정책 - Apple

Apple 정책
앱 및 프로필
키오스크 및 홈 화면
암호
제한
네트워킹
소프트웨어 업데이트
macOS
위치 및 지오펜스
계정
규정 준수 규칙

Apple 정책
Apple 정책은 Cerberus Enterprise가 MDM을 통해 Apple 기기에 적용하는 관리 설정을 정의합니다 . 이러한 설정은 대시보드의 Apple 정책 편집기에서 구성합니다 .

시작하기 전에

Apple 기기 관리를 위해서는 Apple Management(APNs)가 구성되어 있어야 합니다. 필요한 경우 Apple

Management 설정 (APNs) 페이지를 읽어 보십시오.

Apple 정책 편집기 열기
대시보드에서 정책 을 열고 새 Apple 정책 만들기 를 클릭하십시오 . 기존 Apple 정책을 편집하려면 정책 표에서 해당 행을 클릭하십시오 .

편집기 레이아웃
Apple 정책 편집기는 확장 가능한 섹션 집합으로 구성됩니다 . 페이지 상단에서는 항상 다음을 편집할 수 있습니다:

이름 (필수)
ID (읽기 전용)
설명 (선택 사항)

정책 섹션
아래 섹션은 현재 Apple 정책 편집기에서 사용할 수 있는 패널과 일치합니다 . 저장된 정책을 열면 설정이 변경된 섹션은 이미 열려 있고 나머지는 닫혀 있습니다:

앱 관리: 앱 관련 제한, 관리되는 앱 및 Cerberus Enterprise 앱 설정을 구성합니다 .
키오스크 및 홈 화면: 단일 앱 모드, 허용 및 차단된 앱, 홈 화면 레이아웃, 웹 클립, 알림 설정 및
잠금 화면 메시지.
보안: 자동 잠금 해제 및 생체 인증 잠금 해제와 같은 기능을 제어합니다 .

암호 설정: 암호 요구 사항 및 관련 규칙을 구성합니다 .
멀티미디어 : 카메라 및 관련 기능을 허용 /허용하지 않습니다.
셀룰러: 셀룰러 관련 설정 (앱 셀룰러 데이터 설정, eSIM, 요금제 변경)과 셀룰러 APN을 제어합니다 . 네트워킹 : Wi-Fi 네트워크 (엔터프라이즈 802.1X 포함), VPN, 인증서, 전역 프록시, 암호화된 DNS 및 웹 콘텐츠 필터, AirDrop 및 Bluetooth와 같은 연결 제한을 구성합니다 .
시스템 및 사용자 인터페이스 : Handoff, 기기 이름, 화면 보호기와 같은 시스템 기능을
제한합니다 .
소프트웨어 업데이트 : 기한까지 OS 버전을 요구하고 업데이트가 다운로드 및 설치되는 방식을 제어합니다 .
macOS: Mac의 방화벽, Gatekeeper, 화면 보호기 및 잠금, 외부 및 네트워크 저장 공간, 화면 공유 , 개인정보 보호 권한 및 로그인 항목.
Apple 앱 및 서비스: iMessage, Game Center, 나의 찾기와 같은 Apple 앱 및 서비스를
제한합니다 .
Siri 및 Apple Intelligence: Siri, 받아쓰기 및 Apple Intelligence 기능을 제한합니다 . iCloud: 특정 iCloud 서비스 (백업, 키체인 동기화, 비공개 릴레이 등)를 허용하거나 허용하지 않습니다.
위치 및 지오펜스 : Cerberus Enterprise 앱이 설치된 iPhone 및 iPad가 들어가거나 나갈 때 보고하는 영역으로, 이벤트 규칙에 사용됩니다 .
계정: 계정 수정을 제한하고 Mail, Exchange, Google, 캘린더, 연락처 및 디렉터리 계정을
구성합니다 .
규정 준수 규칙: 기기를 규정 비준수 상태로 만드는 요구 사항 (암호, 최소 OS 버전, 감독, FileVault)이며, 선택적 차단이 있습니다.

Apple 정책 편집기의 많은 옵션에는 요구 사항 및 지원되는 OS 버전을 설명하는 도구 설명이 포함되어 있습니다.

저장, 삭제 및 연결된 기기
정책 저장 을 사용하여 변경 사항을 적용하십시오 . 보류 중인 편집이 없거나 라이선스가 만료된 경우 버튼이 비활성화됩니다 .

기존 정책을 편집할 때 페이지에는 정책 삭제 동작도 표시됩니다 . 편집기 하단에 연결된 기기 목록이 표시되어 현재 정책을 사용 중인 기기 수를 확인할 수 있습니다.

다음 페이지
앱 & 프로필: 설치된 앱 및 구성 프로필을 구성합니다 .
키오스크 및 홈 화면: 단일 앱 모드, 허용된 앱, 홈 화면 레이아웃 및 웹 클립.
암호: 암호 요구 사항 및 관련 보안 옵션을 구성합니다 .
제한: 허용되는 기능 및 OS 수준 제한을 정의합니다 .

네트워킹: Wi-Fi 네트워크, VPN, 인증서 및 연결 제한.
소프트웨어 업데이트: 필수 OS 업데이트 및 소프트웨어 업데이트 설정.
macOS: Mac의 방화벽, Gatekeeper, 화면 잠금, 저장 공간, 개인정보 보호 권한 및 로그인 항목. 위치 및 지오펜스: iPhone 및 iPad가 들어가고 나가는 것을 보고하는 영역과 작동에 필요한 사항. 계정: 메일, Exchange, Google, 캘린더, 연락처 및 디렉터리 계정.
규정 준수 규칙: 기기에 대한 요구 사항 및 비준수 기기 차단.

앱 및 프로필
이 섹션에서는 Apple 기기의 관리형 애플리케이션과 계정 페이로드를 구성하는 방법을 설명합니다 .

앱 관리
앱 관리 패널에는 앱 관련 일반 제한과 관리형 앱 목록이 모두 포함되어 있습니다.

일반 앱 제한

App Clips 허용
앱 설치 허용
앱 제거 허용
자동 앱 다운로드 허용
앱 숨기기 허용
앱 잠금 허용
앱 내 구입 허용
기본 브라우저 수정 허용
엔터프라이즈 앱 신뢰 허용

관리형 앱

애플리케이션 추가 를 사용하여 정책에 앱을 추가합니다 . 각 관리형 앱은 카드로 표시됩니다 . 카드를 확장하여 설정을 편집하고 삭제 작업으로 앱을 제거할 수 있습니다.

App Store ID: 관리형 앱의 App Store 식별자입니다 .
번들 ID: 앱 번들 식별자입니다 .
설치 동작: 앱을 계속 설치해야 하는지 또는 사용자가 설치 /제거할 수 있는지 제어합니다 .
할당: Cerberus가 각 기기에 대해 선택하는 라이선스 유형으로, 회사 기기에는 기기 라이선스, 개인
iPhone 및 iPad(User Enrollment)에는 Managed Apple Account의 사용자 라이선스가
적용됩니다 . 이 필드는 변경할 수 없습니다.
VPP 라이선스 : App Store를 통해 설치하는 데 사용되는 VPP 라이선스 유형입니다 .

앱 선택 목록에는 각 앱의 사용 가능한 라이선스와 전체 라이선스가 표시됩니다 . 무료 앱에는 무제한 이 표시되며, Apple이 무제한 라이선스를 제공합니다 . 앱은 정책에 한 번만 추가할 수 있습니다. 정책에 이미
있는 앱과 동일한 App Store ID 또는 번들 ID를 가진 앱은 거부되며, 동일한 앱을 두 번 나열한 정책도 저장 시 거부됩니다 .

앱 선택 목록에는 Apple Business 라이브러리의 앱이 표시됩니다 . 앱을 추가하려면 Apple Business에서 Apps & Services → Apps & Books → App Store를 열고 앱을 검색한 후 View를 클릭합니다 . 무료
앱은 Add를 클릭하고 All current and future(또는 Apps and Books 토큰의 조직 단위)를 Organizational Units에서 선택한 다음 Add를 클릭하고 Review를 클릭해 확인합니다 . 유료 앱은 가격을 클릭하고 Managed Licenses를 License Type으로 선택한 후 (교환 코드는 Cerberus Enterprise에서 사용할 수 없음), Apps and Books 토큰의 Organizational Unit을 선택하고 Licenses 수를 입력한 다음 (주문당 최대 1,000개) Review를 클릭하고 구매합니다 . 먼저 Settings → Payments & Billing → Apps & Services → Payment Methods에서 결제 방법을 설정해야 합니다. 그러면 앱이 앱 선택 목록에
표시됩니다 .

개인 기기의 앱 (User Enrollment)
User Enrollment으로 등록된 개인 iPhone 및 iPad에는 일련번호가 없으므로, 기기에 로그인된 Managed Apple Account의 사용자 라이선스 로 정책의 App Store 앱을 받습니다. Cerberus는 해당 계정을 Apps and Books에 등록하고 무료 앱을 포함하여 라이선스를 직접 할당합니다 . Managed Apple Account와 Apps and Books 토큰은 동일한 Apple Business 조직에 속해야 합니다. 유료 앱은 계정당 라이선스 하나를 사용하며, 해당 계정의 모든 개인 기기가 이를 공유합니다 .

사용자 라이선스 대기 중: 앱은 Apple이 라이선스를 확인한 후에만 기기로 전송되며, 보통 몇 분
이내에 확인됩니다 . 기기의 애플리케이션 패널에 이유가 표시됩니다 .
사용자 라이선스 실패: 예를 들어 유료 앱에 남은 라이선스가 없어 Apple이 라이선스를 할당하지
못했습니다 . Apple Business에서 라이선스를 추가한 다음 다시 요청 을 사용하세요 . Cerberus도
매일 자동으로 다시 시도합니다 .
설치 프롬프트 : iOS는 각 앱을 설치하기 전에 사용자에게 묻습니다. 사용자가 취소하면 앱에
사용자의 설치 승인 대기 중 이 표시되며, 다시 요청 을 선택하면 프롬프트가 다시 표시됩니다 .
해제: 정책에서 앱을 제거하거나 계정의 마지막 개인 기기를 등록 해제하면 앱이 제거되고
라이선스가 해제됩니다 . 단, 동일한 계정의 다른 등록된 기기가 여전히 해당 앱을 필요로 하는
경우는 예외입니다 .

자세한 내용은 Apple 계정 기반 등록 을 참조하세요 .

관리형 구성

관리형 구성은 앱 공급업체가 문서화한 방식대로 앱에 설정 (예: 서버 주소 또는 계정 이름)을 제공합니다 . 정책에서 앱을 열고 관리형 구성 추가 를 클릭하세요 . 이 구성은 iOS 또는 iPadOS 18.4 이상 이 설치된 iPhone 및 iPad와 macOS 27 이상 이 설치된 Mac으로 전송되며, Apple Vision Pro에는 아직 전송되지 않습니다. 앱이 관리형 구성을 지원해야 하며, 이를 읽지 않는 앱은 무시합니다 . 앱 패널에는 앱 이름 옆에 키 수가 표시됩니다 .

키: 각 행에는 키, 유형, 값이 있습니다. 유형은 Text, Integer, Decimal number, Boolean, Date,
Text list, Integer list입니다. 키는 대소문자를 구분하며 고유해야 합니다. 키 추가 는 행을 추가하고
, 구성 제거 는 모든 키를 제거합니다 .

변수: Text 및 Text list 값에는 $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$, $UDID$를 포함할 수 있으며, 각 기기와 해당 사용자의 값으로 대체됩니다 . 값이 없는 변수 (예: 사용자가 없는 기기의 $EMAIL$)는 비워 두며 시스템 로그에 그렇게 기록됩니다 . 사용자 세부 정보가 변경되면
기기에 새 값이 적용됩니다 . Google Directory에서 동기화된 사용자의 경우 정책 또는 기기가
다음에 변경될 때 값이 업데이트됩니다 .
구성 가져오기 : 앱 공급업체가 MDM용으로 게시한 파일을 열거나 붙여넣은 다음 읽기 를
클릭합니다 . AppConfig 사양 파일 (specfile.xml)에는 앱이 지원하는 모든 키와 해당 설명, 유형, 기본값, 허용된 값이 나열됩니다 . 가져올 키를 선택하고 (기본값이 있는 키는 이미 선택됨) 가져온 후 나머지를 입력합니다 . 사양 파일이 다른 앱용이면 경고가 표시됩니다 . 속성 목록 (전체 속성 목록 또는 해당 <dict>만)은 그대로 가져옵니다 . 그런 다음 현재 키를 바꿀지 추가할지 선택합니다 . 중첩된 사전, 데이터 값, 혼합되거나 알 수 없는 유형의 목록은 지원되지 않으며 건너뛴 것으로 표시됩니다 . Apple은 앱의 구성 키를 게시하지 않으므로 문서에 없으면 공급업체에 파일을
요청하세요 . plist로 복사 는 변수가 대체되기 전에 기기가 받는 그대로의 구성을 복사합니다 . 제한: 앱당 최대 200개 키, 키당 최대 255자, 텍스트 값 최대 4,096자, 목록당 최대 200개 항목 (항목당 최대 1,024자), 1970~9999년 사이의 날짜, 앱당 전체 64 KB입니다.
비밀번호에는 사용하지 마세요: 구성은 구성된 기기로만 전송되고 로그에는 키 이름과 유형만 표시되지만 , 대시보드 관리자는 값을 읽을 수 있으며 기기가 구성을 다운로드하는 주소가 값에 따라 변경되므로 추측하기 쉬운 값 (부울 또는 작은 숫자)은 유추될 수 있습니다. 관리형 구성에
비밀번호나 기타 비밀을 넣지 마세요.
상태: 기기에서 앱이 구성을 수락하지 않았다고 보고하면 기기의 애플리케이션 패널에서 앱 옆에
구성이 수락되지 않음 이 표시됩니다 . 이는 기기를 규정 미준수 상태로 만들지 않습니다. 기기가
다운로드할 수 없는 구성은 기기를 규정 미준수 상태로 만듭니다.

앱 옵션

정책의 각 앱 (App Store 및 사용자 지정 앱)에는 이러한 옵션이 있습니다. 기기 기본값 은 선택을 기기에 맡깁니다. 옵션을 지원하지 않는 기기에는 해당 옵션이 적용되지 않지만 앱은 계속 설치됩니다 .

자동 업데이트 : App Store 설정, 항상 또는 안 함. iOS, iPadOS, macOS, visionOS 26 이상.
사용자 지정 앱의 경우 App Store 설정은 안 함처럼 동작합니다 .
셀룰러를 통한 다운로드 : 자동 설치 및 업데이트에 대한 App Store 설정, 항상 또는 안 함. 감독된 iPhone 및 iPad(iOS 또는 iPadOS 26 이상)에만 적용됩니다 .
앱 데이터 백업: 앱 데이터가 기기 백업에 포함되는지 여부입니다 . Mac에서는 지원되지 않습니다. 사용자가 앱을 숨길 수 있음 및 사용자가 앱을 잠글 수 있음: iOS 및 iPadOS 18.1 이상, 감독된 기기에서 적용됩니다 . 잠금을 허용하지 않으면 숨기기도 방지됩니다 . 앱 숨기기 허용 및 앱 잠금 허용 제한은 모든 앱에 적용됩니다 .
고객 PIN이 필요한 Tap to Pay 거래 후 기기 잠금: iPhone에만 적용됩니다 .
연결된 도메인: 앱이 연결된 도메인 (예: 유니버설 링크 또는 비밀번호 자동 완성용)이며 최대 50 개입니다. applinks:, 와일드카드 또는 ?mode= 없이 www.example.com 같은 일반 호스트
이름을 입력하세요 . Mac에서는 지원되지 않습니다.
도메인 직접 확인: 기기가 Apple 서버를 거치지 않고 도메인의 사이트 연결 파일을 직접
확인합니다 . 인터넷에서 접근할 수 없는 내부 도메인에만 활성화하세요 .
제거: 필수 로 설치된 앱은 사용자가 제거할 수 없습니다.

Mac App Store 앱
앱 선택 목록에는 각 앱의 플랫폼 (iPhone/iPad, Mac, Apple TV, Vision)이 표시되며, Mac 전용 앱은 Mac 아이콘이 표시됩니다 . Mac 전용 앱은 추가하면 Mac에 적용됩니다 . Mac 버전이 없는 App Store 앱은 Mac 으로 전송되지 않으며, 정책의 적용 대상 아래에 "이 앱에는 Mac 버전이 없으므로 Mac으로 전송되지
않습니다 "가 표시됩니다 . Mac은 App Store ID로 App Store 앱을 받으므로 Mac에서 번들 ID가 다른 앱도 올바르게 설치됩니다 .

Cerberus Enterprise 앱
Cerberus는 Cerberus Enterprise 앱을 iOS 또는 iPadOS 18.4 이상 이 (가) 설치된 모든 iPhone 및 iPad에 정책 유무와 관계없이 설치합니다 . 앱은 기기 위치를 공유하고 알림 및 실시간 추적 요청을 받습니다. 필수 로 설치되며 Apps and Books의 기기 라이선스 (개인 기기에서는 사용자 라이선스)를 사용하므로
사용자가 삭제할 수 없습니다.

일회성 설정: 무료 앱을 라이브러리에 한 번 추가합니다 . Apple Business에서 Apps & Services
→ Apps & Books → App Store를 열고 "Cerberus Enterprise"를 검색한 후 View를 클릭하고,
Add를 클릭한 다음 All current and future를 Organizational Units에서 선택하고 Add를
클릭한 후 Review를 클릭해 확인합니다 . 앱에 Manage가 표시되면 이미 라이브러리에 있는
것이므로 앱을 열어 조직 단위가 All current and future units인지 확인하세요 . 그때까지
대시보드에는 배너가 표시되고 기기에는 앱이 설치되지 않은 것으로 표시됩니다 . 계정 설정 을 참조하세요 .
정책에 포함할 수 없음: 이 앱은 정책에 추가할 수 없습니다. 앱 선택 목록에서 비활성화되고
사용자 지정 앱 (동일한 번들 ID)으로도 거부됩니다 . 이미 이 앱을 나열한 정책은 열 때 해당 항목이 제거되며, 정책을 저장하여 확인합니다 .
설치되지 않는 기기: iOS 또는 iPadOS 18.4 이전 버전의 기기입니다 . Shared iPad는 설치가 지원되지만 해당 기기에서 앱 기능은 검증되지 않았습니다 .
개인 기기: User Enrollment로 등록된 iPhone 및 iPad에도 설치 프롬프트와 Managed Apple Account의 사용자 라이선스와 함께 앱이 설치됩니다 . 앱은 조직에서 보낸 메시지를 받으며,
정책에서 개인 기기의 위치 및 지오펜스 를 켜고 사용자가 허용하지 않는 한 위치에 접근하지 않습니다.
설치 유지: Apps and Books 토큰이 만료되거나 앱이 라이브러리에서 제외되어도 앱은 기기에
남아 있으며, 기기 페이지에는 Apps and Books에 주의가 필요하다고 표시됩니다 . 24시간 후에도
앱이 라이브러리에 없을 때만 제거됩니다 .

사용자 지정 앱

사용자 지정 앱은 App Store 없이 배포되는 조직의 iPhone 및 iPad 앱 (.ipa 파일)입니다. Xcode에서 Enterprise 배포용으로 앱을 내보내거나 (Apple Developer Enterprise Program: 모든 기기에 설치됨) Ad Hoc 배포용으로 내보냅니다 (해당 프로비저닝 프로필에 등록된 기기에만 설치됨). App Store 빌드는
업로드할 수 없습니다.

사용자 지정 앱 추가 를 클릭하여 조직의 사용자 지정 앱을 엽니다. 앱 업로드 는 .ipa 파일 (최대 2GB)을 추가합니다 . 앱을 선택하고 정책에 추가 를 클릭합니다 . 목록에는 버전, 서명 유형, Ad Hoc 앱 프로필의 기기 수, 프로비저닝 프로필 만료 날짜가 표시됩니다 .

새 버전: 동일한 번들 ID로 앱을 업로드합니다 . 이전 버전을 대체하며, 해당 앱을 사용하는 정책의
기기가 앱을 업데이트합니다 .
요구 사항: iOS 17.2 이상이 설치된 iPhone 및 iPad. 앱을 설치할 수 없는 기기에는 앱이 제공되지
않습니다. 예를 들어 iPhone에서 iPad 전용 앱, 앱에 필요한 것보다 오래된 iOS, Ad Hoc 앱
프로필에 없는 기기, 만료된 프로비저닝 프로필 등이 해당됩니다 .
만료: 프로비저닝 프로필이 만료되면 앱이 더 이상 열리지 않습니다. 만료 날짜 전에 새 프로필로
서명된 버전을 업로드하세요 .
예약된 번들 ID: Cerberus Enterprise 앱의 번들 ID(com.lsdroid.Cerberus.Enterprise)를
사용하는 사용자 지정 앱은 Cerberus가 해당 앱을 직접 설치하므로 정책에 추가할 수 없습니다. 삭제: 먼저 해당 정책에서 앱을 제거하세요 . 그러면 기기에서 앱이 제거됩니다 .

Mac 패키지

사용자 지정 앱은 Mac 설치 패키지 (.pkg 파일)도 지원합니다 . 패키지는 productbuild로 빌드한 배포 패키지여야 하며 (pkgbuild로만 만든 구성 요소 패키지는 거부됨), Developer ID Installer 인증서로
서명해야 합니다. 공증하고 티켓을 스테이플링하는 것 (notarytool 및 stapler)을 권장합니다 . 서명되지
않은 패키지, 서명 후 변경된 패키지, 다른 인증서로 서명된 패키지는 거부됩니다 .

앱 업로드 로 .pkg 파일을 업로드하고 정책에 추가하세요 . 그러면 Mac 패키지 아래에 표시됩니다 . iPhone과 iPad는 이를 무시합니다 .

macOS 26 이상 을 실행하는 Mac(감독됨, 수동으로 등록한 Mac 포함, 사용자 등록 제외)은 패키지를 선언 으로 받습니다. Mac이 스스로 다운로드, 설치, 재시도, 업데이트하고 상태를 보고합니다 . 구형 Mac과 관리형 앱으로 설치된 패키지는 모든 macOS 버전에서 MDM 명령 으로 받습니다. macOS 26으로 업그레이드된
Mac은 자동으로 선언 방식으로 전환되며, 각 패키지를 한 번 더 설치할 수 있습니다. Mac이 동일한 패키지가 포함된 다른 정책으로 이동할 때도 같은 일이 발생할 수 있습니다.

새 버전: 동일한 패키지 식별자로 패키지를 업로드하세요 . 이전 버전을 대체하며, 해당 패키지를
사용하는 정책의 Mac이 새 버전을 설치합니다 .
건너뛴 Mac: 패키지가 허용하는 것보다 오래된 macOS를 실행하는 Mac과 Apple silicon
전용으로 빌드된 패키지의 경우 Intel Mac입니다. 기기 페이지에서 패키지가 건너뜀으로 표시되고
이유가 나옵니다. 이전에 설치된 버전은 Mac에 그대로 남습니다.
설치: 필수 (기본값)는 Mac에 패키지를 설치하고, 선택 사항 은 설치하지 않고 Mac에서 패키지를
사용할 수 있게 합니다. macOS 26은 시스템 설정이나 App Store에서 사용자에게 선택 사항
패키지를 표시하지 않으므로 (macOS 26.3에서 테스트), Mac의 앱이나 스크립트가 이를 설치해야 합니다. 그런 것이 있을 때만 선택 사항을 선택하세요 . macOS 26 이상 Mac에 적용되며, 구형 Mac 은 항상 패키지를 설치합니다 . 관리형 앱으로 설치된 패키지에는 이 선택을 사용할 수 없습니다. 정책에서 나갈 때 패키지 파일 제거 (macOS 27 이상): 패키지가 정책에서 제거되면 macOS 27 이상 Mac이 설치한 파일을 삭제합니다 . 기본적으로 꺼져 있습니다. 구형 Mac에서는 파일이 남습니다. 관리형 앱으로 설치된 패키지에는 사용할 수 없습니다.

- [illegible] : [illegible] [illegible] (macOS 11 [illegible], [illegible] [illegible]). [illegible] macOS[illegible] [illegible] [illegible] [illegible] MDM[illegible] [illegible] [illegible] [illegible] . [illegible] [illegible] [illegible] [illegible] [illegible] [illegible], **Developer ID Application** [illegible] [illegible] [illegible] [illegible] . macOS 11~13[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] (Gatekeeper [illegible] [illegible] [illegible]). [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] . Mac[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [

정책에 계정 페이로드를 추가하려면 Google 계정 추가 또는 메일 계정 추가 를 사용하세요 . 각 계정은 구성 필드와 함께 카드로 표시됩니다 .

사용자의 계정 자격 증명

Google 및 메일 계정 카드에는 모두 사용자의 계정 자격 증명 토글이 있습니다. 활성화하면 시스템이
사용자별로 계정 자격 증명을 적용합니다 . 비활성화하면 정책에 계정 ID를 직접 입력합니다 .

Google 계정 필드
표시 이름: 사용자에게 표시되는 계정 이름입니다 .
Google 이메일 주소: 사용자 이메일 주소입니다 .
전체 이름: 사용자의 전체 이름입니다 .

메일 계정 필드

메일 계정에는 ID 필드와 수신 /발신 서버 구성이 포함됩니다 . 호스트 이름은 필수입니다 .

표시 이름: 사용자에게 표시되는 메일 계정 이름입니다 .
이메일 주소: 사용자 이메일 주소입니다 .
전체 이름: 사용자의 전체 이름입니다 .

수신 서버

서버 유형: 메일 프로토콜 (예: IMAP 또는 POP)입니다.
인증 방법: 서버의 인증 방법입니다 .
IMAP 경로 접두사: 서버 유형이 IMAP일 때만 표시됩니다 . 호스트 이름: 필수입니다 .
포트: 서버 포트 (1–65535)입니다.

발신 서버

인증 방법
호스트 이름: 필수입니다 .
포트: 서버 포트 (1–65535)입니다.

S/MIME 옵션

메일 계정의 경우 S/MIME 암호화 및 서명 동작도 구성할 수 있습니다.

암호화

- **S/MIME** 암호화
- **ID** 사용자 재정의 가능
- 메시지별 스위치 활성화됨
- 사용자 재정의 가능

서명

- **S/MIME** 서명
- **ID** 사용자 재정의 가능
- 사용자 재정의 가능

> 계정 및 제한 옵션에는 대시보드에 필수 조건과 지원되는 OS 버전을 설명하는 도구 설명이 포함됩니다.

키오스크 및 홈 화면
키오스크 및 홈 화면 섹션은 기기를 하나의 앱에 고정하고, 열 수 있는 앱을 선택하고, 홈 화면을 정렬하고, 웹 사이트 아이콘을 추가합니다 . 각 설정은 구성 프로필로 기기에 설치됩니다 .

Apple은 이러한 설정 대부분을 감독되는 iPhone 및 iPad(Automated Device Enrollment로
등록되었거나 Apple Configurator로 준비된 기기)에만 적용합니다 . 다른 기기에는 적용되지 않습니다.
웹 클립은 감독되지 않은 iPhone 및 iPad에서도 작동합니다 . Mac에는 이러한 설정이 적용되지
않습니다.

앱 선택
앱은 번들 ID로 식별됩니다 . 앱 이름을 입력하여 내장 Apple 앱과 정책의 앱에서 선택하거나 , com.example.app 같은 번들 ID를 직접 입력하세요 .

단일 앱 모드
기기는 선택한 앱만 실행합니다 . 사용자는 홈 화면으로 돌아가거나 다른 앱을 열 수 없습니다. 먼저 정책으로 앱을 설치하세요 . 설정을 끄거나 앱을 제거하면 기기가 단일 앱 모드에서 벗어납니다 .

옵션: 터치 스크린, 회전, 볼륨 버튼, 벨소리 /무음 스위치, 측면 버튼 또는 자동 잠금을 비활성화하고 , VoiceOver 또는 Zoom 같은 손쉬운 사용 기능을 켭니다.
사용자가 켤 수 있는 손쉬운 사용 기능: 사용자가 측면 버튼을 세 번 클릭하여 켤 수 있는
기능입니다 .

허용 및 차단된 앱
차단된 앱: 기기는 이러한 앱을 숨기고 열지 않습니다. com.apple.webapp 은 (는) 모든 웹 클립을
차단합니다 . 설정 및 iPhone의 경우 전화는 차단할 수 없습니다.
일부 앱만 허용: 기기에서 이러한 앱만 표시합니다 . 목록을 비워 두면 모든 앱을 허용합니다 . 정책
앱 은 정책으로 설치된 앱을 추가하고, com.apple.webapp 는 모든 웹 클립을 허용합니다 .
단일 앱 모드를 시작할 수 있는 앱: 필요한 동안 (예: 시험 중) 기기를 자신에게 잠글 수 있는 앱입니다.

일부 앱만 허용 을 (를) 사용하면 목록에 없는 모든 앱이 기기에서 사라지며, 정책의 앱도
마찬가지입니다 . 설정 및 iPhone의 경우 전화는 항상 유지됩니다 .

홈 화면 레이아웃
홈 화면의 Dock과 페이지를 정렬합니다 . 추가 위치 로 위치를 선택하여 앱, 앱 폴더, 정책의 웹 클립을 추가하고, 아이콘을 드래그하여 Dock과 페이지 사이에서 이동하세요 . 폴더를 클릭하면 이름과 앱을 변경할 수 있습니다.

사용자는 아이콘을 이동하거나 홈 화면에서 앱을 제거할 수 없습니다. 레이아웃에 없는 앱은 정의한 페이지
뒤의 페이지로 이동합니다 . iPhone은 Dock에 아이콘 네 개를 표시합니다 . 사용자는 설정의 저장 공간
화면에서 필수가 아닌 앱을 여전히 삭제할 수 있습니다. 이를 방지하려면 앱 관리에서 앱 제거 허용 을 (를) 끄세요.

웹 클립
웹 클립은 홈 화면에서 웹 사이트를 여는 아이콘입니다 . 레이블과 URL, 선택적으로 이미지 (PNG 또는 JPEG, 정사각형으로 자름)를 설정하세요 .

사용자가 제거할 수 있음: 끄면 아이콘이 기기에 유지됩니다 .
전체 화면: 웹 사이트가 Safari 주소 표시줄 없이 웹 앱으로 열립니다. 다른 웹 사이트에서도 전체
화면 유지 를 사용하면 다른 웹 사이트로 가는 링크도 웹 앱에서 열립니다.
이 앱으로 열기: Safari 대신 URL을 여는 앱입니다.

알림 설정
일부 앱의 알림이 기기에 표시되는 방식을 선택하세요 . 허용 여부, 표시 위치 (잠금 화면, 알림 센터, CarPlay), 배지, 사운드, 중요 알림, 배너 스타일, 그룹화, 미리보기 등입니다. 사용자는 이러한 설정을 변경할 수 없습니다.

잠금 화면 메시지
잠금 화면 하단에 표시되는 메시지 (예: 기기를 찾았을 때 연락할 사람)와 자산 태그입니다 . 둘 다 $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$, $UDID$ 변수를 포함할 수 있으며, 기기에 값이 없는 변수는 비워 둡니다.

암호
암호 설정 섹션은 기기 암호 요구 사항과 관련 보안 규칙 (예: 최소 길이 및 복잡성)을 제어합니다 . Mac(macOS 13 이상, 사용자 등록 제외)에서는 이러한 규칙이 사용자의 로그인 비밀번호에 적용됩니다 .

옵션
Apple 정책 편집기에서 암호 옵션은 토글과 숫자 필드를 조합하여 구성합니다 . 많은 필드에 지원되는 OS 버전과 감독 요구 사항을 나타내는 도구 설명이 있습니다.

암호 토글

다음 인증 시 변경: 사용자가 다음에 인증할 때 암호 재설정을 강제합니다 .
영숫자 암호 요구: 영문자 하나와 숫자 하나 이상을 요구합니다 .
복잡한 암호 요구: “복잡한 ” 암호 (반복 /연속 패턴 없음, 영숫자가 아닌 문자 하나 이상)를
요구합니다 .
암호 요구: 추가 길이 /품질 요구 사항 없이 암호를 요구합니다 . 참고: 다른 암호 키를 설정하면
암호가 암시적으로 필요합니다 .

숫자 필드

실패 시도 초기화 (분): 실패 시도 횟수가 초기화되기까지의 시간 (분)입니다 (최대 실패 시도 횟수 필요).
최대 실패 시도 횟수: iPhone 또는 iPad가 지워지거나 Mac이 잠기기 전에 허용되는 실패 시도 횟수입니다 (범위: 2–11).
최대 유예 기간 (분): 암호 없이 기기 잠금을 해제할 수 있는 시간입니다 (0 = 없음).
최대 비활성 시간 (분): 기기가 잠기기까지의 유휴 시간입니다 (범위: 0–15).
최대 암호 사용 기간 (일): 강제 변경 전 최대 암호 사용 기간입니다 (범위: 0–730).
최소 복잡 문자 수: “복잡 ” 문자의 최소 수입니다 (범위: 0–4).
최소 길이: 최소 암호 길이입니다 (범위: 0–16).
암호 재사용 제한: 이전 암호 재사용을 방지하기 위한 암호 기록 길이입니다 (범위: 1–50).

제한
제한 섹션은 관리형 Apple 기기에서 허용되는 OS 기능을 제어합니다 . Apple 정책 편집기에서 이러한 옵션은 여러 토글이 있는 그룹 패널로 제공됩니다 .

앱 관리 및 네트워킹 패널의 토글은 Apple 정책의 앱 및 프로필 및 네트워킹 페이지에 설명되어 있습니다.

많은 제한은 특정 OS 버전에서만 지원되며 감독되는 기기가 필요할 수 있습니다. 정확한 요구 사항은
대시보드의 도구 설명을 참조하세요 .

사용자 등록 기기 (회사 계정으로 로그인하여 등록한 개인 기기)에는 Apple이 허용하지 않는 제한이
전송되지 않습니다. 정책의 제한 중 적용되는 것이 없으면 이러한 기기에는 제한 프로필이 제공되지
않습니다. 정책 편집기에는 사용자 등록 기기에 적용되지 않는 제한 수가 표시됩니다 .

보안
자동 잠금 해제 허용
지문으로 잠금 해제 허용
지문 수정 허용
콘텐츠 및 설정 지우기 허용
제한 활성화 허용
사용자의 프로필 설치 허용
호스트 페어링 허용
진단 데이터 제출 허용
진단 데이터 제출 수정 허용
Apple 맞춤형 광고 허용
원격 관리 수정 허용

멀티미디어
카메라 허용
파일 공유 수정 허용
파일 앱의 USB 드라이브 접근 허용
통화 녹음 허용
AirPrint 허용

AirPrint 자격 증명 저장 허용
AirPrint iBeacon 검색 허용

셀룰러
앱 셀룰러 데이터 수정 허용
셀룰러 요금제 수정 허용
eSIM 수정 허용
eSIM 외부 전송 허용
기기 지우기 시 eSIM 유지
로밍 중 백그라운드 가져오기 허용

셀룰러 APN

셀룰러 APN: 통신사에서 제공한 액세스 포인트 이름 (APN)을 설정합니다 . 예를 들어 사설 또는 업무용
모바일 네트워크에 사용합니다 . 액세스 포인트 이름 과, 통신사에서 요구하는 경우 인증 (PAP 또는 CHAP), 사용자 이름 ($EMAIL$ 같은 변수 허용), 비밀번호, IP 버전 (로밍 시 포함), 프록시 서버와 해당 포트 및 XLAT464를 설정하세요 . 통신사에서 네트워크 연결용으로 별도 APN을 제공하는 경우에만 APN 연결 을 켜세요.

iPhone 및 셀룰러 iPad에만 적용되며, 감독되지 않은 기기에도 적용됩니다 . 사용자 등록 (개인 기기)
으로 등록된 기기에는 적용되지 않습니다.
셀룰러 데이터에 사용되는 SIM에만 적용됩니다 . 다른 방식으로 이미 APN 프로필이 설치된 기기에는
설치되지 않습니다.
비밀번호는 다른 네트워크 비밀번호와 동일하게 보호됩니다 . 프로필은 해당 프로필이 만들어진
기기에만 전송되며 비밀번호는 로그에 기록되지 않습니다.

잘못된 APN은 기기의 셀룰러 데이터를 끊습니다. 먼저 통신사의 SIM이 있는 테스트 기기에서 설정을 사용해 보세요.

시스템 및 사용자 인터페이스
Handoff 허용
자동 수정 허용
자동 디밍 허용
자동 화면 보호기 허용
QuickPath 키보드 허용
정의 조회 허용

기기 이름 수정 허용
기기 잠자기 허용
iPhone 미러링 허용
Mac에서 iPhone 위젯 허용
키보드 단축키 허용

Apple 앱 및 서비스
iMessage 허용
Game Center 허용
Game Center 친구 추가 허용
나의 기기 찾기 허용
나의 친구 찾기 허용
나의 친구 찾기 수정 허용
Book Store 허용
Book Store 성인 콘텐츠 허용
엔터프라이즈 도서 백업 허용
엔터프라이즈 도서 메타데이터 동기화 허용
iTunes Store 허용
성인 콘텐츠 허용

Siri 및 Apple Intelligence
Siri 허용
Siri 사용자 생성 콘텐츠 허용
잠금 상태에서 Siri 허용
받아쓰기 허용
외부 인텔리전스 통합 허용
외부 인텔리전스 로그인 허용
Genmoji 허용
Image Playground 허용
Image Wand 허용

iCloud

iCloud 주소록 허용
iCloud 백업 허용
iCloud 책갈피 허용

iCloud 캘린더 허용
iCloud 데스크톱 및 문서 허용
iCloud 문서 동기화 허용
iCloud Freeform 허용
iCloud 키체인 동기화 허용
iCloud 메일 허용
iCloud 메모 허용
iCloud 사진 보관함 허용
iCloud 비공개 릴레이 허용
iCloud 미리 알림 허용

계정 (제한)
계정 패널에는 제한과 (선택적으로) 계정 구성이 모두 포함됩니다 . 제한 토글은 사용자가 시스템 계정을 수정할 수 있는지 여부를 제어합니다 .

계정 수정 허용

네트워킹
Apple 정책 편집기의 네트워킹 섹션에서는 기기의 Wi-Fi 네트워크와 VPN을 구성하고, 인증서를 설치하며, AirDrop 및 Bluetooth와 같은 연결 기능을 제한합니다 . 각 Wi-Fi 네트워크, VPN 및 인증서는 자체 구성 프로필로 설치되며, 기기의 설정 > 일반 > VPN & 기기 관리 (Mac: 시스템 설정 > 일반 > 기기 관리, 또는 macOS 13 및 14에서는 개인 정보 보호 및 보안 > 프로필) 및 기기 페이지의 프로필, 인증서 및 보안 패널에서 확인할 수 있습니다.

인증서는 인증서 페이지에서 가져옵니다 . 먼저 해당 페이지에서 가져오세요 . 정책은 인증서를 참조만
하므로 정책에 인증서가 복사되지 않습니다.

제한
AirDrop 허용
AirPlay 수신 요청 허용
Bluetooth 수정 허용
Bluetooth 공유 수정 허용
파일 앱의 네트워크 드라이브 접근 허용
인터넷 공유 수정 허용
콘텐츠 캐싱 허용
iTunes 파일 공유 허용

Wi-Fi 네트워크
Wi-Fi 네트워크 추가 를 클릭하고 다음을 입력하세요 :

네트워크 이름 (SSID): 네트워크 이름이며 최대 32자입니다.
보안: 없음 (개방형 네트워크), WEP, WPA 또는 WPA2, WPA2 또는 WPA3, WPA3만, 또는 모두. 비밀번호 : 개인 네트워크의 비밀번호입니다 .
자동으로 연결 및 숨겨진 네트워크 (이름을 브로드캐스트하지 않는 네트워크용)입니다.
프록시: 없음, 수동 (서버 및 포트) 또는 자동 (PAC 파일 URL, 비워 두면 WPAD로 네트워크에서
설정을 찾음)입니다.
프로필 이름 (선택 사항) 및 적용 대상: 네트워크를 일부 기기 유형으로 제한합니다 .

엔터프라이즈 네트워크 (802.1X)

사용자가 공유 비밀번호 대신 자체 자격 증명이나 인증서로 인증하는 경우 엔터프라이즈 (802.1X)를 켜세요.

인증: PEAP, TTLS(내부 인증 포함, 예: MSCHAPv2) 또는 TLS(인증서만).
기기 사용자의 자격 증명: 각 기기는 사용자 페이지에서 설정한 사용자의 EAP ID, 익명 ID,
비밀번호를 사용합니다 . 사용자가 없는 기기에는 네트워크가 적용되지 않습니다.
ID, 익명 ID 및 비밀번호 : 모든 기기에 동일합니다 . ID에는 $EMAIL$, $USERNAME$,
$FULLNAME$, $SERIAL$, $UDID$ 변수를 포함할 수 있습니다. 비밀번호를 비워 두면 사용자가
기기에서 직접 입력합니다 .
ID 인증서: 기기가 제시하는 클라이언트 인증서입니다 (TLS에 필요). 아래 인증서 옵션을
참조하세요 .
신뢰할 수 있는 인증서: RADIUS 서버의 인증서를 발급한 CA 인증서입니다 . 네트워크와 함께
설치됩니다 .
신뢰할 수 있는 서버 이름: 기기가 허용하는 RADIUS 서버 인증서의 이름입니다 . 예: radius.example.com 또는 *.example.com.

VPN

VPN 추가 를 클릭하여 iOS, iPadOS, macOS에 내장된 IKEv2 또는 Cisco IPSec VPN을 구성하세요 (VPN 앱 필요 없음).

유형 및 서버. IKEv2의 경우 원격 ID(서버 ID, 비어 있으면 서버 주소)와 로컬 ID도 설정합니다 .
로컬 ID에는 $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$, $UDID$ 변수를 포함할 수
있습니다.
인증 (기기): 인증서 (인증서 페이지, 기기 사용자의 인증서, 또는 SCEP 서버에서 요청), 공유 비밀
(IPSec의 선택적 그룹 이름 포함), 또는 사용자 이름과 비밀번호만 확인하는 IKEv2 서버의 경우 없음

.

신뢰할 수 있는 인증서: VPN 서버의 CA 인증서이며 VPN과 함께 설치됩니다 . IKEv2의 경우 예상
서버 인증서 발급자와 이름도 설정할 수 있습니다.
사용자 이름 및 비밀번호 : 사용자는 사용자 이름 (변수 허용)과 비밀번호 (IKEv2는 EAP, IPSec은 XAuth)로도 인증합니다 . 비밀번호를 비워 두면 사용자가 기기에서 직접 입력합니다 .
VPN 이름 (설정에 표시됨) 및 적용 대상.

연결

사용자가 설정에서 연결: VPN이 설치되며 사용자가 필요할 때 켭니다.
요청 시: 기기가 VPN에 자동으로 연결합니다 . 신뢰할 수 있는 Wi-Fi 제외 를 사용하면 나열한 Wi-
Fi 네트워크 (예: 사무실 네트워크)에서는 VPN을 사용하지 않습니다.
상시 연결 (IKEv2, 감독되는 iPhone 및 iPad만 해당): 셀룰러와 Wi-Fi에서 모든 트래픽이 VPN을
통과하며 사용자가 끌 수 없습니다. 다른 기기에는 이 VPN이 적용되지 않습니다. VPN이 사용자
이름을 사용하는 경우 정책에 비밀번호를 설정해야 합니다.
앱별 VPN: 일부 앱만 VPN을 사용합니다 . 앱 관리 섹션에서 각 앱의 VPN을 선택하고 (앱의 VPN 필드, Mac에서는 사용할 수 없음), 선택적으로 이를 사용하는 Safari 도메인을 나열하세요 .

상시 연결 또는 요청 시 VPN은 먼저 테스트 기기에서 테스트하세요 . 서버에 연결할 수 없으면 기기가 연결되지 않을 수 있습니다.

전역 프록시, 암호화된 DNS 및 웹 콘텐츠 필터
이 설정은 기기의 모든 트래픽에 적용됩니다 . 해당 토글로 켜세요.

전역 HTTP 프록시 (감독되는 iPhone 및 iPad, Mac): 모든 HTTP 트래픽이 모든 네트워크에서
프록시를 통과합니다 . 서버와 포트 (선택적 사용자 이름 및 비밀번호 포함) 또는 자동 구성 (PAC 파일 URL, 비워 두면 네트워크에서 찾음)을 설정하세요 . Wi-Fi 로그인 페이지 허용 은 사용자가 프록시
없이 공용 Wi-Fi 네트워크에 로그인할 수 있게 합니다.
암호화된 DNS: 기기가 DNS over HTTPS(서버 URL) 또는 DNS over TLS(서버 이름)를 통해
사용자의 DNS 서버로 이름을 확인하며, 선택적으로 일부 도메인에만 적용할 수 있습니다. 감독되는 기기에서는 사용자가 이를 끄지 못하게 할 수 있습니다.
웹 콘텐츠 필터 (감독되는 iPhone 및 iPad): iOS에 내장된 필터가 성인 웹 사이트를 제한하며, 항상
허용 또는 항상 차단할 웹 사이트 목록을 사용하거나 웹 사이트 목록만 허용하고 Safari에 책갈피로
표시합니다 .

잘못된 프록시나 DNS 서버는 기기를 연결 불가 상태로 만들 수 있습니다. 먼저 테스트 기기에서
설정을 사용해 보세요.

인증서
인증서 추가 를 클릭하여 인증서를 단독으로 설치하세요 . Safari와 앱이 신뢰해야 하는 인증 기관이거나 앱이 사용하는 ID입니다. Wi-Fi 네트워크나 VPN의 인증서는 여기에 추가할 필요가 없습니다.

인증서 옵션

인증서 페이지의 인증서: 모든 기기에 동일한 인증서입니다 . 인증서 선택 을 클릭하여 선택하세요 .
기기 사용자의 인증서: 각 기기가 사용자와 연결된 클라이언트 인증서를 받습니다. 사용자에게
인증서가 없는 기기에는 적용되지 않습니다. 사용자에게 다른 인증서를 연결하면 기기가
업데이트됩니다 .
SCEP 서버에서 요청: 각 기기가 SCEP 서버 (예: Microsoft NDES)에서 자체 인증서를 요청하므로
개인 키가 기기를 떠나지 않습니다. 서버 URL, 서버가 요구하는 경우 챌린지, 주체 (예: CN=$EMAIL$), 대체 이름, 키 크기, 키 사용을 설정하세요 .

이전 RC2 암호화로 보호된 클라이언트 인증서 (.p12)는 Apple 기기에 설치할 수 없습니다. 가져오기
전에 3DES 또는 AES 암호화로 다시 내보내세요 .

보안
비밀번호나 개인 키가 포함된 프로필은 해당 프로필이 만들어진 기기에만 전송됩니다 . 기기는 관리 인증서로 요청에 서명해야 합니다. 비밀번호와 인증서는 로그에 기록되지 않습니다.

소프트웨어 업데이트
Apple 정책 편집기의 소프트웨어 업데이트 섹션은 기기를 최신 상태로 유지합니다 . 특정 OS 버전을
기한까지 요구할 수 있고, 기기가 업데이트를 다운로드하고 설치하는 방식을 제어할 수 있습니다.

필수 OS 업데이트
필수 업데이트 추가 를 클릭하여 OS 버전을 요구하십시오 . 기기는 업데이트를 다운로드하고 사용자에게
기한을 알리며, 사용자가 그 전에 설치하지 않으면 기한에 설치합니다 . 이미 해당 버전 이상을 실행하는 기기는 이를 무시합니다 . iOS 및 iPadOS 17 또는 macOS 14가 필요합니다 .

적용 대상 (필수): iPhone 및 iPad 또는 Mac. 각 OS에는 고유한 버전 번호가 있으므로 각각 하나의
필수 업데이트를 추가하십시오 .
OS 버전: 설치할 버전입니다 (예: 18.5 또는 15.4.1).
빌드 (선택 사항): 특정 빌드입니다 (예: 베타 또는 백그라운드 보안 개선).
설치 기한: 각 기기의 현지 시간 기준 기한입니다 . 과거 날짜를 지정하면 기기가 가능한 한 빨리
업데이트를 설치합니다 .
세부 정보 URL (선택 사항): 사용자에게 표시되는 업데이트 관련 웹 페이지입니다 .

기기는 기기 페이지의 기기 상태 패널에 업데이트 진행 상황 (다운로드, 설치, 실패)을 보고합니다 .

소프트웨어 업데이트 설정
iPhone 및 iPad용 소프트웨어 업데이트 설정 또는 Mac용 소프트웨어 업데이트 설정 을 켜서 해당 기기의 업데이트를 제어하십시오 . 토글이 꺼져 있으면 기기는 자체 설정을 유지합니다 . iOS 및 iPadOS 18 또는 macOS 15가 필요합니다 . 이전 기기는 이러한 설정을 무시합니다 .

업데이트 연기: 새 업데이트는 지정된 일수 (1~90일)가 지난 후에만 사용자에게 표시됩니다 . Mac
에서는 주요 업데이트, 마이너 업데이트 및 기타 시스템 업데이트에 대해 서로 다른 기간을 설정할
수 있습니다.
사용자에게 표시되는 업데이트 (iPhone 및 iPad): 사용 가능한 업데이트가 두 개 이상일 때 모두
표시하거나 , 가장 오래된 마이너 업데이트만 표시하거나 , 가장 최신 업데이트만 표시합니다 .
표준 사용자가 업데이트를 설치할 수 있음 (Mac): 관리자 권한이 없는 사용자가 macOS 업데이트를 설치할 수 있습니다.
필수 업데이트에 대해 사용자에게 알림: 필수 업데이트 및 기한에 대한 알림을 표시합니다 .

자동 다운로드 , 자동 설치 및 자동 보안 업데이트 : 사용자가 결정하도록 하거나 (Apple의 기본값
), 항상 켜짐 또는 항상 꺼짐으로 유지합니다 .
백그라운드 보안 개선: 사용자에게 Apple의 신속한 보안 수정을 제공하고, 사용자가 이를 제거할
수 있는지 선택합니다 .
베타 프로그램 : 사용자가 Apple 베타 프로그램에 참여하도록 허용하거나 , 기기를 프로그램에서
제거하고 차단합니다 (iPhone 및 iPad의 경우 감독된 기기만 해당).

기기 페이지에서 업데이트 설치
기기의 기기 상태 패널에는 해당 기기에 사용 가능한 업데이트가 나열됩니다 . 업데이트 확인 을 사용하여
기기에 목록을 요청하고, 설치 를 사용하여 지금 설치하거나 다운로드하여 사용자가 설치하도록 하십시오. 이 기능은 감독된 iPhone 및 iPad와 Mac에서 작동합니다 . Apple은 iOS, iPadOS 및 macOS 27에서 이러한 명령을 제거합니다 . 해당 버전에서는 정책의 필수 업데이트를 사용하십시오 .

macOS

macOS 섹션은 Mac의 보안, 개인 정보 보호, 로그인 설정을 관리합니다 : FileVault, 방화벽, Gatekeeper,
화면 보호기 및 잠금, 외부 및 네트워크 저장 공간, 화면 공유, 개인 정보 보호 권한, 로그인 항목, 로드가
허용되는 시스템 및 커널 확장입니다 . 또한 시스템 서비스와 백그라운드 작업의 구성 파일을 설치합니다 .
정책의 다른 기기에는 이러한 설정이 적용되지 않습니다. 설정을 관리하려면 켜세요. 꺼져 있는 동안 사용자는
자신의 선택을 유지합니다 .

대부분의 설정은 구성 프로필로 Mac에 설치되며, 시스템 설정 > 일반 > 기기 관리에서 확인할 수
있습니다. FileVault, 개인 정보 보호 권한, 로그인 항목, 확장 설정에는 사용자가 승인한 MDM이
필요합니다 . 등록 URL이나 QR 코드로 등록한 Mac에서는 사용자가 시스템 설정에서 등록 프로필을
승인합니다 . 기기 페이지의 사용자 승인 MDM 필드에 표시됩니다 . 사용자가 나중에 승인하면 Mac이
이러한 설정을 자동으로 받습니다.

FileVault

FileVault는 Mac의 디스크를 암호화합니다 . 이 설정을 켜면 사용자에게 비밀번호로 FileVault를 켜라는
메시지가 표시되고, Mac은 조직에만 속한 키로 암호화된 개인 복구 키를 Cerberus Enterprise에 보냅니다.
키는 기기 페이지의 FileVault 필드에서 확인하고 변경할 수 있습니다 (기기 명령 참조). 이 설정에는 macOS
13 이상과 사용자 승인 MDM이 필요합니다 . 사용자 승인 MDM이 없으면 Mac에 FileVault를 켜라는 메시지가
표시되지 않지만, 사용자가 켜면 해당 키가 저장됩니다 .

로그인 시 필수: 다음 로그인 시, 여러 번 건너뛴 후 (사용자는 로그인 및 로그아웃할 때마다 다시
요청받음), 또는 사용자가 로그아웃할 때만 해당합니다 .
로그아웃 시 묻지 않음: 사용자는 로그인할 때만 요청받습니다 . "로그아웃 시에만 요청 "과 함께
사용할 수 없습니다.
사용자에게 복구 키 표시: 기본적으로 꺼져 있으므로 관리자만 기기 페이지에서 키를 알 수
있습니다.
FileVault 끄기 방지: 기본적으로 켜져 있습니다.
대기 중 메모리에서 키 제거: Mac이 대기 상태에서 깨어나면 사용자가 비밀번호를 다시
입력합니다 .
키 보관 위치: 로그인 화면에서 사용자에게 표시되는 텍스트입니다 . 예를 들어 Mac 복구를 위해
연락할 사람 (기본값 "Cerberus Enterprise")입니다.

설정을 받을 때 이미 암호화되어 있던 Mac은 현재 키를 유지하며, Cerberus Enterprise는 이 키를
받지 않습니다. 사용자가 FileVault를 껐다가 다시 켜야 ("FileVault 끄기 방지 " 끔) 키가 저장됩니다 .
설정을 끄거나 Mac을 관리에서 제거해도 FileVault는 꺼지지 않으며 저장된 키는 계속 작동합니다 .

서버가 복구 키를 저장하도록 구성되지 않은 경우 설정을 저장할 수 없습니다.

방화벽
방화벽 켜기: 꺼져 있으면 방화벽이 꺼진 상태로 유지되며 사용자가 켤 수 없습니다.
모든 수신 연결 차단: 기본 네트워크 서비스 (DHCP, Bonjour, IPSec)만 연결을 받을 수 있습니다. 스텔스 모드: Mac이 ping 요청과 닫힌 포트로의 연결에 응답하지 않습니다.
내장 소프트웨어 허용 및 다운로드한 서명된 앱 허용: 사용자에게 묻지 않고 연결을 받을 수
있습니다 (macOS 12.3 이상).
특정 앱에 대한 규칙: 번들 ID로 앱의 수신 연결을 허용하거나 차단합니다 .

Gatekeeper
Gatekeeper는 앱을 열기 전에 검사합니다 . Mac이 App Store 앱만 열지, 식별된 개발자의 앱도 열지
선택하세요 . Gatekeeper를 끄면 서명되지 않았거나 손상된 앱을 포함해 모든 앱을 열 수 있습니다. macOS 15 이상에서는 차단된 악성 코드를 Apple에 보내도록 사용자에게 요청할지도 선택할 수 있습니다.

화면 보호기 및 잠금
일정 시간 동안 활동이 없으면 화면 보호기를 시작하고, 화면 보호기가 시작되거나 디스플레이가 잠들 때 즉시 또는 지연 후 비밀번호를 요청합니다 . 관리되지 않음 으로 남겨 둔 설정은 사용자의 선택으로 유지됩니다 .

외부 및 네트워크 저장 공간
Mac의 외부 저장 공간 (USB 드라이브, SD 카드, 외장 디스크)과 네트워크 저장 공간 (파일 공유)을 허용, 읽기 전용으로 설정 또는 차단합니다 . macOS 15 이상이 필요합니다 .

화면 공유
화면 공유로 이 Mac에 연결하는 사람의 제한: Mac에서 파일 복사 또는 Mac으로 파일 복사, 고성능 연결, 가상 디스플레이 수입니다. 화면 공유 켜기는 사용자의 선택으로 유지됩니다 . macOS 14 이상이 필요합니다 .

개인 정보 보호 권한
사용자가 시스템 설정 > 개인 정보 보호 및 보안에서 허용할 앱 접근 권한을 부여하거나 거부합니다 . 예를
들어 백업 앱에 전체 디스크 접근 권한을 주거나 앱의 카메라 접근을 거부합니다 . 각 권한에 대해 선택하세요 :

권한: 전체 디스크 접근 권한, 손쉬운 사용, 자동화, 폴더, 연락처, 캘린더, 사진, 카메라, 마이크,
화면 기록 및 개인 정보 보호 및 보안의 기타 항목입니다 .
접근: 허용 또는 거부합니다 . 카메라, 마이크, 화면 기록, 입력 모니터링은 프로필로 허용할 수 없고
거부만 가능합니다 . 화면 기록과 입력 모니터링의 경우 관리자 권한 없이도 사용자가 허용하도록 할
수 있습니다.
앱: 앱의 번들 ID 또는 프로그램의 경로 (예: 명령줄 도구)입니다.
코드 요구 사항: 서명으로 앱을 식별합니다 . Terminal에서 codesign -dr -
/Applications/Example.app 를 실행하고 designated => 뒤의 텍스트를 복사하세요 .
자동화 에는 제어되는 앱 (예: Finder)과 해당 코드 요구 사항도 필요합니다 .

로그인 및 백그라운드 항목
규칙과 일치하는 로그인 항목과 백그라운드 항목은 관리됩니다 . 묻지 않고 실행되며, 사용자는 시스템 설정 > 일반 > 로그인 항목에서 이를 끌 수 없습니다. 규칙은 앱의 개발자 팀 ID, 번들 ID 또는 실행 데몬이나
에이전트의 레이블 (첫 부분으로도 가능)과 일치합니다 . macOS 13 이상이 필요합니다 .

시스템 확장
시스템 확장은 앱이 macOS를 확장하는 현대적인 방법입니다 : 네트워크 필터 및 VPN, 엔드포인트 보안
에이전트 및 드라이버. 이 설정을 켜면 나열된 개발자 팀의 시스템 확장이 사용자에게 묻지 않고 로드됩니다 . macOS 10.15 이상과 사용자 승인 MDM이 필요합니다 .

팀 ID: 개발자의 10자 팀 ID입니다 (예: 앱의 "서명자 " 세부 정보 또는 codesign -dv). 각 팀은 한
번만 나타날 수 있습니다.
허용: 팀의 모든 확장 또는 나열된 번들 ID를 가진 확장만 허용합니다 .
유형: 팀을 드라이버, 네트워크 또는 엔드포인트 보안 확장으로 제한합니다 . 아무것도 선택하지
않으면 모든 유형이 허용됩니다 .
제거 (나열된 확장에만 해당): 앱이 관리자 없이 확장을 제거할 수 있음 (macOS 12 이상), 시스템 무결성 보호가 켜져 있는 동안 확장을 끄거나 제거할 수 없음, 또는 시스템 설정과 Finder에서 확장을 제거할 수 없음 (macOS 15 이상). 이전 macOS의 Mac은 제거 옵션 없이 확장을 계속 허용합니다 .
사용자가 다른 시스템 확장을 승인할 수 있음: 기본적으로 켜져 있습니다. 끄면 프로필에서 허용한 확장만 로드됩니다 . Mac의 프로필 중 하나라도 이를 끄면 꺼진 상태입니다 .

macOS 11.3이상에서는 이 설정을 제거하면 허용했던 시스템 확장 (예 : 보안 에이전트나 네트워크 필터)이 꺼집니다 . 설정을 끄거나 , 정책을 삭제하거나 , Mac이 이 설정이 없는 정책으로 이동할 때 발생합니다 . 편집기는 설정을 끄기 전에 확인을 요청합니다 .

커널 확장 (레거시)

커널 확장은 macOS를 확장하는 더 오래되고 지원 중단된 방법입니다 . 공급업체가 제공하는 경우 시스템 확장을 선호하세요 . 나열된 팀의 커널 확장 (팀의 모든 확장 또는 나열된 번들 ID만)은 재시작 후 사용자에게 묻지 않고 로드됩니다 . macOS 10.13.2 이상과 사용자 승인 MDM이 필요합니다 .

- 사용자가 다른 커널 확장을 승인할 수 있음 : 기본적으로 꺼져 있으므로 나열된 팀만 커널 확장을 로드할 수 있습니다 .
- 표준 사용자도 승인할 수 있음 : 사용자 승인이 켜져 있으면 관리자 권한이 없는 사용자도 승인할 수 있습니다 (macOS 11 이상).

Apple silicon Mac에서는 프로필만으로는 충분하지 않습니다 . 누군가 Mac을 recoveryOS로 시작하고 , 시동 보안 유틸리티에서 보안 감소를 선택하고 , 식별된 개발자의 커널 확장에 대한 사용자 관리를 허용해야 합니다 . 커널 확장을 승인하려면 Cerberus Enterprise에 에스크로된 Bootstrap Token도 필요할 수 있습니다 (기기 페이지의 Bootstrap Token 필드 참조).

Mac 파일

서비스 구성 파일과 백그라운드 작업은 조직의 **Mac** 파일 에 업로드한 파일을 사용합니다 . zip 아카이브와 속성 목록 (.plist), 최대 20MB입니다 . macOS 섹션의 **Mac** 파일 버튼이나 설정의 파일 선택 으로 업로드하고 , 사용 위치를 확인하거나 삭제하세요 . 정책에서 사용 중인 파일은 삭제할 수 없습니다 . 파일을 변경하려면 새 버전을 업로드하고 정책에서 선택하세요 . 그러면 Mac이 다시 다운로드합니다 .

서비스 구성 파일

zip 아카이브에서 시스템 서비스의 구성 파일을 설치합니다 . 기본 서비스는 SSH 서버 (sshd), sudo, PAM, 프린트 (CUPS), Apache 웹 서버 , bash, zsh, 스마트 카드 로그인 및 인증입니다 . `com.example.service` 같은 역방향 DNS 식별자로 자체 서비스를 사용할 수도 있으며 , macOS의 관리형 구성 파일 라이브러리에서 파일을 찾습니다 . 각 서비스에는 하나의 설정이 있을 수 있습니다 . macOS 14 이상이 필요합니다 .

기본 서비스는 아카이브의 파일만 사용하고 자체 파일 (예 : sshd의 /etc/ssh)은 무시합니다 . 전체 구성을 디스크 루트에서 시작하는 폴더에 넣어 아카이브에 포함하세요 (예 : `etc/ssh/sshd_config`).

파일은 Mac에서 읽기 전용이며 설정과 함께 제거됩니다 . 먼저 한 Mac에서 아카이브를 테스트하세요 . 잘못된 sudo 또는 PAM 구성은 사용자가 로그인하거나 관리자 권한을 사용하지 못하게 할 수 있습니다

.

백그라운드 작업
launchd가 시작하는 백그라운드에서 실행되는 프로그램과 스크립트입니다 . 사용자는 이를 끌 수 없으며 설정과 함께 제거됩니다 . macOS 15 이상이 필요합니다 . 각 작업에 대해 선택하세요 :

작업 식별자: com.example.task 같은 역방향 DNS 식별자로, 각 작업마다 달라야 합니다.
프로그램 및 스크립트 (선택 사항): Mac이 /var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/ 뒤에 작업 식별자를 붙인 폴더에 압축을 푸는 zip 아카이브입니다 . 파일의 실행 권한을 유지하고 속성 목록은 넣지 마세요. launchd 속성 목록: 프로그램을 시작하는 작업으로, 데몬 (전체 시스템, root) 또는 에이전트 (각
사용자 세션)로 로드됩니다 . 프로그램은 위 폴더의 경로로 참조하세요 .

작업에는 프로그램 또는 하나 이상의 속성 목록이 필요합니다 . 파일이 변경되면 Mac이 작업을 다시 시작합니다 .

위치 및 지오펜스
Apple 정책 편집기의 위치 및 지오펜스 섹션에서는 사이트나 창고 같은 영역을 정의합니다 . Cerberus Enterprise 앱이 설치된 iPhone 및 iPad는 이러한 영역에 들어가거나 나갈 때 이를 보고하며, 이벤트 규칙이 이에 반응할 수 있습니다. 이메일 보내기, 기기 잠금 또는 비활성화, 다시 활성화 등입니다.

지오펜스 필드
새 항목을 만들려면 지오펜스 추가 를 사용하세요 . 정책에는 최대 지오펜스 10개 를 포함할 수 있으며, 이름은 정책 내에서 고유해야 합니다. 각 지오펜스에는 다음 필드가 포함됩니다 :

이름: 필수이며 고유해야 합니다.
위도 및 경도: 영역의 중심입니다 . 지도를 클릭하여 설정할 수도 있습니다.
반경 (m): 필수이며 200~10000미터입니다 .
설명: 관리자를 위한 선택적 메모입니다 .
입장 보고 및 퇴장 보고: 생성할 이벤트를 선택하세요 . 하나 이상은 켜져 있어야 합니다.
활성: 지오펜스를 삭제하지 않고 활성화하거나 비활성화합니다 .

각 지오펜스에는 지도 미리보기가 있습니다. 저장된 지오펜스의 중심과 반경은 잠겨 있으므로 지도의 잠금 버튼을 사용하여 변경하세요 . 다른 버튼은 지도를 영역이나 현재 위치로 이동합니다 .

정책을 저장하면 Cerberus Enterprise가 정책의 iPhone 및 iPad에 새 지오펜스를 가져오도록 요청합니다 . 보통 몇 분이 걸리지만, iOS는 저전력 모드나 네트워크 연결 없음 등의 상황에서 이를 지연할 수 있습니다. 앱이 아직 최신 지오펜스를 적용하지 않았으면 기기 페이지에 표시됩니다 .

요구 사항
지오펜스는 Cerberus Enterprise 앱이 설치된 iPhone 및 iPad에서 작동합니다 . Mac은 이를 무시합니다 . 기기에서:

Cerberus Enterprise 앱이 설치되어 있고 (Cerberus가 설치함) 사용자가 한 번 이상 열었음;
앱의 위치 접근 권한이 항상 으로 설정되어 있음;
앱에 대해 정확한 위치 가 켜져 있음;
백그라운드 앱 새로 고침 이 켜져 있습니다.

개인 기기의 위치 및 지오펜스 , 섹션 상단에서 기본적으로 꺼져 있습니다. 꺼져 있는 동안 Cerberus
는 개인 기기 (사용자 등록)의 위치를 수집하지 않으며, 해당 기기의 지오펜스 이벤트가 생성되지 않고,

기기 페이지에서 위치 찾기나 실시간 추적을 제공하지 않습니다. 이 옵션을 켜면 정책의 개인 기기가
회사 기기처럼 위치와 지오펜스 이벤트를 공유하지만 , 사용자가 Cerberus Enterprise 앱에 대해
위치를 허용한 경우에만 그렇습니다 . 앱은 iOS가 요청하기 전에 사용자에게 이를 설명합니다 . 조직은 사용자에게 알리고 직원 위치에 관한 현지 규정을 준수할 책임이 있습니다. 분실 모드와 MDM 위치
요청은 개인 기기에서 절대 사용할 수 없습니다 (Apple이 허용하지 않음).

저전력 모드 에서도 지오펜스는 계속 작동하지만 , iOS가 영역을 벗어났음을 더 늦게, 덜 정확한 위치로 보고하며, 정책 변경 후 새 지오펜스를 가져오는 것을 앱이 다시 실행될 때까지 (예: 다음 경계 통과 시 또는 사용자가 앱을 열 때) 몇 시간 지연할 수 있습니다.

이벤트가 도착하는 방식
iOS는 앱에 대해 해당 영역을 감시하고 기기가 경계를 넘으면 앱이 열려 있지 않아도 앱을 깨웁니다. 이벤트는 경계를 넘은 후 몇 분 뒤에 도착할 수 있으며, 작은 영역이나 짧은 방문은 놓칠 수 있습니다. iOS는 기기가
경계를 상당히 지나 이동하고 한동안 그곳에 머물러야 하기 때문입니다 .

앱이 실행될 수 없는 경우 (예: 기기 잠금 해제 전 재시작 후) 서버는 앱이 보낸 위치에서 경계 통과를 나중에 감지합니다 . 앱이 감지하든 서버가 감지하든 각 통과는 이벤트 규칙을 한 번만 트리거합니다 .

앱이 몇 시간 동안 서버에 연결하지 않으면 서버는 iOS에 앱을 깨워 지오펜스를 다시 확인하도록 요청합니다 . iOS는 이러한 요청을 보장하지 않습니다.

기기 페이지
기기 페이지의 지오펜스 탭은 위치 지도 패널에서 기기의 전환을 표시합니다 . 정책에 활성 지오펜스가
있으면 상태 줄에서 기기에서 지오펜싱이 작동하는지 , 또는 작동하지 않는 이유를 알려 줍니다: 앱이 서버에 연결하지 않았거나 업데이트가 필요함, 위치 접근 권한이 항상 이 아님, 정확한 위치 또는 백그라운드 앱 새로 고침 이 꺼져 있음, 앱이 마지막으로 설정을 보고했을 때 저전력 모드 가 켜져 있었음, 또는 앱이 아직 최신 지오펜스를 적용하지 않음.

지오펜스 전환과 위치는 90일 동안 보존되며, 이보다 오래된 데이터는 매일 밤 자동으로 삭제됩니다 . 등록된 각 기기의 최신 위치는 항상 보존되므로 지도에 계속 표시됩니다 .

제한 사항
정책을 복사해도 지오펜스는 복사되지 않습니다. 복사본에서 다시 추가하세요 .
iPhone 및 iPad의 지오펜스 이벤트는 최선 노력 방식입니다 . iOS가 앱을 실행할 수 있는 시점을
결정합니다 .

계정
Apple 정책 편집기의 계정 섹션은 iPhone, iPad, Mac에 메일, Exchange, Google, 캘린더, 연락처, 디렉터리 계정을 추가합니다 . 계정 추가 를 클릭하고 유형을 선택하세요 . 이 섹션에는 계정 수정 허용 제한 (감독된 기기)도 포함되어 있습니다.

Mac(macOS 13 이상)에서는 관리에 등록된 사용자, 일반적으로 Mac을 등록한 사용자의 세션에
로그인되어 있을 때 계정이 설치됩니다 . 기기 페이지에는 이러한 사용자가 Mac 사용자 아래에 계정
상태와 함께 나열됩니다 . 기기 사용자로부터 이메일 주소를 가져오는 계정은 Cerberus Enterprise
에서 Mac에 할당된 사용자를 사용합니다 .

공통 설정
기기 사용자의 이름 및 이메일 (메일, Exchange, Google): 각 기기는 사용자 페이지에 설정된
해당 사용자의 이름과 이메일 주소를 사용합니다 (Google의 경우 사용자의 Google 계정). 사용자가
없거나 사용자에게 이메일 주소가 없는 기기에는 계정이 제공되지 않습니다. 그렇지 않은 경우 고정
이메일 주소와 전체 이름을 설정하세요 .
계정 이름 (선택 사항): 설정 및 앱에 표시되는 계정 이름입니다 .
사용자 이름 및 비밀번호 (선택 사항): 사용자 이름에는 $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$, $UDID$ 변수를 포함할 수 있습니다. 사용자가 기기에서 비밀번호를 입력하도록
비밀번호를 비워 두거나, 사용자가 둘 다 입력하도록 둘 다 비워 두세요.
적용 대상: 계정을 일부 기기 유형으로 제한합니다 .

계정 유형
메일 계정: IMAP 또는 POP 수신 서버와 발신 서버, 해당 포트 및 인증입니다 . 발신 서버는 수신
서버와 동일한 사용자 이름 및 비밀번호를 사용할 수 있습니다.
Exchange 계정 (Exchange ActiveSync): 서버를 입력하거나 , 이메일 주소에서 찾도록 비워 두세요. 서비스 (메일, 연락처, 캘린더, 미리 알림, 메모)와 사용자가 이를 변경할 수 있는지 여부를 선택합니다 . 최신 인증 (OAuth)을 사용하면 사용자가 ID 공급자 (예: Microsoft 365)의 페이지에서 로그인합니다 . 인증용 인증서 (iOS 17 이상)는 인증서로 기기를 인증합니다 .
Google 계정: 사용자가 지정된 이메일 주소로 Google 계정에 로그인합니다 .
캘린더 계정 (CalDAV) 및 연락처 계정 (CardDAV): 서버, 포트 및 경로.
디렉터리 (LDAP): 서버와 포트, 그리고 연락처를 조회하는 데 사용되는 검색 (검색 기준, 범위 및 설명).
구독 캘린더: 캘린더의 URL(https, http 또는 webcal).

S/MIME

메일 및 Exchange 계정은 S/MIME(iOS 17 이상)으로 메시지에 서명하고 암호화할 수 있습니다. 각 계정에 대해 인증서 페이지의 인증서, 기기 사용자의 인증서 또는 SCEP 서버에서 요청한 인증서 중 하나를 선택합니다 . 사용자가 이를 끄고 다른 인증서를 선택할 수 있도록 허용할 수 있으며, 암호화의 경우 각 메시지에 스위치를 표시할 수 있습니다.

보안
비밀번호와 인증서는 기기로 전송되는 설정의 일부가 아닙니다. 각 기기는 관리 인증서로 요청에 서명하여 Cerberus Enterprise에서 자체 자격 증명을 다운로드합니다 . 이들은 로그에 기록되지 않습니다.

규정 준수 규칙
Apple 정책 편집기의 규정 준수 규칙 섹션은 정책의 기기에 대한 요구 사항을 설정합니다 . 규칙을 위반한 기기는 즉시 규정 미준수 상태가 됩니다. 기기 페이지의 기기가 규정을 준수하지 않는 이유 에 이유가 표시되고, 기기 목록에도 규정 미준수로 표시됩니다 . 정책의 설정을 기기에 적용할 수 없는 경우에도 기기는 규정 미준수 상태가 됩니다.

규칙
암호: 기기에 암호가 있으며 정책의 암호 설정을 충족합니다 .
최소 OS 버전: iPhone 및 iPad 또는 Mac에 해당합니다 . 기기를 업데이트하려면 소프트웨어
업데이트에서 필수 업데이트를 추가하세요 .
감독되는 기기: 등록 프로필 또는 사용자 등록으로 등록된 기기는 감독되지 않습니다.
FileVault 켜짐 (Mac): Mac의 디스크가 FileVault로 암호화되어 있습니다. 다른 기기는 영향을
받지 않습니다.

규칙은 기기가 상태를 보낼 때, 정책이 저장될 때, 그리고 매시간 확인됩니다 . 상태를 알 수 없는 기기 (예: FileVault를 아직 보고하지 않은 Mac)는 규칙을 위반하지 않습니다.

기기 차단
기기가 계속 규정을 준수하지 않으면 차단 을 켜고 며칠 후에 차단할지 설정하세요 (0이면 즉시 차단). 감독되는 iPhone 및 iPad는 설정한 메시지와 함께 분실 모드로 전환됩니다 . 다른 기기는 한 번 잠기며, Mac은 재시작 후 PIN을 요청합니다 . PIN은 명령 기록의 명령 세부 정보에 표시됩니다 .

차단 해제: 기기가 다시 규정을 준수하면 분실 모드가 자동으로 해제됩니다 .
직접 분실 모드 해제: 기기가 규정을 준수하게 된 뒤 다시 규칙을 위반할 때까지 다시 차단되지
않습니다. 사용자가 기기를 수정할 수 있도록 할 때 사용하세요 .

알림을 받거나 다른 방식으로 대응하려면 기기가 규정 미준수 상태가 됨 에 대한 이벤트 규칙을
만드세요. 그러면 이유도 함께 제공됩니다 .