SOPHOS

Cybersecurity made simple.

Sophos Mobile

Guida all'installazione

Versione prodotto: 9.6

Sommario

1 Informazioni sulla guida

Questa guida descrive i processi di installazione e impostazione di Sophos Mobile 9.6. Inoltre, indica come aggiornare installazioni già esistenti di Sophos Mobile.

A meno che non venga diversamente specificato, tutte le procedure devono essere svolte effettuando l'accesso come amministratore di Microsoft Windows Server, oppure come utente del gruppo interessato.

2 Informazioni su Sophos Mobile

Sophos Mobile

Sophos Mobile è la soluzione di EMM per le aziende che desiderano minimizzare il tempo e l'impegno da investire in gestione e protezione dei dispositivi. Permette di gestire i dispositivi mobili con la semplicissima interfaccia unificata e basata sul web Sophos Central Admin, insieme alla sicurezza by Sophos per endpoint, rete o server. App container e supporto dell'uso dei container per iOS, iPadOS, Android Enterprise e Samsung Knox garantiscono la separazione dei dati aziendali da quelli personali nel dispositivo.

Con protezione dei dati di primissima classe, sicurezza completa, un ottimo rapporto qualità-prezzo e opzioni di gestione flessibili, Sophos Mobile è il modo migliore per autorizzare l'uso dei dispositivi mobili sul posto di lavoro, pur garantendo massimi livelli di produttività degli utenti, sicurezza dei dati aziendali, e riservatezza dei dati personali.

Sophos Intercept X for Mobile

Sophos Intercept X for Mobile protegge i dispositivi mobili senza incidere sulla performance e sulla durata della batteria. Grazie alle tecnologie antimalware leader di settore by Sophos, Sophos Intercept X for Mobile offre un livello pluripremiato di protezione antimalware e antivirus, oltre a: rilevamento delle app potenzialmente indesiderate (PUA), Privacy e Security Advisor, protezione contro furto e smarrimento dei dispositivi, protezione web e molto altro ancora.

Sophos Secure Workspace

Sophos Secure Workspace è un'app basata sui container; offre un metodo sicuro per proteggere, gestire e distribuire documenti e contenuti web aziendali. I documenti Office possono essere modificati senza uscire dall'ambiente del container, per garantire la sicurezza dei contenuti cifrati. L'antiphishing protegge gli utenti da link e contenuti malevoli nei documenti.

Se gestita con Sophos Mobile, permette agli amministratori di limitare l'accesso ai contenuti secondo le regole di conformità dei dispositivi. Con Sophos SafeGuard Encryption, Sophos Secure Workspace garantisce l'invio trasparente di file cifrati (archiviati localmente o nel cloud) tra utenti Windows, Mac, iPhone, iPad e Android.

Sophos Secure Email

Sophos Secure Email è un'app a funzionalità complete sicura e basata sui container che, quando gestita da Sophos Mobile, consente di isolare e-mail, calendario e contatti aziendali dai dati personali in un dispositivo mobile. Tutte le informazioni aziendali sono protette con cifratura AES-256, ed è possibile revocare i diritti di accesso secondo le regole di conformità del dispositivo. Inoltre, Sophos Secure Email permette al personale IT di effettuare il provisioning della posta aziendale in maniera sicura e omogenea su dispositivi e sistemi operativi diversi.

3 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.

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.

3.1 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.

3.2 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.

3.3 Aggiornamento delle licenze

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

4 Impostazione di Sophos Mobile

Questa sezione spiega come installare il nuovo server di Sophos Mobile. Per informazioni su come aggiornare un'installazione già esistente, vedere Aggiornamento di Sophos Mobile (pagina 26).

4.1 Prerequisiti per l'installazione

Verificare i seguenti prerequisiti, prima di installare il server di Sophos Mobile:

- Aver letto la Sophos Mobile Guida alla distribuzione di Server. Questo documento contiene esempi di architettura per l'integrazione del server di Sophos Mobile nell'infrastruttura della propria organizzazione, nonché linee guida per la scelta della giusta soluzione e un elenco delle porte e dei protocolli di rete richiesti.
- Aver letto le Sophos Mobile Note di rilascio e verificato che il computer che ospita il server di Sophos Mobile, i dispositivi che si desidera gestire e altri componenti utili siano supportati da Sophos Mobile.
- Avere un certificato SSL/TLS per il server di Sophos Mobile.
- Nel computer server non deve essere installato alcun server web Internet Information Services (IIS) o altra applicazione che utilizzi le porte 80 o 443.
- Il nome DNS del computer server deve poter essere risolto su internet.
- Devono essere presenti uno o più gruppi LDAP contenenti gli utenti autorizzati a utilizzare il portale self-service, se gli account utente sono memorizzati in una directory LDAP.

Prerequisiti se si desidera gestire il database di Sophos Mobile con un server di database già esistente:

- Microsoft SQL Server o Microsoft SQL Server Express:
  - Occorre utilizzare l'autenticazione Windows o l'autenticazione SQL Server.
  - TCP/IP deve essere attivato.
  - Il servizio SQL Server Browser deve essere abilitato.
  - La lingua impostata nell'account utilizzato per accedere a SQL deve essere l'inglese.
- Microsoft SQL Server Express:
  - Devono essere installati gli strumenti di gestione di SQL.

Attività correlate

Richiesta di un certificato SSL/TLS (pagina 5)
Inclusa tra i file del prodotto Sophos, si trova la procedura guidata "SSL Certificate Wizard" per la richiesta del certificato SSL/TLS per il proxy di EAS di Sophos Mobile.

Informazioni correlate

Guida alla distribuzione di Server di Sophos Mobile (in inglese)
Sophos Mobile Note di rilascio

4.2 Requisiti di sistema dell’ambiente

Il programma di installazione di Sophos Mobile esegue una serie di test per verificare che l'ambiente di sistema soddisfi tutti i requisiti di Sophos Mobile.

Requisiti obbligatori

Il programma di installazione di Sophos Mobile si avvia solamente se vengono soddisfatti i seguenti requisiti:

- Deve essere stato effettuato l'accesso al computer con un account amministratore locale.
- Il sistema operativo del computer utilizzato deve essere supportato da Sophos Mobile.
- Il computer deve avere come minimo una scheda di rete.
- Il computer deve disporre di almeno 4 GB di RAM.
- Il server web di Microsoft Internet Information Services (IIS) deve essere disattivato nel computer utilizzato.
- Le porte HTTP/S 80, 443 e 818 devono essere disponibili nel computer.
- Il computer deve essere in grado di connettersi ai seguenti servizi web:
  - Apple Push Notification service (APNs)
  - Google Firebase Cloud Messaging (FCM)
  - Google reCAPTCHA
  - Windows Push Notification Services (WNS)
  - Servizi Sophos

Requisiti opzionali

Alcune funzionalità di Sophos Mobile sono disponibili solo se il computer è in grado di connettersi ai seguenti servizi web:

- Apple Volume Purchase Program (VPP)
- Apple iTunes
- Bypass del blocco attivazione Apple
- Apple Device Enrollment Program (DEP)
- Google Android Enterprise
- Microsoft Azure
- TeamViewer

4.3 Richiesta di un certificato SSL/TLS

Inclusa tra i file del prodotto Sophos, si trova la procedura guidata “SSL Certificate Wizard” per la richiesta del certificato SSL/TLS per il proxy di EAS di Sophos Mobile.

Eseguire la procedura guidata dalla cartella *%MDM_HOME%*\tools\Wizard, oppure scaricarla da www.sophos.it/mysophos.

Nota
Se si utilizza un certificato autofirmato o un certificato emesso dalla propria autorità di certificazione (Certificate Authority, CA), verranno applicate le seguenti restrizioni:

- Occorre installare manualmente il certificato autofirmato o il certificato della propria CA nei dispositivi, prima di effettuarne la registrazione a Sophos Mobile. Se non si dovesse procedere come indicato, l'app Sophos Mobile Control non riterrà il server come attendibile e rifiuterà la connessione. I certificati emessi da un'autorità di certificazione attendibile a livello globale non richiedono l'installazione manuale di cui sopra.
- Le app Android non possono essere installate da file APK ospitati nel server di Sophos Mobile.
- Non è possibile utilizzare la registrazione Zero Touch di Android o il Samsung Knox Mobile Enrollment.
- Se si utilizza un certificato autofirmato che non è stato creato dalla procedura guidata di configurazione di Sophos Mobile o dalla procedura guidata dei certificati SSL, attenersi alle istruzioni indicate nell'articolo di Apple Requisiti per i certificati attendibili in iOS 13 e macOS 10.15.

Per richiedere il certificato SSL/TLS:

- Eseguire il file Sophos Mobile SSL Certificate Wizard.exe per avviare la procedura guidata "SSL Certificate Wizard".

  La procedura guidata è una guida passo dopo passo che vi segue durante l'intero processo di installazione. Inserire le informazioni richieste, tenendo presente le seguenti istruzioni:

  a) Nella pagina **Upload CSR**, è possibile cliccare sul pulsante **Open CSR** per aprire il file CSR, se il vendor del certificato supporta la funzione copia e incolla.

  b) Nella pagina **Import Certificate Files**, inserire nel campo **Select CA certificate file** il certificato CA scaricato nella pagina **Upload CSR**.

  c) Nella pagina **Certificate created**, viene mostrato il percorso del certificato. Occorrerà fare riferimento a questo percorso durante l'impostazione di Sophos Mobile.

Nota
Si consiglia di creare un backup della cartella contenente i file dei certificati.

Informazioni correlate
Requisiti per i certificati attendibili in iOS 13 e macOS 10.15 (collegamento esterno)

4.4 Installazione e impostazione del server di Sophos Mobile

Prerequisiti:

- Se si intende connettere Sophos Mobile a un database già esistente, verificare di essere in possesso delle credenziali di accesso per il database disponibile, prima di avviare l'installazione; accertarsi inoltre di possedere tutte le autorizzazioni necessarie per creare nuovi archivi di dati, account utente e record di dati.

- Se il database non è memorizzato localmente, è necessario avere accesso alla porta di connessione del server del database. Le porte predefinite sono TCP 1433 per Microsoft SQL Server e TCP 3306 per MySQL. Inoltre, sarà necessario disporre di un account con privilegi di amministrazione che possa essere utilizzato dal server di Sophos Mobile per accedere al database.

1. Accedere a Windows con un account utente che disponga di diritti di amministratore locale.
2. Avviare il programma di installazione di Sophos Mobile.
3. Nella pagina **System Property Checks**, cliccare su **Check** per eseguire test che verificheranno se l'ambiente del sistema soddisfa tutti i requisiti necessari per Sophos Mobile. Vedere Requisiti di sistema dell'ambiente (pagina 5).

   È possibile cliccare su **Report** per generare un report dei risultati del test.
4. Nella pagina **Choose Install Location**, selezionare la cartella di destinazione del server di Sophos Mobile.
5. Nella pagina **Database Type Selection**, selezionare il tipo di database che si desidera utilizzare:
   - **Install and use Microsoft SQL Server Express**: Installa Microsoft SQL Server Express, e lo configura per l'uso con Sophos Mobile.
   - **Use existing Microsoft SQL Server installation**: utilizza l'installazione attuale di Microsoft SQL Server e crea un nuovo database per Sophos Mobile.
   - **Use existing MySQL installation**: utilizza l'installazione attuale di MySQL e crea un nuovo database per Sophos Mobile.
6. Nella pagina **Database Settings**, inserire le credenziali di accesso per il database.

   Nota
   Se si seleziona l'opzione **Use SQL Server Authentication**, occorrerà accertarsi che la lingua di accesso di SQL sia impostata su Inglese. Vedere Modifica della lingua per l'accesso a SQL (pagina 10) per informazioni dettagliate.

7. Nella pagina **Database Selection**, cliccare su **Create a new database named** e inserire un nome per il database che verrà creato, ad es. SMCDB.
8. Nella pagina **Database Configuration**, vengono visualizzati i messaggi di stato relativi alla creazione del database.
   Una volta terminata la creazione e il popolamento del database, cliccare su **Next** per continuare.
9. Se per l'accesso al database è stata selezionata l'autenticazione con Windows, sarà presente una pagina **Set service credentials**, nella quale è possibile impostare l'account Windows nel quale eseguire Sophos Mobile.

   È possibile utilizzare l'account di sistema locale, oppure un account utente. Nel caso si scegliesse quest'ultimo, immettere l'account utente come `<nome computer>\<nome utente>` oppure come `<dominio>\<nome utente>`.

   Il programma di installazione attribuirà diritti di accesso al database all'account specificato.

Nota
Per motivi di sicurezza, si consiglia di eseguire il servizio Sophos Mobile come utente con diritti di accesso limitati. L'account utente deve avere le seguenti proprietà:

- L'account utente deve essere un account locale di Windows nel computer sul quale è installato Sophos Mobile.
- L'utente non deve essere membro di alcun gruppo, neppure del gruppo *utenti*.
- L'utente deve essere in grado di accedere al database di SQL con i necessari diritti di modifica. Per un database MS-SQL, ciò significa che l'utente deve essere membro dei ruoli *db_datareader* e *db_datawriter*.

10. Nella pagina **Configure super admin account**, configurare i dettagli dell'account del super administrator.

    Il ruolo del super administrator è principalmente quello di gestire i clienti, e non deve essere utilizzato per le normali operazioni di gestione dei dispositivi. Il super administrator effettua l'accesso al cliente super administrator e può, ad esempio, predefinire le impostazione dei nuovi clienti e implementare il push di impostazioni e configurazioni sui dispositivi dei clienti già esistenti. Per ulteriori informazioni, consultare la Guida per super administrator di Sophos Mobile (in inglese).

    Nota
    Le credenziali del super administrator sono richieste per il primo accesso a Sophos Mobile Admin. Dopo l'installazione, è possibile aggiungere altri super administrator in Sophos Mobile Admin.

11. Nella pagina **Configure external server name**, inserire un nome server per Sophos Mobile (ad es. smc.mycompany.com).

    Nota
    Il nome server deve essere risolvibile dai dispositivi gestiti.

12. Nella pagina **Configure server certificate**, importare un certificato per l'accesso sicuro (HTTPS) al server web.
    - Se si dispone di un certificato attendibile, cliccare su **Import a certificate from a trusted issuer** e selezionare un'opzione dall'elenco a discesa.
    - Se ancora non si dispone di un certificato attendibile, selezionare **Create self-signed certificate**.

    Nota
    Inclusa tra i file del prodotto Sophos, si trova la procedura guidata "SSL Certificate Wizard", che può essere utilizzata per richiedere il certificato SSL/TLS per Sophos Mobile. Vedere Richiesta di un certificato SSL/TLS (pagina 5).

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

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

14. Nella pagina **Server Information**, verificare le informazioni del server, e successivamente cliccare su **Next** per confermare il server e il processo di configurazione.
15. Una volta terminata l'installazione, verrà visualizzata la casella di dialogo **Sophos Mobile Control - Installation finished**. Verificare che la casella di controllo **Start Sophos Mobile server now** sia selezionata, e cliccare su **Finish** per avviare il servizio Sophos Mobile per la prima volta.

Nota
Una volta avviato il servizio, potrebbero trascorrere alcuni minuti prima che l'interfaccia web di Sophos Mobile risulti disponibile.

Una volta terminata l'installazione, si dovrà seguire una breve procedura per la configurazione iniziale:

- Configurare il server web di Sophos Mobile in modo che accetti solamente le richieste dirette al proprio nome di dominio. Vedere Configurazione del server web di Sophos Mobile (pagina 9).
- Accedere a Sophos Mobile Admin per la prima volta, per avviare la procedura guidata **I primi passi**. Consultare la Guida di avvio di Sophos Mobile.
- Per iPhone, iPad e Mac, occorre ottenere un certificato Apple Push Notification service. Consultare la Guida di avvio di Sophos Mobile.
- Opzionalmente, è possibile impostare un proxy di EAS standalone per il filtraggio delle e-mail. Vedere Proxy EAS standalone (pagina 11).

4.5 Configurazione del server web di Sophos Mobile

Sophos Mobile include un componente server web che fornisce i contenuti delle applicazioni web Sophos Mobile Admin e Self Service Portal (portale self-service). Il server web può essere configurato e modificato in base alle esigenze del proprio ambiente.

Le richieste a un server web includono, nell'intestazione, un campo Host in cui viene specificata l'applicazione web che deve elaborare la richiesta. Potenzialmente, gli autori degli attacchi possono manipolare il valore di questo campo Host in modo da provocare un comportamento non previsto.

Dopo l'installazione, il componente server web di Sophos Mobile non verifica il valore del campo Host. Si consiglia di configurare il server web in modo che accetti solamente le richieste dirette al proprio nome di dominio.

1. Sul computer in cui è installato il server di Sophos Mobile, eseguire lo script *%MDM_HOME%*`\tools\HostValidationUndertowFilter\addModule.bat`

   Sostituire *%MDM_HOME%* con la propria cartella di installazione di Sophos Mobile.

2. Aprire il file *%MDM_HOME%*\wildfly\standalone\configuration\smc-config.xml in un editor di testo e cercare questa sezione:

```
<filter name="hostheadervalidation" ...>
    <param name="allowedHosts" value="localhost"/>
</filter>
```

3. Dopo localhost, aggiungere il nome di dominio utilizzato per Sophos Mobile Admin e per il portale self-service.

   Ad esempio, se il proprio nome di dominio è smc.esempio.com, modificare questa riga come segue:

```
<param name="allowedHosts" value="localhost,smc.esempio.com"/>
```

   Se il server di Sophos Mobile è accessibile tramite più di un nome di dominio, inserire tutti i nomi, separandoli con virgole.

4. Salvare il file smc-config.xml
5. Riavviare il servizio Sophos Mobile.

4.6 Modifica della lingua per l'accesso a SQL

Se il server di Sophos Mobile è stato configurato in modo da utilizzare l'autenticazione tramite SQL Server per connettersi al database, la lingua di accesso di SQL deve essere impostata su Inglese. Altrimenti si verificherà un errore all'avvio del servizio Sophos Mobile.

Questa sezione descrive come modificare la lingua di accesso a SQL e impostarla su Inglese.

1. Arrestare il servizio Sophos Mobile.
2. Aprire SQL Server Management Studio sul server, e selezionare **Sicurezza > Accessi**.
3. Nella pagina **Generali** delle **Proprietà account di accesso**, impostare la **Lingua predefinita** su Inglese, e successivamente cliccare su **OK** per salvare le modifiche.
4. Riavviare il servizio Sophos Mobile.

5 Proxy EAS standalone

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

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

Esistono due tipi di proxy di EAS:

- Il proxy di EAS interno, che viene installato automaticamente con Sophos Mobile. Supporta il traffico di ActiveSync in entrata che viene utilizzato da Microsoft Exchange o IBM Notes Traveler per dispositivi iOS e Samsung Knox.
- Un proxy di EAS standalone, che può essere scaricato e installato separatamente. Comunica con il server di Sophos Mobile attraverso un'interfaccia web HTTPS.

Per un elenco dei server di posta supportati dal proxy di EAS standalone, vedere le Note di rilascio di Sophos Mobile.

Nota
Per questioni di performance, si consiglia di utilizzare il server proxy di EAS standalone, al posto della versione interna, per gestire il traffico e-mail di più di 500 dispositivi client.

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

Funzionalità

Il proxy EAS standalone dispone di funzionalità aggiuntive rispetto alla versione interna:

- Supporto di IBM Notes Traveler per dispositivi non iOS (ad esempio Android). Per questi dispositivi, il client di Traveler adopera un protocollo (non ActiveSync) che non è supportato dal proxy di EAS interno.
- Supporto di server di posta elettronica Microsoft Exchange o IBM Notes Traveler multipli. È possibile impostare un'istanza di proxy di EAS per ciascun server di posta.
- Supporto di bilanciatori del carico. È possibile impostare istanze di proxy di EAS standalone su computer diversi, per poi utilizzare un bilanciatore del carico per distribuire tra di esse le richieste del client.
- Supporto dell'autenticazione al client basata su certificato. È possibile selezionare, da un'autorità di certificazione (CA), un certificato dal quale devono essere derivati i certificati client.
- Supporto del controllo dell'accesso alle e-mail tramite PowerShell. In questo scenario, il servizio proxy EAS comunica con il server di posta tramite PowerShell per controllare l'accesso alle e-

mail dei dispositivi gestiti. Il traffico e-mail si verifica direttamente tra i dispositivi e i server di posta, senza essere reindirizzato tramite un proxy. Vedere Impostazione del controllo dell'accesso alle e-mail tramite PowerShell (pagina 16).

- Il proxy EAS ricorderà lo stato del dispositivo per 24 ore. Se il server di Sophos Mobile dovesse essere off-line, ad esempio in caso di aggiornamento, il traffico e-mail verrà filtrato in base all'ultimo stato conosciuto del dispositivo. Dopo 24 ore, l'intero traffico e-mail verrà bloccato.

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

5.1 Scenari di utilizzo del proxy di EAS

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

Utilizzare IBM Notes Traveler (precedentemente IBM Lotus Notes Traveler) per i dispositivi non iOS

Il proxy di EAS interno non è adatto a questo scenario, in quanto supporta solamente il protocollo ActiveSync, che viene utilizzato da Microsoft Exchange e da IBM Notes Traveler per i dispositivi iPhone e iPad. IBM Notes Traveler per dispositivi non-iOS (ad es. Android) adopera un protocollo diverso, che è supportato dal proxy di EAS standalone.

Per i dispositivi non-iOS si richiede un software client Traveler dedicato. Questo software è disponibile su `<traveler-server>/servlet/traveler`, oppure nel file system di Traveler. Le funzionalità *Installa App* e *Disinstalla App* di Sophos Mobile possono essere utilizzate per installare e disinstallare il software client Traveler. La configurazione deve essere effettuata manualmente.

Si desidera supportare server backend multipli

Con il proxy di EAS standalone è possibile impostare istanze multiple di sistemi backend per la posta elettronica. Ciascuna istanza richiede una porta TCP in entrata. Ciascuna porta può connettersi a un backend diverso. Occorre un URL per ciascuna istanza di proxy di EAS.

Si desidera impostare il bilanciamento del carico per EAS

È possibile impostare istanze di proxy EAS standalone su computer diversi, per poi utilizzare un bilanciatore del carico per distribuire tra di esse le richieste del client.

Questo scenario richiede la presenza di un bilanciatore del carico per HTTP che sia già esistente.

Si desidera usare l'autenticazione al client basata su certificato

Questo scenario richiede la presenza di una PKI già esistente; inoltre, occorre impostare la parte pubblica del certificato CA nel proxy di EAS.

Occorre gestire più di 500 dispositivi

Per questioni di performance, si consiglia di utilizzare il server proxy EAS standalone, al posto della versione interna, per gestire il traffico e-mail di più di 500 dispositivi client.

5.2 Download del programma di installazione del proxy di EAS

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

Il file di installazione verrà salvato nel computer locale.

5.3 Installazione del proxy EAS standalone

Prerequisiti:

- Aver installato e impostato Sophos Mobile.
- Tutti i server di posta richiesti devono essere accessibili. Il programma di installazione del proxy EAS non configurerà le connessioni ai server che non sono disponibili.
- Occorre aver effettuato l'accesso come amministratore sul computer in cui si intende installare il proxy EAS.

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

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

Se richiesto, selezionare **Use proxy server** per configurare un server proxy che il proxy di EAS dovrà utilizzare per connettersi al server di Sophos Mobile.

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

Opzionalmente, selezionare **Use client certificates for authentication** se si desidera che, per l'autenticazione, i client adoperino anche un certificato, oltre alle credenziali del proxy di EAS. Così facendo si aggiunge un ulteriore livello di sicurezza alla connessione.

Selezionare **Allow all certificates** se il server di Sophos Mobile presenta certificati variabili al proxy di EAS, ad esempio quando esistono diverse istanze di server dietro a un bilanciatore di carico, e ciascuna istanza adopera un certificato diverso. Quando è selezionata questa opzione, il proxy EAS accetterà qualsiasi certificato dal server di Sophos Mobile.

Attenzione
Poiché l'opzione **Allow all certificates** diminuisce il livello di sicurezza della comunicazione del server, si consiglia vivamente di selezionarla solamente se richiesta dall'ambiente di rete.

4. Se in precedenza è stata selezionata l'opzione **Use SSL for incoming connections (Clients to EAS Proxy)**, verrà visualizzata la pagina **Configure server certificate**. In questa pagina è possibile creare o importare un certificato per l'accesso sicuro (HTTPS) al proxy EAS.

   Nota
   Inclusa tra i file del prodotto Sophos, si trova la procedura guidata "SSL Certificate Wizard", che può essere utilizzata per richiedere il certificato SSL/TLS per il proxy di EAS di Sophos Mobile. Per ulteriori informazioni, vedere Richiesta di un certificato SSL/TLS (pagina 5).

   - Se ancora non si dispone di un certificato attendibile, selezionare **Create self-signed certificate**.
   - Se si dispone di un certificato attendibile, cliccare su **Import a certificate from a trusted issuer** e selezionare una delle seguenti operazioni dall'elenco:
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**
5. Nella pagina successiva, inserire le informazioni del certificato che riguardano il certificato selezionato.

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

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

   Quando un client cercherà di effettuare la connessione, il proxy di EAS verificherà se il certificato sia derivato dalla CA specificata in questo campo.
7. Nella pagina **EAS Proxy instance setup**, configurare una o più istanze del proxy di EAS.
   - **Instance type**: Selezionare **EAS proxy**.
   - **Instance name**: Un nome che identifica l'istanza.

- **Server port**: La porta del proxy EAS per il traffico e-mail in entrata. Se viene impostata più di un'unica istanza di proxy, ciascuna di esse dovrà utilizzare una porta diversa.
- **Require client certificate authentication**: I client di posta devono autentificarsi quando si connettono al proxy EAS.
- **ActiveSync server**: Il nome o indirizzo IP dell'istanza del server di Exchange ActiveSync a cui si connetterà l'istanza del proxy.
- **SSL**: La comunicazione tra l'istanza del proxy e il server di Exchange ActiveSync è protetta tramite SSL o TLS (a seconda della compatibilità del server).
- **Allow EWS (Sophos Secure Email)**: Autorizzare le richieste del client di posta all'interfaccia Servizi Web Exchange (EWS) del server di Exchange.

  Attivare questa impostazione solo se si utilizza Sophos Secure Email su iPhone e iPad.
- **Enable Traveler client access**: Selezionare questa casella di controllo solamente se si desidera autorizzare l'accesso ai client di IBM Notes Traveler da dispositivi non iOS.

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

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

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

10. Prendere nota della cartella del certificato. Questa informazione verrà richiesta in seguito, al momento di caricare il certificato su Sophos Mobile.
11. Richiesto: Cliccare nuovamente su **Add** per configurare ulteriori istanze del proxy EAS.
12. Una volta configurate tutte le istanze del proxy EAS richieste, cliccare su **Next**.
    Si procederà quindi al test delle porte server che sono state inserite, e verranno configurate le regole in entrata per Windows Firewall.
13. La pagina **Allowed mail user agents** consente di specificare i Mail User Agent (ovvero le applicazioni client di posta elettronica) che sono autorizzati a connettersi al proxy EAS. Quando un client si connette al proxy di EAS utilizzando un'applicazione di posta non specificata, la richiesta viene respinta.
    - Selezionare **Allow all mail user agents** per configurare l'assenza di restrizioni.
    - Selezionare **Only allow the specified mail user agents** e successivamente selezionare un utente e-mail dall'elenco. Cliccare su **Add** per aggiungere la voce all'elenco di agenti autorizzati. Ripetere questa procedura per tutti i Mail User Agent a cui è consentito connettersi al proxy EAS.
14. Nella pagina **Sophos Mobile EAS Proxy - Configuration Wizard finished**, cliccare su **Finish** per chiudere la procedura guidata di configurazione e tornare alla procedura guidata di impostazione.
15. Nella procedura guidata di impostazione, verificare che sia selezionata la casella **Start Sophos Mobile EAS Proxy server now**, e successivamente cliccare su **Finish** per completare la configurazione e avviare il proxy di EAS di Sophos Mobile per la prima volta.

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

16. Accedere a Sophos Mobile Admin come super administrator.
17. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Proxy EAS**.
18. Sotto **Esterno**, cliccare su **Carica file**. Caricare il certificato creato durante la configurazione.

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

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

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

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

Quando il proxy di EAS standalone viene impostato in modalità PowerShell, si connette al server di posta di Exchange tramite PowerShell e imposta l'accesso alla posta elettronica in base allo stato di conformità del dispositivo.

In modalità PowerShell, il traffico di posta viene inviato dal server di posta di Exchange direttamente ai dispositivi, senza un proxy. Per uno schema del flusso di comunicazione di PowerShell, consultare la Sophos Mobile Guida alla distribuzione.

Vantaggi della modalità PowerShell:

- Non occorre aprire sul server Sophos Mobile una porta dedicata al traffico e-mail in entrata proveniente dai dispositivi.
- È possibile impedire ai dispositivi che non sono registrati a Sophos Mobile di accedere alle e-mail.

Il server di posta di Exchange può essere un server di Exchange o Exchange Online che fa parte di Office 365. Le versioni supportate sono:

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

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

Per impostare il controllo dell'accesso alle e-mail tramite PowerShell, procedere come segue.

Informazioni correlate
Guida alla distribuzione di Server di Sophos Mobile (in inglese)

Configurazione di PowerShell

1. Richiesto: Se richiesto, installare Windows PowerShell sul computer su cui si desidera installare il proxy di EAS.
2. Aprire PowerShell con privilegi di amministratore ed eseguire il seguente comando:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

Il server di Exchange richiede una configurazione aggiuntiva:

3. Aprire Exchange Management Shell.
4. Impostare il criterio di esecuzione di PowerShell:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

5. Ottenere il nome della directory virtuale di PowerShell:

   ```
   Get-PowerShellVirtualDirectory -Server <nome server>
   ```

   <nome server> è il nome del computer su cui è installato il server di Exchange.

   In un'installazione standard, la directory virtuale di PowerShell è `PowerShell (Default Web Site)`.

6. Impostare un'autenticazione di base per la directory virtuale di PowerShell:

   ```
   Set-PowerShellVirtualDirectory -Identity "PowerShell (Default Web Site)"
    -BasicAuthentication $true
   ```

Informazioni correlate

Installazione di Windows PowerShell (documento Microsoft)

Aprire Exchange Management Shell (documento Microsoft)

Creazione di un account di servizio

Un account di servizio è un account utente speciale sul server di posta di Exchange che viene utilizzato da Sophos Mobile per eseguire i comandi di PowerShell.

1. Accedere alla console di amministrazione richiesta:
   - Per Exchange Server: **Interfaccia di amministrazione di Exchange**
   - Per Exchange Online: **Interfaccia di amministrazione di Office 365**
2. Creare un account utente.
   - Utilizzare un nome utente come ad es. `smc_powershell`, che descriva lo scopo dell'account.
   - Disattivare l’impostazione che prevede la modifica della password da parte dell’utente all’accesso successivo.
   - Rimuovere eventuali licenze Office 365 automaticamente assegnate al nuovo account. Gli account di servizio non richiedono alcuna licenza.
3. Creare un nuovo gruppo di ruoli e assegnarvi le autorizzazioni richieste.
   - Adoperare un nome per il gruppo di ruoli quale ad es. `smc_powershell`.
   - Aggiungere i ruoli **Mail Recipients** e **Organization Client Access**.
   - Aggiungere l'account utente come membro.

Configurazione della connessione PowerShell

1. Utilizzare l'Impostazione Assistita analogamente a quando si installa un proxy di EAS standalone. Nella pagina **EAS Proxy instance setup**, configurare le seguenti impostazioni:
   - **Instance type**: Selezionare **PowerShell Exchange/Office 365**.
   - **Instance name**: Un nome che identifica l'istanza.
   - **Exchange server**: Per Exchange Server, immettere il nome o l'indirizzo IP del proprio server.

     Per Exchange Online, immettere `outlook.office365.com`, se si utilizza il servizio Office 365 globale. Per altri servizi, ad esempio Office 365 Germany, l'indirizzo viene indicato nel documento Microsoft Connettersi a PowerShell per Exchange Online.

     Non immettere il protocollo `https://` o il suffisso `/powershell-liveid` nel nome, in quanto la procedura guidata di installazione li aggiunge automaticamente.
   - **Allow all certificates**: Il proxy di EAS non verifica il certificato del server. Selezionare questa opzione se ad esempio si utilizza il server di Exchange con un certificato autofirmato.

     Avviso
     Questa impostazione riduce la protezione delle connessioni del server di posta. Selezionare questa opzione solo se richiesta dall'ambiente di rete.

   - **Service account**: Il nome dell'account utente creato nella console di amministrazione del server di Exchange o di Exchange Online.
   - **Password**: La password dell'account utente.
2. Cliccare su **Add** per aggiungere l'istanza all'elenco **Instances**.
3. Ripetere i passaggi di cui sopra per impostare connessioni PowerShell ad altre istanze del server di Exchange.
4. Completare l'impostazione.
5. Richiesto: Se necessario, configurare un server proxy che il proxy di EAS possa utilizzare per connettersi al server di Exchange o a Exchange Online. Sul computer in cui è stato installato il proxy di EAS, aprire un prompt dei comandi utilizzando l'opzione **Esegui come amministratore** e digitare il comando seguente:

   ```
   netsh winhttp set proxy <nome server o IP>:<porta>
   ```

   Avviso
   Questo comando configura un proxy a livello di sistema e potrebbe avere ripercussioni su altri programmi in esecuzione nel computer.

Informazioni correlate
Connettersi a PowerShell per Exchange Online (documento Microsoft)

Upload del certificato di PowerShell

Caricare il certificato della connessione PowerShell su Sophos Mobile.

1. Accedere a Sophos Mobile Admin come super administrator.

2. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione Sophos** e successivamente sulla scheda **Proxy EAS**.
3. Richiesto: In **Generale**, selezionare **Limita a Sophos Secure Email** per limitare l'accesso alle e-mail all'app Sophos Secure Email, disponibile per Android e iOS.
4. Sotto **Esterno**, cliccare su **Carica file**. Caricare il certificato creato durante la configurazione.

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

5.5 Blocco dell'accesso alle e-mail per i dispositivi non gestiti

È possibile impedire ai dispositivi che non sono registrati a Sophos Mobile di accedere alle e-mail.

Prerequisito: Aver impostato il proxy di EAS standalone in modalità PowerShell.

In queste istruzioni, il termine "Exchange" definisce il server di Exchange on-premise, oppure il proprio piano Exchange Online incluso in Office 365.

È possibile configurare Exchange in modo che metta in quarantena i dispositivi non gestiti. Gli utenti riceveranno un'e-mail in cui si richiede di registrare il dispositivo a Sophos Mobile. Dopo la registrazione, il dispositivo verrà automaticamente rimosso dalla quarantena.

Avviso
Prima di applicare queste impostazioni in un ambiente di produzione, verificare che i dispositivi siano registrati e che sia possibile effettuarne la sincronizzazione con Sophos Mobile. Tutti i dispositivi verranno messi in quarantena per impostazione predefinita e avranno accesso alle e-mail solo se il server di Sophos Mobile li imposta come conformi.

Inoltre, i dispositivi registrati verranno messi in quarantena se il proxy di EAS non ne conosce lo stato di conformità. Questo può accadere quando un dispositivo non si sincronizza con Sophos Mobile da un periodo di tempo eccessivo, oppure quando il proxy di EAS non è in grado di comunicare con il server di Sophos Mobile.

Per bloccare l'accesso alle e-mail per i dispositivi non gestiti:

1. Aprire Exchange Management Shell (se si ha un server di Exchange), oppure connettersi a PowerShell per Exchange Online.

   Per informazioni dettagliate, vedere i link nelle informazioni correlate.
2. Eseguire il seguente comando (in un'unica riga):

```
Set-ActiveSyncOrganizationSettings -DefaultAccessLevel quarantine
-UserMailInsert "Registrare il dispositivo a Sophos Mobile."
```

   Il testo specificato con `-UserMailInsert` sarà aggiunto all'e-mail di notifica che Exchange invierà agli utenti quando il dispositivo viene messo in quarantena.

Per ulteriori informazioni generali su come controllare l'accesso alle e-mail, consultare il documento Microsoft Controlling Exchange ActiveSync device access using the Allow/Block/Quarantine list (Controllo dell'accesso ai dispositivi con Exchange ActiveSync tramite l'elenco Autorizza/Blocca/Quarantena).

Informazioni correlate

Impostazione del proxy di EAS standalone in modalità PowerShell (pagina 16)
Quando il proxy di EAS standalone viene impostato in modalità PowerShell, si connette al server di posta di Exchange tramite PowerShell e imposta l'accesso alla posta elettronica in base allo stato di conformità del dispositivo.

Aprire Exchange Management Shell (documento Microsoft)

Connettersi a PowerShell per Exchange Online (documento Microsoft)

Controlling Exchange ActiveSync device access using the Allow/Block/Quarantine list (Controllo dell'accesso ai dispositivi con Exchange ActiveSync tramite l'elenco Autorizza/Blocca/Quarantena, documento Microsoft)

6 Bilanciamento del carico e disponibilità elevata

Sophos Mobile consente di impostare un ambiente a disponibilità elevata. Garantisce la la costante accessibilità esterna al server di SMC, e permette di elaborare ulteriormente le operazioni, anche in seguito a un eventuale errore di un nodo del server di Sophos Mobile. Per ottenere questi risultati è richiesto il bilanciamento del carico, che distribuisce tra i nodi disponibili le sessioni di client e browser mediante Round Robin DNS.

Quanto segue descrive l'impostazione del clustering per Sophos Mobile e la configurazione del bilanciamento del carico tramite Sophos UTM.

6.1 Requisiti

- Un server Windows diverso per ciascun nodo di Sophos Mobile.
- Tutti i nodi devono essere situati nella stessa rete.
- Un server o cluster di database Microsoft SQL o MySQL.
- Sophos UTM o Apache Reverse Proxy (mod_proxy) per il bilanciamento del carico. Il bilanciamento del carico deve supportare cookie di sessione permanenti e certificati SSL/TLS officiali per server web.

Nota
Per informazioni dettagliate sui requisiti di installazione, consultare Note di rilascio di Sophos Mobile 9.6 (in inglese).

Architettura

Per un esempio di cluster a tre nodi di Sophos Mobile, consultare la Guida alla distribuzione di Server di Sophos Mobile (in inglese).

Opzionalmente, per la comunicazione multicast tra i singoli nodi individuali di Sophos Mobile, è possibile utilizzare una rete a parte. L'interfaccia di rete da utilizzare può essere selezionata durante la configurazione del cluster, come descritto nella sezione Impostazione del primo nodo (pagina 22). Deve anche essere una VLAN.

Nota
Se si desidera utilizzare un secondo cluster di Sophos Mobile a scopo di test, occorrerà una rete separata.

Porte e protocolli

La seguente tabella mostra le porte e i protocolli richiesti per la comunicazione tra i singoli nodi individuali di un cluster di server di Sophos Mobile.

Protocollo	Porte	Destinazione
TCP	7600, 8181, 57600	*<In entrata>*
TCP	7600, 8181, 57600	*<In uscita>*
UDP	45700	*<In entrata>*

Certificati del server

Durante l'impostazione di Sophos Mobile, viene configurato un certificato server web SSL/TLS che consente all'app Sophos Mobile Control di stabilire una connessione sicura al server di Sophos Mobile. Si consiglia di utilizzare un'autorità di certificazione (Certificate Authority, CA) attendibile a livello globale. In un ambiente di cluster in cui sono presenti vari nodi di server di Sophos Mobile dietro a un bilanciatore di carico, questo accorgimento potrebbe non essere pratico. Potrebbe essere consigliabile utilizzare un certificato autofirmato al posto di questa opzione.

Attività correlate

Richiesta di un certificato SSL/TLS (pagina 5)
Inclusa tra i file del prodotto Sophos, si trova la procedura guidata "SSL Certificate Wizard" per la richiesta del certificato SSL/TLS per il proxy di EAS di Sophos Mobile.

6.2 Impostazione di nodi cluster

Per impostare un ambiente di cluster, installare il primo nodo come indicato nella sezione Installazione e impostazione del server di Sophos Mobile (pagina 6). I cluster veri e propri vengono poi attivati utilizzando la **Procedura guidata di configurazione**.

Per tutti gli altri nodi, occorre selezionare il database creato durante l'installazione del primo nodo, e attivare il clustering.

Nota
È anche possibile configurare un server di SMC già esistente per il clustering, e l'ambiente può essere esteso aggiungendo altri nodi.

6.2.1 Impostazione del primo nodo

1. Installare Sophos Mobile come descritto nella sezione Installazione e impostazione del server di Sophos Mobile (pagina 6) e annotare il nome del database creato. Specificare questo database durante l'installazione di ulteriori nodi.
2. Al termine dell'installazione, deselezionare l'opzione **Start Sophos Mobile server now** nella finestra di dialogo **Sophos Mobile - Installation finished**.

Nota
Se il servizio Sophos Mobile è già stato avviato, verrà arrestato automaticamente e riavviato durante la configurazione descritta in questa sezione. In alternativa, è possibile arrestare il servizio manualmente dal menù dell'icona dell'area di notifica di Sophos Mobile.

3. Sul server, cliccare su **Start**, selezionare **Sophos Mobile** e cliccare su **SMC Configuration Wizard**.
4. Verrà visualizzata la pagina **Welcome** della procedura guidata Sophos Mobile Configuration Wizard. Cliccare su **Next**.
5. Nella pagina **Database Selection**, selezionare **Skip database configuration** e cliccare su **Next**.
6. Nella pagina **Choose configuration steps**, selezionare **Configure cluster support** e cliccare su **Next**.
7. Nella pagina **Cluster Configuration**, adoperare il menù a discesa delle interfacce di rete disponibili per selezionare l'interfaccia da utilizzare per la comunicazione multicast tra il nodo del server che si sta impostando e gli altri nodi.
8. Procedere con le altre pagine della procedura guidata di configurazione. Accertarsi di cliccare su **Yes** quando viene richiesto se si desidera avviare il servizio SMC.
   La configurazione del primo nodo del server di SMC è ora completata. Cliccare su **Finish** nella finestra di dialogo **Sophos Mobile - Configuration Wizard finished**.

6.2.2 Impostazione di altri nodi

1. Avviare l'installazione di Sophos Mobile come descritto nella sezione Installazione e impostazione del server di Sophos Mobile (pagina 6).
2. Nella pagina **Database selection**, selezionare il database creato durante l'installazione del primo nodo, e cliccare su **Next**.

   Verrà visualizzata la finestra di dialogo **Database configuration**. Mostra l'avanzamento del processo di configurazione.
3. Nella pagina **Database configuration**, attendere il completamento del processo di configurazione, e cliccare su **Next**.
4. Nella pagina **Choose configuration steps**, selezionare **Configure cluster support** e cliccare su **Next**.
5. Nella pagina **Configure server certificate**, creare un certificato autofirmato, come descritto nella sezione Installazione e impostazione del server di Sophos Mobile (pagina 6) e cliccare su **Next**.
6. Nella pagina **Cluster Configuration**, adoperare il menù a discesa delle interfacce di rete disponibili, per selezionare l'interfaccia del nodo del server di Sophos Mobile che si sta per impostare, e cliccare su **Next**.
7. Procedere con le altre pagine della procedura guidata di configurazione. Nella pagina **Sophos Mobile - Installation finished**, selezionare **Start Sophos Mobile server now** per avviare il nodo del cluster appena configurato.
8. Se nel primo nodo il componente server web di Sophos Mobile è stato configurato in modo tale da accettare solamente le richieste dirette al proprio nome di dominio, ripetere questo passaggio per tutti gli altri nodi. Vedere Configurazione del server web di Sophos Mobile (pagina 9).

Se occorre, ripetere questa procedura per configurare altri nodi.

6.3 Impostazione del bilanciamento del carico con Sophos UTM

Questa sezione descrive come impostare Sophos UTM come bilanciatore del carico per un cluster di nodi del server di Sophos Mobile. Per ulteriori informazioni sulla configurazione di Sophos UTM, consultare la documentazione di Sophos UTM.

Nota

- Per poter utilizzare Sophos UTM, occorre una licenza Sophos UTM con sottoscrizione **Sophos Webserver Protection**.
- Come vedremo in questa sezione, occorre specificare un certificato per proteggere la comunicazione tra i dispositivi gestiti e il server web virtuale che è stato impostato in Sophos UTM. Per semplificare il processo, si consiglia di utilizzare lo stesso certificato adoperato per il server di Sophos Mobile (vedere Richiesta di un certificato SSL/TLS (pagina 5)). Se è stato utilizzato un certificato autofirmato, sarà obbligatorio adoperare lo stesso certificato.

1. Accedere alla WebAdmin di Sophos UTM.
2. Dalla sezione del menù di WebAdmin che si chiama **Webserver Protection**, selezionare la scheda **Web Application Firewall > Server web fisici**.
3. Cliccare su **Nuovo server web fisico** per creare un nodo di SMC.
4. Nella finestra di dialogo **Aggiungi server web fisico**, inserire le seguenti impostazioni:
   a) **Nome**: Inserire un nome descrittivo per il server web (ad esempio `Nodo di SMC`).
   b) **Host**: Selezionare o aggiungere un host. Selezionare un host cliccando sul simbolo raffigurante una cartella vicino al campo **Host**. Trascinare un host dall'elenco di host disponibili al campo **Host**.
      Per ulteriori informazioni su come aggiungere una definizione, consultare la sezione *Definizioni di rete* della Guida all'amministrazione con UTM.
   c) **Tipo**: Selezionare **Cifrato/a (HTTPS)**.

   Cliccare su **Salva** per salvare la configurazione.

   Ripetere il passaggio precedente per ciascun nodo del server di Sophos Mobile.
5. Dalla sezione **Webserver Protection** del menù di WebAdmin, selezionare la scheda **Gestione dei certificati > Certificato**.
6. Cliccare su **Nuovo certificato** per caricare un certificato server web SSL/TLS.
7. Nella finestra di dialogo **Aggiungi certificato**, inserire le seguenti impostazioni:
   a) **Nome**: Inserire un nome descrittivo per il certificato.
   b) **Metodo**: Selezionare **Carica**.
   c) **Tipo di file**: Selezionare **PKCS#12(Cert+CA)**
   d) **Password**: Inserire la password per il file di certificato.
   e) **File**: Cliccare sull'icona raffigurante una cartella accanto alla casella **File**, selezionare il certificato che si desidera caricare e cliccare su **Avvia upload**.

   Cliccare su **Salva** per salvare la configurazione. Il certificato viene aggiunto all'elenco di **Certificati**.
8. Dalla sezione **Webserver Protection** del menù di WebAdmin, selezionare la scheda **Web Application Firewall > Server web virtuali**.
9. Cliccare su **Nuovo server web virtuale** per aggiungere un server web virtuale per il cluster.
10. Nella finestra di dialogo **Aggiungi server web virtuale**, inserire le seguenti impostazioni:
    a) **Nome**: Inserire un nome descrittivo per il server web virtuale (ad esempio `Cluster di SMC`).
    b) Nell'elenco **Interfaccia**, selezionare l'interfaccia WAN tramite la quale il cluster deve essere accessibile dall'esterno.
    c) **Tipo**: Selezionare **Cifrato/a (HTTPS) & reindirizza**.
    d) Nell'elenco **Certificato**, selezionare il certificato del server web precedentemente caricato.

e) **Domini** (solamente con certificato con caratteri jolly, ovvero un certificato a chiave pubblica che può essere utilizzato con sottodomini multipli): Inserire i domini di responsabilità del server web, ad esempio `shop.example.com`, oppure utilizzare l'icona **Aziona** per importare un elenco di nomi di dominio.

I domini devono essere inseriti come nomi di dominio completi (FQDN).

È possibile utilizzare un asterisco (*) come carattere jolly per il prefisso del dominio, ad esempio: `*.mydomain.com`. I domini con caratteri jolly vengono considerati impostazioni di fallback. Il server web virtuale avente voce di dominio con carattere jolly viene utilizzato solamente quando non sono stati configurati altri server web con un nome di dominio più specifico.

Esempio: Una richiesta client ad `a.b.c` troverà corrispondenza con `a.b.c` prima di `*.b.c`, e prima di `*.c`.

f) **Server web fisici**: Selezionare i nodi di SMC creati in precedenza.

Nota
Evitare di selezionare un profilo firewall.

Cliccare su **Salva** per salvare la configurazione. Il server viene viene aggiunto all'elenco di **Server web virtuali**.

11. Attivare il server web virtuale.

    Il nuovo server web virtuale è disattivato per impostazione predefinita. Cliccare sul pulsante attiva/disattiva per attivare il server web virtuale. Il colore del pulsante attiva/disattiva dovrebbe ora cambiare da grigio (disattivato) a verde (attivato).
12. Selezionare la scheda **Routing di percorso del sito**.
13. Nell'elenco **Server web virtuali**, selezionare il server web virtuale che è stato aggiunto e cliccare su **Modifica**.
14. Nella finestra di dialogo **Modifica route di percorso del sito**, cliccare su **Avanzate** e selezionare **Abilita cookie di sessione come 'sticky'**.
    Cliccare su **Salva** per salvare la configurazione.

7 Aggiornamento di Sophos Mobile

Le installazioni server di Sophos Mobile possono essere aggiornate direttamente dalle versioni 9 e 9.5 alla versione 9.6.

Le versioni precedenti a queste dovranno prima essere aggiornate a Sophos Mobile 9. Per informazioni più dettagliate, consultare la documentazione di Sophos Mobile 9.

7.1 Aggiornamento del server di Sophos Mobile

Per aggiornare un'installazione server di Sophos Mobile alla versione 9.6, avviare il programma di installazione di Sophos Mobile 9.6, e seguire le istruzioni. Il programma di installazione rileva automaticamente l'eventuale presenza di un'installazione già esistente che richieda l'aggiornamento.

Prima di avviare l'aggiornamento, verrà effettuata una verifica delle proprietà di sistema. Se tutte le verifiche vengono superate, è possibile procedere con l'aggiornamento. Database e file verranno aggiornati automaticamente, senza alcun bisogno dell'interazione degli utenti. Una volta completato l'aggiornamento, il servizio Sophos Mobile si riavvierà.

Nota
Se durante l'installazione iniziale del server di Sophos Mobile è stata utilizzata l'autenticazione Windows, l'opzione **Start Sophos Mobile server now** non sarà selezionabile. Occorrerà avviare il servizio manualmente.

7.2 Operazioni post-aggiornamento

7.2.1 Riconfigurazione del server web di Sophos Mobile

Se il componente server web di Sophos Mobile è stato configurato in modo da accettare solamente le richieste dirette al proprio nome di dominio, occorrerà ripetere questo passaggio dopo l'aggiornamento di Sophos Mobile. Vedere Configurazione del server web di Sophos Mobile (pagina 9).

7.3 Aggiornamento di un cluster del server

Durante il processo di aggiornamento di un cluster di nodi del server di Sophos Mobile, è importante verificare che tutti i nodi siano sempre eseguiti sulla stessa versione e che la versione del server sia identica alla versione del database. Per assicurarsi che vengano rispettati questi requisiti:

1. Arrestare tutti i nodi del server, interrompendo il servizio Sophos Mobile sui computer interessati.
2. Aggiornare il primo nodo come descritto nella sezione Aggiornamento del server di Sophos Mobile (pagina 26).

   Con questa operazione, si aggiornerà anche il database.
3. Avviare il nodo del server aggiornato e verificare che l'aggiornamento sia stato completato correttamente.

4. Aggiornare tutti gli altri nodi del server.

Consiglio
Se si utilizza il proxy di EAS standalone, i dispositivi gestiti potranno accedere al server di posta elettronica anche quando vengono arrestati tutti i nodi del server di Sophos Mobile. Ciò è possibile perché, quando non è connesso al server di Sophos Mobile, il proxy di EAS memorizza nella cache lo stato del dispositivo per un massimo di 60 minuti.

7.4 Aggiornamento di un proxy di EAS standalone

Per aggiornare il proxy di EAS standalone, avviare il programma di installazione del proxy di EAS e seguire le istruzioni. Il programma di installazione rileva automaticamente l'eventuale presenza di un'installazione già esistente che richieda l'aggiornamento.

Se si utilizza un cluster di nodi server per il proxy di EAS dietro a un bilanciatore di carico, è possibile aggiornare questi nodi in maniera individuale e in qualsiasi sequenza.

Consiglio
I nodi del server per il proxy di EAS non devono essere arrestati nello stesso momento. Questo accorgimento garantisce la continuità delle comunicazioni e-mail nei dispositivi mobili durante l'aggiornamento.

8 Riferimento tecnico

8.1 Funzionalità server di Sophos Mobile

Il componente principale del prodotto Sophos Mobile è il server di Sophos Mobile. Le sue caratteristiche principali includono quanto segue:

- Il server è connesso a internet.
- Il server consente di impostare un ambiente a disponibilità elevata.
- L'amministratore controlla il server tramite l'interfaccia web.
- Gli utenti finali possono registrare i propri dispositivi nel portale self-service, oppure possono ottenere dall'amministratore un dispositivo che è già stato predisposto per l’autoregistrazione.
- I dispositivi gestiti si sincronizzano con il server tramite HTTPS.
- È possibile adoperare un database Microsoft SQL Server o MySQL già esistente per salvare informazioni relative a dispositivi e applicazioni. In alternativa, si può consentire al programma di installazione di Sophos Mobile di creare un nuovo database utilizzando Microsoft SQL Server Express.
- Il database può essere situato sullo stesso computer, oppure su uno diverso. Ciò permette di utilizzare cluster di database.
- Il server supporta impostazioni multi-tenant, per permettere la presenza di clienti diversi sullo stesso server.
- L'accesso e-mail è possibile grazie all'uso di un proxy EAS integrato o standalone. Per la variante standalone, si richiede accesso HTTPS al server di SMC.

Il server di Sophos Mobile è stato sviluppato per Java EE (Enterprise Edition). Si installa e si esegue nell'application server WildFly, che ha superato diversi test e che rispetta gli standard di settore.

Il server può essere installato in ambienti virtuali.

8.2 Interfacce web di Sophos Mobile

8.2.1 Interfaccia di amministrazione di Sophos Mobile

Sophos Mobile è gestito per mezzo di un'interfaccia web protetta da login e da un meccanismo di sessione. È possibile implementare criteri per la password. Il controllo dell'accesso permette l'uso di ruoli utente diversi. Questi ruoli possiedono set di diritti di accesso diversi. A ciascun utente è possibile assegnare solamente un ruolo.

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

8.2.2 Interfaccia del Super administrator

Il super administrator viene utilizzato principalmente per impostare e gestire i clienti nel processo di gestione dei dispositivi. Il primo account super administrator viene creato durante l'impostazione di Sophos Mobile. Vedere Installazione e impostazione del server di Sophos Mobile (pagina 6).

Quando si effettua l'accesso come super administrator, si accede al cliente super administrator, anch'esso creato durante l'impostazione di Sophos Mobile. Per il cliente super administrator, Sophos Mobile Admin mostra una vista personalizzata per le operazioni dei super administrator.

8.2.3 Portale self-service

Il Portale self-service è protetto da: accesso, meccanismo di sessione e un criterio password. L'account deve essere impostato dall'amministratore di Sophos Mobile e può essere associato a qualsiasi tenant. Il Portale self-service è progettato in modo da consentire agli utenti finali di registrare i dispositivi su Sophos Mobile. Gli utenti finali hanno inoltre la possibilità di svolgere determinate operazioni sui propri dispositivi, ad esempio il blocco o la formattazione in remoto. Le operazioni che possono essere effettuate variano a seconda della piattaforma e della configurazione del dispositivo. Effettuando l'accesso come amministratore, è possibile configurare le funzionalità del Portale self-service che sono disponibili per gli utenti finali.

Per informazioni su come configurare il portale self-service per gli utenti finali, consultare la Guida per amministratori di Sophos Mobile.

9 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.

10 Note legali