

보안 허브

Contents

시트릭스 시큐어 허브™	19
Secure Hub 관리	19
시트릭스 핀	19
인증서 고정	20
Secure Hub용 인증서 + 일회용 암호 인증 구성	21
Android 장치용 ADS 연결을 위한 포트 요구 사항	25
Secure Hub 기능	27
시트릭스 시큐어 허브™	30
현재 버전의 새로운 기능	30
iOS용 시큐어 허브 26.8.1	30
Android용 시큐어 허브 26.8.0	30
COSU 모드에서 런처 구성 정책에 자동 실행 앱 설정	30
MDM 장치 인증서의 자동 감지 및 갱신	31
이전 버전의 새로운 기능	31
iOS용 Secure Hub 버전 26.8.0	31
iOS/iPadOS 27 지원	31
Android용 Secure Hub 버전 26.5.0	31
Android 17 지원	31
Android용 시큐어 허브 26.2.0	31
장치 인증서 문제 해결 개선	31
iOS용 시큐어 허브 25.8.0	32
iOS 26 지원	32
Android용 시큐어 허브 25.10.0	32
16KB 메모리 페이지 크기 지원	32
Android용 시큐어 허브 25.7.0	32
iOS용 시큐어 허브 25.6.0	32

Android용 시큐어 허브 25.4.0	32
Android 16 지원	32
TLS 1.3 프로토콜 지원	32
Android용 보안 허브 25.1.0	33
iOS용 보안 허브 25.1.0	33
iOS용 시큐어 허브 24.11.0	33
Android용 시큐어 허브 24.10.0	33
Android 15 지원	33
iOS용 시큐어 허브 24.9.0	33
장치 등록 프로그램에 약관 표시	33
Android용 시큐어 허브 24.8.0	34
Android 장치 규정 준수 확인 (기술 미리 보기)	34
안드로이드용 Secure Hub 24.6.0	34
개선된 로그 수집 및 보고	34
아이오에스용 Secure Hub 24.5.0	34
iOS 17 서비스 복귀 지원	34
Android용 Secure Hub 24.3.0 버전	35
Samsung Knox 향상된 인증 v3 지원	35
Android용 보안 허브 23.12.0	35
Samsung Knox로 강화된 보안	35
사용자 개인 프로필에서 Secure Mail 액세스	35
iOS용 시큐어 허브 24.1.0	36
Android용 시큐어 허브 23.12.0	36
로그인 페이지에 인증 PIN에 대한 힌트 추가	36
nFactor 인증에서 단일 Sign-On 기능 지원	37
직접 부팅 모드에서 전체 초기화 지원	37
Secure Hub 앱 스토어의 로딩 속도 최적화	37
iOS용 보안 허브 23.11.0	37

로그인 페이지에 인증 PIN에 대한 힌트 추가	37
nFactor 인증, 단일 Sign-On 기능 지원	37
보안 허브 23.10.0	37
Android용 시큐어 허브	38
시큐어 허브 23.9.0	38
안드로이드용 Secure Hub	38
시큐어 허브 23.8.1	38
iOS용 시큐어 허브	38
시큐어 허브 23.8.0	38
iOS용 시큐어 허브	38
시큐어 허브 23.7.0	38
안드로이드용 Secure Hub	38
시큐어 허브 23.4.0	38
iOS용 시큐어 허브	38
시큐어 허브 23.4.1	39
안드로이드용 Secure Hub	39
시큐어 허브 23.4.0	39
안드로이드용 Secure Hub	39
시큐어 허브 23.2.0	40
안드로이드용 Secure Hub	40
시큐어 허브 22.11.0	40
안드로이드용 Secure Hub	40
시큐어 허브 22.9.0	41
안드로이드용 시큐어 허브	41
시큐어 허브 22.7.0	42
Android용 시큐어 허브	42
시큐어 허브 22.6.0	42
안드로이드용 Secure Hub	42

시큐어 허브 22.5.0	42
iOS용 시큐어 허브	42
시큐어 허브 22.4.0	42
안드로이드용 Secure Hub	42
시큐어 허브 22.2.0	42
iOS용 시큐어 허브	42
Android용 시큐어 허브	42
시큐어 허브 21.11.0	43
Android용 시큐어 허브	43
보안 허브 21.10.0	43
iOS용 보안 허브	43
안드로이드용 Secure Hub	43
시큐어 허브 21.8.0	43
iOS용 시큐어 허브	43
시큐어 허브 21.7.1	43
안드로이드용 시큐어 허브	43
시큐어 허브 21.7.0	44
iOS용 시큐어 허브	44
Android용 시큐어 허브	44
시큐어 허브 21.6.0	44
iOS용 시큐어 허브	44
Android용 시큐어 허브	44
시큐어 허브 21.5.1	44
iOS를 위한 Secure Hub	44
Android를 위한 Secure Hub	44
시큐어 허브 21.5.0	44
iOS용 시큐어 허브	44
보안 허브 21.4.0	44

보안 허브 21.3.2	44
iOS용 시큐어 허브	44
시큐어 허브 21.3.0	45
시큐어 허브 21.2.0	45
Android용 시큐어 허브	45
시큐어 허브 21.1.0	45
iOS용 시큐어 허브	45
Android용 시큐어 허브	45
시큐어 허브 20.12.0	45
iOS용 시큐어 허브	45
Android용 시큐어 허브	45
시큐어 허브 20.11.0	45
Android용 시큐어 허브	45
시큐어 허브 20.10.5	45
시큐어 허브 20.9.0	45
iOS용 시큐어 허브	45
Android용 시큐어 허브	46
시큐어 허브 20.7.5	46
Android용 시큐어 허브	46
시큐어 허브 20.6.5	46
Android용 시큐어 허브	46
iOS용 시큐어 허브	46
시큐어 허브 20.3.0	47
iOS용 시큐어 허브	47
시큐어 허브 20.2.0	47
iOS용 시큐어 허브	47
시큐어 허브 20.1.5	47
시큐어 허브 19.12.5	47

시큐어 허브 19.11.5	48
시큐어 허브 19.10.5	48
Android용 시큐어 허브	48
시큐어 허브 19.10.0	48
시큐어 허브 19.9.5	48
iOS용 시큐어 허브	48
Android용 시큐어 허브	48
시큐어 허브 19.9.0	48
iOS용 시큐어 허브	48
Android용 시큐어 허브	48
Android용 시큐어 허브 19.8.5	48
시큐어 허브 19.8.0	49
iOS용 시큐어 허브	49
Android용 시큐어 허브	49
Secure Hub 19.7.5 버전	49
iOS를 위한 Secure Hub	49
Android를 위한 Secure Hub	49
Secure Hub 19.3.5에서 19.6.6까지	49
Secure Hub 19.3.0 버전	49
Secure Hub 19.2.0 버전	50
시큐어 허브 19.1.5	50
시큐어 허브 19.1.0	50
Secure Hub 18.12.0 버전	50
Secure Hub 18.11.5 버전	50
시큐어 허브 18.10.0	50
시큐어 허브 10.8.60 ~ 18.9.0	51
시큐어 허브 10.8.60	51
보안 허브 10.8.55	52

Secure Hub 관리	53
시트릭스 핀	53
인증서 고정	54
인증서 + 일회용 암호 인증	55
Android 장치용 ADS 연결을 위한 포트 요구 사항	59
계정 삭제 옵션 비활성화	61
Secure Hub 사용	61
Secure Mail 자동 등록	64
사용자 지정 Store	65
구성된 도움말 옵션	65
위치 정책	66
충돌 수집 및 분석	66
Secure Hub용 장치 측 로그 생성	66
알려진 문제 및 해결된 문제	68
iOS용 시큐어 허브 26.8.1	68
해결된 문제	68
알려진 문제	68
Android용 시큐어 허브 26.8.0	68
해결된 문제	68
알려진 문제	68
iOS용 시큐어 허브 26.8.0	69
해결된 문제	69
알려진 문제	69
Android용 시큐어 허브 26.5.0	69
해결된 문제	69
알려진 문제	69
안드로이드용 시큐어 허브 26.2.0	69
해결된 문제	69

알려진 문제	70
안드로이드용 시큐어 허브 25.10.0	70
해결된 문제	70
알려진 문제	70
iOS용 보안 허브 25.8.0	70
해결된 문제	70
알려진 문제	70
Android용 보안 허브 25.7.0	70
해결된 문제	70
알려진 문제	70
iOS용 보안 허브 25.6.0	71
해결된 문제	71
알려진 문제	71
Android용 보안 허브 25.4.0	71
해결된 문제	71
알려진 문제	71
iOS용 시큐어 허브 25.1.0	71
해결된 문제	71
알려진 문제	71
Android용 시큐어 허브 25.1.0	71
해결된 문제	71
알려진 문제	72
iOS용 보안 허브 24.11.0	72
해결된 문제	72
알려진 문제	72
Android용 보안 허브 24.10.0	72
해결된 문제	72
알려진 문제	72

iOS용 보안 허브 24.9.0	72
해결된 문제	72
알려진 문제	72
안드로이드용 시큐어 허브 24.8.0	72
해결된 문제	72
알려진 문제	73
안드로이드용 시큐어 허브 24.6.0	73
해결된 문제	73
알려진 문제	73
iOS용 시큐어 허브 24.5.0	73
해결된 문제	73
알려진 문제	73
Android용 Secure Hub 버전 24.3.0	73
해결된 문제	73
알려진 문제	73
iOS용 Secure Hub 버전 24.1.0	73
해결된 문제	73
Android용 시큐어 허브 23.12.0	74
해결된 문제	74
iOS용 시큐어 허브 23.11.0	74
해결된 문제	74
Android용 시큐어 허브 23.10.0	74
해결된 문제	74
알려진 문제	75
Android용 시큐어 허브 23.9.0	75
해결된 문제	75
알려진 문제	75
iOS용 Secure Hub의 23.8.1 버전	75

해결된 문제	75
알려진 문제	75
iOS용 Secure Hub의 23.8.0 버전	75
해결된 문제	75
알려진 문제	75
이전 버전의 알려진 문제 및 해결된 문제	75
Secure Hub 알려진 문제 및 해결된 문제 기록	76
Android용 보안 허브 23.7.0	76
해결된 문제	76
알려진 문제	76
iOS용 보안 허브 23.4.0	76
해결된 문제	76
알려진 문제	77
안드로이드용 Secure Hub 23.4.1	77
해결된 문제	77
알려진 문제	77
안드로이드용 Secure Hub 23.4.0	77
해결된 문제	77
알려진 문제	77
Android용 시큐어 허브 23.2.0	77
해결된 문제	77
시큐어 허브 22.11.0	78
시트릭스 시큐어 허브 22.9.0	78
시큐어 허브 22.7.0	78
해결된 문제	78
시큐어 허브 22.6.0	78
시큐어 허브 22.5.0	79
시큐어 허브 22.4.0	79

시큐어 허브 22.2.0	79
Secure Hub 22.2.0의 알려진 문제	79
Secure Hub 22.2.0의 해결된 문제	79
iOS용 시트릭스 시큐어 허브	79
Android용 시큐어 허브	79
시큐어 허브 21.11.0	80
Secure Hub 21.11.0의 알려진 문제	80
Secure Hub 21.11.0에서 해결된 문제	80
안드로이드용 시큐어 허브	80
시큐어 허브 21.10.0	80
Secure Hub 21.10.0의 알려진 문제	80
Secure Hub 21.10.0에서 해결된 문제	80
iOS용 시큐어 허브	80
안드로이드용 시큐어 허브	80
시큐어 허브 21.8.0	81
iOS용 시큐어 허브	81
Secure Hub 21.8.0의 알려진 문제	81
Secure Hub 21.8.0에서 해결된 문제	81
시큐어 허브 21.7.1	81
Android용 시큐어 허브	81
이전 버전의 알려진 문제 및 해결된 문제	81
Secure Hub 21.7.1 릴리스	81
안드로이드용 Secure Hub	81
Secure Hub 버전 21.7.0	81
iOS용 시큐어 허브	81
Android용 시큐어 허브	82
Secure Hub 21.7.0의 알려진 문제	82
Secure Hub 21.7.0에서 해결된 문제	82

시큐어 허브 21.6.0	82
iOS용 시큐어 허브	82
Secure Hub 21.6.0의 알려진 문제	82
Secure Hub 21.6.0에서 해결된 문제	82
안드로이드용 Secure Hub	82
Secure Hub 21.6.0의 알려진 문제	82
Secure Hub 21.6.0의 해결된 문제	82
시큐어 허브 21.5.1	82
아이오에스용 Secure Hub	82
Android용 시큐어 허브	83
시큐어 허브 21.5.0	83
Secure Hub 21.5.0의 알려진 문제	83
Secure Hub 21.5.0의 해결된 문제	83
시큐어 허브 21.4.0	83
시큐어 허브 21.3.2 버전	83
iOS용 시큐어 허브	83
Secure Hub 21.3.2의 알려진 문제	83
Secure Hub 21.3.2에서 해결된 문제	83
시큐어 허브 21.3.0	83
Secure Hub 21.3.0의 알려진 문제	83
Secure Hub 21.3.0에서 해결된 문제	84
시큐어 허브 21.2.0	84
Android용 시큐어 허브	84
Secure Hub 21.2.0의 알려진 문제	84
Secure Hub 21.2.0에서 해결된 문제	84
시큐어 허브 21.1.0	84
Secure Hub 21.1.0의 알려진 문제	84
Secure Hub 21.1.0에서 해결된 문제	84

시큐어 허브 20.12.0	85
Secure Hub 20.12.0의 알려진 문제	85
Secure Hub 20.12.0에서 해결된 문제	85
시큐어 허브 20.11.0	85
Android용 시큐어 허브	85
Secure Hub 20.11.0의 알려진 문제	85
Secure Hub 20.11.0의 해결된 문제	85
시큐어 허브 20.10.5	85
Secure Hub 20.10.5의 알려진 문제	85
Secure Hub 20.10.5의 해결된 문제	85
시큐어 허브 20.9.0	86
Secure Hub 20.9.0의 알려진 문제	86
Secure Hub 20.9.0의 해결된 문제	86
시큐어 허브 20.7.5	86
Secure Hub 20.7.5의 알려진 문제	86
Secure Hub 20.7.5의 해결된 문제	86
시큐어 허브 20.6.5	87
시큐어 허브 20.3.0	87
iOS를 위한 Secure Hub	87
시큐어 허브 20.2.0	87
iOS용 보안 허브	87
Secure Hub 20.2.0의 알려진 문제	87
Secure Hub 20.2.0의 해결된 문제	87
시큐어 허브 20.1.5	87
시큐어 허브 19.12.5	87
Secure Hub 19.12.5의 알려진 문제	87
Secure Hub 19.12.5의 해결된 문제	87
시큐어 허브 19.11.5	88

Secure Hub 19.11.5의 알려진 문제	88
Secure Hub 19.11.5의 해결된 문제	88
시큐어 허브 19.10.5	88
Android용 시큐어 허브	88
Secure Hub 19.10.5의 알려진 문제	88
Secure Hub 19.10.5의 해결된 문제	88
시큐어 허브 19.10.0	88
Secure Hub 19.10.0의 알려진 문제	88
Secure Hub 19.10.0의 해결된 문제	88
시큐어 허브 19.9.5	88
시큐어 허브 19.9.0	89
Secure Hub 19.9.0의 알려진 문제	89
Secure Hub 19.9.0의 해결된 문제	89
시큐어 허브 19.8.5	89
시큐어 허브 19.8.0	89
Secure Hub 19.8.0의 알려진 문제	89
Secure Hub 19.8.0에서 해결된 문제	89
시큐어 허브 19.7.5	89
Secure Hub 19.7.5의 알려진 문제	89
Secure Hub 19.7.5에서 해결된 문제	89
시큐어 허브 19.6.5	90
Secure Hub 19.6.5의 알려진 문제	90
Secure Hub 19.6.5의 해결된 문제	90
시큐어 허브 19.5.5	90
Secure Hub 19.5.5의 알려진 문제	90
Secure Hub 19.5.5의 해결된 문제	91
시큐어 허브 19.5.0	91
Secure Hub 19.5.0의 알려진 문제	91

Secure Hub 19.5.0의 해결된 문제	91
시큐어 허브 19.4.5	91
Secure Hub 19.4.5의 알려진 문제	91
Secure Hub 19.4.5의 해결된 문제	91
시큐어 허브 19.3.5	92
Secure Hub 19.3.5의 알려진 문제	92
Secure Hub 19.3.5의 해결된 문제	92
시큐어 허브 19.3.0	92
Secure Hub 19.3.0의 알려진 문제	92
Secure Hub 19.3.0의 해결된 문제	93
시큐어 허브 19.2.0	93
Secure Hub 19.2.0의 알려진 문제	93
Secure Hub 19.2.0의 해결된 문제	93
시큐어 허브 19.1.5	93
Secure Hub 19.1.5의 알려진 문제	93
Secure Hub 19.1.5에서 해결된 문제	94
시큐어 허브 19.1.0	94
Secure Hub 19.1.0의 알려진 문제	94
Secure Hub 18.12.0에서 해결된 문제	94
시큐어 허브 18.11.0	94
Secure Hub 18.11.0에서 해결된 문제	94
시큐어 허브 18.10.5	94
Secure Hub 18.10.5의 해결된 문제	94
Secure Hub 버전 10.8.25 ~ 18.10.6	95
Secure Hub 버전 10.8.25 ~ 18.10.6의 해결된 문제	95
시큐어 허브 18.10.0	95
Secure Hub 18.10.0의 해결된 문제	95
시큐어 허브 10.8.60	95

Secure Hub 10.8.60의 해결된 문제	95
보안 허브 10.8.55	96
Secure Hub 10.8.55의 해결된 문제	96
버전 10.8.55의 MDX 관련 해결된 문제	96
보안 허브 10.8.55	96
Secure Hub 10.8.55의 알려진 문제	96
시큐어 허브 10.8.50	96
Secure Hub 10.8.50의 알려진 문제	96
시큐어 허브 10.8.35	96
Secure Hub 10.8.35에서 해결된 문제	96
시큐어 허브 10.8.25	97
Secure Hub 10.8.25에서 해결된 문제	97
시큐어 허브 10.8.20	97
Secure Hub 10.8.20에서 해결된 문제	97
시큐어 허브 10.8.15	97
Secure Hub 10.8.15의 해결된 문제	97
시큐어 허브 10.8.10	97
Secure Hub 10.8.10의 해결된 문제	97
Android 및 iOS용 Secure Hub - 미리 보기	98
기능 플래그 관리	99
인증 프롬프트 시나리오	100
자격 증명 유형	101
Secure Hub 화면 전환 정보	103
장치 암호의 암호 복잡성 (Android 12 이상)	104
파생 자격 증명을 사용하여 장치 등록	105
파생 자격 증명 사용 시 장치 등록 단계	105
Citrix Endpoint Management™ 콘솔을 통해 힌트 구성	111
텍스트로 힌트 구성	111

웹 페이지 링크로 힌트 텍스트 구성	112
Android 기기 규정 준수 확인 (기술 미리 보기)	113

시트릭스 시큐어 허브™

Citrix Secure Hub는 Citrix Endpoint Management™(이전 명칭: XenMobile) 경험을 위한 시작점입니다. 사용자는 Store에 액세스하기 위해 Secure Hub에 장치를 등록합니다. Store에서 Citrix가 개발한 모바일 생산성 앱과 타사 앱을 추가할 수 있습니다.

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

Secure Hub 관리

Endpoint Management의 초기 구성 중에 Secure Hub와 관련된 대부분의 관리 작업을 수행합니다. iOS 및 Android 사용자가 Secure Hub를 사용할 수 있도록 하려면 Secure Hub를 iOS App Store 및 Google Play Store에 업로드하십시오.

Citrix 앱을 위한 포털을 제공하는 것 외에도, Secure Hub는 사용자의 Citrix Gateway 세션이 Citrix Gateway를 사용하여 인증 후 갱신될 때 설치된 앱에 대해 Endpoint Management에 저장된 대부분의 MDX 정책을 새로 고칩니다.

중요:

다음 정책 중 하나라도 변경되면 업데이트된 정책을 적용하기 위해 사용자가 앱을 삭제하고 다시 설치해야 합니다. 보안 그룹, 암호화 사용, Secure Mail Exchange Server.

시트릭스 핀

Secure Hub가 Citrix PIN을 사용하도록 구성할 수 있습니다. 이 기능은 Endpoint Management 콘솔의 **설정 > 클라이언트 속성**에서 활성화되는 보안 기능입니다. 이 설정은 등록된 모바일 장치 사용자가 Secure Hub에 로그인하고 개인 식별 번호(PIN)를 사용하여 MDX 래핑된 앱을 활성화하도록 요구합니다.

Citrix PIN 기능은 보안 래핑된 앱에 로그인할 때 사용자 인증 경험을 간소화합니다. 사용자는 Active Directory 사용자 이름 및 암호와 같은 다른 자격 증명을 반복해서 입력할 필요가 없습니다.

Secure Hub에 처음 로그인하는 사용자는 Active Directory 사용자 이름과 암호를 입력해야 합니다. 로그인하는 동안 Secure Hub는 Active Directory 자격 증명 또는 클라이언트 인증서를 사용자 장치에 저장한 다음 사용자에게 PIN을 입력하라는 메시지를 표시합니다. 사용자가 다시 로그인할 때, 활성 사용자 세션의 다음 유효 시간 초과 기간이 끝날 때까지 PIN을 입력하여 Citrix 앱과 Store에 안전하게 액세스합니다. 관련 클라이

언트 속성을 통해 PIN을 사용하여 비밀을 암호화하고, PIN의 암호 유형을 지정하고, PIN 강도 및 길이 요구 사항을 지정할 수 있습니다. 자세한 내용은 [클라이언트 속성](#)을 참조하십시오.

지문 인증이 활성화되면, 앱 비활성으로 인해 오프라인 인증이 필요한 경우 사용자는 지문을 사용하여 로그인할 수 있습니다. 사용자는 Secure Hub에 처음 로그인할 때, 장치를 다시 시작할 때, 그리고 비활성 타이머가 만료된 후에는 여전히 PIN을 입력해야 합니다. 지문 인증 활성화에 대한 자세한 내용은 [지문 또는 Touch ID 인증](#)을 참조하십시오.

인증서 고정

iOS 및 Android용 Secure Hub는 SSL 인증서 고정을 지원합니다. 이 기능은 Citrix 클라이언트가 Endpoint Management와 통신할 때 기업에서 서명한 인증서가 사용되도록 합니다. 인증서 고정은 장치에 루트 인증서를 설치하여 SSL 세션이 손상될 때 클라이언트가 Endpoint Management에 연결하는 것을 방지합니다. Secure Hub가 서버 공개 키에 대한 변경 사항을 감지하면 Secure Hub는 연결을 거부합니다.

Android N부터 운영 체제는 더 이상 사용자가 추가한 인증 기관(CA)을 허용하지 않습니다. Citrix는 사용자가 추가한 CA 대신 공용 루트 CA를 사용할 것을 권장합니다.

Android N으로 업그레이드하는 사용자는 개인 또는 자체 서명된 CA를 사용하는 경우 문제가 발생할 수 있습니다. Android N 장치에서의 연결은 다음 시나리오에서 끊어집니다:

- 개인/자체 서명된 CA와 AutoDiscovery Service의 Endpoint Management용 필수 신뢰 CA 옵션이 **ON**으로 설정된 경우. 자세한 내용은 [Endpoint Management AutoDiscovery Service](#)를 참조하십시오.
- 개인/자체 서명된 CA와 AutoDiscovery Service(ADS)에 연결할 수 없는 경우. 보안 문제로 인해 ADS에 연결할 수 없으면 초기 설정이 **OFF**였더라도 필수 신뢰 CA가 **ON**으로 전환됩니다.

장치를 등록하거나 Secure Hub를 업그레이드하기 전에 인증서 고정을 활성화하는 것을 고려하십시오. 이 옵션은 기본적으로 **꺼져** 있으며 Endpoint Management Auto Discovery Service(ADS)에서 관리합니다. 인증서 고정을 활성화하면 사용자는 자체 서명된 인증서로 Endpoint Management에 등록할 수 없습니다. 사용자가 자체 서명된 인증서로 등록하려고 하면 인증서가 신뢰할 수 없다는 경고를 받습니다. 사용자가 인증서를 수락하지 않으면 등록이 실패합니다.

인증서 고정을 사용하려면 Citrix에 Citrix ADS 서버로 인증서를 업로드하도록 요청하십시오. [Citrix 지원 포털](#)을 사용하여 기술 지원 사례를 여십시오. 그런 다음 다음 정보를 제공하십시오:

- 사용자가 등록할 계정이 포함된 도메인.
- Endpoint Management 정규화된 도메인 이름(FQDN).
- Endpoint Management 인스턴스 이름. 기본적으로 인스턴스 이름은 zdm이며 대소문자를 구분합니다.
- 사용자 ID 유형(UPN 또는 이메일). 기본적으로 유형은 UPN입니다.

- 기본 포트 8443에서 포트 번호를 변경한 경우 iOS 등록에 사용되는 포트.
- 기본 포트 443에서 포트 번호를 변경한 경우 Endpoint Management가 연결을 수락하는 포트.
- Citrix Gateway의 전체 URL.
- 선택 사항으로, Endpoint Management 관리자의 이메일 주소.
- 도메인에 추가하려는 PEM 형식 인증서.

Secure Hub용 인증서 + 일회용 암호 인증 구성

Secure Hub가 인증서와 일회용 암호 역할을 하는 보안 토큰을 사용하여 인증하도록 Citrix ADC를 구성할 수 있습니다. 이 구성은 장치에 Active Directory 흔적을 남기지 않는 강력한 보안 옵션을 제공합니다.

Secure Hub가 이 유형의 인증을 사용하도록 설정하려면 Citrix ADC에서 Citrix Gateway 로그인 유형을 나타내는 **X-Citrix-AM-GatewayAuthType: CertAndRSA** 형식의 사용자 지정 응답 헤더를 삽입하는 재작성 작업 및 재작성 정책을 추가합니다.

일반적으로 Secure Hub는 Endpoint Management 콘솔에 구성된 Citrix Gateway 로그인 유형을 사용합니다. 그러나 이 정보는 Secure Hub가 처음 로그온을 완료할 때까지 Secure Hub에서 사용할 수 없습니다. 따라서 Secure Hub가 이를 수행할 수 있도록 사용자 지정 헤더가 필요합니다.

참고:

Endpoint Management와 Citrix ADC에 다른 로그인 유형이 설정된 경우 Citrix ADC 구성이 해당 구성을 재정의합니다. 자세한 내용은 [Citrix Gateway](#) 및 [Endpoint Management](#)를 참조하십시오.

1. Citrix ADC에서 **Configuration > AppExpert > Rewrite > Actions**로 이동합니다.
2. **Add**를 클릭합니다.

Create Rewrite Action 화면이 나타납니다.

3. 다음 그림에 표시된 대로 각 필드를 채운 다음 **Create**를 클릭합니다.

Create Rewrite Action

Name*
InsertGatewayAuthTypeHeader ?

Type*
INSERT_HTTP_HEADER ▼

Use this action type to insert a header.

Header Name*
X-Citrix-AM-GatewayAuthType

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** 화면에 다음 결과가 나타납니다.

NetScaler > AppExpert > Rewrite > Rewrite Actions

Add Edit Delete Action ▼ 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. 재작성 작업을 재작성 정책으로 가상 서버에 바인딩합니다. **Configuration > NetScaler® Gateway > Virtual Servers**로 이동한 다음 가상 서버를 선택합니다.

Dashboard Configuration Reporting Documentation Downloads

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action ▼ Search ▼

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	Up	10.71.12.30	500	SSL	0	0	0

Integrate with Citrix Products

- XenMobile
- XenApp and XenDesktop
- Unified Gateway

5. **편집**을 클릭합니다.
6. **가상 서버 구성** 화면에서 아래로 스크롤하여 **정책**으로 이동합니다.
7. 정책을 추가하려면 **++**를 클릭합니다.

The screenshot shows the 'Profiles' configuration page. The 'Profiles' section lists Net Profile, TCP Profile, and HTTP Profile (nshttp_default_strict_validation). The 'Published Applications' section lists 'No Next HOP Server', '1 STA Server', and 'No Url'. The 'Other Settings' section includes ICMP Virtual Server Response (Passive), RHI State (Passive), Redirect to Home page (true), Listen Priority (NONE), Listen Policy Expression (NONE), ShareFile, AppController (https://camamappc8.camam.net:8443), and L2 Connection (false). The 'Policies' section shows 'Request Policies' with 3 Session Policies, 2 ClientlessAccess Policies, and 5 Cache Policies. A hand icon points to the '+' button in the Policies section to add a new policy.

8. **정책 선택** 필드에서 **재작성**을 선택합니다.
9. **유형 선택** 필드에서 **응답**을 선택합니다.

The screenshot shows the 'Choose Type' dialog box. It has a title bar 'Choose Type' and a subtitle 'Choose Type'. Below the subtitle is a section titled 'Policies'. Inside this section are two dropdown menus: 'Choose Policy*' with 'Rewrite' selected, and 'Choose Type*' with 'Response' selected. At the bottom are two buttons: 'Continue' (highlighted with a hand icon) and 'Cancel'.

10. 계속을 클릭합니다.

정책 바인딩 섹션이 확장됩니다.

Choose Type

Choose Type [X]

Policies [Edit]

Choose Policy Rewrite Choose Type Response

Policy Binding

Select Policy*
Click to select [+] [Edit] [?]

Binding Details

Priority*
100 [?]

Goto Expression*
END [v]

[Bind] [Close]

11. 정책 선택을 클릭합니다.

사용 가능한 정책이 있는 화면이 나타납니다.

Choose Type > Rewrite Policies [?] [X]

Rewrite Policies

[Select] [Add] [Edit] [Delete] [Show Bindings] [Policy Manager] [Statistics] [Action] [Show built-in Rewrite Policies] [Search]

Name	Expression	Action	Undefined-Result Action	Hits	Undefined Hits	Active
InsertGatewayAuthTypePolicy	true	InsertGatewayAuthTypeHeader	Use Global	0	0	[X]

12. 방금 생성한 정책의 행을 클릭한 다음 선택을 클릭합니다. 정책 바인딩 화면이 다시 나타나고 선택한 정책이 채워집니다.

13. 바인딩을 클릭합니다.

바인딩이 성공하면 완료된 재작성 정책이 표시된 기본 구성 화면이 나타납니다.

성공적인 바인딩 이미지(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-bind-successful.png)

14. 정책 세부 정보를 보려면 **재작성 정책**을 클릭합니다.

재작성 정책 세부 정보 이미지(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-rewrite-policy.png)

Android 장치용 ADS 연결을 위한 포트 요구 사항

포트 구성은 Secure Hub에서 연결하는 Android 장치가 회사 네트워크 내에서 Citrix ADS에 액세스할 수 있도록 보장합니다. ADS를 통해 제공되는 보안 업데이트를 다운로드할 때 ADS에 액세스하는 기능은 중요합니다. ADS 연결은 프록시 서버와 호환되지 않을 수 있습니다. 이 시나리오에서는 ADS 연결이 프록시 서버를 우회하도록 허용합니다.

중요:

Android 및 iOS용 Secure Hub는 Android 장치가 ADS에 액세스하도록 허용해야 합니다. 자세한 내용은 Endpoint Management 설명서의 [포트 요구 사항](#)을 참조하십시오. 이 통신은 아웃바운드 포트 443에서 이루어집니다. 기존 환경은 이 액세스를 허용하도록 설계되었을 가능성이 높습니다. 이 통신을 보장할 수 없는 고객은 Secure Hub 10.2로 업그레이드하지 않는 것이 좋습니다. 궁금한 점이 있으면 Citrix 지원팀에 문의하십시오.

인증서 고정을 사용하려면 다음 필수 구성 요소를 수행해야 합니다.

- Endpoint Management 및 Citrix ADC 인증서를 수집합니다. 인증서는 PEM 형식이어야 하며 개인 키가 아닌 공개 인증서여야 합니다.
- Citrix 지원팀에 문의하여 인증서 고정 활성화 요청을 제출합니다. 이 과정에서 인증서를 요청받게 됩니다.

새로운 인증서 고정 개선 사항은 장치가 등록하기 전에 ADS에 연결해야 합니다. 이렇게 하면 장치가 등록되는 환경에 대한 최신 보안 정보가 Secure Hub에서 제공됩니다. 장치가 ADS에 연결할 수 없으면 Secure Hub는 장치 등록을 허용하지 않습니다. 따라서 내부 네트워크 내에서 ADS 액세스를 개방하는 것은 장치 등록을 가능하게 하는 데 중요합니다.

Android용 Secure Hub의 ADS에 대한 액세스를 허용하려면 다음 IP 주소 및 FQDN에 대해 포트 443을 엽니다.

FQDN	IP 주소	포트	IP 및 포트 사용
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	Secure Hub - ADS 통신
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	Secure Hub - ADS 통신
<code>ads.xm.cloud.com</code> : SecureHub 버전 10.6.15 이상에서는 <code>ads.xm.cloud.com</code> 를 사용합니다.	34.194.83.188	443	Secure Hub - ADS 통신
<code>ads.xm.cloud.com</code> : SecureHub 버전 10.6.15 이상에서는	34.193.202.23	443	Secure Hub - ADS 통신

FQDN	IP 주소	포트	IP 및 포트 사용
ads.xml.cloud.com 를 사용합니다.			

인증서 고정이 활성화된 경우:

- Secure Hub는 장치 등록 중에 엔터프라이즈 인증서를 고정합니다.
- 업그레이드 중에 Secure Hub는 현재 고정된 인증서를 모두 삭제한 다음, 등록된 사용자의 첫 연결 시 서버 인증서를 고정합니다.

참고:

업그레이드 후 인증서 고정을 활성화하는 경우, 사용자는 다시 등록해야 합니다.

- 인증서 공개 키가 변경되지 않은 경우, 인증서 갱신 시 재등록이 필요하지 않습니다.

인증서 고정은 중간 또는 발급자 인증서가 아닌 리프 인증서를 지원합니다. 인증서 고정은 Endpoint Management 및 Citrix Gateway와 같은 Citrix 서버에 적용되며 타사 서버에는 적용되지 않습니다.

Secure Hub 기능

Secure Hub를 사용하면 모바일 정책을 모니터링하고 적용하는 동시에 Store 및 실시간 지원에 액세스할 수 있습니다. 사용자는 Apple, Android 또는 Windows 앱 스토어에서 Secure Hub를 장치에 다운로드하는 것으로 시작합니다.

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

Android용 Secure Hub에서 초기 설치 및 등록 중에 다음 메시지가 나타납니다. Secure Hub가 장치의 사진, 미디어 및 파일에 액세스하도록 허용하시겠습니까?

이 메시지는 Citrix가 아닌 Android 운영 체제에서 제공됩니다. **허용**을 탭해도 Citrix 및 Secure Hub를 관리하는 관리자는 언제든지 개인 데이터를 볼 수 없습니다. 하지만 관리자와 원격 지원 세션을 진행하는 경우, 관리자는 세션 내에서 개인 파일을 볼 수 있습니다.

등록되면 사용자는 **내 앱** 탭에서 푸시한 모든 앱과 데스크톱을 볼 수 있습니다. 사용자는 Store에서 더 많은 앱을 추가할 수 있습니다. 휴대폰에서는 Store 링크가 왼쪽 상단 모서리에 있는 설정 햄버거 아이콘 아래에 있습니다.

Store 링크 이미지 (/en-us/mobile-productivity-apps/media/secure-hub-settings.png)

태블릿에서는 Store가 별도의 탭으로 표시됩니다.

태블릿의 Store 이미지 (/en-us/mobile-productivity-apps/media/secure-hub-ipad-myapps.png)

iOS 9 이상을 실행하는 iPhone 사용자가 Endpoint Management 앱 스토어에서 모바일 생산성 앱을 설치하면, 엔터프라이즈 개발자인 Citrix가 해당 iPhone에서 신뢰할 수 없으며 개발자가 신뢰될 때까지 앱을 사용할 수 없다는 메시지가 표시됩니다. 이 메시지가 나타나면 Secure Hub는 사용자에게 iPhone용 Citrix 엔터프라이즈 앱을 신뢰하는 과정을 안내하는 가이드를 보도록 안내합니다.

MAM 전용 배포의 경우, 이메일 자격 증명을 사용하여 Secure Hub에 등록하는 Android 또는 iOS 장치 사용자가 Secure Mail에 자동으로 등록되도록 Endpoint Management를 구성할 수 있습니다. 사용자는 Secure Mail에 등록하기 위해 추가 정보를 입력하거나 추가 단계를 수행할 필요가 없습니다.

Secure Mail을 처음 사용할 때 Secure Mail은 Secure Hub에서 사용자의 이메일 주소, 도메인 및 사용자 ID를 가져옵니다. Secure Mail은 자동 검색을 위해 이메일 주소를 사용합니다. Exchange 서버는 도메인 및 사용자 ID를 사용하여 식별되며, 이를 통해 Secure Mail은 사용자를 자동으로 인증할 수 있습니다. 정책이 암호를 통과하지 않도록 설정된 경우 사용자에게 암호를 입력하라는 메시지가 표시되지만, 사용자는 더 이상 정보를 입력할 필요가 없습니다.

이 기능을 활성화하려면 다음 세 가지 속성을 생성하십시오.

- 서버 속성 MAM_MACRO_SUPPORT. 지침은 [서버 속성](#)을 참조하십시오.
- 클라이언트 속성 ENABLE_CREDENTIAL_STORE 및 SEND_LDAP_ATTRIBUTES. 지침은 [클라이언트 속성](#)을 참조하십시오.

Store를 사용자 지정하려면 **설정 > 클라이언트 브랜딩**으로 이동하여 이름을 변경하고 로고를 추가하며 앱 표시 방식을 지정하십시오.

클라이언트 브랜딩 이미지 (/en-us/mobile-productivity-apps/media/worxhome-client-branding.png)

Endpoint Management 콘솔에서 앱 설명을 편집할 수 있습니다. **구성**을 클릭한 다음 **앱**을 클릭합니다. 테이블에서 앱을 선택한 다음 **편집**을 클릭합니다. 편집 중인 설명이 있는 앱의 플랫폼을 선택한 다음 **설명** 상자에 텍스트를 입력합니다.

설명 상자 이미지 (/en-us/mobile-productivity-apps/media/worxhome-edit-app-descriptions-xm.png)

스토어에서 사용자는 Endpoint Management에서 구성하고 보호한 앱과 데스크톱만 찾아볼 수 있습니다. 앱을 추가하려면 사용자는 **세부 정보**를 탭한 다음 **추가**를 탭합니다.

Secure Hub는 또한 사용자에게 다양한 도움말을 얻을 수 있는 방법을 제공합니다. 태블릿에서는 오른쪽 상단 모서리에 있는 물음표를 탭하면 도움말 옵션이 열립니다. 휴대폰에서는 왼쪽 상단 모서리에 있는 햄버거 메뉴 아이콘을 탭한 다음 **도움말**을 탭합니다.

도움말 화면 이미지(/en-us/mobile-productivity-apps/media/secure-hub-helpdesk.png)

IT 부서에는 사용자가 앱에서 직접 액세스할 수 있는 회사 헬프 데스크의 전화번호와 이메일이 표시됩니다. Endpoint Management 콘솔에서 전화번호와 이메일 주소를 입력합니다. 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다. **자세히**를 클릭한 다음 **클라이언트 지원**을 클릭합니다. 정보를 입력하는 화면이 나타납니다.

클라이언트 지원 화면 이미지(/en-us/mobile-productivity-apps/media/workhome-edit-client-support-xm.png)

문제 보고에는 앱 목록이 표시됩니다. 사용자는 문제가 있는 앱을 선택합니다. Secure Hub는 자동으로 로그를 생성한 다음, 로그가 zip 파일로 첨부된 Secure Mail 메시지를 엽니다. 사용자는 제목과 문제 설명을 추가합니다. 스크린샷도 첨부할 수 있습니다.

Citrix에 피드백 보내기는 Citrix 지원 주소가 채워진 Secure Mail 메시지를 엽니다. 메시지 본문에서 사용자는 Secure Mail 개선을 위한 제안을 입력할 수 있습니다. Secure Mail이 장치에 설치되어 있지 않으면 기본 메일 프로그램이 열립니다.

사용자는 **Citrix 지원**을 탭하여 **Citrix Knowledge Center**를 열 수도 있습니다. 여기에서 모든 Citrix 제품에 대한 지원 문서를 검색할 수 있습니다.

기본 설정에서 사용자는 자신의 계정 및 장치에 대한 정보를 찾을 수 있습니다.

예를 들어, 회사 소유 장치가 특정 지리적 경계를 벗어나지 않도록 하려면 Secure Hub는 지리적 위치 및 지리적 추적 정책도 제공합니다. 자세한 내용은 **위치 장치 정책**을 참조하십시오. 또한 Secure Hub는 실패 정보를 자동으로 수집하고 분석하여 특정 실패의 원인을 파악할 수 있도록 합니다. 이 기능은 Crashlytics 소프트웨어에서 지원됩니다.

시트릭스 시큐어 허브™

Citrix Secure Hub는 모바일 생산성 앱을 위한 런치패드입니다. 사용자는 앱 스토어에 액세스하기 위해 Secure Hub에 장치를 등록합니다. 앱 스토어에서 Citrix에서 개발한 모바일 생산성 앱과 타사 앱을 추가할 수 있습니다.

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

Secure Hub 및 모바일 생산성 앱에 대한 기타 시스템 요구 사항은 [시스템 요구 사항](#)(를) 참조하십시오.

모바일 생산성 앱에 대한 최신 정보는 [최신 공지 사항](#)(를) 참조하십시오.

다음 섹션에서는 Secure Hub의 현재 및 이전 릴리스에 포함된 새로운 기능을 나열합니다.

참고:

Secure Hub의 Android 9.x 및 iOS 11.x 버전에 대한 지원은 2025년 4월에 종료되었습니다.

현재 버전의 새로운 기능

iOS용 시큐어 허브 26.8.1

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

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제를](#)(을) 참조하십시오.

Android용 시큐어 허브 26.8.0

COSU 모드에서 런처 구성 정책에 자동 실행 앱 설정

Citrix Launcher를 실행하는 Android Enterprise 키오스크(COSU) 장치에서 관리자는 이제 런처 구성 정책에 자동 실행 앱을 설정하여 장치 부팅 시 하나의 관리되는 앱을 자동으로 시작할 수 있습니다. Secure Hub는 이 설정을 Citrix Launcher로 전달하고, Citrix Launcher가 실행을 수행합니다.

MDM 장치 인증서의 자동 감지 및 갱신

Android용 Secure Hub는 이제 유효하지 않거나, 누락되었거나, 만료된 MDM 장치 인증서를 자동으로 감지하고 백그라운드에서 갱신합니다. 이를 통해 사용자가 수동으로 인증서 문제를 해결하거나 장치를 재등록할 필요 없이 장치 연결이 복원됩니다.

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

이전 버전의 새로운 기능

iOS용 Secure Hub 버전 26.8.0

iOS/iPadOS 27 지원

iOS용 Secure Hub 26.8.0 릴리스부터 이 앱은 iOS/iPadOS 27과 호환됩니다. 장치를 iOS/iPadOS 27로 업그레이드하고 Secure Hub의 최신 버전을 계속 사용할 수 있습니다.

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

Android용 Secure Hub 버전 26.5.0

Android 17 지원

Android용 Secure Hub 26.5.0 릴리스부터 이 앱은 Android 17과 호환됩니다. 장치를 Android 17로 업그레이드하고 Secure Hub의 최신 버전을 계속 사용할 수 있습니다.

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

Android용 시큐어 허브 26.2.0

장치 인증서 문제 해결 개선

Android용 Secure Hub 26.2.0 릴리스부터 Secure Hub에는 해지되거나 유효하지 않은 클라이언트 인증서로 인해 발생하는 장치 연결 문제를 진단하고 해결하는 데 도움이 되는 셀프 서비스 장치 인증서 문제 해결 도구가 포함되어 있습니다.

인증서 문제가 감지되면 도구가 자동으로 인증서 갱신을 시도하여 연결을 복원합니다. 이 도구에 액세스하려면 [도움말 > 문제 해결 > 장치 인증서](#)로 이동하여 [문제 해결](#)을 탭합니다.

장치 인증서 문제 해결 이미지(/en-us/mobile-productivity-apps/media/device-certificate-troubleshooting.png)

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

iOS용 시큐어 허브 25.8.0

iOS 26 지원

iOS용 Secure Hub 25.8.0 릴리스부터 앱은 iOS 26에서 실행되는 장치를 지원합니다. Secure Hub 버전 25.8.0으로 업그레이드하면 iOS 26으로 업데이트된 장치에 대한 지속적인 지원 및 호환성이 보장됩니다.

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

Android용 시큐어 허브 25.10.0

16KB 메모리 페이지 크기 지원

Android용 Secure Hub 25.10.0 릴리스부터 앱은 성능을 최적화하고 Google Play 요구 사항을 준수하기 위해 16KB 메모리 페이지 크기를 지원합니다.

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

Android용 시큐어 허브 25.7.0

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

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

iOS용 시큐어 허브 25.6.0

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

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

Android용 시큐어 허브 25.4.0

Android 16 지원

Android용 Secure Hub 25.4.0 릴리스부터 이 앱은 Android 16과 호환됩니다. 장치를 Android 16으로 업그레이드하고 Secure Hub의 최신 버전을 계속 사용할 수 있습니다.

TLS 1.3 프로토콜 지원

Android용 Secure Hub 25.4.0 릴리스부터 이 앱은 Android 장치에서 TLS 1.3 프로토콜을 지원합니다. TLS 1.3은 TLS 프로토콜의 최신 버전으로, TLS 1.2에 비해 더 빠른 성능, 향상된 보안 및 사이버 공격에 대한 뛰어난 복원력을 제공합니다. 또한 TLS 1.3은 네트워크 대기 시간을 줄여 더 빠른 HTTPS 연결과 더 나은 사용자 경험을 제공합니다.

TLS 1.3에 대해 자세히 알아보려면 [전송 계층 보안\(TLS\) 프로토콜 버전 1.3](#)을 참조하십시오.

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

Android용 보안 허브 25.1.0

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

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

iOS용 보안 허브 25.1.0

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

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

iOS용 시큐어 허브 24.11.0

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

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

Android용 시큐어 허브 24.10.0

Android 15 지원

Secure Hub 버전을 24.10.0으로 업그레이드하면 Android 15로 업데이트된 장치에 대한 지속적인 지원이 보장됩니다.

버그 수정에 대한 자세한 내용은 [알려진 문제 및 해결된 문제](#)를 참조하십시오.

iOS용 시큐어 허브 24.9.0

장치 등록 프로그램에 약관 표시

iOS용 Secure Hub 24.9.0부터 관리자는 Citrix Endpoint Management(CEM)를 통해 약관 장치 정책을 구성할 수 있습니다. 구성되면 Apple의 DEP(Device Enrollment Program)를 통해 등록된 장치의 등록 프로세스 중에 **약관** 페이지가 표시됩니다. 이를 통해 사용자는 등록을 완료하기 전에 약관을 검토하고 승인하여 장치 온보딩 중 규정 준수 및 보안 조치를 강화할 수 있습니다.

Android용 시큐어 허브 24.8.0

Android 장치 규정 준수 확인 (기술 미리 보기)

참고:

이 기능은 *장치 소유자* 모드로 등록된 Android 장치에 적용됩니다.

이 릴리스부터 Secure Hub는 Citrix Endpoint Management를 통해 관리자가 구성한 정책에 대해 Android 장치의 규정 준수를 확인합니다. 이러한 규정 준수 확인에는 장치 암호 강도 보장, 필수 앱 설치 확인, 금지된 앱 제거 확인이 포함됩니다.

장치가 관리자가 설정한 정책을 준수하지 않는 것으로 확인되면 Secure Hub는 모든 앱을 잠그고 사용자에게 규정 준수 문제를 해결하여 잠금을 해제하도록 요청합니다. 장치가 규정을 준수하지 않을 경우 사용자 장치에 다음 알림이 나타납니다.

규정 미준수 알림 (/en-us/mobile-productivity-apps/media/compliance-sh-android-notification.png)

자세한 내용은 [Android 장치 규정 준수 확인](#)을 참조하십시오.

안드로이드용 Secure Hub 24.6.0

개선된 로그 수집 및 보고

Secure Hub는 Secure Hub를 열지 않고도 문제를 보고하고 로그를 원활하게 보낼 수 있는 향상된 기능을 제공합니다. 이 릴리스부터 사용자는 Secure Hub 앱 아이콘을 길게 눌러 **문제 보고** 옵션에 액세스할 수 있습니다. **문제 보고** 옵션을 클릭하면 Secure Hub가 **문제 보고** 페이지를 직접 엽니다.

문제 보고 (/en-us/mobile-productivity-apps/media/sh-report-issue.png)

아이오에스용 Secure Hub 24.5.0

iOS 17 서비스 복귀 지원

Secure Hub는 iOS 17의 Return to Service 기능을 지원하여 보다 효율적이고 안전한 Mobile Device Management (MDM) 환경을 제공합니다. 이전에는 장치를 초기화한 후 새 사용자를 위해 수동으로 구성해야 했습니다. 이제 Return to Service 기능은 회사 장치를 용도 변경하거나 개인 장치 (BYOD)를 올바른 보안 정책과 통합하는 경우에도 이 프로세스를 자동화합니다.

Return to Service 기능을 사용하면 MDM 서버가 Wi-Fi 세부 정보와 기본 MDM 등록 프로필을 포함하는 지우기 명령을 사용자 장치로 보낼 수 있습니다. 그러면 장치는 모든 사용자 데이터를 자동으로 지우고, 지정된 Wi-Fi 네트워크에 연결하며, 제공된 등록 프로필을 사용하여 MDM 서버에 다시 등록됩니다.

Android용 Secure Hub 24.3.0 버전

Samsung Knox 향상된 인증 v3 지원

Secure Hub는 이제 Samsung Enhanced Attestation v3를 지원하며, Knox attestation을 활용하여 Citrix Endpoint Management를 통해 관리되는 Samsung 장치의 보안 조치를 강화합니다. 이 고급 증명 프로토콜은 장치의 무결성 및 보안 상태를 확인하여 장치가 루팅되지 않았고 승인된 펌웨어를 실행하고 있는지 확인합니다. 이 기능은 보안 위협에 대한 필수적인 보호 계층을 제공하고 기업 보안 정책 준수를 보장합니다.

Android용 보안 허브 23.12.0

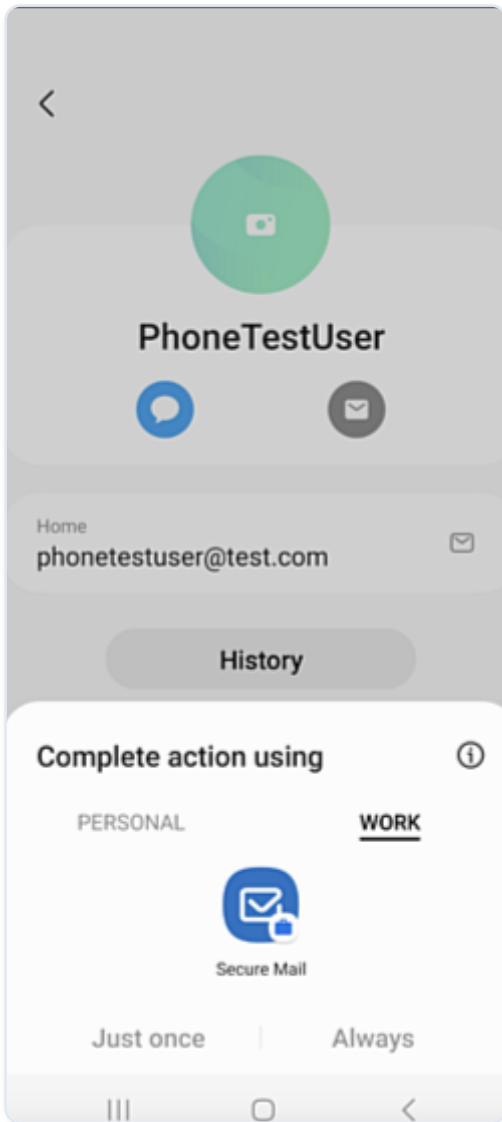
Samsung Knox로 강화된 보안

Citrix Endpoint Management에 Knox Platform for Enterprise Key 장치 정책이 추가되면서 Samsung 장치에서 Secure Hub의 보안 기능이 크게 향상되었습니다. 이 정책을 통해 필요한 Samsung Knox Platform for Enterprise(KPE) 라이선스 정보를 제공하고 KPE 라이선스를 사용하여 Samsung 장치의 보안을 강화할 수 있습니다. Samsung Knox는 관리 용이성과 원활한 사용자 경험을 유지하면서 엔터프라이즈 데이터를 보호합니다.

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

사용자 개인 프로필에서 Secure Mail 액세스

이제 사용자는 개인 프로필에서 작업 프로필의 Secure Mail에 액세스하고 사용할 수 있습니다. 사용자가 개인 프로필 주소록에서 이메일 주소를 클릭하면 작업 프로필에서 Secure Mail을 사용할 수 있는 옵션이 제공됩니다. 이 기능은 사용자가 개인 프로필에서 이메일을 보낼 수 있도록 하여 편의성을 제공합니다. 이 기능은 BYOD 또는 WPCOD 장치에 적용됩니다.



iOS용 시큐어 허브 24.1.0

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

Android용 시큐어 허브 23.12.0

로그인 페이지에 인증 PIN에 대한 힌트 추가

23.12.0 릴리스부터 로그인 페이지에 인증 PIN에 대한 힌트를 추가할 수 있습니다. 이 기능은 선택 사항이며 2단계 인증에 등록된 장치에 적용됩니다. 힌트는 PIN에 액세스하는 방법을 알려줍니다.

힌트를 텍스트 또는 링크로 구성할 수 있습니다. 힌트 텍스트는 PIN에 대한 간결한 정보를 제공하며, 링크는 PIN에 액세스하는 방법에 대한 자세한 정보를 제공합니다. 힌트 구성 방법에 대한 자세한 내용은 [Citrix Endpoint Management 콘솔을 통해 힌트 구성](#)을 참조하십시오.

nFactor 인증에서 단일 Sign-On 기능 지원

Android용 Secure Hub 버전 23.12.0부터 Mobile Application Management(MAM) 등록 또는 로그인용 nFactor는 단일 Sign-On(SSO) 기능을 지원합니다. 이 기능을 통해 이전에 입력한 로그인 자격 증명이 MAM 등록 또는 로그인 프로세스를 통과하여 사용자가 다시 수동으로 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 재부팅된 장치에서 전체 초기화 명령을 실행하려면 장치 잠금을 해제해야 했습니다. 이제 장치가 잠겨 있더라도 직접 부팅 모드에서 전체 초기화 명령을 실행할 수 있습니다. 이 기능은 특히 장치가 승인되지 않은 개인의 소유에 있을 때 보안 관점에서 유용합니다. 전체 초기화 명령에 대한 자세한 내용은 Citrix Endpoint Management 설명서의 [보안 작업](#)을 참조하십시오.

Secure Hub 앱 스토어의 로딩 속도 최적화

Secure Hub의 앱 스토어가 이전보다 빠르게 로드되어 사용자가 더 빠르게 액세스할 수 있습니다.

iOS용 보안 허브 23.11.0

로그인 페이지에 인증 PIN에 대한 힌트 추가

23.11.0 릴리스부터 로그인 페이지에 인증 PIN에 대한 힌트를 추가할 수 있습니다. 이 기능은 선택 사항이며 2단계 인증에 등록된 장치에 적용됩니다. 힌트를 통해 PIN에 액세스하는 방법을 알 수 있습니다.

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

nFactor 인증, 단일 Sign-On 기능 지원

iOS용 Secure Hub 버전 23.11.0부터 MAM(모바일 애플리케이션 관리) 등록 또는 로그인용 nFactor는 SSO(단일 Sign-On) 기능을 지원합니다. 이 기능을 통해 이전에 입력한 로그인 자격 증명이 MAM 등록 또는 로그인 프로세스를 통과하여 사용자가 다시 수동으로 입력할 필요가 없습니다.

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

보안 허브 23.10.0

Android용 시큐어 허브

Android용 Secure Hub 23.10.0은 Android 14를 지원합니다. Secure Hub 버전을 23.10.0으로 업그레이드하면 Android 14로 업데이트된 장치에 대한 지속적인 지원이 보장됩니다.

시큐어 허브 23.9.0

안드로이드용 Secure Hub

이 릴리스는 전반적인 성능과 안정성을 개선하는 영역을 다룹니다.

시큐어 허브 23.8.1

iOS용 시큐어 허브

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

시큐어 허브 23.8.0

iOS용 시큐어 허브

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

시큐어 허브 23.7.0

안드로이드용 Secure Hub

플레이 integrity API

SafetyNet Attestation API는 Google의 지원 중단 일정에 따라 곧 지원이 중단되며, 권장되는 Play Integrity API로 마이그레이션됩니다.

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

지원 중단 세부 정보는 Citrix Endpoint Management 문서의 [지원 중단 및 제거](#)를 참조하십시오.

Android SafetyNet 기능에 대해 알아보려면 [SafetyNet](#)을 참조하십시오.

시큐어 허브 23.4.0

iOS용 시큐어 허브

향상된 사용자 경험

23.4.0 버전부터 iOS용 Secure Hub는 다음 사용자 경험을 개선합니다:

- 스토어 경험:

◆ 이전에는 내 앱 페이지가 먼저 나타났습니다. 23.4.0 버전부터는 스토어 페이지가 먼저 나타납니다.

◆ 이전에는 사용자가 스토어 옵션을 클릭할 때마다 Secure Hub 스토어가 새로고침 작업을 수행했습니다.

23.4.0 버전부터 사용자 경험이 향상되었습니다. 이제 사용자가 앱을 처음 실행하거나, 앱을 다시 시작하거나, 화면을 아래로 스와이프할 때 앱이 다시 로드됩니다.

- 사용자 인터페이스: 이전에는 로그오프 옵션이 화면 왼쪽 하단에 있었습니다. 23.4.0 버전부터는 로그오프 옵션이 주 메뉴의 일부이며 정보 옵션 위에 있습니다.
- 하이퍼링크: 이전에는 앱의 세부 정보 페이지에 있는 하이퍼링크가 일반 텍스트로 나타났습니다. 23.4.0 버전부터는 하이퍼링크를 클릭할 수 있으며 링크를 나타내기 위해 밑줄 서식이 적용됩니다.

MDX에서 MAM SDK로의 전환 경험

23.4.0 버전부터 레거시 MDX에서 MAM SDK로의 전환 경험이 iOS 듀얼 모드 앱에 대해 향상되었습니다. 이 기능은 경고 메시지를 줄이고 Secure Hub로 전환하여 모바일 생산성 앱 사용 시 사용자 경험을 개선합니다.

Citrix PIN을 사용하여 앱 잠금 해제

이전에는 최종 사용자가 모바일 앱 관리(MAM) 기반 앱의 잠금을 해제하기 위해 장치 암호를 입력했습니다.

23.4.0 버전부터 최종 사용자는 Citrix PIN을 암호로 입력하여 MAM 기반 앱의 잠금을 해제할 수 있습니다. 관리자는 CEM 서버의 클라이언트 속성을 사용하여 암호의 복잡성을 구성할 수 있습니다.

앱이 허용된 시간보다 오래 비활성 상태일 때마다 최종 사용자는 관리자가 설정한 구성에 따라 Citrix PIN을 입력하여 앱의 잠금을 해제할 수 있습니다.

안드로이드용 Secure Hub의 경우, MAM 애플리케이션에서 비활성 타이머를 처리하는 방법을 구성하는 별도의 클라이언트 속성이 있습니다. 자세한 내용은 [안드로이드용 별도 비활성 타이머](#)를 참조하십시오.

시큐어 허브 23.4.1

안드로이드용 Secure Hub

이 릴리스는 전반적인 성능과 안정성을 향상하는 데 도움이 되는 몇 가지 문제를 해결합니다.

시큐어 허브 23.4.0

안드로이드용 Secure Hub

이 릴리스는 전반적인 성능과 안정성을 향상하는 데 도움이 되는 몇 가지 문제를 해결합니다.

시큐어 허브 23.2.0

안드로이드용 Secure Hub

참고:

- 유럽 연합(EU), 유럽 경제 지역(EEA), 스위스 및 영국(UK) 사용자에게 대해서는 분석 데이터가 수집되지 않습니다.

MDX 전체 터널 모드 VPN

MDX Micro VPN(전체 터널 모드)은 더 이상 사용되지 않습니다.

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

안드로이드용 별도 비활성 타이머

이전에는 **비활성 타이머** 클라이언트 속성이 Android 및 iOS용 Secure Hub에 공통으로 적용되었습니다.

23.2.0 버전부터 IT 관리자는 새로운 클라이언트 속성 **Inactivity_Timer_For_Android**를 사용하여 iOS와 비활성 타이머를 분리할 수 있습니다. IT 관리자는 **Inactivity_Timer_For_Android**의 값을 0으로 설정하여 Android 비활성 타이머를 독립적으로 비활성화할 수 있습니다. 이러한 방식으로 Secure Hub를 포함한 작업 프로필의 모든 앱은 작업 PIN만 요구합니다.

The screenshot shows the 'Add New Client Property' window. The 'Key' field is highlighted with a red border and contains the text 'INACTIVITY_TIMER_FOR_ANDROID'. Below it, the 'Value' field contains '1', the 'Name' field contains 'INACTIVITY_TIMER_FOR_ANDROID', and the 'Description' field contains 'Inactivity Timer for Android'.

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

시큐어 허브 22.11.0

안드로이드용 Secure Hub

이번 릴리스에는 버그 수정이 포함되어 있습니다.

시큐어 허브 22.9.0

안드로이드용 시큐어 허브

이번 릴리스에는 다음이 포함됩니다.

- 장치 암호의 암호 복잡성 (Android 12 이상)
- SDK 31 지원
- 버그 수정

장치 암호의 암호 복잡성 (Android 12 이상)

암호 복잡성은 사용자 지정 암호 요구 사항보다 선호됩니다. 암호 복잡성 수준은 미리 정의된 수준 중 하나입니다. 따라서 최종 사용자는 더 낮은 복잡성 수준의 암호를 설정할 수 없습니다.

Android 12 이상 기기의 암호 복잡성은 다음과 같습니다.

- **암호 복잡성 적용:** 사용자 지정 암호 요구 사항 대신 플랫폼에서 정의한 복잡성 수준의 암호가 필요합니다. Android 12 이상을 실행하고 Secure Hub 22.9 이상을 사용하는 기기에만 해당됩니다.
- **복잡성 수준:** 미리 정의된 암호 복잡성 수준입니다.
 - **없음:** 암호가 필요하지 않습니다.
 - **낮음:** 암호는 다음 중 하나일 수 있습니다.
 - 패턴
 - 최소 4자리 숫자의 PIN
 - **중간:** 암호는 다음 중 하나일 수 있습니다.
 - 반복되는 시퀀스(4444) 또는 순서가 있는 시퀀스(1234)가 없으며 최소 4자리 숫자의 PIN
 - 최소 4자의 알파벳
 - 최소 4자의 영숫자
 - **높음:** 암호는 다음 중 하나일 수 있습니다.
 - 반복되는 시퀀스(4444) 또는 순서가 있는 시퀀스(1234)가 없으며 최소 8자리 숫자의 PIN
 - 최소 6자의 알파벳
 - 최소 6자의 영숫자

참고:

- BYOD 장치의 경우 최소 길이, 필수 문자, 생체 인식 및 고급 규칙과 같은 암호 설정은 Android 12 이상에서는 적용되지 않습니다. 대신 암호 복잡성을 사용하십시오.
- 작업 프로필에 대한 암호 복잡성이 활성화된 경우 장치 측에 대한 암호 복잡성도 활성화되어야 합니다.

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

시큐어 허브 22.7.0

Android용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 22.6.0

안드로이드용 Secure Hub

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 22.5.0

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 22.4.0

안드로이드용 Secure Hub

이번 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 22.2.0

iOS용 시큐어 허브

이번 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브

이번 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.11.0

Android용 시큐어 허브

회사 소유 장치용 작업 프로필 지원

Android Enterprise 장치에서 이제 Secure Hub를 회사 소유 장치용 작업 프로필 모드로 등록할 수 있습니다. 이 기능은 Android 11 이상을 실행하는 장치에서 사용할 수 있습니다. 이전에 Corporate Owned Personally Enabled (COPE) 모드로 등록된 장치는 장치가 Android 10에서 Android 11 이상으로 업그레이드될 때 회사 소유 장치용 작업 프로필 모드로 자동 마이그레이션됩니다.

보안 허브 21.10.0

iOS용 보안 허브

이번 릴리스에는 버그 수정 사항이 포함되어 있습니다.

안드로이드용 Secure Hub

Android 12 지원. 이번 릴리스부터 Secure Hub는 Android 12를 실행하는 장치에서 지원됩니다.

시큐어 허브 21.8.0

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.7.1

안드로이드용 시큐어 허브

이미 등록된 장치에서 Android 12 지원. Android 12로 업그레이드할 계획이라면 먼저 Secure Hub를 버전 21.7.1로 업데이트해야 합니다. Secure Hub 21.7.1은 Android 12로 업그레이드하는 데 필요한 최소 버전입니다. 이 릴리스는 이미 등록된 사용자를 위해 Android 11에서 Android 12로 원활하게 업그레이드할 수 있도록 합니다.

참고:

Android 12로 업그레이드하기 전에 Secure Hub가 버전 21.7.1로 업데이트되지 않으면 장치에서 이전 기능을 복구하기 위해 재등록 또는 공장 초기화가 필요할 수 있습니다.

Citrix는 Android 12에 대한 Day 1 지원을 제공하기 위해 노력하고 있으며, Android 12를 완벽하게 지원하기 위해 Secure Hub의 후속 버전에 추가 업데이트를 제공할 예정입니다.

시큐어 허브 21.7.0

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.6.0

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.5.1

iOS를 위한 Secure Hub

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android를 위한 Secure Hub

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.5.0

iOS용 시큐어 허브

이 릴리스부터 MDX Toolkit 버전 19.8.0 이하로 래핑된 앱은 더 이상 작동하지 않습니다. 올바른 기능을 다시 시작하려면 최신 MDX Toolkit으로 앱을 래핑해야 합니다.

보안 허브 21.4.0

Secure Hub의 색상 개편. Secure Hub는 Citrix 브랜드 색상 업데이트를 준수합니다.

보안 허브 21.3.2

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.3.0

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.2.0

Android용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 21.1.0

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 20.12.0

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브

Android용 Secure Hub는 Direct Boot 모드를 지원합니다. Direct Boot 모드에 대한 자세한 내용은 [Developer.android.com](https://developer.android.com)에서 Android 설명서를 참조하십시오.

시큐어 허브 20.11.0

Android용 시큐어 허브

Secure Hub는 Android 10에 대한 Google Play의 현재 대상 API 요구 사항을 지원합니다.

시큐어 허브 20.10.5

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 20.9.0

iOS용 시큐어 허브

iOS용 Secure Hub는 iOS 14를 지원합니다.

Android용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 20.7.5

Android용 시큐어 허브

- Android용 Secure Hub는 Android 11을 지원합니다.
- **앱용 Secure Hub 32비트에서 64비트로 전환.** Secure Hub 버전 20.7.5에서는 앱용 32비트 아키텍처 지원이 종료되었으며, Secure Hub는 64비트로 업데이트되었습니다. Citrix는 고객이 20.6.5에서 20.7.5 버전으로 업그레이드할 것을 권장합니다. 사용자가 Secure Hub 버전 20.6.5로의 업그레이드를 건너뛰고 20.1.5에서 20.7.5로 직접 업데이트하는 경우, 다시 인증해야 합니다. 재인증에는 자격 증명 입력 및 Secure Hub PIN 재설정이 포함됩니다. Secure Hub 버전 20.6.5는 Google Play 스토어에서 사용할 수 있습니다.
- **App Store에서 업데이트 설치.** Android용 Secure Hub에서 앱에 대한 업데이트가 있는 경우, 해당 앱이 강조 표시되고 App Store 화면에 **사용 가능한 업데이트** 기능이 나타납니다.

사용 가능한 업데이트를 탭하면 보류 중인 업데이트가 있는 앱 목록을 보여주는 스토어로 이동합니다. 업데이트를 설치하려면 앱 옆의 **세부 정보**를 탭합니다. 앱이 업데이트되면 **세부 정보**의 아래쪽 화살표가 확인 표시로 변경됩니다.

시큐어 허브 20.6.5

Android용 시큐어 허브

앱용 32비트에서 64비트로 전환. Secure Hub 20.6.5 릴리스는 Android 모바일 앱용 32비트 아키텍처를 지원하는 마지막 릴리스입니다. 이후 릴리스에서는 Secure Hub가 64비트 아키텍처를 지원합니다. Citrix는 사용자가 Secure Hub 버전 20.6.5로 업그레이드하여 재인증 없이 이후 버전으로 업그레이드할 수 있도록 권장합니다. 사용자가 Secure Hub 버전 20.6.5로의 업그레이드를 건너뛰고 20.7.5로 직접 업데이트하는 경우, 다시 인증해야 합니다. 재인증에는 자격 증명 입력 및 Secure Hub PIN 재설정이 포함됩니다.

참고:

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

iOS용 시큐어 허브

iOS 장치에 구성된 프록시 활성화. iOS용 Secure Hub는 사용자가 **설정 > Wi-Fi**에서 구성하는 프록시 서버를 사용하도록 허용하려면 새 클라이언트 속성, `ALLOW_CLIENTSIDE_PROXY` 을(를) 활성화해야 합니다. 자세한 내용은 [클라이언트 속성 참조](#)의 `ALLOW_CLIENTSIDE_PROXY` 을(를) 참조하십시오.

시큐어 허브 20.3.0

참고:

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

iOS용 시큐어 허브

- **네트워크 확장 비활성화.** App Store 검토 지침의 최근 변경 사항으로 인해 릴리스 20.3.0부터 Secure Hub는 iOS를 실행하는 장치에서 네트워크 확장(NE)을 지원하지 않습니다. NE는 Citrix가 개발한 모바일 생산성 앱에는 영향을 미치지 않습니다. 그러나 NE 제거는 배포된 엔터프라이즈 MDX 래핑 앱에 일부 영향을 미칩니다. 최종 사용자는 인증 토큰, 타이머 및 PIN 재시도와 같은 구성 요소를 동기화하는 동안 Secure Hub로의 추가 전환을 경험할 수 있습니다.

참고:

새 사용자는 VPN 설치를 요청받지 않습니다.

- **향상된 등록 프로필 지원.** Secure Hub는 [등록 프로필 지원](#)에서 발표된 Citrix Endpoint Management용 향상된 등록 프로필 기능을 지원합니다.

시큐어 허브 20.2.0

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 20.1.5

이 릴리스에는 다음이 포함됩니다.

- 사용자 개인 정보 보호 정책 서식 및 표시 업데이트. 이 기능 업데이트는 Secure Hub 등록 흐름을 변경합니다.
- 버그 수정.

시큐어 허브 19.12.5

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 19.11.5

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 19.10.5

Android용 시큐어 허브

Secure Hub를 COPE 모드로 등록합니다. Android Enterprise 장치에서 Citrix Endpoint Management가 COPE 등록 프로필로 구성된 경우 Secure Hub를 기업 소유 개인 사용 가능(COPE) 모드로 등록합니다.

시큐어 허브 19.10.0

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 19.9.5

iOS용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브

Android Enterprise 작업 프로필 및 완전 관리형 장치에 대한 키가드 기능 관리 지원. Android 키가드는 장치 및 작업 챌린지 잠금 화면을 관리합니다. Citrix Endpoint Management의 키가드 관리 장치 정책을 사용하여 작업 프로필 장치에서 키가드 관리와 완전 관리형 및 전용 장치에서 키가드 관리를 제어합니다. 키가드 관리를 통해 사용자는 키가드 화면을 잠금 해제하기 전에 신뢰 에이전트 및 보안 카메라와 같이 사용 가능한 기능을 지정할 수 있습니다. 또는 모든 키가드 기능을 비활성화하도록 선택할 수 있습니다.

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

시큐어 허브 19.9.0

iOS용 시큐어 허브

iOS용 Secure Hub는 iOS 13을 지원합니다.

Android용 시큐어 허브

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브 19.8.5

이 릴리스에는 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 19.8.0

iOS용 시큐어 허브

이 릴리스에는 성능 향상 및 버그 수정 사항이 포함되어 있습니다.

Android용 시큐어 허브

Android Q 지원. 이 릴리스에는 Android Q 지원이 포함됩니다. Android Q 플랫폼으로 업그레이드하기 전에: Google Device Administration API의 사용 중단이 Android Q를 실행하는 장치에 미치는 영향에 대한 정보는 [장치 관리에서 Android Enterprise로 마이그레이션](#)을 참조하십시오. 또한 블로그 [Citrix Endpoint Management 및 Android Enterprise - 변화의 계절](#)도 참조하십시오.

Secure Hub 19.7.5 버전

iOS를 위한 Secure Hub

이 릴리스에는 성능 향상 및 버그 수정 사항이 포함되어 있습니다.

Android를 위한 Secure Hub

Samsung Knox SDK 3.x 지원. Android용 Secure Hub는 Samsung Knox SDK 3.x를 지원합니다. Samsung Knox 3.x로 마이그레이션하는 방법에 대한 자세한 내용은 Samsung Knox 개발자 설명서를 참조하십시오. 이 릴리스에는 새로운 Samsung Knox 네임스페이스에 대한 지원도 포함됩니다. 이전 Samsung Knox 네임스페이스 변경 사항에 대한 자세한 내용은 [이전 Samsung Knox 네임스페이스 변경 사항을 참조](#)하십시오.

참고:

Android용 Secure Hub는 Android 5를 실행하는 장치에서 Samsung Knox 3.x를 지원하지 않습니다.

Secure Hub 19.3.5에서 19.6.6까지

이 릴리스에는 성능 향상 및 버그 수정 사항이 포함되어 있습니다.

Secure Hub 19.3.0 버전

Samsung Knox Platform for Enterprise에 대한 지원이 추가되었습니다. Android용 Secure Hub는 Android Enterprise 장치에서 Knox Platform for Enterprise (KPE)를 지원합니다.

Secure Hub 19.2.0 버전

이 릴리스에는 성능 향상 및 버그 수정 사항이 포함되어 있습니다.

시큐어 허브 19.1.5

Android Enterprise용 Secure Hub는 이제 다음 정책을 지원합니다:

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

시큐어 허브 19.1.0

Secure Hub는 글꼴, 색상 및 기타 UI 개선 사항을 개편했습니다. 이러한 개선은 당사의 모든 모바일 생산성 앱 제품군에서 Citrix 브랜드 미학과 밀접하게 일치하면서 풍부한 사용자 경험을 제공합니다.

Secure Hub 18.12.0 버전

이 릴리스에는 성능 향상 및 버그 수정 사항이 포함되어 있습니다.

Secure Hub 18.11.5 버전

- **Android Enterprise용 제한 장치 정책 설정.** 제한 장치 정책의 새로운 설정을 통해 사용자는 Android Enterprise 장치에서 다음 기능에 액세스할 수 있습니다. 상태 표시줄, 잠금 화면 키가드, 계정 관리, 위치 공유, Android Enterprise 장치 화면 켜기 유지. 자세한 내용은 [제한 장치 정책](#)을 참조하십시오.

Secure Hub 18.10.5부터 18.11.0까지는 성능 향상 및 버그 수정이 포함됩니다.

시큐어 허브 18.10.0

- **Samsung DeX 모드 지원:** Samsung DeX를 사용하면 KNOX 지원 장치를 외부 디스플레이에 연결하여 PC와 유사한 인터페이스에서 앱을 사용하고, 문서를 검토하고, 비디오를 시청할 수 있습니다. Samsung DeX 장치 요구 사항 및 Samsung DeX 설정에 대한 자세한 내용은 [Samsung DeX 작동 방식](#)을 참조하십시오.

Citrix Endpoint Management에서 Samsung DeX 모드 기능을 구성하려면 Samsung Knox에 대한 제한 장치 정책을 업데이트하십시오. 자세한 내용은 [제한 장치 정책의 Samsung KNOX 설정](#)을 참조하십시오.

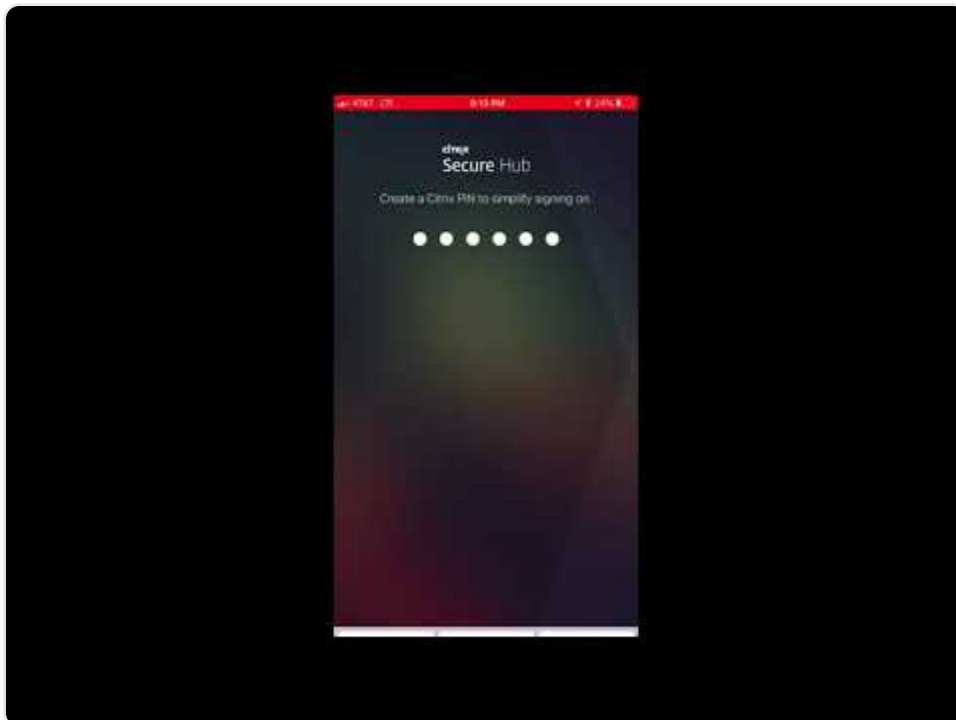
- **Android SafetyNet 지원:** Endpoint Management를 구성하여 **Android SafetyNet** 기능을 사용하여 Secure Hub가 설치된 Android 장치의 호환성 및 보안을 평가할 수 있습니다. 결과는 장치에서 자동화된 작업을 트리거하는 데 사용될 수 있습니다. 자세한 내용은 [Android SafetyNet](#)을 참조하십시오.
- **Android Enterprise 장치에서 카메라 사용 방지:** 제한 장치 정책의 새로운 **카메라 사용 허용** 설정을 통해 사용자가 Android Enterprise 장치에서 카메라를 사용하지 못하도록 할 수 있습니다. 자세한 내용은 [제한 장치 정책](#)을 참조하십시오.

시큐어 허브 10.8.60 ~ 18.9.0

이 릴리스에는 성능 향상 및 버그 수정이 포함됩니다.

시큐어 허브 10.8.60

- 폴란드어 지원.
- Android P 지원.
- Workspace 앱 스토어 사용 지원. Secure Hub를 열 때 사용자는 더 이상 Secure Hub 스토어를 볼 수 없습니다. **앱 추가** 버튼을 통해 사용자는 Workspace 앱 스토어로 이동합니다. 다음 비디오는 Citrix Workspace™ 앱을 사용하여 Citrix Endpoint Management에 등록을 수행하는 iOS 장치를 보여줍니다.



중요:

이 기능은 신규 고객에게만 제공됩니다. 현재 기존 고객을 위한 마이그레이션은 지원하지 않습니다.

이 기능을 사용하려면 다음을 구성하십시오.

- 암호 캐싱 및 암호 인증 정책을 활성화합니다. 정책 구성에 대한 자세한 내용은 [모바일 생산성 앱을 위한 MDX 정책 한눈에 보기](#)를 참조하십시오.
- Active Directory 인증을 AD 또는 AD+Cert로 구성합니다. 이 두 가지 모드를 지원합니다. 인증 구성에 대한 자세한 내용은 [도메인 또는 도메인과 보안 토큰 인증](#)을 참조하십시오.
- Endpoint Management용 Workspace 통합을 활성화합니다. Workspace 통합에 대한 자세한 내용은 [Workspace 구성](#)을 참조하십시오.

중요:

이 기능이 활성화되면 Citrix Files SSO는 Endpoint Management(이전 XenMobile®)가 아닌 Workspace를 통해 발생합니다. Workspace 통합을 활성화하기 전에 Endpoint Management 콘솔에서 Citrix Files 통합을 비활성화하는 것이 좋습니다.

보안 허브 10.8.55

- 구성 JSON을 사용하여 Google zero-touch 및 Samsung Knox Mobile Environment (KME) 포털에 사용자 이름과 암호를 전달하는 기능. 자세한 내용은 [Samsung Knox 대량 등록](#)을 참조하십시오.
- 인증서 고정을 활성화하면 사용자는 자체 서명된 인증서로 Endpoint Management에 등록할 수 없습니다. 사용자가 자체 서명된 인증서로 Endpoint Management에 등록하려고 하면 해당 인증서가 신뢰할 수 없다는 경고를 받습니다.

Secure Hub 10.8.25: Android용 Secure Hub에는 Android P 장치 지원이 포함됩니다.

참고:

Android P 플랫폼으로 업그레이드하기 전에: 서버 인프라가 subjectAltName (SAN) 확장명에 일치하는 호스트 이름이 있는 보안 인증서를 준수하는지 확인하십시오. 호스트 이름을 확인하려면 서버는 일치하는 SAN이 있는 인증서를 제시해야 합니다. 호스트 이름과 일치하는 SAN을 포함하지 않는 인증서는 더 이상 신뢰할 수 없습니다. 자세한 내용은 Android 개발자 설명서를 참조하십시오.

March 19, 2018에 Secure Hub for iOS 업데이트: iOS용 Secure Hub 버전 10.8.6은 VPP 앱 정책 문제를 해결하기 위해 제공됩니다.

Secure Hub 10.8.5: Android용 Secure Hub에서 Android Work (Android for Work)의 COSU 모드 지원. 자세한 내용은 [Citrix Endpoint Management 설명서](#)를 참조하십시오.

Secure Hub 관리

Endpoint Management의 초기 구성 중에 Secure Hub와 관련된 대부분의 관리 작업을 수행합니다. iOS 및 Android 사용자가 Secure Hub를 사용할 수 있도록 하려면 Secure Hub를 iOS App Store 및 Google Play Store에 업로드하십시오.

또한 Secure Hub는 사용자의 Citrix Gateway 세션이 Citrix Gateway를 사용하여 인증 후 갱신될 때 설치된 앱에 대해 Endpoint Management에 저장된 대부분의 MDX 정책을 새로 고칩니다.

중요:

이러한 정책 중 하나라도 변경되면 업데이트된 정책을 적용하기 위해 사용자가 앱을 삭제하고 다시 설치해야 합니다. 해당 정책은 보안 그룹, 암호화 사용, Secure Mail Exchange Server입니다.

시트릭스 핀

Secure Hub가 Citrix PIN을 사용하도록 구성할 수 있습니다. Citrix PIN은 Endpoint Management 콘솔의 **설정 > 클라이언트 속성**에서 활성화되는 보안 기능입니다. 이 설정은 등록된 모바일 장치 사용자가 Secure Hub에 로그인하고 개인 식별 번호(PIN)를 사용하여 MDX 래핑된 앱을 활성화하도록 요구합니다.

Citrix PIN 기능은 보안 래핑된 앱에 로그인할 때 사용자 인증 환경을 간소화합니다. 사용자는 Active Directory 사용자 이름 및 암호와 같은 다른 자격 증명을 반복해서 입력할 필요가 없습니다.

Secure Hub에 처음 로그인하는 사용자는 Active Directory 사용자 이름과 암호를 입력해야 합니다. 로그인하는 동안 Secure Hub는 Active Directory 자격 증명 또는 클라이언트 인증서를 사용자 장치에 저장한 다음 사용자에게 PIN을 입력하라는 메시지를 표시합니다. 사용자가 다시 로그인할 때 PIN을 입력하여 Citrix 앱 및 Store에 안전하게 액세스할 수 있으며, 이는 활성 사용자 세션에 대한 다음 유효 시간 초과 기간이 끝날 때까지 유효합니다. 관련 클라이언트 속성을 통해 PIN을 사용하여 비밀을 암호화하고, PIN의 암호 유형을 지정하고, PIN 강도 및 길이 요구 사항을 지정할 수 있습니다. 자세한 내용은 [클라이언트 속성](#)을 참조하십시오.

지문(Touch ID) 인증이 활성화되면 앱 비활성으로 인해 오프라인 인증이 필요할 때 사용자는 지문을 사용하여 로그인할 수 있습니다. 사용자는 Secure Hub에 처음 로그인할 때, 장치를 다시 시작할 때, 그리고 비활성 태이머가 만료된 후에는 여전히 PIN을 입력해야 합니다. 지문 인증 활성화에 대한 자세한 내용은 [지문 또는 Touch ID 인증](#)을 참조하십시오.

인증서 고정

iOS 및 Android용 Secure Hub는 SSL 인증서 고정을 지원합니다. 이 기능은 Citrix 클라이언트가 Endpoint Management와 통신할 때 기업에서 서명한 인증서가 사용되도록 보장하여, 장치에 루트 인증서를 설치하여 SSL 세션이 손상될 경우 클라이언트에서 Endpoint Management로의 연결을 방지합니다. Secure Hub는 서버 공개 키에 대한 변경 사항을 감지하면 연결을 거부합니다.

Android N부터 운영 체제는 더 이상 사용자가 추가한 인증 기관(CA)을 허용하지 않습니다. Citrix는 사용자가 추가한 CA 대신 공개 루트 CA를 사용할 것을 권장합니다.

Android N으로 업그레이드하는 사용자는 개인 또는 자체 서명 CA를 사용하는 경우 문제가 발생할 수 있습니다. Android N 장치에서의 연결은 다음 시나리오에서 중단됩니다.

- 개인/자체 서명 CA를 사용하고 Endpoint Management에 필요한 신뢰할 수 있는 CA 옵션이 **ON**으로 설정된 경우. 자세한 내용은 [장치 관리](#)를 참조하십시오.
- 개인/자체 서명 CA 및 Endpoint Management 자동 검색 서비스(ADS)에 연결할 수 없습니다. 보안 문제로 인해 ADS에 연결할 수 없는 경우, 초기 설정이 **꺼짐**이었다더라도 필수 신뢰 CA가 **켜짐**으로 전환됩니다.

장치를 등록하거나 Secure Hub를 업그레이드하기 전에 인증서 고정을 활성화하는 것을 고려하십시오. 이 옵션은 기본적으로 **꺼져** 있으며 ADS에서 관리합니다. 인증서 고정을 활성화하면 사용자는 자체 서명된 인증서로 Endpoint Management에 등록할 수 없습니다. 사용자가 자체 서명된 인증서로 등록하려고 하면 인증서가 신뢰할 수 없다는 경고를 받습니다. 사용자가 인증서를 수락하지 않으면 등록이 실패합니다.

인증서 고정을 사용하려면 Citrix에 Citrix ADS 서버로 인증서를 업로드하도록 요청하십시오. [Citrix 지원 포털](#)을 사용하여 기술 지원 사례를 여십시오. 개인 키를 Citrix에 보내지 않도록 하십시오. 그런 다음 다음 정보를 제공하십시오.

- 사용자가 등록하는 계정을 포함하는 도메인.
- Endpoint Management 정규화된 도메인 이름(FQDN).
- Endpoint Management 인스턴스 이름. 기본적으로 인스턴스 이름은 zdm이며 대소문자를 구분합니다.
- 사용자 ID 유형(UPN 또는 이메일). 기본적으로 유형은 UPN입니다.
- 기본 포트 8443에서 포트 번호를 변경한 경우 iOS 등록에 사용되는 포트.
- 기본 포트 443에서 포트 번호를 변경한 경우 Endpoint Management가 연결을 수락하는 포트.
- Citrix Gateway의 전체 URL.
- 선택 사항으로, 관리자의 이메일 주소.
- 도메인에 추가하려는 PEM 형식 인증서(공개 인증서여야 하며 개인 키가 아니어야 함).

- 기존 서버 인증서 처리 방법: 이전 서버 인증서를 즉시 제거할지(손상되었으므로) 또는 만료될 때까지 이전 서버 인증서를 계속 지원할지 여부.

세부 정보와 인증서가 Citrix 서버에 추가되면 기술 지원 사례가 업데이트됩니다.

인증서 + 일회용 암호 인증

Citrix ADC를 구성하여 Secure Hub가 인증서와 일회용 암호 역할을 하는 보안 토큰을 사용하여 인증하도록 할 수 있습니다. 이 구성은 장치에 Active Directory 흔적을 남기지 않는 강력한 보안 옵션을 제공합니다.

Secure Hub가 인증서 + 일회용 암호 유형의 인증을 사용하도록 설정하려면 다음을 수행하십시오. Citrix ADC에서 Citrix Gateway 로그인 유형을 나타내는 **X-Citrix-AM-GatewayAuthType: CertAndRSA** 형식의 사용자 지정 응답 헤더를 삽입하는 재작성 작업 및 재작성 정책을 추가합니다.

일반적으로 Secure Hub는 Endpoint Management 콘솔에 구성된 Citrix Gateway 로그인 유형을 사용합니다. 그러나 이 정보는 Secure Hub가 처음 로그인을 완료할 때까지 Secure Hub에서 사용할 수 없습니다. 따라서 사용자 지정 헤더가 필요합니다.

참고:

Endpoint Management와 Citrix ADC에 다른 로그인 유형이 설정된 경우 Citrix ADC 구성이 재정의됩니다. 자세한 내용은 [Citrix Gateway 및 Endpoint Management](#)를 참조하십시오.

1. Citrix ADC에서 **Configuration > AppExpert > Rewrite > Actions**로 이동합니다.
2. **Add**를 클릭합니다.

Create Rewrite Action 화면이 나타납니다.

3. 다음 그림에 표시된 대로 각 필드를 채운 다음 **Create**를 클릭합니다.

Create Rewrite Action

Name*
InsertGatewayAuthTypeHeader ?

Type*
INSERT_HTTP_HEADER ▼

Use this action type to insert a header.

Header Name*
X-Citrix-AM-GatewayAuthType

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** 화면에 다음 결과가 나타납니다.

NetScaler > AppExpert > Rewrite > Rewrite Actions

Add Edit Delete Action ▼ 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. 재작성 작업을 재작성 정책으로 가상 서버에 바인딩합니다. **Configuration > NetScaler® Gateway > Virtual Servers**로 이동한 다음 가상 서버를 선택합니다.

Dashboard Configuration Reporting Documentation Downloads

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action ▼ Search ▼

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	Up	10.71.12.30	500	SSL	0	0	0

Integrate with Citrix Products

- XenMobile
- XenApp and XenDesktop
- Unified Gateway

5. **Edit**를 클릭합니다.
6. 가상 서버 구성 화면에서 아래로 스크롤하여 **정책**으로 이동합니다.
7. 정책을 추가하려면 **++**를 클릭합니다.

The screenshot shows the 'Profiles' configuration page. The 'Profiles' section lists Net Profile, TCP Profile, and HTTP Profile (nshttp_default_strict_validation). The 'Published Applications' section lists 'No Next HOP Server', '1 STA Server', and 'No Url'. The 'Other Settings' section includes ICMP Virtual Server Response (Passive), RHI State (Passive), Redirect to Home page (true), Listen Priority (NONE), Listen Policy Expression (NONE), ShareFile, AppController (https://camamappc8.camam.net:8443), and L2 Connection (false). The 'Policies' section has a '+' button highlighted by a hand icon, indicating where to click to add a new policy. The 'Request Policies' section lists '3 Session Policies', '2 ClientlessAccess Policies', and '5 Cache Policies'. A 'Done' button is at the bottom left.

8. 정책 선택 필드에서 **재작성**을 선택합니다.
9. 유형 선택 필드에서 **응답**을 선택합니다.

The screenshot shows the 'Choose Type' dialog box. It has a title bar 'Choose Type' and a subtitle 'Choose Type'. Under the 'Policies' section, there are two dropdown menus: 'Choose Policy*' with 'Rewrite' selected and 'Choose Type*' with 'Response' selected. At the bottom, there are two buttons: 'Continue' (highlighted by a hand icon) and 'Cancel'.

10. 계속을 클릭합니다.

정책 바인딩 섹션이 확장됩니다.

Choose Type

Choose Type

Policies

Choose Policy: Rewrite

Choose Type: Response

Policy Binding

Select Policy*
Click to select

Binding Details

Priority*: 100

Goto Expression*: END

Bind Close

11. 정책 선택을 클릭합니다.

사용 가능한 정책이 있는 화면이 나타납니다.

Choose Type > Rewrite Policies

Rewrite Policies

Select Add Edit Delete Show Bindings Policy Manager Statistics Action

Show built-in Rewrite Policies Search

Name	Expression	Action	Undefined-Result Action	Hits	Undefined Hits	Active
InsertGatewayAuthTypePolicy	true	InsertGatewayAuthTypeHeader	Use Global	0	0	X

12. 생성한 정책의 행을 클릭한 다음 선택을 클릭합니다. 정책 바인딩 화면이 다시 나타나고 선택한 정책이 채워집니다.

13. 바인딩을 클릭합니다.

바인딩이 성공하면 완료된 재작성 정책이 표시된 기본 구성 화면이 나타납니다.

성공적인 바인딩 이미지(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-bind-successful.png)

14. 정책 세부 정보를 보려면 **재작성 정책**을 클릭합니다.

재작성 정책 세부 정보 이미지(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-rewrite-policy.png)

Android 장치용 ADS 연결을 위한 포트 요구 사항

포트 구성은 Secure Hub에서 연결하는 Android 장치가 회사 네트워크 내에서 Citrix ADS에 액세스할 수 있도록 합니다. ADS를 통해 제공되는 보안 업데이트를 다운로드할 때 ADS에 액세스하는 기능은 중요합니다. ADS 연결은 프록시 서버와 호환되지 않을 수 있습니다. 이 시나리오에서는 ADS 연결이 프록시 서버를 우회하도록 허용합니다.

중요:

Android 및 iOS용 Secure Hub는 Android 장치가 ADS에 액세스하도록 허용해야 합니다. 자세한 내용은 Citrix Endpoint Management 설명서의 [포트 요구 사항](#)을 참조하십시오. 이 통신은 아웃바운드 포트 443에서 이루어집니다. 기존 환경은 이 액세스를 허용하도록 설계되었을 가능성이 높습니다. 이 통신을 보장할 수 없는 고객은 Secure Hub 10.2로 업그레이드하지 않는 것이 좋습니다. 질문이 있는 경우 Citrix 지원팀에 문의하십시오.

사전 요구 사항:

- Endpoint Management 및 Citrix ADC 인증서를 수집합니다. 인증서는 PEM 형식이어야 하며 개인 키가 아닌 공개 인증서여야 합니다.
- Citrix 지원팀에 문의하여 인증서 고정 활성화 요청을 제출하십시오. 이 과정에서 인증서를 요청받게 됩니다.

새로운 인증서 고정 개선 사항은 장치가 등록되기 전에 ADS에 연결해야 합니다. 이 사전 요구 사항은 장치가 등록되는 환경에 대한 최신 보안 정보가 Secure Hub에서 사용 가능하도록 보장합니다. 장치가 ADS에 연결할 수 없는 경우 Secure Hub는 장치 등록을 허용하지 않습니다. 따라서 내부 네트워크 내에서 ADS 액세스를 개방하는 것은 장치 등록을 가능하게 하는 데 중요합니다.

Android용 Secure Hub의 ADS에 대한 액세스를 허용하려면 다음 IP 주소 및 FQDN에 대해 포트 443을 엽니다.

FQDN	IP 주소	포트	IP 및 포트 사용
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	Secure Hub - ADS 통신
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	Secure Hub - ADS 통신
<code>ads.xm.cloud.com</code> : Secure Hub 버전 10.6.15 이상에서는 <code>ads.xm.cloud.com</code> 를 사용합니다.	34.194.83.188	443	Secure Hub - ADS 통신
<code>ads.xm.cloud.com</code> : Secure Hub 버전 10.6.15 이상에서는	34.193.202.23	443	시큐어 허브 - ADS 통신

FQDN	IP 주소	포트	IP 및 포트 사용
ads.xm.cloud.com 를 사용합니다.			

인증서 고정이 활성화된 경우:

- 시큐어 허브는 장치 등록 중에 엔터프라이즈 인증서를 고정합니다.
- 업그레이드 중 시큐어 허브는 현재 고정된 인증서를 폐기하고, 등록된 사용자의 첫 연결 시 서버 인증서를 고정합니다.

참고:

업그레이드 후 인증서 고정을 활성화하는 경우, 사용자는 다시 등록해야 합니다.

- 인증서 공개 키가 변경되지 않은 경우, 인증서 갱신 시 재등록이 필요하지 않습니다.

인증서 고정은 리프 인증서를 지원하며, 중간 또는 발급자 인증서는 지원하지 않습니다. 인증서 고정은 Endpoint Management 및 Citrix Gateway와 같은 Citrix 서버에 적용되며, 타사 서버에는 적용되지 않습니다.

계정 삭제 옵션 비활성화

자동 검색 서비스(ADS)가 활성화된 환경에서 시큐어 허브의 **계정 삭제** 옵션을 비활성화할 수 있습니다.

계정 삭제 옵션을 비활성화하려면 다음 단계를 수행하십시오.

1. 도메인에 대해 ADS를 구성합니다.
2. Citrix Endpoint Management에서 **자동 검색 서비스 정보**를 열고 `displayReenrollLink` 값을 **False**로 설정합니다. 기본적으로 이 값은 **True**입니다.
3. 장치가 MDM+MAM(ENT) 모드로 등록된 경우, 변경 사항을 적용하려면 로그오프했다가 다시 로그인하십시오. 장치가 다른 모드로 등록된 경우, 장치를 다시 등록해야 합니다.

Secure Hub 사용

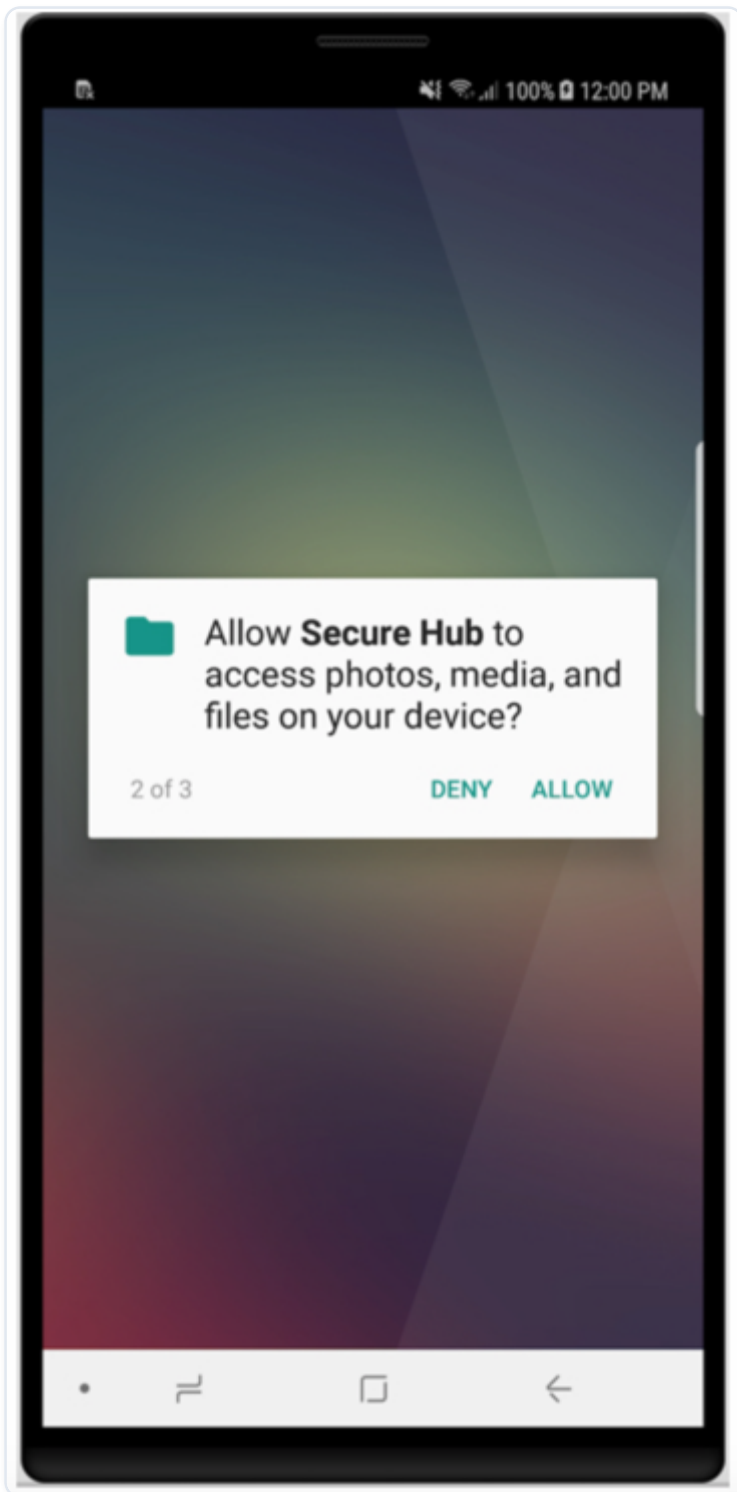
사용자는 Apple 또는 Android 스토어에서 Secure Hub를 장치에 다운로드하는 것으로 시작합니다.

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

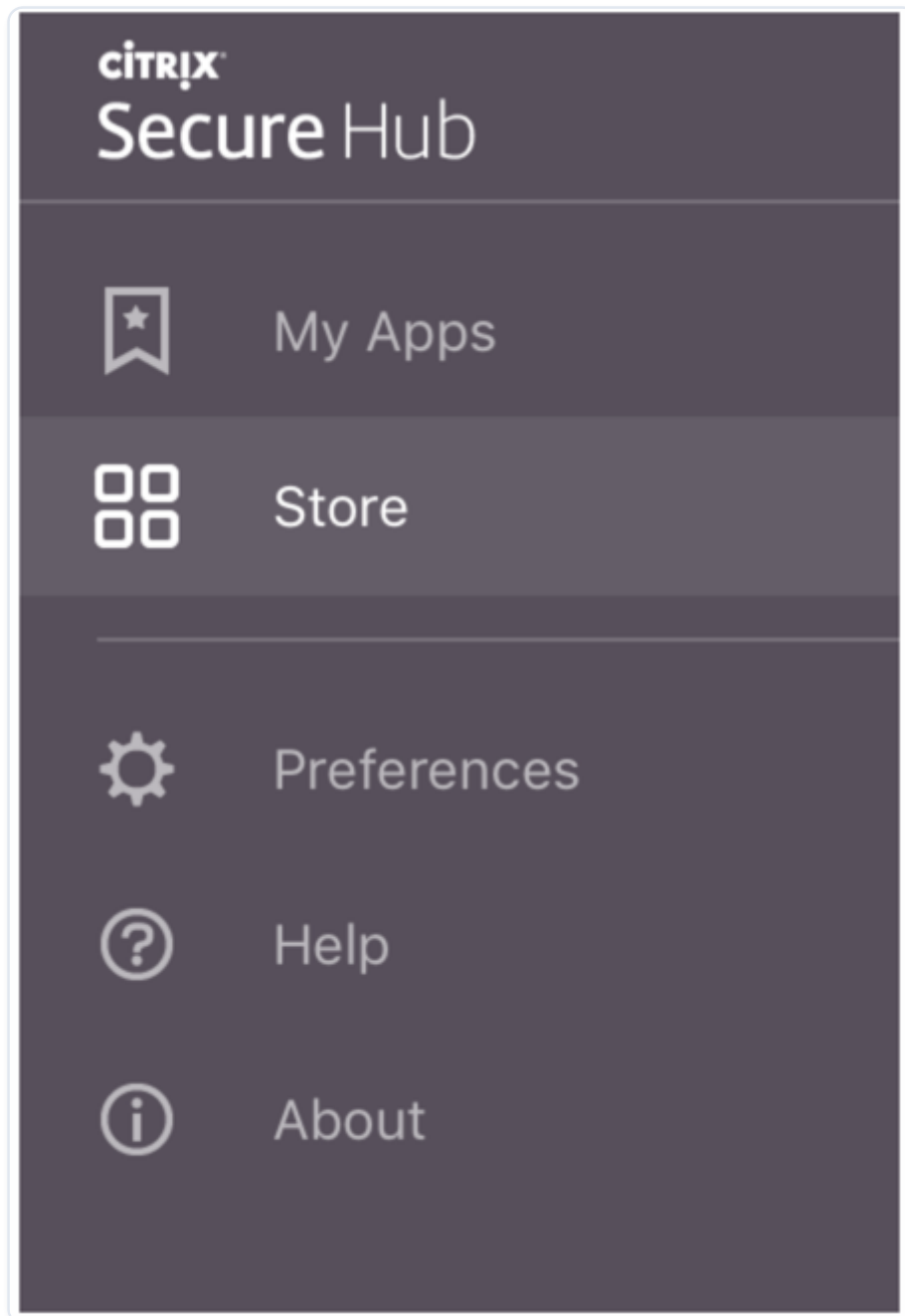
Android용 Secure Hub에서 초기 설치 및 등록 중에 다음 메시지가 나타납니다. Secure Hub가 장치의 사진, 미디어 및 파일에 액세스하도록 허용하시겠습니까?

이 메시지는 Android 운영 체제에서 오는 것이며 Citrix에서 오는 것이 아닙니다. **허용**을 탭하더라도 Citrix 및 Secure Hub를 관리하는 관리자는 사용자의 개인 데이터를 언제든지 볼 수 없습니다. 그러나 관리자와 원격 지원 세션을 수행하는 경우, 관리자는 세션 내에서 사용자의 개인 파일을 볼 수 있습니다.

등록되면 사용자는 **내 앱** 탭에서 푸시한 모든 앱과 데스크톱을 볼 수 있습니다. 사용자는 스토어에서 더 많은 앱을 추가할 수 있습니다. 휴대폰에서는 스토어 링크가 왼쪽 상단 모서리에 있는 **설정** 햄버거 아이콘 아래에 있습니다.



태블릿에서는 스토어가 별도의 탭으로 표시됩니다.



iOS 9 이상을 실행하는 iPhone 사용자가 스토어에서 모바일 생산성 앱을 설치하면 메시지가 표시됩니다. 이 메시지는 엔터프라이즈 개발자인 Citrix가 해당 iPhone에서 신뢰할 수 없다고 명시합니다. 이 메시지는 개발자가 신뢰할 수 있을 때까지 앱을 사용할 수 없다고 알립니다. 이 메시지가 나타나면 Secure Hub는 사용자에게 iPhone용 Citrix 엔터프라이즈 앱을 신뢰하는 과정을 안내하는 가이드를 보도록 요청합니다.

Secure Mail 자동 등록

MAM 전용 배포의 경우, Endpoint Management를 구성하여 이메일 자격 증명을 사용하여 Secure Hub에 등록하는 Android 또는 iOS 장치 사용자가 Secure Mail에 자동으로 등록되도록 할 수 있습니다. 사용자는 Secure Mail에 등록하기 위해 추가 정보를 입력하거나 추가 단계를 수행할 필요가 없습니다.

Secure Mail을 처음 사용할 때 Secure Mail은 Secure Hub에서 사용자의 이메일 주소, 도메인 및 사용자 ID를 가져옵니다. Secure Mail은 자동 검색을 위해 이메일 주소를 사용합니다. Exchange Server는 도메인 및 사용자 ID를 사용하여 식별되며, 이를 통해 Secure Mail은 사용자를 자동으로 인증할 수 있습니다. 정책이 암호를 통과하지 않도록 설정된 경우 사용자에게 암호를 입력하라는 메시지가 표시됩니다. 그러나 사용자는 추가 정보를 입력할 필요가 없습니다.

이 기능을 활성화하려면 세 가지 속성을 생성하십시오.

- 서버 속성 MAM_MACRO_SUPPORT. 지침은 [서버 속성\(를\)](#) 참조하십시오.
- 클라이언트 속성 ENABLE_CREDENTIAL_STORE 및 SEND_LDAP_ATTRIBUTES. 지침은 [클라이언트 속성\(를\)](#) 참조하십시오.

사용자 지정 Store

Store를 사용자 지정하려면 **설정 > 클라이언트 브랜딩**으로 이동하여 이름을 변경하고 로고를 추가하며 앱이 표시되는 방식을 지정하십시오.

클라이언트 브랜딩 이미지의 이미지(/en-us/mobile-productivity-apps/media/worxhome-client-branding.png)

Endpoint Management 콘솔에서 앱 설명을 편집할 수 있습니다. **구성**을 클릭한 다음 **앱**을 클릭합니다. 테이블에서 앱을 선택한 다음 **편집**을 클릭합니다. 편집 중인 설명이 있는 앱의 플랫폼을 선택한 다음 **설명** 상자에 텍스트를 입력합니다.

설명 상자의 이미지(/en-us/mobile-productivity-apps/media/worxhome-edit-app-descriptions-xm.png)

Store에서 사용자는 Endpoint Management에서 구성하고 보호한 앱 및 데스크톱만 찾아볼 수 있습니다. 앱을 추가하려면 사용자는 **세부 정보**를 탭한 다음 **추가**를 탭합니다.

구성된 도움말 옵션

Secure Hub는 사용자에게 도움을 받을 수 있는 다양한 방법을 제공합니다. 태블릿에서 오른쪽 상단 모서리에 있는 물음표를 탭하면 도움말 옵션이 열립니다. 휴대폰에서 사용자는 왼쪽 상단 모서리에 있는 햄버거 메뉴 아이콘을 탭한 다음 **도움말**을 탭합니다.

도움말 화면의 이미지(/en-us/mobile-productivity-apps/media/secure-hub-helpdesk.png)

IT 부서에는 사용자가 앱에서 직접 액세스할 수 있는 회사 헬프 데스크의 전화번호와 이메일이 표시됩니다. Endpoint Management 콘솔에서 전화번호와 이메일 주소를 입력합니다. 오른쪽 상단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. **설정** 페이지가 나타납니다. **자세히**를 클릭한 다음 **클라이언트 지원**을 클릭합니다. 정보를 입력하는 화면이 나타납니다.

클라이언트 지원 화면의 이미지(/en-us/mobile-productivity-apps/media/worxhome-edit-client-support-xm.png)

문제 보고는 앱 목록을 표시합니다. 사용자는 문제가 있는 앱을 선택합니다. Secure Hub는 자동으로 로그를 생성한 다음 로그가 zip 파일로 첨부된 Secure Mail 메시지를 엽니다. 사용자는 문제의 제목과 설명을 추가합니다. 스크린샷을 첨부할 수도 있습니다.

Citrix에 피드백 보내기는 Citrix 지원 주소가 채워진 Secure Mail 메시지를 엽니다. 메시지 본문에서 사용자는 Secure Mail 개선을 위한 제안을 입력할 수 있습니다. Secure Mail이 장치에 설치되어 있지 않으면 기본 메일 프로그램이 열립니다.

사용자는 **Citrix Support**를 탭할 수도 있으며, 그러면 **Citrix Knowledge Center**가 열립니다. 여기에서 모든 Citrix 제품에 대한 지원 문서를 검색할 수 있습니다.

기본 설정에서 사용자는 자신의 계정 및 장치에 대한 정보를 찾을 수 있습니다.

위치 정책

Secure Hub는 예를 들어 회사 소유 장치가 특정 지리적 경계를 벗어나지 않도록 하려는 경우 지리적 위치 및 지리적 추적 정책도 제공합니다. 자세한 내용은 **위치 장치 정책**을 참조하십시오.

충돌 수집 및 분석

Secure Hub는 실패 정보를 자동으로 수집하고 분석하여 특정 실패의 원인을 파악할 수 있도록 합니다. Crashlytics 소프트웨어가 이 기능을 지원합니다.

iOS 및 Android에서 사용할 수 있는 더 많은 기능에 대해서는 **Citrix Secure Hub**의 플랫폼별 기능 매트릭스를 참조하십시오.

Secure Hub용 장치 측 로그 생성

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

Secure Mail 로그를 얻으려면 다음을 수행하십시오.

1. **Secure Hub > 도움말 > 문제 보고**로 이동합니다. 앱 목록에서 Secure Mail을 선택합니다. 조직의 헬프 데스크로 보내는 이메일이 열립니다.
2. 지원 팀에서 지시한 경우에만 로그 설정을 변경하십시오. 항상 설정이 올바르게 지정되었는지 확인하십시오.
3. Secure Mail로 돌아가 문제를 재현합니다. 문제가 재현되기 시작한 시간과 문제가 발생하거나 오류 메시지가 표시되는 시간을 기록합니다.

4. **Secure Hub > 도움말 > 문제 보고**로 돌아갑니다. 앱 목록에서 Secure Mail을 선택합니다. 조직의 헬프 데스크로 보내는 이메일이 열립니다.
5. 제목과 본문에 문제에 대한 간략한 설명을 입력합니다. 3단계에서 수집한 타임스탬프를 포함하고 **보내기**를 클릭합니다. 압축된 로그 파일이 첨부된 완성된 메시지가 열립니다.
6. 다시 **보내기**를 누릅니다.

전송된 zip 파일에는 다음 로그가 포함됩니다.

- CtxLog_AppInfo.txt (아이오에스), Device_And_AppInfo.txt (안드로이드), logx.txt, 및 WH_logx.txt (윈도우 폰)

앱 정보 로그에는 장치 및 앱에 대한 정보가 포함됩니다.

알려진 문제 및 해결된 문제

Citrix®는 모바일 생산성 앱의 지난 두 버전에서 업그레이드를 지원합니다.

iOS용 시큐어 허브 26.8.1

해결된 문제

- Citrix Workspace 앱을 통해 iOS용 Secure Hub에서 HDX 앱을 실행할 때 앱이 실행되지 않을 수 있습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Android용 시큐어 허브 26.8.0

해결된 문제

- Android Enterprise 제한 정책에서 특정 시스템 앱 허용 목록을 구성하면 **모두#** 설정이 재정의되어 이미 허용 목록에 있는 시스템 앱이 다시 숨겨질 수 있습니다.
- Android Enterprise 키오스크(COSU) 장치에서 장치가 지오펜스 경계를 벗어났을 때 Secure Hub가 적용한 장치 잠금 PIN이 장치가 허용된 영역으로 돌아온 후에도 제거되지 않을 수 있습니다. 결과적으로 장치는 계속 PIN을 요청하며, 관리자는 콘솔에서 PIN을 검색하여 장치를 수동으로 잠금 해제해야 합니다.
- Android 16 및 Android 17을 실행하는 장치(One UI 8.5를 실행하는 Samsung 장치 포함)에서 완전 관리형 장치 또는 전용 장치 등록이 완료된 후에도 장치가 잠금 작업(키오스크) 모드로 유지될 수 있습니다. 결과적으로 사용자는 Secure Hub 화면을 벗어날 수 없으며, 등록이 불완전하게 표시되고 장치를 다시 시작해야 합니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 시큐어 허브 26.8.0

해결된 문제

- Microsoft 인증 라이브러리(MSAL) 로그아웃을 호출할 때, 경쟁 조건 또는 교착 상태로 인해 Secure Hub이(가) 충돌할 수 있습니다.
- `mam-app-data-sharing` 기능 플래그가 활성화된 경우 Secure Mail 및 Secure Web이(가) 처음 사용할 때 실패할 수 있습니다.
- DEP 장치에서 보안 앱에 의해 트리거된 선택적 초기화 중에 MDM 프로필이 삭제되지 않을 수 있습니다.
- 사용자가 Secure Hub에서 피드백을 제출할 때, 피드백이 오래된 지원 이메일 주소로 전송될 수 있습니다.
- 계정이 삭제된 후에도 PIN 팝업이 계속 표시될 수 있습니다.
- 로그 전송 버튼을 탭해도 응답하지 않을 수 있습니다.
- Secure Hub에 불필요한 `NSAppleMusicUsageDescription` 권한이 포함될 수 있습니다.
- 2100개 이상의 라이선스를 보유한 테넌트의 경우, VPP(Volume Purchase Program) 앱을 설치할 때 앱을 설치하는 대신 사용자를 App Store로 리디렉션할 수 있습니다.
- 공유 키체인 저장소를 로드하는 동안 Secure Hub이(가) SIGABRT 오류와 함께 충돌할 수 있습니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

Android용 시큐어 허브 26.5.0

해결된 문제

ADS 서버 URL에 잘못된 포트 값이 포함된 경우 Secure Hub 자동 검색이 실패할 수 있습니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

안드로이드용 시큐어 허브 26.2.0

해결된 문제

이 버전은 전반적인 성능과 안정성을 향상시키는 영역을 다룹니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

안드로이드용 시큐어 허브 25.10.0

해결된 문제

필수 앱이 설치되지 않아 정책 배포가 차단 해제되지 않을 경우, Secure Hub는 CEM 서버에 배포 실패를 보고합니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

iOS용 보안 허브 25.8.0

해결된 문제

- 모바일 애플리케이션 관리(MAM) 앱 데이터 공유 기능 플래그를 켜고 끌 때, 일부 MAM 앱에서 "앱이 제거되었습니다"라는 팝업 알림이 표시될 수 있습니다.
- Secure Hub 등록을 취소하면 일부 MAM 앱을 계속 사용할 수 있습니다.
- Secure Hub에서 MAM 앱의 로그 설정을 변경하면 변경 사항이 적용되지 않을 수 있습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Android용 보안 허브 25.7.0

해결된 문제

이 버전은 전반적인 성능과 안정성을 개선하는 영역을 다룹니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 보안 허브 25.6.0

해결된 문제

- Secure Hub 앱을 사용할 때 간헐적인 충돌이 발생하거나 여러 번 다시 시도한 후에도 스토어에 액세스할 때 “스토어를 로드할 수 없습니다. 다시 시도하십시오.”라는 오류 메시지가 나타날 수 있습니다.
- MDM(모바일 장치 관리) 전용 모드에서 DEP(장치 등록 프로그램) 또는 RTS(서비스 복귀)를 사용하는 경우 프로세스가 지원되지 않을 수 있습니다.
- 온프레미스 Active Directory에 의해 등록된 장치의 Azure Active Directory(AAD) 등록 중에 오류가 발생할 수 있습니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

Android용 보안 허브 25.4.0

해결된 문제

사용자가 장치를 먼저 초기화하고 CEM 콘솔에서 삭제하지 않고 동일한 장치를 다시 등록하면 서비스가 비활성화된 경우 정책을 수동으로 새로 고칠 수 없습니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

iOS용 시큐어 허브 25.1.0

해결된 문제

이 버전은 전반적인 성능과 안정성을 개선하는 영역을 다룹니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

Android용 시큐어 허브 25.1.0

해결된 문제

이 버전은 전반적인 성능과 안정성을 개선하는 영역을 다룹니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 보안 허브 24.11.0

해결된 문제

iOS 장치가 이미 DEP(장치 등록 프로그램)에 등록되어 있음에도 불구하고 Secure Hub를 열 때 사용자에게 UPN(사용자 계정 이름)을 입력하라는 메시지를 표시합니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Android용 보안 허브 24.10.0

해결된 문제

이 릴리스에는 해결된 문제가 없습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 보안 허브 24.9.0

해결된 문제

이 릴리스에는 해결된 문제가 없습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

안드로이드용 시큐어 허브 24.8.0

해결된 문제

이 릴리스에는 해결된 문제가 없습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

안드로이드용 시큐어 허브 24.6.0

해결된 문제

이 릴리스에는 해결된 문제가 없습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 시큐어 허브 24.5.0

해결된 문제

이 릴리스에는 해결된 문제가 없습니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

Android용 Secure Hub 버전 24.3.0

해결된 문제

공장 초기화 제한 정책이 '아니요'로 설정되어 있어도 사용자는 회사 소유의 Android Enterprise 장치에서 공장 초기화를 수행할 수 있습니다. 이 문제는 사용자가 Secure Hub를 다시 시작할 때 발생합니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

iOS용 Secure Hub 버전 24.1.0

해결된 문제

- Palera1n 앱으로 iOS 장치를 탈옥하면 Citrix Endpoint Management™ 서버가 해당 장치를 탈옥된 것으로 감지하지 못합니다. 결과적으로 Endpoint Management 서버는 탈옥된 장치를 공장 초기화할 수 없습니다. 또한 Endpoint Management 서버는 서버 콘솔에서 탈옥된 장치 항목을 지울 수 없습니다.

- MAM SDK를 사용하여 iOS 앱을 관리할 때 Secure Hub 스토어에서 다음 문제 중 하나가 발생합니다.
 - 앱 업데이트가 있을 때 알림을 보내지 않습니다.
 - 앱이 업데이트된 후에도 업데이트에 대해 계속 알림을 보냅니다.
- MAM SDK를 사용하여 iOS 앱을 관리할 때 다음 규정 준수 경고가 나타날 수 있습니다.

"이 앱이 계정에서 제거되었습니다. 장치에서 제거할 수 있습니다."

MAM SDK와 MDX 툴킷을 동일한 iOS 장치에 모두 설치할 때 이 문제가 발생합니다.

Android용 시큐어 허브 23.12.0

해결된 문제

Citrix Gateway 자격 증명이 만료되면 Secure Hub가 Citrix Gateway 서버에 연결하기 위한 새 인증서를 생성하지 못할 수 있습니다. 결과적으로 Secure Hub는 다음 오류 메시지와 함께 시작되지 않습니다.

"연결에 오류가 발생했습니다. 다시 연결해 보세요."

iOS용 시큐어 허브 23.11.0

해결된 문제

- Citrix Gateway 클라이언트 인증서가 만료될 때 자동으로 갱신되지 않아 iOS 장치에서 Secure Hub 인증이 실패합니다. 이 문제는 Citrix Gateway가 TLSv1.3 프로토콜을 사용할 때 발생합니다.
- Citrix Gateway를 통해 Secure Hub에 로그인할 때 다음 오류 메시지가 나타날 수 있습니다.

"로그인할 수 없습니다. 자격 증명이 올바르지 않습니다. 세션을 종료합니다."

nFactor를 사용하여 iOS 장치를 Citrix Endpoint Management(CEM)에 등록할 때 이 문제가 발생합니다.

Android용 시큐어 허브 23.10.0

해결된 문제

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

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Android용 시큐어 허브 23.9.0

해결된 문제

이 릴리스는 전반적인 성능과 안정성을 개선하는 영역을 다룹니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 Secure Hub의 23.8.1 버전

해결된 문제

- 사용자가 Secure Hub 23.8.0을 사용하여 장치를 등록하려고 시도하고 사용자 이름이 `sAMAccount` 형식인 경우, 다음 오류 메시지와 함께 프로세스가 실패할 수 있습니다.

"등록 실패, MAM 로그인 사용자가 등록된 사용자와 일치하지 않습니다. 다시 등록해 주십시오."

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 Secure Hub의 23.8.0 버전

해결된 문제

- nFactor를 사용하여 Citrix Endpoint Management(CEM)에 iOS 장치를 등록할 때 마이크로 VPN 터널을 설정하는 데 문제가 발생할 수 있습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

이전 버전의 알려진 문제 및 해결된 문제

Secure Hub 이전 버전의 알려진 문제 및 해결된 문제에 대한 자세한 내용은 [Secure Hub 알려진 문제 및 해결된 문제 기록](#)을 참조하십시오.

Secure Hub 알려진 문제 및 해결된 문제 기록

이 문서에는 최근 지원되는 버전 이전의 Secure Hub 버전에 대한 해결된 문제 및 알려진 문제가 나열되어 있습니다. 최신 설명서는 [Citrix Secure Hub](#)를 참조하십시오.

Android용 보안 허브 23.7.0

해결된 문제

- Android Enterprise 플랫폼에서 등록 후 관리 구성 정책이 장치에 적용되지 않을 수 있습니다.
- Android Enterprise 플랫폼에서 등록 후 필요한 공용 앱 스토어 앱이 장치에 자동으로 설치되지 않을 수 있습니다.
- 장치를 재부팅하고 잠금 해제하지 않으면 IT 관리자가 발행한 잠금 명령을 통해 장치 암호를 재설정하지 못할 수 있습니다.

이 방법은 최종 사용자가 장치 암호를 잊어버리거나 장치를 분실한 경우 관리자에게 장치 암호를 재설정하거나 잠금 명령을 통해 장치를 잠그도록 요청할 수 있으므로 유용합니다.

- 최종 사용자가 등록을 위해 특정 Android 장치에서 Secure Hub를 열면 Secure Hub 앱이 응답하지 않습니다.

이 문제는 라이선스 만료로 인해 MDM 등록이 실패할 때 발생합니다. 결과적으로 Secure Mail 앱을 사용할 수 없습니다.

- 인증 목적으로 Citrix Gateway를 ID 공급자(IdP)로 구성하고 게이트웨이에 대한 네트워크 연결이 불안정하면 인증이 실패하고 최종 사용자가 Secure Hub에 로그인할 수 없습니다.

알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

iOS용 보안 허브 23.4.0

해결된 문제

이번 릴리스에서는 전반적인 성능과 안정성을 개선하는 데 도움이 되는 몇 가지 문제가 해결되었습니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

안드로이드용 Secure Hub 23.4.1

해결된 문제

- Secure Hub 앱을 시작할 때 로딩 스피너 UI가 나타납니다. 이 문제는 교착 상태로 인해 발생합니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

안드로이드용 Secure Hub 23.4.0

해결된 문제

- 기기를 Android 11에서 Android 12로, 그리고 Android 13으로 업그레이드한 후 Secure Hub 앱이 시작되지 않습니다.
- 기업 소유 단일 용도(COSU) 장치에 등록한 후 Secure Hub 앱이 Citrix PIN 대신 Active Directory(AD) 암호를 요청합니다. 이 문제는 Secure Hub 버전 23.2.0 이하에서 캐시된 자격 증명이 손실되어 발생할 수 있습니다.
- 코드의 예외로 인해 PIN이 허용되지 않아 Secure Hub 앱이 응답하지 않습니다.

알려진 문제

이번 릴리스에는 알려진 문제가 없습니다.

Android용 시큐어 허브 23.2.0

해결된 문제

- 기업 소유 단일 용도(COSU) 장치에 등록하고 제한 정책에서 SD 카드 사용을 허용하더라도 해당 장치에서 외부 SD 카드에 액세스하지 못할 수 있습니다. 이 문제는 전용 장치이기 때문에 발생합니다.
- Android Enterprise 장치에서 암호 만료에 대한 암호 정책 설정이 예상대로 작동하지 않습니다. 암호 변경 프롬프트가 나타나지 않습니다. 대신 암호를 수동으로 변경해야 합니다.
- 가끔 장치를 Android 11에서 Android 13으로 업그레이드한 후 Secure Hub 앱이 응답하지 않습니다.

- Secure Hub에 로그인할 때마다 앱이 Citrix PIN 대신 Active Directory(AD) 암호를 요청합니다. 이 문제는 AD 암호를 변경한 후에 발생합니다.
- Active Directory(AD) 암호를 변경한 후 Secure Hub에 로그인하려는 시도가 다음 오류 메시지와 함께 실패합니다.

잘못된 자격 증명입니다.

시큐어 허브 22.11.0

- CEM 콘솔에서 **등록 앱** 채널로 푸시 메시지를 보낼 때 메시지는 장치에 도착하지만 소리 알림을 트리거하지 않습니다.
- **자격 증명 정책**을 구성하고 인증서 별칭을 정의할 때, 사용자 지정 인증서 별칭을 사용하면 Citrix SSO 앱이 인증 오류와 함께 VPN에 연결하지 못합니다. 다음 오류 메시지가 나타납니다.

연결 오류: *인증서 ID*에 연결할 수 없습니다. 인터넷 연결을 확인하고 *인증서 ID*에 대한 설정을 확인하십시오.

Citrix SSO 앱용 인증서를 앱이 사용하도록 허용할 때 이 문제가 발생합니다.

시트릭스 시큐어 허브 22.9.0

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 22.7.0

해결된 문제

- 모바일 장치 경험(MDX)에서 Citrix 모바일 애플리케이션 관리(MAM) SDK로 전환하고 XenMobile Server를 10.13 RP4로 업그레이드한 후 Secure Hub/Secure Web을 통해 인트라넷 사이트에 액세스하지 못할 수 있습니다.

다음 오류 메시지가 나타납니다: "Err_Name_not_resolved".

- 회사 소유 장치용 작업 프로파일(WPCOD)로 등록 구성이 설정된 작업 프로파일에는 관리되는 구성 정책 설정이 적용되지 않습니다. 이 문제는 인증이 ID 공급자(IdP)를 통해 이루어지고 작업 프로파일이 프로비저닝됨으로 표시되지 않은 경우 발생합니다.

시큐어 허브 22.6.0

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 22.5.0

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 22.4.0

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 22.2.0

Secure Hub 22.2.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 22.2.0의 해결된 문제

iOS용 시트릭스 시큐어 허브

- Apple 배포 프로그램을 통해 등록된 장치에서 iOS용 Secure Hub에 PIN을 사용하여 등록하라는 메시지가 표시됩니다.
- 장치가 유휴 상태인 후 Secure Mail에 로그인하면 iOS용 Secure Hub가 다음 오류 메시지와 함께 열립니다.

"Secure Hub에서 이 앱을 승인해야 합니다."

승인을 클릭하고 자격 증명을 제공하면 인증이 루프에 빠집니다. 재부팅 후에도 다시 인증하거나 로그인할 수 없습니다.

- iOS 15.1을 실행하는 장치에서 오류를 보고할 때 iOS용 Secure Hub가 응답하지 않게 됩니다.
- iOS용 Secure Hub에서 새 알림이 없는데도 배지 수가 1 또는 2로 표시됩니다.
- iOS용 Secure Hub에서 일부 장치에서 등록이 실패할 수 있습니다.
- Citrix Gateway 세션 시간 초과 정책 값을 30일로 구성하면 iOS용 Secure Hub는 사용자에게 24~72시간마다 다시 인증하도록 요청합니다.

Android용 시큐어 허브

- Samsung DeX 모드에서 PIN을 입력하면 Secure Hub가 응답하지 않게 됩니다.
- 완전 관리 모드에서 Samsung S20 장치를 Android Enterprise에 등록할 때 다음 오류가 나타납니다:
"잘못된 서버 인증서"

- Android 10 또는 11을 실행하는 장치 등록이 실패하고 다음 오류 메시지가 나타납니다: "보안 정책에서 연결을 허용하지 않습니다."
- Android용 Secure Hub에 등록할 때 세로 모드에서 가로 모드로 전환하면 자격 증명이 임의의 숫자로 바뀝니다.

시큐어 허브 21.11.0

Secure Hub 21.11.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.11.0에서 해결된 문제

안드로이드용 시큐어 허브

- Android용 Secure Hub 등록 중에 인증서를 찾을 수 없습니다 오류 메시지가 나타납니다. 인증서 설치를 클릭하면 인증서가 없는 빈 링크가 나타납니다. 취소를 클릭하면 인증 화면이 나타납니다. 이 문제는 Secure Hub에서 로그아웃했다가 다시 로그인할 때도 발생합니다.

시큐어 허브 21.10.0

Secure Hub 21.10.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.10.0에서 해결된 문제

iOS용 시큐어 허브

- iOS용 Secure Hub에서 Apple 배포 프로그램을 통해 등록된 장치에 PIN을 사용하여 등록하라는 메시지가 표시됩니다.

안드로이드용 시큐어 허브

- 회사 소유 장치 모드에서 업무 프로필에 등록하기 위해 Android 장치용 등록 프로필을 생성할 때 **BYOD 업무 프로필** 설정을 활성화해야 합니다. 이 설정을 활성화하지 않으면 장치 등록에 실패합니다.
- Android용 Secure Hub에 로그인하는 동안 이메일 ID가 자동으로 채워집니다.

시큐어 허브 21.8.0

iOS용 시큐어 허브

Secure Hub 21.8.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.8.0에서 해결된 문제

- 장치가 유효 상태인 후 Secure Mail에 로그인하면 iOS용 Secure Hub가 열리고 로그온을 시도하지만 로그온 요청이 실패합니다. Secure Mail은 계속해서 로그온을 요청하며 로그인 루프를 생성합니다.
- 사용자 이름 또는 암호에 특정 특수 문자가 있는 사용자는 등록할 수 없습니다.

시큐어 허브 21.7.1

Android용 시큐어 허브

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

이전 버전의 알려진 문제 및 해결된 문제

이전 버전의 Secure Hub에서 알려진 문제 및 해결된 문제에 대한 자세한 내용은 [Secure Hub 알려진 문제 및 해결된 문제 기록](#)을 참조하십시오.

Secure Hub 21.7.1 릴리스

안드로이드용 Secure Hub

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

Secure Hub 버전 21.7.0

iOS용 시큐어 허브

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

Android용 시큐어 허브

Secure Hub 21.7.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.7.0에서 해결된 문제

- Android용 Secure Hub에서 장치를 재부팅한 후 **도움말 > 문제 보고**로 이동하면 Secure Mail 및 Secure Web 로그가 누락됩니다.

시큐어 허브 21.6.0

iOS용 시큐어 허브

Secure Hub 21.6.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.6.0에서 해결된 문제

iOS용 Secure Hub에서 UPN(사용자 계정 이름)을 사용하여 장치를 등록할 때 사용자 이름이 자동으로 채워지지 않습니다. 이 문제는 자동 검색 서비스가 활성화된 경우 발생합니다.

안드로이드용 Secure Hub

Secure Hub 21.6.0의 알려진 문제

Android용 Secure Hub에서 제공된 FQDN에 대문자가 포함된 경우 MDM+MAM 모드로 장치를 등록할 수 없습니다. 대신 장치는 MAM 모드로 등록됩니다.

Secure Hub 21.6.0의 해결된 문제

Android용 Secure Hub에서 Samsung Knox를 실행하는 초기화된 장치를 장치 관리자 모드로 등록할 수 없습니다.

시큐어 허브 21.5.1

아이오에스용 Secure Hub

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

Android용 시큐어 허브

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 21.5.0

Secure Hub 21.5.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.5.0의 해결된 문제

Android용 Secure Hub에서 Android Enterprise 장치에 Wi-Fi 장치 정책을 배포할 수 없습니다. 정책은 보류 상태로 유지됩니다.

시큐어 허브 21.4.0

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 21.3.2 버전

iOS용 시큐어 허브

Secure Hub 21.3.2의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.3.2에서 해결된 문제

Citrix PIN을 입력한 후 Citrix Endpoint Management™에 장치를 등록할 수 없습니다. Secure Hub에 PIN 요구 사항에 대한 올바른 메시지가 표시되지 않습니다.

시큐어 허브 21.3.0

Secure Hub 21.3.0의 알려진 문제

Secure Hub for Android 버전 20.9.0 이상에서는 Google Pixel 2 장치에서 VPN 모드로 연결할 수 없습니다.

Secure Hub 21.3.0에서 해결된 문제

- Secure Hub for Android에서 SIM 카드가 삽입되지 않은 장치에 대해 ICCID(Integrated Circuit Card ID)가 표시됩니다.
- Secure Hub for Android에서 장치를 다시 시작하면 설치된 모바일 생산성 앱이 **내 앱** 화면에 표시되지 않습니다.
- Secure Hub for Android에서 잘못된 암호를 여러 번 입력하고 장치를 다시 시작하려고 하면 Android Enterprise 장치의 잠금을 해제할 수 없습니다. 다음 오류 메시지가 나타납니다. **휴대폰이 꺼졌습니다.** IT 관리자에게 문의하십시오.

시큐어 허브 21.2.0

Android용 시큐어 허브

Secure Hub 21.2.0의 알려진 문제

Android용 Secure Hub에서 장치를 다시 시작하면 설치된 모바일 생산성 앱이 **내 앱** 화면에 나타나지 않습니다.

Secure Hub 21.2.0에서 해결된 문제

- Android용 Secure Hub가 장치 등록 중에 중단됩니다.
- Android용 Secure Hub의 특정 버전에서 Samsung Knox 장치 등록이 완료되면 **홈** 및 **뒤로** 버튼이 표시되지 않습니다.

시큐어 허브 21.1.0

Secure Hub 21.1.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 21.1.0에서 해결된 문제

- Android를 실행하는 장치에서 연결 예약 장치 정책이 활성화된 경우 Secure Hub가 Citrix Endpoint Management에 연결하지 못합니다.
- 특정 등록된 Samsung 장치에서 Citrix Endpoint Management 콘솔에 잘못된 일련 번호가 보고됩니다.

시큐어 허브 20.12.0

Secure Hub 20.12.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 20.12.0에서 해결된 문제

- iOS용 Secure Hub에서 장치를 등록할 수 없습니다. 다음 오류가 발생합니다: **장치가 등록되지 않았습니다.**
- iOS용 Secure Hub에서 사용자 에이전트 문자열에 MAM+MDM에 등록된 장치의 OS 버전이 포함되지 않습니다.
- Android Enterprise 장치에서 등록 중에 Secure Hub가 충돌합니다.
- Android용 Secure Hub 버전 20.11.0이 특정 Samsung 장치에서 충돌합니다.

시큐어 허브 20.11.0

Android용 시큐어 허브

Secure Hub 20.11.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 20.11.0의 해결된 문제

일부 Samsung 장치에서 Android용 Secure Hub가 충돌하며 다음 오류가 발생합니다: **Secure Hub가 계속 중지됩니다.**

시큐어 허브 20.10.5

Secure Hub 20.10.5의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 20.10.5의 해결된 문제

- Android 11을 실행하는 기업 소유 단일 용도(COSU) 장치에서 Secure Hub를 기본 실행기로 설정할 수 없습니다.
- Android를 실행하는 기기에서 특정 Samsung 기기에서 작업 프로필 생성이 실패합니다. 다음 오류가 발생합니다: **작업 프로필을 구성할 수 없습니다.**

- Citrix Endpoint Management AutoDiscovery Service를 통해 Android 기기의 모바일 앱 관리(MAM) 등록이 실패합니다.
- iOS를 실행하는 기기에서 특정 앱을 실행할 수 없습니다. Secure Hub에 사용할 수 있는 업데이트가 없는 데도 이 앱을 사용하려면 **Secure Hub를 업데이트하십시오**이라는 오류가 발생합니다.
- iOS를 실행하는 기기에서 최대 오프라인 기간이 만료된 후 Secure Mail에서 인증을 요청합니다. 그러면 Secure Mail이 Secure Hub로 전환되어 사용하지 못하게 됩니다.

시큐어 허브 20.9.0

Secure Hub 20.9.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 20.9.0의 해결된 문제

- iOS용 Secure Hub에서 인증서 고정이 활성화된 경우, 서버 중 하나에서 고정된 인증서가 올바르지 않더라도 서버 간에 연결이 설정됩니다.
- iOS용 Secure Hub에서 알림을 받을 수 없습니다. 다음 오류가 발생합니다: **유효한 Secure Hub 토큰이 있는 장치가 없습니다**.

시큐어 허브 20.7.5

Secure Hub 20.7.5의 알려진 문제

Android 11을 실행하는 기업 소유 단일 용도(COSU) 기기에서 Secure Hub를 기본 런처로 설정할 수 없습니다.

Secure Hub 20.7.5의 해결된 문제

- Android용 Secure Hub에서 인증서 고정이 활성화된 경우 Android 기기 등록이 실패합니다.
- Android용 Secure Hub에서 제한 정책의 **날짜 시간 변경** 기능이 Samsung 장치에서 작동하지 않습니다.
- Android용 Secure Hub에서 방화벽 정책은 버전 19.12.5 이상을 실행하는 Samsung 장치에서 작동하지 않습니다.
- Android용 Secure Hub에서 **내 앱**에서 앱을 제거할 수 없습니다.

시큐어 허브 20.6.5

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 20.3.0

iOS를 위한 Secure Hub

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 20.2.0

iOS용 보안 허브

Secure Hub 20.2.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 20.2.0의 해결된 문제

- iOS용 Secure Hub에서 모바일 애플리케이션 관리(MAM) 등록이 일부 iOS 장치에서 실패합니다.
- iOS용 Secure Hub에서 앱이 장치에서 무작위로 제거됩니다.

시큐어 허브 20.1.5

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 19.12.5

Secure Hub 19.12.5의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 19.12.5의 해결된 문제

iOS 13을 실행하는 장치에서, 사용자 인증서 만료를 확인하기 위해 SSL 오류 코드에 의존하는 대신 XenMobile® Server용 사용자 인증서가 실제 만료일에 확인 및 갱신됩니다.

시큐어 허브 19.11.5

Secure Hub 19.11.5의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 19.11.5의 해결된 문제

iOS용 Secure Hub에서 사용자 엔트로피를 비활성화한 후 MDX 래핑 앱의 등록이 실패합니다.

시큐어 허브 19.10.5

Android용 시큐어 허브

Secure Hub 19.10.5의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 19.10.5의 해결된 문제

Android용 Secure Hub에서 자격 증명 정책이 구성된 경우 Secure Hub 버전 19.10.5를 실행하는 장치에 비즈니스 앱을 설치할 수 없습니다.

시큐어 허브 19.10.0

Secure Hub 19.10.0의 알려진 문제

- Android용 Secure Hub에서 Android 버전 10을 실행하는 Google Pixel 2 장치의 장치 소유자 모드 등록이 권한 실패로 인해 실패합니다.
- Android용 Secure Hub에서 Android 버전 10을 실행하는 Google Pixel 장치의 장치 소유자 모드 등록이 위치 권한 유효성 검사 실패로 인해 실패합니다.

Secure Hub 19.10.0의 해결된 문제

이 릴리스에는 해결된 문제가 없습니다.

시큐어 허브 19.9.5

이 릴리스에는 알려지거나 해결된 문제가 없습니다.

시큐어 허브 19.9.0

Secure Hub 19.9.0의 알려진 문제

Android Enterprise가 활성화된 Secure Hub for Android 19.9.0에서 Pixel 2 장치에 다음 문제가 발생합니다. 자격 증명 정책이 성공적으로 배포되지 않습니다. 결과적으로 사용자에게 암호와 함께 인증서가 요청되지 않으며 인증서가 설치되지 않습니다. 해결 방법으로 사용자는 앱에서 **기본 설정 > 장치 정보**로 이동하여 정책을 수동으로 새로 고칠 수 있습니다. 여기에서 **정책 새로 고침**을 누르고 자격 증명을 입력한 다음 성공 메시지를 확인합니다.

Secure Hub 19.9.0의 해결된 문제

이 릴리스에는 해결된 문제가 없습니다.

시큐어 허브 19.8.5

이 릴리스에는 알려진 문제나 해결된 문제가 없습니다.

시큐어 허브 19.8.0

Secure Hub 19.8.0의 알려진 문제

iOS용 Secure Hub에서 공유 장치에 잘못된 암호를 입력하고 다시 로그인하기 위해 **사용자 전환**을 탭하면 잠시 기다려 주십시오 메시지가 무기한으로 나타납니다.

Secure Hub 19.8.0에서 해결된 문제

전체 VPN을 통해 연결될 때 모바일 장치 관리 네트워크가 잘못 라우팅됩니다.

시큐어 허브 19.7.5

Secure Hub 19.7.5의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 19.7.5에서 해결된 문제

- Android용 Secure Hub에서 웹 클립 설치 프롬프트가 빠르게 나타나 Secure Hub PIN 구성에 방해가 됩니다.

- Samsung Knox 장치 버전 3 이상에서 Secure Hub를 프로필 소유자 모드로 등록하고 Android Enterprise 플랫폼용 **Samsung MDM 라이선스 키** 정책을 푸시하면 **장치 컨테이너 암호 재설정** 명령이 실패합니다.
- Apple Store의 새 앱 URL을 사용하여 MAM 모드에서 공용 앱을 구성하려고 할 때 iOS용 Secure Hub에서 다음 오류가 나타납니다. **스토어를 로드할 수 없습니다. 다시 시도하십시오.** 해결 방법은 <https://support.citrix.com/article/CTX256704>를 참조하십시오.
- Secure Hub for Android에서 전체 VPN 터널이 설정된 경우 MDX 앱을 설치할 수 없습니다.
- 공유 장치 모드에서 Secure Hub for Android를 실행하는 Point Mobile PM80 장치에서 세션 시간 초과가 발생하면 다시 로그인할 수 없습니다.
- Secure Hub for Android에서 내부적으로 래핑된 애플리케이션을 설치하고 실행한 후 다음 오류가 발생합니다. 이 앱에서 데이터가 암호화되는 방식이 변경되었습니다. 이 앱을 삭제하고 다시 설치하십시오.

시큐어 허브 19.6.5

Secure Hub 19.6.5의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 19.6.5의 해결된 문제

- iOS를 실행하는 장치에서 글로벌 서버 로드 밸런싱 페일오버가 발생하면 Secure Hub가 스토어를 로드하지 않습니다.
- Secure Hub for Android에서 새로 고침 정책이 실패합니다. 결과적으로 새로운 장치 정책을 배포할 수 없습니다.
- Secure Hub for Android에서 Samsung S10 장치에 대한 등록 또는 새로 고침 정책 작업에 시간이 오래 걸립니다.
- Android를 실행하는 장치에서 Secure Hub가 전체 VPN 연결을 설정하면 관리되지 않는 앱의 연결이 끊어집니다.

시큐어 허브 19.5.5

Secure Hub 19.5.5의 알려진 문제

- Secure Hub for Android에서 COSU(Corporate Owned Single Use) 모드의 장치는 등록 후 몇 분이 지나면 연결이 끊어지고 GCM이 활성화되어 있어도 알림을 받지 못합니다.

- 장치에 위치 정책을 한 번에 프로필 소유자 및 장치 소유자 모드 모두에 배포하면 장치 소유자 모드의 사용자 계정이 삭제됩니다. 이 문제는 NFC 범프 등록 중 및 Endpoint Management가 MDM 모드로 구성된 경우에 발생합니다.

Secure Hub 19.5.5의 해결된 문제

- 이 릴리스부터 Secure Hub는 Android 5.0 이상을 실행하는 장치만 지원합니다.
- Android용 Secure Hub에서 장치 소유자 모드로 장치를 등록하고 새 암호를 설정합니다. 첫 번째 시도에서 장치가 잠기지 않습니다.

시큐어 허브 19.5.0

Secure Hub 19.5.0의 알려진 문제

- 등록 후, OnePlus Android 버전 7.1.1 및 OnePlus 5T Android 버전 9.0.3 장치는 Citrix PIN을 요청하려면 Secure Hub를 수동으로 다시 시작해야 합니다.
- Android용 Secure Hub에서 정책을 새로 고치거나 스토어를 새로 고치지 않으면 필수 앱이 Android 장치에 배포되지 않습니다.

Secure Hub 19.5.0의 해결된 문제

- 이 릴리스부터 Secure Hub는 Android 5.0 이상을 실행하는 장치만 지원합니다.
- Android용 Secure Hub에서 서버 인증서에 여러 주체 대체 이름이 있는 경우 Android 6.0 장치 등록에 실패합니다.
- Android용 Secure Hub에서 장치 등록 해제 후 관리되는 앱이 제거되지 않습니다.
- Samsung S9 장치에서 사용자가 Android P로 업데이트한 후 다음 문제가 발생합니다. Endpoint Management를 통해 장치 암호를 변경하면 장치의 암호가 변경되지 않습니다. 대신 화면이 검은색으로 바뀌고 Endpoint Management 콘솔에 잠긴 장치 상태가 표시됩니다.

시큐어 허브 19.4.5

Secure Hub 19.4.5의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 19.4.5의 해결된 문제

iOS 장치에서 장치 등록 링크를 클릭하면 Endpoint Management FQDN 인스턴스 이름이 Secure Hub에 자동으로 채워지지 않습니다. 장치 등록 요청이 실패합니다.

시큐어 허브 19.3.5

Secure Hub 19.3.5의 알려진 문제

iOS용 Secure Hub에서 알림을 보내면 Secure Hub의 알림 배지 수가 업데이트되지 않습니다.

Secure Hub 19.3.5의 해결된 문제

- Android용 Secure Hub에서 공유 장치를 등록하고 **Webclip** 정책을 배포하며 웹 및 SaaS 앱을 추가하면 배포가 성공합니다. 그러나 이 배포는 Citrix Endpoint Management 콘솔의 **앱 인벤토리** 화면에 실패로 표시됩니다.
- Android용 Secure Hub에서 사용자가 보안 PIN으로 로그인하면 VPN 터널이 설정되지만 Secure Web은 웹 사이트를 로드하지 않습니다. 그러나 Secure Web을 닫았다가 다시 열면 웹 사이트가 예상대로 로드됩니다.
- Microsoft Intune 정책으로 구성된 Android용 Secure Mail은 인증 후 빈 화면을 반환합니다.
- Android용 Secure Hub에서 암호화가 비활성화된 앱이 Secure Hub에서 암호화 키를 얻으려고 시도합니다.
- Intune Company Portal 버전 5.0.4324.0이 설치된 경우 Android용 Secure Mail이 시작 시 충돌합니다.
- Android용 Secure Hub에서 Android 7.1.1을 실행하는 기업 소유 단일 사용(COSU) Android Enterprise 장치에서 시스템 앱을 사용할 수 없습니다.
- Android용 Secure Hub에서 Google Play의 여러 앱을 필수 앱으로 구성하고 등록을 시도하면 첫 번째 앱을 설치하라는 메시지가 표시됩니다. 초기 메시지 직후 두 번째 앱 등을 설치하라는 메시지가 표시됩니다.

시큐어 허브 19.3.0

Secure Hub 19.3.0의 알려진 문제

- Android용 Secure Hub에서 공유 장치를 등록하고 Webclip 정책을 배포하며 웹 및 SaaS 앱을 추가하면 배포가 성공합니다. 그러나 이 배포는 Citrix Endpoint Management 콘솔의 **앱 인벤토리** 화면에 실패로 표시됩니다.
- Android Enterprise 장치에서 위치 정책의 지오펜스 위반에 대한 잠금 작업이 설정된 경우, 장치는 시스템에서 생성된 암호를 사용하는 대신 새 암호를 설정하라는 메시지를 표시합니다.

Secure Hub 19.3.0의 해결된 문제

암호로 잠금 보안 작업을 사용하여 완전 관리형 Android Enterprise 장치를 원격으로 잠그는 작업이 실패 알림 없이 실패할 수 있습니다. 장치가 잠겼는지 확인하려면 암호로 잠금을 두 번 설정하십시오. 장치는 두 번째로 설정한 암호로 잠깁니다.

시큐어 허브 19.2.0

Secure Hub 19.2.0의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Hub 19.2.0의 해결된 문제

- iOS용 Secure Hub에서 사용자가 Secure Hub 스토어에서 로그오프할 때 다음 SSL 핸드셰이크 실패 메시지가 반복적으로 나타납니다. 서버에서 앱을 가져오는 네트워크 요청 시간이 초과되었습니다.
- Android Enterprise용 파일 장치 정책은 작업 프로필 모드의 Android 장치에 배포되지 않습니다.
- Android용 Secure Hub에서 새 사용자의 로그인 권한 부여는 공유 장치에서 시간이 오래 걸립니다. 등록된 사용자로 로그오프하고 새 사용자로 로그인하려고 하면 장치를 재부팅할 때까지 Secure Hub가 계속 로드됩니다.
- Android용 Secure Hub에서 클라우드 고객은 외부 ID 공급자를 사용하여 Android Enterprise 장치를 등록할 수 없습니다.
- Android용 Secure Hub에서 COSU(Corporate Owned Single Use) 모드에 있을 때 Secure Hub에서 앱 아이콘이 겹쳐집니다.
- Android용 Secure Hub에서 기존 설정에 대해 인증서 고정기 활성화된 경우, 인증서에 여러 주체 대체 이름(Subject Alternative Names)이 있으면 인증이 실패하고 첫 사용자 화면으로 돌아갑니다.

시큐어 허브 19.1.5

Secure Hub 19.1.5의 알려진 문제

- Android용 Secure Hub에서 암호 정책 변경으로 인해 암호를 업데이트할 때, 배지 앱이 Samsung Galaxy S8 장치에 나타나지 않습니다.
- Android용 Secure Hub에서 파일 장치 정책 Android Enterprise가 작업 프로필 모드의 장치에 배포되지 않습니다.

Secure Hub 19.1.5에서 해결된 문제

- Android용 Secure Hub에서 사용자가 Secure PIN으로 로그인하면 VPN 터널이 설정되지만, Secure Web은 어떤 웹사이트도 로드하지 않습니다. 그러나 Secure Web을 닫았다가 다시 열면 웹사이트가 예상대로 로드됩니다.
- Android용 Secure Hub에서 Secure PIN으로 로그인하면 VPN 터널이 설정되지만, Secure Web은 어떤 웹사이트도 로드하지 않습니다. 그러나 Secure Web을 닫았다가 다시 열면 웹사이트가 예상대로 로드됩니다.
- Android용 Secure Hub에서 TechXpert라는 사내 앱의 로그를 캡처하려고 하면 Secure Hub가 다시 시작되고 재인증을 요청합니다.

시큐어 허브 19.1.0

Secure Hub 19.1.0의 알려진 문제

iOS용 Secure Hub에서 MDX 및 웹 또는 SaaS 앱을 배포하면 **내 앱** 화면에 나타납니다. **더 보기**를 탭하면 이전 UI 브랜딩 형식의 삭제 및 취소 옵션이 있는 팝업이 나타납니다.

Secure Hub 18.12.0에서 해결된 문제

- Android For Work에 등록된 Samsung Knox 장치에서 암호 정책이 1~2일 내에 만료되도록 구성된 경우, **암호 만료** 메시지가 반복적으로 나타납니다.
- QR 코드 등록 방법을 사용하여 Android Enterprise용 OnePlus 5T 장치를 등록할 수 없습니다.

시큐어 허브 18.11.0

Secure Hub 18.11.0에서 해결된 문제

- Shared Device 모드에 등록된 Android 장치에서 단일 Sign-On을 수행할 수 없습니다. 다음 오류가 나타납니다: **현재 회사 자격 증명을 검색할 수 없습니다. 관리자 정책으로 인해 ShareFile에 대한 수동 로그인**이 차단되었습니다.
- 기업 소유의 단일 용도(COSU) 장치에서 Android 볼륨 수준을 편집할 수 없습니다.

시큐어 허브 18.10.5

Secure Hub 18.10.5의 해결된 문제

- XenMobile Server에서 FIPS 모드를 사용하도록 설정한 경우, 사용자가 iOS용 Secure Hub를 버전 18.10.5로 업데이트한 후 앱을 열면 암호화 관련 오류 메시지가 나타납니다.

Secure Hub 버전 10.8.25 ~ 18.10.6

Secure Hub 버전 10.8.25 ~ 18.10.6의 해결된 문제

- Secure Hub 버전 10.8.25 ~ 18.10.6(Android)에는 알려진 문제가 없습니다. 다음 문제는 Secure Hub에서 해결되었습니다. 이 목록에는 Secure Hub에 영향을 미치는 MDX 관련 문제가 포함됩니다.

시큐어 허브 18.10.0

Secure Hub 18.10.0의 해결된 문제

- EMS 콘솔에서 MVPN 정책이 꺼져 있으면 Secure Hub는 Intune 관리 앱을 열려고 할 때 빈 화면을 표시합니다.

시큐어 허브 10.8.60

Secure Hub 10.8.60의 해결된 문제

- Samsung Galaxy Tab Active 2 SM-T395 장치에서 관리자가 XenMobile에서 공장 초기화 비활성화 제한을 설정하면 Android용 Secure Hub에 대한 전체 초기화 보안 작업이 실패합니다.
- VPN 정책이 구성되어 있고 Citrix SSO 애플리케이션이 장치에 설치되어 있지 않으면 장치 등록 중에 Android용 Secure Hub가 응답하지 않습니다. 뒤로 버튼을 탭하거나 앱을 다시 시작하면 응답합니다.
- Android Enterprise 환경에서 Device Owner 모드로 등록하는 동안 Android용 Secure Hub이(가) 충돌합니다.
- 사용자가 iOS용 Secure Hub에 유효한 PIN을 입력한 후 Secure Hub에서 PIN을 반복적으로 요청합니다.
- Android Enterprise 환경에서 Profile Owner 모드로 등록하는 동안 Android용 Secure Hub이(가) 충돌합니다.
- Android용 Secure Hub에서 Android Enterprise를 사용하면 기본적으로 Google Chrome이 설치됩니다.
- iOS용 Secure Hub을(를) 버전 10.8.55로 업그레이드하면 기존 또는 새 iOS 장치 등록이 허용되지 않습니다.

보안 허브 10.8.55

Secure Hub 10.8.55의 해결된 문제

- G Suite 자격 증명에 Endpoint Management의 자격 증명과 다른 경우 사용자는 Android for Work 계정에 등록하기 위해 Secure Hub에 로그인할 수 없습니다.

버전 10.8.55의 MDX 관련 해결된 문제

- Preferred VPN 모드가 SecureBrowse로 설정된 경우 엔터프라이즈 앱에서 내부 리소스에 대한 연결 문제가 발생할 수 있습니다.
- 애플리케이션 클래스로 android.support.multidex.MultiDexApplication 또는 android.app.Application을 지정하는 앱은 Tunneled – Web SSO 모드에서 내부 네트워크에 연결할 수 없습니다.
- Android 장치에서 여러 인증서가 생성되고 있으며 인증서가 만료일 이전에 해지되고 있습니다.

보안 허브 10.8.55

Secure Hub 10.8.55의 알려진 문제

- 장치에서 Secure Hub 계정을 제거한 후 MDM 재등록이 실패합니다.

시큐어 허브 10.8.50

Secure Hub 10.8.50의 알려진 문제

- Android용 Secure Hub에서 사용자가 웹 링크 바로 가기를 추가할 수 없습니다.

시큐어 허브 10.8.35

Secure Hub 10.8.35에서 해결된 문제

- Android O에서 정책으로 생성된 바로 가기가 장치 홈 화면에 나타나지 않습니다. 이 동작은 Android O의 설계상 의도된 것입니다.
- Android에서 Secure Hub가 일정 시간 비활성 상태 후 Samsung 태블릿에서 열리지 않습니다.
- Android용 Secure Hub에서 Samsung Knox 장치에 푸시 정책을 배포할 수 없습니다.
- iOS용 Secure Hub에서 간헐적으로 다음과 같은 문제가 발생합니다. 사용자가 Active Directory 암호를 변경한 후 PIN을 계속 반복해서 입력해야 합니다.

시큐어 허브 10.8.25

Secure Hub 10.8.25에서 해결된 문제

- MDX Toolkit 버전 10.7.20으로 래핑된 타사 iOS Cordova 앱의 경우, **화면 내용 가리기** 정책을 활성화 하면 PIN 화면 대신 검은색 화면이 나타납니다.
- Android 7을 실행하는 Zebra T51 장치에서 사용자는 Citrix Launcher 앱을 설치할 수 없습니다.

시큐어 허브 10.8.20

Secure Hub 10.8.20에서 해결된 문제

- 사용자가 Android 기기를 버전 8(Oreo)로 업데이트한 후: Endpoint Management에서 배포하는 앱 스토어에서 엔터프라이즈 또는 .apk 앱을 설치할 수 없습니다. 타사 앱 설치를 활성화해도 문제가 지속됩니다. 이 문제는 Samsung 기기에만 국한되지 않습니다.

시큐어 허브 10.8.15

Secure Hub 10.8.15의 해결된 문제

- Android O를 실행하는 기기에서 위치 세부 정보를 가져오는 동안 Android용 Secure Hub가 충돌합니다.

시큐어 허브 10.8.10

Secure Hub 10.8.10의 해결된 문제

- Android 기기에서 여러 앱이 자동으로 설치되지 않거나 사용자가 직접 **설치**를 클릭하지 않으면 앱이 계속 다운로드됩니다. 그 결과 데이터 사용량이 많아집니다.
- Android 7 이상을 실행하는 기기에서: XenMobile Server에서 암호와 함께 잠금 보안 작업을 기기로 보내면 기기가 잠깁니다. 그러나 사용자가 기존 잠금 화면 암호를 가지고 있는 경우 기기 암호는 변경되지 않습니다. 사용자는 원래 암호를 사용하여 기기를 잠금 해제할 수 있습니다.

iOS용 Secure Hub 업데이트(March 19, 2018): iOS용 Secure Hub 버전 10.8.6은 VPP 앱 정책 문제를 해결하기 위해 제공됩니다.

Android 및 iOS용 Secure Hub - 미리 보기

다음 릴리스에서 제공될 새로운 기능과 해결된 문제를 기대해 주세요.

현재 릴리스에 대한 자세한 내용은 [Secure Hub의 새로운 기능을\(를\)](#) 참조하십시오.

기능 플래그 관리

관리자는 미리 보기 기능에 액세스하고 프로덕션에서 기능을 동적으로 제어하기 위해 기능 플래그를 관리할 수 있습니다. 기능 플래그 아래에 있는 기능의 최적 작동을 보장하려면 URL

`features.netscalergateway.net` 으로 트래픽을 활성화해야 합니다. 자세한 내용은 [기능 플래그 관리](#)를 참조하십시오.

인증 프롬프트 시나리오

다양한 시나리오에서 사용자는 장치에 자격 증명을 입력하여 Secure Hub로 인증하라는 메시지를 받습니다.

시나리오는 다음 요인에 따라 변경됩니다.

- Endpoint Management 콘솔 설정의 MDX 앱 정책 및 클라이언트 속성 구성.
- 인증이 오프라인 또는 온라인으로 발생하는지 여부(장치에 Endpoint Management에 대한 네트워크 연결이 필요함).

또한 사용자가 입력하는 자격 증명(예: Active Directory 암호, Citrix PIN 또는 암호, 일회용 암호, 지문 인증(iOS에서는 Touch ID로 알려짐))의 종류도 인증 유형 및 인증 빈도에 따라 변경됩니다.

인증 프롬프트가 발생하는 시나리오부터 시작하겠습니다.

- **장치 재시작:** 사용자가 장치를 재시작하면 Secure Hub로 다시 인증해야 합니다.
- **오프라인 비활성(시간 초과):** 앱 암호 MDX 정책이 활성화된 경우(기본값) 비활성 타이머라는 Endpoint Management 클라이언트 속성이 적용됩니다. 비활성 타이머는 보안 컨테이너를 사용하는 앱에서 사용자 활동 없이 경과할 수 있는 시간 길이를 제한합니다.

비활성 타이머가 만료되면 사용자는 장치의 보안 컨테이너에 다시 인증해야 합니다. 예를 들어, 사용자가 장치를 내려놓고 자리를 비웠을 때 비활성 타이머가 만료되면 다른 사람이 장치를 가져가 컨테이너 내의 민감한 데이터에 액세스할 수 없습니다. **비활성 타이머 클라이언트** 속성은 Endpoint Management 콘솔에서 설정합니다. 기본값은 15분입니다. 앱 암호가 **ON**으로 설정된 것과 비활성 타이머 클라이언트 속성의 조합은 아마도 가장 일반적인 인증 프롬프트 시나리오를 담당합니다.

- **Secure Hub에서 로그오프:** 사용자가 Secure Hub에서 로그오프하면 다음번에 Secure Hub 또는 MDX 앱에 액세스할 때 앱 암호 MDX 정책 및 비활성 타이머 상태에 따라 앱에 암호가 필요한 경우 다시 인증해야 합니다.
- **최대 오프라인 기간:** 이 시나리오는 앱별 MDX 정책에 의해 결정되므로 개별 앱에 특화되어 있습니다. 최대 오프라인 기간 MDX 정책의 기본 설정은 3일입니다. Secure Hub를 통한 온라인 인증 없이 앱이 실행될 수 있는 기간이 경과하면 앱 권한을 확인하고 정책을 새로 고치기 위해 Endpoint Management와의 체크인이 필요합니다. 이 체크인이 발생하면 앱은 Secure Hub에 온라인 인증을 트리거합니다. 사용자는 MDX 앱에 액세스하기 전에 다시 인증해야 합니다.

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

- 활성 폴링 기간은 앱 잠금 및 앱 초기화와 같은 보안 작업을 수행하기 위해 앱이 Endpoint Management와 체크인하는 간격입니다. 또한 앱은 업데이트된 앱 정책도 확인합니다.
- 활성 폴링 기간 정책을 통해 정책 확인에 성공하면 최대 오프라인 기간 타이머가 재설정되고 다시 카운트다운을 시작합니다.

Endpoint Management와의 두 가지 체크인(활성 폴링 기간 및 최대 오프라인 기간 만료) 모두 장치에 유효한 Citrix Gateway 토큰이 필요합니다. 장치에 유효한 Citrix Gateway 토큰이 있으면 앱은 사용자에게 중단 없이 Endpoint Management에서 새 정책을 검색합니다. 앱에 Citrix Gateway 토큰이 필요한 경우 Secure Hub로 전환되고 사용자는 Secure Hub에서 인증 프롬프트를 보게 됩니다.

Android 장치에서는 Secure Hub 활동 화면이 현재 앱 화면 위에 직접 열립니다. 그러나 iOS 장치에서는 Secure Hub가 전경으로 나와야 하므로 현재 앱이 일시적으로 대체됩니다.

사용자가 자격 증명을 입력하면 Secure Hub는 원래 앱으로 다시 전환됩니다. 이 경우 캐시된 Active Directory 자격 증명을 허용하거나 클라이언트 인증서가 구성되어 있으면 사용자는 PIN, 암호 또는 지문 인증을 입력할 수 있습니다. 그렇지 않은 경우 사용자는 전체 Active Directory 자격 증명을 입력해야 합니다.

Citrix ADC 토큰은 Citrix Gateway 세션 비활성 또는 강제 세션 시간 초과 정책으로 인해 무효화될 수 있으며, 이는 다음 Citrix Gateway 정책 목록에서 설명합니다. 사용자가 Secure Hub에 다시 로그인하면 앱을 계속 실행할 수 있습니다.

- **Citrix Gateway 세션 정책:** 두 가지 Citrix Gateway 정책도 사용자에게 인증을 요청하는 시기에 영향을 미칩니다. 이 경우 사용자는 Endpoint Management에 연결하기 위해 Citrix ADC와 온라인 세션을 생성하도록 인증합니다.
 - **세션 시간 초과:** 설정된 기간 동안 네트워크 활동이 없으면 Endpoint Management용 Citrix ADC 세션이 연결 해제됩니다. 기본값은 30분입니다. 그러나 Citrix Gateway 마법사를 사용하여 정책을 구성하는 경우 기본값은 1440분입니다. 사용자는 회사 네트워크에 다시 연결하기 위한 인증 프롬프트를 보게 됩니다.
 - **강제 시간 초과:** 꺼짐으로 설정된 경우, 강제 시간 초과 기간이 경과하면 Endpoint Management용 Citrix ADC 세션이 연결 해제됩니다. 강제 시간 초과는 설정된 기간 후에 재인증을 의무화합니다. 그러면 사용자는 다음 사용 시 회사 네트워크에 다시 연결하기 위한 인증 프롬프트를 보게 됩니다. 기본값은 꺼짐입니다. 그러나 Citrix Gateway 마법사를 사용하여 정책을 구성하는 경우 기본값은 1440분입니다.

자격 증명 유형

이전 섹션에서는 사용자에게 인증을 요청하는 시기에 대해 설명했습니다. 이 섹션에서는 사용자가 입력해야 하는 자격 증명의 종류에 대해 설명합니다. 장치의 암호화된 데이터에 액세스하려면 다양한 인증 방법을 통한

인증이 필요합니다. 장치를 처음 잠금 해제하려면 *기본 컨테이너*를 잠금 해제합니다. 이 작업이 완료되고 컨테이너가 다시 보호되면 다시 액세스하기 위해 *보조 컨테이너*를 잠금 해제합니다.

참고:

*관리되는 앱*이라는 용어는 MDX Toolkit으로 래핑된 앱을 의미하며, 이 앱에서는 기본적으로 앱 암호 MDX 정책을 활성화된 상태로 두고 비활성 타이머 클라이언트 속성을 사용합니다.

자격 증명 유형을 결정하는 상황은 다음과 같습니다.

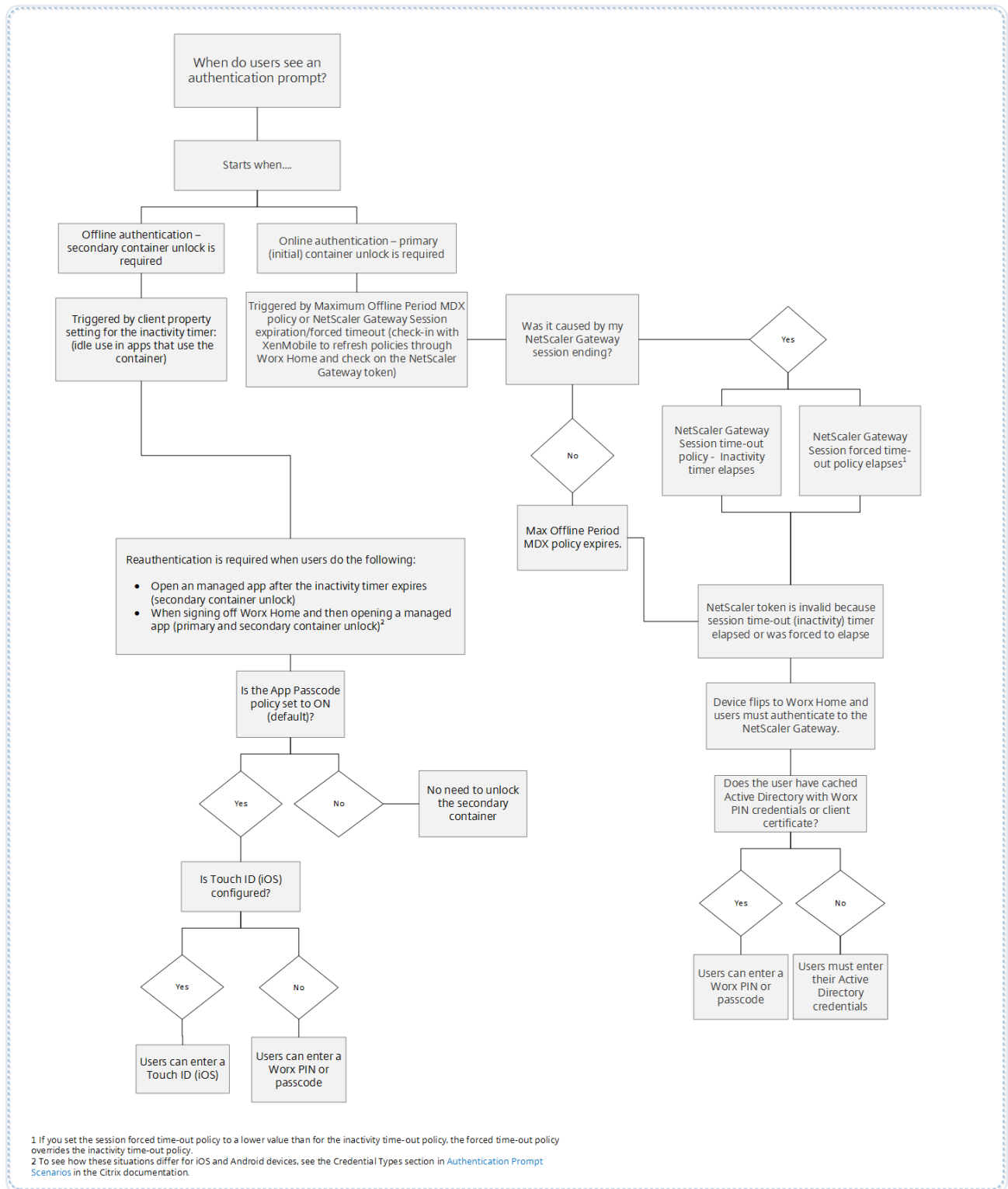
- **기본 컨테이너 잠금 해제:** 기본 컨테이너를 잠금 해제하려면 Active Directory 암호, Citrix PIN 또는 암호, 일회용 암호, Touch ID 또는 지문 ID가 필요합니다.
 - iOS에서 사용자가 장치에 앱을 설치한 후 Secure Hub 또는 관리되는 앱을 처음 열 때.
 - iOS에서 사용자가 장치를 다시 시작한 다음 Secure Hub를 열 때.
 - Android에서, Secure Hub가 실행되고 있지 않을 때 사용자가 관리되는 앱을 열면.
 - Android에서, 장치 재시작을 포함하여 어떤 이유로든 사용자가 Secure Hub를 다시 시작할 때.
- **보조 컨테이너 잠금 해제:** 보조 컨테이너를 잠금 해제하려면 지문 인증(구성된 경우), Citrix PIN 또는 암호, 또는 Active Directory 자격 증명이 필요합니다.
 - 비활성 타이머가 만료된 후 사용자가 관리되는 앱을 열 때.
 - 사용자가 Secure Hub에서 로그오프한 다음 관리되는 앱을 열 때.

다음 조건이 충족될 때 컨테이너 잠금 해제 상황 중 하나에 Active Directory 자격 증명이 필요합니다.

- 사용자가 회사 계정과 연결된 암호를 변경할 때.
- Endpoint Management 콘솔에서 Citrix PIN을 활성화하도록 클라이언트 속성 (ENABLE_PASSCODE_AUTH 및 ENABLE_PASSWORD_CACHING)을 설정하지 않은 경우.
- NetScaler® Gateway 세션이 종료될 때(세션 시간 초과 또는 강제 시간 초과 정책 타이머가 만료되거나, 장치가 자격 증명을 캐시하지 않거나, 클라이언트 인증서가 없는 경우 발생).

지문 인증이 활성화된 경우, 앱 비활성으로 인해 오프라인 인증이 필요할 때 사용자는 지문을 사용하여 로그인할 수 있습니다. 사용자는 Secure Hub에 처음 로그인할 때와 장치를 다시 시작할 때 PIN을 입력해야 합니다. 지문 인증 활성화에 대한 자세한 내용은 [지문 또는 터치 ID 인증](#)을 참조하십시오.

다음 순서도는 인증을 요청받았을 때 사용자가 어떤 자격 증명을 입력해야 하는지 결정하는 의사 결정 흐름을 요약합니다.



Secure Hub 화면 전환 정보

또 다른 주목할 상황은 앱에서 Secure Hub로 전환했다가 다시 앱으로 돌아가야 하는 경우입니다. 전환 시 사용자에게 확인해야 하는 알림이 표시됩니다. 이 경우 인증은 필요하지 않습니다. 이 상황은 최대 오프라인 기간 및 활성 폴링 기간 MDX 정책에 따라 Endpoint Management와 체크인이 발생한 후, Endpoint Management가 Secure Hub를 통해 장치로 푸시해야 하는 업데이트된 정책을 감지할 때 발생합니다.

장치 암호의 암호 복잡성 (Android 12 이상)

암호 복잡성은 사용자 지정 암호 요구 사항보다 선호됩니다. 암호 복잡성 수준은 미리 정의된 수준 중 하나입니다. 따라서 최종 사용자는 더 낮은 복잡성 수준의 암호를 설정할 수 없습니다.

Android 12 이상 기기의 암호 복잡성은 다음과 같습니다.

- **암호 복잡성 적용:** 사용자 지정 암호 요구 사항 대신 플랫폼에서 정의한 복잡성 수준의 암호를 요구합니다. Android 12 이상 기기 및 Secure Hub 22.9 이상 버전을 사용하는 기기에만 해당됩니다.
- **복잡성 수준:** 미리 정의된 암호 복잡성 수준.
 - **없음:** 암호가 필요하지 않습니다.
 - **낮음:** 암호는 다음 중 하나일 수 있습니다.
 - 패턴
 - 최소 4개의 숫자로 구성된 PIN
 - **중간:** 암호는 다음 중 하나일 수 있습니다.
 - 반복되는 시퀀스(4444) 또는 순서가 있는 시퀀스(1234)가 없으며 최소 4개의 숫자로 구성된 PIN
 - 최소 4자 이상으로 구성된 알파벳
 - 최소 4자 이상으로 구성된 영숫자
 - **높음:** 암호는 다음 중 하나일 수 있습니다.
 - 반복되는 시퀀스(4444) 또는 순서가 있는 시퀀스(1234)가 없으며 최소 8개의 숫자로 구성된 PIN
 - 최소 6자 이상으로 구성된 알파벳
 - 최소 6자 이상의 영숫자

참고:

- BYOD 기기의 경우, 최소 길이, 필수 문자, 생체 인식 및 고급 규칙과 같은 암호 설정은 Android 12 이상에서는 적용되지 않습니다. 대신 암호 복잡성을 사용하십시오.
- 작업 프로필에 대한 암호 복잡성이 활성화된 경우, 장치 측에 대한 암호 복잡성도 활성화되어야 합니다.

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

파생 자격 증명을 사용하여 장치 등록

파생 자격 증명은 모바일 장치에 강력한 인증을 제공합니다. 스마트 카드에서 파생된 자격 증명은 카드 대신 모바일 장치에 상주합니다. 스마트 카드는 PIV(개인 신원 확인) 카드 또는 CAC(공통 액세스 카드)입니다.

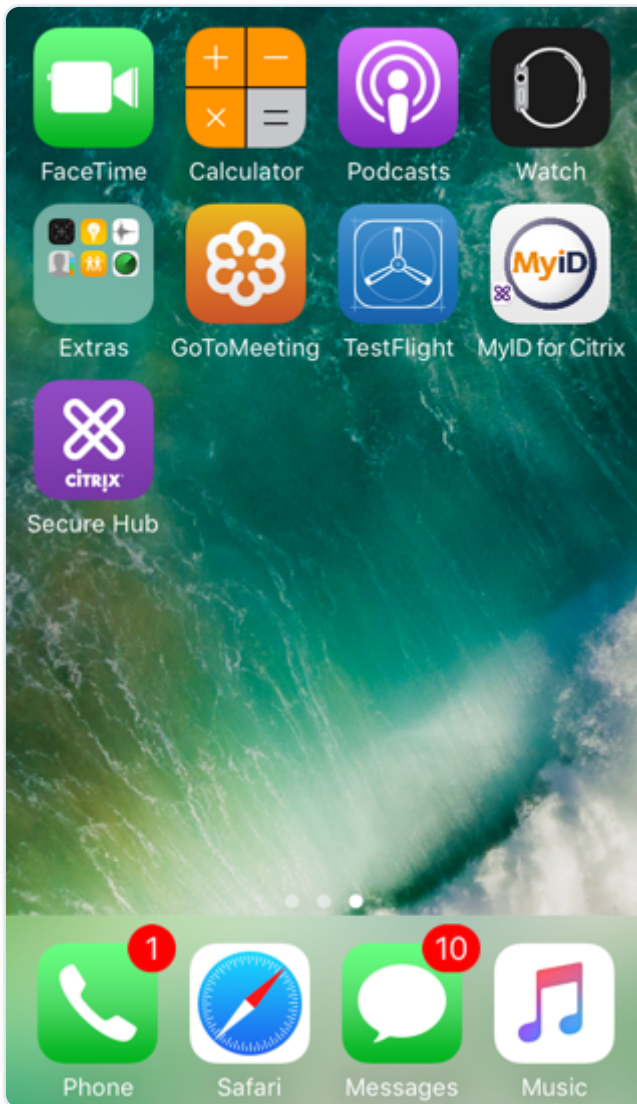
파생 자격 증명은 UPN과 같은 사용자 식별자를 포함하는 등록 인증서입니다. Endpoint Management는 자격 증명 공급자로부터 얻은 자격 증명을 장치의 보안 저장소에 저장합니다.

Endpoint Management는 iOS 장치 등록에 파생 자격 증명을 사용할 수 있습니다. 파생 자격 증명으로 구성된 경우 Endpoint Management는 iOS 장치에 대한 등록 초대 또는 기타 등록 모드를 지원하지 않습니다. 그러나 동일한 Endpoint Management 서버를 사용하여 등록 초대 및 기타 등록 모드를 통해 Android 장치를 등록할 수 있습니다.

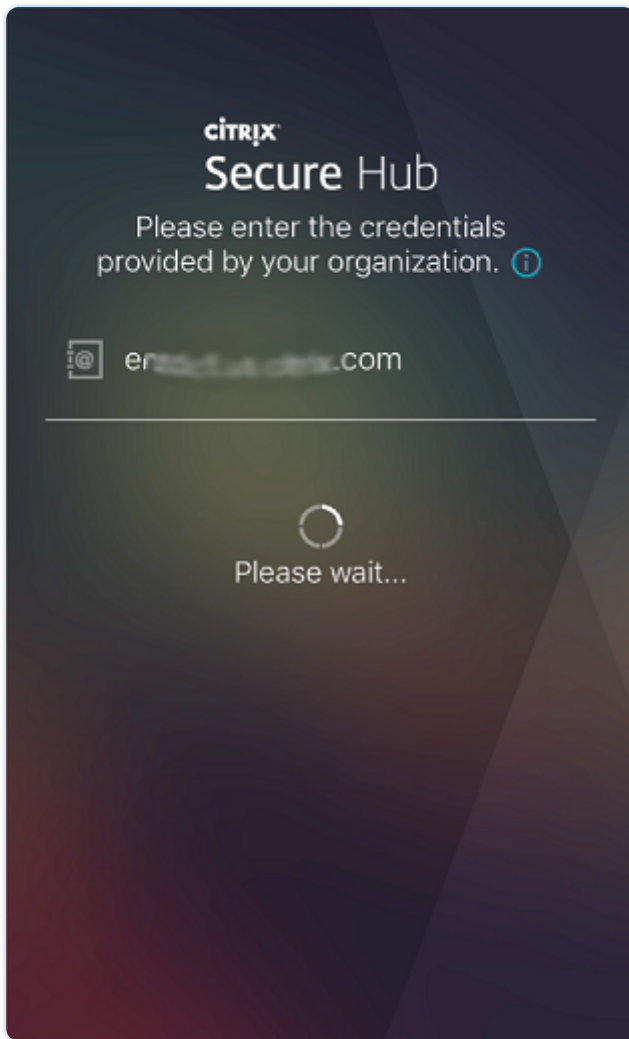
파생 자격 증명 사용 시 장치 등록 단계

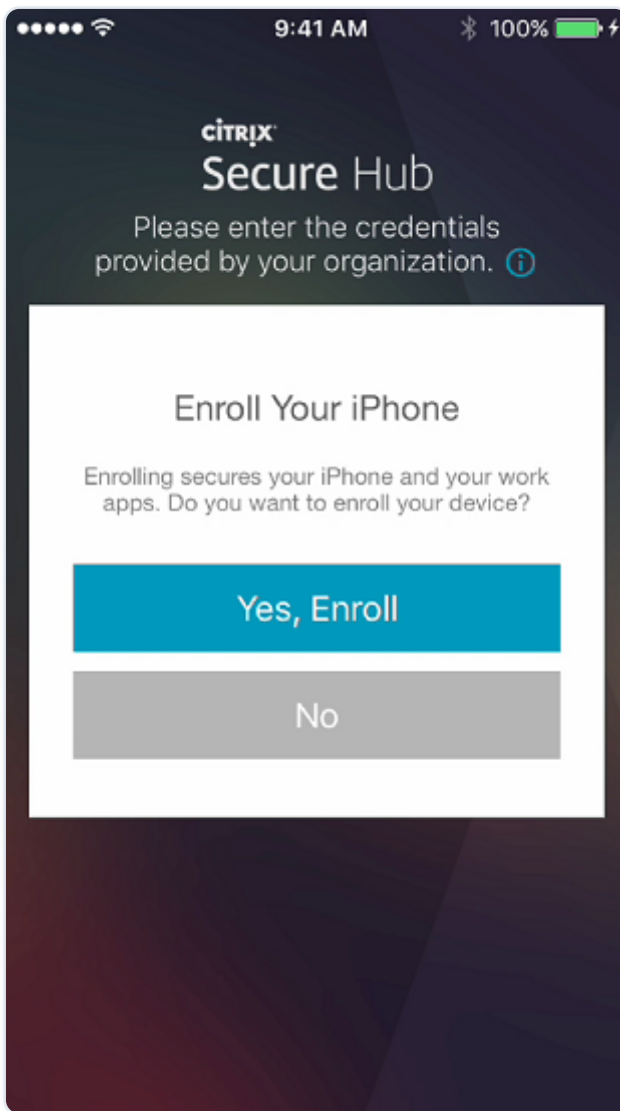
등록하려면 사용자가 스마트 카드를 데스크톱에 연결된 리더에 삽입해야 합니다.

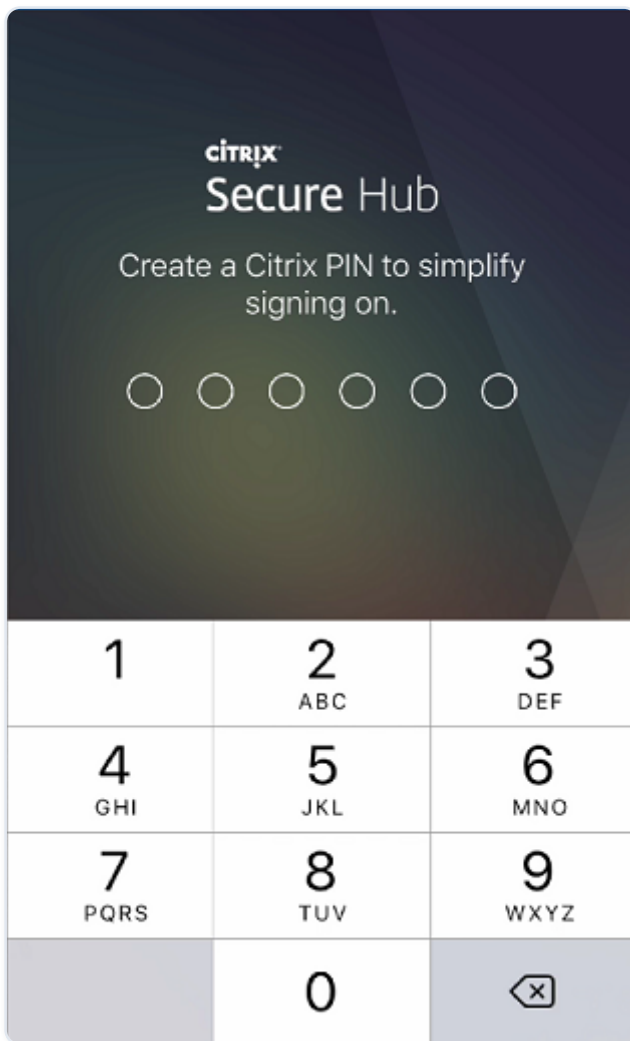
1. 사용자는 Secure Hub와 파생 자격 증명 공급자의 앱을 설치합니다. 이 예에서 ID 공급자 앱은 Intercede MyID Identity Agent입니다.



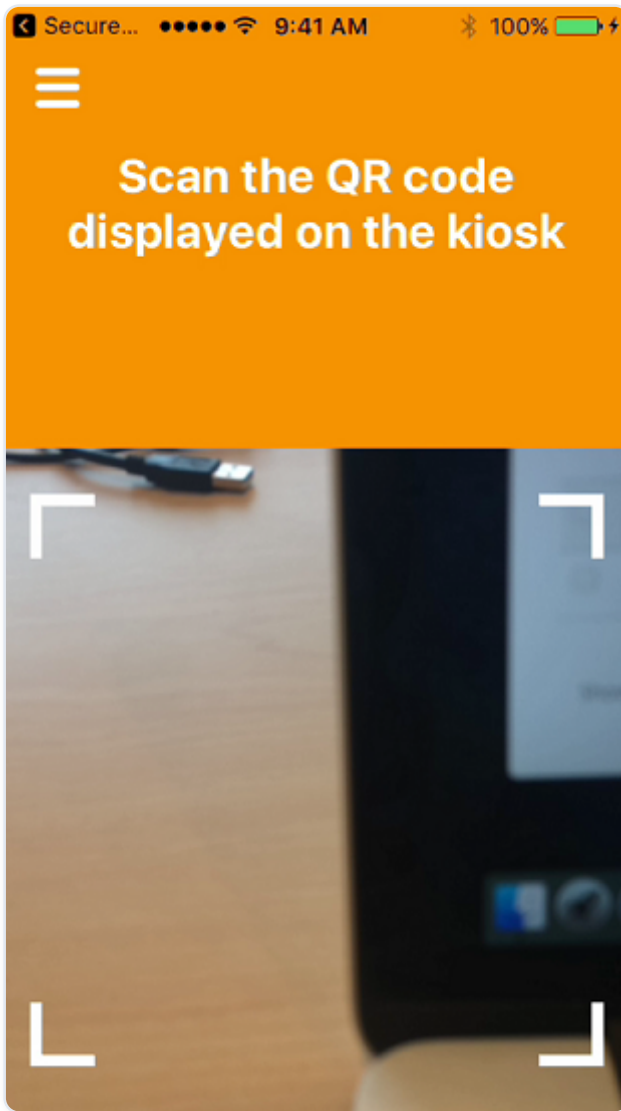
2. 사용자가 Secure Hub를 시작합니다. 메시지가 표시되면 사용자는 Endpoint Management FQDN(정규화된 도메인 이름)을 입력한 다음 다음을 클릭합니다. Secure Hub 등록이 시작됩니다. Endpoint Management가 파생 자격 증명을 지원하는 경우 Secure Hub는 사용자에게 Citrix PIN을 생성하라는 메시지를 표시합니다.







3. 사용자는 지침에 따라 스마트 자격 증명을 활성화합니다. 스플래시 화면이 나타나고 QR 코드를 스캔하라는 메시지가 표시됩니다.



4. 사용자는 카드를 데스크톱에 연결된 스마트 카드 리더에 삽입합니다. 그러면 데스크톱 앱에 QR 코드가 표시되고 사용자에게 모바일 장치를 사용하여 코드를 스캔하라는 메시지가 표시됩니다.

스캔 프롬프트 이미지(/en-us/mobile-productivity-apps/media/derived-credentials-kiosk2.png)

사용자는 메시지가 표시되면 Secure Hub PIN을 입력합니다.

PIN 프롬프트 이미지(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-pin.png)

PIN을 인증한 후 Secure Hub는 인증서를 다운로드합니다. 그런 다음 사용자는 프롬프트에 따라 등록을 완료합니다.

Endpoint Management 콘솔에서 장치 정보를 보려면 다음 중 하나를 수행하십시오.

- **관리 > 장치**로 이동한 다음 장치를 선택하여 명령 상자를 표시합니다. **자세히 표시**를 클릭합니다.
- **분석 > 대시보드**로 이동합니다.

Citrix Endpoint Management™ 콘솔을 통해 힌트 구성

관리자는 등록 모드가 두 가지 요소로 설정된 장치에 대해 Secure Hub 로그인 페이지에 힌트를 구성할 수 있습니다. 다음 방법 중 하나로 힌트를 구성할 수 있습니다.

- 텍스트로 힌트 구성
- 웹 페이지 링크로 힌트 텍스트 구성

텍스트로 힌트 구성

힌트 텍스트를 구성하려면 다음 단계를 수행하십시오.

1. 관리자 자격 증명을 사용하여 Citrix Endpoint Management 콘솔에 로그인합니다.
2. **설정 > 클라이언트 속성**으로 이동하여 **새 클라이언트 속성 추가**를 클릭합니다.
3. 키 드롭다운 목록에서 **사용자 지정 키**를 선택합니다.
4. 키 필드에 **enrollment.twofactor.token.hint**를 입력합니다.
5. 값 필드에 로그인 페이지에 힌트로 표시될 텍스트를 제공할 수 있습니다. 이 힌트는 사용자가 2단계 인증을 위한 PIN을 찾는 데 도움이 됩니다.
6. 이름 필드에 **enrollment.twofactor.token.hint**를 입력합니다.
7. 설명 필드에 구성된 힌트에 대한 설명을 제공할 수 있으며, 이는 향후 참조에 유용할 것입니다.

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. **저장**을 클릭합니다.

구성을 완료하면 로그인 페이지에 힌트 텍스트가 나타납니다.

힌트 텍스트 로그인 페이지 이미지(/en-us/mobile-productivity-apps/media/sh-config-hint-text-2.png)

웹 페이지 링크로 힌트 텍스트 구성

PIN 액세스에 대한 자세한 정보가 포함된 웹 페이지를 구성할 수 있습니다. 나중에 힌트 텍스트에 웹 페이지 링크를 하이퍼링크로 제공합니다. 사용자가 로그인 페이지에서 힌트를 클릭하면 Secure Hub가 내장 브라우저를 열고 이미 구성한 웹 페이지로 이동합니다.

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

1. 관리자 자격 증명을 사용하여 Citrix Endpoint Management 콘솔에 로그인합니다.
2. **설정 > 클라이언트 속성**으로 이동한 다음 **새 클라이언트 속성 추가**를 클릭합니다.
3. **키** 드롭다운 목록에서 **사용자 지정 키**를 선택합니다.
4. **키** 필드에 **enrollment.twofactor.token.hint.url**을 입력합니다.
5. **값** 필드에 구성한 웹 페이지 URL을 입력합니다.
6. **이름** 필드에 **enrollment.twofactor.token.hint.url**을 입력합니다.
7. **설명** 필드에 구성한 힌트에 대한 설명을 제공할 수 있으며, 이는 나중에 참조하는 데 도움이 됩니다.

참고:

사용자가 힌트 링크를 클릭하면 내장 브라우저에 웹 페이지가 나타납니다.

힌트 링크 구성 이미지(/en-us/mobile-productivity-apps/media/sh-config-hint-link-1.png)

8. **저장**을 클릭합니다.

구성을 완료하면 웹페이지 링크가 포함된 힌트 텍스트가 로그인 페이지에 나타납니다.

힌트 링크 로그인 페이지 이미지(/en-us/mobile-productivity-apps/media/sh-config-hint-link-2.png)

Android 기기 규정 준수 확인 (기술 미리 보기)

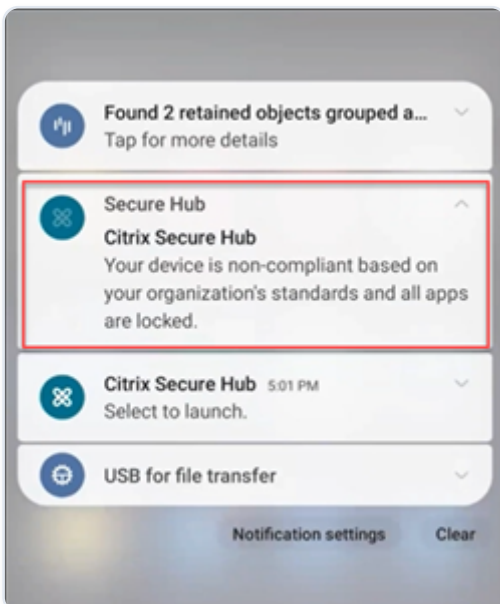
참고:

이 기능은 기기 소유자 모드로 등록된 Android 기기에 적용됩니다.

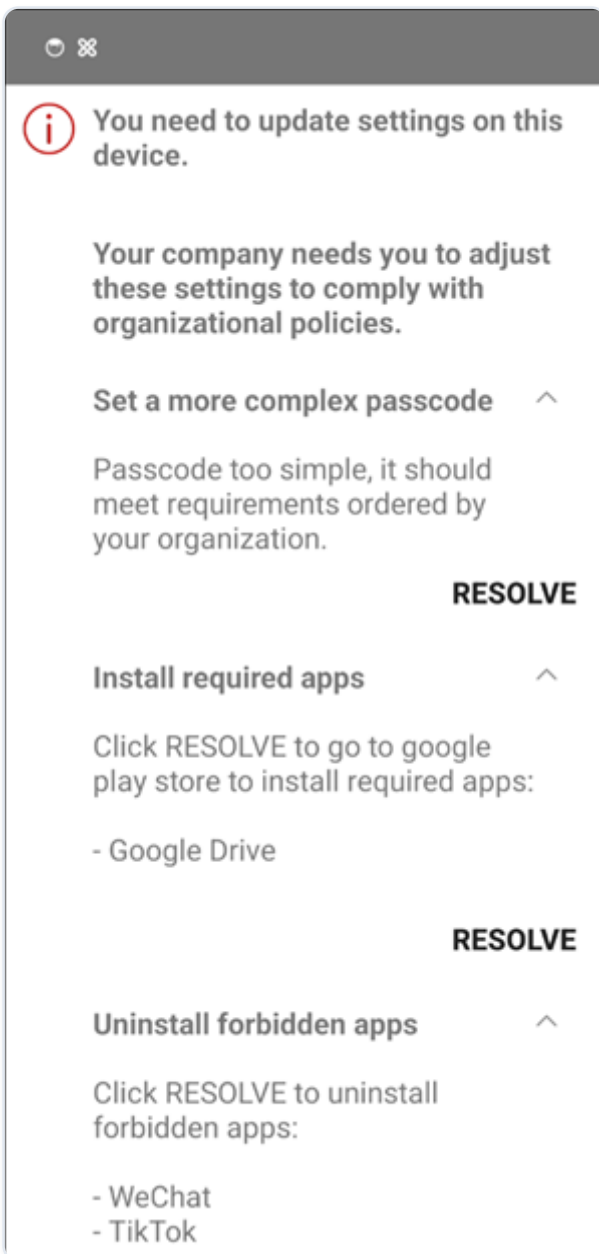
Secure Hub for Android 24.8.0 릴리스부터 Secure Hub는 Citrix Endpoint Management를 통해 관리자가 구성한 정책에 대해 Android 기기의 규정 준수를 확인합니다. 이러한 규정 준수 확인에는 다음이 포함됩니다.

- 기기 암호 강도 보장
- 필수 앱 설치 확인
- 금지된 앱 제거 확인

기기가 규정을 준수하지 않으면 사용자 기기에 다음 알림이 나타납니다.



기기가 규정을 준수하지 않으면 사용자가 Secure Hub를 열 때 다음 메시지가 표시됩니다.



사용자는 **해결** 버튼을 클릭하여 해당 문제를 해결할 수 있습니다.

참고:

- 규정 준수가 충족될 때까지 앱은 잠긴 상태로 유지됩니다.
- 앱 잠금 해제 목록에 추가하여 특정 앱의 잠금을 해제할 수 있습니다. 자세한 내용은 [Android 기기 규정 준수 적용 \(기술 미리 보기\)](#)을 참조하십시오.

정책 및 규정 준수 검사 구성에 대한 자세한 내용은 Citrix Endpoint Management 제품 설명서의 [Android 장치용 규정 준수 적용 \(기술 미리 보기\)](#)을(를) 참조하십시오.