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.

Revision #7
Created 2026-11-10 15:12:52 UTC by Admin
Updated 2026-11-12 09:52:36 UTC by Admin