□□ □□

- □□ □□
- □□ □□
- SIM □□
- □□

기기 개요
대시보드 → 기기 에서 기기 행을 클릭하여 기기를 여십시오. 페이지 제목에는 기기 모델 (사용 가능한 경우) 및 내부 ID가 표시됩니다 .

기록 데이터와 현재 등록
기기에 여러 등록이 있는 경우 Cerberus Enterprise는 읽기 전용 기록 레코드를 표시할 수 있습니다. 이 경우 페이지에 기록 데이터 배너와 현재 등록 데이터로 돌아가는 버튼이 표시됩니다 .

상단 필드
상단 섹션은 기기 ID, 할당 및 관리 상태를 요약합니다 . 일부 필드는 플랫폼별로 제공되며 Android 또는 Apple 기기에서만 표시됩니다 .

ID 및 모델: 읽기 전용 식별자입니다 .
사용자: 현재 할당된 사용자 (있는 경우)를 표시합니다 . 사용자 메뉴에서 사용자 열기 또는 사용자
변경 을 선택하거나 , 설정된 사용자가 없으면 사용자를 할당할 수 있습니다.
관리 모드 및 소유권: UI에 툴팁과 함께 표시됩니다 .
상태: 현재 기기 상태 (아이콘 및 도구 설명 세부정보 포함). 분실 모드인 기기는 Android와 Apple 모두에서 분실 로 표시되며, 페이지 상단의 배너에 다음에 수행할 작업이 표시됩니다 .
ADE 프로필 (Apple 전용): 할당된 Automated Device Enrollment 프로필 (있는 경우)을 표시하고 열거나 변경할 수 있습니다.
정책: 할당된 정책을 표시하고 열거나 변경할 수 있으며, 설정된 정책이 없으면 정책을 할당할 수 있습니다.
정책 규정 준수 상태 (정책이 할당된 경우): 기기가 규정을 준수하는지 나타냅니다 .
정책 버전 (정책이 할당된 경우): 기기에 최신 정책 버전이 적용되었는지 나타냅니다 .
Cerberus Enterprise 앱 (iPhone 및 iPad 전용): Cerberus가 기기에 설치하는 Cerberus Enterprise 앱의 상태입니다 . 사용할 수 없음 (iOS 또는 iPadOS 18.4 이전, 회사 기기에 일련번호 없음, 또는 개인 기기에 Managed Apple Account 없음); 개인 기기에서는 아직 사용할 수 없음; 기기 정보 대기 중; Managed Apple Account의 사용자 라이선스 대기 중 (개인 기기, Apple 이 라이선스를 확인하는 동안); 설치되지 않음 (앱이 Apple Business 라이브러리에 없거나 Apps and Books가 설정되지 않음, 계정 설정 링크 포함); 설치됨 · Apps and Books 확인 필요 (토큰이 만료되었거나 앱이 라이브러리에서 제거됨: 앱은 설치된 상태로 유지됨); 구성 사용할 수 없음; 설치 중 … (기기가 30분 동안 상태 보고서를 보내지 않으면 도구 설명에서 기기가 온라인인지 확인하고 재시작하라고 제안하며, 일반적으로 이렇게 하면 설치가 다시 시작됨); 사용자 승인 대기 중; 사용자가 거부함 및 설치 실패 (둘 다 재시도 로 기기에 다시 요청함); 설치됨 · 앱 시작 대기 중 (앱이 아직 열리지 않음); 설치됨 · 구성이 수락되지 않음; 앱이 등록되면 버전, 마지막 연결 및

알림 활성화 여부가 표시됩니다 .
등록일 및 마지막 상태 보고: 등록 및 마지막으로 보고된 상태의 타임스탬프입니다 .
등록 해제일: 기기가 등록 해제된 경우 표시됩니다 .

일부 데이터와 패널은 기기 정책에서 해당 범주가 활성화된 경우에만 사용할 수 있습니다. 자세한

내용은 상태 보고 및 위치 및 지오펜스 페이지를 참조하세요 .

패널
기기 페이지는 확장 가능한 섹션으로 구성됩니다 . 플랫폼과 상태에 따라 다음 패널 중 하나 이상이 표시될 수 있습니다:

위치 지도: 현재 기기의 위치 기록과 Android 기기, iPhone 및 iPad의 지오펜스 전환을 위한
지오펜스 탭이 있는 탭 패널입니다 .
SIM 관리: 기기 EID와 설치된 SIM 및 eSIM입니다. Android에서는 eSIM 명령과 해당 기록도
표시되며, 회사 소유의 iPhone 및 셀룰러 iPad에서는 데이터 로밍, 개인용 핫스팟 및 셀룰러

요금제 새로 고침 도 표시됩니다 . 전용 SIM 관리 페이지를 참조하십시오 .
명령: 기기에 명령을 보내고 명령 기록을 확인합니다 (플랫폼별로 다름).
보안 상태: 기기의 보안 상태와 위험 요소입니다 . Android에서는 Play Integrity 판정도 포함됩니다
. 기기가 보고할 때까지 지정되지 않음, 또는 보안 데이터를 보내지 않은 Android 기기에서는 아직 보고되지 않음 이 (가) 표시됩니다 .
기기가 규정을 준수하지 않는 이유: 기기가 규정을 준수하지 않을 때만 빨간색 경고 아이콘과
함께 표시됩니다 . 열어서 사유를 확인하세요 . Android에서는 준수하지 않는 정책 설정을 나열하고, Apple에서는 규정 준수 규칙이 기기를 차단했는지도 표시합니다 .
기기 상태 (Apple 전용): 기기가 보고한 OS 버전, 소프트웨어 업데이트 진행 상황, 암호, FileVault, 배터리 및 계정, 그리고 사용 가능한 OS 업데이트입니다 . 명령 페이지를 참조하십시오 .
애플리케이션 (Android): 설치된 앱과 해당 앱의 피드백 및 오류 보고서입니다 .
애플리케이션 (Apple 전용): 정책으로 설치된 앱, 명령으로 설치된 앱 및 사용자가 설치한 앱과 해당 설치 상태, 오류 및 작업 (재시도, 제거)입니다. Mac에서는 정책으로 설치된 패키지도 해당 상태 및 다시 설치 와 함께 나열됩니다 . 관리형 앱으로 설치된 패키지에는 관리형 칩이 표시되며, 패키지가 비관리형으로 설치된 경우와 그 이유, 또는 다운로드 후 한 시간이 지나도 해당 앱을 찾지 못한
경우에 대한 참고 사항이 표시됩니다 . iPhone 및 iPad에서 Cerberus Enterprise 앱에는 Cerberus 에서 설치함 칩이 표시되며 정책 필터 아래에는 나열되지 않습니다. 기기가 관리형 구성을
수락하지 않은 앱에는 구성이 수락되지 않음 칩이 표시됩니다 . 개인 iPhone 및 iPad(사용자 등록) 에서는 한 줄에 App Store 앱이 사용하는 라이선스의 사용자를 보유한 Managed Apple Account가 표시되고, 라이선스를 기다리는 앱에는 사용자 라이선스 대기 중 또는 사용자 라이선스 실패 가 표시되며, 사용자가 설치 프롬프트를 취소한 앱에는 사용자 설치 승인 대기 중 이 표시됩니다 . 다시

요청 은 Apple에 라이선스를 다시 요청하거나 프롬프트를 다시 표시합니다 . 명령 페이지를
참조하십시오 .
프로필, 인증서 및 보안 (Apple 전용): 기기가 보고한 구성 프로필, 인증서 및 보안 상태입니다 .

인벤토리 변경 (Apple 전용): 기기에서 설치, 제거 또는 업데이트된 앱, 프로필 및 인증서의
타임라인으로 , 검색할 수 있고 종류 및 변경 사항별로 필터링할 수 있습니다. 명령 페이지를
참조하십시오 .
Shared iPad 사용자 및 Mac 사용자 (Apple 전용): Shared iPad 사용자와 Mac 사용자입니다 .
명령 페이지를 참조하세요 .
상태 보고서: 기기가 보고한 추가 데이터로, 카테고리와 값의 트리로 표시됩니다 .
등록 기록: 동일한 실제 기기에 대한 이전 등록을 목록으로 표시합니다 .

위치 패널 탭
위치 지도 패널은 탭을 사용하여 위치 기록과 지오펜스 전환을 구분합니다 .

위치: 현재 기기의 기록 필터, 날짜 범위 검색, 위치 마커, 정확도 원 및 실시간 추적 컨트롤을
표시합니다 .
지오펜스 (Android, iPhone 및 iPad): 전용 지도에 지오펜스 전환 기록을 표시하며, 기간 필터,
선택적 보관된 지오펜스 토글 및 전환의 측면 목록이 있습니다. iPhone 및 iPad에서는 상태 줄에
기기에서 지오펜싱이 작동할 수 없는 경우도 알려 줍니다.

이 탭의 전체 동작은 위치 지도 를 참조하십시오 .

작업
페이지 하단에서 플랫폼, 기기 상태 및 라이선스 상태에 따라 데이터를 새로 고치고 작업을 수행할 수 있습니다

.

데이터 새로 고침: 기기 레코드를 다시 로드합니다 .
기기 비활성화 / 기기 활성화 (Android 전용): 지원되는 상태에서 사용할 수 있습니다.
기기 등록 해제: 기기에서 관리를 제거합니다 . 정확한 동작은 플랫폼과 소유권에 따라 다릅니다 (예: Android는 직장 프로필을 초기화하거나 공장 초기화할 수 있음).
기기 삭제: 기기가 이미 등록 해제되어 해당 레코드를 제거할 수 있을 때 사용할 수 있습니다.

위치 지도

이 페이지는 기기 개요 에서 사용할 수 있는 기기별 위치 도구를 설명합니다 . 패널에는 위치 기록을 위한 위치 탭과 Android 기기, iPhone 및 iPad의 지오펜스 전환을 위한 지오펜스 탭이 있습니다.

사전 요구 사항
Android에서는 기기 정책에서 위치 보고가 활성화된 경우에만 기기 위치 데이터가 표시됩니다 . 활성화하려면

정책을 열고 위치 및 지오펜스 → 위치 보고 를 켜세요. 자세한 내용은 위치 및 지오펜스 를 참조하세요 .

iPhone 및 iPad에서 위치는 사용자가 허용한 후 Cerberus Enterprise 앱에서 제공되거나 , 기기가 분실 모드일 때 기기 찾기 명령에서 제공됩니다 . Mac 및 기타 Apple 기기는 위치를 보고하지 않습니다.

완전히 관리되지 않는 기기에서는 위치 데이터가 Cerberus Enterprise 앱에 필요한 위치 권한이
있는지와 기기의 위치 서비스가 활성화되어 있는지에 따라 달라질 수 있습니다.

개인 기기 (User Enrollment)에서는 Apple 정책에서 개인 기기의 위치 및 지오펜스 가 켜져 있고
사용자가 Cerberus Enterprise 앱의 위치 접근을 허용한 경우에만 위치 및 지오펜스를 사용할 수 있습니다. 그렇지 않으면 해당 기기 페이지에 위치 작업이나 실시간 추적이 표시되지 않습니다. 분실 모드는 개인 기기에서 절대 사용할 수 없습니다.

대시보드에서 사용할 수 있는 전역 다중 기기 지도는 대시보드 위치 지도 를 참조하십시오 .

로딩 및 데이터 없음 상태
위치 데이터를 로드하는 동안 패널의 지도에 로딩 오버레이가 표시됩니다 .
기기에 사용 가능한 위치 데이터가 없으면 패널에 사용 가능한 위치 데이터 없음 이라는 메시지가
표시됩니다 . Android에서는 할당된 정책에서 위치 보고가 꺼져 있을 때 이를 활성화하라는 알림이 추가됩니다 . Apple에서는 위치의 출처를 설명하거나 이 유형의 기기는 위치를 보고하지 않는다고 표시합니다 .
날짜 필터가 활성화되어 있고 일치하는 샘플이 없으면 패널에 선택한 날짜 범위에 사용 가능한 데이터 없음 이 표시됩니다 .

위치 탭
위치 탭을 열어 단일 기기의 기록을 검사하십시오 . 사용 가능한 필터에는 마지막으로 확인된 위치, 최근 기록 범위, 사용자 지정 날짜 범위 및 실시간 추적이 있습니다.

마지막: 마지막으로 확인된 위치를 표시합니다 .
오늘, 지난 7일, 지난 30일: 선택한 기간의 기록된 위치를 표시합니다 .
검색: 사용자 지정 날짜 범위를 선택할 수 있습니다.
실시간: 현재 기기의 실시간 추적을 시작하거나 중지합니다 .

위치는 90일 동안 보존되며, 이보다 오래된 위치는 매일 밤 자동으로 삭제됩니다 . 등록된 각 기기의
최신 위치는 항상 보존되므로 오랫동안 보고하지 않은 경우에도 기기가 지도에 계속 표시됩니다 . 제거된 기기와 이전 등록의 경우 90일이 지난 위치는 모두 삭제됩니다 . 이러한 이유로 검색 날짜
범위는 90일보다 이전부터 시작할 수 없습니다.

마커 세부 정보
위치 마커를 클릭하면 다음 정보가 포함된 정보 창이 열립니다:

위치 기록의 타임스탬프입니다 .
보고된 정확도 (미터 단위)입니다.
기기가 제공하는 경우 보고된 속도 입니다.
기기가 제공하는 경우 보고된 방향 또는 방위입니다 .

정확도 원
정보 창이 열려 있으면 마커 주위에 정확도 원이 표시됩니다 . 원의 반지름은 보고된 정확도 (미터 단위)에 해당합니다 . 정보 창을 닫으면 원이 숨겨집니다 .

실시간 추적
기기 기록 보기에서 실시간 필터를 선택하면 해당 기기에 대한 실시간 추적 요청이 시작됩니다 . Cerberus Enterprise는 요청을 시작하기 전에 확인을 요청합니다 .

실시간 추적은 최대 15분 동안 실행됩니다 .

실시간 추적이 활성화되어 있는 동안 Android 기기에는 알림이 표시되고 iPhone 및 iPad에는 위치
표시기가 표시됩니다 .
실시간 추적이 활성화되어 있는 동안 패널은 최신 위치를 계속 새로 고치며 실시간 표시기는 계속
표시됩니다 .
실시간 필터를 다시 선택하면 시간 초과 전에 실시간 추적을 중지할 수 있습니다.
iPhone 및 iPad에서 실시간 추적은 위치 접근 권한이 항상 으로 설정된 상태에서 Cerberus
Enterprise 앱을 통해 실행됩니다 . 이 요청은 일반적으로 앱이 열려 있지 않아도 앱을 깨우며, 앱은
전체 세션 동안 위치를 전송합니다 . iOS는 이러한 요청을 보장하지 않습니다. 예를 들어 저전력
모드이거나 네트워크에 연결되어 있지 않으면 요청이 지연되거나 전달되지 않을 수 있습니다. 2분
이내에 위치가 도착하지 않으면 대시보드가 요청을 취소합니다 . 사용자에게 앱을 한 번 열어 달라고
요청한 다음 다시 시도하십시오 .

지오펜스 탭
Android 기기, iPhone 및 iPad에서 두 번째 탭에는 할당된 정책에 정의된 지오펜스에서 생성된 지오펜스
전환이 표시됩니다 .

지도에는 기록된 전환 지점과 함께 현재 지오펜스 영역이 표시됩니다 .
오른쪽의 전환 목록에서 진입 및 이탈 이벤트를 확인할 수 있습니다.
사용 가능한 필터는 오늘, 최근 7일, 최근 30일 및 사용자 지정 날짜 범위 검색입니다 .
보관된 항목 포함 옵션을 선택하면 현재 정책에 더 이상 없는 이전 지오펜스 정의와 관련된 전환도
표시됩니다 .
지오펜스 전환은 90일 동안 보존되며 이보다 오래된 전환은 매일 밤 자동으로 삭제되므로 , 사용자
지정 날짜 범위 검색은 90일보다 이전부터 시작할 수 없습니다.

iPhone 및 iPad에서는 정책에 활성 지오펜스가 있으면 탭 상단의 상태 줄에 기기에서 지오펜싱이 작동하는지
표시됩니다 . 작동할 수 없는 경우를 알려 줍니다. Cerberus Enterprise 앱이 서버에 연결된 적이 없거나
업데이트해야 하는 경우, 위치 접근 권한이 항상, 정확한 위치 또는 백그라운드 앱 새로 고침 으로 설정되어
있지 않은 경우, 앱이 마지막으로 설정을 보고했을 때 저전력 모드 가 켜져 있었던 경우 (이 경우 지오펜스
이벤트와 변경 사항이 몇 시간 지연될 수 있음), 또는 앱이 최신 지오펜스를 아직 적용하지 않은 경우입니다 .
모든 것이 정상적으로 작동하면 앱이 모니터링하는 지오펜스 수가 표시됩니다 .

지오펜스 전환 세부정보
전환을 선택하면 지도에서 해당 세부정보가 열리고 목록의 해당 항목이 강조 표시됩니다 . 가능한 경우
Cerberus Enterprise는 해당 전환의 기기 좌표와 보고된 정확도도 표시합니다 .

SIM 관리
기기 페이지에는 SIM 관리 패널이 있습니다. Android 기기에서는 기기에 설치된 SIM 및 eSIM 프로필을 관리하고, eSIM 프로필을 추가하거나 제거하며, 기기로 전송된 eSIM 명령 기록을 표시합니다 . 회사 소유 iPhone 및 셀룰러 iPad에서는 기기가 보고한 SIM 및 eSIM 요금제를 표시하고 기기가 통신사에서 준비한 eSIM 요금제를 다운로드할 수 있게 합니다. 아래의 iPhone 및 iPad를 참조하세요 .

기기 정책에서 네트워크 정보 보고가 활성화되어 있으면 완전 관리형 기기에서 SIM 정보가

보고됩니다 (Cerberus Enterprise는 이 옵션을 항상 활성화합니다). 상태 보고 페이지를 참조하십시오

.

기기 EID
EID(eUICC 식별자)는 기기의 eSIM 하드웨어를 식별합니다 . 통신사는 EID를 사용하여 eSIM 프로필을 기기에 바인딩하므로 , EID를 검색하는 것은 일반적으로 eSIM 프로비저닝 워크플로의 첫 번째 단계입니다 .

회사 소유 기기 (Android 13 이상): EID는 기기 상태와 함께 자동으로 보고되며 사용자 상호 작용이
필요하지 않습니다.
개인 소유 기기 (Android 13 이상): EID 요청 버튼을 사용하십시오 . 사용자는 기기에서 EID 공유를
요청하는 알림을 보게 되며 요청을 승인하거나 거부할 수 있습니다. EID는 사용자가 승인한
경우에만 표시됩니다 . 요청이 대기 중인 동안 버튼은 비활성 상태로 유지됩니다 .

EID 요청을 보내면 사용자가 기기에서 알림을 보게 되므로 먼저 확인 대화상자가 표시됩니다 .

설치된 SIM
설치된 SIM 표에는 실제 SIM 및 eSIM 프로필을 포함하여 현재 기기에 대해 알려진 SIM이 나열됩니다 . 개인 소유 기기에서는 기기가 SIM 정보를 보고하지 않더라도 eSIM 추가 명령으로 설치된 eSIM 프로필이
표시됩니다 .

통신사: SIM과 연결된 통신사 이름 (보고된 경우)입니다.
전화번호 : SIM과 연결된 전화번호 (보고된 경우)입니다.
ICCID: SIM의 집적 회로 카드 식별자입니다 .
활성화 상태: eSIM이 활성화되었는지 여부입니다 . Android 15 이상의 eSIM에 대해서만
보고됩니다 .

구성 모드: eSIM이 관리자 또는 사용자에 의해 구성되었는지 여부입니다 . Android 15 이상의 eSIM
에 대해서만 보고됩니다 .
SIM 유형: 기기가 해당 항목을 eSIM으로 보고하는지 표시합니다 .

진행 중이거나 실행된 (실패하지 않은) 제거 명령이 있는 eSIM은 임시 제거 중 활성화 상태를
표시합니다 . 기기가 업데이트된 SIM 목록을 보고하면 해당 항목이 목록에서 사라집니다 . 제거가 진행
중인 동안에는 동일한 명령이 두 번 전송되지 않도록 제거 버튼을 사용할 수 없습니다.

eSIM 제거

설치된 eSIM 옆의 제거 버튼을 사용하여 기기에서 해당 프로필을 제거하십시오 . 명령이 전송되기 전에 확인 대화상자에서 제거할 eSIM의 ICCID를 확인하도록 요청합니다 . eSIM 제거는 Android 15 이상에서
지원됩니다 .

eSIM 추가
eSIM 추가 섹션에서는 기기에 새 eSIM 프로필을 설치합니다 (Android 15 이상 지원). 다음 항목이
필요합니다 :

유효 기간: 명령을 즉시 실행할 수 없는 경우 명령이 유효한 기간입니다 .
활성화 코드: 통신사에서 제공하는 eSIM 프로필의 활성화 코드입니다 . 전체 코드를 입력하거나
SM-DP+ 주소만 입력하여 기기가 통신사가 이미 EID에 연결한 프로필을 검색하도록 할 수 있습니다

.

활성화 상태: 다운로드 후 eSIM 프로필을 자동으로 활성화할지 , 아니면 사용자가 수동으로
활성화할 수 있도록 비활성 상태로 둘지 여부입니다 .

명령 기록
eSIM 추가 섹션 아래에서 패널은 기기로 전송된 eSIM 명령의 기록을 표시합니다 : eSIM 추가, eSIM 제거, EID 요청. 표는 정렬할 수 있으며 페이지 매김을 지원합니다 . 일부 행을 확장하여 명령 매개변수 (예: 활성화
코드 또는 ICCID)와 실행 상태를 볼 수 있으며, 기기에서 작업이 실패하면 eSIM 오류 세부정보도 포함됩니다 .

생성 날짜
명령
유효 기간
상태
오류: 명령 실행에서 보고된 경우 eSIM 오류 상태 (예: 사용자 거부, 잘못된 활성화 코드 또는 ICCID
를 찾을 수 없음)를 표시합니다 .
실행 날짜

초기화 및 등록 해제 시 eSIM 지우기
명령 패널에서 기기를 초기화할 때 eSIM 지우기 플래그는 초기화와 함께 eSIM 프로필을 제거할지 여부를 제어합니다 . 직장 프로필이 있는 개인 소유 기기에서는 이 플래그가 기본적으로 활성화되어 있습니다 (관리형 eSIM은 제거되고 개인 소유 eSIM은 영향을 받지 않음). 기기 등록 해제 확인 대화상자에서도 동일한
플래그를 사용할 수 있습니다.

iPhone 및 iPad
이 패널은 iPhone 및 셀룰러 데이터를 보고한 iPad(Wi-Fi 전용 iPad에는 없음)에 표시되며, 기기가 회사
소유이고 사용자 등록이 아닌 경우에만 표시됩니다 . 기기 정보와 함께 기기의 셀룰러 정보를 요청합니다 . 등록 시, 매일, 기기 정보 새로 고침 시, 소유권이 회사 소유로 변경될 때, 그리고 셀룰러 요금제 새로 고침 후 몇 분 뒤에 요청합니다 .

기기 EID: SIM과 함께 보고된 EID이며, 통신사에 제공할 수 있도록 복사하는 버튼이 있습니다.
기기가 보고하지 않는 경우 사용자는 설정 > 일반 > 정보에서 확인할 수 있습니다.
보고됨, 데이터 로밍, 개인용 핫스팟 및 모뎀 펌웨어: 기기가 응답했는지와 보고한 상태입니다 .
데이터 로밍 및 개인용 핫스팟은 명령 패널의 기기 설정 으로 변경할 수 있으며, 여기에는 현재
상태도 표시됩니다 .
SIM: SIM 또는 eSIM 요금제당 한 행 (듀얼 SIM 기기는 두 개)으로, 기기가 보고한 슬롯, 레이블 및 유형 (기기가 EID와 함께 보고하면 eSIM, 그렇지 않으면 SIM 카드), 통신사 (기기가 다른
네트워크에서 로밍 중인 경우 툴팁에 홈 통신사 표시), 전화번호, ICCID, EID, IMEI, 데이터 및 통화에 사용되는 SIM, 로밍이 표시됩니다 . 요금제가 없는 eSIM 슬롯은 요금제 없음 으로 회색 표시됩니다 .
이 기기는 SIM을 보고하지 않았습니다 는 기기가 SIM 없이 응답했음을 의미합니다 . 아직 셀룰러
정보가 없습니다 는 아직 응답하지 않았음을 의미합니다 : 기기 정보 새로 고침 을 사용하십시오 .

전화번호, ICCID, IMEI 및 EID는 사람과 회선을 식별합니다 . 이러한 정보는 개인 소유 기기나 사용자
등록에 대해 절대 요청되지 않습니다. 기기가 개인 소유가 되면 정보가 즉시 제거되고 명령 기록에서
이전 기기 정보 명령의 결과에서 숨겨집니다 . 내보내지 않으며 시스템 로그에도 기록되지 않습니다.

셀룰러 요금제 새로 고침

iPhone 및 iPad는 활성화 코드로 eSIM을 설치할 수 없습니다. 통신사는 eSIM 서버 (SM-DP+)에서 eSIM 요금제를 기기의 EID에 바인딩 (예약)하고 해당 서버의 주소를 제공합니다 . 그런 다음 셀룰러 요금제 새로 고침 은 기기에 대기 중인 요금제를 다운로드하도록 요청합니다 . 패널의 셀룰러 요금제 새로 고침 버튼은 명령 패널에서 명령을 선택하며, 여기에서 통신사 eSIM 서버 URL을 입력합니다 :

https:// 주소: 그대로 전송됩니다 . http://, 사용자 이름 또는 비밀번호, 또는 # 부분이 포함된
주소는 허용되지 않습니다.

호스트 이름 (예: smdp.carrier.example)은 https://smdp.carrier.example로 전송됩니다 .
LPA 활성화 코드 (LPA:1$server$code, eSIM QR 코드의 텍스트): 명령이 코드를 전달할 수
없으므로 서버만 사용됩니다 . 통신사가 요금제를 기기 EID에 바인딩해야 하며, 그렇지 않으면
기기가 다운로드할 항목을 찾지 못합니다.

기기는 감독되지 않는 경우에도 사용자에게 묻지 않고 요금제를 설치하고 활성화합니다 . 명령 기록의 성공은 기기가 요청을 수락했음을 의미하며 요금제가 설치되었음을 의미하지는 않습니다. 설치에는 최대 3분이 걸릴 수 있으며, Cerberus Enterprise는 약 3분 후에 기기에 SIM을 다시 요청하므로 새 요금제가 패널에
표시됩니다 . 오류 36001(기기가 셀룰러 시스템에 연결할 수 없음), 36002(eSIM 지원 없음) 및 36003(셀룰러 시스템 사용 중, 나중에 다시 시도)은 시스템 로그에 설명되어 있습니다. 한 번 다운로드한 요금제는 다시 다운로드할 수 없습니다. 설치에 실패하면 통신사에 문의하십시오 . 이 명령은 기기 페이지의 Apple 기기 작업 메뉴에서 여러 기기에 동시에 사용할 수도 있습니다.

Apple이 허용하지 않는 작업
활성화 코드로 eSIM 추가: 불가능합니다 . EID에 바인딩된 요금제와 함께 셀룰러 요금제 새로
고침 을 사용하십시오 .
eSIM 제거: eSIM은 원격으로 하나씩 제거할 수 없습니다. eSIM 데이터 요금제 유지 를 끈 상태로
기기를 지우면 모든 eSIM이 제거됩니다 . 단일 요금제를 중지하려면 통신사에 비활성화를
요청하십시오 . 요금제는 기기에 남아 있지만 연결할 수 없습니다.
EID 요청: 필요하지 않습니다. EID는 회사 소유 기기의 SIM과 함께 제공됩니다 .
Mac에는 셀룰러 또는 eSIM 관리 기능이 없습니다.

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 .