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 .

Revision #6
Created 2026-11-10 15:16:45 UTC by Admin
Updated 2026-11-12 09:56:31 UTC by Admin