Stato Dispositivo

- Panoramica dispositivo
- Mappa delle posizioni
- Gestione SIM
- Comandi

Panoramica dispositivo

Apri un dispositivo da **Dashboard** → **Dispositivi** facendo clic sulla riga del dispositivo. Il titolo della pagina mostra il **Modello** del dispositivo (quando disponibile) e l'**Id** interno.

Dati storici e registrazione corrente

Quando un dispositivo ha più registrazioni, Cerberus Enterprise può mostrare un record storico di sola lettura. In tal caso, la pagina visualizza un banner **Dati storici** e un pulsante per tornare ai dati della registrazione corrente.

Campi principali

La sezione superiore riassume l'identità del dispositivo, l'assegnazione e lo stato di gestione. Alcuni campi sono specifici della piattaforma e compaiono solo per dispositivi Android o Apple.

- **Id** e **Modello**: identificatori di sola lettura.
- **Utente**: mostra l'utente attualmente assegnato (se presente). Dal menu utente puoi **Apri utente** o **Cambia utente**, oppure assegnare un utente quando non ce n'è uno impostato.
- **Modalità di gestione** e **Proprietà**: visualizzati con tooltip nell'interfaccia.
- **Stato**: stato attuale del dispositivo (con icona e dettagli nel tooltip). Un dispositivo in modalità smarrito mostra **Smarrito** sia su Android sia su Apple, e un banner nella parte superiore della pagina indica cosa fare successivamente.
- **Profilo ADE** (solo Apple): mostra il profilo di registrazione automatica dei dispositivi assegnato (se presente) e ti consente di aprirlo o modificarlo.
- **Policy**: mostra la policy assegnata e ti consente di aprirla o modificarla, oppure di assegnarne una quando non ce n'è nessuna impostata.
- **Stato di conformità della policy** (quando è assegnata una policy): indica se il dispositivo è conforme.
- **Versione della policy** (quando è assegnata una policy): indica se sul dispositivo è applicata l'ultima versione della policy.
- **App Cerberus Enterprise** (solo iPhone e iPad): lo stato dell'app Cerberus Enterprise che Cerberus installa sul dispositivo. **Non disponibile** (iOS o iPadOS precedente alla 18.4, nessun numero di serie su un dispositivo aziendale o nessun Managed Apple Account su un dispositivo personale); **Non ancora disponibile sui dispositivi personali**; **In attesa**

delle informazioni sul dispositivo; **In attesa della licenza utente del Managed Apple Account** (dispositivi personali, mentre Apple conferma la licenza); **Non installata** (l'app non è nella tua libreria Apple Business o Apps and Books non è configurato, con un collegamento a **Impostazioni account**); **Installata · Apps and Books richiede attenzione** (il token è scaduto o l'app ha lasciato la tua libreria: l'app resta installata); **Configurazione non disponibile**; **Installazione…** (se il dispositivo non invia rapporti di stato per 30 minuti, il tooltip suggerisce di verificare che sia online e di riavviarlo, cosa che di solito riavvia l'installazione); **In attesa dell'approvazione dell'utente**; **L'utente ha rifiutato** e **Installazione non riuscita** (entrambi con **Riprova**, che interroga di nuovo il dispositivo); **Installata · in attesa dell'avvio dell'app** (l'app non è ancora stata aperta); **Installata · configurazione non accettata**; e, una volta registrata l'app, la sua versione, l'ultimo contatto e se le notifiche sono attive.
- **Registrato il** e **Ultima segnalazione di stato**: timestamp per la registrazione e l'ultimo stato riportato.
- **Registrazione annullata il**: mostrato quando la registrazione del dispositivo è stata annullata.

> Alcuni dati e pannelli sono disponibili solo quando la categoria corrispondente è abilitata nella policy del dispositivo. Per maggiori informazioni leggi le pagine **Segnalazione dello stato** e **Posizione e geofence**.

Pannelli

La pagina del dispositivo è organizzata in sezioni espandibili. A seconda della piattaforma e dello stato, potresti vedere uno o più dei seguenti pannelli:

- **Mappa posizioni**: un pannello a schede con la cronologia **Posizione** del dispositivo corrente e, su dispositivi Android, iPhone e iPad, una scheda **Geofence** per le transizioni geofence.
- **Gestione SIM**: EID del dispositivo e SIM ed eSIM installate. Su Android anche i comandi eSIM e la loro cronologia; su iPhone e iPad aziendali con cellulare anche roaming dati, Hotspot personale e **Aggiorna piani cellulari**. Vedi la pagina dedicata **Gestione SIM**.
- **Comandi**: invia comandi al dispositivo e visualizza la cronologia dei comandi (specifico della piattaforma).
- **Postura di sicurezza**: lo stato di sicurezza del dispositivo e i suoi rischi. Su Android anche il verdetto di Play Integrity. Finché il dispositivo non lo segnala, indica **Non specificato**, oppure **Non ancora segnalato** su un dispositivo Android che non ha inviato alcun dato di sicurezza.
- **Perché il dispositivo non è conforme**: mostrato solo quando il dispositivo non è conforme, con un'icona di avviso rossa; aprilo per vedere i motivi. Su Android elenca le impostazioni della policy non conformi; su Apple indica anche se una regola di conformità

ha bloccato il dispositivo.

- **Stato del dispositivo** (solo Apple): versione del sistema operativo, avanzamento dell'aggiornamento software, codice di accesso, FileVault, batteria e account riportati dal dispositivo, e gli aggiornamenti del sistema operativo disponibili. Vedi la pagina **Comandi**.
- **Applicazioni** (Android): app installate e relativi feedback e segnalazioni di errore.
- **Applicazioni** (solo Apple): le app installate dalla policy, le app installate con i comandi e le app installate dall'utente, con il loro stato di installazione, errori e azioni (riprova, rimuovi). Su Mac elenca anche i pacchetti installati dalla policy, con il loro stato e **Installa di nuovo**; i pacchetti installati come app gestite hanno un'etichetta **Gestita**, e una nota indica quando un pacchetto è stato installato non gestito e perché, oppure quando la sua app non è stata trovata un'ora dopo il download. Su iPhone e iPad l'app Cerberus Enterprise ha l'etichetta **Installata da Cerberus**; non è elencata sotto il filtro **Policy**. Un'app la cui configurazione gestita non è stata accettata dal dispositivo ha l'etichetta **Configurazione non accettata**. Su iPhone e iPad personali (registrazione utente) una riga mostra l'Account Apple gestito le cui licenze utente usano le app dell'App Store; le app in attesa della licenza mostrano **In attesa di una licenza utente** o **Licenza utente non riuscita**, un'app la cui richiesta di installazione è stata annullata dall'utente mostra **In attesa dell'approvazione dell'installazione da parte dell'utente**, e **Richiedi di nuovo** chiede di nuovo ad Apple la licenza o mostra di nuovo la richiesta. Vedi la pagina **Comandi**.
- **Profili, certificati e sicurezza** (solo Apple): profili di configurazione, certificati e stato di sicurezza riportati dal dispositivo.
- **Modifiche all'inventario** (solo Apple): una cronologia delle app, dei profili e dei certificati installati, rimossi o aggiornati sul dispositivo, con ricerca e filtri per tipo e modifica. Vedi la pagina **Comandi**.
- **Utenti di iPad condiviso** e **Utenti Mac** (solo Apple): gli utenti di un iPad condiviso e gli utenti di un Mac. Consulta la pagina **Comandi**.
- **Report di stato**: dati aggiuntivi riportati dal dispositivo, visualizzati come un albero di categorie e valori.
- **Cronologia delle registrazioni**: registrazioni precedenti per lo stesso dispositivo fisico, mostrate come elenco.

Schede del pannello Posizione

Il pannello **Mappa delle posizioni** usa schede per tenere separati la cronologia delle posizioni e i passaggi dei geofence.

- **Posizione**: mostra filtri della cronologia, una ricerca per intervallo di date, i marker delle posizioni, il cerchio di precisione e i controlli del tracciamento in tempo reale per il dispositivo corrente.
- **Geofence** (Android, iPhone e iPad): mostra la cronologia delle transizioni geofence su una mappa dedicata, con filtri per periodo, un interruttore facoltativo per i geofence archiviati

e un elenco laterale delle transizioni. Su iPhone e iPad una riga di stato indica anche quando il geofencing non può funzionare sul dispositivo.

Per il comportamento completo di queste schede, vedi **Mappa posizioni**.

Azioni

In fondo alla pagina puoi aggiornare i dati ed eseguire azioni a seconda della piattaforma, dello stato del dispositivo e dello stato della licenza.

- **Aggiorna dati**: ricarica il record del dispositivo.
- **Disabilita dispositivo** / **Abilita dispositivo** (solo Android): disponibile negli stati supportati.
- **Annulla registrazione dispositivo**: rimuove la gestione dal dispositivo. Il comportamento esatto dipende dalla piattaforma e dalla proprietà (ad esempio, Android può cancellare un profilo di lavoro o ripristinare le impostazioni di fabbrica).
- **Elimina dispositivo**: disponibile quando il dispositivo ha già annullato la registrazione e il suo record può essere rimosso.

Mappa delle posizioni

Questa pagina descrive gli strumenti di posizione specifici del dispositivo disponibili in **Panoramica dispositivo**. Il pannello contiene una scheda **Posizione** per la cronologia delle posizioni e, sui dispositivi Android, iPhone e iPad, una scheda **Geofence** per le transizioni dei geofence.

Prerequisiti

Su Android, i dati di posizione del dispositivo vengono mostrati solo quando la segnalazione della posizione è abilitata nella policy del dispositivo. Per abilitarla, apri la policy e attiva **Posizione e geofence** → **Segnala posizione**. Per maggiori dettagli, consulta **Posizione e geofence**.

Su iPhone e iPad, la posizione proviene dall'app Cerberus Enterprise, una volta che l'utente la consente, oppure dal comando **Localizza dispositivo** mentre il dispositivo è in modalità smarrito. I Mac e gli altri dispositivi Apple non segnalano la loro posizione.

> Sui dispositivi non completamente gestiti, i dati sulla posizione possono comunque dipendere dall'app Cerberus Enterprise che dispone delle autorizzazioni di posizione richieste e dall'attivazione dei servizi di localizzazione sul dispositivo.

> Sui dispositivi personali (User Enrollment), posizione e geofence sono disponibili solo quando nella policy Apple è attiva l'opzione **Posizione e geofence sui dispositivi personali** e solo se l'utente consente la posizione per l'app Cerberus Enterprise. In caso contrario la pagina del dispositivo non mostra le azioni di posizione o il tracciamento in tempo reale. La modalità smarrito non è mai disponibile sui dispositivi personali.

> Per la mappa globale multi-dispositivo disponibile dalla dashboard, vedi **Mappa delle posizioni della dashboard**.

Stato di caricamento e assenza di dati

- Mentre i dati sulla posizione vengono caricati, il pannello mostra un overlay di caricamento sulla mappa.
- Se il dispositivo non ha dati di posizione disponibili, il pannello mostra un messaggio che indica **Nessun dato di posizione disponibile**. Su Android aggiunge un promemoria per abilitare la segnalazione della posizione nella policy assegnata, quando è disattivata. Su Apple indica da dove proviene la posizione o che questo tipo di dispositivo non la segnala.
- Se è attivo un filtro per data e nessun campione corrisponde, il pannello mostra **Nessun dato disponibile nell'intervallo di date selezionato**.

Scheda Posizione

Apri la scheda **Posizione** per esaminare la cronologia di un singolo dispositivo. I filtri disponibili includono l'ultima posizione nota, intervalli recenti della cronologia, un intervallo di date personalizzato e il tracciamento in tempo reale.

- **Ultima**: mostra l'ultima posizione nota.
- **Oggi**, **Ultimi 7 giorni** e **Ultimi 30 giorni**: mostrano le posizioni registrate per il periodo selezionato.
- **Cerca**: ti consente di scegliere un intervallo di date personalizzato.
- **Live**: avvia o interrompe il tracciamento in tempo reale per il dispositivo corrente.

> Le posizioni vengono conservate per **90 giorni**: quelle più vecchie vengono eliminate automaticamente ogni notte. L'ultima posizione di ogni dispositivo registrato viene sempre conservata, così il dispositivo resta sulle mappe anche quando non invia dati da molto tempo. Per i dispositivi rimossi e le registrazioni passate, le posizioni più vecchie di 90 giorni vengono eliminate tutte. Per questo motivo l'intervallo di date di **Cerca** non può iniziare più di 90 giorni fa.

Dettagli del marcatore

Quando fai clic su un marcatore di posizione, si apre una finestra informativa con:

- Il timestamp del record di posizione.
- La **precisione** riportata (in metri).
- La **velocità** riportata, quando il dispositivo la fornisce.
- La **direzione** o il rilevamento riportati, quando il dispositivo li fornisce.

Cerchio di precisione

Quando la finestra informativa è aperta, intorno al marker viene visualizzato un cerchio di precisione. Il raggio del cerchio corrisponde alla precisione riportata (in metri). Chiudendo la finestra informativa il cerchio scompare.

Tracciamento in tempo reale

Nella vista della cronologia del dispositivo, selezionando il filtro **Live** viene avviata una richiesta di tracciamento in tempo reale per quello specifico dispositivo. Cerberus Enterprise chiede conferma prima di avviare la richiesta.

- Il tracciamento in tempo reale dura fino a **15 minuti**.
- Mentre il tracciamento in tempo reale è attivo, i dispositivi Android mostrano una notifica e iPhone e iPad mostrano l'indicatore di posizione.
- Mentre il tracciamento in tempo reale è attivo, il pannello continua ad aggiornare l'ultima posizione e l'indicatore live rimane visibile.
- Selezionando di nuovo il filtro live puoi interrompere il tracciamento in tempo reale prima che scada il timeout.
- Su **iPhone e iPad**, il tracciamento in tempo reale funziona tramite l'app Cerberus Enterprise, con l'accesso alla posizione impostato su **Sempre**. La richiesta normalmente riattiva l'app anche quando non è aperta, e l'app invia poi le posizioni per tutta la sessione. iOS non garantisce queste richieste: può ritardarle o non recapitarle, ad esempio in Risparmio energetico o senza connessione di rete. Se non arriva nessuna posizione entro 2 minuti, la dashboard annulla la richiesta: chiedi all'utente di aprire l'app una volta, poi riprova.

Scheda Geofence

Su dispositivi Android, iPhone e iPad, la seconda scheda mostra le transizioni geofence generate dai geofence definiti nella policy assegnata.

- La mappa mostra le aree geofence attuali insieme ai punti di transizione registrati.
- L'elenco delle transizioni a destra ti consente di esaminare gli eventi di **ingresso** e **uscita** .
- I filtri disponibili sono **Oggi**, **Ultimi 7 giorni**, **Ultimi 30 giorni** e una ricerca personalizzata per intervallo di date.
- **Includi archiviati** mostra anche le transizioni relative a vecchie definizioni di geofence non più presenti nella policy corrente.
- Le transizioni geofence vengono conservate per **90 giorni** e quelle più vecchie vengono eliminate automaticamente ogni notte, quindi la ricerca per intervallo di date personalizzato non può iniziare più di 90 giorni fa.

Su iPhone e iPad, quando la policy ha geofence attivi, una riga di stato nella parte superiore della scheda indica se il geofencing funziona sul dispositivo. Ti dice quando non può funzionare: l'app Cerberus Enterprise non ha contattato il server o deve essere aggiornata, l'accesso alla posizione non è impostato su **Sempre**, **Posizione precisa** o **Aggiorna app in background** è disattivato, **Risparmio energetico** era attivo quando l'app ha segnalato le sue impostazioni l'ultima volta (gli eventi geofence e le modifiche possono quindi subire ritardi di ore), oppure l'app non ha ancora applicato gli ultimi geofence. Quando tutto funziona, mostra quanti geofence sta monitorando l'app.

Dettagli della transizione geofence

Selezionando una transizione si aprono i suoi dettagli sulla mappa e viene evidenziata la voce corrispondente nell'elenco. Quando disponibili, Cerberus Enterprise mostra anche le coordinate del dispositivo e la precisione riportata per quella transizione.

Gestione SIM

La pagina del dispositivo fornisce un pannello **Gestione SIM**. Sui dispositivi Android gestisce le SIM e i profili eSIM installati sul dispositivo, aggiunge o rimuove profili eSIM e mostra la cronologia dei comandi eSIM inviati al dispositivo. Su iPhone e iPad cellulari aziendali mostra le SIM e i piani eSIM segnalati dal dispositivo e consente al dispositivo di scaricare i piani eSIM preparati dall'operatore: vedi **iPhone e iPad** di seguito.

> Le informazioni sulla SIM vengono riportate dai dispositivi con gestione completa quando la segnalazione **Informazioni di rete** è abilitata nella policy del dispositivo (questa opzione è sempre abilitata da Cerberus Enterprise). Vedi la pagina **Segnalazione stato**.

EID del dispositivo

L'EID (eUICC Identifier) identifica l'hardware eSIM del dispositivo. Gli operatori lo usano per associare i profili eSIM al dispositivo, quindi recuperarlo è di solito il primo passo di un flusso di provisioning eSIM.

- **Dispositivi aziendali** (Android 13 e versioni successive): l'EID viene riportato automaticamente con lo stato del dispositivo e non è richiesta alcuna interazione dell'utente.
- **Dispositivi personali** (Android 13 e versioni successive): usa il pulsante **Richiedi EID**. L'utente vedrà una notifica sul dispositivo che chiede di condividere l'EID e potrà approvare o rifiutare la richiesta. L'EID viene mostrato solo se l'utente approva. Mentre la richiesta è in sospeso, il pulsante resta disabilitato.

> L'invio di una richiesta EID mostra prima una finestra di conferma, perché l'utente vedrà una notifica sul dispositivo.

SIM installate

La tabella **SIM installate** elenca le SIM attualmente note per il dispositivo, comprese le SIM fisiche e i profili eSIM. Sui dispositivi personali, i profili eSIM installati con il comando **Aggiungi eSIM** vengono mostrati anche quando il dispositivo non riporta informazioni sulla SIM.

- **Operatore**: il nome dell'operatore associato alla SIM (quando riportato).

- **Numero di telefono**: il numero di telefono associato alla SIM (quando riportato).
- **ICCID**: l'identificatore della carta a circuito integrato della SIM.
- **Stato di attivazione**: indica se l'eSIM è attivata o meno. Riportato solo per le eSIM su Android 15 e versioni successive.
- **Modalità di configurazione**: indica se l'eSIM è stata configurata da un amministratore o dall'utente. Riportato solo per le eSIM su Android 15 e versioni successive.
- **Tipo di SIM**: mostra se il dispositivo segnala la voce come eSIM.

> Le eSIM con un comando di rimozione in corso o eseguito (non fallito) mostrano uno stato di attivazione temporaneo **Rimozione in corso**. La voce scompare dall'elenco quando il dispositivo riporta l'elenco SIM aggiornato. Mentre una rimozione è in corso, il pulsante di rimozione non è disponibile, per evitare di inviare due volte lo stesso comando.

Rimuovi eSIM

Usa il pulsante di rimozione accanto a una eSIM installata per rimuovere il suo profilo dal dispositivo. Una finestra di conferma ti chiede di confermare l'ICCID della eSIM da rimuovere prima che il comando venga inviato. La rimozione di una eSIM è supportata su Android 15 e versioni successive.

Aggiungi eSIM

La sezione **Aggiungi eSIM** installa un nuovo profilo eSIM sul dispositivo (supportato su Android 15 e versioni successive). Richiede:

- **Validità**: per quanto tempo il comando è valido se non può essere eseguito immediatamente.
- **Codice di attivazione**: il codice di attivazione del profilo eSIM, fornito dall'operatore. Puoi inserire il codice completo oppure solo l'indirizzo SM-DP+ per consentire al dispositivo di individuare un profilo che l'operatore ha già collegato al suo EID.
- **Stato di attivazione**: indica se il profilo eSIM deve essere attivato automaticamente dopo il download o lasciato non attivato per l'attivazione manuale da parte dell'utente.

Cronologia dei comandi

Sotto la sezione Aggiungi eSIM, il pannello mostra la cronologia dei comandi eSIM inviati al dispositivo: **Aggiungi eSIM**, **Rimuovi eSIM** e **Richiedi EID**. La tabella è ordinabile e supporta la paginazione. Alcune righe possono essere espanse per visualizzare i parametri del comando (ad esempio il codice di attivazione o l'ICCID) e lo stato di esecuzione, inclusi i dettagli dell'errore eSIM

quando un'operazione non riesce sul dispositivo.

- **Data di creazione**
- **Comando**
- **Validità**
- **Stato**
- **Errore**: mostra lo stato di errore eSIM (ad esempio *Utente ha negato*, *Codice di attivazione non valido* o *ICCID non trovato*) quando l'esecuzione del comando lo riporta.
- **Data di esecuzione**

Cancella le eSIM durante la cancellazione e l'annullamento della registrazione

Quando cancelli il dispositivo dal pannello Comandi, il flag **Cancella eSIM** controlla se i profili eSIM vengono rimossi con la cancellazione. Sui dispositivi personali con profilo di lavoro questo flag è abilitato per impostazione predefinita (le eSIM gestite vengono rimosse, le eSIM personali non sono interessate). Lo stesso flag è disponibile nella finestra di conferma **Annulla registrazione dispositivo**.

iPhone e iPad

Il pannello viene mostrato per iPhone e per iPad che hanno riportato dati cellulare (un iPad solo Wi-Fi non ne ha), solo quando il dispositivo è aziendale e non è una registrazione utente. Le informazioni cellulari vengono richieste al dispositivo insieme alle informazioni del dispositivo: alla registrazione, ogni giorno, con **Aggiorna informazioni dispositivo**, quando la proprietà diventa aziendale e pochi minuti dopo **Aggiorna piani cellulari**.

- **EID del dispositivo**: l'EID riportato con le SIM, con un pulsante per copiarlo per l'operatore. Se il dispositivo non lo riporta, l'utente lo trova in Impostazioni > Generali > Info.
- **Riportato**, **Roaming dati**, **Hotspot personale** e **Firmware modem**: quando il dispositivo ha risposto e lo stato riportato. Il roaming dati e l'Hotspot personale possono essere modificati con **Impostazioni dispositivo** nel pannello Comandi, che mostra anche lo stato corrente.
- **SIM**: una riga per ogni SIM o piano eSIM (i dispositivi dual SIM ne hanno due), con lo slot riportato dal dispositivo, la sua etichetta e il suo tipo (**eSIM** quando il dispositivo riporta l'EID insieme ad essa, **Scheda SIM** altrimenti), l'operatore (l'operatore di origine in un

tooltip quando il dispositivo è in roaming su un'altra rete), il numero di telefono, l'ICCID, l'EID, l'IMEI, la SIM usata per i dati e per le chiamate e il roaming. Uno slot eSIM senza piano viene mostrato in grigio come **Nessun piano**.
- **Questo dispositivo non ha riportato SIM** significa che il dispositivo ha risposto senza alcuna SIM; **Nessuna informazione cellulare ancora** significa che non ha ancora risposto: usa **Aggiorna informazioni dispositivo**.

> I numeri di telefono, l'ICCID, l'IMEI e l'EID identificano la persona e la linea: non vengono mai richiesti ai dispositivi personali o alle registrazioni utente. Quando un dispositivo diventa personale, le informazioni vengono rimosse subito e nascoste nei risultati dei vecchi comandi di informazioni dispositivo nella cronologia dei comandi. Non vengono esportate e non vengono scritte nei log di sistema.

Aggiorna piani cellulari

iPhone e iPad non possono installare una eSIM da un codice di attivazione. L'operatore associa (riserva) il piano eSIM all'EID del dispositivo sul proprio server eSIM (SM-DP+) e ti fornisce l'indirizzo di quel server; **Aggiorna piani cellulari** chiede quindi al dispositivo di scaricare i piani in attesa. Il pulsante **Aggiorna piani cellulari** del pannello seleziona il comando nel pannello Comandi, dove inserisci **URL del server eSIM dell'operatore**:

- **Un indirizzo https://**, inviato così com'è. Gli indirizzi con http://, un nome utente o una password, oppure una parte con # non vengono accettati.
- **Un nome host**, ad esempio *smdp.carrier.example*, inviato come https://smdp.carrier.example.
- **Un codice di attivazione LPA** (LPA:1$server$code, il testo di un codice QR eSIM): viene usato solo il server, perché il comando non può trasportare il codice. Il piano deve essere associato all'EID del dispositivo dall'operatore, altrimenti il dispositivo non trova nulla da scaricare.

Il dispositivo installa e attiva il piano senza chiedere conferma all'utente, anche quando non è supervisionato. Il successo nella cronologia dei comandi significa che il dispositivo ha accettato la richiesta, non che un piano è stato installato: l'installazione può richiedere fino a tre minuti e Cerberus Enterprise richiede di nuovo le SIM al dispositivo circa tre minuti dopo, così il nuovo piano appare nel pannello. Gli errori 36001 (il dispositivo non è riuscito a raggiungere il proprio sistema cellulare), 36002 (nessun supporto eSIM) e 36003 (sistema cellulare occupato, riprova più tardi) sono spiegati nei log di sistema. Un piano scaricato una volta non può essere scaricato di nuovo: se l'installazione non riesce, contatta l'operatore. Il comando è disponibile anche per più dispositivi contemporaneamente nel menu **Azioni dispositivo Apple** della pagina Dispositivi.

Cosa non consente Apple

- **Aggiungi eSIM** da un codice di attivazione: non è possibile, usa **Aggiorna piani cellulari** con un piano associato all'EID.
- **Rimuovi eSIM**: una eSIM non può essere rimossa da remoto una alla volta. Cancellando il dispositivo con **Mantieni il piano dati eSIM** disattivato si rimuovono tutte le eSIM. Per fermare un singolo piano, chiedi all'operatore di disattivarlo: il piano resta sul dispositivo ma non può connettersi.
- **Richiedi EID**: non necessario, l'EID arriva con le SIM dei dispositivi aziendali.
- **Mac** non dispongono di gestione cellulare o eSIM.

Comandi

La pagina del dispositivo fornisce un pannello **Comandi** per inviare comandi remoti a un dispositivo gestito. I comandi disponibili dipendono dalla piattaforma (Android o Apple) e dallo stato del dispositivo.

I comandi possono essere inviati solo a un dispositivo attualmente registrato. Su un dispositivo con registrazione annullata, su un dispositivo ADE non ancora registrato e sul record storico di una registrazione passata, il pannello mostra solo la cronologia dei comandi.

> Se il dispositivo non è attualmente online, il comando verrà recapitato ed eseguito non appena il dispositivo si connette a Internet. Per i comandi Android puoi impostare il parametro **Validità** per stabilire per quanto tempo un comando non recapitato rimane valido.

Comandi Android (AMAPI)

Per i dispositivi Android, il pannello Comandi include un campo **Validità** (valore + unità) e un selettore **Comando**. Alcuni comandi richiedono parametri aggiuntivi, che appaiono dinamicamente quando selezioni il comando.

Parametri comuni

- **Validità**: per quanto tempo il comando è valido se non può essere eseguito immediatamente.
- **Comando**: scegli quale azione inviare al dispositivo.

Comandi senza campi aggiuntivi

- **Blocca dispositivo**: blocca il dispositivo.
- **Riavvia dispositivo**: riavvia il dispositivo. Richiede Android 7.0 o versioni successive.
- **Disattiva modalità smarrito**: rimuove il dispositivo dalla modalità smarrito.
- **Rinuncia alla proprietà**: rimuove il profilo di lavoro e tutte le policy da un dispositivo aziendale con Android 8.0 o versioni successive e lo lascia per uso personale. Le app e i dati del profilo personale vengono conservati. Il dispositivo viene eliminato dal server dopo che conferma il comando. Questa operazione non può essere annullata.

Comandi con campi aggiuntivi

- **Reimposta password**: richiede **Nuova password** e **Conferma nuova password**. Gli interruttori facoltativi includono **Blocca ora**, **Richiedi inserimento** e **Non chiedere le credenziali all'avvio**.
- **Cancella dati app**: richiede il **Nome del pacchetto** di destinazione.
- **Attiva modalità smarrito**: richiede un **Messaggio modalità smarrito** e supporta campi di contatto facoltativi (indirizzo, organizzazione, numero di telefono, email). Quando il dispositivo lo segnala, il suo stato diventa **Smarrito**, la pagina del dispositivo mostra un banner e questo comando viene nascosto finché la modalità smarrito non viene disattivata.
- **Cancella dispositivo**: supporta un **Messaggio motivo cancellazione** (mostrato agli utenti sui dispositivi personali) e flag di cancellazione facoltativi, tra cui **Cancella eSIM**.

> I comandi eSIM (**Aggiungi eSIM**, **Rimuovi eSIM**, **Richiedi EID**) sono disponibili nel pannello dedicato **Gestione SIM**.

Cronologia dei comandi

Sotto i controlli di invio, la dashboard mostra una tabella della cronologia dei comandi. La tabella è ordinabile e supporta la paginazione. Alcune righe possono essere espanse per visualizzare parametri aggiuntivi o dettagli di esecuzione.

Colonne della cronologia Android

- **Data di creazione**
- **Comando**
- **Validità**
- **Stato**
- **Errore**
- **Data di esecuzione**

Comandi Apple (MDM)

Per i dispositivi Apple, il pannello Comandi fornisce un selettore **Comando**. Alcuni comandi richiedono input aggiuntivi. Come per Android, di seguito viene mostrata una tabella della cronologia dei comandi.

Comandi con campi aggiuntivi

- **Installa app**: richiede il **Bundle ID** dell'applicazione.
- **Invia notifica**: richiede un **Messaggio di notifica** (lunghezza massima 200 caratteri).

Su iPhone e iPad, **Invia notifica** e il tracciamento in tempo reale raggiungono il dispositivo tramite l'app **Cerberus Enterprise**: sono disabilitati finché l'app non viene installata e non si è registrata per le notifiche (vedi il campo **App Cerberus Enterprise**). L'avvio del tracciamento in tempo reale mostra "Richiesta di tracciamento in tempo reale inviata al dispositivo": il tracciamento inizia quando il dispositivo invia la sua prima posizione. iOS può ritardare la richiesta o non recapitarla, ad esempio in Risparmio energetico o senza connessione di rete: se non arriva nessuna posizione entro 2 minuti, chiedi all'utente di aprire l'app una volta. Quando una richiesta non riesce, il messaggio ne indica il motivo, ad esempio l'app non si è ancora registrata, manca la chiave di notifica del server o il token di notifica del dispositivo non è più valido.

Azioni sul dispositivo

Sono elencati solo i comandi supportati dal dispositivo: alcuni richiedono un iPhone o iPad supervisionato, altri non sono disponibili su un Mac. Quelli più invasivi richiedono una conferma.

- **Blocca dispositivo**: blocca lo schermo, con un messaggio e un numero di telefono facoltativi. Un Mac viene riavviato e bloccato con un PIN a sei cifre, mostrato una volta dopo l'invio del comando e nei dettagli del comando. iPhone mostra il titolo "iPhone smarrito" sopra il tuo messaggio, anche se questo comando non attiva la modalità smarrito.
- **Attiva modalità smarrito** (iPhone e iPad supervisionati): blocca il dispositivo e mostra sulla schermata di blocco il tuo messaggio, il numero di telefono e la nota. Mentre la modalità smarrito è attiva, la pagina mostra un banner e i comandi **Localizza dispositivo** (la posizione appare sulla Mappa delle posizioni), **Riproduci suono** e **Disattiva modalità smarrito**.
- Il dispositivo comunica a chi lo tiene in mano che è stato localizzato: dopo **Localizza dispositivo**, la schermata di blocco mostra **iPhone localizzato** con l'ora e il nome del server che ha ricevuto la posizione, e un pulsante **Continua**. iOS mostra questo avviso e non può essere disattivato.
- **Cancella codice di accesso**: rimuove il codice di accesso di un iPhone o iPad, ad esempio quando l'utente lo ha dimenticato. Se la policy richiede un codice di accesso, all'utente viene chiesto di impostarne uno nuovo.
- **Aggiorna informazioni dispositivo**: chiede al dispositivo le sue informazioni (supervisione, versione del sistema operativo, stato di sicurezza, certificato MDM) e il suo inventario.
- **Impostazioni dispositivo**: apre una finestra per modificare il nome del dispositivo, il nome host di un Mac, Bluetooth, roaming dati, Hotspot personale, fuso orario, sfondo, se il blocco attivazione è consentito e, su un iPad condiviso, le relative impostazioni (vedi sotto). Vengono inviate solo le impostazioni che modifichi; quelle non supportate dal dispositivo sono disattivate con il motivo. Un dispositivo può confermare il roaming dati o l'Hotspot personale senza applicarli (ad esempio quando il piano SIM non include l'Hotspot

personale), quindi Cerberus Enterprise li rilegge circa 30 secondi dopo e scrive un avviso nei registri di sistema se non sono cambiati.
- **Riavvia dispositivo** e **Spegni dispositivo**: riavvia o spegne subito il dispositivo, dopo una conferma.
- **Cancella dispositivo**: cancella tutti i contenuti e le impostazioni e rimuove il dispositivo dalla gestione. Su iPhone e iPad puoi mantenere il piano dati eSIM e saltare la configurazione di prossimità; un Mac riceve un PIN a sei cifre.
- **Return to Service** (opzione di **Cancella dispositivo**, iPhone e iPad con iOS 17 o versioni successive): dopo la cancellazione il dispositivo si configura di nuovo da solo, senza che nessuno lo tocchi, e si registra di nuovo con la sua policy, il suo utente e la sua proprietà attuali. Scegli una rete Wi-Fi della policy del dispositivo per la configurazione, a meno che il dispositivo disponga di Ethernet o dati cellulare: possono essere usate solo reti personali (con password, senza certificati), perché il dispositivo non ha ancora un utente o un certificato. Activation Lock deve essere disattivato.
- **Aggiorna piani cellulari** (iPhone e iPad cellulare, iOS 13 o versioni successive, non User Enrollment): inserisci l'**URL del server eSIM del gestore** fornito dal gestore (un indirizzo https://, un nome host o un codice di attivazione LPA, di cui viene usato solo il server) e il dispositivo scarica i piani eSIM che il gestore ha associato al suo EID. L'EID del dispositivo è mostrato sotto il campo per inviarlo al gestore. Consulta la pagina **Gestione SIM**.
- **Mantieni il piano dati eSIM** disattivato rimuove tutte le eSIM con la cancellazione. La restrizione della policy **Mantieni l'eSIM quando il dispositivo viene cancellato** (dispositivi supervisionati, iOS 17.2 o versioni successive) si applica alle cancellazioni avviate sul dispositivo (troppi tentativi di codice di accesso non riusciti, Cancella tutti i contenuti e le impostazioni): Apple non documenta il suo effetto su questo comando.
- **Disconnetti utente** (iPad condiviso): disconnette l'utente corrente e torna alla schermata di accesso. I dati non ancora sincronizzati con iCloud rimangono sull'iPad.

iPad condiviso

Un iPad condiviso è usato da più persone, ciascuna con il proprio Managed Apple Account, oppure da ospiti con sessioni temporanee. Viene configurato con un profilo ADE che abilita iPad condiviso (vedi la pagina **Apple Automated Device Enrollment**) e il suo campo **Tipo di registrazione** mostra **iPad condiviso**.

- **Utenti iPad condiviso**: gli utenti dell'iPad, con l'utente connesso, lo spazio che utilizzano e se alcuni dati non sono ancora sincronizzati con iCloud. Usa **Aggiorna** per chiedere di nuovo l'elenco all'iPad. Un utente può essere eliminato con i suoi dati, tranne l'utente connesso (disconnettilo prima); **Elimina tutti gli utenti** richiede iPadOS 14 o versioni successive. Quando i dati non sono ancora sincronizzati, la conferma avvisa che andranno persi.
- **Impostazioni dispositivo**: lo spazio per ciascun utente, il numero previsto di utenti, il tempo di inattività dopo il quale utenti e sessioni ospite vengono disconnessi, solo sessioni ospite, i domini Managed Apple Account suggeriti nella schermata di accesso, per quanti giorni un utente può accedere senza verificare la password online e il salto della

configurazione di lingua e regione per i nuovi utenti. I campi vuoti mantengono il valore corrente; le impostazioni che richiedono un iPadOS più recente sono disabilitate.

Utenti Mac

Su un Mac, il pannello **Utenti Mac** elenca gli utenti registrati nella gestione, di solito l'utente che ha registrato il Mac. Gli account della policy vengono installati nelle loro sessioni. Per ogni utente mostra quando è stato registrato, l'ultimo report della sua sessione e lo stato degli account: **Aggiornato**, **In attesa dell'utente** (il Mac li installa quando l'utente è connesso), **Non applicato** con i motivi riportati dal Mac oppure **Nessun account** quando la policy non ne ha. Usa **Ricarica** per leggere di nuovo l'elenco.

Activation Lock

Il campo **Activation Lock** mostra se Activation Lock è attivo. Quando è attivo, un dispositivo cancellato può essere configurato di nuovo solo con l'Apple Account dell'utente o con il codice di bypass del dispositivo. I dispositivi supervisionati attivano Activation Lock solo se è consentito in **Impostazioni dispositivo**. Cerberus Enterprise chiede ai dispositivi supervisionati il loro codice di bypass e lo memorizza: usa **Mostra codice di bypass** nel menu del campo per visualizzarlo (solo gli amministratori possono farlo e ogni visualizzazione viene registrata nel log di sistema), poi inseriscilo come password nella schermata Activation Lock del dispositivo, lasciando vuoto l'Apple Account.

Recovery Lock e password del firmware (Mac)

Un Mac con Apple silicon mostra il campo **Recovery Lock**, un Mac basato su Intel il campo **Password del firmware**. Entrambi proteggono il Mac all'avvio: con Recovery Lock, recoveryOS chiede la password; con una password del firmware, il Mac la chiede per avviarsi da un altro disco o dal ripristino. Il campo mostra se il Mac segnala una password e, nel suo tooltip, quando Cerberus Enterprise l'ha memorizzata e quando è stata verificata l'ultima volta.

- **Imposta o cambia password**: Cerberus Enterprise genera una password di 20 lettere che si trovano sugli stessi tasti con qualsiasi layout di tastiera, oppure un amministratore ne digita una (da 8 a 64 caratteri senza accenti; gli altri ruoli possono solo generarne una, perché non possono vedere le password memorizzate). La password viene memorizzata crittografata prima di essere inviata e sostituisce quella memorizzata solo quando il Mac la conferma. Se il Mac ha già una password impostata al di fuori di Cerberus Enterprise, digitarla come password corrente: viene usata una sola volta e non memorizzata.
- **Verifica password**: chiede al Mac se la password memorizzata è corretta. Il risultato è nel tooltip e nel log di sistema.

- **Mostra password**: solo gli amministratori possono vedere la password memorizzata e ogni visualizzazione viene registrata nel log di sistema. Le password generate sono mostrate in gruppi di quattro lettere: digitale senza spazi.
- **Cancella password**: rimuove la password dal Mac.

Un Mac basato su Intel si riavvia per applicare una modifica della password del firmware: fino ad allora serve ancora la password precedente (Mostra password la elenca) e non può essere inviata un'altra modifica. Apple accetta inoltre un solo comando per la password del firmware ogni 30 secondi. Le password sono nascoste nella cronologia dei comandi.

Quando un Mac esce dalla gestione (registrazione annullata, rimosso dall'utente o cancellato), macOS rimuove Recovery Lock da solo e Cerberus Enterprise elimina la password Recovery Lock memorizzata; fa lo stesso quando il Mac segnala di non avere Recovery Lock, ad esempio dopo essersi registrato di nuovo. Quando annulli la registrazione di un Mac (o elimini la sua policy), una password del firmware memorizzata viene prima cancellata, il Mac si riavvia e poi esce dalla gestione. Se la cancellazione non riesce, il Mac esce comunque dalla gestione e la password rimane memorizzata, così puoi ancora vederla. Un Mac rimosso dalla gestione dall'utente, o cancellato, mantiene la sua password del firmware: anche Cerberus Enterprise la mantiene. Eliminare il record del dispositivo elimina la password memorizzata, quindi ti viene chiesto di confermare prima: annota la password, perché senza di essa solo Apple può rimuoverla.

FileVault (Mac)

Il campo **FileVault** mostra se il disco del Mac è crittografato e, nel suo tooltip, se Cerberus Enterprise memorizza la sua chiave di recupero personale. Un Mac invia la chiave quando FileVault viene attivato dopo aver ricevuto l'impostazione FileVault della sua policy (vedi la pagina **macOS** delle policy Apple).

- **Mostra chiave di recupero**: solo gli amministratori possono vedere la chiave e ogni visualizzazione viene registrata nel log di sistema. Usala nella finestra di accesso del Mac per reimpostare la password dell'utente, oppure in modalità di ripristino per sbloccare il disco. Rimane disponibile dopo che il Mac esce dalla gestione; eliminando il record del dispositivo viene eliminata.
- **Cambia chiave di recupero**: il Mac sostituisce la sua chiave di recupero personale e invia quella nuova, crittografata; la vecchia chiave smette di funzionare. È possibile solo quando la chiave memorizzata può essere letta: il Mac viene sbloccato con essa e non serve la password di un utente. La chiave memorizzata è nascosta nella cronologia dei comandi e viene rimossa dal server quando il Mac risponde (o dopo 7 giorni senza risposta).

Bootstrap Token (Mac)

Un Mac con macOS 10.15 o versioni successive invia il suo **Bootstrap Token** al server di gestione quando un utente con un token sicuro effettua l'accesso. Il server lo conserva e lo restituisce solo a quel Mac, che lo usa per assegnare un token sicuro ai nuovi utenti e, su un Mac con Apple silicon, per installare aggiornamenti software e approvare estensioni del kernel senza chiedere una password di amministratore. Nessuno può vedere il token, nella dashboard o altrove. Il campo **Bootstrap Token** mostra il suo stato:

- **Escrowed**: il server ha il token; il tooltip mostra quando il Mac lo ha inviato.
- **Escrowed in precedenza**: il token memorizzato è stato inviato prima dell'ultima registrazione o del rinnovo del certificato MDM del Mac. Dopo un rinnovo è previsto: il token viene mantenuto e il Mac non lo invia di nuovo. Dopo una nuova registrazione potrebbe non essere più valido: esegui `sudo profiles install -type bootstraptoken` nel Terminale del Mac.
- **Not escrowed**: il Mac non ha ancora inviato un token. Per inviarlo ora, un amministratore del Mac esegue `sudo profiles install -type bootstraptoken` nel Terminale (`sudo profiles status -type bootstraptoken` mostra se è escrowed).

Il tooltip indica anche se il Mac consente il token per l'autenticazione. I Mac configurati con Automated Device Enrollment lo consentono automaticamente; su altri Mac con Apple silicon un utente può consentirlo in Startup Security Utility in recoveryOS. I Mac Intel non possono usare il token per l'autenticazione (**Non supportato**), ma un token escrowed assegna comunque un token sicuro ai nuovi utenti. Ogni volta che un Mac invia, rimuove o richiede il suo token, l'operazione viene registrata nel log di sistema.

Stato del dispositivo e aggiornamenti del sistema operativo

Il pannello **Stato del dispositivo** mostra ciò che il dispositivo segnala su se stesso: la versione e la build del sistema operativo, l'avanzamento di un aggiornamento software (versione in attesa, scadenza, cosa lo ha avviato, errori), se è impostato un codice di accesso e se è conforme alla policy, FileVault su un Mac, la salute della batteria e gli account configurati sul dispositivo.

L'elenco **Aggiornamenti disponibili** mostra gli aggiornamenti del sistema operativo che il dispositivo può installare, raccolti alla registrazione e ogni settimana. Usa **Verifica aggiornamenti** per richiederli subito e **Installa** per installare subito un aggiornamento (il dispositivo si riavvia, dopo una conferma) oppure solo scaricarlo e lasciare che l'utente lo installi. Funziona su iPhone e iPad supervisionati e sui Mac, fino a iOS, iPadOS e macOS 26: nelle versioni successive e per aggiornare molti dispositivi, usa gli aggiornamenti richiesti della policy (vedi la pagina **Aggiornamenti software** delle policy Apple).

Un Mac con Apple silicon installa un aggiornamento senza chiedere una password di amministratore solo quando consente il suo Bootstrap Token per l'autenticazione e il token è escrowed (vedi Bootstrap Token sopra). In caso contrario la conferma indica che un utente

potrebbe dover inserire una password di amministratore prima che l'aggiornamento venga installato.

Applicazioni e inventario

Il pannello **Applicazioni** elenca ogni app del dispositivo in un'unica tabella. Lo stato di installazione delle app installate dalla policy o con un comando viene segnalato in tempo reale dal dispositivo; versioni, dimensioni e app installate dall'utente provengono dall'ultimo elenco di app, raccolto alla registrazione e ogni settimana. Usa **Chiedi al dispositivo** per richiederlo subito.

- **Gestione**: **Policy** per le app installate dalla policy del dispositivo, **Gestita** per le app installate con un comando come **Installa app**, **Non gestita** per quelle installate dall'utente. L'app Cerberus Enterprise ha il chip **Installata da Cerberus**.
- **Richiede attenzione**: app la cui installazione non è riuscita, che sono state rifiutate o rimosse dall'utente oppure che attendono l'utente. Apri una riga per vedere l'errore; le app della policy non riuscite possono essere installate di nuovo con il pulsante di nuovo tentativo. Le app integrate e le app dell'App Store che il dispositivo segnala come non convalidate non vengono conteggiate.
- **Rimuovi app**: le app gestite possono essere rimosse, con i loro dati. Per rimuovere un'app installata dalla policy, rimuovila dalla policy. La policy invia questo comando anche da sola quando un pacchetto Mac installato come app gestita viene rimosso dalla policy.

Il pannello **Profili, certificati e sicurezza** mostra i profili di configurazione, i certificati e lo stato di sicurezza (codice di accesso, crittografia, FileVault e firewall su un Mac) segnalati dal dispositivo.

> Sui dispositivi di proprietà personale le app installate dall'utente non vengono raccolte e sono elencati solo i profili e i certificati gestiti da Cerberus Enterprise.

Il pannello **Modifiche all'inventario** mostra cosa è cambiato tra due elenchi inviati dal dispositivo: app installate, rimosse o aggiornate (con la vecchia e la nuova versione), profili installati, rimossi o aggiornati e certificati aggiunti o rimossi. Una modifica viene rilevata quando il dispositivo invia un nuovo elenco, ogni settimana per app e profili, ogni giorno per i certificati, oppure quando usi **Chiedi al dispositivo**: la data mostrata è quella in cui è stata rilevata, la modifica è avvenuta tra l'elenco precedente e quello. Il primo elenco di un dispositivo, e il primo dopo una nuova registrazione o un cambio di proprietà, viene solo registrato come punto di partenza. Cerca per nome o identificatore e filtra per tipo e modifica. Le modifiche vengono conservate per 365 giorni.

> Quando un aggiornamento del sistema operativo sostituisce molte app Apple contemporaneamente, vengono mostrate come un'unica riga (ad esempio "23 app Apple aggiornate") che puoi espandere. Il rinnovo del certificato MDM è mostrato come **Certificato MDM rinnovato**. Sui dispositivi di proprietà personale sono mostrate solo le modifiche degli elementi gestiti da Cerberus Enterprise.

Colonne della cronologia Apple

- **Data di creazione**
- **Comando**
- **Stato**: **Inviato** (in attesa del dispositivo, consegnato non appena si connette), **Riuscito**, **Risposto** (apri la riga per vedere il risultato), **In attesa del dispositivo** (il dispositivo non può eseguire il comando in questo momento), **Non riuscito** (apri la riga per vedere il motivo) o **Annullato** (la coda dei comandi del dispositivo è stata svuotata, ad esempio quando si è registrato di nuovo).
- **Data di esecuzione**

Aggiorna

Usa l'azione di aggiornamento nel pannello Comandi per ricaricare la cronologia dei comandi.