SOPHOS
Security made simple.

Sophos Mobile Control as a Service
Guida di avvio

Versione prodotto: 3.6
Data documento: novembre 2013

Sommario

1 Informazioni sulla guida....3
2 Passaggi chiave....4
3 Primo accesso....5
4 Modifica del nome dell'utente amministratore....6
5 Attivazione della licenza di Sophos Mobile Security....7
6 Verifica della licenza....8
7 Configurazione delle impostazioni generali....9
8 Configurazione degli utenti del portale self-service....11
9 Creazione e caricamento di un certificato APNS....13
10 Configurazione delle connessioni ai server EAS Proxy autonomi....15
11 Configurazione delle regole di conformità....16
12 Creazione di gruppi di dispositivi....18
13 Configurazione dei dispositivi iOS....19
14 Configurazione dei dispositivi Android....22
15 Aggiornamento delle impostazioni del portale self-service....25
16 Gestione degli utenti del portale self-service (utenti finali)....26
17 Supporto tecnico....31
18 Note legali....32

1 Informazioni sulla guida

Questa guida descrive come effettuare la configurazione iniziale di Sophos Mobile Control per la gestione dei dispositivi mobili.

Ulteriori informazioni sono disponibili nella *Guida per amministratori di Sophos Mobile Control*.

questa guida si concentra sulle piattaforme iOS e Android, in quanto si tratta delle piattaforme più comuni. Le impostazioni qui descritte possono essere applicate in modo simile anche ad altri sistemi operativi.

1.1 Terminologia

In questa guida vengono utilizzati i seguenti termini:

Termine	Definizione
Dispositivo	Il dispositivo mobile da gestire (per es. smartphone o tablet).
Client Sophos Mobile Control	Il componente client di Sophos Mobile Control installato nel dispositivo.
Utente finale	L'utente finale del dispositivo.
Console Web	L'interfaccia Web del server utilizzata per gestire il dispositivo.
Provisioning	La procedura che consente di munire i dispositivi del client di Sophos Mobile Control.
Bundle operazioni	Un pacchetto creato nella console Web per unire insieme diverse operazioni da effettuare nei dispositivi in una sola transazione. Sarà possibile unire insieme tutte le operazioni necessarie per completare la registrazione e rendere operativo un dispositivo.
Portale self-service (PSS)	L'interfaccia Web di Sophos Mobile Control che consente agli utenti finali di registrare i propri dispositivi ed effettuare altre operazioni senza dover richiedere l'intervento dell'helpdesk.
Sophos Mobile Security	Un'app di protezione per telefoni Android e tablet gestibili da Sophos Mobile Control. La funzionalità di gestione di Sophos Mobile Security è un modulo opzionale di Sophos Mobile Control. Per la gestione di Sophos Mobile Security da Sophos Mobile Control, è necessario disporre e avere attivata una licenza valida nella console Web di Sophos Mobile Control.
SMSec	Acronimo di Sophos Mobile Security utilizzato nell'interfaccia utente della console Web di Sophos Mobile Control.

2 Passaggi chiave

Per effettuare la configurazione iniziale di Sophos Mobile Control, eseguire i seguenti passaggi:

1. Reimpostare la password, accedere alla console Web di Sophos Mobile Control e cambiare il nome utente dell'amministratore.
2. Opzionale: attivare la licenza di Sophos Mobile Security.

   Nota: la gestione di Sophos Mobile Security è un modulo opzionale di Sophos Mobile Control. Se non è stata acquistata alcuna licenza di Sophos Mobile Security, non sarà necessario eseguire questo passaggio.

3. Verificare la licenza.
4. Configurare le informazioni generali (piattaforme che si desidera utilizzare, criteri password e informazioni di contatto per il supporto tecnico).
5. Configurare le impostazioni per l'utilizzo del portale self-service da parte degli utenti finali.
6. Creare e caricare il certificato per il servizio Apple Push Notification.
7. Opzionale: configurare le connessioni ai server EAS Proxy autonomi.
8. Configurare le regole di conformità.
9. Creare gruppi di dispositivi.
10. Configurare i dispositivi.
11. Aggiornare le impostazioni, gestire gli utenti (vale a dire gli utenti finali) e testare il provisioning del portale self-service.

    Nota: Sophos Mobile Control mette a disposizione diversi metodi per la gestione degli utenti del portale self-service: gestione degli utenti interni ed esterni. I passaggi di configurazione necessari dipendono dal metodo di gestione degli utenti prescelto. Per ulteriori informazioni, consultare la sezione *Gestione degli utenti del portale self-service (utenti finali)* a pagina 26.

3 Primo accesso

Per ragioni di sicurezza, si consiglia di reimpostare la password non appena effettuato l'accesso alla console Web di Sophos Mobile Control per la prima volta.

1. Nella finestra di dialogo di **Accesso** alla console Web, cliccare su **Password dimenticata?**.

   Viene visualizzata la finestra di dialogo **Reimposta password**.

2. Inserire le informazioni relative a **Cliente** e **Utente** reperibili nell'e-mail ricevuta per l'attivazione dell'account di Sophos Mobile Control as a Service, quindi cliccare su **Reimposta**.

   Si riceverà un'email contenente un link che consentirà di reimpostare la password.

3. Cliccare sul link.

   Viene visualizzata la finestra di dialogo di accesso includente un messaggio che informa dell'invio di un'e-mail contenete la nuova password. Questa seconda mail contiene una password generata casualmente.

4. Inserire la password per eseguire l'accesso.

   Si è effettuato l'accesso alla console Web di Sophos Mobile Control e viene richiesto di cambiare la password.

5. Inserire una nuova password. La nuova password deve essere composta da 10 caratteri. Non ci sono regole specifiche sull'uso di caratteri speciali o cifre.

   Nota: Si tratta di un'impostazione predefinita. È possibile modificare i criteri password direttamente nella console Web di Sophos Mobile Control, quindi cambiare la password in base ai nuovi criteri impostati. Per ulteriori informazioni, consultare la sezione *Configurazione dei criteri delle password* a pagina 9.

4 Modifica del nome dell'utente amministratore

Per motivi di sicurezza, si consiglia di cambiare il nome dell'utente amministratore una volta effettuato il primo accesso.

1. Nella barra dei menu della console Web di Sophos Mobile Control, cliccare su **Amministratori**.

   Viene visualizzata la vista **Mostra amministratori**.

2. Cliccare sull'icona a forma di matita **Modifica**, di fianco all'utente **amministratore**.

   Viene visualizzata la vista **Modifica amministratore**.

3. Nel campo **Nome di accesso**, cambiare il nome utente.
4. Inserire il proprio **Cognome** e **Nome**.
5. Inserire il proprio indirizzo **E-mail**.
6. Cliccare sul pulsante **Salva**.

Il nome utente è stato così cambiato. Durante il prossimo accesso utilizzare il nuovo nome utente.

5 Attivazione della licenza di Sophos Mobile Security

Nota: la gestione di Sophos Mobile Security è un modulo opzionale di Sophos Mobile Control. Se non è stata acquistata alcuna licenza di Sophos Mobile Security, non sarà necessario eseguire questo passaggio.

Sophos Mobile Security è un'app di protezione per dispositivi Android e tablet che consente di proteggere i dispositivi da app malevole, oltre che assistere gli utenti finali nel rilevamento di autorizzazioni per app che potrebbero costituire un rischio alla sicurezza aziendale.

Per la gestione di Sophos Mobile Security da Sophos Mobile Control, è necessario disporre e avere attivata una licenza valida nella console Web di Sophos Mobile Control.

1. Nella barra dei menu della console Web, andare a **Impostazioni** e quindi cliccare su **Installazione del sistema**.

   Viene visualizzata la vista **Installazione del sistema**.

2. Nella scheda **Licenza SMSec**, inserire la chiave di licenza ricevuta da Sophos nel campo **Chiave di licenza**, quindi cliccare su **Attiva**.

La licenza di Sophos Mobile Security viene attivata. Il campo **Attiva chiave di licenza** mostra la chiave di licenza attivata. Il campo **Numero di licenze** mostra il numero di client. Il campo **Valido entro** mostra la data di scadenza della licenza.

6 Verifica della licenza

Nota: a Sophos Mobile Control e Sophos Mobile Security viene-applicata una licenza basata sugli utenti. Tutte le licenze attribuite a un utente vengono considerate come un'unica licenza. I dispositivi a cui non è assegnato alcun utente vengono considerati come singoli utenti.

Nella barra dei menu della console Web, cliccare su **Info** e verificare le informazioni relative alla licenza visualizzate nella vista **Info**:

- **SMC:**
  - **Numero di licenze utente**:

    Mostra quanti utenti possono essere gestiti con Sophos Mobile Control.
  - **Licenze utilizzate:**

    Mostra il numero di licenze in uso.
  - **Licenza valida entro:**

    Mostra la data di scadenza della licenza.
- **SMSec:**

  Nota: La gestione di Sophos Mobile Security è un modulo opzionale di Sophos Mobile Control. Se non è stata acquistata e attivata una licenza di Sophos Mobile Security, non viene visualizzata alcuna informazione relativa alla licenza di Sophos Mobile Security.
  - **Numero di licenze utente:**

    Mostra il numero di utenti per cui l'app di Sophos Mobile Security può essere gestita dalla console Web.
  - **Licenze utilizzate:**

    Mostra il numero di licenze in uso.
  - **Licenza valida entro:**

    Mostra la data di scadenza della licenza.

Nel caso di domande o dubbi sulle informazioni visualizzate relative alla licenza, contattare il proprio partner o rappresentante alle vendite Sophos.

7 Configurazione delle impostazioni generali

Le seguenti impostazioni devono essere configurate:

- Piattaforme che si desidera utilizzare
- Criteri password
- Informazioni di contatto per il supporto tecnico, in modo tale da fornire supporto agli utenti in caso di quesiti o problemi

È possibile configurare queste impostazioni utilizzando la funzione **Impostazioni**.

7.1 Configurazione delle piattaforme

Per utilizzare la console Web di Sophos Mobile Control in modo più efficace, è possibile personalizzare l'interfaccia utente per visualizzare solo le piattaforme su cui si lavora.

Nota: configurando le piattaforme viene modificata solo la vista degli utenti al momento collegati, da cui non è possibile disattivare alcuna funzione.

1. Nella barra dei menu della console Web, andare a **Impostazioni** e quindi cliccare su **Generale**.

   Viene visualizzata la vista **Impostazioni generali**.

2. Nella scheda **Privato** sotto **Piattaforme attive**, selezionare le piattaforme che si desidera utilizzare con Sophos Mobile Control:

   - Android
   - iOS
   - Windows Phone 8
   - Windows Mobile

   Nota: questa guida si concentra sulle piattaforme iOS e Android, in quanto si tratta delle piattaforme più comuni. Per ulteriori informazioni su tutte le piattaforme disponibili, consultare la *Guida per amministratori di Sophos Mobile Control*.

   Il menu viene personalizzato in base alle impostazioni selezionate. Gli oggetti non necessari vengono nascosti.

3. Cliccare sul pulsante **Salva**.

7.2 Configurazione dei criteri delle password

Per applicare una protezione efficace delle password, configurare criteri password specifici per gli utenti della console Web di Sophos Mobile Control e del portale self-service. I criteri password che vengono definiti saranno applicati sia alle password nuove che a quelle modificate. Un criterio predefinito impone che le password contengano 10 caratteri.

Nota: I criteri password vengono applicati solo agli utenti del portale self-service gestiti tramite gestione degli utenti interni e agli utenti della console Web per amministratori. Non vengono

applicati agli utenti del portale self-service gestiti tramite gestione degli utenti esterni. Per ulteriori informazioni sui metodi di gestione degli utenti del portale self-service, consultare la sezione *Gestione degli utenti del portale self-service (utenti finali)* a pagina 26.

1. Nella vista **Impostazioni generali**, andare alla scheda **Criteri password**.
2. Sotto **Criteri password per l'utente della console Web di SMC e dell'utente del PSS - Regole**, definire i valori minimi necessari relativi alle password.
3. Sotto **Criteri password per utenti della console Web di SMC e per utenti del PSS - Impostazioni**, definire le seguenti impostazioni:
   - **Intervallo di modifica password (giorni)**: È possibile inserire un valore compreso fra **0** (non è richiesta alcuna modifica delle password) e **730** giorni.
   - **Numero di password precedenti da non riutilizzare**: È possibile selezionare un valore compreso fra **1** e **10**.
   - **Numero massimo di tentativi di accesso non riusciti**: È possibile selezionare un valore compreso fra **2** e **10**.
4. Sotto **Reimposta impostazioni password**, configurare le e-mail in modo tale che vengano inviate agli utenti che hanno richiesto di reimpostare la password.
   a) Nel campo **Creatore**, inserire l'indirizzo e-mail del mittente.
   b) Sotto **E-mail con link di reset**, l'oggetto e il contenuto dell'e-mail sono predefiniti. È possibile modificarlo in base alle proprie necessità. Per ulteriori informazioni, consultare la *Guida per amministratori di Sophos Mobile Control*.

      Nota: non rimuovere il segnaposto _RESET_TOKEN_LINK_ dal contenuto dell'e-mail.

   c) Sotto **E-mail con la nuova password**, l'oggetto e il contenuto dell'e-mail sono predefiniti. È possibile modificarlo in base alle proprie necessità. Per ulteriori informazioni, consultare la *Guida per amministratori di Sophos Mobile Control*.

      Nota: non rimuovere il segnaposto _NEW_PASSWORD_ dal contenuto dell'e-mail.
5. Cliccare sul pulsante **Salva**.

7.3 Configurazione di contatto per il supporto tecnico

1. Nella vista **Impostazioni generali**, andare alla scheda **Contatto tecnico**.
2. Inserire le informazioni relative al supporto tecnico. Sotto **Informazioni aggiuntive**, è possibile inserire ulteriori informazioni utili per il supporto di utenti aventi quesiti o problemi.
3. Cliccare sul pulsante **Salva**.

8 Configurazione degli utenti del portale self-service

È necessario configurare le impostazioni per l'utilizzo del portale self-service da parte degli utenti finali.

1. Nella barra dei menu della console Web, andare a **Impostazioni** e quindi cliccare su **Portale self-service**.

   Viene visualizzata la vista del **Portale self-service**.

2. Nella scheda **Configurazione**, configurare le impostazioni del portale self-service in base alle proprie esigenze. Per ulteriori informazioni su tutte le impostazioni disponibili, consultare la *Guida per super administrator di Sophos Mobile Control*. Se a questo punto non si è certi di quali impostazioni applicare, sarà possibile conservare le impostazioni predefinite per tutte le opzioni.
3. Andare alla scheda **Consenso** e impostare le seguenti configurazioni:

   a) Sotto **Testo del contratto**, configurare i criteri per i dispositivi mobili, declinazioni di responsabilità o testi di contratto che verranno visualizzati come primo passaggio quando gli utenti effettuano la registrazione dei dispositivi. Per poter continuare gli utenti devono confermare di avere lette tale testo.

      Il testo prodotto supporta semplici tag di formattazione HTML Il testo verrà visualizzato nei relativi browser.

   b) Sotto **Testo di post-installazione**, è possibile inserire il testo da visualizzare nel portale self-service dopo il completamento dei primi passaggi dell'installazione automatica, in modo tale da guidare gli utenti durante i successivi passaggi, per esempio nella configurazione del server nelle app iOS o nella configurazione del client e-mail di Android.

      Il testo prodotto supporta semplici tag di formattazione HTML Il testo verrà visualizzato nei relativi browser.

4. Andare alla scheda **E-mail di benvenuto**. In questa scheda è possibile configurare l'e-mail di benvenuto da inviare agli utenti del portale self-service in cui sono incluse le credenziali per l'accesso. L'e-mail è necessaria per consentire agli utenti di accedere al portale self-service.

   Nota: Questa e-mail viene inviata solo agli utenti del portale self-service gestiti tramite gestione degli utenti interni. Per ulteriori informazioni sui metodi di gestione degli utenti del portale self-service, consultare la sezione *Gestione degli utenti del portale self-service (utenti finali)* a pagina 26.

5. Nel campo **Creatore**, inserire l'indirizzo e-mail del mittente. Nel campo **Oggetto**, l'oggetto dell'e-mail è predefinito. È possibile modificarlo in base alle proprie necessità.
6. Nel campo di testo, il contenuto dell'e-mail è predefinito. È possibile modificarlo in base alle proprie necessità. Per ulteriori informazioni, consultare la *Guida per amministratori di Sophos Mobile Control*.

   Nota: Non rimuovere i segnaposto _CUSTOMERNAME_, _LOGINNAME_ e _RESET_TOKEN_LINK dal contenuto dell'e-mail.

7. Cliccare sul pulsante **Salva**.

9 Creazione e caricamento di un certificato APNS

Per utilizzare il protocollo Mobile Device Management (MDM) incorporato nel dispositivo che esegue Apple iOS 4 (o superiore), Sophos Mobile Control deve utilizzare il servizio Apple Push Notification (APN) per attivare i dispositivi iOS.

Prerequisiti:

- Per configurare la piattaforma iOS, consultare la sezione *Configurazione delle piattaforme* a pagina 9.
- Per creare un certificato APNS, utilizzare la procedura guidata per la creazione dei certificati APNS. La procedura guidata è disponibile per il download nella console Web. Nella barra dei menu della console Web, andare a **Impostazioni** quindi cliccare su **Installazione del sistema** e poi sulla scheda **iOS APNS**. Per scaricare la procedura guidata, cliccare sul link di download.

1. Avviare la procedura guidata per la creazione dei certificati APNS cliccando due volte sul file APNS "Certificate Wizard.exe".

   Viene visualizzata la finestra di dialogo di benvenuto della procedura guidata per la creazione del certificato APNS.

2. Cliccare su **Avanti**.

   Viene visualizzata la finestra di dialogo **Contratto di licenza**.

3. Cliccare su **Do il consenso**.

   Viene visualizzata la finestra di dialogo per la **Richiesta di firma dei certificati**.

4. Inserire il **Nome dell'azienda** e il codice del **Paese** (per es. US o UK). Questi campi sono obbligatori.

   Nota: sotto questi campi, la finestra di dialogo mostra dove vengono archiviati tutti i dati relativi al processo. Annotare questa informazione.

5. Cliccare su **Avanti**.

   Viene visualizzata la finestra di dialogo **Caricamento PLIST**.

6. In questo passaggio, caricare la richiesta di firma del certificato in Apple. Seguire le istruzioni visualizzate nella finestra di dialogo:

   a) Aprire nel browser il sito Web di Apple indicato nella finestra di dialogo.

Nota: non utilizzare Internet Explorer per aprire il sito di Apple perché ciò potrebbe causare problemi. Utilizzare invece Firefox, Chrome o Safari. Si consiglia di utilizzare le versioni più recenti dei browser.

b) Accedere utilizzando l'ID Apple. Nel caso non si disponga di ID Apple, cerarne una.

c) Nella prima finestra di dialogo dell'**Apple Push Certificates Portal**, cliccare su **Create a Certificate**.

d) Accettare i termini e le condizioni.

e) Cercare la richiesta di firma dei certificati (*.plist) e cliccare su **Upload**.

È possibile trovare il nome e il percorso nella finestra di dialogo **Caricamento PLIST** della procedura guidata per la creazione dei certificati APNS di Sophos.

Viene così creato il certificato push di Apple.

f) Scaricare e salvare il file del certificato (*.pem) nella directory indicata nella finestra di dialogo **Caricamento PLIST**.

7. Cliccare su **Avanti**.

   Viene visualizzata la finestra di dialogo **Crea P12**.

8. In questo passaggio, viene creato il certificato APNS per Sophos Mobile Control. Inserire una password per il certificato APNS. Questa password verrà richiesta successivamente, quando si caricherà il file del certificato .P12 in Sophos Mobile Control.

   Nota: la finestra di dialogo **Crea P12** mostra la directory in cui verrà archiviato il certificato. Memorizzare questa informazione. Si consiglia di creare un backup della cartella in cui vengono conservati i certificati.

9. Cliccare su **Avanti**.

   Viene visualizzata la finestra di dialogo di **conclusione della procedura guidata di creazione dei certificati APNS di Sophos Mobile Control**.

10. Cliccare su **Fine**.
11. Nella barra dei menu della console Web, andare a **Impostazioni** quindi cliccare su **Installazione del sistema** e poi sulla scheda **iOS APNS**.
12. Andare alla p.12 del file del certificato appena creato e inserire la password. In alternativa è possibile inserire l'ID Apple come riferimento futuro. Cliccare su **Carica**.

    Una volta caricato il file, nell'intestazione viene visualizzato un messaggio di conferma e vengono visualizzate le informazioni su **Argomento**, **Tipo** e **Data di scadenza** del certificato APNS.

13. Cliccare su **Salva**.

10 Configurazione delle connessioni ai server EAS Proxy autonomi

Sophos Mobile Control consente di impostare un server EAS Proxy esterno completo di più istanze. A questo scopo Sophos Mobile Control offre un programma di installazione per EAS Proxy separato. Per informazioni su funzioni e scenari di utilizzo, consultare la *Guida all'installazione di Sophos Mobile Control.* Il programma di installazione per EAS Proxy è disponibile per il download nella console Web, sotto **Impostazioni** > **Installazione del sistema** nella scheda **EAS Proxy**.

Per configurare la connessione a un server EAS Proxy autonomo, eseguire il programma di installazione EAS proxy. Per ulteriori informazioni sui singoli passaggi, consultare la *Guida all'installazione di Sophos Mobile Control*. Per completare la configurazione, è necessario caricare il certificato generato durante l'impostazione nella console Web.

10.1 Caricamento del certificato di EAS Proxy

1. Nella barra dei menu della console Web, andare a **Impostazioni** e quindi cliccare su **Installazione del sistema**.

   Viene visualizzata la vista **Installazione del sistema**.

2. Andare alla scheda **EAS Proxy**, cercare il certificato e cliccare su **Carica**.

   Il certificato viene così caricato e visualizzato nella scheda **EAS Proxy**.

3. Cliccare sul pulsante **Salva**.

   Nota: Il certificato deve essere caricato prima di poter avviare il server EAS Proxy. In caso contrario, Sophos Mobile Control rifiuta il server e il servizio non potrà essere avviato.

11 Configurazione delle regole di conformità

Nella console Web è possibile:

- Configurare regole di conformità per tutti i tipi di dispositivi (piattaforme) disponibili.
- Definire le azioni che si desidera intraprendere sui dispositivi che risultano non essere più conformi alle regole indicate.
- Definire più regole e assegnarle ai gruppi di dispositivi. Nei gruppi di dispositivi, è possibile scegliere diverse regole specifiche per dispositivi aziendali o privati. Ciò consente l'applicazione di diversi livelli di protezione per differenti gruppi di dispositivi.

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

1. Nella barra dei menu della console Web, cliccare su **Regole di conformità**.

   Viene visualizzato l'elenco delle **Regole di conformità**.

2. Cliccare sul pulsante **Aggiungi**.

   Viene visualizzata la vista **Regole di conformità** comprensiva di schede per tutti i tipi di dispositivi.

3. Inserire un **Nome** e una **Descrizione** per il nuovo set di ruoli di conformità.
4. Andare alla scheda relativa a uno specifico tipo di dispositivo.
5. Verificare che il campo **Abilita piattaforma** sia selezionato.

   Nota: in caso contrario, la conformità dei dispositivi appartenenti alle piattaforme desiderate non potrà essere verificata.

6. Sotto **Regola**, configurare i requisiti di conformità per il tipo di dispositivo selezionato. Per una descrizione di tutte le impostazioni disponibili per ogni tipo di dispositivo, consultare la *Guida per amministratori di Sophos Mobile Control* .
7. Sotto **Rimuovi autorizzazione per Active Sync**, è possibile indicare che l'accesso all'e-mail venga bloccato automaticamente, nel caso in cui i dispositivi risultino non conformi. Selezionare le caselle di spunta necessarie, localizzate di fianco alle relative regole.

   Nota: Questa colonna sarà disponibile solo se è stato configurato un server EAS Proxy (opzionale). Per ulteriori informazioni, consultare la sezione *Configurazione delle connessioni ai server EAS Proxy autonomi* a pagina 15.

8. Per informare gli amministratori nel caso in cui non vengano rispettate le regole stabilite, selezionare la casella di spunta **Notifica amministratore** di fianco alle relative regole.
9. Sotto **Trasferisci bundle delle operazioni**, è possibile scegliere i bundle delle operazioni che si desidera trasferire per le impostazioni della **Regola**. A questo punto lasciare i campi vuoti. 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 adeguati alle regole di conformità, è necessaria una conoscenza approfondita del sistema.
10. Una volta definite tutte le impostazioni in tutte le scheda relative ai tipi di dispositivo necessari, cliccare sul pulsante **Salva**.

11. Nella vista **Regole di conformità** viene visualizzato il nuovo set di regole di conformità.
12. Nel caso in cui si sia scelto che gli amministratori ricevano e-mail di notifica sui dispositivi non conformi, indicare i destinatari di tali e-mail sotto **Destinatari delle e-mail di amministrazione** e il programma delle notifiche, sotto **Conformità dell'orario delle e-mail**. Utilizzare il punto e virgola (;) per separare i diversi amministratori nel campo **Destinatari delle e-mail di amministrazione**. Cliccare sul pulsante **Salva**.

Per aggiungere ulteriori regole di conformità, ripetere i passaggi qui descritti. Una volta creati gruppi di dispositivi vi è possibile assegnare una o più delle regole di conformità qui create. Se si desidera gestire sia dispositivi privati che aziendali, si consiglia di definire impostazioni separate, almeno per questi due tipi di dispositivi.

12 Creazione di gruppi di dispositivi

Si consiglia di organizzare i dispositivi nei gruppi. Ciò ne consentirà una gestione efficace, dal momento che sarà possibile effettuare operazioni sui gruppi piuttosto che ripeterle per ciascun singolo dispositivo.

Nota: si consiglia di unire nello stesso gruppo solo dispositivi aventi lo stesso sistema operativo. Ciò renderà più semplice l'utilizzo dei gruppi per effettuare installazioni e altre operazioni specifiche dei sistemi operativi in esecuzione.

Per creare un nuovo gruppo di dispositivi:

1. Nella barra dei menu della console Web, andare a **Inventario** e quindi cliccare su **Gruppi di dispositivi**.

   Viene visualizzata la vista **Gruppi di dispositivi**.

2. Cliccare sul pulsante **Crea nuovo gruppo di dispositivi**.

   Viene visualizzata la vista **Modifica il gruppo di dispositivi**.

3. Inserire un **Nome** e una **Descrizione** per il nuovo gruppo di dispositivi.
4. Sotto **Regole di conformità**, nei campi **Dispositivi aziendali** e **Dispositivi dei dipendenti**, scegliere le impostazioni di conformità che si desidera applicare.
5. Cliccare sul pulsante **Salva**.

Viene creato un nuovo gruppo di dispositivi e visualizzato nella vista **Gruppi di dispositivi**. È ora possibile aggiungere dispositivi al nuovo gruppo di dispositivi.

Nota: se si cancella un gruppo di dispositivi, i membri di tale gruppo vengono trasferiti a un altro gruppo da specificare. Se non è presente alcun gruppo in cui spostare i dispositivi, il gruppo rimasto non potrà essere cancellato. Prima di cancellare un gruppo viene visualizzato un messaggio di allarme.

13 Configurazione dei dispositivi iOS

13.1 Creazione di profili per dispositivi Apple iOS

In questa sezione si descrive la creazione di un profilo per la configurazione iniziale dei dispositivi iOS. La procedura di configurazione iniziale consigliata include l'impostazione di criteri password ed eventuali restrizioni da applicare ai dispositivi. Si consiglia di includere in profili separati le impostazioni di Exchange, VPN o WiFi.

Nota: Sophos Mobile Control mette a disposizione due metodi di creazione dei profili per dispositivi iOS:

- È possibile creare profili iOS direttamente nella console Web.
- È possibile importare i profili creati utilizzando l'utilità di configurazione di Apple iPhone direttamente nella console Web.

In questa sezione si descrive come creare profili direttamente nella console Web. Per ulteriori informazioni su come importare i profili creati utilizzando l'utilità di configurazione di iPhone, consultare la *Guida per amministratori di Sophos Mobile Control*.

1. Nella barra dei menu della console Web, andare a **Profili** e quindi cliccare su **Apple iOS**.

   Viene visualizzata la vista **Profili**.

2. Cliccare sul pulsante **Crea nuovo profilo**.

   Viene visualizzata la vista **Modifica profilo**.

3. Inserire **Nome** e **Versione** del nuovo profilo.

   Si consiglia di utilizzare il nome "iOS SSP profile" per i profili applicati durante la procedura di registrazione tramite portale self-service.

4. Nel campo **Nome**, inserire l'ID univoco del profilo, per esempio "com.mycompany.smc.baseprofile".

   Nota: caratteri speciali quali dieresi o spazi non sono supportati nelle ID dei profili iOS.

5. Nel campo **Azienda**, inserire il nome dell'azienda relativo al profilo.
6. Nel campo **Descrizione**, inserire una descrizione del profilo, per esempio "profilo di base".
7. Nel campo **L'utente può rimuovere il profilo**, scegliere se l'utente possa o meno rimuovere il profilo dal proprio dispositivo:

   - **Sempre**
   - **Con autenticazione**
   - **Mai**

   Nota: si consiglia di selezionare l'opzione **Mai**.

8. Nel campo **Rimuovi automaticamente il**, è possibile indicare una data per la rimozione automatica del profilo dai dispositivi degli utenti.

   Nota: si consiglia di non impostare alcuna data per la rimozione automatica del profilo.

   Nota: questa funzione è supportata in iOS 6.

9. Sotto **Sistemi operativi**, scegliere il sistema operativo a cui viene applicato il profilo. Selezionare tutte le versioni iOS per questo profilo.
10. Cliccare sul pulsante **Aggiungi** per aggiungere al profilo impostazioni di configurazione per iPhone.

    Viene visualizzata la vista **Configurazioni disponibili**.

11. Scegliere **Criteri password** e cliccare su **Avanti**.

    Viene visualizzata la vista **Criteri password**.

12. Indicare le impostazioni dei criteri password per questo profilo. Per una descrizione dettagliata delle impostazioni disponibili, consultare la *Guida per amministratori di Sophos Mobile Control*.
13. Cliccare sul pulsante **Applica**.

    La configurazione dei **Criteri password** viene visualizzata nella vista **Modifica profilo** sotto **Configurazioni**.

14. Per aggiungere al profilo le impostazioni delle **Restrizioni**, cliccare nuovamente sul pulsante **Aggiungi**.

    Nota: le impostazioni supportate dipendono dalla versione iOS in esecuzione nei singoli dispositivi. A seconda del tipo di dispositivo dell'utente finale, alcune delle impostazioni disponibili potrebbero essere irrilevanti. Per ulteriori informazioni, vedere la matrice di funzione presentata nella *Guida tecnica di Sophos Mobile Control*.

15. Nella vista **Configurazioni disponibili**, selezionare **Restrizioni**, quindi cliccare su **Avanti**.

    Viene visualizzata la vista **Restrizioni**.

16. Indicare le restrizioni per questo profilo. Per una descrizione dettagliata delle impostazioni disponibili, consultare la *Guida per amministratori di Sophos Mobile Control*.
17. Cliccare sul pulsante **Applica**.

    La configurazione delle **Restrizioni** viene visualizzata nella vista **Modifica profilo** sotto **Configurazioni**.

18. Cliccare sul pulsante **Salva**.

Il profilo è ora disponibile per il trasferimento e viene visualizzato nella vista **Profili**. Per configurare profili con impostazioni di Exchange, VPN e WiFi, ripetere i passaggi qui descritti.

13.2 Creazione di bundle delle operazioni per profili iOS

1. Nella barra dei menu della console Web, cliccare su **Bundle delle operazioni**.

   Viene visualizzata la vista **Bundle delle operazioni**.

2. Cliccare sul pulsante **Crea nuovo bundle delle operazioni**.

   Viene visualizzata la vista **Modifica bundle delle operazioni**.

3. Inserire **Nome** e **Versione** del nuovo bundle delle operazioni.

   Si consiglia di utilizzare il nome "OS SSP task bundle" per i bundle delle operazioni applicati durante la procedura di registrazione tramite portale self-service.

4. Sotto **Sistemi operativi**, scegliere i sistemi operativi a cui viene applicata il nuovo bundle delle operazioni. Selezionare tutte le impostazioni iOS per questo bundle delle operazioni.
5. Sotto **Operazioni**, cliccare sul pulsante **Crea una nuova operazione**.

   a) Per prima cosa, selezionare il tipo di operazione **Esegui il bootstrap del client iOS MDM**, quindi cliccare su **Avanti**. Attribuire all'operazione un nome significativo, per esempio "MDM bootstrap", quindi cliccare su **Avanti**.

   b) Aggiungere una seconda operazione del tipo **Installa un profilo iOS**, quindi cliccare su **Avanti**. Selezionare il profilo creato ("iOS SSP profile", nel caso si sia utilizzato il nome consigliato) e cliccare su **Avanti**. Attribuire all'operazione un nome significativo, per esempio "installazione profilo provisioning", quindi cliccare su **Avanti**. Se sono stati configurati profili con impostazioni di Exchange, VPN e WiFi, ripetere questo passaggio per ciascun profilo.

   c) Aggiungere una terza operazione del tipo **Installa un pacchetto software**. Selezionare il pacchetto client di Sophos Mobile Control, quindi cliccare su **Avanti**. Attribuire all'operazione un nome significativo, per esempio "installazione app SMC", quindi cliccare su **Avanti**.

   d) Ripetere questa procedura se si desidera aggiungere ulteriori operazioni. È possibile scegliere l'ordine di installazione delle operazioni selezionate utilizzando le frecce di ordinamento nella parte destra dell'elenco delle **Operazioni**.

6. Una volta aggiunte tutte le operazioni necessarie al bundle delle operazioni, cliccare sul pulsante **Salva** presente nella vista **Modifica bundle delle operazioni**.

Il bundle delle operazioni è ora disponibile per il trasferimento e viene visualizzato nella vista **Bundle delle operazioni**.

14 Configurazione dei dispositivi Android

14.1 Creazione di profili per dispositivi Android

In questa sezione si descrive come configurare un profilo per la configurazione iniziale dei dispositivi Android. La procedura di configurazione iniziale consigliata include l'impostazione di criteri password ed eventuali restrizioni da applicare ai dispositivi. Si consiglia di includere in profili separati le impostazioni di Exchange, VPN o WiFi (se i propri dispositivi Android supportano tali impostazioni). Si consiglia inoltre di caricare in profili separati certificati root e client.

1. Nella console Web, andare a **Profili** e quindi cliccare su **Android**.

   Viene visualizzata la vista **Profili**.

2. Cliccare sul pulsante **Crea nuovo profilo**.

   Viene visualizzata la vista **Modifica profilo**.

3. Inserire **Nome** e **Versione** del nuovo profilo.

   Si consiglia di utilizzare il nome "Android SSP profile" per i profili applicati durante la procedura di registrazione tramite portale self-service.

4. Nel campo **Nome**, inserire l'ID univoco del profilo, per esempio "com.mycompany.smc.baseprofile".
5. Nel campo **Descrizione**, inserire una descrizione del profilo, per esempio "profilo di base".
6. Sotto **Sistemi operativi**, scegliere il sistema operativo a cui viene applicato il profilo. Selezionare tutte le versioni Android per questo profilo.
7. Cliccare sul pulsante **Aggiungi** per aggiungere al profilo configurazioni aventi impostazione per Android.

   Viene visualizzata la vista **Configurazioni disponibili**.

8. Scegliere **Criteri password** e cliccare su **Avanti**.

   Viene visualizzata la vista **Criteri password**.

9. Nel campo **Tipo di password**, indicare il tipo di password che si desidera definire (per es. **Complesso**), quindi cliccare su **Avanti**.
10. Indicare le impostazioni dei criteri password per questo profilo. Per una descrizione dettagliata delle impostazioni disponibili, consultare la *Guida per amministratori di Sophos Mobile Control*.
11. Cliccare sul pulsante **Applica**.

    La configurazione dei **Criteri password** viene visualizzata nella vista **Modifica profilo** sotto **Configurazioni**.

12. Per aggiungere al profilo le impostazioni delle **Restrizioni**, cliccare nuovamente sul pulsante **Aggiungi**.

13. Nella vista **Configurazioni disponibili**, selezionare **Restrizioni**, quindi cliccare su **Avanti**.

    Viene visualizzata la vista **Restrizioni**.

14. Indicare le restrizioni per questo profilo. Per una descrizione dettagliata delle impostazioni disponibili, consultare la *Guida per amministratori di Sophos Mobile Control*.
15. Cliccare sul pulsante **Applica**.

    La configurazione delle **Restrizioni** viene visualizzata nella vista **Modifica profilo** sotto **Configurazioni**.

16. Cliccare sul pulsante **Salva**.

Il profilo è ora disponibile per il trasferimento e viene visualizzato nella vista **Profili**.

14.2 Creazione di bundle delle operazioni per dispositivi Android

1. Nella barra dei menu della console Web, cliccare su **Bundle delle operazioni**.

   Viene visualizzata la vista **Bundle delle operazioni**.

2. Cliccare sul pulsante **Crea nuovo bundle delle operazioni**.

   Viene visualizzata la vista **Modifica bundle delle operazioni**.

3. Inserire **Nome** e **Versione** del nuovo bundle delle operazioni.

   Si consiglia di utilizzare il nome "Android SSP task bundle" per i bundle delle operazioni applicati durante la procedura di registrazione tramite portale self-service.

4. Sotto **Sistemi operativi**, selezionare i sistemi operativi compatibili per il nuovo bundle delle operazioni. Selezionare tutte le impostazioni Android per questo bundle delle operazioni.
5. Sotto **Operazioni**, cliccare sul pulsante **Crea una nuova operazione**.

   a) Come prima operazione, selezionare il tipo di operazione **Installa l'agente MDM**, quindi cliccare su **Avanti**. Selezionare il client Android di Sophos Mobile Control, quindi cliccare su **Avanti**. Attribuire all'operazione un nome significativo quindi cliccare su **Avanti**.

      Nota: il nome qui impostato verrà visualizzato nel portale self-service durante l'elaborazione delle operazioni.

   b) Aggiungere una seconda operazione del tipo **Installa un profilo Android**, quindi cliccare su **Avanti**. Selezionare il profilo creato ("Android SSP profile", nel caso si sia utilizzato il nome consigliato) e cliccare su **Avanti**. Attribuire all'operazione un nome significativo quindi cliccare su **Avanti**. Se sono stati configurati ulteriori criteri, ripetere questo passaggio per ciascun profilo.

   c) Ripetere questa procedura se si desidera aggiungere ulteriori operazioni. È possibile scegliere l'ordine di installazione delle operazioni selezionate utilizzando le frecce di ordinamento nella parte destra dell'elenco delle **Operazioni**.

6. Una volta aggiunte tutte le operazioni necessarie al bundle delle operazioni, cliccare sul pulsante **Salva** presente nella vista **Modifica bundle delle operazioni**.

Il bundle delle operazioni è ora disponibile per il trasferimento e viene visualizzato nella vista **Bundle delle operazioni**. Per creare ulteriori bundle delle operazioni, ripetere i passaggi qui descritti.

15 Aggiornamento delle impostazioni del portale self-service

Una volta creati bundle delle operazioni da trasferire quando gli utenti registrano i propri dispositivi nel portale self-service di Sophos Mobile Control, è necessario aggiornare le impostazioni del portale self-service con le impostazioni di gruppo richieste:

1. Nella barra dei menu della console Web, andare a **Impostazioni** e quindi cliccare su **Portale self-service**.

   Viene visualizzata la vista del **Portale self-service**.

2. Andare alla scheda **Impostazioni del gruppo**.
3. Sotto **Impostazioni del gruppo**, cliccare sull'icona a forma di matita **Modifica**, di fianco al gruppo **Predefinito** del portale self-service.
4. Sotto **Piattaforma** selezionare i tipi di dispositivo che si desidera rendere disponibili nel portale self-service:

   - **Android**
   - **iOS**
   - **Windows Phone 8**
   - **Windows Mobile**

   Nota: questa guida si concentra sulle piattaforme iOS e Android, in quanto si tratta delle piattaforme più comuni. Per ulteriori informazioni su tutte le piattaforme disponibili, consultare la *Guida per super administrator di Sophos Mobile Control*.

5. Nel campo **Aggiungi al gruppo di dispositivi**, selezionare il gruppo di dispositivi registrato tramite portale self-service che deve essere aggiunto.
6. Nel campo **Pacchetto di registrazione**, selezionare i bundle delle operazioni creati per i dispositivi iOS e Android, quindi cliccare su **Applica**.
7. Nella scheda del **Portale self-service**, cliccare sul pulsante **Salva**.

16 Gestione degli utenti del portale self-service (utenti finali)

Sophos Mobile Control mette a disposizione diversi metodi per la gestione degli utenti finali:

- Gestione utenti interni

  Con la gestione degli utenti interni è possibile creare utenti aggiungendoli manualmente alla console Web o importandoli da un file ".csv".

- Gestione utenti esterni

  Con la gestione degli utenti esterni è possibile connettersi a una directory LDAP esistente così da non dover più gestire gli utenti separatamente. È inoltre possibile assegnare dispositivi a gruppi e profili in base alla directory di appartenenza.

Si dovrà a questo punto decidere quale modalità di gestione utilizzare, configurare la modalità prescelta nella console Web, quindi eseguire i passaggi di configurazione necessari.

Nota: Una volta effettuato il collegamento fra dispositivi e utenti agli utenti, non sarà più possibile cambiare il metodo di gestione degli utenti.

16.1 Configurazione del metodo di gestione degli utenti del portale self-service

1. Nella barra dei menu della console Web, andare a **Impostazioni** e quindi cliccare su **Installazione del sistema**.

   Viene visualizzata la vista **Installazione del sistema**.

2. Andare alla scheda **Impostazione utente**. In questa scheda, è possibile selezionare la fonte dei dati per gli utenti del portale self-(PSS) gestiti da Sophos Mobile Control.

   - Selezionare **Directory interna** per utilizzare la gestione degli utenti interni per gli utenti del portale self-service di Sophos Mobile Control.
   - Selezionare **Directory esterna** per applicare la gestione degli utenti esterni agli utenti del portale self-service di Sophos Mobile Control. Per ulteriori informazioni, consultare la sezione *Utilizzo della gestione utenti esterni* a pagina 29.

   Nota: la configurazione della gestione utente non può essere modificata fermo restando che i dispositivi siano collegati alla directory. Se si tenta di modificare la configurazione quando i dispositivi sono ancora collegati, viene visualizzato un messaggio di errore.

3. Cliccare sul pulsante **Salva**.

I successivi passaggi di configurazione dipendono dal metodo di gestione degli utenti prescelto.

- Gestione utenti interni:
  - Creare un utente del portale self-service.
  - Testare il provisioning utilizzando questo utente.

- Importare il proprio elenco utenti.

  Per ulteriori informazioni, consultare la sezione *Utilizzo della gestione utenti interni* a pagina 27.

- Gestione utenti esterni:
  - Configurare la connessione a una directory esterna.
  - Testare il provisioning.

Per ulteriori informazioni, consultare la sezione *Utilizzo della gestione utenti esterni* a pagina 29.

16.2 Utilizzo della gestione utenti interni

16.2.1 Creazione di un utente del portale self-service con gestione utenti internai

Per testare il provisioning tramite portale self-service, creare un proprio account utente del portale self-service. Con questo account utente si potrà effettuare l'accesso al portale self-service.

1. Nella barra dei menu della console Web, cliccare su **Utenti**.

   Viene visualizzata la vista **Mostra utenti**.

2. Cliccare sul pulsante **Crea nuovo utente**.

   Viene visualizzata la vista **Modifica utente**.

3. Inserire le seguenti informazioni relative al nuovo utente del portale self-service:

   a) Verificare che il campo **Invia e-mail di benvenuto** sia selezionato. Il campo viene visualizzato, se si è configurata un'e-mail di benvenuto nella scheda **E-mail di benvenuto per PSS** della vista **Impostazioni**. nel caso in cui questo campo non venga visualizzato, sarà necessario configurare per prima cosa un'e-mail di benvenuto. L'e-mail di benvenuto deve includere tutte le informazioni relative alle credenziali di accesso necessarie.

   b) **Nome utente**

   c) **Cognome**

   d) **Nome**

   e) **E-mail**

   f) **Numero telefonico** (opzionale)

Il nuovo utente del portale self-service viene visualizzato nella vista **Mostra utenti**. All'indirizzo e-mail specificato verrà inviata un'e-mail in cui è inclusa l'URL del portale self-service e le relative credenziali utente.

16.2.2 Test del provisioning tramite portale self-service

Si consiglia di testare su un utente la procedura di provisioning tramite portale self-service, prima di distribuire l'utilizzo del portale self-service a ulteriori utenti.

Accedere al portale self-service utilizzando il relativo account utente creato, quindi registrare il dispositivo ed effettuarne il provisioning. Si consiglia di testare tutte le piattaforme in cui si desidera utilizzare Sophos Mobile Control.

Per ulteriori informazioni su come utilizzare il portale self-service, consultare le *Guide per utenti di Sophos Mobile Control per Android, Apple iOS, Windows Phone 8 e Windows Mobile*.

Nota: questa guida si concentra sulle piattaforme iOS e Android, in quanto si tratta delle piattaforme più comuni. Per ulteriori informazioni su tutte le piattaforme disponibili, consultare la *Guida per amministratori di Sophos Mobile Control*.

16.2.3 Caricamento dell'elenco degli utenti in Sophos Mobile Control

Una volta effettuato il test del provisioning tramite portale self-service, importare l'elenco degli utenti in Sophos Mobile Control.

1. Nella barra dei menu della console Web, cliccare su **Utenti**.

   Viene visualizzata la vista **Mostra utenti**.

2. Cliccare sul pulsante **Importa utenti**.

   Viene visualizzata la vista **Importa utenti**.

   Nel caso non si disponga ancora di un file in formato .csv con l'elenco degli utenti, è possibile scaricare un file campione e utilizzarlo per creare il proprio file di importazione.

3. Verificare che il campo **Invia e-mail di benvenuto** sia selezionato. Il campo è disponibile, se si è configurata una e-mail di benvenuto nella scheda **E-mail di benvenuto** della vista **Impostazioni**, sotto **Portale self-service**. nel caso in cui questo campo non venga visualizzato, sarà necessario configurare per prima cosa un'e-mail di benvenuto. L'e-mail di benvenuto deve includere tutte le informazioni relative alle credenziali di accesso necessarie.
4. Selezionare il file .csv che si desidera importare, quindi cliccare su **Carica file**.

   Le voci del file .csv vengono controllate alla ricerca di eventuali errori e quindi visualizzate nella pagina relativa all'importazione.

   Nota: nel caso di errori nel file .csv, il file non potrà essere importato. Viene visualizzato un messaggio di errore di fianco alle voci coinvolte. Correggere il file .csv e provare di nuovo.

5. Se tutte le voci sono corrette, cliccare sul pulsante **Fine**.

Gli utenti vengono importati e visualizzati nella vista **Mostra utenti**. Gli utenti potranno ora utilizzare il portale self-service per effettuare la registrazione e il provisioning dei dispositivi.

16.3 Utilizzo della gestione utenti esterni

16.3.1 Configurazione della connessione di directory esterne per Active Directory

1. Nella barra dei menu della console Web, andare a **Impostazioni** e quindi cliccare su **Installazione del sistema**.

   Viene visualizzata la vista **Installazione del sistema**.

2. Nella scheda **Impostazione utente**, selezionare **Directory esterna** per utilizzare la gestione degli utenti esterni per gli utenti del portale self-service di Sophos Mobile Control.
3. Cliccare su **Configura directory esterna** per specificare i dettagli del server di directory.

   Viene visualizzata la vista **Dettagli sul server della directory**.

4. In questa vista, inserire le informazioni riportate qui di seguito:

   a) Nel campo **URL principale**, inserire l'URL del server. È possibile inserire l'IP o il nome del server. Selezionare **SSL** per utilizzare SSL come connessione server.

   b) Nel campo **URL di backup**, inserire l'URL del server. È possibile inserire l'IP o il nome del server. Selezionare **SSL** per utilizzare SSL come connessione server.

   c) Nel campo **Utente**, inserire un utente con diritti in lettura del server. Sarà necessario inserire un utente avente il dominio appropriato. I formati supportati sono: <dominio>\<nome utente> o <nome utente>@<dominio>.<codice dominio>.

   d) Nel campo **Password**, inserire la password relativa all'utente specificato.

   Cliccare su **Avanti**.

   Viene visualizzata la vista **Searchbase**.

5. Selezionare la searchbase. La searchbase definisce dove cercare l'utente/gruppo che effettua l'accesso al portale self-service. Cliccare su **Avanti**.

   Viene visualizzata la vista **Campi di ricerca**.

6. In questo passaggio si definisce quali campi debbano essere utilizzati per la risoluzione dei segnaposto %_USERNAME_% e %_EMAILADDRESS_% nei profili. Selezionare i campi richiesti dagli elenchi a discesa **Nome utente** e **E-mail**.

   Nota: i campi elencati sono i campi LDAP definiti per l'utente specificato. Per esempio: se per questo utente non è stato indicato alcun indirizzo e-mail, il campo e-mail non è incluso nell'elenco. È possibile inserire manualmente i nomi dei campi.

   Cliccare su **Avanti**.

   Viene visualizzata la vista **Configurazione PSS di LDAP**.

7. Nel campo **Gruppi PSS**, inserire il nome del gruppo a cui consentire l'accesso al portale self-service. Questo gruppo deve essere definito nel server LDAP. Una volta inserito il gruppo, cliccare sul pulsante **Risolvi gruppo** per sostituire il nome del gruppo con un nome distinto (ND).
8. Cliccare sul pulsante **Fine**.

   Viene visualizzata nuovamente la vista **Installazione del sistema**.

9. Per salvare le modifiche apportate cliccare sul pulsante **Salva**.

16.3.2 Test del provisioning tramite portale self-service

Si consiglia di testare su un utente la procedura di provisioning tramite portale self-service, prima di distribuire l'utilizzo del portale self-service a ulteriori utenti.

Accedere al portale self-service utilizzando le credenziali di Active Directory, quindi registrare il dispositivo ed effettuarne il provisioning. Si consiglia di testare tutte le piattaforme in cui si desidera utilizzare Sophos Mobile Control.

Per ulteriori informazioni su come utilizzare il portale self-service, consultare le *Guide per utenti di Sophos Mobile Control per Android, Apple iOS, Windows Phone 8 e Windows Mobile*.

Nota: questa guida si concentra sulle piattaforme iOS e Android, in quanto si tratta delle piattaforme più comuni. Per ulteriori informazioni su tutte le piattaforme disponibili, consultare la *Guida per amministratori di Sophos Mobile Control*.

17 Supporto tecnico

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

- Visitando la community SophosTalk su *http://community.sophos.com* e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su *http://www.sophos.com/it-it/support.aspx*.
- Scaricando la documentazione del prodotto su *http://www.sophos.com/it-it/support/documentation/mobile-control.aspx*.
- Inviando un'e-mail a *support@sophos.it*, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

18 Note legali

Copyright © 2011 - 2013 Sophos Ltd. Tutti i diritti riservati.

Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos è un marchio registrato di Sophos Ltd. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.