SOPHOS
Security made simple.

Sophos Mobile

Guida di avvio

Versione prodotto: 8

Sommario

1 Informazioni sulla guida

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

Ulteriori informazioni sono disponibili nella Guida in linea per amministratori di Sophos Mobile.

Questa guida si concentra sulle piattaforme Android e iOS, in quanto si tratta delle piattaforme più comunemente utilizzate. Le impostazioni qui descritte possono essere applicate in modo simile anche agli altri sistemi operativi supportati.

2 Sophos Mobile licenze

Sophos Mobile offre due tipi di licenza:

- Licenza Mobile Standard
- Licenza di Mobile Advanced

Con una licenza di tipo Mobile Advanced è possibile gestire le app Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email.

Per maggiori informazioni sulla gestione di Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email con Sophos Mobile, consultare la Guida in linea per amministratori di Sophos Mobile.

Effettuando l'accesso come super administrator, è possibile attivare le licenze da voi acquistate nel cliente super administrator, e assegnare a ciascun cliente individuale il corrispettivo numero di utenti dotati di licenza.

2.1 Licenza di prova

Sophos consente di effettuare la prova gratuita di Sophos Mobile. È possibile registrarsi per la prova gratuita direttamente dal sito Web di Sophos: http://www.sophos.com/it-it/products/free-trials/mobile-control.aspx.

La licenza di prova consente di gestire fino a cinque utenti per la durata di 30 giorni.

Per attivare la prova gratuita di Sophos Mobile, è semplicemente necessario fornire l'indirizzo e-mail utilizzato per effettuare la registrazione al momento del download del programma di installazione.

2.2 Upgrade delle licenze di prova a licenze complete

Per effettuare l'upgrade delle licenze di prova e tramutarle in licenze complete, basta inserire l'intera chiave di licenza in Sophos Mobile. Per ulteriori informazioni, consultare la Guida in linea per amministratori di Sophos Mobile.

2.3 Aggiornamento delle licenze

Per aggiornare le licenze, occorre attivare la nuova chiave di licenza in Sophos Mobile. Per ulteriori informazioni, consultare la Guida per super administrator di Sophos Mobile.

3 Passaggi chiave

Per cominciare ad utilizzare Sophos Mobile:

1. Accedere a Sophos Mobile Admin come super administrator.
2. Avviare la procedura guidata di configurazione per effettuare la configurazione iniziale del server di Sophos Mobile.

> **Nota**
> La procedura guidata di configurazione prevede anche un'opzione per la richiesta di una prova gratuita.

3. Verificare i dati relativi alla licenza.
4. Creare un nuovo cliente per la gestione dei dispositivi.
5. Passare al nuovo cliente.
6. Creare un amministratore per il nuovo cliente e utilizzarlo per accedere a Sophos Mobile Admin.
7. 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.
8. Caricare un certificato per l'Apple Push Notification service per gestire i dispositivi iOS.
9. Creare criteri di conformità.
10. Creare gruppi di dispositivi.
11. Configurare i dispositivi.
12. Aggiornare le impostazioni del portale self-service e aggiungere un utente di test al portale self-service.
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.
    Il procedimento viene descritto nella *Guida per super administrator di Sophos Mobile*.
15. Effettuare un test della registrazione nel portale self-service.

4 Accesso come super administrator

Occorre accedere a Sophos Mobile Admin utilizzando l'account super administrator configurato durante l'installazione di Sophos Mobile, per svolgere alcune procedure iniziali di configurazione.

1. Aprire l'indirizzo web di Sophos Mobile Admin, che è stato configurato durante l'installazione di Sophos Mobile.
2. Nella finestra di dialogo di accesso, inserire il nome del cliente del super administrator e le credenziali del super administrator, e successivamente cliccare su **Accesso**.

Nota

Quando si effettua l'accesso come super administrator, viene caricata una versione speciale di Sophos Mobile Admin, che è ottimizzata per svolgere le attività del super administrator.

Per una descrizione dettagliata di come utilizzare Sophos Mobile Admin come super administrator, consultare la *Guida per super administrator di Sophos Mobile*.

5 Avvio della procedura guidata di configurazione

Quando si effettua l'accesso a Sophos Mobile Admin per la prima volta dopo l'installazione, viene avviata una procedura guidata per la configurazione di determinate impostazioni del server.

È necessario fornire:

- Una chiave di licenza Mobile Standard e opzionalmente anche una chiave di licenza Mobile Advanced
- Certificato/i SSL/TLS
- Credenziali SMTP

Nota
Effettuando l'accesso come super administrator, è possibile modificare queste impostazioni anche in un secondo momento, nella pagina **Impostazione del sistema** di Sophos Mobile Admin. Per aprire la pagina **Impostazione del sistema** dalla barra laterale del menù, cliccare su **IMPOSTAZIONI > Impostazione > Impostazione del sistema**.

Per eseguire la procedura guidata di configurazione:

1. Una volta effettuato l'accesso a Sophos Mobile Admin, viene visualizzata la vista di **Benvenuto**. Cliccare su **Avanti**.
2. Nella vista **Licenze**, inserire la chiave di licenza Mobile Standard, oppure richiedere una licenza di prova:
   - **Chiave di licenza Mobile Standard:**

     Quando si inserisce la chiave di licenza Mobile Standard e si clicca su **Attiva**, viene fornita l'opzione di inserire anche una chiave di licenza Mobile Advanced. Se sono state acquistate licenze Mobile Advanced, inserirne la chiave in **Chiave di licenza Advanced**.
   - **Richiesta di una licenza di prova:**

     Per richiedere una licenza di prova gratuita cliccare su **Richiedi prova** e inserire l'indirizzo e-mail utilizzato per effettuare la registrazione e scaricare il programma di installazione di Sophos Mobile da www.sophos.it. Cliccare quindi nuovamente su **Richiedi prova**.

   Nota
   È possibile modificare le impostazioni della licenza ogniqualvolta lo si desideri tramite Sophos Mobile Admin.

   Cliccare su **Avanti**.
3. Nella vista **SSL/TLS**, configurare i certificati da utilizzare per garantire una connessione SSL o TLS sicura tra il server di Sophos Mobile e i client.

   È possibile configurare sino a un massimo di quattro certificati, in quanto, a seconda dell'architettura della rete, potrebbero essere in uso certificati diversi per i client che si connettono da internet, o dall'intranet locale. Il server di Sophos Mobile comunicherà l'elenco di certificati ai client. Al momento di stabilire una connessione SSL o TLS, i client riterranno il server attendibile solamente se il certificato presentato appartiene a questo elenco (*certificate pinning*).

a) Cliccare su **Certificato/i di individuazione automatica**.

Nella maggior parte dei casi la funzionalità di individuazione automatica è in grado di individuare i certificati in uso.

b) Nel caso in cui i certificati non possano essere individuati in maniera automatica, è possibile caricarli manualmente cliccando su **Carica file** e selezionando il giusto file CER o DER.

I certificati vengono visualizzati nella vista **SSL/TLS**.

Importante

Aggiornare l'elenco quando si modificano o si rinnovano i certificati SSL. Deve sempre essere disponibile almeno un certificato valido. Altrimenti i client non riterranno il server attendibile e non vi effettueranno la connessione.

4. Nella vista **SMTP**, configurare le informazioni relative al server SMTP e le credenziali di accesso. SMTP deve essere configurato in modo da consentire l'invio di e-mail contenenti le credenziali di accesso ai nuovi utenti. Deve anche essere configurato per permettere la registrazione tramite e-mail.

Opzione	Descrizione
Host SMTP	L'indirizzo del server SMTP.
Porta di connessione	La porta server a cui effettuare la connessione. **Nota** I tipi di connessione visualizzati (TLS, SSL e non cifrata) mostrano solamente gli utilizzi delle porte standard. Consultare la documentazione del server SMTP per indicazioni sulla porta da utilizzare.
Utente VPP	Se richiesto dal server SMTP, inserire il nome di un utente autorizzato alla connessione.
Password SMTP	La password dell'utente SMTP.
Creatore e-mail	L'indirizzo e-mail che comparirà nel campo *Da* delle e-mail inviate da Sophos Mobile.
Nome creatore	Il nome dell'autore dell'e-mail che comparirà nel campo *Da*. All'occorrenza, è successivamente possibile configurare un diverso nome (ma non indirizzo e-mail) del creatore del messaggio per ciascun cliente. Consultare la Guida in linea per amministratori di Sophos Mobile.
Invia e-mail di errore	Sophos Mobile invierà e-mail di errore, ad es. alla scadenza di un certificato APNs.
Destinatari e-mail	Inserire gli indirizzi e-mail dei destinatari a cui inviare le e-mail di errore.

Nota
Sophos Mobile non supporta il meccanismo OAUTH per l'autenticazione SMTP. I provider di servizi e-mail che prediligono l'utilizzo di OAUTH (come ad es. Google Gmail) potrebbero classificare come non sicuri i tentativi di accesso da Sophos Mobile.

5. Dopo aver configurato tutte le informazioni necessarie, cliccare su **Invia e-mail di test** per verificare la configurazione delle e-mail.
6. Cliccare su **Salva**.

6 Attivazione di licenze Mobile Advanced

Con le licenze Mobile Advanced, è possibile utilizzare Sophos Mobile per gestire le app Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email.

Se durante la configurazione iniziale di Sophos Mobile non sono state attivate licenze Mobile Advanced, il super administrator può effettuarne l'attivazione in un secondo momento dalla Sophos Mobile Admin:

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**.
2. Sotto la scheda **Licenze**, inserire la chiave di licenza all'interno del campo **Chiave di licenza Advanced** e cliccare su **Attiva**.

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

7 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.

Per verificare le licenze disponibili:

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**.
2. Nella pagina **Impostazione del sistema**, cliccare 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.

  Se il super administrator non ha precedentemente impostato una quota per il cliente, il numero delle licenze sarà limitato dal numero complessivo del server di Sophos Mobile.
- **Licenze utilizzate**: Numero di licenze in uso.
- **Valido entro**: La data di scadenza della licenza.
- **URL con licenza**: L'URL del server di Sophos Mobile per cui è stata rilasciata la licenza.

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

8 Creazione di un cliente

Per svolgere questa operazione, occorre accedere a Sophos Mobile Admin come super administrator.

1. Nella barra laterale del menù, sotto **INFORMAZIONI**, cliccare su **Pannello di controllo**.
2. Cliccare su **Crea cliente**.
3. Nella pagina **Modifica cliente**, configurare le seguenti impostazioni:

Opzione	Descrizione
Nome	Il nome del cliente.
Descrizione	Testo che descrive lo scopo dell'account del cliente.
Numero massimo di licenze	Il numero di utenti dei dispositivi e di dispositivi non assegnati che è possibile gestire per il cliente.
Licenze avanzate	Quando viene selezionata questa opzione, il cliente può utilizzare Sophos Mobile per gestire le app Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email.
Valido entro	La data di scadenza delle licenze assegnate al cliente. Dopo tale data non sarà possibile creare nuove operazioni per i dispositivi che sono gestiti per questo cliente.
Disattiva account	Selezionando questa opzione si disattiva la possibilità di accedere a questo cliente. Effettuando l'accesso come super administrator, si potrà comunque passare alla vista del cliente, utilizzando l'elenco dei clienti situato nell'intestazione della pagina. Un account disattivato può essere nuovamente attivato deselezionando la casella di controllo **Disattiva account**.
Piattaforme attive	Selezionare le piattaforme per le quali è possibile effettuare la registrazione dei dispositivi.
Localizza dispositivo	Selezionare **Consentita per utente** per consentire agli utenti di utilizzare la geolocalizzazione dei propri dispositivi in caso di furto o smarrimento. Selezionare **Consentita per amministratore** per consentire agli amministratori di individuare la posizione dei dispositivi.
Clona impostazioni	Selezionare la casella di controllo **Impostazioni e pacchetti** se si desidera che tutti i profili, bundle e pacchetti creati dall'account super administrator vengano resi disponibili nell'account del cliente.
Directory utente	Selezionare la fonte dei dati per gli utenti del portale self-service (SSP) che devono essere gestiti da Sophos Mobile. Le opzioni disponibili sono: • **Nessuna. Non è disponibile alcun profilo SSP specifico per l'utente, né alcun amministratore di LDAP**: questa opzione disattiva la creazione di account utente per il portale self-service e la ricerca, da una directory LDAP, di account per Sophos Mobile Admin.

Opzione	Descrizione
	• **Directory interna**: abilita la gestione degli utenti interni per Sophos Mobile Admin e il portale self-service. Per ulteriori informazioni, consultare la Guida in linea per amministratori di Sophos Mobile. • **Directory LDAP esterna**: oltre alla gestione degli utenti interni, consente la ricerca, da una directory LDAP, di account per Sophos Mobile Admin e per il portale self-service. Cliccare su **Configura LDAP esterno** per specificare i dettagli del server.

4. Cliccare su **Salva**.

Il cliente è stato creato.

9 Passaggio al nuovo cliente

Per completare la configurazione iniziale del cliente creato nella sezione precedente, occorre passare dal cliente super administrator al cliente in questione.

Per passare alla vista del nuovo cliente:

1. Nell'intestazione della pagina della vista del super administrator, cliccare sul nome del cliente attuale per aprire l'elenco di clienti disponibili.

   Nell'elenco, il cliente super administrator è contrassegnato da un asterisco e viene visualizzato in cima alla lista.
2. Selezionare il cliente creato nella sezione precedente.

La vista si trasformerà nella vista del cliente selezionato, ovvero nella vista che si ottiene effettuando l'accesso come amministratore di quel cliente in particolare.

10 Creazione di un amministratore per il cliente

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Amministratori**.
2. Nella pagina **Mostra amministratori**, cliccare su **Crea amministratore**.
3. Nella pagina **Modifica amministratore**, configurare i dettagli dell'account per l'amministratore.
   - Quando **Directory LDAP esterna** è selezionata come directory utente per il cliente, è possibile cliccare su **Ricerca utente con LDAP** per selezionare un account LDAP già esistente.
   - Quando o **Directory interna** o **Nessuna** è selezionata come directory utente per il cliente, inserire i dati applicabili nei campi **Nome di accesso**, **Nome**, **Cognome**, **Indirizzo e-mail** e **Password**.

   La password che verrà specificata sarà una password one-time. Al primo accesso, verrà richiesto all'amministratore di modificarla.
4. Nell'elenco **Ruolo**, selezionare il ruolo utente **Amministratore**.
5. Cliccare su **Salva** per creare l'account amministratore.

Per procedere con la configurazione del cliente, disconnettersi da Sophos Mobile Admin ed effettuare nuovamente l'accesso utilizzando le credenziali dell'amministratore appena creato (nome del cliente, nome di accesso, password one-time).

11 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

11.1 Configurazione delle impostazioni personali

Per utilizzare Sophos Mobile Admin in maniera più efficace, è possibile personalizzare l'interfaccia utente in modo tale da visualizzare solo le piattaforme in uso.

> **Nota**
> Configurando le piattaforme viene modificata solamente la vista degli utenti al momento collegati, da cui non è possibile disattivare alcuna funzione.

Prerequisito: aver effettuato l'accesso a Sophos Mobile Admin utilizzando l'account amministratore creato per il nuovo cliente.

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

Opzione	Descrizione
Lingua	Selezionare la lingua in cui si desidera visualizzare Sophos Mobile Admin.
Fuso orario	Selezionare il fuso orario in cui vengono indicate data e ora.
Unità di misura	Selezionare le unità di misura per i valori di lunghezza (**Metriche** or **Imperiali**).
Righe per pagina nelle tabelle	Selezionare il numero massimo di righe per tabella che si desidera visualizzare in ciascuna pagina.
Mostra dettagli dispositivo estesi	Selezionare questa casella di spunta per visualizzare tutte le informazioni disponibili sul dispositivo. Le schede **Proprietà personalizzate** e **Proprietà interne** verranno aggiunte alla pagina **Mostra dispositivo**.
Piattaforme attive	Selezionare le piattaforme che si desidera gestire per questo cliente: - **Android** - **Android Things** - **iOS** - **Windows Mobile** (include i sistemi operativi Windows Phone 8.1 e Windows 10 Mobile) - **Windows**

Opzione	Descrizione
	▪ **Windows IoT** L'interfaccia utente di Sophos Mobile Admin cambierà in base alle piattaforme selezionate. Verranno visualizzate solamente le viste e le funzionalità che riguardano le piattaforme selezionate. **Nota** l'elenco delle piattaforme disponibili dipende dalle impostazioni relative alla piattaforma in esecuzione configurate dal super administrator. Per ulteriori informazioni, consultare la Guida per super administrator di Sophos Mobile.

3. Cliccare su **Salva**.

11.2 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. Per informazioni sulla gestione esterna degli utenti, consultare la Guida per super administrator di Sophos Mobile.

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale**, e successivamente cliccare 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. Cliccare su **Salva**.

11.3 Configurazione dei dati di contatto del supporto tecnico

Per fornire supporto agli utenti che avessero domande o problemi, potete fornire i dettagli di come contattare il supporto tecnico. Le informazioni qui inserite verranno visualizzate nell'app Sophos Mobile Control e nel portale self-service.

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale**, e successivamente cliccare sulla scheda **Contatto tecnico**.
2. Inserire le informazioni relative al supporto tecnico.
3. Cliccare su **Salva**.

11.4 Configurazione delle impostazioni del portale self-service

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Portale self-service**.
   Si aprirà la pagina del **Portale self-service**.
2. Nella scheda **Configurazione**, configurare le impostazioni del portale self-service in base alle proprie esigenze.

   Se a questo punto non si fosse sicuri di quali impostazioni applicare, si consiglia di adoperare le impostazioni predefinite.

   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.
3. Nella scheda **Termini di utilizzo**, cliccare su **Modifica** per inserire un testo contenente una declinazione di responsabilità, o un consenso, per il criterio per i dispositivi mobili.

   Questo testo verrà visualizzato all'inizio del processo di registrazione del dispositivo. Gli utenti devono accettare il testo prima di poter effettuare la registrazione.

   Consiglio
   È possibile utilizzare la barra degli strumenti editor per applicare al testo una formattazione HTML di base. Ciò è valido anche per il testo di post-installazione descritto nel passaggio successivo.

4. Opzionale: Nella scheda **Testo di post-installazione**, cliccare su **Modifica** per inserire un testo da visualizzare al completamento della registrazione del dispositivo.

   Il testo può essere utilizzato anche per descrivere qualsivoglia passaggio successivo che l'utente debba svolgere dopo la registrazione.
5. Cliccare su **Salva**.

12 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.

Sophos Mobile gestisce i certificati APNs in base al cliente. Occorre creare e caricare i certificati per ciascun cliente utilizzato.

I certificati APNs sono validi per un anno.

Per semplificare il rinnovo dei certificati APNs, il super administrator ha la possibilità di rinnovare in un solo passaggio i certificati di tutti i clienti che utilizzano lo stesso certificato. Consultare la Guida in linea per amministratori di Sophos Mobile.

Le sezioni che seguono definiscono i requisiti da soddisfare e le azioni da intraprendere per ottenere l'accesso ai server di APNs con il proprio certificato client.

12.1 Requisiti

Per la comunicazione con Apple Push Notification Service (APNs), occorre autorizzare il traffico TCP in entrata e in uscita dalle seguenti porte:

- Il server di Sophos Mobile deve potersi connettere a `gateway.push.apple.com:2195 TCP (17.0.0.0/8)`
- Ciascun dispositivo iOS dotato solamente di accesso Wi-Fi deve potersi connettere a `*.push.apple.com:5223 TCP (17.0.0.0/8)`

12.2 Creazione di un certificato APNs

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema** e successivamente sulla scheda **APNs**.

   La descrizione di questa scheda indica la procedura dettagliata da seguire per richiedere un certificato da Apple e caricarlo in Sophos Mobile.
2. Nel passaggio **Scaricare la richiesta di firma del certificato**, cliccare su **Scarica richiesta di firma del certificato**.

   Questa operazione salva il file di richiesta di firma del certificato `apple.csr` sul computer locale. Il file di richiesta di firma del certificato è univoco per il cliente attuale.
3. 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. Nel passaggio **Creazione di un ID Apple**, cliccare su **Creare un nuovo ID 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.

4. Come riferimento, inserire il nuovo ID Apple nel campo **ID Apple** nella parte alta della scheda **APNs**.

   Ogni anno, al rinnovo del certificato, occorrerà sempre utilizzare lo stesso ID Apple.
5. Nel passaggio **Creazione o rinnovo di un certificato APNs**, cliccare su **Apple Push Certificates Portal**.

   Verrà aperto l'Apple Push Certificates Portal.
6. Accedere con il proprio ID Apple e caricare il file di richiesta di firma del certificato `apple.csr`.
7. Scaricare il file `.pem` del certificato APNs e salvarlo nel computer.
8. Nel passaggio **Upload di un Certificato APNs**, cliccare su **Carica certificato** e cercare il file `.pem` ricevuto dall'Apple Push Certificates Portal.
9. Cliccare su **Salva** per aggiungere il certificato APNs a Sophos Mobile.

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

13 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.

13.1 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 il contenitore Sophos 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 il super administrator ha configurato una connessione al proxy EAS interno o standalone. Consultare la Guida per super administrator di Sophos Mobile. Questa azione è disponibile solamente per i dispositivi Android, iOS, Windows e Windows Mobile.
Blocca contenitore	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 il super administrator ha configurato Network Access Control (controllo dell'accesso alla rete). Consultare la Guida per super administrator di Sophos Mobile.
Crea avviso	Crea 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 in linea per amministratori di Sophos Mobile. **Importante** 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.

7. Una volta specificate le impostazioni per tutte le piattaforme richieste, cliccare su **Salva** per salvare il criterio di conformità con il nome indicato.
Il nuovo criterio di conformità viene visualizzato nella pagina **Criteri di conformità**.

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

14 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.

14.1 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. Cliccare su **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 in linea per amministratori di Sophos Mobile.

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

15 Configurazione dei dispositivi iOS

15.1 Creazione di un profilo per dispositivi iOS

Questa sezione descrive la creazione di un profilo per la configurazione iniziale dei dispositivi iOS.

Si consiglia di impostare profili separati per:

- Criteri e restrizioni della password
- Impostazioni di account per Exchange (se richiesto)
- Impostazioni VPN (se richiesto)
- Impostazioni Wi-Fi (se richiesto)
- Certificati root e client (se richiesto)

Nota

Sophos Mobile offre due metodi per creare profili per i dispositivi iOS:

- Creazione dei profili direttamente da Sophos Mobile Admin.
- Importazione dei profili creati con Apple Configurator.

Questa sezione descrive come creare profili in Sophos Mobile Admin. Per informazioni su come importare i profili creati utilizzando Apple Configurator, consultare la Guida in linea per amministratori di Sophos Mobile.

Per creare il profilo di un dispositivo iOS per criteri e restrizioni della password:

1. Nella barra laterale dei menù, sotto **CONFIGURA**, cliccare su **Profili, criteri > iOS**.
2. Nella pagina **Profili e criteri**, cliccare su **Crea > Profilo del dispositivo**.
3. Nella pagina **Modifica profilo**, configurare le seguenti impostazioni:
   a) **Nome**: Inserire un nome per il profilo. Si consiglia di utilizzare il nome `Profilo SSP iOS` per i profili applicati durante la registrazione tramite portale self-service (Self-Service Portal, SSP).
   b) **Azienda**: Inserire il nome dell'organizzazione da assegnare al profilo, ad esempio il nome di un'azienda.
   c) **Descrizione**: Inserire una descrizione per il profilo, ad esempio `profilo di base`.
4. Per aggiungere criteri per la password al profilo, cliccare su **Aggiungi configurazione**, selezionare **Criteri password**.
5. Nella pagina **Criteri password**, configurare le necessarie impostazioni per la password.
   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.
6. Per salvare le impostazioni, cliccare su **Applica**.
   La configurazione dei **Criteri password** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
7. Per aggiungere restrizioni, cliccare su **Aggiungi configurazione**, selezionare **Restrizioni**.
8. Nella pagina **Restrizioni**, selezionare la restrizione richiesta.

   Alcune restrizioni richiedono tipi di dispositivo o versioni di iOS specifici. Questi requisiti vengono visualizzati sulla destra, accanto a ciascuna restrizione.

   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.

9. Per salvare le impostazioni, cliccare su **Applica**.
   La configurazione delle **Restrizioni** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
10. Nella pagina **Modifica profilo**, cliccare su **Salva** per salvare il profilo.

Il profilo viene visualizzato nella pagina **Profili e criteri** ed è disponibile per essere trasferito sui dispositivi iOS.

All'occorrenza, creare profili aggiuntivi per: impostazioni di account per Exchange, impostazioni VPN, impostazioni Wi-Fi e installazione di certificati root e client.

15.2 Creazione di un bundle delle operazioni per profili iOS

1. Nella barra laterale dei menù, sotto **CONFIGURA**, cliccare su **Bundle delle operazioni > iOS**.
2. Nella pagina **Bundle delle operazioni**, cliccare su **Crea bundle delle operazioni**.
   Verrà visualizzata la pagina **Modifica bundle delle operazioni**.
3. Inserire nei campi corrispondenti nome e, opzionalmente, una descrizione per il nuovo bundle delle operazioni.

   Il numero della versione viene incrementato automaticamente a ogni salvataggio del bundle delle operazioni.
4. Richiesto: Selezionare **Selezionabile per effettuare azioni di conformità** per trasferire il bundle delle operazioni su un dispositivo, quando viola una regola di conformità. Vedere Criteri di conformità (pagina 19).

   Nota
   Questa opzione è disattivata durante la modifica di bundle delle operazioni esistenti, o nel caso in cui il bundle delle operazioni sia già utilizzato per effettuare azioni di conformità.
5. Richiesto: Per i bundle delle operazioni iOS, selezionare **Ignora errori di installazione delle app** per procedere all'elaborazione del bundle delle operazioni anche se non dovesse essere possibile installare un'app.

   Questa opzione è disattivata quando il bundle delle operazioni non contiene alcuna operazione **Installa app**.
6. Cliccare su **Crea operazione**, selezionare **Registrati** e inserire un nome per l'operazione. Cliccare su **Applica** per creare l'operazione.

   È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.
7. Cliccare nuovamente su **Crea operazione** e selezionare **Installa profilo o assegna criterio**. Attribuire all'operazione un nome significativo, ad esempio `Installa profilo per i criteri della password`, e selezionare il profilo creato. Cliccare su **Applica** per creare l'operazione.
8. Se sono stati configurati profili per le impostazioni di Exchange, VPN o Wi-Fi, ripetere questo passaggio per ciascun profilo.
9. Richiesto: Aggiungere altre operazioni al bundle delle operazioni.

Consiglio
È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.

10. Una volta aggiunte tutte le operazioni necessarie al bundle delle operazioni, cliccare su **Salva** nella pagina **Modifica bundle delle operazioni**.

Il bundle delle operazioni sarà ora disponibile per il trasferimento e verrà visualizzato nella pagina **Bundle delle operazioni**.

16 Configurazione dei dispositivi Android

16.1 Creazione di un profilo per dispositivi Android

In questa sezione si descrive la creazione di un profilo per la configurazione iniziale dei dispositivi Android.

Si consiglia di impostare profili separati per:

- Criteri e restrizioni della password
- Impostazioni di account per Exchange (se richiesto)
- Impostazioni VPN (se richiesto)
- Impostazioni Wi-Fi (se richiesto)
- Certificati root e client (se richiesto)

1. Nella barra laterale del menù, sotto **CONFIGURA**, cliccare su **Profili, criteri > Android**.
2. Nella pagina **Profili e criteri**, cliccare su **Crea > Profilo del dispositivo**.
3. Nella pagina **Modifica profilo**, configurare le seguenti impostazioni:
   a) **Nome**: Inserire un nome per il profilo. Si consiglia di utilizzare il nome `Profilo SSP Android` per i profili applicati durante la registrazione tramite Portale self-service.
   b) Richiesto: **Descrizione**: Inserire una descrizione per il profilo, ad esempio `profilo di base`.
4. Per aggiungere criteri per la password al profilo, cliccare su **Aggiungi configurazione**, selezionare **Criteri password**.
   Viene visualizzata la pagina **Criteri password**.
5. Sotto **Tipo di password**, indicare il tipo di password che si desidera definire, ad esempio **Complesso**.
6. Configurare le impostazioni della password richieste.
   Le impostazioni disponibili dipendono dal tipo di password selezionato. Per una descrizione dettagliata de tutte le impostazioni, cliccare su **?** nell'intestazione della pagina.
7. Per salvare le impostazioni, cliccare su **Applica**.
   La configurazione dei **Criteri password** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
8. Per aggiungere restrizioni, cliccare su **Aggiungi configurazione**, selezionare **Restrizioni**.
9. Nella pagina **Restrizioni**, selezionare la restrizione richiesta.
   Alcune restrizioni richiedono tipi di dispositivo o versioni di Android specifici. Questi requisiti vengono visualizzati sulla destra, accanto a ciascuna restrizione.
   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.
10. Per salvare le impostazioni, cliccare su **Applica**.
    La configurazione delle **Restrizioni** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
11. Nella pagina **Modifica profilo**, cliccare su **Salva** per salvare il profilo.

Il profilo viene visualizzato nella pagina **Profili e criteri**, ed è disponibile per essere trasferito sui dispositivi Android.

All'occorrenza, creare profili aggiuntivi per: impostazioni di account per Exchange, impostazioni VPN, impostazioni Wi-Fi e installazione di certificati root e client.

16.2 Creazione di un bundle delle operazioni per dispositivi Android

1. Nella barra laterale del menù, sotto **CONFIGURA**, cliccare su **Bundle delle operazioni > Android**.
2. Nella pagina **Bundle delle operazioni**, cliccare su **Crea bundle delle operazioni**.
   Verrà visualizzata la pagina **Modifica bundle delle operazioni**.
3. Inserire nei campi corrispondenti nome e, opzionalmente, una descrizione per il nuovo bundle delle operazioni.

   Il numero della versione viene incrementato automaticamente a ogni salvataggio del bundle delle operazioni.
4. Richiesto: Selezionare **Selezionabile per effettuare azioni di conformità** per trasferire il bundle delle operazioni su un dispositivo, quando viola una regola di conformità. Vedere Criteri di conformità (pagina 19).

   Nota
   Questa opzione è disattivata durante la modifica di bundle delle operazioni esistenti, o nel caso in cui il bundle delle operazioni sia già utilizzato per effettuare azioni di conformità.
5. Richiesto: Per i bundle delle operazioni iOS, selezionare **Ignora errori di installazione delle app** per procedere all'elaborazione del bundle delle operazioni anche se non dovesse essere possibile installare un'app.

   Questa opzione è disattivata quando il bundle delle operazioni non contiene alcuna operazione **Installa app**.
6. Cliccare su **Crea operazione**, selezionare **Registrati** e inserire un nome per l'operazione. Cliccare su **Applica** per creare l'operazione.

   È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.
7. Cliccare nuovamente su **Crea operazione** e selezionare **Installa profilo o assegna criterio**. Attribuire all'operazione un nome significativo, ad esempio `Installa profilo per i criteri della password`, e selezionare il profilo creato. Cliccare su **Applica** per creare l'operazione.
8. Se sono stati configurati profili per le impostazioni di Exchange, VPN o Wi-Fi, ripetere questo passaggio per ciascun profilo.
9. Richiesto: Aggiungere altre operazioni al bundle delle operazioni.

   Consiglio
   È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.
10. Una volta aggiunte tutte le operazioni necessarie al bundle delle operazioni, cliccare su **Salva** nella pagina **Modifica bundle delle operazioni**.

Il bundle delle operazioni sarà ora disponibile per il trasferimento e verrà visualizzato nella pagina **Bundle delle operazioni**.

17 Aggiornamento delle impostazioni del portale self-service

Una volta creati bundle delle operazioni da trasferire quando gli utenti registrano i propri dispositivi nel portale self-service, occorre aggiornare le impostazioni del portale self-service con le necessarie impostazioni di gruppo:

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Portale self-service**, e successivamente cliccare sulla scheda **Impostazioni gruppo**.
2. Cliccare sull'impostazione del gruppo **Predefinita**.
   Si aprirà la finestra di dialogo **Modifica impostazioni gruppo**.
3. Negli elenchi **Pacchetto iniziale - dispositivi aziendali** e **Pacchetto iniziale - dispositivi personali**, selezionare i bundle delle operazioni creati per i dispositivi Android e iOS.
4. Selezionare la casella di spunta **Attiva** per le piattaforme che si desidera rendere disponibili nel portale self-service:
5. Nell'elenco **Aggiungi al gruppo di dispositivi**, selezionare il gruppo al quale saranno aggiunti i dispositivi quando ne viene effettuata la registrazione nel portale self-service.
6. Cliccare su **Applica**.
7. Nella scheda **Impostazioni gruppo**, cliccare su **Salva**.

18 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.

Nota

La procedura presume che il cliente sia stato creato con la gestione degli utenti interni, vedere Creazione di un cliente (pagina 10). Per informazioni sulla gestione esterna degli utenti, consultare la *Guida per super administrator di Sophos Mobile*.

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

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Utenti**, e successivamente su **Crea utente**.
2. Configurare i dovuti dettagli dell'account.
   Verificare che il campo **Invia e-mail di registrazione** sia selezionato.
3. Cliccare su **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 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 28), ed effettuare registrazioni di prova per tutte le piattaforme che si desidera gestire con Sophos Mobile.

20 Importazione degli utenti su Sophos Mobile

Una volta effettuato il test di registrazione 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.

Per informazioni sulla gestione esterna degli utenti, consultare la *Guida per super administrator di Sophos Mobile*.

È possibile aggiungere nuovi utenti del portale self-service importando un file con valori delimitati da virgole (CSV) e con codifica UTF-8 che può includere sino a un massimo di 300 utenti.

Nota

Utilizzare un editor di testo per apportare modifiche al file CSV. Se si utilizza Microsoft Excel, i valori inseriti potrebbero non essere risolti in modo corretto. Verificare che il file venga salvato con l'estensione `.csv`.

Consiglio

Un file di esempio, in cui vengono riportati i nomi e l'ordine corretto delle colonne, è scaricabile dalla pagina **Importa utenti**.

Per importare gli utenti da un file CSV:

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Utenti**, e successivamente su **Importa utenti**.
2. Nella pagina **Importa utenti**, selezionare **Invia e-mail di registrazione**.
3. Cliccare su **Carica file** e navigare sul file CSV preparato in precedenza.
   Le voci verranno lette dal file e visualizzate.
4. 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.
5. Cliccare su **Fine** per creare gli account utente.

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

21 Utilizzo della procedura guidata di registrazione del dispositivo per assegnare e registrare nuovi dispositivi

I nuovi dispositivi possono essere registrati in maniera molto semplice, grazie alla procedura guidata di registrazione dei dispositivi. 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.
- Facoltativa: Trasferisce un bundle delle operazioni al dispositivo.

Per avviare la procedura guidata di registrazione del dispositivo:

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Dispositivi**, e successivamente su **Aggiungi > Procedura guidata di registrazione**.

> **Consiglio**
> In alternativa, la procedura guidata può essere avviata dalla pagina **Pannello di controllo**, cliccando sul widget **Aggiungi dispositivo**.

2. Nella pagina **Inserisci parametri di ricerca utente** della procedura guidata, è possibile inserire 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. Una volta inserito un criterio di ricerca, la procedura guidata visualizzerà un elenco di utenti che hanno riscontrato una corrispondenza. Selezionare l'utente desiderato.
4. Nella pagina **Dettagli dispositivo** della procedura guidata, configurare le seguenti impostazioni:

Opzione	Descrizione
Piattaforma	La piattaforma del dispositivo. È possibile selezionare solamente una piattaforma che sia abilitata per il cliente selezionato in fase di accesso.
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.

Opzione	Descrizione
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. Selezionare un bundle delle operazioni da trasferire sul dispositivo dopo la registrazione. In alternativa, selezionare **Registra solo il dispositivo** per registrare il dispositivo senza trasferire un bundle delle operazioni.
   Cliccando su **Avanti**, il dispositivo verrà aggiunto a Sophos Mobile.
6. Nella pagina della procedura guidata **Registrazione**, seguire le istruzioni per completare il processo di registrazione.

Nota
Nei Mac, la procedura di registrazione deve essere effettuata dall'utente che sarà gestito da Sophos Mobile. Per installare il profilo di registrazione, l'utente deve immettere una password di amministrazione.

7. Una volta completata la registrazione, cliccare su **Fine** per chiudere la procedura guidata di registrazione del dispositivo.

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

cliente	Colui che gestisce il dispositivo.
dispositivo	Il dispositivo da gestire (ad es. smartphone, tablet o dispositivo Windows 10).
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.
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.
Licenza Mobile Advanced	Con una licenza di tipo Mobile Advanced è possibile gestire le app Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email con Sophos Mobile.
SMSec	Acronimo di Sophos Mobile Security.
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 Mobile Security	Un'app di protezione per i dispositivi Android. 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 contenitore 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.

23 Supporto tecnico

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 che hanno riscontrato lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto su www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket col team di supporto su https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

24 Note legali

Ultimo aggiornamento: 20171212