Policy - Apple

- Apple policy
- App e profili
- Chiosco e schermata Home
- Codice
- Restrizioni
- Rete
- Aggiornamenti software
- macOS
- Posizione e geofence
- Account
- Regole di conformità

Apple policy

Le Apple policy definiscono le impostazioni di gestione che Cerberus Enterprise applica ai dispositivi Apple tramite MDM. Queste impostazioni si configurano dalla dashboard nell'Apple policy editor.

Prima di iniziare

La gestione dei dispositivi Apple richiede la configurazione di Apple Management (APNs). Se necessario, leggi la pagina Configurazione di Apple Management (APNs).

Apri l'Apple Policy Editor

Nella dashboard, apri **Policy** e fai clic su **Crea nuova Apple policy**. Per modificare una Apple policy esistente, fai clic sulla sua riga nella tabella delle policy.

Struttura dell'editor

L'Apple Policy Editor è organizzato in una serie di sezioni espandibili. In cima alla pagina puoi sempre modificare:

- **Nome** (obbligatorio)
- **Id** (sola lettura)
- **Descrizione** (facoltativo)

Sezioni della policy

Le sezioni seguenti corrispondono ai pannelli attualmente disponibili nell'Apple Policy Editor. Quando apri una policy salvata, le sezioni con impostazioni modificate sono già aperte e le altre restano chiuse:

- **Gestione app**: configura le limitazioni relative alle app, le app gestite e le impostazioni dell'app Cerberus Enterprise.

- **Kiosk e schermata Home**: Modalità app singola, app consentite e bloccate, layout della schermata Home, web clip, impostazioni delle notifiche e messaggio della schermata di blocco.
- **Sicurezza**: controlla funzioni come lo sblocco automatico e lo sblocco biometrico.
- **Impostazioni del codice di accesso**: configura i requisiti del codice di accesso e le regole correlate.
- **Multimedia**: consenti/nega la fotocamera e le funzioni correlate.
- **Cellulare**: controlla le impostazioni relative alla rete cellulare (impostazioni dei dati cellulare per le app, eSIM, modifiche del piano) e l'APN cellulare.
- **Rete**: reti Wi-Fi (anche enterprise 802.1X), VPN, certificati, proxy globale, DNS crittografato e filtro dei contenuti web, e restrizioni di connettività come AirDrop e Bluetooth.
- **Sistema e interfaccia utente**: limita funzionalità di sistema come Handoff, il nome del dispositivo e il salvaschermo.
- **Aggiornamenti software**: richiedi una versione del sistema entro una scadenza e controlla come vengono scaricati e installati gli aggiornamenti.
- **macOS**: firewall, Gatekeeper, salvaschermo e blocco, archivi esterni e di rete, Condivisione schermo, autorizzazioni per la privacy e oggetti di login dei Mac.
- **App e servizi Apple**: limita app e servizi Apple come iMessage, Game Center e Dov'è.
- **Siri e Apple Intelligence**: limita Siri, la dettatura e le funzionalità di Apple Intelligence.
- **iCloud**: consenti o nega specifici servizi iCloud (backup, sincronizzazione del portachiavi, inoltro privato, ecc.).
- **Posizione e geofence**: aree in cui gli iPhone e gli iPad con l'app Cerberus Enterprise segnalano l'ingresso o l'uscita, per le regole degli eventi.
- **Account**: limita la modifica degli account e configura gli account Mail, Exchange, Google, calendario, contatti e directory.
- **Regole di conformità**: requisiti (codice di accesso, versione minima del sistema, supervisione, FileVault) che rendono i dispositivi non conformi, con blocco facoltativo.

> Molte opzioni dell'Apple Policy Editor includono un tooltip che documenta i requisiti e le versioni del sistema supportate.

Salvataggio, eliminazione e dispositivi associati

Usa **Salva policy** per applicare le modifiche. Il pulsante è disattivato quando non ci sono modifiche in sospeso o quando la licenza è scaduta.

Quando modifichi una policy esistente, la pagina mostra anche un'azione **Elimina policy**. L'editor può mostrare in fondo un elenco **Dispositivi associati**, così puoi vedere quanti dispositivi stanno

attualmente usando la policy.

Pagine successive

- App e profili: configura le app installate e i profili di configurazione.
- Kiosk e schermata Home: Modalità app singola, app consentite, layout della schermata Home e web clip.
- Codice di accesso: configura i requisiti del codice di accesso e le opzioni di sicurezza correlate.
- Limitazioni: definisci le funzioni consentite e le limitazioni a livello di sistema.
- Rete: reti Wi-Fi, VPN, certificati e restrizioni di connettività.
- Aggiornamenti software: aggiornamenti del sistema richiesti e impostazioni degli aggiornamenti software.
- macOS: firewall, Gatekeeper, blocco schermo, archivi, autorizzazioni per la privacy e oggetti di login dei Mac.
- Posizione e geofence: aree di cui gli iPhone e gli iPad segnalano l'ingresso e l'uscita, e cosa serve perché funzionino.
- Account: account di posta, Exchange, Google, calendario, contatti e directory.
- Regole di conformità: requisiti per i dispositivi e blocco dei dispositivi non conformi.

App e profili

Questa sezione descrive come configurare applicazioni gestite e payload degli account per i dispositivi Apple.

Gestione delle app

Il pannello **Gestione delle app** contiene sia le restrizioni generali relative alle app sia un elenco delle app gestite.

Restrizioni generali delle app

- **Consenti App Clip**
- **Consenti installazione delle app**
- **Consenti rimozione delle app**
- **Consenti download automatici delle app**
- **Consenti di nascondere le app**
- **Consenti di bloccare le app**
- **Consenti acquisti in-app**
- **Consenti modifica del browser predefinito**
- **Consenti attendibilità delle app aziendali**

App gestite

Usa **Aggiungi applicazione** per aggiungere un'app alla policy. Ogni app gestita viene visualizzata come una scheda. Puoi espandere la scheda per modificarne le impostazioni e rimuovere l'app usando l'azione di eliminazione.

- **ID App Store**: l'identificatore App Store dell'app gestita.
- **Bundle ID**: l'identificatore del bundle dell'app.
- **Comportamento di installazione**: controlla se l'app deve rimanere installata o può essere installata/rimossa dall'utente.
- **Assegnazione**: il tipo di licenza, scelto da Cerberus per ogni dispositivo: una licenza dispositivo sui dispositivi aziendali, una licenza utente del Managed Apple Account su iPhone e iPad personali (registrazione utente). Il campo non può essere modificato.
- **Licenza VPP**: tipo di licenza VPP usato per l'installazione tramite l'App Store.

L'elenco di selezione delle app mostra le licenze disponibili e totali di ogni app. Le app gratuite mostrano **Illimitate**: Apple concede loro licenze illimitate. Un'app può essere aggiunta a una policy una sola volta: un'app con lo stesso ID App Store o bundle ID di un'app già presente nella policy viene rifiutata, e lo stesso vale per una policy che elenca due volte la stessa app al momento del salvataggio.

L'elenco di selezione delle app mostra le app della tua libreria di Apple Business. Per aggiungere un'app, in Apple Business apri **Apps & Services → Apps & Books → App Store**, cerca l'app e fai clic su **View**. Per un'app gratuita, fai clic su **Add**, seleziona **All current and future** (o l'unità organizzativa del tuo token di Apps and Books) in **Organizational Units**, fai clic su **Add**, poi su **Review** e conferma. Per un'app a pagamento, fai clic sul suo prezzo, scegli **Managed Licenses** come **License Type** (i codici di riscatto non possono essere usati da Cerberus Enterprise), seleziona l'**Organizational Unit** del tuo token di Apps and Books, inserisci il numero di **Licenses** (fino a 1.000 per ordine), poi **Review** e acquista. Prima deve essere impostato un metodo di pagamento in **Settings → Payments & Billing → Apps & Services → Payment Methods**. Le app compaiono quindi nell'elenco di selezione delle app.

App sui dispositivi personali (registrazione utente)

Gli iPhone e iPad personali registrati con la registrazione utente non hanno un numero di serie, quindi ricevono le app dell'App Store della policy con una **licenza utente** del Managed Apple Account con cui è stato effettuato l'accesso sul dispositivo. Cerberus registra l'account con Apps and Books e assegna le licenze autonomamente, comprese le app gratuite. I Managed Apple Account e il token di Apps and Books devono appartenere alla stessa organizzazione di Apple Business. Un'app a pagamento usa una licenza per account, condivisa da tutti i dispositivi personali di quell'account.

- **In attesa di una licenza utente**: l'app viene inviata al dispositivo solo dopo che Apple ne conferma la licenza, di solito entro pochi minuti. Il pannello **Applicazioni** del dispositivo mostra il motivo.
- **Licenza utente non riuscita**: Apple non è riuscita ad assegnare la licenza, ad esempio perché un'app a pagamento non ha più licenze. Aggiungi licenze in Apple Business, poi usa **Richiedi di nuovo**; Cerberus riprova anche autonomamente ogni giorno.
- **Richiesta di installazione**: iOS chiede all'utente prima di installare ogni app. Se l'utente annulla, l'app mostra **In attesa dell'approvazione dell'installazione da parte dell'utente**; **Richiedi di nuovo** mostra di nuovo la richiesta.
- **Rilascio**: rimuovere l'app dalla policy o annullare la registrazione dell'ultimo dispositivo personale dell'account rimuove l'app e rilascia la sua licenza, a meno che un altro dispositivo registrato dello stesso account ne abbia ancora bisogno.

Per i dettagli, consulta **Registrazione basata sull'account Apple**.

Configurazione gestita

Una configurazione gestita fornisce a un'app le sue impostazioni (ad esempio un indirizzo del server o un nome account), come documentate dal fornitore dell'app. Apri l'app nella policy e fai clic su **Aggiungi configurazione gestita**. Viene inviata a iPhone e iPad con **iOS o iPadOS 18.4 o versioni successive** e ai Mac con **macOS 27 o versioni successive**; non viene ancora inviata ad Apple Vision Pro. L'app deve supportare la configurazione gestita: un'app che non la legge la ignora. Il pannello dell'app mostra il numero di chiavi accanto al nome dell'app.

- **Chiavi**: ogni riga ha una chiave, un tipo e un valore. I tipi sono Testo, Intero, Numero decimale, Booleano, Data, Elenco di testo ed Elenco di interi. Le chiavi distinguono maiuscole e minuscole e devono essere univoche. **Aggiungi chiave** aggiunge una riga; **Rimuovi configurazione** rimuove tutte le chiavi.
- **Variabili**: i valori Testo ed Elenco di testo possono contenere $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$, sostituite con i valori di ogni dispositivo e del suo utente. Una variabile senza valore (ad esempio $EMAIL$ su un dispositivo senza utente) viene lasciata vuota e i log di sistema lo indicano. Quando i dettagli di un utente cambiano, i dispositivi ricevono i nuovi valori; per gli utenti sincronizzati da Google Directory i valori vengono aggiornati alla successiva modifica della policy o del dispositivo.
- **Importa una configurazione**: apri o incolla il file che il fornitore dell'app pubblica per MDM, poi fai clic su **Leggi**. Un **file spec AppConfig** (specfile.xml) elenca ogni chiave supportata dall'app con la sua descrizione, tipo, valore predefinito e valori consentiti: seleziona le chiavi da importare (quelle con un valore predefinito sono già selezionate) e compila le altre dopo l'importazione. Compare un avviso quando il file spec è per un'altra app. Una **property list** (un'intera property list o solo il suo <dict>) viene importata così com'è. Poi scegli se sostituire le chiavi attuali o aggiungerle. I dizionari annidati, i valori di tipo data e gli elenchi con tipi misti o sconosciuti non sono supportati e vengono elencati come ignorati. Apple non pubblica le chiavi di configurazione delle app, quindi chiedi il file al fornitore quando non è nella sua documentazione. **Copia come plist** copia la configurazione come la riceve il dispositivo, prima che le variabili vengano sostituite.
- **Limiti**: fino a 200 chiavi per app; chiavi fino a 255 caratteri; valori di testo fino a 4.096 caratteri; elenchi fino a 200 elementi di massimo 1.024 caratteri ciascuno; date tra il 1970 e il 9999; 64 KB per app in totale.
- **Non per le password**: la configurazione viene inviata solo al dispositivo per cui è costruita e i log mostrano solo nomi e tipi delle chiavi, ma gli amministratori della dashboard possono leggere i valori e l'indirizzo da cui il dispositivo la scarica cambia con i valori, quindi un valore facile da indovinare (un booleano o un numero piccolo) potrebbe essere dedotto. Non inserire password o altri segreti in una configurazione gestita.
- **Stato**: quando il dispositivo segnala che l'app non ha accettato la sua configurazione, il pannello Applicazioni del dispositivo mostra **Configurazione non accettata** accanto all'app. Questo non rende il dispositivo non conforme. Una configurazione che il dispositivo non riesce a scaricare, invece, lo rende non conforme.

Opzioni delle app

Ogni app della policy (App Store e app personalizzate) ha queste opzioni. **Predefinito del dispositivo** lascia la scelta al dispositivo. I dispositivi che non supportano un'opzione non la ricevono; l'app viene comunque installata.

- **Aggiornamenti automatici**: impostazione dell'App Store, Sempre o Mai. iOS, iPadOS, macOS e visionOS 26 o versioni successive. Per le app personalizzate, l'impostazione dell'App Store si comporta come Mai.
- **Download tramite rete cellulare**: impostazione dell'App Store, Sempre o Mai, per installazioni e aggiornamenti automatici. Solo iPhone e iPad supervisionati con iOS o iPadOS 26 o versioni successive.
- **Esegui il backup dei dati dell'app**: indica se i dati dell'app sono inclusi nei backup del dispositivo. Non su Mac.
- **L'utente può nascondere l'app** e **L'utente può bloccare l'app**: iOS e iPadOS 18.1 o versioni successive, applicato sui dispositivi supervisionati. Non consentire il blocco impedisce anche di nascondere. Le restrizioni **Consenti di nascondere le app** e **Consenti di bloccare le app** si applicano a tutte le app.
- **Blocca il dispositivo dopo le transazioni Tap to Pay che richiedono il PIN del cliente**: solo iPhone.
- **Domini associati**: i domini a cui è associata l'app (ad esempio per i link universali o la compilazione automatica delle password), fino a 50. Inserisci nomi host semplici come www.example.com, senza applinks:, caratteri jolly o ?mode=. Non su Mac.
- **Verifica i domini direttamente**: il dispositivo controlla direttamente il file di associazione del sito dei domini invece che tramite i server di Apple. Attivalo solo per i domini interni che non sono raggiungibili da Internet.
- **Rimozione**: le app installate come **Obbligatorie** non possono essere rimosse dall'utente.

App del Mac App Store

L'elenco di selezione delle app mostra le piattaforme di ogni app (iPhone/iPad, Mac, Apple TV, Vision); un'app disponibile solo per Mac mostra l'icona Mac. Un'app disponibile solo per Mac si applica ai Mac quando la aggiungi. Un'app dell'App Store senza versione per Mac non viene inviata ai Mac: la policy mostra "Questa app non ha una versione per Mac: non viene inviata ai Mac" sotto **Si applica a**. I Mac ricevono le app dell'App Store tramite il loro ID App Store, quindi le app con un bundle ID diverso su Mac vengono installate correttamente.

App Cerberus Enterprise

Cerberus installa la sua app **Cerberus Enterprise** su ogni iPhone e iPad con **iOS o iPadOS 18.4 o versioni successive**, con o senza policy. L'app condivide la posizione del dispositivo e riceve notifiche e richieste di tracciamento in tempo reale. Viene installata come **Obbligatoria**, con una licenza dispositivo di Apps and Books (una licenza utente sui dispositivi personali), quindi l'utente non può eliminarla.

- **Configurazione una tantum**: aggiungi una volta l'app gratuita alla tua libreria. In Apple Business, apri **Apps & Services → Apps & Books → App Store**, cerca "Cerberus Enterprise", fai clic su **View**, poi su **Add**, seleziona **All current and future** in **Organizational Units**, fai clic su **Add**, poi su **Review** e conferma. Se l'app mostra **Manage**, è già nella tua libreria: aprila e verifica che le sue unità organizzative siano **All current and future units**. Fino ad allora la dashboard mostra un banner e i dispositivi mostrano l'app come non installata. Vedi **Impostazioni account**
- **Non nelle policy**: l'app non può essere aggiunta a una policy. È disabilitata nell'elenco di selezione delle app e rifiutata come app personalizzata (stesso bundle ID). Una policy che la elenca già vede rimuovere la voce quando la apri: salva la policy per confermare.
- **Non installata su**: dispositivi con iOS o iPadOS precedente alla 18.4. L'installazione su iPad condiviso è supportata, ma le funzionalità dell'app non sono verificate su tali dispositivi.
- **Dispositivi personali**: su iPhone e iPad registrati con User Enrollment, anche l'app viene installata, con una richiesta di installazione e una licenza utente del Managed Apple Account. Riceve messaggi dalla tua organizzazione e non accede alla posizione a meno che la policy attivi **Posizione e geofence sui dispositivi personali** e l'utente lo consenta.
- **Mantenuta installata**: se il token di Apps and Books scade o l'app esce dalla tua libreria, l'app resta sui dispositivi e la pagina del dispositivo indica che Apps and Books richiede attenzione. Viene rimossa solo se l'app è ancora assente dalla tua libreria dopo 24 ore.

App personalizzate

Le app personalizzate sono le tue app per iPhone e iPad (file .ipa), distribuite senza l'App Store. In Xcode, esporta l'app per la distribuzione **Enterprise** (Apple Developer Enterprise Program: si installa su ogni dispositivo) o **Ad Hoc** (si installa solo sui dispositivi registrati nel suo profilo di provisioning). Le build dell'App Store non possono essere caricate.

Fai clic su **Aggiungi app personalizzata** per aprire le app personalizzate della tua organizzazione. **Carica app** aggiunge un file .ipa (fino a 2 GB). Seleziona un'app e fai clic su **Aggiungi alla policy**. L'elenco mostra la versione, il tipo di firma, il numero di dispositivi nel profilo delle app ad hoc e la data di scadenza del profilo di provisioning.

- **Nuova versione**: carica un'app con lo stesso bundle ID. Sostituisce la versione precedente e i dispositivi delle policy che la usano aggiornano l'app.
- **Requisiti**: iPhone e iPad con iOS 17.2 o versioni successive. I dispositivi che non possono installare l'app non la ricevono: un'app solo per iPad su un iPhone, un iOS precedente a quello richiesto dall'app, un dispositivo non presente nel profilo di un'app ad hoc o un profilo di provisioning scaduto.
- **Scadenza**: quando il profilo di provisioning scade, l'app non si apre più. Carica una versione firmata con un nuovo profilo prima della data di scadenza.
- **Bundle ID riservato**: un'app personalizzata con il bundle ID dell'app Cerberus Enterprise (com.lsdroid.Cerberus.Enterprise) non può essere aggiunta a una policy, perché Cerberus

installa quell'app autonomamente.
- **Elimina**: rimuovi prima l’app dalle sue policy; i dispositivi la rimuoveranno poi.

Pacchetti Mac

Anche le app personalizzate accettano pacchetti di installazione per Mac (file .pkg). Il pacchetto deve essere un pacchetto di distribuzione creato con **productbuild** (un pacchetto componente creato solo con pkgbuild viene rifiutato) e firmato con un certificato **Developer ID Installer**. Si consiglia di notarizzarlo e di applicare il ticket (**notarytool** e **stapler**). I pacchetti non firmati, i pacchetti modificati dopo la firma e i pacchetti firmati con altri certificati vengono rifiutati.

Carica il file .pkg con **Carica app** e aggiungilo alla policy: compare in **Pacchetti Mac**. iPhone e iPad lo ignorano.

I Mac con **macOS 26 o versioni successive** (supervisionati, il che include i Mac registrati manualmente, ma non la registrazione utente) ricevono il pacchetto come **dichiarazione**: il Mac lo scarica, lo installa, riprova e lo aggiorna da solo e ne segnala lo stato. I Mac meno recenti, e i pacchetti installati come app gestite, lo ricevono con un **comando MDM**, su qualsiasi versione di macOS. Un Mac aggiornato a macOS 26 passa da solo alla dichiarazione; può installare di nuovo ogni pacchetto una volta. Lo stesso può accadere quando un Mac passa a un’altra policy che contiene lo stesso pacchetto.

- **Nuova versione**: carica un pacchetto con lo stesso identificatore di pacchetto. Sostituisce la versione precedente e i Mac delle policy che lo usano installano quella nuova.
- **Mac saltati**: Mac con una versione di macOS precedente a quella consentita dal pacchetto e Mac Intel per pacchetti creati solo per Apple silicon. La pagina del dispositivo mostra il pacchetto come Saltato, con il motivo; la versione installata in precedenza resta sul Mac.
- **Installa**: **Obbligatorio** (predefinito) installa il pacchetto sul Mac; **Facoltativo** rende il pacchetto disponibile sul Mac senza installarlo. macOS 26 non mostra i pacchetti facoltativi all’utente in Impostazioni di Sistema o nell’App Store (testato su macOS 26.3), quindi un’app o uno script sul Mac deve installarli; scegli Facoltativo solo se ne disponi. Si applica ai Mac con macOS 26 o versioni successive; i Mac meno recenti installano sempre il pacchetto. L’opzione non è disponibile per i pacchetti installati come app gestite.
- **Rimuovi i file del pacchetto quando esce dalla policy (macOS 27 o versioni successive)**: quando il pacchetto viene rimosso dalla policy, i Mac con macOS 27 o versioni successive eliminano i file che ha installato. È disattivato per impostazione predefinita. Sui Mac meno recenti i file restano. Non disponibile per i pacchetti installati come app gestite.
- **Installa come app gestita**: attivalo per un pacchetto della policy per installare la sua app come app gestita (macOS 11 o versioni successive, non con la registrazione utente). macOS segnala quindi quando l’installazione non riesce e MDM può rimuovere l’app. L’app deve essere installata direttamente nella cartella Applicazioni, firmata con un certificato

Developer ID Application e notarizzata; su macOS da 11 a 13 il pacchetto deve contenere solo quell'app (nessun altro file o script). Le app personalizzate mostrano quali pacchetti sono idonei. Quando l'opzione non può essere applicata su un Mac, il pacchetto viene installato lì come al solito e la pagina del dispositivo ne spiega il motivo.

- **Opzioni di rimozione** di un'app gestita: **Rimuovi l'app quando il pacchetto viene rimosso dalla policy** (attivato per impostazione predefinita) e **Rimuovi l'app quando il Mac esce dalla gestione**. La rimozione di un'app elimina anche i suoi dati. Se l'utente aveva già installato la stessa app, quella copia diventa gestita e viene rimossa anch'essa.
- **Rimozione**: il comando MDM non può disinstallare un pacchetto. Per un pacchetto installato come app gestita, rimuoverlo dalla policy rimuove l'app (quando l'opzione è attiva); gli altri suoi file e la ricevuta del pacchetto restano. I pacchetti con **Rimuovi i file del pacchetto** attivo vengono rimossi dai Mac con macOS 27 o versioni successive. Altri pacchetti: rimuoverli dalla policy interrompe solo le nuove installazioni, i file restano sui Mac. Un Mac saltato (ad esempio dopo una nuova versione che richiede un macOS più recente) mantiene l'app finché il pacchetto è nella policy; rimuovendo poi il pacchetto dalla policy viene rimossa anche l'app. Rimuovi i file rimasti sul Mac (ad esempio con il disinstallatore del pacchetto) ed esegui `sudo pkgutil --forget <identifier>` per dimenticare la ricevuta del pacchetto.
- **Stato sul dispositivo**: il pannello Applicazioni del Mac mostra ogni pacchetto della policy come In coda, Accettato (il Mac ha accettato il comando), Scaricato, Installato (solo per i pacchetti che contengono app, quando le app vengono trovate sul Mac) o Non riuscito (con l'errore). macOS non segnala l'installazione di un pacchetto inviato con il comando, quindi Scaricato è l'ultimo stato per i pacchetti senza app. Un pacchetto installato come app gestita diventa Non riuscito anche quando macOS segnala che l'app non è stata installata o è stata rimossa dal Mac. **Installa di nuovo** invia di nuovo il pacchetto al Mac.
- **Stato con la dichiarazione**: i pacchetti consegnati come dichiarazione mostrano il chip **Dichiarazione** e lo stato segnalato dal Mac: In coda, Disponibile (un pacchetto facoltativo che l'utente non ha installato), In attesa dell'utente, Download in corso, Installazione in corso, Installato o Non riuscito (con il motivo, ad esempio un download o un'installazione non riusciti, o una dichiarazione rifiutata dal Mac). Il chip **File rimossi con la policy** contrassegna i pacchetti i cui file vengono rimossi da un Mac con macOS 27 quando escono dalla policy. **Installa di nuovo** compare solo dopo un errore e chiede al Mac di riprovare; non viene offerto quando il Mac ha rifiutato la dichiarazione.

Account

Il pannello **Account** ti consente di configurare gli account applicati ai dispositivi gestiti. Include anche un'opzione di restrizione per la modifica degli account.

Restrizione

- **Consenti la modifica degli account**: se disattivato, gli utenti non possono modificare account come gli account Apple e gli account internet.

Aggiungi account

Usa **Aggiungi account Google** o **Aggiungi account di posta** per aggiungere i payload degli account alla policy. Ogni account compare come una scheda con i suoi campi di configurazione.

Credenziali dell’account fornite dagli utenti

Sia le schede degli account Google sia quelle degli account di posta forniscono un’opzione **Credenziali dell’account fornite dagli utenti**. Se attivata, il sistema applica le credenziali dell’account per singolo utente. Se disattivata, inserisci l’identità dell’account nella policy.

Campi dell’account Google

- **Nome visibile**: il nome mostrato all’utente per l’account.
- **Indirizzo email Google**: l’indirizzo email dell’utente.
- **Nome completo**: il nome completo dell’utente.

Campi dell’account di posta

Gli account di posta includono i campi di identità e la configurazione dei server in entrata e in uscita. I nomi host sono obbligatori.

- **Nome visibile**: il nome mostrato all’utente per l’account di posta.
- **Indirizzo email**: l’indirizzo email dell’utente.
- **Nome completo**: il nome completo dell’utente.

Server in entrata

- **Tipo di server**: protocollo di posta (ad esempio IMAP o POP).
- **Metodo di autenticazione**: metodo di autenticazione per il server.
- **Prefisso del percorso IMAP**: mostrato solo quando il Tipo di server è IMAP.
- **Nome host**: obbligatorio.
- **Porta**: porta del server (1–65535).

Server in uscita

- **Metodo di autenticazione**
- **Nome host**: obbligatorio.
- **Porta**: porta del server (1–65535).

Opzioni S/MIME

Per gli account di posta, puoi anche configurare il comportamento di cifratura e firma S/MIME.

Cifratura

- **Cifratura S/MIME**
- **Identità modificabile dall’utente**
- **Interruttore per singolo messaggio attivo**
- **Modificabile dall’utente**

Firma

- **Firma S/MIME**
- **Identità modificabile dall’utente**
- **Modificabile dall’utente**

> Le opzioni degli account e delle restrizioni includono tooltip nella dashboard che documentano i prerequisiti e le versioni del sistema operativo supportate.

Chiosco e schermata Home

La sezione **Chiosco e schermata Home** dell'Editor delle policy Apple blocca i dispositivi su una sola app, sceglie quali app possono essere aperte, dispone la schermata Home e aggiunge icone di siti web. Ogni impostazione viene installata sui dispositivi come profilo di configurazione.

> Apple applica la maggior parte di queste impostazioni solo agli iPhone e agli iPad supervisionati (dispositivi registrati con Automated Device Enrollment o preparati con Apple Configurator). Gli altri dispositivi non le ricevono. Le web clip funzionano anche su iPhone e iPad non supervisionati. I Mac non ricevono nessuna di queste impostazioni.

Scelta delle app

Le app sono identificate dal loro bundle ID. Digita il nome di un'app per sceglierla tra le app Apple integrate e le app della policy, oppure digita un bundle ID qualsiasi, ad esempio `com.example.app`.

Modalità app singola

Il dispositivo esegue solo l'app scelta: gli utenti non possono tornare alla schermata Home né aprire altre app. Installa prima l'app con la policy. Il dispositivo esce dalla modalità app singola quando disattivi l'impostazione o rimuovi l'app.

- **Opzioni**: disattiva il touchscreen, la rotazione, i pulsanti del volume, l'interruttore Suoneria/Silenzioso, il pulsante laterale o il blocco automatico e attiva funzioni di accessibilità come VoiceOver o Zoom.
- **Funzioni di accessibilità che l'utente può attivare**: funzioni che l'utente può attivare con un triplo clic del pulsante laterale.

App consentite e bloccate

- **App bloccate**: i dispositivi nascondono queste app e non le aprono. `com.apple.webapp` blocca tutte le web clip. Impostazioni e, su iPhone, Telefono non possono essere bloccati.
- **Consenti solo alcune app**: i dispositivi mostrano solo queste app. Lascia vuoto l'elenco per consentire tutte le app. **App della policy** aggiunge le app installate dalla policy; `com.apple.webapp` consente tutte le web clip.

- **App che possono avviare la modalità app singola**: app che possono bloccare il dispositivo su se stesse mentre ne hanno bisogno, ad esempio durante un esame.

> Con **Consenti solo alcune app**, ogni app che non è nell'elenco scompare dai dispositivi, incluse le app della policy. Impostazioni e, su iPhone, Telefono restano sempre.

Layout della schermata Home

Disponi il Dock e le pagine della schermata Home. Aggiungi app, cartelle di app e le web clip della policy, scegliendo dove con **Aggiungi a**, e trascina le icone per spostarle tra il Dock e le pagine. Fai clic su una cartella per modificarne il nome e le app.

Gli utenti non possono spostare le icone né rimuovere app dalla schermata Home. Le app che non sono nel layout vanno nelle pagine successive a quelle definite. Un iPhone mostra quattro icone nel Dock. Gli utenti possono comunque eliminare le app non obbligatorie nella schermata di archiviazione delle Impostazioni. Per impedirlo, disattiva **Consenti rimozione app** in Gestione app.

Web clip

Una web clip è un’icona sulla schermata Home che apre un sito web. Imposta l’etichetta e l’URL e, facoltativamente, un’immagine (PNG o JPEG, ritagliata in un quadrato).

- **Gli utenti possono rimuoverla**: disattiva per mantenere l’icona sui dispositivi.
- **Schermo intero**: il sito web si apre come web app, senza la barra degli indirizzi di Safari. **Resta a schermo intero sugli altri siti web** apre nella web app anche i link ad altri siti web.
- **Apri con questa app**: un’app che apre l’URL al posto di Safari.

Impostazioni delle notifiche

Scegli in che modo i dispositivi mostrano le notifiche di alcune app: se sono consentite, dove compaiono (schermata di blocco, Centro notifiche, CarPlay), i badge, i suoni, gli avvisi critici, lo stile dei banner, il raggruppamento e le anteprime. Gli utenti non possono modificare queste impostazioni.

Messaggio della schermata di blocco

Un messaggio mostrato in fondo alla schermata di blocco, ad esempio chi chiamare se il dispositivo viene trovato, e un’etichetta di inventario. Entrambi possono contenere le variabili $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$: una variabile senza valore per il dispositivo viene lasciata vuota.

Codice

La sezione **Impostazioni del codice di accesso** controlla i requisiti del codice di accesso del dispositivo e le regole di sicurezza correlate (ad esempio lunghezza minima e complessità). Su un Mac (macOS 13 o versione successiva, non con la Registrazione utente) le regole si applicano alla password di accesso degli utenti.

Opzioni

Nell'Editor delle policy Apple, le opzioni del codice di accesso vengono configurate con una combinazione di interruttori e campi numerici. Molti campi includono tooltip che indicano le versioni del sistema operativo supportate e i requisiti di supervisione.

Interruttori del codice di accesso

- **Cambia alla prossima autenticazione**: forza la reimpostazione del passcode alla prossima autenticazione dell'utente.
- **Richiedi passcode alfanumerico**: richiedi almeno un carattere alfabetico e un numero.
- **Richiedi passcode complesso**: richiedi un passcode "complesso" (nessun pattern ripetitivo/sequenziale e almeno un carattere non alfanumerico).
- **Richiedi passcode**: richiedi un passcode senza ulteriori requisiti di lunghezza/qualità. Nota: impostare altre chiavi del passcode richiede implicitamente un passcode.

Campi numerici

- **Reimpostazione tentativi non riusciti (minuti)**: minuti prima che il contatore dei tentativi non riusciti venga reimpostato (richiede Numero massimo di tentativi non riusciti).
- **Numero massimo di tentativi non riusciti**: tentativi non riusciti consentiti prima che un iPhone o un iPad venga cancellato, o un Mac venga bloccato (intervallo: 2–11).
- **Periodo di tolleranza massimo (minuti)**: per quanto tempo il dispositivo può restare sbloccato senza richiedere il passcode (0 = nessuno).
- **Inattività massima (minuti)**: tempo di inattività prima che il dispositivo si blocchi (intervallo: 0–15).
- **Durata massima del passcode (giorni)**: durata massima del passcode prima di una modifica forzata (intervallo: 0–730).
- **Caratteri complessi minimi**: numero minimo di caratteri "complessi" (intervallo: 0–4).
- **Lunghezza minima**: lunghezza minima del passcode (intervallo: 0–16).

- **Limite riutilizzo passcode**: lunghezza della cronologia dei passcode per evitare il riutilizzo di passcode precedenti (intervallo: 1–50).

Restrizioni

Le sezioni Restrizioni controllano quali funzioni del sistema operativo sono consentite sui dispositivi Apple gestiti. Nell’Editor delle policy Apple, queste opzioni sono presentate come pannelli raggruppati con più interruttori.

Le opzioni dei pannelli **Gestione app** e **Rete** sono descritte nelle pagine App e profili e Rete delle policy Apple.

> Molte restrizioni sono supportate solo su versioni specifiche del sistema operativo e possono richiedere dispositivi supervisionati. Usa i tooltip nella dashboard per i requisiti ufficiali.

> Sui dispositivi con registrazione utente (dispositivi personali registrati effettuando l’accesso con un account di lavoro), le restrizioni che Apple non consente in quel contesto non vengono inviate. Se nessuna delle restrizioni della policy si applica, questi dispositivi non ricevono alcun profilo di restrizioni. L’editor delle policy mostra quante restrizioni non si applicano ai dispositivi con registrazione utente.

Sicurezza

- **Consenti lo sblocco automatico**
- **Consenti l’impronta digitale per lo sblocco**
- **Consenti la modifica dell’impronta digitale**
- **Consenti cancellazione contenuti e impostazioni**
- **Consenti abilitazione delle restrizioni**
- **Consenti installazione dei profili da parte degli utenti**
- **Consenti associazione con host**
- **Consenti invio dati diagnostici**
- **Consenti modifica dell'invio di dati diagnostici**
- **Consenti pubblicità personalizzata Apple**
- **Consenti modifica di Remote Management**

Multimedia

- **Consenti fotocamera**

- **Consenti modifica condivisione file**
- **Consenti accesso alle unità USB in File**
- **Consenti registrazione delle chiamate**
- **Consenti AirPrint**
- **Consenti memorizzazione credenziali AirPrint**
- **Consenti rilevamento iBeacon per AirPrint**

Cellulare

- **Consenti modifica dati cellulare delle app**
- **Consenti modifica piano cellulare**
- **Consenti modifica eSIM**
- **Consenti trasferimenti eSIM in uscita**
- **Mantieni l'eSIM quando il dispositivo viene cancellato**
- **Consenti recupero in background durante il roaming**

APN cellulare

APN cellulare imposta il nome del punto di accesso (APN) fornito dal tuo operatore, ad esempio per una rete mobile privata o aziendale. Imposta il **nome del punto di accesso** e, se l'operatore li richiede, l'autenticazione (PAP o CHAP), il nome utente (sono consentite variabili come $EMAIL$), la password, le versioni IP (anche in roaming), un server proxy con la sua porta e XLAT464. Attiva **Collega APN** solo se l'operatore ti fornisce un APN separato per connettersi alla rete.

- Lo ricevono solo iPhone e iPad cellulari, anche senza supervisione. I dispositivi registrati con la registrazione utente (dispositivi personali) non lo ricevono.
- Si applica solo alla SIM usata per i dati cellulare. Un dispositivo che ha già installato un profilo APN in un altro modo non lo installa.
- La password è protetta come le altre password di rete: il profilo viene inviato solo al dispositivo per cui è stato creato e la password non viene scritta nei log.

> Un APN errato lascia i dispositivi senza dati cellulare: prova prima le impostazioni su un dispositivo di test con una SIM dell'operatore.

Sistema e interfaccia utente

- **Consenti Handoff**
- **Consenti correzione automatica**

- **Consenti oscuramento automatico**
- **Consenti salvaschermo automatico**
- **Consenti tastiera QuickPath**
- **Consenti ricerca delle definizioni**
- **Consenti modifica del nome del dispositivo**
- **Consenti sospensione del dispositivo**
- **Consenti iPhone Mirroring**
- **Consenti widget iPhone su Mac**
- **Consenti scorciatoie da tastiera**

App e servizi Apple

- **Consenti iMessage**
- **Consenti Game Center**
- **Consenti aggiunta di amici in Game Center**
- **Consenti Dov'è dispositivo**
- **Consenti Dov'è amici**
- **Consenti modifica di Dov'è amici**
- **Consenti Book Store**
- **Consenti contenuti erotici in Book Store**
- **Consenti backup dei libri aziendali**
- **Consenti sincronizzazione dei metadati dei libri aziendali**
- **Consenti iTunes Store**
- **Consenti contenuti espliciti**

Siri e Apple Intelligence

- **Consenti Siri**
- **Consenti contenuti generati dagli utenti in Siri**
- **Consenti Siri quando il dispositivo è bloccato**
- **Consenti dettatura**
- **Consenti integrazioni con intelligenze esterne**
- **Consenti accesso alle intelligenze esterne**
- **Consenti Genmoji**
- **Consenti Image Playground**
- **Consenti Image Wand**

iCloud

- **Consenti la rubrica iCloud**
- **Consenti il backup iCloud**
- **Consenti i segnalibri iCloud**
- **Consenti il calendario iCloud**
- **Consenti Scrivania e Documenti iCloud**
- **Consenti la sincronizzazione dei documenti iCloud**
- **Consenti Freeform iCloud**
- **Consenti la sincronizzazione del portachiavi iCloud**
- **Consenti Mail iCloud**
- **Consenti Note iCloud**
- **Consenti Libreria foto iCloud**
- **Consenti Inoltro privato iCloud**
- **Consenti Promemoria iCloud**

Account (limitazione)

Il pannello Account contiene sia una limitazione sia (facoltativamente) la configurazione degli account. L'interruttore della limitazione controlla se l'utente può modificare gli account di sistema.

- **Consenti modifica account**

Rete

La sezione **Rete** dell'Apple Policy Editor configura reti Wi-Fi e VPN sui dispositivi, installa certificati e limita funzionalità di connettività come AirDrop e Bluetooth. Ogni rete Wi-Fi, VPN e certificato viene installato come profilo di configurazione separato, che puoi vedere sul dispositivo in **Impostazioni > Generali > VPN e gestione dispositivo** (Mac: **Impostazioni di Sistema > Generali > Gestione dispositivo**, oppure **Privacy e sicurezza > Profili** su macOS 13 e 14) e nel pannello **Profili, certificati e sicurezza** della pagina del dispositivo.

> I certificati vengono presi dalla pagina **Certificati**: importali prima lì. La policy vi fa solo riferimento, quindi un certificato non viene mai copiato nella policy.

Restrizioni

- **Consenti AirDrop**
- **Consenti richieste AirPlay in entrata**
- **Consenti modifica Bluetooth**
- **Consenti modifica condivisione Bluetooth**
- **Consenti accesso alle unità di rete in File**
- **Consenti modifica condivisione Internet**
- **Consenti cache dei contenuti**
- **Consenti condivisione file di iTunes**

Reti Wi-Fi

Fai clic su **Aggiungi rete Wi-Fi** e compila:

- **Nome della rete (SSID)**: il nome della rete, fino a 32 caratteri.
- **Sicurezza**: nessuna (rete aperta), WEP, WPA o WPA2, WPA2 o WPA3, solo WPA3 oppure qualsiasi.
- **Password**: la password di una rete personale.
- **Unisciti automaticamente** e **Rete nascosta** (per le reti che non trasmettono il proprio nome).
- **Proxy**: nessuno, manuale (server e porta) o automatico (l’URL di un file PAC, oppure vuoto per trovare le impostazioni sulla rete con WPAD).

- **Nome del profilo** (facoltativo) e **Si applica a**, per limitare la rete ad alcuni tipi di dispositivi.

Reti aziendali (802.1X)

Attiva **Aziendale (802.1X)** quando gli utenti si autenticano con le proprie credenziali o un certificato invece di una password condivisa.

- **Autenticazione**: PEAP, TTLS (con la sua autenticazione interna, ad esempio MSCHAPv2) o TLS (solo certificato).
- **Credenziali dell'utente del dispositivo**: ogni dispositivo usa l'identità EAP, l'identità anonima e la password del suo utente, impostate nella pagina Utenti. I dispositivi senza utente non ricevono la rete.
- **Identità**, **Identità anonima** e **Password**: le stesse per ogni dispositivo. L'identità può contenere le variabili $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$. Lascia vuota la password per consentire all'utente di digitarla sul dispositivo.
- **Certificato di identità**: il certificato client che il dispositivo presenta (obbligatorio per TLS). Vedi le opzioni dei certificati di seguito.
- **Certificati attendibili**: i certificati CA che hanno emesso il certificato del tuo server RADIUS. Vengono installati con la rete.
- **Nomi dei server attendibili**: i nomi dei certificati del server RADIUS che i dispositivi accettano, ad esempio radius.example.com o *.example.com.

VPN

Fai clic su **Aggiungi VPN** per configurare una VPN IKEv2 o Cisco IPSec, integrata in iOS, iPadOS e macOS (non serve un'app VPN).

- **Tipo** e **Server**. Per IKEv2 anche l'**Identificatore remoto** (l'identità del server, vuoto significa l'indirizzo del server) e l'**Identificatore locale**, che può contenere le variabili $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$.
- **Autenticazione** del dispositivo: un certificato (dalla pagina Certificati, il certificato dell'utente del dispositivo o richiesto a un server SCEP), un segreto condiviso (con il nome del gruppo facoltativo per IPSec) oppure nessuna per i server IKEv2 che controllano solo nome utente e password.
- **Certificati attendibili**: i certificati CA del tuo server VPN, installati con la VPN. Per IKEv2 puoi anche impostare l'emittente e il nome attesi del certificato del server.
- **Nome utente e password**: l'utente si autentica anche con un nome utente (variabili consentite) e una password (EAP per IKEv2, XAuth per IPSec). Lascia vuota la password per consentire all'utente di digitarla sul dispositivo.
- **Nome VPN** (mostrato in Impostazioni) e **Si applica a**.

Connessione

- **L’utente si connette in Impostazioni**: la VPN viene installata e l’utente la attiva quando serve.
- **Su richiesta**: il dispositivo connette automaticamente la VPN. Con **tranne che su Wi-Fi attendibili** la VPN non viene usata sulle reti Wi-Fi che elenchi, ad esempio la rete dell’ufficio.
- **Sempre attiva** (IKEv2, solo iPhone e iPad supervisionati): tutto il traffico passa attraverso la VPN su rete cellulare e Wi-Fi e l’utente non può disattivarla. Gli altri dispositivi non ricevono questa VPN. Se la VPN usa un nome utente, la password deve essere impostata nella policy.
- **VPN per app**: solo alcune app usano la VPN. Scegli la VPN per ogni app nella sezione **Gestione app** (campo **VPN** dell’app, non disponibile su Mac) e, facoltativamente, elenca i domini Safari che la usano.

> Prova prima una VPN Sempre attiva o su richiesta su un dispositivo di test: se il server non è raggiungibile, il dispositivo potrebbe non avere alcuna connessione.

Proxy globale, DNS cifrato e filtro dei contenuti web

Queste impostazioni si applicano a tutto il traffico del dispositivo. Attivale con il rispettivo interruttore.

- **Proxy HTTP globale** (iPhone e iPad supervisionati, Mac): tutto il traffico HTTP passa attraverso il proxy, su ogni rete. Imposta il server e la porta (con nome utente e password facoltativi) oppure una configurazione automatica (URL del file PAC, oppure vuoto per trovarlo sulla rete). **Consenti le pagine di accesso Wi-Fi** permette all’utente di accedere alle reti Wi-Fi pubbliche senza il proxy.
- **DNS cifrato**: il dispositivo risolve i nomi con il tuo server DNS tramite DNS over HTTPS (URL del server) o DNS over TLS (nome del server), facoltativamente solo per alcuni domini. Sui dispositivi supervisionati puoi impedire all’utente di disattivarlo.
- **Filtro dei contenuti web** (iPhone e iPad supervisionati): il filtro integrato in iOS limita i siti web per adulti, con elenchi di siti web sempre consentiti o sempre bloccati, oppure consente solo un elenco di siti web, mostrati come segnalibri in Safari.

> Un proxy o un server DNS errato può lasciare i dispositivi senza connessione: prova prima le impostazioni su un dispositivo di test.

Certificati

Fai clic su **Aggiungi certificato** per installare un certificato da solo: un’autorità di certificazione a cui Safari e le app devono fidarsi, oppure un’identità usata dalle app. I certificati di una rete Wi-Fi o di una VPN non devono essere aggiunti qui.

Opzioni dei certificati

- **Un certificato della pagina Certificati**: lo stesso certificato su ogni dispositivo. Fai clic su **Scegli un certificato** per selezionarlo.
- **Il certificato dell’utente del dispositivo**: ogni dispositivo riceve il certificato client collegato al suo utente. I dispositivi il cui utente non ha un certificato non lo ricevono. Quando colleghi un altro certificato all’utente, i dispositivi vengono aggiornati.
- **Richiesto a un server SCEP**: ogni dispositivo richiede il proprio certificato al tuo server SCEP (ad esempio Microsoft NDES), così la chiave privata non lascia mai il dispositivo. Imposta l’URL del server, la challenge se il server la richiede, il soggetto (ad esempio CN=$EMAIL$), i nomi alternativi, la dimensione della chiave e l’utilizzo della chiave.

> I certificati client (.p12) protetti con la vecchia crittografia RC2 non possono essere installati sui dispositivi Apple. Esportali di nuovo con crittografia 3DES o AES prima di importarli.

Sicurezza

I profili che contengono password o chiavi private vengono inviati solo al dispositivo per cui sono stati creati: il dispositivo deve firmare la sua richiesta con il suo certificato di gestione. Le password e i certificati non vengono scritti nei log.

Aggiornamenti software

La sezione **Aggiornamenti software** dell'Apple Policy Editor mantiene i dispositivi aggiornati: può richiedere una versione specifica del sistema entro una scadenza e controllare come i dispositivi scaricano e installano gli aggiornamenti.

Aggiornamenti del sistema richiesti

Fai clic su **Aggiungi aggiornamento richiesto** per richiedere una versione del sistema. Il dispositivo scarica l'aggiornamento, comunica all'utente la scadenza e lo installa alla scadenza se l'utente non l'ha già fatto. I dispositivi che eseguono già quella versione o una successiva lo ignorano. Richiede iOS e iPadOS 17 o macOS 14.

- **Si applica a** (obbligatorio): iPhone e iPad, oppure Mac. Ogni sistema ha i propri numeri di versione, quindi aggiungi un aggiornamento richiesto per ciascuno.
- **Versione del sistema**: la versione da installare, ad esempio 18.5 o 15.4.1.
- **Build** (facoltativo): una build specifica, ad esempio una beta o un Miglioramento della sicurezza in background.
- **Installa entro**: la scadenza, nell'ora locale di ciascun dispositivo. Una data passata fa sì che i dispositivi installino l'aggiornamento il prima possibile.
- **URL dei dettagli** (facoltativo): una pagina web sull'aggiornamento, mostrata all'utente.

> Il dispositivo segnala l'avanzamento dell'aggiornamento (download, installazione, errori) nel pannello **Stato dispositivo** della pagina del dispositivo.

Impostazioni degli aggiornamenti software

Attiva **Impostazioni degli aggiornamenti software per iPhone e iPad** o **Impostazioni degli aggiornamenti software per Mac** per controllare gli aggiornamenti su quei dispositivi. Quando un interruttore è disattivato, i dispositivi mantengono le proprie impostazioni. Richiede iOS e iPadOS 18 o macOS 15: i dispositivi meno recenti ignorano queste impostazioni.

- **Posticipa aggiornamenti**: i nuovi aggiornamenti vengono mostrati all'utente solo dopo il numero di giorni indicato (da 1 a 90). Su un Mac puoi impostare periodi diversi per gli aggiornamenti major, gli aggiornamenti minor e gli altri aggiornamenti di sistema.
- **Aggiornamenti mostrati all'utente** (iPhone e iPad): quando è disponibile più di un aggiornamento, mostrali tutti, solo l'aggiornamento minor più vecchio o solo il più recente.
- **Gli utenti standard possono installare gli aggiornamenti** (Mac): gli utenti senza diritti di amministratore possono installare gli aggiornamenti di macOS.
- **Notifica all'utente gli aggiornamenti richiesti**: mostra le notifiche sugli aggiornamenti richiesti e la loro scadenza.
- **Download automatico**, **Installazione automatica** e **Aggiornamenti di sicurezza automatici**: lascia decidere all'utente (impostazione predefinita di Apple) oppure mantienili sempre attivi o sempre disattivati.
- **Miglioramenti della sicurezza in background**: offri all'utente le correzioni di sicurezza rapide di Apple e scegli se l'utente può rimuoverle.
- **Programmi beta**: consenti all'utente di partecipare ai programmi beta di Apple, oppure rimuovi il dispositivo e bloccali (su iPhone e iPad, solo dispositivi supervisionati).

Installare un aggiornamento dalla pagina del dispositivo

Il pannello **Stato dispositivo** di un dispositivo elenca gli aggiornamenti disponibili. Usa **Verifica aggiornamenti** per chiedere al dispositivo l'elenco e **Installa** per installarne uno subito o per scaricarlo e lasciare che lo installi l'utente. Funziona su iPhone e iPad supervisionati e sui Mac. Apple rimuove questi comandi in iOS, iPadOS e macOS 27: su quelle versioni usa gli aggiornamenti richiesti della policy.

macOS

La sezione **macOS** dell'Editor delle policy Apple gestisce le impostazioni di sicurezza, privacy e accesso dei Mac: FileVault, firewall, Gatekeeper, salvaschermo e blocco, archiviazione esterna e di rete, Condivisione schermo, autorizzazioni per la privacy, elementi di accesso e le estensioni di sistema e del kernel autorizzate a caricarsi. Installa anche i file di configurazione dei servizi di sistema e delle attività in background. Gli altri dispositivi della policy non ricevono queste impostazioni. Attiva un'impostazione per gestirla; finché è disattivata, gli utenti mantengono le proprie scelte.

> La maggior parte delle impostazioni viene installata sul Mac come profili di configurazione, visibili in Impostazioni di Sistema > Generali > Gestione dispositivo. FileVault, le autorizzazioni per la privacy, gli elementi di accesso e le impostazioni delle estensioni richiedono un MDM approvato dall'utente: su un Mac registrato con l'URL di registrazione o il codice QR, l'utente approva il profilo di registrazione in Impostazioni di Sistema. La pagina del dispositivo lo mostra nel campo **MDM approvato dall'utente**. Quando l'utente lo approva in seguito, il Mac riceve automaticamente queste impostazioni.

FileVault

FileVault cifra il disco del Mac. Con questa impostazione attiva, agli utenti viene chiesto di attivare FileVault con la loro password e il Mac invia la sua chiave di recupero personale a Cerberus Enterprise, cifrata con una chiave che appartiene solo alla tua organizzazione. La chiave viene mostrata e modificata dal campo **FileVault** della pagina del dispositivo (vedi Comandi dispositivo). L'impostazione richiede macOS 13 o versioni successive e un MDM approvato dall'utente; senza un MDM approvato dall'utente al Mac non viene chiesto di attivare FileVault, ma se un utente lo attiva, la sua chiave viene memorizzata.

- **Richiesto all'accesso**: al prossimo accesso, dopo un certo numero di rinvii (all'utente viene chiesto di nuovo a ogni accesso e alla disconnessione) oppure solo quando l'utente si disconnette.
- **Non chiedere alla disconnessione**: all'utente viene chiesto solo all'accesso. Non può essere combinato con "Chiesto solo alla disconnessione".
- **Mostra la chiave di recupero all'utente**: disattivato per impostazione predefinita, quindi solo gli amministratori conoscono la chiave, dalla pagina del dispositivo.
- **Impedisci la disattivazione di FileVault**: attivato per impostazione predefinita.
- **Rimuovi la chiave dalla memoria in standby**: l'utente digita di nuovo la password quando il Mac si riattiva dallo standby.

- **Dove viene conservata la chiave**: testo mostrato all’utente nella finestra di accesso, ad esempio chi chiamare per recuperare il Mac (predefinito "Cerberus Enterprise").

> Un Mac già cifrato quando ha ricevuto l’impostazione mantiene la chiave attuale, che Cerberus Enterprise non riceve: la chiave viene memorizzata solo dopo che l’utente disattiva e riattiva FileVault (con "Impedisci la disattivazione di FileVault" disattivato). Disattivare l’impostazione o rimuovere il Mac dalla gestione non disattiva FileVault e la chiave memorizzata continua a funzionare. L’impostazione non può essere salvata quando il server non è configurato per memorizzare le chiavi di recupero.

Firewall

- **Attiva il firewall**: quando è disattivato, il firewall resta spento e gli utenti non possono attivarlo.
- **Blocca tutte le connessioni in entrata**: solo i servizi di rete di base (DHCP, Bonjour, IPSec) possono ricevere connessioni.
- **Modalità invisibile**: il Mac non risponde alle richieste ping e alle connessioni verso porte chiuse.
- **Consenti al software integrato** e **Consenti alle app firmate scaricate** di ricevere connessioni senza chiedere all’utente (macOS 12.3 o versioni successive).
- **Regole per app specifiche**: consenti o blocca le connessioni in entrata di un’app, tramite bundle ID.

Gatekeeper

Gatekeeper controlla le app prima che si aprano. Scegli se i Mac aprono solo app dell’App Store o anche app di sviluppatori identificati. Con Gatekeeper disattivato, qualsiasi app può essere aperta, anche quelle non firmate o danneggiate. Su macOS 15 o versioni successive puoi anche scegliere se agli utenti viene chiesto di inviare ad Apple il malware bloccato.

Salvaschermo e blocco

Avvia il salvaschermo dopo un periodo di inattività e chiedi la password quando il salvaschermo si avvia o il display va in standby, subito o dopo un ritardo. Un’impostazione lasciata su **Non gestita** resta una scelta dell’utente.

Archiviazione esterna e di rete

Consenti, imposta come sola lettura o blocca l’archiviazione esterna (unità USB, schede SD, dischi esterni) e l’archiviazione di rete (condivisioni file) dei Mac. Richiede macOS 15 o versioni successive.

Condivisione schermo

Limiti per le persone che si connettono a questi Mac con la Condivisione schermo: copia di file da o verso il Mac, connessioni ad alte prestazioni e numero di display virtuali. Attivare la Condivisione schermo resta una scelta dell’utente. Richiede macOS 14 o versioni successive.

Autorizzazioni per la privacy

Concedi o nega alle app l’accesso che gli utenti altrimenti consentirebbero in Impostazioni di Sistema > Privacy e sicurezza, ad esempio Accesso completo al disco per un’app di backup, oppure nega la fotocamera a un’app. Per ogni autorizzazione scegli:

- **Autorizzazione**: Accesso completo al disco, Accessibilità, Automazione, le cartelle, i contatti, i calendari, le foto, la fotocamera, il microfono, la registrazione dello schermo e le altre di Privacy e sicurezza.
- **Accesso**: consenti o nega. La fotocamera, il microfono, la registrazione dello schermo e il monitoraggio dell’input non possono essere consentiti da un profilo, ma solo negati; per la registrazione dello schermo e il monitoraggio dell’input puoi consentire agli utenti di autorizzarli anche senza diritti di amministratore.
- **App**: il bundle ID di un’app o il percorso di un programma (ad esempio uno strumento da riga di comando).
- **Requisito del codice**: identifica l’app tramite la sua firma. Ottienilo nel Terminale con `codesign -dr - /Applications/Example.app` e copia il testo dopo `designated =>`.
- **Automazione** richiede anche l’app controllata (ad esempio il Finder) e il suo requisito del codice.

Elementi di accesso e in background

Gli elementi di accesso e gli elementi in background che corrispondono alle regole sono gestiti: vengono eseguiti senza chiedere e gli utenti non possono disattivarli in Impostazioni di Sistema > Generali > Elementi di accesso. Una regola corrisponde al team ID dello sviluppatore di un'app, al suo bundle ID o all'etichetta di un launch daemon o agent (anche tramite la loro prima parte). Richiede macOS 13 o versioni successive.

Estensioni di sistema

Le estensioni di sistema sono il modo moderno con cui le app estendono macOS: filtri di rete e VPN, agenti di sicurezza degli endpoint e driver. Con questa impostazione attiva, le estensioni di sistema dei team di sviluppatori elencati si caricano senza chiedere all'utente. Richiede macOS 10.15 o versioni successive e un MDM approvato dall'utente.

- **Team ID**: il team ID di 10 caratteri dello sviluppatore (ad esempio nei dettagli "Firmato da" dell'app o con `codesign -dv`). Ogni team può comparire una sola volta.
- **Consenti**: tutte le estensioni del team o solo le estensioni con i bundle ID elencati.
- **Tipi**: limita il team a driver, estensioni di rete o di sicurezza degli endpoint. Se non ne viene scelto nessuno, sono consentiti tutti i tipi.
- **Rimozione** (solo per le estensioni elencate): l'app può rimuovere la sua estensione senza un amministratore (macOS 12 e versioni successive), l'estensione non può essere disattivata o rimossa mentre la Protezione integrità sistema è attiva oppure non può essere rimossa in Impostazioni di Sistema e nel Finder (macOS 15 e versioni successive). I Mac con una versione precedente di macOS consentono comunque l'estensione, senza l'opzione di rimozione.
- **Gli utenti possono approvare altre estensioni di sistema**: attivato per impostazione predefinita. Quando è disattivato, possono caricarsi solo le estensioni consentite da un profilo; se un profilo sul Mac lo disattiva, è disattivato.

> Su macOS 11.3 e versioni successive, rimuovere questa impostazione disattiva le estensioni di sistema che consentiva, ad esempio un agente di sicurezza o un filtro di rete. Questo accade quando l'impostazione viene disattivata, quando la policy viene eliminata e quando il Mac passa a una policy che non la contiene. L'editor chiede conferma prima di disattivare l'impostazione.

Estensioni del kernel (legacy)

Le estensioni del kernel sono il modo più vecchio e deprecato di estendere macOS: preferisci le estensioni di sistema quando il fornitore le offre. Le estensioni del kernel dei team elencati (tutte le estensioni di un team o solo i bundle ID elencati) si caricano senza chiedere all'utente, dopo un riavvio. Richiede macOS 10.13.2 o versioni successive e un MDM approvato dall'utente.

- **Gli utenti possono approvare altre estensioni del kernel**: disattivato per impostazione predefinita, quindi solo i team elencati possono caricare estensioni del kernel.
- **Anche gli utenti standard possono approvarle**: con le approvazioni degli utenti attive, anche gli utenti senza diritti di amministratore possono approvarle (macOS 11 e versioni successive).

> Sui Mac con Apple silicon, un profilo da solo non basta: qualcuno deve avviare il Mac in recoveryOS, scegliere Sicurezza ridotta in Utility Sicurezza avvio e consentire la gestione utente delle estensioni del kernel da sviluppatori identificati. Il Mac può anche richiedere un Bootstrap Token depositato in Cerberus Enterprise per approvarle (vedi il campo Bootstrap Token della pagina del dispositivo).

File Mac

I file di configurazione dei servizi e le attività in background usano file che carichi nei **File Mac** della tua organizzazione: archivi zip e property list (.plist) fino a 20 MB. Caricali, controlla dove sono usati o eliminali con il pulsante **File Mac** della sezione macOS oppure con **Scegli file** in un'impostazione. Un file usato da una policy non può essere eliminato. Per modificare un file, carica la nuova versione e sceglila nella policy: i Mac la scaricano di nuovo.

File di configurazione dei servizi

Installa i file di configurazione di un servizio di sistema da un archivio zip. I servizi integrati sono il server SSH (sshd), sudo, PAM, la stampa (CUPS), il server web Apache, bash, zsh, l'accesso con smart card e l'autorizzazione. Puoi anche usare un tuo servizio, con un identificatore DNS inverso come `com.example.service`: trova i file con la libreria dei file di configurazione gestiti di macOS. Ogni servizio può avere un'impostazione. Richiede macOS 14 o versioni successive.

> Un servizio integrato usa solo i file dell'archivio e ignora i propri file, ad esempio /etc/ssh per sshd: inserisci l'intera configurazione nell'archivio, in cartelle che partono dalla radice del disco (ad esempio `etc/ssh/sshd_config`). I file sono di sola lettura sul Mac e vengono rimossi con l'impostazione. Prova prima l'archivio su un Mac: una configurazione sudo o PAM errata può impedire agli utenti di accedere o di usare i diritti di amministratore.

Attività in background

Programmi e script eseguiti in background, avviati da launchd. Gli utenti non possono disattivarli e vengono rimossi con l’impostazione. Richiede macOS 15 o versioni successive. Per ogni attività scegli:

- **Identificatore dell’attività**: un identificatore DNS inverso, come `com.example.task`, diverso per ogni attività.
- **Programmi e script** (facoltativo): un archivio zip che il Mac scompatta in `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/` seguito dall’identificatore dell’attività. Mantieni il permesso di esecuzione dei file e non inserirvi property list.
- **Property list di launchd**: i job che avviano i programmi, caricati come daemon (per l’intero sistema, come root) o come agent (in ogni sessione utente). Fai riferimento ai programmi con il loro percorso nella cartella precedente.

Un’attività richiede i programmi o almeno una property list. Quando i file cambiano, i Mac riavviano l’attività.

Posizione e geofence

La sezione **Posizione e geofence** dell'Apple Policy Editor definisce aree, ad esempio un sito o un magazzino. Gli iPhone e gli iPad con l'app Cerberus Enterprise segnalano quando entrano o escono da una di queste aree e le regole degli eventi possono reagire: inviare un'email, bloccare o disabilitare il dispositivo oppure abilitarlo di nuovo. I Mac non usano i geofence.

Campi geofence

Usa **Aggiungi geofence** per creare una nuova voce. Una policy può contenere fino a **10 geofence** e i loro nomi devono essere univoci all’interno della policy. Ogni geofence contiene questi campi:

- **Nome**: obbligatorio e univoco.
- **Latitudine** e **Longitudine**: il centro dell’area. Puoi anche fare clic sulla mappa per impostarlo.
- **Raggio (m)**: obbligatorio, da **200** a **10000** metri.
- **Descrizione**: note facoltative per gli amministratori.
- **Segnala ingresso** e **Segnala uscita**: scegli quali eventi vengono generati. Almeno uno deve restare attivo.
- **Attivo**: attiva o disattiva il geofence senza eliminarlo.

Ogni geofence ha un’anteprima della mappa. Il centro e il raggio di un geofence salvato sono bloccati: usa il pulsante di blocco sulla mappa per modificarli. Gli altri pulsanti centrano la mappa sull’area o sulla tua posizione attuale.

Quando salvi la policy, Cerberus Enterprise chiede agli iPhone e agli iPad della policy di ricevere i nuovi geofence. In genere servono alcuni minuti, ma iOS può ritardare l’operazione, ad esempio con il Risparmio energia attivo o senza connessione di rete. La pagina del dispositivo mostra quando l’app non ha ancora applicato i geofence più recenti.

Requisiti

I geofence funzionano su iPhone e iPad con l’app Cerberus Enterprise. I Mac li ignorano. Sul dispositivo:

- l’app Cerberus Enterprise è installata (la installa Cerberus) e l’utente l’ha aperta almeno una volta;

- l’accesso alla posizione per l’app è impostato su **Sempre**;
- **Posizione precisa** è attiva per l’app;
- **Aggiorna app in background** è attivo.

> **Posizione e geofence sui dispositivi personali**, in cima alla sezione, è disattivato per impostazione predefinita. Finché è disattivato, Cerberus non raccoglie la posizione dei dispositivi personali (registrazione utente), i loro eventi geofence non vengono generati e la loro pagina del dispositivo non offre Localizza o il tracciamento in tempo reale. Quando lo attivi, i dispositivi personali della policy condividono la loro posizione e i loro eventi geofence come i dispositivi aziendali, ma solo se l’utente consente la posizione per l’app Cerberus Enterprise; l’app lo spiega all’utente prima che iOS chieda. La tua organizzazione è responsabile di informare gli utenti e di rispettare le norme locali sulla posizione dei dipendenti. La modalità smarrito e la richiesta di posizione MDM non sono mai disponibili sui dispositivi personali (Apple non lo consente).

Con il **Risparmio energia** attivo i geofence continuano a funzionare, ma iOS segnala l’uscita da un’area più tardi e con una posizione meno precisa e può ritardare di ore la ricezione dei nuovi geofence dopo una modifica della policy, finché l’app non viene eseguita di nuovo (ad esempio al passaggio successivo o quando l’utente la apre).

Come arrivano gli eventi

iOS monitora le aree per l’app e la risveglia quando il dispositivo attraversa un confine, anche quando l’app non è aperta. Gli eventi possono arrivare alcuni minuti dopo l’attraversamento e un’area piccola o una visita breve possono essere perse: iOS richiede che il dispositivo si allontani dal confine per una certa distanza e rimanga lì per un po’.

Se l’app non può essere eseguita, ad esempio dopo un riavvio prima che il dispositivo venga sbloccato, anche il server rileva l’attraversamento, più tardi, dalle posizioni inviate dall’app. Ogni attraversamento attiva le regole di evento una volta, sia che lo rilevi l’app sia che lo rilevi il server.

Quando l’app non contatta il server per diverse ore, il server chiede a iOS di risvegliarla in modo che possa controllare di nuovo i suoi geofence. iOS non garantisce queste richieste.

Pagina del dispositivo

Nella pagina del dispositivo, la scheda **Geofence** del pannello **Mappa posizione** mostra le transizioni del dispositivo. Quando la policy ha geofence attivi, una riga di stato indica se il geofencing funziona sul dispositivo o perché non può funzionare: l’app non ha contattato il server o deve essere aggiornata, l’accesso alla posizione non è impostato su **Sempre**, oppure **Posizione precisa** o **Aggiorna app in background** sono disattivati, il **Risparmio energia** era attivo

quando l’app ha segnalato per l’ultima volta le sue impostazioni oppure l’app non ha ancora applicato i geofence più recenti.

> Le transizioni geofence e le posizioni vengono conservate per **90 giorni** e i dati più vecchi vengono eliminati automaticamente ogni notte. L'ultima posizione di ogni dispositivo registrato viene sempre conservata, così il dispositivo resta sulle mappe.

Limitazioni

- Copiare una policy non copia i suoi geofence: aggiungili di nuovo nella copia.
- Gli eventi geofence su iPhone e iPad non sono garantiti: iOS decide quando l’app può essere eseguita.

> Per reagire agli eventi geofence, crea una regola di evento per **Il dispositivo entra in un geofence** o **Il dispositivo esce da un geofence**. Vedi **Regole di evento**.

Account

La sezione **Account** dell'editor delle policy Apple aggiunge account di posta, Exchange, Google, calendario, contatti e directory a iPhone, iPad e Mac. Fai clic su **Aggiungi account** e scegli il tipo. La sezione contiene anche la restrizione **Consenti modifica account** (dispositivi supervisionati).

> Su un Mac (macOS 13 o versioni successive) gli account vengono installati nella sessione degli utenti registrati nella gestione, di solito l'utente che ha registrato il Mac, quando hanno effettuato l'accesso. La pagina del dispositivo elenca questi utenti in **Utenti Mac**, con lo stato dei loro account. Gli account che prendono l'indirizzo email dall'utente del dispositivo usano l'utente assegnato al Mac in Cerberus Enterprise.

Impostazioni comuni

- **Nome ed email dell'utente del dispositivo** (Mail, Exchange, Google): ogni dispositivo usa il nome e l'indirizzo email del suo utente, impostati nella pagina Utenti (per Google, l'account Google dell'utente). I dispositivi senza utente, o il cui utente non ha un indirizzo email, non ricevono l'account. Altrimenti, imposta un indirizzo email e un nome completo fissi.
- **Nome account** (facoltativo): il nome dell'account in Impostazioni e nelle app.
- **Nome utente** e **Password** (facoltativi): il nome utente può contenere le variabili $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$. Lascia vuota la password per consentire all'utente di digitarla sul dispositivo, oppure lascia vuoti entrambi per consentire all'utente di digitarli.
- **Si applica a**: limita l'account ad alcuni tipi di dispositivo.

Tipi di account

- **Account di posta**: server in entrata IMAP o POP e server in uscita, con le relative porte e autenticazione. Il server in uscita può usare lo stesso nome utente e la stessa password di quello in entrata.
- **Account Exchange** (Exchange ActiveSync): il server, oppure vuoto per ricavarlo dall'indirizzo email. Scegli i servizi (posta, contatti, calendari, promemoria, note) e se l'utente può modificarli. Con l'**autenticazione moderna (OAuth)** l'utente accede tramite la pagina del tuo provider di identità, ad esempio Microsoft 365. Un **certificato di autenticazione** (iOS 17 o versioni successive) autentica il dispositivo con un certificato.

- **Account Google**: l'utente accede all'account Google con l'indirizzo email indicato.
- **Account calendario (CalDAV)** e **Account contatti (CardDAV)**: il server, la porta e il percorso.
- **Directory (LDAP)**: il server e la porta, e le ricerche (base di ricerca, ambito e descrizione) usate per cercare i contatti.
- **Calendario sottoscritto**: l'URL del calendario (https, http o webcal).

S/MIME

Gli account di posta ed Exchange possono firmare e crittografare i messaggi con S/MIME (iOS 17 o versioni successive). Per ciascuno, scegli il certificato: uno della pagina Certificati, il certificato dell'utente del dispositivo oppure richiesto a un server SCEP. Puoi consentire all'utente di disattivarlo, scegliere un altro certificato e, per la crittografia, mostrare un interruttore per ogni messaggio.

Sicurezza

Le password e i certificati non fanno parte delle impostazioni inviate ai dispositivi: ogni dispositivo scarica le proprie credenziali da Cerberus Enterprise, firmando la richiesta con il proprio certificato di gestione. Non vengono scritti nei log.

Regole di conformità

La sezione **Regole di conformità** dell'Editor delle policy Apple stabilisce i requisiti per i dispositivi della policy. Un dispositivo che infrange una regola è subito non conforme: la pagina del dispositivo ne mostra il motivo in **Perché il dispositivo non è conforme** e l'elenco dei dispositivi lo mostra come non conforme. Un dispositivo è inoltre non conforme quando un'impostazione della policy non può essere applicata su di esso.

Regole

- **Codice di accesso**: il dispositivo ha un codice di accesso e rispetta le impostazioni del codice di accesso della policy.
- **Versione minima del sistema operativo**: per iPhone e iPad o per Mac. Per aggiornare i dispositivi, aggiungi un aggiornamento obbligatorio in Aggiornamenti software.
- **Dispositivo supervisionato**: i dispositivi registrati con il profilo di registrazione o con la registrazione utente non sono supervisionati.
- **FileVault attivo (Mac)**: il disco del Mac è cifrato con FileVault. Gli altri dispositivi non sono interessati.

Una regola viene controllata quando il dispositivo invia il suo stato, quando la policy viene salvata e ogni ora. Un dispositivo il cui stato è sconosciuto (ad esempio un Mac che non ha ancora segnalato FileVault) non infrange la regola.

Blocco del dispositivo

Attiva **Blocca il dispositivo se è ancora non conforme** e imposta dopo quanti giorni (0 blocca subito). Gli iPhone e gli iPad supervisionati entrano in modalità smarrito con il messaggio che hai impostato. Gli altri dispositivi vengono bloccati una volta; un Mac si riavvia e chiede un PIN, mostrato nei dettagli del comando nella cronologia dei comandi.

- **Sblocca**: quando il dispositivo torna conforme, la modalità smarrito viene disattivata automaticamente.
- **Disattivare tu stesso la modalità smarrito**: il dispositivo non viene bloccato di nuovo finché non torna conforme e infrange di nuovo una regola. Usalo per consentire all'utente di sistemare il dispositivo.

> Per ricevere una notifica o reagire in altri modi, crea una regola di evento per **Il dispositivo diventa non conforme**: riceve anche i motivi.