용되거나차단된앱을지정합니다. 추가를클릭한다음앱패키지이름의쉼표로구분된목록을입력합니다.

- 사용자지정 **XML:** 추가를클릭한다음사용자지정매개변수를입력합니다. XenMobile 은 Citrix VPN 에대해다음매개변수를지원합니다.
  - **DisableUserProfiles:** 선택사항입니다. 이매개변수를사용하려면 값에 예를입력합니다. 사용하도록설정한경우 XenMobile 은사용자가추가한 VPN 연결을표시하지않으며사용자가연결을추가할수없습니다. 이설정은글로벌제한이며모든 VPN 프로필에적용됩니다.
  - **userAgent:** 문자열값입니다. 각 HTTP 요청에보낼사용자지정사용자에이전트문자열을지정할수있습니다. 지정한사용자에이전트문자열이기존 Citrix VPN 사용자에이전트에추가됩니다.

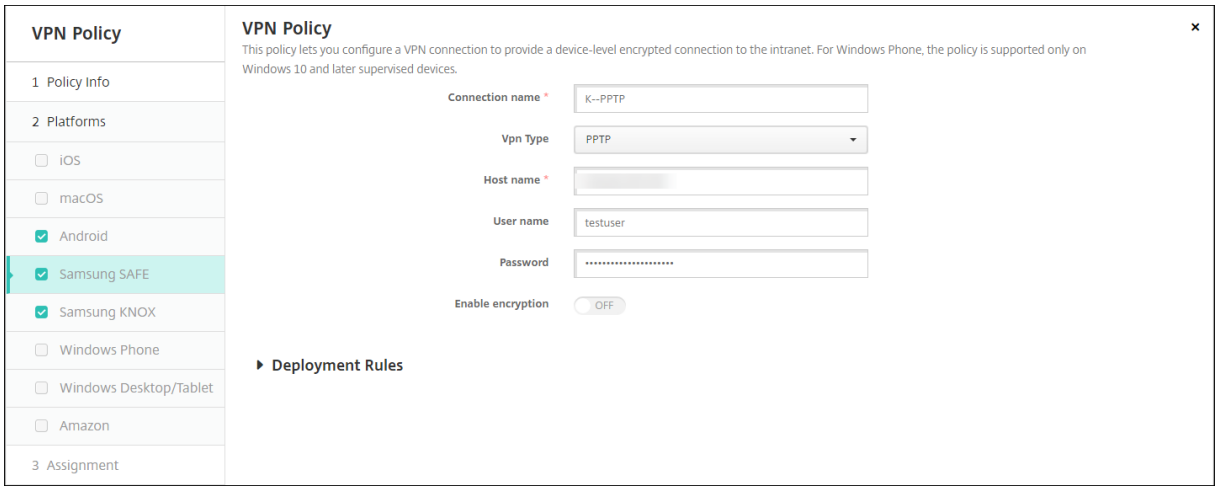
NAC 를지원하도록 **VPN** 구성

1. 연결유형을 사용자지정 **SSL** 로사용하여 NAC 필터를구성합니다.
2. **VPN** 의 연결이름을지정합니다.
3. 사용자지정 **XML** 에서 추가를클릭하고다음을수행합니다.
   - 매개변수이름**: XenMobileDeviceId** 를입력합니다. 이필드는 XenMobile 의장치등록을기준으로 NAC 확인에사용할장치 ID 입니다. XenMobile 에서장치를등록하고관리하는경우 VPN 연결이허용됩니다. 그렇지않으면 VPN 설정시인증이거부됩니다.
   - 값**: XenMobileDeviceId** 매개변수의값인 **DeviceID_${device.id}** 를입력합니다.
   - 저장을클릭하여매개변수를저장합니다.

Android Enterprise 에대한 **VPN** 구성

Android Enterprise 장치에대한 VPN 을구성하려면 Citrix SSO 앱에대한관리되는구성장치정책을만듭니다. Android Enterprise 에대한 VPN 프로필구성을참조하십시오.

Samsung SAFE 설정



- 연결이름**:** 연결이름을입력합니다.
- **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 인증을상호인증에사용합니다.
- **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.
  - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.

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:** 이구성에대한선택적식별자를입력합니다.
- **IPsec** 그룹 **ID** 유형**:** 목록에서사용할 IPsec 그룹 ID 유형을선택합니다. 기본값은 기본값입니다. 사용가능한옵션은다음과같습니다.
  - 기본값
  - **IPv4** 주소
  - **FQDN(**정규화된도메인이름**)**
  - 사용자 **FQDN**
  - **IKE** 키 **ID**
- **IKE** 버전**:** 목록에서사용할 Internet Key Exchange 버전을선택합니다. 기본값은 **IKEv1** 입니다.
- 인증방법**:** 목록에서사용할인증방법을선택합니다. 기본값은 인증서입니다. 사용가능한옵션은다음과같습니다.
  - 인증서**:** 인증서인증을사용합니다. 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 인증을상호인증에사용합니다.
  - **CAC** 기반인증**:** CAC(Common Access Card) 를인증에사용합니다.
- **ID** 자격증명**:** 목록에서사용할 ID 자격증명을선택합니다. 기본값은 없음입니다.
- **CA** 인증서**:** 목록에서사용할인증서를선택합니다.
- 데드피어감지사용**:** 피어에접속하여활성상태를확인할지여부를선택합니다. 기본값은 꺼짐입니다.
- 기본경로사용**:** VPN 서버에대한기본경로를사용할지여부를선택합니다.
- 모바일옵션사용**:** 모바일옵션을사용할지여부를선택합니다.
- **IKE** 수명 **(**분**):** VPN 연결을다시설정하기전까지의시간 (분) 을입력합니다. 기본값은 1440 분 (24 시간) 입니다.
- **ipsec** 수명 **(**분**):** VPN 연결을다시설정하기전까지의시간 (분) 을입력합니다. 기본값은 1440 분 (24 시간) 입니다.
- **Diffie-Hellman** 그룹값 **(**키강도**):** 목록에서사용할키강도를선택합니다. 기본값은 **0** 입니다.
- **IKE** 단계 **1** 키교환모드**:** IKE 단계 1 교환모드에대해 기본또는 적극적을선택합니다. 기본값은 기본입니다.
  - 기본**:** 협상중에잠재적공격자에게정보가노출되지않지만 적극적모드보다느립니다.
  - 적극적**:** 협상중에일부정보 (예: 협상중인피어의 ID) 가잠재적공격자에게노출되지만 기본모드보다빠릅니다.
- **PFS(Perfect Forward Secrecy)** 값**:** 연결을재협상할때새 PFS 를사용하여새키교환을요구할지여부를선택합니

다.

- 분할터널유형**:** 목록에서사용할분할터널유형을선택합니다. 사용가능한옵션은다음과같습니다.
  - 자동**:** 분할터널링이자동으로사용됩니다.
  - 수동**:** VPN 서버에지정된 IP 주소및포트를통해분할터널링이사용됩니다.
  - 사용안함**:** 분할터널링이사용되지않습니다.
- **IPSEC** 암호화알고리즘**:** IPsec 프로토콜이사용하는 VPN 구성입니다.
- **IKE** 암호화알고리즘**:** IPsec 프로토콜이사용하는 VPN 구성입니다.
- **IKE** 무결성알고리즘**:** IPsec 프로토콜이사용하는 VPN 구성입니다.
- 공급업체**:** Knox API 와통신하는일반에이전트의개인프로필입니다.
- 전달경로**:** 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
  - 전달경로**:** 전달경로의 IP 주소를입력합니다.
  - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.
- 앱별 **VPN:** 추가할각앱별 VPN 에대해 추가를클릭하고다음을수행합니다.
  - 앱별 **VPN:** 앱이통신에사용하는 VPN 구성입니다.
  - 저장을클릭하여앱별 VPN 을저장하거나 취소를클릭하여앱별 VPN 을저장하지않습니다.

Samsung SAFE 용 **SSL** 연결유형설정구성

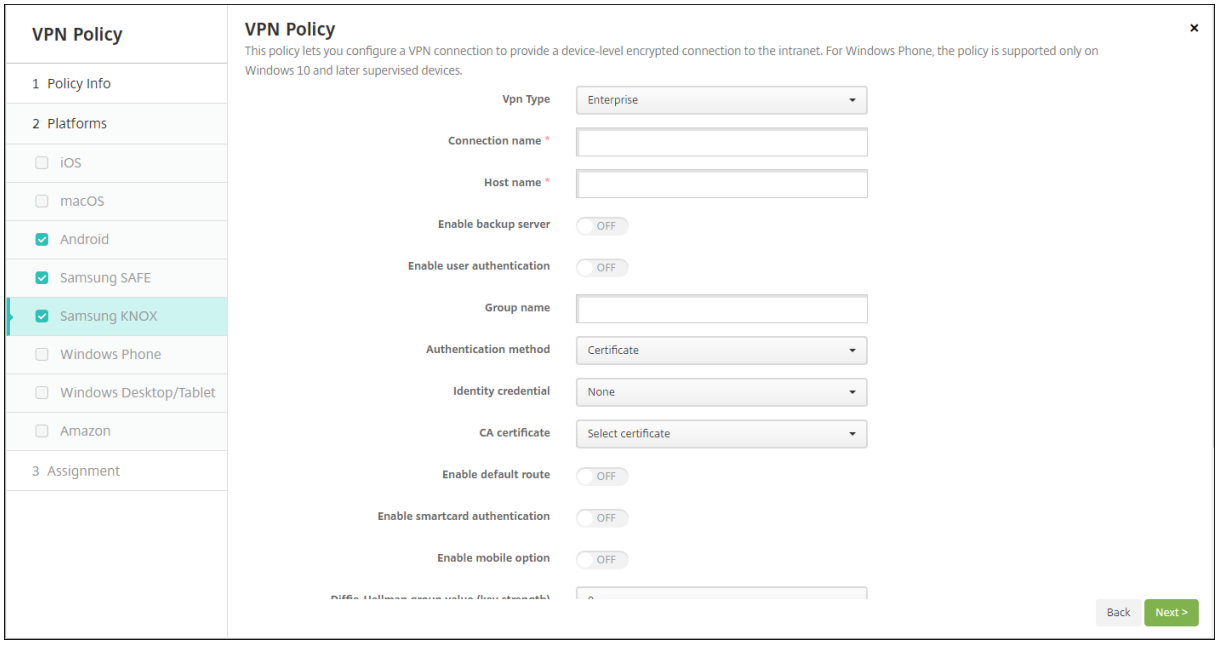
- 인증방법**:** 목록에서사용할인증방법을선택합니다. 기본값은 해당없음입니다. 사용가능한옵션은다음과같습니다.
  - 해당없음
  - 인증서**:** 인증서인증을사용합니다. 선택한경우 **ID** 자격증명목록에서사용할자격증명을선택합니다. 기본값은 없음입니다.
  - **CAC** 기반인증**:** CAC(Common Access Card) 를인증에사용합니다.
- **CA** 인증서**:** 목록에서사용할인증서를선택합니다.
- 기본경로사용**:** VPN 서버에대한기본경로를사용할지여부를선택합니다.
- 모바일옵션사용**:** 모바일옵션을사용할지여부를선택합니다.
- 분할터널유형**:** 목록에서사용할분할터널유형을선택합니다. 사용가능한옵션은다음과같습니다.
  - 자동**:** 분할터널링이자동으로사용됩니다.
  - 수동**:** VPN 서버에지정된 IP 주소및포트를통해분할터널링이사용됩니다.
  - 사용안함**:** 분할터널링이사용되지않습니다.
- **SSL** 알고리즘**:** 클라이언트-서버협상에사용할 SSL 알고리즘을입력합니다.
- 공급업체**:** Knox API 와통신하는일반에이전트의개인프로필입니다.
- 전달경로**:** 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
  - 전달경로**:** 전달경로의 IP 주소를입력합니다.
  - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.
- 앱별 **VPN:** 추가할각앱별 VPN 에대해 추가를클릭하고다음을수행합니다.
  - 앱별 **VPN:** 앱이통신에사용하는 VPN 구성입니다.
  - 저장을클릭하여앱별 VPN 을저장하거나 취소를클릭하여앱별 VPN 을저장하지않습니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시

간) 입니다.

  * 날짜선택: 달력을클릭하여제거할특정날짜를선택합니다.
  * 제거할때까지의기간 (시간): 정책제거가발생할때까지시간을숫자로입력합니다.

- 사용자가정책을제거하도록허용: 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
- 프로필범위: 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

Samsung Knox 설정



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 인증서를사용한하이브리드인증을사용합니다.
  - **EAP MD5:** EAP 피어를 EAP 서버로인증하지만상호인증은수행하지않습니다.
  - **EAP MSCHAPv2:** Microsoft 의 Challenge Handshake 인증을상호인증에사용합니다.
- **CA** 인증서**:** 목록에서사용할인증서를선택합니다.
- 기본경로사용**:** VPN 서버에대한기본경로를사용할지여부를선택합니다.
- 스마트카드인증사용**:** 스마트카드를사용한사용자인증을허용할지여부를선택합니다. 기본값은 꺼짐입니다.
- 모바일옵션사용**:** 모바일옵션을사용할지여부를선택합니다.
- **Diffie-Hellman** 그룹값 **(**키강도**):** 목록에서사용할키강도를선택합니다. 기본값은 **0** 입니다.
- 분할터널유형**:** 목록에서사용할분할터널유형을선택합니다. 사용가능한옵션은다음과같습니다.
  - 자동**:** 분할터널링이자동으로사용됩니다.
  - 수동**:** VPN 서버에지정된 IP 주소및포트를통해분할터널링이사용됩니다.
  - 사용안함**:** 분할터널링이사용되지않습니다.
- **SuiteB** 유형**:** 목록에서사용할 NSA Suite B 암호화수준을선택합니다. 사용가능한옵션은다음과같습니다.
  - **GCM-128:** 128 비트 AES-GCM 암호화를사용합니다. 이설정은기본값입니다.
  - **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 서버가다수의경로테이블을지원하는경우 추가를클릭하여선택적전달경로를추가합니다.

Samsung Knox 용제네릭프로토콜구성

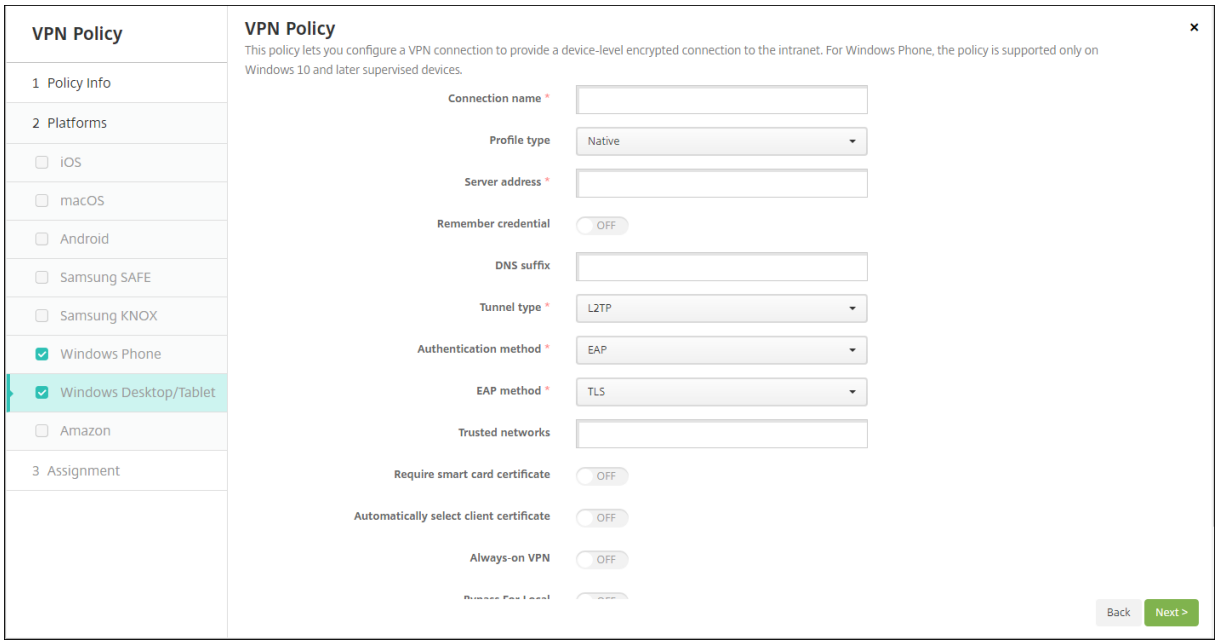
- 연결이름**:** 연결이름을입력합니다. 이것은필수필드입니다.
- 패키지이름에이전트 **VPN:** 장치에설치된 VPN 의패키지이름또는 ID 입니다 (예: Mocana 또는 Pulse Secure).
- 호스트이름**:** VPN 호스트의이름을입력합니다. 이옵션은필수입니다.
- 사용자인증사용**:** 사용자인증이필요한지여부를선택합니다. 사용하는경우다음설정을구성합니다.
  - 사용자이름**:** 사용자이름을입력합니다.
  - 암호**:** 사용자암호를입력합니다.
- **ID:** 이구성에대한선택적식별자를입력합니다. **Vpn** 연결유형 **= IPSEC** 인경우에만적용됩니다.
- **VPN** 연결유형**:** 목록에서사용할연결유형으로 **IPSEC** 또는 **SSL** 을선택합니다. 기본값은 **IPSEC** 입니다. 다음섹션에서는각연결유형에대한구성설정을설명합니다.
- **IPSEC** 연결설정구성
  - **IPsec** 그룹 **ID** 유형**:** 목록에서사용할 IPsec 그룹 ID 유형을선택합니다. 기본값은 기본값입니다. 사용가능한옵션은다음과같습니다.
    - 기본값
    - **IPv4** 주소

    * **FQDN(**정규화된도메인이름**)**
    * 사용자 **FQDN**
    * **IKE** 키 **ID**
- **IKE** 버전**:** 목록에서사용할 Internet Key Exchange 버전을선택합니다. 기본값은 **IKEv1** 입니다.
- 인증방법**:** 목록에서사용할인증방법을선택합니다. 기본값은 인증서입니다. 사용가능한옵션은다음과같습니다.
    * 인증서**:** 인증서인증을사용합니다. 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 인증을상호인증에사용합니다.
    * **CAC** 기반인증**:** CAC(Common Access Card) 를인증에사용합니다.
- **CA** 인증서**:** 목록에서사용할인증서를선택합니다.
- 데드피어감지사용**:** 피어에접속하여활성상태를확인할지여부를선택합니다. 기본값은 꺼짐입니다.
- 기본경로사용**:** VPN 서버에대한기본경로를사용할지여부를선택합니다.
- 모바일옵션사용**:** 모바일옵션을사용할지여부를선택합니다.
- **IKE** 수명 **(**분**):** VPN 연결을다시설정하기전까지의시간 (분) 을입력합니다. 기본값은 1440 분 (24 시간) 입니다.
- **ipsec** 수명 **(**분**):** VPN 연결을다시설정하기전까지의시간 (분) 을입력합니다. 기본값은 1440 분 (24 시간) 입니다.
- **Diffie-Hellman** 그룹값 **(**키강도**):** 목록에서사용할키강도를선택합니다. 기본값은 **0** 입니다.
- **IKE** 단계 **1** 키교환모드**:** IKE 단계 1 교환모드에대해 기본또는 적극적을선택합니다. 기본값은 기본입니다.
    * 기본**:** 협상중에잠재적공격자에게정보가노출되지않지만 적극적모드보다느립니다.
    * 적극적**:** 협상중에일부정보 (예: 협상중인피어의 ID) 가잠재적공격자에게노출되지만 기본모드보다빠릅니다.
- **PFS(Perfect Forward Secrecy)** 값**:** 연결을재협상할때새 PFS 를사용하여새키교환을요구할지여부를선택합니다.
- 분할터널유형**:** 목록에서사용할분할터널유형을선택합니다. 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.
- **IPSEC** 암호화알고리즘**:** IPsec 프로토콜이사용하는 VPN 구성입니다.
- **IKE** 암호화알고리즘**:** IPsec 프로토콜이사용하는 VPN 구성입니다.
- **IKE** 무결성알고리즘**:** IPsec 프로토콜이사용하는 VPN 구성입니다.

- **Knox:** Samsung Knox 전용구성입니다.
- 공급업체**:** Knox API 와통신하는일반에이전트의개인프로필입니다.
- 전달경로**:** 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
  - 전달경로**:** 전달경로의 IP 주소를입력합니다.
  - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.
- 앱별 **VPN:** 추가할각앱별 VPN 에대해 추가를클릭하고다음을수행합니다.
  - 앱별 **VPN:** 앱이통신에사용하는 VPN 구성입니다.
  - 저장을클릭하여앱별 VPN 을저장하거나 취소를클릭하여앱별 VPN 을저장하지않습니다.

- **SSL** 연결설정구성
  - 인증방법**:** 목록에서사용할인증방법을클릭합니다. 사용가능한옵션은다음과같습니다.
    - 해당없음**:** 인증방법이적용되지않습니다. 이설정은기본값입니다.
    - 인증서**:** 인증서인증을사용합니다. 이설정은기본값입니다. 선택한경우 ID 자격증명목록에서사용할자격증명을선택합니다. 기본값은없음입니다.
    - **CAC** 기반인증**:** CAC(Common Access Card) 를인증에사용합니다.
  - **CA** 인증서**:** 목록에서사용할인증서를선택합니다.
  - 기본경로사용**:** VPN 서버에대한기본경로를사용할지여부를선택합니다.
  - 모바일옵션사용**:** 모바일옵션을사용할지여부를선택합니다.
  - 분할터널유형**:** 목록에서사용할분할터널유형을선택합니다. 사용가능한옵션은다음과같습니다.
    - 자동**:** 분할터널링이자동으로사용됩니다.
    - 수동**:** 지정된 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**:** 암호화사용안함**:** 클라이언트-서버협상에사용할 SSL 알고리즘을입력합니다.
  - **SSL** 알고리즘**:** 클라이언트-서버협상에사용할 SSL 알고리즘을입력합니다.
  - **Knox:** Samsung Knox 전용구성입니다.
  - 공급업체**:** Knox API 와통신하는일반에이전트의개인프로필입니다.
  - 전달경로**:** 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
    - 전달경로**:** 전달경로의 IP 주소를입력합니다.
    - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.
  - 앱별 **VPN:** 추가할각앱별 VPN 에대해 추가를클릭하고다음을수행합니다.
    - 앱별 **VPN:** 앱이통신에사용하는 VPN 구성입니다.
    - 저장을클릭하여앱별 VPN 을저장하거나 취소를클릭하여앱별 VPN 을저장하지않습니다.

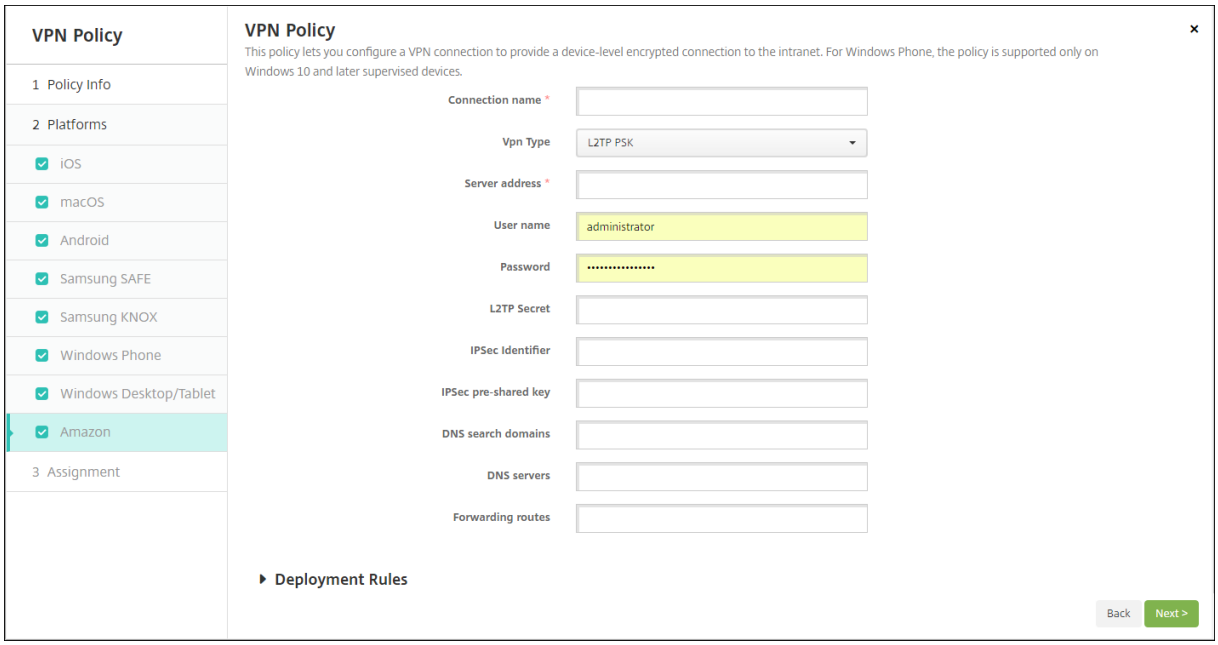
Windows 데스크톱/태블릿설정



- 연결이름**:** 연결이름을입력합니다. 이것은필수필드입니다.
- 프로필유형**:** 목록에서 기본또는 플러그인을선택합니다. 기본값은 기본입니다.
- 기본프로필유형구성**:** 사용자의 Windows 장치에기본제공되는 VPN 에적용되는설정입니다.
  - 서버주소**:** VPN 서버의 FQDN 또는 IP 주소를입력합니다. 이것은필수필드입니다.
  - 자격증명저장**:** 자격증명을캐시할지여부를선택합니다. 기본값은 꺼짐입니다. 사용하면가능한경우항상자격증명이캐시됩니다.
  - **DNS** 접미사**:** DNS 접미사를입력합니다.
  - 터널유형**:** 목록에서사용할 VPN 터널유형을선택합니다. 기본값은 **L2TP** 입니다. 사용가능한옵션은다음과같습니다.
    - **L2TP:** 미리공유한키인증을사용하는계층 2 터널링프로토콜입니다.
    - **PPTP:** 지점간터널링입니다.
    - **IKEv2:** Internet Key Exchange 버전 2 입니다.
  - 인증방법**:** 목록에서사용할인증방법을선택합니다. 기본값은 **EAP** 입니다. 사용가능한옵션은다음과같습니다.
    - **EAP:** Extended Authentication Protocol 의약어로확장인증프로토콜을의미합니다.
    - **MSChapV2:** Microsoft 의 Challenge Handshake 인증을상호인증에사용합니다. **IKEv2** 를터널유형으로선택하는경우이옵션을사용할수없습니다.
  - **EAP** 방법**:** 목록에서사용할 EAP 방법을선택합니다. 기본값은 **TLS** 입니다. MSChapV2 인증을사용하는경우이필드를사용할수없습니다. 사용가능한옵션은다음과같습니다.
    - **TLS:** 전송계층보안
    - **PEAP:** 보호되는확장인증프로토콜
  - 신뢰할수있는네트워크**:** 액세스시 VPN 연결이필요하지않은네트워크목록을쉼표로구분하여입력합니다. 예를들어회사무선네트워크에있는사용자는보호되는리소스에직접액세스할수있습니다.
  - 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 연결이필요하지않은네트워크목록을쉼표로구분하여입력합니다. 예를들어 회사무선네트워크에있는사용자는보호되는리소스에직접액세스할수있습니다.
  - 항상 **VPN** 연결**:** VPN 을항상연결할지여부를선택합니다. 기본값은 꺼짐입니다. 사용하는경우사용자가수동으로 연결을끊기전까지 VPN 연결이연결된상태로유지됩니다.
  - 로컬에대해서는바이패스**:** 로컬리소스의프록시서버바이패스를허용할주소및포트번호를입력합니다.

Amazon 설정



- 연결이름**:** 연결이름을입력합니다.
- **VPN** 유형**:** 연결유형을선택합니다. 사용가능한옵션은다음과같습니다.
  - **L2TP PSK:** 미리공유한키인증을사용하는계층 2 터널링프로토콜입니다. 이설정은기본값입니다.
  - **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 꺼짐입니다.
- 전달경로**:** 회사 VPN 서버가전달경로를지원하는경우사용할각전달경로에대해 추가를클릭하고다음을수행합니다.
  - 전달경로**:** 전달경로의 IP 주소를입력합니다.
  - 저장을클릭하여경로를저장하거나 취소를클릭하여경로를저장하지않습니다.

배경화면장치정책

August 18, 2021

iOS 장치잠금화면, 홈화면또는둘다에배경화면을설정할.png 또는.jpg 파일을추가할수있습니다. iOS 7.1.2 이상에서는감독되는장치에만사용할수있습니다. iPad 및 iPhone 에서서로다른배경화면을사용하려면서로다른배경화면정책을만들어해당사용자에게배포해야합니다.

다음표에는 iOS 장치에대한 Apple 의권장이미지크기가나와있습니다.

iPhone

장치	이미지크기 (픽셀)
iPhone 12 Pro Max	2778 x 1284
iPhone 12 및 iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 2 세대	1334 x 750
iPhone 7 PLus, 8 PLus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 PLus	1334 x 750
iPhone 8	1334 x 750

iPad

장치	이미지크기 (픽셀)
iPad Pro (1, 2, 3 세대 12.9 인치)	2732 x 2048
iPad Pro 10.5 인치	2224 x 1668
iPad Pro(9.7 인치)	1536 x 2048
iPad Air 2	2048 x 1536

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 적용대상**:** 목록에서 잠금화면, 홈 **(**아이콘목록**)** 화면또는 잠금및홈화면을선택하여배경화면이나타날위치를설정합니다.
- 배경화면파일**:** 찾아보기를클릭하고파일위치로이동하여배경화면파일을선택합니다.

웹콘텐츠필터장치정책

January 5, 2022

허용및차단목록에추가한특정사이트와함께 Apple 의자동필터기능을사용하여 iOS 장치에서웹콘텐츠를필터링하는장치정책을 XenMobile 에서추가할수있습니다. 감독모드에서 iOS 7.0 이상의장치에서만이정책을사용할수있습니다. iOS 장치를감독모드로설정하는방법에대한자세한내용은 Apple Configurator 를사용하여 iOS 장치를감독모드로전환을참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 필터유형**:** 목록에서 기본제공또는 플러그인을클릭한후선택한옵션에대한절차를따릅니다. 기본값은 기본제공입니다.

기본제공필터유형

- 웹콘텐츠필터
  - 자동필터사용**:** Apple 의자동필터기능을사용하여웹사이트의부적절한콘텐츠를분석할지여부를선택합니다. 기본값은 꺼짐입니다.
  - 허용 **URL:** 자동필터사용이 꺼짐으로설정된경우이목록이무시됩니다. 자동필터사용이 켜짐으로설정된경우자동필터가액세스를허용하는지여부에관계없이항상이목록의항목에액세스할수있습니다. 허용목록에추가할각 URL 에대해 추가를클릭하여다음을수행합니다.

        * 허용된웹사이트의 URL 을입력합니다. 웹주소앞에 `http://` 또는 `https://`를추가해야합니다.
        * 웹사이트를허용목록에저장하려면 저장을클릭하고, 저장하지않으려면 취소를클릭합니다.
    - 블랙리스트 **URL:** 이목록의항목은항상차단됩니다. 차단목록에추가할각 URL 에대해 추가를클릭하여다음을수행합니다.
        * 차단할웹사이트의 URL 을입력합니다. 웹주소앞에 `http://` 또는 `https://`를추가해야합니다.
        * 웹사이트를차단목록에저장하려면 저장을클릭하고, 저장하지않으려면 취소를클릭합니다.

          > 참고:
          > XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는용어가포함됩니다. 향후릴리스에서이러한용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.

- 책갈피화이트리스트
    - 책갈피화이트리스트**:** 사용자가액세스할수있는사이트를지정합니다. 웹사이트에액세스할수있도록하려면해당웹사이트의 URL 을추가합니다.
        * **URL:** 사용자가액세스할수있는각웹사이트의 URL 입니다. 예를들어 Secure Hub 스토어에액세스할수있도록하려면 **URL** 목록에 XenMobile Server URL 을추가합니다. 웹주소앞에 `http://` 또는 `https://`를추가해야합니다. 이것은필수필드입니다.
        * 책갈피폴더**:** 선택적책갈피폴더이름을입력합니다. 이필드를비워두면책갈피가책갈피기본디렉터리에추가됩니다.
        * 제목**:** 웹사이트를설명하는제목을입력합니다. 예를들어, URL 이 `https://google.com`인경우 “Google” 을입력합니다.
        * 웹사이트를허용목록에저장하려면 저장을클릭하고, 저장하지않으려면 취소를클릭합니다.

플러그인필터유형

- 필터이름**:** 필터에대한고유한이름을입력합니다.
- 식별자**:** 필터링서비스를제공하는플러그인의번들 ID 를입력합니다.
- 서비스주소**:** 선택적서버주소를입력합니다. 올바른형식은 IP 주소, 호스트이름또는 URL 입니다.
- 사용자이름**:** 서비스에대한선택적사용자이름을입력합니다.
- 암호**:** 서비스에대한선택적암호를입력합니다.
- 인증서**:** 목록에서서비스에사용자를인증하는데사용할선택적 ID 인증서를클릭합니다. 기본값은 없음입니다.
- **WebKit** 트래픽필터링**:** WebKit 트래픽을필터링할것인지를선택합니다.
- 소켓트래픽필터링**:** 소켓트래픽을필터링할것인지를선택합니다.
- 사용자지정데이터**:** 웹필터에추가할각사용자지정키에대해 추가를클릭한후다음을수행합니다.
    - 키**:** 사용자지정키를입력합니다.
    - 값**:** 사용자지정키값을입력합니다.
    - 사용자지정키를저장하려면 저장을클릭하고, 저장하지않으려면 취소를클릭합니다.
- 정책설정
    - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
        * 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
        * 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용

할수있습니다.

웹클립장치정책

January 5, 2022

웹사이트에대한바로가기또는웹클립을배치하여앱과나란히사용자장치에표시할수있습니다. iOS, iPadOS, macOS X 및 Android 장치의웹클립을나타내는사용자지정아이콘을지정할수있습니다. Windows 태블릿에는레이블과 URL 만필요합니다. iOS 및 iPadOS 장치의경우만든웹클립을구성하도록홈화면레이아웃장치정책을구성합니다. iOS 에서앱액세스를제한할경우웹클립을허용하도록제한장치정책을구성해야합니다. 이러한정책구성에대한자세한내용은 홈화면레이아웃장치정책 및 제한장치정책을참조하십시오.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

iOS 설정

- 레이블**:** 웹클립과함께표시할레이블을입력합니다.
- **URL:** 웹클립과연관된 URL 을입력합니다. URL 은프로토콜 (예: `https://server`) 로시작해야합니다.
- 제거가능**:** 사용자가웹클립을제거할수있는지여부를선택합니다. 기본값은 꺼짐입니다.
- 업데이트할아이콘**:** 찾아보기를클릭하고파일의위치로이동하여웹클립에사용할아이콘을선택합니다.
- 미리작성된아이콘**:** 아이콘에적용된효과 (둥근모서리, 그림자및반사광택) 가있는지여부를선택합니다. 기본값은효과를추가하는 꺼짐입니다.
- 전체화면**:** 링크된웹페이지를전체화면모드로열지여부를선택합니다. 기본값은 꺼짐입니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

macOS 설정

- 레이블**:** 웹클립과함께표시할레이블을입력합니다.
- **URL:** 웹클립과연관된 URL 을입력합니다. URL 은프로토콜 (예: `https://server`) 로시작해야합니다.
- 업데이트할아이콘**:** 찾아보기를클릭하고파일의위치로이동하여웹클립에사용할아이콘을선택합니다.

Android 설정

- 규칙**:** 이정책으로웹클립을추가할지아니면제거할지선택합니다. 기본값은 추가입니다.
- 레이블**:** 웹클립과함께표시할레이블을입력합니다.
- **URL:** 웹클립과연관된 URL 을입력합니다.
- 아이콘정의**:** 아이콘파일사용여부를선택합니다. 기본값은 꺼짐입니다.
- 아이콘파일**:** 아이콘정의가 켜짐인경우 찾아보기를클릭하고파일위치로이동하여사용할아이콘파일을선택합니다.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    - 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    - 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다.
  - 사용자가정책을제거하도록허용**:** 사용자가장치에서정책을제거할수있는시기를선택할수있습니다. 메뉴에서 항상, 암호필요또는 안함을선택합니다. 암호필요를선택한경우 제거암호필드에암호를입력합니다.
  - 프로필범위**:** 이정책을 사용자에적용할지, 전체 시스템에적용할지선택합니다. 기본값은 사용자입니다. 이옵션은 macOS 10.7 이상에서만사용할수있습니다.

Windows 데스크톱/태블릿설정

- 이름**:** 웹클립과함께표시할레이블을입력합니다.
- **URL:** 웹클립과연관된 URL 을입력합니다.

Wi-Fi 장치정책

August 12, 2022

XenMobile 에서 Wi-Fi 장치정책을새로만들거나기존 Wi-Fi 장치정책을편집하려면 구성 **>** 장치정책페이지를사용합니다. Wi-Fi 정책을사용하면다음항목을정의하여사용자가장치를 Wi-Fi 네트워크에연결하는방식을관리할수있습니다.

- 네트워크이름및유형
- 인증및보안정책
- 프록시서버사용
- 기타 WiFi 관련정보

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

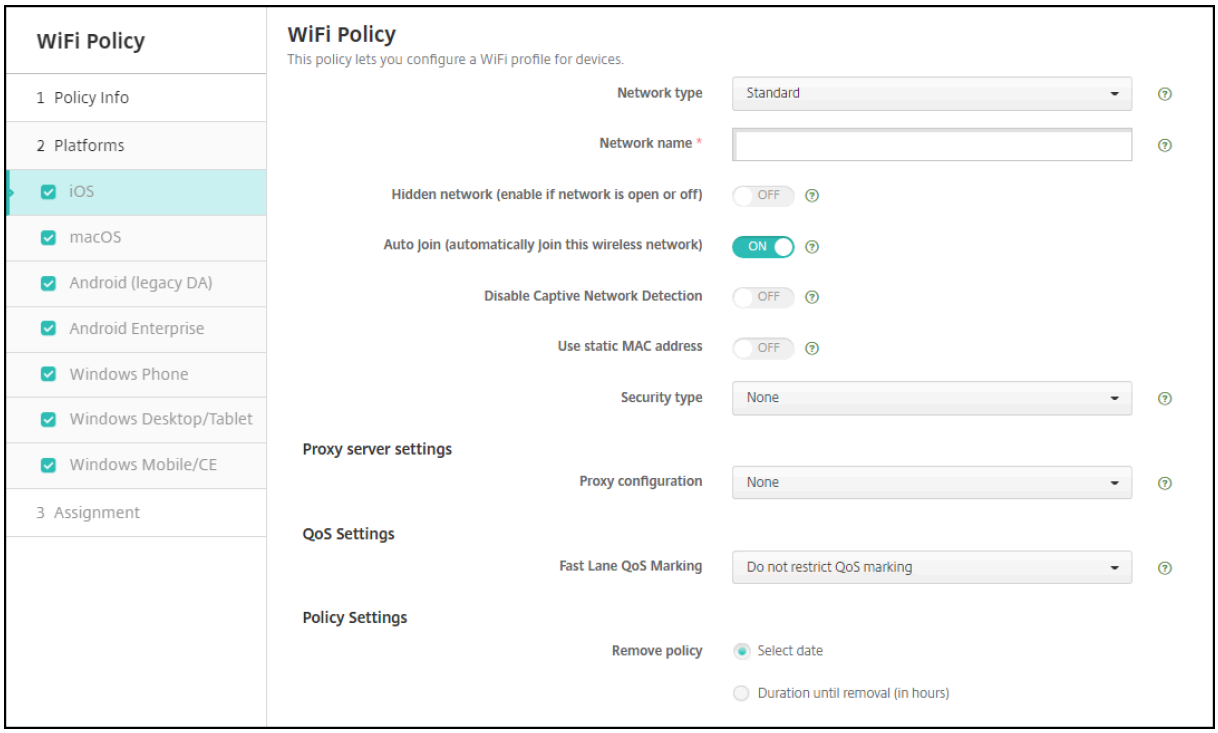
사전요구사항

정책을만들려면먼저다음단계를완료해야합니다.

- 사용하려는배달그룹을만듭니다.
- 네트워크이름과유형을파악합니다.
- 사용할인증또는보안유형을파악합니다.
- 필요할수있는프록시서버정보를파악합니다.
- 필요한모든 CA 인증서를설치합니다.
- 필요한공유키를확보합니다.
- 인증서기반인증을위한 PKI 엔터티를만듭니다.
- 자격증명공급자를구성합니다.

자세한내용은 인증 및그하위문서를참조하십시오.

iOS 설정



- 네트워크유형**:** 목록에서 표준, 레거시핫스폿또는 **Hotspot 2.0** 을선택하여사용할네트워크유형을설정합니다.
- 네트워크이름**:** 장치의사용가능한네트워크목록에표시되는 SSID 를입력합니다. **Hotspot 2.0** 에는적용되지않습니다.
- 숨겨진네트워크 **(**네트워크가열려있거나꺼져있는경우에사용**):** 네트워크를숨길지여부를선택합니다.
- 자동참가 **(**이무선네트워크에자동참가**):** 네트워크를자동으로참가시킬지여부를선택합니다. iOS 장치가이미다른네트워크에연결되어있으면이네트워크에연결되지않습니다. 장치가자동으로연결되기전에사용자가이전네트워크와의연결을끊어야합니다. 기본값은 켜짐입니다.
- 정적 **MAC** 주소사용**:** MAC 주소는장치가네트워크내에서전송하는고유식별자입니다. 개인정보보호를강화하기위해 iOS 및 iPadOS 장치에서는네트워크에연결할때마다다른 MAC 주소를사용할수있습니다. 켜짐인경우장치에서이네트워크에연결할때항상동일한 MAC 주소를사용합니다. 꺼짐인경우장치에서이네트워크에연결할때마다다른 MAC 주소를사용합니다. 기본값은 꺼짐입니다.

- 보안유형**:** 목록에서사용하려는보안유형을선택합니다. **Hotspot 2.0** 에는적용되지않습니다.
  - 없음 - 추가구성이필요없습니다.
  - WEP
  - WPA/WPA2 개인
  - 임의 (개인)
  - WEP 엔터프라이즈
  - WPA/WPA2 엔터프라이즈: WPA-2 엔터프라이즈를사용하려면 SCEP(단순인증서등록프로토콜) 를구성해야합니다. 그런다음 XenMobile 에서장치에인증서를보내 Wi-Fi 서버인증을수행할수있습니다. SCEP 를구성하려면 설정 **>** 자격증명공급자의배포페이지로이동합니다. 자세한내용은 자격증명공급자를참조하십시오.
  - 임의 (엔터프라이즈)

다음섹션에는위의각연결유형에대해구성하는옵션이나열되어있습니다.

iOS 의 **WPA, WPA** 개인**,** 임의 **(**개인**)** 설정

암호**:** 선택적암호를입력합니다. 이필드를공백으로두면사용자가로그온할때암호를입력하라는메시지가표시될수있습니다.

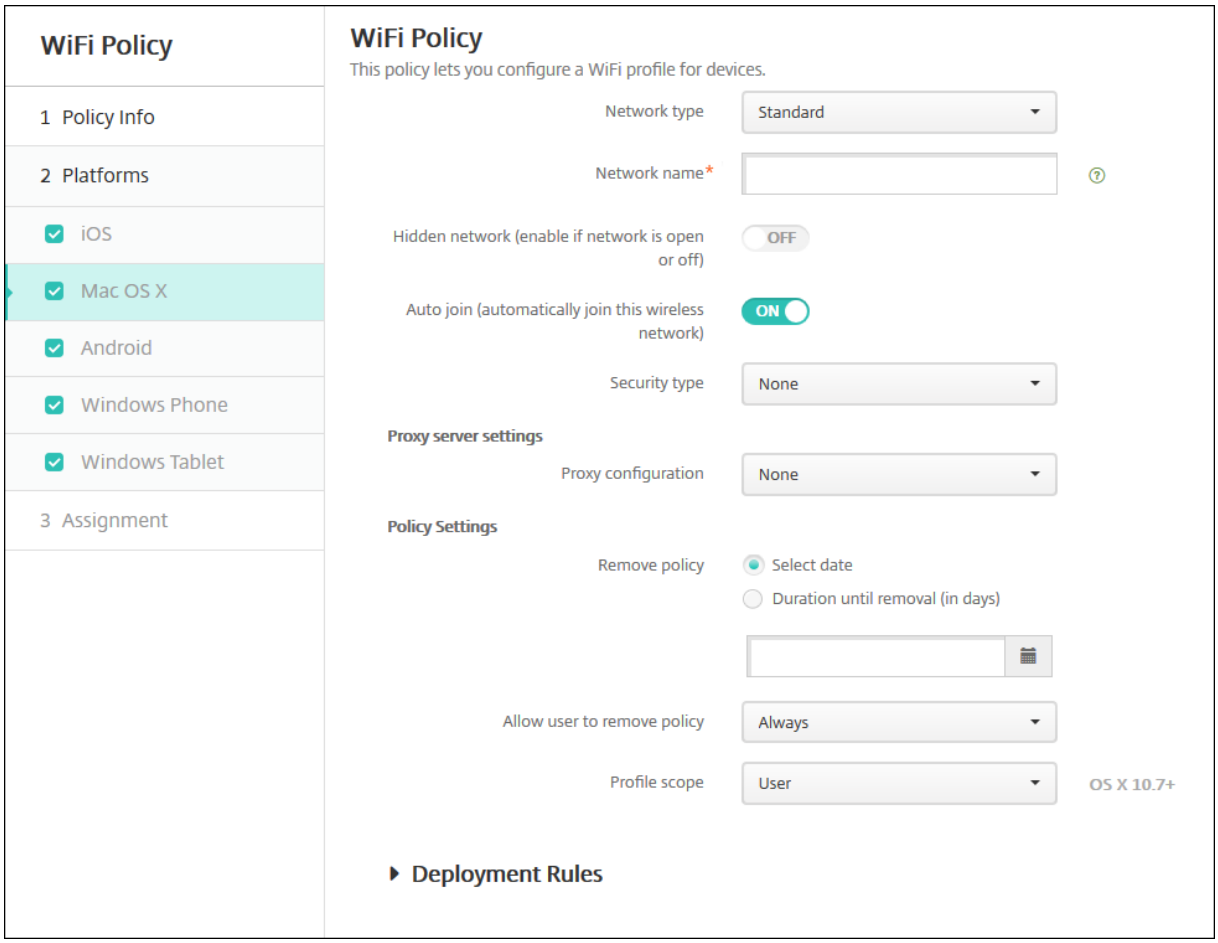
iOS 의 **WEP** 엔터프라이즈**, WPA** 엔터프라이즈**, WPA2** 엔터프라이즈**,** 임의 **(**엔터프라이즈**)** 설정

이러한설정중하나를선택하면해당설정이 프록시서버설정뒤에나열됩니다.

- 프로토콜**,** 허용되는 **EAP** 유형**:** 지원할 EAP 유형을사용하도록설정한후관련설정을구성합니다. 사용가능한각 EAP 유형에서기본값은 꺼짐입니다.
- 내부인증 **(TTLS):** *TTLS* 를사용하는경우에만필요합니다. 목록에서사용할내부인증방법을선택합니다. 사용가능한옵션은 **PAP**, **CHAP**, **MSCHAP** 또는 **MSCHAPv2** 입니다. 기본값은 **MSCHAPv2** 입니다.
- 프로토콜**, EAP-FAST:** PAC(보호액세스자격증명) 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**:** 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.
- 정책설정
  - 정책제거**:** 정책제거를예약할때사용할방법을선택합니다. 사용가능한옵션은 날짜선택과 제거할때까지의기간 **(**시간**)** 입니다.
    * 날짜선택**:** 달력을클릭하여제거할특정날짜를선택합니다.
    * 제거할때까지의기간 **(**시간**):** 정책제거가발생할때까지시간을숫자로입력합니다. iOS 6.0 이상에서만사용할수있습니다.

macOS 설정



- 네트워크유형**:** 목록에서 표준, 레거시핫스폿또는 **Hotspot 2.0** 을선택하여사용할네트워크유형을설정합니다.
- 네트워크이름**:** 장치의사용가능한네트워크목록에표시되는 SSID 를입력합니다. **Hotspot 2.0** 에는적용되지않습니다.
- 숨겨진네트워크 **(**네트워크가열려있거나꺼져있는경우에사용**):** 네트워크를숨길지여부를선택합니다.
- 자동참가 **(**이무선네트워크에자동참가**):** 네트워크를자동으로참가시킬지여부를선택합니다. 장치가이미다른네트워크에연결되어있으면이네트워크에연결되지않습니다. 장치가자동으로연결되기전에사용자가이전네트워크와의연결을끊어야합니다. 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.

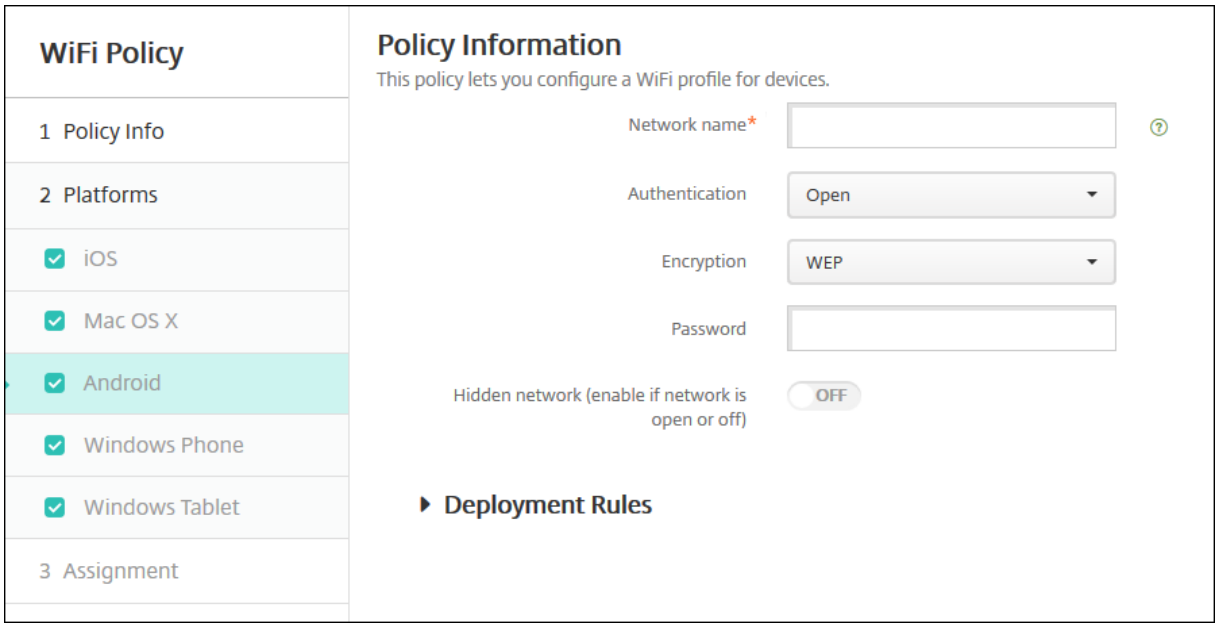
macOS 의 **WEP** 엔터프라이즈**, WPA** 엔터프라이즈**, WPA2** 엔터프라이즈**,** 임의 **(**엔터프라이즈**)** 설정

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(보호액세스자격증명) 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 켜짐입니다.
- 로그인윈도구성으로사용**:** 로그인창에입력한자격증명을동일하게사용하여사용자를인증할지여부를선택합니다.
- 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.

Android 설정



- 네트워크이름**:** 사용자장치의사용가능한네트워크목록에있는 SSID 를입력합니다.
- 인증**:** 목록에서 Wi-Fi 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.

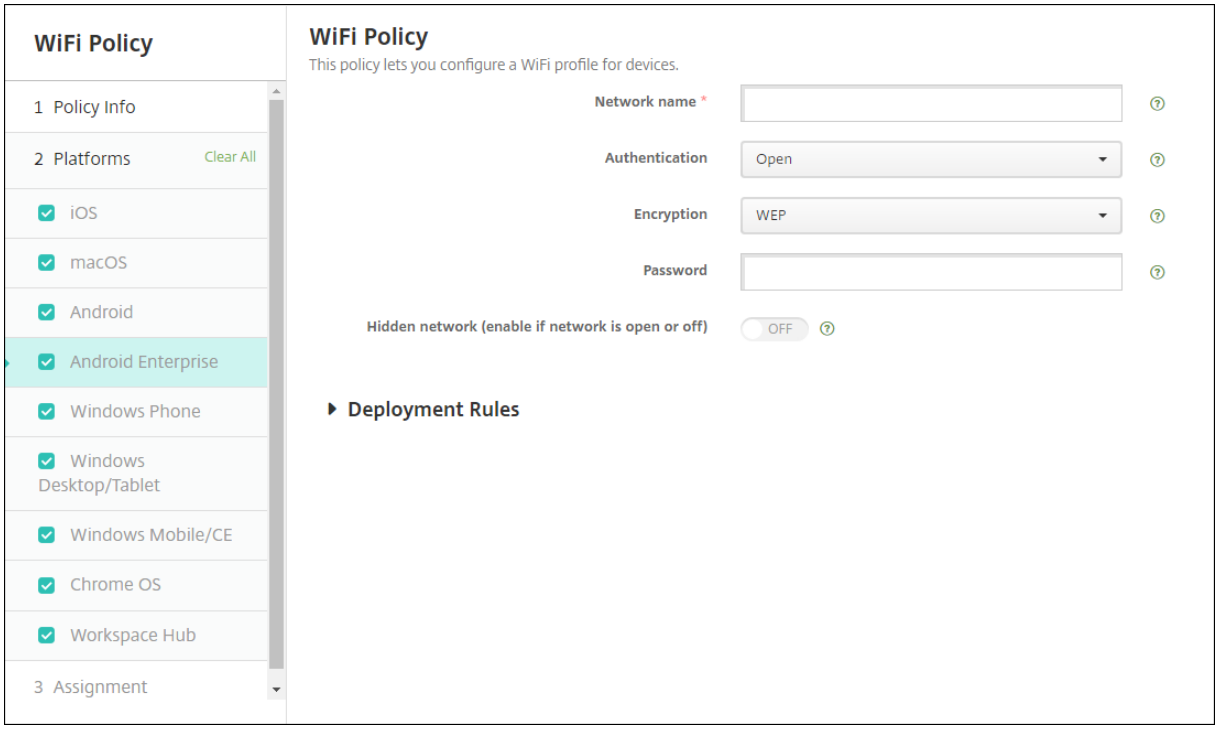
Android 의 **WPA, WPA-PSK, WPA2, WPA2-PSK** 설정

- 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 Wi-Fi 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.

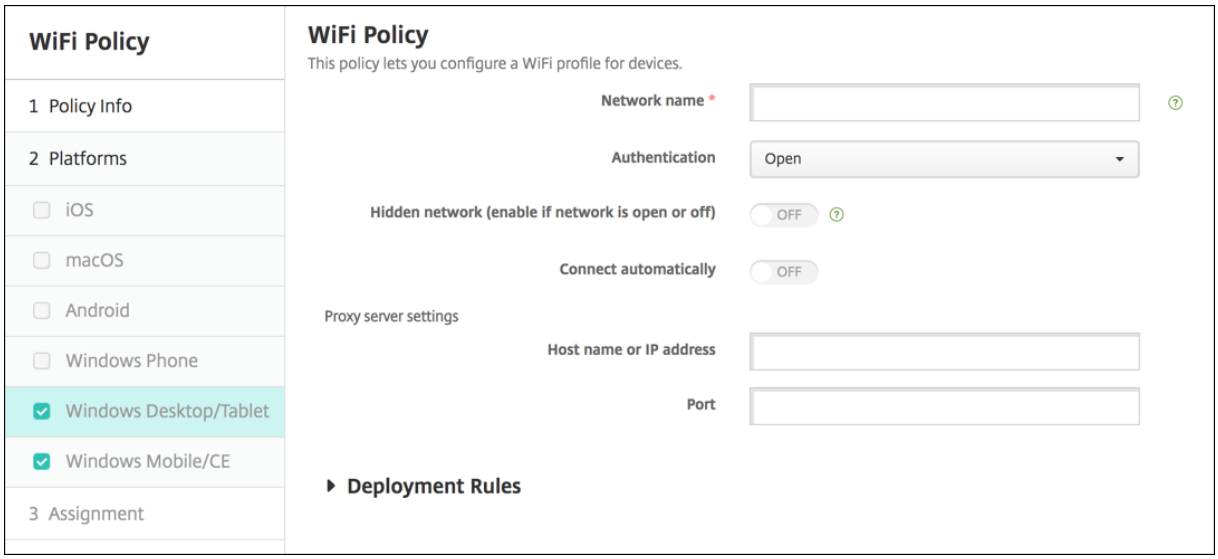
Android 의 **WPA, WPA-PSK, WPA2, WPA2-PSK** 설정

- 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.

Windows 10 및 **Windows 11** 설정



- 인증**:** 목록에서 Wi-Fi 연결에사용할보안유형을클릭합니다.
  - 공개
  - WPA 개인
  - WPA-2 개인
  - WPA 엔터프라이즈
  - WPA-2 엔터프라이즈: WPA-2 엔터프라이즈를사용하려면 SCEP 를구성해야합니다. SCEP 구성을사용하면 XenMobile 에서장치에인증서를보내 Wi-Fi 서버인증을수행할수있습니다. SCEP 를구성하려면 설정 **>** 자격증명공급자의 배포페이지로이동합니다. 자세한내용은 자격증명공급자를참조하십시오.

다음섹션에는위의각연결유형에대해구성하는옵션이나열되어있습니다.

Windows 10 및 **Windows 11** 설정열기

- 숨겨진네트워크 **(**네트워크가열려있거나꺼져있는경우에사용**):** 네트워크를숨길지여부를선택합니다.
- 자동연결**:** 네트워크에자동으로연결할지여부를선택합니다.

Windows 10 및 **Windows 11** 의 **WPA** 개인**, WPA-2** 개인설정

- 암호화**:** 목록에서 **AES** 또는 **TKIP** 를선택하여암호화유형을설정합니다. 기본값은 **AES** 입니다.
- 숨겨진네트워크 **(**네트워크가열려있거나꺼져있는경우에사용**):** 네트워크를숨길지여부를선택합니다.
- 자동연결**:** 네트워크에자동으로연결할지여부를선택합니다.

Windows 10 및 **Windows 11** 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**:** 네트워크를숨길지여부를선택합니다.
- 자동연결**:** 네트워크에자동으로연결할지여부를선택합니다.
- **SCEP** 를통해인증서푸시**:** SCEP(단순인증서등록프로토콜) 를통해사용자장치에인증서를푸시할지여부를선택합니다.
- **SCEP** 의자격증명공급자**:** 목록에서 SCEP 자격증명공급자를선택합니다. 기본값은 없음입니다.

Windows Information Protection 장치정책

August 12, 2022

이전의 EDP(엔터프라이즈데이터보호) 인 WIP(Windows Information Protection) 는엔터프라이즈데이터의잠재적유출을차단하는 Windows 기술입니다. 데이터유출은엔터프라이즈에서보호되지않는앱, 앱간또는조직네트워크외부로엔터프라이즈데이터를공유하는과정에서발생할수있습니다. 자세한내용은 Protect your enterprise data using Windows Information Protection (WIP)(WIP(Windows Information Protection) 를사용하여엔터프라이즈데이터보호)를 참조하십시오.

XenMobile 에서장치정책을생성하여설정한적용수준의 Windows Information Protection 이필요한앱을지정할수있습니다. Windows Information Protection 정책은감독되는 Windows 10 또는 Windows 11 실행태블릿및데스크톱에적용됩니다.

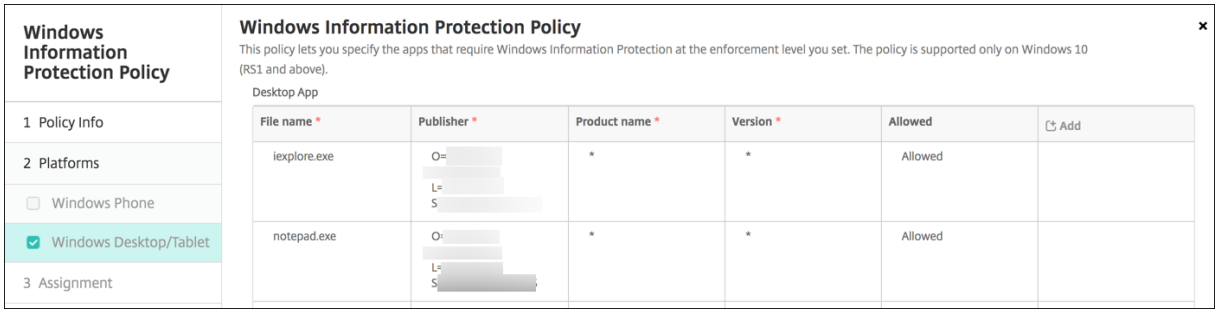
XenMobile 에는자주사용되는앱몇가지가포함되어있으며다른앱도추가할수있습니다. 사용자환경에영향을미치는정책적용수준을지정할수있습니다. 예를들어다음을수행할수있습니다.

- 부적절한데이터공유차단
- 부적절한데이터공유에대해경고하고사용자가정책을재정의할수있도록허용
- 부적절한데이터공유를로깅하고허용하는동안 WIP 를자동으로실행

Windows Information Protection 에서앱을제외하려면 Microsoft AppLocker XML 파일에서앱을정의한다음이파일을 XenMobile 로가져옵니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Windows 10 및 Windows 11 설정



- 데스크톱앱 (Windows 10 또는 Windows 11 태블릿), 스토어앱 (Windows 10 및 Windows 11 태블릿): XenMobile 에는위의샘플처럼몇가지자주사용되는앱이포함되어있습니다. 필요에따라이러한앱을편집하거나제거할수있습니다.

  다른앱을추가하려면: 데스크톱앱또는 스토어앱테이블에서 추가를클릭하고앱정보를제공합니다.

  허용되는앱은엔터프라이즈데이터를읽고, 만들고, 업데이트할수있습니다. 거부되는앱은엔터프라이즈데이터에액세스할수없습니다. 예외앱은엔터프라이즈데이터를읽을수있지만데이터를만들거나수정할수는없습니다.

  - **AppLocker XML:** Microsoft 는 WIP 와호환성문제가있는것으로알려진 Microsoft 앱의목록을제공합니다. 이러한앱을 WIP 에서제외하려면 찾아보기를클릭하고목록을업로드합니다. XenMobile 은업로드된 AppLocker XML 과구성된데스크톱및스토어앱을장치로전송된정책에서결합합니다. 자세한내용은 Windows Information Protection 에대한권장거부목록을참조하십시오.
  - 적용수준**:** Windows Information Protection 이데이터공유를보호하고관리할방식을지정하는옵션을선택합니다. 기본값은 꺼짐입니다.
    * **0-**꺼짐**:** WIP 가꺼지며데이터를보호또는감사하지않습니다.
    * **1-**무음**:** WIP 가자동으로실행되면서부적절한데이터공유를기록하고아무것도차단하지않습니다. 보고 CSP를통해로그에액세스할수있습니다.
    * **2-**재정의**:** WIP 가잠재적으로안전하지않은데이터공유에대해사용자에게경고합니다. 사용자는경고를재정의하고데이터를공유할수있습니다. 이모드는사용자재정의를포함한작업을감사로그에기록합니다.
    * **3-**차단**:** WIP 는사용자가안전하지않을수있는데이터공유를수행하는것을차단합니다.
  - 보호되는도메인이름**:** 엔터프라이즈가사용자 ID 에사용하는도메인입니다. 관리되는 ID 도메인의이목록은기본도메인과함께관리엔터프라이즈의 ID 를구성합니다. 목록에서첫번째도메인은 Windows UI 에사용되는기본회사 ID 입니다. “|“를사용하여목록항목을구분합니다. 예: `domain1.com | domain2.com`
  - 데이터복구인증서**:** 찾아보기를클릭한다음암호화된파일의데이터복구에사용할복구인증서를선택합니다. 이인증서는그룹정책이아니라 MDM 을통해배달된다는점이외에는 EFS(암호화파일시스템) 에대한 DRA(데이터복구에이전트) 와동일합니다. 복구인증서를사용할수없는경우새로만듭니다. 자세한내용은이섹션의 “데이터복구인증서만들기” 를참조하십시오.
  - 네트워크도메인이름**:** 엔터프라이즈의경계를구성하는도메인의목록입니다. WIP 는목록의정규화된도메인에대한모든트래픽을보호합니다. 이설정은 **IP** 범위설정과함께사용되어네트워크끝점이엔터프라이즈인지아니면사설망의개인인지를감지합니다. 쉼표를사용하여목록항목을구분합니다. 예: corp.example.com,region.example.com
  - **IP** 범위**:** 엔터프라이즈네트워크의컴퓨터를정의하는엔터프라이즈 IPv4 및 IPv6 범위의목록입니다. WIP 는이러한위치를엔터프라이즈데이터를공유해도안전한대상으로고려합니다. 쉼표를사용하여목록항목을구분합니다. 예:

    `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff:ffff`
  - **IP** 범위목록을신뢰할수있음**:** Windows 에의한 IP 범위의자동감지를방지하려면이설정을 켜짐으로변경합니다. 기본값은 꺼짐입니다.

- 프록시서버**:** 엔터프라이즈가회사리소스에사용할수있는프록시서버의목록입니다. 네트워크에서프록시를사용하는경우이설정이필요합니다. 프록시서버가없으면프록시뒤에있는클라이언트가엔터프라이즈리소스를사용하지못할수있습니다. 예를들어호텔및식당의특정 WiFi 핫스폿에서리소스를사용하지못할수있습니다. 쉼표를사용하여목록항목을구분합니다. 예:

  ```
  proxy.example.com:80;157.54.11.118:443
  ```

- 내부프록시서버**:** 장치가클라우드리소스에연결하기위해통과하는프록시서버의목록입니다. 이서버유형을사용하면, 연결하는클라우드리소스가엔터프라이즈리소스임을나타냅니다. 이목록에 WIP 비보호트래픽에사용되는 프록시서버설정의서버를포함하지마십시오. 쉼표를사용하여목록항목을구분합니다. 예:

  ```
  example.internalproxy1.com;10.147.80.50
  ```

- 클라우드리소스**:** WIP 로보호되는클라우드리소스의목록입니다. 원하는경우각클라우드리소스에대해, 이클라우드리소스에대한트래픽을라우팅할 프록시서버목록의프록시서버를지정할수도있습니다. 프록시서버를통해라우팅되는모든트래픽은엔터프라이즈트래픽으로취급됩니다. 쉼표를사용하여목록항목을구분합니다. 예:

  ```
  domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
  domain2.com
  ```

- 등록취소할때 **WIP** 인증서해지**:** Windows Information Protection 에서등록취소될때사용자장치에서로컬암호화키를해지할지여부를지정합니다. 암호화키가해지되면사용자는암호화된회사데이터에액세스할수없습니다. 꺼짐인경우키가해지되지않으며사용자는등록취소후에도보호된파일에계속액세스할수있습니다. 기본값은 켜짐입니다.

- 오버레이아이콘표시**:** 탐색기의회사파일및시작메뉴의엔터프라이즈전용앱타일에 Windows Information Protection 아이콘오버레이를포함할지여부를지정합니다. 기본값은 꺼짐입니다.

데이터복구인증서만들기

Windows Information Protection 정책을사용하도록설정하려면데이터복구인증서가필요합니다.

1. XenMobile 콘솔이실행되는컴퓨터에서명령프롬프트를열고인증서를만들려는폴더 (Windows\System32 이외의폴더) 로이동합니다.
2. 다음명령을실행합니다.

   ```
   cipher /r:ESFDRA
   ```

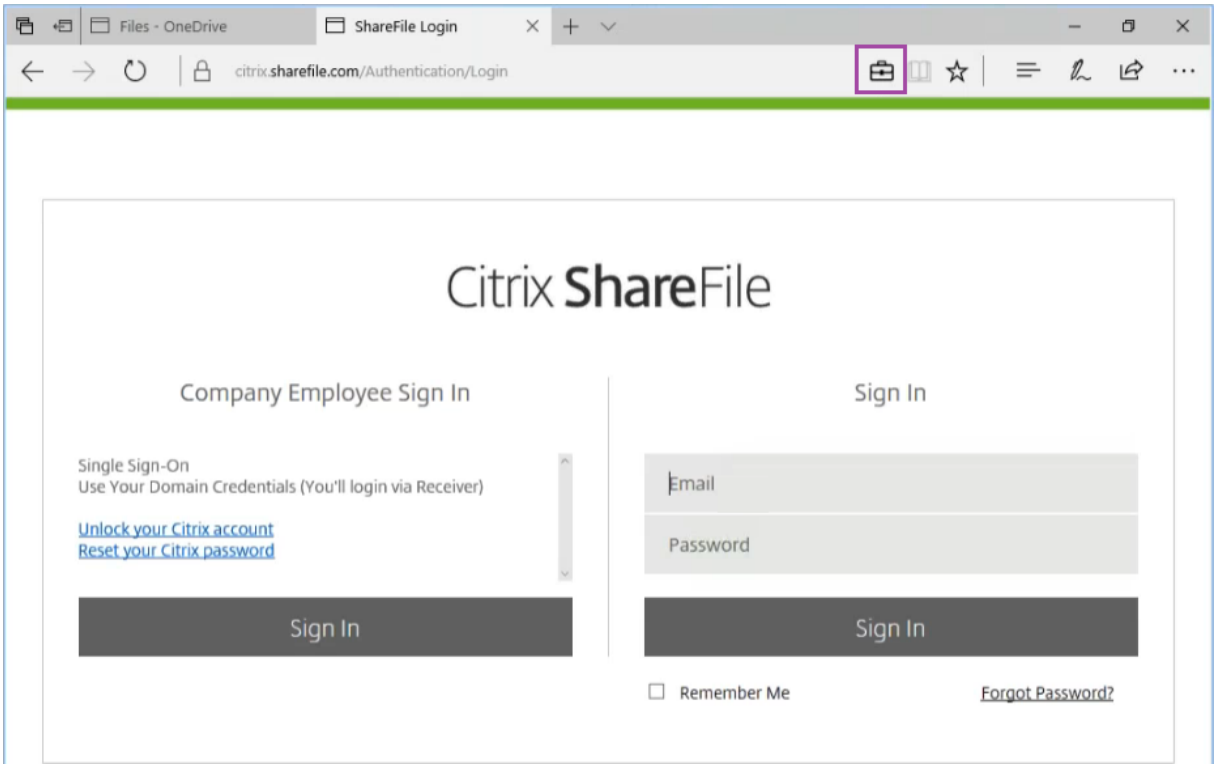
3. 메시지가나타나면개인키파일을보호하기위한암호를입력합니다.

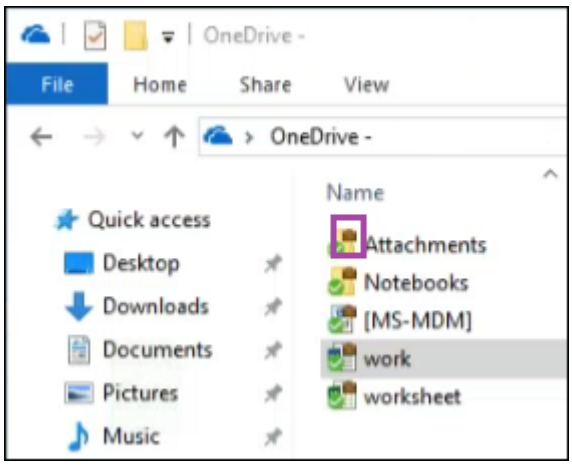
   암호화명령은.cer 및.pfx 파일을생성합니다.

4. XenMobile 콘솔에서 설정 **>** 인증서로이동하고 Windows 10 및 Windows 11 태블릿에적용되는.cer 파일을가져옵니다.

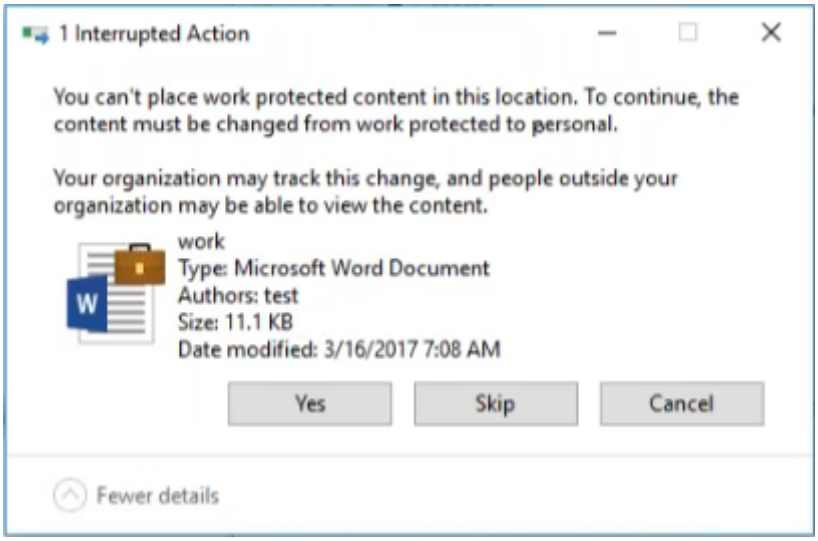
사용자환경

Windows Information Protection 이적용될때는앱과파일에다음아이콘이포함됩니다.





사용자가보호되는파일을보호되지않는위치로복사하거나저장할경우구성된적용수준에따라다음알림이나타납니다.



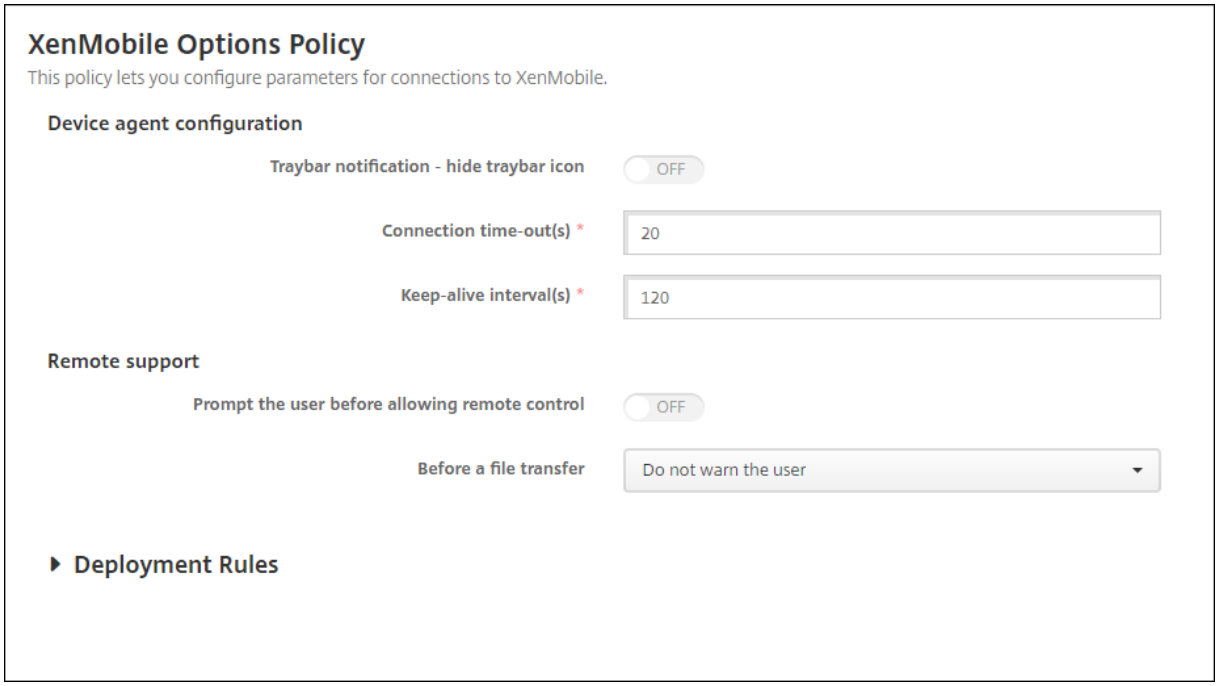
XenMobile 옵션장치정책

August 12, 2022

Android 장치에서 XenMobile 에연결할때 Secure Hub 동작을구성하는 XenMobile 옵션정책을추가합니다.

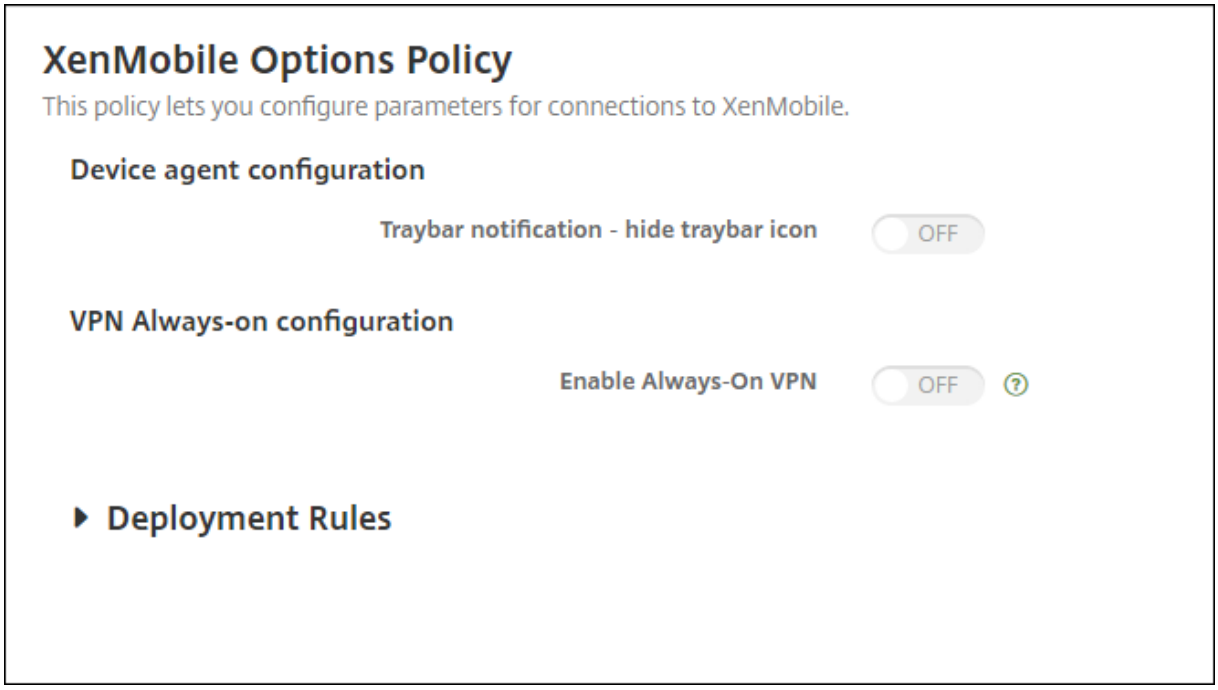
이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

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.

Android Enterprise 설정



Android 버전 7 부터지원됩니다.

- 트레이표시줄알림 - 트레이표시줄아이콘숨기기: 트레이표시줄아이콘을표시할지, 아니면숨길지를선택합니다. 기본값은 꺼짐입니다.
- 항상 **VPN** 연결사용. 항상 VPN 연결을사용할지여부를선택합니다. 이설정이 켜짐인경우장치의전원이켜지면 VPN 서비스가시작되고장치가켜져있는동안계속실행됩니다. 기본값은 꺼짐입니다.
- **VPN** 패키지. 장치에서사용하는 VPN 앱의패키지이름을입력합니다. 기본적으로이필드에는 Citrix SSO 앱의패키지이름인 **com.CitrixVPN** 이자동으로채워집니다.

XenMobile 제거장치정책

August 12, 2022

XenMobile 에서장치정책을추가하여 Android 장치에서 XenMobile 을제거할수있습니다. 이정책을배포하면배포그룹에있는모든장치에서 XenMobile 이제거됩니다.

이정책을추가하거나구성하려면 구성 **>** 장치정책으로이동합니다. 자세한내용은 장치정책을참조하십시오.

Android 설정구성

- 장치에서 **XenMobile** 제거**:** 이정책을배포할모든장치에서 XenMobile 을제거할지여부를선택합니다. 기본값은 꺼짐입니다.

앱추가

January 6, 2022

XenMobile 에앱을추가하면 MAM(모바일애플리케이션관리) 기능을이용할수있습니다. XenMobile 은응용프로그램제공, 소프트웨어라이선스, 구성및응용프로그램수명주기관리를지원합니다.

MDX 지원앱은대부분의앱유형을사용자장치에배포하기위해준비하는데중요한부분입니다. MDX 에대한소개는 MDX Toolkit 정보 [및](/en-us/mdx-toolkit/mam-sdk-overview.html)MAM SDK 개요를참조하십시오.

- Citrix 에서는 MDX 지원앱에 MAM SDK 를사용할것을권장합니다. 또는 MDX Toolkit 이더이상사용되지않을때까지 MDX 래핑앱을계속사용할수있습니다. 사용중단을참조하십시오.
- MDX Toolkit 을사용하여 Citrix 모바일생산성앱을래핑할수없습니다. Citrix 다운로드에서모바일생산성앱 MDX 파일을다운로드하십시오.

XenMobile 콘솔에앱을추가하면다음작업을수행할수있습니다.

- 앱설정을구성합니다.
- 필요에따라앱을범주로정렬하여 Secure Hub 에서앱을구성합니다.
- 필요에따라사용자의앱액세스를허용하기전에승인이필요하도록워크플로를정의합니다.
- 사용자에게앱을배포합니다.

이문서에서는앱추가에관한일반적인워크플로를설명합니다. 플랫폼별자세한내용은다음문서를참조하십시오.

- Android Enterprise 앱배포
- Apple 앱배포

앱유형및기능

다음표에는 XenMobile 로배포할수있는앱유형이요약되어있습니다.

앱유형	출처	참고	참조
MDX	사용자용으로개발하는 iOS 및 Android 앱과 Citrix 모바일생산성앱입니다.	MAM SDK 로 iOS 또는 Android 앱을개발하거나 MDX Toolkit 으로앱을래핑합니다. 모바일생산성앱의경우 Citrix 다운로드에서 공용스토어 MDX 파일을다운로드합니다. 그런다음 XenMobile 에앱을추가합니다.	MDX 앱추가
공용앱스토어	Google Play 또는 Apple App Store 와같은 공용앱스토어의무료또는유료앱입니다.	앱, MDX 지원앱을업로드하고앱을 XenMobile 에추가합니다.	공용앱스토어앱추가
웹및 SaaS	내부네트워크 (웹앱) 또는공용네트워크 (SaaS)	Citrix Workspace 는 MDM 에등록된 iOS 및 Android 장치에서기본 SaaS 앱에대한모바일 Single Sign-on 을제공합니다. 또는 SAML(Security Assertion Markup Language) 응용프로그램커넥터를사용합니다.	웹또는 SaaS 앱추가
Enterprise	Win32 앱등 MDX 를지원하지않는개인앱과 MDX 지원개인 Android Enterprise 앱입니다. Enterprise 앱은 CDN(Content Delivery Network) 위치또는 XenMobile 서버에상주합니다.	XenMobile 에앱을추가합니다.	엔터프라이즈앱추가
웹링크	Single Sign-On 이필요하지않은인터넷웹주소, 인트라넷웹주소또는웹앱입니다.	XenMobile 에서웹링크를구성합니다.	웹링크추가

앱배포를계획할때는다음기능을고려하십시오.

- 자동설치정보
- 필수앱과선택적앱정보
- 앱범주정보
- Microsoft 365 앱사용
- 워크플로적용
- 앱스토어및 Citrix Secure Hub 브랜딩

자동설치정보

Citrix 는 iOS, Android Enterprise 및 Samsung 앱의자동설치및업그레이드를지원합니다. 자동설치에서는장치에배포한앱을설치하라는메시지가사용자에게표시되지않습니다. 앱이백그라운드에서자동으로설치됩니다.

자동설치를구현하기위한필수구성요소:

- iOS 의경우관리되는 iOS 장치를감독모드로전환합니다. 자세한내용은 iOS 및 macOS 프로필장치정책가져오기를참조하십시오.
- Android Enterprise 경우앱이장치의 Android 작업프로필에설치됩니다. 자세한내용은 Android Enterprise를참조하십시오.
- Samsung 장치의경우장치에서 Samsung Knox 를사용합니다.

  이작업을수행하려면 Samsung MDM 라이센스키장치정책을설정하여 Samsung ELM 및 Knox 라이센스키를생성합니다. 자세한내용은 Samsung MDM 라이센스키장치정책을참조하십시오.

필수앱과선택적앱정보

배달그룹에앱을추가하는경우선택적앱인지, 아니면필수앱인지를선택해야합니다. Citrix 에서는앱을 필수로배포하기를권장합니다.

- 필수앱은사용자장치에자동으로설치되므로상호작용이최소화됩니다. 이러한기능을사용하면앱을자동으로업데이트할수도있습니다.
- 옵션앱을통해사용자는설치할앱을선택할수있지만사용자는 Secure Hub 를통해수동으로설치를개시해야합니다.

필수로표시된앱의경우사용자는다음과같은경우에곧바로업데이트를받을수있습니다.

- 사용자가새앱을업로드하고필수앱으로표시합니다.
- 사용자가기존앱을필수앱으로표시합니다.
- 사용자가필수앱을삭제합니다.
- Secure Hub 업데이트가제공됩니다.

필수앱의강제배포를위한요구사항

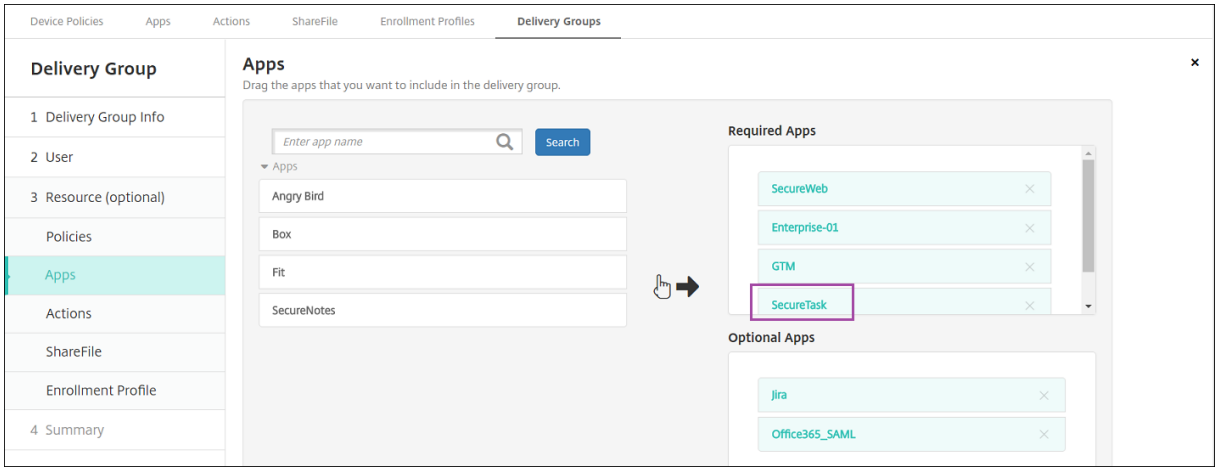
- XenMobile Server 10.6(최소버전)

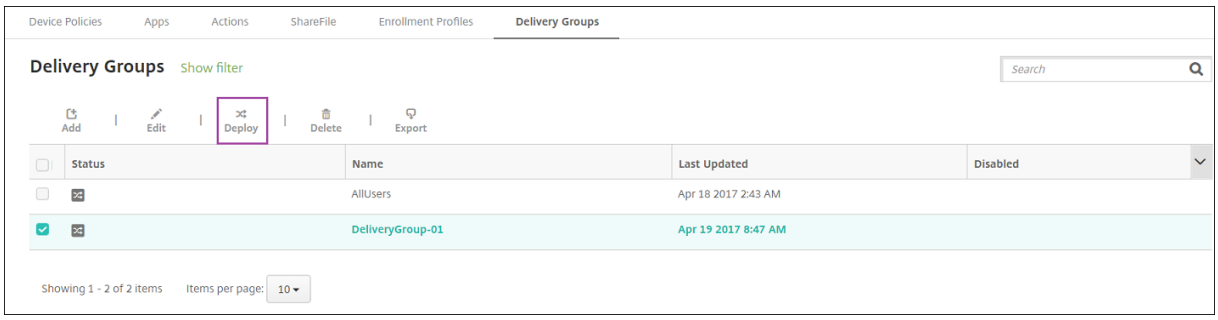
- Secure Hub 10.5.15(iOS 의경우) 및 10.5.20(Android 의경우)(최소버전)
- MAM SDK 또는 MDX Toolkit 10.6(최소버전)
- 사용자지정서버속성, force.server.push.required.apps.

  필수앱의강제배포가기본적으로사용되지않도록설정됩니다. 이기능을사용하도록설정하려면사용자지정키서버속성을만드십시오. 키및 표시이름을 **force.server.push.required.apps** 로설정하고 값을 **true** 로설정합니다.
- XenMobile Server 및 Secure Hub 업그레이드후: 등록된장치가있는사용자는로그오프후 Secure Hub 에로그온하여필수앱배포업데이트를받아야합니다.

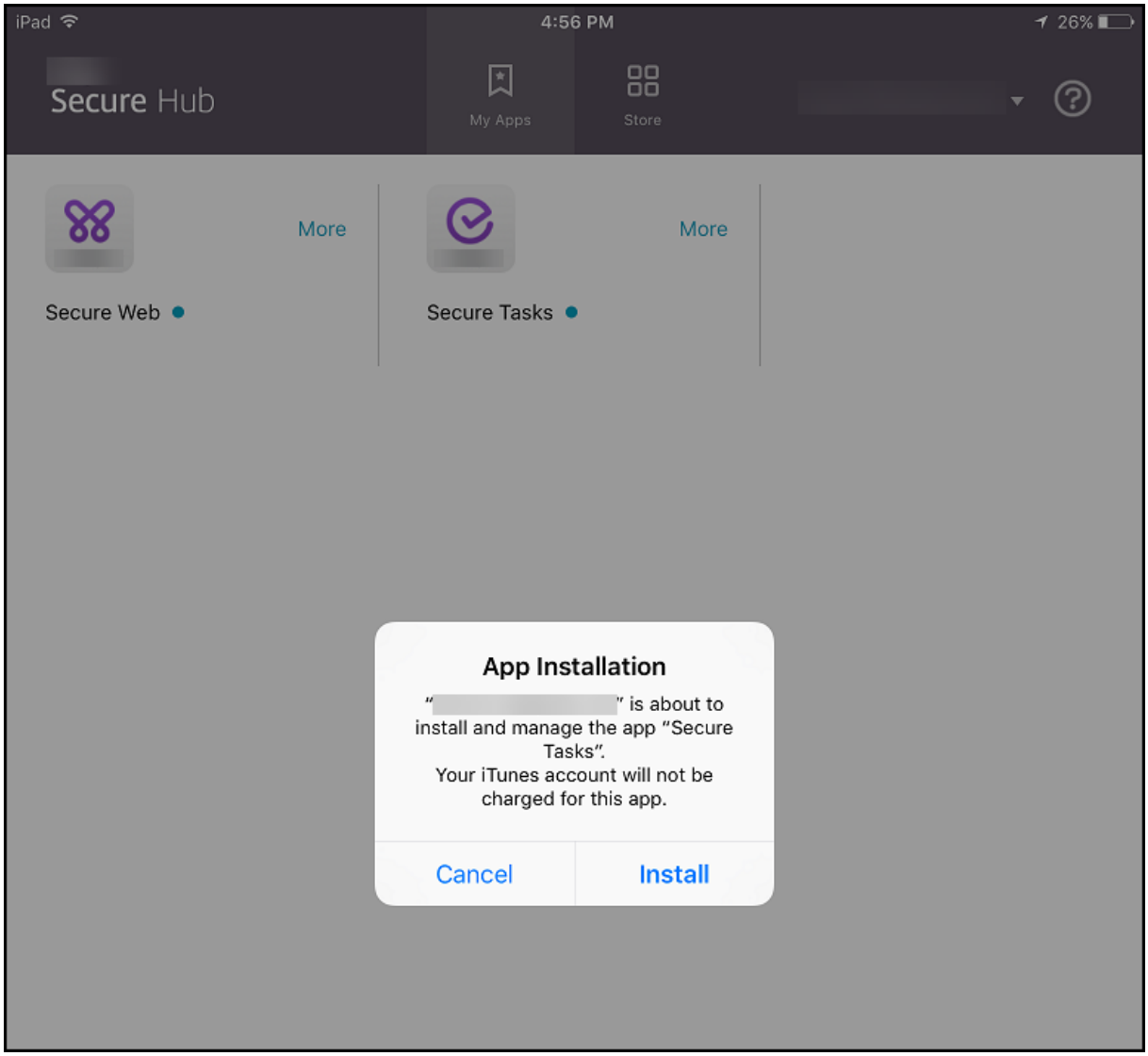
예제

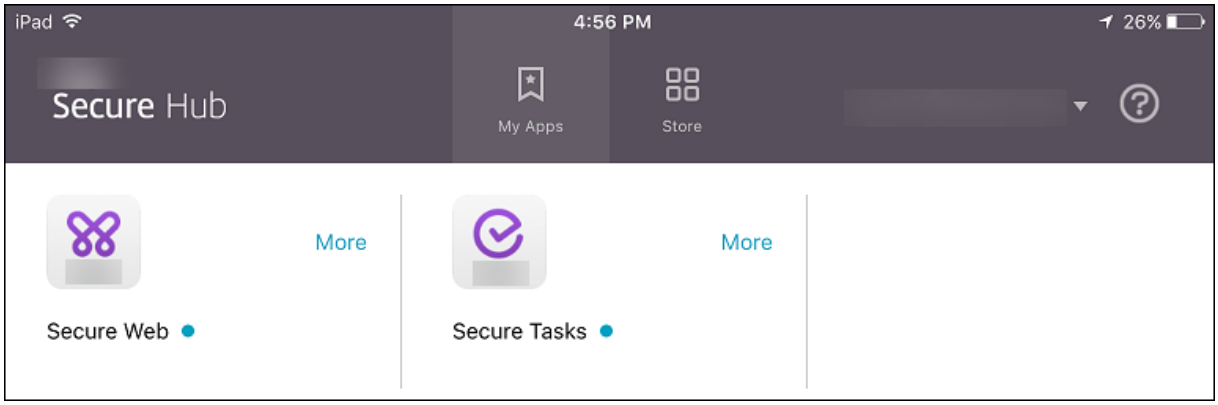
다음예제에는 Secure Tasks 로명명된앱을배달그룹에추가한후배달그룹을배포하는작업의순서가나와있습니다.





샘플앱인 Secure Tasks 가사용자장치에배포되면 Secure Hub 가앱을설치하라는메시지를표시합니다.





> 중요:
>
> 엔터프라이즈앱및공용앱스토어앱을포함한 MDX 지원필수앱이즉시업그레이드됩니다. 관리자가앱업데이트유예기간에대한 MDX 정책을구성하고사용자가앱을나중에업그레이드하도록선택하는경우에도업그레이드가수행됩니다.

엔터프라이즈및공용스토어앱을위한 **iOS** 필수앱워크플로

1. 초기등록중에 XenMobile App 을배포합니다. 필수앱이장치에설치됩니다.
2. XenMobile 콘솔에서앱을업데이트합니다.
3. XenMobile 콘솔에서필수앱을배포합니다.
4. 홈화면의앱이업데이트됩니다. 또한공용스토어앱의경우업그레이드가자동으로시작됩니다. 사용자에게업데이트하라는메시지가표시되지않습니다.
5. 사용자가홈화면에서앱을엽니다. 앱업데이트유예기간을설정했더라도사용자가나중에앱을업그레이드하기위해누르면앱이곧바로업그레이드됩니다.

엔터프라이즈앱을위한 **Android** 필수앱워크플로

1. 초기등록중에 XenMobile App 을배포합니다. 필수앱이장치에설치됩니다.
2. XenMobile 콘솔에서필수앱을배포합니다.
3. 앱이업그레이드됩니다. (Nexus 장치에서는업데이트를설치하라는메시지가표시되지만 Samsung 장치에서는자동설치됩니다.)
4. 사용자가홈화면에서앱을엽니다. 앱업데이트유예기간을설정했더라도사용자가나중에앱을업그레이드하기위해누르면앱이곧바로업그레이드됩니다. (Samsung 장치에서는자동설치가수행됩니다.)

공용스토어앱을위한 **Android** 필수앱워크플로

1. 초기등록중에 XenMobile App 을배포합니다. 필수앱이장치에설치됩니다.
2. XenMobile 콘솔에서앱을업데이트합니다.
3. XenMobile 콘솔에서필수앱을배포합니다. 또는장치에서 Secure Hub 스토어를엽니다. 스토어에업데이트아이콘이나타납니다.
4. 앱업그레이드가자동으로시작됩니다. (Nexus 장치에서는업데이트를설치하라는메시지가표시됩니다.)
5. 홈화면에서앱을엽니다. 앱이업그레이드됩니다. 유예기간동안사용자에게메시지가표시되지않습니다. (Samsung 장치에서는자동설치가수행됩니다.)

앱이구성되어있는경우필요에따라앱제거

사용자가구성된앱을필요에따라제거하도록허용할수있습니다. 구성 **>** 배달그룹으로이동하여앱을 필수앱에서 선택적앱으로옮깁니다.

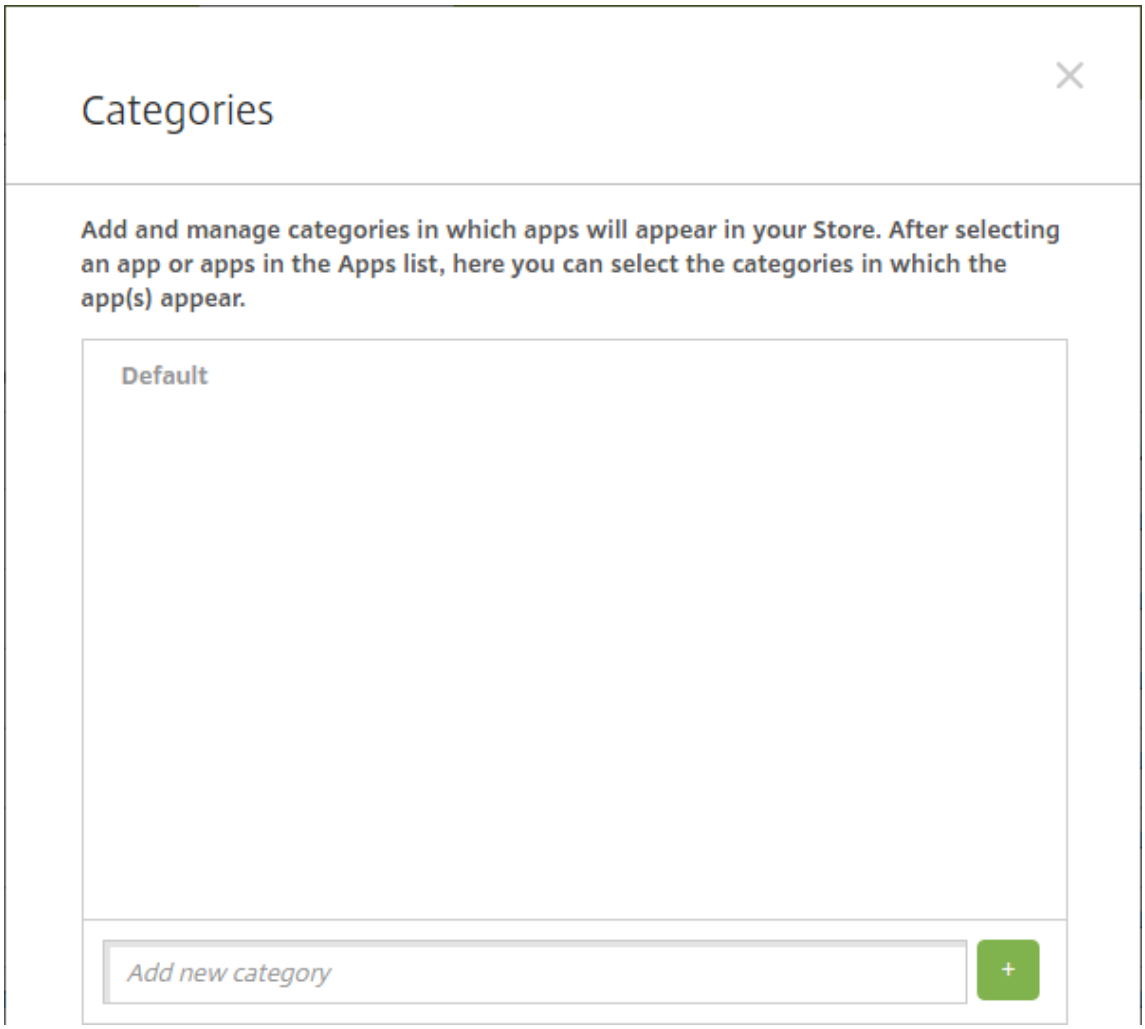
권장사항**:** 특정사용자가앱을제거할수있도록특수배달그룹을사용하여앱을선택사항으로잠시변경합니다. 그러면기존필수앱을선택사항으로변경하고해당배달그룹으로앱을배포한다음장치에서앱을제거할수있습니다. 이후향후해당배달그룹등록에앱이필요하도록하려면다시앱을필수로설정하면됩니다.

앱범주정보

사용자가 Secure Hub 에로그온하면 XenMobile 에서설정한앱, 웹링크및스토어목록이표시됩니다. 앱범주를사용하면사용자가액세스할수있는특정앱, 스토어또는웹링크를지정할수있습니다. 예를들어재무범주를만든후재무와관련된앱만범주에추가할수있습니다. 또는영업범주를구성하여영업앱을할당할수있습니다.

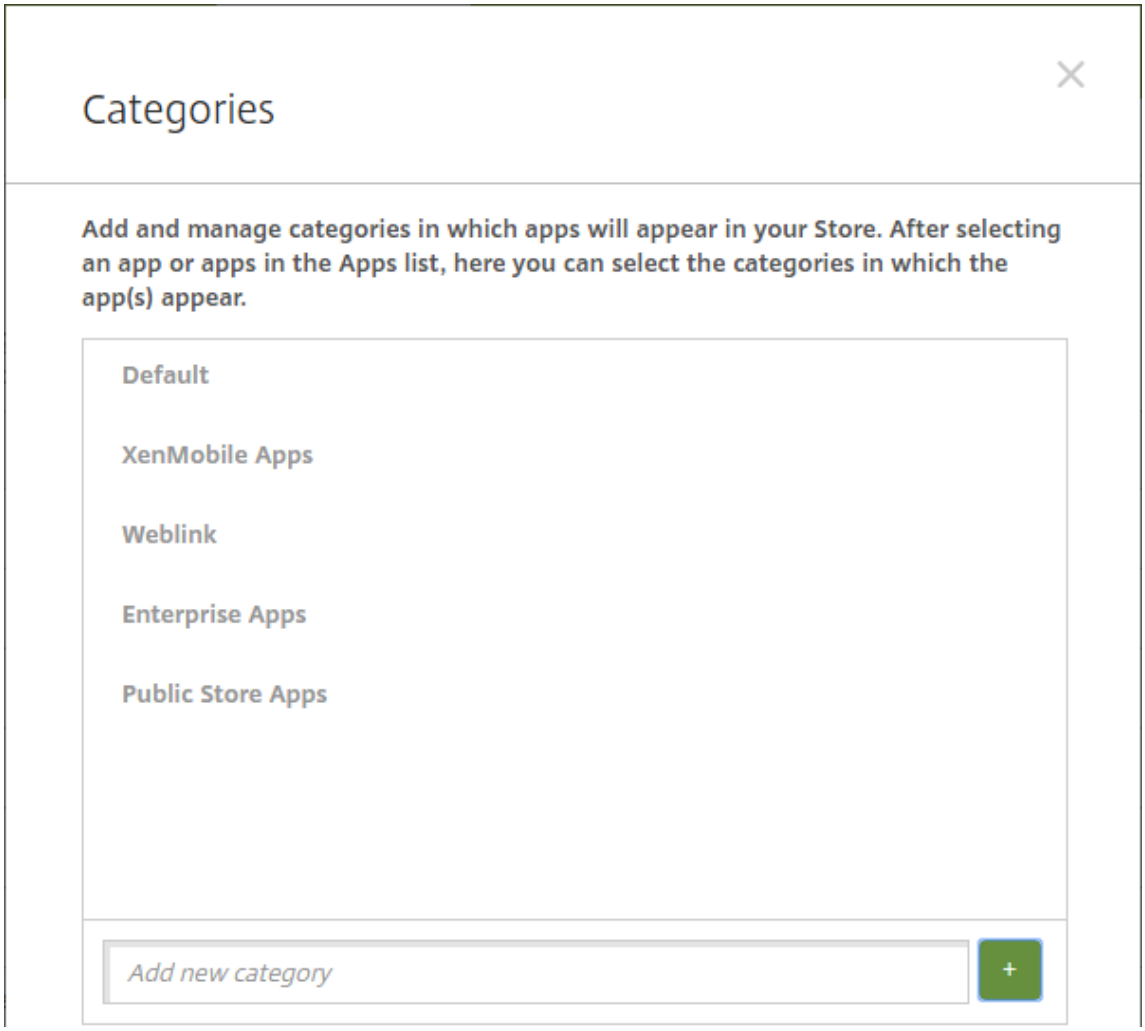
앱, 웹링크또는스토어를추가하거나편집할때이전에구성한하나이상의범주에앱을추가할수있습니다.

1. XenMobile 콘솔에서 구성 **>** 앱 **>** 범주를클릭합니다. 범주대화상자가나타납니다.



2. 추가할각범주에대해다음을수행합니다.

   - 대화상자의맨아래쪽에있는 새범주추가필드에추가할범주의이름을입력합니다. 예를들어엔터프라이즈앱에대한범주를만들려는경우엔터프라이즈앱을입력할수있습니다.
   - 더하기기호 (+) 를클릭하여범주를추가합니다. 새로만들어진범주가추가되고 범주대화상자에표시됩니다.



3. 범주추가가완료되면 범주대화상자를닫습니다.
4. 앱페이지에서기존앱을새범주에배치할수있습니다.
   - 범주로분류할앱을선택합니다.
   - 편집을클릭합니다. 앱정보페이지가나타납니다.
   - 앱범주목록에서범주확인란을선택하여새범주를적용합니다. 앱에적용하지않을기존범주에대한확인란을선택취소합니다.
   - 배달그룹할당탭을클릭하거나다음페이지에서 다음을클릭하여나머지앱설정페이지단계를이동합니다.
   - 배달그룹할당페이지에서 저장을클릭하여새범주를적용합니다. 새범주가앱에적용되고 앱테이블에표시됩니다.

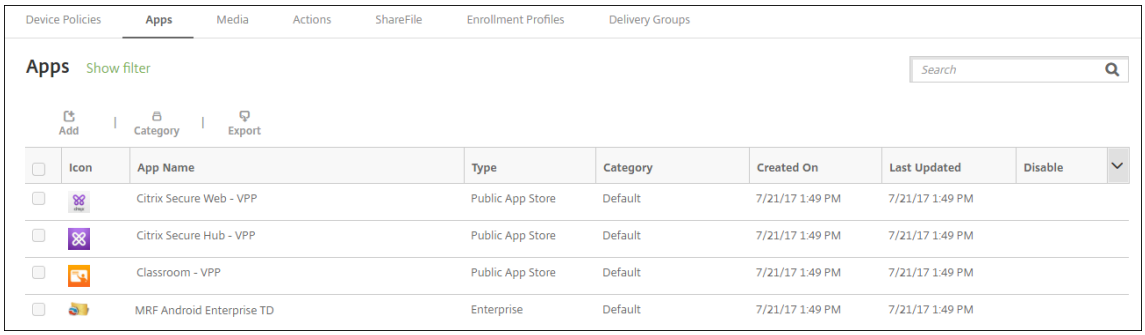
MDX 앱추가

iOS 또는 Android 앱에서사용할수있는 MDX 파일을받으면앱을 XenMobile 에업로드할수있습니다. 앱을업로드한후앱세부정보및정책설정을구성할수있습니다. 각장치플랫폼유형에사용할수있는앱정책에대한자세한내용은다음을참조하십시오.

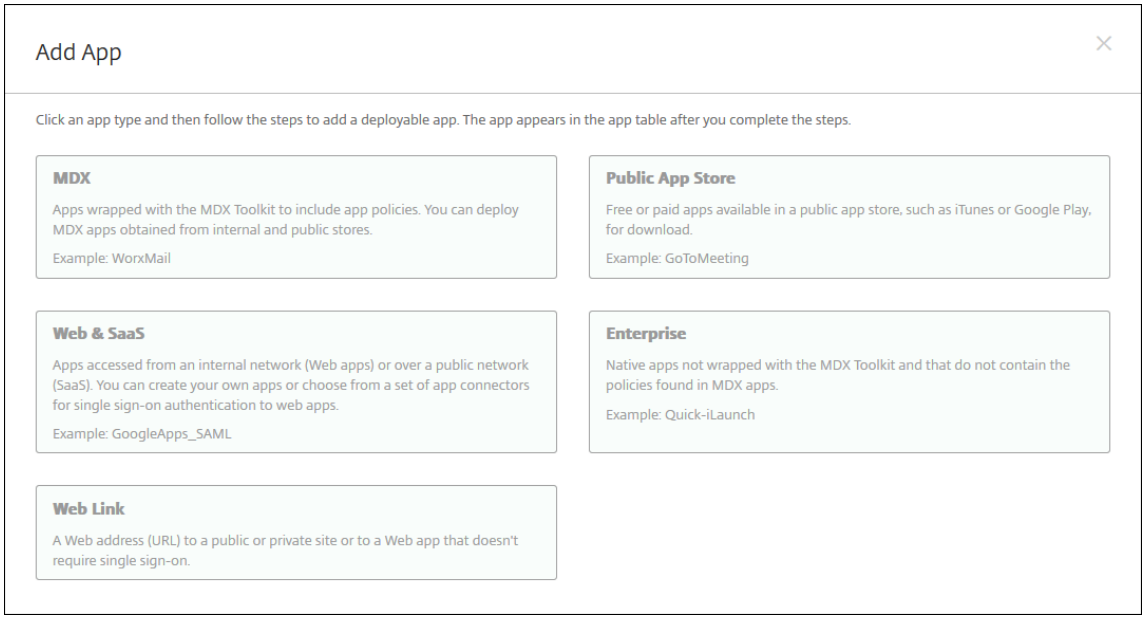
- MAM SDK Overview(MAM SDK 개요)

- MDX 정책요약

1. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 앱페이지가나타납니다.



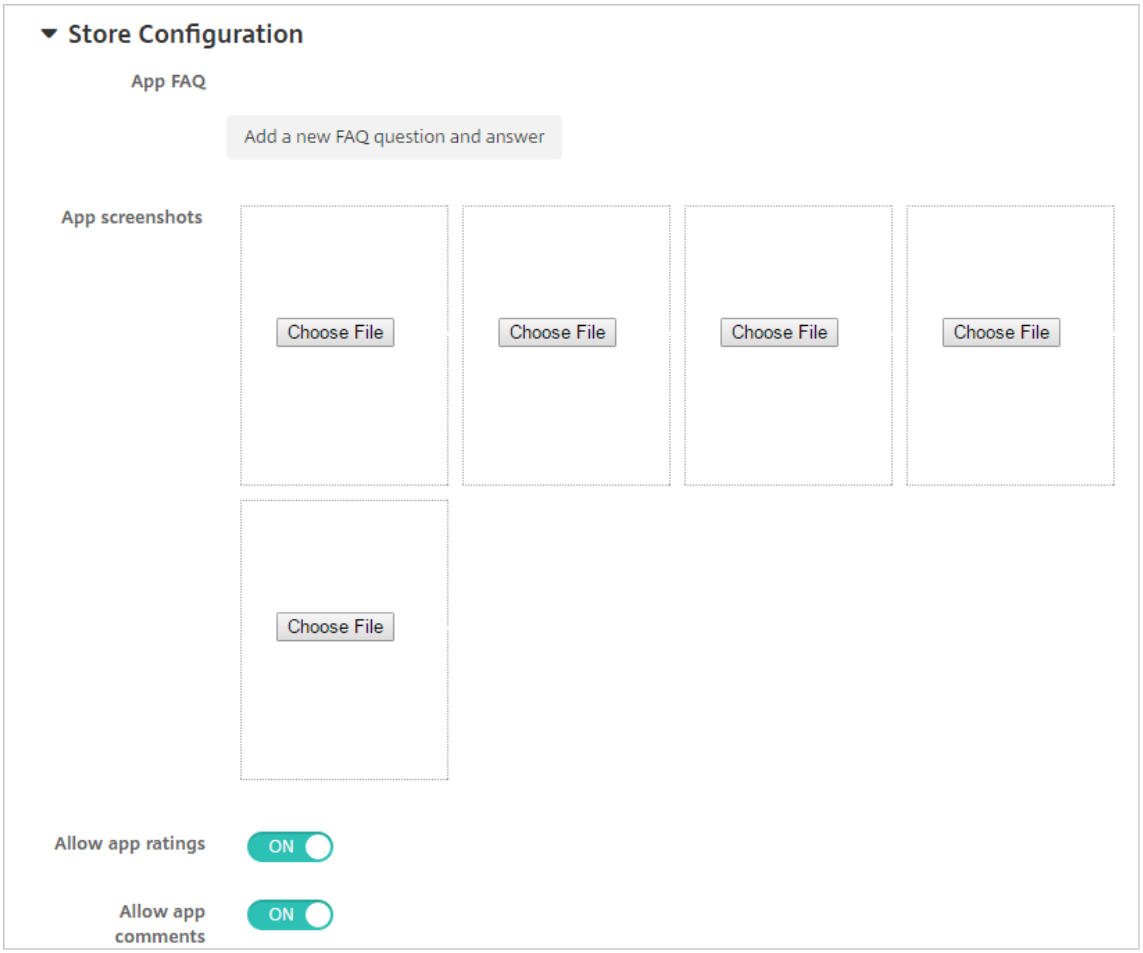
2. 추가를클릭합니다. 앱추가대화상자가나타납니다.



3. **MDX** 를클릭합니다. **MDX** 앱정보페이지가나타납니다.
4. 앱정보창에서다음정보를입력합니다.
   - 이름**:** 앱을설명하는이름을입력합니다. 이이름은 앱테이블의 앱이름아래에표시됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은앱범주정보를참조하십시오.
5. 다음을클릭합니다. 앱플랫폼페이지가나타납니다.
6. 플랫폼아래에서추가할플랫폼을선택합니다. 하나의플랫폼에대해서만구성하는경우다른플랫폼의선택을취소합니다.
7. 업로드할 MDX 파일을선택하려면 업로드를클릭하고파일의위치로이동합니다.
8. 앱정보페이지에서다음설정을구성합니다.
   - 파일이름**:** 앱에연결된파일이름을입력합니다.

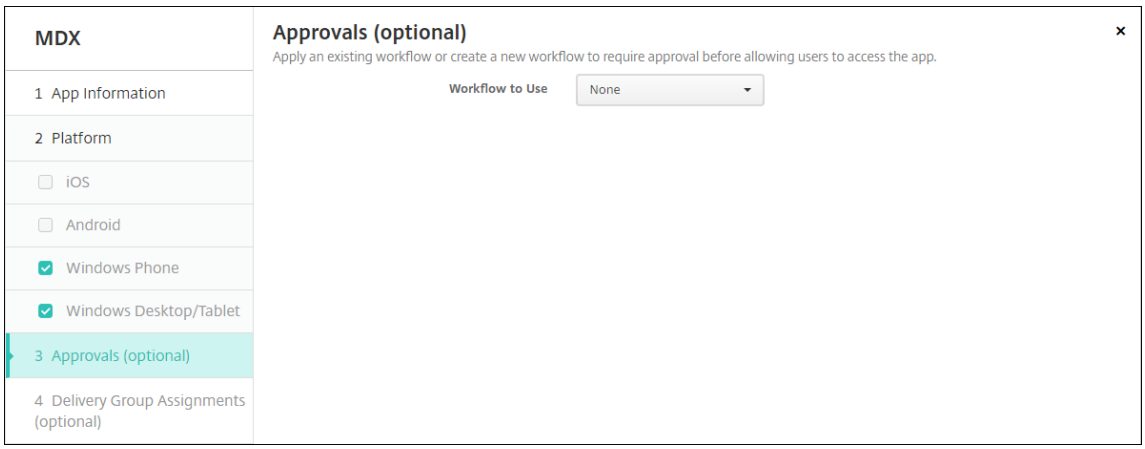
- 앱설명**:** 앱에대한설명을입력합니다.
- 앱버전**:** 필요한경우앱버전번호를입력합니다.
- 패키지 **ID:** 관리되는 Google Play 스토어에서가져온앱의패키지 ID 를입력합니다.
- 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
- 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
- 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.
- **MDM** 프로필이제거된경우앱제거**:** MDM 프로필이제거된경우 iOS 장치에서앱을제거할지여부를선택합니다. 기본값은 켜짐입니다.
- 앱데이터백업방지**:** 사용자가 iOS 장치에서앱데이터를백업하는것을방지할지여부를선택합니다. 기본값은 켜짐입니다.
- 제품트랙**:** iOS 장치로푸시할제품트랙을지정합니다. 테스트용으로설계된추적이있는경우해당추적을선택하여사용자에게할당할수있습니다. 기본값은 프로덕션입니다.
- 강제로앱관리**:** 관리되지않는앱으로설치한앱의경우감독되지않는 iOS 장치에서해당앱의관리를허용할것인지묻는메시지를사용자에게표시할지여부를선택합니다. 기본값은 켜짐입니다.
- 볼륨구매를통해배포된앱**:** Apple 볼륨구매를사용하여앱을배포할지여부를선택합니다. 켜짐인경우앱의 MDX 버전을배포하고볼륨구매를사용하여앱을배포하면 Secure Hub 에볼륨구매인스턴스만표시됩니다. 기본값은 꺼짐입니다.

9. **MDX** 정책을구성합니다. MDX 정책은플랫폼별로다르며인증, 장치보안, 앱제한과같은정책영역에대한옵션이포함됩니다. 콘솔에서각정책에는정책을설명하는도구설명이포함됩니다.
10. 배포규칙을구성합니다. 자세한내용은 배포규칙을참조하십시오.
11. 스토어구성을확장합니다.



- 앱 **FAQ:** 새 **FAQ** 질의응답추가를클릭하여앱에대한 FAQ 를만듭니다.
- 휴대폰/태블릿용스크린샷추가**:** 앱스토어에표시할화면캡처를추가합니다.
- 앱평가허용**:** 사용자가앱스토어에서앱을평가하도록허용합니다.
- 앱댓글허용**:** 사용자가앱스토어에서앱에관한댓글을남길수있도록허용합니다.

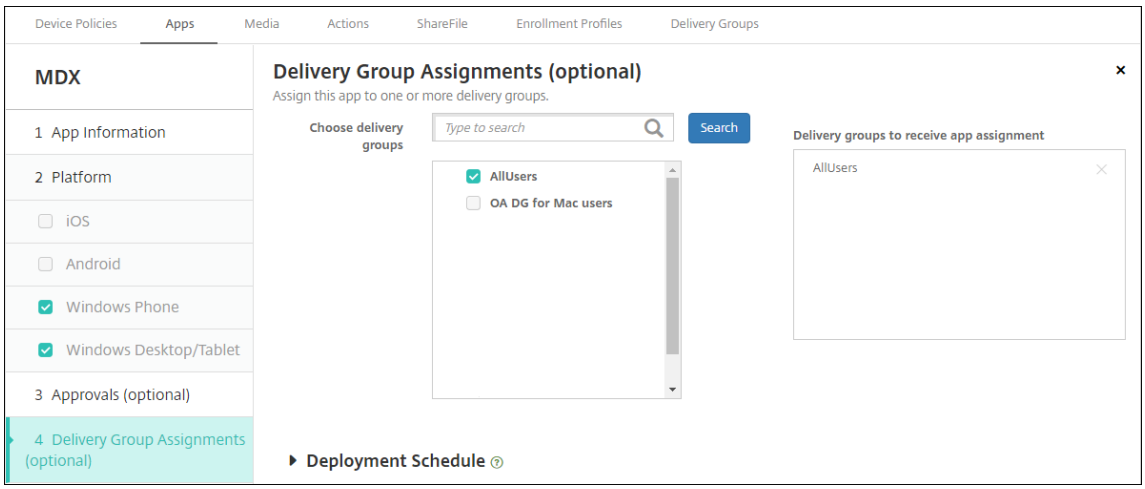
12. 다음을클릭합니다. 승인페이지가나타납니다.



워크플로를사용하여사용자의앱액세스를허용하기전에승인을요구하려면워크플로적용을참조하십시오. 승인워크플로를

설정하지않으려면다음단계로계속진행합니다.

13. 다음을클릭합니다. 배달그룹할당페이지가나타납니다.



14. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.

15. 배포일정을확장하고다음설정을구성합니다.

    - 배포**:** 앱을장치에배포할지여부를선택합니다. 기본값은 켜짐입니다.
    - 배포일정**:** 앱을 지금배포할지 나중에배포할지선택합니다. 나중에를선택할경우앱을배포할날짜와시간을구성합니다. 기본값은 지금입니다.
    - 배포조건**:** 장치를연결할때마다앱을배포하려면 연결할때마다를선택합니다. 장치에서이전에앱을받지못한경우 이전배포가실패한경우에만을선택하여앱을배포합니다. 기본값은 연결할때마다입니다.

    설정 **>** 서버속성에서백그라운드배포예약키를구성한경우 상시연결에대해배포가적용됩니다.

    구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은 상시연결에대해배포를제외하고모든플랫폼에적용됩니다.

16. 저장을클릭합니다.

공용앱스토어앱추가

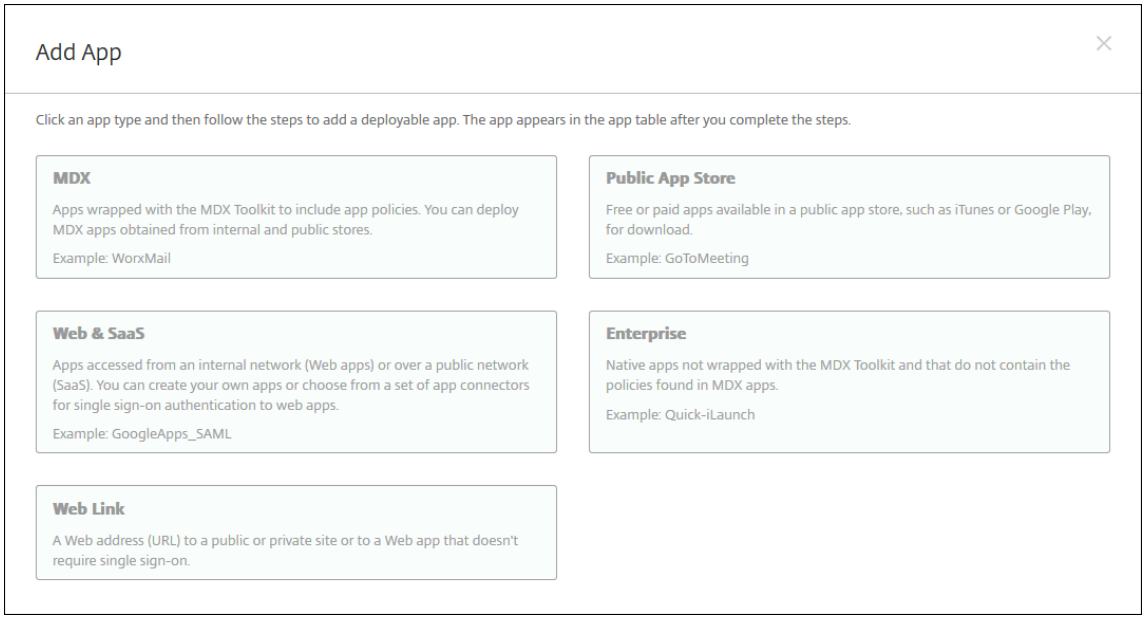
Apple App Store 또는 Google Play 와같은공용앱스토어에서무료또는유료로제공되는앱을 XenMobile 에추가할수있습니다.

Apple App Store 에서앱이름및설명을검색하는설정을구성할수있습니다. 스토어에서앱정보를검색하면 XenMobile 이기존이름과설명을덮어씁니다. Google Play Store 앱정보를수동으로구성합니다.

Android Enterprise 용으로유료공용앱스토어앱을추가할경우대량구매라이센스상태를검토할수있습니다. 이상태는사용가능한총라이센스수, 현재사용중인라이센스수및라이센스를사용하고있는각사용자의전자메일주소입니다. Android Enterprise 의대량구매프로그램은조직의앱및기타데이터를대량으로찾고, 구입하고, 배포하는프로세스를간소화합니다.

앱정보를구성하고앱을전달할플랫폼선택

1. XenMobile 콘솔에서 구성 **>** 앱 **>** 추가를클릭합니다. 앱추가대화상자가나타납니다.



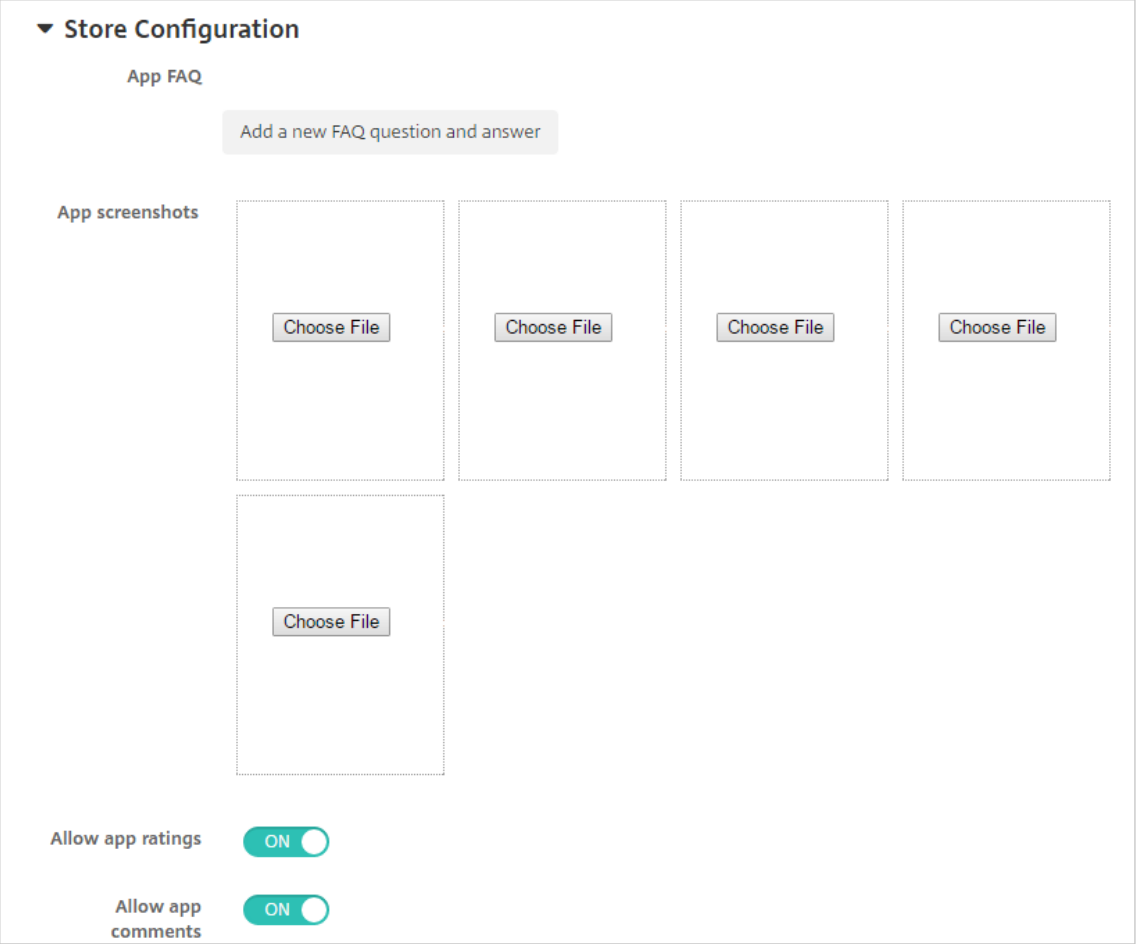
2. 공용앱스토어를클릭합니다. 앱정보페이지가나타납니다.
3. 앱정보창에서다음정보를입력합니다.
   - 이름**:** 앱의설명적이름을입력합니다. 이이름은 앱테이블의 앱이름아래에표시됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은앱범주정보를참조하십시오.
4. 다음을클릭합니다. 앱플랫폼페이지가나타납니다.
5. 플랫폼아래에서추가할플랫폼을선택합니다. 하나의플랫폼에대해서만구성하는경우다른플랫폼의선택을취소합니다.

각플랫폼에대한앱설정을구성합니다. 참조:

- Google Play 앱에대한앱설정구성
- 관리되는앱스토어앱
- iOS 앱에대한앱설정구성

플랫폼설정구성을마치면플랫폼배포규칙을설정하고앱스토어구성을저장합니다.

1. 배포규칙을구성합니다. 자세한내용은 배포규칙을참조하십시오.
2. 스토어구성을확장합니다.



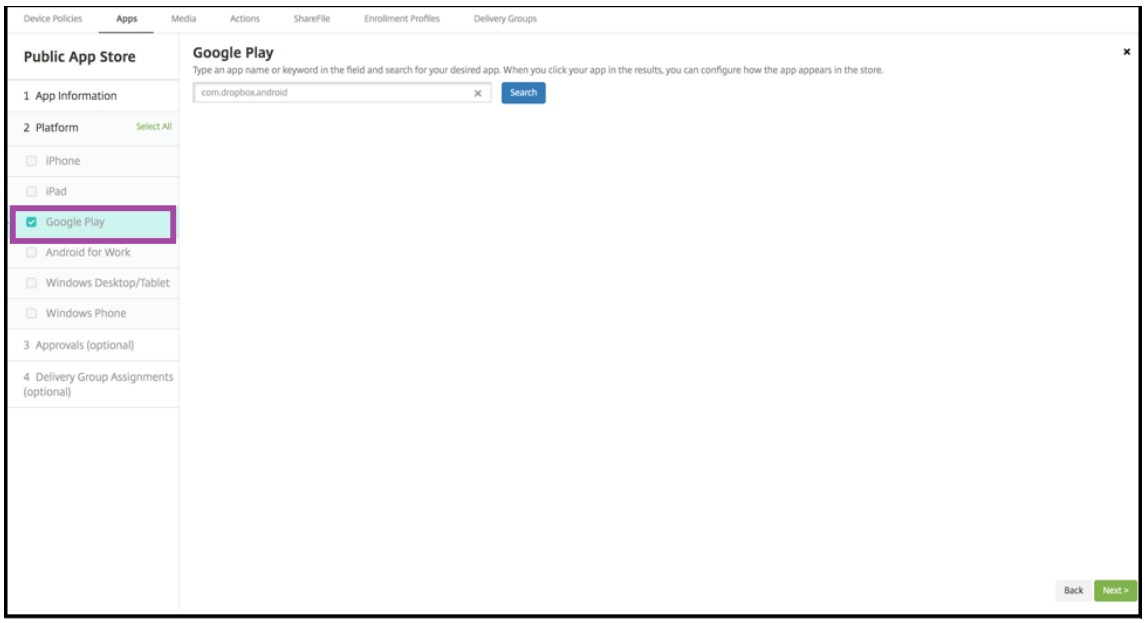
- 앱 **FAQ:** 새 **FAQ** 질의응답추가를클릭하여앱에대한 FAQ 를만듭니다.
- 휴대폰/태블릿용스크린샷추가**:** 앱스토어에표시할화면캡처를추가합니다.
- 앱평가허용**:** 사용자가앱스토어에서앱을평가하도록허용합니다.
- 앱댓글허용**:** 사용자가앱스토어에서앱에관한댓글을남길수있도록허용합니다.

Google Play 앱에대한앱설정구성

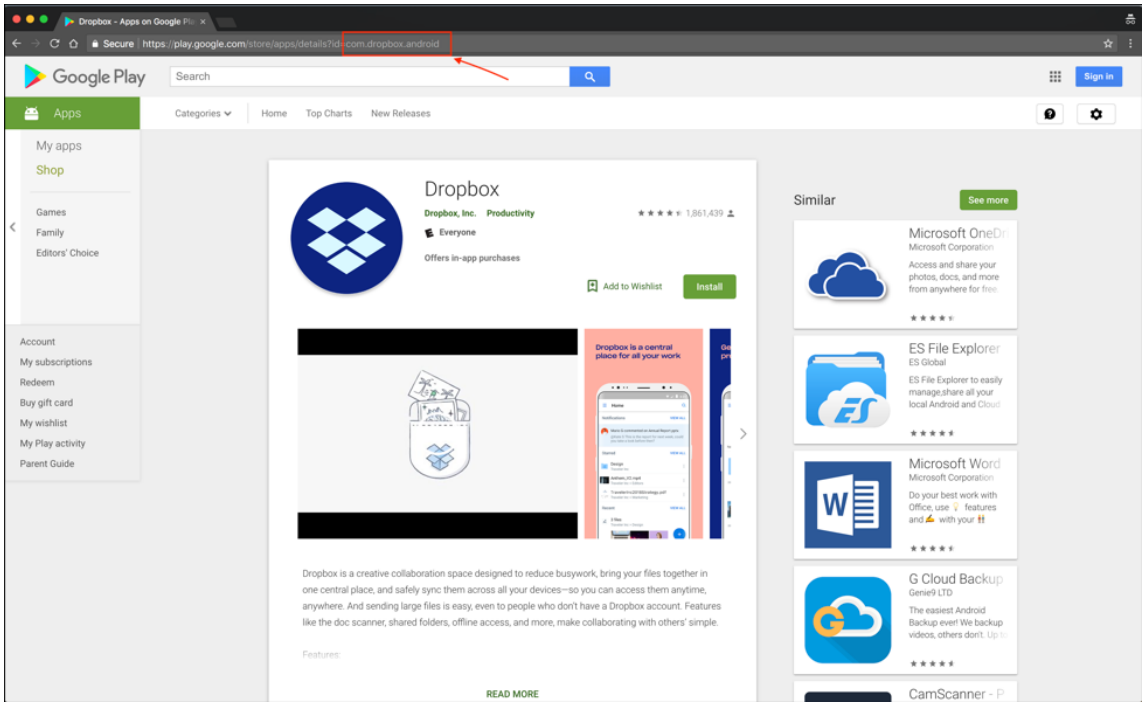
> 참고**:**
>
> 관리되는 Google Play 에서 Google Play Store 의모든앱에액세스하려면 XenMobile 서버속성 관리되는 **Google Play Store** 의모든앱에액세스를사용합니다. 서버속성을참조하십시오. 이속성을 **true** 로설정하면모든 Android Enterprise 사용자에대한공용 Google Play Store 앱이허용됩니다. 이후 제한장치정책을사용하여이러한앱에대한액세스를제어할수있습니다.

Google Play Store 앱설정을구성하려면다른플랫폼과다른단계를수행해야합니다. Google Play Store 앱정보를수동으로구성해야합니다.

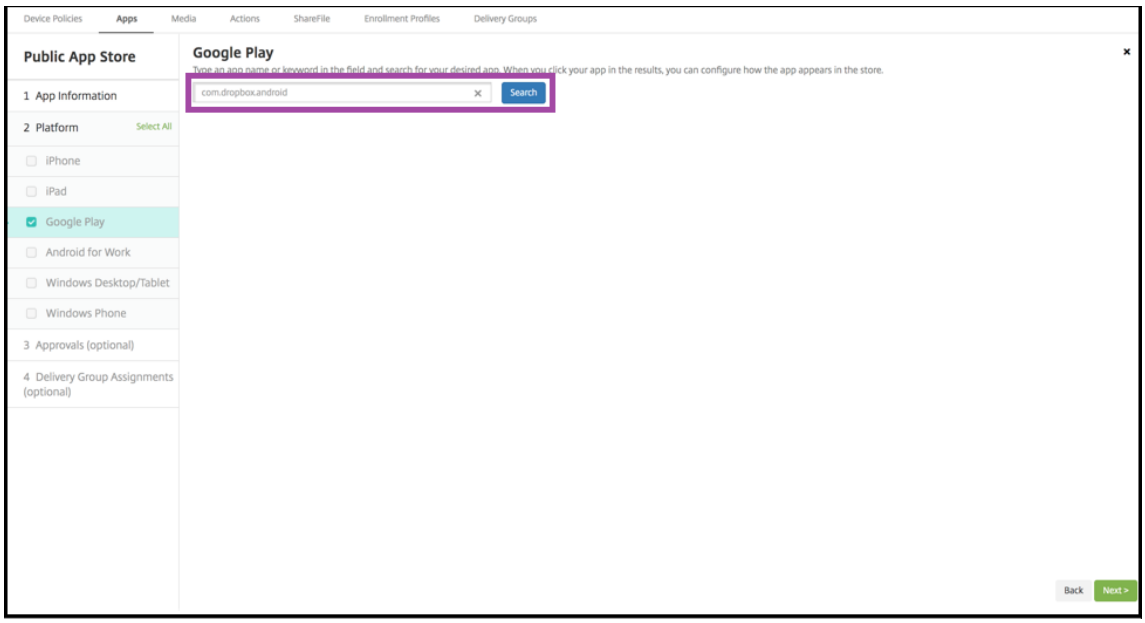
1. 플랫폼에서 **Google Play** 가선택되어있는지확인합니다.



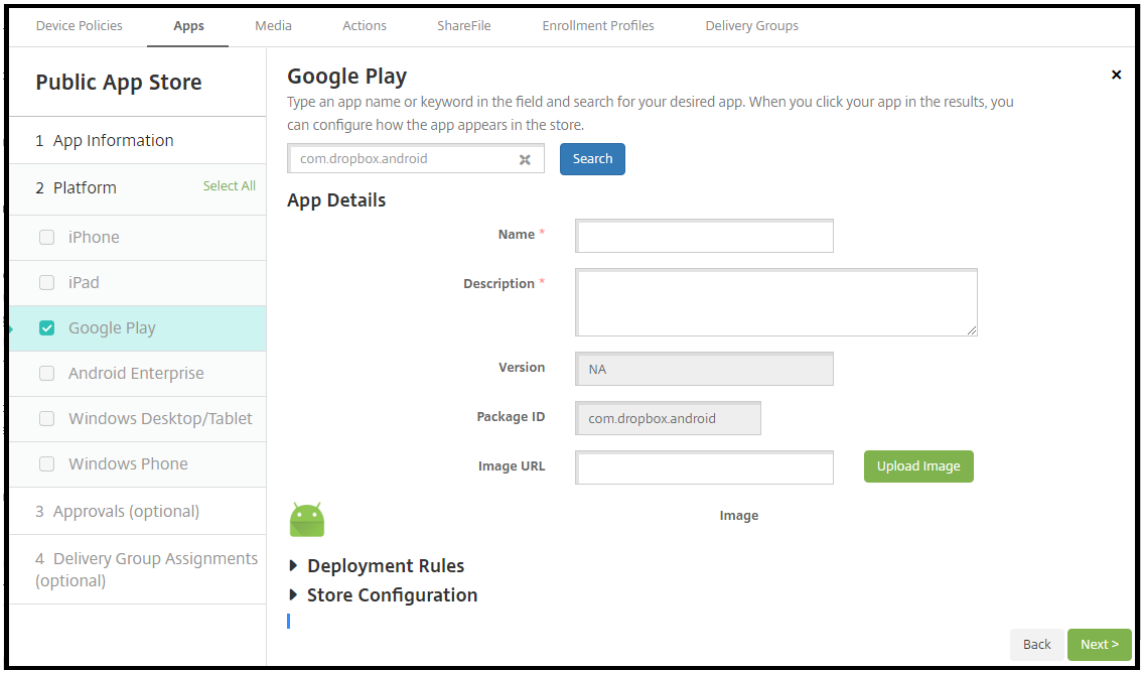
2. Google Play Store 로이동합니다. Google Play Store 에서패키지 ID 를복사합니다. ID 는앱의 URL 에서찾을수 있습니다.



3. XenMobile Server 콘솔에서공용스토어앱을추가할때검색창에패키지 ID 를붙여넣습니다. **Search(**검색**)** 를클릭합니다.



4. 패키지 ID 가유효하면앱세부정보를입력할수있는 UI 가나타납니다.



5. 스토어의앱과함께표시되도록이미지의 URL 을구성할수있습니다. Google Play Store 의이미지를사용하려면:

   a) Google Play Store 로이동합니다. 앱이미지를마우스오른쪽버튼으로클릭하고이미지주소를복사합니다.

   b) **Image URL(**이미지 **URL)** 필드에이미지주소를붙여넣습니다.

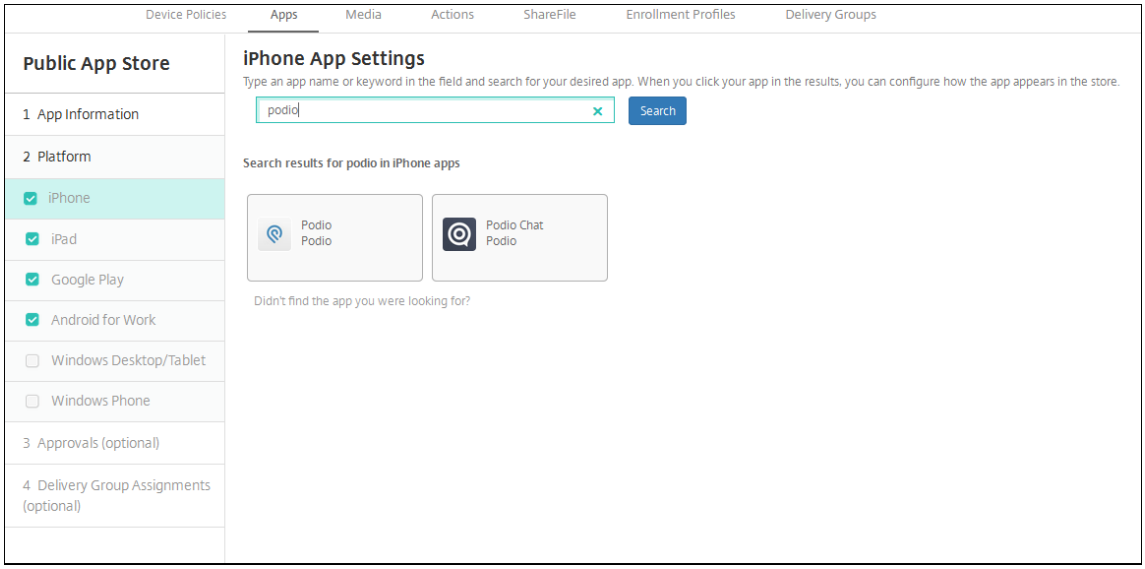
   c) **Upload Image(**이미지업로드**)** 를클릭합니다. **Image(**이미지**)** 옆에이미지가나타납니다.

이미지를구성하지않으면일반 Android 이미지가앱과함께나타납니다.

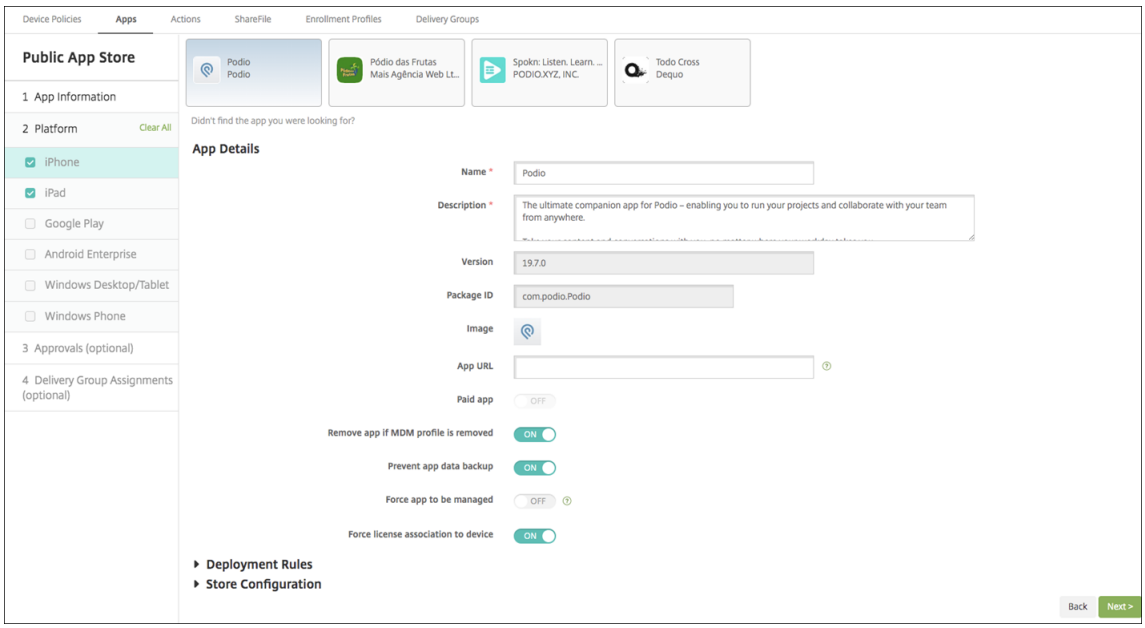
iOS 앱에대한앱설정구성

1. 검색상자에앱이름을입력하고 검색을클릭합니다. 검색기준과일치하는앱이표시됩니다. 검색기준과일치하는앱이표시됩니다.

   다음그림은 iPhone 앱에서 **podio** 에대한검색결과를보여줍니다.



2. 추가할앱을클릭합니다.
3. 선택한앱과관련된정보 (이름, 설명, 버전번호, 관련이미지등) 로 앱세부정보필드가채워집니다.

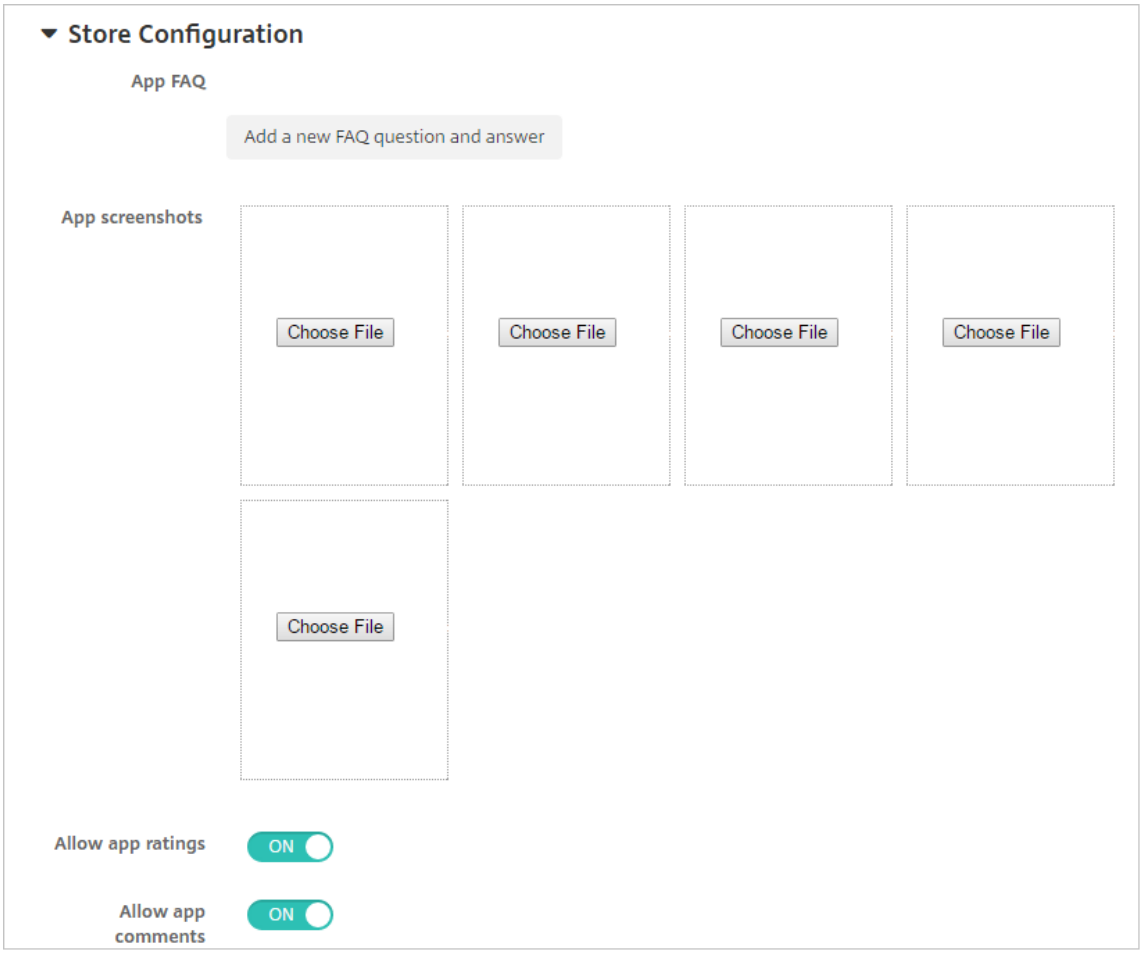


4. 다음설정을구성합니다.

   - 필요한경우앱의이름및설명을변경합니다.
   - 유료앱**:** 이필드는미리구성되며변경할수없습니다.

- **MDM** 프로필이제거된경우앱제거**:** MDM 프로필이제거된경우앱을제거할지여부를선택합니다. 기본값은 켜짐입니다.
- 앱데이터백업방지**:** 앱이데이터를백업하는것을방지할지여부를선택합니다. 기본값은 켜짐입니다.
- 제품트랙**:** 사용자장치로푸시할제품트랙을지정합니다. 테스트용으로설계된추적이있는경우해당추적을선택하여사용자에게할당할수있습니다. 기본값은 프로덕션입니다.
- 강제로앱관리**:** 앱이관리되지않는앱으로설치될경우감독되지않는장치에서해당앱의관리를허용할것인지묻는메시지를표시할지여부를선택합니다. 기본값은 꺼짐입니다. iOS 9.0 이상에서사용할수있습니다.
- 장치에강제로라이센스연결**:** 장치연결을사용하는상태에서개발된앱을사용자가아닌장치에연결할지여부를선택합니다. iOS 9 이상에서사용할수있습니다. 선택한앱이장치할당을지원하지않는경우이필드를변경할수없습니다.

5. 배포규칙을구성합니다. 자세한내용은 배포규칙을참조하십시오.
6. 스토어구성을확장합니다.



- 앱 **FAQ:** 새 **FAQ** 질의응답추가를클릭하여앱에대한 FAQ 를만듭니다.
- 휴대폰/태블릿용스크린샷추가**:** 앱스토어에표시할화면캡처를추가합니다.
- 앱평가허용**:** 사용자가앱스토어에서앱을평가하도록허용합니다.
- 앱댓글허용**:** 사용자가앱스토어에서앱에관한댓글을남길수있도록허용합니다.

7. iPhone 또는 iPad 의경우 볼륨구매를펼칩니다.

a) XenMobile 을사용하여앱에볼륨구매라이센스를적용하려면 볼륨구매라이센스목록에서 볼륨구매라이센스업로드를클릭합니다.

b) 표시되는대화상자에서라이센스를가져옵니다.

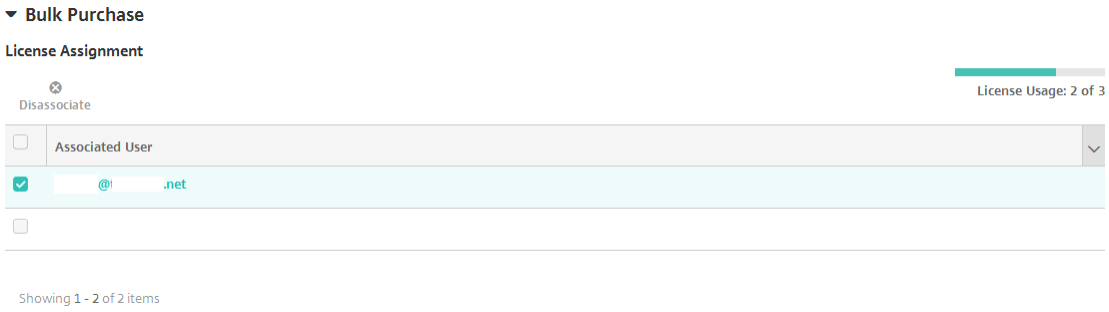
라이센스할당테이블에사용가능한총라이센스수와앱에사용중인라이센스수가표시됩니다.

개별사용자의볼륨구매라이센스연결을해제할수있습니다. 이렇게하면라이센스할당이종료되고라이센스가확보됩니다.

8. Android Enterprise 의경우 대량구매섹션을확장합니다.

라이센스할당테이블에사용가능한총라이센스수와앱에사용중인라이센스수가표시됩니다.

사용자를선택하고 연결해제를클릭하여라이센스할당을종료하고다른사용자를위한라이센스를확보할수있습니다. 그러나 사용자가특정앱이포함된배달그룹에속하지않는경우에만라이센스연결을해제할수있습니다.



9. 볼륨구매또는 대량구매설정을완료한후 다음을클릭합니다. 승인페이지가나타납니다.

워크플로를사용하여사용자의앱액세스를허용하기전에승인을요구하려면워크플로적용을참조하십시오. 승인워크플로가필요하지않은경우다음단계로계속진행합니다.

10. 다음을클릭합니다. 배달그룹할당페이지가나타납니다.

11. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.

12. 배포일정을확장하고다음설정을구성합니다.

- 배포**:** 앱을장치에배포할지여부를선택합니다. 기본값은 켜짐입니다.
- 배포일정**:** 앱을 지금배포할지 나중에배포할지선택합니다. 나중에를선택할경우앱을배포할날짜와시간을구성합니다. 기본값은 지금입니다.
- 배포조건**:** 장치를연결할때마다앱을배포하려면 연결할때마다를선택합니다. 장치에서이전에앱을받지못한경우 이전배포가실패한경우에만을선택하여앱을배포합니다. 기본값은 연결할때마다입니다.

설정 **>** 서버속성에서백그라운드배포예약키를구성한경우 상시연결에대해배포가적용됩니다.

구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은 상시연결에대해배포를제외하고모든플랫폼에적용됩니다.

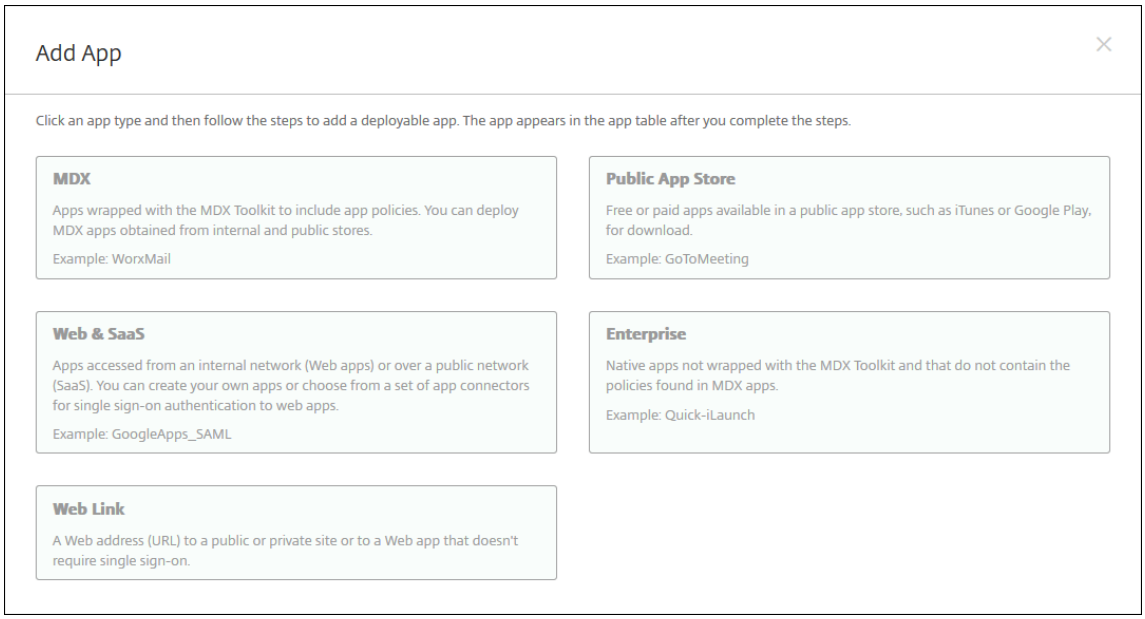
13. 저장을클릭합니다.

웹또는 **SaaS** 앱추가

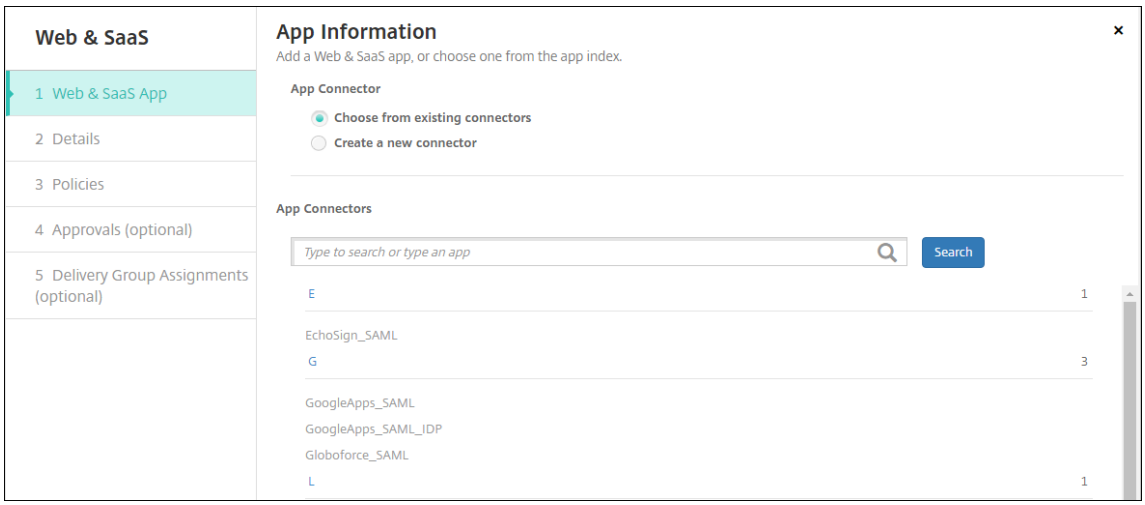
XenMobile 콘솔에서사용자에게모바일, 엔터프라이즈, 웹및 SaaS 앱에대한 SSO(Single Sign-On) 인증을제공할수있습니다. 응용프로그램커넥터템플릿을사용하여앱에서 SSO 를사용하도록할수있습니다. XenMobile 에서제공되는커넥터유형의목록은 앱커넥터유형을참조하십시오. XenMobile 에서웹또는 SaaS 앱을추가할때직접커넥터를만들수도있습니다.

SSO 전용으로제공되는앱의경우설정을저장하면 XenMobile 콘솔의 앱탭에앱이표시됩니다.

1. XenMobile 콘솔에서 구성 **>** 앱 **>** 추가를클릭합니다. 앱추가대화상자가나타납니다.



2. 웹및 **SaaS** 를클릭합니다. 앱정보페이지가나타납니다.



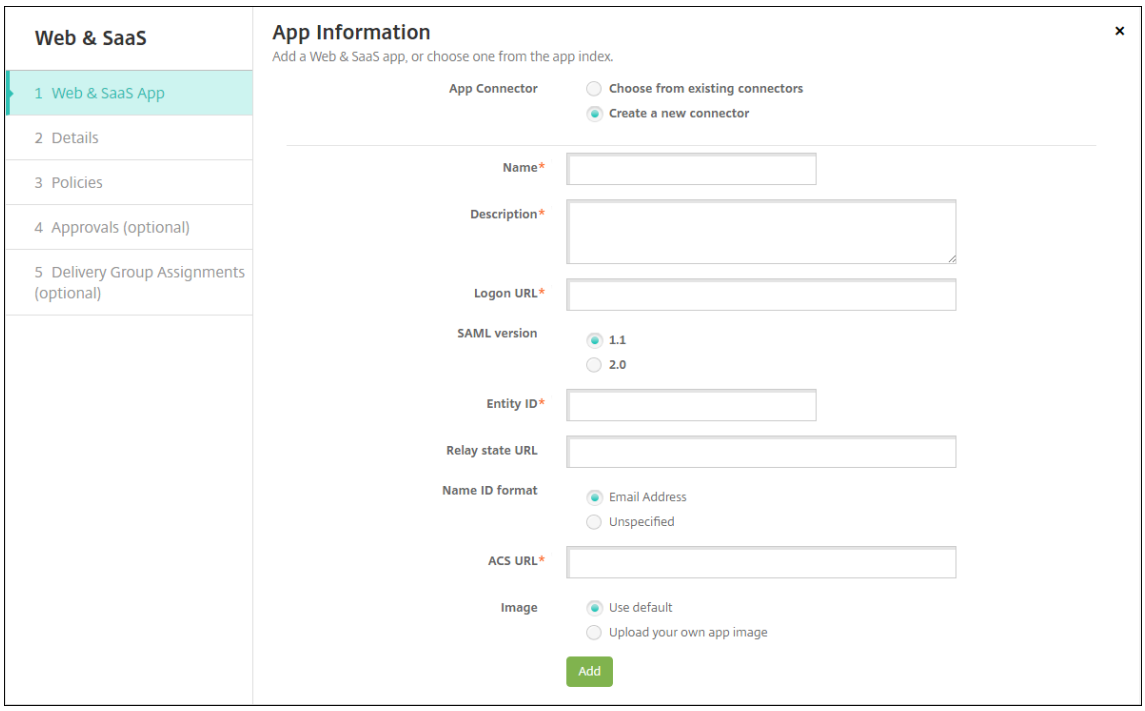
3. 다음과같이기존또는새앱커넥터를구성합니다.

기존앱커넥터를구성하려면

1. 이전에표시된것과같이 앱정보페이지에서 기존커넥터에서선택이이미선택되어있습니다. 앱커넥터목록에서사용할커넥터를클릭합니다. 앱커넥터정보페이지가나타납니다.
2. 다음설정을구성합니다.
   - 앱이름**:** 미리채워진이름을사용하거나새이름을입력합니다.
   - 앱설명**:** 미리채워진설명을사용하거나직접설명을입력합니다.
   - **URL:** 미리채워진 URL 을사용하거나앱의웹주소를입력합니다. 선택한커넥터에따라다음페이지로이동하기전에바꿔야하는자리표시자가이필드에포함될수있습니다.
   - 도메인이름**:** 해당하는경우앱의도메인이름을입력합니다. 이필드는필수입니다.
   - 앱이내부네트워크에서호스트됨**:** 앱이내부네트워크의서버에서실행되는지여부를선택합니다. 원격위치에서내부앱에연결하는사용자의경우 Citrix Gateway 를통해연결해야합니다. 이옵션을 켜짐으로설정하면 VPN 키워드가앱에추가되고사용자가 Citrix 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**):** 목록에서사용자이름규칙에사용할사용자특성의문자수를클릭합니다. 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.

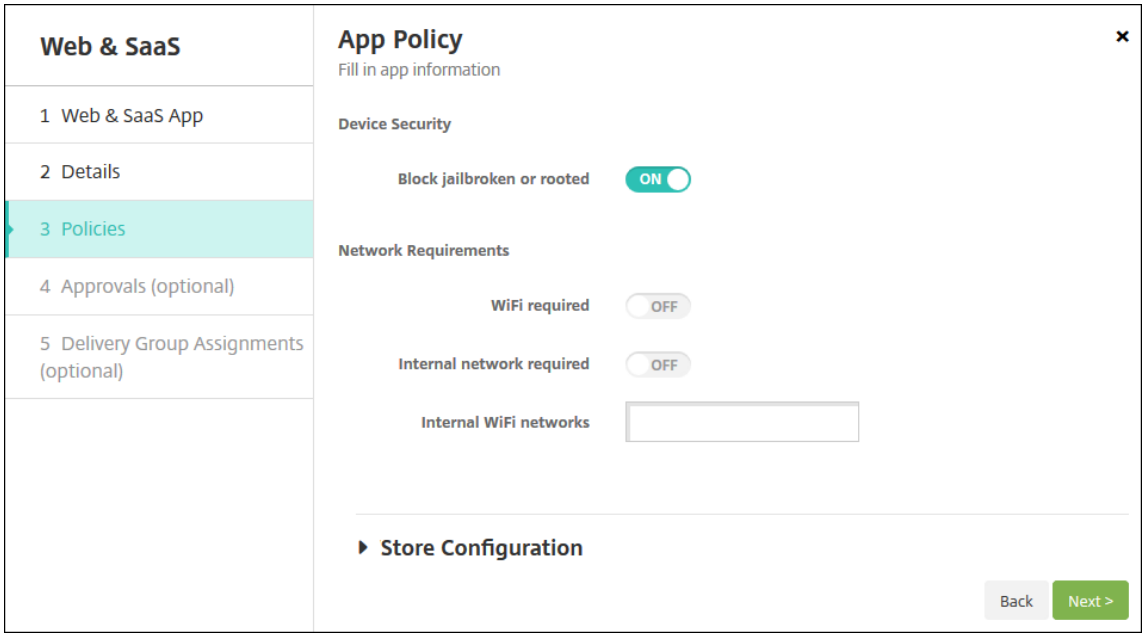


2. 다음설정을구성합니다.

   - 이름**:** 커넥터이름을입력합니다. 이것은필수필드입니다.
   - 설명**:** 커넥터에대한설명을입력합니다. 이것은필수필드입니다.
   - 로그온 **URL:** 사용자가사이트에로그온하는 URL 을입력하거나복사후붙여넣습니다. 예를들어추가하려는앱에로그온페이지가있는경우웹브라우저를열고앱의로그온페이지 (예: `https://www.example.com/logon`) 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, 고유한앱이미지를업로드할지여부를선택합니다. 기본값은기본값사용입니다.
     - 고유한이미지를업로드하려면 찾아보기를클릭하고파일의위치로이동합니다. 파일은.PNG 파일이어야합니다. JPEG 또는 GIF 파일은업로드할수없습니다. 사용자지정그래픽을추가하면나중에변경할수없습니다.

3. 완료되면 추가를클릭합니다. 세부정보페이지가나타납니다.

4. 다음을클릭합니다. 앱정책페이지가나타납니다.

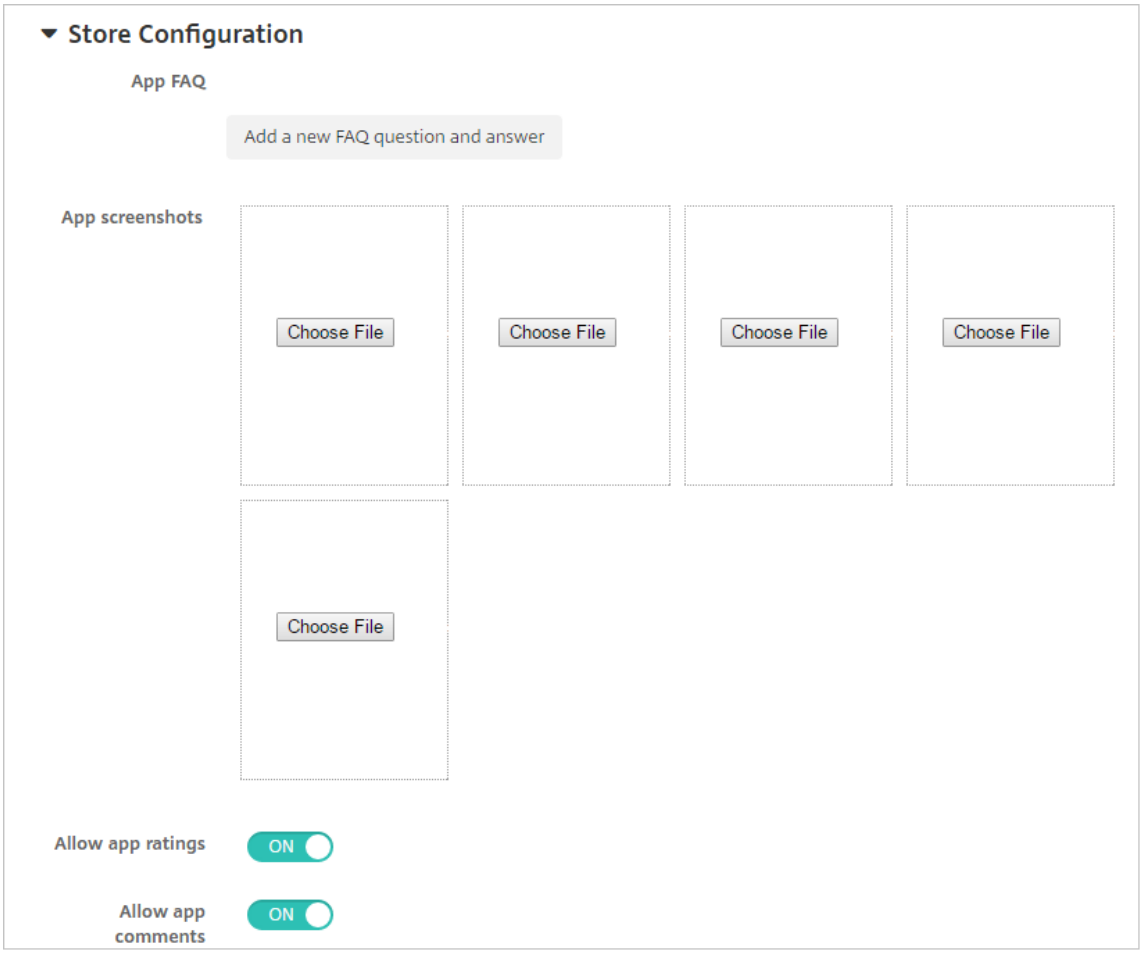


5. 다음설정을구성합니다.

   - 장치보안
   - 탈옥또는루팅차단**:** 탈옥또는루팅장치가앱에액세스하는것을차단할지여부를선택합니다. 기본값은 켜짐입니다.
   - 네트워크요구사항
   - **WiFi** 필요**:** 앱을실행하는데 Wi-Fi 연결이필요한지여부를선택합니다. 기본값은 꺼짐입니다.
   - 내부네트워크필요**:** 앱을실행하는데내부네트워크가필요한지여부를선택합니다. 기본값은 꺼짐입니다.
   - 내부 **WiFi** 네트워크**: Wi-Fi** 필요를사용하는경우사용할내부 Wi-Fi 네트워크를입력합니다.

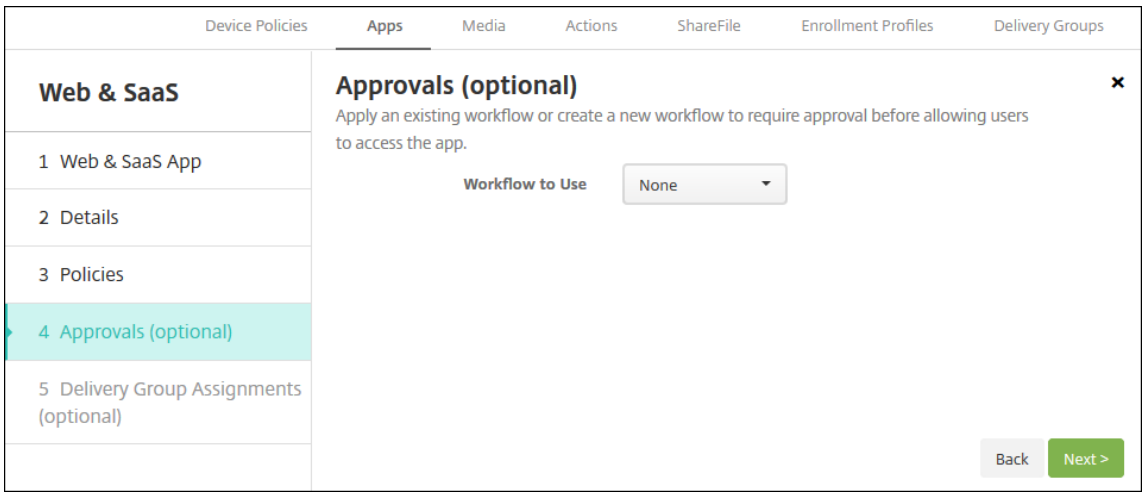
6. 배포규칙을구성합니다. 자세한내용은 배포규칙을참조하십시오.

7. 스토어구성을확장합니다.



- 앱 **FAQ:** 새 **FAQ** 질의응답추가를클릭하여앱에대한 FAQ 를만듭니다.
- 휴대폰/태블릿용스크린샷추가**:** 앱스토어에표시할화면캡처를추가합니다.
- 앱평가허용**:** 사용자가앱스토어에서앱을평가하도록허용합니다.
- 앱댓글허용**:** 사용자가앱스토어에서앱에관한댓글을남길수있도록허용합니다.

8. 다음을클릭합니다. 승인페이지가나타납니다.



워크플로를사용하여사용자의앱액세스를허용하기전에승인을요구하려면워크플로적용을참조하십시오.

9. 다음을클릭합니다. 배달그룹할당페이지가나타납니다.
10. 배달그룹선택옆에서배달그룹을입력하여찾거나그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.
11. 배포일정을확장하고다음설정을구성합니다.

    - 배포**:** 앱을장치에배포할지여부를선택합니다. 기본값은 켜짐입니다.
    - 배포일정**:** 앱을 지금배포할지 나중에배포할지선택합니다. 나중에를선택할경우앱을배포할날짜와시간을구성합니다. 기본값은 지금입니다.
    - 배포조건**:** 장치를연결할때마다앱을배포하려면 연결할때마다를선택합니다. 장치에서이전에앱을받지못한경우 이전배포가실패한경우에만을선택하여앱을배포합니다. 기본값은 연결할때마다입니다.

    설정 **>** 서버속성에서백그라운드배포예약키를구성한경우 상시연결에대해배포가적용됩니다.

    구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은 상시연결에대해배포를제외하고모든플랫폼에적용됩니다.
12. 저장을클릭합니다.

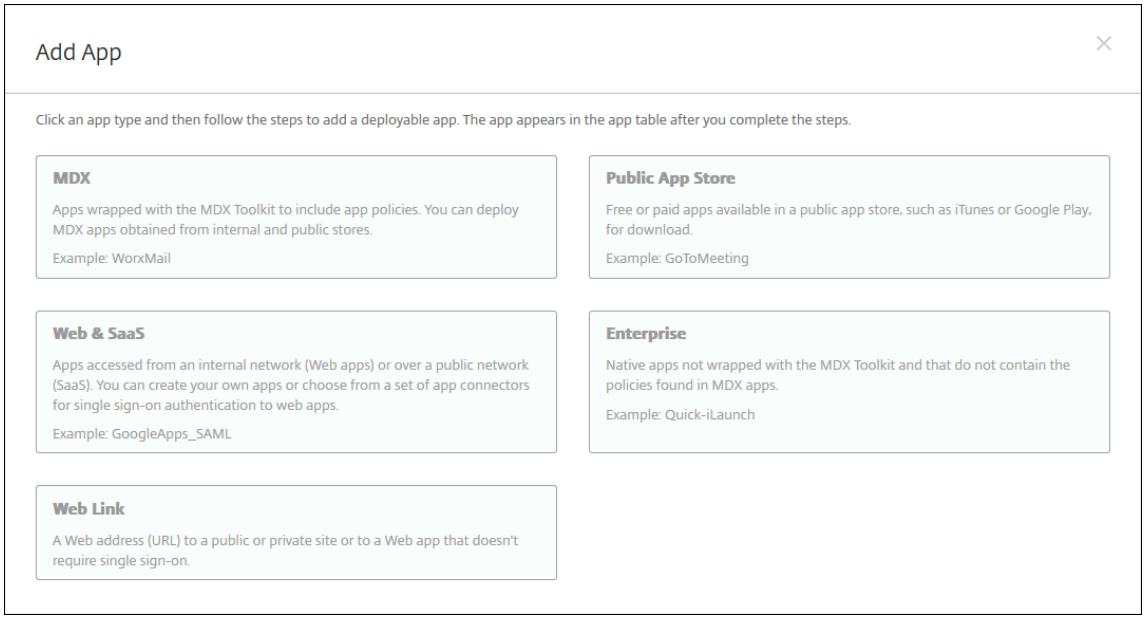
엔터프라이즈앱추가

XenMobile 에서엔터프라이즈앱은 MAM SDK 또는 MDX Toolkit 으로준비되지않은기본앱을나타냅니다. 이러한앱에는 MDX 앱에연결된정책이포함되지않습니다. XenMobile 콘솔의 앱탭에서엔터프라이즈앱을업로드할수있습니다. 엔터프라이즈앱은다음플랫폼 (및해당하는파일형식) 을지원합니다.

- iOS(.ipa 파일)
- Android(.apk 파일)
- Samsung Knox(.apk 파일)
- Android Enterprise(.apk 파일)
- 참고항목: MDX 지원개인앱

Google Play Store 에서엔터프라이즈앱으로다운로드한앱을추가하는작업은지원되지않습니다. 대신, Google Play Store 의앱을공용앱스토어앱으로추가하십시오. 공용앱스토어앱추가를참조하십시오.

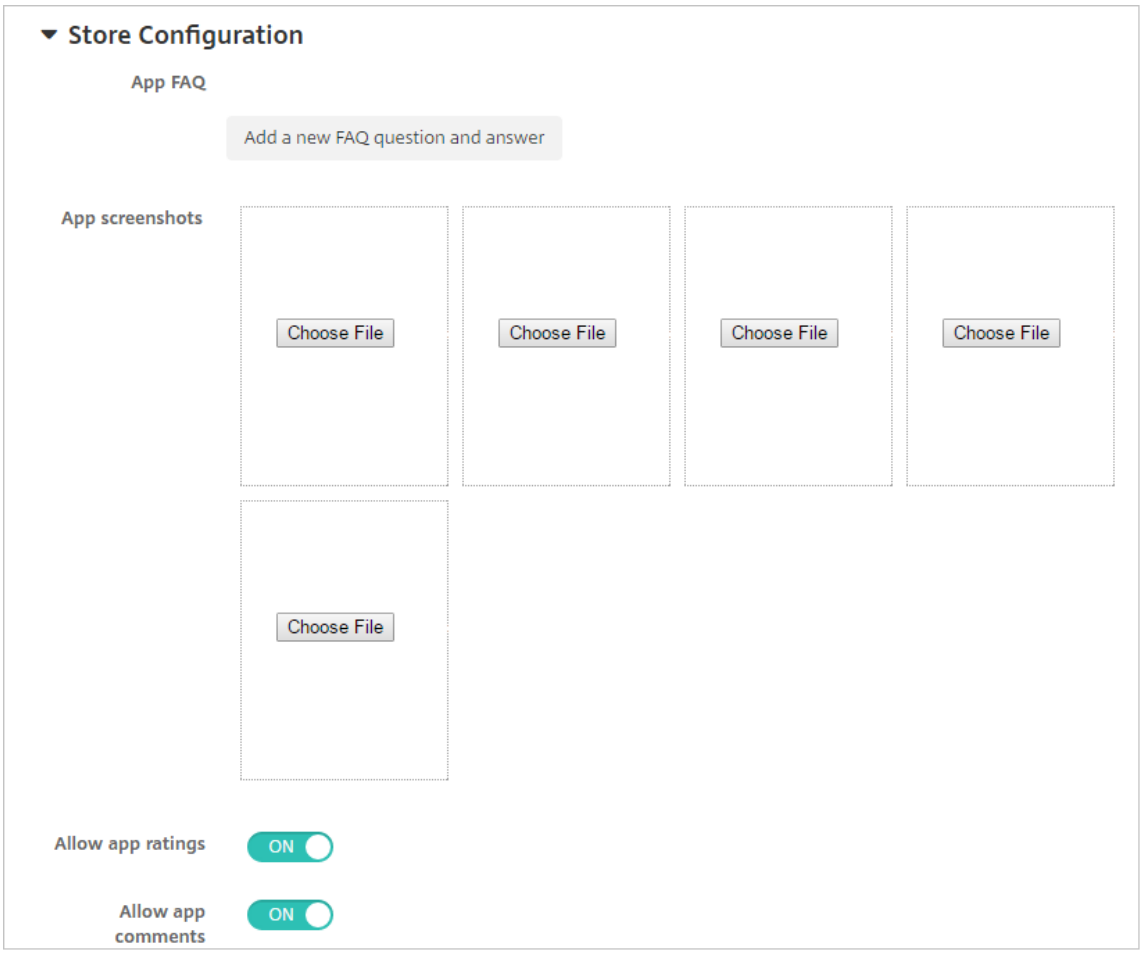
1. XenMobile 콘솔에서 구성 **>** 앱 **>** 추가를클릭합니다. 앱추가대화상자가나타납니다.



2. 엔터프라이즈를클릭합니다. 앱정보페이지가나타납니다.
3. 앱정보창에서다음정보를입력합니다.
   - 이름**:** 앱의설명적이름을입력합니다. 이이름은앱테이블의앱이름아래에나열됩니다.
   - 설명**:** 앱의선택적설명을입력합니다.
   - 앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은앱범주정보를참조하십시오.
4. 다음을클릭합니다. 앱플랫폼페이지가나타납니다.
5. 플랫폼아래에서추가할플랫폼을선택합니다. 하나의플랫폼에대해서만구성하는경우다른플랫폼의선택을취소합니다.
6. 선택한각플랫폼에대해 업로드를클릭하고파일의위치로이동하여업로드할파일을선택합니다.
7. 다음을클릭합니다. 플랫폼에대한앱정보페이지가나타납니다.
8. 다음과같은플랫폼유형에대한설정을구성합니다.
   - 파일이름**:** 필요한경우앱의새이름을입력합니다.
   - 앱설명**:** 필요한경우앱에대한새설명을입력합니다.
   - 앱버전**:** 이필드는변경할수없습니다.
   - 최소 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행할수있는운영체제의가장이전버전을입력합니다.
   - 최대 **OS** 버전**:** 필요한경우장치에서앱을사용할때실행해야하는운영체제의가장최신버전을입력합니다.
   - 제외된장치**:** 필요한경우앱을실행할수없는장치의제조업체또는모델을입력합니다.
   - 패키지 **ID:** 앱의고유식별자입니다.
   - **MDM** 프로필이제거된경우앱제거**:** MDM 프로필이제거된경우장치에서앱을제거할지여부를선택합니다. 기본값은 켜짐입니다.
   - 앱데이터백업방지**:** 앱이데이터를백업하는것을방지할지여부를선택합니다. 기본값은 켜짐입니다.

- 강제로앱관리**:** 관리되지않는앱을설치하는경우감독되지않는장치의사용자에게앱관리를허용하라는메시지를표시하려면 켜짐을선택합니다. 사용자가메시지를수락하면앱이관리됩니다.

9. 배포규칙을구성합니다. 자세한내용은 배포규칙을참조하십시오.
10. 스토어구성을확장합니다.



- 앱 **FAQ:** 새 **FAQ** 질의응답추가를클릭하여앱에대한 FAQ 를만듭니다.
- 휴대폰/태블릿용스크린샷추가**:** 앱스토어에표시할화면캡처를추가합니다.
- 앱평가허용**:** 사용자가앱스토어에서앱을평가하도록허용합니다.
- 앱댓글허용**:** 사용자가앱스토어에서앱에관한댓글을남길수있도록허용합니다.

11. 다음을클릭합니다. 승인페이지가나타납니다.

    워크플로를사용하여사용자의앱액세스를허용하기전에승인을요구하려면워크플로적용을참조하십시오. 승인워크플로가필요하지않은경우다음단계를계속진행합니다.

12. 다음을클릭합니다. 배달그룹할당페이지가나타납니다.
13. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.
14. 배포일정을확장하고다음설정을구성합니다.

- 배포**:** 앱을장치에배포할지여부를선택합니다. 기본값은 켜짐입니다.
- 배포일정**:** 앱을 지금배포할지 나중에배포할지선택합니다. 나중에를선택할경우앱을배포할날짜와시간을구성합니다. 기본값은 지금입니다.
- 배포조건**:** 장치를연결할때마다앱을배포하려면 연결할때마다를선택합니다. 장치에서이전에앱을받지못한경우 이전배포가실패한경우에만을선택하여앱을배포합니다. 기본값은 연결할때마다입니다.

설정 **>** 서버속성에서백그라운드배포예약키를구성한경우 상시연결에대해배포가적용됩니다.

구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은 상시연결에대해배포를제외하고모든플랫폼에적용됩니다.

15. 저장을클릭합니다.

웹링크추가

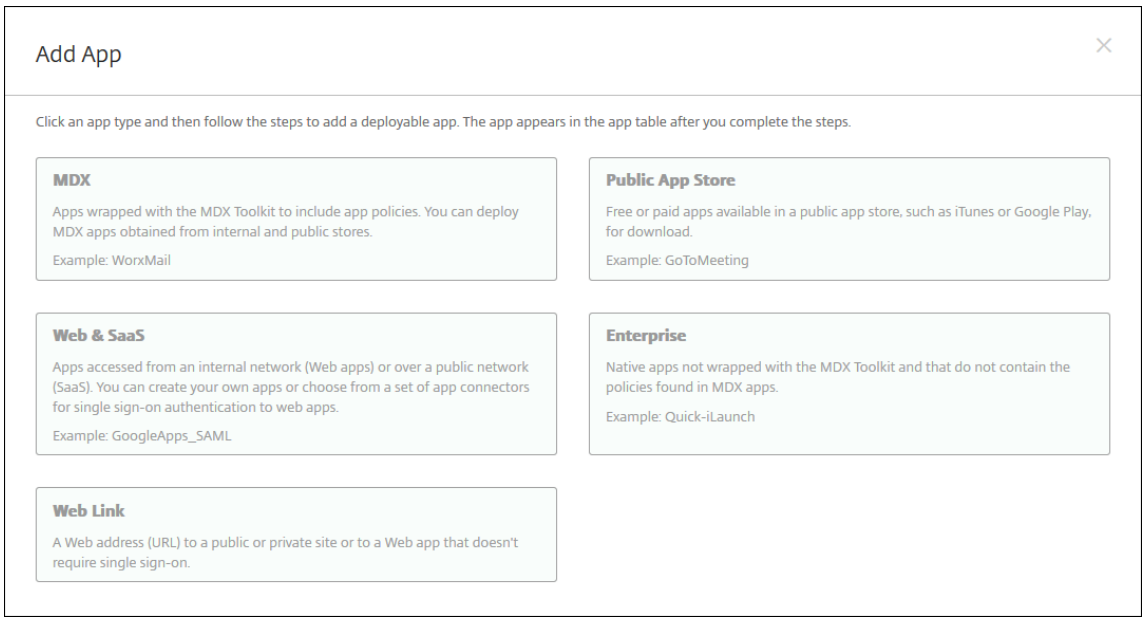
웹링크는인터넷또는인트라넷사이트에대한웹주소입니다. 웹링크는 SSO 가필요하지않은웹응용프로그램을가리킬수도있습니다. 웹링크구성을마치면링크가앱스토어에서아이콘으로표시됩니다. 사용자가 Secure Hub 에로그온하면사용가능한앱및데스크톱의목록과함께링크가표시됩니다.

XenMobile 콘솔의 앱탭에서웹링크를구성할수있습니다. 웹링크구성을마치면링크가 앱테이블의목록에링크아이콘으로나타납니다. 사용자가 Secure Hub 에로그온하면사용가능한앱및데스크톱의목록과함께링크가표시됩니다.

링크를추가하려면다음정보를제공합니다.

- 링크이름
- 링크설명
- 웹주소 (URL)
- 범주
- 역할
- .png 형식의이미지 (선택사항)

1. XenMobile 콘솔에서 구성 **>** 앱 **>** 추가를클릭합니다. 앱추가대화상자가나타납니다.

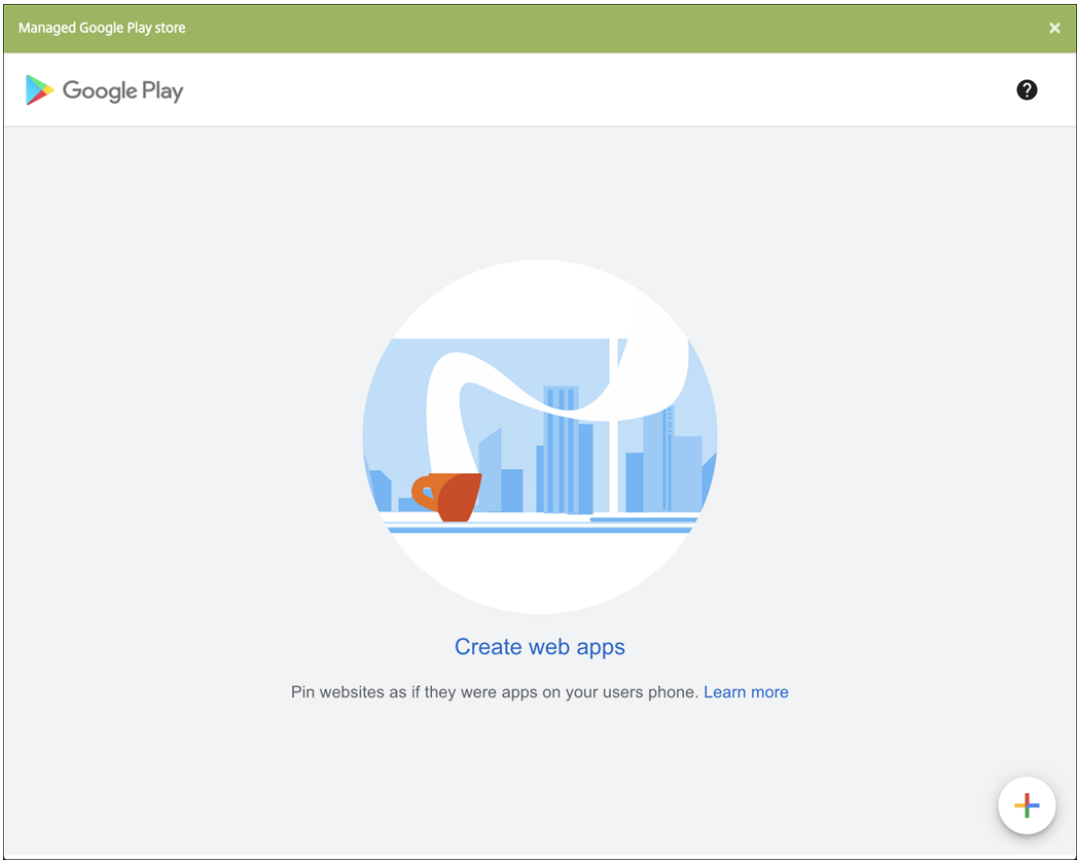


2. 웹링크를클릭합니다. 앱정보페이지가나타납니다.
3. 앱정보창에서다음정보를입력합니다.

   이름**:** 앱의설명적이름을입력합니다. 이이름은앱테이블의앱이름아래에나열됩니다.
   설명**:** 앱의선택적설명을입력합니다.
   앱범주**:** 필요한경우목록에서앱을추가할범주를클릭합니다. 앱범주에대한자세한내용은앱범주정보를참조하십시오.

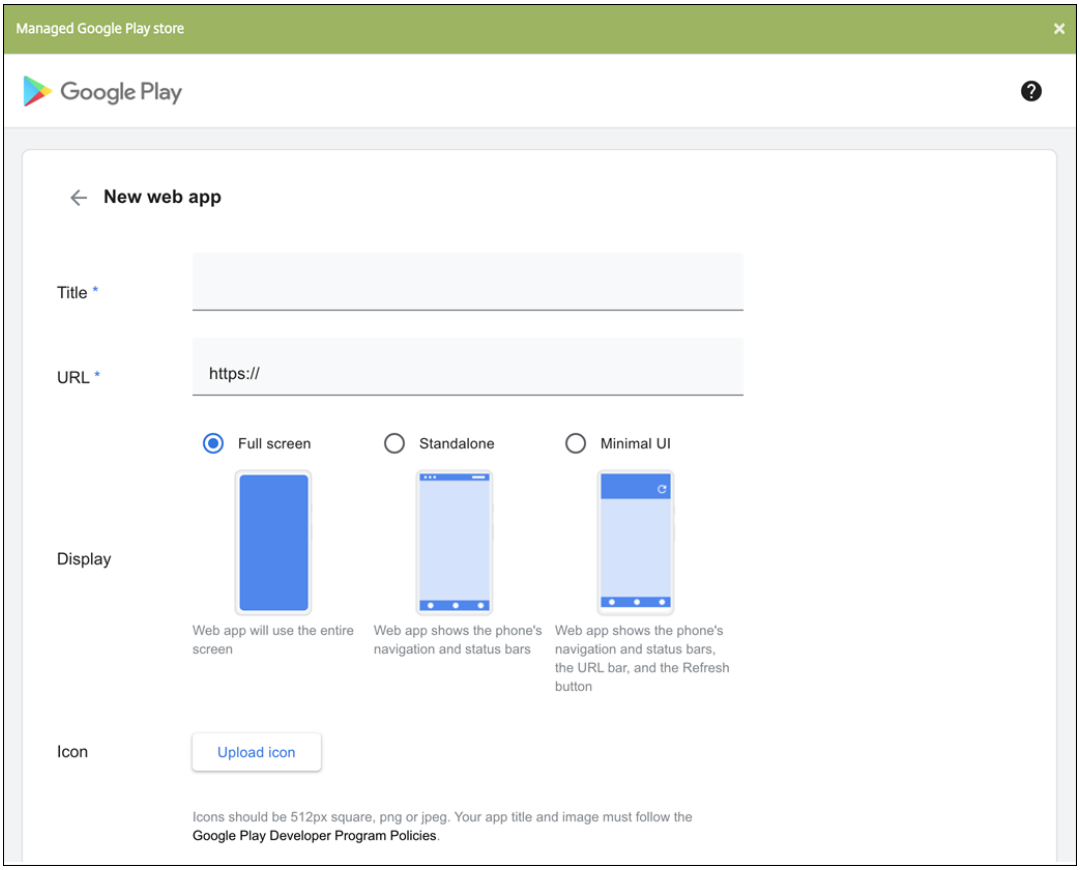
4. 다음을클릭합니다. 앱플랫폼페이지가나타납니다.
5. 플랫폼에서 iOS 및 Android(레거시 DA) 용웹앱을추가할 기타플랫폼을선택하거나 **Android Enterprise** 를선택합니다. 추가하지않을확인란을선택해제합니다.

   - 기타플랫폼을선택한경우다음단계를계속진행하여설정을구성합니다.
   - **Android Enterprise** 를선택할경우 업로드버튼을클릭하여관리되는 Google Play 스토어를엽니다. 개발자계정을등록하지않고도웹앱을게시할수있습니다. 계속하려면오른쪽아래의 **+** 아이콘을클릭합니다.



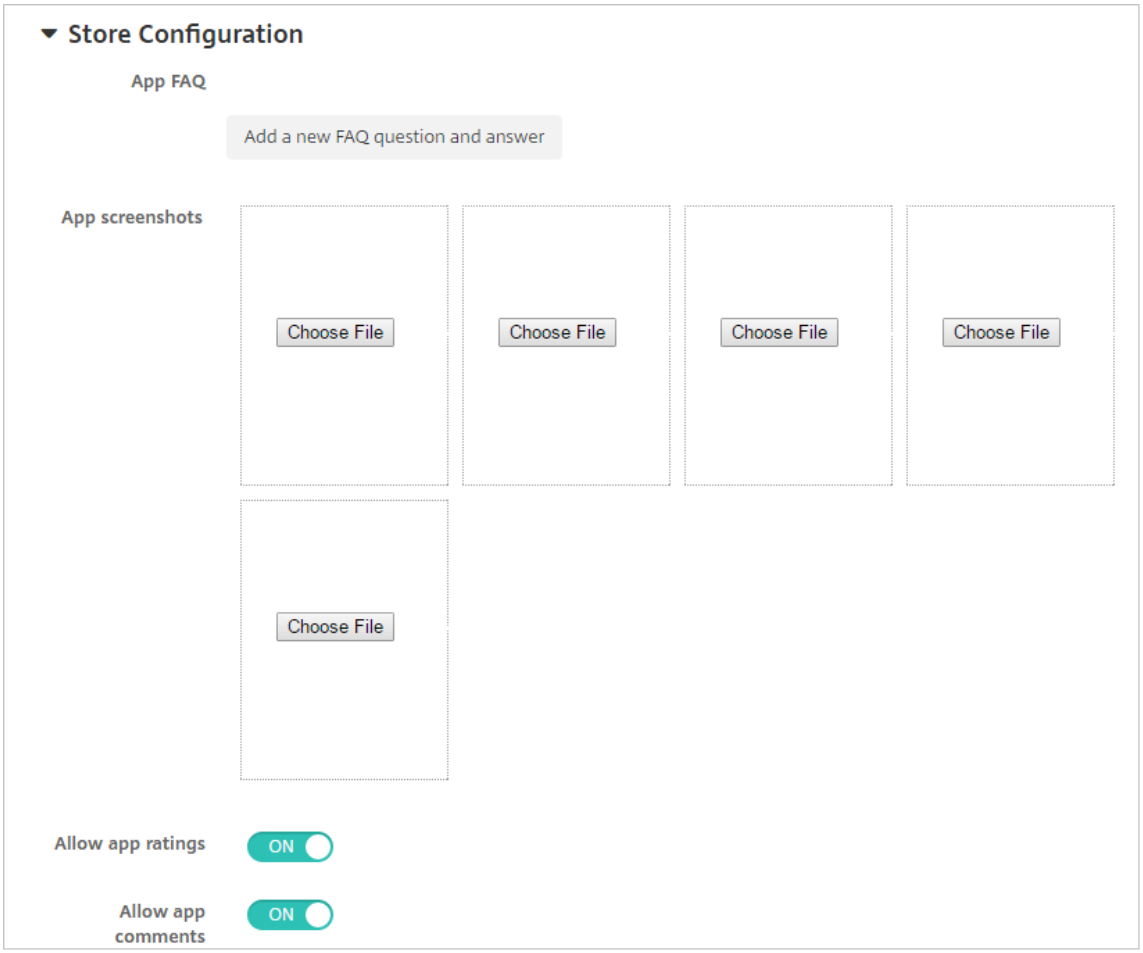
다음설정을구성합니다.

- 제목**:** 웹앱의이름을입력합니다.
- **URL:** 앱의웹주소를입력합니다.
- 표시**:** 사용자장치에웹앱을표시하는방식을선택합니다. 사용가능한옵션은 전체화면, 독립실행형, 최소 **UI** 입니다.
- 아이콘**:** 웹앱을나타내는자체이미지를업로드합니다.



작업을마치면 **Create(**만들기**)** 를클릭합니다. 웹앱을게시하는데최대 10 분이걸릴수있습니다.

6. Android Enterprise 가아닌플랫폼에서는다음설정을구성합니다.
   - 앱이름**:** 미리채워진이름을사용하거나새이름을입력합니다.
   - 앱설명**:** 미리채워진설명을사용하거나직접설명을입력합니다.
   - **URL:** 미리채워진 URL 을사용하거나앱의웹주소를입력합니다. 선택한커넥터에따라다음페이지로이동하기전에바꿔야하는자리표시자가이필드에포함될수있습니다.
   - 앱이내부네트워크에서호스트됨**:** 앱이내부네트워크의서버에서실행되는지여부를선택합니다. 원격위치에서내부앱에연결하는사용자의경우 Citrix Gateway 를통해연결해야합니다. 이옵션을 켜짐으로설정하면 VPN 키워드가앱에추가되고사용자가 Citrix Gateway 를통해연결할수있습니다. 기본값은 꺼짐입니다.
   - 앱범주**:** 목록에서앱에적용할선택적범주를클릭합니다.
   - 이미지**:** 기본 Citrix 이미지를사용할지, 고유한앱이미지를업로드할지여부를선택합니다. 기본값은기본값사용입니다.
     - 고유한이미지를업로드하려면 찾아보기를클릭하고파일의위치로이동합니다. 파일은.PNG 파일이어야합니다. JPEG 또는 GIF 파일은업로드할수없습니다. 사용자지정그래픽을추가하면나중에변경할수없습니다.
7. 배포규칙을구성합니다. 자세한내용은 배포규칙을참조하십시오.
8. 스토어구성을확장합니다.



- 앱 **FAQ:** 새 **FAQ** 질의응답추가를클릭하여앱에대한 FAQ 를만듭니다.
- 휴대폰/태블릿용스크린샷추가**:** 앱스토어에표시할화면캡처를추가합니다.
- 앱평가허용**:** 사용자가앱스토어에서앱을평가하도록허용합니다.
- 앱댓글허용**:** 사용자가앱스토어에서앱에관한댓글을남길수있도록허용합니다.

9. 다음을클릭합니다. 배달그룹할당페이지가나타납니다.
10. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을하나이상선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.
11. 배포일정을확장하고다음설정을구성합니다.

    - 배포**:** 앱을장치에배포할지여부를선택합니다. 기본값은 켜짐입니다.
    - 배포일정**:** 앱을 지금배포할지 나중에배포할지선택합니다. 나중에를선택할경우앱을배포할날짜와시간을구성합니다. 기본값은 지금입니다.
    - 배포조건**:** 장치를연결할때마다앱을배포하려면 연결할때마다를선택합니다. 장치에서이전에앱을받지못한경우 이전배포가실패한경우에만을선택하여앱을배포합니다. 기본값은 연결할때마다입니다.

    설정 **>** 서버속성에서백그라운드배포예약키를구성한경우 상시연결에대해배포가적용됩니다.

    구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은 상시연결에대해배포를제외하고모든플랫폼에적용됩

니다.

12. 저장을클릭합니다.

Microsoft 365 앱사용

MDX 컨테이너를열어 Secure Mail, Secure Web 및 Citrix Files 에서 Microsoft Office 365 앱으로문서및데이터를전송할수있습니다. 자세한내용은 Office 365 앱과 Secure 상호작용허용을참조하십시오.

워크플로적용

다음설정을구성하여워크플로를할당하거나만듭니다.

- 사용할워크플로**:** 목록에서기존워크플로를클릭하거나 새워크플로만들기를클릭합니다. 기본값은 없음입니다.

  새워크플로만들기를선택하는경우다음설정을구성합니다.

  - 이름**:** 워크플로의고유한이름을입력합니다.
  - 설명**:** 필요한경우워크플로의설명을입력합니다.
  - 전자메일승인템플릿**:** 목록에서할당할전자메일승인템플릿을선택합니다. 이필드오른쪽에있는눈모양아이콘을클릭하면템플릿을미리볼수있는대화상자가나타납니다.
  - 관리자승인수준**:** 목록에서이워크플로에필요한관리자승인수준의번호를선택합니다. 기본값은 1 수준입니다. 사용가능한옵션은다음과같습니다.

    * 필요없음
    * 1 수준
    * 2 수준
    * 3 수준

  - **Active Directory** 도메인선택**:** 목록에서워크플로에사용할적절한 Active Directory 도메인을선택합니다.
  - 추가로필요한승인자찾기**:** 검색필드에추가로필요한사람의이름을입력하고 검색을클릭합니다. 이름은 Active Directory 에서가져옵니다.
  - 필드에이름이나타나면해당하는이름옆의확인란을선택합니다. 이름과전자메일주소가 추가로필요한승인자선택됨목록에나타납니다.

    추가로필요한승인자선택됨목록에서사용자를제거하려면다음중하나를수행합니다.

    * 선택한도메인에있는모든사용자의목록을표시하려면 검색을클릭합니다.
    * 검색결과를제한하려면검색상자에이름전체또는일부를입력한다음 검색을클릭합니다.
    * 추가로필요한승인자선택됨목록에있는사용자는검색결과목록에서해당이름옆에확인표시가있습니다. 목록을스크롤하고제거하려는각이름옆에있는확인란의선택을취소합니다.

앱스토어및 **Citrix Secure Hub** 브랜딩

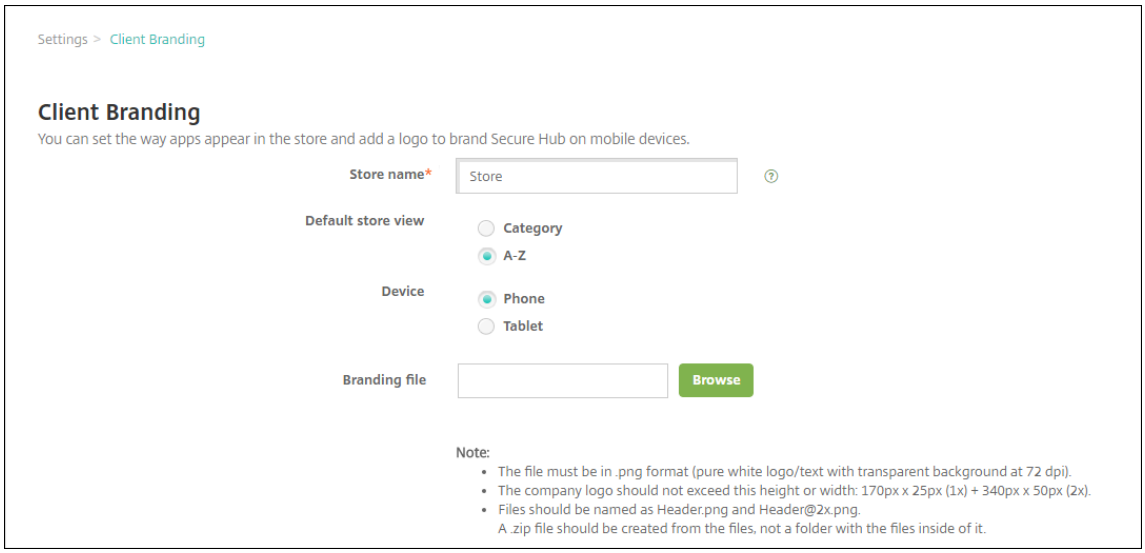
앱이스토어에나타나는방식을설정하고 Secure Hub 및앱스토어브랜드를나타내는로고를추가할수있습니다. 이러한브랜드기능은 iOS 및 Android 장치에서사용할수있습니다.

시작하기전에사용자지정이미지가준비되었으며액세스할수있는지확인하십시오.

사용자지정이미지는다음과같은요구사항을충족해야합니다.

- 파일은.png 형식이어야합니다.
- 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 Server 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**:** 찾아보기를클릭하고파일위치로이동하여브랜딩에사용할이미지또는이미지의.zip 파일을선택합니다.

3. 저장을클릭합니다.

앱커넥터유형

August 24, 2018

다음표에는웹또는 SaaS 앱을추가할때 XenMobile 에서사용할수있는커넥터와커넥터유형이나와있습니다. 또한웹또는 SaaS 앱을추가할때새커넥터를 XenMobile 에추가할수도있습니다.

이표에는커넥터가사용자계정관리를지원하는지여부도나타나있습니다. 지원되는경우새계정을자동으로또는워크플로를사용하여만들수있습니다.

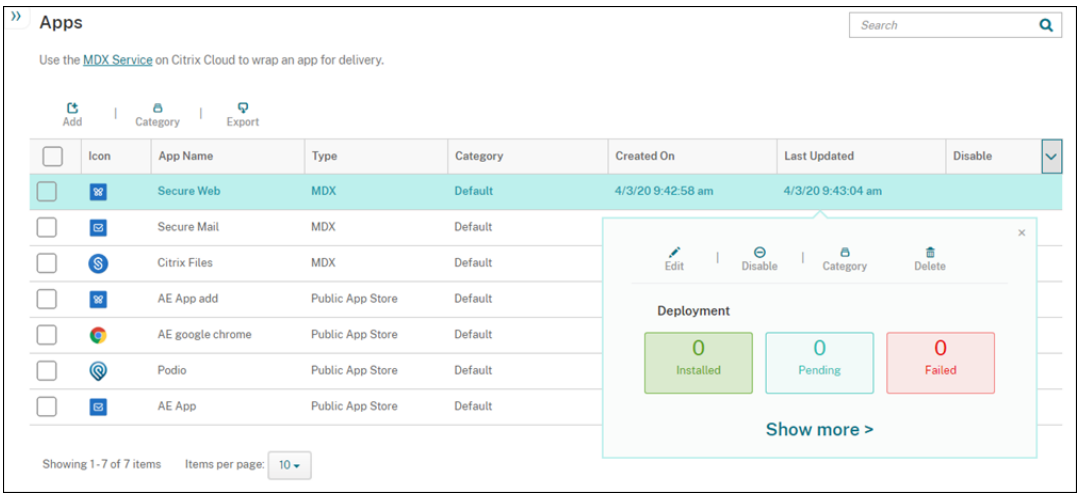
커넥터이름	SSO SAML	사용자계정관리지원
EchoSign_SAML	예	예
Globoforce_SAML		참고**:** 이커넥터를사용하는경우원활한 SSO 통합을위해 User Management for Provisioning 을사용하도록설정해야합니다.
GoogleApps_SAML	예	예
GoogleApps_SAML_IDP	예	예
Lynda_SAML	예	예
Office365_SAML	예	예
Salesforce_SAML	예	예
Salesforce_SAML_SP	예	예
SandBox_SAML	예	
SuccessFactors_SAML	예	
ShareFile_SAML	예	
ShareFile_SAML_SP	예	
WebEx_SAML_SP	예	예

MDX 또는엔터프라이즈앱업그레이드

January 5, 2022

XenMobile 에서 MDX 또는엔터프라이즈앱을업그레이드하려면 XenMobile 콘솔에서앱을비활성화한다음새버전의앱을업로드합니다. Citrix Secure Mail 과같은공용앱스토어앱은비활성화하지않아도됩니다.

1. XenMobile 콘솔에서 구성 **>** 앱을클릭합니다. 앱페이지가나타납니다.
2. 관리되는장치 (모바일장치관리를위해 XenMobile 에등록된장치) 인경우 3 단계로건너뛰십시오. 관리되지않는장치 (엔터프라이즈앱관리용도로만 XenMobile 에등록된장치) 인경우다음을수행하십시오.
   a) 앱테이블에서앱옆에있는확인란을선택하거나업데이트하려는앱이포함된라인을클릭합니다.
   b) 나타나는메뉴에서 사용안함을클릭합니다.



   c) 확인대화상자에서 사용안함을클릭합니다. 앱의 사용안함열에 사용안함이나타납니다.

> 참고:
>
> 앱을사용하지않도록설정한동안로그오프하면앱에다시연결할수없습니다. 앱을사용하지않도록설정하는것은선택적이지만앱기능에문제가발생하지않도록앱을사용하지않도록설정하는것이좋습니다. 예를들어사용자가새버전을업로드하는동시에앱을다운로드하도록요청하는경우문제가발생할수있습니다.

3. 앱테이블에서앱옆에있는확인란을클릭하거나업데이트하려는앱이포함된라인을클릭합니다.
4. 나타나는메뉴에서 편집을클릭합니다. 선택한앱에대해원래선택한플랫폼을보여주는 앱정보페이지가나타납니다.
5. 다음설정을구성합니다.
   - 이름**:** 필요한경우앱이름을변경합니다.
   - 설명**:** 필요한경우앱설명을변경합니다.
   - 앱범주**:** 필요한경우앱범주를변경합니다.
6. 다음을클릭합니다. 선택한첫번째플랫폼페이지가나타납니다. 선택한각플랫폼에대해다음을수행합니다.
   a) 업로드를클릭하고파일위치로이동하여업로드하려는대체파일을선택합니다. XenMobile 에앱이업로드됩니다.

      Android Enterprise 용앱을업로드할경우관리되는 Google Play 창이나타납니다. 여기에새버전의앱을업로드하십시오. 자세한내용은 Android Enterprise 앱배포를참조하십시오.

b) 필요한경우앱세부정보및플랫폼에대한정책설정을변경합니다.

c) 필요한경우배포규칙및 XenMobile Store 구성을구성합니다. 자세한내용은 앱추가에서 MDX 앱추가를참조하십시오.

7. 저장을클릭합니다. 앱페이지가나타납니다.
8. 2 단계에서앱을사용하지않도록설정한경우다음을수행하십시오.

a) 앱테이블에서업데이트한앱을클릭하여선택한다음나타나는메뉴에서 사용을클릭합니다.
b) 나타나는확인대화상자에서 사용을클릭합니다. 이제사용자가앱에액세스하여앱을업그레이드하라는알림을받을수있습니다.

Citrix Launcher

March 14, 2022

Citrix Launcher 교체

Citrix 는 2020 년 8 월에 Citrix Launcher 를앱스토어에서제거했습니다. Citrix Launcher 대신이미제공되는기능을사용할수있습니다.

장치를키오스크 (전용장치) 로프로비저닝하려면:

1. XenMobile 관리자가 XenMobile 배포에전용장치를등록하는데필요한 RBAC 역할을추가합니다. 전용 Android Enterprise 장치프로비전을참조하십시오.
2. 등록유형이 완전관리형프로필/작업프로필인등록프로필을만듭니다. 등록프로필을만들려면을참조하십시오.
3. 작업잠금모드설정을사용하도록설정하여장치화면에앱을고정하도록구성하는키오스크장치정책을만듭니다. Android Enterprise 설정을참조하십시오.

Citrix Launcher 정보

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.

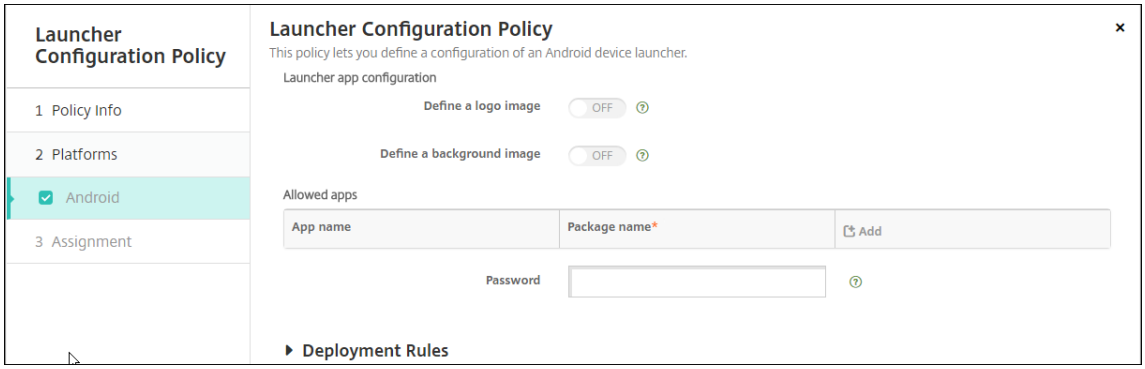
이러한 Citrix Launcher 기능을제어하는 **Launcher** 구성정책을추가할수있습니다.

- 사용자가지정된앱에만액세스할수있도록 Android 장치를관리합니다.
- 필요에따라 Citrix Launcher 아이콘의사용자지정로고이미지와 Citrix Launcher 의사용자지정배경이미지를지정합니다.
- 사용자가 Launcher 를종료할때입력해야하는암호를지정합니다.

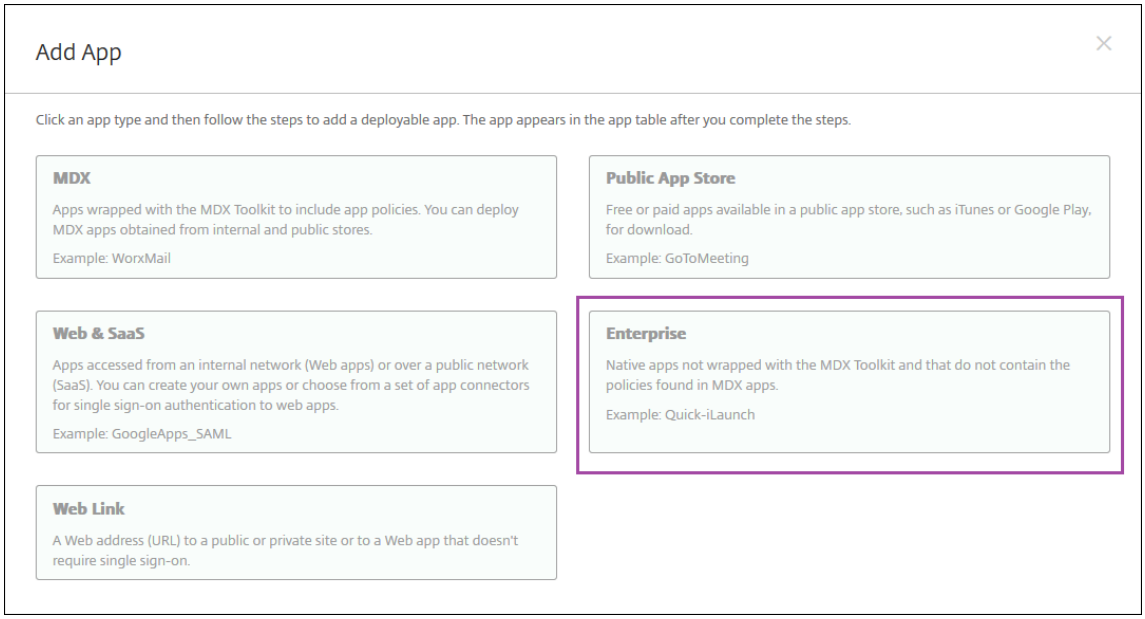
Citrix Launcher 를사용하면이러한장치수준의제한을적용할수있는동시에사용자에게 Wi-Fi 설정, Bluetooth 설정및장치암호설정과같은장치설정에대한기본제공액세스를부여할수있습니다. Citrix Launcher 는장치플랫폼이이미제공하는보안에추가적인보안계층을더하기위한것이아닙니다.

Android 장치에 Citrix Launcher 를제공하려면다음과같은일반단계를따르십시오.

1. Citrix Launcher 앱을다운로드하려면: https://www.citrix.com/downloads로이동합니다. **Citrix Launcher** 를검색합니다. 파일이름은 CitrixLauncher.apk 입니다. 이파일은 XenMobile 에업로드가능하며래핑이필요없습니다.
2. 장치정책 **Launcher** 구성정책을추가합니다. 구성 **>** 장치정책으로이동한후 추가를클릭하고 새정책추가대화상자에서 **Launcher** 를입력합니다. 자세한내용은 Launcher 구성정책을참조하십시오.

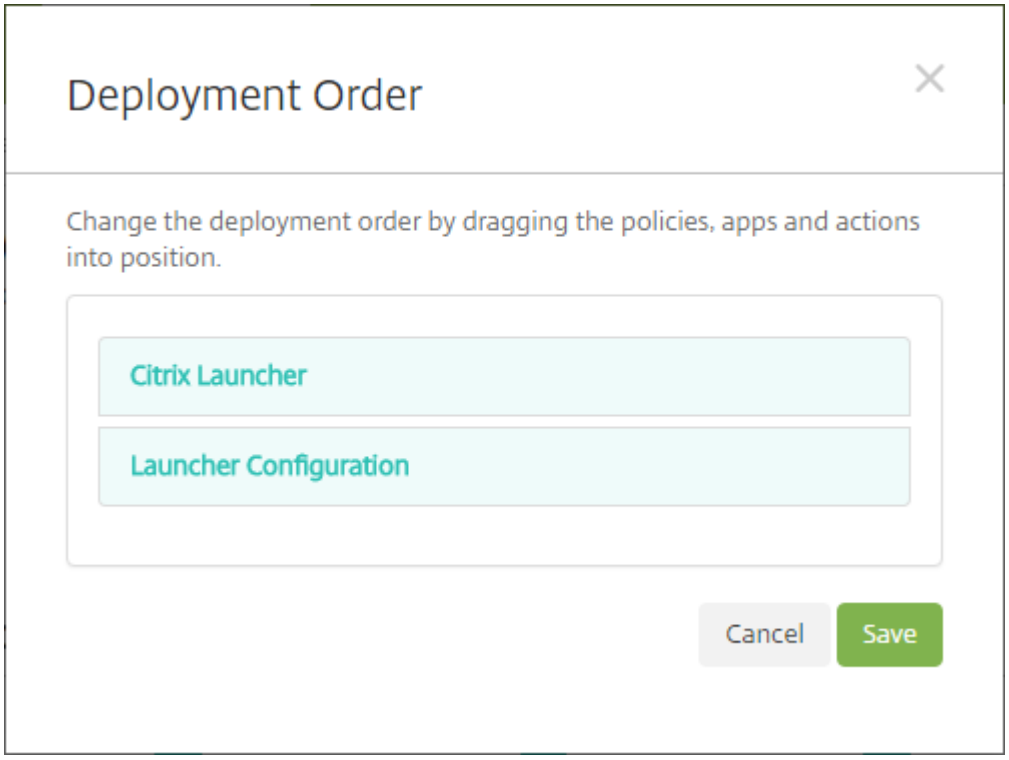


3. Citrix Launcher 앱을 XenMobile 에엔터프라이즈앱으로추가합니다. 구성 **>** 앱에서 추가를클릭한후 엔터프라이즈를클릭합니다. 자세한내용은 엔터프라이즈앱추가를참조하십시오.



4. 구성 **>** 배달그룹에서다음구성을사용하여 Citrix Launcher 에대한배달그룹을만듭니다.
   - 정책페이지에서 **Launcher** 구성정책을추가합니다.
   - 앱페이지에서 **Citrix Launcher** 를 필수앱으로끌어옵니다.

- 요약페이지에서 배포순서를클릭하고 **Citrix Launcher** 앱이 **Launcher** 구성정책보다앞에있는지확인합니다.



자세한내용은 리소스배포를참조하십시오.

Apple 볼륨구매

January 5, 2022

Apple iOS 볼륨구매를사용하여 iOS 앱라이센스를관리할수있습니다. 볼륨구매솔루션은조직의앱및기타데이터를대량으로찾고, 구입하고, 배포하는프로세스를간소화합니다.

볼륨구매를사용하면 XenMobile 에서공용앱스토어앱을배포할수있습니다.

- MAM 등록에는볼륨구매가지원되지않습니다. MDM 또는 MDM+MAM 에서볼륨구매장치를등록해야합니다.
- Citrix 모바일생산성앱에는볼륨구매가지원되지않습니다.
- XenMobile 공용스토어앱을볼륨구매로배포할수는있지만최적화된배포가아닙니다. 이러한제한을해결하려면 XenMobile 과 Secure Hub 스토어가개선되어야합니다.
- 볼륨구매를통한 XenMobile 공용스토어앱배포와관련된알려진문제의목록은 Citrix Knowledge Center의이문서를참조하십시오.

볼륨구매를사용하여해당하는앱을장치에직접배포할수있습니다. 또는상환가능한코드를사용하여사용자에게콘텐츠를할당할수있습니다. XenMobile 에서 iOS 볼륨구매와관련된설정을구성할수있습니다.

XenMobile 은 Apple 에서볼륨구매라이센스를주기적으로다시가져와해당라이센스에모든변경내용이반영되었는지확인합니

다. 볼륨구매에서가져온앱을수동으로삭제하는경우가이러한변경에포함됩니다. 기본적으로 XenMobile 에서볼륨구매라이센스 기준은최소 1440 분 (24 시간) 마다새로고쳐집니다. 새서버속성인 `VPP.baseline`을사용하여볼륨구매기준간격을변경할 수있습니다. 서버속성을참조하십시오.

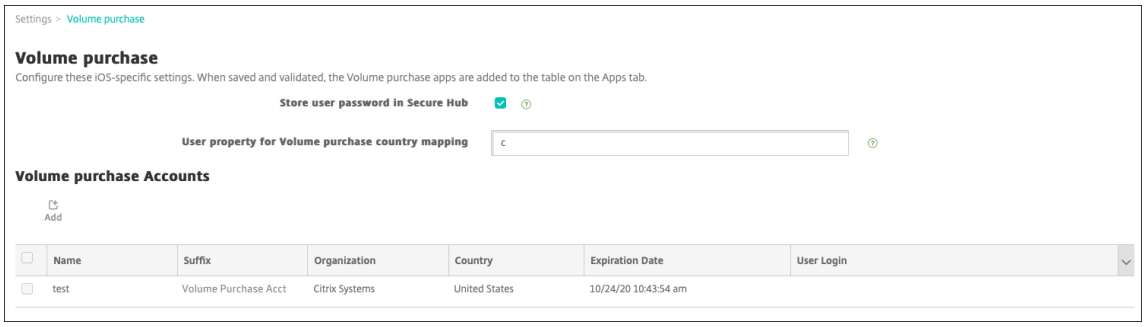
앱자동업데이트설정은 `VPP.baseline` 서버속성과해당속성에설정된동일한일정의앱업데이트에따라서도달라집니다.

이문서에서는관리되는라이센스로볼륨구매를사용하여 XenMobile 에서앱을배포하는방법을집중적으로설명합니다. 현재상환 코드를사용하고있고관리되는배포로변경하려는경우이 Apple 지원문서 (볼륨구입프로그램을통해사용권코드를관리배포로마이그레이션하기) 를참조하십시오.

iOS 볼륨구매에대한자세한내용은 https://volume.itunes.apple.com/us/store에서확인하십시오. 볼륨구매에등록하려면 https://deploy.apple.com/qforms/open/register/index/avs로이동하십시오. iTunes 에서볼륨구매스토어에액세스하려면 https://volume.itunes.apple.com/?l=en으로이동하십시오.

이러한 iOS 볼륨구매설정을 XenMobile 에저장하면구입한앱이 XenMobile 콘솔의 구성 **>** 앱페이지에나타납니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 볼륨구매를클릭합니다. 볼륨구매구성페이지가나타납니다.



3. 다음설정을구성합니다.

   - **Secure Hub** 에사용자암호저장**:** XenMobile 인증을위한사용자이름과암호를 Secure Hub 에저장할지여부를선택합니다. 기본값은이보안방법을사용하여정보를저장하는것입니다.
   - 볼륨구매국가매핑을위한사용자속성**:** 사용자가국가별앱스토어에서앱을다운로드할수있도록하는코드를입력합니다.

   XenMobile 은이매핑을사용하여볼륨구매의속성풀을선택합니다. 예를들어사용자속성이미국인경우볼륨구매코드가영국과관련되어있으면해당사용자가앱을다운로드할수없습니다. 국가매핑코드에대한자세한내용은볼륨구매프로그램관리자에게문의하십시오.

4. 추가할각볼륨구매계정에대해 추가를클릭합니다. 볼륨구매계정추가대화상자가나타납니다.
5. 추가하는각계정에대해다음설정을구성합니다.

   > 참고**:**
   >
   > Apple Configurator 1 을사용하는경우라이센스파일을업로드합니다. 구성 **>** 앱으로이동한다음플랫폼페이지에서 볼륨구매을확장합니다.

   - 이름**:** 볼륨구매계정이름을입력합니다.

- 접미사**:** 볼륨구매계정을통해받은앱이름과함께표시할접미사를입력합니다. 예를들어 **VP** 를입력하면 Secure Mail 앱이앱목록에 **Secure Mail - VP** 로표시됩니다.
- 회사토큰**:** Apple 에서받은볼륨구매서비스토큰을복사하고붙여넣습니다. 토큰을받으려면: Apple 볼륨구매포털의 계정요약페이지에서 다운로드단추를클릭하여볼륨구매파일을생성하고다운로드합니다. 이파일에는서비스토큰및기타정보 (예: 국가코드및만료일) 가포함되어있습니다. 파일을안전한위치에저장합니다.
- 사용자로그인**:** 사용자지정 B2B 앱을가져올때사용할권한이있는볼륨구매계정관리자이름을선택적으로입력합니다.
- 사용자암호**:** 볼륨구매계정관리자암호를입력합니다.
- 앱자동업데이트**:** 켜짐인경우 Apple 스토어에업데이트가있으면볼륨구매앱이자동으로업데이트됩니다. 기본값은꺼짐입니다.

6. 저장을클릭하여대화상자를닫습니다.
7. 볼륨구매구성을저장하려면 저장을클릭합니다.

   XenMobile 의 구성 **>** 앱페이지의목록에앱이추가된다는메시지가표시됩니다. 이페이지에서볼륨구매계정의앱이름에이전구성에입력한접미사가포함된것을알수있습니다.

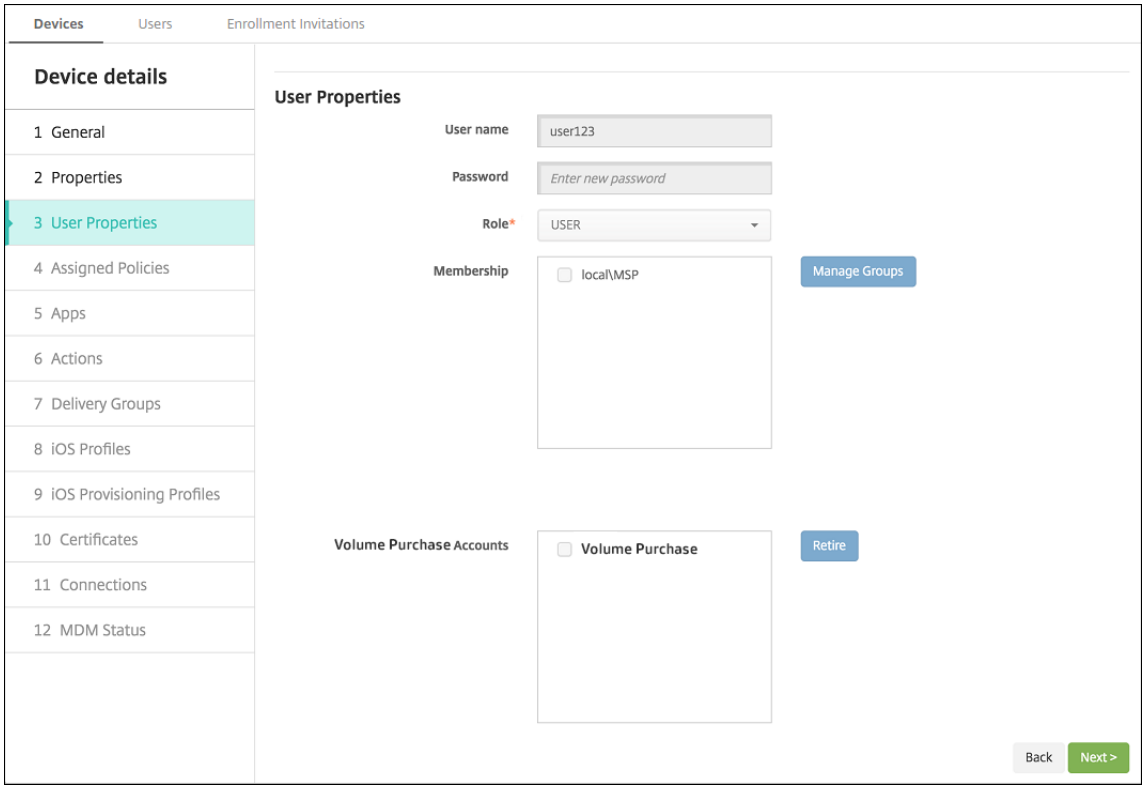
이제볼륨구매앱설정을구성하고볼륨구매앱에대한배달그룹및배달정책설정을조정할수있습니다. 이러한구성이완료되면사용자가장치를등록할수있습니다. 다음참고는이러한프로세스에대한고려사항을제공합니다.

- 볼륨구매앱설정을구성할때 (구성 **>** 앱) 장치에강제로라이센스연결을사용합니다. Apple 볼륨구매및배포프로그램을감독되는장치에서사용할경우 XenMobile 을사용하여사용자수준이아닌장치수준에서앱을할당할수있다는장점이있습니다. 따라서 Apple ID 장치를사용하지않아도됩니다. 또한사용자에게 Apple 볼륨구매가입을위한초대가전송되지않습니다. 사용자또한 iTunes 계정에로그인하지않고앱을다운로드할수있습니다.

  해당앱에대한볼륨구매정보를보려면 볼륨구매를확장합니다. 볼륨구매라이센스키표에서라이센스가장치에연결된것을볼수있습니다. 사용자가토큰을제거한후다시가져오면 Apple 개인정보보호제한으로인해일련번호대신 숨김단어가표시됩니다.

  라이센스연결을해제하려면라이센스에대한행을클릭한후 연결해제를클릭합니다.

  볼륨구매라이센스를사용자에게연결하면 XenMobile 에서사용자가볼륨구매계정에통합되고사용자의 iTunes ID 가볼륨구매계정에연결됩니다. 사용자의 iTunes ID 는회사또는 XenMobile Server 에절대표시되지않습니다. Apple 은이연결을투명하게생성하여사용자개인정보를보호합니다. 사용자의 Apple 볼륨구매사용을중지하여사용자계정에서모든라이센스연결을해제할수있습니다. 사용자를사용중지하려면 관리 **>** 장치로이동합니다.



- XenMobile 에서앱을배달그룹에할당하면기본적으로앱이선택적앱으로식별됩니다. XenMobile 이앱을장치에배포하도록하려면 구성 **>** 배달그룹으로이동합니다. 앱페이지에서앱을 필수앱목록으로이동합니다.
- 공용앱스토어앱에대한업데이트가제공되는경우: 볼륨구매에서앱을푸시하면장치에서앱이자동으로업데이트됩니다. 사용자가아닌장치에할당된 Secure Hub 에대한업데이트를푸시하려면다음을수행합니다. 구성 **>** 앱의플랫폼페이지에서 업데이트확인을클릭하고업데이트를적용합니다.

  Apple 볼륨구매가만료되면 XenMobile 에서라이센스만료경고를표시합니다.

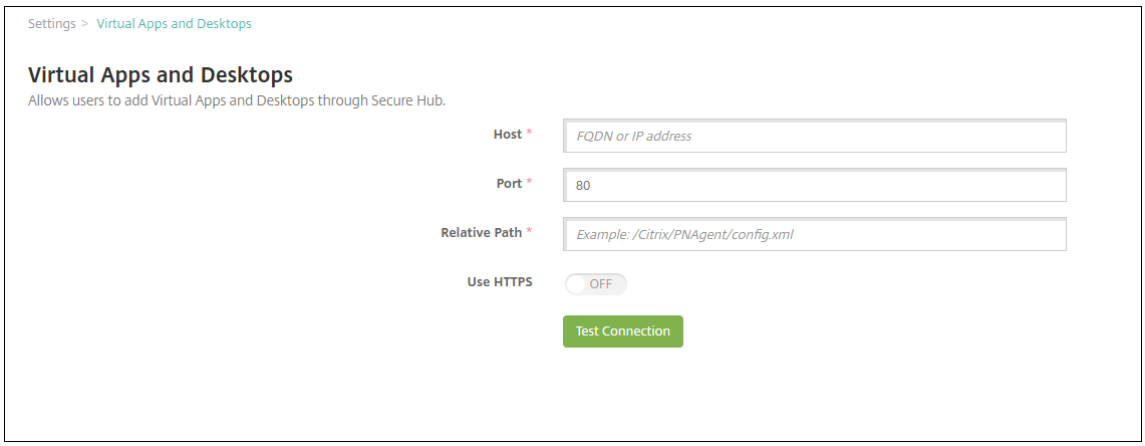
Citrix Secure Hub 를통한 Virtual Apps and Desktops

December 1, 2020

XenMobile 에서는 Virtual Apps and Desktops 에서앱을수집하고 XenMobile Store 를통해이러한앱을모바일장치사용자에게제공할수있습니다. 사용자는 XenMobile Store 내에서직접앱을구독하고 Secure Hub 에서앱을시작할수있습니다. 앱을시작하려면 Citrix Receiver 를사용자장치에설치해야하지만이를구성할필요는없습니다.

이설정을구성하려면 Web Interface 사이트나 StoreFront 의 FQDN(정규화된도메인이름) 또는 IP 주소및포트번호가필요합니다.

1. XenMobile 웹콘솔에서오른쪽위모서리의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. **Virtual Apps and Desktops** 를클릭합니다. **Virtual Apps and Desktops** 페이지가나타납니다.



3. 다음설정을구성합니다.
   - 호스트**:** Web Interface 사이트나 StoreFront 의 FQDN(정규화된도메인이름) 또는 IP 주소를입력합니다.
   - 포트**:** Web Interface 사이트나 StoreFront 의포트번호를입력합니다. 기본값은 80 입니다.
   - 상대경로**:** 경로를입력합니다. 예를들어, /Citrix/PNAgent/config.xml 을입력할수있습니다.
   - **HTTPS** 사용**:** Web Interface 사이트또는 StoreFront 와클라이언트장치사이에보안인증을사용할것인지를선택합니다. 기본값은 꺼짐입니다.
4. 연결테스트를클릭하여 XenMobile 에서지정된 Virtual Apps and Desktops 서버에연결할수있는지확인합니다.
5. 저장을클릭합니다.

XenMobile 에서 Citrix Content Collaboration 사용

January 5, 2022

Citrix Files 와 StorageZone 커넥터라는두가지옵션을사용하여 XenMobile 을 Citrix Content Collaboration 과통합할수있습니다. Citrix Files 또는 StorageZone 커넥터통합에는 XenMobile Enterprise Edition 이필요합니다.

Citrix Files

XenMobile Enterprise Edition 을사용하는경우 Citrix Files 계정에대한액세스를제공하도록 XenMobile 을구성할수있습니다. 이구성은다음과같습니다.

- 모바일사용자에게파일공유, 파일동기화및 StorageZone 커넥터와같은전체 Enterprise 기능집합에대한액세스권한을부여합니다.
- Citrix Files 에 XenMobile App 사용자의 Single Sign-on 인증과포괄적인액세스제어정책을제공할수있습니다.
- XenMobile 콘솔을통해 Citrix Files 구성, 서비스수준모니터링및라이센스사용현황모니터링을제공합니다.

Citrix Files 에대해 XenMobile 을구성하는방법에대한자세한내용은 Citrix Files 를사용하는 Single Sign-on 을위한 SAML을참조하십시오.

StorageZone 커넥터

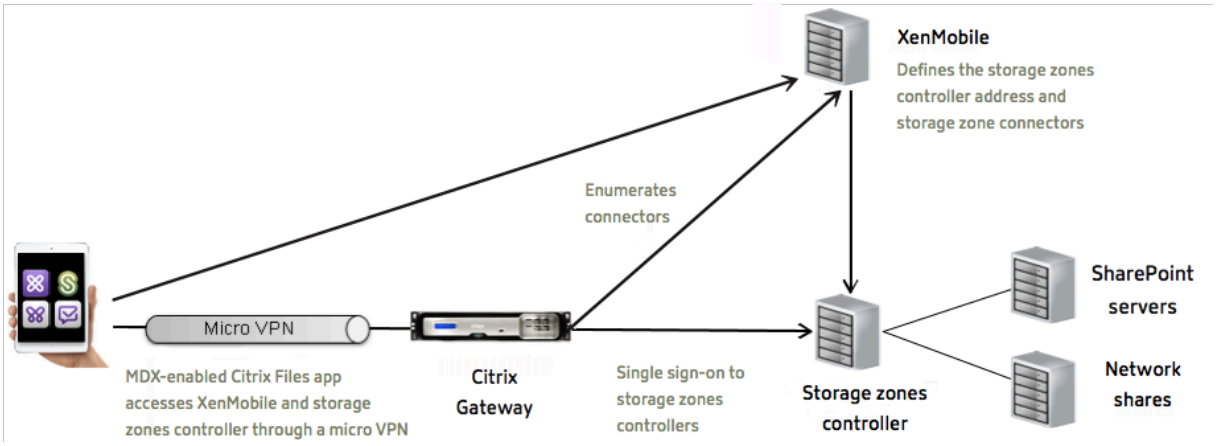
XenMobile 콘솔을통해만든 StorageZone 커넥터에대한액세스만제공하도록 XenMobile 을구성할수있습니다. 이구성은 다음과같습니다.

- SharePoint 사이트및네트워크파일공유등의기존온-프레미스스토리지저장소에대한보안모바일액세스를제공합니다.
- Citrix Content Collaboration 하위도메인을설정하거나 Citrix Files 데이터를호스팅할필요가없습니다.
- 사용자가모바일에서 iOS 및 Android 용 Citrix Files 모바일생산성앱을통해데이터에모바일액세스할수있습니다. 사용자가 Microsoft Office 문서를편집할수있습니다. 또한모바일장치에서 Adobe PDF 파일을미리보고주석을달수있습니다.
- 사용자정보가회사네트워크밖으로유출되지않도록하는보안제한사항을준수합니다.
- XenMobile 콘솔을통해 StorageZone 커넥터를간단하게설치할수있습니다. 나중에전체 Citrix Files 기능을 XenMobile 에서사용하기로결정한경우 XenMobile 콘솔에서구성을변경할수있습니다.
- XenMobile Enterprise Edition 이필요합니다.

XenMobile 과 StorageZone 커넥터전용통합의경우:

- Citrix Content Collaboration 은 Citrix Gateway 에대한 Single Sign-On 구성을사용하여 StorageZones Controller 에인증합니다.
- Citrix Files 제어부가사용되지않기때문에 XenMobile 이 SAML 을통해인증하지않습니다.

다음다이어그램은 XenMobile 과 StorageZone 커넥터를함께사용할때의아키텍처개요를보여줍니다.



요구사항

- 최소구성요소버전:
  - XenMobile Server 10.5(온-프레미스)
  - ShareFile for iOS(MDX) 5.3
  - ShareFile for Android(MDX) 5.3
  - StorageZones Controller 5.0

    이문서에는 StorageZones Controller 5.0 구성방법에대한지침이포함되어있습니다.

- StorageZones Controller 를실행하는서버가시스템요구사항을충족하는지확인하십시오. 요구사항은 시스템요구사항을참조하십시오.

XenMobile 과 StorageZone 커넥터만통합하는경우 Citrix Files 데이터용 StorageZone 및제한된 StorageZone 에대한요구사항이적용되지않습니다.

XenMobile 은 Documentum 커넥터를지원하지않습니다.

- PowerShell 스크립트를실행하려면:
  - 32 비트 (x86) 버전의 PowerShell 에서스크립트를실행합니다.

설치작업

나와있는순서대로다음작업을완료하여 StorageZones Controller 를설치하고설정합니다. 이러한단계는 XenMobile 과 StorageZone 커넥터전용통합에만적용됩니다. 이러한문서중일부는 StorageZones Controller 설명서에포함되어있습니다.

1. StorageZones Controller 를사용하도록 Citrix ADC 구성

   Citrix ADC 를 StorageZones Controller 의 DMZ 프록시로사용할수있습니다.

2. SSL 인증서설치

   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 에대한프록시서버지정

   StorageZones Controllers 콘솔을사용하여 StorageZones Controllers 의프록시서버를지정할수있습니다. 다른방법을사용하여프록시서버를지정할수도있습니다.

7. 위임을위해 StorageZones Controller 를신뢰하도록도메인컨트롤러구성

   네트워크공유또는 SharePoint 사이트에서 NTLM 또는 Kerberos 인증을지원하도록도메인컨트롤러를구성합니다.

8. 보조 StorageZones Controller 를 StorageZone 에연결

   StorageZone 에고가용성을구성하려면영역에적어도두개의 StorageZones Controller 를연결합니다.

StorageZones Controller 설치

1. StorageZones Controller 소프트웨어다운로드및설치:

a) https://www.citrix.com/downloads로이동합니다. **ShareFile** 을검색한다음최신 StorageZones Controller 설치관리자를다운로드합니다.

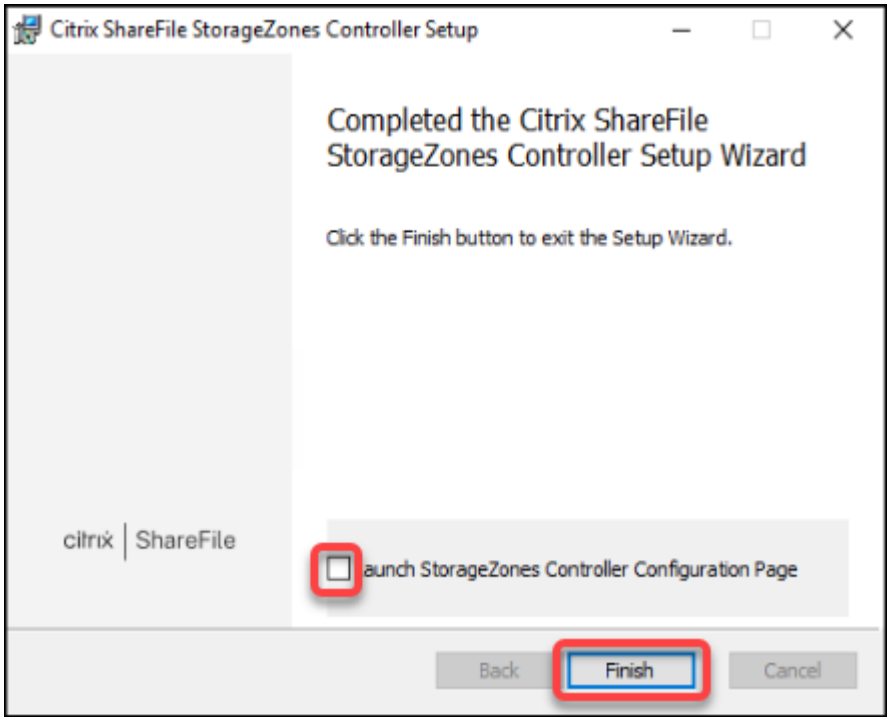
b) StorageZones Controller 를설치하면서버의기본웹사이트가컨트롤러의설치경로로변경됩니다. 기본웹사이트에서 익명인증을사용하도록설정합니다.

2. StorageZones Controller 를설치하려는서버에서 StorageCenter.msi 를실행합니다.

   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. 메시지가나타나면 StorageZones Controller 를다시시작합니다.

5. 설치가성공적이었는지테스트하려면 `https://localhost/`로이동합니다. 설치가성공적이면 Citrix Files 로고가나타납니다.

   Citrix Files 로고가나타나지않으면브라우저캐시를지우고다시시도하십시오.

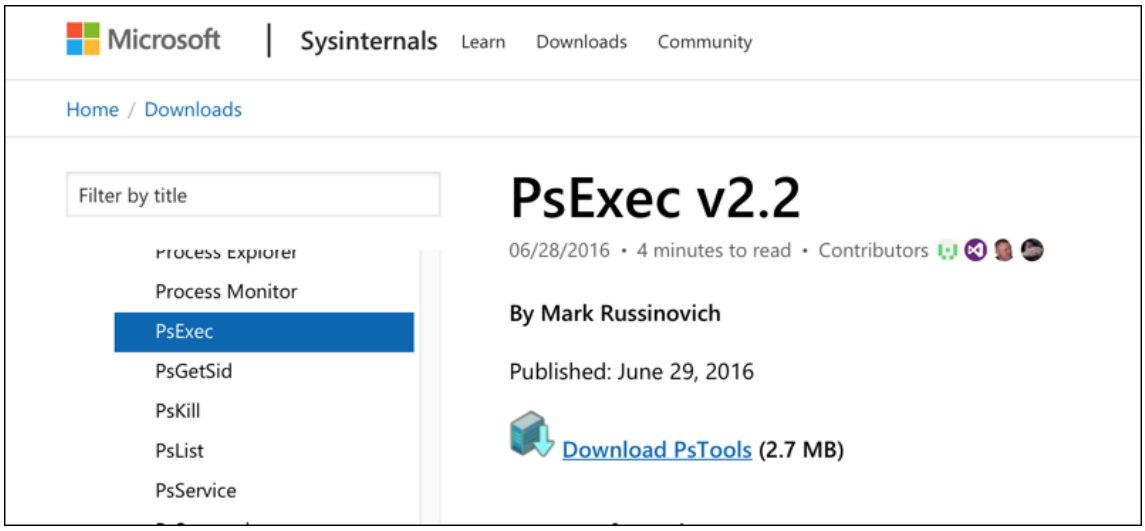
   > 중요:
   >
   > StorageZones Controller 를복제하려는경우 StorageZones Controller 구성을계속하기전에디스크이미지를캡처하십시오.

StorageZone 커넥터전용으로사용하도록 **StorageZones Controller** 준비

StorageZone 커넥터전용통합의경우 StorageZones Controller 관리콘솔을사용하지않습니다. 이인터페이스에는이솔루션에필요하지않은 Citrix Files 관리자계정이필요합니다. 따라서 PowerShell 스크립트를실행하여 Citrix Files 제어부없이 사용하도록 StorageZones Controller 를준비합니다. 스크립트는다음을수행합니다.

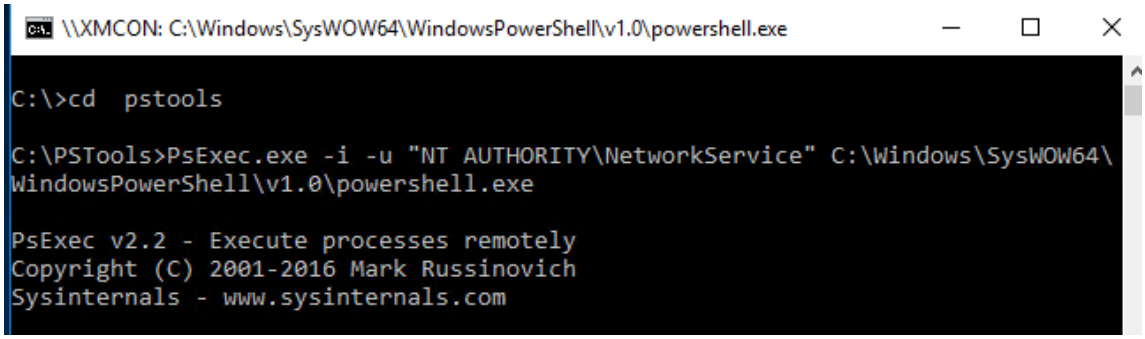
- 현재 StorageZones Controller 를기본 StorageZones Controller 로다시시작합니다. 나중에보조 StorageZones Controller 를기본컨트롤러에가입시킬수있습니다.
- 영역을만들고사용할암호를설정합니다.

1. StorageZone Controller 서버에서 PsExec 도구다운로드: Microsoft Windows Sysinternals로이동한다음 **Download PsTools(PsTools** 다운로드**)** 를클릭합니다. C 드라이브루트에도구의압축을풉니다.

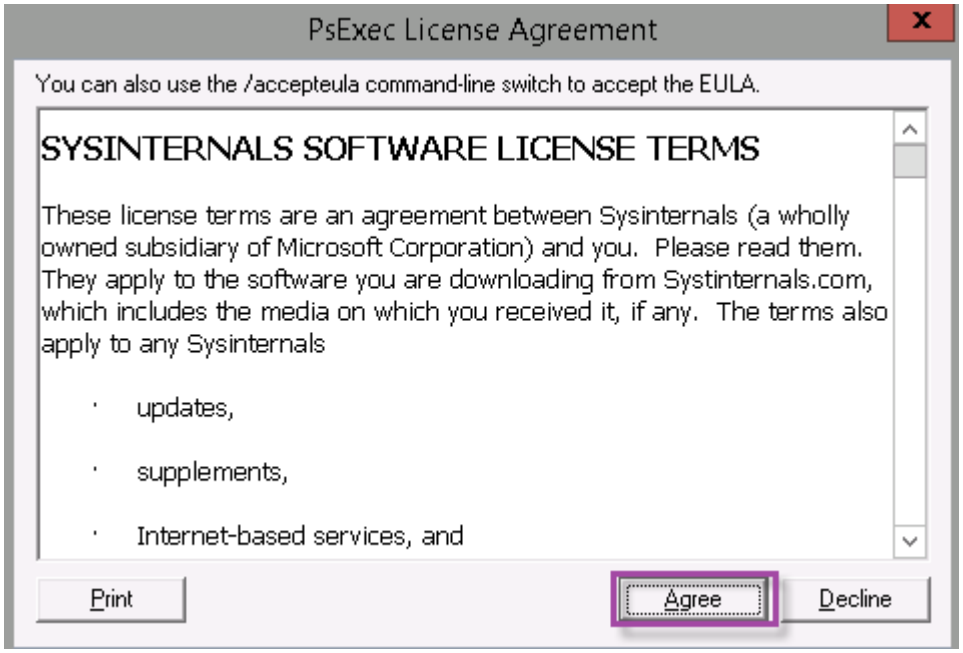


2. PsExec 도구실행: 관리자사용자로명령프롬프트를열고다음을입력합니다.

```
cd c:\pstools
PsExec.exe -i -u ”NT AUTHORITY\NetworkService” C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy-->
```



3. 메시지가나타나면 **Agree(**동의**)** 를클릭하여 Sysinternals 도구를실행합니다.



PowerShell 창이열립니다.

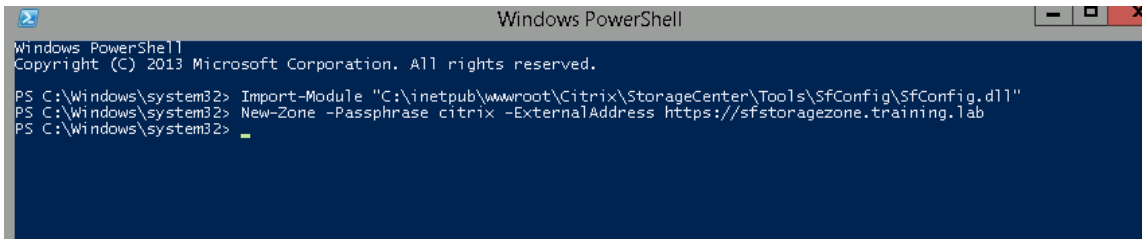
4. PowerShell 창에서다음을입력합니다.

```
1 Import-Module ”C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll”
2 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
3 <!--NeedCopy-->
```

여기서:

Passphrase: 사이트에할당할암호입니다. 암호를기록합니다. 컨트롤러에서암호를복구할수없습니다. 암호를분실한 경우 StorageZones Controller 를다시설치할수없습니다. 추가 StorageZones Controller 를 StorageZone 에연결하거나서버에장애가발생하는경우 StorageZone 을복구해야합니다.

ExternalAddress: StorageZones Controller 서버의외부 FQDN(정규화된도메인이름) 입니다.



이제기본 StorageZones Controller 가준비되었습니다.

StorageZone 커넥터를만들기위해 XenMobile 에로그인하기전: 해당되는경우다음구성을완료합니다.

StorageZone 에대한프록시서버지정

위임을위해 StorageZones Controller 를신뢰하도록도메인컨트롤러구성

보조 StorageZones Controller 를 StorageZone 에연결

StorageZone 커넥터를만들려면XenMobile 에서 StorageZones Controller 연결정의를참조하십시오.

보조 **StorageZones Controller** 를 **StorageZone** 에연결

StorageZone 에고가용성을구성하려면영역에적어도두개의 StorageZones Controller 를연결합니다. 보조 StorageZones Controller 를영역에가입시키려면보조서버에 StorageZones Controller 를설치합니다. 그런다음해당컨트롤러를기본컨트롤러의영역에가입시킵니다.

1. 주서버에가입시키려는 StorageZones Controller 서버에서 PowerShell 창을엽니다.
2. PowerShell 창에서다음을입력합니다.

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

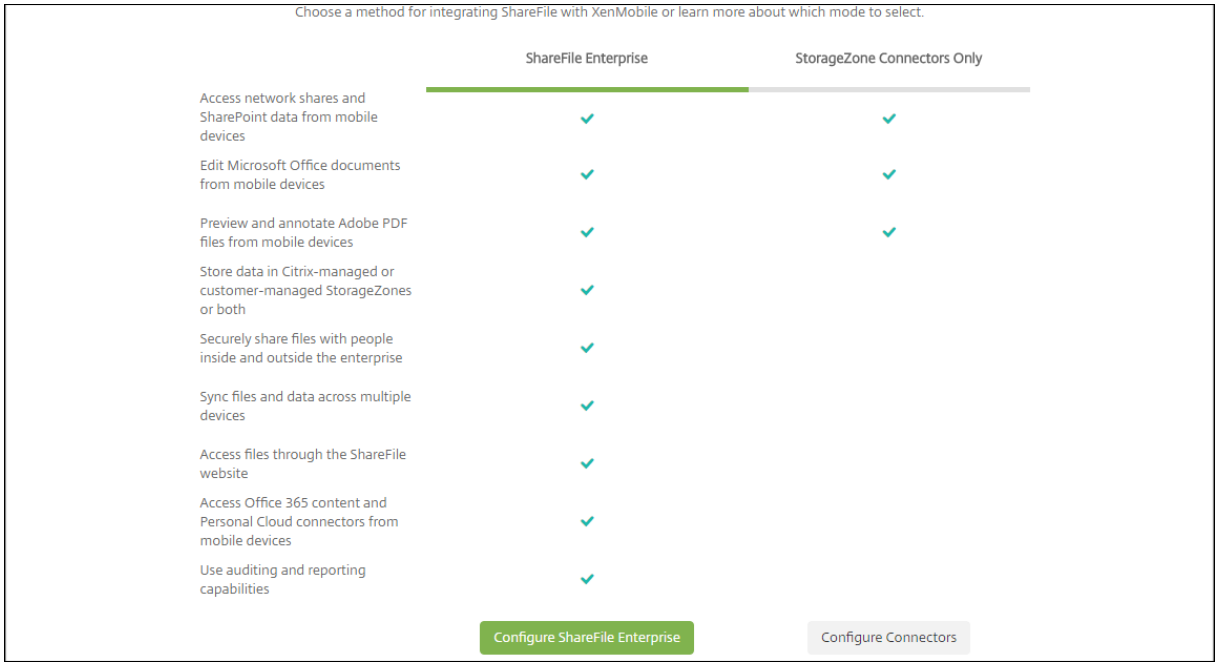
   예:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

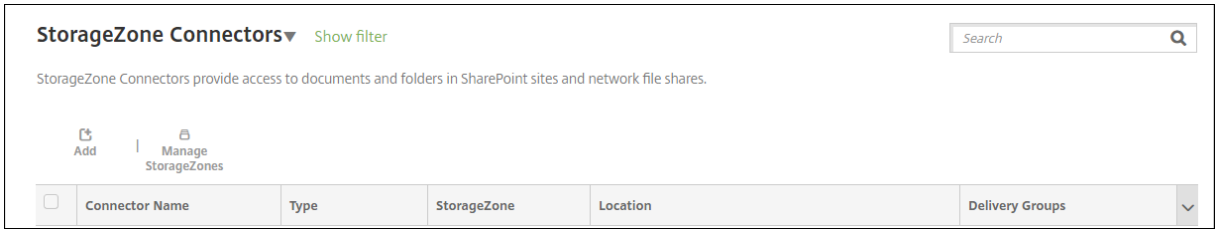
XenMobile 에서 **StorageZones Controller** 연결정의

StorageZone 커넥터를추가하기전에 StorageZone 커넥터에대해사용하도록설정한각 StorageZone Controller 에대한연결정보를구성합니다. 이섹션에설명된대로또는커넥터를추가할때 StorageZones Controller 를정의할수있습니다.

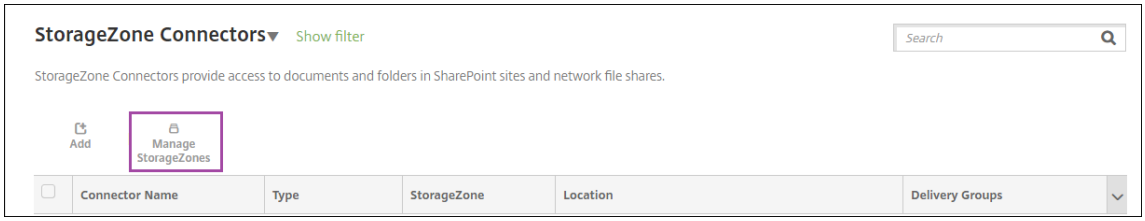
구성 **> ShareFile** 페이지를처음방문하면페이지에 XenMobile 에서 Enterprise 계정을사용할때와 StorageZone 커넥터를사용할때의차이점이요약되어있습니다.



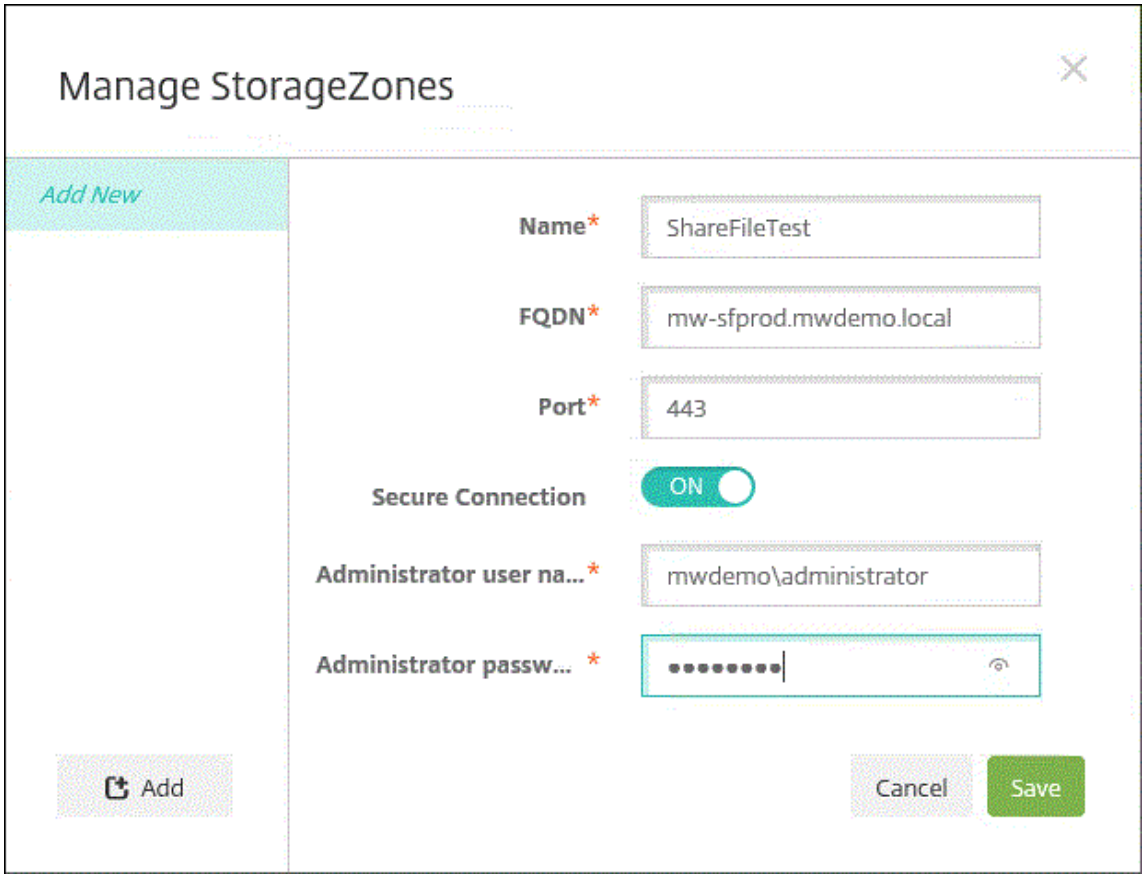
커넥터구성을클릭하여이문서의구성단계를계속수행합니다.



1. 구성 **> ShareFile** 에서 **StorageZone** 관리를클릭합니다.



2. **StorageZone** 관리에서연결정보를추가합니다.



- 이름**:** XenMobile 에서 StorageZone 을식별하는데사용되는 StorageZone 의설명적인이름입니다. 이름에 공백이나특수문자를사용하지마십시오.
- **FQDN** 및포트**:** XenMobile Server 에서연결할수있는 StorageZones Controller 의 FQDN(정규화된도메인이름) 및포트번호입니다.

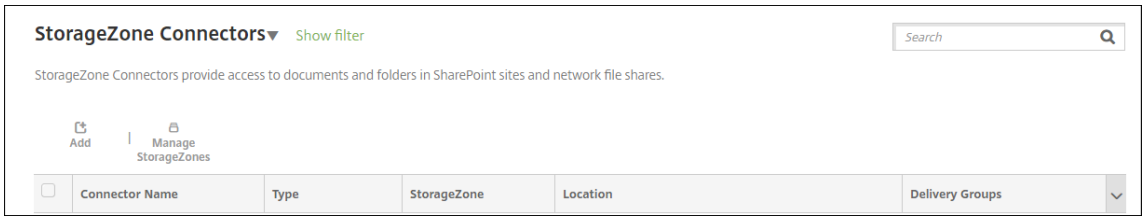
- 보안연결**:** StorageZones Controller 에연결하기위해 SSL 을사용하는경우기본설정인켜짐을사용합니다. 연결에 SSL 을사용하지않는다면이설정을꺼짐으로변경합니다.
- 관리자사용자이름및 관리자암호**:** 관리자서비스계정사용자이름 (domain\admin 형식) 및암호입니다. 또는 StorageZones Controller 에대한읽기및쓰기권한이있는사용자계정입니다.

3. 저장을클릭합니다.
4. 연결을테스트하려면 XenMobile Server 가포트 443 에서 StorageZones Controller 의 FQDN(정규화된도메인이름) 에연결할수있는지확인합니다.
5. 다른 StorageZones Controller 연결을정의하려면 **StorageZone** 관리에서 추가단추를클릭합니다.

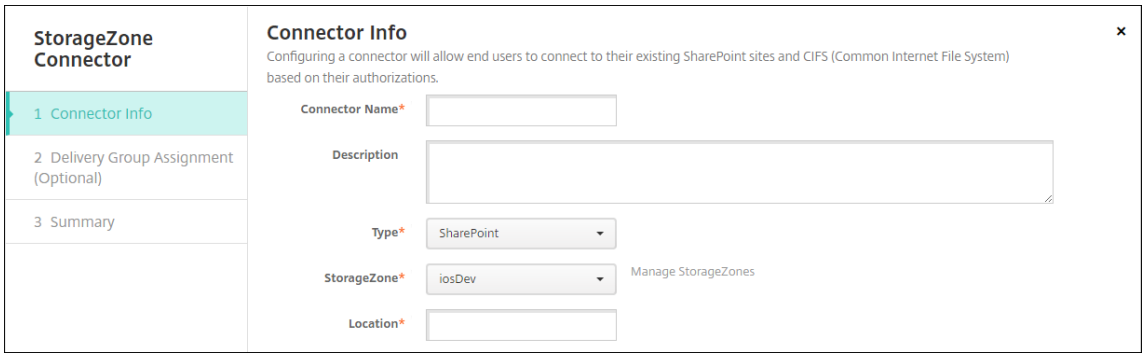
   StorageZones Controller 연결에대한정보를편집하거나삭제하려면 **StorageZone** 관리에서연결이름을선택합니다. 그런다음 편집또는 삭제를클릭합니다.

XenMobile 에서 **StorageZone** 커넥터추가

1. 구성 **> ShareFile** 로이동한다음 추가를클릭합니다.

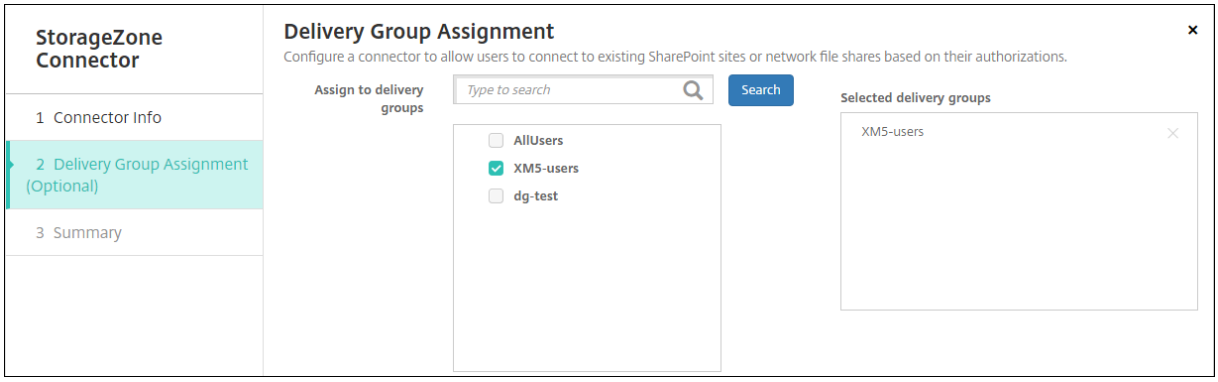


2. 커넥터정보페이지에서다음설정을구성합니다.



- 커넥터이름**:** XenMobile 에서 StorageZone 커넥터를식별하는이름입니다.
- 설명**:** 이커넥터에대한선택적인메모입니다.
- 유형**: SharePoint** 또는 네트워크를선택합니다.
- **StorageZone:** 커넥터와연결된 StorageZone 을선택합니다. StorageZone 이나열되지않으면 **StorageZone** 관리를클릭하여 StorageZones Controller 를정의합니다.
- 위치**:** SharePoint 의경우 SharePoint 루트수준사이트, 사이트컬렉션또는문서라이브러리의 URL 을 `https://sharepoint.company.com` 형식으로지정합니다. 네트워크공유의경우 UNC(Uniform Naming Convention) 경로의정규화된도메인이름을 \\server\share 형식으로지정합니다.

3. 배달그룹할당페이지에서선택적으로커넥터를배달그룹에할당합니다. 또는 구성 **>** 배달그룹을사용하여커넥터를배달그룹에연결할수있습니다.



1. 요약페이지에서구성한옵션을검토할수있습니다. 구성을조정하려면 뒤로를클릭합니다.
2. 저장을클릭하여커넥터를저장합니다.
3. 커넥터를테스트합니다.

   a) Citrix Files 클라이언트를래핑하는경우다음을수행합니다.

      - 네트워크액세스정책을 내부네트워크로터널링됨으로설정합니다.

      이작동모드에서는 XenMobile MDX 프레임워크가 Citrix Files 클라이언트의모든네트워크트래픽을가로챕니다. 트래픽은앱전용 Micro VPN 을사용하여 Citrix Gateway 를통해리디렉션됩니다.

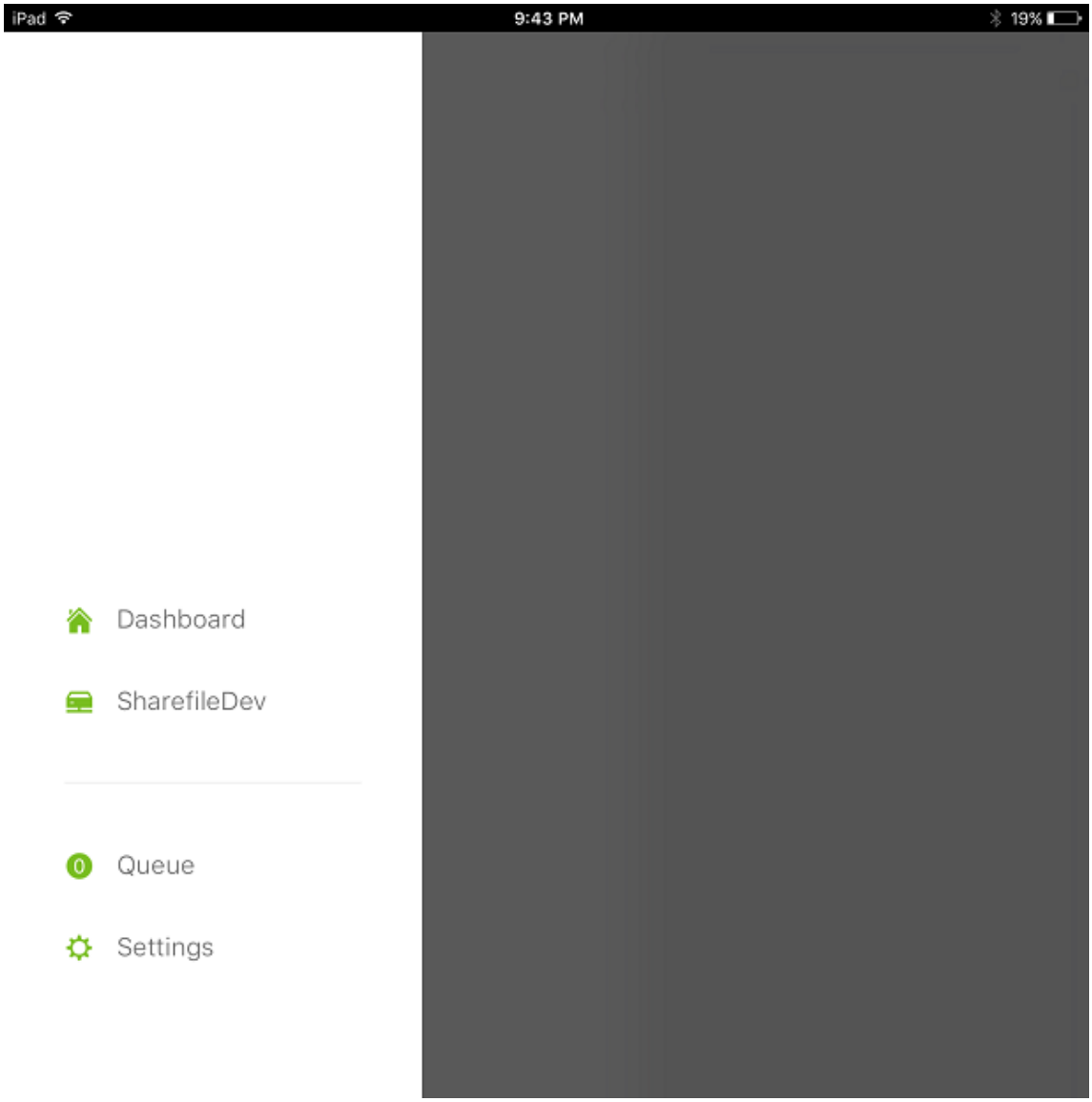
      - 기본설정 VPN 모드정책을 터널링됨 **-** 웹 **SSO** 로설정합니다.

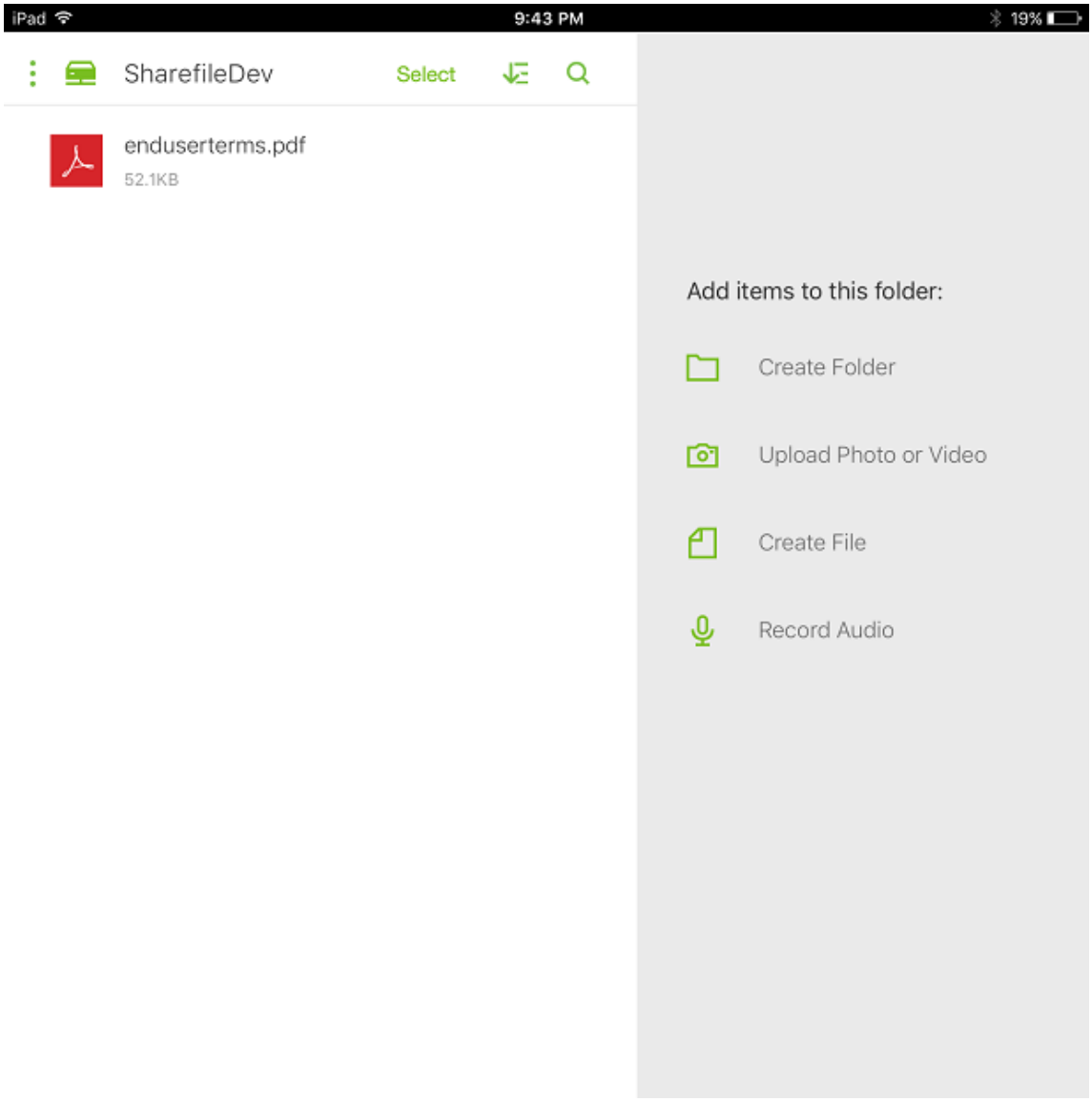
      이터널링모드에서는 MDX 프레임워크가 MDX 앱의 SSL/HTTP 트래픽을종료합니다. 그런다음 MDX 가사용자대신내부연결로의새연결을시작합니다. 이정책설정은 MDX 프레임워크가웹서버에서발행된인증챌린지를감지하고이에응답할수있게합니다.

   b) Citrix Files 클라이언트를 XenMobile 에추가합니다. 자세한내용은 Citrix Files for Endpoint Management 클라이언트통합및제공을참조하십시오.

   c) 지원되는장치에서 Citrix Files 및커넥터에대한 Single Sign-On 을확인합니다.

   다음샘플에서 ShareFileDev 가커넥터이름입니다.

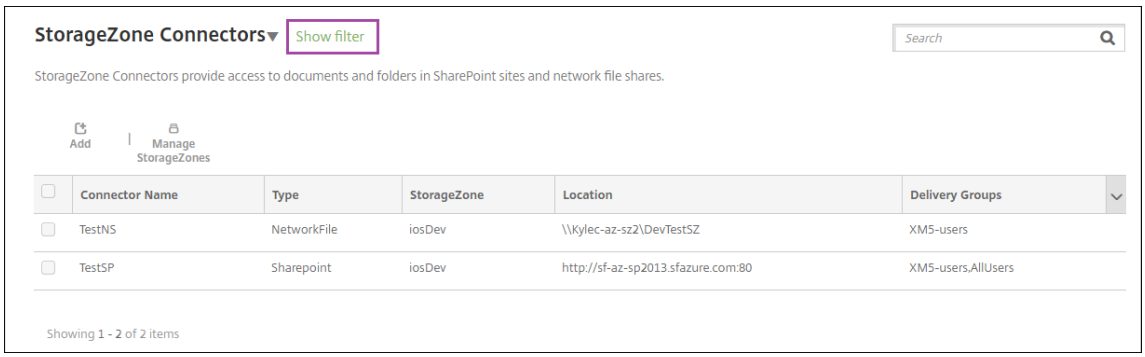




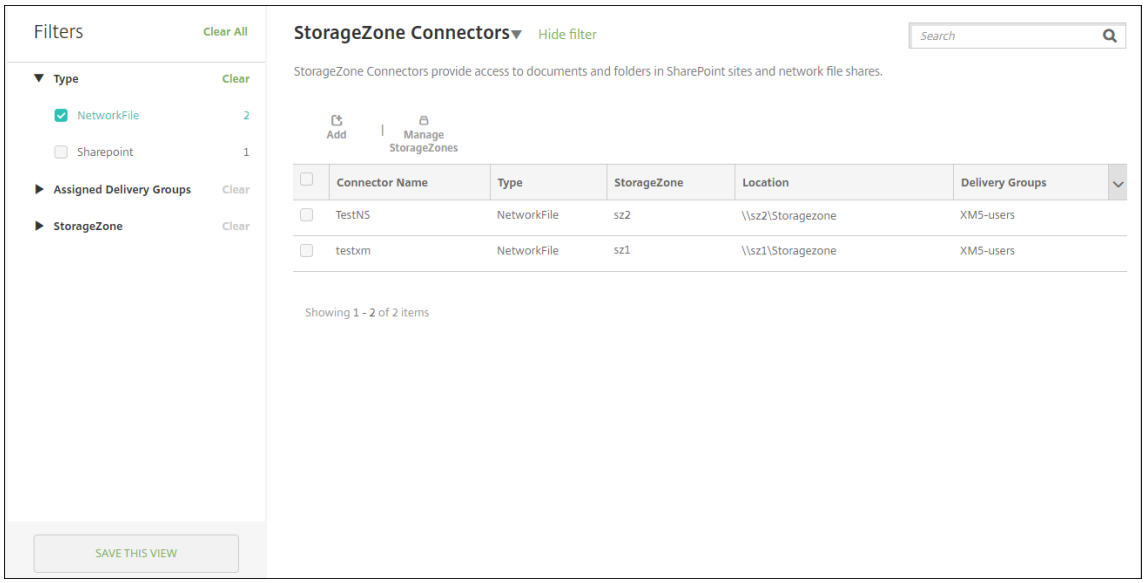
StorageZone 커넥터목록필터링

커넥터유형, 할당된배달그룹및 StorageZone 을기준으로 StorageZone 커넥터의목록을필터링할수있습니다.

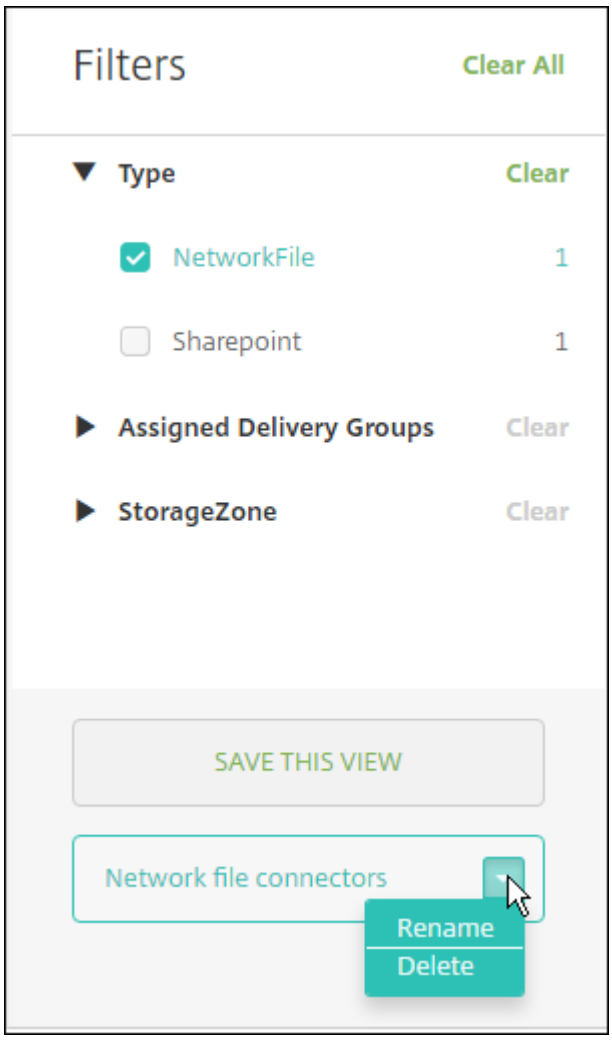
1. 구성 **> ShareFile** 로이동한다음 필터표시를클릭합니다.



2. 필터머리글을확장하여선택할수있게만듭니다. 필터를저장하려면 이보기저장을클릭하고필터이름을입력한다음 저장을클릭합니다.



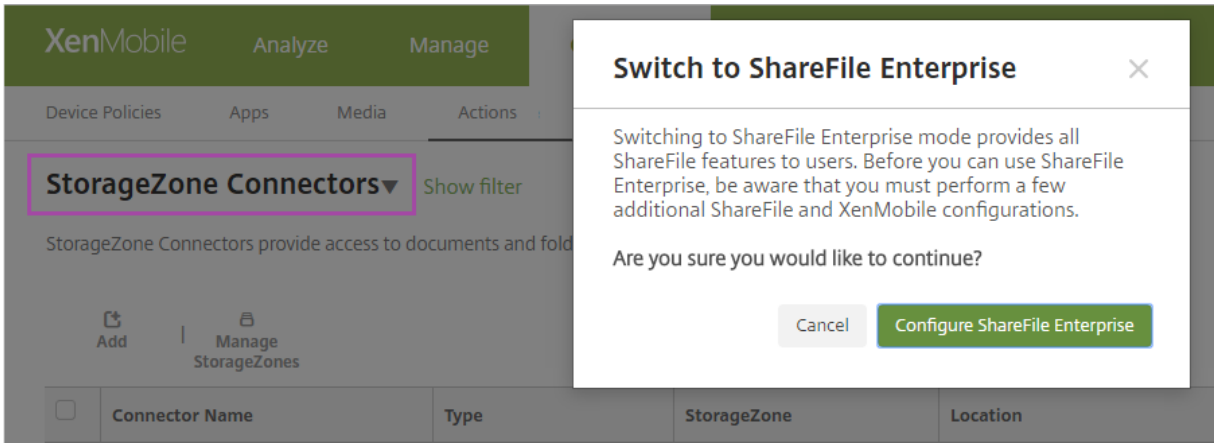
3. 필터이름을바꾸거나필터를삭제하려면필터이름옆의화살표아이콘을클릭합니다.



Citrix Files 로전환

StorageZone 커넥터를 XenMobile 과통합한후나중에전체 Enterprise 기능집합으로전환할수있습니다. Citrix Files 기능집합을사용하려면 XenMobile Enterprise Edition 이필요합니다. XenMobile 은기존 StorageZone 커넥터통합설정을유지합니다.

구성 **> ShareFile** 로이동하고 **StorageZone** 커넥터드롭다운메뉴를클릭한다음 **ShareFile Enterprise** 구성을클릭합니다.



Citrix Files 를구성하는방법에대한정보는 Citrix Files 를사용하는 Single Sign-on 을위한 SAML을참조하십시오.

HDX 앱용 SmartAccess

January 5, 2022

이기능을사용하면장치속성, 장치의사용자속성또는장치에설치된응용프로그램을기반으로 HDX 앱에대한액세스권한을제어할수 있습니다. 장치를규정위반으로표시하여해당장치액세스를거부하는자동화된동작을설정하여이기능을사용합니다. 이기능과함께 사용되는 HDX 앱은 Virtual Apps and Desktops 에서규정위반장치에대한액세스를거부하는 SmartAccess 정책을사용하여구성됩니다. XenMobile 은서명되고암호화된태그를사용하여장치상태를 StoreFront 에전달합니다. 그러면 StoreFront 가앱의액세스제어정책에따라액세스를허용하거나거부합니다.

이기능을사용하려면배포에다음이포함되어야합니다.

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 또는 3.8
- StoreFront 서버에서 HDX 앱을집계하도록구성된 XenMobile Server
- 태그서명및암호화에사용되는 SAML 인증서가구성된 XenMobile Server. 동일한인증서가개인키가없는상태로 StoreFront 서버에업로드됩니다.

이기능을사용하려면:

- StoreFront 저장소에대한 XenMobile Server 인증서구성
- 필요한 SmartAccess 정책을사용하여하나이상의 Virtual Apps and Desktops 배달그룹구성
- XenMobile 에서자동화된작업설정

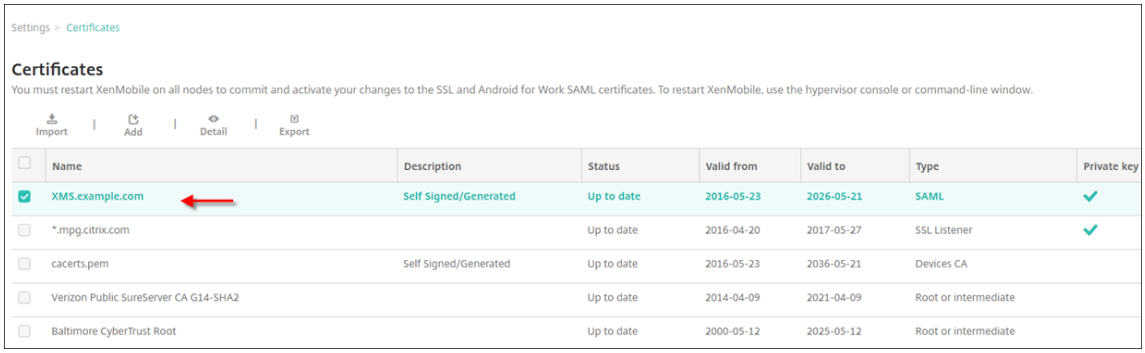
XenMobile Server 인증서를내보내고구성하여 StoreFront 저장소에업로드

SmartAccess 는서명되고암호화된태그를사용하여 XenMobile 및 StoreFront 서버간에통신합니다. 이통신을사용하도록 설정하려면 XenMobile Server 인증서를 StoreFront 저장소에추가합니다.

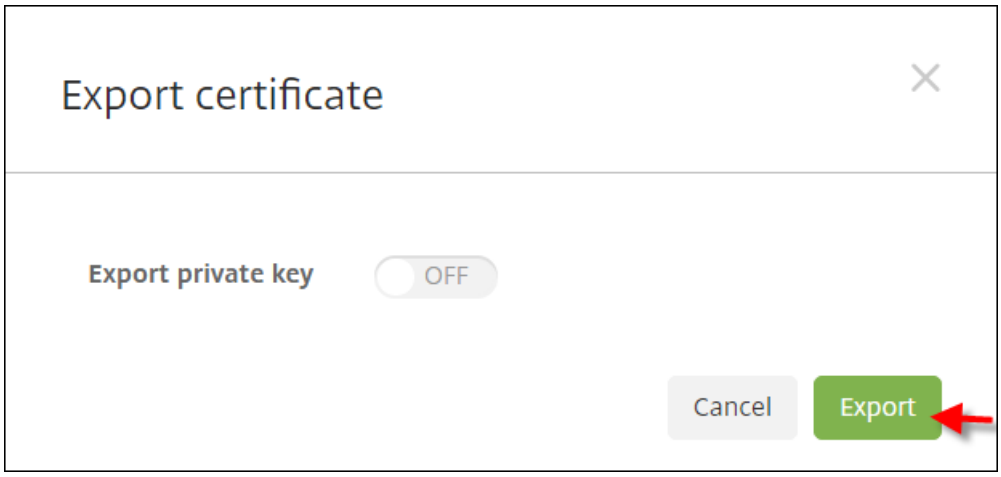
XenMobile 이도메인및인증서기반인증을사용하도록설정된경우 StoreFront 및 XenMobile 의통합에대한자세한내용은 Support Knowledge Center를참조하십시오.

XenMobile Server 에서 **SAML** 인증서내보내기

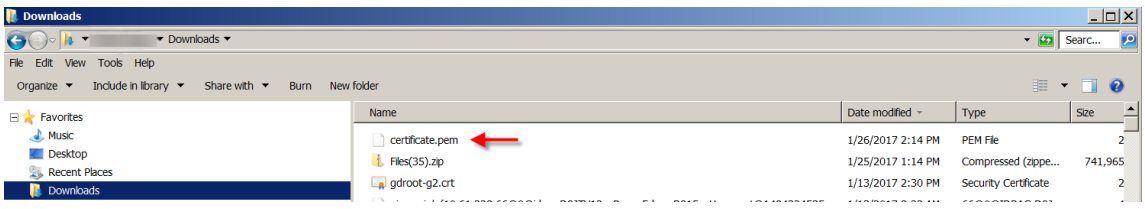
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다. 인증서를클릭합니다.
2. XenMobile Server 의 SAML 인증서를찾습니다.



3. 개인키내보내기가 꺼짐으로설정되어있는지확인합니다. 내보내기를클릭하여인증서를다운로드디렉터리로내보냅니다.

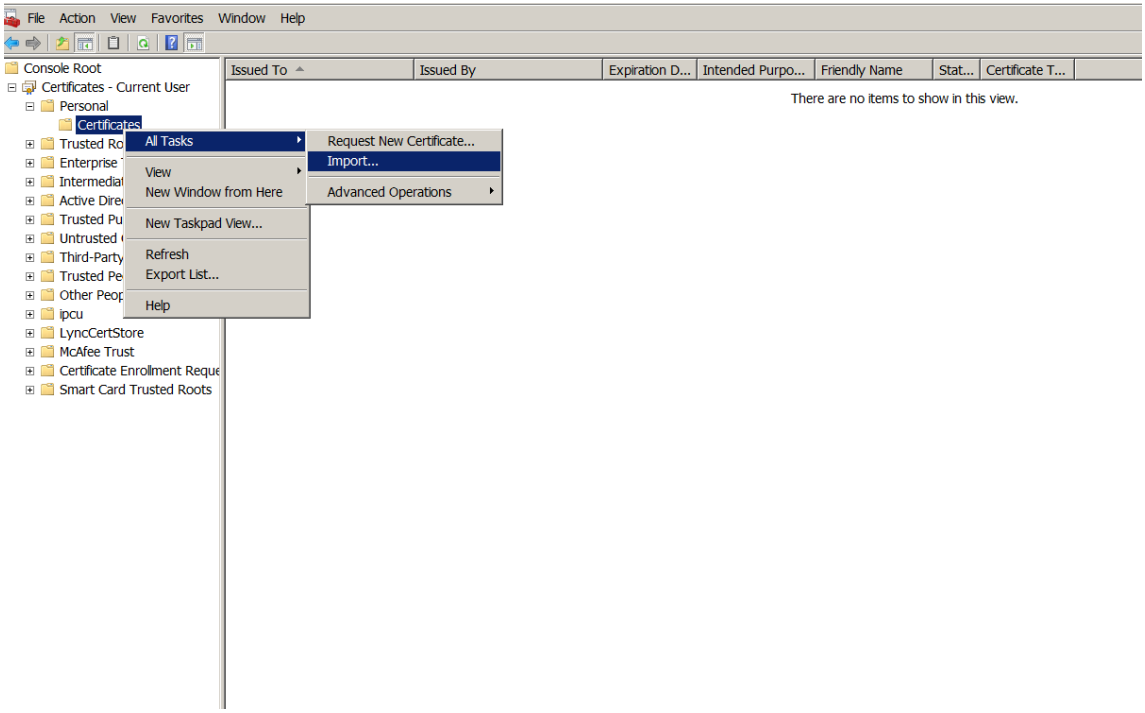


4. 다운로드디렉터리에서인증서를찾습니다. 인증서는 PEM 형식입니다.

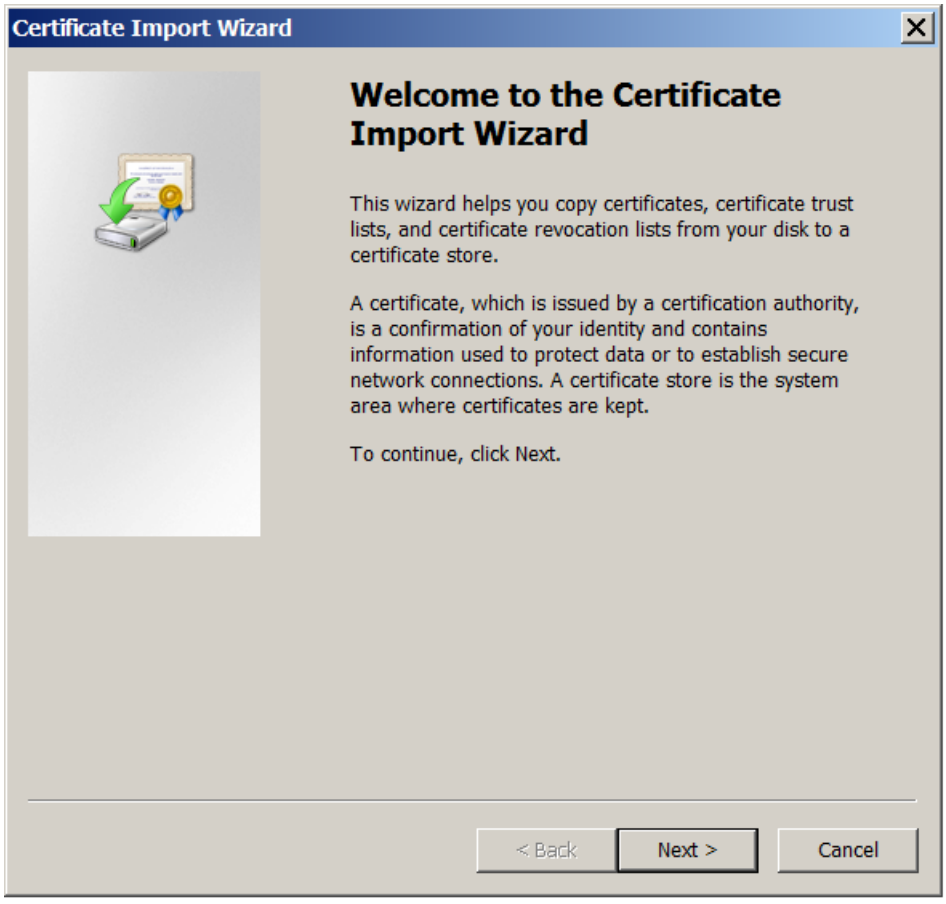


인증서를 **PEM** 에서 **CER** 로변환

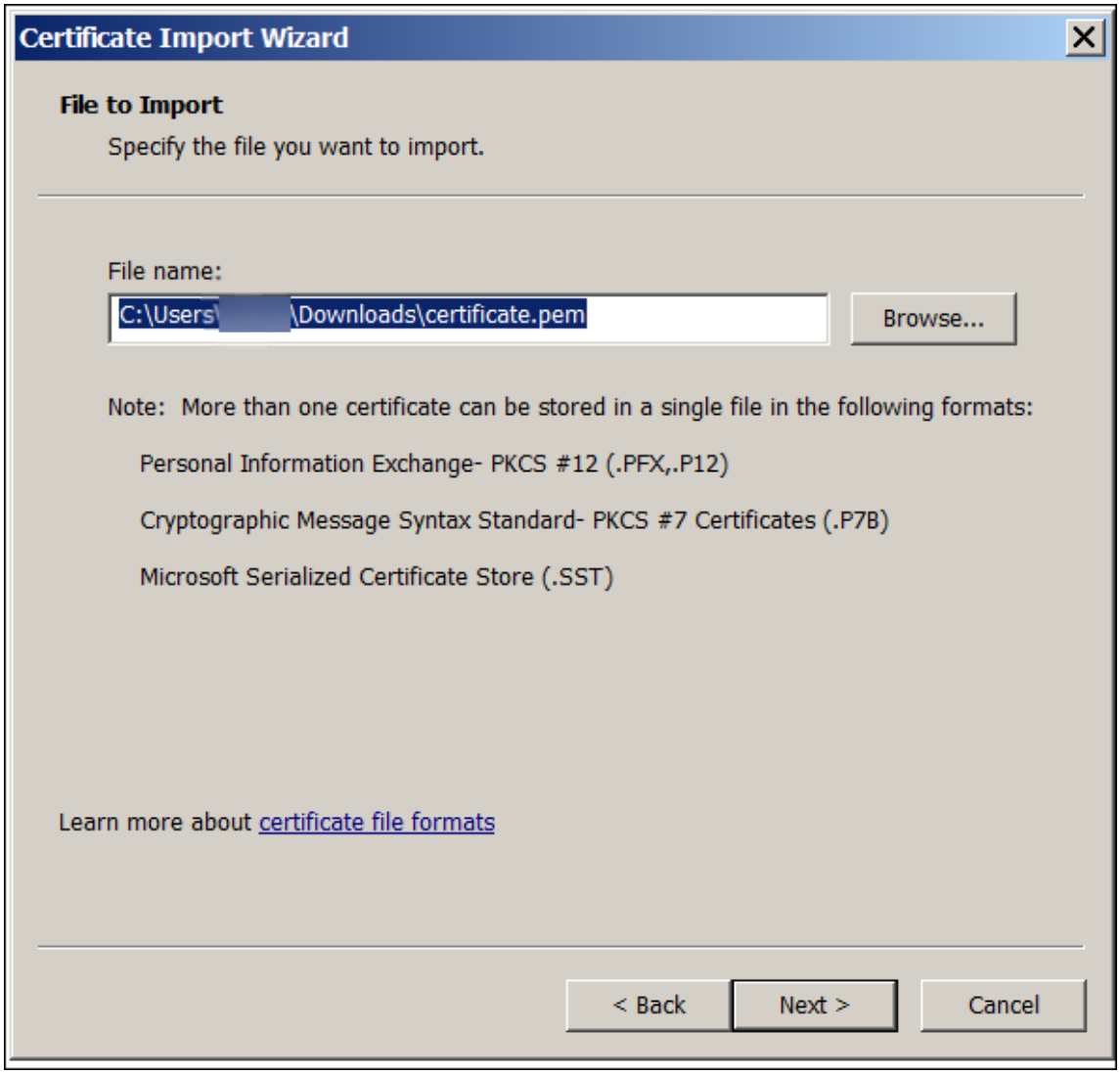
1. MMC(Microsoft Management Console) 를열고마우스오른쪽단추를클릭하여 인증서 **>** 모든작업 **>** 가져오기를 선택합니다.



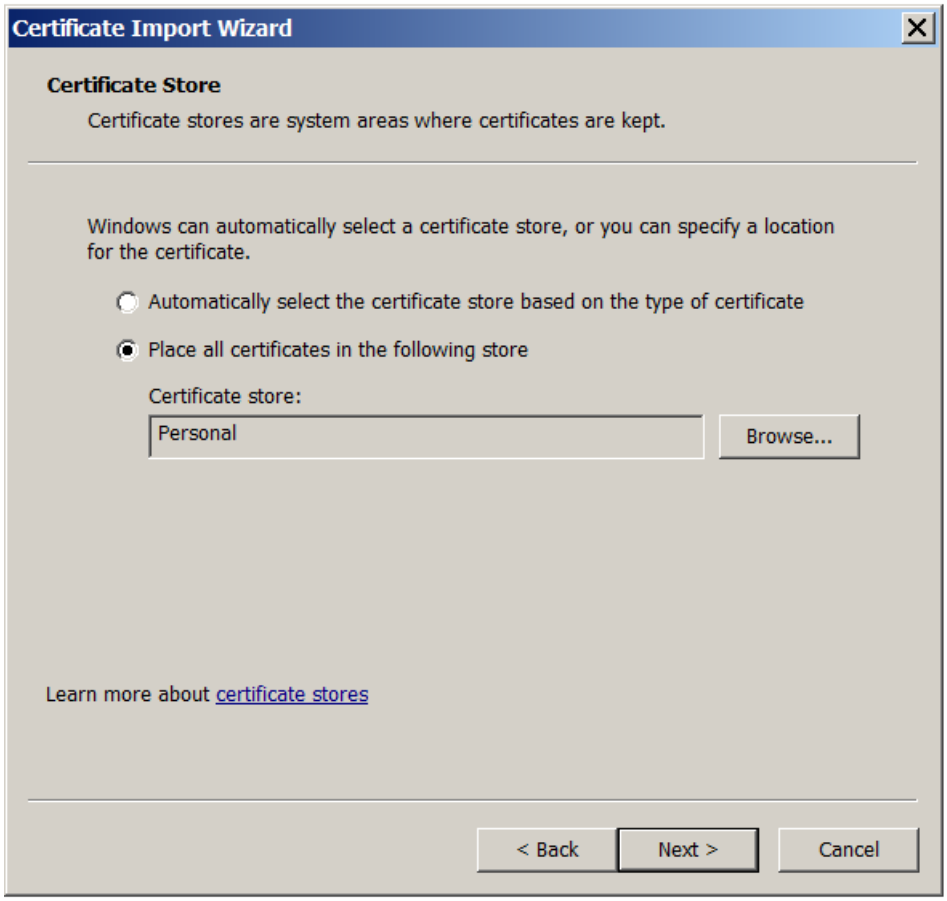
2. 인증서가져오기마법사가나타나면 다음을클릭합니다.



3. 다운로드디렉터리에있는인증서를찾아선택합니다.

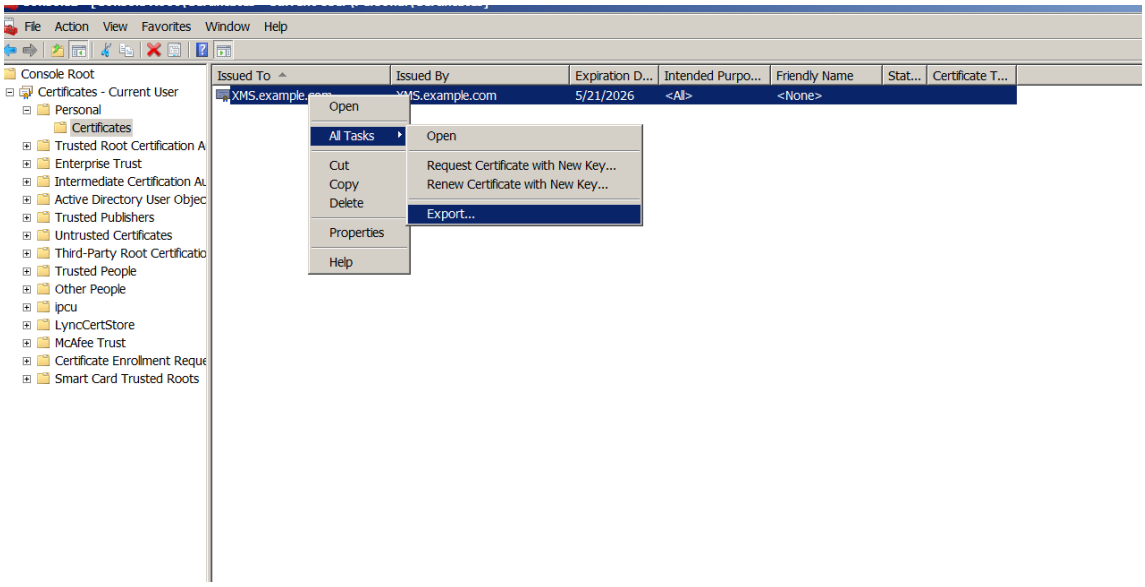


4. 모든인증서를다음저장소에저장을선택하고인증서저장소로 개인을선택합니다. 다음을클릭합니다.



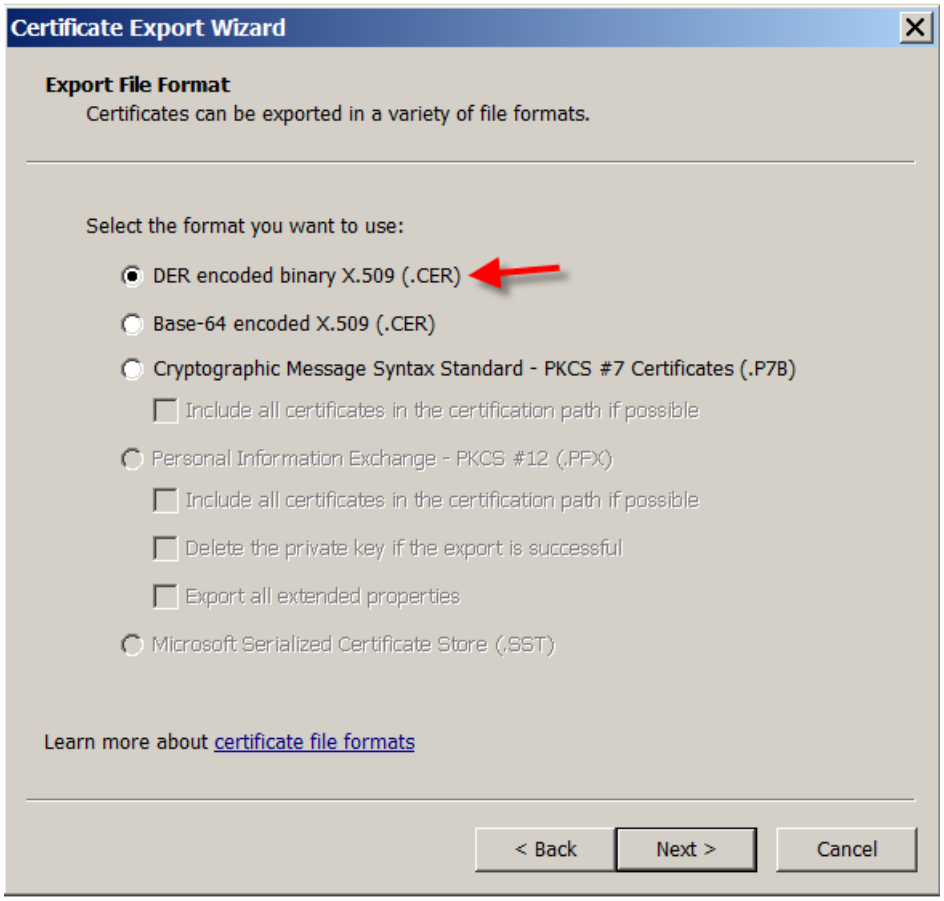
5. 선택내용을검토하고 마침을클릭합니다. 확인을클릭하여확인창을닫습니다.

6. MMC 에서인증서를마우스오른쪽단추로클릭하고 모든작업 **>** 내보내기를선택합니다.

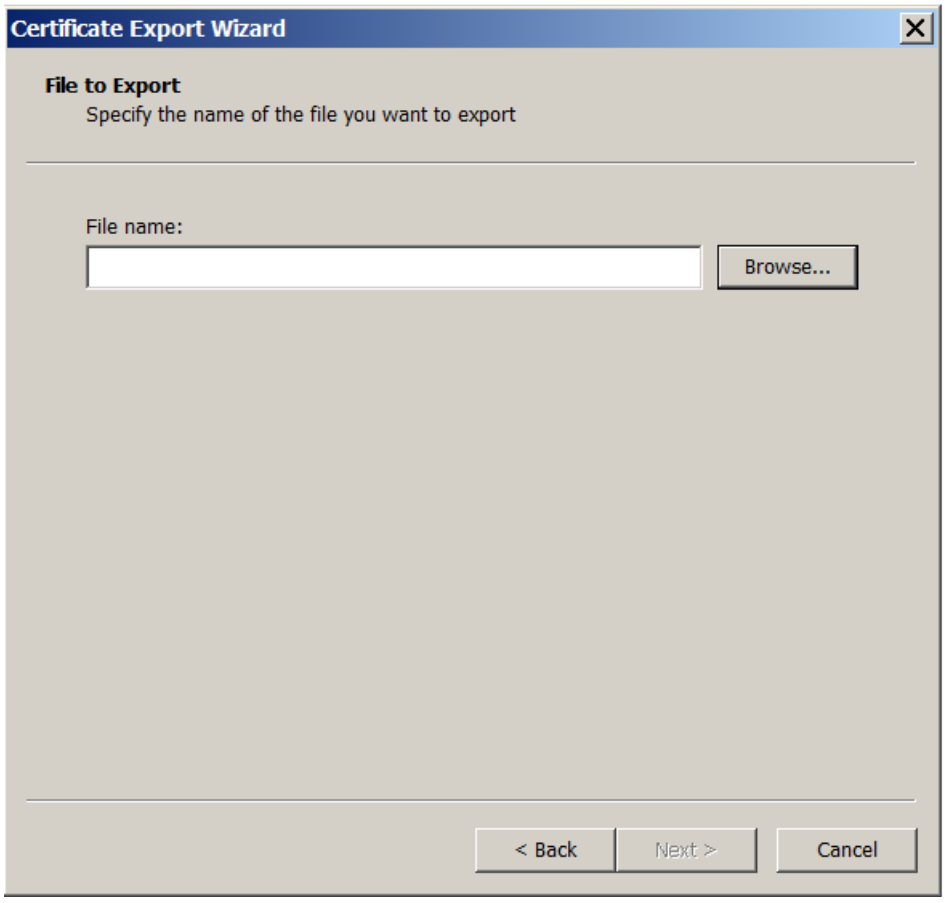


7. 인증서내보내기마법사가나타나면 다음을클릭합니다.

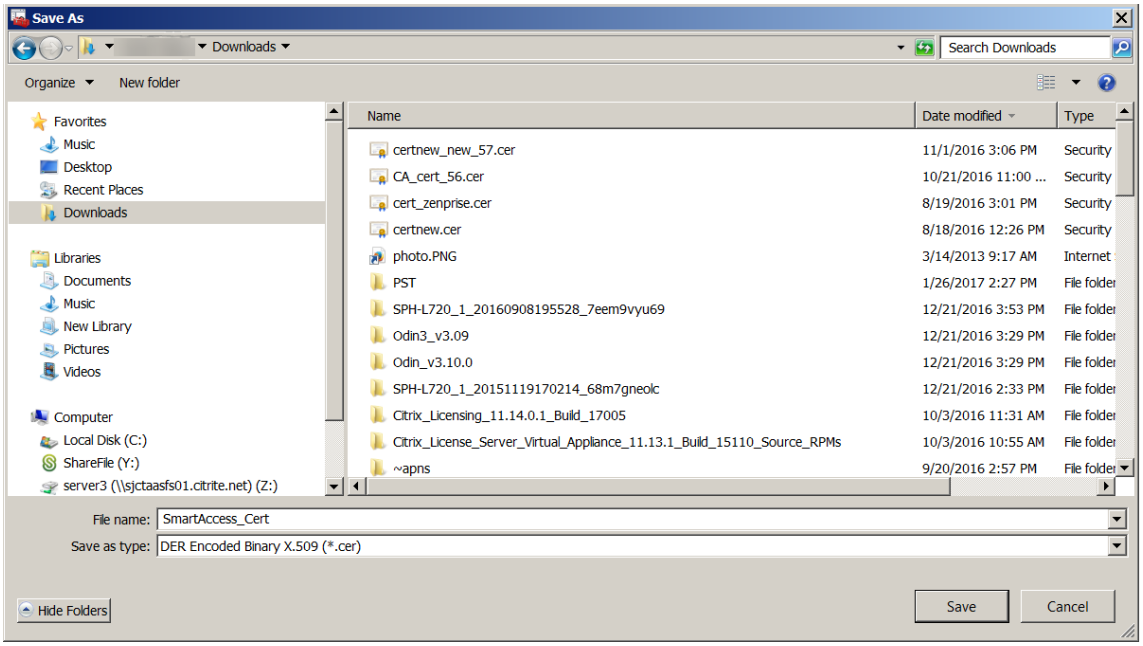
8. **DER** 로인코딩된바이너리 **X.509(.CER)** 형식을선택합니다. 다음을클릭합니다.



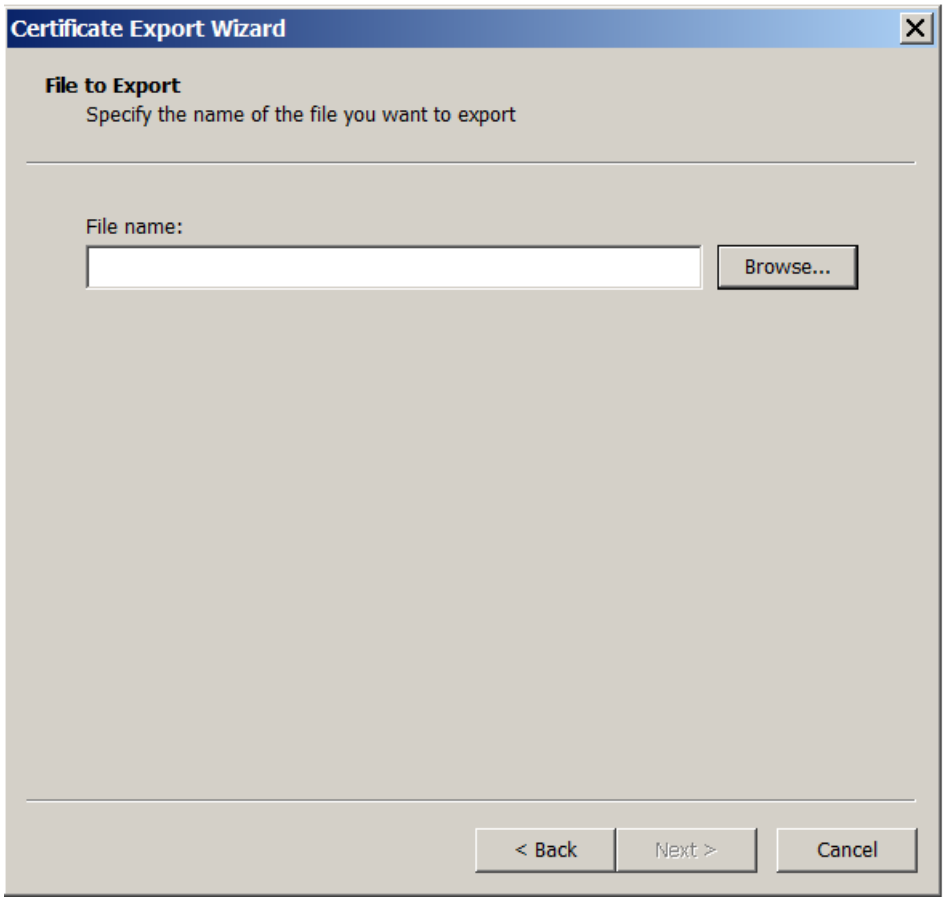
9. 인증서를찾아봅니다. 인증서의이름을입력한후 다음을클릭합니다.



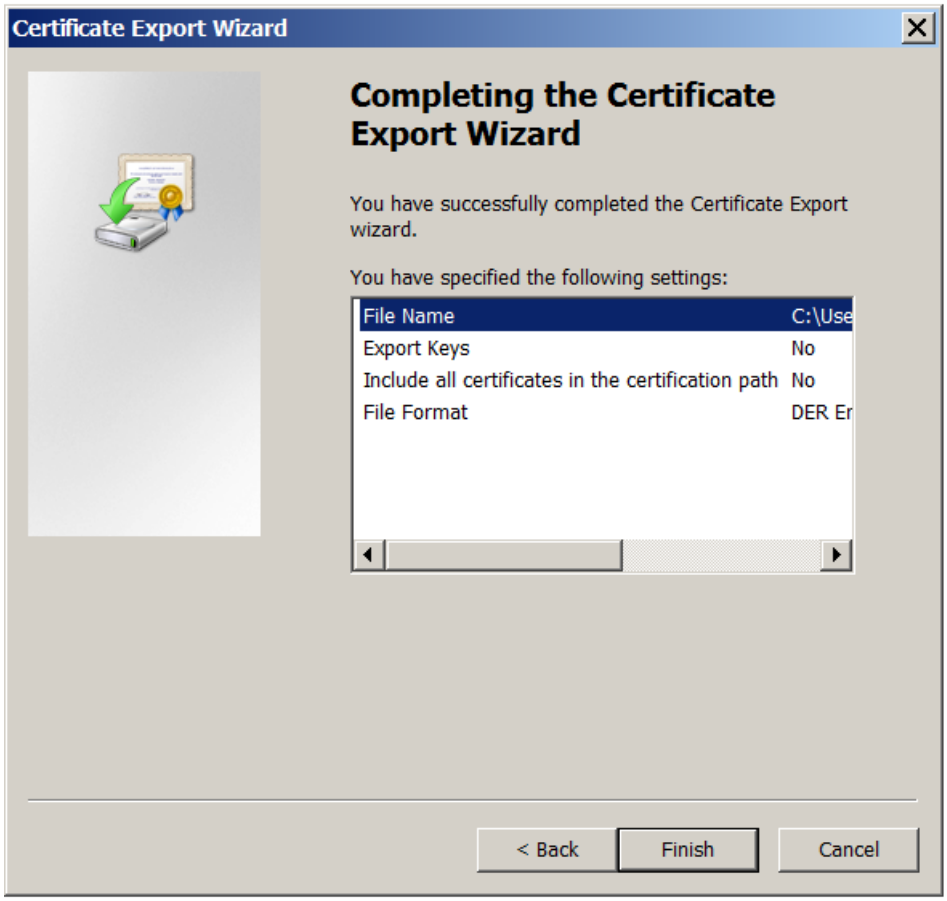
10. 인증서를저장합니다.



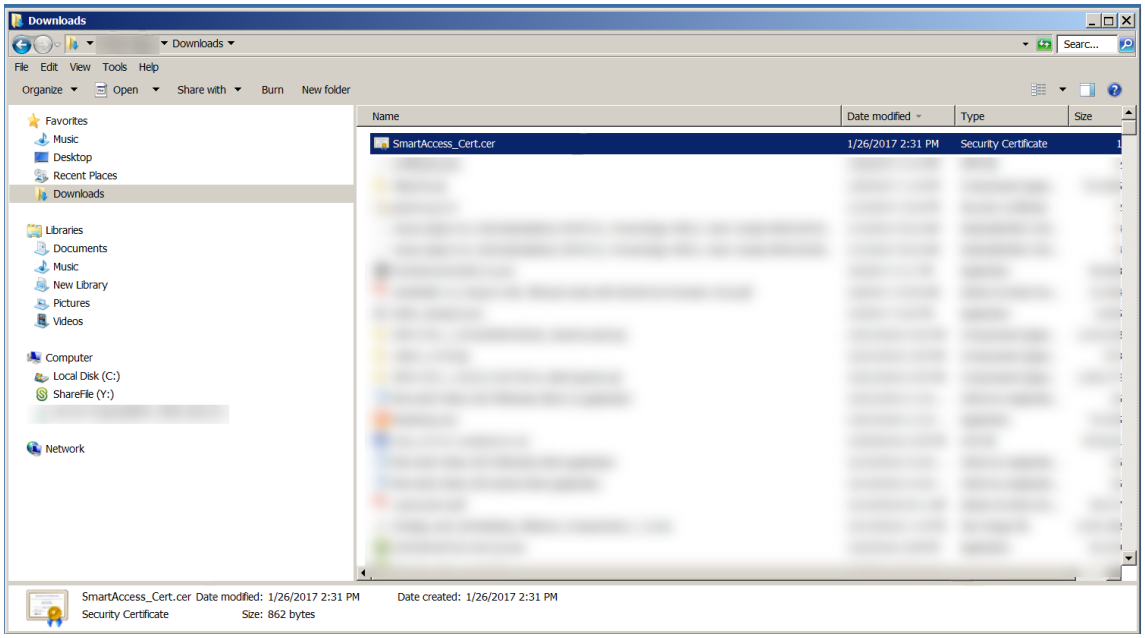
11. 인증서를찾아선택하고 다음을클릭합니다.



12. 선택내용을검토하고 마침을클릭합니다. 확인을클릭하여확인창을닫습니다.

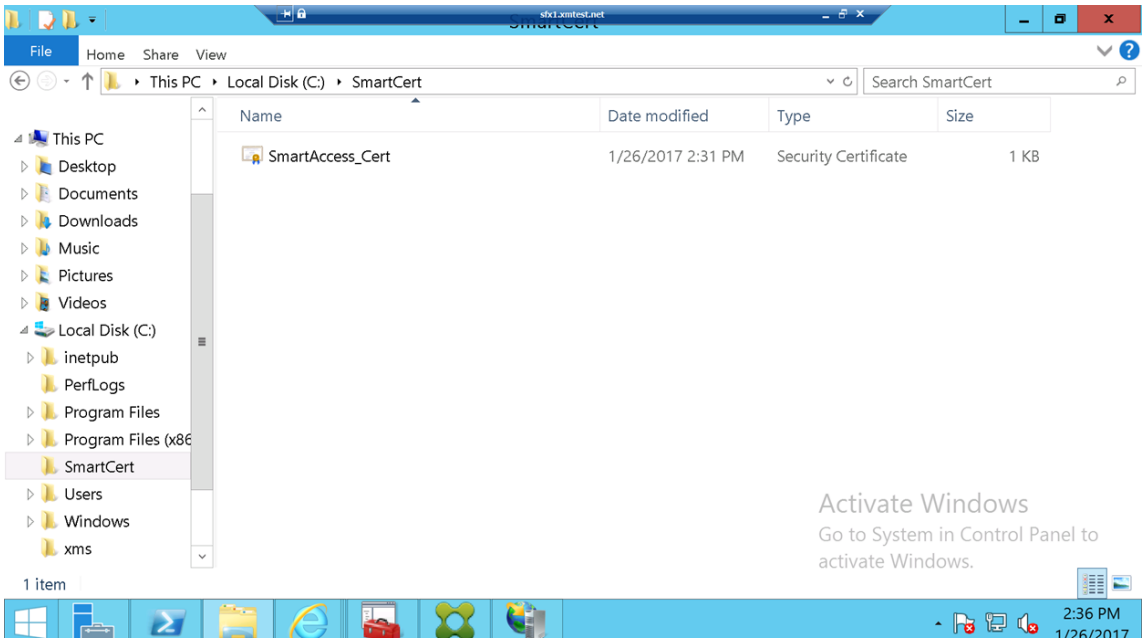


13. 다운로드디렉터리에서인증서를찾습니다. 인증서는 CER 형식입니다.



인증서를 **StoreFront** 서버에복사합니다

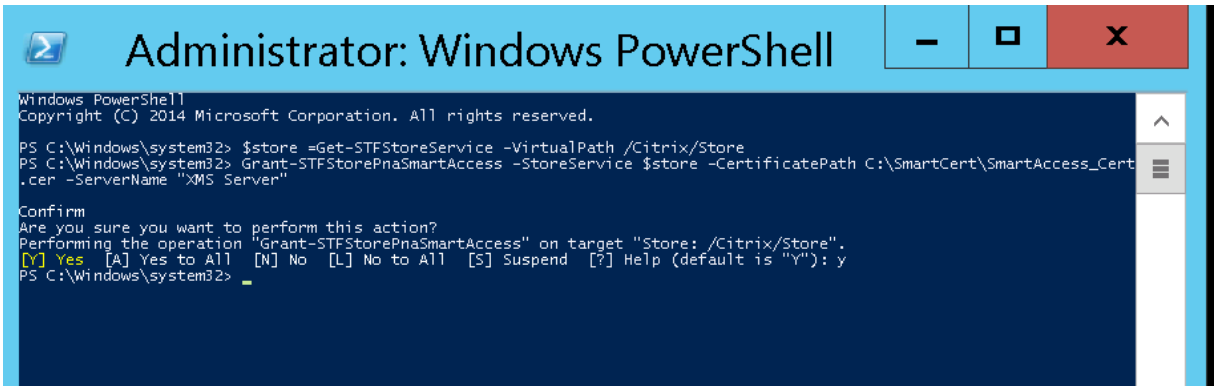
1. StoreFront 서버에서 **SmartCert** 라는폴더를만듭니다.
2. 인증서를 **SmartCert** 폴더에복사합니다.



StoreFront 저장소에서인증서구성

StoreFront 서버에서다음 PowerShell 명령을실행하여저장소에서변환된 XenMobile Server 인증서를구성합니다.

```
1     Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2 <!--NeedCopy-->
```



StoreFront 저장소에기존인증서가있는경우다음 PowerShell 명령을실행하여인증서를해지합니다.


```
    Revoke-STFStorePnaSmartAccess  -StoreService $store  -All
<!--NeedCopy-->
```

또는다음 PowerShell 명령중하나를 StoreFront 서버에서실행하여 StoreFront 저장소의기존인증서를해지할수있습니다.

- 이름으로해지:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -ServerName  “
       My XM Server”
<!--NeedCopy-->
```

- 지문으로해지:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -
       CertificateThumbprint  “ReplaceWithThumbprint”
<!--NeedCopy-->
```

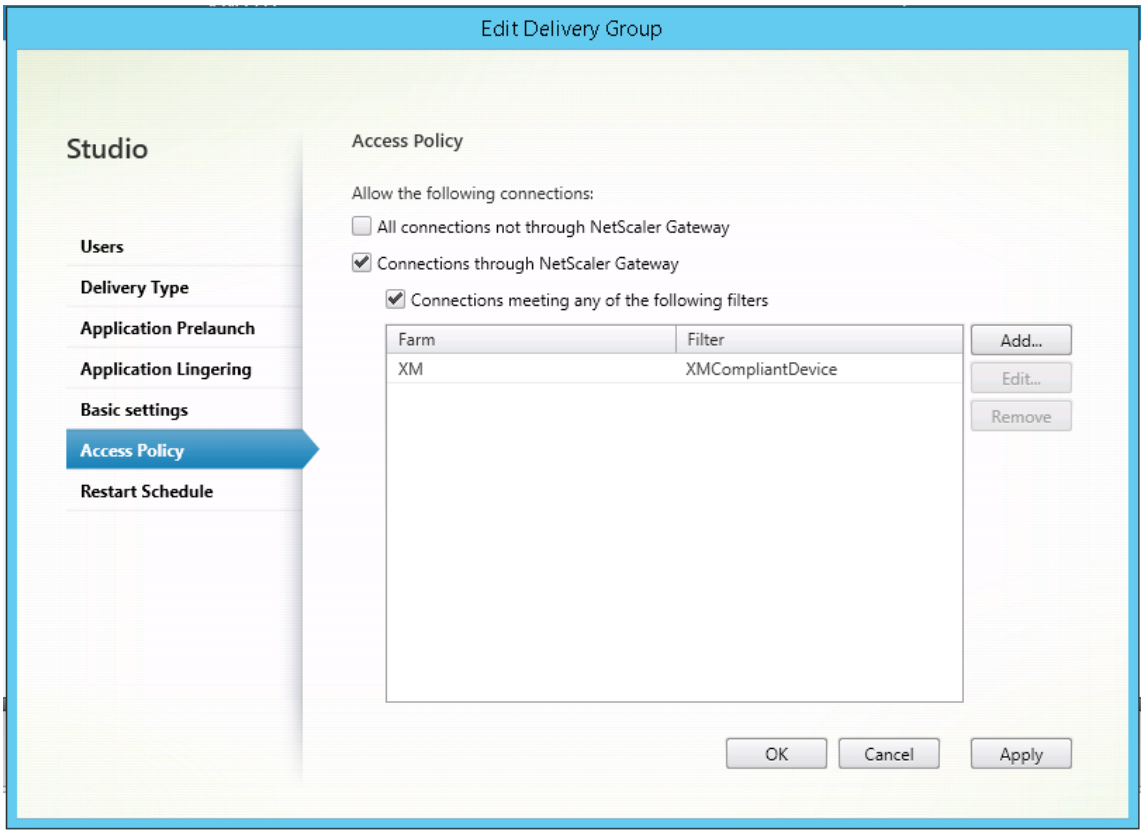
- 서버개체로해지:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess  -StoreService $store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

Virtual Apps and Desktops 에대한 SmartAccess 정책구성

필요한 SmartAccess 정책을 HDX 앱을전달하는배달그룹에추가하려면:

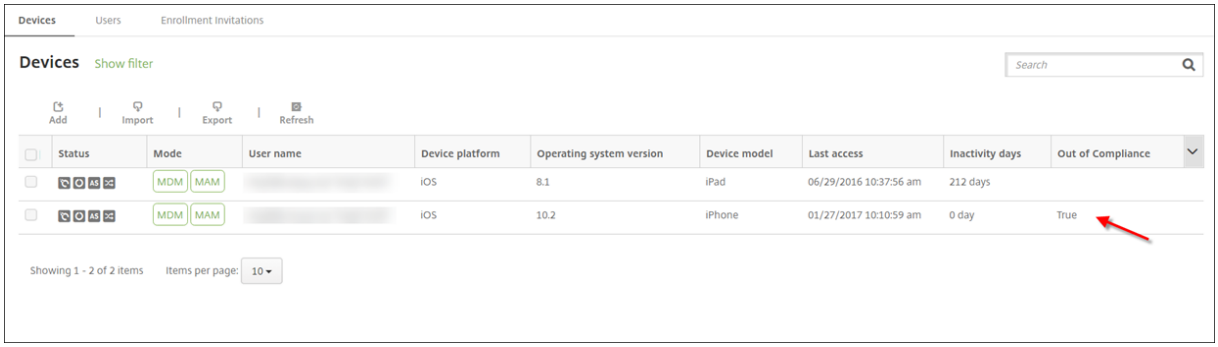
1. Virtual Apps and Desktops 서버에서 Citrix Studio 를엽니다.
2. Studio 탐색창에서 **Delivery Groups(**배달그룹**)** 를선택합니다.
3. 액세스권한을제어하려는하나이상의앱을전달하는그룹을선택합니다. **Actions(**동작**)** 창에서 **Edit Delivery Group(**배달그룹편집**)** 을선택합니다.
4. **Access Policy(**액세스정책**)** 페이지에서 **Connections through NetScaler Gateway(NetScaler Gateway** 를통한연결**)** 및 **Connection meeting any of the following(**다음과일치하는연결**)** 을선택합니다.
5. 추가를클릭합니다.
6. **Farm(**팜**)** 이 **XM** 이고 **Filter(**필터**)** 가 **XMCompliantDevice** 인액세스정책을추가합니다.



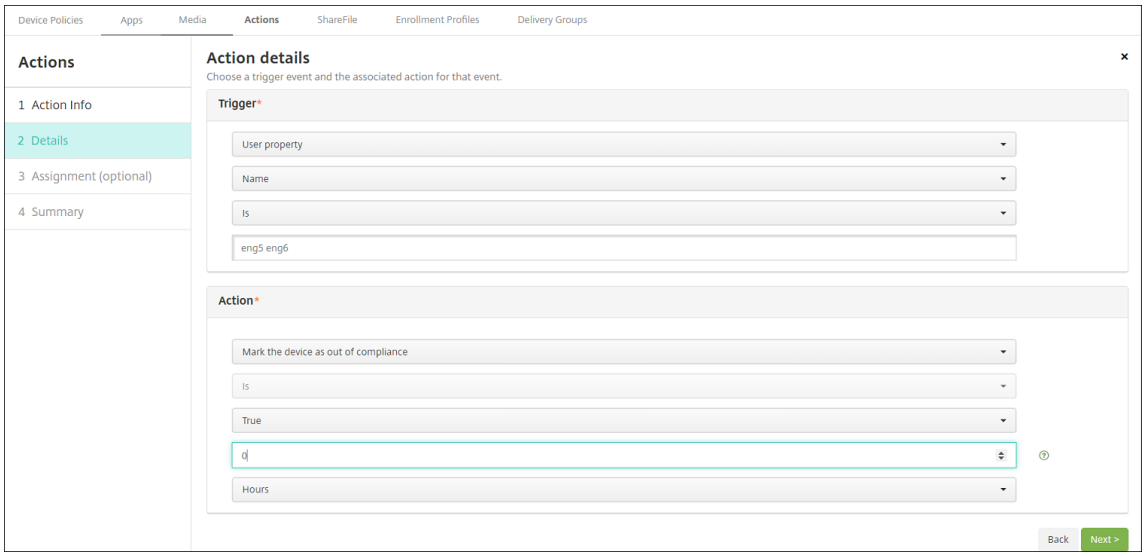
7. **Apply(**적용**)** 를클릭하여모든변경내용을적용하고창을열린채로두거나, **OK(**확인**)** 를클릭하여변경내용을적용하고창을닫습니다.

XenMobile 에서자동화된동작설정

HDX 앱에대한배달그룹에설정된 SmartAccess 정책은장치가규정을위반하면장치에대한액세스를거부합니다. 장치를규정위반으로표시하는자동화된동작을사용합니다.



1. XenMobile 콘솔에서 구성 **>** 동작을클릭합니다. 동작페이지가나타납니다.
2. 추가를클릭하여동작을추가합니다. 동작정보페이지가나타납니다.
3. 동작정보페이지에서동작의이름및설명을입력합니다.
4. 다음을클릭합니다. 동작세부정보페이지가나타납니다. 다음예에서는장치에사용자속성이름 **eng5** 또는 **eng6** 이있는경우즉시장치를규정위반으로표시하는트리거를만듭니다.

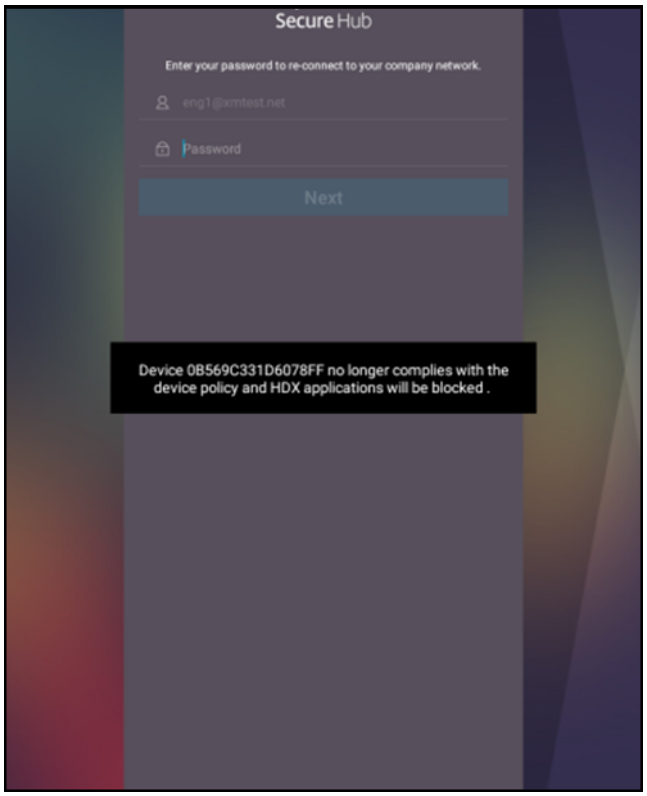


5. 트리거목록에서 장치속성, 사용자속성또는 설치된앱이름을선택합니다. SmartAccess 는이벤트트리거를지원하지않습니다.
6. 동작목록에서다음을수행합니다.
   - 장치를규정위반으로표시를선택합니다.
   - **Is** 를선택합니다.
   - **True** 를선택합니다.
   - 트리거조건이충족되면즉시장치를규정위반으로표시하도록동작을설정하려면시간프레임을 **0** 으로설정합니다.
7. 이동작을적용할 XenMobile 배달그룹을하나이상선택합니다.
8. 동작요약을검토합니다.
9. 다음을클릭한후 저장을클릭합니다.

장치가규정위반으로표시된경우 Secure Hub 저장소에더이상 HDX 앱이나타나지않습니다. 사용자는더이상앱을구독하지않습니다. 장치에알림이전송되지않으며 Secure Hub 저장소에 HDX 응용프로그램이이전에사용가능했다는내용이표시되지않습니다.

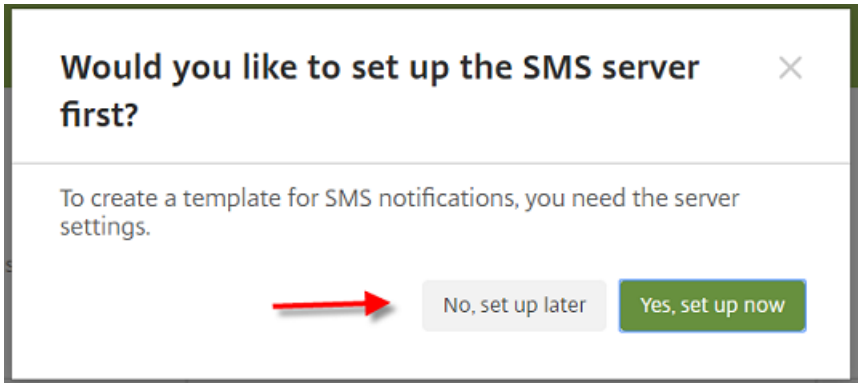
장치가규정위반으로표시될때사용자에게알리려면알림을만든다음해당알림을보내는자동화된동작을만듭니다.

이예에서는다음과같은알림을만들고장치가규정위반으로표시되는경우알림을보냅니다. “Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked.(장치일련번호또는전화번호가더이상장치정책을준수하지않으므로 HDX 응용프로그램이차단됩니다.)”



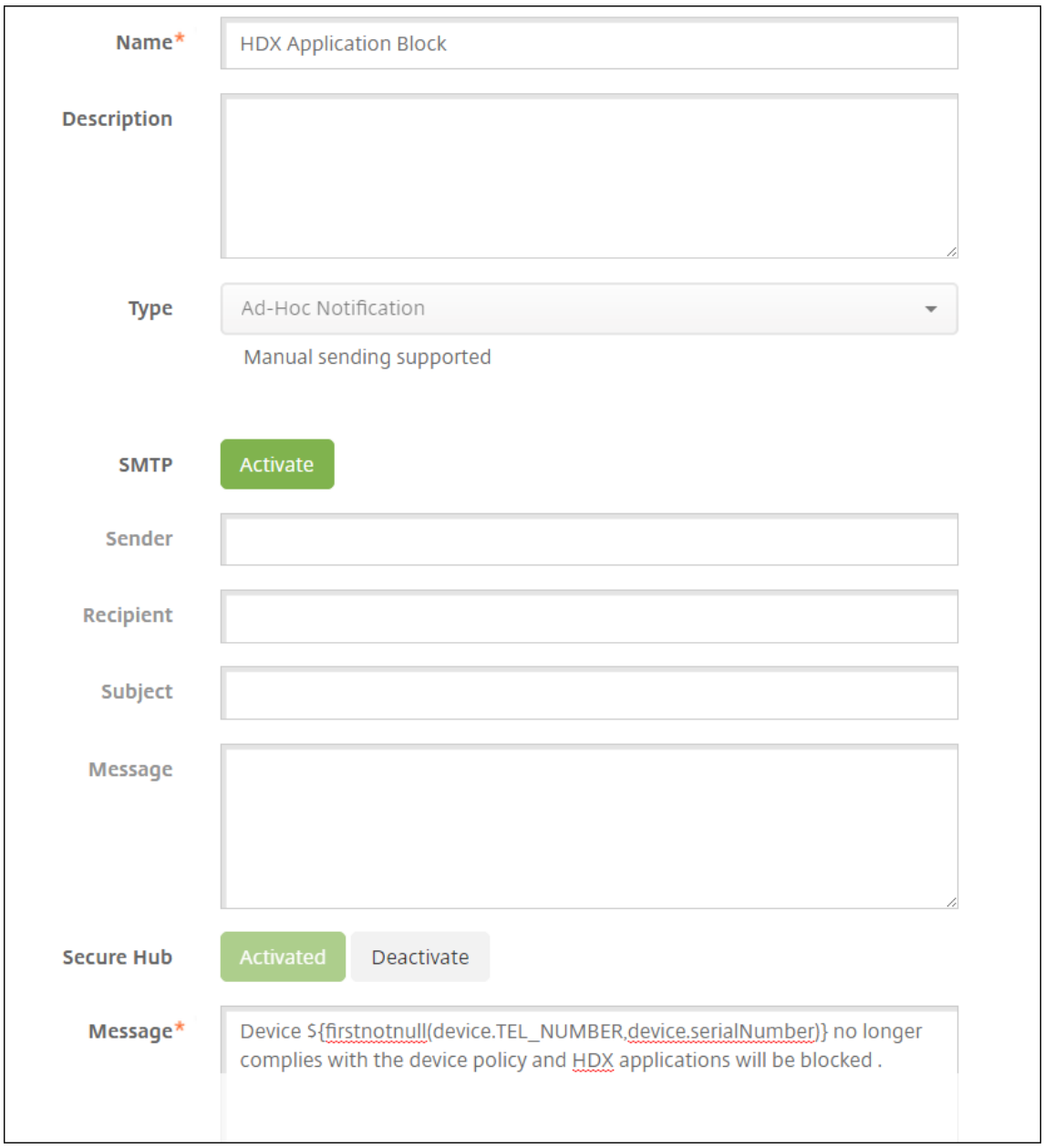
장치가규정위반으로표시될때사용자에게표시되는알림만들기

1. XenMobile 콘솔에서콘솔의오른쪽맨위에있는기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 알림템플릿을클릭합니다. 알림템플릿페이지가나타납니다.
3. 추가를클릭하여 알림템플릿페이지에추가합니다.
4. SMS 서버를먼저설정하라는메시지가나타나면 아니요**,** 나중에설정합니다를클릭합니다.



5. 다음설정을구성합니다.

   - 이름**:** HDX Application Block
   - 설명**:** Agent notification when device is out of compliance
   - 유형**:** 임시알림
   - **Secure Hub:** 활성화됨
   - 메시지**:** Device ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

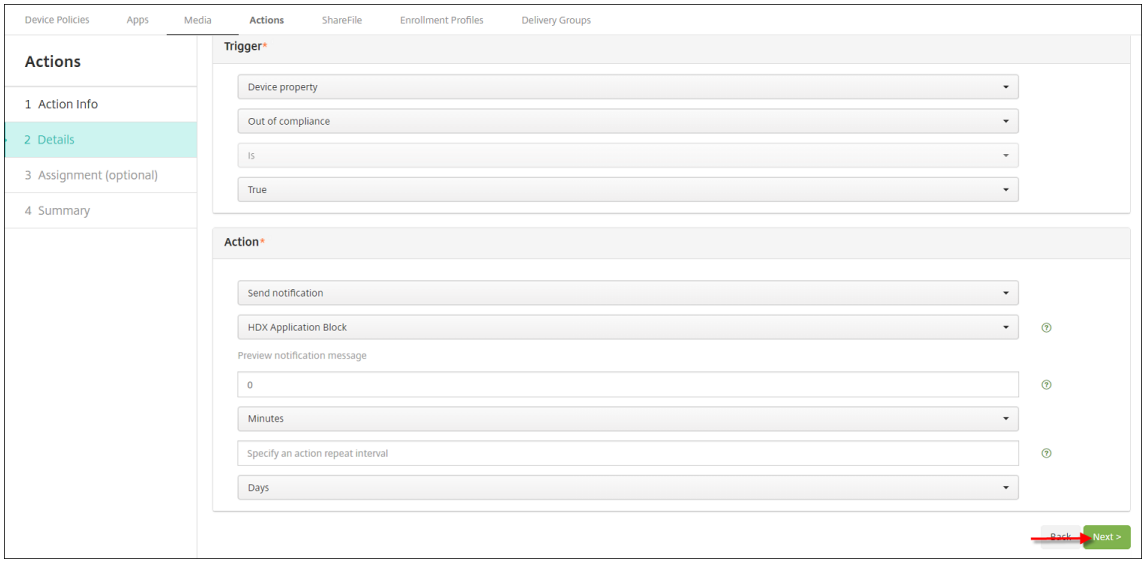


6. 저장을클릭합니다.

장치가규정위반으로표시되면알림을보내는동작만들기

1. XenMobile 콘솔에서 구성 **>** 동작을클릭합니다. 동작페이지가나타납니다.
2. 추가를클릭하여동작을추가합니다. 동작정보페이지가나타납니다.
3. 동작정보페이지에서동작의이름및설명을입력합니다.
   - 이름**:** HDX 차단알림
   - 설명: 장치가규정을위반할경우 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.

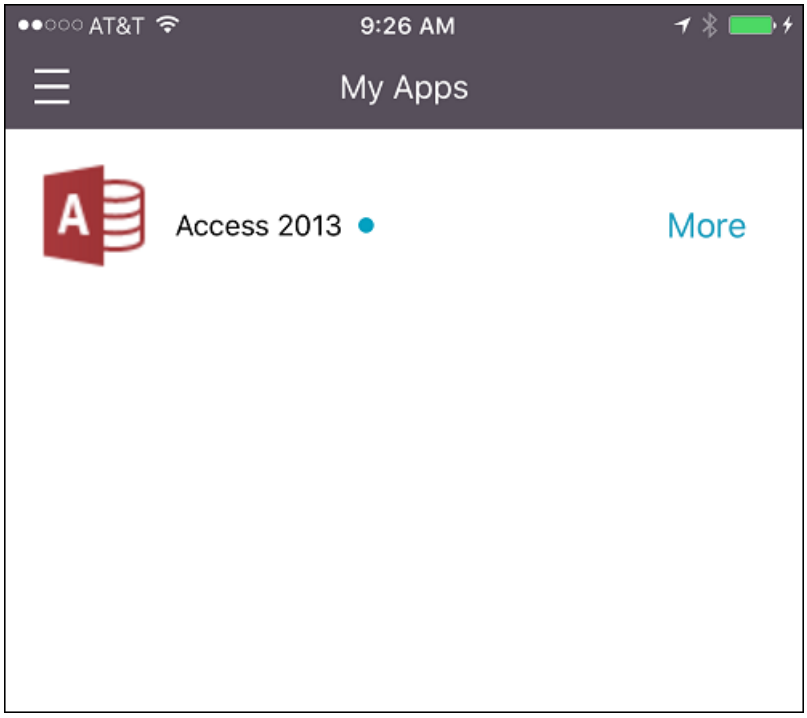
자동화된동작을설정하는것에대한자세한내용은 자동화된동작을참조하십시오.

사용자가 **HDX** 앱에대한액세스권한을복구하는방법

장치가다시규정을준수하게되면 HDX 앱에액세스할수있게됩니다.

1. 장치에서 Secure Hub 저장소로이동하여저장소의앱을새로고칩니다.
2. 앱으로이동하고앱에대한 추가를누릅니다.

앱이추가되면내앱에나타나며새로설치된앱이기때문에옆에파란색점이있습니다.



미디어추가

March 19, 2021

XenMobile 에미디어를추가하여사용자장치에미디어를배포합니다. XenMobile 을사용하여 Apple 볼륨구매를통해취득한 Apple Book 을배포할수있습니다.

XenMobile 에서볼륨구매계정을구성하면 구성 **>** 미디어에구입한서적및무료서적이나타납니다. 미디어페이지에서배달그룹을선택하고배포규칙을지정하여 iOS 장치에배포할서적을구성합니다.

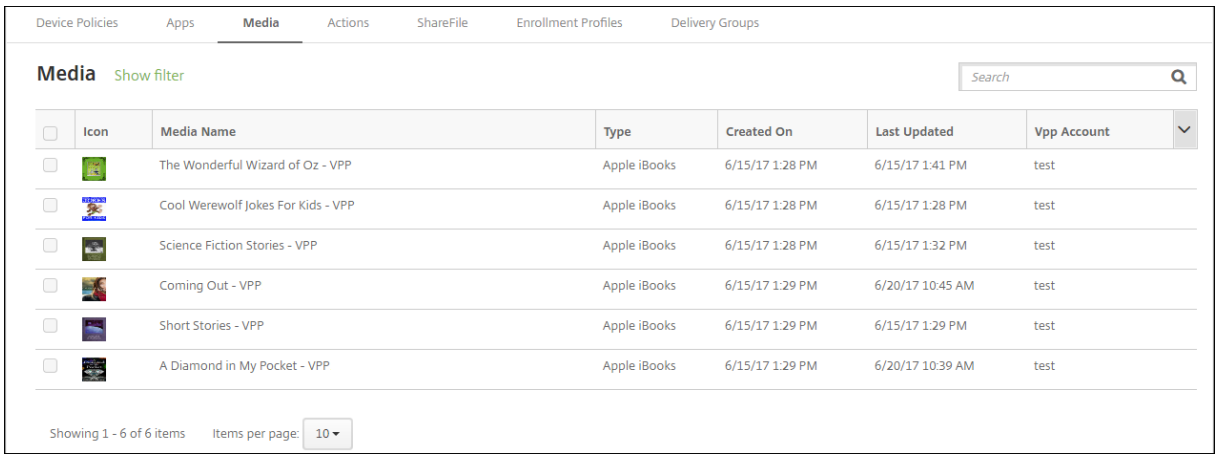
사용자가처음으로서적을수신하고볼륨구매라이센스를수락하면배포된서적이장치에설치됩니다. 서적은 Apple Book 앱에표시됩니다. 관리자는사용자에게서서적라이센스를분리하거나장치에서서적을제거할수없습니다. XenMobile 은서적을필수미디어로설치합니다. 사용자가장치에서설치된서적을삭제하는경우서적은 Apple Book 앱에유지되며바로다운로드할수있습니다.

사전요구사항

- iOS 장치
- Apple 볼륨구매에설명된대로 XenMobile 에서 Apple 볼륨구매를구성합니다.

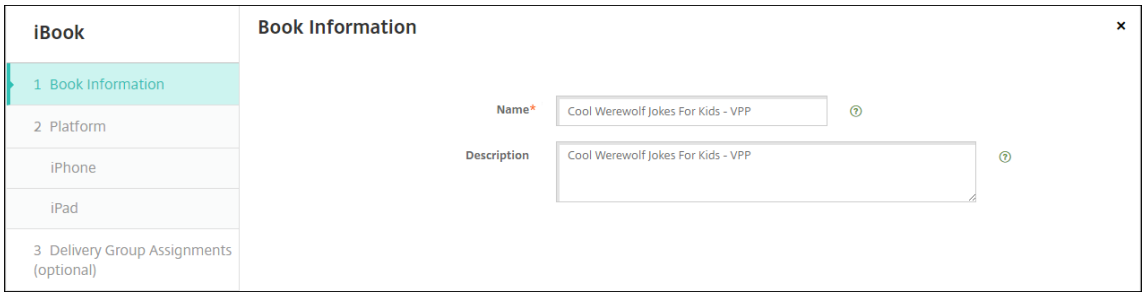
서적구성

볼륨구매를통해취득한 Apple Book 은 구성 **>** 미디어페이지에표시됩니다.



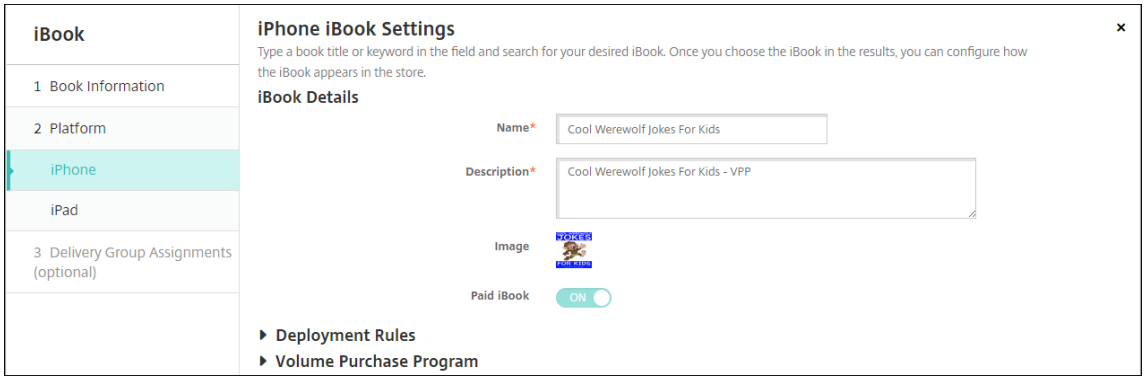
배포할 **Apple Book** 구성

1. 구성 **>** 미디어에서서적을선택하고 편집을클릭합니다. 서적정보페이지가나타납니다.

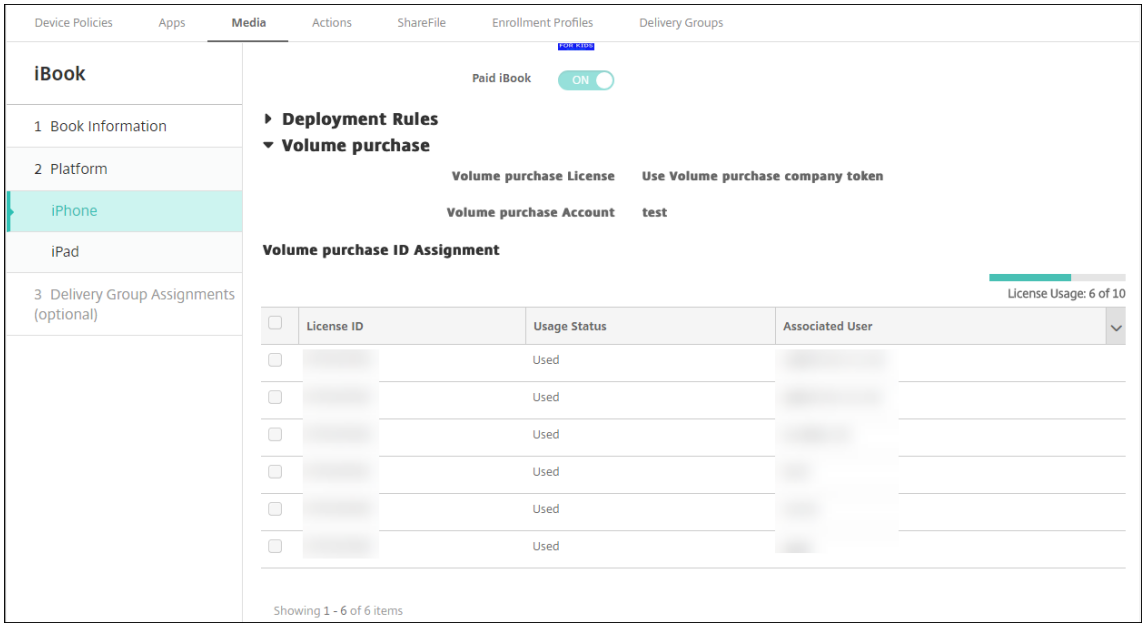


이름및 설명은 XenMobile 콘솔과로그에만표시됩니다.

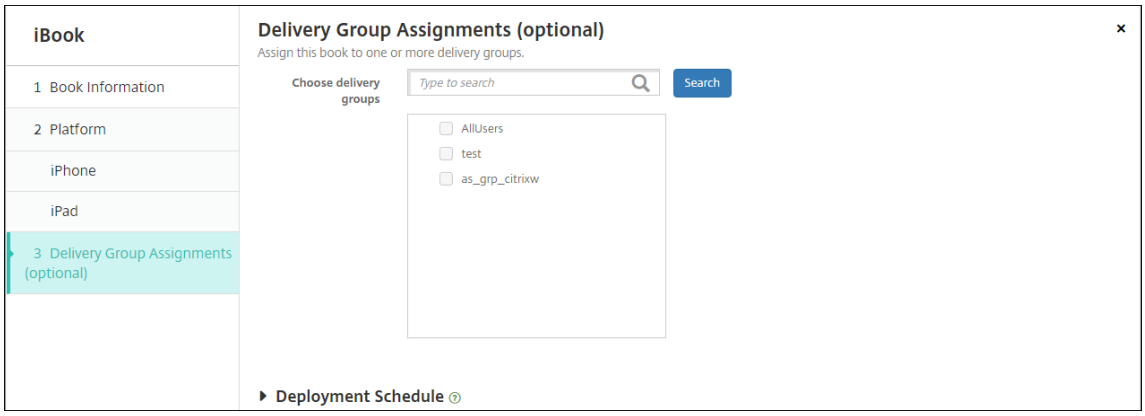
2. **iPhone iBook** 설정및 **iPad iBook** 설정페이지에서: 필요한경우서적이름과설명을변경할수있지만 Citrix 에서는이러한설정을변경하지않기를권장합니다. 이미지는정보를위한것이며편집할수없습니다. 유료 **iBook** 은 Apple 볼륨구매를통해구매한서적을나타냅니다.



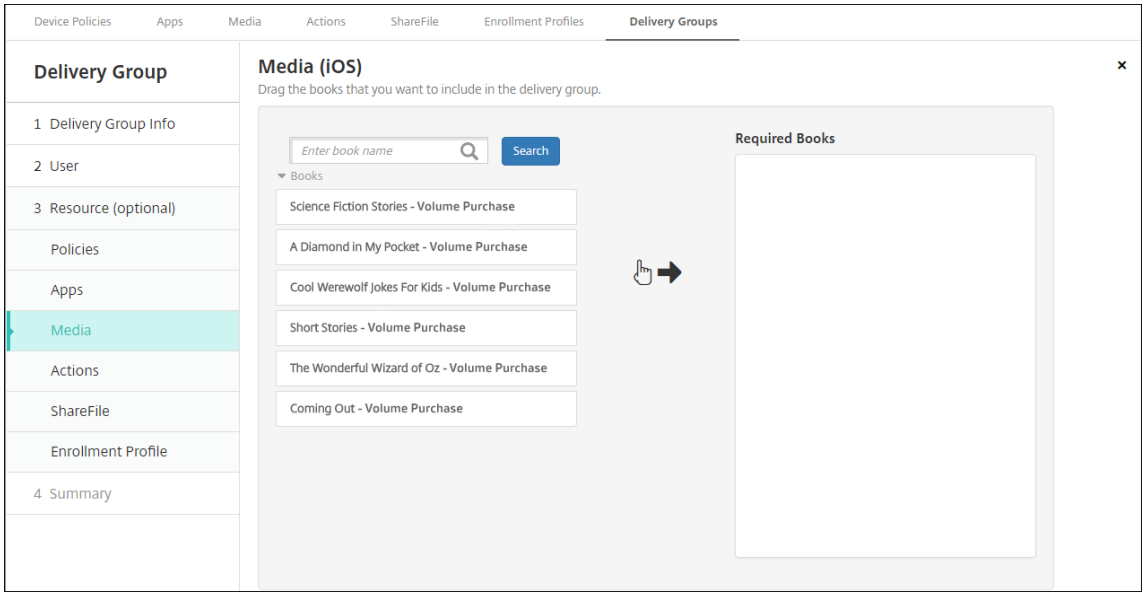
배포규칙을지정하거나볼륨구매정보를볼수도있습니다.



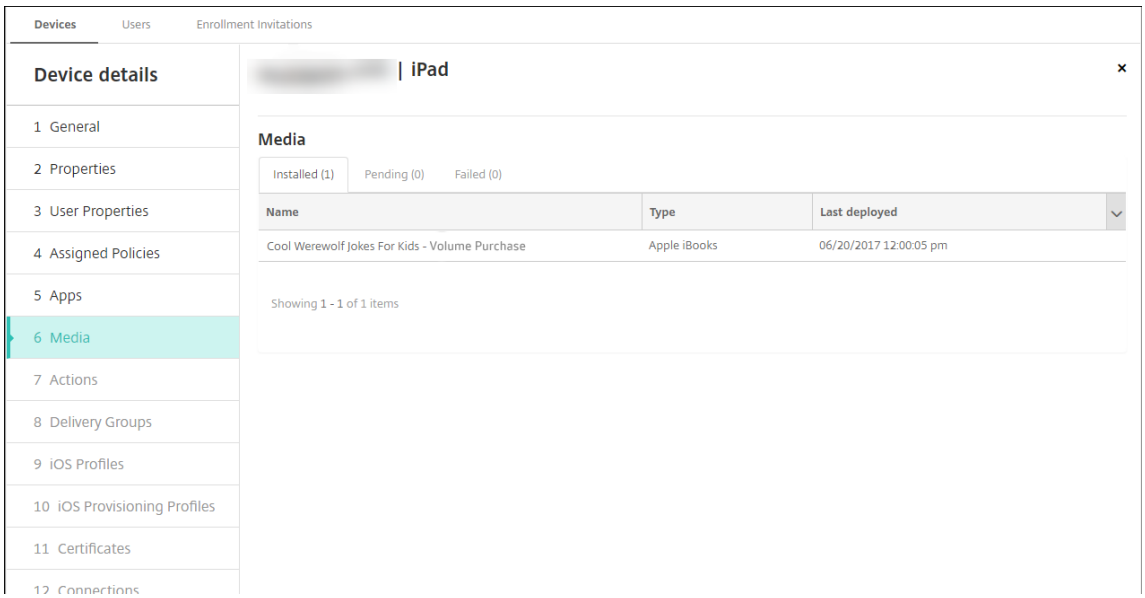
3. 필요한경우서적을배달그룹에할당하고배포일정을설정합니다.



또한 구성 **>** 배달그룹의 미디어탭에서배달그룹에서적을할당할수도있습니다. XenMobile 은필수서적배포만지원합니다.

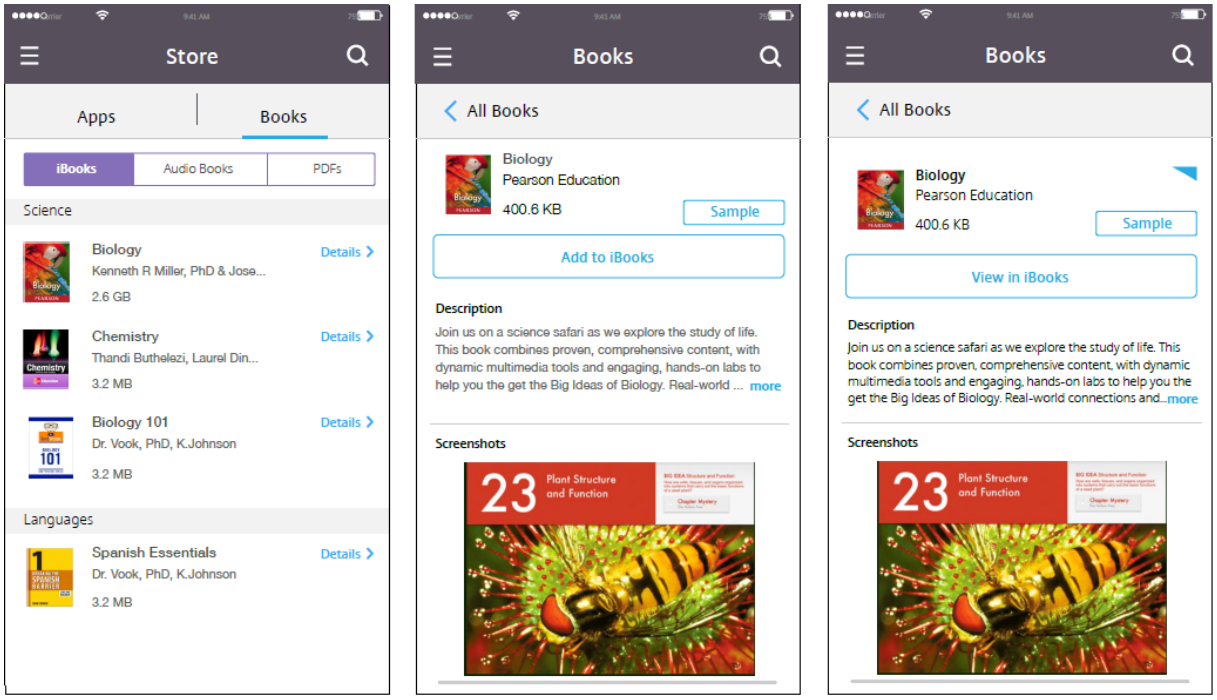


4. 배포상태를보려면 관리 **>** 장치의 미디어탭을사용합니다.



> 참고:
>
> 구성 **>** 미디어페이지에서서적을선택하고 삭제를클릭하면 XenMobile 이목록에서해당서적을제거합니다. 그러나 Apple 볼륨구매에서서적을제거하지않은경우 XenMobile 이다음에 Apple 볼륨구매와동기화되면해당서적이목록에다시표시됩니다. 목록에서서적을제거해도장치에서서적이삭제되지는않습니다.

서적은다음예에표시된것과같이사용자장치에표시됩니다.



리소스배포

August 12, 2022

장치구성및관리에는일반적으로 XenMobile 콘솔에서리소스 (정책, 앱및미디어) 및동작을만들고배달그룹을사용하여패키징하는단계가포함됩니다. XenMobile 이배달그룹의리소스및동작을장치로푸시하는순서를배포순서라고합니다. 이문서에서설명하는내용:

- 배달그룹추가, 관리및배포
- 배달그룹에서리소스및작업의배포순서변경
- XenMobile 은사용자가중복또는충돌하는정책이있는여러배달그룹에속한경우에배포순서를결정합니다.

배달그룹은정책, 앱, 미디어및동작조합을배포하는대상장치의사용자범주를지정합니다. 일반적으로회사, 국가, 부서, 사무실주소, 직함과같은사용자의특성에따라특정배달그룹에사용자를포함시킵니다. 배달그룹을통해누가어떤리소스를어떤경우에이용할수있는지를보다효과적으로제어할수있습니다. 배달그룹은모든사용자에게배포하거나좀더구체적으로정의된그룹의사용자에게배포할수있습니다.

배달그룹에배포한다는것은지원되는 iOS 및 Windows 장치의모든사용자에게푸시알림을보내는것을의미합니다. 이러한사용자는배달그룹에속해있어야 XenMobile 에다시연결됩니다. 장치를재평가하고배달그룹에포함되는정책, 앱, 미디어및동작을배포할수있습니다.

Android 장치사용자: 이미연결된경우즉시리소스를받습니다. 그렇지않은경우에는예약정책에기반하여다음에연결할때리소스를받습니다.

XenMobile 을설치하고구성하면기본 AllUsers 배달그룹이만들어집니다. 여기에는모든로컬사용자와 Active Directory 사용자가포함되어있습니다. AllUsers 그룹은삭제할수없지만일부사용자에게리소스를푸시하지않으려는경우이그룹을사용하지않도록설정할수있습니다.

배포순서

배포순서는 XenMobile 이장치에리소스를푸시하는순서입니다. 배포순서는 MDM(장치관리) 에대해구성된등록프로필이있는배달그룹의장치에만적용됩니다.

배포순서를결정할때 XenMobile 은리소스에배포규칙및배포일정과같은필터와제어조건을적용합니다. 리소스에는정책, 앱, 동작및배달그룹이포함됩니다. 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

일반적인환경에서는단일사용자에게여러배달그룹이할당되어다음과같은결과가나타날가능성이큽니다.

- 배달그룹내에서중복된개체가존재합니다.
- 사용자에게할당된여러배달그룹에서특정정책이서로다르게구성됩니다.

이러한상황이발생할경우 XenMobile 은특정장치에배달하거나관련작업을수행해야하는모든개체의배포순서를계산합니다. 계산단계는장치플랫폼에독립적입니다.

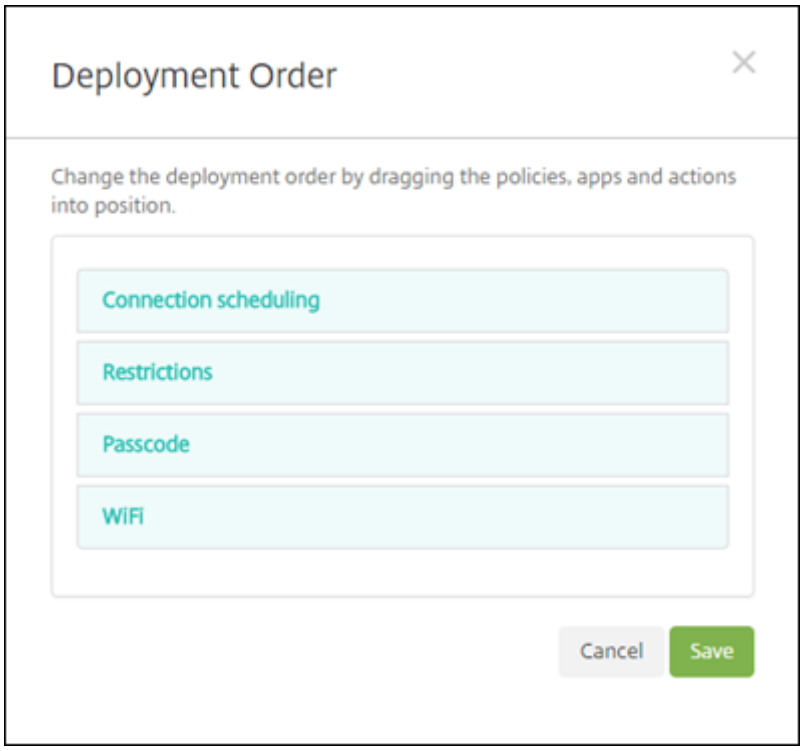
계산단계

1. 사용자, 그룹및배포규칙의필터에기반하여특정사용자의모든배달그룹을결정합니다.
2. 선택된배달그룹내의모든리소스 (정책, 앱, 미디어및동작) 의순서지정된목록을만듭니다. 목록은장치플랫폼, 배포규칙및배포일정의필터를기반으로합니다. 순서지정알고리즘은다음과같습니다.
    a) 사용자정의배포순서가있는배달그룹의리소스를사용자정의배포순서가없는배달그룹의리소스보다먼저배치합니다. 이렇게배치하는이유는이러한단계다음에설명되어있습니다.
    b) 배달그룹간에순서가동일한경우에는배달그룹이름에따라배달그룹리소스순서를지정합니다. 예를들어, 배달그룹 A 의리소스를배달그룹 B 의리소스보다먼저배치합니다.
    c) 정렬할때는배달그룹리소스에사용자정의배포순서가지정된경우해당순서를유지합니다. 그렇지않은경우리소스이름으로배달그룹내리소스를정렬합니다.
    d) 동일한리소스가두번이상나타나는경우중복된리소스를제거합니다.

사용자정의순서가있는리소스는사용자정의순서가없는리소스보다먼저배포됩니다. 하나의리소스가사용자에게할당된여러배달그룹에존재할수있습니다. 위의단계에나온것처럼계산알고리즘은중복된리소스를제거하고이목록에있는첫번째리소스만제공합니다. 이러한방식으로중복된리소스를제거함으로써 XenMobile 은 XenMobile 관리자가정의한순서를적용합니다.

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** 정책보다먼저배달하려고합니다.



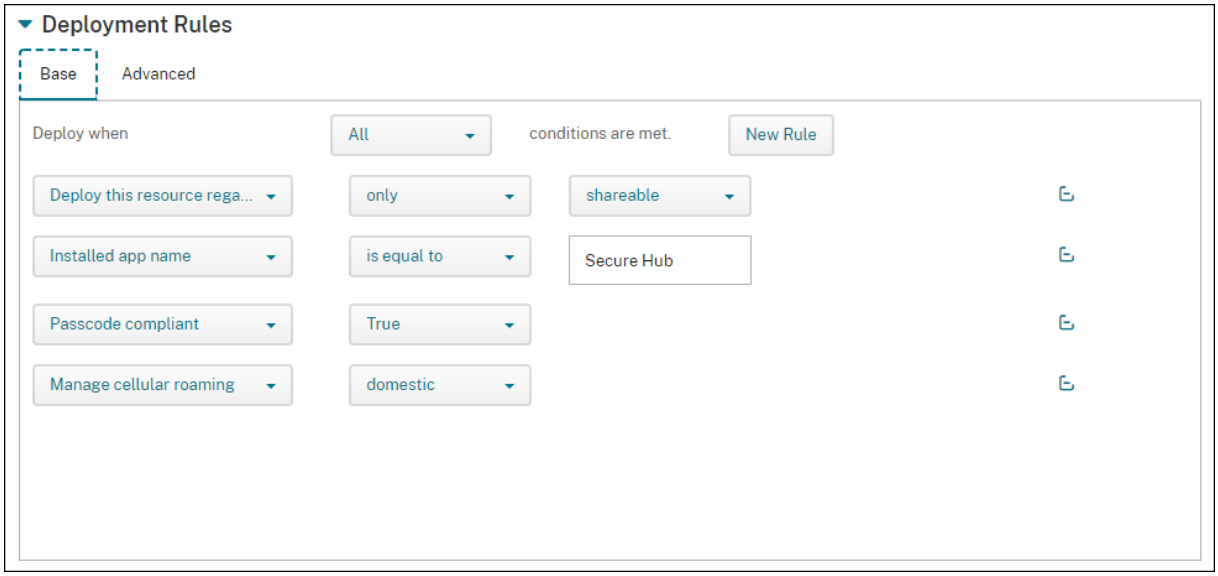
계산알고리즘이이름으로만배포그룹순서를지정한경우 XenMobile 은배달그룹계정관리자 1 부터시작하여 **WiFi**, 암호, 연결예약, 제한순서로배포를수행합니다. 계정관리자 2 배달그룹의 암호및 **WiFi** 두가지는중복되므로무시됩니다.

하지만계정관리자 2 그룹에는관리자가지정한배포순서가있습니다. 따라서계산알고리즘은계정관리자 2 배달그룹의리소스를다른배달그룹의리소스보다높은순서로목록에배치합니다. 따라서 XenMobile 은 연결예약, 제한, 암호, **WiFi** 순서로정책을배포합니다. 계정관리자 1 배달그룹의 **WiFi** 및 암호정책은중복되므로무시됩니다. 이처럼계산알고리즘은 XenMobile 관리자가지정한순서를따릅니다.

배포규칙

특정조건이있는경우에만리소스를제공하도록배포규칙을구성합니다. 기본또는고급배포규칙을구성할수있습니다.

기본편집기를사용하여배포규칙을추가할때는먼저리소스를배포할시기를선택합니다.

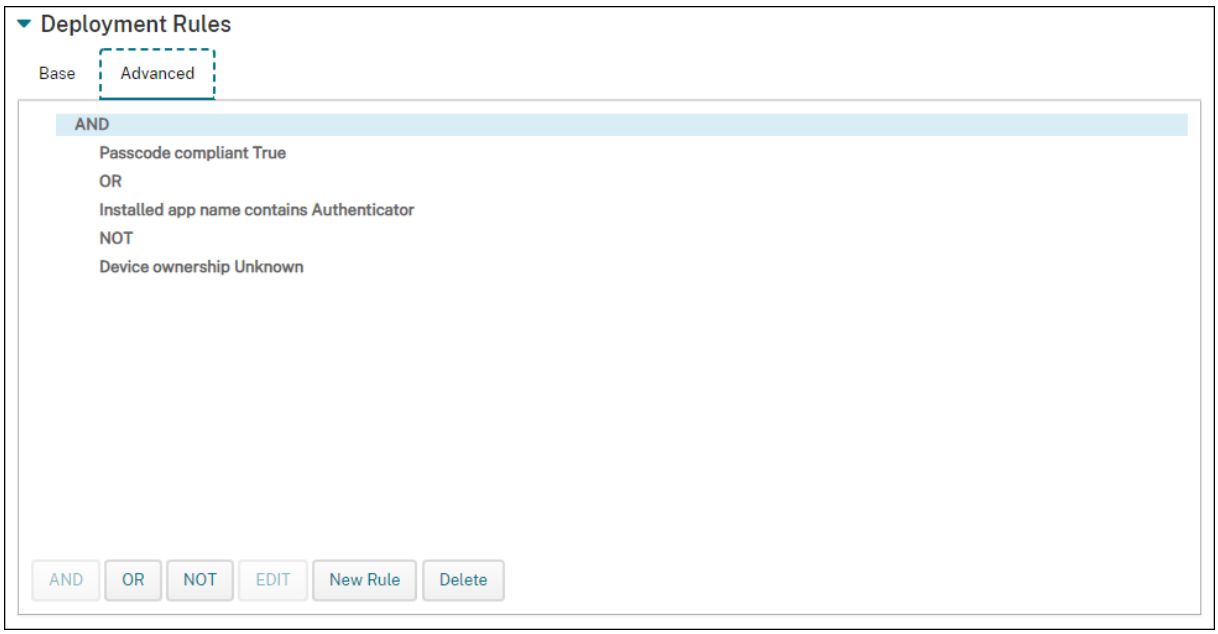


- 모두**:** 사용자또는장치가구성한모든조건을충족하면리소스를전달합니다.
- 모두**:** 사용자또는장치가구성한조건중하나이상을충족하는경우리소스를제공합니다.

새규칙을클릭하여조건을추가합니다. 규칙은배포중인리소스와리소스를구성하는플랫폼에따라다릅니다. 몇가지유형의규칙이있습니다. 다음경우에리소스를배포하도록선택할수있습니다.

- 선택한속성이존재하는경우만또는선택한속성이존재하는경우제외
- 속성이정확히입력한텍스트와일치할경우속성에입력한텍스트가포함되거나속성이입력한텍스트와일치하지않습니다.
- 장치또는사용자가선택한속성을준수하거나선택한속성을준수하지않는경우
- 장치또는사용자속성이미리정의된목록에서선택한조건과일치하는경우

고급편집기를사용하여보다복잡한배포규칙을만들수있습니다. 더많은규칙을선택할수있으며고급규칙을만들때서로다른부울논리연산자를결합할수있습니다.

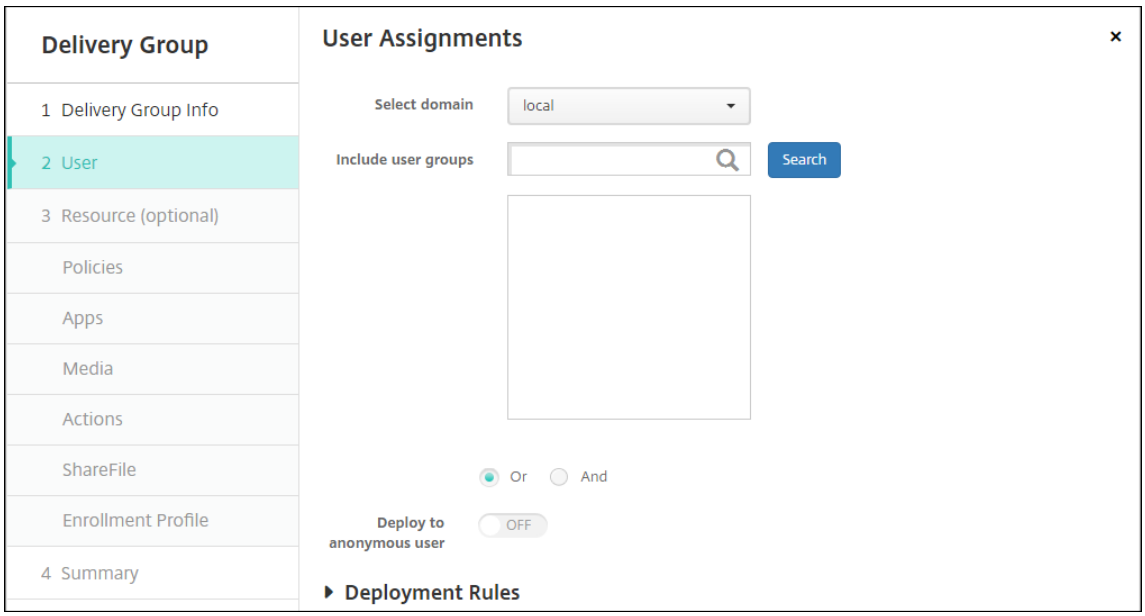


배달그룹을추가하려면

Citrix 에서는장치정책과등록프로필을만들기전에배달그룹을만들것을권장합니다.

1. 콘솔에서 구성 **>** 배달그룹을클릭합니다.
2. 배달그룹페이지에서 추가를클릭합니다.
3. 배달그룹정보페이지에서배달그룹의이름과설명을입력하고 다음을클릭합니다.

   사용자가등록프로필이다른여러배달그룹에속하는경우사용되는등록프로필은배달그룹의이름에따라결정됩니다. XenMobile 은사전순으로표시된배달그룹목록의마지막에나타나는배달그룹을선택합니다. 자세한내용은 등록프로필을 참조하십시오.
4. 사용자할당페이지에서배달그룹사용자할당관리방식을지정합니다.



> 중요:
>
> 사용자그룹이만들어진후에는 사용자할당관리설정을변경할수없습니다.

- 도메인선택: 목록에서사용자를선택할도메인을선택합니다.
- 사용자그룹포함: 다음중하나를수행합니다.
  - 사용자그룹목록에서추가하려는그룹을클릭합니다. 선택한그룹이 선택된사용자그룹목록에나타납니다.
  - 검색을클릭하여선택된도메인의모든사용자그룹목록을봅니다.
  - 검색상자에전체또는일부그룹이름을입력한다음 검색을클릭하여사용자그룹의목록을제한합니다.

  선택된사용자그룹목록에서사용자그룹을제거하려면다음중하나를수행합니다.

  - 선택된사용자그룹목록에서제거할각그룹옆에있는 **X** 를클릭합니다.
  - 검색을클릭하여선택된도메인의모든사용자그룹목록을봅니다. 목록을스크롤하면서제거할각그룹의확인란을선택취소합니다.
  - 검색상자에전체또는일부그룹이름을입력한다음 검색을클릭하여사용자그룹의목록을제한합니다. 목록을스크롤하면서제거할각그룹의확인란을선택취소합니다.
- 또는/및: 리소스를배포하기위해사용자가임의의그룹에있을수있는지 (또는), 아니면모든그룹에있어야하는지 (및)를선택합니다.
- 익명사용자에게배포: 배달그룹의인증되지않은사용자에게배포할것인지여부를선택합니다. 인증되지않은사용자는 인증하지못했지만 XenMobile 에장치를연결할수있도록허용한사용자입니다.

5. 배포규칙을구성합니다.
6. 다음을클릭합니다. 배달그룹리소스페이지가나타납니다. 필요한경우배달그룹에대한정책, 앱또는동작을추가할수도있습니다. 이단계를건너뛰려면 배달그룹아래에서 요약을클릭하여배달그룹구성의요약을봅니다.

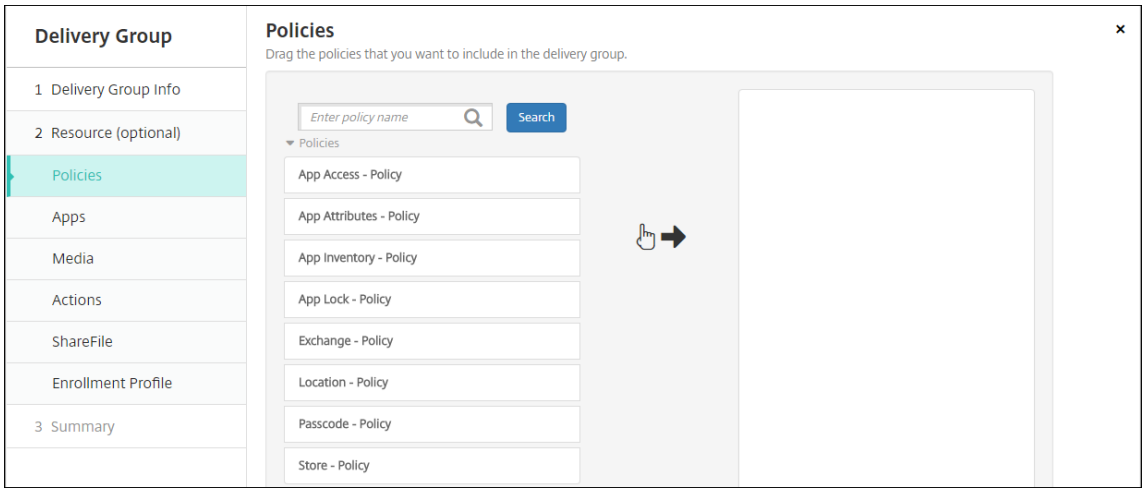
   리소스를건너뛰려면 리소스 (선택사항) 아래에서추가할리소스를클릭하고해당리소스에대한단계를수행합니다.

정책을추가하려면

1. 추가하려는각정책에대해다음을수행합니다.

    - 사용가능한정책목록을스크롤하면서추가할정책을찾습니다.
    - 또는검색상자에전체또는일부정책이름을입력한다음 검색을클릭하여정책목록을제한합니다.
    - 추가할정책을클릭하고오른쪽의상자로끌어옵니다.

    정책을제거하려면오른쪽상자에서정책이름옆에있는 **X** 를클릭합니다.



2. 다음을클릭합니다. 앱페이지가나타납니다.

앱을추가하려면

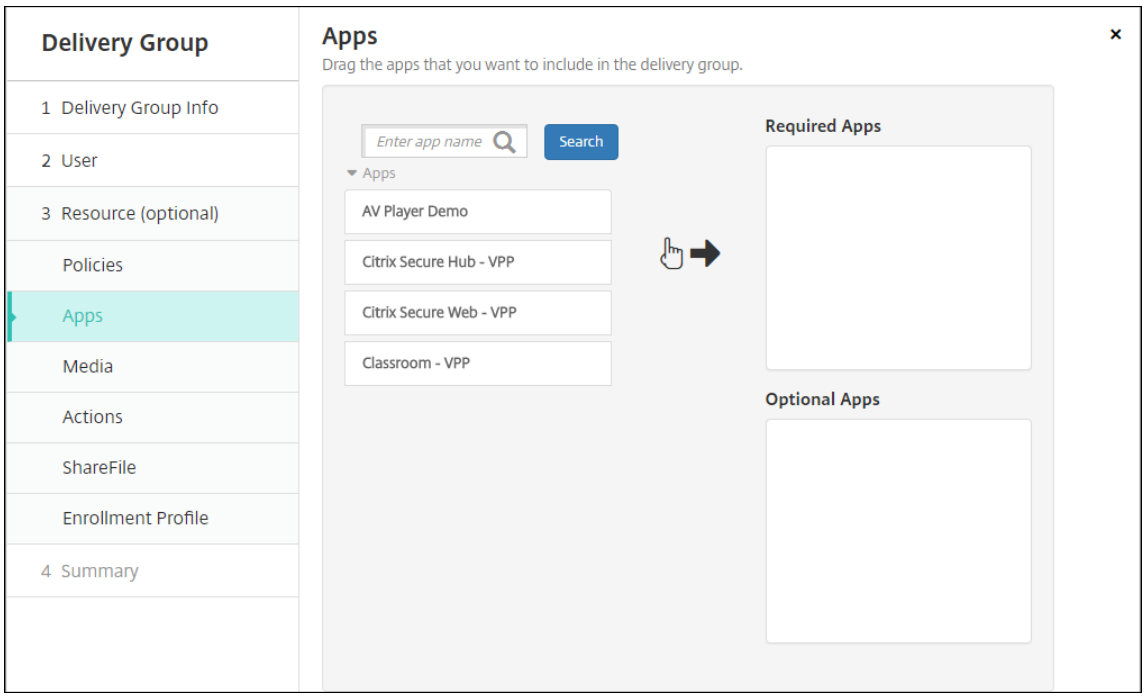
1. 추가하려는각앱에대해다음을수행합니다.

    - 사용가능한앱목록을스크롤하면서추가할앱을찾습니다.
    - 검색상자에전체또는일부앱이름을입력한다음 검색을클릭하여앱목록을제한합니다.
    - 추가할앱을클릭하고 필수앱상자또는 선택적앱상자로끕니다.

    필수로표시된앱의경우사용자는다음과같은경우에곧바로업데이트를받을수있습니다.

    - 사용자가새앱을업로드하고필수앱으로표시합니다.
    - 사용자가기존앱을필수앱으로표시합니다.
    - 사용자가필수앱을삭제합니다.
    - Secure Hub 업데이트가제공됩니다.

    기능을사용하도록설정하는방법을포함하여필수앱의강제배포에대한자세한내용은 필수앱과선택적앱정보를참조하십시오.

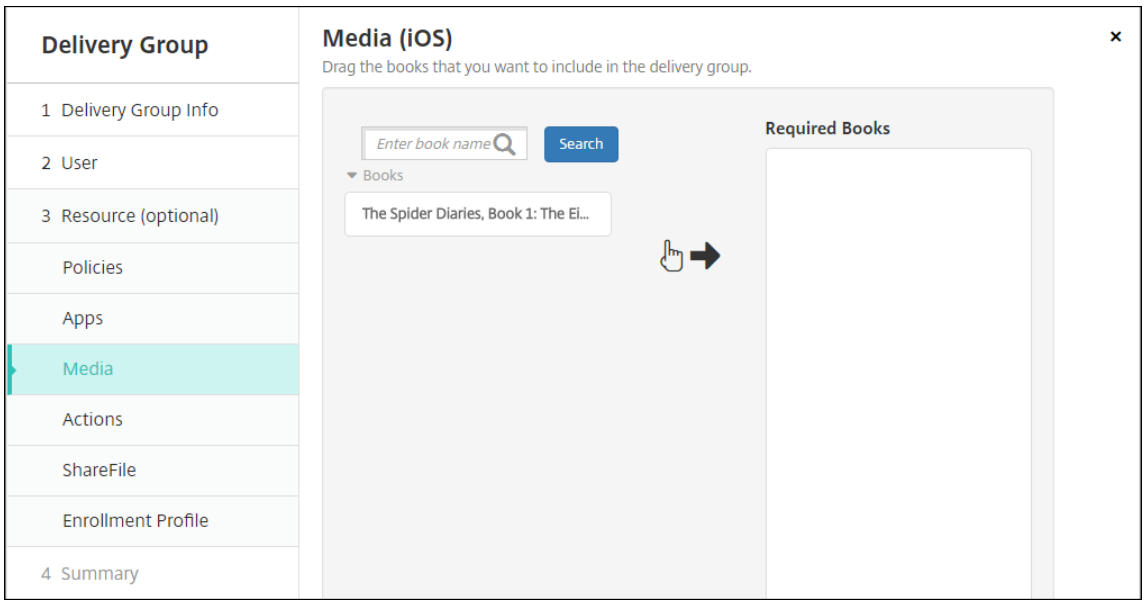


앱을제거하려면오른쪽상자에서앱이름옆에있는 **X** 를클릭합니다.

2. 다음을클릭합니다. 미디어페이지가나타납니다.

미디어를추가하려면

1. 추가할각서적에대해다음을수행합니다.
   - 사용가능한서적목록을스크롤하면서추가할서적을찾습니다.
   - 검색상자에전체또는일부서적이름을입력한다음 검색을클릭하여서적목록을제한합니다.
   - 추가할서적을클릭하고 필수서적상자로끌어옵니다.



필수로표시된서적의경우사용자는다음과같은경우에곧바로업데이트를받습니다.

- 새서적을업로드하고필수앱으로표시합니다.
- 기존서적을필수서적으로표시합니다.
- 사용자가필수서적을삭제합니다.
- Secure Hub 업데이트가제공됩니다.

서적을제거하려면오른쪽상자에서서적이름옆에있는 **X** 를클릭합니다.

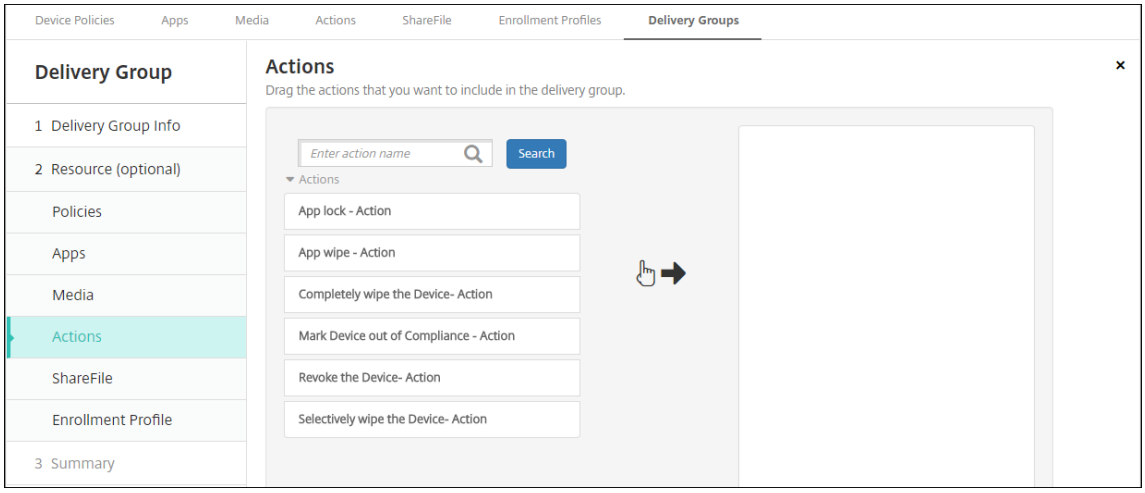
2. 다음을클릭합니다. 동작페이지가나타납니다.

동작을추가하려면

1. 추가할각동작에대해다음을수행합니다.

   - 사용가능한동작목록을스크롤하면서추가할동작을찾습니다.
   - 검색상자에전체또는일부동작이름을입력한다음 검색을클릭하여동작목록을제한합니다.
   - 추가할동작을클릭하고오른쪽상자로끌어옵니다.

   동작을제거하려면오른쪽상자에서동작이름옆에있는 **X** 를클릭합니다.

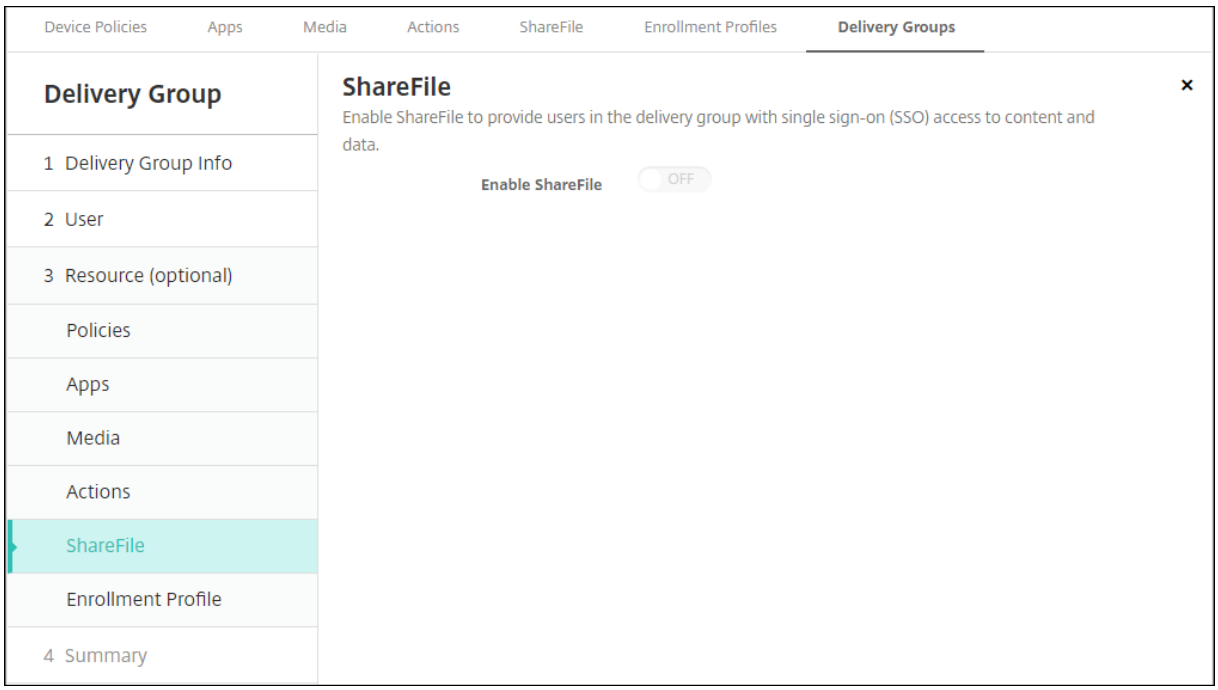


2. 다음을클릭합니다. **ShareFile** 페이지가나타납니다.

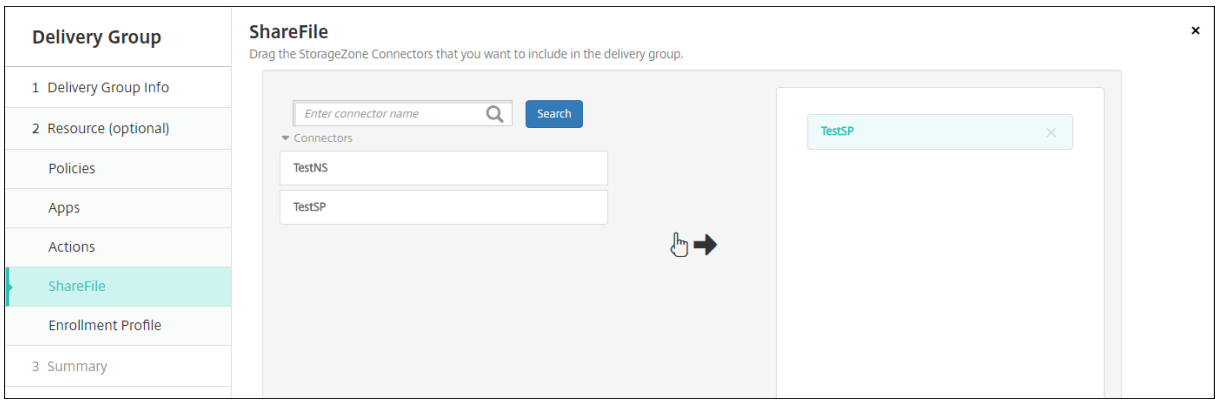
Citrix Content Collaboration 구성을적용하려면

Content Collaboration 페이지는 XenMobile(구성 **> ShareFile**) 에 Enterprise 계정을사용하도록구성했는지, 아니면 StorageZone 커넥터를사용하도록구성했는지에따라달라집니다.

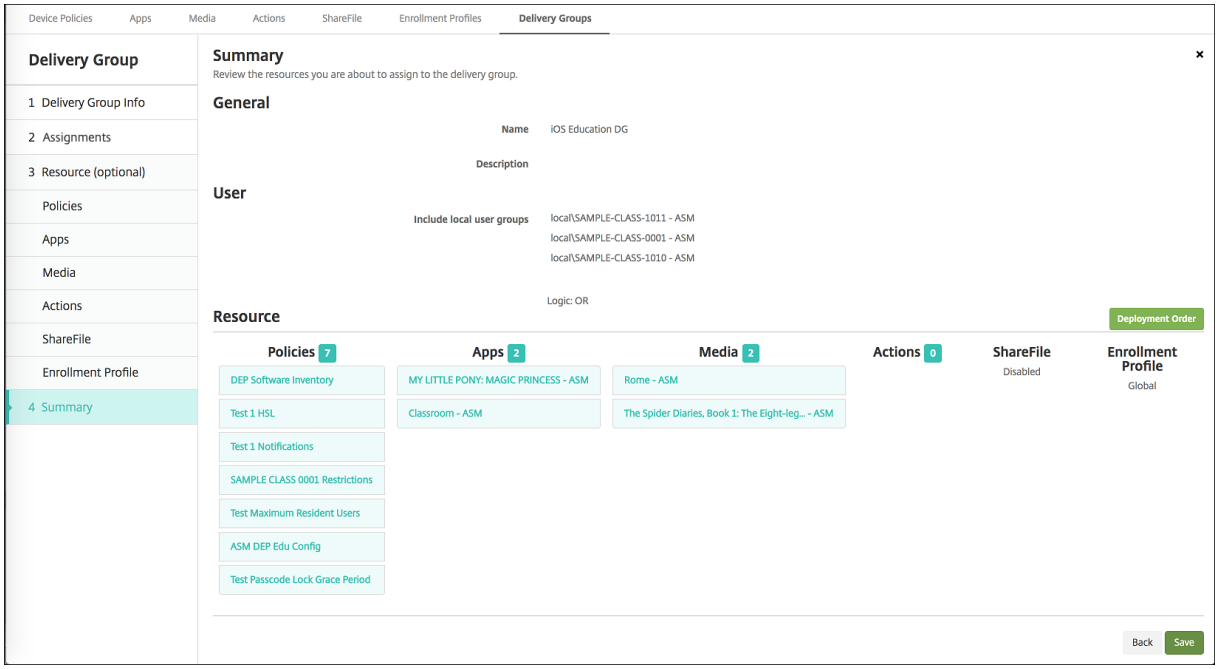
XenMobile 에 Enterprise 계정을사용하도록구성한경우 **ShareFile** 사용을 켜짐으로설정하여배달그룹에 Content Collaboration 콘텐츠및데이터에대한 SSO(Single Sign-On) 액세스를제공합니다.



XenMobile 에 StorageZone 커넥터를사용하도록구성한경우배달그룹에포함할 StorageZone 커넥터를선택합니다.

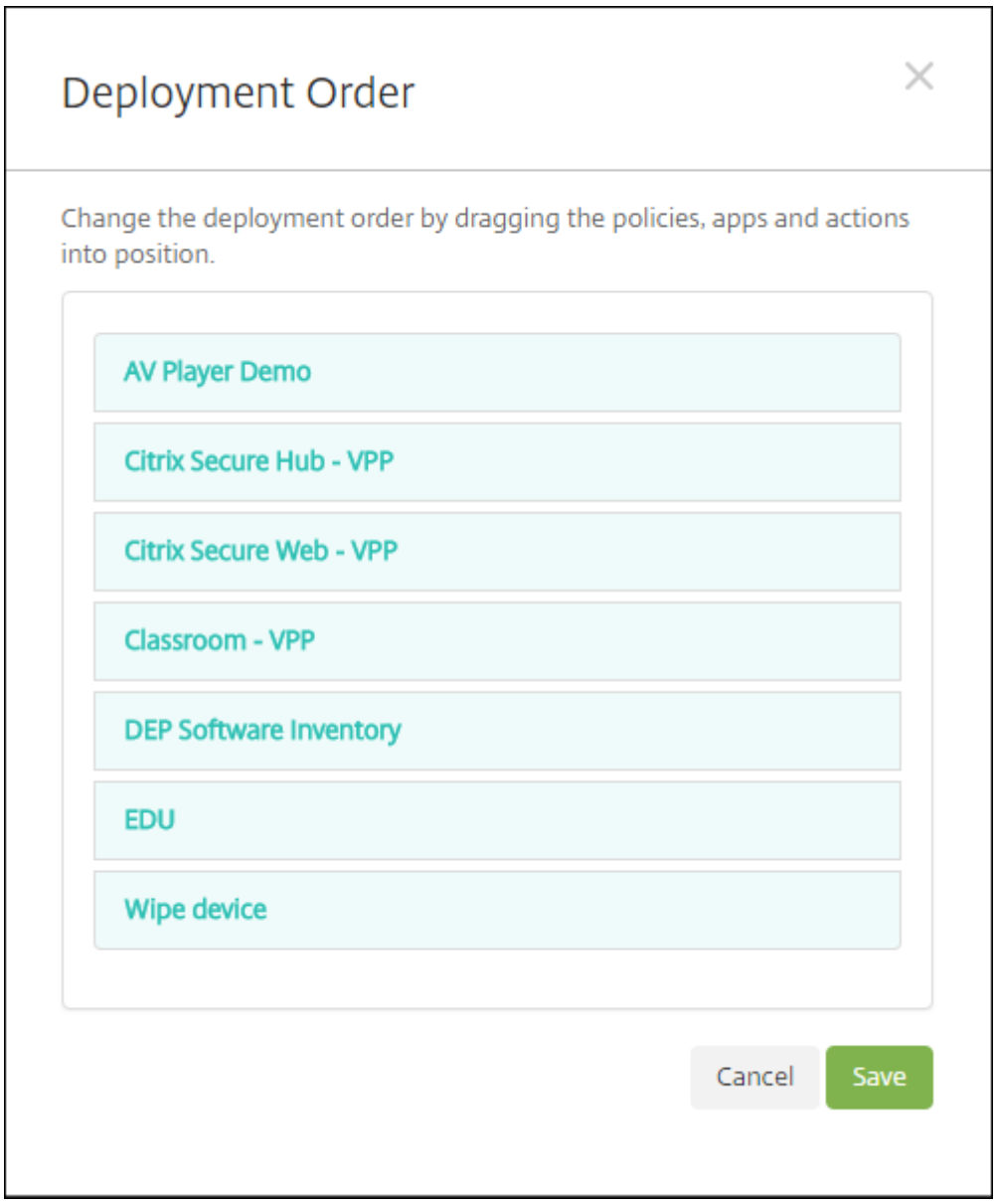


구성된옵션을검토하고배포순서를변경하려면



요약페이지에서배달그룹에구성한옵션을검토하고리소스의배포순서를변경할수있습니다. 요약페이지에리소스가범주별로표시됩니다. 요약페이지에는배포순서는반영되지않습니다.

1. 뒤로를클릭하여이전페이지로돌아가서구성에필요한조정을수행합니다.
2. 배포순서를클릭하여배포순서를확인하거나재정렬합니다. 배포순서대화상자가나타납니다.



3. 리소스를클릭하고배포할위치로끌어옵니다. 배포순서를변경한후 XenMobile 은목록의위에서아래로리소스를배포합니다.
4. 저장을클릭하여배포순서를저장합니다.
5. 저장을클릭하여배달그룹을저장합니다.

배달그룹을편집하려면

기존배달그룹의이름은변경할수없습니다. 다른설정을업데이트하려면: 구성 **>** 배달그룹으로이동하고편집할그룹을선택한후 편집을클릭합니다.

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 를사용하지않도록설정한경우에만사용할수있습니다. 배달그룹테이블의 사용안함머리글아래에 사용안함이사라집니다.

배달그룹에배포하려면

배달그룹에배포한다는것은 iOS 및 Windows 태블릿장치의모든사용자에게푸시알림을보내는것을의미합니다. 이러한사용자는 배달그룹에속해있어야 XenMobile 에다시연결됩니다. 이방법을통해장치를재평가하고앱, 정책및작업을배포할수있습니다.

다른플랫폼장치의사용자: 해당장치가이미 XenMobile 에연결된경우즉시리소스를받습니다. 그렇지않은경우에는예약정책에기반하여다음에연결할때리소스를받습니다. Android Enterprise 플랫폼의사용자는 Firebase Cloud Messaging 알림시스템에서알림을받은다음 XenMobile Server 에연결하여리소스를검색합니다.

Android 장치에있는 XenMobile Store 의업데이트사용가능목록에업데이트된앱이표시되게하려면먼저앱인벤토리정책을사용자장치에배포해야합니다.

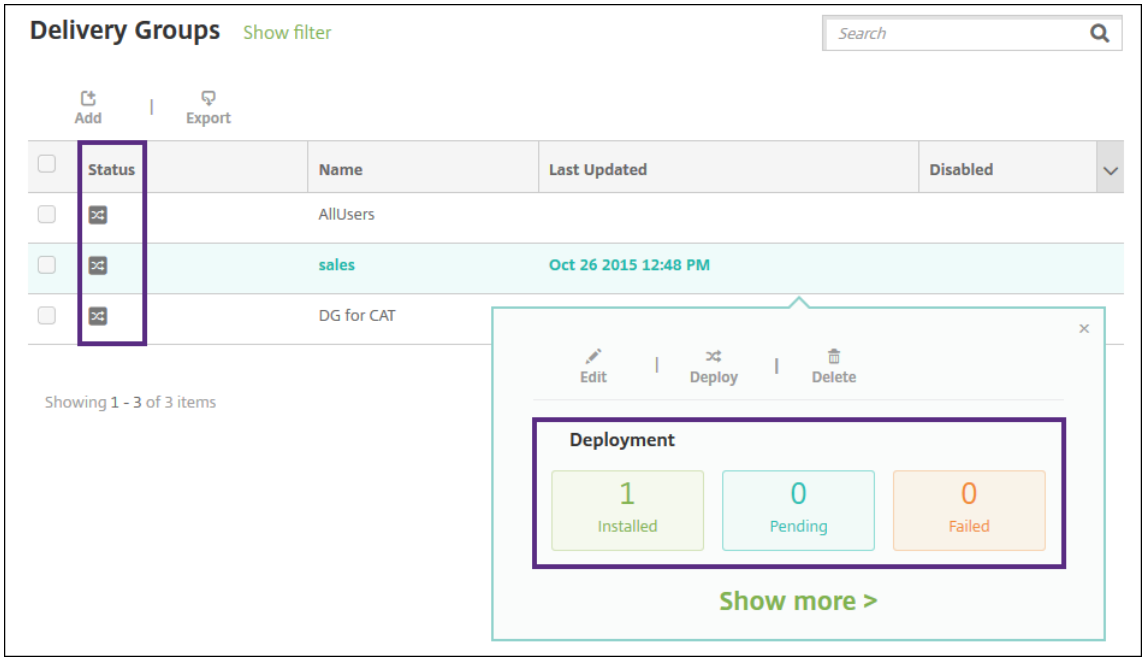
1. 배달그룹페이지에서다음중하나를수행합니다.
   - 한번에둘이상의배달그룹에배포하려면배포하려는그룹옆에있는확인란을선택합니다.
   - 하나의배달그룹에배포하려면해당이름옆의확인란을선택하거나해당이름이포함된줄을클릭합니다.
2. 배포를클릭합니다.

   배달그룹을선택한방법에따라배달그룹위또는오른쪽에 배포명령이나타납니다.

   앱, 정책및동작을배포할그룹이나열되어있는지확인하고 배포를클릭합니다. 장치플랫폼과예약정책에따라선택한그룹에 앱, 정책및동작이배포됩니다.

   배달그룹페이지에서다음방법중하나로배포상태를확인할수있습니다.

   - 배달그룹의 상태머리글아래에있는배포아이콘을확인합니다. 배포가실패한경우이아이콘에나타납니다.
   - 배달그룹이포함된줄을클릭하여 설치됨, 보류중및 실패배포를나타내는오버레이를표시합니다.



배달그룹을삭제하려면

AllUsers 배달그룹은삭제할수없지만일부사용자에게리소스를푸시하지않으려는경우이그룹을사용하지않도록설정할수있습니다.

1. 배달그룹페이지에서다음중하나를수행합니다.
   - 한번에둘이상의배달그룹을삭제하려면삭제하려는그룹옆에있는확인란을선택합니다.
   - 하나의배달그룹을삭제하려면해당이름옆의확인란을선택하거나해당이름이포함된줄을클릭합니다.
2. 삭제를클릭합니다. 삭제대화상자가나타납니다.

   단일배달그룹을선택하는방법에따라배달그룹위또는오른쪽에 삭제명령이나타납니다.

   > 중요:
   >
   > 삭제는실행취소할수없습니다.

3. 삭제를클릭합니다.

배달그룹테이블을내보내려면

1. 배달그룹테이블위에있는 내보내기단추를클릭합니다. 배달그룹테이블에있는정보를추출하여.csv 파일로변환합니다.
2. 브라우저의일반적인단계에따라.csv 파일을열거나저장합니다. 또한작업을취소할수도있습니다.

매크로

May 6, 2022

XenMobile 은다음항목의텍스트필드내에사용자또는장치속성데이터를채우기위한방법으로매크로를제공합니다.

- 정책
- 알림
- 등록템플릿
- 자동화된동작
- 자격증명공급자인증서서명요청

XenMobile 은매크로를해당사용자또는시스템값으로바꿉니다. 예를들어사용자수천명에대해단일 Exchange 프로필을보유한각사용자의사서함값을미리채울수있습니다.

매크로구문

매크로는다음과같은형식을사용할수있습니다.

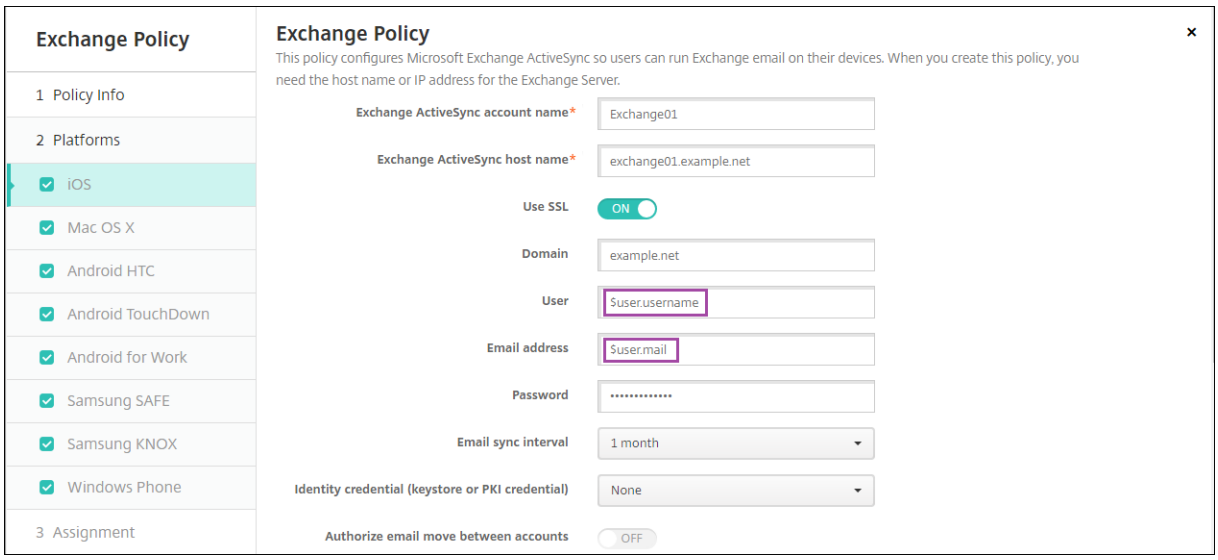
- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

달러기호 ($) 뒤에오는모든구문은중괄호 ({ }) 로묶습니다.

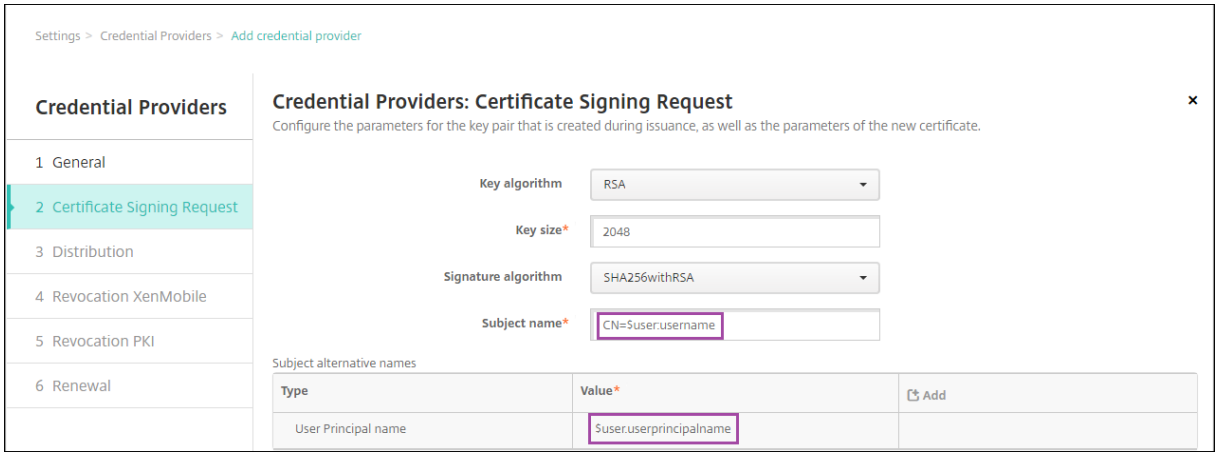
- 정규화된속성이름은사용자속성, 장치속성또는사용자지정속성을참조합니다.
- 정규화된속성이름은접두사와접두사뒤에오는실제속성이름으로구성됩니다.
- 사용자속성은 `${ user.[PROPERTYNAME] (prefix="user.")}` 형식을사용합니다.
- 장치속성은 `${ device.[PROPERTYNAME] (prefix="device.")}` 형식을사용합니다.
- 속성이름은대/소문자를구분합니다.
- 함수는제한된목록또는함수를정의하는타사참조에대한링크일수있습니다. 알림메시지를위한다음매크로에는함수 **firstnotnull** 이포함됩니다.

  `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 장치는차단되었습니다...
- 사용자지정매크로 (사용자가정의하는속성) 의접두사는 `${ custom }`입니다. 접두사는생략할수있습니다.

다음은정책의텍스트필드에사용자이름값을채우는널리사용되는매크로 `${ user.username }`의예제입니다. 이매크로는다수의사용자가사용하는 Exchange ActiveSync 프로필및기타프로필을구성할때유용합니다. 다음예제에서는 Exchange 정책에서매크로를사용하는방법을보여줍니다. 사용자에대한매크로는 **`${ user.username }`**입니다. 전자메일주소에대한매크로는 **`${ user.mail }`**입니다.

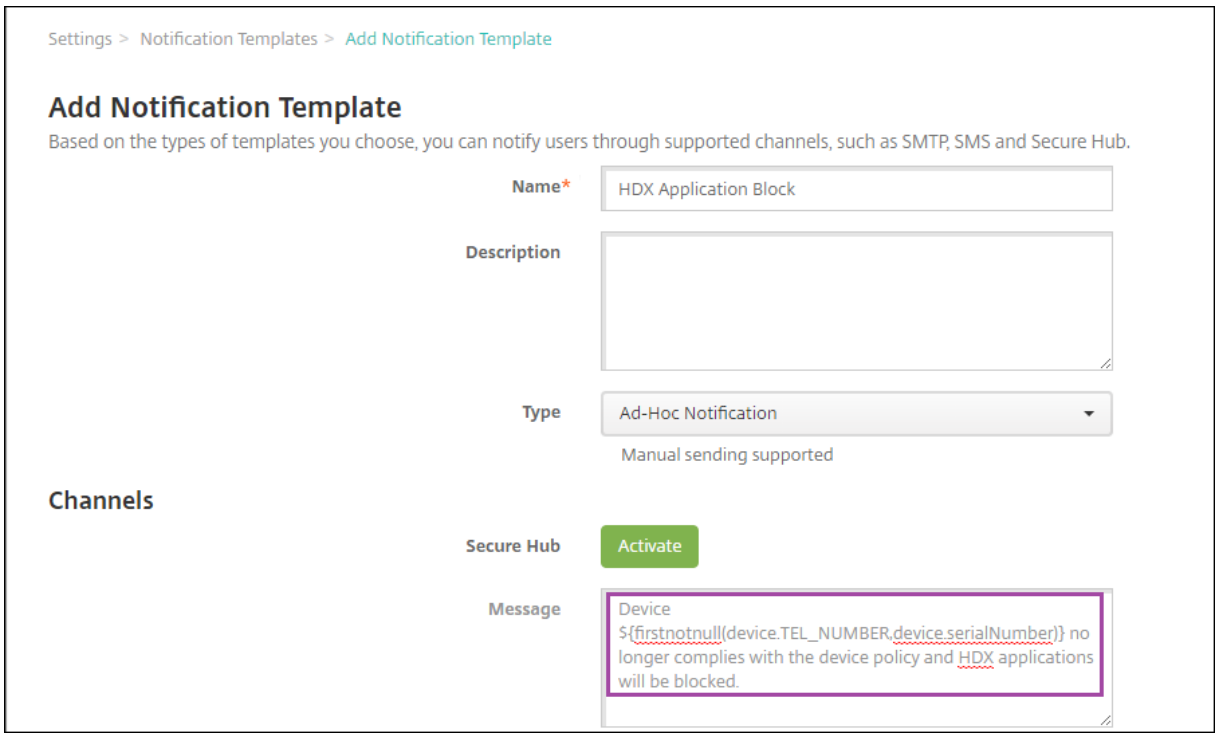


다음예제에서는인증서서명요청에매크로를사용하는방법을보여줍니다. 주체이름에대한매크로는 **CN=$user.username**입니다. 주체대체이름의 값에대한매크로는 **$user.userprincipalname**입니다.



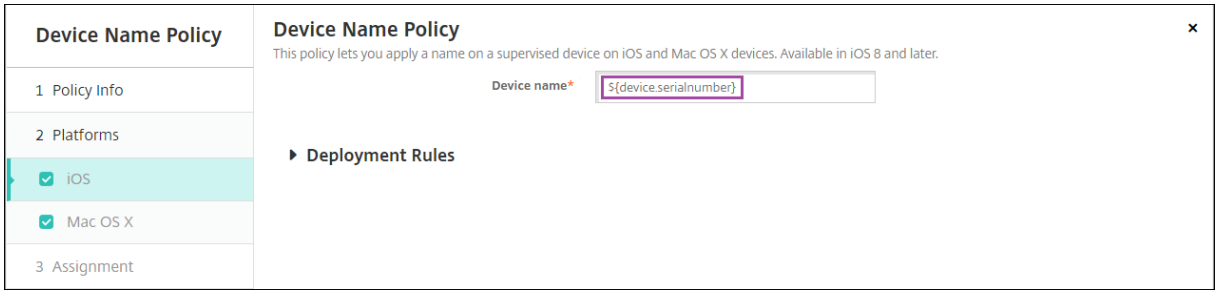
다음예제에서는알림템플릿에서매크로를사용하는방법을보여줍니다. 예제템플릿은 HDX 응용프로그램이규정을준수하지않는장치때문에차단되었을때사용자에게보내는메시지를정의합니다. 메시지에대한매크로는다음과같습니다.

Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` no longer complies with the device policy and HDX applications will be blocked.



알림에사용되는매크로에대한더많은예제를보려면 설정 > 알림템플릿으로이동하고사전정의된템플릿을선택한다음 편집을클릭하십시오.

다음예제에서는장치이름장치정책의매크로를보여줍니다. 매크로, 매크로조합또는매크로와텍스트조합을입력하여각장치에고유한이름을지정할수있습니다. 예를들어 `${ device.serialnumber }`를사용하여장치이름을각장치의일련번호로설정합니다. 장치이름에사용자이름을포함하려면 `${ device.serialnumber } ${ user.username }`을사용합니다. 장치이름장치정책은감독되는 iOS 및 macOS 장치에서작동합니다.



기본알림템플릿에대한매크로

기본알림템플릿에서사용할수있는매크로는다음과같습니다.

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`

- ${ enrollment.pin }
- ${ enrollment.url }
- ${ enrollment.urls }
- ${ enrollment.ios.url }
- ${ enrollment.macos.url }
- ${ enrollment.android.url }
- ${ enrollment.ios.platform }
- ${ enrollment.macos.platform }
- ${ enrollment.android.platform }
- ${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}
- ${ firstnotnull(device.TEL_NUMBER,user.mobile)}
- ${ outofcompliance.reason(smg_block)}
- ${ outofcompliance.reason(whitelist_blacklist_apps_name)}

  > 참고:
  >
  > XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는용어가포함됩니다. 향후릴리스에서이러한 용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.

- ${ 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.

- `${ webeas-url }`

Samsung MDM 라이센스키장치정책의경우 **ELM** 라이센스키에다음매크로를사용할수있습니다.

- `${ elm.license.key }`

기본제공장치속성을가져오는매크로

표시이름	매크로
장치 ID	`$device.id`
장치 GUID	`$device.uniqueid`
장치 IMEI	`$device.imei`
OS 제품군	`$device.OSFamily`
일련번호	`$device.serialNumber`

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_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_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.DESCRIPTION}

장치식별자

- Activesyncid
- ${device.activesyncid}

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}

홈모바일국가코드

- SIM_MCC
- ${device.SIM_MCC}

홈모바일네트워크코드

- SIM_MNC
- ${device.SIM_MNC}

ICCID

- ICCID

- ${device.ICCID}

ID

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY}

IMEI/MEID 번호

- IMEI
- ${device.IMEI}

IMSI

- SIM_ID
- ${device.SIM_ID}

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}

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}

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0}

경계위반

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH}

정기적인확인

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck}

개인핫스폿이활성화됨

- 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}

감독됨

- SUPERVISED
- ${device.SUPERVISED}

일시중단이유

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_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)	`${ user.domainname }`
loginname(사용자이름 + 도메인이름)	`${ user.loginname }`
username(도메인이있는경우도메인을제외한로그인이름)	`${ user.username }`

모든사용자속성에대한매크로

표시이름	웹요소	매크로
Active Directory 실패한로그온시도횟수	badpwdcount	${ user.badpwdcount }
ActiveSync 사용자전자메일	asuseremail	${ user.asuseremail }
ASM 데이터원본	asmpersonsource	${ user.asmpersonsource }
ASM DEP 계정이름	asmdepaccount	${ user.asmdepaccount }
ASM 관리되는 Apple ID	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
ASM 암호유형	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ASM 사용자 ID	asmpersonid	${ user.asmpersonid }
ASM 사용자상태	asmpersonstatus	${ user.asmpersonstatus }
ASM 사용자직위	asmpersontitle	${ user.asmpersontitle }
ASM 사용자고유 ID	asmpersonuniqueid	${ user.asmpersonuniqueid }
ASM 소스시스템 ID	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
ASM 학생의학년	asmpersongrade	${ user.asmpersongrade }
BES 사용자전자메일	besuseremail	${ user.besuseremail }
회사	company	${ user.company }
회사이름	companyname	${ user.companyname }
국가	c	${ user.c }
부서	department	${ user.department }
설명	description	${ user.description }
사용하지않는사용자	disableduser	${ user.disableduser }

표시이름	웹요소	매크로
표시이름	displayname	${ user.displayname }
고유이름	distinguishedname	${ user.distinguishedname }
도메인이름	domainname	${ user.domainname }
전자메일	mail	${ user.mail }
이름	givenname	${ user.givenname }
집주소	homestreetaddress	${ user.homestreetaddress }
집구/군/시	homecity	${ user.homecity }
집국가	homecountry	${ user.homecountry }
집팩스	homefax	${ user.homefax }
집전화	homephone	${ user.homephone }
집시/도/지역	homestate	${ user.homestate }
집우편번호	homezip	${ user.homezip }
IP 전화	ipphone	${ user.ipphone }
중간이니셜	middleinitial	${ user.middleinitial }
중간이름	middlename	${ user.middlename }
모바일	mobile	${ user.mobile }
이름	cn	${ user.cn }
사무실주소	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
사무실구/군/시	l	${ user.l }
사무실팩스번호	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
사무실시/도	st	${ user.st }
사무실세부주소	officestreetaddress	${ user.officestreetaddress }

표시이름	웹요소	매크로
사무실전화번호	telephonenumber	${ user.telephonenumber }
사무실우편번호	postalcode	${ user.postalcode }
사서함	postofficebox	${ user.postofficebox }
호출기	pager	${ user.pager }
주그룹 ID	primarygroupid	${ user.primarygroupid }
SAM 계정	samaccountname	${ user.samaccountname }
세부주소	streetaddress	${ user.streetaddress }
성	sn	${ user.sn }
직위	title	${ user.title }
사용자로그온이름	userprincipalname	${ user.userprincipalname }

자동화된동작

January 5, 2022

XenMobile 에서이벤트, 사용자또는장치속성또는사용자장치의앱존재에대한반응을프로그래밍하는자동화된동작을만들수있습니다. 자동화된동작을만드는경우 XenMobile 에연결하는사용자장치에서수행되는동작은동작에정의된트리거에따라결정됩니다. 이벤트가트리거되면더심각한동작이수행되기전에문제를수정하도록사용자에게알림을보낼수있습니다.

자동으로발생하도록설정하는효과의범위는다음과같습니다.

- 장치를전체적으로또는선택적으로초기화
- 장치를규정위반으로설정
- 장치해지
- 더심각한조치가취해지기전에문제를수정하도록사용자에게알림전송

MAM 전용모드에대해앱잠금및앱초기화동작을구성할수있습니다.

> 참고:
>
> 사용자에게알림을보내려면 XenMobile 이메시지를보낼수있도록먼저 SMTP 및 SMS 에대한 XenMobile 설정에서알

> 림서버를구성해야합니다. 자세한내용은 알림을참조하십시오. 또한계속하기전에사용하려는모든알림템플릿을설정합니다. 자세한내용은 알림템플릿만들기및업데이트를참조하십시오.

예제작업

다음은자동화된작업을사용하는몇가지예입니다.

예제 1

- 이전에차단한앱 (예: “Words with Friends”) 을검색하려고합니다. 이경우 “Words with Friends” 가검색되면사용자장치를규정위반으로설정하는트리거를지정할수있습니다. 이동작은이어서사용자에게앱을제거하여장치를규정준수상태로되돌리라는알림을보냅니다. 또한사용자가준수할때까지대기할기간에대한시간제한을설정할수있습니다. 이시간제한이지나면정의된동작 (예: 장치를선택적으로초기화) 이수행됩니다.

예제 2

- 고객이최신펌웨어를사용하고있는지확인하고사용자가장치를업데이트해야하는경우리소스에대한액세스를차단하려고합니다. 사용자장치에최신버전이없는경우사용자장치를규정위반으로설정하는트리거를지정할수있습니다. 자동화된작업을사용하여리소스를차단하고고객에게알릴수있습니다.

예제 3

- 사용자장치가규정위반상태가되고사용자가장치를수정합니다. 장치를규정준수상태로재설정하는패키지를배포하도록정책을구성할수있습니다.

예제 4

- 특정기간동안비활성상태인사용자장치를규정위반으로표시하려고합니다. 비활성장치에대해다음과같이자동화된작업을생성할수있습니다.

  1. XenMobile 콘솔에서 설정 **>** 네트워크액세스제어로이동한다음 비활성장치를선택합니다. 비활성장치설정에대한자세한내용은 네트워크액세스제어에서확인하십시오.
  2. 작업추가및관리에설명된대로단계에따라작업을추가합니다. 유일한차이점은 작업세부정보페이지에서다음과같이설정을구성한다는것입니다.
     - 트리거. 장치속성, 규정위반, **True** 를선택합니다.
     - 작업. 알림전송을선택하고 설정에서 알림템플릿을사용하여생성한템플릿을선택합니다. 그런다음동작을수행하기전의지연기간을일, 시간또는분단위로설정합니다. 사용자가동작을트리거한문제를해결할때까지동작을반복할간격을설정합니다.

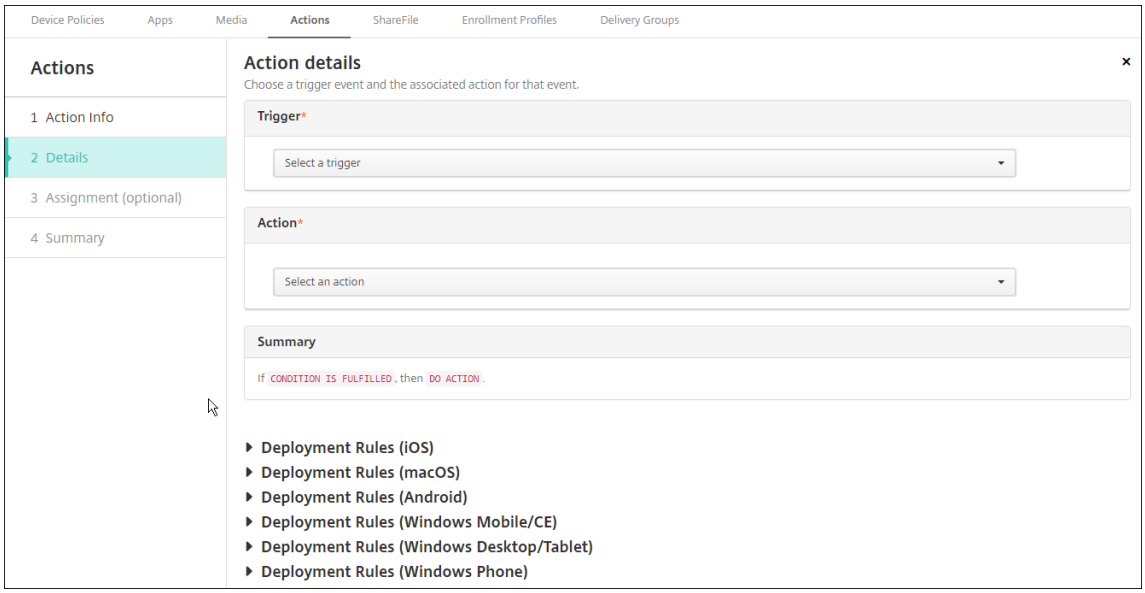
> **팁:**
>
> 비활성장치를대량으로삭제하려면 REST 서비스용공용 API을사용합니다. 먼저삭제할비활성장치의장치 ID 를수동으로얻은다음삭제 API 를실행하여대량으로삭제합니다.

작업추가및관리

자동화된작업을추가, 편집및필터링하려면다음을수행합니다.

1. XenMobile 콘솔에서 구성 **>** 동작을클릭합니다. 동작페이지가나타납니다.
2. 동작페이지에서다음중하나를수행합니다.
   - 추가를클릭하여동작을추가합니다.
   - 기존동작을선택하여편집하거나삭제합니다. 사용할옵션을클릭합니다.
3. 동작정보페이지가나타납니다.
4. 동작정보페이지에서다음정보를입력하거나수정합니다.
   - 이름**:** 동작을고유하게식별하는이름을입력합니다. 이것은필수필드입니다.
   - 설명**:** 동작의의미를설명합니다.
5. 다음을클릭합니다. 동작세부정보페이지가나타납니다.

   다음예제는 이벤트트리거를설정하는방법을보여줍니다. 다른트리거를선택할경우여기에표시된것과다른옵션이표시됩니다.



6. 동작세부정보페이지에서다음정보를입력하거나수정합니다.

   트리거목록에서이동작에대한이벤트트리거유형을클릭합니다. 각트리거의의미는다음과같습니다.

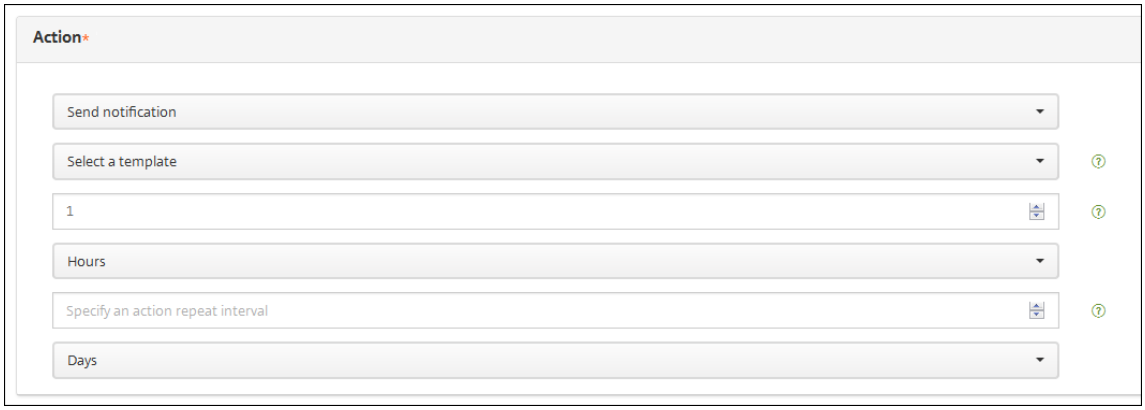
   - 이벤트**:** 미리정의된이벤트에반응합니다.
   - 장치속성**:** MDM 관리장치에서장치특정을확인하고이에반응합니다. 자세한내용은 장치속성이름및값을참조하십시오.
   - 사용자속성**:** 일반적으로 Active Directory 의사용자특성에반응합니다.
   - 설치된앱이름**:** 설치되는앱에반응합니다. MAM 전용모드에는적용되지않습니다. 장치에서앱인벤토리정책을사용하도록설정해야합니다. 앱인벤토리정책은모든플랫폼에서기본적으로사용하도록설정됩니다. 자세한내용은 앱인벤토리장치정책을참조하십시오.
7. 다음목록에서트리거에대한응답을클릭합니다.

8. 동작목록에서트리거조건이충족될때수행할동작을클릭합니다. 알림보내기를제외하고사용자가트리거를야기한문제를해결할수있는시간을선택합니다. 해당시간내에문제가해결되지않으면선택한동작이수행됩니다. 동작의정의는 보안동작을 참조하십시오.

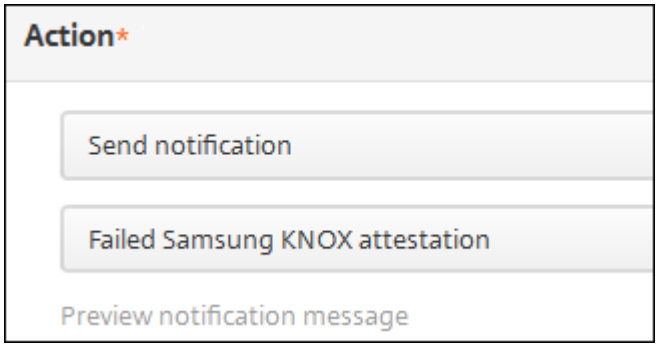
   알림보내기를선택하는경우다음단계를사용하여알림동작을보냅니다.

9. 다음목록에서알림에사용할템플릿을선택합니다. 해당알림유형에대한템플릿이없는경우를제외하고선택한이벤트와관련된알림템플릿이나타납니다. 해당하는템플릿이없는경우에는 "이이벤트유형에대한템플릿이없습니다" 라는메시지와함께 템플릿구성메시지가표시됩니다. 설정에서 알림템플릿을사용하여템플릿을만듭니다.

   사용자에게알림을보내려면 XenMobile 이메시지를보낼수있도록먼저 SMTP 및 SMS 에대한설정에서알림서버를구성해야합니다. 알림을참조하십시오. 또한계속하기전에사용하려는모든알림템플릿을설정합니다. 알림템플릿설정에대한자세한내용은 알림템플릿만들기및업데이트를참조하십시오.



   템플릿을선택한후 알림메시지미리보기를클릭하여알림을미리볼수있습니다.



10. 다음필드에서동작을수행하기전의지연기간을일, 시간또는분단위로설정합니다. 사용자가동작을트리거한문제를해결할때까지동작을반복할간격을설정합니다.

11. 요약에서의도한자동화동작이만들어졌는지확인합니다.

12. 동작세부정보를구성한후각플랫폼에대한배포규칙을개별적으로구성할수있습니다. 이렇게하려면선택한각플랫폼에대한 13 단계를완료합니다.
13. 배포규칙을구성합니다. 배포규칙구성에대한일반정보는 리소스배포를참조하십시오.

    이예에서:

    - 장치소유권은 **BYOD** 여야합니다.
    - 장치로컬암호화는 **True** 여야합니다.
    - 장치는암호규정을준수해야합니다.
    - 장치 MCC(모바일국가코드) 로안도라만지정될수는없습니다.
14. 동작에대한플랫폼배포규칙을구성한후 다음을클릭합니다. 동작할당페이지가나타나면여기에서배달그룹에동작을할당합니다. 이단계는선택사항입니다.
15. 배달그룹선택옆에서배달그룹을입력하여찾거나목록에서그룹을선택합니다. 선택한그룹이 앱할당을받을배달그룹목록에나타납니다.
16. 배포일정을확장하고다음설정을구성합니다.

    - 배포옆에서 켜짐을클릭하여배포를예약하거나 꺼짐을클릭하여배포를차단합니다. 기본옵션은 켜짐입니다. 꺼짐을선택하는경우다른옵션은필요하지않습니다.
    - 배포일정옆에서 지금또는 나중에를클릭합니다. 기본옵션은 지금입니다.
    - 나중에를클릭하는경우달력아이콘을클릭하고배포날짜와시간을선택합니다.
    - 배포조건옆에서 모든연결에서를클릭하거나 이전배포가실패한경우에만을클릭합니다. 기본옵션은 모든연결에서입니다.
    - 상시연결에대해배포옆에서 켜짐또는 꺼짐을클릭합니다. 기본옵션은 꺼짐입니다.

      설정 **>** 서버속성에서백그라운드배포예약키를구성한경우에만이옵션이적용됩니다. iOS 장치에는상시연결옵션을사용할수없습니다.

    구성하는배포일정은모든플랫폼에동일하게적용됩니다. 변경사항은모든플랫폼에적용되지만 상시연결에대해배포를선택한경우 iOS 에는적용되지않습니다.
17. 다음을클릭합니다. 요약페이지가나타나고여기서동작구성을확인할수있습니다.
18. 저장을클릭하여동작을저장합니다.

MAM 전용모드에대한앱잠금및앱초기화동작

XenMobile 콘솔에나열된모든 4 개범주의트리거 (이벤트, 장치속성, 사용자속성및설치된앱이름) 에대한응답으로장치의앱을초기화하거나잠글수있습니다.

자동앱초기화또는앱잠금을구성하려면

1. XenMobile 콘솔에서 구성 **>** 동작을클릭합니다.
2. 동작페이지에서 추가를클릭합니다.
3. 동작정보페이지에서동작이름과선택적설명을입력합니다.
4. 동작세부정보페이지에서원하는트리거를선택합니다.
5. 동작에서동작을선택합니다.

   이단계에서는다음조건을유의하십시오.

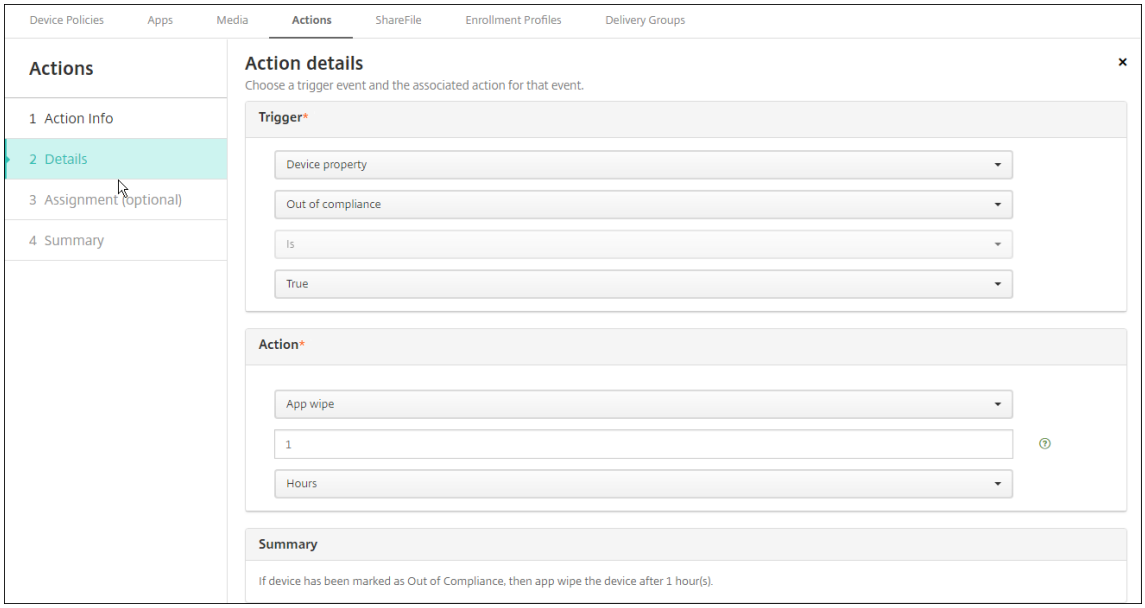
   트리거유형이 이벤트이고값이 **Active Directory** 에서사용하지않도록설정된사용자인경우 앱초기화및 앱잠금동작이표시되지않습니다.

   트리거유형이 장치속성이고값이 **MDM** 분실모드활성화인경우다음동작이표시되지않습니다.

   - 장치를선택적으로초기화
   - 장치를완전히초기화
   - 장치해지

   각옵션에대해 1 시간이지연이자동으로설정되지만지연기간을분, 시간또는일단위로선택할수있습니다. 지연의목적은동작이발생하기전에사용자에게문제를수정할시간을주기위한것입니다. 앱초기화및앱잠금동작에대한자세한내용은 보안동작을참조하십시오.

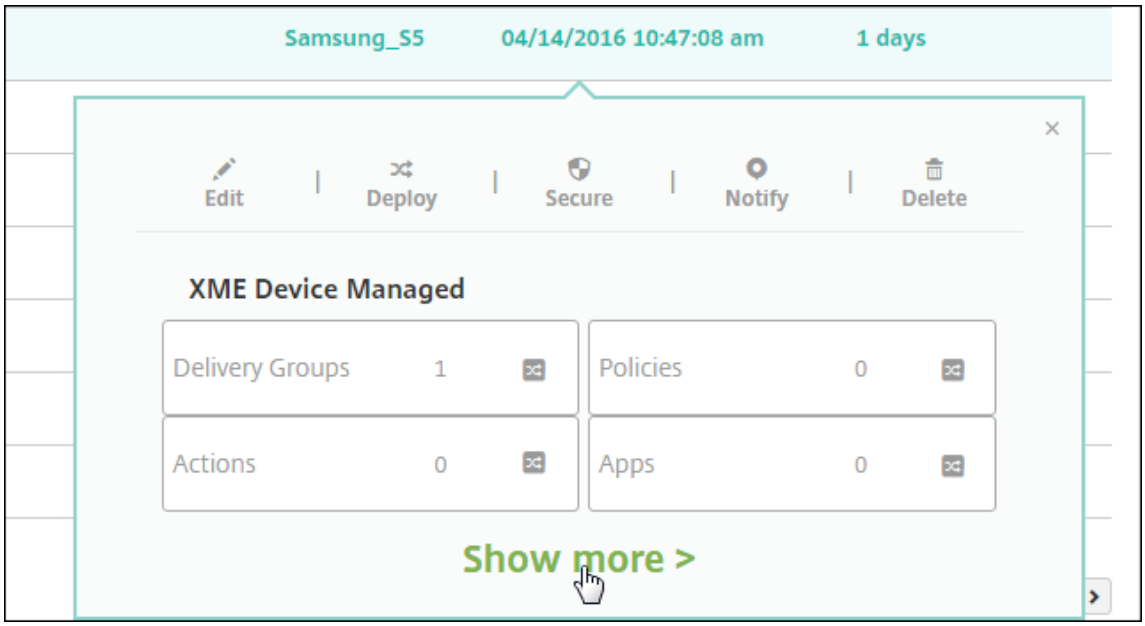
   > 참고**:**
   >
   > 트리거를 이벤트로설정하는경우반복간격은자동으로최소 1 시간으로설정됩니다. 알림을수신하려면장치에서정책새로고침을수행하여서버와동기화해야합니다. 일반적으로장치는사용자가로그온하거나 Secure Hub 를통해수동으로정책을새로고칠때서버와동기화됩니다.
   >
   > Active Directory 데이터베이스가 XenMobile 과동기화될수있도록동작이수행되기전에약 1 시간의추가지연이발생할수있습니다.



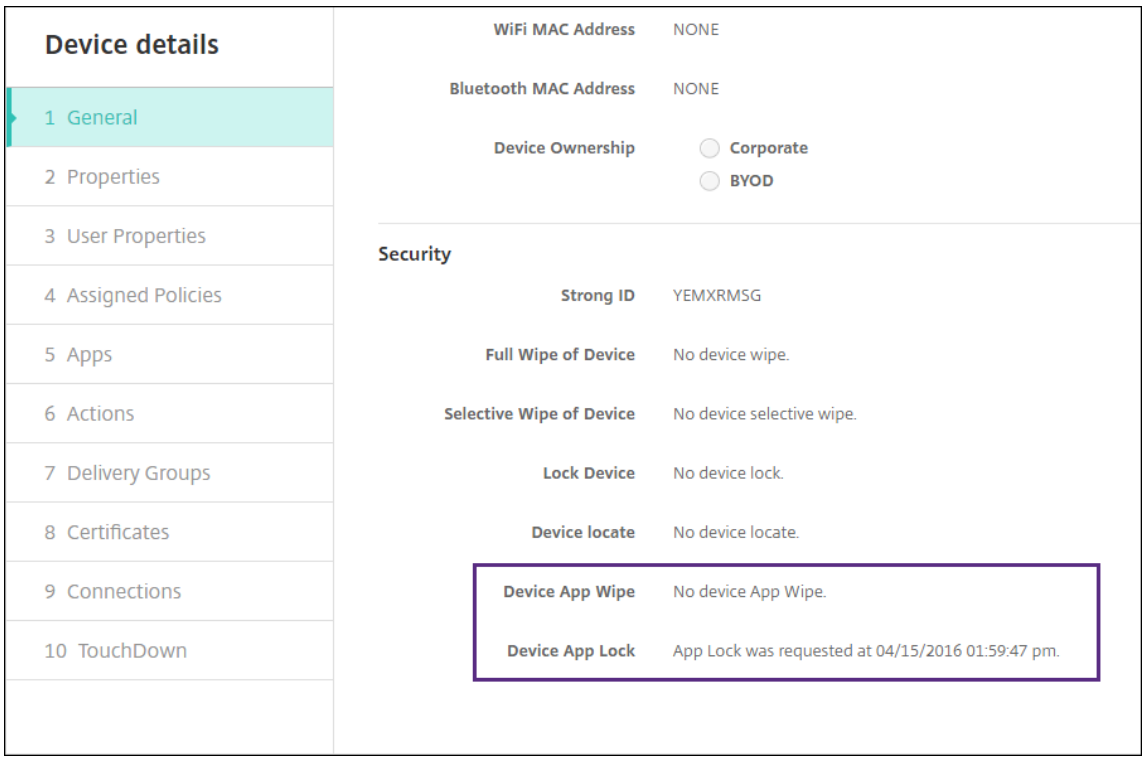
6. 배포규칙을구성하고 다음을클릭합니다.
7. 배달그룹할당및배포일정을구성하고 다음을클릭합니다.
8. 저장을클릭합니다.

앱잠금또는앱초기화상태를확인하려면

1. 관리 **>** 장치로이동하고장치를클릭한후 자세히표시를클릭합니다.



2. 장치앱초기화및 장치앱잠금으로스크롤합니다.



장치가초기화되면 PIN 코드를입력하라는메시지가표시됩니다. 사용자가코드를잊은경우장치세부정보에서코드를조회할 수있습니다.

모니터링및지원

January 5, 2022

XenMobile 대시보드및 XenMobile 지원페이지를사용하여 XenMobile Server 를모니터링하고문제를해결할수있습니다. XenMobile 지원페이지를사용하여지원관련정보및도구에액세스합니다.

온-프레미스 XenMobile Server 의경우 XenMobile CLI 에서도동작을수행할수있습니다. 자세한내용은 CLI(명령줄인터페이스) 옵션을참조하십시오.

XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다.

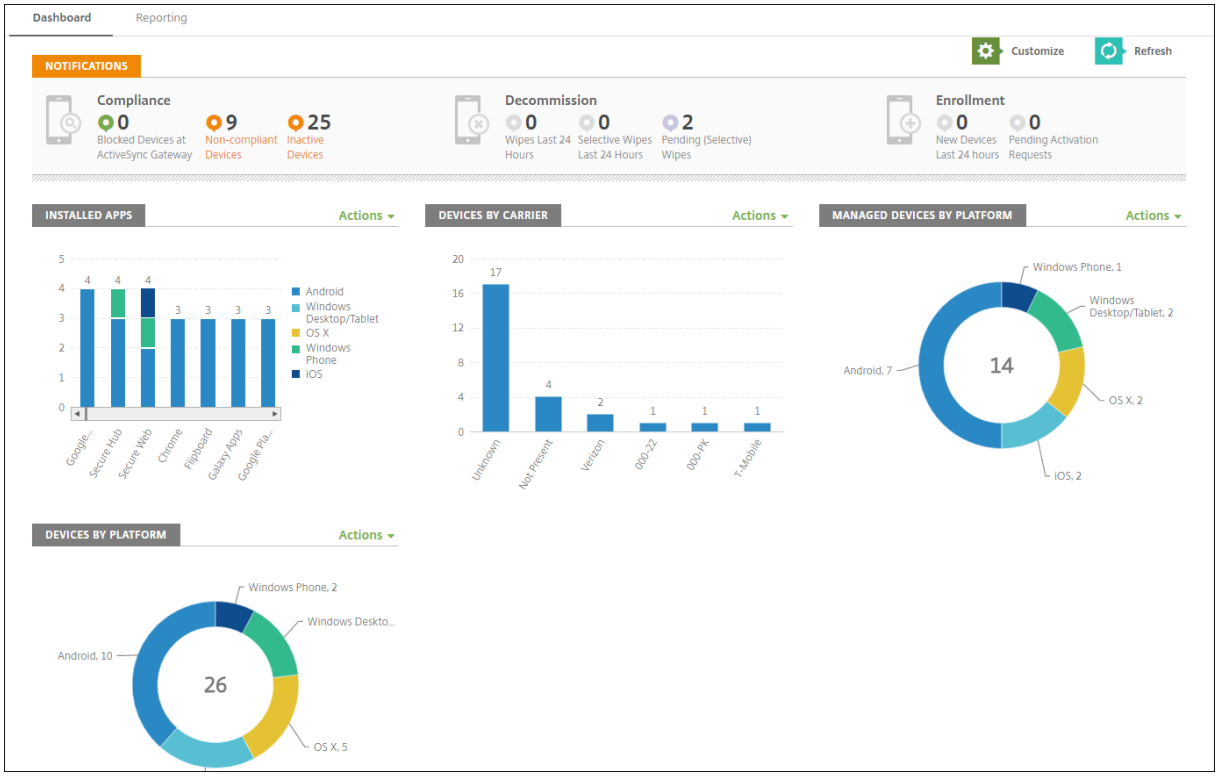
문제해결및지원페이지가표시됩니다.

XenMobile 지원페이지를사용하여다음을수행합니다.

- 진단액세스
- 지원번들만들기 (온-프레미스설치에만해당)

- Citrix 제품설명서및 Knowledge Center 에대한링크액세스
- 로그작업액세스
- 고급구성옵션사용
- 도구및유틸리티집합액세스

또한 XenMobile 콘솔대시보드에액세스하여정보를한눈에볼수있습니다. 이러한정보를사용하면위젯을통해신속하게문제점과 성공여부를확인할수있습니다.

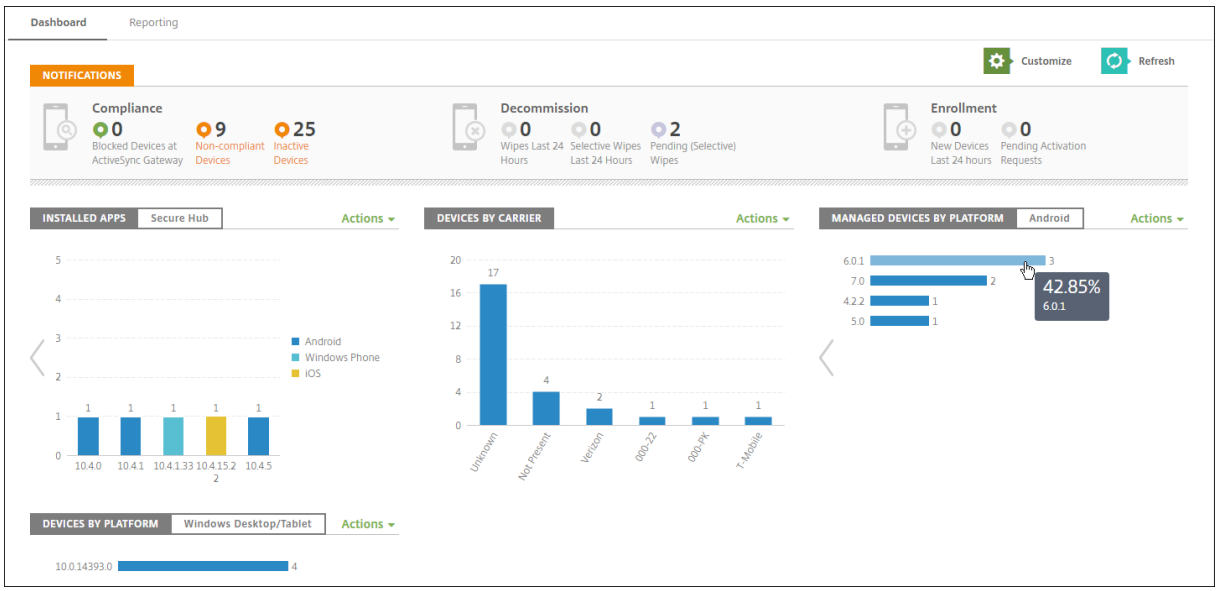


대시보드는일반적으로 XenMobile 콘솔에로그온할때처음나타나는페이지입니다. 콘솔의다른곳에서대시보드에액세스하려면 분석을클릭합니다. 페이지의레이아웃을편집하고나타나는위젯을편집하려면대시보드에서 사용자지정을클릭합니다.

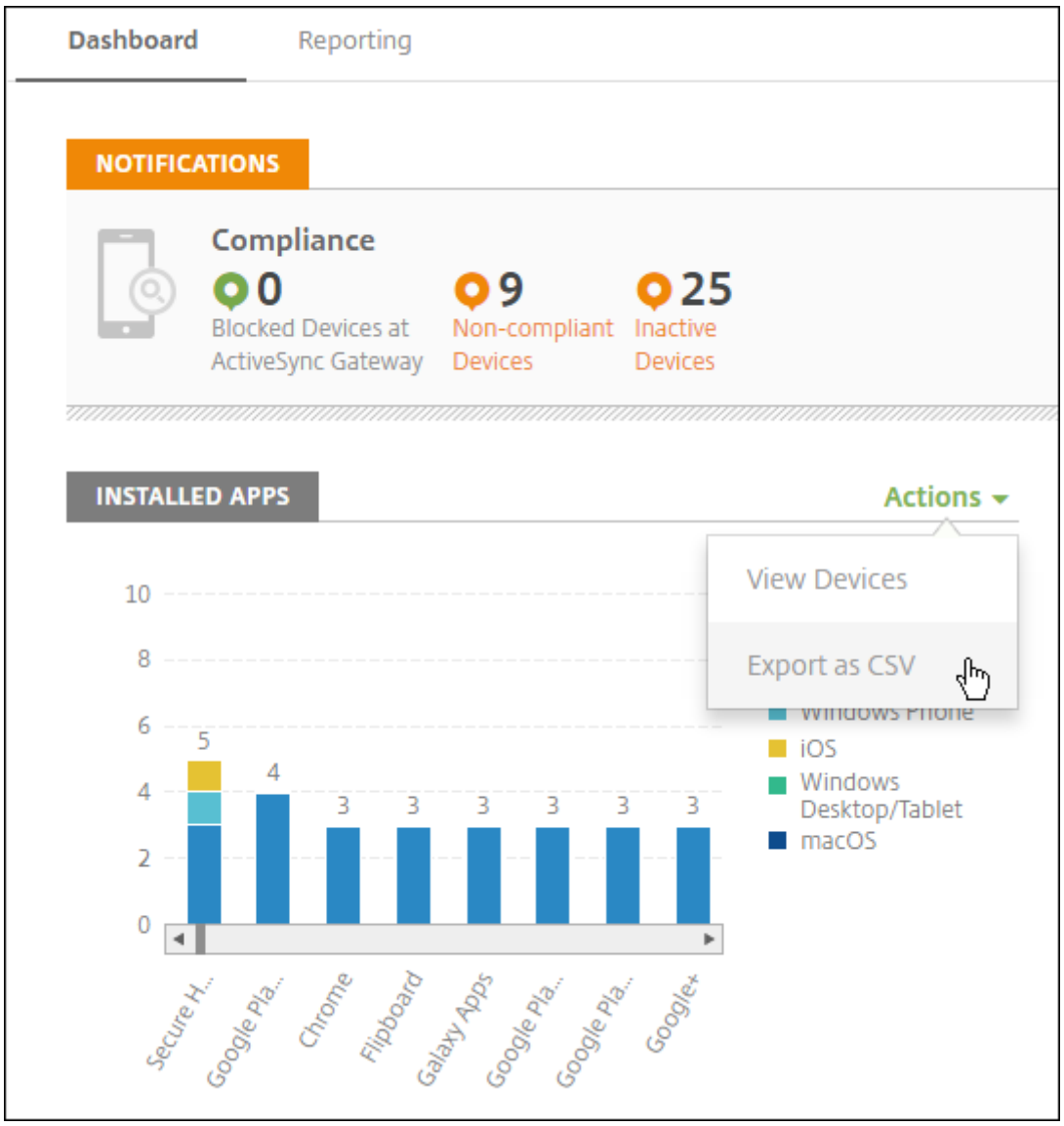
- 내대시보드**:** 최대네개의대시보드를저장할수있습니다. 이러한대시보드를개별적으로편집하고저장된대시보드를선택하여 각대시보드를볼수있습니다.
- 레이아웃스타일**:** 이행에서는대시보드에표시되는위젯수와위젯배치방법을선택할수있습니다.
- 위젯선택**:** 대시보드에표시할정보를선택할수있습니다.
  - 알림**:** 왼쪽의숫자위에있는확인란을선택하여위젯위에알림표시줄을추가합니다. 이표시줄에는규격장치, 비활성장 치및지난 24 시간동안초기화되거나등록된장치의수가표시됩니다.
  - 장치 **(**플랫폼기준**):** 플랫폼별로관리되는장치와관리되지않는장치의수를표시합니다.
  - 장치 **(**이동통신사업자기준**):** 이동통신사업자별로관리되는장치와관리되지않는장치의수를표시합니다. 각표시줄 을클릭하여플랫폼별분석을볼수있습니다.
  - 관리되는장치 **(**플랫폼기준**):** 플랫폼별로관리되는장치의수를표시합니다.
  - 관리되지않는장치 **(**플랫폼기준**):** 플랫폼별로관리되지않는장치의수를표시합니다. 이차트에나타나는장치는에이 전트가설치되어있지만권한이해지되었거나초기화되었을수있습니다.

- 장치 **(ActiveSync Gateway** 상태기준**):** ActiveSync Gateway 상태별로그룹화된장치수를표시합니다. 정보에는차단됨, 허용됨또는알수없음상태가표시됩니다. 각표시줄을클릭하여플랫폼별로데이터를분류할수있습니다.
- 장치 **(**소유권기준**):** 소유권상태별로그룹화된장치수를표시합니다. 정보에는회사소유, 직원소유또는알수없는소유권상태가표시됩니다.
- 실패한배달그룹배포**:** 패키지당실패한배포의총수를표시합니다. 배포에실패한패키지만나타납니다.
- 장치 **(**차단된이유기준**):** ActiveSync 에의해차단된장치의수를표시합니다.
- 설치된앱**:** 앱정보의그래프에대한앱이름을입력합니다.
- 볼륨구매앱라이센스사용현황**:** Apple 볼륨구매앱에대한라이센스사용현황통계를표시합니다.

각위젯에서개별부분을클릭하여자세한정보를드릴다운할수있습니다.



또한 동작드롭다운을클릭하여정보를.csv 파일로내보낼수도있습니다.

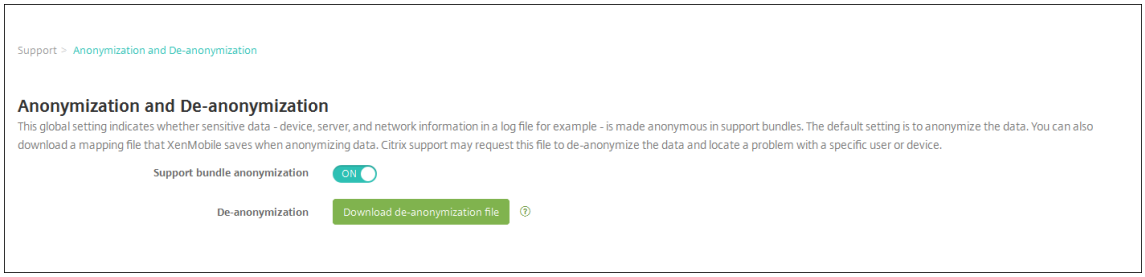


지원번들의데이터익명화

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.

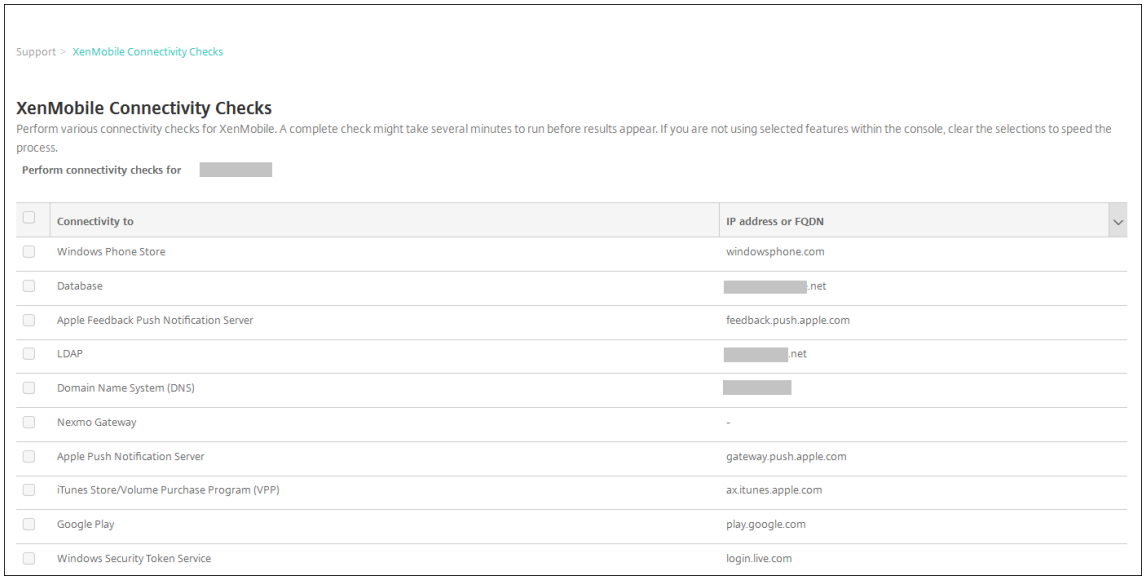
연결확인

December 1, 2020

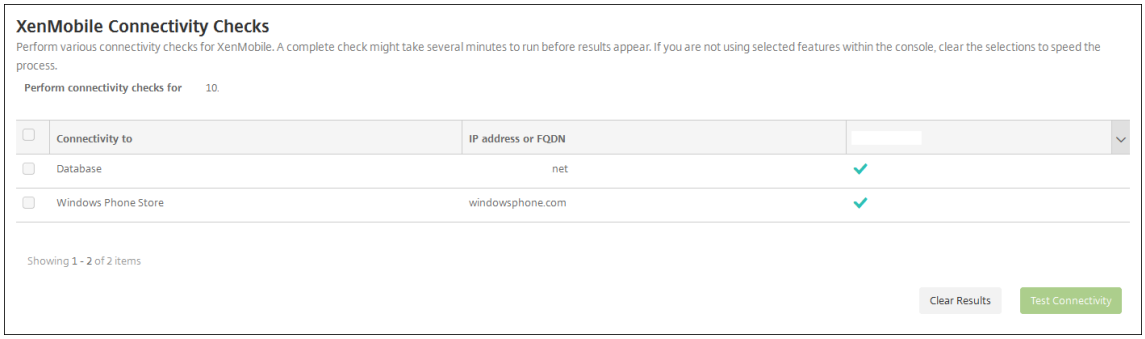
XenMobile 지원페이지에서 Citrix Gateway 및기타서버/위치에대한 XenMobile 연결을확인할수있습니다.

XenMobile 연결확인수행

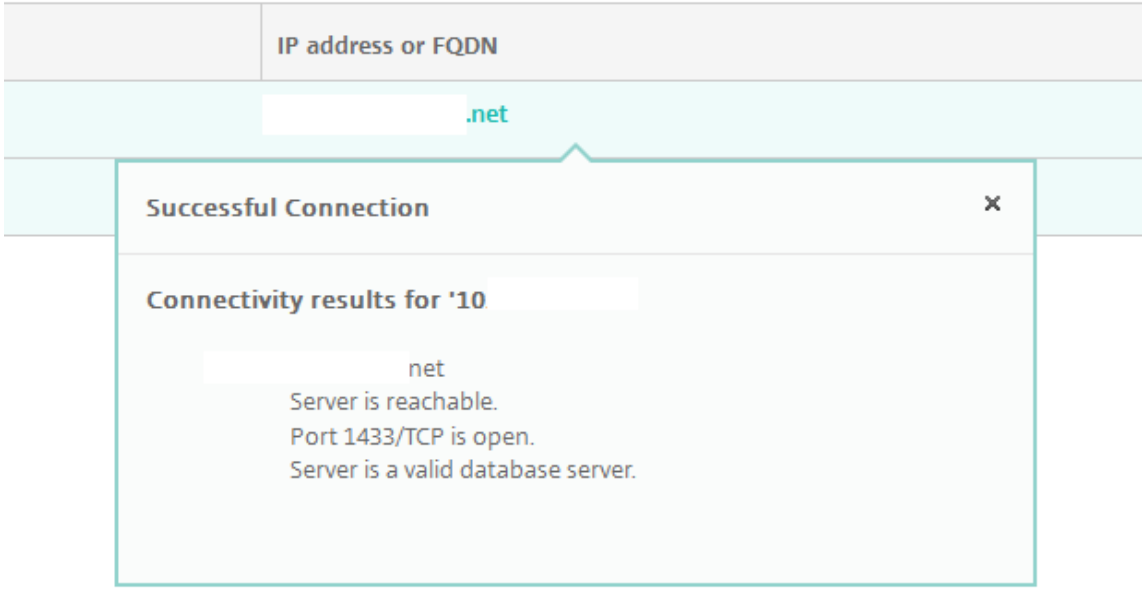
1. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다. 지원페이지가나타납니다.
2. 진단아래에서 **XenMobile** 연결확인을클릭합니다. **XenMobile** 연결확인페이지가나타납니다. XenMobile 환경에클러스터된노드가포함되는경우모든노드가표시됩니다.



3. 연결테스트에포함할서버를선택한후 연결테스트를클릭합니다. 테스트결과페이지가나타납니다.

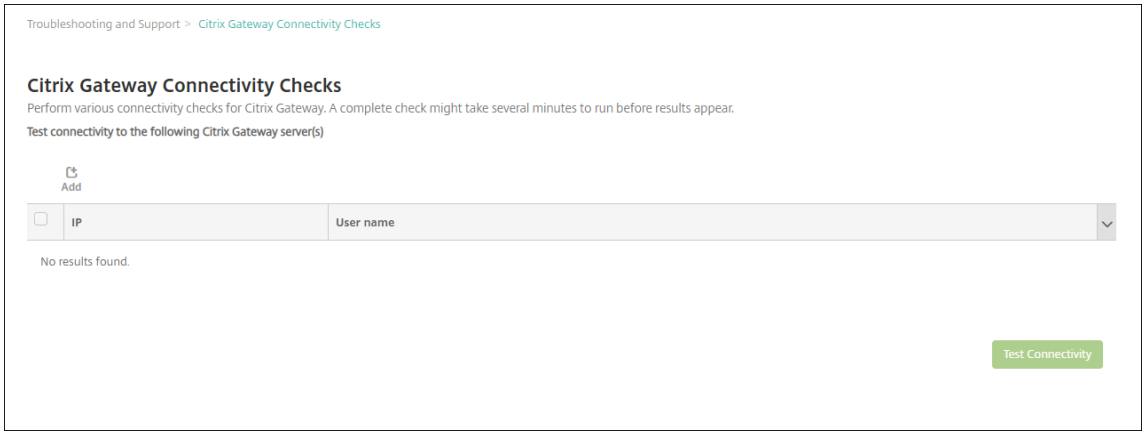


4. 테스트결과테이블에서서버를선택하여해당서버에대한자세한결과를확인합니다.

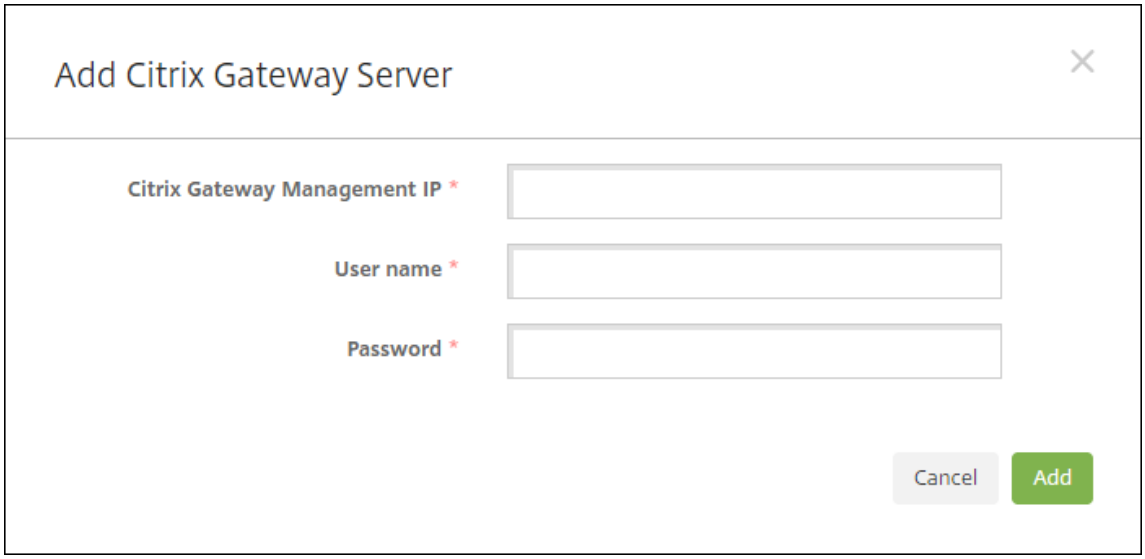


Citrix Gateway 연결확인수행

1. 지원페이지의 진단아래에서 **Citrix Gateway** 연결확인을클릭합니다. **Citrix Gateway** 연결확인페이지가나타납니다. Citrix Gateway 서버를추가하지않은경우테이블은비어있습니다.



2. 추가를클릭합니다. **Citrix Gateway** 서버추가대화상자가나타납니다.



3. **Citrix Gateway** 관리 **IP** 에서테스트하려는 Citrix Gateway 가실행되는서버의관리 IP 주소를입력합니다.

> 참고:
>
> 이전에이미추가된 Citrix Gateway 서버에대한연결확인을수행하는경우해당 IP 주소가제공됩니다.

4. 이 Citrix Gateway 의관리자자격증명을입력합니다.

> 참고:
>
> 이전에이미추가된 Citrix Gateway 서버에대한연결확인을수행하는경우해당사용자이름이제공됩니다.

5. 추가를클릭합니다. Citrix Gateway 가 **Citrix Gateway** 연결확인페이지의테이블에추가됩니다.
6. Citrix Gateway 서버를선택한후에 연결테스트를클릭합니다. 테스트결과테이블에결과가표시됩니다.
7. 테스트결과테이블에서서버를선택하여해당서버에대한자세한결과를확인합니다.

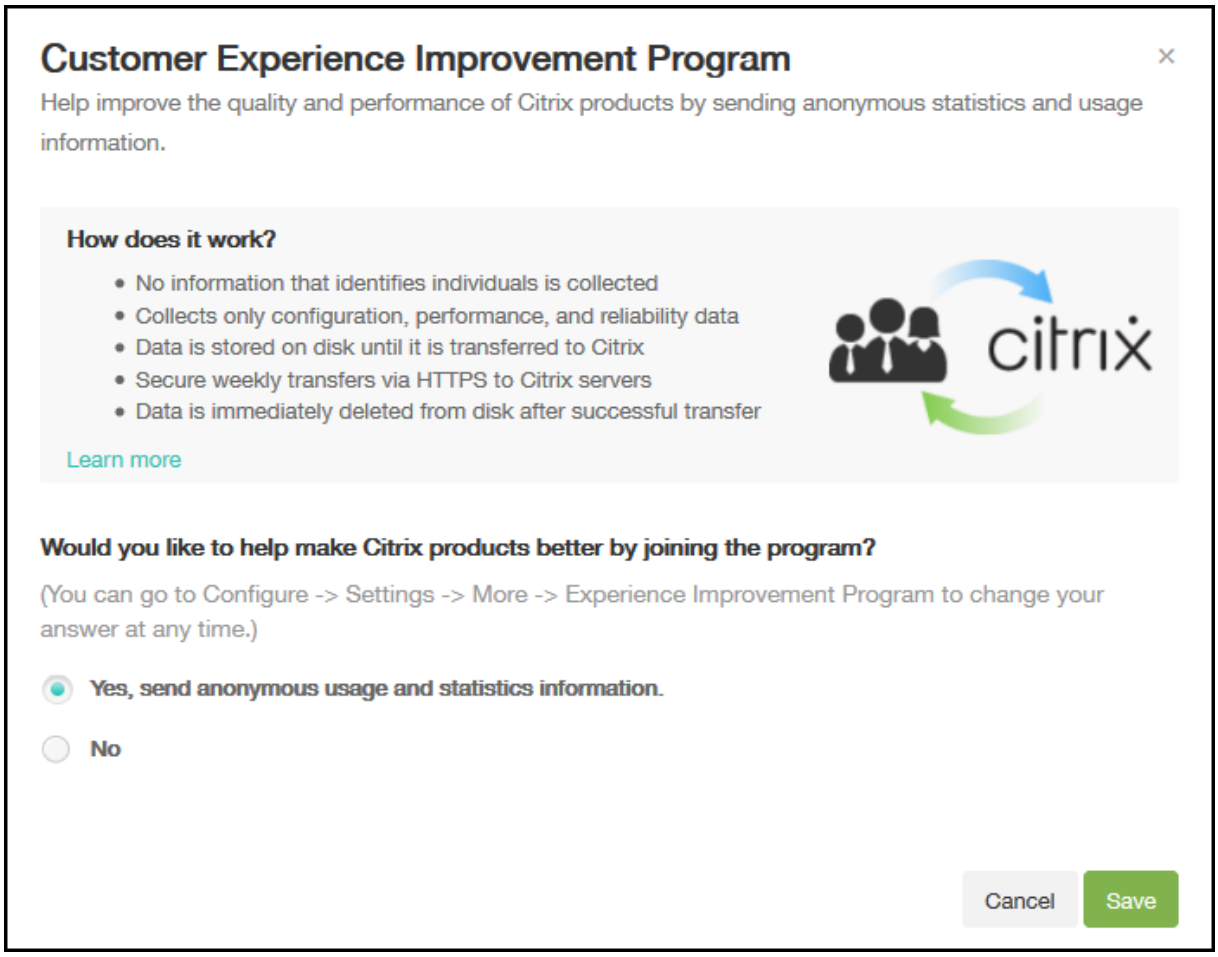
사용자환경개선프로그램

January 5, 2022

Citrix CEIP(사용자환경개선프로그램) 는 XenMobile 에서익명의구성및사용현황데이터를수집하여 Citrix 에보냅니다. 이데이터는 Citrix 가 XenMobile 의품질, 안정성및성능을개선하는데도움이됩니다. CEIP 참여는전적으로자발적입니다. XenMobile 을처음설치하거나업데이트를설치할때 CEIP 참여를선택할수있습니다. 참여하는경우일반적으로주단위로데이터가수집되며성능및사용현황데이터는매시간수집됩니다. 데이터는디스크에저장되고 HTTPS 를통해안전하게 Citrix 로매주전송됩니다. XenMobile 콘솔에서 CEIP 참여여부를변경할수있습니다. CEIP 에대한자세한내용은 About the Citrix Customer Experience Improvement Program (CEIP)(Citrix CEIP(사용자환경개선프로그램) 정보)를참조하십시오.

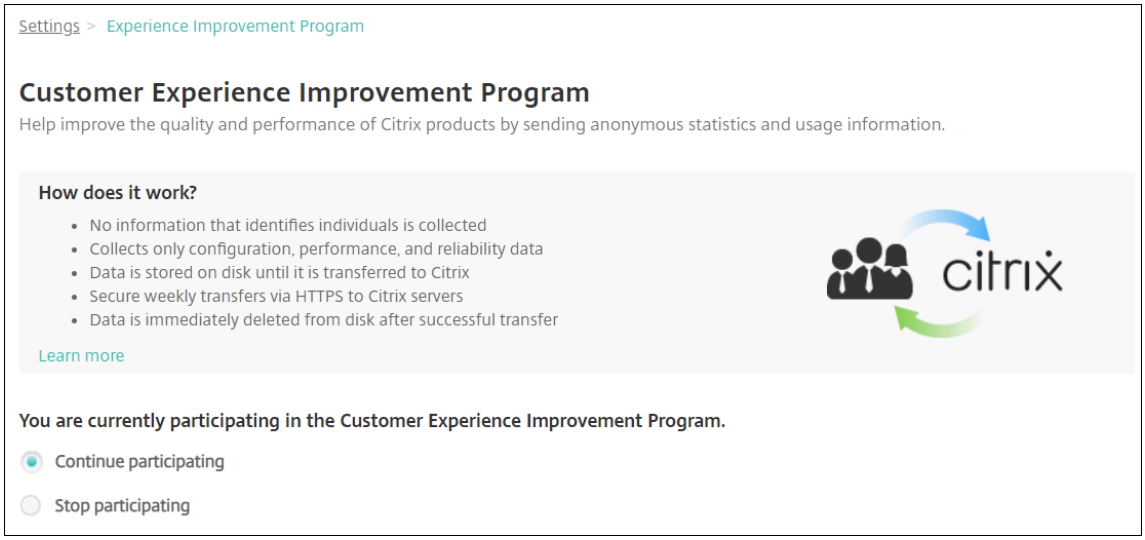
CEIP 참여선택

XenMobile 을처음설치하거나업데이트를수행하면참여할지를묻는다음대화상자가표시됩니다.



CEIP 참여설정변경

1. CEIP 참여설정을변경하려면 XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭하여 설정페이지를엽니다.
2. 서버에서 환경개선프로그램을클릭합니다. 사용자환경개선프로그램페이지가나타납니다. 표시되는정확한페이지는현재 CEIP 참여여부에따라다릅니다.



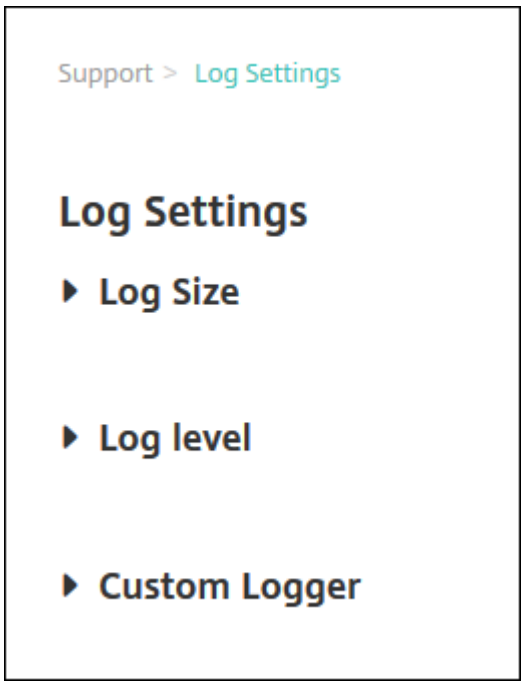
3. 현재 CEIP 에참여중이고참여를중지하려는경우 참여중지를클릭합니다.
4. 현재 CEIP 에참여하고있지않고참여를시작하려는경우 참여시작을클릭합니다.
5. 저장을클릭합니다.

로그

January 6, 2020

XenMobile 에서생성하는로그출력을사용자지정하도록로그설정을구성할수있습니다. 클러스터된 XenMobile 서버가있는경우 XenMobile 콘솔에서로그설정을구성하면해당설정이클러스터의다른모든서버와공유됩니다.

1. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다. 지원페이지가나타납니다.
2. 로그작업아래에서 로그설정을클릭합니다. 로그설정페이지가나타납니다.

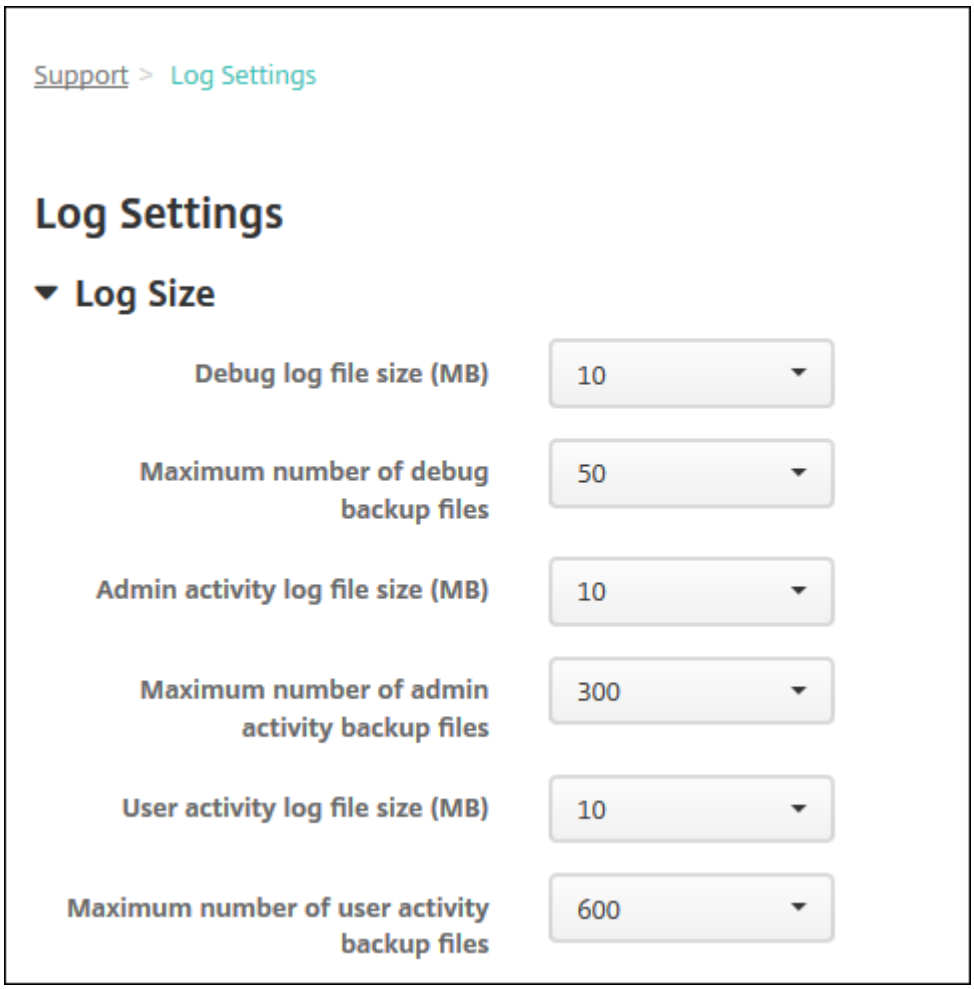


로그설정페이지에서다음과같은옵션에액세스할수있습니다.

- 로그크기. 이옵션을사용하여로그파일의크기와데이터베이스에유지되는최대로그백업파일수를제어합니다. 로그크기는 XenMobile 에서지원하는각로그 (디버그로그, 관리자작업로그및사용자작업로그) 에적용됩니다.
- 로그수준. 이옵션을사용하여로그수준을변경하거나설정을유지할수있습니다.
- 사용자지정로거. 이옵션을사용하여사용자지정로거를만듭니다. 사용자지정로그에는클래스이름과로그수준이필요합니다.

로그크기옵션을구성하려면

1. 로그설정페이지에서 로그크기를확장합니다.



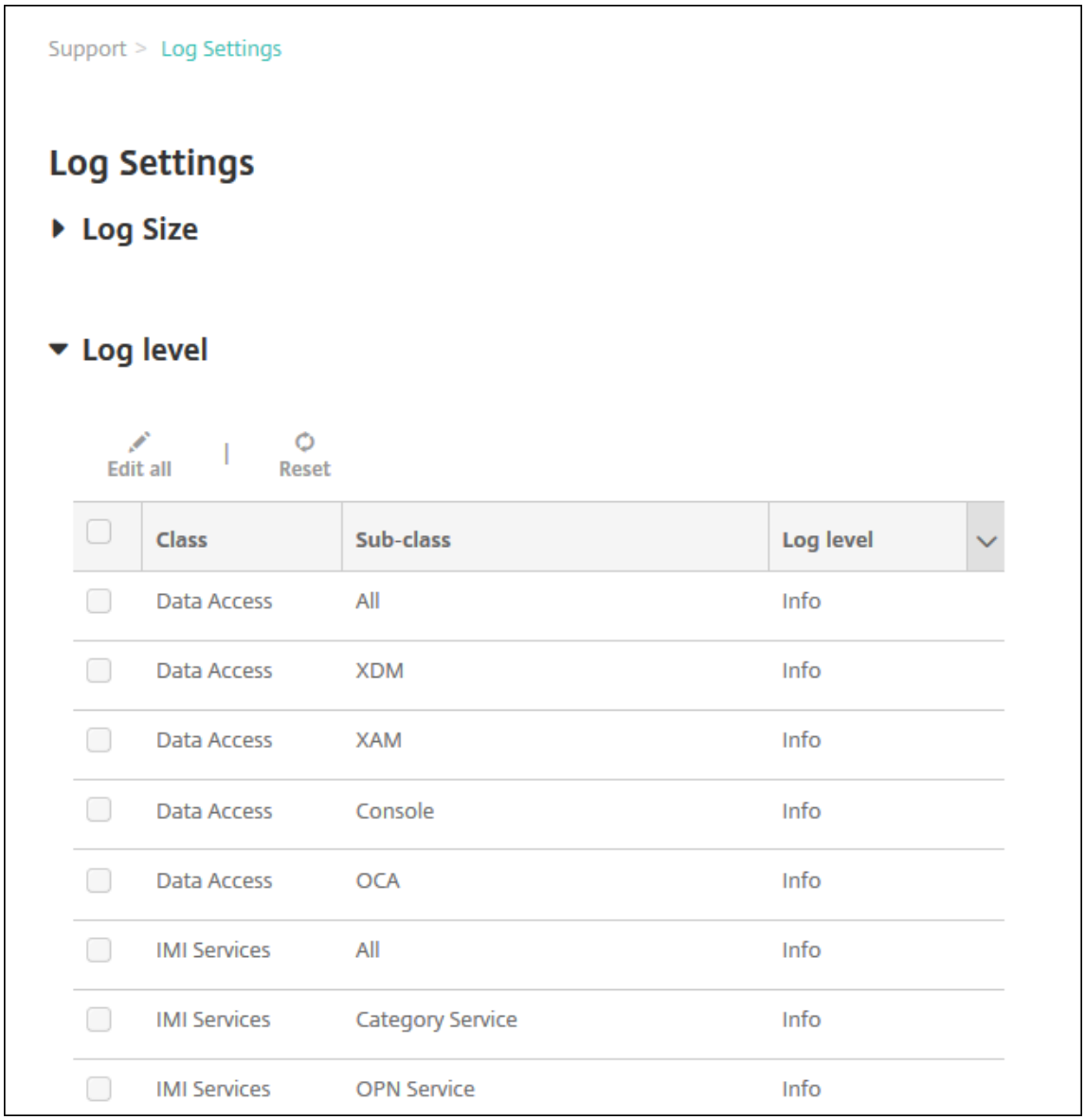
2. 다음설정을구성합니다.

   - 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.

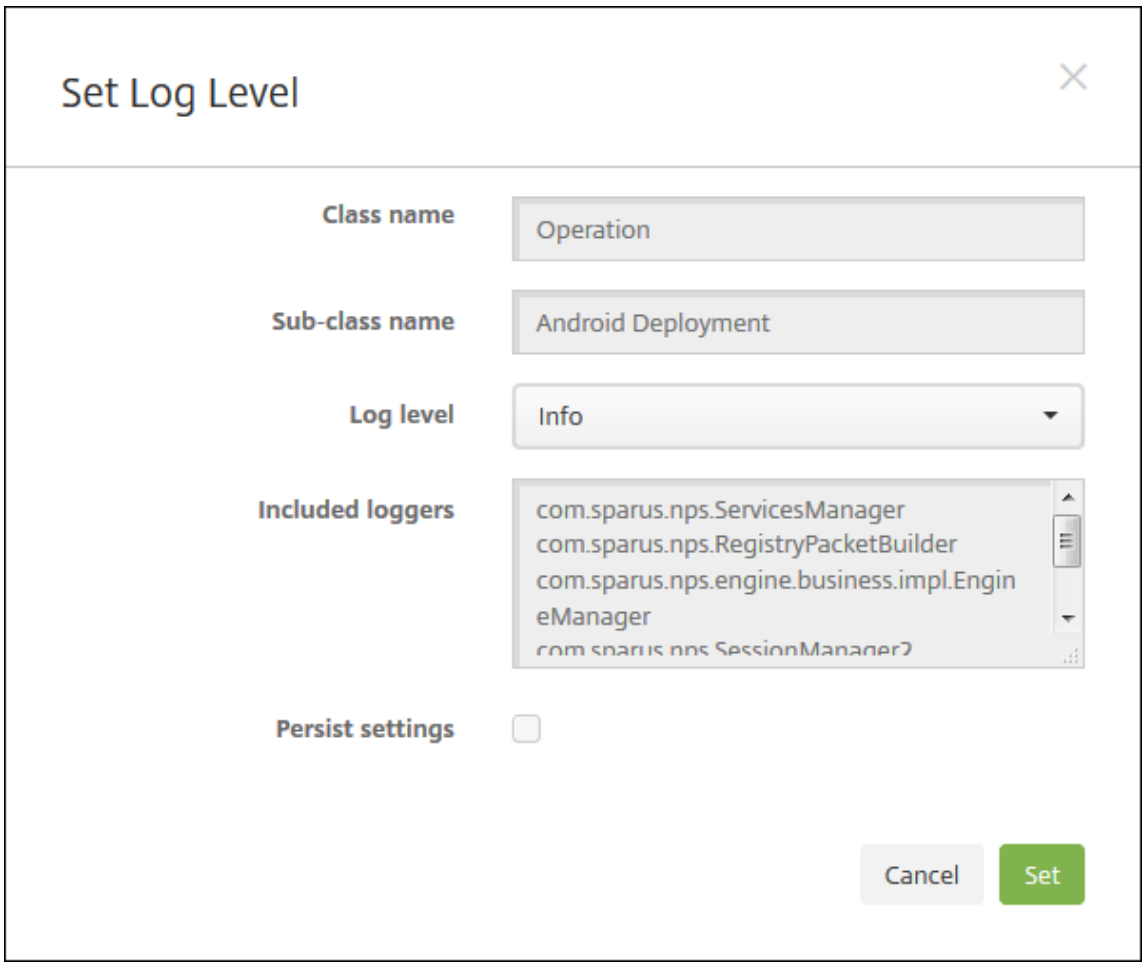
1. 로그설정페이지에서 로그수준을확장합니다. 모든로그클래스의테이블이나타납니다.



2. 다음중하나를수행합니다.

   - 원하는클래스옆에있는확인란을클릭한다음 수준설정을클릭하여해당클래스의로그수준을변경합니다.
   - 모두편집을클릭하여로그수준변경내용을테이블의모든클래스에적용합니다.

   로그수준을설정하고 XenMobile 서버를다시부팅할때로그수준설정을유지할지여부를선택할수있는 로그수준설정대화상자가나타납니다.

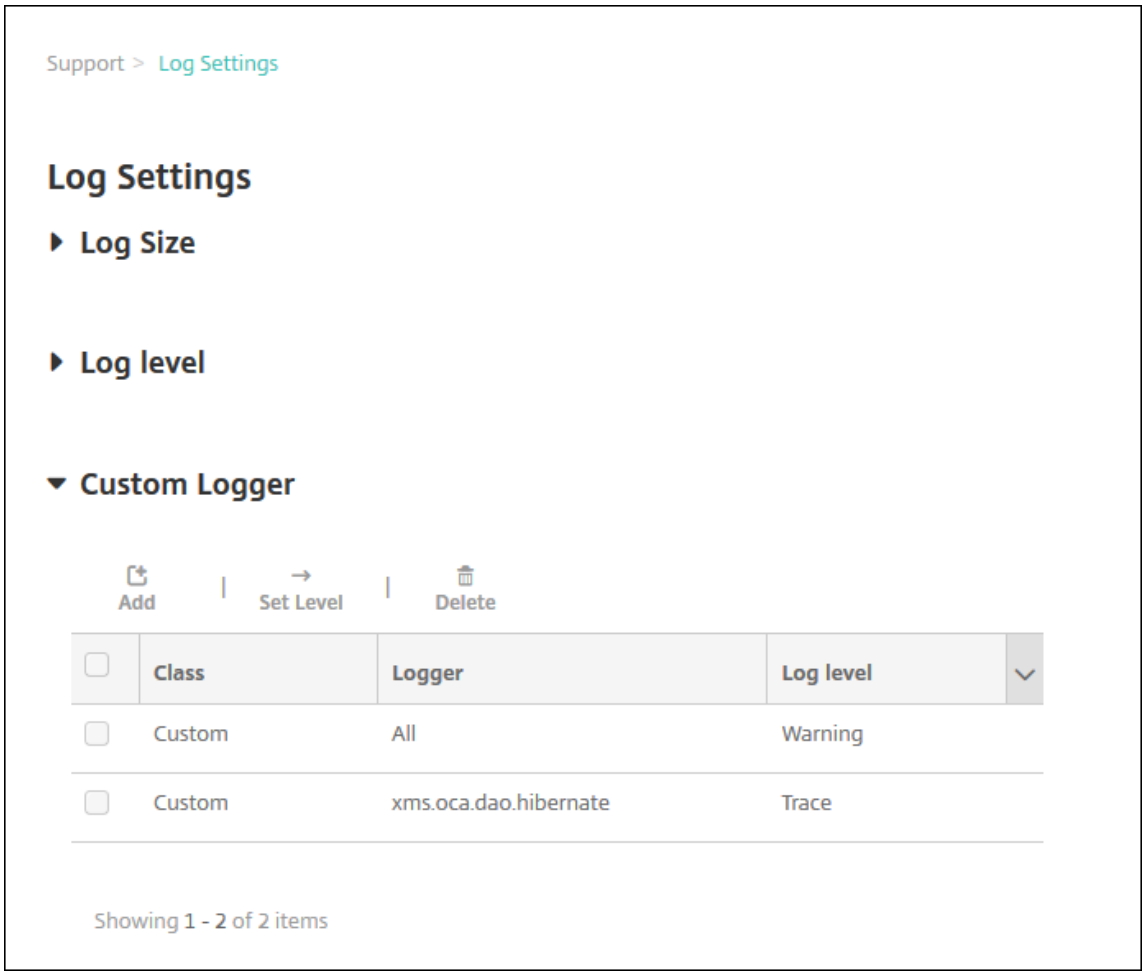


- 클래스이름**:** 모든클래스의로그수준을변경할때에는이필드에 '모두' 가표시되지만, 그렇지않은경우에는개별클래스이름이표시됩니다. 이필드는편집할수없습니다.
- 하위클래스이름**:** 모든클래스의로그수준을변경할때에는이필드에 '모두' 가표시되지만, 그렇지않은경우에는개별클래스의하위클래스이름이표시됩니다. 이필드는편집할수없습니다.
- 로그수준**:** 목록에서로그수준을클릭합니다. 지원되는로그수준은다음과같습니다.
  - 심각
  - 오류
  - 경고
  - 정보
  - 디버그
  - 추적
  - 꺼짐
- 포함된로거**:** 모든클래스의로그수준을변경하는경우에는이필드가비어있지만개별클래스의경우에는현재구성된로거가표시됩니다. 이필드는편집할수없습니다.
- 설정유지**:** 서버를다시부팅할때로그수준설정을유지하려면이확인란을선택합니다. 이확인란을선택하지않으면서버를다시부팅할때로그수준설정이기본값으로되돌아갑니다.

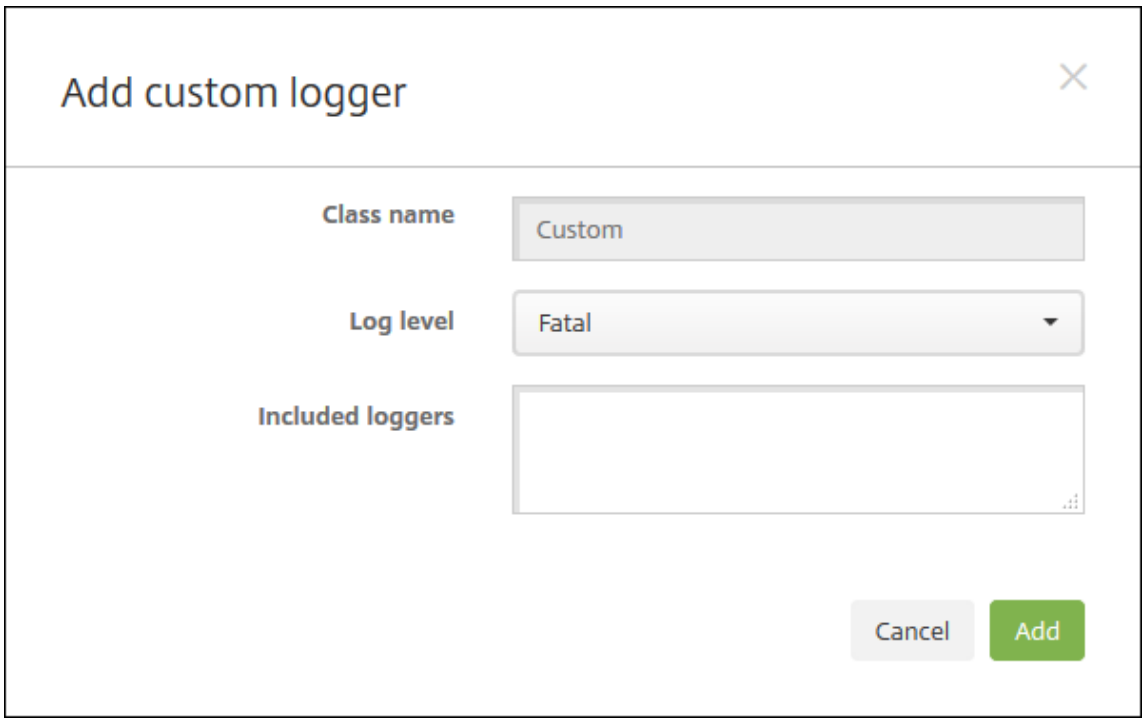
3. 설정을클릭하여변경내용을커밋합니다.

사용자지정로거를추가하려면

1. 로그설정페이지에서 사용자지정로거를확장합니다. 사용자지정로거테이블이나타납니다. 사용자지정로거를추가하지않은경우에는테이블이비어있습니다.



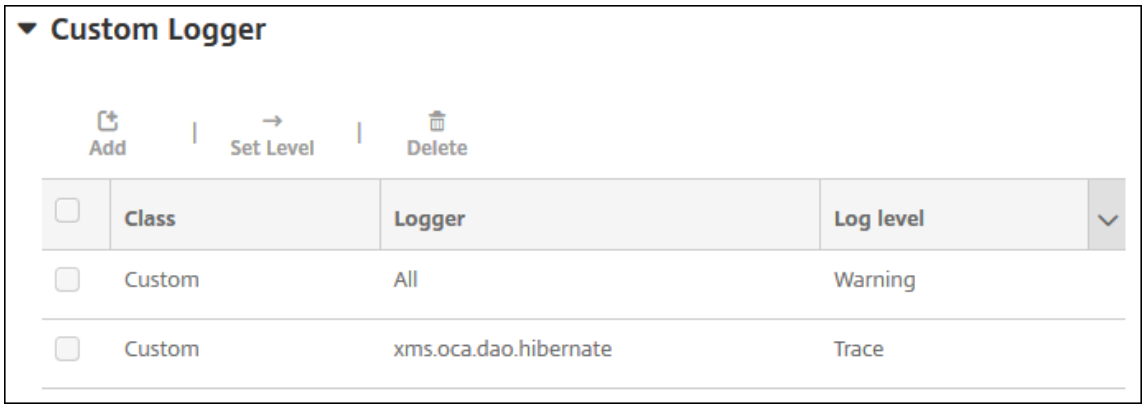
2. 추가를클릭합니다. 사용자지정로거추가대화상자가나타납니다.



3. 다음설정을구성합니다.

   - 클래스이름**:** 이필드에는 사용자지정이표시됩니다. 이필드는편집할수없습니다.
   - 로그수준**:** 목록에서로그수준을클릭합니다. 지원되는로그수준은다음과같습니다.
     - 심각
     - 오류
     - 경고
     - 정보
     - 디버그
     - 추적
     - 꺼짐
   - 포함된로거**:** 사용자지정로거에포함시키려는특정로거를입력하거나모든로거를포함시키려면필드를비워둡니다.

4. 추가를클릭합니다. 사용자지정로거가 사용자지정로거테이블에추가됩니다.



사용자지정로거를삭제하려면

1. 로그설정페이지에서 사용자지정로거를확장합니다.
2. 삭제할사용자지정로거를선택합니다.
3. 삭제를클릭합니다. 사용자지정로거를삭제할지묻는대화상자가나타납니다. 확인을클릭합니다.

> 중요:
>
> 이작업은실행취소할수없습니다.

모바일서비스공급자

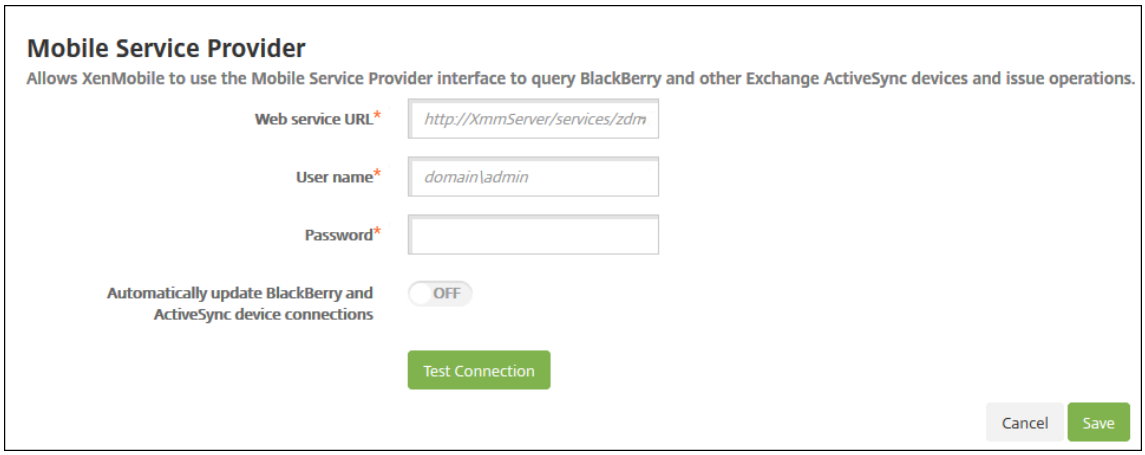
January 6, 2020

XenMobile 에서모바일서비스공급자인터페이스를사용하여 BlackBerry 및 Exchange ActiveSync 장치를쿼리하고작업을실행할수있습니다.

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.



3. 다음설정을구성합니다.
   - 웹서비스 **URL:** 웹서비스의 URL 을입력합니다 (예: `https://<XmmServer>/services/xdmservice`).
   - 사용자이름: domain\admin 형식으로사용자이름을입력합니다.

- 암호**:** 암호를입력합니다.
- **BlackBerry** 및 **ActiveSync** 장치연결자동업데이트**:** 장치연결을자동으로업데이트할지여부를선택합니다. 기본값은 꺼짐입니다.
- 연결테스트를클릭하여연결을확인합니다.

4. 저장을클릭합니다.

보고서

August 10, 2020

XenMobile 은앱및장치배포를분석하는데사용할수있는미리정의된보고서를제공합니다. 각보고서는표와차트로표시됩니다. 열을기준으로표를정렬하고필터링할수있습니다. 차트의특정요소를선택하여더자세한정보를볼수있습니다.

- 앱배포총시도횟수**:** 사용자가자신의장치에설치하려고시도한배포된앱을나열합니다.
- 플랫폼별앱**:** 앱과앱버전을장치플랫폼및버전별로나열합니다.
- 유형별앱**:** 버전, 유형및범주별로앱을나열합니다.
- 장치등록**:** 등록된모든장치를나열합니다.
- 장치및앱**:** 관리되는앱을실행중인장치를나열합니다.
- 비활성장치**:** XenMobile Server 속성 device.inactivity.days.threshold 로지정된일수동안활동이없었던장치의목록입니다.
- 탈옥/루팅장치**:** 탈옥 iOS 장치및루팅 Android 장치를나열합니다.
- 약관**:** 약관계약에동의및거부한사용자를나열합니다. 차트일부를선택하여더자세히볼수있습니다.
- 상위 **10** 개앱**:** 배포에실패한앱을 10 개까지나열합니다.
- 장치및사용자의블랙리스트앱**:** 사용자의장치에있는차단된앱을나열합니다.

  > 참고**:**
  >
  > XenMobile Server 콘솔에는 “블랙리스트” 및 “화이트리스트” 라는용어가포함됩니다. 향후릴리스에서이러한용어를 “차단목록” 및 “허용목록” 으로변경하는중입니다.

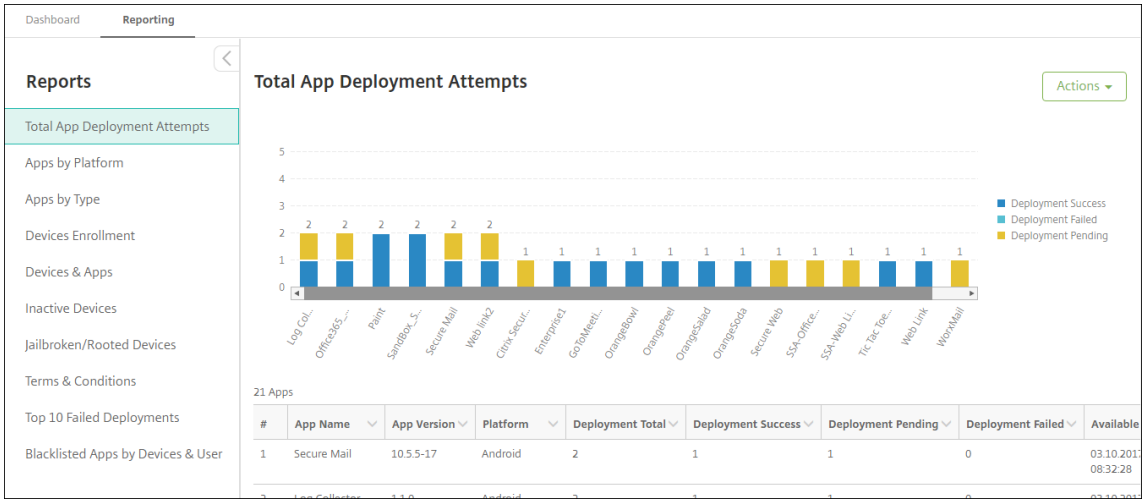
- 규정을준수하지않는장치**:** 장치의탈옥여부, OS 버전실행여부, 장치에암호가있는지여부와같은규정준수기준을충족하지않는장치를나열합니다.

각표의데이터를.csv 형식으로내보낼수있으며 Microsoft Excel 과같은프로그램을사용하여열수있습니다. 각보고서의차트를 PDF 형식으로내보낼수있습니다.

보고서를생성하려면

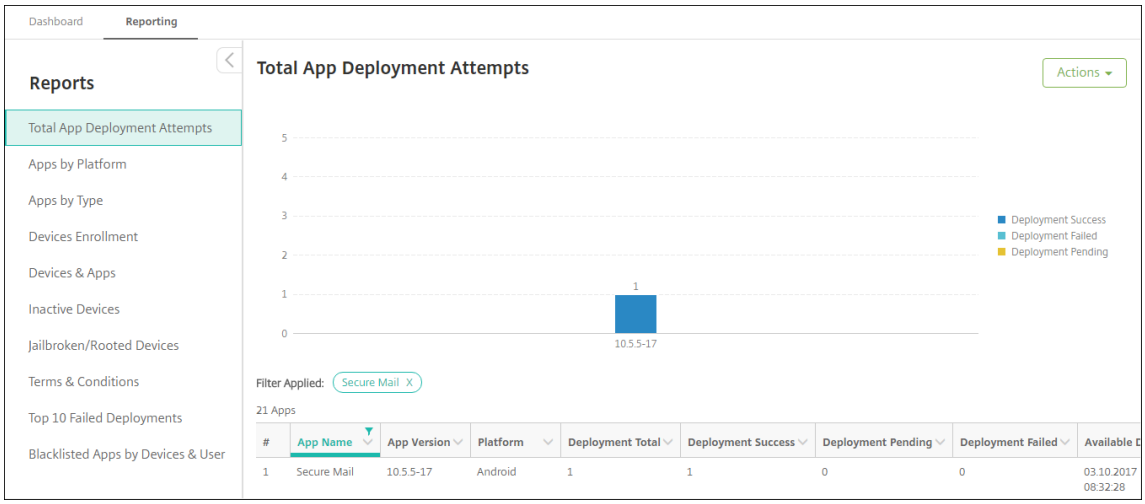
1. XenMobile 콘솔에서 분석 **>** 보고를클릭합니다. 보고페이지가나타납니다.

2. 생성할보고서를클릭합니다.

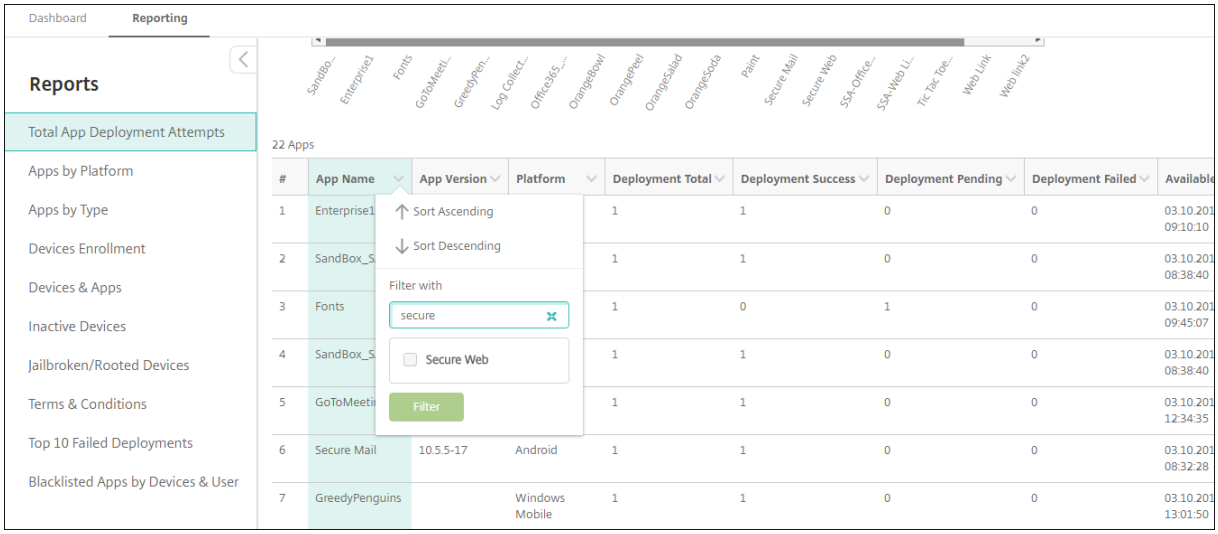


보고서의더상세한정보를보려면

1. 자세히볼차트부분을클릭하면상세정보가표시됩니다.

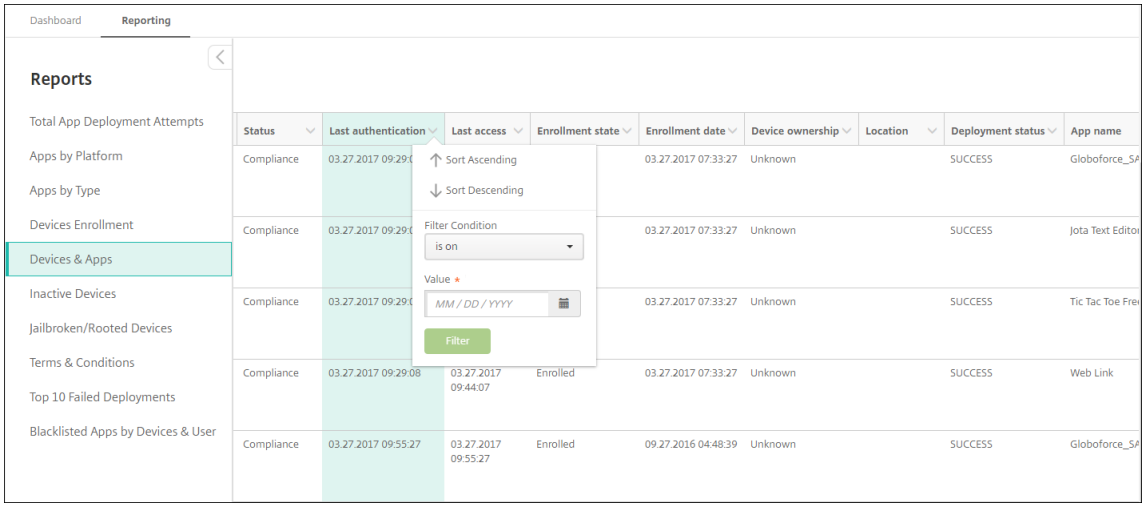


표열을정렬, 필터링또는검색하려면열머리글을클릭합니다

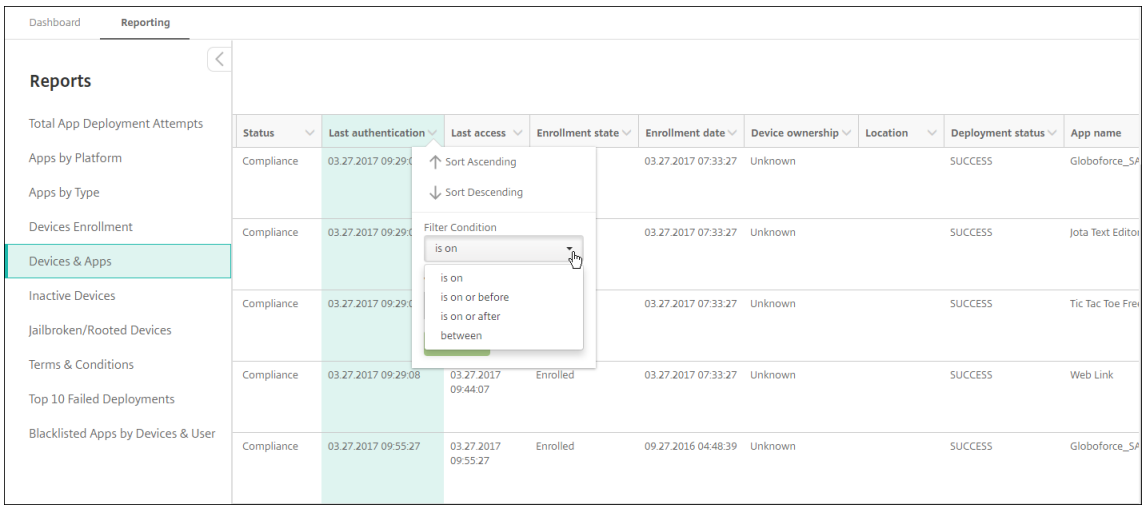


보고서를날짜로필터링하려면

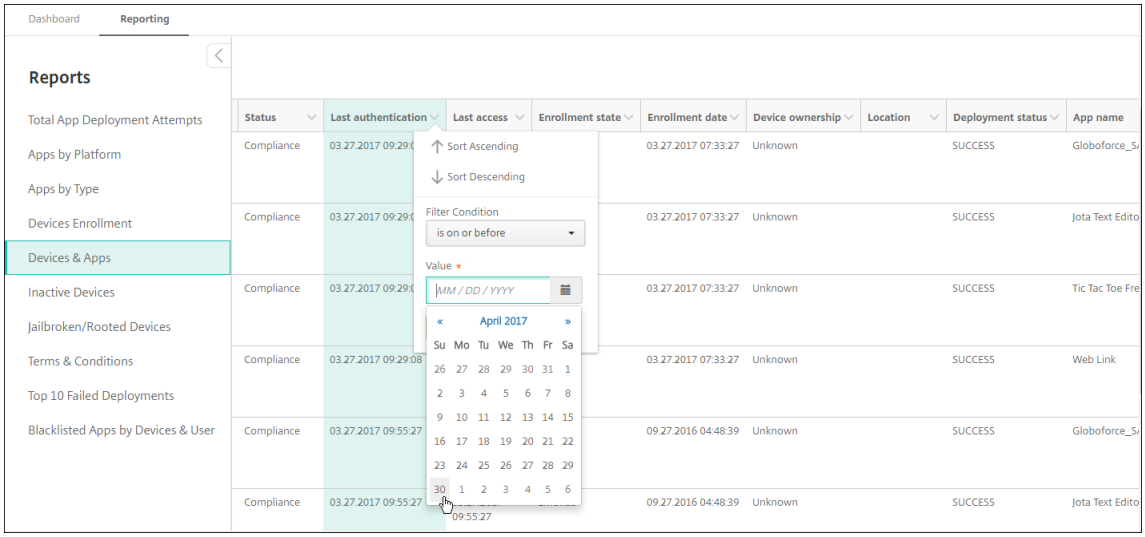
1. 열머리글을클릭하면필터설정이표시됩니다.



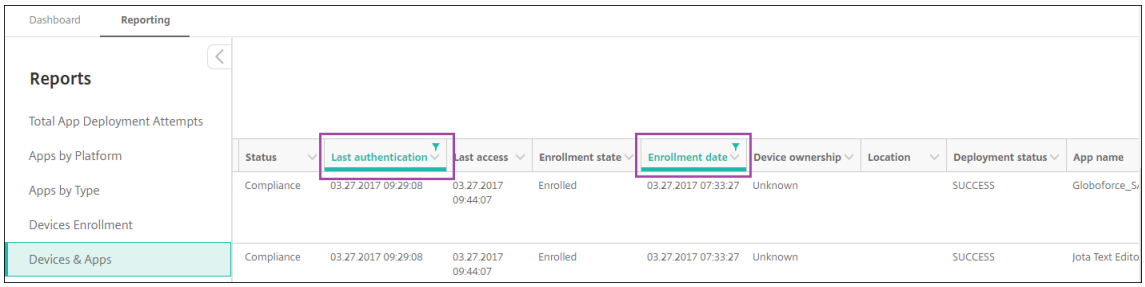
2. 필터조건에서보고되는날짜를제한할방법을선택합니다.



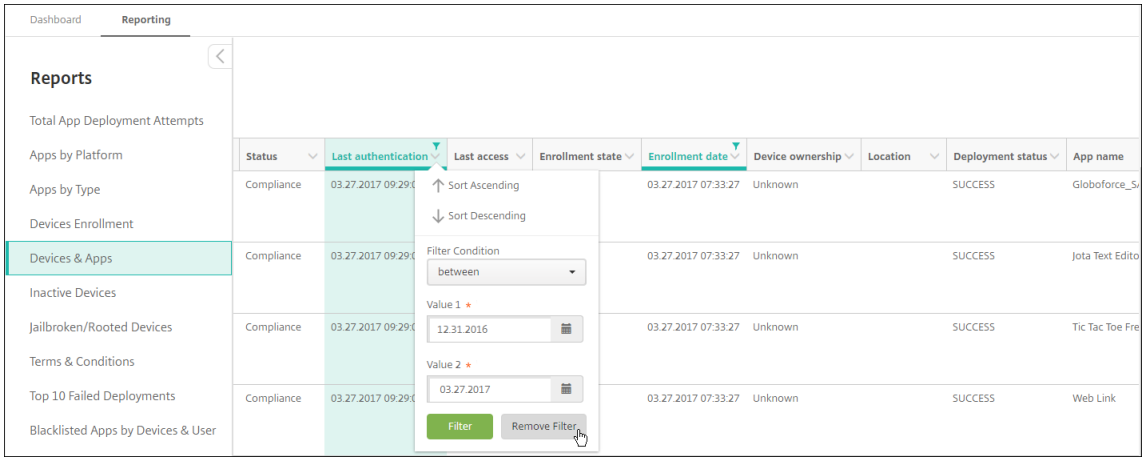
3. 날짜선택기를사용하여날짜를지정합니다.



4. 날짜필터가있는열이다음예제처럼표시됩니다.

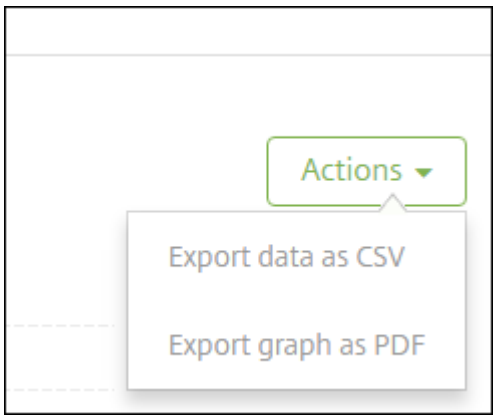


5. 필터를제거하려면열머리글을클릭한다음 필터제거를클릭합니다.



차트또는표를내보내려면

- 차트를 PDF 형식으로내보내려면 동작, **PDF** 로그래프내보내기를차례로클릭합니다.
- 표데이터를 CSV 형식으로내보내려면 동작, **CVS** 로데이터내보내기를차례로클릭합니다.



> 중요:
>
> SQL Server 를사용하여사용자지정보고서를만들수있지만이방법은권장하지않습니다. Citrix 는스키마를게시하지않으며알림없이스키마를변경할수있습니다. 이방법의보고를사용하기로결정한경우읽기전용계정을사용하여 SQL 쿼리를실행해야합니다. 여러조인이포함되어실행에시간이다소걸리는쿼리는그시간동안 XenMobile Server 성능에영향을미칠수있습니다.

SNMP 모니터링

August 12, 2022

XenMobile Server 에서 SNMP 모니터링을사용하도록설정하여모니터링시스템이 XenMobile 노드를쿼리하고노드의정보를가져오도록허용할수있습니다. 쿼리에는프로세서로드, 로드평균, 메모리사용현황및연결같은매개변수가사용됩니다. 인증및암호화사양을비롯하여 SNMP v3 에대한자세한내용은 RFC 3414에대한공식 SNMP 설명서를참조하십시오.

> 참고:
>
> SNMP v3 모니터링은 XenMobile Server 10.8 이상에서지원됩니다.

SCOM 과같은 SNMP 모니터링을지원하는다양한모니터링응용프로그램을사용할수있습니다. SCOM 구성에대한자세한내용은 이 Citrix Support Knowledge Center 문서를참조하십시오.

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 포트요구사항을참조하십시오.

SNMP 를포함하는온-프레미스 XenMobile 배포의아키텍처다이어그램은 온-프레미스배포용참조아키텍처를참조하십시오.

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 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. 연결에실패하면 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 라이센스서버연결

- 모니터링 **OID(**개체 **ID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- 설명**:** 사용자정의된모든간격마다 Citrix 라이센스서버와 XenMobile 노드사이의연결을모니터링합니다. 연결에실패하면 XenMobile 이 SNMP 트랩을생성합니다.

트랩이름**:** Citrix Gateway 연결

- 모니터링 **OID(**개체 **ID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- 설명**:** 사용자정의된모든간격마다 Citrix 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.

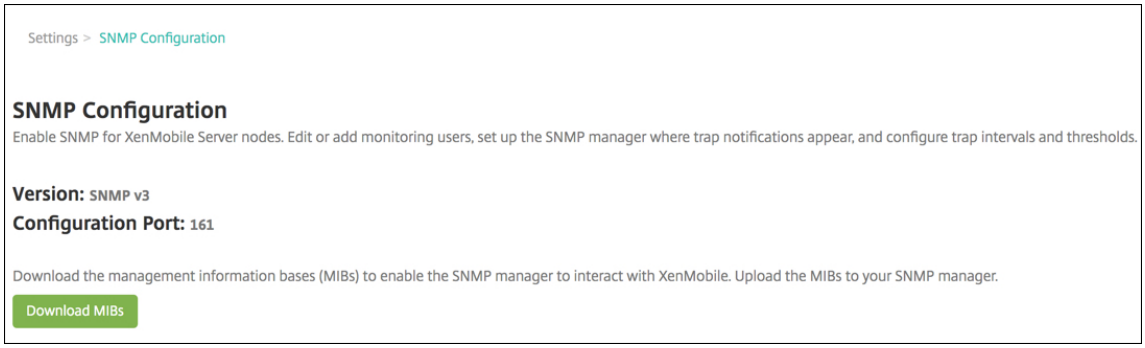
SNMP 임계값을구성할때최상의서버성능을유지하려면다음요인을고려하십시오.

- 호출빈도
- 수집할트랩데이터와임계값확인
- 노드간통신메커니즘
- 연결확인빈도
- 확인중실패에대한시간초과

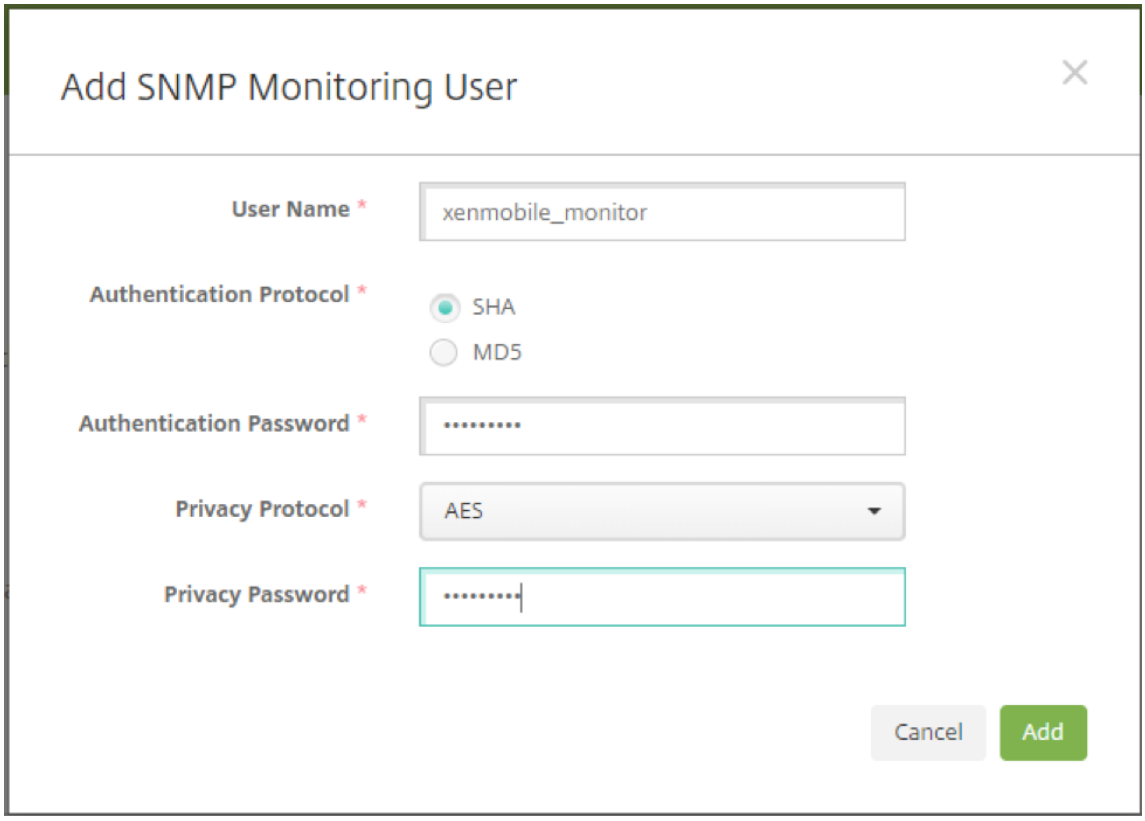
SNMP 사용자를추가하려면

SNMP 사용자는 SNMP 관리자와상호작용하고트랩을수신합니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. 모니터링에서 **SNMP** 구성을클릭합니다. **SNMP** 구성페이지가나타납니다.



3. **SNMP** 모니터링사용자에서 추가를클릭합니다.
4. **SNMP** 모니터링사용자추가대화상자에서다음설정을구성합니다.



사용자이름**:** SNMP 관리자에로그온할때사용되는사용자이름입니다. 영숫자, 밑줄및하이픈을사용할수있지만공백과다른특수문자는사용자이름에사용할수없습니다.

> 참고**:**
>
> “xmsmonitor” 는 XenMobile 의내부사용을위해예약된이름이므로사용자이름으로추가할수없습니다.

인증프로토콜**:**

- **SHA**(권장)
- **MD5**

인증암호**:** 8~18 자의암호를입력합니다. 영숫자와특수문자를포함할수있습니다.

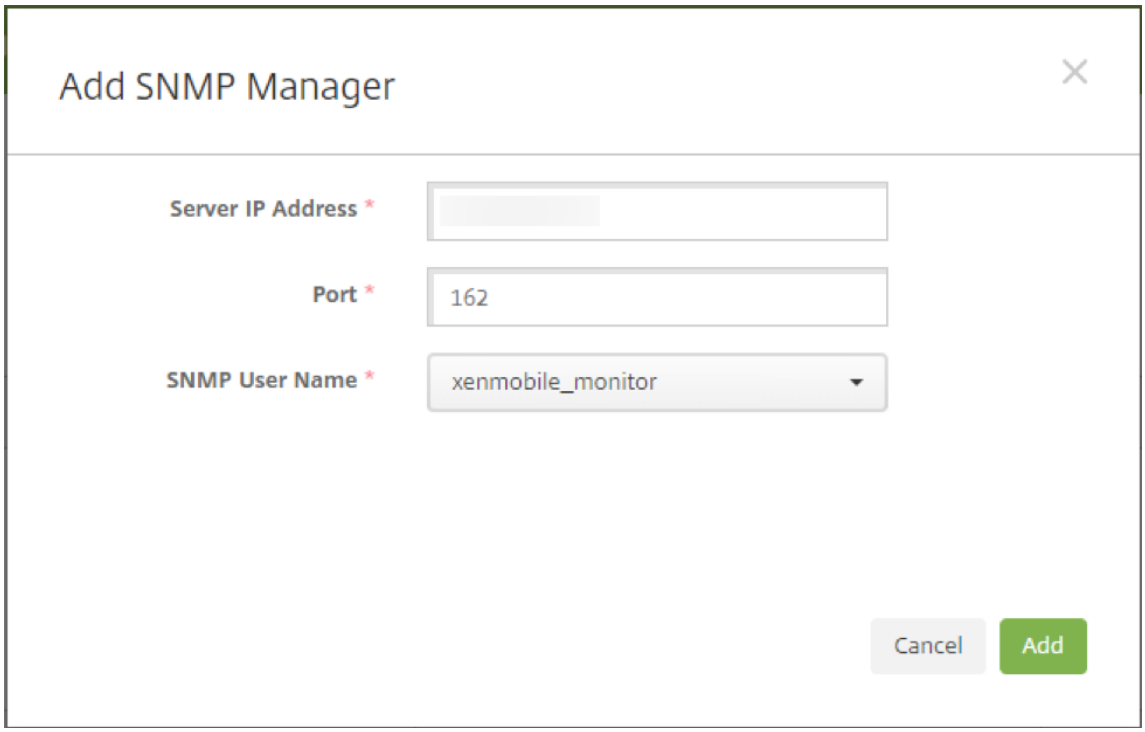
개인정보프로토콜**:**

- **DES**
- **AES 128**(권장)

개인정보암호**:** 8~18 자의암호를입력합니다. 영숫자와특수문자를포함할수있습니다.

SNMP 관리자를추가하려면

1. **SNMP** 관리자에서 추가를클릭합니다.
2. **SNMP** 관리자추가대화상자에서다음설정을구성합니다.



서버 **IP** 주소**:** SNMP 관리자의 IP 주소를입력합니다.

포트**:** 필요한경우포트번호를변경합니다. 기본값은 162 입니다.

SNMP 사용자이름**:** 관리자에액세스할수있는사용자이름을선택합니다.

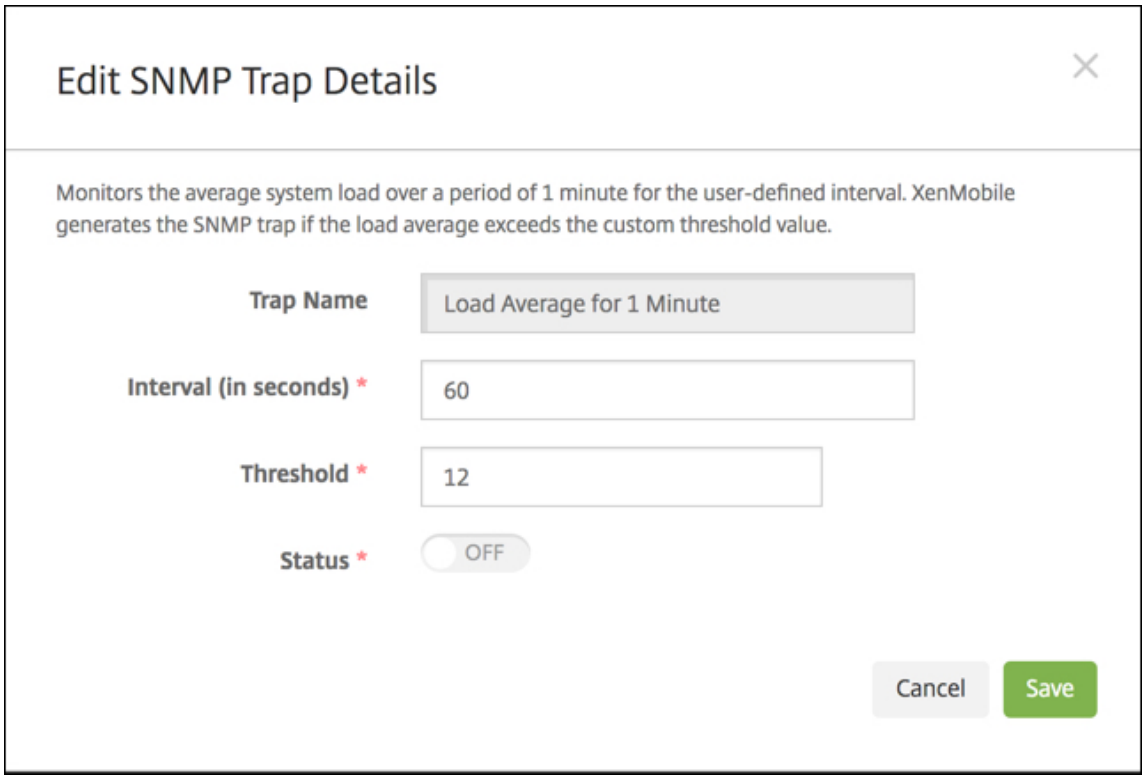
SNMP 트랩을사용하고구성하려면

환경에적합한트랩설정을확인하려면 확장성및성능을참조하십시오. 예를들어 1 분동안 XenMobile 로드평균을모니터링하려면 1 분동안의로드평균을사용하도록설정하고임계값을입력합니다. XenMobile Server 의 1 분동안의로드평균이지정된임계값을초과하면구성된 SNMP 관리자에서트랩을수신합니다.

1. 개별트랩을사용하려면다음중하나를수행합니다.
   - 매개변수옆의확인란을선택하고 사용을클릭합니다.

- 목록의모든트랩을사용하려면맨위의확인란을선택하고 사용을클릭합니다.

2. 트랩을편집하려면매개변수를선택하고 편집을클릭합니다.
3. **SNMP** 트랩세부정보편집대화상자에서개별트랩의임계값을편집할수있습니다.



트랩이름**:** 트랩의이름입니다. 이필드는편집할수없습니다.

간격 **(**초**):** 60~86400(24 시간) 범위의값을사용할수있습니다.

임계값**:** 다음트랩의임계값만변경할수있습니다.

- 프로세서로드
- 1 분동안의로드평균
- 5 분동안의로드평균
- 15 분동안의로드평균
- 사용가능한총메모리
- 사용된총디스크스토리지
- Java 힙메모리사용현황
- Java Metaspace 사용현황

상태**:** 트랩에 SNMP 모니터링을사용하려면 켜짐을선택합니다. 모니터링을사용하지않으려면 꺼짐을선택합니다.

SNMP 를사용한 XenMobile 모니터링에대한도움이되는정보를보려면이 블로그게시물을참조하십시오.

지원번들

January 5, 2022

Citrix 에문제를보고하거나문제를해결하려면지원번들을만듭니다. 그런다음지원번들을 CIS(Citrix Insight Services) 에업로드합니다.

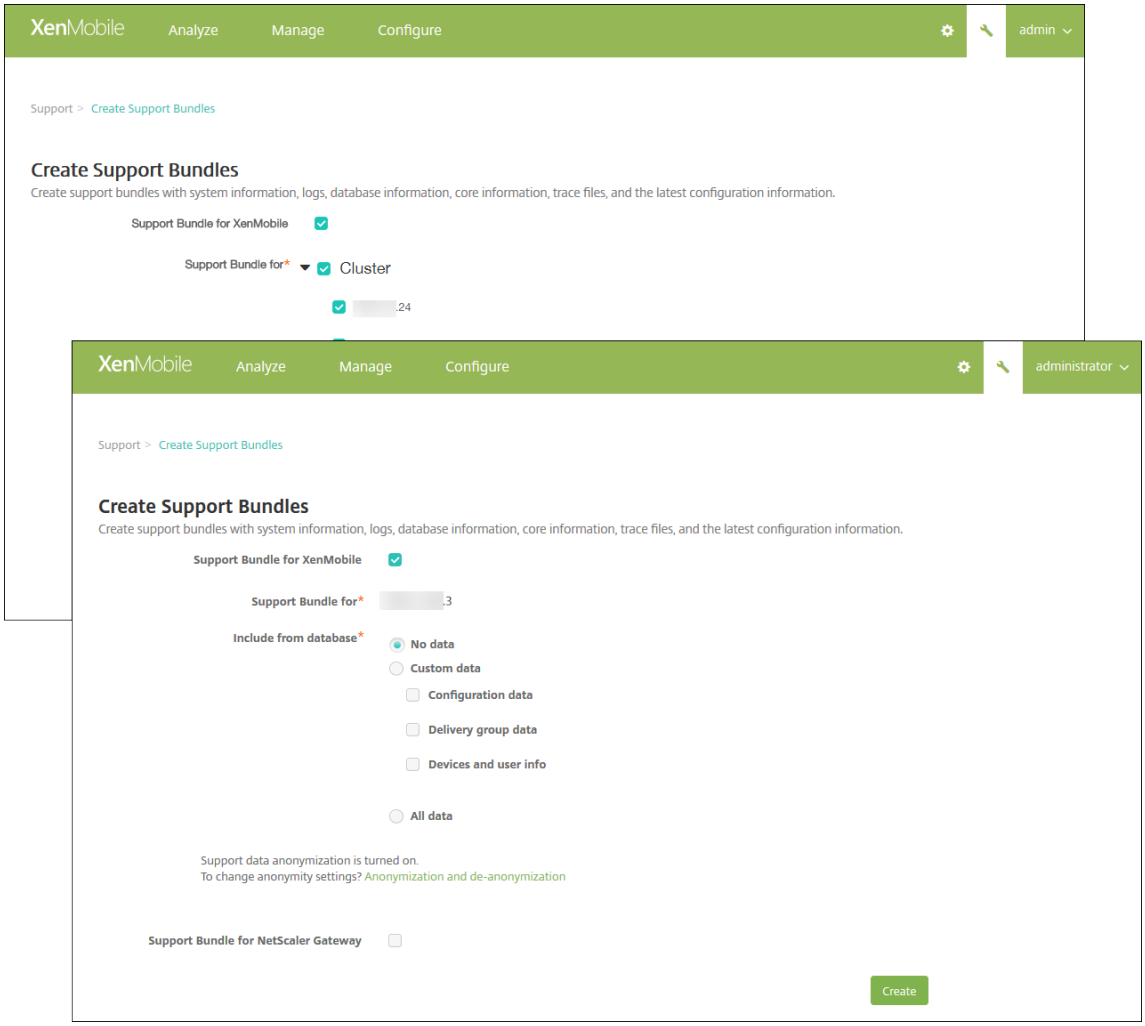
기본적으로지원번들에는다음파일에대한최대 100 개의백업아카이브가포함됩니다. 이러한파일의기본파일크기는 10MB 입니다.

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

지원번들에이러한각범주에대한 100 개의로그아카이브파일이포함되는경우로그파일이롤오버됩니다. 로그파일의최대수를이보다작게구성하면 XenMobile 이해당노드의추가로그파일을즉시삭제합니다. 로그파일수를구성하려면 문제해결및지원 **>** 로그설정으로이동합니다.

지원번들을만들려면:

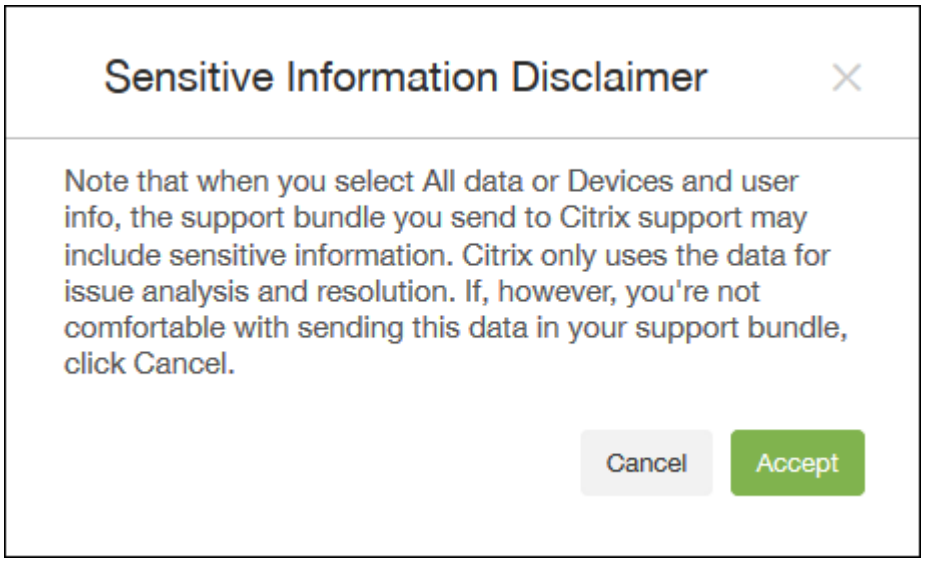
1. XenMobile 콘솔에서오른쪽맨위의렌치아이콘을클릭합니다. 지원페이지가나타납니다.
2. 지원페이지에서 지원번들만들기를클릭합니다. 지원번들만들기페이지가나타납니다. XenMobile 환경에클러스터된노드가포함되는경우모든노드가표시됩니다.



3. **XenMobile** 용지원번들확인란이선택되어있는지확인합니다.
4. XenMobile 환경에클러스터된노드가포함되는경우 다음을위한지원번들에서모든노드를선택하거나데이터를가져올노드 조합을선택할수있습니다.
5. 데이터베이스에서포함에서다음중하나를수행합니다.
   - 데이터없음을클릭합니다.
   - 사용자지정데이터를클릭합니다. 기본적으로이모든옵션이선택됩니다.
     - 구성데이터**:** 인증서구성및장치관리자정책이포함됩니다.
     - 배달그룹데이터**:** 앱유형및앱배달정책세부정보를포함한앱배달그룹정보가포함됩니다.
     - 장치및사용자정보**:** 장치정책, 앱, 동작및배달그룹이포함됩니다.
   - 모든데이터를클릭합니다.

> 참고**:**
>
> 장치및사용자정보또는 모든데이터를선택하고처음으로지원번들을만든경우 중요한정보에대한고지사항대화상자가 나타납니다. 고지사항을읽고 동의또는 취소를클릭합니다. 취소를클릭하면지원번들을 Citrix 에업로드할수없습니

> 다. 동의를클릭하면지원번들을 Citrix 에업로드할수있으며다음에장치또는사용자데이터가포함된지원번들을만들 때고지사항이표시되지않습니다.

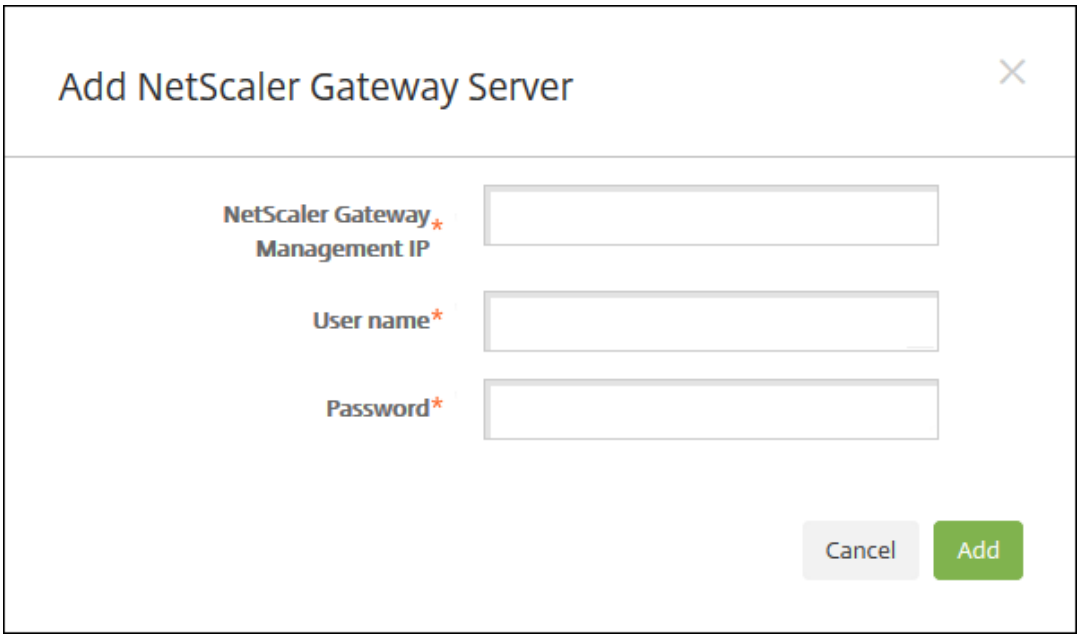


6. 지원데이터익명화가켜져있습니다옵션은기본설정이데이터를익명화하는것임을나타냅니다. 데이터익명화는중요한사용자, 서버및네트워크데이터가지원번들에서익명으로표시되는것을의미합니다.

   이설정을변경하려면 익명화및익명화취소를클릭합니다. 데이터익명화에대한자세한내용은 지원번들의데이터익명화를참조하십시오.

7. Citrix Gateway 의지원번들을포함하려면: **Citrix Gateway** 용지원번들확인란을선택하고다음을수행합니다.

   a) 추가를클릭합니다. **Citrix Gateway** 서버추가대화상자가나타납니다.



   b) **Citrix Gateway** 관리 **IP** 에지원번들데이터를가져올 Citrix Gateway 의 Citrix ADC 관리 IP 주소를입력합니다.

> 참고:
>
> 이미추가된 Citrix Gateway 서버에서번들을만드는경우 IP 주소가입력됩니다.

c) 사용자이름및 암호에 Citrix Gateway 실행서버에액세스하는데필요한사용자자격증명을입력합니다.

> 참고:
>
> 이미추가된 Citrix Gateway 서버에서번들을만드는경우사용자이름이입력됩니다.

8. 추가를클릭합니다. 새 Citrix Gateway 지원번들이테이블에추가됩니다.
9. Citrix Gateway 지원번들을추가하려면 7 단계를반복합니다.
10. **Create(**만들기**)** 를클릭합니다. 지원번들이만들어지고두개의새단추인 **CIS** 에업로드및 클라이언트에다운로드가나타납니다.

Citrix Insight Services 에지원번들업로드

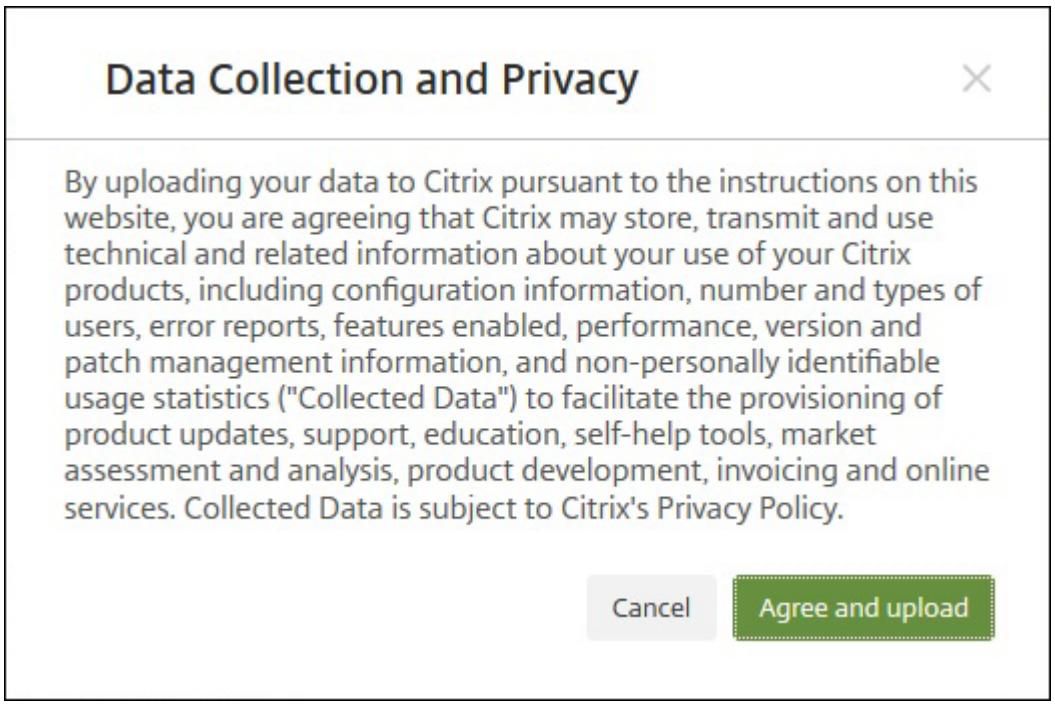
지원번들을만든후번들을 CIS(Citrix Insight Services) 에업로드하거나컴퓨터에다운로드할수있습니다.

XenMobile 에서 CIS 로의업로드에는 SSL 아웃바운드연결이사용됩니다. CIS 서버 IP 주소 (52.88.24.76, 52.88.118.220, 52.11.72.119) 에대해포트 443 을엽니다. 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. 계약을읽고 동의및업로드를클릭합니다. 지원번들이업로드됩니다.

컴퓨터에지원번들다운로드

지원번들을만든후번들을 CIS 에업로드하거나컴퓨터에다운로드할수있습니다. 직접문제를해결하려는경우지원번들을컴퓨터에다운로드합니다.

지원번들만들기페이지에서클라이언트에다운로드를클릭합니다. 번들이컴퓨터에다운로드됩니다.

지원번들에는다양한분석값의파일이포함되어있습니다. 파일목록및분석값은다음표를참고하십시오.

파일이름	유형	설명	값
DbDump.json	JSON 데이터베이스덤프	사용자/장치/애플리케이션 정보	높음
Garbage.html	HTML 파일	Java 가비지수집기	Low(낮음)
MemoryInfo.html	HTML 파일	메모리사용현황 - Java 관련메모리사용현황	높음
MultiNodeClusterInfo.html	HTML 파일	클러스터구성	높음
Patches.html	HTML 파일	패치정보. xmspatches.txt 보다개선됨	높음
pg_dump0.sql	PG 덤프	기본포스트그레스인스턴스덤프	중간

파일이름	유형	설명	값
rt_db/*	DB 복사본 (중복, pg_dump0.sql 의이진 표현임)		해당없음
sas_config/c3p0.properties	속성파일	C3P0 DB 구성속성	중간
sas_config/catalina.pol	정책파일	웹서버 Catalina 정책 - 파일이변경되지않음	Low(낮음)
sas_config/catalina.properties	속성파일	웹서버 Catalina 속성 - 파일이변경되지않음	Low(낮음)
sas_config/ew-config.properties	속성파일	XM 서버구성에대한정보	높음
sas_config/ew-config-reloadable.properties	속성파일	보안모델정보	높음
sas_config/hazelcast.xr	XML 파일	Hazelcast 로그 - 별로도움이되지않을수있음	Low(낮음)
sas_config/pki.xml	XML 파일	타사 PKI 서버를사용중인지확인하는데사용할수있음	높음
sas_config/push_servic	XML 파일	푸시서비스 - 파일이변경되지않음	Low(낮음)
sas_config/server.xml	XML 파일	여기에암호정보 - 보안관련	높음
sas_config/sftu_config/	속성파일	AppC 속성 - 파일이변경되지않음	Low(낮음)
sas_config/sftu_config/catalina.policy	정책파일	Catalina 정책 - 파일이변경되지않음	Low(낮음)
sas_config/sftu_config/	속성파일	Catalina 속성 - 파일이변경되지않음	Low(낮음)
sas_config/sftu_config/logging.properties	속성파일	로깅속성 - 파일이변경되지않음	Low(낮음)
sas_config/sftu_config/	XML 파일	여기에암호정보 - 보안관련	높음
sas_config/sftu_config/schema_migration.xml	XML 파일	마이그레이션정보	높음
sas_config/sftu_config/	XML 파일	최초사용자설정	높음
sas_config/sftu_config/tomcat-users.xml	XML 파일	TomCat 사용자 - 파일이변경되지않음	Low(낮음)
sas_config/sftu_config/	XML 파일	웹 - 파일이변경되지않음	Low(낮음)

파일이름	유형	설명	값
sas_config/sftu.properties	속성파일	SFTU 구성속성	높음
sas_config/variables.xm	XML 파일	변수 - 파일이변경되지않음	Low(낮음)
sas_config/web.xml	XML 파일	웹서버관련정보	중간
sas_log/AdminAuditLog	Linux 로그파일	모든구성변경사항	높음
sas_log/create_sb_output.sh	Linux 로그파일	지원생성명령출력	Low(낮음)
sas_log/DebugLogFile.l	Linux 로그파일	모든기능로그	높음
sas_log/HibernateStats.log	Linux 로그파일	최대절전모드기록	Low(낮음)
sas_log/kafka-consumer.log	Linux 로그파일	Kafka 로그	Low(낮음)
sas_log/kafka-server.log	Linux 로그파일	Kafka 로그	Low(낮음)
sas_log/kafka-topics.log	Linux 로그파일	Kafka 로그	Low(낮음)
sas_log/LPE.log	Linux 로그파일	LPE 로그	Low(낮음)
sas_log/migration.log	Linux 로그파일	마이그레이션프로세스출력	중간
sas_log/PlatformAuditLogFile.log	Linux 로그파일	백엔드감사수준정보	높음
sas_log/PlatformDebug	텍스트파일	백엔드서버관련로그	높음
sas_log/postgres.log	Linux 로그파일	PostGres 로그	중간
sas_log/SFTU.log	Linux 로그파일	SFTU 로그	중간
sas_log/tc1/catalina.log	Linux 로그파일	Catalina 로그	Low(낮음)
sas_log/tc1/console	Linux 로그파일	콘솔	Low(낮음)
sas_log/tc1/host-manager.log	Linux 로그파일	호스트관리자	Low(낮음)
sas_log/tc1/localhost.lo	Linux 로그파일	LocalHost	Low(낮음)
sas_log/updates.log	Linux 로그파일	패치프로세스출력	중간
sas_log/UserAuditLogF	Linux 로그파일	사용자작업	높음
sas_log/zookeeper.txt	텍스트파일	Zookeeper 로그	Low(낮음)
snmp/snmpd_etc_nets	속성파일	SNMP 구성속성	Low(낮음)
snmp/snmpd_privileges.conf	속성파일	SNMP 구성속성	Low(낮음)
sys_info/arp_entries.txt	텍스트파일	XMS 서버의 ARP 항목	중간

파일이름	유형	설명	값
sys_info/chrony.txt	텍스트파일	Chrony 로그	Low(낮음)
sys_info/diskspace_usa	텍스트파일	디스크공간사용현황	높음
sys_info/firewall_rules.txt	텍스트파일	XMS 에정의된방화벽규칙	중간
sys_info/interface_conf	텍스트파일	시스템명령출력	중간
sys_info/net_connections.txt	텍스트파일	시스템명령출력	중간
sys_info/root_account_	텍스트파일	시스템명령출력	중간
sys_info/routing_table.txt	텍스트파일	높은값	높음
sys_info/running_proce	텍스트파일	높은값	높음
sys_info/top.txt	텍스트파일	시스템명령출력	중간
ThreadDump.html	HTML 파일	더이상사용되지않음	Low(낮음)
ThreadDumpV2.html	HTML 파일	스레드스택추적등	중간
var_log/auth.log	Linux 로그파일	OS 수준로그	중간
var_log/boot.log	Linux 로그파일	OS 수준로그	중간
var_log/btmp	Linux 로그파일	OS 수준로그	중간
var_log/daemon.log	Linux 로그파일	OS 수준로그	중간
var_log/kern.log	Linux 로그파일	OS 수준로그	중간
var_log/lastlog	Linux 로그파일	OS 수준로그	중간
var_log/mail.log	Linux 로그파일	OS 수준로그	중간
var_log/sys.log	Linux 로그파일	OS 수준로그	중간
var_log/user.log	Linux 로그파일	OS 수준로그	중간
var_log/wtmp	Linux 로그파일	OS 수준로그	중간
version.txt	텍스트파일	XM 서버버전	중간
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	XML 파일	XMS 서버의연결확인결과	중간
xmspatches.txt	텍스트파일	패치정보.	높음

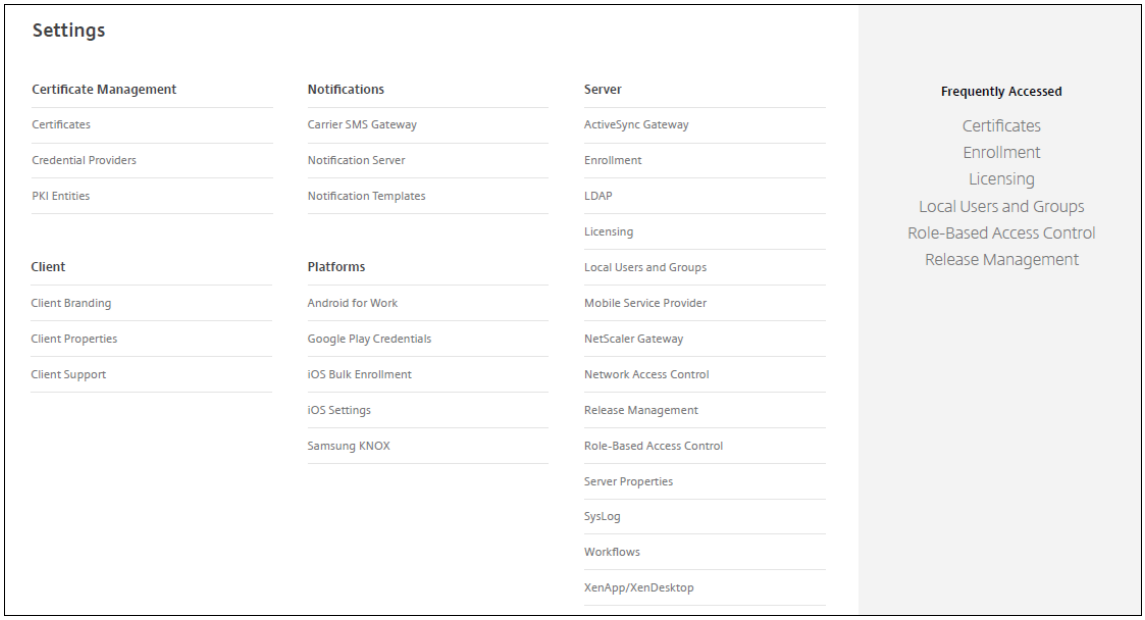
지원옵션및원격지원

August 12, 2022

사용자가지원담당자에게연락할수있도록전자메일주소를제공할수있습니다. 사용자가장치에서지원을요청하면전자메일주소가표시됩니다.

또한사용자가장치에서지원센터로로그를보내는방법도구성할수있습니다. 직접또는전자메일을사용하여로그를보내도록구성할수있습니다.

1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.



2. 클라이언트에서 클라이언트지원을클릭합니다. 클라이언트지원페이지가나타납니다.
3. 다음설정을구성합니다.
   - 지원전자메일 **(IT** 지원센터**):** IT 지원센터연락처의전자메일주소를입력합니다.
   - 장치로그를 **IT** 지원센터에보내기**:** 장치로그를 직접보낼지아니면 전자메일로보낼지를선택합니다. 기본값은 전자메일로입니다.
     - 직접을사용하면 ShareFile(현재의 Citrix Content Collaboration) 에로그저장에대한설정이나타납니다. Store logs on Citrix Content Collaboration(Citrix Content Collaboration 에로그저장)을사용하도록설정하면로그가 Citrix Files 로직접전송됩니다. 그렇지않은경우 XenMobile 로전송된다음전자메일을통해지원센터로전송됩니다. 또한기본적으로사용하도록설정되는 직접보내기가실패하면전자메일사용옵션이나타납니다. 클라이언트전자메일을사용하여서버문제에대한로그를전송하지않으려면이옵션을사용하지않을수있습니다. 그러나이옵션을사용하지않고서버문제가발생하면로그가전송되지않습니다.
     - 전자메일로를사용하면로그를전송할때클라이언트전자메일이항상사용됩니다.
4. 저장을클릭합니다.

원격지원

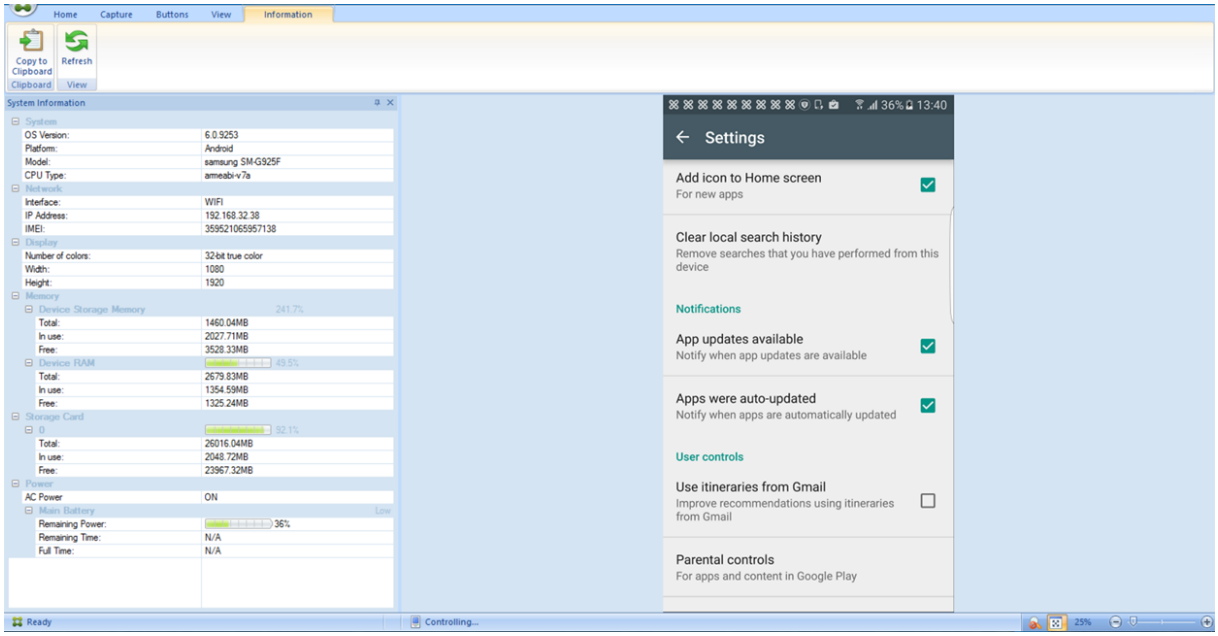
> 참고:
>
> 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.

온-프레미스 XenMobile Server 배포의경우: 원격지원을사용하면지원센터담당자가관리되는 Android 모바일장치를원격으로제어할수있습니다. 스크린캐스트는 Samsung Knox 장치에서만지원됩니다.

원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다.

원격제어세션중에:

- 사용자의모바일장치에원격제어세션이활성상태임을나타내는아이콘이표시됩니다.
- 원격지원사용자는원격지원응용프로그램창과원격제어창에서제어되는장치의렌더링을볼수있습니다.



원격지원을사용하여다음을수행할수있습니다.

- 사용자장치에원격으로로그온하고화면을제어합니다. 사용자는원격지원담당자가화면을탐색하는것을지켜볼수있으며이는교육용으로도유용합니다.
- 원격장치를실시간으로탐색하고복구합니다. 구성을변경하고, 운영체제문제를해결하고, 문제가되는앱또는프로세스를사용하지않도록설정하거나중지할수있습니다.
- 네트워크액세스를원격으로사용하지않도록설정하고, 불법프로세스를중지하고, 앱또는맬웨어를제거하여위협이다른모바일장치로확산되기전에격리하고억제합니다.
- 장치벨소리를원격으로사용하도록설정하고전화를걸어사용자가장치를찾을수있도록합니다. 사용자가장치를찾을수없는경우장치를초기화하여중요한데이터가손상되지않도록합니다.

또한지원담당자는원격지원을사용하여다음을수행할수있습니다.

- 하나이상의 XenMobile 인스턴스내에서연결된모든장치목록을표시합니다.

- 장치모델, 운영체제수준, IMEI(International Mobile Station Equipment Identity), 일련번호, 메모리및배터리상태, 연결등을비롯한시스템정보를표시합니다.
- XenMobile 의사용자및그룹을표시합니다.
- 활성프로세스를표시및종료하고모바일장치를다시시작할수있는장치작업관리자를실행합니다.
- 모바일장치와중앙파일서버간의양방향파일전송을포함하는원격파일전송을실행합니다.
- 소프트웨어프로그램을일괄처리로하나이상의모바일장치에다운로드하고설치합니다.
- 장치에서원격레지스트리키설정을구성합니다.
- 실시간장치화면원격제어를사용하여저대역폭셀룰러네트워크에서응답시간을최적화합니다.
- 대부분의모바일장치브랜드및모델에대한장치스킨을표시합니다. 스킨편집기를표시하여새장치모델을추가하고물리적키를매핑합니다.
- 비디오 AVI 파일을만드는장치에서일련의상호작용을캡처하는기능을통해장치화면캡처, 녹화및재생을사용하도록설정합니다.
- 모바일사용자와지원직원간에공유화이트보드, VoIP 기반음성통신및채팅을사용하여라이브모임을수행합니다.

원격지원시스템요구사항

원격지원소프트웨어는다음요구사항을충족하는 Windows 기반컴퓨터에설치됩니다. 포트요구사항은 포트요구사항을참조하십시오.

지원되는플랫폼:

- Intel Xeon/Pentium 4 -1GHz 워크스테이션급이상
- 512MB RAM 이상
- 최소 100MB 디스크여유공간

지원되는운영체제:

- Microsoft Windows 2003 Server Standard Edition 또는 Enterprise Edition SP1 이상
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 이상
- Microsoft Windows Vista SP1 이상
- Microsoft Windows 10 또는 Windows 11
- Microsoft Windows 8
- Microsoft Windows 7

명령줄에서원격지원을설치하려면

다음명령을실행합니다.

```
1 \*RemoteSupport\*.exe /S
```

RemoteSupport 는설치프로그램의이름입니다. 예:


```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

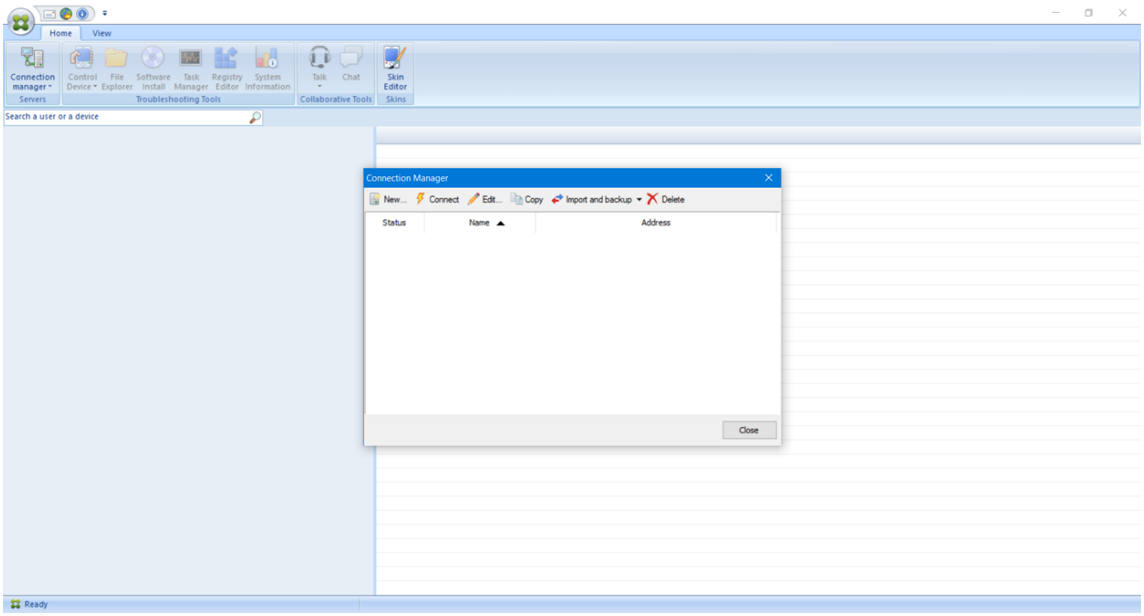
원격지원소프트웨어를설치할때다음변수를사용할수있습니다.

- /S: 기본매개변수를사용하여자동으로원격지원소프트웨어를설치합니다.
- /D=dir: 사용자지정설치디렉터리를지정합니다.

원격지원을 **XenMobile** 에연결하려면

관리되는장치에대한원격지원연결을설정하려면장치를관리하는하나이상의 XenMobile Server 에원격지원의연결을추가해야합니다. 이러한연결은 Android 장치에대한장치정책인터널 MDM 정책에서정의한앱터널을통해실행됩니다. 원격지원을 XenMobile 에연결하려면먼저앱터널을정의해야합니다. 자세한내용은 앱터널링장치정책을참조하십시오.

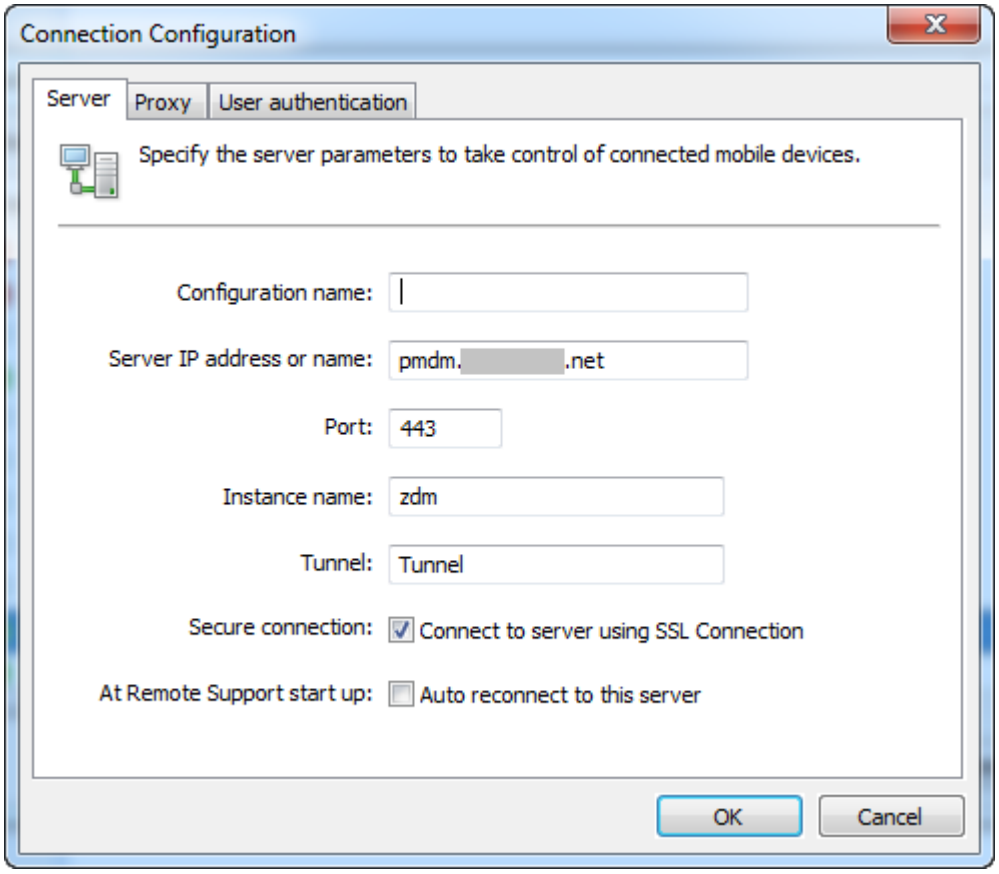
1. 원격지원소프트웨어를시작하고 XenMobile 자격증명을사용하여로그온합니다.
2. **Connection Manager(**연결관리자**)** 에서 **New(**새로만들기**)** 를클릭합니다.



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) 원격지원응용프로그램을시작할때마다구성된 XenMobile Server 에연결하려면 **Auto reconnect to this server(**이서버에자동으로다시연결**)** 확인란을선택합니다.



4. **Proxy(**프록시**)** 탭에서 **Use an http proxy server(http** 프록시서버사용**)** 를선택하고다음정보를입력합니다.

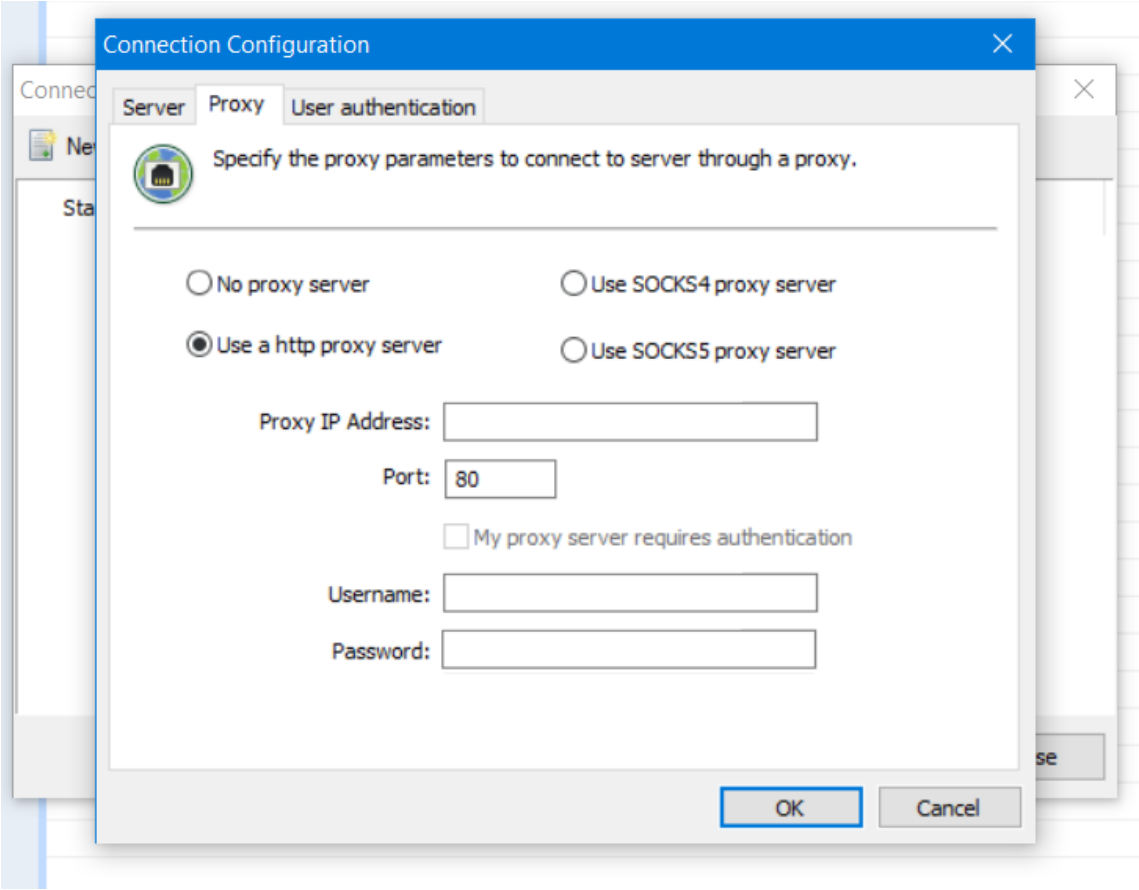
a) **Proxy IP Address(**프록시 **IP** 주소**)** 에프록시서버의 IP 주소를입력합니다.

b) **Port(**포트**)** 에프록시에서사용하는 TCP 포트번호를입력합니다.

c) 프록시서버에트래픽허용을위한인증이필요한경우 **My proxy server requires authentication(**내프록시서버에인증필요**)** 확인란을선택합니다.

d) **Username(**사용자이름**)** 에프록시서버에서인증할사용자이름을입력합니다.

e) **Password(**암호**)** 에프록시서버에서인증할암호를입력합니다.



5. **User Authentication(**사용자인증**)** 탭에서 **Remember my login and password(**로그인및암호저장**)** 확인란을선택하고자격증명을입력합니다.
6. 확인을클릭합니다.

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 라이센스키장치정책을구성해야합니다. 이정책을구성하는경우 **Samsung KNOX** 플랫폼만선택합니다. SAFE 플랫폼의경우 Samsung 장치가 XenMobile 에등록될때 ELM 키가자동으로배포됩니다. 따라서이정책에는 Samsung SAFE 플랫폼을선택하지마십시오. 자세한내용은 Samsung MDM 라이센스키를참조하십시오.

원격지원정책구성에대한자세한내용은 원격지원장치정책을참조하십시오.

원격지원세션을사용하려면

원격지원을시작하면원격지원응용프로그램창의왼쪽에 XenMobile 콘솔에서정의한 XenMobile 사용자그룹이표시됩니다. 기본적으로현재연결된사용자를포함하는그룹만표시됩니다. 사용자항목옆에서각사용자의장치를볼수있습니다.

1. 모든사용자를보려면왼쪽열에서각그룹을확장합니다.
   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.
- 장치작업관리자에액세스하여메모리사용량, CPU 사용량및실행중인앱과같은항목을관리합니다.
- 모바일장치의로컬디렉터리를탐색합니다. 파일을전송합니다.
- 장치시스템정보및설치된모든소프트웨어를표시합니다.
- 모바일장치와 XenMobile Server 의연결상태를업데이트합니다.

SysLog

December 1, 2020

시스템로그 (syslog) 서버에로그파일을보내도록 XenMobile Server(온-프레미스) 를구성할수있습니다. 서버호스트이름또는 IP 주소가필요합니다.

Syslog 는장비에서실행되는감사모듈과원격시스템에서실행될수있는서버라는두가지구성요소가있는표준로깅프로토콜입니다. Syslog 프로토콜에서는데이터전송에 UDP(User Datagram Protocol) 를사용합니다. 관리자이벤트및사용자이벤트가기록됩니다.

다음과같은유형의정보를수집하도록서버를구성할수있습니다.

- XenMobile 에서수행한동작의레코드가포함된시스템로그
- XenMobile 의시스템작업을시간순으로기록한감사로그

syslog 서버가장비에서수집하는로그정보는메시지형태로로그파일에저장됩니다. 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 메시지데이터는특정형식이없는일반텍스트입니다.

이정보를사용하여경고출처를분석하고필요한경우교정조치를취할수있습니다.

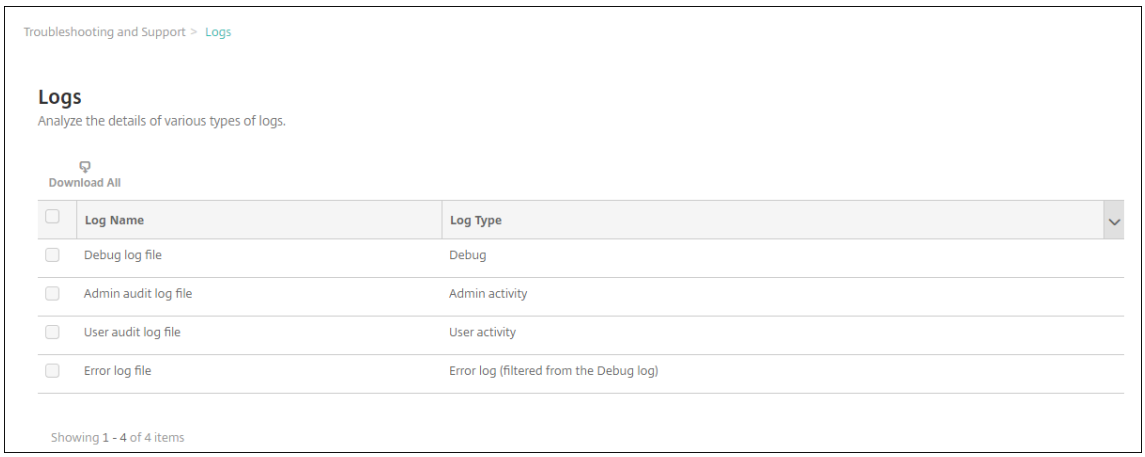
1. XenMobile 콘솔에서오른쪽맨위의기어아이콘을클릭합니다. 설정페이지가나타납니다.
2. **Syslog** 를클릭합니다. **Syslog** 페이지가나타납니다.
3. 다음설정을구성합니다.
   - 서버**:** syslog 서버의 IP 주소또는 FQDN(정규화된도메인이름) 을입력합니다.
   - 포트**:** 포트번호를입력합니다. 기본적으로포트는 514 로설정됩니다.
   - 로깅할정보**:** 시스템로그및 감사를선택하거나선택취소합니다.
     - 시스템로그는 XenMobile 에서수행한동작을포함합니다.
     - 감사로그는 XenMobile 의시스템작업을시간순으로기록한레코드를포함합니다.
     - XenMobile 의디버그로그
4. 저장을클릭합니다.

XenMobile 에서로그파일보기

September 29, 2021

XenMobile 을사용한관리에도움이되는로그를보고조작하고다운로드할수있습니다.

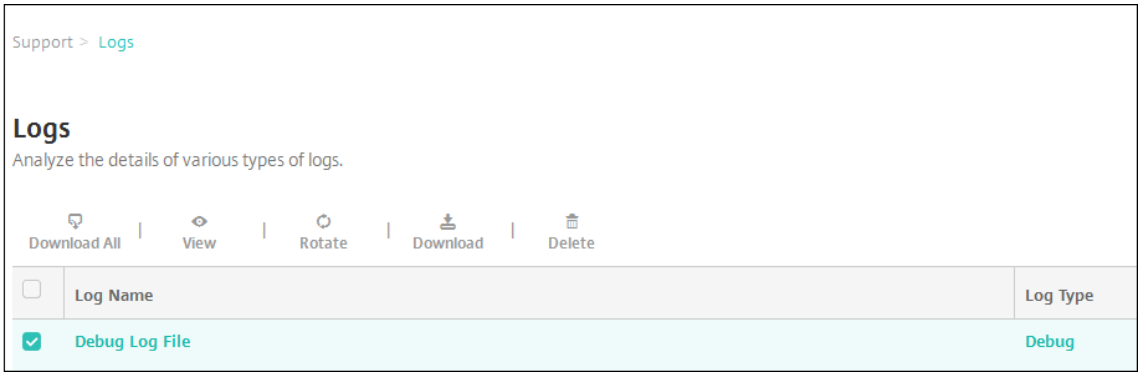
1. XenMobile 콘솔에서오른쪽위모서리의렌치아이콘을클릭합니다. 지원페이지가열립니다.
2. 로그작업아래에서 로그를클릭합니다. 로그페이지가나타납니다. 개별로그가테이블에표시됩니다.



3. 보려는로그를선택합니다.

   - 디버그로그파일에는오류메시지, 서버관련동작등 Citrix 지원에대한유용한정보가들어있습니다.
   - 관리자감사로그파일에는 XenMobile 콘솔작업에대한감사정보가포함되어있습니다.
   - 사용자감사로그파일에는구성된사용자와관련된정보가포함되어있습니다.
   - 오류로그파일에는디버그로그에서필터링된오류메시지만포함되어있습니다.

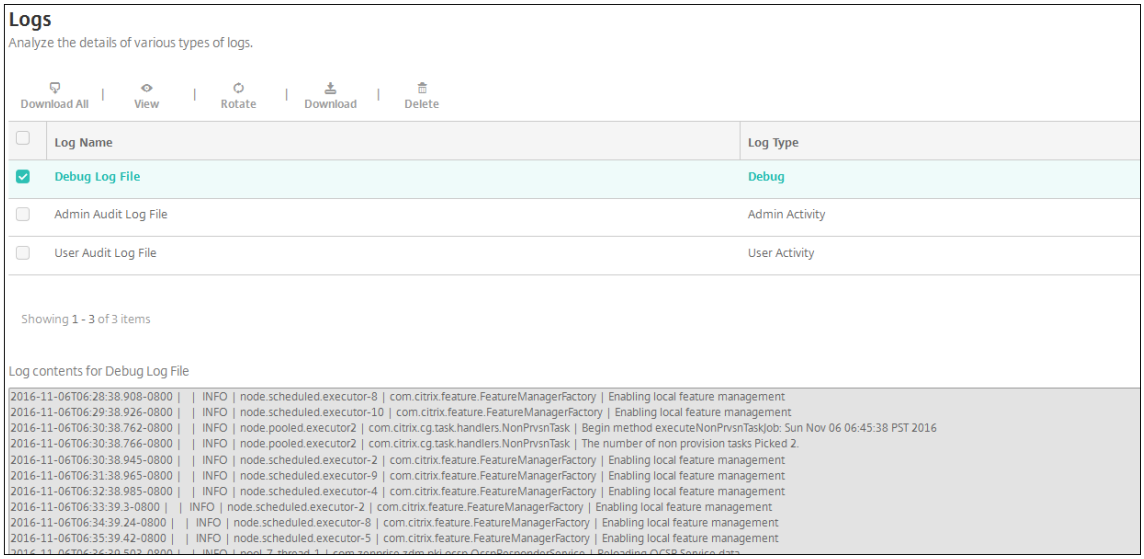
4. 테이블상단에있는모두다운로드, 보기, 순환, 단일로그다운로드또는선택한로그삭제동작을수행합니다.



> 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.



XenMobile Analyzer 도구

May 11, 2022

XenMobile Analyzer 는 XenMobile 의구성및기타기능관련문제를진단하고해결하는데사용할수있는클라우드기반도구입니다. 이도구는 XenMobile 환경내의장치또는사용자등록및인증문제를검사합니다.

XenMobile Server 를가리키도록도구를구성하고서버배포유형, 모바일플랫폼, 인증유형및사용자자격증명과같은정보를제공해야합니다. 그러면도구가서버에연결하고환경을검사하여구성문제를확인합니다. XenMobile Analyzer 에의해문제가검색되면문제해결을위한권장사항이제공됩니다.

주요기능

- 모든 XenMobile 관련문제를해결하는안전한클라우드기반의마이크로서비스입니다.
- XenMobile 구성문제를해결하는정확한권장사항입니다.
- 지원요청을줄이고 XenMobile 환경의문제해결을가속화합니다.
- XenMobile Server 릴리스에대한즉각적인지원입니다.
- 일별또는주별로상태확인을예약합니다.
- Citrix ADC 구성확인.
- Secure Web 테스트를통해인트라넷사이트연결가능성을확인합니다.
- Secure Mail 자동검색서비스를확인합니다.
- Citrix Files SSO(Single Sign-On) 를확인합니다.

새로운항목

- Citrix ADC 구성보고서에권장사항의수를나타내는배지알림이표시됩니다. 권장사항은특정 Citrix Gateway 에대한 Essential Configuration 확인을기반으로합니다.
- 테스트환경목록페이지의글로벌탐색모음내에있는아이콘이더나은사용자환경을위해재정렬되었습니다.

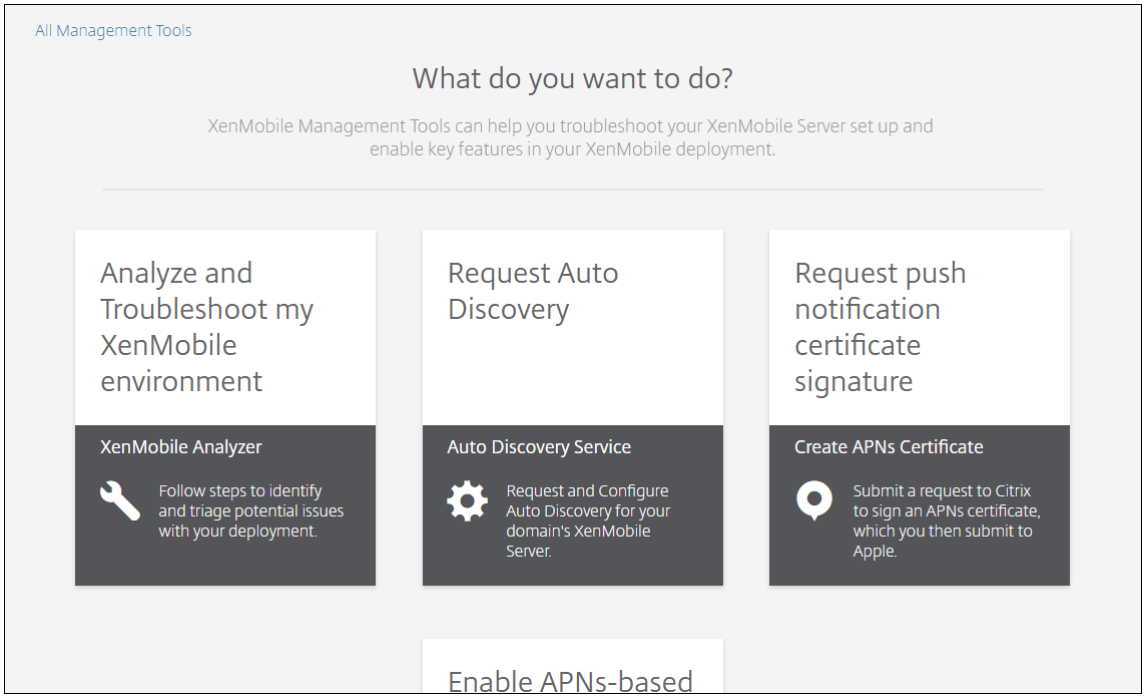
XenMobile Analyzer 액세스및시작

사전요구사항

제품	지원되는버전
XenMobile Server	10.1.0 이상
Citrix Gateway	10.5 이상
Client Enrollment Simulation	iOS 및 Android

다음방법중하나를사용하여 XenMobile Analyzer 에액세스합니다.

- XenMobile 콘솔에서오른쪽맨위의렌치아이콘을클릭하여 문제해결및지원페이지를엽니다.
- https://cemtoolsui.xm.cloud.com/에서 My Citrix 자격증명을사용하여도구에액세스합니다. XenMobile Management Tools 페이지에서 XenMobile Analyzer 를시작하려면 **Analyze and Troubleshoot my XenMobile Environment(**내 **XenMobile** 환경분석및문제해결**)** 를클릭합니다.



XenMobile Analyzer 에는분류프로세스를통해지원티켓의수를줄이도록설계된 5 개옵션이포함되어있습니다. 이옵션을사용

하면모든사용자의비용을낮출수있습니다.

옵션은다음과같습니다.

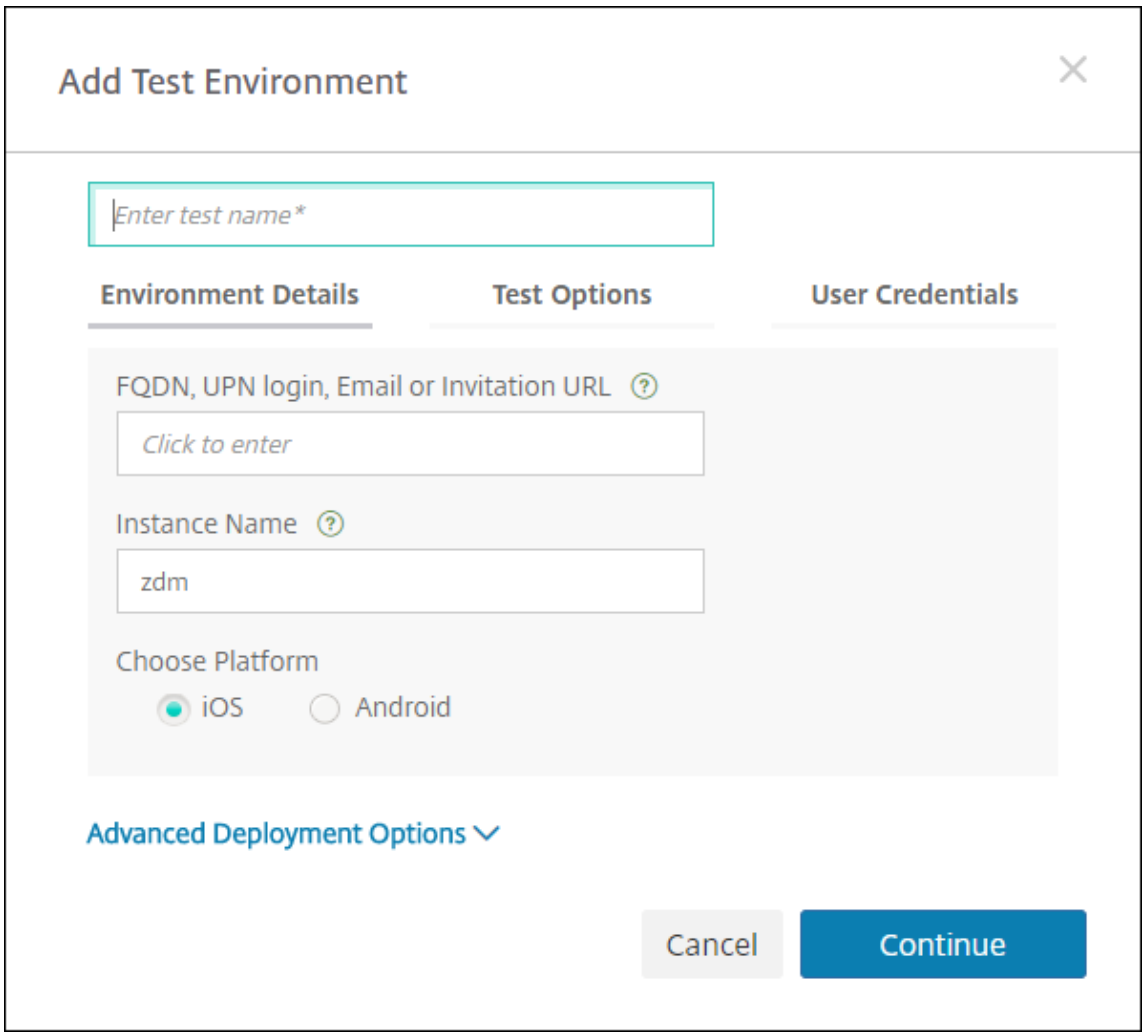
- **Environment Check(**환경검사**):** 이단계는설정을검사하여문제를확인하는테스트를안내합니다. 또한장치, 사용자등록및인증문제에대한권장사항및해결방법도제공합니다.
- **Citrix ADC Check(Citrix ADC** 확인**):** 이단계는 Citrix ADC 구성의 XenMobile 배포준비상태를확인하는과정을안내합니다.
- **Advanced Diagnostics(**고급진단**):** 이단계는 Citrix Insight Services 를사용하여환경검사에서놓친추가문제를찾는방법에대한정보를제공합니다.
- **Server Connectivity Checks(**서버연결확인**):** 이단계는서버연결을테스트하는데필요한지침을제공합니다.
- **Contact Citrix support(Citrix** 지원문의**):** 여전히문제가해결되지않는경우이단계의링크를통해 Citrix 지원사례를만들수있는사이트로이동할수있습니다.

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**)** 에서버액세스에사용되는정보를입력합니다.

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**)** 을클릭합니다.

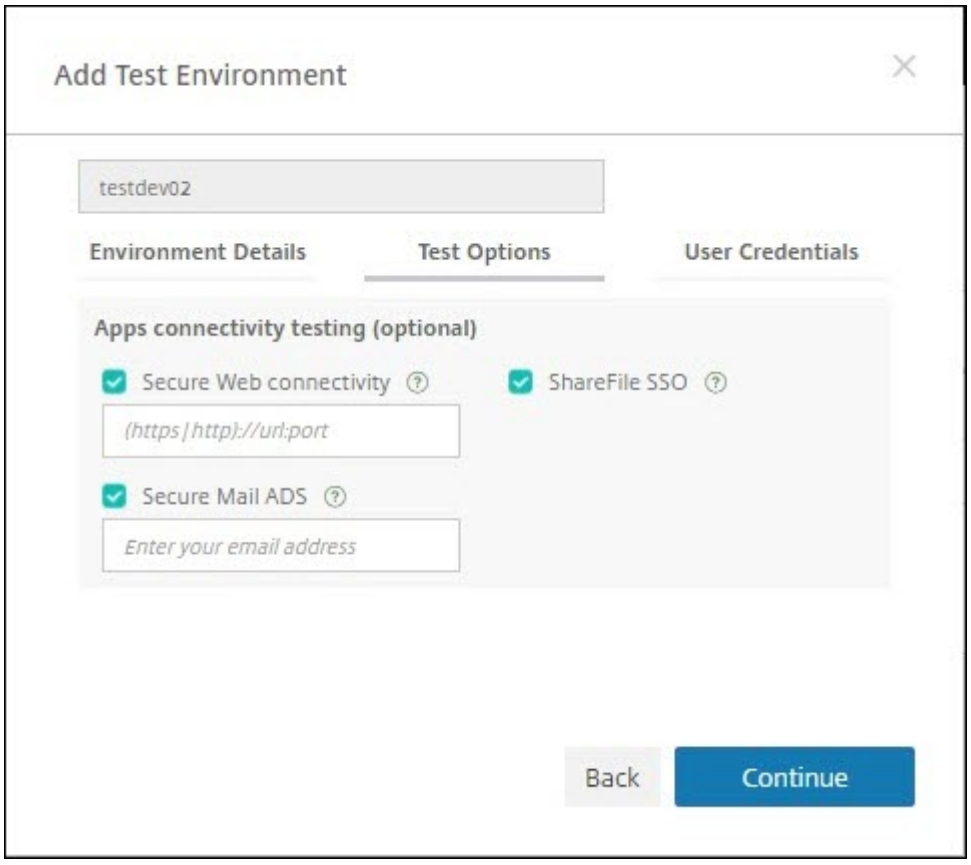
4. **Test Options(**테스트옵션**)** 탭에서다음테스트중하나이상을선택하고 **Continue(**계속**)** 를클릭합니다.

a) **Secure Web Connectivity(Secure Web** 연결**)**. 인트라넷 URL 을입력합니다. URL 의연결가능성이테스트됩니다. 이테스트는 Secure Web 앱에서인트라넷 URL 에연결을시도하는동안발생할수있는잠재적연결문

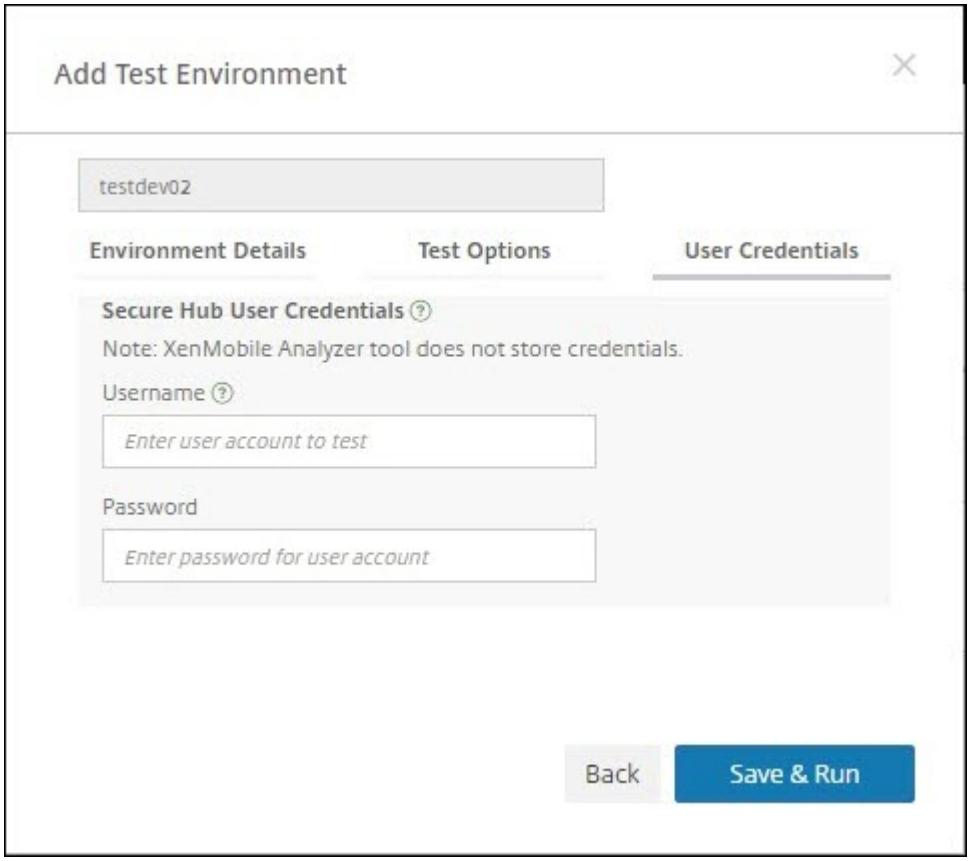
제를감지합니다.

b) **Secure Mail ADS**. 사용자전자메일 ID 를입력합니다. 이 ID 는 XenMobile 환경에서 Microsoft Exchange Server 의자동검색을테스트하는데사용됩니다. 이테스트는 Secure Mail 자동검색과관련된모든문제를감지합니다.

c) **ShareFile SSO**. 선택할경우 XenMobile Analyzer 는 Citrix Files DNS 확인이제대로수행되는지테스트합니다. 또한도구는 Citrix Files SSO(Single Sign-On) 가제공된사용자자격증명과호환되는지확인합니다.



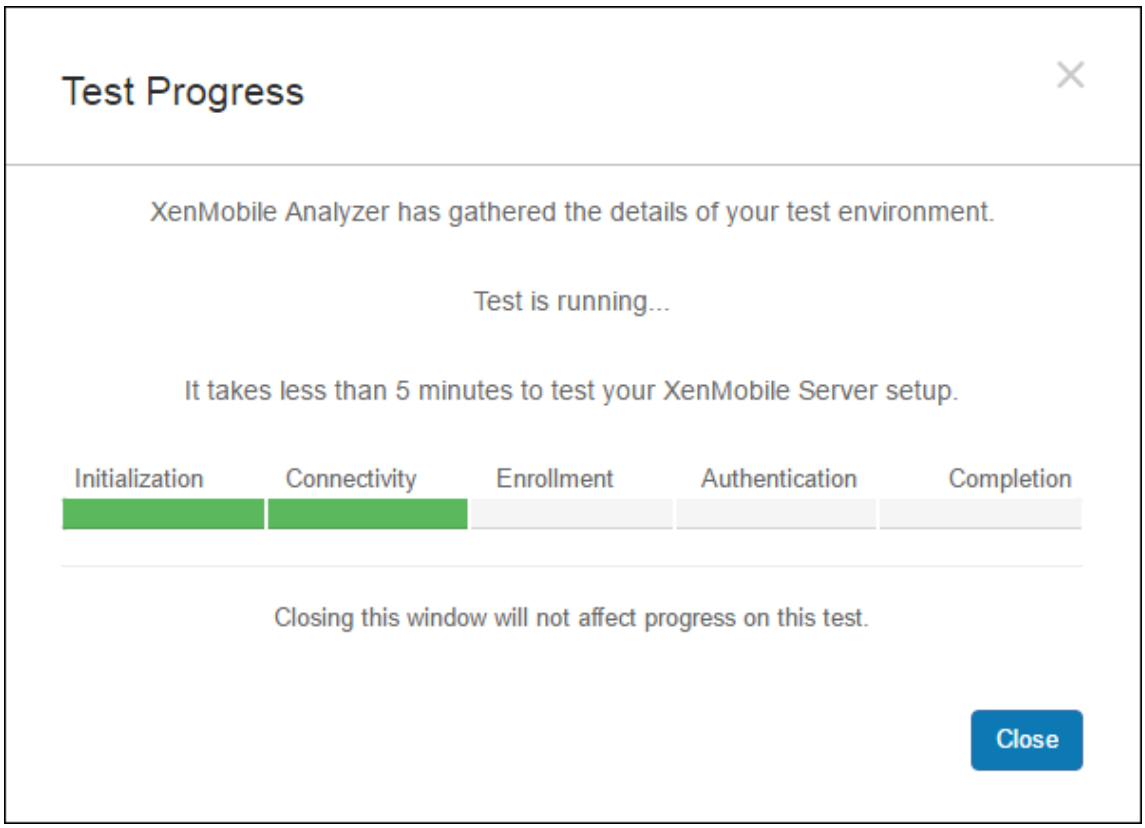
5. 서버설정에따라 **User Credentials(**사용자자격증명**)** 탭에다른필드가표시될수있습니다. 가능한필드는 **Username(**사용자이름**)**, **Username and Password(**사용자이름과암호**)** 또는 **Username, Password(**사용자이름**,** 암호**)** 및 **Enrollment PIN(**등록 **PIN)** 입니다.



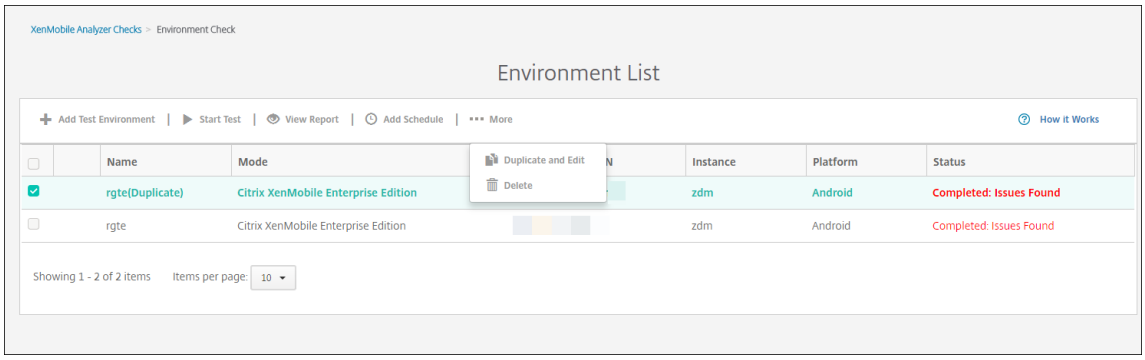
6. **Save & Run(**저장및실행**)** 을클릭하여테스트를시작합니다.

   진행률알림이나타납니다. 진행률대화상자를열린체로두거나대화상자를닫고테스트실행을계속할수있습니다.

   통과한테스트는녹색으로표시됩니다. 실패한테스트는빨간색으로표시됩니다.



진행률대화상자를닫으면 **Environments List(**환경목록**)** 페이지로돌아옵니다.



Results(결과**)** 페이지에 Test Details(테스트세부정보), Recommendations(권장사항) 및 Results(결과) 가표시됩니다.

7. **View Report(**보고서보기**)** 아이콘을클릭하여테스트결과를봅니다.

   권장사항에 Citrix 기술자료문서가연결된경우해당문서가이페이지에나열됩니다.

8. **Results(**결과**)** 탭을클릭하여결과와함께도구가수행한개별범주및테스트를표시합니다.

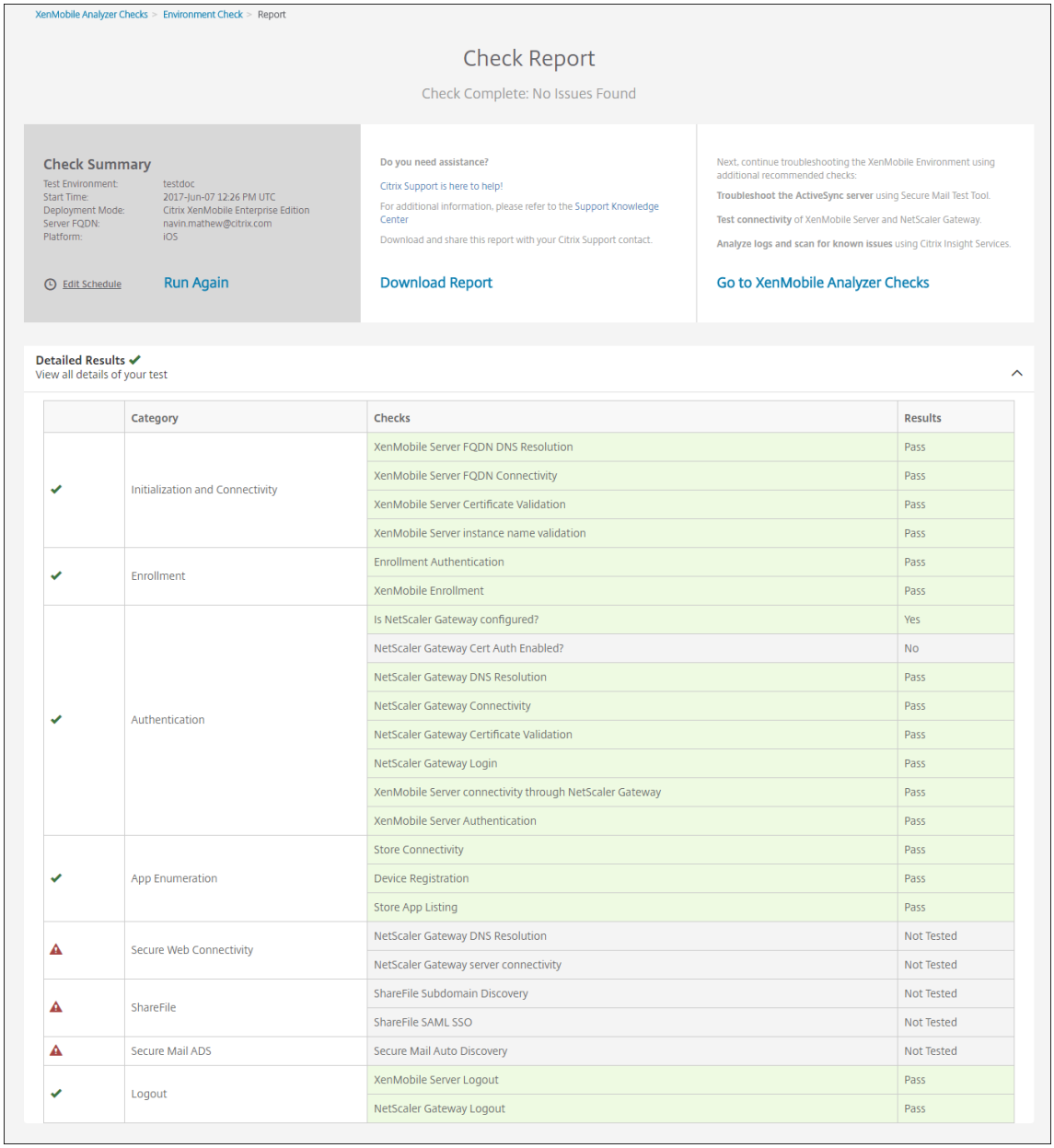
   a) 보고서를다운로드하려면 **Download Report(**보고서다운로드**)** 를클릭합니다.

   b) 테스트환경목록으로돌아가려면 **Environment Check(**환경검사**)** 를클릭합니다.

   c) 동일한테스트로다시실행하려면 **Run Again(**다시실행**)** 을클릭합니다.

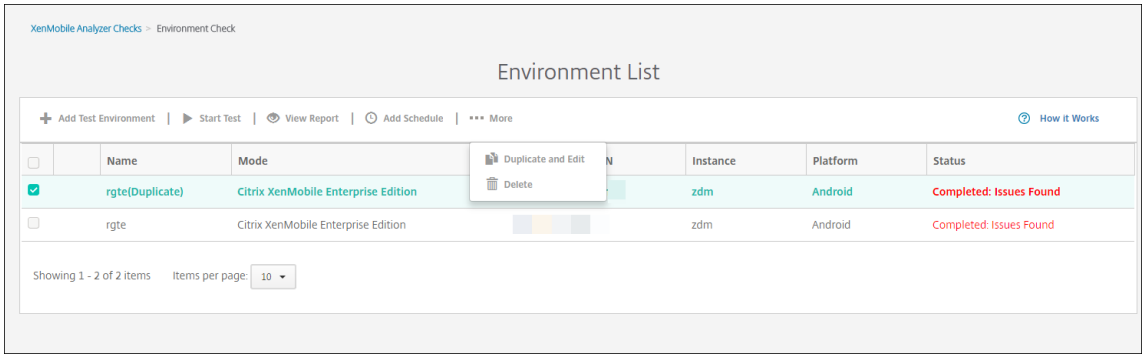
d) 다른테스트를다시실행하려면 **Test Environments(**환경테스트**)** 로이동하고테스트를선택한후 **Start Test(**테스트시작**)** 를클릭합니다.

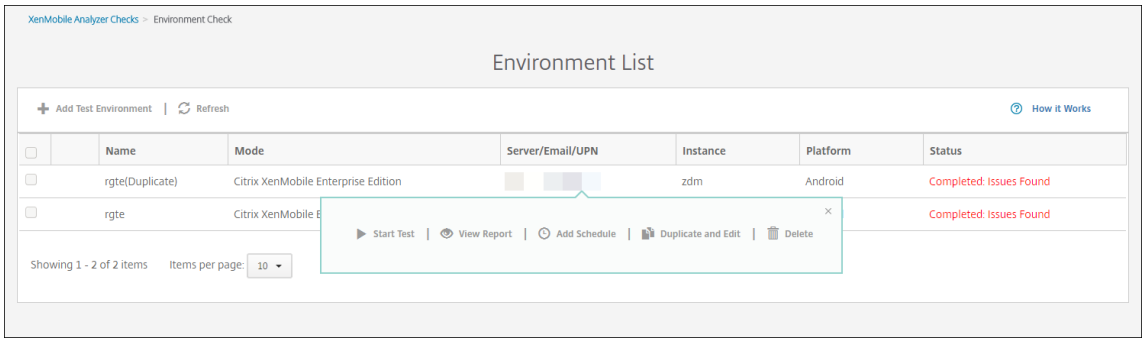
e) 다른 XenMobile Analyzer 옵션을선택하려면 **Go To XenMobile Analyzer Checks(XenMobile Analyzer** 검사로이동**)** 를클릭합니다.

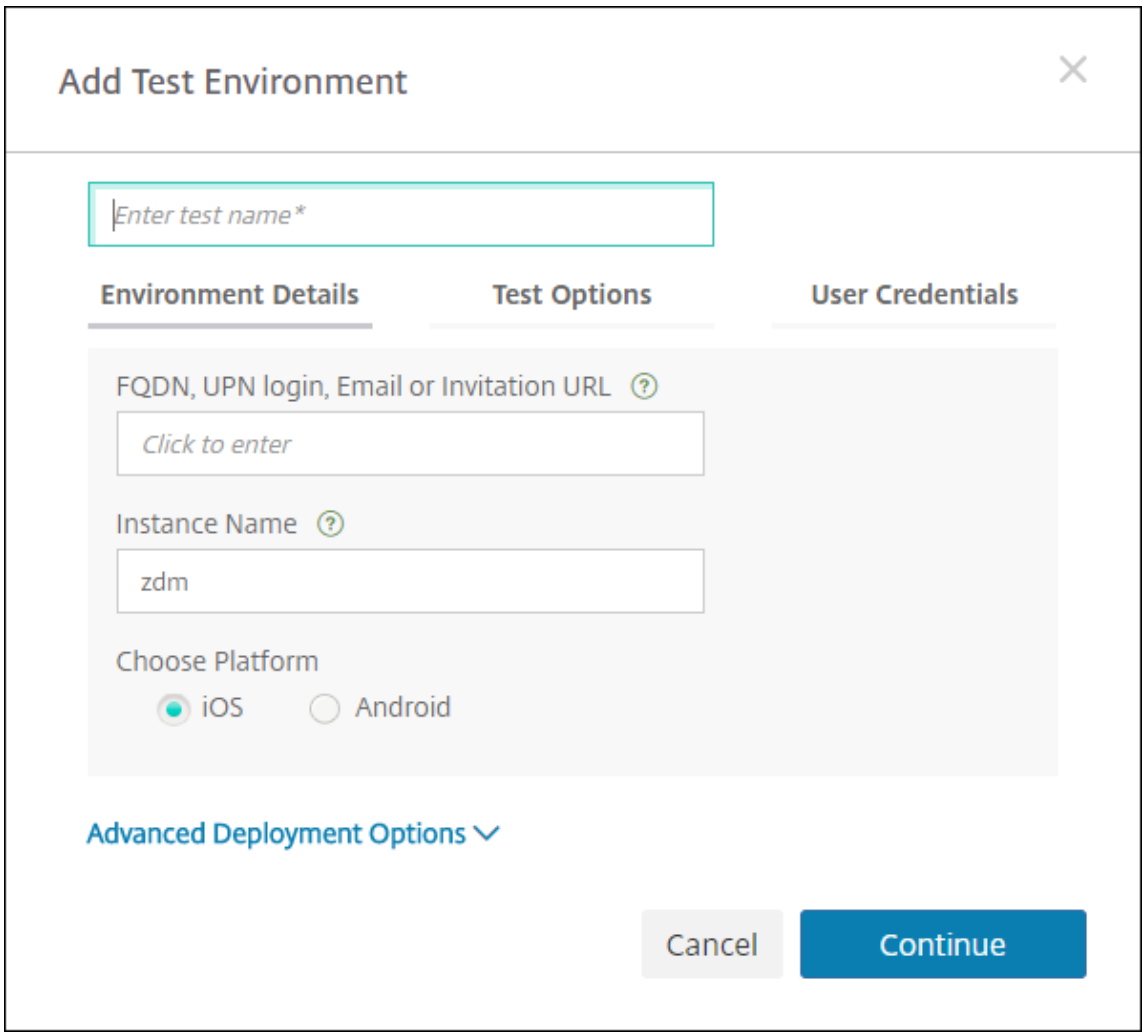


9. Test Environments(환경테스트) 페이지에서테스트를복사하고편집할수있습니다. 그렇게하려면테스트를선택하고 **More(**더보기**)** 를클릭한다음 **Duplicate and Edit(**복제및편집**)** 를클릭합니다.

   선택한테스트의복사본이만들어지고 Add Test Environment(테스트환경추가) 페이지가열리면새테스트를수정할수있습니다.



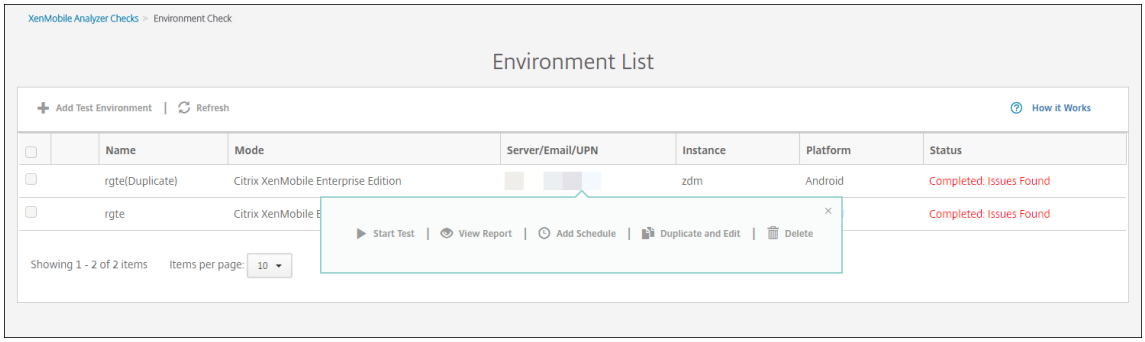




환경검사일정추가

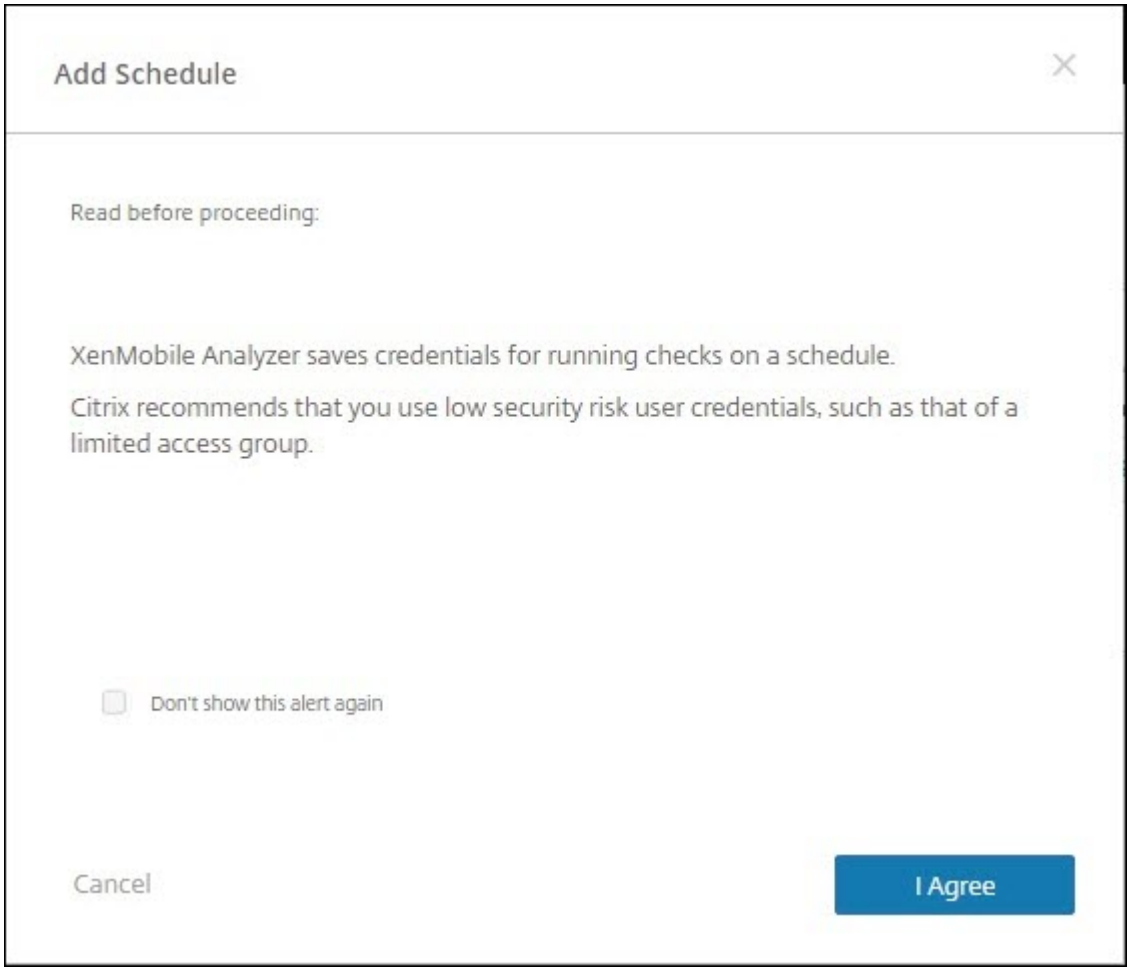
예약된일정에자동으로테스트가실행되고결과가구성된사용자목록으로전송되도록테스트를구성할수있습니다.

1. **Environment List(**환경목록**)** 페이지에서일정을설정할환경을선택하고 **Add Schedule(**일정추가**)** 을클릭합니다.

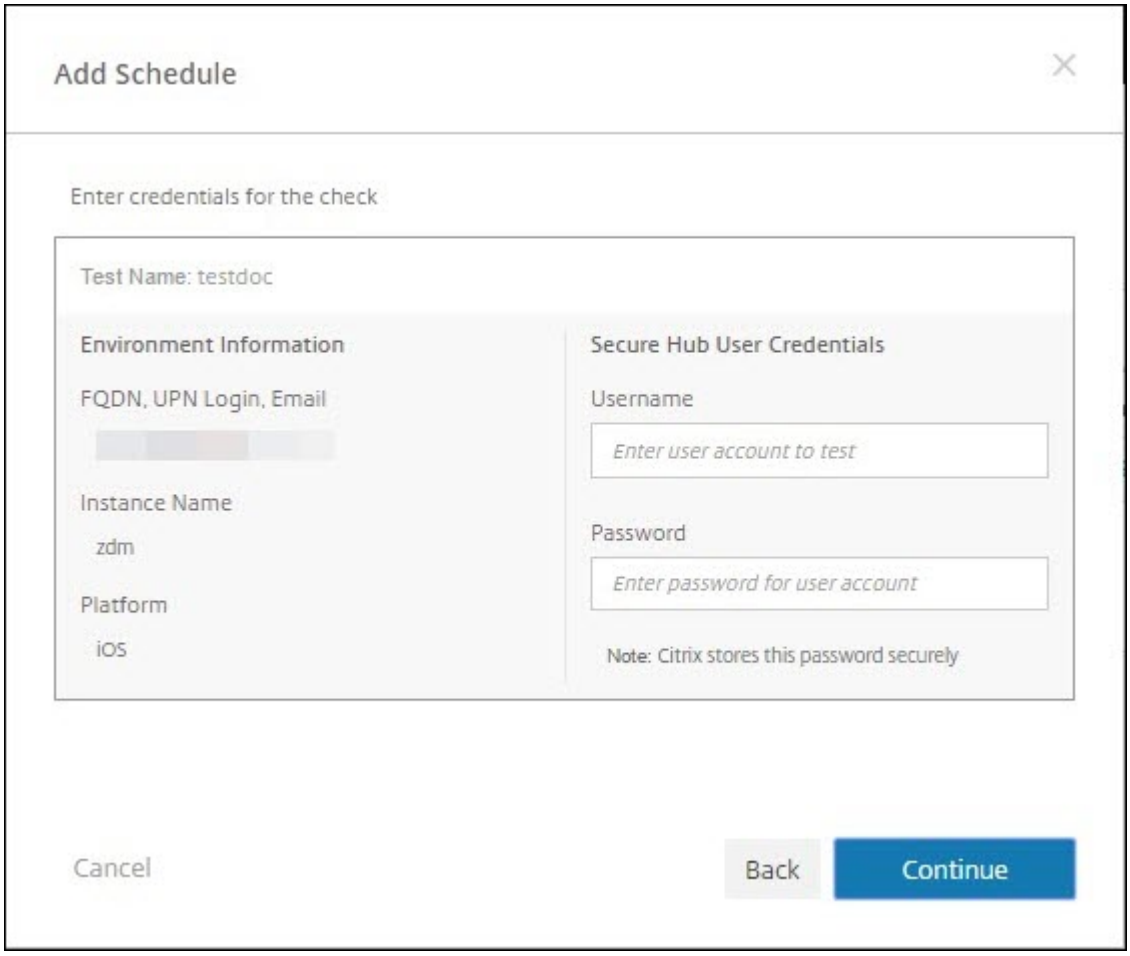


2. **Add Schedule(**일정추가**)** 창에예약된테스트실행을위한자격증명이 XenMobile Analyzer 에저장된다는경고메시지가표시됩니다. 예약된테스트를실행할때는액세스권한이제한된계정을사용하는것이좋습니다. **I Agree(**동의**)** 를클릭

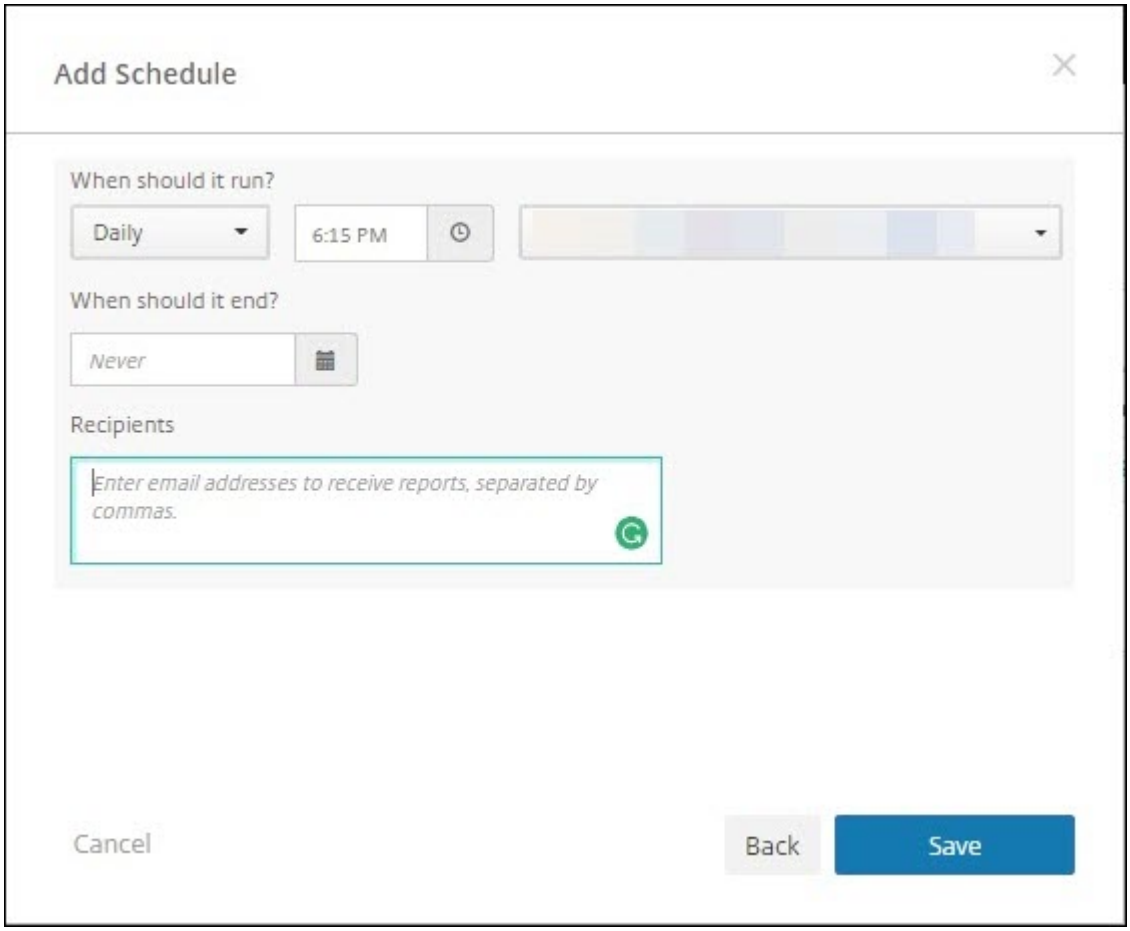
하여계속합니다.



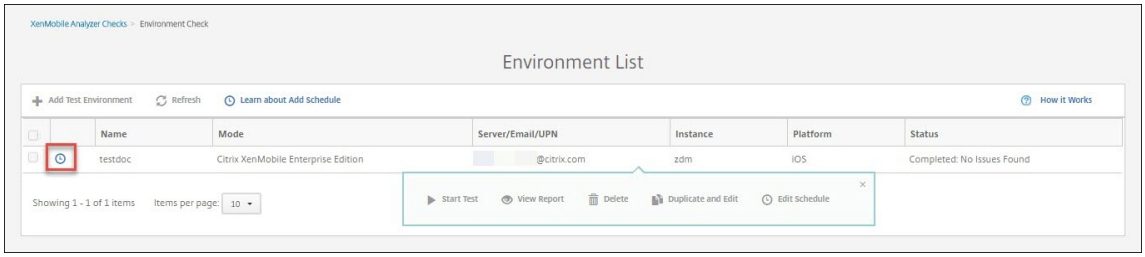
3. 테스트실행을위한 **Username(**사용자이름**)** 및 **Password(**암호**)** 를입력합니다.



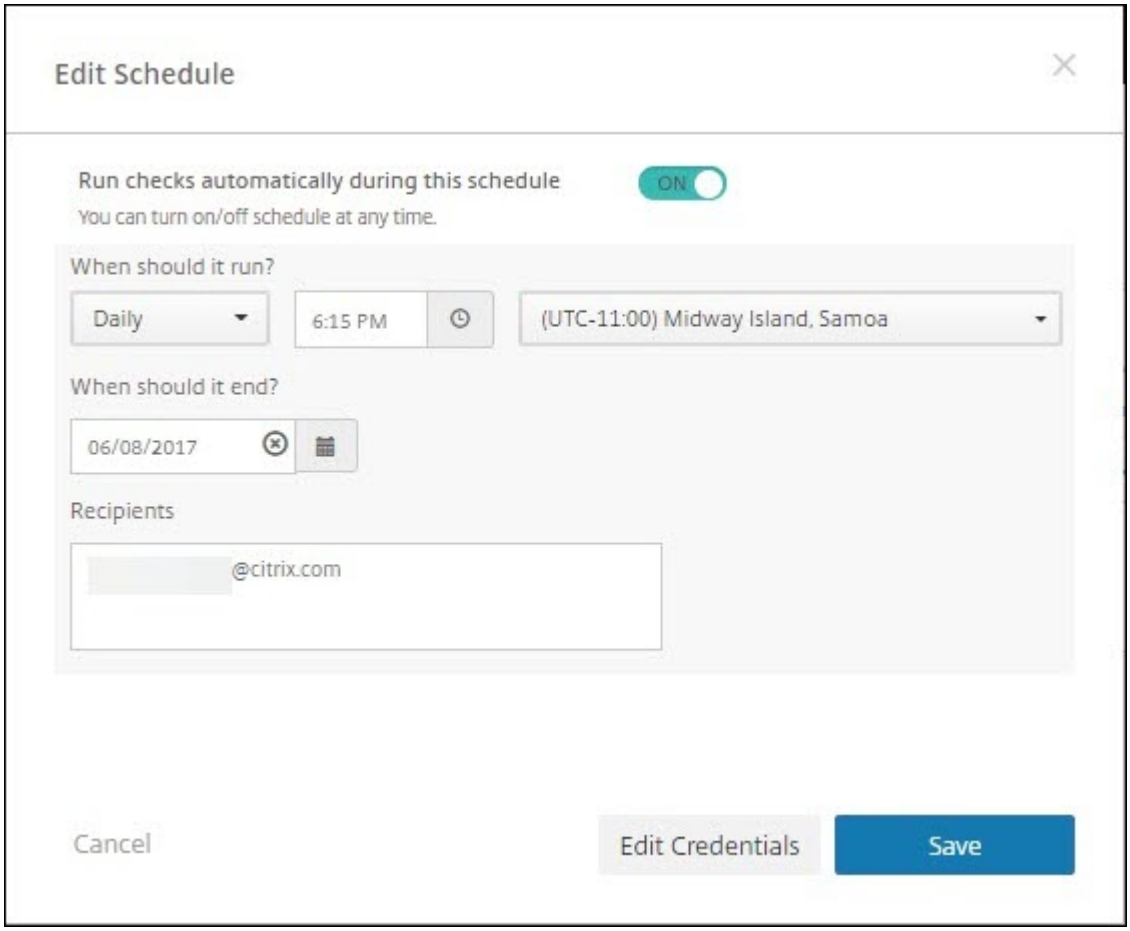
4. 테스트를실행할일정을구성합니다. 드롭다운에서 **Daily(**매일**)** 또는 **Weekly(**매주**)** 를선택할수있습니다. 테스트를실행할시간과표준시간대를선택합니다. 날짜선택기를사용하여예약된테스트의실행을중지할날짜를선택하거나테스트를무기한실행하도록비워둡니다. 보고서를받을전자메일주소목록을쉼표로구분하여입력합니다. 저장을클릭합니다.



5. 테스트왼쪽의시계기호는일정이구성되었음을나타냅니다. 테스트를선택하는경우 **Edit Schedule(**일정편집**)** 을클릭하여테스트를실행할시기를변경할수있습니다.



6. 이창에서테스트실행시기를변경할수있습니다. 또한맨위의스위치를클릭하여사용하지않을수도있습니다. 완료되면 **Save(**저장**)** 를클릭합니다.



기타정보검사수행

XenMobile Analyzer 의환경검사단계와직접상호작용하여테스트를수행할수있지만다른옵션은정보를제공하는용도입니다. 이러한각옵션은 XenMobile 환경이올바르게설정되었는지확인하는데사용할수있는다른지원도구에관한정보를제공합니다.

- **Advanced Diagnostics(**고급진단**):** 환경의정보를수집한후 Citrix Insight Services 에업로드하는데필요한지침을제공합니다. 이도구는데이터를분석하고권장해결방법이포함된맞춤형보고서를제공합니다.
- **Secure Mail Readiness(Secure Mail** 준비**):** XenMobile Exchange ActiveSync Test 응용프로그램다운로드를위한지침을제공합니다. 이응용프로그램은 ActiveSync 서버문제를해결하여 XenMobile 환경에배포할수있도록준비합니다. 응용프로그램이실행되면보고서를보거나다른사용자와공유할수있습니다.
- **Server Connectivity Checks(**서버연결확인**):** XenMobile 서버, 인증서버및 Content Collaboration 서버에대한연결을확인하는지침을제공합니다.
- **Contact Citrix support(Citrix** 지원문의**):** 다른모든방법에서실패한경우 Citrix 지원을통해지원티켓을만들수있습니다.

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 5, 2022

> 참고:
>
> 이문서에서는 XenMobile Server 용 REST API 에대해다룹니다. Endpoint Management 용 REST API 에대해서는 REST API를참조하십시오.

XenMobile REST API 를사용하여 XenMobile 콘솔을통해표시되는서비스를호출할수있습니다. 모든 REST 클라이언트를사용하여 REST 서비스를호출할수있습니다. API 를사용하면 XenMobile 콘솔에로그온하지않고서비스를호출할수있습니다.

현재사용가능한전체 API 집합을보려면 REST 서비스에대한공용 API PDF 를다운로드하십시오.

REST API 액세스에필요한권한

REST API 에액세스하려면다음권한중하나가필요합니다.

- 공용 API 액세스권한은역할기반액세스구성의일부로설정됩니다. 자세한내용은 RBAC 를사용하여역할구성을참조하십시오.
- 슈퍼사용자권한

REST API 서비스를호출하려면

REST 클라이언트또는 CURL 명령을사용하여 REST API 서비스를호출할수있습니다. 다음예제에서는 Chrome 용 Advanced REST 클라이언트를사용합니다.

> 참고:
>
> 다음예제에서호스트이름및포트번호를환경에맞게변경하십시오.

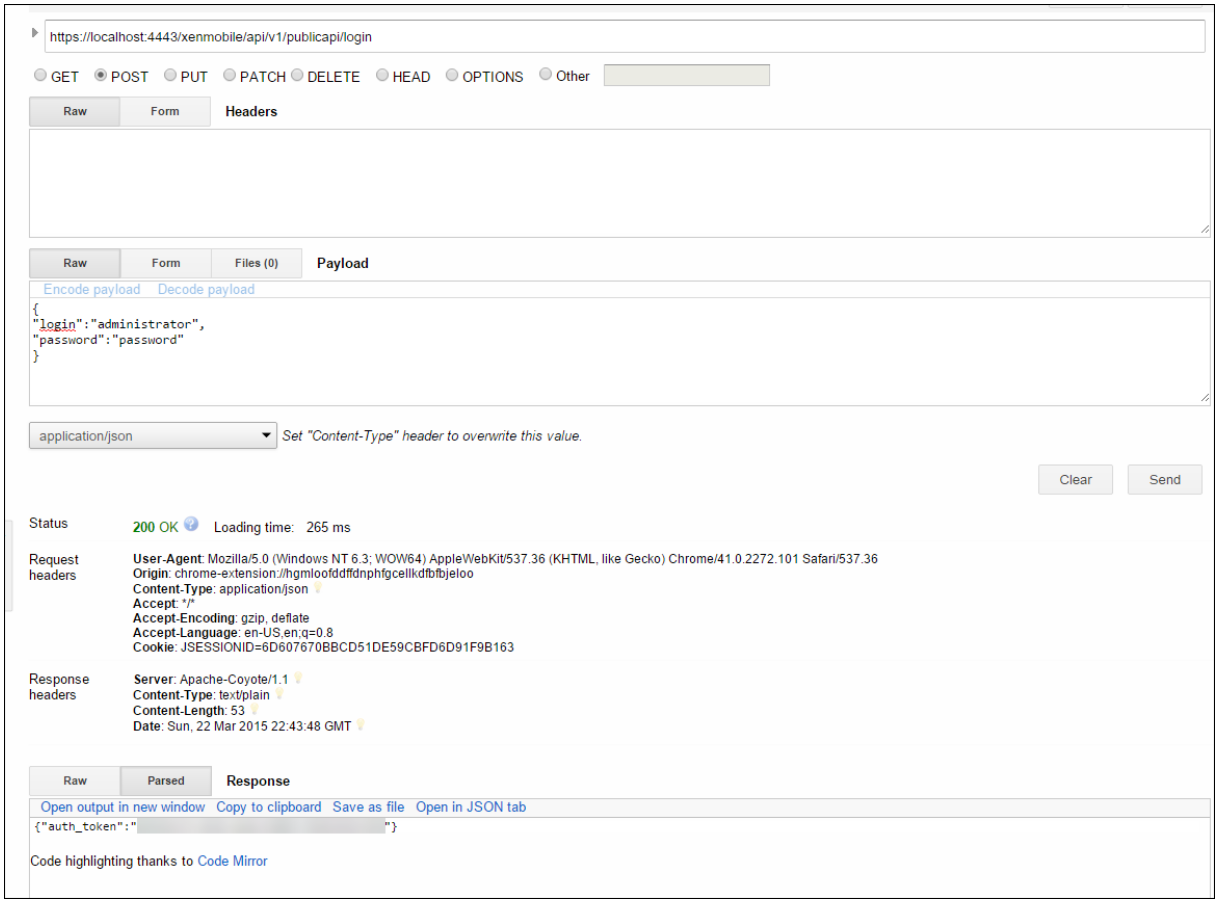
로그인

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

요청: `{ "login":"administrator", "password":"password"}`

메서드형식: POST

콘텐츠형식: application/json



관련정보

- XenMobile REST API

Exchange ActiveSync 용 Endpoint Management 커넥터

March 14, 2022

XenMobile Mail Manager 는이제 Exchange ActiveSync 용 Endpoint Management 커넥터입니다. Citrix 통합포트폴리오에대한자세한내용은 Citrix 제품가이드를참조하십시오.

이커넥터는다음과같이 XenMobile 의기능을확장합니다.

- EAS(Exchange Active Sync) 장치에대한동적액세스제어. EAS 장치는 Exchange 서비스에대한액세스가자동으로허용또는차단될수있습니다.
- XenMobile 이 Exchange 에서제공하는 EAS 장치파트너관계정보에액세스하는기능.
- EAS 상태를기반으로모바일장치를초기화하는 XenMobile 의기능입니다.
- XenMobile 이 Blackberry 장치에대한정보에액세스하고초기화및 ResetPassword 같은제어작업을수행하는기능.

EAS 상태를기반으로장치를초기화하려면 ActiveSync 트리거로자동화된작업을구성합니다. 자동화된동작을참조하십시오.

Exchange ActiveSync 용 Endpoint Management 커넥터를다운로드하려면:

1. https://www.citrix.com/downloads로이동합니다.
2. **Citrix Endpoint Management(**및 **Citrix XenMobile Server) > XenMobile Server(**온-프레미스**) >** 제품소프트웨어 **> XenMobile Server 10 >** 서버구성요소로이동합니다.
3. **Exchange ActiveSync** 용 **Citrix Endpoint Management** 커넥터타일에서 파일다운로드를클릭합니다.

> 중요**:**
>
> 2022 년 10 월부터 Exchange ActiveSync 용 Endpoint Management 및 Citrix Gateway 커넥터는 Microsoft 가 여기에서발표한인증변경사항에따라더이상 Exchange Online 을지원하지않습니다. Exchange 용 Endpoint Management 커넥터는 Microsoft Exchange Server(온-프레미스) 에서계속작동합니다.

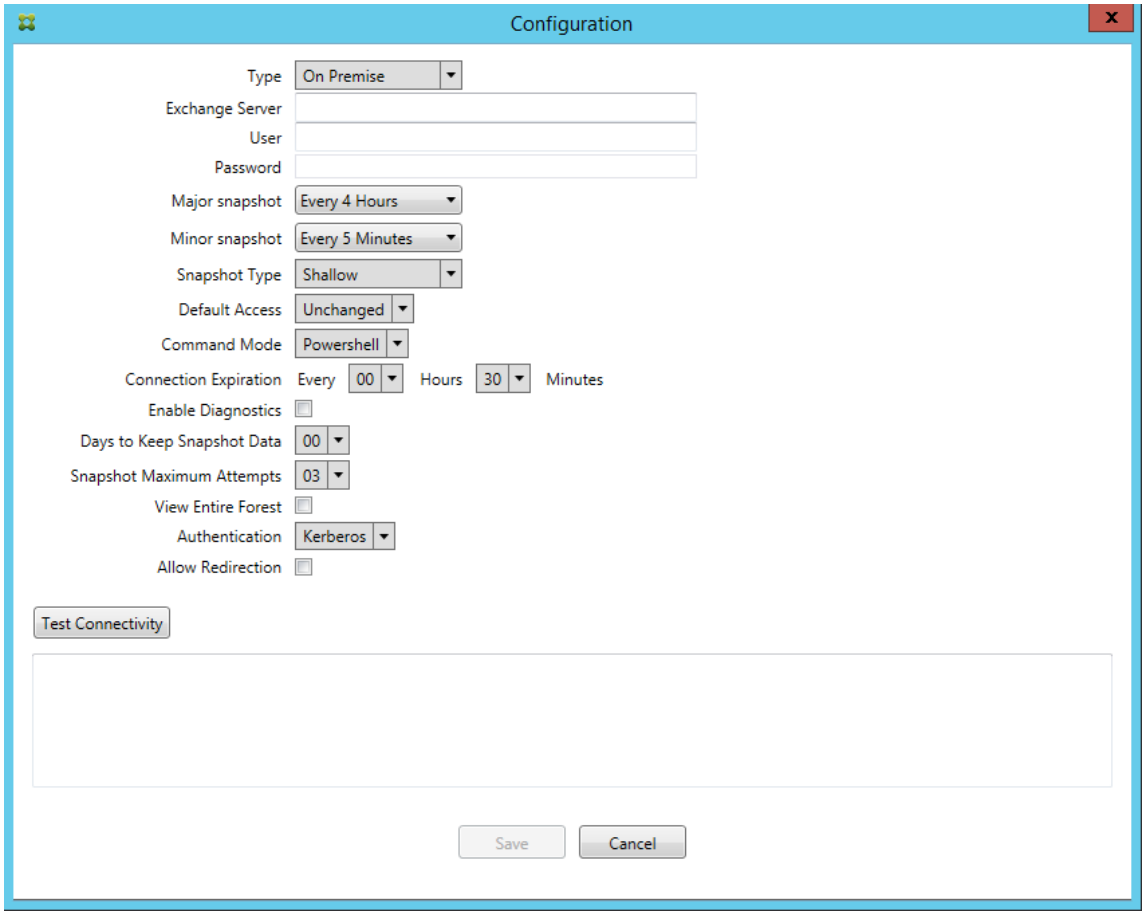
새로운항목

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]

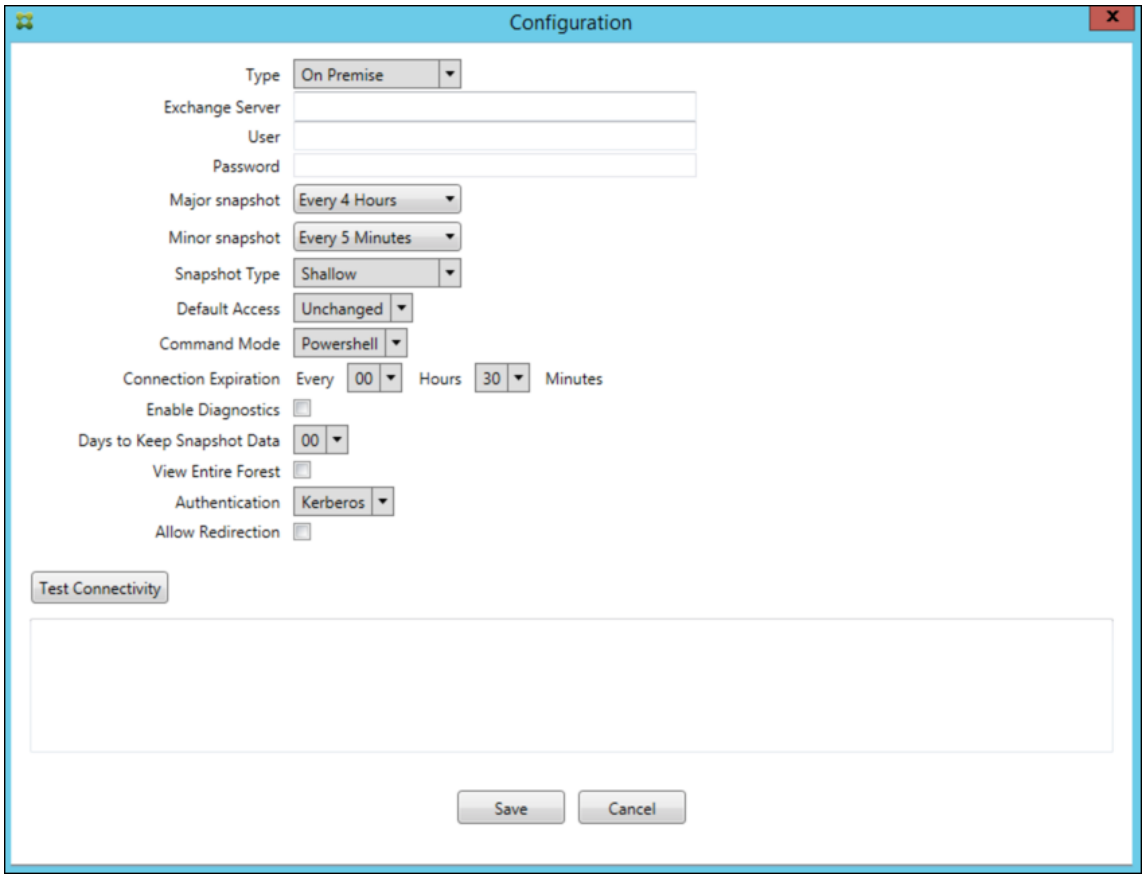
이전버전의새로운기능

다음섹션에는 Exchange ActiveSync 용 Endpoint Management 커넥터의이전버전에포함된기능과수정된문제가나와 있습니다.

버전 **10.1.9** 의새로운기능

다음문제는버전 10.1.9 에서수정되었습니다.

- 이제구성변경이보다일관된방식으로처리됩니다. 서비스가구성변경을감지하면각내부하위시스템이중지됩니다. 즉, 모든활성또는예약처리가중단됩니다. 그런다음새구성이로드되고하위시스템이다시시작됩니다. 즉, 모든예약및기타내부인프라가새설정으로다시설정됩니다. 이문제는버전 10.1.8 의알려진문제를수정합니다. [CXM-47709, CXM-61330]
- 업그레이드중에기존데이터베이스구성이새구성파일에병합되지않았습니다. 이제데이터베이스구성이업그레이드된구성파일에병합됩니다. [CXM-49326]
- 스냅샷관련진단파일에서열헤더가누락되었습니다. 헤더가복원되었습니다. [CXM-62680]
- 이전버전에서업그레이드하는경우사용중인구성파일의유사한섹션이구성파일의기본값섹션을덮어씁니다. 이문제로인해업그레이드후기본값섹션에추가또는개선사항이로드되지않습니다. 이버전부터는기본값섹션에항상최신구성이반영됩니다. [CXM-62681]
- 관리자는응용프로그램을실행할때더이상 Shift 키를눌러특정옵션에액세스할수없습니다. 이러한옵션은이전에 Citrix 사용권한으로사용할수있었습니다. 이제리디렉션허용과같은일부옵션을완벽하게사용할수있으며감지중지및개수수정같은다른옵션은사용되지않습니다. [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. 제한이적용되면다

음명령을전송하기전에서비스를지정된기간동안일시중지해야합니다. 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 기본액세스상태가허용됨상태여야하지만차단됨인경우사용자는전자메일에액세스하지못할수있습니다. 또는전자메일에대한액세스가차단되어야하는사용자에게액세스권한이부여될수있습니다. 이제 Exchange ActiveSync 용 Citrix Endpoint Management 커넥터가원하는상태의모든장치를각 **Set-CasMailbox** 명령에포함합니다. [CXM-61251]

다음은버전 10.1.8 에서알려진문제입니다.

스냅샷또는정책평가같은장기작업이서비스에서실행되는동안관리자가구성응용프로그램에서구성데이터를수정하는변경을수행하면서비스가규정불가능한상태로전환될수있습니다. 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]
- 진단을개선하기위해최근에사서함허용/차단됨상태를설정하는데사용되는장치 ID 목록에대한문자열형식을변경했습니다. 하지만너무많은장치를지정하면최대문자열크기가초과되었습니다. 이제내부배열데이터구조를사용합니다. 이구조에는크기제한이없으며데이터의형식을진단용도에적합하게지정합니다. [CXM-52610]
- Exchange 와동기화되지않은장치정책이검색되는경우해당명령에관련사서함에속하지않는장치가포함되어있을수있습니다. 이제 Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange 에대한명령에관련사서함에속한장치만나타나게합니다. [CXM-54842]
- 일부환경에서 Microsoft 어셈블리를사용할수없습니다. 필요한어셈블리가이제응용프로그램과함께명시적으로설치됩니다. [CXM-55439]

- 장치또는사서함의고유이름에서특성이름과등호사이및/또는등호와값사이에공백이있는경우 Exchange ActiveSync 용 Endpoint Management 커넥터가장치와사서함을올바르게일치시키지못할수있습니다. 결과적으로스냅샷조정중에일부장치및/또는사서함이거부될수있습니다. [CXM-56088]

> 참고:
>
> 이후섹션에서는 Exchange ActiveSync 용 Endpoint Management 커넥터가이전이름인 XenMobile Mail Manager 로나타납니다. 이이름은버전 10.1.7 에서변경되었습니다.

버전 **10.1.6.20** 의업데이트

10.1.6 에대한업데이트에는버전 10.1.6.20 의다음과같은수정사항이포함되어있습니다.

- Exchange 와동기화되지않은장치정책이검색되는경우해당명령에관련사서함에속하지않는장치가포함되어있을수있습니다. 이제 XenMobile Mail Manager 는 Exchange 에대한명령에관련사서함에속한장치만나타나게합니다. [CXM-54842]

버전 **10.1.6** 의새로운기능

XenMobile Mail Manager 버전 10.1.6 에는다음과같은수정된문제와개선사항이포함되어있습니다.

- 경우에따라스냅샷기록창이더이상업데이트되지않는상태로전환됩니다. 더욱안정적으로업데이트되도록창새로고침메커니즘이개선되었습니다. [CXM-47983]
- 파티셔닝된스냅샷과파티셔닝되지않은스냅샷에두가지별도의모드와코드경로가사용되었습니다. 파티셔닝되지않은스냅샷은단일 “*” 파티션을사용하는구성의파티셔닝된스냅샷과동일하기때문에파티셔닝되지않은스냅샷모드가제거되었습니다. 이제 36 개의파티션 (0–9, A–Z) 이있는파티셔닝된스냅샷이기본스냅샷모드입니다. [CXM-49093]
- 스냅샷기록창에서오류메시지가상태메시지로덮어써집니다. 이제 XenMobile Mail Manager 에두개의별도필드가표시되어사용자가상태와오류를동시에볼수있습니다. [CXM-51942]
- Exchange Online(Office 365) 에연결할때스냅샷관련쿼리로인해데이터집합이잘릴수있습니다. 이문제는 XenMobile Mail Manager 가다중명령파이프라인이있는스크립트를실행하는경우에발생할수있습니다. 업스트림명령이다운스트림명령에충분히빠르게데이터를전달할수없어작업이조기에완료되고불완전한데이터가생깁니다. 이제 XenMobile Mail Manager 가파이프라인자체를모방하고업스트림명령이완료될때까지기다린후에다운스트림명령을호출할수있습니다. 이변경사항에따라이제모든데이터가처리되고캡처됩니다. [CXM-52280]
- Exchange 에대한정책업데이트명령에서해결할수없는오류가발생할경우동일한명령이오랫동안반복적으로작업대기열에반환됩니다. 이경우해당명령이 Exchange 에여러번전송되었습니다. 이 XenMobile Mail Manager 버전에서는오류를일으키는명령이작업대기열에불연속적으로만반환됩니다. [CXM-52633]
- 특정사서함에대한정책업데이트에모든장치허용또는차단이포함된경우 **Set-CASMailbox** 명령실행이실패합니다. 빈목록이 **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 에서제한이해제될때까지주스냅샷의시작이금지됩니다. [CXM-49617]
- 주스냅샷작업중 XenMobile Mail Manager 에 Exchange 의제한이적용될경우다음스냅샷을실행하기까지허용되는경과시간이부족할수있습니다. 이문제로인해제한이연장되고스냅샷이실패합니다. 이제 XenMobile Mail Manager 가 Exchange 에서지정한최소스냅샷시도대기간격동안대기합니다. [CXM-49618]
- 진단이사용되는경우명령파일에서 **Set-CasMailbox** 명령의각속성이름앞에하이픈이누락된것으로나타납니다. 이문제는진단파일의형식에서만발생하며 Exchange 에대한실제명령에서는발생하지않습니다. 하이픈누락으로인해사용자는테스트또는유효성검사를위해명령을잘라내어 PowerShell 프롬프트에바로붙여넣지는못합니다. 하이픈이추가되었습니다. [CXM-52520]
- 사서함 ID 가 "lastname, firstname" 형식인경우 Exchange 가쿼리에서데이터를반환할때쉼표앞에백슬래시를추가합니다. XenMobile Mail Manager 가추가데이터쿼리를위해 ID 를사용할때이백슬래시를제거해야합니다. [CXM-52635]

알려진제한사항

> 참고**:**
>
> 다음제한사항은버전 10.1.6 에서해결되었습니다.

XenMobile Mail Manager 에는알려진제한제한이있으며, 이로인해 Exchange 에대한명령이실패할수있습니다. Exchange 에정책변경사항을적용하기위해 XenMobile Mail Manager 는 **Set_CASMailbox** 명령을실행합니다. 이명령은두가지장치목록, 즉허용목록과차단목록을사용할수있습니다. 이명령은사서함에연결된장치에적용됩니다.

이러한목록은 Microsoft API 에의해각각 256 자로제한됩니다. 이러한목록중하나가제한을초과할경우명령이완전히실패하여사서함의해당장치에대한모든정책이설정되지않습니다. XenMobile Mail Manager 로그에다음과같은오류가보고됩니다. 차단목록에대한예입니다.

"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 길이는달라질수있지만일반적으로동시에 10 개이상의허용또는차단장치가포함될경우제한이초과될수있습니다. 특정사서함에많은장치가연결되는경우는드물지만있을수있습니다. XenMobile Mail Manager 가이러한경우를처리하도록개선될때까지사용자와사서함에연결되는장치수를 10 개이하로제한하는것이좋습니다. [CXM-52633]

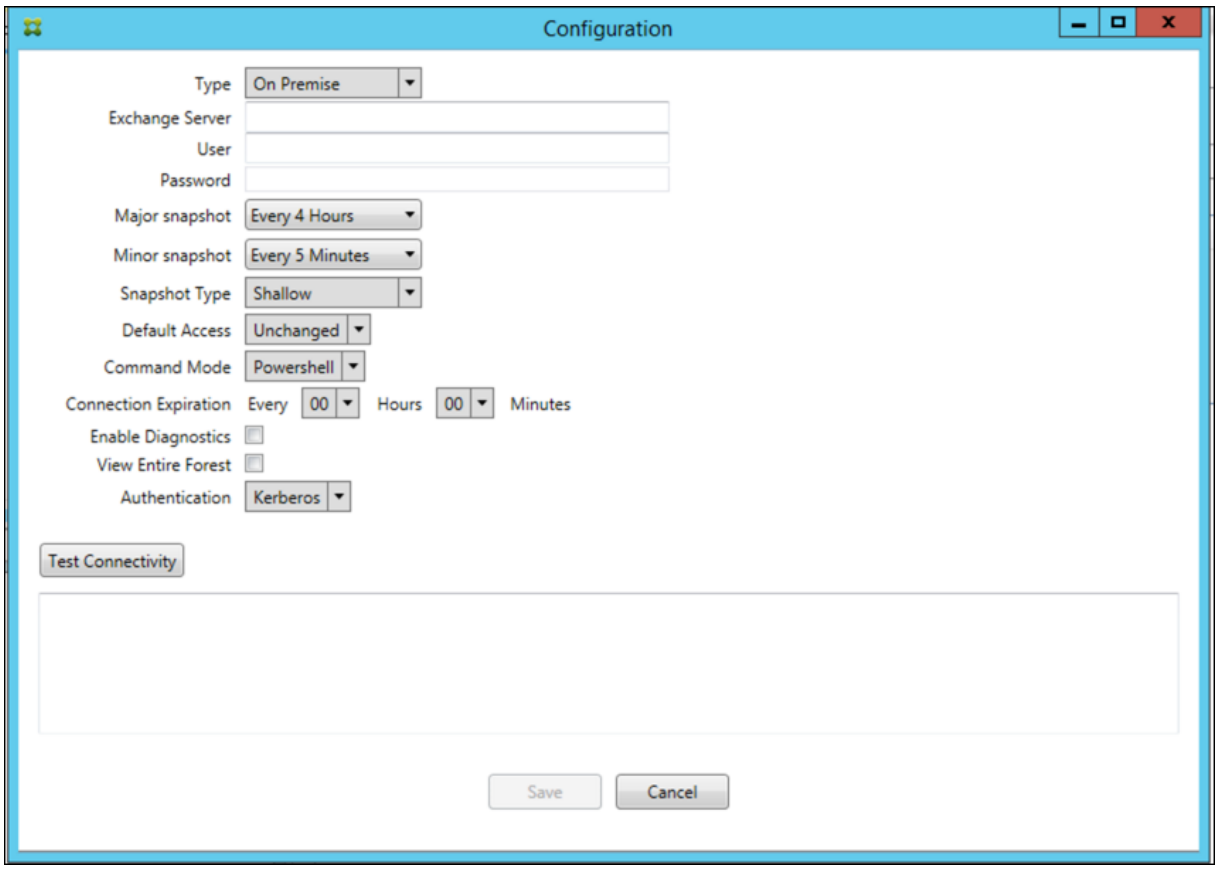
버전 **10.1.4** 의새로운기능

XenMobile Mail Manager 버전 10.1.4 에는다음과같은수정된문제가포함되어있습니다.

- PCI Council 에서는보안이취약한 TLS 1.0 의사용을중지하고있습니다. XenMobile Mail Manager 에는 TLS 1.1 및 1.2 에대한지원이추가되었습니다. [CXM-38573, CXM-32560]
- XenMobile Mail Manager 에는새로운진단파일이포함됩니다. Exchange 사양에서 **Enable Diagnostics(**진단사용**)** 를선택하면새스냅샷기록파일이생성됩니다. 스냅샷을시도할때마다스냅샷의결과로파일에행이추가됩니다. [CXM-49631]
- **Set-CASMailbox** 명령에대한명령진단파일에허용되거나차단된장치목록이나타나지않았습니다. 대신, 파일의관련된 인수에내부클래스이름이표시되었습니다. 이제 XenMobile Mail Manager 의 deviceID 목록이쉼표로구분된목록으로표시됩니다. [CXM-50693]
- 잘못된사양으로인해 Exchange 에대한연결시도가실패할경우오류메시지가 “All connections in use(모든연결을사용중임)” 라는잘못된메시지로재정의되었습니다. 이제보다설명적인메시지가나타납니다. 예를들어 “All connections are inoperable(모든연결이작동하지않음)”, “Connection pool is empty(연결풀이비어있음)”, “All connections are throttled(모든연결이제한됨)” 및 “No available connections(사용가능한연결없음)” 같은메시지가나타납니다. [CXM-50783]
- 경우에따라허용/차단/초기화명령이 XenMobile Mail Manager 내부캐시의대기열에여러번배치됩니다. 이문제로인해 Exchange 로전송되는명령이지연됩니다. 이제 XenMobile Mail Manager 가각명령에대한단일인스턴스만대기열에배치합니다. [CXM-51524]

버전 **10.1.3** 의새로운기능

- **Google Analytics** 지원**:** XenMobile Mail Manager 가어떻게사용되는지를확인하여제품의개선영역에집중할수 있습니다.
- 진단사용설정**: Configuration(**구성**)** 대화상자의 Configure console(콘솔구성) 에 **Enable Diagnostic(**진단사용**)** 확인란이나타납니다.



버전 **10.1.3** 의수정된문제

- **Snapshot History(**스냅샷기록**)** 창에서스냅샷의현재상태를보여주는도구설명에실제상태가반영되지않습니다. [CXM-5570]
  가끔, XenMobile Mail Manager 에서명령진단파일이작성되지않습니다. 이경우명령기록이하나도기록되지않습니다. [CXM-49217]
- 연결오류가발생하는경우연결이 “errored” 로표시되지않습니다. 그결과후속명령에서연결사용을시도하고다른오류가발생할수있습니다. [CXM-49495]
- Exchange Server 에서제한이발생하면상태확인루틴에서예외가발생할수있습니다. 그결과오류가발생하거나만료된연결을삭제하지못할수있습니다. 또한 XenMobile Mail Manager 에서제한시간이만료되기전까지연결을만들지못할수있습니다. [CXM-49794].
- Exchange 의최대세션수가초과되면 XenMobile Mail Manager 가정확한메시지가아닌 “Device Capture Failed(장치캡처실패)” 오류를보고합니다. XenMobile Mail Manager 가 Exchange 통신에정상적으로사용하는세션두개가사용중임을나타내는메시지가보고되어야합니다. [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. 연결이만료시간에도달하면 XenMobile Mail Manager 가 PowerShell 세션을정상적으로종료하고세션을만들수있습니다. 이렇게하면 PowerShell 세션이불안정해질가능성이줄고스냅샷실패확률이크게감소합니다.

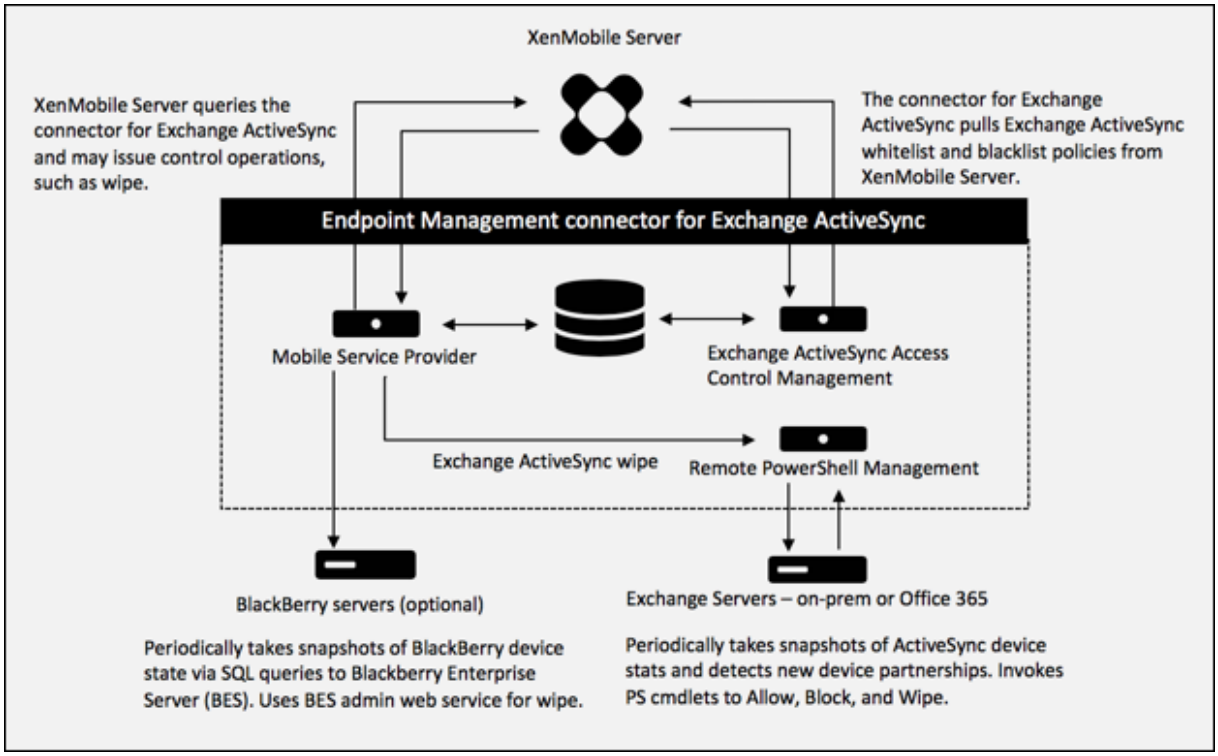
- 스냅샷워크플로개선: 주스냅샷을생성하는데시간이오래걸리고프로세스가복잡합니다. 이제스냅샷생성중에오류가발생할경우 XenMobile Mail Manager 가여러번의시도 (최대 3 회) 를통해스냅샷을완료합니다. 후속시도는처음부터시작되지않습니다. XenMobile Mail Manager 는중단된위치에서시도를계속합니다. 스냅샷을진행하는동안일시적인오류를넘길수있으므로일반적으로스냅샷성공률이개선됩니다.
- 진단개선: 스냅샷중에선택적으로생성할수있는새로운세가지진단파일을사용하여스냅샷문제를이제보다쉽게해결할수있습니다. 이러한파일은 PowerShell 명령문제, 정보가누락된사서함및사서함에연결할수없는장치를식별하는데도움이됩니다. 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 에대한연결개선으로이문제가해결됩니다. (XMHELP-293, XMHELP-311, XMHELP-801)
- 정확하지않은사서함및장치수: XenMobile Mail Manager 의사서함-장치연결알고리즘이개선되었습니다. 개선된진단기능을사용하면 XenMobile Mail Manager 가책임영역내에없다고간주하는사서함및장치를식별할수있습니다. (XMHELP-623)
- 허용/차단/초기화명령이인식되지않음: 가끔 XenMobile Mail Manager 허용/차단/초기화명령이인식되지않는버그가수정되었습니다. (XMHELP-489)
- 메모리관리: 메모리관리및완화가개선되었습니다. (XMHELP-419)

아키텍처

다음그림에서는 Exchange ActiveSync 용 Endpoint Management 커넥터의주요구성요소를보여줍니다. 자세한참조아키텍처다이어그램은 아키텍처를참조하십시오.



세가지주요구성요소는다음과같습니다.

- **Exchange ActiveSync** 액세스제어관리**:** XenMobile 과통신하여 XenMobile 에서 Exchange ActiveSync 정책을검색하고이정책을로컬로정의된정책과병합하여 Exchange 에대한액세스가허용또는거부되어야하는 Exchange ActiveSync 장치를결정합니다. 로컬정책을통해 Active Directory 그룹, 사용자, 장치유형또는장치사용자에이전트(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 장치를쿼리하고이러한장치에대한초기화같은제어작업을실행할수있도록웹서비스인터페이스를제공합니다.

시스템요구사항및사전요구사항

다음은 Exchange ActiveSync 용 Endpoint Management 커넥터를사용하는데필요한최소시스템요구사항입니다.

- Windows Server 2016, Windows Server 2012 R2 또는 Windows Server 2008 R2 서비스팩 1. 영어기반서버여야합니다. Windows Server 2008 R2 서비스팩 1 에대한지원은 2020 년 1 월 14 일에종료됩니다.
- Microsoft SQL Server 2016 서비스팩 2 또는 SQL Server 2014 서비스팩 3.
- 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 를사용하도록요구하므로각장치에대해동일한고유 ActiveSync ID 를일관되게생성하는전자메일클라이언트만지원됩니다. 다음과같은전자메일클라이언트는 Citrix 의테스트에서오류없이실행되는것으로확인되었습니다.
  - Samsung 기본전자메일클라이언트
  - iOS 기본전자메일클라이언트
- **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 커넥터가전체포리스트를보도록구성된경우 **Set-AdServerSettings -ViewEntireForest $true** 를실행할수있는권한이부여되어있어야합니다.
  - 제공된자격증명에원격셸을통해 Exchange Server 에연결할수있는권한이있어야합니다. 기본적으로 Exchange 를설치한사용자가이권한을갖습니다.
  - 원격연결을설정하고원격명령을실행하려면원격컴퓨터관리자인사용자에해당하는자격증명이있어야합니다. Set-PSSessionConfiguration 을사용하여관리요구사항을제거할수있지만이명령에대한설명은이문서에나와있지않습니다. 자세한내용은 Microsoft 문서 세션구성정보를참조하십시오.
  - HTTP 를통해원격 PowerShell 요청을지원하도록 Exchange Server 를구성해야합니다. 일반적으로 Exchange Server 에서다음 PowerShell 명령을실행하는관리자이면됩니다. WinRM QuickConfig.
  - Exchange 에는많은제한정책이있습니다. 정책중하나는사용자당허용되는동시 PowerShell 연결수를제어합니다. Exchange 2010 의경우사용자당허용되는동시연결수의기본값은 18 입니다. 연결제한에도달하면, Exchange ActiveSync 용 Endpoint Management 커넥터에서 Exchange Server 에연결할수없습니다. PowerShell 을통해허용되는최대동시연결수를변경하는방법이있지만이문서의범위를벗어나있습니다. 관심있는경우 PowerShell 을통한원격관리와관련된 Exchange 제한정책에대해알아보십시오.

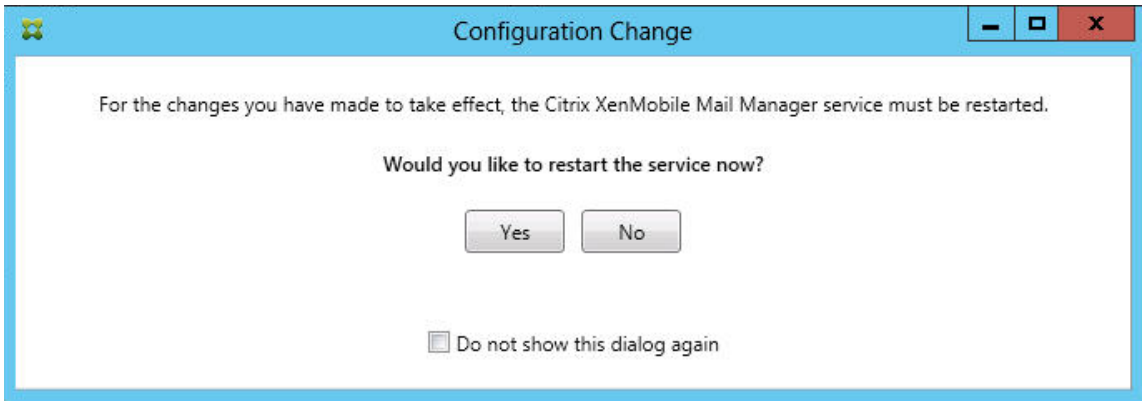
Office 365 Exchange 에대한요구사항

- 권한**:** Exchange 구성 UI 에지정된자격증명으로 Office 365 에연결할수있고다음 Exchange 관련 PowerShell cmdlet 을실행할수있는전체권한이이자격증명에있어야합니다.
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- 권한**:** 제공된자격증명에원격셸을통해 Office 365 서버에연결할수있는권한이있어야합니다. 기본적으로 Office 365 온라인관리자에게는필수권한이있습니다.
- 제한정책**:** Exchange 에는많은제한정책이있습니다. 정책중하나는사용자당허용되는동시 PowerShell 연결수를제어합니다. Office 365 의경우사용자당허용되는동시연결수의기본값은 3 입니다. 연결제한에도달하면, Exchange ActiveSync 용 Endpoint Management 커넥터에서 Exchange Server 에연결할수없습니다. PowerShell 을통해허용되는최대동시연결수를변경하는방법이있지만이문서의범위를벗어나있습니다. 관심있는경우 PowerShell 을통한원격관리와관련된 Exchange 제한정책에대해알아보십시오.

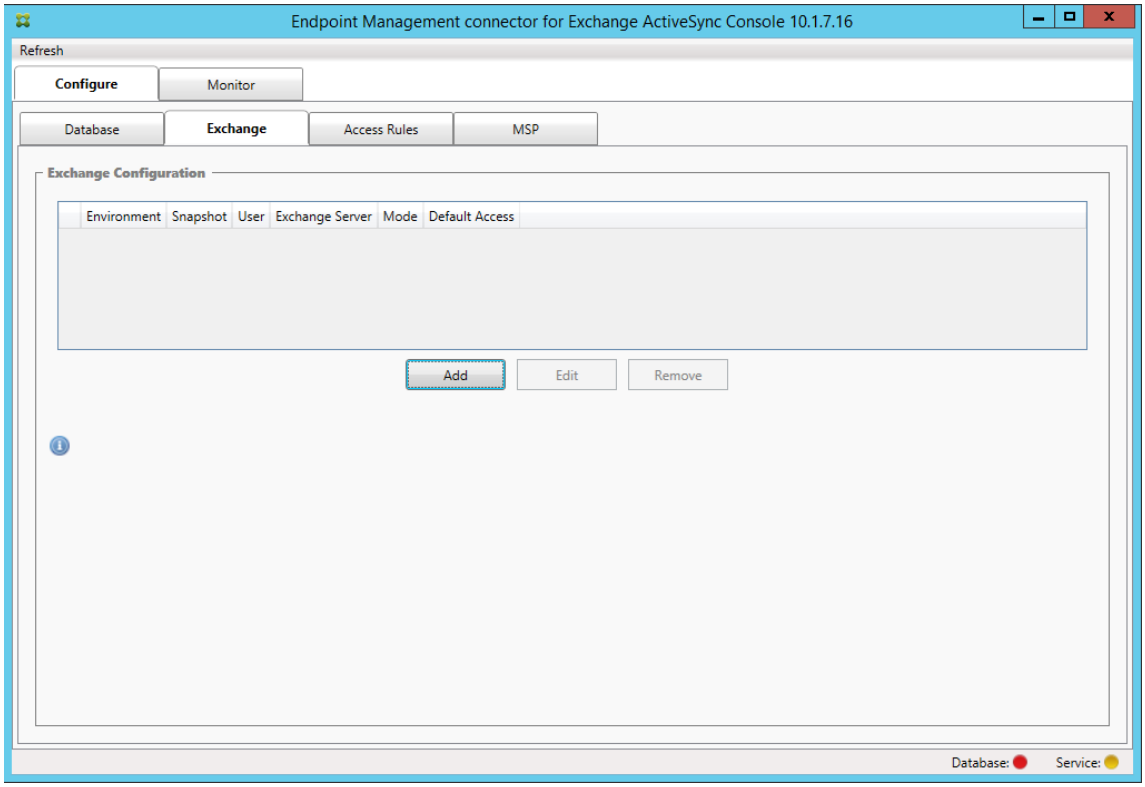
설치및구성

1. XmmSetup.msi 파일을클릭한후설치프로그램의메시지에따라 Exchange ActiveSync 용 Endpoint Management 커넥터를설치합니다.
2. 설치마법사의마지막화면에서 **Launch the Configure utility(**구성유틸리티실행**)** 를선택한상태로둡니다. 또는 **Start(**시작**)** 메뉴에서 Exchange ActiveSync 용 Endpoint Management 커넥터를엽니다.
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**):** 이옵션을선택하는경우 Exchange ActiveSync 용 Endpoint Management 커넥터서비스의로그온자격증명을 SQL Server 액세스권한이있는 Windows 계정으로변경해야합니다. 이렇게하려면 제어판 **>** 관리도구 **>** 서비스를열고 Exchange ActiveSync 용 Endpoint Management 커넥터서비스항목을마우스오른쪽단추로클릭한후 로그온탭을클릭합니다.

   BlackBerry 데이터베이스연결에 Windows 통합을선택하는경우여기서지정하는 Windows 계정에 BlackBerry 데이터베이스액세스권한이있어야합니다.
5. **Test Connectivity(**연결테스트**)** 를클릭하여 SQL Server 에연결되는지확인한후 **Save(**저장**)** 를클릭합니다.
6. 서비스를다시시작하라는메시지가표시됩니다. **Yes(**예**)** 를클릭합니다.



7. 하나이상의 Exchange Server 를구성합니다.
   - 단일 Exchange 환경을관리하는경우단일서버만지정합니다. 여러 Exchange 환경을관리하는경우각 Exchange 환경에하나의 Exchange Server 를지정합니다.
   - **Configure(**구성**) > Exchange** 탭을클릭하고 **Add(**추가**)** 를클릭합니다.

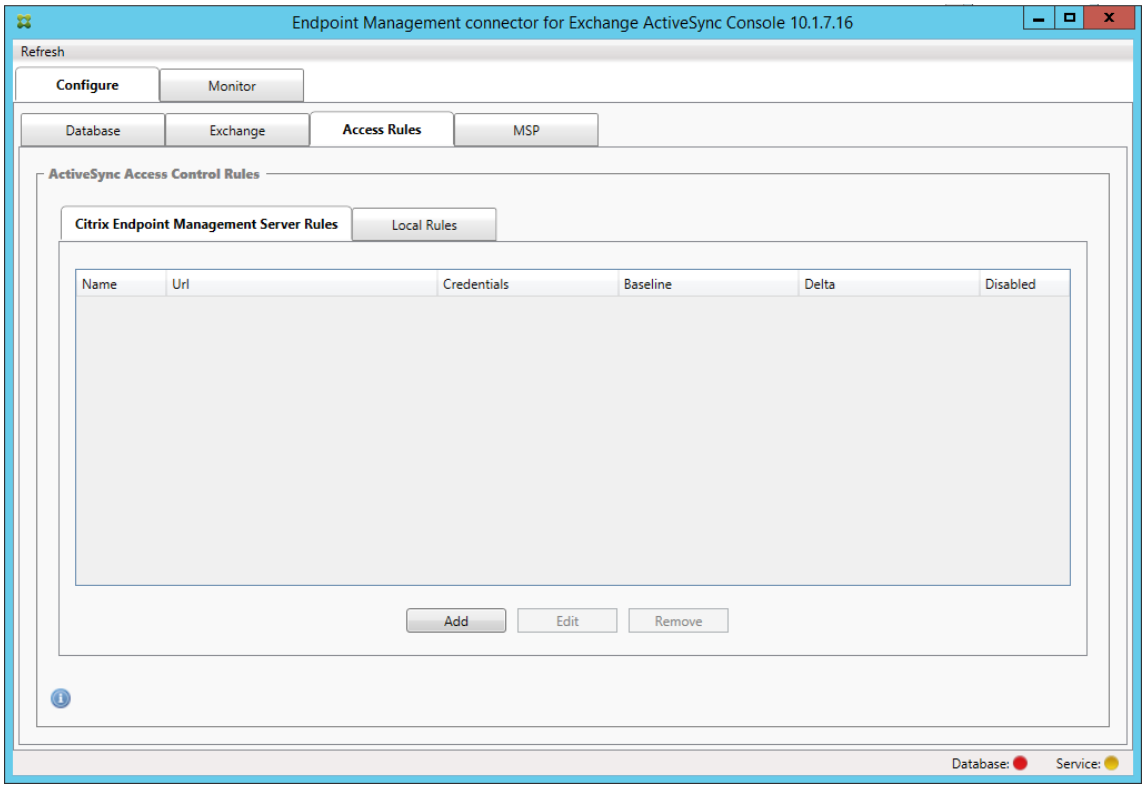


8. Exchange Server 환경유형을 **On Premise**(온프레미스) 또는 **Office 365** 중에서선택합니다.

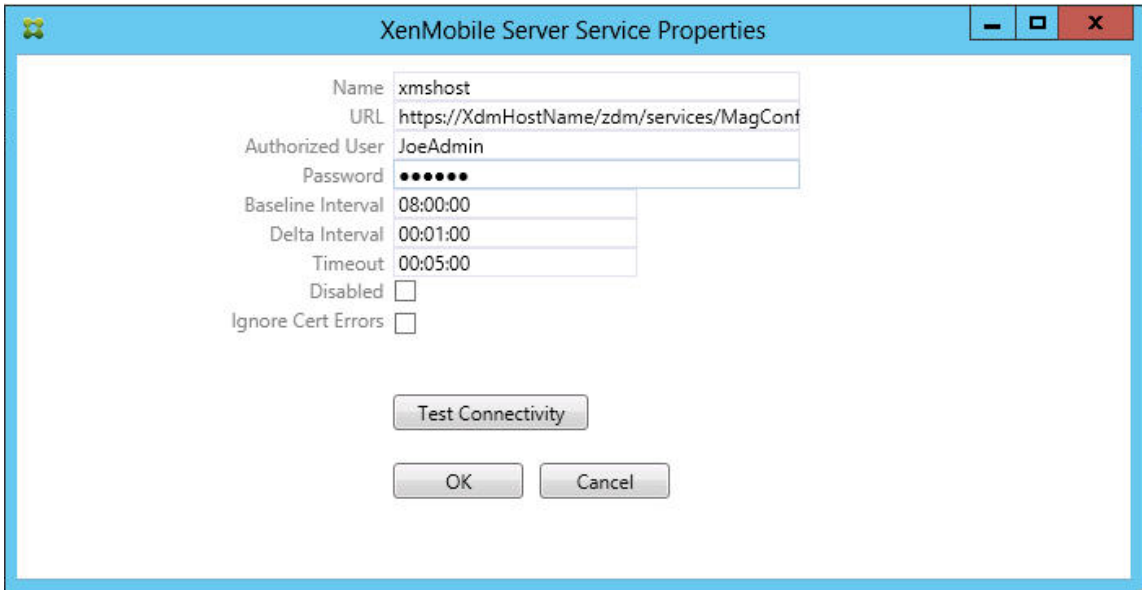
   - **On Premise**(온-프레미스) 를선택하는경우원격 PowerShell 명령에사용할 Exchange Server 의이름을입력합니다.
   - Requirements(요구사항) 섹션에명시된대로적절한 Exchange Server 권한이있는 Windows ID 의 사용자이름을입력하고사용자에대한 암호를입력합니다.
   - 주스냅샷을실행할일정을선택합니다. 주스냅샷은모든 Exchange ActiveSync 파트너관계를검색합니다.
   - 부스냅샷을실행할일정을선택합니다. 부스냅샷은새로생성된 Exchange ActiveSync 파트너관계를검색합니다.
   - 스냅샷유형을 **Deep**(전체) 또는 **Shallow**(단순) 중에서선택합니다. 단순스냅샷은일반적으로훨씬빠르며 Exchange ActiveSync 용 Endpoint Management 커넥터의모든 Exchange ActiveSync 액세스제어기능을수행하기에충분합니다. 전체스냅샷은더긴시간이소요될수있으며 ActiveSync 에대해모바일서비스공급자를사용하는경우에만필요합니다. 이옵션을사용하면 XenMobile 에서관리되지않는장치를쿼리할수있습니다.
   - **Allow**(허용), **Block**(차단) 또는 **Unchanged**(변경되지않음) 중에서기본액세스권한을선택합니다. 이설정은명시적인 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.



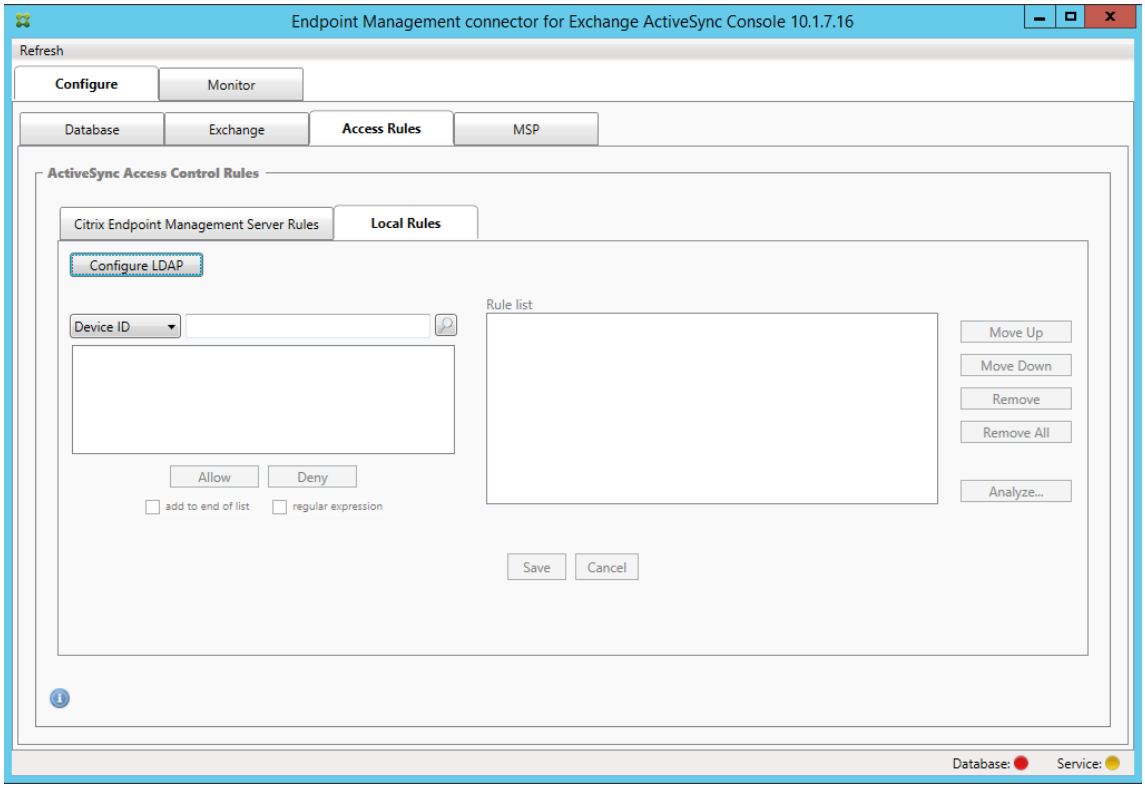
10. **XenMobile server Service Properties(XenMobile** 서버서비스속성**)** 페이지에서 XenMobile Server 를가리키도록 URL 문자열을수정합니다. 예를들어인스턴스이름이 **zdm** 인경우 `https://<XdmHostName>/zdm/services/MagConfigService`를입력합니다. 이예에서는 **XdmHostName** 을 XenMobile Server 의 IP 또는 DNS 주소로바꿉니다.



- 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.

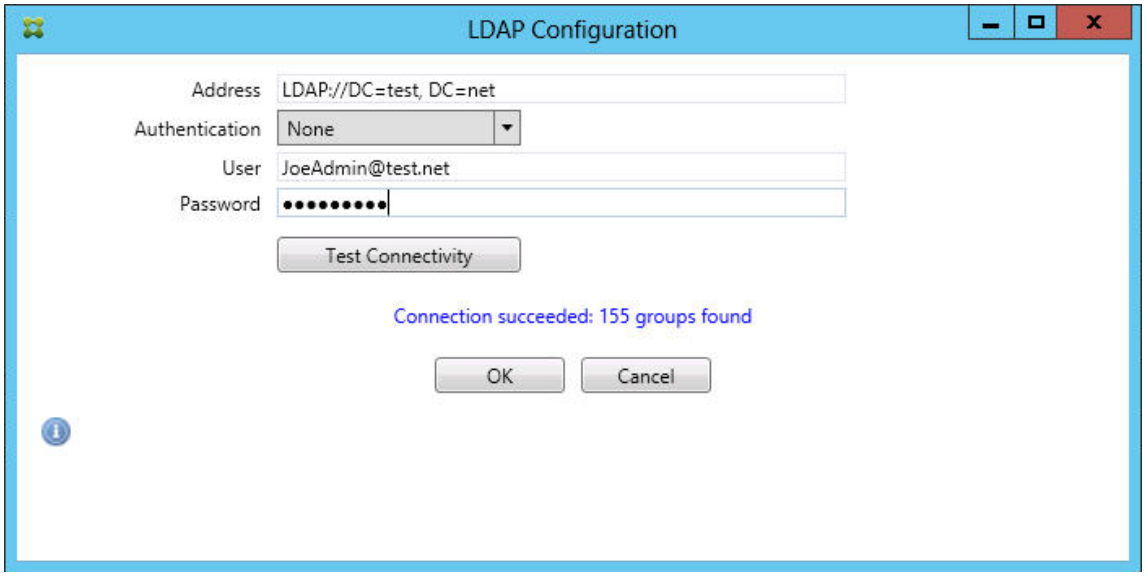


- ActiveSync 장치 ID, 장치유형, AD 그룹, 사용자또는장치 UserAgent 를기준으로로컬규칙을추가할수있습니다. 목록에서해당하는유형을선택합니다.
- 텍스트상자에텍스트또는텍스트부분을입력합니다. 필요한경우쿼리단추를클릭하여부분과일치하는엔터티를봅니다.

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.

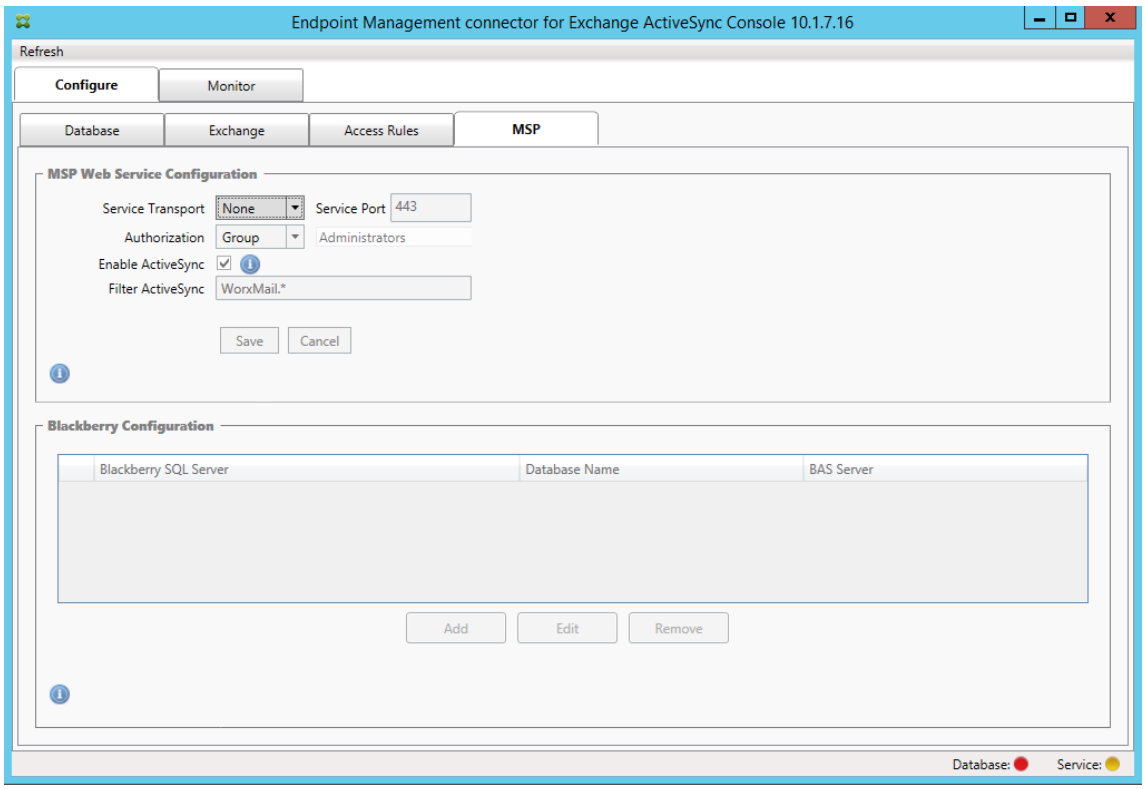
12. Active Directory 그룹에서작동하는로컬규칙을구성하려는경우 **Configure LDAP(LDAP** 구성**)** 를클릭한후 LDAP 연결속성을구성합니다.



13. 모바일서비스공급자를구성합니다.

    모바일서비스공급자는선택사항입니다. 이설정은모바일서비스공급자인터페이스를사용하여관리되지않는장치를쿼리하도록 XenMobile 을구성한경우에만필요합니다.

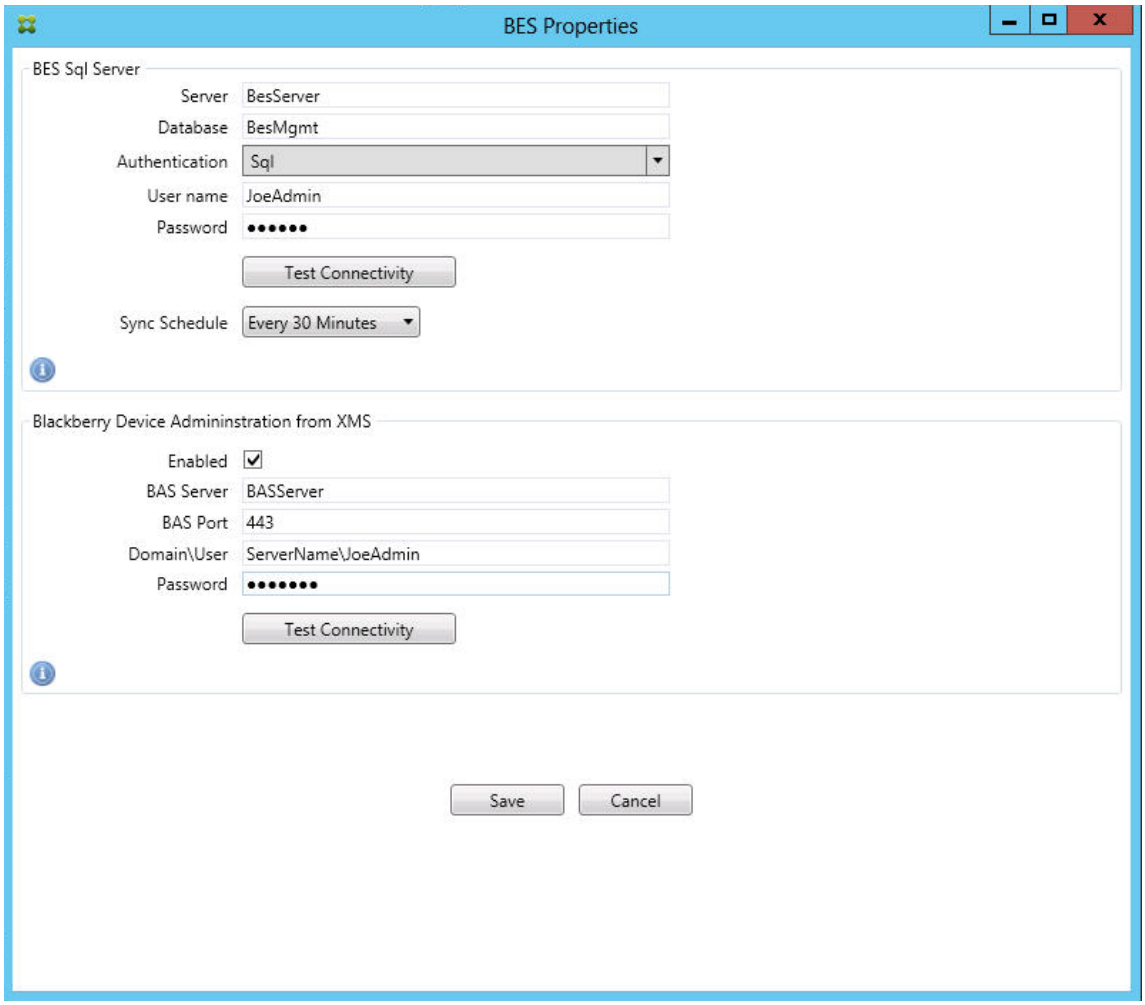
    - **Configure(**구성**) > MSP** 탭을클릭합니다.



    - 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. 이경우스냅샷생성시성능이크게저하될수있습니다.
- 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

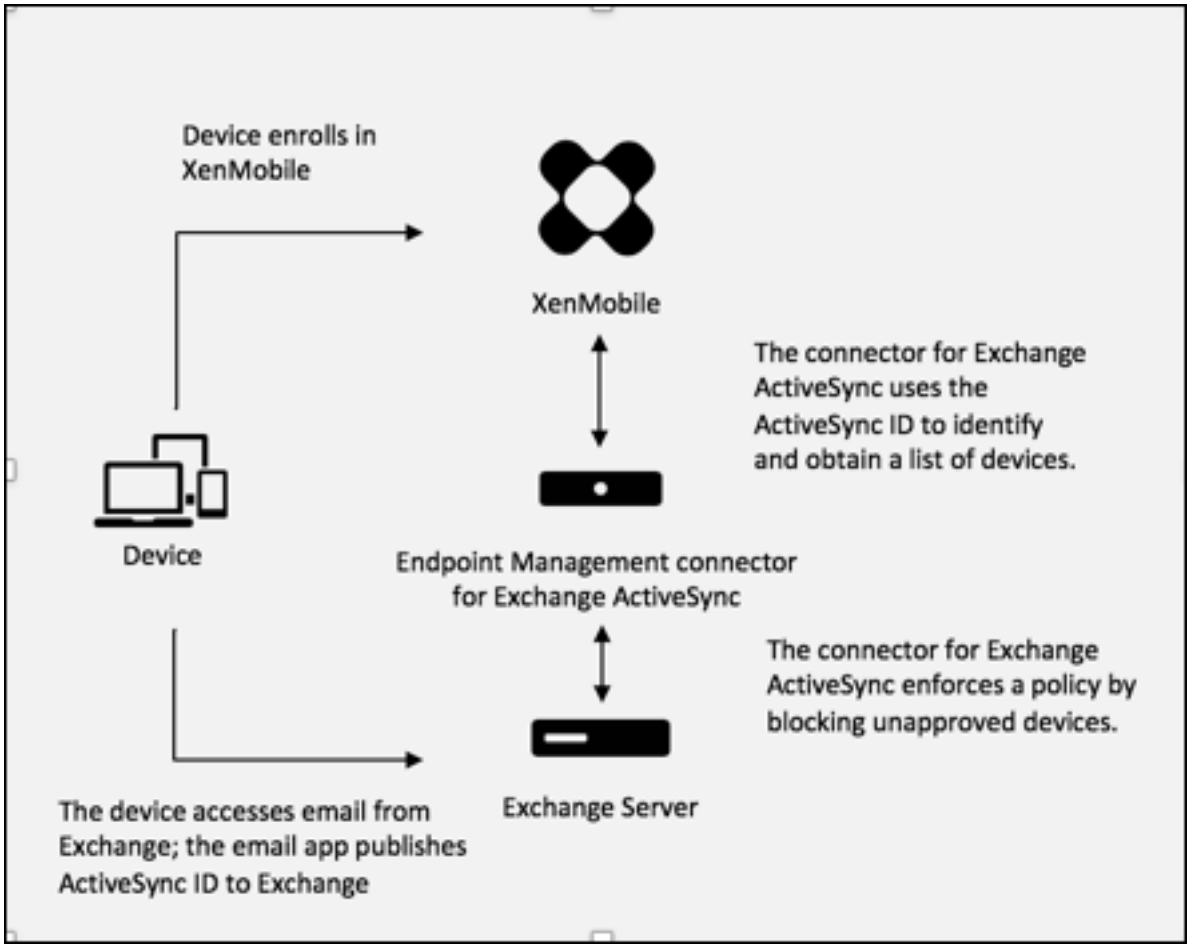
Endpoint Management 커넥터서비스의사용자계정이 BES SQL Server 에연결할때사용되는계정입니다. Exchange ActiveSync 용 Endpoint Management 커넥터데이터베이스연결에대해서도 Windows 통합인증을선택하는경우여기서지정한 Windows 계정에 Exchange ActiveSync 용 Endpoint Management 커넥터데이터베이스에액세스할수있는권한이있어야합니다.

- **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. 이정책을준수하려면직원이그와같은장치에서회사전자메일에액세스할수없도록해야합니다. 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 에알릴수없습니다.

ActiveSync ID 일치는대부분의플랫폼에서안정적으로작동합니다. 하지만일부 Android 구현환경에서장치의 ActiveSync ID 가메일클라이언트가 Exchange 에알리는 ID 와다르다는것이밝혀졌습니다. 이문제를완화하려면다음을수행할수있습니다.

- Samsung SAFE 플랫폼에서는 XenMobile 에서장치 ActiveSync 구성을푸시합니다.

회사전자메일액세스정책이올바르게적용되도록하려면방어적보안입장을채택하고기본적으로거부하는정적정책을설정하여전자메일을차단하도록 Exchange ActiveSync 용 Endpoint Management 커넥터를구성할수있습니다. 즉, 직원이 Android 장치에서전자메일클라이언트를구성하는경우와 ActiveSync ID 검색이제대로작동하지않는경우해당직원의회사전자메일액세스가거부됩니다.

액세스제어규칙

Exchange ActiveSync 용 Endpoint Management 커넥터는 Exchange ActiveSync 장치에대한액세스제어를동적으로구성하는규칙기반접근방식을제공합니다. Exchange ActiveSync 용 Endpoint Management 커넥터액세스제어규칙은일치하는식과원하는액세스상태 (허용또는차단) 의두부분으로구성됩니다. 지정된 Exchange ActiveSync 장치에대해규

칙을평가하여규칙이장치에적용되는지또는장치와일치하는지를결정할수있습니다. 일치하는식에는여러종류가있습니다. 예를들어규칙은지정된장치유형의모든장치또는특정 Exchange ActiveSync 장치 ID 또는특정사용자의모든장치와일치할수있습니다.

규칙목록의규칙을추가, 제거및재정렬하는동안언제든지 **Cancel(**취소**)** 단추를클릭하면처음규칙목록을열었을때의상태로목록이되돌려집니다. **Save(**저장**)** 를클릭하지않고구성도구를닫으면이창에서수행한변경내용이손실됩니다.

Exchange ActiveSync 용 Endpoint Management 커넥터에는로컬규칙, XenMobile Server 규칙 (XDM 규칙이라고도함) 및기본액세스규칙의세가지규칙이있습니다.

로컬규칙**:** 로컬규칙은우선순위가가장높습니다. 로컬규칙에일치하는장치가있을경우규칙평가가중지됩니다. XenMobile Server 규칙또는기본액세스규칙은확인되지않습니다. 로컬규칙은 **Configure(**구성**) > Access Rules(**액세스규칙**) > Local Rules(**로컬규칙**)** 탭을통해 Exchange ActiveSync 용 Endpoint Management 커넥터에로컬로구성됩니다. 지원일치는지정된 Active Directory 그룹내의사용자구성원자격에기반합니다. 지원일치는다음필드에대한정규식에기반합니다.

- ActiveSync Device ID(ActiveSync 장치 ID)
- ActiveSync Device Type(ActiveSync 장치유형)
- User Principal Name (UPN)(UPN(사용자계정이름))
- ActiveSync User Agent(ActiveSync 사용자에이전트)(일반적으로장치플랫폼또는전자메일클라이언트)

주스냅샷이완료되고장치를찾은경우일반또는정규식규칙을추가할수있습니다. 주스냅샷이완료되지않은경우정규식규칙만추가할수있습니다.

XenMobile 서버규칙**:** XenMobile Server 규칙은관리되는장치에대한규칙을제공하는외부 XenMobile Server 에대한참조입니다. XenMobile Server 는 XenMobile 에알려진속성 (예: 장치가탈옥장치인지여부또는장치에금지된앱이포함되었는지여부) 을기반으로장치를허용또는차단된장치로식별하는간략한규칙으로구성될수있습니다. XenMobile 은이간략한규칙을평가하고허용또는차단된 ActiveSync 장치 ID 집합을생성한다음 Exchange ActiveSync 용 Endpoint Management 커넥터에전달합니다.

기본액세스규칙**:** 기본액세스규칙은잠재적으로모든장치와일치할수있고항상마지막에평가된다는것이특징입니다. 이규칙은지정된장치가로컬또는 XenMobile Server 규칙과일치하지않을경우기본액세스규칙의원하는액세스상태가장치의원하는액세스상태를결정하는광범위한규칙입니다.

- **Default Access – Allow(**기본액세스 **-** 허용**):** 로컬또는 XenMobile Server 규칙과일치하지않는모든장치가허용됩니다.
- **Default Access – Block(**기본액세스 **-** 차단**):** 로컬또는 XenMobile Server 규칙과일치하지않는모든장치가차단됩니다.
- **Default Access - Unchanged(**기본액세스 **-** 변경되지않음**):** 로컬또는 XenMobile Server 규칙과일치하지않는모든장치의액세스상태가 Exchange ActiveSync 용 Endpoint Management 커넥터에의해수정되지않습니다. 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 문서 장치액세스제어를참조하십시오.

분석은동일한필드에여러규칙이정의된경우특히유용합니다. 규칙간의관계문제를해결할수있습니다. 분석은규칙필드의관점에서수행됩니다. 예를들어 ActiveSync 장치 ID, ActiveSync 장치유형, 사용자, 사용자에이전트등일치되는필드에기반한그룹으로규칙이분석됩니다.

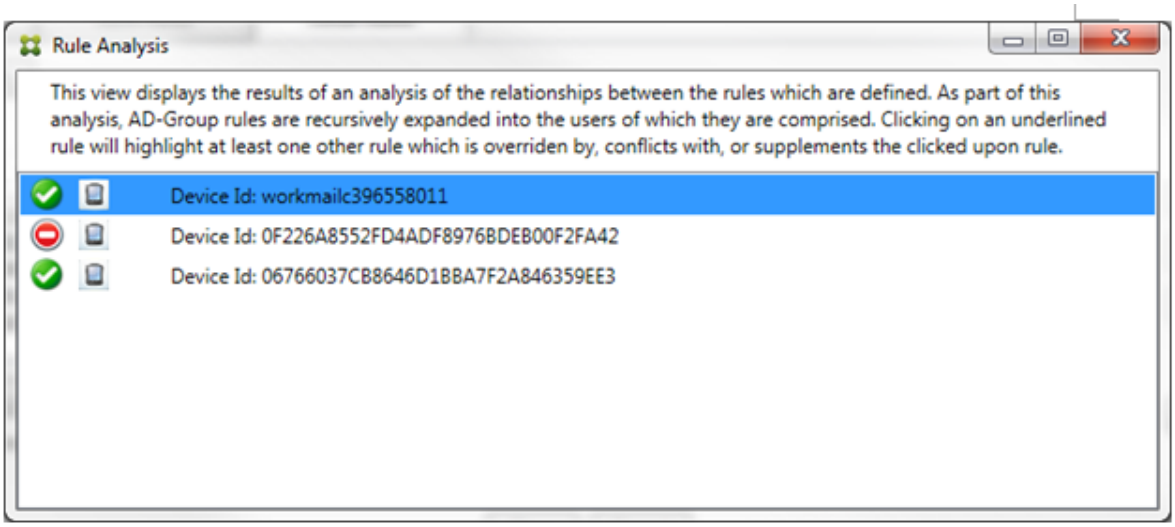
규칙용어

- 재정의규칙**:** 재정의는둘이상의규칙이동일한장치에적용될수있는경우발생합니다. 규칙은목록의우선순위에따라평가되므로적용될수있는마지막의규칙인스턴스가평가되지않을수있습니다.
- 충돌규칙**:** 충돌은둘이상의규칙이동일한장치에적용될수있지만액세스 (허용/차단) 가일치하지않는경우발생합니다. 충돌규칙이정규식규칙이아닌경우충돌은항상암시적으로재정의를의미합니다.
- 보완규칙**:** 보완은둘이상의규칙이정규식규칙이어서둘이상의정규식을하나의정규식규칙으로결합할수있는지, 또는중복되는기능이아닌지를확인해야할때발생합니다. 보완규칙은액세스 (허용/차단) 에서도충돌할수있습니다.
- 주규칙**:** 주규칙은대화상자안에서클릭된규칙입니다. 이규칙은실선테두리로표시됩니다. 또한위또는아래를가리키는녹색화살표가하나또는두개포함됩니다. 화살표가위를가리키는경우주규칙앞에보조규칙이있음을나타냅니다. 화살표가아래를가리키는경우주규칙뒤에보조규칙이있음을나타냅니다. 한번에하나의주규칙만활성화될수있습니다.
- 보조규칙**:** 보조규칙은재정의, 충돌또는추가관계를통해주규칙과관련됩니다. 이규칙은파선테두리로표시됩니다. 각주규칙에대해여러개의보조규칙이있을수있습니다. 밑줄이표시된항목을클릭하면항상주규칙의관점에서보조규칙인규칙이강조표시됩니다. 예를들어보조규칙은주규칙으로재정의되고주규칙과액세스에서충돌하며주규칙을보완합니다.

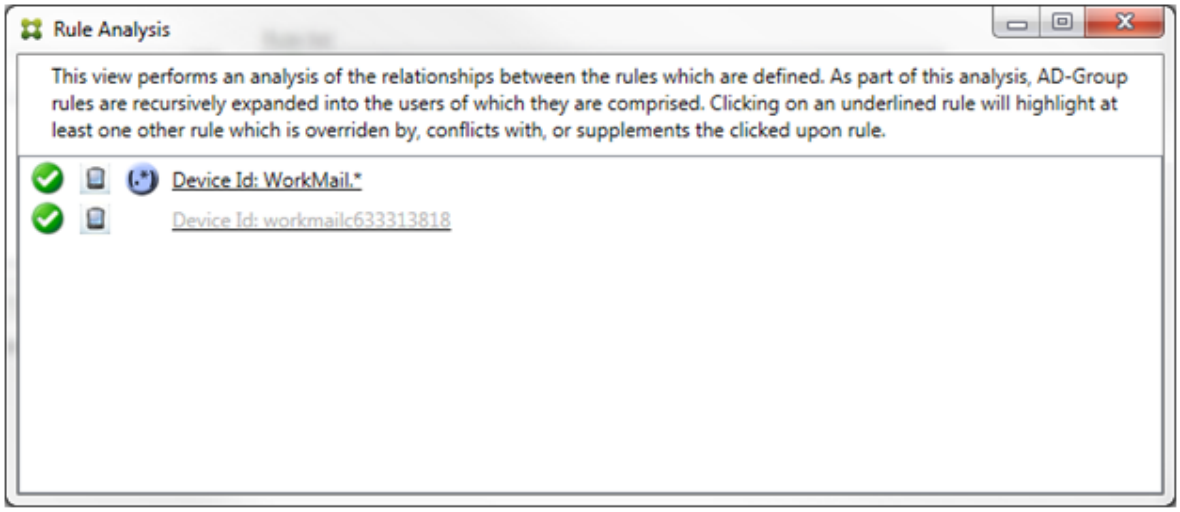
Rule Analysis(규칙분석**)** 대화상자에규칙유형이표시되는방법

충돌, 재정의또는보완이없는경우 Rule Analysis(규칙분석) 대화상자에밑줄이그어진항목이표시되지않습니다. 항목을클릭해도아무런영향이없습니다. 예를들어선택된항목이일반적으로모습으로표시됩니다.

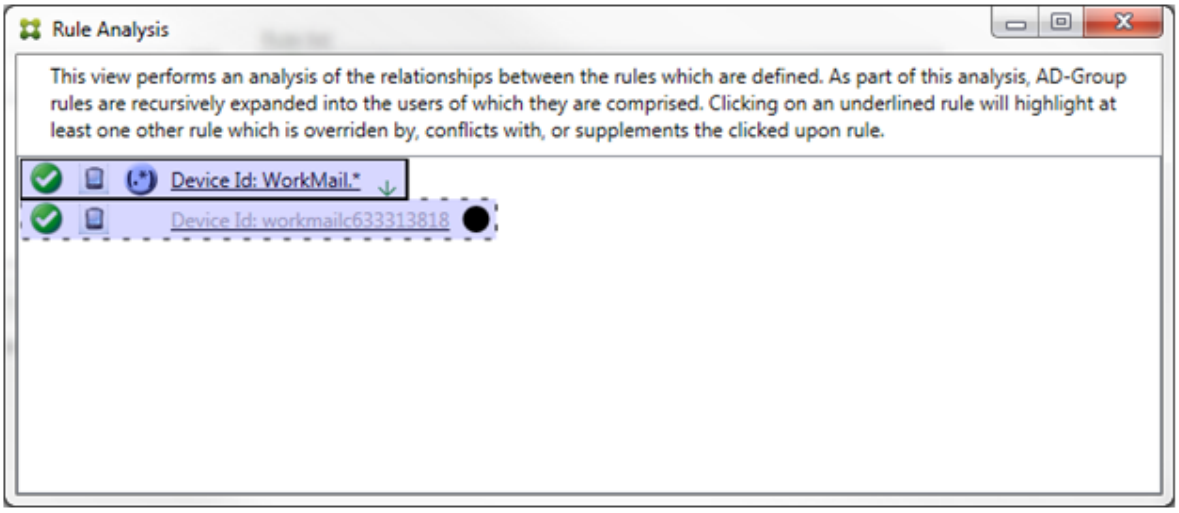
Rule Analysis(규칙분석) 창에는선택할경우충돌, 재정의, 중복또는보완규칙만표시되는확인란이있습니다.



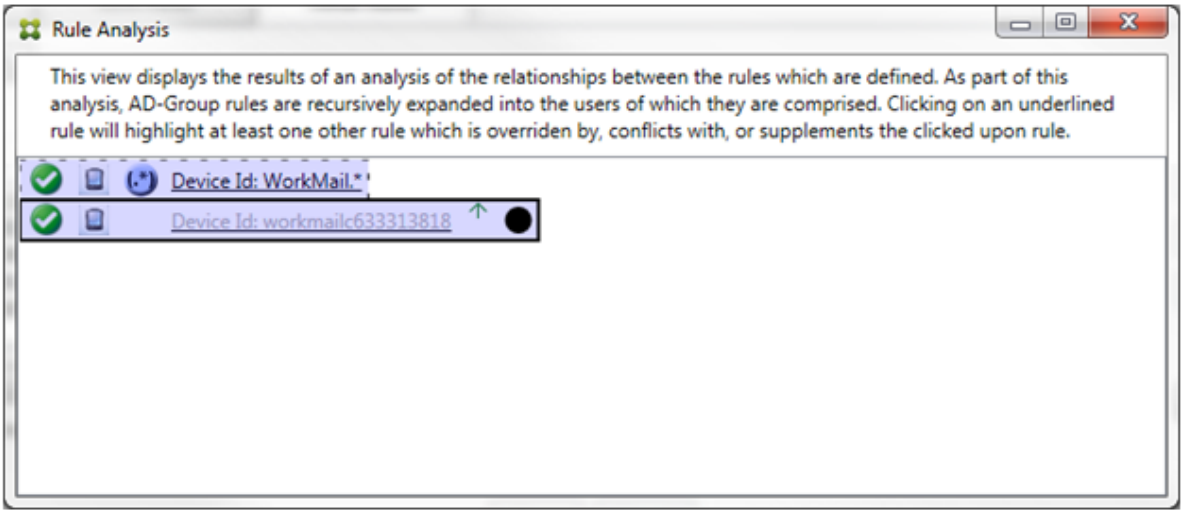
재정의가발생하는경우 2 개이상의규칙 (주규칙과보조규칙) 에밑줄이표시됩니다. 우선순위가더높은규칙으로재정의된하나이상의보조규칙은연한글꼴로표시됩니다. 재정의된규칙을클릭하면해당규칙을재정의한규칙을볼수있습니다. 규칙이주규칙이되거나보조규칙이되어재정의된규칙이강조표시되면그옆에해당규칙이비활성상태임을나타내는검정색원이표시됩니다. 예를들어규칙을클릭하기전에대화상자는다음과같이표시됩니다.



우선순위가가장높은규칙을클릭하면대화상자가다음과같이표시됩니다.

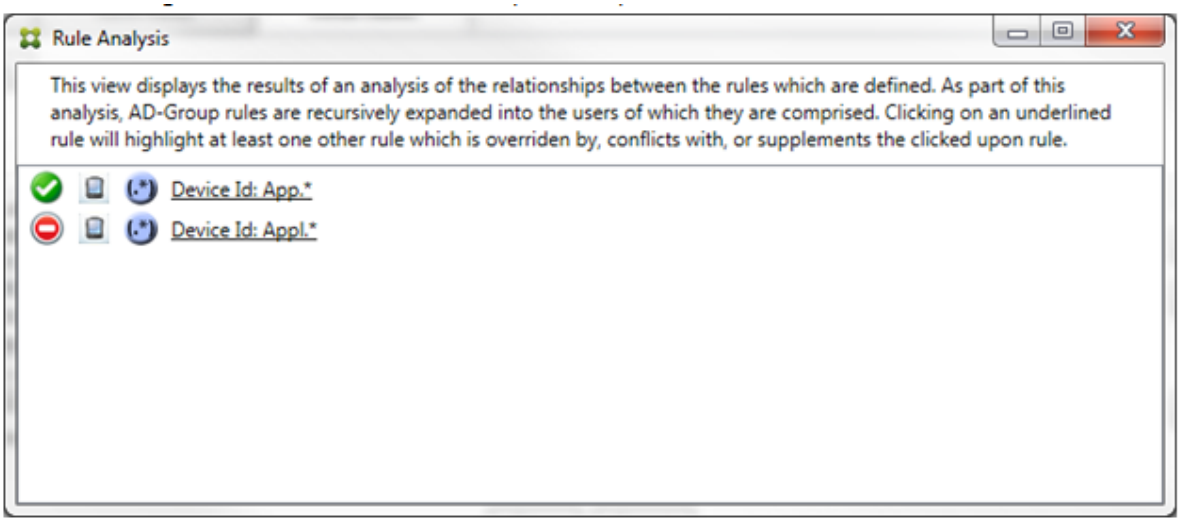


이예에서정규식규칙 `WorkMail.*`는주규칙 (실선테두리로표시됨) 이고일반규칙 `workmailc633313818`은보조규칙 (파선테두리로표시됨) 입니다. 보조규칙옆의검정색점은이규칙보다우선하는더높은우선순위의정규식규칙이있어해당규칙이비활성화 (따라서평가되지않음) 되었음을나타내는시각적표시입니다. 재정의된규칙을클릭한후대화상자는다음과같이표시됩니다.

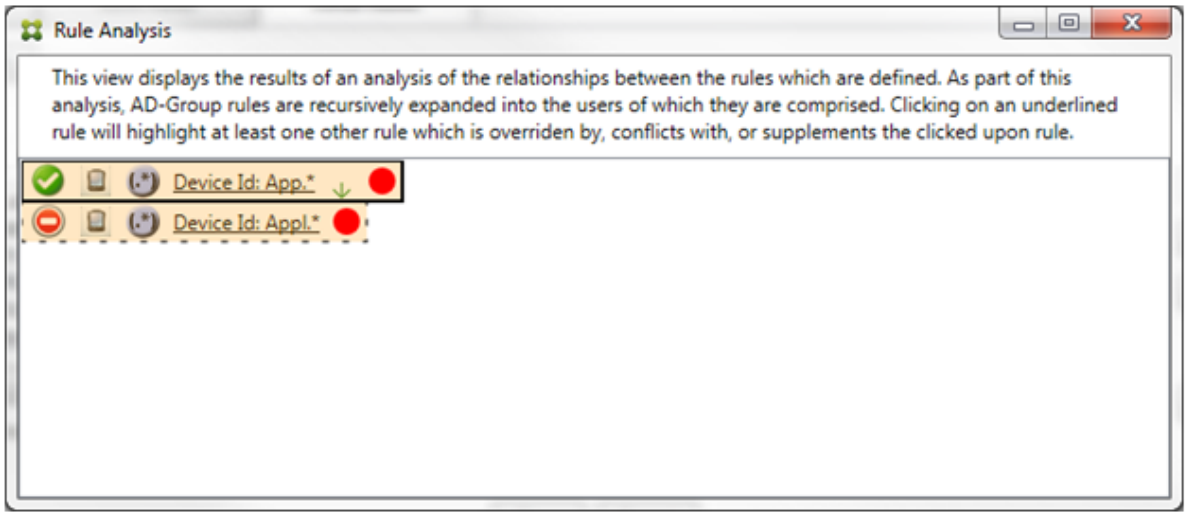


이전예에서정규식규칙 `WorkMail.*`는보조규칙 (파선테두리로표시됨) 이고일반규칙 `workmailc633313818`은주규칙 (실선테두리로표시됨) 입니다. 이단순예제에서는큰차이가없습니다. 더복잡한예제는이항목의뒷부분에나오는복합식예제를참조하십시오. 여러개의규칙이정의된시나리오에서재정의된규칙을클릭하면해당규칙을재정의한규칙을빠르게식별할수있습니다.

충돌이발생하는경우 2 개이상의규칙 (주규칙과보조규칙) 에밑줄이표시됩니다. 충돌하는규칙은빨간색점으로표시됩니다. 서로충돌하는규칙은둘이상의정규식이정의된경우에만가능합니다. 다른모든충돌시나리오에서는충돌이발생하지않으며재정의만발생합니다. 단순예제에서규칙중하나를클릭하기전의대화상자는다음과같이표시됩니다.

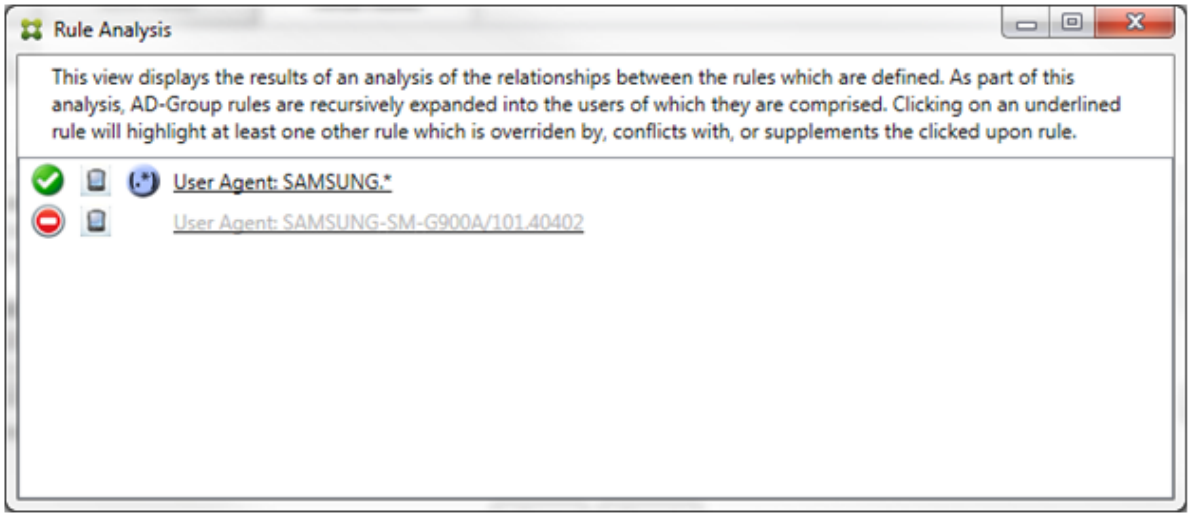


두정규식규칙을검사하면첫번째규칙은장치 ID 에 “App” 이포함된모든장치를허용하고, 두번째규칙은장치 ID 에 “Appl” 이포함된모든장치를거부하는것을알수있습니다. 또한두번째규칙이장치 ID 에 “Appl” 이포함된모든장치를거부하지만허용규칙의우선순위가더높기때문에두번째규칙의조건과일치하는장치가거부되지않습니다. 첫번째규칙을클릭한후대화상자는다음과같이표시됩니다.



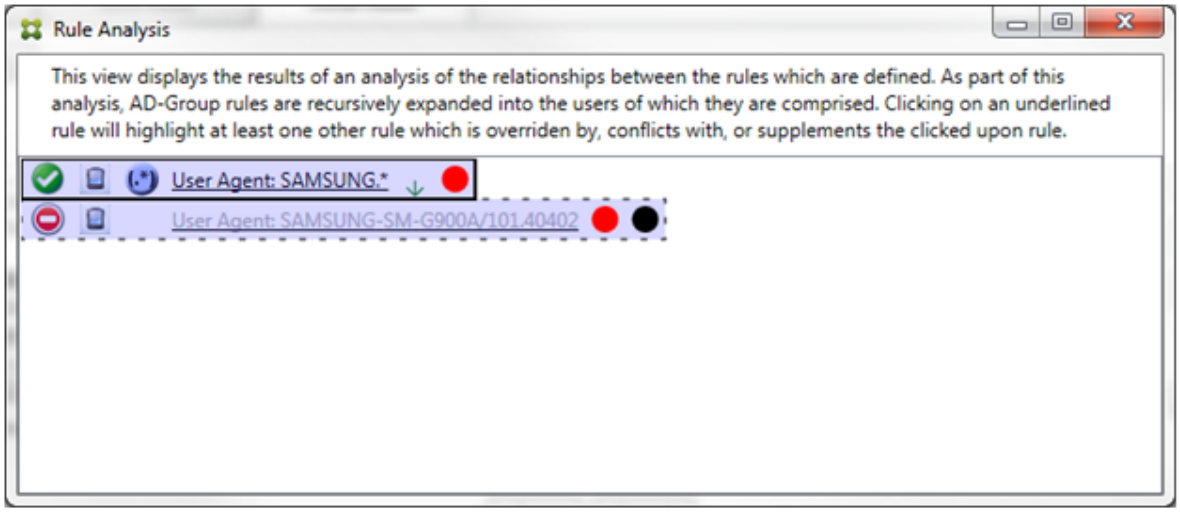
앞의시나리오에서는주규칙 (정규식규칙 `App.*`) 과보조규칙 (정규식규칙 `Appl.*`) 이모두노란색으로강조표시됩니다. 이는둘이상의정규식규칙이단일의일치가능한필드에적용되어중복성문제또는보다심각한문제가발생할수있음을알리는시각적경고입니다.

충돌과재정의가모두발생하는시나리오에서는주규칙 (정규식규칙 `App.*`) 과보조규칙 (정규식규칙 `Appl.*`) 이노란색으로강조표시됩니다. 이는둘이상의정규식규칙이단일의일치가능한필드에적용되어중복성문제또는보다심각한문제가발생할수있음을알리는시각적경고입니다.



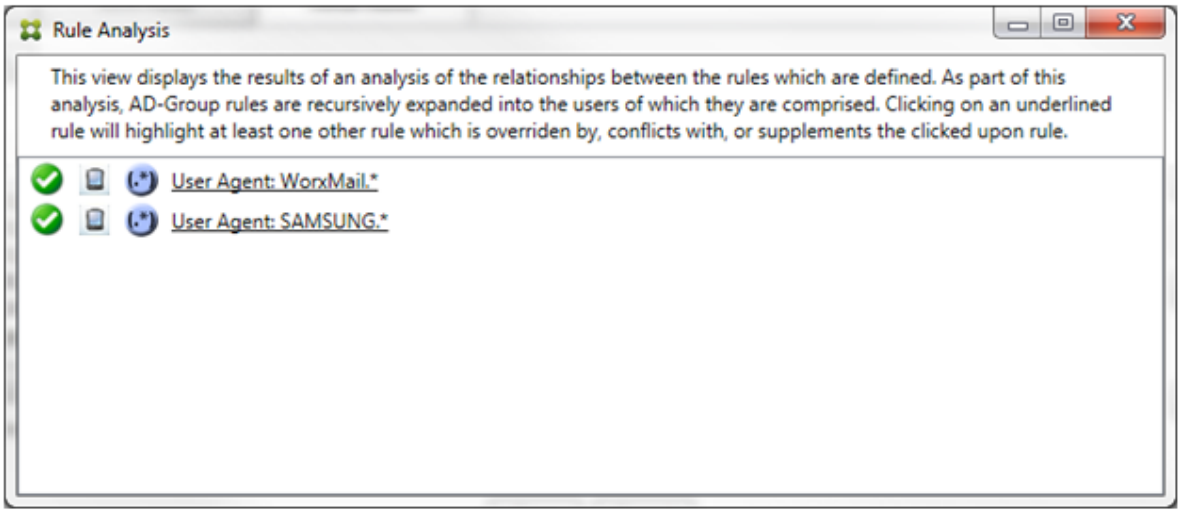
앞의예제에서첫번째규칙 (정규식규칙 `SAMSUNG.*`) 은다음규칙 (일반규칙 `SAMSUNG-SM-G900A/101.40402`) 을재정의할뿐아니라액세스 (주규칙은허용을지정하고보조규칙은차단을지정함) 에서도다르다는것을알수있습니다. 두번째규칙 (일반규칙 `SAMSUNG-SM-G900A/101.40402`) 은재정의되고비활성화되었음을나타내는색이연한텍스트로표시됩니다.

정규식규칙을클릭한후대화상자는다음과같이표시됩니다.

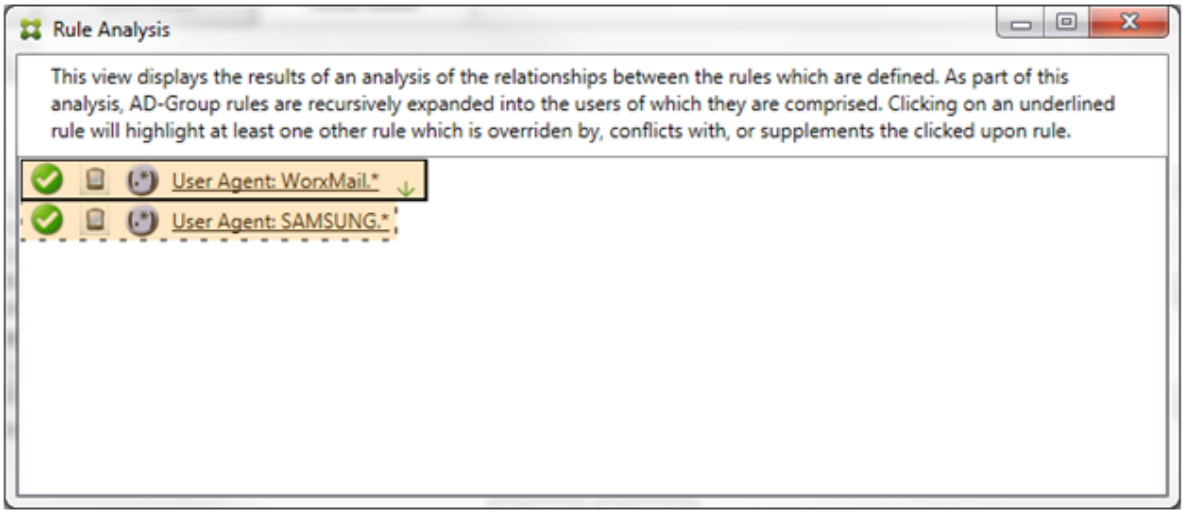


주규칙 (정규식규칙 `SAMSUNG.*`) 뒤에액세스상태가하나이상의보조규칙과충돌함을나타내는빨간색점이표시됩니다. 보조규칙 (일반규칙 `SAMSUNG-SM-G900A/101.40402`) 뒤에액세스상태가주규칙과충돌함을나타내는빨간색점이표시됩니다. 이규칙뒤에는규칙이재정의되었고그로인해비활성화되었음을나타내는검정색점도표시됩니다.

2 개이상의규칙 (주규칙과보조규칙) 에밑줄이표시됩니다. 다른규칙을보완하는규칙에는정규식규칙만포함됩니다. 다른규칙을보완하는규칙은노란색오버레이로표시됩니다. 단순예제에서규칙중하나를클릭하기전의대화상자는다음과같이표시됩니다.



Exchange ActiveSync 용 Endpoint Management 커넥터의 ActiveSync 장치 ID 필드에정규식규칙인두규칙이모두적용된것을쉽게알수있습니다. 첫번째규칙을클릭한후대화상자는다음과같이표시됩니다.

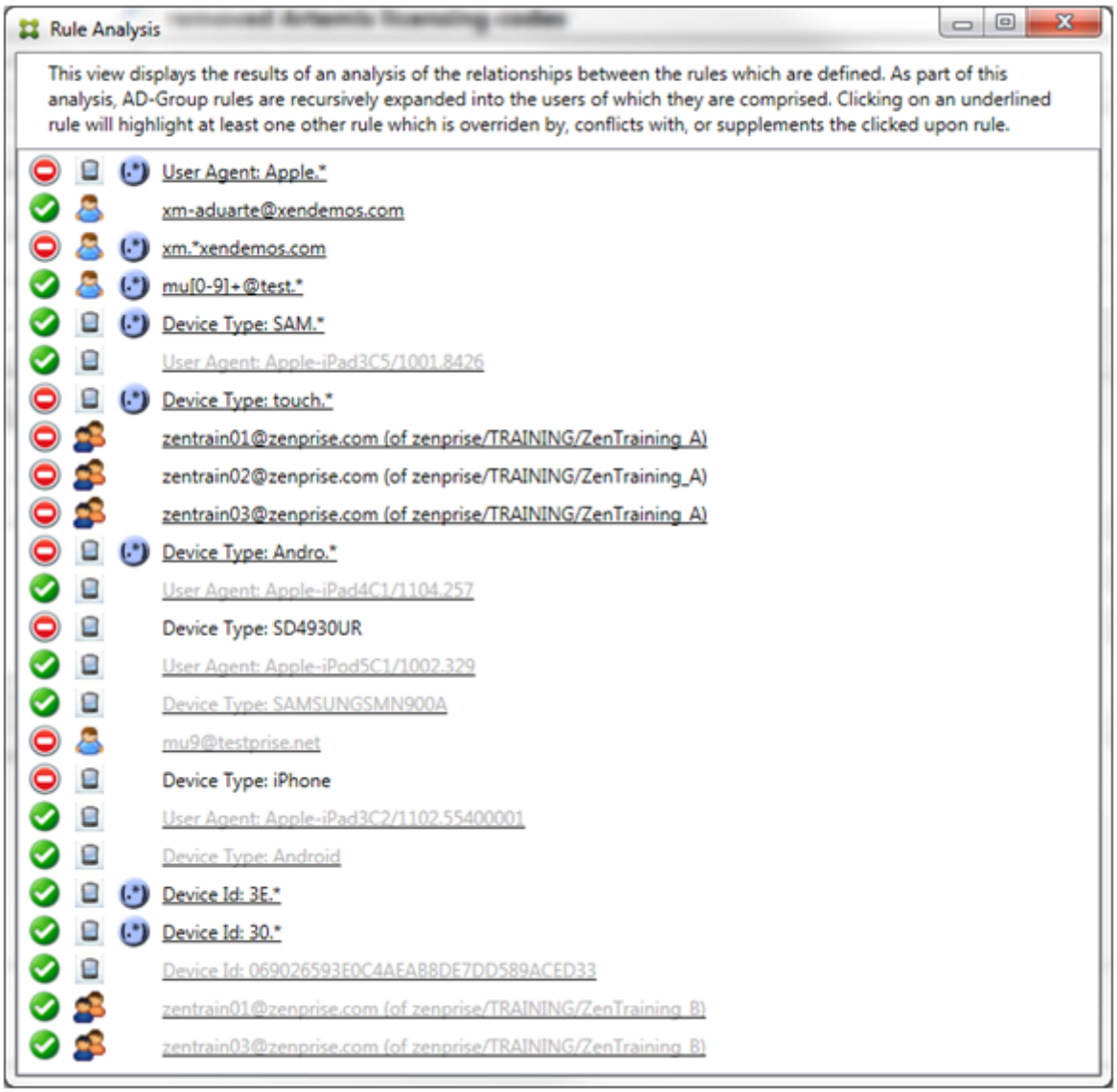


주규칙 (정규식규칙 `WorkMail.*`) 이하나이상의추가보조규칙 (정규식규칙) 이있음을나타내는노란색오버레이로강조표시됩니다. 보조규칙 (정규식규칙 `SAMSUNG.*`) 이 Exchange ActiveSync 용 Endpoint Management 커넥터의동일한필드 (ActiveSync 장치 ID 필드) 에이규칙과주규칙 (모두정규식규칙임) 이적용되고있음을나타내는노란색오버레이로강조표시됩니다. 이경우필드는 ActiveSync 장치 ID 입니다. 정규식은겹치거나겹치지않을수있습니다. 정규식이적절하게작성되었는지여부는직접판단해야합니다.

복합식의예제

재정의, 충돌또는보완이발생할수있는상황은많습니다. 따라서가능한모든시나리오의예를제공하기란불가능합니다. 다음예제에서는하지말아야할사항을설명하고규칙분석의시각적구조가제공하는모든기능을설명합니다. 다음그림에는항목의대부분에밑줄이표시되어있습니다. 문제의규칙이우선순위가더높은규칙으로재정의되었음을나타내는연한글꼴로렌더링된항목이많습니다.

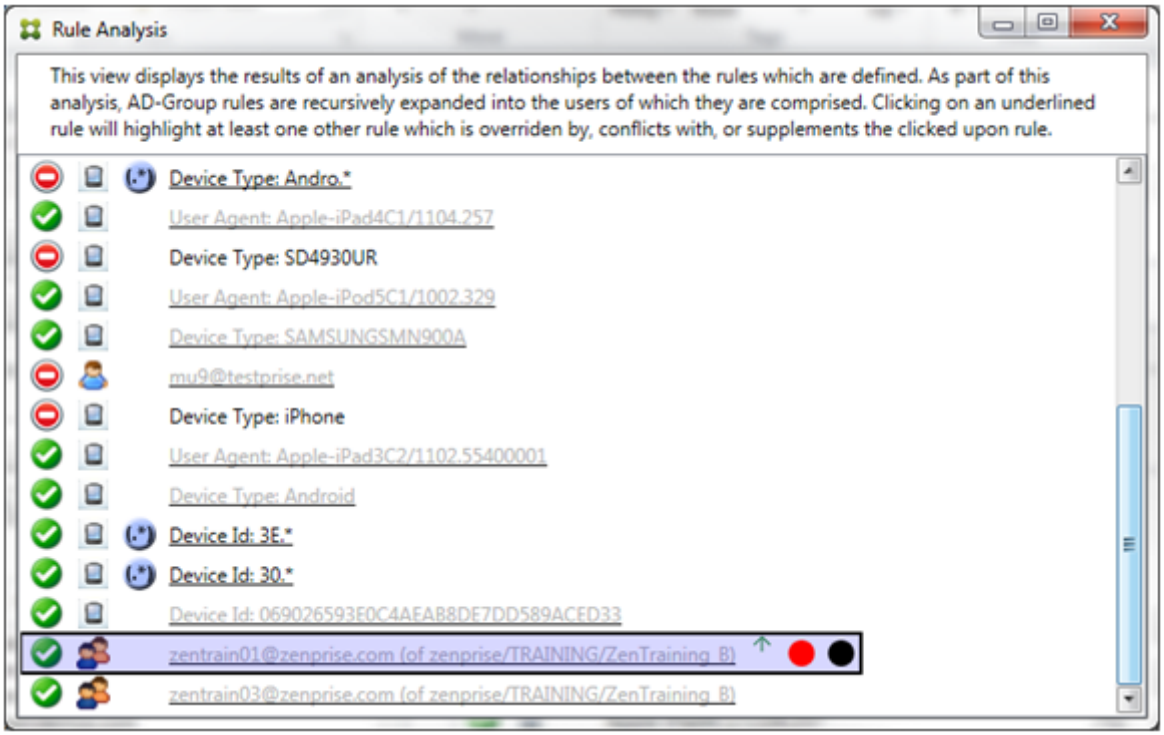

아이콘으로표시되는정규식규칙의수도목록에포함되어있습니다.



재정의를분석하는방법

특정규칙을재정의한규칙을보려면규칙을클릭합니다.

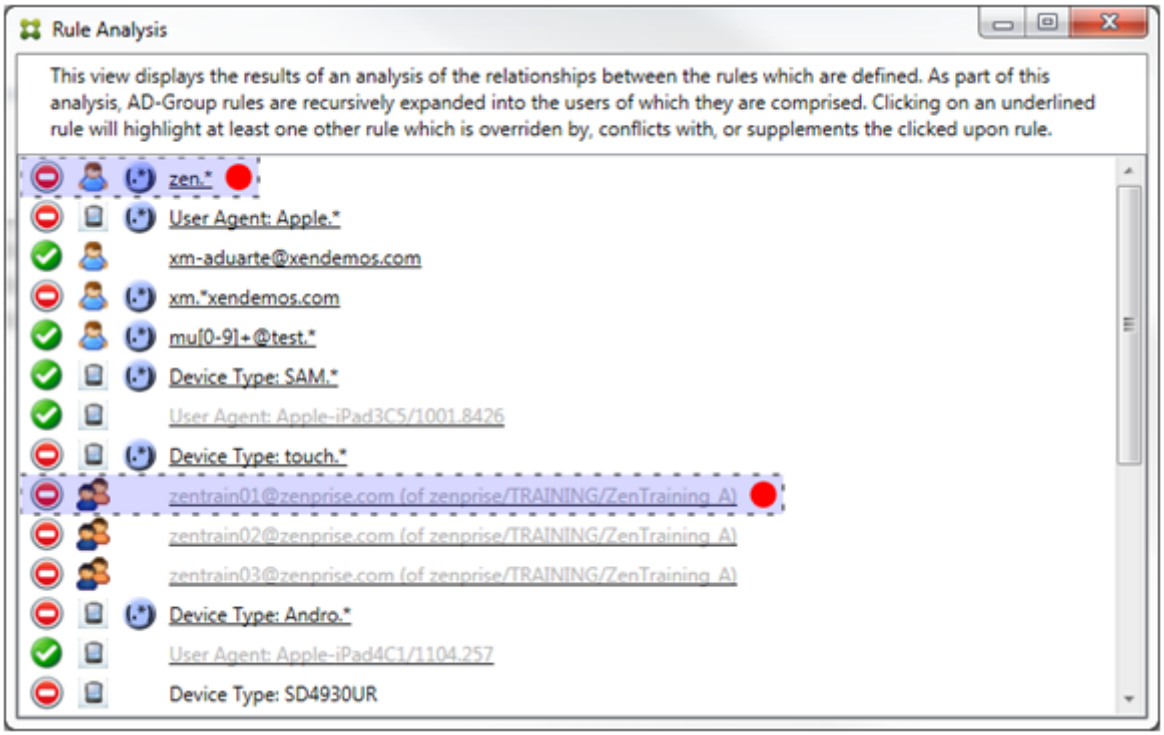
예제 **1**: 이예제에서는 `zentrain01@zenprise.com`이재정의된이유를검사합니다.



주규칙 (AD 그룹규칙 `zenprise/TRAINING/ZenTraining B`, 여기서 `zentrain01@zenprise.com`은구성원임) 의특징은다음과같습니다.

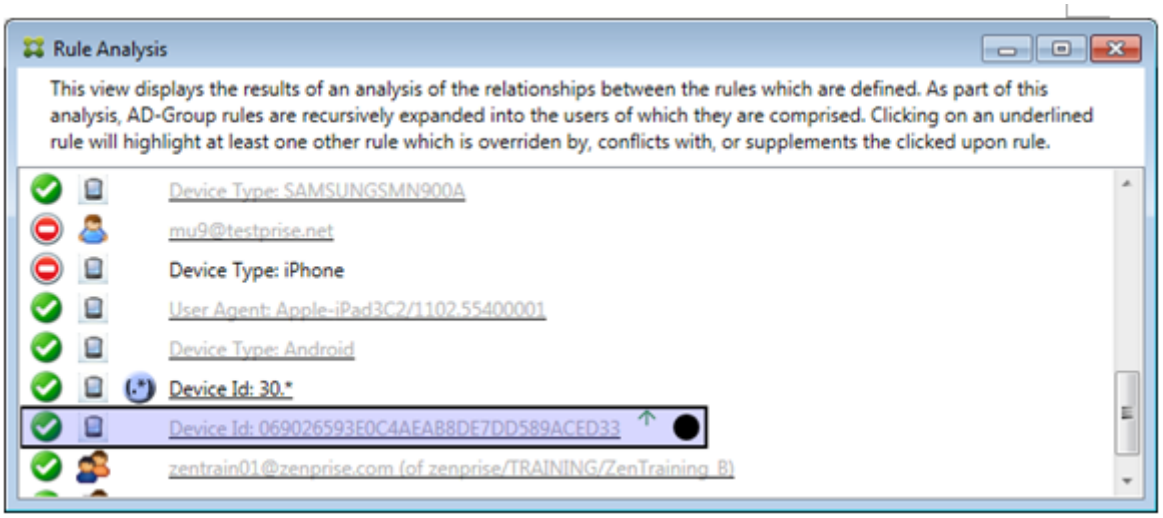
- 파란색으로강조표시되고실선테두리가포함되어있습니다.
- 위쪽을가리키는녹색화살표가있습니다 (위에보조규칙이있음을나타냄).
- 각각하나이상의보조규칙과액세스상태가충돌하고, 주규칙으로재정의되어비활성화되었음을나타내는빨간색원과검정색원이뒤에있습니다.

위로스크롤하면다음이표시됩니다.



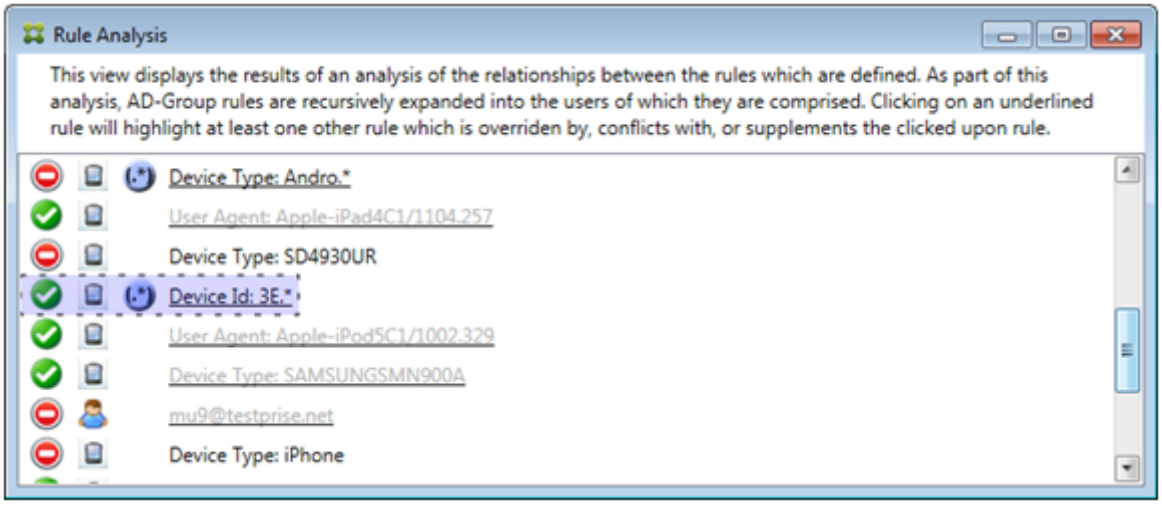
이 예 에 서 는 정 규 식 규 칙 인 `zen.*`과 일 반 규 칙 인 `zentrain01@zenprise.com`(`zenprise/TRAINING/ZenTraining A`) 의 보 조 규 칙 2 개 가 주 규 칙 을 재 정 의 합 니 다 . 두 번 째 보 조 규 칙 에 서 는 Active Directory 그 룹 규 칙 `ZenTraining A`에 사 용 자 `zentrain01@zenprise.com`이 포 함 되 고 Active Directory 그 룹 규 칙 `ZenTraining B`에도사용자 `zentrain01@zenprise.com`이포함됩니다. 그러나보조규칙이주규칙보다우선순위가높기때문에주규칙이재정의되었습니다. 주규칙의액세스는허용이고두보조규칙의액세스는차단이므로액세스가충돌함을나타내는빨간색원이뒤에표시됩니다.

예제 **2**: 이예제에서는 ActiveSync 장치 ID 가 `069026593E0C4AEAB8DE7DD589ACED33`인장치가재정의된이유를보여줍니다.



주규칙 (일반장치 ID 규칙 `069026593E0C4AEAB8DE7DD589ACED33`) 의특징은다음과같습니다.

- 파란색으로강조표시되고실선테두리가포함되어있습니다.
- 위쪽을가리키는녹색화살표가있습니다 (위에보조규칙이있음을나타냄).
- 주규칙이보조규칙으로재정의되어비활성화되었음을나타내는검정색원이뒤에표시되어있습니다.

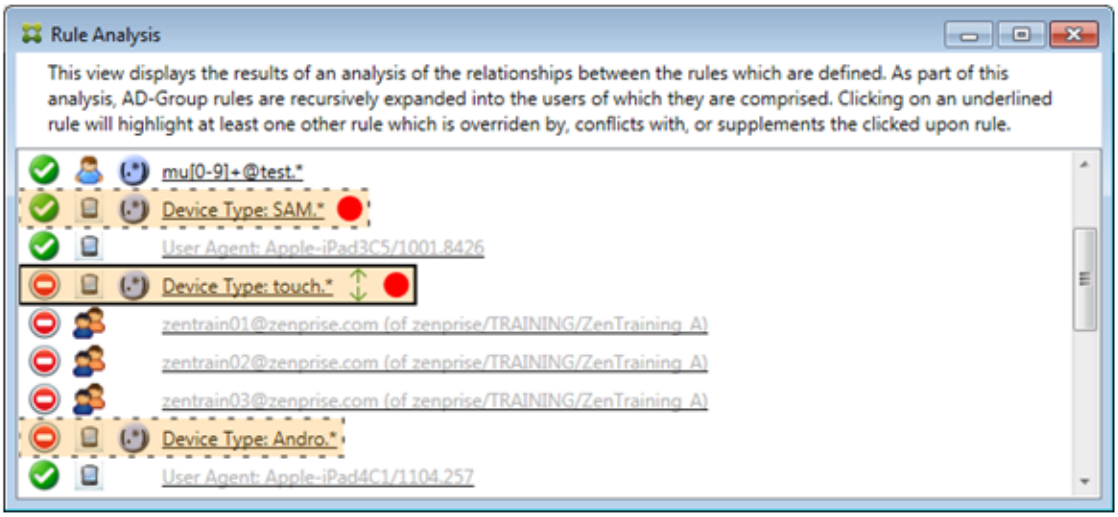


이예에서는단일의보조규칙이주규칙을재정의합니다. 정규식 ActiveSync 장치 ID 규칙은 `3E.*`입니다. 정규식 `3E.*`가 `069026593E0C4AEAB8DE7DD589ACED33`과일치하므로주규칙이평가되지않습니다.

보완및충돌을분석하는방법

이예에서기본규칙은정규식 ActiveSync 장치유형규칙인 `touch.*`입니다. 특징은다음과같습니다.

- 특정규칙필드 (이예에서는 ActiveSync 장치유형) 에둘이상의정규식규칙이작동함을나타내는경고로노란색오버레이가실선테두리와함께표시되어있습니다.
- 각각위쪽과아래쪽을가리키는두개의화살표가있습니다 (우선순위가높은보조규칙과우선순위가낮은보조규칙이 1 개이상있음을나타냄).
- 액세스상태가허용으로설정되어주규칙의액세스상태인차단과충돌하는보조규칙이 1 개이상임을나타내는빨간색원이옆에표시되어있습니다.
- 정규식 ActiveSync 장치유형규칙 `SAM.*` 및정규식 ActiveSync 장치유형규칙 `Andro.*`의보조규칙 2 개가있습니다.
- 두보조규칙은보조규칙임을나타내는파선테두리로표시되어있습니다.
- 두보조규칙에는 ActiveSync 장치유형규칙필드에도적용됨을나타내는노란색오버레이가표시되어있습니다.
- 이러한시나리오에서는정규식규칙이중복되지않는지확인해야합니다.



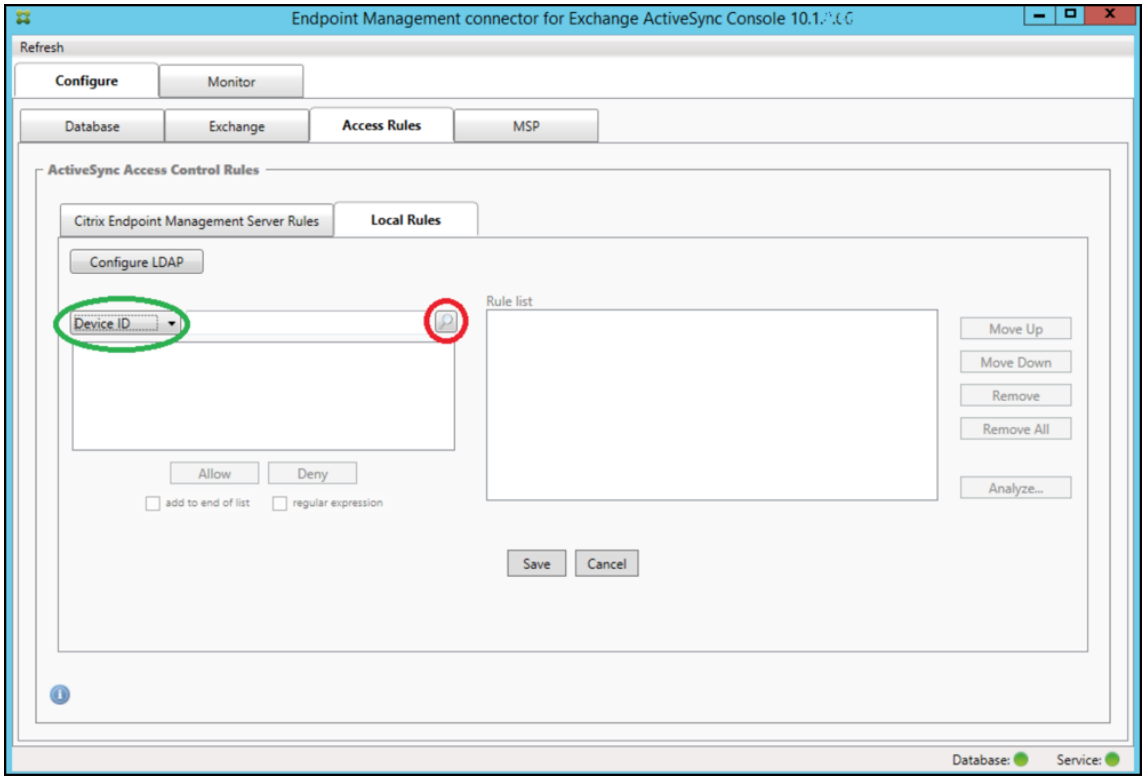
규칙을추가로분석하는방법

이예제에서는규칙관계가항상주규칙의관점에서파생된다는점을설명합니다. 앞의예제에서는정규식규칙클릭이값이 `touch.*`인장치유형의필드에적용되는방법을보여줬습니다. 보조규칙 `Andro.*`를클릭하면다른보조규칙집합이강조표시됩니다.

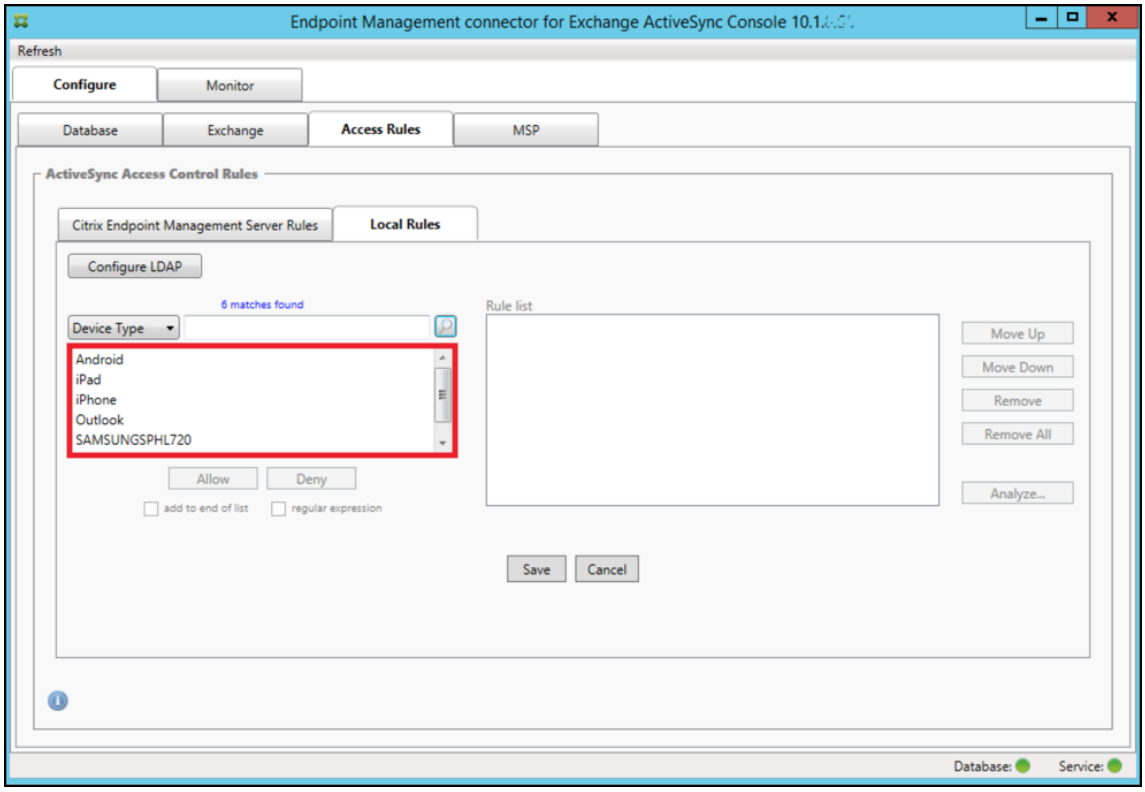
이예제는규칙관계에포함된재정의된규칙을보여줍니다. 이규칙은일반 ActiveSync 장치유형규칙인 `Android`이며재정의 (연한글꼴로표시되고검정색원이표시됨) 되었으며주규칙인정규식 ActiveSync 장치유형규칙 `Andro.*`와액세스상태가충돌합니다. 이규칙은클릭하기전에보조규칙이었습니다. 앞의예에서일반 ActiveSync 장치유형규칙 `Android`는보조규칙으로표시되지않았습니다. 주규칙 (정규식 ActiveSync 장치유형규칙 `touch.*`) 의관점에서주규칙과관련되지않았기때문입니다.

일반식로컬규칙을구성하려면

1. **Access Rules(**액세스규칙**)** 탭을클릭합니다.



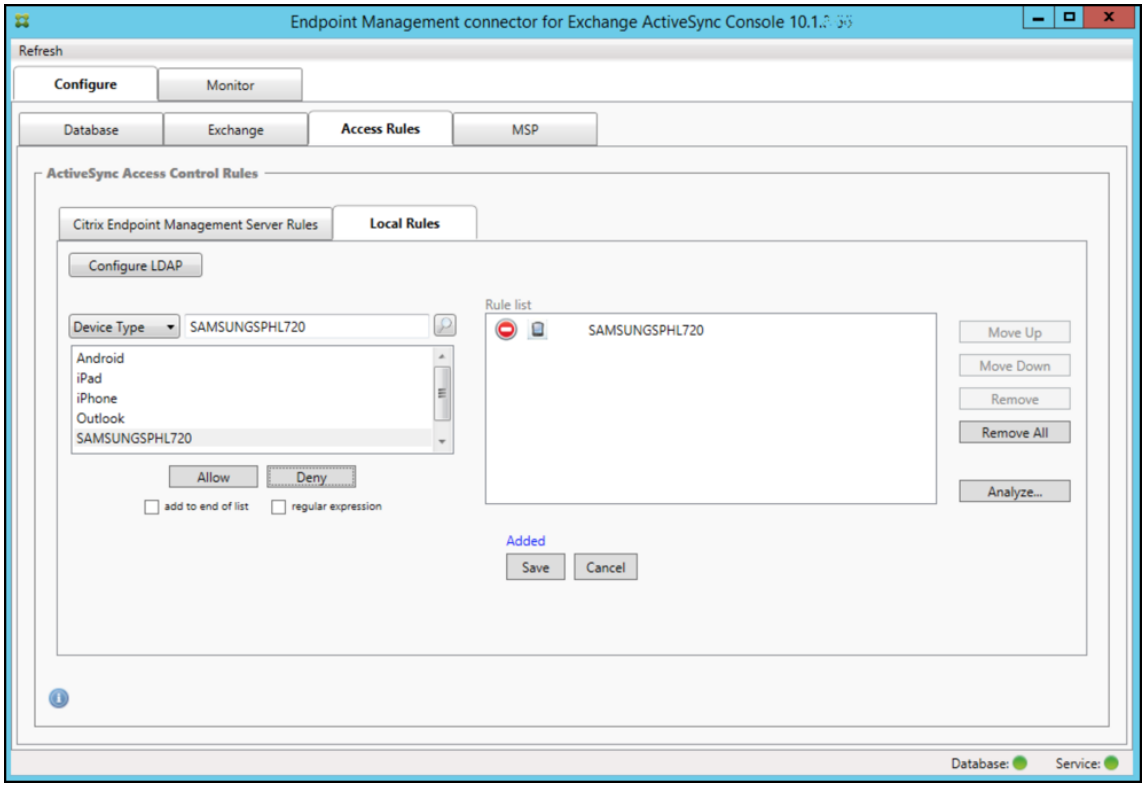
2. **Device ID(**장치 **ID)** 목록에서로컬규칙을만들필드를선택합니다.
3. 돋보기아이콘을클릭하여선택한필드의모든고유한일치항목을표시합니다. 이예제에서는 **Device Type(**장치유형**)** 필드가선택되었고목록상자아래에선택항목이표시되어있습니다.



4. 결과목록상자에서항목하나를클릭하고다음옵션중하나를클릭합니다.

   - **Allow(**허용**)** 을클릭하면일치하는모든장치의 ActiveSync 트래픽을허용하도록 Exchange 가구성됩니다.
   - **Deny(**거부**)** 을클릭하면일치하는모든장치의 ActiveSync 트래픽을거부하도록 Exchange 가구성됩니다.

   이예에서는장치유형이 SamsungSPhl720 인모든장치의액세스가거부됩니다.



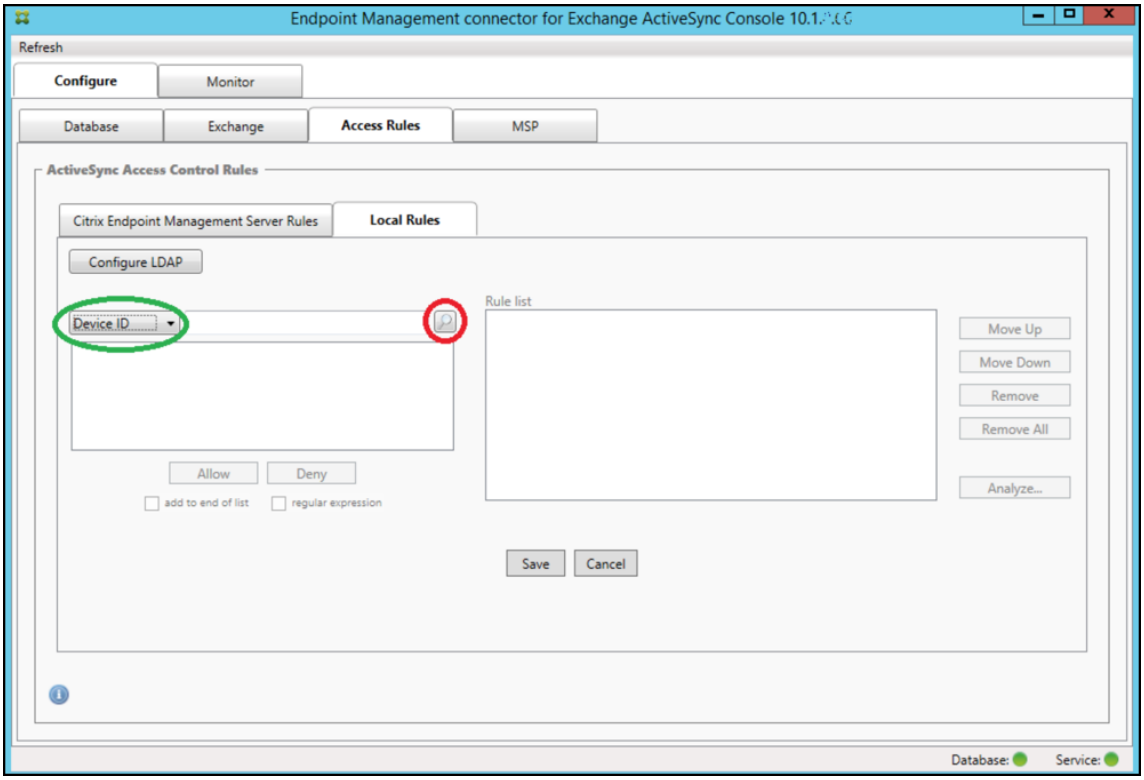
정규식을추가하려면

정규식로컬규칙은옆에표시되는  아이콘으로구분할수있습니다.

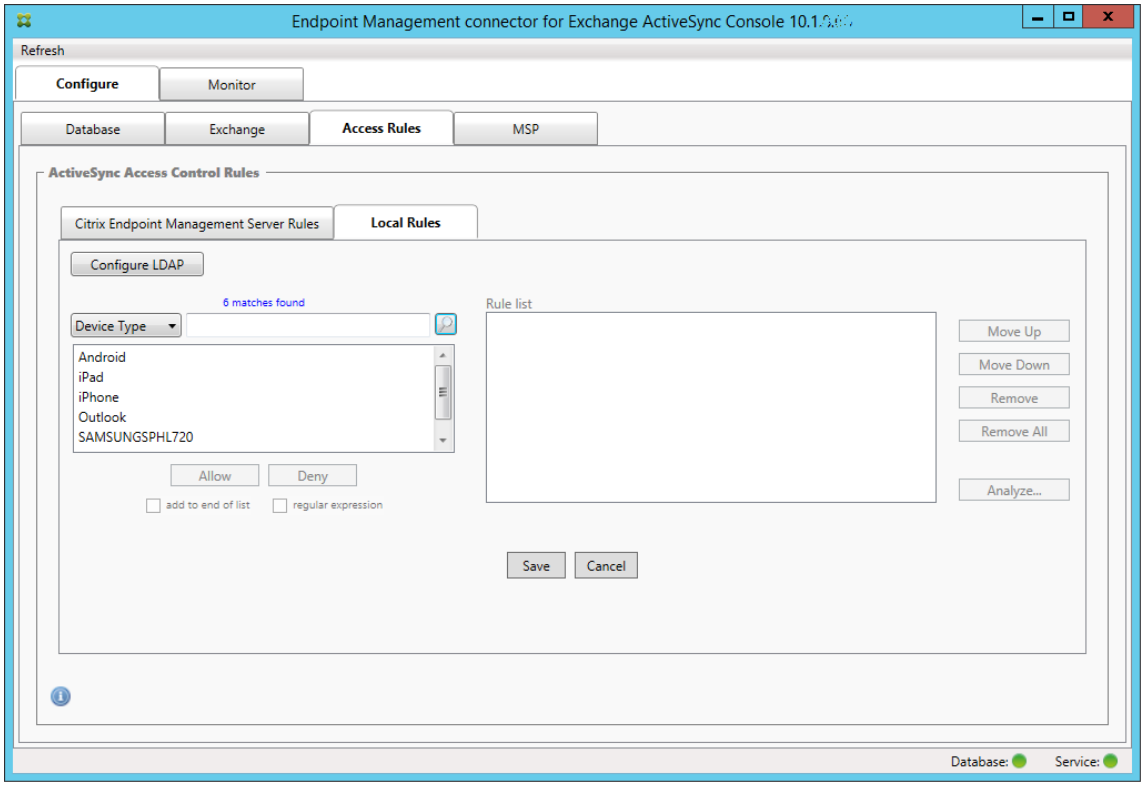
정규식규칙을추가하려면지정된필드에대한결과목록의기존값을사용하여정규식규칙을작성하거나 (주스냅샷이완료되어야함) 원하는정규식을입력하면됩니다.

기존필드값에서정규식을작성하려면

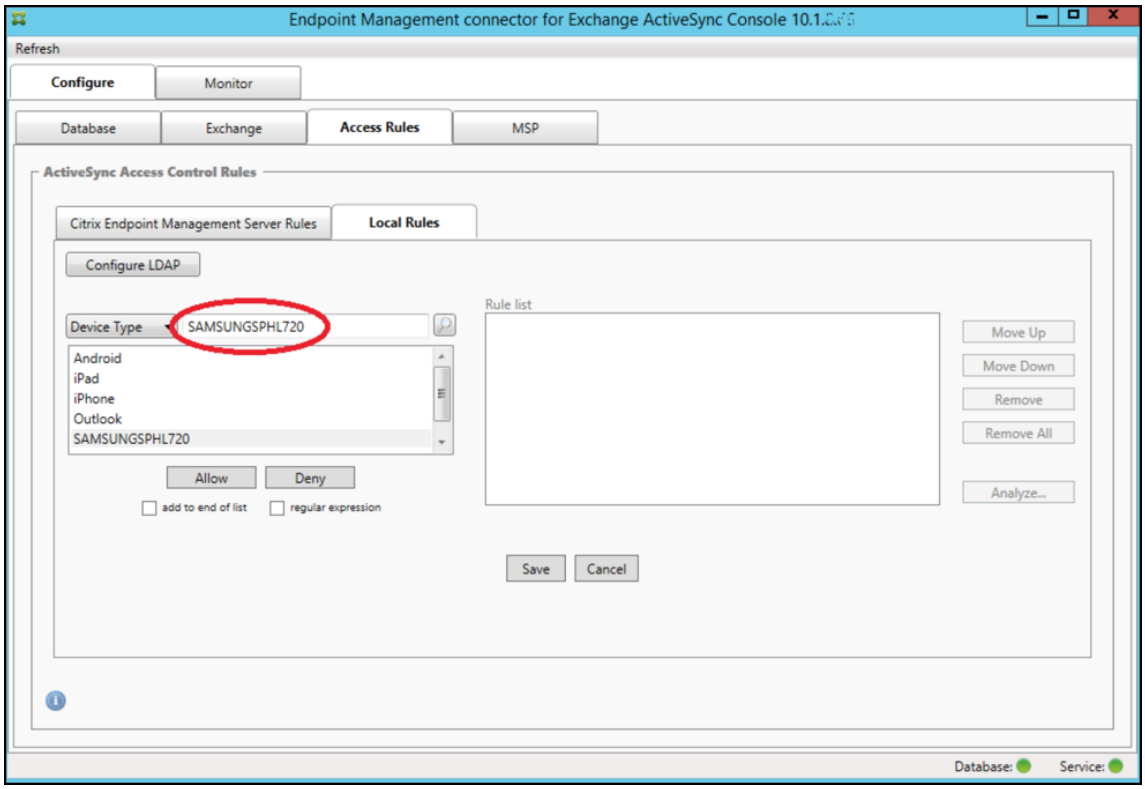
1. **Access Rules(**액세스규칙**)** 탭을클릭합니다.



2. **Device ID(**장치 **ID)** 목록에서정규식로컬규칙을만들필드를선택합니다.
3. 돋보기아이콘을클릭하여선택한필드의모든고유한일치항목을표시합니다. 이예제에서는 **Device Type(**장치유형**)** 필드가선택되었고목록상자아래에선택항목이표시되어있습니다.



4. 결과목록에서항목중하나를클릭합니다. 이예제에서는 **SAMSUNGSPHL720** 이선택되었고 **Device Type(**장치유형**)** 옆의텍스트상자에표시되어있습니다.



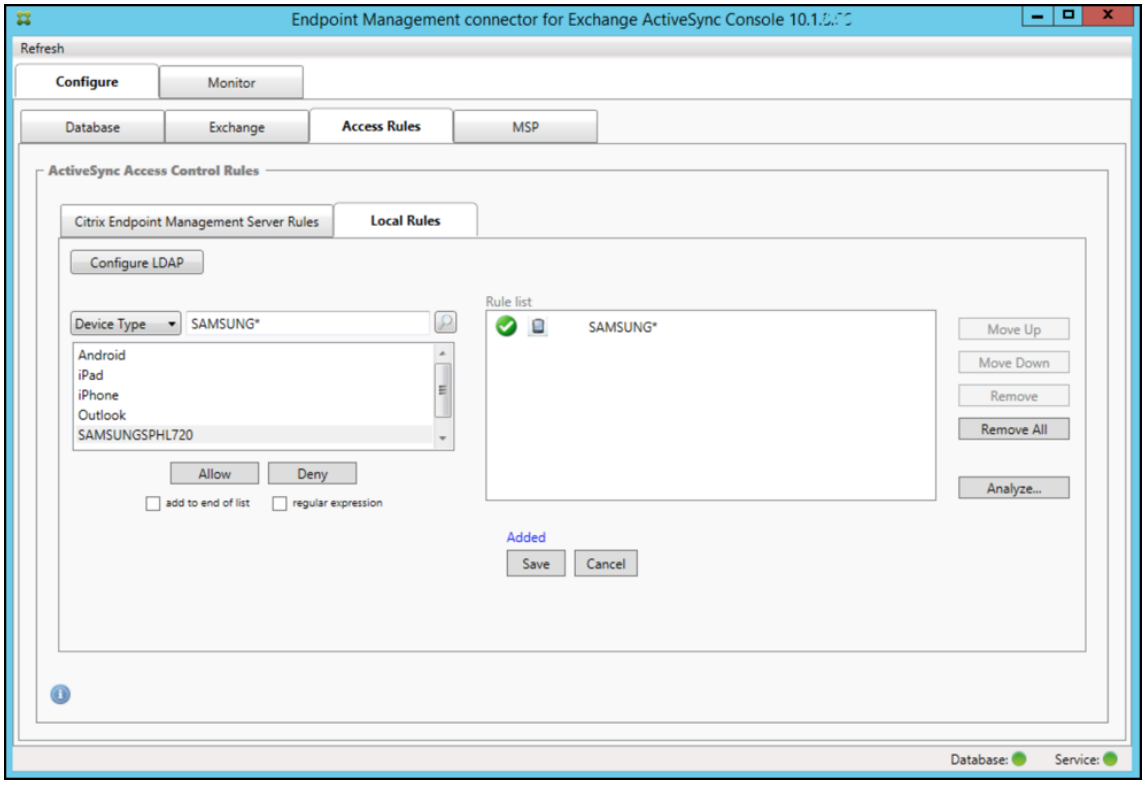
5. 장치유형값에 “Samsung” 이포함되는모든장치유형을허용하려면다음단계에따라정규식규칙을추가합니다.

   a) 선택한항목텍스트상자안쪽을클릭합니다.

   b) 텍스트를 **SAMSUNGSPHL720** 에서다음으로변경합니다. **SAMSUNG.***.

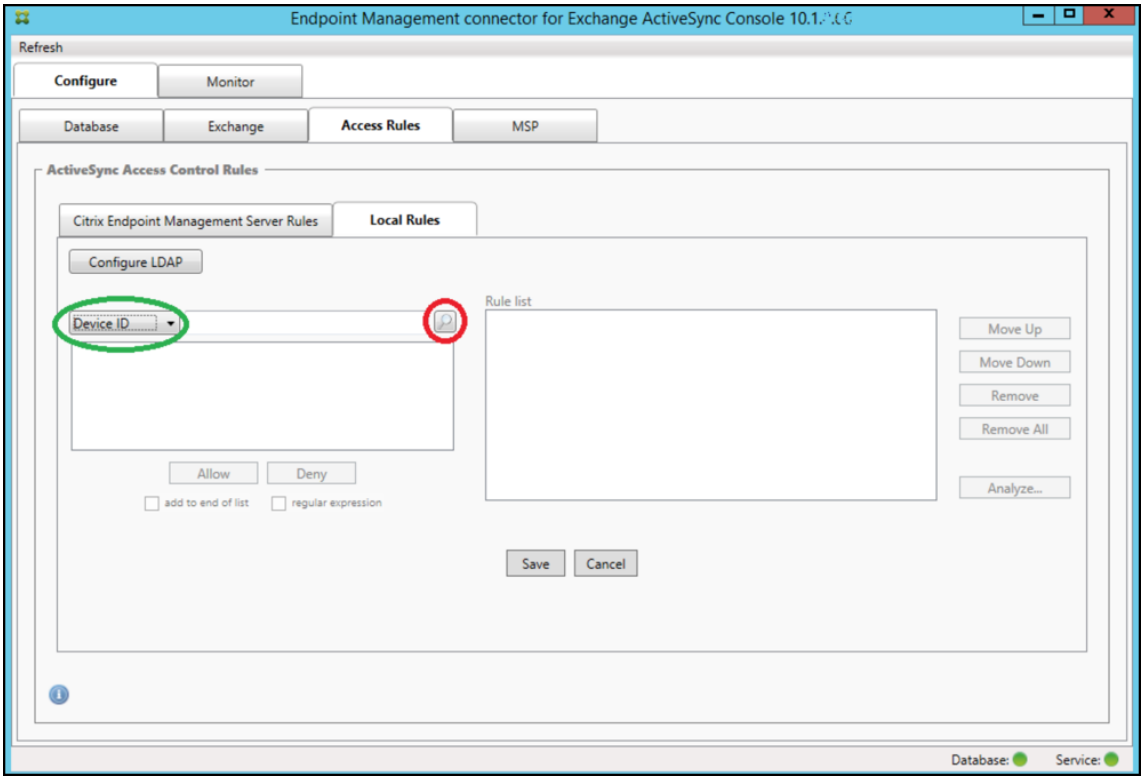
   c) regular expression(정규식) 확인란이선택되어있는지확인합니다.

   d) **Allow(**허용**)** 를클릭합니다.

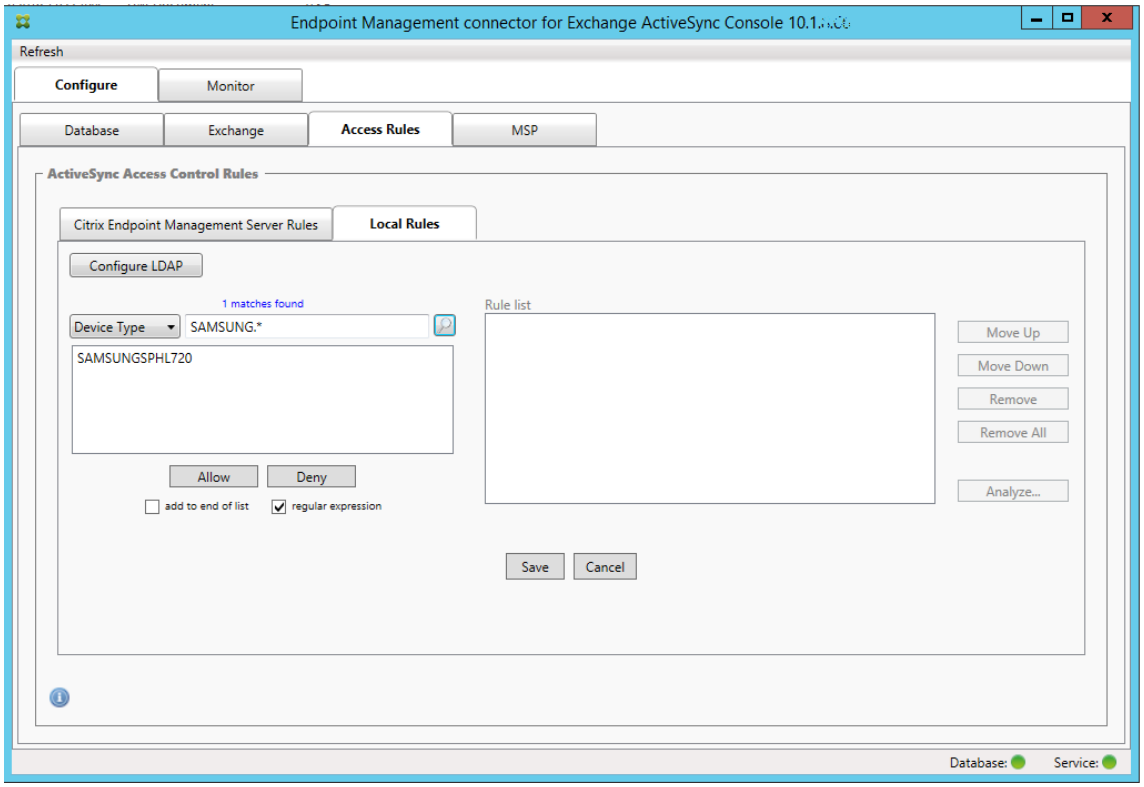


액세스규칙을작성하려면

1. **Local Rules(**로컬규칙**)** 탭을클릭합니다.
2. 정규식을입력하려면 Device ID(장치 ID) 목록과선택한항목텍스트상자를모두사용해야합니다.



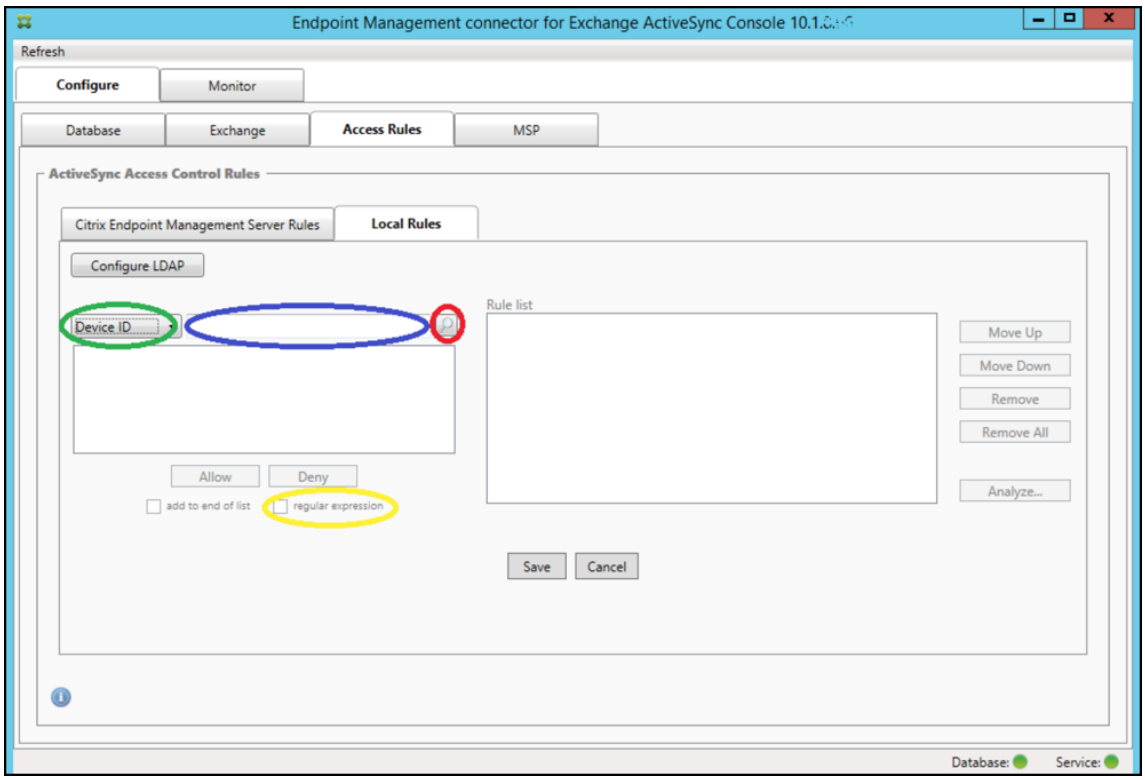
3. 일치기준으로사용할필드를선택합니다. 이예제에서는 Device Type(장치유형) 을사용합니다.
4. 정규식을입력합니다. 이예에서는다음을사용합니다. `samsung.*`
5. regular expression(정규식) 확인란이선택되었는지확인한후 **Allow(**허용**)** 또는 **Deny(**거부**)** 를클릭합니다. 이예에서는 **Allow(**허용**)** 를선택합니다. 최종결과는다음과같습니다.



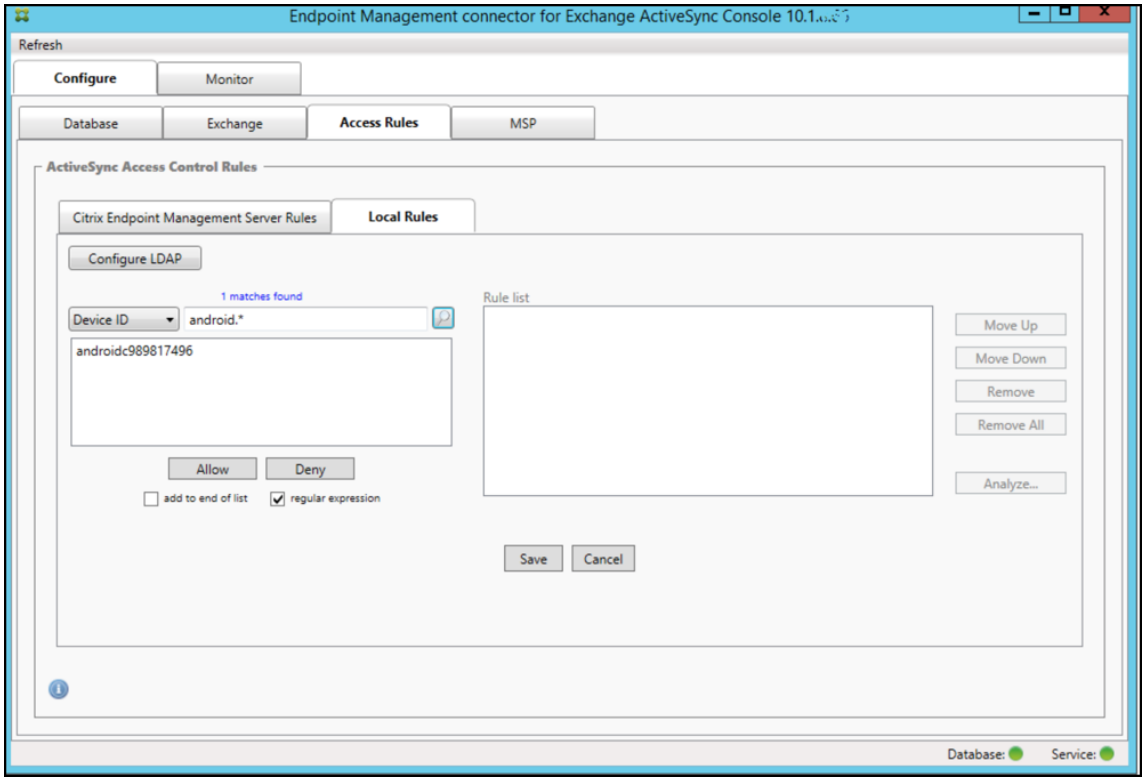
장치를찾으려면

정규식확인란을선택하면지정된식과일치하는특정장치에대한검색을실행할수있습니다. 이기능은주스냅샷을성공적으로완료한경우에만사용할수있습니다. 정규식규칙을사용할계획이없는경우에도이기능을사용할수있습니다. 예를들어 ActiveSync 장치 ID에 “workmail” 텍스트가포함된모든장치를찾을수있습니다. 이렇게하려면다음절차를따르십시오.

1. **Access Rules(**액세스규칙**)** 탭을클릭합니다.
2. 장치일치필드선택기가 Device ID(장치 ID)(기본값) 로설정되었는지확인합니다.



3. 선택한항목텍스트상자 (이전그림에서파란색으로표시됨) 안쪽을클릭한후 **`workmail.*`**를입력합니다.
4. regular expression(정규식) 확인란이선택되었는지확인한후돋보기아이콘을클릭하여다음그림에표시된것과같이일치하는항목을표시합니다.

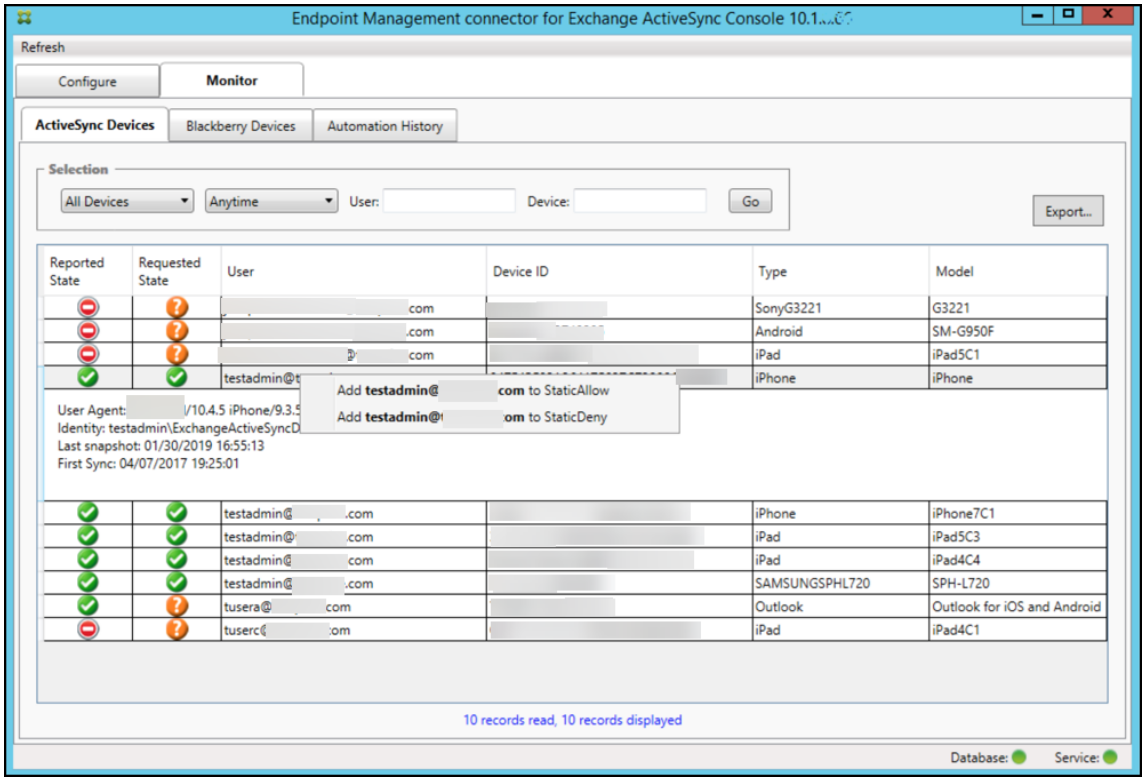


개별사용자, 장치또는장치유형을정적규칙에추가하려면

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**)** 탭을사용하면검색된 Exchange ActiveSync 및 BlackBerry 장치와자동화된 PowerShell 명령의실행기록을탐색할수있습니다. **Monitor(**모니터**)** 탭에는다음과같은세개의탭이있습니다.

- **ActiveSync Devices(ActiveSync** 장치**)**:
  - **Export(**내보내기**)** 단추를클릭하여표시된 ActiveSync 장치파트너관계를내보낼수있습니다.
  - **User(**사용자**)**, **Device ID(**장치 **ID)** 또는 **Type(**유형**)** 열을마우스오른쪽단추로클릭하고적절한허용또는차단규칙유형을선택하여로컬 (정적) 규칙을추가할수있습니다.
  - 확장된행을축소하려면 Ctrl 키를누른채로확장된행을클릭합니다.
- **Blackberry Devices(Blackberry** 장치**)**
- **Automation History(**자동화기록**)**

Configure(구성) 탭에는모든스냅샷기록이표시됩니다. 스냅샷기록은스냅샷생성시점, 스냅샷지속기간, 검색된장치수및발생한모든오류를보여줍니다.

- **Exchange** 탭에서원하는 Exchange Server 의정보아이콘을클릭합니다.
- **MSP** 탭에서원하는 BlackBerry Server 의정보아이콘을클릭합니다.

문제해결및진단

Exchange ActiveSync 용 Endpoint Management 커넥터는오류및기타작업정보를해당로그파일 (설치폴더\log\XmmWindowsService.log) 에기록합니다. 또한 Exchange ActiveSync 용 Endpoint Management 커넥터는중요한이벤트를 Windows 이벤트로그에기록합니다.

로깅수준을변경하려면

Exchange ActiveSync 용 Endpoint Management 커넥터에는오류, 정보, 경고, 디버그및추적로깅수준이포함됩니다.

> 참고:
>
> 뒤로갈수록더많은세부정보 (더많은데이터) 가생성됩니다. 예를들어오류수준은가장작은세부정보를제공하며추적수준은가장많은세부정보를제공합니다.

로깅수준을변경하려면다음을수행합니다.

1. C:\Program Files\Citrix\Citrix Endpoint Management 커넥터에서 nlog.config 파일을엽니다.
2. <rules> 섹션에서 *minilevel* 매개변수를원하는로깅수준으로변경합니다. 예:

```
1      <rules>
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. 파일을저장합니다.

   변경사항은즉시적용됩니다. Exchange ActiveSync 에대한커넥터를다시시작할필요가없습니다.

일반적인오류

다음목록에는일반적인오류가포함되어있습니다.

- Exchange ActiveSync 용 Endpoint Management 커넥터서비스가시작되지않음

  로그파일및 Windows 이벤트로그에서오류를확인합니다. 일반적인원인은다음과같습니다.

  - Exchange ActiveSync 용 Endpoint Management 커넥터서비스가 SQL Server 에액세스할수없습니다. 원인은다음문제일수있습니다.

    * SQL Server 서비스가실행되고있지않습니다.
    * 인증에실패했습니다.

    Windows 통합인증이구성된경우 Exchange ActiveSync 용 Endpoint Management 커넥터서비스의사용자계정이허용된 SQL 로그온이어야합니다. Exchange ActiveSync 용 Endpoint Management 커넥터서비스의계정은기본적으로로컬시스템으로설정되지만로컬관리자권한이없는다른계정으로변경될수있습니다. SQL 인증이구성된경우 SQL 에서 SQL 로그온이적절히구성되어야합니다.

  - MSP(모바일서비스공급자) 에대해구성된포트를사용할수없습니다. 시스템의다른프로세스에서사용하지않는수신포트를선택해야합니다.

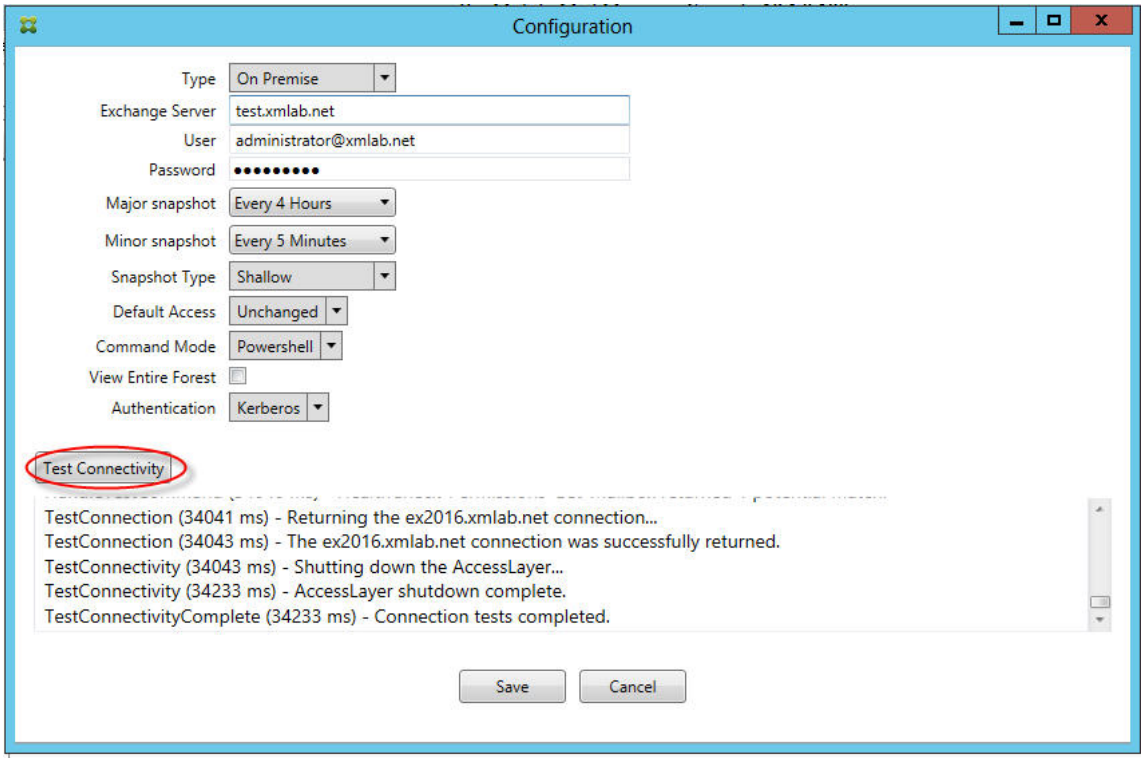
- XenMobile 에서 MSP 에연결할수없음

  Exchange ActiveSync 용 Endpoint Management 커넥터콘솔의 **Configure(**구성**) > MSP** 탭에서 MSP 서비스포트및전송이올바르게구성되었는지확인합니다. 인증그룹또는사용자가올바르게설정되었는지확인합니다.

  HTTPS 가구성된경우유효한 SSL 서버인증서가설치되어야합니다. IIS 가설치된경우 IIS Manager 를사용하여인증서를설치할수있습니다. IIS 가설치되지않은경우 How to configure a port with an SSL certificate(SSL 인증서로포트를구성하는방법)에서인증서설치에대한자세한내용을확인하십시오.

  Exchange ActiveSync 용 Endpoint Management 커넥터에는 MSP 서비스연결을테스트하는유틸리티프로그램이있습니다. *InstallFolder*\MspTestServiceClient.exe 프로그램을실행하고 URL 및자격증명을 XenMobile 에서구성할 URL 및자격증명으로설정한후 연결테스트를클릭합니다. XenMobile Server 에서실행하는웹서비스요청이시뮬레이션됩니다. HTTPS 가구성된경우서버의실제호스트이름을지정해야합니다 (SSL 인증서에지정된이름).

  연결테스트를사용하는경우하나이상의 ActiveSyncDevice 레코드가있어야합니다. 그렇지않을경우테스트가실패합니다.



문제해결도구

Support\PowerShell 폴더에문제해결을위한일련의 PowerShell 유틸리티가있습니다.

문제해결도구는사용자사서함및장치를심층분석하여오류조건및잠재적오류영역을감지하고사용자에대한 RBAC 분석을수행합니다. 모든 cmdlet 의원시출력을텍스트파일에저장할수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터

March 14, 2022

XenMobile Citrix ADC Connector 는이제 Exchange ActiveSync 용 Citrix Gateway 입니다. Citrix 통합포트폴리오에대한자세한내용은 Citrix 제품가이드를참조하십시오.

Exchange ActiveSync 용커넥터는 Exchange ActiveSync 프로토콜의역방향프록시역할을하는 Citrix ADC 에 ActiveSync 클라이언트의장치수준인증서비스를제공합니다. 인증은 XenMobile 내에서정의된정책의조합과 Exchange ActiveSync 용 Citrix Gateway 커넥터에서로컬로정의된규칙으로제어됩니다.

자세한내용은 ActiveSync Gateway를참조하십시오.

자세한참조아키텍처다이어그램은 아키텍처를참조하십시오.

Exchange ActiveSync 용 Citrix Gateway 커넥터의현재릴리스는버전 8.5.2 입니다.

> 중요:
>
> 2022 년 10 월부터 Exchange ActiveSync 용 Endpoint Management 및 Citrix Gateway 커넥터는 Microsoft 가 여기에서발표한인증변경사항에따라더이상 Exchange Online 을지원하지않습니다. Exchange 용 Endpoint Management 커넥터는 Microsoft Exchange Server(온-프레미스) 에서계속작동합니다.

새로운항목

이후섹션에는이전의 XenMobile Citrix ADC 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 Citrix ADC Connector 는이제 Exchange ActiveSync 용 Citrix Gateway 입니다.

이릴리스에서는다음과같은문제가수정되었습니다.

- 둘이상의기준이정책규칙을정의하는데사용되고이러한기준중하나에사용자 ID 가포함된경우사용자에게여러별칭이있으면규칙을적용할때별칭이확인되지않는문제가발생할수있습니다. [CXM-55355]

> 참고:
>
> 다음의새로운기능섹션에는 Exchange ActiveSync 용 Citrix Gateway 커넥터가이전이름인 XenMobile Citrix ADC Connector 로나타납니다. 이이름은버전 8.5.2 에서변경되었습니다.

버전 **8.5.1.11** 의새로운기능

- 시스템요구사항변경**:** Citrix ADC Connector 의현재버전에는 Microsoft .NET Framework 4.5 가필요합니다.
- **Google Analytics** 지원**:** XenMobile Citrix ADC Connector 가어떻게사용되는지를확인하여제품의개선영역에집중할수있습니다.
- **TLS 1.1** 및 **1.2** 에대한지원**:** PCI Council 에서는보안이취약한 TLS 1.0 의사용을중지하고있습니다. XenMobile Citrix ADC Connector 에는 TLS 1.1 및 1.2 에대한지원이추가되었습니다.

Exchange ActiveSync 용 **Citrix Gateway** 커넥터모니터링

Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티는 Exchange Server 를통과하면서 Secure Mobile Gateway 에의해허용또는차단된모든트래픽을볼수있는자세한로깅을제공합니다.

로그탭을사용하면권한부여를위해 Citrix ADC 가 Exchange ActiveSync 용커넥터로전달한 ActiveSync 요청의기록을볼 수있습니다.

또한 Exchange ActiveSync 용 Citrix Gateway 커넥터웹서비스가실행중인지확인하려면커넥터서버의브라우저에 URL `https://<host:port>/services/ActiveSync/Version`을로드합니다. URL 이제품버전을문자열로반환하면웹서비스가응답하는상태입니다.

Exchange ActiveSync 용 **Citrix Gateway** 커넥터로 **ActiveSync** 트래픽을시뮬레이션하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터를사용하여정책과관련된 ActiveSync 트래픽을시뮬레이션할수있습니다. 커넥터구성유틸리티에서 **Simulator(**시뮬레이터**)** 탭을선택합니다. 결과에는구성한규칙에따라정책이적용되는방식이표시됩니다.

Exchange ActiveSync 용 **Citrix Gateway** 커넥터에대한필터선택

Exchange ActiveSync 용 Citrix Gateway 커넥터필터는장치의정책위반또는속성설정을분석하여작동합니다. 장치가조건을충족하면장치가장치목록에배치됩니다. 이장치목록은허용목록이나차단목록이아닙니다. 정의된조건을충족하는장치의목록입니다. XenMobile 내에서커넥터에사용가능한필터는다음과같습니다. 각필터에는 **Allow(**허용**)** 또는 **Deny(**거부**)** 의두옵션이있습니다.

- 익명장치**:** XenMobile 에등록되었지만사용자의 ID 를알수없는장치를허용또는거부합니다. 예를들어등록은되었지만사용자의 Active Directory 암호가만료된사용자또는알수없는자격증명으로등록된사용자일수있습니다.
- **Samsung KNOX** 증명실패**:** Samsung 장치에는보안과진단을위한기능이있습니다. 이필터는장치가 KNOX 에대해설정되었다는확인을제공합니다. 자세한내용은 Samsung Knox를참조하십시오.
- 금지된앱**:** 차단목록정책에정의된장치목록및차단된앱의존재여부를기준으로장치를허용하거나거부합니다.
- 암시적허용**/**거부**:** 다른필터규칙조건을충족하지않는모든장치의장치목록을만들고해당목록을기반으로허용또는거부합니다. 암시적허용/거부옵션을사용하면장치탭에서 Exchange ActiveSync 용 Citrix Gateway 커넥터상태가사용되고장치의커넥터상태가표시됩니다. 또한암시적허용/거부옵션은선택되지않은다른모든커넥터필터도제어합니다. 예를들어차단된앱은커넥터에의해거부되지만암시적허용/거부옵션이 허용으로설정되었기때문에다른모든필터는허용됩니다.
- 비활성장치**:** 지정된시간동안 XenMobile 과통신하지않은장치의장치목록을만듭니다. 이러한장치는비활성상태인것으로간주됩니다. 필터는그에따라장치를허용또는거부합니다.
- 누락된필수앱**:** 사용자가등록하면설치해야하는필수앱목록을받게됩니다. 누락된필수앱필터는예를들어사용자가하나이상의앱을삭제하여하나이상의앱이더이상없음을나타냅니다.
- 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 인증에사용됩니다.
3. **Url** 에서 XenMobile GCS 의웹주소를입력합니다 (일반적으로 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 형식). *MagConfigService* 이름은대/소문자를구분합니다.
4. **Password(**암호**)** 에서 XenMobile Server 와의기본 HTTP 인증에사용될암호를입력합니다.
5. **Managing Host(**호스트관리**)** 에서커넥터서버이름을입력합니다.
6. **Baseline Interval(**기준간격**)** 에서새로고친동적규칙집합을 Device Manager 에서가져올기간을지정합니다.
7. **Delta interval(**델타간격**)** 에서동적규칙의업데이트를가져올기간을지정합니다.
8. **Request Timeout(**요청시간초과**)** 에서서버요청시간초과간격을지정합니다.
9. **Config Provider(**구성공급자**)** 에서구성공급자서버인스턴스가정책구성을제공하는지여부를선택합니다.
10. **Events Enabled(**이벤트사용**)** 에서는장치가차단되었을때커넥터가 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. 이설정은다수의 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**)**. 이정책모드는커넥터를통과하는모든트래픽에대한액세스를허용합니다. 다른필터링규칙은사용되지않습니다.
- **Deny All(**모두거부**)**. 이정책모드는커넥터를통과하는모든트래픽에대한액세스를거부합니다. 다른필터링규칙은사용되지않습니다.
- **Static Rules: Block Mode(**정적규칙**:** 차단모드**)**. 이정책모드는끝에암시적거부또는차단문이있는정적규칙을실행합니다. 커넥터는다른필터규칙을통해허용되지않는장치를차단합니다.
- **Static Rules: Permit Mode(**정적규칙**:** 허용모드**)**. 이정책모드는끝에암시적허용문이있는정적규칙을실행합니다. 다른필터규칙을통해차단또는거부되지않는장치는커넥터를통해허용됩니다.
- **Static + ZDM Rules**: Block Mode(정적 + ZDM 규칙: 차단모드). 이정책모드는정적규칙을먼저실행한다음, 끝에암시적거부또는차단문이있는 XenMobile 의동적규칙을실행합니다. 장치는정의된필터및 Device Manager 규칙에기반하여허용또는거부됩니다. 정의된필터및규칙에일치하지않는모든장치는차단됩니다.
- **Static + ZDM Rules**: Permit Mode(정적 + ZDM 규칙: 허용모드). 이정책모드는정적규칙을먼저실행한다음, 끝에암시적허용문이있는 XenMobile 의동적규칙을실행합니다. 장치는정의된필터및 XenMobile 규칙에기반하여허용또는거부됩니다. 정의된필터및규칙에일치하지않는모든장치는허용됩니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터프로세스는 XenMobile 에서수신된 iOS 및 Windows 기반모바일장치의고유 ActiveSync ID 를기반으로하여동적규칙에대한허용또는거부를처리합니다. Android 장치의동작은제조사에따라다르며일부는고유 ActiveSync ID 를제공하지않습니다. 이에따라 XenMobile 은허용또는차단을결정하기위해 Android 장치의사용자 ID 정보를보냅니다. 그결과사용자에게 Android 장치가하나인경우에는허용및차단이정상적으로작동합니다. 사용자에게 Android 장치가여러개인경우에는 Android 장치를구분할수없기때문에모든장치가허용됩니다. 알려진장치의경우 ActiveSyncID 가이러한장치를정적으로차단하도록게이트웨이를구성할수있습니다. 또한장치유형또는사용자에이전트에따라차단하도록게이트웨이를구성할수도있습니다.

정책모드를지정하려면 SMG Controller Configuration 유틸리티에서다음을수행합니다.

1. **Path Filters(**경로필터**)** 탭을클릭하고 **Add(**추가**)** 를클릭합니다.
2. **Path Properties(**경로속성**)** 대화상자의 **Policy(**정책**)** 목록에서정책모드를선택한다음 **Save(**저장**)** 를클릭합니다.

구성유틸리티의 **Policies(**정책**)** 탭에서규칙을검토할수있습니다. 규칙은 Exchange ActiveSync 용 Citrix Gateway 커넥터에서하향식으로처리됩니다. 허용정책에는녹색확인표시가나타납니다. 거부정책은선이그어진빨간색원으로표시됩니다. 화면을새로고쳐최근업데이트된규칙을보려면 **Refresh(**새로고침**)** 를클릭합니다. config.xml 파일에서규칙순서를수정할수도있습니다.

규칙을테스트하려면 **Simulator(**시뮬레이터**)** 탭을클릭합니다. 필드에값을지정합니다. 로그에서가져올수도있습니다. Allow(허용) 또는 Block(차단) 을지정하는결과메시지가나타납니다.

정적규칙을구성하려면

ActiveSync 연결 HTTP 요청의 ISAPI 필터링이읽는값이포함된정적규칙을입력합니다. 정적규칙을사용하면 Exchange ActiveSync 용 Citrix Gateway 커넥터가다음조건에따라트래픽을허용하거나차단할수있습니다.

- **User(**사용자**)**. Exchange ActiveSync 용 Citrix Gateway 커넥터는장치등록도중캡처된권한부여된사용자값및이름구조를사용합니다. 이러한구조는일반적으로 LDAP 를통해 Active Directory 에연결된 XenMobile 이실행되는서버가참조하는도메인\사용자이름으로발견됩니다. 커넥터구성유틸리티내의 **Log(**로그**)** 탭에커넥터를통해전달되는값이표시됩니다. 값구조를구분해야하거나값구조가다른경우값이전달됩니다.
- **Deviceid(ActiveSyncID)**. 연결된장치의 ActiveSyncID 라고도합니다. 이값은일반적으로 XenMobile 콘솔의특정장치속성페이지내에서볼수있습니다. 또한이값은커넥터구성유틸리티의로그탭에서숨겨질수도있습니다.
- **DeviceType**. 커넥터는장치가 iPhone, iPad 또는기타장치유형중무엇인지판별하고이조건에따라허용또는차단할수있습니다. 다른값과마찬가지로커넥터구성유틸리티는 ActiveSync 연결을처리중인모든연결된장치유형을표시할수있습니다.
- **UserAgent**. 사용되는 ActiveSync 클라이언트에대한정보가포함됩니다. 대개의경우지정된값은모바일장치플랫폼의특정운영체제빌드및버전에해당합니다.

서버에서실행되는커넥터구성유틸리티는항상정적규칙을관리합니다.

1. SMG Controller 구성유틸리티에서 **Static Rules(**정적규칙**)** 탭을클릭한다음 **Add(**추가**)** 를클릭합니다.
2. **Static Rule Properties(**정적규칙속성**)** 대화상자에서조건으로사용할값을지정합니다. 예를들어사용자이름 (예: AllowedUser) 을입력한다음 **Disabled(**사용안함**)** 확인란을선택취소하여액세스를허용할사용자를입력할수있습니다.
3. 저장을클릭합니다.

   이제정적규칙이적용됩니다. 또한정규식을사용하여값을정의할수있지만 config.xml 파일에서규칙처리모드를사용하도록설정해야합니다.

동적규칙을구성하려면

XenMobile 의장치정책및속성은동적규칙을정의하며동적 Exchange ActiveSync 용 Citrix Gateway 커넥터필터를트리거할수있습니다. 이러한필터는정책위반또는속성설정의존재유무에따라트리거됩니다. 커넥터필터는장치의정책위반또는속성설정을분석하여작동합니다. 장치가조건을충족하면장치가장치목록에배치됩니다. 이장치목록은허용목록이나차단목록이아닙니다. 정의된조건을충족하는장치의목록입니다. 다음구성옵션을사용하면장치목록의장치를커넥터를사용하여허용하거나거부할지여부를정의할수있습니다.

> 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** 파일을편집하여사용자지정정책을구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티 **Policies(**정책**)** 탭의기본구성에서기본정책을볼수있습니다. 사용자지정정책을만들려면 Exchange ActiveSync 용 Citrix Gateway 커넥터 XML 구성파일 (config\config.xml) 을편집할수있습니다.

1. 파일에서 **PolicyList** 섹션을찾은다음새 정책요소를추가합니다.
2. 다른정적그룹이나다른 GCP 를지원하기위한그룹과같은새그룹도필요한경우 **GroupList** 섹션에새 그룹요소를추가합니다.
3. 필요한경우 **GroupRef** 요소를재정렬하여기존정책내의그룹순서를변경할수있습니다.

Exchange ActiveSync 용 **Citrix Gateway** 커넥터 **XML** 파일구성

Exchange ActiveSync 용 Citrix Gateway 커넥터는 XML 구성파일을사용하여커넥터동작을설명합니다. 이파일은다른항목중그룹파일과 HTTP 요청을평가할때필터가수행할관련동작을지정합니다. 기본적으로파일의이름은 config.xml 이며..\Program Files\Citrix\XenMobile Citrix ADC Connector\config 위치에서찾을수있습니다.

GroupRef 노드

GroupRef 노드는논리적그룹이름을정의합니다. 기본값은 AllowGroup 및 DenyGroup 입니다.

> 참고:
>
> GroupRefList 노드에나타나는 GroupRef 노드의순서는중요한의미를갖습니다.

GroupRef 노드의 ID 값은특정사용자계정또는장치를찾는데사용되는구성원의논리적컨테이너또는컬렉션을식별합니다. 작업 특성은컬렉션의규칙에일치하는구성원을어떤방식으로필터링하는지를지정합니다. 예를들어 AllowGroup 집합의규칙과일치하는사용자계정또는장치는 “통과” 됩니다. 통과란 Exchange CAS 에대한액세스가허용되는것을의미합니다. DenyGroup 집합의규칙과일치하는사용자계정또는장치는 “거부” 됩니다. 거부란 Exchange CAS 에대한액세스가허용되지않는것을의미합니다.

특정사용자계정/장치또는조합이두그룹모두의규칙을충족할경우에는우선권규칙이사용되어요청의결과가도출됩니다. 우선권은 config.xml 파일에서위에서아래로 GroupRef 노드의순서를따릅니다. GroupRef 노드는우선순위에따라순위가매겨집니다. 허용그룹의특정조건에대한규칙은거부그룹의동일조건에대한규칙보다항상더높은우선순위를가집니다.

그룹노드

config.xml 에서는그룹노드도정의합니다. 이러한노드는논리적컨테이너 AllowGroup 및 DenyGroup 을외부 XML 파일에연결합니다. 외부파일에저장된항목이필터규칙의기본을구성합니다.

> 참고:
>
> 이릴리스에서는외부 XML 파일만지원됩니다.

기본설치는구성에서두개의 XML 파일인 allow.xml 및 deny.xml 을구현합니다.

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, 사용가능한운영체제플랫폼과앱의수가매우많기때문에허용모델의사용은취약한선택입니다. 대개의조직에서는제한모델이더논리적인선택입니다.

Citrix 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를 XenMobile 과통합할때허용하는구성시나리오는다음과 같습니다.

허용모델 **(**허용모드**)**

허용보안모델은기본적으로모든것이허용되거나액세스권한이부여된다는전제하에작동합니다. 규칙및필터링을통해서만무언가차단되고제한이적용됩니다. 허용보안모델은모바일장치에대한보안우려가비교적느슨한조직에적합합니다. 이모델은해당하는경우 (정책규칙이실패한경우) 액세스를거부하는제한적인제어만적용합니다.

제한모델 **(**차단모드**)**

제한보안모델은기본적으로어떤것도허용되지않거나액세스권한이부여되지않는전제하에작동합니다. 보안검사점을통과하는모든항목이필터링및검사되며액세스를허용하는규칙을통과하지못하면액세스가거부됩니다. 제한보안모델은모바일장치에대한보안기준이비교적엄격한조직에적합합니다. 이모드에서는액세스허용을위한모든규칙을통과한경우네트워크서비스의기능및사용에대한액세스를허용합니다.

Exchange ActiveSync 용 **Citrix Gateway** 커넥터관리

Exchange ActiveSync 용 Citrix Gateway 커넥터를사용하여액세스제어규칙을작성할수있습니다. 액세스제어규칙은관리되는장치의 ActiveSync 연결요청에대한액세스를허용하거나차단합니다. 액세스는장치상태, 앱허용또는차단목록및기타규정준수조건에따라허용되거나차단됩니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티를사용하면회사전자메일정책을적용하여규정표준을위반하는사용자를차단할수있는동적및정적규칙을만들수있습니다. 또한전자메일첨부파일암호화를설정하여, Exchange Server 를통과하여관리되는장치로전송되는모든첨부파일을암호화하고권한있는사용자만관리되는장치에서이를볼수있도록할수있습니다.

Exchange ActiveSync 용 **Citrix Gateway** 커넥터를제거하려면

1. 관리자계정으로 XncInstaller.exe 를실행합니다.
2. 화면지침에따라제거를완료합니다.

Exchange ActiveSync 용 **Citrix Gateway** 커넥터를설치**,** 업그레이드또는제거하려면

1. 관리자계정으로 XncInstaller.exe 를실행하여커넥터를설치하거나기존커넥터의업그레이드또는제거를허용합니다.

2. 화면지침에따라설치, 업그레이드또는제거를완료합니다.

커넥터를설치한후에는 XenMobile 구성서비스및알림서비스를수동으로다시시작해야합니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터설치

Exchange ActiveSync 용 Citrix Gateway 커넥터를자체 Windows Server 에설치합니다.

커넥터가서버에가하는 CPU 부하는관리되는장치수에따라다릅니다. 장치수가많은경우 (50,000 개초과) 클러스터링환경이아니라면둘이상의코어를프로비전해야할수있습니다. 커넥터의메모리사용량은추가메모리가필요할정도로높지않습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터시스템요구사항

Exchange ActiveSync 용 Citrix Gateway 커넥터는 Citrix ADC 장비에구성된 SSL 브리지를통해 Citrix ADC 와통신합니다. 이 SSL 브리지는장비가모든보안트래픽을 XenMobile 에직접연결할수있도록해줍니다. 커넥터에는다음의최소시스템구성이필요합니다.

구성요소	요구사항
컴퓨터및프로세서	733MHz Pentium III 733MHz 이상프로세서. 2.0GHz Pentium III 이상프로세서 (권장)
Citrix ADC	소프트웨어버전 10 Citrix ADC 장비
메모리	1GB
하드디스크	150MB 의사용가능한하드디스크공간이있으며 NTFS 로포맷된로컬파티션
운영체제	Windows Server 2016, Windows Server 2012 R2 또는 Windows Server 2008 R2 서비스팩 1. 영어기반서버여야합니다. 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 지원되는장치운영체제를참조하십시오.

장치전자메일클라이언트

일부전자메일클라이언트는한장치에대해동일한 ActiveSync ID 를일관되게반환하지않습니다. Exchange ActiveSync 용 Citrix Gateway 커넥터에서는각장치에고유한 ActiveSync ID 를사용하도록요구하므로각장치에대해동일한고유 ActiveSync ID 를일관되게생성하는전자메일클라이언트만지원됩니다. 다음과같은전자메일클라이언트는 Citrix 의테스트에서오류없이실행되는것으로확인되었습니다.

- Samsung 기본전자메일클라이언트
- iOS 기본전자메일클라이언트

Exchange ActiveSync 용 Citrix Gateway 커넥터배포

Exchange ActiveSync 용 Citrix Gateway 커넥터를사용하면 Citrix ADC 를통해 XenMobile Server 와 XenMobile 관리되는장치의통신을프록시및부하분산할수있습니다. 커넥터는주기적으로 XenMobile 과통신하여정책을동기화합니다. 커넥터및 XenMobile 은함께또는독립적으로클러스터링될수있으며 Citrix ADC 로부하분산될수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터구성요소

- **Exchange ActiveSync 용 Citrix Gateway 커넥터서비스:** 이서비스는장치로부터의 ActiveSync 요청이인증되었는지확인하기위해 Citrix ADC 가호출할수있는 REST 웹서비스인터페이스를제공합니다.
- **XenMobile 구성서비스:** 이서비스는 XenMobile 과통신하여 XenMobile 정책변경내용을커넥터와동기화합니다.
- **XenMobile 알림서비스:** 이서비스는권한이없는장치액세스의알림을 XenMobile 에보냅니다. 이렇게하면 XenMobile 이장치가차단된이유를사용자에게알리는등의적절한조치를취할수있습니다.
- **Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티:** 관리자는이응용프로그램을사용하여커넥터를구성하고모니터링할수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터에대한수신주소를설정하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터에서 Citrix ADC 의 ActiveSync 트래픽승인요청을수신할수있도록하려면다음을수행합니다. 커넥터가 Citrix ADC 웹서비스호출을수신하는포트를지정합니다.

1. **Start(**시작**)** 메뉴에서 Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티를선택합니다.
2. **Web Service(**웹서비스**)** 탭을클릭한다음커넥터웹서비스의수신주소를입력합니다. **HTTP** 또는 **HTTPS** 또는둘다를선택할수있습니다. 커넥터와 XenMobile 이동일한서버에함께설치된경우에는 XenMobile 과충돌하지않는포트값을선택하십시오.
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) 는규칙에의해명시적으로식별되지않는모든장치가 ActiveSync 에액세스할수있도록허용됨을의미합니다. Block Mode(차단모드) 는이러한장치가차단됨을의미합니다.
4. 정책을설정한후 **Save(**저장**)** 를클릭합니다.

XenMobile 과의통신을구성하려면

Exchange ActiveSync 용 Citrix Gateway 커넥터및 Citrix ADC 와함께사용할 XenMobile Server(구성공급자라고도함) 의이름과속성을지정합니다.

> 참고**:**
>
> 이작업에서는이미 XenMobile 을설치및구성한것으로간주합니다.

1. Exchange ActiveSync 용 Citrix Gateway 커넥터구성유틸리티에서 **Config Providers(**구성공급자**)** 탭을클릭하고 **Add(**추가**)** 를클릭합니다.
2. 이배포에서사용중인 XenMobile Server 의이름과 URL 을입력합니다. 다중테넌트배포에서여러 XenMobile Server 를배포한경우이이름은각서버인스턴스에대해고유해야합니다. 예를들어 **Name(**이름**)** 에 **XMS** 를입력할수있습니다.
3. **Url** 에서 XenMobile GCP(GlobalConfig Provider) 의웹주소를입력합니다 (일반적으로 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 형식). *MagConfigService* 이름은대/소문자를구분합니다.
4. **Password(**암호**)** 에서 XenMobile 웹서버와의기본 HTTP 인증에사용될암호를입력합니다.
5. **Managing Host(**관리호스트**)** 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를설치한서버이름을입력합니다.
6. **Baseline Interval(**기준간격**)** 에서새로고친동적규칙집합을 XenMobile 에서가져올기간을지정합니다.
7. **Request Timeout(**요청시간초과**)** 에서서버요청시간초과간격을지정합니다.
8. **Config Provider(**구성공급자**)** 에서구성공급자서버인스턴스가정책구성을제공하는지여부를선택합니다.
9. **Events Enabled(**이벤트사용**)** 에서는장치가차단되었을때 Secure Mobile Gateway 가 XenMobile 에알리도록하려면이옵션을선택합니다. Device Manager 자동화된동작에서 Secure Mobile Gateway 규칙을사용하는경우이옵션이필요합니다.
10. 서버를구성한후 **Test Connectivity(**연결테스트**)** 를클릭하여 XenMobile 연결을테스트합니다.
11. 연결이되면 **Save(**저장**)** 를클릭합니다.

중복성및확장성을위한 **Exchange ActiveSync** 용 **Citrix Gateway** 커넥터배포

Exchange ActiveSync 용 Citrix Gateway 커넥터및 XenMobile 배포를확장하려면모두동일한 XenMobile 인스턴스를가리키는커넥터인스턴스를여러 Windows 서버에설치한다음 Citrix ADC 를사용하여서버의부하를분산할수있습니다.

Exchange ActiveSync 용 Citrix Gateway 커넥터구성에는두가지모드가있습니다.

- 비공유모드에서는각 Exchange ActiveSync 용 Citrix Gateway 커넥터인스턴스가 XenMobile Server 와통신하며결과정책의자체사본을유지합니다. 예를들어 XenMobile Server 의클러스터가있는경우커넥터인스턴스를각 XenMobile Server 에서실행할수있으며커넥터는로컬 XenMobile 인스턴스에서정책을가져옵니다.
- 공유모드에서는하나의커넥터노드가주노드로지정되며이노드가 XenMobile 과통신합니다. 결과구성은 Windows 네트워크공유또는 Windows(또는타사) 복제에의해다른노드간에공유됩니다.

전체커넥터구성은하나의폴더 (몇개의 XML 파일로구성됨) 에있습니다. 커넥터프로세스는이폴더에있는모든파일의변경내용을감지하여자동으로구성을다시로드합니다. 공유모드에서는주노드에대한장애조치 (failover) 가없습니다. 하지만마지막으로알려진정상구성이커넥터프로세스에캐시되기때문에시스템은주서버중지를몇분동안 (예를들어다시시작할때까지) 허용합니다.

고급개념

January 5, 2022

> 참고:
>
> 이문서에서는 XenMobile Server 의고급개념에대해다룹니다. Endpoint Management 의고급정보에대해서는 고급개념을참조하십시오.

XenMobile 고급개념문서는 XenMobile 의제품설명서에대한상세한정보를제공합니다. 전문기술을통해배포시간을단축하는것이목표인이문서에는콘텐츠를작성한기술전문가의설명이인용될수있습니다.

전체 XenMobile 환경에대한의사결정사안, 권장사항, 일반적인질문및사용사례는이섹션의 XenMobile 배포안내서를참조하십시오.

XenMobile 의커뮤니티지원포럼은 Citrix Discussions를참조하십시오.

온-프레미스 **XenMobile** 과 **Active Directory** 상호작용

January 5, 2022

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 도메인인증또는도메인및보안토큰인증을참조하십시오.

인라인상호작용

XenMobile Server 는관리자가구성한 LDAP 설정을사용하여 Active Directory 와통신합니다. 이설정은사용자및그룹에대한정보를검색합니다. 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 데이터베이스에저장되지않습니다.

    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 를사용하여고유이름및 sAMAccountName 특성의현재값이확인되고관심그룹의고유이름또는 sAMAccountName 값에대한변경내용이데이터베이스에업데이트됩니다.

   > 참고:
   >
   > 이작업은사용자-그룹구성원자격정보를업데이트하지않습니다.

2. 중첩그룹동기화작업. 이작업은관심그룹의중첩계층에대한변경내용을업데이트합니다. XenMobile Server 에서는관심그룹의직접구성원과간접구성원에게권한을부여할수있습니다. 사용자의직접구성원자격은사용자기반인라인상호작용

에서업데이트됩니다. 백그라운드에서실행되는경우이작업은간접구성원자격을추적합니다. 간접구성원자격은관심그룹의구성원인그룹에사용자가포함되는경우를말합니다.

이작업은 XenMobile Server 데이터베이스에서 Active Directory 그룹목록을수집합니다. 이러한그룹은배포그룹또는 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

백그라운드작업은기본적으로얼마의빈도로실행됩니까?

- 현지시간으로 02:00 부터 5 시간에한번씩그룹동기화작업이실행됩니다.
- 중첩그룹동기화작업은현지시간으로자정부터하루에한번실행됩니다.

그룹동기화작업이필요한이유는무엇입니까?

- Active Directory 에있는사용자레코드의 memberOf 특성에는사용자가직접구성원인그룹목록이나와있습니다. 그룹의 OU 가변경되면 memberOf 특성에고유이름의최신값이반영됩니다. XenMobile Server 데이터베이스도마지막으로새로고쳐진값으로업데이트됩니다. 그룹의고유이름이일치하지않으면사용자가배포그룹에액세스할수없게됩니다. 또한해당배포그룹에연결된앱및정책에도액세스하지못할수있습니다.
- 백그라운드작업은 XenMobile Server 데이터베이스에포함되는그룹의고유이름특성을최신상태로유지하여사용자가부여받은권한에따라액세스할수있도록합니다.
- 동기화작업은 Active Directory 내그룹이자주변경되지않을것으로가정하여 5 시간마다실행되도록예약됩니다.

그룹동기화작업을끌수있습니까?

- 관심그룹의 OU 가변경되지않은것을알고있다면이작업을꺼도됩니다.

중첩된그룹을처리하는백그라운드작업이필요한이유는무엇입니까?

- Active Directory 에서그룹중첩에대한변경은일상적으로발생하는작업이아닙니다. 관심그룹의중첩계층이변경되면영향받는사용자의권한부여가변경됩니다. 그룹이계층에추가되면구성원사용자에게해당하는역할이부여됩니다. 그룹을중첩계층밖으로이동하면그룹의구성원사용자가역할기반권한에액세스하지못할수있습니다.
- 중첩에대한변경내용은사용자를새로고칠때캡처되지않습니다. 중첩변경내용은주문형으로캡처할수없으며백그라운드작업을통해캡처됩니다.
- 중첩변경은자주발생하지않는다는전제에따라변경내용을확인하는백그라운드작업은하루에한번실행됩니다.

중첩된그룹을처리하는작업을끌수있습니까?

- 관심그룹의중첩이변경되지않은것을알고있다면이작업을꺼도됩니다.

XenMobile 배포

December 1, 2020

XenMobile 배포를계획할때는고려할사항이많습니다.

- 어떤장치를선택할지,
- 어떤장치를관리할지,
- 네트워크를보호하면서뛰어난사용자환경을어떻게조성할지,
- 어떤하드웨어가필요하고문제는어떻게해결할수있는지.

이섹션의목표는이와같은질문에답을할수있도록지원하는것입니다. 배포관련항목에대한사용사례및권장사항도확인할수있습니다.

일부환경또는사용사례에는지침또는권장사항이적용되지않을수있습니다. XenMobile 을실제로배포하기전에테스트환경을설정하십시오.

이섹션의문서에서는다음과같은분야를다룹니다.

- **평가:** 배포계획시고려해야할일반적인사용사례및질문
- **설계및구성:** 환경의설계및구성에대한권장사항
- **작동및모니터링:** 실행중인환경이원활하게작동하는지확인

평가

다른배포와마찬가지로가장먼저요구사항을평가해야합니다. XenMobile 을통해기본적으로해결해야하는요구사항은무엇입니까? 환경의모든장치를관리해야합니까? 아니면앱만관리하면됩니까? 둘다관리해야합니까? XenMobile 환경에필요한보안수준은무엇입니까? 다음으로배포계획시고려해야하는일반적인사용사례및질문에대해살펴봅니다.

- 관리모드
- 장치요구사항
- 보안및사용자환경
- 앱
- 사용자커뮤니티
- 전자메일전략
- XenMobile 통합
- 다중사이트요구사항

설계및구성

배포요구사항을평가한후에는환경의설계및구성을결정할수있습니다. 계획해야할몇가지사항:

- 서버의하드웨어선택
- 앱및장치에대한정책설정

- 등록된사용자가져오기

이섹션에는이러한각시나리오에대한사용사례및권장사항이포함되어있습니다.

- Citrix ADC 및 Citrix Gateway 통합
- MDX 앱에대한 SSO 및프록시고려사항
- 인증
- 온-프레미스배포용참조아키텍처
- 서버속성
- 장치및앱정책
- 사용자등록옵션
- XenMobile 작업조정

작동및모니터링

XenMobile 을시작하고실행한후에는모니터링을통해원활하게작동하는지확인해야합니다. 모니터링섹션에서는 XenMobile 및해당구성요소가생성하는다양한로그및메시지를찾을수있는위치와이러한로그를판독하는방법을설명합니다. 또한이섹션에는고객지원피드백시간을줄일수있는일반적인문제해결단계가포함되어있습니다.

- 앱프로비전및프로비전해제
- 대시보드기반작업
- 역할기반액세스제어및 XenMobile 지원
- 시스템모니터링
- 재해복구
- Citrix 지원프로세스

관리모드

August 12, 2022

각 XenMobile 인스턴스 (단일서버또는노드클러스터) 에대해장치, 앱또는둘다를관리할지여부를선택할수있습니다. XenMobile 에서는장치및앱관리모드에다음용어를사용합니다.

- MDM 모드 (모바일기기관리모드)
- MAM 모드 (모바일앱관리모드)
- MDM+MAM 모드 (엔터프라이즈모드)

MDM 모드 **(**모바일기기관리모드**)**

> 중요**:**
>
> MDM 모드를구성하고나중에 ENT 모드로변경하는경우동일한인증 (Active Directory) 을사용해야합니다.

> XenMobile 은사용자등록후의인증모드변경을지원하지않습니다. 자세한내용은 업그레이드를참조하십시오.

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.
- 사용자가모바일장치의기본전자메일클라이언트로전자메일을전송하기만하면되고이미외부액세스가가능한 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 사용모바일앱을사용하여앱별컨테이너화및제어를제공할수있습니다. MAM 모드를 MAM 전용모드라고도합니다. 이용어는이모드를레거시 MAM 모드와구분합니다.

XenMobile 은 MDX 정책을활용하여네트워크액세스 (예: Micro VPN), 앱및장치상호작용, 데이터암호화및앱액세스를앱수준에서제어합니다.

MAM 은주로 BYO(Bring-Your-Own) 장치에적합합니다. 이모드에서는장치가관리되지않지만회사데이터가보호되는상태로유지되기때문입니다. MDX 에는 MDM 컨트롤이필요하지않은 MAM 전용정책이많이있습니다.

또한 MAM 은모바일생산성앱을지원합니다. 이지원에는 Citrix Secure Mail 로의보안전자메일전송, 보안이적용된모바일생산성앱간의데이터공유및 Citrix Files 의보안데이터스토리지가포함됩니다. 자세한내용은 모바일생산성앱을참조하십시오.

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 정책을통한장치관리가필요하거나필요하지않을수있습니다.

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.

사용할수있는관리모드및기타기능은다음표에표시된것과같이라이센스가있는 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
-	-	ShareConnect
-	-	Citrix Files

관리모드및등록프로필

관리모드와등록프로필은함께작동합니다. 등록프로필을사용하여 Android 및 iOS 기기의장치관리및앱관리등록옵션을구성합니다. Android 의경우 MDM+MAM 서버모드에제공되는등록옵션은 MDM 모드의옵션과다릅니다. 자세한내용은 등록프로필을참조하십시오.

장치관리및 **MDM** 등록

XenMobile Enterprise 환경에는여러사용사례가혼재할수있으며일부사용사례에는 MAM 리소스에액세스할때 MDM 정책을통한장치관리가필요합니다. 모바일생산성앱을사용자에게배포하기전에사용사례를철저히평가하고 MDM 등록이필요한지여

부를결정해야합니다. MDM 등록에대한요구사항을나중에변경하려는경우사용자가장치를재등록해야합니다.

> 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 Citrix ADC, XenMobile Server 및응용프로그램별시간초과를구성하여추가계층의보호를제공할 수있습니다.
- MDM 동작은장치에적용되지않지만일부 MDX 정책을사용하여 MAM 액세스를거부할수있습니다. 거부는시스템설정 (예: 탈옥또는루팅장치) 에따라수행됩니다.
- 사용자가첫사용시장치를 MDM 에등록할지여부를선택할수있습니다.

단점:

- MDM 에등록되지않은장치에서 MAM 리소스를사용할수있습니다.
- MDM 정책및동작을 MDM 등록장치에서만사용할수있습니다.

완화옵션:

- 사용자가규정위반을선택하는경우책임을져야한다는회사약관에동의하도록합니다. 관리자에게관리되지않는장치를모니터링하도록합니다.
- 응용프로그램타이머를사용하여응용프로그램액세스및보안을관리합니다. 시간초과값을줄이면보안이개선되지만사용자 경험에영향을미칠수있습니다.
- 필요한경우두번째 XenMobile 환경에서 MDM 등록을요구할수있습니다. 이옵션을고려할때는두환경을관리하는것으로인해추가오버헤드가발생하고리소스가추가로필요하다는점을염두에두십시오.

MDM 등록이필수인경우

장점:

- MAM 리소스에대한액세스를 MDM 관리장치로만제한할수있습니다.
- 원하는경우 MDM 정책및동작을환경의모든장치에적용할수있습니다.
- 사용자가장치등록을취소할수없습니다.

단점:

- 모든사용자가필수적으로 MDM 에등록해야합니다.
- 회사에서개인장치를관리하는것을반대하는사용자의채택이감소할수있습니다.

완화옵션:

- XenMobile 이실제로장치에서관리하는항목과관리자가액세스할수있는정보를사용자에게알려줍니다.
- MDM 관리가필요하지않은장치에대해 MAM 서버모드 (MAM 전용모드) 의두번째 XenMobile 환경을사용할수있습니다. 이옵션을고려할때는두환경을관리하는것으로인해추가오버헤드가발생하고리소스가추가로필요하다는점을염두에두십시오.

MAM 모드와레거시 **MAM** 모드정보

XenMobile 10.3.5 에는새로운 MAM 전용서버모드가도입되었습니다. 이전 MAM 모드와새 MAM 모드를구분하기위해설명서에는다음과같은용어가사용됩니다. 새모드는 MAM 전용또는 MA 라고하며이전 MAM 모드는레거시 MAM 모드라고합니다.

MAM 전용모드는 XenMobile 의서버모드속성이 MAM 일때적용됩니다. 장치는 MAM 모드에서등록됩니다.

레거시 MAM 기능은 XenMobile 의서버모드속성이 ENT 이고사용자가장치등록을선택하지않는경우적용됩니다. 이경우장치는 MAM 모드에서등록됩니다. MDM 관리를등록취소하는사용자에게는계속해서레거시 MAM 기능이제공됩니다.

> 참고**:**
>
> 이전에는서버모드속성을 MAM 으로설정해도 ENT 로설정할때와동일한효과가있었습니다. MDM 관리를선택하지않은사용자에게레거시 MAM 기능이제공되었습니다.

다음표에는특정라이센스유형및원하는장치모드에사용되는서버모드설정이요약되어있습니다.

라이센스버전	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.

- 인증서기반인증**:** MAM 전용모드는인증서기반인증을지원합니다. 사용자는 Active Directory 암호가만료된경우에도계속해서앱에액세스할수있습니다. MAM 장치에서인증서기반인증을사용하는경우 Citrix Gateway 를구성해야합니다. 기본적으로 **XenMobile** 설정 **> Citrix Gateway** 에서인증을위한사용자인증서제공은 꺼짐으로설정되어있습니다. 이는사용자이름과암호인증이사용됨을의미합니다. 이설정을 켜짐으로설정하면인증서인증이사용됩니다.
- 자가지원포털**:** 사용자가직접앱잠금및앱초기화를수행할수있습니다. 이러한동작은장치의모든앱에적용됩니다. 구성 **>** 동작에서앱잠금및앱초기화동작을구성할수있습니다.
- 모든등록보안모드**:** 관리 **>** 등록초대에서구성된높은수준의보안, 초대 URL 및 2 단계가포함됩니다.

- **Android** 및 **iOS** 장치에대한장치등록제한**:** 사용자당장치수서버속성이 구성 **>** 등록프로필로이동했고이제모든서버모드에적용됩니다.
- **MAM** 전용 **API:** MAM 전용장치에서 REST 서비스를호출할수있습니다. REST 클라이언트와 XenMobile REST API 를사용하여 XenMobile 콘솔에표시되는서비스를호출할수있습니다.
- MAM 전용 API 를사용하여다음을수행할수있습니다.
  - 초대 URL 과일회용 PIN 을전송합니다.
  - 장치에서앱잠금치초기화를실행합니다.

다음표에는레거시 MAM 기능과 MAM 전용기능의차이점이요약되어있습니다.

등록시나리오및기타기능	레거시 **MAM(ENT** 서버모드**)**	**MAM** 전용모드 **(MAM** 서버모드**)**
인증서인증	지원되지않음.	지원됨. 인증서인증을사용하려면 Citrix Gateway 가필요합니다.
배포요구사항	장치에서직접 XenMobile Server 에액세스하지않아도됩니다.	장치에서직접 XenMobile Server 에액세스하지않아도됩니다.
등록옵션	Citrix 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 사용자가삭제될 때의기본제공동작	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 을사용하여장치를등록합니다. (레거시 MAM 모드에서는 Citrix Gateway FQDN 을사용하여장치를등록합니다.)

장치요구사항

January 5, 2022

모든배포에서가장중요한고려사항중하나는롤아웃할장치입니다. iOS, Android 및 Windows 플랫폼에서옵션은많습니다. XenMobile 이지원하는장치목록은 지원되는장치플랫폼을참조하십시오.

BYOD(Bring Your Own Device) 환경에서는여러유형의지원되는플랫폼이사용될수있습니다. 그러나등록할수있는장치를사용자에게알릴때에는지원되는장치플랫폼문서의제한사항을고려하십시오. 환경에서 1~2 개의장치만허용한다하더라도 XenMobile 은 iOS, Android 및 Windows 장치에서조금씩다르게작동합니다. 각플랫폼에서사용할수있는기능집합이다릅니다.

또한모든앱이태블릿폼팩터와휴대폰폼팩터모두에서사용할수있도록설계되는것은아닙니다. 대대적인변경을수행하기전에앱을테스트하여롤아웃하려는장치화면에앱이맞는지확인하십시오.

다음과같은등록요소도고려할수있습니다. Apple 및 Google 은엔터프라이즈등록프로그램을제공합니다. Apple 배포프로그램과 Google Android Enterprise를통해직원이바로사용할수있도록미리구성된장치를구입할수있습니다.

등록에대한자세한내용은 사용자등록옵션을참조하십시오.

보안및사용자환경

February 2, 2022

보안은모든조직에서중요하지만보안과사용자환경사이의균형을맞춰야합니다. 예를들어매우안전하지만사용하기가어려운환경을구축할수있는가하면, 액세스제어가엄격하지않은사용자친화적인환경을구축할수도있습니다. 보안기능은이가상안내서의다른섹션에서자세히다룹니다. 이문서의목적은일반적인보안우려사항과 XenMobile 에서제공되는보안옵션을대략적으로설명하는것입니다.

다음은각사용사례에서주로고려해야할사항입니다.

- 특정앱, 전체장치또는둘다를보호해야합니까?
- 사용자 ID 를인증할때어떤방법을사용하고싶습니까? LDAP 인증, 인증서기반인증또는두인증의조합을사용할계획입니까?

- 사용자세션시간초과는어떻게처리하려고합니까? 백그라운드서비스, Citrix ADC 및오프라인중앱액세스에대한시간초과값이서로다르다는점에유의하십시오.
- 사용자가장치수준암호, 앱수준암호또는모두를설정해야합니까? 사용자가시도할수있는로그온횟수는몇번입니까? MAM으로구현되는추가적인앱별인증요구사항이사용자환경에미치는영향을염두에두십시오.
- 사용자에게적용하려는다른제한사항은무엇입니까? 사용자가 Siri 와같은클라우드서비스에액세스하길원합니까? 사용자는제공된각앱을사용하여무엇을할수있고무엇을할수없습니까? 사무실공간안에있는동안셀룰러데이터요금이소비되지않도록회사 Wi-Fi 정책을배포해야합니까?

앱과장치

일단모바일앱관리 (MAM) 를사용하여특정한앱의보안만확보할지여부를먼저고려해야합니다. 아니면모바일장치관리 (MDM) 를사용하여전체장치를관리할수도있습니다. 일반적으로, 장치수준제어가필요하지않은경우, 특히조직에서 BYOD(Bring Your Own Device) 를지원하는경우에는모바일앱만관리하면됩니다.

XenMobile 을통해관리되지않는장치의사용자는앱스토어를통해앱을설치할수있습니다. 선택적초기화또는전체초기화같은장치수준제어대신앱정책을사용하여앱액세스를제어할수있습니다. 설정한값에따라정책은장치에서주기적으로 XenMobile 에연결하여앱실행이허용되는지여부를확인해야합니다.

MDM 을사용하면하나의장치에모든소프트웨어의인벤토리를가져오는기능등전체장치의보안을확보할수있습니다. 장치가탈옥또는루팅되거나장치에안전하지않은소프트웨어가설치되면등록할수없게만들수있습니다. 그러나이수준의제어를사용하면사용자가개인장치에이렇게많은권한을허용하는것을주저하고등록비율이감소할수있습니다.

인증

인증은사용자환경과많은관련이있는영역입니다. 이미 Active Directory 를실행중인조직에서는 Active Directory 를사용하여시스템에대한사용자액세스를제공하는것이가장간단한방법입니다.

인증사용자환경에서중요한또다른요소는시간초과입니다. 보안수준이높은환경에서는사용자가시스템에액세스할때마다로그온해야하지만일부조직에서는이옵션이적합하지않습니다. 예를들어전자메일에액세스할때마다자격증명을입력하도록하면사용자환경에크게영향을미칠수있습니다.

사용자엔트로피

보안을추가하려면 사용자엔트로피라고하는기능을사용할수있습니다. Citrix Secure Hub 와일부다른앱은암호, PIN 및인증서같은공통데이터를공유하여모든기능이올바르게작동되도록합니다. 이정보는 Secure Hub 의일반저장소에저장됩니다. **Encrypt Secrets(**암호암호화**)** 옵션을통해사용자엔트로피를사용하면 XenMobile 이 UserEntropy 라는이름의새저장소를만듭니다. XenMobile 은이정보를일반저장소에서새저장소로옮깁니다. Secure Hub 또는다른앱에서데이터에액세스하려면사용자가암호또는 PIN 을입력해야합니다.

사용자엔트로피를사용하면여러위치에서인증계층이추가됩니다. 그결과, 사용자는앱이 UserEntropy 저장소에서인증서등의공유데이터에대한액세스를요구할때마다암호또는 PIN 을입력해야합니다.

사용자엔트로피에대한자세한내용은 XenMobile 설명서에서 About the MDX Toolkit(MDX Toolkit 정보)를참조하십시오. 사용자엔트로피를켜려면 클라이언트속성에서관련설정을찾을수있습니다.

정책

MDX 정책과 MDM 정책은조직에많은유연성을제공하지만사용자를제한할수도있습니다. 예를들면 Siri 또는 iCloud 와같이민감한데이터를여러위치로전송할가능성이있는클라우드응용프로그램에대한액세스를차단하는것이좋습니다. 이러한서비스에대한액세스를차단하는정책을설정할수있지만이러한정책으로인해의도치않은결과가발생할수있다는점을고려해야합니다. iOS 키보드마이크에도클라우드액세스가사용되며이기능에대한액세스도차단할수있습니다.

앱

EMM(엔터프라이즈모빌리티관리) 은 MDM(모바일기기관리) 과 MAM(모바일응용프로그램관리) 으로나뉩니다. MDM 은모바일장치의보안및제어에사용되고 MAM 은응용프로그램의제공및관리를용이하게합니다. BYOD 채택이증가하면 MAM 솔루션을구현하여응용프로그램제공, 소프트웨어라이센스, 구성및응용프로그램수명주기관리를지원할수있습니다.

XenMobile 을사용하면특정 MAM 정책및 VPN 설정을구성하여데이터유출및기타보안위협을방지함으로써이러한앱을추가로보호할수있습니다. XenMobile 을사용하면조직에서는다음솔루션중하나를유연하게배포할수있습니다.

- MAM 전용환경
- MDM 전용환경
- 동일한플랫폼에서 MDM 및 MAM 기능을모두제공하는통합 XenMobile 엔터프라이즈환경

모바일장치에앱을제공하는것에더해 XenMobile 은 MDX 기술을통해앱을컨테이너화할수있는기능을제공합니다. MDX 은플랫폼에서제공하는장치수준암호화와는다른암호화를통해앱의보안을확보합니다. 앱을삭제하거나잠글수있으며앱은점진적인정책기반제어의대상이됩니다. ISV(독립소프트웨어공급업체) 는 Mobile Apps SDK 를사용하여이러한제어를적용할수있습니다.

기업환경에서사용자는다양한모바일앱을사용하여업무를지원합니다. 공용앱스토어의앱, 사내에서개발한앱및기본앱이여기에포함될수있습니다. XenMobile 은이러한앱을다음과같이범주화합니다.

공용앱: Apple App Store 또는 Google Play 와같은공용앱스토어에서무료또는유료로제공되는앱이포함됩니다. 조직외부의공급업체는주로공용앱스토어를통해앱을제공합니다. 이옵션을사용하는경우공급업체의고객이인터넷에서직접앱을다운로드할수있습니다. 조직의사용자는사용자요구사항에따라수많은공용앱을사용할수있습니다. 예를들어 GoToMeeting, Salesforce 및 EpicCare 앱이이러한앱에포함됩니다.

Citrix 는공용앱스토어에서직접앱이진을다운로드한다음 MDX Toolkit 을사용하여엔터프라이즈배포용으로래핑하는것을지원하지않습니다. 타사응용프로그램에 MDX 를사용하려면앱공급업체에문의하여앱바이너리를받아야합니다. MDX Toolkit 으로바이너리를래핑하거나바이너리와 MAM SDK 를통합할수있습니다.

사내앱: 많은조직이사내개발자를통해특정기능을제공하는앱을만듭니다. 사내개발자는조직내에서이러한앱을독립적으로개발하고배포합니다. 경우에따라일부조직에서는 ISV 가제공하는앱을사용하기도합니다. 이러한앱을기본앱으로배포하거나 XenMobile 같은 MAM 솔루션을사용하여앱을컨테이너화할수있습니다. 예를들어의료조직에서는의사가모바일장치에서환자정보를볼수있도록하는사내앱을만들수있습니다. 그런다음조직에서는앱에 MAM SDK 를사용하거나 MDM 를래핑하여환자정보를보호하고백엔드환자데이터베이스서버에대한 VPN 액세스를지원할수있습니다.

웹및 **SaaS** 앱**:** 내부네트워크에서액세스되는앱 (웹앱) 또는공용네트워크를통해액세스되는앱 (SaaS) 이포함됩니다. XenMobile 에서는앱커넥터목록을사용하여사용자지정웹및 SaaS 앱을만들수도있습니다. 이러한앱커넥터를사용하면기존웹앱에대한 SSO(Single Sign-on) 를쉽게구현할수있습니다. 자세한내용은 앱커넥터유형을참조하십시오. 예를들어 Google Apps 에대한 SAML(Security Assertion Markup Language) 기반 SSO 에는 Google Apps SAML 을사용할수있습니다.

모바일생산성앱**:** Citrix 에서개발한앱으로, XenMobile 라이센스에포함됩니다. 자세한내용은 모바일생산성앱정보를참조하십시오. 또한 Citrix 는다른 ISV 에서 Worx App SDK 를사용하여개발하는다른 비즈니스용앱을제공합니다.

HDX 앱**:** Windows 에서호스트되는앱으로, StoreFront 를사용하여게시합니다. Citrix Virtual Apps and Desktops 환경이있는경우이러한앱을 XenMobile 과통합하여등록된사용자에게앱을제공할수있습니다.

XenMobile 을사용하여배포하고관리하려는모바일앱의유형에따라기본구성과아키텍처가달라집니다. 예를들어권한수준이서로다른여러사용자그룹이단일앱을사용하려는경우개별배달그룹을만들어앱의두가지버전을배포할수있습니다. 또한사용자장치에서정책불일치가발생하지않도록사용자그룹구성원자격이상호배타적인지확인해야합니다.

Apple 볼륨구매를사용하여 iOS 응용프로그램라이센스를관리하는것이좋을수도있습니다. 이옵션을사용하려면 Apple 볼륨구매에등록하고 XenMobile 콘솔에서 XenMobile 볼륨구매설정을구성해서볼륨구매라이센스로앱을배포해야합니다. 이와같은다양한활용사례에서는 XenMobile 환경을구현하기전에 MAM 전략을평가하고계획하는것이중요합니다. MAM 전략을계획하려면먼저다음을정의합니다.

앱유형 - 지원하려는서로다른유형의앱을나열하고범주화합니다. 예를들면, 공용, 기본, 모바일생산성앱, 웹, 사내, ISV, 앱등이있습니다. 또한서로다른장치플랫폼 (예: iOS 및 Android) 에대한앱을범주화합니다. 이러한범주화는각앱유형에필요한 XenMobile 설정을조정하는데유용합니다. 예를들어, 특정앱은래핑할수없거나다른앱과의인터랙션을위해특수한 API 를지원하는 Mobile Apps SDK 가필요할수있습니다.

네트워크요구사항**:** 특정네트워크액세스요구사항및적절한설정으로앱을구성합니다. 예를들어, 특정앱은 VPN 을통해내부네트워크에액세스해야할수있습니다. 일부앱은 DMZ 를통해인터넷액세스를라우팅해야할수있습니다. 이러한앱에서필요한네트워크에연결할수있으려면다양한설정을적절히구성해야합니다. 앱별네트워크요구사항을정의하면아키텍처의사결정이조기에확정되므로전체구현프로세스가간소화됩니다.

보안요구사항**:** 개별앱또는모든앱에적용할보안요구사항을정의하는것은중요합니다. 이러한계획을통해 XenMobile Server 설치시올바른구성을만들수있습니다. MDX 정책과같은설정은개별앱에적용하더라도세션및인증설정은모든앱에적용됩니다. 일부앱에는배포의간소화를위해사전에개괄적으로살펴볼수있는구체적인암호화, 컨테이너화, 래핑, 암호화, 인증, 지오펜싱, 암호또는데이터공유요구사항이있을수있습니다.

배포요구사항**:** 정책기반배포를사용하면규정을준수하는사용자만게시된앱을다운로드하도록허용할수있습니다. 예를들어, 특정앱에서다음중하나를요구하길원할수있습니다.

- 플랫폼기반장치암호화사용설정됨
- 장치가관리됨
- 장치가최소운영체제버전을충족함
- 특정앱이기업사용자에게만제공됨

또한특정앱을회사사용자에게만제공할수도있습니다. 이러한요구사항을사전에간략히정의해야적절한배포규칙또는동작을구성할수있습니다.

라이센스요구사항**:** 앱관련라이센스요구사항을기록합니다. 이러한메모는라이센스사용현황을효과적으로관리하고, XenMobile 에서라이센스를용이하게하는특정기능을구성할지여부를결정하는데도움이됩니다. 예를들어무료또는유료 iOS 앱을배포할경우 Apple 에서는사용자가반드시 iTunes 계정에로그인하도록하여해당앱에라이센스요구사항을실행합니다. Apple 볼륨구매에등록하면이러한앱을 XenMobile 을통해배포하고관리할수있습니다. 볼륨구매를사용하면사용자가 iTunes 계정에로그인하지않고앱을다운로드할수있습니다. 또한 Samsung SAFE 및 Samsung Knox 같은도구에는기능을배포하기전에완료해야하는특수한라이센스요구사항이있습니다.

허용목록및차단목록요구사항**:** 사용자가일부앱을설치하거나사용하지못하도록할수있습니다. 장치를규정위반으로만드는앱의허용목록을만듭니다. 그런다음장치가규정을준수하지않을때트리거할정책을설정합니다. 또한사용은허용되지만어떤이유로차단목록에포함되는앱이존재할수있습니다. 이경우허용목록에앱을추가하고, 앱을사용할수있지만필수는아님을나타낼수있습니다. 또한새장치에미리설치된앱에는운영체제의일부는아니지만자주사용되는앱이포함될수있습니다. 이러한앱은차단목록전략과충돌할수있습니다.

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.
- **Citrix Files:** 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 로호스트된응용프로그램을열때사용하는모바일앱입니다.
- **GoToMeeting:** 사용자가다른컴퓨터사용자, 고객, 클라이언트또는동료와인터넷을통해실시간으로만날수있도록하는온라인모임, 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 스마트폰을통해시간과장소에관계없이 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
Citrix Files	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	**VPN** 필요	상호작용	상호작용	플랫폼기반장치암호화
		(컨테이너외부의앱과상호작용**)**	**(**컨테이너외부의앱에서상호작용**)**	
————	—	————————	————————	————
Secure Mail	예	선택적으로허용	허용	필요없음
Secure Web	예	허용	허용	필요없음
Citrix Files	예	허용	허용	필요없음
Secure Hub	예	해당없음	해당없음	해당없음
Citrix Receiver	예	해당없음	해당없음	해당없음
GoToMeeting	아니요	해당없음	해당없음	해당없음
SalesForce1	아니요	해당없음	해당없음	해당없음
RSA SecurID	아니요	해당없음	해당없음	해당없음
Epic Haiku	예	해당없음	해당없음	해당없음
Epic Canto	예	해당없음	해당없음	해당없음
Epic Rover	예	해당없음	해당없음	해당없음
Epic Hyperspace	예	해당없음	해당없음	해당없음
Vocera	예	차단됨	차단됨	필요없음
HCMail	예	차단됨	차단됨	필수
PatientRounding	예	해당없음	해당없음	필수
Outlook Web Access	예	해당없음	해당없음	필요없음
SharePoint	예	해당없음	해당없음	필요없음

앱이름	프록시필터링	라이센스	지오펜스	**Mobile Apps SDK**	최소운영체제버전
Secure Mail	필수	해당없음	선택적으로필요	해당없음	적용
Secure Web	필수	해당없음	필요없음	해당없음	적용
Citrix Files	필수	해당없음	필요없음	해당없음	적용

앱이름	프록시필터링	라이센스	지오펜스	**Mobile Apps SDK**	최소운영체제버전
Secure Hub	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
Citrix Receiver	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
GoToMeeting	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
SalesForce1	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
RSA SecurID	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
Epic Haiku	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
Epic Canto	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
Epic Rover	필요없음	볼륨구매	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. 이러한사용자커뮤니티는사용자의모바일장치를통해제공되는다양한리소스를사용하여서로다른작업및사무기능을수행합니다. 사용자는관리자가제공한모바일장치를사용하여재택근무를하거나원격사무실에서근무할수있습니다. 또는개인모바일장치를사용하여특정보안규정준수규칙이적용되는도구에액세스할수있습니다.

모바일장치를사용하는사용자커뮤니티가많아지면 EMM(엔터프라이즈모빌리티관리) 을통해데이터유출을방지하고보안제한을시행해야합니다. 관리자는효율적이고정교한모바일기기관리를위해사용자커뮤니티를범주화할수있습니다. 이렇게하면사용자를리소스에매핑하는작업이간소화되고올바른보안정책을해당하는사용자에게적용할수있습니다.

다음예는의료조직의사용자커뮤니티를 EMM 용으로분류하는방법을설명합니다.

사용자커뮤니티사용사례

이예의의료조직은기술리소스및액세스권한을다수의사용자 (예: 네트워크및계열사직원및자원봉사자) 에게제공합니다. 조직은 EMM 솔루션을일반사용자에게만롤아웃하기로선택했습니다.

이조직의사용자역할및기능은임상, 비임상및계약업체를포함하는하위그룹으로분류될수있습니다. 선택한사용자집합에는회사모바일장치가제공되고다른사용자집합은개인장치에서제한된회사리소스에액세스할수있습니다. 적절한수준의보안제한을적용하고데이터유출을방지하기위해조직은회사 IT 부서를통해회사에서제공하거나 BYOD 인각등록장치를관리하기로결정했습니다. 또한사용자는단일장치만등록할수있습니다.

다음섹션에는각하위그룹의역할및기능에대한개요가나와있습니다.

임상

- 간호사
- 의사 (진료의, 외과의등)
- 전문가 (영양사, 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, 환자액세스솔루션, 매출주기솔루션등다양한건강관리, 관리서비스및비즈니스프로세스공급자솔루션을수행하는사무실근로자)
- 지원서비스 (복리후생관리, 임상통합, 커뮤니케이션, 보상및실적관리, 설비및부동산서비스, HR 기술시스템, 정보서비스, 내부감사및프로세스개선등다양한비임상기능을수행하는사무실근로자)
- 자선프로그램 (자선프로그램지원과관련된다양한기능을수행하는사무실및모바일근로자)

계약업체

- 제조업체및공급업체파트너 (내부에서근무하거나사이트간 VPN 을통해원격으로연결하여다양한비임상지원기능을제공)

이조직에서는위의정보를바탕으로다음과같은엔터티를만들었습니다. XenMobile 의배달그룹에대한자세한내용은 리소스배포를참조하십시오.

Active Directory OU(조직구성단위**)** 및그룹

OU = XenMobile 리소스인경우:

- 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
- 임상의사
- 임상전문가
- 임상외부의사
- 임상가정건강서비스
- 임상연구전문가
- 임상교육및훈련
- 비임상공유서비스
- 비임상의사서비스
- 비임상지원서비스
- 비임상자선프로그램

배달그룹과사용자그룹매핑

Active Directory 그룹	**XenMobile** 배달그룹

XM 간호사	임상간호사
XM 의사	임상의사
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. 첫번째표는모바일앱할당을보여줍니다. 두번째표는공용앱, 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 Hyperspace**	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. 자세한내용

은 서버속성을참조하십시오.

- SQL Server 데이터베이스의 dbo.userlistgrps 아래에서항목을삭제하여 XenMobile 배달그룹에서사용자그룹을삭제할수있습니다.
  주의**:** 이동작을수행하기전에 XenMobile 및데이터베이스의백업을만드십시오.

XenMobile 의장치소유권정보

사용자장치의소유자에따라사용자를그룹화할수있습니다. 장치소유권에는회사소유장치와 BYOD(Bring Your Own Device) 라고하는사용자소유장치가포함됩니다. XenMobile 콘솔의 설정페이지에서각리소스유형의배포규칙과서버속성을통해 BYOD 장치의네트워크연결방법을제어할수있습니다. 배포규칙에대한자세한내용은 XenMobile 설명서에서 배포규칙구성을참조하십시오. 서버속성에대한자세한내용은 서버속성을참조하십시오.

앱에액세스하려는모든 BYOD 사용자에게회사의장치관리에대한동의를요구할수있습니다. 또는장치관리를요구하지않고회사앱에대한액세스권한을제공할수있습니다.

서버설정 **wsapi.mdm.required.flag** 를 **true** 로설정하면 XenMobile 이모든 BYOD 장치를관리하며등록을거부하는사용자는앱액세스가거부됩니다. 엔터프라이즈 IT 팀이보안을강화하는동시에사용자에게긍정적인사용자환경을조성해야한다면 XenMobile 에서사용자장치를등록할때 **wsapi.mdm.required.flag** 를 **true** 로설정하는방안을고려하십시오.

wsapi.mdm.required.flag 를기본설정인 **false** 로유지하면사용자가등록을거부할수있지만사용자는장치에서 XenMobile Store 를통해앱에액세스할수있습니다. 장치관리없이엔터프라이즈앱관리만으로개인정보보호, 법적또는규제제한을준수할수있는환경에서는 **wsapi.mdm.required.flag** 를 **false** 로설정하는것이좋습니다.

XenMobile 을통해관리되지않는장치의사용자는 XenMobile Store 를통해앱을설치할수있습니다. 선택적초기화또는전체초기화같은장치수준제어대신앱정책을사용하여앱액세스를제어할수있습니다. 설정한값에따라정책은장치에서주기적으로 XenMobile Server 에연결하여앱실행이허용되는지여부를확인해야합니다.

보안요구사항

XenMobile 환경을배포할때의보안고려사항은그수가급속도로많아질수있습니다. 서로맞물린항목과설정이많습니다. 허용되는수준의보호를시작하고선택할수있도록지원하기위해 Citrix 에서는다음표에간략히설명된바와같이높은수준의보안, 더높은수준의보안및가장높은수준의보안에대한권장사항을제공합니다.

배포모드선택에는보안우려사항이상의요소가개입됩니다. 또한배포모드를선택하기전에사용사례의요구사항을검토하고보안고려사항을완화할수있는지여부를결정해야합니다.

높음**:** 이러한설정을사용하면최적의사용자환경을제공하면서대부분의조직에허용되는기본적인수준의보안을유지할수있습니다.

더높음**:** 이러한설정은보안과사용편의성간에더적절한균형을잡습니다.

가장높음**:** 이러한권장사항을따르면사용편의성및사용자채택을포기하고높은수준의보안을제공할수있습니다.

배포모드보안고려사항

다음표에는각보안수준에대한배포모드가명시되어있습니다.

높은수준의보안	더높은수준의보안	최고수준의보안
MAM 또는 MDM	MDM+MAM	MDM+MAM 및 FIPS

참고:

- 사용사례에따라 MDM 전용또는 MAM 전용배포로보안요구사항을충족하고우수한사용자환경을제공할수있습니다.
- 앱컨테이너화, Micro VPN 또는앱별정책이필요하지않은경우 MDM 만으로도충분히장치를관리하고보호할수있습니다.
- 앱컨테이너화만으로도모든비즈니스및보안요구사항을충족할수있는 BYOD 와같은사용사례의경우 Citrix 에서는 MAM 전용모드를권장합니다.
- 보안수준이높은환경 (및회사에서발행한장치) 에서는 MDM+MAM 모드를사용하여제공되는모든보안기능을활용하는것이좋습니다. MDM 등록을실행해야합니다.
- FIPS 옵션은정부기관처럼가장높은보안수준이요구되는환경을위한옵션입니다.

FIPS 모드를사용하는경우 SQL 트래픽을암호화하도록 SQL Server 를구성해야합니다.

Citrix ADC 및 **Citrix Gateway** 보안고려사항

다음표에는각보안수준에대한 Citrix ADC 및 Citrix Gateway 권장사항이명시되어있습니다.

높은수준의보안	더높은수준의보안	최고수준의보안
Citrix ADC 를사용하는것이좋습니다. MAM 및 ENT 의경우 Citrix Gateway 가필요하며 MDM 의경우 권장됩니다.	XenMobile 이 DMZ 에있는경우 SSL 브리지가지원되는 XenMobile 용표준 Citrix ADC 마법사구성이권장됩니다. XenMobile Server 가내부네트워크에있는경우보안표준을충족해야한다면 SSL 오프로드를사용합니다.	SSL 오프로드및종단간암호화

참고:

- MDM 의경우 NAT 또는기존타사프록시및부하분산장치를통해 XenMobile Server 를인터넷에노출할수있습니다. 그러나이설정을사용하면 SSL 트래픽이 XenMobile Server 에서종료되어야하며이로인해보안위험이제기될수있습니다.
- 보안수준이높은환경에서기본 XenMobile 구성의 Citrix ADC 는일반적으로보안요구사항을충족하거나초과합니다.
- 보안요구사항이가장높은 MDM 환경에서는 Citrix ADC 에서 SSL 을종료하여경계에서트래픽을검사하고종단간 SSL 암호화를유지할수있습니다.
- 필요한경우 SSL/TLS 암호화를정의할수있습니다.

- SSL FIPS Citrix ADC 하드웨어도사용할수있습니다.
- 자세한내용은 Citrix Gateway 및 Citrix ADC 통합을참조하십시오.

등록보안고려사항

다음표에는각보안수준에대한 Citrix ADC 및 Citrix Gateway 권장사항이명시되어있습니다.

높은수준의보안	더높은수준의보안	최고수준의보안
Active Directory 그룹구성원자격만사용됩니다. 모든사용자배달그룹은사용되지않습니다.	초대전용등록보안모드를사용합니다. Active Directory 그룹구성원자격만사용됩니다. 모든사용자배달그룹은사용되지않습니다.	장치 ID 에연결된등록보안모드를사용합니다. Active Directory 그룹구성원자격만사용됩니다. 모든사용자배달그룹은사용되지않습니다.

참고:

- 일반적으로, 미리정의된 Active Directory 그룹의사용자로만등록을제한하는것이좋습니다. 이설정에서는기본제공되는모든사용자배달그룹을비활성화해야합니다.
- 등록초대를사용하여초대를받은사용자로등록을제한할수있습니다. Windows 장치에서는등록초대를사용할수없습니다.
- OTP(일회용 PIN) 등록초대를 2 단계인증솔루션으로사용하고사용자가등록할수있는장치수를제어할수있습니다. Windows 장치에서는 OTP 초대를사용할수없습니다.

장치암호보안고려사항

다음표에는각보안수준에대한장치암호권장사항이명시되어있습니다.

높은수준의보안	더높은수준의보안	최고수준의보안
권장됩니다. 장치수준암호화에는높은수준의보안이필요합니다. MDM 을사용하여적용됩니다. MDX 정책, 정책비준수장치동작을사용하여 MAM 전용에대한필수로높은보안을설정할수있습니다.	MDM, MDX 정책또는둘다를사용하여적용됩니다.	MDM 및 MDX 정책을사용하여적용됩니다. MDM 복잡한암호정책.

참고:

- Citrix 는장치암호의사용을권장합니다.

- 장치암호는 MDM 정책을통해적용할수있습니다.
- MDX 정책을사용하여장치암호를관리되는앱사용을위한요구사항중하나로만들수있습니다. BYOD 사용사례를예로들수있습니다.
- MDM 과 MDX 정책옵션을결합하여 MDM+MAM 환경의보안을강화하는것이좋습니다.
- 보안요구사항이가장높은환경에서는복잡한암호정책을구성하고 MDM 을통해적용할수있습니다. 장치가암호정책을준수하지않는경우관리자에게알리거나선택적/전체장치초기화를실행하는자동화된동작을구성할수있습니다.

앱

August 24, 2022

EMM(엔터프라이즈모빌리티관리) 은 MDM(모바일기기관리) 과 MAM(모바일응용프로그램관리) 으로나뉩니다. MDM 은모바일장치의보안및제어에사용되고 MAM 은응용프로그램의제공및관리를용이하게합니다. BYOD 채택을지원하기위해보통 XenMobile 과같은 MAM 솔루션을구현하여다음을지원할수있습니다.

- 응용프로그램제공
- 소프트웨어라이선싱
- 구성
- 응용프로그램수명주기관리

사용자가 MDM 관리도선택하도록요구또는허용할수있습니다.

XenMobile 을사용하면특정 MAM 정책및 VPN 설정을구성하여데이터유출및기타보안위협을방지함으로써이러한앱을추가로보호할수있습니다. XenMobile 을사용하면조직에서는솔루션을다음으로유연하게배포할수있습니다.

- MAM 전용환경
- MDM 전용환경
- MDM 및 MAM 기능을모두제공하는통합 XenMobile 엔터프라이즈환경

모바일장치에앱을제공하는것에더해 XenMobile 은 MDX 기술을통해앱을컨테이너화할수있는기능을제공합니다. 앱은점진적인정책기반제어의대상이됩니다. ISV(독립소프트웨어공급업체) 는 Mobile Apps SDK 를사용하여이러한제어를적용할수있습니다.

기업환경에서사용자는다양한모바일앱을사용하여업무를지원합니다. 공용앱스토어의앱, 사내에서개발한앱또는기본앱이여기에포함될수있습니다. XenMobile 은이러한앱을다음과같이범주화합니다.

- 공용앱**:** Apple App Store 또는 Google Play 와같은공용앱스토어에서무료또는유료로제공되는앱이포함됩니다. 조직외부의공급업체는주로공용앱스토어를통해앱을제공합니다. 이옵션을사용하는경우공급업체의고객이인터넷에서직접앱을다운로드할수있습니다. 조직의사용자는사용자요구사항에따라수많은공용앱을사용할수있습니다. 예를들어 GoToMeeting, Salesforce 및 EpicCare 앱이이러한앱에포함됩니다.
  - **MAM SDK** 를사용하는경우**:** 앱공급업체로부터앱바이너리를확보합니다. 그런다음 MAM SDK 를앱에통합합니다.

  - **MDX Toolkit** 을사용하는경우**:** Citrix 는공용앱스토어에서직접앱이진을다운로드한다음 MDX Toolkit 을사용하여엔터프라이즈배포용으로래핑하는것을지원하지않습니다. 타사응용프로그램을래핑하려면앱공급업체를통해앱바이너리를받아야합니다. 이후에 MDX Toolkit 을사용하여바이너리를래핑할수있습니다.

- 사내앱**:** 많은조직이사내개발자를통해특정기능을제공하는앱을만듭니다. 사내개발자는조직내에서이러한앱을독립적으로개발하고배포합니다. 경우에따라일부조직에서는 ISV 가제공하는앱을사용하기도합니다. 이러한앱을기본앱으로배포하거나 XenMobile 같은 MAM 솔루션을사용하여앱을컨테이너화할수있습니다.

  예를들어의료조직에서는의사가모바일장치에서환자정보를볼수있도록하는사내앱을만들수있습니다. 그러면조직에서는다음중하나를사용하여환자정보의보안을확보하고환자데이터베이스에대한 VPN 액세스를설정할수있습니다.

  - MAM SDK
  - MDX Toolkit

- 웹및 **SaaS** 앱**:** 내부네트워크에서액세스되는앱 (웹앱) 또는공용네트워크를통해액세스되는앱 (SaaS) 이포함됩니다. XenMobile 에서는앱커넥터목록을사용하여사용자지정웹및 SaaS 앱을만들수도있습니다. 이러한앱커넥터를사용하면기존웹앱에대한 SSO(Single Sign-on) 를쉽게구현할수있습니다. 자세한내용은 앱커넥터유형을참조하십시오. 예를들어 Google Apps 에대한 SAML(Security Assertion Markup Language) 기반 SSO 에는 Google Apps SAML 을사용할수있습니다.

- 모바일생산성앱**:** 모바일생산성앱은 Citrix 에서개발한앱으로, XenMobile 라이센스에포함됩니다. 자세한내용은 모바일생산성앱정보를참조하십시오. 또한 Citrix 는다른 ISV 에서 Worx App SDK 를사용하여개발하는다른 비즈니스용앱을제공합니다.

- **HDX** 앱**:** HDX 앱은 Windows 에서호스트되는앱으로, StoreFront 를사용하여게시합니다. Citrix Virtual Apps and Desktops 와 Citrix Workspace 를사용한다면 HDX 앱이등록된사용자에게제공됩니다.

XenMobile 을사용하여배포하고관리하려는모바일앱의유형에따라기본구성이달라질수있습니다. 예를들어, 권한수준이다른여러사용자그룹이단일앱을사용할수있습니다. 이경우개별배달그룹을만들어동일한앱의두가지개별버전을배포할수있습니다. 또한사용자장치에서정책불일치가발생하지않도록사용자그룹구성원자격이상호배타적인지확인해야합니다.

Apple 볼륨구매를사용하여 iOS 응용프로그램라이센스를관리할수도있습니다. 이옵션을사용하려면볼륨구매프로그램에등록하고 XenMobile 콘솔에서볼륨구매설정을구성해야합니다. 이구성을사용하면볼륨구매라이센스로앱을배포할수있습니다. 이와같은다양한활용사례에서는 XenMobile 환경을구현하기전에 MAM 전략을평가하고계획하는것이중요합니다. MAM 전략을계획하려면먼저다음을정의합니다.

- 앱유형 - 지원하려는서로다른유형의앱을나열하고공용, 기본, 웹, 사내, ISV 앱으로앱을범주화합니다. 또한서로다른장치플랫폼 (예: iOS 및 Android) 에대한앱을범주화합니다. 이러한범주화는각앱유형에필요한여러 XenMobile 설정을조정하는데유용합니다. 예를들어일부앱의경우 Mobile Apps SDK 로다른앱과의상호작용을위한특수 API 를사용하도록설정해야할수있습니다.

- 네트워크요구사항**:** 특정네트워크액세스요구사항이있는앱설정을구성합니다. 예를들어, 특정앱은 VPN 을통해내부네트워크에액세스해야할수있습니다. 일부앱은 DMZ 를통해인터넷액세스를라우팅해야할수있습니다. 이러한앱에서필요한네트워크에연결할수있으려면다양한설정을적절히구성해야합니다. 앱별네트워크요구사항을정의하면아키텍처의사결정이조기에확정되므로전체구현프로세스가간소화됩니다.

- 보안요구사항**:** 개별앱또는모든앱에적용할보안요구사항을정의할수있습니다.

  - MDX 정책과같은설정은개별앱에적용됩니다.
  - 세션및인증설정은모든앱에적용됩니다.
  - 일부앱에는구체적인컨테이너화, MDX, 인증, 지오펜싱, 암호또는데이터공유요구사항이있을수있습니다.

  사전에이러한요구사항을개략적으로설명하면배포를간소화할수있습니다. Endpoint Management 의보안에대한자세한내용은 보안및사용자환경을참조하십시오.

- 배포요구사항 - 정책기반배포를사용하면규정을준수하는사용자만게시된앱을다운로드하도록허용할수있습니다. 예를들어특정앱에서는장치가관리되거나장치가최소운영체제버전을충족해야할수있습니다. 또한특정앱을회사사용자에게만제공할수있습니다. 이러한요구사항을사전에간략히정의해야적절한배포규칙또는동작을구성할수있습니다.

- 라이센스요구사항**:** 앱관련라이센스요구사항을기록합니다. 이러한메모는라이센스사용현황을효과적으로관리하고, XenMobile 에서라이센스를용이하게하는특정기능을구성할지여부를결정하는데도움이됩니다. 예를들어무료또는유료 iOS 앱을배포할경우 Apple 에서는해당앱에라이센스요구사항을실행합니다. 그결과, 사용자는반드시 Apple App Store 계정에로그인해야합니다.

  그러나, Apple 볼륨구매에등록하면이러한앱을 XenMobile 로배포하고관리할수있습니다. 볼륨구매를사용하면사용자가 Apple App Store 계정에로그인하지않고앱을다운로드할수있습니다.

  또한 Samsung SAFE, Samsung Knox 같은일부플랫폼에는기능을배포하기전에완료해야하는특수한라이센스요구사항이있습니다.

- 허용목록및차단목록요구사항**:** 사용자가설치또는사용하지않아야할앱을식별할수있습니다. 차단목록을만들면규정위반이벤트가정의됩니다. 그런다음이러한이벤트발생시트리거할정책을설정할수있습니다. 또한사용은허용되지만어떤이유로차단목록에포함되는앱이존재할수있습니다. 이경우허용목록에앱을추가하고, 앱을사용할수있지만필수는아님을나타낼수있습니다. 또한새장치에미리설치된앱에는운영체제의일부는아니지만자주사용되는앱이포함될수있습니다. 이러한앱은차단목록전략과충돌할수있습니다.

사용사례

한의료조직에서 XenMobile 을배포하여모바일앱의 MAM 솔루션으로사용하려고합니다. 모바일앱은회사및 BYOD 사용자에게제공됩니다. IT 부서에서는다음앱을제공하고관리하기로결정합니다.

모바일생산성앱**:** Citrix 가제공하는 iOS 및 Android 앱입니다. 자세한내용은 모바일생산성앱을참조하십시오.

Citrix Secure Hub: XenMobile 과통신하는모든모바일장치에사용되는클라이언트입니다. Secure Hub 로보안설정, 구성및모바일앱을모바일장치에푸시합니다. Android 및 iOS 장치는 Secure Hub 를통해 XenMobile 에등록됩니다.

Citrix Receiver: 모바일장치사용자가 Citrix Virtual Apps 로호스트된응용프로그램을열때사용하는모바일앱입니다.

GoToMeeting: 사용자가다른컴퓨터사용자, 고객, 클라이언트또는동료와인터넷을통해실시간으로만날수있도록하는온라인모임, 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 에서 HDX 앱을제공합니다.

- **Epic Hyperspace:** 전자의료기록관리를위한 Epic 클라이언트응용프로그램입니다.

ISV:

- **Vocera:** HIPAA 준수 VoIP(Voice-over IP) 및메시징모바일앱으로, iPhone 및 Android 스마트폰을통해시간과장소에관계없이 Vocera 음성기술의이점을활용할수있도록합니다.

사내앱**:**

- **HCMail:** 암호화된메시지를작성하고, 내부메일서버의주소록을검색하고, 암호화된메시지를전자메일클라이언트를사용하여연락처로보내는데유용한앱입니다.

사내웹앱**:**

- **PatientRounding:** 여러부서에서환자건강정보를기록하는데사용되는웹응용프로그램입니다.
- **Outlook Web Access:** 웹브라우저를통해전자메일에액세스할수있습니다.
- **SharePoint:** 조직전체의파일및데이터공유에사용됩니다.

다음표에는 MAM 구성에필요한기본정보가나와있습니다.

앱이름	앱유형	**MAM SDK** 통합또는 **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
Citrix Files	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	**VPN** 필요	상호작용 **(**컨테이너 외부앱과 의상호작용**)**	상호작용 **(**컨테이너 외부앱에 서의상호작용**)**	프록시필터링	라이센싱	지오펜스	**Mobile Apps SDK**	최소운영체제버전
Secure Mail	예	선택적으로허용	허용	필수	해당없음	선택적으로필요	해당없음	적용
Secure Web	예	허용	허용	필수	해당없음	필요없음	해당없음	적용
Citrix Files	예	허용	허용	필수	해당없음	필요없음	해당없음	적용
Secure Hub	예	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
Citrix Re-ceiver	예	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
GoToMeeting	아니요	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지않음
SalesForc	아니요	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지않음

앱이름	**VPN** 필요	상호작용 **(**컨테이너 외부앱과 의상호작용**)**	상호작용 **(**컨테이너 외부앱에서의상호작용**)**	프록시필터링	라이센싱	지오펜스	**Mobile Apps SDK**	최소운영체제버전
RSA SecurID	아니요	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지 않음
Epic Haiku	예	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지 않음
Epic Canto	예	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지 않음
Epic Rover	예	해당없음	해당없음	필요없음	볼륨구매	필요없음	해당없음	적용되지 않음
Epic Hyper-space	예	해당없음	해당없음	필요없음	해당없음	필요없음	해당없음	적용되지 않음
Vocera	예	차단됨	차단됨	필수	해당없음	필수	필수	적용
HCMail	예	차단됨	차단됨	필수	해당없음	필수	필수	적용
PatientRc ing	예	해당없음	해당없음	필수	해당없음	필요없음	해당없음	적용되지 않음
Outlook Web Access	예	해당없음	해당없음	필수	해당없음	필요없음	해당없음	적용되지 않음
SharePoi	예	해당없음	해당없음	필수	해당없음	필요없음	해당없음	적용되지 않음

사용자커뮤니티

January 5, 2022

모든조직은서로다른기능적역할로운영되는다양한사용자커뮤니티로구성됩니다. 이러한사용자커뮤니티는사용자모바일장치를통해제공되는다양한리소스를사용하여서로다른작업및사무기능을수행합니다. 사용자는관리자가제공한모바일장치를사용하여재택근무를하거나원격사무실에서근무할수있습니다. 또는개인모바일장치를사용하여특정보안규정준수규칙이적용되는도구에액세스할수있습니다.

모바일장치를사용하는사용자커뮤니티가많아지면 EMM(엔터프라이즈모빌리티관리) 을통해데이터유출을방지하고조직의보안

제한을시행해야합니다. 관리자는효율적이고정교한모바일기기관리를위해사용자커뮤니티를범주화할수있습니다. 이렇게하면사용자를리소스에매핑하는작업이간소화되고올바른보안정책을해당하는사용자에게적용할수있습니다.

사용자커뮤니티를범주화하는작업에는다음과같은구성요소가사용됩니다.

- Active Directory OU(조직구성단위) 및그룹

  특정 Active Directory 보안그룹에추가된사용자는정책및리소스 (예: 앱) 를받을수있습니다. Active Directory 보안그룹에서사용자를제거하면이전에허용되었던 XenMobile 리소스에대한액세스권한이제거됩니다.

- XenMobile 로컬사용자및그룹

  Active Directory 에계정이없는사용자는로컬 XenMobile 사용자로만들수있습니다. 관리자는로컬사용자를 Active Directory 사용자와동일한방식으로배달그룹에추가하고리소스를프로비전할수있습니다.

- XenMobile 배달그룹

  권한수준이서로다른여러사용자그룹이단일앱을사용하려는경우개별배달그룹을만들어야할수있습니다. 개별배달그룹을사용하면동일한앱의두가지개별버전을배포할수있습니다.

- 배달그룹과사용자그룹매핑

  Active Directory 그룹에대한배달그룹매핑은일대일또는일대다방식일수있습니다. 기본정책및앱을일대다배달그룹매핑에할당합니다. 기능별정책및앱을일대일배달그룹매핑에할당합니다.

- 배달그룹과앱리소스매핑

  특정앱을각배달그룹에할당합니다.

- 배달그룹과 MDM 리소스매핑

  앱및특정장치관리리소스를각배달그룹에할당합니다. 예를들어앱유형 (공용, HDX 및기타), 앱유형별특정앱및리소스 (예: 장치정책및자동화된동작) 를혼합하여배달그룹을구성합니다.

다음예는의료조직의사용자커뮤니티를 EMM 용으로분류하는방법을설명합니다.

사용사례

이예의의료조직은기술리소스및액세스권한을다수의사용자 (예: 네트워크및계열사직원및자원봉사자) 에게제공합니다. 조직은 EMM 솔루션을일반사용자에게만롤아웃하기로선택했습니다.

이조직의사용자역할및기능은임상, 비임상및계약업체를포함하는하위그룹으로나눌수있습니다. 선택한사용자집합에는회사모바일장치가제공되고다른사용자집합은개인장치 (BYOD) 에서제한된회사리소스에액세스할수있습니다. 적절한수준의보안제한을적용하고데이터유출을방지하기위해조직은회사 IT 부서를통해등록된각장치를관리하기로결정했습니다. 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, 환자액세스솔루션, 매출주기솔루션등다양한건강관리, 관리서비스및비즈니스프로세스공급자솔루션을수행하는사무실근로자)
- 지원서비스 (복리후생관리, 임상통합, 커뮤니케이션, 보상및실적관리, 설비및부동산서비스, HR 기술시스템, 정보서비스, 내부감사및프로세스개선등다양한비임상기능을수행하는사무실근로자)
- 자선프로그램 (자선프로그램지원과관련된다양한기능을수행하는사무실및모바일근로자)

계약업체

- 제조업체및공급업체파트너 (내부에서근무하거나사이트간 VPN 을통해원격으로연결하여다양한비임상지원기능을제공)

이조직에서는위의정보를바탕으로다음과같은엔터티를만들었습니다. XenMobile 의배달그룹에대한자세한내용은 XenMobile 제품설명서에서 리소스배포를참조하십시오.

Active Directory OU(조직구성단위**)** 및그룹

OU = XenMobile 리소스인경우

- 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
- 임상의사
- 임상전문가
- 임상외부의사
- 임상가정건강서비스
- 임상연구전문가
- 임상교육및훈련
- 비임상공유서비스
- 비임상의사서비스
- 비임상지원서비스
- 비임상자선프로그램

배달그룹과사용자그룹매핑

Active Directory 그룹	**XenMobile** 배달그룹
XM 간호사	임상간호사
XM 의사	임상의사
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	ShareFile	Receiver	SalesForce	RSA SecurID	EpicCare Haiku	Epic Hyperspace
임상간호사	X	X	X					
임상의사								
임상전문가								
임상외부의사	X		X					
임상가정건강서비스	X		X					
임상연구전문가	X		X					
임상교육및훈련							X	X
비임상공유서비스							X	X
비임상의사서비스							X	X
비임상지원서비스	X		X				X	X

비임상자 선프로그램	X	X			X	X
계약업체	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. 마찬가지로사용자가여러그룹의구성원인경우 XenMobile 은해당사용자를 XenMobile 에매핑된그룹의구성원으로범주화합니다.
- MDM 등록을필수로규정하려면 XenMobile 콘솔의 서버속성에서 등록필요옵션을 **True** 로설정합니다. 자세한내용은

서버속성을참조하십시오.

- XenMobile 배달그룹에서사용자그룹을삭제하려면 SQL Server 데이터베이스의 dbo.userlistgrps 아래에서항목을삭제합니다.

  > 주의:
  >
  > 이동작을수행하기전에 XenMobile 및데이터베이스의백업을만드십시오.

XenMobile 의장치소유권정보

사용자장치의소유자에따라사용자를그룹화할수있습니다. 장치소유권에는회사소유장치와 BYOD(Bring Your Own Device)라고하는사용자소유장치가포함됩니다. XenMobile 콘솔의 설정페이지에서배포규칙과 XenMobile 서버속성을사용하여 BYOD 장치의네트워크연결방법을제어할수있습니다. 배포규칙에대한자세한내용은 XenMobile 설명서에서 리소스배포를참조하십시오. 서버속성에대한자세한내용은이안내서에서 서버속성을참조하십시오.

앱에액세스하려는모든 BYOD 사용자에게회사의장치관리에대한동의를요구하도록서버속성을설정할수있습니다. 또는장치관리를요구하지않고회사앱에대한액세스권한을제공할수있습니다.

서버속성 **wsapi.mdm.required.flag** 를 **true** 로설정하면 XenMobile 이모든 BYOD 장치를관리하며등록을거부하는사용자는앱액세스가거부됩니다. 엔터프라이즈 IT 팀이보안을강화하는동시에사용자에게개선된등록경험을제공해야한다면 **wsapi.mdm.required.flag** 를 **true** 로설정하는것이좋습니다.

wsapi.mdm.required.flag 를기본설정인 **false** 로유지하면사용자가등록을거부할수있습니다. 그러나사용자는장치에서 XenMobile Store 를통해앱에액세스할수있습니다. 장치관리없이엔터프라이즈앱관리만으로개인정보보호, 법적또는규제제한을준수할수있는환경에서는 **wsapi.mdm.required.flag** 를 **false** 로설정하는것이좋습니다.

XenMobile 을통해관리되지않는장치의사용자는 XenMobile Store 를통해앱을설치할수있습니다. 선택적초기화또는전체초기화같은장치수준제어대신앱정책을사용하여앱액세스를제어할수있습니다. 일부정책설정을사용하려면장치에서주기적으로 XenMobile 서버에연결하여앱실행이허용되는지여부를확인해야합니다.

전자메일전략

January 22, 2021

조직에서모빌리티관리이니셔티브를시행하는주된이유는모바일장치에서전자메일에안전하게액세스할수있도록하기위해서입니다. XenMobile 설계의주요구성요소중하나는올바른전자메일전략을결정하는것입니다. XenMobile 은보안, 사용자환경및통합요구사항에따라다양한사용사례를수용하는다수의옵션을제공합니다. 이문서에서는클라이언트선택부터메일트래픽흐름에이르는올바른솔루션을선택하기위한일반적인설계의사결정프로세스와고려사항에대해다룹니다.

전자메일클라이언트선택

전체전자메일전략을설계할때는일반적으로클라이언트를가장먼저선택합니다. Citrix Secure Mail, 특정모바일플랫폼운영체제에포함되는기본메일또는공용앱스토어를통해제공되는타사클라이언트를포함하는여러클라이언트중에서선택할수있습니다. 요

구사항에따라단일 (표준) 클라이언트를사용하여사용자커뮤니티를지원하거나클라이언트조합을사용해야할수있습니다.

다음표에는사용가능한여러클라이언트옵션에대한몇가지간략한설계고려사항이나와있습니다.

항목	**Secure Mail**	기본 **(예: iOS Mail)**	타사메일
최소 XenMobile 버전	고급	MDM	MDM
구성	MDX 정책을통해구성된 Exchange 계정프로필.	MDM 정책을통해구성된 Exchange 계정프로필. Android 지원은 SAFE/KNOX 및 Android Enterprise 로 제한됩니다. 다른모든클라이언트는타사클라이언트로 간주됩니다.	일반적으로사용자가수동으로구성해야합니다.
보안	설계시부터보안이적용되어 가장높은수준의보안을제공합니다. 데이터암호화수준 이추가된 MDX 정책을사용합니다. Secure Mail 은 MDX 정책을통해완벽하게 관리되는앱입니다. Citrix PIN 을사용하여인증계층을 추가합니다.	공급업체/앱기능집합에따릅니다. 더높은수준의보안을 제공합니다. 장치암호화설정을사용합니다 (MDX 정책을통한보안없음). 앱액세스에대해장치수준인증을사용합니다.	공급업체/앱기능집합에따릅니다. 높은수준의보안을제공합니다.
통합	기본적으로관리되는앱 (MDX) 과의상호작용을허용합니다. Citrix Secure Web 을사용하여웹 URL 을엽니다. 파일저장및첨부 시 Citrix Files 를사용합니다. GoToMeeting 에직접 참여하고전화접속합니다.	기본적으로관리되지않는다른앱 (비 MDX) 과의상호작용만가능합니다.	기본적으로관리되지않는다른앱 (비 MDX) 과의상호작용만가능합니다.
배포/라이센스	공용앱스토어에서 MDM 을통해직접 Secure Mail 을 푸시할수있습니다. XenMobile Advanced 및 Enterprise 라이센스에 포함됩니다.	플랫폼운영체제에포함된클라이언트앱입니다. 추가라이센스요구사항이없습니다.	MDM 을통해엔터프라이즈앱으로푸시하거나공용앱스토어에서직접푸시할수있습니다. 앱공급업체에따라연결된라이센스모델/비용이적용됩니다.

지원	클라이언트및 EMM 솔루션을단일공급업체 (Citrix) 가지원합니다. Secure Hub/앱디버그로깅기능에지원연락처가포함되어있습니다. 하나의클라이언트만지원하면됩니다.	공급업체 (Apple/Google) 가정의한지원을사용할수있습니다. 장치플랫폼에따라여러클라이언트를지원해야할수있습니다.	공급업체가정의한지원을사용할수있습니다. 모든관리되는장치플랫폼에서타사클라이언트가지원된다고가정하면하나의클라이언트만지원하면됩니다.

메일트래픽흐름및필터링고려사항

이섹션에서는 XenMobile 의컨텍스트에서메일 (ActiveSync) 트래픽의흐름과관련된세가지주요시나리오및설계고려사항에대해설명합니다.

시나리오 **1:** 공개된 **Exchange**

일반적으로 Exchange ActiveSync 서비스를인터넷에공개하는외부클라이언트를지원하는환경입니다. 모바일 ActiveSync 클라이언트는이외부대상경로를통해역방향프록시 (예: Citrix ADC) 또는에지서버를사용하여연결합니다. 이옵션은기본또는타사메일클라이언트를사용하려는경우필요하며이시나리오에서이러한클라이언트가주로사용될수있도록합니다. 일반적인사례는아니지만이시나리오에서 Secure Mail 클라이언트를사용할수도있습니다. 이경우앱의 MDX 정책및관리를통해제공되는보안기능을활용할수있습니다.

시나리오 **2: Citrix ADC** 를통해터널링됨 **(Micro VPN** 및 **STA)**

Secure Mail 클라이언트를사용하는경우 Micro VPN 기능을사용하려면이시나리오가기본적으로적용됩니다. 이경우 Secure Mail 클라이언트는 Citrix Gateway 를통해 ActiveSync 에대한보안연결을설정합니다. 기본적으로, Secure Mail 은내부네트워크에서 ActiveSync 에직접연결하는클라이언트로간주될수있습니다. Citrix 고객은 Secure Mail 을모바일 ActiveSync 클라이언트로표준화하는경우가많습니다. 이러한표준화는첫번째시나리오에설명된것과같이공개된 Exchange Server 에서 ActiveSync 서비스가인터넷에공개되는것을방지하기위해수행됩니다.

MAM SDK 사용또는 MDX 래핑앱에서만마이크로 VPN 기능을사용할수있습니다. MDX 래핑을사용하는경우이시나리오는기본클라이언트에적용되지않습니다. 타사클라이언트를 MDX Toolkit 으로래핑할수도있지만일반적인사례는아닙니다. 장치수준 VPN 클라이언트를사용하여기본또는타사클라이언트에대한터널링된액세스를허용하려는솔루션은과정이복잡하고실행가능하지않은것으로검증되었습니다.

시나리오 **3:** 클라우드에서호스트되는 **Exchange** 서비스

클라우드에서호스트되는 Exchange 서비스 (예: Microsoft Office 365) 의인기가높아지고있습니다. XenMobile 의컨텍스트에서이시나리오는첫번째시나리오와동일하게다뤄질수있습니다. ActiveSync 서비스가인터넷에공개되기때문입니다. 이

경우클라우드서비스공급자요구사항에따라클라이언트를선택해야합니다. 일반적으로대부분의 ActiveSync 클라이언트 (예: Secure Mail) 및다른기본또는타사클라이언트를선택할수있습니다.

XenMobile 은이시나리오의세가지영역에서더많은가치를제공합니다.

- Secure Mail 의 MDX 정책및앱관리를사용하는클라이언트
- 지원되는기본이메일클라이언트에서 MDM 정책을사용하여클라이언트구성
- Exchange ActiveSync 용 Endpoint Management 커넥터를사용한 ActiveSync 필터링옵션

메일트래픽필터링고려사항

인터넷에공개되는대부분의서비스와마찬가지로, 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 커넥터는 Citrix ADC 를 ActiveSync 트래픽의프록시로사용하여경계에서 ActiveSync 필터링을제공합니다. 필터링구성요소가메일트래픽흐름의경로에배치되므로메일이환경에들어오거나환경에서나갈때트래픽을가로챕니다. Exchange ActiveSync 용 Citrix Gateway 커넥터는 Citrix ADC 와 XenMobile Server 의중간자역할을합니다. 장치가 Citrix ADC 의 ActiveSync 가상서버를통해 Exchange 와통신하면 Citrix ADC 가 Exchange ActiveSync 용커넥터서비스에대한 HTTP 콜아웃을수행합니다. 그러면이서비스가 XenMobile 을통해장치상태를확인합니다. 장치상태에따라 Exchange ActiveSync 용커넥터는연결허용또는거부에대한회신을 Citrix ADC 로보냅니다. 사용자, 에이전트및장치유형또는 ID 에따라액세스를필터링하는정적규칙을구성할수도있습니다.

이설정을사용하면추가보안계층을통해 Exchange ActiveSync 서비스를인터넷에공개하여허가되지않은액세스를방지할수있습니다. 설계고려사항은다음과같습니다.

- Windows Server: Exchange ActiveSync 용커넥터구성요소를사용하려면 Windows Server 가필요합니다.
- 필터링규칙설정: Exchange ActiveSync 용커넥터는사용자정보가아닌장치상태및정보를바탕으로필터링하도록설계되었습니다. 사용자 ID 로필터링하는정적규칙을구성할수는있지만예를들어 Active Directory 그룹구성원자격으로필터링하는옵션은없습니다. Active Directory 그룹필터링에대한요구사항이있는경우 Exchange ActiveSync 용 Endpoint Management 커넥터를대신사용할수있습니다.
- Citrix ADC 확장성: Citrix ADC 를통한 ActiveSync 트래픽프록시에대한요구사항이있는경우 Citrix ADC 인스턴스크기를올바르게조정하여모든 ActiveSync SSL 연결의추가된작업부하를지원하는것이중요합니다.
- Citrix ADC 통합캐싱: Citrix ADC 의 Exchange ActiveSync 용커넥터구성은통합캐싱기능을사용하여 Exchange ActiveSync 용커넥터의응답을캐싱합니다. 이구성으로인해 Citrix ADC 는지정된세션의모든 ActiveSync 트랜잭션에대한요청을 Exchange ActiveSync 용 Citrix Gateway 커넥터에전송하지않아도됩니다. 이구성은충분한성능및확장성에대해서도중요한역할을합니다. 통합캐싱은 Citrix ADC Platinum Edition 을통해사용하거나 Enterprise Edition 의기능에대한라이센스를개별적으로취득할수있습니다.

- 사용자지정필터링정책: 사용자지정 Citrix ADC 정책을만들어표준의기본모바일클라이언트외의특정 ActiveSync 클라이언트를제한해야할수있습니다. 이구성을사용하려면 ActiveSync HTTP 요청및 Citrix ADC 응답자정책만들기에대한지식이있어야합니다.
- Secure Mail 클라이언트: Secure Mail 에는 Micro VPN 기능이있습니다. 이기능을사용하면경계에서필터링을수행하지않아도됩니다. Secure Mail 클라이언트는 Citrix Gateway 를통해연결되는경우일반적으로내부 (신뢰할수있는) ActiveSync 클라이언트로여겨집니다. 기본및타사 (Exchange ActiveSync 용커넥터포함) 클라이언트와 Secure Mail 클라이언트를모두지원해야합니다. Secure Mail 트래픽은 Exchange ActiveSync 용커넥터에사용된 Citrix ADC 가상서버를통하지않는것이좋습니다. 이트래픽이 DNS 를통해흐르도록하고 Exchange ActiveSync 용커넥터정책이 Secure Mail 클라이언트에영향을미치지않도록할수있습니다.

XenMobile 배포의 Exchange ActiveSync 용 Citrix Gateway 커넥터다이어그램은 온-프레미스배포용참조아키텍처를 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 커넥터와마찬가지로 Exchange ActiveSync 용 Endpoint Management 커넥터는 XenMobile 을통해장치상태를확인하여장치규정준수에따라액세스를필터링합니다. 장치유형또는 ID, 에이전트버전및 Active Directory 그룹구성원자격에따라액세스를필터링하는정적규칙을구생할수도있습니다.

이솔루션에는 Citrix ADC 의사용이필요하지않습니다. 기존 ActiveSync 트래픽의라우팅을변경하지않고 Exchange ActiveSync 용 Endpoint Management 커넥터를배포할수있습니다. 설계고려사항은다음과같습니다.

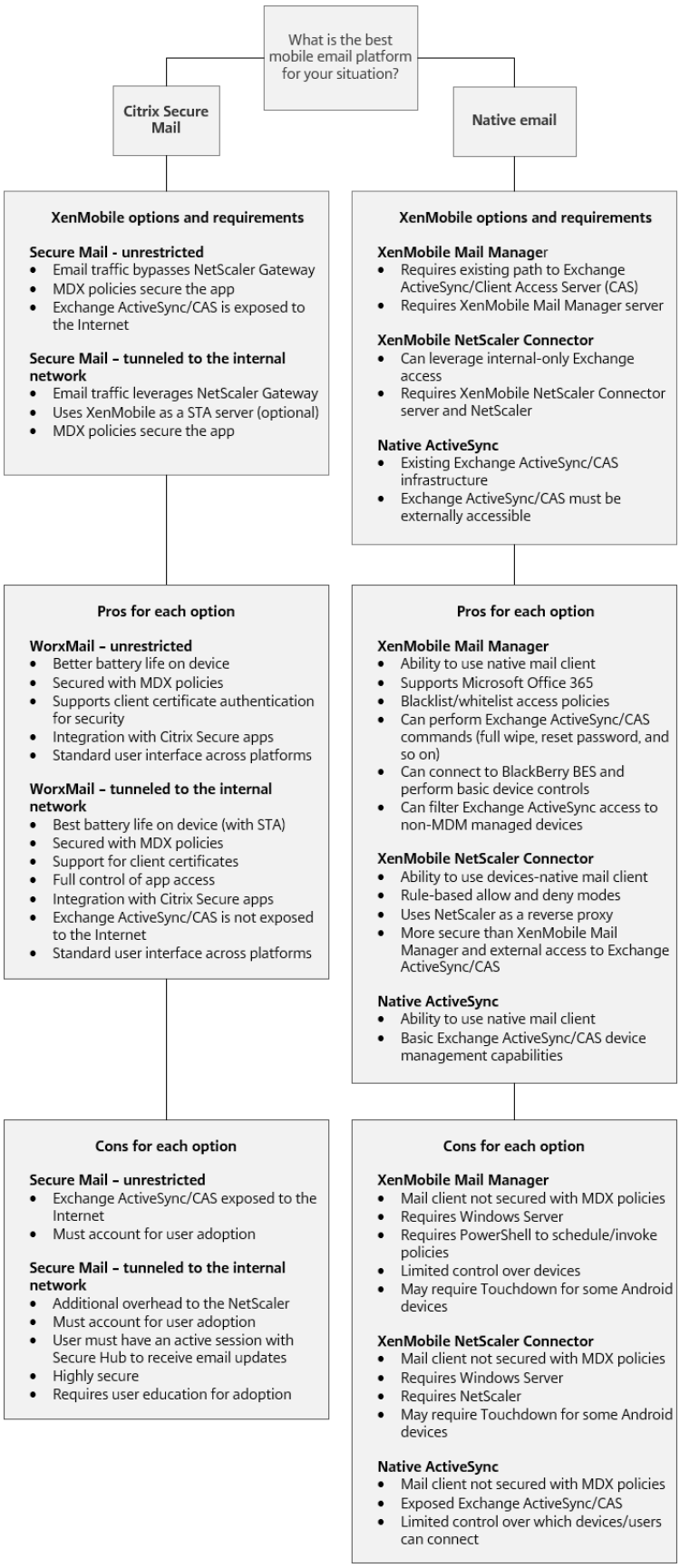
- Windows Server: Exchange ActiveSync 용 Endpoint Management 커넥터구성요소를사용하려면 Windows Server 를배포해야합니다.
- 필터링규칙설정: Exchange ActiveSync 용 Citrix Gateway 커넥터와마찬가지로 Exchange ActiveSync 용 Endpoint Management 커넥터에는장치상태를평가하는필터링규칙이포함됩니다. 또한 Exchange ActiveSync 용 Endpoint Management 커넥터는 Active Directory 그룹구성원자격을기준으로필터링하는정적규칙을지원합니다.
- Exchange 통합: Exchange ActiveSync 용 Endpoint Management 커넥터는 ActiveSync 역할을호스트하는 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 커넥터를직접통합하면 XenMobile 이모바일장치에서 Exchange ActiveSync 초기화를수행할수있습니다. 또한

XenMobile 은 Exchange ActiveSync 용 Endpoint Management 커넥터를통해 Blackberry 장치에대한정보에액세스하고다른제어작업을수행할수있습니다.

XenMobile 배포의 Exchange ActiveSync 용 Endpoint Management 커넥터다이어그램은 온-프레미스배포용참조아키텍처를참조하십시오.

전자메일플랫폼의사결정트리

다음그림은 XenMobile 배포에서기본전자메일과 Secure Mail 솔루션을사용할때의장점과단점을이해하는데도움이됩니다. 연결된 XenMobile 옵션과서버, 네트워크및데이터베이스액세스지원을위한요구사항을고려하여솔루션을선택할수있습니다. 장점및단점에는보안, 정책및사용자인터페이스고려사항에대한세부정보가포함됩니다.



XenMobile 통합

January 5, 2022

이문서에서는 XenMobile 과기존네트워크및솔루션의통합을계획할때고려해야할사항에대해다룹니다. 예를들어 Virtual Apps and Desktops 에 Citrix ADC 를사용중인경우다음을고려해야할수있습니다.

- 기존 Citrix ADC 인스턴스를사용해야합니까? 새로운전용인스턴스를사용해야합니까?
- StoreFront 를사용하여게시된 HDX 앱을 XenMobile 과통합하려고합니까?
- XenMobile 에서 Citrix Files 를사용할계획입니까?
- XenMobile 에통합하려는네트워크액세스제어솔루션이있습니까?
- 네트워크의모든아웃바운드트래픽에대한웹프록시를배포합니까?

Citrix ADC 및 Citrix Gateway

XenMobile ENT 및 MAM 모드에는 Citrix Gateway 가필요합니다. Citrix Gateway 는모든회사리소스에액세스할수있는 Micro VPN 경로를제공하며강력한다중단계인증을지원합니다. 다음의경우모든 XenMobile Server 장치모드에 Citrix ADC 부하분산이필요합니다.

- 다수의 XenMobile Server 가있는경우
- XenMobile Server 가 DMZ 또는내부네트워크에있는경우 (트래픽이장치에서 Citrix ADC 를거쳐 XenMobile 로 흐르는경우).

기존 Citrix ADC 인스턴스를사용하거나 XenMobile 전용의새인스턴스를설정할수있습니다. 다음섹션에서는기존 Citrix ADC 인스턴스또는새로운전용 Citrix ADC 인스턴스를사용할때의장점과단점을살펴봅니다.

XenMobile 용으로만든 Citrix Gateway VIP 를 Citrix ADC MPX 와공유

장점:

- 모든 Citrix 원격연결 (Citrix Virtual Apps and Desktops, 전체 VPN 및클라이언트없는 VPN) 에공통된 Citrix ADC 인스턴스를사용합니다.
- 인증서인증및 DNS, LDAP 및 NTP 같은서비스액세스시기존 Citrix ADC 구성을사용합니다.
- 단일 Citrix ADC 플랫폼라이센스를사용합니다.

단점:

- 동일한 Citrix ADC 에서두개의다른사용사례를처리하는경우확장을계획하기가더어렵습니다.
- 가끔, Citrix Virtual Apps and Desktops 사용사례에대한특정 Citrix ADC 버전이필요할수있습니다. 이러한버전에는 XenMobile 의알려진문제가포함될수있습니다. 또는 XenMobile 에 Citrix ADC 버전의알려진문제가포함될수있습니다.
- Citrix Gateway 가있는경우 XenMobile 에대한 Citrix ADC 구성을만들때 XenMobile 용 Citrix ADC 마법사를두번실행할수없습니다.

- Citrix Gateway 11.1 이상에서 Platinum 라이센스를사용하는경우를제외하고 Citrix ADC 에설치되고 VPN 연결에필요한사용자액세스라이센스가풀링됩니다. 모든 Citrix ADC 가상서버에서이러한라이센스를사용할수있으므로 XenMobile 외의다른서비스에의해라이센스가소비될수있습니다.

전용 **Citrix ADC VPX/MPX** 인스턴스

장점:

Citrix ADC 의전용인스턴스를사용하는것이좋습니다.

- 확장을계획하기가쉽고 XenMobile 트래픽이이미리소스제약이있을수있는 Citrix ADC 인스턴스와분리됩니다.
- XenMobile 과 Citrix Virtual Apps and Desktops 에서서로다른 Citrix ADC 소프트웨어버전을사용해야하는경우문제가방지됩니다. XenMobile 과호환되는최신 Citrix ADC 버전및빌드를사용하는것이일반적으로권장됩니다.
- XenMobile 용기본제공 Citrix ADC 마법사를통해 XenMobile 에서 Citrix ADC 를구성할수있습니다.
- 가상서비스와물리적서비스가분리됩니다.
- Citrix Gateway 11.1 이상에서 Platinum 라이센스를사용하는경우를제외하고 XenMobile 에필요한사용자라이센스가 Citrix ADC 의 XenMobile 서비스에만제공됩니다.

단점:

- Citrix ADC 에서 XenMobile 구성을지원하는추가서비스를설정해야합니다.
- 다른 Citrix ADC 플랫폼라이센스가필요합니다. 각 Citrix ADC 인스턴스에 Citrix Gateway 라이센스가있어야합니다.

Citrix ADC 및 Citrix Gateway 를 XenMobile 서버모드와통합할때의고려사항에대한자세한내용은 Citrix ADC 와 Citrix Gateway 의통합을참조하십시오.

StoreFront

Citrix Virtual Apps and Desktops 환경이있는경우 StoreFront 를사용하여 HDX 응용프로그램을 XenMobile 과통합할수있습니다. HDX 앱을 XenMobile 과통합하는경우:

- XenMobile 에등록한사용자가앱을사용할수있습니다.
- XenMobile Store 에다른모바일앱과함께앱이표시됩니다.
- XenMobile 이 StoreFront 의레거시 PNAgent(서비스) 사이트를사용합니다.
- Citrix Receiver 가장치에설치된경우 HDX 앱이 Citrix Receiver 사용을시작합니다.

StoreFront 에는 StoreFront 인스턴스당하나의서비스사이트를사용해야하는제한이있습니다. 여러저장소가있고이러한저장소를다른프로덕션사용과구분해야하는경우 XenMobile 에사용할새 StoreFront 인스턴스및서비스사이트를만드는것이좋습니다.

고려사항은다음과같습니다.

- StoreFront 에대한특정인증요구사항이있습니까? StoreFront 서비스사이트에로그온하려면 Active Directory 자격증명이필요합니다. 인증서기반인증만사용하는고객은동일한 Citrix Gateway 를사용하는 XenMobile 을통해응용프로그램을열거할수없습니다.

- 동일한저장소를사용합니까? 새저장소를만듭니까?
- 동일한 StoreFront 서버를사용합니까? 새 StoreFront 서버를사용합니까?

다음섹션에서는 Receiver 및모바일생산성앱에대해개별 StoreFront 또는결합된 StoreFront 를사용할때의장점과단점을살펴봅니다.

기존 **StoreFront** 인스턴스를 **XenMobile** 서버와통합

장점:

- 동일한저장소: 동일한 Citrix ADC VIP 를 HDX 액세스에사용하는것으로가정할경우 XenMobile 용 StoreFront 를추가로구성할필요가없습니다. 동일한저장소를사용하고 Receiver 액세스를새 Citrix ADC VIP 로연결한다고가정할수있습니다. 이경우적절한 Citrix 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 저장소에대한구성변경이기존 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 를통한 Virtual Apps and Desktops를참조하십시오.

Citrix Content Collaboration 및 Citrix Files

사용자는 Citrix Files 를사용하여모든장치의모든데이터에액세스하고동기화할수있습니다. Citrix Files 를사용하면조직내부및외부사용자와안전하게데이터를공유할수있습니다. Citrix Content Collaboration 을 XenMobile Advanced Edition 또는 Enterprise Edition 과통합하면 XenMobile 을통해 Citrix Files 에다음을제공할수있습니다.

- XenMobile App 사용자의 SSO(Single Sign-on) 인증.

- Active Directory 기반사용자계정프로비전.
- 포괄적인액세스제어정책.

모바일사용자는모든 Enterprise 계정기능집합을사용할수있습니다.

또는 StorageZone 커넥터만통합하도록 XenMobile 을구성할수있습니다. Citrix Files 는 StorageZone 커넥터를통해다음에대한액세스를제공합니다.

- 문서및폴더
- 네트워크파일공유
- SharePoint 사이트: 사이트모음및문서라이브러리.

연결된파일공유에는 Citrix Virtual Apps and Desktops 환경에사용된것과동일한네트워크홈드라이브가포함될수있습니다. XenMobile 콘솔을사용하여 Citrix Files 또는 StorageZones 커넥터와의통합을구성할수있습니다. 자세한내용은 XenMobile 에서 Citrix Files 사용을참조하십시오.

다음섹션에서는 Citrix Files 에대한설계의사결정을내릴때고려할수있는질문을살펴봅니다.

Citrix Files 또는 **StorageZone** 커넥터만통합

질문:

- Citrix 에서관리하는 StorageZones 에데이터를저장해야합니까?
- 사용자에게파일공유및동기화기능을제공하려고합니까?
- 사용자가 Citrix Files 웹사이트의파일에액세스할수있어야합니까? 또는모바일장치에서 Office 365 콘텐츠및개인용클라우드커넥터에액세스해야합니까?

설계의사결정:

- 위질문중하나이상에대한답이 “예” 인경우 Citrix Files 와통합합니다.
- StorageZone 커넥터만통합하는경우 SharePoint 사이트및네트워크파일공유등의기존온-프레미스스토리지저장소에대한보안모바일액세스를 iOS 사용자에게제공할수있습니다. 이구성에서는 Content Collaboration 하위도메인을설정하거나, Citrix Files 에사용자를프로비전하거나, Citrix Files 데이터를호스팅하지않습니다. StorageZones 커넥터를 XenMobile 과함께사용하면사용자정보가회사네트워크밖으로유출되지않도록하는보안제한사항을준수할수있습니다.

StorageZones Controller 서버위치

질문:

- 온-프레미스스토리지또는기능 (예: StorageZone 커넥터) 이필요합니까?
- Citrix Files 의온-프레미스기능을사용하는경우 StorageZones Controller 는네트워크의어디에위치합니까?

설계의사결정:

- StorageZones Controller 서버의위치 (Citrix Files 클라우드, 온-프레미스단일테넌트스토리지시스템또는지원되는타사클라우드스토리지) 를결정합니다.

- StorageZones Controller 를사용하려면인터넷액세스를통해 Citrix Files 제어부와통신해야합니다. 직접액세스, NAT/PAT 구성또는프록시구성등다양한방법으로연결할수있습니다.

StorageZone 커넥터

질문:

- CIFS 공유경로는무엇입니까?
- SharePoint URL 은무엇입니까?

설계의사결정:

- 온-프레미스 StorageZones Controller 에서이러한위치에액세스해야하는지여부를결정합니다.
- StorageZone 커넥터에서파일저장소, CIFS 공유및 SharePoint 같은내부리소스와통신해야하므로 StorageZones Controller 를내부네트워크의 DMZ 방화벽뒤와 Citrix ADC 앞에배치하는것이좋습니다.

SAML 과 **XenMobile Enterprise** 통합

질문:

- Citrix Files 에 Active Directory 인증이필요합니까?
- XenMobile 용 Citrix Files 앱을처음으로사용할때 SSO 가필요합니까?
- 현재환경에표준 IdP 가있습니까?
- SAML 을사용해야하는도메인은몇개입니까?
- Active Directory 사용자에대한전자메일별칭이여러개입니까?
- Active Directory 도메인마이그레이션이진행중이거나곧예약되어있습니까?

설계의사결정:

XenMobile Enterprise 환경에서는 SAML 을 Citrix Files 의인증메커니즘으로사용할수있습니다. 인증옵션은다음과같습니다.

- XenMobile 서버를 SAML 의 IdP(ID 공급자) 로사용합니다.

이옵션을사용하면사용자환경을향상하고 Citrix Files 계정생성을자동화하는동시에모바일앱 SSO 기능을지원할수있습니다.

- XenMobile 서버에서이프로세스가향상되며 Active Directory 동기화가필요하지않습니다.
- Citrix Files 사용자관리도구를사용자프로비전에사용합니다.
- 지원되는타사공급업체를 SAML 의 IdP 로사용합니다.

기존의지원되는 IdP 가있고모바일앱 SSO 기능이필요하지않은경우이옵션이가장적합할수있습니다. 이옵션을사용하려면계정프로비전에 Citrix Files 사용자관리도구를사용해야합니다.

타사 IdP 솔루션 (예: ADFS) 을사용하는경우 Windows 클라이언트측에서 SSO 기능을사용할수도있습니다. Citrix Files SAML IdP 를선택하기전에사용사례를평가하십시오.

또한두사용사례를모두충족하기위해 ADFS 및 XenMobile 을이중 IdP 로구성할수있습니다.

모바일앱

질문:

- 사용하려는 Citrix Files 모바일앱은무엇입니까 (공용, MDM, MDX)?

설계의사결정:

- Apple App Store 및 Google Play Store 로부터모바일생산성앱을배포할수있습니다. 공용앱스토어배포를사용하는경우 Citrix 다운로드페이지에서래핑된앱을받을수있습니다.
- 보안수준이낮고컨테이너화가필요하지않은경우공용 Citrix Files 응용프로그램은적합하지않을수있습니다. MDM 전용 환경에서는 XenMobile 을 MDM 모드에서사용하여 Citrix Files 앱의 MDM 버전을제공할수있습니다.
- 자세한내용은 XenMobile 용 Citrix Files에서 앱을참조하십시오.

보안, 정책및액세스제어

질문:

- 데스크톱, 웹및모바일사용자에게적용해야하는제한은무엇입니까?
- 사용자에게적용하려는표준액세스제어설정은무엇입니까?
- 사용하려는파일보존정책은무엇입니까?

설계의사결정:

- Citrix Files 를사용하여직원권한및장치보안을관리할수있습니다. 자세한내용은 Employee Permissions(직원권한)와 Managing Devices and Apps(장치및앱관리)를참조하십시오.
- 일부 Citrix Files 장치보안설정및 MDX 정책은동일한기능을제어합니다. 이러한경우 XenMobile 정책이우선하며 Citrix Files 장치보안설정이그다음으로적용됩니다. 예: Citrix Files 에서외부앱을사용하지않도록설정하고 XenMobile 에서사용하도록설정하면외부앱이 Citrix Files 에서사용되지않습니다. XenMobile 에서는 PIN/암호를 사용하지않고 Citrix Files 앱에서 PIN/암호를사용하도록앱을구성할수있습니다.

표준 **StorageZone** 와제한된 **StorageZone** 비교

질문:

- 제한된 StorageZone 이필요합니까?

설계의사결정:

- 표준 StorageZone 은중요하지않은데이터에사용되며이를통해직원들은직원이외의사람들과데이터를공유할수있습니다. 이옵션은도메인외부의데이터공유와관련된워크플로를지원합니다.
- 제한된 StorageZone 은중요한데이터를보호합니다. 인증된도메인사용자만해당영역에저장된데이터에액세스할수있습니다.

웹프록시

HTTP(S)/SOCKS 프록시를통해 XenMobile 트래픽을라우팅하는가장일반적인시나리오는 XenMobile 서버가상주하는서브넷에서아웃바운드인터넷액세스를통해필요한 Apple, Google 또는 Microsoft IP 주소에액세스할수없는경우입니다. XenMobile 에서모든인터넷트래픽을프록시서버로라우팅하도록프록시서버설정을지정할수있습니다. 자세한내용은 프록시서버사용을참조하십시오.

다음표에서는 XenMobile 에사용되는가장일반적인프록시의장점및단점에대해설명합니다.

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. 회사의인터넷연결이브라우징을제한하는경우이구성이인터넷브라우징성능에영향을미칠수있습니다.

분할터널링에대한 Citrix ADC 세션프로필구성은트래픽에다음과같은영향을미칩니다.

Citrix ADC 분할터널링이 꺼짐인경우:

- MDX 네트워크액세스정책이 내부네트워크로터널링됨인경우: 모든트래픽에 Citrix Gateway 로다시터널링되는 Micro VPN 또는 cVPN(클라이언트없는 VPN) 터널이사용됩니다.
- 프록시서버에대한 Citrix ADC 트래픽정책/프로필을구성하고 Citrix 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)를참조하십시오.

Citrix ADC 분할터널링이 켜짐인경우:

- MDX 네트워크액세스정책이 내부네트워크로터널링됨으로구성된앱의경우: 앱이웹리소스에직접액세스를시도합니다. 웹리소스가공개적으로제공되지않는경우이러한앱은 Citrix Gateway 로폴백합니다.
- 프록시서버에대한 Citrix ADC 트래픽정책및프로필을구성합니다. 그런다음이러한정책및프로필을 Citrix Gateway VIP 에바인딩합니다.

> 중요:
>
> Secure Hub cVPN 트래픽을프록시에서제외하십시오.

Split DNS(DNS 분할)(**Client experience(**클라이언트환경**)** 아래) 에대한 Citrix ADC 세션프로필구성은분할터널링과유사하게작동합니다.

Split DNS(DNS 분할**)** 를사용하고 둘다로설정한경우:

- 클라이언트가 FQDN 을로컬로확인한다음실패시 Citrix ADC 로폴백하여 DNS 를확인합니다.

Split DNS(DNS 분할**)** 를 원격으로설정한경우:

- DNS 확인이 Citrix ADC 에서만수행됩니다.

Split DNS(DNS 분할**)** 를 로컬로설정한경우:

- 클라이언트가 FQDN 을로컬로확인합니다. Citrix ADC 는 DNS 확인에사용되지않습니다.

액세스제어

회사에서네트워크내부및외부의모바일장치를관리할수있습니다. XenMobile 같은엔터프라이즈모빌리티관리솔루션은모바일장치의위치에관계없이보안및제어를제공할수있습니다. 그뿐만아니라 NAC(네트워크액세스제어) 솔루션과함께사용할경우 QoS 를추가하고네트워크내부의장치를보다세부적으로제어할수있습니다. 이러한결합을사용할경우 XenMobile 장치의보안평가를 NAC 솔루션을통해확장할수있습니다. 그런다음 NAC 솔루션에서 XenMobile 보안평가를사용하여인증의사결정을지원하고처리할수있습니다.

다음솔루션중하나를사용하여 NAC 정책을적용할수있습니다.

- Citrix Gateway
- Cisco Identity Services Engine(ISE)
- ForeScout

Citrix 는다른 NAC 솔루션에대한통합을보장하지않습니다.

NAC 솔루션과 XenMobile 의통합은다음과같은장점을제공합니다.

- 엔터프라이즈네트워크의모든끝점에대한보안, 규정준수및제어가개선됩니다.
- NAC 솔루션은다음과같은기능을제공합니다.
  - 회사네트워크에연결하는장치를즉시감지합니다.
  - XenMobile 에장치특성을쿼리합니다.
  - 해당장치정보를사용하여이러한장치를허용, 차단, 제한또는리디렉션할지결정합니다. 이러한결정은회사에서선택하는보안정책에따라다릅니다.
- IT 관리자는 NAC 솔루션을사용하여관리되지않는장치와규정을준수하지않는장치를확인할수있습니다.

XenMobile 에서지원되는 NAC 규정준수필터에대한설명및구성개요는 네트워크액세스제어에서확인하십시오.

다중사이트요구사항

January 5, 2022

고가용성및재해복구를위한여러사이트를포함하는 XenMobile 배포를설계하고구성할수있습니다. 이문서에서는 XenMobile 배포에사용되는고가용성및재해복구모델의개요를제공합니다.

고가용성

- XenMobile 클러스터노드의경우 Citrix ADC 가부하분산을처리합니다. 자세한내용은 클러스터링구성을참조하십시오.
- XenMobile 서버노드는활성/활성구성으로작동합니다.
- 용량이필요하면추가 XenMobile 서버노드가고가용성클러스터에추가됩니다. 단일노드는최대약 8,500 개의사용자장치를처리할수있습니다 (자세한내용은 확장성및성능 참조).
- 8,500 개사용자장치를처리하는서버하나와중복성을위한추가서버하나를나타내는 “n+1” 로 XenMobile 서버를구성하는것이좋습니다.
- 가능한경우모든 Citrix ADC 인스턴스에대해고가용성을구성하여두번째 Citrix ADC 와구성을동기화하는것이좋습니다.
- 표준 Citrix ADC 고가용성쌍은활성/비활성구성으로작동합니다.

일반적인고가용성 XenMobile 배포에는다음이포함됩니다.

- Citrix ADC 인스턴스 2 개 (VPX 또는 MPX). Citrix ADC SDX 플랫폼을사용하는경우에도고가용성을고려해야합니다.
- 동일한데이터베이스설정으로구성된둘이상의 XenMobile 서버.

재해복구

활성데이터센터 1 개와비활성데이터센터 1 개로구성된데이터센터 2 개를사용하여 XenMobile 의재해복구를구성할수있습니다. 활성/활성설정의사용자환경을제공하기위해활성/활성데이터경로를만들려면 Citrix ADC 와 GSLB(Global Server Load Balancing) 를사용합니다.

재해복구를위한 XenMobile 배포에는다음이포함됩니다.

- 하나이상의 Citrix ADC 인스턴스, XenMobile 서버및 SQL Server 데이터베이스가포함된데이터센터 2 개.
- 트래픽을데이터센터로전달하는 GSLB 서버. 사이트에대한트래픽을처리하는 XenMobile 등록 URL 과 Citrix Gateway URL 모두에대해 GSLB 서버를구성합니다.
- XenMobile 용 Citrix ADC 마법사를사용하여 Citrix Gateway 를구성하는경우기본적으로 GSLB 가 XenMobile 등록서버에대한트래픽과 Citrix Gateway 에대한트래픽을 MAM 부하분산서버로이동하는중에확인하도록설정되지않으므로추가단계를수행해야합니다. 이러한단계의준비및구현에대한자세한내용은 재해복구를참조하십시오.
- Always On 가용성그룹의클러스터링된 SQL Server.
- XenMobile 서버와 SQL Server 간대기시간은 5 밀리초미만이어야합니다.

> 참고:
>
> 이안내서에설명된재해복구방법은액세스계층에대한자동재해복구만제공합니다. 장치에서 XenMobile 서버에연결하려면장애조치 (failover) 사이트에서모든 XenMobile 서버노드와 SQL Server 데이터베이스를수동으로시작해야합니다.

Citrix Gateway 및 Citrix ADC 통합

January 5, 2022

Citrix Gateway 를 XenMobile 과통합하면내부네트워크로원격액세스하는 MAM 장치에대한인증메커니즘을사용할수있습니다. 이통합을사용하면마이크로 VPN 을통해인트라넷의기업서버에모바일생산성앱을연결할수있습니다. 모바일장치의앱에서 Citrix Gateway 로마이크로 VPN 이생성됩니다. Citrix Gateway 는모든회사리소스에액세스할수있는 Micro VPN 경로를제공하며강력한다중단계인증을지원합니다.

다음의경우모든 XenMobile Server 장치모드에 Citrix ADC 부하분산이필요합니다.

- 다수의 XenMobile Server 가있는경우
- XenMobile Server 가 DMZ 또는내부네트워크에있는경우 (트래픽이장치에서 Citrix ADC 를거쳐 XenMobile 로흐르는경우)

XenMobile Server 모드에대한통합요구사항

Citrix Gateway 및 Citrix ADC 의통합요구사항은 XenMobile Server 모드 (MAM, MDM 및 ENT) 에따라다릅니다.

MAM

XenMobile Server 를 MAM 모드에서사용:

- **Citrix Gateway** 가필요합니다. Citrix Gateway 는모든회사리소스에액세스할수있는 Micro VPN 경로를제공하며강력한다중단계인증을지원합니다.
- 부하분산에는 **Citrix ADC** 가권장됩니다.

  XenMobile 앞에부하분산장치를배치하는고가용성구성으로 XenMobile 을배포하는것이좋습니다. 자세한내용은 MAM 모드와레거시 MAM 모드정보를참조하십시오.

MDM

XenMobile Server 를 MDM 모드에서사용:

- Citrix Gateway 가필요하지않습니다. MDM 배포의경우 Citrix Gateway 는모바일장치 VPN 에권장됩니다.

- 보안및부하분산에는 Citrix ADC 가권장됩니다.

  보안및부하분산을위해 Citrix ADC 장비를 XenMobile Server 앞에배포하는것이좋습니다. XenMobile 을 DMZ 에배포하는표준배포의경우 XenMobile 용 Citrix ADC 마법사와함께 XenMobile Server 부하분산을 SSL 브리지 모드에서사용하는것이좋습니다. 다음과같은배포의경우 SSL 오프로드도고려할수있습니다.

  - XenMobile Server 가 DMZ 가아닌내부네트워크에있는배포
  - 보안팀에서 SSL 브리지구성을요구하는배포

  Citrix 에서는 NAT 또는기존타사프록시또는 MDM 용부하분산장치를통해 XenMobile Server 를인트라넷에노출하는것을권장하지않습니다. XenMobile Server(SSL 브리지) 에서 SSL 트래픽이종료되더라도이러한구성은잠재적인 보안위험을유발합니다.

  보안수준이높은환경에서기본 XenMobile 구성의 Citrix ADC 는보안요구사항을충족하거나초과합니다.

  보안요구사항이가장높은 MDM 환경에서는 SSL 을 Citrix ADC 에서종료하여경계에서트래픽을검사하는동시에종단간 SSL 암호화를유지할수있습니다. 자세한내용은 보안요구사항을참조하십시오. Citrix ADC 는 SSL/TLS 암호화및 SSL FIPS Citrix ADC 하드웨어를정의하는옵션을제공합니다.

ENT(MAM+MDM)

XenMobile Server 를 ENT 모드에서사용:

- Citrix Gateway 가필요합니다. Citrix Gateway 는모든회사리소스에액세스할수있는 Micro VPN 경로를제공하며 강력한다중단계인증을지원합니다.

  XenMobile Server 모드가 ENT 이고사용자가 MDM 등록을선택하는경우장치는레거시 MAM 모드에서작동합니다. 레거시 MAM 모드에서는 Citrix Gateway FQDN 을사용하여장치를등록합니다. 자세한내용은 MAM 모드와레거시 MAM 모드정보를참조하십시오.

- 부하분산에는 Citrix ADC 가권장됩니다. 자세한내용은이문서에서앞서살펴본 “MDM” 아래의 Citrix ADC 요점을참고하십시오.

> 중요:
>
> 초기등록의경우사용자장치의트래픽은 SSL 오프로드또는 SSL 브리지에대한부하분산가상서버의구성여부와관계없이 XenMobile Server 에서인증됩니다.

설계의사결정

다음섹션에는 Citrix Gateway 와 XenMobile 의통합을계획할때고려해야하는다수의설계의사결정이요약되어있습니다.

라이센스및버전

의사결정세부정보:

- 사용하려는 Citrix ADC 버전은무엇입니까?

- Citrix ADC 에플랫폼라이센스를적용했습니까?
- MAM 기능이필요한경우 Citrix ADC Universal Access 라이센스를적용했습니까?

설계지침:

Citrix Gateway 에올바른라이센스를적용하십시오. Exchange ActiveSync 용 Citrix Gateway 커넥터를사용하는경우통합캐싱이필요할수있습니다. 따라서, 적절한 Citrix ADC 버전이있어야합니다.

Citrix ADC 기능을사용하기위한라이센스요구사항은다음과같습니다.

- XenMobile MDM 부하분산을사용하려면 Citrix ADC Standard 이상의플랫폼라이센스가필요합니다.
- StorageZones Controller 를통한 Content Collaboration 부하분산을사용하려면 Citrix ADC Standard 이상의플랫폼라이센스가필요합니다.
- XenMobile Enterprise Edition 에는 MAM 에필요한 Citrix Gateway Universal 라이센스가포함되어있습니다.
- Exchange 부하분산을사용하려면 Citrix ADC Platinum 플랫폼라이센스또는 Citrix ADC Enterprise 플랫폼라이센스 (통합캐싱라이센스포함) 가필요합니다.

XenMobile 용 **Citrix ADC** 버전

의사결정세부정보:

- XenMobile 환경에서실행되는 Citrix ADC 버전은무엇입니까?
- 별도의인스턴스가필요합니까?

설계지침:

Citrix Gateway 가상서버를위한전용 Citrix ADC 인스턴스를사용하는것이좋습니다. XenMobile 환경에서필요한최소버전의 Citrix ADC 와빌드가사용되고있는지확인하십시오. 일반적으로 XenMobile 과호환되는최신 Citrix ADC 버전및빌드를사용하는것이가장좋습니다. Citrix Gateway 업그레이드가기존환경에영향을미칠수있는경우 XenMobile 을위한두번째전용인스턴스를만드는것이적절할수있습니다.

XenMobile 의 Citrix ADC 인스턴스를 VPN 연결을사용하는다른앱과공유하려는경우두앱에서사용하기에충분한 VPN 라이센스가있는지확인하십시오. XenMobile 테스트및프로덕션환경에서는 Citrix ADC 인스턴스를공유할수없습니다.

인증서

의사결정세부정보:

- XenMobile 환경을등록하고액세스할때더높은수준의보안이필요합니까?
- LDAP 를사용할수없습니까?

설계지침:

XenMobile 에대한기본구성은사용자이름및암호인증입니다. XenMobile 환경에대한등록및액세스시추가보안계층을추가하려면인증서기반인증을사용하는것이좋습니다. 인증서를 LDAP 와함께 2 단계인증에사용하여 RSA 서버없이더높은수준의보안을제공할수있습니다.

LDAP 를허용하지않고스마트카드또는유사한방법을사용하는경우인증서를구성하면 XenMobile 에스마트카드를나타낼수있습니다. 그런다음사용자는 XenMobile 에서생성된고유한 PIN 을사용하여등록합니다. 사용자가액세스권한을획득하면 XenMobile 이 XenMobile 환경에인증하는데사용될인증서를만들어배포합니다.

XenMobile 은타사인증기관에대해서만 CRL(인증서해지목록) 을지원합니다. Microsoft CA 가구성된경우 XenMobile 은 Citrix ADC 를사용하여인증서해지를관리합니다. 클라이언트인증서기반인증을구성하는경우 Citrix ADC CRL(인증서해지목록) 설정인 **Enable CRL Auto Refresh(CRL** 자동새로고침사용**)** 를구성해야하는지여부를고려합니다. 이단계는 MAM 전용으로등록된장치사용자가장치의기존인증서를사용하여인증할수없도록합니다. XenMobile 에서는인증서가해지된경우사용자가사용자인증서를생성할수있으므로새인증서가다시발급됩니다. 이설정을사용하면 CRL 이만료된 PKI 엔터티를확인하는경우 PKI 엔터티의보안이강화됩니다.

네트워킹토폴로지

의사결정세부정보:

- 필요한 Citrix ADC 토폴로지는무엇입니까?

설계지침:

XenMobile 에는 Citrix ADC 인스턴스를사용하는것이좋습니다. 하지만네트워크내부에서 DMZ 로나가는트래픽을원하지않을수도있습니다. 이경우에는 Citrix ADC 추가인스턴스설정을고려해보십시오. 내부사용자를위한 Citrix ADC 인스턴스하나, 외부사용자를위한인스턴스하나를사용합니다. 사용자가내부네트워크와외부네트워크를전환하는경우 DNS 레코드캐싱으로인해 Secure Hub 에서로그온시도가증가할수있습니다.

XenMobile 은 Citrix Gateway 이중홉을지원하지않습니다.

전용또는공유 **Citrix Gateway VIP**

의사결정세부정보:

- 현재 Virtual Apps and Desktops 에 Citrix Gateway 를사용하고있습니까?
- XenMobile 에서 Virtual Apps and Desktops 와동일한 Citrix Gateway 를사용할계획입니까?
- 두트래픽흐름에대한인증요구사항은무엇입니까?

설계지침:

Citrix 환경에 XenMobile 에더해 Virtual Apps and Desktops 가포함되는경우동일한 Citrix ADC 인스턴스와 Citrix Gateway 가상서버를동시에사용할수있습니다. 버전관리충돌및환경격리가발생할수있으므로각 XenMobile 환경에서전용 Citrix ADC 인스턴스및 Citrix Gateway 를사용하는것이좋습니다. 그러나전용 Citrix ADC 인스턴스를사용할수없는경우 Citrix 에서는전용 Citrix Gateway 가상서버를사용하여 Secure Hub 트래픽흐름을분리하기를권장합니다. 가상서버대신이러한구성이 XenMobile 과 Virtual Apps and Desktops 사이에공유됩니다.

LDAP 인증을사용하는경우 Receiver 및 Secure Hub 에서동일한 Citrix Gateway 에문제없이인증할수있습니다. 인증서기반인증을사용하는경우 XenMobile 은인증서를 MDX 컨테이너에푸시하고 Secure Hub 는이인증서를사용하여 Citrix Gateway 에인증합니다. Receiver 는 Secure Hub 와분리되며 Secure Hub 와동일한인증서를사용하여동일한 Citrix Gateway 에인증할수없습니다.

이경우두개의 Citrix Gateway VIP 에동일한 FQDN 을사용하는다음과같은문제해결방식을고려해볼수있습니다.

- IP 주소가동일한 Citrix Gateway VIP 를두개만듭니다. Secure Hub 에사용할 VIP 에는표준 443 포트를사용하고 Virtual Apps and Desktops(Receiver 배포) 에사용할 VIP 에는포트 444 를사용합니다.
- 그러면하나의 FQDN 이동일한 IP 주소로확인됩니다.
- 이해결방법을사용하는경우기본값이포트 443 이아닌포트 444 에대해 ICA 파일을반환하도록 StoreFront 를구성할수있습니다. 이해결방법을사용하는경우사용자가포트번호를입력할필요가없습니다.

Citrix Gateway 시간초과

의사결정세부정보:

- XenMobile 트래픽에대한 Citrix Gateway 시간초과를어떻게구성할것입니까?

설계지침:

Citrix Gateway 에는 Session time-out(세션시간초과) 및 Forced time-out(강제시간초과) 라는설정이포함됩니다. 자세한내용은 권장되는구성을참조하십시오. 백그라운드서비스, Citrix ADC 및오프라인중응용프로그램액세스에대한시간초과값이서로다르다는점에유의하십시오.

MAM 에대한 **XenMobile** 부하분산장치 **IP** 주소

의사결정세부정보:

- VIP 에내부또는외부 IP 주소를사용합니까?

설계지침:

공용 IP 주소를 Citrix Gateway VIP 에사용할수있는환경에서 XenMobile 부하분산 VIP 및주소를이방식으로할당하면등록실패가발생할수있습니다.

이시나리오에서등록실패를방지하려면부하분산 VIP 에내부 IP 가사용되어야합니다. 이가상 IP 주소는사설 IP 주소의 RFC 1918 표준을준수해야합니다. 비사설 IP 주소를이가상서버에사용하는경우 Citrix ADC 가인증프로세스중에 XenMobile Server 에연결할수없습니다. 자세한내용은 https://support.citrix.com/article/CTX200430에서참조하십시오.

MDM 부하분산메커니즘

의사결정세부정보:

- Citrix Gateway 로 XenMobile Servers 의부하를분산하려면어떻게해야합니까?

설계지침:

XenMobile 이 DMZ 에있는경우 SSL 브리지를사용합니다. XenMobile 이내부네트워크에있는경우보안표준을충족해야한다면 SSL 오프로드를사용합니다.

- SSL 브리지모드에서 Citrix ADC VIP 를사용하여 XenMobile Server 부하를분산하는경우인터넷트래픽이 XenMobile Server 로직접흐르고여기서연결이종료됩니다. SSL 브리지모드는설정및문제해결이가장간단한모드입니다.
- SSL 오프로드모드에서 Citrix ADC VIP 를사용하여 XenMobile Server 부하를분산하는경우인터넷트래픽이 Citrix ADC 로직접흐르고여기서연결이종료됩니다. 그런다음 Citrix ADC 는 Citrix ADC 에서 XenMobile Server 로의새세션을설정합니다. SSL 오프로드모드는설정및문제해결이좀더복잡합니다.

SSL 오프로드를통한 **MDM** 부하분산의서비스포트

의사결정세부정보:

- 부하분산에 SSL 오프로드모드를사용하려는경우백엔드서비스에사용할포트는무엇입니까?

설계지침:

SSL 오프로드의경우다음과같이포트 80 또는 8443 을선택합니다.

- 포트 80 을사용하여 XenMobile Server 에다시연결함으로써완벽한오프로드를수행합니다.
- 종단간암호화, 즉트래픽재암호화는지원되지않습니다. 자세한내용은 Citrix 지원문서 Supported Architectures Between NetScaler and XenMobile Server(NetScaler 와 XenMobile Server 간에지원되는아키텍처)를참조하십시오.

등록 **FQDN**

의사결정세부정보:

- 등록및 XenMobile 인스턴스/부하분산 VIP 에무엇을 FQDN 으로사용할계획입니까?

설계지침:

클러스터의첫번째 XenMobile Server 를처음으로구성할때는 XenMobile Server FQDN 을제공해야합니다. 이 FQDN 은 MDM VIP URL 및내부 MAM LB VIP URL 과일치해야합니다. (내부 Citrix ADC 주소레코드는 MAM LB VIP 를확인합니다.) 자세한내용은이문서의나중에나오는 “관리모드별등록 FQDN” 을참조하십시오.

추가로, 다음과동일한인증서를사용해야합니다.

- XenMobile SSL 수신기인증서
- 내부 MAM LB VIP 인증서
- MDM VIP 인증서 (MDM VIP 에 SSL 오프로드를사용중인경우)

> 중요**:**
>
> 등록 FQDN 을구성한후에는변경할수없습니다. 새등록 FQDN 을사용하려면새 SQL Server 데이터베이스와 XenMobile Server 를다시구축해야합니다.

Secure Web 트래픽

의사결정세부정보:

- Secure Web 을내부웹브라우징으로만제한할계획입니까?
- 내부및외부웹브라우징에 Secure Web 을사용할계획입니까?

설계지침:

내부웹브라우징에만 Secure Web 을사용할계획이라면 Citrix Gateway 구성이간편합니다. Secure Web 은기본적으로모든내부사이트에도달해야합니다. 방화벽과프록시서버를구성해야할수있습니다.

내부와외부브라우징에모두 Secure Web 을사용할계획이라면 SNIP 에서아웃바운드인터넷액세스가가능해야합니다. IT 에서는일반적으로등록된장치 (MDX 컨테이너사용) 를기업네트워크의확장으로봅니다. 따라서, IT 에서는보통 Secure Web 연결이 Citrix ADC 로돌아와서프록시서버를거친다음인터넷으로나가기를원합니다. 기본적으로 Secure Web 에서는내부네트워크로의응용프로그램별 VPN 터널이모든네트워크액세스에사용됩니다. Citrix ADC 는분할터널설정을사용합니다.

Secure Web 연결에대한설명은 사용자연결구성을참조하십시오.

Secure Mail 에대한푸시알림

의사결정세부정보:

- 푸시알림을사용할계획입니까?

iOS 용설계지침:

Citrix Gateway 구성에 Secure Ticket Authority(STA) 가포함되고분할터널링이사용중지되어있을수있습니다. 그러면 Citrix Gateway 는 Secure Mail 에서 iOS 용 Secure Mail 의푸시알림에지정된 Citrix 수신기서비스 URL 로의트래픽을허용해야합니다.

Android 용설계지침:

FCM(Firebase Cloud Messaging) 을사용하여 Android 장치의 XenMobile 연결방법및시기를제어합니다. FCM 을구성하면모든보안동작또는배포명령이실행될때사용자에게 XenMobile Server 에다시연결하라는메시지를표시하는 Secure Hub 푸시알림이트리거됩니다.

HDX STA

의사결정세부정보:

- HDX 응용프로그램액세스를통합할계획이라면사용할 STA 는무엇입니까?

설계지침:

HDX STA 는 StoreFront 의 STA 와일치해야하며 Virtual Apps and Desktops 팜에서유효해야합니다.

Citrix Files 및 Citrix Content Collaboration

의사결정세부정보:

- 환경에서 Storage Zone Controller 를사용할계획입니까?
- 사용할 Citrix Files VIP URL 은무엇입니까?

설계지침:

환경에 Storage Zone Controller 를포함할예정이라면다음을올바르게구성해야합니다.

- Citrix Files 스위치 VIP(Citrix Files 제어부에서 StorageZone Controller 서버와통신하는데사용됨)
- Citrix Files 부하분산 VIP
- 모든필수정책및프로필

자세한내용은 StorageZones Controller 설명서를참조하십시오.

SAML IdP

의사결정세부정보:

- Citrix Files 에 SAML 이필요한경우 XenMobile 을 SAML IdP 로사용할것입니까?

설계지침:

권장되는모범사례는 Citrix Files 를 XenMobile Advanced Edition 또는 XenMobile Enterprise Edition 과통합하는것입니다. 이방법은 SAML 기반페더레이션을구성하는것보다간단합니다. 이러한 XenMobile 버전으로 Citrix Files 을사용할경우 XenMobile 은 Citrix Files 에다음을제공합니다.

- 모바일생산성앱사용자의 Single sign-on(SSO) 인증
- Active Directory 기반사용자계정프로비전
- 포괄적인액세스제어정책

XenMobile 콘솔을사용하여 Citrix Files 구성을수행하고서비스수준및라이센스사용현황을모니터링할수있습니다.

Citrix Files 클라이언트에는 XenMobile 용 Citrix Files 클라이언트 (래핑된 Citrix Files) 와 Citrix Files Mobile 클라이언트 (래핑되지않은 Citrix Files) 의두가지가있습니다. 차이점을알아보려면 Citrix Files for XenMobile 클라이언트와 Citrix Files 모바일클라이언트의차이점을참조하십시오.

SSO 액세스권한을제공하기위해 SAML 을사용하도록 XenMobile 및 Citrix Content Collaboration 을구성할수있습니다.

- Citrix Files 모바일앱
- 웹사이트, Outlook 플러그인또는동기화클라이언트와같이래핑되지않은 Citrix Files 클라이언트

XenMobile 을 Citrix Files 의 SAML IdP 로사용하려면적절한구성이있는지확인합니다. 자세한내용은 Citrix Files SSO 용 SAML을참조하십시오.

ShareConnect 직접연결

의사결정세부정보:

- ShareConnect 를실행하는컴퓨터또는모바일장치에서사용자가호스트컴퓨터에액세스할때직접연결을사용해야합니까?

설계지침:

ShareConnect 를사용할경우사용자는 iPad, Android 태블릿및 Android 휴대폰을통해컴퓨터에안전하게연결하여파일및응용프로그램에액세스할수있습니다. 직접연결의경우, XenMobile 은 Citrix Gateway 를사용하여로컬네트워크외부의리소스에대한보안액세스를제공합니다. 구성에대한자세한내용은 ShareConnect를참조하십시오.

각관리모드의등록 **FQDN**

관리모드	등록 **FQDN**
엔터프라이즈 (MDM+MAM) 및 MDM 등록필수	XenMobile Server FQDN
엔터프라이즈 (MDM+MAM) 및 MDM 등록선택	XenMobile Server FQDN 또는 Citrix Gateway FQDN
MDM 전용	XenMobile Server FQDN
MAM 전용 (레거시)	Citrix Gateway FQDN
MAM 전용	XenMobile Server FQDN

배포요약

올바른구성을위해 XenMobile 용 Citrix ADC 마법사를사용하는것이좋습니다. 마법사는한번만사용할수있습니다. 테스트, 개발및프로덕션환경을위한다수의 XenMobile 인스턴스가있는경우추가환경에대한 Citrix ADC 를수동으로구성해야합니다. 작동중인환경에서는 XenMobile 에서사용할 Citrix ADC 를수동으로구성하기전에설정을기록해두십시오.

마법사를사용하는경우결정해야하는중요한사항은 XenMobile Server 에대한통신에 HTTPS 를사용할지, 아니면 HTTP 를사용할지입니다. HTTPS 는 Citrix ADC 와 XenMobile 간의트래픽을암호화하는보안백엔드통신을제공합니다. 재암호화는 XenMobile Server 성능에영향을미칩니다. HTTP 는 XenMobile Server 성능을개선합니다. Citrix ADC 와 XenMobile 사이의트래픽은암호화되지않습니다. 다음표에 XenMobile Server 용 Citrix ADC 의 HTTP 및 HTTPS 포트 요구사항이나와있습니다.

HTTPS

일반적으로, Citrix ADC MDM 가상서버구성에는 SSL 브리지가권장됩니다. MDM 가상서버에서사용되는 Citrix ADC SSL 오프로드의경우 XenMobile 은포트 80 만백엔드서비스로지원합니다.

관리모드	**Citrix ADC** 부하분산방법	**SSL** 재암호화	**XenMobile** 서버포트
MDM	SSL 브리지	해당없음	443, 8443
MAM	SSL 오프로드	사용	8443
Enterprise	MDM: SSL 브리지	해당없음	443, 8443
Enterprise	MAM: SSL 오프로드	사용	8443

HTTP

관리모드	**Citrix ADC** 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 Citrix Gateway 다이어그램은 온-프레미스배포용참조아키텍처를참조하십시오.

MDX 앱에대한 **SSO** 및프록시고려사항

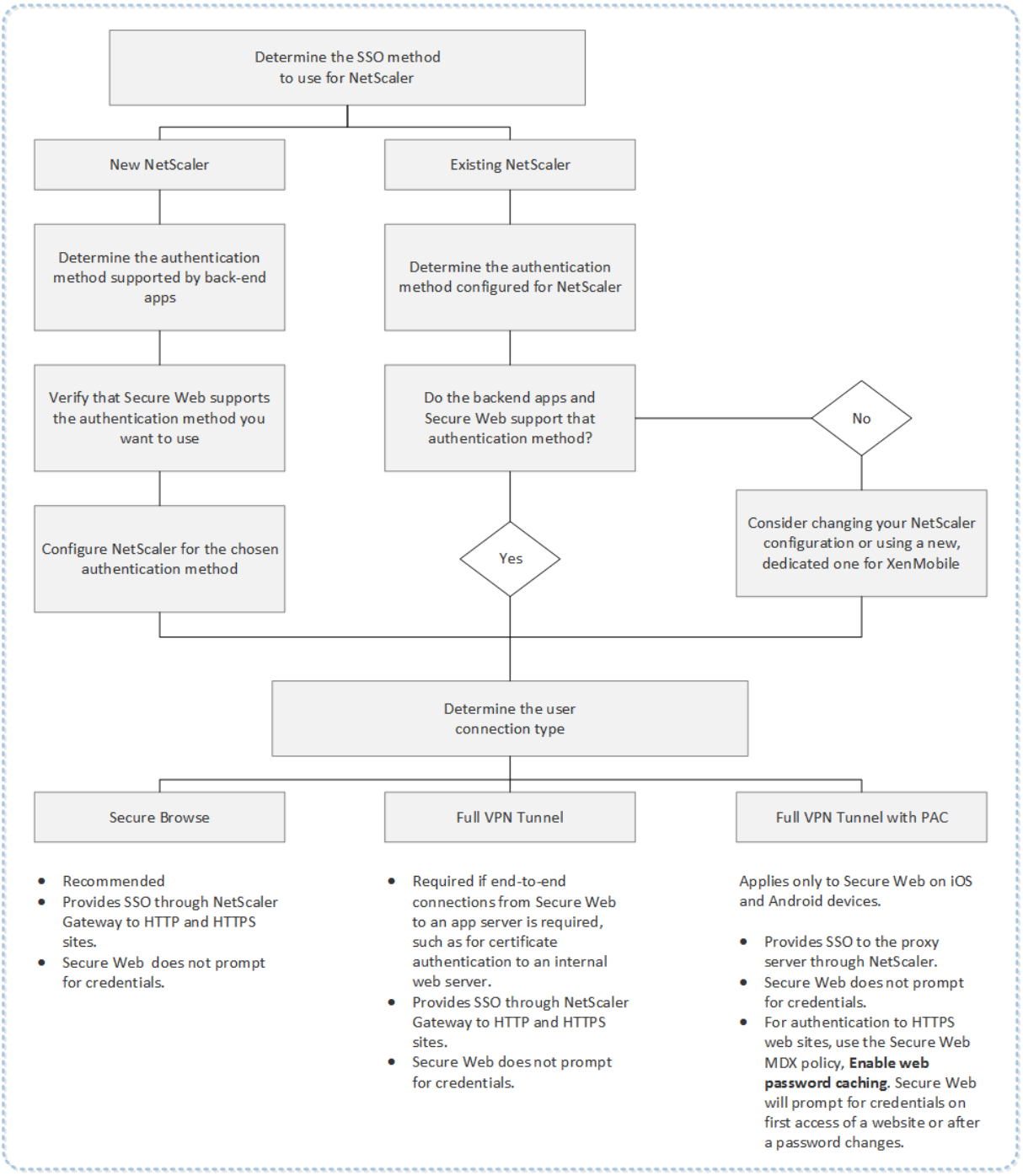
January 5, 2022

XenMobile 을 Citrix ADC 와통합하면모든백엔드 HTTP/HTTPS 리소스에대한 SSO(Single Sign-on) 를사용자에게제공할수있습니다. SSO 인증요구사항에따라다음옵션중하나를사용하도록 MDX 앱에대한사용자연결을구성할수있습니다.

- 클라이언트없는 VPN 유형인 Secure Browse
- 전체 VPN 터널

환경에서 SSO 를제공하기에 Citrix ADC 가적합하지않은경우정책기반로컬암호캐싱을통해 MDX 앱을구성할수있습니다. 이문서에서는 Secure Web 을중심으로다양한 SSO 및프록시옵션에대해알아봅니다. 개념은다른 MDX 앱에도적용됩니다.

다음순서도는 SSO 및사용자연결에대한의사결정흐름을요약한것입니다.



Citrix ADC 인증방법

이섹션에서는 Citrix ADC 가지원하는인증방법에대한일반정보를제공합니다.

SAML 인증

SAML(Security Assertion Markup Language) 을사용하도록 Citrix ADC 를구성하는경우사용자는 SSO(Single Sign-on) 에 SAML 프로토콜을지원하는웹앱에연결할수있습니다. Citrix Gateway 는 SAML 웹앱에대해 IdP(ID 공급자) SSO(Single Sign-on) 를지원합니다.

필요한구성:

- Citrix ADC 트래픽프로필에서 SAML SSO 를구성합니다.
- 요청한서비스에대한 SAML IdP 를구성합니다.

NTLM 인증

세션프로필에서웹앱에대한 SSO 를사용하도록설정하면 Citrix ADC 가자동으로 NTLM 인증을수행합니다.

필요한구성:

- Citrix ADC 세션또는트래픽프로필에서 SSO 를사용하도록설정합니다.

Kerberos 가장

XenMobile 은 Secure Web 에대해서만 Kerberos 를지원합니다. Kerberos SSO 를사용하도록 Citrix ADC 를구성하는경우사용자암호가 Citrix ADC 에제공되면 Citrix ADC 가가장을사용합니다. 가장은 Citrix ADC 가 Secure Web 같은서비스에액세스하는데필요한티켓을사용자자격증명을사용하여가져온다는것을의미합니다.

필요한구성:

- 연결에서 Kerberos 영역을식별할수있도록 Citrix ADC “Worx” 세션정책을구성합니다.
- Citrix ADC 에서 KCD(Kerberos 제한위임) 계정을구성합니다. 이계정을암호없이구성하고 XenMobile 게이트웨이의트래픽정책에바인딩합니다.
- 이러한구성및다른구성에대한세부정보는 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 Citrix ADC 를구성하는경우사용자암호가 Citrix ADC 에제공되지않으면 Citrix ADC 가제한위임을사용합니다.

제한위임을사용하는경우 Citrix ADC 는사용자및서비스에대한티켓을가져올때지정된관리자계정을사용합니다.

필요한구성:

- Citrix ADC 의필요한권한및 KCD 계정을사용하여 Active Directory 에서 KCD 계정을구성합니다.
- Citrix ADC 트래픽프로필에서 SSO 를사용하도록설정합니다.
- Kerberos 인증에대한백엔드웹사이트를구성합니다.

양식입력인증

양식기반 SSO(Single Sign-on) 를사용하도록 Citrix ADC 를구성하는경우사용자는단한번의로그온으로네트워크의모든보호되는앱에액세스할수있습니다. 이인증방법은 Secure Browse 또는전체 VPN 모드를사용하는앱에적용됩니다.

필요한구성:

- Citrix ADC 트래픽프로필에서양식기반 SSO 를구성합니다.

다이제스트 **HTTP** 인증

세션프로필에서웹앱에대한 SSO 를사용하도록설정하면 Citrix ADC 가자동으로다이제스트 HTTP 인증을수행합니다. 이인증방법은 Secure Browse 또는전체 VPN 모드를사용하는앱에적용됩니다.

필요한구성:

- Citrix ADC 세션또는트래픽프로필에서 SSO 를사용하도록설정합니다.

기본 **HTTP** 인증

세션프로필에서웹앱에대한 SSO 를사용하도록설정하면 Citrix ADC 가자동으로기본 HTTP 인증을수행합니다. 이인증방법은 Secure Browse 또는전체 VPN 모드를사용하는앱에적용됩니다.

필요한구성:

- Citrix ADC 세션또는트래픽프로필에서 SSO 를사용하도록설정합니다.

Secure Browse, 전체 **VPN** 터널또는 **PAC** 포함전체 **VPN** 터널

다음섹션에서는 Secure Web 에대한사용자연결유형에대해설명합니다. 자세한내용은 Citrix 설명서에서 Secure Web 문서 사용자연결구성을참조하십시오.

전체 **VPN** 터널

내부네트워크로터널링되는연결은전체 VPN 터널을사용할수있습니다. Secure Web 의기본설정 VPN 모드정책을사용하여전체 VPN 터널을구성할수있습니다. 클라이언트인증서또는종단간 SSL 을사용하여내부네트워크의리소스로연결되는경우전체 VPN 터널을사용하는것이좋습니다. 전체 VPN 터널은모든프로토콜을 TCP 를통해처리합니다. 전체 VPN 터널을 Windows, Mac, iOS 및 Android 장치에서사용할수있습니다.

전체 VPN 터널모드에서 Citrix ADC 는 HTTPS 세션내부를볼수없습니다.

Secure Browse

내부네트워크에터널링되는연결은 Secure Browse 라고하는클라이언트없는 VPN 의변형을사용할수있습니다. Secure Browse 는 Secure Web 의 기본설정 **VPN** 모드정책에대해지정된기본구성입니다. SSO(Single Sign-On) 가필요한연결에는 Secure Browse 를사용하는것이좋습니다.

Secure Browse 모드에서 Citrix ADC 는 HTTPS 세션을두부분으로분리합니다.

- 클라이언트에서 Citrix ADC 로
- Citrix ADC 에서백엔드리소스서버로

Citrix ADC 는이와같은분리를통해클라이언트와서버간의모든트랜잭션을파악하고 SSO 를제공합니다.

Secure Browse 모드에서사용될때 Secure Web 에대해프록시서버를구성할수도있습니다. 자세한 XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode(Secure Browse 모드에서프록시서버를통한 XenMobile WorxWeb 트래픽) 블로그를참조하십시오.

PAC 포함전체 **VPN** 터널

iOS 및 Android 장치의 Secure Web 에대해전체 VPN 터널배포와함께 PAC(Proxy Automatic Configuration) 파일을사용할수있습니다. XenMobile 은 Citrix ADC 에의해제공되는프록시인증을지원합니다. PAC 파일에는웹브라우저에서해당 URL 에액세스하기위해프록시를선택하는방식을정의하는규칙이포함됩니다. PAC 파일규칙은내부및외부사이트에대한처리방식을지정할수있습니다. Secure Web 은 PAC 파일규칙을구문분석하고프록시서버정보를 Citrix Gateway 로보냅니다. Citrix Gateway 는 PAC 파일또는프록시서버를인지하지못합니다.

HTTPS 웹사이트인증의경우 Secure Web MDX 정책인 웹암호캐싱사용을통해 Secure Web 을인증하고 MDX 를통해프록시서버에 SSO 를제공할수있습니다.

Citrix ADC 분할터널링

SSO 및프록시구성을계획할때는 Citrix ADC 분할터널링을사용할지여부또한결정해야합니다. Citrix ADC 분할터널링은필요한경우에만사용하는것이좋습니다. 이섹션에서는분할터널링의작동방식을간략히설명합니다. Citrix ADC 는라우팅테이블에따라트래픽경로를결정합니다. Citrix ADC 분할터널링이켜져있는경우 Secure Hub 는인터넷트래픽에서내부 (보호되는) 네트워크트래픽을구분합니다. Secure Hub 는 DNS 접미사및인트라넷응용프로그램을사용하여트래픽을구분합니다. 그런다음 Secure Hub 는내부네트워크트래픽만 VPN 터널을통해터널링합니다. Citrix ADC 분할터널링이꺼져있는경우모든트래픽이 VPN 터널을통과합니다.

- 보안상의이유로모든트래픽을모니터링해야하는경우 Citrix ADC 분할터널링을사용중지하십시오. 그러면모든트래픽이 VPN 터널을통과합니다.
- PAC 포함전체 VPN 터널을사용하는경우 Citrix Gateway 분할터널링을사용하지않아야합니다. 분할터널링이켜져있고 PAC 파일이구성된경우 PAC 파일규칙이 Citrix ADC 분할터널링규칙보다우선합니다. 트래픽정책에구성된프록시서버는 Citrix ADC 분할터널링규칙을재정의하지않습니다.

기본적으로 네트워크액세스정책은 Secure Web 에대해 내부네트워크로터널링됨으로설정됩니다. 이구성에서 MDX 앱은 Citrix ADC 분할터널링설정을사용합니다. 일부다른모바일생산성앱의경우 네트워크액세스정책의기본값이다릅니다.

Citrix Gateway 에는 Micro VPN 역분할터널링모드도있습니다. 이구성에서는 Citrix ADC 로터널링되지않는 IP 주소로구성된제외목록을사용할수있습니다. 이러한주소는장치의인터넷연결을사용하여전송됩니다. 역분할터널링에대한자세한내용은 Citrix Gateway 설명서를참조하십시오.

XenMobile 에는 역분할터널링제외목록이포함됩니다. 특정웹사이트를 Citrix Gateway 를통해터널링하지않으려는경우 LAN 을대신사용하여연결하는 FQDN(정규화된도메인이름) 또는 DNS 접미사의쉼표로구분된목록을추가할수있습니다. 이목록은역분할터널링이구성된 Citrix Gateway 의 Secure Browse 모드에서만적용됩니다.

인증

January 5, 2022

XenMobile 배포에서인증을구성하는방법을결정할때는여러요소를고려해야합니다. 이섹션에서는다음을설명하여인증에영향을 미치는다양한요소를쉽게이해할수있도록합니다.

- 인증과관련된기본 MDX 정책, XenMobile 클라이언트속성및 Citrix Gateway 설정.
- 이러한정책, 클라이언트속성및설정의상호작용방식.
- 각선택의득실.

이문서에는보안수준을높이려는경우권장되는구성에대한세가지예제도포함되어있습니다.

광범위하게말해보안이강력하면사용자가더자주인증해야하므로사용자환경이덜최적화됩니다. 이러한요소의균형을맞추는방식은 조직의요구사항및우선순위에따라다릅니다. 권장되는세가지구성을검토하여사용가능한인증방법의상호작용과 XenMobile 환경의배포를최적화하는방법을파악하십시오.

인증모드

온라인인증**:** 사용자가 XenMobile 네트워크에들어갈수있습니다. 인터넷연결이필요합니다.

오프라인인증**:** 인증이장치에서수행됩니다. 사용자가보안저장소의잠금을해제하고, 다운로드된메일, 캐싱된웹사이트및메모같은 항목에오프라인으로액세스합니다.

인증방법

1 단계

LDAP: XenMobile 에서 LDAP(Lightweight Directory Access Protocol) 와호환되는하나이상의디렉터리 (예: Active Directory) 에대한연결을구성할수있습니다. 회사환경에대한 SSO(Single Sign-on) 를제공할때주로사용되는방법입니다. Active Directory 암호캐싱을통해 Citrix PIN 을사용하도록선택하면 LDAP 로사용자환경을개선하는동시에등록, 암호만료및계정잠금시복잡한암호를사용하는보안을제공할수있습니다.

자세한내용은 도메인또는도메인및 STA를참조하십시오.

클라이언트인증서**:** XenMobile 을업계표준인증기관과통합하여인증서를온라인인증의유일한방법으로사용할수있습니다. XenMobile 은일회용암호, 초대 URL 또는 LDAP 자격증명이필요한사용자등록후이인증서를제공합니다. 클라이언트인증서를 기본적인인증방법으로사용하는경우 Citrix PIN 을사용하여클라이언트인증서전용환경에서장치의인증서를보호해야합니다.

XenMobile 은타사인증기관에대해서만 CRL(인증서해지목록) 을지원합니다. Microsoft CA 가구성된경우 XenMobile 은 Citrix ADC 를사용하여인증서해지를관리합니다. 클라이언트인증서기반인증을구성하는경우 Citrix ADC CRL(인증서해지목록) 설정인 Enable CRL Auto Refresh(CRL 자동새로고침사용) 를구성해야하는지여부를고려합니다. 이렇게하면 MAM 전용모드의장치사용자가장치의기존인증서를사용하여인증할수없습니다. 이경우 XenMobile 은새인증서를다시발급합니다. 사용자인증서가해지된경우사용자의인증서생성을제한하지않기때문입니다. 이설정을사용하면 CRL 이만료된 PKI 엔터티를확인하는경우 PKI 엔터티의보안이강화됩니다.

인증서기반인증을사용하여사용자를인증하거나엔터프라이즈 CA(인증기관) 를사용하여장치인증서를발급하려는경우필요한배포를보여주는다이어그램은 온-프레미스배포용참조아키텍처를참조하십시오.

2 단계

LDAP + 클라이언트인증서**:** XenMobile 환경에서이구성은 Citrix ADC 의 2 단계인증을통한보안과최상의 SSO 기능으로보안과사용자환경을최적화합니다. LDAP 와클라이언트인증서를모두사용하면사용자가알고있는것 (Active Directory 암호) 과사용자가가지고있는것 (장치의클라이언트인증서) 을사용하여보안을제공할수있습니다. Secure Mail(및다른모바일생산성앱) 은올바르게구성된 Exchange 클라이언트액세스서버환경에서클라이언트인증서인증을통해처음사용하는사용자를위한원활한환경을자동으로구성하고제공할수있습니다. 사용편의성을최적화하기위해이옵션을 Citrix PIN 및 Active Directory 암호캐싱과결합할수있습니다.

LDAP + 토큰**:** 이구성에서는전형적인 LDAP 자격증명구성에더해 RADIUS 프로토콜을사용하는일회용암호를사용할수있습니다. 사용편의성을최적화하기위해이옵션을 Citrix PIN 및 Active Directory 암호캐싱과결합할수있습니다.

인증과관련된중요정책**,** 설정및클라이언트속성

다음은권장되는세가지구성에서중요한역할을하는정책, 설정및클라이언트속성입니다.

MDX 정책

앱암호**:** 켜짐인경우, 앱을시작하거나비활성화된후다시시작할때앱잠금을해제하려면 Citrix PIN 또는암호가필요합니다. 기본값은 켜짐입니다.

모든앱에대해비활성화타이머를구성하려면 XenMobile 콘솔에서 설정탭의 클라이언트속성에서 INACTIVITY_TIMER 값을 분으로설정합니다. 기본값은 15 분입니다. 비활성화타이머를사용하지않고앱을시작할때만 PIN 또는암호입력메시지가표시되도록하려면값을 0 으로설정합니다.

> 참고**:**
>
> 암호화키정책에대해보안오프라인을선택하는경우이정책이자동으로사용됩니다.

온라인세션필요**:** 켜짐인경우, 사용자가엔터프라이즈네트워크에연결되어있고세션이활성상태여야장치의앱에액세스할수있습니다. 꺼짐인경우활성세션이없어도장치의앱에액세스할수있습니다. 기본값은 꺼짐입니다.

최대오프라인기간 **(**시간**):** XenMobile 에서앱권한부여재확인및정책새로고침없이앱을실행할수있는최대기간을정의합니다. 최대오프라인기간을설정하는경우 iOS 용 Secure Hub 에유효한 Citrix Gateway 토큰이있으면앱이사용자작업중단없이 XenMobile 에서 MDX 앱에대한새정책을검색합니다. Secure Hub 에유효한 Citrix ADC 토큰이없는경우앱정책을업데이트

하려면사용자가 Secure Hub 를통해인증해야합니다. Citrix Gateway 세션이비활성화되거나세션시간초과정책이적용되는 경우 Citrix ADC 토큰이무효화될수있습니다. 사용자가 Secure Hub 에다시로그온하면앱을계속실행할수있습니다.

이기간이만료되기 30 분, 15 분및 5 분전에사용자에게로그온하라는메시지가표시되며이기간이만료되면사용자가로그온할때까지앱은잠긴상태를유지합니다. 기본값은 **72** 시간 **(3** 일**)** 입니다. 최소기간은 1 시간입니다.

> 참고**:**
>
> 사용자가이동이잦고해외로밍을사용해야할수있는시나리오의경우 72 시간 (3 일) 의기본값이너무짧을수있습니다.

백그라운드서비스티켓만료**:** 백그라운드네트워크서비스티켓이유효한기간입니다. Secure Mail 이 Citrix Gateway 를통해 ActiveSync 를실행하는 Exchange Server 에연결하는경우 XenMobile 에서 Secure Mail 이내부 Exchange Server 에연결하는데사용할토큰을발급합니다. 이속성설정에따라 Secure Mail 이인증및 Exchange Server 에대한연결에사용할새 토큰을요구하지않고토큰을사용할수있는기간이결정됩니다. 시간제한이만료되면사용자가다시로그온해야새토큰이생성됩니다. 기본값은 **168** 시간 **(7** 일**)** 입니다. 이시간제한이만료되면메일알림이중단됩니다.

온라인세션에필요한유예기간 **(**분**):** 온라인세션필요정책에따라앱을더이상사용하지못하게될때까지온라인세션의유효성이검사 되지않고도사용자가앱을오프라인으로사용할수있는시간 (분) 을결정합니다. 기본값은 0(유예기간없음) 입니다.

인증정책에대한정보는다음을참조하십시오.

- MAM SDK 를사용하는경우: MAM SDK 개요
- MDX Toolkit 을사용하는경우: iOS 용 MDX 정책 및 Android 용 MDX 정책

XenMobile 클라이언트속성

> 참고**:**
>
> 클라이언트속성은 XenMobile 에연결하는모든장치에적용되는글로벌설정입니다.

Citrix PIN: 단순한로그인환경을제공하려면 Citrix PIN 을사용하도록선택할수있습니다. PIN 을사용하면사용자가 Active Directory 사용자이름및암호같은다른자격증명을반복적으로입력하지않아도됩니다. Citrix PIN 을독립실행형오프라인인증으로만구성하거나 PIN 을 Active Directory 암호캐싱과결합하여인증을간소화함으로써사용편의성을최적화할수있습니다. XenMobile 콘솔의 설정 **>** 클라이언트 **>** 클라이언트속성에서 Citrix PIN 을구성할수있습니다.

다음은몇가지속성을요약한것입니다. 자세한내용은 클라이언트속성을참조하십시오.

ENABLE_PASSCODE_AUTH

표시이름**:** Enable Citrix PIN Authentication(Citrix PIN 인증사용)

이키를사용하여 Citrix PIN 기능을활성화할수있습니다. Citrix PIN 또는암호를사용하는경우 Active Directory 암호대신사용할 PIN 을정의하라는메시지가나타납니다. **ENABLE_PASSWORD_CACHING** 을사용하도록설정했거나 XenMobile 에서인증서인증을사용하는경우이설정을사용하도록설정해야합니다.

가능한값**: true** 또는 **false**

기본값**: false**

ENABLE_PASSWORD_CACHING

표시이름**:** Enable User Password Caching(사용자암호캐싱사용)

이키를사용하면사용자의 Active Directory 암호가모바일장치에로컬로캐싱됩니다. 이키를 true 로설정하면 Citrix PIN 또는암호를설정하라는메시지가사용자에게표시됩니다. 이키를 **true** 로설정하는경우 ENABLE_PASSCODE_AUTH 키를 true 로설정해야합니다.

가능한값**: true** 또는 **false**

기본값**: false**

PASSCODE_STRENGTH

표시이름**:** PIN Strength Requirement(PIN 강도요구사항)

이키는 Citrix PIN 또는암호의강도를정의합니다. 이설정을변경하면사용자가다음번에인증을수행할때새 Citrix PIN 또는암호를설정하라는메시지가나타납니다.

가능한값**:** 약함, 중간, 강함

기본값**:** 중간

INACTIVITY_TIMER

표시이름**:** Inactivity Timer(비활성타이머)

이키는사용자가장치를비활성상태로둔후에 Citrix PIN 또는암호를입력하라는메시지없이앱에액세스할수있는시간 (분단위) 을정의합니다. MDX 앱에대해이설정을사용되도록설정하려면앱암호설정을 켜짐으로설정해야합니다. 앱암호설정이 꺼짐으로설정된경우사용자는전체인증을수행하기위해 Secure Hub 로리디렉션됩니다. 이설정을변경하면다음에사용자에게인증하라는메시지가표시될때값이적용됩니다. 기본값은 15 분입니다.

ENABLE_TOUCH_ID_AUTH

표시이름**:** Enable Touch ID Authentication(Touch ID 인증사용)

오프라인인증에서지문판독기 (iOS 만해당) 를사용할수있습니다. 온라인인증에서는기본인증방법을사용해야합니다.

ENCRYPT_SECRETS_USING_PASSCODE

표시이름**:** Encrypt secrets using Passcode(암호를사용하여암호암호화)

이키를사용하면민감한데이터를 iOS 키집합과같은플랫폼기반기본저장소가아닌모바일장치의기밀저장소에저장할수있습니다. 이구성키는주요아티팩트의강력한암호화를활성화하지만사용자엔트로피 (사용자만알고있는사용자생성임의 PIN 코드) 도증가합니다.

가능한값**: true** 또는 **false**

기본값**: false**

Citrix ADC 설정

Session time-out(세션시간초과**):** 이설정을사용하면 Citrix ADC 에서지정된간격동안네트워크활동이감지되지않을경우 Citrix Gateway 가세션연결을끊습니다. 이설정은 Citrix Gateway 플러그인, Citrix Receiver, Secure Hub 또는웹브라우저를통해연결하는사용자에게적용됩니다. 기본값은 **1440** 분입니다. 이값을 0 으로설정하면설정이사용되지않습니다.

Forced time-out(시간초과강제적용**):** 이설정을사용하면 Citrix Gateway 가시간초과간격이지난후사용자의활동여부와관계없이세션연결을끊습니다. 시간초과간격이경과하면사용자는어떠한작업으로도연결중단을방지할수없습니다. 이설정은 Citrix Gateway 플러그인, Citrix Receiver, Secure Hub 또는웹브라우저를통해연결하는사용자에게적용됩니다. Secure Mail 에서특수 Citrix ADC 모드인 STA 를사용하는경우 Secure Mail 세션에는시간초과강제적용설정이적용되지않습니다. 기본값은 **1440** 분입니다. 이값을비워두면설정이사용되지않습니다.

Citrix Gateway 의시간초과설정에대한자세한내용은 Citrix ADC 설명서를참조하십시오.

장치에서자격증명을입력하여 XenMobile 을통해인증하라는메시지를사용자에게표시하는시나리오에대한자세한내용은 인증프롬프트시나리오를참조하십시오.

기본구성설정

이러한설정은다음에서제공하는기본값입니다.

- NetScaler for XenMobile 마법사
- MAM SDK 또는 MDX Toolkit
- XenMobile 콘솔

설정	설정을찾는위치	기본설정
세션시간초과	Citrix Gateway	1440 분
Force time-out(강제시간초과)	Citrix Gateway	1440 분
최대오프라인기간	MDX 정책	72 시간
백그라운드서비스티켓만료	MDX 정책	168 시간 (7 일)
온라인세션필요	MDX 정책	꺼짐
온라인세션에필요한유예기간	MDX 정책	0
앱암호	MDX 정책	켜짐
Encrypt secrets using Passcode(암호를사용하여암호암호화)	XenMobile 클라이언트속성	False
Enable Citrix PIN Authentication(Citrix PIN 인증사용)	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

설정	설정을찾는위치	기본설정
Inactivity Timer(비활성화타이머)	XenMobile 클라이언트속성	15
Enable Touch ID Authentication(Touch ID 인증 사용)	XenMobile 클라이언트속성	False

권장되는구성

이섹션에서는가장낮은수준의보안과최적의사용자환경부터가장높은수준의보안과좀더불편한사용자환경에이르는세가지 XenMobile 구성예제를제공합니다. 이러한예제는자체구성을적용할위치를결정할때유용한참조로사용될수있습니다. 이러한설정을수정하려면다른설정도함께변경해야합니다. 예를들어최대오프라인기간은세션시간초과보다작아야합니다.

최고수준의보안

이구성은가장높은수준의보안을제공하지만사용편의성이크게떨어지는단점이있습니다.

설정	설정을찾는위치	권장되는설정	동작의영향
세션시간초과	Citrix Gateway	1440	사용자는온라인인증이요구되는경우에만 24 시간마다 Secure Hub 자격증명을 입력합니다.
Force time-out(강제시간초과)	Citrix Gateway	1440	온라인인증이 24 시간마다 엄격히요구됩니다. 활동이 있다고해서세션수명이연장되지는않습니다.
최대오프라인기간	MDX 정책	23	매일정책을새로고쳐야합니다.

백그라운드서비스티켓만료	MDX 정책	72 시간	STA 에대한시간제한으로, Citrix Gateway 세션토큰없이세션수명을연장할수있습니다. Secure Mail 의경우 STA 시간초과를세션시간초과보다길게설정하면사용자가세션이만료되기전에앱을열지않은경우사용자에게메시지를표시하지않고메일알림이중지되는상황을방지할수있습니다.
온라인세션필요	MDX 정책	꺼짐	유효한네트워크연결및 Citrix 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 강도요구사항)	XenMobile 클라이언트속성	Strong(강함)	높은수준의암호복잡성을요구합니다.
PIN Type(PIN 유형)	XenMobile 클라이언트속성	영숫자	영숫자시퀀스의 PIN 을사용합니다.
Enable Password Caching(암호캐싱사용)	XenMobile 클라이언트속성	False	Active Directory 암호는캐싱되지않으며오프라인인증의경우 Citrix PIN 이사용됩니다.

Inactivity Timer(비활성화타이머)	XenMobile 클라이언트속성	15	사용자가이기간에 MDX 앱 또는 Secure Hub 를사용하지않으면오프라인인증에대한메시지가표시됩니다.
Enable Touch ID Authentication(Touch ID 인증사용)	XenMobile 클라이언트속성	False	iOS 에서오프라인인증에대해 Touch ID 를사용하지않도록설정합니다.

더높은수준의보안

중도에가까운접근방식인이구성은 7 일대신최대 3 일에한번씩사용자인증을요구하고보안을강화합니다. 인증횟수가증가하여컨테이너가더자주잠기므로장치를사용하지않을때의데이터보안이강화됩니다.

설정	설정을찾는위치	권장되는설정	동작의영향
세션시간초과	Citrix Gateway	4320	사용자는온라인인증이요구되는경우에만 3 일마다 Secure Hub 자격증명을입력합니다.
Force time-out(강제시간초과)	Citrix Gateway	값을지정하지않음	활동이있는경우세션이연장됩니다.
최대오프라인기간	MDX 정책	71	정책을 3 일마다새로고쳐야합니다. 시간차이를두면세션시간초과전에정책을새로고칠수있습니다.

백그라운드서비스티켓만료	MDX 정책	168 시간	STA 에대한시간제한으로, Citrix Gateway 세션토큰없이세션수명을연장할수있습니다. Secure Mail 의경우 STA 시간초과를세션시간초과보다길게설정하면사용자가세션이만료되기전에앱을열지않은경우사용자에게메시지를표시하지않고메일알림이중지되는상황을방지할수있습니다.
온라인세션필요	MDX 정책	꺼짐	유효한네트워크연결및 Citrix 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 강도요구사항)	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(비활성화타이머)	XenMobile 클라이언트속성	30	사용자가이기간에 MDX 앱 또는 Secure Hub 를사용하지않으면오프라인인증에대한메시지가표시됩니다.
Enable Touch ID Authentication(Touch ID 인증사용)	XenMobile 클라이언트속성	true	iOS 에서오프라인인증에대해 Touch ID 를사용하도록설정합니다.

높은수준의보안

이구성은사용자에게가장편리한환경과기본수준의보안을제공합니다.

설정	설정을찾는위치	권장되는설정	동작의영향
세션시간초과	Citrix Gateway	10080	사용자는온라인인증이요구되는경우에만 7 일마다 Secure Hub 자격증명을입력합니다.
Force time-out(강제시간초과)	Citrix Gateway	값을지정하지않음	활동이있는경우세션이연장됩니다.
최대오프라인기간	MDX 정책	167	정책을매주 (7 일마다) 새로고쳐야합니다. 시간차이를두면세션시간초과전에정책을새로고칠수있습니다.
백그라운드서비스티켓만료	MDX 정책	240	STA 에대한시간제한으로, Citrix Gateway 세션토큰없이세션수명을연장할수있습니다. Secure Mail 의경우 STA 시간초과를세션시간초과보다길게설정하면사용자가세션이만료되기전에앱을열지않은경우사용자에게메시지를표시하지않고메일알림이중지되는상황을방지할수있습니다.

온라인세션필요	MDX 정책	꺼짐	유효한네트워크연결및 Citrix 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 강도요구사항)	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 암호를보호하는데사용됩니다.
Inactivity Timer(비활성화타이머)	XenMobile 클라이언트속성	90	사용자가이기간에 MDX 앱 또는 Secure Hub 를사용하지않으면오프라인인증에대한메시지가표시됩니다.
Enable Touch ID Authentication(Touch ID 인증사용)	XenMobile 클라이언트속성	true	iOS 에서오프라인인증에대해 Touch ID 를사용하도록설정합니다.

상위단계인증사용

일부앱에는향상된인증 (예: 토큰또는적극적세션시간초과같은보조인증요소) 이필요할수있습니다. 이인증방법을 MDX 정책을통해제어할수있습니다. 또한이방법을사용하려면별개의가상서버를사용하여동일하거나다른 Citrix ADC 장비에서인증방법을제어해야합니다.

설정	설정을찾는위치	권장되는설정	동작의영향
대체 Citrix Gateway	MDX 정책	보조 Citrix ADC 장비의 FQDN 및포트가필요합니다.	보조 Citrix ADC 장비인증및세션정책을사용하여향상된인증을제어할수있습니다.

사용자가대체 Citrix Gateway 인스턴스에로그온하는앱을열면다른모든앱이이 Citrix Gateway 인스턴스를사용하여내부네트워크와통신합니다. 세션은향상된보안을사용하는 Citrix Gateway 인스턴스에서세션이시간초과되는경우에만하위수준의보안을사용하는 Citrix Gateway 인스턴스로전환됩니다.

온라인세션필요사용

Secure Web 같은특정응용프로그램의경우사용자세션이인증되고장치가인터넷에연결된동안에만사용자의앱실행을허용해야할수있습니다. 이정책을사용하면이옵션이적용되고유예기간동안사용자가작업을마칠수있습니다.

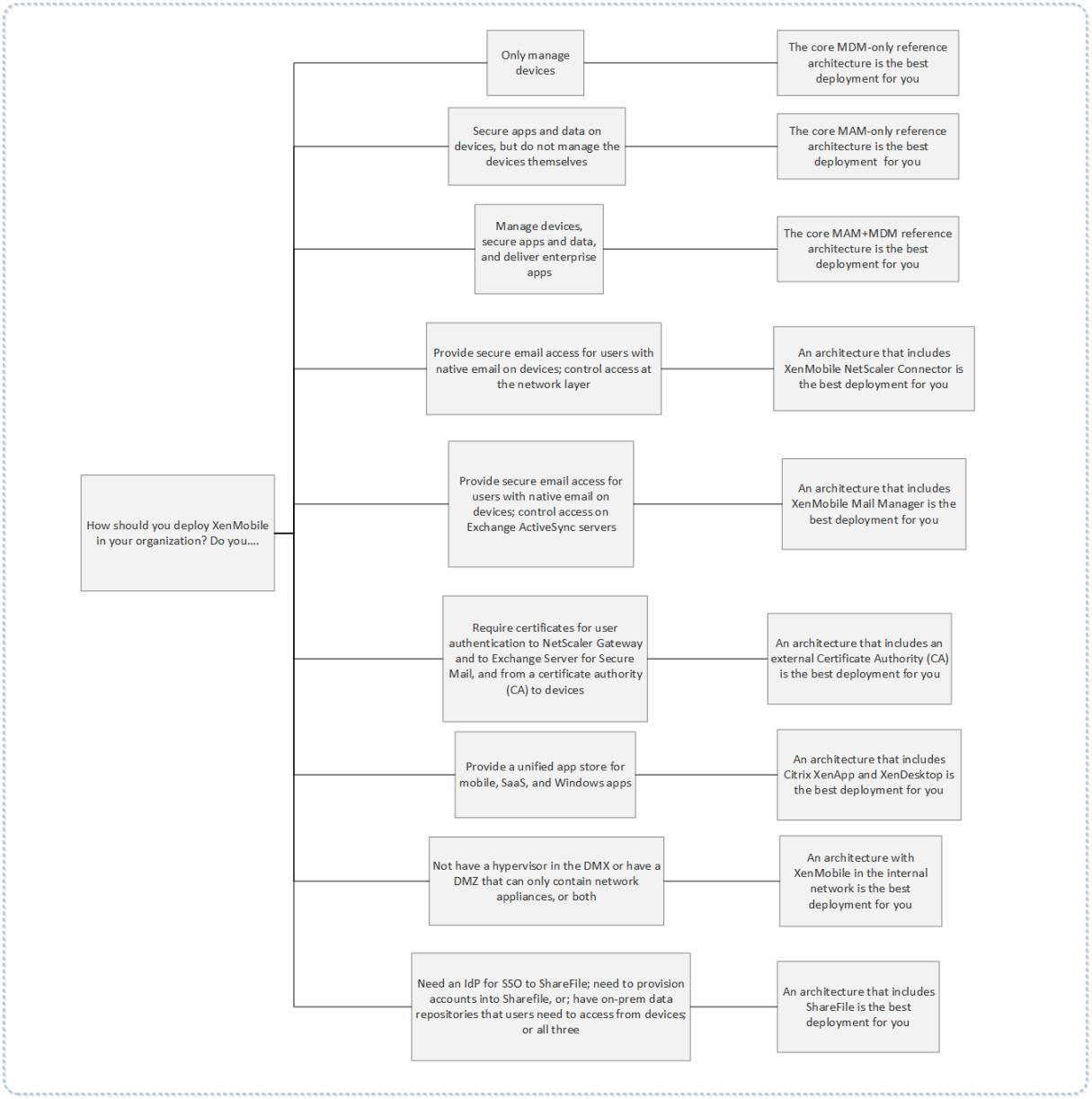
설정	설정을찾는위치	권장되는설정	동작의영향
온라인세션필요	MDX 정책	켜짐	장치가온라인상태이고유효한인증토큰이있는지확인합니다.
온라인세션에필요한유예기간	MDX 정책	15	사용자의앱사용을중지하기전에 15 분의유예기간을허용합니다.

온-프레미스배포용참조아키텍처

January 5, 2022

이문서의그림은 XenMobile 의온-프레미스배포에대한참조아키텍처를설명합니다. 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.

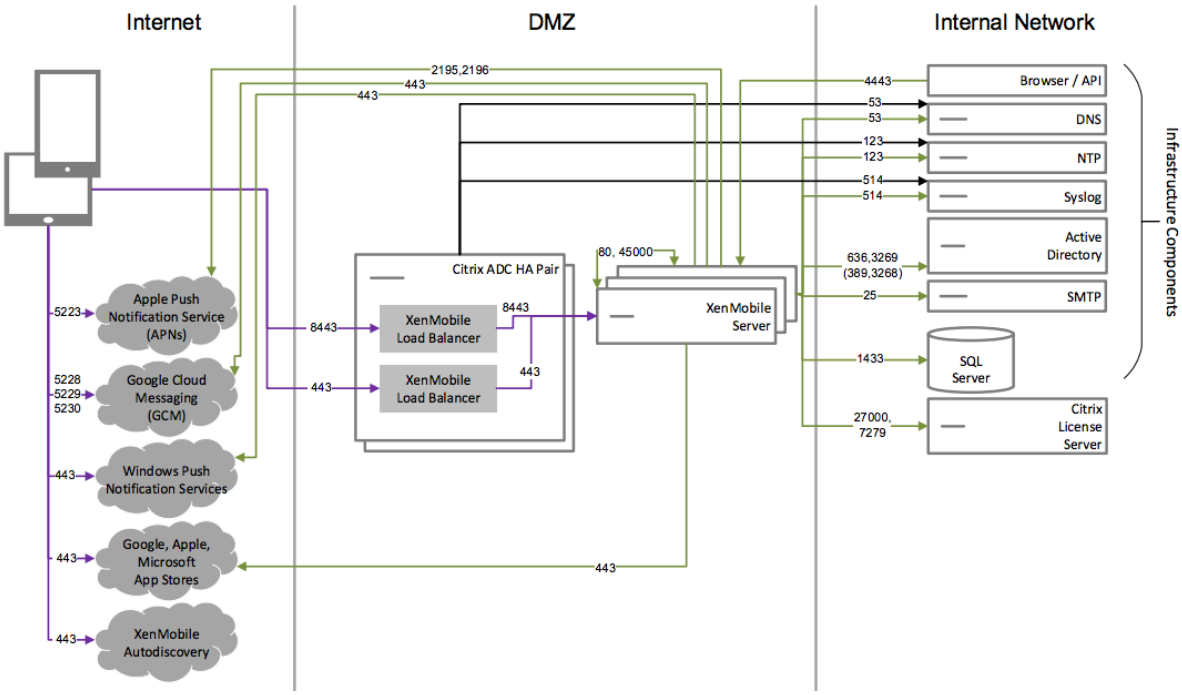
이차트를배포의사결정의일반지침으로사용하십시오.



그림에서커넥터위의숫자는구성요소간연결을허용하기위해열어야하는포트를나타냅니다. 전체포트목록은 XenMobile 설명서에서 포트요구사항을참조하십시오.

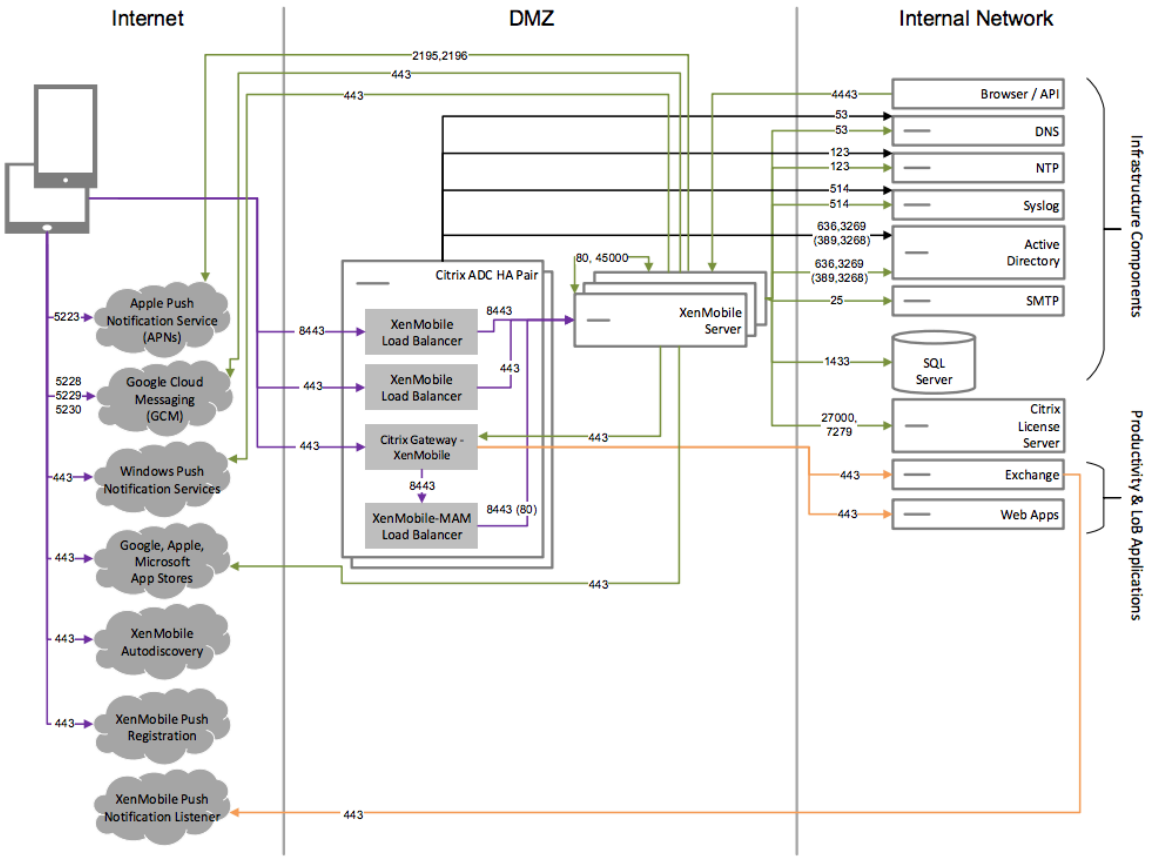
핵심 **MDM** 전용참조아키텍처

XenMobile 의 MDM 기능만사용하려는경우이아키텍처를배포합니다. 예를들어회사에서발급한장치를 MDM 을통해관리하여장치정책및앱을배포하고, 자산인벤토리를검색하고, 장치초기화같은동작을장치에수행해야하는경우이아키텍처를배포합니다.



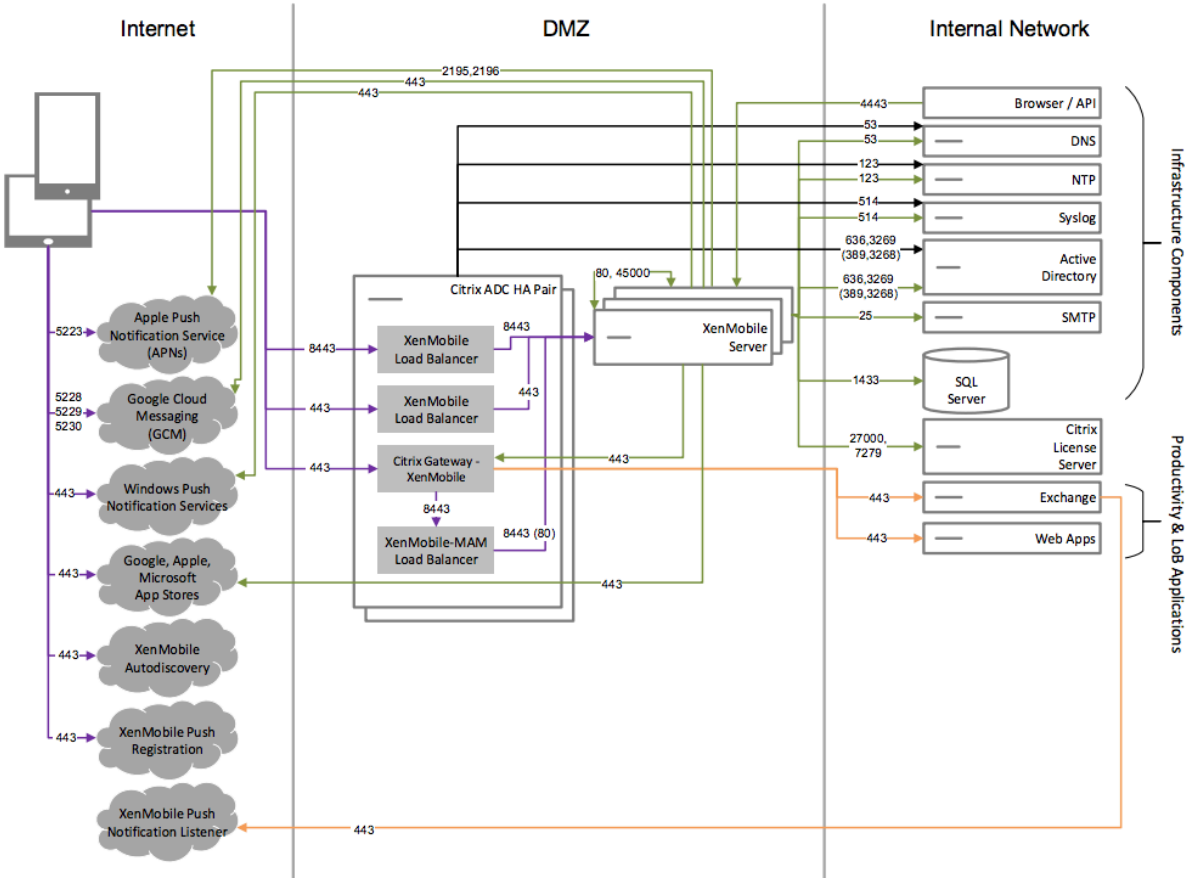
핵심 **MAM** 전용참조아키텍처

MDM 에대한장치등록없이 XenMobile 의 MAM 기능만사용하려는경우이아키텍처를배포합니다. 예를들어 BYO 모바일장치의앱및데이터를보호하려는경우와엔터프라이즈모바일앱을제공하고앱잠금및데이터초기화기능을사용하려는경우이아키텍처를배포할수있습니다. 장치를 MDM 에등록할수없습니다.



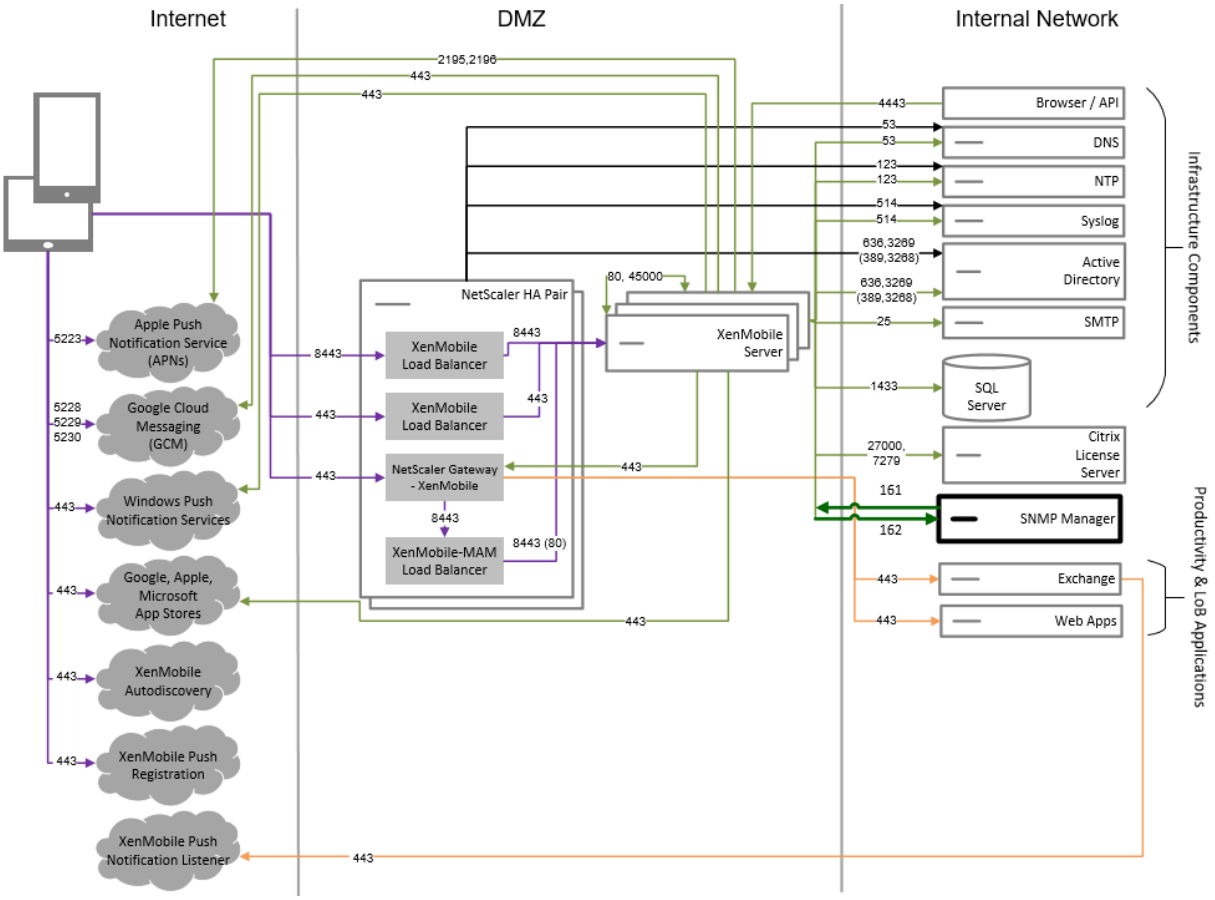
핵심 **MAM+MDM** 참조아키텍처

XenMobile 의 MDM+MAM 기능을사용하려는경우이아키텍처를배포합니다. 예를들어회사가발급한장치를 MDM 을통해관리하려는경우, 장치정책및앱을배포하려는경우, 자산인벤토리를검색하고장치를초기화하는기능을사용하려는경우이아키텍처를배포합니다. 또한엔터프라이즈모바일앱을제공하고앱잠금및장치의데이터초기화기능을사용하려는경우에도이아키텍처를배포할 수있습니다.



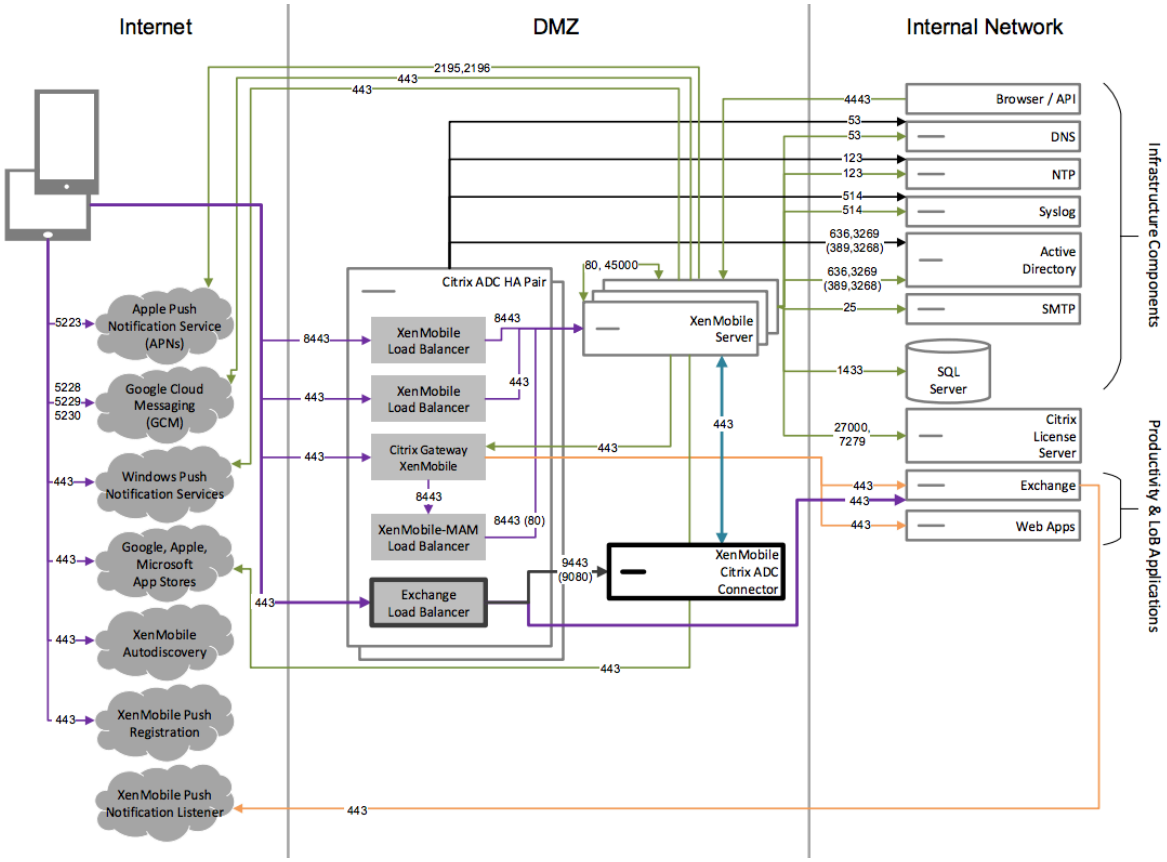
SNMP 를사용하는참조아키텍처

XenMobile 과함께 SNMP 모니터링을사용하려는경우이아키텍처를배포합니다. 예를들어모니터링시스템이 XenMobile 노드를쿼리하고노드의정보를가져오도록허용하려는경우이아키텍처를배포할수있습니다. 자세한내용은 SNMP 모니터링을참조하십시오.



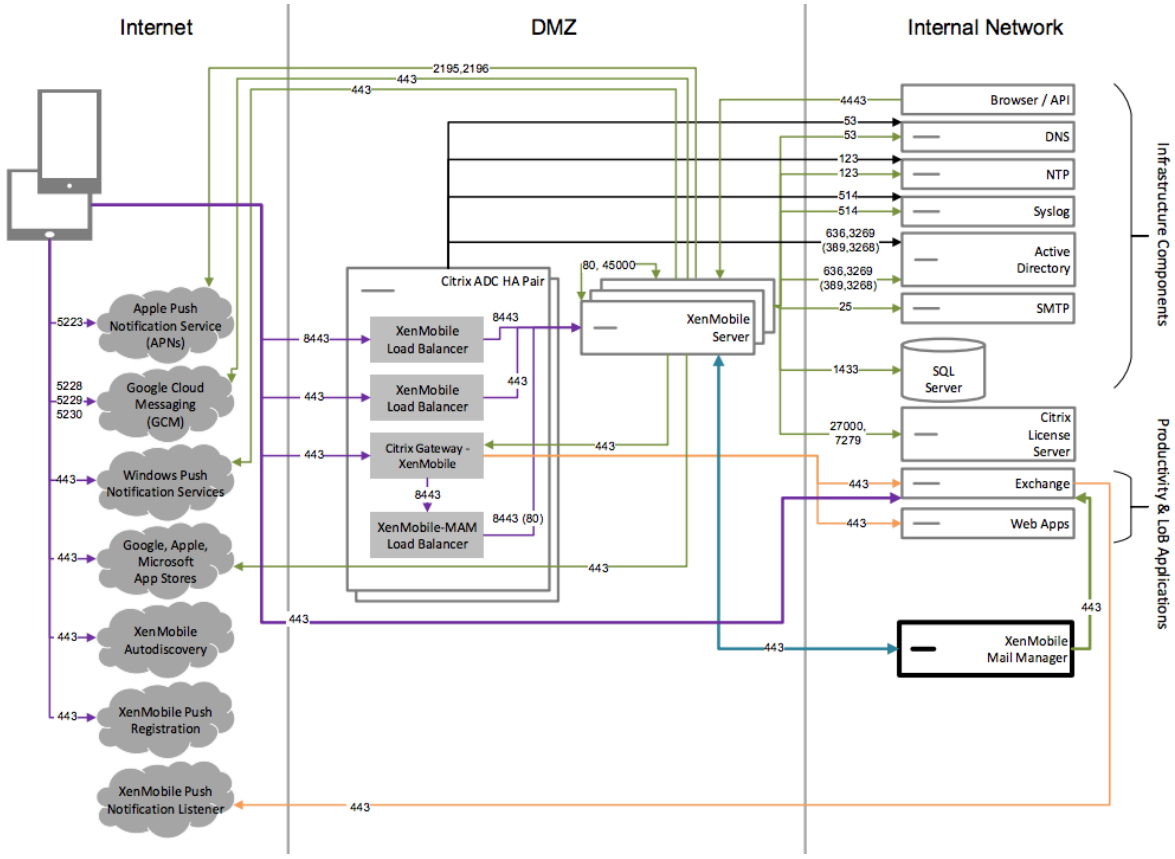
Exchange ActiveSync 용 **Citrix Gateway** 커넥터가포함된참조아키텍처

XenMobile 에서 Exchange ActiveSync 용 Citrix Gateway 커넥터를사용할계획이라면이아키텍처를배포하십시오. 예를들어기본모바일전자메일앱을사용하는사용자에게보안전자메일액세스를제공해야하는경우이아키텍처를배포할수있습니다. 이러한사용자는계속해서기본앱을통해전자메일에액세스하거나시간이지남에따라 Citrix Secure Mail 로전환할수있습니다. 액세스제어는트래픽이 Exchange Active Sync 서버에도달하기전에네트워크계층에서수행되어야합니다. 다이어그램에는 Exchange ActiveSync 용커넥터가 MDM 과 MAM 아키텍처에배포된것으로표시되었지만 Exchange ActiveSync 용커넥터를동일한방식으로 MDM 전용아키텍처의일부로배포할수도있습니다.



Exchange ActiveSync 용 **Endpoint Management** 커넥터가포함된참조아키텍처

XenMobile 에서 Exchange ActiveSync 용 Endpoint Management 커넥터를사용할계획이라면이아키텍처를배포하십시오. 예를들어기본모바일전자메일앱을사용하는사용자에게보안전자메일액세스를제공해야하는경우이아키텍처를배포할수있습니다. 이러한사용자는계속해서기본앱을통해전자메일에액세스하거나시간이지남에따라 Secure Mail 로전환할수있습니다. 액세스제어는 Exchange ActiveSync 서버에서수행할수있습니다. 다이어그램에는 MDM 및 MAM 아키텍처에배포된 Exchange ActiveSync 용 Endpoint Management 커넥터가표시되어있지만동일한방식으로 MDM 전용아키텍처의일부로 Exchange ActiveSync 용 Endpoint Management 커넥터를배포할수도있습니다.

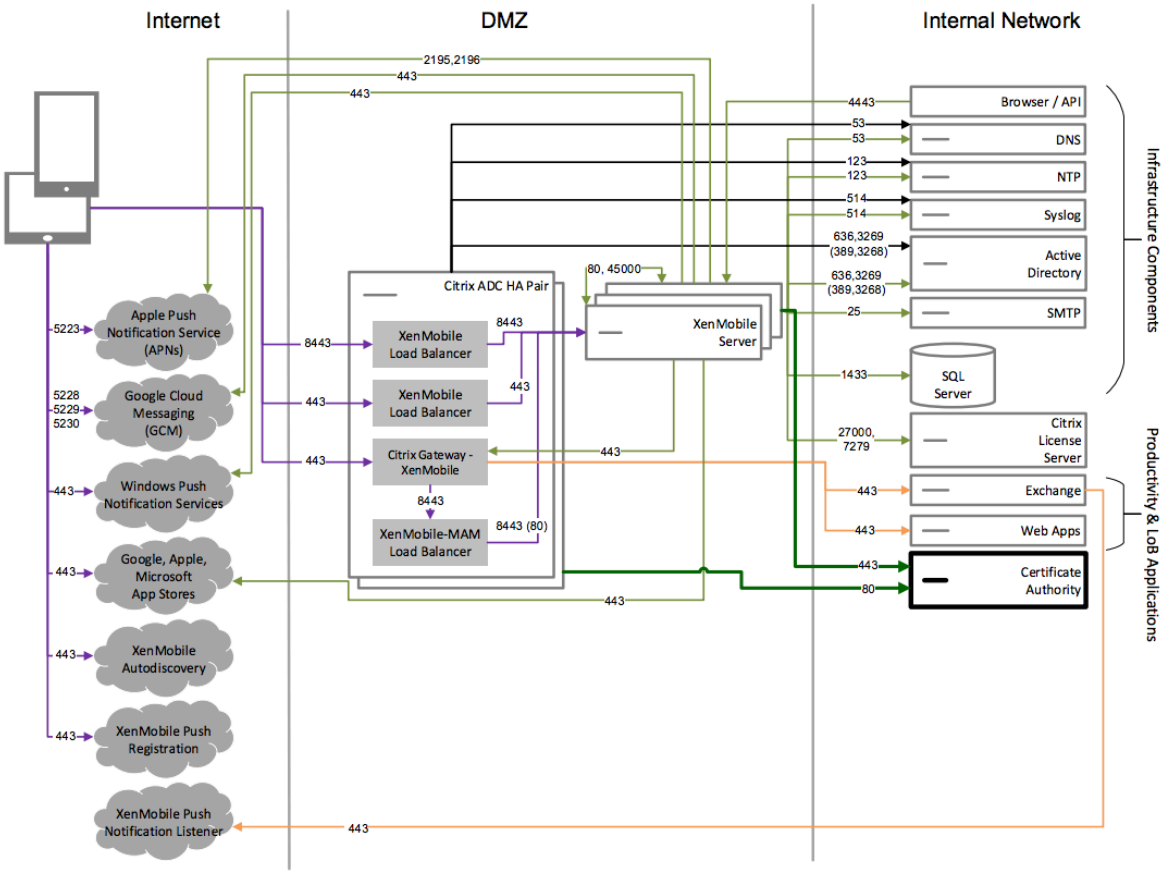


외부인증기관을사용하는참조아키텍처

외부인증기관을포함하는배포는다음요구사항을하나이상충족해야하는경우권장됩니다.

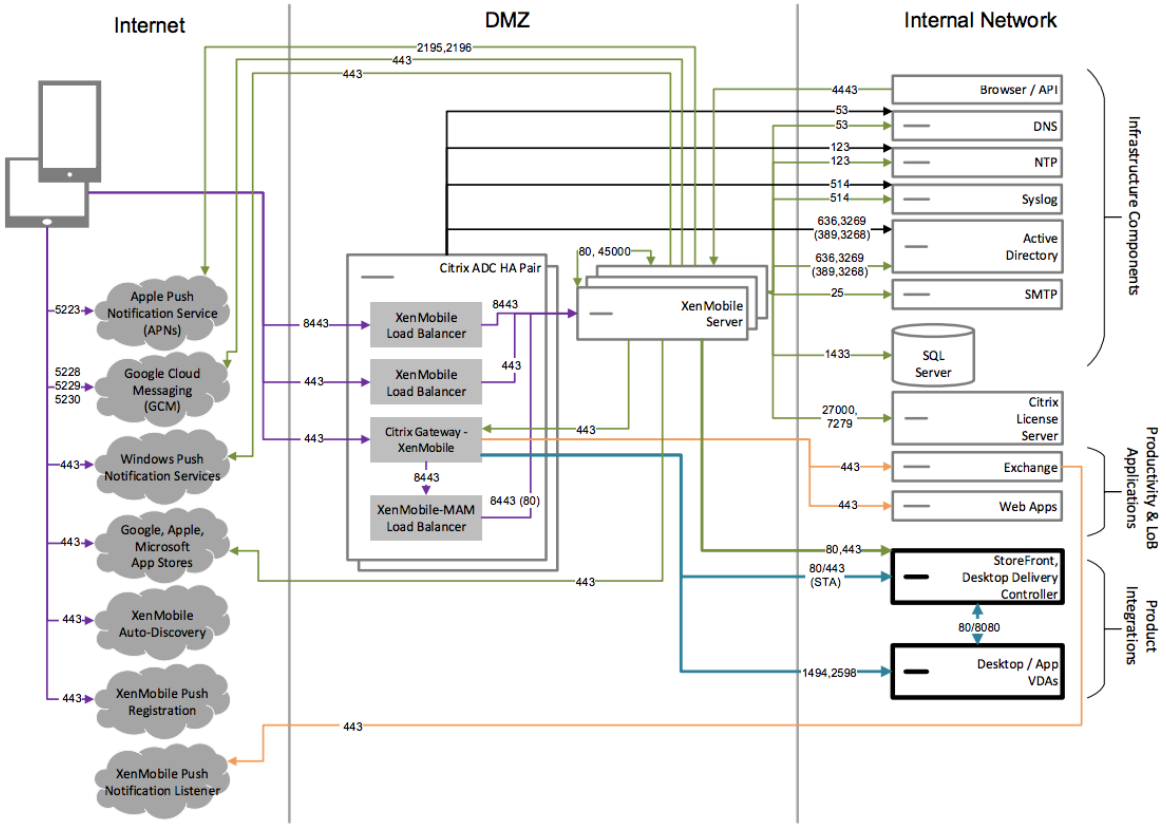
- Citrix Gateway 에대한사용자인증 (인트라넷액세스) 에사용자인증서를사용해야합니다.
- Secure Mail 사용자에게사용자인증서를사용하여 Exchange Server 에인증하도록해야합니다.
- 회사인증기관에서발급한인증서를모바일장치 (예: WiFi 액세스시) 에푸시해야합니다.

다이어그램에는 MDM+MAM 아키텍처로배포된외부인증기관이표시되어있지만외부인증기관을동일한방식으로 MDM 전용또는 MAM 전용아키텍처의일부로배포할수도있습니다.



Virtual Apps and Desktops 를사용하는참조아키텍처

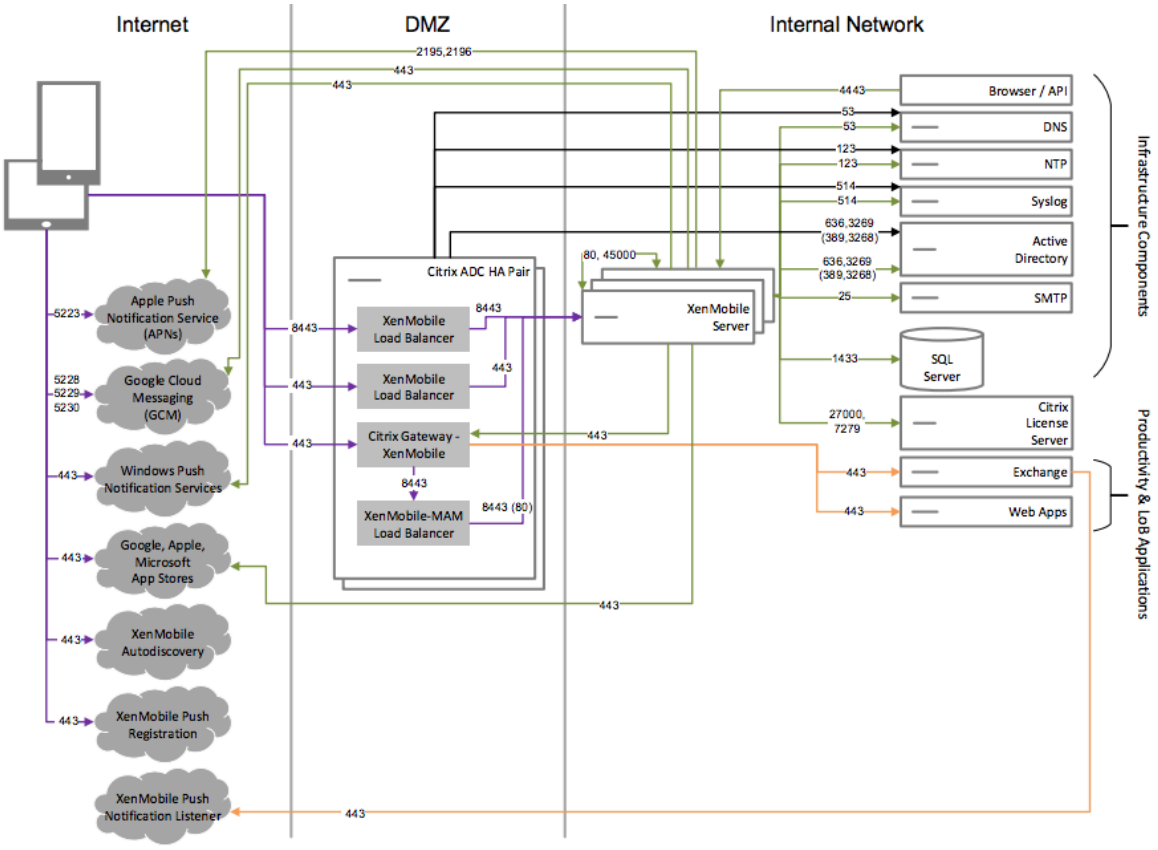
Virtual Apps and Desktops 를 XenMobile 과통합하려는경우이아키텍처를배포합니다. 예를들어모바일사용자에게모든유형의응용프로그램 (모바일, SaaS 및 Windows) 에대한통합앱스토어를제공해야하는경우이아키텍처를배포할수있습니다. 다이어그램에는 Virtula Desktops 가 MDM+MAM 아키텍처로배포된것으로표시되었지만이러한데스크톱을동일한방식으로 MAM 전용아키텍처의일부로배포할수도있습니다.



XenMobile 이내부네트워크에있는참조아키텍처

다음요구사항중하나이상을충족해야하는경우내부네트워크의 XenMobile 을사용하는아키텍처를배포할수있습니다.

- DMZ 에하이퍼바이저가없거나배치할수없습니다.
- DMZ 에는네트워크장비만포함되어야합니다.
- 보안요구사항에따라 SSL 오프로드를사용해야합니다.



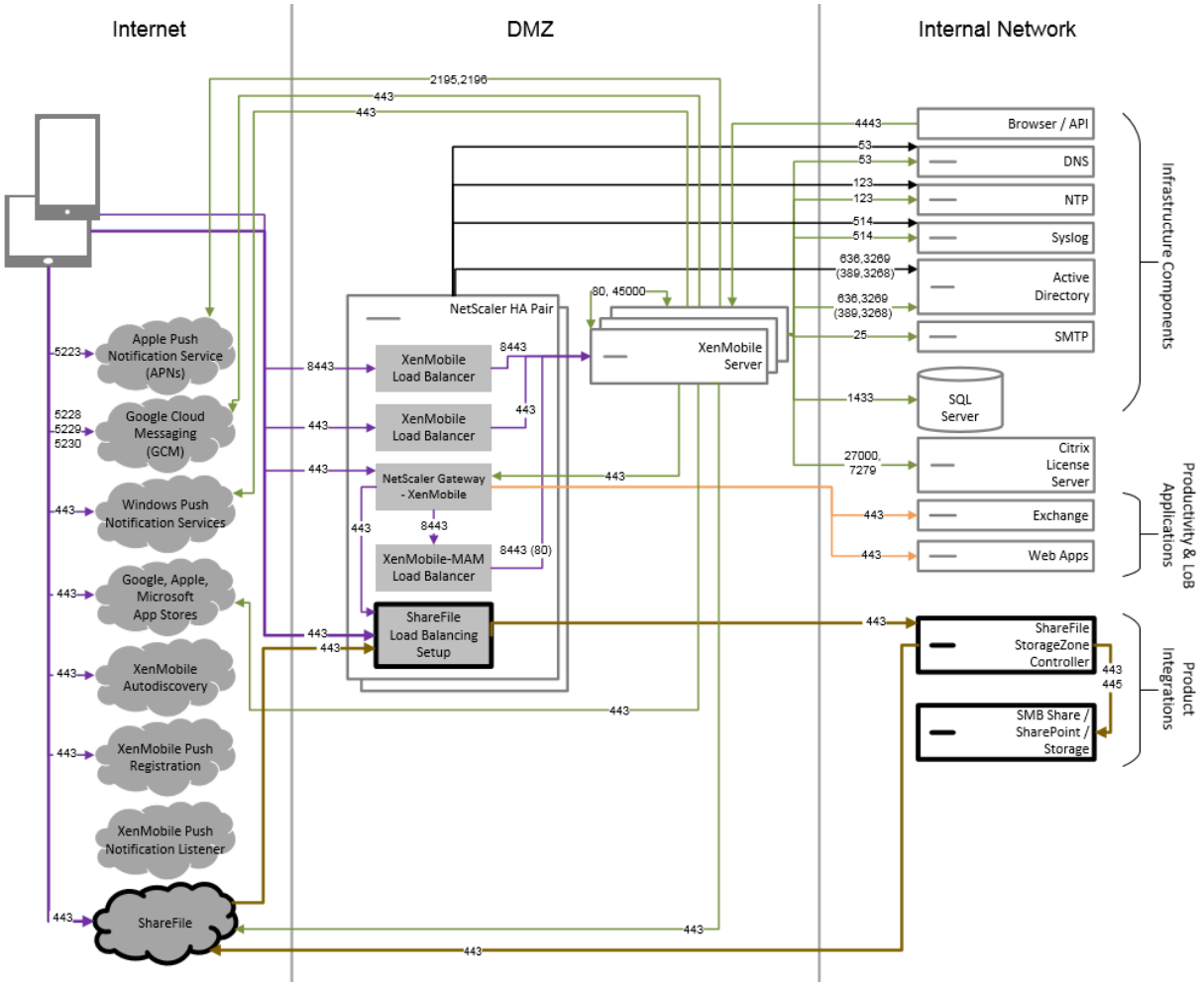
Citrix Content Collaboration 참조아키텍처

Citrix Files 또는 StorageZone 커넥터만 XenMobile 과통합하려는경우이아키텍처를배포합니다. Citrix Files 를통합하면다음요구사항중하나이상을충족할수있습니다.

- IDP 를통해 ShareFile.com 에대한 SSO(Single Sign-on) 를사용자에게제공해야합니다.
- ShareFile.com 에계정을프로비전할수있어야합니다.
- 모바일장치에서액세스해야하는온-프레미스데이터저장소가있습니다.

StorageZone 커넥터만통합하는경우 SharePoint 사이트및네트워크파일공유등의기존온-프레미스스토리지저장소에대한보안모바일액세스를사용자에게제공할수있습니다. 이구성에서는 Citrix Content Collaboration 하위도메인을설정하거나, Citrix Files 에사용자를프로비전하거나, Citrix Files 데이터를호스팅할필요가없습니다.

다이어그램에는 Citrix Files 가 MDM+MAM 아키텍처로배포된것으로표시되었지만 Citrix Files 를동일한방식으로 MAM 전용아키텍처의일부로배포할수도있습니다.



서버속성

May 6, 2022

서버속성은전체 XenMobile 인스턴스의작업, 사용자및장치에적용되는글로벌속성입니다. 이문서에서다루는서버속성이현재환경에해당하는지여부를평가하는것이좋습니다. 다른서버속성을변경하기전에 Citrix 에문의하십시오.

일부서버속성을변경하려면각 XenMobile 서버노드를다시시작해야합니다. 다시시작이필요한경우 XenMobile 이알림을제공합니다.

일부서버속성은성능및안정성을개선하는데도움이됩니다. 자세한내용은 XenMobile 작업조정을참조하십시오.

Android Enterprise 장치에레거시 **Android** 앱제공**:** `afw.allow.legacy.apps`가 **`true`**로설정된경우 Android Enterprise 장치는레거시 Android 앱과 Android Enterprise 앱을모두수신합니다. **`false`**인경우 Android Enterprise 장치는 Android Enterprise 앱만수신합니다. 기본값은 **`true`**입니다.

파일정책에대한파일확장명허용**:** 관리자가 Files 장치정책을사용해업로드할수있는쉼표로구분된파일유형목록으로

file.extension.allowlist를구성합니다. 다음파일유형은이허용목록에추가해도업로드할수없습니다.

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

기본값은 7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,sh,tcl,txt,htm,html,doc,docx,rtf,xap입니다.

관리되는 **Google Play Store** 의모든앱에액세스**.** **true**인경우 XenMobile 은관리되는 Google Play Store 에서공용 Google Play Store 의모든앱에액세스할수있게합니다. 이속성을 **true**로설정하면모든 Android Enterprise 사용자에대한공용 Google Play Store 앱이허용됩니다. 이후관리자는 제한장치정책을사용하여이러한앱에대한액세스를제어할수있습니다. **false**로기본설정되어있습니다.

회사소유의장치등록에대한 **Android Enterprise** 작업프로필입니다. afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled가 **true**로설정된경우 Android 11 이상을실행하는장치는회사소유장치모드의작업프로필 (WPCOD) 에서등록할수있습니다. XenMobile Server 콘솔에는이등록모드에대한변경사항이반영됩니다. **false**로설정하면 WPCOD 설정을사용할수없습니다. 기본값은 **true**입니다.

추가적인 **Android Enterprise** 제한설정입니다. afw.restriction.policy.v2 속성이 **true**로설정된경우 Android Enterprise 장치에대해다음과같은제한설정을사용할수있습니다.

- 앱제거허용
- Bluetooth 공유허용

이러한설정에대한자세한내용은 제한장치정책을참조하십시오.

COPE 장치에대한 **Android Enterprise** 제한사항입니다. 제한장치정책에서 회사소유장치의작업프로필이있는완전관리형장치에적용설정을사용하려면 afw.restriction.cope을 **true**로설정합니다. 기본값은 **true**입니다. 이설정에대한자세한내용은 제한장치정책을참조하십시오.

iOS App Store 링크에호스트이름허용**:** ios.app.store.allowed.hostnames 속성은공용 API 를사용하여공용앱스토어앱을서버에업로드할때허용되는호스트이름의목록입니다. 서버를통해앱을업로드하지않고공용 API 를사용하여공용앱스토어앱을업로드할계획이라면이속성을구성하십시오. 기본값은 itunes.apple.com,vpp.itunes.apple.com,apps.apple.com입니다.

대체 **APN** 포트입니다. 포트 443 대신포트 2197 을사용하여 api.push.apple.com에서 APN 알림을보내고받을수있습니다. 포트는 HTTP/2 기반 APN 공급자 API 를사용합니다. 포트 2197 을사용하려면 **true** 속성을 apns.http2.alternate.port.enabled로설정합니다. 서버속성 apns.http2.alternate.port.enabled의기본값은 **false**입니다.

로컬사용자가약한암호를사용하지못하도록암호유효성검사를활성화합니다. enable.password.strength.validation을 **true**로설정하면약한암호를사용하는로컬사용자를추가할수없습니다. **false**로설정하면약한암호로로컬

사용자를만들수있습니다. 기본값은 **true**입니다.

루팅된 **Android** 및탈옥 **iOS** 장치의등록차단**:** 이속성이 **true**인경우 XenMobile 은루팅된 Android 장치와탈옥 iOS 장치에대한등록을차단합니다. 기본값은 **true**입니다. 권장되는설정은모든보안수준에대해 **true**입니다.

등록필요**:** `wsapi.mdm.required.flag` XenMobile Server 모드가 ENT 인경우에만적용되며사용자의 MDM 등록을필수로규정할지여부를지정합니다. 이속성은 XenMobile 인스턴스의모든사용자및장치에적용됩니다. 등록이필수이면더높은수준의보안이제공됩니다. 그러나이러한결정은 MDM 을요구할지여부에따라달라집니다. 기본적으로등록은필수가아닙니다.

이속성이 **false**인경우사용자는등록을거부할수있으며장치에서 XenMobile Store 를통해앱에액세스할수있습니다. 이속성이 **true**인경우등록을거부하는모든사용자는앱액세스가거부됩니다.

사용자등록후이속성을변경하면사용자가재등록해야합니다.

MDM 등록의필수여부에대한설명은 장치관리및 MDM 등록을참조하십시오.

다중모드등록지원**:** `enable.multimode.xms` 속성을사용하면 Android 및 iOS 장치의장치와앱모두를관리하기위해등록설정을제어하는하나의 XenMobile Server 에서등록프로필을만들수있습니다. 또한, 새롭게강화된등록프로필기능은 Android 전용장치등록과 Android 및 iOS 장치의 MAM 전용등록을지원합니다. 이속성이 **false**인경우등록프로필설정시이러한등록옵션을사용할수없습니다. 기본값은 **true**입니다. 속성이 **true**일때등록한장치는속성을 **false**로변경해도계속작동합니다.

자가지원포털사용**:** `shp.console.enable`이 **false**인경우자가지원포털에액세스할수없습니다. 포트 443 에서자가지원포털로이동하는사용자에게는 404 오류가표시됩니다. 포트 4443 에서포털로이동하는사용자에게는 "액세스거부" 메시지가표시됩니다. **true**인경우포트 443 을통해자가지원포털에액세스할수있습니다. **false**로기본설정되어있습니다.

로컬사용자계정잠금한도**:** 제한정책을사용하여 Active Directory 사용자의로그인시도에한도를설정할수있습니다. `local.user.account.lockout.limit` 키를사용하여로컬사용자계정에도동일한작업을수행할수있습니다. 사용자가지정된횟수만큼로그인을시도한후에는일정시간이지나기전까지다시시도할수없습니다. 로컬사용자계정잠금시간속성으로해당시간을구성합니다. 기본값은 6입니다.

로컬사용자계정잠금시간**:** `local.user.account.lockout.time` 속성을사용하면잠긴로컬사용자계정으로다시로그인을시도할수있기전에지나야하는시간 (분) 을설정할수있습니다. 기본값은 30분입니다.

설정된파일업로드최대크기제한**:** `max.file.size.upload.restriction`을 **true**로설정하여최대업로드파일크기를제한할수있습니다. 이제한을설정하면 `max.file.size.upload.allowed`로최대파일크기를구성할수있습니다. 이속성의기본값은 **true**입니다.

허용되는파일업로드최대크기**:** `max.file.size.upload.allowed`를사용하여업로드의최대파일크기를지정할수있습니다. 예시값으로는 `500 B`, `1 KB`, `1 MB`, `1 MiB`, `1 G` 또는 `1 GiB`가있습니다. 기본값은 `5 MB`입니다.

비활성시간제한 **(**분**):** XenMobile Server 의공용 API 를사용하여 XenMobile 콘솔또는타사앱에액세스한비활성사용자가 XenMobile 에서로그아웃되기까지의시간 (분) 입니다. 시간제한값이 0이면비활성사용자가로그인된상태로유지됩니다. API 에액세스하는타사앱의경우일반적으로로그인유지가필요합니다. 기본값은 5입니다.

iOS 장치관리등록루트 **CA** 설치필요**:** Apple 의최신등록워크플로에서사용자는 MDM 프로필을수동으로설치해야합니다. Apple Business Manager 또는 Apple School Manager 에서할당된서버에대한 MDM 등록에는이워크플로가적용되지않습니다. 그러나 MDM 수동등록중에 iOS 장치사용자에게는등록중에 MDM 장치인증서를묻는메시지만표시됩니다.

수동등록중에더나은사용자환경을제공할수있도록 `ios.mdm.enrollment.installRootCaIfRequired` 서버 속성을 **`false`**로변경하는것이좋습니다. 기본값은 **`true`**입니다. 이변경이적용되면 MDM 등록중에사용자가간편하게프로필을설치할수있는 Safari 창이열립니다.

VPP 기준간격**:** `vpp.baseline` 속성은 XenMobile 이 Apple 에서볼륨구매라이센스를다시가져오는최소간격을설정합니다. 라이센스정보를새로고치면볼륨구매에서가져온앱을수동으로삭제하는것과같은모든변경내용을 XenMobile 에반영할수있습니다. 기본적으로 XenMobile 에서볼륨구매라이센스기준은최소 1440분마다새로고쳐집니다.

설치된볼륨구매라이센스가많은경우 (예: 50,000 개초과) Citrix 에서는라이센스가져오기의오버헤드가줄도록기준간격을늘릴것을권장합니다. Apple 에서볼륨구매라이센스가자주변경될것으로예상되는경우 Citrix 에서는 XenMobile 에변경내용이업데이트되도록값을낮출것을권장합니다. 두기준사이의최소간격은 60 분입니다. cron 작업은 60 분마다실행되므로볼륨구매기준간격이 60 분인경우기준사이의간격이최대 119 분까지지연될수있습니다.

XenMobile MDM 자가지원포털콘솔의최대비활성간격입니다 **(분):** 이속성이름에는이전 XenMobile 버전이반영됩니다. 이 속성은 XenMobile 콘솔의최대비활성간격을제어합니다. 이간격은 XenMobile 콘솔에서비활성사용자가로그아웃되기까지의 시간 (분) 입니다. 시간제한이 0 인경우비활성사용자가로그인상태로유지됩니다. 기본값은 30입니다.

장치및앱정책

January 5, 2022

XenMobile 장치및앱정책을사용하면다음과같은요소간의균형을최적화할수있습니다.

- 엔터프라이즈보안
- 회사데이터및자산보호
- 사용자개인정보보호
- 사용자환경의생산성및품질개선

이러한요소간의최적화된균형은상황에따라다를수있습니다. 예를들어규제가많은조직 (예: 금융) 의경우기본적으로사용자생산성이고려되는교육, 소매등의다른업종보다엄격한보안제어가필요합니다.

사용자 ID, 장치, 위치및연결유형에따라정책을중앙에서제어하고구성하여회사콘텐츠의악의적사용을제한할수있습니다. 장치의분실또는도난이발생하는경우비즈니스응용프로그램및데이터를원격으로사용하지않도록설정하거나, 잠그거나, 초기화할수있습니다. 전체적인결과는직원만족도및생산성을개선하는동시에보안및관리제어를보장하는솔루션을구현하는것입니다.

이문서에서는보안과관련된다수의장치및앱정책을중점적으로다룹니다.

보안위험을해결하는정책

XenMobile 의장치및앱정책은보안위험을나타낼수있는다수의상황을해결합니다. 예를들면다음과같습니다.

- 사용자가신뢰할수없는장치와예측할수없는위치에서앱및데이터에액세스를시도하는경우
- 사용자가장치간에데이터를이동하는경우
- 권한이없는사용자가데이터에액세스를시도하는경우

- 회사에서자신의장치 (BYOD) 를사용한사용자가퇴사한경우
- 사용자가장치를부적절한장소에두는경우
- 사용자가항상안전하게네트워크에액세스해야하는경우
- 사용자가직접장치를관리하고, 관리자가업무용데이터와개인용데이터를분리해야하는경우
- 유휴상태의장치에서사용자자격증명을다시확인해야하는경우
- 사용자가중요한콘텐츠를복사하여보호되지않는전자메일시스템에붙여넣는경우
- 사용자가중요한데이터가포함된전자메일첨부파일또는웹링크를개인계정과회사계정이모두저장된장치에서수신하는경우

이러한상황은다음과같은회사데이터를보호할때두가지영역과관련하여고려되어야합니다.

- 유휴데이터
- 전송중데이터

XenMobile 이유휴데이터를보호하는방법

모바일장치에저장된데이터를유휴데이터라고합니다. XenMobile 은 iOS 및 Android 플랫폼에서제공하는장치암호화를사용합니다. XenMobile 은 Citrix MAM SDK 를통해제공되는규정준수확인등의기능이포함된플랫폼기반암호화를보완합니다.

XenMobile 의 MAM(모바일응용프로그램관리) 기능을사용하면모바일생산성앱, MDX 사용앱및연결된데이터를완벽하게관리하고, 보호하고, 제어할수있습니다.

Mobile Apps SDK 를사용하면앱에서 Citrix MDX 앱컨테이너기술을사용하여 XenMobile 을배포할수있습니다. 컨테이너기술은회사앱및데이터를사용자장치의개인앱및데이터와분리합니다. 데이터를분리하면포괄적인정책기반제어를통해사용자지정개발, 타사또는 BYO 모바일앱을보호할수있습니다.

XenMobile 에는앱수준암호화도포함되어있습니다. XenMobile 은모든 MDX 사용앱안에저장된데이터를개별적으로암호화하며장치암호가필요하지않고정책을적용하기위해장치를관리할필요가없습니다.

정책및 Mobile Apps SDK 를사용하면다음을수행할수있습니다.

- 비즈니스앱및데이터와개인용앱및데이터를안전한모바일컨테이너로분리합니다.
- 암호화및기타모바일 DLP(데이터손실방지) 기술을사용하여앱을보호합니다.

MDX 정책은다양한운영제어를제공합니다. 모든커뮤니케이션을제어하면서동시에 MAM SDK 사용앱이나 MDX 래핑앱사이를원활하게통합할수있습니다. 이렇게하면 MAM SDK 사용또는 MDX 래핑앱에서만데이터에액세스할수있도록하는등의정책을적용할수있습니다.

장치및앱정책제어외에유휴데이터를보호하는가장좋은방법은암호화입니다. XenMobile 은 MDX 사용앱에저장된모든데이터에암호화계층을추가하여공개파일암호화, 개인파일암호화및암호화제외같은기능을정책을통해제어할수있도록합니다. Mobile Apps SDK 는 FIPS 140-2 호환 AES 256 비트암호화와함께보호되는 Citrix Secret Vault 에저장된키를사용합니다.

XenMobile 이전송중데이터를보호하는방법

사용자의모바일장치와회사의내부네트워크를이동하는데이터를전송중데이터라고합니다. MDX 앱컨테이너기술은 Citrix Gateway 를통해내부네트워크에대한응용프로그램별 VPN 액세스를제공합니다.

직원이모바일장치에서보안되는기업네트워크에상주하는다음리소스에액세스하려는상황을고려해보십시오.

- 회사전자메일서버
- 회사인트라넷에서호스팅되는 SSL 지원웹응용프로그램
- 파일서버또는 Microsoft SharePoint 에저장된문서

MDX 를사용하면모바일장치에서응용프로그램별 Micro VPN 을통해이모든엔터프라이즈리소스에액세스할수있습니다. 각장치에는전용 Micro VPN 터널이생성됩니다.

Micro VPN 기능은신뢰할수없는모바일장치의보안을침해할수있는장치전체 VPN 을사용하지않습니다. 따라서내부네트워크가전체회사시스템을감염시킬수있는맬웨어또는공격에노출되지않습니다. 회사모바일앱과개인용모바일앱이한장치에서공존할수있습니다.

더강력한수준의보안을제공하려면 MDX 사용앱을앱인증및 Micro VPN 세션에사용되는대체 Citrix Gateway 정책으로구성할수있습니다. 대체 Citrix Gateway 를정책이필요한온라인세션에서사용하여앱에서특정게이트웨이에대한재인증을강제할수있습니다. 이러한게이트웨이는보통다른 (높은수준의보장) 인증요구사항및트래픽관리정책을가지게됩니다.

마이크로 VPN 기능은보안기능외에도압축알고리즘등의데이터최적화기법을제공합니다. 압축알고리즘으로다음이가능해집니다.

- 최소한의데이터만전송됩니다.
- 전송이가장빠른시간내에완료됩니다. 속도는사용자환경을개선하며, 이는모바일장치채택의핵심적인성공요인입니다.

다음과같은상황에서는장치정책을주기적으로재평가합니다.

- XenMobile 의새버전에장치운영체제업데이트릴리스로인한새정책또는업데이트된정책이포함되는경우
- 다음과같이새장치유형을추가하는경우

  많은정책이모든장치에공통적으로적용되지만각장치에해당운영체제와관련된일련의정책이있습니다. 따라서 iOS, Android 및 Windows 장치간에는물론여러제조업체의 Android 장치사이에서도차이가있을수있습니다.
- XenMobile 작업을엔터프라이즈또는산업변경 (예: 새로운회사보안정책또는규정준수규제) 과동기화해야하는경우
- MAM SDK 의새버전에새로운정책또는업데이트된정책이포함되는경우
- 앱을추가하거나업데이트하는경우
- 새앱또는새요구사항의결과로새로운사용자워크플로를통합하려는경우

앱정책및사용사례시나리오

Secure Hub 를통해제공할앱을선택할수있지만이러한앱이 XenMobile 과상호작용하는방식을정의해야할수도있습니다. 다음경우에앱정책을사용합니다.

- 특정기간이지난후사용자를인증하려는경우
- 사용자에게정보에대한오프라인액세스권한을제공하려는경우

다음섹션에는몇가지정책및예시사용현황이포함되어있습니다.

- MAM SDK 로 iOS 및 Android 앱에통합할수있는타사정책목록은 MAM SDK 개요를참고하시기바랍니다.
- 각플랫폼에대한모든 MDX 앱정책의목록은 MDX 정책요약을참조하십시오.

인증정책

- 장치암호

  이정책의용도**:** 사용자가장치암호를사용하는장치에서만 MDX 앱에액세스할수있도록하려면장치암호정책을사용하도록설정합니다. 이기능은장치수준에서 iOS 암호화가사용되도록합니다.

  사용자예**:** 이정책을사용하면사용자가 iOS 장치에서암호를설정해야 MDX 앱에액세스할수있습니다.

- 앱암호

  이정책의용도**:** 사용자가앱을열고데이터에액세스하기전에관리되는앱에인증하라는 Secure Hub 메시지를표시하려면앱암호정책을사용하도록설정합니다. 사용자는관리자가 XenMobile Server 설정의클라이언트속성에서구성한설정에따라 Active Directory 암호, Citrix PIN 또는 iOS TouchID 를사용하여인증할수있습니다. 클라이언트속성에서비활성타이머를설정하면사용이지속되는동안타이머가다시만료되기전까지 Secure Hub 가관리되는앱에대한사용자인증메시지를표시하지않습니다.

  앱암호는장치암호와다릅니다. 장치암호정책이장치에푸시된경우 Secure Hub 는암호또는 PIN 을구성하라는메시지를표시합니다. 장치를켜거나비활성타이머가만료되는경우사용자는구성한암호또는 PIN 을사용하여장치잠금을해제해야장치에액세스할수있습니다. 자세한내용은배포안내서의 XenMobile 의인증을참조하십시오.

  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 분으로설정한경우앱잠금명령을 XenMobile 에서장치로전송하면마지막폴링시간으로부터 60 분내에잠금이수행됩니다.

규정을준수하지않는장치동작정책

장치가최소규정준수요구사항을충족하지못하는경우규정을준수하지않는장치동작정책을사용하여수행할작업을선택할수있습니다. 자세한내용은 규정을준수하지않는장치동작을참조하십시오.

앱상호작용정책

이정책의용도**:** MDX 앱에서장치의다른앱으로이동하는문서및데이터의흐름을제어하려면앱상호작용정책을사용합니다. 예를들어사용자는컨테이너외부의개인용앱으로데이터를이동하거나컨테이너외부의데이터를컨테이너화된앱에붙여넣을수없습니다.

사용자예**:** 앱상호작용정책을제한됨으로설정하면사용자가 Secure Mail 의텍스트를 Secure Web 에복사할수있지만이데이터를컨테이너외부의개인용 Safari 또는 Chrome 브라우저에복사할수없습니다. 또한사용자는 Secure Mail 의첨부문서를 Citrix Files 또는 Quick Edit 에서열수있지만컨테이너외부의개인용파일보기앱에서는이첨부문서를열수없습니다.

앱제한정책

이정책의용도**:** MDX 앱이열려있는동안사용자가액세스할수있는기능을제어하려면앱제한정책을사용합니다. 이정책을사용하면앱이실행되는동안악의적인활동을수행할수없습니다. 앱제한정책은 iOS 와 Android 에서조금다릅니다. 예를들어 iOS 에서는 MDX 앱이실행되는동안 iCloud 에대한액세스를차단할수있습니다. Android 에서는 MDX 앱이실행되는동안 NFC 사용을중지할수있습니다.

사용자예**:** 앱제한정책을사용하여 iOS 의 MDX 앱에서받아쓰기를차단하는경우사용자는 MDX 앱이실행되는동안 iOS 키보드에서받아쓰기기능을사용할수없습니다. 따라서사용자가받아쓴데이터가보안되지않은타사클라우드받아쓰기서비스로전달되지않습니다. 사용자가컨테이너외부의개인용앱을열때는개인커뮤니케이션용으로받아쓰기옵션을사용할수있습니다.

앱네트워크액세스정책

이정책의용도**:** 장치의컨테이너에있는 MDX 앱에서회사네트워크안의데이터에액세스할수있도록하려면앱네트워크액세스정책을사용합니다. 네트워크액세스정책에서 내부네트워크로터널링됨옵션을설정하면 MDX 앱에서 Citrix ADC 를통한백엔드웹서비스또는데이터저장소로의 Micro VPN 이자동화됩니다.

사용자예**:** 사용자가터널링을사용하는 MDX 앱 (예: Secure Web) 을열면사용자가 VPN 을시작하지않아도브라우저가열리고인트라넷사이트가시작됩니다. Secure Web 앱이 Micro VPN 기술을사용하여내부사이트에자동으로액세스합니다.

앱지오로케이션및지오펜스정책

이정책의용도**:** 앱지오로케이션및지오펜스를제어하는정책에는중심점경도, 중심점위도및반경이포함됩니다. 이러한정책은 MDX 앱의데이터에대한액세스를특정지리적영역으로제한합니다. 정책은위도및경도좌표의반경을사용하여지리적영역을정의합니다. 사용자가정의된반경밖에서앱을사용하려고하면앱이잠긴상태로유지되고사용자가앱데이터에액세스할수없습니다.

사용자예**:** 사용자는사무실위치에있는동안합병및인수데이터에액세스할수있습니다. 사무실위치밖으로이동하면이중요한데이터에액세스할수없게됩니다.

Secure Mail 앱정책

- 백그라운드네트워크서비스

  이정책의용도**:** Secure Mail 의백그라운드네트워크서비스는실질적으로 SOCKS5 프록시인 STA(Secure Ticket Authority) 를활용하여 Citrix Gateway 를통해연결합니다. STA 는오래유지되는연결을지원하며 Micro VPN 에비해개선된배터리수명을제공합니다. 따라서 STA 는지속적으로연결되는메일에적합합니다. Secure Mail 을사용하는경우이러한설정을구성하는것이좋습니다. XenMobile 용 Citrix ADC 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**:** 이설정은사용자가 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 이서버에저장된이전전자메일을표시합니다. Secure Mail 을설치한후각사용자는요구사항에적합하게이설정을변경할수있습니다.

장치정책및사용사례동작

장치정책은 MDM 정책이라고도하며 XenMobile 이장치에서작동하는방식을결정합니다. 많은정책이모든장치에공통적으로적용되지만각장치에해당운영체제와관련된일련의정책이있습니다. 다음목록에는일부장치정책과정책을사용하는방법이포함되어있습니다. 모든장치정책의목록은 장치정책 아래문서를참조하십시오.

- 앱인벤토리정책

  이정책의용도**:** 사용자에의해설치된앱을확인해야하는경우장치에앱인벤토리정책을배포합니다. 앱인벤토리정책을배포하지않은경우사용자가 XenMobile Store 에서설치한앱만표시되며개인적으로설치한응용프로그램은표시되지않습니다. 회사장치에서실행할수없는특정앱을차단하려는경우이정책을사용해야합니다.

  사용자예**:** MDM 으로관리되는장치의사용자는이기능을사용하지않도록설정할수없습니다. 사용자가개인적으로설치한응용프로그램이 XenMobile 관리자에게표시됩니다.

- 앱잠금정책

  이정책의용도**:** Android 용앱잠금정책을사용하면앱을차단하거나허용할수있습니다. 예를들어앱을허용하여키오스크장치를구성할수있습니다. 일반적으로앱잠금정책은사용자가설치할수있는앱을제한하므로회사소유장치에만배포됩니다. 재정의암호를설정하여차단된앱에대한사용자액세스를제공할수있습니다.

  사용자예**:** Angry Birds 앱을차단하는앱잠금정책을배포한다고가정할경우사용자는 Angry Birds 앱을 Google Play 에서설치할수있지만앱을열면관리자가앱을차단했다는내용의메시지가표시됩니다.

- 연결예약정책

  이정책의용도**:** Windows Mobile 장치에서 MDM 관리, 앱푸시및정책배포를위해 XenMobile Server 에다시연결할수있도록하려면연결예약정책을사용해야합니다. Android, Android Enterprise 및 Chrome OS 장치의경우이정책대신 Google FCM(Firebase Cloud Messaging) 을사용하여 XenMobile Server 에대한연결을제어합니다. 예약옵션은다음과같습니다.

  - 항상**:** 연결을영구적으로활성상태로유지합니다. 보안을최적화하려면이옵션을사용하는것이좋습니다. 항상을선택하는경우연결로인해배터리가소진되지않도록연결타이머정책도사용하십시오. 연결을활성상태로유지하면초기화또는잠금과같은보안명령을주문형으로장치에푸시할수있습니다. 또한장치에배포하는각정책에서배포일정옵션 상시연결에대해배포를선택해야합니다.
  - 안함**:** 수동으로연결합니다. 안함옵션을사용하면보안정책을장치에배포할수없어사용자가새앱또는정책을받을수없으므로프로덕션배포에사용하지않는것이좋습니다.
  - 매**:** 지정된간격으로연결합니다. 이옵션이적용될때잠금또는초기화와같은보안정책을전송하면다음번장치연결시 XenMobile 에서정책이처리됩니다.
  - 일정정의**:** 사용하면네트워크연결이끊긴후 XenMobile 이사용자장치를 XenMobile Server 에다시연결하고제어패킷을정의된시간내에정기적으로전송하여연결을모니터링합니다.

  사용자예**:** 등록된장치에암호정책을배포하려고합니다. 예약정책을사용하면장치가정기적인간격으로서버에다시연결하여새정책을수집합니다.

- 자격증명정책

  이정책의용도**:** 주로 WiFi 정책과함께사용됩니다. 자격증명정책을사용하면인증서인증이필요한내부리소스에대한인증에사용할인증서를배포할수있습니다.

  사용자예**:** 장치의무선네트워크를구성하는 WiFi 정책을배포합니다. WiFi 네트워크를사용하려면인증서로인증해야합니다. 자격증명정책은인증서를배포하고배포된인증서는운영체제키저장소에저장됩니다. 그러면사용자가내부리소스에연결할때인증서를선택할수있습니다.

- **Exchange** 정책

  이정책의용도**:** XenMobile 에서는두가지옵션을사용하여 Microsoft Exchange ActiveSync 전자메일을전송할수있습니다.

  - **Secure Mail** 앱**:** 공용앱스토어또는 XenMobile Store 에서배포하는 Secure Mail 앱을사용하여전자메일을전송합니다.

  - 기본전자메일앱**:** 장치의기본전자메일클라이언트에서 ActiveSync 전자메일을사용하도록설정하려면 Exchange 정책을사용합니다. 기본전자메일에대한 Exchange 정책을사용하는경우 Active Directory 특성에서사용자데이터를채우는매크로를사용할수있습니다. 예를들어 ${user.username} 을사용하여사용자이름을채우고 ${user.domain} 을사용하여사용자도메인을채울수있습니다.

사용자예**:** Exchange 정책을푸시할때 Exchange Server 세부정보를장치에전송합니다. 그러면 Secure Hub 가인증메시지를표시하고전자메일동기화가시작됩니다.

- 위치정책

  이정책의용도**:** 위치정책을사용하면장치가 Secure Hub 에대한 GPS 를사용하는경우지도에서장치의위치를찾을수있습니다. 이정책을배포한후 XenMobile Server 에서위치명령을보내면장치가위치좌표를사용하여응답합니다.

  사용자예**:** 위치정책이배포되고 GPS 가장치에서사용되는경우장치를찾지못하는사용자는 XenMobile 자가지원포털에로그온하고찾기옵션을선택하여지도에서장치의위치를확인할수있습니다. 사용자는 Secure Hub 에서위치서비스를사용할수있도록선택해야합니다. 사용자가직접장치를등록하는경우관리자는위치서비스사용을적용할수없습니다. 이정책을사용할때는배터리수명에미치는영향도고려해야합니다.

- 암호정책

  이정책의용도**:** 암호정책을사용하면관리되는장치에 PIN 코드또는암호를적용할수있습니다. 이암호정책을사용하면장치에암호에대한복잡성및시간초과를설정할수있습니다.

  사용자예**:** 관리되는장치에암호정책을배포하면 Secure Hub 가암호또는 PIN 을구성하라는메시지를표시합니다. 장치를켜거나비활성타이머가만료되는경우사용자는구성한암호또는 PIN 을사용하여장치잠금을해제해야장치에액세스할수있습니다.

- 프로필제거정책

  이정책의용도**:** 사용자그룹에정책을배포하고나중에일부사용자에게서정책을제거해야하는경우프로필제거정책을만들고프로필제거정책을지정된사용자이름에만배포하는배포규칙을사용하여선택한사용자에대한정책을제거할수있습니다.

  사용자예**:** 프로필제거정책을사용자장치에배포하는경우사용자는변경내용을알지못할수있습니다. 예를들어프로필제거정책이장치카메라를사용할수없도록하는제한을제거하는경우사용자는카메라사용이허용된것을알지못합니다. 사용자경험에영향을미치는변경이발생하는경우해당사항을사용자에게알려주는것이좋습니다.

- 제한정책

  이정책의용도**:** 제한정책은관리되는장치의기능을잠그고제어할수있는다수의옵션을제공합니다. 지원되는장치에대한수백가지제한옵션을사용할수있으며여기에는장치의카메라또는마이크사용을제한하는옵션부터앱스토어같은타사서비스에대한로밍규칙및액세스를적용하는옵션이포함됩니다.

  사용자예**:** iOS 장치에제한을배포하는경우사용자는 iCloud 또는 Apple App Store 에액세스하지못할수있습니다.

- 약관정책

  이정책의용도**:** 관리자는장치관리와관련된법적영향을사용자에게알려야할수있습니다. 또한회사데이터를장치에푸시할때의보안위험을사용자가숙지할수있도록해야합니다. 사용자가등록하기전에관리자는사용자지정약관문서를사용하여규칙및고지사항을게시할수있습니다.

사용자예**:** 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.

  사용자예**:** VPN 정책을사용하면사용자가내부도메인에액세스할때사용자장치에서 VPN 연결이열립니다.

- 웹클립정책

  이정책의용도**:** 웹사이트를직접여는아이콘을장치에푸시하려면웹클립정책을사용합니다. 웹클립에는웹사이트링크가포함되며사용자지정아이콘을포함할수있습니다. 장치에서웹클립은앱아이콘처럼표시됩니다.

  사용자예**:** 사용자는웹클립아이콘을클릭하여액세스가필요한서비스를제공하는인터넷사이트를열수있습니다. 웹링크를사용하면브라우저앱을열고링크주소를입력하는것보다편리합니다.

- **WiFi** 정책

  이정책의용도**:** WiFi 정책을사용하면 SSID, 인증데이터및구성데이터같은 WiFi 네트워크세부정보를관리되는장치에배포할수있습니다.

  사용자예**:** WiFi 정책을배포하면장치가자동으로 WiFi 네트워크에연결되고사용자를인증합니다. 인증된사용자는네트워크에액세스할수있습니다.

- **Windows Information Protection** 정책

  이정책의용도**:** 엔터프라이즈데이터의잠재적유출을방지하려면 WIP(Windows Information Protection) 정책을사용합니다. 설정한적용수준에서 Windows Information Protection 이필요한앱을지정할수있습니다. 예를들어부적절한데이터공유를차단하거나부적절한데이터공유에대해경고를표시하고사용자의정책재정의를허용할수있습니다. 부적절한데이터공유를로깅하고허용하는동안 WIP 를자동으로실행할수있습니다.

  사용자예**:** 부적절한데이터공유를차단하는 WIP 정책을구성하는경우사용자가보호되는파일을보호되지않는위치로복사하거나저장하면보호되는콘텐츠가포함된작업을이위치에배치할수없다는내용의메시지가표시됩니다.

- **XenMobile Store** 정책

  이정책의용도**:** XenMobile Store 는관리자가사용자에게필요한모든회사앱및데이터리소스를게시할수있는통합앱스토어입니다. 관리자는다음을추가할수있습니다.

  - 웹앱, SaaS 앱, MAM SDK 사용앱또는 MDX 래핑앱
  - Citrix 모바일생산성앱
  - .ipa 또는.apk 파일과같은기본모바일앱
  - Apple App Store 및 Google Play 앱
  - 웹링크
  - Citrix StoreFront 로게시된 Citrix Virtual Apps

사용자예**:** XenMobile 에장치를등록한후사용자는 Citrix Secure Hub 앱을통해 XenMobile Store 에액세스합니다. 여기서사용자는제공되는모든회사앱및서비스를확인할수있습니다. 사용자는 XenMobile Store 에서앱을클릭하여설치하고, 데이터에액세스하고, 앱을평가하고후기를작성하고, 앱업데이트를다운로드할수있습니다.

사용자등록옵션

September 29, 2021

다양한방법으로사용자장치를 XenMobile 에등록하도록할수있습니다. 구체적인사항을고려하기전에 MDM+MAM, MDM 또는 MAM 으로등록하고자하는장치를결정하십시오. 관리모드에대한자세한내용은 관리모드를참조하십시오.

개괄적으로등록옵션에는네가지가있습니다.

- 등록초대**:** 사용자에게등록초대또는초대 URL 을전송합니다. Windows 장치에서는등록초대와 URL 을사용할수없습니다.
- 자가지원포털**:** 사용자가방문하여 Secure Hub 를다운로드하고장치를등록하거나등록초대를직접전송할수있는포털을설정합니다.
- 수동등록**:** 사용자에게시스템을등록할수있음을알리는전자메일, 안내서또는기타커뮤니케이션을전송합니다. 그러면사용자가 Secure Hub 를다운로드하고수동으로장치를등록합니다.
- 엔터프라이즈**:** 다른장치등록옵션은 Apple 배포프로그램및 Google Android Enterprise 를사용하는것입니다. 이러한프로그램을통해미리구성되고직원이사용할수있도록준비된장치를구입할수있습니다. 자세한내용은 Apple 지원의 Apple 배포프로그램문서와 Android Enterprise 웹사이트의 Google Android Enterprise 문서를참조하십시오.

등록초대

iOS, macOS, Android Enterprise 및레거시 Android 장치사용자에게전자메일로등록초대를보낼수있습니다. Windows 장치에서는등록초대와 URL 을사용할수없습니다.

또한 iOS, macOS, Android 또는 Windows 장치사용자에게 SMTP 또는 SMS 를통해설치링크를보낼수있습니다. 자세한내용은 장치등록을참조하십시오.

등록초대방법을사용하기로할경우다음이가능합니다.

- 초대 **URL**, 초대 **URL+PIN** 또는 초대 **URL+** 암호등록보안모드를선택합니다.
- 모드를조합하여사용할수있습니다.
- 설정페이지에서모드를활성화하거나비활성화할수있습니다.

각등록보안모드에대한자세한내용은 등록보안모드구성을참조하십시오.

초대는많은용도로사용됩니다. 초대의가장일반적인용도는사용자에게시스템을사용할수있고등록할수있음을알리는것입니다. 초대 URL 은고유합니다. 사용자가초대 URL 을사용하고나면더이상 URL 을사용할수없습니다. 이속성을사용하여시스템에등록하는사용자또는장치를제한할수있습니다.

등록프로필을구성하면특정사용자가등록할수있는장치수를 Active Directory 그룹에따라제어할수있습니다. 예를들어재무부서에사용자당하나의장치만허용할수있습니다.

특정등록옵션을사용할경우추가비용및문제가발생할수있다는점에주의하십시오. 예를들어 SMS 를사용하여초대장을전송하려면추가적인인프라가필요합니다. 이옵션에대한자세한내용은 알림을참조하십시오.

또한전자메일로초대를보내려면사용자가 Secure Hub 외부에서전자메일에액세스할방법이있는지확인하십시오. MDM 등록의 경우 OTP(일회용암호) 등록보안모드를 Active Directory 암호대신사용할수있습니다.

자가지원포털

사용자는자가지원포털을통해등록초대를요청할수있습니다. 자가지원포털설정에대한자세한내용은 등록보안모드구성을참조하십시오.

수동등록

수동등록에서는사용자가 AutoDiscovery 를사용하거나서버정보를입력하여 XenMobile 에연결합니다. AutoDiscovery 를사용하는경우사용자는전자메일주소또는 Active Directory 자격증명만사용자계정이름형식으로입력하여로그온합니다. AutoDiscovery 를사용하지않는경우사용자는서버주소와 Active Directory 자격증명을입력해야합니다. AutoDiscovery 설정에대한자세한내용은 XenMobile AutoDiscovery Service를참조하십시오.

수동등록은여러가지방법으로간편하게완료할수있습니다. 가이드를생성하고가이드를사용자에게배포한다음직접등록하도록합니다. IT 부서를통해특정시간슬롯의사용자그룹을수동으로등록할수있습니다. 사용자가자격증명, 서버정보또는둘다를입력해야하는유사한방법을사용할수있습니다.

사용자등록

환경을설정한후에는사용자를환경에등록하는방법을결정해야합니다. 사용자등록보안모드에대한구체적인내용은이문서의이전섹션에설명되어있습니다. 이섹션에서는사용자에게연락하는방법을설명합니다.

공개등록과선택적초대

사용자를온보딩할때는다음의두가지기본적인방법을통해등록을허용할수있습니다.

- 공개등록. 기본적으로 LDAP 자격증명과 XenMobile 환경정보가있는모든사용자가등록할수있습니다.
- 제한된등록. 등록초대를받은사용자만허용하여사용자수를제한할수있습니다. Active Directory 그룹을기준으로공개등록을제한할수도있습니다.

초대방법을사용하는경우사용자가등록할수있는장치수를제한할수도있습니다. 공개등록은대부분의경우허용되지만몇가지고려해야할사항이있습니다.

- MAM 등록의경우 Active Directory 그룹구성원자격을통해간편하게공개등록을제한할수있습니다.

- MDM 등록의경우 Active Directory 그룹구성원자격에따라등록할수있는장치의수를제한할수있습니다. 환경에서회사 장치만허용하려는경우이러한제한은보통문제가되지않습니다. 그러나 BYOD 작업공간에서환경의장치수를제한하려는경우이방법을고려하는것이좋습니다.

선택적초대는공개등록보다필요한작업이약간더많기때문에일반적으로덜자주수행됩니다. 사용자가환경에서장치를등록하려면각 사용자에게고유한초대를보내야합니다. 등록초대를보내는방법에대한자세한내용은 등록초대보내기를참조하십시오.

Active Directory 그룹을사용하여초대를일괄적으로생성할수있지만이접근방식은연속적으로수행해야합니다.

먼저사용자에게연락

공개등록또는선택적초대중선택하고이러한환경을설정한후에는사용자에게등록옵션을알려야합니다.

선택적초대방법을사용하는경우전자메일및 SMS 메시지가프로세스에포함됩니다. 공개등록의경우에도 XenMobile 콘솔을통해전자메일을보낼수있습니다. 자세한내용은 등록초대보내기를참조하십시오.

두경우모두전자메일을사용하려면 SMTP 서버가필요합니다. 문자메시지의경우 SMS 서버가필요합니다. 이러한서버의경우의 사결정을내릴때추가비용을고려해야할수있습니다. 방법을선택하기전에새사용자가정보 (예: 전자메일) 에액세스하는방법을고려해야합니다. 모든사용자로하여금 XenMobile 을통해전자메일에액세스하도록하려는경우초대전자메일을보내는것이문제가될 수있습니다.

공개등록환경에서는 XenMobile 이외의다른수단으로도커뮤니케이션을전송할수있습니다. 이옵션의경우관련정보를모두포함해야합니다. 사용자에게 Secure Hub 앱을받을수있는위치와등록에사용하는방법을알려줍니다. 검색이꺼져있으면사용자에게 XenMobile Server 주소도제공합니다. AutoDiscovery 에대한자세한내용은 XenMobile AutoDiscovery Service를 참조하십시오.

XenMobile 작업조정

May 24, 2021

XenMobile 작업의성능및안정성은 XenMobile 의많은설정과관련되며 Citrix ADC 및 SQL Server 데이터베이스구성에따라달라집니다. 이문서에서는 XenMobile 의조정및최적화와관련하여관리자가가장자주구성하는설정을중점적으로설명합니다. XenMobile 을배포하기전에이문서의각설정을평가하는것이좋습니다.

> 중요:
>
> 다음지침은 XenMobile 서버 CPU 및 RAM 이장치수에적합하다고가정합니다. 확장성에대한자세한내용은 확장성및성능을참조하십시오.

다음서버속성은전체 XenMobile 인스턴스의작업, 사용자및장치에글로벌로적용됩니다. 일부서버속성을변경하려면각 XenMobile 서버노드를다시시작해야합니다. 다시시작이필요한경우 XenMobile 이알림을제공합니다.

다음조정지침은클러스터된환경과클러스터되지않은환경에모두적용됩니다.

hibernate.c3p0.idle_test_period

XenMobile Server 속성인사용자지정키는연결유효성이자동으로검사되기까지의유휴시간 (초) 을결정합니다. 다음과같이키를구성합니다. 기본값은 **30** 입니다.

- 키: 사용자지정키
- 키: **hibernate.c3p0. idle_test_period**
- 값: **120**
- 표시이름: **hibernate.c3p0. idle_test_period**
- 설명: **Hibernate** 유휴테스트기간

hibernate.c3p0.max_size

이사용자지정키는 XenMobile 에서 SQL Server 데이터베이스에대해열수있는최대연결수를결정합니다. XenMobile 은이사용자지정키에지정한값을상한으로사용합니다. 필요한경우에만연결이열립니다. 데이터베이스서버의용량에따라설정을결정합니다.

클러스터된구성에서는다음수식을참고하십시오. c3p0 연결에노드수를곱한값은 XenMobile 이 SQL Server 데이터베이스에실제로열수있는최대연결수와동일합니다.

클러스터된구성및클러스터되지않은구성에서 SQL Server 규모를작게하여이값을너무높게설정하면최고부하중에 SQL 측에서리소스문제가발생할수있습니다. 이값을너무낮게설정하면사용가능한 SQL 리소스를활용하지못할수있습니다.

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. 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, 유휴시간초과를낮추도록설정하는것이좋습니다. 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 그룹구성원자격이변경된후정책을업데이트하는속도를제어합니다. 그러므로부하를줄이려면이값을 12~20 시간사이의값으로늘리는것이적절합니다.

iOS MDM APNS 연결풀크기

장치수가 100 대이상인경우 APNs 연결풀이너무작으면 APNs 작업성능에부정적인영향을미칠수있습니다. 앱및정책이장치에느리게배포되고장치등록이느려지는등의성능문제가발생할수있습니다. 기본값은 **1** 입니다. 약 400 개의장치마다이값을 1 씩늘리는것이좋습니다.

auth.ldap.connect.timeout

느린 LDAP 응답을보완하려면다음사용자지정키의서버속성을추가하는것이좋습니다.

- 키: 사용자지정키
- 키: **auth.ldap.connect.timeout**
- 값: **60000**
- 표시이름: **auth.ldap.connect.timeout**
- 설명: **LDAP** 연결시간초과

auth.ldap.read.timeout

느린 LDAP 응답을보완하려면다음사용자지정키의서버속성을추가하는것이좋습니다.

- 키: 사용자지정키
- 키: **auth.ldap.read.timeout**
- 값: **60000**
- 표시이름: **auth.ldap.read.timeout**
- 설명: **LDAP** 읽기시간제한

기타서버최적화

서버속성	기본설정	이설정을변경하는이유
백그라운드배포	1,440 분	백그라운드정책배포의빈도 (분) 입니다. Android 장치의상시연결에만적용됩니다. 정책배포빈도를늘리면서버부하가감소합니다. 권장되는설정은 **1440**(24 시간) 입니다.
백그라운드하드웨어인벤토리	1,440 분	백그라운드하드웨어인벤토리의빈도 (분) 입니다. Android 장치의상시연결에만적용됩니다. 하드웨어인벤토리빈도를늘리면서버부하가감소합니다. 권장되는설정은 **1440**(24 시간) 입니다.
삭제된 **Active Directory** 사용자를확인하는간격	15 분	Active Directory 의표준동기화시간은 **15** 분입니다. 값이 **0** 인경우 XenMobile 이삭제된 Active Directory 사용자를확인하지않습니다. 권장되는설정은 **15** 분입니다.
MaxNumberOfWorker	3	많은수의볼륨구매라이센스를가져올때사용되는스레드수입니다. 기본값은 **3** 입니다. 추가최적화가필요한경우스레드수를늘릴수있습니다. 그러나예를들어 6 과같이스레드수가커지면볼륨구매를가져올때 CPU 사용량이높아진다는점에유의하십시오.

SQL DB 에서교착상태를확인하고기록데이터를삭제하는방법

교착상태가발견되면다음쿼리를실행하여교착상태를확인하십시오. 그런다음데이터베이스관리자또는 Microsoft SQL 팀을통해정보를확인할수있습니다.

SQL 쿼리

```
SELECT

db.name DB_Service,
```



```
4
5  tl.request_session_id,
6
7  wt.blocking_session_id,
8
9  OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,
10
11 tl.resource_type,
12
13 h1.TEXT AS RequestingText,
14
15 h2.TEXT AS BlockingTest,
16
17 tl.request_mode
18
19 FROM sys.dm_tran_locks AS tl
20
21 INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id
22
23 INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
      resource_address
24
25 INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
      resource_associated_entity_id
26
27 INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
      request_session_id
28
29 INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
      blocking_session_id
30
31 CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1
32
33 CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2
34
35 GO
36 <!--NeedCopy-->
```

데이터베이스정리

> 중요:
>
> 테이블을변경하기전에데이터베이스를백업합니다.

1. 다음쿼리를실행하여기록데이터를확인합니다.


```
select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;
select COUNT(\*) as total_record from dbo.EWSESS;
select COUNT(*) as total_record from dbo.EWAUDIT;
<!--NeedCopy-->
```

2. 이전의 3 개테이블에서데이터를삭제합니다.

   > 참고:
   >
   > 기록데이터가테이블에표시되지않을수있습니다. 이경우실행을건너뛰고특정테이블에대한쿼리를잘라냅니다.

```
truncate TABLE dbo.EWDEPLOY_HISTO;
truncate TABLE dbo.EWSESS;
truncate TABLE dbo.EWAUDIT;
<!--NeedCopy-->
```

3. 교착상태로인해차단되었던 SELECT 쿼리를차단해제합니다. 이단계에서추가교착상태가처리됩니다.

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT
    ON WITH ROLLBACK IMMEDIATE
<!--NeedCopy-->
```

4. 기본적으로데이터베이스정리는세션보존및감사보존데이터유지를위해 7 일로설정되며사용자가많은경우값이증가합니다. 정리값을 1 일또는 2 일로변경합니다. 서버속성에서다음변경을수행합니다.

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
zdm.dbcleanup.auditRetentionTimeInDays=1 day
<!--NeedCopy-->
```

KEYSTORE 테이블에서분리된항목정리

XenMobile 노드의성능이좋지않으면 KEYSTORE 테이블이너무크지않은지확인합니다. XenMobile 은등록인증서를 ENROLLMENT_CERTIFICATE 및 KEYSTORE 테이블에저장합니다. 장치를삭제하거나재등록하면 ENROLLMENT_CERTIFICATE 테이블의인증서가삭제됩니다. KEYSTORE 테이블의항목은그대로유지되며, 이로인해성능문제가발생할수있습니다. KEYSTORE 테이블에서분리된항목을정리하려면다음절차를수행하십시오.

> 중요:
>
> 테이블을변경하기전에데이터베이스를백업합니다.

1. 다음쿼리를실행하여기록데이터를확인합니다.

```
select COUNT(*) from KEYSTORE
<!--NeedCopy-->
```

2. 다음쿼리를사용하여 KEYSTORE 테이블에서분리된항목이있는지확인합니다.

```
WITH cte(KEYSTORE_ID)
AS (SELECT KEYSTORE_ID
    FROM ENROLLMENT_CERTIFICATE
    UNION
    SELECT CA_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT CLIENT_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT KEYSTORE_ID
    FROM SAML_SERVICE_PROVIDER
    UNION
    SELECT KEYSTORE_ID
    FROM SERVER_CERTIFICATE)
SELECT keystore.id
FROM keystore
    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
WHERE KEYSTORE_ID IS NULL;
<!--NeedCopy-->
```

3. 다음쿼리를사용하여분리된항목을지웁니다.

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
```



```
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
        UNION
        SELECT KEYSTORE_ID
        FROM SERVER_CERTIFICATE)
    DELETE FROM keystore
    WHERE id IN
    (
        SELECT keystore.id
        FROM keystore
            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
    );
<!--NeedCopy-->
```

4. KEYSTORE 테이블에인덱스를추가하여검색효율성을높입니다.

```
DROP INDEX ”KEYSTORE_NAME_IDX” ON ”KEYSTORE”;
ALTER TABLE ”KEYSTORE” ALTER COLUMN ”NAME” NVARCHAR(255) NULL;
CREATE INDEX ”KEYSTORE_NAME_IDX” ON ”KEYSTORE”(”NAME”) INCLUDE (”
    ID”, ”TYPE”, ”CONTENT”, ”PASSWORD”, ”PUBLICLY_TRUSTED”, ”
    DESCRIPTION”, ”ALIAS”, ”MODIFICATION_DATE”);
<!--NeedCopy-->
```

앱프로비전및프로비전해제

January 5, 2022

응용프로그램프로비전은주로 XenMobile 환경내모바일앱의준비, 구성, 제공및관리로구성되는모바일앱수명주기를중심으로수행됩니다. 일부경우에는응용프로그램코드의배포나수정도프로비전프로세스에포함될수있습니다. XenMobile 에는앱프로비전에사용할수있는다양한도구와프로세스가포함되어있습니다.

앱프로비전에관한이문서를읽기전에다음문서를읽어보는것이좋습니다.

- 앱 - 사용자커뮤니티

조직에서사용자에게제공할앱의유형을확정한후에앱의수명주기관리프로세스에대한개요를작성할수있습니다.

앱프로비전프로세스를정의할때는다음요점을고려하십시오.

- 앱프로파일링**:** 조직에서처음에는제한된수의앱을사용하여시작할수있습니다. 하지만사용자채택률이증가하고환경의규모가확장됨에따라관리하는앱의수가빠른속도로증가할수있습니다. 앱프로비전을쉽게관리하려면처음부터구체적인앱프로필을정의합니다. 앱프로파일링은앱을비기술적인관점의논리적그룹으로범주화하는데도움이됩니다. 예를들어다음과같은요소를기준으로앱프로필을생성할수있습니다.
  - 버전: 추적에사용할앱버전
  - 인스턴스: 서로다른사용자집합 (예: 서로다른액세스수준) 에배포되는다수의인스턴스
  - 플랫폼: iOS, Android 또는 Windows
  - 대상: 표준사용자, 부서, 최고수준경영진
  - 소유권: 앱을소유하는부서
  - 유형: MDX, 공용, 웹및 SaaS 또는웹링크
  - 업그레이드주기: 앱을업그레이드하는빈도
  - 라이센스: 라이센스요구사항및소유권
  - MAM SDK 또는 MDX 정책: MDX 기능을모바일앱에적용합니다.
  - 네트워크액세스: 액세스유형 (예: Secure Browse 또는전체 VPN)

    > 참고**:**
    > 터널링됨 - 웹 SSO 는 MDX 설정에서 Secure Browse 의이름입니다. 동작은동일합니다.

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
라이센스	해당없음	해당없음	해당없음	볼륨구매
MDX 정책	예	예	예	아니요
네트워크액세스	VPN	VPN	VPN	공개

- 앱버전관리**:** 앱버전을유지관리하고추적하는작업은프로비전프로세스의중요한부분입니다. 버전관리는사용자에게미치는영향없이수행됩니다. 앱의새버전을다운로드할수있을때만사용자에게알림이제공됩니다. 관리자의관점에서프로덕션환경에미치는영향을방지하려면비프로덕션용량에서각앱버전을검토하고테스트해야합니다.

  이러한검토및테스트는특정업그레이드가필요한지여부를평가할때에도중요합니다. 앱업그레이드에는보통두가지유형이있습니다. 그중하나는특정버그의수정과같은부차적업그레이드입니다. 다른하나는주요릴리스로, 이를통해앱을대대적으

로변경하고개선합니다. 어떤경우에도앱릴리스정보를꼼꼼하게검토하여업그레이드가필요한지를평가하십시오.

- 앱개발**:** 개발하는모바일응용프로그램에서 MAM SDK 를통합할때이러한앱에 MDX 기능을적용합니다. MAM SDK 개요를참조하십시오.

  MAM SDK 는 2022 년 3 월사용중단이예정된 MDX Toolkit 을대체합니다. 앱래핑에대한자세한내용은 MDX Toolkit을참조하십시오. 래핑된앱의앱프로비전프로세스는래핑되지않은표준앱의프로비전프로세스와다릅니다.

- 앱보안**:** 프로비전프로세스의일부로개별앱또는앱프로필의보안요구사항을정의합니다. 앱을배포하기전에구체적인 MDM 또는 MAM 정책에보안요구사항을매핑할수있습니다. 이렇게계획하면앱배포가간소하고빨라집니다. 예:

  - 특정앱은다르게배포할수있습니다.
  - XenMobile 환경의아키텍처를변경하는것이좋을수도있습니다. 변경사항은앱에필요한보안규정준수유형에따라다릅니다. 예를들어중요한비즈니스인텔리전스앱을사용할수있도록장치를암호화해야하거나종단간 SSL 암호화또는지오펜스가필요한특정앱을사용해야할수있습니다.

- 앱제공**:** XenMobile 에서는앱을 MDM 앱또는 MAM 앱으로제공할수있습니다. MDM 앱은 XenMobile Store 에표시됩니다. 이스토어에서는공개또는기본앱을사용자에게편리하게제공할수있습니다. 관리하는유일한 MDM 앱제어는장치수준제한을시행하기위한것입니다. 그러나 MAM 을사용하여앱을제공하면앱제공및앱자체를완벽하게제어할수있습니다. MAM 을통해앱을제공하는것이보통더적절합니다.

- 응용프로그램유지관리**:**

  - 초기감사수행: 프로덕션환경의앱버전과마지막업그레이드주기를추적합니다. 업그레이드가필요한특정기능또는버그수정을기록하십시오.
  - 기준설정: 각앱의안정적인최신릴리스목록을유지합니다. 업그레이드후예기치않은문제가발생할경우이앱버전으로폴백합니다. 또한, 롤백계획을개발합니다. 프로덕션환경이전에테스트환경에서앱업그레이드를테스트합니다. 가능한경우업그레이드를프로덕션사용자하위집단에먼저배포한다음전체사용자기반으로배포합니다.
  - 앱최신릴리스정보를확인하는것은중요하므로 Citrix 소프트웨어업데이트알림과타사소프트웨어공급업체알림을구독합니다. EAR(Early Access Release) 빌드가테스트를위해제공될수도있습니다.
  - 사용자알림을위한전략고안: 앱업그레이드가제공될때사용자에게알림을전송하는전략을정의합니다. 배포전에교육을제공하여사용자가준비할수있도록합니다. 앱업데이트전에여러번알림을전송할수있습니다. 앱에따라전자메일알림또는웹사이트가가장좋은알림방법이될수있습니다.

앱수명주기관리는앱의초기배포부터사용중지까지의전체수명주기를나타냅니다. 앱수명주기는다음과같은세단계로이루어져있습니다.

1. 사양요구사항: 비즈니스사례및사용자요구사항에서시작됩니다.
2. 개발: 앱이비즈니스요구사항을충족하는지검증합니다.
3. 테스트: 테스트사용자, 문제및버그를식별합니다.
4. 배포: 앱을프로덕션사용자에게배포합니다.
5. 유지관리: 앱버전을업데이트합니다. 프로덕션환경에서앱을업데이트하기전에테스트환경에서앱을배포하십시오.

Secure Mail 을사용한응용프로그램수명주기의예

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 에서해당하는 MDX 파일을배포합니다.
5. 유지관리: Secure Mail 의새로운업데이트가제공됩니다. Citrix 다운로드에서새 MDX 파일을다운로드하고 XenMobile Server 의기존 MDX 파일을대체합니다. 사용자에게업데이트를수행하도록알립니다. 참고: Citrix 는테스트환경에서이프로세스를완료하고테스트하기를권장합니다. 그런다음앱을 XenMobile 프로덕션환경에업로드하고사용자에게배포합니다.

자세한내용은 iOS 모바일앱래핑 및 Android 모바일앱래핑을참조하십시오.

대시보드기반작업

January 5, 2022

XenMobile 콘솔대시보드에액세스하여정보를한눈에볼수있습니다. 이러한정보를사용하면위젯을통해신속하게문제점과성공여부를확인할수있습니다.

대시보드는일반적으로 XenMobile 콘솔에처음로그온할때나타나는화면입니다. 콘솔의다른곳에서대시보드에액세스하려면 분석을클릭합니다. 페이지의레이아웃을편집하고나타나는위젯을편집하려면대시보드에서 사용자지정을클릭합니다.

- 내대시보드**:** 최대네개의대시보드를저장할수있습니다. 이러한대시보드를개별적으로편집하고저장된대시보드를선택하여각대시보드를볼수있습니다.
- 레이아웃스타일**:** 이행에서는대시보드에표시되는위젯수와위젯배치방법을선택할수있습니다.
- 위젯선택**:** 대시보드에표시할정보를선택할수있습니다.
  - 알림**:** 왼쪽의숫자위에있는확인란을선택하여위젯위에알림표시줄을추가합니다. 이표시줄에는규격장치, 비활성장치및지난 24 시간동안초기화되거나등록된장치의수가표시됩니다.
  - 장치 **(**플랫폼기준**):** 플랫폼별로관리되는장치와관리되지않는장치의수를표시합니다.
  - 장치 **(**이동통신사업자기준**):** 이동통신사업자별로관리되는장치와관리되지않는장치의수를표시합니다. 각표시줄을클릭하여플랫폼별분석을볼수있습니다.
  - 관리되는장치 **(**플랫폼기준**):** 플랫폼별로관리되는장치의수를표시합니다.
  - 관리되지않는장치 **(**플랫폼기준**):** 플랫폼별로관리되지않는장치의수를표시합니다. 이차트에나타나는장치는에이전트가설치되어있지만권한이해지되었거나초기화되었을수있습니다.
  - 장치 **(ActiveSync Gateway** 상태기준**):** ActiveSync Gateway 상태별로그룹화된장치수를표시합니다. 정보에는차단됨, 허용됨또는알수없음상태가표시됩니다. 각표시줄을클릭하여플랫폼별로데이터를분류할수있습니다.
  - 장치 **(**소유권기준**):** 소유권상태별로그룹화된장치수를표시합니다. 정보에는회사소유, 직원소유또는알수없는소유권상태가표시됩니다.

- 실패한배달그룹배포**:** 패키지당실패한배포의총수를표시합니다. 배포에실패한패키지만나타납니다.
- 장치 **(**차단된이유기준**):** ActiveSync 에의해차단된장치의수를표시합니다.
- 설치된앱**:** 이위젯을사용하면앱이름을입력하여그래프에해당앱에대한정보를표시할수있습니다.
- 볼륨구매앱라이센스사용현황**:** Apple 볼륨구매앱에대한라이센스사용현황통계를표시합니다.

사용사례

대시보드위젯을사용하여환경을모니터링하는다수의방법에대한몇가지예제는다음과같습니다.

- 모바일생산성앱을배포한후모바일생산성앱이장치에설치되지않는다는내용의지원티켓을받았습니다. 규정위반장치및 설치된앱위젯을사용하여모바일생산성앱이설치되지않은장치를확인합니다.
- 비활성장치를환경에서제거하고라이센스를재확보하기위해비활성장치를모니터링하려고합니다. 비활성장치위젯을사용하여이통계를추적합니다.
- 데이터가올바르게동기화되지않는다는내용의지원티켓을받았습니다. 장치 **(ActiveSync Gateway** 상태기준**)** 및 장치 **(**차단된이유기준**)** 위젯을사용하여문제가 ActiveSync 와관련된것인지여부를확인할수있습니다.

보고

환경설정및사용자등록이완료된후보고서를실행하여배포에관한내용을확인할수있습니다. XenMobile 은환경에서실행되는장치를파악하는데도움이되는다수의보고서를기본적으로제공합니다. 자세한내용은 보고서를참조하십시오.

> 중요**:**
>
> SQL Server 를사용하여사용자지정보고서를만들수있지만이방법은권장하지않습니다. SQL Server 데이터베이스를이방법으로사용하면 XenMobile 배포에예기치않은결과가발생할수있습니다. 이방법의보고를사용하기로결정한경우읽기전용계정을사용하여 SQL 쿼리를실행해야합니다.

역할기반액세스제어및 **XenMobile** 지원

August 12, 2022

XenMobile 은 RBAC(역할기반액세스제어) 를사용하여 XenMobile 시스템기능 (예: XenMobile 콘솔, 원격지원및공용 API) 에대한사용자및그룹의액세스를제한합니다. 이문서에서는 XenMobile 에기본제공되는역할과 XenMobile 에서 RBAC 를활용하는지원모델을결정할때의고려사항에대해설명합니다.

> 참고**:**
>
> 2019 년 1 월 1 일부터신규고객에게는더이상원격지원이제공되지않습니다. 기존고객은제품을계속사용할수있지만 Citrix 는개선사항이나수정사항을제공하지않습니다.

기본제공역할

다음과같은기본제공역할에부여되는액세스권한을변경하고역할을추가할수있습니다. 각역할에연결된액세스및기능권한과역할의 기본설정을모두보려면 XenMobile 설명서에서 Role-Based Access Control Defaults(역할기반액세스제어기본값)를다운로드하십시오. 각기능에대한정의는 XenMobile 설명서에서 RBAC 를사용하여역할구성을참조하십시오.

관리역할

부여되는기본액세스권한:

- 원격지원을제외한전체시스템액세스권한
- 기본적으로관리자는일부지원작업 (예: 연결확인및지원번들만들기) 을수행할수있습니다.

고려사항:

- 일부관리자또는전체관리자가원격지원에액세스해야합니까? 그렇다면관리역할을편집하거나고나리역할을추가할수있습니다.
- 일부관리자또는관리자그룹에대한액세스를추가로제한하려면관리템플릿에따라역할을추가하고권한을편집합니다.

지원

부여되는기본액세스권한:

- 원격지원에대한액세스권한.

고려사항:

- 온-프레미스 XenMobile Server 배포의경우: 원격지원을사용하면지원센터담당자가관리되는 Android 모바일장치를원격으로제어할수있습니다. 스크린캐스트는 Samsung KNOX 장치에서만지원됩니다.
- 원격지원은클러스터링된온-프레미스 XenMobile Server 배포에서지원되지않습니다.

사용자

부여되는기본액세스권한:

- 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 배포및사용자기반에관한이섹션의고려사항을숙지하십시오.

사용자가회사소유의장치를사용합니까**? BYO** 장치를사용합니까**?**
지원에영향을미치는기본적인질문은 XenMobile 환경의사용자장치를누가소유하는지에대한것입니다. 사용자가회사소유의장치를사용하는경우관리자는장치를잠그는방법으로하위수준을지원을제공할수있습니다. 이경우관리자는지원센터를통해장치문제에대한지원및장치사용방법에대한지원을사용자에게제공할수있습니다. 지원해야하는장치의유형에따라지원센터에대한 RBAC 장치프로비전및지원역할을어떻게사용할지고려하십시오.

사용자가 BYO 장치를사용하는경우사용자는장치지원에대한자료를직접찾아야할수있습니다. 이경우조직이제공하는지원은 XenMobile 관련문제에중점을둔관리역할에더가깝습니다.

데스크톱의지원모델은무엇입니까**?**
데스크톱의지원모델이다른회사소유장치에적절한지여부를고려하십시오. 동일한지원조직을사용할수있습니까? 추가로필요한교육은무엇입니까?

XenMobile 자가지원포털에대한액세스권한을사용자에게제공하시겠습니까**?**
설정 **>** 등록을사용하여등록보안모드에자가지원포털을사용설정합니다. 자가지원포털에서사용자는장치를등록하거나등록초대를보내는데사용하는등록링크를생성할수있습니다. 등록보안모드구성을참조하십시오.

시스템모니터링

January 5, 2022

앱액세스및연결을위한작동시간을최적화하려면 XenMobile 환경에서다음과같은핵심구성요소를모니터링해야합니다.

XenMobile 서버

XenMobile 서버는로그를생성하여로컬스토리지에저장합니다. 이로그를시스템로그 (syslog) 서버로내보낼수있습니다. 로그설정을구성하여크기제약또는로그수준을지정하거나특정이벤트를필터링하는사용자지정로거를생성할수있습니다. 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
활성인증서	성공/실패
CSR 인증서	성공/실패
인증서내보내기	성공/실패

이벤트용관리자감사로그메시지	상태
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
DNS 업데이트	성공/실패
네트워크업데이트	성공/실패
로그서버업데이트	성공/실패

이벤트용관리자감사로그메시지	상태
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:

필수적인날짜및타임스탬프값을제외한다른모든특성은선택사항입니다. 선택적필드는메시지에서 " "로표시됩니다. 예를들면다

음과같습니다.

```
<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
Citrix Files 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

MDM 기능	상태
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
SharePoint 구성	성공/실패
프로필제거	성공/실패
응용프로그램제거	성공/실패
관리되지않는응용프로그램제거	성공/실패

MDM 기능	상태
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

Citrix ADC 는각 XenMobile 서버클러스터노드에대한 HTTP 요청을시뮬레이션하는지능형모니터링프로브로구성된 XenMobile 웹서비스상태도모니터링합니다. 이프로브는서비스가온라인상태인지확인한후수신된응답에따라응답합니다. 노드가예상대로응답하지않는경우 Citrix ADC 는서버를중단상태로표시합니다. 또한 Citrix ADC 는노드를부하분산풀에서제거하고, Citrix ADC 모니터링솔루션을통해알림을생성하는데사용할이벤트를기록합니다.

관리자는표준하이퍼바이저모니터링도구를사용하여 XenMobile 가상컴퓨터를모니터링하고 CPU, 메모리, 스토리지사용률메트릭에관한알림을제공할수도있습니다.

SQL Server 및데이터베이스

SQL Server 및데이터베이스성능은 XenMobile Service 에직접적인영향을미칩니다. XenMobile 인스턴스는항상데이터베이스에액세스할수있어야하며 SQL 인프라가중단될경우오프라인으로전환됩니다 (예: 응답하지않음). XenMobile 콘솔은 SQL Server 에서디스크공간문제가발생한후잠시동안작동을계속할수있습니다. 데이터베이스가동시간을최대화하고 XenMobile 작업부하를처리하기에충분한수준의성능을유지하려면 SQL Server 의상태를사전에모니터링해야합니다. SQL Server 모니터링에대한자세한내용은 성능모니터링및튜닝개요를참조하십시오. 또한 XenMobile 환경이확장됨에따라 CPU, 메모리및스토리지에대한리소스할당을조정하여서비스수준계약을보장해야합니다.

Citrix ADC

Citrix ADC 는내부스토리지에메트릭을기록하거나외부로깅서버로로그를보낼수있는기능을제공합니다. Citrix ADC 로그를프로덕션 Splunk 로깅서버로내보내도록 syslog 서버를구성할수있습니다. Citrix ADC 에서는다음과같은로깅수준을사용할수있습니다.

- 긴급
- 알림
- 중요
- 오류
- 경고
- 정보

로그파일은 Citrix ADC 스토리지의 /var/log/ns.log 디렉터리에 newnslog 라는이름으로도저장됩니다. Citrix ADC 는 GZIP 알고리즘을사용하여파일을롤오버하고압축합니다. 로그파일이름은 newnslog.xx.gz 형식을사용하며여기서 xx 는실행번호를나타냅니다.

Citrix ADC 는모니터링옵션으로 SNMP 트랩및알림도지원합니다. SNMP 트랩목록은 SNMP 모니터링을참조하십시오.

재해복구

January 5, 2022

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, Citrix ADC 인프라가포함되며기본사이트에대한연결실패이벤트를통해사용자에게 XenMobile 에대한액세스를제공합니다.

재해복구사이트의 XenMobile 서버는정상작동중에오프라인으로유지되며기본사이트의전체사이트를재해복구사이트로장애조치 (failover) 해야하는재해복구시나리오에서만온라인으로전환됩니다. 재해복구사이트의 SQL Server 는재해복구사이트에서 XenMobile 서버를시작하기전에활성상태이고연결을제공할준비가되어있어야합니다.

이재해복구전략은중단시 MDM 및 MAM 연결을재해복구사이트로라우팅하도록 DNS 를변경함으로써 Citrix ADC 액세스계층을수동으로장애조치 (failover) 합니다.

> 참고**:**
>
> 이아키텍처를사용하려면비동기식데이터베이스백업에대한프로세스와 SQL 인프라의고가용성을보장할방법이있어야합니다.

재해복구장애조치 **(failover)** 프로세스

1. 재해복구장애조치 (failover) 프로세스를테스트하려면기본사이트에서 XenMobile 서버를종료하여사이트장애를시뮬레이션합니다.
2. XenMobile 서버의공용 DNS 레코드를재해복구사이트의외부 IP 주소를가리키도록변경합니다.
3. SQL Server 의내부 DNS 레코드를재해복구사이트의 SQL Server IP 주소를가리키도록변경합니다.
4. 재해복구사이트에서 XenMobile SQL 데이터베이스를온라인으로전환합니다. SQL Server 및데이터베이스가활성상태이고로컬 XenMobile 서버에서사이트로의연결을제공할준비가되었는지확인합니다.
5. 재해복구사이트에서 XenMobile 서버를켭니다.

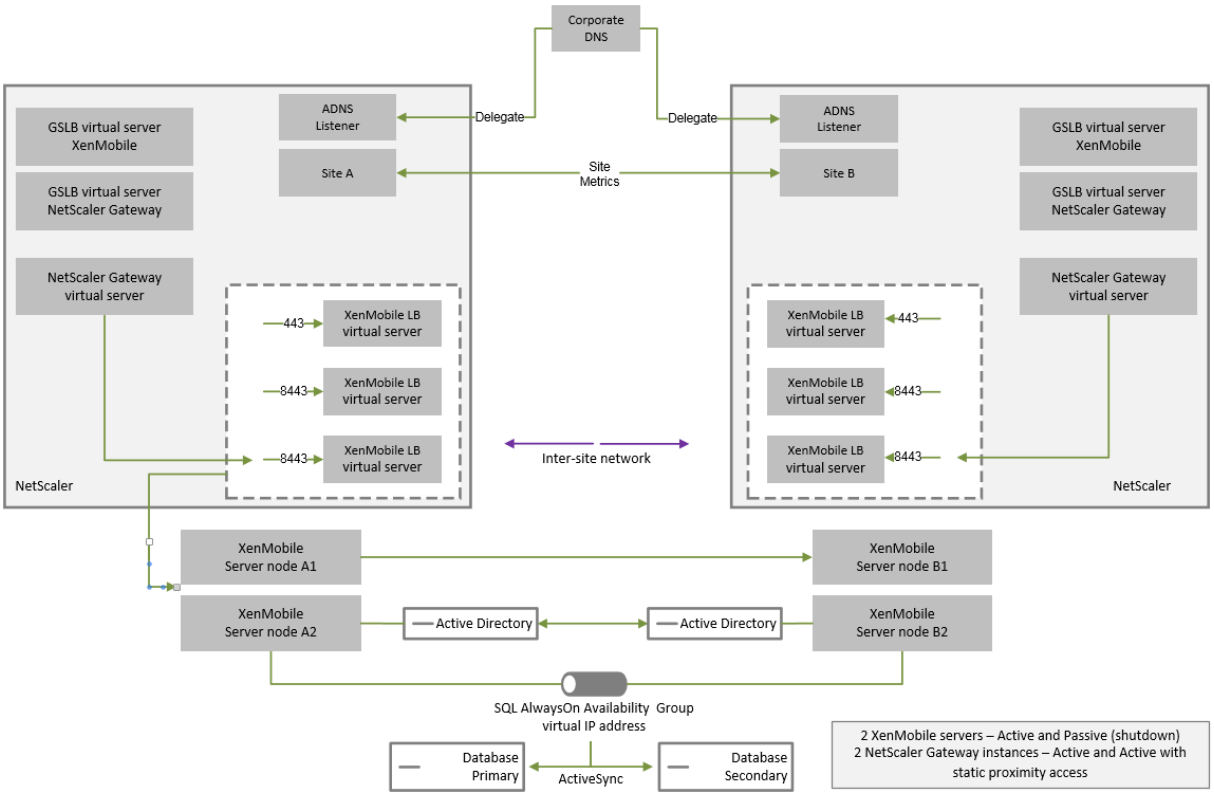
XenMobile 서버업데이트프로세스

패치및릴리스로 XenMobile 을업데이트할때는다음단계에따라기본서버와재해복구서버의코드를동일하게유지하십시오.

1. 기본사이트의 XenMobile 서버에패치가적용되었거나업그레이드되었는지확인합니다.
2. SQL Server 의 DNS 레코드가기본사이트의활성 SQL Server 데이터베이스로확인되는지확인합니다.
3. 재해복구사이트의 XenMobile 서버를온라인으로전환합니다. 이서버는업그레이드프로세스중에만 WAN 의기본사이트데이터베이스에연결합니다.
4. 필요한패치및업데이트를모든재해복구사이트의 XenMobile 서버에적용합니다.
5. XenMobile Server 를다시시작하고패치또는업그레이드가성공했는지확인합니다.

재해복구참조아키텍처다이어그램

다음다이어그램은 XenMobile 의재해복구배포에대한아키텍처개요를보여줍니다.



재해복구용 **GSLB**

이아키텍처의주요요소는 GSLB(Global Server Load Balancing) 를사용하여트래픽을올바른데이터센터로전달하는것입니다.

기본적으로 XenMobile 용 Citrix ADC 마법사에서는재해복구에 GSLB 를사용하지않는방식으로 Citrix Gateway 가구성됩니다. 따라서추가단계를수행해야합니다.

GSLB 의작동방식

GSLB 는 DNS 형태로존재합니다. 참여 Citrix ADC 장비는신뢰할수있는 DNS 서버역할을하며 DNS 레코드를올바른 IP 주소(일반적으로트래픽을수신할수있는 VIP) 로확인합니다. Citrix ADC 장비는트래픽을해당시스템으로전달하는 DNS 쿼리에응답하기전에시스템상태를확인합니다.

레코드가확인되면트래픽을확인하는 GSLB 의역할이완료됩니다. 클라이언트는대상 VIP(가상 IP) 주소와직접통신합니다. DNS 클라이언트동작은레코드의만료방식과시기를제어하는데있어서중요한역할을합니다. 이는주로 Citrix ADC 시스템의경계외부에서수행됩니다. 따라서 GSLB 에는 DNS 이름확인과동일한제한이적용됩니다. 클라이언트가응답을캐시하므로이방식의부하분산은기존의부하분산과달리실시간으로수행되지않습니다.

Citrix ADC 의 GSLB 구성 (사이트, 서비스및모니터포함) 은올바른 DNS 이름확인을제공하는데사용됩니다.

서버게시를위한실제구성 (이시나리오에서는 XenMobile 용 Citrix ADC 마법사에서생성되는구성) 은 GSLB 의영향을받지않습니다. GSLB 는 Citrix ADC 에있는개별서비스입니다.

XenMobile 에서 **GSLB** 를사용하는경우의도메인위임문제

XenMobile 용 Citrix ADC 마법사는 XenMobile 용 Citrix Gateway 를구성합니다. 이마법사는부하분산가상서버세개와 Citrix Gateway 가상서버한개를생성합니다.

부하분산가상서버두개는포트 443 및 8443 에서 MDM 트래픽을처리합니다. Citrix Gateway 는포트 8443 에서 MAM 트래픽을수신한후세번째서버인 MAM 부하분산가상서버에전달합니다. MAM 부하분산가상서버로이동하는모든트래픽은 Citrix Gateway 를통과합니다.

MAM 부하분산가상서버에는 XenMobile 서버와동일한 SSL 인증서가필요하며장치등록시사용된 FQDN 과동일한 FQDN 이 사용됩니다. 또한또 MAM 부하분산서버는 MDM 부하분산서버중하나와동일한포트 (8443) 를사용합니다. 트래픽을확인하기 위해 XenMobile 용 Citrix ADC 마법사는 Citrix 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 Citrix Gateway 가 MDM 부하분산서버로의트래픽을확인할 수없게됩니다.

GSLB 재해복구의 **CNAME** 방법

XenMobile 용 Citrix ADC 마법사의기본구성으로인해발생하는문제를해결하려면상위도메인 (`company.com`) 에 XenMobile 서버 FQDN 에대한 CNAME 레코드를생성하고신뢰할수있는 Citrix ADC 의위임된하위영역 (`gslb.company.com`) 에있는레코드를가리키면됩니다. 이렇게하면트래픽을확인하는데필요한 MAM 부하분산 VIP 주소에대한정적 DNS A 레코드를생성할수있습니다.

1. 외부 DNS 에서 Citrix ADC GSLB 의 GSLB 도메인 FQDN 을가리키는 XenMobile 서버 FQDN 에대한 CNAME 를생성합니다. 두개의 GSLB 도메인이필요합니다. 하나는 MDM 트래픽을위한것이고다른하나는 MAM(Citrix Gateway) 트래픽을위한것입니다.

   예:

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. 각사이트의 Citrix Gateway 인스턴스에서 CNAME 레코드가가리키는 FQDN 으로 GSLB 가상서버를생성합니다.

   예:

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   XenMobile 용 Citrix ADC 마법사를사용하여 Citrix Gateway 를배포하는경우 MAM 부하분산서버를구성할때 XenMobile 서버 URL 을사용하십시오. 그러면 XenMobile 서버 URL 에대한정적 DNS A 레코드가생성됩니다.

3. XenMobile 서버 URL(`xms.company.com`) 을사용하여 Secure Hub 에등록하는클라이언트를테스트합니다.

   이예에서는다음 FQDN 을사용합니다.

   - `xms.company.com` - MDM 트래픽과장치등록에사용되는 URL 이며이예에서는 XenMobile 용 Citrix ADC 마법사를사용하여구성되었습니다.
   - `xms.gslb.company.com` - XenMobile 서버의 GSLB 도메인 FQDN 입니다.

Citrix 지원프로세스

March 24, 2022

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.

지원사례를작성하기전에자가지원리소스및권장사항을완벽하게검토하는것이좋습니다. 예를들어 Citrix 기술전문가가작성한문서와공지에액세스하거나, Citrix 솔루션및기술에대한제품설명서를보거나, Citrix 경영진, 제품팀및기술전문가의직설을읽어볼수있는다수의위치가있습니다. 각각 Knowledge Center, 제품설명서 및 블로그 페이지를참조하십시오.

추가적인대화형지원이필요하다면토론포럼에참여하여다른고객으로부터질문에대한실시간답변을얻거나, 사용자그룹및관심그룹내에서아이디어, 의견, 기술정보및모범사례를공유하거나, Citrix 지원의소셜네트워킹사이트를모니터링하는 Citrix 지원엔지니어와상호작용할수있습니다. 지원포럼 및 Citrix 커뮤니티 페이지를각각참조하십시오.

교육및인증과정에액세스하여기술을강화할수도있습니다. Citrix Education을참조하십시오.

Citrix Insight Services 는단순한온라인문제해결플랫폼과 Citrix 환경을위한상태검사기를제공합니다. XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor 및 Citrix Gateway 에사용할수있습니다. Analysis Tool(분석도구)을참조하십시오.

기술지원을받으려면전화또는웹을통해지원사례를만들어야합니다. 중요도가낮거나중간인문제에대해서는웹을사용하고, 중요도가높은문제에대해서는전화옵션을사용할수있습니다. XenMobile 문제에대해지원을문의하려면 Citrix 지원서비스를참조하십시오.

Citrix 솔루션제공에대한방대한경험을갖춘, 고도로숙련된단일의담당자를원한다면 Citrix 서비스의 Technical Relationship Manager 에게문의할수있습니다. Citrix 서비스제공및이점에대한자세한내용은 Citrix Worldwide Services를참조하십시오.

XenMobile 에서그룹등록초대보내기

September 29, 2021

작성자: John Bartel III

XenMobile Server 에서그룹및중첩그룹에등록초대를보낼수있습니다. Windows 장치에서는등록초대를사용할수없습니다.

그룹초대를설정할때하나이상의장치플랫폼을지정할수있습니다. 또한장치에태그를지정하여회사소유의장치를직원소유의장치와구분하는등의작업을수행할수있습니다. 그런다음사용자장치에대한인증유형을설정합니다.

> 참고:
>
> 사용자지정알림템플릿을사용하려는경우등록모드를구성하기전에템플릿을설정해야합니다. 알림템플릿에대한자세한내용은 알림템플릿만들기및업데이트를참조하십시오.

사용자계정, 역할및등록보안모드와초대의기본구성에대한자세한내용은 사용자계정, 역할및등록을참조하십시오.

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. 등록모드를사용하여사용자에대해선호하는인증보안유형을설정할수있습니다.

   - 사용자이름 + 암호
   - 높은수준의보안
   - 초대 URL
   - 초대 URL + PIN
   - 초대 URL + 암호
   - 2 단계
   - 사용자이름 + PIN

   > 참고:
   >
   > 등록초대를보내기위해서는 초대 **URL**, 초대 **URL + PIN**, 초대 **URL +** 암호등록보안모드만사용할수있습니다. 사용자이름 **+** 암호, **2** 단계또는 사용자이름 **+ PIN** 으로등록하는장치의경우사용자는 Secure Hub 에서자격증명을수동으로입력해야합니다.
8. 에이전트다운로드, 등록 **URL**, 등록 **PIN** 및 등록확인템플릿에대해이전에만든사용자지정알림템플릿을선택합니다. 또는나열된기본값을선택합니다.

   사용자지정알림템플릿을사용하려는경우등록모드를구성하기전에템플릿을설정해야합니다. 알림템플릿에대한자세한내용은 알림을참조하십시오.

이러한알림템플릿에는 XenMobile 내에서구성한 SMTP 서버설정을사용합니다. 계속하기전에 SMTP 정보를먼저설정합니다.

> 참고:
>
> 다음이후에만료및 최대시도횟수옵션은선택한 등록모드옵션에따라변경됩니다. 이러한옵션은변경할수없습니다.

9. 초대보내기에대해켜짐을선택한다음 저장및보내기를클릭하여프로세스를완료합니다.

중첩그룹지원

중첩그룹을사용하여초대를보낼수있습니다. 일반적으로중첩그룹은유사한권한을가진그룹이서로바인딩되어있는대규모환경에서사용됩니다.

설정 **> LDAP** 로이동하고 중첩그룹지원옵션을사용하도록설정합니다.

문제해결및알려진제한

문제**:** Active Directory 그룹에서제거된사용자에게도초대가전송됩니다.

해결방법**:** Active Directory 환경의규모에따라변경내용이모든서버로전파되는데최대 6 시간이소요될수있습니다. 최근에사용자또는중첩그룹을제거한경우 XenMobile 에서이러한사용자가그룹의일부로간주될수있습니다.

그러므로그룹에다른그룹초대를보내기전에최대 6 시간을기다리는것이가장좋습니다.

온-프레미스장치상태증명서버구성

January 5, 2022

작성자: Sanket Mishra

Windows 10 및 Windows 11 모바일장치에대한 DHA(장치상태증명) 를온-프레미스 Windows 서버를통해사용할수있습니다. DHA 온-프레미스를사용하려면먼저 DHA 서버를구성해야합니다.

DHA 서버를구성한후온-프레미스 DHA 서비스를사용하도록설정하는 XenMobile Server 정책을만듭니다. 이정책만들기에대한자세한내용은 장치상태증명장치정책을참조하십시오.

DHA 서버의사전요구사항

- 데스크톱환경설치옵션을사용하여설치된 Windows Server Technical Preview 5 이상을실행하는서버.
- 하나이상의 Windows 10 및 Windows 11 클라이언트장치. 이러한장치에는최신버전의 Windows 를실행하는 TPM 1.2 또는 2.0 이있어야합니다.
- 인증서:

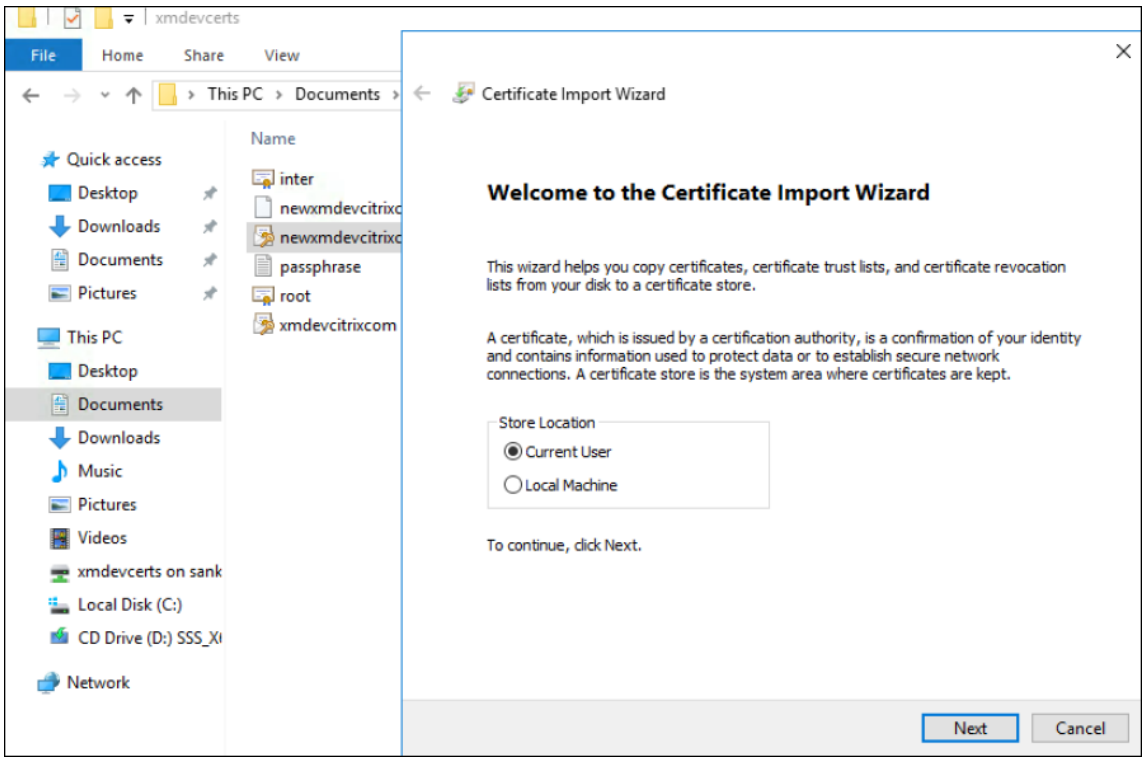
  - **DHA SSL** 인증서**.** 내보내기가능한개인키를사용하여엔터프라이즈의신뢰할수있는루트에체인으로연결되는 x.509 SSL 인증서. 이인증서는서버-서버 (DHA 서비스와 MDM 서버) 및서버-클라이언트 (DHA 서비스와 Windows 10 및 Windows 11 장치) 커뮤니케이션을포함하여전송중인 DHA 데이터통신을보호합니다.
  - **DHA** 서명인증서**.** 내보내기가능한개인키를사용하여엔터프라이즈의신뢰할수있는루트에체인으로연결되는 x.509 인증서. DHA 서비스는이인증서를디지털서명에사용합니다.
  - **DHA** 암호화인증서**.** 내보내기가능한개인키를사용하여엔터프라이즈의신뢰할수있는루트에체인으로연결되는 x.509 인증서. DHA 서비스는이인증서를암호화에도사용합니다.
- 다음과같은인증서유효성검사모드중에서하나를선택합니다.
  - **EKCert.** EKCert 유효성검사모드는인터넷에연결되지않은조직의장치에최적화되었습니다. EKCert 유효성검사모드에서실행되는 DHA 서비스에연결하는장치는인터넷에직접연결할수없습니다.
  - **AIKCert.** AIKCert 유효성검사모드는인터넷에액세스할수있는작동환경에최적화되었습니다. AIKCert 유효성검사모드에서실행되는 DHA 서비스에연결하는장치는인터넷에직접연결할수있고 Microsoft 에서 AIK 인증서를 가져올수있어야합니다.

Windows 서버에 **DHA** 서버역할추가

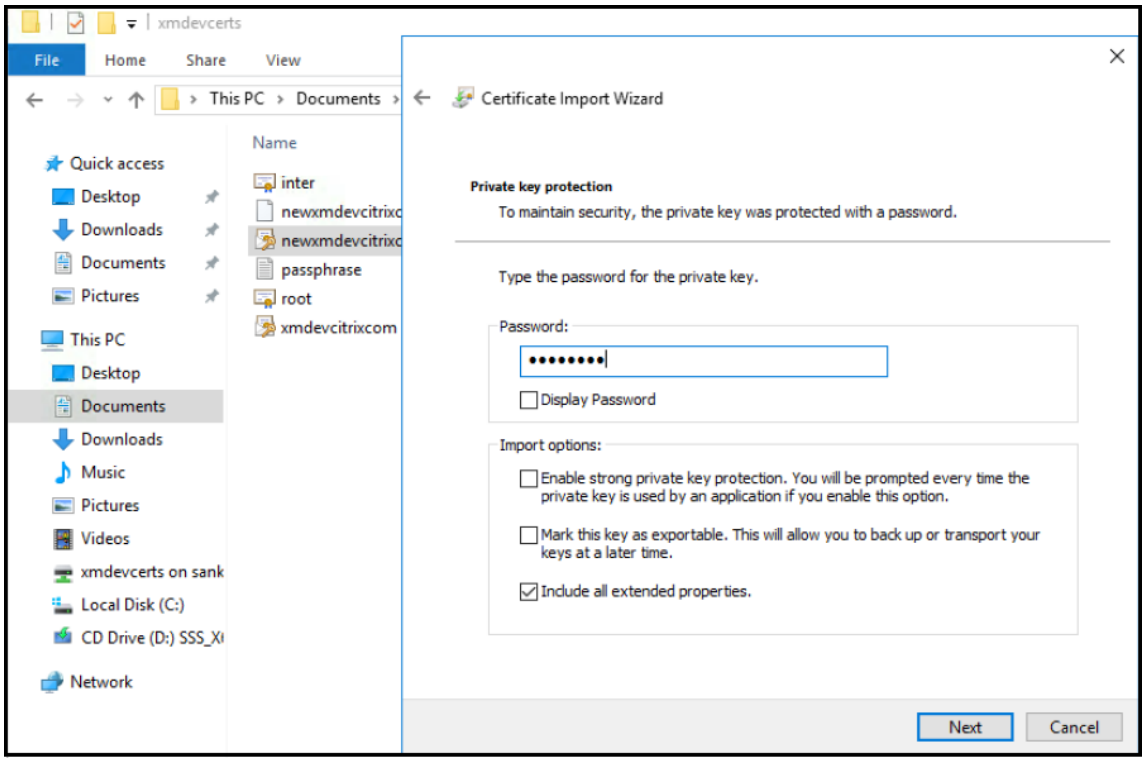
1. Windows 서버에서서버관리자가이미열려있지않은경우 시작을클릭하고 서버관리자를클릭합니다.
2. 역할및기능추가를클릭합니다.
3. 시작하기전에페이지에서 다음을클릭합니다.
4. 설치유형선택페이지에서 역할기반또는기능기반설치를클릭하고 다음을클릭합니다.
5. 대상서버선택페이지에서 서버풀에서서버선택을클릭하고서버를선택한후 다음을클릭합니다.
6. 서버역할선택페이지에서장치상태증명확인란을선택합니다.
7. 선택사항: 기능추가를클릭하여필요한다른역할서비스및기능을설치합니다.
8. 다음을클릭합니다.
9. 기능선택페이지에서 다음을클릭합니다.
10. 웹서버역할 **(IIS)** 페이지에서 다음을클릭합니다.
11. 역할서비스선택페이지에서 다음을클릭합니다.
12. 장치상태증명서비스페이지에서 다음을클릭합니다.
13. 설치선택확인페이지에서 설치를클릭합니다.
14. 설치가완료되면 닫기를클릭합니다.

서버의인증서저장소에 **SSL** 인증서추가

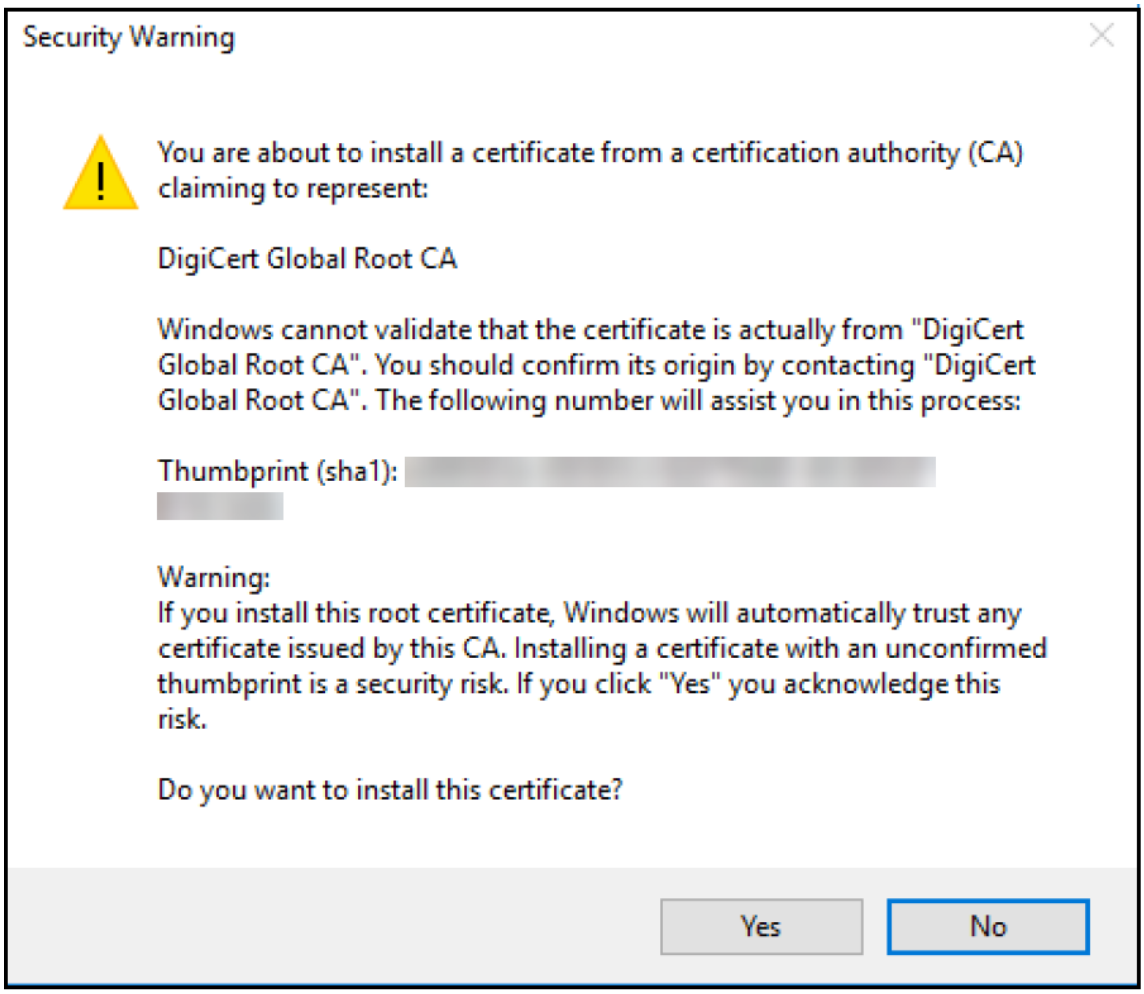
1. SSL 인증서파일로이동하고파일을선택합니다.
2. 현재사용자를저장소위치로선택하고 다음을클릭합니다.



3. 개인키에대한암호를입력합니다.
4. 확장속성모두포함가져오기옵션이선택되었는지확인합니다. 다음을클릭합니다.



5. 이창이나타나면 예를클릭합니다.



6. 인증서가설치되었는지확인합니다.

   a) 명령프롬프트창을엽니다.

   b) **mmc** 를입력하고 Enter 키를누릅니다. 로컬컴퓨터저장소의인증서를보려면관리자역할이있어야합니다.

   c) 파일메뉴에서 스냅인추가/제거를클릭합니다.

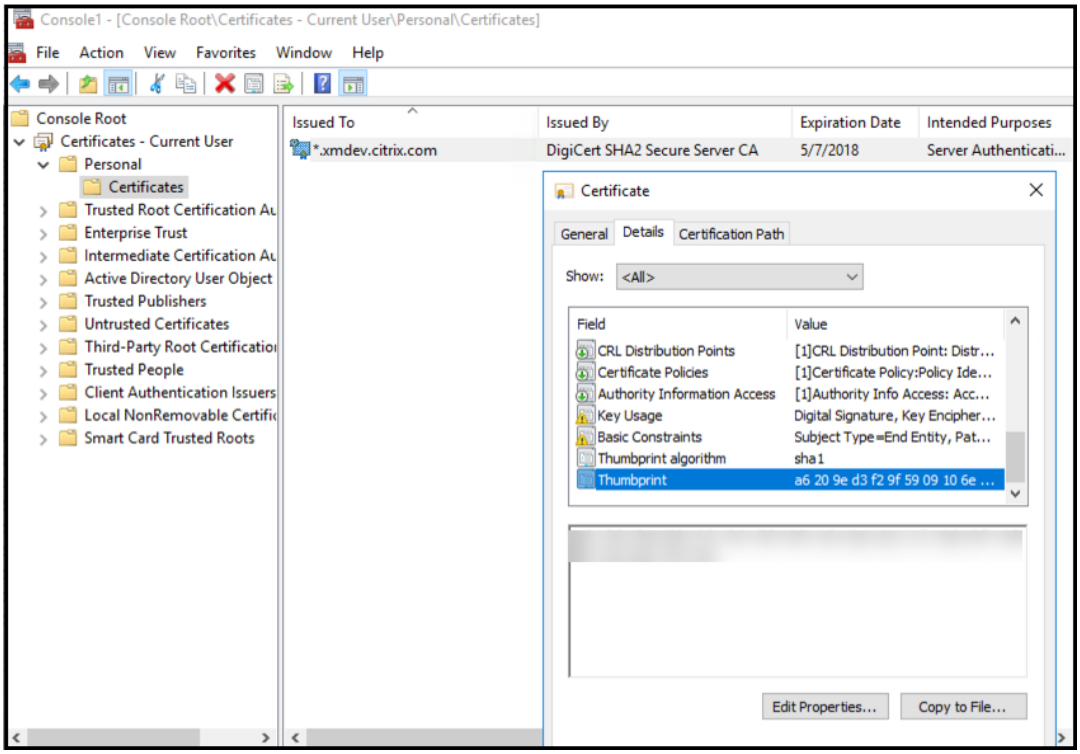
   d) 추가를클릭합니다.

   e) 독립실행형스냅인추가대화상자에서 인증서를선택합니다.

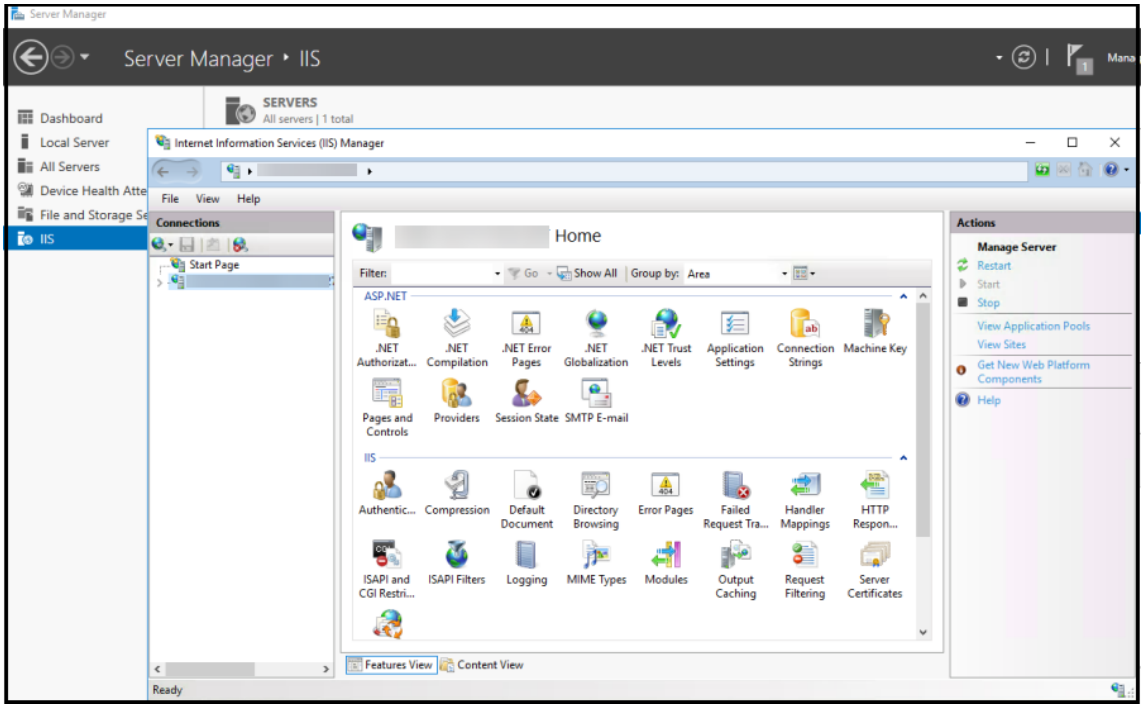
   f) 추가를클릭합니다.

   g) 인증서스냅인대화상자에서 내사용자계정을선택합니다. 서비스계정소유자로로그인한경우 서비스계정을선택합니다.

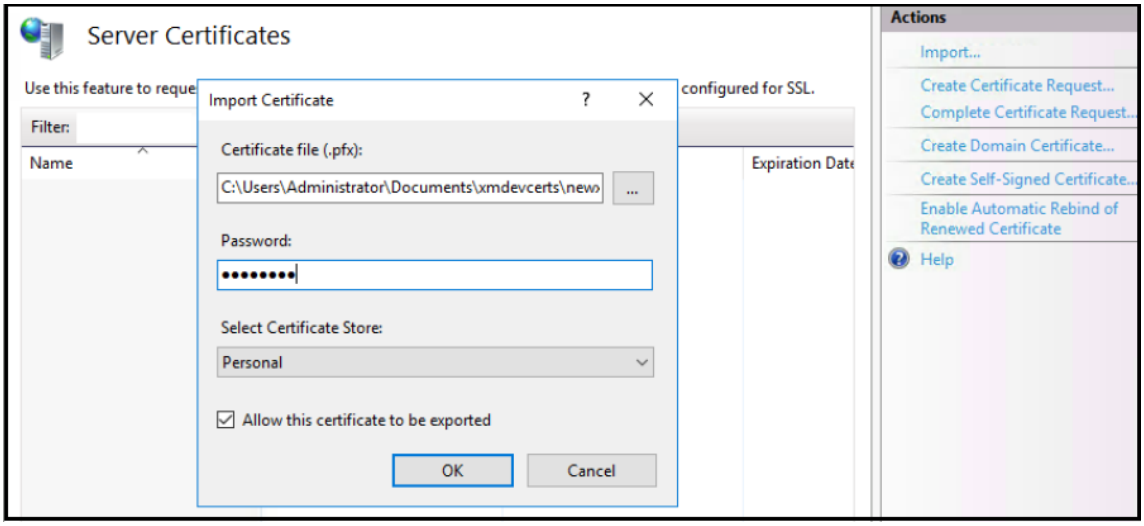
   h) 컴퓨터선택대화상자에서 마침을클릭합니다.



7. 서버관리자 **> IIS** 로이동하고아이콘목록에서 서버인증서를선택합니다.

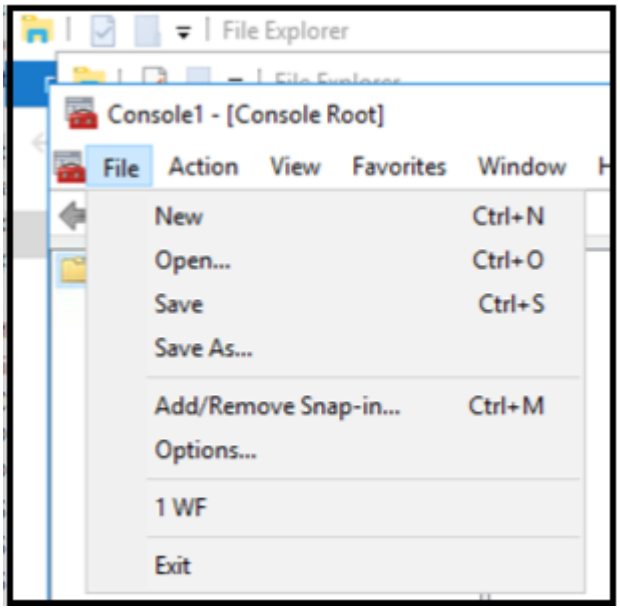


8. 작업메뉴에서 가져오기**...**를선택하여 SSL 인증서를가져옵니다.

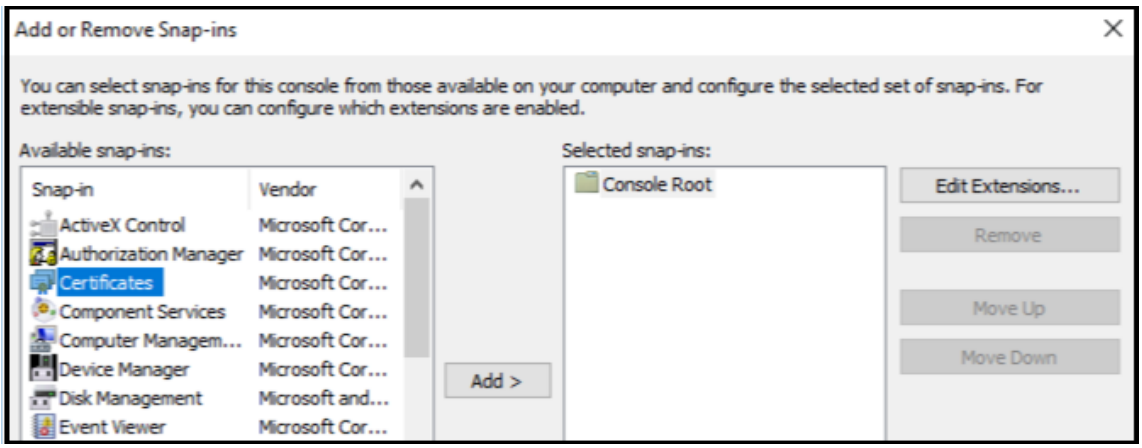


인증서지문검색및저장

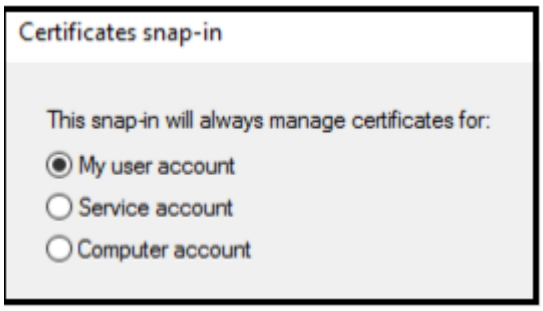
1. 파일탐색기검색표시줄에 **mmc** 를입력합니다.
2. 콘솔루트창에서 파일 **>** 스냅인추가/제거**...**를클릭합니다.



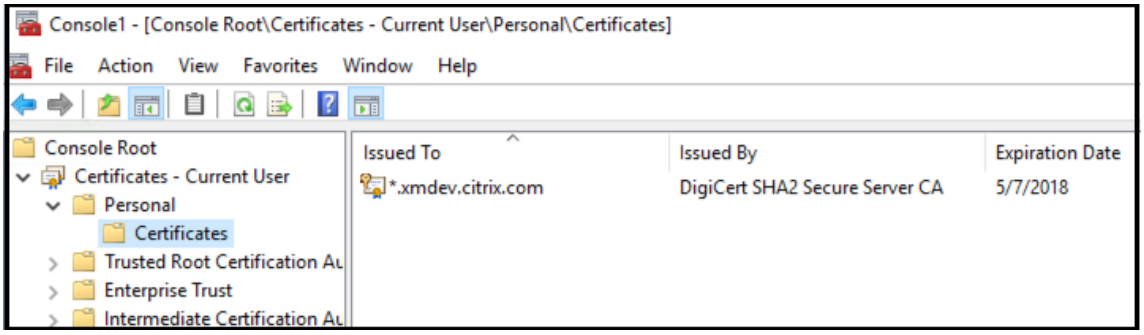
3. 사용가능한스냅인에서인증서를선택하고선택한스냅인에추가합니다.



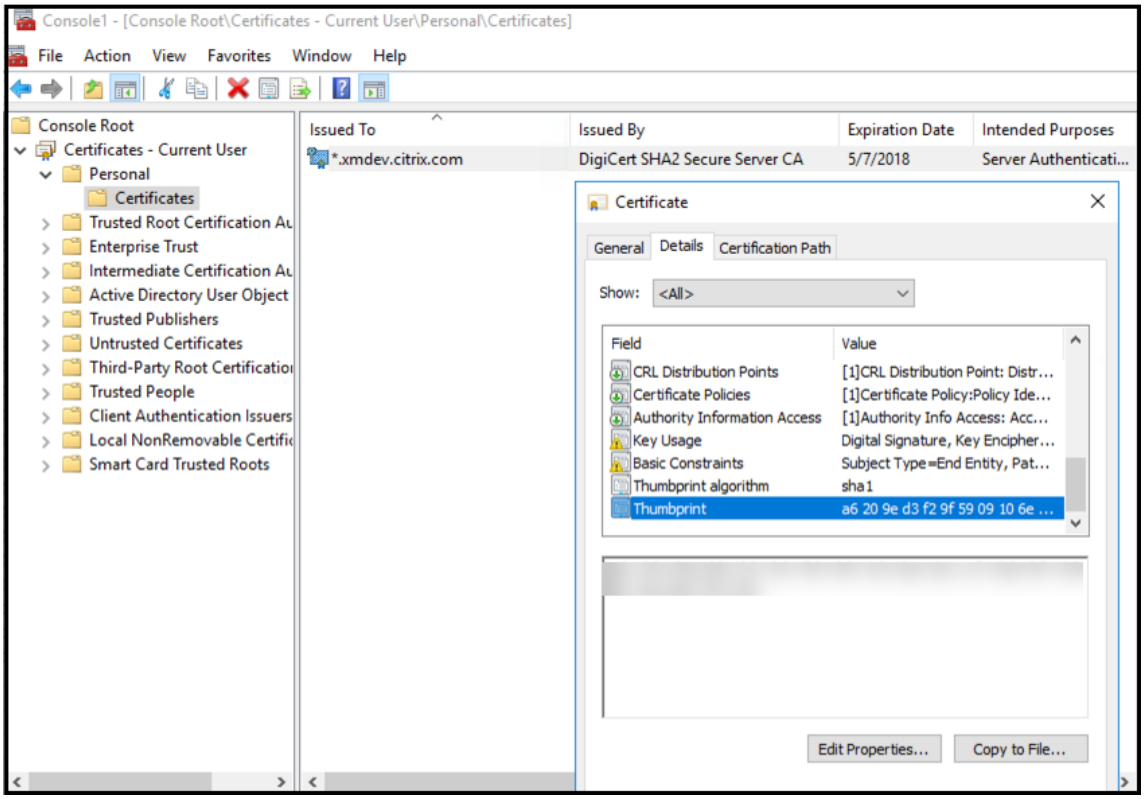
4. 내사용자계정을선택합니다.



5. 인증서를선택하고 확인을클릭합니다.



6. 인증서를두번클릭하고 세부정보탭을선택합니다. 아래로스크롤하여인증서지문을표시합니다.



7. 지문을파일에복사합니다. PowerShell 명령에서지문을사용하는경우공백을제거합니다.

서명및암호화인증서설치

Windows 서버에서다음 PowerShell 명령을실행하여서명및암호화인증서를설치합니다.

표시된것과같이 ReplaceWithThumbprint 자리표시자를바꾸고큰따옴표로묶습니다.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like ”ReplaceWithThumbprint” }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + ”\Microsoft\Crypto\RSA\MachineKeys” +
   $keyname icacls $keypath /grant IIS_IUSRS`:R
<!--NeedCopy-->
```

TPM 루트인증서추출및신뢰할수있는인증서패키지설치

Windows 서버에서다음명령을실행합니다.


```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

DHA 서비스구성

Windows 서버에서다음명령을실행하여 DHA 서비스를구성합니다.

ReplaceWithThumbprint 자리표시자를바꿉니다.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

Windows 서버에서다음명령을실행하여 DHA 서비스에대한인증서체인정책을설정합니다.

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

다음프롬프트에다음과같이응답합니다.

```
  Confirm
```



```
2
3       Are you sure you want to perform this action?
4
5       Performing the operation "Install-DeviceHealthAttestation" on
            target "WIN-N27D1FKCEBT".
6
7       [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
            Help (default is "Y"): A
8
9       Adding SSL binding to website 'Default Web Site'.
10
11      Add SSL binding?
12
13      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15      Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17      Add application pool?
18
19      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21      Adding web application 'DeviceHealthAttestation' to website '
            Default Web Site'.
22
23      Add web application?
24
25      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27      Adding firewall rule 'Device Health Attestation Service' to allow
            inbound connections on port(s) '443'.
28
29      Add firewall rule?
30
31      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33      Setting initial configuration for Device Health Attestation Service
            .
34
35      Set initial configuration?
36
37      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39      Registering User Access Logging.
40
41      Register User Access Logging?
```



```
42
43      [Y] Yes   [N] No   [S] Suspend   [?] Help (default is "Y"): Y
44  <!--NeedCopy-->
```

구성확인

DHASActiveSigningCertificate 가활성상태인지확인하려면서버에서다음명령을실행합니다.

```
Get-DHASActiveSigningCertificate
```

인증서가활성상태인경우인증서유형 (서명) 과지문이표시됩니다.

DHASActiveSigningCertificate 가활성상태인지확인하려면서버에서다음명령을실행합니다.

표시된것과같이 ReplaceWithThumbprint 자리표시자를바꾸고큰따옴표로묶습니다.

```
1  Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
       -Force
2
3  Get-DHASActiveEncryptionCertificate
4  <!--NeedCopy-->
```

인증서가활성상태인경우지문이나타납니다.

최종검사를수행하려면다음 URL 로이동합니다.

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

DHA 서비스가실행중인경우 "메서드를사용할수없음" 이나타납니다.

Secure Mail 푸시알림을통한 **EWS** 의인증서기반인증구성

June 17, 2022

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.

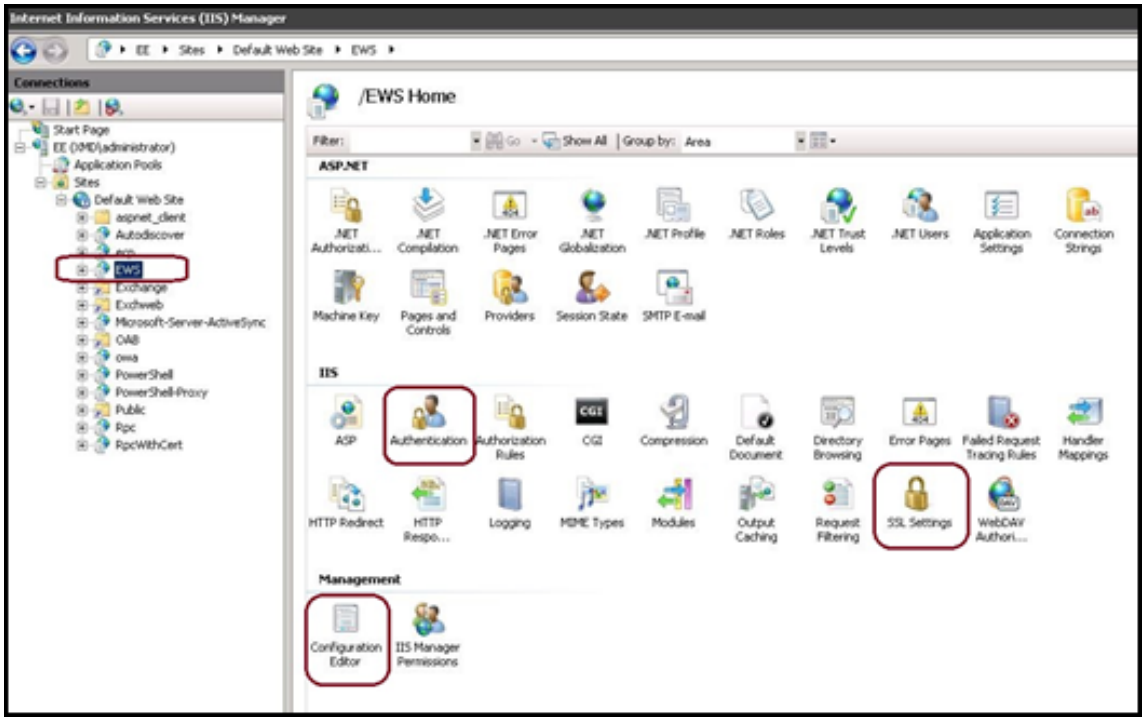
이러한구성을완료하지않으면 Secure Mail 푸시알림에대한구독이실패하고 Secure Mail 에서배지업데이트가수행되지않습니다.

이문서에서는인증서기반인증을구성하는단계를설명합니다. 구성은 Exchange Server 의 EWS 가상디렉터리에대한것입니다.

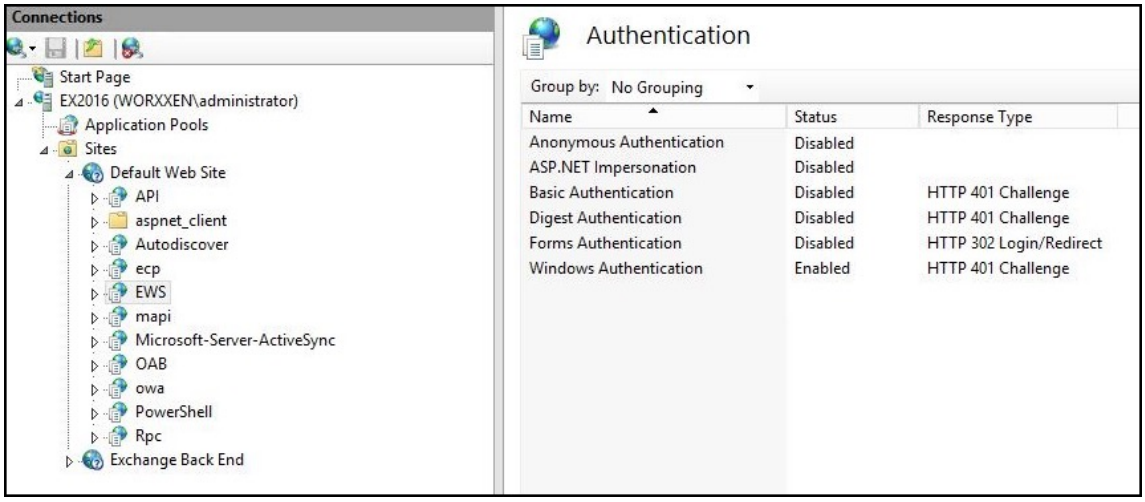
구성을시작하려면다음을수행하십시오.

1. EWS 가상디렉터리가설치된하나이상의서버에로그온합니다.
2. IIS 관리자콘솔을엽니다.
3. 기본웹사이트에서 EWS 가상디렉터리를클릭합니다.

   인증, SSL, 구성편집기스냅인은 IIS 관리자콘솔의오른쪽에표시됩니다.



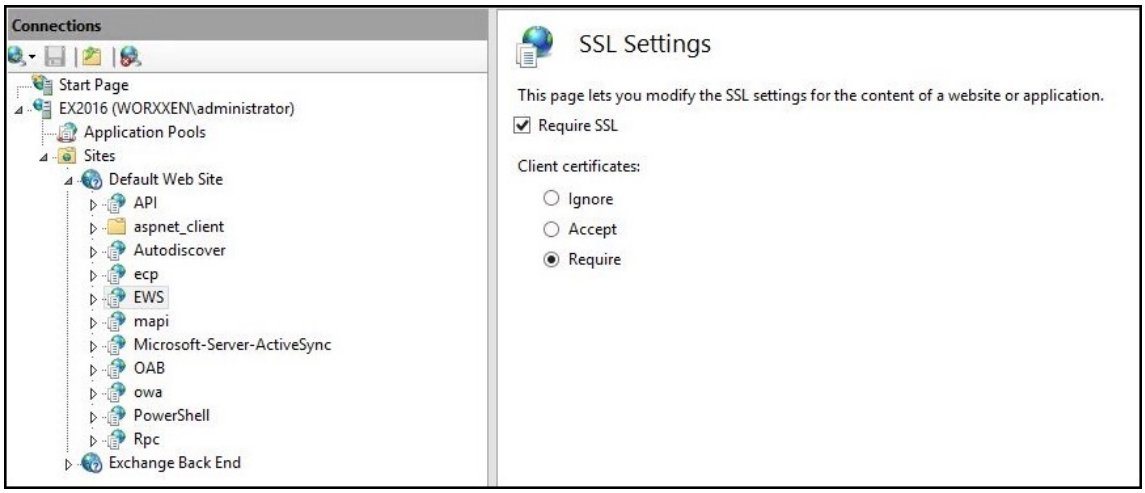
4. EWS 에대한 인증설정이다음그림과같이구성되었는지확인합니다.



5. EWS 가상디렉터리에대한 **SSL** 설정을구성합니다.

   a) **SSL** 필요확인란을선택합니다.

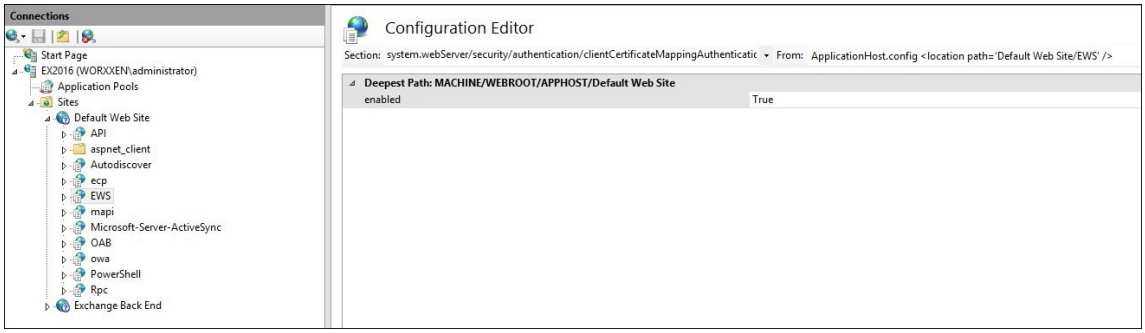
   b) 클라이언트인증서에서 필요를클릭합니다. 다른 EWS 메일클라이언트가사용자이름과암호를자격증명으로사용하여 Exchange Server 에인증하고연결하는경우이옵션을 수락으로설정할수있습니다.



6. 구성편집기를클릭하고 섹션드롭다운목록에서다음섹션으로이동합니다.

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. **enabled** 값을 **True** 로설정합니다.

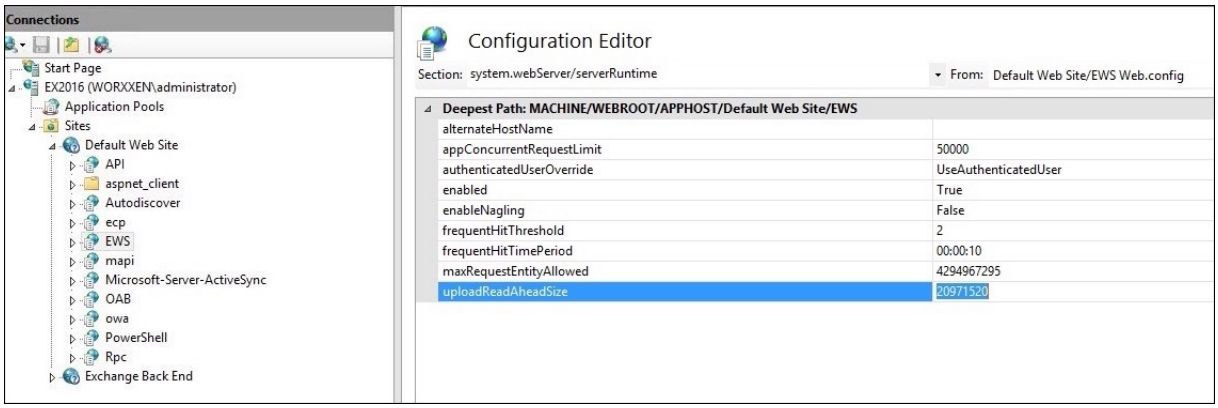


8. 구성편집기를클릭하고 섹션드롭다운목록에서다음섹션으로이동합니다.
   - **system.webServer/serverRuntime**
9. **uploadReadAheadSize** 값을 **10485760**(10MB) 또는 **20971520**(20MB) 으로설정하거나조직에필요한값으로설정합니다.

   > 중요:
   >
   > 이값을올바르게설정하지않으면인증서기반인증이 EWS 푸시알림을구독하는동안실패하고오류코드 413 이표시됩니다.
   >
   > 이값을 **0** 으로설정하지마십시오.

자세한내용은다음타사리소스를참조하십시오.

- Microsoft IIS Server Runtime(Microsoft IIS 서버런타임)
- Butsch Client Management Blog(Butsch 클라이언트관리블로그)



iOS 푸시알림과관련된 Secure Mail 문제를해결하는방법에대한자세한내용은이 Citrix Support Knowledge Center 문서를참조하십시오.

관련정보

iOS 용 Secure Mail 의푸시알림

XenMobile MDM(모바일기기관리) 을 Cisco ISE(ID 서비스엔진) 와통합

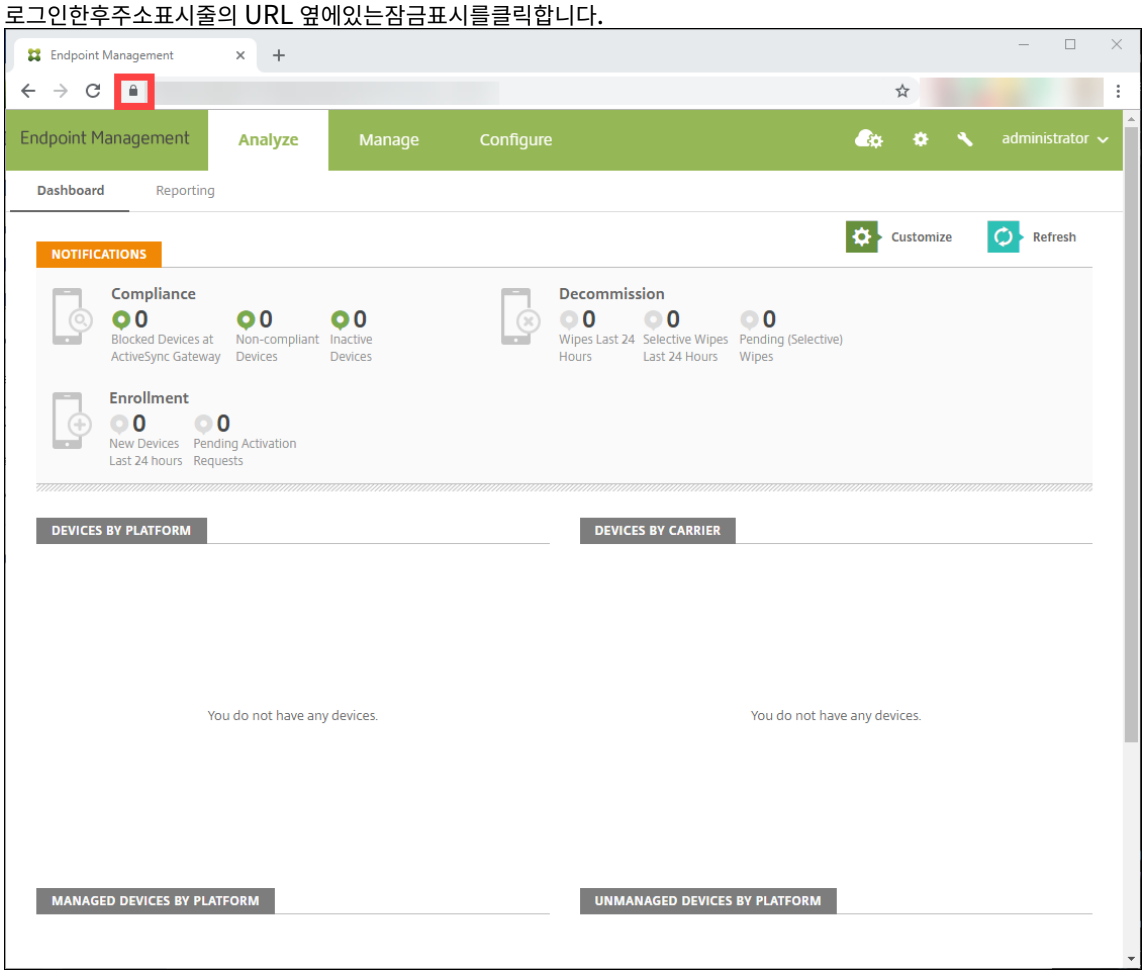
July 18, 2022

작성자: John Bartel III

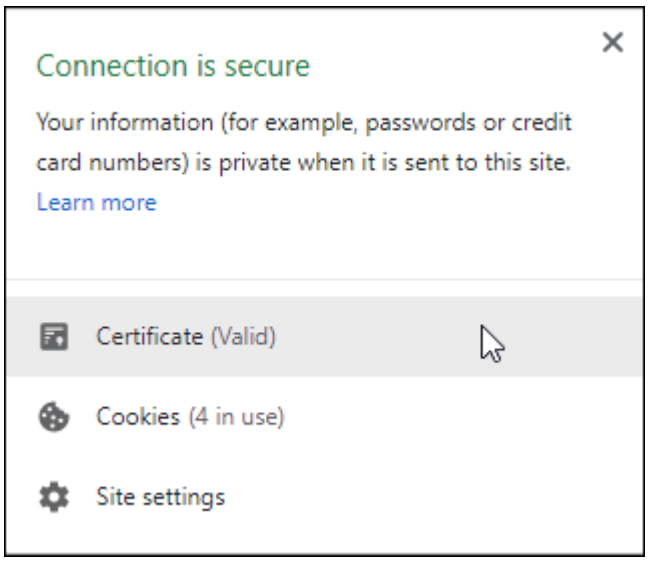
Cisco ISE 는작업공간에서모바일장치를배포, 보안, 모니터링, 통합및관리하는데사용됩니다. 모바일장치에다운로드된소프트웨어를통해응용프로그램및패치의배포를제어하고엔드포인트의데이터및구성을제어할수있습니다. XenMobile 을 Cisco ISE 와통합하면 Cisco ISE 콘솔에서비호환장치및관리되지않는장치를관리할수있습니다. 또한 XenMobile 을사용하면회사서비스에대한액세스를선택적으로허용, 거부또는격리할수있습니다.

XenMobile 과의통합을설정하려면 XenMobile Server 에서관리자 RBAC 역할이할당된로컬서비스계정을만듭니다. Cisco ISE 는이역할을사용하여 XenMobile API 에액세스할수있습니다. ISE 는 XenMobile 인증서를신뢰해야합니다. 이인증서를다운로드하려면웹브라우저를열고서버 URL 로이동하여로그인합니다.

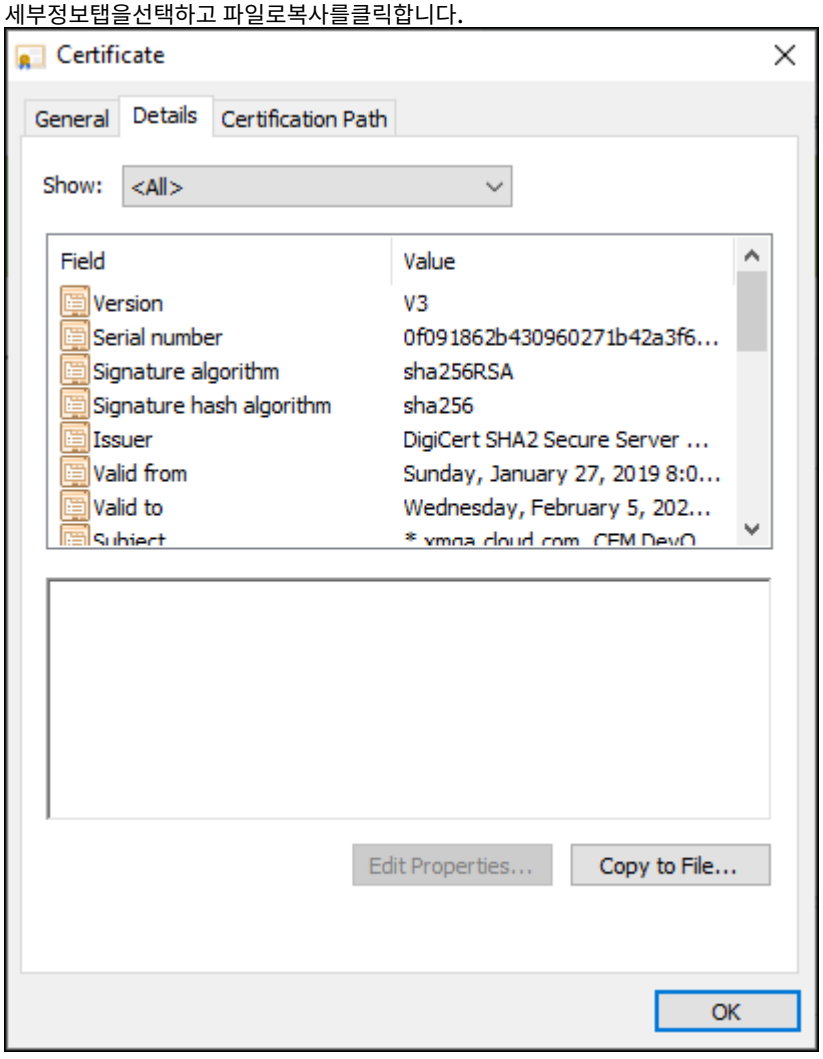
1. 로그인한후주소표시줄의 URL 옆에있는잠금표시를클릭합니다.



2. 인증서를클릭합니다.



3. 세부정보탭을선택하고 파일로복사를클릭합니다.



4. 마법사에따라인증서를로컬로저장합니다.
5. Cisco ISE 콘솔에로그인하고이전에다운로드한 XenMobile 인증서를가져옵니다. 인증서를 Cisco ISE 의신뢰할수있

는인증서저장소로가져옵니다. 이가져오기는 Cisco ISE 가 XenMobile Server 와의통신을신뢰하는데필요합니다.

a) **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Certificate Management(**인증서관리**) > Trusted Certificates(**신뢰할수있는인증서**)** 로이동합니다. 가져오기를클릭합니다.

b) 인증서이름을지정하고 **Trust for authentication within ISE(ISE** 내의인증신뢰**)** 및 **Trust for authentication of Cisco Services(Cisco** 서비스의인증신뢰**)** 확인란을선택합니다.

6. XenMobile 을 Cisco ISE 내부의외부 MDM 으로추가합니다.

a) **Administration(**관리**) > Network Resource(**네트워크리소스**) > External MDM(**외부 **MDM)** 으로이동합니다. **Add(**추가**)** 를클릭하고다음을입력합니다.

- **Server Host(**서버호스트**):** XenMobile FQDN
- **Port(**포트**):** 443
- **Instance name(**인스턴스이름**):** XenMobile Server 의인스턴스이름입니다. 대부분의배포에서인스턴스이름은기본적으로 “zdm” 입니다.
- **User Name(**사용자이름**):** 이작업에대해만든사용자이름을입력합니다. 사용자는원래관리자 RBAC 그룹의로컬관리자계정이어야합니다.
- **Password(**암호**):** 방금추가한사용자의암호입니다.
- **Enable(**사용**)** 확인란을선택합니다.

7. 테스트에성공하면 **Submit(**제출**)** 을클릭합니다.

Cisco ISE 에대한자세한내용은 Cisco 설명서를참조하십시오.

> 참고**:**
>
> 호스팅된 Endpoint Management 에서는 ISE 통합이지원되지않습니다.

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