Secure Hub

Contents

Citrix Secure Hub

June 13, 2019

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

Secure Hub 및기타구성요소를 Citrix Endpoint Management 다운로드페이지에서다운로드할수있습니다.

Secure Hub 및모바일생산성앱의기타시스템요구사항은 시스템요구사항 문서를참조하십시오.

이릴리스의새로운기능

Android 용 Secure Hub 19.5.5

이릴리스에는성능개선사항및버그수정이포함되어있습니다.

이전릴리스의새로운기능

Secure Hub 19.5.0, 19.4.5, 19.3.5

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**.** WiFi 장치정책이이제 Android Enterprise 를지원합니다. 이정책에대한자세한내용은다음을참조하십시오. WiFi 장치정책.
- 사용자지정 **XML** 장치정책**.** 사용자지정 XML 장치정책이이제 Android Enterprise 를지원합니다. 이정책에대한자세한내용은다음을참조하십시오. 사용자지정 XML 장치정책.

- 파일장치정책. Citrix Endpoint Management 에스크립트파일을추가하여 Android Enterprise 장치에서기능을수행할수있습니다. 이정책에대한자세한내용은다음을참조하십시오. 파일장치정책.

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. 자세한정보는 제한장치정책 문서를참조하십시오.

Secure Hub 18.10.5~18.11.0 에는버그수정및성능향상기능이포함되어있습니다.

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) 문서를참조하십시오.

  Citrix Endpoint Management 에서 Samsung DeX 모드기능을구성하려면 Samsung KNOX 에대한제한장치정책을업데이트합니다. 자세한내용은 제한장치정책에서 **Samsung KNOX settings(Samsung KNOX** 설정**)** 를참조하십시오.

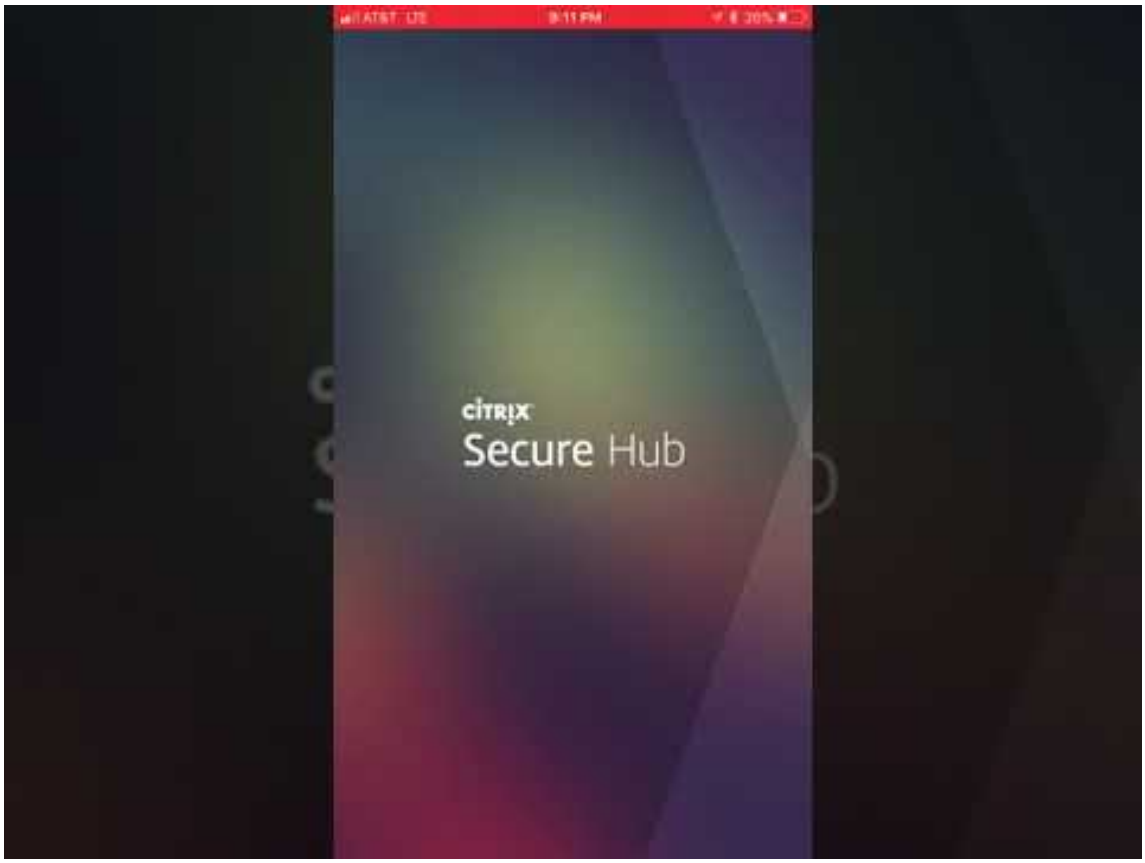
- **Android SafetyNet** 지원: Secure Hub 가설치된 Android 장치의호환성및보안을평가하기위해 **Android SafetyNet** 기능을사용하도록 Endpoint Management 를구성할수있습니다. 평가결과를토대로장치에대한자동화된작업을트리거할수있습니다. 자세한정보는 Android SafetyNet 문서를참조하십시오.
- **Android Enterprise** 장치의카메라사용제한: 제한장치정책의새로운 카메라사용허용설정을통해 Android Enterprise 장치에서카메라를사용하지못하도록제한할수있습니다. 자세한정보는 제한장치정책 문서를참조하십시오.

Secure Hub 10.8.60 ~ 18.9.0

버그수정및성능향상

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 정책요약 문서를참조하십시오.
- AD 또는 AD+Cert 로 Active Directory 인증을구성합니다. 이러한두가지모드가지원됩니다. 인증을구성하는 것에대한자세한내용은 도메인인증또는도메인및보안토큰인증 문서를참조하십시오.
- Endpoint Management 에대한 Workspace 통합기능을사용하도록설정합니다. Workspace 통합에대한 자세한내용은 Workspace Configuration(Workspace 구성) 문서를참조하십시오.

> 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

- Google 제로터치및 Samsung KME(KNOX Mobile Environment) 포털의사용자이름과암호를구성 JSON 을사용하여전달할수있습니다. 자세한내용은 Samsung KNOX 대량등록 문서를참조하십시오.
- 인증서고정을사용하도록설정하면사용자가자체서명된인증서로 Endpoint Management 에등록할수없습니다. 자체서명된인증서로 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 P 동작변경사항에서 Android Developer 사이트문서를참조하십시오.

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 문서 문서를참조하십시오.

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

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 클라이언트속성 문서를참조하십시오.

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

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. 사용자가추가한 CA 대신공용루트 CA 를사용하는것이좋습니다.

Android N 으로업그레이드하는사용자가개인또는자체서명 CA 를사용할경우문제를겪을수있습니다. 다음시나리오에서는 Android N 장치에서의연결이끊깁니다.

- Endpoint Management 에대한개인/자체서명 CA 및필요한신뢰된 CA 옵션은 켜짐으로설정되어있습니다. 자세한내용은 Endpoint Management AutoDiscovery Service(Endpoint Management 자동검색서비스) 문서를참조하십시오.
- 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 지원포털에서기술지원사례를개설합니다. 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
- 도메인에추가하려는 PEM 형식의인증서
- 기존서버인증서를처리하는방식: 오래된서버인증서가손상되어즉시제거할지또는만료될때까지오래된서버인증서를계속지원할지여부

세부정보및인증서가 Citrix 서버에추가되면기술지원사례가업데이트됩니다.

인증서 + 일회용암호인증

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

Secure Hub 가이인증유형을사용하도록설정하려면 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 Management 문서를참조하십시오.

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

   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**)** 를클릭합니다.

    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 포트요구사항 섹션을참조하십시오. 이통신은아웃바운드포트 443 을통해이루어집니다. 기존환경은이액세스를허용하도록설계되었을가능성이매우높습니다. 이통신을지원할수없는고객은 Secure Hub 10.2 로업그레이드하지않는것이좋습니다. 궁금한점이있으면 Citrix 지원팀에문의하십시오.

사전요구사항**:**

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

개선된새인증서고정에서는장치등록전에장치가 ADS 에연결되어야합니다. 그러면장치가등록되고있는환경에서 Secure Hub 가최신보안정보를사용할수있게됩니다. 장치가 ADS 에연결할수없으면 Secure Hub 는장치등록을허용하지않습니다. 따라서내부네트워크내에서 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

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

Secure Hub 사용

사용자는먼저 Apple 또는 Android 스토어에서장치로 Secure Hub 를다운로드합니다.

Secure Hub 가열리면사용자는회사에서제공한자격증명을입력하여 Secure Hub 에장치를등록합니다. 장치등록에대한자세한내용은 사용자계정, 역할및등록 문서를참조하십시오.

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. 앱을추가하려면사용 자가 세부정보를누른후 추가를누릅니다.

구성된도움말옵션

또한 Secure Hub 는도움을받을수있는다양한방법을사용자에게제공합니다. 태블릿에서오른쪽위모서리에있는물음표를누르면 도움말옵션이열립니다. 전화기에서는사용자가왼쪽위모서리의햄버거메뉴아이콘을누른후 도움말을누릅니다.

IT 부서에는사용자가앱에서바로액세스할수있는회사지원센터의전화및전자메일이표시됩니다. 전화번호및전자메일주소를 Endpoint Management 콘솔에입력하십시오. 오른쪽위모서리에서기어아이콘을클릭합니다. 설정페이지가나타납니다. 더 보기를클릭하고 클라이언트지원을클릭합니다. 정보를입력하는화면이나타납니다.

문제보고에앱목록이표시됩니다. 사용자가문제있는앱을선택합니다. Secure Hub 는로그를자동으로생성한후로그가 zip 파일 로첨부된메시지를 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 위치장치정책 문서를참조하십시오.

충돌수집및분석

Secure Hub 는실패정보를자동으로수집및분석하므로특정실패의원인이무엇인지파악할수있습니다. Crashlytics 소프트웨어는이기능을지원합니다.

iOS 및 Android 에서사용할수있는추가기능은 Citrix Secure Hub의플랫폼별기능매트릭스를참조하십시오.

알려진문제와수정된문제

June 13, 2019

Android 용 **Secure Hub 19.5.5** 의알려진문제

- Android 용 Secure Hub 의경우 COSU(회사소유일회사용) 모드일때장치는등록후몇분뒤에연결이끊어지며 GCM 이사용되도록설정된상태에서도알림이수신되지않습니다. [CXM-62977]
- 프로필소유자모드와장치소유자모드모두에대해한번에장치에위치정책을배포하면장치소유자모드의사용자계정이삭제됩니다. 이문제는 NFC 범프를등록할때와 Endpoint Management 가 MDM 모드로구성된경우에발생합니다. [CXM-63429]

Android 용 **Secure Hub 19.5.5** 의수정된문제

- 이릴리스부터 Secure Hub 는 Android 5.0 이상을실행하는장치만지원합니다. [CXM-35542]
- Android 용 Secure Hub 에서장치소유자모드로장치를등록하고새암호를설정하십시오. 장치가첫번째시도에서잠기지않습니다. [CXM-66509]

이전버전의알려진문제와수정된문제

Android 용 **Secure Hub** 버전 **19.5.0** 의알려진문제

- 등록후장치의 OnePlus Android 버전 7.1.1 및 OnePlus 5T Android 버전 9.0.3 에서 Secure Hub 를수동으로다시시작해야 Citrix PIN 을입력하라는메시지가표시됩니다. [CXM-64120]
- 정책을새로고치거나스토어를새로고치지않으면 Android 용 Secure Hub 에서필수앱이 Android 장치에배포되지않습니다. [CXM-65635]

Android 용 **Secure Hub** 버전 **19.5.0** 의수정된문제

- 이릴리스부터 Secure Hub 는 Android 5.0 이상을실행하는장치만지원합니다. [CXM-35542]
- 서버인증서에여러개의주체대체이름이있는경우 Android 용 Secure Hub 에서 Android 6.0 장치등록이실패합니다. [CXM-65030]
- Android 용 Secure Hub 에서장치를등록해제한후관리되는앱이제거되지않습니다. [CXM-65369]
- Samsung S9 장치에서 Android P 로업데이트하면다음과같은문제가발생합니다. Endpoint Management 를통해장치암호를변경하는경우장치의암호가변경되지않습니다. 대신화면이검게변하고 Endpoint Management 콘솔에잠긴장치상태가표시됩니다. [CXM-66391]

Secure Hub 버전 **19.4.5** 의알려진문제

이릴리스에는알려진문제가없습니다.

버전 **19.4.5** 의수정된문제

iOS 용 **Secure Hub**

iOS 장치에서장치등록링크를클릭하면 Secure Hub 에서 Endpoint Management FQDN 인스턴스이름이자동으로입력되지않습니다. 장치등록요청이실패합니다. [CXM-65423]

Android 용 **Secure Hub**

이릴리스에는수정된문제가없습니다.

버전 **19.3.5** 의알려진문제

iOS 용 **Secure Hub**

iOS 용 Secure Hub 에서알림이전송될때알림배지수가 Secure Hub 에대해업데이트되지않습니다. [CXM-53500]

Android 용 Secure Hub

이릴리스에는알려진문제가없습니다.

버전 **19.3.5** 의수정된문제

iOS 용 Secure Hub

이릴리스에는수정된문제가없습니다.

Android 용 Secure Hub

- Android 용 Secure Hub 에서공유장치를등록할경우 웹클립정책을배포하고웹및 SaaS 앱을추가하면배포가성공합니다. 하지만 Citrix Endpoint Management 콘솔의 앱인벤토리화면에는이배포가실패한것으로나타납니다. [CXM-57500]
- Android 용 Secure Hub 에서사용자가보안 PIN 을사용하여로그인하는경우 VPN 터널이설정되지만 Secure Web 은웹사이트를로드하지않습니다. 그러나 Secure Web 을닫았다가다시열면웹사이트가예상대로로드됩니다. [CXM-60751]
- Microsoft Intune 정책으로구성된 Android 용 Secure Mail 이인증후빈화면을반환합니다. [CXM-61457]
- Android 용 Secure Hub 에서암호화를사용하지않도록설정한앱이 Secure Hub 에서암호화키를가져오려고합니다. [CXM-61459]
- Intune Company Portal 버전 5.0.4324.0 이설치되어있으면 Android 용 Secure Mail 이시작시충돌합니다. 자세한내용은이 Support Knowledge Center 문서 문서를참조하십시오. [CXM-62516]
- Android 7.1.1 에서실행되는 COSU(회사소유일회사용) Android Enterprise 장치의시스템앱을 Android 용 Secure Hub 에서사용할수없습니다. [CXM-63653]
- Android 용 Secure Hub 에서 Google Play 의여러앱을필수앱으로구성하고등록하려고하면첫번째앱을설치하라는메시지가표시됩니다. 첫메시지에이어두번째앱을설치하라는메시지가즉시나타납니다. [CXM-63654]

버전 **19.3.0** 의알려진문제

iOS 용 Secure Hub

이릴리스에는알려진문제가없습니다.

Android 용 Secure Hub

- Android 용 Secure Hub 에서공유장치를등록할경우웹클립정책을배포하고웹및 SaaS 앱을추가하면배포가성공합니다. 하지만 Citrix Endpoint Management 콘솔의앱인벤토리화면에는이배포가실패한것으로나타납니다. [CXM-57500]
- Android Enterprise 장치의위치정책에서지오펜스위반에잠금동작을설정할경우시스템에서생성된암호가사용되는것이아니라새암호를설정하라는메시지가나타납니다. [CXM-60425]

버전 **19.3.0** 의수정된문제

iOS 용 **Secure Hub**

이릴리스에는수정된문제가없습니다.

Android 용 **Secure Hub**

완전하게관리되는 Android Enterprise 장치를암호로잠금보안동작을사용하여원격에서잠그면오류알림없이동작이실패할수있습니다. 장치가잠겼는지확인하려면암호로잠금을두번설정합니다. 장치는두번째로설정한암호로잠깁니다. [CXM-61095]

버전 **19.3.0** 의알려진문제

iOS 용 **Secure Hub**

이릴리스에는알려진문제가없습니다.

Android 용 **Secure Hub**

- Android 용 Secure Hub 에서공유장치를등록할경우웹클립정책을배포하고웹및 SaaS 앱을추가하면배포가성공합니다. 하지만 Citrix Endpoint Management 콘솔의앱인벤토리화면에는이배포가실패한것으로나타납니다. [CXM-57500]
- Android Enterprise 장치의위치정책에서지오펜스위반에잠금동작을설정할경우시스템에서생성된암호가사용되는것이아니라새암호를설정하라는메시지가나타납니다. [CXM-60425]

버전 **19.3.0** 의수정된문제

iOS 용 **Secure Hub**

이릴리스에는수정된문제가없습니다.

Android 용 **Secure Hub**

완전하게관리되는 Android Enterprise 장치를암호로잠금보안동작을사용하여원격에서잠그면오류알림없이동작이실패할수있습니다. 장치가잠겼는지확인하려면암호로잠금을두번설정합니다. 장치는두번째로설정한암호로잠깁니다. [CXM-61095]

버전 **19.2.0** 의알려진문제

버전 19.2.0 에는알려진문제가없습니다.

버전 **19.2.0** 의수정된문제

iOS 용 **Secure Hub**

iOS 용 Secure Hub 의경우사용자가 Secure Hub 스토어에서로그오프할때 '서버에서앱을가져오라는네트워크요청시간이초과됨' SSL 핸드셰이크실패메시지가반복적으로나타납니다. [CXM-61339]

Android 용 **Secure Hub**

- Android Enterprise 의파일장치정책은작업프로필모드에서 Android 장치에배포되지않습니다. [CXM-61196]
- Android 용 Secure Hub 의경우공유장치에서새사용자의로그인인증에오랜시간이걸립니다. 등록된사용자로로그오프한후새사용자로로그인하려고하면장치를재부팅하지않는한 Secure Hub 로딩이끝나지않습니다. [CXM-61338]
- Android 용 Secure Hub 의경우클라우드고객이외부 ID 공급자를사용하여 Android Enterprise 장치를등록할수없습니다. [CXM-61738]
- Android 용 Secure Hub 의경우 COSU(회사소유일회사용) 모드일때 Secure Hub 에서앱아이콘들이겹칩니다. [CXM-61740]
- Android 용 Secure Hub 의기존설정에서인증서고정을사용하도록설정하면인증서에여러개의주체대체이름이있는경우인증이실패하고최초사용자화면으로돌아갑니다. [CXM-61933]

버전 **19.1.5** 의알려진문제

- Android 용 Secure Hub 에서암호정책변경으로인해암호를업데이트한경우 Samsung Galaxy S8 장치에서배지앱이나타나지않습니다. [CXM-61177]
- Android 용 Secure Hub 에서 Android Enterprise 의파일장치정책은작업프로필모드에서장치에배포되지않습니다. [CXM-61196]

버전 **19.1.5** 의수정된문제

- Android 용 Secure Hub 에서사용자가 Secure PIN 을사용하여로그인하는경우 VPN 터널이설정되지만 Secure Web 은웹사이트를로드하지않습니다. 그러나 Secure Web 을닫았다가다시열면웹사이트가예상대로로드됩니다. [CXM-58576]
- Android 용 Secure Hub 에서 Secure PIN 을사용하여로그온할경우 VPN 터널이설정되지만 Secure Web 은웹사이트를로드하지않습니다. 그러나 Secure Web 을닫았다가다시열면웹사이트가예상대로로드됩니다. [CXM-60751]
- Android 용 Secure Hub 에서 TechXpert 라는사내앱의로그를캡처하려고하면 Secure Hub 가다시시작되고다시인증하라는메시지가나타납니다. [CXM-61310]

버전 **19.1.0** 의알려진문제

iOS 용 **Secure Hub**

iOS 용 Secure Hub 에서 MDX 및웹또는 SaaS 앱을배포하면 내앱화면에표시됩니다. 자세히를누르면이전 UI 브랜딩형식의 삭제및 취소옵션이포함된팝업이나타납니다. [CXM-60683]

버전 **18.12.0** 의수정된문제

- Android For Work 에등록된 Samsung Knox 장치에서 1 일 ~2 일내에만료되는암호정책을구성하면 "암호만료" 메시지가반복적으로나타납니다. [CXM-59250]
- QR 코드등록방법을사용하여 OnePlus 5T 장치를 Android Enterprise 에등록할수없습니다. [CXM-59288]

버전 **18.11.0** 의수정된문제

Secure Hub iOS

- 공유장치모드에서등록된 Android 장치에서 Single Sign-on 을수행할수없습니다. 다음오류가나타납니다. 지금은회사자격증명을검색할수없습니다. 관리정책때문에 ShareFile 에대한수동로그인이차단되었습니다. [CXM-58238]
- COSU(회사소유의단일사용) 장치에서 Android 볼륨수준을편집할수없습니다. [CXM-58323]

버전 **18.10.5** 의수정된문제

- XenMobile Server 에서 FIPS 모드가사용되도록설정된경우 iOS 용 Secure Hub 를버전 18.10.5 로업데이트한후에앱을열때암호화관련오류메시지가표시됩니다. 해결방법에대한상태업데이트는이 Citrix Knowledge Center 문서 문서를참조하십시오. [CXM-56454]

버전 **10.8.25~18.10.6** 의수정된문제

- Secure Hub 버전 10.8.25~18.10.6(Android) 에는알려진문제가없습니다. 다음문제는 Secure Hub 에서수정되었습니다. 목록에는 Secure Hub 에영향을미치는 MDX 관련문제가포함되어있습니다.

버전 **18.10.0** 의수정된문제

- EMS 콘솔에서 MVPN 정책이해제되어있는경우 Intune 으로관리되는앱을열때빈화면이표시됩니다. [CXM-56033, CXM-56086, CXM-54393, CXM-54823]

버전 **10.8.60** 의수정된문제

- Samsung Galaxy Tab Active 2 SM-T395 장치에서, 관리자가 XenMobile 에서공장기본값으로재설정사용안함 제한을설정한경우 Android 용 Secure Hub 의전체초기화보안작업이실패합니다. [CXM-54452]
- VPN 정책이구성되어있고 Citrix SSO 응용프로그램이장치에설치되어있지않은경우장치등록중 Android 용 Secure Hub 가응답하지않습니다. 뒤로단추를누르거나앱을다시시작하면응답합니다. [CXM-54627]

- Android Enterprise 환경에서장치소유자모드로등록하는동안 Android 용 Secure Hub 가비정상적으로종료됩니다. [CXM-55008]
- 사용자가 iOS 용 Secure Hub 에올바른 PIN 을입력한후에도반복해서 PIN 을입력하라는메시지가표시됩니다. [CXM-55047]
- Android Enterprise 환경에서프로필소유자모드로등록하는동안 Android 용 Secure Hub 가비정상적으로종료됩니다. [CXM-55076]
- Android 용 Secure Hub 에서 Android Enterprise 를사용하는경우 Google Chrome 이기본적으로설치됩니다. [CXM-55232]
- iOS 용 Secure Hub 를버전 10.8.55 로업그레이드하면기존또는새 iOS 장치를등록할수없습니다. [CXM-55267]

버전 **10.8.55** 의수정된문제

- G Suite 자격증명이 Endpoint Management 의자격증명과다른경우사용자가 Secure Hub 에로그온하여 Android for Work 계정에등록할수없습니다. [CXM-53956]

버전 **10.8.55** 의 **MDX** 관련수정된문제

- 기본설정 VPN 모드가 SecureBrowse 로설정된경우엔터프라이즈앱에서내부리소스연결문제가발생할수있습니다. [CXM-52309]
- android.support.multidex.MultiDexApplication 또는 android.app.Application 을응용프로그램클래스로지정하는앱은 Secure Browse 모드에서내부네트워크에연결할수없습니다. [CXM-53126]
- Android 장치에서다수의인증서가생성되고만료날짜전에인증서가해지됩니다. [CXM-53428]

버전 **10.8.55** 의알려진문제

- 장치에서 Secure Hub 계정을제거한후 MDM 재등록이실패합니다. [CXM-54142]

버전 **10.8.50** 의알려진문제

- Android 용 Secure Hub 에서사용자가웹링크바로가기를추가할수없습니다. [XMHELP-952]

버전 **10.8.35** 의수정된문제

- Android O 에서정책을통해생성된바로가기가장치홈화면에표시되지않습니다. 이동작은 Android O 에서의도된것입니다. [CXM-35460]
- Samsung 태블릿에서 Android 용 Secure Hub 가비활성기간후열리지않습니다. [CXM-50797]
- Samsung Knox 장치의 Android 용 Secure Hub 에서푸시정책을배포할수없습니다. [CXM-50869]
- iOS 용 Secure Hub 에서다음문제가가끔발생합니다. 사용자가 Active Directory 암호를변경한후 PIN 을루프에계속입력해야합니다. [CXM-50224]

버전 **10.8.25** 의수정된문제

- MDX Toolkit 버전 10.7.20 으로래핑된타사 iOS Cordova 앱에서 화면콘텐츠가리기정책을사용하도록설정한후 PIN 화면대신검정색화면이나타납니다. [CXM-48471]
- Android 7 을실행하는 Zebra T51 장치에서사용자가 Citrix Launcher 앱을설치할수없습니다. [CXM-50621]

버전 **10.8.20** 의수정된문제

- 사용자가 Android 장치를버전 8(Oreo) 로업데이트한후에 Endpoint Management 에서배포한앱스토어에서엔터프라이즈앱또는.apk 앱을설치할수없습니다. 타사앱을설치할수있도록설정할경우에도문제가지속됩니다. 이문제는 Samsung 장치에국한되지않습니다. [CXM-50401]

버전 **10.8.15** 의수정된문제

- Android O 를실행하는장치에서위치세부정보를가져오는동안 Android 용 Secure Hub 에서충돌이발생합니다. [CXM-47893]

버전 **10.8.10** 의수정된문제

- Android 장치에서다수의앱이자동으로설치되지않거나사용자가직접 설치를클릭하지않는경우앱이계속다운로드됩니다. 그결과데이터사용량이높아집니다. [CXM-46404]
- Android 7 이상을실행하는장치의경우: XenMobile Server 에서장치로암호와함께잠금보안동작을전송하면장치가 잠깁니다. 하지만사용자에게기존잠금화면암호가있는경우장치암호가변경되지않습니다. 사용자는원래암호를사용하여장치잠금을해제할수있습니다. [CXM-47908]

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 문서 문서를참조하십시오.

인증프롬프트시나리오

April 19, 2019

장치에서자격증명을입력하여 Secure Hub 에인증하라는메시지가다양한시나리오에서사용자에게표시됩니다.

시나리오는다음과같은요인에따라달라집니다.

- Endpoint Management 콘솔설정의 MDX 앱정책및클라이언트속성구성
- 인증이오프라인으로이루어지는지또는온라인인증 (장치가 Endpoint Management 로의네트워크연결을필요로함) 이어야하는지여부

또한사용자가입력하는자격증명의종류 (Active Directory 암호, Citrix PIN 또는암호, 일회용암호, 지문인증 (iOS 에서일명 Touch ID)) 도필요한인증유형및인증빈도에따라달라집니다.

인증프롬프트가표시되는시나리오부터살펴보겠습니다.

- 장치다시시작**:** 사용자가장치를다시시작하면 Secure Hub 에서재인증해야합니다.
- **Offline inactivity (time-out)(**오프라인비활성화 **(**시간제한**)):** 앱암호 MDX 정책 (기본적으로사용으로설정됨) 을사용하도록설정된경우비활성화타이머라는 Endpoint Management 클라이언트속성이작동하게됩니다. 비활성화타이머는보안컨테이너를사용하는앱에서사용자활동없이경과할수있는시간의길이를제한합니다.

비활성화타이머가만료되면사용자는장치에서보안컨테이너에인증해야합니다. 예를들어사용자가장치를내려놓고떠나간경우비활성화타이머가만료되면다른사람이해당장치를주워서컨테이너내의민감한데이터에액세스할수없습니다. 비활성화타이머클라이언트속성은 Endpoint Management 콘솔에서설정합니다. 기본값은 15 분입니다. 앱암호를 켜짐으로설정하고비활성화타이머 클라이언트속성이작동하면대부분의일반적인인증프롬프트시나리오에대응할수있습니다.

- **Secure Hub** 에서로그오프**:** 사용자가 Secure Hub 에서로그오프하는경우사용자는다음번에 Secure Hub 또는 MDX 앱에액세스할때앱암호 MDX 정책및비활성화타이머상태에의해앱에서암호를요구하면다시인증해야합니다.
- 최대오프라인기간**:** 이시나리오는앱별 MDX 정책으로구동되는개별앱에관한것입니다. 최대오프라인기간 MDX 정책의 기본설정은 3 일입니다. Secure Hub 에온라인으로인증하지않고앱이실행될수있는기간이경과하면앱권한확인및정책 새로고침을위해 Endpoint Management 체크인이필요합니다. 이체크인이발생하면앱이온라인인증을위해 Secure Hub 를트리거합니다. MDX 앱에액세스하려면먼저사용자가재인증해야합니다.

최대오프라인기간과활성폴링기간 MDX 정책간의관계에유의하십시오.

- 활성폴링기간은앱잠금, 앱초기화등의보안작업을수행하기위해앱이 Endpoint Management 에체크인하는간격입니다. 또한앱은업데이트된앱정책이있는지확인합니다.
- 활성폴링기간정책을통해성공적으로정책을확인한후에최대오프라인기간타이머가재설정되고다시카운트를시작합니다.

활성폴링기간및최대오프라인기간만료의경우 Endpoint Management 에체크인하려면장치에서유효한 Citrix Gateway 토큰이필요합니다. 유효한 Citrix Gateway 토큰이장치에있는경우, 앱은사용자를방해하지않으면서 Endpoint Management 에서새정책을가져옵니다. 앱에서 Citrix Gateway 토큰이필요하면 Secure Hub 로전환되고 Secure Hub 에서는인증프롬프트가사용자에게표시됩니다.

Android 장치에서는 Secure Hub 활동화면이현재앱화면바로위에열립니다. 하지만 iOS 장치에서는 Secure Hub 가포그라운드로전환되어야하므로현재앱이일시적으로사라집니다.

사용자가자격증명을입력한후에 Secure Hub 는다시원래앱으로전환됩니다. 이경우캐싱된 Active Directory 자격증명을허용하거나클라이언트인증서가구성되어있으면사용자가 PIN, 암호또는지문인증을입력할수있습니다. 그렇지않은경우, 사용자는 완전한 Active Directory 자격증명을입력해야합니다.

다음 Citrix Gateway 정책목록에설명된 Citrix Gateway 세션비활성또는강제세션시간제한정책으로인해 Citrix ADC 토큰이유효하지않게될수있습니다. 사용자가 Secure Hub 에다시로그온하면앱을계속실행할수있습니다.

- **Citrix Gateway** 세션정책**:** 두가지 Citrix Gateway 정책은사용자에게인증프롬프트가표시되는시점에도영향을줍니다. 이러한경우사용자는 Endpoint Management 에연결하려고 Citrix ADC 와의온라인세션을만들기위해인증합니다.

- 세션시간초과**:** 설정된기간동안네트워크활동이발생하지않으면 Endpoint Management 에대한 Citrix ADC 세션이연결해제됩니다. 기본값은 30 분입니다. Citrix Gateway 마법사를이용해정책을구성하는경우에는기본값이 1440 분입니다. 시간제한을넘기면회사네트워크에다시연결하라는인증프롬프트가사용자에게표시됩니다.
- 강제시간제한**:** 켜짐인경우, 강제시간제한기간이경과한후에 Endpoint Management 에대한 Citrix ADC 세션이연결해제됩니다. 강제시간제한은설정된기간이후에재인증이필수로수행되도록합니다. 다음에사용할때회사네트워크에재연결하기위해인증프롬프트가사용자에게표시됩니다. 기본값은 꺼짐입니다. Citrix Gateway 마법사를이용해정책을구성하는경우에는기본값이 1440 분입니다.

자격증명유형

앞의섹션에서는사용자에게인증프롬프트가표시되는시점에대해설명했습니다. 이섹션에서는사용자가입력해야하는자격증명의종류를살펴봅니다. 장치에서암호화된데이터에대한액세스권한을얻으려면다양한인증방법을통한인증이필요합니다. 처음에장치를잠금해제하려면 기본컨테이너를잠금해제합니다. 그런후에컨테이너가다시보안되면액세스권한을다시얻기위해 보조컨테이너를잠금해제합니다.

> 참고:
>
> 문서에 관리되는앱이라고나와있는경우, 이용어는 MDX Toolkit 에의해래핑된앱을가리킵니다. 앱암호 MDX 정책은기본적으로사용하도록설정된상태로그대로두고비활성화타이머클라이언트속성을활용합니다.

자격증명유형을결정하는상황은다음과같습니다.

- 기본컨테이너잠금해제**:** 기본컨테이너를잠금해제하려면 Active Directory 암호, Citrix PIN 또는암호, 일회용암호, Touch ID 또는지문 ID 가필요합니다.
  - iOS 에서앱이장치에설치된후사용자가 Secure Hub 또는관리되는앱을처음여는경우
  - iOS 에서사용자가장치를재시작한후, Secure Hub 를여는경우
  - Android 에서 Secure Hub 가실행중이아닐때사용자가관리되는앱을여는경우
  - Android 에서장치재시작등의이유로인해 Secure Hub 를재시작하는경우
- 보조컨테이너잠금해제**:** 보조컨테이너를잠금해제하려면지문인증 (구성된경우), Citrix PIN 또는암호, Active Directory 자격증명이필요합니다.
  - 비활성화타이머만료이후사용자가관리되는앱을여는경우
  - 사용자가 Secure Hub 에서로그오프한후관리되는앱을여는경우

다음조건에해당할경우두가지컨테이너잠금해제상황에대해 Active Directory 자격증명이필요합니다.

- 사용자가 Corporate 계정에연결된암호를변경하는경우
- Endpoint Management 콘솔에서 Citrix PIN(ENABLE_PASSCODE_AUTH 및 ENABLE_PASSWORD_CACHING)을사용하도록클라이언트속성을설정하지않은경우
- 장치가자격증명을캐싱하지않거나장치에클라이언트인증서가없을때 NetScaler Gateway 세션이종료되는경우 (세션시간제한또는강제시간제한정책타이머가만료될때종료됨)

지문인증을사용설정하면사용자는앱이비활성화되어오프라인인증이필요한경우에지문을사용하여로그인할수있습니다. 사용자가 Secure Hub 에처음로그인할때와장치를다시시작할때에는여전히 PIN 을입력해야합니다. 지문인증사용에대한자세한내용은 지문또는 Touch ID 인증 문서를참조하십시오.

다음순서도에는인증프롬프트가표시될때사용자가입력해야하는자격증명을결정하는흐름이요약되어있습니다.

Secure Hub 화면전환정보

앱에서 Secure Hub 로전환된후다시앱으로전환되어야하는상황에도유의해야합니다. 전환과정에서사용자가확인해야할 알림이표시됩니다. 이경우인증은필요하지않습니다. 이상황은최대오프라인기간및활성폴링기간 MDX 정책에의해지정된 대로 Endpoint Management 에체크인하고 Secure Hub 를통해장치에푸시되어야하는업데이트된정책을 Endpoint Management 가감지한후에발생합니다.

iOS VPN 설치

March 13, 2019

iOS 10 이상장치에서는 Secure Hub 와 MDX 앱사이의안전한로컬데이터공유를위해 Secure Hub VPN 이사용됩니다. Secure Hub VPN 은 iOS 10 이상장치에서실행됩니다. Secure Hub VPN 은 Secure Hub 와 MDX 앱이이 VPN 을통해 원활하게통신할수있기때문에이상적인사용자환경을제공합니다.

Secure Hub VPN 은 Apple Enterprise 개발자계정 (‘팀 ID’) 인증서, Citrix 인증서, Enterprise 인증서또는타사 ISV 인증서로서명된앱을위해작동합니다.

Secure Hub VPN 은 iOS 10 장치에서기본적으로사용됩니다. Secure Hub VPN 이 iOS 10 장치에서실행되고있지않으면 MDX 는안전한데이터공유를위해 iOS 공유키집합을사용합니다. iOS 공유키집합메커니즘에서는참여하는모든앱이해당 iOS ‘팀 ID’ 인증서의공유키집합에액세스하기위해서는동일한인증서로서명되어있을것을요구합니다. Citrix 서명 Secure Hub 앱과동일한인증서로앱이서명되어있지않으면필요한정보를얻기위해앱이 Secure Hub 로전환할수도있습니다.

Secure Hub VPN 은 Citrix Endpoint Management Enterprise 및 MAM 전용배포에만사용할수있습니다. Secure Hub VPN 은 Endpoint Management MDM 전용환경에적용되지않고, MDM 전용등록에는 VPN 이설치되어있지않습니다.

Secure Hub VPN 은 Secure Hub 와모바일생산성앱사이의통신에사용됩니다. Secure Hub VPN 은장치의네트워크트래픽을필터링또는모니터링하지않으며 MDX Micro VPN 메커니즘에독립적입니다.

> 참고:
>
> 기본적으로사용설정된환경에서는 Secure Hub VPN 을사용설정상태그대로두는것이좋습니다.
>
> 하지만 iOS 는두개이상의 VPN 클라이언트가동시에 iOS 장치에서실행되도록허용하지않으므로다음상황에유의하시기바랍니다. 장치수준 VPN 연결을설정하기위해다른 VPN 앱 (예: Cisco AnyConnect 또는 Citrix VPN) 을동시에 iOS 장치에서실행해야하는경우 Secure Hub VPN 을사용할수없습니다. Secure Hub VPN 을사용중지하지않고도 iOS 앱별 VPN 을설정할수있습니다. iOS 앱별 VPN 을사용하는앱은앱이포그라운드에서실행될때앱별 VPN 연결을설정합니다.
>
> Secure Hub VPN 을사용중지하려면이문서의다음섹션을참조하십시오. Secure Hub VPN 을사용중지한경우관리되

> 는앱에서 Secure Hub 로전환하는현상이더자주발생할수있습니다.

Endpoint Management 에서 **Secure Hub VPN** 을사용중지하거나다시사용설정

사용자가 iOS 10 에서 Secure Hub 10.3.10 을사용하기시작하면기본적으로 Secure Hub VPN 이사용설정됩니다.

Secure Hub VPN 을사용중지하고배포환경의 iOS 장치가공유키집합메커니즘을사용설정하려면다음을수행하십시오.

1. Endpoint Management 콘솔에서 설정 **>** 클라이언트 **>** 클라이언트속성으로이동합니다.
2. 클라이언트속성페이지에서 **ENABLE_NETWORK_EXTENSION** 이라는사용자지정클라이언트속성을생성하고값을 0 으로설정합니다.

   Secure Hub VPN 을다시사용설정하기위해 Secure Hub VPN 으로이동하고 **ENABLE_NETWORK_EXTENSION** 의값을 1 로설정합니다.

클라이언트장치에 **Secure Hub VPN** 설치

Secure Hub VPN 은 Secure Hub 10.3.10 이상이 iOS 10 장치에설치된후또는사용자가 Secure Hub 10.3.10 이상을실행하는장치를 iOS 10 으로업그레이드하는두가지경우에설치됩니다.

다음정보메시지가사용자에게표시됩니다.

그런다음, VPN 구성추가에대한허가를요청하는 iOS 메시지가사용자에게표시됩니다. 이메시지는 VPN 이처음설치될때한번만표시됩니다. 사용자가 Secure Hub 를다시열때는표시되지않습니다.

이화면의메시지는사용자지정할수없는것으로, 모든 VPN 설치에사용되는표준 iOS 대화상자입니다.

VPN 구성추가에대한허가를요청하는화면에서사용자가 허용안함을선택하는경우, Secure Hub 에액세스하기위해서는 VPN 을설치해야한다는내용의다른메시지가다시표시됩니다.

클라이언트장치에서 **Secure Hub VPN** 실행

설정한대로 Secure Hub VPN 이실행되고있으면 iOS 설정앱의 일반 **> VPN** 화면에 연결중이라는텍스트가표시됩니다.

이는예상된것이고, MDX 공유및통신메커니즘이작동하고있지않음을의미하는것은아닙니다. 이메시지가표시되면사용자가조치를취할필요는없습니다.

파생된자격증명을사용하여장치등록

January 25, 2019

파생된자격증명은모바일장치를위한강력한인증을제공합니다. 이자격증명은스마트카드로부터파생되어카드가아닌모바일장치에상주합니다. 스마트카드는 PIV(Personal Identity Verification) 카드또는 CAC(Common Access Card) 입니다.

파생된자격증명은 UPN 같은사용자식별자가포함된등록인증서입니다. Endpoint Management 는자격증명공급자로부터받은자격증명을장치의보안저장소에저장합니다.

Endpoint Management 는파생된자격증명을 iOS 장치등록에사용할수있습니다. 파생된자격증명을사용하도록구성하면 Endpoint Management 가 iOS 장치에대해등록초대또는기타등록모드를지원하지않습니다. 그러나동일한 Endpoint Management 서버에서등록초대및기타등록모드를통해 Android 장치를등록할수는있습니다.

파생된자격증명을사용하는경우의장치등록단계

등록하려면사용자데스크톱에부착된판독기에스마트카드를삽입해야합니다.

1. 사용자가 Secure Hub 와파생된자격증명공급자로부터받은앱을설치합니다. 이예에서 ID 공급자앱은 Intercede MyID ID Agent 입니다.
2. 사용자가 Secure Hub 를시작합니다. 메시지가나타나면사용자가 Endpoint Management FQDN(정규화된도메인이름) 을입력하고 다음을클릭합니다. Secure Hub 에서등록이시작됩니다. Endpoint Management 에서파생된자격증명을지원하는경우 Secure Hub 에사용자가 Citrix PIN 을생성하도록요청하는메시지가표시됩니다.
3. 사용자가화면의안내에따라스마트자격증명을활성화합니다. 시작화면이나타나고이어서 QR 코드를스캔하라는메시지가나타납니다.
4. 사용자가데스크톱에부착된스마트카드판독기에카드를삽입합니다. 그러면데스크톱앱에 QR 코드가표시되고사용자에게모바일장치를사용하여코드를스캔하라는메시지가표시됩니다.

   메시지가나타나면사용자가 Secure Hub PIN 을입력합니다.

PIN 인증후 Secure Hub 가인증서를다운로드합니다. 그런다음사용자는메시지에따라등록을완료합니다.

Endpoint Management 콘솔에서장치정보를보려면다음중하나를수행하십시오.

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

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