



# Secure Hub

## Contents

|  |           |
|--|-----------|
| <b>Citrix Secure Hub</b>                       | <b>2</b>  |
| 알려진 문제와 수정된 문제                                 | <b>36</b> |
| 인증 프롬프트 시나리오                                   | <b>39</b> |
| 파생된 자격 증명을 사용하여 장치 등록                          | <b>43</b> |
| <b>Citrix Endpoint Management</b> 콘솔을 통한 힌트 구성 | <b>51</b> |

## Citrix Secure Hub

June 6, 2024

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

Secure Hub 및 기타 구성 요소를 [Citrix Endpoint Management 다운로드 페이지](#)에서 다운로드할 수 있습니다.

Secure Hub 및 모바일 생산성 앱의 기타 시스템 요구 사항은 [시스템 요구 사항](#)을 참조하십시오.

모바일 생산성 앱에 대한 최신 정보는 [최근 발표 내용](#)을 참조하십시오.

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

### 참고:

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

현재 버전의 새로운 기능

### iOS 용 Secure Hub 24.5.0

#### iOS 17 작동 상태 복귀 지원

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

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

이전 버전의 새로운 기능

### Android 용 Secure Hub 24.3.0

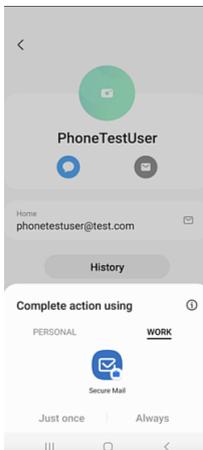
**Samsung Knox 고급 증명 v3 지원** 이제 Secure Hub 에서 Samsung 고급 증명 v3 을 지원하므로 Knox 증명을 활용하여 Citrix Endpoint Management 를 통해 관리되는 Samsung 장치에 대한 보안 조치를 강화할 수 있습니다. 이 고급 증명 프로토콜은 장치의 무결성과 보안 상태를 확인하여 장치가 루팅되지 않고 인증된 펌웨어를 실행하고 있는지 확인합니다. 이 기능은 보안 위협에 대한 필수 보호 계층을 제공하고 기업 보안 정책을 준수하도록 보장합니다.

## Android 용 Secure Hub 23.12.0

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

자세한 내용은 [Knox Platform for Enterprise Key 장치 정책](#)을 참조하십시오.

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



## iOS 용 Secure Hub 24.1.0

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

## Android 용 Secure Hub 23.12.0

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

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

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

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

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

### iOS 용 Secure Hub 23.11.0

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

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

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

nFactor SSO 속성에 대한 자세한 내용은 Citrix Endpoint Management 설명서의 [클라이언트 속성 참조](#)를 참조하십시오.

### Secure Hub 23.10.0

#### Android 용 Secure Hub

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

## Secure Hub 23.9.0

### Android 용 Secure Hub

이 릴리스에서는 전반적인 성능 및 안정성을 개선하는 영역을 다룹니다.

## Secure Hub 23.8.1

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

## Secure Hub 23.8.0

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

## Secure Hub 23.7.0

### Android 용 Secure Hub

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

자세한 내용은 Citrix Endpoint Management 문서의 [Play Integrity API](#)를 참조하십시오.

지원 중단에 대한 자세한 내용은 Citrix Endpoint Management 문서의 [지원 중단 및 제거](#)를 참조하십시오.

Android SafetyNet 기능에 대한 자세한 내용은 [SafetyNet](#)을 참조하십시오.

## Secure Hub 23.4.0

### iOS 용 Secure Hub

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

- 저장소 경험:

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

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

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

- 사용자 인터페이스: 이전에는 로그오프 옵션이 화면 왼쪽 하단에 위치했습니다. 23.4.0 버전에서는 로그오프 옵션이 기본 메뉴의 일부이며 정보 옵션 위에 있습니다.
- 하이퍼링크: 이전에는 앱 정보 페이지의 하이퍼링크가 일반 텍스트로 표시되었습니다. 23.4.0 버전에서는 하이퍼링크를 클릭할 수 있으며 링크를 나타내는 밑줄 서식이 적용됩니다.

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

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

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

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

Android 용 Secure Hub 에는 MAM 애플리케이션의 비활성 타이머 처리 방식을 구성하는 별도의 클라이언트 속성이 있습니다. 자세한 내용은 [Android 의 별도 비활성화 타이머](#)를 참조하십시오.

### Secure Hub 23.4.1

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

### Secure Hub 23.4.0

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

### Secure Hub 23.2.0

#### Android 용 Secure Hub

**참고:**

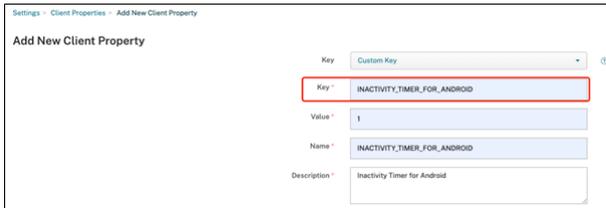
- 유럽 연합 (EU), 유럽 경제 지역 (EEA), 스위스 및 영국의 사용자에 대한 분석 데이터는 수집되지 않습니다.

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

자세한 내용은 Citrix Endpoint Management 설명서의 [지원 중단](#)을 참조하십시오.

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

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



클라이언트 속성을 추가하고 수정하는 방법에 대한 자세한 내용은 XenMobile 설명서의 [클라이언트 속성](#)을 참조하십시오.

## Secure Hub 22.11.0

**Android** 용 **Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

## Secure Hub 22.9.0

**Android** 용 **Secure Hub** 이 릴리스에는 다음이 포함되어 있습니다.

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

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

Android 12 이상 장치의 암호 복잡성은 다음과 같습니다.

- 암호 복잡성 적용: 사용자 지정 암호 요구 사항이 아닌 플랫폼에서 정의한 복잡성 수준의 암호가 필요합니다. Android 12 이상 버전 및 Secure Hub 22.9 이상을 사용하는 장치에만 해당됩니다.
- 복잡성 수준: 사전 정의된 암호 복잡성 수준입니다.
  - 없음: 비밀번호가 필요하지 않습니다.
  - 낮음: 암호는 다음일 수 있습니다.
    - \* 패턴
    - \* 최소 네 개의 숫자로 구성된 PIN
  - 미디어: 암호는 다음일 수 있습니다.

- \* 반복되거나 (4444) 이어지지 (1234) 않는 최소 네 개의 숫자로 이루어진 PIN
- \* 최소 네 자 이상의 알파벳
- \* 최소 네 자 이상의 영숫자
- 높음: 암호는 다음일 수 있습니다.
  - \* 반복되거나 (4444) 이어지지 (1234) 않는 최소 여덟 개의 숫자로 이루어진 PIN
  - \* 최소 여섯 자의 알파벳
  - \* 최소 여섯 자의 영숫자

참고:

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

자세한 내용은 Citrix Endpoint Management 설명서에서 [Android Enterprise 설정](#)을 참조하십시오.

### Secure Hub 22.7.0

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 22.6.0

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 22.5.0

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 22.4.0

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 22.2.0

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

## Secure Hub 21.11.0

### Android 용 Secure Hub

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

## Secure Hub 21.10.0

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

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

## Secure Hub 21.8.0

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

## Secure Hub 21.7.1

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

#### 참고:

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

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

## Secure Hub 21.7.0

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### **Secure Hub 21.6.0**

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### **Secure Hub 21.5.1**

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### **Secure Hub 21.5.0**

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

### **Secure Hub 21.4.0**

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

### **Secure Hub 21.3.2**

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### **Secure Hub 21.3.0**

이 릴리스에는 버그 수정이 포함되어 있습니다.

### **Secure Hub 21.2.0**

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### **Secure Hub 21.1.0**

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 20.12.0

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

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

### Secure Hub 20.11.0

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

### Secure Hub 20.10.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 20.9.0

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

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 20.7.5

#### Android 용 Secure Hub

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

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

## Secure Hub 20.6.5

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

**참고:**

20.6.5 릴리스는 장치 관리자 모드에서 Android 10 을 실행하는 장치의 등록을 차단하지 않습니다.

**iOS 용 Secure Hub** iOS 장치에 구성된 프록시를 활성화합니다. 사용자가 설정 > **Wi-Fi** 에서 구성된 프록시 서버를 사용할 수 있게 하려면 이제 iOS 용 Secure Hub 에서는 새 클라이언트 속성 (**ALLOW\_CLIENTSIDE\_PROXY**) 을 사용 설정해야 합니다. 자세한 내용은 [클라이언트 속성 참조](#)의 **ALLOW\_CLIENTSIDE\_PROXY**에서 참조하십시오.

## Secure Hub 20.3.0

**참고:**

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

## iOS 용 Secure Hub

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

**참고:**

새 사용자에게는 VPN 설치 메시지가 표시되지 않습니다.

- 향상된 등록 프로필 지원. Secure Hub 는 [등록 프로필 지원](#)에서 Citrix Endpoint Management 에 대해 발표한 향상된 등록 프로필 기능을 지원합니다.

## Secure Hub 20.2.0

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 20.1.5

이 릴리스에는 다음이 포함되어 있습니다.

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

### Secure Hub 19.12.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 19.11.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 19.10.5

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

### Secure Hub 19.10.0

이 릴리스에는 버그 수정이 포함되어 있습니다.

### Secure Hub 19.9.5

**iOS 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

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

기능 설정 및 장치 정책 구성 방법에 대한 자세한 내용은 [Keyguard 관리 장치 정책](#)을 참조하십시오.

## Secure Hub 19.9.0

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

**Android 용 Secure Hub** 이 릴리스에는 버그 수정이 포함되어 있습니다.

## Android 용 Secure Hub 19.8.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

## Secure Hub 19.8.0

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

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

## Secure Hub 19.7.5

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

**Android 용 Secure Hub Samsung Knox SDK 3.x.** 지원 Android 용 Secure Hub 가 Samsung Knox SDK 3.x 를 지원합니다. Samsung Knox 3.x 로 마이그레이션하는 방법에 대한 자세한 내용은 Samsung Knox 개발자 설명서를 참조하십시오. 이 릴리스에는 새로운 Samsung Knox 네임스페이스에 대한 지원도 포함되어 있습니다. 이전 Samsung Knox 네임스페이스로 변경하는 방법에 대한 자세한 내용은 [이전 Samsung Knox 네임스페이스 변경 사항](#)에서 참조하십시오.

### 참고:

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

## Secure Hub 19.3.5 ~ 19.6.6

이러한 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

### Secure Hub 19.3.0

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

### Secure Hub 19.2.0

이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

### Secure Hub 19.1.5

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

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

### Secure Hub 19.1.0

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

### Secure Hub 18.12.0

이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

### Secure Hub 18.11.5

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

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

### Secure Hub 18.10.0

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

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

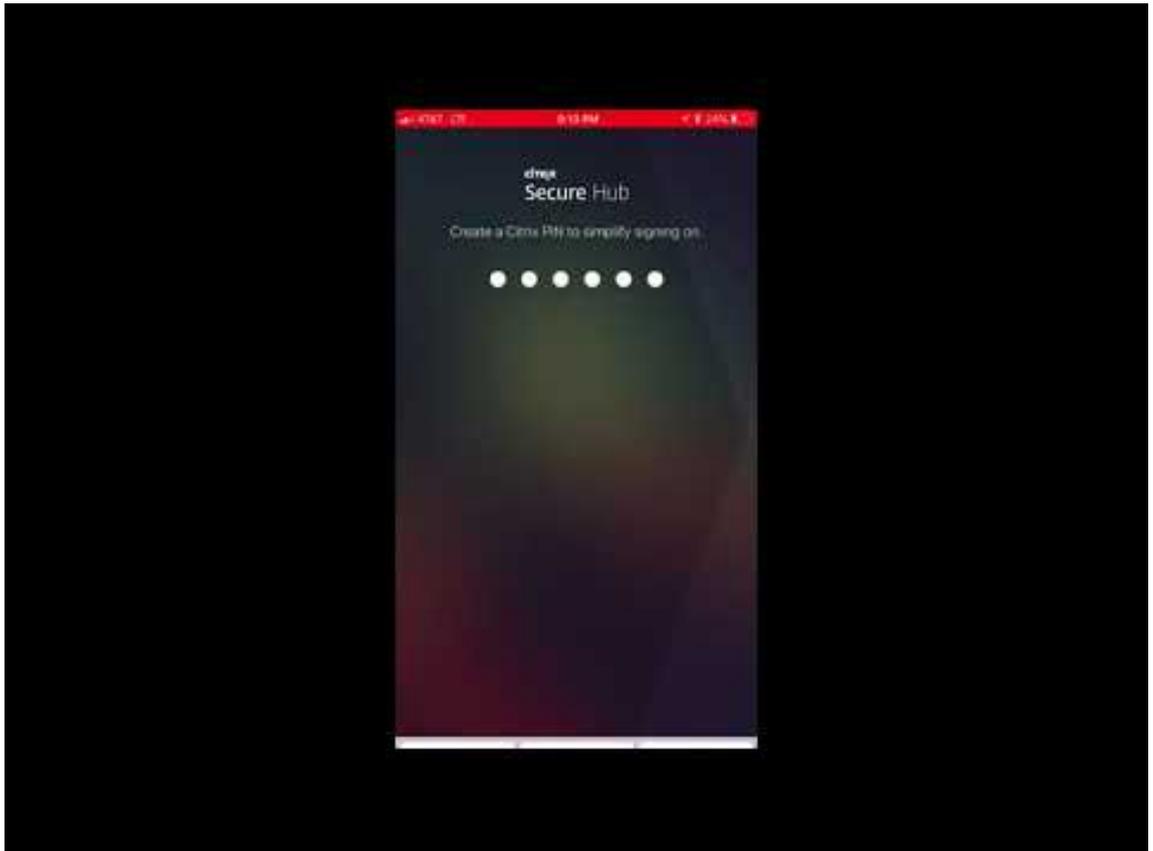
- **Android SafetyNet** 지원: Secure Hub 가 설치된 Android 장치의 호환성 및 보안을 평가하기 위해 **Android SafetyNet** 기능을 사용하도록 Endpoint Management 를 구성할 수 있습니다. 평가 결과를 토대로 장치에 대한 자동화된 작업을 트리거할 수 있습니다. 자세한 내용은 [Android SafetyNet](#)을 참조하십시오.
- **Android Enterprise** 장치의 카메라 사용 제한: 제한 장치 정책의 새로운 카메라 사용 허용 설정을 통해 Android Enterprise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

### Secure Hub 10.8.60 ~ 18.9.0

이러한 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

### Secure Hub 10.8.60

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



**중요:**

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

이 기능을 사용하려면 다음과 같이 구성합니다.

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

**중요:**

이 기능을 사용하도록 설정하면 Citrix Files SSO 가 Endpoint Management(이전 명칭: XenMobile) 대신 Workspace 를 통해 이루어집니다. Workspace 통합 기능을 사용하도록 설정하기 전에 Endpoint Management 콘솔에서 Citrix Files 통합 기능을 사용하지 않도록 설정하는 것이 좋습니다.

### Secure Hub 10.8.55

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

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

**참고:**

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

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

**Secure Hub 10.8.5:** Android 용 Secure Hub 에서 Android Work(Android for Work) 의 COSU 모드가 지원됩니다. 자세한 내용은 [Citrix Endpoint Management 설명서](#)를 참조하십시오.

### Secure Hub 관리

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

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

**중요:**

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

### Citrix PIN

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

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

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

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

### 인증서 고정

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

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

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

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

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

인증서 고정을 사용하려면 Citrix 에 인증서를 Citrix ADS 서버에 업로드해 달라고 요청합니다. [Citrix 지원 포털](#)을 사용하여 기술 지원 사례를 엽니다. 개인 키를 Citrix 에 보내지 않도록 합니다. 이후 다음 정보를 입력합니다.

- 사용자가 등록될 계정을 포함하는 도메인
- Endpoint Management 의 FQDN(정규화된 도메인 이름)
- Endpoint Management 의 인스턴스 이름. 기본적으로 인스턴스 이름은 zdm 이고 대/소문자를 구분합니다.
- 사용자 ID 유형 (UPN 또는 전자 메일일 수 있음). 기본적으로 이 유형은 UPN 입니다.
- iOS 등록에 사용된 포트 (포트 번호를 기본 포트 8443 에서 변경한 경우)
- Endpoint Management 가 연결을 받아들이는 포트 (포트 번호를 기본 포트 443 에서 변경한 경우)

- Citrix Gateway 의 전체 URL.
- 또는 관리자의 전자 메일 주소
- 도메인에 추가할 PEM 형식의 인증서입니다. 이 인증서는 개인 키가 아닌 공개 인증서여야 합니다.
- 기존 서버 인증서를 처리하는 방식: 오래된 서버 인증서가 손상되어 즉시 제거할지 또는 만료될 때까지 오래된 서버 인증서를 계속 지원할지 여부

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

### 인증서 + 일회용 암호 인증

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

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

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

#### 참고:

여러 가지 로그인 유형이 Endpoint Management 및 Citrix ADC 에 설정된 경우, Citrix ADC 구성이 우선합니다. 자세한 내용은 [Citrix Gateway](#) 및 [Endpoint Management](#)를 참조하십시오.

1. Citrix ADC 에서 **Configuration(구성) > AppExpert > Rewrite(다시 쓰기) > Actions(작업)** 로 이동합니다.
2. 추가를 클릭합니다.  
**Create Rewrite Action(다시 쓰기 작업 만들기)** 화면이 나타납니다.
3. 다음 그림과 같이 각 필드를 채우고 **Create(만들기)** 를 클릭합니다.

**Create Rewrite Action**

Name\*  
 ?

Type\*

Use this action type to insert a header.

Header Name\*

Expression Expression Editor

Operators  Saved Policy Expressions  Frequently Used Expressions  Clear

"CertAndRSA"

Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

Create Close

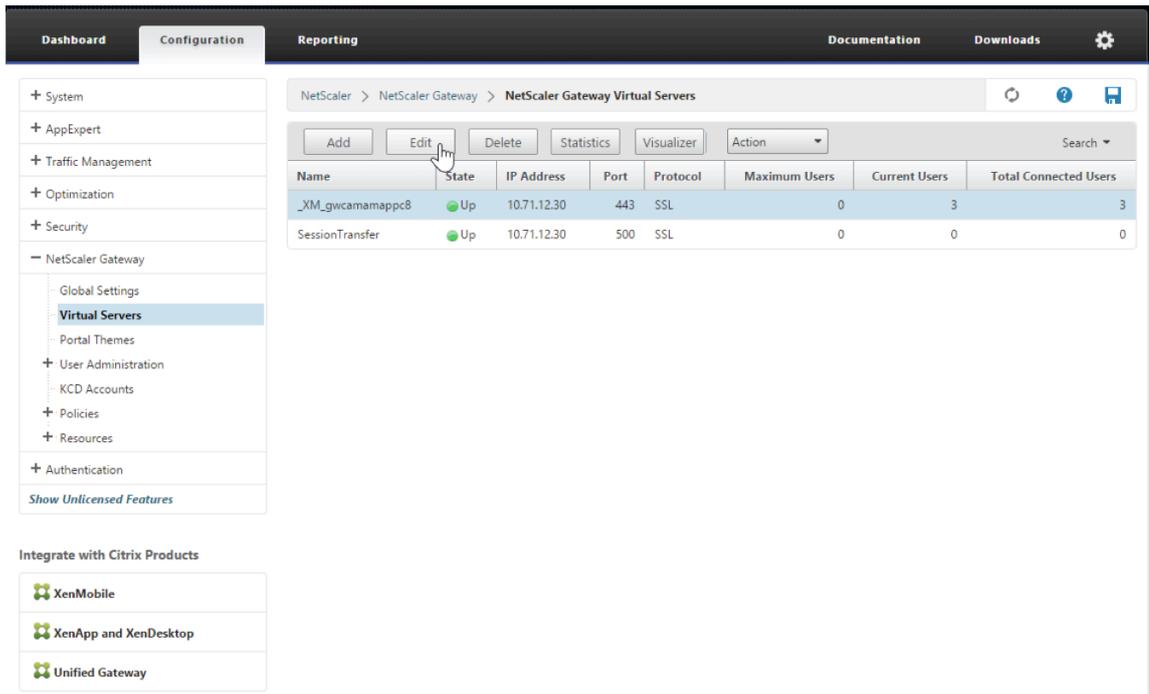
기본 **Rewrite Actions**(다시 쓰기 작업) 화면에 다음 결과가 나타납니다.

NetScaler > AppExpert > Rewrite > Rewrite Actions ↻ ? 📄

Show built-in Rewrite Actions Search ▾

| Name                          | Type               | Target Expression           | Expression  | Pattern                                    |
|-------------------------------|--------------------|-----------------------------|---|--|
| ns_cvpn_sp_js_checkout_rw_act | insert_after_all   | TEXT                        | "\'+window.location.pathname.split(\'\')[1]+\'+wi.. | re~a.substr(0,3).toLowerCase(\\)=\'%2f\'a= |
| InsertGatewayAuthTypeHeader   | insert_http_header | X-Citrix-AM-GatewayAuthType | "CertAndRSA"  |  |

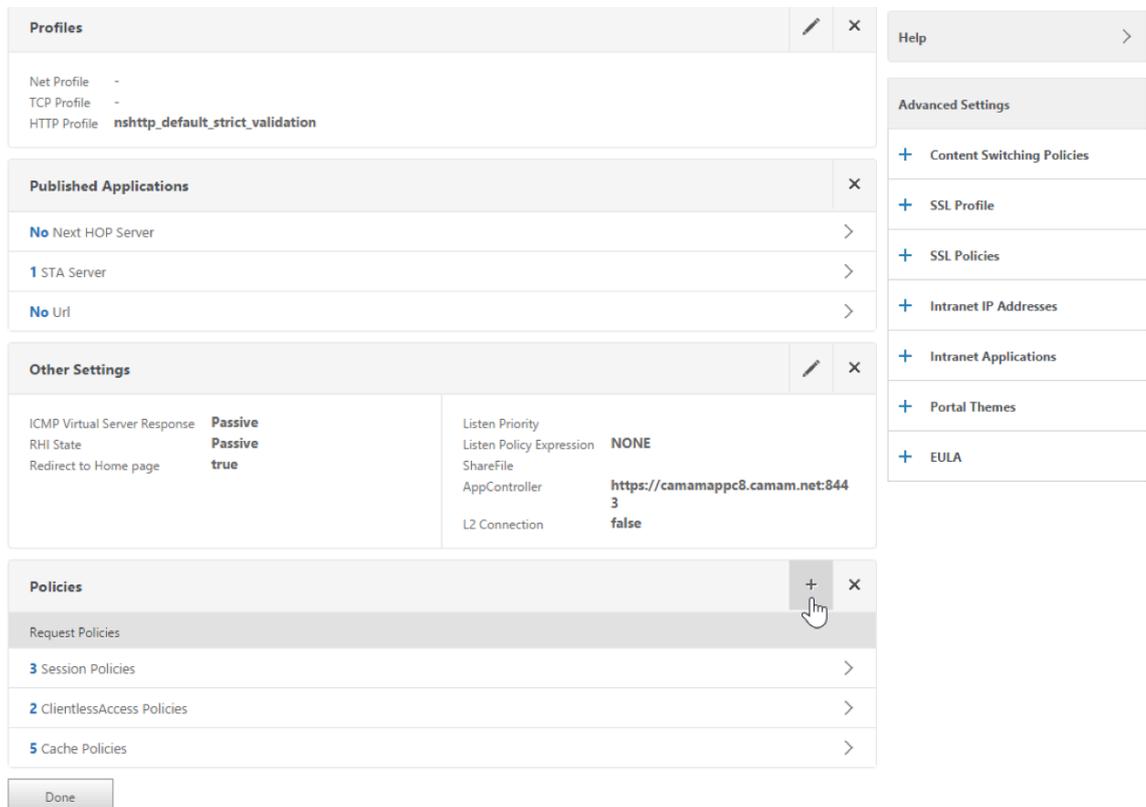
4. 다시 쓰기 작업을 가상 서버에 다시 쓰기 정책으로 바인딩합니다. **Configuration(구성) > NetScaler Gateway > Virtual Servers(가상 서버)** 로 이동한 후, 가상 서버를 선택합니다.



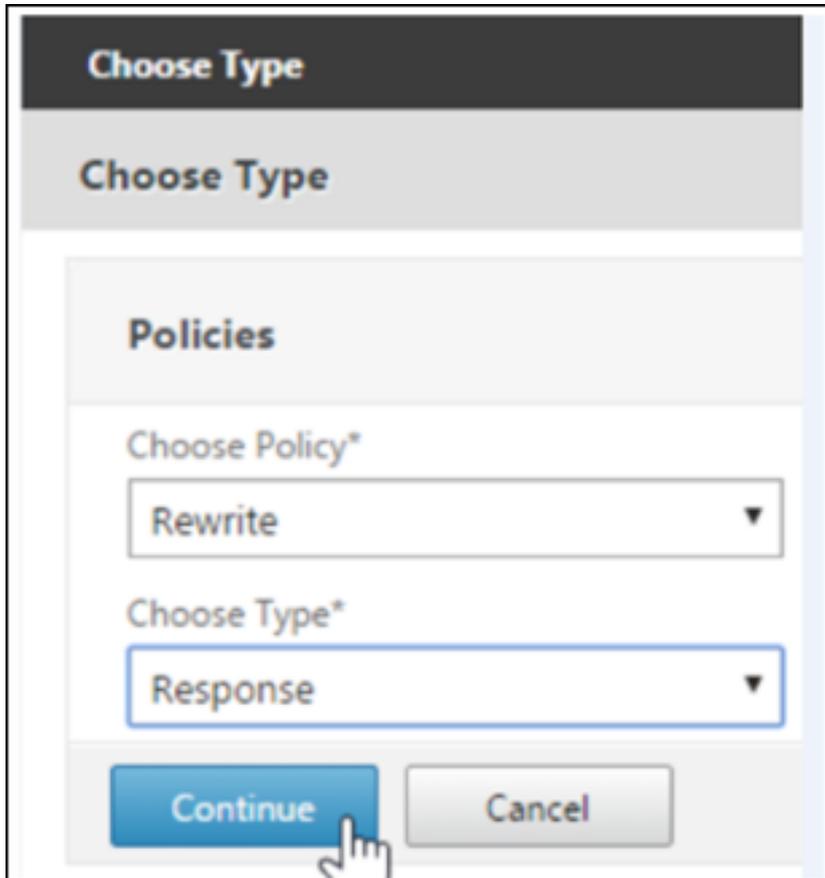
5. 편집을 클릭합니다.

6. **Virtual Servers configuration**(가상 서버 구성) 화면에서 아래로 스크롤하여 **Policies**(정책) 로 이동합니다.

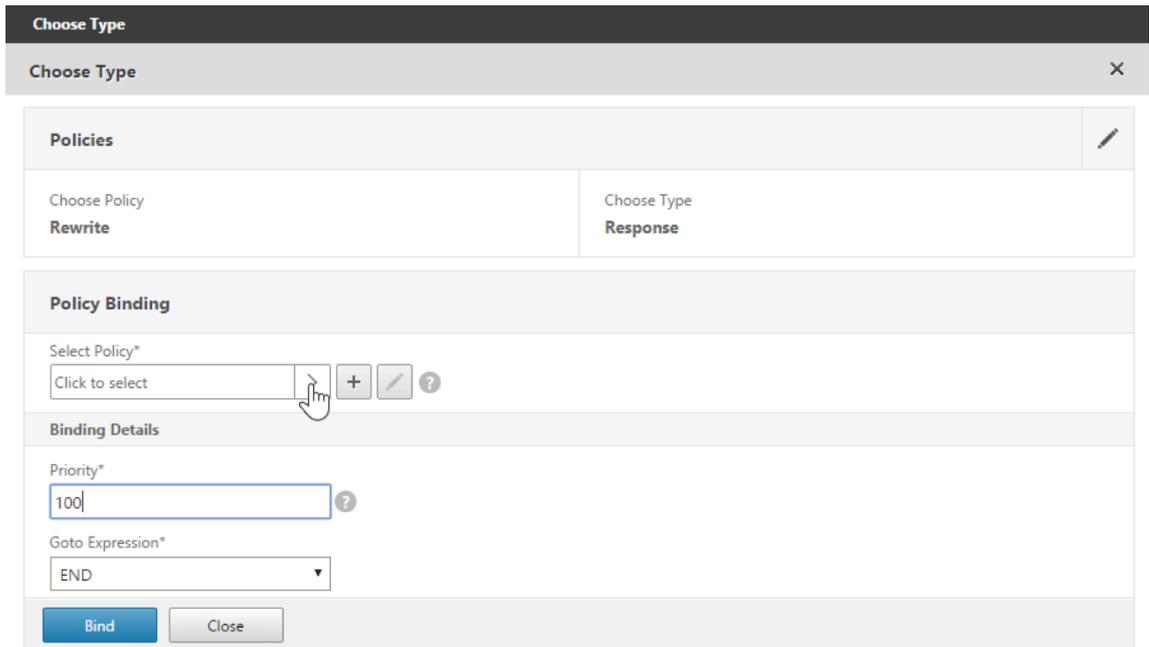
7. + 를 클릭하여 정책을 추가합니다.



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

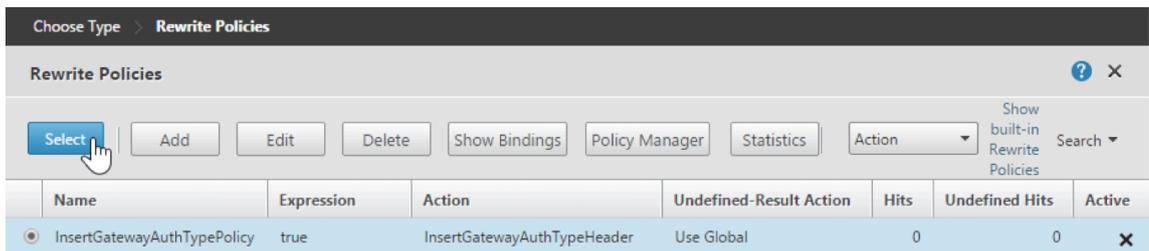


10. **Continue**(계속) 를 클릭합니다.  
**Policy Binding**(정책 바인딩) 섹션이 확장됩니다.

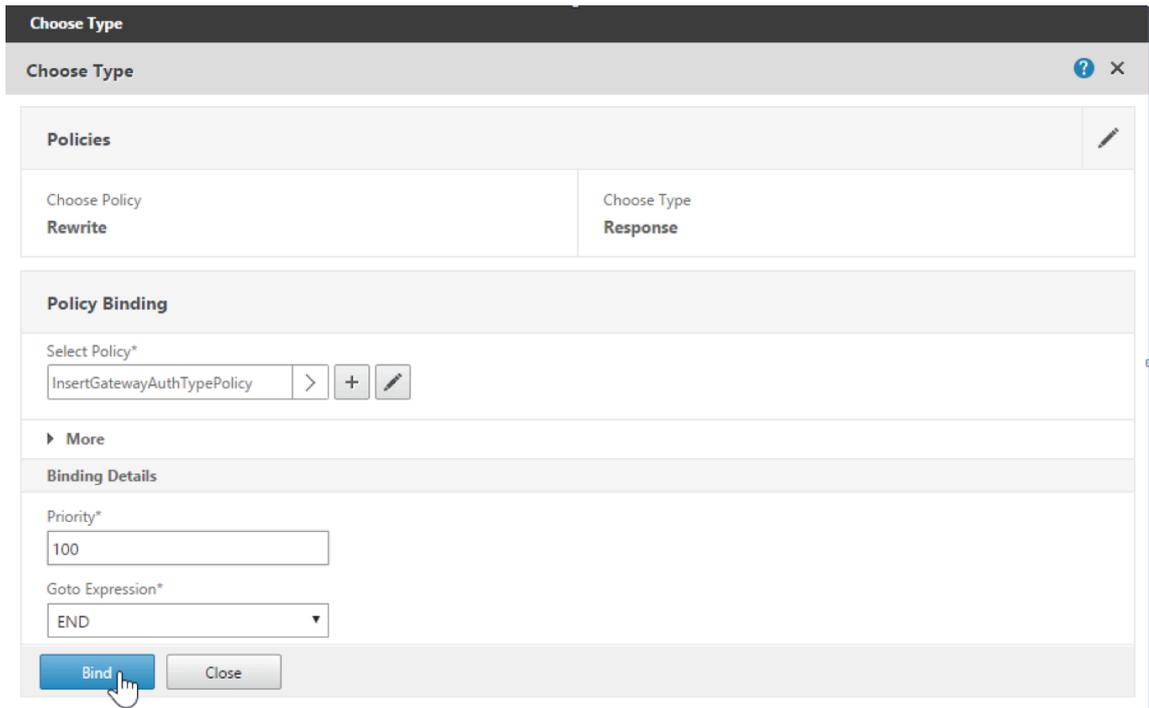


11. **Select Policy**(정책 선택) 를 클릭합니다.

사용 가능한 정책을 포함하는 화면이 나타납니다.

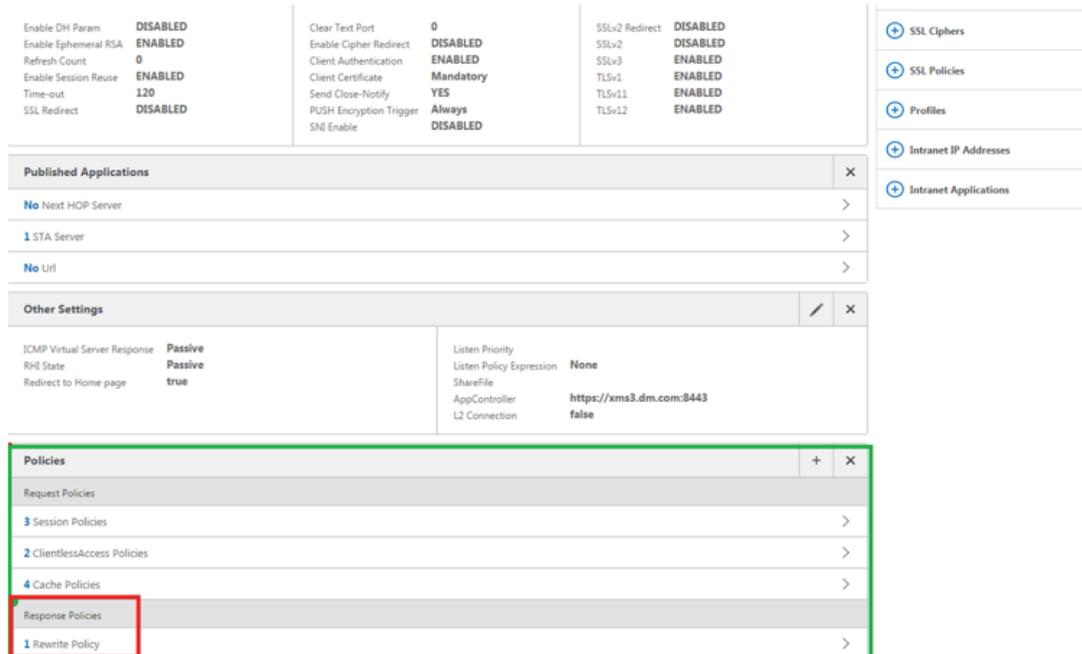


12. 앞에서 생성한 정책의 행을 클릭한 후 **Select**(선택) 를 클릭합니다. 선택한 정책이 채워진 채로 **Policy Binding**(정책 바인딩) 화면이 다시 나타납니다.

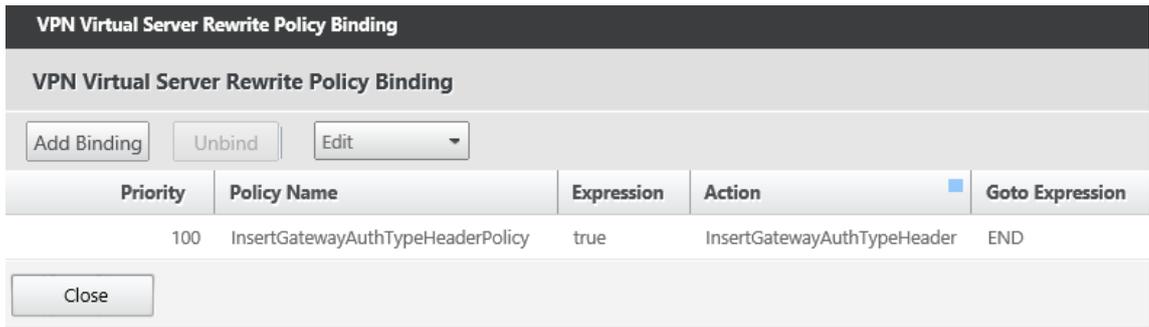


13. **Bind**(바인딩) 를 클릭합니다.

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



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



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

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

**필수 구성 요소:**

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

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

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

| FQDN                                       | IP 주소       | 포트  | IP 및 포트 사용          |
|--|-------------|-----|---------------------|
| <a href="#">discovery.mdm.zenprise.com</a> | 52.5.138.94 | 443 | Secure Hub - ADS 통신 |
| <a href="#">discovery.mdm.zenprise.com</a> | 52.1.30.122 | 443 | Secure Hub - ADS 통신 |

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

인증서 고정이 사용 설정된 경우:

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

참고:

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

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

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

계정 삭제 옵션 비활성화

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

계정 삭제 옵션을 사용 중지하려면 다음 단계를 수행하십시오.

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

### Secure Hub 사용

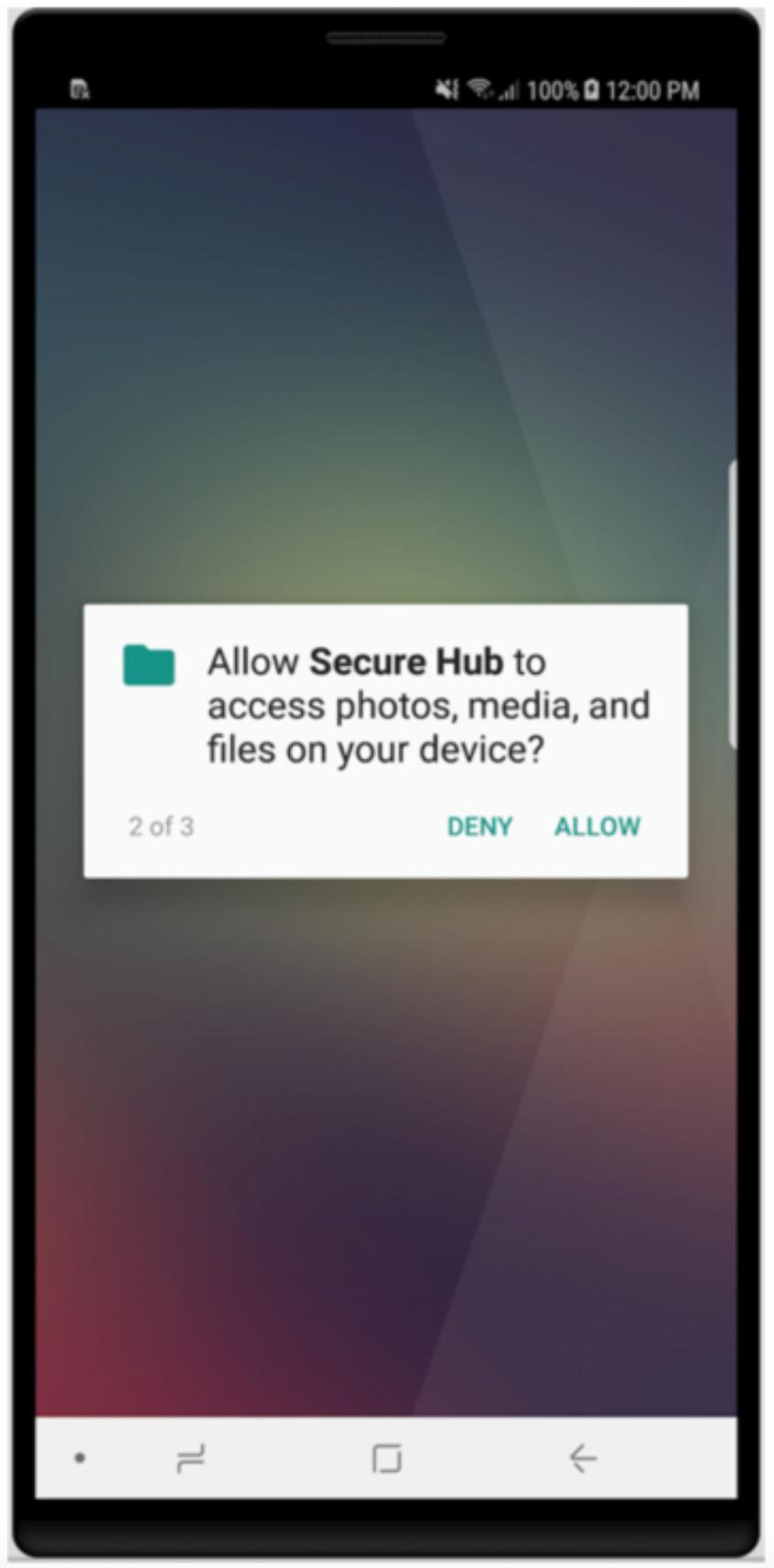
사용자는 먼저 Apple 또는 Android 스토어에서 장치로 Secure Hub 를 다운로드합니다.

Secure Hub 가 열리면 사용자는 회사에서 제공한 자격 증명을 입력하여 Secure Hub 에 장치를 등록합니다. 장치 등록에 대한 자세한 내용은 [사용자](#), [계정](#), [역할 및 등록](#)을 참조하십시오.

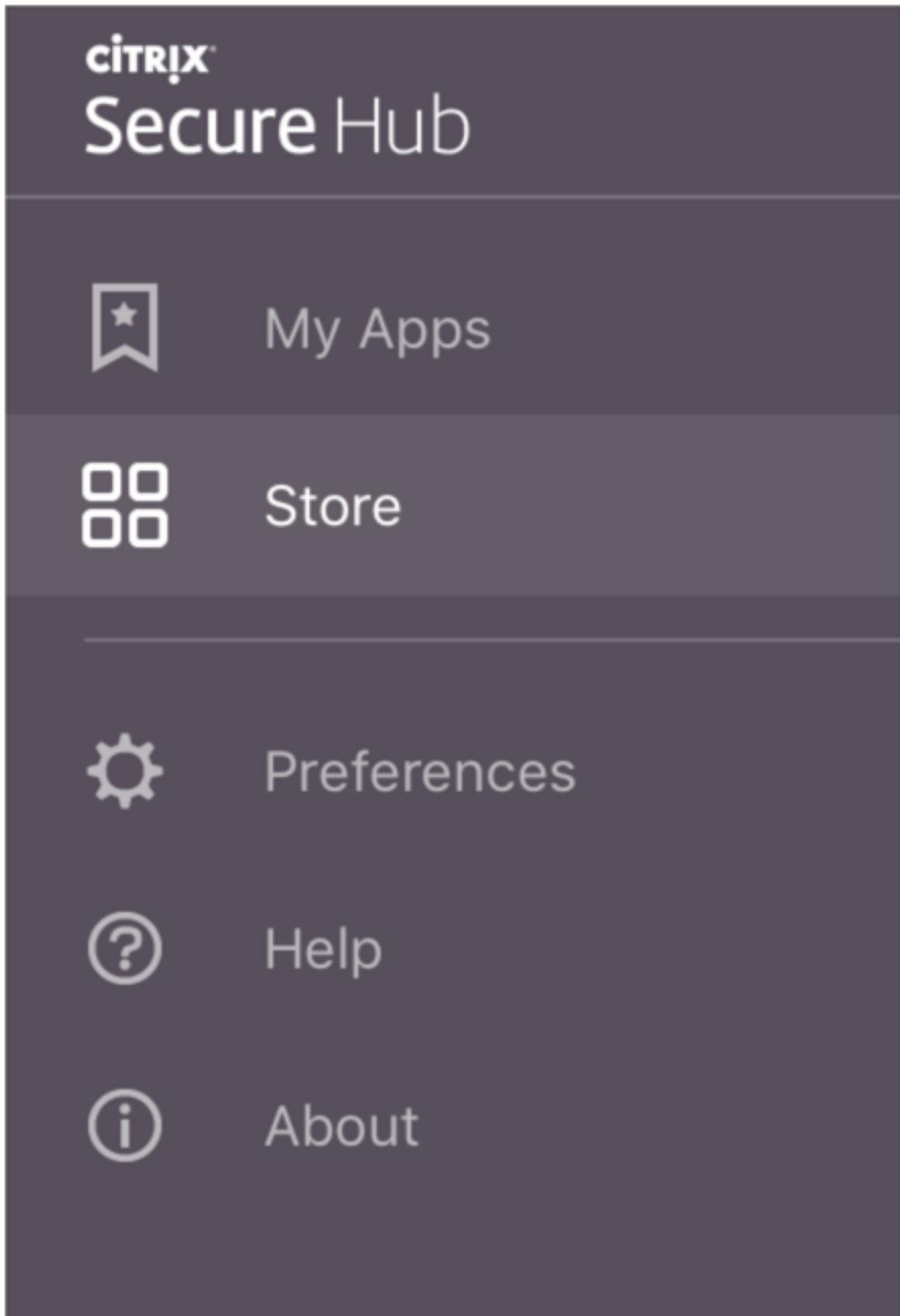
Android 용 Secure Hub 에서 초기 설치 및 등록 시 다음 메시지가 나타납니다. “Allow Secure Hub to access photos, media, and files on your device?(Secure Hub 가 장치의 사진, 미디어 및 파일에 액세스하도록 허용하시겠습니까?)”

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

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



태블릿에서는 저장소가 별도 탭입니다.



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

### Secure Mail 에 자동 등록

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

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

이 기능을 사용 설정하려면 다음 세 가지 속성을 생성합니다.

- 서버 속성 MAM\_MACRO\_SUPPORT. 지침은 [서버 속성](#)을 참조하십시오.
- 클라이언트 속성 ENABLE\_CREDENTIAL\_STORE 및 SEND\_LDAP\_ATTRIBUTES. 지침은 [클라이언트 속성](#)을 참조하십시오.

### 사용자 지정된 스토어

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

Settings > Client Branding

### Client Branding

You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.

Store name\*  ⓘ

Default store view

Category

A-Z

Device

Phone

Tablet

Branding file

**Note:**

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
- A .zip file should be created from the files, not a folder with the files inside of it.

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

Device Policies > Apps > App Information

### MDX

#### App Information

1 App Information

2 Platform

iOS

Android

Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Name\*  ⓘ

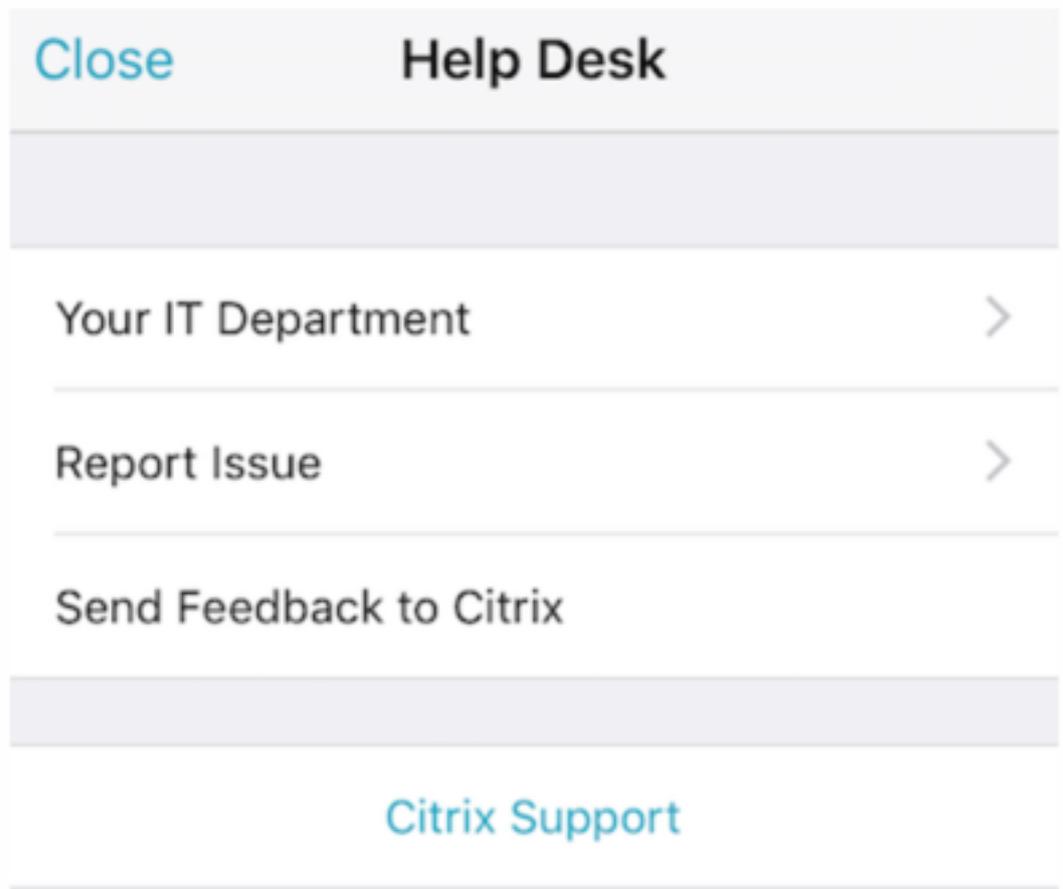
Description

App category

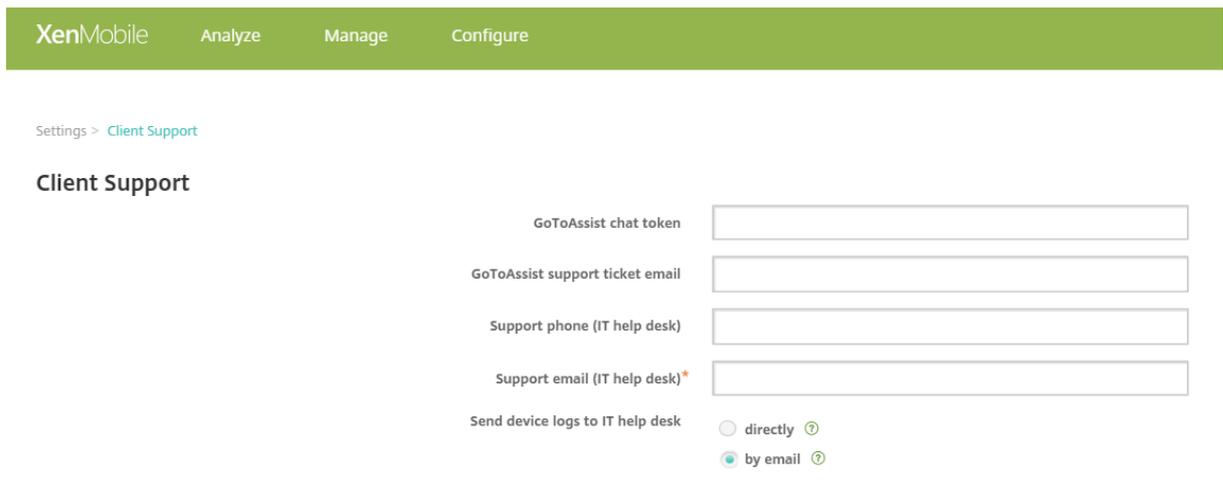
스토어에서 사용자는 Endpoint Management 에서 구성되고 보안된 앱 및 데스크톱만 찾아볼 수 있습니다. 앱을 추가하려면 사용자가 세부 정보를 누른 후 추가를 누릅니다.

#### 구성된 도움말 옵션

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



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



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

할 수 있습니다.

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

사용자는 **Citrix** 지원을 눌러 [Citrix Knowledge Center](#)를 열 수도 있습니다. 여기에서 모든 Citrix 제품에 대한 지원 문서를 검색할 수 있습니다.

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

### 위치 정책

또한 Secure Hub 는 회사 소유 장치가 특정 지리적 경계선을 벗어나지 못하게 하려는 경우 등에 지역 위치 및 지역 추적 정책을 제공합니다. 자세한 내용은 [위치 장치 정책](#)을 참조하십시오.

### 충돌 수집 및 분석

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

iOS 및 Android 에서 사용할 수 있는 추가 기능은 [Citrix Secure Hub](#)의 플랫폼별 기능 매트릭스를 참조하십시오.

### Secure Hub 의 장치 측 로그 생성

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

Secure Mail 로그를 획득하려면 다음을 수행하십시오.

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

- CtxLog\_AppInfo.txt(iOS), Device\_And\_AppInfo.txt(Android), logx.txt 및 WH\_logx.txt(Windows Phone)

앱 정보 로그에는 장치 및 앱에 대한 정보가 포함됩니다.

## 알려진 문제와 수정된 문제

June 6, 2024

Citrix에서는 이전 두 버전의 모바일 생산성 앱의 업그레이드를 지원합니다.

### **iOS 용 Secure Hub 24.5.0**

수정된 문제

이 릴리스에는 수정된 문제가 없습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

### **Android 용 Secure Hub 24.3.0**

수정된 문제

사용자는 공장 초기화에 대한 제한 정책이 NO로 설정된 경우에도 회사 소유의 Android Enterprise 장치에서 공장 초기화를 수행할 수 있습니다. 이 문제는 사용자가 Secure Hub를 다시 시작하는 경우에 발생합니다. [XMHELP-4479]

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

### **iOS 용 Secure Hub 24.1.0**

수정된 문제

- Palera1n 앱을 사용하여 iOS 장치를 탈옥할 때 Citrix Endpoint Management 서버는 해당 장치를 탈옥된 것으로 감지하지 못합니다. 따라서 Endpoint Management 서버는 탈옥 장치를 공장 초기화할 수 없습니다. 또한 Endpoint Management 서버는 서버 콘솔에서 탈옥 장치 항목을 지울 수 없습니다. [XMHELP-4397]

- MAM SDK 를 사용하여 iOS 앱을 관리할 때 Secure Hub 스토어에 다음 문제 중 하나가 발생합니다.
  - 앱에 대한 업데이트가 있을 때는 알림을 보내지 않습니다.
  - 앱이 업데이트된 후에도 지속적으로 업데이트에 대해 알려줍니다.

[XMHELP-4427]

- MAM SDK 를 사용하여 iOS 앱을 관리할 때 다음과 같은 규정 준수 알림이 표시될 수 있습니다.

“이 앱은 계정에서 삭제되었습니다. 장치에서 제거할 수 있습니다. “

이 문제는 MAM SDK 와 MDX 툴킷을 모두 동일한 iOS 장치에 설치할 때 발생합니다. [XMHELP-4463]

### **Android 용 Secure Hub 23.12.0**

수정된 문제

Citrix Gateway 자격 증명이 만료되면 Secure Hub 가 Citrix Gateway 서버에 연결하기 위한 새 인증서를 생성하지 못할 수 있습니다. 따라서 Secure Hub 가 시작되지 않고 다음 오류 메시지가 표시됩니다.

“연결에 오류가 발생했습니다. 다시 연결을 시도해 보십시오.”

[XMHELP-4446]

### **iOS 용 Secure Hub 23.11.0**

수정된 문제

- Citrix Gateway 클라이언트 인증서는 만료되어도 자동으로 갱신되지 않기 때문에 iOS 장치에서는 Secure Hub 인증이 실패합니다. 이 문제는 Citrix Gateway 가 TLSv1.3 프로토콜을 사용할 때 발생합니다. [XMHELP-4396]
- Citrix Gateway 를 통해 Secure Hub 에 로그인하면 다음과 같은 오류 메시지가 나타날 수 있습니다.

“로그인할 수 없습니다. 자격 증명이 잘못되었습니다. 세션을 종료합니다.”

이 문제는 nFactor 를 사용하여 iOS 장치를 Citrix Endpoint Management(CEM) 에 등록할 때 발생합니다.

[XMHELP-4423]

### **Android 용 Secure Hub 23.10.0**

수정된 문제

Android 버전 11 이상에서는 Android Enterprise 장치의 Wi-Fi 정책이 배포되지 않을 수 있습니다. 이 문제는 Wi-Fi 정책의 익명 필드에 도메인 값이 지정되지 않은 경우 발생합니다. [XMHELP-4379]

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

**Android 용 Secure Hub 23.9.0**

수정된 문제

이 릴리스에서는 전반적인 성능 및 안정성을 개선하는 영역을 다룹니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

**iOS 용 Secure Hub 23.8.1**

수정된 문제

- 사용자가 Secure Hub 23.8.0 을 사용하여 장치를 등록하려고 할 때 사용자 이름 형식 (sAMAccount) 이 같으면 프로세스가 실패하고 다음 오류 메시지가 표시될 수 있습니다.

“등록에 실패했습니다. MAM 에 로그인한 사용자가 등록된 사용자와 일치하지 않습니다. 다시 등록해 보십시오.”  
[XMHELP-4410]

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

**iOS 용 Secure Hub 23.8.0**

수정된 문제

- nFactor 를 사용하여 Citrix Endpoint Management(CEM) 에 iOS 장치를 등록하면 마이크로 VPN 터널을 설정하는 데 문제가 발생할 수 있습니다. [XMHELP-4390]

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

### 이전 버전의 알려진 문제 및 수정된 문제

이전 버전의 Secure Hub 에 대한 알려진 문제와 수정된 문제는 [Secure Hub 의 알려진 문제 및 수정된 문제에 대한 기록](#)을 참조하십시오.

### 인증 프롬프트 시나리오

November 1, 2022

장치에서 자격 증명을 입력하여 Secure Hub 에 인증하라는 메시지가 다양한 시나리오에서 사용자에게 표시됩니다.

시나리오는 다음과 같은 요인에 따라 달라집니다.

- Endpoint Management 콘솔 설정의 MDX 앱 정책 및 클라이언트 속성 구성
- 인증이 오프라인 또는 온라인으로 이루어지는지 여부 (장치가 Endpoint Management 로의 네트워크 연결을 필요로 함)

또한 사용자가 입력하는 자격 증명의 종류 (Active Directory 암호, Citrix PIN 또는 암호, 일회용 암호, 지문 인증 (iOS 에서 일명 Touch ID)) 도 인증 유형 및 인증 빈도에 따라 달라집니다.

인증 프롬프트가 표시되는 시나리오부터 살펴보겠습니다.

- 장치 다시 시작: 사용자가 장치를 다시 시작하면 Secure Hub 에서 재인증해야 합니다.
- 오프라인 비활성화 (시간 제한): 앱 암호 MDX 정책이 기본적으로 사용하도록 설정된 경우 비활성화 타이머라는 Endpoint Management 클라이언트 속성이 작동하게 됩니다. 비활성화 타이머는 보안 컨테이너를 사용하는 앱에서 사용자 활동 없이 경과할 수 있는 시간의 길이를 제한합니다.

비활성화 타이머가 만료되면 사용자는 장치에서 보안 컨테이너에 인증해야 합니다. 예를 들어 사용자가 장치를 내려 놓고 떠나간 경우 비활성화 타이머가 만료되면 다른 사람이 해당 장치를 주워서 컨테이너 내의 민감한 데이터에 액세스할 수 없습니다. 비활성화 타이머 클라이언트 속성은 Endpoint Management 콘솔에서 설정합니다. 기본값은 15 분입니다. 앱 암호를 커짐으로 설정하고 비활성화 타이머 클라이언트 속성이 작동하면 대부분의 일반적인 인증 프롬프트 시나리오에 대응할 수 있습니다.

- **Secure Hub** 에서 로그오프: 사용자가 Secure Hub 에서 로그오프하는 경우 사용자는 다음번에 Secure Hub 또는 MDX 앱에 액세스할 때 앱 암호 MDX 정책 및 비활성화 타이머 상태에 의해 앱에서 암호를 요구하면 다시 인증해야 합니다.
- 최대 오프라인 기간: 이 시나리오는 앱별 MDX 정책으로 구동되는 개별 앱에 관한 것입니다. 최대 오프라인 기간 MDX 정책의 기본 설정은 3 일입니다. Secure Hub 에 온라인으로 인증하지 않고 앱이 실행될 수 있는 기간이 경과하면 앱 권한 확인 및 정책 새로 고침을 위해 Endpoint Management 체크인이 필요합니다. 이 체크인이 발생하면 앱이 온라인 인증을 위해 Secure Hub 를 트리거합니다. MDX 앱에 액세스하려면 먼저 사용자가 재인증해야 합니다.

최대 오프라인 기간과 활성 폴링 기간 MDX 정책 간의 관계에 유의하십시오.

- 활성 풀링 기간은 앱 잠금, 앱 초기화 등의 보안 작업을 수행하기 위해 앱이 Endpoint Management 에 체크인하는 간격입니다. 또한 앱은 업데이트된 앱 정책이 있는지 확인합니다.
- 활성 풀링 기간 정책을 통해 성공적으로 정책을 확인한 후에 최대 오프라인 기간 타이머가 재설정되고 다시 카운트를 시작합니다.

활성 풀링 기간 및 최대 오프라인 기간 만료의 경우 Endpoint Management 에 체크인하려면 장치에서 유효한 Citrix Gateway 토큰이 필요합니다. 유효한 Citrix Gateway 토큰이 장치에 있는 경우, 앱은 사용자를 방해하지 않으면서 Endpoint Management 에서 새 정책을 가져옵니다. 앱에서 Citrix Gateway 토큰이 필요하다면 Secure Hub 로 전환되고 Secure Hub 에서는 인증 프롬프트가 사용자에게 표시됩니다.

Android 장치에서는 Secure Hub 활동 화면이 현재 앱 화면 바로 위에 열립니다. 하지만 iOS 장치에서는 Secure Hub 가 포그라운드로 전환되어야 하므로 현재 앱이 일시적으로 사라집니다.

사용자가 자격 증명을 입력한 후에 Secure Hub 는 다시 원래 앱으로 전환됩니다. 이 경우 캐싱된 Active Directory 자격 증명을 허용하거나 클라이언트 인증서가 구성되어 있으면 사용자가 PIN, 암호 또는 지문 인증을 입력할 수 있습니다. 그렇지 않은 경우, 사용자는 완전한 Active Directory 자격 증명을 입력해야 합니다.

다음 Citrix Gateway 정책 목록에 설명된 Citrix Gateway 세션 비활성 또는 강제 세션 시간 제한 정책으로 인해 Citrix ADC 토큰이 유효하지 않게 될 수 있습니다. 사용자가 Secure Hub 에 다시 로그인하면 앱을 계속 실행할 수 있습니다.

- **Citrix Gateway 세션 정책:** 두 가지 Citrix Gateway 정책은 사용자에게 인증 프롬프트가 표시되는 시점에도 영향을 줍니다. 이러한 경우 사용자는 Endpoint Management 에 연결할 수 있도록 Citrix ADC 와의 온라인 세션을 만들기 위해 인증합니다.
  - 세션 시간 초과: 설정된 기간 동안 네트워크 활동이 발생하지 않으면 Endpoint Management 에 대한 Citrix ADC 세션이 연결 해제됩니다. 기본값은 30 분입니다. Citrix Gateway 마법사를 이용해 정책을 구성하는 경우에는 기본값이 1440 분입니다. 시간 제한을 넘기면 회사 네트워크에 다시 연결하라는 인증 프롬프트가 사용자에게 표시됩니다.
  - 강제 시간 제한: 꺼짐인 경우, 강제 시간 제한 기간이 경과한 후에 Endpoint Management 에 대한 Citrix ADC 세션이 연결 해제됩니다. 강제 시간 제한은 설정된 기간 이후에 재인증이 필수로 수행되도록 합니다. 다음에 사용할 때 회사 네트워크에 재연결하기 위해 인증 프롬프트가 사용자에게 표시됩니다. 기본값은 꺼짐입니다. Citrix Gateway 마법사를 이용해 정책을 구성하는 경우에는 기본값이 1440 분입니다.

### 자격 증명 유형

앞의 섹션에서는 사용자에게 인증 프롬프트가 표시되는 시점에 대해 설명했습니다. 이 섹션에서는 사용자가 입력해야 하는 자격 증명의 종류를 살펴봅니다. 장치에서 암호화된 데이터에 대한 액세스 권한을 얻으려면 다양한 인증 방법을 통한 인증이 필요합니다. 처음에 장치를 잠금 해제하려면 기본 컨테이너를 잠금 해제합니다. 그런 후에 컨테이너가 다시 보안되면 액세스 권한을 다시 얻기 위해 보조 컨테이너를 잠금 해제합니다.

참고:

관리되는 앱이라는 용어는 MDX Toolkit 에 의해 래핑된 앱을 가리킵니다. 앱 암호 MDX 정책은 기본적으로 사용하도록 설정된 상태로 그대로 두고 비활성화 타이머 클라이언트 속성을 사용합니다.

자격 증명 유형을 결정하는 상황은 다음과 같습니다.

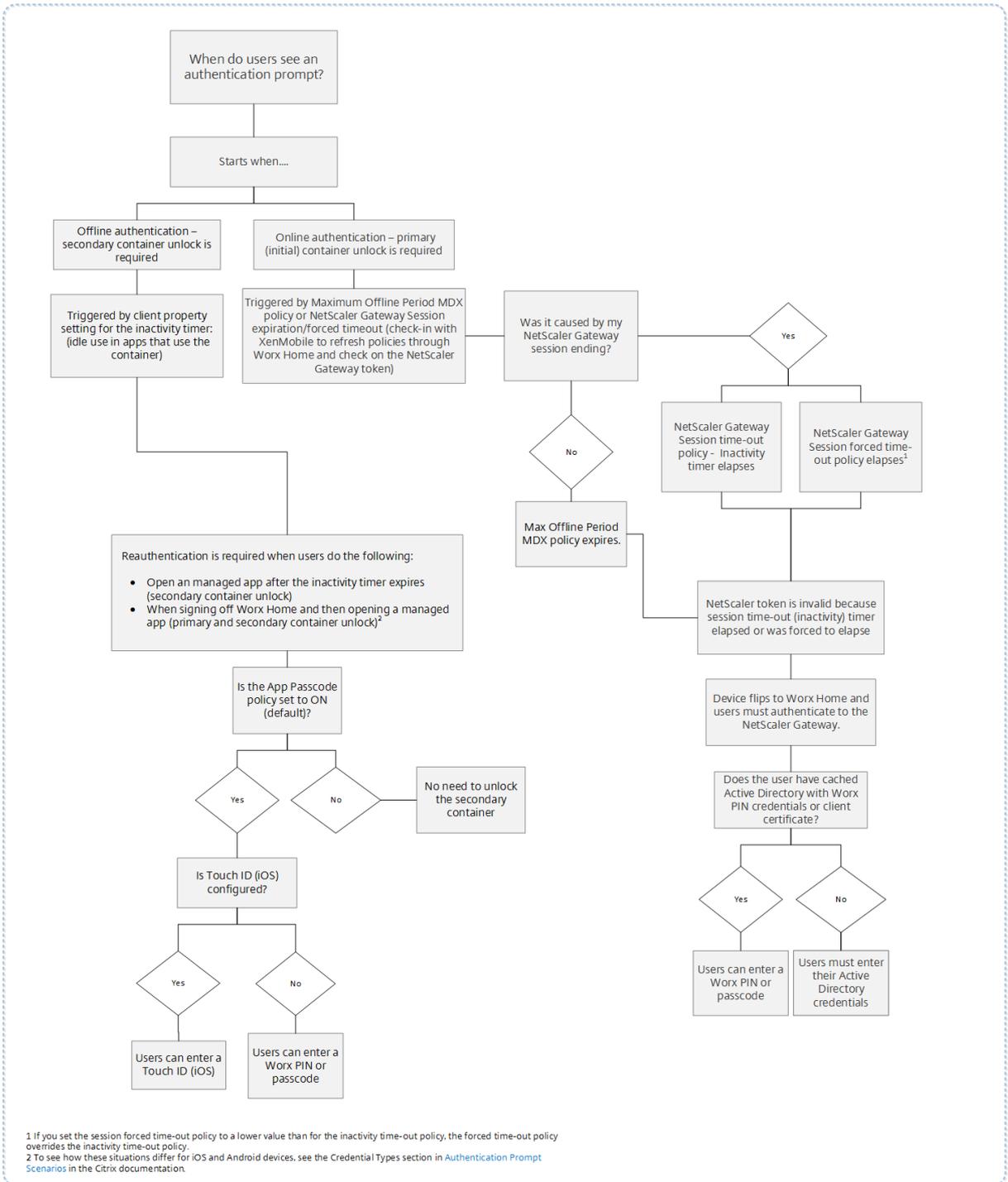
- 기본 컨테이너 잠금 해제: 기본 컨테이너를 잠금 해제하려면 Active Directory 암호, Citrix PIN 또는 암호, 일회용 암호, Touch ID 또는 지문 ID 가 필요합니다.
  - iOS 에서 앱이 장치에 설치된 후 사용자가 Secure Hub 또는 관리되는 앱을 처음 여는 경우
  - iOS 에서 사용자가 장치를 재시작한 후, Secure Hub 를 여는 경우
  - Android 에서 Secure Hub 가 실행 중이 아닐 때 사용자가 관리되는 앱을 여는 경우
  - Android 에서 장치 재시작 등의 이유로 인해 Secure Hub 를 재시작하는 경우
- 보조 컨테이너 잠금 해제: 보조 컨테이너를 잠금 해제하려면 지문 인증 (구성된 경우), Citrix PIN 또는 암호, Active Directory 자격 증명이 필요합니다.
  - 비활성화 타이머 만료 이후 사용자가 관리되는 앱을 여는 경우
  - 사용자가 Secure Hub Hub 에서 로그오프한 다음 관리되는 앱을 여는 경우

다음 조건에 해당할 경우 두 가지 컨테이너 잠금 해제 상황에 대해 Active Directory 자격 증명이 필요합니다.

- 사용자가 Corporate 계정에 연결된 암호를 변경하는 경우
- Endpoint Management 콘솔에서 Citrix PIN(ENABLE\_PASSCODE\_AUTH 및 ENABLE\_PASSWORD\_CACHING) 을 사용하도록 클라이언트 속성을 설정하지 않은 경우
- 장치가 자격 증명을 캐싱하지 않거나 장치에 클라이언트 인증서가 없을 때 NetScaler Gateway 세션이 종료되는 경우 (세션 시간 제한 또는 강제 시간 제한 정책 타이머가 만료될 때 종료됨)

지문 인증을 사용 설정하면 사용자는 앱이 비활성화되어 오프라인 인증이 필요한 경우에 지문을 사용하여 로그인할 수 있습니다. 사용자가 Secure Hub 에 처음 로그인할 때와 장치를 다시 시작할 때에는 여전히 PIN 을 입력해야 합니다. 지문 인증 사용에 대한 자세한 내용은 [지문 또는 Touch ID 인증](#)을 참조하십시오.

다음 순서도에는 인증 프롬프트가 표시될 때 사용자가 입력해야 하는 자격 증명을 결정하는 흐름이 요약되어 있습니다.



### Secure Hub 화면 전환 정보

앱에서 Secure Hub 로 전환된 후 다시 앱으로 전환되어야 하는 상황에도 유의해야 합니다. 전환 과정에서 사용자가 확인해야 할 알림이 표시됩니다. 이 경우 인증은 필요하지 않습니다. 이 상황은 최대 오프라인 기간 및 활성 폴링 기간 MDX 정책에 의해 지정된 대로 Endpoint Management 에 체크인하고 Secure Hub 를 통해 장치에 푸시되어야 하는 업데이트된 정책을

Endpoint Management 가 감지한 후에 발생합니다.

### 장치 암호의 암호 복잡성 (**Android 12+**)

사용자 지정 암호 요구 사항보다 복잡한 암호가 선호됩니다. 암호 복잡성 수준은 사전 정의된 수준 중 하나입니다. 따라서 최종 사용자는 복잡도 수준이 낮은 암호를 설정할 수 없습니다.

Android 12 이상 기기의 암호 복잡성은 다음과 같습니다.

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

#### 참고:

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

자세한 내용은 Citrix Endpoint Management 설명서에서 [Android Enterprise 설정](#)을 참조하십시오.

### 파생된 자격 증명을 사용하여 장치 등록

January 25, 2019

파생된 자격 증명은 모바일 장치를 위한 강력한 인증을 제공합니다. 이 자격 증명은 스마트 카드로부터 파생되어 카드가 아닌 모바일 장치에 상주합니다. 스마트 카드는 PIV(Personal Identity Verification) 카드 또는 CAC(Common Access Card)입니다.

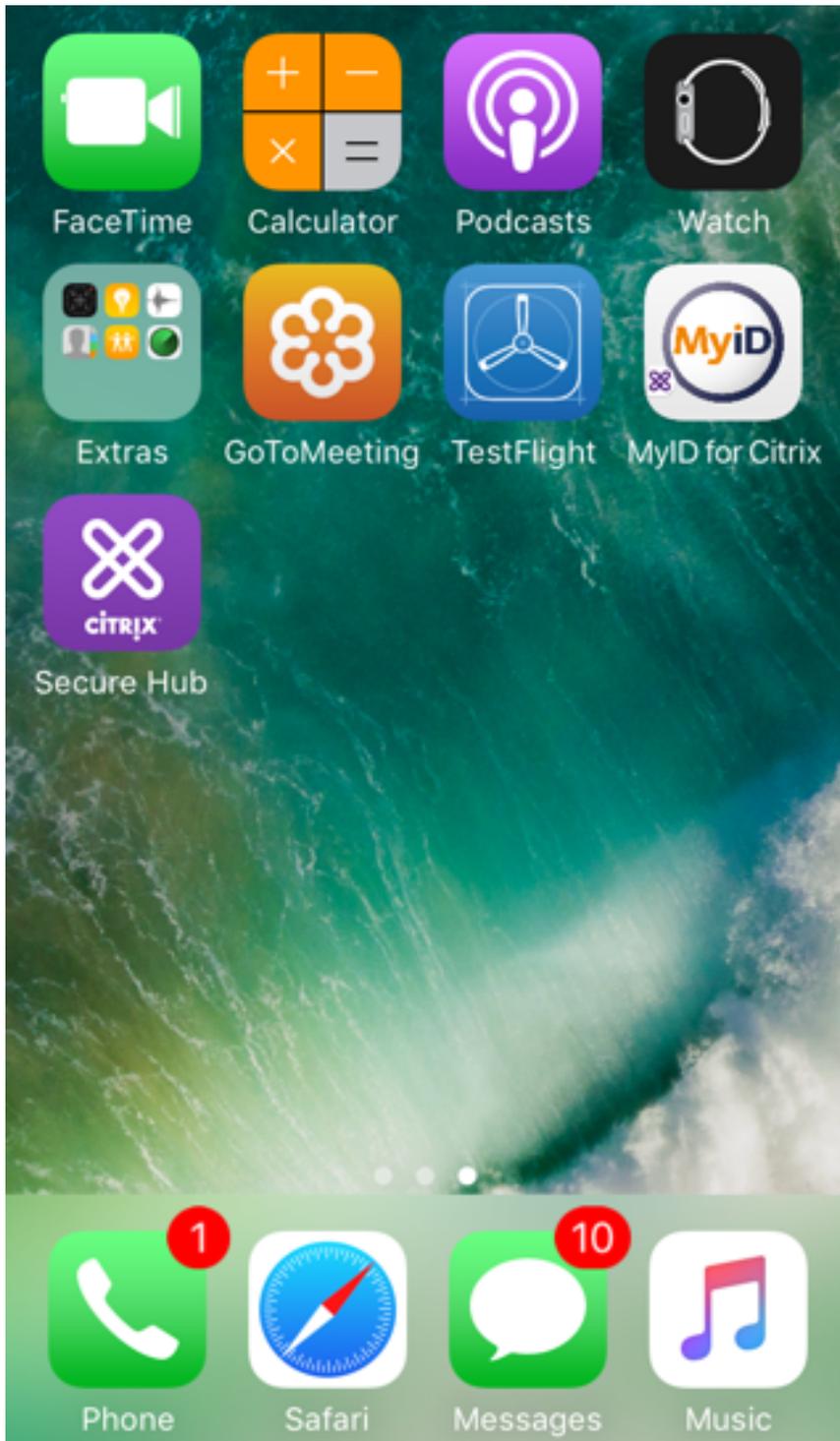
파생된 자격 증명은 UPN 같은 사용자 식별자가 포함된 등록 인증서입니다. Endpoint Management 는 자격 증명 공급자로부터 받은 자격 증명을 장치의 보안 저장소에 저장합니다.

Endpoint Management 는 파생된 자격 증명을 iOS 장치 등록에 사용할 수 있습니다. 파생된 자격 증명을 사용하도록 구성하면 Endpoint Management 가 iOS 장치에 대해 등록 초대 또는 기타 등록 모드를 지원하지 않습니다. 그러나 동일한 Endpoint Management 서버에서 등록 초대 및 기타 등록 모드를 통해 Android 장치를 등록할 수는 있습니다.

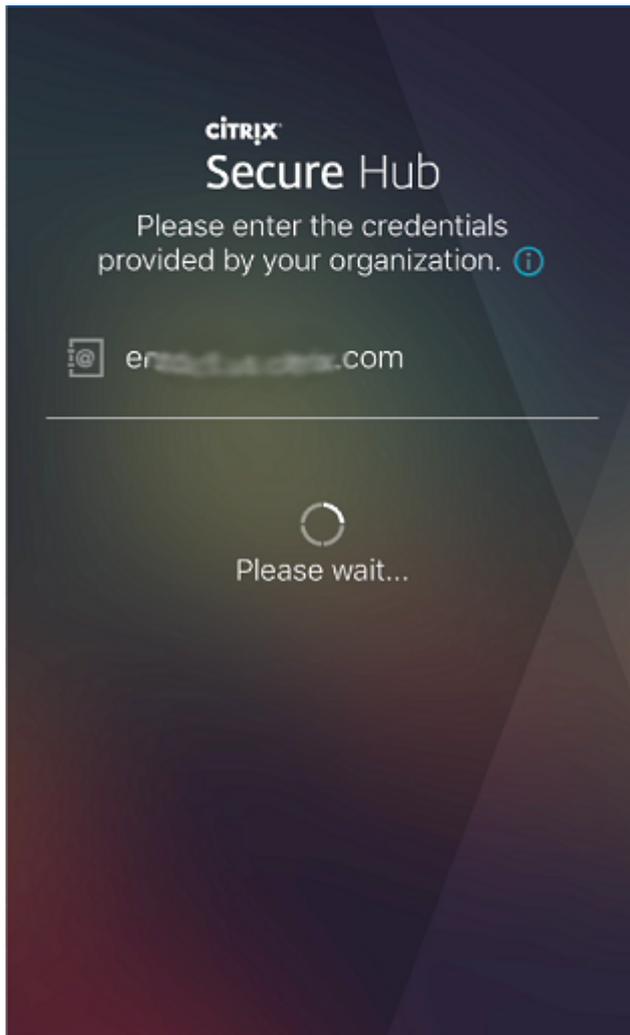
파생된 자격 증명을 사용하는 경우의 장치 등록 단계

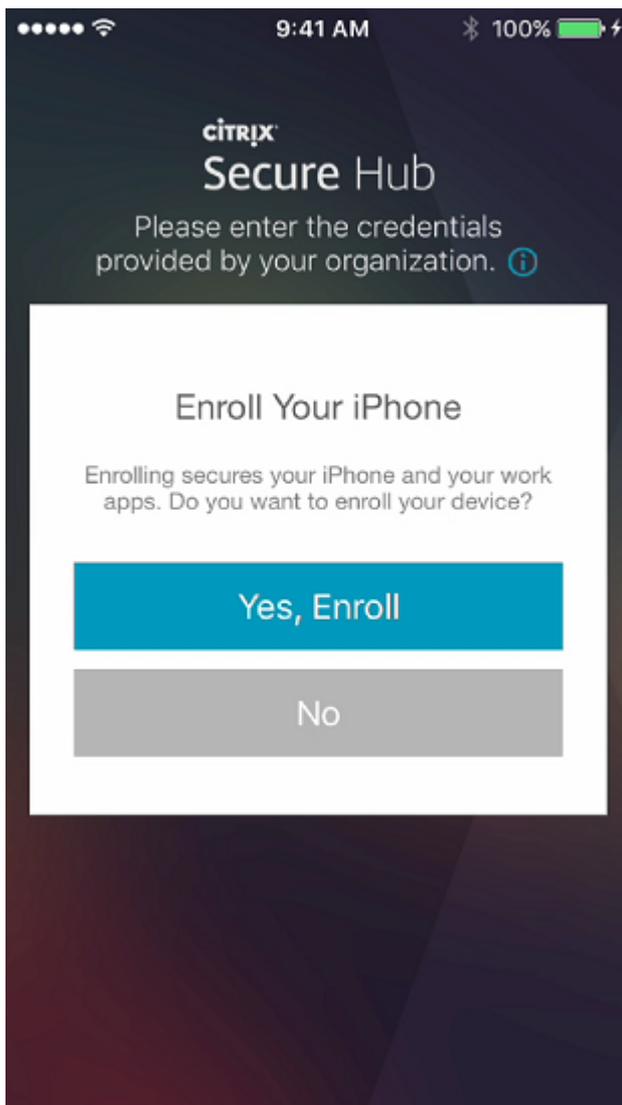
등록하려면 사용자 데스크톱에 부착된 판독기에 스마트 카드를 삽입해야 합니다.

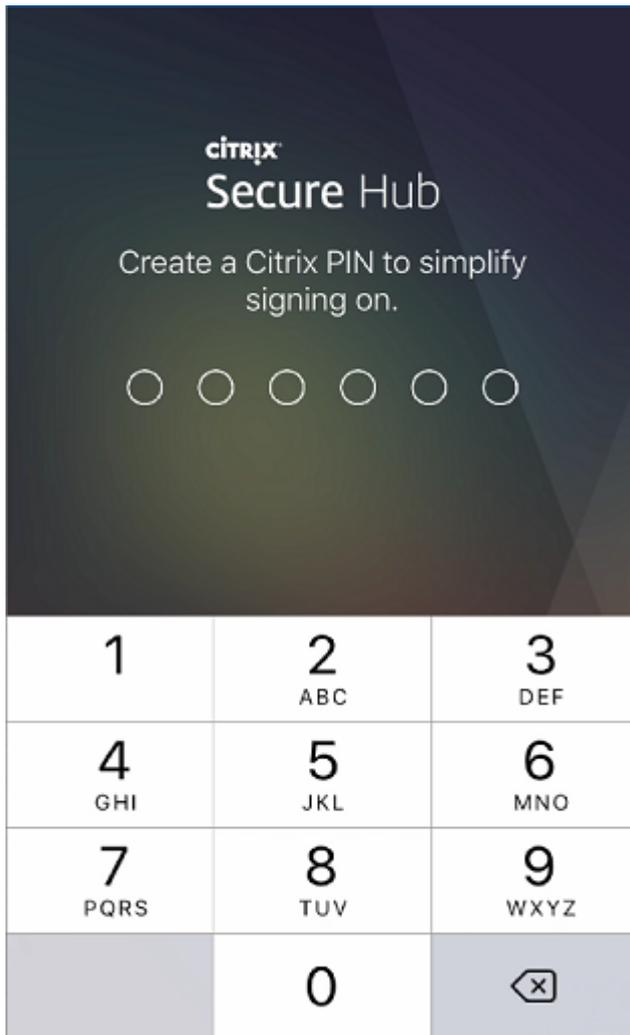
1. 사용자가 Secure Hub 와 파생된 자격 증명 공급자로부터 받은 앱을 설치합니다. 이 예에서 ID 공급자 앱은 Intercede MyID ID Agent 입니다.



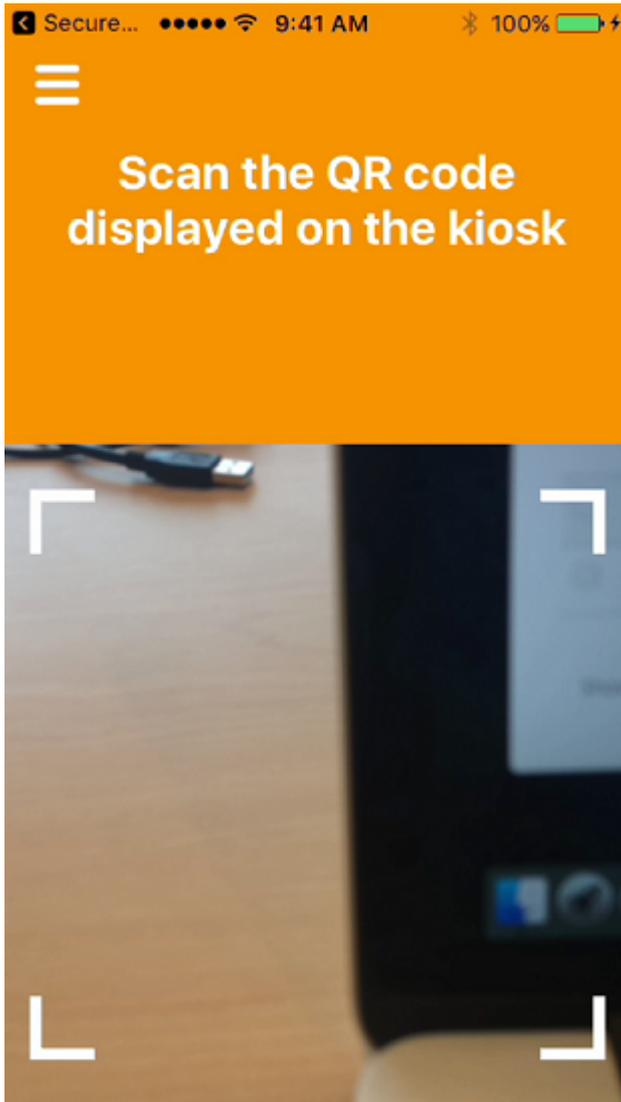
2. 사용자가 Secure Hub 를 시작합니다. 메시지가 나타나면 사용자가 Endpoint Management FQDN(정규화된 도메인 이름) 을 입력하고 다음을 클릭합니다. Secure Hub 에서 등록이 시작됩니다. Endpoint Management 에서 파생된 자격 증명을 지원하는 경우 Secure Hub 에 사용자가 Citrix PIN 을 생성하도록 요청하는 메시지가 표시됩니다.



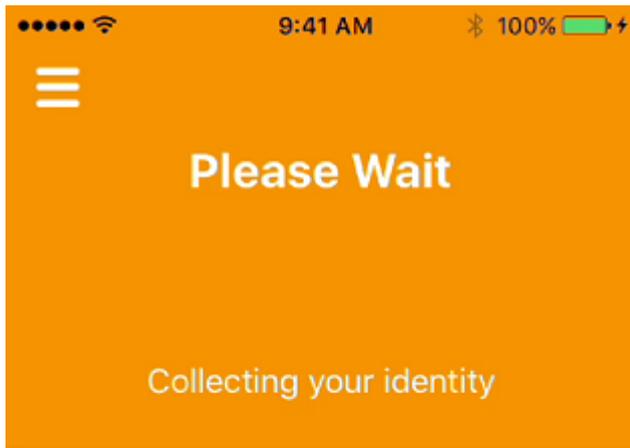




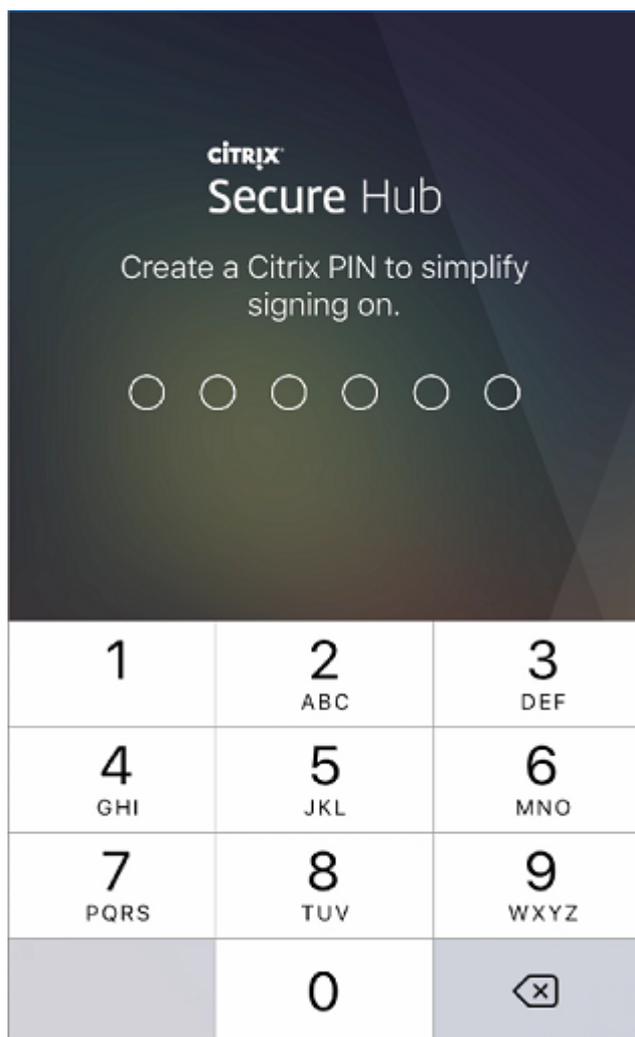
3. 사용자가 화면의 안내에 따라 스마트 자격 증명을 활성화합니다. 시작 화면이 나타나고 이어서 QR 코드를 스캔하라는 메시지가 나타납니다.



4. 사용자가 데스크톱에 부착된 스마트 카드 판독기에 카드를 삽입합니다. 그러면 데스크톱 앱에 QR 코드가 표시되고 사용자에게 모바일 장치를 사용하여 코드를 스캔하라는 메시지가 표시됩니다.



메시지가 나타나면 사용자가 Secure Hub PIN 을 입력합니다.



PIN 인증 후 Secure Hub 가 인증서를 다운로드합니다. 그런 다음 사용자는 메시지에 따라 등록을 완료합니다.

Endpoint Management 콘솔에서 장치 정보를 보려면 다음 중 하나를 수행하십시오.

- 관리 > 장치로 이동한 다음 명령 상자를 표시할 장치를 선택합니다. 자세히 표시를 클릭합니다.
- 분석 > 대시보드로 이동합니다.

## Citrix Endpoint Management 콘솔을 통한 힌트 구성

February 27, 2024

관리자는 등록 모드가 2 단계로 설정된 장치의 Secure Hub 로그인 페이지에서 힌트를 구성할 수 있습니다. 다음 방법 중 하나로 힌트를 구성할 수 있습니다.

- 힌트를 텍스트로 구성

- 웹 페이지 링크로 힌트 텍스트 구성

### 힌트를 텍스트로 구성

힌트 텍스트를 구성하려면 다음 단계를 수행하십시오.

1. 관리자 자격 증명을 사용하여 Citrix Endpoint Management 콘솔에 로그인합니다.
2. 설정 > 클라이언트 속성으로 이동한 다음 새 클라이언트 속성 추가를 클릭합니다.
3. 키 드롭다운 목록에서 사용자 지정 키를 선택합니다.
4. 키 필드에 **enrollment.twofactor.token.hint** 를 입력합니다.
5. 값 필드에 로그인 페이지에 힌트로 표시되는 텍스트를 입력할 수 있습니다. 힌트는 사용자가 2 단계 인증을 위한 PIN 을 찾도록 안내합니다.
6. 이름 필드에 **enrollment.twofactor.token.hint** 를 입력합니다.
7. 설명 필드에 구성된 힌트에 대한 설명을 입력할 수 있습니다. 이는 나중에 참조할 때 도움이 됩니다.

Settings > Client Properties > Add New Client Property

#### Add New Client Property

|               |  |
|---------------|--|
| Key           | Custom Key   |
| Key *         | enrollment.twofactor.token.hint  |
| Value *       | Please check your mail for security token/PIN  |
| Name *        | enrollment.twofactor.token.hint  |
| Description * | Please check your mail for security token/PIN. This is where to get your security token/PIN. |

8. 저장을 클릭합니다.

구성을 완료하면 로그인 페이지에 힌트 텍스트가 나타납니다.

citrix | Secure Hub

Please enter the credentials provided by your organization.

Username

Password

Pin

Please check your mail for security token/PIN

Back Next

[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

## 웹 페이지 링크로 힌트 텍스트 구성

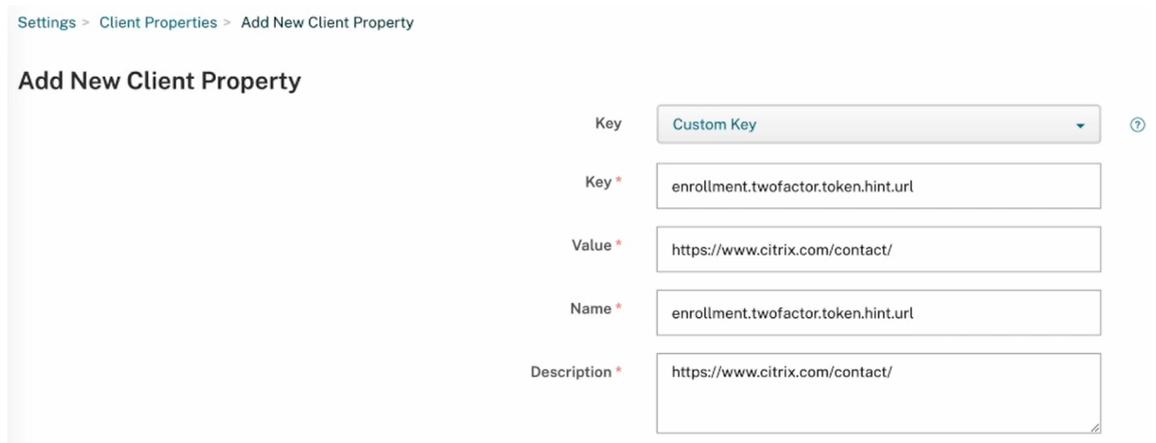
PIN 액세스에 대한 자세한 정보가 포함된 웹 페이지를 구성할 수 있습니다. 나중에 힌트 텍스트에서 웹 페이지 링크를 하이퍼링크로 제공합니다. 사용자가 로그인 페이지에서 힌트를 클릭하면 Secure Hub 가 내장된 브라우저를 열고 이미 구성된 웹 페이지로 이동합니다.

웹 페이지 링크로 힌트 텍스트를 구성하려면 먼저 [힌트를 텍스트로 구성](#) 문서에 설명된 대로 힌트 텍스트를 구성해야 합니다. 완료되면 다음 단계를 계속 진행하십시오.

1. 관리자 자격 증명을 사용하여 Citrix Endpoint Management 콘솔에 로그인합니다.
2. 설정 > 클라이언트 속성으로 이동한 다음 새 클라이언트 속성 추가를 클릭합니다.
3. 키 드롭다운 목록에서 사용자 지정 키를 선택합니다.
4. 키 필드에 **enrollment.twofactor.token.hint.url** 을 입력합니다.
5. 값 필드에 구성된 웹 페이지 URL 을 입력합니다.
6. 이름 필드에 **enrollment.twofactor.token.hint.url** 을 입력합니다.
7. 설명 필드에 구성된 힌트에 대한 설명을 입력할 수 있습니다. 이는 나중에 참조할 때 도움이 됩니다.

### 참고:

사용자가 힌트 링크를 클릭하면 내장된 브라우저에 웹 페이지가 나타납니다.



Settings > Client Properties > Add New Client Property

### Add New Client Property

|               |                                     |
|---------------|-------------------------------------|
| Key           | Custom Key                          |
| Key *         | enrollment.twofactor.token.hint.url |
| Value *       | https://www.citrix.com/contact/     |
| Name *        | enrollment.twofactor.token.hint.url |
| Description * | https://www.citrix.com/contact/     |

8. 저장을 클릭합니다.

구성을 완료하면 웹 페이지 링크가 포함된 힌트 텍스트가 로그인 페이지에 나타납니다.

citrix | Secure Hub

Please enter the credentials provided by your organization.

 Username

 Password

 Pin

Where to get your enrollment token?

[Back](#) [Next](#)

[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).