SOPHOS

Cybersecurity made simple.

Sophos Mobile

guida di avvio (on-premise)

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.

Queste descrizioni sono applicabili alle installazioni on-premise di Sophos Mobile.

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

2 Licenze Sophos Mobile

Sophos Mobile offre due tipi di licenza:

- Licenza Mobile Standard
- Licenza di Mobile Advanced

Con una licenza di tipo Mobile Advanced è possibile gestire Sophos Intercept X for Mobile ,Sophos Secure Workspace e Sophos Secure Email.

Per ulteriori informazioni, consultare la Guida 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 per amministratori di Sophos Mobile.

2.3 Aggiornamento delle licenze

Per aggiornare le licenze, occorre attivare la nuova chiave di licenza in Sophos Mobile Admin.

3 Passaggi chiave

Per cominciare ad utilizzare Sophos Mobile:

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

   Nota
   La procedura guidata di **I primi passi** 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 che consenta di gestire iPhone, iPad e Mac.
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 Configurazione delle impostazioni di sistema

Quando si effettua l'accesso a Sophos Mobile Admin per la prima volta dopo l'installazione, viene avviata la procedura guidata **I primi passi**, che offre assistenza durante la configurazione delle impostazioni di sistema.

Occorre fornire le seguenti informazioni:

- L'indirizzo del server proxy HTTP (se applicabile).
- La chiave di licenza di Sophos Mobile.
- I certificati SSL/TLS.
- Le credenziali del server SMTP.

Nota
Tutte le impostazioni possono essere modificate in un secondo momento, selezionando **Impostazione > Impostazione Sophos**.

1. Nella pagina **Proxy HTTP**, immettere l'indirizzo e la porta di un server proxy da utilizzare per le connessioni HTTP e SSL/TLS in uscita.
2. Nella pagina **Licenze**, immettere la chiave di licenza o richiedere una licenza di prova gratuita:
   - **Chiave di licenza Standard**: Immettere la chiave di licenza di Mobile Standard e cliccare su **Attiva**.
   - **Chiave di licenza Advanced**: Immettere la chiave di licenza di Mobile Advanced e cliccare su **Attiva**. Occorre prima immettere una chiave di licenza Mobile Standard.
   - **Richiedi prova**: Immettere l'indirizzo e-mail utilizzato per scaricare il programma di installazione di Sophos Mobile dal sito web di Sophos.
3. Nella pagina **SSL/TLS**, configurare i certificati SSL/TLS utilizzati per proteggere le connessioni tra il server di Sophos Mobile e i client.
   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) Se i certificati non vengono individuati in maniera automatica, caricarli manualmente: Cliccare su **Carica file** e selezionare il file di certificato con codifica CER o DER.

   È possibile configurare fino a quattro certificati perché, a seconda della struttura della rete, potrebbero essere presenti certificati diversi per i client che si connettono da internet o dalla rete 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").

Attenzione
Aggiornare l'elenco dei certificati dopo la modifica o il rinnovo dei 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 pagina **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 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.
Nuovo destinatario 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 le informazioni di SMTP, cliccare su **Invia e-mail di test** per verificare la configurazione della posta elettronica.
6. Cliccare su **Fine** per chiudere la procedura guidata **I primi passi**.

6 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.

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 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.

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.

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.

  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 dei menù, sotto **GESTISCI**, cliccare su **Clienti**.
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	Se questa opzione è selezionata, il cliente può gestire Sophos Intercept X for Mobile, 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.
Impostazioni di privacy del dispositivo	Selezionare **Consenti agli utenti di localizzare i dispositivi** per consentire agli utenti di individuare la posizione dei propri dispositivi in caso di furto o smarrimento. Selezionare **Consenti agli amministratori di localizzare i dispositivi** per consentire agli amministratori di individuare la posizione dei dispositivi. Selezionare **Mostra app installate** per mostrare le app installate nei dettagli del dispositivo.
Clona impostazioni	Selezionare la casella di controllo **Impostazioni e pacchetti** se si desidera che tutti i criteri, 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:

Opzione	Descrizione
	• **Nessuna. Non è disponibile alcun criterio 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. • **Directory interna**: abilita la gestione degli utenti interni per Sophos Mobile Admin e il portale self-service. Per ulteriori informazioni, consultare la Guida 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. Selezionare **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 **ImpostazioneAmministratori**.
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

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. Accedere a Sophos Mobile Admin con l'account di amministrazione creato per il nuovo cliente.
2. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale** e successivamente sulla scheda **Personale**.
3. 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.

4. Selezionare **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.

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**.

11.3 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**.

12 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.

12.1 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

12.2 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` e il nome del cliente di Sophos Mobile. Per esempio:

   ```
   Nome organizzazione (Sophos Mobile/Nome cliente)
   ```

   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.

13 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.

13.1 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. Il file di richiesta di firma del certificato è univoco per il cliente attuale.
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**.

14 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.

14.1 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 il super administrator ha configurato una connessione al proxy EAS interno o standalone. Consultare la Guida per super administrator di Sophos Mobile (in inglese). 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 il super administrator ha configurato Network Access Control (controllo dell'accesso alla rete). Consultare la Guida per super administrator di Sophos Mobile (in inglese). 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.

15 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.

15.1 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**.

16 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.

17 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.

18 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.

19 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.

20 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 9). 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 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.

21 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.

22 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.

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

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.

Informazioni correlate
Guida in linea per super amministratori di Sophos Mobile

23 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. 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.
Proprietario	Selezionare il tipo di proprietario del dispositivo: **Aziendale** o **Personale**.

Opzione	Descrizione
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.

24 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.
cliente	Un cliente rappresenta un ambito di gestione separato all'interno di Sophos Mobile. È possibile impostare clienti diversi e gestirne i dispositivi in maniera indipendente. Questa struttura viene anche detta *multi-tenant*.
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.

25 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.

26 Note legali