모바일 생산성 앱

Contents

모바일 생산성 앱 릴리스 일정

September 4, 2024

Citrix 모바일 생산성 앱은 2 주에 걸쳐 출시됩니다. 정확한 날짜는 변경될 수 있지만 미리 계획을 세울 수 있도록 일정을 제공해 드립니다. 또한, 이를 통해 앱 배포 및 업데이트를 더 쉽게 관리할 수 있기를 바랍니다.

Secure Mail 및 **Secure Web** 단계별 릴리스 프로세스 정보

Secure Mail 및 Secure Web 의 새 버전이 제공되면 다음과 같은 단계별 접근 방식으로 릴리스가 제공됩니다.

- iOS 및 Android 사용자의 경우 App Store 및 Google Play Store 에서 1 주일 (7 일) 간 점진적으로 확대되는 Secure Mail 및 Secure Web 업데이트를 사용할 수 있습니다.
- iOS 용 Secure Mail 및 Secure Web 의 새 다운로드는 해당 주 안에 새 버전으로 제공됩니다. Android 용 Secure Mail 및 Secure Web 의 새 다운로드는 해당 주 동안 이전 버전으로 실행되다가 모든 사용자에게 제공되는 새 릴리스가 100% 가 되면 새 버전으로 제공됩니다.
- 사용자를 위해 일부 기능은 점진적 단계로 릴리스됩니다.

기능 플래그 관리를 위한 필수 구성 요소

운영 중인 Secure Hub 또는 Secure Mail 에서 문제가 발생하는 경우 Citrix 에서 앱 코드 내에서 영향을 받는 기능을 사용 중지할 수 있습니다. 이를 위해 Citrix 에서는 기능 플래그와 LaunchDarkly 라는 타사 서비스를 사용하고 있습니다. LaunchDarkly 로의 트래픽을 사용하도록 설정하기 위해 별도의 구성은 필요 없습니다. 단, 방화벽이나 프록시로 아웃바운드 트래픽을 차단하는 경우에는 별도의 구성이 필요합니다. 위의 두 가지 경우에는 정책 요구 사항에 따라 특정 URL 이나 IP 주소를 통해 LaunchDarkly 로의 트래픽을 사용하도록 설정해야 합니다. 모바일 생산성 앱 10.6.15 이후 MDX 가 터널링에서 도메인의 제외를 지원하는 데 대한 자세한 내용은 MDX Toolkit 설명서를 참조하십시오. 기능 플래그 및 LaunchDarkly 에 대한 FAQ 는 이 Support Knowledge Center 문서를 참조하십시오.

> 참고:
> 단계적으로 중단되는 Citrix Endpoint Management 기능에 대한 사전 알림은 사용 중단을 참조하십시오.

모바일 생산성 앱 지원

February 27, 2024

자동 업데이트를 사용하도록 설정한 사용자는 앱 스토어에서 최신 버전을 받습니다. 모바일 생산성 앱의 최신 버전은 다음과 같습니다.

- 23.10.0(Android 용 Secure Web)
- 23.9.0(iOS 용 Secure Mail 및 Secure Web)
- 23.8.2(Android 용 Secure Mail)

Citrix 에서는 이전 두 버전의 모바일 생산성 앱의 업그레이드를 지원합니다. 모바일 생산성 앱의 이전 두 버전은 다음과 같습니다.

- 23.8.1(Android 용 Secure Mail)
- 23.8.0(Android 용 Secure Web)
- 23.7.0(Android 용 Secure Mail, iOS 용 Secure Mail)
- 23.5.0(iOS 용 Secure Mail 및 Android 용 Secure Web)
- 23.2.0(iOS 용 Secure Web)
- 22.9.1(iOS 용 Secure Web)

> 중요:
>
> MDX 암호화는 2020 년 9 월 1 일에 EOL(수명 종료) 에 도달했습니다. 레거시 장치 관리 (DA) 에 등록된 장치의 경우:
>
> - MDX 암호화를 사용하지 않는 경우 별도의 조치가 필요하지 않습니다.
> - MDX 암호화를 사용하는 경우 Android 장치를 Android Enterprise 로 마이그레이션합니다. Android 10 을 실행하는 장치는 Android Enterprise 를 사용하여 등록하거나 재등록해야 합니다. 여기에는 MAM 전용 모드의 Android 장치가 포함됩니다. 자세한 내용은 Android Enterprise 로 장치 관리 마이그레이션을 참조하십시오.

지원되는 운영 체제

모바일 생산성 앱은 다음 운영 체제를 지원합니다.

제품 이름	운영 체제	최소 배포 버전	최신 버전 사용 가능
Secure Hub	Android	7.x	14.x
	iOS	12.x	17.x
Secure Mail	Android	8.x	14.x
	iOS	13.x	17.x
Secure Web	Android	8.x	14.x
	iOS	13.x	17.x

모바일 생산성 앱의 최신 버전은 Citrix Endpoint Management 의 최신 버전 및 두 이전 버전과 호환됩니다. Citrix Endpoint Management 에서 지원하는 운영 체제에 대한 자세한 내용은 지원되는 장치 운영 체제를 참조하십시오.

최신 버전의 모바일 생산성 앱에는 최신 버전의 Secure Hub 가 필요합니다. Secure Hub 를 최신 상태로 유지해야 합니다.

> 참고:
>
> Citrix 는 항상 Android 및 iOS 운영 체제의 최신 버전과 이전 두 버전 (N, N-1 및 N-2) 만 지원합니다.

기타 고려 사항 및 제한 사항

단계적으로 중단되는 Citrix Endpoint Management 기능에 대한 사전 알림은 사용 중단을 참조하십시오.

Secure Mail

- Endpoint Management 는 STA(Secure Ticket Authority) 및 Secure Mail 의 문제로 인해 현재 NetScaler 12.0.41.16 을 지원하지 않습니다. 이 문제는 NetScaler 12.0 빌드 41.22 에서 수정되었습니다.
- Exchange 2007 용 Secure Mail 및 Lotus Notes 8.5.3 에 대한 지원이 2017 년 9 월 30 일에 EOL(수명 종료) 상태에 도달했습니다.
- Citrix Files 첨부 파일 보내기에서 최상의 성능을 얻으려면 Citrix Files 최신 버전을 사용하는 것이 좋습니다. Windows 에서는 Citrix Files 가 지원되지 않습니다.
- IBM Notes 환경에서는 IBM Domino Traveler 서버 버전 9.0 을 구성해야 합니다. 자세한 내용은 Exchange Server 또는 IBM Notes Traveler 서버 통합을 참조하십시오.

> 참고:
>
> - XenMobile 용 Citrix Files 는 2023 년 7 월 1 일에 EOL 에 도달했습니다. 자세한 내용은 EOL 및 더 이상 사용되지 않는 앱을 참조하십시오.

Secure Web

장치에 최신 버전의 Android WebView 를 설치합니다. 사용자는 Google Play Store 에서 Android WebView 를 다운로드할 수 있습니다.

QuickEdit

QuickEdit 는 계속해서 모바일 생산성 앱으로 제공됩니다. 이전에 알려드린 대로 EOL(수명 종료) 상태는 2018 년 9 월 1 일에 적용되지 않습니다.

Citrix Content Collaboration for Endpoint Management

버전 6.5 이후에는 공용 앱 스토어에서 Citrix Content Collaboration for Endpoint Management 에 액세스합니다.

ShareConnect

ShareConnect 는 2020 년 6 월 30 일에 EOL(수명 종료) 에 도달했습니다. 자세한 내용은 EOL 및 사용되지 않는 앱을 참조하십시오.

Citrix Secure Notes 및 Citrix Secure Tasks

Citrix Secure Notes 및 Citrix Secure Tasks 는 2018 년 12 월 31 일에 EOL(수명 종료) 상태에 도달했습니다. 자세한 내용은 EOL 및 사용되지 않는 앱을 참조하십시오.

관리자 작업 및 고려 사항

September 4, 2024

이 문서에서는 모바일 생산성 앱의 관리자와 관련된 작업 및 고려 사항에 대해 설명합니다.

기능 플래그 관리

운영 중인 모바일 생산성 앱에서 문제가 발생하는 경우 Citrix 에서 앱 코드 내에서 영향을 받는 기능을 사용하지 않도록 설정할 수 있습니다. Citrix 에서 iOS 및 Android 용 Secure Hub, Secure Mail 및 Secure Web 에 대한 기능을 사용하지 않도록 설정할 수 있습니다. 이를 위해 Citrix 에서는 기능 플래그와 LaunchDarkly 라는 타사 서비스를 사용하고 있습니다. LaunchDarkly 로의 트래픽을 사용하도록 설정하기 위해 별도의 구성은 필요 없습니다. 단, 방화벽이나 프록시로 아웃바운드 트래픽을 차단하는 경우에는 별도의 구성이 필요합니다. 위의 두 가지 경우에는 정책 요구 사항에 따라 특정 URL 이나 IP 주소를 통해 LaunchDarkly 로의 트래픽을 사용하도록 설정해야 합니다. 터널링에서 도메인의 제외를 지원하는 데 대한 자세한 내용은 MAM SDK 설명서를 참조하십시오.

다음과 같은 방법으로 LaunchDarkly 로의 트래픽 및 통신을 사용하도록 설정할 수 있습니다.

다음 **URL** 에 대한 트래픽을 사용하도록 설정

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

도메인별 허용 목록 만들기

이전에는 내부 정책에 IP 주소만 나열하면 되는 경우 사용할 수 있는 IP 주소 목록을 제공했습니다. 이제 Citrix 의 인프라 개선으로 인해 2018 년 7 월 16 일부터 공용 IP 주소가 제공되지 않습니다. 가능한 경우 도메인별 허용 목록을 만드는 것이 좋습니다.

허용 목록에 **IP** 주소 나열

화이트리스트에 IP 주소를 나열해야 하는 경우 현재의 모든 IP 주소 범위 목록은 이 LaunchDarkly 공용 IP 목록을 참조하십시오. 이 목록을 사용하면 인프라 업데이트에 따라 방화벽 구성을 자동으로 업데이트할 수 있습니다. 인프라 변경 상태에 대한 자세한 내용은 LaunchDarkly Statuspage를 참조하십시오.

> 참고:
>
> 공용 앱 스토어 앱은 처음 배포할 때 새로 설치해야 합니다. 앱의 현재 엔터프라이즈 래핑된 버전에서 공용 스토어 버전으로 업그레이드할 수는 없습니다.
>
> 공용 앱 스토어 배포의 경우, Citrix 가 개발한 앱을 더 이상 MDX Toolkit 으로 서명하고 래핑하지 않습니다. 타사 또는 엔터프라이즈 앱은 MDX Toolkit 을 사용하여 래핑할 수 있습니다.

LaunchDarkly 시스템 요구 사항

- Endpoint Management 10.7 이상.
- Citrix ADC 에서 분할 터널링이 꺼짐으로 설정되어 있는 경우 앱이 다음 서비스와 통신 가능한지 확인하십시오.
  - LaunchDarkly 서비스
  - APNs 수신기 서비스

지원되는 앱 스토어

모바일 생산성 앱은 Apple App Store 및 Google Play 에서 구할 수 있습니다.

Google Play 를 이용할 수 없는 중국에서는 다음 앱 스토어에서 Android 용 Secure Hub 를 구할 수 있습니다.

- https://shouji.baidu.com
- http://apk.hiapk.com
- https://apk.91.com

공용 앱 스토어 배포 사용

1. iOS 및 Android 용 공용 스토어 .mdx 파일을 Endpoint Management 다운로드 페이지에서 다운로드합니다.
2. Endpoint Management 콘솔에.mdx 파일을 업로드합니다. 모바일 생산성 앱의 공용 스토어 버전은 여전히 MDX 응용 프로그램으로 업로드되므로 서버에 공용 스토어 앱으로 앱을 업로드하지 마십시오. 단계를 보려면 앱 추가를 참조하십시오.
3. 보안 정책에 기반하여 정책을 기본값에서 변경합니다 (선택 사항).
4. 앱을 필수 앱으로 푸시합니다 (선택 사항). 이 단계를 사용하려면 모바일 기기 관리를 사용하도록 환경을 설정해야 합니다.
5. 장치에 App Store, Google Play 또는 Endpoint Management 앱 스토어의 앱을 설치합니다.

- Android 장치의 경우 앱을 설치하도록 사용자가 Play Store 으로 이동됩니다. iOS 장치에서는 MDM 이 포함된 배포인 경우 사용자가 앱 스토어로 이동하지 않고 앱이 설치됩니다.
- App Store 또는 Play Store 에서 앱을 설치하는 경우 다음 작업이 수행됩니다. 해당하는.mdx 파일이 서버에 업로드되면 앱이 관리되는 앱으로 전환됩니다. 관리되는 앱으로 전환될 때 앱에서 Citrix PIN 을 묻는 메시지가 표시됩니다. 사용자가 Citrix PIN 을 입력하면 Secure Mail 에 계정 구성 화면이 표시됩니다.

6. Secure Hub 에 등록되어 있고 해당하는.mdx 파일이 서버에 있는 경우에만 앱에 액세스할 수 있습니다. 조건 중 어느 한 쪽이 충족되지 않아도 사용자가 앱을 설치할 수 있지만 앱 사용이 차단됩니다.

현재 공용 앱 스토어에 있는 Citrix Ready Marketplace 의 앱을 사용하고 있는 경우, 이미 익숙한 배포 프로세스가 진행됩니다. 모바일 생산성 앱에는 여러 ISV 가 현재 사용하는 것과 동일한 접근 방법이 사용됩니다. MDX SDK 를 앱 내에 포함시켜 앱을 공용 스토어에서 사용 가능하도록 준비합니다.

> 참고:
>
> iOS 및 Android 용 Citrix Files 앱의 공용 스토어 버전은 이제 범용이므로, 스마트폰 및 태블릿용 Citrix Files 앱이 동일합니다.

Apple 푸시 알림

푸시 알림 구성에 대한 자세한 내용은 푸시 알림을 사용하도록 Secure Mail 구성을 참조하십시오.

공용 앱 스토어 **FAQ**

- 서로 다른 사용자 그룹에 공용 스토어 앱의 여러 복사본을 배포할 수 있습니까? 가령 서로 다른 사용자 그룹에 서로 다른 정책을 배포하고 싶습니다.

  각 사용자 그룹에 대해 서로 다른.mdx 파일을 업로드합니다. 그러나 이 경우 단일 사용자가 여러 그룹에 속할 수는 없습니다. 사용자가 여러 그룹에 속한 경우 동일한 앱의 복사본 여러 개가 해당 사용자에게 할당됩니다. 앱 ID 는 변경할 수 없으므로 공용 스토어 앱의 여러 복사본을 동일한 장치에 배포할 수 없습니다.

- 공용 스토어 앱을 필수 앱으로 푸시할 수 있습니까?

  예. 앱을 장치로 푸시하려면 MDM 이 필요합니다. MAM 전용 배포에 대해서는 지원되지 않습니다.

- 사용자 에이전트 기반의 트래픽 정책 또는 Exchange Server 규칙을 업데이트해야 합니까?

  다음은 플랫폼별 사용자 에이전트 기반 정책 및 규칙에 해당하는 문자열입니다.

  > 중요:
  >
  > Secure Notes 및 Secure Tasks 는 2018 년 12 월 31 일에 EOL(수명 종료) 상태에 도달했습니다. 자세한 내용은 EOL 및 사용되지 않는 앱을 참조하십시오.

Android

앱	서버	사용자-에이전트 문자열
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		WorxMail
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

앱	서버	사용자-에이전트 문자열
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- 앱이 업그레이드되지 않게 할 수 있습니까?

  아니요. 업그레이드가 공용 앱 스토어에 게시되면 자동 업데이트 사용이 설정된 모든 사용자가 업데이트를 받게 됩니다.

- 앱 업그레이드를 적용할 수 있습니까?

  예. 업그레이드는 업그레이드 유예 기간 정책을 통해 적용됩니다. 이 정책은 업데이트된 앱 버전에 상응하는 새.mdx 파일이 Endpoint Management 로 업로드될 때 설정됩니다.

- 업데이트 일정을 통제할 수 없는 경우 업데이트가 사용자에게 도달하기 전에 앱을 테스트하려면 어떻게 해야 합니까?

  Secure Hub 의 프로세스와 유사하게, EAR 기간 동안 iOS 용 TestFlight 에서 앱을 테스트할 수 있습니다. Android 의 경우, EAR 기간 동안 Google Play 베타 프로그램을 통해 앱을 사용할 수 있습니다. 이 기간 중에 앱 업데이트를 테스트할 수 있습니다.

- 자동 업데이트가 사용자 장치에 도달하기 전에 새.mdx 파일을 업데이트하지 않으면 어떻게 됩니까?

  업데이트된 앱은 이전.mdx 파일과 계속 호환됩니다. 새 정책이 적용되는 새로운 기능은 사용할 수 없습니다.

- Secure Hub 가 설치되어 있으면 앱이 관리되는 앱으로 전환됩니까, 아니면 앱을 등록해야 합니까?

  공용 스토어 앱이 관리되는 앱 (MDX 에 의해 보안됨) 으로 활성화되고 사용 가능해지려면 사용자가 Secure Hub 에 등록되어야 합니다. Secure Hub 가 설치되어 있지만 등록되지 않은 사용자는 공용 스토어 앱을 사용할 수 없습니다.

- 공용 스토어 앱을 위해 Apple Enterprise 개발자 계정이 필요합니까?

  아니요. 이제 Citrix 가 모바일 생산성 앱의 인증서와 프로비전 프로필을 유지 관리하므로 앱을 사용자에게 배포하기 위해 Apple Enterprise 개발자 계정이 필요하지 않습니다.

- 배포한 모든 래핑된 응용 프로그램에 엔터프라이즈 배포 종료가 적용됩니까?

  아니요. 모바일 생산성 앱, 즉 Secure Mail, Secure Web 및 Citrix Content Collaboration for Endpoint Management, QuickEdit 및 ShareConnect 에만 적용됩니다. 자체적으로 또는 타사를 통해 개발하여 배포한 모든 엔터프라이즈 래핑된 앱은 계속 엔터프라이즈 래핑을 사용할 수 있습니다. MDX Toolkit 은 앱 개발자를 위해 엔터프라이즈 래핑을 계속 지원합니다.

- Google Play 에서 앱을 설치할 때 오류 코드가 505 인 Android 오류가 발생합니다.

  > 참고:
  >
  > Android 5.x 에 대한 지원은 2018 년 12 월 31 일에 종료되었습니다.

  이는 Google Play 및 Android 5.x 버전의 알려진 문제입니다. 이 오류가 발생하는 경우 장치에서 앱 설치를 막는 오래된 데이터를 몇 가지 단계를 거쳐 삭제할 수 있습니다.

1. 장치를 재시작합니다.
2. 장치 설정을 통해 Google Play 관련 캐시 및 데이터를 지웁니다.
3. 최후의 수단으로 장치에서 Google 계정을 제거했다가 다시 추가합니다.

자세한 내용을 보려면 “Fix Google Play Store Error 505 in Android: Unknown Error Code” 키워드를 사용하여 이 사이트를 검색하십시오.

- Google Play 의 앱이 프로덕션 환경으로 릴리스되었고 사용할 수 있는 새 베타 릴리스가 없는 경우에도 Google Play 에서 앱 제목 뒤에 Beta 가 표시되는 이유는 무엇입니까?

  EAR(Early Access Release) 프로그램에 참여하고 있는 경우 앱 제목 옆에 Beta 가 항상 표시됩니다. 이 이름은 단순히 특정 앱에 대한 사용자의 액세스 수준을 사용자에게 알려줍니다. Beta 라는 이름은 사용자가 앱의 사용 가능한 최신 버전을 받는다는 의미입니다. 최신 버전이란 프로덕션 트랙에 게시된 최신 버전이거나 베타 트랙에 게시된 최신 버전일 수 있습니다.

- 앱을 설치하고 연 후에.mdx 파일이 Endpoint Management 콘솔에 있는 경우에도 사용자에게 권한이 부여되지 않은 앱이라는 메시지가 표시됩니다.

  이 문제는 사용자가 App Store 또는 Google Play 에서 앱을 직접 설치하고 Secure Hub 가 새로 고쳐지지 않은 경우에 발생할 수 있습니다. 비활성 타이머가 만료되면 Secure Hub 를 새로 고쳐야 합니다. 사용자가 Secure Hub 를 열고 재인증하면 정책이 새로 고쳐집니다. 다음에 사용자가 앱을 열 때 앱 권한이 부여됩니다.

- 앱을 사용하려면 액세스 코드가 필요합니까? App Store 또는 Play Store 에서 앱을 설치할 때 액세스 코드를 입력하라는 메시지를 표시하는 화면이 나타납니다.

  액세스 코드를 요청하는 화면이 표시되는 경우 Secure Hub 를 통해 Endpoint Management 에 등록하지 않은 것입니다. Secure Hub 로 등록한 후 앱의.mdx 파일이 서버에 배포되어 있는지 확인하십시오. 또한 앱을 사용할 수 있는지 확인해야 합니다. 액세스 코드는 Citrix 내부 용도로만 제한됩니다. 앱을 사용하려면 Endpoint Management 배포를 활성화해야 합니다.

- VPP 또는 DEP 를 통해 iOS 공용 스토어 앱을 배포할 수 있습니까?

  Endpoint Management 는 MDX 가 사용 설정되지 않은 공용 스토어 앱의 VPP 배포용으로 최적화되었습니다. Endpoint Management 공용 스토어 앱을 VPP 로 배포할 수는 있지만 Endpoint Management 와 Secure Hub 저장소를 향상하여 제한 사항을 처리해야만 배포가 최적화됩니다. VPP 를 통한 Endpoint Management 공용 스토어 앱 배포와 관련된 알려진 문제 및 가능한 해결 방법의 목록은 Citrix Knowledge Center의 이 문서를 참조하십시오.

모바일 생산성 앱의 **MDX** 정책

MDX 정책을 사용하여 Endpoint Management 가 적용할 설정을 구성할 수 있습니다. 이 정책에는 인증, 장치 보안, 네트워크 요구 사항과 액세스 권한, 암호화, 앱 상호 작용, 앱 제한 등이 포함됩니다. 대부분의 MDX 정책이 모든 모바일 생산성 앱에 적용되지만, 일부 정책은 특정 앱에만 적용됩니다.

정책 파일은 모바일 생산성 앱의 공용 스토어 버전에 해당하는.mdx 파일로 제공됩니다. 또한 앱을 추가할 때 Endpoint Management 콘솔에서 정책을 구성할 수도 있습니다.

MDX 정책에 대한 자세한 설명은 이 섹션에서 다음 문서를 참조하십시오.

- 모바일 생산성 앱의 MDX 정책 요약
- Android 용 모바일 생산성 앱의 MDX 정책
- iOS 용 모바일 생산성 앱의 MDX 정책

다음 섹션에서는 사용자 연결과 관련된 MDX 정책에 대해 설명합니다.

Android 용 **Secure Mail** 의 듀얼 모드

MAM(모바일 애플리케이션 관리) SDK 를 사용하여 iOS 및 Android 플랫폼에서 제공되지 않는 MDX 기능의 영역을 대체할 수 있습니다. MDX 래핑 기술은 2021 년 9 월에 EOL(수명 종료) 에 도달할 예정입니다. 엔터프라이즈 응용 프로그램을 계속 관리하려면 MAM SDK 를 포함해야 합니다.

버전 20.8.0 에서 Android 앱은 앞서 언급한 MDX EOL 전략에 대비하기 위해 MDX 및 MAM SDK 가 포함된 상태로 릴리스됩니다. MDX 듀얼 모드는 현재 MDX Toolkit 에서 새 MAM SDK 로의 전환 경로를 제공하기 위한 것입니다. 듀얼 모드를 사용하면 다음과 같은 작업이 가능해집니다.

- MDX Toolkit(이제 Endpoint Management 콘솔에서는 레거시 MDX 라고 함) 을 사용한 지속적인 앱 관리

- 새 MAM SDK 를 통합하는 앱을 관리합니다.

  > 참고:
  >
  > MAM SDK 를 사용하는 경우 앱을 래핑할 필요가 없습니다.

MAM SDK 로 전환한 후에는 추가 단계가 필요하지 않습니다.

MAM SDK 에 대한 자세한 내용은 다음 문서를 참조하십시오.

- MAM SDK Overview(MAM SDK 개요)
- MAM SDK 의 최신 릴리스
- 장치 관리에 대한 Citrix Developer 섹션
- Citrix 블로그 게시물

사전 요구 사항

듀얼 모드 기능을 성공적으로 배포하려면 다음을 확인하십시오.

- Citrix Endpoint Management 를 버전 10.12 RP2 이상 또는 10.11 RP5 이상으로 업데이트합니다.
- 모바일 앱을 버전 20.8.0 이상으로 업데이트합니다.
- 정책 파일을 버전 20.8.0 이상으로 업데이트합니다.
- 조직에서 타사 앱을 사용하는 경우 Citrix 모바일 생산성 앱에 대한 MAM SDK 옵션으로 전환하기 전에 MAM SDK 를 타사 앱에 통합해야 합니다. 관리되는 모든 앱을 한 번에 MAM SDK 로 이동해야 합니다.

> 참고:
>
> MAM SDK 는 모든 클라우드 기반 고객에 대해 지원됩니다.

제한 사항

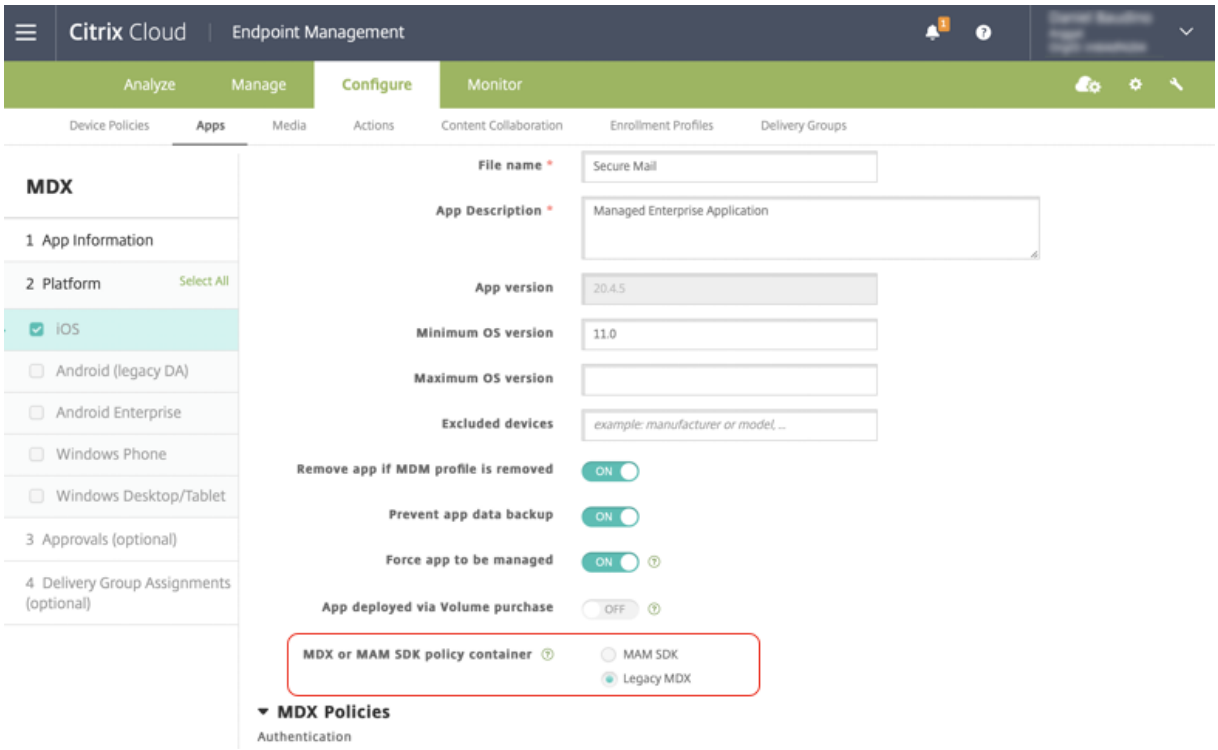
- MAM SDK 는 Citrix Endpoint Management 배포의 Android Enterprise 플랫폼에 게시된 앱만 지원합니다. 새로 게시된 앱의 경우 플랫폼 기반 암호화가 기본 암호화입니다.
- MAM SDK 는 MDX 암호화가 아닌 플랫폼 기반 암호화만 지원합니다.
- Citrix Endpoint Management 를 업데이트하지 않고 버전 20.8.0 이상에서 모바일 앱에 대해 정책 파일을 실행하면 Secure Mail 에 대한 네트워킹 정책의 중복 항목이 만들어집니다.

Citrix Endpoint Management 에서 Secure Mail 을 구성할 때 듀얼 모드 기능을 사용하면 MDX Toolkit(현재의 레거시 MDX) 을 사용하여 계속해서 앱을 관리하거나 새로운 MAM SDK 로 전환하여 앱을 관리할 수 있습니다. MAM SDK 는 모듈식이므로 조직에서 사용하는 MDX 기능의 하위 집합만 사용할 수 있습니다. 따라서 Citrix 에서는 MAM SDK 로 전환하도록 권장합니다.

MDX 또는 **MAM SDK** 정책 컨테이너에서 다음과 같은 정책 설정 옵션을 사용할 수 있습니다.

- **MAM SDK**

- 레거시 **MDX**



MDX 또는 **MAM SDK** 정책 컨테이너 정책에서는 레거시 **MDX** 에서 **MAM SDK** 로만 옵션을 변경할 수 있습니다. **MAM SDK** 에서 레거시 **MDX** 로 전환하는 옵션은 허용되지 않으며 앱을 다시 게시해야 합니다. 기본값은 레거시 **MDX** 입니다. 동일한 장치에서 실행되는 Secure Mail 과 Secure Web 모두에 대해 동일한 정책 모드를 설정해야 합니다. 동일한 장치에서 두 개의 서로 다른 모드를 실행할 수 없습니다.

내부 네트워크로의 사용자 연결

내부 네트워크에 터널링되는 연결에서는 전체 VPN 터널을 사용하거나, 터널링됨-웹 SSO 라고 하는 클라이언트 없는 VPN 의 변형을 사용할 수 있습니다. 해당 동작은 기본 설정 VPN 모드 정책에 의해 제어됩니다. 기본적으로 연결 시 SSO 를 필요로 하는 연결에 대해 권장되는 터널링됨-웹 SSO 를 사용합니다. 클라이언트 인증서 또는 종단 간 SSL 을 사용하여 내부 네트워크의 리소스로 연결되는 경우 전체 VPN 터널 설정을 사용하는 것이 좋습니다. 이 설정은 TCP 기반의 모든 프로토콜을 처리하고, Windows 및 Mac 컴퓨터뿐 아니라 iOS 및 Android 장치에서도 사용될 수 있습니다.

VPN 모드 전환 허용 정책은 필요에 따라 전체 VPN 터널 모드와 터널링됨 - 웹 SSO 모드 간의 자동 전환을 허용합니다. 기본적으로 이 정책은 꺼져 있습니다. 이 정책이 켜진 경우, 기본 설정 VPN 모드에서 처리할 수 없는 인증 요청으로 인해 실패한 네트워크 요청은 다른 모드에서 다시 시도됩니다. 예를 들어 클라이언트 인증서에 대한 서버 챌린지는 전체 VPN 터널 모드에서 수용될 수 있지만 터널링됨 - 웹 SSO 모드에서는 수용될 수 없습니다. 마찬가지로 HTTP 인증 챌린지는 터널링됨 - 웹 SSO 모드를 사용할 경우에 SSO 로 더 쉽게 서비스될 수 있습니다.

네트워크 액세스 제한

네트워크 액세스 정책은 네트워크 액세스에 대한 제한이 적용되는지 여부를 지정합니다. 기본적으로 Secure Mail 액세스는 제한되지 않으므로 네트워크 액세스에 대한 제한이 적용되지 않습니다. 앱은 장치가 연결된 네트워크에 제한 없이 액세스할 수 있습니다. 기본적으로 Secure Web 액세스는 내부 네트워크로 터널링되므로 내부 네트워크로의 응용 프로그램별 VPN 터널이 모든 네트워크 액세스에 사용되고 Citrix ADC 분할 터널링 설정이 사용됩니다. 또한 장치에 네트워크 연결이 없는 것처럼 앱이 작동하도록 차단된 액세스를 지정할 수도 있습니다.

AirPrint, iCloud, Facebook 및 Twitter API 등의 기능을 허용하려는 경우 네트워크 액세스 정책을 차단하지 마십시오.

네트워크 액세스 정책은 백그라운드 네트워크 서비스 정책과 상호 작용합니다. 자세한 내용은 Exchange Server 또는 IBM Notes Traveler 서버 통합을 참조하십시오.

Endpoint Management 클라이언트 속성

클라이언트 속성은 사용자 장치에서 Secure Hub 에 직접 제공되는 정보를 포함합니다. 클라이언트 속성은 Endpoint Management 콘솔에서 설정 **>** 클라이언트 **>** 클라이언트 속성에 있습니다.

클라이언트 속성은 다음과 같은 설정을 구성하는 데 사용됩니다.

사용자 암호 캐싱

사용자 암호 캐싱은 사용자의 Active Directory 암호가 모바일 장치에 로컬로 캐싱될 수 있게 합니다. 사용자 암호 캐싱이 사용되도록 설정하면 Citrix PIN 또는 암호를 설정하라는 메시지가 사용자에게 표시됩니다.

비활성화 타이머

비활성화 타이머는 사용자가 장치를 비활성 상태로 둔 후에 Citrix PIN 또는 암호를 입력하라는 메시지 없이 앱에 액세스할 수 있는 시간 (분 단위) 을 정의합니다. MDX 앱에 대해 이 설정을 사용되도록 설정하려면 앱 암호 정책을 켜짐으로 설정해야 합니다. 앱 암호 정책이 꺼짐인 경우, 사용자는 전체 인증을 수행하기 위해 Secure Hub 로 리디렉션됩니다. 이 설정을 변경하면 다음에 사용자에게 인증하라는 메시지가 표시될 때 값이 적용됩니다.

Citrix PIN 인증

Citrix PIN 은 사용자 인증 환경을 간소화합니다. PIN 은 클라이언트 인증서를 보안하거나 Active Directory 자격 증명을 장치에 로컬로 저장하는 데 사용됩니다. PIN 설정을 구성한 경우 사용자 로그온 환경은 다음과 같습니다.

1. 사용자가 처음으로 Secure Hub 를 시작하면 PIN 을 입력하라는 메시지가 사용자에게 표시되고, Active Directory 자격 증명이 캐싱됩니다.
2. 다음번에 사용자가 Secure Mail 과 같은 모바일 생산성 앱을 시작할 때 사용자는 PIN 을 입력하고 로그온합니다.

클라이언트 속성을 사용하여 PIN 인증이 사용되도록 설정하고 PIN 유형을 지정하고 PIN 강도, 길이를 지정하고 요구 사항을 변경합니다.

지문 또는 **Touch ID** 인증

iOS 장치의 지문 인증 (Touch ID 인증이라고도 함) 은 Citrix PIN 의 대안 기능으로, Secure Hub 를 제외한 래핑된 앱이 비활성화 타이머가 만료되는 등의 상황에서 오프라인 인증을 필요로 할 경우에 유용합니다. 다음과 같은 인증 시나리오에서 이 기능이 사용되도록 설정할 수 있습니다.

- Citrix PIN + 클라이언트 인증서 구성
- Citrix PIN + 캐싱된 AD 암호 구성
- Citrix PIN + 클라이언트 인증서 구성 및 캐싱된 AD 암호 구성
- Citrix PIN 이 꺼짐

지문 인증이 실패하거나 사용자가 지문 인증 프롬프트를 취소하면 래핑된 앱이 Citrix PIN 또는 AD 암호 인증으로 폴백됩니다.

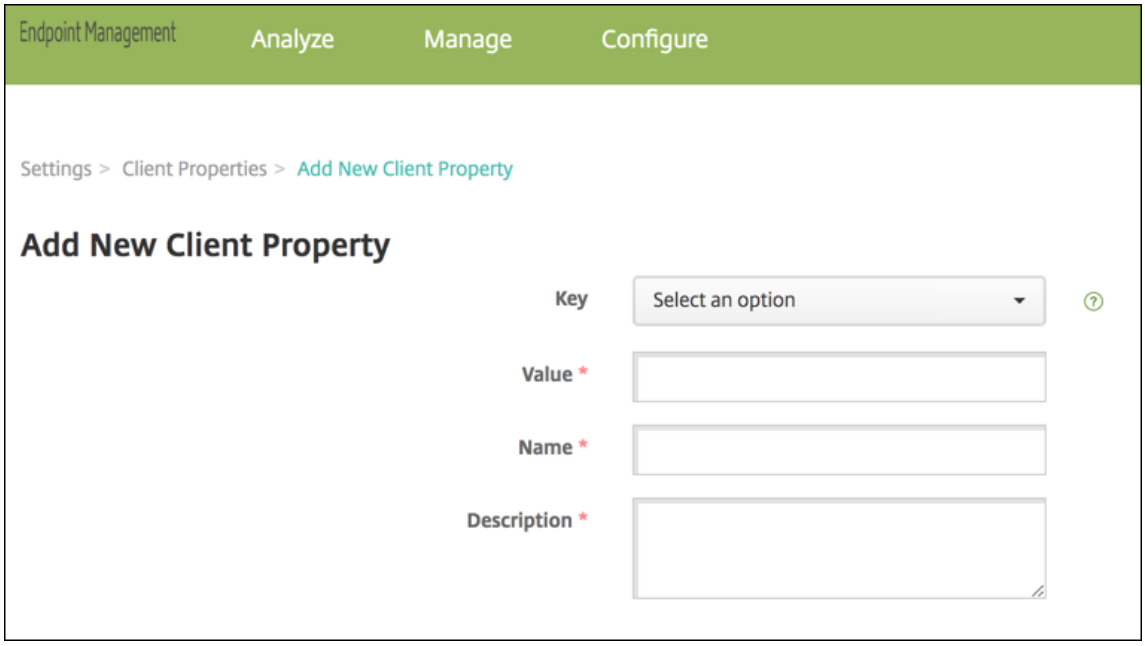
지문 인증 요구 사항

- 지문 인증을 지원하고 최소 1 개의 지문이 구성되어 있는 iOS 장치 (버전 8.1 이상).
- 사용자 엔트로피가 꺼져 있어야 합니다.

지문 인증을 구성하려면

> 중요:
>
> 사용자 엔트로피가 켜져 있으면 Touch ID 인증 사용 속성이 무시됩니다. 사용자 엔트로피는 Encrypt secrets using Passcode key(암호 키를 사용한 암호 암호화) 를 통해 사용 설정합니다.

1. Endpoint Management 콘솔에서 설정 **>** 클라이언트 **>** 클라이언트 속성으로 이동합니다.
2. 추가를 클릭합니다.



3. **ENABLE_TOUCH_ID_AUTH** 키를 추가하고 값을 **True** 로 설정하고 정책 이름을 **Enable Touch Fingerprint Authentication(**지문 인증 사용 설정**)** 으로 지정합니다.

지문 인증을 구성한 후에 사용자가 장치를 다시 등록할 필요가 없습니다.

암호 코드 키 및 클라이언트 속성을 사용한 암호화 암호에 대한 자세한 내용은 Endpoint Management 문서의 클라이언트 속성을 참조하십시오.

Google Analytics

Citrix Secure Mail 은 제품 품질을 개선하기 위해 Google Analytics 를 사용하여 앱 통계 및 사용 정보 분석 데이터를 수집합니다. Citrix 는 다른 개인 사용자 정보를 수집하거나 저장하지 않습니다.

Google Analytics 비활성화

관리자는 사용자 지정 클라이언트 속성 **DISABLE_GA** 를 구성하여 Google Analytics 를 비활성화할 수 있습니다. Google Analytics 를 비활성화하려면 다음을 수행합니다.

1. Citrix Endpoint Management 콘솔에 로그인하고 설정 > 클라이언트 속성 > 새 클라이언트 속성 추가로 이동합니다.
2. 키 필드에 **DISABLE_GA** 값을 추가합니다.
3. 클라이언트 속성의 값을 **true** 로 설정합니다.

> 참고:
>
> Citrix Endpoint Management 콘솔에서 **DISABLE_GA** 값을 구성하지 않으면 Google Analytics 데이터가 활

> 성화됩니다.

플랫폼별 기능

June 6, 2024

다음 표에는 Citrix 모바일 생산성 앱의 기능이 요약되어 있습니다. **X** 는 해당 플랫폼에서 기능을 사용할 수 있음을 나타냅니다. QuickEdit 에서의 기능은 Citrix QuickEdit를 참조하십시오.

Citrix Secure Hub

기능	iOS	Android
인증을 위한 로그온	X	X
정책 준수 모니터링	X	X
앱 및 데스크톱 액세스	X	X
HDX 앱 및 데스크톱	X	X
문제 로그 생성 및 보내기	X	X
로그에 스크린샷 첨부	X	X
앱 내에서 지원 센터에 연락	X	X
앱 내에서 Citrix 지원 팀에 연락	X	X
충돌 수집 및 분석	X	X
오프라인 인증	X	X
Citrix Secure Mail 을 통해 로그 보내기	X	X
Google Analytics	X	X
세로 및 가로 모드	X	X
앱 신뢰를 위한 앱 내 가이드	X	X
전자 메일로 등록한 경우 Secure Mail 에 자동 등록 (MAM 만 해당)	X	X
Touch ID 오프라인 인증	X	X
파생된 자격 증명으로 등록	X	
생체 인증		X

기능	iOS	Android
Workspace 앱 스토어 사용	X	X

Citrix Secure Mail

기능	iOS	Android
전자 메일 생산성		
임시 보관함 최소화	X	X
보낸 메일 실행 취소		X
암호화 관리	X	X
일정 목록에 대한 위젯		X
Secure Mail 의 연락처 사진	X	X
반응형 전자 메일 지원	X	X
임시 보관함 폴더 자동 동기화	X	X
임시 보관함 폴더에서 첨부 파일 동기화		X
전자 메일 보내기, 받기, 회신, 모두 회신, 전달	X	X
초안 만들기, 편집, 삭제	X	X
메일에 플래그 지정	X	X
읽지 않음으로 표시	X	X
모든 폴더 및 하위 폴더 보기	X	X
앱이 백그라운드로 전환될 때 초안 자동 저장	X	X
Citrix Secure Notes 로 전자 메일을 메모로 변환. 중요**:** Secure Notes 는 2018 년 12 월 31 일에 EOL(수명 종료) 상태에 도달했습니다. 자세한 내용은 EOL 및 사용되지 않는 앱을 참조하십시오.	X	X
메일 검색 (로컬 및 서버)	X	X
메일 동기화 기간 선택 (최대 1 개월 또는 모든 메일)	X	X

기능	iOS	Android
읽지 않은 메일 보기	X	X
보안 첨부 파일 이미지, 비디오 및 오디오 보기/재생	X	X
다중 첨부 파일	X	X
첨부 파일 회신 및 전달	X	X
Citrix Files 에서 파일 첨부	X	X
Citrix Files 제한된 영역 및 커넥터로부터 파일 첨부	X	X
첨부 파일 저장소	X	X
서식 있는 텍스트 편집	X	X
제목, 잠금 화면 미리 보기가 포함된 메일 알림	X	X
알림 화면에서 메일 및 초대에 회신 및 삭제	X	
사진 첨부 또는 촬영	X	X
다중 메시지 선택	X	X
첨부 파일 다운로드	X	X
이미지 인라인 로드	X	X
빠른 정렬	X	X
.zip 첨부 파일 보내기, 받기, 열기 및 저장	X	X
세로 및 가로 모드	X: 메일 목록, 메일 읽기, 작성, 일정 및 연락처 보기 전반	X: 메일 읽기 및 작성 보기만
붙여 넣은 텍스트에서 서식 유지	X	X
연락처에서 보낸 SMS	X	X
연락처에서 보낸 FaceTime	X	
연결 문제 또는 가득 찬 사서함으로 인해 보내지지 않은 메시지를 보낼 편지함에 보관	X	X
최근 폴더 버블업		X
아래로 당겨 메일 새로 고침	X	X
마지막 새로 고침 타임스탬프	X	X

기능	iOS	Android
왼쪽으로 살짝 밀어 메시지 작업	X	X
Microsoft Exchange 및 IBM Notes Traveler 지원	X	X
눌러서 메일, 일정 및 연락처 새로 고침	X	X
장치 접근성/글꼴 크기 설정을 메일 보기에서 유지	X	X
S/MIME 서명 및 암호화	X	X
전자 메일로 S/MIME 인증서 가져오기	X	X
S/MIME, Intercede 통합	X	
S/MIME, Entrust 통합	X	
메시지 본문에 대한 Microsoft IRM 보호	X	X
푸시 알림	X	X
받은 편지함으로 알림을 푸시하여 일정을 비롯한 모든 폴더를 자동으로 업데이트	X	
Office 365 문서 열기	X	X
3D Touch 동작	X	
잠금 화면에서 상황에 맞는 아이콘	X	X
폴더 검색	X	X
VIP 메일 폴더	X	X
동적 유형 지원	X	X
확장된 폴더 유지	X	X
메시지 분류 마커	X	X
맞춤법 검사	X	
마지막으로 찍은 사진 첨부	X	X
URL 미리 보기	X	X
Citrix Files 에서 Citrix Files 링크 열기	X	X
`.pass` 파일 지원	X	
검색 모드에서 여러 개의 전자 메일 선택	X	X
이미지 인라인 삽입	X	X

기능	iOS	Android
EAS(Exchange ActiveSync) 버전 16 으로 업그레이드	X	X
사용자가 알 수 없는 도메인 또는 개인 도메인을 사용하지 못하도록 제한	X	
슈퍼 와이드 장치 화면 지원		X
여러 Exchange 계정 구성	X	X
왼쪽 또는 오른쪽으로 살짝 밀어 자세히 작업	X	X
암호화된 메일의 회신 또는 전달 암호화	X	
전자 메일 및 인라인 이미지 인쇄	X	
설정에서 줄 미리 보기를 사용하여 사서함 보기에 미리 보기로 표시되는 전자 메일 본문의 줄 수 구성	X	
반응형 전자 메일 지원	X	X
첨부 파일의 앱 내 미리 보기 (MS Office 또는 이미지)	X	X
개인 연락처 그룹	X	X
전자 메일 주소 (UPN) 로 사용자 이름 마이그레이션	X	X
피싱 전자 메일 보고	X	X
최신 인증 (OAuth)	X	X
첨부 파일 인쇄	X	
Android Enterprise(Android for Work)	X	
서식 있는 텍스트 서명	X	
다양한 방식의 푸시 알림	X	
피드	X	X
사진 첨부 개선	X	X
그룹 알림	X	
Slack 통합 (미리 보기)	X	X
피드 관리	X	
내부 도메인	X	X

기능	iOS	Android
피드 관리	X	X
MS Teams 통합	X	X
자체 진단 (문제 해결) 옵션		X
듀얼 모드 (MAM SDK)	X	X
자가 진단 도구		X
일정		
ICS 파일 미리 보기 및 일정 이벤트로 가져오기		X
일정 이벤트 끌어서 놓기	X	X
일, 주, 월 및 일정 목록 보기	X	X
잠금 화면에서의 상세한 미리 알림	X	X
6 개월간 동기화	X	X
이벤트를 개인적인 것으로 설정	X	X
첫 번째 이벤트 이전 시간으로 스크롤	X	
수동 새로 고침 옵션	X	X
미리 알림 설정	X	X
눌러서 주소 매핑	X	X
주 번호	X	X
동적 유형 지원	X	X
보안 분류 마커	X	X
주소 길게 누르기	X	
주당 근무 시간 시작일 설정	X	X
선택한 날짜의 주에 초점 맞춰 보기	X	
현재 날짜가 항상 강조 표시됨	X	X
첨부 파일 저장소의 일정 첨부 파일	X	X
개인 일정 지원	X	X
개인 일정 이벤트와의 충돌 표시		X
일정 이벤트 인쇄	X	
일정 제목 줄의 전화 번호 및 웹 주소 누르기	X	

기능	iOS	Android
일정 검색	X	
모임		
모임 회신, 모두 회신, 전달	X	X
초대 응답에 대한 주최자 보기	X	X
초대 대상자의 상태 및 제안된 상태에 대한 주최자 보기	X	X
눌러서 온라인 모임에 참가 참고: WebEx 및 Lync 의 경우 Citrix Endpoint Management 에서 이러한 앱의 사용을 위한 정책을 구성해야 합니다.	X	X
눌러서 오디오 회의에 참가	X	X
새 초대에서 온라인 모임, 오디오, 회의 예약	X	X
새 초대에 ShareFile 링크 추가	X	X
첨부 파일을 포함하여 초대 전달	X	X
눌러서 “지각” 전자 메일 보내기	X	X
눌러서 모임 주최자에게 회신	X	X
눌러서 모든 모임 초대에 회신	X	X
눌러서 모든 모임 초대 대상자에게 회신	X	X
눌러서 모든 모임 초대 대상자에게 첨부 파일을 포함하여 회신	X	X
GoToMeeting 에 전화 접속	X	X
잠금 화면 또는 알림 화면에서 초대에 응답	X	X
WebEx 또는 Lync 모임에 전화 접속	X	X
거부된 이벤트 숨기기	X	X
동시 이벤트를 3 개 넘게 표시	X	X
초대 대상자 상태 빠른 보기	X	X
취소된 이벤트에 대한 설명 삭제, 회신, 모두 회신, 추가	X	X
전달된 초대장에 주최자 이름 표시	X	X

기능	iOS	Android
공유 장치	X	X
Skype for Business 모임 참가	X	X
수락, 거부 및 미정을 사용하여 회의 알림에 응답	X	X
회신 및 삭제를 사용하여 메시지 알림에 응답	X	
연락처		
연락처에 폴더 만들기		X
양방향 연락처 동기화	X	X
상세한 연락처 정보 GAL 검색	X	X
Secure Mail 연락처를 로컬 연락처로 내보내기 및 동기화	X	X
연락처: 즐겨찾기 및 범주		X
내보내지는 연락처 필드 제어	X	X
Secure Mail 이외의 연락처 세부 정보	X	X
동적 유형 지원	X	X
연락처를 VIP 로 표시	X	X
`.vcards`와 연락처 공유	X	X
길게 눌러 연락처 보기		X
기본 메일 계정이 있는 경우에도 연락처 내보내기	X	X
폴더 및 하위 폴더 보기	X	
장치에 구성된 설정		
iMessage 지원	X	
알림 제어를 위한 고급 옵션	X	X
잠금 화면 알림 제어	X	X
메일 및 일정 알림 사운드	X	X
폴더 자동 새로 고침	X	X
내부 및 외부 부재 중 알림	X	X
삭제 전 확인	X	X
스레드형 대화 또는 시간순 보기	X	X

기능	iOS	Android
Wi-Fi 에서 첨부 파일 로드	X	X
Wi-Fi 에서 첨부 파일 로드를 기본값으로 지정	X	X
메일 동기화 기간 설정	X	X
무제한 동기화/모든 메일 동기화		X
전자 메일 서명 설정	X	X
성 또는 이름 기준으로 연락처 나열	X	X
자동 진행	X	X
기본 표준 시간대 사용		X
빠른 응답 템플릿		X
메일 구성 푸시 빈도		X
설정 내보내기/가져오기	X	X
장치에서 뒤로 단추를 눌러 부동 작업 단추 옵션 해제		X
Microsoft Teams	X	X

Citrix Secure Web

기능	iOS	Android
멀티태스킹을 통해 두 개의 앱을 동시에 사용	X	
파일 다운로드	X	X
즐겨찾기 추가	X	X
저장된 사용자 이름 및 암호 지우기	X	X
캐시/기록/쿠키 삭제	X	X
팝업 차단	X	X
오프라인 페이지 저장	X	X
주소 표시줄에서 검색	X	X
알림에서 다운로드한 항목 열기	X	X
암호 자동 저장	X	X

기능	iOS	Android
프록시 지원		
엔터프라이즈 프록시	X	X
URL 차단 목록 및 허용 목록	X	X
기록	X	X
기본 홈 페이지	X	X
탭	X	X
책갈피 푸시	X	X
화면 캡처 차단		X
현재 페이지에서 검색	X	X
3D Touch 동작	X	
공유 장치	X	X
공유 장치를 통해 파일 변조 방지	X	
설정 내보내기/가져오기	X	X
세로 및 가로 모드	X	X
Android Enterprise(Android for Work)		X
당겨서 화면의 콘텐츠 새로 고침	X	X
Secure Web 를 기본 브라우저로 사용		X

Citrix Secure Hub

September 4, 2024

Citrix Secure Hub 는 모바일 생산성 앱의 실행 패드입니다. 사용자는 Secure Hub 에 장치를 등록하여 앱 스토어 액세스 권한을 얻습니다. 사용자는 앱 스토어에서 Citrix 가 개발한 모바일 생산성 앱 및 타사 앱을 추가할 수 있습니다.

Secure Hub 및 기타 구성 요소를 Citrix Endpoint Management 다운로드 페이지에서 다운로드할 수 있습니다.

Secure Hub 및 모바일 생산성 앱의 기타 시스템 요구 사항은 시스템 요구 사항을 참조하십시오.

모바일 생산성 앱에 대한 최신 정보는 최근 발표 내용을 참조하십시오.

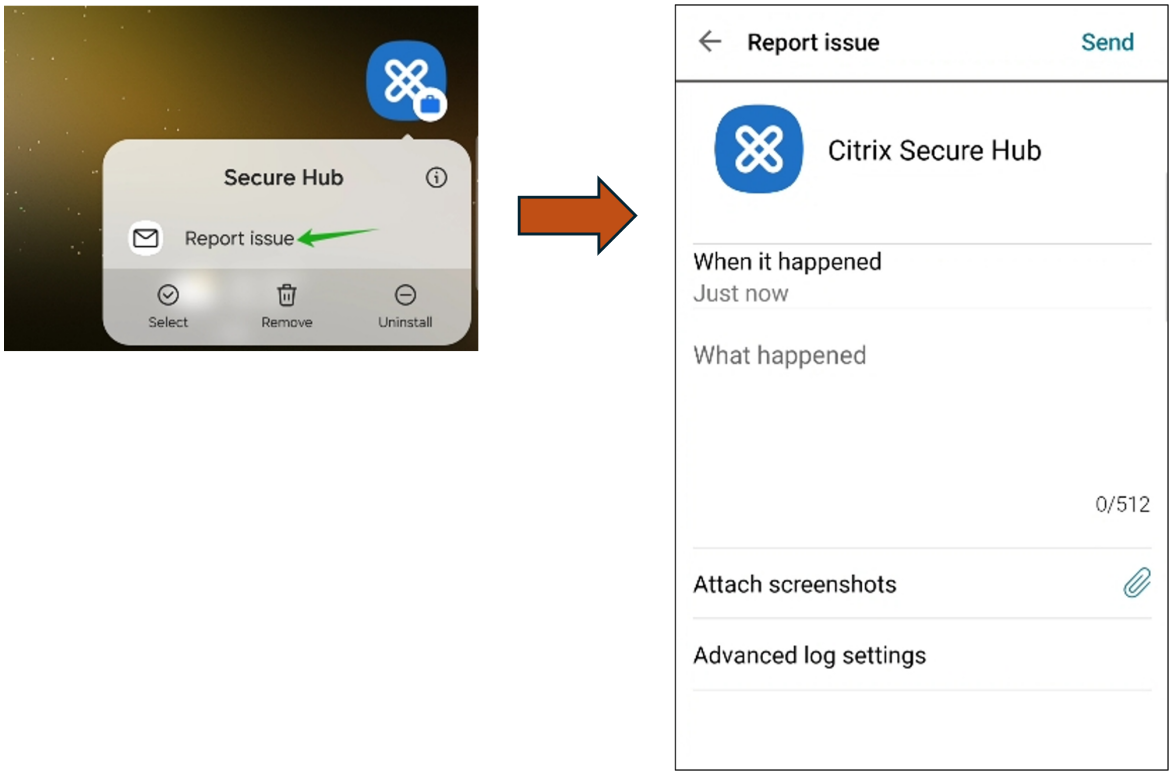
다음 섹션에서는 현재 및 이전 Secure Hub 릴리스의 새로운 기능에 대해 설명합니다.

> 참고:
>
> Secure Hub 의 Android 6.x 및 iOS 11.x 버전에 대한 지원은 2023 년 10 월에 종료되었습니다.

현재 버전의 새로운 기능

Android 용 Secure Hub 24.6.0

향상된 로그 수집 및 보고 Secure Hub 에는 Secure Hub 를 열지 않고도 원활하게 문제를 보고하고 로그를 전송할 수 있는 향상된 기능이 도입되었습니다. 이번 릴리스부터 사용자는 Secure Hub 앱 아이콘을 길게 눌러 문제 보고 옵션에 액세스할 수 있습니다. 문제 보고 옵션을 클릭하면 Secure Hub 가 문제 보고 페이지를 직접 엽니다.



이전 버전의 새로운 기능

iOS 용 Secure Hub 24.5.0

iOS 17 작동 상태 복귀 지원 Secure Hub 는 iOS 17 의 서비스 복귀 기능을 지원합니다. 이 기능은 보다 효율적이고 안전한 모바일 장치 관리 (MDM) 환경을 제공합니다. 이전에는 장치를 초기화한 후 새 사용자를 위해 설정하려면 수동으로 구성해야 했습니다. 이제 서비스 복원 기능을 통해 회사 장치의 용도를 변경하든 개인 장치 (BYOD) 를 올바른 보안 정책과 통합하든 이 프로세스를 자동화할 수 있습니다.

서비스 복원 기능을 사용할 경우 MDM 서버에서 Wi-Fi 세부 정보 및 기본 MDM 등록 프로필이 포함된 삭제 명령을 사용자 장치에 보낼 수 있습니다. 그러면 장치가 모든 사용자 데이터를 자동으로 초기화하고 지정된 Wi-Fi 네트워크에 연결한 다음 제공된 등록 프로필을 사용하여 MDM 서버에 다시 등록합니다.

Android 용 **Secure Hub 24.3.0**

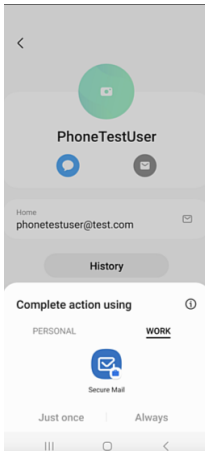
Samsung Knox 고급 증명 **v3** 지원 이제 Secure Hub 에서 Samsung 고급 증명 v3 을 지원하므로 Knox 증명을 활용하여 Citrix Endpoint Management 를 통해 관리되는 Samsung 장치에 대한 보안 조치를 강화할 수 있습니다. 이 고급 증명 프로토콜은 장치의 무결성과 보안 상태를 확인하여 장치가 루팅되지 않고 인증된 펌웨어를 실행하고 있는지 확인합니다. 이 기능은 보안 위협에 대한 필수 보호 계층을 제공하고 기업 보안 정책을 준수하도록 보장합니다.

Android 용 **Secure Hub 23.12.0**

Samsung Knox 를 통한 보안 강화 Citrix Endpoint Management 에 Knox Platform for Enterprise Key 장치 정책이 추가되어 삼성 장치에서 Secure Hub 의 보안 기능이 크게 향상되었습니다. 이 정책을 통해 필수 Samsung Knox Platform for Enterprise(KPE) 라이선스 정보를 제공하고 KPE 라이선스를 사용하여 Samsung 장치의 보안을 강화할 수 있습니다. Samsung Knox 는 기업 데이터를 보호하는 동시에 관리 용이성과 원활한 사용자 경험을 보장합니다.

자세한 내용은 Knox Platform for Enterprise Key 장치 정책을 참조하십시오.

사용자의 개인 프로필에서 **Secure Mail** 에 액세스 이제 사용자는 개인 프로필의 작업 프로필에서 Secure Mail 에 액세스하고 사용할 수 있습니다. 사용자가 개인 프로필 주소록에서 전자 메일 주소를 클릭하면 작업 프로필에서 Secure Mail 을 사용할 수 있는 옵션이 나타납니다. 이 기능을 사용하면 사용자가 개인 프로필에서 이메일을 보낼 수 있어 편리합니다. 이 기능은 BYOD 또는 WPCOD 장치에 적용할 수 있습니다.



iOS 용 **Secure Hub 24.1.0**

이 릴리스는 전반적인 성능 및 안정성을 개선하는 데 도움이 되는 몇 가지 문제를 해결합니다.

Android 용 **Secure Hub 23.12.0**

로그인 페이지에 인증 **PIN** 에 대한 힌트 추가 23.12.0 릴리스부터 로그인 페이지에 인증 PIN 에 대한 힌트를 추가할 수 있습니다. 이 기능은 선택 사항이며 2 단계 인증을 위해 등록된 장치에 적용됩니다. 힌트를 통해 PIN 에 액세스하는 방법을 알 수 있습니다.

힌트를 텍스트 또는 링크로 구성할 수 있습니다. 힌트 텍스트는 PIN 에 대한 간결한 정보를 제공하고 링크는 PIN 에 액세스하는 방법에 대한 자세한 정보를 제공합니다. 힌트를 구성하는 방법에 대한 자세한 내용은 Citrix Endpoint Management 콘솔을 통한 힌트 구성을 참조하십시오.

Single Sign-on 기능을 지원하는 **nFactor** 인증 Android 용 Secure Hub 버전 23.12.0 부터 모바일 애플리케이션 관리 (MAM) 용 nFactor 등록 또는 로그인은 Single Sign-on(SSO) 기능을 지원합니다. 이 기능을 사용하면 이전에 입력한 로그인 자격 증명이 MAM 등록 또는 로그인 프로세스를 거치므로 사용자가 수동으로 다시 입력할 필요가 없습니다. nFactor SSO 속성에 대한 자세한 내용은 Citrix Endpoint Management 설명서의 클라이언트 속성 참조를 참조하십시오.

직접 부팅 모드에서 전체 초기화 지원 이전에는 재부팅한 장치에서 전체 초기화 명령을 실행하려면 장치의 잠금을 해제해야 했습니다. 이제 장치가 잠긴 경우에도 직접 부팅 모드에서 전체 초기화 명령을 실행할 수 있습니다. 이 기능은 보안 관점에서 유용하며, 특히 장치가 승인되지 않은 개인이 소유하고 있는 경우에 유용합니다. 전체 초기화 명령에 대한 자세한 내용은 Citrix Endpoint Management 설명서의 보안 작업을 참조하십시오.

Secure Hub 앱 스토어 로딩 속도 최적화 이제 Secure Hub 의 앱 스토어가 이전보다 빠르게 로드되어 사용자가 더 빠르게 액세스할 수 있습니다.

iOS 용 **Secure Hub 23.11.0**

로그인 페이지에 인증 **PIN** 에 대한 힌트 추가 23.11.0 릴리스부터 로그인 페이지에 인증 PIN 에 대한 힌트를 추가할 수 있습니다. 이 기능은 선택 사항이며 2 단계 인증을 위해 등록된 장치에 적용됩니다. 힌트를 통해 PIN 에 액세스하는 방법을 알 수 있습니다.

힌트를 텍스트 또는 링크로 구성할 수 있습니다. 힌트 텍스트는 PIN 에 대한 간결한 정보를 제공하고 링크는 PIN 에 액세스하는 방법에 대한 자세한 정보를 제공합니다. 힌트를 구성하는 방법에 대한 자세한 내용은 Citrix Endpoint Management 콘솔을 통한 힌트 구성 문서를 참조하십시오.

Single Sign-on 기능을 지원하는 **nFactor** 인증 iOS 용 Secure Hub 버전 23.11.0 부터 모바일 애플리케이션 관리 (MAM) 용 nFactor 등록 또는 로그인은 Single Sign-on(SSO) 기능을 지원합니다. 이 기능을 사용하면 이전에 입력한 로그인 자격 증명이 MAM 등록 또는 로그인 프로세스를 거치므로 사용자가 수동으로 다시 입력할 필요가 없습니다.

nFactor SSO 속성에 대한 자세한 내용은 Citrix Endpoint Management 설명서의 클라이언트 속성 참조를 참조하십시오.

Secure Hub 23.10.0

Android 용 Secure Hub

Android 용 Secure Hub 23.10.0 은 Android 14 를 지원합니다. Secure Hub 버전을 23.10.0 으로 업그레이드하면 Android 14 로 업데이트된 장치를 계속 지원할 수 있습니다.

Secure Hub 23.9.0

Android 용 Secure Hub

이 릴리스에서는 전반적인 성능 및 안정성을 개선하는 영역을 다룹니다.

Secure Hub 23.8.1

iOS 용 Secure Hub 이 릴리스는 전반적인 성능 및 안정성을 개선하는 데 도움이 되는 몇 가지 문제를 해결합니다.

Secure Hub 23.8.0

iOS 용 Secure Hub 이 릴리스는 전반적인 성능 및 안정성을 개선하는 데 도움이 되는 몇 가지 문제를 해결합니다.

Secure Hub 23.7.0

Android 용 Secure Hub

Play Integrity API SafetyNet Attestation API 는 지원 중단 일정에 따라 Google 에서 곧 지원을 중단하며 제안된 Play Integrity API 로 이전될 예정입니다.

자세한 내용은 Citrix Endpoint Management 문서의 Play Integrity API를 참조하십시오.

지원 중단에 대한 자세한 내용은 Citrix Endpoint Management 문서의 지원 중단 및 제거를 참조하십시오.

Android SafetyNet 기능에 대한 자세한 내용은 SafetyNet을 참조하십시오.

Secure Hub 23.4.0

iOS 용 Secure Hub

사용자 환경 개선 23.4.0 버전부터 iOS 용 Secure Hub 는 다음과 같은 사용자 경험을 개선합니다.

- 저장소 경험:

  ⊠ 이전에는 My Apps 페이지가 먼저 표시되었습니다. 23.4.0 버전에서는 저장소 페이지가 가장 먼저 나타납니다.

  ⊠ 이전에는 Secure Hub 저장소에서 사용자가 저장소 옵션을 클릭할 때마다 다시 로드 작업을 수행했습니다.

  23.4.0 버전에서는 사용자 경험이 개선되었습니다. 이제 사용자가 처음으로 앱을 시작하거나, 앱을 다시 시작하거나, 화면을 아래로 살짝 밀면 앱이 다시 로드됩니다.

- 사용자 인터페이스: 이전에는 로그오프 옵션이 화면 왼쪽 하단에 위치했습니다. 23.4.0 버전에서는 로그오프 옵션이 기본 메뉴의 일부이며 정보 옵션 위에 있습니다.

- 하이퍼링크: 이전에는 앱 정보 페이지의 하이퍼링크가 일반 텍스트로 표시되었습니다. 23.4.0 버전에서는 하이퍼링크를 클릭할 수 있으며 링크를 나타내는 밑줄 서식이 적용됩니다.

MDX 에서 **MAM SDK** 로의 전환 경험 23.4.0 버전부터 iOS 듀얼 모드 앱의 기존 MDX 에서 MAM SDK 로 전환하는 경험이 향상되었습니다. 이 기능은 알림 메시지를 줄이고 Secure Hub 로 전환하여 모바일 생산성 앱을 사용할 때 사용자 경험을 개선합니다.

Citrix PIN 을 사용한 앱 잠금 해제 이전에는 최종 사용자가 장치 암호를 입력하여 MAM(모바일 앱 관리) 기반 앱을 잠금 해제했습니다.

23.4.0 버전부터 최종 사용자는 Citrix PIN 을 암호로 입력하여 MAM 기반 앱을 잠금 해제할 수 있습니다. 관리자는 CEM 서버의 클라이언트 속성을 사용하여 암호의 복잡성을 구성할 수 있습니다.

앱이 허용된 시간을 초과하여 비활성화될 때마다 최종 사용자는 관리자가 설정한 구성에 따라 Citrix PIN 을 입력하여 앱을 잠금 해제할 수 있습니다.

Android 용 Secure Hub 에는 MAM 애플리케이션의 비활성 타이머 처리 방식을 구성하는 별도의 클라이언트 속성이 있습니다. 자세한 내용은 Android 의 별도 비활성화 타이머를 참조하십시오.

Secure Hub 23.4.1

Android 용 **Secure Hub** 이 릴리스는 전반적인 성능 및 안정성을 개선하는 데 도움이 되는 몇 가지 문제를 해결합니다.

Secure Hub 23.4.0

Android 용 **Secure Hub** 이 릴리스는 전반적인 성능 및 안정성을 개선하는 데 도움이 되는 몇 가지 문제를 해결합니다.

Secure Hub 23.2.0

Android 용 Secure Hub

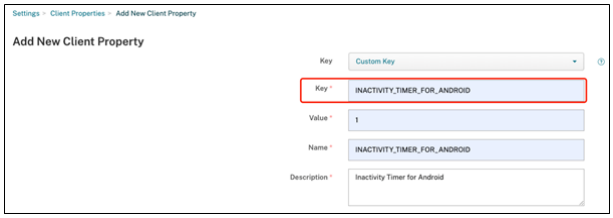
> 참고:
>
> - 유럽 연합 (EU), 유럽 경제 지역 (EEA), 스위스 및 영국의 사용자에 대한 분석 데이터는 수집되지 않습니다.

MDX 전체 터널 모드 VPN MDX Micro VPN(전체 터널 모드) 은 지원 중단되었습니다.

자세한 내용은 Citrix Endpoint Management 설명서의 지원 중단을 참조하십시오.

Android 용 비활성 타이머 분리 이전에는 Android 및 iOS 용 Secure Hub 에서 비활성 타이머 클라이언트 속성이 일반적이었습니다.

23.2.0 버전부터 IT 관리자는 새로운 클라이언트 속성인 **Inactivity_Timer_For_Android** 를 사용하여 iOS 의 비활성 타이머에서 분리할 수 있습니다. IT 관리자는 **Inactivity_Timer_For_Android** 의 값을 0 으로 설정하여 Android 비활성 타이머를 독립적으로 비활성화할 수 있습니다. 이렇게 하면 Secure Hub 를 비롯한 작업 프로필의 모든 앱이 작업 PIN 에만 인증 질문을 요구합니다.



클라이언트 속성을 추가하고 수정하는 방법에 대한 자세한 내용은 XenMobile 설명서의 클라이언트 속성을 참조하십시오.

Secure Hub 22.11.0

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 22.9.0

Android 용 Secure Hub 이 릴리스에는 다음이 포함되어 있습니다.

- 장치 암호의 암호 복잡성 (Android 12+)
- SDK 31 에 대한 지원
- 버그 수정

장치 암호의 암호 복잡성 (Android 12+) 사용자 지정 암호 요구 사항보다 복잡한 암호가 선호됩니다. 암호 복잡성 수준은 사전 정의된 수준 중 하나입니다. 따라서 최종 사용자는 복잡도 수준이 낮은 암호를 설정할 수 없습니다.

Android 12 이상 장치의 암호 복잡성은 다음과 같습니다.

- 암호 복잡성 적용**:** 사용자 지정 암호 요구 사항이 아닌 플랫폼에서 정의한 복잡성 수준의 암호가 필요합니다. Android 12 이상 버전 및 Secure Hub 22.9 이상을 사용하는 장치에만 해당됩니다.
- 복잡성 수준**:** 사전 정의된 암호 복잡성 수준입니다.
  - 없음**:** 비밀번호가 필요하지 않습니다.
  - 낮음**:** 암호는 다음일 수 있습니다.
    - 패턴
    - 최소 네 개의 숫자로 구성된 PIN
  - 미디어**:** 암호는 다음일 수 있습니다.
    - 반복되거나 (4444) 이어지지 (1234) 않는 최소 네 개의 숫자로 이루어진 PIN
    - 최소 네 자 이상의 알파벳
    - 최소 네 자 이상의 영숫자
  - 높음**:** 암호는 다음일 수 있습니다.
    - 반복되거나 (4444) 이어지지 (1234) 않는 최소 여덟 개의 숫자로 이루어진 PIN
    - 최소 여섯 자의 알파벳
    - 최소 여섯 자의 영숫자

> 참고**:**
>
> - BYOD 장치의 경우 최소 길이, 필수 문자, 생체 인식 및 고급 규칙과 같은 암호 설정은 Android 12 이상에서 적용되지 않습니다. 대신 암호 복잡성을 사용하십시오.
> - 작업 프로필의 암호 복잡성을 활성화한 경우 장치 측의 암호 복잡성도 활성화해야 합니다.

자세한 내용은 Citrix Endpoint Management 설명서에서 Android Enterprise 설정을 참조하십시오.

Secure Hub 22.7.0

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 22.6.0

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 22.5.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 22.4.0

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 22.2.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.11.0

Android 용 Secure Hub

회사 소유 장치에 대한 작업 프로필 지원 이제 Android Enterprise 장치에서 회사 소유 장치의 작업 프로필 모드로 Secure Hub 를 등록할 수 있습니다. 이 기능은 Android 11 이상을 실행하는 장치에서 사용할 수 있습니다. 장치가 Android 10 에서 Android 11 이상으로 업그레이드되면 이전에 COPE(회사 소유 개인 사용) 모드에 등록된 장치는 회사 소유 장치의 작업 프로필 모드로 자동 마이그레이션됩니다.

Secure Hub 21.10.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub **Android 12** 를 지원합니다. 이번 릴리스부터 Android 12 를 실행하는 장치에서 Secure Hub 가 지원됩니다.

Secure Hub 21.8.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.7.1

Android 용 Secure Hub 이미 등록된 장치에서 **Android 12** 를 지원합니다**.** Android 12 로 업그레이드하려는 경우 먼저 Secure Hub 를 버전 21.7.1 로 업데이트해야 합니다. Secure Hub 21.7.1 은 Android 12 로 업그레이드하는 데 필요한 최소 버전입니다. 이 릴리스에서는 이미 등록된 사용자를 위해 Android 11 에서 Android 12 로 원활하게 업그레이드할 수 있습니다.

> 참고**:**
>
> Android 12 로 업그레이드하기 전에 Secure Hub 가 버전 21.7.1 로 업데이트되지 않은 경우 이전 기능을 복구하려면 장치를 다시 등록하거나 공장 초기화해야 할 수 있습니다.

> Citrix 는 Android 12 에 대한 1 일차 지원을 제공하기 위해 최선을 다하고 있으며 Android 12 를 완벽하게 지원하기 위해 후속 버전의 Secure Hub 에 업데이트를 추가할 예정입니다.

Secure Hub 21.7.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.6.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.5.1

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.5.0

iOS 용 Secure Hub 이 릴리스에서는 MDX Toolkit 버전 19.8.0 이하로 래핑된 앱이 더 이상 작동하지 않습니다. 적절한 기능을 다시 시작하려면 최신 MDX Toolkit 으로 앱을 래핑해야 합니다.

Secure Hub 21.4.0

Secure Hub 의 색상이 개선되었습니다. Secure Hub 는 Citrix 브랜드 색상 업데이트를 준수합니다.

Secure Hub 21.3.2

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.3.0

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.2.0

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 21.1.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 20.12.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub Android 용 Secure Hub 는 Direct Boot 모드를 지원합니다. Direct Boot 에 대한 자세한 정보는 *Developer.android.com* 에서 Android 설명서를 참조하십시오.

Secure Hub 20.11.0

Android 용 Secure Hub Secure Hub 는 Android 10 에 대한 Google Play 의 현재 대상 API 요구 사항을 지원합니다.

Secure Hub 20.10.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 20.9.0

iOS 용 Secure Hub iOS 용 Secure Hub 는 iOS 14 을 지원합니다.

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 20.7.5

Android 용 Secure Hub

- Android 용 Secure Hub 는 Android 11 을 지원합니다.
- 앱의 경우 **Secure Hub 32** 비트에서 **64** 비트로 전환합니다**.** Secure Hub 버전 20.7.5 에서는 앱의 32 비트 아키텍처에 대한 지원이 종료되며, Secure Hub 는 64 비트로 업데이트되었습니다. Citrix 에서는 버전 20.6.5 에서 20.7.5 로 업그레이드할 것을 권장합니다. 사용자가 Secure Hub 버전 20.6.5 로의 업그레이드를 건너뛰고 대신 20.1.5 에서 20.7.5 로 바로 업그레이드할 경우 재인증이 필요합니다. 재인증을 수행하려면 자격 증명을 입력하고 Secure Hub PIN 을 재설정해야 합니다. Secure Hub 버전 20.6.5 는 Google Play 스토어에서 제공됩니다.
- **App Store** 에서 업데이트를 설치합니다**.** Android 용 Secure Hub 에서 앱에 사용 가능한 업데이트가 있는 경우 앱이 강조 표시되고 App Store 화면에 사용 가능한 업데이트 기능이 나타납니다.

  사용 가능한 업데이트를 탭하면 업데이트 대기 중인 앱 목록이 표시된 스토어로 이동합니다. 업데이트를 설치하려면 앱에 대한 세부 정보를 탭합니다. 앱이 업데이트되면 세부 정보의 아래쪽 화살표가 확인 표시로 변경됩니다.

Secure Hub 20.6.5

Android 용 Secure Hub 앱의 경우 **32** 비트에서 **64** 비트로 전환합니다**.** Secure Hub 20.6.5 릴리스는 Android 모바일 앱용 32 비트 아키텍처를 지원하는 마지막 릴리스입니다. 이후 릴리스에서 Secure Hub 는 64 비트 아키텍처를 지원합니다. Citrix 에서는 사용자가 재인증 없이 최신 버전으로 업그레이드할 수 있도록 Secure Hub 버전 20.6.5 로 업그레이드할 것을 권장합니다. 사용자가 Secure Hub 버전 20.6.5 로의 업그레이드를 건너뛰고 대신 20.7.5 로 직접 업데이트하는 경우 재인증이 필요합니다. 재인증을 수행하려면 자격 증명을 입력하고 Secure Hub PIN 을 재설정해야 합니다.

> 참고**:**
>
> 20.6.5 릴리스는 장치 관리자 모드에서 Android 10 을 실행하는 장치의 등록을 차단하지 않습니다.

iOS 용 Secure Hub **iOS** 장치에 구성된 프록시를 활성화합니다**.** 사용자가 설정 **> Wi-Fi** 에서 구성한 프록시 서버를 사용할 수 있게 하려면 이제 iOS 용 Secure Hub 에서는 새 클라이언트 속성 (`ALLOW_CLIENTSIDE_PROXY`) 을 사용 설정해야 합니다. 자세한 내용은 클라이언트 속성 참조의 `ALLOW_CLIENTSIDE_PROXY`에서 참조하십시오.

Secure Hub 20.3.0

> 참고**:**
>
> Android 6.x 및 iOS 11.x 버전의 Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱에 대한 지원이 2020 년 6 월에 종료됩니다.

iOS 용 Secure Hub

- 네트워크 확장 사용 안 함. App Store 검토 지침에 대한 최근 변경으로 인해 릴리스 20.3.0 부터 Secure Hub 는 iOS 를 실행하는 장치에서 NE(네트워크 확장) 를 지원하지 않습니다. NE 는 Citrix 가 개발한 모바일 생산성 앱에는 영향을 미치지 않습니다. 그러나 NE 를 제거하면 배포된 엔터프라이즈 MDX 래핑 앱에 약간의 영향이 있습니다. 권한 부여 토큰, 타이머 및 PIN 재시도와 같은 구성 요소를 동기화하는 동안 최종 사용자의 Secure Hub 에서 추가 전환이 발생할 수 있습니다. 자세한 내용은 https://support.citrix.com/article/CTX270296 항목을 참조하십시오.

> 참고:
>
> 새 사용자에게는 VPN 설치 메시지가 표시되지 않습니다.

- 향상된 등록 프로필 지원. Secure Hub 는 등록 프로필 지원에서 Citrix Endpoint Management 에 대해 발표한 향상된 등록 프로필 기능을 지원합니다.

Secure Hub 20.2.0

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 20.1.5

이 릴리스에는 다음이 포함되어 있습니다.

- 업데이트된 사용자 개인정보보호정책 서식 및 표시. 이 기능 업데이트로 인해 Secure Hub 등록 과정이 변경됩니다.
- 버그 수정

Secure Hub 19.12.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 19.11.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 19.10.5

Android 용 Secure Hub **COPE 모드에서 Secure Hub 등록.** COPE 등록 프로필에 Citrix Endpoint Management 가 구성된 경우 Android Enterprise 장치에서 COPE(회사 소유 개인 사용) 모드로 Secure Hub 를 등록할 수 있습니다.

Secure Hub 19.10.0

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 19.9.5

iOS 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub **Android Enterprise** 작업 프로필 및 완전히 관리되는 장치에 대한 **Keyguard** 관리 기능 지원**.** Android Keyguard 는 장치 및 Work Challenge 잠금 화면을 관리합니다. Citrix Endpoint Management 의 Keyguard 관리 장치 정책을 사용하여 작업 프로필 장치의 Keyguard 관리와 완전히 관리되는 장치 및 전용 장치의 Keyguard 관리를 제어할 수 있습니다. Keyguard 관리를 사용하면 Keyguard 화면을 잠금 해제하기 전에 사용자가 사용할 수 있는 기능 (예: 신뢰 에이전트 및 보안 카메라) 을 지정할 수 있습니다. 또는 모든 Keyguard 기능을 사용하지 않도록 선택할 수 있습니다.

기능 설정 및 장치 정책 구성 방법에 대한 자세한 내용은 Keyguard 관리 장치 정책을 참조하십시오.

Secure Hub 19.9.0

iOS 용 Secure Hub iOS 용 Secure Hub 는 iOS 13 을 지원합니다.

Android 용 Secure Hub 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub 19.8.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Hub 19.8.0

iOS 용 Secure Hub 이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub **Android Q 지원.** 이 릴리스에는 Android Q 에 대한 지원이 포함되어 있습니다. Android Q 플랫폼으로 업그레이드하기 전에 Google Device Administration API 의 사용 중단이 Android Q 를 실행하는 장치에 미치는 영향에 대해 장치 관리에서 Android Enterprise 로 마이그레이션에서 자세한 내용을 참조하십시오. 또한 블로그 Citrix Endpoint Management and Android Enterprise - a Season of Change(Citrix Endpoint Management 및 Android Enterprise - 변화의 계절)의 내용을 참조하십시오.

Secure Hub 19.7.5

iOS 용 Secure Hub 이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Android 용 Secure Hub Samsung Knox SDK 3.x. 지원 Android 용 Secure Hub 가 Samsung Knox SDK 3.x 를 지원합니다. Samsung Knox 3.x 로 마이그레이션하는 방법에 대한 자세한 내용은 Samsung Knox 개발자 설명서를 참조하십시오. 이 릴리스에는 새로운 Samsung Knox 네임스페이스에 대한 지원도 포함되어 있습니다. 이전 Samsung Knox 네임스페이스로 변경하는 방법에 대한 자세한 내용은 이전 Samsung Knox 네임스페이스 변경 사항에서 참조하십시오.

> 참고:
>
> Android 용 Secure Hub 는 Android 5 를 실행하는 Samsung Knox 3.x 장치를 지원하지 않습니다.

Secure Hub 19.3.5 ~ 19.6.6

이러한 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Secure Hub 19.3.0

엔터프라이즈용 **Samsung Knox** 플랫폼 지원**.** Android 용 Secure Hub 는 Android Enterprise 장치에서 KPE(엔터프라이즈용 Knox 플랫폼) 를 지원합니다.

Secure Hub 19.2.0

이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Secure Hub 19.1.5

Android Enterprise 용 Secure Hub 는 이제 다음과 같은 정책을 지원합니다.

- **WiFi** 장치 정책**.** Wi-Fi 장치 정책이 이제 Android Enterprise 를 지원합니다. 이 정책에 대한 자세한 내용은 Wi-Fi 장치 정책을 참조하십시오.
- 사용자 지정 **XML** 장치 정책**.** 사용자 지정 XML 장치 정책이 이제 Android Enterprise 를 지원합니다. 이 정책에 대한 자세한 내용은 사용자 지정 XML 장치 정책을 참조하십시오.
- 파일 장치 정책**.** Citrix Endpoint Management 에 스크립트 파일을 추가하여 Android Enterprise 장치에서 기능을 수행할 수 있습니다. 이 정책에 대한 자세한 내용은 파일 장치 정책을 참조하십시오.

Secure Hub 19.1.0

Secure Hub 의 글꼴**,** 색상 및 기타 **UI** 항목이 개선되었습니다**.** 이로써 전체 모바일 생산성 앱 제품군에 Citrix 브랜드의 심미성을 따른 뛰어난 사용자 환경이 구현되었습니다.

Secure Hub 18.12.0

이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Secure Hub 18.11.5

- **Android Enterprise** 에 대한 제한 사항 장치 정책 설정**.** 제한 사항 장치 정책에 대한 새로운 설정은 Android Enterprise 장치에서 다음과 같은 기능에 대한 사용자 액세스를 허용합니다. Android Enterprise 장치의 상태 표시줄, 잠금 화면 키 보호, 계정 관리, 위치 공유 및 장치 화면을 켠 상태로 유지. 자세한 내용은 Restrictions device policy(제한 장치 정책)를 참조하십시오.

Secure Hub 18.10.5~18.11.0 에는 성능 향상 기능 및 버그 수정이 포함되어 있습니다.

Secure Hub 18.10.0

- **Samsung DeX** 모드 지원**:** Samsung DeX 를 사용하면 KNOX 기반 장치를 외부 디스플레이에 연결하여 PC 와 같은 인터페이스에서 앱을 사용하고 문서를 검토하며 비디오를 볼 수 있습니다. Samsung DeX 장치 요구 사항 및 Samsung DeX 설정 방법에 대한 자세한 내용은 How Samsung DeX works(Samsung Dex 작동 방식)을 참조하십시오.

  Citrix Endpoint Management 에서 Samsung DeX 모드 기능을 구성하려면 Samsung Knox 에 대한 제한 장치 정책을 업데이트합니다. 자세한 내용은 **Samsung KNOX settings(Samsung KNOX** 설정**)** 및 Restrictions device policy(제한 장치 정책)를 참조하십시오.

- **Android SafetyNet** 지원**:** Secure Hub 가 설치된 Android 장치의 호환성 및 보안을 평가하기 위해 **Android SafetyNet** 기능을 사용하도록 Endpoint Management 를 구성할 수 있습니다. 평가 결과를 토대로 장치에 대한 자동화된 작업을 트리거할 수 있습니다. 자세한 내용은 Android SafetyNet을 참조하십시오.
- **Android Enterprise** 장치의 카메라 사용 제한**:** 제한 장치 정책의 새로운 카메라 사용 허용 설정을 통해 Android Enterprise 장치에서 카메라를 사용하지 못하도록 제한할 수 있습니다. 자세한 내용은 Restrictions device policy(제한 장치 정책)를 참조하십시오.

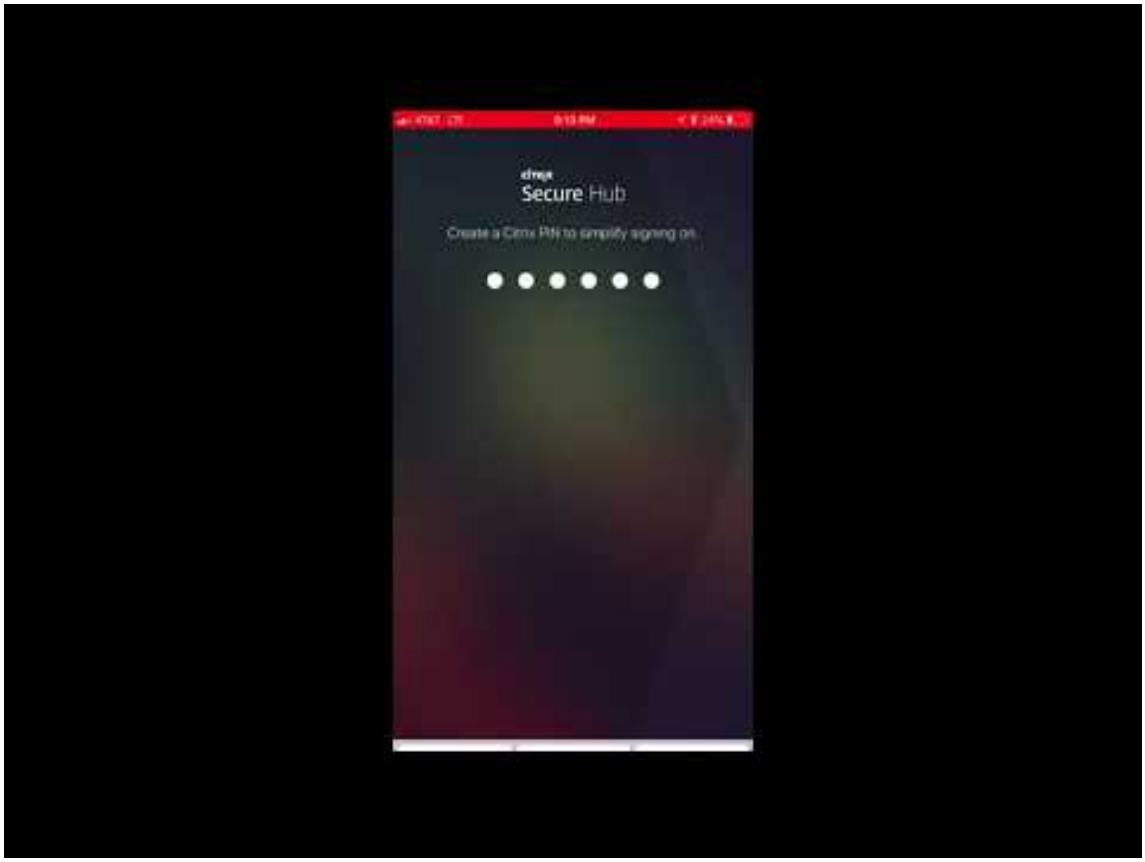
Secure Hub 10.8.60 ~ 18.9.0

이러한 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Secure Hub 10.8.60

- 폴란드어 지원
- Android P 지원

- Workspace 앱 스토어 사용 지원
  Secure Hub 를 열 때 Secure Hub 스토어가 더 이상 표시되지 않습니다. 앱 추가 단추를 누르면 Workspace 앱 스토어로 이동합니다. 다음 비디오에서는 Citrix Workspace 앱을 사용하여 Citrix Endpoint Management 에 등록하는 iOS 장치를 보여줍니다.



> 중요:
>
> 이 기능은 새로운 고객만 사용할 수 있습니다. 기존 고객을 위한 마이그레이션은 현재 지원되지 않습니다.

이 기능을 사용하려면 다음과 같이 구성합니다.

- 암호 캐싱 및 암호 인증 정책을 사용하도록 설정합니다. 정책을 구성하는 것에 대한 자세한 내용은 모바일 생산성 앱의 MDX 정책 요약을 참조하십시오.
- AD 또는 AD+Cert 로 Active Directory 인증을 구성합니다. 이러한 두 가지 모드가 지원됩니다. 인증을 구성하는 것에 대한 자세한 내용은 도메인 인증 또는 도메인 및 보안 토큰 인증을 참조하십시오.
- Endpoint Management 에 대한 Workspace 통합 기능을 사용하도록 설정합니다. Workspace 통합에 대한 자세한 내용은 Workspace 구성을 참조하십시오.

> 중요:
>
> 이 기능을 사용하도록 설정하면 Citrix Files SSO 가 Endpoint Management(이전 명칭: XenMobile) 대신 Workspace 를 통해 이루어집니다. Workspace 통합 기능을 사용하도록 설정하기 전에 Endpoint

> Management 콘솔에서 Citrix Files 통합 기능을 사용하지 않도록 설정하는 것이 좋습니다.

Secure Hub 10.8.55

- 구성 JSON 을 사용하여 Google 제로 터치 및 Samsung KME(Knox Mobile Environment) 포털의 사용자 이름과 암호를 전달할 수 있습니다. 자세한 내용은 Samsung Knox 대량 등록을 참조하십시오.
- 인증서 고정을 사용하도록 설정하면 사용자가 자체 서명된 인증서로 Endpoint Management 에 등록할 수 없습니다. 자체 서명된 인증서로 Endpoint Management 에 등록하려고 하면 인증서를 신뢰할 수 없다는 내용의 경고가 표시됩니다.

Secure Hub 10.8.25: Android 용 Secure Hub 에 Android P 장치에 대한 지원이 포함됩니다.

> 참고**:**
>
> Android P 플랫폼으로 업그레이드하기 전에: 서버 인프라가 subjectAltName(SAN) 확장에 일치하는 호스트 이름을 가진 보안 인증서와 호환되는지 확인하십시오. 호스트 이름을 확인하려면 서버가 일치하는 SAN 이 포함된 인증서를 제공해야 합니다. 호스트 이름과 일치하는 SAN 이 포함되지 않은 인증서는 더 이상 신뢰할 수 없습니다. 자세한 내용은 Android 개발자 설명서를 참조하십시오.

iOS 용 **Secure Hub** 의 **2018** 년 **3** 월 **19** 일 업데이트**:** iOS 용 Secure Hub 버전 10.8.6 을 사용하여 VPP 앱 정책 관련 문제를 해결할 수 있습니다. 자세한 내용은 이 Citrix Knowledge Center 문서를 참조하십시오.

Secure Hub 10.8.5: Android 용 Secure Hub 에서 Android Work(Android for Work) 의 COSU 모드가 지원됩니다. 자세한 내용은 Citrix Endpoint Management 설명서를 참조하십시오.

Secure Hub 관리

Endpoint Management 초기 구성 중에 Secure Hub 와 관련된 관리 작업의 대부분이 수행됩니다. iOS 및 Android 에서 사용자가 Secure Hub 를 사용할 수 있게 하려면 iOS App Store 및 Google Play Store 에 Secure Hub 를 업로드합니다.

Secure Hub 는 인증된 이후 사용자의 Citrix Gateway 세션이 갱신될 때 Citrix Gateway 를 사용하여 설치된 앱에 대해 Endpoint Management 에 저장된 대부분의 MDX 정책을 새로 고칩니다.

> 중요**:**
>
> 보안 그룹, 암호화 사용 및 Secure Mail Exchange Server 정책 중 하나를 변경한 경우 사용자가 앱을 삭제하고 다시 설치하여 업데이트된 정책을 적용해야 합니다.

Citrix PIN

Endpoint Management 콘솔의 설정 > 클라이언트 속성에 설정된 보안 기능인 Citrix PIN 을 사용하도록 Secure Hub 를 구성할 수 있습니다. 이 설정에서는 등록된 모바일 장치 사용자가 Secure Hub 에 로그온하고 MDX 래핑된 앱을 PIN(개인 식별 번호) 을 사용하여 활성화해야 합니다.

Citrix PIN 기능을 사용하면 래핑된 보안 앱에 로그온할 때 사용자 인증 환경이 간소화됩니다. 사용자는 Active Directory 사용자 이름 및 암호 같은 다른 자격 증명을 반복적으로 입력하지 않아도 됩니다.

Secure Hub 에 처음 로그인하는 사용자는 Active Directory 사용자 이름 및 암호를 입력해야 합니다. 로그인 중에 Secure Hub 는 Active Directory 자격 증명 또는 클라이언트 인증서를 사용자 장치에 저장한 후, 사용자에게 PIN 을 입력하라는 메시지를 표시합니다. 사용자가 다시 로그온할 경우, 사용자는 PIN 을 입력하여 활성 사용자 세션에 대한 다음 유휴 시간 초과 기간이 끝날 때까지 Citrix 앱 및 저장소에 안전하게 액세스합니다. 관련된 클라이언트 속성을 통해 PIN 을 사용하여 비밀 정보를 암호화할 수 있으며 PIN 암호 유형을 지정하고 PIN 강도 및 길이 요구 사항을 지정할 수 있습니다. 자세한 내용은 클라이언트 속성을 참조하십시오.

지문 인증 (Touch ID) 을 사용하도록 설정하면 사용자는 앱이 비활성화되어 오프라인 인증이 필요한 경우에 지문을 사용하여 로그온할 수 있습니다. 사용자는 Secure Hub 에 처음 로그인할 때, 장치를 재시작할 때 그리고 비활성화 타이머가 만료된 후에는 여전히 PIN 을 입력해야 합니다. 지문 인증 사용에 대한 자세한 내용은 지문 또는 Touch ID 인증을 참조하십시오.

인증서 고정

iOS 및 Android 용 Secure Hub 는 SSL 인증서 고정을 지원합니다. 이 기능은 Citrix 클라이언트가 Endpoint Management 와 통신할 때 기업에서 서명한 인증서가 사용되도록 하여 장치에서의 루트 인증서 설치로 인해 SSL 세션이 손상될 경우 클라이언트에서 Endpoint Management 로 연결되지 못하게 합니다. Secure Hub 에서 서버 공개 키 변경을 감지하면 Secure Hub 는 연결을 거부합니다.

Android N 의 경우, 이 운영 체제는 사용자가 추가한 CA(인증 기관) 를 더 이상 허용하지 않습니다. Citrix 에서는 사용자가 추가한 CA 대신 공용 루트 CA 를 사용하도록 권장합니다.

Android N 으로 업그레이드하는 사용자가 개인 또는 자체 서명 CA 를 사용할 경우 문제를 겪을 수 있습니다. 다음 시나리오에서는 Android N 장치에서의 연결이 끊깁니다.

- Endpoint Management 에 대한 개인/자체 서명 CA 및 필요한 신뢰된 CA 옵션은 켜짐으로 설정되어 있습니다. 자세한 내용은 장치 관리를 참조하십시오.
- 개인/자체 서명 CA 와 Endpoint Management ADS(자동 검색 서비스) 를 연결할 수 없습니다. ADS 에 연결할 수 없으면, 보안을 고려하여 필요한 신뢰할 수 있는 CA 가 초기에 꺼짐으로 설정되었더라도 켜짐으로 바뀝니다.

장치를 등록하거나 Secure Hub 를 업그레이드하기 전에 인증서 고정을 사용하도록 설정하는 것이 좋습니다. 이 옵션은 기본적으로 꺼짐으로 설정되며 ADS 를 통해 관리됩니다. 인증서 고정을 사용하도록 설정하면 사용자가 자체 서명된 인증서로 Endpoint Management 에 등록할 수 없습니다. 자체 서명된 인증서로 등록하려고 하면 인증서를 신뢰할 수 없다는 내용의 경고가 표시됩니다. 사용자가 인증서를 수락하지 않으면 등록이 실패합니다.

인증서 고정을 사용하려면 Citrix 에 인증서를 Citrix ADS 서버에 업로드해 달라고 요청합니다. Citrix 지원 포털을 사용하여 기술 지원 사례를 엽니다. 개인 키를 Citrix 에 보내지 않도록 합니다. 이후 다음 정보를 입력합니다.

- 사용자가 등록될 계정을 포함하는 도메인
- Endpoint Management 의 FQDN(정규화된 도메인 이름)
- Endpoint Management 의 인스턴스 이름. 기본적으로 인스턴스 이름은 zdm 이고 대/소문자를 구분합니다.
- 사용자 ID 유형 (UPN 또는 전자 메일일 수 있음). 기본적으로 이 유형은 UPN 입니다.

- iOS 등록에 사용된 포트 (포트 번호를 기본 포트 8443 에서 변경한 경우)
- Endpoint Management 가 연결을 받아들이는 포트 (포트 번호를 기본 포트 443 에서 변경한 경우)
- Citrix Gateway 의 전체 URL.
- 또는 관리자의 전자 메일 주소
- 도메인에 추가할 PEM 형식의 인증서입니다. 이 인증서는 개인 키가 아닌 공개 인증서여야 합니다.
- 기존 서버 인증서를 처리하는 방식: 오래된 서버 인증서가 손상되어 즉시 제거할지 또는 만료될 때까지 오래된 서버 인증서를 계속 지원할지 여부

세부 정보 및 인증서가 Citrix 서버에 추가되면 기술 지원 사례가 업데이트됩니다.

인증서 **+** 일회용 암호 인증

Secure Hub 가 인증서 및 일회용 암호 역할을 하는 보안 토큰을 사용하여 인증되도록 Citrix ADC 를 구성할 수 있습니다. 이 구성은 Active Directory 흔적을 장치에 남기지 않는 강력한 보안 옵션을 제공합니다.

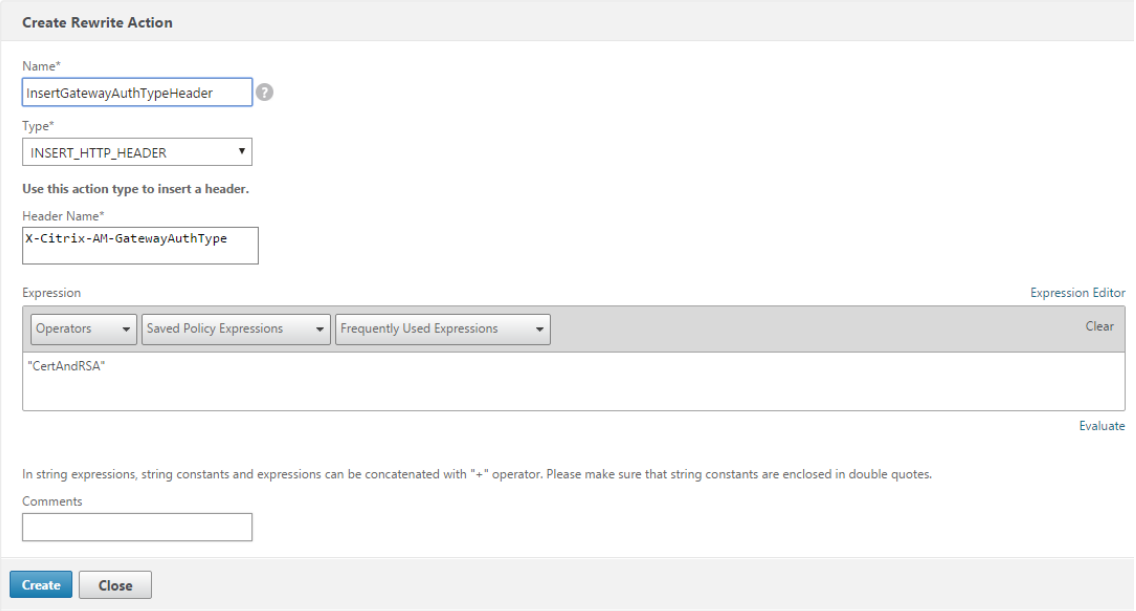
Secure Hub 가 인증서 + 일회용 암호 인증 유형을 사용하도록 설정하려면 Citrix Gateway 로그온 유형을 나타내기 위해 **X-Citrix-AM-GatewayAuthType: CertAndRSA** 형태의 사용자 지정 응답 헤더를 삽입하는 다시 쓰기 작업 및 다시 쓰기 정책을 Citrix ADC 에서 추가합니다.

일반적으로 Secure Hub 는 Endpoint Management 콘솔에서 구성한 Citrix Gateway 로그온 유형을 사용합니다. 그러나 Secure Hub 가 로그온을 처음 완료할 때까지는 Secure Hub 에서 이 정보를 사용할 수 없기 때문에 사용자 지정 헤더가 필요합니다.

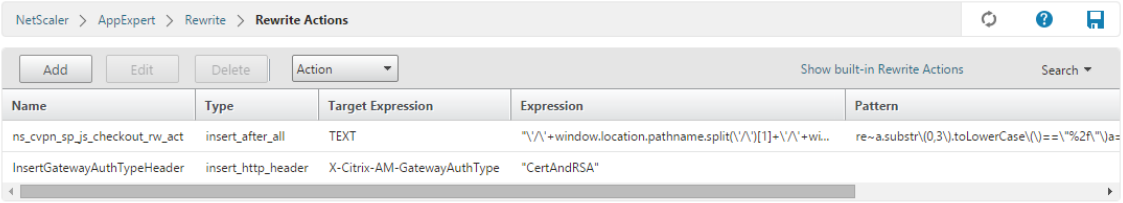
> 참고**:**
>
> 여러 가지 로그온 유형이 Endpoint Management 및 Citrix ADC 에 설정된 경우, Citrix ADC 구성이 우선합니다. 자세한 내용은 Citrix Gateway 및 Endpoint Management를 참조하십시오.

1. Citrix ADC 에서 **Configuration(**구성**) > AppExpert > Rewrite(**다시 쓰기**) > Actions(**작업**)** 로 이동합니다.
2. 추가를 클릭합니다.

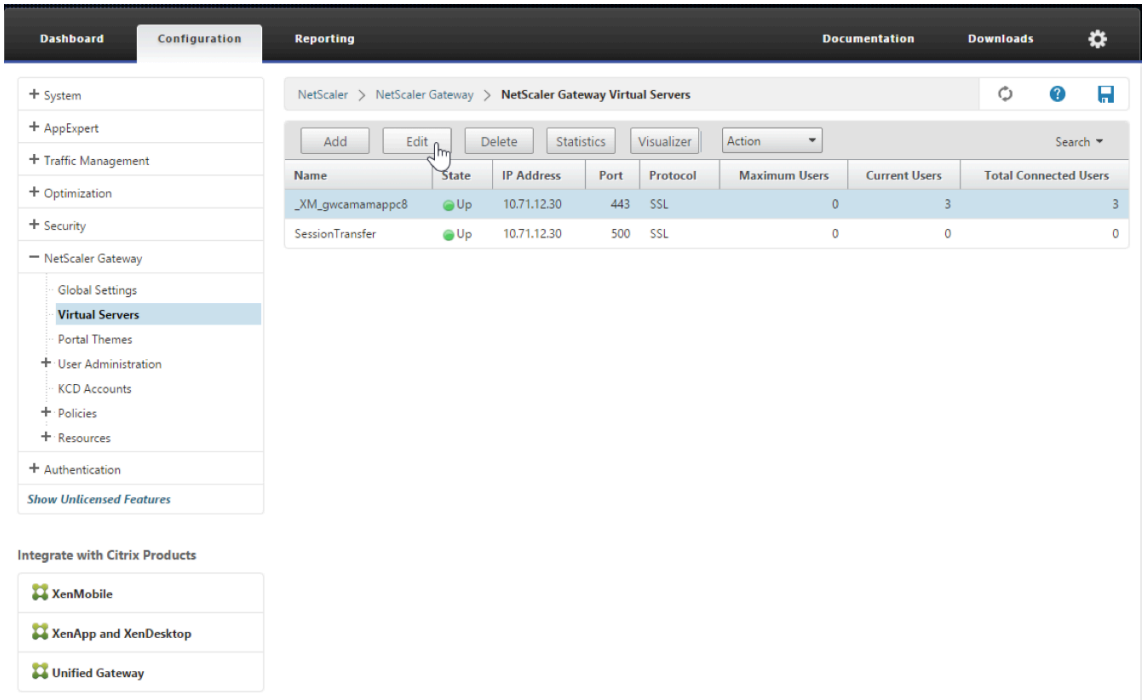
   Create Rewrite Action(다시 쓰기 작업 만들기**)** 화면이 나타납니다.
3. 다음 그림과 같이 각 필드를 채우고 **Create(**만들기**)** 를 클릭합니다.



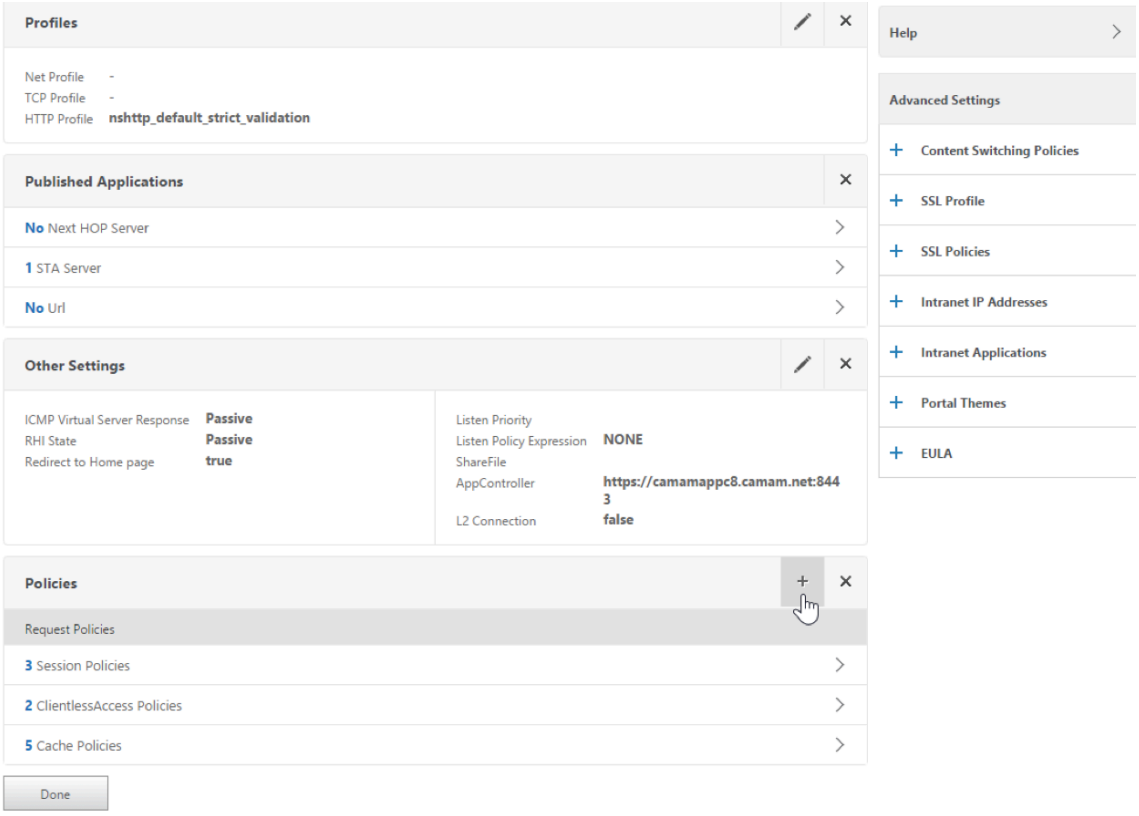
기본 **Rewrite Actions(**다시 쓰기 작업**)** 화면에 다음 결과가 나타납니다.



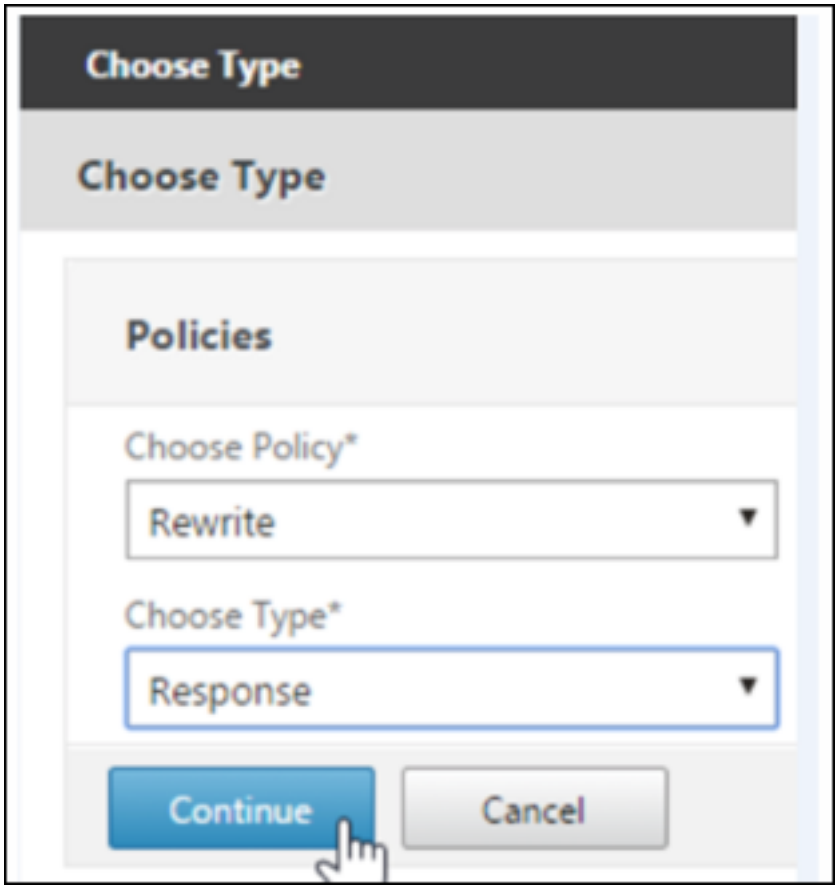
4. 다시 쓰기 작업을 가상 서버에 다시 쓰기 정책으로 바인딩합니다. **Configuration(**구성**) > NetScaler Gateway > Virtual Servers(**가상 서버**)** 로 이동한 후, 가상 서버를 선택합니다.



5. 편집을 클릭합니다.
6. **Virtual Servers configuration(**가상 서버 구성**)** 화면에서 아래로 스크롤하여 **Policies(**정책**)** 로 이동합니다.
7. **+** 를 클릭하여 정책을 추가합니다.

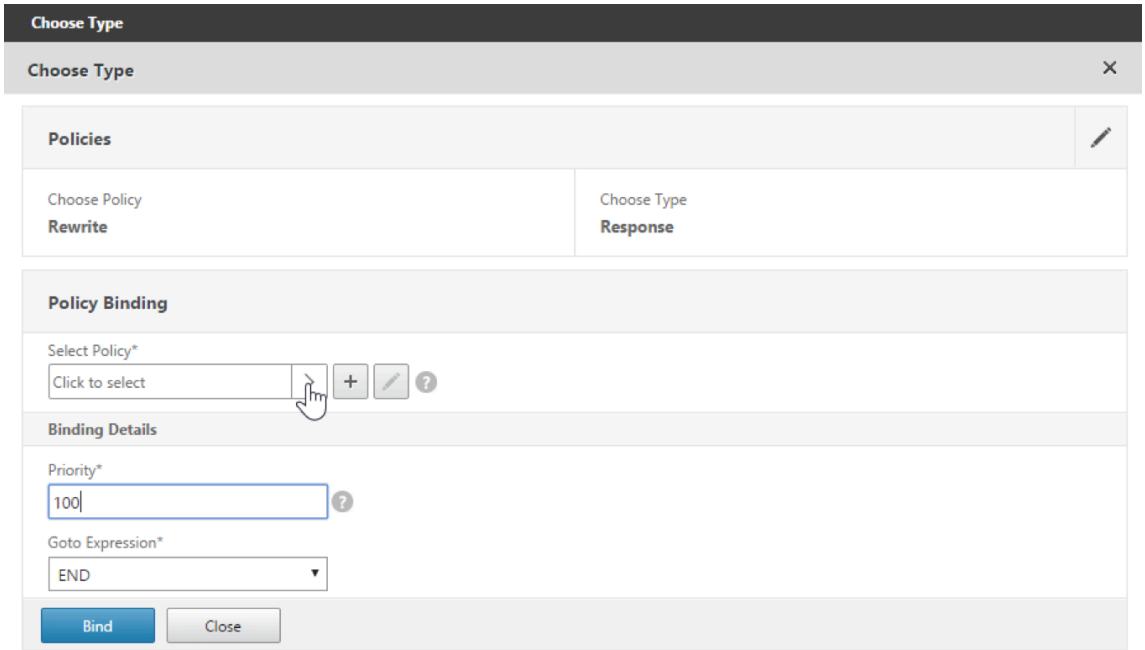


8. **Choose Policy(**정책 선택**)** 필드에서 **Rewrite(**다시 쓰기**)** 를 선택합니다.
9. **Choose Type(**유형 선택**)** 필드에서 **Response(**응답**)** 를 선택합니다.



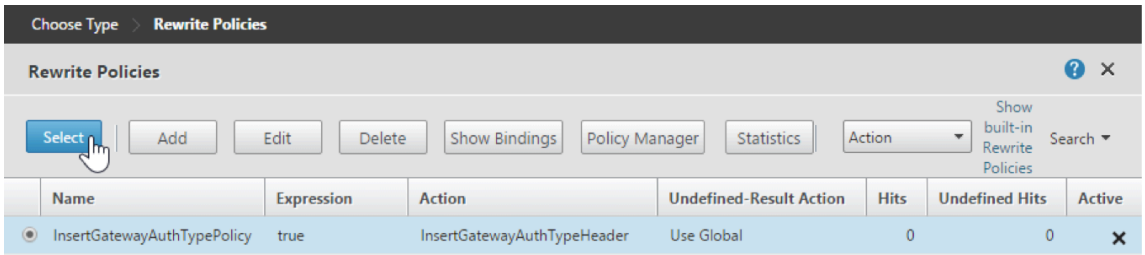
10. **Continue(**계속**)** 을 클릭합니다.

    Policy Binding(정책 바인딩**)** 섹션이 확장됩니다.

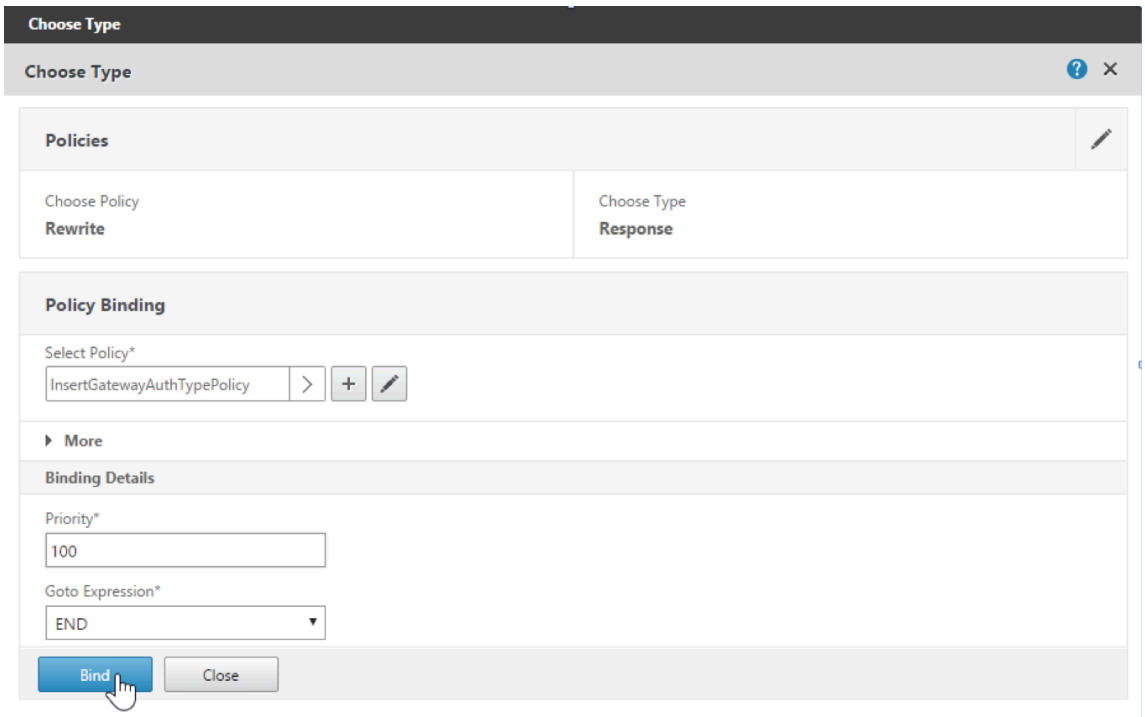


11. **Select Policy(**정책 선택**)** 를 클릭합니다.

    사용 가능한 정책을 포함하는 화면이 나타납니다.

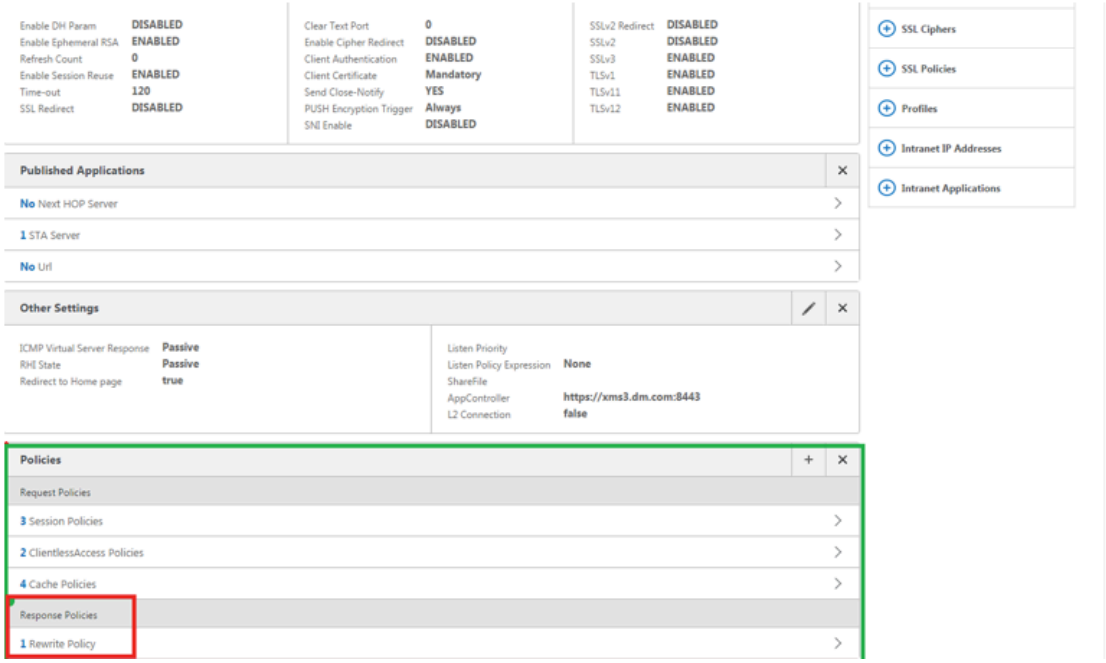


12. 앞에서 생성한 정책의 행을 클릭한 후 **Select(**선택**)** 를 클릭합니다. 선택한 정책이 채워진 채로 **Policy Binding(**정책 바인딩**)** 화면이 다시 나타납니다.

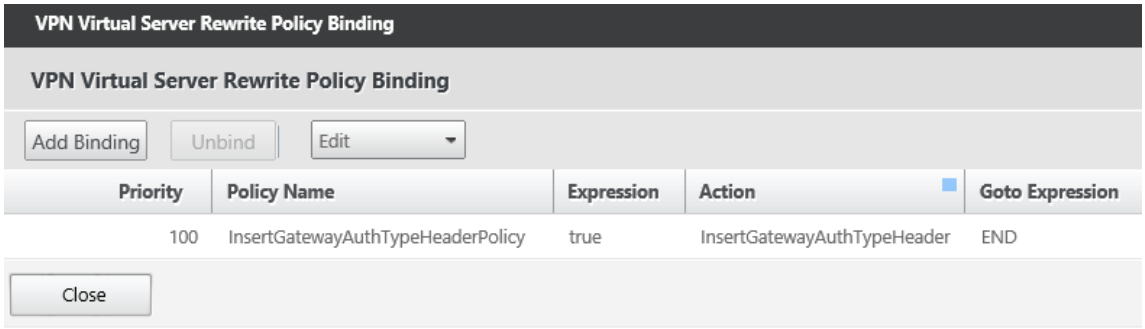


13. **Bind(**바인딩**)** 를 클릭합니다.

바인딩이 성공적이면 기본 구성 화면이 나타나고 완성된 다시 쓰기 정책이 표시됩니다.



14. 정책 세부 정보를 보려면 **Rewrite Policy(**다시 쓰기 정책**)** 를 클릭합니다.



Android 장치의 **ADS** 연결을 위한 포트 요구 사항 포트 구성은 Secure Hub 로부터 연결되는 Android 장치가 회사 네트워크 내에서 Citrix ADS 에 액세스할 수 있도록 합니다. ADS 를 통해 사용 가능해진 보안 업데이트를 다운로드할 경우 ADS 에 액세스할 수 있는 것이 중요합니다. 프록시 서버에서 ADS 연결이 작동하지 않을 수 있습니다. 이 시나리오에서는 ADS 연결이 프록시 서버를 우회할 수 있게 허용합니다.

> 중요:
>
> Android 및 iOS 용 Secure Hub 의 경우 Android 장치가 ADS 에 액세스하도록 허용해야 합니다. 자세한 내용은 Citrix Endpoint Management 설명서에서 포트 요구 사항을 참조하십시오. 이 통신은 아웃바운드 포트 443 을 통해 이루어집니다. 기존 환경은 이 액세스를 허용하도록 설계되었을 가능성이 매우 높습니다. 이 통신을 지원할 수 없는 고객은 Secure Hub 10.2 로 업그레이드하지 않는 것이 좋습니다. 궁금한 점이 있으면 Citrix 지원 팀에 문의하십시오.

필수 구성 요소:

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

개선된 새 인증서 고정에서는 장치 등록 전에 장치가 ADS 에 연결되어야 합니다. 그러면 장치가 등록되고 있는 환경에서 Secure Hub 가 최신 보안 정보를 사용할 수 있게 됩니다. 장치가 ADS 에 연결할 수 없으면 Secure Hub 는 장치 등록을 허용하지 않습니다. 따라서 내부 네트워크 내에서 ADS 액세스를 가능하게 하는 것은 장치가 등록될 수 있게 하는 데 매우 중요합니다.

Android 용 Secure Hub 에 대해 ADS 액세스를 허용하려면 다음 IP 주소 및 FQDN 으로 포트 443 을 엽니다.

FQDN	IP 주소	포트	IP 및 포트 사용
`discovery.mdm.zenprise.com`	52.5.138.94	443	Secure Hub - ADS 통신
`discovery.mdm.zenprise.com`	52.1.30.122	443	Secure Hub - ADS 통신

FQDN	IP 주소	포트	IP 및 포트 사용
`ads.xm.cloud.com`: Secure Hub 버전 10.6.15 이상은 다음 사용: `ads.xm.cloud.com`.	34.194.83.188	443	Secure Hub - ADS 통신
`ads.xm.cloud.com`: Secure Hub 버전 10.6.15 이상은 다음 사용: `ads.xm.cloud.com`.	34.193.202.23	443	Secure Hub - ADS 통신

인증서 고정이 사용 설정된 경우:

- Secure Hub 는 장치 등록 중에 엔터프라이즈 인증서를 고정합니다.
- 업그레이드 중에 Secure Hub 는 현재 고정되어 있는 인증서를 폐기한 후 등록된 사용자의 첫 번째 연결에서 서버 인증서를 고정합니다.

  > 참고:
  >
  > 업그레이드 이후 인증서 고정을 사용하도록 설정한 경우 사용자가 다시 등록해야 합니다.

- 인증서 공개 키가 변경되지 않은 경우 인증서 갱신에는 재등록이 필요하지 않습니다.

인증서 고정은 중간 또는 발급자 인증서가 아니라 리프 인증서를 지원합니다. 인증서 고정은 타사 서버가 아니라 Endpoint Management 및 Citrix Gateway 등의 Citrix 서버에 적용됩니다.

계정 삭제 옵션 비활성화

ADS(자동 검색 서비스) 가 사용 설정된 환경에서 Secure Hub 의 계정 삭제 옵션을 사용 중지할 수 있습니다.

계정 삭제 옵션을 사용 중지하려면 다음 단계를 수행하십시오.

1. 도메인의 ADS 를 구성합니다.
2. Citrix Endpoint Management 에서 자동 검색 서비스 정보를 열고 `displayReenrollLink` 값을 **False** 로 설정합니다.
   기본적으로 이 값은 **True** 입니다.
3. 장치가 MDM+MAM(ENT) 모드로 등록된 경우 로그오프한 후 다시 로그인하여 변경 사항을 적용하십시오.
   장치가 다른 모드로 등록되어 있는 경우 다시 등록해야 합니다.

Secure Hub 사용

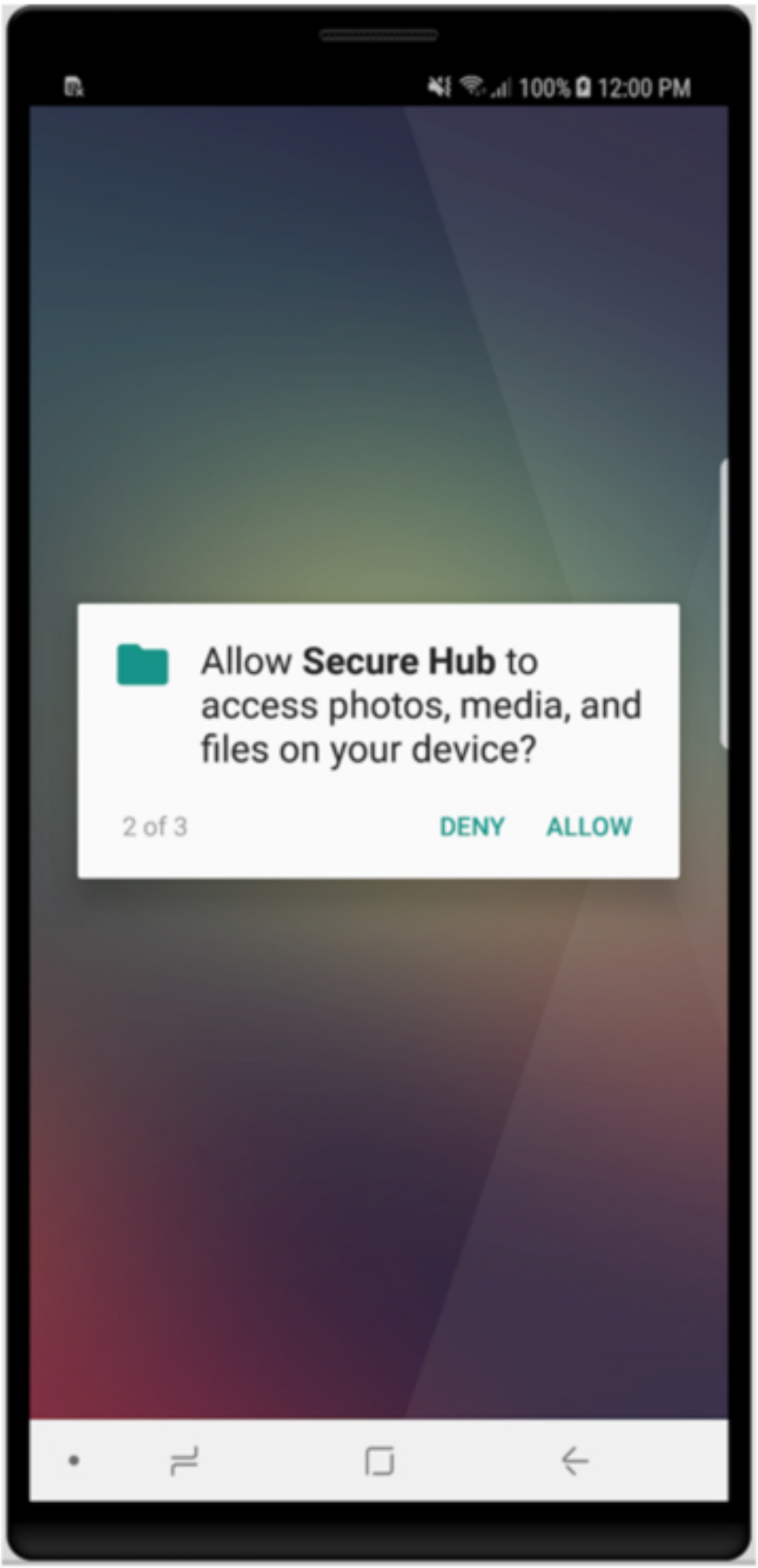
사용자는 먼저 Apple 또는 Android 스토어에서 장치로 Secure Hub 를 다운로드합니다.

Secure Hub 가 열리면 사용자는 회사에서 제공한 자격 증명을 입력하여 Secure Hub 에 장치를 등록합니다. 장치 등록에 대한 자세한 내용은 사용자, 계정, 역할 및 등록을 참조하십시오.

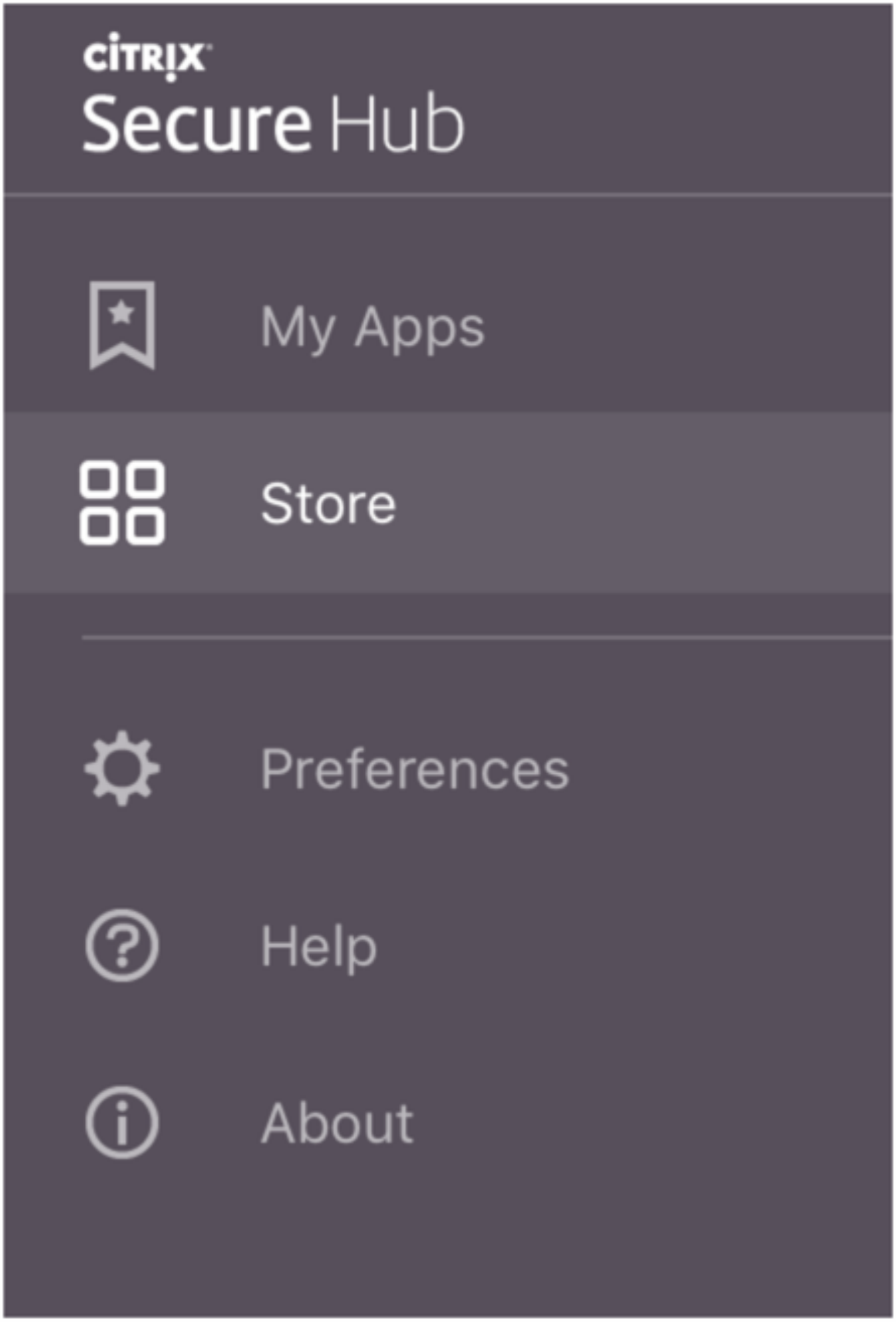
Android 용 Secure Hub 에서 초기 설치 및 등록 시 다음 메시지가 나타납니다. "Allow Secure Hub to access photos, media, and files on your device?(Secure Hub 가 장치의 사진, 미디어 및 파일에 액세스하도록 허용하시겠습니까?)"

이 메시지는 Citrix 가 아닌 Android 운영 체제의 메시지입니다. **Allow(**허용**)** 을 탭하더라도 Citrix 와 Secure Hub 를 관리하는 관리자가 사용자의 개인 데이터를 아무 때나 보는 것은 아닙니다. 하지만 관리자와 원격 지원 세션을 수행하는 경우 관리자가 세션 내에서 사용자의 개인 파일을 볼 수 있습니다.

등록된 후에 사용자는 내 앱 탭에서 푸시한 앱 및 데스크톱을 볼 수 있습니다. 사용자는 저장소의 앱을 더 추가할 수 있습니다. 전화기에서 저장소 링크는 왼쪽 맨 위의 설정 햄버거 아이콘 아래에 있습니다.



태블릿에서는 저장소가 별도 탭입니다.



iOS 9 이상을 실행하는 iPhone 사용자가 스토어에서 모바일 생산성 앱을 설치할 경우 Enterprise 개발자인 Citrix 는 해당 iPhone 에서 신뢰되지 않는다는 메시지가 표시됩니다. 이 메시지는 개발자가 신뢰될 때까지 해당 앱을 사용할 수 없음을 나타냅니다. 이 메시지가 나타나면 Secure Hub 는 Citrix 엔터프라이즈 앱이 iPhone 에서 신뢰되도록 하는 과정을 안내하는 가이드를 살펴볼 것을 사용자에게 요청합니다.

Secure Mail 에 자동 등록

MAM 전용 배포의 경우, 전자 메일 자격 증명을 사용하여 Secure Hub 에 등록한 Android 또는 iOS 장치 사용자가 자동으로 Secure Mail 에서 등록되도록 Endpoint Management 를 구성할 수 있습니다. 따라서 Secure Mail 에서 등록하기 위해 사용자가 더 많은 정보를 입력하거나 더 많은 절차를 거치지 않아도 됩니다.

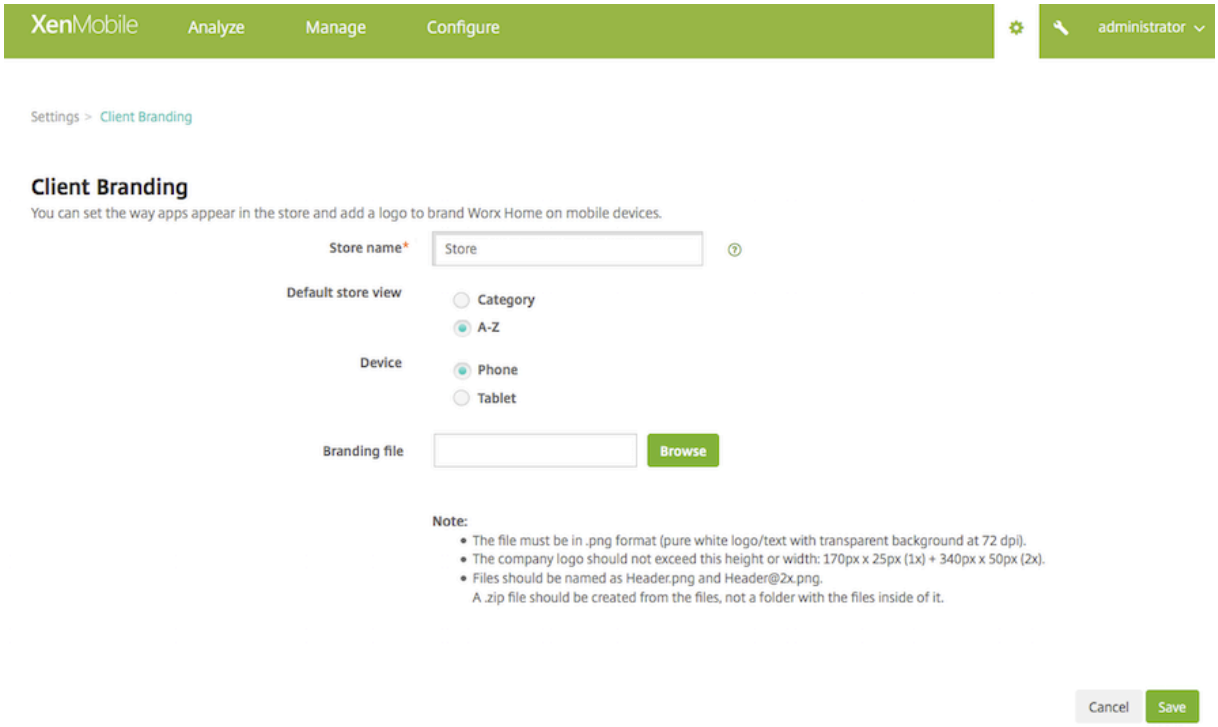
Secure Mail 을 처음 사용할 때 Secure Mail 은 사용자의 전자 메일 주소, 도메인 및 사용자 ID 를 Secure Hub 로부터 얻습니다. Secure Mail 은 전자 메일 주소를 자동 검색에 사용합니다. Exchange Server 는 도메인 및 사용자 ID 를 사용하여 식별되고, 이를 통해 Secure Mail 이 사용자를 자동으로 인증할 수 있습니다. 암호를 전달하지 못하도록 정책이 설정된 경우 암호를 입력하라는 메시지가 사용자에게 표시됩니다. 하지만 사용자는 이외의 정보를 입력하지 않아도 됩니다.

이 기능을 사용 설정하려면 다음 세 가지 속성을 생성합니다.

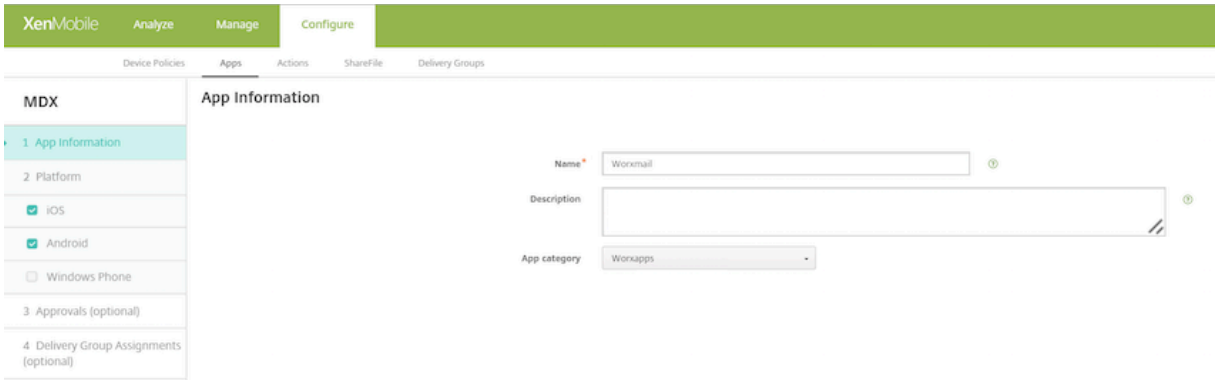
- 서버 속성 MAM_MACRO_SUPPORT. 지침은 서버 속성을 참조하십시오.
- 클라이언트 속성 ENABLE_CREDENTIAL_STORE 및 SEND_LDAP_ATTRIBUTES. 지침은 클라이언트 속성을 참조하십시오.

사용자 지정된 스토어

저장소를 사용자 지정하려면 설정 **>** 클라이언트 브랜딩으로 이동하여 이름을 변경하고 로고를 추가하고 앱 표시 방식을 지정합니다.



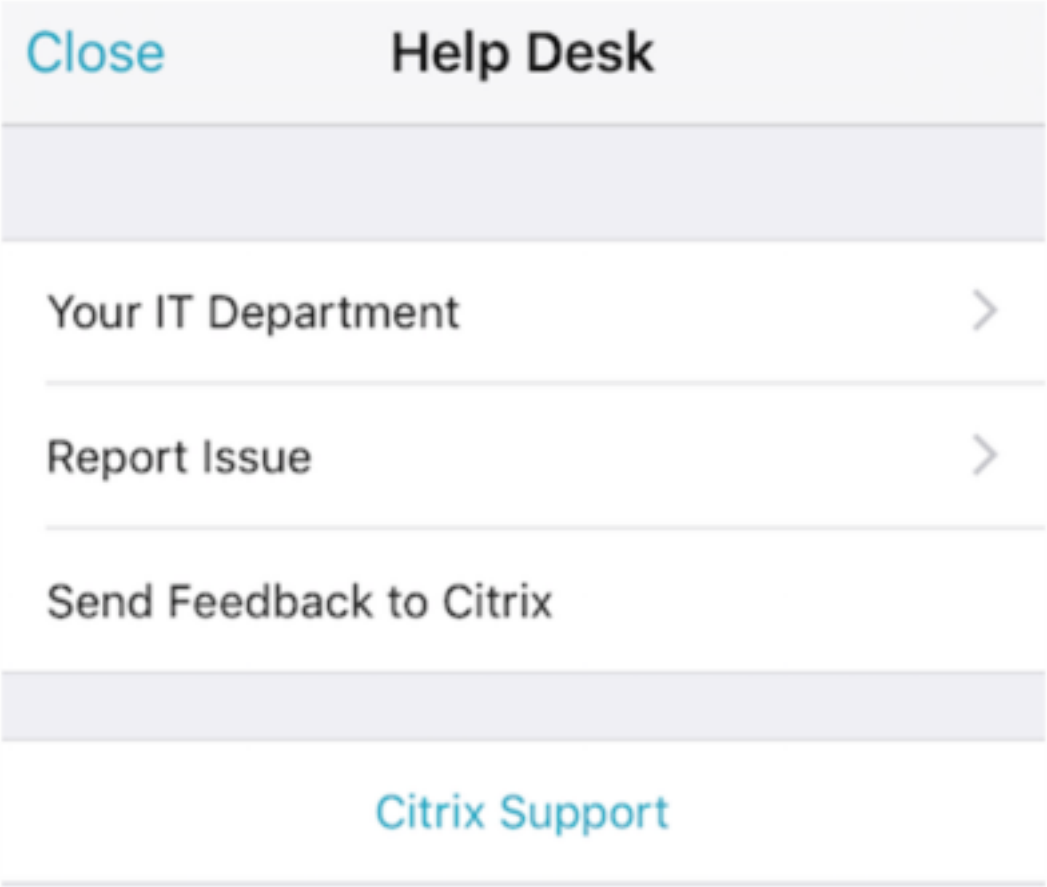
Endpoint Management 콘솔에서 앱 설명을 편집할 수 있습니다. 구성을 클릭한 후 앱을 클릭합니다. 테이블에서 앱을 선택하고 편집을 클릭합니다. 설명을 편집할 앱의 플랫폼을 선택하고 설명 상자에 텍스트를 입력합니다.



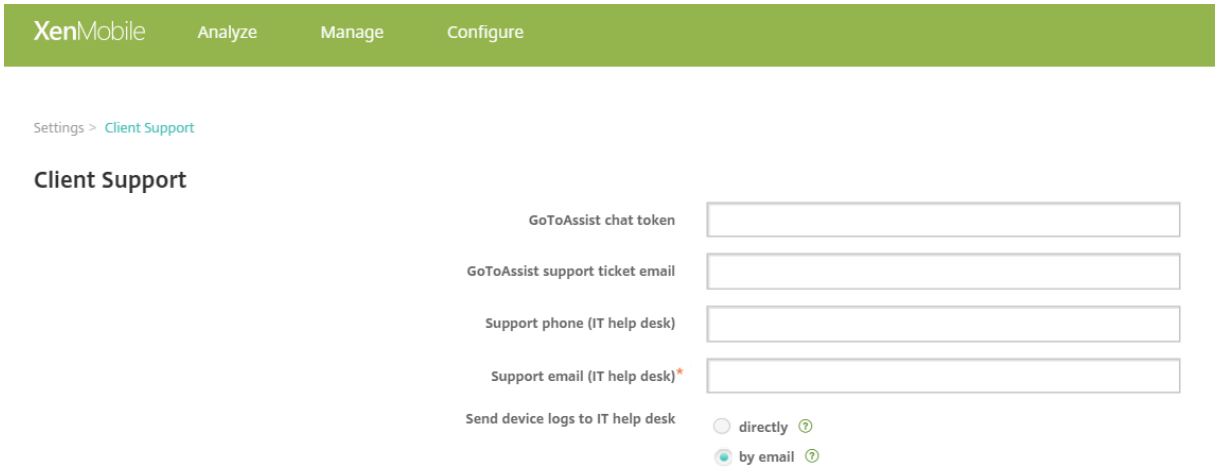
스토어에서 사용자는 Endpoint Management 에서 구성되고 보안된 앱 및 데스크톱만 찾아볼 수 있습니다. 앱을 추가하려면 사용자가 세부 정보를 누른 후 추가를 누릅니다.

구성된 도움말 옵션

또한 Secure Hub 는 도움을 받을 수 있는 다양한 방법을 사용자에게 제공합니다. 태블릿에서 오른쪽 위 모서리에 있는 물음표를 누르면 도움말 옵션이 열립니다. 전화기에서는 사용자가 왼쪽 위 모서리의 햄버거 메뉴 아이콘을 누른 후 도움말을 누릅니다.



IT 부서에는 사용자가 앱에서 바로 액세스할 수 있는 회사 지원 센터의 전화 및 전자 메일이 표시됩니다. 전화 번호 및 전자 메일 주소를 Endpoint Management 콘솔에 입력하십시오. 오른쪽 위 모서리에서 기어 아이콘을 클릭합니다. 설정 페이지가 나타납니다. 더 보기를 클릭하고 클라이언트 지원을 클릭합니다. 정보를 입력하는 화면이 나타납니다.



문제 보고에 앱 목록이 표시됩니다. 사용자가 문제 있는 앱을 선택합니다. Secure Hub 는 로그를 자동으로 생성한 후 로그가 zip 파일로 첨부된 메시지를 Secure Mail 에서 엽니다. 사용자가 제목 줄 및 문제에 대한 설명을 추가합니다. 스크린샷도 첨부

할 수 있습니다.

Citrix 에 피드백 보내기는 Citrix 지원 팀 주소가 채워진 메시지를 Secure Mail 에서 엽니다. 메시지 본문에서 사용자는 Secure Mail 개선을 위한 제안을 입력할 수 있습니다. Secure Mail 이 장치에 설치되지 않은 경우 기본 메일 프로그램이 열립니다.

사용자는 **Citrix** 지원을 눌러 Citrix Knowledge Center를 열 수도 있습니다. 여기에서 모든 Citrix 제품에 대한 지원 문서를 검색할 수 있습니다.

기본 설정에서는 사용자가 자신의 계정 및 장치에 대한 정보를 찾을 수 있습니다.

위치 정책

또한 Secure Hub 는 회사 소유 장치가 특정 지리적 경계선을 벗어나지 못하게 하려는 경우 등에 지역 위치 및 지역 추적 정책을 제공합니다. 자세한 내용은 위치 장치 정책을 참조하십시오.

충돌 수집 및 분석

Secure Hub 는 실패 정보를 자동으로 수집 및 분석하므로 특정 실패의 원인이 무엇인지 파악할 수 있습니다. Crashlytics 소프트웨어는 이 기능을 지원합니다.

iOS 및 Android 에서 사용할 수 있는 추가 기능은 Citrix Secure Hub의 플랫폼별 기능 매트릭스를 참조하십시오.

Secure Hub 의 장치 측 로그 생성

이 섹션에서는 Secure Hub 장치 측 로그를 생성하고 해당 로그에 올바른 디버그 수준을 설정하는 방법을 설명합니다.

Secure Mail 로그를 획득하려면 다음을 수행하십시오.

1. **Secure Hub >** 도움말 **>** 문제 보고로 이동합니다. 앱 목록에서 Secure Mail 을 선택합니다.
   해당 조직의 지원 센터로 보내지는 전자 메일이 열립니다.
2. 로그 설정은 지원 팀의 지시가 있는 경우에만 변경합니다. 설정이 올바르게 설정되었는지 항상 확인하십시오.
3. Secure Mail 로 돌아가서 문제를 재현하십시오. 문제가 재현되기 시작한 시간과 문제가 발생하거나 오류 메시지가 표시되는 시간을 기록해 둡니다.
4. **Secure Hub >** 도움말 **>** 문제 보고로 돌아갑니다. 앱 목록에서 Secure Mail 을 선택합니다.
   해당 조직의 지원 센터로 보내지는 전자 메일이 열립니다.
5. 문제에 대해 설명하는 몇 개의 단어로 제목 줄 및 본문을 채웁니다. 3 단계에서 수집한 타임스탬프를 포함하고 보내기를 클릭합니다.
   압축된 로그 파일이 첨부된 상태로 완성된 메시지가 열립니다.
6. 보내기를 다시 클릭합니다.

   전송되는 zip 파일에는 다음 로그가 포함되어 있습니다.

- CtxLog_AppInfo.txt(iOS), Device_And_AppInfo.txt(Android), logx.txt 및 WH_logx.txt(Windows Phone)

앱 정보 로그에는 장치 및 앱에 대한 정보가 포함됩니다.

Secure Mail 개요

June 6, 2024

Citrix Secure Mail 을 통해 사용자는 휴대폰 및 태블릿에서 전자 메일, 일정 및 연락처를 관리할 수 있습니다. Microsoft Outlook 또는 IBM Notes 계정으로부터 연속성이 유지되도록 Secure Mail 은 Microsoft Exchange Server 및 IBM Notes Traveler 서버와 동기화됩니다.

Citrix 앱 제품군의 하나인 Secure Mail 은 Citrix Secure Hub 와의 SSO(Single Sign-On) 호환성을 갖습니다. 사용자는 Secure Hub 에 로그온한 후 사용자 이름 및 암호를 다시 입력할 필요 없이 Secure Mail 로 매끄럽게 이동할 수 있습니다. 사용자의 장치가 Secure Hub 에 등록될 때 해당 장치로 Secure Mail 이 자동으로 푸시되도록 구성하거나 사용자가 Store 에서 이 앱을 추가할 수 있습니다.

> **참고:**
>
> Exchange Server 2010 에 대한 지원은 2020 년 10 월 13 일에 종료되었습니다.

Secure Mail 은 다음과 호환됩니다.

- Exchange Server 2019 누적 업데이트 14
- Exchange Server 2019 누적 업데이트 13
- Exchange Server 2019 누적 업데이트 12
- Exchange Server 2019 누적 업데이트 11
- Exchange Server 2019 누적 업데이트 10
- Exchange Server 2019 누적 업데이트 9
- Exchange Server 2019 누적 업데이트 8
- Exchange Server 2019 누적 업데이트 7
- Exchange Server 2019 누적 업데이트 6
- Exchange Server 2016 누적 업데이트 23
- Exchange Server 2016 누적 업데이트 22
- Exchange Server 2016 누적 업데이트 21
- Exchange Server 2016 누적 업데이트 20
- Exchange Server 2016 누적 업데이트 19
- Exchange Server 2016 누적 업데이트 18
- Exchange Server 2016 누적 업데이트 17
- Exchange Server 2013 누적 업데이트 23

- Exchange Server 2013 누적 업데이트 22
- Exchange Server 2013 누적 업데이트 21
- HCL Domino 버전 12.0.2 FP2
- HCL Traveler 버전 12.0.2.1 빌드 202302010413_30
- HCL Domino 11(이전의 Lotus Notes)
- HCL Domino 10.0.1(이전의 Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197(이전의 Lotus Notes)
- HCL Domino 10.0.1.0 build 201811191126_20(이전의 Lotus Notes)
- HCL Domino 9.0.1.21(이전의 Lotus Notes)
- Microsoft Office 365(Exchange Online)

먼저 Secure Mail 및 기타 Endpoint Management 구성 요소를 Citrix Endpoint Management 다운로드에서 다운로드합니다.

Secure Mail 및 기타 모바일 앱 시스템 요구 사항은 시스템 요구 사항을 참조하십시오.

앱이 백그라운드에서 실행되고 있거나 닫힌 경우 iOS 및 Android 용 Secure Mail 의 알림에 대한 내용은 Secure Mail 을 위한 푸시 알림을 참조하십시오.

Secure Mail 에서 지원되는 iOS 기능은 Secure Mail 의 iOS 기능을 참조하십시오.

Secure Mail 에서 지원되는 Android 기능은 Secure Mail 의 Android 기능을 참조하십시오.

Secure Mail 에서 지원되는 iOS 및 Android 기능은 Secure Mail 의 iOS 및 Android 기능을 참조하십시오.

사용자 도움말 설명서는 Citrix User Help Center 의 Citrix Secure Mail 페이지를 참조하십시오.

Citrix Secure Web

July 18, 2023

Citrix Secure Web 은 내부 및 외부 사이트에 대한 보안 액세스를 제공하는 HTML5 호환 모바일 웹 브라우저입니다. 사용자의 장치가 Secure Hub 에 등록될 때 해당 장치로 Secure Web 이 자동으로 푸시되도록 구성할 수 있습니다. 또는 Endpoint Management 앱 스토어에서 앱을 추가할 수 있습니다.

Secure Web 및 기타 모바일 생산성 앱 시스템 요구 사항은 시스템 요구 사항을 참조하십시오.

Secure Web 통합 및 제공

> 참고:
>
> MDX Toolkit 10.7.10 은 모바일 생산성 앱의 래핑을 지원하는 마지막 릴리스입니다. 사용자는 공용 앱 스토어에서 모바일 생산성 앱 버전 10.7.5 이상에 액세스할 수 있습니다.

Secure Web 을 통합하여 제공하려면 다음 일반 단계를 따르십시오.

1. 내부 네트워크에 대한 SSO(Single Sign-on) 를 사용하도록 Citrix Gateway 를 구성합니다.

   HTTP 트래픽의 경우, Citrix ADC 는 Citrix ADC 에 의해 지원되는 모든 프록시 인증 유형에 대해 SSO 를 제공할 수 있습니다. HTTPS 트래픽의 경우, 웹 암호 캐싱 정책으로 Secure Web 이 인증할 수 있고 MDX 를 통해 프록시 서버에 SSO 를 제공할 수 있습니다. MDX 는 기본, 다이제스트 및 NTLM 프록시 인증만 지원합니다. 암호는 MDX 를 사용하여 캐싱되고 민감한 앱 데이터의 보안 스토리지 영역인 Endpoint Management 공유 저장소에 저장됩니다. Citrix Gateway 구성에 대한 자세한 내용은 Citrix Gateway를 참조하십시오.

2. Secure Web 을 다운로드합니다.

3. 내부 네트워크에 대한 사용자 연결을 어떻게 구성할지 결정합니다.

4. 다른 MDX 앱과 동일한 절차에 따라 Secure Web 을 Endpoint Management 에 추가한 다음 MDX 정책을 구성합니다. Secure Web 관련 정책에 대한 자세한 내용은 이 문서 뒷부분에 있는 "Secure Web 정책 정보" 를 참조하십시오.

사용자 연결 구성

Secure Web 은 다음과 같은 사용자 연결 구성을 지원합니다.

- 터널링됨—웹 **SSO:** 내부 네트워크로 터널링되는 연결은 터널링됨—웹 SSO 라고 하는 클라이언트 없는 VPN 의 변형을 사용할 수 있습니다. 이는 기본 설정 **VPN** 모드 정책에 대해 지정된 기본 구성입니다. SSO(Single Sign-On) 가 필요한 연결에 대해 터널링됨 - 웹 SSO 를 사용하는 것이 좋습니다.
- 전체 **VPN** 터널**:** 내부 네트워크로 터널링되는 연결은 기본 설정 **VPN** 모드 정책에 의해 구성된 전체 VPN 터널을 사용할 수 있습니다. 클라이언트 인증서 또는 종단 간 SSL 을 사용하여 내부 네트워크의 리소스로 연결되는 경우 전체 VPN 터널을 사용하는 것이 좋습니다. 그러나 Secure Web 은 모바일 장치에 저장된 클라이언트 인증서를 읽을 수 있는 앱이 아닙니다. 이 기능을 제공할 수 있는 래핑된 타사 엔터프라이즈 앱을 설치할 수 있습니다. 전체 VPN 터널은 TCP 기반의 모든 프로토콜을 처리하고, Windows 및 Mac 컴퓨터뿐 아니라 iOS 및 Android 장치에서도 사용될 수 있습니다.
- **VPN** 모드 전환 허용 정책은 필요에 따라 전체 VPN 터널 모드와 터널링됨 - 웹 SSO 모드 간의 자동 전환을 허용합니다. 기본적으로 이 정책은 꺼져 있습니다. 이 정책이 켜진 경우, 기본 설정 VPN 모드에서 처리할 수 없는 인증 요청으로 인해 실패한 네트워크 요청은 다른 모드에서 다시 시도됩니다. 예를 들어 전체 VPN 터널 모드에서는 클라이언트 인증서에 대한 서버 챌린지를 수용할 수 있지만 터널링됨 - 웹 SSO 모드에서는 수용할 수 없습니다. 마찬가지로 HTTP 인증 챌린지는 터널링됨 - 웹 SSO 모드를 사용할 경우에 SSO 로 더 쉽게 서비스될 수 있습니다.

다음 표에서는 구성 및 사이트 유형별로 Secure Web 이 사용자에게 자격 증명을 요구하는지 여부를 설명합니다.

연결 모드	사이트 유형	암호 캐싱	Citrix Gateway 에 대해 구성된 SSO	처음 웹 사이트에 액세스할 경우 Secure Web 이 자격 증명 묻기	이후에 웹 사이트에 액세스할 경우 Secure Web 이 자격 증명 묻기	암호 변경 후 Secure Web 이 자격 증명 묻기
터널링됨 - 웹 SSO	HTTP	아니요	예	아니요	아니요	아니요
터널링됨 - 웹 SSO	HTTPS	아니요	예	아니요	아니요	아니요
전체 VPN	HTTP	아니요	예	아니요	아니요	아니요
전체 VPN	HTTPS	예: Secure Web MDX 정책인 웹 암호 캐싱 사용 설정이 켜짐인 경우	아니요	예: 자격 증명을 Secure Web 에 캐싱하는 데 필요함	아니요	예

Secure Web 정책

Secure Web 을 추가할 경우, Secure Web 과 관련된 다음 MDX 정책에 유의하십시오. 지원되는 모든 모바일 장치에 해당:

허용 또는 차단된 웹 사이트

일반적으로 Secure Web 은 웹 링크를 필터링하지 않습니다. 이 정책을 사용하면 허용 또는 차단된 사이트의 구체적인 목록을 구성할 수 있습니다. 쉼표로 구분된 목록 형식의 URL 패턴을 구성하여 브라우저에서 열 수 있는 웹 사이트를 제한할 수 있습니다. 목록의 각 패턴 앞에는 더하기 기호 (+) 또는 빼기 기호 (-) 가 올 수 있습니다. 브라우저가 일치 항목이 발견될 때까지 나열된 순서대로 URL 을 패턴과 비교합니다. 일치 항목이 발견되면 다음과 같이 접두사에 따라 작업이 결정됩니다.

- 빼기 (-) 접두사가 있으면 브라우저에서 URL 을 차단합니다. 이 경우 URL 은 웹 서버 주소를 확인할 수 없는 것처럼 처리됩니다.
- 더하기 (+) 접두사가 있으면 URL 이 정상적으로 처리됩니다.
- 패턴에 + 또는 - 접두사가 없는 경우에는 +(허용) 로 간주됩니다.
- URL 과 일치하는 패턴이 목록에 없는 경우 URL 이 허용됩니다.

다른 모든 URL 을 차단하려면 목록의 끝에 빼기 기호와 별표 (-*) 를 추가합니다. 예:

- 정 책 값 `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*`는 `mycorp.com` 도메인 내의 HTTP URL 을 허용하고 그 외 다른 위치의 URL 은 차단하며, 모든 위치의 HTTPS 및 FTP URL 은 허용하고 다른 모든 URL 은 차단합니다.

- 정책 값 `+http://*.training.lab/*,+https://*.training.lab/*,-*`는 사용자가 Training.lab 도메인 (인트라넷) 의 모든 사이트를 HTTP 또는 HTTPS 를 통해 여는 것을 허용합니다. 그러나 프로토콜에 관계없이 Facebook, Google 및 Hotmail 과 같은 공용 URL 을 열 수 없습니다.

기본값은 비어 있습니다 (모든 URL 이 허용됨).

팝업 차단

팝업은 사용자의 허가 없이 웹사이트가 열 수 있는 새 탭입니다. 이 정책은 Secure Web 에서 팝업을 허용할지 여부를 결정합니다. 켜짐인 경우, Secure Web 은 웹사이트가 팝업을 열지 못하게 합니다. 기본값은 꺼짐입니다.

미리 로드된 책갈피

Secure Web 브라우저에 대해 미리 로드되는 책갈피 집합을 정의합니다. 이 정책은 폴더 이름, 식별 이름 및 웹 주소를 포함하는 튜플이 쉼표로 구분되어 있는 목록입니다. 각 목록은 폴더, 이름, URL 형식이어야 하며 이름은 선택적으로 큰따옴표 (“) 로 묶일 수 있습니다.

예를 들어, 정책 값 `,"Mycorp, Inc. home page",https://www.mycorp.com, "MyCorp Links",Account logon,https://www.mycorp.com/Accounts "MyCorp Links/Investor Relations","Contact us",https://www.mycorp.com/IR/Contactus.aspx`는 3 개의 책갈피를 정의합니다. 첫 번째는 “Mycorp, Inc. home page” 라는 이름의 기본 링크 (폴더 이름 없음) 입니다. 두 번째 링크는 “MyCorp Links” 라는 이름의 폴더에 배치되고 “Account logon” 이라는 레이블이 지정됩니다. 세 번째는 “MyCorp Links” 폴더의 “Investor Relations” 하위 폴더에 배치되고 “Contact us” 로 표시됩니다.

기본값은 비어 있습니다.

홈 페이지 **URL**

Secure Web 을 시작할 때 로드할 웹 사이트를 정의합니다. 기본값은 비어 있습니다 (기본 시작 페이지).

지원되는 Android 및 iOS 장치에만 해당:

브라우저 사용자 인터페이스

Secure Web 에 대해 브라우저 사용자 인터페이스 컨트롤의 동작 및 가시성을 지정합니다. 일반적으로 모든 탐색 컨트롤을 사용할 수 있습니다. 앞으로, 뒤로, 주소 표시줄 및 새로 고침/중지 컨트롤이 여기에 포함됩니다. 이러한 컨트롤 중 일부의 용도 및 가시성을 제한하기 위해 이 정책을 구성할 수 있습니다. 기본값은 모든 컨트롤을 표시하는 것입니다.

옵션

- 모든 컨트롤 표시. 모든 컨트롤을 볼 수 있고 사용자는 제한 없이 이러한 컨트롤을 사용할 수 있습니다.
- 읽기 전용 주소 표시줄. 모든 컨트롤을 볼 수 있지만 사용자가 브라우저 주소 필드를 편집할 수는 없습니다.
- 주소 표시줄 숨기기. 주소 표시줄을 숨기지만 다른 컨트롤은 숨기지 않습니다.
- 모든 컨트롤 숨기기. 전체 도구 모음이 표시되지 않도록 하여 프레임 없는 탐색 환경을 제공합니다.

웹 암호 캐싱 사용

웹 리소스를 액세스하거나 요청할 때 Secure Web 사용자가 자격 증명을 입력하는 경우, Secure Web 이 자동으로 암호를 장치에 캐싱하는지 여부를 이 정책이 결정합니다. 이 정책은 웹 양식에 입력한 암호가 아니라 인증 대화 상자에 입력한 암호에 적용됩니다.

켜짐인 경우, Secure Web 은 웹 리소스 요청 시에 사용자가 입력하는 모든 암호를 캐싱합니다. 꺼짐인 경우, Secure Web 은 암호를 캐싱하지 않고 기존의 캐싱된 암호를 제거합니다. 기본값은 꺼짐입니다.

이 앱에 대해 기본 VPN 정책을 전체 VPN 터널로 설정한 경우에만 이 정책을 사용하도록 설정됩니다.

프록시 서버

터널링됨 - 웹 SSO 모드에서 사용될 때 Secure Web 에 대해 프록시 서버를 구성할 수도 있습니다. 자세한 내용은 이 블로그 게시물을 참조하십시오.

DNS suffixes(DNS 접미사)

DNS 접미사가 구성되지 않은 경우 Android 에서 VPN 이 실패할 수도 있습니다. DNS 접미사 구성에 대한 자세한 내용은 Supporting DNS Queries by Using DNS Suffixes for Android Devices(Android 장치에 대해 DNS 접미사를 사용한 DNS 쿼리 지원)를 참조하십시오.

Secure Web 을 위한 인트라넷 사이트 준비

이 섹션은 Android 및 iOS 용 Secure Web 과 함께 사용할 인트라넷 사이트를 준비해야 하는 웹 사이트 개발자를 대상으로 합니다. 데스크톱 브라우저에 맞춰 설계된 인트라넷 사이트가 Android 및 iOS 장치에서 올바로 작동하려면 사이트를 변경해야 합니다.

Secure Web 은 Android WebView 및 iOS WkWebView 를 통해 웹 기술 지원을 제공합니다. Secure Web 에서 지원하는 일부 웹 기술은 다음과 같습니다.

- AngularJS
- ASP .NET
- JavaScript
- jQuery

- WebGL

Secure Web 에서 지원하지 않는 일부 웹 기술은 다음과 같습니다.

- Flash
- Java

다음 표에서는 Secure Web 에 대해 지원되는 HTML 렌더링 기능 및 기술을 보여 줍니다. X 는 플랫폼, 브라우저 및 구성 요소 조합에 기능을 사용할 수 있음을 나타냅니다.

기술	iOS Secure Web	Android 6.x/7.x Secure Web
JavaScript 엔진	JavaScriptCore	V8
로컬 스토리지	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
Navigation Timing API		X
Resource Timing API		X

기술은 여러 장치에 걸쳐 동일하게 작동하고, Secure Web 은 장치에 따라 서로 다른 사용자 에이전트 문자열을 반환합니다. Secure Web 에 사용되는 브라우저 버전을 확인하려면 사용자 에이전트 문자열을 보면 됩니다. Secure Web 에서 https://whatsmyuseragent.com/으로 이동합니다.

인트라넷 사이트 문제 해결

인트라넷 사이트를 Secure Web 에서 볼 때의 렌더링 문제를 해결하려면 Secure Web 및 호환되는 타사 브라우저에서 웹 사이트가 어떻게 렌더링되는지 비교합니다.

iOS 의 경우 테스트와 호환되는 타사 브라우저는 Chrome 및 Dolphin 입니다.

Android 의 경우 테스트와 호환되는 타사 브라우저는 Dolphin 입니다.

> 참고:
>
> Chrome 은 Android 에서 기본 브라우저입니다. 이 브라우저를 비교 작업에 사용하지 마십시오.

iOS 의 경우 브라우저에 장치 수준 VPN 지원 기능이 있는지 확인하십시오. 설정 **> VPN > VPN** 구성 추가로 이동하여 장치에 VPN 을 구성할 수 있습니다.

또한 App Store 에서 다운로드할 수 있는 Citrix VPN,Cisco AnyConnect 또는 Pulse Secure 등의 VPN 클라이언트 앱을 사용할 수 있습니다.

- 웹 페이지가 두 브라우저에서 동일하게 렌더링되면 웹 사이트에 문제가 있는 것입니다. 사이트를 업데이트하고 OS 에 대해 사이트가 잘 작동하는지 확인합니다.
- Secure Web 에서만 웹 페이지에 문제가 나타나면 Citrix 지원 팀에 문의하여 지원 티켓을 엽니다. 테스트한 브라우저 및 OS 유형을 포함하여 문제 해결 절차를 제공하십시오. iOS 용 Secure Web 에 렌더링 문제가 있는 경우, 다음 절차에 설명된 대로 페이지의 웹 보관을 포함하십시오. 그러면 Citrix 에서 문제를 더 신속히 해결하는 데 도움이 됩니다.

웹 보관 파일을 생성하려면

macOS 10.9 이상에서 Safari 를 사용하면 웹 보관 파일 (읽기 목록이라고 함) 로 웹 페이지를 저장할 수 있습니다. 웹 보관 파일에는 이미지, CSS 및 JavaScript 와 같은 모든 연결된 파일이 포함됩니다.

1. Safari 에서 읽기 목록 폴더를 비우고 **Finder** 에서 메뉴 표시줄에 있는 이동 메뉴를 클릭하고 폴더로 이동을 선택한 후, 경로 이름 ~/Library/Safari/ReadingListArchives/를 입력하고 해당 위치에 있는 모든 폴더를 삭제합니다.
2. 메뉴 표시줄에서 **Safari >** 환경설정 **>** 고급으로 이동하고 메뉴 표시줄에서 개발자용 메뉴 보기를 사용하도록 설정합니다.
3. 메뉴 표시줄에서 개발 **>** 사용자 에이전트로 이동하고 Secure Web 사용자 에이전트를 입력합니다 (Mozilla/5.0 (iPad; CPU OS 8_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25).
4. Safari 에서 읽기 목록 (웹 보관 파일) 으로 저장할 웹 사이트를 엽니다.
5. 메뉴 표시줄에서 책갈피 **>** 읽기 목록에 추가로 이동합니다. 보관은 백그라운드에서 이루어지며 몇 분이 걸릴 수 있습니다.
6. 보관된 읽기 목록을 찾습니다. 메뉴 표시줄에서 보기 **>** 읽기 목록 사이드바 보기로 이동합니다.
7. 보관 파일을 확인합니다.
   - Mac 으로의 네트워크 연결을 끕니다.
   - 읽기 목록에서 웹 사이트를 엽니다.

     웹 사이트가 완전히 렌더링됩니다.
8. 보관 파일을 압축합니다. **Finder** 에서 메뉴 표시줄에 있는 이동 메뉴를 클릭하고 폴더로 이동을 선택한 후, 경로 이름 ~/Library/Safari/ReadingListArchives/를 입력합니다. 이제 임의의 16 진수 문자열이 파일 이름인 폴더를 압축합니다. 지원 티켓을 열 때 Citrix 지원 팀으로 이 파일을 보낼 수 있습니다.

Secure Web 기능

Secure Web 은 모바일 데이터 교환 기술을 활용해 전용 VPN 터널을 생성하여 사용자가 내부와 외부 웹 사이트 및 다른 모든 웹 사이트를 액세스할 수 있게 합니다. 조직의 정책으로 보안되는 환경에서 민감한 정보가 포함된 사이트도 여기에 포함됩니다.

Secure Web 을 Secure Mail 및 Citrix Files 와 통합하면 보안 Endpoint Management 컨테이너 내에서 원활한 사용자 환경이 제공됩니다. 통합 기능의 일부 예는 다음과 같습니다.

- 사용자가 **Mailto** 링크를 누르면 추가적인 인증을 요구하지 않고 새 전자 메일 메시지가 Citrix Secure Mail 에서 열립니다.
- iOS 에서는 **ctxmobilebrowser://**를 URL 의 앞에 삽입하여 기본 메일 앱으로부터 Secure Web 에 링크를 열 수 있습니다. 예를 들어 기본 메일 앱에서 `example.com`을 열려면 URL ctxmobilebrowser://example.com 을 사용합니다.
- 사용자가 전자 메일 메시지에서 인트라넷 링크를 클릭하면 Secure Web 이 추가적인 인증 없이 해당 사이트로 이동합니다.
- 사용자는 Secure Web 에서 웹으로부터 다운로드한 파일을 Citrix Files 에 업로드할 수 있습니다.

Secure Web 사용자는 다음 작업을 수행할 수도 있습니다.

- 팝업 차단.

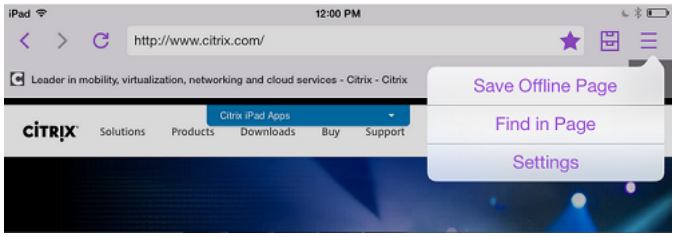
  > 참고:
  >
  > Secure Web 메모리의 많은 부분이 팝업 렌더링에 사용되므로 설정에서 팝업을 차단할 경우 보통 성능이 향상됩니다.

- 즐겨찾기 사이트를 책갈피로 지정합니다.
- 파일을 다운로드합니다.
- 페이지를 오프라인으로 저장합니다.
- 암호를 자동 저장합니다.
- 캐시/기록/쿠키를 지웁니다.
- 쿠키 및 HTML5 로컬 스토리지를 사용하지 않도록 설정합니다.
- 다른 사용자와 안전하게 장치를 공유합니다.
- 주소 표시줄 내에서 검색합니다.
- Secure Web 과 함께 실행되는 웹 앱이 위치에 액세스할 수 있도록 허용합니다.
- 설정을 내보내고 가져옵니다.
- 파일을 다운로드할 필요 없이 Citrix Files 에서 파일을 직접 엽니다. 이 기능을 사용하도록 설정하려면 Endpoint Management 에서 **ctx-sf**: 를 허용된 URL 정책에 추가합니다.
- iOS 에서 3D 터치 동작을 사용하여 새 탭을 열고 홈 화면에서 바로 오프라인 페이지, 즐겨찾기 사이트 및 다운로드에 액세스합니다.

- iOS 에서 모든 크기의 파일을 다운로드하고 Citrix Files 또는 다른 앱에서 파일을 엽니다.

  > 참고:
  >
  > Secure Web 을 백그라운드로 전환하면 다운로드가 중지됩니다.

- **Find in Page**(페이지에서 찾기) 를 사용하여 현재 페이지 보기 내에서 용어를 검색합니다.



Secure Web 에는 동적 텍스트 지원도 포함됩니다. 사용자가 장치에서 설정한 글꼴이 앱에 표시됩니다.

> 참고:
>
> - XenMobile 용 Citrix Files 는 2023 년 7 월 1 일에 EOL 에 도달했습니다. 자세한 내용은 EOL 및 더 이상 사용되지 않는 앱을 참조하십시오.

Citrix Content Collaboration for Endpoint Management

September 4, 2024

Citrix Content Collaboration for Endpoint Management 클라이언트는 MDX 기반의 Citrix Files 모바일 클라이언트 버전입니다. 이러한 클라이언트는 다른 MDX 래핑된 앱의 데이터에 대해 보안된 통합형 액세스를 제공합니다. 또한 Citrix Content Collaboration for Endpoint Management 클라이언트는 Micro VPN, Secure Hub SSO(Single Sign-On), 2 단계 인증 같은 MDX 기능을 활용할 수 있습니다.

Citrix Files 는 엔터프라이즈 파일 동기화 및 공유 서비스로서 사용자가 손쉽고 안전하게 문서를 교환할 수 있게 합니다. Citrix Files 는 Android 휴대폰용 Citrix Files 및 iPad 용 Citrix Files 등의 Citrix Files Mobile 클라이언트를 비롯하여 다양한 액세스 옵션을 사용자에게 제공합니다.

Citrix Files 를 Endpoint Management 와 통합하여 전체 Citrix Files 기능을 제공하거나 StorageZone 커넥터에 대한 액세스만 제공할 수 있습니다. 기본적으로 Citrix Endpoint Management 콘솔에서는 Citrix Files 만 구성할 수 있습니다. 대신 StorageZone 커넥터와 함께 사용하도록 Endpoint Management 를 구성하려면 Citrix Endpoint Management 설명서의 Citrix Content Collaboration 과 Endpoint Management 사용을 참조하십시오.

다음과 같이 Endpoint Management, Citrix Files, StorageZones Controller 및 Citrix ADC 를 사용하여 Citrix Content Collaboration for Endpoint Management 클라이언트를 배포하고 관리할 수 있습니다.

- Endpoint Management 가 Citrix Files 와 함께 구성된 경우 Endpoint Management 는 SAML IdP(ID 공급자) 역할을 하며 Citrix Content Collaboration for Endpoint Management 클라이언트를 배포합니다. Citrix

Files 데이터는 Citrix Files 에서 관리됩니다. Citrix Files 데이터는 Endpoint Management 를 통해 전달되지 않습니다.

- Endpoint Management 가 Citrix Files 또는 StorageZone 커넥터와 함께 구성된 경우 StorageZone Controller 에서 네트워크 공유 및 SharePoint 의 데이터에 연결해 줍니다. 사용자는 Citrix Files 모바일 생산성 앱을 통해 저장된 데이터에 액세스합니다. 사용자는 모바일 장치에서 Microsoft Office 문서를 편집하고, Adobe PDF 파일을 미리 보고, 주석을 달 수 있습니다.
- Citrix ADC 는 StorageZone 커넥터에 대한 보안 연결, 요청의 부하 분산 및 콘텐츠 스위칭 처리 등 외부 사용자의 요청을 관리합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트를 다운로드하려면 Citrix 다운로드를 참조하십시오.

Citrix Content Collaboration for Endpoint Management 및 기타 모바일 생산성 앱 시스템 요구 사항은 모바일 생산성 앱 지원을 참조하십시오.

Citrix Content Collaboration for Endpoint Management 클라이언트가 **Citrix Files** 모바일 클라이언트와 다른 점

Citrix Content Collaboration for Endpoint Management 클라이언트와 Citrix Files 모바일 클라이언트의 차이점은 다음과 같습니다.

사용자 액세스

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Secure Hub 에서 Citrix Content Collaboration for Endpoint Management 클라이언트를 가져와서 엽니다.

Citrix Files 모바일 클라이언트*:*

Citrix Files 모바일 클라이언트는 앱 스토어에서 가져옵니다.

SSO

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Endpoint Management 를 Citrix Files 와 통합하는 경우: Endpoint Management 를 Citrix Files 의 SAML IdP 로 구성할 수 있습니다. 이 구성에서는 Secure Hub 가 Endpoint Management 를 SAML IdP 로 사용하여 Citrix Content Collaboration for Endpoint Management 클라이언트를 위한 SAML 토큰을 얻습니다. Secure Hub 에 로그인하지 않고 Citrix Content Collaboration for Endpoint Management 클라이언트를 시작하면 Secure Hub 에 로그온하라는 메시지가 표시됩니다. 사용자가 Citrix Files 도메인 또는 계정 정보를 알아야 하는 것은 아닙니다.

Citrix Files 모바일 클라이언트*:*

Endpoint Management 및 Citrix Gateway 를 Citrix Files 의 SAML IdP 로 구성할 수 있습니다. 이 구성에서 웹 브라우저 또는 다른 Citrix Files 클라이언트를 사용하여 Citrix Files 에 로그온하는 사용자는 사용자 인증을 위해 Endpoint Management 환경으로 리디렉션됩니다. Endpoint Management 에 의해 성공적으로 인증된 후에 사용자는 Citrix Files 계정으로 로그온하는 데 유효한 SAML 토큰을 받게 됩니다.

Micro VPN

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

원격 사용자는 VPN 또는 Micro VPN 연결을 사용하여 Citrix Gateway 를 통해 연결하고 내부 네트워크의 앱 및 데스크톱에 액세스할 수 있습니다. Endpoint Management 와 Citrix ADC 의 통합을 통해 사용 가능한 이 기능은 자동으로 처리됩니다.

Citrix Files 모바일 클라이언트*:*

해당 없음.

2 단계 인증

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Endpoint Management 와의 Citrix ADC 통합은 클라이언트 인증서 인증과 다른 인증 유형 (예: LDAP 또는 RADIUS) 의 조합을 사용한 인증도 지원합니다.

Citrix Files 모바일 클라이언트*:*

해당 없음.

폴더 권한

Citrix Content Collaboration for Endpoint Management 클라이언트 및 *Citrix Files* 모바일 클라이언트*:*

Citrix Files 와 Endpoint Management 를 통합하는 경우: Citrix Files 에서 결정됩니다.

문서 액세스 보호

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

사용자는 Secure Mail 로 받거나 MDX 래핑된 앱에서 다운로드한 첨부 파일을 열 수 있습니다. 사용자가 열기 작업을 수행할 경우 MDX 래핑된 앱만 표시됩니다. 래핑되지 않은 앱의 데이터는 Citrix Content Collaboration for Endpoint Management 클라이언트에서 사용할 수 없습니다. Secure Mail 사용자는 파일을 장치로 다운로드할 필요 없이 Citrix Files 저장소로부터 파일을 첨부할 수 있습니다. 사용자의 장치에 래핑된 Citrix Files 및 래핑되지 않은 Citrix Files 가 있는 경우, 래핑된 Citrix Files 클라이언트는 사용자의 개인 Citrix Files 계정에 있는 파일에 액세스할 수 없습니다. 래핑된 Citrix Files 클라이언트는 Endpoint Management 에 구성된 Citrix Files 하위 도메인에만 액세스할 수 있습니다.

Citrix Files 모바일 클라이언트*:*

사용자가 모든 앱에서 첨부 파일을 열 수 있습니다.

Citrix Files 계정 액세스

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Citrix Files 와 Endpoint Management 를 통합하는 경우: 개인 Citrix Files 계정 또는 타사 Citrix Files 계정에 액세스하려면 해당 장치에서 비 MDX 버전의 Citrix Files 를 사용해야 합니다.

Citrix Files 모바일 클라이언트*:*

Citrix Files 와 Endpoint Management 를 통합하는 경우: Citrix Files 클라이언트에서 사용할 수 있습니다.

장치 정책

Citrix Content Collaboration for Endpoint Management 클라이언트 및 *Citrix Files* 모바일 클라이언트*:*

Endpoint Management 와 Citrix Files 장치 정책이 모두 Citrix Content Collaboration for Endpoint Management 클라이언트에 적용됩니다. 예를 들어 Endpoint Management 콘솔에서 장치 초기화를 수행할 수 있습니다. Citrix Files 콘솔에서 Citrix Files 앱을 원격으로 초기화할 수 있습니다.

MDX 정책

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

MDX 정책을 통해 Endpoint Management 앱 스토어가 적용할 Citrix Endpoint Management 설정을 구성할 수 있습니다. MDX 를 통해서만 사용 가능한 정책은 카메라, 마이크, 전자 메일 작성, 화면 캡처 및 클립보드 잘라내기, 복사 및 붙여넣기 작업을 차단할 수 있는 기능을 포함합니다.

Citrix Files 모바일 클라이언트*:*

해당 없음.

데이터 암호화

Citrix Content Collaboration for Endpoint Management 클라이언트 및 *Citrix Files* 모바일 클라이언트*:*

저장된 모든 데이터를 AES-256 를 사용하여 암호화하고 전송 중인 데이터를 SSL 3.0 및 128 비트 이상의 암호화를 사용하여 보호합니다.

상태

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Citrix Content Collaboration for Endpoint Management 클라이언트는 Endpoint Management Advanced 및 Enterprise Edition 에 포함되어 있습니다.

Citrix Files 모바일 클라이언트*:*

모든 Endpoint Management Edition 에 모든 Citrix Files 기능이 포함되어 있습니다. Endpoint Management 를 전체 Citrix Files 기능과 통합하거나 StorageZone 커넥터와만 통합할 수 있습니다.

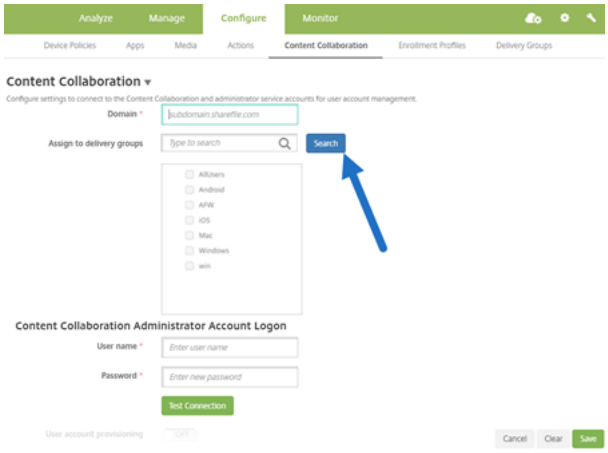
Citrix Content Collaboration for Endpoint Management 클라이언트 통합 및 제공

Citrix Content Collaboration for Endpoint Management 클라이언트를 통합하여 제공하려면 다음 일반 단계를 따르십시오.

1. Citrix Files 클라이언트에서 Citrix Files 에 대한 SSO 를 제공하도록 Endpoint Management 를 Citrix Files 의 SAML IdP 로 사용하도록 설정합니다. 이렇게 하려면 Endpoint Management 에서 Citrix Files 계정 정보를 구성해야 합니다. 자세한 내용은 "Endpoint Management 에서 SSO 에 Citrix Files 계정 정보를 구성하려면" 섹션을 참조하십시오.

   > 중요**:**
   >
   > Citrix Files 웹 앱 및 Citrix Files 동기화 클라이언트 같은 비 MDX Citrix Files 클라이언트를 위한 SAML IdP 로 Endpoint Management 를 사용하려는 경우 추가 구성이 필요합니다. 자세한 내용은 Citrix Files 지원 사이트에서
   >
   > Citrix Files(ShareFile) Single Sign-On SSO 문서를 참조하십시오. 이 문서에는 Endpoint Management 구성 가이드 다운로드 링크가 포함되어 있습니다.

2. Citrix Files 클라이언트를 다운로드합니다.
3. Citrix Files 클라이언트를 Endpoint Management 에 추가합니다. 자세한 내용은 이 문서에서 "Citrix Files 를 Endpoint Management 에 추가하려면" 을 참조하십시오.
4. 구성 유효성을 검사합니다. 자세한 내용은 이 문서의 뒷부분에서 "Citrix Files 클라이언트의 유효성을 검사하려면" 을 참조하십시오.



설정 정보**:**

- 도메인은 클라이언트에 대해 사용될 Citrix Files 하위 도메인입니다.
- 선택한 DG 의 사용자만 클라이언트에서 Citrix Files 로 SSO 액세스하게 됩니다.

  DG 의 사용자에게 Citrix Files 계정이 없는 경우 Citrix Files 클라이언트를 Endpoint Management 에 추가하면 Endpoint Management 가 Citrix Files 에 사용자를 프로비전합니다.
- Citrix Files 관리자 계정 로그온 정보는 SAML 설정을 Citrix Files 제어부에 저장하기 위해 Endpoint Management 에 의해 사용됩니다.

> 중요**:**
>
> Citrix Files 클라이언트부터 Citrix Files 까지 SSO 가 사용될 수 있게 하는 구성은 네트워크 공유 또는 SharePoint 문서 라이브러리에 사용자를 인증하지 않습니다. 이러한 커넥터 데이터 원본에 액세스하려면 네트워크 공유 또는 SharePoint Server 가 있는 Active Directory 도메인에 인증해야 합니다.

Endpoint Management 에서 **SSO** 에 **Citrix Files** 계정 정보를 구성하려면

Secure Hub 에서 모바일 생산성 앱에 대한 SSO 를 사용하려면 Endpoint Management 콘솔에서 Citrix Files 계정 및 Citrix Files 관리자 서비스 계정 정보를 지정합니다. 해당 구성에서 Endpoint Management 는 Citrix Files, 모바일 생산성 앱 클라이언트, Citrix Files 클라이언트 및 비 MDX Citrix Files 클라이언트를 위한 SAML IdP 역할을 합니다. 사용자가 모바일 생산성 앱 클라이언트를 시작하면 Secure Hub 가 Endpoint Management 에서 해당 사용자를 위한 SAML 토큰을 가져와서 Citrix Files 클라이언트로 보냅니다.

Endpoint Management 콘솔에서 구성 > Citrix Files 의 이전 명칭인 **Content Collaboration** 을 클릭합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트를 **Endpoint Management** 에 추가하려면

Citrix Content Collaboration for Endpoint Management 클라이언트를 Endpoint Management 에 추가하는 경우 Citrix Content Collaboration for Endpoint Management 클라이언트에서 커넥터 데이터 원본에 대한 SSO 액

세스를 사용하도록 설정할 수 있습니다. 그렇게 하려면 네트워크 액세스 정책 및 기본 설정 VPN 모드 정책을 이 섹션에 설명된 대로 구성합니다.

사전 요구 사항

- Endpoint Management 에서 Citrix Files 하위 도메인에 연결할 수 있어야 합니다. 연결을 테스트하려면 Endpoint Management 서버에서 Citrix Files 하위 도메인에 대한 Ping 을 수행합니다.
- Citrix Files 계정에 대해 구성된 표준 시간대와 Endpoint Management 를 실행하는 하이퍼바이저에 대해 구성된 표준 시간대가 같아야 합니다. 표준 시간대가 다르면 SAML 토큰이 예상한 기간 내에 Citrix Files 에 도달하지 못할 수 있기 때문에 SSO 요청이 실패할 수 있습니다. Endpoint Management 에 대한 NTP 서버를 구성하려면 Endpoint Management 명령줄 인터페이스를 사용합니다.

  > 참고**:**
  >
  > Linux VM 에서는 Hyper-V 호스트가 시간을 UTC 가 아닌 로컬 표준 시간대로 설정합니다.

- 관리자로 ShareFile 계정에 로그인하고 설정 > 관리자 설정 > 보안 > 로그인 및 보안 정책 > **Single Sign-on/SAML 2.0** 구성에서 SAML SSO 설정을 확인합니다.
- Citrix Content Collaboration for Endpoint Management 클라이언트를 다운로드합니다.

단계**:**

1. Endpoint Management 콘솔에서 구성 **>** 앱을 클릭한 후 추가를 클릭합니다.
2. **MDX** 를 클릭합니다.
3. 이름을 입력하고 필요에 따라 앱에 대해 설명 및 앱 범주를 입력합니다.
4. 다음을 클릭하고 Citrix Content Collaboration for Endpoint Management 클라이언트에 대한.mdx 파일을 업로드합니다.
5. 다음을 클릭하여 앱 정보 및 정책을 구성합니다.

   Citrix Content Collaboration for Endpoint Management 클라이언트에서 Citrix Files 로의 SSO 를 사용하는 구성은 네트워크 공유 또는 SharePoint 문서 라이브러리에 대해 사용자를 인증하지 않습니다.
6. Secure Hub Micro VPN 과 StorageZones Controller 사이에서 SSO 가 가능하도록 하려면 다음 정책 구성을 완료하십시오.

   - 네트워크 액세스 정책을 내부 네트워크로 터널링됨으로 설정합니다.

     이 모드에서는 MDX 프레임워크가 Citrix Content Collaboration for Endpoint Management 클라이언트에서 들어오는 모든 네트워크 트래픽을 가로챕니다. 네트워크 트래픽은 앱 전용 Micro VPN 을 사용하여 Citrix Gateway 를 통해 리디렉션됩니다.
   - 기본 설정 VPN 모드 정책을 터널링됨-웹 **SSO** 로 설정합니다.

이 터널링 모드에서는 MDX 프레임워크가 MDX 앱으로부터의 SSL/HTTP 트래픽을 종료하면 MDX 앱이 사용자를 위해 내부 네트워크로의 새 연결을 시작합니다. 이 정책 설정은 MDX 프레임워크가 웹 서버에서 발행된 인증 챌린지를 감지하고 이에 응답할 수 있게 합니다.

7. 승인 및 DG(배달 그룹) 할당을 필요에 따라 완료합니다.

선택된 DG 의 사용자만 Citrix Content Collaboration for Endpoint Management 클라이언트에서 SSO 를 사용하여 Citrix Files 에 액세스하게 됩니다. DG 의 사용자에게 Citrix Files 계정이 없는 경우 Citrix Content Collaboration for Endpoint Management 클라이언트를 Endpoint Management 에 추가하면 Endpoint Management 가 Citrix Files 에 사용자를 프로비전합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트의 유효성을 검사하려면

1. 이 문서에서 설명된 구성을 완료한 후에 Citrix Content Collaboration for Endpoint Management 클라이언트를 시작합니다. Citrix Files 에서 로그온 메시지를 표시하지 않습니다.
2. Secure Mail 에서 전자 메일을 작성하고 Citrix Files 첨부 파일을 추가합니다. 로그온 메시지 없이 Citrix Files 홈 페이지가 열립니다.

> 참고:
>
> - XenMobile 용 Citrix Files 는 2023 년 7 월 1 일에 EOL 에 도달했습니다. 자세한 내용은 EOL 및 더 이상 사용되지 않는 앱을 참조하십시오.

EOL 및 사용되지 않는 앱

June 6, 2024

다음 앱은 EOL(수명 종료) 에 도달했거나 EOL 상태에 도달합니다. 제품 릴리스가 EOL 에 도달한 경우 제품 라이센스 계약 기간 내에는 제품을 사용할 수 있지만 사용 가능한 지원 옵션이 제한됩니다. 기록 정보는 Knowledge Center 또는 기타 온라인 리소스에 표시됩니다. 문서는 더 이상 업데이트되지 않으며 현재 상태로 제공됩니다. 제품 수명 주기 단계는 Product Matrix(제품 매트릭스)를 참조하십시오.

> 참고:
>
> 단계적으로 중단되는 Citrix Endpoint Management 기능에 대한 사전 알림은 사용 중단을 참조하십시오.

XenMobile 용 Citrix Files(MDX): XenMobile 용 Citrix Files 는 2023 년 7 월 1 일에 EOL 에 도달했습니다.

고객들은 Apple App Store 와 Google Play 에서 제공되는 Citrix Files 를 사용하는 것이 좋습니다. MAM SDK 를 지원합니다.

Intune SDK 용 Secure Mail(iOS 및 Android): Secure Mail 은 2023 년 4 월 30 일에 EOL 에 도달했습니다.

Intune 용 Citrix Files: 2020 년 12 월 31 일부터 사용되지 않습니다.

Android Enterprise(작업 프로필 포함) 및 iOS 사용자 등록을 통해 일반 Citrix Files 앱 (앱 스토어에서 사용 가능) 을 컨테이너화하기 위해 플랫폼 기능을 활용하는 옵션을 살펴보는 것이 좋습니다.

ShareConnect: ShareConnect 가 2020 년 6 월 30 일에 EOL 에 도달했습니다.

Secure Notes: EOL 수명 주기 날짜는 2018 년 12 월 31 일입니다.

Secure Notes 및 Secure Tasks 의 기능이 필요한 경우 MDX 정책을 사용하여 보안을 유지할 수 있는 타사 앱인 Notate for Citrix 를 권장합니다.

Secure Notes 및 Secure Tasks 사용자가 Outlook 에 데이터를 저장한 경우 Notate 에서 액세스할 수 있습니다. ShareFile(현재 Citrix Files) 에 데이터를 저장한 경우에는 데이터가 마이그레이션되지 않습니다.

사용자는 EOL 날짜 이후 플랫폼 운영 체제의 사용자 인터페이스 지원이 중지될 때까지 Secure Notes 를 계속해서 실행할 수 있습니다. 그러나 지원되지 않는 제품은 사용하지 않는 것이 좋습니다.

Secure Tasks: EOL 수명 주기 날짜는 2018 년 12 월 31 일입니다.

Secure Forms: EOL 수명 주기 날짜는 2018 년 3 월 31 일입니다. 고객은 Citrix Files Platinum 및 Premium 계정에 포함된 Citrix ShareFile Workflows 로 전환하는 것이 좋습니다. 자세한 내용은 Citrix ShareFile Workflows를 참조하십시오.

ScanDirect: ScanDirect 는 2018 년 9 월 1 일에 EOL(수명 종료) 에 도달했습니다.

Office 365 앱과 보안 상호 작용 허용

September 4, 2024

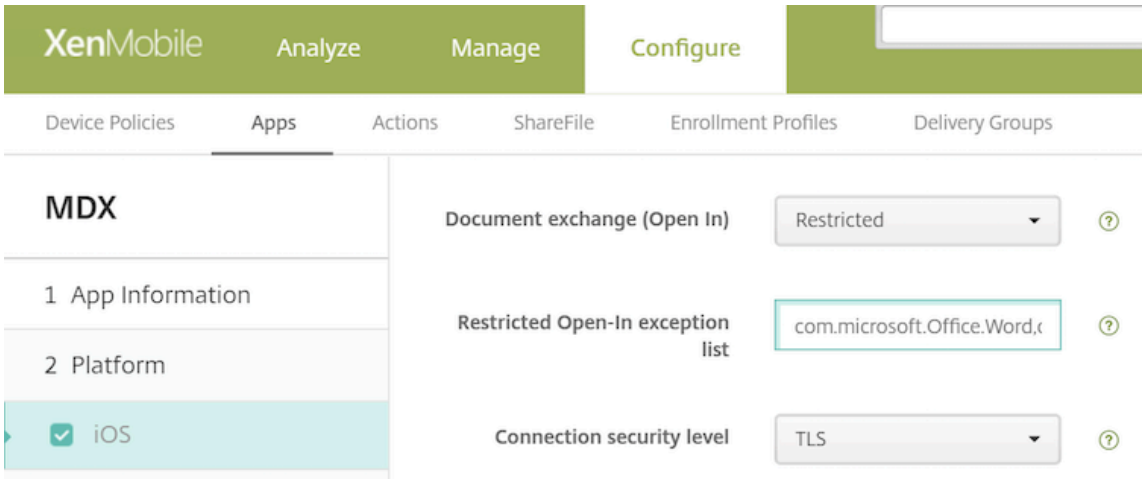
Citrix Secure Mail, Citrix Secure Web 및 Citrix Files 는 사용자가 문서 및 데이터를 Microsoft Office 365 앱으로 전송할 수 있도록 MDX 컨테이너를 여는 옵션을 제공합니다. Endpoint Management 콘솔에서 열기 정책을 통해 iOS 및 Android 플랫폼에 대해 이 기능을 관리할 수 있습니다.

Microsoft 앱에서 열린 후에 데이터는 MDX 컨테이너에서 더 이상 보안되거나 암호화되지 않습니다. 이 기능을 사용하도록 설정하기 전에 보안에 미치는 영향을 고려하십시오. 특히 데이터 손실 방지에 주된 관심이 있거나 HIPAA 또는 다른 엄격한 규정 준수 요건이 적용되는 고객은 컨테이너 열기에 따르는 장단점을 비교 평가해야 합니다.

iOS 에서 Office 365 를 사용하도록 설정

1. Secure Mail, Secure Web 또는 Citrix Files 앱의 최신 버전을 Endpoint Management 다운로드 페이지에서 다운로드합니다.
2. Endpoint Management 콘솔에 파일을 업로드합니다.

3. 문서 교환 **(열기)** 정책을 찾아 제한됨으로 설정합니다. 제한된 열기 제외 목록에서 Microsoft Word, Excel, PowerPoint, OneNote 및 Outlook 이 자동으로 나열됩니다. 예를 들어 com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook 이 표시됩니다.



MDM 등록에서 iOS 장치를 위한 추가적인 컨트롤을 사용할 수 있습니다.

iTunes 앱을 Endpoint Management 콘솔에 업로드하고 이 앱을 장치로 푸시할 수 있습니다. 이 옵션을 선택한 경우, 다음 정책을 켜짐으로 설정합니다.

- MDM 프로필이 제거된 경우 앱 제거
- 앱 데이터 백업 방지
- 강제로 앱 관리 (선택적 초기화를 통해 앱 및 데이터가 제거됨)

문서 및 데이터가 Microsoft 앱에서 장치의 관리되지 않는 앱으로 이동하는 것을 방지하려면 Endpoint Management 콘솔에서 구성 **>** 장치 **>** 제한 사항 **> iOS** 로 이동한 후, 관리되지 않는 앱에 있는 관리되는 앱의 문서 및 관리되는 앱에 있는 관리되지 않는 앱의 문서를 꺼짐으로 설정합니다.

Android 에서 **Office 365** 를 사용하도록 설정

1. Secure Mail, Secure Web 또는 Citrix Files 앱의 최신 버전을 Endpoint Management 다운로드 페이지에서 다운로드합니다.
2. Endpoint Management 콘솔에 파일을 업로드합니다.
3. 아래로 스크롤하여 문서 교환 **(열기)** 정책으로 이동한 후 제한됨을 선택합니다.
4. 제한된 열기 제외 목록에서 다음 패키지 ID 를 추가합니다.

   ```
   { package=com.microsoft.office.word } { package=com.microsoft.
   office.powerpoint } { package=com.microsoft.office.excel }
   ```

5. 다른 앱 정책을 일반적으로 구성하고 앱을 저장합니다.

장치에서 Secure Mail, Secure Web 또는 Citrix Files 의 파일을 저장하고 이 파일을 Office 365 앱으로 열어야 합니다.

iOS 및 Android 의 경우, 사용자가 다음 파일 유형을 장치에서 열고 편집할 수 있습니다.

지원되는 파일 형식

지원되는 파일 형식을 보려면 Microsoft Office 문서를 참조하십시오.