

모바일 생산성 앱

Contents

모바일 생산성 앱 릴리스 타임라인	21
Secure Mail 및 Secure Web 단계별 릴리스 프로세스 정보	21
기능 플래그 관리의 전제 조건	21
모바일 생산성 앱 지원	22
지원되는 운영 체제	22
기타 고려 사항 및 제한 사항	23
보안 메일	23
보안 웹	24
QuickEdit	24
Citrix Content Collaboration™ 엔드포인트 관리용	24
ShareConnect	24
시트릭스 시큐어 노트 및 시트릭스 시큐어 태스크	24
관리자 작업 및 고려 사항	25
기능 플래그 관리	25
다음 URL로 트래픽 활성화	25
도메인별 허용 목록 생성	25
허용 목록에 IP 주소 나열	25
LaunchDarkly 시스템 요구 사항	26
지원되는 앱 스토어	26
공개 앱 스토어 배포 사용	26
Apple 푸시 알림	27
공개 앱 스토어 FAQ	27
안드로이드	28
iOS	28
모바일 생산성 앱용 MDX 정책	30
Android용 Secure Mail의 이중 모드	31

필수 구성 요소	31
제한 사항	32
내부 네트워크에 대한 사용자 연결	33
네트워크 액세스 제한	34
엔드포인트 관리 클라이언트 속성	34
사용자 암호 캐싱	34
비활성 타이머	34
Citrix PIN 인증	34
지문 또는 Touch ID 인증	35
지문 인증 요구 사항	35
지문 인증을 구성하려면	35
구글 애널리틱스	36
Google Analytics 비활성화	36
모바일 생산성 앱용 MDX 정책 한눈에 보기	36
인증	36
장치 암호	36
앱 암호	37
온라인 세션 필수 유예 기간 (분)	37
최대 오프라인 기간	37
대체 Citrix Gateway 설정	37
장치 보안	38
탈옥 또는 루팅된 기기 차단	38
기기 잠금 필요	38
네트워크 요구 사항	38
Wi-Fi 필요	38
허용된 Wi-Fi 네트워크	38
기타 액세스	38
앱 업데이트 유예 기간(시간)	38

필수 업그레이드 비활성화	39
잠금 시 앱 데이터 지우기	39
활성 폴링 기간(분)	39
암호화	39
암호화 유형	39
규정 미준수 기기 동작	40
MDX 암호화 활성화	40
암호화 키	40
개인 파일 암호화	40
개인 파일 암호화 제외	40
공용 파일에 대한 액세스 제한	41
공개 파일 암호화	41
공개 파일 암호화 제외	41
공개 파일 마이그레이션	41
암호화 사용	42
데이터베이스 암호화 제외	42
파일 암호화 제외	42
앱 상호 작용	42
보안 그룹	42
잘라내기 및 복사	42
붙여넣기	43
문서 교환 (다음에서 열기)	43
필터링에서 제외된 URL 도메인	43
허용된 Secure Web 도메인	43
연결 보안 수준	43
인바운드 문서 교환 (Open In)	43
제한된 Open In 예외 목록	44
앱 URL 스키마	44

허용된 URL	44
명시적 로그오프 알림	44
앱 상호 작용(아웃바운드 URL)	44
URL 필터링에서 제외된 도메인	44
허용된 URL	45
허용된 보안 웹 도메인	45
앱 제한	45
카메라 차단	45
갤러리 차단	45
사진 라이브러리 차단	45
마이크 녹음 차단	45
받아쓰기 차단	46
위치 서비스 차단	46
SMS 작성 차단	46
화면 캡처 차단	46
장치 센서 차단	46
NFC 차단	46
iCloud 차단	46
찾아보기 차단	47
파일 백업 차단	47
AirPrint 차단	47
인쇄 차단	47
AirDrop 차단	47
파일 첨부 차단	47
이메일 작성 차단	48
Facebook 및 Twitter API 차단	48
화면 내용 가리기	48
타사 키보드 차단	48

앱 로그 차단	48
ShareFile 사용	48
파일에서 첨부 사용	49
앱 네트워크 액세스	49
네트워크 액세스	49
micro VPN 세션 필요	49
micro VPN 세션 필요 유예 기간(분)	49
제외 목록	49
localhost 연결 차단	49
인증서 레이블	50
앱 로그	50
기본 로그 출력	50
기본 로그 수준	50
최대 로그 파일 수	50
최대 로그 파일 크기	50
앱 로그 리디렉션	50
로그 암호화	51
앱 지오펜스	51
중심점 경도	51
중심점 위도	51
반경	51
앱 설정	51
시큐어 메일 익스체인지 서버	51
Secure Mail 사용자 도메인	52
백그라운드 네트워크 서비스	52
백그라운드 서비스 티켓 만료	52
백그라운드 네트워크 서비스 게이트웨이	52
연락처 내보내기	53

내보낼 연락처 필드	53
모든 SSL 인증서 허용	53
잠금 화면 알림 제어	53
보안 연결 사용	53
기본 이메일 알림	54
기본 동기화 간격	54
메일 검색 제한	54
최대 동기화 간격	54
주 번호 사용	54
Wi-Fi를 통한 첨부 파일 다운로드 사용	54
오프라인 문서 허용	55
정보 권한 관리	55
이메일 분류	55
이메일 분류 표시	55
이메일 분류 네임스페이스	55
이메일 분류 버전	55
기본 이메일 분류	56
초안 이메일 자동 저장 활성화	56
iOS 데이터 보호 활성화	56
푸시 알림 EWS 호스트 이름	56
푸시 알림	56
푸시 알림 지역	56
Secure Mail 첫 시작 시 S/MIME 사용	56
초기 인증 메커니즘	57
초기 인증 자격 증명	57
주 번호 사용	57
캘린더 웹 및 오디오 옵션	57
S/MIME 공개 인증서 원본	57

LDAP 서버 주소	57
LDAP 기본 DN	58
익명으로 LDAP 액세스	58
허용된 이메일 도메인	58
인증 실패 시 사용자 이름 마이그레이션 시도	58
피싱 메일 주소 보고	58
피싱 보고 메커니즘	58
비즈니스용 Skype 회의 도메인	59
캘린더 내보내기	59
Slack 사용	59
Slack 작업 공간 이름	59
발신자 식별	59
분석	60
Google Analytics 사용 설정	60
Google Analytics 세부 정보 수준	60
보고	60
Citrix 보고	60
토큰 업로드	60
Wi-Fi로만 보고서 전송	60
보고 파일 캐시 최대값	61
Office 365용 OAuth 지원	61
Office 365에 최신 인증 사용	61
Office 365 인증 메커니즘	61
신뢰할 수 있는 Exchange Online 호스트 이름	61
신뢰할 수 있는 AD FS 호스트 이름	61
최신 인증을 위한 사용자 지정 사용자 에이전트	61
메일 리디렉션	62
메일 리디렉션	62

Slack 통합	62
Slack 활성화	62
Slack 작업 공간 이름	62
Android용 모바일 생산성 앱을 위한 MDX 정책	62
인증	62
앱 암호	62
최대 오프라인 기간(시간)	63
대체 시트릭스 게이트웨이	63
장치 보안	63
탈옥 또는 루팅된 장치 차단	63
장치 암호화 요구	63
장치 잠금 요구	64
네트워크 요구 사항	64
Wi-Fi 요구	64
허용된 Wi-Fi 네트워크	64
기타 액세스	64
앱 업데이트 유예 기간(시간)	64
필수 업그레이드 비활성화	65
잠금 시 앱 데이터 지우기	65
활성 폴링 기간(분)	65
암호화	66
암호화 유형	66
비규격 장치 동작	66
암호화 키	66
개인 파일 암호화	66
개인 파일 암호화 제외	66
공용 파일에 대한 액세스 제한	67
공용 파일 암호화	67

공용 파일 암호화 제외	67
공용 파일 마이그레이션	68
앱 상호 작용	68
보안 그룹	68
잘라내기 및 복사	69
붙여넣기	69
문서 교환(열기)	69
필터링에서 제외된 URL 도메인	69
허용된 Secure Web 도메인	69
제한된 열기 예외 목록	69
인바운드 문서 교환(열기)	70
인바운드 문서 교환 허용 목록	70
연결 보안 수준	70
앱 제한	70
카메라 차단	71
갤러리 차단	71
마이크 녹음 차단	71
위치 서비스 차단	71
SMS 작성 차단	71
화면 캡처 차단	71
장치 센서 차단	71
NFC 차단	72
앱 로그 차단	72
인쇄 차단	72
ShareFile 사용	72
앱 네트워크 액세스	72
네트워크 액세스	72
Micro VPN 세션 필요	73

제외 목록	73
로컬 호스트 연결 차단	73
인증서 레이블	73
앱 로그	73
기본 로그 출력	73
기본 로그 수준	73
최대 로그 파일 수	74
최대 로그 파일 크기	74
앱 로그 리디렉션	74
로그 암호화	74
앱 지오펜스	75
중심점 경도	75
중심점 위도	75
반경	75
분석	75
Google Analytics 상세 정보	75
앱 설정	75
보안 메일 Exchange 서버	75
Secure Mail 사용자 도메인	76
백그라운드 네트워크 서비스	76
백그라운드 서비스 티켓 만료	76
백그라운드 네트워크 서비스 게이트웨이	76
연락처 내보내기	76
내보낼 연락처 필드	77
모든 SSL 인증서 허용	77
보안 연결 사용	77
정보 권한 관리	77
잠금 화면 알림 제어	77

기본 동기화 간격	77
Wi-Fi를 통한 첨부 파일 다운로드 활성화	78
오프라인 문서 허용	78
이메일 초안 자동 저장 활성화	78
초기 인증 메커니즘	78
초기 인증 자격 증명	78
주 번호 사용	78
이메일 분류	78
이메일 분류 표시	78
이메일 분류 네임스페이스	79
이메일 분류 버전	79
기본 이메일 분류	79
메일 검색 제한	79
최대 동기화 간격	79
캘린더 웹 및 오디오 옵션	79
S/MIME 공개 인증서 원본	80
LDAP 서버 주소	80
LDAP 기본 DN	80
익명으로 LDAP 액세스	80
허용된 이메일 도메인	80
푸시 알림	80
푸시 알림 EWS 호스트 이름	80
푸시 알림 지역	80
인증 실패 시 사용자 이름 마이그레이션 시도	81
피싱 메일 주소 보고	81
피싱 보고 메커니즘	81
비즈니스용 Skype 모임 도메인	81
캘린더 내보내기	82

Office 365용 OAuth 지원	82
O365용 최신 인증 사용	82
신뢰할 수 있는 Exchange Online 호스트 이름	82
신뢰할 수 있는 AD FS 호스트 이름	82
최신 인증을 위한 사용자 지정 사용자 에이전트	83
Slack 통합	83
Slack 사용	83
Slack 작업 공간 이름	83
iOS용 모바일 생산성 앱을 위한 MDX 정책	83
인증	83
장치 암호	83
앱 암호	83
최대 오프라인 기간(시간)	84
대체 시트릭스 게이트웨이	84
장치 보안	84
탈옥 또는 루팅 차단	84
네트워크 요구 사항	84
Wi-Fi 필요	84
허용된 Wi-Fi 네트워크	84
기타 액세스	85
필수 업그레이드 비활성화	85
앱 업데이트 유예 기간(시간)	85
잠금 시 앱 데이터 지우기	85
활성 폴링 기간(분)	85
암호화	86
암호화 유형	86
비준수 장치 동작	86
MDX 암호화 사용	86

데이터베이스 암호화 제외	86
파일 암호화 제외	87
앱 상호 작용	87
잘라내기 및 복사	87
붙여넣기	87
문서 교환 (다음으로 열기)	87
제한된 Open-In 예외 목록	88
연결 보안 수준	88
인바운드 문서 교환(Open In)	88
앱 URL 스키마	88
앱 상호 작용 (아웃바운드 URL)	89
URL 필터링에서 제외된 도메인	89
허용된 URL	90
허용된 Secure Web 도메인	92
앱 제한	92
카메라 차단	92
사진 보관함 차단	92
마이크 녹음 차단	92
받아쓰기 차단	92
위치 서비스 차단	93
SMS 작성 차단	93
이메일 작성 차단	93
iCloud 차단	93
조회 차단	93
파일 백업 차단	93
AirPrint 차단	93
AirDrop 차단	93
파일 첨부 차단	94

Facebook 및 Twitter API 차단	94
화면 내용 가리기	94
타사 키보드 차단(iOS 11 이상만 해당)	94
앱 로그 차단	94
ShareFile 사용	94
파일에서 첨부 사용	94
앱 네트워크 액세스	94
네트워크 액세스	94
Micro VPN 세션 필요	95
Micro VPN 세션 필요 유예 기간(분)	95
인증서 레이블	95
제외 목록	95
앱 로그	96
기본 로그 출력	96
기본 로그 수준	96
최대 로그 파일	96
최대 로그 파일 크기	96
앱 지오펜스	96
중심점 경도	96
중심점 위도	97
반경	97
Google 애널리틱스 활성화	97
분석	97
Google Analytics 세부 정보 수준	97
보고	97
Citrix 보고	97
업로드 토큰	98
Wi-Fi로만 보고서 전송	98

보고서 파일 캐시 최대값	98
앱 상호 작용	98
명시적 로그오프 알림	98
앱 설정	98
보안 메일 익스체인지 서버	98
Secure Mail 사용자 도메인	98
백그라운드 네트워크 서비스	99
백그라운드 서비스 티켓 만료	99
백그라운드 네트워크 서비스 게이트웨이	99
연락처 내보내기	99
내보낼 연락처 필드	100
모든 SSL 인증서 허용	100
잠금 화면 알림 제어	100
기본 이메일 알림	100
기본 동기화 간격	100
메일 검색 제한	100
최대 동기화 간격	101
주 번호 사용	101
Wi-Fi를 통한 첨부 파일 다운로드 사용	101
오프라인 문서 허용	101
정보 권한 관리	101
이메일 분류	101
이메일 분류 표시	101
이메일 분류 네임스페이스	101
이메일 분류 버전	102
기본 이메일 분류	102
이메일 초안 자동 저장 사용	102
초기 인증 메커니즘	102

초기 인증 자격 증명	102
사용자 이름 자동 채우기 사용	102
iOS 데이터 보호 사용	102
푸시 알림 EWS 호스트 이름	103
푸시 알림	103
푸시 알림 지역	103
S/MIME 공개 인증서 원본	103
Secure Mail 첫 시작 시 S/MIME 활성화	103
캘린더 웹 및 오디오 옵션	104
S/MIME 공개 인증서 소스	104
LDAP 서버 주소	104
LDAP 기본 DN	104
LDAP 익명 액세스	104
허용된 이메일 도메인	104
인증 실패 시 사용자 이름 마이그레이션 시도	104
피싱 메일 주소 보고	104
피싱 보고 메커니즘	105
비즈니스용 Skype 모임 도메인	105
캘린더 내보내기	106
발신자 식별	106
Office 365용 OAuth 지원	106
Office 365 인증 메커니즘	106
신뢰할 수 있는 Exchange Online 호스트 이름	106
신뢰할 수 있는 AD FS 호스트 이름	107
메일 리디렉션	107
메일 리디렉션	107
Slack 통합	107
Slack 사용	107

Slack 작업 공간 이름	107
플랫폼별 기능	108
시트릭스 시큐어 허브™	108
시트릭스 보안 메일	109
시트릭스 시큐어 웹™	119
기능 플래그 관리	122
IP 주소	122
시스템 요구 사항	122
시트릭스 시큐어 허브™	124
Secure Hub 관리	124
시트릭스 핀	124
인증서 고정	125
Secure Hub용 인증서 + 일회용 암호 인증 구성	126
Android 장치용 ADS 연결을 위한 포트 요구 사항	130
Secure Hub 기능	132
Secure Mail 개요	135
시트릭스 시큐어 웹™	137
Secure Web 통합 및 제공	137
사용자 연결 구성	138
Secure Web 정책	139
허용 또는 차단된 웹사이트	139
팝업 차단	140
미리 로드된 즐겨찾기	140
홈 페이지 URL	140
브라우저 사용자 인터페이스	140
옵션	140
웹 암호 캐싱 사용	141
프록시 서버	141

DNS 접미사	141
Secure Web용 인트라넷 사이트 준비	141
인트라넷 사이트 문제 해결	142
웹 아카이브 파일 생성 방법	143
Secure Web 기능	144
엔드포인트 관리용 Citrix Content Collaboration™	146
Endpoint Management용 Citrix Content Collaboration 클라이언트가 Citrix Files 모바일 클라이언트와 다른 점	147
사용자 액세스	147
SSO	147
마이크로 VPN	147
2단계 인증	148
폴더 권한	148
문서 액세스 보호	148
Citrix Files 계정 액세스	148
장치 정책	149
MDX 정책	149
데이터 암호화	149
가용성	149
Endpoint Management 클라이언트를 위한 Citrix Content Collaboration 통합 및 제공	150
SSO를 위해 Endpoint Management에서 Citrix Files 계정 정보 구성	151
Endpoint Management에 Endpoint Management 클라이언트용 Citrix Content Collaboration을 추가하려면	151
필수 구성 요소	151
Citrix Content Collaboration for Endpoint Management 클라이언트의 유효성을 검사하려면	153
EOL 및 지원 중단된 앱	154
Office 365 앱과의 보안 상호 작용 허용	156
iOS에서 Office 365 활성화	156

Android에서 Office 365 활성화	157
지원되는 파일 형식	157
모바일 생산성 앱 문서 기록	158

모바일 생산성 앱 릴리스 타임라인

Citrix® 모바일 생산성 앱은 2주 간격으로 릴리스됩니다. 정확한 날짜는 변경될 수 있지만, 이 주기를 알면 미리 계획하는 데 도움이 됩니다. 또한 앱 배포 및 업데이트를 더 쉽게 관리할 수 있도록 지원하고자 합니다.

Secure Mail 및 Secure Web 단계별 릴리스 프로세스 정보

Secure Mail 및 Secure Web의 새 버전이 출시되면 다음과 같이 단계별로 릴리스가 배포됩니다.

- iOS 및 Android 사용자의 경우 Secure Mail 및 Secure Web 업데이트는 일주일(7일) 동안 App Store 및 Google Play 스토어에서 점진적으로 더 많은 사용자에게 제공됩니다.
- iOS용 Secure Mail 및 Secure Web의 신규 다운로드는 이번 주 내에 새 버전을 받게 됩니다. Android용 Secure Mail 및 Secure Web의 신규 다운로드는 새 릴리스의 배포가 모든 사용자의 100%에 도달할 때까지 일주일 동안 이전 버전을 실행합니다.
- 사용자의 경우 일부 기능은 점진적인 단계로 릴리스됩니다.

기능 플래그 관리의 전제 조건

프로덕션 환경에서 Secure Hub 또는 Secure Mail에 문제가 발생하면 앱 코드 내에서 영향을 받는 기능을 비활성화할 수 있습니다. 이를 위해 기능 플래그와 LaunchDarkly라는 타사 서비스를 사용합니다. 방화벽 또는 프록시가 아웃바운드 트래픽을 차단하는 경우를 제외하고는 LaunchDarkly로의 트래픽을 활성화하기 위해 어떤 구성도 할 필요가 없습니다. 이 경우 정책 요구 사항에 따라 특정 URL 또는 IP 주소를 통해 LaunchDarkly로의 트래픽을 활성화합니다. 모바일 생산성 앱 10.6.15부터 터널링에서 도메인 제외에 대한 MDX 지원에 대한 자세한 내용은 [MDX Toolkit documentation](#)을 참조하십시오. 기능 플래그 및 LaunchDarkly에 대한 FAQ는 이 [Support Knowledge Center article](#)을 참조하십시오.

참고: 단계적으로 중단되는 Citrix Endpoint Management 기능에 대한 사전 통지는 [Deprecation](#)을 참조하십시오.

모바일 생산성 앱 지원

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

- 23.10.0 (Android용 시큐어 웹)
- 23.9.0 (iOS용 시큐어 메일 및 시큐어 웹)
- 23.8.2 (Android용 보안 메일)

Citrix®는 모바일 생산성 앱의 이전 두 버전에서 업그레이드를 지원합니다. 모바일 생산성 앱의 이전 두 버전은 다음과 같습니다.

- 23.8.1 (Android용 보안 메일)
- 23.8.0 (Android용 보안 웹)
- 23.7.0 (Android용 보안 메일 및 iOS용 보안 메일)
- 23.5.0 (iOS용 시큐어 메일, 및 Android용 시큐어 웹)
- 23.2.0 (iOS용 시큐어 웹)
- 22.9.1 (iOS용 보안 웹)

중요:

MDX 암호화는 September 1, 2020에 수명 종료(EOL)에 도달했습니다. 레거시 장치 관리(DA)에 등록된 장치의 경우:

- MDX 암호화를 사용하지 않는 경우 별도의 조치가 필요하지 않습니다.
- MDX 암호화를 사용하는 경우, Android 장치를 Android Enterprise로 마이그레이션하십시오. Android 10을 실행하는 장치는 Android Enterprise를 사용하여 등록하거나 재등록해야 합니다. 여기에는 MAM 전용 모드의 Android 장치도 포함됩니다. 자세한 내용은 [장치 관리를 Android Enterprise로 마이그레이션](#)을 참조하십시오.

지원되는 운영 체제

모바일 생산성 앱은 다음 운영 체제를 지원합니다.

제품 이름	운영 체제	최소 배포 버전	사용 가능한 최신 버전
시큐어 허브	안드로이드	7.x	14.x
동일	iOS	12.x	17.x
시큐어 메일	안드로이드	8.x	14.x
	iOS	13.x	17.x
시큐어 웹	안드로이드	8.x	14.x
	iOS	13.x	17.x

Mobile productivity apps의 최신 버전은 Citrix Endpoint Management의 최신 버전 및 이전 두 버전과 호환됩니다. Citrix Endpoint Management에서 지원하는 운영 체제에 대한 자세한 내용은 [지원되는 장치 운영 체제](#)를 참조하십시오.

Mobile productivity apps의 최신 버전에는 Secure Hub의 최신 버전이 필요합니다. Secure Hub를 최신 상태로 유지하십시오.

참고:

Citrix는 항상 Android 및 iOS 운영 체제의 최신 버전과 이전 두 버전(N, N-1, N-2)만 지원합니다.

기타 고려 사항 및 제한 사항

단계적으로 중단되는 Citrix Endpoint Management 기능에 대한 사전 알림은 [사용 중단](#)을 참조하십시오.

보안 메일

- Endpoint Management는 Secure Ticket Authority(STA) 및 Secure Mail 문제로 인해 현재 NetScaler 12.0.41.16을 지원하지 않습니다. 이 문제는 NetScaler 12.0 빌드 41.22에서 해결되었습니다.
- Exchange 2007 및 Lotus Notes 8.5.3용 Secure Mail 지원은 September 30, 2017에 수명 종료(EOL)에 도달했습니다.
- Citrix Files 첨부 파일을 보낼 때 최상의 성능을 위해 최신 버전의 Citrix Files를 사용하는 것이 좋습니다. Citrix Files는 Windows에서 지원되지 않습니다.

- IBM Notes 환경에서는 IBM Domino Traveler 서버 버전 9.0을 구성해야 합니다. 자세한 내용은 Exchange Server 또는 IBM Notes Traveler Server 통합을 참조하십시오.

참고:

- XenMobile용 Citrix Files는 July 1, 2023에 EOL에 도달했습니다. 자세한 내용은 [EOL 및 사용 중단된 앱을 참조하십시오](#).

보안 웹

기기에 최신 버전의 Android WebView를 설치하십시오. 사용자는 Google Play 스토어에서 Android WebView를 다운로드할 수 있습니다.

QuickEdit

QuickEdit은 모바일 생산성 앱으로 계속 사용할 수 있습니다. 이전에 공지된 바와 같이 수명 종료(EOL) 상태는 September 1, 2018에 적용되지 않습니다.

Citrix Content Collaboration™ 엔드포인트 관리용

사용자는 버전 6.5 이후부터 공용 앱 스토어에서 Citrix Content Collaboration for Endpoint Management에 액세스할 수 있습니다.

ShareConnect

ShareConnect은 June 30, 2020에 수명 종료(EOL)에 도달했습니다. 자세한 내용은 [EOL 및 사용 중단된 앱을 참조하십시오](#).

시트릭스 시큐어 노트 및 시트릭스 시큐어 태스크

Citrix Secure Notes 및 Citrix Secure Tasks는 December 31, 2018에 수명 종료(EOL) 상태에 도달했습니다. 자세한 내용은 [EOL 및 사용 중단된 앱을 참조하십시오](#).

관리자 작업 및 고려 사항

이 문서에서는 모바일 생산성 앱 관리자에게 관련된 작업 및 고려 사항에 대해 설명합니다.

기능 플래그 관리

프로덕션 환경에서 모바일 생산성 앱에 문제가 발생하면 앱 코드 내에서 영향을 받는 기능을 비활성화할 수 있습니다. iOS 및 Android용 Secure Hub, Secure Mail, Secure Web의 기능을 비활성화할 수 있습니다. 이를 위해 기능 플래그와 LaunchDarkly라는 타사 서비스를 사용합니다. 방화벽 또는 프록시가 아웃바운드 트래픽을 차단하는 경우를 제외하고 LaunchDarkly로의 트래픽을 활성화하기 위한 구성은 필요하지 않습니다. 이 경우 정책 요구 사항에 따라 특정 URL 또는 IP 주소를 통해 LaunchDarkly로의 트래픽을 활성화합니다. 터널링에서 도메인 제외 지원에 대한 자세한 내용은 [MAM SDK 설명서](#)를 참조하십시오.

다음 방법으로 LaunchDarkly로의 트래픽 및 통신을 활성화할 수 있습니다.

다음 URL로 트래픽 활성화

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

도메인별 허용 목록 생성

이전에는 내부 정책에서 IP 주소만 나열하도록 요구하는 경우 사용할 IP 주소 목록을 제공했습니다. 이제 Citrix®가 인프라 개선을 완료함에 따라 July 16, 2018부터 공용 IP 주소를 단계적으로 폐지하고 있습니다. 가능한 경우 도메인별 허용 목록을 생성하는 것이 좋습니다.

허용 목록에 IP 주소 나열

허용 목록에 IP 주소를 나열해야 하는 경우, 모든 현재 IP 주소 범위 목록은 이 [LaunchDarkly 공용 IP 목록](#)을 참조하십시오. 이 목록을 사용하여 인프라 업데이트에 따라 방화벽 구성이 자동으로 업데이트되도록 할 수 있습니다. 인프라 변경 상태에 대한 자세한 내용은 [LaunchDarkly 상태 페이지](#)를 참조하십시오.

참고:

공개 앱 스토어 앱은 처음 배포할 때 새로 설치해야 합니다. 현재 엔터프라이즈 래핑 버전의 앱에서 공개 스토어 버전으로 업그레이드할 수 없습니다.

공개 앱 스토어 배포의 경우 MDX Toolkit으로 Citrix 개발 앱에 서명하고 래핑하지 않습니다. MDX Toolkit을 사용하여 타사 또는 엔터프라이즈 앱을 래핑할 수 있습니다.

LaunchDarkly 시스템 요구 사항

- 엔드포인트 관리 10.7 이상.
- Citrix ADC에서 분할 터널링이 **OFF**로 설정된 경우 앱이 다음 서비스와 통신할 수 있는지 확인하십시오.
 - LaunchDarkly 서비스
 - APNs 수신기 서비스

지원되는 앱 스토어

모바일 생산성 앱은 Apple App Store 및 Google Play에서 사용할 수 있습니다.

Google Play를 사용할 수 없는 중국에서는 Android용 Secure Hub를 다음 앱 스토어에서 사용할 수 있습니다.

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

공개 앱 스토어 배포 사용

1. [Endpoint Management 다운로드 페이지](#)에서 iOS 및 Android용 공개 스토어 .mdx 파일을 다운로드하십시오.
2. .mdx 파일을 Endpoint Management 콘솔에 업로드합니다. 모바일 생산성 앱의 공개 스토어 버전은 여전히 MDX 애플리케이션으로 업로드됩니다. 서버에 앱을 공개 스토어 앱으로 업로드하지 마십시오. 단계는 [앱 추가](#)를 참조하십시오.
3. 보안 정책에 따라 정책을 기본값에서 변경합니다(선택 사항).
4. 필수 앱으로 앱을 푸시합니다(선택 사항). 이 단계에서는 모바일 장치 관리가 환경에서 활성화되어 있어야 합니다.
5. App Store, Google Play 또는 Endpoint Management 앱 스토어에서 장치에 앱을 설치합니다.

- Android에서는 사용자가 Play 스토어로 이동하여 앱을 설치합니다. iOS에서는 MDM이 있는 배포에서 사용자가 앱 스토어로 이동하지 않고 앱이 설치됩니다.
- App Store 또는 Play 스토어에서 앱을 설치하면 다음 작업이 발생합니다. 해당 .mdx 파일이 서버에 업로드되어 있는 한 앱은 관리되는 앱으로 전환됩니다. 관리되는 앱으로 전환될 때 앱은 Citrix PIN을 요청합니다. 사용자가 Citrix PIN을 입력하면 Secure Mail에 계정 구성 화면이 표시됩니다.

6. 앱은 Secure Hub에 등록되어 있고 해당 .mdx 파일이 서버에 있는 경우에만 액세스할 수 있습니다. 두 조건 중 하나라도 충족되지 않으면 사용자는 앱을 설치할 수 있지만 앱 사용은 차단됩니다.

현재 공개 앱 스토어에 있는 Citrix Ready Marketplace™의 앱을 사용하는 경우 배포 프로세스에 이미 익숙할 것입니다. 모바일 생산성 앱은 많은 ISV가 현재 사용하는 것과 동일한 접근 방식을 채택합니다. 앱 내에 MDX SDK를 포함하여 앱을 공개 스토어에 게시할 준비를 합니다.

참고:

iOS 및 Android용 Citrix Files 앱의 공개 스토어 버전은 이제 유니버설입니다. Citrix Files 앱은 휴대폰과 태블릿에서 동일합니다.

Apple 푸시 알림

푸시 알림 구성에 대한 자세한 내용은 [푸시 알림용 Secure Mail 구성](#)을 참조하십시오.

공개 앱 스토어 FAQ

- 공개 스토어 앱의 여러 복사본을 다른 사용자 그룹에 배포할 수 있습니까? 예를 들어, 다른 사용자 그룹에 다른 정책을 배포하고 싶습니다.

각 사용자 그룹에 대해 다른 .mdx 파일을 업로드합니다. 그러나 이 경우 단일 사용자는 여러 그룹에 속할 수 없습니다. 사용자가 여러 그룹에 속하는 경우 동일한 앱의 여러 복사본이 해당 사용자에게 할당됩니다. 앱 ID를 변경할 수 없으므로 공개 스토어 앱의 여러 복사본을 동일한 장치에 배포할 수 없습니다.

- 공개 스토어 앱을 필수 앱으로 푸시할 수 있습니까?

예. 장치에 앱을 푸시하려면 MDM이 필요하며, MAM 전용 배포에서는 지원되지 않습니다.

- 사용자 에이전트를 기반으로 하는 트래픽 정책 또는 Exchange Server 규칙을 업데이트해야 합니까?

플랫폼별 사용자 에이전트 기반 정책 및 규칙에 대한 문자열은 다음과 같습니다.

중요:

Secure Notes 및 Secure Tasks는 December 31, 2018에 수명 종료(EOL) 상태에 도달했습니다. 자세한 내용은 [EOL 및 더 이상 사용되지 않는 앱을 참조하십시오](#).

안드로이드

앱	서버	사용자 에이전트 문자열
Citrix 시큐어 메일™	익스체인지	WorxMail
	로터스 노트 트래블러	Apple - iPhone 워크스메일
시트릭스 시큐어 웹™		WorxMail
시트릭스 시큐어 태스크	익스체인지	WorxMail
시트릭스 시큐어 노트	익스체인지	WorxMail
	시트릭스 파일	시큐어 노트

iOS

앱	서버	사용자 에이전트 문자열
시트릭스 시큐어 메일	익스체인지	WorxMail
	로터스 노트 트래블러	Apple - iPhone 워크스메일
Citrix 시큐어 웹		com.citrix.browser
Citrix 시큐어 태스크	익스체인지	WorxTasks
Citrix 시큐어 노트	익스체인지	WorxNotes
	Citrix 파일	시큐어 노트

- 앱 업그레이드를 방지할 수 있습니까?

아니요. 공용 앱 스토어에 업데이트가 게시되면 자동 업데이트가 활성화된 모든 사용자가 업데이트를 받습니다.

- 앱 업그레이드를 강제할 수 있습니까?

예, 업그레이드는 업그레이드 유예 기간 정책을 통해 강제 적용됩니다. 이 정책은 업데이트된 앱 버전에 해당하는 새 .mdx 파일이 Endpoint Management에 업로드될 때 설정됩니다.

- 업데이트 타임라인을 제어할 수 없는 경우 업데이트가 사용자에게 도달하기 전에 앱을 어떻게 테스트합니까?

Secure Hub와 유사하게, EAR 기간 동안 iOS용 TestFlight에서 앱을 테스트할 수 있습니다. Android의 경우 EAR 기간 동안 Google Play 베타 프로그램을 통해 앱을 사용할 수 있습니다. 이 기간 동안 앱 업데이트를 테스트할 수 있습니다.

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

업데이트된 앱은 이전 .mdx 파일과 호환됩니다. 새 정책에 종속되는 새로운 기능은 활성화되지 않습니다.

- Secure Hub가 설치되면 앱이 관리형으로 전환됩니까, 아니면 앱을 등록해야 합니까?

공용 스토어 앱이 관리형 앱(MDX로 보호됨)으로 활성화되고 사용 가능하려면 사용자가 Secure Hub에 등록되어야 합니다. Secure Hub가 설치되었지만 등록되지 않은 경우 사용자는 공용 스토어 앱을 사용할 수 없습니다.

- 공용 스토어 앱에 Apple Enterprise 개발자 계정이 필요합니까?

아니요. Citrix가 이제 모바일 생산성 앱에 대한 인증서 및 프로비저닝 프로필을 유지 관리하므로, 사용자에게 앱을 배포하는 데 Apple Enterprise 개발자 계정이 필요하지 않습니다.

- 엔터프라이즈 배포 종료가 배포한 모든 래핑된 애플리케이션에 적용됩니까?

아니요, 모바일 생산성 앱인 Secure Mail, Secure Web, Endpoint Management용 Citrix Content Collaboration™, QuickEdit 및 ShareConnect에만 적용됩니다. 사내에서 개발되었거나 타사에서 개발된 배포된 모든 엔터프라이즈 래핑 앱은 계속해서 엔터프라이즈 래핑을 사용할 수 있습니다. MDX Toolkit은 앱 개발자를 위한 엔터프라이즈 래핑을 계속 지원합니다.

- Google Play에서 앱을 설치할 때 오류 코드 505와 함께 Android 오류가 발생합니다.

참고:

Android 5.x 지원은 December 31, 2018에 종료되었습니다.

이는 Google Play 및 Android 5.x 버전의 알려진 문제입니다. 이 오류가 발생하면 다음 단계에 따라 앱 설치를 방해하는 장치의 오래된 데이터를 지울 수 있습니다.

1. 장치를 다시 시작합니다.
2. 장치 설정을 통해 Google Play의 캐시 및 데이터를 지웁니다.

3. 최후의 수단으로 장치에서 Google 계정을 제거한 다음 다시 추가합니다.

자세한 내용은 다음 키워드 "Fix Google Play Store Error 505 in Android: Unknown Error Code"를 사용하여 이 [사이트](#)를 검색하십시오.

- Google Play의 앱이 프로덕션에 릴리스되었고 새로운 베타 릴리스를 사용할 수 없는데도 Google Play의 앱 제목 뒤에 Beta가 표시되는 이유는 무엇입니까?

얼리 액세스 릴리스(EAR) 프로그램에 참여하는 경우 앱 제목 옆에 항상 Beta가 표시됩니다. 이 이름은 특정 앱에 대한 사용자의 액세스 수준을 단순히 알려줍니다. Beta 이름은 사용자가 사용 가능한 앱의 최신 버전을 받는다는 것을 나타냅니다. 최신 버전은 프로덕션 트랙 또는 베타 트랙에 게시된 최신 버전일 수 있습니다.

- 앱을 설치하고 열면 .mdx 파일이 Endpoint Management 콘솔에 있음에도 불구하고 사용자에게 '앱이 승인되지 않음' 메시지가 표시됩니다.

이 문제는 사용자가 App Store 또는 Google Play에서 직접 앱을 설치하고 Secure Hub가 새로 고쳐지지 않은 경우 발생할 수 있습니다. 비활성 타이머가 만료되면 Secure Hub를 새로 고쳐야 합니다. 사용자가 Secure Hub를 열고 다시 인증하면 정책이 새로 고쳐집니다. 사용자가 다음에 앱을 열 때 앱이 승인됩니다.

- 앱을 사용하려면 액세스 코드가 필요합니까? App Store 또는 Play Store에서 앱을 설치할 때 액세스 코드를 입력하라는 메시지가 표시됩니다.

액세스 코드를 요청하는 화면이 표시되면 Secure Hub를 통해 Endpoint Management에 등록되지 않은 것입니다. Secure Hub에 등록하고 앱의 .mdx 파일이 서버에 배포되었는지 확인하십시오. 또한 앱을 사용할 수 있는지 확인하십시오. 액세스 코드는 Citrix 내부용으로만 제한됩니다. 앱을 활성화하려면 Endpoint Management 배포가 필요합니다.

- VPP 또는 DEP를 통해 iOS 공개 스토어 앱을 배포할 수 있습니까?

Endpoint Management는 MDX가 활성화되지 않은 공개 스토어 앱의 VPP 배포에 최적화되어 있습니다. VPP를 통해 Endpoint Management 공개 스토어 앱을 배포할 수 있지만, 제한 사항을 해결하기 위해 Endpoint Management 및 Secure Hub 스토어에 대한 추가 개선 사항이 적용될 때까지 배포가 최적화되지 않습니다. VPP를 통해 Endpoint Management 공개 스토어 앱을 배포할 때 알려진 문제 목록과 잠재적인 해결 방법에 대해서는 [Citrix 지식 센터](#)의 이 문서를 참조하십시오.

모바일 생산성 앱용 MDX 정책

MDX 정책을 사용하면 Endpoint Management가 적용하는 설정을 구성할 수 있습니다. 이 정책은 인증, 장치 보안, 네트워크 요구 사항 및 액세스, 암호화, 앱 상호 작용, 앱 제한 등을 다룹니다. 많은 MDX 정책이 모든 모바일 생산성 앱에 적용됩니다. 일부 정책은 앱별로 다릅니다.

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

MDX 정책에 대한 자세한 설명은 이 섹션의 다음 문서를 참조하십시오.

- [모바일 생산성 앱용 MDX 정책 한눈에 보기](#)
- [Android용 모바일 생산성 앱용 MDX 정책](#)
- [iOS용 모바일 생산성 앱용 MDX 정책](#)

다음 섹션에서는 사용자 연결과 관련된 MDX 정책에 대해 설명합니다.

Android용 Secure Mail의 이중 모드

모바일 애플리케이션 관리(MAM) SDK는 iOS 및 Android 플랫폼에서 다루지 않는 MDX 기능 영역을 대체하는 데 사용할 수 있습니다. MDX 래핑 기술은 2021년 9월에 수명 종료(EOL)에 도달할 예정입니다. 엔터프라이즈 애플리케이션을 계속 관리하려면 MAM SDK를 통합해야 합니다.

버전 20.8.0부터 Android 앱은 앞서 언급한 MDX EOL 전략에 대비하기 위해 MDX 및 MAM SDK와 함께 릴리스됩니다. MDX 이중 모드는 현재 MDX Toolkit에서 새로운 MAM SDK로 전환하는 방법을 제공하기 위한 것입니다. 이중 모드를 사용하면 다음 중 하나를 수행할 수 있습니다.

- MDX Toolkit(현재 Endpoint Management 콘솔에서 레거시 MDX로 명명됨)을 사용하여 앱 관리 계속
- 새로운 MAM SDK를 통합하는 앱 관리.

참고:

MAM SDK를 사용하는 경우 앱을 래핑할 필요가 없습니다.

MAM SDK로 전환한 후에는 추가 단계가 필요하지 않습니다.

MAM SDK에 대한 자세한 내용은 다음 문서를 참조하십시오.

- [MAM SDK 개요](#)
- [MAM SDK의 최신 릴리스](#)
- Citrix 개발자 섹션의 [장치 관리](#)
- [Citrix 블로그 게시물](#)

필수 구성 요소

이중 모드 기능을 성공적으로 배포하려면 다음 사항을 확인하십시오.

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

참고:

MAM SDK는 모든 클라우드 기반 고객에게 지원됩니다.

제한 사항

- MAM SDK는 Citrix Endpoint Management™ 배포에서 Android Enterprise 플랫폼에 게시된 앱만 지원합니다. 새로 게시된 앱의 경우 기본 암호화는 플랫폼 기반 암호화입니다.
- MAM SDK는 플랫폼 기반 암호화만 지원하며 MDX 암호화는 지원하지 않습니다.
- Citrix Endpoint Management를 업데이트하지 않고 모바일 앱에 대해 정책 파일이 버전 20.8.0 이상에서 실행되는 경우 Secure Mail에 대해 네트워킹 정책의 중복 항목이 생성됩니다.

Citrix Endpoint Management에서 Secure Mail을 구성할 때 이중 모드 기능을 사용하면 MDX Toolkit(현재 Legacy MDX)을 사용하여 앱 관리를 계속하거나 새로운 MAM SDK로 전환하여 앱을 관리할 수 있습니다. Citrix는 MAM SDK로 전환할 것을 권장합니다. MAM SDK는 더 모듈화되어 있으며 조직에서 사용하는 MDX 기능의 하위 집합만 사용할 수 있도록 하기 위함입니다.

MDX 또는 MAM SDK 정책 컨테이너에서 정책 설정에 대한 다음 옵션을 사용할 수 있습니다.

- **MAM SDK**
- **레거시 MDX**

MDX 또는 MAM SDK 정책 컨테이너 정책에서 옵션을 **Legacy MDX**에서 **MAM SDK**로만 변경할 수 있습니다. **MAM SDK**에서 **Legacy MDX**로 전환하는 옵션은 허용되지 않으며 앱을 다시 게시해야 합니다. 기본 값은 **Legacy MDX**입니다. 동일한 장치에서 실행되는 Secure Mail과 Secure Web 모두에 대해 동일한 정책 모드를 설정해야 합니다. 동일한 장치에서 두 가지 다른 모드를 실행할 수 없습니다.

내부 네트워크에 대한 사용자 연결

내부 네트워크로 터널링되는 연결은 전체 VPN 터널 또는 Tunneled – Web SSO라고 하는 클라이언트리스 VPN의 변형을 사용할 수 있습니다. 기본 VPN 모드 정책이 이 동작을 제어합니다. 기본적으로 연결은 SSO가 필요한 연결에 권장되는 Tunneled – Web SSO를 사용합니다. 전체 VPN 터널 설정은 클라이언트 인증서 또는 내부 네트워크의 리소스에 대한 종단 간 SSL을 사용하는 연결에 권장됩니다. 이 설정은 TCP를 통한 모든 프로토콜을 처리하며 Windows 및 Mac 컴퓨터, iOS 및 Android 장치와 함께 사용할 수 있습니다.

VPN 모드 전환 허용 정책은 필요에 따라 전체 VPN 터널과 Tunneled – Web SSO 모드 간의 자동 전환을 허용합니다. 기본적으로 이 정책은 꺼져 있습니다. 이 정책이 켜져 있으면 기본 VPN 모드에서 처리할 수 없는 인증 요청으로 인해 실패한 네트워크 요청이 대체 모드에서 다시 시도됩니다. 예를 들어, 클라이언트 인증서에 대한 서버 챌린지는 전체 VPN 터널 모드에서는 수용할 수 있지만 Tunneled – Web SSO 모드에서는 수용할 수 없습니다. 마찬가지로 HTTP 인증 챌린지는 Tunneled – Web SSO 모드를 사용할 때 SSO로 처리될 가능성이 더 높습니다.

네트워크 액세스 제한

네트워크 액세스 정책은 네트워크 액세스에 제한이 적용되는지 여부를 지정합니다. 기본적으로 Secure Mail 액세스는 무제한이며, 이는 네트워크 액세스에 제한이 없음을 의미합니다. 앱은 장치가 연결된 네트워크에 무제한으로 액세스할 수 있습니다. 기본적으로 Secure Web 액세스는 내부 네트워크로 터널링됩니다. 즉, 모든 네트워크 액세스에 대해 내부 네트워크로의 애플리케이션별 VPN 터널이 사용되며 Citrix ADC 분할 터널 설정이 사용됩니다. 또한 앱이 네트워크 연결이 없는 것처럼 작동하도록 액세스를 차단하도록 지정할 수도 있습니다.

AirPrint, iCloud, Facebook 및 Twitter API와 같은 기능을 허용하려면 네트워크 액세스 정책을 차단하지 마십시오.

네트워크 액세스 정책은 백그라운드 네트워크 서비스 정책과도 상호 작용합니다. 자세한 내용은 [Exchange Server](#) 또는 [IBM Notes Traveler Server 통합](#)을 참조하십시오.

엔드포인트 관리 클라이언트 속성

클라이언트 속성에는 사용자 장치의 Secure Hub에 직접 제공되는 정보가 포함되어 있습니다. 클라이언트 속성은 Endpoint Management 콘솔의 [설정 > 클라이언트 > 클라이언트 속성](#)에 있습니다.

클라이언트 속성은 다음과 같은 설정을 구성하는 데 사용됩니다.

사용자 암호 캐싱

사용자 암호 캐싱을 사용하면 사용자의 Active Directory 암호를 모바일 장치에 로컬로 캐시할 수 있습니다. 사용자 암호 캐싱을 활성화하면 사용자에게 Citrix PIN 또는 암호를 설정하라는 메시지가 표시됩니다.

비활성 타이머

비활성 타이머는 사용자가 장치를 비활성 상태로 두고 Citrix PIN 또는 암호를 묻는 메시지 없이 앱에 액세스할 수 있는 시간을 분 단위로 정의합니다. MDX 앱에 대해 이 설정을 활성화하려면 앱 암호 정책을 **켜기**로 설정해야 합니다. 앱 암호 정책이 **끄기**인 경우 사용자는 전체 인증을 수행하기 위해 Secure Hub로 리디렉션됩니다. 이 설정을 변경하면 사용자가 인증하라는 메시지가 표시될 때 다음번에 값이 적용됩니다.

Citrix PIN 인증

Citrix PIN은 사용자 인증 환경을 단순화합니다. PIN은 클라이언트 인증서를 보호하거나 Active Directory 자격 증명을 장치에 로컬로 저장하는 데 사용됩니다. PIN 설정을 구성하면 사용자 로그인 환경은 다음과 같습니다.

1. 사용자가 Secure Hub를 처음 시작할 때 PIN을 입력하라는 메시지가 표시되며, 이 PIN은 Active Directory 자격 증명을 캐시합니다.

2. 사용자가 다음에 Secure Mail과 같은 모바일 생산성 앱을 시작할 때 PIN을 입력하고 로그인합니다.

클라이언트 속성을 사용하여 PIN 인증을 활성화하고, PIN 유형을 지정하고, PIN 강도, 길이 및 변경 요구 사항을 지정합니다.

지문 또는 Touch ID 인증

iOS 장치용 지문 인증(Touch ID 인증으로도 알려짐)은 Citrix PIN의 대안입니다. 이 기능은 Secure Hub를 제외한 래핑된 앱이 비활성 타이머가 만료될 때와 같이 오프라인 인증이 필요할 때 유용합니다. 다음 인증 시나리오에서 이 기능을 활성화할 수 있습니다.

- Citrix PIN + 클라이언트 인증서 구성
- Citrix PIN + 캐시된 AD 암호 구성
- Citrix PIN + 클라이언트 인증서 구성 및 캐시된 AD 암호 구성
- Citrix PIN이 꺼져 있습니다.

지문 인증에 실패하거나 사용자가 지문 인증 프롬프트를 취소하면 래핑된 앱은 Citrix PIN 또는 AD 암호 인증으로 대체됩니다.

지문 인증 요구 사항

- 지문 인증을 지원하고 하나 이상의 지문이 구성된 iOS 장치(최소 버전 8.1).
- 사용자 엔트로피는 꺼져 있어야 합니다.

지문 인증을 구성하려면

중요:

사용자 엔트로피가 켜져 있으면 Touch ID 인증 활성화 속성은 무시됩니다. 사용자 엔트로피는 암호 키를 사용하여 비밀을 암호화(Encrypt secrets using the Passcode key)를 통해 활성화됩니다.

1. Endpoint Management 콘솔에서 **설정 > 클라이언트 > 클라이언트 속성**으로 이동합니다.
2. **추가**를 클릭합니다.

새 클라이언트 속성 화면 이미지(/en-us/mobile-productivity-apps/media/add-client-property-endpointmanagement.png)

3. 키 **ENABLE_TOUCH_ID_AUTH**를 추가하고, 값을 **True**로 설정한 다음, 정책 이름을 **지문 인증 활성화**로 설정합니다.

지문 인증을 구성한 후에는 사용자가 장치를 다시 등록할 필요가 없습니다.

Encrypt Secrets using Passcode 키 및 일반적인 클라이언트 속성에 대한 자세한 내용은 [클라이언트 속성](#)에 대한 Endpoint Management 문서를 참조하십시오.

구글 애널리틱스

Citrix Secure Mail은 제품 품질 개선을 위해 앱 통계 및 사용 정보 분석 데이터를 수집하는 데 Google Analytics를 사용합니다. Citrix는 다른 개인 사용자 정보를 수집하거나 저장하지 않습니다.

Google Analytics 비활성화

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

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

참고:

Citrix Endpoint Management 콘솔에서 **DISABLE_GA** 값을 구성하지 않으면 Google Analytics 데이터가 활성화됩니다.

모바일 생산성 앱용 MDX 정책 한눈에 보기

이 문서에서는 iOS 및 Android용 Citrix 모바일 생산성 앱에 대한 MDX 앱 정책과 기본값을 설명합니다. Citrix Endpoint Management 콘솔에서 정책 설정을 변경할 수 있습니다. 자세한 내용은 [앱 추가](#)를 참조하십시오.

참고:

Secure Hub는 특정 작업 중에 정책을 새로 고칩니다. 자세한 내용은 [Secure Hub 관리](#)를 참조하십시오.

인증

장치 암호

- iOS: 예

- Android: 아니요
- 기본 설정: 끄기

참고:

이 정책은 Citrix®에서 더 이상 지원하지 않는 iOS 9 장치에만 적용되었습니다.

앱 암호

- iOS: 예
- 안드로이드: 예
- 기본 설정: 켜기

온라인 세션 필수 유예 기간 (분)

- iOS: 예
- Android: 아니요
- 기본 설정: 0

최대 오프라인 기간

- iOS: 예
- Android: 지원됩니다.
- 기본 설정: 168시간 (7일)

대체 Citrix Gateway 설정

참고:

Endpoint Management 콘솔에서 이 정책 이름은 대체 NetScaler® Gateway입니다.

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

장치 보안

탈옥 또는 루팅된 기기 차단

- iOS: 예
- 안드로이드: 예
- 기본 설정: 켜짐

기기 잠금 필요

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 꺼짐

참고:

Android M 기기에서 기기 PIN 또는 암호 및 기기 패턴 화면 잠금 옵션은 동일한 효과를 가집니다. 이러한 옵션 중 하나를 사용하면 기기에 PIN, 암호 또는 패턴 화면 잠금이 설정되어 있지 않은 경우 앱이 잠깁니다.

네트워크 요구 사항

Wi-Fi 필요

- iOS: 예
- 안드로이드: 예
- 기본 설정: 꺼짐

허용된 Wi-Fi 네트워크

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

기타 액세스

앱 업데이트 유예 기간(시간)

- iOS: 예

- 안드로이드: 예
- 기본 설정: 168시간(7일)

참고:

Citrix는 0이 아닌 값을 사용하는 것을 권장합니다. 값이 0이면 사용자가 업데이트를 다운로드하여 설치할 때까지 경고 없이 실행 중인 앱을 즉시 사용할 수 없게 됩니다. 이 설정으로 인해 사용자가 앱을 강제로 종료하고 작업 내용을 잃을 수 있습니다.

필수 업그레이드 비활성화

- iOS: 예
- 안드로이드: 예
- 기본 설정: 켜짐

잠금 시 앱 데이터 지우기

- iOS: 예
- 안드로이드: 예
- 기본 설정: 끄기

활성 폴링 기간(분)

- iOS: 예
- 안드로이드: 예
- 기본 설정: 60분(1시간)

참고:

위험도가 높은 앱의 경우에만 이 값을 기본값보다 낮게 설정하십시오. 그렇지 않으면 성능에 영향을 미칠 수 있습니다.

암호화**암호화 유형**

- iOS: 예
- 안드로이드: 예

- 기본 설정: MDX 암호화

주의:

새로 추가된 앱의 경우, **Platform encryption with compliance enforcement**에서 **MDX encryption**으로 변경하면 앱을 제거하고 다시 설치해야 합니다. 새로 추가된 앱의 기본 설정은 **Platform encryption with compliance enforcement**입니다.

규정 미준수 기기 동작

- iOS: 예
- 안드로이드: 예
- 기본 설정: 경고 후 앱 허용

MDX 암호화 활성화

- iOS: 예
- Android: 아니요
- 기본 설정: 컴

주의:

앱 배포 후 이 정책을 변경하면 사용자는 앱을 다시 설치해야 합니다.

암호화 키

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 오프라인 액세스 허용만 사용 가능한 옵션입니다.

개인 파일 암호화

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: SecurityGroup

개인 파일 암호화 제외

- iOS: 아니요

- 안드로이드: 예
- 기본 설정: 비어 있음

공용 파일에 대한 액세스 제한

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 비어 있음

참고:

공용 파일 암호화 정책을 활성화하면 이 정책이 적용됩니다 (비활성화 옵션에서 SecurityGroup 또는 애플리케이션 옵션으로 변경됨). 이 정책은 기존의 암호화되지 않은 공용 파일에만 적용되며, 파일을 암호화할 시기를 지정합니다.

공개 파일 암호화

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: SecurityGroup

공개 파일 암호화 제외

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 비어 있음

공개 파일 마이그레이션

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 쓰기 (RO/RW)

참고:

기존 공개 파일을 암호화하면 동일한 암호화 키가 없는 다른 앱에서 해당 파일을 사용할 수 없게 됩니다.

암호화 사용

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

참고:

기존 앱에 대해 이 정책을 변경하는 경우, 정책 변경 사항을 적용하려면 사용자가 앱을 제거하고 다시 설치해야 합니다.

데이터베이스 암호화 제외

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

파일 암호화 제외

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

앱 상호 작용

보안 그룹

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 비어 있음

참고:

기존 앱에 대해 이 정책을 변경하는 경우, 정책 변경 사항을 적용하려면 사용자가 앱을 제거하고 다시 설치해야 합니다.

잘라내기 및 복사

- iOS: 예

- 안드로이드: 예
- 기본 설정: 제한됨

붙여넣기

- iOS: 예
- 안드로이드: 예
- 기본 설정: 제한 없음

문서 교환 (다음에서 열기)

- iOS: 예
- 안드로이드: 예
- 기본 설정: 제한됨

필터링에서 제외된 URL 도메인

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 비어 있음

허용된 Secure Web 도메인

- iOS: 아니요
- Android: 지원됨
- 기본 설정: 비어 있음

연결 보안 수준

- iOS: 예
- Android: 지원됨
- 기본 설정: TLS

인바운드 문서 교환 (Open In)

- iOS: 예
- 안드로이드: 예
- 기본 설정: 제한 없음

제한된 Open In 예외 목록

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음 (Android의 경우); Office 365 앱 (iOS의 경우)

참고:

Android에서는 이 정책이 이전에 Open In 제외로 명명되었습니다. iOS에서는 이 정책이 숨겨져 있습니다. 자세한 내용은 [iOS 앱용 MDX 정책](#)을 참조하십시오.

앱 URL 스키마

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음. 등록된 모든 앱 URL 스키마는 차단됩니다.

허용된 URL

- iOS: 예
- Android: 아니요
- 기본 설정: 기본 설정에 대한 자세한 내용은 iOS 앱용 MDX 정책의 앱 상호 작용 섹션을 참조하십시오.

명시적 로그오프 알림

- iOS: 예
- Android: 아니요
- 기본 설정: Secure Mail의 경우 공유 장치에만 해당

앱 상호 작용(아웃바운드 URL)

URL 필터링에서 제외된 도메인

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

허용된 URL

- iOS: 예
- Android: 아니요
- 기본 설정: 또는 기본 설정에 대한 자세한 내용은 [MDX policies for iOS apps](#)의 앱 상호 작용(아웃바운드 URL) 섹션을 참조하십시오.

허용된 보안 웹 도메인

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

앱 제한

카메라 차단

- iOS: 예
- 안드로이드: 예
- 기본 설정: iOS의 경우 끄; Android의 경우 켜

갤러리 차단

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 끄

사진 라이브러리 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

마이크 녹음 차단

- iOS: 예
- Android: 지원됨
- 기본 설정: 켜짐

받아쓰기 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

위치 서비스 차단

- iOS: 예
- Android: 지원됨
- 기본 설정: Android의 경우: Secure Mail의 기본값은 꺼짐입니다. 다른 앱의 기본값은 켜짐입니다.

SMS 작성 차단

- iOS: 예
- Android: 지원됩니다.
- 기본 설정: 켜짐

화면 캡처 차단

- iOS: 아니요
- Android: 지원됩니다.
- 기본 설정: 켜짐

장치 센서 차단

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 켜짐

NFC 차단

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 켜짐

iCloud 차단

- iOS: 예
- Android: 아니요

- 기본 설정: 켜짐

찾아보기 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

파일 백업 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

AirPrint 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

인쇄 차단

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 켜짐

AirDrop 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

파일 첨부 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 꺼짐

이메일 작성 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

Facebook 및 Twitter API 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

화면 내용 가리기

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

타사 키보드 차단

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

참고

iOS 11 이상

앱 로그 차단

- iOS: 예
- 안드로이드: 예
- 기본 설정: 끄

ShareFile 사용

- iOS:
- 안드로이드: 예

- 기본 설정: 켜

파일에서 첨부 사용

- iOS: 예
- Android: 아니요
- 기본 설정: 켜

앱 네트워크 액세스

네트워크 액세스

- iOS: 예
- 안드로이드: 예
- 기본 설정: 새로 업로드된 앱의 경우 Secure Mail을 제외한 모든 앱의 기본값은 **차단됨**입니다. Intune에는 차단 상태가 없으므로 Secure Mail의 기본값은 **제한 없음**입니다.

micro VPN 세션 필요

- iOS: 예
- 안드로이드: 예
- 기본 설정: 이전 설정 사용. 새로 업로드된 앱의 경우 기본값은 아니요입니다.

micro VPN 세션 필요 유예 기간(분)

- iOS: 예
- 안드로이드: 예
- 기본 설정: 0 (유예 기간 없음)

제외 목록

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

localhost 연결 차단

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 끄

인증서 레이블

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

앱 로그

기본 로그 출력

- iOS: 예
- 안드로이드: 예
- 기본 설정: 파일

기본 로그 수준

- iOS: 예
- 안드로이드: 예
- 기본 설정: 4 (정보 메시지)

최대 로그 파일 수

- iOS: 예
- 안드로이드: 예
- 기본 설정: 2

최대 로그 파일 크기

- iOS: 예
- 안드로이드: 예
- 기본 설정: 2MB

앱 로그 리디렉션

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 켜기

로그 암호화

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 끄

앱 지오펜스

중심점 경도

- iOS: 예
- 안드로이드: 예
- 기본 설정: 0

중심점 위도

- iOS: 예
- 안드로이드: 예
- 기본 설정: 0

반경

- iOS: 예
- 안드로이드: 예
- 기본 설정: 0 (비활성화됨)

참고:

반경을 미터 단위로 설정합니다. 0으로 설정하면 지오펜스가 비활성화됩니다.

앱 설정

시큐어 메일 익스체인지 서버

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

참고:

기존 앱에 대해 이 정책을 변경하는 경우, 정책 변경 사항을 적용하려면 사용자가 앱을 제거하고 다시 설치해야 합니다.

Secure Mail 사용자 도메인

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

백그라운드 네트워크 서비스

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

참고:

이 정책을 구성하는 경우 네트워크 액세스 정책을 내부 네트워크로 터널링으로 설정하면 이 정책이 적용됩니다. Exchange Server가 내부 네트워크에 있고 Citrix Gateway를 사용하여 내부 Exchange Server에 대한 연결을 프록시하려는 경우 이 정책을 사용하십시오.

백그라운드 서비스 티켓 만료

- iOS: 예
- 안드로이드: 예
- 기본 설정: 168시간 (7일)

백그라운드 네트워크 서비스 게이트웨이

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

참고:

이 정책을 구성하는 경우 네트워크 액세스 정책을 내부 네트워크로 터널링으로 설정하면 이 정책이 적용됩니다. Exchange Server가 내부 네트워크에 있거나 Citrix Gateway를 사용하여 내부 Exchange Server에 대한 연결을 프록시하려는 경우 이 정책을 사용하십시오. 이 정책은 네트워크 액세스 정책을 구성할 때 적용됩니다.

연락처 내보내기

- iOS: 예
- Android: 지원됨
- 기본 설정: 끄기

내보낼 연락처 필드

- iOS: 예
- Android: 지원됨
- 기본 설정: 모두

모든 SSL 인증서 허용

- iOS: 예
- 안드로이드: 예
- 기본 설정: 끄기

잠금 화면 알림 제어

- iOS: 예
- 안드로이드: 예
- 기본 설정: 허용

보안 연결 사용

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 컴

기본 이메일 알림

- iOS: 예
- Android: 아니요
- 기본 설정: 컴

기본 동기화 간격

- iOS: 예
- 안드로이드: 예
- 기본 설정: 3일

참고:

Exchange ActiveSync 사서함 정책 설정인 최대 이메일 보존 기간 필터가 이 정책보다 우선합니다 . Secure Mail은 최대 이메일 보존 기간 필터보다 작은 동기화 간격 값만 표시합니다.

메일 검색 제한

- iOS: 예
- 안드로이드: 예
- 기본 설정: 무제한

최대 동기화 간격

- iOS: 예
- 안드로이드: 예
- 기본 설정: 모두

주 번호 사용

- iOS: 예
- 안드로이드: 예
- 기본 설정: 해제

Wi-Fi를 통한 첨부 파일 다운로드 사용

- iOS: 예
- 안드로이드: 예

- 기본 설정: 끄

오프라인 문서 허용

- iOS: 예
- 안드로이드: 예
- 기본 설정: 무제한

정보 권한 관리

- iOS: 예
- 안드로이드: 예
- 기본 설정: 끄

이메일 분류

- iOS: 예
- Android: 아니요
- 기본 설정: 끄

이메일 분류 표시

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

이메일 분류 네임스페이스

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

이메일 분류 버전

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

기본 이메일 분류

- iOS: 예
- Android: 아니요
- 기본 설정: 비공식

초안 이메일 자동 저장 활성화

- iOS: 예
- 안드로이드: 예
- 기본 설정: 켜짐

iOS 데이터 보호 활성화

- iOS: 예
- Android: 아니요
- 기본 설정: 꺼짐

푸시 알림 EWS 호스트 이름

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

푸시 알림

- iOS: 예
- Android: 아니요
- 기본 설정: 꺼짐

푸시 알림 지역

- iOS: 예
- Android: 아니요
- 기본 설정: 미주

Secure Mail 첫 시작 시 S/MIME 사용

- iOS: 예
- Android: 아니요

- 기본 설정: 해제

초기 인증 메커니즘

- iOS: 예
- 안드로이드: 예
- 기본 설정: MDX에서 제공하는 메일 서버 주소 사용

초기 인증 자격 증명

- iOS: 예
- 안드로이드: 예
- 기본 설정: 등록 사용자 이름

주 번호 사용

- iOS: 예
- 안드로이드: 예
- 기본 설정: 끄기

캘린더 웹 및 오디오 옵션

- iOS: 예
- 안드로이드: 예
- 기본 설정: GoToMeeting 및 사용자 입력

S/MIME 공개 인증서 원본

- iOS: 예
- Android: 지원됨
- 기본 설정: Exchange

LDAP 서버 주소

- iOS: 예
- Android: 지원됨
- 기본 설정: 비어 있음

LDAP 기본 DN

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

익명으로 LDAP 액세스

- iOS: 예
- 안드로이드: 예
- 기본 설정: 끄

허용된 이메일 도메인

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

참고

비어 있는 경우 도메인을 제한하지 않습니다.

인증 실패 시 사용자 이름 마이그레이션 시도

- iOS: 예
- Android: 지원
- 기본 설정: 끄

피싱 메일 주소 보고

- iOS: 예
- Android: 지원
- 기본 설정: 비어 있음

피싱 보고 메커니즘

- iOS: 아니요
- 안드로이드: 예

- 기본 설정: 첨부 파일(.eml)을 통해 보고

비즈니스용 Skype 회의 도메인

- iOS: 예
- Android: 지원
- 기본 설정: 비어 있음

캘린더 내보내기

- iOS: 예
- Android: 지원
- 기본 설정: 회의 시간

Slack 사용

- iOS: 예
- Android: 지원
- 기본 설정: 끄

Slack 작업 공간 이름

- iOS: 예
- Android: 지원
- 기본 설정: 비어 있음

발신자 식별

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

참고:

켜짐으로 설정하면 Secure Mail이 발신자 식별을 위해 저장된 연락처의 이름과 전화번호를 iOS에 제공합니다.

분석

Google Analytics 사용 설정

- iOS: 예
- Android: 아니요
- 기본 설정: 켜짐

Google Analytics 세부 정보 수준

- iOS: 예
- 안드로이드: 예
- 기본 설정: 완료

보고

Citrix 보고

- iOS: 예
- Android: 아니요
- 기본 설정: 끄

참고:

Citrix는 기능 플래그를 사용하여 이 기능을 제어할 수도 있습니다. 이 기능이 작동하려면 기능 플래그와 이 정책이 모두 활성화되어야 합니다.

토큰 업로드

- iOS: 예
- Android: 아니요
- 기본 설정: 비어 있음

Wi-Fi로만 보고서 전송

- iOS: 예
- Android: 아니요
- 기본 설정: 켜

보고 파일 캐시 최대값

- iOS: 예
- Android: 아니요
- 기본 설정: 2MB

Office 365용 OAuth 지원

Office 365에 최신 인증 사용

- iOS: 아니요
- 안드로이드: 예
- 기본 설정: 해제

Office 365 인증 메커니즘

- iOS: 예
- Android: 아니요
- 기본 설정: OAuth 사용 안 함

신뢰할 수 있는 Exchange Online 호스트 이름

- iOS: 예
- 안드로이드: 예
- 기본 설정: outlook.office365.com

신뢰할 수 있는 AD FS 호스트 이름

- iOS: 예
- Android: 지원
- 기본 설정: login.microsoftonline.com

최신 인증을 위한 사용자 지정 사용자 에이전트

- iOS: 아니요
- Android: 지원
- 기본 설정: 비어 있음

참고:

이 정책을 구성하지 않으면 최신 인증 중에 기본 Secure Mail 사용자 에이전트가 사용됩니다.

메일 리디렉션

메일 리디렉션

- iOS: 예
- Android: 아니요
- 기본 설정: Secure Mail

Slack 통합

Slack 활성화

- iOS: 예
- 안드로이드: 예
- 기본 설정: 끄

Slack 작업 공간 이름

- iOS: 예
- 안드로이드: 예
- 기본 설정: 비어 있음

Android용 모바일 생산성 앱을 위한 MDX 정책

이 문서에서는 Android 앱용 MDX 정책에 대해 설명합니다. Citrix Endpoint Management 콘솔에서 정책 설정을 변경합니다. 자세한 내용은 [앱 추가](#)를 참조하십시오.

다음 목록에는 Secure Web에 특정한 MDX 정책이 포함되어 있지 않습니다. Secure Web에 표시되는 정책에 대한 자세한 내용은 [Secure Web 정책](#)을 참조하십시오.

인증

앱 암호

켜짐으로 설정하면 앱이 시작되거나 비활성 기간 후 다시 시작될 때 앱 잠금을 해제하려면 PIN 또는 암호가 필요합니다. 기본값은 **켜짐**입니다.

모든 앱에 대한 비활성 타이머를 구성하려면 **설정** 탭의 **클라이언트 속성**에서 INACTIVITY_TIMER 값을 분 단위로 설정합니다. 기본 비활성 타이머 값은 60분입니다. 비활성 타이머를 비활성화하여 앱 시작 시에만 PIN 또는 암호 프롬프트가 나타나도록 하려면 값을 0으로 설정합니다.

참고:

암호화 키 정책에 대해 오프라인 보안을 선택하면 이 정책이 자동으로 활성화됩니다.

최대 오프라인 기간(시간)

자격 재확인 및 정책 새로 고침을 위해 네트워크 로그인 없이 앱이 오프라인으로 실행될 수 있는 최대 기간을 정의합니다. 기본값은 **168시간**(7일)입니다. 최소 기간은 1시간입니다.

사용자에게 기간 만료 30분, 15분, 5분 전에 로그인하도록 알림이 표시됩니다. 만료 후에는 사용자가 성공적으로 네트워크 로그인을 완료할 때까지 앱이 잠긴 상태로 유지됩니다.

대체 시트릭스 게이트웨이

참고:

Endpoint Management 콘솔의 이 정책 이름은 대체 **NetScaler® Gateway**입니다.

이 앱의 인증 및 마이크로 VPN 세션에 사용되는 특정 대체 Citrix Gateway(이전 명칭: NetScaler Gateway) 주소입니다. **대체 NetScaler Gateway**는 온라인 세션 필수 정책과 함께 사용될 때 앱이 특정 게이트웨이에 다시 인증하도록 강제하는 선택적 정책입니다. 이러한 게이트웨이는 일반적으로 다른(더 높은 보증) 인증 요구 사항 및 트래픽 관리 정책을 가집니다. 비워두면 항상 서버의 기본값이 사용됩니다. 기본값은 비어 있습니다.

장치 보안

탈옥 또는 루팅된 장치 차단

켜짐으로 설정하면 장치가 탈옥 또는 루팅되었을 때 앱이 잠깁니다. **꺼짐**으로 설정하면 장치가 탈옥 또는 루팅되었더라도 앱을 실행할 수 있습니다. 기본값은 **켜짐**입니다.

장치 암호화 요구

켜짐으로 설정하면 장치에 암호화가 구성되지 않은 경우 앱이 잠깁니다. **꺼짐**으로 설정하면 장치에 암호화가 구성되지 않았더라도 앱을 실행할 수 있습니다. 기본값은 **꺼짐**입니다.

참고:

이 정책은 Android 3.0(Honeycomb)에서만 지원됩니다. 정책을 **꺼짐**으로 설정하면 이전 버전에서는 앱이 실행되지 않습니다.

장치 잠금 요구

장치 PIN 또는 암호를 선택하면 장치에 PIN 또는 암호가 없는 경우 앱이 잠깁니다. **장치 패턴 화면 잠금**을 선택하면 장치에 패턴 화면 잠금이 설정되지 않은 경우 앱이 잠깁니다. **꺼짐**으로 설정하면 장치에 PIN, 암호 또는 패턴 화면 잠금이 설정되지 않았더라도 앱을 실행할 수 있습니다. 기본값은 **꺼짐**입니다.

장치 PIN 또는 암호는 Android 4.1(Jelly Bean) 이상 버전을 필요로 합니다. 정책을 **장치 PIN 또는 암호**로 설정하면 이전 버전에서는 앱이 실행되지 않습니다.

Android M 장치에서는 **장치 PIN 또는 암호** 및 **장치 패턴 화면 잠금** 옵션이 동일한 효과를 가집니다. 이 옵션 중 어느 것을 사용하든 장치에 PIN, 암호 또는 패턴 화면 잠금이 설정되지 않은 경우 앱이 잠깁니다.

네트워크 요구 사항**Wi-Fi 요구**

꺼짐으로 설정하면 장치가 Wi-Fi 네트워크에 연결되지 않았을 때 앱이 잠깁니다. **꺼짐**으로 설정하면 장치에 4G/3G, LAN 또는 Wi-Fi 연결과 같은 활성 연결이 있는 경우 앱을 실행할 수 있습니다. 기본값은 **꺼짐**입니다.

허용된 Wi-Fi 네트워크

허용된 Wi-Fi 네트워크의 심표로 구분된 목록입니다. 네트워크 이름에 영숫자가 아닌 문자(심표 포함)가 포함된 경우 이름은 큰따옴표로 묶어야 합니다. 앱은 나열된 네트워크 중 하나에 연결된 경우에만 실행됩니다. 비워두면 모든 네트워크가 허용됩니다. 이 값은 셀룰러 네트워크 연결에 영향을 미치지 않습니다. 기본값은 비어 있습니다.

기타 액세스**앱 업데이트 유예 기간(시간)**

시스템이 앱 업데이트를 사용할 수 있음을 감지한 후 앱을 사용할 수 있는 유예 기간을 정의합니다. 기본값은 **168시간(7일)**입니다.

참고:

0을 사용하는 것은 권장되지 않습니다. 업데이트가 다운로드되어 설치될 때까지(사용자에게 경고 없이) 실행 중인 앱을 즉시 사용할 수 없게 만들기 때문입니다. 이 값은 앱을 실행 중인 사용자가 필수 업데이트를 준수하기 위해 앱을 강제로 종료(작업 손실 가능성 있음)해야 하는 상황으로 이어질 수 있습니다.

필수 업그레이드 비활성화

사용자가 앱 스토어에서 최신 버전의 앱으로 업그레이드해야 하는 요구 사항을 비활성화합니다. 기본값은 **ON**입니다.

잠금 시 앱 데이터 지우기

앱이 잠길 때 데이터를 지우고 앱을 재설정합니다. **Off**로 설정하면 앱이 잠겨도 앱 데이터가 지워지지 않습니다. 기본값은 **Off**입니다.

앱은 다음 이유 중 하나로 잠길 수 있습니다.

- 사용자에게 대한 앱 권한 상실
- 앱 구독 제거됨
- 계정 제거됨
- Secure Hub 제거됨
- 너무 많은 앱 인증 실패
- 탈옥된 장치 감지됨(정책 설정에 따름)
- 다른 관리 작업으로 인해 장치가 잠금 상태로 전환됨

활성 폴링 기간(분)

앱이 시작되면 MDX 프레임워크는 Citrix Endpoint Management를 폴링하여 현재 앱 및 장치 상태를 확인합니다. Endpoint Management를 실행하는 서버에 연결할 수 있다고 가정하면 프레임워크는 장치의 잠금/지우기 상태와 앱의 활성화/비활성화 상태에 대한 정보를 반환합니다. 서버에 연결할 수 있는지 여부에 관계없이 활성 폴링 기간 간격에 따라 후속 폴링이 예약됩니다. 기간이 만료되면 새 폴링이 다시 시도됩니다. 기본값은 **60분(1시간)**입니다.

중요:

위험도가 높은 앱에 대해서만 이 값을 낮게 설정하십시오. 그렇지 않으면 성능에 영향을 미칠 수 있습니다.

암호화

암호화 유형

MDX 또는 장치 플랫폼이 데이터 암호화를 처리할지 여부를 선택할 수 있습니다. **MDX 암호화**를 선택하면 MDX가 데이터를 암호화합니다. **규정 준수 적용을 통한 플랫폼 암호화**를 선택하면 장치 플랫폼이 데이터를 암호화합니다. 기본값은 **MDX 암호화**입니다.

비규격 장치 동작

장치가 최소 암호화 규정 준수 요구 사항을 따르지 않을 때 수행할 작업을 선택할 수 있습니다. 앱이 정상적으로 실행되도록 **앱 허용**을 선택합니다. 경고가 나타난 후 앱이 실행되도록 **경고 후 앱 허용**을 선택합니다. 앱 실행을 차단하려면 **차단**을 선택합니다. 기본값은 **경고 후 앱 허용**입니다.

암호화 키

암호화 키 파생에 사용되는 비밀을 장치에 유지할 수 있도록 합니다. 오프라인 액세스 허용만 사용 가능한 옵션입니다.

Citrix는 암호화된 콘텐츠에 대한 액세스를 보호하기 위해 네트워크 로그인 또는 오프라인 암호 챌린지를 활성화하도록 인증 정책을 설정할 것을 권장합니다.

개인 파일 암호화

다음 위치에 있는 개인 데이터 파일의 암호화를 제어합니다: /data/data/<appname> 및 /mnt/sdcard/Android/data/<appname>.

Disabled 옵션은 개인 파일이 암호화되지 않음을 의미합니다. **SecurityGroup** 옵션은 동일한 보안 그룹에 있는 모든 MDX 앱이 공유하는 키를 사용하여 개인 파일을 암호화합니다. **Application** 옵션은 이 앱에 고유한 키를 사용하여 개인 파일을 암호화합니다. 기본값은 **SecurityGroup**입니다.

개인 파일 암호화 제외

쉼표로 구분된 파일 경로 목록을 포함합니다. 각 경로는 암호화된 하나 이상의 파일을 나타내는 정규식입니다. 파일 경로는 내부 및 외부 샌드박스에 상대적입니다. 기본값은 비어 있습니다.

제외는 다음 폴더에만 적용됩니다:

- 내부 저장소:

```
/data/data/<your_package_name>
```

- SD 카드:

```
/storage/emulated/<SD Card Slot>/Android/data/<your_package_name>
```

```
/storage/emulated/legacy/Android/data/<your_package_name>
```

예시

제외할 파일	개인 파일 암호화 제외 값
/data/data/com.citrix.mail/files/a.txt	^files/a.txt
/storage/emulated/0/Android/data/com.citrix.mail/files에 있는 모든 텍스트 파일	^files/(.)+.txt\$
/data/data/com.citrix.mail/files에 있는 모든 파일	^파일/

공용 파일에 대한 액세스 제한

쉼표로 구분된 목록을 포함합니다. 각 항목은 (NA), (RO) 또는 (RW)가 뒤따르는 정규식 경로입니다. 경로와 일치하는 파일은 **액세스 없음**, **읽기 전용** 또는 **읽기/쓰기** 액세스로 제한됩니다. 목록은 순서대로 처리되며, 첫 번째 일치하는 경로가 액세스 제한을 설정하는 데 사용됩니다. 기본값은 비어 있습니다.

이 정책은 **공용 파일 암호화가 활성화된** 경우에만 적용됩니다(**비활성화** 옵션에서 **SecurityGroup** 또는 **Application** 옵션으로 변경됨). 이 정책은 기존의 암호화되지 않은 공용 파일에만 적용되며, 이러한 파일이 암호화되는 시기를 지정합니다.

제외할 파일	개인 파일 암호화의 값
외부 저장소의 다운로드 폴더 읽기 전용	EXT:^Download/(RO)
가상 저장소의 Music 폴더에 있는 모든 MP3 파일 액세스 없음	VS:^Music/(.)+.mp3\$(NA)

공용 파일 암호화

공용 파일의 암호화를 제어합니다. **사용 안 함**으로 설정하면 공용 파일이 암호화되지 않습니다. **보안 그룹**으로 설정하면 동일한 보안 그룹에 있는 모든 MDX 앱이 공유하는 키를 사용하여 공용 파일을 암호화합니다. **애플리케이션**으로 설정하면 이 앱에 고유한 키를 사용하여 공용 파일을 암호화합니다.

기본값은 **보안 그룹**입니다.

공용 파일 암호화 제외

쉼표로 구분된 파일 경로 목록을 포함합니다. 각 경로는 암호화되지 않는 하나 이상의 파일을 나타내는 정규식입니다. 파일 경로는 기본 외부 저장소 및 장치별 외부 저장소에 상대적입니다.

공용 파일 암호화 제외는 외부 폴더 위치만 포함합니다.

예시

제외할 파일	공용 파일 암호화 제외의 값
SD 카드에 있는 다운로드 폴더	다운로드
음악 폴더의 모든 MP3 파일	\\Music/(.)+.mp3\$

공용 파일 마이그레이션

이 정책은 공용 파일 암호화 정책을 활성화할 때만 적용됩니다(**사용 안 함**에서 **보안 그룹** 또는 **애플리케이션**으로 변경). 이 정책은 기존의 암호화되지 않은 공용 파일에만 적용되며, 이러한 파일이 암호화되는 시기를 지정합니다. 기본값은 ****쓰기(RO/RW)****입니다.

사용 안 함 옵션은 기존 파일이 암호화되지 않음을 의미합니다. **쓰기(RO/RW)** 옵션은 기존 파일이 쓰기 전용 또는 읽기-쓰기 액세스를 위해 열릴 때만 암호화합니다. **모두** 옵션은 기존 파일이 어떤 모드로든 열릴 때 암호화합니다. 옵션:

- **사용 안 함.** 기존 파일을 암호화하지 않습니다.
- **쓰기(RO/RW).** 기존 파일이 쓰기 전용 또는 읽기-쓰기 액세스를 위해 열릴 때만 암호화합니다.
- **모두.** 기존 파일이 어떤 모드로든 열릴 때 암호화합니다.

참고:

-덮어쓴 새 파일 또는 기존의 암호화되지 않은 파일은 모든 경우에 대체 파일을 암호화합니다. -기존 공용 파일을 암호화하면 동일한 암호화 키가 없는 다른 앱에서 해당 파일을 사용할 수 없게 됩니다.

앱 상호 작용

보안 그룹

Citrix Endpoint Management™에서 관리하는 모든 모바일 앱이 서로 정보를 교환하도록 하려면 이 필드를 비워 두십시오. 특정 앱 세트(예: 재무 또는 인사)에 대한 보안 설정을 관리하려면 보안 그룹 이름을 정의하십시오.

주의:

기존 앱에 대한 이 정책을 변경하는 경우, 정책 변경 사항을 적용하려면 사용자가 앱을 삭제하고 다시 설치해야 합니다.

잘라내기 및 복사

이 앱에 대한 클립보드 잘라내기 및 복사 작업을 차단, 허용 또는 제한합니다. **제한됨**으로 설정하면 복사된 클립보드 데이터는 MDX 앱에서만 사용할 수 있는 개인 클립보드에 저장됩니다. 기본값은 **제한됨**입니다.

붙여넣기

이 앱에 대한 클립보드 붙여넣기 작업을 차단, 허용 또는 제한합니다. **제한됨**으로 설정하면 붙여넣기된 클립보드 데이터는 MDX 앱에서만 사용할 수 있는 개인 클립보드에서 가져옵니다. 기본값은 **제한 없음**입니다.

문서 교환(열기)

앱의 문서 교환 작업을 차단, 허용 또는 제한합니다. **제한됨**으로 설정하면 문서는 다른 MDX 앱 및 제한된 열기 예외 목록 정책에 지정된 앱 예외와만 교환할 수 있습니다. **제한 없음**으로 설정하면 사용자가 래핑되지 않은 앱에서 문서를 열 수 있도록 개인 파일 암호화 및 공용 파일 암호화 정책을 **비활성화됨**으로 설정합니다. 기본값은 **제한됨**입니다.

필터링에서 제외된 URL 도메인

이 정책은 특정 아웃바운드 URL을 MDX 필터링에서 제외하는 데 사용됩니다. 다음 심표로 구분된 FQDN(정규화된 도메인 이름) 또는 DNS 접미사 목록은 모든 MDX 필터링에서 제외됩니다. 이 정책에 항목이 포함되어 있으면 목록의 항목 중 하나 이상과 일치하는 호스트 필드를 가진 URL(DNS 접미사 일치를 통해)은 기본 브라우저로 변경되지 않고 전송됩니다. 기본값은 비어 있습니다.

허용된 Secure Web 도메인

이 정책은 URL 필터링 정책에 의해 제외되지 않은 도메인에만 적용됩니다. 문서 교환이 제한될 때 Secure Web 앱으로 리디렉션되는 FQDN(정규화된 도메인 이름) 또는 DNS 접미사의 심표로 구분된 목록을 추가합니다.

이 정책에 항목이 포함되어 있으면 문서 교환이 제한될 때 목록의 항목 중 하나 이상과 일치하는 호스트 필드를 가진 URL(DNS 접미사 일치를 통해)만 Secure Web 앱으로 리디렉션됩니다.

다른 모든 URL은 기본 Android 웹 브라우저로 전송됩니다(문서 교환 제한 정책을 우회). 기본값은 비어 있습니다.

제한된 열기 예외 목록

문서 교환(열기) 정책이 **제한됨**으로 설정된 경우, 이 Android 인텐트 목록은 관리되지 않는 앱으로 전달될 수 있습니다. 목록에 필터를 추가하려면 Android 인텐트에 대한 지식이 필요합니다. 필터는 작업, 패키지, 스키마 또는 이들의 조합을 지정할 수 있습니다.

예시

```
{action=android.intent.action.MAIN}

{package=com.sharefile.mobile}

{action=android.intent.action.DIAL scheme=tel}

{action=android.intent.action.VIEW scheme=msteams
package=com.microsoft.teams}
```

주의

이 정책의 보안 영향을 반드시 고려하십시오. 예외 목록은 관리되지 않는 앱과 MDX 환경 간에 콘텐츠가 이동하도록 허용합니다.

인바운드 문서 교환(열기)

이 앱의 인바운드 문서 교환 작업을 차단, 제한 또는 허용합니다. **제한됨**으로 설정하면 문서는 다른 MDX 앱과만 교환할 수 있습니다. 기본값은 **제한 없음**입니다.

차단됨 또는 **제한됨**인 경우, 인바운드 문서 교환 허용 목록 정책을 사용하여 이 앱으로 문서를 보낼 수 있는 앱을 지정할 수 있습니다. 다른 정책 상호 작용에 대한 정보는 갤러리 차단 정책을 참조하십시오.

옵션: **무제한**, **차단됨** 또는 **제한됨**

인바운드 문서 교환 허용 목록

인바운드 문서 교환 정책이 제한되거나 차단된 경우, MDX가 아닌 앱을 포함한 심표로 구분된 이 앱 ID 목록은 앱으로 문서를 보낼 수 있습니다. 이 정책은 숨겨져 있으며 편집할 수 없습니다.

연결 보안 수준

연결에 사용되는 TLS/SSL의 최소 버전을 결정합니다. **TLS**인 경우, 연결은 모든 TLS 프로토콜을 지원합니다. **SSLv3** 및 **TLS**인 경우, 연결은 SSL 3.0 및 TLS를 지원합니다. 기본값은 **TLS**입니다.

앱 제한

중요:

앱이 휴대폰 기능에 액세스하거나 사용하는 것을 차단하는 정책의 보안 영향을 반드시 고려하십시오. 해당 정책이 **해제**된 경우, 관리되지 않는 앱과 보안 환경 간에 콘텐츠가 이동할 수 있습니다.

카메라 차단

설정된 경우, 앱이 카메라 하드웨어를 직접 사용하는 것을 방지합니다. 기본값은 **설정**입니다.

갤러리 차단

설정된 경우, 앱이 장치의 갤러리에 액세스하는 것을 방지합니다. 기본값은 **해제**입니다. 이 정책은 인바운드 문서 교환(Open In) 정책과 함께 작동합니다.

- 인바운드 문서 교환(Open In)이 **제한됨**으로 설정된 경우, 관리되는 앱에서 작업하는 사용자는 갤러리 차단 설정과 관계없이 갤러리에서 이미지를 첨부할 수 없습니다.
- 인바운드 문서 교환(Open In)이 **무제한**으로 설정된 경우, 관리되는 앱에서 작업하는 사용자는 다음을 경험합니다.
 - 갤러리 차단(Block Gallery)이 ****해제(Off)****로 설정된 경우 사용자는 이미지를 첨부할 수 있습니다.
 - 갤러리 차단(Block Gallery)이 ****설정(On)****된 경우 사용자는 이미지를 첨부할 수 없습니다.

마이크 녹음 차단

****설정(On)****하면 앱이 마이크 하드웨어를 직접 사용하는 것을 방지합니다. 기본값은 ****설정(On)****입니다.

위치 서비스 차단

****설정(On)****하면 앱이 위치 서비스 구성 요소(GPS 또는 네트워크)를 사용하는 것을 방지합니다. Secure Mail의 기본값은 ****해제(Off)****입니다.

SMS 작성 차단

****설정(On)****하면 앱이 앱에서 SMS/문자 메시지를 보내는 데 사용되는 SMS 작성 기능을 사용하는 것을 방지합니다. 기본값은 ****설정(On)****입니다.

화면 캡처 차단

****설정(On)****하면 앱이 실행되는 동안 사용자가 화면 캡처를 찍는 것을 방지합니다. 또한 사용자가 앱을 전환할 때 앱 화면을 가립니다. 기본값은 ****설정(On)****입니다.

Android 근거리 무선 통신(NFC) 기능을 사용할 때 일부 앱은 콘텐츠를 전송하기 전에 자체 스크린샷을 찍습니다. 래핑된 앱에서 이 기능을 활성화하려면 **화면 캡처 차단(Block screen capture)** 정책을 ****해제(Off)****로 변경하십시오.

장치 센서 차단

****설정(On)****하면 앱이 장치 센서(가속도계, 모션 센서, 자이로스코프 등)를 사용하는 것을 방지합니다. 기본값은 ****설정(On)****입니다.

NFC 차단

****설정(On)****하면 앱이 근거리 무선 통신(NFC)을 사용하는 것을 방지합니다. 기본값은 ****설정(On)****입니다.

앱 로그 차단

켜짐으로 설정하면 앱이 모바일 생산성 앱 진단 로깅 기능을 사용하지 못하도록 합니다. **꺼짐**으로 설정하면 앱 로그가 기록되며 Secure Hub 이메일 지원 기능을 사용하여 수집될 수 있습니다. 기본값은 **꺼짐**입니다.

인쇄 차단

켜짐으로 설정하면 앱이 데이터를 인쇄하지 못하도록 합니다. 앱에 공유 명령이 있는 경우 인쇄를 완전히 차단하려면 문서 교환(다음으로 열기)을 **제한됨** 또는 **차단됨**으로 설정해야 합니다. 기본값은 **켜짐**입니다.

ShareFile 사용

사용자가 ShareFile을 사용하여 파일을 전송할 수 있도록 합니다. 기본값은 **켜짐**입니다.

앱 네트워크 액세스

네트워크 액세스

참고:

터널링됨 - 웹 SSO는 설정에서 **보안 브라우징**의 이름입니다. 동작은 동일합니다.

설정 옵션은 다음과 같습니다.

- **이전 설정 사용:** 이전 정책에서 설정한 값으로 기본 설정됩니다. 이 옵션을 변경하는 경우 이 옵션으로 되돌리지 않아야 합니다. 또한 새 정책에 대한 변경 사항은 사용자가 앱을 버전 18.12.0 이상으로 업그레이드할 때까지 적용되지 않습니다.
- **차단됨:** 앱에서 사용하는 네트워킹 API가 실패합니다. 이전 지침에 따라 이러한 실패를 정상적으로 처리해야 합니다.
- **제한 없음:** 모든 네트워크 호출이 직접 이루어지며 터널링되지 않습니다.
- **터널링됨 - 전체 VPN:** 관리되는 앱의 모든 트래픽이 Citrix Gateway를 통해 터널링됩니다.
- **터널링됨 - 웹 SSO:** HTTP/HTTPS URL이 다시 작성됩니다. 이 옵션은 HTTP 및 HTTPS 트래픽의 터널링만 허용합니다. **터널링됨 - 웹 SSO**의 중요한 장점은 HTTP 및 HTTPS 트래픽에 대한 단일 Sign-On(SSO)과 PKINIT 인증입니다. Android에서 이 옵션은 설정 오버헤드가 낮으므로 웹 검색 유형 작업에 선호되는 옵션입니다.

터널링 모드 중 하나를 선택하면 초기 모드에서 앱별 VPN 터널이 엔터프라이즈 네트워크로 다시 생성됩니다. 여기서는 Citrix Gateway 분할 터널 설정이 사용됩니다. Citrix는 엔터프라이즈 네트워크의 리소스에 대한 클라이언트 인증서 또는 종단 간 SSL을 사용하는 연결에 **터널링 전체 VPN**을 권장합니다. Citrix는 단일 Sign-On(SSO)이 필요한 연결에 **터널링됨 - 웹 SSO**를 권장합니다.

Micro VPN 세션 필요

예인 경우 사용자는 엔터프라이즈 네트워크에 연결되어 있어야 하며 활성 세션이 있어야 합니다. **아니요**인 경우 활성 세션이 필요하지 않습니다. 기본값은 **이전 설정 사용**입니다. 새로 업로드된 앱의 경우 기본값은 **아니요**입니다. 이 정책으로 업그레이드하기 전에 선택한 설정은 **이전 설정 사용** 이외의 옵션을 선택할 때까지 계속 적용됩니다.

제외 목록

VPN 연결을 통하지 않고 직접 액세스할 FQDN 또는 DNS 접미사의 심표로 구분된 목록입니다. 이 정책은 Citrix Gateway가 분할 터널 역방향 모드로 구성된 경우 **터널링됨 - 웹 SSO** 모드에만 적용됩니다.

로컬 호스트 연결 차단

켜짐인 경우 앱은 로컬 호스트 연결을 할 수 없습니다. 로컬 호스트는 장치에서 로컬로 발생하는 통신을 위한 주소(예: 127.0.0.1)입니다. 로컬 호스트는 로컬 네트워크 인터페이스 하드웨어를 우회하고 호스트에서 실행되는 네트워크 서비스에 액세스합니다. **꺼짐**인 경우 이 정책은 네트워크 액세스 정책을 재정의합니다. 즉, 장치에서 프록시 서버가 로컬로 실행 중인 경우 앱이 보안 컨테이너 외부로 연결할 수 있습니다. 기본값은 **꺼짐**입니다.

인증서 레이블

StoreFront™ 인증서 통합 서비스와 함께 사용될 때 이 레이블은 이 앱에 필요한 특정 인증서를 식별합니다. 레이블이 제공되지 않으면 공개 키 인프라(PKI)와 함께 사용할 수 있는 인증서가 제공되지 않습니다. 기본값은 비어 있습니다(인증서 사용 안 함).

앱 로그

기본 로그 출력

Citrix Endpoint Management 앱 진단 로깅 기능에서 기본적으로 사용되는 출력 매체를 결정합니다. 가능한 값은 파일, 콘솔 또는 둘 다입니다. 기본값은 파일입니다.

기본 로그 수준

모바일 생산성 앱 진단 로깅 기능의 기본 상세도를 제어합니다. 숫자가 높을수록 더 자세한 로깅이 포함됩니다.

- 0 - 아무것도 기록되지 않음

- 1 - 치명적인 오류
- 2 - 오류
- 3 - 경고
- 4 - 정보 메시지
- 5 - 상세 정보 메시지
- 6~15 - 디버그 레벨 1~10

기본값은 레벨 4 (정보 메시지)입니다.

최대 로그 파일 수

모바일 생산성 앱 진단 로깅 기능이 롤오버되기 전에 보관하는 로그 파일 수를 제한합니다. 최소값은 2입니다. 최대값은 8입니다. 기본값은 2입니다.

최대 로그 파일 크기

모바일 생산성 앱 진단 로깅 기능이 롤오버되기 전에 보관하는 로그 파일의 MB 단위 크기를 제한합니다. 최소값은 1MB입니다. 최대값은 5MB입니다. 기본값은 2MB입니다.

앱 로그 리디렉션

켜짐으로 설정하면 앱의 시스템 또는 콘솔 로그를 가로채서 모바일 생산성 앱 진단 기능으로 리디렉션합니다. 이 설정이 **꺼짐**으로 설정되면 앱의 시스템 또는 콘솔 로그 사용이 가로채지지 않습니다. 기본값은 **켜짐**입니다.

로그 암호화

켜짐으로 설정된 경우 Citrix Endpoint Management는 진단 로그를 기록할 때 암호화합니다. **꺼짐**으로 설정된 경우 진단 로그는 앱 샌드박스에 암호화되지 않은 상태로 유지됩니다.

주의:

구성된 로그 수준에 따라 로그 암호화는 앱 성능 및 배터리 수명에 상당한 영향을 미칠 수 있습니다.

기본값은 **꺼짐**입니다.

앱 지오펜스

중심점 경도

앱이 작동하도록 제한되는 지점/반경 지오펜스의 중심점 경도(X 좌표)입니다. 구성된 지오펜스 외부에서 작동하면 앱은 잠긴 상태로 유지됩니다. 값은 부호 있는 도 형식(DDD.dddd)으로 표현해야 합니다(예: "-31.9635"). 서경은 마이너스 부호로 시작해야 합니다. 기본값은 **0**입니다.

중심점 위도

앱이 작동하도록 제한되는 지점/반경 지오펜스의 중심점 위도(Y 좌표)입니다. 구성된 지오펜스 외부에서 작동하면 앱은 잠긴 상태로 유지됩니다.

값은 부호 있는 도 형식(DDD.dddd)으로 표현해야 합니다(예: "43.06581"). 남위는 마이너스 부호로 시작해야 합니다. 기본값은 **0**입니다.

반경

앱이 작동하도록 제한되는 지오펜스의 반경입니다. 구성된 지오펜스 외부에서 작동하면 앱은 잠긴 상태로 유지됩니다. 값은 미터 단위로 표현해야 합니다. 0으로 설정하면 지오펜스가 비활성화됩니다. 기본값은 0(비활성화됨)입니다.

분석

Google Analytics 상세 정보

Citrix는 제품 품질 향상을 위해 분석 데이터를 수집합니다. 익명을 선택하면 회사 식별 정보를 포함하지 않도록 선택됩니다.

앱 설정

보안 메일 Exchange 서버

Exchange Server의 정규화된 도메인 이름(FQDN) 또는 (iOS에만 해당) IBM Notes Traveler 서버의 정규화된 도메인 이름(FQDN)입니다. 기본값은 비어 있습니다. 이 필드에 도메인 이름을 제공하면 사용자는 이를 편집할 수 없습니다. 필드를 비워두면 사용자가 자체 서버 정보를 제공합니다.

주의:

기존 앱에 대해 이 정책을 변경하는 경우, 사용자는 정책 변경 사항을 적용하려면 앱을 삭제하고 다시 설치해야 합니다.

Secure Mail 사용자 도메인

Exchange 사용자 또는 (iOS에만 해당) Notes 사용자를 위한 기본 Active Directory 도메인 이름입니다. 기본값은 비어 있습니다.

백그라운드 네트워크 서비스

백그라운드 네트워크 액세스가 허용되는 서비스 주소의 FQDN 및 포트입니다. 이 값은 내부 네트워크 또는 Secure Mail이 연결하는 다른 네트워크(예: mail.example.com:443)에 있는 Exchange Server 또는 ActiveSync 서버일 수 있습니다.

이 정책을 구성하는 경우, 네트워크 액세스 정책을 **내부 네트워크로 터널링됨**으로 설정합니다. 이 정책은 네트워크 액세스 정책을 구성할 때 적용됩니다. Exchange Server가 내부 네트워크에 있고 NetScaler Gateway를 사용하여 내부 Exchange Server에 대한 연결을 프록시하려는 경우 이 정책을 사용합니다.

기본값은 비어 있으며, 이는 백그라운드 네트워크 서비스를 사용할 수 없음을 의미합니다.

백그라운드 서비스 티켓 만료

백그라운드 네트워크 서비스 티켓이 유효하게 유지되는 기간입니다. 만료 후에는 티켓을 갱신하기 위해 엔터프라이즈 로그인에 필요합니다. 기본값은 **168시간(7일)**입니다.

백그라운드 네트워크 서비스 게이트웨이

백그라운드 네트워크 서비스에 사용할 대체 게이트웨이 주소(FQDN:포트 형식)입니다. 이 주소는 Secure Mail이 내부 Exchange Server에 연결하는 데 사용하는 Citrix Gateway FQDN 및 포트 번호입니다. Citrix Gateway 구성 유틸리티에서 Secure Ticket Authority(STA)를 구성하고 정책을 가상 서버에 바인딩해야 합니다.

기본값은 비어 있으며, 이는 대체 게이트웨이가 존재하지 않음을 의미합니다.

이 정책을 구성하는 경우, 네트워크 액세스 정책을 **내부 네트워크로 터널링됨**으로 설정합니다. 이 정책은 네트워크 액세스 정책을 구성할 때 적용됩니다. Exchange Server가 내부 네트워크에 있고 Citrix Gateway를 사용하여 내부 Exchange Server에 대한 연결을 프록시하려는 경우 이 정책을 사용하십시오.

연락처 내보내기

중요:

사용자가 Exchange Server에 직접 액세스할 수 있는 경우(즉, Citrix Gateway 외부에서) 이 기능을 활성화하지 마십시오. 그렇지 않으면 장치와 Exchange에서 연락처가 중복됩니다.

끔으로 설정하면 Secure Mail 연락처가 장치로 단방향 동기화되는 것을 방지하고 Secure Mail 연락처 공유 (vCard 형식)를 방지합니다. 기본값은 **끔**입니다.

내보낼 연락처 필드

주소록으로 내보낼 연락처 필드를 제어합니다. **모두**로 설정하면 모든 연락처 필드가 내보내집니다. **이름 및 전화**로 설정하면 이름 및 전화 관련 연락처 필드가 모두 내보내집니다. **이름, 전화 및 이메일**로 설정하면 이름, 전화 및 이메일 관련 연락처 필드가 모두 내보내집니다. 기본값은 **모두**입니다.

모든 SSL 인증서 허용

켄으로 설정하면 Secure Mail은 모든 SSL 인증서(유효 여부와 관계없이)를 허용하고 액세스를 허용합니다. **끔**으로 설정하면 Secure Mail은 인증서 오류가 발생할 때 액세스를 차단하고 경고를 표시합니다. 기본값은 **끔**입니다.

보안 연결 사용

켄으로 설정하면 Secure Mail은 보안 연결을 사용합니다. **끔**으로 설정하면 Secure Mail은 보안 연결을 사용하지 않습니다. 기본값은 **켄**입니다.

정보 권한 관리

켄으로 설정하면 Secure Mail은 Exchange 정보 권한 관리(IRM) 기능을 지원합니다. 기본값은 **끔**입니다.

잠금 화면 알림 제어

잠금 장치 화면에 메일 및 캘린더 알림이 표시되는지 여부를 제어합니다. **허용**을 선택하면 알림에 포함된 모든 정보가 표시됩니다. **차단**을 선택하면 알림이 표시되지 않습니다. **이메일 발신자 또는 이벤트 제목**을 선택하면 이메일 발신자 이름 또는 캘린더 이벤트 제목만 표시됩니다. **개수만**을 선택하면 메일 및 회의 초대 개수와 캘린더 미리 알림 시간만 표시됩니다. 기본값은 **허용**입니다.

기본 동기화 간격

Secure Mail의 기본 동기화 간격을 지정합니다. Secure Mail 사용자는 기본값을 변경할 수 있습니다.

Exchange ActiveSync 사서함 정책 설정인 **최대 이메일 보관 기간 필터**가 이 정책보다 우선합니다. 최대 이메일 보관 기간 필터보다 큰 기본 동기화 간격을 지정하면 **최대 이메일 보관 기간 필터** 설정이 대신 사용됩니다. Secure Mail은 **Active Sync 최대 이메일 보관 기간 필터** 설정보다 작은 동기화 간격 값만 표시합니다.

기본값은 **3일**입니다.

Wi-Fi를 통한 첨부 파일 다운로드 활성화

켜짐으로 설정하면 Secure Mail 첨부 파일 다운로드 옵션이 활성화되어 사용자가 기본적으로 내부 Wi-Fi 네트워크를 통해 첨부 파일을 다운로드할 수 있습니다. **꺼짐**으로 설정하면 Secure Mail 첨부 파일 다운로드 옵션이 비활성화되어 사용자가 기본적으로 Wi-Fi를 통해 첨부 파일을 다운로드할 수 없습니다. 기본값은 **꺼짐**입니다.

오프라인 문서 허용

사용자가 장치에 오프라인 문서를 저장할 수 있는지 여부와 저장 기간을 지정합니다. 기본값은 **무제한**입니다.

이메일 초안 자동 저장 활성화

켜짐으로 설정하면 Secure Mail은 메시지를 **초안** 폴더에 자동으로 저장하는 것을 지원합니다. 기본값은 **켜짐**입니다.

초기 인증 메커니즘

이 정책은 MDX에서 제공하는 메일 서버 주소가 첫 사용 프로비저닝 화면의 **주소** 필드를 채우는 데 사용되는지 아니면 사용자 이메일 주소가 사용되는지를 나타냅니다. 기본값은 **메일 서버 주소**입니다.

초기 인증 자격 증명

이 정책은 초기 첫 사용 프로비저닝 화면에 채워질 사용자 이름으로 선택해야 하는 값을 정의합니다. 기본값은 **등록 사용자 이름**입니다.

주 번호 사용

켜짐으로 설정하면 달력 보기에 주 번호가 포함됩니다. 기본값은 **꺼짐**입니다.

이메일 분류

켜짐으로 설정하면 Secure Mail은 SEC(보안) 및 DLM(배포 제한 마커)에 대한 이메일 분류 표시를 지원합니다. 분류 표시는 이메일 헤더에 **X-Protective-Marking** 값으로 나타납니다. 관련 이메일 분류 정책을 구성해야 합니다. 기본값은 **꺼짐**입니다.

이메일 분류 표시

최종 사용자에게 제공될 분류 표시를 지정합니다. 목록이 비어 있으면 Secure Mail은 보호 표시 목록을 포함하지 않습니다. 표시 목록에는 세미콜론으로 구분된 값 쌍이 포함됩니다. 각 쌍에는 Secure Mail에 나타나는 값과 Secure Mail의 이메일 제목 및 헤더에 추가되는 텍스트인 표시 값이 포함됩니다. 예를 들어, 표시 쌍 `"UNOFFICIAL, SEC=UNOFFICIAL;"`에서 목록 값은 `***UNOFFICIAL***`이고 표시 값은 `***SEC=UNOFFICIAL***`입니다.

이메일 분류 네임스페이스

사용된 분류 표준에 따라 이메일 헤더에 필요한 분류 네임스페이스를 지정합니다. 예를 들어, "gov.au" 네임스페이스는 헤더에 "NS=gov.au"로 나타납니다. 기본값은 비어 있습니다.

이메일 분류 버전

사용된 분류 표준에 따라 이메일 헤더에 필요한 분류 버전을 지정합니다. 예를 들어, "2012.3" 버전은 헤더에 "VER=2012.3"으로 나타납니다. 기본값은 비어 있습니다.

기본 이메일 분류

사용자가 표시를 선택하지 않을 경우 Secure Mail이 이메일에 적용하는 보호 표시를 지정합니다. 이 값은 이메일 분류 표시 정책 목록에 있어야 합니다. 기본값은 **UNOFFICIAL**입니다.

메일 검색 제한

메일 서버 검색에 포함되는 일수를 제한하여 모바일 장치에서 액세스할 수 있는 메일 기록의 양을 제한합니다. 모바일 장치에 동기화되는 메일의 양을 제한하려면 최대 동기화 간격 정책을 구성하십시오. 기본값은 **무제한**입니다.

최대 동기화 간격

동기화 기간을 제한하여 모바일 장치에 로컬로 저장되는 메일의 양을 제어합니다.

장치가 메일 서버에서 검색할 수 있는 기간을 제한하려면 메일 서버 검색 제한 정책을 구성하십시오.

값은 다음과 같습니다.

- 3일
- 1주
- 2주
- 1개월
- 모두

기본값은 **모두**입니다.

캘린더 웹 및 오디오 옵션

- **GoToMeeting 및 사용자 입력** - 이 옵션을 선택하면 사용자는 설정하려는 회의 유형을 선택할 수 있습니다. 옵션에는 GoToMeeting 페이지를 여는 GoToMeeting과 사용자가 회의 정보를 수동으로 입력할 수 있는 기타 회의가 포함됩니다.

- **사용자 입력만** - 이 옵션을 선택하면 사용자는 회의 정보를 수동으로 입력할 수 있는 기타 회의 페이지로 바로 이동합니다.

S/MIME 공개 인증서 원본

S/MIME 공개 인증서의 원본을 지정합니다. **Exchange**인 경우 Secure Mail은 Exchange Server에서 인증서를 가져옵니다. **LDAP**인 경우 Secure Mail은 LDAP 서버에서 인증서를 가져옵니다. 기본값은 **Exchange**입니다.

LDAP 서버 주소

포트 번호를 포함한 LDAP 서버 주소입니다. 기본값은 비어 있습니다.

LDAP 기본 DN

LDAP 기본 고유 이름입니다. 기본값은 비어 있습니다.

익명으로 LDAP 액세스

이 정책이 **켜짐**으로 설정된 경우 Secure Mail은 사전 인증 없이 LDAP를 검색할 수 있습니다. 기본값은 **꺼짐**입니다.

허용된 이메일 도메인

server.company.com, server.company.co.uk와 같이 쉼표로 구분된 형식으로 허용된 이메일 도메인 목록을 정의합니다. 기본값은 비어 있으며, 이는 Secure Mail이 이메일 도메인을 필터링하지 않고 모든 이메일 도메인을 지원함을 의미합니다. Secure Mail은 나열된 도메인을 이메일 주소의 도메인 이름과 일치시킵니다.

예를 들어, server.company.com이 나열된 도메인 이름이고 이메일 주소가 user@internal.server.company.com인 경우 Secure Mail은 해당 이메일 주소를 지원합니다.

푸시 알림

사서함 활동에 대한 FCM 기반 알림을 활성화합니다. **켜짐**으로 설정된 경우 Secure Mail은 푸시 알림을 지원합니다. 기본값은 **꺼짐**입니다.

푸시 알림 EWS 호스트 이름

메일용 Exchange 웹 서비스(EWS)를 호스팅하는 서버입니다. 값은 포트 번호와 함께 EWS의 URL이어야 합니다. 기본값은 비어 있습니다.

푸시 알림 지역

Secure Mail 사용자를 위한 FCM 호스트가 위치한 지역입니다. 옵션은 미주, EMEA, PAC입니다. 기본값은 미주입니다.

인증 실패 시 사용자 이름 마이그레이션 시도

이 정책은 인증을 위해 Exchange 사용자 이름을 UPN으로 마이그레이션하려고 시도합니다. 기본값은 **해제**입니다.

피싱 메일 주소 보고

구성된 경우, 의심스러운 피싱 메일을 지정된 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록으로 보고할 수 있습니다. 기본값은 비어 있습니다. 이 정책을 구성하지 않으면 피싱 메시지를 보고할 수 없습니다.

피싱 보고 메커니즘

이 정책은 의심스러운 피싱 메일을 보고하는 데 사용되는 메커니즘을 나타냅니다.

- 첨부 파일(.eml)로 보고 – 피싱 메일을 첨부 파일로 보고합니다. 첨부 파일은 피싱 메일 주소 보고 정책에 구성된 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록으로 전송됩니다.
- 전달로 보고 – 피싱 메일을 전달로 보고합니다. 메일은 피싱 메일 주소 보고 정책에 구성된 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록으로 전달됩니다.

참고:

이 정책은 Microsoft Exchange 서버에서만 사용할 수 있습니다.

기본값은 첨부 파일(.eml)로 보고입니다.

비즈니스용 Skype 모임 도메인

이 정책에는 비즈니스용 Skype 모임에 사용되는 쉼표로 구분된 도메인 목록이 포함되어 있습니다. Secure Mail은 이미 다음과 같은 URL 접두사가 있는 모임을 처리합니다.

- `https://join`
- `https://meet`
- `https://lync`

이 정책을 사용하면 다른 Skype for Business 도메인을 `https://*domain*` 형식으로 추가할 수 있습니다. 도메인은 영숫자 문자열이어야 하며 특수 문자를 포함할 수 없습니다. 선행 `https://` 또는 후행 마침표를 입력하지 마십시오.

예시

정책 값이 `customDomain1,customDomain2` 인 경우 Skype for Business에 지원되는 URL 접두사는 다음과 같습니다. `https://customDomain1` `http://customDomain1` `https://customDomain2` `http://customDomain2`

기본값은 비어 있습니다.

캘린더 내보내기

이 정책을 사용하면 Secure Mail 캘린더 이벤트를 장치 또는 개인 캘린더로 내보낼 수 있습니다. 개인 캘린더에서 이벤트를 볼 수 있습니다. Secure Mail을 사용하여 이벤트를 편집할 수 있습니다. 기본값은 **회의 시간**입니다.

개인 캘린더에 표시되는 캘린더 이벤트 필드에 사용할 수 있는 MDX 정책 값은 다음과 같습니다.

- 없음 (내보내지 않음)
- 회의 시간
- 회의 시간, 위치
- 회의 시간, 제목, 위치
- 회의 시간, 사용 가능 여부, 참석자, 제목, 위치, 메모

Office 365용 OAuth 지원

O365용 최신 인증 사용

이 정책이 **켜짐**인 경우 Secure Mail은 Office 365에서 계정을 구성하는 동안 인증을 위해 OAuth 프로토콜을 사용합니다. **꺼짐**인 경우 Secure Mail은 기본 인증을 사용합니다. 기본값은 **꺼짐**입니다.

신뢰할 수 있는 Exchange Online 호스트 이름

계정을 구성하는 동안 인증을 위해 OAuth 메커니즘을 사용하는 신뢰할 수 있는 Exchange Online 호스트 이름 목록을 정의합니다. 이 값은 server.company.com, server.company.co.uk와 같은 쉼표로 구분된 형식입니다. 목록이 비어 있으면 Secure Mail은 계정 구성에 기본 인증을 사용합니다. 기본값은 outlook.office365.com입니다.

신뢰할 수 있는 AD FS 호스트 이름

Office 365 OAuth 인증 중에 암호가 자동으로 채워지는 웹 페이지에 대해 신뢰할 수 있는 AD FS 호스트 이름 목록을 정의합니다. 이 값은 sts.companynamename.com, sts.company.co.uk와 같은 쉼표로 구분된 형식입니다. 목록이 비어 있으면 Secure Mail은 암호를 자동으로 채우지 않습니다. Secure Mail은 Office 365 인증 중에 발견된 웹 페이지의 호스트 이름과 나열된 호스트 이름을 일치시키고 해당 페이지가 HTTPS 프로토콜을 사용하는지 확인합니다.

예를 들어, sts.company.com이 나열된 호스트 이름이고 사용자가 https://sts.company.com으로 이동하면 Secure Mail은 페이지에 암호 필드가 있는 경우 암호를 채웁니다. 기본값은 login.microsoftonline.com입니다.

최신 인증을 위한 사용자 지정 사용자 에이전트

이 정책을 사용하면 최신 인증을 위한 기본 사용자 에이전트 문자열을 변경할 수 있습니다. 구성된 경우 이 사용자 에이전트 문자열은 Microsoft AD FS를 사용한 인증에 사용됩니다. 이 정책을 구성하지 않으면 최신 인증 중에 기본 Secure Mail 사용자 에이전트가 사용됩니다.

Slack 통합

Slack 사용

Slack 통합을 차단하거나 허용합니다. **켜짐**으로 설정하면 Secure Mail 인터페이스에 Slack 기능이 포함됩니다. **꺼짐**으로 설정하면 Secure Mail 인터페이스에 Slack 기능이 포함되지 않습니다.

Slack 작업 공간 이름

회사 Slack 작업 공간 이름입니다. 이름을 제공하면 Secure Mail은 로그인 시 작업 공간 이름을 미리 채웁니다. 이름을 제공하지 않으면 사용자는 작업 공간 이름(name.slack.com)을 직접 입력해야 합니다.

iOS용 모바일 생산성 앱을 위한 MDX 정책

이 문서에서는 iOS 앱용 MDX 정책에 대해 설명합니다. Citrix Endpoint Management 콘솔에서 정책 설정을 변경합니다. 자세한 내용은 [앱 추가](#)를 참조하십시오.

다음 목록에는 Secure Web에 특정한 MDX 정책이 포함되어 있지 않습니다. Secure Web에 나타나는 정책에 대한 자세한 내용은 [Secure Web 정책](#)을 참조하십시오.

인증

장치 암호

켜짐으로 설정하면, 비활성 기간 후 장치가 시작되거나 다시 시작될 때 장치 잠금을 해제하려면 PIN 또는 암호가 필요합니다. Apple 파일 암호화를 사용하여 앱 데이터를 암호화하려면 장치 암호가 필요합니다. 장치의 모든 앱 데이터는 암호화됩니다. 기본값은 **켜짐**입니다.

앱 암호

켜짐으로 설정하면, 비활성 기간 후 앱이 시작되거나 다시 시작될 때 앱 잠금을 해제하려면 PIN 또는 암호가 필요합니다. 기본값은 **켜짐**입니다.

모든 앱에 대한 비활성 타이머를 구성하려면 **설정** 탭의 **클라이언트 속성**에서 **INACTIVITY_TIMER** 값을 분 단위로 설정합니다. 기본 비활성 타이머 값은 **60**분입니다. 비활성 타이머를 비활성화하여 앱이 시작될 때만 PIN 또는 암호 프롬프트가 나타나도록 하려면 값을 0으로 설정합니다.

참고:

암호화 키 정책에 대해 **오프라인 보안**을 선택하면 이 정책이 자동으로 활성화됩니다.

최대 오프라인 기간(시간)

앱 사용 권한을 재확인하고 Citrix Endpoint Management에서 정책을 새로 고치지 않고 앱이 실행될 수 있는 최대 기간을 정의합니다. 만료 시 필요한 경우 서버 로그온이 트리거될 수 있습니다. 기본값은 **168시간(7일)**입니다. 최소 기간은 **1시간**입니다.

대체 시트릭스 게이트웨이**참고:**

Endpoint Management 콘솔의 이 정책 이름은 **Alternate NetScaler® Gateway**입니다.

이 앱과 함께 인증 및 마이크로 VPN 세션에 사용해야 하는 특정 대체 Citrix Gateway의 주소입니다. 이 정책은 선택 사항입니다. 온라인 세션 필수 정책과 함께 사용하면 이 정책은 앱이 특정 게이트웨이에 다시 인증하도록 강제합니다. 이러한 게이트웨이는 일반적으로 다른(더 높은 보증) 인증 요구 사항 및 트래픽 관리 정책을 가집니다. 비워두면 서버의 기본 게이트웨이가 항상 사용됩니다. 기본값은 비어 있습니다.

장치 보안**탈옥 또는 루팅 차단**

켜짐으로 설정하면 장치가 탈옥 또는 루팅된 경우 앱이 잠깁니다. **꺼짐**으로 설정하면 장치가 탈옥 또는 루팅된 경우에도 앱을 실행할 수 있습니다. 기본값은 **켜짐**입니다.

네트워크 요구 사항**Wi-Fi 필요**

켜짐으로 설정하면 장치가 Wi-Fi 네트워크에 연결되어 있지 않을 때 앱이 잠깁니다. **꺼짐**으로 설정하면 장치에 4G/3G, LAN 또는 Wi-Fi 연결과 같은 활성 연결이 있는 경우 앱을 실행할 수 있습니다. 기본값은 **꺼짐**입니다.

허용된 Wi-Fi 네트워크

심표로 구분된 Wi-Fi 네트워크 목록입니다. 네트워크 이름에 영숫자가 아닌 문자(심표 포함)가 포함된 경우 이름은 큰따옴표로 묶어야 합니다. 앱은 나열된 네트워크 중 하나에 연결된 경우에만 실행됩니다. 비워두면

모든 네트워크가 허용됩니다. 이 값은 셀룰러 네트워크 연결에 영향을 주지 않습니다. 기본값은 비어 있습니다.

기타 액세스

필수 업그레이드 비활성화

사용자가 App Store에서 앱의 최신 버전으로 업그레이드해야 하는 요구 사항을 비활성화합니다. 기본값은 켜짐입니다.

앱 업데이트 유예 기간(시간)

시스템이 앱 업데이트를 사용할 수 있음을 감지한 후 앱을 계속 사용할 수 있는 유예 기간을 정의합니다. 기본값은 **168시간(7일)**입니다.

참고:

0 값을 사용하지 않는 것이 좋습니다. 0 값은 업데이트가 다운로드되어 설치될 때까지 실행 중인 앱이 즉시 사용되지 못하도록 합니다(사용자에게 경고 없이). 이 값을 사용하면 사용자가 필수 업데이트를 준수하기 위해 앱을 종료해야 하는 상황(작업 손실 가능성 있음)이 발생할 수 있습니다.

잠금 시 앱 데이터 지우기

앱이 잠길 때 데이터를 지우고 앱을 재설정합니다. **끄기**로 설정하면 앱이 잠겨도 앱 데이터가 지워지지 않습니다. 기본값은 **끄기**입니다.

앱은 다음 이유 중 하나로 잠길 수 있습니다.

- 사용자의 앱 권한 상실
- 앱 구독 제거됨
- 계정 제거됨
- Secure Hub 제거됨
- 너무 많은 앱 인증 실패
- 탈옥된 장치 감지됨(정책 설정에 따름)
- 다른 관리 작업으로 인해 장치가 잠금 상태로 전환됨

활성 폴링 기간(분)

앱이 시작되면 MDX Framework는 Citrix Endpoint Management를 폴링하여 현재 앱 및 장치 상태를 확인합니다. Endpoint Management를 실행하는 서버에 연결할 수 있다고 가정하면, 프레임워크는 장치의 잠금/

지우기 상태와 앱의 활성화/비활성화 상태에 대한 정보를 반환합니다. 서버에 연결할 수 있는지 여부와 관계없이, 활성 폴링 기간 간격에 따라 후속 폴링이 예약됩니다. 기간이 만료되면 새 폴링이 다시 시도됩니다. 기본 값은 **60분(1시간)**입니다.

중요:

위험도가 높은 앱의 경우에만 이 값을 낮게 설정하십시오. 그렇지 않으면 성능에 영향을 미칠 수 있습니다.

암호화

암호화 유형

MDX 또는 장치 플랫폼이 데이터 암호화를 처리할지 여부를 선택할 수 있습니다. **MDX 암호화**를 선택하면 MDX가 데이터를 암호화합니다. **규정 준수 적용을 통한 플랫폼 암호화**를 선택하면 장치 플랫폼이 데이터를 암호화합니다. 기본값은 **MDX 암호화**입니다.

비준수 장치 동작

장치가 암호화의 최소 규정 준수 요구 사항을 따르지 않을 때 수행할 작업을 선택할 수 있습니다. 앱이 정상적으로 실행되도록 하려면 **앱 허용**을 선택합니다. 경고가 나타난 후 앱이 실행되도록 하려면 **경고 후 앱 허용**을 선택합니다. 앱 실행을 차단하려면 **차단**을 선택합니다. 기본값은 **경고 후 앱 허용**입니다.

MDX 암호화 사용

끔으로 설정하면 장치에 저장된 데이터가 암호화되지 않습니다. 켜로 설정하면 장치에 저장된 데이터가 암호화됩니다. 기본값은 **켄**입니다.

주의:

앱을 배포한 후 이 정책을 변경하면 사용자가 앱을 다시 설치해야 합니다.

데이터베이스 암호화 제외

자동으로 암호화되지 않는 데이터베이스의 제외 목록입니다. 특정 데이터베이스의 암호화를 방지하려면 이 쉘표로 구분된 정규식 목록에 항목을 추가하십시오. 데이터베이스 경로 이름이 정규식 중 하나와 일치하면 해당 데이터베이스는 암호화에서 제외됩니다. 제외 패턴은 Posix 1003.2 확장 정규식 구문을 지원합니다. 패턴 일치는 대소문자를 구분하지 않습니다.

예시

`\\.db$,\\.sqlite$` 은 `.db` 또는 `.sqlite` 으로 끝나는 모든 데이터베이스 경로 이름을 제외합니다.

\\Database\\unencrypteddb\\.db는 Database 하위 폴더의 unencrypteddb.db 데이터베이스와 일치합니다.

****\\Database****는 경로에 ****/Database/****를 포함하는 모든 데이터베이스와 일치합니다.

기본값은 비어 있습니다.

파일 암호화 제외

자동으로 암호화되지 않는 파일의 제외 목록입니다. 특정 파일 집합에 대한 암호화를 방지하려면 이 쉘표로 구분된 정규식 목록에 항목을 추가하십시오. 파일 경로 이름이 정규식 중 하나와 일치하면 해당 파일은 암호화에서 제외됩니다. 제외 패턴은 Posix 1003.2 확장 정규식 구문을 지원합니다. 패턴 일치는 대소문자를 구분하지 않습니다.

예시

\\.log\$,\\.dat\$ 은 **.log** 또는 **.dat** 로 끝나는 모든 파일 경로 이름을 제외합니다.

\\Documents\\unencrypteddoc\\.txt는 Documents 하위 폴더에 있는 unencrypteddoc.txt 파일의 내용과 일치합니다.

\\Documents\\UnencryptedDocs\\.*\\.txt는 하위 경로 /Documents/UnencryptedDocs/ 아래의 ".txt" 파일과 일치합니다.

기본값은 비어 있습니다.

앱 상호 작용

잘라내기 및 복사

이 앱에 대한 클립보드 잘라내기 및 복사 작업을 차단, 허용 또는 제한합니다. **제한됨**으로 설정하면 복사된 클립보드 데이터는 MDX 앱에서만 사용할 수 있는 개인 클립보드에 저장됩니다. 기본값은 **제한됨**입니다.

붙여넣기

이 앱에 대한 클립보드 붙여넣기 작업을 차단, 허용 또는 제한합니다. **제한됨**으로 설정하면 붙여넣기된 클립보드 데이터는 MDX 앱에서만 사용할 수 있는 개인 클립보드에서 가져옵니다. 기본값은 **제한 없음**입니다.

문서 교환 (다음으로 열기)

이 앱의 문서 교환 작업을 차단, 허용 또는 제한합니다. **제한됨**으로 설정하면 다른 MDX 앱과만 문서를 교환할 수 있습니다.

제한 없음으로 설정된 경우, 사용자가 래핑되지 않은 앱에서 문서를 열 수 있도록 암호화 사용 정책을 **켜기**로 설정합니다. 수신 앱이 래핑되지 않았거나 암호화가 비활성화된 경우 Citrix Endpoint Management가 문서를 해독합니다. 기본값은 **제한됨**입니다.

제한된 Open-In 예외 목록

문서 교환(Open In) 정책이 **제한됨**으로 설정된 경우, MDX 앱은 이 심표로 구분된 관리되지 않는 앱 ID 목록과 문서를 공유할 수 있습니다. 이는 문서 교환(Open In) 정책이 **제한됨**이고 암호화 사용이 **켜기**인 경우에도 마찬가지입니다. 기본 예외 목록은 Office 365 앱을 허용합니다.

com.microsoft.Office.Word,com.microsoft.Office.Excel,com.microsoft.Office.Powerpoint,
com.microsoft.onenote,com.microsoft.onenoteiPad,com.microsoft.Office.Outlook

이 정책은 Office 365 앱만 지원합니다.

주의:

이 정책의 보안 영향을 반드시 고려하십시오. 예외 목록은 관리되지 않는 앱과 MDX 환경 간에 콘텐츠가 이동하도록 허용합니다.

연결 보안 수준

연결에 사용되는 TLS/SSL의 최소 버전을 결정합니다. **TLS**로 설정하면 연결은 모든 TLS 프로토콜을 지원합니다. **SSLv3** 및 **TLS**로 설정하면 연결은 SSL 3.0 및 TLS를 지원합니다. 기본값은 **TLS**입니다.

인바운드 문서 교환(Open In)

이 앱의 인바운드 문서 교환 작업을 차단, 제한 또는 허용합니다. **제한됨**으로 설정하면 다른 MDX 앱과만 문서를 교환할 수 있습니다. 기본값은 **제한 없음**입니다.

차단됨 또는 **제한됨**으로 설정된 경우, 인바운드 문서 교환 허용 목록 정책을 사용하여 이 앱으로 문서를 보낼 수 있는 앱을 지정할 수 있습니다.

옵션: **제한 없음**, **차단됨**, 또는 **제한됨**

앱 URL 스키마

iOS 앱은 특정 스키마(예: "http://")를 처리하도록 등록된 다른 앱으로 URL 요청을 보낼 수 있습니다. 이 기능은 앱이 다른 앱에 도움 요청을 전달하는 메커니즘을 제공합니다. 이 정책은 이 앱으로 전달되어 처리되는 스키마(즉, 인바운드 URL)를 필터링하는 역할을 합니다. 기본값은 비어 있으며, 이는 등록된 모든 앱 URL 스키마가 차단됨을 의미합니다.

정책은 각 패턴 앞에 더하기 기호 "+" 또는 빼기 기호 "-"가 붙는 심표로 구분된 패턴 목록으로 포맷되어야 합니다. 인바운드 URL은 일치하는 항목이 발견될 때까지 나열된 순서대로 패턴과 비교됩니다. 일치하면 접두사가 취할 작업을 지시합니다.

- 빼기 기호 "-" 접두사는 URL이 이 앱으로 전달되는 것을 차단합니다.
- 더하기 기호 "+" 접두사는 URL이 처리될 수 있도록 앱으로 전달되는 것을 허용합니다.
- 패턴에 "+" 또는 "-"가 제공되지 않으면 "+" (허용)로 간주됩니다.
- 인바운드 URL이 목록의 어떤 패턴과도 일치하지 않으면 해당 URL은 차단됩니다.

다음 표에는 앱 URL 스키마의 예가 포함되어 있습니다.

스키마	URL 스키마를 필요로 하는 앱	목적
<code>ctxmobilebrowser</code>	보안 웹-	Secure Web이 다른 앱의 HTTP: URL을 처리하도록 허용합니다.-
<code>ctxmobilebrowsers</code>	보안 웹-	Secure Web이 다른 앱의 HTTPS: URL을 처리하도록 허용합니다.
<code>ctxmail</code>	보안 메일-	Secure Mail이 다른 앱의 <code>mailto:</code> URL을 처리하도록 허용합니다.
COL-G2M	GoToMeeting-	래핑된 GoToMeeting 앱이 회의 요청을 처리하도록 허용합니다.
<code>ctxsalesforce</code>	Salesforce를 위한 Citrix -	Citrix for Salesforce가 Salesforce 요청을 처리하도록 허용합니다.
<code>wbx</code>	WebEx	래핑된 WebEx 앱이 회의 요청을 처리하도록 허용합니다.

앱 상호 작용 (아웃바운드 URL)

URL 필터링에서 제외된 도메인

이 정책은 "허용된 URL" 필터링에서 아웃바운드 URL을 제외합니다. "허용된 URL" 필터링에서 제외할 FQDN(정규화된 도메인 이름) 또는 DNS 접미사의 심표로 구분된 목록을 추가합니다. 이 정책이 비어 있는 경우(기본값), 정의된 "허용된 URL" 필터링은 URL을 처리합니다. 이 정책에 항목이 포함되어 있으면 목록의

항목 중 하나 이상과 일치하는 호스트 필드를 가진 URL(DNS 접미사 일치를 통해)은 변경되지 않은 상태로 iOS로 전송됩니다. 이 통신은 "허용된 URL" 필터링 로직을 우회합니다. 기본값은 비어 있습니다.

허용된 URL

iOS 앱은 특정 스키마(예: "http://")를 처리하도록 등록된 다른 애플리케이션으로 URL 요청을 보낼 수 있습니다. 이 기능은 앱이 다른 앱에 도움 요청을 전달하는 메커니즘을 제공합니다. 이 정책은 이 앱에서 다른 앱으로 처리하기 위해 전달되는 URL(즉, 아웃바운드 URL)을 필터링하는 역할을 합니다.

정책은 각 패턴 앞에 더하기 "+" 또는 빼기 "-"가 올 수 있는 심표로 구분된 패턴 목록으로 포맷되어야 합니다. 아웃바운드 URL은 일치하는 항목이 발견될 때까지 나열된 순서대로 패턴과 비교됩니다. 일치하면 접두사가 수행할 작업을 결정합니다. 빼기 "-" 접두사는 URL이 다른 앱으로 전달되는 것을 차단합니다. 더하기 "+" 접두사는 URL이 다른 앱으로 처리되도록 허용합니다. 패턴에 "+" 또는 빼기 "-"가 제공되지 않으면 "+" (허용)로 간주됩니다. "="로 구분된 한 쌍의 값은 첫 번째 문자열의 발생이 두 번째 문자열로 대체되는 치환을 나타냅니다. 정규식 "\^" 접두사를 사용하여 문자열을 검색하여 URL의 시작 부분에 고정할 수 있습니다. 아웃바운드 URL이 목록의 어떤 패턴과도 일치하지 않으면 차단됩니다.

기본값

+maps.apple.com

+itunes.apple.com

\^http:=ctxmobilebrowser::

\^https:=ctxmobilebrowsers::

\^mailto:=ctxmail::

+\\^citrixreceiver::

+\\^telprompt::

+\\^tel::

+\\^lmi-g2m::

+\\^maps:ios_addr

+\\^mapitem::

+\\^sms::

+\\^facetime::

`+\\^ctxnotes:``+\\^ctxnotesex:``+\\^ctxtasks:``+\\^facetime-audio:``+\\^itms-apps:``+\\^ctx-sf:``+\\^sharefile:``+\\^lync:``+\\^slack:``+\\^msteams:`

설정이 비어 있으면 다음을 제외한 모든 URL이 차단됩니다.

- `http:`
- `https:`
- `+citrixreceiver: +tel:`

다음 표에는 허용되는 URL의 예가 나와 있습니다.

URL 형식	설명
<code>\\^mailto:=ctxmail:</code>	모든 <code>mailto:</code> URL은 Secure Mail에서 열립니다.
<code>\\^http:</code>	모든 HTTP URL은 Secure Web에서 열립니다.
<code>\\^https:</code>	모든 HTTPS URL은 Secure Web에서 열립니다.
<code>\\^tel:</code>	사용자가 전화를 걸 수 있도록 허용합니다.
<code>-//www.dropbox.com</code>	관리되는 앱에서 전송된 Dropbox URL을 차단합니다.
<code>+\\^COL-G2M:</code>	관리되는 앱이 GoToMeeting 클라이언트 앱을 열 수 있도록 허용합니다.

URL 형식	설명
<code>- \^SMS:</code>	메시징 채팅 클라이언트 사용을 차단합니다.
<code>- \^wbx:</code>	관리되는 앱이 WebEx 클라이언트 앱을 열지 못하도록 차단합니다.
<code>+ \^ctxsalesforce:</code>	Citrix for Salesforce가 Salesforce 서버와 통신할 수 있도록 허용합니다.

허용된 Secure Web 도메인

이 정책은 URL을 Secure Web 앱(`\^ http://ctxmobilebrowser:` 및 `\^https://ctxmobilebrowsers:`)으로 리디렉션하는 "허용된 URL" 정책 항목에만 영향을 미칩니다. Secure Web 앱으로 리디렉션할 수 있는 정규화된 도메인 이름(FQDN) 또는 DNS 접미사의 심표로 구분된 목록을 추가합니다. 이 정책이 비어 있는 경우(기본값) 모든 도메인이 Secure Web 앱으로 리디렉션될 수 있습니다. 이 정책에 항목이 포함되어 있으면 목록의 항목 중 하나 이상과 일치하는 호스트 필드를 가진 URL(DNS 접미사 일치를 통해)만 Secure Web 앱으로 리디렉션됩니다. 다른 모든 URL은 Secure Web 앱을 우회하여 iOS로 변경되지 않은 채 전송됩니다. 기본값은 비어 있습니다.

앱 제한

중요:

앱이 전화 기능에 액세스하거나 사용하는 것을 차단하는 정책의 보안 영향을 반드시 고려하십시오. 해당 정책이 **해제**되면 관리되지 않는 앱과 보안 환경 간에 콘텐츠가 이동할 수 있습니다.

카메라 차단

켜짐으로 설정하면 앱이 카메라 하드웨어를 직접 사용하는 것을 방지합니다. 기본값은 **꺼짐**입니다.

사진 보관함 차단

켜짐으로 설정하면 앱이 장치의 사진 보관함에 액세스하는 것을 방지합니다. 기본값은 **켜짐**입니다.

마이크 녹음 차단

켜짐으로 설정하면 앱이 마이크 하드웨어를 직접 사용하는 것을 방지합니다. 기본값은 **켜짐**입니다.

받아쓰기 차단

켜짐으로 설정하면 앱이 받아쓰기 서비스를 직접 사용하는 것을 방지합니다. 기본값은 **켜짐**입니다.

위치 서비스 차단

켜짐으로 설정하면 앱이 위치 서비스 구성 요소(GPS 또는 네트워크)를 사용하는 것을 방지합니다. Secure Mail의 기본값은 꺼짐입니다.

SMS 작성 차단

켜짐으로 설정하면 앱이 앱에서 SMS/문자 메시지를 보내는 데 사용되는 SMS 작성 기능을 사용하는 것을 방지합니다. 기본값은 꺼짐입니다.

이메일 작성 차단

켜짐으로 설정하면 앱이 앱에서 이메일 메시지를 보내는 데 사용되는 이메일 작성 기능을 사용하는 것을 방지합니다. 기본값은 꺼짐입니다.

iCloud 차단

켜짐으로 설정하면 앱이 설정 및 데이터를 저장하고 공유하기 위해 iCloud를 사용하는 것을 방지합니다.

참고

iCloud 데이터 파일은 파일 백업 차단 정책에 의해 제어됩니다.

기본값은 꺼짐입니다.

조회 차단

켜짐으로 설정하면 앱이 사전, iTunes, App Store, 영화 상영 시간, 주변 위치 등에서 강조 표시된 텍스트를 검색하는 조회 기능을 사용하지 못하도록 합니다. 기본값은 꺼짐입니다.

파일 백업 차단

켜짐으로 설정하면 iCloud 또는 iTunes가 데이터 파일을 백업하지 못하도록 합니다. 기본값은 꺼짐입니다.

AirPrint 차단

켜짐으로 설정하면 앱이 AirPrint 지원 프린터로 데이터를 인쇄하는 AirPrint 기능을 사용하지 못하도록 합니다. 기본값은 꺼짐입니다.

AirDrop 차단

켜짐으로 설정하면 앱이 AirDrop을 사용하지 못하도록 합니다. 기본값은 꺼짐입니다.

파일 첨부 차단

참고

이 정책은 iOS 11 이상에서 적용됩니다.

켜짐으로 설정하면 첨부 파일 처리가 비활성화됩니다. 기본값은 **꺼짐**입니다.

Facebook 및 Twitter API 차단

이 정책이 **On**이면 앱이 iOS Facebook 및 Twitter API를 사용하지 못하도록 합니다. 기본값은 **On**입니다.

화면 내용 가리기

이 정책이 **On**이면 사용자가 앱을 전환할 때 화면이 가려집니다. 이 정책은 iOS가 화면 내용을 기록하고 미리 보기를 표시하는 것을 방지합니다. 기본값은 **On**입니다.

타사 키보드 차단(iOS 11 이상만 해당)

이 정책이 **On**이면 앱이 iOS 8 이상에서 타사 키보드 확장을 사용하지 못하도록 합니다. 기본값은 **On**입니다.

앱 로그 차단

이 정책이 **On**이면 앱이 모바일 생산성 앱 진단 로깅 기능을 사용하지 못하도록 합니다. **Off**이면 앱 로그가 기록되며 Secure Hub 이메일 지원 기능을 사용하여 수집될 수 있습니다. 기본값은 **Off**입니다.

ShareFile 사용

사용자가 ShareFile을 사용하여 파일을 전송할 수 있도록 허용합니다. 기본값은 **On**입니다.

파일에서 첨부 사용

사용자가 iOS 파일 앱에서 첨부 파일을 추가할 수 있도록 허용합니다. 기본값은 **On**입니다.

앱 네트워크 액세스

네트워크 액세스

참고:

Tunneled - Web SSO는 설정에서 **Secure Browse**의 이름입니다. 동작은 동일합니다.

설정 옵션은 다음과 같습니다.

- **차단됨:** 모든 네트워크 액세스가 차단됩니다. 앱에서 사용하는 네트워킹 API가 실패합니다. 이전 지침에 따라 이러한 실패를 정상적으로 처리해야 합니다.
- **제한 없음:** 모든 네트워크 호출이 직접 이루어지며 터널링되지 않습니다.
- **터널링됨 - 웹 SSO:** HTTP/HTTPS URL이 다시 작성됩니다. 이 옵션은 HTTP 및 HTTPS 트래픽의 터널링만 허용합니다. 터널링됨 - 웹 SSO의 중요한 장점은 HTTP 및 HTTPS 트래픽에 대한 단일 Sign-On(SSO)과 PKINIT 인증입니다. Android에서는 이 옵션의 설정 오버헤드가 낮으므로 웹 브라우징 유형 작업에 선호되는 옵션입니다.

터널링됨 - 전체 VPN 또는 터널링됨 - 전체 VPN 및 웹 SSO 정책을 사용하는 경우 터널링됨 - 웹 SSO 정책으로 전환해야 합니다. 더 이상 사용되지 않는 정책을 계속 사용하면 이메일 동기화가 실패합니다.

참고:

터널링됨 - 전체 VPN을 사용하고 STA(Secure Ticket Authority)가 구성된 경우 최신 인증 화면이 로드되지 않습니다.

Micro VPN 세션 필요

예인 경우 사용자는 엔터프라이즈 네트워크에 연결되어 있고 활성 세션이 있어야 합니다. 아니요인 경우 활성 세션이 필요하지 않습니다. 기본값은 **이전 설정 사용**입니다. 새로 업로드된 앱의 경우 기본값은 **아니요**입니다. 이 새 정책으로 업그레이드하기 전에 선택된 설정은 **이전 설정 사용** 이외의 옵션을 선택할 때까지 계속 적용됩니다.

Micro VPN 세션 필요 유예 기간(분)

이 값은 온라인 세션 필요 정책이 추가 사용을 방지하기 전(온라인 세션이 유효성 검사를 통과할 때까지) 사용자가 앱을 사용할 수 있는 시간을 분 단위로 결정합니다. 기본값은 **0**(유예 기간 없음)입니다. 이 정책은 Microsoft Intune/EMS와의 통합에는 적용되지 않습니다.

인증서 레이블

StoreFront™ 인증서 통합 서비스와 함께 사용될 때 이 레이블은 이 앱에 필요한 특정 인증서를 식별합니다. 레이블이 제공되지 않으면 PKI(공개 키 인프라)와 함께 사용할 수 있는 인증서가 제공되지 않습니다. 기본값은 비어 있습니다(인증서 사용 안 함).

제외 목록

VPN 연결을 통하지 않고 직접 액세스할 FQDN 또는 DNS 접미사의 심표로 구분된 목록입니다. 이 값은 Citrix Gateway가 분할 터널 역방향 모드로 구성된 경우 터널링됨 - 웹 SSO 모드에만 적용됩니다.

앱 로그

기본 로그 출력

기본적으로 모바일 생산성 앱 진단 로깅 기능에서 사용되는 출력 미디어를 결정합니다. 가능한 값은 파일, 콘솔 또는 둘 다입니다. 기본값은 **파일**입니다.

기본 로그 수준

모바일 생산성 앱 진단 로깅 기능의 기본 상세도를 제어합니다. 각 수준에는 더 낮은 값의 수준이 포함됩니다. 가능한 수준의 범위는 다음과 같습니다.

- 0 - 아무것도 로깅되지 않음
- 1 - 심각한 오류
- 2 - 오류
- 3 - 경고
- 4 - 정보 메시지
- 5 - 상세 정보 메시지
- 6 ~ 15 - 디버그 수준 1 ~ 10

기본값은 수준 4(정보 메시지)입니다.

최대 로그 파일

모바일 생산성 앱 진단 로깅 기능이 롤오버하기 전에 보관하는 로그 파일 수를 제한합니다. 최소값은 2입니다. 최대값은 8입니다. 기본값은 2입니다.

최대 로그 파일 크기

모바일 생산성 앱 진단 로깅 기능에서 롤오버하기 전에 보관하는 로그 파일의 MB 단위 크기를 제한합니다. 최소값은 1MB입니다. 최대값은 5MB입니다. 기본값은 2MB입니다.

앱 지오편스

중심점 경도

앱이 작동하도록 제한되는 지점/반경 지오편스의 중심점 경도(X 좌표)입니다. 구성된 지오편스 외부에서 작동하면 앱이 잠긴 상태로 유지됩니다.

값은 부호 있는 도 형식(DDD.dddd)으로 표현해야 합니다(예: "-31.9635"). 서경은 마이너스 부호로 시작해야 합니다. 기본값은 **0**입니다.

중심점 위도

앱이 작동하도록 제한되는 지점/반경 지오펜스의 중심점 위도(Y 좌표)입니다. 구성된 지오펜스 외부에서 작동하면 앱이 잠긴 상태로 유지됩니다.

값은 부호 있는 도 형식(DDD.dddd)으로 표현해야 합니다(예: "43.06581"). 남위는 마이너스 부호로 시작해야 합니다. 기본값은 0입니다.

반경

앱이 작동하도록 제한되는 지오펜스의 반경입니다. 구성된 지오펜스 외부에서 작동하면 앱이 잠긴 상태로 유지됩니다.

값은 미터 단위로 표현해야 합니다. 0으로 설정하면 지오펜스가 비활성화됩니다. 위치 서비스 차단 정책이 활성화되면 지오펜싱이 제대로 작동하지 않습니다. 기본값은 0 (비활성화됨)입니다.

Google 애널리틱스 활성화

켜짐으로 설정하면 Citrix는 제품 품질 향상을 위해 익명 데이터를 수집합니다. **꺼짐**으로 설정하면 데이터가 수집되지 않습니다. 기본값은 **켜짐**입니다.

분석

Google Analytics 세부 정보 수준

Citrix는 제품 품질 향상을 위해 분석 데이터를 수집합니다. **익명**을 선택하면 회사 식별 정보를 포함하지 않도록 사용자가 옵트아웃됩니다. 기본값은 완료입니다.

보고

Citrix 보고

켜짐으로 설정하면 Citrix는 문제 해결을 돕기 위해 충돌 보고서 및 진단 정보를 수집합니다. **꺼짐**으로 설정하면 Citrix는 데이터를 수집하지 않습니다.

참고

Citrix는 기능 플래그를 사용하여 이 기능을 제어할 수도 있습니다. 이 기능이 작동하려면 기능 플래그와 이 정책이 모두 활성화되어야 합니다.

기본값은 **꺼짐**입니다.

업로드 토큰

Citrix Insight Services (CIS) 계정에서 업로드 토큰을 얻을 수 있습니다. 이 선택적 토큰을 지정하면 CIS는 장치에서 업로드된 충돌 보고서 및 진단 정보에 대한 액세스를 제공합니다. Citrix는 동일한 정보에 액세스할 수 있습니다. 기본값은 비어 있습니다.

Wi-Fi로만 보고서 전송

켜짐으로 설정하면 Citrix는 Wi-Fi 네트워크에 연결되어 있을 때만 충돌 보고서 및 진단 정보를 보냅니다. 기본값은 켜짐입니다.

보고서 파일 캐시 최대값

캐시를 지우기 전에 유지되는 충돌 보고서 및 진단 번들의 크기를 제한합니다. 최소값은 1MB입니다. 최대값은 5MB입니다. 기본값은 2MB입니다.

앱 상호 작용

명시적 로그오프 알림

비활성화됨으로 설정하면 사용자 로그오프 시 앱이 활성화되지 않습니다. **공유 장치**만으로 설정하면 장치가 공유 장치로 구성된 경우에만 사용자 로그오프 시 앱이 활성화됩니다. Secure Mail의 기본값은 **공유 장치**만입니다.

앱 설정

보안 메일 익스체인지 서버

Exchange Server의 정규화된 도메인 이름(FQDN) 또는 iOS에만 해당되는 IBM Notes Traveler 서버의 정규화된 도메인 이름(FQDN)입니다. 기본값은 비어 있습니다. 이 필드에 도메인 이름을 제공하면 사용자가 편집할 수 없습니다. 필드를 비워두면 사용자가 자체 서버 정보를 제공합니다.

주의

기존 앱에 대해 이 정책을 변경하는 경우, 정책 변경 사항을 적용하려면 사용자가 앱을 삭제하고 다시 설치해야 합니다.

Secure Mail 사용자 도메인

Exchange 사용자 또는 iOS에만 해당되는 Notes 사용자를 위한 기본 Active Directory 도메인 이름입니다. 기본값은 비어 있습니다.

백그라운드 네트워크 서비스

백그라운드 네트워크 액세스에 허용되는 서비스 주소의 FQDN 및 포트입니다. 이 값은 내부 네트워크 또는 Secure Mail이 연결하는 다른 네트워크(예: mail.example.com:443)에 있는 Exchange Server 또는 ActiveSync 서버일 수 있습니다.

이 정책을 구성하는 경우, 네트워크 액세스 정책을 **내부 네트워크로 터널링됨**으로 설정하십시오. 이 정책은 네트워크 액세스 정책을 구성할 때 적용됩니다. Exchange Server가 내부 네트워크에 있고 Citrix Gateway(이전 명칭: NetScaler Gateway)를 사용하여 내부 Exchange Server로의 연결을 프록시하려는 경우 이 정책을 사용하십시오.

기본값은 비어 있으며, 이는 백그라운드 네트워크 서비스를 사용할 수 없음을 의미합니다.

백그라운드 서비스 티켓 만료

백그라운드 네트워크 서비스 티켓이 유효한 기간입니다. 만료 후에는 티켓을 갱신하기 위해 엔터프라이즈 로그인에 필요합니다. 기본값은 **168시간(7일)**입니다.

백그라운드 네트워크 서비스 게이트웨이

백그라운드 네트워크 서비스에 사용할 대체 게이트웨이 주소(`fqdn:port` 형식). 이 값은 Secure Mail이 내부 Exchange Server에 연결하는 데 사용하는 Citrix Gateway FQDN 및 포트 번호입니다. Citrix Gateway 구성 유틸리티에서 Secure Ticket Authority(STA)를 구성하고 정책을 가상 서버에 바인딩해야 합니다. 기본값은 비어 있으며, 이는 대체 게이트웨이가 없음을 의미합니다.

이 정책을 구성하는 경우 네트워크 액세스 정책을 **내부 네트워크로 터널링됨**으로 설정합니다. 이 정책은 네트워크 액세스 정책을 구성할 때 적용됩니다. Exchange Server가 내부 네트워크에 있고 Citrix Gateway를 사용하여 내부 Exchange Server에 대한 연결을 프록시하려는 경우 이 정책을 사용하십시오.

연락처 내보내기

중요:

사용자가 Exchange Server에 직접(즉, Citrix Gateway 외부에서) 액세스할 수 있는 경우 이 기능을 활성화하지 마십시오. 그렇지 않으면 장치와 Exchange에 중복 연락처가 생성됩니다.

끔으로 설정하면 Secure Mail 연락처가 장치로 단방향 동기화되는 것과 Secure Mail 연락처를 (vCard로) 공유하는 것을 방지합니다. 기본값은 **끔**입니다.

내보낼 연락처 필드

주소록으로 내보낼 연락처 필드를 제어합니다. **모두**로 설정하면 모든 연락처 필드가 내보내집니다. **이름 및 전화**로 설정하면 이름 및 전화 관련 연락처 필드가 모두 내보내집니다. **이름, 전화 및 이메일**로 설정하면 이름, 전화 및 이메일 관련 연락처 필드가 모두 내보내집니다.

기본값은 **모두**입니다.

모든 SSL 인증서 허용

켜짐으로 설정하면 Secure Mail이 모든 SSL 인증서(유효 여부와 관계없이)를 수락하고 액세스를 허용합니다. **끔**으로 설정하면 Secure Mail이 인증서 오류 발생 시 액세스를 차단하고 경고를 표시합니다.

기본값은 **끔**입니다.

잠금 화면 알림 제어

잠긴 장치 화면에 메일 및 캘린더 알림이 표시되는지 여부를 제어합니다. **허용**으로 설정하면 알림에 포함된 모든 정보가 표시됩니다. **차단**으로 설정하면 알림이 표시되지 않습니다. **이메일 보낸 사람 또는 이벤트 제목**으로 설정하면 이메일 보낸 사람의 이름 또는 캘린더 이벤트의 제목만 표시됩니다. **개수만**으로 설정하면 메일 및 회의 초대 개수와 캘린더 미리 알림 시간이 표시됩니다. 기본값은 **허용**입니다.

기본 이메일 알림

켜짐으로 설정하면 Secure Mail은 이메일에 대한 잠금 화면 알림을 표시합니다. 기본값은 **켜짐**입니다.

기본 동기화 간격

Secure Mail의 기본 동기화 간격을 지정합니다. Secure Mail 사용자는 기본값을 변경할 수 있습니다.

Exchange ActiveSync mailbox 정책 설정인 **Maximum email age filter**가 이 정책보다 우선합니다. Maximum email age filter보다 큰 기본 동기화 간격을 지정하면 **Maximum email age filter** 설정이 대신 사용됩니다.

Secure Mail은 **Active Sync Maximum email age filter** 설정보다 작은 동기화 간격 값만 표시합니다.

기본값은 **3일**입니다.

메일 검색 제한

메일 서버 검색에 포함되는 일수를 제한하여 모바일 장치에서 액세스할 수 있는 메일 기록의 양을 제한합니다. 기본값은 **무제한**입니다.

모바일 장치에 동기화되는 메일의 양을 제한하려면 Maximum client sync period policy를 구성하십시오.

최대 동기화 간격

동기화 기간을 제한하여 모바일 장치에 로컬로 저장되는 메일의 양을 제어합니다. 기본값은 **모두**입니다. 장치가 메일 서버에서 검색할 수 있는 기간을 제한하려면 Mail server search limit policy를 구성하십시오.

주 번호 사용

켜짐으로 설정하면 달력 보기에 주 번호가 포함됩니다. 기본값은 **꺼짐**입니다.

Wi-Fi를 통한 첨부 파일 다운로드 사용

켜짐으로 설정하면 Secure Mail Download attachments option이 활성화되어 사용자가 기본적으로 허용된 내부 Wi-Fi 네트워크를 통해 첨부 파일을 다운로드할 수 있습니다. **꺼짐**으로 설정하면 Secure Mail Download attachments option이 비활성화되어 사용자가 기본적으로 Wi-Fi를 통해 첨부 파일을 다운로드할 수 없습니다.

기본값은 **끔**입니다.

오프라인 문서 허용

사용자가 장치에 오프라인 문서를 저장할 수 있는지 여부와 저장 기간을 지정합니다. 기본값은 **무제한**입니다.

정보 권한 관리

켄으로 설정하면 Secure Mail은 Exchange 정보 권한 관리(IRM) 기능을 지원합니다. 기본값은 **끔**입니다.

이메일 분류

켄으로 설정하면 Secure Mail은 SEC(보안) 및 DLM(배포 제한 마커)에 대한 이메일 분류 표시를 지원합니다. 분류 표시는 이메일 헤더에 "X-Protective-Marking" 값으로 나타납니다. 관련 이메일 분류 정책을 구성해야 합니다.

기본값은 **끔**입니다.

이메일 분류 표시

사용자가 사용할 수 있는 분류 표시를 지정합니다. 목록이 비어 있으면 Secure Mail은 보호 표시 목록을 포함하지 않습니다. 표시 목록에는 세미콜론으로 구분된 값 쌍이 포함됩니다. 각 쌍에는 Secure Mail에 나타나는 값과 Secure Mail의 이메일 제목 및 헤더에 추가되는 표시 값 텍스트가 포함됩니다. 예를 들어, 표시 쌍 "UNOFFICIAL,SEC=UNOFFICIAL;"에서 목록 값은 "UNOFFICIAL"이고 표시 값은 "SEC=UNOFFICIAL"입니다.

이메일 분류 네임스페이스

사용된 분류 표준에 따라 이메일 헤더에 필요한 분류 네임스페이스를 지정합니다. 예를 들어, 네임스페이스 "gov.au"는 헤더에 "NS=gov.au"로 나타납니다.

기본값은 비어 있습니다.

이메일 분류 버전

사용된 분류 표준에 따라 이메일 헤더에 필요한 분류 버전을 지정합니다. 예를 들어, 버전 "2012.3"은 헤더에 "VER=2012.3"으로 나타냅니다.

기본값은 비어 있습니다.

기본 이메일 분류

사용자가 마킹을 선택하지 않을 경우 Secure Mail이 이메일에 적용하는 보호 마킹을 지정합니다. 이 값은 이메일 분류 마킹 정책 목록에 있어야 합니다.

기본값은 **UNOFFICIAL**입니다.

이메일 초안 자동 저장 사용

켜짐으로 설정하면 Secure Mail은 메시지를 **초안** 폴더에 자동으로 저장하는 것을 지원합니다.

기본값은 **켜짐**입니다.

초기 인증 메커니즘

이 정책은 MDX에서 제공하는 메일 서버 주소 또는 사용자의 이메일 주소를 사용하여 최초 사용 프로비저닝 화면의 "주소" 필드를 채워야 하는지 여부를 나타냅니다.

기본값은 ****"메일 서버 주소"***입니다.

초기 인증 자격 증명

이 정책은 초기 최초 사용 프로비저닝 화면에 채울 사용자 이름으로 선택해야 하는 값을 정의합니다.

기본값은 ****"등록 사용자 이름"***입니다.

사용자 이름 자동 채우기 사용

활성화된 경우 사용자 이름이 계정 프로비저닝 사용자 인터페이스에 자동으로 채워집니다. 기본값은 **ON**입니다.

iOS 데이터 보호 사용

참고:

이 정책은 호주 신호국(ASD) 컴퓨터 보안 요구 사항을 충족해야 하는 기업을 위한 것입니다.

파일 작업 시 iOS 데이터 보호를 사용하도록 설정합니다. **켜짐**으로 설정하면 앱 샌드박스에서 파일을 생성하고 열 때 파일 보호 수준을 지정합니다. 기본값은 **꺼짐**입니다.

푸시 알림 EWS 호스트 이름

메일용 EWS(Exchange Web Services)를 호스팅하는 서버입니다. 값은 포트 번호와 함께 EWS의 URL이어야 합니다. 기본값은 비어 있습니다.

푸시 알림

사서함 활동에 대한 APN 기반 알림을 사용하도록 설정합니다. **켜짐**으로 설정하면 Secure Mail이 푸시 알림을 지원합니다.

기본값은 **꺼짐**입니다.

푸시 알림 지역

Secure Mail 사용자를 위한 APN 호스트가 위치한 지역입니다. 옵션은 **미주**, **EMEA**, **APAC**입니다. 기본값은 **미주**입니다.

S/MIME 공개 인증서 원본

S/MIME 인증서의 원본을 지정합니다. **이메일**로 설정하면 사용자 인증서를 사용자에게 이메일로 보내야 하며, 사용자는 Secure Mail에서 이메일을 열고 첨부된 인증서를 가져옵니다.

공유 저장소로 설정하면 지원되는 디지털 ID 공급자가 Secure App 공유 저장소에 인증서를 제공합니다. 타사 공급자와의 통합을 위해서는 관련 앱을 사용자에게 게시해야 합니다. 사용자 경험에 대한 자세한 내용은 Secure Mail 첫 시작 시 S/MIME 사용 정책에 대한 설명을 참조하십시오.

기본값은 **이메일**입니다.

Secure Mail 첫 시작 시 S/MIME 활성화

S/MIME 인증서 소스 정책이 **공유 저장소**인 경우, Secure Mail이 첫 시작 시 S/MIME를 활성화할지 여부를 결정합니다. **켜짐**으로 설정하면, 공유 저장소에 사용자의 인증서가 있는 경우 Secure Mail이 S/MIME를 활성화합니다. 공유 저장소에 인증서가 없으면 사용자에게 인증서 가져오기를 요청합니다. 두 시나리오 모두에서 사용자는 Secure Mail에서 계정을 생성하기 전에 지원되는 디지털 ID 공급자 앱에서 인증서를 구성해야 합니다.

꺼짐으로 설정하면 Secure Mail은 S/MIME를 활성화하지 않으며, 사용자가 Secure Mail 설정에서 활성화할 수 있습니다. 기본값은 **꺼짐**입니다.

캘린더 웹 및 오디오 옵션

- **GoToMeeting 및 사용자 입력:** 사용자는 설정하려는 회의 유형을 선택할 수 있습니다. 옵션에는 GoToMeeting 페이지를 여는 **GoToMeeting**과 사용자가 회의 정보를 수동으로 입력할 수 있는 **기타 회의**가 있습니다.
- **사용자 입력 전용:** 사용자는 회의 정보를 수동으로 입력할 수 있는 기타 회의 페이지로 직접 이동합니다.

S/MIME 공개 인증서 소스

S/MIME 공개 인증서의 소스를 지정합니다. **Exchange**인 경우 Secure Mail은 Exchange Server에서 인증서를 가져옵니다. **LDAP**인 경우 Secure Mail은 LDAP 서버에서 인증서를 가져옵니다. 기본값은 **Exchange**입니다.

LDAP 서버 주소

포트 번호를 포함한 LDAP 서버 주소입니다. 기본값은 비어 있습니다.

LDAP 기본 DN

LDAP 기본 고유 이름입니다. 기본값은 비어 있습니다.

LDAP 익명 액세스

이 정책이 **켜짐**으로 설정된 경우 Secure Mail은 사전 인증 없이 LDAP를 검색할 수 있습니다. 기본값은 **꺼짐**입니다.

허용된 이메일 도메인

server.company.com,server.company.co.uk와 같이 쉼표로 구분된 형식으로 허용되는 이메일 도메인 목록을 정의합니다. 기본값은 비어 있으며, 이는 Secure Mail이 이메일 도메인을 필터링하지 않고 모든 이메일 도메인을 지원함을 의미합니다. Secure Mail은 나열된 도메인을 이메일 주소의 도메인 이름과 일치시킵니다. 예를 들어, server.company.com이 나열된 도메인 이름이고 이메일 주소가 user@internal.server.company.com인 경우 Secure Mail은 해당 이메일 주소를 지원합니다.

인증 실패 시 사용자 이름 마이그레이션 시도

인증을 위해 Exchange 사용자 이름을 UPN으로 마이그레이션하려고 시도합니다. 기본값은 **해제**입니다.

피싱 메일 주소 보고

구성된 경우, 의심스러운 피싱 메일을 지정된 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록으로 보고할 수 있습니다. 기본값은 비어 있습니다. 이 정책을 구성하지 않으면 피싱 메시지를 보고할 수 없습니다.

피싱 보고 메커니즘

이 정책은 의심스러운 피싱 메일을 보고하는 데 사용되는 메커니즘을 나타냅니다.

- **첨부 파일로 보고:** 피싱 메일을 첨부 파일로 보고합니다. 첨부 파일은 피싱 메일 주소 보고 정책에 구성된 이메일 주소 또는 심표로 구분된 이메일 주소 목록으로 전송됩니다.
- **전달로 보고:** 피싱 메일을 전달로 보고합니다. 메일은 피싱 메일 주소 보고 정책에 구성된 이메일 주소 또는 심표로 구분된 이메일 주소 목록으로 전달됩니다.

참고:

이 정책은 Microsoft Exchange Server에서만 사용할 수 있습니다.

기본값은 **첨부 파일로 보고**입니다.

비즈니스용 Skype 모임 도메인

이 정책에는 비즈니스용 Skype 모임에 사용되는 심표로 구분된 도메인 목록이 포함되어 있습니다.

Secure Mail은 이미 다음 URL 접두사를 가진 모임을 처리합니다.

- `https://join`
- `https://meet`
- `https://lync`

이 정책을 사용하면 다른 Skype for Business 도메인을 `https://*domain*` 형식으로 추가할 수 있습니다. 도메인은 영숫자 문자열이어야 하며 특수 문자를 포함할 수 없습니다. 선행 `https://` 또는 후행 점을 입력하지 마십시오.

예:

정책 값이 **customDomain1,customDomain2**인 경우 Skype for Business에 지원되는 URL 접두사는 다음과 같습니다.

- `https://customDomain1`
- `http://customDomain1`
- `https://customDomain2`
- `http://customDomain2`

기본값은 비어 있습니다.

캘린더 내보내기

이 정책을 사용하면 Secure Mail 캘린더 이벤트를 장치 또는 개인 캘린더로 내보낼 수 있습니다. 개인 캘린더에서 이벤트를 볼 수 있습니다. Secure Mail을 사용하여 이벤트를 편집할 수 있습니다. 기본값은 **회의 시간**입니다.

개인 캘린더에 표시되는 캘린더 이벤트 필드에 사용할 수 있는 MDX 정책 값은 다음과 같습니다.

- 없음 (내보내지 않음)
- 회의 시간
- 회의 시간, 위치
- 회의 시간, 제목, 위치
- 회의 시간, 제목, 위치, 메모

발신자 식별

켄으로 설정하면 Secure Mail은 발신자 식별을 위해 저장된 연락처의 이름과 연락처 번호를 iOS에 제공합니다. 이 데이터는 저장된 Secure Mail 연락처 목록에서 걸려오는 전화의 세부 정보를 식별하고 표시하는 데만 사용됩니다. 기본값은 **켄**입니다.

Office 365용 OAuth 지원

Office 365 인증 메커니즘

이 정책은 Office 365에서 계정을 구성할 때 인증에 사용되는 OAuth 메커니즘을 나타냅니다.

- **OAuth 사용 안 함:** OAuth는 사용되지 않으며 Secure Mail은 계정 구성을 위해 기본 인증을 사용합니다.
- **사용자 이름 및 암호로 OAuth 사용:** 사용자는 OAuth 흐름을 위해 사용자 이름과 암호, 그리고 선택적으로 MFA 코드를 제공해야 합니다.
- **클라이언트 인증서로 OAuth 사용:** 사용자는 클라이언트 인증서를 사용하여 OAuth 흐름을 인증합니다.

기본값은 *****OAuth 사용 안 함*****입니다.

신뢰할 수 있는 Exchange Online 호스트 이름

계정을 구성할 때 인증을 위해 OAuth 메커니즘을 사용하는 신뢰할 수 있는 Exchange Online 호스트 이름 목록을 정의합니다. 이 값은 server.company.com, server.company.co.uk와 같은 쉼표로 구분된 형식입니다. 목록이 비어 있으면 Secure Mail은 계정 구성을 위해 기본 인증을 사용합니다. 기본값은 **outlook.office365.com**입니다.

신뢰할 수 있는 AD FS 호스트 이름

Office 365 OAuth 인증 중에 암호가 채워지는 웹 페이지에 대한 신뢰할 수 있는 AD FS 호스트 이름 목록을 정의합니다. 이 값은 sts.companyname.com, sts.company.co.uk와 같이 쉼표로 구분된 형식입니다. 목록이 비어 있으면 Secure Mail은 암호를 자동으로 채우지 않습니다. Secure Mail은 나열된 호스트 이름을 Office 365 인증 중에 발견된 웹 페이지의 호스트 이름과 일치시키고 페이지가 HTTPS 프로토콜을 사용하는지 확인합니다. 예를 들어, sts.company.com이 나열된 호스트 이름이고 사용자가 `https://sts.company.com`으로 이동하는 경우, 페이지에 암호 필드가 있으면 Secure Mail이 암호를 채웁니다. 기본값은 **login.microsoftonline.com**입니다.

메일 리디렉션

메일 리디렉션

메일 작성을 차단하거나 제한합니다. Secure Mail은 메일 작성을 Secure Mail로 리디렉션합니다. 계정이 설정된 경우 기본 메일은 메일 작성을 기본 메일로 리디렉션합니다. 기본값은 **Secure Mail**입니다.

Slack 통합

Slack 사용

Slack 통합을 차단하거나 허용합니다. **ON**인 경우 Secure Mail 인터페이스에 Slack 기능이 포함됩니다. **OFF**인 경우 Secure Mail 인터페이스에 Slack 기능이 포함되지 않습니다. 기본값은 **OFF**입니다.

Slack 작업 공간 이름

회사에 대한 Slack 작업 공간 이름입니다. 이름을 제공하면 Secure Mail이 로그인 중에 작업 공간 이름을 미리 채웁니다. 이름을 제공하지 않으면 사용자가 작업 공간 이름(name.slack.com)을 입력해야 합니다. 기본값은 비어 있습니다.

플랫폼별 기능

다음 표는 Citrix 모바일 생산성 앱의 기능을 요약한 것입니다. **X**는 해당 플랫폼에서 기능을 사용할 수 있음을 나타냅니다. QuickEdit의 기능에 대해서는 [Citrix QuickEdit](#)을 참조하십시오.

시트릭스 시큐어 허브™

기능	IOS	안드로이드
인증을 위해 로그인	X	X
정책 준수 모니터링	X	X
앱 및 데스크톱 액세스	X	X
HDX™ 앱 및 데스크톱	X	X
문제 로그 생성 및 전송	X	X
로그에 스크린샷 첨부	X	X
앱 내에서 헬프 데스크에 문의	X	X
앱 내에서 Citrix® 지원팀에 문의	X	X
크래시 수집 및 분석	X	X
오프라인 인증	X	X
Citrix Secure Mail™로 로그 전송	X	X
구글 애널리틱스	X	X
세로 및 가로 모드	X	X
앱 신뢰를 위한 인앱 가이드	X	X

기능	IOS	안드로이드
이메일로 등록 시 Secure Mail 에 자동 등록 (MAM 전용)	X	X
Touch ID 오프라인 인증	X	X
파생 자격 증명으로 등록	X	
생체 인증		X
Workspace 앱 스토어 사용	X	X

시트릭스 보안 메일

기능	IOS	안드로이드
이메일 생산성		
초안 최소화	X	X
보낸 메일 취소		X
암호화 관리	X	X
캘린더 일정 위젯		X
Secure Mail의 연락처 사진	X	X
반응형 이메일 지원	X	X
초안 폴더 자동 동기화	X	X
초안 폴더의 첨부 파일 동기화		X
메일 보내기, 받기, 회신, 전체 회신, 전달	X	X
초안 생성, 편집, 삭제	X	X
메일 플래그 지정	X	X
읽지 않은 상태로 표시	X	X

기능	IOS	안드로이드
모든 폴더 및 하위 폴더 보기	X	X
앱이 백그라운드에 있을 때 초안 자동 저장	X	X
Citrix Secure Notes를 사용한 이메일-메모 변환. 중요: Secure Notes는 December 31, 2018 에 EOL(End of Life) 상태에 도달했습니다. 자세한 내용은 EOL 및 사용 중단된 앱을 참조하십시오 .	X	X
메일 검색(로컬 및 서버)	X	X
메일 동기화 기간 선택(최대 1개 월 또는 모든 메일)	X	X
읽지 않은 메일 보기	X	X
이미지, 비디오 및 오디오의 보안 첨부 파일 보기/재생	X	X
여러 첨부 파일	X	X
첨부 파일 회신 및 전달	X	X
Citrix Files에서 파일 첨부	X	X
Citrix Files 제한 구역 및 커넥터에서 파일 첨부	X	X
첨부 파일 저장소	X	X
서식 있는 텍스트 편집	X	X
잠금 화면에서 제목 및 미리보기가 포함된 메일 알림	X	X
알림 화면에서 메일 및 초대 회신 및 삭제	X	

기능	IOS	안드로이드
사진 첨부 또는 촬영	X	X
여러 메시지 선택	X	X
첨부 파일 다운로드	X	X
인라인 이미지 로드	X	X
빠른 정렬	X	X
.zip 파일 첨부 파일 보내기, 받기, 열기 및 저장	X	X
세로 및 가로 모드	X; 메일 목록, 메일 읽기, 작성, 캘린더 및 연락처 보기 전반	X: 메일 읽기 및 작성 보기 전용
붙여넣은 텍스트는 서식을 유지합니다	X	X
연락처에서 SMS	X	X
연락처에서 FaceTime	X	
연결 문제 또는 사서함 용량 초과로 인해 전송되지 않은 메시지가 보낼 편지함에 저장됨	X	X
최근 폴더 표시		X
아래로 당겨 메일 새로 고침	X	X
마지막 새로 고침 타임스탬프	X	X
메시지 작업에 대한 왼쪽 스와이프	X	X
마이크로소프트 익스체인지 및 IBM 노트스 트래블러 지원	X	X
탭하여 메일, 캘린더 및 연락처 새로 고침	X	X

기능	IOS	안드로이드
메일 보기에서 장치 접근성/글꼴 크기 설정 준수	X	X
S/MIME 서명 및 암호화	X	X
이메일을 통한 S/MIME 인증서 가져오기	X	X
S/MIME, Intercede 통합	X	
S/MIME, Entrust 통합	X	
메시지 본문에 대한 Microsoft IRM 보호	X	X
푸시 알림	X	X
받은 편지함으로 푸시 알림을 보내면 캘린더를 포함한 모든 폴더가 자동으로 업데이트됩니다.	X	
Office 365 문서 열기	X	X
3D Touch 동작	X	
잠금 화면의 상황별 아이콘	X	X
폴더 검색	X	X
VIP 메일 폴더	X	X
동적 유형 지원	X	X
확장된 폴더 유지	X	X
메시지 분류 마커	X	X
맞춤법 검사	X	
마지막으로 찍은 사진 첨부	X	X
URL 미리 보기	X	X

기능	IOS	안드로이드
Citrix Files에서 Citrix Files 링크 열기	X	X
<code>.pass</code> 파일 지원	X	
검색 모드에서 여러 이메일 선택	X	X
이미지 인라인 삽입	X	X
Exchange ActiveSync (EAS) 버전 16으로 업그레이드	X	X
사용자가 알 수 없거나 개인 도메인을 사용하지 못하도록 제한	X	
초광폭 장치 화면 지원		X
여러 Exchange 계정 구성	X	X
더 많은 작업을 위해 왼쪽 또는 오른쪽으로 스와이프	X	X
암호화된 메일에 대한 회신 또는 전달 암호화	X	
이메일 및 인라인 이미지 인쇄	X	
설정에서 미리 보기 줄을 사용하여 사서함 보기에서 이메일 본문의 몇 줄이 미리 보기로 표시되는지 구성합니다.	X	
반응형 이메일 지원	X	X
첨부 파일(MS Office 또는 이미지)의 앱 내 미리 보기	X	X
개인 연락처 그룹	X	X
사용자 이름을 이메일 주소(UPN)로 마이그레이션	X	X

기능	IOS	안드로이드
피싱 이메일 보고	X	X
최신 인증 (OAuth)	X	X
첨부 파일 인쇄	X	
안드로이드 엔터프라이즈 (Android for Work)	X	
서식 있는 텍스트 서명	X	
서식 있는 푸시 알림	X	
피드	X	X
사진 첨부 개선	X	X
그룹 알림	X	
Slack 통합 (미리 보기)	X	X
피드 관리	X	
내부 도메인	X	X
피드 관리	X	X
MS Teams 통합	X	X
자가 진단 (문제 해결) 옵션		X
듀얼 모드 (MAM SDK)	X	X
자가 진단 도구		X
캘린더		
ICS 파일을 캘린더 이벤트로 미리 보고 가져오기		X
캘린더 이벤트 끌어서 놓기	X	X

기능	IOS	안드로이드
일, 주, 월 및 일정 보기	X	X
잠금 화면의 상세 알림	X	X
6개월 동기화	X	X
이벤트를 비공개로 설정	X	X
첫 번째 이벤트 한 시간 전으로 스크롤	X	
수동 새로 고침 옵션	X	X
알림 설정	X	X
탭하여 주소 매핑	X	X
주 번호	X	X
동적 유형 지원	X	X
보안 분류 마커	X	X
주소 길게 누르기	X	
주간 근무 시작일 설정	X	X
선택한 날짜 주 보기 집중	X	
현재 날짜 항상 강조 표시	X	X
첨부 파일 저장소의 캘린더 첨부 파일	X	X
개인 캘린더 지원	X	X
개인 캘린더 이벤트와의 충돌 표시		X
캘린더 이벤트 인쇄	X	

기능	IOS	안드로이드
캘린더 제목 줄에서 전화번호 및 웹 주소 탭	X	
캘린더 검색	X	
회의		
회의 회신, 전체 회신, 전달	X	X
초대 응답에 대한 주최자 보기	X	X
초대 대상자의 사용 가능 여부 및 제안된 사용 가능 여부에 대한 주최자 보기	X	X
탭하여 온라인 회의에 참여합니다. 참고: WebEx 및 Lync의 경우, 이러한 앱을 사용하려면 Citrix Endpoint Management™에서 정책을 구성해야 합니다.	X	X
탭하여 오디오 회의에 참여	X	X
새로운 초대에서 온라인 회의, 오디오, 컨퍼런스 예약	X	X
새로운 초대에 ShareFile 링크 추가	X	X
첨부 파일과 함께 초대 전달	X	X
"늦습니다" 이메일 전송을 위해 탭	X	X
회의 주최자에게 회신하려면 탭	X	X
모든 회의 초대에 회신하려면 탭	X	X
모든 회의 초대 대상자에게 회신하려면 탭	X	X

기능	IOS	안드로이드
첨부 파일과 함께 모든 회의 초대 대상자에게 회신하려면 탭	X	X
GoToMeeting으로 전화 걸기	X	X
잠금 화면 또는 알림 화면에서 초대에 응답	X	X
WebEx 또는 Lync 회의에 전화 접속	X	X
거절된 이벤트 숨기기	X	X
3개 이상의 동시 이벤트 표시	X	X
초대자 상태 빠른 보기	X	X
취소된 이벤트 삭제, 회신, 전체 회신, 댓글 추가	X	X
전달된 초대에 주최자 이름 표시	X	X
공유 장치	X	X
비즈니스용 Skype 모임 참가	X	X
수락, 거절, 미정 등 모임 알림에 응답합니다.	X	X
회신 및 삭제로 메시지 알림에 응답	X	
연락처		
연락처에 폴더 생성		X
양방향 연락처 동기화	X	X
자세한 연락처 정보 GAL 검색	X	X
Secure Mail 연락처를 로컬 연락처로 내보내고 동기화	X	X

기능	IOS	안드로이드
연락처: 즐겨찾기 및 범주		X
내보낼 연락처 필드 제어	X	X
보안 메일이 아닌 연락처 세부 정보	X	X
동적 유형 지원	X	X
연락처를 VIP로 표시	X	X
.vcards 과(와) 연락처 공유	X	X
길게 눌러 연락처 보기		X
기본 메일 계정이 있어도 연락처 내보내기	X	X
폴더 및 하위 폴더 보기	X	
장치에 구성된 설정		
iMessage 지원	X	
알림 제어를 위한 고급 옵션	X	X
잠금 화면 알림 제어	X	X
메일 및 캘린더 알림 소리	X	X
폴더 자동 새로 고침	X	X
내부 및 외부 부재중 알림 설정	X	X
삭제 전 확인	X	X
스레드 대화 또는 시간순 보기	X	X
Wi-Fi에서 첨부 파일 로드	X	X
Wi-Fi에서 첨부 파일 로드를 기본 값으로 설정	X	X

기능	IOS	안드로이드
메일 동기화 기간 설정	X	X
무제한 동기화/모든 메일 동기화		X
이메일 서명 설정	X	X
연락처를 이름 또는 성으로 나열	X	X
자동 진행	X	X
홈 시간대 사용		X
빠른 응답 템플릿		X
푸시 메일 구성 빈도		X
설정 내보내기/가져오기	X	X
장치의 뒤로 가기 버튼을 탭하여 플로팅 작업 버튼 옵션을 닫습니다.		X
마이크로소프트 팀즈	X	X

시트릭스 시큐어 웹™

기능	IOS	안드로이드
멀티태스킹으로 두 개의 앱을 동시에 사용	X	
파일 다운로드	X	X
즐거찾기 추가	X	X
저장된 사용자 이름 및 암호 지우기	X	X
캐시/기록/쿠키 삭제	X	X
팝업 차단	X	X

기능	IOS	안드로이드
오프라인 페이지 저장	X	X
주소 표시줄에서 검색	X	X
알림에서 다운로드한 항목 열기	X	X
암호 자동 저장	X	X
프록시 지원		
엔터프라이즈 프록시	X	X
URL 차단 목록 및 허용 목록	X	X
기록	X	X
기본 홈페이지	X	X
탭	X	X
북마크 푸시	X	X
화면 캡처 차단		X
현재 페이지에서 검색	X	X
3D Touch 동작	X	
공유 장치	X	X
공유 장치를 통한 파일 변조 방지	X	
설정 내보내기/가져오기	X	X
세로 및 가로 모드	X	X
안드로이드 엔터프라이즈 (Android for Work)		X
화면의 콘텐츠를 당겨서 새로 고 침	X	X

기능	IOS	안드로이드
Secure Web을 기본 브라우저로		X

기능 플래그 관리

기능 플래그가 적용된 기능의 최적 작동을 보장하려면 `features.netscalergateway.net` URL로 트래픽을 활성화해야 합니다.

기능 플래그는 기능을 동적으로 활성화하거나 비활성화하는 데 사용됩니다. 프로덕션 환경에서 모바일 생산성 앱에 문제가 발생하면 기능이 출시된 후에도 해당 기능을 동적으로 비활성화할 수 있습니다. 이를 위해 Citrix에서 관리하는 기능 플래그를 사용합니다.

아웃바운드 트래픽을 차단하는 방화벽 또는 프록시가 있는 경우를 제외하고는 기능 관리 트래픽을 활성화하기 위해 수동 구성이 필요하지 않습니다. 이 경우 정책 요구 사항에 따라 특정 URL 또는 IP 주소를 사용하여 트래픽을 활성화해야 합니다.

IP 주소

허용 목록에 IP 주소를 나열해야 하는 경우, `features.netscalergateway.net` 으로의 트래픽을 허용하려면 다음 IP 주소를 포함하십시오.

- 57.153.121.183 (유럽 서부 지역용)
- 172.202.161.151 (미국 남중부 지역용)
- 48.218.128.128 (일본 동부 지역용)

이러한 IP 주소를 추가하여 인프라 업데이트에 따라 방화벽 구성이 자동으로 업데이트되도록 할 수 있습니다.

시스템 요구 사항

스플릿 터널링이 **OFF**로 설정된 NetScaler Gateway를 사용하는 경우, NetScaler가 포트 443을 통해 `features.netscalergateway.net` 을 확인하고 연결할 수 있는지 확인하십시오.

다음 표는 기능 플래그 관리를 지원하는 모바일 생산성 앱의 최소 버전을 나열합니다.

모바일 생산성 앱	운영 체제	지원되는 최소 버전
시큐어 허브	안드로이드	24.8.0 이상
시큐어 허브	iOS	24.9.0 이상

모바일 생산성 앱	운영 체제	지원되는 최소 버전
MAM SDK	안드로이드	24.9.0 이상
MAM SDK	iOS	24.7.1 이상
시큐어 메일	안드로이드, iOS	24.9.0 이상
보안 웹	안드로이드	24.8.0 이상
보안 웹	iOS	24.9.0 이상

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.

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

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.

Secure Mail 개요

Citrix Secure Mail™을 통해 사용자는 모바일 폰과 태블릿에서 이메일, 캘린더 및 연락처를 관리할 수 있습니다. Microsoft Outlook 또는 IBM Notes 계정과의 연속성을 유지하기 위해 Secure Mail은 Microsoft Exchange Server 및 IBM Notes Traveler Server와 동기화됩니다.

Citrix 앱 제품군의 일부인 Secure Mail은 Citrix Secure Hub와의 단일 Sign-On(SSO) 호환성 이점을 제공합니다. 사용자가 Secure Hub에 로그인하면 사용자 이름과 암호를 다시 입력할 필요 없이 Secure Mail로 원활하게 이동할 수 있습니다. 장치가 Secure Hub에 등록될 때 Secure Mail이 사용자 장치로 자동으로 푸시되도록 구성하거나, 사용자가 Store에서 앱을 추가할 수 있습니다.

참고:

- Exchange Server 2010에 대한 지원은 October 13, 2020에 종료되었습니다.
- Exchange Server 2013에 대한 지원은 April 11, 2023에 종료되었습니다.

Secure Mail은 다음을 지원합니다:

- 익스체인지 서버 SE RTM
- Exchange Server 2019 누적 업데이트 15
- Exchange Server 2019 누적 업데이트 14
- Exchange Server 2019 누적 업데이트 13
- Exchange Server 2019 누적 업데이트 12
- Exchange Server 2019 누적 업데이트 11
- Exchange Server 2019 누적 업데이트 10
- Exchange Server 2019 누적 업데이트 9
- Exchange Server 2019 누적 업데이트 8
- Exchange Server 2019 누적 업데이트 7
- Exchange Server 2019 누적 업데이트 6
- Exchange Server 2016 누적 업데이트 23

- Exchange Server 2016 누적 업데이트 22
- Exchange Server 2016 누적 업데이트 21
- Exchange Server 2016 누적 업데이트 20
- Exchange Server 2016 누적 업데이트 19
- Exchange Server 2016 누적 업데이트 18
- Exchange Server 2016 누적 업데이트 17
- HCL Domino 버전 14.0 FP1
- HCL Domino 버전 12.0.2 FP2
- HCL Traveler 버전 12.0.2.1 빌드 202302010413_30
- HCL Domino 11 (이전 이름: Lotus Notes)
- HCL Domino 10.0.1 (이전 이름: Lotus Notes)
- HCL 도미노 9.0.1 FP10 HF197 (구 로터스 노트)
- HCL 도미노 10.0.1.0 빌드 201811191126_20 (구 로터스 노트)
- HCL 도미노 9.0.1.21 (구 로터스 노트)
- 마이크로소프트 오피스 365 (익스체인지 온라인)

시작하려면 [Citrix Endpoint Management 다운로드](#)에서 Secure Mail 및 기타 Endpoint Management 구성 요소를 다운로드하십시오.

Secure Mail 및 기타 모바일 앱 시스템 요구 사항은 [시스템 요구 사항을\(를\)](#) 참조하십시오.

앱이 백그라운드에서 실행 중이거나 닫혀 있을 때 iOS 및 Android용 Secure Mail의 알림에 대한 자세한 내용은 [Secure Mail용 푸시 알림을\(를\)](#) 참조하십시오.

Secure Mail에서 지원되는 iOS 기능은 [Secure Mail용 iOS 기능을\(를\)](#) 참조하십시오.

Secure Mail에서 지원되는 Android 기능은 [Secure Mail용 Android 기능을\(를\)](#) 참조하십시오.

Secure Mail에서 지원되는 iOS 및 Android 기능은 [Secure Mail용 iOS 및 Android 기능을\(를\)](#) 참조하십시오.

사용자 도움말 설명서는 Citrix 사용자 도움말 센터의 [Citrix Secure Mail](#) 페이지를 참조하십시오.

시트릭스 시큐어 웹™

Citrix Secure Web은 내부 및 외부 사이트에 대한 보안 액세스를 제공하는 HTML5 호환 모바일 웹 브라우저입니다. Secure Hub에 장치가 등록되면 Secure Web이 사용자 장치로 자동으로 푸시되도록 구성할 수 있습니다. 또는 Endpoint Management 앱 스토어에서 앱을 추가할 수 있습니다.

Secure Web 및 기타 모바일 생산성 앱 시스템 요구 사항에 대한 자세한 내용은 [시스템 요구 사항](#)을 참조하십시오.

Secure Web 통합 및 제공

참고:

MDX Toolkit 10.7.10은 모바일 생산성 앱 래핑을 지원하는 최종 릴리스입니다. 사용자는 공용 앱 스토어에서 모바일 생산성 앱 버전 10.7.5 이상에 액세스합니다.

Secure Web을 통합하고 제공하려면 다음 일반 단계를 따르십시오.

1. 내부 네트워크에 대한 Single sign-on(SSO)을 사용하도록 설정하려면 Citrix Gateway를 구성하십시오.

HTTP 트래픽의 경우 Citrix ADC는 Citrix ADC에서 지원하는 모든 프록시 인증 유형에 대해 SSO를 제공할 수 있습니다. HTTPS 트래픽의 경우 웹 암호 캐싱 정책을 통해 Secure Web이 MDX를 통해 프록시 서버에 인증하고 SSO를 제공할 수 있습니다. MDX는 기본, 다이제스트 및 NTLM 프록시 인증만 지원합니다. 암호는 MDX를 사용하여 캐시되며 중요한 앱 데이터를 위한 보안 저장 영역인 Endpoint Management 공유 저장소에 저장됩니다. Citrix Gateway 구성에 대한 자세한 내용은 [Citrix Gateway](#)를 참조하십시오.

2. Secure Web을 다운로드합니다.
3. 내부 네트워크에 대한 사용자 연결을 구성하는 방법을 결정합니다.
4. 다른 MDX 앱과 동일한 단계를 사용하여 Secure Web을 Endpoint Management에 추가한 다음 MDX 정책을 구성합니다. Secure Web에 특정한 정책에 대한 자세한 내용은 이 문서의 뒷부분에 있는 "Secure Web 정책 정보"를 참조하십시오.

사용자 연결 구성

Secure Web은 사용자 연결에 대해 다음 구성을 지원합니다.

- **터널링됨 – 웹 SSO:** 내부 네트워크로 터널링되는 연결은 터널링됨 – 웹 SSO라고 하는 클라이언트리스 VPN의 변형을 사용할 수 있습니다. 이는 **기본 VPN 모드** 정책에 지정된 기본 구성입니다. 터널링됨 – 웹 SSO는 Single sign-on(SSO)이 필요한 연결에 권장됩니다.
- **전체 VPN 터널:** 내부 네트워크로 터널링되는 연결은 **기본 VPN** 모드 정책으로 구성된 전체 VPN 터널을 사용할 수 있습니다. 전체 VPN 터널은 클라이언트 인증서 또는 내부 네트워크의 리소스에 대한 종단 간 SSL을 사용하는 연결에 권장됩니다. 그러나 Secure Web은 모바일 장치에 저장된 클라이언트 인증서를 읽을 수 있는 앱이 아닙니다. 이 기능을 제공할 수 있는 일부 타사 래핑된 엔터프라이즈 앱이 설치될 수 있습니다. 전체 VPN 터널은 TCP를 통한 모든 프로토콜을 처리하며 iOS 및 Android 장치 외에도 Windows 및 Mac 컴퓨터와 함께 사용할 수 있습니다.
- **VPN 모드 전환 허용** 정책은 필요에 따라 전체 VPN 터널과 터널링 – 웹 SSO 모드 간의 자동 전환을 허용합니다. 기본적으로 이 정책은 꺼져 있습니다. 이 정책이 켜져 있으면 기본 VPN 모드에서 처리할 수 없는 인증 요청으로 인해 실패한 네트워크 요청은 대체 모드에서 다시 시도됩니다. 예를 들어, 전체 VPN 터널 모드는 클라이언트 인증서에 대한 서버 챌린지를 수용하지만 터널링 – 웹 SSO 모드는 그렇지 않습니다. 마찬가지로, HTTP 인증 챌린지는 터널링 – 웹 SSO 모드를 사용할 때 SSO를 통해 서비스될 가능성이 더 높습니다.

다음 표는 구성 및 사이트 유형에 따라 Secure Web이 사용자에게 자격 증명을 요청하는지 여부를 나타냅니다.

연결 모드	사이트 유형	암호 캐싱	CITRIX GATEWAY용으로 구성된 SSO	SECURE WEB이 웹 사이트 첫 액세스 시 자격 증명 요청	SECURE WEB이 웹 사이트 후속 액세스 시 자격 증명 요청	SECURE WEB이 암호 변경 후 자격 증명 요청
터널링 – 웹 SSO	HTTP	아니요	예	아니요	아니요	아니요
터널링됨 – 웹 SSO	HTTPS	아니요	예	아니요	아니요	아니요
전체 VPN	HTTP	아니요	예	아니요	아니요	아니요
전체 VPN	HTTPS	예; Secure Web MDX 정책 '웹 암호 캐싱'	아니요	예; Secure Web에서 자격 증명	아니요	예

연결 모드	사이트 유형	암호 캐싱	CITRIX GATEWAY용으로 구성된 SSO	SECURE WEB이 웹 사이트 첫 액세스 시 자격 증명 요청	SECURE WEB이 웹 사이트 후속 액세스 시 자격 증명 요청	SECURE WEB이 암호 변경 후 자격 증명 요청
		호 캐싱 사용'이 켜져 있는 경우.		을 캐시하는 데 필요합니다.		

Secure Web 정책

Secure Web을 추가할 때 Secure Web에 특정한 다음 MDX 정책에 유의하십시오. 지원되는 모든 모바일 장치에 대해:

허용 또는 차단된 웹사이트

Secure Web은 일반적으로 웹 링크를 필터링하지 않습니다. 이 정책을 사용하여 허용되거나 차단된 사이트의 특정 목록을 구성할 수 있습니다. 브라우저가 열 수 있는 웹사이트를 제한하기 위해 심표로 구분된 목록 형식으로 URL 패턴을 구성합니다. 목록의 각 패턴 앞에는 더하기 기호(+) 또는 빼기 기호(-)가 붙습니다. 브라우저는 일치하는 항목을 찾을 때까지 나열된 순서대로 URL을 패턴과 비교합니다. 일치하는 항목이 발견되면 접두사가 다음과 같이 수행할 작업을 결정합니다.

- 빼기(-) 접두사는 브라우저가 URL을 차단하도록 지시합니다. 이 경우 URL은 웹 서버 주소를 확인할 수 없는 것처럼 처리됩니다.
- 더하기(+) 접두사는 URL이 정상적으로 처리되도록 허용합니다.
- 패턴에 + 또는 -가 제공되지 않으면 + (허용)로 간주됩니다.
- URL이 목록의 어떤 패턴과도 일치하지 않으면 URL이 허용됩니다.

다른 모든 URL을 차단하려면 목록을 빼기 기호 뒤에 별표(*)로 끝냅니다. 예를 들어:

- 정책 값 `+http://*.mycorp.com/*, -http://*, +https://*, +ftp://*, -*` 은 `mycorp.com` 도메인 내의 HTTP URL을 허용하지만 다른 곳에서는 차단하며, HTTPS 및 FTP URL은 어디에서나 허용하고, 다른 모든 URL은 차단합니다.
- 정책 값 `+http://*.training.lab/*, +https://*.training.lab/*, -*` 은 사용자가 HTTP 또는 HTTPS를 통해 Training.lab 도메인(인트라넷)의 모든 사이트를 열 수 있도록 허용합니다. 그러나 프로토콜에 관계없이 Facebook, Google, Hotmail과 같은 공용 URL은 열 수 없습니다.

기본값은 비어 있습니다(모든 URL 허용).

팝업 차단

팝업은 웹사이트가 사용자 허락 없이 여는 새 탭입니다. 이 정책은 Secure Web이 팝업을 허용할지 여부를 결정합니다. '켜짐'으로 설정하면 Secure Web은 웹사이트가 팝업을 여는 것을 방지합니다. 기본값은 '꺼짐'입니다.

미리 로드된 즐겨찾기

Secure Web 브라우저에 미리 로드된 즐겨찾기 세트를 정의합니다. 이 정책은 폴더 이름, 친숙한 이름 및 웹 주소를 포함하는 튜플의 심표로 구분된 목록입니다. 각 세 쌍은 folder, name, url 형식이어야 하며, 여기서 folder와 name은 선택적으로 큰따옴표(")로 묶을 수 있습니다.

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

기본값은 비어 있습니다.

홈 페이지 URL

Secure Web 시작 시 로드되는 웹사이트를 정의합니다. 기본값은 비어 있습니다(기본 시작 페이지).

지원되는 Android 및 iOS 장치에만 해당:

브라우저 사용자 인터페이스

Secure Web의 브라우저 사용자 인터페이스 컨트롤의 동작 및 가시성을 결정합니다. 일반적으로 모든 브라우저 컨트롤을 사용할 수 있습니다. 여기에는 앞으로, 뒤로, 주소 표시줄 및 새로 고침/중지 컨트롤이 포함됩니다. 이 정책을 구성하여 이러한 컨트롤 중 일부의 사용 및 가시성을 제한할 수 있습니다. 기본값은 모든 컨트롤을 표시합니다.

옵션

- 모든 컨트롤 표시. 모든 컨트롤이 표시되며 사용자는 이를 사용하는 데 제한을 받지 않습니다.
- 읽기 전용 주소 표시줄. 모든 컨트롤이 표시되지만, 사용자는 브라우저 주소 필드를 편집할 수 없습니다.
- 주소 표시줄 숨기기. 주소 표시줄은 숨기지만, 다른 컨트롤은 숨기지 않습니다.
- 모든 컨트롤 숨기기. 프레임 없는 브라우저 환경을 제공하기 위해 전체 도구 모음을 숨깁니다.

웹 암호 캐싱 사용

Secure Web 사용자가 웹 리소스에 액세스하거나 요청할 때 자격 증명을 입력하면, 이 정책은 Secure Web이 장치에 암호를 자동으로 캐시할지 여부를 결정합니다. 이 정책은 인증 대화 상자에 입력된 암호에 적용되며 웹 양식에 입력된 암호에는 적용되지 않습니다.

켜짐으로 설정하면 Secure Web은 사용자가 웹 리소스를 요청할 때 입력하는 모든 암호를 캐시합니다. **꺼짐**으로 설정하면 Secure Web은 암호를 캐시하지 않으며 기존 캐시된 암호를 제거합니다. 기본값은 **꺼짐**입니다.

이 정책은 Preferred VPN 정책을 이 앱에 대해 Full VPN tunnel로 설정한 경우에만 활성화됩니다.

프록시 서버

Tunneled – Web SSO 모드에서 Secure Web을 사용할 때 프록시 서버를 구성할 수도 있습니다. 자세한 내용은 이 [블로그 게시물](#)을 참조하십시오.

DNS 접미사

Android에서 DNS 접미사가 구성되지 않은 경우 VPN이 실패할 수 있습니다. DNS 접미사 구성에 대한 자세한 내용은 [Android 장치용 DNS 접미사를 사용하여 DNS 쿼리 지원](#)을 참조하십시오.

Secure Web용 인트라넷 사이트 준비

이 섹션은 Android 및 iOS용 Secure Web과 함께 사용할 인트라넷 사이트를 준비해야 하는 웹 사이트 개발자를 위한 것입니다. 데스크톱 브라우저용으로 설계된 인트라넷 사이트는 Android 및 iOS 장치에서 제대로 작동하려면 변경이 필요합니다.

Secure Web은 웹 기술 지원을 제공하기 위해 Android WebView 및 iOS WkWebView에 의존합니다. Secure Web에서 지원하는 웹 기술 중 일부는 다음과 같습니다.

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets

Secure Web에서 지원하지 않는 웹 기술 중 일부는 다음과 같습니다.

- 플래시

- 자바

다음 표는 Secure Web에서 지원하는 HTML 렌더링 기능 및 기술을 보여줍니다. X는 플랫폼, 브라우저 및 구성 요소 조합에서 해당 기능을 사용할 수 있음을 나타냅니다.

기술	IOS 시큐어 웹	ANDROID 6.X/7.X 시큐어 웹
JavaScript 엔진	JavaScriptCore	V8
로컬 스토리지	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
스르셋	X	X
WebGL		X
requestAnimationFrame API		X
내비게이션 타이밍 API		X
리소스 타이밍 API		X

기술은 모든 장치에서 동일하게 작동하지만, Secure Web은 장치마다 다른 사용자 에이전트 문자열을 반환합니다. Secure Web에 사용된 브라우저 버전을 확인하려면 해당 사용자 에이전트 문자열을 볼 수 있습니다.

Secure Web에서 [<https://whatsmyuseragent.com/>](https://whatsmyuseragent.com/) (으)로 이동합니다.

인트라넷 사이트 문제 해결

Secure Web에서 인트라넷 사이트를 볼 때 렌더링 문제를 해결하려면 Secure Web과 호환되는 타사 브라우저에서 웹사이트가 어떻게 렌더링되는지 비교하십시오.

iOS의 경우 테스트에 호환되는 타사 브라우저는 Chrome 및 Dolphin입니다.

Android의 경우, 테스트에 호환되는 타사 브라우저는 Dolphin입니다.

참고:

Chrome은 Android의 기본 브라우저입니다. 비교를 위해 사용하지 마십시오.

iOS에서는 브라우저에 장치 수준 VPN 지원이 있는지 확인하십시오. **설정 > VPN > VPN 구성 추가**로 이동하여 장치에서 VPN을 구성할 수 있습니다.

App Store에서 제공되는 [Citrix VPN](#), [Cisco AnyConnect](#), 또는 [Pulse Secure](#)와 같은 VPN 클라이언트 앱을 사용할 수도 있습니다.

- 두 브라우저에서 웹 페이지가 동일하게 렌더링되면 문제는 웹 사이트에 있습니다. 사이트를 업데이트하고 OS에서 잘 작동하는지 확인하십시오.
- 웹 페이지 문제가 Secure Web에서만 나타나면 Citrix 지원팀에 문의하여 지원 티켓을 여십시오. 테스트한 브라우저 및 OS 유형을 포함한 문제 해결 단계를 제공하십시오. iOS용 Secure Web에 렌더링 문제가 있는 경우, 다음 단계에 설명된 대로 페이지의 웹 아카이브를 포함하십시오. 이렇게 하면 Citrix가 문제를 더 빨리 해결하는 데 도움이 됩니다.

웹 아카이브 파일 생성 방법

macOS 10.9 이상에서 Safari를 사용하면 웹 페이지를 웹 아카이브 파일(읽기 목록이라고 함)로 저장할 수 있습니다. 웹 아카이브 파일에는 이미지, CSS, JavaScript와 같은 모든 연결된 파일이 포함됩니다.

1. Safari에서 읽기 목록 폴더를 비웁니다. **Finder**에서 **메뉴** 막대의 **이동** 메뉴를 클릭하고, **폴더로 이동**을 선택한 다음, 경로 이름 ~/Library/Safari/ReadingListArchives/를 입력하고 해당 위치의 모든 폴더를 삭제합니다.
2. **메뉴** 막대에서 **Safari > 환경설정 > 고급**으로 이동하여 메뉴 막대에서 **개발자 메뉴 보기**를 활성화합니다.
3. **메뉴** 막대에서 **개발 > 사용자 에이전트**로 이동하여 Secure Web 사용자 에이전트를 입력합니다:
(Mozilla/5.0 (iPad; CPU OS 8_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25).
4. Safari에서 읽기 목록(웹 아카이브 파일)으로 저장하려는 웹 사이트를 엽니다.
5. **메뉴** 막대에서 **책갈피 > 읽기 목록에 추가**로 이동합니다. 아카이빙은 백그라운드에서 진행되며 몇 분이 걸릴 수 있습니다.
6. 아카이브된 읽기 목록을 찾습니다. **메뉴** 막대에서 **보기 > 읽기 목록 사이드바 표시**로 이동합니다.
7. 아카이브 파일을 확인합니다:
 - Mac의 네트워크 연결을 끕니다.

- 읽기 목록에서 웹사이트를 엽니다.

웹사이트가 완전히 렌더링됩니다.

8. 아카이브 파일 압축: **Finder**에서 **메뉴** 막대의 **이동** 메뉴를 클릭하고 **폴더로 이동**을 선택한 다음 경로 이름 ~/Library/Safari/ReadingListArchives/를 입력합니다. 이제 파일 이름으로 임의의 16진수 문자열이 있는 폴더를 압축합니다. 지원 티켓을 열 때 이 파일을 Citrix 지원팀에 보낼 수 있습니다.

Secure Web 기능

Secure Web은 모바일 데이터 교환 기술을 사용하여 사용자가 내부 및 외부 웹사이트와 기타 모든 웹사이트에 액세스할 수 있도록 전용 VPN 터널을 생성합니다. 여기에는 조직 정책에 의해 보호되는 환경에서 민감한 정보가 포함된 사이트도 포함됩니다.

Secure Web과 Secure Mail 및 Citrix Files의 통합은 보안 Endpoint Management 컨테이너 내에서 원활한 사용자 환경을 제공합니다. 통합 기능의 몇 가지 예는 다음과 같습니다.

- 사용자가 **Mailto** 링크를 탭하면 추가 인증 없이 Citrix Secure Mail™에서 새 이메일 메시지가 열립니다.
- iOS에서 사용자는 URL 앞에 ****ctxmobilebrowser://****를 삽입하여 기본 메일 앱에서 Secure Web의 링크를 열 수 있습니다. 예를 들어, 기본 메일 앱에서 **example.com** 을(를) 열려면 URL **ctxmobilebrowser://example.com**을(를) 사용합니다.
- 사용자가 이메일 메시지에서 인트라넷 링크를 클릭하면 Secure Web은 추가 인증 없이 해당 사이트로 이동합니다.
- 사용자는 Secure Web에서 웹에서 다운로드한 파일을 Citrix Files에 업로드할 수 있습니다.

Secure Web 사용자는 다음 작업도 수행할 수 있습니다.

- 팝업 차단.

참고:

Secure Web 메모리의 상당 부분은 팝업 렌더링에 사용되므로, 설정에서 팝업을 차단하면 성능이 향상되는 경우가 많습니다.

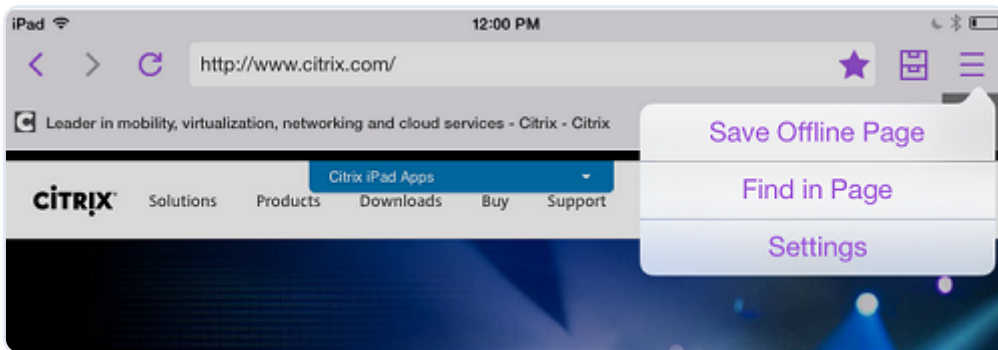
- 즐겨찾는 사이트를 북마크합니다.
- 파일을 다운로드합니다.
- 페이지를 오프라인으로 저장합니다.
- 암호를 자동 저장합니다.

- 캐시/기록/쿠키를 지웁니다.
- 쿠키 및 HTML5 로컬 스토리지를 비활성화합니다.
- 다른 사용자와 장치를 안전하게 공유합니다.
- 주소 표시줄 내에서 검색합니다.
- Secure Web으로 실행하는 웹 앱이 사용자의 위치에 액세스하도록 허용합니다.
- 설정을 내보내고 가져옵니다.
- 파일을 다운로드할 필요 없이 Citrix Files에서 직접 파일을 엽니다. 이 기능을 사용하려면 Endpoint Management의 허용된 URL 정책에 **ctx-sf**를 추가합니다.
- iOS에서 3D Touch 동작을 사용하여 새 탭을 열고 홈 화면에서 직접 오프라인 페이지, 즐겨찾는 사이트 및 다운로드에 액세스합니다.
- iOS에서 모든 크기의 파일을 다운로드하고 Citrix Files 또는 다른 앱에서 엽니다.

참고:

Secure Web을 백그라운드에 두면 다운로드가 중지됩니다.

- 페이지에서 찾기를 사용하여 현재 페이지 보기 내에서 용어를 검색합니다.



Secure Web은 동적 텍스트도 지원합니다. 앱은 사용자가 장치에 설정한 글꼴을 표시합니다.

참고:

- XenMobile용 Citrix Files는 July 1, 2023에 EOL에 도달했습니다. 자세한 내용은 [EOL 및 사용 중단된 앱을 참조하십시오](#).

엔드포인트 관리용 Citrix Content Collaboration™

Endpoint Management용 Citrix Content Collaboration 클라이언트는 Citrix Files 모바일 클라이언트의 MDX 지원 버전입니다. 이러한 클라이언트는 다른 MDX 래핑 앱의 데이터에 대한 안전하고 통합된 액세스를 제공합니다. Endpoint Management용 Citrix Content Collaboration 클라이언트는 마이크로 VPN, Secure Hub를 통한 단일 Sign-On(SSO) 및 2단계 인증과 같은 MDX 기능의 이점도 누립니다.

Citrix Files는 사용자가 문서를 쉽고 안전하게 교환할 수 있도록 하는 엔터프라이즈 파일 동기화 및 공유 서비스입니다. Citrix Files는 Citrix Files for Android Phone 및 Citrix Files for iPad와 같은 Citrix Files 모바일 클라이언트를 포함하여 사용자에게 다양한 액세스 옵션을 제공합니다.

Citrix Files를 Endpoint Management와 통합하여 전체 Citrix Files 기능 세트를 제공하거나 스토리지 영역 커넥터에만 액세스를 제공할 수 있습니다. 기본적으로 Citrix Endpoint Management 콘솔은 Citrix Files만 구성할 수 있도록 합니다. 대신 스토리지 영역 커넥터와 함께 사용하도록 Endpoint Management를 구성하려면 Citrix Endpoint Management 설명서에서 [Endpoint Management](#)와 [Citrix Content Collaboration](#) 사용을 참조하십시오.

Endpoint Management용 Citrix Content Collaboration 클라이언트를 배포하고 관리하기 위해 Endpoint Management, Citrix Files, 스토리지 영역 컨트롤러 및 Citrix ADC를 다음과 같이 사용합니다.

- Endpoint Management가 Citrix Files로 구성된 경우 Endpoint Management는 SAML ID 공급자 (IdP) 역할을 하며 Endpoint Management용 Citrix Content Collaboration 클라이언트를 배포합니다. Citrix Files는 Citrix Files 데이터를 관리합니다. Citrix Files 데이터는 Endpoint Management를 통과하지 않습니다.
- Endpoint Management가 Citrix Files 또는 스토리지 영역 커넥터로 구성된 경우 스토리지 영역 컨트롤러는 네트워크 공유 및 SharePoint의 데이터에 대한 연결을 제공합니다. 사용자는 Citrix Files 모바일 생산성 앱을 통해 저장된 데이터에 액세스합니다. 사용자는 모바일 장치에서 Microsoft Office 문서를 편집하고 Adobe PDF 파일을 미리 보고 주석을 달 수 있습니다.
- Citrix ADC는 외부 사용자로부터의 요청을 관리하고, 연결을 보호하며, 요청의 로드 밸런싱을 수행하고, 스토리지 영역 커넥터에 대한 콘텐츠 전환을 처리합니다.

Endpoint Management용 Citrix Content Collaboration 및 기타 모바일 생산성 앱 시스템 요구 사항에 대한 자세한 내용은 [모바일 생산성 앱 지원](#)을 참조하십시오.

Endpoint Management용 Citrix Content Collaboration 클라이언트가 Citrix Files 모바일 클라이언트와 다른 점

다음은 Endpoint Management용 Citrix Content Collaboration 클라이언트와 Citrix Files 모바일 클라이언트 간의 차이점을 설명합니다.

사용자 액세스

엔드포인트 관리용 Citrix Content Collaboration 클라이언트:

사용자는 Secure Hub에서 Endpoint Management용 Citrix Content Collaboration 클라이언트를 획득하고 엽니다.

Citrix Files 모바일 클라이언트:

사용자는 앱 스토어에서 Citrix Files 모바일 클라이언트를 얻습니다.

SSO

엔드포인트 관리 클라이언트용 시트릭스 콘텐츠 콜라보레이션:

Citrix Files와 Endpoint Management 통합의 경우: Endpoint Management를 Citrix Files용 SAML IdP로 구성할 수 있습니다. 이 구성에서 Secure Hub는 Endpoint Management를 SAML IdP로 사용하여 Endpoint Management 클라이언트용 Citrix Content Collaboration에 대한 SAML 토큰을 얻습니다. Endpoint Management 클라이언트용 Citrix Content Collaboration을 시작했지만 Secure Hub에 로그인하지 않은 사용자는 Secure Hub에 로그인하라는 메시지가 표시됩니다. 사용자는 Citrix Files 도메인 또는 계정 정보를 알 필요가 없습니다.

Citrix Files 모바일 클라이언트:

Endpoint Management 및 Citrix Gateway를 Citrix Files용 SAML IdP로 구성할 수 있습니다. 이 구성에서 웹 브라우저 또는 다른 Citrix Files 클라이언트를 사용하여 Citrix Files에 로그인하는 사용자는 사용자 인증을 위해 Endpoint Management 환경으로 리디렉션됩니다. Endpoint Management에 의한 인증이 성공하면 사용자는 Citrix Files 계정에 로그인하는 데 유효한 SAML 토큰을 받습니다.

마이크로 VPN

엔드포인트 관리 클라이언트용 시트릭스 콘텐츠 콜라보레이션:

원격 사용자는 Citrix Gateway를 통해 VPN 또는 마이크로 VPN 연결을 사용하여 내부 네트워크의 앱 및 데스크톱에 액세스할 수 있습니다. Endpoint Management와 Citrix ADC 통합을 통해 제공되는 이 기능은 사용자에게 투명합니다.

Citrix Files 모바일 클라이언트:

해당 없음.

2단계 인증

엔드포인트 관리용 Citrix Content Collaboration 클라이언트:

Endpoint Management와 Citrix ADC 통합은 클라이언트 인증서 인증과 LDAP 또는 RADIUS와 같은 다른 인증 유형의 조합을 사용한 인증도 지원합니다.

Citrix Files 모바일 클라이언트:

해당 없음.

폴더 권한

Endpoint Management 클라이언트용 Citrix Content Collaboration 및 Citrix Files 모바일 클라이언트:

Endpoint Management와 Citrix Files 통합의 경우: Citrix Files에 의해 결정됩니다.

문서 액세스 보호

엔드포인트 관리용 Citrix Content Collaboration 클라이언트:

사용자는 Secure Mail에서 수신했거나 MDX로 래핑된 앱에서 다운로드한 첨부 파일을 열 수 있습니다. 사용자가 '다음으로 열기' 작업을 수행할 때 MDX로 래핑된 앱만 나타납니다. 래핑되지 않은 앱의 데이터는 Endpoint Management 클라이언트용 Citrix Content Collaboration에서 사용할 수 없습니다. Secure Mail 사용자는 파일을 장치에 다운로드할 필요 없이 Citrix Files 리포지토리에서 파일을 첨부할 수 있습니다. 사용자가 장치에 래핑된 Citrix Files와 래핑되지 않은 Citrix Files를 모두 가지고 있는 경우, 래핑된 Citrix Files 클라이언트는 사용자의 개인 Citrix Files 계정에 있는 파일에 액세스할 수 없습니다. 래핑된 Citrix Files 클라이언트는 Endpoint Management에 구성된 Citrix Files 하위 도메인에만 액세스할 수 있습니다.

Citrix Files 모바일 클라이언트:

사용자는 모든 앱에서 첨부 파일을 열 수 있습니다.

Citrix Files 계정 액세스

Citrix Content Collaboration Endpoint Management를 위한 클라이언트:

Endpoint Management와 Citrix Files 통합의 경우: 개인 Citrix Files 계정 또는 타사 Citrix Files 계정에 액세스하려면 사용자는 장치에서 MDX가 아닌 버전의 Citrix Files를 사용해야 합니다.

Citrix Files 모바일 클라이언트:

Endpoint Management와 Citrix Files 통합의 경우: Citrix Files 클라이언트에서 사용할 수 있습니다.

장치 정책

Endpoint Management 클라이언트용 Citrix Content Collaboration 및 Citrix Files 모바일 클라이언트:

Endpoint Management 및 Citrix Files 장치 정책은 모두 Endpoint Management 클라이언트용 Citrix Content Collaboration에 적용됩니다. 예를 들어, Endpoint Management 콘솔에서 장치 초기화를 수행할 수 있습니다. Citrix Files 콘솔에서 Citrix Files 앱을 원격으로 초기화할 수 있습니다.

MDX 정책

Citrix Content Collaboration Endpoint Management를 위한 클라이언트:

MDX 정책을 사용하면 Endpoint Management 앱 스토어에서 적용하는 Citrix Endpoint Management™ 설정을 구성할 수 있습니다. MDX를 통해서만 사용할 수 있는 정책에는 카메라, 마이크, 이메일 작성, 화면 캡처, 클립보드 잘라내기, 복사 및 붙여넣기 작업을 차단하는 기능이 포함됩니다.

Citrix Files 모바일 클라이언트:

해당 없음.

데이터 암호화

Endpoint Management 클라이언트용 Citrix Content Collaboration 및 Citrix Files 모바일 클라이언트:

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

가용성

엔드포인트 관리 클라이언트를 위한 Citrix Content Collaboration:

Endpoint Management 클라이언트용 Citrix Content Collaboration은 Endpoint Management Advanced 및 Enterprise 에디션에 포함되어 있습니다.

Citrix Files 모바일 클라이언트:

모든 Endpoint Management 에디션에는 모든 Citrix Files 기능이 포함됩니다. Endpoint Management를 전체 Citrix Files 기능 세트 또는 스토리지 영역 커넥터와 통합할 수 있습니다.

Endpoint Management 클라이언트를 위한 Citrix Content Collaboration 통합 및 제공

Endpoint Management 클라이언트를 위한 Citrix Content Collaboration을 통합하고 제공하려면 다음 일반 단계를 따르십시오.

1. Citrix Files 클라이언트에서 Citrix Files로 SSO를 제공하기 위해 Endpoint Management를 Citrix Files용 SAML IdP로 활성화합니다. 이렇게 하려면 Endpoint Management에서 Citrix Files 계정 정보를 구성해야 합니다. 자세한 내용은 "SSO를 위해 Endpoint Management에서 Citrix Files 계정 정보를 구성하는 방법" 섹션을 참조하십시오.

중요:

Citrix Files 웹 앱 및 Citrix Files Sync 클라이언트와 같은 비-MDX Citrix Files 클라이언트에 Endpoint Management를 SAML IdP로 사용하려면 추가 구성이 필요합니다.

2. Citrix Files 클라이언트를 다운로드합니다.
3. Citrix Files 클라이언트를 Endpoint Management에 추가합니다. 자세한 내용은 이 문서의 뒷부분에 있는 "Endpoint Management에 Citrix Files를 추가하는 방법"을 참조하십시오.
4. 구성을 검증합니다. 자세한 내용은 이 문서의 뒷부분에 있는 "Citrix Files 클라이언트를 검증하는 방법"을 참조하십시오.

Endpoint Management에서 Citrix Files를 구성하기 위한 이미지(/en-us/mobile-productivity-apps/media/configure-sharefile-endpointmanagement.png)

설정에 대하여:

- 도메인은 클라이언트에 사용될 Citrix Files 하위 도메인입니다.
- 선택한 DG의 사용자만 클라이언트에서 Citrix Files에 대한 SSO 액세스 권한을 가집니다.

DG의 사용자가 Citrix Files 계정이 없는 경우, Endpoint Management에 Citrix Files 클라이언트를 추가하면 Endpoint Management가 해당 사용자를 Citrix Files에 프로비저닝합니다.

- Citrix Files 관리자 계정 로그인 정보는 Endpoint Management에서 Citrix Files 제어 평면에 SAML 설정을 저장하는 데 사용됩니다.

중요:

Citrix Files 클라이언트에서 Citrix Files로 SSO를 활성화하는 구성은 사용자를 네트워크 공유 또는 SharePoint 문서 라이브러리에 인증하지 않습니다. 이러한 커넥터 데이터 소스에 액세스하려면 네트워크 공유 또는 SharePoint 서버가 있는 Active Directory 도메인에 대한 인증이 필요합니다.

SSO를 위해 Endpoint Management에서 Citrix Files 계정 정보 구성

Secure Hub에서 모바일 생산성 앱으로 SSO를 활성화하려면 Endpoint Management 콘솔에서 Citrix Files 계정 및 Citrix Files 관리자 서비스 계정 정보를 지정합니다. 이 구성을 통해 Endpoint Management는 모바일 생산성 앱 클라이언트, Citrix Files 클라이언트 및 비 MDX Citrix Files 클라이언트를 위한 Citrix Files의 SAML IdP 역할을 합니다. 사용자가 모바일 생산성 앱 클라이언트를 시작하면 Secure Hub는 Endpoint Management에서 사용자를 위한 SAML 토큰을 가져와 Citrix Files 클라이언트로 보냅니다.

Endpoint Management 콘솔에서 **Configure > Content Collaboration**을 클릭합니다. Content Collaboration은 Citrix Files의 이전 이름입니다.

Endpoint Management에 Endpoint Management 클라이언트용 Citrix Content Collaboration을 추가하려면

Endpoint Management에 Endpoint Management 클라이언트용 Citrix Content Collaboration을 추가할 때 Endpoint Management 클라이언트용 Citrix Content Collaboration에서 커넥터 데이터 소스에 대한 SSO 액세스를 활성화할 수 있습니다. 이렇게 하려면 이 섹션에 설명된 대로 네트워크 액세스 정책 및 기본 VPN 모드 정책을 구성합니다.

필수 구성 요소

- Endpoint Management는 Citrix Files 하위 도메인에 연결할 수 있어야 합니다. 연결을 테스트하려면 Endpoint Management 서버에서 Citrix Files 하위 도메인으로 ping을 보냅니다.
- Citrix Files 계정 및 Endpoint Management를 실행하는 하이퍼바이저에 대해 구성된 시간대가 동일해야 합니다. 시간대가 다르면 SAML 토큰이 예상 시간 내에 Citrix Files에 도달하지 못하여 SSO 요청이 실패할 수 있습니다. Endpoint Management용 NTP 서버를 구성하려면 Endpoint Management 명령 줄 인터페이스를 사용하십시오.

참고:

Hyper-V 호스트는 Linux VM의 시간을 UTC가 아닌 로컬 시간대로 설정합니다.

- 관리자로 ShareFile 계정에 로그인하고 **Settings > Admin Settings > Security > Login & Security Policy > Single sign-on / SAML 2.0 Configuration**에서 SAML SSO 설정을 확인합니다.
- Endpoint Management 클라이언트용 Citrix Content Collaboration을 다운로드합니다.

단계:

1. Endpoint Management 콘솔에서 **Configure > Apps**를 클릭한 다음 **Add**를 클릭합니다.
2. **MDX**를 클릭합니다.
3. 앱에 대한 **이름**을 입력하고, 선택적으로 **설명**과 **앱 범주**를 입력합니다.
4. **다음**을 클릭한 다음 Citrix Content Collaboration for Endpoint Management 클라이언트에 대한 .mdx 파일을 업로드합니다.
5. 앱 정보 및 정책을 구성하려면 **다음**을 클릭합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트에서 Citrix Files로 SSO를 활성화하는 구성은 사용자를 네트워크 공유 또는 SharePoint 문서 라이브러리에 인증하지 않습니다.

6. Secure Hub 마이크로 VPN과 스토리지 영역 컨트롤러 간에 SSO를 활성화하려면 다음 정책 구성을 완료합니다.
 - 네트워크 액세스 정책을 **내부 네트워크로 터널링됨**으로 설정합니다.

이 모드에서 MDX 프레임워크는 Citrix Content Collaboration for Endpoint Management 클라이언트의 모든 네트워크 트래픽을 가로챍니다. 그런 다음 네트워크 트래픽은 앱별 마이크로 VPN을 사용하여 Citrix Gateway를 통해 리디렉션됩니다.

- 기본 VPN 모드 정책을 **터널링됨 – 웹 SSO**로 설정합니다.

이 터널링 모드에서 MDX 프레임워크는 MDX 앱의 SSL/HTTP 트래픽을 종료하고, 그런 다음 사용자 대신 내부 연결에 대한 새 연결을 시작합니다. 이 정책 설정을 통해 MDX 프레임워크는 웹 서버에서 발행한 인증 챌린지를 감지하고 응답할 수 있습니다.

7. 필요에 따라 승인 및 배달 그룹(DG) 할당을 완료합니다.

선택한 DG의 사용자만 Citrix Content Collaboration for Endpoint Management 클라이언트에서 Citrix Files로 SSO 액세스 권한을 가집니다. DG의 사용자가 Citrix Files 계정이 없는 경우, Endpoint Management에 Citrix Content Collaboration for Endpoint Management 클라이언트를 추가하면 Endpoint Management가 해당 사용자를 Citrix Files에 프로비저닝합니다.

Citrix Content Collaboration for Endpoint Management 클라이언트의 유효성을 검사하려면

1. 이 문서에 설명된 구성을 완료한 후 Citrix Content Collaboration for Endpoint Management 클라이언트를 시작합니다. Citrix Files는 로그인하라는 메시지를 표시하지 않습니다.
2. Secure Mail에서 이메일을 작성하고 Citrix Files에서 첨부 파일을 추가합니다. 로그인하라는 메시지 없이 Citrix Files 홈 페이지가 열립니다.

참고:

- XenMobile용 Citrix Files는 July 1, 2023부로 EOL(수명 종료)되었습니다. 자세한 내용은 [EOL 및 사용 중단된 앱을\(를\) 참조하십시오](#).

EOL 및 지원 중단된 앱

다음 앱은 EOL(수명 종료)에 도달했거나 도달할 예정입니다. 제품 릴리스가 EOL에 도달하면 제품 라이선스 계약 조건 내에서 제품을 사용할 수 있지만, 사용 가능한 지원 옵션은 제한됩니다. 과거 정보는 Knowledge Center 또는 기타 온라인 리소스에 나타납니다. 설명서는 더 이상 업데이트되지 않으며 있는 그대로 제공됩니다. 제품 수명 주기 마일스톤에 대한 자세한 내용은 [제품 매트릭스](#)를 참조하십시오.

참고:

단계적으로 중단되는 Citrix Endpoint Management 기능에 대한 사전 통지를 보려면 [지원 중단](#)을 참조하십시오.

Citrix Files for XenMobile® (MDX): Citrix Files for XenMobile은 July 1, 2023에 EOL에 도달했습니다.

고객은 Apple App Store 및 Google Play에서 사용할 수 있는 Citrix Files를 사용하는 것이 좋습니다. MAM SDK를 지원합니다.

Secure Mail for Intune SDK (iOS & Android): Secure Mail은 April 30, 2023에 EOL에 도달했습니다.

Citrix Files for Intune: December 31, 2020에 지원 중단되었습니다.

Android Enterprise(작업 프로필 포함) 및 iOS 사용자 등록을 통해 플랫폼 기능을 활용하여 일반 Citrix Files 앱(앱 스토어에서 사용 가능)을 컨테이너화하는 옵션을 살펴보시기 바랍니다.

ShareConnect: ShareConnect은 June 30, 2020에 EOL에 도달했습니다.

Secure Notes: EOL 수명 주기 날짜는 December 31, 2018이었습니다.

Secure Notes 및 Secure Tasks의 기능이 필요한 경우, MDX 정책으로 보호할 수 있는 타사 앱인 Notate for Citrix를 권장합니다.

Secure Notes 및 Secure Tasks 사용자가 Outlook에 데이터를 저장한 경우, Notate에서 해당 데이터에 액세스할 수 있습니다. 사용자가 ShareFile(현재 Citrix Files)에 데이터를 저장한 경우, 데이터는 마이그레이션되지 않습니다.

사용자는 플랫폼 운영 체제가 사용자 인터페이스 지원을 중단할 때까지 EOL 날짜 이후에도 Secure Notes를 계속 실행할 수 있습니다. 그러나 지원되지 않는 제품을 사용하는 것은 권장하지 않습니다.

Secure Tasks: EOL 수명 주기 날짜는 December 31, 2018이었습니다.

Secure Forms: EOL 수명 주기 날짜는 March 31, 2018이었습니다. 고객은 Citrix Files Platinum 및 Premium 계정에 포함된 Citrix ShareFile Workflows로 전환하는 것이 좋습니다. 자세한 내용은 [Citrix ShareFile Workflows](#)를 참조하십시오.

ScanDirect: ScanDirect는 September 1, 2018에 EOL에 도달했습니다.

Full VPN tunnel: EOL 날짜는 2021년 9월이었습니다. 자세한 내용은 Citrix Endpoint Management 제품 설명서의 [사용 중단](#)을 참조하십시오.

Full VPN tunnel- Android: 2020년 3월에 사용 중단되었습니다. EOL 날짜는 2021년 9월이었습니다. 고객은 대안으로 MAM SDK 웹 SSO 모드를 사용하는 것이 좋습니다.

Permit VPN mode switching - Android: 2020년 3월에 사용 중단되었습니다. EOL 날짜는 2021년 9월이었습니다.

Inbound Document Exchange - Android: 2020년 3월에 사용 중단되었습니다. EOL 날짜는 2021년 9월이었습니다.

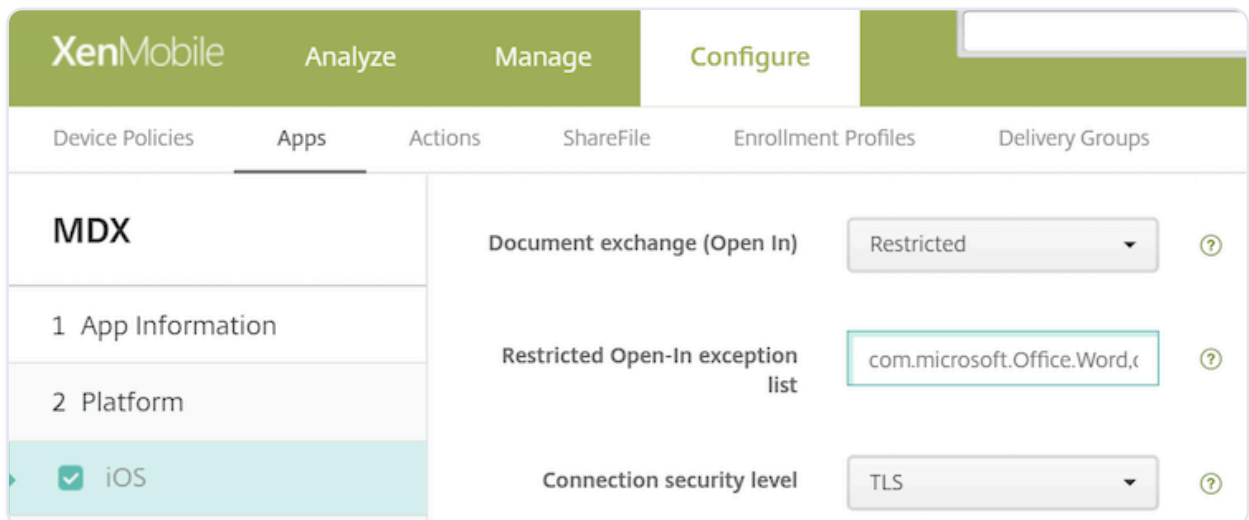
Office 365 앱과의 보안 상호 작용 허용

Citrix Secure Mail™, Citrix Secure Web 및 Citrix Files는 사용자가 문서와 데이터를 Microsoft Office 365 앱으로 전송할 수 있도록 MDX 컨테이너를 열 수 있는 옵션을 제공합니다. 이 기능은 Endpoint Management 콘솔의 열기 정책을 통해 iOS 및 Android 플랫폼용으로 관리합니다.

Microsoft 앱에서 열리면 데이터는 더 이상 MDX 컨테이너에서 보안되거나 암호화되지 않습니다. 이 기능을 활성화하기 전에 보안 영향을 고려하십시오. 특히 데이터 손실 방지에 관심이 있거나 HIPAA 또는 기타 엄격한 규정 준수 요구 사항을 따르는 고객은 컨테이너를 여는 것의 장단점을 신중하게 고려해야 합니다.

iOS에서 Office 365 활성화

1. [Endpoint Management 다운로드 페이지](#)에서 Secure Mail, Secure Web 또는 Citrix Files 앱의 최신 버전을 다운로드합니다.
2. 파일을 Endpoint Management 콘솔에 업로드합니다.
3. **문서 교환(열기)** 정책을 찾아서 **제한됨**으로 설정합니다. **제한된 열기 예외 목록**에서 Microsoft Word, Excel, PowerPoint, OneNote 및 Outlook이 자동으로 나열됩니다. 예: com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook



MDM 등록 시 iOS 장치에 더 많은 제어 기능이 제공됩니다.

iTunes 앱을 Endpoint Management 콘솔에 업로드하고 장치로 푸시할 수 있습니다. 이 옵션을 선택하는 경우 다음 정책을 **켜기**로 설정합니다.

- MDM 프로필이 제거되면 앱 제거
- 앱 데이터 백업 방지
- 앱을 관리하도록 강제 적용 (선택적 초기화는 앱과 모든 데이터를 제거합니다.)

Microsoft 앱에서 장치의 관리되지 않는 앱으로 문서 및 데이터가 흐르는 것을 방지하려면 Endpoint Management 콘솔에서 **구성 > 장치 > 제한 > iOS**로 이동한 다음 **관리되지 않는 앱의 관리되는 앱 문서 및 관리되는 앱의 관리되지 않는 앱 문서를 끄기**로 설정합니다.

Android에서 Office 365 활성화

1. Endpoint Management 다운로드 페이지(<https://www.citrix.com/downloads/citrix-endpoint-management/>)에서 Secure Mail, Secure Web 또는 Citrix Files 앱의 최신 버전을 다운로드합니다.
2. 파일을 Endpoint Management 콘솔에 업로드합니다.
3. **문서 교환 (Open In)** 정책으로 스크롤한 다음 **제한됨**을 선택합니다.
4. **제한된 Open-in 예외 목록**에서 다음 패키지 ID를 추가합니다.

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

5. 다른 앱 정책을 평소와 같이 구성하고 앱을 저장합니다.

사용자는 Secure Mail, Secure Web 또는 Citrix Files에서 파일을 장치에 저장하고 Office 365 앱으로 파일을 열어야 합니다.

iOS 및 Android 모두에서 사용자는 장치에서 다음 유형의 파일을 열고 편집할 수 있습니다.

지원되는 파일 형식

지원되는 파일 형식에 대한 자세한 내용은 Microsoft Office 설명서를 참조하십시오.

모바일 생산성 앱 문서 기록

다음 표에는 모바일 생산성 앱 제품 설명서의 중요한 변경 사항이 설명되어 있습니다. 이러한 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

날짜	변경	설명
30 May 2025	iOS용 Secure Mail 25.5.0의 EAR	다음 릴리스 미리 보기
30 May 2025	iOS용 Secure Web 25.5.0의 EAR	다음 릴리스 미리 보기
21 May 2025	Android용 Secure Hub 버전 25.4.0 릴리스	현재 버전의 새로운 기능
02 Apr 2025	Android용 Secure Mail 버전 25.3.0 릴리스	현재 버전의 새로운 기능
02 Apr 2025	Android용 Secure Web 버전 25.3.0 릴리스	현재 버전의 새로운 기능
17 Feb 2025	Android용 Secure Mail 버전 25.1.0 릴리스	현재 버전의 새로운 기능
17 Feb 2025	iOS용 Secure Hub 버전 25.1.0 릴리스	현재 버전의 새로운 기능
12 Feb 2025	iOS용 Secure Mail 버전 25.1.0 릴리스	현재 버전의 새로운 기능
10 Feb 2025	Android용 Secure Hub 버전 25.1.0 릴리스	현재 버전의 새로운 기능
10 Feb 2025	iOS용 Secure Web 버전 25.1.0 릴리스	현재 버전의 새로운 기능
10 Feb 2025	Android용 Secure Web 버전 25.1.0 릴리스	현재 버전의 새로운 기능

날짜	변경	설명
09 Dec 2024	iOS용 Secure Mail 버전 24.11.0 릴리스	현재 버전의 새로운 기능
09 Dec 2024	iOS용 Secure Hub 버전 24.11.0 릴리스	현재 버전의 새로운 기능
06 Dec 2024	iOS용 Secure Web 버전 24.11.0 릴리스	현재 버전의 새로운 기능
05 Dec 2024	Android용 Secure Mail 버전 24.11.0 릴리스	현재 버전의 새로운 기능
04 Dec 2024	Android용 Secure Mail 24.11.0의 EAR	다음 릴리스 미리 보기
04 Dec 2024	iOS용 Secure Mail 24.11.0의 EAR	다음 릴리스 미리 보기
26 Nov 2024	iOS용 Secure Web 24.11.0의 EAR	다음 릴리스 미리 보기
26 Nov 2024	iOS용 Secure Hub 24.11.0의 EAR	다음 릴리스 미리 보기
25 Nov 2024	새로운 장: 기능 플래그 관리	기능 플래그 관리
05 Nov 2024	Android용 Secure Hub 버전 24.10.0 릴리스	현재 버전의 새로운 기능
24 Oct 2024	Android 24.10.0용 Secure Hub의 EAR	다음 릴리스 미리 보기
22 Oct 2024	Android용 Secure Mail 버전 24.9.1 릴리스	현재 버전의 새로운 기능
15 Oct 2024	iOS용 Secure Hub 버전 24.9.0 릴리스	현재 버전의 새로운 기능
09 Oct 2024	Android용 Secure Web 버전 24.9.0 릴리스	현재 버전의 새로운 기능

날짜	변경	설명
09 Oct 2024	Android용 Secure Mail 버전 24.9.0 릴리스	현재 버전의 새로운 기능
09 Oct 2024	iOS용 Secure Hub 24.9.0의 EAR	다음 릴리스 미리 보기
27 Sep 2024	Android용 Secure Web 24.9.0의 EAR	다음 릴리스 미리 보기
27 Sep 2024	Android용 Secure Mail 24.9.0의 EAR	다음 릴리스 미리 보기
20 Sep 2024	iOS용 Secure Mail 버전 24.9.0 릴리스	현재 버전의 새로운 기능
16 Sep 2024	iOS용 Secure Web 버전 24.9.0 릴리스	현재 버전의 새로운 기능
06 Sep 2024	Android용 Secure Hub 버전 24.8.0의 릴리스 수정	현재 버전의 새로운 기능
04 Sep 2024	iOS용 Secure Mail 24.9.0의 EAR	다음 릴리스 미리 보기
03 Sep 2024	iOS용 Secure Web 24.9.0의 EAR	다음 릴리스 미리 보기
02 Sep 2024	Android용 Secure Hub 버전 24.8.0 릴리스	현재 버전의 새로운 기능
28 Aug 2024	Android용 Secure Web 버전 24.8.0 릴리스	현재 버전의 새로운 기능
23 Aug 2024	Android용 Secure Web 버전 24.8.0의 EAR	다음 릴리스 미리 보기
21 Aug 2024	Android용 Secure Hub 24.8.0의 EAR	다음 릴리스 미리 보기
29 Jul 2024	Android용 Secure Mail 버전 24.7.0 릴리스	Secure Mail 24.7.0: 현재 버전의 새로운 기능

날짜	변경	설명
16 Jul 2024	Android용 Secure Mail 24.7.0의 EAR	다음 릴리스 미리 보기
01 Jul 2024	Android용 Secure Hub 버전 24.6.0 릴리스	Secure Hub 24.6.0: 현재 버전의 새로운 기능
06 May 2024	iOS용 Secure Hub 버전 24.5.0 릴리스	Secure Hub 24.5.0: 현재 버전의 새로운 기능
22 Apr 2024	Android용 Secure Hub 버전 24.3.0의 릴리스를 새로운 기능으로 수정했습니다.	Secure Hub 24.3.0: 현재 버전의 새로운 기능
22 Apr 2024	Android용 Secure Hub 버전 23.12.0의 릴리스를 새로운 기능으로 수정했습니다.	Secure Hub 23.12.0: 현재 버전의 새로운 기능
11 Apr 2024	Android용 Secure Hub 버전 24.3.0 릴리스	Secure Hub 24.3.0: 버그 수정
25 Mar 2024	iOS용 Secure Web 버전 24.3.0 릴리스	Secure Web 24.3.0: 버그 수정
25 Mar 2024	iOS용 Secure Mail 버전 24.3.0 릴리스	Secure Mail 24.3.0: 버그 수정
18 Mar 2024	Android용 Secure Web 버전 24.3.0 릴리스	Secure Web 24.3.0: 버그 수정
21 Feb 2024	iOS용 Secure Web 버전 24.2.0 릴리스	Secure Web 24.2.0: 버그 수정
21 Feb 2024	iOS용 Secure Web 버전 24.2.0 릴리스	Secure Web 24.2.0: 현재 버전의 새로운 기능
21 Feb 2024	iOS용 Secure Mail 버전 24.2.0 릴리스	Secure Mail 24.2.0: 버그 수정
21 Feb 2024	iOS용 Secure Mail 버전 24.2.0 릴리스	Secure Mail 24.2.0: 현재 버전의 새로운 기능

날짜	변경	설명
19 Feb 2024	Android용 Secure Web 버전 24.1.0 릴리스	Secure Web 24.1.0: 버그 수정
19 Feb 2024	Android용 Secure Mail 버전 24.1.0 릴리스	Secure Mail 24.1.0: 버그 수정
19 Feb 2024	Android용 Secure Mail 버전 24.1.0 릴리스	Secure Mail 24.1.0: 현재 버전의 새로운 기능
16 Jan 2024	iOS용 Secure Hub 버전 24.1.0 릴리스	Secure Hub 24.1.0: 현재 버전의 새로운 기능
16 Jan 2024	iOS용 Secure Hub 버전 24.1.0 릴리스	Secure Hub 24.1.0: 버그 수정
16 Jan 2024	Android용 Secure Hub 버전 23.12.0 릴리스	Secure Hub 23.12.0: 현재 버전의 새로운 기능 및 버그 수정
04 Dec 2023	화면 가리기 문서 추가	Secure Mail: 화면 콘텐츠 가리기
28 Nov 2023	iOS용 Secure Hub 버전 23.11.0 릴리스	Secure Hub 23.11.0: 현재 버전의 새로운 기능
28 Nov 2023	iOS용 Secure Hub 버전 23.11.0 릴리스	Secure Hub 23.11.0: 버그 수정
17 Nov 2023	Android용 Secure Web 버전 23.10.0 릴리스	Secure Web 23.10.0: 현재 버전의 새로운 기능
17 Nov 2023	Android용 Secure Mail 버전 23.10.0 릴리스	Secure Mail 23.10.0: 버그 수정
27 Oct 2023	Android용 Secure Mail 버전 23.8.2 릴리스	Secure Mail 23.8.2: 현재 버전의 새로운 기능
19 Oct 2023	Android용 Secure Hub 버전 23.10.0 릴리스	Secure Hub 23.10.0: 현재 버전의 새로운 기능
04 Oct 2023	Android용 Secure Mail 버전 23.7.0 릴리스	Secure Mail 23.7.0: 현재 버전의 새로운 기능

날짜	변경	설명
04 Oct 2023	iOS용 Secure Mail 버전 23.7.0 릴리스	Secure Mail 23.7.0: 현재 버전의 새로운 기능
29 Sep 2023	Android용 Secure Mail 버전 23.8.1 릴리스	Secure Mail 23.8.1: 현재 버전의 새로운 기능
20 Sep 2023	iOS용 Secure Web 버전 23.9.0 릴리스	Secure Web 23.9.0: 현재 버전의 새로운 기능
20 Sep 2023	iOS용 Secure Mail 버전 23.9.0 릴리스	Secure Mail 23.9.0: 현재 버전의 새로운 기능
20 Sep 2023	Android용 Secure Web 버전 23.8.0 릴리스	Secure Web 23.8.0: 현재 버전의 새로운 기능
20 Sep 2023	Android용 Secure Mail 버전 23.8.0 릴리스	Secure Mail 23.8.0: 현재 버전의 새로운 기능
01 Sep 2023	Android용 Secure Hub 버전 23.9.0 릴리스	Secure Hub 23.9.0: 현재 버전의 새로운 기능
25 Aug 2023	iOS용 Secure Hub 버전 23.8.1 릴리스	Secure Hub 23.8.1: 현재 버전의 새로운 기능
08 Aug 2023	iOS용 Secure Hub 버전 23.8.0 릴리스	Secure Hub 23.8.0: 현재 버전의 새로운 기능
31 Jul 2023	Android용 Secure Web 버전 23.7.0 릴리스	Secure Web 23.7.0: 현재 버전의 새로운 기능
31 Jul 2023	Android용 Secure Mail 버전 23.7.0 릴리스	Secure Mail 23.7.0: 현재 버전의 새로운 기능
26 Jul 2023	Android용 Secure Hub 버전 23.7.0 릴리스	Secure Hub 23.7.0: 현재 버전의 새로운 기능
07 Jul 2023	iOS용 Secure Hub 버전 23.4.0 릴리스	Secure Hub 23.4.0: 현재 버전의 새로운 기능
22 Jun 2023	알려진 문제인 CXM-110137 추가됨	Android용 Secure Mail의 알려진 문제

날짜	변경	설명
07 Jun 2023	Android용 Secure Mail 버전 23.6.0 릴리스	Secure Mail 23.6.0: 현재 버전의 새로운 기능
31 May 2023	iOS용 Secure Web 버전 23.5.0 릴리스	Secure Web 23.5.0: 현재 버전의 새로운 기능
31 May 2023	iOS용 Secure Mail 버전 23.5.0 릴리스	Secure Mail 23.5.0: 현재 버전의 새로운 기능
26 May 2023	Android용 Secure Hub 버전 23.4.0 릴리스	Secure Hub 23.4.0: 현재 버전의 새로운 기능
23 May 2023	Android용 Secure Hub 버전 23.2.0 릴리스	Secure Hub 23.2.0: 현재 버전의 새로운 기능
12 Apr 2023	Android용 Secure Web 버전 23.3.5 릴리스	알려진 문제 추가
28 Mar 2023	Android용 Secure Web 버전 23.3.5 릴리스	Secure Web 23.3.5: 현재 버전의 새로운 기능
28 Mar 2023	Android용 Secure Mail 버전 23.3.5 릴리스	Secure Mail 23.3.5: 현재 버전의 새로운 기능
09 Jan 2023	Android용 Secure Hub 버전 22.11.0 릴리스	Secure Hub 22.11.0: 현재 버전의 새로운 기능
01 Feb 2023	iOS 및 Android용 Secure Web 버전 23.2.0 릴리스	Secure Web 23.2.0: 현재 버전의 새로운 기능
01 Feb 2023	Android용 Secure Mail 버전 23.2.0 릴리스	Secure Mail 23.2.0: 현재 버전의 새로운 기능
28 Oct 2022	Android용 Secure Mail 버전 22.11.0 릴리스	Secure Mail 22.11.0: 현재 버전의 새로운 기능
12 Oct 2022	Android용 Secure Hub 버전 22.9.0 릴리스	Secure Hub 22.9.0: 현재 버전의 새로운 기능
28 Sep 2022	Android용 Secure Mail 버전 22.9.0 릴리스	Secure Mail 22.9.0: 현재 버전의 새로운 기능

날짜	변경	설명
28 Sep 2022	Android용 Secure Web 버전 22.9.0 릴리스	Secure Web 22.9.0: 현재 버전의 새로운 기능
08 Sep 2022	iOS용 Secure Web 버전 22.9.1 릴리스	Secure Web 22.9.1: 현재 버전의 새로운 기능
07 Sep 2022	iOS용 Secure Web 버전 22.9.0 릴리스	Secure Web 22.9.0: 현재 버전의 새로운 기능
07 Sep 2022	Secure Mail 버전 22.9.0 릴리스	Secure Mail 22.9.0: 현재 버전의 새로운 기능
01 Sep 2022	iOS용 Secure Web 버전 22.9.0 릴리스	Secure Web 22.9.0은 2022년 9월 2일에 롤백되었습니다. 현재 수정 작업을 적극적으로 진행 중이며 곧 릴리스를 발표할 예정입니다.
01 Sep 2022	Secure Mail 버전 22.9.0 릴리스	Secure Mail 22.9.0은 2022년 9월 2일에 롤백되었습니다. 현재 수정 작업을 적극적으로 진행 중이며 곧 릴리스를 발표할 예정입니다.
26 Jul 2022	Android용 Secure Hub 버전 22.7.0 릴리스	Secure Hub 22.7.0: 현재 버전의 새로운 기능
13 Jul 2022	iOS용 Secure Web 버전 22.6.0 릴리스	Secure Web 22.6.0: 현재 버전의 새로운 기능
14 Jun 2022	Secure Mail 버전 22.6.0 릴리스	Secure Mail 22.6.0: 현재 버전의 새로운 기능
14 Jun 2022	Android용 Secure Web 버전 22.6.0 릴리스	Secure Web 22.6.0: 현재 버전의 새로운 기능
14 Jun 2021	Android용 Secure Hub 버전 22.6.0 릴리스	Secure Hub 22.6.0: 현재 버전의 새로운 기능
09 Feb 2022	Secure Mail 버전 22.2.0 릴리스	Secure Mail 22.2.0: 현재 버전의 새로운 기능

날짜	변경	설명
09 Feb 2022	Secure Web 버전 22.2.0 릴리스	Secure Web 22.2.0: 현재 버전의 새로운 기능
08 Dec 2021	Secure Mail 버전 21.12.0 릴리스	Secure Mail 21.12.0: 현재 버전의 새로운 기능
08 Dec 2021	Secure Web 버전 21.12.0 릴리스	Secure Web 21.12.0: 현재 버전의 새로운 기능
27 Oct 2021	Secure Mail 버전 21.10.5 릴리스	Secure Mail 21.10.5: 현재 버전의 새로운 기능
27 Oct 2021	Secure Web 버전 21.10.5 릴리스	Secure Web 21.10.5: 현재 버전의 새로운 기능
13 Oct 2021	Secure Hub 버전 21.10.0 릴리스	Secure Hub 21.10.0: 현재 버전의 새로운 기능
13 Oct 2021	Secure Mail 버전 21.10.0 릴리스	Secure Mail 21.10.0: 현재 버전의 새로운 기능
13 Oct 2021	Secure Web 버전 21.10.0 릴리스	Secure Web 21.10.0: 현재 버전의 새로운 기능
20 Sep 2021	Secure Mail 버전 21.9.1 릴리스	Secure Mail 21.9.1: 현재 버전의 새로운 기능
20 Sep 2021	Secure Web 버전 21.9.1 릴리스	Secure Web 21.9.1: 현재 버전의 새로운 기능
08 Sep 2021	Secure Mail 버전 21.9.0 릴리스	Secure Mail 21.9.0: 현재 버전의 새로운 기능
08 Sep 2021	Secure Web 버전 21.9.0 릴리스	Secure Web 21.9.0: 현재 버전의 새로운 기능
24 Aug 2021	Android용 Secure Mail 버전 21.8.5 릴리스	Secure Mail 21.8.5: 현재 버전의 새로운 기능
24 Aug 2021	Android용 Secure Web 버전 21.8.5 릴리스	Secure Web 21.8.5: 현재 버전의 새로운 기능

날짜	변경	설명
13 Aug 2021	iOS용 Secure Hub 버전 21.8.0 릴리스	Secure Hub 21.8.0: 현재 버전의 새로운 기능
13 Aug 2021	Secure Mail 버전 21.8.0 릴리스	Secure Mail 21.8.0: 현재 버전의 새로운 기능
13 Aug 2021	Secure Web 버전 21.8.0 릴리스	Secure Web 21.8.0: 현재 버전의 새로운 기능
10 Aug 2021	Android용 Secure Hub 버전 21.7.1 릴리스	Secure Hub 21.7.1: 현재 버전의 새로운 기능
15 Jul 2021	Secure Mail 버전 21.7.0 릴리스	Secure Mail 21.7.0: 현재 버전의 새로운 기능
15 Jul 2021	Secure Web 버전 21.7.0 릴리스	Secure Web 21.7.0: 현재 버전의 새로운 기능
07 Jul 2021	iOS용 Secure Hub 버전 21.7.0 릴리스	Secure Hub 21.7.0: 현재 버전의 새로운 기능
06 Jul 2021	Android용 Secure Hub 버전 21.7.0 릴리스	Secure Hub 21.7.0: 현재 버전의 새로운 기능
24 Jun 2021	iOS용 Secure Mail 버전 21.6.0 릴리스	Secure Mail 21.6.0: 현재 버전의 새로운 기능
16 Jun 2021	Secure Hub 버전 21.6.0 릴리스	Secure Hub 21.6.0: 현재 버전의 새로운 기능
16 Jun 2021	Android용 Secure Mail 버전 21.6.0 릴리스	Secure Mail 21.6.0: 현재 버전의 새로운 기능
16 Jun 2021	Secure Web 버전 21.6.0 릴리스	Secure Web 21.6.0: 현재 버전의 새로운 기능
20 May 2021	Secure Hub 버전 21.5.1 릴리스	Secure Hub 21.5.1: 현재 버전의 새로운 기능
12 May 2021	Secure Hub 버전 21.5.0 릴리스	Secure Hub 21.5.0: 현재 버전의 새로운 기능

날짜	변경	설명
12 May 2021	Secure Mail 버전 21.5.0 릴리스	Secure Mail 21.5.0: 현재 버전의 새로운 기능
12 May 2021	iOS용 Secure Web 버전 21.5.0 릴리스	Secure Web 21.5.0: 버그 수정
04 May 2021	Android용 Secure Mail 버전 21.4.5 릴리스	Secure Mail 21.4.5: 현재 버전의 새로운 기능
04 May 2021	Android용 Secure Web 버전 21.4.5 릴리스	Secure Web 21.4.5: 버그 수정
15 Apr 2021	Secure Hub 버전 21.4.0 릴리스	Secure Hub 21.4.0: 현재 버전의 새로운 기능
15 Apr 2021	iOS용 Secure Mail 버전 21.4.0 릴리스	Secure Mail 21.4.0: 버그 수정
31 Mar 2021	iOS용 Secure Hub 버전 21.3.2 릴리스	Secure Hub 21.3.2: 버그 수정
30 Mar 2021	Android용 Secure Mail 버전 21.3.5 릴리스	Secure Mail 21.3.5: 현재 버전의 새로운 기능
30 Mar 2021	Android용 Secure Web 버전 21.3.5 릴리스	Secure Web 21.3.0: 버그 수정
22 Mar 2021	iOS용 Secure Mail 버전 21.3.0 릴리스	Secure Mail 21.3.0: 현재 버전의 새로운 기능
17 Mar 2021	Secure Hub 버전 21.3.0 릴리스	Secure Hub 21.3.0: 버그 수정
17 Mar 2021	Android용 Secure Mail 버전 21.3.0 릴리스	Secure Mail 21.3.0: 현재 버전의 새로운 기능
17 Mar 2021	Android용 Secure Web 버전 21.3.0 릴리스	Secure Web 21.3.0: 버그 수정
24 Feb 2021	Secure Mail 버전 21.2.0 릴리스	Secure Mail 21.2.0: 현재 버전의 새로운 기능

날짜	변경	설명
24 Feb 2021	Secure Web 버전 21.2.0 릴리스	Secure Web 21.2.0: 현재 버전의 새로운 기능
18 Feb 2021	Android용 Secure Hub 버전 21.2.0 릴리스	Secure Hub 21.2.0: 버그 수정
01 Feb 2021	iOS용 Secure Mail 버전 21.1.5 릴리스	Secure Mail 21.1.5: 버그 수정
01 Feb 2021	iOS용 Secure Web 버전 21.1.5 릴리스	Secure Web 21.1.5: 버그 수정
14 Jan 2021	Secure Mail 버전 21.1.0 릴리스	Secure Mail 21.1.0: 버그 수정
14 Jan 2021	Secure Web 버전 21.1.0 릴리스	Secure Web 21.1.0: 버그 수정
12 Jan 2021	Secure Hub 버전 21.1.0 릴리스	Secure Web 21.1.0: 버그 수정
15 Dec 2020	Secure Hub 버전 20.12.0 릴리스	Secure Hub 20.12.0: 현재 버전의 새로운 기능
15 Dec 2020	iOS용 Secure Mail 버전 20.12.0 릴리스	Secure Mail 20.12.0: 버그 수정
15 Dec 2020	iOS용 Secure Web 버전 20.12.0 릴리스	Secure Web 20.12.0: 버그 수정
19 Nov 2020	Android용 Secure Hub 버전 20.11.0 릴리스	Secure Hub 20.11.0: 현재 버전의 새로운 기능
19 Nov 2020	Android용 Secure Mail 버전 20.11.0 릴리스	Secure Mail 20.11.0: 현재 버전의 새로운 기능
19 Nov 2020	Android용 Secure Web 버전 20.11.0 릴리스	Secure Web 20.11.0: 버그 수정
17 Nov 2020	iOS용 Secure Mail 버전 20.11.0 릴리스	Secure Mail 20.11.0: 현재 버전의 새로운 기능

날짜	변경	설명
17 Nov 2020	iOS용 Secure Web 버전 20.11.0 릴리스	Secure Web 20.11.0: 버그 수정
27 Oct 2020	Secure Mail 버전 20.10.5 릴리스	Secure Mail 20.10.5: 현재 버전의 새로운 기능
27 Oct 2020	Android용 Secure Web 버전 20.10.5 릴리스	Secure Web 20.10.5: 현재 버전의 새로운 기능
27 Oct 2020	iOS용 Secure Hub 버전 20.10.5 릴리스	Secure Hub 20.10.5: 버그 수정
21 Oct 2020	Android용 Secure Hub 버전 20.10.5 릴리스	Secure Hub 20.10.5: 버그 수정
15 Oct 2020	Secure Mail 버전 20.10.0 릴리스	Secure Mail 20.10.0: 현재 버전의 새로운 기능
15 Oct 2020	Android용 Secure Web 버전 20.10.0 릴리스	Secure Mail 20.10.0: 현재 버전의 새로운 기능
29 Sep 2020	Android용 Secure Mail 버전 20.9.5 릴리스	Secure Mail 20.9.5: 버그 수정
29 Sep 2020	iOS용 Secure Web 버전 20.9.5 릴리스	Secure Web 20.9.5: 버그 수정
17 Sep 2020	Secure Mail 버전 20.9.0 릴리스	Secure Mail 20.9.0: 버그 수정
17 Sep 2020	Android용 Secure Web 버전 20.9.0 릴리스	Secure Web 20.9.0: 현재 버전의 새로운 기능
04 Sep 2020	Secure Hub 버전 20.9.0 릴리스	Secure Hub 20.9.0: 현재 버전의 새로운 기능
27 Aug 2020	Secure Mail 버전 20.8.5 릴리스	Secure Mail 20.8.5: 현재 버전의 새로운 기능
27 Aug 2020	Secure Web 버전 20.8.5 릴리스	Secure Web 20.8.5: 현재 버전의 새로운 기능

날짜	변경	설명
20 Aug 2020	Secure Hub 버전 20.7.5 릴리스	Secure Hub 20.7.5: 현재 버전의 새로운 기능
19 Aug 2020	Secure Mail 버전 20.8.0 릴리스	Secure Mail 20.8.0: 현재 버전의 새로운 기능
19 Aug 2020	Secure Web 버전 20.8.0 릴리스	Secure Web 20.8.0: 현재 버전의 새로운 기능
12 Aug 2020	Citrix ShareConnect가 EOL(수명 종료)에 도달했습니다.	자세한 내용은 제품 매트릭스 의 제품 수명 주기 단계를 참조하십시오.
29 Jul 2020	Secure Mail 버전 20.7.5 릴리스	Secure Mail 20.7.5: 현재 버전의 새로운 기능
29 Jul 2020	Secure Web 버전 20.7.5 릴리스	Secure Web 20.7.5: 버그 수정
14 Jul 2020	Secure Mail 버전 20.7.0 릴리스	Secure Mail 20.7.0: 버그 수정
14 Jul 2020	Secure Web 버전 20.7.0 릴리스	Secure Web 20.7.0: 현재 버전의 새로운 기능
10 Jul 2020	Wi-Fi 설정에 구성된 프록시 서버를 사용하려면 iOS 장치에 구성된 프록시를 사용하도록 설정합니다.	Secure Hub의 새로운 기능 에서 자세한 내용을 확인하십시오.
06 Jul 2020	앱의 경우 32비트에서 64비트로 전환합니다. 최신 버전으로 업그레이드할 때 재인증이 발생하지 않도록 Android 장치를 Secure Hub 버전 20.6.5로 업그레이드합니다.	Secure Hub의 새로운 기능 에서 자세한 내용을 확인하십시오.
01 Jul 2020	Secure Hub 버전 20.6.5 릴리스	Secure Hub 20.6.5: 버그 수정

날짜	변경	설명
01 Jun 2020	Secure Mail 버전 20.6.5 릴리스	Secure Mail 20.6.5: 버그 수정
19 Jun 2020	QuickEdit의 플랫폼 암호화	QuickEdit 암호화 의 세부 정보 보기
16 Jun 2020	Secure Mail 버전 20.6.0 릴리스	Secure Mail 20.6.0: 버그 수정
16 Jun 2020	Secure Web 버전 20.6.0 릴리스	Secure Web 20.6.0: 버그 수정
02 Jun 2020	MDX 암호화 수명 종료가 빠르게 다가오고 있습니다. 2020년 9월 1일 이전에 모든 장치를 플랫폼 암호화로 이동해야 합니다.	최근 발표 내용 에서 세부 정보 보기
19 May 2020	iOS용 Secure Mail 버전 20.5.0 릴리스	Secure Mail 20.5.0: 버그 수정
19 May 2020	iOS용 Secure Web 버전 20.5.0 릴리스	Secure Web 20.5.0: 버그 수정
11 May 2020	iOS용 Secure Mail 버전 20.4.5 릴리스	Secure Mail 20.4.5: 현재 버전의 새로운 기능
11 May 2020	iOS용 Secure Web 버전 20.4.5 릴리스	Secure Web 20.4.5: 현재 버전의 새로운 기능
28 Apr 2020	Android용 Secure Mail 버전 20.4.5 릴리스	Secure Mail 20.4.5: 현재 버전의 새로운 기능
28 Apr 2020	Android용 Secure Web 버전 20.4.5 릴리스	Secure Web 20.4.5: 버그 수정
21 Apr 2020	iOS용 Secure Mail 버전 20.4.0 릴리스	Secure Mail 20.4.0: 현재 버전의 새로운 기능
21 Apr 2020	iOS용 Secure Web 버전 20.4.0 릴리스	Secure Web 20.4.0: 버그 수정

날짜	변경	설명
14 Apr 2020	Android용 Secure Mail 버전 20.4.0 릴리스	Secure Mail 20.4.0: 현재 버전의 새로운 기능
14 Apr 2020	Android용 Secure Web 버전 20.4.0 릴리스	Secure Web 20.4.0: 버그 수정
31 Mar 2020	iOS용 Secure Hub 버전 20.3.0 릴리스	Secure Hub 20.3.0: 현재 버전의 새로운 기능
24 Mar 2020	Secure Mail 버전 20.3.0 릴리스	Secure Mail 20.3.0: 현재 버전의 새로운 기능
24 Mar 2020	Secure Web 버전 20.3.0 릴리스	Secure Web 20.3.0: 버그 수정
11 Feb 2020	iOS용 Secure Hub 버전 20.2.0 릴리스	Secure Hub 20.2.0: 버그 수정
11 Feb 2020	Secure Mail 버전 20.2.0 릴리스	Secure Mail 20.2.0: 현재 버전의 새로운 기능
29 Jan 2020	Secure Hub 버전 20.1.5 릴리스	Secure Hub 20.1.5: 버그 수정
29 Jan 2020	Secure Mail 버전 20.1.5 릴리스	Secure Mail 20.1.5: 현재 버전의 새로운 기능
07 Jan 2020	Secure Mail 버전 20.1.0 릴리스	Secure Mail 20.1.0: 현재 버전의 새로운 기능
12 Dec 2019	Secure Hub 버전 19.12.5 릴리스	Secure Hub 19.12.5: 버그 수정
12 Dec 2019	Secure Mail 버전 19.12.5 릴리스	Secure Mail 19.12.5: 현재 버전의 새로운 기능
12 Dec 2019	Secure Web 버전 19.10.5 릴리스	Secure Web 19.12.5: 버그 수정
13 Nov 2019	Secure Mail 버전 19.11.5 릴리스	Secure Mail 19.11.5: 현재 버전의 새로운 기능

날짜	변경	설명
13 Nov 2019	Secure Web 버전 19.11.5 릴리스	Secure Web 19.11.5: 버그 수정
06 Nov 2019	Secure Hub 버전 19.11.5 릴리스	Secure Hub 19.11.5: 버그 수정
22 Oct 2019	iOS용 Secure Mail 버전 19.10.6 릴리스	iOS용 Secure Mail 19.10.6: 버그 수정
15 Oct 2019	Secure Mail 버전 19.10.5 릴리스	Secure Mail 19.10.5: 현재 버전의 새로운 기능
15 Oct 2019	Secure Web 버전 19.10.5 릴리스	Secure Web 19.10.5: 버그 수정
14 Oct 2019	Android용 Secure Hub 버전 19.10.5 릴리스	Secure Hub 19.10.5: 현재 버전의 새로운 기능
03 Oct 2019	iOS용 Secure Hub 버전 19.10.0 릴리스	Secure Hub 19.10.0: 버그 수정
03 Oct 2019	iOS용 Secure Mail 버전 19.10.0 릴리스	Secure Mail 19.10.0: 현재 버전의 새로운 기능
03 Oct 2019	iOS용 Secure Web 버전 19.10.0 릴리스	Secure Web 19.10.0: 현재 버전의 새로운 기능
01 Oct 2019	Android용 Secure Mail 버전 19.10.0 릴리스	Secure Mail 19.10.0: 현재 버전의 새로운 기능
01 Oct 2019	Android용 Secure Web 버전 19.10.0 릴리스	Secure Web 19.10.0: 현재 버전의 새로운 기능
24 Sep 2019	Android용 Secure Hub 버전 19.10.0 릴리스	Secure Hub 19.10.0: 버그 수정
19 Sep 2019	iOS용 Secure Mail 버전 19.9.5 릴리스	Secure Mail 19.9.5: 현재 버전의 새로운 기능
19 Sep 2019	iOS용 Secure Web 버전 19.9.5 릴리스	Secure Web 19.9.5: 버그 수정

날짜	변경	설명
17 Sep 2019	Android용 Secure Mail 버전 19.9.5 릴리스	Secure Mail 19.9.5: 현재 버전의 새로운 기능
17 Sep 2019	Android용 Secure Web 버전 19.9.5 릴리스	Secure Web 19.9.5: 현재 버전의 새로운 기능
11 Sep 2019	Android용 Secure Hub 버전 19.9.5 릴리스	Secure Hub 19.9.5: 현재 버전의 새로운 기능
04 Sep 2019	Secure Mail 버전 19.9.0 릴리스	Secure Mail 19.9.0: 현재 버전의 새로운 기능
04 Sep 2019	Secure Web 버전 19.9.0 릴리스	Secure Web 19.9.0: 현재 버전의 새로운 기능
03 Sep 2019	Secure Hub 버전 19.9.0 릴리스	Secure Hub 19.9.0: 현재 버전의 새로운 기능
23 Aug 2019	Secure Hub 버전 19.8.5 릴리스	Secure Hub 19.8.5: 현재 버전의 새로운 기능
23 Aug 2019	Android용 Secure Mail 버전 19.8.5 릴리스	Secure Mail 19.8.5: 성능 개선 사항 및 버그 수정
23 Aug 2019	Android용 Secure Web 버전 19.8.5 릴리스	Secure Web 19.8.5: 성능 개선 사항 및 버그 수정
09 Aug 2019	Android용 Secure Mail 버전 19.8.0 릴리스	Secure Mail 19.8.0: 현재 버전의 새로운 기능
09 Aug 2019	Android용 Secure Web 버전 19.8.0 릴리스	Secure Web 19.8.0: 성능 개선 사항 및 버그 수정
31 Jul 2019	Secure Hub 버전 19.8.0 릴리스	Secure Hub 19.8.0: 현재 버전의 새로운 기능
02 Aug 2019	iOS용 Secure Mail 버전 19.8.0 릴리스	Secure Mail 19.8.0: 현재 버전의 새로운 기능
02 Aug 2019	iOS용 Secure Web 버전 19.8.0 릴리스	Secure Web 19.8.0: 성능 개선 사항 및 버그 수정

날짜	변경	설명
18 Jul 2019	Secure Hub 버전 19.7.5 릴리스	Secure Hub 19.7.5: 현재 버전의 새로운 기능
18 Jul 2019	Secure Mail 버전 19.7.5 릴리스	Secure Mail 19.7.5: 현재 버전의 새로운 기능
18 Jul 2019	Secure Web 버전 19.7.5 릴리스	Secure Web 19.7.5: 성능 개선 사항 및 버그 수정
30 Jun 2019	iOS용 Secure Hub 버전 19.6.6 릴리스	iOS용 Secure Hub 19.6.6: 성능 개선 사항 및 버그 수정
27 Jun 2019	Android용 Secure Mail 19.6.5의 새로운 기능 목록	Secure Mail 19.6.5: 현재 버전의 새로운 기능
27 Jun 2019	Secure Web 버전 19.6.5 릴리스	Secure Web 19.6.5: 성능 개선 사항 및 버그 수정
26 Jun 2019	Secure Hub 버전 19.6.5 릴리스	Secure Hub 19.6.5: 알려진 문제
17 Jun 2019	iOS용 Secure Mail 19.5.5의 새로운 기능 목록	Secure Mail 19.5.5: 현재 버전의 새로운 기능
05 Jun 2019	Android용 Secure Hub, Secure Mail 및 Secure Web 버전 19.5.5 릴리스	Secure Mail 및 Secure Web의 단계별 릴리스 프로세스를 이해하려면 모바일 생산성 앱 릴리스 일정 을 참조하십시오.
23 May 2019	Android용 Secure Mail 임시 보관함 동기화 기능에 대한 1분 비디오	Android용 Secure Mail 버전 19.5.0에서 릴리스된 임시 보관함 폴더 동기화 기능에 대한 비디오를 추가했습니다. 임시 보관함 폴더 자동 동기화
08 May 2019	Secure Hub 버전 19.5.0 릴리스	Secure Hub 19.5.0 알려진 문제 및 해결된 문제
08 May 2019	Secure Mail 버전 19.5.0 릴리스	Secure Mail 19.5.0 해결된 문제

날짜	변경	설명
08 May 2019	Secure Web 19.5.0 릴리스	Secure Web 19.5.0 수정 문제
05 Apr 2019	Secure Hub 버전 19.3.5 릴리스	Secure Hub 19.3.5 알려진 문제 및 수정된 문제
05 Apr 2019	Secure Mail 버전 19.3.5 릴리스	Secure Mail 19.3.5 해결된 문제
05 Apr 2019	Secure Web 19.3.5 릴리스	Secure Web 19.3.5 수정 문제