citrix

모바일생산성앱

Contents

모바일생산성앱릴리스일정

December 10, 2021

Citrix 모바일생산성앱은 2 주에걸쳐출시됩니다. 정확한날짜는변경될수있지만미리계획을세울수있도록일정을제공해드립니다. 또한, 이를통해앱배포및업데이트를더쉽게관리할수있기를바랍니다.

Secure Mail 및 **Secure Web** 단계별릴리스프로세스정보

Secure Mail 및 Secure Web 의새버전이제공되면다음과같은단계별접근방식으로릴리스가제공됩니다.

- iOS 및 Android 사용자의경우 App Store 및 Google Play Store 에서 1 주일 (7 일) 간점진적으로확대되는 Secure Mail 및 Secure Web 업데이트를사용할수있습니다.
- iOS 용 Secure Mail 및 Secure Web 의새다운로드는해당주안에새버전으로제공됩니다. Android 용 Secure Mail 및 Secure Web 의새다운로드는해당주동안이전버전으로실행되다가모든사용자에게제공되는새릴리스가 100% 가되면새버전으로제공됩니다.
- 사용자를위해일부기능은점진적단계로릴리스됩니다.

기능플래그관리를위한필수구성요소

운영중인 Secure Hub 또는 Secure Mail 에서문제가발생하는경우 Citrix 에서앱코드내에서영향을받는기능을사용중지할수있습니다. 이를위해 Citrix 에서는기능플래그와 LaunchDarkly 라는타사서비스를사용하고있습니다. LaunchDarkly 로의트래픽을사용하도록설정하기위해별도의구성은필요없습니다. 단, 방화벽이나프록시로아웃바운드트래픽을차단하는경우에는별도의구성이필요합니다. 위의두가지경우에는정책요구사항에따라특정 URL 이나 IP 주소를통해 LaunchDarkly 로의트래픽을사용하도록설정해야합니다. 모바일생산성앱 10.6.15 이후 MDX 가터널링에서도메인의제외를지원하는데대한자세한내용은 MDX Toolkit 설명서를참조하십시오. 기능플래그및 LaunchDarkly 에대한 FAQ 는이 Support Knowledge Center 문서를참조하십시오.

> 참고**:**
> 단계적으로중단되는 Citrix Endpoint Management 기능에대한사전알림은 사용중단을참조하십시오..

모바일생산성앱지원

May 14, 2022

자동업데이트를사용하도록설정한사용자는앱스토어에서최신버전을받습니다. 모바일생산성앱의최신버전은다음과같습니다.

- 22.3.0(Secure Hub 제외)

Citrix 에서는이전두버전의모바일생산성앱의업그레이드를지원합니다. 모바일생산성앱의이전두버전은다음과같습니다.

- 22.2.0

- 21.12.0(Secure Hub 제외)

지원되는운영체제

Secure Hub, MDX Toolkit 및모바일생산성앱의최신버전은 Endpoint Management 의최신버전및두이전버전과호환됩니다. 자세한내용은 지원되는장치운영체제를참조하십시오.

최신버전의모바일생산성앱에는최신버전의 Secure Hub 가필요합니다. Secure Hub 를최신상태로유지해야합니다.

> 참고:
>
> Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱은 2020 년 6 월부터 Android 6.x 및 iOS 11.x 를지원하지않습니다.

MDX 암호화에지원되는장치

Citrix 에서는다음과같은브랜드장치제품군목록에서 MDX 암호화를지원합니다.

Android:

- Samsung Note
- Samsung Galaxy
- Google Pixel
- Motorola

iOS:

- 이전목록의지원되는 OS 버전이있는모든 iOS 장치에서는 MDX 암호화가지원됩니다.

기타고려사항및제한사항

단계적으로중단되는 Citrix Endpoint Management 기능에대한사전알림은 사용중단을참조하십시오.

Secure Mail

- Endpoint Management 는 STA(Secure Ticket Authority) 및 Secure Mail 의문제로인해현재 NetScaler 12.0.41.16 을지원하지않습니다. 이문제는 NetScaler 12.0 빌드 41.22 에서수정되었습니다.
- Exchange 2007 용 Secure Mail 및 Lotus Notes 8.5.3 에대한지원이 2017 년 9 월 30 일에 EOL(수명종료) 상태에도달했습니다.
- Citrix Files 첨부파일보내기에서최상의성능을얻으려면 Citrix Files 최신버전을사용하는것이좋습니다. Windows 에서는 Citrix Files 가지원되지않습니다.
- IBM Notes 환경에서는 IBM Domino Traveler 서버버전 9.0 을구성해야합니다. 자세한내용은 Exchange Server 또는 IBM Notes Traveler 서버통합을참조하십시오.

Secure Web

장치에최신버전의 Android WebView 를설치합니다. 사용자는 Google Play Store 에서 Android WebView 를다운로드할수있습니다.

QuickEdit

QuickEdit 는계속해서모바일생산성앱으로제공됩니다. 이전에알려드린대로 EOL(수명종료) 상태는 2018 년 9 월 1 일에적용되지않습니다.

Citrix Content Collaboration for Endpoint Management

버전 6.5 이후에는공용앱스토어에서 Citrix Content Collaboration for Endpoint Management 에액세스합니다.

ShareConnect

ShareConnect 는 2020 년 6 월 30 일에 EOL(수명종료) 에도달했습니다. 자세한내용은 EOL 및사용되지않는앱을참조하십시오.

Citrix Secure Notes 및 Citrix Secure Tasks

Citrix Secure Notes 및 Citrix Secure Tasks 는 2018 년 12 월 31 일에 EOL(수명종료) 상태에도달했습니다. 자세한내용은 EOL 및사용되지않는앱을참조하십시오.

관리자작업및고려사항

March 14, 2022

이문서에서는모바일생산성앱의관리자와관련된작업및고려사항에대해설명합니다.

기능플래그관리

운영중인모바일생산성앱에서문제가발생하는경우 Citrix 에서앱코드내에서영향을받는기능을사용하지않도록설정할수있습니다. Citrix 에서 iOS 및 Android 용 Secure Hub, Secure Mail 및 Secure Web 에대한기능을사용하지않도록설정할수있습니다. 이를위해 Citrix 에서는기능플래그와 LaunchDarkly 라는타사서비스를사용하고있습니다. LaunchDarkly 로의트래픽을사용하도록설정하기위해별도의구성은필요없습니다. 단, 방화벽이나프록시로아웃바운드트래픽을차단하는경우에는별도의구성이필요합니다. 위의두가지경우에는정책요구사항에따라특정 URL 이나 IP 주소를통해 LaunchDarkly 로의트래픽을사용하도록설정해야합니다. 터널링에서도메인을제외하기위한 MDX 의지원과관련된자세한내용은 MDX Toolkit 설명서를참조하십시오.

다음과같은방법으로 LaunchDarkly 로의트래픽및통신을사용하도록설정할수있습니다.

다음 **URL** 에대한트래픽을사용하도록설정

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

도메인별허용목록만들기

이전에는내부정책에 IP 주소만나열하면되는경우사용할수있는 IP 주소목록을제공했습니다. 이제 Citrix 의인프라개선으로인해 2018 년 7 월 16 일부터공용 IP 주소가제공되지않습니다. 가능한경우도메인별허용목록을만드는것이좋습니다.

허용목록에 **IP** 주소나열

화이트리스트에 IP 주소를나열해야하는경우현재의모든 IP 주소범위목록은이 LaunchDarkly 공용 IP 목록을참조하십시오. 이목록을사용하면인프라업데이트에따라방화벽구성을자동으로업데이트할수있습니다. 인프라변경상태에대한자세한내용은 LaunchDarkly Statuspage를참조하십시오.

> 참고:
>
> 공용앱스토어앱은처음배포할때새로설치해야합니다. 앱의현재엔터프라이즈래핑된버전에서공용스토어버전으로업그레이드할수는없습니다.
>
> 공용앱스토어배포의경우, Citrix 가개발한앱을더이상 MDX Toolkit 으로서명하고래핑하지않습니다. 타사또는엔터프라이즈앱은 MDX Toolkit 을사용하여래핑할수있습니다.

LaunchDarkly 시스템요구사항

- Endpoint Management 10.7 이상.
- Citrix ADC 에서분할터널링이 꺼짐으로설정되어있는경우앱이다음서비스와통신가능한지확인하십시오.
  - LaunchDarkly 서비스
  - APNs 수신기서비스

지원되는앱스토어

모바일생산성앱은 Apple App Store 및 Google Play 에서구할수있습니다. Windows 장치에서기본생산성앱의보안을유지하고앱을배포하려면 Windows Information Protection 장치정책을참조하십시오.

Google Play 를이용할수없는중국에서는다음앱스토어에서 Android 용 Secure Hub 를구할수있습니다.

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

공용앱스토어배포사용

1. iOS 및 Android 용공용스토어 .mdx 파일을 Endpoint Management 다운로드페이지에서다운로드합니다.
2. Endpoint Management 콘솔에.mdx 파일을업로드합니다. 모바일생산성앱의공용스토어버전은여전히 MDX 응용프로그램으로업로드되므로서버에공용스토어앱으로앱을업로드하지마십시오. 단계를보려면 앱추가를참조하십시오.
3. 보안정책에기반하여정책을기본값에서변경합니다 (선택사항).
4. 앱을필수앱으로푸시합니다 (선택사항). 이단계를사용하려면모바일기기관리를사용하도록환경을설정해야합니다.
5. 장치에 App Store, Google Play 또는 Endpoint Management 앱스토어의앱을설치합니다.
    - Android 장치의경우앱을설치하도록사용자가 Play Store 으로이동됩니다. iOS 장치에서는 MDM 이포함된배포인경우사용자가앱스토어로이동하지않고앱이설치됩니다.
    - App Store 또는 Play Store 에서앱을설치하는경우다음작업이수행됩니다. 해당하는.mdx 파일이서버에업로드되면앱이관리되는앱으로전환됩니다. 관리되는앱으로전환될때앱에서 Citrix PIN 을묻는메시지가표시됩니다. 사용자가 Citrix PIN 을입력하면 Secure Mail 에계정구성화면이표시됩니다.
6. Secure Hub 에등록되어있고해당하는.mdx 파일이서버에있는경우에만앱에액세스할수있습니다. 조건중어느한쪽이충족되지않아도사용자가앱을설치할수있지만앱사용이차단됩니다.

현재공용앱스토어에있는 Citrix Ready Marketplace 의앱을사용하고있는경우, 이미익숙한배포프로세스가진행됩니다. 모바일생산성앱에는여러 ISV 가현재사용하는것과동일한접근방법이사용됩니다. MDX SDK 를앱내에포함시켜앱을공용스토어에서사용가능하도록준비합니다.

> 참고:
>
> iOS 및 Android 용 Citrix Files 앱의공용스토어버전은이제범용이므로, 스마트폰및태블릿용 Citrix Files 앱이동일합니다.

Apple 푸시알림

푸시알림구성에대한자세한내용은 푸시알림을사용하도록 Secure Mail 구성을참조하십시오.

공용앱스토어 **FAQ**

- 서로다른사용자그룹에공용스토어앱의여러복사본을배포할수있습니까? 가령서로다른사용자그룹에서로다른정책을배포하고싶습니다.

  각사용자그룹에대해서로다른.mdx 파일을업로드합니다. 그러나이경우단일사용자가여러그룹에속할수는없습니다. 사용자가여러그룹에속한경우동일한앱의복사본여러개가해당사용자에게할당됩니다. 앱 ID 는변경할수없으므로공용스토어앱의여러복사본을동일한장치에배포할수없습니다.

- 공용스토어앱을필수앱으로푸시할수있습니까?

  예. 앱을장치로푸시하려면 MDM 이필요합니다. MAM 전용배포에대해서는지원되지않습니다.

- 사용자에이전트기반의트래픽정책또는 Exchange Server 규칙을업데이트해야합니까?

  다음은플랫폼별사용자에이전트기반정책및규칙에해당하는문자열입니다.

> 중요:
>
> Secure Notes 및 Secure Tasks 는 2018 년 12 월 31 일에 EOL(수명종료) 상태에도달했습니다. 자세한내용은 EOL 및사용되지않는앱을참조하십시오.

Android

앱	서버	사용자-에이전트문자열
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-에이전트문자열
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

- 앱이업그레이드되지않게할수있습니까?

  아니요. 업그레이드가공용앱스토어에게시되면자동업데이트사용이설정된모든사용자가업데이트를받게됩니다.

- 앱업그레이드를적용할수있습니까?

  예. 업그레이드는업그레이드유예기간정책을통해적용됩니다. 이정책은업데이트된앱버전에상응하는새.mdx 파일이 Endpoint Management 로업로드될때설정됩니다.

- 업데이트일정을통제할수없는경우업데이트가사용자에게도달하기전에앱을테스트하려면어떻게해야합니까?

  Secure Hub 의프로세스와유사하게, EAR 기간동안 iOS 용 TestFlight 에서앱을테스트할수있습니다. Android 의

경우, EAR 기간동안 Google Play 베타프로그램을통해앱을사용할수있습니다. 이기간중에앱업데이트를테스트할수있습니다.

- 자동업데이트가사용자장치에도달하기전에새.mdx 파일을업데이트하지않으면어떻게됩니까?

  업데이트된앱은이전.mdx 파일과계속호환됩니다. 새정책이적용되는새로운기능은사용할수없습니다.

- Secure Hub 가설치되어있으면앱이관리되는앱으로전환됩니까, 아니면앱을등록해야합니까?

  공용스토어앱이관리되는앱 (MDX 에의해보안됨) 으로활성화되고사용가능해지려면사용자가 Secure Hub 에등록되어야합니다. Secure Hub 가설치되어있지만등록되지않은사용자는공용스토어앱을사용할수없습니다.

- 공용스토어앱을위해 Apple Enterprise 개발자계정이필요합니까?

  아니요. 이제 Citrix 가모바일생산성앱의인증서와프로비전프로필을유지관리하므로앱을사용자에게배포하기위해 Apple Enterprise 개발자계정이필요하지않습니다.

- 배포한모든래핑된응용프로그램에엔터프라이즈배포종료가적용됩니까?

  아니요. 모바일생산성앱, 즉 Secure Mail, Secure Web 및 Citrix Content Collaboration for Endpoint Management, QuickEdit 및 ShareConnect 에만적용됩니다. 자체적으로또는타사를통해개발하여배포한모든엔터프라이즈래핑된앱은계속엔터프라이즈래핑을사용할수있습니다. MDX Toolkit 은앱개발자를위해엔터프라이즈래핑을계속지원합니다.

- Google Play 에서앱을설치할때오류코드가 505 인 Android 오류가발생합니다.

  > 참고:
  >
  > Android 5.x 에대한지원은 2018 년 12 월 31 일에종료되었습니다.

  이는 Google Play 및 Android 5.x 버전의알려진문제입니다. 이오류가발생하는경우장치에서앱설치를막는오래된데이터를몇가지단계를거쳐삭제할수있습니다.

  1. 장치를재시작합니다.
  2. 장치설정을통해 Google Play 관련캐시및데이터를지웁니다.
  3. 최후의수단으로장치에서 Google 계정을제거했다가다시추가합니다.

자세한내용을보려면 “Fix Google Play Store Error 505 in Android: Unknown Error Code” 키워드를사용하여이 사이트를검색하십시오.

- Google Play 의앱이프로덕션환경으로릴리스되었고사용할수있는새베타릴리스가없는경우에도 Google Play 에서앱 제목뒤에 Beta 가표시되는이유는무엇입니까?

  EAR(Early Access Release) 프로그램에참여하고있는경우앱제목옆에 Beta 가항상표시됩니다. 이이름은단순히특정앱에대한사용자의액세스수준을사용자에게알려줍니다. Beta 라는이름은사용자가앱의사용가능한최신버전을받는다는의미입니다. 최신버전이란프로덕션트랙에게시된최신버전이거나베타트랙에게시된최신버전일수있습니다.

- 앱을설치하고연후에.mdx 파일이 Endpoint Management 콘솔에있는경우에도사용자에게권한이부여되지않은앱이라는메시지가표시됩니다.

이문제는사용자가 App Store 또는 Google Play 에서앱을직접설치하고 Secure Hub 가새로고쳐지지않은경우에발생할수있습니다. 비활성타이머가만료되면 Secure Hub 를새로고쳐야합니다. 사용자가 Secure Hub 를열고재인증하면정책이새로고쳐집니다. 다음에사용자가앱을열때앱권한이부여됩니다.

- 앱을사용하려면액세스코드가필요합니까? App Store 또는 Play Store 에서앱을설치할때액세스코드를입력하라는메시지를표시하는화면이나타납니다.

  액세스코드를요청하는화면이표시되는경우 Secure Hub 를통해 Endpoint Management 에등록하지않은것입니다. Secure Hub 로등록한후앱의.mdx 파일이서버에배포되어있는지확인하십시오. 또한앱을사용할수있는지확인해야합니다. 액세스코드는 Citrix 내부용도로만제한됩니다. 앱을사용하려면 Endpoint Management 배포를활성화해야합니다.

- VPP 또는 DEP 를통해 iOS 공용스토어앱을배포할수있습니까?

  Endpoint Management 는 MDX 가사용설정되지않은공용스토어앱의 VPP 배포용으로최적화되었습니다. Endpoint Management 공용스토어앱을 VPP 로배포할수는있지만 Endpoint Management 와 Secure Hub 저장소를향상하여제한사항을처리해야만배포가최적화됩니다. VPP 를통한 Endpoint Management 공용스토어앱배포와관련된알려진문제및가능한해결방법의목록은 Citrix Knowledge Center의이문서를참조하십시오.

모바일생산성앱의 **MDX** 정책

MDX 정책을사용하여 Endpoint Management 가적용할설정을구성할수있습니다. 이정책에는인증, 장치보안, 네트워크요구사항과액세스권한, 암호화, 앱상호작용, 앱제한등이포함됩니다. 대부분의 MDX 정책이모든모바일생산성앱에적용되지만, 일부정책은특정앱에만적용됩니다.

정책파일은모바일생산성앱의공용스토어버전에해당하는.mdx 파일로제공됩니다. 또한앱을추가할때 Endpoint Management 콘솔에서정책을구성할수도있습니다.

MDX 정책에대한자세한설명은이섹션에서다음문서를참조하십시오.

- 모바일생산성앱의 MDX 정책요약
- Android 용모바일생산성앱의 MDX 정책
- iOS 용모바일생산성앱의 MDX 정책

다음섹션에서는사용자연결과관련된 MDX 정책에대해설명합니다.

Android 용 **Secure Mail** 의듀얼모드

MAM(모바일애플리케이션관리) SDK 를사용하여 iOS 및 Android 플랫폼에서제공되지않는 MDX 기능의영역을대체할수있습니다. MDX 래핑기술은 2021 년 9 월에 EOL(수명종료) 에도달할예정입니다. 엔터프라이즈응용프로그램을계속관리하려면 MAM SDK 를포함해야합니다.

버전 20.8.0 에서 Android 앱은앞서언급한 MDX EOL 전략에대비하기위해 MDX 및 MAM SDK 가포함된상태로릴리스됩니다. MDX 듀얼모드는현재 MDX Toolkit 에서새 MAM SDK 로의전환경로를제공하기위한것입니다. 듀얼모드를사용하면다음과같은작업이가능해집니다.

- MDX Toolkit(이제 Endpoint Management 콘솔에서는레거시 MDX 라고함) 을사용한지속적인앱관리
- 새 MAM SDK 를통합하는앱을관리합니다.

> 참고:
>
> MAM SDK 를사용하는경우앱을래핑할필요가없습니다.

MAM SDK 로전환한후에는추가단계가필요하지않습니다.

MAM SDK 에대한자세한내용은다음문서를참조하십시오.

- MAM SDK Overview(MAM SDK 개요)
- 장치관리에대한 Citrix Developer 섹션
- Citrix 블로그게시물
- Citrix 다운로드에로그온할때 SDK 다운로드

사전요구사항

듀얼모드기능을성공적으로배포하려면다음을확인하십시오.

- Citrix Endpoint Management 를버전 10.12 RP2 이상또는 10.11 RP5 이상으로업데이트합니다.
- 모바일앱을버전 20.8.0 이상으로업데이트합니다.
- 정책파일을버전 20.8.0 이상으로업데이트합니다.
- 조직에서타사앱을사용하는경우 Citrix 모바일생산성앱에대한 MAM SDK 옵션으로전환하기전에 MAM SDK 를타사앱에통합해야합니다. 관리되는모든앱을한번에 MAM SDK 로이동해야합니다.

> 참고:
>
> MAM SDK 는모든클라우드기반고객에대해지원됩니다.

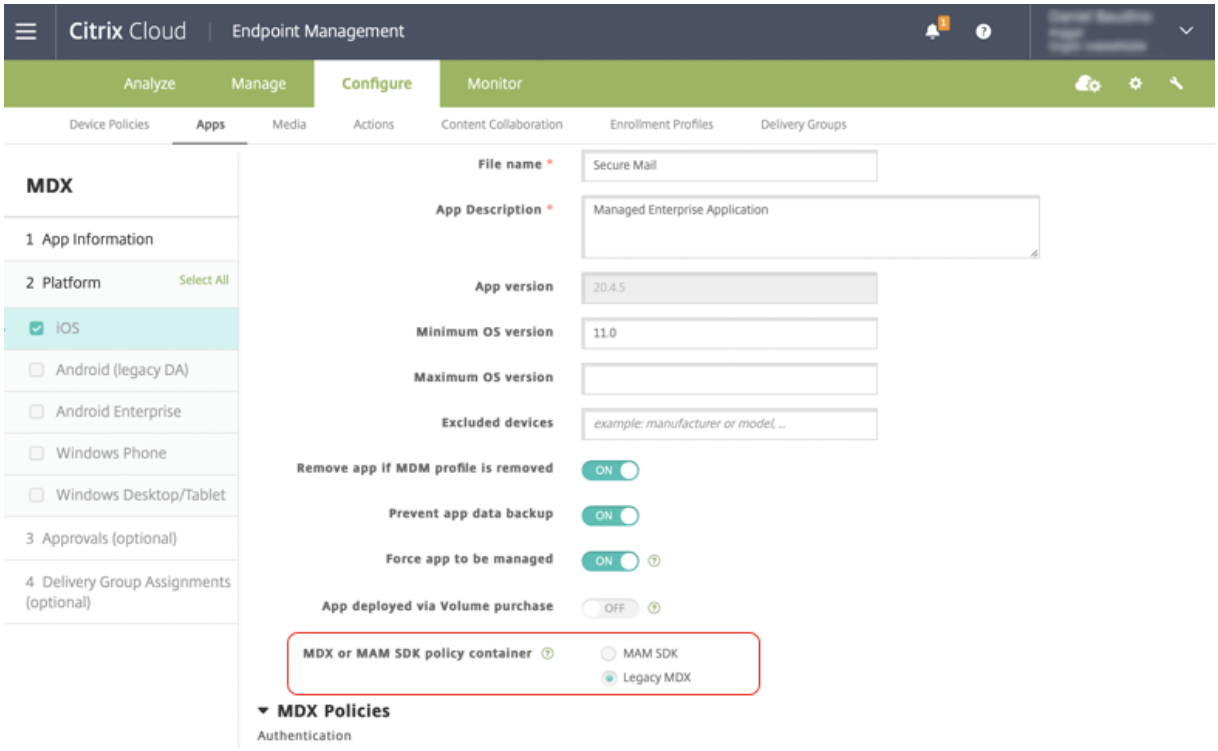
제한사항

- MAM SDK 는 Citrix Endpoint Management 배포의 Android Enterprise 플랫폼에게시된앱만지원합니다. 새로게시된앱의경우플랫폼기반암호화가기본암호화입니다.
- MAM SDK 는 MDX 암호화가아닌플랫폼기반암호화만지원합니다.
- Citrix Endpoint Management 를업데이트하지않고버전 20.8.0 이상에서모바일앱에대해정책파일을실행하면 Secure Mail 에대한네트워킹정책의중복항목이만들어집니다.

Citrix Endpoint Management 에서 Secure Mail 을구성할때듀얼모드기능을사용하면 MDX Toolkit(현재의레거시 MDX) 을사용하여계속해서앱을관리하거나새로운 MAM SDK 로전환하여앱을관리할수있습니다. MAM SDK 는모듈식이므로조직에서사용하는 MDX 기능의하위집합만사용할수있습니다. 따라서 Citrix 에서는 MAM SDK 로전환하도록권장합니다.

MDX 또는 **MAM SDK** 정책컨테이너에서다음과같은정책설정옵션을사용할수있습니다.

- **MAM SDK**
- 레거시 **MDX**



MDX 또는 **MAM SDK** 정책컨테이너정책에서는 레거시 **MDX** 에서 **MAM SDK** 로옵션을변경할수만있습니다. **MAM SDK** 에서 레거시 **MDX** 로전환하는옵션은허용되지않으며앱을다시게시해야합니다. 기본값은 레거시 **MDX** 입니다. 동일한장치에서 실행되는 Secure Mail 과 Secure Web 모두에대해동일한정책모드를설정해야합니다. 동일한장치에서두개의서로다른모드를실행할수없습니다.

내부네트워크로의사용자연결

내부네트워크에터널링되는연결에서는전체 VPN 터널을사용하거나, 보안탐색이라고하는클라이언트없는 VPN 의변형을사용할 수있습니다. 해당동작은기본설정 VPN 모드정책에의해제어됩니다. 기본적으로연결시 SSO 를필요로하는연결에대해권장되는보안탐색을사용합니다. 클라이언트인증서또는종단간 SSL 을사용하여내부네트워크의리소스로연결되는경우전체 VPN 터널설정을사용하는것이좋습니다. 이설정은 TCP 기반의모든프로토콜을처리하고, Windows 및 Mac 컴퓨터뿐아니라 iOS 및 Android 장치에서도사용될수있습니다.

iOS 및 Android 용 Secure Web 에서는 PAC(Proxy Automatic Configuration) 파일을전체 VPN 터널배포와함께사용할수있도록지원합니다. 예를들어프록시인증을위해 Citrix ADC 를사용하는경우가여기에해당합니다.

VPN 모드전환허용정책은필요에따라전체 VPN 터널모드와 Secure Browse 모드간의자동전환을허용합니다. 기본적으로이정책은꺼져있습니다. 이정책이켜진경우, 기본설정 VPN 모드에서처리할수없는인증요청으로인해실패한네트워크요청은다른모드에서다시시도됩니다. 예를들어클라이언트인증서에대한서버챌린지는전체 VPN 터널모드에서수용될수있지만 Secure Browse 모드에서는수용될수없습니다. 마찬가지로 HTTP 인증챌린지는 Secure Browse 모드를사용할경우에 SSO 로더쉽게서비스될수있습니다.

네트워크액세스제한

네트워크액세스정책은네트워크액세스에대한제한이적용되는지여부를지정합니다. 기본적으로 Secure Mail 액세스는제한되지않으므로네트워크액세스에대한제한이적용되지않습니다. 앱은장치가연결된네트워크에제한없이액세스할수있습니다. 기본적으로 Secure Web 액세스는내부네트워크로터널링되므로내부네트워크로의응용프로그램별 VPN 터널이모든네트워크액세스에사용되고 Citrix ADC 분할터널링설정이사용됩니다. 또한장치에네트워크연결이없는것처럼앱이작동하도록차단된액세스를지정할수도있습니다.

AirPrint, iCloud, Facebook 및 Twitter API 등의기능을허용하려는경우네트워크액세스정책을차단하지마십시오.

네트워크액세스정책은백그라운드네트워크서비스정책과상호작용합니다. 자세한내용은 Exchange Server 또는 IBM Notes Traveler 서버통합을참조하십시오.

Endpoint Management 클라이언트속성

클라이언트속성은사용자장치에서 Secure Hub 에직접제공되는정보를포함합니다. 클라이언트속성은 Endpoint Management 콘솔에서 설정 **>** 클라이언트 **>** 클라이언트속성에있습니다.

클라이언트속성은다음과같은설정을구성하는데사용됩니다.

사용자암호캐싱

사용자암호캐싱은사용자의 Active Directory 암호가모바일장치에로컬로캐싱될수있게합니다. 사용자암호캐싱이사용되도록설정하면 Citrix PIN 또는암호를설정하라는메시지가사용자에게표시됩니다.

비활성화타이머

비활성화타이머는사용자가장치를비활성상태로둔후에 Citrix PIN 또는암호를입력하라는메시지없이앱에액세스할수있는시간(분단위) 을정의합니다. MDX 앱에대해이설정을사용되도록설정하려면앱암호정책을 켜짐으로설정해야합니다. 앱암호정책이 꺼짐인경우, 사용자는전체인증을수행하기위해 Secure Hub 로리디렉션됩니다. 이설정을변경하면다음에사용자에게인증하라는메시지가표시될때값이적용됩니다.

Citrix PIN 인증

Citrix PIN 은사용자인증환경을간소화합니다. PIN 은클라이언트인증서를보안하거나 Active Directory 자격증명을장치에로컬로저장하는데사용됩니다. PIN 설정을구성한경우사용자로그온환경은다음과같습니다.

1. 사용자가처음으로 Secure Hub 를시작하면 PIN 을입력하라는메시지가사용자에게표시되고, Active Directory 자격증명이캐싱됩니다.
2. 다음번에사용자가 Secure Mail 과같은모바일생산성앱을시작할때사용자는 PIN 을입력하고로그온합니다.

클라이언트속성을사용하여 PIN 인증이사용되도록설정하고 PIN 유형을지정하고 PIN 강도, 길이를지정하고요구사항을변경합니다.

지문또는 **Touch ID** 인증

iOS 장치의지문인증 (Touch ID 인증이라고도함) 은 Citrix PIN 의대안기능으로, Secure Hub 를제외한래핑된앱이비활성화타이머가만료되는등의상황에서오프라인인증을필요로할경우에유용합니다. 다음과같은인증시나리오에서이기능이사용되도록설정할수있습니다.

- Citrix PIN + 클라이언트인증서구성
- Citrix PIN + 캐싱된 AD 암호구성
- Citrix PIN + 클라이언트인증서구성및캐싱된 AD 암호구성
- Citrix PIN 이꺼짐

지문인증이실패하거나사용자가지문인증프롬프트를취소하면래핑된앱이 Citrix PIN 또는 AD 암호인증으로폴백됩니다.

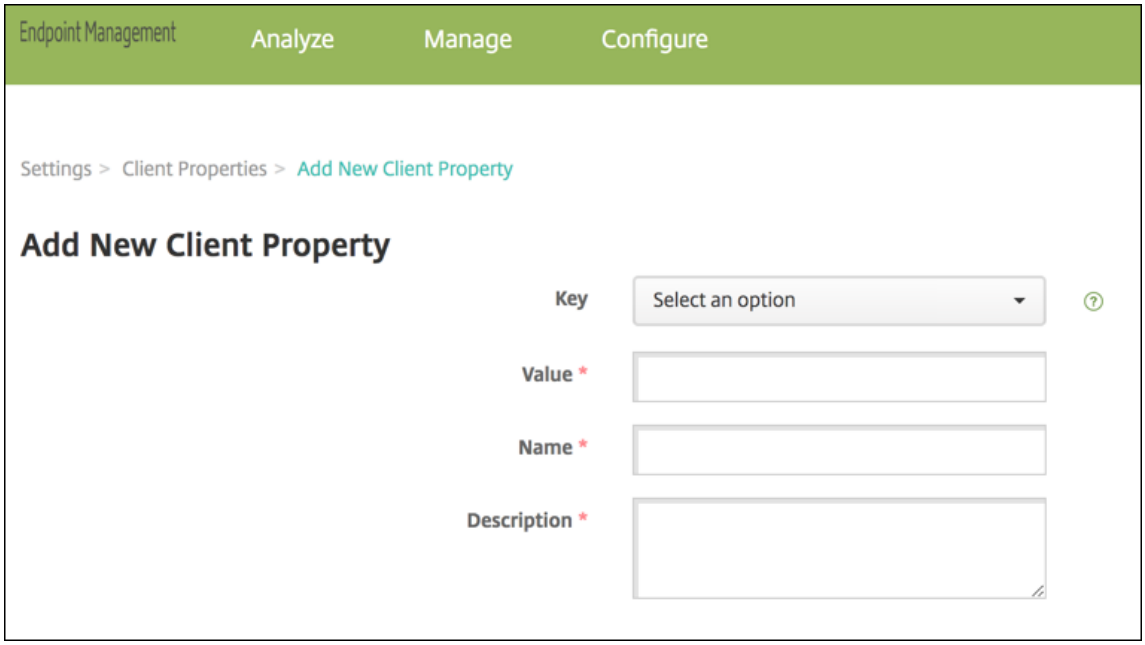
지문인증요구사항

- 지문인증을지원하고최소 1 개의지문이구성되어있는 iOS 장치 (버전 8.1 이상).
- 사용자엔트로피가꺼져있어야합니다.

지문인증을구성하려면

> 중요:
>
> 사용자엔트로피가켜져있으면 Touch ID 인증사용속성이무시됩니다. 사용자엔트로피는 Encrypt secrets using Passcode key(암호키를사용한암호암호화) 를통해사용설정합니다.

1. Endpoint Management 콘솔에서 설정 **>** 클라이언트 **>** 클라이언트속성으로이동합니다.
2. 추가를클릭합니다.



3. **ENABLE_TOUCH_ID_AUTH** 키를추가하고 값을 **True** 로설정하고정책이름을 **Enable Touch Fingerprint Authentication(**지문인증사용설정**)** 으로지정합니다.

지문인증을구성한후에사용자가장치를다시등록할필요가없습니다.

암호코드키및클라이언트속성을사용한암호화암호에대한자세한내용은 Endpoint Management 문서의 클라이언트속성을참조하십시오.

Google Analytics

Citrix Secure Mail 은제품품질을개선하기위해 Google Analytics 를사용하여앱통계및사용정보분석데이터를수집합니다. Citrix 는다른개인사용자정보를수집하거나저장하지않습니다.

Google Analytics 비활성화

관리자는사용자지정클라이언트속성 **DISABLE_GA** 를구성하여 Google Analytics 를비활성화할수있습니다. Google Analytics 를비활성화하려면다음을수행합니다.

1. Citrix Endpoint Management 콘솔에로그인하고 설정 > 클라이언트속성 > 새클라이언트속성추가로이동합니다.
2. 키필드에 **DISABLE_GA** 값을추가합니다.
3. 클라이언트속성의값을 **true** 로설정합니다.

> 참고**:**
>
> Citrix Endpoint Management 콘솔에서 **DISABLE_GA** 값을구성하지않으면 Google Analytics 데이터가활성화됩니다.

플랫폼별기능

November 19, 2021

다음표에는 Citrix 모바일생산성앱의기능이요약되어있습니다. **X** 는해당플랫폼에서기능을사용할수있음을나타냅니다. QuickEdit 에서의기능은 Citrix QuickEdit 문서를참조하십시오.

Citrix Secure Hub

기능	iOS	Android
인증을위한로그온	X	X
정책준수모니터링	X	X
앱및데스크톱액세스	X	X

기능	iOS	Android
HDX 앱및데스크톱	X	X
문제로그생성및보내기	X	X
로그에스크린샷첨부	X	X
앱내에서지원센터에연락	X	X
앱내에서 Citrix 지원팀에연락	X	X
충돌수집및분석	X	X
오프라인인증	X	X
Citrix Secure Mail 을통해로그보내기	X	X
Google Analytics	X	X
세로및가로모드	X	X
앱신뢰를위한앱내가이드	X	X
전자메일로등록한경우 Secure Mail 에자동등록 (MAM 만해당)	X	X
Touch ID 오프라인인증	X	X
파생된자격증명으로등록	X	
생체인증		X
Workspace 앱스토어사용	X	X

Citrix Secure Mail

기능	iOS	Android
전자메일생산성		
임시보관함최소화	X	X
보낸메일실행취소		X
암호화관리	X	X
일정목록에대한위젯		X
Secure Mail 의연락처사진	X	X
반응형전자메일지원	X	X
임시보관함폴더자동동기화	X	X

기능	iOS	Android
임시보관함폴더에서첨부파일동기화		X
전자메일보내기, 받기, 회신, 모두회신, 전달	X	X
초안만들기, 편집, 삭제	X	X
메일에플래그지정	X	X
읽지않음으로표시	X	X
모든폴더및하위폴더보기	X	X
앱이백그라운드로전환될때초안자동저장	X	X
Citrix Secure Notes 로전자메일을 메모로변환. 중요**:** Secure Notes 는 2018 년 12 월 31 일에 EOL(수명 종료) 상태에도달했습니다. 자세한내용은 EOL 및사용되지않는앱을참조하십시오.	X	X
메일검색 (로컬및서버)	X	X
메일동기화기간선택 (최대 1 개월또는 모든메일)	X	X
읽지않은메일보기	X	X
보안첨부파일이미지, 비디오및오디오보기/재생	X	X
다중첨부파일	X	X
첨부파일회신및전달	X	X
Citrix Files 에서파일첨부	X	X
Citrix Files 제한된영역및커넥터로부터파일첨부	X	X
첨부파일저장소	X	X
서식있는텍스트편집	X	X
제목, 잠금화면미리보기가포함된메일알림	X	X
알림화면에서메일및초대에회신및삭제	X	
사진첨부또는촬영	X	X

기능	iOS	Android
다중메시지선택	X	X
첨부파일다운로드	X	X
이미지인라인로드	X	X
빠른정렬	X	X
.zip 첨부파일보내기, 받기, 열기및저장	X	X
세로및가로모드	X: 메일목록, 메일읽기, 작성, 일정및연락처보기전반	X: 메일읽기및작성보기만
붙여넣은텍스트에서서식유지	X	X
연락처에서보낸 SMS	X	X
연락처에서보낸 FaceTime	X	
연결문제또는가득찬사서함으로인해보내지지않은메시지를보낼편지함에보관	X	X
최근폴더버블업		X
아래로당겨메일새로고침	X	X
마지막새로고침타임스탬프	X	X
왼쪽으로살짝밀어메시지작업	X	X
Microsoft Exchange 및 IBM Notes Traveler 지원	X	X
눌러서메일, 일정및연락처새로고침	X	X
장치접근성/글꼴크기설정을메일보기에서유지	X	X
S/MIME 서명및암호화	X	X
전자메일로 S/MIME 인증서가져오기	X	X
S/MIME, Intercede 통합	X	
S/MIME, Entrust 통합	X	
메시지본문에대한 Microsoft IRM 보호	X	X
푸시알림	X	X
받은편지함으로알림을푸시하여일정을비롯한모든폴더를자동으로업데이트	X	

기능	iOS	Android
Office 365 문서열기	X	X
3D Touch 동작	X	
잠금화면에서상황에맞는아이콘	X	X
폴더검색	X	X
VIP 메일폴더	X	X
동적유형지원	X	X
확장된폴더유지	X	X
메시지분류마커	X	X
맞춤법검사	X	
마지막으로찍은사진첨부	X	X
URL 미리보기	X	X
Citrix Files 에서 Citrix Files 링크 열기	X	X
`.pass` 파일지원	X	
검색모드에서여러개의전자메일선택	X	X
이미지인라인삽입	X	X
EAS(Exchange ActiveSync) 버전 16 으로업그레이드	X	X
사용자가알수없는도메인또는개인도메인을사용하지못하도록제한	X	
슈퍼와이드장치화면지원		X
여러 Exchange 계정구성	X	X
왼쪽또는오른쪽으로살짝밀어자세히작업	X	X
암호화된메일의회신또는전달암호화	X	
전자메일및인라인이미지인쇄	X	
설정에서줄미리보기를사용하여사서함보기에미리보기로표시되는전자메일본문의줄수구성	X	
반응형전자메일지원	X	X

기능	iOS	Android
첨부파일의앱내미리보기 (MS Office 또는이미지)	X	X
개인연락처그룹	X	X
전자메일주소 (UPN) 로사용자이름마이그레이션	X	X
피싱전자메일보고	X	X
최신인증 (OAuth)	X	X
첨부파일인쇄	X	
Android Enterprise(Android for Work)	X	
서식있는텍스트서명	X	
다양한방식의푸시알림	X	
피드	X	X
사진첨부개선	X	X
그룹알림	X	
Slack 통합 (미리보기)	X	X
피드관리	X	
내부도메인	X	X
피드관리	X	X
MS Teams 통합	X	X
자체진단 (문제해결) 옵션		X
듀얼모드 (MAM SDK)	X	X
자가진단도구		X
일정		
ICS 파일미리보기및일정이벤트로가져오기		X
일정이벤트끌어서놓기	X	X
일, 주, 월및일정목록보기	X	X
잠금화면에서의상세한미리알림	X	X
6 개월간동기화	X	X

기능	iOS	Android
이벤트를개인적인것으로설정	X	X
첫번째이벤트이전시간으로스크롤	X	
수동새로고침옵션	X	X
미리알림설정	X	X
눌러서주소매핑	X	X
주번호	X	X
동적유형지원	X	X
보안분류마커	X	X
주소길게누르기	X	
주당근무시간시작일설정	X	X
선택한날짜의주에초점맞춰보기	X	
현재날짜가항상강조표시됨	X	X
첨부파일저장소의일정첨부파일	X	X
개인일정지원	X	X
개인일정이벤트와의충돌표시		X
일정이벤트인쇄	X	
일정제목줄의전화번호및웹주소누르기	X	
일정검색	X	
모임		
모임회신, 모두회신, 전달	X	X
초대응답에대한주최자보기	X	X
초대대상자의상태및제안된상태에대한주최자보기	X	X
눌러서온라인모임에참가 참고**:** WebEx 및 Lync 의경우 Citrix Endpoint Management 에서이러한앱의사용을위한정책을구성해야합니다.	X	X
눌러서오디오회의에참가	X	X

기능	iOS	Android
새초대에서온라인모임, 오디오, 회의 예약	X	X
새초대에 ShareFile 링크추가	X	X
첨부파일을포함하여초대전달	X	X
눌러서 “지각” 전자메일보내기	X	X
눌러서모임주최자에게회신	X	X
눌러서모든모임초대에회신	X	X
눌러서모든모임초대대상자에게회신	X	X
눌러서모든모임초대대상자에게첨부파일을포함하여회신	X	X
GoToMeeting 에전화접속	X	X
잠금화면또는알림화면에서초대에응답	X	X
WebEx 또는 Lync 모임에전화접속	X	X
거부된이벤트숨기기	X	X
동시이벤트를 3 개넘게표시	X	X
초대대상자상태빠른보기	X	X
취소된이벤트에대한설명삭제, 회신, 모두회신, 추가	X	X
전달된초대장에주최자이름표시	X	X
공유장치	X	X
Skype for Business 모임참가	X	X
수락, 거부및미정을사용하여회의알림에응답	X	X
회신및삭제를사용하여메시지알림에응답	X	
연락처		
연락처에폴더만들기		X
양방향연락처동기화	X	X
상세한연락처정보 GAL 검색	X	X
Secure Mail 연락처를로컬연락처로내보내기및동기화	X	X

기능	iOS	Android
연락처: 즐겨찾기및범주		X
내보내지는연락처필드제어	X	X
Secure Mail 이외의연락처세부정보	X	X
동적유형지원	X	X
연락처를 VIP 로표시	X	X
`.vcards`와연락처공유	X	X
길게눌러연락처보기		X
기본메일계정이있는경우에도연락처내보내기	X	X
폴더및하위폴더보기	X	
장치에구성된설정		
iMessage 지원	X	
알림제어를위한고급옵션	X	X
잠금화면알림제어	X	X
메일및일정알림사운드	X	X
폴더자동새로고침	X	X
내부및외부부재중알림	X	X
삭제전확인	X	X
스레드형대화또는시간순보기	X	X
Wi-Fi 에서첨부파일로드	X	X
Wi-Fi 에서첨부파일로드를기본값으로지정	X	X
메일동기화기간설정	X	X
무제한동기화/모든메일동기화		X
전자메일서명설정	X	X
성또는이름기준으로연락처나열	X	X
자동진행	X	X
기본표준시간대사용		X
빠른응답템플릿		X

기능	iOS	Android
메일구성푸시빈도		X
설정내보내기/가져오기	X	X
장치에서뒤로단추를눌러부동작업단추옵션해제		X

Citrix Secure Web

기능	iOS	Android
멀티태스킹을통해두개의앱을동시에사용	X	
파일다운로드	X	X
즐겨찾기추가	X	X
저장된사용자이름및암호지우기	X	X
캐시/기록/쿠키삭제	X	X
팝업차단	X	X
오프라인페이지저장	X	X
주소표시줄에서검색	X	X
알림에서다운로드한항목열기	X	X
암호자동저장	X	X
프록시지원		
엔터프라이즈프록시	X	X
URL 차단목록및허용목록	X	X
기록	X	X
기본홈페이지	X	X
탭	X	X
책갈피푸시	X	X
화면캡처차단		X
현재페이지에서검색	X	X
3D Touch 동작	X	
공유장치	X	X

기능	iOS	Android
공유장치를통해파일변조방지	X	
설정내보내기/가져오기	X	X
세로및가로모드	X	X
Android Enterprise(Android for Work)		X
당겨서화면의콘텐츠새로고침	X	X

Citrix Secure Hub

May 14, 2022

Citrix Secure Hub 는모바일생산성앱의실행패드입니다. 사용자는 Secure Hub 에장치를등록하여앱스토어액세스권한을얻습니다. 사용자는앱스토어에서 Citrix 가개발한모바일생산성앱및타사앱을추가할수있습니다.

Secure Hub 및기타구성요소를 Citrix Endpoint Management 다운로드페이지에서다운로드할수있습니다.

Secure Hub 및모바일생산성앱의기타시스템요구사항은 시스템요구사항을참조하십시오.

모바일생산성앱에대한최신정보는 최근발표내용 문서를참조하십시오.

다음섹션에서는현재및이전 Secure Hub 릴리스의새로운기능에대해설명합니다.

> 참고:
>
> Android 6.x 및 iOS 11.x 버전의 Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱에대한지원이 2020 년 6 월에종료되었습니다.

현재버전의새로운기능

Secure Hub 22.2.0

iOS 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Android 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

이전버전의새로운기능

Secure Hub 21.11.0

Android 용 **Secure Hub**

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.10.0

iOS 용 **Secure Hub**

이릴리스에는버그수정이포함되어있습니다.

Android 용 **Secure Hub**

Android 12 를지원합니다. 이번릴리스부터 Android 12 를실행하는장치에서 Secure Hub 가지원됩니다.

Secure Hub 21.8.0

iOS 용 **Secure Hub**

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.7.1

Android 용 **Secure Hub**

이미등록된기기에서 **Android 12** 를지원합니다**.** Android 12 로업그레이드하려는경우먼저 Secure Hub 를버전 21.7.1 로업데이트해야합니다. Secure Hub 21.7.1 은 Android 12 로업그레이드하는데필요한최소버전입니다. 이릴리스에서는이미등록된사용자를위해 Android 11 에서 Android 12 로원활하게업그레이드할수있습니다.

> 참고**:**
>
> Android 12 로업그레이드하기전에 Secure Hub 가버전 21.7.1 로업데이트되지않은경우이전기능을복구하려면장치를다시등록하거나공장초기화해야할수있습니다.
>
> Citrix 는 Android 12 에대한 1 일차지원을제공하기위해최선을다하고있으며 Android 12 를완벽하게지원하기위해후속버전의 Secure Hub 에업데이트를추가할예정입니다.

Secure Hub 21.7.0

iOS 용 **Secure Hub**

이릴리스에는버그수정이포함되어있습니다.

Android 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.6.0

iOS 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Android 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.5.1

iOS 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Android 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.5.0

iOS 용 Secure Hub

이릴리스에서는 MDX Toolkit 버전 19.8.0 이하로래핑된앱이더이상작동하지않습니다. 적절한기능을다시시작하려면최신 MDX Toolkit 으로앱을래핑해야합니다.

Secure Hub 21.4.0

Secure Hub 의색상이개선되었습니다. Secure Hub 는 Citrix 브랜드색상업데이트를준수합니다.

Secure Hub 21.3.2

iOS 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.3.0

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.2.0

Android 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 21.1.0

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 20.12.0

iOS 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Android 용 Secure Hub

Android 용 Secure Hub 는 Direct Boot 모드를지원합니다. Direct Boot 에대한자세한정보는 *Developer.android.com* 에서 Android 설명서를참조하십시오.

Secure Hub 20.11.0

Android 용 Secure Hub

Secure Hub 는 Android 10 에대한 Google Play 의현재대상 API 요구사항을지원합니다.

Secure Hub 20.10.5

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 20.9.0

iOS 용 Secure Hub

iOS 용 Secure Hub 는 iOS 14 을지원합니다.

Android 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 20.7.5

Android 용 Secure Hub

- Android 용 Secure Hub 는 Android 11 을지원합니다.
- 앱의경우 **Secure Hub 32** 비트에서 **64** 비트로전환합니다**.** Secure Hub 버전 20.7.5 에서는앱의 32 비트아키텍처에대한지원이종료되며, Secure Hub 는 64 비트로업데이트되었습니다. Citrix 에서는버전 20.6.5 에서 20.7.5 로업그레이드할것을권장합니다. 사용자가 Secure Hub 버전 20.6.5 로의업그레이드를건너뛰고대신 20.1.5 에서 20.7.5 로바로업그레이드할경우재인증이필요합니다. 재인증을수행하려면자격증명을입력하고 Secure Hub PIN 을재설정해야합니다. Secure Hub 버전 20.6.5 는 Google Play 스토어에서제공됩니다.
- **App Store** 에서업데이트를설치합니다**.** Android 용 Secure Hub 에서앱에사용가능한업데이트가있는경우앱이강조표시되고 App Store 화면에 사용가능한업데이트기능이나타납니다.

  사용가능한업데이트를탭하면업데이트대기중인앱목록이표시된스토어로이동합니다. 업데이트를설치하려면앱에대한 세부정보를탭합니다. 앱이업데이트되면 세부정보의아래쪽화살표가확인표시로변경됩니다.

Secure Hub 20.6.5

Android 용 Secure Hub

앱의경우 **32** 비트에서 **64** 비트로전환합니다**.** Secure Hub 20.6.5 릴리스는 Android 모바일앱용 32 비트아키텍처를지원하는마지막릴리스입니다. 이후릴리스에서 Secure Hub 는 64 비트아키텍처를지원합니다. Citrix 에서는사용자가재인증없이최신버전으로업그레이드할수있도록 Secure Hub 버전 20.6.5 로업그레이드할것을권장합니다. 사용자가 Secure Hub 버전 20.6.5 로의업그레이드를건너뛰고대신 20.7.5 로직접업데이트하는경우재인증이필요합니다. 재인증을수행하려면자격증명을입력하고 Secure Hub PIN 을재설정해야합니다.

> 참고**:**
>
> 20.6.5 릴리스는장치관리자모드에서 Android 10 을실행하는장치의등록을차단하지않습니다.

iOS 용 Secure Hub

iOS 장치에구성된프록시를활성화합니다**.** 사용자가 설정 **> Wi-Fi** 에서구성한프록시서버를사용할수있게하려면이제 iOS 용 Secure Hub 에서는새클라이언트속성 (`ALLOW_CLIENTSIDE_PROXY`) 을사용설정해야합니다. 자세한내용은 클라이언트속성참조의 `ALLOW_CLIENTSIDE_PROXY`에서참조하십시오.

Secure Hub 20.3.0

> 참고**:**
>
> Android 6.x 및 iOS 11.x 버전의 Secure Hub, Secure Mail, Secure Web 및 Citrix Workspace 앱에대한지원이 2020 년 6 월에종료됩니다.

iOS 용 Secure Hub

- 네트워크확장사용안함. App Store 검토지침에대한최근변경으로인해릴리스 20.3.0 부터 Secure Hub 는 iOS 를실행하는장치에서 NE(네트워크확장) 를지원하지않습니다. NE 는 Citrix 가개발한모바일생산성앱에는영향을미치지않습니다. 그러나 NE 를제거하면배포된엔터프라이즈 MDX 래핑앱에약간의영향이있습니다. 권한부여토큰, 타이머및 PIN 재시도와같은구성요소를동기화하는동안최종사용자의 Secure Hub 에서추가전환이발생할수있습니다. 자세한내용은 https://support.citrix.com/article/CTX270296 항목을참조하십시오.

> 참고:
>
> 새사용자에게는 VPN 설치메시지가표시되지않습니다.

- 향상된등록프로필지원. Secure Hub 는 등록프로필지원에서 Citrix Endpoint Management 에대해발표한향상된등록프로필기능을지원합니다.

Secure Hub 20.2.0

iOS 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 20.1.5

이릴리스에는다음이포함되어있습니다.

- 업데이트된사용자개인정보보호정책서식및표시. 이기능업데이트로인해 Secure Hub 등록과정이변경됩니다.
- 버그수정

Secure Hub 19.12.5

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 19.11.5

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 19.10.5

Android 용 Secure Hub

COPE 모드에서 **Secure Hub** 등록. COPE 등록프로필에 Citrix Endpoint Management 가구성된경우 Android Enterprise 장치에서 COPE(회사소유개인사용) 모드로 Secure Hub 를등록할수있습니다.

Secure Hub 19.10.0

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 19.9.5

iOS 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Android 용 Secure Hub

Android Enterprise 작업프로필및완전히관리되는장치에대한 **Keyguard** 관리기능지원**.** Android Keyguard 는장치 및 Work Challenge 잠금화면을관리합니다. Citrix Endpoint Management 의 Keyguard 관리장치정책을사용하여작업프로필장치의 Keyguard 관리와완전히관리되는장치및전용장치의 Keyguard 관리를제어할수있습니다. Keyguard 관리를사용하면 Keyguard 화면을잠금해제하기전에사용자가사용할수있는기능 (예: 신뢰에이전트및보안카메라) 을지정할수있습니다. 또는모든 Keyguard 기능을사용하지않도록선택할수있습니다.

기능설정및장치정책구성방법에대한자세한내용은 Keyguard 관리장치정책을참조하십시오.

Secure Hub 19.9.0

iOS 용 Secure Hub

iOS 용 Secure Hub 는 iOS 13 을지원합니다.

Android 용 Secure Hub

이릴리스에는버그수정이포함되어있습니다.

Android 용 Secure Hub 19.8.5

이릴리스에는버그수정이포함되어있습니다.

Secure Hub 19.8.0

iOS 용 Secure Hub

이릴리스에는성능개선사항및버그수정이포함되어있습니다.

Android 용 Secure Hub

Android Q 지원. 이릴리스에는 Android Q 에대한지원이포함되어있습니다. Android Q 플랫폼으로업그레이드하기전에 Google Device Administration API 의사용중단이 Android Q 를실행하는장치에미치는영향에대해 장치관리에서 Android Enterprise 로마이그레이션에서자세한내용을참조하십시오. 또한블로그 Citrix Endpoint Management and Android Enterprise - a Season of Change(Citrix Endpoint Management 및 Android Enterprise - 변화의계절)의내용을참조하십시오.

Secure Hub 19.7.5

iOS 용 Secure Hub

이릴리스에는성능개선사항및버그수정이포함되어있습니다.

Android 용 Secure Hub

Samsung Knox SDK 3.x. 지원 Android 용 Secure Hub 가 Samsung Knox SDK 3.x 를지원합니다. Samsung Knox 3.x 로마이그레이션하는방법에대한자세한내용은 Samsung Knox 개발자설명서를참조하십시오. 이릴리스에는새로운 Samsung Knox 네임스페이스에대한지원도포함되어있습니다. 이전 Samsung Knox 네임스페이스로변경하는방법에대한자세한내용은 이전 Samsung Knox 네임스페이스변경사항에서참조하십시오.

> 참고:
>
> Android 용 Secure Hub 는 Android 5 를실행하는 Samsung Knox 3.x 장치를지원하지않습니다.

Secure Hub 19.3.5 ~ 19.6.6

이러한릴리스에는성능개선사항및버그수정이포함되어있습니다.

Secure Hub 19.3.0

엔터프라이즈용 **Samsung Knox** 플랫폼지원. Android 용 Secure Hub 는 Android Enterprise 장치에서 KPE(엔터프라이즈용 Knox 플랫폼) 를지원합니다.

Secure Hub 19.2.0

이릴리스에는성능개선사항및버그수정이포함되어있습니다.

Secure Hub 19.1.5

Android Enterprise 용 Secure Hub 는이제다음과같은정책을지원합니다.

- **WiFi** 장치정책. Wi-Fi 장치정책이이제 Android Enterprise 를지원합니다. 이정책에대한자세한내용은 Wi-Fi 장치정책을참조하십시오.

- 사용자지정 **XML** 장치정책**.** 사용자지정 XML 장치정책이이제 Android Enterprise 를지원합니다. 이정책에대한자세한내용은 사용자지정 XML 장치정책을참조하십시오.
- 파일장치정책**.** Citrix Endpoint Management 에스크립트파일을추가하여 Android Enterprise 장치에서기능을수행할수있습니다. 이정책에대한자세한내용은 파일장치정책을참조하십시오.

Secure Hub 19.1.0

Secure Hub 의글꼴**,** 색상및기타 **UI** 항목이개선되었습니다**.** 이로써전체모바일생산성앱제품군에 Citrix 브랜드의심미성을따른뛰어난사용자환경이구현되었습니다.

Secure Hub 18.12.0

이릴리스에는성능개선사항및버그수정이포함되어있습니다.

Secure Hub 18.11.5

- **Android Enterprise** 에대한제한사항장치정책설정**.** 제한사항장치정책에대한새로운설정은 Android Enterprise 장치에서다음과같은기능에대한사용자액세스를허용합니다. Android Enterprise 장치의상태표시줄, 잠금화면키보호, 계정관리, 위치공유및장치화면을켠상태로유지. 자세한내용은 Restrictions device policy(제한장치정책)를참조하십시오.

Secure Hub 18.10.5~18.11.0 에는성능향상기능및버그수정이포함되어있습니다.

Secure Hub 18.10.0

- **Samsung DeX** 모드지원**:** Samsung DeX 를사용하면 KNOX 기반장치를외부디스플레이에연결하여 PC 와같은인터페이스에서앱을사용하고문서를검토하며비디오를볼수있습니다. Samsung DeX 장치요구사항및 Samsung DeX 설정방법에대한자세한내용은 How Samsung DeX works(Samsung Dex 작동방식)을참조하십시오.

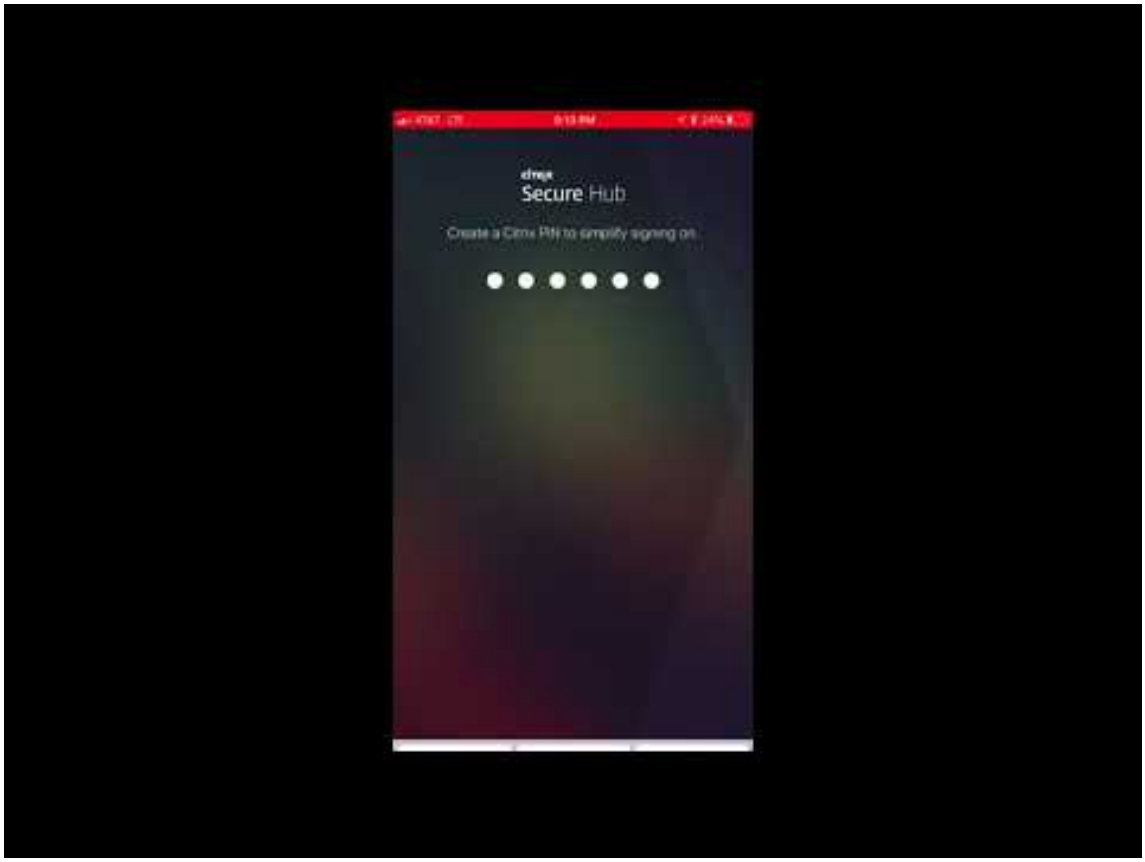
  Citrix Endpoint Management 에서 Samsung DeX 모드기능을구성하려면 Samsung Knox 에대한제한장치정책을업데이트합니다. 자세한내용은 **Samsung KNOX settings(Samsung KNOX** 설정**)** 및 Restrictions device policy(제한장치정책)를참조하십시오.
- **Android SafetyNet** 지원**:** Secure Hub 가설치된 Android 장치의호환성및보안을평가하기위해 **Android SafetyNet** 기능을사용하도록 Endpoint Management 를구성할수있습니다. 평가결과를토대로장치에대한자동화된작업을트리거할수있습니다. 자세한내용은 Android SafetyNet을참조하십시오.
- **Android Enterprise** 장치의카메라사용제한**:** 제한장치정책의새로운 카메라사용허용설정을통해 Android Enterprise 장치에서카메라를사용하지못하도록제한할수있습니다. 자세한내용은 Restrictions device policy(제한장치정책)를참조하십시오.

Secure Hub 10.8.60 ~ 18.9.0

이러한릴리스에는성능개선사항및버그수정이포함되어있습니다.

Secure Hub 10.8.60

- 폴란드어지원
- Android P 지원
- Workspace 앱스토어사용지원
  Secure Hub 를열때 Secure Hub 스토어가더이상표시되지않습니다. 앱추가단추를누르면 Workspace 앱스토어로이동합니다. 다음비디오에서는 Citrix Workspace 앱을사용하여 Citrix Endpoint Management 에등록하는 iOS 장치를보여줍니다.



> 중요:
>
> 이기능은새로운고객만사용할수있습니다. 기존고객을위한마이그레이션은현재지원되지않습니다.

이기능을사용하려면다음과같이구성합니다.

  - 암호캐싱및암호인증정책을사용하도록설정합니다. 정책을구성하는것에대한자세한내용은 모바일생산성앱의 MDX 정책요약을참조하십시오.

- AD 또는 AD+Cert 로 Active Directory 인증을구성합니다. 이러한두가지모드가지원됩니다. 인증을구성하는 것에대한자세한내용은 도메인인증또는도메인및보안토큰인증을참조하십시오.
- Endpoint Management 에대한 Workspace 통합기능을사용하도록설정합니다. Workspace 통합에대한 자세한내용은 Workspace 구성을참조하십시오.

> 중요:
>
> 이기능을사용하도록설정하면 Citrix Files SSO 가 Endpoint Management(이전명칭: XenMobile) 대신 Workspace 를통해이루어집니다. Workspace 통합기능을사용하도록설정하기전에 Endpoint Management 콘솔에서 Citrix Files 통합기능을사용하지않도록설정하는것이좋습니다.

Secure Hub 10.8.55

- 구성 JSON 을사용하여 Google 제로터치및 Samsung KME(Knox Mobile Environment) 포털의사용자이름과 암호를전달할수있습니다. 자세한내용은 Samsung Knox 대량등록을참조하십시오.
- 인증서고정을사용하도록설정하면사용자가자체서명된인증서로 Endpoint Management 에등록할수없습니다. 자체 서명된인증서로 Endpoint Management 에등록하려고하면인증서를신뢰할수없다는내용의경고가표시됩니다.

Secure Hub 10.8.25: Android 용 Secure Hub 에 Android P 장치에대한지원이포함됩니다.

> 참고:
>
> Android P 플랫폼으로업그레이드하기전에: 서버인프라가 subjectAltName(SAN) 확장에일치하는호스트이름을가진보안인증서와호환되는지확인하십시오. 호스트이름을확인하려면서버가일치하는 SAN 이포함된인증서를제공해야합니다. 호스트이름과일치하는 SAN 이포함되지않은인증서는더이상신뢰할수없습니다. 자세한내용은 Android 개발자설명서를참조하십시오.

iOS 용 Secure Hub 의 2018 년 3 월 19 일업데이트: iOS 용 Secure Hub 버전 10.8.6 을사용하여 VPP 앱정책관련문제를해결할수있습니다. 자세한내용은이 Citrix Knowledge Center 문서를참조하십시오.

Secure Hub 10.8.5: Android 용 Secure Hub 에서 Android Work(Android for Work) 의 COSU 모드가지원됩니다. 자세한내용은 Citrix Endpoint Management 설명서를참조하십시오.

Secure Hub 관리

Endpoint Management 초기구성중에 Secure Hub 와관련된관리작업의대부분이수행됩니다. iOS 및 Android 에서사용자가 Secure Hub 를사용할수있게하려면 iOS App Store 및 Google Play Store 에 Secure Hub 를업로드합니다.

Secure Hub 는인증된이후사용자의 Citrix Gateway 세션이갱신될때 Citrix Gateway 를사용하여설치된앱에대해 Endpoint Management 에저장된대부분의 MDX 정책을새로고칩니다.

> 중요:
>
> 보안그룹, 암호화사용및 Secure Mail Exchange Server 정책중하나를변경한경우사용자가앱을삭제하고다시설치하여업데이트된정책을적용해야합니다.

Citrix PIN

Endpoint Management 콘솔의 설정 > 클라이언트속성에설정된보안기능인 Citrix PIN 을사용하도록 Secure Hub 를구성할수있습니다. 이설정에서는등록된모바일장치사용자가 Secure Hub 에로그온하고 MDX 래핑된앱을 PIN(개인식별번호)을사용하여활성화해야합니다.

Citrix PIN 기능을사용하면래핑된보안앱에로그온할때사용자인증환경이간소화됩니다. 사용자는 Active Directory 사용자이름및암호같은다른자격증명을반복적으로입력하지않아도됩니다.

Secure Hub 에처음로그인하는사용자는 Active Directory 사용자이름및암호를입력해야합니다. 로그인중에 Secure Hub 는 Active Directory 자격증명또는클라이언트인증서를사용자장치에저장한후, 사용자에게 PIN 을입력하라는메시지를표시합니다. 사용자가다시로그온할경우, 사용자는 PIN 을입력하여활성사용자세션에대한다음유휴시간초과기간이끝날때까지 Citrix 앱및저장소에안전하게액세스합니다. 관련된클라이언트속성을통해 PIN 을사용하여비밀정보를암호화할수있으며 PIN 암호유형을지정하고 PIN 강도및길이요구사항을지정할수있습니다. 자세한내용은 클라이언트속성을참조하십시오.

지문인증 (Touch ID) 을사용하도록설정하면사용자는앱이비활성화되어오프라인인증이필요한경우에지문을사용하여로그온할수있습니다. 사용자는 Secure Hub 에처음로그인할때, 장치를재시작할때그리고비활성화타이머가만료된후에는여전히 PIN 을입력해야합니다. 지문인증사용에대한자세한내용은 지문또는 Touch ID 인증을참조하십시오.

인증서고정

iOS 및 Android 용 Secure Hub 는 SSL 인증서고정을지원합니다. 이기능은 Citrix 클라이언트가 Endpoint Management 와통신할때기업에서서명한인증서가사용되도록하여장치에서의루트인증서설치로인해 SSL 세션이손상될경우클라이언트에서 Endpoint Management 로연결되지못하게합니다. Secure Hub 에서서버공개키변경을감지하면 Secure Hub 는연결을거부합니다.

Android N 의경우, 이운영체제는사용자가추가한 CA(인증기관) 를더이상허용하지않습니다. Citrix 에서는사용자가추가한 CA 대신공용루트 CA 를사용하도록권장합니다.

Android N 으로업그레이드하는사용자가개인또는자체서명 CA 를사용할경우문제를겪을수있습니다. 다음시나리오에서는 Android N 장치에서의연결이끊깁니다.

- Endpoint Management 에대한개인/자체서명 CA 및필요한신뢰된 CA 옵션은 켜짐으로설정되어있습니다. 자세한내용은 장치관리를참조하십시오.
- 개인/자체서명 CA 와 Endpoint Management ADS(자동검색서비스) 를연결할수없습니다. ADS 에연결할수없으면, 보안을고려하여필요한신뢰할수있는 CA 가초기에 꺼짐으로설정되었더라도 켜짐으로바뀝니다.

장치를등록하거나 Secure Hub 를업그레이드하기전에인증서고정을사용하도록설정하는것이좋습니다. 이옵션은기본적으로 꺼짐으로설정되며 ADS 를통해관리됩니다. 인증서고정을사용하도록설정하면사용자가자체서명된인증서로 Endpoint Management 에등록할수없습니다. 자체서명된인증서로등록하려고하면인증서를신뢰할수없다는내용의경고가표시됩니다. 사용자가인증서를수락하지않으면등록이실패합니다.

인증서고정을사용하려면 Citrix 에인증서를 Citrix ADS 서버에업로드해달라고요청합니다. Citrix 지원포털을사용하여기술지원사례를엽니다. 개인키를 Citrix 에보내지않도록합니다. 이후다음정보를입력합니다.

- 사용자가등록될계정을포함하는도메인

- Endpoint Management 의 FQDN(정규화된도메인이름)
- Endpoint Management 의인스턴스이름. 기본적으로인스턴스이름은 zdm 이고대/소문자를구분합니다.
- 사용자 ID 유형 (UPN 또는전자메일일수있음). 기본적으로이유형은 UPN 입니다.
- iOS 등록에사용된포트 (포트번호를기본포트 8443 에서변경한경우)
- Endpoint Management 가연결을받아들이는포트 (포트번호를기본포트 443 에서변경한경우)
- Citrix Gateway 의전체 URL.
- 또는관리자의전자메일주소
- 도메인에추가할 PEM 형식의인증서입니다. 이인증서는개인키가아닌공개인증서여야합니다.
- 기존서버인증서를처리하는방식: 오래된서버인증서가손상되어즉시제거할지또는만료될때까지오래된서버인증서를계속지원할지여부

세부정보및인증서가 Citrix 서버에추가되면기술지원사례가업데이트됩니다.

인증서 **+** 일회용암호인증

Secure Hub 가인증서및일회용암호역할을하는보안토큰을사용하여인증되도록 Citrix ADC 를구성할수있습니다. 이구성은 Active Directory 흔적을장치에남기지않는강력한보안옵션을제공합니다.

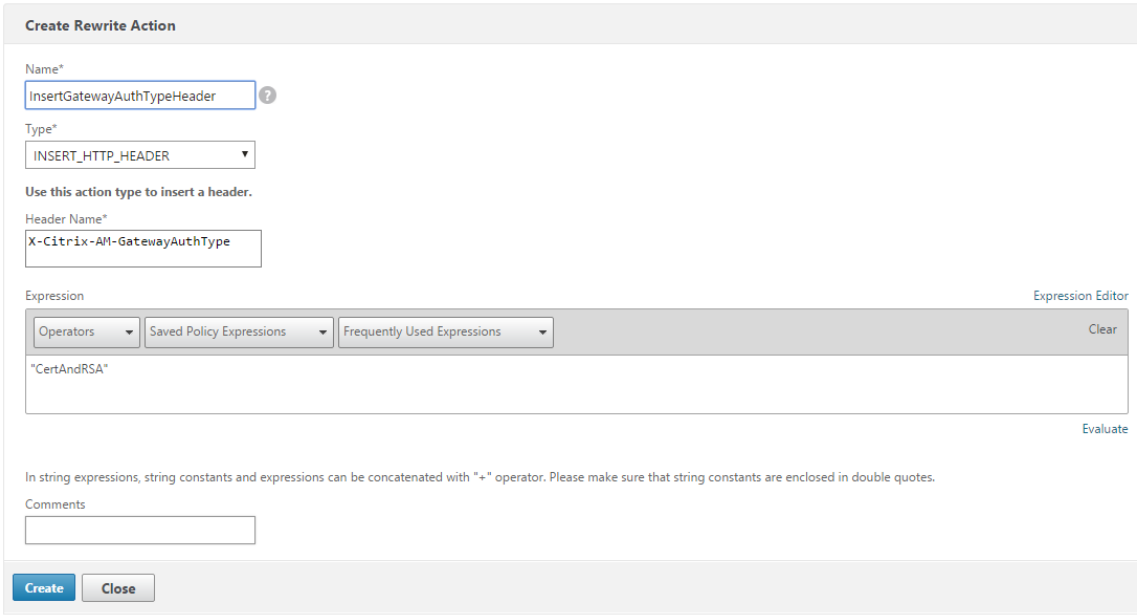
Secure Hub 가인증서 + 일회용암호인증유형을사용하도록설정하려면 Citrix Gateway 로그온유형을나타내기위해 **X-Citrix-AM-GatewayAuthType: CertAndRSA** 형태의사용자지정응답헤더를삽입하는다시쓰기작업및다시쓰기정책을 Citrix ADC 에서추가합니다.

일반적으로 Secure Hub 는 Endpoint Management 콘솔에서구성한 Citrix Gateway 로그온유형을사용합니다. 그러나 Secure Hub 가로그온을처음완료할때까지는 Secure Hub 에서이정보를사용할수없기때문에사용자지정헤더가필요합니다.

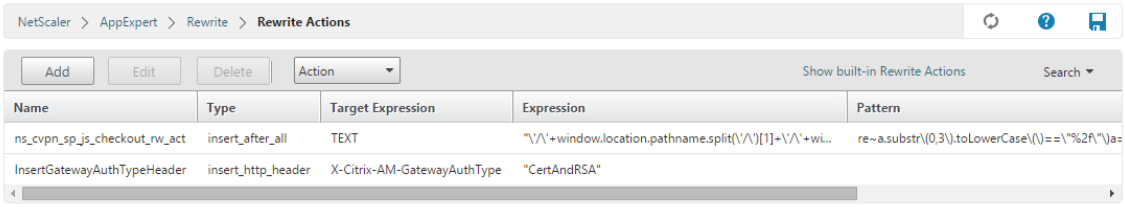
> 참고**:**
>
> 여러가지로그온유형이 Endpoint Management 및 Citrix ADC 에설정된경우, Citrix ADC 구성이우선합니다. 자세한내용은 Citrix Gateway 및 Endpoint Management를참조하십시오.

1. Citrix ADC 에서 **Configuration(**구성**) > AppExpert > Rewrite(**다시쓰기**) > Actions(**작업**)** 로이동합니다.
2. 추가를클릭합니다.

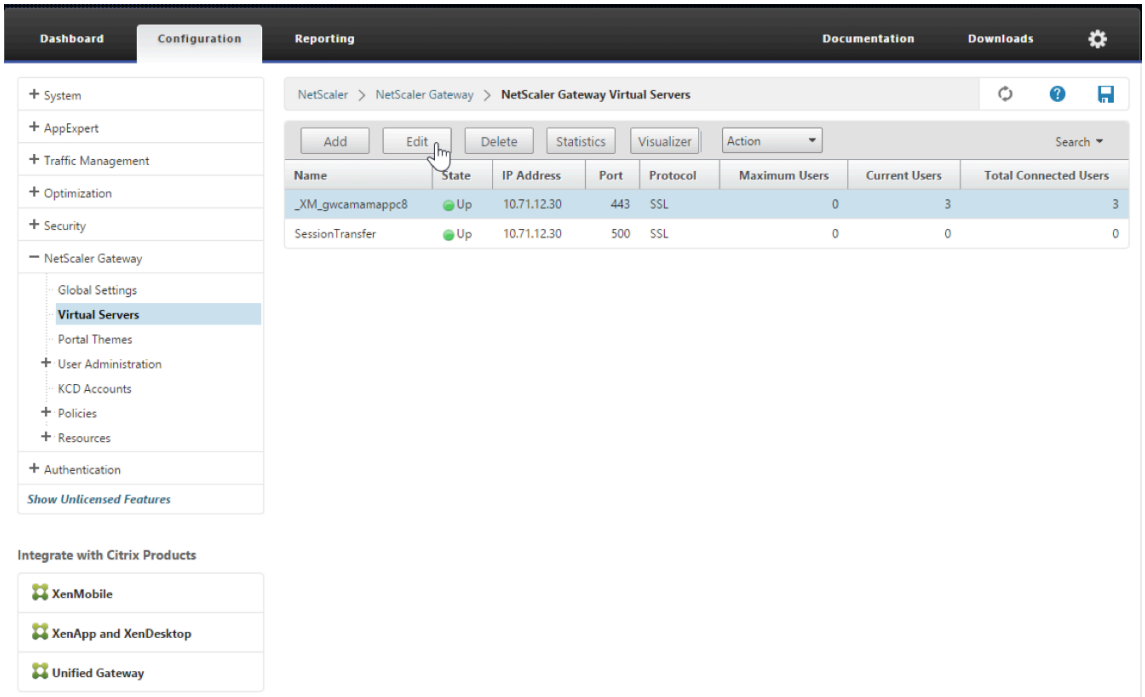
   Create Rewrite Action(다시쓰기작업만들기**)** 화면이나타납니다.
3. 다음그림과같이각필드를채우고 **Create(**만들기**)** 를클릭합니다.



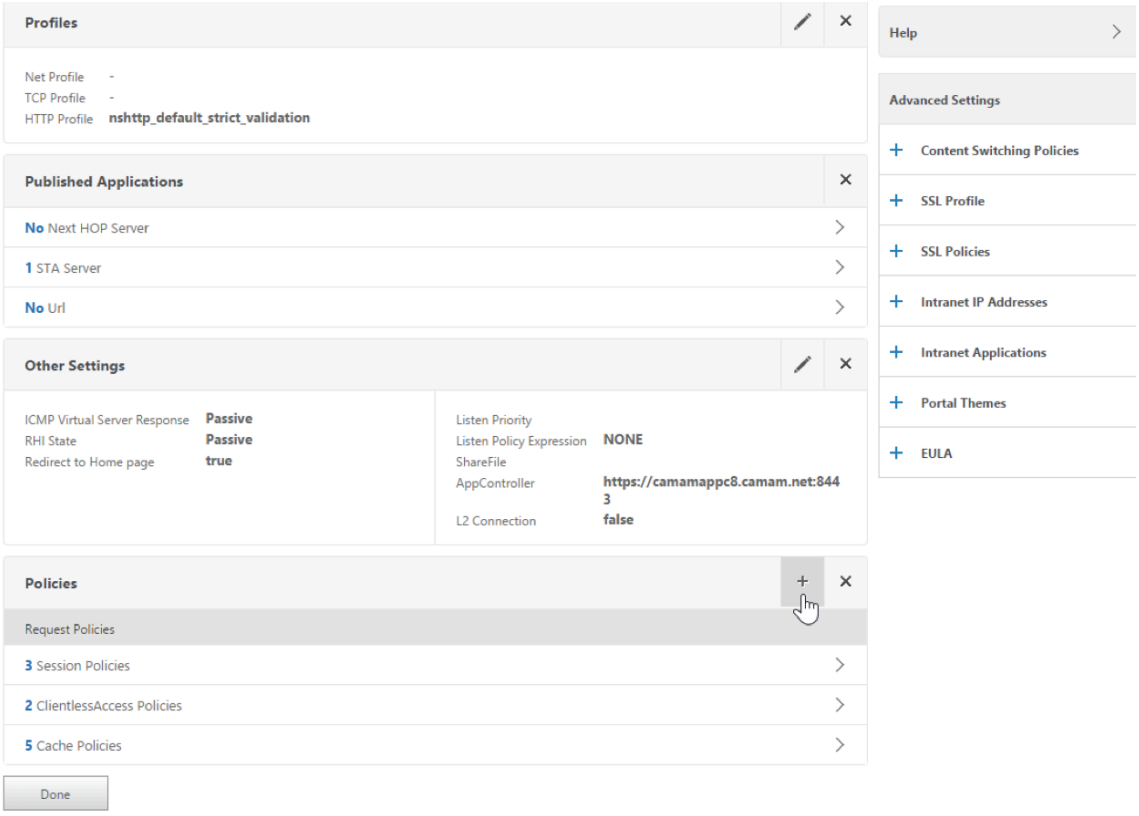
기본 **Rewrite Actions(**다시쓰기작업**)** 화면에다음결과가나타납니다.



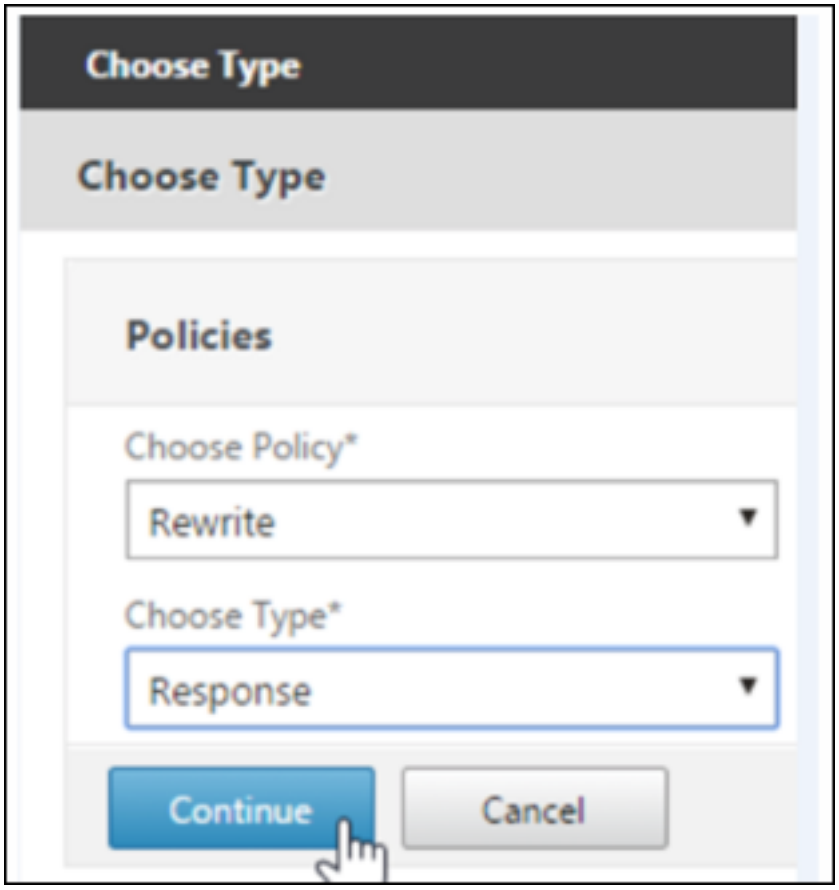
4. 다시쓰기작업을가상서버에다시쓰기정책으로바인딩합니다. **Configuration(**구성**) > NetScaler Gateway > Virtual Servers(**가상서버**)** 로이동한후, 가상서버를선택합니다.



5. 편집을클릭합니다.
6. **Virtual Servers configuration(**가상서버구성**)** 화면에서아래로스크롤하여 **Policies(**정책**)** 로이동합니다.
7. **+** 를클릭하여정책을추가합니다.

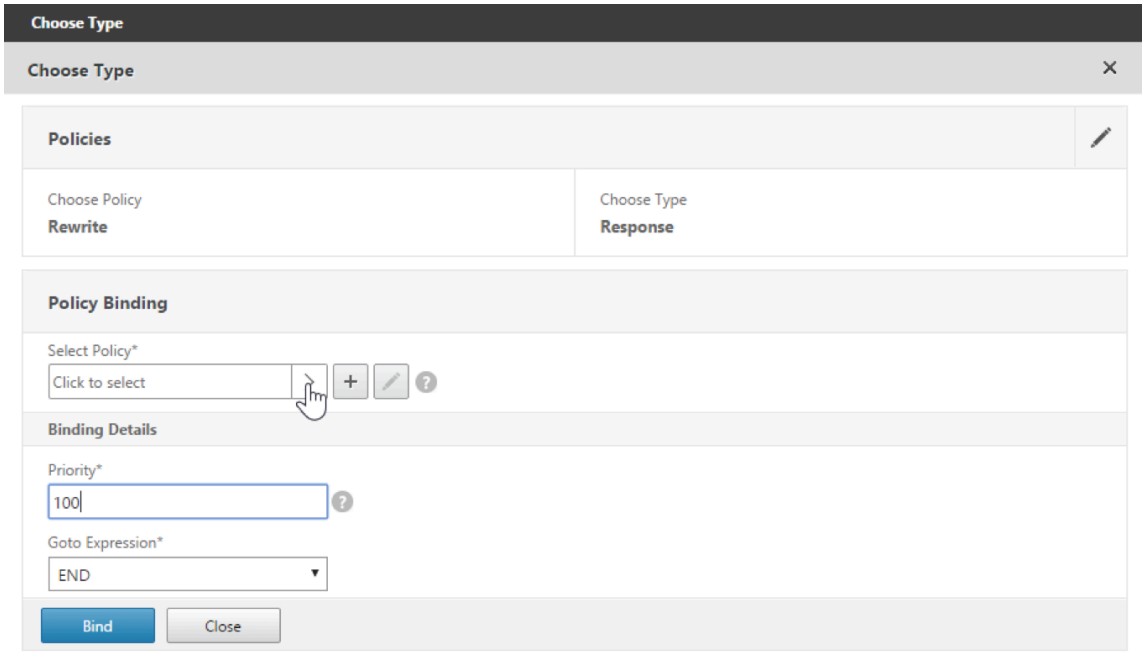


8. **Choose Policy(**정책선택**)** 필드에서 **Rewrite(**다시쓰기**)** 를선택합니다.
9. **Choose Type(**유형선택**)** 필드에서 **Response(**응답**)** 를선택합니다.



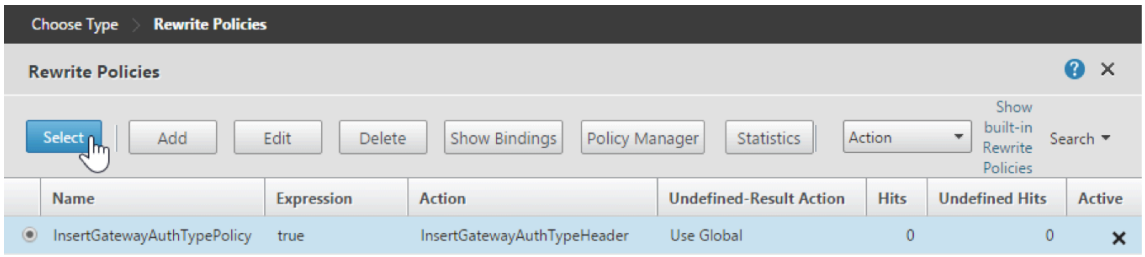
10. **Continue(**계속**)** 을클릭합니다.

    Policy Binding(정책바인딩**)** 섹션이확장됩니다.

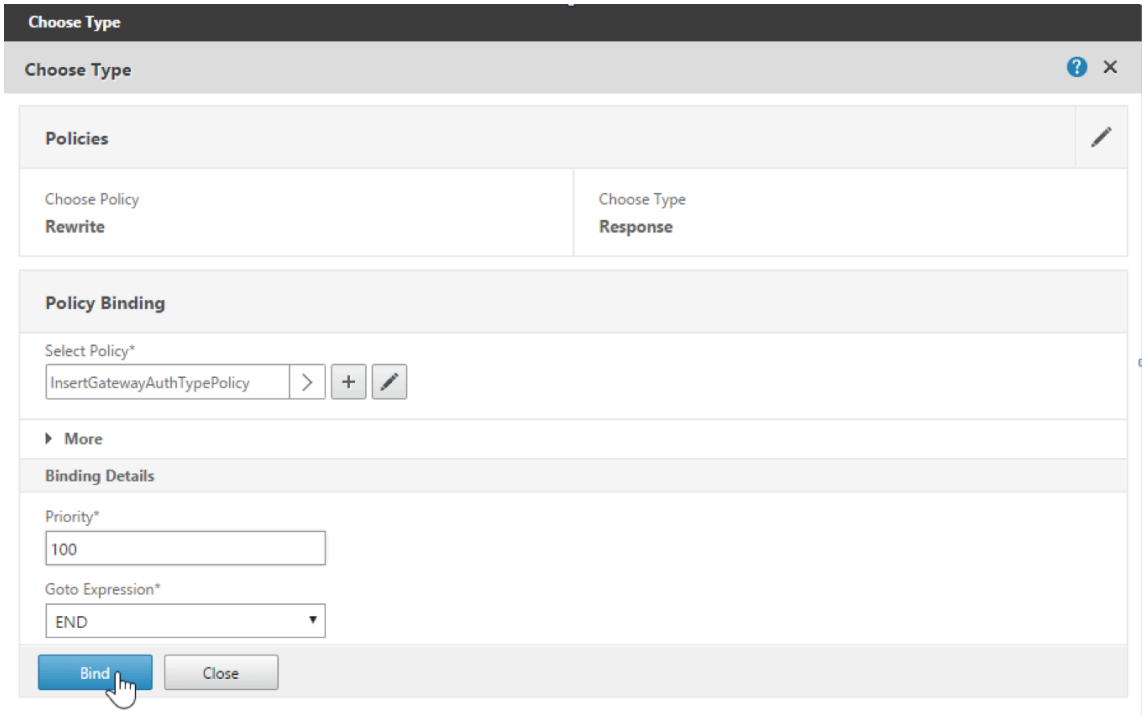


11. **Select Policy(**정책선택**)** 를클릭합니다.

    사용가능한정책을포함하는화면이나타납니다.

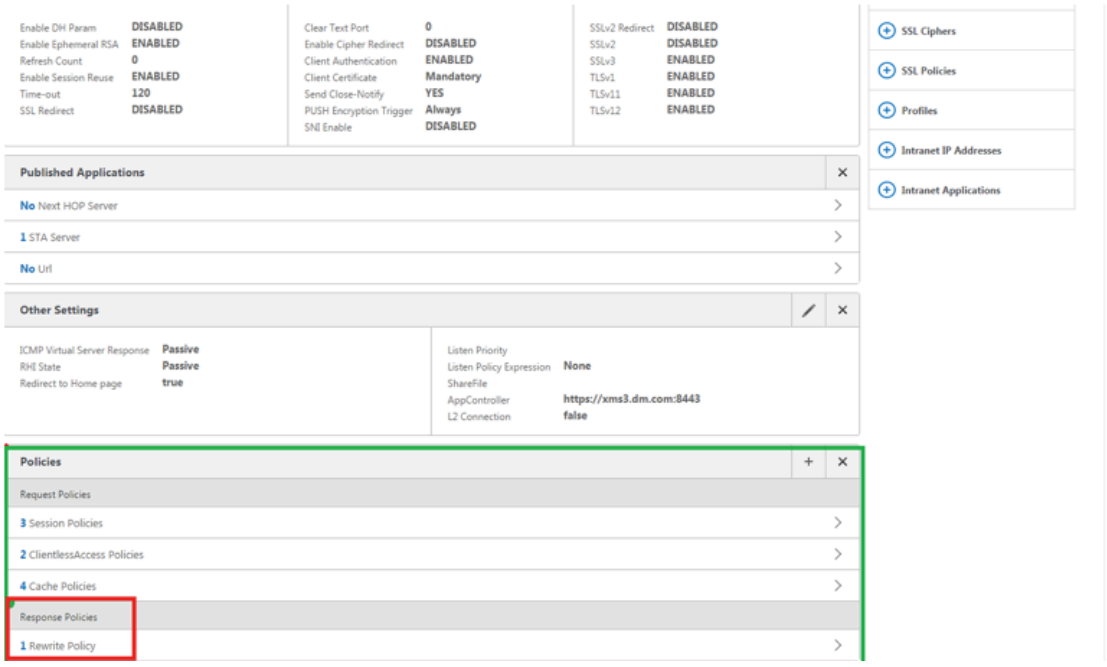


12. 앞에서생성한정책의행을클릭한후 **Select(**선택**)** 를클릭합니다. 선택한정책이채워진채로 **Policy Binding(**정책바인딩**)** 화면이다시나타납니다.

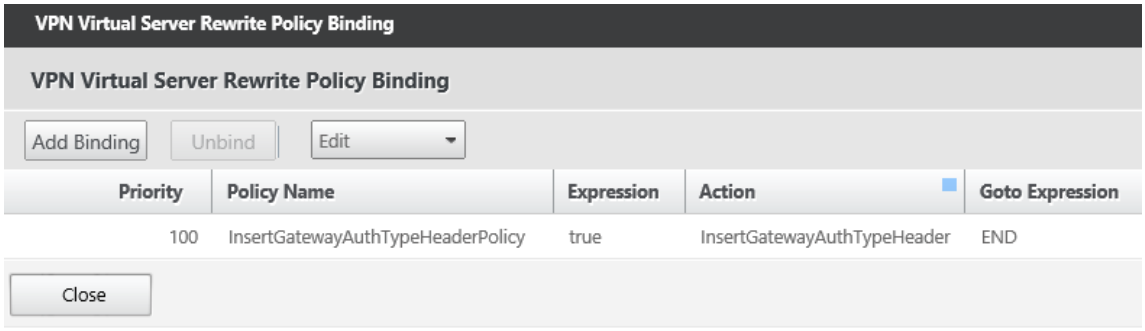


13. **Bind(**바인딩**)** 를클릭합니다.

    바인딩이성공적이면기본구성화면이나타나고완성된다시쓰기정책이표시됩니다.



14. 정책세부정보를보려면 **Rewrite Policy(**다시쓰기정책**)** 를클릭합니다.



Android 장치의 **ADS** 연결을위한포트요구사항

포트구성은 Secure Hub 로부터연결되는 Android 장치가회사네트워크내에서 Citrix ADS 에액세스할수있도록합니다. ADS 를통해사용가능해진보안업데이트를다운로드할경우 ADS 에액세스할수있는것이중요합니다. 프록시서버에서 ADS 연결이작동하지않을수있습니다. 이시나리오에서는 ADS 연결이프록시서버를우회할수있게허용합니다.

> 중요:
>
> Android 및 iOS 용 Secure Hub 의경우 Android 장치가 ADS 에액세스하도록허용해야합니다. 자세한내용은 Citrix Endpoint Management 설명서에서 포트요구사항을참조하십시오. 이통신은아웃바운드포트 443 을통해이루어집니다. 기존환경은이액세스를허용하도록설계되었을가능성이매우높습니다. 이통신을지원할수없는고객은 Secure Hub 10.2 로업그레이드하지않는것이좋습니다. 궁금한점이있으면 Citrix 지원팀에문의하십시오.

사전요구사항:

- Endpoint Management 및 Citrix ADC 인증서를수집합니다. 인증서는 PEM 형식이어야하고공용인증서여야하며 개인키가아니어야합니다.
- Citrix 지원팀에연락하여인증서고정을사용하기위한요청을제출하십시오. 이과정에서인증서를요구받게됩니다.

개선된새인증서고정에서는장치등록전에장치가 ADS 에연결되어야합니다. 그러면장치가등록되고있는환경에서 Secure Hub 가최신보안정보를사용할수있게됩니다. 장치가 ADS 에연결할수없으면 Secure Hub 는장치등록을허용하지않습니다. 따라서 내부네트워크내에서 ADS 액세스를가능하게하는것은장치가등록될수있게하는데매우중요합니다.

Android 용 Secure Hub 에대해 ADS 액세스를허용하려면다음 IP 주소및 FQDN 으로포트 443 을엽니다.

FQDN	IP 주소	포트	IP 및포트사용
`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
`ads.xm.cloud.com`: Secure Hub 버전 10.6.15 이상은다음사용: `ads.xm.cloud.com`.	34.194.83.188	443	Secure Hub - ADS 통신

FQDN	IP 주소	포트	IP 및포트사용
ads.xm.cloud.com: Secure Hub 버전 10.6.15 이상은다음사용: ads.xm.cloud.com.	34.193.202.23	443	Secure Hub - ADS 통신

인증서고정이사용설정된경우:

- Secure Hub 는장치등록중에엔터프라이즈인증서를고정합니다.
- 업그레이드중에 Secure Hub 는현재고정되어있는인증서를폐기한후등록된사용자의첫번째연결에서서버인증서를고정합니다.

  > 참고:
  >
  > 업그레이드이후인증서고정을사용하도록설정한경우사용자가다시등록해야합니다.

- 인증서공개키가변경되지않은경우인증서갱신에는재등록이필요하지않습니다.

인증서고정은중간또는발급자인증서가아니라리프인증서를지원합니다. 인증서고정은타사서버가아니라 Endpoint Management 및 Citrix Gateway 등의 Citrix 서버에적용됩니다.

계정삭제옵션비활성화

ADS(자동검색서비스) 가사용설정된환경에서 Secure Hub 의 계정삭제옵션을사용중지할수있습니다.

계정삭제옵션을사용중지하려면다음단계를수행하십시오.

1. 도메인의 ADS 를구성합니다.
2. Citrix Endpoint Management 에서 자동검색서비스정보를열고 `displayReenrollLink` 값을 **False** 로설정합니다.
   기본적으로이값은 **True** 입니다.
3. 장치가 MDM+MAM(ENT) 모드로등록된경우로그오프한후다시로그인하여변경사항을적용하십시오.
   장치가다른모드로등록되어있는경우다시등록해야합니다.

Secure Hub 사용

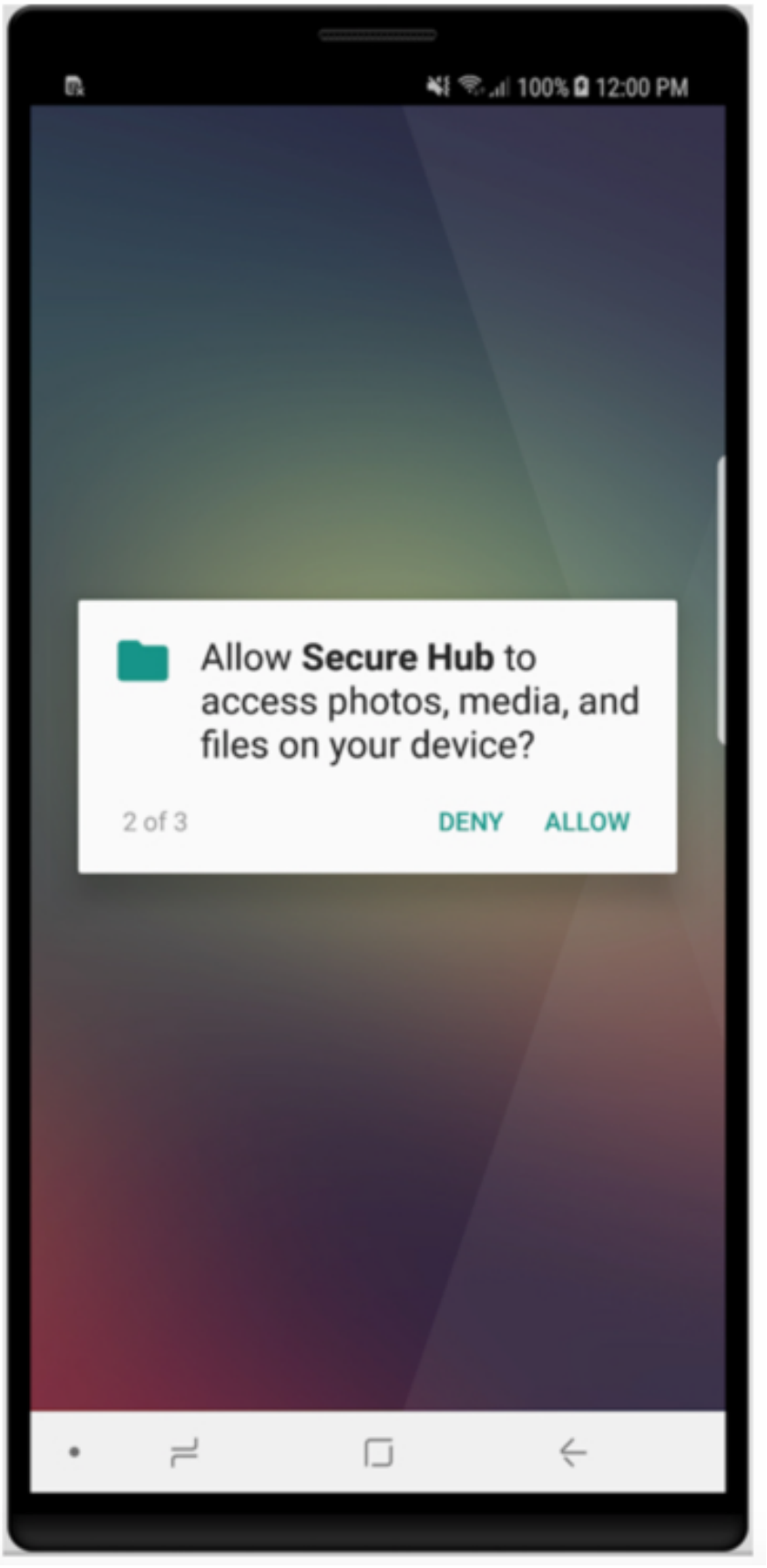
사용자는먼저 Apple 또는 Android 스토어에서장치로 Secure Hub 를다운로드합니다.

Secure Hub 가열리면사용자는회사에서제공한자격증명을입력하여 Secure Hub 에장치를등록합니다. 장치등록에대한자세한내용은 사용자, 계정, 역할및등록을참조하십시오.

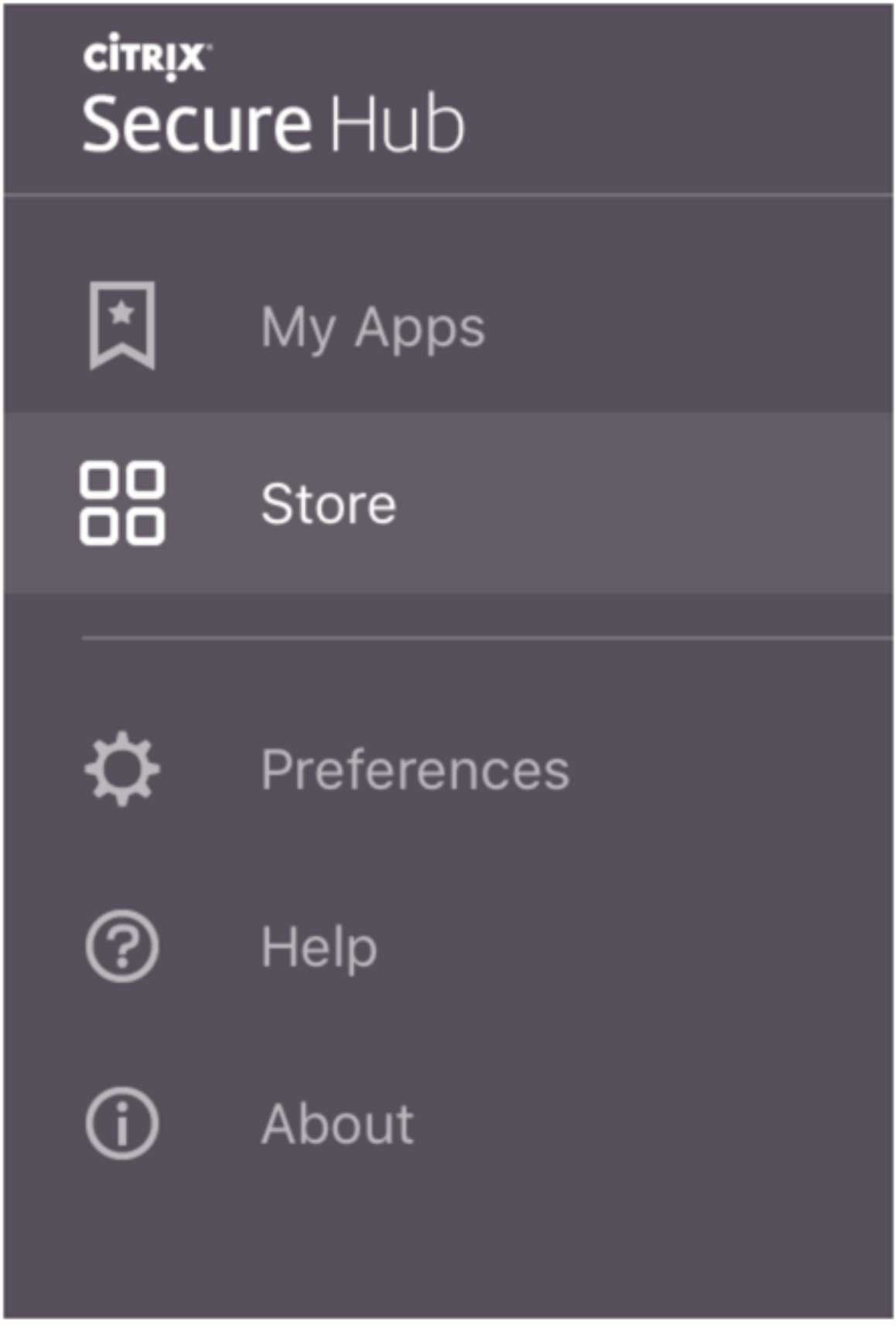
Android 용 Secure Hub 에서초기설치및등록시다음메시지가나타납니다. “Allow Secure Hub to access photos, media, and files on your device?(Secure Hub 가장치의사진, 미디어및파일에액세스하도록허용하시겠습니까?)”

이메시지는 Citrix 가아닌 Android 운영체제의메시지입니다. **Allow(**허용**)** 을탭하더라도 Citrix 와 Secure Hub 를관리하는관리자가사용자의개인데이터를아무때나보는것은아닙니다. 하지만관리자와원격지원세션을수행하는경우관리자가세션내에서사용자의개인파일을볼수있습니다.

등록된후에사용자는 내앱탭에서푸시한앱및데스크톱을볼수있습니다. 사용자는저장소의앱을더추가할수있습니다. 전화기에서저장소링크는왼쪽맨위의 설정햄버거아이콘아래에있습니다.



태블릿에서는저장소가별도탭입니다.



iOS 9 이상을실행하는 iPhone 사용자가스토어에서모바일생산성앱을설치할경우 Enterprise 개발자인 Citrix 는해당 iPhone 에서신뢰되지않는다는메시지가표시됩니다. 이메시지는개발자가신뢰될때까지해당앱을사용할수없음을나타냅니다. 이 메시지가나타나면 Secure Hub 는 Citrix 엔터프라이즈앱이 iPhone 에서신뢰되도록하는과정을안내하는가이드를살펴볼것 을사용자에게요청합니다.

Secure Mail 에자동등록

MAM 전용배포의경우, 전자메일자격증명을사용하여 Secure Hub 에등록한 Android 또는 iOS 장치사용자가자동으로 Secure Mail 에서등록되도록 Endpoint Management 를구성할수있습니다. 따라서 Secure Mail 에서등록하기위해사 용자가더많은정보를입력하거나더많은절차를거치지않아도됩니다.

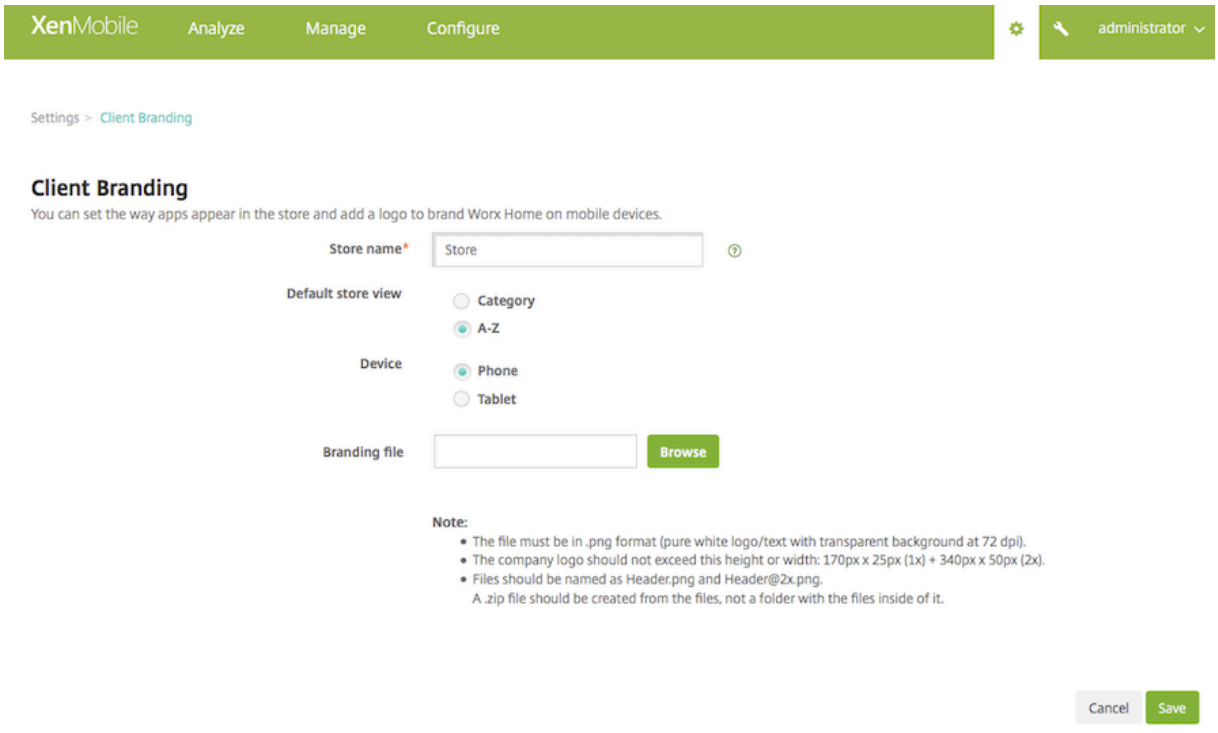
Secure Mail 을처음사용할때 Secure Mail 은사용자의전자메일주소, 도메인및사용자 ID 를 Secure Hub 로부터얻습니다. Secure Mail 은전자메일주소를자동검색에사용합니다. Exchange Server 는도메인및사용자 ID 를사용하여식별되고, 이를 통해 Secure Mail 이사용자를자동으로인증할수있습니다. 암호를전달하지못하도록정책이설정된경우암호를입력하라는메시지 가사용자에게표시됩니다. 하지만사용자는이외의정보를입력하지않아도됩니다.

이기능을사용설정하려면다음세가지속성을생성합니다.

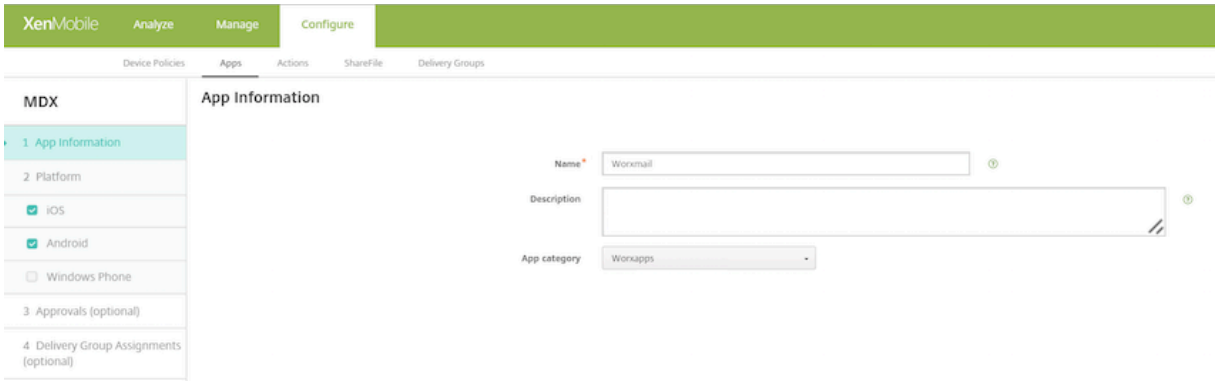
- 서버속성 MAM_MACRO_SUPPORT. 지침은 서버속성을참조하십시오.
- 클라이언트속성 ENABLE_CREDENTIAL_STORE 및 SEND_LDAP_ATTRIBUTES. 지침은 클라이언트속성을참 조하십시오.

사용자지정된스토어

저장소를사용자지정하려면 설정 **>** 클라이언트브랜딩으로이동하여이름을변경하고로고를추가하고앱표시방식을지정합니다.



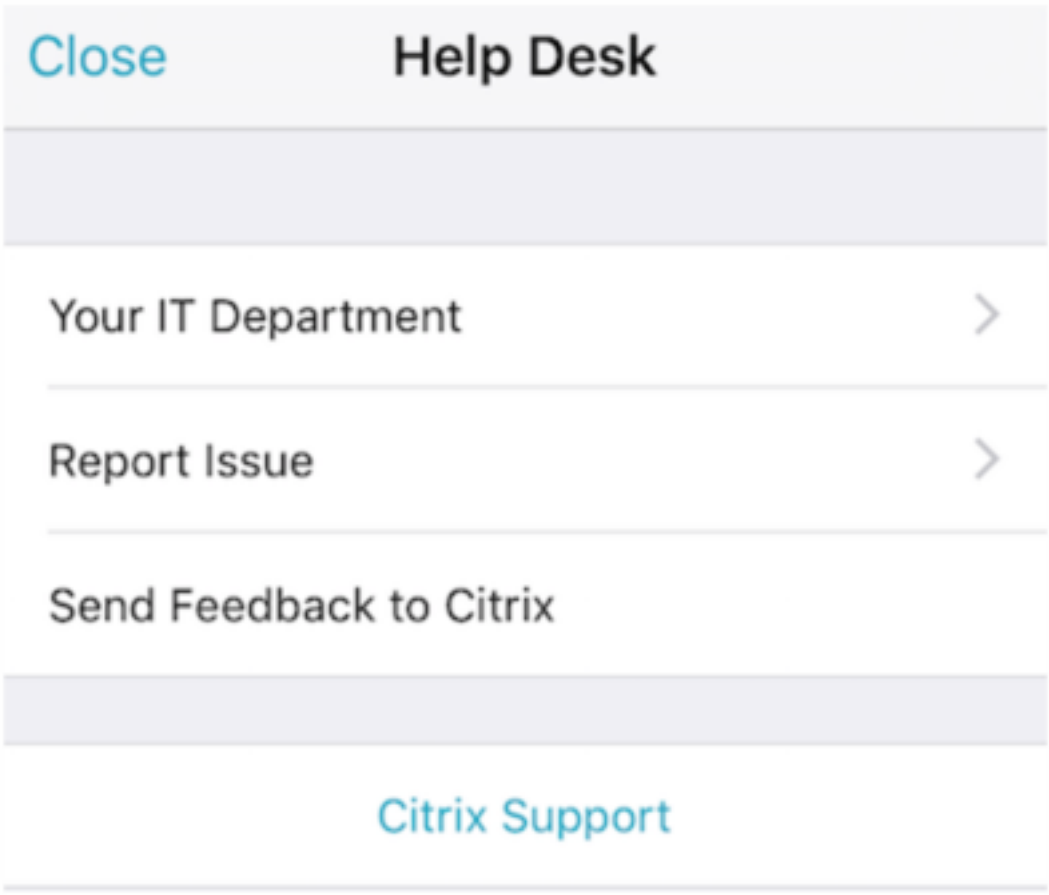
Endpoint Management 콘솔에서앱설명을편집할수있습니다. 구성을클릭한후 앱을클릭합니다. 테이블에서앱을선택하고 편집을클릭합니다. 설명을편집할앱의플랫폼을선택하고 설명상자에텍스트를입력합니다.



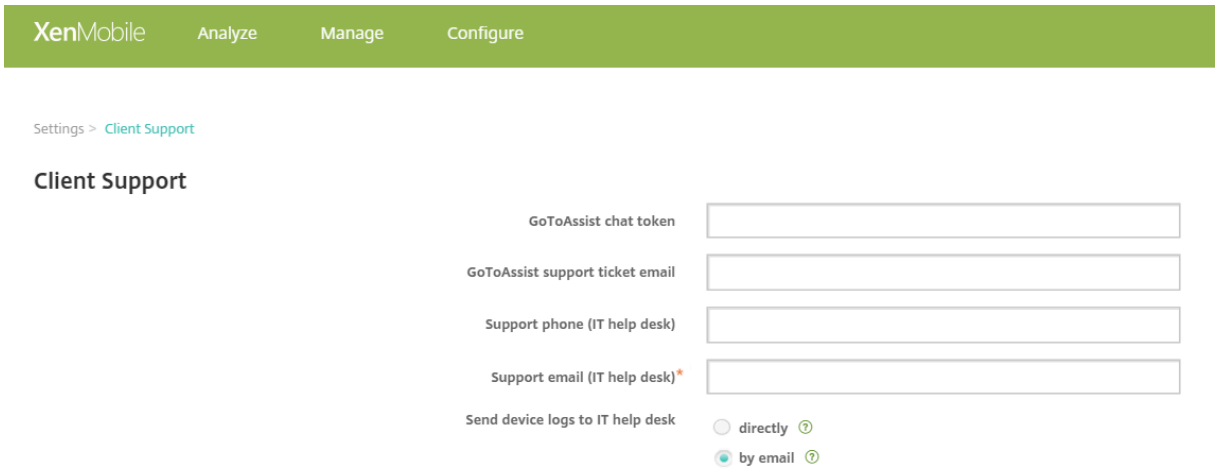
스토어에서사용자는 Endpoint Management 에서구성되고보안된앱및데스크톱만찾아볼수있습니다. 앱을추가하려면사용자가 세부정보를누른후 추가를누릅니다.

구성된도움말옵션

또한 Secure Hub 는도움을받을수있는다양한방법을사용자에게제공합니다. 태블릿에서오른쪽위모서리에있는물음표를누르면 도움말옵션이열립니다. 전화기에서는사용자가왼쪽위모서리의햄버거메뉴아이콘을누른후 도움말을누릅니다.



IT 부서에는사용자가앱에서바로액세스할수있는회사지원센터의전화및전자메일이표시됩니다. 전화번호및전자메일주소를 Endpoint Management 콘솔에입력하십시오. 오른쪽위모서리에서기어아이콘을클릭합니다. 설정페이지가나타납니다. 더보기를클릭하고 클라이언트지원을클릭합니다. 정보를입력하는화면이나타납니다.



문제보고에앱목록이표시됩니다. 사용자가문제있는앱을선택합니다. Secure Hub 는로그를자동으로생성한후로그가 zip 파일로첨부된메시지를 Secure Mail 에서엽니다. 사용자가제목줄및문제에대한설명을추가합니다. 스크린샷도첨부할수있습니다.

Citrix 에피드백보내기는 Citrix 지원팀주소가채워진메시지를 Secure Mail 에서엽니다. 메시지본문에서사용자는 Secure Mail 개선을위한제안을입력할수있습니다. Secure Mail 이장치에설치되지않은경우기본메일프로그램이열립니다.

사용자는 **Citrix** 지원을눌러 Citrix Knowledge Center를열수도있습니다. 여기에서모든 Citrix 제품에대한지원문서를검색할수있습니다.

기본설정에서는사용자가자신의계정및장치에대한정보를찾을수있습니다.

위치정책

또한 Secure Hub 는회사소유장치가특정지리적경계선을벗어나지못하게하려는경우등에지역위치및지역추적정책을제공합니다. 자세한내용은 위치장치정책을참조하십시오.

충돌수집및분석

Secure Hub 는실패정보를자동으로수집및분석하므로특정실패의원인이무엇인지파악할수있습니다. Crashlytics 소프트웨어는이기능을지원합니다.

iOS 및 Android 에서사용할수있는추가기능은 Citrix Secure Hub의플랫폼별기능매트릭스를참조하십시오.

Secure Mail 개요

March 14, 2022

Citrix Secure Mail 을통해사용자는휴대폰및태블릿에서전자메일, 일정및연락처를관리할수있습니다. Microsoft Outlook 또는 IBM Notes 계정으로부터연속성이유지되도록 Secure Mail 은 Microsoft Exchange Server 및 IBM Notes Traveler 서버와동기화됩니다.

Citrix 앱제품군의하나인 Secure Mail 은 Citrix Secure Hub 와의 SSO(Single Sign-On) 호환성을갖습니다. 사용자는 Secure Hub 에로그온한후사용자이름및암호를다시입력할필요없이 Secure Mail 로매끄럽게이동할수있습니다. 사용자의장치가 Secure Hub 에등록될때해당장치로 Secure Mail 이자동으로푸시되도록구성하거나사용자가 Store 에서이앱을추가할수있습니다.

> 참고:
>
> Exchange Server 2010 에대한지원은 2020 년 10 월 13 일에종료되었습니다.

Secure Mail 은다음과호환됩니다.

- Exchange Server 2019 누적업데이트 11
- Exchange Server 2019 누적업데이트 10
- Exchange Server 2019 누적업데이트 9
- Exchange Server 2019 누적업데이트 8
- Exchange Server 2019 누적업데이트 7
- Exchange Server 2019 누적업데이트 6
- Exchange Server 2016 누적업데이트 22
- Exchange Server 2016 누적업데이트 21
- Exchange Server 2016 누적업데이트 20
- Exchange Server 2016 누적업데이트 19
- Exchange Server 2016 누적업데이트 18
- Exchange Server 2016 누적업데이트 17
- Exchange Server 2013 누적업데이트 23
- Exchange Server 2013 누적업데이트 22
- Exchange Server 2013 누적업데이트 21
- 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 및기타 Endpoint Management 구성요소를 Citrix Endpoint Management 다운로드에서다운로드합니다.

Secure Mail 및기타모바일앱시스템요구사항은 시스템요구사항을참조하십시오.

앱이백그라운드에서실행되고있거나닫힌경우 iOS 및 Android 용 Secure Mail 의알림에대한내용은 Secure Mail 을위한푸시알림을참조하십시오.

Secure Mail 에서지원되는 iOS 기능은 Secure Mail 의 iOS 기능을참조하십시오.

Secure Mail 에서지원되는 Android 기능은 Secure Mail 의 Android 기능을참조하십시오.

Secure Mail 에서지원되는 iOS 및 Android 기능은 Secure Mail 의 iOS 및 Android 기능을참조하십시오.

사용자도움말설명서는 Citrix User Help Center 의 Citrix Secure Mail 페이지를참조하십시오.

Citrix Secure Web

December 10, 2021

Citrix Secure Web 은내부및외부사이트에대한보안액세스를제공하는 HTML5 호환모바일웹브라우저입니다. 사용자의장치가 Secure Hub 에등록될때해당장치로 Secure Web 이자동으로푸시되도록구성할수있습니다. 또는 Endpoint Management 앱스토어에서앱을추가할수있습니다.

Secure Web 및기타모바일생산성앱시스템요구사항은 시스템요구사항을참조하십시오.

Secure Web 통합및제공

> 참고:
>
> MDX Toolkit 10.7.10 은모바일생산성앱의래핑을지원하는마지막릴리스입니다. 사용자는공용앱스토어에서모바일생산성앱버전 10.7.5 이상에액세스할수있습니다.

Secure Web 을통합하여제공하려면다음일반단계를따르십시오.

1. 내부네트워크에대한 SSO(Single Sign-on) 를사용하도록 Citrix Gateway 를구성합니다.

   HTTP 트래픽의경우, Citrix ADC 는 Citrix ADC 에의해지원되는모든프록시인증유형에대해 SSO 를제공할수있습니다. HTTPS 트래픽의경우, 웹암호캐싱정책으로 Secure Web 이인증할수있고 MDX 를통해프록시서버에 SSO 를제공할수있습니다. MDX 는기본, 다이제스트및 NTLM 프록시인증만지원합니다. 암호는 MDX 를사용하여캐싱되고민감한앱데이터의보안스토리지영역인 Endpoint Management 공유저장소에저장됩니다. Citrix Gateway 구성에대한자세한내용은 Citrix Gateway를참조하십시오.

2. Secure Web 을다운로드합니다.
3. 내부네트워크에대한사용자연결을어떻게구성할지결정합니다.
4. 다른 MDX 앱과동일한절차에따라 Secure Web 을 Endpoint Management 에추가한다음 MDX 정책을구성합니다. Secure Web 관련정책에대한자세한내용은이문서뒷부분에있는 “Secure Web 정책정보” 를참조하십시오.

사용자연결구성

Secure Web 은다음과같은사용자연결구성을지원합니다.

- **Secure browse:** 내부네트워크에터널링되는연결은 Secure Browse 라고하는클라이언트없는 VPN 의변형을사용할수있습니다. 이는 기본설정 **VPN** 모드정책에대해지정된기본구성입니다. Secure Browse 는 SSO(Single Sign-On) 가필요한연결에권장됩니다.

- 전체 **VPN** 터널**:** 내부네트워크로터널링되는연결은 기본설정 **VPN** 모드정책에의해구성된전체 VPN 터널을사용할수있습니다. 클라이언트인증서또는종단간 SSL 을사용하여내부네트워크의리소스로연결되는경우전체 VPN 터널을사용하는것이좋습니다. 그러나 Secure Web 은모바일장치에저장된클라이언트인증서를읽을수있는앱이아닙니다. 이기능을제공할수있는래핑된타사엔터프라이즈앱을설치할수있습니다. 전체 VPN 터널은 TCP 기반의모든프로토콜을처리하고, Windows 및 Mac 컴퓨터뿐아니라 iOS 및 Android 장치에서도사용될수있습니다.
- **VPN** 모드전환허용정책은필요에따라전체 VPN 터널모드와 Secure Browse 모드간의자동전환을허용합니다. 기본적으로이정책은꺼져있습니다. 이정책이켜진경우, 기본설정 VPN 모드에서처리할수없는인증요청으로인해실패한네트워크요청은다른모드에서다시시도됩니다. 예를들어전체 VPN 터널모드에서는클라이언트인증서에대한서버챌린지를수용할수있지만 Secure Browse 모드에서는수용할수없습니다. 마찬가지로 HTTP 인증챌린지는 Secure Browse 모드를사용할경우에 SSO 로더쉽게서비스될수있습니다.
- **PAC** 포함전체 **VPN** 터널**:** iOS 및 Android 장치에전체 VPN 터널배포와함께 PAC(Proxy Automatic Configuration) 파일을사용할수있습니다. PAC 파일에는웹브라우저에서해당 URL 에액세스하기위해프록시를선택하는방식을정의하는규칙이포함됩니다. PAC 파일규칙은내부및외부사이트에대한처리방식을지정할수있습니다. Secure Web 은 PAC 파일규칙을구문분석하고프록시서버정보를 Citrix Gateway 로보냅니다.
- PAC 파일을사용할경우의전체 VPN 터널링성능은 Secure Browse 모드와비슷합니다. PAC 구성에대한자세한내용은 PAC 포함전체 VPN 터널링을참조하십시오.

다음표에서는구성및사이트유형별로 Secure Web 이사용자에게자격증명을요구하는지여부를설명합니다.

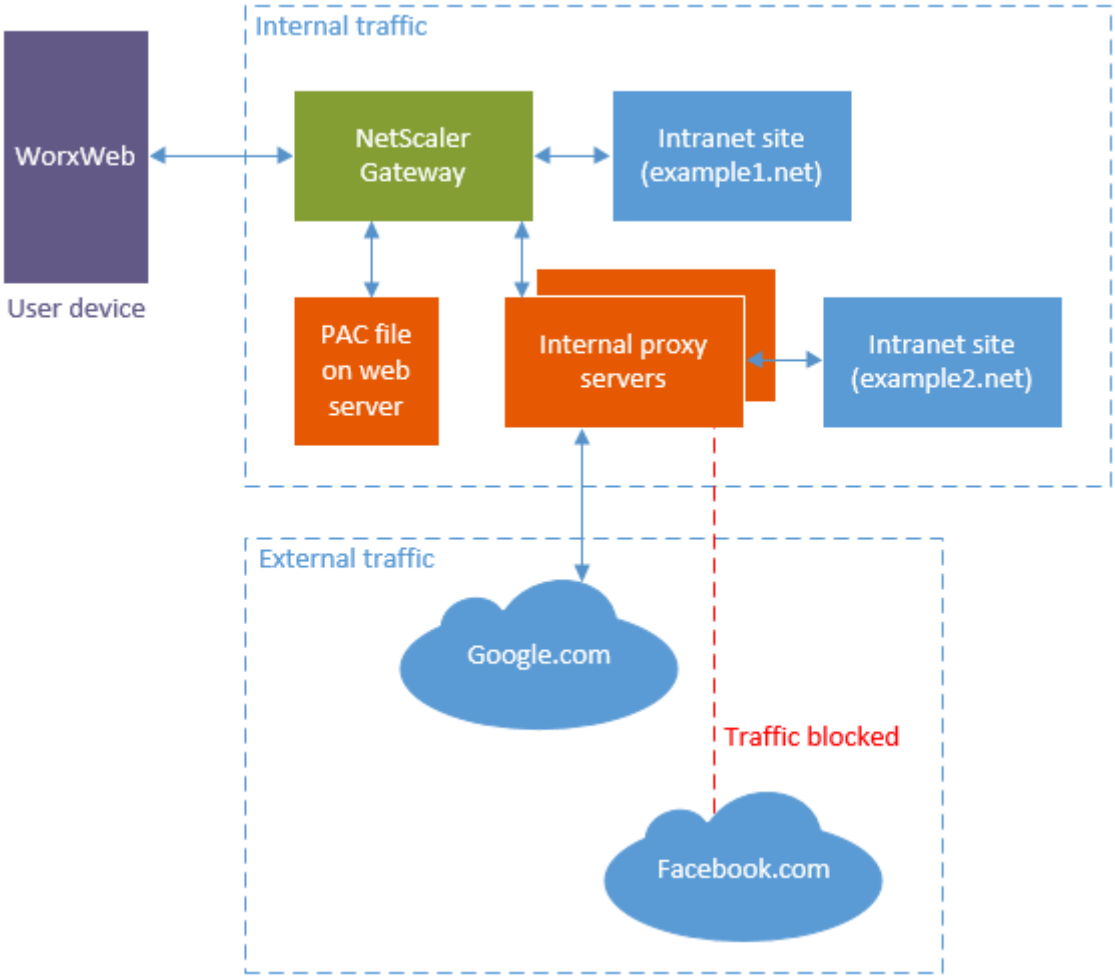
연결모드	사이트유형	암호캐싱	Citrix Gateway 에 대해구성된 SSO	처음웹사이트에액세스할경우 Secure Web 이자격증명묻기	이후에웹사이트에액세스할경우 Secure Web 이자격증명묻기	암호변경후 Secure Web 이자격증명묻기
Secure Browse	HTTP	아니요	예	아니요	아니요	아니요
Secure Browse	HTTPS	아니요	예	아니요	아니요	아니요
전체 VPN	HTTP	아니요	예	아니요	아니요	아니요
전체 VPN	HTTPS	예: Secure Web MDX 정책인웹암호캐싱사용설정이켜짐인경우	아니요	예: 자격증명을 Secure Web 에캐싱하는데필요함	아니요	예

PAC 포함전체 **VPN** 터널링

> 중요:
>
> Secure Web 이 PAC 파일과함께구성되어있고 Citrix ADC 가프록시작동을위해구성된경우 Secure Web 이시간초과됩니다. 전체 VPN 터널링및 PAC 를사용하기전에프록시에대해구성된 Citrix Gateway 트래픽정책을제거해야합니다.

전체 VPN 터널링및 PAC 파일또는프록시서버에대해 Secure Web 을구성하면 Secure Web 이 Citrix Gateway 를통해프록시로모든트래픽을보냅니다. 그러면 Citrix Gateway 가프록시구성규칙에따라트래픽을라우팅합니다. 이구성에서 Citrix Gateway 는 PAC 파일또는프록시서버를인지하지못합니다. 트래픽흐름은 PAC 없는전체 VPN 터널링의경우와동일합니다.

다음다이어그램은 Secure Web 사용자가웹사이트를탐색할경우의트래픽흐름을보여줍니다.



이예에서트래픽규칙은다음을지정합니다.

- Citrix Gateway 가인트라넷사이트 `example1.net`에직접연결됩니다.
- 인트라넷사이트 `example2.net`(으) 로의트래픽이내부프록시서버를통해프록싱됩니다.
- 외부트래픽은내부프록시서버를통해프록싱됩니다. 프록시규칙이다음으로의외부트래픽을차단합니다. `Facebook.com`.

PAC 포함전체 VPN 터널링을구성하려면

1. PAC 파일의유효성을검사하고파일을테스트합니다.

   > 참고:
   >
   > PAC 파일생성및사용에대한자세한내용은 https://findproxyforurl.com/을참조하십시오.

   Pacparser 등의 PAC 유효성검사도구를사용하여 PAC 파일의유효성을검사합니다. PAC 파일을읽을때 Pacparser 결과가예상한대로인지확인합니다. PAC 파일에구문오류가있으면모바일장치가 PAC 파일을무시합니다. PAC 파일은모바일장치의메모리에만저장됩니다.

   PAC 파일은하향식으로처리되고, 규칙이현재쿼리와일치하면처리가중지됩니다.

   Endpoint Management 의 PAC/프록시필드에입력하기전에 PAC 파일 URL 을웹브라우저로테스트합니다. PAC 파일이위치하는네트워크에컴퓨터가액세스할수있는지확인합니다.

   ```
   https://webserver.local/GenericPAC.pac
   ```
   ```
   https://webserver.local/GenericPAC.pac
   ```

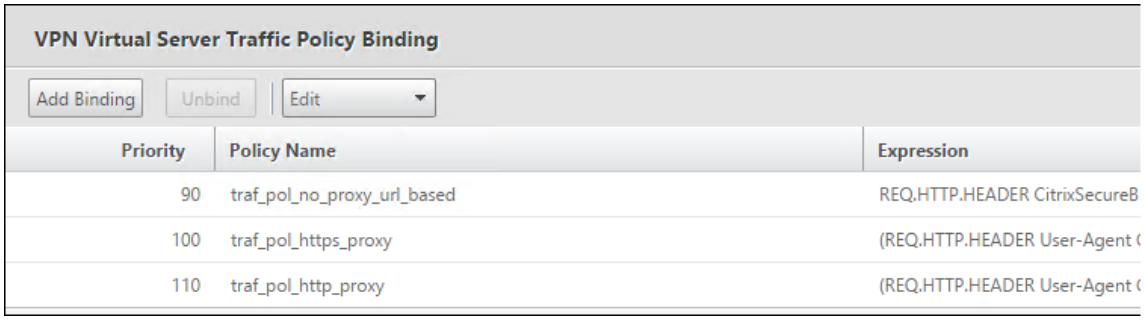
   테스트한 PAC 확장명은.txt 또는.pac 입니다.

   PAC 파일의콘텐츠는웹브라우저내부에표시됩니다.

   > 중요:
   >
   > Secure Web 과함께사용되는 PAC 파일을업데이트할때마다사용자에게 Secure Web 을닫고다시열어야한다는것을알려줍니다.

2. Citrix Gateway 구성:

   - Citrix Gateway 분할터널링이사용되지않도록설정합니다. 분할터널링이켜져있고 PAC 파일이구성된경우 PAC 파일규칙이 Citrix ADC 분할터널링규칙보다우선합니다. 프록시는 Citrix ADC 분할터널링규칙을무시하지않습니다.
   - 프록시에대해구성된 Citrix Gateway 트래픽정책을제거합니다. 이는 Secure Web 이올바로작동하는데필요합니다. 다음그림은제거할정책규칙의예를보여줍니다.



3. Secure Web 정책구성:

   - 기본설정 VPN 모드정책을 전체 **VPN** 터널로설정합니다.
   - VPN 모드전환허용정책을 꺼짐으로설정합니다.

- PAC 파일 URL 또는프록시서버정책을구성합니다. Secure Web 은기본포트및기본이아닌포트외에도 HTTP 및 HTTPS 를지원합니다. HTTPS 의경우, 인증서가자체서명되었거나신뢰할수없으면루트인증기관이장치에설치되어있어야합니다.

  정책을구성하기전에웹브라우저에서 URL 또는프록시서버주소를테스트하십시오.

  PAC 파일 URL 예:

  ```
  http[s]://example.com/proxy.pac
  http[s]://10.10.0.100/proxy.txt
  ```

  프록시서버예 (포트는필수임):

  ```
  myhost.example.com:port
  ```

  ```
  10.10.0.100:port
  ```

  > 참고:
  >
  > PAC 파일또는프록시서버를구성하는경우 Wi-Fi 에대한시스템프록시설정에서 PAC 를구성하지마십시오.

- 웹암호캐싱사용정책을 켜짐으로설정합니다. 웹암호캐싱은 HTTPS 사이트에대한 SSO 를처리합니다.

  프록시가동일한인증인프라를지원하는경우 Citrix ADC 는내부프록시에대해 SSO 를수행할수있습니다.

PAC 파일지원제한사항

Secure Web 은다음을지원하지않습니다.

- 한프록시서버에서다른프록시서버로의장애조치 (failover). PAC 파일평가에서단일호스트이름에대해여러개의프록시서버가반환될수있습니다. Secure Web 은반환된첫번째프록시서버만사용합니다.
- PAC 파일에서의 FTP 및 gopher 같은프로토콜
- PAC 파일에서의 SOCKS 프록시서버
- WPAD(Web Proxy AutoDiscovery Protocol)

Secure Web 은 PAC 파일함수경고를무시하므로이러한호출을포함하지않는 PAC 파일을구문분석할수있습니다.

Secure Web 정책

Secure Web 을추가할경우, Secure Web 과관련된다음 MDX 정책에유의하십시오. 지원되는모든모바일장치에해당:

허용또는차단된웹사이트

일반적으로 Secure Web 은웹링크를필터링하지않습니다. 이정책을사용하면허용또는차단된사이트의구체적인목록을구성할수있습니다. 쉼표로구분된목록형식의 URL 패턴을구성하여브라우저에서열수있는웹사이트를제한할수있습니다. 목록의각패턴앞에는더하기기호 (+) 또는빼기기호 (-) 가올수있습니다. 브라우저가일치항목이발견될때까지나열된순서대로 URL 을패턴과비교합니다. 일치항목이발견되면다음과같이접두사에따라작업이결정됩니다.

- 빼기 (-) 접두사가있으면브라우저에서 URL 을차단합니다. 이경우 URL 은웹서버주소를확인할수없는것처럼처리됩니다.
- 더하기 (+) 접두사가있으면 URL 이정상적으로처리됩니다.
- 패턴에 + 또는 - 접두사가없는경우에는 +(허용) 로간주됩니다.
- URL 과일치하는패턴이목록에없는경우 URL 이허용됩니다.

다른모든 URL 을차단하려면목록의끝에빼기기호와별표 (-*) 를추가합니다. 예:

- 정책값 +http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*는 mycorp.com 도메인내의 HTTP URL 을허용하고그외다른위치의 URL 은차단하며, 모든위치의 HTTPS 및 FTP URL 은허용하고다른모든 URL 은차단합니다.
- 정책값 +http://*.training.lab/*,+https://*.training.lab/*,-*는 사용자가 Training.lab 도메인 (인트라넷) 의모든사이트를 HTTP 또는 HTTPS 를통해여는것을허용합니다. 그러나프로토콜에관계없이 Facebook, Google 및 Hotmail 과같은공용 URL 을열수없습니다.

기본값은비어있습니다 (모든 URL 이허용됨).

팝업차단

팝업은사용자의허가없이웹사이트가열수있는새탭입니다. 이정책은 Secure Web 에서팝업을허용할지여부를결정합니다. 켜짐인경우, Secure Web 은웹사이트가팝업을열지못하게합니다. 기본값은꺼짐입니다.

미리로드된책갈피

Secure Web 브라우저에대해미리로드되는책갈피집합을정의합니다. 이정책은폴더이름, 식별이름및웹주소를포함하는튜플이쉼표로구분되어있는목록입니다. 각목록은폴더, 이름, URL 형식이어야하며이름은선택적으로큰따옴표 (“) 로묶일수있습니다.

예를들어, 정책값 ,”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.aspx는 3 개의책갈피를정의합니다. 첫번째는 “Mycorp, Inc. home page” 라는이름의기본링크 (폴더이름없음) 입니다. 두번째링크는 “MyCorp Links” 라는이름의폴더에배치되고 “Account logon” 이라는레이블이지정됩니다. 세번째는 “MyCorp Links” 폴더의 “Investor Relations” 하위폴더에배치되고 “Contact us” 로표시됩니다.

기본값은비어있습니다.

홈페이지 **URL**

Secure Web 을시작할때로드할웹사이트를정의합니다. 기본값은비어있습니다 (기본시작페이지).

지원되는 Android 및 iOS 장치에만해당:

브라우저사용자인터페이스

Secure Web 에대해브라우저사용자인터페이스컨트롤의동작및가시성을지정합니다. 일반적으로모든탐색컨트롤을사용할수있습니다. 앞으로, 뒤로, 주소표시줄및새로고침/중지컨트롤이여기에포함됩니다. 이러한컨트롤중일부의용도및가시성을제한하기위해이정책을구성할수있습니다. 기본값은모든컨트롤을표시하는것입니다.

옵션

- 모든컨트롤표시. 모든컨트롤을볼수있고사용자는제한없이이러한컨트롤을사용할수있습니다.
- 읽기전용주소표시줄. 모든컨트롤을볼수있지만사용자가브라우저주소필드를편집할수는없습니다.
- 주소표시줄숨기기. 주소표시줄을숨기지만다른컨트롤은숨기지않습니다.
- 모든컨트롤숨기기. 전체도구모음이표시되지않도록하여프레임없는탐색환경을제공합니다.

웹암호캐싱사용

웹리소스를액세스하거나요청할때 Secure Web 사용자가자격증명을입력하는경우, Secure Web 이자동으로암호를장치에캐싱하는지여부를이정책이결정합니다. 이정책은웹양식에입력한암호가아니라인증대화상자에입력한암호에적용됩니다.

켜짐인경우, Secure Web 은웹리소스요청시에사용자가입력하는모든암호를캐싱합니다. 꺼짐인경우, Secure Web 은암호를캐싱하지않고기존의캐싱된암호를제거합니다. 기본값은 꺼짐입니다.

이앱에대해기본 VPN 정책을전체 VPN 터널로설정한경우에만이정책을사용하도록설정됩니다.

프록시서버

Secure Browse 모드에서사용될때 Secure Web 에대해프록시서버를구성할수도있습니다. 자세한내용은이 블로그게시물을참조하십시오.

DNS suffixes(DNS 접미사)

DNS 접미사가구성되지않은경우 Android 에서 VPN 이실패할수도있습니다. DNS 접미사구성에대한자세한내용은 Supporting DNS Queries by Using DNS Suffixes for Android Devices(Android 장치에대해 DNS 접미사를사용한 DNS 쿼리지원)를참조하십시오.

Secure Web 을위한인트라넷사이트준비

이섹션은 Android 및 iOS 용 Secure Web 과함께사용할인트라넷사이트를준비해야하는웹사이트개발자를대상으로합니다. 데스크톱브라우저에맞춰설계된인트라넷사이트가 Android 및 iOS 장치에서올바로작동하려면사이트를변경해야합니다.

Secure Web 은 Android WebView 및 iOS WkWebView 를통해웹기술지원을제공합니다. Secure Web 에서지원하는일부웹기술은다음과같습니다.

- AngularJS

- ASP .NET
- JavaScript
- jQuery
- WebGL

Secure Web 에서지원하지않는일부웹기술은다음과같습니다.

- Flash
- Java

다음표에서는 Secure Web 에대해지원되는 HTML 렌더링기능및기술을보여줍니다. X 는플랫폼, 브라우저및구성요소조합에기능을사용할수있음을나타냅니다.

기술	iOS Secure Web	Android 6.x/7.x Secure Web
JavaScript 엔진	JavaScriptCore	V8
로컬스토리지	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

기술은여러장치에걸쳐동일하게작동하고, Secure Web 은장치에따라서로다른사용자에이전트문자열을반환합니다. Secure Web 에사용되는브라우저버전을확인하려면사용자에이전트문자열을보면됩니다. Secure Web 에서 https://whatsmyuseragent.com/으로이동합니다.

인트라넷사이트문제해결

인트라넷사이트를 Secure Web 에서볼때의렌더링문제를해결하려면 Secure Web 및호환되는타사브라우저에서웹사이트가어떻게렌더링되는지비교합니다.

iOS 의경우테스트와호환되는타사브라우저는 Chrome 및 Dolphin 입니다.

Android 의경우테스트와호환되는타사브라우저는 Dolphin 입니다.

> 참고:
>
> Chrome 은 Android 에서기본브라우저입니다. 이브라우저를비교작업에사용하지마십시오.

iOS 의경우브라우저에장치수준 VPN 지원기능이있는지확인하십시오. 설정 **> VPN > VPN** 구성추가로이동하여장치에 VPN 을구성할수있습니다.

또한 App Store 에서다운로드할수있는 Citrix VPN,Cisco AnyConnect 또는 Pulse Secure 등의 VPN 클라이언트앱을 사용할수있습니다.

- 웹페이지가두브라우저에서동일하게렌더링되면웹사이트에문제가있는것입니다. 사이트를업데이트하고 OS 에대해사이트가잘작동하는지확인합니다.
- Secure Web 에서만웹페이지에문제가나타나면 Citrix 지원팀에문의하여지원티켓을엽니다. 테스트한브라우저및 OS 유형을포함하여문제해결절차를제공하십시오. iOS 용 Secure Web 에렌더링문제가있는경우, 다음절차에설명된대로 페이지의웹보관을포함하십시오. 그러면 Citrix 에서문제를더신속히해결하는데도움이됩니다.

웹보관파일을생성하려면

macOS 10.9 이상에서 Safari 를사용하면웹보관파일 (읽기목록이라고함) 로웹페이지를저장할수있습니다. 웹보관파일에는이미지, CSS 및 JavaScript 와같은모든연결된파일이포함됩니다.

1. Safari 에서읽기목록폴더를비우고 **Finder** 에서 메뉴표시줄에있는 이동메뉴를클릭하고 폴더로이동을선택한후, 경로이름 ~/Library/Safari/ReadingListArchives/를입력하고해당위치에있는모든폴더를삭제합니다.
2. 메뉴표시줄에서 **Safari >** 환경설정 **>** 고급으로이동하고메뉴표시줄에서 개발자용메뉴보기를사용하도록설정합니다.
3. 메뉴표시줄에서 개발 **>** 사용자에이전트로이동하고 Secure Web 사용자에이전트를입력합니다 (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 에서읽기목록 (웹보관파일) 으로저장할웹사이트를엽니다.
5. 메뉴표시줄에서 책갈피 **>** 읽기목록에추가로이동합니다. 보관은백그라운드에서이루어지며몇분이걸릴수있습니다.
6. 보관된읽기목록을찾습니다. 메뉴표시줄에서 보기 **>** 읽기목록사이드바보기로이동합니다.
7. 보관파일을확인합니다.
    - Mac 으로의네트워크연결을끕니다.
    - 읽기목록에서웹사이트를엽니다.

      웹사이트가완전히렌더링됩니다.
8. 보관파일을압축합니다. **Finder** 에서 메뉴표시줄에있는 이동메뉴를클릭하고 폴더로이동을선택한후, 경로이름 ~/Library/Safari/ReadingListArchives/를입력합니다. 이제임의의 16 진수문자열이파일이름인폴더를압축합니다. 지원티켓을열때 Citrix 지원팀으로이파일을보낼수있습니다.

Secure Web 기능

Secure Web 은모바일데이터교환기술을활용해전용 VPN 터널을생성하여사용자가내부와외부웹사이트및다른모든웹사이트를액세스할수있게합니다. 조직의정책으로보안되는환경에서민감한정보가포함된사이트도여기에포함됩니다.

Secure Web 을 Secure Mail 및 Citrix Files 와통합하면보안 Endpoint Management 컨테이너내에서원활한사용자환경이제공됩니다. 통합기능의일부예는다음과같습니다.

- 사용자가 **Mailto** 링크를누르면추가적인인증을요구하지않고새전자메일메시지가 Citrix Secure Mail 에서열립니다.
- iOS 에서는 **ctxmobilebrowser://**를 URL 의앞에삽입하여기본메일앱으로부터 Secure Web 에링크를열수있습니다. 예를들어기본메일앱에서 `example.com`을열려면 URL ctxmobilebrowser://example.com 을사용합니다.
- 사용자가전자메일메시지에서인트라넷링크를클릭하면 Secure Web 이추가적인인증없이해당사이트로이동합니다.
- 사용자는 Secure Web 에서웹으로부터다운로드한파일을 Citrix Files 에업로드할수있습니다.

Secure Web 사용자는다음작업을수행할수도있습니다.

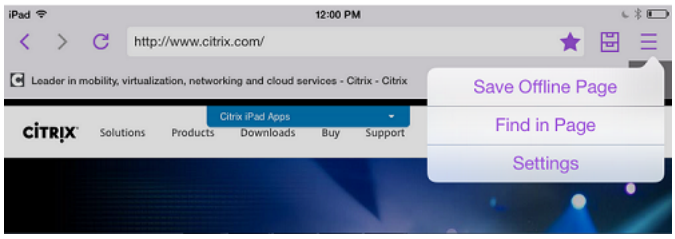
- 팝업차단.

  > 참고**:**
  >
  > Secure Web 메모리의많은부분이팝업렌더링에사용되므로설정에서팝업을차단할경우보통성능이향상됩니다.

- 즐겨찾기사이트를책갈피로지정합니다.
- 파일을다운로드합니다.
- 페이지를오프라인으로저장합니다.
- 암호를자동저장합니다.
- 캐시/기록/쿠키를지웁니다.
- 쿠키및 HTML5 로컬스토리지를사용하지않도록설정합니다.
- 다른사용자와안전하게장치를공유합니다.
- 주소표시줄내에서검색합니다.
- Secure Web 과함께실행되는웹앱이위치에액세스할수있도록허용합니다.
- 설정을내보내고가져옵니다.
- 파일을다운로드할필요없이 Citrix Files 에서파일을직접엽니다. 이기능을사용하도록설정하려면 Endpoint Management 에서 **ctx-sf**: 를허용된 URL 정책에추가합니다.
- iOS 에서 3D 터치동작을사용하여새탭을열고홈화면에서바로오프라인페이지, 즐겨찾기사이트및다운로드에액세스합니다.
- iOS 에서모든크기의파일을다운로드하고 Citrix Files 또는다른앱에서파일을엽니다.

> 참고:
>
> Secure Web 을백그라운드로전환하면다운로드가중지됩니다.

- **Find in Page(**페이지에서찾기**)** 를사용하여현재페이지보기내에서용어를검색합니다.



Secure Web 에는동적텍스트지원도포함됩니다. 사용자가장치에서설정한글꼴이앱에표시됩니다.

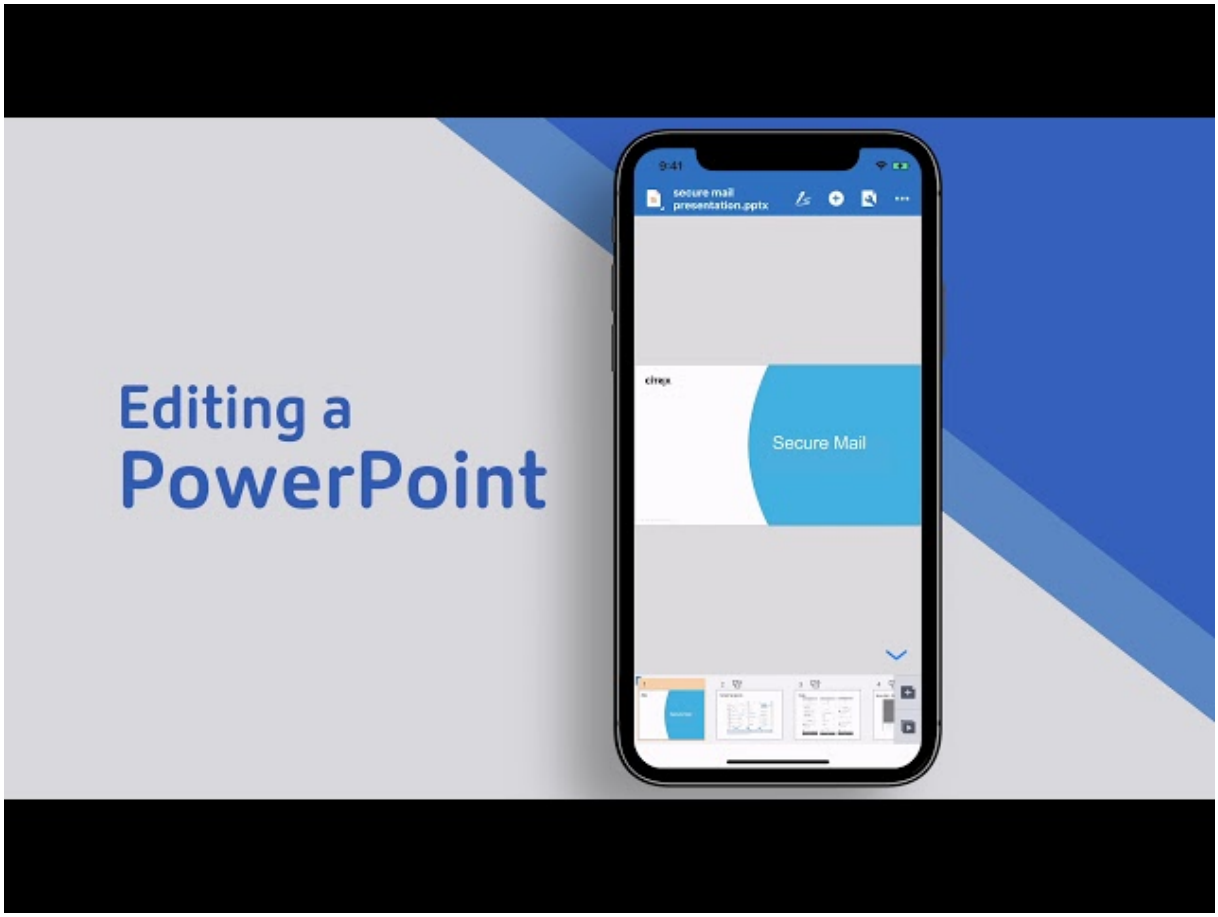
모바일생산성앱을위한 **Citrix QuickEdit**

December 10, 2021

Citrix QuickEdit 은모바일생산성앱을위한편집도구입니다. Citrix Secure Mail 및 Citrix Content Collaboration for Endpoint Management 와호환되므로보안 Endpoint Management 환경내에서워크플로를원활하게수행할수있습니다.

> 업데이트:
>
> - **2020** 년 **6** 월 **19** 일업데이트: MDX 암호화는 2020 년 9 월 1 일에 EOL(수명종료) 에도달합니다. 따라서 2020 년 7 월까지 MDX 암호화마이그레이션을테스트하고계획해야합니다.
> - **2018** 년 **7** 월 **2** 일업데이트: QuickEdit 는계속해서모바일생산성앱으로제공됩니다. 이전에알려드린 2018 년 9 월 1 일에 EOL(수명종료) 상태를적용하지않습니다. 대신, QuickEdit 의콘텐츠관리구성요소를업데이트할계획입니다.

Citrix QuickEdit 기능에대한비디오를보려면 Citrix YouTube 채널에있는이비디오를살펴보십시오.



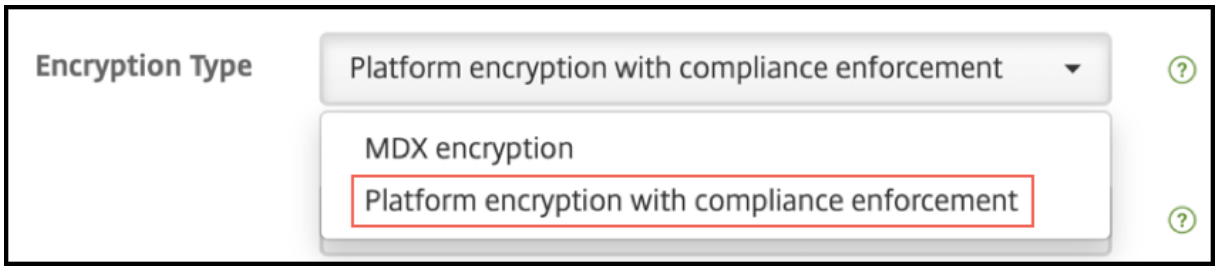
QuickEdit 및기타모바일생산성앱시스템요구사항은 시스템요구사항을참조하십시오.

사용자의장치가 Secure Hub 에등록될때해당장치로 QuickEdit 가자동으로푸시되도록구성할수있습니다. 또는사용자가앱스토어에서앱을추가할수도있습니다.

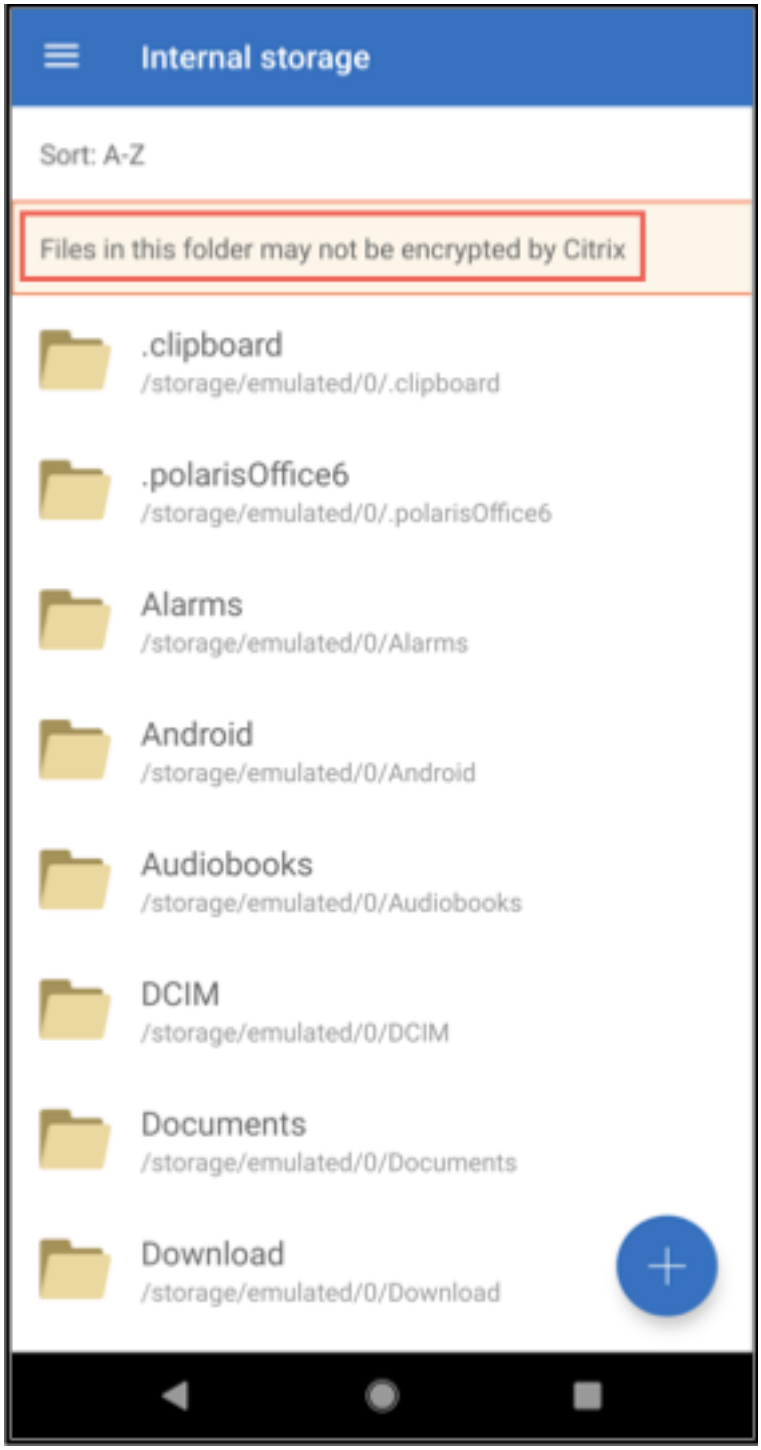
또한 QuickEdit 은첨부파일또는 Citrix Files 링크로서손쉽게파일을공유하거나전송하기위해기본메일프로그램과호환됩니다.

암호화

QuickEdit 버전 20.5.0 이상에서는데이터암호화유형을선택할수있습니다. 데이터를암호화하려면장치플랫폼에대해 규정준수를적용하여플랫폼암호화암호화유형을선택합니다.



규정준수를적용하여플랫폼암호화암호화유형을선택하면데이터가장치의 SD 카드에유지되지만 SD 카드에있는파일은암호화되지않습니다. 장치에다음과같은경고가표시됩니다.



클라우드리포지토리에저장된파일의경우데이터암호화유형만변경됩니다.

지원되는파일형식

- Microsoft Word – .doc 및.docx
- Microsoft Excel – .xls 및.xlsx

- Microsoft PowerPoint – .ppt 및.pptx
- .csv, .txt
- .jpeg, .png, .png, .svg, .bmp

.docm, .xlsm, .pptm 및.rft 파일형식은최신릴리스부터더이상사용되지않습니다.

QuickEdit 통합및제공

QuickEdit 을 Endpoint Management 와통합하여제공하려면다음일반단계를따르십시오.

1. 선택적으로 Secure Hub 에서 SSO 가사용되도록설정할수있습니다. 이를위해 Endpoint Management 에서 Citrix Files 계정정보를구성하여 Endpoint Management 를 Citrix Files 용 SAML ID 공급자로사용하도록설정합니다.

   Endpoint Management 에서 Citrix Files 계정정보를구성하는것은모든 Endpoint Management, Citrix Files 및비 MDX Citrix Files 클라이언트에사용되는일회용설정입니다. 자세한내용은 Citrix Files 클라이언트통합및제공을참조하십시오.

2. QuickEdit 을다운로드합니다.
   - QuickEdit 은 Endpoint Management 다운로드페이지에서다운로드할수있습니다.
   - 새로운사용자인경우 Citrix Workspace 플랫폼에서도 QuickEdit 을사용할수있습니다. 자세한내용은 Citrix Workspace platform(Citrix Workspace 플랫폼)을참조하십시오.
3. 다른 MDX 앱과동일한절차에따라 QuickEdit 을 Endpoint Management 에추가합니다. 자세한내용은 앱추가를참조하십시오.

파일업로드

장치에서 ShareFile 와같은클라우드리포지토리에파일을업로드하고다른장치에서액세스할수있습니다. 현재 QuickEdit 은 iOS 및 Android 에서만지원됩니다. 그러나파일을클라우드리포지토리에마이그레이션하면장치에서다른도구를사용하여동일하게편집할수있습니다.

현재릴리스에서수정된문제및알려진문제

최신릴리스에서알려진문제또는수정된문제는다음과같습니다.

수정된문제

- QuickEdit for iOS 또는 ScanDirect 에서 Secure Mail 로파일을보내려고하면전송이실패합니다. 이문제를해결하려면이러한앱에대한정책설정에서다음파일암호화제외를추가합니다. “/tmp/.com.apple.Pasteboard” (버전 6.14)

알려진문제

- 페이지크기가 10,000 포인트 (너비또는높이) 를초과할경우잠재적메모리오류를방지하기위해문서가열리지않습니다.
- 디지털서명및인라인이미지는 QuickEdit 에서지원되지않습니다.
- iOS 12 장치의경우 QuickEdit 에서파일을생성하면 “Due to insufficient memory(메모리부족으로인한)” 문제가발생합니다.
- 사용자는편집모드에서파일을연후주석옵션을선택한경우에만 PDF 파일에대한주석을볼수있습니다.
- 150MB 가넘는 PDF 파일을열면 “Unsupported file(지원되지않는파일)” 오류메시지가표시됩니다.
- iPad 의경우 QuickEdit 에서 편집모드사용시키보드가예상대로나타나지않습니다.
- 두개이상의사진이포함된 PowerPoint(.ppt) 파일을생성할수없습니다.

제한사항

- 공유장치에서 QuickEdit 가지원되지않습니다.
- 공유장치를지원하는이전버전의 QuickEdit 를실행중이고 iOS 용 QuickEdit 버전 7.4.0 이상으로업그레이드하면로컬에서관리되는모든파일및폴더가손실됩니다. 그러나 Citrix Files 데이터는영향을받지않으며계속액세스할수있습니다.

ShareConnect

December 10, 2021

> 중요:
>
> ShareConnect 는 2020 년 6 월 30 일에 EOL(수명종료) 에도달했습니다. 자세한내용은 EOL 및사용되지않는앱을참조하십시오.

ShareConnect 를사용할경우, 사용자는 iPad, Android 태블릿및 Android 휴대폰을통해컴퓨터에안전하게연결하여파일및응용프로그램에액세스할수있습니다. 사용자는다음을수행할수있습니다.

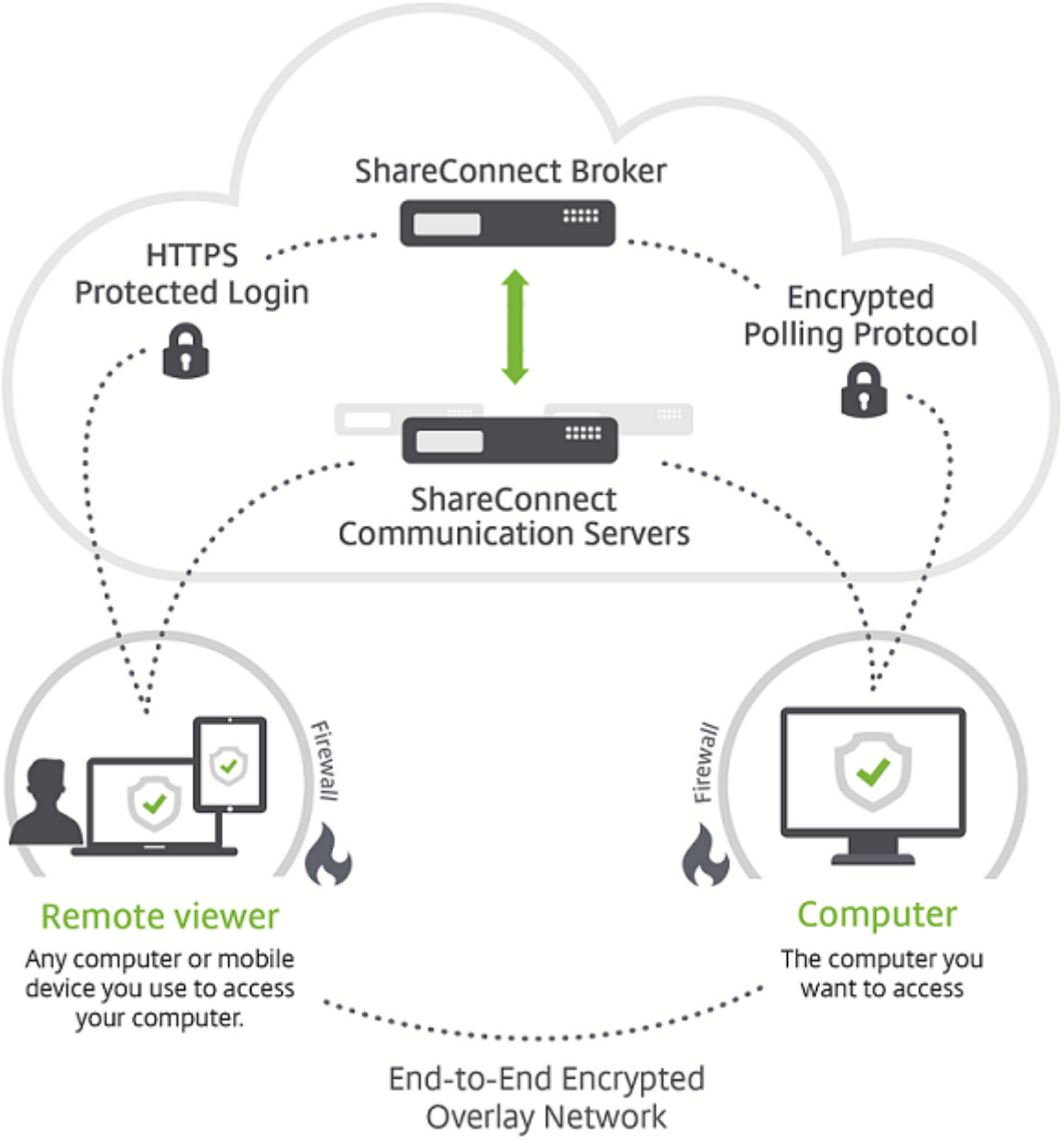
- 컴퓨터및연결된네트워크드라이브에있는파일을사용해작업합니다.
- ShareConnect 내에서대상시스템으로부터앱을실행합니다.
- 다른모바일생산성앱을래핑할필요없이모바일앱에액세스합니다.
- 모바일에최적화된액세스를위해 Citrix Virtual Desktops 에서 ShareConnect 를실행합니다.

ShareConnect 의 MDX 버전은 Endpoint Management 다운로드 페이지에서다운로드할수있습니다.

ShareConnect 설치및사용방법에대한일반적인정보는 Citrix Knowledge Center를참조하십시오.

아키텍처개요

ShareConnect 구성요소에는다음그림과같이 Citrix 자체의 ShareConnect Broker 및 ShareConnect Communication Server 가포함됩니다. ShareConnect Broker 는사용자를컴퓨터에매핑하는응용프로그램서버및데이터베이스로, 매핑후에호스트컴퓨터가온라인상태인지아니면오프라인상태인지사용자에게알려줍니다. ShareConnect Communication Server 는호스트와클라이언트컴퓨터간에데이터를교환하는데사용됩니다. 이데이터는 **Endpoint Management** 설정에기반하여보안 Micro VPN 터널을통해호스트와클라이언트컴퓨터간에흐를수있습니다.



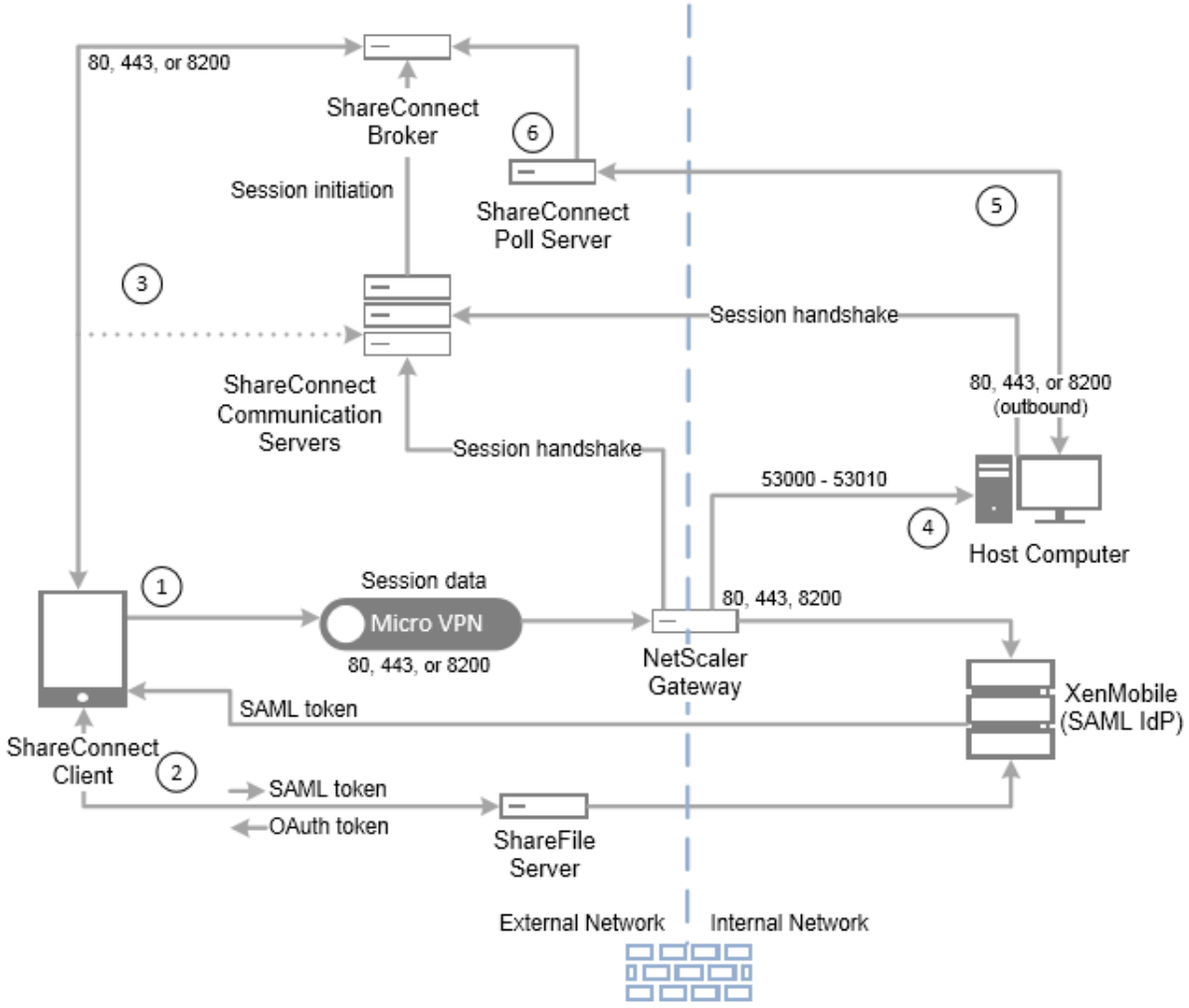
또한 Citrix Files 는 Endpoint Management 또는 ADFS(Active Directory Federation Services) 등의 SAML IdP(ID 공급자) 를사용한 SSO(Single Sign On) 를통해사용자인증을제공할수있습니다. Endpoint Management 를사용한배포에서네트워크외부의리소스에대한액세스는 Citrix Gateway 를통해제공됩니다.

ShareConnect 에서의연결작동방식

ShareConnect 는직접또는간접연결을설정합니다.

- 직접연결**.** 동일한 LAN 또는 Wi-Fi 네트워크에컴퓨터가있는경우 ShareConnect 는클라이언트컴퓨터와호스트컴퓨터간에직접연결을설정합니다. 이시나리오에서데이터는클라이언트컴퓨터간에또는호스트컴퓨터에액세스하기위해사용되는모바일장치간에직접흐를수있습니다. 데이터가 ShareConnect Communication Server 를통해흐르지않기때문에성능은최적화됩니다. 직접연결의경우, Endpoint Management 는 Citrix Gateway 를사용하여로컬네트워크외부의리소스에대한보안액세스를제공합니다.
- 간접연결**.** ShareConnect 는컴퓨터에직접연결할수없을경우클라이언트컴퓨터와호스트컴퓨터간에간접연결을설정합니다. 이시나리오에서데이터는 ShareConnect Communication Server 를통해흐릅니다.

다음그림은 ShareConnect 를실행하는컴퓨터또는모바일장치에서직접연결을사용해사용자가호스트컴퓨터에액세스할때사용되는연결을보여줍니다. 연결단계는그림다음에설명되어있습니다.



 이시나리오에서 Endpoint Management 는 Citrix Files 를위한 SAML IdP 로작동하여 Secure Hub 에서의 SSO 를제공하도록구성되어있습니다. ShareConnect 는 SAML 토큰을 Secure Hub 에요청하고, Secure Hub 는 Citrix Gateway 를통해 Endpoint Management 로요청을전달합니다. 그런다음 Endpoint Management 가 SAML 토큰을

ShareConnect 로보냅니다.

- ShareConnect 가유효성검사를위해 SAML 토큰을 Citrix Files 로보내고 SAML 토큰을 OAuth 토큰과교환합니다.
- ShareConnect 가 OAuth 토큰을 ShareConnect 브로커로보내고, 이브로커는세션토큰을 ShareConnect 로보냅니다.
- ShareConnect 가 ShareConnect Broker 에서호스트컴퓨터목록을얻고호스트컴퓨터자격증명을요구합니다. 그런 다음 ShareConnect 가 ShareConnect Communication Server 와의직접연결을설정합니다. 호스트컴퓨터가자격증명의유효성을검사한후, ShareConnect 는파일및앱의목록을호스트컴퓨터로부터얻습니다. 사용자가파일또는앱을열면 ShareConnect 와호스트컴퓨터가직접연결됩니다.
- 호스트컴퓨터의 ShareConnect 에이전트가 ShareConnect Poll Server 로상태메시지를보내어온라인상태인지또는오프라인상태인지나타냅니다.
- ShareConnect Poll Server 가 ShareConnect 에이전트로부터의부하분산된요청을 ShareConnect Broker 로보내고호스트상태업데이트를 ShareConnect Broker 로보냅니다.

ShareConnect 보안

ShareConnect 는기본제공 128 비트 AES 암호화를사용하여 ShareConnect 클라이언트와 ShareConnect 에이전트를실행하는호스트컴퓨터사이에서전송되는모든데이터가종단간에완전히암호화되도록합니다. 암호화키는각연결별로고유합니다. 가장정교한장치라고해도암호화를해독하는데필요한데이터를가로챌수없습니다.

ShareConnect 클라이언트와호스트컴퓨터간에데이터가직접라우팅되도록 ShareConnect 를구성하는것이일반적입니다. 무제한액세스가가능하도록네트워크액세스정책을구성하지않은경우데이터는 ShareConnect Communication Server 를통해라우팅되지않습니다. 정책에대한자세한내용은이문서에서 Endpoint Management 에 ShareConnect 추가를참조하십시오.

직접또는간접연결에서연결설정에필요한 IP 주소및포트등의암호화된메타데이터가 ShareConnect 서버로보내집니다.

또한 ShareConnect 의 MDX 래핑은 MDX Vault 를통한데이터암호화를제공합니다. MDX Vault 는 iOS(iOS 9 이전) 및 Android 장치에서 MDX 래핑된앱및연관된저장데이터를암호화합니다. 암호화는 OpenSSL 에의해제공되는 FIPS 인증암호화모듈을사용하여수행됩니다.

보안설정및관리자컨트롤에대한정보는다음보안백서에서찾을수있습니다.

ShareConnect 보안백서

ShareConnect 관리자가이드

ShareConnect 포트요구사항

다음포트를열어 ShareConnect 통신을허용합니다. 포트요구사항은연결유형에따라다릅니다. 컴퓨터가동일한 LAN 또는 Wi-Fi 네트워크에있는경우직접연결이이루어질수있고, 클라이언트와호스트컴퓨터를서로직접연결할수없는경우간접연결이이루어질수있습니다.

직접연결의경우

TCP 포트 80 - Citrix Gateway 에서 app.shareconnect.com 으로의아웃바운드연결에사용됩니다.

원본 - Citrix Gateway

대상 - app.shareconnect.com

TCP 포트 80, 443, 8200 - 이러한포트중하나이상이 Citrix Gateway 에서 ShareConnect Communication Server 로의아웃바운드연결에필요합니다.

원본 - Citrix Gateway

대상 - ShareConnect Communication Server

TCP 포트 80, 443, 8200 - ShareConnect 호스트컴퓨터에서 Citrix 서버로의아웃바운드연결에사용됩니다.

출처 - ShareConnect 호스트컴퓨터

대상 - poll.shareconnect.com, ShareConnect Communication Server

TCP 포트 443 - Citrix Gateway 에서필요한사이트로의아웃바운드연결에사용됩니다.

원본 - Citrix Gateway

대상 - crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

TCP 포트 53000 - 53010 - Citrix Gateway 에서 ShareConnect 호스트컴퓨터로의아웃바운드연결에사용됩니다.

원본 - Citrix Gateway

대상 - LAN 기반 ShareConnect 호스트컴퓨터

TCP 포트 53000 - 53010 - Citrix Gateway 에서 ShareConnect 호스트컴퓨터로의인바운드연결에사용됩니다.

원본 - Citrix Gateway

대상 - LAN 기반 ShareConnect 호스트컴퓨터

간접연결의경우

TCP 포트 80 - ShareConnect 에이전트에서 app.shareconnect.com 으로의아웃바운드연결에사용됩니다.

출처 - ShareConnect 에이전트

대상 - app.shareconnect.com

TCP 포트 80, 443, 8200 - 이러한포트중하나이상이 ShareConnect 에이전트에서 ShareConnect Communication Server 로의아웃바운드연결에필요합니다.

출처 - ShareConnect 에이전트

대상 - ShareConnect Communication Server

TCP 포트 80, 443, 8200 - ShareConnect 호스트컴퓨터에서 Citrix 서버로의아웃바운드연결에사용됩니다.

출처 - ShareConnect 호스트컴퓨터

대상 - poll.shareconnect.com, ShareConnect Communication Server

TCP 포트 443 - ShareConnect 에이전트에서필요한사이트로의아웃바운드연결에사용됩니다.

출처 - ShareConnect 에이전트

대상 - crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

ShareConnect 통합및제공

ShareConnect 를 Endpoint Management 와통합하여제공하려면다음일반단계를따르십시오.

1. 선택적으로 Secure Hub 에서 SSO 가사용되도록설정할수있습니다. 이를위해 Endpoint Management 에서 Citrix Files 계정정보를구성하여 Endpoint Management 를 Citrix Files 용 SAML IdP 로사용하도록설정합니다.

   Endpoint Management 콘솔에서 Citrix Files 계정정보를구성하는것은일회용설정입니다. 이일회용설정은모든모바일생산성앱클라이언트, Citrix Files 클라이언트및비 MDX Citrix Files 클라이언트에사용됩니다.

2. ShareConnect 를 다운로드하고 래핑합니다. 자세한내용은 MDX Toolkit 정보를참조하십시오.
3. ShareConnect 를 Endpoint Management 에추가하고 MDX 정책을구성합니다.
4. 호스트컴퓨터에 ShareConnect 에이전트를설치합니다. ShareConnect 에이전트는 MSI 패키지입니다. 따라서 기존소프트웨어배포방법을사용하여에이전트를배포하고설치할수있습니다. 그런다음, 사용자가설치이후 1 시간내에 Citrix Files 자격증명을사용하여에이전트에로그온하여호스트컴퓨터를등록해야합니다.

   또는사용자가 ShareConnect 를통해연결할컴퓨터에 ShareConnect 에이전트를설치할수도있습니다. 자세한내용은이문서에서 “컴퓨터에 ShareConnect 에이전트를설치하려면” 섹션을참조하십시오.

Endpoint Management 에 **ShareConnect** 추가

다른 MDX 앱과동일한절차에따라 ShareConnect 를 Endpoint Management 에추가합니다. 자세한내용은 MDX 앱추가를참조하십시오. ShareConnect 를추가할경우, 다음표에표시된것과같이 MDX 정책을구성합니다.

정책	값	결과
네트워크액세스	내부네트워크로터널링됨또는제한없음	내부네트워크로터널링됨은모든네트워크액세스를위해내부네트워크로의응용프로그램별 VPN 터널을사용합니다. 이구성은 ShareConnect 와호스트컴퓨터간에직접연결을제공합니다. 제한없음 Citrix 소유의 Communication Server 를사용하여호스트컴퓨터와 ShareConnect 간에암호화된데이터를라우팅합니다. 네트워크액세스에대해내부네트워크로터널링됨을사용할계획인경우에도무제한액세스로설정을테스트하여모든것이제대로작동하는지확인해야합니다.
기본설정 VPN 모드	Secure Browse	SSO 가필요한연결에적절하게초기연결모드를설정합니다.
암호화사용	켜짐	태블릿에저장된데이터를암호화합니다.
잘라내기및복사	제한없음	ShareConnect 에서잘라내기및복사작업이가능하게합니다.
붙여넣기	제한없음	ShareConnect 에서붙여넣기작업이가능하게합니다.
문서교환 (열기)	제한없음	연결된컴퓨터또는 ShareConnect 에서연결된네트워크드라이브에있는파일을사용자가열수있게합니다.
암호저장	꺼짐	사용자가 ShareConnect 에로그온할때마다컴퓨터의사용자이름및암호를입력하도록사용자에게요구합니다.

컴퓨터에 **ShareConnect** 에이전트를설치하려면

다음단계에서는지원되는모바일장치로부터연결하려는각물리적또는가상컴퓨터에사용자가 ShareConnect 에이전트를설치하는방법에대해설명합니다.

이러한단계를수행하기전에사용자가먼저 Secure Hub 를설치해야합니다. 그런다음표시되는메시지에따라지원되는모바일장치에모바일생산성앱이설치되도록허용해야합니다.

1. 태블릿에서 Secure Hub 에로그온합니다.
2. ShareConnect 를엽니다.
3. 전자메일다운로드링크를누릅니다.

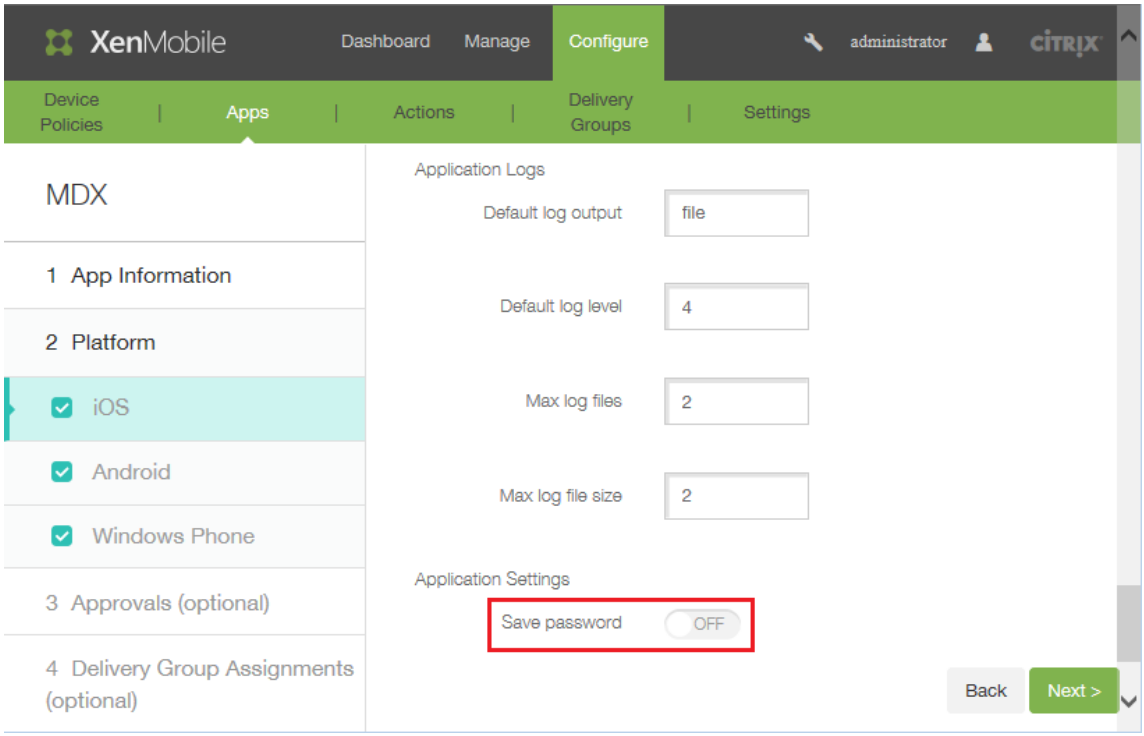
   Citrix 가 no-reply@shareconnect.com 발신의전자메일을보냅니다.
4. ShareConnect 로부터액세스하려는호스트컴퓨터에서전자메일을엽니다.
5. 전자메일에서 Set up this computer(이컴퓨터설정) 를클릭합니다.
6. **ShareConnect_Installer.exe** 를두번클릭하여설치를시작합니다.

   호스트컴퓨터에 ShareConnect 에이전트가설치됩니다. 설치중에 ShareConnect 는 Citrix Files SSO 가구성된경우전자메일주소를요구합니다. 또는 ShareConnect 는 Citrix Files SSO 가구성되지않은 Citrix Files 자격증명을요구합니다.
7. ShareConnect 및시작하기마법사에서제공하는지침을따르십시오.

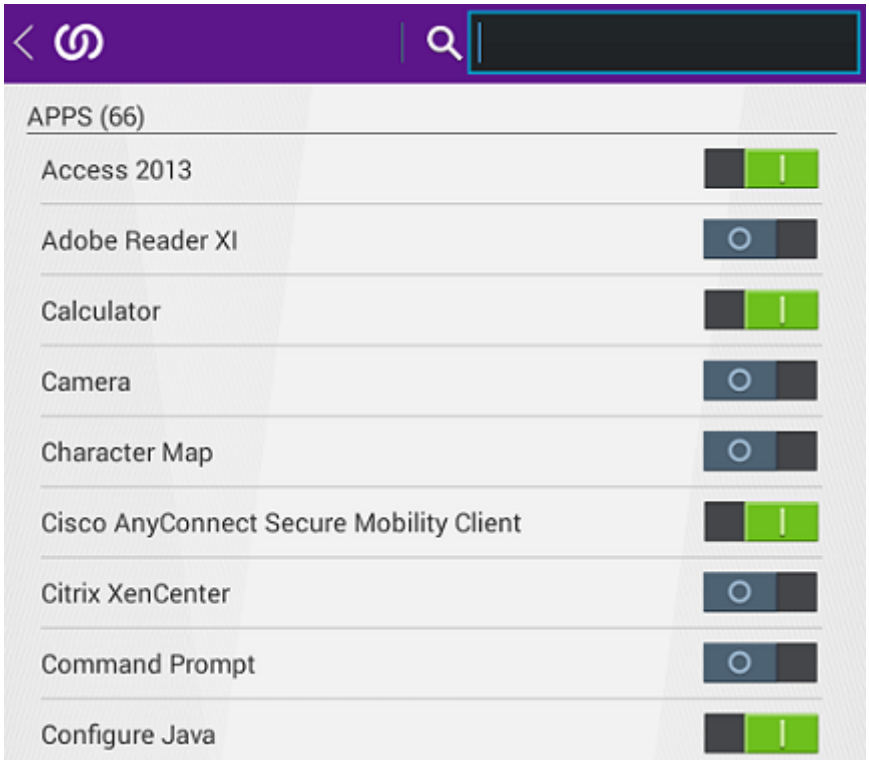
그런다음 ShareConnect 에이전트가호스트컴퓨터를등록합니다. 호스트컴퓨터가켜져있고하나이상의게시된포트 (80, 443 또는 8200) 에서 poll.shareconnect.com 에연결할수있을경우 ShareConnect 클라이언트에서호스트컴퓨터에연결할수있습니다.

ShareConnect 기능

- 호스트컴퓨터추가. 사용자는지원되는모바일장치에서 ShareConnect 를사용하여원격호스트컴퓨터를추가하고해당컴퓨터에연결할수있습니다.
- 파일액세스. 사용자는최근파일목록을볼수있고호스트컴퓨터및연결된드라이브에서파일을찾아보고검색할수있습니다.
- 파일편집. 사용자는태블릿에서호스트컴퓨터에있는데스크톱응용프로그램에액세스하여파일을편집할수있습니다. 사용자는전체화면으로응용프로그램을사용할수있습니다.
- 화면공유. 단일파일또는앱을보는대신, 사용자가화면공유기능을사용하여컴퓨터의바탕화면을볼수있습니다.
- **Citrix Files** 통합. 사용자가호스트컴퓨터와 Citrix Files 간에파일을이동하거나공유할수있습니다.
- 키보드및마우스. ShareConnect 는 Bluetooth 키보드와 Citrix XI Prototype 마우스를동시에사용하는것을지원합니다.
- 제한된포트. ShareConnect 는 53000~53010 포트만사용합니다.
- 로그온할때마다암호강제적용. 보안향상을위해이옵션을구성하여사용자가 ShareConnect 에로그온할때마다컴퓨터암호를입력하도록사용자에게요구할수있습니다. 다음그림에서와같이암호저장정책이꺼져있으면사용자는모든연결에대해로그온자격증명을입력해야합니다.



- 앱추가또는삭제. 사용자는각앱옆에있는스위치를전환하여앱을선택하거나선택취소함으로써 ShareConnect 에있는앱트레이에서앱을추가하거나삭제할수있습니다.



- 미리보기한파일캐싱. ShareConnect 는이미액세스한파일을캐싱하여사용자가다른파일을미리본후에이전파일로돌아올경우파일이다시다운로드되지않게합니다. 이기능은나중에사용자가파일을액세스할때로드시간이개선되도록합니다.

ShareConnect 문제해결

ShareConnect 에이전트설치문제

문제	설명및해결방법
사용자가 ShareConnect 에이전트를다운로드한후 1 시간이상기다렸다가설치를시작하는경우, 사용자는 Citrix Files 계정이름및암호를입력하여 ShareConnect 에이전트를등록해야합니다.	ShareConnect 에이전트설치프로그램은다운로드이후 1 시간뒤에만료되는토큰을포함합니다. 사용자가토큰만료이전에설치를시작하지않으면사용자는 Citrix Files 계정에두번로그온해야합니다. 처음에는 ShareConnect 에이전트를등록하기위해로그온하고두번째는설치완료이후에이전트에로그온하기위해서입니다. 사용자가 1 시간내에 ShareConnect 에이전트를다운로드하고설치하면로그온하라는메시지가한번만나타납니다.
ShareConnect 에이전트등록중에에이전트가연결되지않고 “Please check your connection and try again(연결을확인하고다시시도하십시오).” 같은오류메시지가나타납니다.	poll.shareconnect.com 으로의포트가차단되어있지않는지확인합니다. 자세한내용은이문서앞부분의시스템요구사항을참조하십시오.

ShareConnect 연결문제

> 중요:
>
> ShareConnect 를테스트하기위해네트워크액세스정책을 제한없음으로설정하여포트및네트워크설정관련문제를배제하는것이좋습니다. 무제한액세스는 ShareConnect 가 ShareConnect Communication Server 를통해연결되도록하여 ShareConnect 모바일장치및호스트컴퓨터에내부액세스가있을경우연결을테스트할수있게합니다.

문제	설명및해결방법
ShareConnect 가시작되지만호스트컴퓨터에연결되지않고자격증명을요구하지않습니다.	이문서앞부분의시스템요구사항에서자세히설명된포트요구사항이해당설정으로충족되는지확인합니다.
사용자는 Citrix Files 계정자격증명을사용하여 ShareConnect 에로그온할수없습니다.	ShareConnect 로의 SSO 를위해서는 Citrix Files 계정이 SAML IdP 를통해구성되어야합니다. Endpoint Management 를 SAML IdP 로사용하는것에대한자세한내용은 Citrix Content Collaboration for Endpoint Management를참조하십시오. 다른 IdP 구성에대한자세한내용은이 Knowledge Center 문서를참조하십시오. SSO 가계정에대해구성되지않은경우 iOS 용 ShareConnect 는사용자의 Citrix Files 사용자이름및암호를요구합니다.

문제	설명및해결방법
사용자가 ShareConnect 에로그온한후, ShareConnect 는호스트컴퓨터에연결할수없습니다.	ShareConnect 가직접연결을위해구성된경우 (즉, 네트워크액세스정책이내부네트워크로터널링됨으로설정된경우), 방화벽차단또는프록시서버같은제한이네트워크설정에구성되어있으면연결이실패할수있습니다.

Citrix ShareFile Workflows

October 22, 2018

> 참고:
>
> Secure Forms 는 2018 년 3 월 31 일에 EOL(수명종료) 에도달했습니다. Citrix Files Platinum 및 Premium 계정에포함된 ShareFile Workflows 를사용하는것이좋습니다.

ShareFile Workflows 는 Citrix Files 사용자지정워크플로기능의모바일구성요소입니다. 사용자는이기능을사용해여러트리거와동작이포함된사용자지정워크플로를만들수있습니다. 사용자지정양식을워크플로템플릿에추가하고사용자에게할당할수있습니다.

사용자에게양식을할당하면사용자가 ShareFile Workflows 모바일앱을통해양식을작성하여제출할수있습니다. 양식데이터스토리지는 Citrix Files 와안전하게통합되고여기에워크플로파일이검토, 참조및검색을위해보관됩니다.

Citrix Files 웹응용프로그램내에서워크플로및양식템플릿이생성되고관리됩니다.

사용자설명서

워크플로및양식템플릿의생성및관리와관련된사용자문서는 Citrix Knowledge Center 에있습니다.

- 워크플로템플릿만들기
- 양식템플릿만들기
- 워크플로모바일앱을통해양식제출

Citrix Content Collaboration for Endpoint Management

December 10, 2021

Citrix Content Collaboration for Endpoint Management 클라이언트는 MDX 기반의 Citrix Files 모바일클라이언트버전입니다. 이러한클라이언트는다른 MDX 래핑된앱의데이터에대해보안된통합형액세스를제공합니다. 또한 Citrix Content Collaboration for Endpoint Management 클라이언트는 Micro VPN, Secure Hub SSO(Single Sign-On), 2 단계인증같은 MDX 기능을활용할수있습니다.

Citrix Files 는엔터프라이즈파일동기화및공유서비스로서사용자가손쉽고안전하게문서를교환할수있게합니다. Citrix Files 는 Android 휴대폰용 Citrix Files 및 iPad 용 Citrix Files 등의 Citrix Files Mobile 클라이언트를비롯하여다양한액세스옵션을사용자에게제공합니다.

Citrix Files 를 Endpoint Management 와통합하여전체 Citrix Files 기능을제공하거나 StorageZone 커넥터에대한액세스만제공할수있습니다. 기본적으로 Citrix Endpoint Management 콘솔에서는 Citrix Files 만구성할수있습니다. 대신 StorageZone 커넥터와함께사용하도록 Endpoint Management 를구성하려면 Citrix Endpoint Management 설명서의 Citrix Content Collaboration 과 Endpoint Management 사용을참조하십시오.

다음과같이 Endpoint Management, Citrix Files, StorageZones Controller 및 Citrix ADC 를사용하여 Citrix Content Collaboration for Endpoint Management 클라이언트를배포하고관리할수있습니다.

- Endpoint Management 가 Citrix Files 와함께구성된경우 Endpoint Management 는 SAML IdP(ID 공급자) 역할을하며 Citrix Content Collaboration for Endpoint Management 클라이언트를배포합니다. Citrix Files 데이터는 Citrix Files 에서관리됩니다. Citrix Files 데이터는 Endpoint Management 를통해전달되지않습니다.
- Endpoint Management 가 Citrix Files 또는 StorageZone 커넥터와함께구성된경우 StorageZone Controller 에서네트워크공유및 SharePoint 의데이터에연결해줍니다. 사용자는 Citrix Files 모바일생산성앱을통해저장된데이터에액세스합니다. 사용자는모바일장치에서 Microsoft Office 문서를편집하고, Adobe PDF 파일을미리보고, 주석을달수있습니다.
- Citrix ADC 는 StorageZone 커넥터에대한보안연결, 요청의부하분산및콘텐츠스위칭처리등외부사용자의요청을관리합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트를다운로드하려면 Citrix.com 다운로드를참조하십시오.

Citrix Content Collaboration for Endpoint Management 및기타모바일생산성앱시스템요구사항은 모바일생산성앱 지원을참조하십시오.

Citrix Content Collaboration for Endpoint Management 클라이언트가 **Citrix Files** 모바일클라이언트와다른점

Citrix Content Collaboration for Endpoint Management 클라이언트와 Citrix Files 모바일클라이언트의차이점은 다음과같습니다.

사용자액세스

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Secure Hub 에서 Citrix Content Collaboration for Endpoint Management 클라이언트를가져와서엽니다.

Citrix Files 모바일클라이언트*:*

Citrix Files 모바일클라이언트는앱스토어에서가져옵니다.

SSO

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Endpoint Management 를 Citrix Files 와통합하는경우: Endpoint Management 를 Citrix Files 의 SAML IdP 로구성할수있습니다. 이구성에서는 Secure Hub 가 Endpoint Management 를 SAML IdP 로사용하여 Citrix Content Collaboration for Endpoint Management 클라이언트를위한 SAML 토큰을얻습니다. Secure Hub 에로그인하지않고 Citrix Content Collaboration for Endpoint Management 클라이언트를시작하면 Secure Hub 에로그온하라는메시지가표시됩니다. 사용자가 Citrix Files 도메인또는계정정보를알아야하는것은아닙니다.

Citrix Files 모바일클라이언트*:*

Endpoint Management 및 Citrix Gateway 를 Citrix Files 의 SAML IdP 로구성할수있습니다. 이구성에서웹브라우저또는다른 Citrix Files 클라이언트를사용하여 Citrix Files 에로그온하는사용자는사용자인증을위해 Endpoint Management 환경으로리디렉션됩니다. Endpoint Management 에의해성공적으로인증된후에사용자는 Citrix Files 계정으로로그온하는데유효한 SAML 토큰을받게됩니다.

Micro VPN

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

원격사용자는 VPN 또는 Micro VPN 연결을사용하여 Citrix Gateway 를통해연결하고내부네트워크의앱및데스크톱에액세스할수있습니다. Endpoint Management 와 Citrix ADC 의통합을통해사용가능한이기능은자동으로처리됩니다.

Citrix Files 모바일클라이언트*:*

해당없음.

2 단계인증

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Endpoint Management 와의 Citrix ADC 통합은클라이언트인증서인증과다른인증유형 (예: LDAP 또는 RADIUS) 의조합을사용한인증도지원합니다.

Citrix Files 모바일클라이언트*:*

해당없음.

폴더권한

Citrix Content Collaboration for Endpoint Management 클라이언트및 *Citrix Files* 모바일클라이언트*:*

Citrix Files 와 Endpoint Management 를통합하는경우: Citrix Files 에서결정됩니다.

문서액세스보호

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

사용자는 Secure Mail 로받거나 MDX 래핑된앱에서다운로드한첨부파일을열수있습니다. 사용자가열기작업을수행할경우 MDX 래핑된앱만표시됩니다. 래핑되지않은앱의데이터는 Citrix Content Collaboration for Endpoint Management 클라이언트에서사용할수없습니다. Secure Mail 사용자는파일을장치로다운로드할필요없이 Citrix Files 저장소로부터파일을첨부할수있습니다. 사용자의장치에래핑된 Citrix Files 및래핑되지않은 Citrix Files 가있는경우, 래핑된 Citrix Files 클라이언트는사용자의개인 Citrix Files 계정에있는파일에액세스할수없습니다. 래핑된 Citrix Files 클라이언트는 Endpoint Management 에구성된 Citrix Files 하위도메인에만액세스할수있습니다.

Citrix Files 모바일클라이언트*:*

사용자가모든앱에서첨부파일을열수있습니다.

Citrix Files 계정액세스

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Citrix Files 와 Endpoint Management 를통합하는경우: 개인 Citrix Files 계정또는타사 Citrix Files 계정에액세스하려면해당장치에서비 MDX 버전의 Citrix Files 를사용해야합니다.

Citrix Files 모바일클라이언트*:*

Citrix Files 와 Endpoint Management 를통합하는경우: Citrix Files 클라이언트에서사용할수있습니다.

장치정책

Citrix Content Collaboration for Endpoint Management 클라이언트및 *Citrix Files* 모바일클라이언트*:*

Endpoint Management 와 Citrix Files 장치정책이모두 Citrix Content Collaboration for Endpoint Management 클라이언트에적용됩니다. 예를들어 Endpoint Management 콘솔에서장치초기화를수행할수있습니다. Citrix Files 콘솔에서 Citrix Files 앱을원격으로초기화할수있습니다.

MDX 정책

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

MDX 정책을통해 Endpoint Management 앱스토어가적용할 Citrix Endpoint Management 설정을구성할수있습니다. MDX 를통해서만사용가능한정책은카메라, 마이크, 전자메일작성, 화면캡처및클립보드잘라내기, 복사및붙여넣기작업을차단할수있는기능을포함합니다.

Citrix Files 모바일클라이언트*:*

해당없음.

데이터암호화

Citrix Content Collaboration for Endpoint Management 클라이언트및 *Citrix Files* 모바일클라이언트*:*

저장된모든데이터를 AES-256 를사용하여암호화하고전송중인데이터를 SSL 3.0 및 128 비트이상의암호화를사용하여보호합니다.

상태

Citrix Content Collaboration for Endpoint Management 클라이언트*:*

Citrix Content Collaboration for Endpoint Management 클라이언트는 Endpoint Management Advanced 및 Enterprise Edition 에포함되어있습니다.

Citrix Files 모바일클라이언트*:*

모든 Endpoint Management Edition 에모든 Citrix Files 기능이포함되어있습니다. Endpoint Management 를전체 Citrix Files 기능과통합하거나 StorageZone 커넥터와만통합할수있습니다.

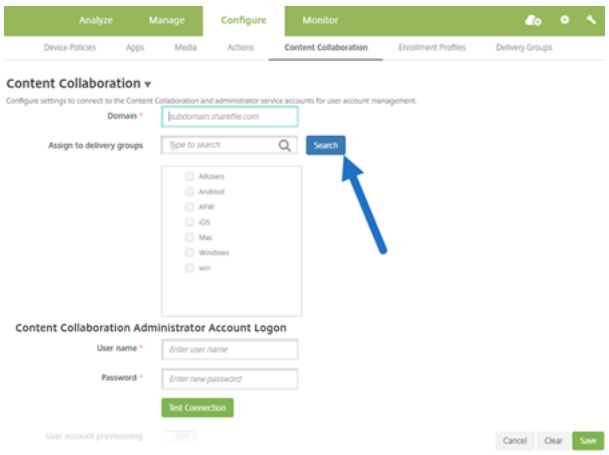
Citrix Content Collaboration for Endpoint Management 클라이언트통합및제공

Citrix Content Collaboration for Endpoint Management 클라이언트를통합하여제공하려면다음일반단계를따르십시오.

1. Citrix Files 클라이언트에서 Citrix Files 에대한 SSO 를제공하도록 Endpoint Management 를 Citrix Files 의 SAML IdP 로사용하도록설정합니다. 이렇게하려면 Endpoint Management 에서 Citrix Files 계정정보를구성해야합니다. 자세한내용은 “Endpoint Management 에서 SSO 에 Citrix Files 계정정보를구성하려면” 섹션을참조하십시오.

   > 중요**:**
   >
   > Citrix Files 웹앱및 Citrix Files 동기화클라이언트같은비 MDX Citrix Files 클라이언트를위한 SAML IdP 로 Endpoint Management 를사용하려는경우추가구성이필요합니다. 자세한내용은 Citrix Files 지원사이트에서
   >
   > Citrix Files(ShareFile) Single Sign-On SSO 문서를참조하십시오. 이문서에는 Endpoint Management 구성가이드다운로드링크가포함되어있습니다.

2. Citrix Files 클라이언트를다운로드합니다.
3. Citrix Files 클라이언트를 Endpoint Management 에추가합니다. 자세한내용은이문서에서 “Citrix Files 를 Endpoint Management 에추가하려면” 을참조하십시오.
4. 구성유효성을검사합니다. 자세한내용은이문서의뒷부분에서 “Citrix Files 클라이언트의유효성을검사하려면” 을참조하십시오.



설정정보**:**

- 도메인은클라이언트에대해사용될 Citrix Files 하위도메인입니다.
- 선택한 DG 의사용자만클라이언트에서 Citrix Files 로 SSO 액세스하게됩니다.

  DG 의사용자에게 Citrix Files 계정이없는경우 Citrix Files 클라이언트를 Endpoint Management 에추가하면 Endpoint Management 가 Citrix Files 에사용자를프로비전합니다.
- Citrix Files 관리자계정로그온정보는 SAML 설정을 Citrix Files 제어부에저장하기위해 Endpoint Management 에의해사용됩니다.

> 중요**:**
>
> Citrix Files 클라이언트부터 Citrix Files 까지 SSO 가사용될수있게하는구성은네트워크공유또는 SharePoint 문서라이브러리에사용자를인증하지않습니다. 이러한커넥터데이터원본에액세스하려면네트워크공유또는 SharePoint Server 가있는 Active Directory 도메인에인증해야합니다.

Endpoint Management 에서 **SSO** 에 **Citrix Files** 계정정보를구성하려면

Secure Hub 에서모바일생산성앱에대한 SSO 를사용하려면 Endpoint Management 콘솔에서 Citrix Files 계정및 Citrix Files 관리자서비스계정정보를지정합니다. 해당구성에서 Endpoint Management 는 Citrix Files, 모바일생산성앱클라이언트, Citrix Files 클라이언트및비 MDX Citrix Files 클라이언트를위한 SAML IdP 역할을합니다. 사용자가모바일생산성앱클라이언트를시작하면 Secure Hub 가 Endpoint Management 에서해당사용자를위한 SAML 토큰을가져와서 Citrix Files 클라이언트로보냅니다.

Endpoint Management 콘솔에서 구성 > Citrix Files 의이전명칭인 **Content Collaboration** 을클릭합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트를 **Endpoint Management** 에추가하려면

Citrix Content Collaboration for Endpoint Management 클라이언트를 Endpoint Management 에추가하는경우 Citrix Content Collaboration for Endpoint Management 클라이언트에서커넥터데이터원본에대한 SSO 액세스를사용하도록설정할수있습니다. 그렇게하려면네트워크액세스정책및기본설정 VPN 모드정책을이섹션에설명된대로구성합니다.

사전요구사항

- Endpoint Management 에서 Citrix Files 하위도메인에연결할수있어야합니다. 연결을테스트하려면 Endpoint Management 서버에서 Citrix Files 하위도메인에대한 Ping 을수행합니다.
- Citrix Files 계정에대해구성된표준시간대와 Endpoint Management 를실행하는하이퍼바이저에대해구성된표준시간대가같아야합니다. 표준시간대가다르면 SAML 토큰이예상한기간내에 Citrix Files 에도달하지못할수있기때문에 SSO 요청이실패할수있습니다. Endpoint Management 에대한 NTP 서버를구성하려면 Endpoint Management 명령줄인터페이스를사용합니다.

  > 참고**:**
  >
  > Linux VM 에서는 Hyper-V 호스트가시간을 UTC 가아닌로컬표준시간대로설정합니다.

- 관리자로 ShareFile 계정에로그인하고 설정 > 관리자설정 > 보안 > 로그인및보안정책 > **Single Sign-on/SAML 2.0** 구성에서 SAML SSO 설정을확인합니다.
- Citrix Content Collaboration for Endpoint Management 클라이언트를다운로드합니다.

단계**:**

1. Endpoint Management 콘솔에서 구성 **>** 앱을클릭한후 추가를클릭합니다.
2. **MDX** 를클릭합니다.
3. 이름을입력하고필요에따라앱에대해 설명및 앱범주를입력합니다.
4. 다음을클릭하고 Citrix Content Collaboration for Endpoint Management 클라이언트에대한.mdx 파일을업로드합니다.
5. 다음을클릭하여앱정보및정책을구성합니다.

   Citrix Content Collaboration for Endpoint Management 클라이언트에서 Citrix Files 로의 SSO 를사용하는구성은네트워크공유또는 SharePoint 문서라이브러리에대해사용자를인증하지않습니다.
6. Secure Hub Micro VPN 과 StorageZones Controller 사이에서 SSO 가가능하도록하려면다음정책구성을완료하십시오.
   - 네트워크액세스정책을 내부네트워크로터널링됨으로설정합니다.

     이모드에서는 MDX 프레임워크가 Citrix Content Collaboration for Endpoint Management 클라이언트에서들어오는모든네트워크트래픽을가로챕니다. 네트워크트래픽은앱전용 Micro VPN 을사용하여 Citrix Gateway 를통해리디렉션됩니다.
   - 기본설정 VPN 모드정책을 **Secure Browse** 로설정합니다.

     이터널링모드에서는 MDX 프레임워크가 MDX 앱으로부터의 SSL/HTTP 트래픽을종료하면 MDX 앱이사용자를위해내부네트워크로의새연결을시작합니다. 이정책설정은 MDX 프레임워크가웹서버에서발행된인증챌린지를감지하고이에응답할수있게합니다.
7. 승인및 DG(배달그룹) 할당을필요에따라완료합니다.

선택된 DG 의사용자만 Citrix Content Collaboration for Endpoint Management 클라이언트에서 SSO 를사용하여 Citrix Files 에액세스하게됩니다. DG 의사용자에게 Citrix Files 계정이없는경우 Citrix Content Collaboration for Endpoint Management 클라이언트를 Endpoint Management 에추가하면 Endpoint Management 가 Citrix Files 에사용자를프로비전합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트의유효성을검사하려면

1. 이문서에서설명된구성을완료한후에 Citrix Content Collaboration for Endpoint Management 클라이언트를시작합니다. Citrix Files 에서로그온메시지를표시하지않습니다.
2. Secure Mail 에서전자메일을작성하고 Citrix Files 첨부파일을추가합니다. 로그온메시지없이 Citrix Files 홈페이지가열립니다.

EOL 및사용되지않는앱

November 19, 2021

다음앱은 EOL(수명종료) 에도달했거나 EOL 상태에도달합니다. 제품릴리스가 EOL 에도달한경우제품라이센스계약기간내에는제품을사용할수있지만사용가능한지원옵션이제한됩니다. 기록정보는 Knowledge Center 또는기타온라인리소스에표시됩니다. 문서는더이상업데이트되지않으며현재상태로제공됩니다. 제품수명주기단계는 Product Matrix(제품매트릭스)를참조하십시오.

> 참고:
> 단계적으로중단되는 Citrix Endpoint Management 기능에대한사전알림은 사용중단을참조하십시오..

Intune 용 **Citrix Files:** 2020 년 12 월 31 일부터사용되지않습니다.

Android Enterprise(작업프로필포함) 및 iOS 사용자등록을통해일반 Citrix Files 앱 (앱스토어에서사용가능) 을컨테이너화하기위해플랫폼기능을활용하는옵션을살펴보는것이좋습니다.

Secure Notes: EOL 수명주기날짜는 2018 년 12 월 31 일입니다.

Secure Notes 및 Secure Tasks 의기능이필요한경우 MDX 정책을사용하여보안을유지할수있는타사앱인 Notate for Citrix 를권장합니다.

Secure Notes 및 Secure Tasks 사용자가 Outlook 에데이터를저장한경우 Notate 에서액세스할수있습니다. ShareFile(현재 Citrix Files) 에데이터를저장한경우에는데이터가마이그레이션되지않습니다.

사용자는 EOL 날짜이후플랫폼운영체제의사용자인터페이스지원이중지될때까지 Secure Notes 를계속해서실행할수있습니다. 그러나지원되지않는제품은사용하지않는것이좋습니다.

Secure Tasks: EOL 수명주기날짜는 2018 년 12 월 31 일입니다.

Secure Forms: EOL 수명주기날짜는 2018 년 3 월 31 일입니다. 고객은 Citrix Files Platinum 및 Premium 계정에포함된 Citrix ShareFile Workflows 로전환하는것이좋습니다. 자세한내용은 Citrix ShareFile Workflows를참조하십시오.

ScanDirect: ScanDirect 는 2018 년 9 월 1 일에 EOL(수명종료) 에도달했습니다.

ShareConnect: ShareConnect 가 2020 년 6 월 30 일에 EOL 에도달했습니다.

Office 365 앱과보안상호작용허용

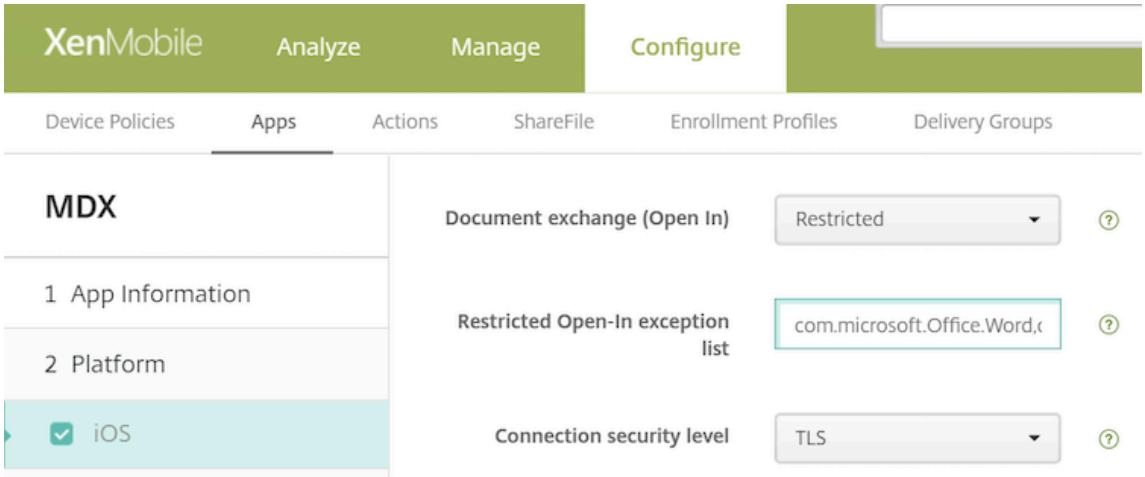
August 27, 2020

Citrix Secure Mail, Citrix Secure Web 및 Citrix Files 는사용자가문서및데이터를 Microsoft Office 365 앱으로전송할수있도록 MDX 컨테이너를여는옵션을제공합니다. Endpoint Management 콘솔에서열기정책을통해 iOS 및 Android 플랫폼에대해이기능을관리할수있습니다.

Microsoft 앱에서열린후에데이터는 MDX 컨테이너에서더이상보안되거나암호화되지않습니다. 이기능을사용하도록설정하기전에보안에미치는영향을고려하십시오. 특히데이터손실방지에주된관심이있거나 HIPAA 또는다른엄격한규정준수요건이적용되는고객은컨테이너열기에따르는장단점을비교평가해야합니다.

iOS 에서 Office 365 를사용하도록설정

1. Secure Mail, Secure Web 또는 Citrix Files 앱의최신버전을 Endpoint Management 다운로드페이지에서다운로드합니다.
2. Endpoint Management 콘솔에파일을업로드합니다.
3. 문서교환 (열기) 정책을찾아 제한됨으로설정합니다. 제한된열기제외 목록에서 Microsoft Word, Excel, PowerPoint, OneNote 및 Outlook 이자동으로나열됩니다. 예를들어 com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook 이표시됩니다.



MDM 등록에서 iOS 장치를위한추가적인컨트롤을사용할수있습니다.

iTunes 앱을 Endpoint Management 콘솔에업로드하고이앱을장치로푸시할수있습니다. 이옵션을선택한경우, 다음정책을켜짐으로설정합니다.

- MDM 프로필이제거된경우앱제거
- 앱데이터백업방지
- 강제로앱관리 (선택적초기화를통해앱및데이터가제거됨)

문서및데이터가 Microsoft 앱에서장치의관리되지않는앱으로이동하는것을방지하려면 Endpoint Management 콘솔에서 구성 **>** 장치 **>** 제한사항 **> iOS** 로이동한후, 관리되지않는앱에있는관리되는앱의문서및 관리되는앱에있는관리되지않는앱의문서를 꺼짐으로설정합니다.

Android 에서 **Office 365** 를사용하도록설정

1. Secure Mail, Secure Web 또는 Citrix Files 앱의최신버전을 Endpoint Management 다운로드페이지에서다운로드합니다.
2. Endpoint Management 콘솔에파일을업로드합니다.
3. 아래로스크롤하여 문서교환 **(**열기**)** 정책으로이동한후 제한됨을선택합니다.
4. 제한된열기제외목록에서다음패키지 ID 를추가합니다.

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

5. 다른앱정책을일반적으로구성하고앱을저장합니다.

장치에서 Secure Mail, Secure Web 또는 Citrix Files 의파일을저장하고이파일을 Office 365 앱으로열어야합니다.

iOS 및 Android 의경우, 사용자가다음파일유형을장치에서열고편집할수있습니다.

지원되는파일형식

지원되는파일형식을보려면 Microsoft Office 문서를참조하십시오.

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