명령

기기 페이지에는 관리형 기기로 원격 명령을 보낼 수 있는 명령 패널이 있습니다. 사용 가능한 명령은 플랫폼 (Android 또는 Apple)과 기기 상태에 따라 다릅니다.

명령은 현재 등록된 기기에만 보낼 수 있습니다. 등록 해제된 기기, 아직 등록되지 않은 ADE 기기 및 과거 등록 기록에서는 패널에 명령 기록만 표시됩니다 .

기기가 현재 온라인 상태가 아니면 기기가 인터넷에 연결되는 즉시 명령이 전달되고 실행됩니다 .
Android 명령의 경우 유효 기간 매개변수를 설정하여 전달되지 않은 명령의 유효 기간을 지정할 수 있습니다.

Android(AMAPI) 명령
Android 기기의 경우 명령 패널에는 유효 기간 필드 (값 + 단위)와 명령 선택기가 포함됩니다 . 일부 명령은 추가 매개변수가 필요하며, 명령을 선택하면 동적으로 표시됩니다 .

공통 매개변수

유효 기간: 명령을 즉시 실행할 수 없는 경우 명령이 유효한 기간입니다 .
명령: 기기에 보낼 작업을 선택합니다 .

추가 필드가 없는 명령

기기 잠금: 기기를 잠급니다.
기기 재시작: 기기를 재시작합니다 . Android 7.0 이상이 필요합니다 .
분실 모드 비활성화 : 기기를 분실 모드에서 해제합니다 .
소유권 포기: Android 8.0 이상의 회사 소유 기기에서 업무 프로필과 모든 정책을 제거하고 개인
용도로 남겨 둡니다. 개인 프로필의 앱과 데이터는 유지됩니다 . 기기가 명령을 확인한 후 서버에서
기기가 삭제됩니다 . 이 작업은 취소할 수 없습니다.

추가 필드가 있는 명령

비밀번호 재설정: 새 비밀번호 와 새 비밀번호 확인 이 필요합니다 . 선택적 토글에는 지금 잠금,
입력 요구, 부팅 시 자격 증명 요청 안 함 이 있습니다.

앱 데이터 지우기: 대상 패키지 이름 이 필요합니다 .
분실 모드 활성화: 분실 모드 메시지 가 필요하며 선택적 연락처 필드 (도로명 주소, 조직, 전화번호
, 이메일)를 지원합니다 . 기기가 이를 보고하면 상태가 분실 이 되고, 기기 페이지에 배너가 표시되며
분실 모드가 비활성화될 때까지 이 명령이 숨겨집니다 .
기기 지우기: 지우기 사유 메시지 (개인 기기의 사용자에게 표시됨)와 선택적 지우기 플래그를
지원하며, eSIM 지우기 를 포함합니다 .

eSIM 명령 (eSIM 추가, eSIM 제거, EID 요청)은 전용 SIM 관리 패널에서 사용할 수 있습니다.

명령 기록

전송 컨트롤 아래에 대시보드가 명령 기록 표를 표시합니다 . 이 표는 정렬 가능하며 페이지 매김을 지원합니다 . 일부 행은 펼쳐서 추가 매개변수나 실행 세부 정보를 볼 수 있습니다.

Android 기록 열

생성 날짜
명령
유효 기간
상태
오류
실행 날짜

Apple(MDM) 명령
Apple 기기의 경우 명령 패널에서 명령 선택기를 제공합니다 . 일부 명령은 추가 입력이 필요합니다 . Android 와 마찬가지로 아래에 명령 기록 표가 표시됩니다 .

추가 필드가 있는 명령

앱 설치: 애플리케이션 번들 ID가 필요합니다 .
알림 보내기: 알림 메시지 (최대 길이 200자)가 필요합니다 .

iPhone 및 iPad에서 알림 보내기 및 실시간 추적은 Cerberus Enterprise 앱을 통해 기기에 도달합니다 . 앱이 설치되어 알림 등록을 완료할 때까지 이러한 기능은 비활성화됩니다 (Cerberus Enterprise 앱 필드 참조). 실시간 추적을 시작하면 "실시간 추적 요청이 기기로 전송되었습니다 "가 표시됩니다 . 추적은 기기가 첫 위치를 보낼 때 시작됩니다 . iOS는 저전력 모드나 네트워크 연결 없음과 같은 상황에서 요청을 지연하거나
전달하지 않을 수 있습니다. 2분 이내에 위치가 도착하지 않으면 사용자에게 앱을 한 번 열어 달라고
요청하세요 . 요청이 실패하면 메시지에 사유가 표시됩니다 . 예를 들어 앱이 아직 등록되지 않았거나, 서버 알림 키가 없거나, 기기의 알림 토큰이 더 이상 유효하지 않은 경우입니다 .

기기 작업

기기에서 지원하는 명령만 나열됩니다 . 일부는 감독된 iPhone 또는 iPad가 필요하고, 일부는 Mac에서 사용할 수 없습니다. 중단을 일으키는 명령은 확인을 요청합니다 .

기기 잠금: 화면을 잠그며 선택적 메시지와 전화번호를 설정할 수 있습니다. Mac은 재시작되고 6
자리 PIN으로 잠기며, PIN은 명령 전송 후 한 번 표시되고 명령 세부정보에서도 확인할 수 있습니다. iPhone은 이 명령이 분실 모드를 활성화하지 않더라도 메시지 위에 "Lost iPhone" 제목을
표시합니다 .
분실 모드 활성화 (감독된 iPhone 및 iPad): 기기를 잠그고 잠금 화면에 메시지, 전화번호 및 각주를 표시합니다 . 분실 모드가 켜져 있는 동안 페이지에 배너와 기기 찾기 (위치는 위치 지도에 표시됨), 소리 재생 및 분실 모드 비활성화 명령이 표시됩니다 .
기기는 이를 소지한 사람에게 위치가 확인되었음을 알립니다. 기기 찾기 후 잠금 화면에 iPhone 위치 확인됨 이 (가) 시간 및 위치를 수신한 서버 이름과 함께 표시되고, 계속 버튼이 표시됩니다 . iOS는 이 알림을 표시하며 끌 수 없습니다.
암호 지우기: 예를 들어 사용자가 잊어버린 경우 iPhone 또는 iPad의 암호를 제거합니다 . 정책에서 암호를 요구하는 경우 사용자에게 새 암호를 설정하라는 메시지가 표시됩니다 .
기기 정보 새로 고침: 기기에 정보 (감독, OS 버전, 보안 상태, MDM 인증서)와 인벤토리를
요청합니다 .
기기 설정: 기기 이름, Mac의 호스트 이름, Bluetooth, 데이터 로밍, 개인용 핫스팟, 시간대, 배경화면, Activation Lock 허용 여부, Shared iPad의 설정 (아래 참조)을 변경하는 창을 엽니다. 변경한 설정만 전송되며, 기기에서 지원하지 않는 설정은 사유와 함께 비활성화됩니다 . 기기는 데이터 로밍이나 개인용 핫스팟을 적용하지 않고 확인만 할 수 있으므로 (예: SIM 요금제에 개인용 핫스팟이 없는 경우) Cerberus Enterprise는 약 30초 후에 이를 다시 읽고 변경되지 않았으면
시스템 로그에 경고를 기록합니다 .
기기 재시작 및 기기 종료: 확인 후 기기를 즉시 재시작하거나 끕니다.
기기 지우기: 모든 콘텐츠와 설정을 지우고 기기를 관리에서 제거합니다 . iPhone 및 iPad에서는 eSIM 데이터 요금제를 유지하고 근접 설정을 건너뛸 수 있으며, Mac은 6자리 PIN을 받습니다. 서비스로 복귀 (기기 지우기 의 옵션, iOS 17 이상의 iPhone 및 iPad): 지운 후 기기는 아무도 건드리지 않아도 스스로 다시 설정되고 현재 정책, 사용자 및 소유권으로 다시 등록됩니다 . 기기에 이더넷이나 셀룰러 데이터가 없는 한 설정에는 기기 정책의 Wi-Fi 네트워크를 선택하십시오 .
기기에는 아직 사용자나 인증서가 없으므로 개인 네트워크 (비밀번호가 있고 인증서가 없음)만
사용할 수 있습니다. Activation Lock은 꺼져 있어야 합니다.
셀룰러 요금제 새로 고침 (iPhone 및 셀룰러 iPad, iOS 13 이상, User Enrollment 제외):
통신사에서 제공한 통신사 eSIM 서버 URL(https:// 주소, 호스트 이름 또는 LPA 활성화 코드이며
이 중 서버만 사용됨)을 입력하면 기기가 통신사가 EID에 연결한 eSIM 요금제를 다운로드합니다 .

통신사에 전송할 수 있도록 기기 EID가 필드 아래에 표시됩니다 . SIM 관리 페이지를 참조하십시오 . eSIM 데이터 요금제 유지 를 끄면 지우기 시 모든 eSIM이 제거됩니다 . 정책 제한 기기 지우기 시 eSIM 유지 (감독된 기기, iOS 17.2 이상)는 기기에서 시작된 지우기 (암호 시도 횟수 초과, 모든
콘텐츠 및 설정 지우기)에 적용됩니다 . Apple은 이 명령에 대한 효과를 문서화하지 않았습니다 . 사용자 로그아웃 (Shared iPad): 현재 사용자를 로그아웃시키고 로그인 화면으로 돌아갑니다 . 아직 iCloud에 동기화되지 않은 데이터는 iPad에 남아 있습니다.

Shared iPad

Shared iPad Managed Apple Account . Shared iPad ADE (**Apple Automated Device Enrollment**), **Shared iPad** .

- **Shared iPad** : iPad , iCloud iPad . iPadOS 14 .
- : Managed Apple Account , iPadOS .

Mac

Mac **Mac** Mac (Mac) . . , , Mac , Mac .

Activation Lock

Activation Lock Activation Lock . Apple Account . Activation Lock . Cerberus Enterprise . ( ), Activation Lock Apple Account .

Recovery Lock (Mac)

Recovery Lock Apple silicon Mac , Intel Mac . Mac . Recovery Lock recoveryOS , Mac . Mac Cerberus Enterprise .

암호 설정 또는 변경: Cerberus Enterprise는 모든 키보드 레이아웃에서 동일한 키에 있는 20자 암호를 생성하거나 , 관리자가 직접 입력합니다 (악센트 없는 8~64자, 다른 역할은 저장된 암호를 볼 수 없으므로 생성만 가능). 암호는 전송 전에 암호화되어 저장되며, Mac이 확인한 경우에만 저장된 암호를 대체합니다 . Mac에 Cerberus Enterprise 외부에서 설정된 암호가 이미 있는 경우 현재 암호로 입력하십시오 . 이 암호는 한 번만 사용되며 저장되지 않습니다.
암호 확인: 저장된 암호가 올바른지 Mac에 묻습니다. 결과는 도구 설명과 시스템 로그에
표시됩니다 .
암호 표시: 관리자만 저장된 암호를 볼 수 있으며 각 조회는 시스템 로그에 기록됩니다 . 생성된
암호는 네 글자씩 그룹으로 표시되며, 공백 없이 입력하십시오 .
암호 지우기: Mac에서 암호를 제거합니다 .

Intel 기반 Mac은 펌웨어 암호 변경을 적용하기 위해 재시작합니다 . 그때까지는 이전 암호가 여전히 필요하며 (암호 표시에 나열됨), 다른 변경은 전송할 수 없습니다. 또한 Apple은 30초에 하나의 펌웨어 암호 명령만
허용합니다 . 암호는 명령 기록에서 숨겨집니다 .

Mac이 관리에서 이탈하면 (등록 해제, 사용자가 제거 또는 지우기) macOS가 Recovery Lock을 스스로
제거하고 Cerberus Enterprise는 저장된 Recovery Lock 암호를 삭제합니다 . Mac이 다시 등록된 후처럼 Recovery Lock이 없다고 보고하는 경우에도 마찬가지입니다 . Mac을 등록 해제하거나 정책을 삭제하면
저장된 펌웨어 암호가 먼저 지워지고 Mac이 재시작된 후 관리에서 이탈합니다 . 지우기에 실패하면 Mac은 그래도 관리에서 이탈하며 암호는 계속 저장되어 확인할 수 있습니다. 사용자가 관리에서 제거했거나 지운 Mac은 펌웨어 암호를 유지하며 Cerberus Enterprise도 이를 유지합니다 . 기기 레코드를 삭제하면 저장된 암호가 삭제되므로 먼저 확인을 요청합니다 . 암호를 기록해 두십시오. 암호가 없으면 Apple만 제거할 수 있습니다.

FileVault(Mac)

FileVault 필드는 Mac의 디스크가 암호화되었는지 여부와, 툴팁에서 Cerberus Enterprise가 개인 복구 키를 저장하는지 여부를 보여줍니다 . Mac은 정책의 FileVault 설정을 받은 후 FileVault가 켜지면 키를

전송합니다 (Apple 정책의 macOS 페이지 참조).

복구 키 표시: 관리자만 키를 볼 수 있으며 각 조회는 시스템 로그에 기록됩니다 . Mac의 로그인
창에서 사용자 비밀번호를 재설정하거나 복구 모드에서 디스크 잠금을 해제하는 데 사용하십시오 . Mac이 관리에서 이탈한 후에도 계속 사용할 수 있으며, 기기 레코드를 삭제하면 삭제됩니다 .
복구 키 변경: Mac이 개인 복구 키를 교체하고 새 키를 암호화하여 전송하며 이전 키는 작동을
멈춥니다. 저장된 키를 읽을 수 있는 경우에만 가능하며, Mac은 해당 키로 잠금이 해제되고 사용자
비밀번호는 필요하지 않습니다. 저장된 키는 명령 기록에서 숨겨지며 Mac이 응답하면 (또는 응답이
없으면 7일 후에) 서버에서 제거됩니다 .

Bootstrap Token(Mac)
macOS 10.15 이상의 Mac은 보안 토큰을 가진 사용자가 로그인하면 Bootstrap Token을 관리 서버로 전송합니다 . 서버는 이를 보관하고 해당 Mac에만 돌려주며, Mac은 이를 사용하여 새 사용자에게 보안 토큰을 부여하고 Apple silicon이 탑재된 Mac에서는 관리자 비밀번호를 묻지 않고 소프트웨어 업데이트를 설치하고

커널 확장을 승인합니다 . 대시보드나 다른 곳에서도 누구도 토큰을 볼 수 없습니다. Bootstrap Token 필드에는 상태가 표시됩니다 :

보관됨: 서버에 토큰이 있으며, 도구 설명에 Mac이 전송한 시점이 표시됩니다 .
이전에 에스크로됨 : 저장된 토큰이 Mac의 최근 등록 또는 MDM 인증서 갱신 이전에
전송되었습니다 . 갱신 후에는 예상된 동작입니다 . 토큰은 유지되며 Mac은 이를 다시 전송하지
않습니다. 새 등록 후에는 더 이상 유효하지 않을 수 있습니다. Mac의 Terminal에서 sudo
profiles install -type bootstraptoken 명령을 실행하세요 .
보관되지 않음: Mac이 아직 토큰을 전송하지 않았습니다 . 지금 전송하려면 Mac 관리자가
터미널에서 sudo profiles install -type bootstraptoken 을 실행하십시오 (sudo profiles
status -type bootstraptoken 은 보관 여부를 표시합니다).

도구 설명에는 Mac이 인증에 토큰을 허용하는지도 표시됩니다 . Automated Device Enrollment로 설정된 Mac은 자동으로 허용하며, 다른 Apple silicon Mac에서는 사용자가 recoveryOS의 시작 보안 유틸리티에서
허용할 수 있습니다. Intel Mac은 인증에 토큰을 사용할 수 없지만 (지원되지 않음), 보관된 토큰은 여전히 새 사용자에게 보안 토큰을 제공합니다 . Mac이 토큰을 전송, 제거 또는 요청할 때마다 시스템 로그에 기록됩니다 .

기기 상태 및 OS 업데이트

기기 상태 패널에는 기기가 자체적으로 보고하는 정보가 표시됩니다 . OS 버전 및 빌드, 소프트웨어 업데이트
진행 상황 (대기 중인 버전, 기한, 시작 원인, 실패), 암호 설정 여부 및 정책 준수 여부, Mac의 FileVault,
배터리 상태, 기기에 구성된 계정 등입니다.

사용 가능한 업데이트 목록에는 기기가 설치할 수 있는 OS 업데이트가 표시되며, 등록 시 및 매주
수집됩니다 . 업데이트 확인 을 사용하여 지금 요청하고, 설치 를 사용하여 업데이트를 즉시 설치하거나 (확인 후 기기 재시작) 다운로드만 하여 사용자가 설치하도록 할 수 있습니다. 이는 감독된 iPhone 및 iPad와 Mac 에서 iOS, iPadOS 및 macOS 26까지 작동합니다 . 이후 버전과 많은 기기를 업데이트하려면 정책의 필수

업데이트를 사용하십시오 (소프트웨어 업데이트 페이지 참조).

Apple silicon이 탑재된 Mac은 Bootstrap Token을 인증에 허용하고 토큰이 보관된 경우에만 관리자
비밀번호를 묻지 않고 업데이트를 설치합니다 (위의 Bootstrap Token 참조). 그렇지 않으면 확인 메시지에 업데이트 설치 전에 사용자가 관리자 비밀번호를 입력해야 할 수 있다고 표시됩니다 .

애플리케이션 및 인벤토리

애플리케이션 패널에는 기기의 모든 앱이 하나의 표에 나열됩니다 . 정책 또는 명령으로 설치된 앱의 설치 상태는 기기에서 실시간으로 보고됩니다 . 버전, 크기, 사용자가 설치한 앱은 등록 시 및 매주 수집되는 마지막 앱 목록에서 가져옵니다 . 기기에 요청 을 사용하여 지금 요청할 수 있습니다.

관리: 정책 은 기기 정책으로 설치된 앱, 관리됨 은 앱 설치 와 같은 명령으로 설치된 앱, 관리되지
않음 은 사용자가 설치한 앱입니다. Cerberus Enterprise 앱에는 Cerberus에서 설치함 칩이
표시됩니다 .
주의 필요: 설치에 실패했거나 , 사용자가 거부 또는 제거했거나 , 사용자를 기다리는 앱입니다. 행을
열어 오류를 확인하십시오 . 실패한 정책 앱은 재시도 버튼으로 다시 설치할 수 있습니다. 기기가

검증되지 않았다고 보고하는 내장 앱 및 App Store 앱은 집계되지 않습니다.
앱 제거: 관리되는 앱은 데이터와 함께 제거할 수 있습니다. 정책으로 설치된 앱을 제거하려면
정책에서 제거하십시오 . 관리되는 앱으로 설치된 Mac 패키지가 정책에서 제거될 때 정책도 이
명령을 자체적으로 전송합니다 .

프로필, 인증서 및 보안 패널에는 기기에서 보고한 구성 프로필, 인증서 및 보안 상태 (Mac의 암호, 암호화, FileVault 및 방화벽)가 표시됩니다 .

개인 소유 기기에서는 사용자가 설치한 앱이 수집되지 않으며 Cerberus Enterprise에서 관리하는
프로필과 인증서만 나열됩니다 .

인벤토리 변경 패널에는 기기에서 보낸 두 목록 사이에 변경된 내용이 표시됩니다 . 설치, 제거 또는
업데이트된 앱 (이전 및 새 버전 포함), 설치, 제거 또는 업데이트된 프로필, 추가 또는 제거된 인증서 등입니다. 변경 사항은 기기가 새 목록을 보낼 때 (앱 및 프로필은 매주, 인증서는 매일) 또는 기기에 요청 을 사용할 때 감지됩니다 . 표시되는 날짜는 변경이 감지된 시점이며, 변경은 이전 목록과 해당 목록 사이에 발생했습니다 . 기기의 첫 목록과 새 등록 또는 소유권 변경 후의 첫 목록은 시작 지점으로만 기록됩니다 . 이름 또는 식별자로 검색하고 종류 및 변경으로 필터링할 수 있습니다. 변경 사항은 365일 동안 보관됩니다 .

OS 업데이트로 여러 Apple 앱이 한 번에 교체되면 펼칠 수 있는 한 줄로 표시됩니다 (예: "Apple 앱 23
개 업데이트됨 "). MDM 인증서 갱신은 MDM 인증서 갱신됨 으로 표시됩니다 . 개인 소유 기기에서는
Cerberus Enterprise에서 관리하는 항목의 변경 사항만 표시됩니다 .

Apple 기록 열

생성 날짜
명령
상태: 전송됨 (기기를 기다리는 중이며, 기기가 연결되는 즉시 전달됨), 성공, 응답됨 (결과를
보려면 행을 여세요), 기기 대기 중 (기기가 지금 명령을 실행할 수 없음), 실패 (사유를 보려면 행을 여세요) 또는 취소됨 (기기의 명령 대기열이 지워짐, 예: 기기가 다시 등록된 경우).
실행 날짜

새로 고침
명령 패널의 새로 고침 작업을 사용하여 명령 기록을 다시 불러오십시오 .

Revision #7
Created 2026-11-10 15:17:00 UTC by Admin
Updated 2026-11-12 09:56:28 UTC by Admin