SOPHOS

Cybersecurity made simple.

Sophos Mobile

guida di avvio (SaaS)

Versione prodotto: 9.5

Sommario

1 Contenuti di questo documento

Questo documento descrive tutte le fasi dell'impostazione di Sophos Mobile come sistema di gestione dei dispositivi.

Le descrizioni sono applicabili a Sophos Mobile as-a-Service.

Per altre versioni di questo documento, consultare la pagina web della documentazione di Sophos Mobile.

2 Passaggi chiave

Per cominciare ad utilizzare Sophos Mobile:

1. Reimpostare la password, accedere a Sophos Mobile Admin e cambiare il nome utente dell'amministratore.
2. Richiesto: Attivare le licenze Mobile Advanced per gestire Sophos Intercept X for Mobile, Sophos Secure Workspace e Sophos Secure Email.
3. Verificare i dati relativi alla licenza.
4. Configurare le impostazioni personali, i criteri per la password da applicare agli account amministratore, i dati di contatto del supporto tecnico, e le impostazioni per il portale self-service.
5. Caricare un certificato per l’Apple Push Notification service che consenta di gestire iPhone, iPad e Mac.
6. Richiesto: Impostare un proxy di EAS standalone per filtrare il traffico e-mail proveniente dai dispositivi gestiti e dirigerlo verso un server di posta elettronica.
7. Richiesto: Configurare l’interfaccia per sistemi di Network Access Control di terzi.
8. Creare criteri di conformità.
9. Creare gruppi di dispositivi.
10. Configurare i dispositivi.
11. Aggiornare le impostazioni del portale self-service.
12. Configurare la gestione degli utenti
13. Se si utilizza la gestione degli utenti interni: Aggiungere utenti sia creandoli che caricando elenchi di utenti.
14. Se si utilizza la gestione degli utenti esterni: Configurare la connessione alla directory di LDAP.
15. Effettuare un test della registrazione nel portale self-service.

3 Modifica della password

Per questioni di sicurezza, si consiglia di reimpostare la password prima di effettuare l'accesso a Sophos Mobile Admin per la prima volta.

1. Aprire Sophos Mobile Admin nel browser web.
2. Nella finestra di dialogo di **Accesso**, cliccare su **Password dimenticata?**.
3. Nella finestra di dialogo **Reimposta password**, inserire le informazioni relative a **Cliente** e **Utente** reperibili nell'e-mail ricevuta per l'attivazione dell'account di Sophos Mobile as a Service, quindi cliccare su **Reimposta password**.
   Una volta portata a termine questa procedura, riceverà un'e-mail contenente un link che le consentirà di reimpostare la password.
4. Cliccare sul link per aprire la finestra di dialogo **Cambia password**.
5. Inserire la nuova password, e cliccare su **Cambia password**.

   La password è stata modificata. Ricordarsi di utilizzare questa password al prossimo accesso alla console.

Nota
Si consiglia di modificare i criteri della password per implementare password più sicure, ad esempio richiedendo un numero minimo di caratteri minuscoli, maiuscoli o speciali. Vedere Configurazione dei criteri delle password (pagina 8).

4 Modifica del nome di accesso

Per motivi di sicurezza, si consiglia di cambiare il nome di accesso dopo aver effettuato il primo accesso a Sophos Mobile Admin.

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **ImpostazioneAmministratori**.
2. Cliccare sul nome di accesso.
3. Nella pagina **Modifica amministratore**, inserire un valore diverso nel campo **Nome di accesso**.
4. Richiesto: Modificare i valori degli altri campi:
   - **Nome**
   - **Cognome**
   - **Indirizzo e-mail**
5. Selezionare **Salva**.

I dettagli dell'account sono stati modificati. Ricordarsi di utilizzare il nuovo nome di accesso al prossimo accesso a Sophos Mobile Admin.

5 Attivazione di licenze Mobile Advanced

Le licenze Mobile Advanced consentono di utilizzare Sophos Mobile per gestire Sophos Intercept X for Mobile,Sophos Secure Workspace e Sophos Secure Email.

Le licenze Mobile Advanced vengono attivate in Sophos Mobile Admin:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Licenze**.
2. Immettere la chiave di licenza nel campo **Chiave di licenza Advanced** e cliccare su **Attiva**.

Una volta attivata la chiave, verranno visualizzati i dettagli della licenza.

6 Verifica delle licenze

Sophos Mobile utilizza un sistema di licenze basato sul numero di utenti. Una sola licenza è valida per tutti i dispositivi assegnati a un utente. I dispositivi non assegnati ad alcun utente richiedono invece una licenza ciascuno.

Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Licenze**.

Verranno visualizzate le seguenti informazioni:

- **Numero massimo di licenze**: Il numero massimo di utenti dei dispositivi (e dispositivi non assegnati) che è possibile gestire.
- **Licenze utilizzate**: Numero di licenze in uso.
- **Valido entro**: La data di scadenza della licenza.

Nel caso di domande o dubbi sulle informazioni relative alla licenza che sono visualizzate, contattare il proprio rappresentante commerciale Sophos.

7 Configurazione delle impostazioni

Configurare le seguenti impostazioni:

- Impostazioni personali, per esempio le piattaforme che si desidera gestire
- Criteri password
- Dati di contatto del supporto tecnico
- Impostazioni del portale self-service

7.1 Configurazione delle impostazioni personali

L'aspetto di Sophos Mobile Admin può essere modificato a seconda dei propri gusti personali. È ad esempio possibile impostare lingua, fuso orario o le piattaforme dei dispositivi che sono visibili.

Nota
Queste impostazioni riguardano solamente l'account di amministrazione con cui è stato effettuato l'accesso.

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale** e successivamente sulla scheda **Personale**.
2. Configurare le seguenti impostazioni:

Opzione	Descrizione
Lingua	La lingua dell'interfaccia utente.
Fuso orario	Il fuso orario secondo il quale vengono visualizzate le date.
Unità di misura	Il sistema di unità di misura per i valori di lunghezza (**Metrico** or **Imperiale**).
Righe per pagina nelle tabelle	Il numero massimo di voci visualizzate per ciascuna pagina della tabella.
Modalità avanzata	Questa impostazione attiva ulteriori funzionalità: • La pagina **Mostra dispositivo** include la scheda **Proprietà personalizzate** con le proprietà personalizzate del dispositivo. • La pagina **Mostra dispositivo** include la scheda **Proprietà interne** con le proprietà aggiuntive segnalate dal dispositivo. • Diverse pagine di configurazione dei criteri includono la sezione **Impostazioni aggiuntive** per la configurazione di impostazioni opzionali.
Piattaforme attive	Le piattaforma del dispositivo che si desidera visualizzare.

Opzione	Descrizione
	In Sophos Mobile Admin, vengono visualizzate solamente le pagine e le impostazioni che riguardano le piattaforme selezionate.

3. Selezionare **Salva**.

7.2 Configurazione dei criteri delle password

Per implementare la protezione delle password, configurare criteri delle password per gli utenti di Sophos Mobile Admin e del Portale self-service.

Nota
I criteri delle password non sono applicabili agli utenti provenienti da una directory LDAP esterna.

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale** e successivamente sulla scheda **Criteri password**.
2. Sotto **Regole**, è possibile definire requisiti per le password, come ad es. la quantità minima di caratteri maiuscoli, minuscoli o numerici che una password deve contenere per essere considerata valida.
3. Sotto **Impostazioni**, configurare le seguenti impostazioni:
   a) **Intervallo di modifica password (giorni)**: Inserire il numero di giorni dopo il quale una password verrà ritenuta scaduta (tra `1` e `730`), oppure lasciare il campo vuoto per disattivare la scadenza della password.
   b) **Numero di password precedenti da non riutilizzare**: Selezionare un valore compreso tra `1` e `10`, oppure selezionare `---` per disattivare questa restrizione.
   c) **Numero massimo di tentativi di accesso non riusciti**: Selezionare il numero di tentativi di accesso non riusciti dopo il quale l'account debba essere bloccato (cifra compresa tra `1` e `10`), oppure selezionare `---` per consentire una quantità illimitata di tentativi di accesso non riusciti.
4. Selezionare **Salva**.

7.3 Configurazione del contatto del supporto tecnico

Si consiglia di specificare i dati di contatto del supporto tecnico, in modo da permettere agli utenti di ricevere assistenza per eventuali domande o problemi.

Le informazioni immesse in questo campo vengono visualizzate nel portale self-service e sui dispositivi degli utenti.

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale** e successivamente sulla scheda **Contatto IT**.
2. Immettere le informazioni di contatto.
3. Selezionare **Salva**.

8 Impostazione della modalità di gestione di Android

Per i dispositivi Android, è possibile scegliere tra le modalità di gestione **Android Enterprise** e **Amministratore dispositivo (funzionalità legacy)**.

Si consiglia di utilizzare Android Enterprise.

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, selezionare **Impostazione > Impostazione Android** e successivamente la scheda **Android**.
2. In **Modalità di gestione**, selezionare **Android Enterprise**.
3. Selezionare **Salva**.

Successivamente, impostare Android Enterprise per l'organizzazione.

8.1 Impostazione di Android Enterprise - Panoramica

Per impostare Android Enterprise per l'organizzazione, è possibile scegliere tra scenari diversi. Lo scenario Account Google Play gestito è il metodo più semplice per impostare Android Enterprise ed è quello descritto in questo documento.

Per informazioni dettagliate sugli altri scenari di Android Enterprise, consultare la Guida per amministratori di Sophos Mobile.

Informazioni correlate

Guida in linea per amministratori di Sophos Mobile

8.2 Impostazione di Android Enterprise (scenario con account Google Play gestito)

Sophos Mobile offre assistenza in tutti i passaggi della procedura di impostazione di Android Enterprise per la propria organizzazione.

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, selezionare **Impostazione > Impostazione Android** e successivamente la scheda **Android Enterprise**.
2. Selezionare **Configura**.
3. Selezionare **Lo scenario “Account Google Play gestito”** e successivamente **Avanti**.
4. Selezionare **Registra account**.

   Con questa azione si verrà reindirizzati su un sito web di Google, dove sarà possibile effettuare la registrazione della propria organizzazione ad Android Enterprise.
5. Accedere al sito web di Google con il proprio account Google.

Nota
Si consiglia di creare un nuovo account Google, riservato esclusivamente a tale scopo.

6. Nel sito web di Google, seguire i passaggi indicati, per completare il processo di registrazione della propria organizzazione.

   Consiglio
   Quando si specifica il nome dell'organizzazione, si consiglia di includere la dicitura `Sophos Mobile`. Per esempio:

   ```
   Nome organizzazione (Sophos Mobile)
   ```

   Una volta completati i passaggi di registrazione, si sarà nuovamente reindirizzati dal sito web di Google a Sophos Mobile.
7. In Sophos Mobile, selezionare **Finalizza impostazione** per completare il processo di registrazione.

Nota
Una volta impostata Android Enterprise, non sarà possibile modificare la modalità di gestione degli utenti. Ad esempio, non sarà possibile passare dalla gestione interna degli utenti a una directory LDAP esterna.

9 Certificati Apple Push Notification service

Per utilizzare il protocollo Mobile Device Management (MDM) incorporato nei dispositivi iOSe macOS, Sophos Mobile deve utilizzare il servizio Apple Push Notification (APNs) per l'attivazione dei dispositivi.

I certificati APNs sono validi per un anno.

9.1 Creazione di un certificato APNs

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Apple** e successivamente sulla scheda **APNs**.
2. Cliccare su **Procedura guidata per il certificato APNs**.
3. Nella pagina **Modalità**, cliccare su **Crea un nuovo certificato APNs**.
4. Nella pagina **CSR**, cliccare su **Scaricare la richiesta di firma del certificato**.

   Questa operazione salva il file di richiesta di firma del certificato `apple.csr` sul computer locale.
5. Occorre un ID Apple. Anche se si è già in possesso di un ID, si consiglia di crearne uno nuovo da utilizzare esclusivamente per Sophos Mobile. Nella pagina **ID Apple**, cliccare su **Crea l'ID Apple nel portale di Apple**.

   Si aprirà una pagina web di Apple nella quale sarà possibile creare un ID Apple per l’azienda.

   Nota
   Conservare le credenziali in un posto sicuro, a cui i colleghi possano accedere. L’azienda avrà bisogno di queste credenziali ogni anno, per rinnovare il certificato.

6. Nella procedura guidata, immettere il nuovo ID Apple nel campo **ID Apple**.
7. Nella pagina **Certificato**, cliccare su **Crea certificato nel portale di Apple**.

   Verrà aperto l’Apple Push Certificates Portal.
8. Accedere con il proprio ID Apple e caricare il file di richiesta di firma del certificato `apple.csr`.
9. Scaricare il file `.pem` del certificato APNs e salvarlo nel computer.
10. Nella pagina **Carica**, cliccare su **Carica certificato** e cercare il file `.pem` ricevuto dall’Apple Push Certificates Portal.
11. Selezionare **Salva**.

Sophos Mobile leggerà il certificato e visualizzerà i dettagli del certificato nella scheda **APNs**.

10 Proxy EAS standalone

È possibile impostare un proxy di EAS per controllare l'accesso dei dispositivi gestiti a un server di posta. Il traffico e-mail dei dispositivi gestiti verrà reindirizzato attraverso il proxy specificato. È possibile bloccare l'accesso alle e-mail per i dispositivi, ad esempio nel caso in cui sia presente un dispositivo che viola una regola di conformità.

I dispositivi devono essere configurati in modo da utilizzare il proxy di EAS come server di posta elettronica per le e-mail in entrata e in uscita. Il proxy EAS inoltrerà il traffico al server di posta elettronica solamente se il dispositivo è noto a Sophos Mobile, e se soddisfa i criteri richiesti. Ciò garantisce un livello di sicurezza più elevato, in quanto non occorre che il server di posta sia accessibile da Internet, e può essere raggiunto solamente dai dispositivi autorizzati (configurati correttamente, ad es. seguendo linee guida per il passcode). Inoltre, è anche possibile configurare il proxy di EAS in modo che impedisca l'accesso da dispositivi specifici.

Il proxy di EAS deve essere scaricato e installato separatamente da Sophos Mobile. Comunica con il server di Sophos Mobile attraverso un'interfaccia web HTTPS.

Nota
Poiché macOS non supporta il protocollo ActiveSync, non è possibile utilizzare il proxy di EAS per filtrare il traffico e-mail proveniente dai Mac.

Funzionalità

- Supporto di server di posta elettronica Microsoft Exchange o IBM Notes Traveler multipli. È possibile impostare un'istanza di proxy di EAS per ciascun server di posta.
- Supporto di bilanciatori del carico. È possibile impostare istanze di proxy di EAS standalone su computer diversi, per poi utilizzare un bilanciatore del carico per distribuire tra di esse le richieste del client.
- Supporto dell'autenticazione al client basata su certificato. È possibile selezionare, da un'autorità di certificazione (CA), un certificato dal quale devono essere derivati i certificati client.
- Supporto del controllo dell'accesso alle e-mail tramite PowerShell. In questo scenario, il servizio proxy EAS comunica con il server di posta tramite PowerShell per controllare l'accesso alle e-mail dei dispositivi gestiti. Il traffico e-mail si verifica direttamente tra i dispositivi e i server di posta, senza essere reindirizzato tramite un proxy. Vedere Impostazione del controllo dell'accesso alle e-mail tramite PowerShell (pagina 16).
- Il proxy EAS ricorderà lo stato del dispositivo per 24 ore. Se il server di Sophos Mobile dovesse essere off-line, ad esempio in caso di aggiornamento, il traffico e-mail verrà filtrato in base all'ultimo stato conosciuto del dispositivo. Dopo 24 ore, l'intero traffico e-mail verrà bloccato.

Nota
Per i dispositivi non iOS, le capacità di filtraggio del proxy EAS standalone sono limitate per via delle specifiche del protocollo di IBM Notes Traveler. Sui dispositivi non iOS, i client di Traveler non inviano l'ID del dispositivo con tutte le richieste. Le richieste senza un ID del dispositivo verranno comunque inoltrate al server di Traveler, anche se il proxy EAS non dovesse essere in grado di verificare che il dispositivo è autorizzato.

10.1 Download del programma di installazione del proxy di EAS

1. Accedere a Sophos Mobile Admin.
2. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Proxy EAS**.
3. Sotto **Esterno**, cliccare sul link per scaricare il programma di installazione del proxy di EAS.

Il file di installazione verrà salvato nel computer locale.

10.2 Installazione del proxy EAS standalone

Prerequisiti:

- Tutti i server di posta richiesti devono essere accessibili. Il programma di installazione del proxy EAS non configurerà le connessioni ai server che non sono disponibili.
- Occorre aver effettuato l'accesso come amministratore sul computer in cui si intende installare il proxy EAS.
- Conoscere l'URL del server di Sophos Mobile. Vedere Determinazione dell'URL del server di Sophos Mobile (pagina 19).

Nota
La Guida alla distribuzione di Server di Sophos Mobile (in inglese) contiene diagrammi schematici per l'integrazione del proxy di EAS standalone nell'infrastruttura aziendale. Si consiglia di leggere le informazioni prima di procedere con l'installazione e la distribuzione del proxy di EAS standalone.

1. Eseguire `Sophos Mobile EAS Proxy Setup.exe` per avviare **Sophos Mobile EAS Proxy - Setup Wizard**.
2. Nella pagina **Choose Install Location**, selezionare la cartella di destinazione e cliccare su **Install** per avviare l'installazione.
   Una volta completata l'installazione, viene avviato automaticamente **Sophos Mobile EAS Proxy - Configuration Wizard**, che fornisce una guida passo dopo passo per l'intera procedura di configurazione.
3. Nella finestra di dialogo **Sophos Mobile server configuration**, immettere l'URL del server di Sophos Mobile a cui il proxy di EAS effettuerà la connessione.

   Si consiglia di selezionare anche **Use SSL for incoming connections (Clients to EAS Proxy)** per proteggere la comunicazione tra i client e il proxy di EAS.

   Opzionalmente, selezionare **Use client certificates for authentication** se si desidera che, per l'autenticazione, i client adoperino anche un certificato, oltre alle credenziali del proxy di EAS. Così facendo si aggiunge un ulteriore livello di sicurezza alla connessione.
4. Se in precedenza è stata selezionata l'opzione **Use SSL for incoming connections (Clients to EAS Proxy)**, verrà visualizzata la pagina **Configure server certificate**. In questa pagina è possibile creare o importare un certificato per l'accesso sicuro (HTTPS) al proxy EAS.

Nota
La procedura guidata "SSL Certificate Wizard" può essere scaricata da MySophos e utilizzata per richiedere il certificato SSL/TLS per il proxy di EAS di Sophos Mobile.

Per informazioni generali sul download dei software Sophos, consultare l'articolo 111195 della knowledge base Sophos.

- Se ancora non si dispone di un certificato attendibile, selezionare **Create self-signed certificate**.
- Se si dispone di un certificato attendibile, cliccare su **Import a certificate from a trusted issuer** e selezionare una delle seguenti operazioni dall'elenco:
  - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
  - **Separate files for certificate, private key, intermediate and CA certificate**

5. Nella pagina successiva, inserire le informazioni del certificato che riguardano il certificato selezionato.

Nota
Nel caso di un certificato autofirmato, occorrerà specificare un server che sia accessibile dai dispositivi client.

6. Se in precedenza è stata selezionata l'opzione **Use client certificates for authentication**, verrà visualizzata la pagina **SMC client authentication configuration**. Su questa pagina è possibile selezionare, da un'autorità di certificazione (CA), un certificato dal quale devono essere derivati i certificati client.

   Quando un client cercherà di effettuare la connessione, il proxy di EAS verificherà se il certificato sia derivato dalla CA specificata in questo campo.
7. Nella pagina **EAS Proxy instance setup**, configurare una o più istanze del proxy di EAS.
   - **Instance type**: Selezionare **EAS proxy**.
   - **Instance name**: Un nome che identifica l'istanza.
   - **Server port**: La porta del proxy EAS per il traffico e-mail in entrata. Se viene impostata più di un'unica istanza di proxy, ciascuna di esse dovrà utilizzare una porta diversa.
   - **Require client certificate authentication**: I client di posta devono autentificarsi quando si connettono al proxy EAS.
   - **ActiveSync server**: Il nome o indirizzo IP dell'istanza del server di Exchange ActiveSync a cui si connetterà l'istanza del proxy.
   - **SSL**: La comunicazione tra l'istanza del proxy e il server di Exchange ActiveSync è protetta tramite SSL o TLS (a seconda della compatibilità del server).
   - **Allow EWS subscription requests from Secure Email**: Selezionare questa opzione per consentire alla app Sophos Secure Email su iOS di effettuare la sottoscrizione alle notifiche push tramite Exchange Web Services (EWS). Le notifiche push informano il dispositivo quando sono presenti messaggi per Secure Email.

Nota

— Per impostazione predefinita, il proxy di EAS blocca tutte le richieste rivolte all'interfaccia EWS del server di Exchange; ciò è per questioni di sicurezza. Selezionando questa casella di controllo, verranno autorizzate le richieste di sottoscrizione. Le altre richieste rimarranno bloccate.

— Per informazioni su come configurare EWS per il server di Exchange, consultare l'articolo 127137 della knowledge base Sophos.

- **Enable Traveler client access**: Selezionare questa casella di controllo solamente se si desidera autorizzare l'accesso ai client di IBM Notes Traveler da dispositivi non iOS.

8. Dopo aver inserito le informazioni relative all'istanza, cliccare su **Add** per aggiungere l'istanza all'elenco **Instances**.

   Per ciascuna istanza di proxy, il programma di installazione creerà un certificato che dovrà essere caricato sul server di Sophos Mobile. Una volta cliccato su **Add**, comparirà una finestra di messaggio che descriverà come procedere per caricare il certificato.
9. Nella finestra di messaggio, cliccare su **OK**.
   Si aprirà una finestra di dialogo che mostra la cartella nella quale è stato creato il certificato.

Nota

È anche possibile aprire la finestra di dialogo selezionando l'istanza desiderata e cliccando sul link **Export config and upload to Sophos Mobile server** nella pagina **EAS Proxy instance setup**.

10. Prendere nota della cartella del certificato. Questa informazione verrà richiesta in seguito, al momento di caricare il certificato su Sophos Mobile.
11. Richiesto: Cliccare nuovamente su **Add** per configurare ulteriori istanze del proxy EAS.
12. Una volta configurate tutte le istanze del proxy EAS richieste, cliccare su **Next**.
    Si procederà quindi al test delle porte server che sono state inserite, e verranno configurate le regole in entrata per Windows Firewall.
13. La pagina **Allowed mail user agents** consente di specificare i Mail User Agent (ovvero le applicazioni client di posta elettronica) che sono autorizzati a connettersi al proxy EAS. Quando un client si connette al proxy di EAS utilizzando un'applicazione di posta non specificata, la richiesta viene respinta.

    - Selezionare **Allow all mail user agents** per configurare l'assenza di restrizioni.
    - Selezionare **Only allow the specified mail user agents** e successivamente selezionare un utente e-mail dall'elenco. Cliccare su **Add** per aggiungere la voce all'elenco di agenti autorizzati. Ripetere questa procedura per tutti i Mail User Agent a cui è consentito connettersi al proxy EAS.
14. Nella pagina **Sophos Mobile EAS Proxy - Configuration Wizard finished**, cliccare su **Finish** per chiudere la procedura guidata di configurazione e tornare alla procedura guidata di impostazione.
15. Nella procedura guidata di impostazione, verificare che sia selezionata la casella **Start Sophos Mobile EAS Proxy server now**, e successivamente cliccare su **Finish** per completare la configurazione e avviare il proxy di EAS di Sophos Mobile per la prima volta.

Per completare la configurazione del proxy di EAS, caricare su Sophos Mobile i certificati creati per ciascuna istanza del proxy:

16. Accedere a Sophos Mobile Admin.
17. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Proxy EAS**.

18. Sotto **Esterno**, cliccare su **Carica file**. Caricare il certificato creato dalla procedura guidata di configurazione.

    Se è stata impostata più di un'istanza, ripetere questa procedura per i certificati di tutte le istanze.
19. Selezionare **Salva**.
20. In Windows, aprire la finestra di dialogo **Servizi** e riavviare il servizio **EASProxy**.

Si conclude così l'impostazione iniziale del proxy EAS standalone.

Nota
Ogni giorno, le voci di log del proxy EAS vengono trasferite su un nuovo file, utilizzando il pattern `EASProxy.log.aaaa-mm-gg` per il nome. Questi file di log quotidiano non vengono eliminati automaticamente, per cui col passare del tempo possono causare problemi di spazio disponibile su disco. Si consiglia di impostare un processo che trasferisca i file di log su un percorso di backup.

10.3 Impostazione del controllo dell'accesso alle e-mail tramite PowerShell

È possibile impostare una connessione PowerShell a un server di Exchange oppure Office 365. In questo modo, il servizio proxy EAS comunicherà con il server di posta tramite PowerShell per controllare l'accesso alle e-mail dei dispositivi gestiti. Il traffico e-mail verrà inviato direttamente dai dispositivi al server di posta. Non sarà reindirizzato tramite proxy.

Nota
Poiché macOS non supporta il protocollo ActiveSync, non è possibile utilizzare PowerShell per controllare l'accesso alle e-mail dai Mac.

Lo scenario che prevede l'uso di PowerShell presenta i seguenti vantaggi:

- I dispositivi comunicano direttamente con il server di Exchange.
- Non occorre aprire sul server una porta dedicata al traffico e-mail in entrata proveniente dai dispositivi gestiti.

I server di posta supportati sono:

- Exchange Server 2013
- Exchange Server 2016
- Office 365 con piano Exchange Online

Per il setup di PowerShell:

1. Configurare PowerShell.
2. Creare un account di servizio sul server di Exchange o in Office 365. Questo account verrà utilizzato da Sophos Mobile per eseguire comandi PowerShell.
3. Impostare una o più istanze di connessione PowerShell a Exchange oppure Office 365.
4. Caricare i certificati delle istanze su Sophos Mobile.

Configurazione di PowerShell

1. Nel computer sul quale verrà installato il proxy EAS, aprire Windows PowerShell come amministratore e inserire:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Nota
Se PowerShell non fosse disponibile, effettuarne l'installazione come indicato nell'articolo Installazione di Windows PowerShell (link esterno) di Microsoft.

2. Se si desidera effettuare la connessione a un server di Exchange locale, aprire Windows PowerShell come amministratore sul computer interessato e inserire lo stesso comando indicato in precedenza:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Nota
Questo passaggio non è richiesto per Office 365.

Creazione di un account di servizio

3. Accedere alla console di amministrazione richiesta:
   - Per Exchange Server 2013/2016: **Interfaccia di amministrazione di Exchange**
   - Per Office 365: **Interfaccia di amministrazione di Office 365**
4. Creare un account utente. Questo account verrà utilizzato da Sophos Mobile come account di servizio, per eseguire comandi PowerShell.
   - Adoperare un nome utente, come ad es. `smc_powershell`, che identifichi lo scopo dell'account.
   - Disattivare l'impostazione che prevede la modifica della password da parte dell'utente all'accesso successivo.
   - Rimuovere eventuali licenze Office 365 automaticamente assegnate al nuovo account. Gli account di servizio non richiedono alcuna licenza.
5. Creare un nuovo gruppo di ruoli e assegnarvi le autorizzazioni richieste.
   - Adoperare un nome per il gruppo di ruoli quale ad es. `smc_powershell`.
   - Aggiungere i ruoli **Mail Recipients** e **Organization Client Access**.
   - Aggiungere l'account di servizio come membro.

Impostazione delle connessioni PowerShell

6. Utilizzare la procedura guidata come se si desiderasse impostare un proxy di EAS standalone. Nella pagina della procedura intitolata **EAS Proxy instance setup**, configurare queste due impostazioni:
   - **Instance type**: Selezionare **PowerShell Exchange/Office 365**.
   - **Instance name**: Un nome che identifica l'istanza.
   - **Exchange server**: Il nome o indirizzo IP del server di Exchange (per un'installazione locale del server di Exchange), oppure `outlook.office365.com` (per Office 365). Non includere un prefisso `https://` o un suffisso `/powershell`. Verranno aggiunti automaticamente.
   - **Allow all certificates**: Il certificato presentato dal server di Exchange non sarà verificato. Utilizzare questa opzione se ad esempio nel server di Exchange è installato un certificato autofirmato. Poiché l'opzione **Allow all certificates** diminuisce il livello di sicurezza della

comunicazione del server, si consiglia vivamente di selezionarla solamente se richiesta dall'ambiente di rete.

- **Service account**: Il nome dell'account utente creato nella console di amministrazione di Exchange oppure Office 365.
- **Password**: La password dell'account utente.

7. Cliccare su **Add** per aggiungere l'istanza all'elenco **Instances**.
8. Ripetere i passaggi di cui sopra per impostare connessioni PowerShell ad altri server di Exchange oppure Office 365.
9. Completare la procedura guidata di installazione come descritto in Installazione del proxy EAS standalone (pagina 13).

Caricamento di certificati

10. Accedere a Sophos Mobile Admin.
11. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Proxy EAS**.
12. Richiesto: In **Generale**, selezionare **Limita a Sophos Secure Email** per limitare l'accesso alle e-mail all'app Sophos Secure Email, disponibile per Android e iOS.

    Questa azione impedisce ad altre app di posta elettronica di connettersi al server di posta.
13. Sotto **Esterno**, cliccare su **Carica file**. Caricare il certificato creato dalla procedura guidata di configurazione.

    Se è stata impostata più di un'istanza, ripetere questa procedura per i certificati di tutte le istanze.
14. Selezionare **Salva**.
15. In Windows, aprire la finestra di dialogo **Servizi** e riavviare il servizio **EASProxy**.

Si conclude così il setup iniziale delle connessioni PowerShell. Il traffico e-mail tra un dispositivo gestito e i server di Exchange oppure Office 365 verrà bloccato se il dispositivo viola una delle regole di conformità. È possibile bloccare un singolo dispositivo impostando su **Nega** la modalità di accesso alle e-mail del dispositivo in questione.

Nota
A seconda della configurazione del server di Exchange, i dispositivi riceveranno una notifica dopo il blocco dell'accesso alle e-mail.

10.4 Configurazione di una connessione al server proxy EAS standalone

Per configurare la connessione tra Sophos Mobile e il proxy EAS standalone, occorre caricare il certificato del server proxy di EAS su Sophos Mobile. Questo certificato è stato generato durante la configurazione dell'istanza del proxy EAS.

Importante
Se il servizio proxy EAS viene avviato prima di aver caricato il certificato, Sophos Mobile rifiuterà la connessione al server, e il servizio non si avvierà.

Per caricare il certificato del proxy EAS standalone:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Proxy EAS**.

2. Richiesto: In **Generale**, selezionare **Limita a Sophos Secure Email** per limitare l'accesso alle e-mail all'app Sophos Secure Email, disponibile per Android e iOS.

   Questa azione impedisce ad altre app di posta elettronica di connettersi al server di posta.
3. In **Esterno**, cliccare su **Carica file** e cercare il file del certificato.

   Se è stata impostata più di un'istanza del proxy EAS, ripetere questa procedura per tutte le istanze.
4. Selezionare **Salva**.
5. In Windows, aprire la finestra di dialogo **Servizi** e riavviare il servizio **EASProxy**.

10.5 Determinazione dell'URL del server di Sophos Mobile

L'URL del server di Sophos Mobile serve a configurare il proxy di EAS standalone. Il valore viene visualizzato nelle impostazioni di sistema di Sophos Mobile.

1. Accedere a Sophos Mobile Admin.
2. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Proxy EAS**.

Sotto **Esterno** viene visualizzato l'URL del server di Sophos Mobile.

11 Configurazione di Network Access Control (controllo dell’accesso alla rete)

Sophos Mobile include un'interfaccia per i sistemi di Network Access Control (NAC) di altri vendor. Configurando le connessioni ai sistemi di NAC, se ne concede il permesso di ottenere un elenco di dispositivi e dei relativi stati di conformità. Inoltre, configurando Network Access Control come descritto in questa sezione, è possibile definire in un secondo momento un criterio di conformità che vieti l'accesso alla rete agli utenti che violano regole di conformità specifiche.

Per informazioni su come definire i criteri di conformità, consultare la Guida per amministratori di Sophos Mobile.

Per configurare Network Access Control:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Network Access Control**.
2. Selezionare una delle opzioni di integrazione di NAC disponibili nell’elenco:

   - **Sophos UTM**

     Questa opzione abilita l'integrazione di Sophos UTM (versione 9.2 e superiore). Per l'integrazione occorre impostare l'URL del server di SMC e le credenziali dell'utente amministratore nell'interfaccia WebAdmin di Sophos UTM, sotto **Gestione > Sophos Mobile**. Per informazioni dettagliate, consultare la *Guida all'amministrazione di Sophos UTM*.

   - **Cisco ISE**

     Questa opzione abilita l’integrazione di Cisco ISE. Configurare le seguenti impostazioni:

Nome utente	Il nome utente che deve essere specificato in Cisco ISE. Verrà usato da Cisco ISE per accedere a Sophos Mobile.
Password	Inserire una password per effettuare l'accesso a Sophos Mobile.
Conferma password	Ripetere la password.
Pagina di reindirizzamento per i dispositivi bloccati	Un URL verso il quale vengono reindirizzati i dispositivi se non sono autorizzati ad accedere alla rete. Si consiglia di utilizzare l’URL del portale self-service, oppure una pagina informativa con un link al portale self-service.

     In Cisco ISE occorre configurare le impostazioni applicabili, in modo tale che, quando si effettua la connessione all'interfaccia di NAC, vengano utilizzati l'URL del server di Sophos Mobile e le credenziali inserite in questi campi.

   - **Check Point**

     Questa opzione consente l'integrazione di Check Point (versione R77.10 e superiore). Configurare le seguenti impostazioni:

Nome utente	Il nome utente che deve essere specificato in Check Point. Verrà usato da Check Point per accedere a Sophos Mobile.

Password	Inserire una password per effettuare l'accesso a Sophos Mobile.
Conferma password	Ripetere la password.

Nel Mobile Access Gateway di Check Point, occorre configurare alcune impostazioni specifiche, come indicato nell'articolo del Check Point Support Center Implementazione cooperativa del MDM per i client dei dispositivi mobili (in inglese).

- **Servizio web**

  Questa opzione consente di connettere il sistema NAC di un altro vendor all'interfaccia del servizio web.

  Sophos Mobile offre un'interfaccia per il servizio web RESTful che fornisce gli indirizzi MAC e lo stato di accesso alla rete dei dispositivi gestiti.

  È possibile connettere il sistema NAC di un altro vendor a questa interfaccia, utilizzando le credenziali di accesso dell'account di un amministratore di Sophos Mobile.

  Per dettagli specifici sull'implementazione dell'interfaccia per il servizio web, consultare la Guida all'interfaccia per Network Access Control di Sophos Mobile (in inglese).

- **Personalizza**

  Questa opzione consente di configurare l'accesso all'interfaccia NAC basato sul certificato.

  Nota
  L'opzione legacy **Personalizza** è obsoleta e verrà rimossa in una delle prossime release. Utilizzare al suo posto l'opzione **Servizio web** per connettere il sistema NAC di un altro vendor a Sophos Mobile.

  Cliccare su **Carica file** e cercare il certificato del sistema NAC dell'altro vendor. Il certificato viene caricato e visualizzato in una tabella.

  Un sistema NAC di terzi che presenta il certificato al server di Sophos Mobile potrà accedere all'interfaccia di NAC.

3. Nella scheda **Network Access Control**, cliccare su **Salva**.

12 Criteri di conformità

Con i criteri di conformità è possibile:

- Autorizzare, vietare o implementare funzionalità specifiche in un dispositivo.
- Definire le azioni da eseguire quando viene violata una regola di conformità.

È possibile creare criteri di conformità diversi, per poi assegnarli ai gruppi di dispositivi. Ciò consente di applicare livelli di protezione diversi ai dispositivi gestiti.

Consiglio
Se si ha intenzione di gestire sia dispositivi aziendali che personali, si consiglia di definire criteri di conformità ben distinti, almeno per quanto riguarda questi due tipi di dispositivi.

12.1 Crea criterio di conformità

1. Nella barra laterale dei menù, sotto **CONFIGURA**, cliccare su **Criteri di conformità**.
2. Nella pagina **Criteri di conformità**, cliccare su **Crea criterio di conformità** e successivamente selezionare il modello su cui si desidera sia basato il criterio:
   - **Modello predefinito**: una selezione di regole di conformità, senza azioni definite.
   - **Modello PCI**, **Modello HIPAA**: regole di conformità basate, rispettivamente, sugli standard di sicurezza HIPAA e PCI DSS.

   Il modello selezionato non limita le opzioni di configurazione successive.
3. Inserire un nome e, opzionalmente, una descrizione per il criterio di conformità.

Ripetere la seguente procedura per tutte le piattaforme, a seconda delle esigenze.

4. Verificare che la casella di spunta **Abilita piattaforma** risulti selezionata in tutte le schede.

   Se questa casella non è selezionata, non sarà possibile verificare la conformità dei dispositivi appartenenti alla piattaforma corrispondente.
5. Sotto **Regola**, configurare le regole di conformità per la piattaforma selezionata.

   Per una descrizione delle regole disponibili per ciascun tipo di dispositivo, cliccare su **?** nell'intestazione della pagina.

   Nota
   Ciascuna regola di conformità possiede un livello di gravità fisso (alto, medio, basso), che viene segnalato da un'icona blu. Il livello di gravità aiuta a valutare l'importanza di ciascuna regola e le azioni da implementare in caso di violazione.

   Nota
   Per i dispositivi nei quali Sophos Mobile gestisce Sophos Container e non il dispositivo intero, è applicabile un solo sotto-set di regole di conformità. Sotto **Evidenzia regole**, selezionare un tipo di gestione che evidenzi le regole applicabili.

6. Sotto **Se viene violata una regola**, definire le azioni da intraprendere in caso di violazione di una regola:

Opzione	Descrizione
Nega e-mail	Vieta accesso alle e-mail Questa azione può essere effettuata solamente se è stata configurata una connessione al proxy EAS standalone. Vedere Configurazione di una connessione al server proxy EAS standalone (pagina 18). Questa azione è disponibile solamente per i dispositivi Android, iOS, Windows e Windows Mobile.
Blocca container	Disattiva le app Sophos Secure Workspace e Secure Email. Ciò incide sui documenti, le e-mail e l'accesso al web gestiti da queste app. Questa azione può essere effettuata solamente dopo l'attivazione di una licenza Mobile Advanced. Questa azione è disponibile solamente per i dispositivi Android e iOS.
Nega rete	Vieta accesso alla rete Questa azione può essere effettuata solamente se è stato configurato Network Access Control (controllo dell'accesso alla rete). Vedere Configurazione di Network Access Control (controllo dell'accesso alla rete) (pagina 20). Questa sezione non è disponibile per i dispositivi in cui Sophos Mobile gestisce solamente Sophos Container.
Crea avviso	Attiva un avviso. Gli avvisi sono visualizzati nella pagina **Avvisi**.
Trasferisci bundle delle operazioni	Trasferisce un bundle delle operazioni specifico al dispositivo. Questa azione è disponibile solamente per i dispositivi Android, iOS, macOS e Windows. Si consiglia per il momento di impostare questa opzione su **Nessuno**. Per ulteriori informazioni, consultare la Guida per amministratori di Sophos Mobile. **Attenzione** Se utilizzati in modo improprio, i bundle delle operazioni potrebbero essere configurati in modo errato o potrebbero addirittura portare alla cancellazione dei dati dal dispositivo. Per assegnare i bundle delle operazioni corretti alle regole di conformità, è necessaria una conoscenza approfondita del sistema.

Nota
Quando un dispositivo Android Enterprise completamente gestito diventa non conforme ai criteri, vengono disattivate tutte le app.

7. Una volta specificate le impostazioni per tutte le piattaforme richieste, cliccare su **Salva** per salvare il criterio di conformità con il nome indicato.

Per utilizzare un criterio di conformità, assegnare il criterio a un gruppo di dispositivi. Questa procedura viene descritta nella sezione successiva.

13 Gruppi di dispositivi

I gruppi di dispositivi vengono utilizzati per categorizzare i dispositivi. Permettono di gestire i dispositivi in maniera efficace, in quanto prevedono l'esecuzione delle operazioni su un gruppo, per evitare di doverle ripetere per ciascun singolo dispositivo.

Un dispositivo appartiene sempre a un gruppo di dispositivi. È possibile assegnare un dispositivo a un gruppo di dispositivi durante la sua aggiunta a Sophos Mobile.

Consiglio
Unire nello stesso gruppo solo dispositivi con lo stesso sistema operativo. Ciò semplificherà l'uso dei gruppi per le attività di installazione e per altre operazioni specifiche del sistema operativo.

13.1 Crea gruppo di dispositivi

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Gruppi dispositivi**, e successivamente su **Crea gruppo di dispositivi**.
2. Nella pagina **Modifica il gruppo di dispositivi**, inserire un nome e una descrizione per il nuovo gruppo di dispositivi.
3. Nell'opzione **Criteri di conformità**, selezionare i criteri di conformità da applicare a dispositivi aziendali e personali.
4. Selezionare **Salva**.

Nota
Le impostazioni del gruppo di dispositivi includono l'opzione **Consenti la registrazione automatica per iOS**. Questa opzione consente di effettuare la registrazione dei dispositivi iOS all'Apple Configurator. Per ulteriori informazioni, consultare la Guida per amministratori di Sophos Mobile.

Il nuovo gruppo verrà così creato e visualizzato nella pagina **Gruppi di dispositivi**.

14 Impostazione iniziale dei criteri dei dispositivi

La procedura guidata **Avvio per i criteri** aiuta a creare criteri dei dispositivi di base per tutte le piattaforme. I criteri possono essere ottimizzati in un secondo momento.

Restrizione
Queste istruzioni non sono applicabili ai dispositivi Chrome.

Per creare criteri con la procedura guidata **Avvio per i criteri**:

1. Nel pannello di controllo, cliccare su **Procedura guidata di avvio per i criteri** nel widget **Operazioni per iniziare**.

   Consiglio
   Se il widget non è visualizzato, cliccare su **Aggiungi widget > Per iniziare**.

2. Nella pagina **Piattaforme**, selezionare le piattaforme dei dispositivi per le quali si desidera creare un criterio.

   Selezionare **Android** e **iOS**.
3. Per **Android**, è possibile selezionare una modalità di gestione.

   Questa impostazione avrà ripercussioni sui tipi di criterio disponibili. Si consiglia di utilizzare la modalità **Android Enterprise**.
4. Nella pagina **Criteri**, configurare le seguenti impostazioni:

   a) Immettere un nome del criterio.

   Viene creato un criterio con questo nome per ciascuna piattaforma.

   b) Selezionare gli ambiti che saranno gestiti dal criterio.

   Se viene deselezionata una casella, verrà saltata la rispettiva pagina della procedura guidata. Gli ambiti da ignorare (e altre opzioni) possono essere configurati in un secondo momento.

   Si consiglia di selezionare come minimo **Requisiti della password** e **Restrizioni**.
5. Nella pagina **Password**, configurare i requisiti della password del dispositivo.
6. Nella pagina **Restrizioni**, configurare le restrizioni da applicare ai dispositivi, come ad es. la disattivazione della fotocamera o di altre funzionalità del dispositivo che potrebbero costituire un rischio di sicurezza.
7. Nella pagina **Wi#Fi**, configurare la connessione alla rete Wi-Fi aziendale.

   Se la rete Wi-Fi adopera un tipo di sicurezza diverso da **WPA/WPA2 PSK**, l'impostazione potrà essere modificata in un secondo momento.
8. Nella pagina **E-mail**, configurare la connessione al server e-mail di Microsoft Exchange aziendale.

   I segnaposti `%_USERNAME_%` e `%_EMAILADDRESS_%` verranno sostituiti dal nome e dall'indirizzo e-mail dell'utente assegnato al dispositivo.
9. Cliccare su **Fine**.

La procedura guidata creerà un criterio per ciascuna piattaforma selezionata.

Per visualizzare il criterio, cliccare su **Criteri** nella barra laterale del menù e selezionare la piattaforma del dispositivo.

Per modificare gli ambiti gestiti, cliccare sul nome del criterio e successivamente su **Aggiungi configurazione**.

Se è stata selezionata la modalità **Android Enterprise**, occorre impostare Android Enterprise per la propria organizzazione prima di poter registrare dispositivi. Consultare la Guida per amministratori di Sophos Mobile.

15 Creazione di un bundle delle operazioni per dispositivi Android

È possibile creare bundle delle operazioni separati per Android, iOS e altre piattaforme di dispositivi che si desidera gestire.

Per creare un bundle delle operazioni di registrazione per i dispositivi Android:

1. Nella barra laterale dei menù, sotto **CONFIGURA**, selezionare **Bundle delle operazioni > Android**.
2. Nella pagina **Bundle delle operazioni**, selezionare **Crea bundle delle operazioni**.
3. Nella pagina **Modifica bundle delle operazioni**, inserire un nome e, facoltativamente, una descrizione per il bundle delle operazioni.

   Il numero della versione viene incrementato automaticamente a ogni salvataggio del bundle delle operazioni.
4. Richiesto: Selezionando **Selezionabile per effettuare azioni di conformità**, è possibile trasferire il bundle delle operazioni sui dispositivi, quando diventano non conformi.

   Questa opzione può essere configurata in un criterio di conformità.
5. Selezionare **Aggiungi operazione > Registrati**. Vengono fornite istruzioni dettagliate per aggiungere un'operazione di registrazione al bundle delle operazioni.
   a) Richiesto: Modificare il nome dell'operazione.

      Il nome verrà visualizzato nel Portale self-service dopo la registrazione del dispositivo.
   b) Selezionare il tipo di registrazione.

      Per registrare dispositivi Android Enterprise completamente gestiti con questo bundle delle operazioni, selezionare **Gestione completa dei dispositivi Android Enterprise**.
   c) Nella pagina successiva, selezionare il criterio che verrà assegnato al dispositivo al momento della registrazione.

      Vengono visualizzati solo i criteri che trovano una corrispondenza con il tipo di registrazione selezionato.
   d) Selezionare **Fine**.
6. Richiesto: Selezionare **Aggiungi operazione > Assegna criterio** per aggiungere altri criteri al bundle delle operazioni, ad esempio se sono stati configurati criteri separati per le impostazioni di Exchange, VPN o Wi-Fi.
7. Richiesto: Aggiungere altre operazioni al bundle delle operazioni, ad esempio per installare applicazioni o visualizzare un messaggio sul dispositivo.
8. Richiesto: È possibile modificare l'ordine di installazione delle operazioni utilizzando le icone a forma di frecce nella parte destra dell'elenco di operazioni.

16 Creazione di un bundle delle operazioni per profili iOS

È possibile creare bundle delle operazioni separati per Android, iOS e altre piattaforme di dispositivi che si desidera gestire.

Per creare un bundle delle operazioni di registrazione per iPhone e iPad:

1. Nella barra laterale dei menù, sotto **CONFIGURA**, selezionare **Bundle delle operazioni > iOS**.
2. Nella pagina **Bundle delle operazioni**, selezionare **Crea bundle delle operazioni**.
3. Nella pagina **Modifica bundle delle operazioni**, inserire un nome e, facoltativamente, una descrizione per il bundle delle operazioni.

   Il numero della versione viene incrementato automaticamente a ogni salvataggio del bundle delle operazioni.
4. Richiesto: Selezionando **Selezionabile per effettuare azioni di conformità**, è possibile trasferire il bundle delle operazioni sui dispositivi, quando diventano non conformi.

   Questa opzione può essere configurata in un criterio di conformità.
5. Richiesto: Selezionare **Ignora errori di installazione delle app** per proseguire con l'elaborazione del bundle delle operazioni anche se non dovesse essere possibile installare un'app.

   Questa opzione è disponibile solamente se il bundle delle operazioni contiene un'operazione **Installa app**.
6. Selezionare **Aggiungi operazione > Registrati**. Vengono fornite istruzioni dettagliate per aggiungere un'operazione di registrazione al bundle delle operazioni.

   a) Richiesto: Modificare il nome dell'operazione.

      Il nome verrà visualizzato nel Portale self-service dopo la registrazione del dispositivo.

   b) Selezionare il tipo di registrazione.

      Per registrare dispositivi completamente gestiti con questo bundle delle operazioni, selezionare **MDM completa**.

   c) Nella pagina successiva, selezionare il criterio che verrà assegnato al dispositivo al momento della registrazione.

      Vengono visualizzati solo i criteri che trovano una corrispondenza con il tipo di registrazione selezionato.

   d) Selezionare **Fine**.
7. Richiesto: Selezionare **Aggiungi operazione > Assegna criterio** per aggiungere altri criteri al bundle delle operazioni, ad esempio se sono stati configurati criteri separati per le impostazioni di Exchange, VPN o Wi-Fi.
8. Richiesto: Aggiungere altre operazioni al bundle delle operazioni, ad esempio per installare applicazioni o visualizzare un messaggio sul dispositivo.
9. Richiesto: È possibile modificare l'ordine di installazione delle operazioni utilizzando le icone a forma di frecce nella parte destra dell'elenco di operazioni.

17 Creazione di configurazioni per gli utenti del portale self-service

La configurazione del Portale self-service permette di configurare: i tipi di dispositivi che possono essere registrati dagli utenti, i dettagli di registrazione e le azioni del dispositivo che possono essere eseguite nel Portale self-service.

È possibile utilizzare configurazioni del Portale self-service diverse per utenti diversi. Per svolgere questa operazione, aggiungere utenti a un gruppo di utenti e associare il gruppo a una configurazione. I dettagli sui gruppi di utenti sono reperibili nelle informazioni correlate.

Se un utente appartiene a più gruppi associati a configurazioni del Portale self-service, verrà applicata la configurazione con la priorità più elevata.

Per creare una configurazione del Portale self-service:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, selezionare **Impostazione > Portale self-service**.
2. Selezionare **Testi di registrazione** e successivamente aggiungere un testo per i termini di utilizzo e un testo di post-registrazione.

   Quando vengono assegnati alla configurazione del portale self-service, questi testi verranno visualizzati rispettivamente prima e dopo la registrazione.
3. Nella pagina **Configurazioni del portale self-service**, selezionare **Aggiungi** per creare una configurazione.
4. Configurare le seguenti impostazioni:

Opzione	Descrizione
Nome	Il nome della configurazione. Nel portale self-service, gli utenti selezioneranno una configurazione con questo nome.
Gruppi di utenti	Selezionare **Aggiungi** e immettere un gruppo di utenti. La configurazione verrà applicata a tutti i membri di questo gruppo.
Numero massimo di dispositivi	Il numero massimo di dispositivi che un utente può registrare nel portale self-service.
Azioni	Selezionare **Mostra** e selezionare le azioni di gestione che un utente è autorizzato a svolgere nel portale self-service.

5. Selezionare **Aggiungi > Android**.
6. Nella finestra di dialogo **Configura impostazioni di piattaforma**, configurare le seguenti impostazioni:

Opzione	Descrizione
Visualizza nome	Il nome delle impostazioni della piattaforma. Nel portale self-service, gli utenti selezioneranno un tipo di registrazione con questo nome.

Opzione	Descrizione
Descrizione	Una descrizione delle impostazioni della piattaforma. Questa descrizione viene visualizzata nel portale self-service accanto al nome.
Proprietario	La modalità proprietario (aziendale o personale) dei dispositivi registrati con questa configurazione.
Gruppo di dispositivi	Il gruppo di dispositivi a cui viene aggiunto il dispositivo registrato.
Pacchetto di registrazione	Selezionare il bundle delle operazioni Android creato in precedenza.
Termini di utilizzo	Il testo da visualizzare nel portale self-service prima della registrazione. Lasciare vuoto questo campo per non visualizzare alcun testo. Gli utenti dovranno accettare il testo per procedere con la registrazione.
Testo di post-registrazione	Il testo da visualizzare nel portale self-service dopo la registrazione. Lasciare vuoto questo campo per non visualizzare alcun testo.

7. Selezionare **Applica** per aggiungere le impostazioni della piattaforma alla configurazione del portale self-service.
8. Selezionare **Aggiungi > iOS** e ripetere i passaggi di configurazione effettuati per Android.
9. Nella pagina **Modifica configurazione del portale self-service**, selezionare **Salva**.

È sempre presente una configurazione di **Default**. Questa configurazione ha la priorità più bassa, per cui viene utilizzata solamente quando non esiste un'altra configurazione che trovi corrispondenza con l'utente.

18 Configurazione della gestione degli utenti

Sophos Mobile offre due metodi diversi per gestire gli account utenti per Sophos Mobile Admin e il portale self-service:

- Con la **gestione degli utenti interni** è possibile creare utenti aggiungendoli manualmente da Sophos Mobile Admin, oppure importandoli da un file CSV.
- Con la **gestione degli utenti esterni**, è possibile effettuare la connessione a una directory LDAP già esistente, e assegnare i dispositivi a gruppi e profili in base alla loro appartenenza a una directory.

Nota

- Non è possibile cambiare metodo di gestione degli utenti una volta che i dispositivi sono stati assegnati agli utenti.
- Per la gestione degli utenti esterni, deve essere disponibile un ambiente LDAPS (LDAP su SSL/TLS). Sophos Mobile si connette al server LDAP utilizzando la porta LDAPS numero 636.

Per selezionare il metodo di gestione degli utenti:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Impostazione utente**.
2. Selezionare l'origine dei dati degli account per Sophos Mobile Admin e il portale self-service (SSP):
   - Selezionare **Directory interna** per utilizzare la gestione utenti interni.
   - Selezionare **Directory LDAP esterna** per adoperare la gestione degli utenti esterni invece di o in combinazione con la gestione degli utenti interni.
3. Se è stata selezionata **Directory LDAP esterna**, cliccare su **Configura LDAP esterno** per specificare i dettagli del server. Vedere Configurazione della connessione a una directory esterna (pagina 35).
4. Selezionare **Salva**.

Nota

Una volta salvate le impostazioni, nella scheda **Impostazione utente** sarà disponibile solamente il metodo di gestione degli utenti selezionato. Per modificare questa selezione in un secondo momento, selezionare **Nessuno** e salvare. Selezionare prima **Non è disponibile alcun profilo SSP specifico per l'utente, né alcun amministratore di LDAP.** per rendere nuovamente disponibili tutte le opzioni.

19 Utilizzo della gestione utenti interni

19.1 Creazione di un utente di test per il portale self-service

Per testare il provisioning tramite portale self-service, creare un proprio account utente del portale self-service. Questo account verrà utilizzato per accedere al portale self-service e per testare la registrazione dei dispositivi.

Per creare un account utente di test per il portale self-service:

1. Nella barra laterale dei menù, sotto **GESTISCI**, selezionare **Persone**.
2. Cliccare su **Crea utente**.
3. Configurare i dovuti dettagli dell'account.

   Verificare che il campo **Invia e-mail di registrazione** sia selezionato.
4. Selezionare **Salva**.

L'utente viene aggiunto all'elenco di utenti del portale self-service, e un'e-mail di registrazione viene inviata all'indirizzo e-mail specificato nei dettagli dell'account.

19.2 Test della registrazione del dispositivo tramite portale self-service

Si consiglia di testare la procedura di registrazione tramite portale self-service, prima di mettere il portale self-service a disposizione degli utenti.

Accedere al portale self-service con l'account dell'utente di test creato nella sezione Creazione di un utente di test per il portale self-service (pagina 33), ed effettuare registrazioni di prova per tutte le piattaforme che si desidera gestire con Sophos Mobile.

19.3 Importa utenti

Una volta effettuato il test di registrazione dei dispositivi tramite Portale self-service, è possibile importare l'elenco degli utenti in Sophos Mobile.

L'importazione degli utenti è applicabile solamente per la gestione degli utenti interni. Per la gestione degli utenti esterni, tutti gli utenti assegnati a un determinato gruppo LDAP possono effettuare l'accesso al sistema.

È possibile importare fino a un massimo di 500 utenti.

Se viene specificato un gruppo inesistente, Sophos Mobile lo creerà.

Il file CSV deve avere le seguenti specifiche:

- La prima riga viene considerata un'intestazione e non viene importata.
- I valori devono essere separati da punto e virgola, non da virgola.

- Tutte le righe devono contenere il numero giusto di caratteri punto e virgola, anche se dovessero essere eliminati dei valori opzionali.
- L'estensione del file deve essere `.csv`.
- Per garantire una corretta importazione dei caratteri che non appartengono alla lingua inglese, il file deve essere codificato in UTF-8.

Consiglio
Nella pagina **Importa utenti**, selezionare **Esempio di CSV** per scaricare un file di esempio.

Per importare gli utenti da un file CSV:

1. Nella barra laterale dei menù, sotto **GESTISCI**, selezionare **Persone**.
2. Selezionare **Importa utenti**.
3. Nella pagina **Importa utenti**, selezionare **Invia e-mail di registrazione**.
4. Selezionare **Carica file** e caricare il file CSV preparato in precedenza.
   Le voci verranno lette dal file e visualizzate.
5. Se i dati non vengono impostati nel giusto formato, o se sono inconsistenti, non sarà possibile importare l'intero file. In tale eventualità, esaminare i messaggi di errore visualizzati accanto alle relative voci, correggere il contenuto del file CSV a seconda di quanto richiesto e caricarlo nuovamente.
6. Selezionare **Fine** per creare gli account utente.

Gli utenti verranno importati e visualizzati nella pagina **Persone**. Riceveranno e-mail con le credenziali di accesso per il portale self-service.

20 Utilizzo della gestione utenti esterni

20.1 Configurazione della connessione a una directory esterna

Per gestire gli account utente per Sophos Mobile Admin e il portale self-service in una directory utente LDAP esterna, occorre configurare la connessione al proprio server LDAP.

Sophos Mobile è in grado di connettersi ai seguenti server LDAP:

- **Active Directory**
- **Google Cloud Directory**
- **IBM Domino**
- **NetIQ eDirectory**
- **Red Hat Directory Server**
- **Zimbra**

Per le versioni supportate, consultare le Note di rilascio di Sophos Mobile 9.5 (in inglese).

Nota
Non viene effettuata alcuna sincronizzazione tra la directory LDAP e Sophos Mobile. Sophos Mobile accede alla directory LDAP solamente per cercare informazioni sugli utenti. Eventuali modifiche a un account utente LDAP non verranno implementate nel database di Sophos Mobile, e viceversa.

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Impostazione utente**.
2. Selezionare **Directory LDAP esterna**.
3. Cliccare su **Configura LDAP esterno**.

La configurazione dipenderà dal tipo di server LDAP. Le seguenti istruzioni si riferiscono ad Active Directory.

4. Nella pagina **Dettagli server**, configurare le seguenti impostazioni:
   a) Nel campo **Tipo LDAP**, selezionare il tipo di server LDAP.
   b) Nel campo **URL primario**, immettere l'indirizzo IP o il nome del server di directory primario.
      Selezionare **SSL/TLS** per proteggere la connessione del server con SSL o TLS (a seconda della compatibilità del server).
   c) Richiesto: Nel campo **URL secondario**, immettere l'indirizzo IP o il nome di un servizio di directory che Sophos Mobile può utilizzare come fallback qualora il server primario non dovesse essere disponibile.
   d) Nei campi **Utente** e **Password**, immettere le credenziali che Sophos Mobile dovrà utilizzare per autenticarsi con il server LDAP.
      Utilizzare uno dei seguenti formati:
      - `<dominio>\<nome utente>`

- `<nome utente>@<dominio>.<codice dominio>`

Nota
Per motivi di sicurezza, si consiglia di selezionare un account che non abbia autorizzazioni di scrittura per la directory.

5. Nella pagina **Base di ricerca**, immettere il distinguished name (DN) dell'oggetto della base di ricerca.

   L'oggetto della base di ricerca definisce il percorso nella directory da cui comincia la ricerca LDAP.
6. Nella pagina **Campi di ricerca**, configurare gli attributi del servizio di directory che contiene le proprietà utente adoperate da Sophos Mobile.

   Selezionare i nomi degli attributi dall'elenco o immetterli manualmente.

   Utilizzare le seguenti mappature per Active Directory:

Proprietà in Sophos Mobile	Attributo in Active Directory
Nome utente	`sAMAccountName`
Nome	`givenName`
Cognome	`sn`
E-mail	`mail`

7. Nella pagina **Configurazione SSP**, specificare gli utenti a cui è consentito accedere al portale self-service. Inserire le informazioni pertinenti nel campo **Gruppo di directory LDAP**, adoperando una delle seguenti opzioni:

   - Se si inserisce il nome di un gruppo che è definito nel server di directory, si concederà l'accesso al portale self-service a tutti i membri del gruppo in questione. Una volta immesso il nome del gruppo, cliccare su **Prova gruppo** per risolvere il nome del gruppo a un nome distinto (Distinguished Name, DN).
   - Se il campo viene lasciato vuoto, nessun utente del server di directory potrà accedere al portale self-service. Utilizzare questa opzione se si desidera abilitare la gestione degli utenti esterni per Sophos Mobile Admin ma non per il portale self-service.

   Nota
   Il gruppo che viene specificato in questo campo non ha nessuna correlazione con il gruppo utenti che viene definito nella scheda **Impostazioni del gruppo** della pagina **Portale self-service**. Queste altre impostazioni servono per definire i bundle delle operazioni, l'appartenenza al gruppo Sophos Mobile e le piattaforme per dispositivi mobili che sono disponibili per ciascun gruppo utenti.

   Per ulteriori informazioni sulle impostazioni per i gruppi del portale self-service, consultare la Guida per amministratori di Sophos Mobile.

8. Selezionare **Applica**.
9. Nella scheda **Impostazione utente**, cliccare su **Salva**.

Informazioni correlate

Come connettere un server di Sophos Mobile 8.0 a un'Azure Active Directory (articolo 128081 della knowledge base Sophos)

Connettere Sophos Mobile a Google Cloud Identity / Google Cloud Directory utilizzando Secure LDAP (articolo 132870 della knowledge base Sophos)

20.2 Test della registrazione del dispositivo per gli utenti LDAP

Si consiglia di testare la procedura di registrazione tramite portale self-service, prima di mettere il portale self-service a disposizione degli utenti.

Accedere al portale self-service con le proprie credenziali LDAP, ed effettuare prove di registrazione per tutte le piattaforme che si desidera gestire con Sophos Mobile.

21 Utilizzo della procedura guidata **Aggiungi dispositivo**

I nuovi dispositivi possono essere registrati in maniera molto semplice, grazie alla procedura guidata **Aggiungi dispositivo**. Offre un flusso di lavoro che unisce e combina le seguenti operazioni:

- Aggiunta di un nuovo dispositivo a Sophos Mobile.
- Opzionale: Assegnazione di un utente al dispositivo.
- Registrazione del dispositivo.
- Opzionale: Trasferisce un bundle delle operazioni al dispositivo.

1. Nella barra laterale dei menù, sotto **GESTISCI**, cliccare su **Dispositivi** e successivamente cliccare su **Aggiungi > Aggiungi procedura guidata per i dispositivi**.

   Consiglio
   È anche possibile avviare la procedura guidata dalla pagina **Pannello di controllo**, cliccando sul widget **Aggiungi dispositivo**.

2. Nella pagina **Utente**, immettere i criteri di ricerca per l'individuazione di un utente a cui assegnare il dispositivo, oppure selezionare **Salta assegnazione utente** per registrare un dispositivo che per il momento non si desidera assegnare ad alcun utente.
3. Nella pagina **Selezione utente**, selezionare l'utente desiderato dall'elenco di utenti che soddisfano i criteri di ricerca.
4. Nella pagina **Dettagli dispositivo**, configurare le seguenti impostazioni:

Opzione	Descrizione
Piattaforma	La piattaforma del dispositivo.
Nome	Un nome univoco che contraddistinguerà il dispositivo per la gestione con Sophos Mobile.
Descrizione	Una descrizione opzionale del dispositivo.
Numero telefonico	Un numero di telefono opzionale. Inserire il numero, completo di prefisso internazionale, ad esempio: `+491701234567`.
Indirizzo e-mail	L'indirizzo e-mail a cui inviare le istruzioni per la registrazione. Se per il cliente è configurata la gestione degli utenti, sarà l'indirizzo e-mail dell'utente assegnato al dispositivo. Se non è configurata alcuna gestione degli utenti, immettere un indirizzo e-mail.
Proprietario	Selezionare il tipo di proprietario del dispositivo: **Aziendale** o **Personale**.
Gruppo di dispositivi	Selezionare il gruppo a cui verrà assegnato il dispositivo. Se non sono ancora stati creati gruppi di dispositivi, è possibile selezionare il gruppo **Predefinito**, che è sempre disponibile.

5. Nella pagina **Tipo di registrazione**, selezionare se si desidera registrare il dispositivo o solamente Sophos Container.

Selezionare **Registra dispositivo**.

6. Selezionare il bundle delle operazioni configurato per la piattaforma del dispositivo.
7. Nella pagina **Registrazione**, seguire le istruzioni per completare il processo di registrazione.
8. Una volta completato il processo di registrazione, cliccare su **Fine**.

Nota

- Una volta effettuate tutte le selezioni, è possibile chiudere la procedura guidata senza dover attendere che compaia il pulsante **Fine**. Un'operazione di registrazione verrà così creata ed elaborata in background.

22 Glossario

profilo di provisioning ad hoc	Un profilo di provisioning per la distribuzione che viene aggiunto a un'app iOS sviluppata autonomamente. Consente di installare l'app sui dispositivi designati senza doverla pubblicare nell'App Store.
registrazione	La registrazione di un dispositivo a Sophos Mobile.
Enterprise App Store	Un archivio di app ospitate sul server di Sophos Mobile. L'amministratore può aggiungere app all'Enterprise App Store utilizzando Sophos Mobile Admin. Gli utenti possono quindi adoperare l'app Sophos Mobile Control per installare le suddette app sui propri dispositivi.
Licenza Mobile Advanced	Con una licenza di tipo Mobile Advanced è possibile gestire Sophos Intercept X for Mobile ,Sophos Secure Workspace e Sophos Secure Email.
provisioning	Il processo di installazione dell'app Sophos Mobile Control su un dispositivo.
Portale self-service	L'interfaccia web che consente agli utenti di registrare i propri dispositivi ed effettuare altre operazioni senza dover richiedere l'intervento dell'helpdesk.
Client Sophos Mobile	L'app Sophos Mobile Control installata sui dispositivi gestiti da Sophos Mobile.
Console di Sophos Mobile	L'interfaccia web utilizzata per gestire i dispositivi.
Sophos Intercept X for Mobile	Un'app di protezione per i dispositivi Android e iOS. Questa app può essere gestita da Sophos Mobile, a patto che si disponga di una licenza Mobile Advanced attiva.
Sophos Secure Email	Un'app per dispositivi Android e iOS che fornisce un container sicuro per la gestione di e-mail, calendario e contatti. Questa app può essere gestita da Sophos Mobile, a patto che si disponga di una licenza Mobile Advanced attiva.
Sophos Secure Workspace	Un'app per dispositivi Android e iOS che offre un'area di lavoro sicura, nella quale gli utenti possono navigare, gestire, modificare, condividere, cifrare e decifrare documenti provenienti da vari provider di servizi di archiviazione, o distribuiti dalla vostra azienda. Questa app può essere gestita da Sophos Mobile, a patto che si disponga di una licenza Mobile Advanced attiva.

bundle delle operazioni	Un pacchetto creato per includere varie operazioni diverse in un'unica transazione. Sarà possibile unire insieme tutte le operazioni necessarie per completare la registrazione e rendere operativo un dispositivo.
Team ID	Ogni app iOS e macOS viene firmata con un Team ID. Il Team ID viene fornito da Apple e corrisponde in maniera univoca a un team di sviluppo specifico.

23 Supporto

È possibile ricevere supporto tecnico per i prodotti Sophos in ciascuno dei seguenti modi:

- Visitando la Sophos Community su community.sophos.com/ e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto da www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket per il nostro supporto tecnico alla pagina https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

24 Note legali