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.

Revision #60
Created 2025-12-17 09:49:39 UTC by Admin
Updated 2026-11-12 09:52:54 UTC by Admin